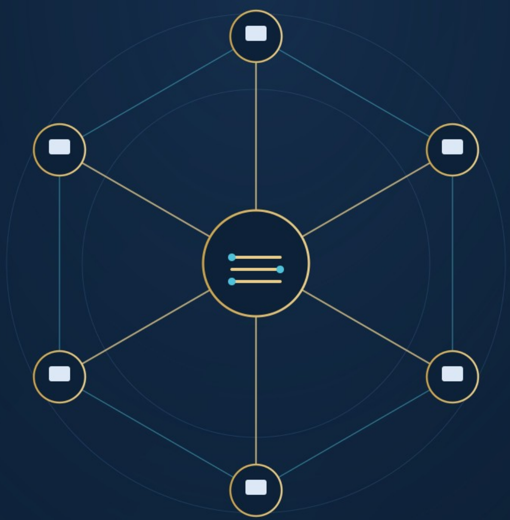
POLITEKNIK NEGERI PADANG
JURUSAN TEKNOLOGI INFORMASI • PROGRAM STUDI D3 TEKNIK KOMPUTER

BUKU AJAR

ENTERPRISE NETWORKING

Perancangan, Konfigurasi, dan Pengamanan Jaringan Komputer Skala Enterprise



Mata Kuliah Enterprise Networking • CEN3302
2 SKS Teori • Semester 3

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

POLITEKNIK NEGERI PADANG
2026

BUKU AJAR

ENTERPRISE NETWORKING

Perancangan, Konfigurasi, dan Pengamanan Jaringan Komputer Skala Enterprise

Mata Kuliah : Enterprise Networking
Kode Mata Kuliah : CEN3302
Bobot : 2 SKS Teori — Semester 3
Program Studi : D3 Teknik Komputer
Institusi : Politeknik Negeri Padang

Disusun oleh:
Ir. H. A. Mooduto, M.Kom.

POLITEKNIK NEGERI PADANG
2026

LEMBAR PENGESAHAN

Buku ajar ini disusun sebagai bahan pembelajaran resmi untuk mata kuliah berikut:

Judul Buku Ajar	:	Buku Ajar *Enterprise Networking*
Mata Kuliah	:	Enterprise Networking
Kode Mata Kuliah	:	CEN3302
Program Studi	:	D3 Teknik Komputer
Jurusan	:	Teknologi Informasi
Institusi	:	Politeknik Negeri Padang
Penulis / Dosen Pengampu	:	Ir. H. A. Mooduto, M.Kom.
NIP / NIDN	:	196605101994031003 / 0010056606

Padang, ... 2026

Mengetahui, Ketua Jurusan Teknologi Informasi	Menyetujui, Ketua Program Studi D3 Teknik Komputer
Dr. Ir. Yuhefizar, S.Kom., M.Kom. NIP. 197601132006041002	Fitri Nova, S.ST., MT. NIP. 198505292014042001

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat dan karunia-Nya penyusunan Buku Ajar Enterprise Networking ini dapat diselesaikan dengan baik. Buku ajar ini disusun sebagai bahan pembelajaran utama bagi mahasiswa Program Studi D3 Teknik Komputer, Politeknik Negeri Padang, pada mata kuliah Enterprise Networking (MKK-EN01).

Mata kuliah Enterprise Networking merupakan mata kuliah pendalaman pada Pilar Keilmuan Jaringan dan Infrastruktur Komputer yang membahas konsep, arsitektur, dan praktik perancangan jaringan komputer skala menengah hingga besar. Kehadiran buku ajar ini dilatarbelakangi oleh kebutuhan akan bahan pembelajaran yang terstruktur, sistematis, dan selaras dengan Rencana Pembelajaran Semester (RPS) yang telah ditetapkan, sehingga proses pembelajaran dapat berlangsung secara terarah menuju ketercapaian Capaian Pembelajaran Lulusan (CPL) Program Studi.

Penyusunan buku ajar ini bertujuan untuk: (1) menyediakan materi pembelajaran yang runtut dan sesuai dengan capaian pembelajaran mata kuliah (CPMK) dan sub-capaian pembelajaran mata kuliah (Sub-CPMK); (2) memberikan panduan praktik konfigurasi jaringan enterprise yang aplikatif; (3) menjadi acuan bagi dosen dan mahasiswa dalam proses belajar-mengajar yang berbasis capaian (outcome-based education); dan (4) mendukung kesiapan mahasiswa dalam menghadapi jalur sertifikasi profesi di bidang jaringan.

Penulis menyampaikan ucapan terima kasih kepada pimpinan Politeknik Negeri Padang, Ketua Jurusan Teknologi Informasi, Ketua Program Studi D3 Teknik Komputer, rekan sejawat dosen, serta seluruh pihak yang telah memberikan dukungan, masukan, dan kontribusi selama proses penyusunan buku ajar ini.

Penulis menyadari bahwa buku ajar ini masih memiliki keterbatasan dan jauh dari kesempurnaan. Oleh karena itu, kritik dan saran yang membangun dari pembaca, baik dosen maupun mahasiswa, sangat diharapkan demi penyempurnaan buku ajar ini pada edisi berikutnya. Semoga buku ajar ini bermanfaat bagi peningkatan kualitas pembelajaran mata kuliah Enterprise Networking.

Padang, Agustus 2026

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

PETUNJUK PENGGUNAAN BUKU AJAR

Buku ajar ini disusun secara sistematis untuk memudahkan mahasiswa mempelajari materi Enterprise Networking secara mandiri maupun terbimbing. Agar pembelajaran berlangsung optimal, mahasiswa disarankan mengikuti panduan penggunaan berikut.

A. Panduan Umum bagi Mahasiswa

- Pelajari setiap bab secara berurutan, karena materi disusun berjenjang dari konsep dasar hingga topik lanjut.
- Perhatikan bagian CPMK dan Sub-CPMK pada awal setiap bab sebagai acuan capaian yang harus dikuasai.
- Baca Tujuan Pembelajaran Khusus (TPK) sebelum mempelajari uraian materi agar fokus belajar lebih terarah.
- Kerjakan Latihan/Soal pada akhir bab secara mandiri sebelum melihat kunci jawaban atau berdiskusi dengan dosen.
- Manfaatkan sesi praktik simulasi (Packet Tracer/GNS3) untuk memperkuat pemahaman konfigurasi yang dibahas.
- Gunakan Daftar Pustaka pada setiap bab untuk memperdalam materi secara mandiri.

B. Struktur Setiap Bab

Setiap bab dalam buku ajar ini disusun dengan struktur baku sebagai berikut:

- CPMK Terkait — capaian pembelajaran mata kuliah yang didukung oleh bab tersebut.
- Sub-CPMK — kemampuan akhir yang diharapkan dapat dicapai pada bab tersebut.
- Tujuan Pembelajaran Khusus (TPK) — rincian operasional capaian belajar yang dapat diukur.
- Peta Konsep — gambaran ringkas alur materi bab.
- Uraian Materi — pembahasan konsep disertai ilustrasi topologi dan contoh konfigurasi.
- Studi Kasus/Lembar Kerja Praktik — skenario simulasi jaringan sesuai pengalaman belajar pada RPS.
- Rangkuman — ringkasan poin-poin penting bab.
- Latihan/Soal — soal pemahaman konsep dan soal konfigurasi/praktik.
- Daftar Pustaka — referensi yang digunakan pada bab tersebut.

DAFTAR ISI

PETA KOMPETENSI / PETA KURIKULUM

A. Posisi Mata Kuliah dalam Struktur Kurikulum

Mata kuliah Enterprise Networking (MKK-EN01) merupakan mata kuliah pendalaman pada Pilar Keilmuan Jaringan dan Infrastruktur Komputer dalam kurikulum Program Studi D3 Teknik Komputer, Politeknik Negeri Padang. Mata kuliah ini ditempatkan pada Semester 3 dengan bobot 2 SKS Teori, sebagai kelanjutan dari mata kuliah dasar jaringan komputer pada semester sebelumnya, dan menjadi bekal bagi mahasiswa untuk mengikuti mata kuliah lanjutan maupun praktik kerja lapangan/tugas akhir yang berkaitan dengan jaringan dan infrastruktur komputer.

B. Peta Kontribusi CPMK terhadap CPL Program Studi

CPMK	Fokus Kompetensi	CPL yang Didukung
CPMK-1	Konsep & model desain jaringan enterprise	CPL-2, CPL-5
CPMK-2	Perancangan & konfigurasi VLAN, Layer 3 switching, routing dinamis, redundansi gateway	CPL-2, CPL-5
CPMK-3	Teknologi WAN dan konektivitas enterprise	CPL-5, CPL-10
CPMK-4	Keamanan dan tata kelola jaringan enterprise	CPL-5, CPL-8
CPMK-5	Dokumentasi teknis dan komunikasi hasil kerja tim	CPL-5, CPL-9
CPMK-6	Jalur pengembangan kompetensi dan sertifikasi profesi	CPL-10

Catatan: pemetaan lengkap CPMK, Sub-CPMK, dan indikator penilaian terhadap kelima CPL Program Studi (CPL-2, CPL-5, CPL-8, CPL-9, CPL-10) mengacu pada Matriks Korelasi CPL–CPMK dan CPL–Sub-CPMK pada dokumen RPS Enterprise Networking, serta dokumen kurikulum OBE Program Studi D3 Teknik Komputer PNP.

BAB 1
PENGANTAR JARINGAN ENTERPRISE

A. PENDAHULUAN

1. Deskripsi Singkat

Bab ini membahas konsep dasar jaringan enterprise sebagai fondasi awal sebelum mahasiswa mempelajari topik-topik lanjut seperti switching, routing dinamis, WAN, dan keamanan jaringan pada bab-bab berikutnya. Pembahasan diawali dengan definisi dan karakteristik jaringan enterprise, dilanjutkan dengan perbandingan sistematis antara jaringan enterprise dan jaringan skala kecil (Small Office/Home Office atau SOHO), kemudian diperdalam melalui pembahasan tiga kebutuhan utama jaringan enterprise, yaitu skalabilitas, ketersediaan (availability), dan keamanan. Bab ini ditutup dengan studi kasus organisasi skala menengah-besar untuk membantu mahasiswa mengaitkan konsep teoretis dengan konteks dunia kerja yang nyata.

Sebagai mata kuliah pendalaman pada Pilar Keilmuan Jaringan dan Infrastruktur Komputer, pemahaman yang kuat terhadap materi pada bab ini menjadi prasyarat konseptual bagi seluruh materi lanjutan pada mata kuliah Enterprise Networking, karena seluruh keputusan desain dan konfigurasi teknis pada bab-bab berikutnya senantiasa berangkat dari kebutuhan bisnis dan karakteristik organisasi yang dibahas di sini.

2. Capaian Pembelajaran Mata Kuliah (CPMK) yang Dicapai

Kode CPMK	:	CPMK-1
Rumusan CPMK	:	Mampu menjelaskan konsep, karakteristik, dan model arsitektur jaringan enterprise sebagai dasar perancangan jaringan skala menengah-besar.
Bobot CPMK	:	14% dari keseluruhan capaian mata kuliah
CPL yang Didukung	:	CPL-2 (penguasaan konsep teoretis bidang teknik komputer) dan CPL-5 (kemampuan merancang, menginstalasi, mengonfigurasi, dan memelihara jaringan komputer)

3. Sub-CPMK yang Dicapai

Kode Sub-CPMK	:	Sub-CPMK 1.1
Rumusan Sub-CPMK	:	Mampu menjelaskan kebutuhan dan karakteristik jaringan enterprise dibandingkan jaringan skala kecil.
Pertemuan	:	Pertemuan ke-1
Indikator Penilaian	:	Ketepatan mengidentifikasi karakteristik jaringan enterprise

(dinilai melalui partisipasi diskusi), bobot 1% dari total penilaian mata kuliah.

4. Tujuan Pembelajaran Khusus (TPK)

Setelah mempelajari bab ini secara tuntas, mahasiswa diharapkan mampu:

1. Menjelaskan definisi jaringan enterprise dan mengidentifikasi minimal tiga karakteristik utama yang membedakannya dari jaringan skala kecil, secara tepat dan disertai contoh nyata.

2. Membandingkan jaringan enterprise dan jaringan SOHO dari aspek skala pengguna, kompleksitas topologi, kebutuhan pengelolaan, serta tingkat kekritisan layanan.

3. Menganalisis kebutuhan skalabilitas, ketersediaan (high availability), dan keamanan pada jaringan organisasi skala menengah-besar berdasarkan studi kasus yang diberikan.

4. Mengaitkan karakteristik jaringan enterprise dengan kebutuhan bisnis riil suatu organisasi multi-lokasi atau multi-divisi.

5. Menumbuhkan kesadaran akan pentingnya perencanaan jaringan yang matang dan sistematis sebagai dasar sebelum tahap perancangan teknis dimulai.

5. Peta Konsep

Alur pembahasan materi pada Bab 1 disajikan dalam peta konsep berikut, yang menggambarkan keterkaitan logis antar-subbab menuju pencapaian Sub-CPMK 1.1.

Definisi & Karakteristik Jaringan Enterprise	→	Perbedaan dengan Jaringan SOHO	→	Kebutuhan Skalabilitas, Ketersediaan & Keamanan	→	Studi Kasus Organisasi

6. Prasyarat

Sebelum mempelajari bab ini, mahasiswa disarankan telah menguasai konsep dasar jaringan komputer, meliputi topologi jaringan, model referensi OSI dan TCP/IP, konsep dasar pengalamatan IP (IPv4), serta perangkat jaringan dasar (switch, router, access point) yang umumnya diperoleh pada mata kuliah jaringan komputer dasar di semester sebelumnya. Penguasaan istilah-istilah dasar tersebut akan sangat membantu mahasiswa memahami karakteristik jaringan enterprise yang dibahas pada bab ini.

B. URAIAN MATERI

1.1 Definisi dan Karakteristik Jaringan Enterprise

a. Penjelasan Konsep/Teori

Jaringan enterprise (enterprise network) adalah infrastruktur jaringan komunikasi data yang dirancang untuk mendukung operasional suatu organisasi berskala menengah hingga besar, yang umumnya memiliki banyak pengguna, banyak departemen atau divisi, dan seringkali tersebar pada lebih dari satu lokasi fisik (multi-site). Berbeda dengan jaringan rumahan atau kantor kecil yang biasanya hanya melayani beberapa hingga puluhan pengguna dengan kebutuhan yang relatif sederhana, jaringan enterprise dirancang untuk melayani ratusan hingga ribuan pengguna dengan berbagai jenis aplikasi bisnis yang berjalan secara bersamaan, seperti sistem informasi manajemen, basis data transaksional, layanan komunikasi (VoIP, video conference), serta aplikasi berbasis cloud.

Terdapat beberapa karakteristik utama yang menjadi ciri khas jaringan enterprise, yaitu sebagai berikut.

- Skala dan Kompleksitas Besar — melibatkan ratusan hingga ribuan perangkat jaringan (switch, router, firewall, access point) yang saling terhubung dalam topologi yang kompleks dan berjenjang.
- Ketersediaan Layanan yang Tinggi (High Availability) — jaringan enterprise umumnya mendukung layanan bisnis yang kritis, sehingga downtime sekecil apa pun dapat menimbulkan kerugian finansial maupun reputasi organisasi.
- Skalabilitas — jaringan harus mampu berkembang mengikuti pertumbuhan organisasi, baik dari sisi jumlah pengguna, jumlah lokasi, maupun jenis layanan yang didukung, tanpa memerlukan perancangan ulang secara menyeluruh.
- Segmentasi dan Tata Kelola yang Terstruktur — jaringan dibagi ke dalam beberapa segmen logis (VLAN, zona keamanan) untuk memisahkan lalu lintas data antar-departemen serta menerapkan kebijakan akses yang berbeda-beda.
- Kebutuhan Keamanan Berlapis — mengingat data dan aset organisasi yang bernilai tinggi, jaringan enterprise memerlukan mekanisme keamanan berlapis (defense in depth) mulai dari firewall, ACL, hingga sistem monitoring.
- Manajemen Terpusat — perangkat jaringan enterprise umumnya dikelola secara terpusat melalui sistem manajemen jaringan (network management system) untuk memudahkan pemantauan dan pemeliharaan.

b. Contoh Aplikasi

Sebagai contoh, sebuah perusahaan perbankan nasional dengan ratusan kantor cabang di berbagai kota memerlukan jaringan enterprise yang menghubungkan seluruh kantor cabang ke pusat data (data center) secara aman dan andal, agar transaksi nasabah dapat diproses secara real-time tanpa gangguan. Contoh lain adalah universitas besar dengan puluhan gedung dan ribuan mahasiswa serta staf yang membutuhkan akses jaringan kampus (baik kabel maupun nirkabel) untuk keperluan akademik, administrasi, dan penelitian secara bersamaan.

1.2 Perbedaan dengan Jaringan Skala Kecil (SOHO)

a. Penjelasan Konsep/Teori

Jaringan SOHO (Small Office/Home Office) adalah jaringan berskala kecil yang biasanya digunakan pada rumah tangga atau kantor kecil dengan jumlah pengguna terbatas, umumnya kurang dari 20 pengguna. Jaringan SOHO biasanya hanya menggunakan satu perangkat all-in-one (router nirkabel) yang menggabungkan fungsi router, switch, access point, dan firewall dasar dalam satu perangkat, dengan konfigurasi yang relatif sederhana dan minim kebutuhan akan redundansi maupun segmentasi jaringan.

Perbedaan mendasar antara jaringan enterprise dan jaringan SOHO dapat dilihat dari beberapa aspek, sebagaimana dirangkum pada Tabel 1.1 berikut.

Aspek	Jaringan Enterprise	Jaringan SOHO
Jumlah Pengguna	Ratusan hingga ribuan pengguna	Beberapa hingga puluhan pengguna
Topologi	Hierarkis/berjenjang, multi-lokasi	Sederhana, satu lokasi
Perangkat	Multi-vendor, terpisah per fungsi (switch, router, firewall)	Umumnya satu perangkat all-in-one
Redundansi	Diperlukan (FHRP, jalur ganda)	Umumnya tidak tersedia
Segmentasi Jaringan	Menggunakan VLAN dan zona keamanan	Umumnya satu segmen jaringan datar (flat network)
Manajemen	Terpusat, menggunakan sistem monitoring	Manual, per perangkat
Kebutuhan Keamanan	Berlapis (ACL, firewall, monitoring)	Dasar (password Wi-Fi, firewall bawaan)
Ketersediaan Layanan	Kritis, menargetkan uptime tinggi	Toleransi gangguan relatif tinggi

Tabel 1.1 Perbandingan Karakteristik Jaringan Enterprise dan Jaringan Skala Kecil

b. Contoh Aplikasi

Sebagai ilustrasi, sebuah toko kelontong dengan tiga karyawan dan satu unit komputer kasir cukup menggunakan satu router nirkabel rumahan yang terhubung langsung ke modem internet — inilah contoh jaringan SOHO. Sebaliknya, jaringan sebuah rumah sakit besar dengan puluhan ruangan, ratusan perangkat medis yang terhubung ke jaringan (medical IoT), serta sistem rekam medis elektronik yang harus selalu tersedia, memerlukan jaringan enterprise dengan segmentasi VLAN per unit layanan, redundansi jalur, dan pengawasan keamanan yang ketat.

1.3 Kebutuhan Skalabilitas, Ketersediaan, dan Keamanan

a. Penjelasan Konsep/Teori

Tiga kebutuhan utama yang mendasari perancangan jaringan enterprise adalah skalabilitas (scalability), ketersediaan (availability), dan keamanan (security). Ketiganya saling berkaitan dan menjadi pertimbangan utama pada seluruh tahap perancangan jaringan yang akan dibahas pada bab-bab selanjutnya.

1) Skalabilitas

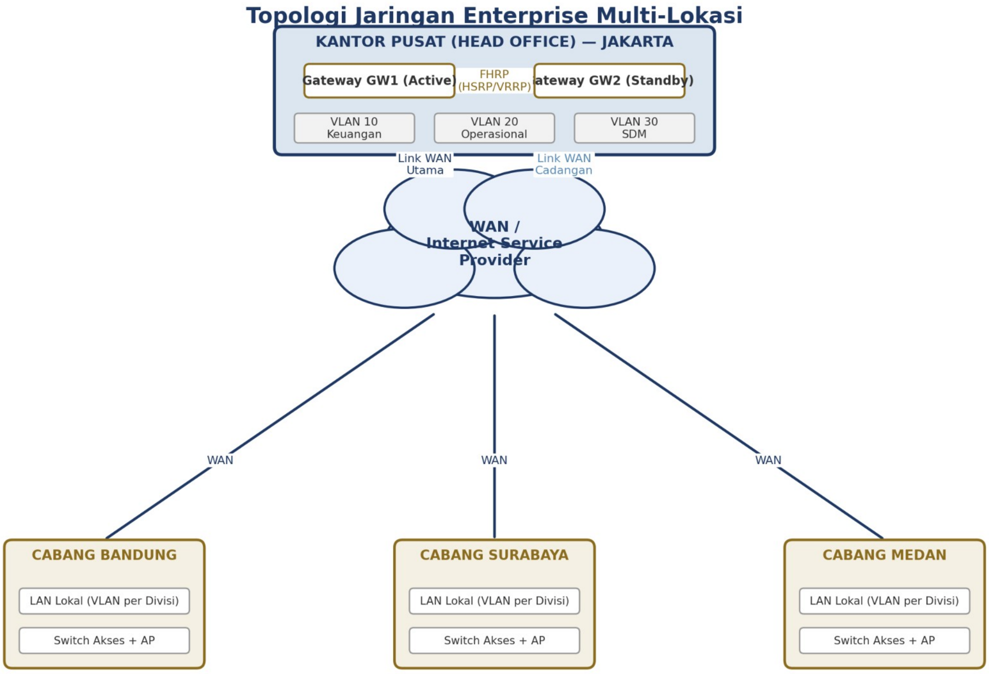
Skalabilitas adalah kemampuan jaringan untuk berkembang mengikuti pertumbuhan organisasi — baik penambahan jumlah pengguna, perangkat, maupun lokasi baru — tanpa memerlukan perombakan arsitektur secara menyeluruh. Jaringan yang skalabel dirancang dengan struktur modular (misalnya model hierarchical three-tier yang akan dibahas pada Bab 2) sehingga penambahan kapasitas dapat dilakukan secara bertahap.

2) Ketersediaan (Availability)

Ketersediaan mengacu pada kemampuan jaringan untuk tetap beroperasi dan dapat diakses oleh pengguna secara konsisten, termasuk pada saat terjadi kegagalan pada salah satu komponennya. Konsep ini erat kaitannya dengan high availability, yang akan dibahas lebih rinci pada Bab 6 melalui penerapan protokol redundansi gateway (HSRP, VRRP, GLBP).

3) Keamanan (Security)

Keamanan jaringan enterprise mencakup perlindungan terhadap data dan aset organisasi dari ancaman internal maupun eksternal, mulai dari kontrol akses (ACL), firewall, hingga pemantauan lalu lintas jaringan secara berkelanjutan. Topik ini akan diperdalam pada Bab 10 hingga Bab 12.



Gambar 1.1 Ilustrasi Topologi Jaringan Enterprise Multi-Lokasi

Diagram di atas menggambarkan sebuah organisasi dengan kantor pusat (head office) di Jakarta yang terhubung ke tiga kantor cabang (Bandung, Surabaya, dan Medan) melalui jalur WAN. Kantor pusat memiliki dua jalur koneksi WAN yang redundan (jalur utama dan jalur cadangan) menuju penyedia layanan, serta dua perangkat gateway (GW1 aktif dan GW2 standby) yang dikonfigurasi dengan protokol redundansi FHRP (HSRP/VRRP) agar layanan tetap tersedia meskipun salah satu jalur atau perangkat mengalami gangguan. Setiap lokasi memiliki jaringan lokal (LAN) yang tersegmentasi ke dalam beberapa VLAN sesuai fungsi/departemen, seperti VLAN Keuangan, Operasional, dan SDM pada kantor pusat.

b. Contoh Aplikasi

Perusahaan e-commerce besar merupakan contoh nyata penerapan ketiga kebutuhan ini secara bersamaan: skalabilitas diperlukan untuk mengantisipasi lonjakan trafik pada masa promosi besar; ketersediaan tinggi diperlukan agar layanan transaksi tidak terhenti sedetik pun; serta keamanan berlapis diperlukan untuk melindungi data pelanggan dan transaksi pembayaran dari serangan siber.

1.4 Studi Kasus Organisasi

a. Penjelasan Konsep/Teori

Untuk memperkuat pemahaman konsep, berikut disajikan sebuah studi kasus organisasi yang dapat digunakan sebagai bahan diskusi kelas.

Studi Kasus: PT Nusantara Retail Group

PT Nusantara Retail Group merupakan perusahaan ritel nasional yang memiliki satu kantor pusat di Jakarta, tiga gudang distribusi regional, dan 85 gerai (outlet) yang tersebar di berbagai kota di Indonesia. Setiap gerai memiliki sistem kasir (Point of Sale) yang harus terhubung secara real-time ke sistem inventori pusat. Kantor pusat juga mengelola sistem informasi sumber daya manusia, keuangan, dan customer relationship management (CRM) yang diakses oleh seluruh cabang.

Pertanyaan diskusi: Identifikasikan karakteristik jaringan enterprise apa saja yang dibutuhkan oleh PT Nusantara Retail Group, serta jelaskan mengapa jaringan SOHO tidak dapat memenuhi kebutuhan organisasi tersebut.

b. Contoh Aplikasi

Studi kasus di atas dapat dikembangkan oleh dosen menjadi diskusi kelompok pada pertemuan pertama, dengan mahasiswa diminta mengidentifikasi minimal tiga karakteristik jaringan enterprise yang relevan dengan konteks PT Nusantara Retail Group, sebagaimana menjadi indikator penilaian partisipasi diskusi pada Sub-CPMK 1.1.

C. RANGKUMAN

- Jaringan enterprise adalah infrastruktur jaringan yang dirancang untuk mendukung operasional organisasi skala menengah-besar dengan banyak pengguna, banyak departemen, dan seringkali tersebar di beberapa lokasi.
- Karakteristik utama jaringan enterprise meliputi skala dan kompleksitas besar, kebutuhan ketersediaan tinggi, skalabilitas, segmentasi dan tata kelola terstruktur, keamanan berlapis, serta manajemen terpusat.
- Jaringan SOHO berbeda dari jaringan enterprise dalam hal jumlah pengguna, topologi, jenis perangkat, redundansi, segmentasi, manajemen, kebutuhan keamanan, dan tingkat ketersediaan layanan.
- Tiga kebutuhan utama jaringan enterprise adalah skalabilitas, ketersediaan (availability), dan keamanan (security), yang menjadi dasar pertimbangan pada seluruh tahap perancangan jaringan enterprise.
- Studi kasus organisasi nyata membantu mahasiswa mengaitkan konsep teoretis jaringan enterprise dengan kebutuhan bisnis yang sesungguhnya.

D. LATIHAN/SOAL

Petunjuk pengerjaan: Kerjakan seluruh soal berikut secara mandiri. Soal nomor 1–6 merupakan soal pemahaman konsep (jawaban singkat/uraian), sedangkan soal nomor 7–10 merupakan soal analisis yang memerlukan penjelasan disertai contoh. Seluruh soal mengacu pada capaian Sub-CPMK 1.1.

1. Jelaskan definisi jaringan enterprise menurut pemahaman Anda, disertai satu contoh organisasi yang menerapkannya.

2. Sebutkan dan jelaskan minimal empat karakteristik utama jaringan enterprise.

3. Apa yang dimaksud dengan jaringan SOHO? Berikan contoh penerapannya.

4. Jelaskan tiga perbedaan mendasar antara jaringan enterprise dan jaringan SOHO ditinjau dari aspek topologi dan manajemen.

5. Mengapa jaringan enterprise memerlukan segmentasi jaringan (VLAN), sedangkan jaringan SOHO umumnya tidak?

6. Jelaskan pengertian skalabilitas, ketersediaan, dan keamanan dalam konteks jaringan enterprise.

7. Sebuah rumah sakit besar berencana membangun jaringan baru yang menghubungkan seluruh unit layanan (rawat inap, laboratorium, farmasi, administrasi). Analisislah kebutuhan skalabilitas jaringan tersebut untuk lima tahun ke depan.

8. Berdasarkan studi kasus PT Nusantara Retail Group pada bab ini, identifikasikan risiko yang mungkin terjadi apabila perusahaan tersebut hanya menggunakan jaringan SOHO pada seluruh gerainya.

9. Analisislah mengapa ketersediaan layanan (availability) menjadi kebutuhan kritis pada jaringan perbankan, dan jelaskan dampak yang dapat terjadi apabila jaringan mengalami downtime.

10. Pilihlah satu organisasi nyata (perusahaan, instansi, atau institusi pendidikan) yang Anda ketahui, kemudian analisislah karakteristik jaringan enterprise apa saja yang relevan diterapkan pada organisasi tersebut, disertai alasan yang mendukung.

E. DAFTAR PUSTAKA

Cisco Networking Academy. (2022). CCNP Enterprise: Core networking technologies (ENCOR) companion guide. Cisco Press.

Froom, R., Frahim, E., & Sivasubramanian, B. (2021). Implementing Cisco IP switched networks (SWITCH) foundation learning guide (2nd ed.). Cisco Press.

Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson.

Marschke, D., Doraswamy, N., & Ghosh, A. (2021). SD-WAN: A comprehensive approach for enterprise networking. Packt Publishing.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 1 (2nd ed.). Cisco Press.

F. TUGAS/STUDI KASUS

Tugas Individu: Analisis Kebutuhan Jaringan Enterprise

Pilihlah satu organisasi (dapat berupa perusahaan, instansi pemerintah, rumah sakit, atau institusi pendidikan) yang memiliki lebih dari satu lokasi atau lebih dari 100 pengguna jaringan. Susunlah sebuah laporan singkat (2–3 halaman) yang memuat:

1. Profil singkat organisasi yang dipilih (bidang usaha/layanan, jumlah pengguna, jumlah lokasi).

2. Identifikasi minimal lima karakteristik jaringan enterprise yang relevan dengan organisasi tersebut.

3. Analisis kebutuhan skalabilitas, ketersediaan, dan keamanan organisasi tersebut, disertai justifikasi/alasan.

4. Argumentasi mengapa jaringan SOHO tidak memadai untuk memenuhi kebutuhan organisasi tersebut.

Laporan dikumpulkan dalam bentuk dokumen (PDF/Word) sesuai tenggat waktu yang ditentukan dosen pengampu. Tugas ini akan dinilai menggunakan rubrik pada Rubrik Penilaian per Pertemuan 1 (aspek Identifikasi Karakteristik Jaringan Enterprise) sebagaimana tercantum pada Lampiran buku ajar ini.

BAB 2
MODEL DESAIN JARINGAN ENTERPRISE

A. PENDAHULUAN

1. Deskripsi Singkat

Bab ini membahas dua model desain arsitektur jaringan enterprise yang paling umum digunakan dalam industri, yaitu model hierarchical three-tier yang lazim diterapkan pada jaringan kampus/kantor, dan model spine-leaf yang banyak digunakan pada jaringan pusat data (data center) modern. Pembahasan diawali dengan konsep dan struktur masing-masing model, dilanjutkan dengan kriteria pemilihan model desain yang tepat berdasarkan kebutuhan organisasi, mencakup pertimbangan skalabilitas, latensi, biaya, dan kompleksitas pengelolaan.

Materi pada bab ini merupakan kelanjutan langsung dari Bab 1, di mana mahasiswa telah memahami karakteristik dan kebutuhan jaringan enterprise secara umum. Pemahaman terhadap model desain jaringan menjadi dasar penting sebelum mahasiswa mempelajari implementasi teknis switching dan routing pada Bab 3 hingga Bab 6, karena pemilihan model desain akan sangat memengaruhi keputusan konfigurasi VLAN, routing, dan redundansi pada bab-bab tersebut.

2. Capaian Pembelajaran Mata Kuliah (CPMK) yang Dicapai

Kode CPMK	:	CPMK-1
Rumusan CPMK	:	Mampu menjelaskan konsep, karakteristik, dan model arsitektur jaringan enterprise sebagai dasar perancangan jaringan skala menengah-besar.
Bobot CPMK	:	14% dari keseluruhan capaian mata kuliah
CPL yang Didukung	:	CPL-2 (penguasaan konsep teoretis bidang teknik komputer) dan CPL-5 (kemampuan merancang, menginstalasi, mengonfigurasi, dan memelihara jaringan komputer)

3. Sub-CPMK yang Dicapai

Kode Sub-CPMK	:	Sub-CPMK 1.2
Rumusan Sub-CPMK	:	Mampu menjelaskan model desain jaringan enterprise (hierarchical three-tier, spine-leaf).
Pertemuan	:	Pertemuan ke-2
Indikator Penilaian	:	Ketepatan analisis pemilihan model desain sesuai kebutuhan organisasi (dinilai melalui tugas kelompok), bobot 3% dari total penilaian mata kuliah.

4. Tujuan Pembelajaran Khusus (TPK)

Setelah mempelajari bab ini secara tuntas, mahasiswa diharapkan mampu:

1. Menjelaskan konsep dan struktur model desain hierarchical three-tier beserta fungsi masing-masing lapisan (core, distribution, access).

2. Menjelaskan konsep dan struktur model desain spine-leaf beserta prinsip kerja topologi full-mesh antara spine dan leaf.

3. Membandingkan model hierarchical three-tier dan spine-leaf dari aspek skalabilitas, latensi, biaya, dan kompleksitas pengelolaan.

4. Menganalisis kriteria pemilihan model desain jaringan yang tepat berdasarkan kebutuhan dan karakteristik suatu organisasi.

5. Merekomendasikan model desain jaringan yang sesuai untuk studi kasus topologi kampus/kantor maupun pusat data, disertai justifikasi teknis.

5. Peta Konsep

Alur pembahasan materi pada Bab 2 disajikan dalam peta konsep berikut, yang menggambarkan keterkaitan logis antar-subbab menuju pencapaian Sub-CPMK 1.2.

Model Hierarchical Three-Tier → **Model Spine-Leaf** → **Kriteria Pemilihan Model Desain**

6. Prasyarat

Sebelum mempelajari bab ini, mahasiswa disarankan telah memahami materi Bab 1 mengenai karakteristik dan kebutuhan jaringan enterprise (skalabilitas, ketersediaan, keamanan), serta menguasai konsep dasar perangkat switching dan routing (fungsi switch Layer 2 dan router Layer 3) yang diperoleh pada mata kuliah jaringan komputer dasar.

B. URAIAN MATERI

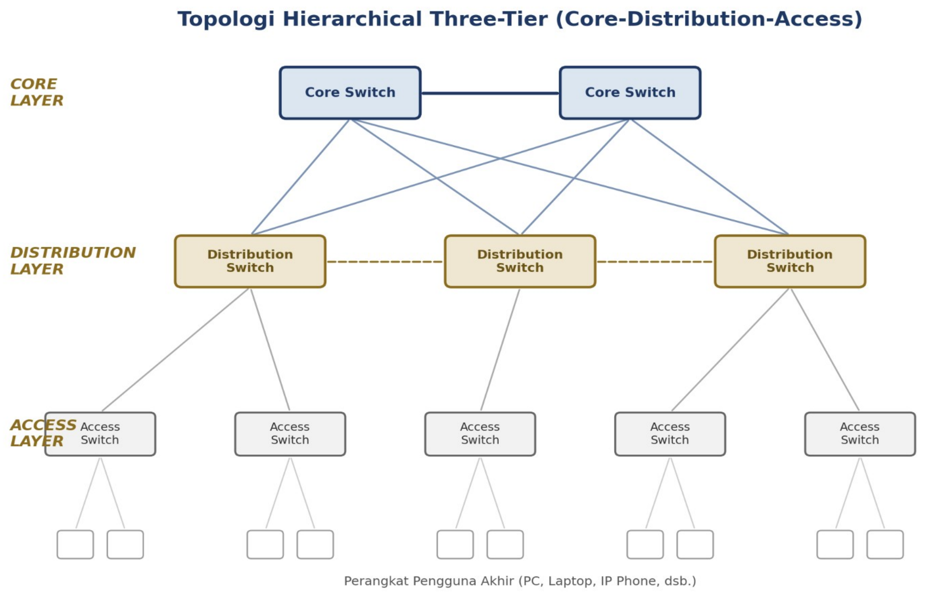
2.1 Model Hierarchical Three-Tier

a. Penjelasan Konsep/Teori

Model hierarchical three-tier (tiga lapis hierarkis) merupakan model desain jaringan enterprise yang paling banyak diterapkan pada jaringan kampus dan kantor, khususnya oleh Cisco sebagai salah satu praktik terbaik (best practice) desain jaringan. Model ini membagi arsitektur jaringan menjadi tiga lapisan fungsional yang berbeda, yaitu lapisan core, distribution, dan access, dengan tanggung jawab masing-masing lapisan yang jelas terpisah.

- Lapisan Core — merupakan tulang punggung (backbone) jaringan yang bertugas melakukan forwarding data berkecepatan sangat tinggi antar-lapisan distribution. Lapisan ini dirancang untuk kecepatan dan keandalan maksimum, sehingga umumnya tidak melakukan pemrosesan kebijakan (policy) yang kompleks seperti ACL atau filtering, agar latensi tetap minimal. Perangkat pada lapisan core biasanya dipasang secara redundan (dua atau lebih switch core).
- Lapisan Distribution — berfungsi sebagai penghubung antara lapisan core dan access, sekaligus menjadi titik penerapan kebijakan jaringan seperti routing antar-VLAN (inter-VLAN routing), ACL, quality of service (QoS), serta agregasi trafik dari beberapa switch access. Lapisan ini juga menjadi batas antara domain Layer 2 dan Layer 3 pada banyak implementasi.
- Lapisan Access — merupakan titik masuk (edge) jaringan yang menghubungkan perangkat pengguna akhir (PC, laptop, IP phone, printer, access point) ke jaringan. Lapisan ini bertanggung jawab atas fungsi dasar seperti port security, penetapan VLAN, dan Power over Ethernet (PoE) untuk perangkat seperti IP phone dan access point.

Struktur berjenjang ini memberikan beberapa keunggulan, antara lain memudahkan troubleshooting karena setiap lapisan memiliki fungsi yang jelas, mendukung skalabilitas karena penambahan kapasitas cukup dilakukan pada lapisan yang relevan, serta memungkinkan penerapan redundansi secara modular pada setiap lapisan.



Gambar 2.1 Topologi Hierarchical Three-Tier (Core-Distribution-Access)

Diagram di atas menggambarkan struktur tiga lapis jaringan enterprise. Dua Core Switch pada lapisan paling atas saling terhubung untuk redundansi dan melayani forwarding kecepatan tinggi. Tiga Distribution Switch pada lapisan tengah masing-masing terhubung ke kedua Core Switch (dual-homed) untuk menjamin ketersediaan jalur, serta saling terhubung satu sama lain. Lima Access Switch pada lapisan bawah terhubung ke Distribution Switch terdekat dan melayani perangkat pengguna akhir secara langsung.

b. Contoh Aplikasi

Model hierarchical three-tier sangat sesuai diterapkan pada jaringan kampus perguruan tinggi, di mana lapisan core menghubungkan gedung-gedung utama, lapisan distribution ditempatkan pada setiap gedung untuk mengelola VLAN per fakultas/unit, dan lapisan access melayani ruang kelas, laboratorium, serta ruang kerja staf pada masing-masing gedung.

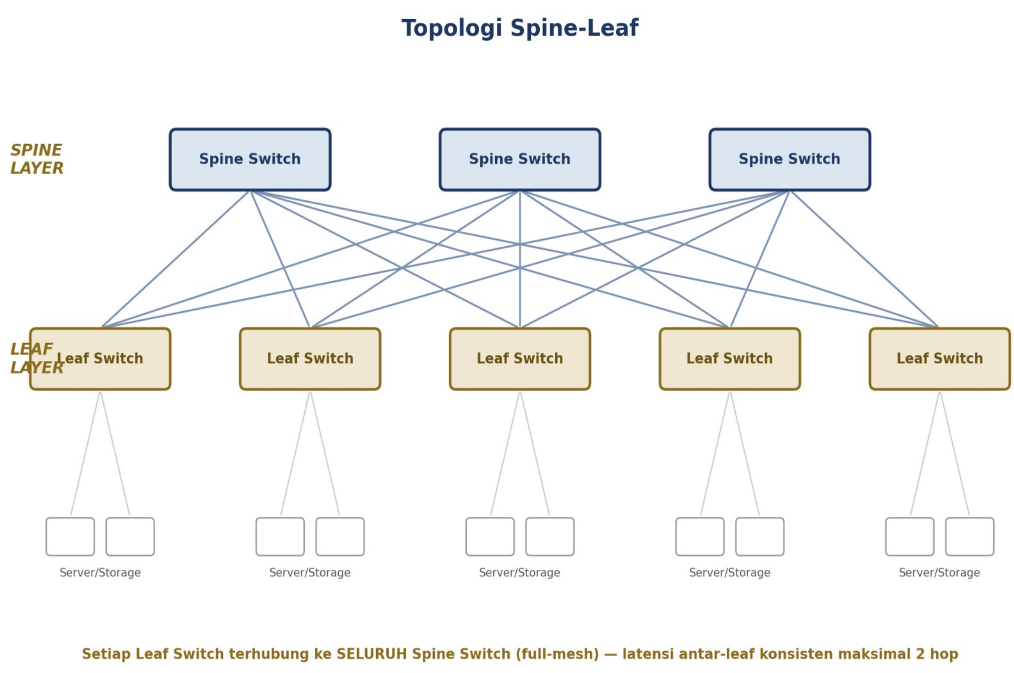
2.2 Model Spine-Leaf

a. Penjelasan Konsep/Teori

Model spine-leaf merupakan model desain jaringan yang berkembang seiring kebutuhan pusat data (data center) modern yang mengutamakan latensi rendah dan bandwidth tinggi untuk trafik east-west (trafik antar-server dalam data center), berbeda dengan model tradisional yang lebih mengutamakan trafik north-south (trafik antara pengguna dan server). Model ini hanya terdiri atas dua lapisan, yaitu lapisan spine dan lapisan leaf.

- Lapisan Spine — berfungsi sebagai tulang punggung penghubung seluruh switch leaf. Setiap switch spine terhubung ke seluruh switch leaf yang ada, namun switch spine tidak saling terhubung satu sama lain maupun langsung ke perangkat pengguna akhir.
- Lapisan Leaf — merupakan titik koneksi bagi server, storage, dan perangkat akhir lainnya. Setiap switch leaf wajib terhubung ke seluruh switch spine (topologi full-mesh antar-lapisan), namun antar-switch leaf tidak saling terhubung langsung.

Struktur full-mesh antara spine dan leaf ini memastikan bahwa lalu lintas data dari satu leaf ke leaf lainnya selalu menempuh jumlah hop yang sama dan minimal (maksimal dua hop: leaf-spine-leaf), sehingga latensi jaringan menjadi sangat konsisten dan dapat diprediksi. Karakteristik ini sangat penting bagi aplikasi modern seperti komputasi terdistribusi, virtualisasi skala besar, dan aplikasi berbasis microservices yang menghasilkan volume trafik antar-server yang sangat tinggi. Selain itu, penambahan kapasitas pada model spine-leaf dilakukan dengan menambahkan switch leaf baru (untuk menambah port akses) atau switch spine baru (untuk menambah bandwidth agregat), tanpa mengubah struktur topologi secara keseluruhan.



Gambar 2.2 Topologi Spine-Leaf

Diagram di atas menggambarkan tiga Spine Switch pada lapisan atas yang masing-masing terhubung ke seluruh lima Leaf Switch pada lapisan bawah, membentuk topologi full-mesh. Setiap Leaf Switch melayani beberapa server/storage secara langsung. Dengan struktur ini, komunikasi data dari server pada satu leaf ke server pada leaf lainnya selalu menempuh maksimal dua hop (leaf–spine–leaf), sehingga latensi antar-server tetap konsisten meskipun jaringan terus bertumbuh.

b. Contoh Aplikasi

Model spine-leaf banyak diterapkan pada data center penyedia layanan cloud, platform e-commerce dengan trafik tinggi, serta pusat data perusahaan finansial yang memerlukan pemrosesan data dengan latensi sangat rendah dan konsisten antar-server.

2.3 Kriteria Pemilihan Model Desain

a. Penjelasan Konsep/Teori

Pemilihan model desain jaringan yang tepat bergantung pada karakteristik dan kebutuhan spesifik organisasi. Terdapat empat kriteria utama yang perlu dipertimbangkan, yaitu skalabilitas, latensi, biaya, dan kompleksitas pengelolaan, sebagaimana dirangkum pada Tabel 2.1 berikut.

Aspek	Hierarchical Three-Tier	Spine-Leaf
Skalabilitas	Baik untuk pertumbuhan bertahap per lapisan; kurang optimal untuk pertumbuhan trafik east-west yang sangat besar	Sangat baik; penambahan leaf/spine dapat dilakukan tanpa mengubah struktur keseluruhan
Latensi	Bervariasi; trafik antar-access dapat menempuh banyak hop melalui distribution dan core	Konsisten dan rendah; maksimal dua hop antar-leaf
Biaya	Umumnya lebih rendah untuk skala kampus/kantor menengah	Relatif lebih tinggi karena kebutuhan interkoneksi full-mesh dan bandwidth besar
Kompleksitas Pengelolaan	Sedang; fungsi tiap lapisan jelas terpisah, mudah dipahami	Lebih tinggi; memerlukan pemahaman desain data center dan sering dikombinasikan dengan otomasi/overlay
Penggunaan Umum	Jaringan kampus, kantor, gedung bertingkat	Pusat data (data center), cloud, platform trafik tinggi

Tabel 2.1 Perbandingan Model Hierarchical Three-Tier dan Spine-Leaf

Selain keempat aspek di atas, pemilihan model desain juga perlu mempertimbangkan jenis trafik yang dominan pada organisasi (north-south atau east-west), proyeksi pertumbuhan organisasi dalam beberapa tahun ke depan, ketersediaan sumber daya manusia yang kompeten mengelola arsitektur yang dipilih, serta anggaran investasi infrastruktur yang tersedia.

b. Contoh Aplikasi

Sebagai ilustrasi, sebuah kantor pemerintahan dengan satu gedung berlantai lima dan kebutuhan trafik yang didominasi akses pengguna ke server internal (trafik north-south) akan lebih tepat menggunakan model hierarchical three-tier. Sebaliknya, sebuah perusahaan rintisan (startup) teknologi yang membangun data center sendiri untuk melayani aplikasi berbasis microservices dengan komunikasi antar-server yang sangat intensif akan lebih diuntungkan dengan model spine-leaf.

C. RANGKUMAN

- Model hierarchical three-tier membagi jaringan menjadi tiga lapisan fungsional: core (backbone berkecepatan tinggi), distribution (penerapan kebijakan dan agregasi), dan access (titik masuk perangkat pengguna).
- Model spine-leaf terdiri atas dua lapisan (spine dan leaf) dengan struktur full-mesh antar-lapisan, dirancang untuk latensi rendah dan konsisten pada trafik east-west di pusat data.
- Hierarchical three-tier umumnya digunakan pada jaringan kampus/kantor, sedangkan spine-leaf umumnya digunakan pada jaringan pusat data (data center) modern.
- Kriteria pemilihan model desain meliputi skalabilitas, latensi, biaya, dan kompleksitas pengelolaan, yang harus disesuaikan dengan jenis trafik dominan dan kebutuhan pertumbuhan organisasi.
- Keputusan pemilihan model desain jaringan pada tahap awal akan sangat memengaruhi keputusan konfigurasi teknis (VLAN, routing, redundansi) pada tahap perancangan selanjutnya.

D. LATIHAN/SOAL

Petunjuk pengerjaan: Kerjakan seluruh soal berikut secara mandiri. Soal nomor 1–6 merupakan soal pemahaman konsep (jawaban singkat/uraian), sedangkan soal nomor 7–10 merupakan soal analisis yang memerlukan penjelasan disertai justifikasi teknis. Seluruh soal mengacu pada capaian Sub-CPMK 1.2.

1. Jelaskan tiga lapisan pada model hierarchical three-tier beserta fungsi utama masing-masing lapisan.

2. Mengapa lapisan core pada model hierarchical three-tier dirancang untuk tidak melakukan pemrosesan kebijakan (policy) yang kompleks?

3. Jelaskan konsep topologi full-mesh pada model spine-leaf dan bagaimana hal tersebut memengaruhi latensi jaringan.

4. Apa perbedaan mendasar antara trafik north-south dan trafik east-west? Jelaskan model desain mana yang lebih sesuai untuk masing-masing jenis trafik.

5. Sebutkan minimal tiga keunggulan model hierarchical three-tier dibandingkan jaringan datar (flat network).

6. Jelaskan bagaimana proses penambahan kapasitas (scale-out) dilakukan pada model spine-leaf.

7. Sebuah universitas dengan lima gedung dan kebutuhan trafik yang didominasi akses mahasiswa ke server akademik pusat berencana membangun jaringan baru. Analisislah model desain yang paling sesuai beserta alasannya.

8. Sebuah perusahaan teknologi finansial (fintech) sedang membangun data center sendiri untuk mendukung aplikasi transaksi real-time dengan komunikasi antar-server yang sangat intensif. Analisislah model desain yang paling sesuai beserta alasannya.

9. Berdasarkan Tabel 2.1, analisislah mengapa biaya implementasi model spine-leaf umumnya lebih tinggi dibandingkan hierarchical three-tier.

10. Sebuah organisasi memiliki jaringan kampus (hierarchical three-tier) dan juga berencana membangun data center kecil untuk kebutuhan internal. Rekomendasikan pendekatan desain yang tepat untuk kedua kebutuhan tersebut, disertai justifikasi teknis.

E. DAFTAR PUSTAKA

Cisco Networking Academy. (2022). CCNP Enterprise: Core networking technologies (ENCOR) companion guide. Cisco Press.

Froom, R., Frahim, E., & Sivasubramanian, B. (2021). Implementing Cisco IP switched networks (SWITCH) foundation learning guide (2nd ed.). Cisco Press.

Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 1 (2nd ed.). Cisco Press.

Teare, D., & Paquet, C. (2022). Implementing Cisco IP routing (ROUTE) foundation learning guide (2nd ed.). Cisco Press.

F. TUGAS/STUDI KASUS

Tugas Kelompok: Analisis Perbandingan Model Desain

Bentuklah kelompok kerja (3–4 mahasiswa). Setiap kelompok akan diberikan salah satu dari dua studi kasus organisasi berikut secara bergantian oleh dosen pengampu:

Studi Kasus A: Kampus Politeknik Multi-Gedung

Sebuah politeknik memiliki enam gedung (gedung kuliah, laboratorium, perpustakaan, rektorat, asrama, dan gedung olahraga) yang perlu terhubung ke server akademik pusat dan internet. Jumlah pengguna aktif sekitar 4.000 mahasiswa dan 300 staf.

Studi Kasus B: Data Center Perusahaan Rintisan Teknologi

Sebuah perusahaan rintisan (startup) teknologi sedang membangun data center internal berskala kecil-menengah untuk menjalankan aplikasi berbasis microservices dengan komunikasi antar-server yang sangat intensif, guna mendukung layanan aplikasi mobile miliknya yang memiliki jutaan pengguna.

Setiap kelompok diminta menyusun laporan analisis (3–4 halaman) yang memuat:

1. Rekomendasi model desain jaringan (hierarchical three-tier atau spine-leaf) yang paling sesuai untuk studi kasus yang diberikan.

2. Justifikasi teknis pemilihan model, ditinjau dari aspek skalabilitas, latensi, biaya, dan kompleksitas pengelolaan.

3. Sketsa/diagram topologi usulan (dapat digambar manual maupun menggunakan aplikasi bantu seperti draw.io atau Packet Tracer).

4. Identifikasi tantangan yang mungkin dihadapi dalam implementasi model yang direkomendasikan.

Laporan dipresentasikan secara singkat pada awal pertemuan berikutnya dan dikumpulkan dalam bentuk dokumen (PDF/Word). Tugas ini dinilai menggunakan rubrik pada Rubrik Penilaian per Pertemuan 2 (aspek Tugas Kelompok: Analisis Perbandingan Model Desain dan Partisipasi Diskusi) sebagaimana tercantum pada Lampiran buku ajar ini.

BAB 3
VLAN, TRUNKING, DAN VTP

A. PENDAHULUAN

1. Deskripsi Singkat

Bab ini membahas tiga topik teknis yang saling berkaitan dan menjadi fondasi konfigurasi switching pada jaringan enterprise, yaitu Virtual Local Area Network (VLAN), trunking dengan standar IEEE 802.1Q, dan VLAN Trunking Protocol (VTP). VLAN memungkinkan segmentasi jaringan secara logis tanpa memerlukan perangkat fisik terpisah, trunking memungkinkan satu tautan fisik membawa lalu lintas dari banyak VLAN sekaligus, sedangkan VTP memudahkan sinkronisasi informasi VLAN antar-switch dalam satu domain. Bab ini disertai praktik konfigurasi langsung menggunakan perintah Cisco IOS pada simulator jaringan (Packet Tracer/GNS3), sesuai dengan pengalaman belajar yang ditetapkan pada RPS.

Penguasaan materi pada bab ini menjadi dasar teknis yang sangat penting sebelum mahasiswa mempelajari EtherChannel dan routing antar-VLAN pada Bab 4, karena kedua topik tersebut dibangun langsung di atas konsep VLAN dan trunking yang dibahas di sini.

2. Capaian Pembelajaran Mata Kuliah (CPMK) yang Dicapai

Kode CPMK	:	CPMK-2
Rumusan CPMK	:	Mampu merancang dan mengonfigurasi topologi jaringan enterprise menggunakan VLAN, Layer 3 switching, routing dinamis, dan protokol redundansi gateway untuk mendukung high availability.
Bobot CPMK	:	29% dari keseluruhan capaian mata kuliah (bobot CPMK terbesar)
CPL yang Didukung	:	CPL-2 (penguasaan konsep teoretis bidang teknik komputer) dan CPL-5 (kemampuan merancang, menginstalasi, mengonfigurasi, dan memelihara jaringan komputer)

3. Sub-CPMK yang Dicapai

Kode Sub-CPMK	:	Sub-CPMK 2.1
Rumusan Sub-CPMK	:	Mampu mengonfigurasi VLAN, trunking (802.1Q), dan VTP pada switch enterprise.
Pertemuan	:	Pertemuan ke-3
Indikator Penilaian	:	Ketepatan konfigurasi VLAN/trunking sesuai skenario (dinilai melalui tugas praktik), bobot 3% dari total penilaian

mata kuliah.

4. Tujuan Pembelajaran Khusus (TPK)

Setelah mempelajari bab ini secara tuntas, mahasiswa diharapkan mampu:

1. Menjelaskan konsep VLAN, jenis-jenis VLAN, serta manfaatnya dalam segmentasi jaringan enterprise.

2. Mengonfigurasi VLAN pada switch Cisco menggunakan perintah dasar Cisco IOS, termasuk penamaan dan penetapan port ke VLAN tertentu.

3. Menjelaskan konsep trunking 802.1Q serta mengonfigurasi trunk link antar-switch, termasuk pengaturan native VLAN dan allowed VLAN.

4. Menjelaskan fungsi, mode kerja (server, client, transparent), dan risiko penggunaan VLAN Trunking Protocol (VTP) pada jaringan enterprise.

5. Mempraktikkan konfigurasi VLAN, trunking, dan VTP secara terintegrasi pada skenario topologi switch enterprise sederhana, serta memverifikasi hasil konfigurasi menggunakan perintah verifikasi Cisco IOS.

5. Peta Konsep

Alur pembahasan materi pada Bab 3 disajikan dalam peta konsep berikut, yang menggambarkan keterkaitan logis antar-subbab menuju pencapaian Sub-CPMK 2.1.

Konsep VLAN → **Trunking 802.1Q** → **VLAN Trunking Protocol (VTP)** → **Praktik Konfigurasi VLAN & Trunking**

6. Prasyarat

Sebelum mempelajari bab ini, mahasiswa disarankan telah memahami materi Bab 1 dan Bab 2 mengenai karakteristik dan model desain jaringan enterprise, serta menguasai konsep dasar switching Layer 2 (broadcast domain, collision domain, MAC address table) dan dasar antarmuka baris perintah (command-line interface) Cisco IOS, meliputi mode user EXEC, privileged EXEC, global configuration, dan interface configuration.

B. URAIAN MATERI

3.1 Konsep VLAN

a. Penjelasan Konsep/Teori

Virtual Local Area Network (VLAN) adalah teknik segmentasi jaringan pada Layer 2 yang memungkinkan sebuah switch fisik dibagi menjadi beberapa broadcast domain logis yang terpisah, tanpa memerlukan perangkat switch fisik tambahan. Setiap VLAN berperilaku seolah-olah merupakan jaringan LAN yang berdiri sendiri: lalu lintas broadcast, unicast yang belum diketahui (unknown unicast), dan multicast pada satu VLAN tidak akan diteruskan ke VLAN lain kecuali melalui perangkat Layer 3 (router atau Layer 3 switch).

Berdasarkan fungsinya, VLAN pada jaringan enterprise umumnya dikelompokkan ke dalam beberapa jenis berikut.

- Data VLAN — VLAN yang membawa lalu lintas data pengguna umum, biasanya dipisahkan per departemen atau fungsi (contoh: VLAN Keuangan, VLAN Operasional).
- Voice VLAN — VLAN khusus untuk lalu lintas suara (VoIP) dari IP phone, yang dipisahkan dari data VLAN untuk menjamin kualitas layanan (QoS) komunikasi suara.
- Native VLAN — VLAN yang lalu lintasnya dikirim tanpa tag 802.1Q pada trunk link; secara default adalah VLAN 1, namun sebagai praktik keamanan yang baik sebaiknya diubah ke VLAN yang tidak digunakan.
- Management VLAN — VLAN yang digunakan khusus untuk akses manajemen perangkat (misalnya akses SSH/Telnet ke switch), yang sebaiknya dipisahkan dari VLAN data pengguna demi keamanan.
- Default VLAN — VLAN 1, yang secara otomatis aktif pada seluruh port switch Cisco dan tidak dapat dihapus, sehingga sebaiknya tidak digunakan untuk lalu lintas data produksi.

VLAN diidentifikasi dengan VLAN ID (VID) yang memiliki rentang tertentu, sebagaimana dirangkum pada Tabel 3.1 berikut.

Rentang VLAN ID	Kategori	Keterangan Peruntukan
0, 4095	Reserved	Dicadangkan oleh sistem, tidak dapat digunakan
1	Default VLAN	Aktif otomatis pada seluruh port; sebaiknya tidak dipakai untuk data produksi
2 – 1001	Normal Range	Dapat digunakan bebas untuk VLAN data, voice, dan manajemen; disimpan pada database VTP (vlan.dat)
1002 – 1005	Reserved (legacy)	Dicadangkan untuk VLAN legacy Token Ring

Rentang VLAN ID	Kategori	Keterangan Peruntukan
		dan FDDI, tidak digunakan pada jaringan modern
1006 – 4094	Extended Range	Digunakan pada jaringan berskala sangat besar; tidak disimpan pada database VTP versi 1 dan 2

Tabel 3.1 Rentang VLAN ID dan Peruntukannya

Konfigurasi VLAN dasar pada switch Cisco IOS dilakukan melalui mode global configuration, sebagaimana dicontohkan pada perintah berikut.

```
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 OPERASIONAL
Switch(config-vlan)# exit
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# end
Switch# show vlan brief
```

Contoh 3.1 Perintah dasar pembuatan VLAN dan penetapan access port pada Cisco IOS

b. Contoh Aplikasi

Pada sebuah kantor dengan satu switch yang melayani tiga departemen (Keuangan, Operasional, SDM), VLAN memungkinkan ketiga departemen tersebut tetap berada pada satu perangkat switch fisik, namun lalu lintas broadcast masing-masing departemen tetap terisolasi satu sama lain, sehingga meningkatkan keamanan dan mengurangi beban broadcast pada jaringan.

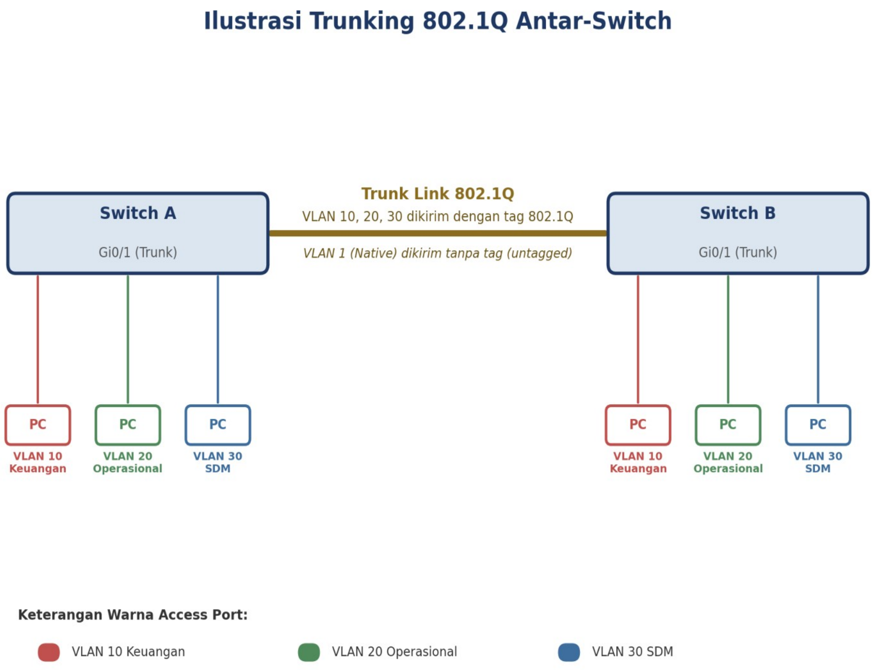
3.2 Trunking 802.1Q

a. Penjelasan Konsep/Teori

Trunking adalah mekanisme yang memungkinkan satu tautan fisik (biasanya antar-switch, atau antara switch dan router) membawa lalu lintas dari banyak VLAN sekaligus. Standar trunking yang paling umum digunakan pada industri adalah IEEE 802.1Q, yang bekerja dengan menyisipkan tag VLAN (VLAN tag) berukuran 4 byte ke dalam frame Ethernet, sehingga perangkat penerima dapat mengidentifikasi frame tersebut berasal dari VLAN mana.

Beberapa istilah penting dalam trunking 802.1Q adalah sebagai berikut.

- Trunk Port — port switch yang dikonfigurasi untuk membawa lalu lintas dari banyak VLAN sekaligus, biasanya menghubungkan antar-switch atau switch ke router.
- Tagging — proses penyisipan informasi VLAN ID ke dalam header frame Ethernet, sehingga switch penerima dapat meneruskan frame tersebut ke VLAN yang sesuai.
- Native VLAN — satu-satunya VLAN pada trunk link yang lalu lintasnya dikirim tanpa tag (untagged); native VLAN pada kedua ujung trunk link harus sama untuk menghindari masalah keamanan dan konektivitas.
- Allowed VLAN List — daftar VLAN yang diizinkan melewati suatu trunk link; secara default seluruh VLAN diizinkan, namun dapat dibatasi menggunakan perintah tertentu untuk kebutuhan keamanan atau efisiensi.



Gambar 3.1 Ilustrasi Trunking 802.1Q Antar-Switch

Diagram di atas menggambarkan dua switch (Switch A dan Switch B) yang terhubung melalui satu trunk link 802.1Q. Trunk link tersebut membawa lalu lintas dari tiga VLAN (VLAN 10 Keuangan, VLAN 20 Operasional, VLAN 30 SDM) yang dikirim dengan tag 802.1Q, sementara VLAN 1 sebagai native VLAN dikirim tanpa tag. Pada masing-masing switch, setiap VLAN memiliki access port yang menghubungkan perangkat pengguna akhir (PC) sesuai departemennya.

Konfigurasi trunk link pada switch Cisco IOS dicontohkan pada perintah berikut.

```
Switch(config)# interface gigabitEthernet 0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 99
Switch(config-if)# switchport trunk allowed vlan 10,20,30
Switch(config-if)# end
Switch# show interfaces gigabitEthernet 0/1 trunk
```

Contoh 3.2 Perintah konfigurasi trunk link 802.1Q pada Cisco IOS

b. Contoh Aplikasi

Trunking sangat diperlukan ketika satu departemen (misalnya Keuangan dengan VLAN 10) memiliki perangkat yang tersebar pada dua switch berbeda di lantai yang berbeda pula. Dengan trunk link antar-switch, VLAN 10 pada kedua switch tersebut dapat saling berkomunikasi seolah-olah berada pada satu switch yang sama.

3.3 VLAN Trunking Protocol (VTP)

a. Penjelasan Konsep/Teori

VLAN Trunking Protocol (VTP) adalah protokol milik Cisco yang berfungsi menyinkronkan informasi konfigurasi VLAN (VLAN ID dan nama VLAN) secara otomatis di antara seluruh switch dalam satu domain VTP yang sama, sehingga administrator tidak perlu mengonfigurasi VLAN secara manual pada setiap switch satu per satu. Sinkronisasi dilakukan melalui trunk link dan menggunakan nomor revisi konfigurasi (configuration revision number) untuk menentukan informasi VLAN mana yang paling baru.

VTP memiliki tiga mode kerja yang dapat dikonfigurasi pada setiap switch.

- Server — mode default pada sebagian besar switch Cisco; dapat membuat, mengubah, dan menghapus VLAN, serta menyebarkan (advertise) perubahan tersebut ke switch lain dalam domain yang sama.
- Client — tidak dapat membuat atau mengubah VLAN secara lokal; hanya menerima dan meneruskan informasi VLAN dari switch bermode server dalam domain yang sama.
- Transparent — tidak berpartisipasi dalam sinkronisasi VTP; VLAN dikonfigurasi secara lokal pada switch tersebut, namun switch tetap meneruskan (forward) pesan VTP yang diterima ke switch lain.

Perhatian: Risiko VTP Configuration Revision

Salah satu risiko signifikan dalam penggunaan VTP adalah ketika sebuah switch dengan mode server dan nomor revisi konfigurasi yang lebih tinggi (meskipun berasal dari domain lama atau pengujian sebelumnya) dihubungkan ke jaringan produksi. Switch tersebut dapat menimpa (overwrite) seluruh database VLAN pada switch lain dalam domain yang sama, termasuk menghapus VLAN yang sedang digunakan, sehingga menyebabkan gangguan jaringan yang luas. Oleh karena itu, praktik terbaik industri merekomendasikan penggunaan mode transparent atau VTP versi 3 dengan fitur autentikasi/primary server untuk jaringan produksi, serta selalu memeriksa nomor revisi sebelum menghubungkan switch baru ke jaringan.

Konfigurasi dasar VTP pada switch Cisco IOS dicontohkan pada perintah berikut.

```
Switch(config)# vtp domain PNP-NETLAB
Switch(config)# vtp mode server
Switch(config)# vtp password Cisco123
Switch(config)# vtp version 2
Switch(config)# end
Switch# show vtp status
```

Contoh 3.3 Perintah konfigurasi domain, mode, dan password VTP pada Cisco IOS

b. Contoh Aplikasi

Pada sebuah kampus dengan sepuluh switch access yang tersebar di berbagai gedung, VTP memudahkan administrator jaringan untuk menambahkan VLAN baru cukup dari satu switch server, dan perubahan tersebut akan otomatis tersebar ke seluruh switch client dalam domain yang sama, tanpa perlu login satu per satu ke setiap switch.

3.4 Praktik Konfigurasi VLAN dan Trunking

a. Penjelasan Konsep/Teori

Sub-bab ini menyajikan skenario praktik terintegrasi yang menggabungkan konfigurasi VLAN, trunking, dan VTP pada topologi sederhana yang terdiri atas dua switch access (SW-Access-1 dan SW-Access-2) yang terhubung melalui trunk link, dengan skema VLAN sebagai berikut: VLAN 10 (Keuangan), VLAN 20 (Operasional), dan VLAN 30 (SDM). SW-Access-1 dikonfigurasi sebagai VTP server, sedangkan SW-Access-2 dikonfigurasi sebagai VTP client dalam domain VTP yang sama.

Tahapan praktik dilakukan secara berurutan sebagai berikut: (1) konfigurasi VTP domain dan mode pada kedua switch; (2) pembuatan VLAN pada switch server; (3) konfigurasi trunk link antar-switch; (4) penetapan access port pada masing-masing switch sesuai VLAN; dan (5) verifikasi hasil konfigurasi.

Verifikasi hasil konfigurasi dilakukan menggunakan beberapa perintah show pada Cisco IOS, sebagaimana dicontohkan berikut.

```
SW-Access-1# show vlan brief
SW-Access-1# show vtp status
SW-Access-1# show interfaces trunk
SW-Access-2# show vlan brief
SW-Access-2# show interfaces gigabitEthernet 0/1 switchport
```

Contoh 3.4 Perintah verifikasi konfigurasi VLAN, trunk, dan status VTP

Perintah show vlan brief menampilkan daftar VLAN beserta port yang tergabung pada masing-masing VLAN; show vtp status menampilkan mode VTP, domain, dan nomor revisi konfigurasi saat ini; sedangkan show interfaces trunk menampilkan status trunk link, native VLAN, dan daftar VLAN yang diizinkan (allowed VLAN) pada trunk tersebut. Ketepatan hasil verifikasi ini menjadi indikator utama penilaian tugas praktik pada Sub-CPMK 2.1.

b. Contoh Aplikasi

Skenario praktik ini dapat dikembangkan lebih lanjut oleh dosen dengan menambahkan switch access ketiga, atau dengan menyisipkan kesalahan konfigurasi (misalnya native VLAN mismatch) yang harus diidentifikasi dan diperbaiki oleh mahasiswa sebagai latihan troubleshooting dasar.

C. RANGKUMAN

- VLAN adalah teknik segmentasi jaringan pada Layer 2 yang membagi satu switch fisik menjadi beberapa broadcast domain logis, terdiri atas beberapa jenis (data, voice, native, management, default VLAN) dengan rentang VLAN ID normal dan extended.
- Trunking 802.1Q memungkinkan satu tautan fisik membawa lalu lintas dari banyak VLAN sekaligus melalui mekanisme tagging, dengan native VLAN sebagai satu-satunya VLAN yang dikirim tanpa tag.
- VTP menyinkronkan informasi VLAN antar-switch dalam satu domain melalui tiga mode kerja (server, client, transparent), namun memiliki risiko configuration revision yang dapat menimpa database VLAN jika tidak dikelola dengan hati-hati.
- Konfigurasi VLAN, trunking, dan VTP pada Cisco IOS dilakukan melalui mode global configuration dan interface configuration, serta diverifikasi menggunakan perintah show vlan brief, show interfaces trunk, dan show vtp status.
- Praktik konfigurasi terintegrasi pada topologi dua switch access membantu mahasiswa memahami keterkaitan antara VLAN, trunking, dan VTP dalam satu skenario jaringan enterprise yang realistis.

D. LATIHAN/SOAL

Petunjuk pengerjaan: Kerjakan seluruh soal berikut secara mandiri. Soal nomor 1–5 merupakan soal pemahaman konsep (jawaban singkat/uraian), soal nomor 6–8 merupakan soal konfigurasi (tuliskan perintah Cisco IOS yang diperlukan), dan soal nomor 9–10 merupakan soal analisis/troubleshooting. Seluruh soal mengacu pada capaian Sub-CPMK 2.1.

1. Jelaskan definisi VLAN dan manfaat utamanya dalam segmentasi jaringan enterprise.

2. Sebutkan dan jelaskan minimal empat jenis VLAN berdasarkan fungsinya.

3. Jelaskan perbedaan antara VLAN normal range dan extended range.

4. Jelaskan konsep tagging pada trunking 802.1Q dan fungsi native VLAN pada trunk link.

5. Jelaskan perbedaan ketiga mode VTP (server, client, transparent) beserta karakteristik masing-masing.

6. Tuliskan perintah Cisco IOS lengkap untuk membuat VLAN 40 dengan nama MARKETING dan menetapkan port FastEthernet 0/5 sebagai access port pada VLAN tersebut.

7. Tuliskan perintah Cisco IOS lengkap untuk mengonfigurasi interface GigabitEthernet 0/2 sebagai trunk link dengan encapsulation dot1q, native VLAN 99, dan hanya mengizinkan VLAN 10, 20, dan 30.

8. Tuliskan perintah Cisco IOS untuk mengonfigurasi sebuah switch sebagai VTP client pada domain bernama KAMPUS-NET dengan password Rahasia2026.

9. Sebuah switch baru dengan VTP mode server dan nomor revisi konfigurasi 25 dihubungkan ke jaringan produksi yang memiliki switch lain dengan nomor revisi 12 pada domain VTP yang sama. Analisislah apa yang akan terjadi dan bagaimana cara mencegah insiden tersebut.

10. Pada saat verifikasi menggunakan perintah show interfaces trunk, ditemukan bahwa VLAN 30 tidak muncul pada daftar allowed VLAN meskipun sudah dikonfigurasi pada kedua switch. Analisislah kemungkinan penyebab masalah tersebut dan langkah troubleshooting yang perlu dilakukan.

E. DAFTAR PUSTAKA

Cisco Networking Academy. (2022). CCNP Enterprise: Core networking technologies (ENCOR) companion guide. Cisco Press.

Froom, R., Frahim, E., & Sivasubramanian, B. (2021). Implementing Cisco IP switched networks (SWITCH) foundation learning guide (2nd ed.). Cisco Press.

Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 1 (2nd ed.). Cisco Press.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 2 (2nd ed.). Cisco Press.

F. TUGAS/STUDI KASUS

Tugas Praktik: Konfigurasi VLAN dan Trunking pada Simulator Jaringan

Menggunakan simulator jaringan (Cisco Packet Tracer atau GNS3), bangunlah topologi yang terdiri atas dua switch access yang saling terhubung melalui trunk link, dengan ketentuan sebagai berikut.

1. Buat tiga VLAN pada kedua switch: VLAN 10 (nama: KEUANGAN), VLAN 20 (nama: OPERASIONAL), dan VLAN 30 (nama: SDM).

2. Konfigurasikan kedua switch dalam satu domain VTP yang sama, dengan Switch 1 sebagai VTP server dan Switch 2 sebagai VTP client.

3. Konfigurasikan trunk link antar-kedua switch menggunakan encapsulation dot1q, dengan native VLAN 99 dan hanya mengizinkan VLAN 10, 20, dan 30.

4. Hubungkan minimal dua PC pada setiap VLAN (pada kedua switch), lalu uji konektivitas antar-PC dalam VLAN yang sama serta pastikan PC pada VLAN berbeda tidak dapat saling terhubung secara langsung.

5. Lakukan verifikasi konfigurasi menggunakan perintah show vlan brief, show vtp status, dan show interfaces trunk pada kedua switch, lalu sertakan hasil tangkapan layar (screenshot) pada laporan.

Laporan praktik (mencakup topologi, seluruh perintah konfigurasi, dan hasil verifikasi) dikumpulkan dalam bentuk dokumen (PDF/Word) disertai file simulasi (.pkt/.gns3) sesuai tenggat waktu yang ditentukan dosen pengampu. Tugas ini dinilai menggunakan rubrik pada Rubrik Penilaian per Pertemuan 3 (aspek Tugas Praktik: Konfigurasi VLAN & Trunking dan Partisipasi Diskusi: Demonstrasi Konfigurasi VLAN) sebagaimana tercantum pada Lampiran buku ajar ini.

BAB 4
ETHERCHANNEL DAN ROUTING ANTAR-VLAN

A. PENDAHULUAN

1. Deskripsi Singkat

Bab ini membahas dua topik teknis lanjutan pada switching enterprise, yaitu EtherChannel sebagai teknik agregasi tautan (link aggregation) untuk meningkatkan bandwidth dan redundansi, serta Layer 3 switching dan inter-VLAN routing sebagai mekanisme yang memungkinkan komunikasi antar-VLAN yang berbeda memanfaatkan switched virtual interface (SVI). Bab ini juga membahas mekanisme load balancing pada EtherChannel yang menentukan bagaimana lalu lintas didistribusikan ke seluruh tautan fisik dalam satu bundel logis.

Materi pada bab ini merupakan kelanjutan langsung dari Bab 3, di mana mahasiswa telah menguasai konfigurasi VLAN dan trunking. Kedua topik pada bab ini banyak diterapkan pada tautan antara lapisan distribution dan access (untuk EtherChannel) serta pada lapisan distribution itu sendiri (untuk inter-VLAN routing), sehingga menjadi bekal penting sebelum mahasiswa mempelajari routing dinamis OSPF pada Bab 5.

2. Capaian Pembelajaran Mata Kuliah (CPMK) yang Dicapai

Kode CPMK	:	CPMK-2
Rumusan CPMK	:	Mampu merancang dan mengonfigurasi topologi jaringan enterprise menggunakan VLAN, Layer 3 switching, routing dinamis, dan protokol redundansi gateway untuk mendukung high availability.
Bobot CPMK	:	29% dari keseluruhan capaian mata kuliah (bobot CPMK terbesar)
CPL yang Didukung	:	CPL-2 (penguasaan konsep teoretis bidang teknik komputer) dan CPL-5 (kemampuan merancang, menginstalasi, mengonfigurasi, dan memelihara jaringan komputer)

3. Sub-CPMK yang Dicapai

Kode Sub-CPMK	:	Sub-CPMK 2.2
Rumusan Sub-CPMK	:	Mampu menerapkan EtherChannel dan routing antar-VLAN pada Layer 3 switching.
Pertemuan	:	Pertemuan ke-4
Indikator Penilaian	:	Fungsi EtherChannel dan routing antar-VLAN berjalan

sesuai skenario (dinilai melalui tugas praktik), bobot 3% dari total penilaian mata kuliah.

4. Tujuan Pembelajaran Khusus (TPK)

Setelah mempelajari bab ini secara tuntas, mahasiswa diharapkan mampu:

1. Menjelaskan konsep EtherChannel serta mengonfigurasi EtherChannel menggunakan protokol LACP dan PAgP pada switch Cisco IOS.

2. Menjelaskan konsep Layer 3 switching serta perbedaannya dengan switching Layer 2 tradisional dan routing pada router konvensional.

3. Mengonfigurasi inter-VLAN routing menggunakan switched virtual interface (SVI) pada Layer 3 switch.

4. Menjelaskan mekanisme load balancing pada EtherChannel beserta faktor-faktor yang memengaruhi algoritme distribusi trafik.

5. Mempraktikkan konfigurasi EtherChannel dan inter-VLAN routing secara terintegrasi pada topologi jaringan enterprise sederhana, serta memverifikasi hasil konfigurasi.

5. Peta Konsep

Alur pembahasan materi pada Bab 4 disajikan dalam peta konsep berikut, yang menggambarkan keterkaitan logis antar-subbab menuju pencapaian Sub-CPMK 2.2.

Konsep & Konfigurasi EtherChannel (LACP/PAgP)	→	Layer 3 Switching	→	Inter-VLAN Routing & Load Balancing

6. Prasyarat

Sebelum mempelajari bab ini, mahasiswa disarankan telah menguasai materi Bab 3 mengenai VLAN dan trunking 802.1Q, serta memahami konsep dasar routing IP, termasuk subnetting, default gateway, dan tabel routing, yang diperoleh pada mata kuliah jaringan komputer dasar.

B. URAIAN MATERI

4.1 Konsep dan Konfigurasi EtherChannel (LACP/PAgP)

a. Penjelasan Konsep/Teori

EtherChannel adalah teknologi agregasi tautan (link aggregation) yang memungkinkan penggabungan beberapa tautan fisik (physical link) antara dua perangkat menjadi satu tautan logis (logical link) dengan bandwidth gabungan yang lebih besar. Selain meningkatkan bandwidth, EtherChannel juga meningkatkan ketersediaan (availability), karena apabila salah satu tautan fisik dalam bundel mengalami gangguan, lalu lintas data akan tetap berjalan melalui tautan fisik lain yang masih aktif tanpa menyebabkan downtime maupun perubahan pada topologi spanning-tree.

Terdapat dua protokol negosiasi otomatis yang umum digunakan untuk membentuk EtherChannel, yaitu sebagai berikut.

- LACP (Link Aggregation Control Protocol) — protokol standar terbuka (IEEE 802.3ad) yang didukung oleh hampir seluruh vendor perangkat jaringan. LACP memiliki dua mode: active (secara aktif menginisiasi negosiasi) dan passive (menunggu ajakan negosiasi dari perangkat lain). Minimal salah satu ujung tautan harus dikonfigurasi pada mode active agar EtherChannel dapat terbentuk.
- PAgP (Port Aggregation Protocol) — protokol milik Cisco (proprietary) dengan dua mode: desirable (secara aktif menginisiasi negosiasi) dan auto (menunggu ajakan negosiasi). Sama seperti LACP, minimal salah satu ujung harus dikonfigurasi pada mode desirable.
- Mode On (Manual) — EtherChannel dapat pula dibentuk tanpa protokol negosiasi (mode on pada kedua ujung), namun praktik ini tidak direkomendasikan karena tidak ada mekanisme deteksi kesalahan konfigurasi antar-ujung tautan, sehingga rentan menimbulkan loop atau kegagalan yang sulit dideteksi.

Agar beberapa port fisik dapat digabungkan ke dalam satu EtherChannel, seluruh port anggota harus memiliki konfigurasi yang identik, meliputi kecepatan (speed), mode duplex, mode switchport (access atau trunk), VLAN yang diizinkan (pada mode trunk), dan native VLAN. Ketidaksesuaian pada salah satu parameter tersebut akan menyebabkan port tidak dapat bergabung ke dalam bundel EtherChannel.

Konfigurasi EtherChannel menggunakan LACP pada switch Cisco IOS dicontohkan pada perintah berikut.

```
Switch(config)# interface range gigabitEthernet 0/1 - 2
Switch(config-if-range)# channel-group 1 mode active
Switch(config-if-range)# exit
Switch(config)# interface port-channel 1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20,30
Switch(config-if)# end
Switch# show etherchannel summary
```

Contoh 4.1 Perintah konfigurasi EtherChannel menggunakan LACP pada Cisco IOS

b. Contoh Aplikasi

EtherChannel banyak diterapkan pada tautan antara switch distribution dan switch access yang melayani trafik tinggi, misalnya menggabungkan dua tautan GigabitEthernet menjadi satu Port-Channel berkapasitas 2 Gbps, sekaligus memberikan redundansi apabila salah satu kabel terputus.

4.2 Layer 3 Switching

a. Penjelasan Konsep/Teori

Layer 3 switching adalah kemampuan sebuah switch untuk melakukan fungsi routing (Layer 3) selain fungsi switching (Layer 2) yang menjadi fungsi dasarnya. Berbeda dengan router konvensional yang memproses routing menggunakan perangkat lunak (software-based routing) sehingga relatif lebih lambat, Layer 3 switch memproses keputusan routing menggunakan perangkat keras khusus (Application-Specific Integrated Circuit atau ASIC), sehingga mampu melakukan routing dengan kecepatan mendekati kecepatan switching Layer 2.

Terdapat dua jenis interface pada Layer 3 switch yang perlu dipahami.

- Switched Port (Access/Trunk) — port yang beroperasi pada Layer 2 sebagaimana switch pada umumnya, digunakan untuk menghubungkan perangkat pengguna akhir atau tautan trunk antar-switch.
- Routed Port — port fisik yang dikonfigurasi untuk beroperasi murni pada Layer 3 (menggunakan perintah no switchport), sehingga dapat diberikan alamat IP secara langsung layaknya interface pada router, umumnya digunakan untuk tautan point-to-point antar-switch Layer 3 atau ke router.

Agar Layer 3 switch dapat melakukan routing antar-VLAN, fitur routing harus diaktifkan secara eksplisit menggunakan perintah global ip routing, karena secara default sebagian besar switch Cisco beroperasi murni sebagai perangkat Layer 2. Konfigurasi dasar Layer 3 switching dicontohkan pada perintah berikut.

```
Switch(config)# ip routing
Switch(config)# interface gigabitEthernet 0/3
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.252
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch# show ip route
```

Contoh 4.2 Perintah mengaktifkan ip routing dan konfigurasi routed port pada Layer 3 switch

b. Contoh Aplikasi

Pada jaringan kampus dengan model hierarchical three-tier (Bab 2), fungsi Layer 3 switching umumnya diterapkan pada lapisan distribution, sehingga proses routing antar-VLAN dapat dilakukan lebih dekat dengan pengguna, mengurangi beban pada lapisan core yang berfungsi murni sebagai backbone berkecepatan tinggi.

4.3 Inter-VLAN Routing dan Load Balancing

a. Penjelasan Konsep/Teori

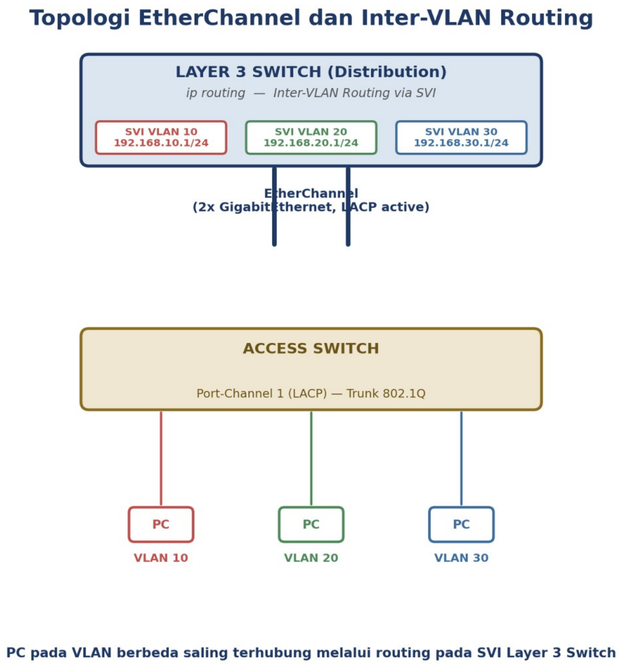
Inter-VLAN routing adalah proses routing yang memungkinkan perangkat pada satu VLAN berkomunikasi dengan perangkat pada VLAN lain. Pada jaringan enterprise modern, inter-VLAN routing umumnya diimplementasikan menggunakan switched virtual interface (SVI) pada Layer 3 switch, yaitu interface virtual yang mewakili satu VLAN tertentu dan diberikan alamat IP yang berfungsi sebagai default gateway bagi seluruh perangkat pada VLAN tersebut. Pendekatan ini menggantikan metode lama yang disebut router-on-a-stick (menggunakan satu interface fisik router dengan sub-interface per VLAN), yang kurang efisien untuk jaringan berskala besar karena seluruh trafik antar-VLAN harus melalui satu tautan fisik tunggal menuju router.

Konfigurasi SVI untuk inter-VLAN routing pada Layer 3 switch dicontohkan pada perintah berikut, melanjutkan skema VLAN pada Bab 3 (VLAN 10 Keuangan, VLAN 20 Operasional, VLAN 30 SDM).

```
Switch(config)# interface vlan 10
Switch(config-if)# ip address 192.168.10.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface vlan 20
```

```
Switch(config-if)# ip address 192.168.20.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface vlan 30
Switch(config-if)# ip address 192.168.30.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch# show ip interface brief | include Vlan
```

Contoh 4.3 Perintah konfigurasi Switched Virtual Interface (SVI) untuk inter-VLAN routing



Gambar 4.1 Topologi EtherChannel dan Inter-VLAN Routing

Diagram di atas menggambarkan sebuah Layer 3 Switch pada lapisan distribution yang memiliki tiga SVI (VLAN 10, 20, dan 30) sekaligus berfungsi sebagai default gateway bagi masing-masing VLAN. Layer 3 Switch terhubung ke Access Switch melalui EtherChannel (Port-Channel 1) yang dibentuk dari dua tautan GigabitEthernet menggunakan LACP, dikonfigurasi sebagai trunk 802.1Q untuk membawa ketiga VLAN sekaligus. Pada Access Switch, setiap VLAN memiliki access port yang menghubungkan PC pengguna. Dengan konfigurasi ini, PC pada VLAN 10 dapat berkomunikasi dengan PC pada VLAN 20 maupun VLAN 30 melalui proses routing yang terjadi pada SVI Layer 3 Switch.

Selain fungsi routing, mekanisme load balancing pada EtherChannel menentukan bagaimana lalu lintas didistribusikan ke seluruh tautan fisik dalam satu bundel Port-Channel. Distribusi ini tidak dilakukan secara round-robin per paket, melainkan menggunakan algoritme hashing berdasarkan kombinasi informasi tertentu pada paket, seperti alamat MAC sumber/tujuan, alamat IP sumber/tujuan, atau nomor port Layer 4, tergantung metode yang dikonfigurasi. Penggunaan metode load balancing yang tepat penting untuk memastikan distribusi trafik merata ke seluruh tautan fisik, menghindari kondisi salah satu tautan menjadi jauh lebih sibuk dibandingkan tautan lainnya.

```
Switch(config)# port-channel load-balance src-dst-ip
Switch# show etherchannel load-balance
Switch# show etherchannel port-channel
```

Contoh 4.4 Perintah konfigurasi dan verifikasi metode load balancing pada EtherChannel

b. Contoh Aplikasi

Sebagai ilustrasi, pada kantor dengan tiga departemen yang telah dipisahkan ke dalam VLAN 10, 20, dan 30 (Bab 3), inter-VLAN routing memungkinkan karyawan Keuangan (VLAN 10) mengakses server aplikasi milik Operasional (VLAN 20) tanpa harus menyatukan kedua VLAN tersebut, sehingga keamanan dan segmentasi tetap terjaga sementara komunikasi antar-departemen tetap dapat berjalan sesuai kebijakan akses yang diinginkan.

C. RANGKUMAN

- EtherChannel menggabungkan beberapa tautan fisik menjadi satu tautan logis untuk meningkatkan bandwidth dan redundansi, dibentuk menggunakan protokol LACP (standar terbuka) atau PAgP (milik Cisco), dengan mode on manual yang tidak direkomendasikan.
- Seluruh port anggota EtherChannel harus memiliki konfigurasi yang identik (kecepatan, duplex, mode switchport, VLAN) agar dapat bergabung ke dalam satu bundel Port-Channel.
- Layer 3 switching memungkinkan switch melakukan fungsi routing menggunakan perangkat keras (ASIC), dengan dua jenis interface: switched port (Layer 2) dan routed port (Layer 3, menggunakan perintah no switchport).
- Inter-VLAN routing pada jaringan enterprise modern umumnya diimplementasikan menggunakan switched virtual interface (SVI) pada Layer 3 switch, menggantikan metode router-on-a-stick yang kurang efisien untuk jaringan berskala besar.
- Load balancing pada EtherChannel menggunakan algoritme hashing (berdasarkan MAC, IP, atau port Layer 4) untuk mendistribusikan trafik ke seluruh tautan fisik dalam satu bundel secara merata.

D. LATIHAN/SOAL

Petunjuk pengerjaan: Kerjakan seluruh soal berikut secara mandiri. Soal nomor 1–5 merupakan soal pemahaman konsep (jawaban singkat/uraian), soal nomor 6–8 merupakan soal konfigurasi (tuliskan perintah Cisco IOS yang diperlukan), dan soal nomor 9–10 merupakan soal analisis/troubleshooting. Seluruh soal mengacu pada capaian Sub-CPMK 2.2.

1. Jelaskan definisi EtherChannel dan dua manfaat utamanya bagi jaringan enterprise.

2. Jelaskan perbedaan antara protokol LACP dan PAgP, termasuk mode kerja masing-masing.

3. Mengapa konfigurasi mode on (manual) pada EtherChannel tidak direkomendasikan dalam praktik industri?

4. Jelaskan perbedaan antara switched port dan routed port pada Layer 3 switch.

5. Jelaskan konsep switched virtual interface (SVI) dan perannya dalam inter-VLAN routing.

6. Tuliskan perintah Cisco IOS lengkap untuk menggabungkan interface GigabitEthernet 0/3 dan 0/4 ke dalam EtherChannel menggunakan LACP dengan mode active, lalu menjadikannya trunk link.

7. Tuliskan perintah Cisco IOS lengkap untuk mengaktifkan ip routing dan membuat SVI VLAN 40 dengan alamat IP 192.168.40.1/24.

8. Tuliskan perintah Cisco IOS untuk mengubah metode load balancing EtherChannel menjadi berbasis kombinasi alamat IP sumber dan tujuan.

9. Pada saat verifikasi menggunakan perintah show etherchannel summary, status Port-Channel menunjukkan salah satu port anggota dalam kondisi suspended. Analisislah kemungkinan penyebab kondisi tersebut dan langkah troubleshooting yang perlu dilakukan.

10. Sebuah switch access baru saja dikonfigurasi dengan SVI VLAN 50, namun PC pada VLAN 50 tetap tidak dapat berkomunikasi dengan PC pada VLAN 10. Analisislah dua kemungkinan penyebab utama masalah tersebut, ditinjau dari aspek konfigurasi routing maupun VLAN.

E. DAFTAR PUSTAKA

Cisco Networking Academy. (2022). CCNP Enterprise: Core networking technologies (ENCOR) companion guide. Cisco Press.

Froom, R., Frahim, E., & Sivasubramanian, B. (2021). Implementing Cisco IP switched networks (SWITCH) foundation learning guide (2nd ed.). Cisco Press.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 1 (2nd ed.). Cisco Press.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 2 (2nd ed.). Cisco Press.

Teare, D., & Paquet, C. (2022). Implementing Cisco IP routing (ROUTE) foundation learning guide (2nd ed.). Cisco Press.

F. TUGAS/STUDI KASUS

Tugas Praktik: Konfigurasi EtherChannel dan Inter-VLAN Routing

Menggunakan simulator jaringan (Cisco Packet Tracer atau GNS3), bangunlah topologi yang terdiri atas satu Layer 3 Switch dan satu Access Switch, melanjutkan skema VLAN pada tugas praktik Bab 3 (VLAN 10 Keuangan, VLAN 20 Operasional, VLAN 30 SDM), dengan ketentuan sebagai berikut.

1. Hubungkan Layer 3 Switch dan Access Switch menggunakan dua tautan fisik yang digabungkan menjadi satu EtherChannel (Port-Channel 1) menggunakan protokol LACP mode active, dikonfigurasi sebagai trunk 802.1Q yang mengizinkan VLAN 10, 20, dan 30.

2. Aktifkan ip routing pada Layer 3 Switch, lalu buat SVI untuk ketiga VLAN dengan skema alamat: VLAN 10 → 192.168.10.1/24, VLAN 20 → 192.168.20.1/24, VLAN 30 → 192.168.30.1/24.

3. Konfigurasikan minimal satu PC pada setiap VLAN dengan alamat IP sesuai subnet masing-masing dan default gateway sesuai SVI yang relevan.

4. Uji konektivitas antar-PC pada VLAN yang berbeda (misalnya PC pada VLAN 10 melakukan ping ke PC pada VLAN 20) untuk memastikan inter-VLAN routing berjalan dengan benar.

5. Lakukan verifikasi menggunakan perintah show etherchannel summary, show ip route, dan show ip interface brief, lalu sertakan hasil tangkapan layar (screenshot) pada laporan.

Laporan praktik (mencakup topologi, seluruh perintah konfigurasi, dan hasil verifikasi) dikumpulkan dalam bentuk dokumen (PDF/Word) disertai file simulasi (.pkt/.gns3) sesuai tenggat waktu yang ditentukan dosen pengampu. Tugas ini dinilai menggunakan rubrik pada Rubrik Penilaian per Pertemuan 4 (aspek Tugas Praktik: Konfigurasi EtherChannel & Inter-VLAN Routing dan Partisipasi Diskusi: Diskusi Layer 3 Switching) sebagaimana tercantum pada Lampiran buku ajar ini.

BAB 5
ROUTING DINAMIS OSPF MULTI-AREA

A. PENDAHULUAN

1. Deskripsi Singkat

Bab ini membahas Open Shortest Path First (OSPF), salah satu protokol routing dinamis berbasis link-state yang paling banyak digunakan pada jaringan enterprise karena sifatnya yang terbuka (open standard), konvergensi cepat, dan mendukung skalabilitas melalui konsep pembagian jaringan ke dalam beberapa area (multi-area). Pembahasan diawali dengan konsep dasar OSPF dan proses pembentukan adjacency, dilanjutkan dengan peran Area Border Router (ABR) dalam menghubungkan antar-area, konfigurasi OSPF multi-area pada Cisco IOS, serta pemahaman metric/cost dan verifikasi konvergensi routing.

Materi pada bab ini merupakan kelanjutan dari Bab 4, di mana mahasiswa telah memahami Layer 3 switching dan inter-VLAN routing menggunakan SVI. Apabila inter-VLAN routing pada Bab 4 menangani komunikasi antar-VLAN dalam satu perangkat/lokasi, OSPF pada bab ini menangani pertukaran informasi routing antar-perangkat dan antar-lokasi pada skala jaringan enterprise yang lebih luas, menjadi dasar penting sebelum mahasiswa mempelajari protokol redundansi gateway pada Bab 6.

2. Capaian Pembelajaran Mata Kuliah (CPMK) yang Dicapai

Kode CPMK	:	CPMK-2
Rumusan CPMK	:	Mampu merancang dan mengonfigurasi topologi jaringan enterprise menggunakan VLAN, Layer 3 switching, routing dinamis, dan protokol redundansi gateway untuk mendukung high availability.
Bobot CPMK	:	29% dari keseluruhan capaian mata kuliah (bobot CPMK terbesar)
CPL yang Didukung	:	CPL-5 (kemampuan merancang, menginstalasi, mengonfigurasi, dan memelihara jaringan komputer)

3. Sub-CPMK yang Dicapai

Kode Sub-CPMK	:	Sub-CPMK 2.3
Rumusan Sub-CPMK	:	Mampu mengonfigurasi protokol routing dinamis OSPF multi-area pada jaringan enterprise.
Pertemuan	:	Pertemuan ke-5
Indikator Penilaian	:	Ketepatan konfigurasi dan konvergensi routing OSPF (dinilai melalui tugas individu), bobot 4% dari total penilaian mata kuliah.

4. Tujuan Pembelajaran Khusus (TPK)

Setelah mempelajari bab ini secara tuntas, mahasiswa diharapkan mampu:

1. Menjelaskan konsep dasar OSPF sebagai protokol routing link-state, termasuk proses pembentukan adjacency dan prinsip kerja algoritma Shortest Path First (SPF).

2. Menjelaskan konsep OSPF multi-area serta peran Area Border Router (ABR) dalam menghubungkan antar-area menuju area backbone (Area 0).

3. Mengonfigurasi OSPF multi-area pada router/Layer 3 switch menggunakan perintah Cisco IOS, termasuk penentuan router ID dan penetapan interface ke area yang sesuai.

4. Menghitung dan menjelaskan metric/cost OSPF serta pengaruhnya terhadap pemilihan jalur terbaik menuju suatu tujuan.

5. Memverifikasi konvergensi routing OSPF menggunakan perintah verifikasi Cisco IOS, serta menganalisis tabel routing dan status neighbor OSPF.

5. Peta Konsep

Alur pembahasan materi pada Bab 5 disajikan dalam peta konsep berikut, yang menggambarkan keterkaitan logis antar-subbab menuju pencapaian Sub-CPMK 2.3.

Konsep OSPF	→	**Area Border Router (ABR)**	→	**Konfigurasi OSPF Multi-Area**	→	**Metric/Cost & Verifikasi Konvergensi**

6. Prasyarat

Sebelum mempelajari bab ini, mahasiswa disarankan telah menguasai materi Bab 4 mengenai Layer 3 switching dan inter-VLAN routing, serta memahami konsep dasar routing statis, tabel routing (routing table), dan subnetting IP yang diperoleh pada mata kuliah jaringan komputer dasar.

B. URAIAN MATERI

5.1 Konsep OSPF

a. Penjelasan Konsep/Teori

Open Shortest Path First (OSPF) adalah protokol routing dinamis berbasis link-state yang bekerja di dalam satu sistem otonom (Autonomous System) dan merupakan standar terbuka (open standard) yang didefinisikan pada RFC 2328 (OSPFv2 untuk IPv4). Berbeda dengan protokol routing berbasis distance-vector yang hanya mengetahui arah dan jarak menuju suatu tujuan dari sudut pandang tetangga langsung, protokol link-state seperti OSPF memungkinkan setiap router memiliki peta topologi jaringan yang identik dan lengkap, sehingga dapat menghitung jalur terbaik secara independen menggunakan algoritma Shortest Path First (dikenal juga sebagai algoritma Dijkstra).

Proses kerja OSPF secara garis besar berlangsung melalui tahapan berikut.

- Neighbor Discovery — router OSPF saling mengirimkan paket Hello secara periodik (setiap 10 detik pada jaringan broadcast) untuk menemukan dan mengenali router tetangga (neighbor) yang berada pada segmen jaringan yang sama.
- Pembentukan Adjacency — setelah saling mengenali, dua router yang memenuhi syarat kecocokan parameter (area ID, subnet, hello/dead interval, dan autentikasi jika digunakan) akan membentuk hubungan adjacency, yaitu hubungan yang memungkinkan pertukaran informasi routing secara penuh.
- Pertukaran Link State Advertisement (LSA) — router yang telah membentuk adjacency saling bertukar LSA, yaitu paket yang berisi informasi mengenai status tautan (link) yang dimiliki router tersebut, sehingga seluruh router dalam satu area memiliki basis data topologi yang identik, disebut Link State Database (LSDB).
- Perhitungan SPF — setiap router menjalankan algoritma SPF terhadap LSDB yang dimilikinya untuk membangun pohon jalur terpendek (shortest path tree) menuju seluruh tujuan, yang kemudian digunakan untuk mengisi tabel routing.

Setiap router OSPF diidentifikasi dengan sebuah Router ID (RID) berupa alamat IP unik, yang ditentukan berdasarkan urutan prioritas berikut: (1) dikonfigurasi secara manual menggunakan perintah router-id; (2) apabila tidak dikonfigurasi manual, dipilih alamat IP tertinggi dari interface loopback yang aktif; (3) apabila tidak ada interface loopback, dipilih alamat IP tertinggi dari interface fisik yang aktif. Praktik terbaik industri merekomendasikan konfigurasi router-id secara manual menggunakan alamat loopback agar RID tetap stabil meskipun terjadi perubahan pada interface fisik.

Konfigurasi dasar OSPF single-area pada router/Layer 3 switch Cisco IOS dicontohkan pada perintah berikut.

```
Router(config)# router ospf 1
Router(config-router)# router-id 1.1.1.1
Router(config-router)# network 192.168.10.0 0.0.0.255 area 0
Router(config-router)# network 10.0.0.0 0.0.0.3 area 0
Router(config-router)# end
Router# show ip ospf neighbor
```

Contoh 5.1 Perintah konfigurasi dasar OSPF dan penetapan network ke Area 0

b. Contoh Aplikasi

OSPF banyak diterapkan pada jaringan enterprise dengan topologi kompleks yang melibatkan banyak router, misalnya jaringan kampus dengan puluhan gedung, karena kemampuannya melakukan konvergensi yang cepat ketika terjadi perubahan topologi (misalnya tautan terputus), dibandingkan protokol routing distance-vector yang konvergensinya relatif lebih lambat.

5.2 Area Border Router (ABR)

a. Penjelasan Konsep/Teori

Pada jaringan berskala besar, menjalankan OSPF dalam satu area tunggal (single area) akan menyebabkan ukuran Link State Database yang sangat besar pada setiap router, meningkatkan beban komputasi algoritma SPF, serta memperlambat konvergensi ketika terjadi perubahan topologi. Untuk mengatasi hal tersebut, OSPF mendukung pembagian jaringan ke dalam beberapa area (multi-area), di mana setiap area memiliki LSDB tersendiri yang lebih kecil, sementara ringkasan informasi routing antar-area dipertukarkan melalui Area Border Router (ABR).

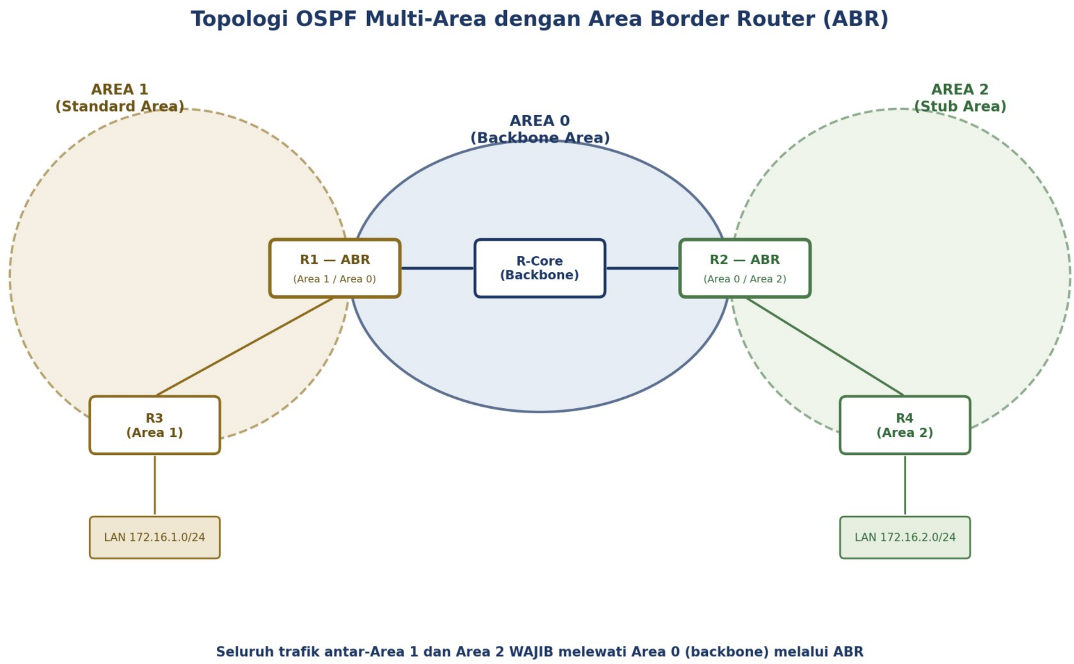
OSPF mengenal beberapa jenis area dengan karakteristik yang berbeda, sebagaimana dirangkum pada Tabel 5.1 berikut.

Jenis Area	Area ID	Karakteristik Utama
Backbone Area	Area 0	Area wajib pada setiap jaringan OSPF multi-area; seluruh area lain harus terhubung langsung ke Area 0
Standard Area	Selain 0	Menerima seluruh jenis LSA (intra-area, inter-area, dan eksternal); area non-backbone paling umum digunakan
Stub Area	Selain 0	Tidak menerima LSA eksternal (rute dari luar sistem otonom); rute default digunakan untuk menuju tujuan di luar area
Totally Stubby Area	Selain 0	Tidak menerima LSA eksternal maupun inter-area; hanya menerima satu rute default dari ABR (fitur

Jenis Area	Area ID	Karakteristik Utama
		khusus Cisco)
Not-So-Stubby Area (NSSA)	Selain 0	Mirip stub area, namun tetap dapat menyisipkan rute eksternal terbatas dari router ASBR di dalam area tersebut

Tabel 5.1 Jenis-Jenis Area pada OSPF Multi-Area

Sebuah router berperan sebagai ABR apabila memiliki minimal satu interface yang berada pada Area 0 dan minimal satu interface lain yang berada pada area non-backbone. ABR bertanggung jawab menghasilkan ringkasan rute (Summary LSA) dari satu area untuk disebarkan ke area lainnya melalui Area 0, sehingga aturan fundamental dalam OSPF multi-area adalah seluruh trafik antar-area non-backbone wajib melewati Area 0, tidak diperbolehkan ada koneksi langsung antar-dua area non-backbone (kecuali menggunakan fitur virtual link untuk kondisi khusus).



Gambar 5.1 Topologi OSPF Multi-Area dengan Area Border Router

Diagram di atas menggambarkan jaringan OSPF yang terbagi menjadi tiga area: Area 0 (backbone) di tengah, Area 1 (standard area) di sebelah kiri, dan Area 2 (stub area) di sebelah kanan. Router R1 berperan sebagai ABR yang menghubungkan Area 1 dengan Area 0, sedangkan Router R2 berperan sebagai ABR yang menghubungkan Area 0 dengan Area 2. Router R3 pada Area 1 dan Router R4 pada Area 2 merupakan router internal area yang melayani jaringan LAN pada masing-masing lokasi. Sesuai aturan OSPF multi-area, seluruh trafik yang mengalir antara Area 1 dan Area 2 wajib melewati Area 0 melalui kedua ABR tersebut.

b. Contoh Aplikasi

Pada jaringan kampus dengan lima gedung, setiap gedung dapat dijadikan satu area OSPF tersendiri (misalnya Area 1 hingga Area 5), sementara jaringan tulang punggung yang menghubungkan seluruh gedung dijadikan Area 0. Dengan pembagian ini, perubahan topologi pada satu gedung (misalnya penambahan switch baru) tidak akan memicu perhitungan ulang SPF secara menyeluruh pada seluruh router di gedung lain, sehingga meningkatkan stabilitas dan skalabilitas jaringan secara keseluruhan.

5.3 Konfigurasi OSPF Multi-Area

a. Penjelasan Konsep/Teori

Konfigurasi OSPF multi-area pada dasarnya merupakan perluasan dari konfigurasi OSPF single-area, dengan perbedaan utama pada penetapan interface ke area yang berbeda-beda sesuai posisi router dalam topologi. Mengacu pada topologi Gambar 5.1, berikut adalah contoh konfigurasi pada ketiga jenis router: ABR (R1), router backbone (R-Core), dan router internal area (R3).

```
! Konfigurasi pada R1 (ABR – Area 1 dan Area 0)
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 172.16.1.0 0.0.0.255 area 1
R1(config-router)# network 10.0.0.0 0.0.0.3 area 0
R1(config-router)# end

! Konfigurasi pada R-Core (Backbone – Area 0)
R-Core(config)# router ospf 1
R-Core(config-router)# router-id 2.2.2.2
R-Core(config-router)# network 10.0.0.0 0.0.0.3 area 0
R-Core(config-router)# network 10.0.0.4 0.0.0.3 area 0
R-Core(config-router)# end

! Konfigurasi pada R3 (Router Internal – Area 1)
R3(config)# router ospf 1
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 172.16.1.0 0.0.0.255 area 1
R3(config-router)# end
```

Contoh 5.2 Perintah konfigurasi OSPF multi-area pada ABR, router backbone, dan router internal area

Perlu diperhatikan bahwa perintah network pada OSPF menggunakan wildcard mask (kebalikan dari subnet mask), bukan subnet mask biasa. Sebagai contoh, subnet 172.16.1.0/24 (subnet mask 255.255.255.0) dituliskan dengan wildcard mask 0.0.0.255 pada perintah network.

b. Contoh Aplikasi

Dalam praktiknya, administrator jaringan perlu merencanakan skema pembagian area terlebih dahulu (area planning) sebelum melakukan konfigurasi, dengan mempertimbangkan batas fisik lokasi (gedung, lantai, kampus) serta ukuran maksimum router dan LSA yang direkomendasikan per area agar performa konvergensi tetap optimal.

5.4 Metric/Cost dan Verifikasi Konvergensi

a. Penjelasan Konsep/Teori

OSPF menggunakan metric yang disebut cost untuk menentukan jalur terbaik menuju suatu tujuan, di mana jalur dengan total cost kumulatif terendah akan dipilih sebagai jalur utama pada tabel routing. Cost pada setiap interface dihitung menggunakan formula berikut.

Formula Perhitungan OSPF Cost

Cost = Reference Bandwidth ÷ Bandwidth Interface

Secara default, Cisco IOS menggunakan reference bandwidth sebesar 100 Mbps. Sebagai contoh, interface FastEthernet (100 Mbps) memiliki cost 1, sedangkan interface Ethernet 10 Mbps memiliki cost 10. Pada jaringan modern dengan tautan GigabitEthernet (1000 Mbps) atau lebih tinggi, nilai reference bandwidth default seringkali tidak lagi relevan karena menghasilkan cost minimum yang sama (dibulatkan menjadi 1) untuk berbagai kecepatan interface yang berbeda, sehingga administrator perlu menyesuaikan reference bandwidth menggunakan perintah auto-cost reference-bandwidth agar OSPF dapat membedakan cost antar-tautan berkecepatan tinggi secara lebih akurat.

Total cost menuju suatu tujuan merupakan penjumlahan cost seluruh interface keluar (outbound) yang dilalui sepanjang jalur tersebut, bukan dihitung berdasarkan jumlah hop sebagaimana pada protokol distance-vector. Dengan demikian, OSPF dapat memilih jalur dengan jumlah hop lebih banyak namun bandwidth lebih tinggi, apabila total cost jalur tersebut lebih rendah dibandingkan jalur dengan hop lebih sedikit namun bandwidth rendah.

Verifikasi konvergensi routing OSPF dilakukan menggunakan beberapa perintah show pada Cisco IOS, sebagaimana dicontohkan berikut.

```
Router# show ip ospf neighbor
Router# show ip ospf database
Router# show ip route ospf
Router# show ip protocols
Router# show ip ospf interface brief
```

Contoh 5.3 Perintah verifikasi status neighbor, database, dan tabel routing OSPF

Perintah show ip ospf neighbor menampilkan daftar router tetangga beserta status adjacency (idealnya berstatus FULL untuk jaringan point-to-point atau DR/BDR pada jaringan broadcast); show ip ospf database menampilkan isi Link State Database; show ip route ospf menampilkan rute-rute yang dipelajari melalui OSPF pada tabel routing (ditandai dengan kode O untuk intra-area dan O IA untuk inter-area); sedangkan show ip protocols menampilkan ringkasan konfigurasi protokol routing yang aktif, termasuk area yang dikonfigurasi pada router tersebut. Konvergensi dinyatakan tercapai apabila seluruh router memiliki status neighbor yang stabil dan tabel routing yang konsisten tanpa perubahan (flapping) yang berulang.

b. Contoh Aplikasi

Pemahaman metric/cost sangat penting ketika administrator jaringan merancang jalur redundan (misalnya dua tautan WAN menuju kantor cabang yang sama); dengan mengatur cost pada masing-masing interface, administrator dapat menentukan jalur mana yang menjadi jalur utama (primary path) dan jalur mana yang menjadi jalur cadangan (backup path) tanpa harus menonaktifkan OSPF pada tautan cadangan tersebut.

C. RANGKUMAN

- OSPF adalah protokol routing dinamis berbasis link-state yang bersifat open standard, bekerja melalui tahapan neighbor discovery, pembentukan adjacency, pertukaran LSA, dan perhitungan SPF untuk membangun tabel routing.
- OSPF multi-area membagi jaringan menjadi beberapa area untuk mengurangi ukuran LSDB dan mempercepat konvergensi, dengan Area 0 (backbone) sebagai area wajib yang menjadi penghubung seluruh area lain.
- Area Border Router (ABR) adalah router yang memiliki interface pada Area 0 dan area non-backbone sekaligus, bertanggung jawab menghasilkan ringkasan rute antar-area; seluruh trafik antar-area non-backbone wajib melewati Area 0.
- OSPF mengenal beberapa jenis area (standard, stub, totally stubby, NSSA) dengan karakteristik penerimaan LSA yang berbeda-beda, disesuaikan dengan kebutuhan efisiensi tabel routing pada area tersebut.
- OSPF menggunakan cost (dihitung dari reference bandwidth dibagi bandwidth interface) sebagai metric pemilihan jalur terbaik, dengan konvergensi diverifikasi menggunakan perintah show ip ospf neighbor, show ip route ospf, dan show ip protocols.

D. LATIHAN/SOAL

Petunjuk pengerjaan: Kerjakan seluruh soal berikut secara mandiri. Soal nomor 1–5 merupakan soal pemahaman konsep (jawaban singkat/uraian), soal nomor 6–8 merupakan soal konfigurasi dan perhitungan, dan soal nomor 9–10 merupakan soal analisis/troubleshooting. Seluruh soal mengacu pada capaian Sub-CPMK 2.3.

1. Jelaskan perbedaan mendasar antara protokol routing berbasis link-state dan distance-vector.

2. Jelaskan empat tahapan proses kerja OSPF, dari neighbor discovery hingga perhitungan SPF.

3. Mengapa Area 0 (backbone) wajib ada pada setiap jaringan OSPF multi-area?

4. Jelaskan peran dan tanggung jawab utama Area Border Router (ABR) dalam jaringan OSPF multi-area.

5. Jelaskan perbedaan antara stub area dan totally stubby area.

6. Hitunglah cost OSPF untuk interface dengan bandwidth 100 Mbps dan 10 Mbps menggunakan reference bandwidth default (100 Mbps).

7. Tuliskan perintah Cisco IOS lengkap untuk mengonfigurasi OSPF process 10 dengan router-id 5.5.5.5 dan menetapkan network 192.168.5.0/24 ke Area 2.

8. Tuliskan perintah Cisco IOS untuk menampilkan status neighbor OSPF beserta ringkasan konfigurasi protokol routing yang sedang aktif pada suatu router.

9. Pada saat verifikasi menggunakan perintah show ip ospf neighbor, status salah satu neighbor tertahan pada kondisi EXSTART/EXCHANGE dan tidak pernah mencapai FULL. Analisislah kemungkinan penyebab masalah tersebut.

10. Dua router terhubung melalui dua jalur berbeda menuju tujuan yang sama: Jalur A melalui satu tautan FastEthernet (100 Mbps), dan Jalur B melalui dua tautan Ethernet 10 Mbps yang berurutan. Hitunglah cost masing-masing jalur dan tentukan jalur mana yang akan dipilih OSPF sebagai jalur utama.

E. DAFTAR PUSTAKA

Cisco Networking Academy. (2022). CCNP Enterprise: Core networking technologies (ENCOR) companion guide. Cisco Press.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 2 (2nd ed.). Cisco Press.

Teare, D., & Paquet, C. (2022). Implementing Cisco IP routing (ROUTE) foundation learning guide (2nd ed.). Cisco Press.

Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson.

Stallings, W. (2023). Network security essentials: Applications and standards (7th ed.). Pearson.

F. TUGAS/STUDI KASUS

Tugas Individu: Konfigurasi OSPF Multi-Area

Menggunakan simulator jaringan (Cisco Packet Tracer atau GNS3), bangunlah topologi OSPF multi-area yang terdiri atas minimal empat router dengan ketentuan sebagai berikut, mengacu pada skema topologi Gambar 5.1.

1. Bangun tiga area OSPF: Area 0 (backbone, terdiri atas minimal satu router backbone), Area 1, dan Area 2, masing-masing dengan minimal satu router internal area yang melayani satu jaringan LAN.

2. Konfigurasikan router-id secara manual pada setiap router menggunakan interface loopback.

3. Pastikan kedua router pada batas antar-area dikonfigurasi sebagai ABR yang menghubungkan area non-backbone dengan Area 0.

4. Lakukan verifikasi status neighbor pada seluruh router menggunakan show ip ospf neighbor dan pastikan seluruh adjacency mencapai status FULL.

5. Lakukan verifikasi tabel routing menggunakan show ip route ospf pada router di Area 1 dan pastikan router tersebut memiliki rute menuju subnet LAN di Area 2 (ditandai kode O IA), lalu sertakan hasil tangkapan layar (screenshot) seluruh perintah verifikasi pada laporan.

Laporan tugas individu (mencakup topologi, seluruh perintah konfigurasi, dan hasil verifikasi) dikumpulkan dalam bentuk dokumen (PDF/Word) disertai file simulasi (.pkt/.gns3) sesuai tenggat waktu yang ditentukan dosen pengampu. Tugas ini dinilai menggunakan rubrik pada Rubrik Penilaian per Pertemuan 5 (aspek Tugas Individu: Konfigurasi OSPF Multi-Area dan Partisipasi Diskusi: Diskusi Routing Dinamis) sebagaimana tercantum pada Lampiran buku ajar ini.

BAB 6
PROTOKOL REDUNDANSI GATEWAY DAN HIGH AVAILABILITY

A. PENDAHULUAN BAB

1. Deskripsi Singkat

Bab ini membahas First Hop Redundancy Protocol (FHRP), yaitu kelompok protokol yang menyediakan default gateway redundan bagi perangkat pengguna akhir, sehingga apabila router/Layer 3 switch yang berperan sebagai gateway utama mengalami kegagalan, perangkat pengguna tetap dapat terhubung ke jaringan tanpa perlu mengubah konfigurasi default gateway secara manual. Tiga protokol FHRP yang dibahas adalah HSRP, VRRP, dan GLBP, dilanjutkan dengan konsep high availability secara umum, serta praktik skenario failover dan pengujian redundansi.

Materi pada bab ini merupakan penutup dari rangkaian topik CPMK-2 (Bab 3 hingga Bab 6) yang membahas perancangan dan konfigurasi topologi jaringan enterprise. Setelah mahasiswa menguasai VLAN dan trunking (Bab 3), EtherChannel dan inter-VLAN routing (Bab 4), serta routing dinamis OSPF (Bab 5), protokol redundansi gateway pada bab ini melengkapi aspek ketersediaan (availability) pada lapisan distribution, sebagai bekal sebelum mahasiswa mempelajari teknologi WAN pada Bab 7.

2. Capaian Pembelajaran Mata Kuliah (CPMK) yang Dicapai

Kode CPMK	:	CPMK-2
Rumusan CPMK	:	Mampu merancang dan mengonfigurasi topologi jaringan enterprise menggunakan VLAN, Layer 3 switching, routing dinamis, dan protokol redundansi gateway untuk mendukung high availability.
Bobot CPMK	:	29% dari keseluruhan capaian mata kuliah (bobot CPMK terbesar)
CPL yang Didukung	:	CPL-5 (kemampuan merancang, menginstalasi, mengonfigurasi, dan memelihara jaringan komputer)

3. Sub-CPMK yang Dicapai

Kode Sub-CPMK	:	Sub-CPMK 2.4
Rumusan Sub-CPMK	:	Mampu menerapkan protokol redundansi gateway (HSRP/VRRP/GLBP) untuk mendukung high availability.
Pertemuan	:	Pertemuan ke-6
Indikator Penilaian	:	Keberhasilan skenario failover sesuai desain redundansi

(dinilai melalui tugas kelompok), bobot 4% dari total penilaian mata kuliah.

4. Tujuan Pembelajaran Khusus (TPK)

Setelah mempelajari bab ini secara tuntas, mahasiswa diharapkan mampu:

1. Menjelaskan konsep First Hop Redundancy Protocol (FHRP) serta membandingkan karakteristik HSRP, VRRP, dan GLBP.

2. Mengonfigurasi HSRP dan VRRP pada router/Layer 3 switch menggunakan perintah Cisco IOS, termasuk pengaturan priority dan preemption.

3. Menjelaskan konsep high availability serta peran object tracking dalam mempercepat proses failover gateway.

4. Merancang skenario failover gateway pada topologi jaringan enterprise sederhana menggunakan protokol redundansi yang sesuai.

5. Menguji dan memverifikasi keberhasilan skenario failover gateway menggunakan perintah verifikasi Cisco IOS.

5. Peta Konsep

Alur pembahasan materi pada Bab 6 disajikan dalam peta konsep berikut, yang menggambarkan keterkaitan logis antar-subbab menuju pencapaian Sub-CPMK 2.4.

HSRP, VRRP, dan GLBP	→	**Konsep High Availability**	→	**Skenario Failover & Pengujian Redundansi**

6. Prasyarat

Sebelum mempelajari bab ini, mahasiswa disarankan telah menguasai materi Bab 4 mengenai inter-VLAN routing menggunakan SVI dan Bab 5 mengenai routing dinamis OSPF, serta memahami konsep dasar default gateway dan alamat MAC pada jaringan Ethernet.

B. URAIAN MATERI

6.1 HSRP, VRRP, dan GLBP

a. Penjelasan Konsep/Teori

First Hop Redundancy Protocol (FHRP) adalah kelompok protokol yang memungkinkan dua atau lebih router/Layer 3 switch bekerja sama membentuk satu default gateway virtual bagi perangkat pengguna akhir pada suatu subnet. Perangkat pengguna cukup dikonfigurasi dengan satu alamat IP gateway (alamat IP virtual), tanpa perlu mengetahui router fisik mana yang sedang aktif meneruskan trafik pada waktu tertentu. Terdapat tiga protokol FHRP yang umum digunakan pada jaringan enterprise berbasis Cisco, yaitu HSRP, VRRP, dan GLBP.

- HSRP (Hot Standby Router Protocol) — protokol milik Cisco (proprietary) yang menetapkan satu router sebagai active (meneruskan seluruh trafik) dan satu atau lebih router lain sebagai standby (siaga, siap mengambil alih apabila active gagal). Router dengan nilai priority tertinggi (default 100) menjadi active; apabila terjadi kesamaan priority, alamat IP tertinggi yang menjadi penentu.
- VRRP (Virtual Router Redundancy Protocol) — protokol standar terbuka (open standard, RFC 5798) dengan konsep kerja serupa HSRP, namun menggunakan istilah master (setara active) dan backup (setara standby). VRRP memiliki kelebihan berupa dukungan multi-vendor, serta konsep IP owner, yaitu apabila alamat IP virtual sama persis dengan alamat IP fisik salah satu router, router tersebut akan selalu menjadi master tanpa perlu priority tertinggi.
- GLBP (Gateway Load Balancing Protocol) — protokol milik Cisco yang mengatasi salah satu keterbatasan HSRP dan VRRP, yaitu hanya satu router yang aktif meneruskan trafik sementara router lain menganggur (idle). GLBP memungkinkan hingga empat router meneruskan trafik secara bersamaan (load balancing), melalui satu router yang berperan sebagai Active Virtual Gateway (AVG) yang membagikan alamat MAC virtual berbeda kepada setiap Active Virtual Forwarder (AVF).

Perbandingan karakteristik ketiga protokol tersebut dirangkum pada Tabel 6.1 berikut.

Aspek	HSRP	VRRP	GLBP
Kepemilikan	Cisco (proprietary)	Standar terbuka (RFC 5798)	Cisco (proprietary)
Istilah Peran	Active / Standby	Master / Backup	AVG / AVF
Load Balancing	Tidak (satu router aktif)	Tidak (satu router aktif)	Ya (hingga 4 router aktif)
Priority Default	100	100	100
Alamat MAC Virtual	0000.0c07.acXX	0000.5e00.01XX	0007.b400.XXYY (per AVF)

Tabel 6.1 Perbandingan HSRP, VRRP, dan GLBP

Konfigurasi dasar HSRP dan VRRP pada router/Layer 3 switch Cisco IOS dicontohkan pada perintah berikut, menggunakan VLAN 10 (192.168.10.0/24) sebagai subnet yang dilayani.

```
! Konfigurasi HSRP pada GW1 (calon Active)
GW1(config)# interface vlan 10
GW1(config-if)# ip address 192.168.10.2 255.255.255.0
GW1(config-if)# standby 1 ip 192.168.10.1
GW1(config-if)# standby 1 priority 150
GW1(config-if)# standby 1 preempt
GW1(config-if)# end

! Konfigurasi VRRP pada GW1 (calon Master)
GW1(config)# interface vlan 10
GW1(config-if)# vrrp 1 ip 192.168.10.1
GW1(config-if)# vrrp 1 priority 150
GW1(config-if)# end
```

Contoh 6.1 Perintah konfigurasi dasar HSRP dan VRRP pada Cisco IOS

b. Contoh Aplikasi

HSRP dan VRRP banyak digunakan pada jaringan kantor/kampus dengan dua router distribution yang melayani satu VLAN yang sama, sedangkan GLBP lebih sesuai diterapkan pada jaringan dengan trafik sangat tinggi yang ingin memanfaatkan seluruh kapasitas kedua router secara bersamaan, bukan hanya satu router aktif dan satu router menganggur.

6.2 Konsep High Availability

a. Penjelasan Konsep/Teori

High availability (ketersediaan tinggi) adalah karakteristik desain sistem yang memastikan layanan tetap dapat diakses dengan gangguan seminimal mungkin, termasuk pada saat terjadi kegagalan komponen. Pada konteks redundansi gateway, terdapat beberapa konsep penting yang menentukan efektivitas high availability.

- Priority — nilai yang menentukan router mana yang menjadi active/master; router dengan priority tertinggi akan dipilih sebagai gateway utama.
- Preemption — mekanisme yang memungkinkan router dengan priority lebih tinggi untuk mengambil alih kembali peran active/master apabila router tersebut kembali aktif setelah sempat mengalami gangguan; tanpa preemption, router yang sempat menjadi standby akan tetap pada perannya meskipun router asal sudah pulih.
- Hello dan Hold Timer — interval waktu pengiriman pesan Hello antar-router (default 3 detik pada HSRP) dan batas waktu tunggu sebelum router standby menganggap router active telah gagal (default 10 detik pada HSRP); semakin kecil

nilai timer, semakin cepat proses failover terdeteksi, namun meningkatkan beban trafik kontrol.

- Object Tracking — mekanisme yang memungkinkan router menurunkan nilai priority-nya secara otomatis apabila suatu kondisi tertentu terpenuhi, misalnya ketika interface uplink menuju jaringan inti mengalami gangguan, sehingga memicu proses failover meskipun router itu sendiri masih beroperasi normal.

Object tracking menjadi sangat penting karena FHRP secara default hanya memantau status router pasangannya (melalui pesan Hello), namun tidak mengetahui apakah router active masih memiliki konektivitas ke jaringan inti (upstream). Tanpa object tracking, sebuah router dapat tetap berstatus active meskipun tautan uplink-nya terputus, menyebabkan black hole trafik (trafik diterima namun tidak dapat diteruskan ke tujuan). Konfigurasi object tracking pada HSRP dicontohkan pada perintah berikut.

```
GW1(config)# track 1 interface gigabitEthernet 0/1 line-protocol
GW1(config)# interface vlan 10
GW1(config-if)# standby 1 track 1 decrement 60
GW1(config-if)# end
```

Contoh 6.2 Perintah konfigurasi object tracking pada interface uplink untuk HSRP

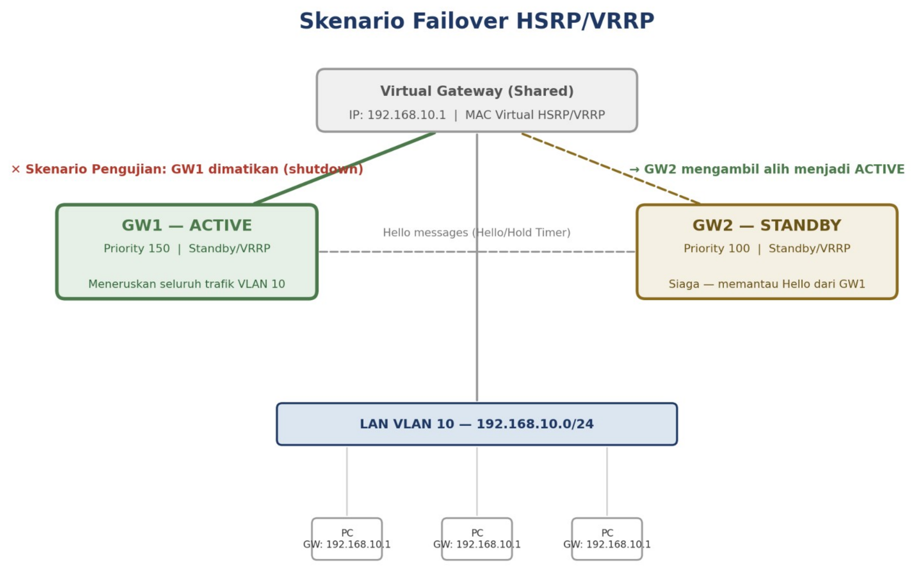
b. Contoh Aplikasi

Pada jaringan enterprise dengan dua router distribution yang masing-masing memiliki tautan uplink terpisah menuju router core, object tracking memastikan bahwa apabila tautan uplink pada router active terputus (meskipun router itu sendiri masih menyala), priority-nya akan diturunkan secara otomatis sehingga router standby yang masih memiliki uplink aktif akan mengambil alih peran active, menghindari kondisi trafik yang diterima namun tidak dapat diteruskan.

6.3 Skenario Failover Gateway dan Pengujian Redundansi

a. Penjelasan Konsep/Teori

Sub-bab ini menyajikan skenario praktik terintegrasi untuk merancang dan menguji failover gateway menggunakan HSRP pada topologi dua router/Layer 3 switch (GW1 dan GW2) yang melayani satu VLAN yang sama. Skenario dirancang agar GW1 berperan sebagai active (priority 150, dengan preempt diaktifkan) dan GW2 berperan sebagai standby (priority default 100), sebagaimana digambarkan pada Gambar 6.1 berikut.



Gambar 6.1 Skenario Failover HSRP/VRRP

Diagram di atas menggambarkan dua gateway (GW1 dan GW2) yang membentuk satu virtual gateway dengan alamat IP virtual 192.168.10.1, melayani LAN VLAN 10 yang berisi beberapa PC pengguna. GW1 berperan sebagai ACTIVE (priority 150) dan meneruskan seluruh trafik dari PC menuju jaringan luar, sedangkan GW2 berperan sebagai STANDBY (priority 100) dan hanya memantau pesan Hello dari GW1 melalui hello/hold timer. Pada skenario pengujian, GW1 dimatikan (shutdown) untuk mensimulasikan kegagalan, sehingga GW2 akan mengambil alih peran ACTIVE dan melanjutkan penerusan trafik tanpa mengubah konfigurasi default gateway pada sisi PC.

Tahapan pengujian skenario failover dilakukan sebagai berikut: (1) memastikan status awal GW1 sebagai active dan GW2 sebagai standby melalui perintah verifikasi; (2) menjalankan proses ping berkelanjutan (continuous ping) dari salah satu PC menuju alamat di luar jaringan lokal melalui virtual gateway; (3) memutus/mematikan GW1 (baik dengan mencabut kabel maupun perintah shutdown pada interface) untuk mensimulasikan kegagalan; (4) mengamati jumlah paket ping yang hilang (packet loss) selama proses failover berlangsung; dan (5) memverifikasi bahwa GW2 telah berubah status menjadi active setelah hold timer terlampaui.

Verifikasi status dan hasil failover dilakukan menggunakan perintah berikut.

```
GW1# show standby brief
GW2# show standby brief
GW1# show standby vlan10
GW2# show standby vlan10
! Setelah GW1 dimatikan:
GW2# show standby brief
```

Contoh 6.3 Perintah verifikasi status HSRP sebelum dan sesudah skenario failover

Perintah show standby brief menampilkan ringkasan status HSRP pada seluruh interface, meliputi peran (active/standby), alamat IP virtual, dan priority masing-masing router; sedangkan show standby vlan10 menampilkan detail status HSRP pada interface VLAN 10 secara spesifik, termasuk informasi timer dan status preemption. Keberhasilan skenario redundansi ditandai dengan perubahan status GW2 dari standby menjadi active setelah GW1 dimatikan, disertai packet loss yang minimal selama proses konvergensi berlangsung.

b. Contoh Aplikasi

Skenario pengujian failover semacam ini merupakan praktik standar dalam pengelolaan jaringan enterprise, biasa dilakukan secara berkala (disaster recovery drill) untuk memastikan mekanisme redundansi benar-benar berfungsi sebagaimana dirancang sebelum benar-benar dibutuhkan pada kondisi gangguan nyata.

C. RANGKUMAN

- FHRP (First Hop Redundancy Protocol) memungkinkan dua atau lebih router membentuk satu default gateway virtual, terdiri atas tiga protokol utama: HSRP (Cisco, active/standby), VRRP (standar terbuka, master/backup), dan GLBP (Cisco, mendukung load balancing hingga 4 router aktif).
- Priority menentukan router mana yang menjadi active/master; preemption memungkinkan router dengan priority lebih tinggi mengambil alih kembali perannya setelah pulih dari gangguan.
- Object tracking memungkinkan router menurunkan priority secara otomatis ketika tautan uplink-nya terputus, mencegah kondisi black hole trafik pada router yang masih berstatus active namun kehilangan konektivitas upstream.
- Skenario failover gateway diuji dengan mematikan router active secara sengaja dan mengamati proses pengambilalihan oleh router standby, diverifikasi menggunakan perintah show standby brief.
- Pemilihan protokol FHRP yang tepat (HSRP, VRRP, atau GLBP) disesuaikan dengan kebutuhan lingkungan multi-vendor dan kebutuhan pemanfaatan kapasitas seluruh router gateway secara bersamaan.

D. LATIHAN/SOAL

Petunjuk pengerjaan: Kerjakan seluruh soal berikut secara mandiri. Soal nomor 1–5 merupakan soal pemahaman konsep (jawaban singkat/uraian), soal nomor 6–8 merupakan soal konfigurasi, dan soal nomor 9–10 merupakan soal analisis/troubleshooting. Seluruh soal mengacu pada capaian Sub-CPMK 2.4.

1. Jelaskan tujuan utama penggunaan FHRP pada jaringan enterprise.

2. Jelaskan perbedaan istilah peran router pada HSRP dan VRRP.

3. Jelaskan keunggulan utama GLBP dibandingkan HSRP dan VRRP.

4. Jelaskan fungsi preemption pada protokol redundansi gateway, disertai contoh kondisi ketika preemption berperan penting.

5. Jelaskan konsep object tracking dan mengapa fitur ini penting untuk mencegah kondisi black hole trafik.

6. Tuliskan perintah Cisco IOS lengkap untuk mengonfigurasi HSRP group 5 dengan virtual IP 172.16.5.1, priority 200, dan preempt diaktifkan pada interface VLAN 5.

7. Tuliskan perintah Cisco IOS untuk mengonfigurasi object tracking yang memantau interface GigabitEthernet 0/2 dan menurunkan priority HSRP sebesar 50 apabila interface tersebut down.

8. Tuliskan perintah Cisco IOS untuk menampilkan ringkasan status HSRP pada seluruh interface suatu router.

9. Dua router dikonfigurasi HSRP dengan GW1 priority 150 (preempt aktif) dan GW2 priority 100. Setelah GW1 sempat mati dan GW2 menjadi active, GW1 kembali menyala. Analisislah apa yang akan terjadi pada peran masing-masing router.

10. Sebuah organisasi memiliki jaringan dengan tautan uplink ganda menuju ISP berbeda pada masing-masing router gateway, namun tidak menggunakan object tracking. Analisislah risiko yang dapat terjadi apabila salah satu tautan uplink terputus, serta rekomendasikan solusi konfigurasi yang tepat.

E. DAFTAR PUSTAKA

Cisco Networking Academy. (2022). CCNP Enterprise: Core networking technologies (ENCOR) companion guide. Cisco Press.

Froom, R., Frahim, E., & Sivasubramanian, B. (2021). Implementing Cisco IP switched networks (SWITCH) foundation learning guide (2nd ed.). Cisco Press.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 2 (2nd ed.). Cisco Press.

Teare, D., & Paquet, C. (2022). Implementing Cisco IP routing (ROUTE) foundation learning guide (2nd ed.). Cisco Press.

Stallings, W. (2023). Network security essentials: Applications and standards (7th ed.). Pearson.

F. TUGAS/STUDI KASUS

Tugas Kelompok: Skenario Failover Gateway

Bentuklah kelompok kerja (3–4 mahasiswa). Menggunakan simulator jaringan (Cisco Packet Tracer atau GNS3), bangunlah topologi yang terdiri atas dua router/Layer 3 switch (GW1 dan GW2) yang melayani satu VLAN yang sama, mengacu pada skema topologi Gambar 6.1, dengan ketentuan sebagai berikut.

1. Konfigurasikan HSRP pada kedua gateway dengan virtual IP 192.168.10.1, GW1 sebagai active (priority 150, preempt aktif) dan GW2 sebagai standby (priority default).

2. Konfigurasikan object tracking pada GW1 yang memantau interface uplink-nya, dengan penurunan priority yang cukup besar apabila uplink tersebut down (agar GW2 dapat mengambil alih peran active).

3. Konfigurasikan minimal tiga PC pada VLAN yang dilayani, dengan default gateway mengarah ke alamat IP virtual.

4. Lakukan pengujian failover dengan mematikan (shutdown) interface GW1 sambil menjalankan continuous ping dari salah satu PC menuju jaringan luar, lalu catat jumlah packet loss yang terjadi selama proses konvergensi.

5. Lakukan verifikasi status HSRP pada kedua gateway sebelum dan sesudah pengujian menggunakan show standby brief, lalu sertakan hasil tangkapan layar (screenshot) beserta analisis waktu konvergensi pada laporan.

Laporan kelompok (mencakup topologi, seluruh perintah konfigurasi, hasil pengujian, dan analisis waktu konvergensi) dikumpulkan dalam bentuk dokumen (PDF/Word) disertai file simulasi (.pkt/.gns3) sesuai tenggat waktu yang ditentukan dosen pengampu. Tugas ini dinilai menggunakan rubrik pada Rubrik Penilaian per Pertemuan 6 (aspek Tugas Kelompok: Skenario Failover Gateway dan Partisipasi Diskusi: Diskusi Kelompok Skenario Failover) sebagaimana tercantum pada Lampiran buku ajar ini.

BAB 7
TEKNOLOGI WAN ENTERPRISE

A. PENDAHULUAN BAB

1. Deskripsi Singkat

Bab ini membuka pembahasan Capaian Pembelajaran Mata Kuliah ketiga (CPMK-3) mengenai teknologi WAN dan konektivitas enterprise. Apabila Bab 3 hingga Bab 6 berfokus pada perancangan dan konfigurasi jaringan lokal (LAN) pada satu lokasi, bab ini beralih membahas bagaimana organisasi menghubungkan berbagai lokasi yang terpisah secara geografis (kantor pusat, kantor cabang, gudang, pusat data) melalui jaringan area luas (Wide Area Network atau WAN). Tiga teknologi WAN utama yang dibahas adalah MPLS, leased line, dan broadband, dilengkapi dengan perbandingan sistematis dari aspek biaya, keandalan, latensi, dan skalabilitas, serta kriteria pemilihan teknologi WAN yang tepat sesuai kebutuhan organisasi multi-cabang.

Bab ini bersifat konseptual dan analitis, menekankan kemampuan mahasiswa dalam menganalisis dan memberikan justifikasi bisnis-teknis, berbeda dengan bab-bab sebelumnya yang menekankan praktik konfigurasi perangkat. Pemahaman yang baik terhadap materi bab ini menjadi dasar penting sebelum mahasiswa mempelajari konfigurasi VPN site-to-site pada Bab 9 dan konsep SD-WAN pada Bab 10, sekaligus menjadi materi terakhir yang diujikan pada Ujian Tengah Semester (Pertemuan 8), yang mencakup keseluruhan materi Bab 1 hingga Bab 7.

2. Capaian Pembelajaran Mata Kuliah (CPMK) yang Dicapai

Kode CPMK	:	CPMK-3
Rumusan CPMK	:	Mampu menerapkan teknologi WAN dan konektivitas enterprise (WAN tradisional, VPN, SD-WAN, dan konektivitas cloud) sesuai kebutuhan organisasi multi-lokasi.
Bobot CPMK	:	21% dari keseluruhan capaian mata kuliah
CPL yang Didukung	:	CPL-5 (kemampuan merancang, menginstalasi, mengonfigurasi, dan memelihara jaringan komputer) dan CPL-10 (pengembangan diri berkelanjutan mengikuti perkembangan teknologi jaringan)

3. Sub-CPMK yang Dicapai

Kode Sub-CPMK	:	Sub-CPMK 3.1
Rumusan Sub-CPMK	:	Mampu menjelaskan dan membandingkan teknologi WAN (MPLS, leased line, broadband) untuk kebutuhan enterprise.
Pertemuan	:	Pertemuan ke-7
Indikator Penilaian	:	Ketepatan justifikasi pemilihan teknologi WAN (dinilai melalui tugas analisis), bobot 3% dari total penilaian mata kuliah.

4. Tujuan Pembelajaran Khusus (TPK)

Setelah mempelajari bab ini secara tuntas, mahasiswa diharapkan mampu:

1. Menjelaskan konsep dan karakteristik teknologi WAN MPLS, leased line, dan broadband.

2. Membandingkan ketiga teknologi WAN tersebut dari aspek biaya, keandalan, latensi, dan skalabilitas.

3. Menganalisis kriteria pemilihan teknologi WAN yang tepat berdasarkan kebutuhan organisasi multi-cabang.

4. Menjelaskan konsep pendekatan hybrid WAN yang menggabungkan lebih dari satu teknologi untuk optimalisasi biaya dan keandalan.

5. Merekomendasikan teknologi WAN yang sesuai untuk studi kasus organisasi multi-lokasi, disertai justifikasi teknis dan bisnis yang tepat.

5. Peta Konsep

Alur pembahasan materi pada Bab 7 disajikan dalam peta konsep berikut, yang menggambarkan keterkaitan logis antar-subbab menuju pencapaian Sub-CPMK 3.1.

6. Prasyarat

Sebelum mempelajari bab ini, mahasiswa disarankan telah memahami materi Bab 1 mengenai karakteristik jaringan enterprise multi-lokasi dan Bab 5 mengenai routing dinamis OSPF, karena beberapa konsep routing pada WAN (khususnya pada MPLS VPN) memanfaatkan prinsip routing yang serupa dengan yang telah dipelajari sebelumnya.

B. URAIAN MATERI

7.1 MPLS, Leased Line, dan Broadband

a. Penjelasan Konsep/Teori

Wide Area Network (WAN) adalah jaringan yang menghubungkan lokasi-lokasi yang secara geografis terpisah, biasanya melalui infrastruktur milik penyedia layanan (service provider) karena organisasi pada umumnya tidak memiliki hak untuk menggelar kabel sendiri melintasi area publik antar-kota atau antar-negara. Terdapat tiga kategori teknologi WAN yang paling umum digunakan pada jaringan enterprise, yaitu sebagai berikut.

- MPLS (Multiprotocol Label Switching) — teknologi WAN berbasis label switching yang disediakan sebagai layanan terkelola (managed service) oleh penyedia layanan, di mana paket data diteruskan berdasarkan label pendek, bukan melalui pencarian tabel routing IP secara penuh pada setiap hop, sehingga forwarding menjadi lebih cepat. Implementasi paling umum pada jaringan enterprise adalah MPLS Layer 3 VPN, yang memungkinkan topologi konektivitas any-to-any antar-seluruh lokasi organisasi melalui satu jaringan penyedia layanan tunggal, disertai dukungan Class of Service (CoS) untuk memprioritaskan trafik kritis seperti VoIP.
- Leased Line — sirkuit privat dedicated point-to-point yang disewa langsung dari penyedia layanan, menghubungkan dua lokasi secara eksklusif tanpa berbagi bandwidth dengan pelanggan lain. Leased line menawarkan bandwidth simetris (kecepatan unggah dan unduh sama) yang tetap (fixed) dan sangat andal, namun dengan biaya yang relatif tinggi, terutama untuk jarak yang jauh, dan topologi yang terbentuk umumnya point-to-point atau hub-and-spoke (memerlukan sirkuit terpisah untuk setiap pasangan lokasi yang ingin terhubung langsung).
- Broadband — akses internet publik bersama (shared) yang dijual secara massal kepada pelanggan bisnis maupun rumahan, mencakup teknologi seperti DSL, kabel (cable), dan fiber to the home/business (FTTH/FTTB). Dibandingkan MPLS dan leased line, broadband menawarkan biaya jauh lebih rendah dan kecepatan yang kompetitif, namun performanya dapat bervariasi (tidak konsisten) karena bandwidth dibagi bersama pengguna lain, serta umumnya tidak disertai Service Level Agreement (SLA) yang seketat layanan dedicated.

Karena broadband melewati jaringan internet publik yang tidak terjamin keamanannya, penggunaan broadband untuk menghubungkan antar-lokasi organisasi secara aman umumnya dipadukan dengan teknologi Virtual Private Network (VPN) yang akan dibahas secara mendalam pada Bab 9.

b. Contoh Aplikasi

Sebuah perusahaan perbankan dengan kebutuhan transaksi real-time yang sangat kritis umumnya memilih MPLS sebagai tulang punggung WAN utama karena jaminan kualitas layanan (SLA) dan Class of Service yang ditawarkan; sebuah pabrik yang hanya perlu menghubungkan dua lokasi tetap dalam kota yang sama dapat memanfaatkan leased line; sedangkan sebuah jaringan retail dengan puluhan gerai kecil seringkali memanfaatkan broadband yang dipadukan VPN sebagai solusi konektivitas dengan biaya terjangkau.

7.2 Perbandingan Biaya, Keandalan, Latensi, dan Skalabilitas

a. Penjelasan Konsep/Teori

Pemilihan teknologi WAN yang tepat memerlukan pertimbangan menyeluruh terhadap beberapa aspek utama, yaitu biaya, keandalan, latensi, dan skalabilitas, sebagaimana dirangkum pada Tabel 7.1 berikut.

Aspek	MPLS	Leased Line	Broadband
Biaya	Tinggi (biaya per lokasi + biaya bandwidth)	Sangat tinggi (terutama untuk jarak jauh)	Rendah hingga sedang
Keandalan (SLA)	Tinggi, disertai SLA dari provider	Sangat tinggi, dedicated dan eksklusif	Bervariasi, umumnya tanpa SLA ketat
Latensi	Rendah dan konsisten	Sangat rendah dan konsisten (dedicated)	Bervariasi, dapat tinggi pada jam sibuk
Skalabilitas Topologi	Sangat baik (any-to-any melalui satu jaringan provider)	Terbatas (memerlukan sirkuit baru per pasangan lokasi)	Baik, namun bergantung ketersediaan layanan di lokasi
Dukungan QoS/CoS	Ya, mendukung prioritas kelas trafik	Tidak relevan (dedicated, tidak ada kontensi)	Umumnya tidak tersedia

Tabel 7.1 Perbandingan Teknologi WAN (MPLS, Leased Line, Broadband)

Keempat aspek tersebut seringkali saling bertentangan (trade-off): teknologi dengan keandalan dan latensi terbaik (leased line) umumnya memiliki biaya tertinggi dan skalabilitas topologi paling terbatas, sedangkan teknologi dengan biaya paling rendah (broadband) memiliki keandalan yang paling sulit diprediksi. MPLS umumnya diposisikan sebagai titik keseimbangan (middle ground) antara ketiganya, meskipun dengan biaya yang tetap lebih tinggi dibandingkan broadband.

b. Contoh Aplikasi

Sebagai ilustrasi, sebuah rumah sakit yang mengandalkan sistem rekam medis elektronik antar-cabang memerlukan keandalan dan latensi rendah yang konsisten (mengarah pada MPLS atau leased line), sedangkan sebuah jaringan kedai kopi dengan puluhan gerai yang hanya memerlukan konektivitas untuk sistem kasir dan Wi-Fi pelanggan dapat memprioritaskan biaya rendah (mengarah pada broadband dengan VPN).

7.3 Pemilihan Teknologi WAN

a. Penjelasan Konsep/Teori

Proses pemilihan teknologi WAN yang tepat bagi suatu organisasi perlu mempertimbangkan beberapa faktor keputusan berikut, selain keempat aspek teknis pada Tabel 7.1.

- Kekritisan Aplikasi — aplikasi yang sangat sensitif terhadap latensi dan kehilangan paket (misalnya VoIP, transaksi finansial real-time, aplikasi kontrol industri) memerlukan teknologi WAN dengan SLA dan QoS yang terjamin, seperti MPLS atau leased line.
- Anggaran (Budget) — organisasi dengan keterbatasan anggaran namun memiliki banyak lokasi (misalnya jaringan retail dengan puluhan hingga ratusan gerai) umumnya lebih realistis menggunakan broadband, karena biaya MPLS atau leased line per lokasi akan sangat membebani anggaran total.
- Jumlah dan Sebaran Lokasi — semakin banyak lokasi yang perlu saling terhubung secara langsung (any-to-any), semakin MPLS menjadi pilihan yang lebih efisien dibandingkan leased line yang memerlukan sirkuit terpisah untuk setiap pasangan lokasi.
- Ketersediaan Layanan — tidak seluruh teknologi WAN tersedia di semua lokasi geografis; daerah terpencil mungkin hanya memiliki akses broadband nirkabel atau satelit, sehingga membatasi pilihan yang tersedia bagi organisasi.
- Proyeksi Pertumbuhan — organisasi yang berencana membuka banyak cabang baru dalam waktu dekat perlu mempertimbangkan teknologi WAN yang mudah diskalakan tanpa proses pengadaan yang lama, sebagaimana ditawarkan oleh solusi berbasis broadband dan SD-WAN (dibahas lebih lanjut pada Bab 10).

Pendekatan Hybrid WAN

Dalam praktik industri saat ini, semakin banyak organisasi enterprise mengadopsi pendekatan hybrid WAN, yaitu menggabungkan lebih dari satu teknologi WAN secara bersamaan pada satu lokasi — misalnya MPLS sebagai jalur utama (primary path) untuk trafik kritis, dipadukan dengan broadband berbiaya rendah sebagai jalur cadangan (backup path) atau untuk trafik non-kritis seperti akses internet umum. Pendekatan ini memberikan keseimbangan antara keandalan dan efisiensi biaya, dan menjadi dasar konseptual bagi teknologi SD-WAN yang akan dibahas secara mendalam pada Bab 10.

b. Contoh Aplikasi

Sebuah perusahaan manufaktur dengan satu pabrik utama dan sepuluh gudang distribusi regional dapat menerapkan pendekatan hybrid: MPLS untuk menghubungkan pabrik utama dengan pusat data (data center) mengingat kekritisan sistem produksi, sementara kesepuluh gudang distribusi cukup menggunakan broadband dengan VPN mengingat kebutuhan konektivitasnya yang lebih sederhana (sinkronisasi data inventori secara berkala).

C. RANGKUMAN

- WAN menghubungkan lokasi-lokasi organisasi yang terpisah secara geografis, umumnya melalui infrastruktur milik penyedia layanan, dengan tiga teknologi utama: MPLS, leased line, dan broadband.
- MPLS menawarkan konektivitas any-to-any yang skalabel dengan dukungan QoS, leased line menawarkan keandalan dan latensi terbaik namun biaya tertinggi dan skalabilitas topologi terbatas, sedangkan broadband menawarkan biaya rendah namun keandalan yang bervariasi.
- Pemilihan teknologi WAN mempertimbangkan trade-off antara biaya, keandalan, latensi, dan skalabilitas, yang seringkali saling bertentangan satu sama lain.
- Faktor keputusan pemilihan teknologi WAN meliputi kekritisan aplikasi, anggaran, jumlah dan sebaran lokasi, ketersediaan layanan di lokasi tersebut, serta proyeksi pertumbuhan organisasi.
- Pendekatan hybrid WAN menggabungkan lebih dari satu teknologi (misalnya MPLS sebagai primary dan broadband sebagai backup) untuk mengoptimalkan keseimbangan antara keandalan dan biaya, menjadi dasar konseptual teknologi SD-WAN.

D. LATIHAN/SOAL

Petunjuk pengerjaan: Kerjakan seluruh soal berikut secara mandiri. Soal nomor 1–6 merupakan soal pemahaman konsep (jawaban singkat/uraian), sedangkan soal nomor 7–10 merupakan soal analisis yang memerlukan penjelasan disertai justifikasi teknis dan bisnis. Seluruh soal mengacu pada capaian Sub-CPMK 3.1.

1. Jelaskan definisi WAN dan mengapa organisasi umumnya bergantung pada penyedia layanan untuk membangun konektivitas WAN.

2. Jelaskan konsep dasar MPLS dan keunggulan utamanya dibandingkan teknologi WAN tradisional.

3. Jelaskan karakteristik leased line, termasuk kelebihan dan keterbatasannya.

4. Jelaskan karakteristik broadband dan mengapa teknologi ini umumnya dipadukan dengan VPN untuk konektivitas antar-lokasi organisasi.

5. Jelaskan perbedaan topologi any-to-any pada MPLS dengan topologi hub-and-spoke yang umum ditemui pada leased line.

6. Jelaskan konsep pendekatan hybrid WAN beserta manfaat utamanya.

7. Sebuah rumah sakit dengan satu rumah sakit pusat dan lima klinik satelit memerlukan konektivitas dengan latensi rendah dan keandalan tinggi untuk sistem rekam medis elektronik. Analisislah teknologi WAN yang paling sesuai beserta justifikasinya.

8. Sebuah jaringan minimarket dengan 150 gerai yang tersebar di seluruh Indonesia memiliki anggaran terbatas namun tetap memerlukan konektivitas untuk sistem kasir dan pelaporan penjualan harian. Analisislah teknologi WAN yang paling sesuai beserta justifikasinya.

9. Berdasarkan Tabel 7.1, jelaskan mengapa leased line memiliki skalabilitas topologi yang terbatas dibandingkan MPLS, meskipun keandalannya lebih tinggi.

10. Sebuah perusahaan multinasional memiliki kantor pusat, dua pabrik, dan dua puluh kantor penjualan regional. Rancanglah rekomendasi pendekatan hybrid WAN untuk perusahaan tersebut, dengan menjelaskan teknologi WAN apa yang sebaiknya digunakan pada masing-masing jenis lokasi beserta alasannya.

E. DAFTAR PUSTAKA

Cisco Networking Academy. (2022). CCNP Enterprise: Core networking technologies (ENCOR) companion guide. Cisco Press.

Marschke, D., Doraswamy, N., & Ghosh, A. (2021). SD-WAN: A comprehensive approach for enterprise networking. Packt Publishing.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 2 (2nd ed.). Cisco Press.

Teare, D., & Paquet, C. (2022). Implementing Cisco IP routing (ROUTE) foundation learning guide (2nd ed.). Cisco Press.

Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson.

F. TUGAS/STUDI KASUS

Tugas Analisis: Pemilihan Teknologi WAN untuk Organisasi Multi-Cabang

Perhatikan studi kasus berikut.

Studi Kasus: PT Sinergi Logistik Nusantara

PT Sinergi Logistik Nusantara adalah perusahaan logistik dan pergudangan dengan satu kantor pusat di Jakarta yang menjalankan sistem manajemen gudang (Warehouse Management System) terpusat, dua pusat distribusi regional di Surabaya dan Medan yang beroperasi 24 jam dan sangat bergantung pada akses real-time ke sistem terpusat, serta 40 titik agen pengiriman kecil yang tersebar di berbagai kota kecil, yang hanya memerlukan akses sesekali untuk input data pengiriman dan pengecekan status paket.

Susunlah laporan analisis individu (2–3 halaman) yang memuat:

1. Rekomendasi teknologi WAN (MPLS, leased line, broadband, atau kombinasi/hybrid) untuk masing-masing kategori lokasi (kantor pusat–pusat distribusi, dan kantor pusat–agen pengiriman kecil).

2. Justifikasi teknis untuk setiap rekomendasi, ditinjau dari aspek kekritisan aplikasi, biaya, keandalan, dan latensi.

3. Estimasi trade-off (kelebihan dan risiko) dari rekomendasi yang diajukan, dibandingkan dengan alternatif teknologi WAN lain yang tidak dipilih.

4. Tabel ringkasan rekomendasi akhir yang memetakan setiap kategori lokasi dengan teknologi WAN yang direkomendasikan.

Laporan analisis dikumpulkan dalam bentuk dokumen (PDF/Word) sesuai tenggat waktu yang ditentukan dosen pengampu. Tugas ini dinilai menggunakan rubrik pada Rubrik Penilaian per Pertemuan 7 (aspek Tugas Analisis: Pemilihan Teknologi WAN dan Partisipasi Diskusi: Diskusi Teknologi WAN) sebagaimana tercantum pada Lampiran buku ajar ini. Materi Bab 1 hingga Bab 7 akan diujikan pada Ujian Tengah Semester (Pertemuan 8).

BAB 8
EVALUASI TENGAH SEMESTER

(Rangkuman dan Kisi-Kisi Materi Bab 1–7)

A. PENGANTAR EVALUASI TENGAH SEMESTER

Ujian Tengah Semester (UTS) dilaksanakan pada Pertemuan ke-8 dan mencakup keseluruhan materi yang telah dibahas pada Bab 1 hingga Bab 7, meliputi konsep dasar dan model desain jaringan enterprise (CPMK-1), perancangan dan konfigurasi switching, routing dinamis, serta redundansi gateway (CPMK-2), hingga pengenalan teknologi WAN enterprise (CPMK-3, Sub-CPMK 3.1). UTS dilaksanakan dalam bentuk ujian tertulis dan/atau praktik, sesuai kebijakan dosen pengampu, dengan bobot 30% dari keseluruhan nilai akhir mata kuliah.

Bab ini disusun sebagai panduan persiapan UTS bagi mahasiswa, berisi rangkuman komprehensif seluruh materi, peta keterkaitan antar-bab, kisi-kisi soal, contoh latihan soal simulasi, serta rubrik penilaian yang akan digunakan. Bab ini bukan merupakan materi baru, melainkan konsolidasi dari Bab 1 hingga Bab 7 yang telah dipelajari sebelumnya.

Cakupan CPMK dan Sub-CPMK yang Diujikan

CPMK	Sub-CPMK yang Diujikan	Bab Terkait
CPMK-1	Sub-CPMK 1.1, Sub-CPMK 1.2 (seluruh)	Bab 1, Bab 2
CPMK-2	Sub-CPMK 2.1, 2.2, 2.3, 2.4 (seluruh)	Bab 3, Bab 4, Bab 5, Bab 6
CPMK-3	Sub-CPMK 3.1 (sebagian — hanya materi sebelum UTS)	Bab 7

CPL yang diukur melalui UTS adalah CPL-2 (penguasaan konsep teoretis bidang teknik komputer) dan CPL-5 (kemampuan merancang, menginstalasi, mengonfigurasi, dan memelihara jaringan komputer), sebagaimana tercantum pada RPS mata kuliah Enterprise Networking.

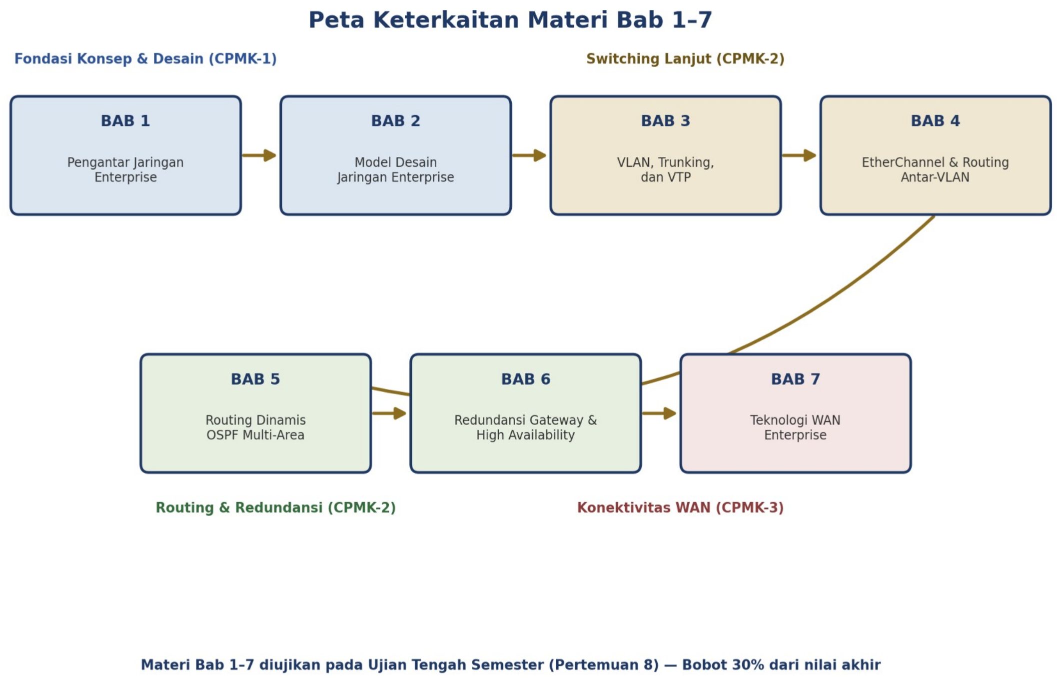
B. RANGKUMAN KOMPREHENSIF MATERI BAB 1–7

Tabel berikut menyajikan ringkasan poin-poin kunci dari setiap bab sebagai bahan tinjauan cepat (quick review) sebelum menghadapi UTS. Untuk pemahaman mendalam, mahasiswa tetap disarankan mempelajari kembali uraian materi lengkap pada masing-masing bab.

Bab	Konsep Kunci
Bab 1 Pengantar Jaringan Enterprise	• Definisi dan karakteristik jaringan enterprise (skala besar, high availability, skalabilitas, segmentasi, keamanan berlapis, manajemen terpusat) • Perbedaan jaringan enterprise dengan jaringan SOHO (jumlah pengguna, topologi, redundansi, manajemen) • Tiga kebutuhan utama: skalabilitas, ketersediaan (availability), dan keamanan (security)
Bab 2 Model Desain Jaringan Enterprise	• Model hierarchical three-tier: core (backbone), distribution (kebijakan & agregasi), access (titik masuk pengguna) • Model spine-leaf: full-mesh spine-leaf, latensi konsisten maksimal 2 hop, untuk data center • Kriteria pemilihan: skalabilitas, latensi, biaya, kompleksitas pengelolaan
Bab 3 VLAN, Trunking, dan VTP	• VLAN: segmentasi Layer 2, jenis (data, voice, native, management, default), rentang ID normal & extended • Trunking 802.1Q: tagging, native VLAN, allowed VLAN list • VTP: mode server/client/transparent, risiko configuration revision number
Bab 4 EtherChannel dan Routing Antar-VLAN	• EtherChannel: agregasi link, protokol LACP (standar terbuka) dan PAgP (Cisco) • Layer 3 switching: switched port vs routed port (no switchport), ip routing • Inter-VLAN routing via SVI; load balancing berbasis hashing (MAC/IP/port)
Bab 5 Routing Dinamis OSPF Multi-Area	• OSPF: link-state, tahapan neighbor discovery → adjacency → LSA → SPF • Multi-area: Area 0 (backbone) wajib, ABR menghubungkan area non-backbone ke Area 0 • Jenis area: standard, stub, totally stubby, NSSA; cost = reference bandwidth ÷ bandwidth interface
Bab 6 Redundansi Gateway dan High Availability	• FHRP: HSRP (active/standby, Cisco), VRRP (master/backup, standar terbuka), GLBP (load balancing, Cisco) • Priority menentukan router aktif; preemption; object tracking mencegah black hole trafik • Skenario failover diuji dengan mematikan gateway aktif dan verifikasi show standby brief
Bab 7 Teknologi WAN Enterprise	• MPLS: any-to-any, mendukung QoS/CoS, biaya sedang-tinggi • Leased line: dedicated, keandalan tertinggi, biaya tertinggi, skalabilitas topologi terbatas • Broadband: biaya rendah, keandalan bervariasi, umumnya dipadukan VPN; pendekatan hybrid WAN

C. PETA KETERKAITAN ANTAR-MATERI

Diagram berikut menggambarkan keterkaitan logis antar-bab yang telah dipelajari, mengelompokkan materi ke dalam empat klaster besar sesuai kontribusinya terhadap CPMK: fondasi konsep dan desain (Bab 1–2), switching lanjut (Bab 3–4), routing dan redundansi (Bab 5–6), serta konektivitas WAN (Bab 7).



Gambar 8.1 Peta Keterkaitan Materi Bab 1–7

Diagram di atas menunjukkan alur pembelajaran dari Bab 1 hingga Bab 7 secara berjenjang. Bab 1 dan Bab 2 membangun fondasi konsep dan model desain jaringan enterprise (CPMK-1). Bab 3 dan Bab 4 memperdalam keterampilan switching lanjut berupa VLAN, trunking, EtherChannel, dan inter-VLAN routing (CPMK-2). Bab 5 dan Bab 6 melanjutkan dengan routing dinamis OSPF dan redundansi gateway untuk mendukung high availability (CPMK-2). Bab 7 memperluas cakupan ke konektivitas WAN antar-lokasi (CPMK-3), menjadi jembatan menuju materi VPN dan SD-WAN yang akan dibahas setelah UTS.

D. KISI-KISI SOAL UJIAN TENGAH SEMESTER

Kisi-kisi berikut disusun berdasarkan Rubrik Penilaian Pertemuan 8 pada dokumen RPS, yang mengelompokkan soal UTS ke dalam tiga bagian besar sesuai cakupan Sub-CPMK.

Bagian	Cakupan Sub-CPMK	Bab Terkait	Bentuk Soal	Bobot
I	Sub-CPMK 1.1–1.2 (Konsep Arsitektur & Model Desain)	Bab 1–2	Uraian konsep	8%
II	Sub-CPMK 2.1–2.2 (Switching: VLAN, Trunking, EtherChannel)	Bab 3–4	Konfigurasi CLI + analisis	11%
III	Sub-CPMK 2.3–2.4, 3.1 (Routing OSPF, Redundansi Gateway, Analisis WAN)	Bab 5–7	Konfigurasi CLI + analisis	11%

Total bobot UTS: 30% dari nilai akhir mata kuliah.

E. LATIHAN SOAL SIMULASI UJIAN TENGAH SEMESTER

Latihan soal berikut disusun menyerupai format UTS sesungguhnya, terbagi ke dalam tiga bagian sesuai kisi-kisi pada Bagian D. Kerjakan sebagai simulasi mandiri sebelum menghadapi UTS yang sebenarnya.

Bagian I — Konsep Arsitektur dan Model Desain Enterprise (Bobot 8%)

1. Jelaskan tiga karakteristik utama yang membedakan jaringan enterprise dari jaringan SOHO.

2. Bandingkan model hierarchical three-tier dan spine-leaf dari aspek latensi dan skalabilitas.

3. Sebuah kantor pemerintahan berlantai tiga dengan trafik yang didominasi akses pengguna ke server internal berencana membangun jaringan baru. Rekomendasikan model desain yang sesuai beserta alasannya.

4. Jelaskan mengapa lapisan core pada model hierarchical three-tier dirancang untuk tidak melakukan pemrosesan kebijakan yang kompleks.

Bagian II — Switching: VLAN, Trunking, dan EtherChannel (Bobot 11%)

1. Tuliskan perintah Cisco IOS lengkap untuk membuat VLAN 50 dengan nama GUDANG dan menetapkan port FastEthernet 0/8 sebagai access port pada VLAN tersebut.

2. Jelaskan fungsi native VLAN pada trunk link 802.1Q dan risiko yang timbul apabila native VLAN pada kedua ujung trunk tidak sama.

3. Jelaskan risiko utama penggunaan VTP mode server tanpa pengelolaan configuration revision number yang tepat.

4. Tuliskan perintah Cisco IOS untuk menggabungkan interface GigabitEthernet 0/1 dan 0/2 menjadi EtherChannel menggunakan LACP mode active.

5. Jelaskan perbedaan switched port dan routed port pada Layer 3 switch, disertai contoh perintah konfigurasinya.

6. Sebuah SVI VLAN 60 telah dikonfigurasi dengan benar, namun PC pada VLAN 60 tetap tidak dapat mengakses PC pada VLAN 10. Analisislah dua kemungkinan penyebab utama masalah tersebut.

Bagian III — Routing OSPF, Redundansi Gateway, dan Analisis WAN (Bobot 11%)

1. Jelaskan mengapa Area 0 (backbone) wajib ada pada setiap jaringan OSPF multi-area.

2. Tuliskan perintah Cisco IOS lengkap untuk mengonfigurasi OSPF process 1 dengan router-id 4.4.4.4 dan menetapkan network 172.20.1.0/24 ke Area 1.

3. Hitunglah cost OSPF untuk interface dengan bandwidth 1000 Mbps menggunakan reference bandwidth default (100 Mbps).

4. Jelaskan perbedaan antara HSRP dan GLBP dari aspek pemanfaatan kapasitas router gateway.

5. Jelaskan fungsi object tracking pada konfigurasi HSRP dan berikan contoh skenario ketika fitur ini berperan penting.

6. Sebuah perusahaan dengan sepuluh cabang kecil dan anggaran terbatas memerlukan konektivitas WAN yang terjangkau namun tetap aman. Rekomendasikan teknologi WAN yang sesuai beserta justifikasinya.

F. PETUNJUK PENGERJAAN DAN TATA TERTIB UJIAN

- UTS berlangsung selama 100 menit, sesuai alokasi waktu 2 SKS teori (2 × 50 menit) pada Pertemuan ke-8.
- Bagian I (konsep) dikerjakan secara tertutup (closed book) tanpa akses catatan maupun internet, kecuali dinyatakan lain oleh dosen pengampu.
- Bagian II dan III yang bersifat konfigurasi dapat dikerjakan menggunakan simulator jaringan (Packet Tracer/GNS3) apabila UTS dilaksanakan dalam format praktik, sesuai kebijakan dosen pengampu.
- Mahasiswa wajib menuliskan jawaban secara sistematis dan menyertakan penjelasan/justifikasi pada soal analisis, bukan hanya jawaban akhir.
- Kecurangan akademik dalam bentuk apa pun (menyontek, kerja sama tanpa izin, penggunaan alat bantu yang tidak diizinkan) akan dikenai sanksi sesuai peraturan akademik Politeknik Negeri Padang yang berlaku.

G. RUBRIK PENILAIAN UJIAN TENGAH SEMESTER

Rubrik berikut merupakan rubrik resmi Pertemuan 8 sebagaimana tercantum pada dokumen RPS dan Rubrik Penilaian per Pertemuan mata kuliah Enterprise Networking, digunakan sebagai acuan penilaian jawaban UTS.

Pemahaman Konsep Arsitektur & Model Desain Enterprise (Sub-CPMK 1.1–1.2) (Bobot: 8%)

Kategori	Skor	Indikator
Sangat Baik	85–100	Menjelaskan karakteristik dan model desain jaringan enterprise secara tepat, sistematis, dan mampu mengaitkan konsep dengan kebutuhan organisasi nyata.
Baik	70–84	Menjelaskan konsep dengan benar namun kurang sistematis atau kurang mengaitkan dengan konteks nyata.
Cukup	55–69	Menjelaskan sebagian konsep dengan benar, terdapat kesalahan pemahaman pada aspek penting.
Kurang	< 55	Tidak mampu menjelaskan konsep arsitektur/model desain enterprise dengan tepat.

Ketepatan Konfigurasi/Analisis Switching (VLAN, Trunking, EtherChannel — Sub-CPMK 2.1–2.2) (Bobot: 11%)

Kategori	Skor	Indikator
Sangat Baik	85–100	Soal konfigurasi dan analisis VLAN/trunking/EtherChannel dijawab dengan tepat dan lengkap sesuai skenario, termasuk verifikasi dan troubleshooting dasar.
Baik	70–84	Sebagian besar soal switching dijawab benar dengan sedikit kesalahan konfigurasi/analisis.
Cukup	55–69	Sebagian soal switching dijawab benar, namun terdapat kesalahan mendasar pada konsep VLAN/trunking.
Kurang	< 55	Sebagian besar jawaban terkait switching tidak tepat atau tidak dikerjakan.

Ketepatan Konfigurasi Routing OSPF, Redundansi Gateway, dan Analisis WAN (Sub-CPMK 2.3–2.4, 3.1) (Bobot: 11%)

Kategori	Skor	Indikator
Sangat Baik	85–100	Soal OSPF multi-area, redundansi gateway (FHRP), dan analisis pemilihan teknologi WAN dijawab dengan tepat, sistematis, dan disertai justifikasi teknis yang kuat.
Baik	70–84	Sebagian besar soal dijawab benar dengan sedikit kesalahan konsep atau konfigurasi.
Cukup	55–69	Sebagian soal dijawab benar, pemahaman dasar terlihat namun belum mampu mengintegrasikan konsep secara menyeluruh.
Kurang	< 55	Sebagian besar jawaban tidak tepat atau soal konfigurasi/analisis tidak terselesaikan.

BAB 9
VPN SITE-TO-SITE DAN REMOTE ACCESS

A. PENDAHULUAN

1. Deskripsi Singkat

Bab ini membahas Virtual Private Network (VPN), teknologi yang memungkinkan organisasi membangun konektivitas yang aman melintasi jaringan publik, termasuk internet/broadband yang telah dibahas pada Bab 7. VPN menjadi solusi penting ketika organisasi ingin memanfaatkan biaya broadband yang jauh lebih rendah dibandingkan MPLS atau leased line, tanpa mengorbankan keamanan data yang dikirimkan antar-lokasi. Pembahasan diawali dengan konsep dasar VPN dan jenisnya, dilanjutkan dengan parameter enkripsi dan autentikasi pada protokol IPsec, konfigurasi VPN site-to-site untuk menghubungkan antar-kantor, serta konsep VPN remote access bagi pengguna individual yang bekerja dari jarak jauh.

Materi pada bab ini merupakan kelanjutan langsung dari Bab 7, yang telah membahas berbagai teknologi WAN termasuk broadband sebagai opsi konektivitas berbiaya rendah namun memerlukan pengamanan tambahan. VPN pada bab ini menjadi jawaban atas kebutuhan tersebut, sekaligus menjadi bekal penting sebelum mahasiswa mempelajari SD-WAN pada Bab 10, yang banyak memanfaatkan VPN sebagai salah satu komponen pembentuk jaringan overlay-nya.

2. Capaian Pembelajaran Mata Kuliah (CPMK) yang Dicapai

Kode CPMK	:	CPMK-3
Rumusan CPMK	:	Mampu menerapkan teknologi WAN dan konektivitas enterprise (WAN tradisional, VPN, SD-WAN, dan konektivitas cloud) sesuai kebutuhan organisasi multi-lokasi.
Bobot CPMK	:	21% dari keseluruhan capaian mata kuliah
CPL yang Didukung	:	CPL-5 (kemampuan merancang, menginstalasi, mengonfigurasi, dan memelihara jaringan komputer) dan CPL-8 (penerapan prinsip keamanan siber dasar dan tata kelola teknologi informasi)

3. Sub-CPMK yang Dicapai

Kode Sub-CPMK	:	Sub-CPMK 3.2
Rumusan Sub-CPMK	:	Mampu mengonfigurasi VPN site-to-site dan remote access untuk konektivitas aman antar-lokasi.

Pertemuan	:	Pertemuan ke-9
Indikator Penilaian	:	Konektivitas VPN berhasil sesuai skenario keamanan (dinilai melalui tugas praktik), bobot 3% dari total penilaian mata kuliah.

4. Tujuan Pembelajaran Khusus (TPK)

Setelah mempelajari bab ini secara tuntas, mahasiswa diharapkan mampu:

1. Menjelaskan konsep VPN serta manfaatnya dalam membangun konektivitas aman melalui jaringan publik.

2. Menjelaskan parameter enkripsi dan autentikasi yang digunakan dalam protokol IPsec, termasuk proses IKE Phase 1 dan IKE Phase 2.

3. Mengonfigurasi VPN site-to-site menggunakan IPsec pada router Cisco IOS untuk menghubungkan dua lokasi secara aman.

4. Menjelaskan konsep dan skenario penerapan VPN remote access bagi pengguna mobile/jarak jauh, serta perbedaannya dengan VPN site-to-site.

5. Menguji dan memverifikasi keberhasilan konektivitas VPN sesuai skenario keamanan yang telah ditentukan.

5. Peta Konsep

Alur pembahasan materi pada Bab 9 disajikan dalam peta konsep berikut, yang menggambarkan keterkaitan logis antar-subbab menuju pencapaian Sub-CPMK 3.2.

Konsep VPN → **Parameter Enkripsi & Autentikasi** → **Konfigurasi VPN Site-to-Site** → **VPN Remote Access**

6. Prasyarat

Sebelum mempelajari bab ini, mahasiswa disarankan telah memahami materi Bab 7 mengenai teknologi WAN, khususnya karakteristik broadband, serta memiliki pemahaman dasar mengenai konsep enkripsi dan autentikasi secara umum yang diperoleh pada mata kuliah keamanan jaringan dasar.

B. URAIAN MATERI

9.1 Konsep VPN

a. Penjelasan Konsep/Teori

Virtual Private Network (VPN) adalah teknologi yang membangun koneksi logis yang aman dan terenkripsi antar-dua titik melalui jaringan publik yang tidak terpercaya (untrusted), seperti internet, sehingga seolah-olah kedua titik tersebut terhubung melalui jaringan privat khusus (private network), meskipun secara fisik data tetap melintasi infrastruktur bersama milik pihak lain. VPN bekerja melalui mekanisme tunneling, yaitu proses membungkus (encapsulation) paket data asli ke dalam paket baru yang dilengkapi header tambahan, kemudian mengenkripsi isi paket tersebut agar tidak dapat dibaca oleh pihak yang tidak berwenang meskipun berhasil disadap di tengah jalur pengiriman.

Berdasarkan skenario penggunaannya, VPN pada jaringan enterprise umumnya dibedakan menjadi dua kategori utama.

- VPN Site-to-Site — menghubungkan dua jaringan LAN yang berada pada lokasi berbeda (misalnya kantor pusat dan kantor cabang) secara permanen, di mana tunnel VPN dibentuk antar-perangkat gateway (router/firewall) pada masing-masing lokasi, sehingga seluruh perangkat pada kedua LAN dapat saling berkomunikasi secara transparan tanpa memerlukan konfigurasi VPN pada perangkat pengguna akhir.
- VPN Remote Access — menghubungkan satu perangkat pengguna individual (laptop, smartphone) dari lokasi mana pun menuju jaringan organisasi, umumnya digunakan oleh karyawan yang bekerja dari rumah atau sedang bepergian (mobile worker), di mana tunnel VPN dibentuk langsung dari perangkat pengguna menggunakan aplikasi klien VPN atau melalui portal berbasis web (clientless).

Terdapat beberapa protokol tunneling yang umum digunakan untuk membangun VPN, di antaranya IPsec (Internet Protocol Security) yang bekerja pada Layer 3 dan paling umum digunakan untuk VPN site-to-site karena mampu mengenkripsi seluruh trafik IP secara transparan; SSL/TLS VPN yang bekerja pada Layer 4 ke atas dan umum digunakan untuk VPN remote access karena dapat diakses langsung melalui peramban web tanpa instalasi perangkat lunak tambahan; serta GRE (Generic Routing Encapsulation) yang menyediakan tunneling namun tanpa enkripsi bawaan, sehingga sering dikombinasikan dengan IPsec (GRE over IPsec) apabila diperlukan dukungan routing dinamis dan multicast di dalam tunnel.

b. Contoh Aplikasi

Sebuah perusahaan retail yang memanfaatkan broadband sebagai konektivitas WAN antar-gerai (sebagaimana dibahas pada Bab 7) dapat membangun VPN site-to-site antara setiap gerai dan kantor pusat, sehingga sistem kasir di gerai dapat mengakses server inventori pusat secara aman meskipun melalui jaringan internet publik. Di sisi lain, karyawan bagian penjualan yang sering bepergian ke luar kota dapat menggunakan VPN remote access untuk mengakses email dan sistem CRM perusahaan secara aman dari hotel atau tempat kerja sementara.

9.2 Parameter Enkripsi dan Autentikasi

a. Penjelasan Konsep/Teori

IPsec bukanlah satu protokol tunggal, melainkan kerangka kerja (framework) yang terdiri atas beberapa protokol yang bekerja sama untuk menyediakan kerahasiaan (confidentiality), integritas (integrity), dan autentikasi (authentication) pada trafik data. Proses pembentukan tunnel IPsec berlangsung melalui dua fase negosiasi menggunakan protokol Internet Key Exchange (IKE).

- IKE Phase 1 — membentuk kanal komunikasi yang aman (ISAKMP Security Association) antar-kedua perangkat gateway, meliputi negosiasi metode autentikasi (umumnya pre-shared key atau sertifikat digital), algoritme enkripsi (misalnya AES), algoritme hashing untuk integritas data (misalnya SHA), dan grup Diffie-Hellman untuk pertukaran kunci enkripsi secara aman. Fase ini dapat berjalan pada mode main mode (lebih aman, enam pertukaran pesan) atau aggressive mode (lebih cepat, tiga pertukaran pesan, namun kurang aman).
- IKE Phase 2 — menggunakan kanal aman yang telah terbentuk pada Phase 1 untuk menegosiasikan parameter IPsec Security Association (IPsec SA) yang sesungguhnya akan digunakan untuk mengenkripsi trafik data pengguna, meliputi transform set (kombinasi algoritme enkripsi dan integritas untuk data), mode tunnel (tunnel mode, membungkus seluruh paket IP asli) atau transport mode (hanya membungkus payload, umum digunakan untuk komunikasi host-to-host), serta lifetime (durasi sebelum SA harus dinegosiasikan ulang).

Terdapat dua protokol keamanan utama dalam IPsec, yaitu Authentication Header (AH) yang hanya menyediakan autentikasi dan integritas tanpa enkripsi (sehingga jarang digunakan pada implementasi modern), dan Encapsulating Security Payload (ESP) yang menyediakan autentikasi, integritas, sekaligus enkripsi data, sehingga menjadi protokol yang paling umum digunakan pada implementasi VPN site-to-site saat ini.

Konfigurasi parameter IKE Phase 1 dan Phase 2 pada Cisco IOS dicontohkan pada perintah berikut.

```
! IKE Phase 1 (ISAKMP Policy)
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# hash sha256
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 14
R1(config-isakmp)# exit
R1(config)# crypto isakmp key VpnKuat2026! address 198.51.100.1

! IKE Phase 2 (Transform Set)
R1(config)# crypto ipsec transform-set TS-KANTOR esp-aes 256 esp-sha256-hmac
R1(config)# mode tunnel
```

Contoh 9.1 Perintah konfigurasi parameter IKE Phase 1 dan transform set IKE Phase 2 pada Cisco IOS

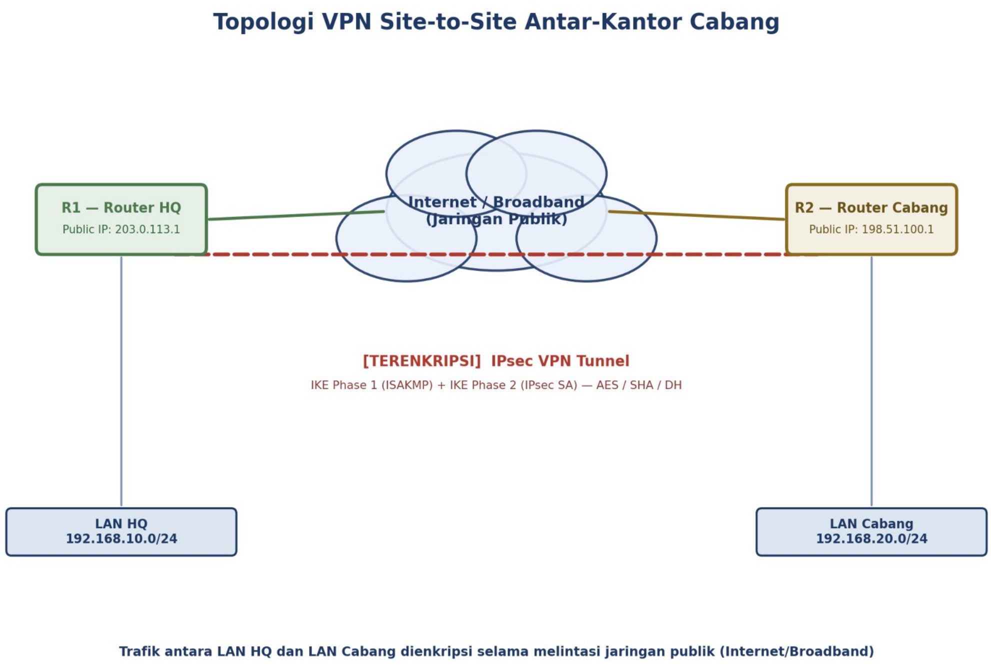
b. Contoh Aplikasi

Pemilihan parameter enkripsi dan hashing yang lebih kuat (misalnya AES-256 dan SHA-256 dibandingkan DES atau MD5 yang sudah usang) menjadi pertimbangan penting terutama bagi organisasi yang menangani data sensitif, seperti data nasabah pada institusi keuangan, guna memenuhi standar keamanan siber dan regulasi perlindungan data yang berlaku.

9.3 Konfigurasi VPN Site-to-Site

a. Penjelasan Konsep/Teori

Setelah parameter IKE Phase 1 dan Phase 2 dikonfigurasi, tahap selanjutnya adalah mendefinisikan trafik yang akan dienkripsi (disebut interesting traffic) menggunakan access control list (ACL), kemudian mengikat seluruh parameter tersebut ke dalam sebuah crypto map yang diterapkan pada interface publik router. Mengacu pada topologi Gambar 9.1, berikut adalah contoh konfigurasi lengkap VPN site-to-site pada router R1 (kantor pusat), yang melanjutkan konfigurasi IKE pada Contoh 9.1.



Gambar 9.1 Topologi VPN Site-to-Site Antar-Kantor Cabang

Diagram di atas menggambarkan Router R1 (kantor pusat) dan Router R2 (kantor cabang) yang masing-masing terhubung ke internet/broadband melalui alamat IP publik. Tunnel IPsec VPN dibentuk antara kedua router melalui jaringan publik tersebut, melindungi trafik yang mengalir antara LAN HQ (192.168.10.0/24) dan LAN Cabang (192.168.20.0/24). Seluruh trafik yang melintasi tunnel dienkripsi menggunakan parameter yang dinegosiasikan melalui IKE Phase 1 dan IKE Phase 2, sehingga data tetap aman meskipun melintasi jaringan internet yang bersifat publik.

```
! Mendefinisikan interesting traffic (LAN HQ <-> LAN Cabang)
R1(config)# access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.20.0
0.0.0.255

! Membuat crypto map
R1(config)# crypto map CMAP-CABANG 10 ipsec-isakmp
R1(config-crypto-map)# set peer 198.51.100.1
R1(config-crypto-map)# set transform-set TS-KANTOR
R1(config-crypto-map)# match address 100
R1(config-crypto-map)# exit

! Menerapkan crypto map pada interface publik
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# crypto map CMAP-CABANG
R1(config-if)# end
R1# show crypto isakmp sa
R1# show crypto ipsec sa
```

Contoh 9.2 Perintah konfigurasi lengkap VPN site-to-site (ACL, crypto map, penerapan pada interface)

Konfigurasi pada router R2 (kantor cabang) bersifat cerminan (mirror) dari konfigurasi R1, dengan parameter set peer diarahkan ke alamat IP publik R1 dan ACL yang membalik urutan subnet sumber dan tujuan. Tunnel VPN akan terbentuk secara otomatis (on-demand) ketika terdapat trafik yang sesuai dengan interesting traffic yang telah didefinisikan pada ACL.

Verifikasi keberhasilan tunnel dilakukan menggunakan perintah show crypto isakmp sa (menampilkan status Security Association Phase 1, idealnya berstatus QM_IDLE) dan show crypto ipsec sa (menampilkan statistik paket yang telah dienkripsi/didekripsi pada Phase 2).

b. Contoh Aplikasi

Konfigurasi VPN site-to-site semacam ini banyak diterapkan pada organisasi dengan jumlah cabang terbatas (puluhan lokasi), karena setiap pasangan lokasi memerlukan konfigurasi crypto map tersendiri; untuk organisasi dengan ratusan cabang, pendekatan yang lebih skalabel seperti DMVPN (Dynamic Multipoint VPN) atau SD-WAN (dibahas pada Bab 10) umumnya lebih dipilih.

9.4 VPN Remote Access

a. Penjelasan Konsep/Teori

Berbeda dengan VPN site-to-site yang menghubungkan dua jaringan secara permanen, VPN remote access dirancang untuk menghubungkan satu perangkat pengguna individual ke jaringan organisasi secara sementara (on-demand), sesuai kebutuhan pengguna tersebut untuk mengakses sumber daya internal. Terdapat dua pendekatan umum dalam implementasi VPN remote access.

- Client-Based VPN — pengguna menginstal aplikasi klien VPN khusus (misalnya Cisco AnyConnect Secure Mobility Client) pada perangkatnya, yang akan membentuk tunnel terenkripsi (umumnya berbasis SSL/TLS atau IPsec) menuju gateway VPN organisasi setiap kali pengguna melakukan autentikasi.
- Clientless VPN (SSL VPN Portal) — pengguna mengakses sumber daya organisasi langsung melalui peramban web tanpa perlu menginstal aplikasi tambahan, umumnya terbatas pada akses ke aplikasi web internal tertentu, cocok untuk skenario akses cepat dari perangkat yang tidak dikelola organisasi (unmanaged device).

Perbandingan karakteristik utama antara VPN site-to-site dan VPN remote access dirangkum pada Tabel 9.1 berikut.

Aspek	VPN Site-to-Site	VPN Remote Access
Pihak yang Terhubung	Dua jaringan LAN (gateway-to-gateway)	Satu perangkat pengguna individual ke jaringan organisasi
Sifat Koneksi	Permanen, selalu aktif (always-on)	Sementara, sesuai kebutuhan pengguna (on-demand)

Aspek	VPN Site-to-Site	VPN Remote Access
Konfigurasi pada Pengguna Akhir	Tidak diperlukan (transparan)	Diperlukan aplikasi klien atau akses portal web
Protokol Umum	IPsec (site-to-site)	SSL/TLS VPN atau IPsec remote access
Contoh Skenario	Kantor pusat menghubungkan kantor cabang	Karyawan bekerja dari rumah/perjalanan dinas

Tabel 9.1 Perbandingan VPN Site-to-Site dan VPN Remote Access

Implementasi VPN remote access pada perangkat Cisco umumnya memanfaatkan fitur SSL VPN (WebVPN) yang dikonfigurasi melalui group policy dan connection profile pada perangkat konsentrator VPN (seperti Cisco ASA) atau router yang mendukung fitur tersebut. Konfigurasi rinci VPN remote access memerlukan perangkat dan lisensi khusus yang berada di luar cakupan konfigurasi dasar pada mata kuliah ini, sehingga mahasiswa cukup memahami konsep dan skenario penerapannya.

b. Contoh Aplikasi

Selama masa kerja jarak jauh (remote working), banyak organisasi mengandalkan VPN remote access agar karyawan tetap dapat mengakses sistem informasi internal, server file, dan aplikasi bisnis secara aman dari rumah masing-masing, tanpa mengekspos sumber daya tersebut secara langsung ke internet publik.

C. RANGKUMAN

- VPN membangun koneksi logis yang aman dan terenkripsi melalui jaringan publik menggunakan mekanisme tunneling, terdiri atas dua kategori utama: VPN site-to-site (LAN-to-LAN, permanen) dan VPN remote access (individual, on-demand).
- IPsec bekerja melalui dua fase negosiasi: IKE Phase 1 (membentuk kanal aman ISAKMP, negosiasi autentikasi dan enkripsi) dan IKE Phase 2 (menegosiasikan IPsec SA untuk data pengguna menggunakan transform set).
- ESP (Encapsulating Security Payload) menyediakan autentikasi, integritas, dan enkripsi sekaligus, menjadikannya protokol keamanan IPsec yang paling umum digunakan dibandingkan AH.
- Konfigurasi VPN site-to-site pada Cisco IOS melibatkan ACL (interesting traffic), crypto map (mengikat peer, transform set, dan ACL), dan penerapan crypto map pada interface publik, diverifikasi menggunakan show crypto isakmp sa dan show crypto ipsec sa.
- VPN remote access menghubungkan perangkat individual ke jaringan organisasi melalui client-based VPN atau clientless SSL VPN portal, cocok untuk skenario kerja jarak jauh atau mobile.

D. LATIHAN/SOAL

Petunjuk pengerjaan: Kerjakan seluruh soal berikut secara mandiri. Soal nomor 1–5 merupakan soal pemahaman konsep (jawaban singkat/uraian), soal nomor 6–8 merupakan soal konfigurasi, dan soal nomor 9–10 merupakan soal analisis/troubleshooting. Seluruh soal mengacu pada capaian Sub-CPMK 3.2.

1. Jelaskan definisi VPN dan mekanisme tunneling yang mendasarinya.

2. Jelaskan perbedaan utama antara VPN site-to-site dan VPN remote access.

3. Jelaskan tujuan IKE Phase 1 dan IKE Phase 2 dalam proses pembentukan tunnel IPsec.

4. Jelaskan perbedaan antara protokol AH dan ESP pada IPsec, dan mengapa ESP lebih umum digunakan.

5. Jelaskan perbedaan antara client-based VPN dan clientless VPN pada skenario remote access.

6. Tuliskan perintah Cisco IOS untuk mengonfigurasi ISAKMP policy dengan enkripsi AES 256, hash SHA256, autentikasi pre-shared key, dan Diffie-Hellman group 14.

7. Tuliskan perintah Cisco IOS untuk membuat access-list yang mendefinisikan interesting traffic antara subnet 10.10.10.0/24 dan 10.10.20.0/24.

8. Tuliskan perintah Cisco IOS untuk membuat crypto map bernama CMAP-HQ yang mengarah ke peer 203.0.113.5, menggunakan transform set TS-VPN, dan menerapkannya pada interface GigabitEthernet 0/0.

9. Pada saat verifikasi menggunakan show crypto isakmp sa, status SA menunjukkan MM_NO_STATE dan tidak pernah mencapai QM_IDLE. Analisislah kemungkinan penyebab masalah tersebut.

10. Sebuah organisasi memiliki 30 kantor cabang dan berencana menghubungkan seluruhnya menggunakan VPN site-to-site konvensional (crypto map per pasangan lokasi). Analisislah tantangan skalabilitas yang akan dihadapi dan usulkan pendekatan alternatif yang lebih sesuai.

E. DAFTAR PUSTAKA

Stallings, W. (2023). Network security essentials: Applications and standards (7th ed.). Pearson.

Cisco Networking Academy. (2022). CCNP Enterprise: Core networking technologies (ENCOR) companion guide. Cisco Press.

Marschke, D., Doraswamy, N., & Ghosh, A. (2021). SD-WAN: A comprehensive approach for enterprise networking. Packt Publishing.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 2 (2nd ed.). Cisco Press.

Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson.

F. TUGAS/STUDI KASUS

Tugas Praktik: Konfigurasi VPN Site-to-Site

Menggunakan simulator jaringan (Cisco Packet Tracer atau GNS3), bangunlah topologi yang terdiri atas dua router (R1 dan R2) yang masing-masing terhubung ke jaringan "internet" simulasi dan melayani satu LAN lokal, mengacu pada skema topologi Gambar 9.1, dengan ketentuan sebagai berikut.

1. Konfigurasikan IKE Phase 1 pada kedua router dengan parameter enkripsi AES 256, hash SHA256, autentikasi pre-shared key, dan Diffie-Hellman group 14.

2. Konfigurasikan IKE Phase 2 (transform set) menggunakan esp-aes 256 dan esp-sha256-hmac, dengan mode tunnel.

3. Definisikan interesting traffic menggunakan access-list yang sesuai dengan subnet LAN pada kedua lokasi, lalu buat dan terapkan crypto map pada interface publik masing-masing router.

4. Konfigurasikan minimal satu PC pada masing-masing LAN, lalu uji konektivitas antar-PC pada kedua lokasi melalui tunnel VPN.

5. Lakukan verifikasi menggunakan show crypto isakmp sa dan show crypto ipsec sa pada kedua router, lalu sertakan hasil tangkapan layar (screenshot) beserta analisis singkat mengenai skenario keamanan yang diterapkan pada laporan.

Laporan praktik (mencakup topologi, seluruh perintah konfigurasi, dan hasil verifikasi) dikumpulkan dalam bentuk dokumen (PDF/Word) disertai file simulasi (.pkt/.gns3) sesuai tenggat waktu yang ditentukan dosen pengampu. Tugas ini dinilai menggunakan rubrik pada Rubrik Penilaian per Pertemuan 9 (aspek Tugas Praktik: Konfigurasi VPN Site-to-Site dan Partisipasi Diskusi: Diskusi Konektivitas Aman Antar-Lokasi) sebagaimana tercantum pada Lampiran buku ajar ini.

BAB 10
SD-WAN DAN KONEKTIVITAS CLOUD

A. PENDAHULUAN

1. Deskripsi Singkat

Bab ini membahas Software-Defined WAN (SD-WAN), pendekatan modern dalam mengelola konektivitas WAN yang mengabstraksikan kebijakan routing dari perangkat keras transport yang mendasarinya, serta konektivitas cloud sebagai kebutuhan yang semakin penting pada jaringan enterprise masa kini. SD-WAN merupakan evolusi lebih lanjut dari konsep hybrid WAN yang telah diperkenalkan pada Bab 7 dan memanfaatkan tunnel VPN yang telah dibahas pada Bab 9 sebagai salah satu komponen pembentuk jaringan overlay-nya. Pembahasan diawali dengan konsep dan arsitektur SD-WAN, dilanjutkan dengan analisis manfaat dan tantangan penerapannya, serta ditutup dengan konsep konektivitas cloud pada jaringan enterprise modern.

Bab ini bersifat konseptual dan analitis, sejalan dengan metode pembelajaran ceramah, diskusi, dan studi kasus industri sebagaimana ditetapkan pada RPS untuk Pertemuan ke-10. Materi pada bab ini menjadi penutup topik CPMK-3 mengenai teknologi WAN dan konektivitas enterprise, sekaligus menjadi jembatan konseptual menuju topik keamanan jaringan (ACL, firewall, monitoring) yang akan dibahas pada Bab 11 hingga Bab 13.

2. Capaian Pembelajaran Mata Kuliah (CPMK) yang Dicapai

Kode CPMK	:	CPMK-3
Rumusan CPMK	:	Mampu menerapkan teknologi WAN dan konektivitas enterprise (WAN tradisional, VPN, SD-WAN, dan konektivitas cloud) sesuai kebutuhan organisasi multi-lokasi.
Bobot CPMK	:	21% dari keseluruhan capaian mata kuliah
CPL yang Didukung	:	CPL-5 (kemampuan merancang, menginstalasi, mengonfigurasi, dan memelihara jaringan komputer) dan CPL-10 (pengembangan diri berkelanjutan mengikuti perkembangan teknologi jaringan)

3. Sub-CPMK yang Dicapai

Kode Sub-CPMK	:	Sub-CPMK 3.3
Rumusan Sub-CPMK	:	Mampu menjelaskan konsep SD-WAN dan konektivitas cloud pada jaringan enterprise modern.
Pertemuan	:	Pertemuan ke-10

Indikator Penilaian : Ketepatan analisis manfaat dan tantangan penerapan SD-WAN (dinilai melalui tugas analisis), bobot 3% dari total penilaian mata kuliah.

4. Tujuan Pembelajaran Khusus (TPK)

Setelah mempelajari bab ini secara tuntas, mahasiswa diharapkan mampu:

1. Menjelaskan konsep dan arsitektur SD-WAN, termasuk komponen utama seperti orchestrator, edge device, underlay, dan overlay.

2. Membandingkan pendekatan SD-WAN dengan WAN tradisional dari aspek biaya, kelincahan (agility), dan pengelolaan.

3. Menganalisis manfaat dan tantangan penerapan SD-WAN pada organisasi multi-lokasi.

4. Menjelaskan konsep konektivitas cloud dan opsi-opsi yang tersedia bagi jaringan enterprise untuk terhubung ke penyedia layanan cloud publik.

5. Menganalisis studi kasus penerapan SD-WAN dan konektivitas cloud pada organisasi multi-lokasi, disertai rekomendasi yang tepat.

5. Peta Konsep

Alur pembahasan materi pada Bab 10 disajikan dalam peta konsep berikut, yang menggambarkan keterkaitan logis antar-subbab menuju pencapaian Sub-CPMK 3.3.

Konsep & Arsitektur SD-WAN → **Manfaat & Tantangan Penerapan** → **Konektivitas Cloud**

6. Prasyarat

Sebelum mempelajari bab ini, mahasiswa disarankan telah memahami materi Bab 7 mengenai teknologi WAN dan pendekatan hybrid WAN, serta Bab 9 mengenai konsep VPN, karena SD-WAN banyak memanfaatkan tunnel VPN sebagai komponen pembentuk jaringan overlay-nya.

B. URAIAN MATERI

10.1 Konsep dan Arsitektur SD-WAN

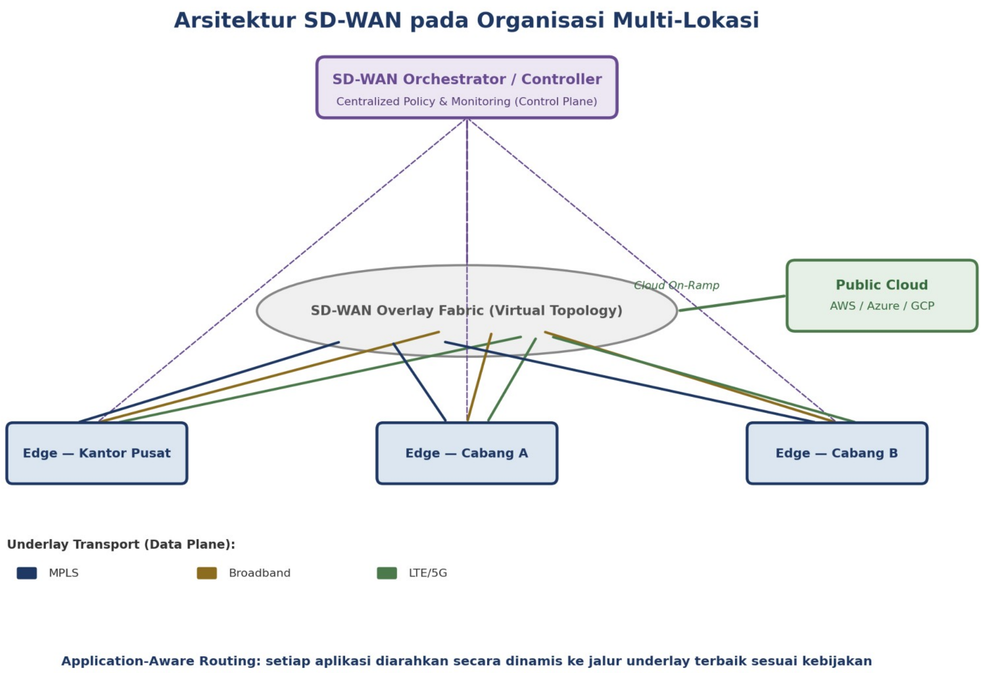
a. Penjelasan Konsep/Teori

Software-Defined WAN (SD-WAN) adalah pendekatan pengelolaan jaringan WAN yang memisahkan (decouple) control plane (pengambilan keputusan routing dan kebijakan) dari data plane (perangkat keras yang meneruskan trafik), sehingga seluruh kebijakan jaringan dapat dikelola secara terpusat dan diterapkan secara otomatis ke seluruh lokasi, terlepas dari jenis media transport fisik yang digunakan pada masing-masing lokasi tersebut. Berbeda dengan pendekatan WAN tradisional yang mengandalkan konfigurasi manual per perangkat dan routing berbasis topologi fisik semata, SD-WAN memungkinkan trafik diarahkan secara dinamis berdasarkan kebijakan aplikasi (application-aware routing), tanpa bergantung pada satu jenis koneksi WAN tertentu.

Arsitektur SD-WAN terdiri atas empat komponen utama.

- Orchestrator/Controller — sistem manajemen terpusat yang menyimpan seluruh kebijakan (policy), memantau kondisi jaringan secara real-time, dan mendistribusikan konfigurasi ke seluruh edge device secara otomatis (zero-touch provisioning), sehingga administrator tidak perlu mengonfigurasi setiap perangkat secara manual satu per satu.
- Edge Device — perangkat SD-WAN yang dipasang pada setiap lokasi (kantor pusat maupun cabang), bertugas membentuk tunnel overlay menuju edge device lain serta menerapkan kebijakan routing yang diterima dari orchestrator.
- Underlay Transport — media transport fisik yang menghubungkan setiap lokasi ke jaringan luar, dapat berupa kombinasi lebih dari satu jenis (MPLS, broadband, bahkan LTE/5G) secara bersamaan pada satu lokasi yang sama.
- Overlay Network — jaringan virtual yang dibentuk di atas underlay transport menggunakan tunnel terenkripsi (umumnya berbasis IPsec, sebagaimana dibahas pada Bab 9), membentuk topologi logis yang independen dari topologi fisik underlay yang sesungguhnya.

Kemampuan kunci yang membedakan SD-WAN dari WAN tradisional adalah application-aware routing (dynamic path selection), yaitu kemampuan untuk memantau kualitas setiap jalur underlay secara real-time (latensi, jitter, packet loss) dan secara otomatis mengarahkan trafik aplikasi tertentu ke jalur yang paling sesuai dengan kebutuhannya — misalnya trafik VoIP diarahkan ke jalur dengan latensi terendah, sementara trafik pencadangan data (backup) berukuran besar diarahkan ke jalur berbiaya rendah.



Gambar 10.1 Arsitektur SD-WAN pada Organisasi Multi-Lokasi

Diagram di atas menggambarkan SD-WAN Orchestrator yang mengelola kebijakan secara terpusat (control plane, garis putus-putus) menuju edge device pada tiga lokasi (Kantor Pusat, Cabang A, dan Cabang B). Setiap edge device terhubung ke SD-WAN Overlay Fabric melalui kombinasi tiga jenis underlay transport (MPLS, broadband, dan LTE/5G) secara bersamaan. Selain menghubungkan antar-lokasi, fabric SD-WAN juga menyediakan cloud on-ramp yang menghubungkan langsung ke penyedia layanan cloud publik (AWS/Azure/GCP), sehingga aplikasi berbasis cloud dapat diakses tanpa harus melalui kantor pusat terlebih dahulu.

b. Contoh Aplikasi

Sebuah perusahaan ritel dengan seratus gerai dapat memanfaatkan SD-WAN untuk menyederhanakan penambahan gerai baru: cukup memasang edge device di lokasi baru dan menghubungkannya ke internet, seluruh kebijakan jaringan (VLAN, keamanan, prioritas trafik) akan diterapkan secara otomatis oleh orchestrator tanpa memerlukan kunjungan teknisi jaringan senior ke lokasi tersebut.

10.2 Manfaat dan Tantangan Penerapan

a. Penjelasan Konsep/Teori

Penerapan SD-WAN pada jaringan enterprise memberikan sejumlah manfaat signifikan, sekaligus turut membawa beberapa tantangan yang perlu dipertimbangkan secara matang sebelum organisasi memutuskan untuk bermigrasi.

- Efisiensi Biaya — organisasi dapat mengurangi ketergantungan pada MPLS yang mahal dengan memanfaatkan kombinasi broadband berbiaya rendah, tanpa mengorbankan keandalan berkat kemampuan dynamic path selection dan failover otomatis antar-underlay.

- Penyederhanaan Manajemen — konfigurasi terpusat melalui orchestrator secara signifikan mengurangi kompleksitas dan waktu yang dibutuhkan untuk mengelola jaringan berskala besar dengan banyak lokasi.
- Peningkatan Performa Aplikasi — application-aware routing memastikan aplikasi kritis mendapatkan jalur dengan kualitas terbaik yang tersedia pada waktu tertentu, meningkatkan pengalaman pengguna.
- Kelincahan (Agility) — penambahan lokasi baru menjadi jauh lebih cepat dibandingkan menunggu proses pengadaan sirkuit MPLS yang dapat memakan waktu berminggu-minggu hingga berbulan-bulan.
- Ketergantungan pada Kualitas Internet — apabila organisasi mengurangi porsi MPLS secara signifikan, keandalan jaringan menjadi lebih bergantung pada kualitas layanan internet/broadband di setiap lokasi, yang dapat bervariasi antar-wilayah.
- Kompleksitas Migrasi — transisi dari infrastruktur WAN tradisional menuju SD-WAN memerlukan perencanaan matang, termasuk periode migrasi bertahap agar tidak mengganggu operasional bisnis yang sedang berjalan.
- Ketergantungan pada Vendor (Vendor Lock-In) — sebagian besar solusi SD-WAN bersifat proprietary, sehingga organisasi perlu mempertimbangkan risiko ketergantungan jangka panjang terhadap satu vendor tertentu.
- Kesenjangan Kompetensi — tim jaringan internal perlu mendapatkan pelatihan tambahan untuk mengelola platform SD-WAN yang baru, karena paradigma pengelolaannya berbeda dari perangkat WAN tradisional.

Perbandingan karakteristik SD-WAN dan WAN tradisional dirangkum pada Tabel 10.1 berikut.

Aspek	WAN Tradisional	SD-WAN
Pengelolaan	Konfigurasi manual per perangkat	Terpusat melalui orchestrator (zero-touch provisioning)
Pemanfaatan Jalur	Umumnya satu jalur utama, jalur cadangan idle (active/backup)	Seluruh jalur underlay dapat dimanfaatkan bersamaan (active/active)
Pemilihan Jalur	Statis, berdasarkan konfigurasi routing tetap	Dinamis, berdasarkan kualitas real-time dan kebijakan aplikasi
Kecepatan Penambahan Lokasi	Lambat (bergantung proses pengadaan sirkuit)	Cepat (edge device + koneksi internet yang tersedia)
Biaya	Tinggi, terutama dengan MPLS sebagai tulang punggung	Lebih rendah, memanfaatkan broadband sebagai bagian dari underlay

Tabel 10.1 Perbandingan SD-WAN dan WAN Tradisional

b. Contoh Aplikasi

Sebuah perusahaan multinasional yang bermigrasi dari WAN berbasis MPLS penuh menuju SD-WAN dapat mempertahankan MPLS sebagai salah satu underlay untuk trafik kritis, sambil menambahkan broadband sebagai underlay tambahan untuk trafik non-kritis, sehingga migrasi dapat dilakukan secara bertahap tanpa risiko gangguan besar pada operasional bisnis.

10.3 Konektivitas Cloud

a. Penjelasan Konsep/Teori

Seiring semakin banyaknya organisasi yang memindahkan aplikasi dan infrastrukturnya ke penyedia layanan cloud publik (seperti AWS, Microsoft Azure, atau Google Cloud Platform), desain jaringan enterprise modern perlu mempertimbangkan bagaimana lokasi-lokasi organisasi dapat mengakses layanan cloud tersebut secara optimal, tidak hanya mengandalkan akses internet biasa. Terdapat dua pendekatan utama dalam membangun konektivitas cloud.

- Akses Berbasis Internet — cara paling sederhana, di mana pengguna mengakses layanan cloud melalui koneksi internet publik biasa (dapat dipadukan dengan VPN untuk keamanan tambahan). Pendekatan ini mudah diterapkan namun performanya bergantung pada kualitas internet publik yang tidak dapat dijamin (best-effort).
- Direct Cloud Connect — koneksi privat khusus (dedicated) antara jaringan organisasi dan penyedia layanan cloud, tanpa melalui internet publik, seperti AWS Direct Connect, Azure ExpressRoute, atau Google Cloud Interconnect. Pendekatan ini menawarkan latensi yang lebih rendah, bandwidth yang lebih konsisten, dan keandalan yang lebih tinggi, namun dengan biaya tambahan dan umumnya memerlukan titik interkoneksi fisik (colocation) di penyedia layanan tertentu.

Solusi SD-WAN modern umumnya turut menyediakan fitur cloud on-ramp, yaitu titik interkoneksi optimal antara fabric SD-WAN dan penyedia layanan cloud besar (sebagaimana ditunjukkan pada Gambar 10.1), memungkinkan trafik dari cabang mana pun diarahkan langsung ke cloud tanpa harus melalui kantor pusat terlebih dahulu (menghindari pendekatan backhaul yang tidak efisien). Hal ini juga relevan dengan tren pemanfaatan aplikasi Software as a Service (SaaS) seperti email dan produktivitas berbasis cloud (misalnya Microsoft 365 atau Google Workspace), yang idealnya diakses melalui local internet breakout di setiap lokasi cabang, bukan diarahkan kembali (backhaul) ke kantor pusat yang justru akan menambah latensi tanpa manfaat keamanan yang signifikan.

b. Contoh Aplikasi

Sebuah perusahaan yang menjalankan sebagian besar sistem enterprise resource planning (ERP) pada infrastruktur cloud publik dapat memanfaatkan Direct Cloud Connect dari kantor pusat untuk menjamin performa aplikasi kritis tersebut, sementara kantor-kantor cabang cukup memanfaatkan local internet breakout melalui SD-WAN untuk mengakses aplikasi SaaS sehari-hari seperti email dan konferensi video.

C. RANGKUMAN

- SD-WAN memisahkan control plane (kebijakan, dikelola terpusat oleh orchestrator) dari data plane (edge device dan underlay transport), memungkinkan pengelolaan WAN yang lebih sederhana dan fleksibel.
- Arsitektur SD-WAN terdiri atas orchestrator/controller, edge device, underlay transport (dapat berupa kombinasi MPLS, broadband, LTE/5G), dan overlay network berbasis tunnel terenkripsi.
- Application-aware routing memungkinkan SD-WAN mengarahkan trafik aplikasi secara dinamis ke jalur underlay terbaik berdasarkan kondisi real-time, berbeda dari WAN tradisional yang statis.
- Manfaat SD-WAN meliputi efisiensi biaya, penyederhanaan manajemen, peningkatan performa aplikasi, dan kelincahan; tantangannya meliputi ketergantungan pada kualitas internet, kompleksitas migrasi, vendor lock-in, dan kesenjangan kompetensi tim jaringan.
- Konektivitas cloud dapat dibangun melalui akses berbasis internet (sederhana, best-effort) atau Direct Cloud Connect (dedicated, lebih andal namun berbiaya lebih tinggi), dengan SD-WAN modern umumnya menyediakan fitur cloud on-ramp untuk optimalisasi akses cloud dari seluruh lokasi cabang.

D. LATIHAN/SOAL

Petunjuk pengerjaan: Kerjakan seluruh soal berikut secara mandiri. Soal nomor 1–6 merupakan soal pemahaman konsep (jawaban singkat/uraian), sedangkan soal nomor 7–10 merupakan soal analisis yang memerlukan penjelasan disertai justifikasi teknis dan bisnis. Seluruh soal mengacu pada capaian Sub-CPMK 3.3.

1. Jelaskan konsep pemisahan control plane dan data plane pada arsitektur SD-WAN.

2. Sebutkan dan jelaskan empat komponen utama arsitektur SD-WAN.

3. Jelaskan konsep application-aware routing dan bagaimana kemampuan ini membedakan SD-WAN dari WAN tradisional.

4. Jelaskan minimal tiga manfaat utama penerapan SD-WAN bagi organisasi multi-lokasi.

5. Jelaskan minimal tiga tantangan yang perlu dipertimbangkan sebelum organisasi bermigrasi ke SD-WAN.

6. Jelaskan perbedaan antara akses cloud berbasis internet biasa dan Direct Cloud Connect.

7. Sebuah organisasi dengan lima puluh cabang saat ini menggunakan MPLS penuh sebagai WAN utama dengan biaya operasional yang sangat tinggi. Analisislah manfaat dan tantangan yang akan dihadapi organisasi tersebut apabila bermigrasi ke SD-WAN.

8. Berdasarkan Tabel 10.1, jelaskan mengapa SD-WAN mampu memanfaatkan seluruh jalur underlay secara bersamaan (active/active), sedangkan WAN tradisional umumnya hanya memanfaatkan satu jalur utama.

9. Sebuah perusahaan sedang mempertimbangkan apakah aplikasi SaaS (seperti email berbasis cloud) sebaiknya diakses melalui backhaul ke kantor pusat atau melalui local internet breakout di setiap cabang. Analisislah pendekatan mana yang lebih tepat beserta alasannya.

10. Sebuah perusahaan manufaktur menjalankan sistem ERP kritis pada cloud publik dan memiliki dua puluh cabang dengan kebutuhan akses yang lebih sederhana. Rancanglah rekomendasi arsitektur konektivitas cloud (kombinasi Direct Cloud Connect dan/atau SD-WAN dengan local internet breakout) untuk perusahaan tersebut, disertai justifikasi.

E. DAFTAR PUSTAKA

Marschke, D., Doraswamy, N., & Ghosh, A. (2021). SD-WAN: A comprehensive approach for enterprise networking. Packt Publishing.

Cisco Networking Academy. (2022). CCNP Enterprise: Core networking technologies (ENCOR) companion guide. Cisco Press.

Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson.

Stallings, W. (2023). Network security essentials: Applications and standards (7th ed.). Pearson.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 2 (2nd ed.). Cisco Press.

F. TUGAS/STUDI KASUS

Tugas Analisis: Studi Kasus Penerapan SD-WAN

Perhatikan studi kasus berikut.

Studi Kasus: PT Andalan Mitra Sejahtera

PT Andalan Mitra Sejahtera adalah perusahaan distribusi consumer goods dengan satu kantor pusat di Jakarta dan 25 kantor cabang yang tersebar di berbagai provinsi. Saat ini, seluruh cabang terhubung ke kantor pusat menggunakan MPLS, dengan biaya sirkuit yang terus meningkat setiap tahun. Perusahaan baru saja memindahkan sistem ERP dan aplikasi CRM-nya ke penyedia layanan cloud publik, namun pengguna di cabang mengeluhkan performa aplikasi tersebut lambat karena seluruh trafik cabang saat ini masih dialihkan (backhaul) melalui kantor pusat sebelum menuju internet.

Susunlah laporan analisis individu (2–3 halaman) yang memuat:

1. Analisis manfaat yang akan diperoleh PT Andalan Mitra Sejahtera apabila bermigrasi dari MPLS penuh menuju pendekatan SD-WAN.

2. Analisis tantangan dan risiko yang perlu diantisipasi selama proses migrasi tersebut.

3. Rekomendasi arsitektur konektivitas cloud yang tepat untuk mengatasi keluhan performa aplikasi ERP dan CRM berbasis cloud pada cabang.

4. Rekomendasi strategi migrasi bertahap (tidak langsung menghapus seluruh MPLS) agar risiko gangguan operasional dapat diminimalkan.

Laporan analisis dikumpulkan dalam bentuk dokumen (PDF/Word) sesuai tenggat waktu yang ditentukan dosen pengampu. Tugas ini dinilai menggunakan rubrik pada Rubrik Penilaian per Pertemuan 10 (aspek Tugas Analisis: Studi Kasus Penerapan SD-WAN dan Partisipasi Diskusi: Diskusi Studi Kasus Industri SD-WAN) sebagaimana tercantum pada Lampiran buku ajar ini.

BAB 11
ACCESS CONTROL LIST (ACL)

A. PENDAHULUAN

1. Deskripsi Singkat

Bab ini membuka pembahasan Capaian Pembelajaran Mata Kuliah keempat (CPMK-4) mengenai keamanan dan tata kelola jaringan enterprise, dimulai dengan Access Control List (ACL) sebagai mekanisme kontrol akses paling mendasar pada perangkat jaringan Cisco. ACL memungkinkan administrator jaringan menentukan lalu lintas mana yang diizinkan atau ditolak melewati suatu perangkat, berdasarkan kriteria seperti alamat IP sumber, alamat IP tujuan, protokol, dan nomor port. Pembahasan diawali dengan konsep ACL standar dan extended, dilanjutkan dengan proses penyusunan kebijakan akses (access policy), serta praktik konfigurasi dan pengujian ACL pada skenario jaringan enterprise.

Materi pada bab ini menjadi fondasi penting sebelum mahasiswa mempelajari firewall dan segmentasi jaringan pada Bab 12, karena ACL merupakan komponen dasar yang juga digunakan pada berbagai fitur keamanan lanjutan, termasuk sebagai bagian dari kebijakan firewall dan kontrol akses VPN yang telah dibahas pada Bab 9.

2. Capaian Pembelajaran Mata Kuliah (CPMK) yang Dicapai

Kode CPMK	:	CPMK-4
Rumusan CPMK	:	Mampu menerapkan prinsip keamanan dan tata kelola jaringan enterprise melalui ACL, firewall, segmentasi, serta monitoring jaringan.
Bobot CPMK	:	21% dari keseluruhan capaian mata kuliah
CPL yang Didukung	:	CPL-8 (penerapan prinsip keamanan siber dasar dan tata kelola teknologi informasi dalam pengelolaan sistem dan jaringan komputer)

3. Sub-CPMK yang Dicapai

Kode Sub-CPMK	:	Sub-CPMK 4.1
Rumusan Sub-CPMK	:	Mampu mengonfigurasi Access Control List (ACL) standar dan extended untuk pengamanan jaringan.
Pertemuan	:	Pertemuan ke-11
Indikator Penilaian	:	ACL berfungsi sesuai kebijakan akses yang ditentukan (dinilai melalui tugas praktik), bobot 2% dari total penilaian mata kuliah.

4. Tujuan Pembelajaran Khusus (TPK)

Setelah mempelajari bab ini secara tuntas, mahasiswa diharapkan mampu:

1. Menjelaskan konsep dan fungsi ACL sebagai mekanisme kontrol akses dasar dalam pengamanan jaringan enterprise.

2. Membedakan karakteristik dan kriteria penyaringan ACL standar dan ACL extended.

3. Menyusun kebijakan akses (access policy) yang tepat berdasarkan kebutuhan keamanan suatu skenario jaringan.

4. Mengonfigurasi ACL standar dan extended pada router Cisco IOS sesuai kebijakan akses yang telah ditentukan.

5. Menguji dan memverifikasi fungsi ACL untuk memastikan lalu lintas jaringan diizinkan atau ditolak sesuai kebijakan yang diterapkan.

5. Peta Konsep

Alur pembahasan materi pada Bab 11 disajikan dalam peta konsep berikut, yang menggambarkan keterkaitan logis antar-subbab menuju pencapaian Sub-CPMK 4.1.

ACL Standar dan Extended	→	Kebijakan Akses	→	Praktik Konfigurasi & Pengujian ACL

6. Prasyarat

Sebelum mempelajari bab ini, mahasiswa disarankan telah menguasai konsep dasar pengalamatan IP dan wildcard mask (sebagaimana telah digunakan pada konfigurasi OSPF di Bab 5), serta memahami konsep dasar routing dan interface pada router/Layer 3 switch yang telah dibahas pada Bab 4 dan Bab 5.

B. URAIAN MATERI

11.1 ACL Standar dan Extended

a. Penjelasan Konsep/Teori

Access Control List (ACL) adalah kumpulan pernyataan (statement) berurutan yang digunakan router atau Layer 3 switch untuk mengizinkan (permit) atau menolak (deny) lalu lintas jaringan berdasarkan kriteria tertentu. Setiap paket yang melewati interface tempat ACL diterapkan akan dievaluasi terhadap setiap baris ACL secara berurutan dari atas ke bawah, dan segera setelah paket tersebut cocok (match) dengan salah satu baris, tindakan pada baris tersebut (permit/deny) langsung diterapkan tanpa memeriksa baris-baris berikutnya. Apabila suatu paket tidak cocok dengan satu pun baris eksplisit yang telah dikonfigurasi, paket tersebut akan ditolak secara otomatis oleh aturan implisit yang disebut implicit deny any, yang selalu berada di akhir setiap ACL meskipun tidak terlihat dalam konfigurasi.

Cisco IOS mendukung dua jenis ACL berbasis nomor (numbered ACL) yang paling umum digunakan.

- ACL Standar (Standard ACL) — menyaring lalu lintas hanya berdasarkan alamat IP sumber (source), menggunakan rentang nomor 1–99 atau 1300–1999. Karena hanya mempertimbangkan sumber tanpa memperhatikan tujuan maupun jenis trafik, ACL standar sebaiknya diterapkan sedekat mungkin dengan tujuan (destination), untuk menghindari pemblokiran trafik yang tidak diinginkan di titik yang terlalu jauh dari tujuan sebenarnya.
- ACL Extended (Extended ACL) — menyaring lalu lintas berdasarkan kombinasi kriteria yang jauh lebih rinci, meliputi alamat IP sumber, alamat IP tujuan, jenis protokol (TCP, UDP, ICMP, dan lainnya), serta nomor port sumber/tujuan, menggunakan rentang nomor 100–199 atau 2000–2699. Karena mampu menyaring secara spesifik, ACL extended sebaiknya diterapkan sedekat mungkin dengan sumber (source), agar trafik yang tidak diinginkan segera ditolak sebelum menghabiskan bandwidth jaringan menuju tujuan.

Selain ACL bernomor, Cisco IOS juga mendukung named ACL yang menggunakan nama deskriptif (bukan angka) sebagai identitas ACL, memudahkan pengelolaan pada jaringan dengan banyak ACL sekaligus mempermudah proses pengeditan baris tertentu tanpa harus menghapus seluruh ACL.

Perbandingan karakteristik ACL standar dan extended dirangkum pada Tabel 11.1 berikut.

Aspek	ACL Standar	ACL Extended
Kriteria Penyaringan	Hanya alamat IP sumber	Alamat IP sumber, tujuan, protokol, dan port
Rentang Nomor	1–99, 1300–1999	100–199, 2000–2699
Penempatan Terbaik	Sedekat mungkin dengan tujuan (destination)	Sedekat mungkin dengan sumber (source)
Tingkat Kerincian	Rendah (kasar/umum)	Tinggi (spesifik per layanan/aplikasi)
Contoh Kebutuhan	Membatasi akses manajemen (VTY) dari subnet tertentu	Mengizinkan hanya trafik HTTPS menuju server tertentu

Tabel 11.1 Perbandingan ACL Standar dan Extended

Contoh sintaks dasar pembuatan ACL standar dan extended pada Cisco IOS ditunjukkan pada perintah berikut.

```
! ACL Standar – mengizinkan hanya subnet 10.10.99.0/24
R1(config)# access-list 10 permit 10.10.99.0 0.0.0.255
R1(config)# access-list 10 deny any

! ACL Extended – mengizinkan HTTPS menuju 192.168.10.50, menolak trafik lain
dari VLAN 30
R1(config)# access-list 100 permit tcp 192.168.30.0 0.0.0.255 host
192.168.10.50 eq 443
R1(config)# access-list 100 deny ip 192.168.30.0 0.0.0.255 host 192.168.10.50
R1(config)# access-list 100 permit ip any any
```

Contoh 11.1 Perintah dasar pembuatan ACL standar dan ACL extended pada Cisco IOS

b. Contoh Aplikasi

ACL standar sering digunakan untuk membatasi akses manajemen perangkat (misalnya akses Telnet/SSH ke router hanya dari subnet administrator), sedangkan ACL extended lebih sering digunakan untuk kebijakan keamanan yang lebih rinci, seperti mengizinkan hanya trafik web (HTTP/HTTPS) menuju server tertentu sementara jenis trafik lain dari subnet yang sama tetap ditolak.

11.2 Kebijakan Akses

a. Penjelasan Konsep/Teori

Sebelum mengonfigurasi ACL, administrator jaringan perlu menyusun kebijakan akses (access policy) secara sistematis, yaitu dokumen atau rancangan yang mendefinisikan secara jelas siapa (sumber) yang boleh mengakses apa (tujuan/layanan), serta bagaimana kebijakan tersebut akan diterjemahkan ke dalam baris-baris ACL. Proses penyusunan kebijakan akses umumnya mengikuti tahapan berikut.

- Identifikasi Kebutuhan — menentukan sumber daya (server, subnet, layanan) yang perlu dilindungi, serta pihak mana saja yang berwenang mengaksesnya berdasarkan kebutuhan bisnis/organisasi.
- Penyusunan Aturan Berurutan — merancang urutan baris ACL dari yang paling spesifik ke yang paling umum, karena ACL dievaluasi secara berurutan dan berhenti pada baris pertama yang cocok; aturan yang terlalu umum diletakkan di awal dapat menyebabkan aturan spesifik setelahnya tidak pernah tercapai (unreachable).
- Kewaspadaan terhadap Implicit Deny — selalu memastikan bahwa trafik yang seharusnya diizinkan (termasuk trafik penting seperti update routing protocol atau ICMP untuk keperluan troubleshooting) telah dicakup oleh baris permit yang eksplisit, karena implicit deny any di akhir ACL akan menolak seluruh trafik yang tidak secara eksplisit diizinkan.
- Dokumentasi Kebijakan — mendokumentasikan setiap baris ACL beserta tujuannya (misalnya melalui remark pada named ACL atau dokumen terpisah), sehingga administrator lain dapat memahami maksud setiap aturan di kemudian hari.

Kesalahan Umum: Urutan ACL yang Keliru

Salah satu kesalahan paling umum dalam penyusunan ACL adalah meletakkan aturan permit any atau deny any yang bersifat umum di awal daftar, sehingga aturan-aturan spesifik yang seharusnya dievaluasi terlebih dahulu justru tidak pernah tercapai (unreachable statement). Sebagai contoh, apabila baris "deny ip 192.168.30.0 0.0.0.255 any" diletakkan sebelum baris "permit tcp 192.168.30.0 0.0.0.255 host 192.168.10.50 eq 443", maka seluruh trafik dari VLAN 30 akan langsung ditolak pada baris pertama, dan baris permit HTTPS setelahnya tidak akan pernah diperiksa. Urutan aturan ACL harus selalu disusun dari yang paling spesifik menuju yang paling umum.

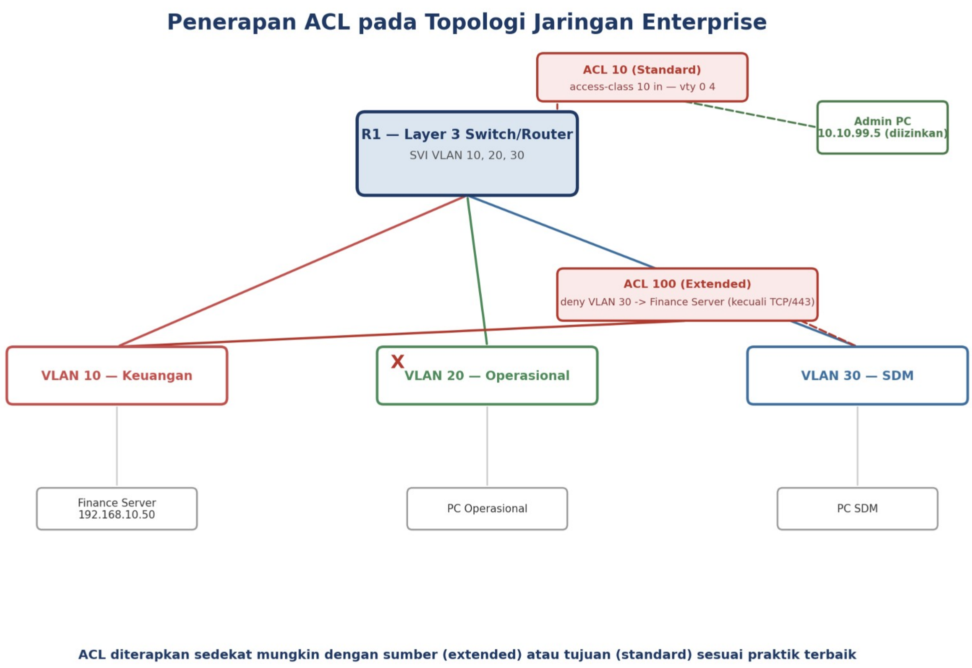
b. Contoh Aplikasi

Sebagai ilustrasi, kebijakan akses pada suatu organisasi dapat menetapkan bahwa hanya subnet Keuangan yang boleh mengakses server payroll melalui port aplikasi tertentu, subnet lain sepenuhnya ditolak mengakses server tersebut, namun seluruh subnet tetap diizinkan mengakses internet secara umum. Kebijakan semacam ini kemudian diterjemahkan menjadi rangkaian baris ACL extended yang diterapkan pada interface yang sesuai.

11.3 Praktik Konfigurasi dan Pengujian ACL

a. Penjelasan Konsep/Teori

Setelah ACL didefinisikan, ACL tersebut harus diterapkan (applied) pada interface yang sesuai menggunakan perintah ip access-group (untuk ACL numbered/named pada interface fisik/SVI) atau access-class (khusus untuk membatasi akses jalur virtual terminal/VTY), disertai penentuan arah (in atau out) relatif terhadap perspektif router.



Gambar 11.1 Penerapan ACL pada Topologi Jaringan Enterprise

Diagram di atas menggambarkan Router R1 yang melayani tiga VLAN (VLAN 10 Keuangan berisi Finance Server, VLAN 20 Operasional, dan VLAN 30 SDM). ACL Extended 100 diterapkan secara inbound pada SVI VLAN 30 untuk menolak akses VLAN 30 menuju Finance Server kecuali melalui port HTTPS (TCP 443), sesuai praktik terbaik penempatan ACL extended sedekat mungkin dengan sumber. Selain itu, ACL Standar 10 diterapkan pada jalur VTY router menggunakan access-class, hanya mengizinkan Admin PC pada subnet 10.10.99.0/24 untuk melakukan akses manajemen (Telnet/SSH) ke Router R1, sementara sumber lain akan ditolak.

Mengacu pada Gambar 11.1, berikut adalah contoh konfigurasi lengkap penerapan kedua ACL tersebut, melanjutkan definisi ACL pada Contoh 11.1.

```
! Menerapkan ACL Extended 100 secara inbound pada SVI VLAN 30
R1(config)# interface vlan 30
R1(config-if)# ip access-group 100 in
R1(config-if)# exit

! Menerapkan ACL Standar 10 pada jalur VTY (akses manajemen)
R1(config)# line vty 0 4
R1(config-line)# access-class 10 in
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Contoh 11.2 Perintah penerapan ACL extended pada SVI dan ACL standar pada jalur VTY

Tahapan pengujian ACL dilakukan sebagai berikut: (1) melakukan ping dan uji koneksi HTTPS dari PC pada VLAN 30 menuju Finance Server, memastikan hanya HTTPS yang berhasil sementara protokol lain (misalnya ping ICMP) ditolak; (2) mencoba melakukan SSH ke Router R1 dari PC pada VLAN 30 maupun VLAN 20, memastikan percobaan tersebut ditolak; (3) mencoba melakukan SSH ke Router R1 dari Admin PC pada subnet 10.10.99.0/24, memastikan percobaan tersebut berhasil; dan (4) memverifikasi statistik ACL menggunakan perintah berikut.

```
R1# show access-lists
R1# show ip interface vlan 30 | include access list
R1# show running-config | section line vty
```

Contoh 11.3 Perintah verifikasi ACL dan penerapannya pada interface/VTY

Perintah show access-lists menampilkan seluruh baris ACL beserta jumlah paket yang cocok (match) dengan setiap baris (match count), sangat berguna untuk memverifikasi apakah suatu aturan benar-benar berfungsi sebagaimana yang diharapkan atau tidak pernah tercapai sama sekali (menandakan kemungkinan kesalahan urutan aturan).

b. Contoh Aplikasi

Pengujian ACL secara menyeluruh, termasuk mencoba mengakses dari sumber yang seharusnya ditolak, merupakan praktik penting untuk memastikan kebijakan keamanan benar-benar berfungsi sebagaimana dirancang, bukan hanya menguji dari sumber yang seharusnya diizinkan saja.

C. RANGKUMAN

- ACL adalah kumpulan pernyataan permit/deny yang dievaluasi secara berurutan, dengan implicit deny any secara otomatis diterapkan di akhir setiap ACL.
- ACL standar menyaring hanya berdasarkan alamat IP sumber (nomor 1–99/1300–1999), sebaiknya diterapkan dekat tujuan; ACL extended menyaring berdasarkan sumber, tujuan, protokol, dan port (nomor 100–199/2000–2699), sebaiknya diterapkan dekat sumber.
- Penyusunan kebijakan akses memerlukan identifikasi kebutuhan, urutan aturan dari spesifik ke umum, kewaspadaan terhadap implicit deny, dan dokumentasi yang jelas.
- ACL diterapkan pada interface menggunakan ip access-group (in/out) atau pada jalur VTY menggunakan access-class, dengan arah penerapan yang menentukan efektivitas penyaringan.
- Verifikasi ACL dilakukan menggunakan show access-lists untuk memeriksa match count setiap baris, membantu memastikan ACL berfungsi sesuai kebijakan yang dirancang.

D. LATIHAN/SOAL

Petunjuk pengerjaan: Kerjakan seluruh soal berikut secara mandiri. Soal nomor 1–5 merupakan soal pemahaman konsep (jawaban singkat/uraian), soal nomor 6–8 merupakan soal konfigurasi, dan soal nomor 9–10 merupakan soal analisis/troubleshooting. Seluruh soal mengacu pada capaian Sub-CPMK 4.1.

1. Jelaskan konsep implicit deny any pada ACL Cisco IOS dan mengapa hal ini penting untuk dipahami administrator jaringan.

2. Jelaskan perbedaan kriteria penyaringan antara ACL standar dan ACL extended.

3. Jelaskan mengapa ACL extended sebaiknya diterapkan sedekat mungkin dengan sumber, sedangkan ACL standar sedekat mungkin dengan tujuan.

4. Jelaskan risiko yang dapat terjadi apabila urutan baris ACL tidak disusun dari yang paling spesifik ke yang paling umum.

5. Jelaskan perbedaan penggunaan perintah ip access-group dan access-class.

6. Tuliskan perintah Cisco IOS lengkap untuk membuat ACL standar bernomor 20 yang hanya mengizinkan subnet 172.16.5.0/24 dan menolak seluruh sumber lainnya.

7. Tuliskan perintah Cisco IOS lengkap untuk membuat ACL extended bernomor 110 yang mengizinkan trafik HTTP (port 80) dari subnet mana pun menuju host 10.1.1.100, dan menolak seluruh trafik lain menuju host tersebut.

8. Tuliskan perintah Cisco IOS untuk menerapkan ACL 110 pada soal sebelumnya secara inbound pada interface GigabitEthernet 0/1.

9. Setelah menerapkan sebuah ACL extended, administrator menemukan bahwa seluruh trafik routing OSPF antar-router pada interface yang sama juga ikut terblokir. Analisislah kemungkinan penyebab masalah tersebut dan langkah perbaikannya.

10. Berdasarkan hasil show access-lists, salah satu baris permit pada ACL menunjukkan match count 0 meskipun trafik yang seharusnya cocok dengan baris tersebut telah dikirim berkali-kali. Analisislah kemungkinan penyebab kondisi tersebut.

E. DAFTAR PUSTAKA

Cisco Networking Academy. (2022). CCNP Enterprise: Core networking technologies (ENCOR) companion guide. Cisco Press.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 1 (2nd ed.). Cisco Press.

Stallings, W. (2023). Network security essentials: Applications and standards (7th ed.). Pearson.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 2 (2nd ed.). Cisco Press.

Teare, D., & Paquet, C. (2022). Implementing Cisco IP routing (ROUTE) foundation learning guide (2nd ed.). Cisco Press.

F. TUGAS/STUDI KASUS

Tugas Praktik: Konfigurasi ACL Standar dan Extended

Menggunakan simulator jaringan (Cisco Packet Tracer atau GNS3), bangunlah topologi yang terdiri atas satu router/Layer 3 switch yang melayani tiga VLAN, mengacu pada skema topologi Gambar 11.1, dengan ketentuan kebijakan akses sebagai berikut.

1. VLAN 30 (SDM) hanya diizinkan mengakses Finance Server pada VLAN 10 melalui protokol HTTPS (TCP 443); seluruh jenis trafik lain dari VLAN 30 menuju Finance Server harus ditolak, menggunakan ACL extended yang diterapkan sedekat mungkin dengan sumber.

2. Akses manajemen (SSH) ke router hanya diizinkan dari subnet Admin (10.10.99.0/24); seluruh sumber lain harus ditolak mengakses jalur VTY router, menggunakan ACL standar.

3. Pastikan trafik routing dan trafik VLAN lain (VLAN 20 Operasional) yang tidak disebutkan dalam kebijakan tetap berjalan normal tanpa terpengaruh ACL yang diterapkan.

4. Uji seluruh skenario: (a) PC VLAN 30 mengakses Finance Server via HTTPS (harus berhasil), (b) PC VLAN 30 melakukan ping ke Finance Server (harus gagal), (c) PC VLAN 30/20 mencoba SSH ke router (harus gagal), (d) Admin PC mencoba SSH ke router (harus berhasil).

5. Lakukan verifikasi menggunakan show access-lists dan show ip interface, lalu sertakan hasil tangkapan layar (screenshot) seluruh pengujian pada laporan.

Laporan praktik (mencakup topologi, seluruh perintah konfigurasi, dan hasil pengujian) dikumpulkan dalam bentuk dokumen (PDF/Word) disertai file simulasi (.pkt/.gns3) sesuai tenggat waktu yang ditentukan dosen pengampu. Tugas ini dinilai menggunakan rubrik pada Rubrik Penilaian per Pertemuan 11 (aspek Tugas Praktik: Konfigurasi ACL) sebagaimana tercantum pada Lampiran buku ajar ini.

BAB 12
FIREWALL DAN SEGMENTASI JARINGAN

A. PENDAHULUAN

1. Deskripsi Singkat

Bab ini melanjutkan pembahasan keamanan jaringan enterprise dari Bab 11, beralih dari ACL sebagai mekanisme kontrol akses dasar menuju firewall sebagai lapisan pertahanan yang lebih terstruktur dan menyeluruh. Pembahasan diawali dengan konsep dan jenis-jenis firewall, dilanjutkan dengan prinsip least privilege dan konsep zonasi keamanan (security zone), serta ditutup dengan rancangan segmentasi jaringan enterprise yang mengintegrasikan VLAN (Bab 3), ACL (Bab 11), dan firewall secara berlapis.

Materi pada bab ini menjadi dasar penting sebelum mahasiswa mempelajari monitoring dan tata kelola jaringan pada Bab 13, karena rancangan segmentasi yang baik akan sangat memengaruhi bagaimana lalu lintas jaringan dipantau dan dianalisis pada tahap selanjutnya.

2. Capaian Pembelajaran Mata Kuliah (CPMK) yang Dicapai

Kode CPMK	:	CPMK-4
Rumusan CPMK	:	Mampu menerapkan prinsip keamanan dan tata kelola jaringan enterprise melalui ACL, firewall, segmentasi, serta monitoring jaringan.
Bobot CPMK	:	21% dari keseluruhan capaian mata kuliah
CPL yang Didukung	:	CPL-8 (penerapan prinsip keamanan siber dasar dan tata kelola teknologi informasi dalam pengelolaan sistem dan jaringan komputer)

3. Sub-CPMK yang Dicapai

Kode Sub-CPMK	:	Sub-CPMK 4.2
Rumusan Sub-CPMK	:	Mampu menjelaskan dan menerapkan konsep firewall serta segmentasi jaringan enterprise.
Pertemuan	:	Pertemuan ke-12
Indikator Penilaian	:	Ketepatan rancangan segmentasi sesuai prinsip keamanan (dinilai melalui tugas praktik), bobot 2% dari total penilaian mata kuliah.

4. Tujuan Pembelajaran Khusus (TPK)

Setelah mempelajari bab ini secara tuntas, mahasiswa diharapkan mampu:

1. Menjelaskan konsep firewall serta membandingkan jenis-jenis firewall (packet-filtering, stateful, next-generation).

2. Menjelaskan prinsip least privilege dan konsep zonasi keamanan (security zone) pada jaringan enterprise.

3. Merancang segmentasi jaringan enterprise berdasarkan prinsip keamanan yang tepat, termasuk konsep DMZ untuk server publik.

4. Menerapkan firewall sederhana berbasis zona (zone-based policy firewall) pada topologi jaringan enterprise menggunakan Cisco IOS.

5. Menguji dan memverifikasi rancangan segmentasi dan firewall sesuai kebijakan keamanan yang telah ditentukan.

5. Peta Konsep

Alur pembahasan materi pada Bab 12 disajikan dalam peta konsep berikut, yang menggambarkan keterkaitan logis antar-subbab menuju pencapaian Sub-CPMK 4.2.

Konsep Firewall	→	Prinsip Least Privilege dan Zonasi	→	Rancangan Segmentasi Jaringan Enterprise

6. Prasyarat

Sebelum mempelajari bab ini, mahasiswa disarankan telah menguasai materi Bab 11 mengenai ACL standar dan extended, serta Bab 3 mengenai VLAN sebagai dasar segmentasi jaringan pada Layer 2.

B. URAIAN MATERI

12.1 Konsep Firewall

a. Penjelasan Konsep/Teori

Firewall adalah perangkat atau perangkat lunak yang berfungsi sebagai penjaga gerbang (gatekeeper) antar-segmen jaringan dengan tingkat kepercayaan (trust level) yang berbeda, menerapkan kebijakan keamanan untuk mengizinkan atau menolak lalu lintas berdasarkan aturan yang telah ditetapkan. Meskipun ACL yang telah dibahas pada Bab 11 juga dapat berfungsi sebagai bentuk penyaringan dasar, firewall modern menawarkan kemampuan yang jauh lebih canggih dan menyeluruh. Firewall dapat dikelompokkan menjadi tiga generasi berdasarkan kemampuannya.

- Packet-Filtering Firewall — generasi paling dasar, menyaring paket secara independen (stateless) berdasarkan header paket (alamat IP, port, protokol) tanpa mengingat konteks koneksi sebelumnya, serupa dengan cara kerja ACL tradisional. Kelemahan utamanya adalah tidak dapat membedakan paket balasan (return traffic) yang sah dari koneksi yang telah diizinkan dengan paket baru yang mencoba masuk secara tidak sah.
- Stateful Firewall — mampu melacak status (state) setiap koneksi yang sedang berlangsung dalam sebuah tabel status koneksi (state table), sehingga hanya mengizinkan paket balasan yang sesuai dengan koneksi yang telah dimulai dari sisi yang tepercaya (trusted), tanpa perlu membuat aturan permit terpisah untuk setiap arah lalu lintas balasan. Firewall jenis ini menjadi standar umum pada kebanyakan perangkat jaringan enterprise saat ini, termasuk fitur Zone-Based Policy Firewall pada Cisco IOS.
- Next-Generation Firewall (NGFW) — generasi terbaru yang menambahkan kemampuan analisis mendalam terhadap konten paket (deep packet inspection), kesadaran terhadap aplikasi tertentu (application awareness, dapat membedakan trafik berdasarkan aplikasi meskipun menggunakan port yang sama), integrasi sistem pencegahan intrusi (Intrusion Prevention System/IPS), serta identifikasi berbasis identitas pengguna, bukan hanya alamat IP semata.

Perbandingan ketiga jenis firewall tersebut dirangkum pada Tabel 12.1 berikut.

Aspek	Packet-Filtering	Stateful	Next-Generation (NGFW)
Kesadaran Koneksi	Tidak (stateless)	Ya (state table)	Ya, disertai analisis konten
Kompleksitas Aturan	Rendah, per paket	Sedang, per sesi/koneksi	Tinggi, per aplikasi/pengguna
Kemampuan Deteksi	Sangat terbatas	Terbatas pada Layer	Luas (IPS, application

Aspek	Packet-Filtering	Stateful	Next-Generation (NGFW)
Ancaman		3/4	control)
Contoh Implementasi	ACL dasar pada router	Zone-Based Firewall (Cisco IOS)	Cisco Firepower, Palo Alto, Fortinet

Tabel 12.1 Perbandingan Jenis-Jenis Firewall

b. Contoh Aplikasi

Pada jaringan kampus berskala menengah, router edge yang mendukung Zone-Based Policy Firewall (stateful) umumnya sudah memadai untuk melindungi jaringan internal dari akses tidak sah dari internet, sementara organisasi dengan kebutuhan keamanan yang lebih tinggi (misalnya institusi keuangan) umumnya menambahkan perangkat NGFW khusus untuk mendapatkan visibilitas dan kontrol yang lebih mendalam terhadap aplikasi dan ancaman siber modern.

12.2 Prinsip Least Privilege dan Zonasi

a. Penjelasan Konsep/Teori

Prinsip least privilege (hak akses minimum) adalah prinsip keamanan fundamental yang menyatakan bahwa setiap entitas (pengguna, perangkat, atau segmen jaringan) hanya diberikan akses yang benar-benar diperlukan untuk menjalankan fungsinya, tidak lebih. Dalam konteks desain jaringan, prinsip ini diterapkan melalui kebijakan default deny, yaitu seluruh lalu lintas ditolak secara default kecuali secara eksplisit diizinkan berdasarkan kebutuhan yang telah diverifikasi.

Penerapan prinsip least privilege pada skala jaringan enterprise umumnya diwujudkan melalui konsep zonasi keamanan (security zone), yaitu pengelompokan interface-interface jaringan yang memiliki tingkat kepercayaan yang setara ke dalam satu zona logis, kemudian kebijakan keamanan didefinisikan di antara pasangan zona (zone-pair), bukan per interface secara individual. Tiga zona keamanan yang paling umum ditemui pada jaringan enterprise adalah sebagai berikut.

- Zona Inside — mencakup seluruh jaringan internal organisasi yang tepercaya (trusted), seperti LAN korporat dengan berbagai VLAN departemen.
- Zona Outside — mencakup jaringan yang tidak tepercaya (untrusted), umumnya internet publik.
- Zona DMZ (Demilitarized Zone) — zona perantara yang berisi server-server yang perlu diakses dari luar (publik), seperti web server atau mail server, namun tetap

diisolasi dari jaringan internal agar apabila server tersebut berhasil disusupi, penyerang tidak dapat langsung mengakses jaringan internal yang lebih sensitif.

Pada firewall berbasis zona (zone-based), secara default seluruh lalu lintas antar-zona yang berbeda akan ditolak, kecuali kebijakan (policy) secara eksplisit didefinisikan untuk pasangan zona tertentu (zone-pair), sedangkan lalu lintas di dalam zona yang sama (intra-zone) secara default diizinkan. Prinsip ini secara langsung mengimplementasikan konsep least privilege pada level arsitektur jaringan.

Contoh sintaks dasar pendefinisian zona keamanan pada Cisco IOS Zone-Based Policy Firewall ditunjukkan pada perintah berikut.

```
R1(config)# zone security INSIDE
R1(config-sec-zone)# exit
R1(config)# zone security OUTSIDE
R1(config-sec-zone)# exit
R1(config)# zone security DMZ
R1(config-sec-zone)# exit

! Menetapkan interface ke masing-masing zona
R1(config)# interface vlan 10
R1(config-if)# zone-member security INSIDE
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# zone-member security OUTSIDE
R1(config)# interface gigabitEthernet 0/1
R1(config-if)# zone-member security DMZ
```

Contoh 12.1 Perintah pendefinisian zona keamanan dan penetapan interface ke zona pada Cisco IOS

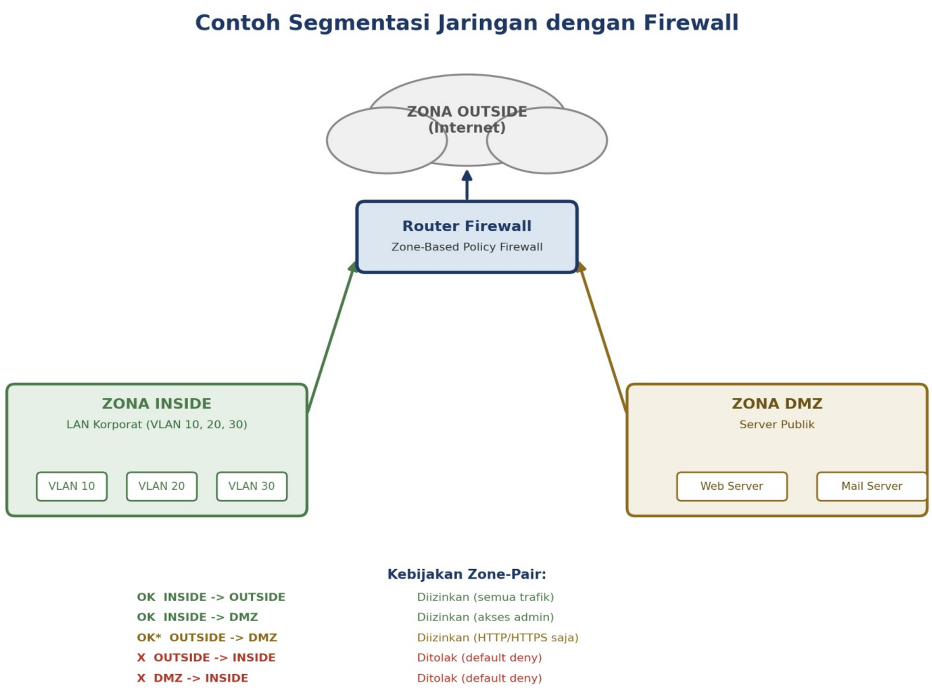
b. Contoh Aplikasi

Sebuah organisasi yang menempatkan server email dan web perusahaan pada zona DMZ dapat memastikan bahwa meskipun server tersebut menjadi sasaran serangan dari internet (zona Outside), penyerang tidak akan memperoleh akses langsung menuju data karyawan atau sistem internal lain yang berada pada zona Inside, karena kebijakan default deny berlaku antara zona DMZ dan zona Inside kecuali dinyatakan lain.

12.3 Rancangan Segmentasi Jaringan Enterprise

a. Penjelasan Konsep/Teori

Rancangan segmentasi jaringan enterprise yang baik mengintegrasikan beberapa lapisan pertahanan sekaligus: VLAN untuk segmentasi Layer 2 dalam satu zona (sebagaimana dibahas pada Bab 3), ACL untuk penyaringan lalu lintas yang lebih rinci pada titik tertentu (Bab 11), dan firewall berbasis zona untuk menegakkan kebijakan keamanan menyeluruh antar-zona kepercayaan yang berbeda. Pendekatan berlapis (defense in depth) semacam ini memastikan bahwa apabila satu lapisan pertahanan berhasil dilewati, lapisan-lapisan lain tetap memberikan perlindungan tambahan.



Gambar 12.1 Contoh Segmentasi Jaringan dengan Firewall

Diagram di atas menggambarkan rancangan segmentasi jaringan enterprise dengan tiga zona keamanan yang dihubungkan melalui satu Router Firewall (Zone-Based Policy Firewall). Zona Inside mencakup LAN korporat dengan VLAN 10, 20, dan 30. Zona DMZ berisi Web Server dan Mail Server yang perlu diakses dari luar. Zona Outside mewakili jaringan internet. Kebijakan zone-pair yang diterapkan mengizinkan Inside mengakses Outside dan DMZ secara bebas, mengizinkan Outside mengakses DMZ hanya melalui protokol HTTP/HTTPS, namun menolak seluruh akses dari Outside maupun DMZ menuju Inside secara default, sesuai prinsip least privilege.

Mengacu pada Gambar 12.1 dan kelanjutan dari Contoh 12.1, berikut adalah contoh konfigurasi kebijakan (policy) zone-based firewall untuk menerapkan aturan zone-pair sesuai rancangan tersebut.

```
! Class-map untuk mengidentifikasi trafik HTTP/HTTPS menuju DMZ
R1(config)# class-map type inspect match-any CM-WEB
R1(config-cmap)# match protocol http
R1(config-cmap)# match protocol https
R1(config-cmap)# exit

! Policy-map: Inside -> Outside (izinkan semua) dan Inside -> DMZ (izinkan
semua)
R1(config)# policy-map type inspect PM-INSIDE-TO-OUTSIDE
R1(config-pmap)# class class-default
R1(config-pmap-c)# inspect
```

```
R1(config)# policy-map type inspect PM-INSIDE-TO-DMZ
R1(config-pmap)# class class-default
R1(config-pmap-c)# inspect

! Policy-map: Outside -> DMZ (hanya izinkan HTTP/HTTPS)
R1(config)# policy-map type inspect PM-OUTSIDE-TO-DMZ
R1(config-pmap)# class CM-WEB
R1(config-pmap-c)# inspect

! Zone-pair — mengikat policy-map ke arah antar-zona yang sesuai
R1(config)# zone-pair security ZP-IN-OUT source INSIDE destination OUTSIDE
R1(config-sec-zone-pair)# service-policy type inspect PM-INSIDE-TO-OUTSIDE
R1(config)# zone-pair security ZP-IN-DMZ source INSIDE destination DMZ
R1(config-sec-zone-pair)# service-policy type inspect PM-INSIDE-TO-DMZ
R1(config)# zone-pair security ZP-OUT-DMZ source OUTSIDE destination DMZ
R1(config-sec-zone-pair)# service-policy type inspect PM-OUTSIDE-TO-DMZ

! Catatan: tidak ada zone-pair Outside->Inside atau DMZ->Inside -> otomatis
DITOLAK (default deny)
```

Contoh 12.2 Perintah konfigurasi class-map, policy-map, dan zone-pair pada Zone-Based Policy Firewall

Salah satu keunggulan penting dari pendekatan zone-based firewall adalah administrator tidak perlu secara eksplisit mengonfigurasi aturan deny antara Outside dan Inside maupun antara DMZ dan Inside — cukup dengan tidak mendefinisikan zone-pair untuk kedua arah tersebut, seluruh lalu lintas di antara keduanya akan otomatis ditolak sesuai kebijakan default deny yang berlaku pada firewall berbasis zona.

Verifikasi rancangan segmentasi dan firewall dilakukan menggunakan perintah berikut.

```
R1# show zone security
R1# show zone-pair security
R1# show policy-map type inspect zone-pair sessions
```

Contoh 12.3 Perintah verifikasi konfigurasi zona keamanan dan zone-pair

b. Contoh Aplikasi

Rancangan segmentasi tiga zona (Inside, DMZ, Outside) sebagaimana dicontohkan pada bab ini merupakan pola rancangan yang sangat umum diterapkan pada jaringan enterprise skala kecil-menengah yang mengelola server publik sendiri, dan menjadi dasar konseptual bagi rancangan segmentasi yang lebih kompleks pada organisasi berskala lebih besar dengan banyak zona keamanan sekaligus (misalnya zona terpisah untuk setiap departemen dengan tingkat sensitivitas data yang berbeda).

C. RANGKUMAN

- Firewall dapat dikelompokkan menjadi tiga generasi: packet-filtering (stateless), stateful (melacak status koneksi), dan next-generation (NGFW, disertai deep packet inspection dan application awareness).
- Prinsip least privilege menyatakan setiap entitas hanya diberikan akses yang benar-benar diperlukan, diwujudkan melalui kebijakan default deny pada tingkat jaringan.
- Zonasi keamanan mengelompokkan interface dengan tingkat kepercayaan setara ke dalam zona (Inside, Outside, DMZ), dengan kebijakan didefinisikan antar-pasangan zona (zone-pair), bukan per interface individual.
- DMZ adalah zona perantara untuk menempatkan server publik, mengisolasi risiko apabila server tersebut disusupi agar tidak langsung berdampak pada jaringan internal.
- Rancangan segmentasi jaringan enterprise yang baik menggabungkan VLAN, ACL, dan firewall berbasis zona secara berlapis (defense in depth), dengan zone-pair yang tidak didefinisikan secara otomatis mengikuti kebijakan default deny.

D. LATIHAN/SOAL

Petunjuk pengerjaan: Kerjakan seluruh soal berikut secara mandiri. Soal nomor 1–5 merupakan soal pemahaman konsep (jawaban singkat/uraian), soal nomor 6–8 merupakan soal konfigurasi/rancangan, dan soal nomor 9–10 merupakan soal analisis/troubleshooting. Seluruh soal mengacu pada capaian Sub-CPMK 4.2.

1. Jelaskan perbedaan mendasar antara packet-filtering firewall dan stateful firewall.

2. Jelaskan kemampuan tambahan yang dimiliki Next-Generation Firewall (NGFW) dibandingkan stateful firewall konvensional.

3. Jelaskan prinsip least privilege dan bagaimana prinsip tersebut diwujudkan pada kebijakan default deny.

4. Jelaskan fungsi zona DMZ dan mengapa server publik sebaiknya tidak ditempatkan langsung pada zona Inside.

5. Jelaskan mengapa pada zone-based firewall, tidak diperlukan konfigurasi eksplisit untuk menolak lalu lintas antar-zona yang tidak didefinisikan zone-pair-nya.

6. Rancanglah skema zonasi keamanan (minimal tiga zona) untuk sebuah rumah sakit yang memiliki sistem rekam medis internal, website informasi publik, dan sistem pendaftaran online untuk pasien.

7. Tuliskan perintah Cisco IOS untuk membuat zona keamanan bernama SERVERFARM dan menetapkan interface GigabitEthernet 0/2 sebagai anggota zona tersebut.

8. Tuliskan perintah Cisco IOS untuk membuat zone-pair dari zona INSIDE menuju zona SERVERFARM yang menerapkan policy-map bernama PM-TO-SERVERFARM.

9. Setelah konfigurasi zone-based firewall diterapkan, pengguna pada zona Inside melaporkan tidak dapat mengakses server pada zona DMZ sama sekali, padahal zone-pair INSIDE-ke-DMZ telah dikonfigurasi. Analisislah kemungkinan penyebab masalah tersebut.

10. Sebuah organisasi ingin menambahkan zona keempat khusus untuk perangkat IoT (Internet of Things) yang memiliki tingkat kepercayaan lebih rendah dibandingkan zona Inside namun tidak perlu diakses dari internet. Rancanglah kebijakan zone-pair yang sesuai untuk zona IoT tersebut terhadap ketiga zona lainnya, disertai justifikasi.

E. DAFTAR PUSTAKA

Stallings, W. (2023). Network security essentials: Applications and standards (7th ed.). Pearson.

Cisco Networking Academy. (2022). CCNP Enterprise: Core networking technologies (ENCOR) companion guide. Cisco Press.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 2 (2nd ed.). Cisco Press.

Froom, R., Frahim, E., & Sivasubramanian, B. (2021). Implementing Cisco IP switched networks (SWITCH) foundation learning guide (2nd ed.). Cisco Press.

Teare, D., & Paquet, C. (2022). Implementing Cisco IP routing (ROUTE) foundation learning guide (2nd ed.). Cisco Press.

F. TUGAS/STUDI KASUS

Tugas Praktik: Rancangan Segmentasi dan Zone-Based Firewall

Menggunakan simulator jaringan (Cisco Packet Tracer atau GNS3), bangunlah topologi zone-based firewall yang terdiri atas tiga zona keamanan (Inside, DMZ, Outside), mengacu pada skema topologi Gambar 12.1, dengan ketentuan kebijakan sebagai berikut.

1. Definisikan tiga zona keamanan (INSIDE, DMZ, OUTSIDE) dan tetapkan interface/SVI yang sesuai sebagai anggota masing-masing zona.

2. Terapkan kebijakan zone-pair INSIDE ke OUTSIDE dan INSIDE ke DMZ yang mengizinkan seluruh trafik.

3. Terapkan kebijakan zone-pair OUTSIDE ke DMZ yang hanya mengizinkan trafik HTTP dan HTTPS menuju Web Server pada zona DMZ.

4. Pastikan tidak ada zone-pair yang dikonfigurasi untuk arah OUTSIDE ke INSIDE maupun DMZ ke INSIDE, sehingga kedua arah tersebut mengikuti kebijakan default deny.

5. Uji seluruh skenario kebijakan: (a) PC Inside mengakses internet dan Web Server DMZ (harus berhasil), (b) PC simulasi Outside mengakses Web Server DMZ via HTTP (harus berhasil), (c) PC simulasi Outside mencoba ping ke PC Inside (harus gagal), lalu verifikasi menggunakan show zone-pair security dan show policy-map type inspect zone-pair sessions, sertakan hasil tangkapan layar pada laporan.

Laporan praktik (mencakup rancangan zonasi, seluruh perintah konfigurasi, dan hasil pengujian) dikumpulkan dalam bentuk dokumen (PDF/Word) disertai file simulasi (.pkt/.gns3) sesuai tenggat waktu yang ditentukan dosen pengampu. Tugas ini dinilai menggunakan rubrik pada Rubrik Penilaian per Pertemuan 12 (aspek Tugas Praktik: Rancangan Segmentasi & Firewall) sebagaimana tercantum pada Lampiran buku ajar ini.

BAB 13
MONITORING DAN TATA KELOLA JARINGAN

A. PENDAHULUAN

1. Deskripsi Singkat

Bab ini membahas monitoring dan tata kelola jaringan sebagai penutup rangkaian topik CPMK-4 mengenai keamanan dan tata kelola jaringan enterprise. Setelah mahasiswa mempelajari mekanisme pengamanan jaringan melalui ACL (Bab 11) dan firewall (Bab 12), bab ini melengkapi siklus keamanan dengan kemampuan memantau (monitor) kondisi jaringan secara berkelanjutan menggunakan protokol SNMP dan teknologi NetFlow, menginterpretasikan data yang diperoleh, serta menyusun kebijakan penggunaan jaringan (acceptable use policy) sebagai bagian dari tata kelola teknologi informasi yang baik.

Materi pada bab ini menjadi penutup seluruh rangkaian pembahasan teknis mata kuliah Enterprise Networking, sekaligus menjadi bekal penting bagi mahasiswa sebelum memasuki tahap akhir mata kuliah, yaitu perancangan dan dokumentasi teknis jaringan enterprise secara menyeluruh pada Bab 14 dan presentasi hasil rancangan pada Bab 15.

2. Capaian Pembelajaran Mata Kuliah (CPMK) yang Dicapai

Kode CPMK	:	CPMK-4
Rumusan CPMK	:	Mampu menerapkan prinsip keamanan dan tata kelola jaringan enterprise melalui ACL, firewall, segmentasi, serta monitoring jaringan.
Bobot CPMK	:	21% dari keseluruhan capaian mata kuliah
CPL yang Didukung	:	CPL-8 (penerapan prinsip keamanan siber dasar dan tata kelola teknologi informasi) dan CPL-9 (kemampuan mengomunikasikan hasil kerja teknis secara lisan dan tertulis)

3. Sub-CPMK yang Dicapai

Kode Sub-CPMK	:	Sub-CPMK 4.3
Rumusan Sub-CPMK	:	Mampu menerapkan prinsip monitoring dan tata kelola jaringan (SNMP, NetFlow, kebijakan penggunaan).
Pertemuan	:	Pertemuan ke-13
Indikator Penilaian	:	Ketepatan interpretasi data monitoring dan kebijakan yang disusun (dinilai melalui tugas praktik), bobot 3% dari total penilaian mata kuliah.

4. Tujuan Pembelajaran Khusus (TPK)

Setelah mempelajari bab ini secara tuntas, mahasiswa diharapkan mampu:

1. Menjelaskan konsep dan cara kerja SNMP (Simple Network Management Protocol) untuk pemantauan status dan kesehatan perangkat jaringan.

2. Menjelaskan konsep dan cara kerja NetFlow untuk analisis pola dan volume lalu lintas jaringan.

3. Menginterpretasikan data monitoring SNMP dan NetFlow untuk mengidentifikasi kondisi normal maupun anomali pada jaringan.

4. Menyusun kebijakan penggunaan jaringan (acceptable use policy) yang sesuai dengan kebutuhan tata kelola suatu organisasi.

5. Mengonfigurasi dan menguji fungsi monitoring dasar (SNMP dan NetFlow) pada perangkat jaringan Cisco IOS.

5. Peta Konsep

Alur pembahasan materi pada Bab 13 disajikan dalam peta konsep berikut, yang menggambarkan keterkaitan logis antar-subbab menuju pencapaian Sub-CPMK 4.3.

SNMP dan NetFlow	→	**Interpretasi Data Monitoring**	→	**Penyusunan Kebijakan Penggunaan Jaringan**

6. Prasyarat

Sebelum mempelajari bab ini, mahasiswa disarankan telah menguasai materi Bab 11 dan Bab 12 mengenai ACL dan firewall, serta memiliki pemahaman dasar mengenai protokol TCP/IP untuk memahami komponen data yang dipantau melalui SNMP dan NetFlow.

B. URAIAN MATERI

13.1 SNMP dan NetFlow

a. Penjelasan Konsep/Teori

Simple Network Management Protocol (SNMP) adalah protokol standar yang digunakan untuk memantau dan mengelola perangkat pada jaringan, memungkinkan administrator memperoleh informasi status perangkat (seperti utilisasi CPU, penggunaan memori, status interface, dan penghitung error) secara terpusat dari satu sistem manajemen jaringan (Network Management System/NMS), tanpa perlu login satu per satu ke setiap perangkat.

Arsitektur SNMP terdiri atas tiga komponen utama.

- SNMP Manager — perangkat lunak yang berjalan pada NMS, bertugas mengirimkan permintaan (query) dan menerima informasi dari perangkat yang dipantau.
- SNMP Agent — perangkat lunak yang berjalan pada perangkat yang dipantau (router, switch, server), bertugas mengumpulkan informasi lokal dan meresponsnya kepada manager, serta dapat mengirimkan notifikasi secara mandiri apabila terjadi kejadian penting.
- MIB (Management Information Base) — basis data hierarkis yang berisi definisi seluruh variabel/informasi yang dapat diakses melalui SNMP pada suatu perangkat, dengan setiap variabel diidentifikasi menggunakan Object Identifier (OID) yang unik.

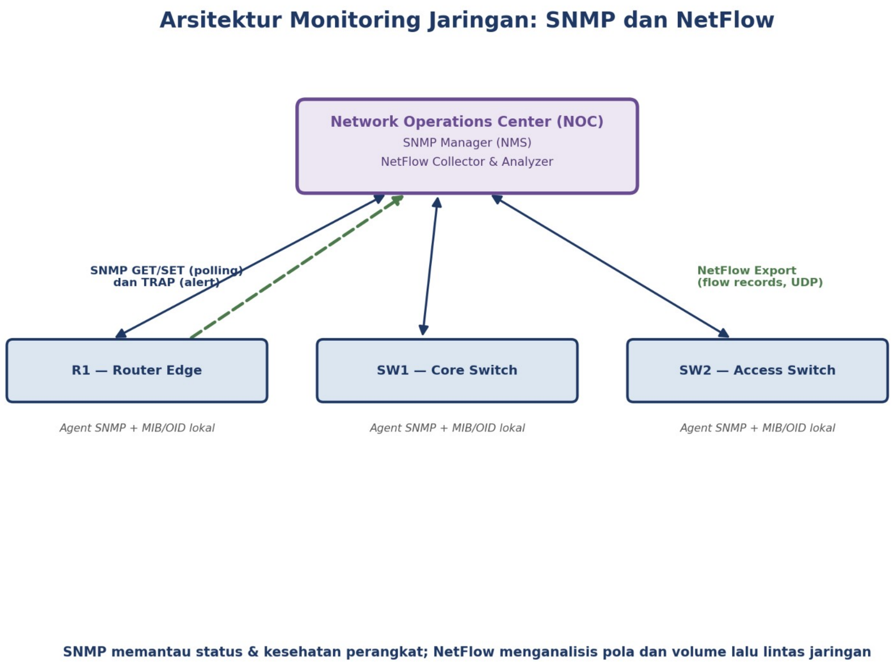
SNMP mendukung beberapa jenis operasi, yaitu GET (manager meminta nilai satu variabel tertentu dari agent), GETNEXT (meminta variabel berikutnya dalam struktur MIB), SET (manager mengubah nilai suatu variabel pada agent), dan TRAP (agent secara mandiri mengirimkan notifikasi kepada manager ketika terjadi kejadian penting, seperti interface down, tanpa menunggu permintaan dari manager). Terdapat tiga versi SNMP: SNMPv1 dan SNMPv2c yang menggunakan community string sebagai bentuk autentikasi sederhana namun dikirim dalam bentuk teks polos (plaintext) sehingga rentan disadap, serta SNMPv3 yang menambahkan autentikasi dan enkripsi yang jauh lebih kuat, sehingga menjadi versi yang direkomendasikan untuk implementasi pada jaringan produksi saat ini.

Berbeda dengan SNMP yang berfokus pada status perangkat, NetFlow adalah teknologi yang dikembangkan oleh Cisco untuk mengumpulkan informasi mengenai lalu lintas IP yang melewati suatu interface, dengan setiap flow (aliran data) diidentifikasi berdasarkan kombinasi tujuh atribut utama: alamat IP sumber, alamat IP tujuan, port sumber, port tujuan, protokol Layer 4, jenis layanan (ToS), dan interface. Informasi flow yang terkumpul kemudian diekspor secara berkala menuju perangkat pengumpul (NetFlow collector) untuk dianalisis lebih lanjut, memberikan visibilitas mengenai aplikasi apa saja yang digunakan, siapa pengguna dengan trafik tertinggi (top talkers), dan pola lalu lintas secara keseluruhan.

Perbandingan karakteristik SNMP dan NetFlow dirangkum pada Tabel 13.1 berikut.

Aspek	SNMP	NetFlow
Fokus Pemantauan	Status dan kesehatan perangkat (CPU, memori, interface)	Pola dan volume lalu lintas jaringan
Mekanisme	Polling (GET/SET) dan notifikasi (TRAP)	Ekspor flow record secara berkala dari perangkat
Granularitas Data	Per perangkat/interface	Per aliran (flow) trafik individual
Kegunaan Utama	Pemantauan kesehatan infrastruktur secara real-time	Analisis kapasitas, deteksi anomali, identifikasi aplikasi

Tabel 13.1 Perbandingan SNMP dan NetFlow



Gambar 13.1 Arsitektur Monitoring Jaringan: SNMP dan NetFlow

Diagram di atas menggambarkan sebuah Network Operations Center (NOC) yang berperan ganda sebagai SNMP Manager dan NetFlow Collector, memantau tiga perangkat jaringan (Router Edge, Core Switch, dan Access Switch). Setiap perangkat menjalankan SNMP Agent yang merespons permintaan GET/SET dari NOC serta mengirimkan TRAP saat terjadi kejadian penting. Router Edge secara khusus juga mengekspor flow record NetFlow menuju NOC untuk dianalisis, memberikan visibilitas terhadap pola lalu lintas yang melewati jaringan secara keseluruhan.

Konfigurasi dasar SNMPv3 dan NetFlow pada Cisco IOS dicontohkan pada perintah berikut.

```
! Konfigurasi SNMPv3 (autentikasi dan enkripsi)
```

```
R1(config)# snmp-server group ADMIN-GROUP v3 priv
R1(config)# snmp-server user netadmin ADMIN-GROUP v3 auth sha AuthPass123 priv
aes 128 PrivPass123
R1(config)# snmp-server host 10.10.99.10 version 3 priv netadmin
R1(config)# snmp-server enable traps

! Konfigurasi NetFlow pada interface dan ekspor ke collector
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip flow ingress
R1(config-if)# ip flow egress
R1(config-if)# exit
R1(config)# ip flow-export destination 10.10.99.10 9996
R1(config)# ip flow-export version 9
```

Contoh 13.1 Perintah konfigurasi SNMPv3 dan NetFlow pada Cisco IOS

b. Contoh Aplikasi

Sebuah tim operasional jaringan (Network Operations Center/NOC) memanfaatkan SNMP untuk menerima peringatan otomatis (trap) ketika sebuah interface penting mengalami gangguan, sementara data NetFlow digunakan secara terpisah untuk menganalisis mengapa utilisasi bandwidth pada jam tertentu meningkat drastis, misalnya untuk mengidentifikasi aplikasi atau pengguna mana yang menjadi penyebab utamanya.

13.2 Interpretasi Data Monitoring

a. Penjelasan Konsep/Teori

Mengumpulkan data monitoring saja tidak cukup tanpa kemampuan menginterpretasikannya secara tepat. Salah satu konsep fundamental dalam interpretasi data monitoring adalah baseline, yaitu pola lalu lintas dan utilisasi sumber daya yang dianggap normal pada kondisi operasional sehari-hari, yang diperoleh dari observasi data monitoring dalam periode waktu tertentu. Baseline inilah yang menjadi acuan pembanding untuk mendeteksi anomali atau penyimpangan yang memerlukan perhatian lebih lanjut.

Beberapa indikator umum yang perlu diperhatikan dalam interpretasi data monitoring adalah sebagai berikut.

- Utilisasi Interface — persentase penggunaan bandwidth suatu interface dibandingkan kapasitas maksimalnya; utilisasi yang secara konsisten mendekati 100% mengindikasikan kebutuhan penambahan kapasitas (upgrade bandwidth atau EtherChannel, sebagaimana dibahas pada Bab 4).
- Penghitung Error (Error Counter) — jumlah paket yang mengalami kesalahan (CRC error, collision, drop) pada suatu interface; peningkatan penghitung error

secara tiba-tiba dapat mengindikasikan masalah fisik pada kabel/konektor atau ketidaksesuaian konfigurasi duplex.

- Top Talkers — host atau aplikasi dengan volume trafik tertinggi berdasarkan data NetFlow; identifikasi top talkers membantu memahami pola penggunaan bandwidth dan menemukan penggunaan yang tidak wajar (misalnya satu host yang tiba-tiba mengonsumsi bandwidth sangat besar).
- Anomali Pola Trafik — penyimpangan signifikan dari baseline, seperti lonjakan trafik menuju port yang tidak umum digunakan, yang dapat mengindikasikan potensi ancaman keamanan seperti pemindaian port (port scanning) atau serangan denial-of-service.

Studi Interpretasi: Lonjakan Trafik Tidak Wajar

Data NetFlow pada suatu pagi hari menunjukkan satu host di VLAN 30 (SDM) yang biasanya hanya menghasilkan trafik sekitar 2 Mbps, tiba-tiba menghasilkan trafik keluar (outbound) sebesar 45 Mbps menuju satu alamat IP tunggal di luar jaringan, pada port TCP 4444 yang tidak umum digunakan aplikasi bisnis apa pun. Pola ini menyimpang jauh dari baseline normal host tersebut dan mengarah pada dugaan host telah terinfeksi malware yang sedang mengirimkan data secara tidak sah (data exfiltration) atau menjadi bagian dari botnet. Administrator perlu segera melakukan investigasi lebih lanjut dan mengisolasi host tersebut dari jaringan menggunakan ACL atau kebijakan firewall yang telah dipelajari pada Bab 11 dan Bab 12.

b. Contoh Aplikasi

Tim keamanan siber pada organisasi enterprise umumnya menetapkan baseline utilisasi bandwidth normal per departemen, sehingga ketika terjadi penyimpangan signifikan pada jam-jam tertentu (misalnya di luar jam kerja), sistem monitoring dapat memicu peringatan dini yang memungkinkan investigasi dilakukan sebelum insiden keamanan berkembang lebih jauh.

13.3 Penyusunan Kebijakan Penggunaan Jaringan

a. Penjelasan Konsep/Teori

Kebijakan Penggunaan Jaringan (Acceptable Use Policy/AUP) adalah dokumen formal yang mengatur bagaimana sumber daya jaringan organisasi boleh dan tidak boleh digunakan oleh seluruh pengguna, menjadi salah satu pilar penting dalam tata kelola teknologi informasi (IT governance) yang melengkapi kontrol teknis seperti ACL dan firewall dengan kontrol administratif. AUP yang baik umumnya mencakup komponen-komponen berikut.

- Ruang Lingkup dan Tujuan — menjelaskan kepada siapa kebijakan berlaku (karyawan, kontraktor, tamu) dan tujuan penyusunan kebijakan tersebut.

- Aktivitas yang Diizinkan dan Dilarang — daftar eksplisit penggunaan sumber daya jaringan yang diperbolehkan (misalnya akses internet untuk keperluan pekerjaan) dan yang dilarang (misalnya mengunduh perangkat lunak bajakan, mengakses situs berbahaya, atau menghubungkan perangkat pribadi tanpa izin ke jaringan internal).
- Kuota dan Prioritas Sumber Daya — batasan penggunaan bandwidth atau sumber daya lain untuk memastikan ketersediaan yang adil bagi seluruh pengguna, serta prioritas untuk aplikasi bisnis kritis.
- Pemberitahuan Pemantauan (Monitoring Notice) — pernyataan eksplisit bahwa organisasi berhak memantau penggunaan jaringan (melalui SNMP, NetFlow, dan mekanisme lain) untuk keperluan keamanan dan kepatuhan, sekaligus menjadi dasar hukum/etika bagi tim IT untuk melakukan monitoring.
- Sanksi Pelanggaran — konsekuensi yang akan diterima pengguna apabila melanggar ketentuan yang telah ditetapkan dalam kebijakan.

Kebijakan penggunaan jaringan yang telah disusun perlu diverifikasi kepatuhannya secara berkala menggunakan data monitoring yang telah dibahas pada sub-bab sebelumnya; sebagai contoh, data NetFlow dapat digunakan untuk memverifikasi apakah kebijakan pembatasan akses ke platform streaming video pada jam kerja benar-benar dipatuhi, sehingga terdapat keterkaitan erat antara kebijakan tata kelola (governance) dan kemampuan teknis monitoring jaringan.

b. Contoh Aplikasi

Sebuah institusi pendidikan dapat menyusun AUP yang membatasi akses mahasiswa terhadap situs perjudian daring dan platform berbagi file ilegal pada jaringan kampus, sekaligus menetapkan kuota bandwidth per pengguna pada jaringan Wi-Fi asrama, dengan kepatuhan terhadap kebijakan tersebut dipantau secara berkala menggunakan data NetFlow dari perangkat jaringan yang relevan.

C. RANGKUMAN

- SNMP memantau status dan kesehatan perangkat jaringan melalui arsitektur manager-agent-MIB, dengan operasi GET/SET/GETNEXT (polling) dan TRAP (notifikasi mandiri); SNMPv3 direkomendasikan karena mendukung autentikasi dan enkripsi.
- NetFlow mengumpulkan informasi lalu lintas IP berdasarkan flow (kombinasi tujuh atribut), diekspor ke collector untuk analisis pola trafik, top talkers, dan deteksi anomali.
- Interpretasi data monitoring memerlukan baseline sebagai acuan kondisi normal, dengan indikator kunci meliputi utilisasi interface, penghitung error, top talkers, dan anomali pola trafik.
- Kebijakan Penggunaan Jaringan (AUP) mengatur penggunaan sumber daya jaringan secara administratif, mencakup ruang lingkup, aktivitas yang diizinkan/dilarang, kuota, pemberitahuan monitoring, dan sanksi pelanggaran.
- Kontrol teknis (SNMP, NetFlow) dan kontrol administratif (AUP) saling melengkapi dalam tata kelola jaringan yang baik, dengan data monitoring menjadi alat verifikasi kepatuhan terhadap kebijakan yang telah disusun.

D. LATIHAN/SOAL

Petunjuk pengerjaan: Kerjakan seluruh soal berikut secara mandiri. Soal nomor 1–5 merupakan soal pemahaman konsep (jawaban singkat/uraian), soal nomor 6–7 merupakan soal konfigurasi, dan soal nomor 8–10 merupakan soal analisis/interpretasi data. Seluruh soal mengacu pada capaian Sub-CPMK 4.3.

1. Jelaskan tiga komponen utama arsitektur SNMP beserta fungsinya masing-masing.

2. Jelaskan perbedaan antara operasi GET, SET, dan TRAP pada SNMP.

3. Mengapa SNMPv3 lebih direkomendasikan dibandingkan SNMPv1/v2c untuk jaringan produksi?

4. Jelaskan konsep flow pada NetFlow dan tujuh atribut yang mengidentifikasinya.

5. Jelaskan konsep baseline dalam interpretasi data monitoring dan mengapa konsep ini penting untuk mendeteksi anomali.

6. Tuliskan perintah Cisco IOS untuk mengonfigurasi SNMPv3 dengan autentikasi SHA dan enkripsi AES pada sebuah user bernama monitor1 dalam group MONITORGROUP.

7. Tuliskan perintah Cisco IOS untuk mengaktifkan NetFlow ingress pada interface GigabitEthernet 0/1 dan mengekspor data ke collector 10.20.30.40 pada port 9996.

8. Data monitoring menunjukkan sebuah interface WAN memiliki utilisasi rata-rata 92% pada jam kerja selama satu bulan terakhir. Analisislah implikasi kondisi tersebut dan rekomendasikan tindakan yang perlu diambil.

9. Berdasarkan data NetFlow, ditemukan satu host yang menghasilkan trafik keluar sangat besar menuju satu alamat IP di luar negeri pada tengah malam, padahal host tersebut biasanya tidak aktif pada jam tersebut. Analisislah kemungkinan penyebab temuan ini dan langkah yang perlu diambil administrator.

10. Susunlah tiga poin utama yang wajib ada dalam kebijakan penggunaan jaringan (AUP) untuk laboratorium komputer kampus yang digunakan mahasiswa secara bergantian, disertai alasan masing-masing poin.

E. DAFTAR PUSTAKA

Stallings, W. (2023). Network security essentials: Applications and standards (7th ed.). Pearson.

Cisco Networking Academy. (2022). CCNP Enterprise: Core networking technologies (ENCOR) companion guide. Cisco Press.

Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 2 (2nd ed.). Cisco Press.

Froom, R., Frahim, E., & Sivasubramanian, B. (2021). Implementing Cisco IP switched networks (SWITCH) foundation learning guide (2nd ed.). Cisco Press.

F. TUGAS/STUDI KASUS

Tugas Praktik: Simulasi Monitoring dan Penyusunan Kebijakan Penggunaan Jaringan

Menggunakan simulator jaringan (Cisco Packet Tracer atau GNS3), lakukan konfigurasi monitoring pada topologi sederhana yang terdiri atas minimal satu router dan satu server monitoring, dengan ketentuan sebagai berikut.

1. Konfigurasikan SNMPv3 pada router dengan autentikasi dan enkripsi, lalu verifikasi menggunakan perintah show snmp user dan show snmp group.

2. Konfigurasikan NetFlow pada interface yang sesuai dan arahkan ekspor data ke server monitoring, lalu verifikasi menggunakan perintah show ip flow interface dan show ip cache flow (atau show flow monitor pada perangkat yang mendukung).

3. Berdasarkan data simulasi/contoh data monitoring yang diberikan oleh dosen pengampu, susunlah interpretasi tertulis mengenai kondisi jaringan tersebut (identifikasi minimal satu indikasi normal dan satu indikasi anomali, apabila ada).

4. Susunlah draf Kebijakan Penggunaan Jaringan (AUP) sederhana (1–2 halaman) untuk organisasi fiktif yang ditentukan dosen pengampu, mencakup seluruh komponen AUP yang telah dibahas pada Bab 13.

Laporan praktik (mencakup topologi, seluruh perintah konfigurasi, hasil verifikasi, interpretasi data monitoring, dan draf AUP) dikumpulkan dalam bentuk dokumen (PDF/Word) disertai file simulasi (.pkt/.gns3) sesuai tenggat waktu yang ditentukan dosen pengampu. Tugas ini dinilai menggunakan rubrik pada Rubrik Penilaian per Pertemuan 13 (aspek Tugas Praktik: Simulasi Monitoring & Kebijakan Penggunaan) sebagaimana tercantum pada Lampiran buku ajar ini.

BAB 14
PERANCANGAN DAN DOKUMENTASI TEKNIS JARINGAN ENTERPRISE

A. PENDAHULUAN

1. Deskripsi Singkat

Bab ini membuka rangkaian proyek kelompok (project-based learning) yang menjadi puncak pembelajaran mata kuliah Enterprise Networking, di mana mahasiswa secara berkelompok merancang jaringan enterprise yang lengkap untuk sebuah studi kasus organisasi, mengintegrasikan seluruh materi yang telah dipelajari sejak Bab 1 hingga Bab 13 — mulai dari model desain jaringan (Bab 2), VLAN dan switching (Bab 3–4), routing dinamis dan redundansi (Bab 5–6), konektivitas WAN dan VPN (Bab 7–10), hingga keamanan dan monitoring (Bab 11–13). Pembahasan pada bab ini berfokus pada bagaimana hasil rancangan tersebut didokumentasikan secara profesional sesuai standar dokumentasi teknis industri, mencakup diagram topologi, tabel pengalamatan IP, dan dokumentasi konfigurasi kunci.

Proyek yang dimulai pada bab ini akan dilanjutkan pada Bab 15, di mana mahasiswa akan mempresentasikan hasil rancangan yang telah didokumentasikan. Kedua bab ini secara bersama-sama menjadi wahana bagi mahasiswa untuk menunjukkan penguasaan menyeluruh atas seluruh capaian pembelajaran mata kuliah, sekaligus melatih keterampilan kerja tim dan komunikasi teknis yang menjadi bagian penting dari kompetensi lulusan D3 Teknik Komputer.

2. Capaian Pembelajaran Mata Kuliah (CPMK) yang Dicapai

Kode CPMK	:	CPMK-5
Rumusan CPMK	:	Mampu menyusun dokumentasi teknis rancangan jaringan enterprise dan mengomunikasikan hasil kerja tim secara profesional.
Bobot CPMK	:	14% dari keseluruhan capaian mata kuliah
CPL yang Didukung	:	CPL-5 (kemampuan merancang, menginstalasi, mengonfigurasi, dan memelihara jaringan komputer) dan CPL-9 (kemampuan bekerja sama dalam tim serta mengomunikasikan hasil kerja teknis secara lisan dan tertulis)

3. Sub-CPMK yang Dicapai

Kode Sub-CPMK	:	Sub-CPMK 5.1
Rumusan Sub-CPMK	:	Mampu menyusun dokumentasi teknis rancangan jaringan enterprise dalam kelompok kerja.
Pertemuan	:	Pertemuan ke-14
Indikator Penilaian	:	Kelengkapan dan kualitas dokumentasi teknis sesuai standar (dinilai melalui tugas proyek), bobot 3% dari total penilaian mata kuliah.

4. Tujuan Pembelajaran Khusus (TPK)

Setelah mempelajari bab ini secara tuntas, mahasiswa diharapkan mampu:

1. Menjelaskan standar dan komponen dokumentasi teknis jaringan yang lazim digunakan pada praktik industri.

2. Menyusun diagram topologi jaringan yang jelas, informatif, dan sesuai standar dokumentasi teknis.

3. Menyusun tabel pengalamatan IP (IP addressing table) dan dokumentasi konfigurasi kunci perangkat secara sistematis.

4. Merancang jaringan enterprise yang lengkap untuk studi kasus organisasi secara berkelompok, mengintegrasikan seluruh materi Bab 1 hingga Bab 13.

5. Menyusun dokumen rancangan jaringan enterprise yang lengkap dan sistematis sesuai standar dokumentasi teknis industri.

5. Peta Konsep

Alur pembahasan materi pada Bab 14 disajikan dalam peta konsep berikut, yang menggambarkan keterkaitan logis antar-subbab menuju pencapaian Sub-CPMK 5.1.

Standar Dokumentasi Teknis Industri → **Topologi, Pengalamatan, dan Konfigurasi Kunci** → **Proyek Kelompok Rancangan Jaringan**

6. Prasyarat

Bab ini bersifat integratif dan mensyaratkan penguasaan seluruh materi Bab 1 hingga Bab 13, karena proyek kelompok yang akan dikerjakan menggabungkan seluruh konsep dan keterampilan konfigurasi yang telah dipelajari sepanjang semester, mulai dari model desain jaringan, switching, routing, redundansi, WAN/VPN, hingga keamanan dan monitoring jaringan.

B. URAIAN MATERI

14.1 Standar Dokumentasi Teknis Industri

a. Penjelasan Konsep/Teori

Dokumentasi teknis jaringan adalah kumpulan dokumen yang mencatat secara sistematis rancangan, konfigurasi, dan kondisi suatu jaringan komputer, menjadi salah satu artefak terpenting dalam siklus hidup pengelolaan jaringan enterprise. Dokumentasi yang baik memberikan manfaat signifikan, antara lain memudahkan proses troubleshooting karena tim teknis dapat merujuk pada kondisi jaringan yang seharusnya (baseline desain), mempercepat proses onboarding staf baru, menjadi bahan audit kepatuhan (compliance), serta menjadi acuan penting dalam proses pemulihan bencana (disaster recovery) apabila terjadi kegagalan besar pada infrastruktur.

Dokumentasi rancangan jaringan enterprise pada praktik industri umumnya mencakup komponen-komponen berikut.

- Ringkasan Eksekutif (Executive Summary) — gambaran umum proyek, tujuan, dan ruang lingkup rancangan, ditulis dengan bahasa yang dapat dipahami baik oleh pihak teknis maupun manajemen non-teknis.
- Diagram Topologi Jaringan — representasi visual struktur jaringan, baik topologi fisik (physical topology, menunjukkan kabel dan lokasi perangkat sesungguhnya) maupun topologi logis (logical topology, menunjukkan alur data dan segmentasi VLAN/subnet tanpa memperhatikan detail fisik).
- Skema Pengalamatan IP (IP Addressing Table) — daftar rinci alokasi alamat IP, subnet, dan VLAN pada seluruh perangkat dan interface dalam jaringan.
- Inventaris Perangkat (Device Inventory) — daftar seluruh perangkat jaringan beserta informasi model, versi perangkat lunak (firmware/IOS), dan lokasi fisik penempatan.
- Dokumentasi Konfigurasi Kunci — ringkasan konfigurasi penting pada setiap perangkat (bukan seluruh running-config secara mentah), disertai penjelasan tujuan setiap bagian konfigurasi.
- Ringkasan Kebijakan Keamanan — rangkuman kebijakan ACL, firewall, dan segmentasi yang diterapkan (mengacu pada Bab 11 dan Bab 12).
- Hasil Pengujian dan Validasi — bukti bahwa rancangan telah diuji dan berfungsi sesuai kebutuhan, termasuk hasil pengujian konektivitas dan skenario redundansi.
- Lampiran — konfigurasi lengkap (running-config) setiap perangkat serta catatan perubahan (change log) apabila terdapat revisi selama proses perancangan.

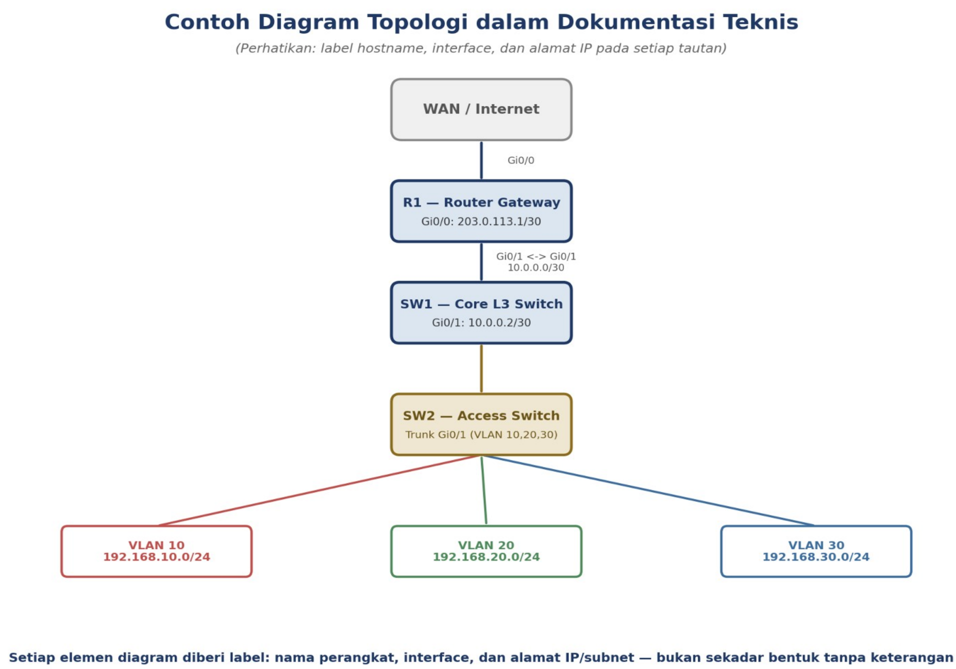
b. Contoh Aplikasi

Sebuah perusahaan konsultan jaringan yang menyelesaikan proyek instalasi jaringan baru bagi kliennya wajib menyerahkan dokumentasi lengkap sebagaimana diuraikan di atas sebagai bagian dari serah terima proyek (project handover), sehingga tim IT internal klien dapat memahami dan mengelola jaringan tersebut secara mandiri di kemudian hari tanpa harus selalu bergantung pada konsultan yang membangunnya.

14.2 Topologi, Pengalamatan, dan Konfigurasi Kunci

a. Penjelasan Konsep/Teori

Diagram topologi yang baik harus memenuhi beberapa kaidah penting agar benar-benar informatif dan dapat digunakan sebagai referensi teknis, bukan sekadar ilustrasi. Setiap perangkat pada diagram harus diberi label nama (hostname) yang jelas dan konsisten dengan konfigurasi sesungguhnya; setiap tautan (link) antar-perangkat harus diberi label nama interface pada kedua ujungnya beserta alamat IP atau subnet yang digunakan; serta penggunaan simbol/ikon standar (router, switch, firewall, server) agar mudah dipahami oleh pembaca yang familier dengan notasi jaringan pada umumnya.



Gambar 14.1 Contoh Diagram Topologi dalam Dokumentasi Teknis

Diagram di atas menunjukkan contoh praktik terbaik penyusunan diagram topologi untuk dokumentasi teknis. Setiap perangkat diberi label hostname yang jelas (R1, SW1, SW2), setiap tautan diberi label nama interface dan alamat IP/subnet yang relevan (misalnya Gi0/1 dengan subnet 10.0.0.0/30 antara SW1 dan R1), serta setiap segmen VLAN pada bagian akses diberi keterangan VLAN ID dan subnet yang *digunakan. Diagram semacam ini jauh lebih bernilai sebagai dokumentasi dibandingkan diagram yang hanya menampilkan bentuk perangkat tanpa keterangan detail teknis.*

Selain diagram topologi, tabel pengalamatan IP (IP addressing table) merupakan komponen dokumentasi yang sama pentingnya, mencatat secara rinci alokasi alamat IP pada setiap interface perangkat. Contoh tabel pengalamatan IP untuk topologi pada Gambar 14.1 ditunjukkan pada Tabel 14.1 berikut.

Perangkat	Interface	Alamat IP	VLAN/Keterangan
R1	GigabitEthernet 0/0	203.0.113.1/30	Uplink ke WAN/Internet
R1	GigabitEthernet 0/1	10.0.0.1/30	Uplink ke SW1 (Core)
SW1	GigabitEthernet 0/1	10.0.0.2/30	Uplink ke R1
SW1	VLAN 10 (SVI)	192.168.10.1/24	Gateway VLAN Keuangan
SW1	VLAN 20 (SVI)	192.168.20.1/24	Gateway VLAN Operasional
SW1	VLAN 30 (SVI)	192.168.30.1/24	Gateway VLAN SDM
SW2	GigabitEthernet 0/1	Trunk (no IP)	Trunk 802.1Q ke SW1 (VLAN 10,20,30)

Tabel 14.1 Contoh Tabel Pengalamatan IP (IP Addressing Table)

Dokumentasi konfigurasi kunci tidak dimaksudkan untuk menyalin seluruh running-config secara mentah ke dalam dokumen utama (yang sebaiknya ditempatkan pada bagian lampiran), melainkan merangkum bagian-bagian konfigurasi yang paling penting untuk dipahami pembaca, seperti skema VLAN dan trunking (Bab 3), protokol routing yang digunakan beserta area OSPF (Bab 5), protokol redundansi gateway yang diterapkan (Bab 6), serta ringkasan kebijakan ACL dan firewall (Bab 11–12), masing-masing disertai penjelasan singkat mengenai tujuan dan cara kerjanya.

b. Contoh Aplikasi

Ketika terjadi gangguan pada jaringan di tengah malam, teknisi yang bertugas jaga (on-call) dapat merujuk pada diagram topologi dan tabel pengalamatan IP yang terdokumentasi dengan baik untuk dengan cepat memahami struktur jaringan dan mengidentifikasi sumber masalah, tanpa harus menunggu kehadiran administrator senior yang lebih memahami jaringan tersebut secara mendalam.

14.3 Proyek Kelompok Rancangan Jaringan

a. Penjelasan Konsep/Teori

Proyek kelompok pada bab ini dilaksanakan melalui beberapa tahapan yang mencerminkan siklus perancangan jaringan pada praktik industri sesungguhnya.

- Pembentukan Kelompok dan Penerimaan Studi Kasus — mahasiswa dibagi ke dalam kelompok kerja (3–5 orang) dan menerima studi kasus organisasi dari dosen pengampu, mencakup profil organisasi, jumlah lokasi, jumlah pengguna, serta kebutuhan bisnis yang relevan.
- Analisis Kebutuhan — kelompok menganalisis kebutuhan organisasi tersebut mengacu pada karakteristik jaringan enterprise (Bab 1) dan menentukan model desain yang sesuai (Bab 2).
- Perancangan Teknis — kelompok merancang skema VLAN (Bab 3), topologi switching dan routing (Bab 4–5), strategi redundansi (Bab 6), konektivitas WAN/VPN antar-lokasi apabila relevan (Bab 7–10), serta kebijakan keamanan dan monitoring (Bab 11–13).
- Implementasi dan Pengujian — kelompok mengimplementasikan rancangan pada simulator jaringan (Packet Tracer/GNS3) dan melakukan pengujian menyeluruh untuk memastikan seluruh kebutuhan terpenuhi.
- Penyusunan Dokumentasi — kelompok menyusun dokumen rancangan jaringan lengkap sesuai standar yang telah dibahas pada Sub-bab 14.1 dan 14.2, sebagai luaran (deliverable) utama Pertemuan 14.

Dokumen rancangan yang telah disusun pada bab ini akan menjadi dasar bagi kelompok untuk mempersiapkan presentasi hasil rancangan pada Bab 15, di mana setiap kelompok akan mempertanggungjawabkan rancangan yang telah dibuat di hadapan dosen dan kelompok lain.

b. Contoh Aplikasi

Sebagai ilustrasi proses kerja kelompok, dosen pengampu dapat memberikan studi kasus seperti "sebuah klinik kesehatan dengan satu lokasi utama dan dua cabang kecil yang memerlukan sistem rekam medis terpusat", kemudian setiap kelompok merancang solusi lengkap mulai dari model desain, skema VLAN per unit layanan klinik, hingga strategi konektivitas WAN antar-lokasi, seluruhnya didokumentasikan sesuai standar yang telah dipelajari.

C. RANGKUMAN

- Dokumentasi teknis jaringan penting untuk memudahkan troubleshooting, onboarding staf baru, audit kepatuhan, dan pemulihan bencana, serta menjadi artefak wajib dalam siklus hidup pengelolaan jaringan enterprise.
- Komponen dokumentasi teknis standar meliputi ringkasan eksekutif, diagram topologi, tabel pengalamatan IP, inventaris perangkat, dokumentasi konfigurasi kunci, ringkasan kebijakan keamanan, hasil pengujian, dan lampiran konfigurasi lengkap.
- Diagram topologi yang baik memberi label hostname, nama interface, dan alamat IP/subnet pada setiap elemen, menggunakan simbol standar agar mudah dipahami.
- Tabel pengalamatan IP mencatat secara rinci alokasi alamat pada setiap interface perangkat, menjadi referensi penting yang saling melengkapi dengan diagram topologi.
- Proyek kelompok rancangan jaringan mencakup lima tahapan: pembentukan kelompok dan penerimaan studi kasus, analisis kebutuhan, perancangan teknis, implementasi dan pengujian, serta penyusunan dokumentasi, mengintegrasikan seluruh materi Bab 1 hingga Bab 13.

D. LATIHAN/SOAL

Petunjuk pengerjaan: Kerjakan seluruh soal berikut secara mandiri sebagai persiapan sebelum mengerjakan proyek kelompok. Soal nomor 1–6 merupakan soal pemahaman konsep (jawaban singkat/uraian), sedangkan soal nomor 7–10 merupakan latihan praktik penyusunan dokumentasi. Seluruh soal mengacu pada capaian Sub-CPMK 5.1.

1. Jelaskan minimal empat manfaat dokumentasi teknis jaringan bagi organisasi.

2. Sebutkan dan jelaskan delapan komponen utama dokumentasi rancangan jaringan enterprise.

3. Jelaskan perbedaan antara topologi fisik dan topologi logis dalam diagram jaringan.

4. Jelaskan mengapa seluruh running-config perangkat sebaiknya ditempatkan pada bagian lampiran, bukan pada badan utama dokumen.

5. Jelaskan informasi minimal apa saja yang harus tercantum pada tabel pengalamatan IP.

6. Sebutkan lima tahapan proses kerja proyek kelompok rancangan jaringan sebagaimana dibahas pada bab ini.

7. Perbaikilah diagram topologi sederhana yang diberikan dosen pengampu (tanpa label) dengan menambahkan label hostname, interface, dan alamat IP yang sesuai standar dokumentasi teknis.

8. Susunlah tabel pengalamatan IP untuk sebuah topologi kecil yang terdiri atas satu router dan satu switch dengan dua VLAN, sesuai format Tabel 14.1.

9. Susunlah ringkasan eksekutif (executive summary) sepanjang satu paragraf untuk sebuah proyek fiktif perancangan jaringan kantor cabang baru.

10. Identifikasi dan jelaskan minimal tiga elemen konfigurasi kunci yang perlu didokumentasikan (bukan seluruh running-config) untuk sebuah Layer 3 switch yang menjalankan VLAN, OSPF, dan HSRP.

E. DAFTAR PUSTAKA

Cisco Networking Academy. (2022). CCNP Enterprise: Core networking technologies (ENCOR) companion guide. Cisco Press.

Froom, R., Frahim, E., & Sivasubramanian, B. (2021). Implementing Cisco IP switched networks (SWITCH) foundation learning guide (2nd ed.). Cisco Press.

Teare, D., & Paquet, C. (2022). Implementing Cisco IP routing (ROUTE) foundation learning guide (2nd ed.). Cisco Press.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 1 (2nd ed.). Cisco Press.

Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson.

F. TUGAS/STUDI KASUS

Tugas Proyek Kelompok: Dokumentasi Rancangan Jaringan Enterprise

Bentuklah kelompok kerja (3–5 mahasiswa). Dosen pengampu akan memberikan satu studi kasus organisasi kepada setiap kelompok (mencakup profil organisasi, jumlah lokasi, jumlah pengguna, dan kebutuhan bisnis yang relevan). Setiap kelompok wajib menyusun dokumen rancangan jaringan enterprise lengkap yang memuat komponen-komponen berikut.

1. Ringkasan eksekutif yang menjelaskan profil organisasi dan tujuan rancangan jaringan.

2. Diagram topologi jaringan (fisik dan/atau logis) yang lengkap dengan label hostname, interface, dan alamat IP, sesuai standar yang dicontohkan pada Gambar 14.1.

3. Tabel pengalamatan IP (IP addressing table) yang mencakup seluruh perangkat dan interface dalam rancangan, sesuai format Tabel 14.1.

4. Dokumentasi konfigurasi kunci yang mencakup skema VLAN, protokol routing (beserta desain area apabila menggunakan OSPF multi-area), strategi redundansi gateway, strategi konektivitas WAN/VPN (apabila relevan dengan studi kasus), serta ringkasan kebijakan ACL dan firewall yang diterapkan.

5. Bukti implementasi dan pengujian pada simulator jaringan (Packet Tracer/GNS3), berupa tangkapan layar konfigurasi kunci dan hasil pengujian konektivitas.

6. Lampiran berupa konfigurasi lengkap (running-config) seluruh perangkat dalam rancangan.

Dokumen rancangan (dalam format PDF/Word, minimal 10 halaman tidak termasuk lampiran) beserta file simulasi (.pkt/.gns3) dikumpulkan sesuai tenggat waktu yang ditentukan dosen pengampu. Dokumen ini akan menjadi dasar presentasi kelompok pada Bab 15 (Pertemuan 15). Tugas ini dinilai menggunakan rubrik pada Rubrik Penilaian per Pertemuan 14 (aspek Tugas Proyek: Dokumentasi Rancangan Jaringan Enterprise) sebagaimana tercantum pada Lampiran buku ajar ini.

BAB 15
PRESENTASI HASIL RANCANGAN DAN JALUR SERTIFIKASI PROFESI

A. PENDAHULUAN

1. Deskripsi Singkat

Bab ini menjadi penutup rangkaian proyek kelompok yang telah dimulai pada Bab 14, berfokus pada teknik mempresentasikan hasil rancangan jaringan enterprise secara profesional dan mempertanggungjawabkan keputusan desain yang telah diambil di hadapan dosen dan kelompok lain. Selain itu, bab ini juga memperkenalkan jalur sertifikasi profesi di bidang jaringan enterprise, khususnya CCNA dan CCNP ENCOR, sebagai bagian dari kesadaran mahasiswa terhadap pentingnya pembelajaran sepanjang hayat (lifelong learning) dalam mengikuti perkembangan teknologi jaringan yang terus berubah.

Bab ini secara unik mendukung dua CPMK sekaligus, yaitu CPMK-5 (dokumentasi dan komunikasi hasil kerja) dan CPMK-6 (pengembangan kompetensi berkelanjutan), sekaligus menjadi penutup seluruh rangkaian materi mata kuliah Enterprise Networking sebelum mahasiswa menghadapi Ujian Akhir Semester pada Pertemuan 16.

2. Capaian Pembelajaran Mata Kuliah (CPMK) yang Dicapai

Kode CPMK	:	CPMK-5
Rumusan CPMK	:	Mampu menyusun dokumentasi teknis rancangan jaringan enterprise dan mengomunikasikan hasil kerja tim secara profesional.
Bobot CPMK	:	14% dari keseluruhan capaian mata kuliah

Kode CPMK	:	CPMK-6
Rumusan CPMK	:	Mampu mengidentifikasi jalur pengembangan kompetensi dan sertifikasi profesi di bidang jaringan enterprise sebagai bagian pembelajaran sepanjang hayat.
Bobot CPMK	:	1% dari keseluruhan capaian mata kuliah
CPL yang Didukung	:	CPL-9 (kemampuan mengomunikasikan hasil kerja teknis secara lisan dan tertulis) dan CPL-10 (pengembangan diri berkelanjutan melalui pembelajaran mandiri dan sertifikasi kompetensi)

3. Sub-CPMK yang Dicapai

Kode Sub-CPMK	:	Sub-CPMK 5.2
Rumusan Sub-CPMK	:	Mampu mempresentasikan hasil rancangan jaringan secara profesional dan mempertanggungjawabkannya.
Pertemuan	:	Pertemuan ke-15
Indikator Penilaian	:	Kualitas presentasi dan kemampuan menjawab pertanyaan (unjuk kerja), bobot 2% dari total penilaian mata kuliah.

Kode Sub-CPMK	:	Sub-CPMK 6.1
Rumusan Sub-CPMK	:	Mampu mengidentifikasi jalur sertifikasi profesi jaringan enterprise (CCNA/CCNP ENCOR) sebagai bagian pembelajaran berkelanjutan.
Pertemuan	:	Pertemuan ke-15
Indikator Penilaian	:	Pemahaman jalur sertifikasi (dinilai melalui partisipasi diskusi), bobot 1% dari total penilaian mata kuliah.

4. Tujuan Pembelajaran Khusus (TPK)

Setelah mempelajari bab ini secara tuntas, mahasiswa diharapkan mampu:

1. Menjelaskan teknik presentasi hasil kerja teknis yang efektif, sistematis, dan profesional.

2. Mempresentasikan hasil rancangan jaringan kelompok secara meyakinkan di hadapan audiens teknis maupun non-teknis.

3. Menjawab pertanyaan terkait rancangan jaringan dengan tepat serta mempertanggungjawabkan setiap keputusan desain yang telah diambil.

4. Menjelaskan struktur dan cakupan jalur sertifikasi profesi CCNA dan CCNP ENCOR pada jenjang karier bidang jaringan.

5. Menyusun rencana pengembangan kompetensi pribadi di bidang jaringan enterprise sebagai bagian dari pembelajaran sepanjang hayat.

5. Peta Konsep

Alur pembahasan materi pada Bab 15 disajikan dalam peta konsep berikut, yang menggambarkan keterkaitan logis antar-subbab menuju pencapaian Sub-CPMK 5.2 dan Sub-CPMK 6.1.

Teknik Presentasi Hasil Kerja Teknis → **Jalur Sertifikasi CCNA/CCNP ENCOR** → **Pengembangan Kompetensi Berkelanjutan**

6. Prasyarat

Sebelum mempelajari bab ini, mahasiswa wajib telah menyelesaikan dokumen rancangan jaringan kelompok pada Bab 14, karena dokumen tersebut menjadi bahan utama presentasi yang akan disampaikan pada pertemuan ini.

B. URAIAN MATERI

15.1 Teknik Presentasi Hasil Kerja Teknis

a. Penjelasan Konsep/Teori

Kemampuan mempresentasikan hasil kerja teknis secara efektif merupakan keterampilan penting yang melengkapi kompetensi teknis seorang praktisi jaringan, sebagaimana dituntut oleh CPL-9 Program Studi. Presentasi teknis yang baik bukan sekadar membacakan isi dokumen, melainkan mengomunikasikan inti permasalahan, solusi yang dirancang, dan bukti bahwa solusi tersebut berhasil, dengan cara yang mudah dipahami audiens.

Beberapa prinsip utama dalam menyusun dan menyampaikan presentasi teknis yang efektif adalah sebagai berikut.

- Struktur yang Sistematis — presentasi sebaiknya mengikuti alur yang jelas: pengantar profil organisasi dan permasalahan/kebutuhan, penjelasan rancangan solusi (model desain, skema VLAN, strategi redundansi, dan sebagainya), bukti implementasi dan pengujian, serta simpulan dan pembelajaran yang diperoleh.
- Kesadaran terhadap Audiens — materi disesuaikan dengan latar belakang pendengar; penjelasan kepada dosen dan sesama mahasiswa teknik komputer dapat menggunakan istilah teknis secara langsung, namun tetap perlu menjelaskan alasan di balik setiap keputusan desain, bukan hanya "apa" yang dilakukan tetapi juga "mengapa".
- Visualisasi yang Efektif — memanfaatkan diagram topologi dan tabel (sebagaimana telah disusun pada Bab 14) sebagai alat bantu visual utama, menghindari slide yang dipenuhi teks panjang yang justru mengalihkan perhatian audiens dari penjelasan lisan presenter.
- Manajemen Waktu — melatih presentasi sebelumnya untuk memastikan seluruh poin penting tersampaikan dalam alokasi waktu yang diberikan, tanpa terburu-buru pada bagian akhir maupun menghabiskan waktu berlebihan pada bagian awal.
- Kesiapan Menjawab Pertanyaan — mempersiapkan diri untuk pertanyaan mengenai alasan pemilihan setiap keputusan desain (misalnya mengapa memilih OSPF dibandingkan protokol routing lain, atau mengapa memilih topologi hierarchical dibandingkan spine-leaf), dengan sikap mendengarkan pertanyaan secara utuh sebelum menjawab, serta jujur mengakui apabila terdapat aspek yang belum sepenuhnya dikuasai kelompok, disertai kesediaan untuk menindaklanjutinya.

Kesalahan Umum dalam Presentasi Teknis

Beberapa kesalahan yang sering ditemui pada presentasi teknis mahasiswa antara lain: menampilkan slide yang berisi paragraf panjang dan dibacakan kata per kata tanpa penjelasan tambahan; tidak melakukan latihan (rehearsal) sebelumnya sehingga alur penjelasan menjadi tidak runtut; hanya menampilkan hasil akhir tanpa menjelaskan proses pengambilan keputusan desain; serta bersikap defensif atau menghindar ketika menerima pertanyaan kritis, alih-alih menerimanya sebagai kesempatan untuk memperjelas dan memperkuat argumentasi rancangan.

b. Contoh Aplikasi

Sebuah tim insinyur jaringan yang mempresentasikan proposal migrasi infrastruktur kepada manajemen perusahaan perlu menyusun narasi yang menghubungkan keputusan teknis (misalnya migrasi ke SD-WAN) dengan manfaat bisnis yang dapat dipahami manajemen (efisiensi biaya, peningkatan kelincahan operasional), bukan hanya menjelaskan aspek teknis semata.

15.2 Jalur Sertifikasi CCNA dan CCNP ENCOR

a. Penjelasan Konsep/Teori

Sertifikasi profesi merupakan salah satu bentuk pengakuan industri terhadap kompetensi teknis seseorang di bidang jaringan komputer, dan menjadi salah satu jalur pengembangan karier yang diakui secara luas, khususnya pada ekosistem perangkat Cisco yang menjadi acuan utama pada mata kuliah ini. Jenjang sertifikasi profesi Cisco (Cisco Career Certifications) tersusun secara hierarkis dari tingkat dasar hingga tingkat ahli, sebagaimana digambarkan pada Gambar 15.1.

Gambar 15.1 Jalur Sertifikasi Profesi Jaringan (Cisco Career Certification)

Diagram di atas menggambarkan lima jenjang sertifikasi profesi Cisco secara berurutan: Entry (CCT, dasar troubleshooting), Associate (CCNA 200-301, fondasi jaringan), Professional (CCNP Enterprise, terdiri atas ujian inti ENCOR ditambah satu ujian konsentrasi), Expert (CCIE Enterprise, disertai ujian laboratorium praktik), dan Architect (CCAr, arsitektur jaringan skala perusahaan besar). Materi yang dibahas sepanjang buku ajar ini — mulai dari model desain jaringan, VLAN dan switching, routing dinamis OSPF, redundansi gateway, hingga WAN, VPN, SD-WAN, dan keamanan jaringan — selaras erat dengan cakupan topik inti ujian ENCOR (350-401) pada jenjang Professional.

Dua sertifikasi yang paling relevan untuk dipahami mahasiswa pada tahap ini adalah sebagai berikut.

- CCNA (Cisco Certified Network Associate) — sertifikasi jenjang associate dengan ujian tunggal (200-301), tidak memerlukan prasyarat sertifikasi sebelumnya, mencakup dasar-dasar jaringan (networking fundamentals), konektivitas IP, layanan IP, fundamental keamanan jaringan, serta pengenalan otomasi dan programmability. CCNA menjadi pijakan awal yang solid bagi siapa pun yang ingin membangun karier di bidang jaringan.
- CCNP Enterprise (Cisco Certified Network Professional) — sertifikasi jenjang professional yang mensyaratkan kelulusan pada ujian inti ENCOR (Implementing Cisco Enterprise Network Core Technologies, kode ujian 350-401) ditambah satu ujian konsentrasi sesuai spesialisasi yang diminati (misalnya SD-WAN, wireless, atau automation). Ujian ENCOR mencakup topik routing dan switching lanjut, arsitektur jaringan enterprise, teknologi WAN dan virtualisasi, keamanan jaringan, serta otomasi jaringan — topik yang sangat beririsan dengan keseluruhan materi yang telah dipelajari pada buku ajar ini.

Perbandingan karakteristik kedua sertifikasi tersebut dirangkum pada Tabel 15.1 berikut.

Aspek	CCNA	CCNP Enterprise
Jenjang	Associate	Professional
Kode Ujian	200-301 (satu ujian)	350-401 ENCOR + satu ujian konsentrasi
Prasyarat	Tidak ada	Tidak ada prasyarat formal, namun disarankan menguasai materi setara CCNA
Cakupan Utama	Fondasi jaringan, IP dasar, keamanan dasar	Routing/switching lanjut, WAN, keamanan, otomasi jaringan enterprise
Keterkaitan dengan Buku Ajar Ini	Sebagian besar tercakup pada mata kuliah jaringan dasar	Sangat beririsan dengan seluruh Bab 1 –14 buku ajar ini

Tabel 15.1 Perbandingan Sertifikasi CCNA dan CCNP Enterprise (ENCOR)

b. Contoh Aplikasi

Seorang lulusan D3 Teknik Komputer yang telah menguasai materi mata kuliah Enterprise Networking secara tuntas memiliki modal pengetahuan yang kuat untuk mempersiapkan diri mengikuti ujian sertifikasi CCNA terlebih dahulu sebagai langkah awal, sebelum melanjutkan ke persiapan ujian ENCOR pada jenjang CCNP Enterprise seiring bertambahnya pengalaman kerja di bidang jaringan.

15.3 Pengembangan Kompetensi Berkelanjutan

a. Penjelasan Konsep/Teori

Bidang jaringan komputer merupakan salah satu bidang teknologi yang berkembang sangat cepat, sebagaimana tercermin dari kemunculan teknologi SD-WAN dan konektivitas cloud yang telah dibahas pada Bab 10, yang bahkan belum menjadi topik umum satu dekade lalu. Oleh karena itu, kesadaran akan pentingnya pembelajaran sepanjang hayat (lifelong learning) menjadi kompetensi yang tidak kalah penting dibandingkan penguasaan teknis itu sendiri, sejalan dengan CPL-10 Program Studi D3 Teknik Komputer.

Selain jalur sertifikasi Cisco yang telah dibahas, terdapat berbagai jalur pengembangan kompetensi lain yang dapat dipertimbangkan mahasiswa sesuai minat dan kebutuhan kariernya.

- Sertifikasi Vendor Lain — vendor perangkat jaringan lain seperti Juniper (JNCIA/JNCIP), Huawei (HCIA/HCIP), atau Fortinet (NSE) menawarkan jalur sertifikasi serupa yang relevan bergantung pada ekosistem perangkat yang digunakan di tempat kerja.

- Sertifikasi Netral-Vendor — sertifikasi seperti CompTIA Network+ memberikan pengakuan kompetensi jaringan yang tidak terikat pada satu vendor tertentu, cocok sebagai fondasi awal yang lebih umum.
- Sertifikasi Cloud Networking — seiring meningkatnya adopsi konektivitas cloud (Bab 10), sertifikasi seperti AWS Certified Advanced Networking atau Azure Network Engineer Associate menjadi semakin relevan bagi praktisi jaringan yang bekerja pada organisasi dengan infrastruktur berbasis cloud.
- Praktik Mandiri (Hands-on Labs) — mempraktikkan konfigurasi secara mandiri menggunakan simulator (Packet Tracer, GNS3) atau perangkat fisik bekas (lab kit) di luar tugas perkuliahan, untuk memperdalam pemahaman praktis secara berkelanjutan.
- Komunitas dan Sumber Belajar — bergabung dengan komunitas profesional jaringan, mengikuti forum diskusi teknis, serta membaca dokumentasi dan pembaruan teknologi terbaru dari vendor maupun badan standar (seperti IETF) untuk tetap mengikuti perkembangan industri.

b. Contoh Aplikasi

Seorang mahasiswa yang tertarik pada bidang keamanan jaringan (setelah mempelajari Bab 11–13) dapat merencanakan jalur pengembangan kompetensi lanjutan menuju sertifikasi keamanan siber seperti CompTIA Security+ atau Cisco CyberOps Associate, melengkapi fondasi jaringan yang telah dikuasai dengan spesialisasi keamanan yang lebih mendalam.

C. RANGKUMAN

- Presentasi teknis yang efektif memerlukan struktur sistematis, kesadaran audiens, visualisasi yang tepat, manajemen waktu, dan kesiapan menjawab pertanyaan secara jujur dan bertanggung jawab.
- Jenjang sertifikasi profesi Cisco tersusun dari Entry (CCT), Associate (CCNA), Professional (CCNP), Expert (CCIE), hingga Architect (CCAr).
- CCNA (200-301) adalah sertifikasi fondasi tanpa prasyarat yang mencakup dasar-dasar jaringan, sedangkan CCNP Enterprise mensyaratkan kelulusan ujian ENCOR (350-401) yang cakupannya sangat beririsan dengan materi buku ajar ini.
- Pembelajaran sepanjang hayat penting mengingat pesatnya perkembangan teknologi jaringan, dengan jalur pengembangan yang dapat ditempuh melalui sertifikasi vendor lain, sertifikasi netral-vendor, sertifikasi cloud networking, praktik mandiri, dan keterlibatan dalam komunitas profesional.
- Bab ini menutup rangkaian materi mata kuliah Enterprise Networking, mengintegrasikan kemampuan teknis (Bab 1–14) dengan keterampilan komunikasi profesional dan kesadaran pengembangan karier berkelanjutan.

D. LATIHAN/SOAL

Petunjuk pengerjaan: Kerjakan seluruh soal berikut secara mandiri. Soal nomor 1–6 merupakan soal pemahaman konsep (jawaban singkat/uraian), sedangkan soal nomor 7–10 merupakan soal reflektif/perencanaan yang berkaitan dengan pengembangan diri. Seluruh soal mengacu pada capaian Sub-CPMK 5.2 dan Sub-CPMK 6.1.

1. Jelaskan struktur sistematis yang sebaiknya digunakan dalam menyusun presentasi hasil rancangan jaringan.

2. Jelaskan mengapa presenter perlu menjelaskan alasan ("mengapa") di balik setiap keputusan desain, tidak hanya "apa" yang dirancang.

3. Sebutkan minimal tiga kesalahan umum yang sering terjadi dalam presentasi teknis.

4. Jelaskan lima jenjang sertifikasi profesi Cisco secara berurutan dari tingkat dasar hingga tingkat ahli.

5. Jelaskan perbedaan cakupan ujian CCNA (200-301) dan ujian ENCOR (350-401) pada jenjang CCNP Enterprise.

6. Jelaskan mengapa pembelajaran sepanjang hayat menjadi penting khususnya di bidang jaringan komputer.

7. Identifikasi minimal dua topik pada buku ajar ini yang menurut Anda paling erat kaitannya dengan cakupan ujian ENCOR, disertai penjelasan singkat.

8. Susunlah rencana pengembangan kompetensi pribadi (personal development plan) sepanjang satu paragraf, mencakup sertifikasi atau jalur pembelajaran yang ingin Anda tempuh dalam dua tahun ke depan beserta alasannya.

9. Pilihlah salah satu jalur sertifikasi selain CCNA/CCNP (dapat berupa sertifikasi vendor lain, netral-vendor, atau cloud networking) yang menarik minat Anda, lalu jelaskan relevansinya dengan rencana karier Anda.

10. Refleksikan pengalaman Anda mengerjakan proyek kelompok pada Bab 14–15: sebutkan satu keterampilan teknis dan satu keterampilan non-teknis (soft skill) yang paling berkembang selama proses tersebut.

E. DAFTAR PUSTAKA

Cisco Networking Academy. (2022). CCNP Enterprise: Core networking technologies (ENCOR) companion guide. Cisco Press.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 1 (2nd ed.). Cisco Press.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 2 (2nd ed.). Cisco Press.

Teare, D., & Paquet, C. (2022). Implementing Cisco IP routing (ROUTE) foundation learning guide (2nd ed.). Cisco Press.

Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson.

F. TUGAS/STUDI KASUS

Tugas 1 (Unjuk Kerja Kelompok): Presentasi Hasil Rancangan Jaringan

Setiap kelompok mempresentasikan dokumen rancangan jaringan enterprise yang telah disusun pada Bab 14 di hadapan dosen pengampu dan kelompok lain, dengan ketentuan sebagai berikut.

1. Durasi presentasi 10–15 menit per kelompok, dilanjutkan sesi tanya-jawab selama 5–10 menit.

2. Presentasi mencakup: profil singkat studi kasus organisasi, ringkasan rancangan (model desain, skema VLAN, strategi routing dan redundansi, konektivitas WAN/VPN apabila relevan, kebijakan keamanan), demonstrasi/bukti hasil pengujian, serta simpulan dan pembelajaran yang diperoleh kelompok.

3. Seluruh anggota kelompok wajib berperan aktif dalam presentasi maupun sesi tanya-jawab.

4. Gunakan diagram topologi dan tabel pengalamatan IP dari dokumen Bab 14 sebagai alat bantu visual utama, hindari slide dengan teks yang terlalu padat.

Presentasi dinilai menggunakan rubrik pada Rubrik Penilaian per Pertemuan 15 (aspek Presentasi Kelompok: Hasil Rancangan Jaringan, bobot 2%) sebagaimana tercantum pada Lampiran buku ajar ini.

Tugas 2 (Individu): Refleksi Jalur Pengembangan Karier

Setiap mahasiswa secara individu menyusun tulisan singkat (setengah hingga satu halaman) yang memuat:

1. Identifikasi jalur sertifikasi profesi (CCNA/CCNP ENCOR atau jalur lain yang relevan) yang ingin ditempuh setelah menyelesaikan mata kuliah ini.

2. Alasan pemilihan jalur tersebut dikaitkan dengan minat dan rencana karier pribadi.

3. Langkah konkret yang akan diambil dalam satu tahun ke depan untuk mendukung pencapaian jalur tersebut (misalnya mengikuti pelatihan, praktik mandiri, atau mengikuti ujian sertifikasi).

Tulisan reflektif ini menjadi bahan diskusi kelas mengenai jalur pengembangan karier dan dinilai menggunakan rubrik pada Rubrik Penilaian per Pertemuan 15 (aspek Partisipasi

Diskusi: Diskusi Jalur Pengembangan Karier/Sertifikasi, bobot 1%) sebagaimana tercantum pada Lampiran buku ajar ini.

BAB 16
EVALUASI AKHIR SEMESTER

(Rangkuman dan Kisi-Kisi Materi Bab 9–15, Terintegrasi dengan Bab 1–8)

A. PENGANTAR EVALUASI AKHIR SEMESTER

Ujian Akhir Semester (UAS) dilaksanakan pada Pertemuan ke-16 dan mencakup materi Pertemuan 9 hingga 15, sekaligus menguji integrasi keseluruhan materi mata kuliah Enterprise Networking dari awal semester. Berbeda dengan UTS yang berfokus pada konsep, model desain, dan switching dasar, UAS menekankan pada konektivitas WAN/VPN/SD-WAN, keamanan dan tata kelola jaringan (ACL, firewall, monitoring), serta kemampuan integratif dalam dokumentasi rancangan dan kesadaran pengembangan profesi. UAS dilaksanakan dalam bentuk ujian tertulis dan/atau praktik disertai studi kasus komprehensif, dengan bobot 30% dari keseluruhan nilai akhir mata kuliah.

Bab ini disusun sebagai panduan persiapan UAS bagi mahasiswa, berisi rangkuman komprehensif seluruh materi Bab 9–15, peta keterkaitan antar-bab yang menghubungkannya dengan fondasi Bab 1–8, kisi-kisi soal, contoh latihan soal simulasi, serta rubrik penilaian yang akan digunakan.

Cakupan CPMK dan Sub-CPMK yang Diujikan

CPMK	Sub-CPMK yang Diujikan	Bab Terkait
CPMK-3	Sub-CPMK 3.2, Sub-CPMK 3.3 (kelanjutan setelah UTS)	Bab 9, Bab 10
CPMK-4	Sub-CPMK 4.1, 4.2, 4.3 (seluruh)	Bab 11, Bab 12, Bab 13
CPMK-5	Sub-CPMK 5.1, Sub-CPMK 5.2 (seluruh)	Bab 14, Bab 15
CPMK-6	Sub-CPMK 6.1 (seluruh)	Bab 15

CPL yang diukur melalui UAS adalah CPL-5, CPL-8, CPL-9, dan CPL-10, sebagaimana tercantum pada RPS mata kuliah Enterprise Networking, mencerminkan cakupan penilaian yang lebih luas dibandingkan UTS karena turut mengukur kemampuan kerja tim, komunikasi, dan kesadaran pengembangan diri berkelanjutan.

B. RANGKUMAN KOMPREHENSIF MATERI BAB 9–15

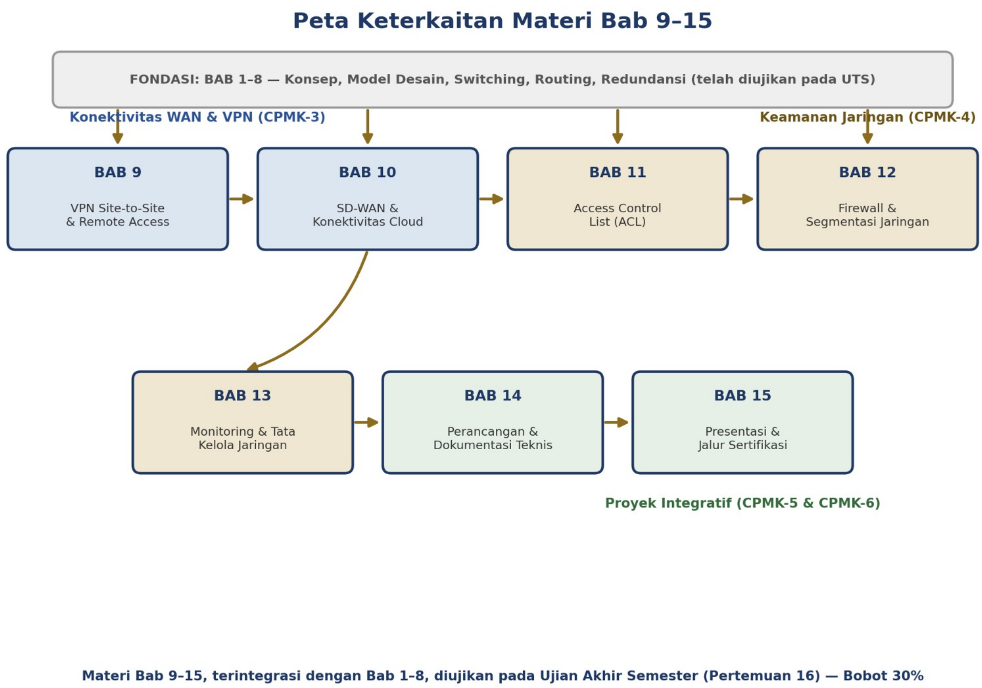
Tabel berikut menyajikan ringkasan poin-poin kunci dari setiap bab sebagai bahan tinjauan cepat (quick review) sebelum menghadapi UAS. Untuk pemahaman mendalam, mahasiswa tetap disarankan mempelajari kembali uraian materi lengkap pada masing-masing bab, termasuk meninjau ulang rangkuman Bab 1–8 pada Bab 8 (Evaluasi Tengah Semester) mengingat sifat UAS yang integratif.

Bab	Konsep Kunci
Bab 9 VPN Site-to-Site dan Remote Access	• VPN site-to-site (permanen, LAN-to-LAN) vs remote access (individual, on-demand) • IPsec: IKE Phase 1 (ISAKMP) dan IKE Phase 2 (transform set); AH vs ESP • Konfigurasi: ACL interesting traffic, crypto map, verifikasi show crypto isakmp/ipsec sa
Bab 10 SD-WAN dan Konektivitas Cloud	• Arsitektur SD-WAN: orchestrator, edge device, underlay (multi-transport), overlay • Application-aware routing; manfaat (biaya, manajemen) vs tantangan (vendor lock-in, migrasi) • Konektivitas cloud: akses berbasis internet vs Direct Cloud Connect; local internet breakout
Bab 11 Access Control List (ACL)	• ACL standar (sumber saja, dekat tujuan) vs extended (sumber+tujuan+protokol+port, dekat sumber) • Implicit deny any; urutan aturan dari spesifik ke umum • Penerapan: ip access-group (interface), access-class (VTY); verifikasi show access-lists
Bab 12 Firewall dan Segmentasi Jaringan	• Jenis firewall: packet-filtering (stateless), stateful, next-generation (NGFW) • Prinsip least privilege; zonasi keamanan (Inside, Outside, DMZ); default deny antar-zona • Zone-based policy firewall: zone security, class-map/policy-map type inspect, zone-pair
Bab 13 Monitoring dan Tata Kelola Jaringan	• SNMP: manager-agent-MIB/OID; operasi GET/SET/TRAP; SNMPv3 direkomendasikan • NetFlow: flow record (7 atribut), analisis top talkers dan anomali trafik • Baseline sebagai acuan normal; Kebijakan Penggunaan Jaringan (AUP)
Bab 14 Perancangan dan Dokumentasi Teknis	• Komponen dokumentasi: executive summary, topologi, IP addressing table, konfigurasi kunci, dsb. • Diagram topologi berlabel lengkap (hostname, interface, IP) sebagai praktik terbaik • Proyek kelompok: analisis kebutuhan → perancangan → implementasi/pengujian → dokumentasi
Bab 15 Presentasi dan Jalur Sertifikasi	• Teknik presentasi teknis: struktur sistematis, kesadaran audiens, visualisasi, kesiapan Q&A • Jenjang sertifikasi Cisco: CCT → CCNA → CCNP (ENCOR) → CCIE → CCAr

Bab	Konsep Kunci
	• Pengembangan kompetensi berkelanjutan: sertifikasi lain, cloud networking, praktik mandiri

C. PETA KETERKAITAN ANTAR-MATERI

Diagram berikut menggambarkan keterkaitan logis antar-bab pada paruh kedua semester (Bab 9–15), sekaligus menunjukkan bagaimana materi tersebut dibangun di atas fondasi konsep, switching, dan routing yang telah dipelajari pada Bab 1–8 dan diujikan pada UTS.



Gambar 16.1 Peta Keterkaitan Materi Bab 9–15

Diagram di atas menunjukkan bahwa seluruh materi Bab 9–15 dibangun di atas fondasi Bab 1–8 yang telah diujikan pada UTS. Bab 9 dan Bab 10 memperluas cakupan konektivitas WAN menuju VPN dan SD-WAN (CPMK-3). Bab 11 dan Bab 12 membangun lapisan keamanan jaringan melalui ACL dan firewall, dilanjutkan Bab 13 dengan monitoring dan tata kelola (CPMK-4). Bab 14 dan Bab 15 menjadi puncak integratif berupa proyek kelompok perancangan, dokumentasi, dan presentasi jaringan enterprise, sekaligus memperkenalkan jalur sertifikasi profesi (CPMK-5 dan CPMK-6).

D. KISI-KISI SOAL UJIAN AKHIR SEMESTER

Kisi-kisi berikut disusun berdasarkan Rubrik Penilaian Pertemuan 16 pada dokumen RPS, yang mengelompokkan soal UAS ke dalam tiga bagian besar sesuai cakupan Sub-CPMK.

Bagian	Cakupan Sub-CPMK	Bab Terkait	Bentuk Soal	Bobot
I	Sub-CPMK 3.2–3.3 (Konfigurasi VPN, Analisis SD-WAN/Cloud)	Bab 9–10	Konfigurasi CLI + analisis	8%
II	Sub-CPMK 4.1–4.3 (Keamanan Jaringan: ACL, Firewall, Monitoring)	Bab 11–13	Konfigurasi CLI + analisis	12%
III	Sub-CPMK 5.1–6.1 (Kualitas Dokumentasi/Integrasi Rancangan dan Pemahaman Jalur Sertifikasi)	Bab 14–15	Studi kasus komprehensif + uraian	10%

Total bobot UAS: 30% dari nilai akhir mata kuliah.

E. LATIHAN SOAL SIMULASI UJIAN AKHIR SEMESTER

Latihan soal berikut disusun menyerupai format UAS sesungguhnya, terbagi ke dalam tiga bagian sesuai kisi-kisi pada Bagian D, sekaligus mengintegrasikan kembali materi Bab 1–8 sebagai konteks studi kasus. Kerjakan sebagai simulasi mandiri sebelum menghadapi UAS yang sebenarnya.

Bagian I — Konfigurasi VPN dan Analisis SD-WAN/Cloud (Bobot 8%)

1. Tuliskan perintah Cisco IOS lengkap untuk mengonfigurasi IKE Phase 1 dengan enkripsi AES 256, hash SHA256, dan autentikasi pre-shared key.

2. Jelaskan perbedaan antara VPN site-to-site dan VPN remote access, disertai contoh skenario penggunaan masing-masing.

3. Sebuah organisasi dengan 40 cabang saat ini menggunakan MPLS penuh dengan biaya tinggi. Analisislah manfaat dan tantangan migrasi menuju SD-WAN untuk organisasi tersebut.

4. Jelaskan perbedaan antara akses cloud berbasis internet biasa dan Direct Cloud Connect, disertai rekomendasi kapan masing-masing pendekatan sebaiknya digunakan.

Bagian II — Keamanan Jaringan: ACL, Firewall, dan Monitoring (Bobot 12%)

1. Tuliskan perintah Cisco IOS lengkap untuk membuat ACL extended yang hanya mengizinkan trafik HTTPS dari subnet 192.168.30.0/24 menuju host 192.168.10.50, dan menolak trafik lain menuju host tersebut.

2. Jelaskan perbedaan antara stateful firewall dan next-generation firewall (NGFW).

3. Rancanglah skema zonasi keamanan (minimal tiga zona) untuk sebuah klinik kesehatan dengan sistem rekam medis internal dan website pendaftaran online untuk pasien, disertai kebijakan zone-pair yang sesuai.

4. Jelaskan perbedaan fokus pemantauan antara SNMP dan NetFlow, disertai contoh skenario ketika masing-masing teknologi paling tepat digunakan.

5. Data NetFlow menunjukkan satu host tiba-tiba menghasilkan trafik keluar sangat besar menuju port yang tidak umum pada tengah malam. Analisislah kemungkinan penyebab dan langkah yang perlu diambil administrator.

6. Susunlah tiga poin utama yang wajib ada dalam kebijakan penggunaan jaringan (AUP) untuk jaringan Wi-Fi tamu pada sebuah kantor.

Bagian III — Studi Kasus Komprehensif: Dokumentasi, Integrasi Rancangan, dan Jalur Sertifikasi (Bobot 10%)

1. Sebuah universitas dengan tiga kampus (pusat, cabang A, cabang B) memerlukan rancangan jaringan enterprise yang lengkap. Susunlah garis besar rancangan yang mengintegrasikan minimal lima topik dari Bab 1–13 (contoh: model desain, VLAN, routing OSPF, redundansi gateway, konektivitas WAN/VPN, dan keamanan), disertai justifikasi singkat setiap pilihan.

2. Jelaskan lima komponen utama yang wajib ada dalam dokumen rancangan jaringan enterprise sesuai standar dokumentasi teknis industri.

3. Jelaskan mengapa presenter perlu mempersiapkan diri menjawab pertanyaan mengenai alasan ("mengapa") di balik keputusan desain, bukan hanya menjelaskan "apa" yang dirancang.

4. Jelaskan cakupan utama ujian ENCOR (350-401) pada jenjang CCNP Enterprise dan kaitannya dengan materi mata kuliah Enterprise Networking secara keseluruhan.

F. PETUNJUK PENGERJAAN DAN TATA TERTIB UJIAN

- UAS berlangsung selama 100 menit, sesuai alokasi waktu 2 SKS teori (2 × 50 menit) pada Pertemuan ke-16.
- Bagian I dan II yang bersifat konfigurasi dapat dikerjakan menggunakan simulator jaringan (Packet Tracer/GNS3) apabila UAS dilaksanakan dalam format praktik, sesuai kebijakan dosen pengampu.
- Bagian III (studi kasus komprehensif) dikerjakan secara tertulis dengan penjelasan yang sistematis dan disertai justifikasi teknis untuk setiap keputusan rancangan yang diusulkan.
- Mahasiswa wajib menuliskan jawaban secara mandiri; kerja sama tanpa izin dianggap sebagai pelanggaran akademik.
- Kecurangan akademik dalam bentuk apa pun akan dikenai sanksi sesuai peraturan akademik Politeknik Negeri Padang yang berlaku.

G. RUBRIK PENILAIAN UJIAN AKHIR SEMESTER

Rubrik berikut merupakan rubrik resmi Pertemuan 16 sebagaimana tercantum pada dokumen RPS dan Rubrik Penilaian per Pertemuan mata kuliah Enterprise Networking, digunakan sebagai acuan penilaian jawaban UAS.

Ketepatan Konfigurasi VPN dan Analisis SD-WAN/Cloud (Sub-CPMK 3.2–3.3) (Bobot: 8%)

Kategori	Skor	Indikator
Sangat Baik	85–100	Soal konfigurasi VPN dan analisis SD-WAN/konektivitas cloud dijawab dengan tepat, sistematis, dan disertai pertimbangan keamanan serta efisiensi yang relevan.
Baik	70–84	Sebagian besar soal dijawab benar dengan sedikit kesalahan konsep/konfigurasi.
Cukup	55–69	Sebagian soal dijawab benar, pemahaman dasar terlihat namun belum menyeluruh.
Kurang	< 55	Sebagian besar jawaban tidak tepat atau soal tidak dikerjakan.

Ketepatan Konfigurasi & Analisis Keamanan Jaringan: ACL, Firewall, Monitoring (Sub-CPMK 4.1–4.3) (Bobot: 12%)

Kategori	Skor	Indikator
Sangat Baik	85–100	Soal ACL, firewall/segmentasi, serta monitoring dan tata kelola jaringan dijawab dengan tepat dan lengkap, menunjukkan kemampuan menerapkan prinsip keamanan secara terintegrasi.
Baik	70–84	Sebagian besar soal keamanan jaringan dijawab benar dengan sedikit kekurangan pada aspek tata kelola.
Cukup	55–69	Sebagian soal keamanan jaringan dijawab benar, namun integrasi antar-komponen keamanan kurang tepat.
Kurang	< 55	Sebagian besar jawaban terkait keamanan jaringan tidak tepat atau tidak dikerjakan.

Kualitas Dokumentasi/Integrasi Rancangan dan Pemahaman Jalur Sertifikasi (Sub-CPMK 5.1–6.1) (Bobot: 10%)

Kategori	Skor	Indikator
Sangat Baik	85–100	Mampu mengintegrasikan seluruh kompetensi (perancangan, keamanan, dokumentasi) dalam studi kasus komprehensif serta menjelaskan relevansi sertifikasi profesi (CCNA/CCNP ENCOR) terhadap karier di bidang jaringan enterprise.
Baik	70–84	Mampu mengintegrasikan sebagian besar kompetensi dengan benar, penjelasan jalur sertifikasi cukup relevan.
Cukup	55–69	Integrasi kompetensi kurang menyeluruh, pemahaman jalur sertifikasi terbatas.
Kurang	< 55	Tidak mampu mengintegrasikan kompetensi yang telah dipelajari atau soal tidak dikerjakan.

PENUTUP BUKU AJAR

Selamat menyelesaikan seluruh rangkaian materi Buku Ajar Enterprise Networking. Mulai dari pengenalan konsep dasar jaringan enterprise (Bab 1) hingga presentasi hasil rancangan dan pengenalan jalur sertifikasi profesi (Bab 15), setiap bab telah dirancang untuk membangun kompetensi mahasiswa secara berjenjang, selaras dengan capaian pembelajaran lulusan Program Studi D3 Teknik Komputer, Politeknik Negeri Padang.

Penguasaan atas materi buku ajar ini diharapkan tidak berhenti pada penilaian UAS semata, melainkan menjadi fondasi bagi mahasiswa untuk terus mengembangkan diri melalui praktik mandiri, jalur sertifikasi profesi, dan pembelajaran berkelanjutan, sebagaimana telah dibahas pada Bab 15. Semoga buku ajar ini bermanfaat dan mengantarkan mahasiswa menuju kesuksesan, baik dalam mata kuliah ini maupun dalam perjalanan karier di bidang jaringan enterprise selanjutnya.

DAFTAR PUSTAKA

Berikut adalah kompilasi seluruh sumber referensi yang digunakan pada Bab 1 hingga Bab 15 buku ajar ini, disusun dalam format APA dan diurutkan berdasarkan abjad nama penulis. Referensi rinci per bab dapat dilihat pada bagian Daftar Pustaka masing-masing bab.

Cisco Networking Academy. (2022). CCNP Enterprise: Core networking technologies (ENCOR) companion guide. Cisco Press.

Froom, R., Frahim, E., & Sivasubramanian, B. (2021). Implementing Cisco IP switched networks (SWITCH) foundation learning guide (2nd ed.). Cisco Press.

Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson.

Marschke, D., Doraswamy, N., & Ghosh, A. (2021). SD-WAN: A comprehensive approach for enterprise networking. Packt Publishing.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 1 (2nd ed.). Cisco Press.

Odom, W. (2023). CCNA 200-301 official cert guide, volume 2 (2nd ed.). Cisco Press.

Stallings, W. (2023). Network security essentials: Applications and standards (7th ed.). Pearson.

Teare, D., & Paquet, C. (2022). Implementing Cisco IP routing (ROUTE) foundation learning guide (2nd ed.). Cisco Press.

GLOSARIUM

Glosarium berikut merangkum seluruh istilah teknis kunci yang dibahas sepanjang Bab 1 hingga Bab 15, disusun berdasarkan abjad.

Istilah	Definisi
ACL (Access Control List)	Daftar aturan permit/deny yang dievaluasi berurutan untuk mengizinkan atau menolak lalu lintas jaringan berdasarkan kriteria tertentu (Bab 11).
AH (Authentication Header)	Protokol keamanan IPsec yang menyediakan autentikasi dan integritas tanpa enkripsi (Bab 9).
Area Border Router (ABR)	Router OSPF yang menghubungkan Area 0 (backbone) dengan area non-backbone lainnya (Bab 5).
AUP (Acceptable Use Policy)	Kebijakan Penggunaan Jaringan yang mengatur aktivitas yang diizinkan/dilarang bagi pengguna jaringan organisasi (Bab 13).
Baseline	Pola lalu lintas dan utilisasi sumber daya yang dianggap normal, menjadi acuan pembanding untuk mendeteksi anomali (Bab 13).
Broadband	Akses internet publik bersama (DSL, kabel, fiber) dengan biaya rendah namun performa bervariasi (Bab 7).
CCNA (Cisco Certified Network Associate)	Sertifikasi jenjang associate Cisco dengan ujian tunggal 200-301, mencakup fondasi jaringan (Bab 15).
CCNP Enterprise	Sertifikasi jenjang professional Cisco yang mensyaratkan ujian inti ENCOR (350-401) dan satu ujian konsentrasi (Bab 15).
DMZ (Demilitarized Zone)	Zona jaringan perantara untuk menempatkan server publik, terisolasi dari jaringan internal (Bab 12).
EtherChannel	Teknologi agregasi tautan yang menggabungkan beberapa link fisik menjadi satu link logis (Bab 4).
ESP (Encapsulating Security Payload)	Protokol keamanan IPsec yang menyediakan autentikasi, integritas, dan enkripsi sekaligus (Bab 9).
Firewall	Perangkat/perangkat lunak yang menegakkan kebijakan keamanan antar-segmen jaringan dengan tingkat kepercayaan berbeda (Bab 12).
GLBP (Gateway Load Balancing Protocol)	Protokol redundansi gateway Cisco yang mendukung load balancing antar-router (Bab 6).
High Availability	Karakteristik desain sistem yang menjamin layanan tetap tersedia meski terjadi kegagalan komponen (Bab 1, Bab 6).
HSRP (Hot Standby Router Protocol)	Protokol redundansi gateway Cisco dengan peran active/standby (Bab 6).
IKE (Internet Key Exchange)	Protokol negosiasi dua fase (Phase 1/2) untuk membentuk tunnel IPsec (Bab 9).
Implicit Deny	Aturan otomatis di akhir setiap ACL yang menolak seluruh trafik yang tidak secara eksplisit diizinkan (Bab 11).
Inter-VLAN Routing	Proses routing yang memungkinkan komunikasi antar-VLAN yang berbeda, umumnya via SVI (Bab 4).
IPsec (Internet Protocol Security)	Kerangka kerja protokol keamanan Layer 3 untuk membangun VPN, terdiri atas AH dan ESP (Bab 9).
LACP (Link Aggregation Control Protocol)	Protokol standar terbuka (IEEE 802.3ad) untuk membentuk EtherChannel (Bab 4).
Leased Line	Sirkuit WAN dedicated point-to-point yang disewa eksklusif, andal namun berbiaya tinggi (Bab 7).
Least Privilege	Prinsip keamanan yang memberikan akses seminimal mungkin sesuai kebutuhan, diwujudkan melalui default deny (Bab 12).
MIB (Management Information Base)	Basis data hierarkis berisi variabel yang dapat diakses melalui SNMP, diidentifikasi dengan OID (Bab 13).
MPLS (Multiprotocol Label Switching)	Teknologi WAN berbasis label switching yang mendukung konektivitas any-to-any dan QoS (Bab 7).

Istilah	Definisi
NetFlow	Teknologi Cisco untuk mengumpulkan dan menganalisis data lalu lintas jaringan berbasis flow (Bab 13).
NGFW (Next-Generation Firewall)	Firewall generasi terbaru dengan deep packet inspection dan application awareness (Bab 12).
Object Tracking	Mekanisme FHRP yang menurunkan priority secara otomatis saat interface uplink terputus (Bab 6).
OSPF (Open Shortest Path First)	Protokol routing dinamis link-state yang mendukung pembagian jaringan ke dalam beberapa area (Bab 5).
PAgP (Port Aggregation Protocol)	Protokol milik Cisco untuk membentuk EtherChannel, alternatif LACP (Bab 4).
Router ID	Alamat IP unik yang mengidentifikasi router pada proses routing OSPF (Bab 5).
SD-WAN (Software-Defined WAN)	Pendekatan WAN berbasis perangkat lunak yang memisahkan control plane dari data plane (Bab 10).
Segmentasi Jaringan	Praktik membagi jaringan menjadi beberapa segmen/zona untuk meningkatkan keamanan dan kinerja (Bab 3, Bab 12).
SNMP (Simple Network Management Protocol)	Protokol standar untuk memantau dan mengelola perangkat jaringan (Bab 13).
Spine-Leaf	Model desain jaringan data center dua lapisan dengan struktur full-mesh antara spine dan leaf (Bab 2).
SVI (Switched Virtual Interface)	Interface virtual pada Layer 3 switch yang mewakili satu VLAN dan berfungsi sebagai default gateway (Bab 4).
Three-Tier Architecture	Model desain jaringan hierarkis dengan tiga lapisan: core, distribution, access (Bab 2).
Trunking (802.1Q)	Mekanisme pengiriman lalu lintas dari beberapa VLAN melalui satu tautan fisik menggunakan tagging (Bab 3).
VLAN (Virtual Local Area Network)	Segmentasi logis jaringan pada Layer 2 yang memisahkan broadcast domain (Bab 3).
VPN (Virtual Private Network)	Teknologi yang membangun koneksi aman dan terenkripsi melalui jaringan publik (Bab 9).
VRRP (Virtual Router Redundancy Protocol)	Protokol redundansi gateway standar terbuka, alternatif HSRP (Bab 6).
VTP (VLAN Trunking Protocol)	Protokol Cisco untuk menyinkronkan konfigurasi VLAN antar-switch dalam satu domain (Bab 3).
Wildcard Mask	Notasi kebalikan dari subnet mask yang digunakan pada konfigurasi ACL dan OSPF (Bab 5, Bab 11).
Zone-Based Policy Firewall	Implementasi firewall stateful pada Cisco IOS berbasis pengelompokan interface ke dalam zona keamanan (Bab 12).

LAMPIRAN

Lampiran 1 — Rencana Pembelajaran Semester (RPS) Enterprise Networking

Dokumen RPS lengkap mata kuliah Enterprise Networking (identitas mata kuliah, CPL, CPMK, Sub-CPMK, matriks korelasi, bahan kajian, dan rencana pembelajaran per pertemuan) menjadi dokumen sumber utama penyusunan buku ajar ini dan dilampirkan secara terpisah sebagai dokumen pendukung resmi mata kuliah.

Lampiran 2 — Ringkasan Rubrik Penilaian per Pertemuan

Tabel berikut merangkum aspek penilaian dan bobot pada setiap pertemuan sepanjang satu semester. Rubrik rinci per kategori (Sangat Baik/Baik/Cukup/Kurang) untuk setiap aspek tercantum pada dokumen Rubrik Penilaian per Pertemuan yang menyertai RPS, serta pada bagian akhir Bab 8 dan Bab 16 untuk pertemuan UTS dan UAS.

Pert.	Topik	Aspek Penilaian	Bobot
1	Pengantar Jaringan Enterprise	Identifikasi Karakteristik Jaringan Enterprise	1%
2	Model Desain Jaringan Enterprise	Tugas Kelompok + Partisipasi Diskusi	3%
3	VLAN, Trunking, dan VTP	Tugas Praktik + Partisipasi Diskusi	3%
4	EtherChannel dan Routing Antar-VLAN	Tugas Praktik + Partisipasi Diskusi	3%
5	Routing Dinamis OSPF Multi-Area	Tugas Individu + Partisipasi Diskusi	4%
6	Redundansi Gateway dan High Availability	Tugas Kelompok + Partisipasi Diskusi	4%
7	Teknologi WAN Enterprise	Tugas Analisis + Partisipasi Diskusi	3%
8	Evaluasi Tengah Semester (UTS)	Tiga Aspek (lihat Bab 8)	30%
9	VPN Site-to-Site dan Remote Access	Tugas Praktik + Partisipasi Diskusi	3%
10	SD-WAN dan Konektivitas Cloud	Tugas Analisis + Partisipasi Diskusi	3%
11	Access Control List (ACL)	Tugas Praktik	2%
12	Firewall dan Segmentasi Jaringan	Tugas Praktik	2%
13	Monitoring dan Tata Kelola Jaringan	Tugas Praktik	3%
14	Perancangan dan Dokumentasi Teknis	Tugas Proyek	3%
15	Presentasi dan Jalur Sertifikasi	Presentasi Kelompok + Partisipasi Diskusi	3%
16	Evaluasi Akhir Semester (UAS)	Tiga Aspek (lihat Bab 16)	30%

Total: Tugas per pertemuan 30% + Partisipasi 10% + UTS 30% + UAS 30% = 100%

Lampiran 3 — Rubrik Penilaian Capaian Pembelajaran Lulusan (CPL)

Rubrik berikut digunakan untuk menilai capaian akhir setiap CPL secara holistik pada akhir semester, dihitung dari agregasi terbobot skor CPMK sesuai Matriks Korelasi CPL–CPMK pada RPS.

CPL	Formula Perhitungan
CPL-2	(0,33 × Skor CPMK-1) + (0,67 × Skor CPMK-2)
CPL-5	(0,14×CPMK-1) + (0,30×CPMK-2) + (0,21×CPMK-3) + (0,21×CPMK-4) + (0,14×CPMK-5)
CPL-8	1,00 × Skor CPMK-4
CPL-9	1,00 × Skor CPMK-5
CPL-10	(0,95 × Skor CPMK-3) + (0,05 × Skor CPMK-6)

Kategori Capaian dan Tindak Lanjut

Kategori	Rentang Skor	Tindak Lanjut
Sangat Baik	85–100	CPL tercapai penuh; diarahkan pada penguatan lanjut (sertifikasi profesi, proyek pengayaan).
Baik	70–84	CPL tercapai sesuai standar minimum program studi; tidak memerlukan tindak lanjut khusus.
Cukup	55–69	CPL tercapai sebagian; direkomendasikan pendampingan/remedial terarah.
Kurang	< 55	CPL belum tercapai; wajib mengikuti program remedial sebelum dinyatakan lulus untuk komponen CPL terkait.

Lampiran 4 — Contoh Lembar Kerja Praktik Simulasi (Packet Tracer/GNS3)

Template berikut dapat digunakan mahasiswa sebagai format standar pelaporan setiap sesi praktik simulasi sepanjang semester.

Komponen	Isian
Nama Kelompok/Individu	…………………………………………………………
Pertemuan Ke- / Topik	…………………………………………………………
Tanggal Pelaksanaan	…………………………………………………………
Tujuan Praktik	…………………………………………………………
Topologi yang Digunakan	(sertakan gambar/screenshot topologi)
Langkah Kerja	(uraikan tahapan konfigurasi secara berurutan)
Perintah Konfigurasi Kunci	(salin perintah CLI utama yang digunakan)
Hasil Verifikasi	(sertakan output perintah show yang relevan)
Kendala dan Penyelesaian	…………………………………………………………
Kesimpulan	…………………………………………………………

Lampiran 5 — Contoh Running-Configuration Perangkat

Contoh berikut menggabungkan beberapa elemen konfigurasi kunci yang telah dibahas pada Bab 3 hingga Bab 6 (VLAN, trunking, inter-VLAN routing, OSPF, dan HSRP) ke dalam satu contoh running-configuration Layer 3 switch yang koheren, sebagai referensi format dokumentasi konfigurasi lengkap.

```
hostname SW1-DISTRIBUTION
!
ip routing
!
vlan 10
 name KEUANGAN
vlan 20
 name OPERASIONAL
vlan 30
 name SDM
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30
!
interface GigabitEthernet0/1
 channel-group 1 mode active
interface GigabitEthernet0/2
 channel-group 1 mode active
!
interface Vlan10
 ip address 192.168.10.2 255.255.255.0
 standby 1 ip 192.168.10.1
 standby 1 priority 150
 standby 1 preempt
!
interface Vlan20
 ip address 192.168.20.2 255.255.255.0
 standby 2 ip 192.168.20.1
 standby 2 priority 150
 standby 2 preempt
!
interface Vlan30
 ip address 192.168.30.2 255.255.255.0
 standby 3 ip 192.168.30.1
 standby 3 priority 150
 standby 3 preempt
!
router ospf 1
 router-id 2.2.2.2
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
```

```
 network 192.168.30.0 0.0.0.255 area 0
 network 10.0.0.0 0.0.0.3 area 0
!
end
```

Lampiran 5.1 Contoh running-configuration Layer 3 switch (distribution) terintegrasi VLAN, EtherChannel, HSRP, dan OSPF

INDEKS

Indeks berikut membantu pembaca menemukan pembahasan suatu istilah dengan cepat, disusun berdasarkan abjad dan merujuk pada bab yang relevan.