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

MODUL PRAKTIKUM

ENTERPRISE NETWORKING

CEN3302

Panduan Praktik Konfigurasi, Pengujian, dan Dokumentasi Jaringan Enterprise Berbasis Simulasi & Perangkat Laboratorium

Praktikum Enterprise Networking • CEN3302/MKK-EN02
1 SKS Praktik (170 menit/minggu) • Semester 3

DOSEN PENGAMPU
Ir. H. A. Mooduto, M.Kom.
Ideva Gaputra, S.Kom., M.Kom.

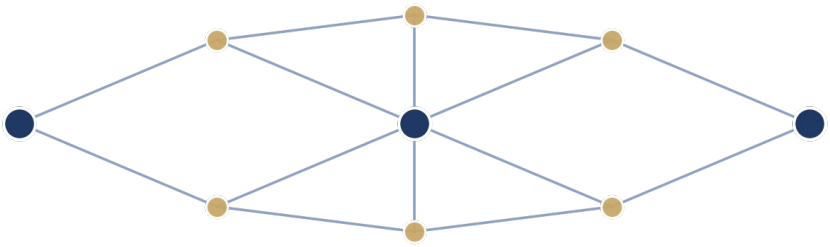
POLITEKNIK NEGERI PADANG
2026

PANDUAN PRAKTIKUM · D3 TEKNIK KOMPUTER

MODUL PRAKTIKUM ENTERPRISE NETWORKING (PRAKTIKUM)

Kode Mata Kuliah: CEN3302 · 1 SKS Praktik · Semester 3

Panduan Praktik Konfigurasi, Pengujian, dan Dokumentasi Jaringan Enterprise Berbasis Simulasi (Cisco Packet Tracer/GNS3) dan Perangkat Laboratorium



Disusun untuk

PROGRAM STUDI D3 TEKNIK KOMPUTER

Jurusan Teknologi Informasi

Politeknik Negeri Padang

POLITEKNIK NEGERI PADANG · 2026

LEMBAR PENGESAHAN

Modul Praktikum Enterprise Networking (Praktikum) ini disusun sebagai perangkat pembelajaran praktik pada Program Studi D3 Teknik Komputer, Politeknik Negeri Padang, mengacu pada Rencana Pembelajaran Semester (RPS), Rubrik Penilaian Praktikum, dan Rubrik Penilaian Capaian Pembelajaran Lulusan (CPL) yang telah ditetapkan.

Nama Modul	Modul Praktikum Enterprise Networking (Praktikum)
Kode Mata Kuliah	CEN3302
Program Studi	D3 Teknik Komputer
Jurusan	Teknologi Informasi
Institusi	Politeknik Negeri Padang (PNP)
Bobot SKS	1 SKS Praktik (170 menit/minggu)
Semester	3 (Tiga)
Mata Kuliah Prasyarat	Jaringan Komputer Dasar
Dosen Pengampu	1. Ir. H. A. Mooduto, M.Kom. 2. Ideva Gaputra, S.Kom., M.Kom.
Tahun Penyusunan	Agustus 2026

Mengetahui,
Ketua Program Studi D3 Teknik Komputer

(Fitri Nova, S.ST., MT.)
NIP. 198505292014042001

Padang, Agustus 2026
Dosen Pengampu / Penyusun

(Ir. H. A. Mooduto, M.Kom.)
NIP. 196605101994031003

KATA PENGANTAR

Puji dan syukur dipanjatkan atas tersusunnya Modul Praktikum Enterprise Networking (Praktikum) untuk Program Studi D3 Teknik Komputer, Politeknik Negeri Padang. Modul ini disusun sebagai panduan hands-on bagi mahasiswa dan instruktur dalam melaksanakan kegiatan praktikum jaringan berskala enterprise, mulai dari konfigurasi dasar perangkat switch dan router hingga topik lanjut seperti routing dinamis, redundansi gateway, konektivitas WAN/VPN, kontrol akses, dan monitoring jaringan.

Penyusunan modul ini mengacu secara ketat pada Rencana Pembelajaran Semester (RPS) mata kuliah Enterprise Networking (Praktikum) CEN3302, mencakup Capaian Pembelajaran Lulusan (CPL), Capaian Pembelajaran Mata Kuliah (CPMK), dan Kemampuan Akhir yang Diharapkan (Sub-CPMK) yang telah ditetapkan, serta selaras dengan deskriptor jenjang 5 Kerangka Kualifikasi Nasional Indonesia (KKNI) sebagaimana diatur dalam Lampiran Peraturan Presiden Nomor 8 Tahun 2012, dan ketentuan penyelenggaraan pembelajaran pada Peraturan Menteri Pendidikan Tinggi, Sains, dan Teknologi (Permendiktisaintek) Nomor 39 Tahun 2025.

Setiap modul praktikum disusun dengan struktur baku yang terdiri atas tujuan praktikum, dasar teori ringkas, alat dan bahan, langkah kerja/prosedur, tugas praktikum, format laporan, serta rubrik penilaian, sehingga memudahkan mahasiswa memahami capaian yang harus dikuasai pada setiap pertemuan sekaligus memberikan acuan penilaian yang konsisten bagi instruktur/dosen pengampu.

Modul ini diharapkan dapat menjadi acuan pelaksanaan praktikum yang sistematis, mendukung pencapaian kompetensi lulusan sesuai standar industri jaringan (CCNA/MTCNA), serta menjadi bagian dari upaya penjaminan mutu internal program studi. Kritik dan saran yang membangun sangat diharapkan demi penyempurnaan modul ini pada masa mendatang.

Padang, Agustus 2026
Penyusun

Ir. H.A. Mooduto, M.Kom

DAFTAR ISI

I. PETUNJUK PENGGUNAAN MODUL

Modul Praktikum Enterprise Networking (Praktikum) ini dirancang untuk digunakan secara terstruktur oleh mahasiswa dan instruktur/dosen pengampu selama satu semester (16 pertemuan). Agar pelaksanaan praktikum berjalan efektif, berikut petunjuk penggunaan modul ini.

A. Struktur Setiap Modul Pertemuan

Setiap modul (Modul 1 s.d. Modul 16) disusun dengan struktur baku sebagai berikut:

1. Identitas Modul — mencantumkan Sub-CPMK, CPL terkait, dan bobot penilaian pertemuan.
2. Tujuan Praktikum — kompetensi spesifik yang harus dicapai mahasiswa pada akhir sesi.
3. Dasar Teori Ringkas — konsep kunci yang relevan sebagai pengantar sebelum praktik.
4. Alat dan Bahan — perangkat lunak (simulator) dan/atau perangkat keras laboratorium yang dibutuhkan.
5. Langkah Kerja/Prosedur — instruksi praktik bertahap yang harus diikuti mahasiswa.
6. Tugas Praktikum — skenario/studi kasus yang harus diselesaikan dan diverifikasi mahasiswa.
7. Format Laporan — struktur laporan praktikum yang harus disusun dan dikumpulkan.
8. Rubrik Penilaian Ringkas — kriteria penilaian sesuai Rubrik Penilaian Praktikum per Pertemuan yang berlaku.

B. Panduan bagi Mahasiswa

- Membaca dasar teori dan tujuan praktikum sebelum sesi praktik dimulai (pre-lab).
- Mematuhi seluruh prosedur K3 Laboratorium yang dijelaskan pada bagian tersendiri modul ini.
- Mengerjakan langkah kerja secara mandiri atau berkelompok sesuai instruksi setiap modul.
- Melakukan verifikasi hasil konfigurasi sebelum menyusun laporan.
- Menyusun dan mengumpulkan laporan praktikum sesuai format dan tenggat waktu yang ditentukan instruktur.

C. Panduan bagi Instruktur/Dosen Pengampu

- Menyampaikan orientasi singkat (demonstrasi) sebelum mahasiswa memulai praktik mandiri/terbimbing.
- Memandu sesi praktik sesuai metode pembelajaran yang tercantum pada RPS (demonstrasi, praktikum terbimbing, studi kasus, project-based learning).
- Menggunakan Rubrik Penilaian Praktikum per Pertemuan sebagai acuan penilaian yang konsisten dan objektif.
- Mendokumentasikan capaian Sub-CPMK setiap mahasiswa sebagai dasar perhitungan capaian CPMK dan CPL pada akhir semester.

D. Alur Penilaian

Nilai setiap pertemuan dihitung secara terbobot dari beberapa aspek penilaian (lihat Rubrik Penilaian Praktikum per Pertemuan pada masing-masing modul), kemudian diakumulasikan menjadi komponen Tugas Praktikum (30%), Partisipasi (10%), UTS (30%), dan UAS (30%) sesuai rekapitulasi

bobot penilaian pada RPS. Nilai capaian tiap CPMK dan CPL dihitung lebih lanjut mengikuti formula pada Rubrik Penilaian CPL, sebagaimana dicontohkan pada bagian akhir modul ini.

II. TATA TERTIB DAN PROSEDUR K3 LABORATORIUM

Bagian ini menjadi acuan bersama bagi seluruh pertemuan praktikum dan mendukung pencapaian CPL-12 (Sikap): kemampuan melaksanakan pekerjaan keteknikan sesuai kode etik profesi, prinsip Keselamatan dan Kesehatan Kerja (K3), serta ketentuan peraturan perundang-undangan yang berlaku.

A. Tata Tertib Umum Laboratorium

9. Mahasiswa wajib hadir tepat waktu dan mengenakan pakaian praktik yang sesuai ketentuan program studi.
10. Mahasiswa dilarang membawa makanan/minuman ke area kerja perangkat aktif.
11. Penggunaan perangkat laboratorium (switch, router, kabel, modul simulasi) harus sesuai penugasan instruktur.
12. Kerusakan atau kehilangan perangkat akibat kelalaian menjadi tanggung jawab mahasiswa/kelompok yang bersangkutan.
13. Mahasiswa wajib mengembalikan perangkat, kabel, dan area kerja pada kondisi rapi setelah sesi praktikum selesai.

B. Prosedur Keselamatan dan Kesehatan Kerja (K3)

- Memeriksa kondisi kabel daya dan perangkat sebelum digunakan; melaporkan kerusakan kepada instruktur.
- Menghindari kontak langsung dengan konektor logam saat perangkat dalam kondisi menyala (live) untuk mencegah risiko elektrostatis (ESD).
- Menggunakan gelang antistatis (jika tersedia) saat menangani komponen internal perangkat.
- Menata kabel dan perangkat pada jalur yang tidak mengganggu akses evakuasi/lalu lintas laboratorium.
- Mematikan dan mencabut perangkat sesuai prosedur (bukan langsung mencabut kabel daya) di akhir sesi.
- Segera melaporkan kepada instruktur apabila terjadi insiden (tersengat listrik, perangkat terbakar/overheat, cedera kerja).

C. Sanksi dan Konsekuensi

Pelanggaran terhadap tata tertib dan prosedur K3 akan memengaruhi komponen penilaian Partisipasi serta aspek Penerapan Prosedur K3 Laboratorium pada Rubrik Penilaian Praktikum Pertemuan 1 dan dapat berdampak pada penilaian sikap (CPL-12) sepanjang semester, sesuai deskriptor pada Rubrik Penilaian CPL.

III. PETA KOMPETENSI (CPL – CPMK – SUB-CPMK)

Peta kompetensi berikut menggambarkan keterkaitan antara Capaian Pembelajaran Lulusan (CPL), Capaian Pembelajaran Mata Kuliah (CPMK), Kemampuan Akhir yang Diharapkan (Sub-CPMK), dan modul praktikum terkait, sebagai acuan bagi mahasiswa dan instruktur dalam memahami alur pencapaian kompetensi sepanjang 16 pertemuan.

A. Tabel 2. Matriks CPMK dan Sub-CPMK per Modul

CPMK	Rumusan Capaian	Sub-CPMK / Modul / CPL Terkait
CPMK-1	Mampu mengonfigurasi VLAN, trunking, VTP, dan EtherChannel pada perangkat switch enterprise sesuai standar industri.	Sub-CPMK 1.1–1.4 (Modul 1–4) | CPL-2, CPL-5, CPL-12
CPMK-2	Mampu mengimplementasikan routing antar-VLAN dan routing dinamis OSPF (single-area dan multi-area).	Sub-CPMK 2.1–2.3 (Modul 5–7) | CPL-2, CPL-5
CPMK-3	Mampu mengonfigurasi redundansi gateway (HSRP/VRRP) dan konektivitas WAN/VPN site-to-site.	Sub-CPMK 3.1–3.2 (Modul 9–10) | CPL-5, CPL-10
CPMK-4	Mampu menerapkan ACL, firewall, segmentasi zona keamanan, serta monitoring dan troubleshooting jaringan dasar.	Sub-CPMK 4.1–4.3 (Modul 11–13) | CPL-5, CPL-8
CPMK-5	Mampu merancang, mendokumentasikan, dan mempresentasikan solusi topologi jaringan enterprise secara kolaboratif.	Sub-CPMK 5.1–5.2 (Modul 14–15) | CPL-9, CPL-10, CPL-12

B. Deskripsi CPL yang Dibebankan

Kode CPL	Deskripsi
CPL-2	Mampu menguasai konsep teoretis bidang teknik komputer secara umum, menyelesaikan pekerjaan teknis berlingkup luas, serta memilih metode penyelesaian yang tepat berdasarkan analisis data.
CPL-5	Mampu merancang, menginstalasi, mengonfigurasi, dan memelihara jaringan komputer (kabel maupun nirkabel) sesuai standar industri dan kebutuhan pengguna.
CPL-8	Mampu menerapkan prinsip keamanan siber dasar dan tata kelola teknologi informasi dalam pengelolaan sistem dan jaringan komputer.
CPL-9	Mampu bekerja sama dalam tim, memimpin kelompok kerja skala kecil-menengah, serta mengomunikasikan hasil kerja teknis secara efektif.
CPL-10	Mampu mengembangkan diri secara berkelanjutan melalui pembelajaran mandiri dan sertifikasi kompetensi.
CPL-12	Mampu melaksanakan pekerjaan keteknikan sesuai kode etik profesi, prinsip K3, serta ketentuan peraturan perundang-undangan yang berlaku.

C. Alur Pencapaian Kompetensi

Kompetensi dibangun secara bertahap dan kumulatif: Modul 1–4 membangun fondasi switching (CPMK-1); Modul 5–7 memperluas ke routing antar-VLAN dan OSPF (CPMK-2), diuji melalui UTS pada Modul 8; Modul 9–10 menambahkan redundansi dan konektivitas WAN/VPN (CPMK-3); Modul 11–13 menekankan keamanan dan tata kelola jaringan (CPMK-4); dan Modul 14–15 mengintegrasikan seluruh kompetensi melalui proyek perancangan kelompok (CPMK-5), yang dievaluasi secara komprehensif pada UAS Modul 16. Nilai capaian setiap CPL dihitung secara akumulatif dari nilai CPMK penyusunnya mengikuti Matriks Korelasi CPL–CPMK pada RPS.

IV. PANDUAN PERANGKAT DAN SIMULATOR

Pelaksanaan praktikum Enterprise Networking menggunakan kombinasi perangkat lunak simulasi jaringan dan/atau perangkat fisik laboratorium, sesuai ketersediaan sumber daya program studi. Tabel berikut merangkum kebutuhan perangkat yang berlaku pada seluruh modul praktikum.

A. Tabel 3. Kebutuhan Perangkat dan Perangkat Lunak

Komponen	Keterangan
Perangkat Lunak Simulasi	Cisco Packet Tracer (versi terbaru) dan/atau GNS3, terpasang pada komputer laboratorium/laptop mahasiswa.
Perangkat Fisik (opsional)	Switch dan router Cisco IOS laboratorium, kabel console, kabel UTP straight/cross, konektor RJ-45.
Spesifikasi Komputer Minimum	Prosesor dual-core, RAM 4 GB (disarankan 8 GB untuk GNS3), ruang penyimpanan 5 GB, sistem operasi Windows 10/11 atau Linux.
Akun/Lisensi	Akun Cisco Networking Academy (NetAcad) untuk akses Packet Tracer resmi.
Alat Pendukung	Kabel console/USB-to-serial, gelang antistatis, alat tulis untuk dokumentasi topologi.

B. Instalasi dan Persiapan Awal

1. Mengunduh dan memasang Cisco Packet Tracer melalui akun NetAcad resmi (lihat Lampiran 5).
2. Memverifikasi kompatibilitas perangkat komputer/laptop sebelum sesi praktikum pertama (Modul 1).
3. Menyiapkan folder kerja terstruktur untuk menyimpan file topologi (.pkt/.gns3) dan dokumentasi laporan setiap modul.
4. Melakukan pencadangan (backup) berkala terhadap file konfigurasi/topologi yang telah dikerjakan.

C. Konvensi Penamaan File dan Topologi

Untuk memudahkan pengelolaan dan penilaian, seluruh file topologi dan laporan praktikum disarankan mengikuti format penamaan berikut:

NIM_NamaMahasiswa_ModulXX_NamaTopik.pkt (untuk file topologi)
NIM_NamaMahasiswa_ModulXX_Laporan.docx/pdf (untuk laporan praktikum)

Format ini konsisten digunakan pada template laporan praktikum (Lampiran 1) dan mempermudah instruktur dalam proses rekapitulasi nilai sesuai Rubrik Penilaian Praktikum per Pertemuan.

MODUL 1

ORIENTASI PRAKTIKUM, PROSEDUR K3 LABORATORIUM, DAN DASAR CLI PERANGKAT JARINGAN (CISCO IOS)

A. Identitas Modul

Modul / Pertemuan	Modul 1 / Pertemuan ke-1
Judul Modul	Orientasi Praktikum, Prosedur K3 Laboratorium, dan Dasar CLI Perangkat Jaringan (Cisco IOS)
Sub-CPMK	Sub-CPMK-1.1 — Mampu mengoperasikan perangkat switch/router sesuai prosedur Keselamatan dan Kesehatan Kerja (K3) laboratorium serta dasar perintah CLI (Command Line Interface).
CPL Terkait	CPL-2, CPL-12
Metode Pembelajaran	Ceramah singkat, demonstrasi, orientasi laboratorium
Alokasi Waktu	170 menit (1 sks praktik)
Bobot Nilai	Kontribusi 1% dari komponen Tugas Praktikum (30%)

B. Tujuan Praktikum

Setelah mengikuti praktikum ini, mahasiswa diharapkan mampu:

1. Menerapkan prosedur Keselamatan dan Kesehatan Kerja (K3) laboratorium jaringan secara konsisten dan mandiri, mencakup penanganan perangkat, kabel, dan pengendalian elektrostatis (ESD).
2. Mengidentifikasi komponen perangkat jaringan (switch, router, port, jenis kabel) beserta fungsinya masing-masing.
3. Membedakan dan berpindah antar-mode Command Line Interface (CLI) Cisco IOS: User EXEC, Privileged EXEC, dan Global Configuration Mode.
4. Menjalankan perintah dasar CLI (hostname, enable secret, show version, show running-config, dan sejenisnya) tanpa kesalahan sintaks.

C. Dasar Teori Ringkas

1. Keselamatan dan Kesehatan Kerja (K3) Laboratorium Jaringan

Laboratorium jaringan komputer melibatkan perangkat elektronik aktif (switch, router) yang rentan terhadap kerusakan akibat electrostatic discharge (ESD), kesalahan penanganan kabel, maupun tata letak kerja yang tidak rapi. Penerapan K3 bertujuan melindungi keselamatan mahasiswa sekaligus menjaga keandalan perangkat laboratorium, sejalan dengan capaian CPL-12 tentang pelaksanaan pekerjaan keteknikan sesuai kode etik profesi dan prinsip K3.

2. Perangkat Dasar Jaringan Enterprise

Switch berfungsi menghubungkan perangkat dalam satu segmen jaringan lokal (LAN) pada lapisan data link, sedangkan router menghubungkan antar-segmen/jaringan berbeda pada lapisan network. Kedua perangkat diakses dan dikonfigurasi melalui antarmuka baris perintah (CLI) menggunakan kabel

console (RJ-45 to DB9/USB) atau melalui emulator terminal pada perangkat lunak simulasi seperti Cisco Packet Tracer.

3. Mode Command Line Interface (CLI) Cisco IOS

- User EXEC Mode — mode awal setelah login, ditandai prompt Switch> atau Router>, hanya mengizinkan perintah pemantauan dasar.
- Privileged EXEC Mode — diakses melalui perintah enable, ditandai prompt Switch# atau Router#, mengizinkan akses penuh ke perintah show dan debug.
- Global Configuration Mode — diakses melalui perintah configure terminal dari Privileged EXEC, ditandai prompt Switch(config)#, digunakan untuk mengubah konfigurasi perangkat secara global.

4. Perintah Dasar CLI yang Digunakan

```
enable                          → masuk ke Privileged EXEC Mode
configure terminal              → masuk ke Global Configuration Mode
hostname <nama>                 → mengubah nama perangkat
enable secret <password>        → mengatur password terenkripsi mode privileged
show version                    → menampilkan informasi versi IOS dan perangkat keras
show running-config             → menampilkan konfigurasi aktif perangkat
exit / end                      → keluar satu level / kembali ke Privileged EXEC
```

D. Alat dan Bahan

Komponen	Keterangan
Perangkat Lunak	Cisco Packet Tracer (versi terbaru)
Perangkat Fisik (opsional)	1 unit switch dan/atau router Cisco IOS, kabel console, adaptor USB-to-serial
Perangkat Pendukung	Komputer/laptop mahasiswa, gelang antistatis (jika tersedia)
Dokumen Pendukung	Checklist K3 Laboratorium (Lampiran 4), Template Laporan Praktikum (Lampiran 1)

E. Langkah Kerja / Prosedur

Tahap 1 — Orientasi dan Penerapan K3 Laboratorium (± 20 menit)

1. Mengisi Checklist K3 Laboratorium (Lampiran 4) sebelum mulai bekerja.
2. Memeriksa kondisi kabel daya, kabel jaringan, dan perangkat sebelum digunakan.
3. Menata area kerja dan kabel agar tidak mengganggu akses maupun keselamatan kerja.

Tahap 2 — Pengenalan Perangkat (± 20 menit)

1. Mengidentifikasi jenis dan fungsi port pada switch/router (console, Ethernet, power).
2. Mengidentifikasi jenis kabel yang digunakan (console, straight-through, crossover).
3. Menghubungkan perangkat ke komputer melalui kabel console atau membuka topologi dasar pada Cisco Packet Tracer.

Tahap 3 — Praktik Mode CLI (± 60 menit)

1. Membuka sesi terminal/console dan mengamati prompt awal (User EXEC Mode).
2. Menjalankan perintah enable untuk masuk ke Privileged EXEC Mode dan mengamati perubahan prompt.
3. Menjalankan perintah configure terminal untuk masuk ke Global Configuration Mode.
4. Berlatih berpindah antar-mode menggunakan exit dan end, serta mengamati perbedaan prompt pada setiap mode.

Tahap 4 — Konfigurasi dan Verifikasi Dasar (± 50 menit)

1. Mengatur hostname perangkat sesuai NIM/nama mahasiswa menggunakan perintah hostname.
2. Mengatur password Privileged EXEC menggunakan perintah enable secret.
3. Menjalankan show version untuk memeriksa informasi perangkat dan versi IOS.
4. Menjalankan show running-config untuk memverifikasi konfigurasi yang telah diterapkan.
5. Mendokumentasikan setiap hasil perintah (screenshot/output CLI) sebagai bukti kerja.

Tahap 5 — Penutupan Sesi (± 20 menit)

1. Menyimpan file topologi/konfigurasi sesuai konvensi penamaan file yang berlaku.
2. Mematikan dan melepas perangkat/kabel sesuai prosedur K3 yang benar.
3. Merapikan area kerja dan mengembalikan perangkat pinjaman kepada instruktur/laboran.

F. Tugas Praktikum

Skenario: Sebuah kantor kecil akan memasang satu unit switch baru. Sebagai teknisi jaringan pemula, mahasiswa ditugaskan melakukan konfigurasi identitas dasar dan pengamanan awal perangkat tersebut sebelum diserahkan ke tim operasional.

Ketentuan tugas:

1. Membuat topologi sederhana pada Cisco Packet Tracer terdiri atas 1 switch dan 1 PC yang terhubung.
2. Mengatur hostname switch dengan format SW-[NIM] (contoh: SW-23TK0412).
3. Mengatur enable secret dengan password sesuai ketentuan instruktur.
4. Menambahkan banner motd berisi pesan peringatan akses tidak sah (unauthorized access).
5. Melakukan verifikasi menggunakan show version dan show running-config, lalu menyertakan tangkapan layar (screenshot) hasil verifikasi tersebut.
6. Menyimpan file topologi (.pkt) sesuai konvensi penamaan yang berlaku.

G. Format Laporan Praktikum

Laporan disusun mengikuti Template Laporan Praktikum (Lampiran 1) dengan struktur sebagai berikut:

1. Halaman Judul (Modul, NIM, Nama, Kelompok jika ada)
2. Tujuan Praktikum
3. Alat dan Bahan yang Digunakan

4. Langkah Kerja beserta Bukti Pelaksanaan (screenshot CLI/topologi pada setiap tahap kunci)
5. Hasil Verifikasi (output show version dan show running-config)
6. Kendala dan Solusi (jika ada)
7. Kesimpulan

Laporan dikumpulkan dalam format PDF/DOCX dengan nama file: NIM_NamaMahasiswa_Modul01_Laporan, sesuai tenggat waktu yang ditentukan instruktur.

H. Rubrik Penilaian Ringkas

Penilaian menggunakan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55). Deskriptor lengkap keempat kategori untuk setiap aspek tersedia pada Rubrik Penilaian Praktikum per Pertemuan (Lampiran 3).

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Penerapan Prosedur K3 Laboratorium	25%	Menerapkan seluruh prosedur K3 secara konsisten dan mandiri.	Mengabaikan prosedur K3 sehingga berisiko terhadap keselamatan/perangkat.
Pengenalan Perangkat & Mode CLI	30%	Mengidentifikasi seluruh komponen dan berpindah antar-mode CLI dengan lancar dan tepat.	Tidak mampu mengidentifikasi perangkat maupun mode CLI dengan benar.
Ketepatan Perintah Dasar	30%	Menjalankan perintah dasar tanpa kesalahan sintaks.	Tidak mampu menjalankan perintah dasar CLI dengan benar.
Sikap & Kedisiplinan Laboratorium	15%	Disiplin, tertib, dan proaktif selama sesi praktikum.	Tidak disiplin sehingga mengganggu jalannya praktikum.

Nilai Pertemuan 1 berkontribusi 1% terhadap komponen Tugas Praktikum (30%) pada nilai akhir mata kuliah, serta mendukung capaian CPL-2 dan CPL-12 sesuai Peta Kompetensi.

MODUL 2

KONFIGURASI VLAN DASAR UNTUK SEGMENTASI JARINGAN

A. Identitas Modul

Modul / Pertemuan	Modul 2 / Pertemuan ke-2
Judul Modul	Konfigurasi VLAN Dasar untuk Segmentasi Jaringan
Sub-CPMK	Sub-CPMK-1.2 — Mampu mengonfigurasi VLAN pada switch untuk segmentasi jaringan sesuai kebutuhan pengguna.
CPL Terkait	CPL-2, CPL-5
Metode Pembelajaran	Demonstrasi, praktikum terbimbing (guided lab), studi kasus
Alokasi Waktu	170 menit (1 sks praktik)
Bobot Nilai	Kontribusi 2% dari komponen Tugas Praktikum (30%)

B. Tujuan Praktikum

Setelah mengikuti praktikum ini, mahasiswa diharapkan mampu:

1. Menjelaskan manfaat dan cara kerja Virtual LAN (VLAN) dalam segmentasi jaringan secara tepat dan runtut.
2. Membuat dan menamai VLAN pada switch sesuai skenario segmentasi departemen/pengguna.
3. Menempatkan port access pada VLAN yang sesuai dengan kebutuhan segmentasi.
4. Memverifikasi isolasi antar-VLAN dan konektivitas dalam VLAN yang sama secara mandiri dan akurat.

C. Dasar Teori Ringkas

1. Konsep Segmentasi VLAN

Virtual LAN (VLAN) adalah teknik segmentasi jaringan pada lapisan data link yang memungkinkan satu switch fisik dibagi menjadi beberapa broadcast domain logis secara independen, tanpa memerlukan perangkat fisik tambahan. Setiap VLAN memiliki domain broadcast tersendiri, sehingga trafik broadcast pada satu VLAN tidak diteruskan ke VLAN lain kecuali melalui perangkat routing.

Segmentasi VLAN memberikan manfaat berupa peningkatan keamanan (isolasi trafik antar-departemen), efisiensi bandwidth (mengurangi domain broadcast), serta fleksibilitas manajemen jaringan tanpa bergantung pada lokasi fisik perangkat pengguna.

2. Jenis Port pada VLAN

- Access Port — port yang hanya menjadi anggota satu VLAN tertentu; umum digunakan untuk menghubungkan perangkat pengguna akhir (PC, printer).
- VLAN ID — angka identitas unik (1–4094) yang membedakan satu VLAN dengan VLAN lainnya; VLAN 1 merupakan VLAN default bawaan perangkat Cisco IOS.
- VLAN Database — tabel internal switch yang menyimpan daftar VLAN beserta nama dan status aktifnya.

3. Perintah Dasar Konfigurasi VLAN

```
vlan <id>                        → membuat/masuk ke VLAN tertentu
name <nama_vlan>                 → memberi nama pada VLAN
interface <tipe/nomor>           → masuk ke konfigurasi interface tertentu
switchport mode access           → mengatur port menjadi access port
switchport access vlan <id>      → menempatkan port ke VLAN tertentu
show vlan brief                  → menampilkan ringkasan VLAN dan keanggotaan
port
```

D. Alat dan Bahan

Komponen	Keterangan
Perangkat Lunak	Cisco Packet Tracer (versi terbaru)
Perangkat Fisik (opsional)	1 unit switch Cisco IOS dengan minimal 4 port aktif
Perangkat Pendukung	4 unit PC/end device, kabel straight-through
Dokumen Pendukung	Template Laporan Praktikum (Lampiran 1), Topologi Referensi Modul 2 (Lampiran 2)

E. Langkah Kerja / Prosedur

Tahap 1 — Persiapan Topologi (± 20 menit)

1. Membuka Cisco Packet Tracer dan membangun topologi 1 switch dengan 4 PC sesuai skenario segmentasi departemen (Marketing, Keuangan, IT, Produksi).
2. Menghubungkan setiap PC ke port switch menggunakan kabel straight-through dan memberikan alamat IP sesuai skema yang ditentukan instruktur.

Tahap 2 — Pembuatan dan Penamaan VLAN (± 40 menit)

1. Masuk ke Global Configuration Mode pada switch.
2. Membuat 4 VLAN dengan ID sesuai skenario (contoh: VLAN 10 Marketing, VLAN 20 Keuangan, VLAN 30 IT, VLAN 40 Produksi) menggunakan perintah vlan <id>.
3. Memberi nama setiap VLAN menggunakan perintah name sesuai departemen terkait.
4. Memverifikasi VLAN database menggunakan show vlan brief.

Tahap 3 — Penempatan Port Access (± 40 menit)

1. Masuk ke konfigurasi setiap interface yang terhubung ke PC.
2. Mengatur mode port menjadi access menggunakan switchport mode access.
3. Menempatkan setiap port ke VLAN yang sesuai menggunakan switchport access vlan <id>.
4. Mengulangi langkah untuk seluruh port yang digunakan pada topologi.

Tahap 4 — Verifikasi Konektivitas (± 50 menit)

1. Melakukan ping antar-PC dalam VLAN yang sama dan mengamati hasil (berhasil).
2. Melakukan ping antar-PC pada VLAN berbeda dan mengamati hasil (gagal/isolasi VLAN).
3. Memverifikasi keanggotaan port pada setiap VLAN menggunakan show vlan brief dan show interfaces status.
4. Mendokumentasikan seluruh hasil pengujian (screenshot) sebagai bukti kerja.

Tahap 5 — Penutupan Sesi (± 20 menit)

1. Menyimpan file topologi (.pkt) sesuai konvensi penamaan file yang berlaku.
2. Merapikan area kerja dan mengembalikan perangkat sesuai prosedur K3.

F. Tugas Praktikum

Skenario: Sebuah kantor cabang memiliki 4 departemen (Marketing, Keuangan, IT, Produksi) yang harus dipisahkan secara logis dalam satu switch fisik untuk alasan keamanan dan efisiensi jaringan.

Ketentuan tugas:

1. Membuat 4 VLAN dengan ID dan nama sesuai departemen yang ditentukan instruktur.
2. Menempatkan minimal 1 PC pada setiap VLAN sesuai topologi yang disiapkan.
3. Melakukan pengujian konektivitas: antar-PC dalam VLAN yang sama (harus berhasil) dan antar-PC pada VLAN berbeda (harus terisolasi).
4. Menyertakan tangkapan layar (screenshot) hasil show vlan brief dan hasil pengujian ping.
5. Menyimpan file topologi (.pkt) sesuai konvensi penamaan yang berlaku.

G. Format Laporan Praktikum

Laporan disusun mengikuti Template Laporan Praktikum (Lampiran 1) dengan struktur sebagai berikut:

1. Halaman Judul (Modul, NIM, Nama, Kelompok jika ada)
2. Tujuan Praktikum
3. Alat dan Bahan yang Digunakan
4. Skema Segmentasi VLAN (tabel VLAN ID, nama, dan keanggotaan port)
5. Langkah Kerja beserta Bukti Pelaksanaan (screenshot konfigurasi dan verifikasi)
6. Hasil Pengujian Konektivitas Antar-Segmen
7. Kendala dan Solusi (jika ada)
8. Kesimpulan

Laporan dikumpulkan dalam format PDF/DOCX dengan nama file:
NIM_NamaMahasiswa_Modul02_Laporan, sesuai tenggat waktu yang ditentukan instruktur.

H. Rubrik Penilaian Ringkas

Penilaian menggunakan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55). Deskriptor lengkap keempat kategori untuk setiap aspek tersedia pada Rubrik Penilaian Praktikum per Pertemuan (Lampiran 3).

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Pemahaman Konsep Segmentasi VLAN	15%	Mampu menjelaskan manfaat dan cara kerja VLAN dalam segmentasi jaringan secara tepat dan runtut.	Tidak memahami konsep dasar VLAN.
Ketepatan Konfigurasi VLAN	40%	Seluruh VLAN dikonfigurasi sesuai skenario (ID, nama, penempatan	VLAN tidak terkonfigurasi atau konfigurasi salah secara

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
		port access) tanpa kesalahan.	keseluruhan.
Verifikasi Konektivitas Antar-Segmen	25%	Mampu memverifikasi isolasi antar-VLAN dan konektivitas dalam VLAN yang sama secara mandiri dan akurat.	Tidak melakukan verifikasi atau hasil verifikasi keliru.
Dokumentasi Laporan Praktikum	20%	Laporan lengkap dan sistematis, disertai bukti konfigurasi dan hasil uji.	Tidak menyusun laporan praktikum.

Nilai Pertemuan 2 berkontribusi 2% terhadap komponen Tugas Praktikum (30%) pada nilai akhir mata kuliah, serta mendukung capaian CPL-2 dan CPL-5 sesuai Peta Kompetensi.

MODUL 3

TRUNKING 802.1Q DAN VLAN TRUNKING PROTOCOL (VTP)

A. Identitas Modul

Modul / Pertemuan	Modul 3 / Pertemuan ke-3
Judul Modul	Trunking 802.1Q dan VLAN Trunking Protocol (VTP)
Sub-CPMK	Sub-CPMK-1.3 — Mampu mengonfigurasi trunking (802.1Q) dan VLAN Trunking Protocol (VTP) untuk propagasi VLAN antar-switch.
CPL Terkait	CPL-2, CPL-5
Metode Pembelajaran	Demonstrasi, praktikum terbimbing, diskusi troubleshooting
Alokasi Waktu	170 menit (1 sks praktik)
Bobot Nilai	Kontribusi 2% dari komponen Tugas Praktikum (30%)

B. Tujuan Praktikum

Setelah mengikuti praktikum ini, mahasiswa diharapkan mampu:

1. Memahami perbedaan access port dan trunk port serta fungsi VTP domain/mode secara tepat.
2. Mengonfigurasi trunk 802.1Q antar-switch untuk membawa trafik multi-VLAN pada satu tautan fisik.
3. Mengonfigurasi VTP domain dan mode (server/client) untuk propagasi VLAN antar-switch.
4. Memverifikasi status trunk dan konsistensi VLAN database antar-switch secara akurat.

C. Dasar Teori Ringkas

1. Trunking 802.1Q

Trunk port adalah jenis port switch yang membawa trafik dari beberapa VLAN sekaligus melalui satu tautan fisik antar-switch, menggunakan mekanisme tagging IEEE 802.1Q. Setiap frame yang melewati trunk diberi tag VLAN ID pada header Ethernet sehingga switch penerima dapat mengetahui VLAN asal frame tersebut. Trunk umum digunakan pada tautan antar-switch (switch-to-switch) atau antara switch dan router (router-on-a-stick).

VLAN native merupakan satu-satunya VLAN pada trunk yang trafiknya dikirim tanpa tag; secara default VLAN native adalah VLAN 1, namun sebaiknya diubah sesuai kebijakan keamanan untuk menghindari VLAN hopping.

2. VLAN Trunking Protocol (VTP)

VTP adalah protokol Cisco yang memungkinkan propagasi informasi VLAN (penambahan, penghapusan, atau pengubahan nama VLAN) secara otomatis ke seluruh switch dalam satu domain VTP, sehingga administrator tidak perlu mengonfigurasi VLAN secara manual pada setiap switch.

- VTP Server — mode yang dapat membuat, mengubah, dan menghapus VLAN, serta menyebarkan perubahan ke switch lain dalam domain yang sama (mode default).

- VTP Client — mode yang menerima dan meneruskan informasi VLAN dari server, namun tidak dapat mengubah VLAN database secara lokal.
- VTP Transparent — mode yang meneruskan iklan VTP tanpa memproses maupun menyinkronkan VLAN database miliknya sendiri.

3. Perintah Dasar Konfigurasi Trunk dan VTP

```
switchport mode trunk                → mengatur port menjadi trunk port
switchport trunk native vlan <id>    → mengubah VLAN native pada trunk
vtp domain <nama_domain>             → mengatur nama domain VTP
vtp mode server|client|transparent   → mengatur mode VTP
vtp password <password>              → mengamankan domain VTP dengan password
show interfaces trunk                → menampilkan status port trunk
show vtp status                      → menampilkan status dan konfigurasi VTP
```

D. Alat dan Bahan

Komponen	Keterangan
Perangkat Lunak	Cisco Packet Tracer (versi terbaru)
Perangkat Fisik (opsional)	2–3 unit switch Cisco IOS dengan minimal 2 port uplink
Perangkat Pendukung	PC/end device secukupnya, kabel straight-through dan crossover
Dokumen Pendukung	Template Laporan Praktikum (Lampiran 1), Topologi Referensi Modul 3 (Lampiran 2)

E. Langkah Kerja / Prosedur

Tahap 1 — Persiapan Topologi Multi-Switch (± 20 menit)

1. Membangun topologi 3 switch yang saling terhubung (misalnya topologi segitiga/star) dengan beberapa PC pada VLAN yang sama di masing-masing switch, melanjutkan konfigurasi VLAN dari Modul 2.
2. Menghubungkan antar-switch menggunakan kabel crossover/otomatis (auto-MDIX) pada port uplink.

Tahap 2 — Konfigurasi Trunk 802.1Q (± 40 menit)

1. Masuk ke interface uplink antar-switch dan mengatur mode menjadi trunk menggunakan switchport mode trunk.
2. Mengatur VLAN native (opsional, sesuai kebijakan) menggunakan switchport trunk native vlan.
3. Mengulangi konfigurasi trunk pada seluruh port uplink antar-switch.
4. Memverifikasi status trunk menggunakan show interfaces trunk.

Tahap 3 — Konfigurasi VTP Domain dan Mode (± 40 menit)

1. Menentukan satu switch sebagai VTP Server dan switch lain sebagai VTP Client sesuai skenario.
2. Mengatur nama domain VTP yang sama pada seluruh switch menggunakan vtp domain.
3. Mengatur mode VTP pada masing-masing switch menggunakan vtp mode.
4. Menambahkan password VTP (opsional) untuk keamanan domain.

Tahap 4 — Pengujian Propagasi VLAN (± 50 menit)

1. Menambahkan VLAN baru pada VTP Server dan mengamati apakah VLAN tersebut otomatis muncul pada switch VTP Client.
2. Memverifikasi konsistensi VLAN database antar-switch menggunakan show vlan brief dan show vtp status pada setiap switch.
3. Menguji konektivitas antar-PC pada VLAN yang sama di switch berbeda untuk membuktikan propagasi VLAN berhasil.
4. Mendokumentasikan hasil pengujian (screenshot) sebagai bukti kerja.

Tahap 5 — Penutupan Sesi (± 20 menit)

1. Menyimpan file topologi (.pkt) sesuai konvensi penamaan file yang berlaku.
2. Merapikan area kerja dan mengembalikan perangkat sesuai prosedur K3.

F. Tugas Praktikum

Skenario: Sebuah kampus memiliki 3 gedung yang masing-masing memiliki switch akses, dan seluruh switch harus memiliki VLAN database yang konsisten agar mahasiswa pada VLAN yang sama di gedung berbeda tetap dapat saling terhubung.

Ketentuan tugas:

1. Mengonfigurasi trunk 802.1Q pada seluruh tautan antar-switch.
2. Menentukan satu switch pusat sebagai VTP Server dan dua switch lainnya sebagai VTP Client dalam domain VTP yang sama.
3. Menambahkan minimal 1 VLAN baru pada VTP Server dan membuktikan VLAN tersebut terpropagasi ke seluruh switch client.
4. Menyertakan tangkapan layar (screenshot) hasil show interfaces trunk dan show vtp status dari setiap switch.
5. Menyimpan file topologi (.pkt) sesuai konvensi penamaan yang berlaku.

G. Format Laporan Praktikum

Laporan disusun mengikuti Template Laporan Praktikum (Lampiran 1) dengan struktur sebagai berikut:

1. Halaman Judul (Modul, NIM, Nama, Kelompok jika ada)
2. Tujuan Praktikum
3. Alat dan Bahan yang Digunakan
4. Skema Trunk dan Domain VTP (topologi, mode VTP tiap switch)
5. Langkah Kerja beserta Bukti Pelaksanaan (screenshot konfigurasi dan verifikasi)
6. Hasil Pengujian Propagasi VLAN
7. Kendala dan Solusi (jika ada)
8. Kesimpulan

Laporan dikumpulkan dalam format PDF/DOCX dengan nama file:
NIM_NamaMahasiswa_Modul03_Laporan, sesuai tenggat waktu yang ditentukan instruktur.

H. Rubrik Penilaian Ringkas

Penilaian menggunakan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55). Deskriptor lengkap keempat kategori untuk setiap aspek tersedia pada Rubrik Penilaian Praktikum per Pertemuan (Lampiran 3).

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Pemahaman Konsep Trunk & VTP	15%	Memahami perbedaan access port dan trunk port serta fungsi VTP domain/mode secara tepat.	Tidak memahami konsep trunking maupun VTP.
Ketepatan Konfigurasi Trunk & VTP	40%	Trunk 802.1Q dan VTP domain/mode terkonfigurasi tepat pada seluruh switch topologi.	Trunk/VTP tidak terkonfigurasi atau konfigurasi salah secara keseluruhan.
Verifikasi Propagasi VLAN	25%	Memverifikasi status trunk dan konsistensi VLAN database antar-switch secara akurat.	Tidak melakukan verifikasi propagasi VLAN.
Dokumentasi Laporan Praktikum	20%	Laporan lengkap, sistematis, disertai bukti status trunk/VTP dan hasil uji propagasi.	Tidak menyusun laporan praktikum.

Nilai Pertemuan 3 berkontribusi 2% terhadap komponen Tugas Praktikum (30%) pada nilai akhir mata kuliah, serta mendukung capaian CPL-2 dan CPL-5 sesuai Peta Kompetensi.

MODUL 4

ETHERCHANNEL (LINK AGGREGATION) DENGAN LACP/PAGP

A. Identitas Modul

Modul / Pertemuan	Modul 4 / Pertemuan ke-4
Judul Modul	EtherChannel (Link Aggregation) dengan LACP/PAgP
Sub-CPMK	Sub-CPMK-1.4 — Mampu mengonfigurasi EtherChannel (LACP/PAgP) untuk agregasi tautan (link aggregation) antar-switch.
CPL Terkait	CPL-2, CPL-5
Metode Pembelajaran	Praktikum mandiri terbimbing, studi kasus redundansi tautan
Alokasi Waktu	170 menit (1 sks praktik)
Bobot Nilai	Kontribusi 2% dari komponen Tugas Praktikum (30%)

B. Tujuan Praktikum

Setelah mengikuti praktikum ini, mahasiswa diharapkan mampu:

1. Memahami tujuan agregasi tautan (link aggregation) dan perbedaan mode protokol LACP dan PAgP secara tepat.
2. Mengonfigurasi EtherChannel antar-switch menggunakan protokol LACP atau PAgP sesuai skenario yang ditentukan.
3. Menguji unjuk kerja agregasi bandwidth pada bundle EtherChannel yang terbentuk.
4. Menguji dan membuktikan proses failover ketika salah satu tautan anggota EtherChannel diputus.

C. Dasar Teori Ringkas

1. Konsep Link Aggregation (EtherChannel)

EtherChannel adalah teknologi yang menggabungkan beberapa tautan (link) fisik antar-switch menjadi satu tautan logis, sehingga meningkatkan total bandwidth yang tersedia serta menyediakan redundansi tautan. Apabila satu tautan anggota mengalami kegagalan, trafik akan secara otomatis dialihkan ke tautan anggota lain yang masih aktif tanpa memutus konektivitas jaringan secara keseluruhan.

2. Protokol Negosiasi EtherChannel

- Link Aggregation Control Protocol (LACP) — protokol standar terbuka (IEEE 802.3ad) yang memiliki mode active (menginisiasi negosiasi) dan passive (menunggu negosiasi dari sisi lain).
- Port Aggregation Protocol (PAgP) — protokol milik Cisco (proprietary) yang memiliki mode desirable (menginisiasi negosiasi) dan auto (menunggu negosiasi dari sisi lain).

Kedua ujung tautan EtherChannel harus menggunakan protokol dan mode yang kompatibel (misalnya active-active atau active-passive untuk LACP) agar bundle dapat terbentuk dengan benar; ketidaksesuaian mode (mode mismatch) akan menyebabkan EtherChannel gagal terbentuk.

3. Perintah Dasar Konfigurasi EtherChannel

```
interface range <tipe/awal-akhir>       → memilih beberapa interface sekaligus
channel-group <no> mode active|passive  → membentuk EtherChannel dengan LACP
channel-group <no> mode desirable|auto  → membentuk EtherChannel dengan PAgP
show etherchannel summary               → menampilkan ringkasan status EtherChannel
show interfaces port-channel <no>       → menampilkan detail interface logis Port-Channel
```

D. Alat dan Bahan

Komponen	Keterangan
Perangkat Lunak	Cisco Packet Tracer (versi terbaru)
Perangkat Fisik (opsional)	2 unit switch Cisco IOS dengan minimal 2 port uplink yang identik
Perangkat Pendukung	PC/end device secukupnya, kabel straight-through/crossover
Dokumen Pendukung	Template Laporan Praktikum (Lampiran 1), Topologi Referensi Modul 4 (Lampiran 2)

E. Langkah Kerja / Prosedur

Tahap 1 — Persiapan Topologi Dua Tautan Paralel (± 20 menit)

1. Membangun topologi 2 switch yang dihubungkan dengan 2 kabel paralel pada port yang identik jenis dan kecepatannya.
2. Memastikan konfigurasi trunk (jika diperlukan sesuai skenario) sudah konsisten pada kedua port sebelum membentuk EtherChannel.

Tahap 2 — Konfigurasi EtherChannel (± 50 menit)

1. Memilih kedua interface uplink menggunakan interface range.
2. Membentuk EtherChannel menggunakan channel-group dengan mode LACP (active/passive) sesuai penugasan instruktur.
3. Mengulangi konfigurasi yang kompatibel pada switch di sisi lain tautan.
4. Memverifikasi status bundle menggunakan show etherchannel summary hingga status menunjukkan bundle aktif (P).

Tahap 3 — Pengujian Agregasi Bandwidth (± 30 menit)

1. Mengirimkan trafik data (ping berkelanjutan/simulasi trafik) melalui Port-Channel yang terbentuk.
2. Mengamati distribusi trafik pada kedua tautan anggota menggunakan show interfaces port-channel.

Tahap 4 — Pengujian Failover Tautan (± 40 menit)

1. Memutus salah satu tautan anggota EtherChannel (menonaktifkan port atau mencabut kabel pada simulasi).
2. Mengamati apakah konektivitas tetap terjaga melalui tautan anggota yang masih aktif (failover otomatis).

3. Memverifikasi status EtherChannel setelah failover menggunakan show etherchannel summary.
4. Mengaktifkan kembali tautan yang diputus dan memverifikasi bundle kembali normal.
5. Mendokumentasikan hasil pengujian (screenshot) sebagai bukti kerja.

Tahap 5 — Penutupan Sesi (± 10 menit)

1. Menyimpan file topologi (.pkt) sesuai konvensi penamaan file yang berlaku.
2. Merapikan area kerja dan mengembalikan perangkat sesuai prosedur K3.

F. Tugas Praktikum

Skenario: Tautan tunggal antar-switch pada jaringan kantor pusat menjadi bottleneck bandwidth dan titik kegagalan tunggal (single point of failure). Sebagai teknisi jaringan, mahasiswa ditugaskan membentuk EtherChannel untuk meningkatkan kapasitas dan keandalan tautan tersebut.

Ketentuan tugas:

1. Membentuk EtherChannel menggunakan 2 tautan fisik antar-switch dengan protokol LACP mode active-active.
2. Memverifikasi bundle EtherChannel terbentuk sempurna (seluruh port anggota berstatus bundled).
3. Melakukan pengujian failover dengan memutus salah satu tautan anggota dan membuktikan konektivitas tetap terjaga.
4. Menyertakan tangkapan layar (screenshot) hasil show etherchannel summary sebelum dan sesudah pengujian failover.
5. Menyimpan file topologi (.pkt) sesuai konvensi penamaan yang berlaku.

G. Format Laporan Praktikum

Laporan disusun mengikuti Template Laporan Praktikum (Lampiran 1) dengan struktur sebagai berikut:

1. Halaman Judul (Modul, NIM, Nama, Kelompok jika ada)
2. Tujuan Praktikum
3. Alat dan Bahan yang Digunakan
4. Skema Tautan dan Mode EtherChannel yang Digunakan
5. Langkah Kerja beserta Bukti Pelaksanaan (screenshot konfigurasi dan verifikasi)
6. Hasil Pengujian Redundansi Tautan (Failover)
7. Kendala dan Solusi (jika ada)
8. Kesimpulan

Laporan dikumpulkan dalam format PDF/DOCX dengan nama file:
NIM_NamaMahasiswa_Modul04_Laporan, sesuai tenggat waktu yang ditentukan instruktur.

H. Rubrik Penilaian Ringkas

Penilaian menggunakan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55). Deskriptor lengkap keempat kategori untuk setiap aspek tersedia pada Rubrik Penilaian Praktikum per Pertemuan (Lampiran 3).

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Pemahaman Konsep Link Aggregation	15%	Memahami tujuan agregasi tautan dan perbedaan mode LACP/PAgP secara tepat.	Tidak memahami konsep link aggregation.
Ketepatan Konfigurasi EtherChannel	40%	EtherChannel terbentuk sempurna (bundle aktif) sesuai mode yang ditentukan pada seluruh port anggota.	EtherChannel gagal terbentuk atau konfigurasi salah total.
Pengujian Redundansi Tautan	25%	Menguji dan membuktikan agregasi bandwidth serta failover saat salah satu tautan diputus, hasil sesuai ekspektasi.	Tidak melakukan pengujian redundansi tautan.
Dokumentasi Laporan Praktikum	20%	Laporan lengkap dan sistematis, disertai bukti status EtherChannel dan hasil uji failover.	Tidak menyusun laporan praktikum.

Nilai Pertemuan 4 berkontribusi 2% terhadap komponen Tugas Praktikum (30%) pada nilai akhir mata kuliah, serta mendukung capaian CPL-2 dan CPL-5 sesuai Peta Kompetensi. Modul ini menutup rangkaian CPMK-1 (Modul 1–4).

MODUL 5

ROUTING ANTAR-VLAN: ROUTER-ON-A-STICK DAN LAYER-3 SWITCHING

A. Identitas Modul

Modul / Pertemuan	Modul 5 / Pertemuan ke-5
Judul Modul	Routing Antar-VLAN: Router-on-a-Stick dan Layer-3 Switching
Sub-CPMK	Sub-CPMK-2.1 — Mampu mengonfigurasi routing antar-VLAN menggunakan metode router-on-a-stick dan Layer-3 switching.
CPL Terkait	CPL-2, CPL-5
Metode Pembelajaran	Demonstrasi, praktikum terbimbing, studi kasus
Alokasi Waktu	170 menit (1 sks praktik)
Bobot Nilai	Kontribusi 2% dari komponen Tugas Praktikum (30%)

B. Tujuan Praktikum

Setelah mengikuti praktikum ini, mahasiswa diharapkan mampu:

1. Memahami perbedaan pendekatan router-on-a-stick dan Layer-3 switching (SVI) untuk routing antar-VLAN secara tepat.
2. Mengonfigurasi sub-interface pada router (router-on-a-stick) agar antar-VLAN dapat saling berkomunikasi.
3. Mengonfigurasi Switch Virtual Interface (SVI) pada switch Layer-3 sebagai gateway antar-VLAN.
4. Memverifikasi konektivitas antar-VLAN secara menyeluruh dan akurat melalui pengujian end-to-end.

C. Dasar Teori Ringkas

1. Kebutuhan Routing Antar-VLAN

VLAN yang telah disegmentasi (Modul 2–3) bersifat terisolasi satu sama lain pada lapisan data link, sehingga host pada VLAN berbeda tidak dapat saling berkomunikasi tanpa bantuan perangkat routing pada lapisan network. Terdapat dua pendekatan umum untuk mengatasi kebutuhan ini: router-on-a-stick dan Layer-3 switching.

2. Router-on-a-Stick

Pendekatan ini menggunakan satu interface fisik router yang dihubungkan ke trunk port switch, kemudian dibagi menjadi beberapa sub-interface logis—masing-masing mewakili satu VLAN dengan alamat IP gateway tersendiri serta konfigurasi encapsulation dot1Q untuk menandai VLAN ID yang diwakilinya.

3. Layer-3 Switching (Switch Virtual Interface)

Pendekatan ini memanfaatkan switch yang mendukung fungsi routing (Layer-3 switch) dengan membuat Switch Virtual Interface (SVI) untuk setiap VLAN. Setiap SVI berfungsi sebagai gateway VLAN

tersebut secara langsung pada switch, tanpa memerlukan router eksternal maupun trunk tambahan ke luar switch, sehingga performa routing antar-VLAN menjadi lebih cepat (dilakukan di ASIC switch, bukan melalui CPU router).

4. Perintah Dasar Konfigurasi

```
Router-on-a-Stick:
interface <tipe>.<sub-id>              → membuat sub-interface
encapsulation dot1Q <vlan-id>          → menandai sub-interface untuk VLAN
tertentu
ip address <ip> <subnet>               → mengatur alamat IP gateway sub-
interface
Layer-3 Switching (SVI):
ip routing                             → mengaktifkan fungsi routing pada
switch
interface vlan <id>                    → membuat/masuk ke SVI VLAN tertentu
ip address <ip> <subnet>               → mengatur alamat IP gateway SVI
no shutdown                            → mengaktifkan interface SVI
```

D. Alat dan Bahan

Komponen	Keterangan
Perangkat Lunak	Cisco Packet Tracer (versi terbaru)
Perangkat Fisik (opsional)	1 router dan 1 switch (skenario A) atau 1 switch Layer-3 (skenario B)
Perangkat Pendukung	PC pada minimal 2 VLAN berbeda, kabel straight-through/crossover
Dokumen Pendukung	Template Laporan Praktikum (Lampiran 1), Topologi Referensi Modul 5 (Lampiran 2)

E. Langkah Kerja / Prosedur

Tahap 1 — Persiapan Topologi (± 20 menit)

1. Melanjutkan topologi VLAN dari Modul 2–3 (minimal 2 VLAN dengan host masing-masing).
2. Menghubungkan router ke switch melalui trunk port (skenario router-on-a-stick), atau menyiapkan switch Layer-3 (skenario L3 switching), sesuai penugasan instruktur.

Tahap 2 — Konfigurasi Router-on-a-Stick (± 45 menit)

1. Masuk ke interface fisik router yang terhubung ke trunk switch dan membuat sub-interface untuk setiap VLAN.
2. Mengonfigurasi encapsulation dot1Q pada setiap sub-interface sesuai VLAN ID terkait.
3. Mengatur alamat IP gateway pada setiap sub-interface sesuai skema pengalamatan VLAN.
4. Mengaktifkan interface fisik router menggunakan no shutdown.

Tahap 3 — Konfigurasi Layer-3 Switching / SVI (± 45 menit)

1. Mengaktifkan fungsi routing pada switch menggunakan ip routing.
2. Membuat SVI untuk setiap VLAN dan mengatur alamat IP gateway masing-masing.
3. Mengaktifkan setiap SVI menggunakan no shutdown.

Tahap 4 — Verifikasi Konektivitas End-to-End (± 40 menit)

1. Mengatur default gateway pada setiap PC sesuai sub-interface/SVI VLAN yang bersangkutan.
2. Melakukan ping antar-host pada VLAN berbeda dan memastikan konektivitas berhasil.
3. Memverifikasi tabel routing pada router/switch Layer-3 menggunakan show ip route.
4. Mendokumentasikan hasil pengujian (screenshot) sebagai bukti kerja.

Tahap 5 — Penutupan Sesi (± 20 menit)

1. Menyimpan file topologi (.pkt) sesuai konvensi penamaan file yang berlaku.
2. Merapikan area kerja dan mengembalikan perangkat sesuai prosedur K3.

F. Tugas Praktikum

Skenario: Kantor cabang yang telah menerapkan segmentasi VLAN pada Modul 2 kini memerlukan komunikasi antar-departemen (misalnya Marketing perlu mengakses server pada VLAN IT). Mahasiswa ditugaskan mengimplementasikan routing antar-VLAN menggunakan salah satu dari dua pendekatan yang dipelajari.

Ketentuan tugas:

1. Mengimplementasikan routing antar-VLAN untuk minimal 3 VLAN menggunakan metode router-on-a-stick ATAU Layer-3 switching sesuai penugasan instruktur.
2. Mengatur alamat IP gateway yang sesuai pada setiap sub-interface/SVI.
3. Membuktikan seluruh host pada VLAN berbeda dapat saling terhubung (ping berhasil end-to-end).
4. Menyertakan tangkapan layar (screenshot) hasil show ip route dan hasil pengujian ping antar-VLAN.
5. Menyimpan file topologi (.pkt) sesuai konvensi penamaan yang berlaku.

G. Format Laporan Praktikum

Laporan disusun mengikuti Template Laporan Praktikum (Lampiran 1) dengan struktur sebagai berikut:

1. Halaman Judul (Modul, NIM, Nama, Kelompok jika ada)
2. Tujuan Praktikum
3. Alat dan Bahan yang Digunakan
4. Skema Pengalamatan IP Antar-VLAN (tabel VLAN, gateway, subnet)
5. Langkah Kerja beserta Bukti Pelaksanaan (screenshot konfigurasi dan verifikasi)
6. Hasil Pengujian Konektivitas End-to-End
7. Kendala dan Solusi (jika ada)
8. Kesimpulan

Laporan dikumpulkan dalam format PDF/DOCX dengan nama file:
NIM_NamaMahasiswa_Modul05_Laporan, sesuai tenggat waktu yang ditentukan instruktur.

H. Rubrik Penilaian Ringkas

Penilaian menggunakan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55). Deskriptor lengkap keempat kategori untuk setiap aspek tersedia pada Rubrik Penilaian Praktikum per Pertemuan (Lampiran 3).

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Pemahaman Konsep Routing Antar-VLAN	15%	Memahami perbedaan pendekatan router-on-a-stick dan Layer-3 switching (SVI) secara tepat.	Tidak memahami konsep routing antar-VLAN.
Ketepatan Konfigurasi Sub-interface/SVI	40%	Sub-interface router atau SVI switch dikonfigurasi tepat (encapsulation dot1Q, IP address) sesuai skenario.	Sub-interface/SVI tidak terkonfigurasi atau konfigurasi salah total.
Verifikasi Konektivitas End-to-End	25%	Memverifikasi konektivitas antar-VLAN secara menyeluruh dan akurat (ping antar-host lintas VLAN).	Tidak melakukan verifikasi konektivitas.
Dokumentasi Laporan Praktikum	20%	Laporan lengkap dan sistematis, disertai skema pengalamatan IP dan bukti hasil uji.	Tidak menyusun laporan praktikum.

Nilai Pertemuan 5 berkontribusi 2% terhadap komponen Tugas Praktikum (30%) pada nilai akhir mata kuliah, serta mendukung capaian CPL-2 dan CPL-5 sesuai Peta Kompetensi. Modul ini membuka rangkaian CPMK-2 (Modul 5–7, topik routing).

MODUL 6

ROUTING DINAMIS OSPF SINGLE-AREA

A. Identitas Modul

Modul / Pertemuan	Modul 6 / Pertemuan ke-6
Judul Modul	Routing Dinamis OSPF Single-Area
Sub-CPMK	Sub-CPMK-2.2 — Mampu mengonfigurasi routing dinamis OSPF single-area pada topologi jaringan enterprise sederhana.
CPL Terkait	CPL-2, CPL-5
Metode Pembelajaran	Demonstrasi, praktikum terbimbing, diskusi kelompok kecil
Alokasi Waktu	170 menit (1 sks praktik)
Bobot Nilai	Kontribusi 2% dari komponen Tugas Praktikum (30%)

B. Tujuan Praktikum

Setelah mengikuti praktikum ini, mahasiswa diharapkan mampu:

1. Memahami konsep area, router-id, cost, dan proses pembentukan neighbor adjacency pada OSPF secara tepat.
2. Mengonfigurasi routing dinamis OSPF single-area pada seluruh router dalam topologi jaringan enterprise sederhana.
3. Memverifikasi status neighbor adjacency antar-router menggunakan perintah show yang sesuai.
4. Memverifikasi dan menganalisis tabel routing hasil pembelajaran OSPF secara akurat.

C. Dasar Teori Ringkas

1. Konsep Dasar OSPF

Open Shortest Path First (OSPF) adalah protokol routing dinamis berbasis link-state yang menghitung jalur terpendek menggunakan algoritma Dijkstra. Berbeda dengan routing statis, OSPF memungkinkan router secara otomatis mempelajari dan menyesuaikan rute ketika terjadi perubahan topologi jaringan.

2. Area, Router-ID, dan Cost

- Area — pengelompokan logis router OSPF; pada implementasi single-area, seluruh router berada dalam satu area yang sama (umumnya Area 0/backbone area).
- Router-ID — angka identitas unik 32-bit yang membedakan setiap router OSPF, umumnya diambil dari alamat IP interface loopback tertinggi atau ditentukan secara manual.
- Cost — metrik OSPF yang dihitung berdasarkan bandwidth interface; jalur dengan total cost terendah dipilih sebagai jalur terbaik menuju suatu tujuan.

3. Pembentukan Neighbor Adjacency

Dua router OSPF yang terhubung langsung akan saling bertukar paket Hello untuk membentuk hubungan neighbor. Status adjacency berkembang melalui beberapa tahap (Down, Init, 2-Way, ExStart, Exchange, Loading) hingga mencapai status FULL, yang menandakan kedua router telah menyinkronkan link-state database secara lengkap.

4. Perintah Dasar Konfigurasi OSPF

```
router ospf <process-id>                  → mengaktifkan proses OSPF pada router
router-id <id>                            → mengatur router-id secara manual
network <network> <wildcard> area <id>    → mengikutsertakan interface ke dalam
OSPF area
show ip ospf neighbor                     → menampilkan status neighbor adjacency
show ip route                             → menampilkan tabel routing (rute OSPF
ditandai kode O)
show ip protocols                         → menampilkan ringkasan parameter
routing protocol aktif
```

D. Alat dan Bahan

Komponen	Keterangan
Perangkat Lunak	Cisco Packet Tracer (versi terbaru)
Perangkat Fisik (opsional)	Minimal 3 unit router Cisco IOS yang saling terhubung
Perangkat Pendukung	PC/end device pada segmen jaringan setiap router, kabel serial/Ethernet sesuai topologi
Dokumen Pendukung	Template Laporan Praktikum (Lampiran 1), Topologi Referensi Modul 6 (Lampiran 2)

E. Langkah Kerja / Prosedur

Tahap 1 — Persiapan Topologi Tiga Router (± 25 menit)

1. Membangun topologi minimal 3 router yang saling terhubung (topologi segitiga atau linear) beserta segmen LAN pada masing-masing router.
2. Mengatur alamat IP pada seluruh interface router dan PC sesuai skema pengalamatan yang ditentukan.

Tahap 2 — Konfigurasi Dasar OSPF (± 45 menit)

1. Mengaktifkan proses OSPF pada setiap router menggunakan router ospf <process-id>.
2. Mengatur router-id secara manual pada setiap router (opsional, namun disarankan untuk memudahkan identifikasi).
3. Mengikutsertakan seluruh network yang terhubung langsung ke dalam Area 0 menggunakan perintah network.

Tahap 3 — Verifikasi Neighbor Adjacency (± 35 menit)

1. Memeriksa status neighbor pada setiap router menggunakan show ip ospf neighbor hingga status menunjukkan FULL.
2. Menganalisis penyebab apabila status neighbor belum FULL (mis. subnet mask tidak sesuai, area mismatch).

3. Memperbaiki konfigurasi yang tidak sesuai hingga seluruh neighbor adjacency terbentuk sempurna.

Tahap 4 — Verifikasi Tabel Routing (± 45 menit)

1. Memeriksa tabel routing pada setiap router menggunakan show ip route dan mengidentifikasi rute yang dipelajari OSPF (kode O).
2. Menguji konektivitas end-to-end antar-segmen LAN pada router yang berbeda menggunakan ping/traceroute.
3. Mendokumentasikan hasil verifikasi (screenshot) sebagai bukti kerja.

Tahap 5 — Penutupan Sesi (± 20 menit)

1. Menyimpan file topologi (.pkt) sesuai konvensi penamaan file yang berlaku.
2. Merapikan area kerja dan mengembalikan perangkat sesuai prosedur K3.

F. Tugas Praktikum

Skenario: Sebuah perusahaan dengan 3 kantor cabang yang saling terhubung memerlukan routing otomatis yang dapat menyesuaikan diri terhadap perubahan topologi, tanpa administrator harus memperbarui rute secara manual pada setiap router.

Ketentuan tugas:

1. Mengonfigurasi OSPF single-area (Area 0) pada seluruh router (minimal 3) dalam topologi yang disiapkan.
2. Memastikan seluruh pasangan router yang terhubung langsung membentuk neighbor adjacency berstatus FULL.
3. Membuktikan seluruh segmen LAN pada masing-masing kantor cabang dapat saling terhubung (ping berhasil end-to-end).
4. Menyertakan tangkapan layar (screenshot) hasil show ip ospf neighbor dan show ip route dari setiap router.
5. Menyimpan file topologi (.pkt) sesuai konvensi penamaan yang berlaku.

G. Format Laporan Praktikum

Laporan disusun mengikuti Template Laporan Praktikum (Lampiran 1) dengan struktur sebagai berikut:

1. Halaman Judul (Modul, NIM, Nama, Kelompok jika ada)
2. Tujuan Praktikum
3. Alat dan Bahan yang Digunakan
4. Skema Topologi dan Pengalamatan IP Antar-Router
5. Langkah Kerja beserta Bukti Pelaksanaan (screenshot konfigurasi dan verifikasi)
6. Hasil Analisis Tabel Routing dan Status Neighbor
7. Kendala dan Solusi (jika ada)
8. Kesimpulan

Laporan dikumpulkan dalam format PDF/DOCX dengan nama file:
NIM_NamaMahasiswa_Modul06_Laporan, sesuai tenggat waktu yang ditentukan instruktur.

H. Rubrik Penilaian Ringkas

Penilaian menggunakan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55). Deskriptor lengkap keempat kategori untuk setiap aspek tersedia pada Rubrik Penilaian Praktikum per Pertemuan (Lampiran 3).

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Pemahaman Konsep OSPF	15%	Memahami konsep area, router-id, cost, dan proses pembentukan neighbor adjacency secara tepat.	Tidak memahami konsep OSPF.
Ketepatan Konfigurasi OSPF	40%	OSPF dikonfigurasi tepat (network statement, area 0, router-id) pada seluruh router topologi.	OSPF tidak terkonfigurasi atau konfigurasi salah total.
Verifikasi Tabel Routing & Neighbor	25%	Memverifikasi status neighbor (FULL) dan tabel routing secara akurat menggunakan show ip ospf neighbor/route.	Tidak melakukan verifikasi neighbor/tabel routing.
Dokumentasi Laporan Praktikum	20%	Laporan lengkap, sistematis, disertai bukti status neighbor dan tabel routing.	Tidak menyusun laporan praktikum.

Nilai Pertemuan 6 berkontribusi 2% terhadap komponen Tugas Praktikum (30%) pada nilai akhir mata kuliah, serta mendukung capaian CPL-2 dan CPL-5 sesuai Peta Kompetensi.

MODUL 7

ROUTING DINAMIS OSPF MULTI-AREA DAN VERIFIKASI RUTE

A. Identitas Modul

Modul / Pertemuan	Modul 7 / Pertemuan ke-7
Judul Modul	Routing Dinamis OSPF Multi-Area dan Verifikasi Rute
Sub-CPMK	Sub-CPMK-2.3 — Mampu mengonfigurasi routing dinamis OSPF multi-area serta melakukan verifikasi dan troubleshooting rute.
CPL Terkait	CPL-2, CPL-5
Metode Pembelajaran	Praktikum mandiri terbimbing, studi kasus kompleks, diskusi troubleshooting
Alokasi Waktu	170 menit (1 sks praktik)
Bobot Nilai	Kontribusi 3% dari komponen Tugas Praktikum (30%)

B. Tujuan Praktikum

Setelah mengikuti praktikum ini, mahasiswa diharapkan mampu:

1. Memahami peran Area Border Router (ABR), backbone area, dan jenis Link State Advertisement (LSA) secara tepat.
2. Mengonfigurasi OSPF multi-area pada topologi jaringan enterprise skala menengah.
3. Melakukan verifikasi rute antar-area menggunakan perintah show yang sesuai.
4. Mengidentifikasi dan memperbaiki penyebab rute yang tidak konvergen secara sistematis.

C. Dasar Teori Ringkas

1. Konsep OSPF Multi-Area

Pada jaringan berskala menengah hingga besar, penggunaan OSPF single-area menyebabkan seluruh router menyimpan link-state database yang identik dan besar, meningkatkan beban komputasi (SPF calculation). OSPF multi-area membagi jaringan menjadi beberapa area logis untuk membatasi ukuran link-state database per area serta membatasi dampak perubahan topologi hanya pada area yang bersangkutan.

2. Area Border Router (ABR) dan Backbone Area

Backbone Area (Area 0) berfungsi sebagai area pusat yang menghubungkan seluruh area lain; setiap area non-backbone wajib terhubung langsung ke Area 0. Area Border Router (ABR) adalah router yang memiliki interface pada lebih dari satu area sekaligus, bertugas meneruskan (menyaring dan meringkas) informasi rute antar-area.

3. Jenis Link State Advertisement (LSA) Utama

- Type 1 (Router LSA) — dihasilkan setiap router, mendeskripsikan interface dan link di dalam areanya sendiri.

- Type 2 (Network LSA) — dihasilkan Designated Router (DR) pada jaringan multi-akses, mendeskripsikan router yang terhubung ke segmen tersebut.
- Type 3 (Summary LSA) — dihasilkan ABR untuk meneruskan informasi rute antar-area ke area lain.

4. Troubleshooting Rute Tidak Konvergen

Penyebab umum rute OSPF tidak konvergen antara lain: area mismatch pada interface yang terhubung langsung, network statement/wildcard mask yang keliru, subnet mask yang tidak konsisten antar-ujung link, serta autentikasi OSPF yang tidak sesuai. Troubleshooting dilakukan secara sistematis dengan memeriksa status neighbor, konfigurasi area pada setiap interface, dan tabel routing pada tiap router yang terlibat.

5. Perintah Verifikasi Tambahan

```
show ip ospf interface brief    → menampilkan area dan status OSPF per interface
show ip ospf database           → menampilkan isi link-state database (LSA)
show ip route ospf              → menampilkan rute yang dipelajari khusus dari OSPF
debug ip ospf adj               → menelusuri proses pembentukan adjacency secara real-time
```

D. Alat dan Bahan

Komponen	Keterangan
Perangkat Lunak	Cisco Packet Tracer (versi terbaru)
Perangkat Fisik (opsional)	Minimal 4–5 unit router Cisco IOS membentuk topologi multi-area
Perangkat Pendukung	PC/end device pada segmen jaringan tiap area, kabel sesuai topologi
Dokumen Pendukung	Template Laporan Praktikum (Lampiran 1), Topologi Referensi Modul 7 (Lampiran 2)

E. Langkah Kerja / Prosedur

Tahap 1 — Persiapan Topologi Multi-Area (± 25 menit)

1. Membangun topologi enterprise skala menengah dengan minimal 3 area (Area 0/backbone, Area 1, Area 2) dan minimal 1 ABR pada setiap batas area.
2. Mengatur alamat IP pada seluruh interface sesuai skema pengalamatan per area.

Tahap 2 — Konfigurasi OSPF Multi-Area (± 45 menit)

1. Mengaktifkan proses OSPF pada seluruh router menggunakan router ospf.
2. Mengikutsertakan setiap interface ke dalam area yang sesuai menggunakan network ... area <id>, memastikan ABR memiliki interface pada lebih dari satu area.
3. Memverifikasi keanggotaan area setiap interface menggunakan show ip ospf interface brief.

Tahap 3 — Verifikasi Rute Antar-Area (± 40 menit)

1. Memeriksa status neighbor pada setiap router menggunakan show ip ospf neighbor.

2. Memeriksa tabel routing pada router non-ABR untuk memastikan rute antar-area muncul dengan kode OIA (inter-area) menggunakan show ip route.
3. Menguji konektivitas end-to-end antar-segmen pada area yang berbeda.

Tahap 4 — Troubleshooting Rute Tidak Konvergen (± 40 menit)

1. Menganalisis skenario gangguan yang disiapkan instruktur (mis. area mismatch atau network statement keliru pada salah satu router).
2. Mengidentifikasi akar masalah secara sistematis menggunakan show ip ospf neighbor, show ip ospf interface brief, dan show running-config.
3. Memperbaiki konfigurasi yang keliru hingga seluruh rute kembali konvergen dan mendokumentasikan proses troubleshooting (screenshot sebelum-sesudah).

Tahap 5 — Penutupan Sesi (± 20 menit)

1. Menyimpan file topologi (.pkt) sesuai konvensi penamaan file yang berlaku.
2. Merapikan area kerja dan mengembalikan perangkat sesuai prosedur K3.

F. Tugas Praktikum

Skenario: Sebuah perusahaan skala menengah dengan kantor pusat dan beberapa kantor regional mengalami kendala salah satu regional tidak dapat menjangkau rute ke regional lain akibat kesalahan konfigurasi OSPF yang dilakukan teknisi sebelumnya. Mahasiswa ditugaskan sebagai teknisi jaringan untuk mengimplementasikan dan memperbaiki konfigurasi multi-area tersebut.

Ketentuan tugas:

1. Mengonfigurasi OSPF multi-area (minimal 3 area) pada topologi yang disiapkan, termasuk peran ABR yang tepat.
2. Menemukan dan memperbaiki kesalahan konfigurasi (disisipkan instruktur) yang menyebabkan rute antar-area tidak konvergen.
3. Membuktikan seluruh area dapat saling terhubung setelah perbaikan (ping berhasil end-to-end lintas-area).
4. Menyertakan tangkapan layar (screenshot) hasil sebelum dan sesudah troubleshooting, serta hasil show ip route yang menunjukkan rute inter-area (OIA).
5. Menyimpan file topologi (.pkt) sesuai konvensi penamaan yang berlaku.

G. Format Laporan Praktikum

Laporan disusun mengikuti Template Laporan Praktikum (Lampiran 1) dengan struktur sebagai berikut:

1. Halaman Judul (Modul, NIM, Nama, Kelompok jika ada)
2. Tujuan Praktikum
3. Alat dan Bahan yang Digunakan
4. Skema Topologi Multi-Area dan Peran ABR
5. Langkah Kerja beserta Bukti Pelaksanaan (screenshot konfigurasi dan verifikasi)
6. Analisis dan Proses Troubleshooting Rute Tidak Konvergen
7. Kendala dan Solusi (jika ada)

8. Kesimpulan

Laporan dikumpulkan dalam format PDF/DOCX dengan nama file:
NIM_NamaMahasiswa_Modul07_Laporan, sesuai tenggat waktu yang ditentukan instruktur.

H. Rubrik Penilaian Ringkas

Penilaian menggunakan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55). Deskriptor lengkap keempat kategori untuk setiap aspek tersedia pada Rubrik Penilaian Praktikum per Pertemuan (Lampiran 3).

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Pemahaman Konsep Multi-Area	15%	Memahami peran Area Border Router (ABR), backbone area, dan jenis LSA secara tepat.	Tidak memahami konsep OSPF multi-area.
Ketepatan Konfigurasi Multi-Area	35%	Seluruh router dan ABR dikonfigurasi tepat pada area masing-masing sesuai topologi enterprise skala menengah.	Konfigurasi multi-area salah total atau tidak terbentuk.
Troubleshooting Rute Tidak Konvergen	30%	Mengidentifikasi dan memperbaiki penyebab rute tidak konvergen secara sistematis dan tepat.	Tidak mampu mengidentifikasi maupun memperbaiki masalah routing.
Dokumentasi Laporan Praktikum	20%	Laporan lengkap, sistematis, disertai analisis troubleshooting dan bukti rute konvergen.	Tidak menyusun laporan praktikum.

Nilai Pertemuan 7 berkontribusi 3% terhadap komponen Tugas Praktikum (30%) pada nilai akhir mata kuliah, serta mendukung capaian CPL-2 dan CPL-5 sesuai Peta Kompetensi. Modul ini menutup rangkaian CPMK-2 (Modul 5–7) dan menjadi materi terakhir sebelum UTS (Modul 8).

MODUL 8

UJIAN TENGAH SEMESTER (UTS) — UJIAN PRAKTIK SWITCHING DAN ROUTING

A. Identitas Modul

Modul / Pertemuan	Modul 8 / Pertemuan ke-8 (Evaluasi Tengah Semester)
Judul Modul	Ujian Tengah Semester (UTS) — Ujian Praktik Switching dan Routing
Cakupan Sub-CPMK	Sub-CPMK-1.1 s.d. Sub-CPMK-2.3 (Modul 1–7)
CPL Terkait	CPL-2, CPL-5, CPL-12
Metode Ujian	Ujian praktik individual (hands-on skill test)
Alokasi Waktu	170 menit (1 sks praktik)
Bobot Nilai	30% dari nilai akhir mata kuliah (komponen UTS)

B. Tujuan Ujian

Ujian Tengah Semester (UTS) bertujuan mengevaluasi ketercapaian Sub-CPMK-1.1 hingga Sub-CPMK-2.3 secara komprehensif dan terintegrasi, yaitu kemampuan mahasiswa dalam:

1. Menerapkan prosedur K3 dan dasar CLI perangkat jaringan (Modul 1).
2. Mengonfigurasi VLAN, trunking, VTP, dan EtherChannel pada perangkat switch (Modul 2–4).
3. Mengimplementasikan routing antar-VLAN dan routing dinamis OSPF single-area maupun multi-area (Modul 5–7).
4. Melakukan verifikasi dan troubleshooting mandiri atas seluruh konfigurasi yang diujikan.

C. Cakupan Materi Ujian

Cakupan materi ujian merangkum seluruh Sub-CPMK yang telah dipraktikkan pada Modul 1–7, tanpa memuat materi baru.

Modul	Materi	Sub-CPMK Diujikan
1	Dasar CLI dan Prosedur K3	Sub-CPMK-1.1
2	Konfigurasi VLAN	Sub-CPMK-1.2
3	Trunking 802.1Q dan VTP	Sub-CPMK-1.3
4	EtherChannel (LACP/PAgP)	Sub-CPMK-1.4
5	Routing Antar-VLAN (RoaS/L3 Switching)	Sub-CPMK-2.1
6	Routing Dinamis OSPF Single-Area	Sub-CPMK-2.2
7	Routing Dinamis OSPF Multi-Area & Troubleshooting	Sub-CPMK-2.3

D. Ketentuan dan Tata Tertib Ujian

1. Ujian bersifat individual (mandiri); dilarang bekerja sama, berbagi jawaban, atau menyalin pekerjaan mahasiswa lain.
2. Mahasiswa wajib menerapkan prosedur K3 laboratorium sebagaimana telah dipelajari pada Modul 1 selama ujian berlangsung.
3. Setiap mahasiswa memperoleh topologi ujian dengan skenario dan parameter yang dapat berbeda-beda (variasi soal) untuk mencegah kecurangan.
4. Mahasiswa dapat menggunakan catatan pribadi ringkas (jika diizinkan instruktur) namun dilarang mengakses internet, forum, atau bantuan eksternal lain.
5. Keterlambatan pengumpulan hasil ujian di luar alokasi waktu 170 menit akan memengaruhi aspek Manajemen Waktu Penyelesaian pada rubrik penilaian.
6. Segala bentuk kecurangan (plagiarisme konfigurasi, kerja sama tidak sah) akan ditindak sesuai kode etik akademik yang berlaku (mendukung capaian CPL-12).

E. Alat dan Bahan Ujian

Komponen	Keterangan
Perangkat Lunak	Cisco Packet Tracer (versi terbaru), file topologi ujian (.pkt) yang dibagikan instruktur
Perangkat Fisik (opsional)	Switch dan router laboratorium sesuai ketersediaan dan kebijakan program studi
Dokumen Pendukung	Lembar Soal Ujian, Lembar Jawaban/Template Pelaporan Hasil Ujian

F. Gambaran Umum Skenario Ujian

Skenario ujian bersifat komprehensif dan mengintegrasikan seluruh topik Modul 1–7 dalam satu topologi enterprise sederhana. Rincian parameter (VLAN ID, alamat IP, area OSPF, dan sejenisnya) ditentukan oleh instruktur pada saat ujian berlangsung dan dapat bervariasi antar-mahasiswa. Contoh cakupan skenario meliputi:

1. Konfigurasi identitas dasar perangkat dan penerapan prosedur K3 (Sub-CPMK-1.1).
2. Pembuatan dan penempatan VLAN sesuai skema segmentasi yang ditentukan (Sub-CPMK-1.2).
3. Konfigurasi trunk 802.1Q dan VTP untuk propagasi VLAN antar-switch (Sub-CPMK-1.3).
4. Pembentukan EtherChannel pada tautan yang ditentukan (Sub-CPMK-1.4).
5. Implementasi routing antar-VLAN menggunakan router-on-a-stick atau Layer-3 switching (Sub-CPMK-2.1).
6. Konfigurasi routing dinamis OSPF (single-area atau multi-area, tergantung variasi soal) beserta verifikasi/troubleshooting rute (Sub-CPMK-2.2 dan 2.3).

Soal ujian lengkap beserta topologi spesifik disampaikan secara terpisah oleh instruktur pada saat pelaksanaan ujian.

G. Prosedur Pelaksanaan Ujian

Tahap 1 — Persiapan (± 10 menit)

1. Instruktur membagikan lembar soal dan file topologi ujian kepada masing-masing mahasiswa.
2. Mahasiswa memeriksa kelengkapan soal dan mengonfirmasi tidak ada kendala teknis pada perangkat/aplikasi.

Tahap 2 — Pengerjaan Mandiri (± 130 menit)

1. Mahasiswa mengerjakan seluruh skenario ujian secara mandiri sesuai urutan yang dianggap paling efisien.
2. Mahasiswa melakukan verifikasi setiap tahap konfigurasi secara berkala untuk memastikan tidak ada kesalahan yang terakumulasi.
3. Mahasiswa melakukan troubleshooting mandiri apabila ditemukan hasil verifikasi yang tidak sesuai target.

Tahap 3 — Verifikasi Akhir dan Pengumpulan (± 30 menit)

1. Mahasiswa melakukan verifikasi akhir menyeluruh (show run, show vlan brief, show ip route, show etherchannel summary, dan sejenisnya sesuai cakupan soal).
2. Mahasiswa menyimpan file topologi akhir dan mengumpulkan hasil ujian sesuai format yang ditentukan (Bagian H).
3. Mahasiswa merapikan area kerja sesuai prosedur K3 setelah ujian selesai.

H. Format Pengumpulan Hasil Ujian

Hasil ujian dikumpulkan dalam bentuk:

1. File topologi akhir (.pkt) dengan nama file: NIM_NamaMahasiswa_UTS.pkt
2. Lembar Jawaban berisi tangkapan layar (screenshot) hasil verifikasi setiap bagian skenario yang diujikan, disusun sesuai urutan soal.
3. Berkas dikumpulkan melalui mekanisme yang ditentukan instruktur (unggah platform pembelajaran/pengumpulan langsung) sebelum batas waktu 170 menit berakhir.

I. Rubrik Penilaian UTS

Penilaian menggunakan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55). Deskriptor lengkap keempat kategori untuk setiap aspek tersedia pada Rubrik Penilaian Praktikum per Pertemuan (Lampiran 3).

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Kelengkapan Konfigurasi Skenario	30%	Seluruh elemen skenario ujian (VLAN, trunk, EtherChannel, routing) dikonfigurasi lengkap sesuai instruksi.	Sebagian besar elemen skenario tidak dikonfigurasi.
Ketepatan Teknis Multi-Topik	35%	Seluruh konfigurasi (VLAN/trunk/EtherChannel/routing antar-VLAN/OSPF) benar secara teknis tanpa kesalahan.	Kesalahan teknis signifikan sehingga jaringan tidak berfungsi sesuai skenario.
Verifikasi & Troubleshooting	20%	Mampu memverifikasi hasil kerja	Tidak mampu memverifikasi

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Mandiri		dan memperbaiki kesalahan secara mandiri tanpa bantuan.	maupun memperbaiki kesalahan konfigurasi.
Manajemen Waktu Penyelesaian	15%	Menyelesaikan seluruh skenario ujian dalam alokasi waktu yang ditentukan dengan efisien.	Tidak menyelesaikan skenario ujian dalam waktu yang tersedia.

Nilai UTS berkontribusi 30% terhadap nilai akhir mata kuliah dan menjadi dasar perhitungan Nilai CPMK-1 dan CPMK-2 (bersama rerata Tugas Praktikum Modul 1–7 dengan proporsi 70% tugas : 30% UTS), yang selanjutnya berkontribusi pada perhitungan capaian CPL-2, CPL-5, dan CPL-12 sesuai Rubrik Penilaian CPL.

MODUL 9

REDUNDANSI GATEWAY: HSRP DAN VRRP

A. Identitas Modul

Modul / Pertemuan	Modul 9 / Pertemuan ke-9
Judul Modul	Redundansi Gateway: HSRP dan VRRP
Sub-CPMK	Sub-CPMK-3.1 — Mampu mengonfigurasi HSRP/VRRP untuk redundansi gateway pada jaringan enterprise.
CPL Terkait	CPL-5, CPL-10
Metode Pembelajaran	Demonstrasi, praktikum terbimbing, simulasi kegagalan perangkat (failover test)
Alokasi Waktu	170 menit (1 sks praktik)
Bobot Nilai	Kontribusi 2% dari komponen Tugas Praktikum (30%)

B. Tujuan Praktikum

Setelah mengikuti praktikum ini, mahasiswa diharapkan mampu:

1. Memahami peran active/standby router, virtual IP, dan mekanisme election HSRP/VRRP secara tepat.
2. Mengonfigurasi HSRP atau VRRP pada dua router gateway untuk menyediakan redundansi default gateway.
3. Mengatur parameter priority dan preempt untuk mengendalikan peran active/standby router.
4. Menguji dan membuktikan proses failover berjalan mulus ketika router aktif dinonaktifkan.

C. Dasar Teori Ringkas

1. Kebutuhan Redundansi Gateway

Pada jaringan enterprise, seluruh host pada satu segmen umumnya mengarahkan trafik keluar melalui satu default gateway. Apabila router gateway tersebut mengalami kegagalan, seluruh host pada segmen tersebut akan kehilangan konektivitas keluar jaringan. First Hop Redundancy Protocol (FHRP) seperti HSRP dan VRRP mengatasi masalah ini dengan menyediakan lebih dari satu router fisik yang berbagi satu alamat IP virtual sebagai gateway bersama.

2. Hot Standby Router Protocol (HSRP)

HSRP adalah protokol milik Cisco (proprietary) yang mengelompokkan dua atau lebih router ke dalam satu grup HSRP dengan satu virtual IP dan virtual MAC bersama. Salah satu router berperan sebagai Active Router (meneruskan trafik), sementara router lain berperan sebagai Standby Router (siap mengambil alih apabila Active Router gagal). Pemilihan Active Router ditentukan berdasarkan nilai priority tertinggi.

3. Virtual Router Redundancy Protocol (VRRP)

VRRP adalah protokol standar terbuka (open standard, RFC 5798) dengan konsep serupa HSRP, namun menggunakan istilah Master Router (setara Active) dan Backup Router (setara Standby). VRRP mendukung interoperabilitas antar-vendor karena bukan merupakan protokol proprietary Cisco.

4. Parameter Priority dan Preempt

- Priority — nilai yang menentukan router mana yang menjadi Active/Master; router dengan priority tertinggi akan terpilih sebagai router aktif.
- Preempt — opsi yang memungkinkan router dengan priority lebih tinggi untuk merebut kembali peran Active/Master ketika ia kembali aktif setelah sebelumnya gagal, meskipun router lain sedang menjabat sebagai Active.

5. Perintah Dasar Konfigurasi

```
HSRP:
standby <group> ip <virtual-ip>          → mengatur virtual IP grup HSRP
standby <group> priority <nilai>         → mengatur priority router
standby <group> preempt                  → mengaktifkan opsi preempt
show standby brief                       → menampilkan ringkasan status HSRP
VRRP:
vrrp <group> ip <virtual-ip>              → mengatur virtual IP grup VRRP
vrrp <group> priority <nilai>             → mengatur priority router
show vrrp brief                           → menampilkan ringkasan status VRRP
```

D. Alat dan Bahan

Komponen	Keterangan
Perangkat Lunak	Cisco Packet Tracer (versi terbaru)
Perangkat Fisik (opsional)	2 unit router Cisco IOS sebagai pasangan gateway redundan
Perangkat Pendukung	1 switch penghubung segmen LAN, PC/end device pada segmen tersebut
Dokumen Pendukung	Template Laporan Praktikum (Lampiran 1), Topologi Referensi Modul 9 (Lampiran 2)

E. Langkah Kerja / Prosedur

Tahap 1 — Persiapan Topologi Dua Router Gateway (± 20 menit)

1. Membangun topologi 2 router yang terhubung ke segmen LAN yang sama melalui switch, serta memiliki koneksi ke jaringan luar (opsional).
2. Mengatur alamat IP fisik pada interface masing-masing router (bukan virtual IP) pada subnet yang sama.

Tahap 2 — Konfigurasi HSRP/VRRP (± 45 menit)

1. Mengonfigurasi grup HSRP/VRRP pada interface kedua router yang menghadap segmen LAN, dengan virtual IP yang sama pada kedua router.
2. Mengatur priority lebih tinggi pada router yang ditetapkan sebagai Active/Master sesuai skenario.
3. Mengaktifkan opsi preempt pada router dengan priority lebih tinggi.

4. Mengatur default gateway pada seluruh PC di segmen LAN menggunakan virtual IP grup HSRP/VRRP.

Tahap 3 — Verifikasi Status Active/Standby (± 30 menit)

1. Memverifikasi peran masing-masing router menggunakan show standby brief atau show vrrp brief.
2. Menguji konektivitas dari PC ke luar segmen melalui virtual IP gateway.

Tahap 4 — Pengujian Failover (± 55 menit)

1. Menonaktifkan interface router Active/Master (menggunakan shutdown) untuk mensimulasikan kegagalan perangkat.
2. Mengamati proses pengambilalihan peran oleh router Standby/Backup dan memverifikasi konektivitas PC tetap terjaga selama proses failover.
3. Mengaktifkan kembali router yang dinonaktifkan dan mengamati apakah peran Active/Master kembali terambil alih (karena preempt aktif).
4. Mendokumentasikan hasil pengujian (screenshot sebelum, saat, dan setelah failover) sebagai bukti kerja.

Tahap 5 — Penutupan Sesi (± 20 menit)

1. Menyimpan file topologi (.pkt) sesuai konvensi penamaan file yang berlaku.
2. Merapikan area kerja dan mengembalikan perangkat sesuai prosedur K3.

F. Tugas Praktikum

Skenario: Sebuah kantor pusat memiliki satu segmen jaringan kritikal yang tidak boleh kehilangan akses gateway meskipun salah satu router mengalami kegagalan (mis. untuk pemeliharaan atau kerusakan perangkat). Mahasiswa ditugaskan mengimplementasikan solusi redundansi gateway pada segmen tersebut.

Ketentuan tugas:

1. Mengonfigurasi HSRP ATAU VRRP (sesuai penugasan instruktur) pada dua router gateway dengan satu virtual IP bersama.
2. Menentukan salah satu router sebagai Active/Master melalui pengaturan priority dan mengaktifkan preempt.
3. Melakukan pengujian failover dengan menonaktifkan router Active/Master dan membuktikan PC pada segmen LAN tetap memiliki konektivitas keluar.
4. Menyertakan tangkapan layar (screenshot) hasil show standby brief/show vrrp brief sebelum dan sesudah failover.
5. Menyimpan file topologi (.pkt) sesuai konvensi penamaan yang berlaku.

G. Format Laporan Praktikum

Laporan disusun mengikuti Template Laporan Praktikum (Lampiran 1) dengan struktur sebagai berikut:

1. Halaman Judul (Modul, NIM, Nama, Kelompok jika ada)
2. Tujuan Praktikum

3. Alat dan Bahan yang Digunakan
4. Skema Redundansi Gateway (topologi, virtual IP, priority masing-masing router)
5. Langkah Kerja beserta Bukti Pelaksanaan (screenshot konfigurasi dan verifikasi)
6. Hasil Pengujian Failover
7. Kendala dan Solusi (jika ada)
8. Kesimpulan

Laporan dikumpulkan dalam format PDF/DOCX dengan nama file: NIM_NamaMahasiswa_Modul09_Laporan, sesuai tenggat waktu yang ditentukan instruktur.

H. Rubrik Penilaian Ringkas

Penilaian menggunakan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55). Deskriptor lengkap keempat kategori untuk setiap aspek tersedia pada Rubrik Penilaian Praktikum per Pertemuan (Lampiran 3).

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Pemahaman Konsep Redundansi Gateway	15%	Memahami peran active/standby router, virtual IP, dan mekanisme election HSRP/VRRP secara tepat.	Tidak memahami konsep HSRP/VRRP.
Ketepatan Konfigurasi HSRP/VRRP	40%	HSRP/VRRP dikonfigurasi tepat (virtual IP, priority, preempt) pada kedua router gateway.	HSRP/VRRP tidak terkonfigurasi atau konfigurasi salah total.
Pengujian Failover	25%	Menguji dan membuktikan proses failover berjalan mulus (tanpa terputus signifikan) saat router aktif dinonaktifkan.	Tidak melakukan pengujian failover atau failover gagal total.
Dokumentasi Laporan Praktikum	20%	Laporan lengkap, sistematis, disertai bukti status HSRP/VRRP dan hasil uji failover.	Tidak menyusun laporan praktikum.

Nilai Pertemuan 9 berkontribusi 2% terhadap komponen Tugas Praktikum (30%) pada nilai akhir mata kuliah, serta mendukung capaian CPL-5 dan CPL-10 sesuai Peta Kompetensi. Modul ini membuka rangkaian CPMK-3 pasca-UTS.

MODUL 10

VPN SITE-TO-SITE BERBASIS IPSEC

A. Identitas Modul

Modul / Pertemuan	Modul 10 / Pertemuan ke-10
Judul Modul	VPN Site-to-Site Berbasis IPSec
Sub-CPMK	Sub-CPMK-3.2 — Mampu mengonfigurasi VPN site-to-site menggunakan IPSec untuk konektivitas antar-lokasi.
CPL Terkait	CPL-5, CPL-10
Metode Pembelajaran	Praktikum mandiri terbimbing, studi kasus konektivitas antar-cabang
Alokasi Waktu	170 menit (1 sks praktik)
Bobot Nilai	Kontribusi 3% dari komponen Tugas Praktikum (30%)

B. Tujuan Praktikum

Setelah mengikuti praktikum ini, mahasiswa diharapkan mampu:

1. Memahami komponen IPSec (ISAKMP/IKE fase 1–2, transform-set, crypto map) secara tepat.
2. Mengonfigurasi tunnel VPN IPSec antara dua router yang merepresentasikan kantor pusat dan kantor cabang.
3. Menentukan interesting traffic yang akan dienkapsulasi melalui tunnel VPN menggunakan Access Control List (ACL).
4. Memverifikasi status tunnel dan membuktikan trafik antar-lokasi terenkripsi dengan benar.

C. Dasar Teori Ringkas

1. Konsep VPN Site-to-Site

Virtual Private Network (VPN) site-to-site memungkinkan dua jaringan privat di lokasi berbeda (misalnya kantor pusat dan kantor cabang) saling terhubung secara aman melalui jaringan publik (internet) seolah-olah berada dalam satu jaringan privat yang sama, dengan trafik yang dienkripsi untuk menjaga kerahasiaan dan integritas data.

2. IPSec dan Fase Negosiasi ISAKMP/IKE

IPSec (Internet Protocol Security) adalah kerangka kerja protokol yang menyediakan layanan keamanan pada lapisan network, mencakup autentikasi, enkripsi, dan integritas data. Pembentukan tunnel IPSec melibatkan dua fase negosiasi menggunakan Internet Key Exchange (IKE)/ISAKMP:

- Fase 1 (ISAKMP) — membentuk secure channel manajemen antar-router (ISAKMP SA) menggunakan parameter autentikasi (pre-shared key), enkripsi, hashing, dan Diffie-Hellman group yang disepakati kedua pihak.
- Fase 2 (IPSec) — membentuk IPSec SA aktual yang digunakan untuk mengenkripsi trafik data pengguna, menggunakan parameter dari transform-set yang telah ditentukan.

3. Transform-Set dan Crypto Map

- Transform-set — kumpulan algoritma enkripsi dan hashing (mis. AES, SHA) yang digunakan untuk melindungi trafik data pada Fase 2 IPSec.
- Crypto map — mengaitkan interesting traffic (didefinisikan melalui ACL), peer tujuan tunnel, dan transform-set menjadi satu kebijakan VPN yang diterapkan pada interface keluar (outbound) router.

4. Perintah Dasar Konfigurasi IPSec

```
crypto isakmp policy <no>                    → membuat kebijakan Fase 1 ISAKMP
crypto isakmp key <key> address <peer-ip>    → mengatur pre-shared key dengan peer
crypto ipsec transform-set <nama> ...        → mendefinisikan transform-set Fase 2
access-list <no> permit ip <src> <dst>       → mendefinisikan interesting traffic
crypto map <nama> <seq> ipsec-isakmp         → membuat crypto map dan mengaitkan parameter
show crypto isakmp sa                        → memverifikasi status Fase 1 (ISAKMP SA)
show crypto ipsec sa                         → memverifikasi status Fase 2 (IPSec SA) dan statistik enkripsi
```

D. Alat dan Bahan

Komponen	Keterangan
Perangkat Lunak	Cisco Packet Tracer (versi terbaru)
Perangkat Fisik (opsional)	2 unit router Cisco IOS yang merepresentasikan kantor pusat dan kantor cabang
Perangkat Pendukung	1 switch dan PC pada masing-masing lokasi, simulasi tautan WAN/internet di antara kedua router
Dokumen Pendukung	Template Laporan Praktikum (Lampiran 1), Topologi Referensi Modul 10 (Lampiran 2)

E. Langkah Kerja / Prosedur

Tahap 1 — Persiapan Topologi Dua Lokasi (± 20 menit)

1. Membangun topologi 2 router (mewakili kantor pusat dan kantor cabang) yang terhubung melalui simulasi tautan WAN/internet, masing-masing dengan segmen LAN privat di belakangnya.
2. Mengatur alamat IP pada interface WAN dan LAN kedua router, serta memastikan konektivitas dasar antar-router WAN sebelum konfigurasi VPN.

Tahap 2 — Konfigurasi Fase 1 ISAKMP (± 30 menit)

1. Membuat kebijakan ISAKMP (enkripsi, hashing, autentikasi, Diffie-Hellman group) yang identik pada kedua router.
2. Mengatur pre-shared key yang sama pada kedua router, mengacu pada alamat IP WAN peer masing-masing.

Tahap 3 — Konfigurasi Fase 2 IPSec dan Interesting Traffic (± 45 menit)

1. Mendefinisikan transform-set (algoritma enkripsi dan hashing) yang identik pada kedua router.
2. Membuat ACL yang mendefinisikan interesting traffic, yaitu trafik dari subnet LAN kantor pusat menuju subnet LAN kantor cabang (dan sebaliknya pada router kedua).
3. Membuat crypto map yang mengaitkan peer, transform-set, dan ACL interesting traffic, kemudian menerapkannya pada interface WAN masing-masing router.

Tahap 4 — Verifikasi Tunnel dan Enkripsi (± 55 menit)

1. Memicu pembentukan tunnel dengan mengirimkan trafik dari PC kantor pusat menuju PC kantor cabang (ping antar-LAN).
2. Memverifikasi status Fase 1 menggunakan show crypto isakmp sa (status QM_IDLE menandakan ISAKMP SA aktif).
3. Memverifikasi status Fase 2 menggunakan show crypto ipsec sa, memeriksa jumlah paket yang dienkripsi (encaps) dan didekripsi (decaps).
4. Mendokumentasikan hasil verifikasi (screenshot) sebagai bukti kerja.

Tahap 5 — Penutupan Sesi (± 20 menit)

1. Menyimpan file topologi (.pkt) sesuai konvensi penamaan file yang berlaku.
2. Merapikan area kerja dan mengembalikan perangkat sesuai prosedur K3.

F. Tugas Praktikum

Skenario: Sebuah perusahaan memiliki kantor pusat dan satu kantor cabang yang terhubung melalui internet publik. Manajemen mensyaratkan seluruh komunikasi data antar-kedua lokasi harus terenkripsi untuk melindungi data sensitif perusahaan dari penyadapan pada jaringan publik.

Ketentuan tugas:

1. Mengonfigurasi tunnel VPN IPSec site-to-site antara router kantor pusat dan kantor cabang.
2. Mendefinisikan interesting traffic yang mencakup seluruh komunikasi antar-subnet LAN kedua lokasi.
3. Membuktikan tunnel VPN berhasil terbentuk dan trafik antar-lokasi terenkripsi (encaps/decaps bertambah pada show crypto ipsec sa).
4. Menyertakan tangkapan layar (screenshot) hasil show crypto isakmp sa dan show crypto ipsec sa dari kedua router.
5. Menyimpan file topologi (.pkt) sesuai konvensi penamaan yang berlaku.

G. Format Laporan Praktikum

Laporan disusun mengikuti Template Laporan Praktikum (Lampiran 1) dengan struktur sebagai berikut:

1. Halaman Judul (Modul, NIM, Nama, Kelompok jika ada)
2. Tujuan Praktikum
3. Alat dan Bahan yang Digunakan
4. Skema Tunnel VPN (topologi, parameter ISAKMP, transform-set, interesting traffic)
5. Langkah Kerja beserta Bukti Pelaksanaan (screenshot konfigurasi dan verifikasi)

6. Hasil Verifikasi Enkripsi dan Konektivitas
7. Kendala dan Solusi (jika ada)
8. Kesimpulan

Laporan dikumpulkan dalam format PDF/DOCX dengan nama file: NIM_NamaMahasiswa_Modul10_Laporan, sesuai tenggat waktu yang ditentukan instruktur.

H. Rubrik Penilaian Ringkas

Penilaian menggunakan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55). Deskriptor lengkap keempat kategori untuk setiap aspek tersedia pada Rubrik Penilaian Praktikum per Pertemuan (Lampiran 3).

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Pemahaman Konsep VPN & IPSec	15%	Memahami komponen IPSec (ISAKMP/IKE fase 1–2, transform-set, crypto map) secara tepat.	Tidak memahami konsep VPN/IPSec.
Ketepatan Konfigurasi Tunnel VPN	40%	Tunnel VPN IPSec terkonfigurasi lengkap dan tepat (ISAKMP, transform-set, crypto map, ACL interesting traffic) pada kedua router.	Tunnel VPN tidak terkonfigurasi atau konfigurasi salah total.
Verifikasi Enkripsi & Konektivitas	25%	Memverifikasi status tunnel (show crypto isakmp/ipsec sa) dan membuktikan trafik terenkripsi antar-lokasi.	Tidak melakukan verifikasi atau tunnel tidak berfungsi.
Dokumentasi Laporan Praktikum	20%	Laporan lengkap, sistematis, disertai bukti status tunnel dan hasil verifikasi enkripsi.	Tidak menyusun laporan praktikum.

Nilai Pertemuan 10 berkontribusi 3% terhadap komponen Tugas Praktikum (30%) pada nilai akhir mata kuliah, serta mendukung capaian CPL-5 dan CPL-10 sesuai Peta Kompetensi. Modul ini menutup topik CPMK-3 (Modul 9–10).

MODUL 11

ACCESS CONTROL LIST (ACL) STANDAR DAN EXTENDED

A. Identitas Modul

Modul / Pertemuan	Modul 11 / Pertemuan ke-11
Judul Modul	Access Control List (ACL) Standar dan Extended
Sub-CPMK	Sub-CPMK-4.1 — Mampu mengonfigurasi Access Control List (ACL) standar dan extended untuk kontrol akses jaringan.
CPL Terkait	CPL-5, CPL-8
Metode Pembelajaran	Demonstrasi, praktikum terbimbing, studi kasus kebijakan akses
Alokasi Waktu	170 menit (1 sks praktik)
Bobot Nilai	Kontribusi 2% dari komponen Tugas Praktikum (30%)

B. Tujuan Praktikum

Setelah mengikuti praktikum ini, mahasiswa diharapkan mampu:

1. Merancang kebijakan ACL yang tepat sesuai kebutuhan pembatasan akses pada skenario yang diberikan.
2. Mengonfigurasi ACL standar untuk menyaring trafik berdasarkan alamat IP sumber.
3. Mengonfigurasi ACL extended untuk menyaring trafik berdasarkan alamat sumber, tujuan, protokol, dan port.
4. Menguji dan membuktikan trafik yang diizinkan/ditolak sesuai kebijakan yang telah dirancang.

C. Dasar Teori Ringkas

1. Konsep Access Control List (ACL)

Access Control List (ACL) adalah kumpulan aturan berurutan (sequential) pada router/switch yang digunakan untuk menyaring trafik jaringan berdasarkan kriteria tertentu, sehingga dapat mengizinkan (permit) atau menolak (deny) paket data yang melewati suatu interface. ACL memproses aturan dari atas ke bawah secara berurutan; begitu satu paket cocok dengan salah satu aturan, pemrosesan ACL berhenti dan aksi (permit/deny) pada aturan tersebut diterapkan. Terdapat implicit deny any di akhir setiap ACL yang menolak seluruh trafik yang tidak cocok dengan aturan eksplisit manapun.

2. ACL Standar

ACL standar (bernomor 1–99 atau 1300–1999) hanya dapat menyaring trafik berdasarkan alamat IP sumber, sehingga bersifat kurang spesifik. Karena hanya memeriksa sumber, ACL standar sebaiknya ditempatkan sedekat mungkin dengan tujuan (destination) agar tidak secara tidak sengaja memblokir trafik yang seharusnya diizinkan menuju tujuan lain.

3. ACL Extended

ACL extended (bernomor 100–199 atau 2000–2699) dapat menyaring trafik berdasarkan kombinasi alamat sumber, alamat tujuan, protokol (TCP/UDP/ICMP), serta nomor port sumber/tujuan, sehingga jauh lebih fleksibel dan spesifik. Karena kemampuannya menyaring berdasarkan tujuan, ACL extended sebaiknya ditempatkan sedekat mungkin dengan sumber (source) trafik untuk menghemat pemrosesan jaringan.

4. Wildcard Mask

ACL menggunakan wildcard mask (bukan subnet mask biasa) untuk menentukan rentang alamat IP yang dicocokkan; bit 0 pada wildcard mask berarti bit tersebut harus cocok persis, sedangkan bit 1 berarti bit tersebut dapat bernilai apa saja (diabaikan).

5. Perintah Dasar Konfigurasi ACL

```
ACL Standar:
access-list <1-99> permit|deny <src> <wildcard>       → membuat aturan ACL standar
ACL Extended:
access-list <100-199> permit|deny <proto> <src> <wc> <dst> <wc> [eq port] → aturan ACL extended
Penerapan pada Interface:
interface <tipe/nomor>                                 → masuk ke interface tujuan
ip access-group <no> in|out                            → menerapkan ACL pada arah in/out
show access-lists                                      → menampilkan seluruh ACL dan jumlah match
```

D. Alat dan Bahan

Komponen	Keterangan
Perangkat Lunak	Cisco Packet Tracer (versi terbaru)
Perangkat Fisik (opsional)	1–2 unit router Cisco IOS dengan beberapa segmen jaringan berbeda
Perangkat Pendukung	PC/end device dan server simulasi (mis. HTTP/FTP server) pada segmen berbeda
Dokumen Pendukung	Template Laporan Praktikum (Lampiran 1), Topologi Referensi Modul 11 (Lampiran 2)

E. Langkah Kerja / Prosedur

Tahap 1 — Persiapan Topologi dan Analisis Kebijakan (± 25 menit)

1. Membangun/melanjutkan topologi dengan minimal 3 segmen jaringan berbeda (mis. segmen pengguna, segmen server, segmen manajemen).
2. Menganalisis kebutuhan pembatasan akses sesuai skenario yang diberikan instruktur dan merancang kebijakan ACL yang sesuai (menentukan trafik apa saja yang perlu diizinkan/ditolak).

Tahap 2 — Konfigurasi ACL Standar (± 35 menit)

1. Membuat ACL standar untuk membatasi akses dari segmen tertentu menuju segmen lain berdasarkan alamat sumber.
2. Menerapkan ACL standar pada interface yang sesuai (sedekat mungkin dengan tujuan) menggunakan ip access-group.
3. Menguji hasil penerapan ACL standar dan mengamati trafik yang diizinkan/ditolak.

Tahap 3 — Konfigurasi ACL Extended (± 45 menit)

1. Membuat ACL extended untuk membatasi akses berdasarkan kombinasi sumber, tujuan, protokol, dan port (mis. hanya mengizinkan trafik HTTP menuju server tertentu).
2. Menerapkan ACL extended pada interface yang sesuai (sedekat mungkin dengan sumber) menggunakan ip access-group.
3. Menguji hasil penerapan ACL extended dan mengamati trafik yang diizinkan/ditolak sesuai protokol dan port yang ditentukan.

Tahap 4 — Pengujian Filter Trafik Menyeluruh (± 45 menit)

1. Melakukan pengujian ping/akses layanan dari berbagai segmen untuk membuktikan seluruh aturan ACL bekerja sesuai kebijakan yang dirancang.
2. Memverifikasi jumlah match pada setiap baris ACL menggunakan show access-lists.
3. Mendokumentasikan hasil pengujian (screenshot) sebagai bukti kerja.

Tahap 5 — Penutupan Sesi (± 20 menit)

1. Menyimpan file topologi (.pkt) sesuai konvensi penamaan file yang berlaku.
2. Merapikan area kerja dan mengembalikan perangkat sesuai prosedur K3.

F. Tugas Praktikum

Skenario: Sebuah perusahaan memiliki segmen jaringan Manajemen, Pengguna, dan Server. Kebijakan keamanan mensyaratkan: (1) hanya segmen Manajemen yang boleh mengakses seluruh layanan pada segmen Server tanpa batasan, (2) segmen Pengguna hanya boleh mengakses layanan web (HTTP) pada segmen Server, dan (3) segmen Pengguna tidak boleh mengakses segmen Manajemen sama sekali.

Ketentuan tugas:

1. Merancang dan menuliskan kebijakan ACL (dalam bentuk tabel: nomor ACL, aturan, arah, interface penerapan) sebelum implementasi.
2. Mengimplementasikan kebijakan menggunakan kombinasi ACL standar dan/atau extended sesuai kebutuhan setiap aturan.
3. Menguji dan membuktikan ketiga kebijakan akses berjalan sesuai skenario (segmen Pengguna hanya bisa HTTP ke Server, tidak bisa akses Manajemen sama sekali, dsb.).
4. Menyertakan tangkapan layar (screenshot) hasil show access-lists dan hasil pengujian akses dari setiap segmen.
5. Menyimpan file topologi (.pkt) sesuai konvensi penamaan yang berlaku.

G. Format Laporan Praktikum

Laporan disusun mengikuti Template Laporan Praktikum (Lampiran 1) dengan struktur sebagai berikut:

1. Halaman Judul (Modul, NIM, Nama, Kelompok jika ada)
2. Tujuan Praktikum
3. Alat dan Bahan yang Digunakan
4. Rancangan Kebijakan ACL (tabel aturan, arah, interface penerapan)
5. Langkah Kerja beserta Bukti Pelaksanaan (screenshot konfigurasi dan verifikasi)
6. Hasil Pengujian Filter Trafik
7. Kendala dan Solusi (jika ada)
8. Kesimpulan

Laporan dikumpulkan dalam format PDF/DOCX dengan nama file:
NIM_NamaMahasiswa_Modul11_Laporan, sesuai tenggat waktu yang ditentukan instruktur.

H. Rubrik Penilaian Ringkas

Penilaian menggunakan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55). Deskriptor lengkap keempat kategori untuk setiap aspek tersedia pada Rubrik Penilaian Praktikum per Pertemuan (Lampiran 3).

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Ketepatan Rancangan Kebijakan Akses	20%	Merancang kebijakan ACL yang tepat sesuai kebutuhan pembatasan akses pada skenario yang diberikan.	Rancangan kebijakan tidak sesuai dengan skenario.
Ketepatan Konfigurasi ACL Standar/Extended	35%	ACL standar/extended dikonfigurasi dan diterapkan (access-group) tepat sesuai urutan (order) dan arah (in/out) yang benar.	ACL tidak terkonfigurasi atau konfigurasi salah total.
Pengujian Filter Trafik	25%	Menguji dan membuktikan trafik yang diizinkan/ditolak sesuai kebijakan secara menyeluruh dan akurat.	Tidak melakukan pengujian filter trafik.
Dokumentasi Laporan Praktikum	20%	Laporan lengkap, sistematis, disertai rancangan kebijakan dan bukti hasil pengujian.	Tidak menyusun laporan praktikum.

Nilai Pertemuan 11 berkontribusi 2% terhadap komponen Tugas Praktikum (30%) pada nilai akhir mata kuliah, serta mendukung capaian CPL-5 dan CPL-8 sesuai Peta Kompetensi. Modul ini membuka topik CPMK-4 (keamanan dan tata kelola jaringan).

MODUL 12

FIREWALL DAN SEGMENTASI ZONA KEAMANAN JARINGAN

A. Identitas Modul

Modul / Pertemuan	Modul 12 / Pertemuan ke-12
Judul Modul	Firewall dan Segmentasi Zona Keamanan Jaringan
Sub-CPMK	Sub-CPMK-4.2 — Mampu mengonfigurasi firewall dan segmentasi zona keamanan jaringan (security zoning).
CPL Terkait	CPL-5, CPL-8
Metode Pembelajaran	Praktikum terbimbing, studi kasus segmentasi zona (DMZ, internal, eksternal)
Alokasi Waktu	170 menit (1 sks praktik)
Bobot Nilai	Kontribusi 2% dari komponen Tugas Praktikum (30%)

B. Tujuan Praktikum

Setelah mengikuti praktikum ini, mahasiswa diharapkan mampu:

1. Merancang dan menerapkan segmentasi zona keamanan (DMZ, internal, eksternal) sesuai prinsip keamanan berlapis (defense in depth).
2. Mengonfigurasi aturan firewall dasar untuk mengendalikan trafik antar-zona keamanan.
3. Menempatkan server/layanan yang dapat diakses publik pada zona DMZ secara tepat.
4. Menguji dan membuktikan trafik antar-zona terkendali sesuai kebijakan keamanan yang dirancang.

C. Dasar Teori Ringkas

1. Konsep Firewall pada Jaringan Enterprise

Firewall adalah perangkat atau fungsi keamanan yang mengendalikan aliran trafik antar-jaringan berdasarkan kebijakan keamanan yang telah ditentukan. Pada perangkat Cisco IOS, fungsi firewall dasar dapat diimplementasikan menggunakan kombinasi ACL extended dan konsep zona keamanan (zone-based policy), yang secara konseptual mengelompokkan interface ke dalam zona-zona dengan tingkat kepercayaan (trust level) berbeda.

2. Segmentasi Zona Keamanan (Security Zoning)

- Zona Internal (Trusted) — segmen jaringan privat perusahaan yang berisi pengguna dan sumber daya internal; memiliki tingkat kepercayaan tertinggi.
- Zona Eksternal (Untrusted) — jaringan publik/internet yang berada di luar kendali organisasi; memiliki tingkat kepercayaan terendah.
- Demilitarized Zone (DMZ) — zona perantara yang menampung server/layanan yang perlu diakses dari luar (mis. web server, mail server), diisolasi dari zona internal agar apabila DMZ diserang, zona internal tetap terlindungi.

3. Prinsip Keamanan Berlapis (Defense in Depth)

Prinsip ini menerapkan beberapa lapis kontrol keamanan sehingga apabila satu lapis berhasil ditembus, lapis berikutnya tetap dapat mencegah ancaman meluas. Pada konteks segmentasi zona, hal ini diwujudkan dengan kebijakan bahwa trafik dari zona eksternal tidak dapat langsung mencapai zona internal, melainkan harus melalui DMZ yang dikontrol ketat, sementara zona internal umumnya diberi akses lebih leluasa menuju DMZ maupun eksternal.

4. Kebijakan Umum Antar-Zona

- Eksternal → DMZ: diizinkan terbatas hanya pada port layanan publik yang disediakan (mis. HTTP/HTTPS).
- Eksternal → Internal: ditolak seluruhnya (tidak ada akses langsung).
- Internal → DMZ/Eksternal: diizinkan sesuai kebutuhan operasional (umumnya lebih longgar dari arah sebaliknya).
- DMZ → Internal: ditolak atau dibatasi sangat ketat untuk mencegah DMZ yang disusupi menjadi batu loncatan menyerang zona internal.

5. Penerapan Teknis

Pada praktikum ini, segmentasi zona dan aturan firewall diimplementasikan menggunakan kombinasi interface terpisah untuk setiap zona pada router/firewall serta ACL extended yang diterapkan pada masing-masing interface sesuai arah trafik dan kebijakan antar-zona yang telah dirancang (melanjutkan keterampilan ACL dari Modul 11).

D. Alat dan Bahan

Komponen	Keterangan
Perangkat Lunak	Cisco Packet Tracer (versi terbaru)
Perangkat Fisik (opsional)	1 router/firewall dengan minimal 3 interface (internal, DMZ, eksternal)
Perangkat Pendukung	PC pada zona internal, server simulasi (HTTP/FTP) pada zona DMZ, PC simulasi zona eksternal
Dokumen Pendukung	Template Laporan Praktikum (Lampiran 1), Topologi Referensi Modul 12 (Lampiran 2)

E. Langkah Kerja / Prosedur

Tahap 1 — Persiapan Topologi Tiga Zona (± 25 menit)

1. Membangun topologi dengan 3 zona keamanan: Internal, DMZ, dan Eksternal, masing-masing terhubung ke interface terpisah pada router/firewall.
2. Menempatkan server layanan publik (mis. web server) pada zona DMZ dan PC pengguna pada zona Internal.

Tahap 2 — Perancangan Kebijakan Antar-Zona (± 25 menit)

1. Menyusun matriks kebijakan antar-zona (Eksternal→DMZ, Eksternal→Internal, Internal→DMZ, Internal→Eksternal, DMZ→Internal) sesuai prinsip keamanan berlapis.

2. Menentukan protokol/port spesifik yang diizinkan pada setiap kebijakan (mis. hanya HTTP/HTTPS dari Eksternal menuju DMZ).

Tahap 3 — Konfigurasi Aturan Firewall (± 50 menit)

1. Mengonfigurasi ACL extended yang merepresentasikan setiap kebijakan antar-zona pada matriks yang telah disusun.
2. Menerapkan ACL pada interface dan arah (in/out) yang sesuai untuk setiap zona.
3. Memverifikasi konfigurasi menggunakan show access-lists dan show running-config.

Tahap 4 — Pengujian Efektivitas Segmentasi (± 50 menit)

1. Menguji akses dari zona Eksternal menuju DMZ (harus berhasil sesuai port yang diizinkan) dan menuju Internal (harus gagal total).
2. Menguji akses dari zona Internal menuju DMZ dan Eksternal (harus berhasil sesuai kebijakan).
3. Menguji akses dari zona DMZ menuju Internal (harus gagal/dibatasi sesuai kebijakan).
4. Mendokumentasikan seluruh hasil pengujian (screenshot) sebagai bukti kerja.

Tahap 5 — Penutupan Sesi (± 20 menit)

1. Menyimpan file topologi (.pkt) sesuai konvensi penamaan file yang berlaku.
2. Merapikan area kerja dan mengembalikan perangkat sesuai prosedur K3.

F. Tugas Praktikum

Skenario: Sebuah perusahaan menyediakan layanan web perusahaan yang dapat diakses publik dari internet, namun harus memastikan jaringan internal perusahaan (berisi data karyawan dan sistem internal) tetap terlindungi meskipun server web tersebut diserang dari luar.

Ketentuan tugas:

1. Merancang segmentasi 3 zona (Internal, DMZ, Eksternal) beserta matriks kebijakan akses antar-zona sesuai prinsip keamanan berlapis.
2. Menempatkan web server pada zona DMZ dan mengizinkan akses HTTP/HTTPS dari zona Eksternal hanya menuju DMZ.
3. Memastikan zona Eksternal maupun zona DMZ sama sekali tidak dapat mengakses zona Internal secara langsung.
4. Menyertakan tangkapan layar (screenshot) hasil pengujian akses dari ketiga zona serta hasil show access-lists.
5. Menyimpan file topologi (.pkt) sesuai konvensi penamaan yang berlaku.

G. Format Laporan Praktikum

Laporan disusun mengikuti Template Laporan Praktikum (Lampiran 1) dengan struktur sebagai berikut:

1. Halaman Judul (Modul, NIM, Nama, Kelompok jika ada)
2. Tujuan Praktikum
3. Alat dan Bahan yang Digunakan
4. Skema Zona Keamanan dan Matriks Kebijakan Antar-Zona

5. Langkah Kerja beserta Bukti Pelaksanaan (screenshot konfigurasi dan verifikasi)
6. Hasil Pengujian Efektivitas Segmentasi
7. Kendala dan Solusi (jika ada)
8. Kesimpulan

Laporan dikumpulkan dalam format PDF/DOCX dengan nama file: NIM_NamaMahasiswa_Modul12_Laporan, sesuai tenggat waktu yang ditentukan instruktur.

H. Rubrik Penilaian Ringkas

Penilaian menggunakan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55). Deskriptor lengkap keempat kategori untuk setiap aspek tersedia pada Rubrik Penilaian Praktikum per Pertemuan (Lampiran 3).

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Ketepatan Segmentasi Zona Keamanan	25%	Merancang dan menerapkan segmentasi zona (DMZ, internal, eksternal) yang tepat sesuai prinsip keamanan berlapis.	Segmentasi zona tidak sesuai atau tidak diterapkan.
Ketepatan Aturan Firewall	35%	Aturan firewall dikonfigurasi lengkap dan tepat untuk mengendalikan trafik antar-zona sesuai kebijakan.	Aturan firewall tidak terkonfigurasi atau konfigurasi salah total.
Pengujian Efektivitas Segmentasi	20%	Menguji dan membuktikan trafik antar-zona terkendali sesuai kebijakan keamanan yang dirancang.	Tidak melakukan pengujian efektivitas segmentasi.
Dokumentasi Laporan Praktikum	20%	Laporan lengkap, sistematis, disertai skema zona dan bukti hasil pengujian.	Tidak menyusun laporan praktikum.

Nilai Pertemuan 12 berkontribusi 2% terhadap komponen Tugas Praktikum (30%) pada nilai akhir mata kuliah, serta mendukung capaian CPL-5 dan CPL-8 sesuai Peta Kompetensi.

MODUL 13

MONITORING JARINGAN (SNMP/SYSLOG) DAN TROUBLESHOOTING SISTEMATIS

A. Identitas Modul

Modul / Pertemuan	Modul 13 / Pertemuan ke-13
Judul Modul	Monitoring Jaringan (SNMP/Syslog) dan Troubleshooting Sistematis
Sub-CPMK	Sub-CPMK-4.3 — Mampu menerapkan monitoring jaringan (SNMP/syslog) serta mendiagnosis dan mengatasi gangguan jaringan (troubleshooting).
CPL Terkait	CPL-5, CPL-8
Metode Pembelajaran	Demonstrasi, praktikum terbimbing, studi kasus gangguan jaringan (fault injection)
Alokasi Waktu	170 menit (1 sks praktik)
Bobot Nilai	Kontribusi 2% dari komponen Tugas Praktikum (30%)

B. Tujuan Praktikum

Setelah mengikuti praktikum ini, mahasiswa diharapkan mampu:

1. Mengonfigurasi SNMP untuk pemantauan status perangkat jaringan secara real-time.
2. Mengonfigurasi syslog untuk pencatatan (logging) kejadian/log perangkat ke server terpusat.
3. Menerapkan metode troubleshooting berlapis secara sistematis (dari physical hingga application layer) pada skenario gangguan jaringan.
4. Mendiagnosis akar masalah (root cause) gangguan jaringan secara tepat dan efisien.

C. Dasar Teori Ringkas

1. Simple Network Management Protocol (SNMP)

SNMP adalah protokol standar untuk memantau dan mengelola perangkat jaringan dari satu titik terpusat (Network Management Station/NMS). Perangkat jaringan (agent) menyimpan informasi status (mis. penggunaan CPU, memori, status interface) dalam struktur data Management Information Base (MIB), yang dapat diambil oleh NMS melalui operasi get atau dikirimkan secara proaktif melalui trap ketika terjadi kejadian tertentu.

2. Syslog

Syslog adalah standar protokol pencatatan log yang memungkinkan perangkat jaringan mengirimkan pesan log (informasi, peringatan, error, hingga kondisi kritikal) ke server syslog terpusat. Setiap pesan syslog memiliki tingkat keparahan (severity level 0–7, dari Emergency hingga Debugging) yang membantu administrator memprioritaskan penanganan berdasarkan urgensi.

3. Metode Troubleshooting Sistematis (Berlapis)

Troubleshooting sistematis dilakukan dengan menelusuri lapisan model OSI/TCP-IP secara berurutan (top-down, bottom-up, atau divide-and-conquer) untuk mengisolasi lapisan mana yang menjadi sumber gangguan, dimulai dari pemeriksaan fisik (kabel, port, indikator LED) hingga lapisan aplikasi

(layanan yang berjalan di atas jaringan). Pendekatan sistematis mencegah troubleshooting yang bersifat coba-coba (trial and error) yang tidak efisien.

- Lapisan Fisik — memeriksa kabel, port, indikator LED, dan status interface (up/down).
- Lapisan Data Link — memeriksa VLAN, trunk, spanning-tree, dan tabel MAC address.
- Lapisan Network — memeriksa alamat IP, tabel routing, dan konfigurasi ACL/firewall.
- Lapisan Aplikasi — memeriksa ketersediaan dan konfigurasi layanan (server, port) yang diakses pengguna.

4. Perintah Dasar Konfigurasi Monitoring

```
SNMP:
snmp-server community <string> RO|RW    → mengatur community string SNMP
snmp-server location <lokasi>            → mengatur informasi lokasi perangkat
snmp-server host <ip> <community>        → mengatur tujuan pengiriman trap SNMP
Syslog:
logging host <ip>                        → mengatur alamat server syslog tujuan
logging trap <level>                     → mengatur tingkat keparahan log yang
dikirim
show logging                             → menampilkan buffer log lokal
perangkat
Troubleshooting:
show interfaces status                   → memeriksa status fisik/data link
interface
show ip interface brief                  → memeriksa status dan alamat IP
seluruh interface
```

D. Alat dan Bahan

Komponen	Keterangan
Perangkat Lunak	Cisco Packet Tracer (versi terbaru), server simulasi SNMP/Syslog
Perangkat Fisik (opsional)	Minimal 2 unit switch/router yang telah dikonfigurasi pada modul sebelumnya
Perangkat Pendukung	1 unit PC/server sebagai NMS dan syslog server
Dokumen Pendukung	Template Laporan Praktikum (Lampiran 1), Topologi Referensi Modul 13 (Lampiran 2)

E. Langkah Kerja / Prosedur

Tahap 1 — Persiapan Topologi Monitoring (± 20 menit)

1. Melanjutkan topologi dari modul sebelumnya dan menambahkan 1 unit PC/server sebagai NMS/syslog server.
2. Memastikan konektivitas dasar antara perangkat yang akan dipantau dengan NMS/syslog server.

Tahap 2 — Konfigurasi SNMP (± 35 menit)

1. Mengatur community string (read-only dan/atau read-write) pada setiap perangkat yang akan dipantau.

2. Mengatur tujuan pengiriman trap SNMP ke alamat IP NMS.
3. Memverifikasi konfigurasi SNMP menggunakan show snmp dan menguji polling dari NMS (jika tersedia).

Tahap 3 — Konfigurasi Syslog (± 35 menit)

1. Mengatur alamat server syslog tujuan pada setiap perangkat menggunakan logging host.
2. Mengatur tingkat keparahan log yang akan dikirimkan menggunakan logging trap.
3. Memverifikasi pesan log yang tercatat menggunakan show logging pada perangkat dan pada tampilan syslog server.

Tahap 4 — Simulasi Gangguan dan Troubleshooting Sistematis (± 60 menit)

1. Menerima skenario gangguan jaringan yang telah disiapkan instruktur (fault injection) tanpa mengetahui penyebabnya terlebih dahulu.
2. Menelusuri gangguan secara sistematis mulai dari lapisan fisik hingga lapisan aplikasi menggunakan perintah show yang relevan pada setiap lapisan.
3. Mengidentifikasi akar masalah (root cause) dan memperbaiki konfigurasi yang menjadi penyebab gangguan.
4. Memverifikasi bahwa gangguan telah teratasi dan mendokumentasikan seluruh proses diagnosis (screenshot tiap lapisan pemeriksaan) sebagai bukti kerja.

Tahap 5 — Penutupan Sesi (± 20 menit)

1. Menyimpan file topologi (.pkt) sesuai konvensi penamaan file yang berlaku.
2. Merapikan area kerja dan mengembalikan perangkat sesuai prosedur K3.

F. Tugas Praktikum

Skenario: Tim operasional jaringan memerlukan sistem pemantauan terpusat agar dapat mendeteksi gangguan sedini mungkin. Pada sesi ini, instruktur akan menyisipkan satu gangguan tersembunyi pada topologi (mis. VLAN salah, ACL memblokir trafik yang seharusnya diizinkan, atau interface dinonaktifkan) yang harus ditemukan dan diperbaiki mahasiswa.

Ketentuan tugas:

1. Mengonfigurasi SNMP dan syslog pada seluruh perangkat topologi menuju satu NMS/syslog server terpusat.
2. Menemukan gangguan tersembunyi yang disiapkan instruktur melalui proses troubleshooting sistematis (menyebutkan lapisan mana yang diperiksa dan urutannya).
3. Memperbaiki konfigurasi yang menjadi akar masalah hingga jaringan kembali berfungsi normal.
4. Menyertakan tangkapan layar (screenshot) proses diagnosis bertahap serta hasil show logging dari syslog server.
5. Menyimpan file topologi (.pkt) sesuai konvensi penamaan yang berlaku.

G. Format Laporan Praktikum

Laporan disusun mengikuti Template Laporan Praktikum (Lampiran 1) dengan struktur sebagai berikut:

1. Halaman Judul (Modul, NIM, Nama, Kelompok jika ada)

2. Tujuan Praktikum
3. Alat dan Bahan yang Digunakan
4. Konfigurasi Monitoring (SNMP dan Syslog)
5. Log Hasil Monitoring dan Catatan Proses Troubleshooting (bertahap per lapisan)
6. Akar Masalah (Root Cause) dan Solusi yang Diterapkan
7. Kendala Tambahan (jika ada)
8. Kesimpulan

Laporan dikumpulkan dalam format PDF/DOCX dengan nama file: NIM_NamaMahasiswa_Modul13_Laporan, sesuai tenggat waktu yang ditentukan instruktur.

H. Rubrik Penilaian Ringkas

Penilaian menggunakan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55). Deskriptor lengkap keempat kategori untuk setiap aspek tersedia pada Rubrik Penilaian Praktikum per Pertemuan (Lampiran 3).

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Ketepatan Konfigurasi Monitoring	30%	SNMP/syslog dikonfigurasi lengkap dan tepat sehingga status perangkat dan log kejadian dapat dipantau secara real-time.	Monitoring tidak terkonfigurasi atau tidak berfungsi.
Penerapan Metode Troubleshooting Sistematis	35%	Menerapkan metode troubleshooting berlapis (dari physical hingga application layer) secara sistematis pada skenario gangguan yang diberikan.	Tidak mampu mengidentifikasi maupun mengatasi gangguan yang diberikan.
Ketepatan Diagnosis Gangguan	20%	Berhasil mendiagnosis akar masalah (root cause) gangguan jaringan secara tepat dan efisien.	Tidak berhasil mendiagnosis akar masalah gangguan.
Dokumentasi Laporan Praktikum	15%	Laporan lengkap, sistematis, disertai log hasil monitoring dan catatan proses troubleshooting.	Tidak menyusun laporan praktikum.

Nilai Pertemuan 13 berkontribusi 2% terhadap komponen Tugas Praktikum (30%) pada nilai akhir mata kuliah, serta mendukung capaian CPL-5 dan CPL-8 sesuai Peta Kompetensi. Modul ini menutup topik CPMK-4 (Modul 11–13).

MODUL 14

PERANCANGAN TOPOLOGI DAN DOKUMENTASI TEKNIS JARINGAN ENTERPRISE (PROYEK KELOMPOK, BAGIAN 1)

A. Identitas Modul

Modul / Pertemuan	Modul 14 / Pertemuan ke-14 (Proyek Kelompok, Bagian 1)
Judul Modul	Perancangan Topologi dan Dokumentasi Teknis Jaringan Enterprise
Sub-CPMK	Sub-CPMK-5.1 — Mampu merancang topologi dan menyusun dokumentasi teknis jaringan enterprise secara berkelompok.
CPL Terkait	CPL-9, CPL-10
Metode Pembelajaran	Project-based learning, kerja kelompok, konsultasi (asistensi)
Alokasi Waktu	170 menit (1 sks praktik)
Bobot Nilai	Kontribusi 2% dari komponen Tugas Praktikum (30%)

B. Tujuan Praktikum

Setelah mengikuti praktikum ini, mahasiswa diharapkan mampu:

1. Merancang topologi jaringan enterprise skala kecil-menengah yang layak dan sesuai kebutuhan skenario perusahaan/organisasi yang ditentukan.
2. Menyusun skema pengalamatan IP, pembagian VLAN, dan kebijakan (ACL/keamanan) secara tepat dan efisien.
3. Menyusun dokumentasi teknis proyek jaringan yang lengkap dan profesional.
4. Bekerja sama secara efektif dalam kelompok kerja kecil-menengah dengan pembagian tugas yang jelas.

C. Dasar Teori Ringkas

1. Prinsip Perancangan Jaringan Enterprise

Perancangan jaringan enterprise yang baik mengacu pada model hierarkis (access, distribution, core) yang memisahkan fungsi jaringan berdasarkan lapisan agar mudah dikelola, diskalakan, dan ditelusuri ketika terjadi gangguan. Rancangan juga perlu mempertimbangkan aspek redundansi, skalabilitas, keamanan, dan kemudahan pemeliharaan, sesuai praktik-praktik yang telah dipelajari pada Modul 1–13 (VLAN, routing, redundansi gateway, VPN, ACL, firewall, dan monitoring).

2. Perencanaan Alokasi IP dan VLAN

Skema pengalamatan IP yang efisien mempertimbangkan jumlah host pada setiap segmen, potensi pertumbuhan di masa depan, serta penggunaan teknik subnetting/VLSM (Variable Length Subnet Mask) agar alokasi alamat tidak boros. Pembagian VLAN disusun berdasarkan kebutuhan fungsional/departemen organisasi, sejalan dengan praktik pada Modul 2–3.

3. Dokumentasi Teknis Proyek Jaringan

Dokumentasi teknis yang baik mencakup diagram topologi (fisik dan logis), tabel alokasi IP dan VLAN, deskripsi kebijakan keamanan yang diterapkan, serta justifikasi teknis atas setiap keputusan desain. Dokumentasi berfungsi sebagai referensi bagi tim implementasi maupun pemeliharaan jaringan di masa mendatang, dan menjadi bagian penting dari praktik keteknikan profesional (mendukung CPL-9 dan CPL-10).

4. Kerja Kelompok dalam Proyek Teknis

Proyek jaringan skala kecil-menengah pada praktik industri umumnya dikerjakan secara tim dengan pembagian peran (mis. perancang topologi, penanggung jawab alokasi IP/VLAN, penanggung jawab dokumentasi, dan koordinator kelompok). Pembagian tugas yang jelas dan kontribusi merata dari setiap anggota menjadi kunci keberhasilan proyek serta mendukung pengembangan kompetensi kerja sama tim (CPL-9).

D. Alat dan Bahan

Komponen	Keterangan
Perangkat Lunak	Cisco Packet Tracer (versi terbaru), aplikasi pengolah dokumen/diagram (mis. Word, Visio, atau draw.io)
Perangkat Pendukung	Laptop/komputer masing-masing anggota kelompok
Dokumen Pendukung	Lembar Skenario Studi Kasus Proyek, Template Dokumentasi Teknis Proyek (Lampiran 1), Rubrik Penilaian Proyek Kelompok (Lampiran 3)

E. Langkah Kerja / Prosedur

Tahap 1 — Pembentukan Kelompok dan Pemilihan Studi Kasus (± 20 menit)

1. Membentuk kelompok kerja beranggotakan 3–4 orang sesuai pembagian instruktur.
2. Memilih atau menerima penugasan studi kasus perusahaan/organisasi (mis. kantor cabang retail, kampus, rumah sakit, hotel) dari daftar yang disediakan instruktur.
3. Menyepakati pembagian peran dalam kelompok (perancang topologi, penanggung jawab IP/VLAN, penanggung jawab dokumentasi, koordinator).

Tahap 2 — Analisis Kebutuhan dan Perancangan Topologi (± 50 menit)

1. Menganalisis kebutuhan jaringan studi kasus (jumlah departemen/segmen, estimasi jumlah pengguna, kebutuhan redundansi, kebutuhan keamanan).
2. Merancang topologi jaringan (diagram fisik dan logis) yang mengintegrasikan minimal: segmentasi VLAN, routing antar-VLAN, redundansi gateway, dan kebijakan keamanan dasar.

Tahap 3 — Penyusunan Skema Alokasi IP, VLAN, dan Kebijakan (± 45 menit)

1. Menyusun skema pengalamatan IP (subnetting/VLSM) untuk seluruh segmen sesuai kebutuhan studi kasus.
2. Menyusun tabel VLAN (ID, nama, keanggotaan segmen) dan kebijakan akses (ACL/firewall) yang akan diterapkan.

Tahap 4 — Penyusunan Dokumentasi Teknis (± 35 menit)

1. Menyusun dokumentasi teknis proyek sesuai Template Dokumentasi Teknis Proyek (Lampiran 1), mencakup diagram topologi, tabel alokasi, dan deskripsi kebijakan.
2. Melakukan sesi konsultasi (asistensi) dengan instruktur untuk mendapatkan umpan balik atas rancangan sementara.

Tahap 5 — Penutupan Sesi (± 20 menit)

1. Menyimpan seluruh berkas rancangan dan dokumentasi kelompok sesuai konvensi penamaan file yang berlaku.
2. Menyepakati pembagian tugas lanjutan untuk implementasi dan persiapan presentasi pada Modul 15.

F. Tugas Praktikum

Skenario: Setiap kelompok berperan sebagai konsultan jaringan yang ditugaskan merancang infrastruktur jaringan enterprise skala kecil-menengah untuk studi kasus organisasi yang ditentukan instruktur (mis. kantor cabang retail 3 lantai dengan 5 departemen).

Ketentuan tugas:

1. Merancang topologi jaringan yang mencakup minimal: segmentasi VLAN (≥ 4 VLAN), routing antar-VLAN, redundansi gateway, dan kebijakan ACL dasar.
2. Menyusun skema pengalamatan IP (subnetting) untuk seluruh VLAN/segmen yang dirancang.
3. Menyusun dokumentasi teknis lengkap (diagram topologi, tabel alokasi IP/VLAN, deskripsi kebijakan) sesuai template yang disediakan.
4. Memastikan pembagian tugas kelompok tercatat dengan jelas (nama anggota dan peran masing-masing) dalam dokumentasi.
5. Menyerahkan dokumentasi teknis (draf) pada akhir sesi sebagai bahan konsultasi/asistensi lanjutan menuju Modul 15.

G. Format Dokumentasi Teknis Proyek

Dokumentasi teknis proyek kelompok disusun mengikuti Template Dokumentasi Teknis Proyek (Lampiran 1) dengan struktur sebagai berikut:

1. Halaman Judul Proyek (nama kelompok, anggota beserta peran, studi kasus yang dipilih)
2. Deskripsi dan Analisis Kebutuhan Studi Kasus
3. Diagram Topologi Jaringan (fisik dan logis)
4. Skema Pengalamatan IP dan Pembagian VLAN (tabel lengkap)
5. Deskripsi Kebijakan Keamanan (ACL/firewall) yang Direncanakan
6. Justifikasi Teknis Keputusan Desain
7. Rencana Implementasi dan Pembagian Tugas Lanjutan (untuk Modul 15)

Dokumentasi dikumpulkan dalam format PDF/DOCX dengan nama file:
Kelompok[X]_Modul14_DokumentasiTeknis, sesuai tenggat waktu yang ditentukan instruktur.

H. Rubrik Penilaian Ringkas

Penilaian menggunakan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55). Deskriptor lengkap keempat kategori untuk setiap aspek tersedia pada Rubrik Penilaian Praktikum per Pertemuan (Lampiran 3).

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Kelayakan & Kelengkapan Rancangan Topologi	30%	Rancangan topologi lengkap, layak diimplementasikan, dan sesuai kebutuhan skenario perusahaan/organisasi yang ditentukan.	Rancangan topologi tidak layak atau tidak diselesaikan.
Ketepatan Alokasi IP, VLAN & Kebijakan	25%	Skema pengalamatan IP, pembagian VLAN, dan kebijakan (ACL/keamanan) dirancang tepat dan efisien.	Skema tidak dirancang atau dirancang secara keliru.
Kualitas Dokumentasi Teknis	25%	Dokumentasi teknis lengkap dan profesional (diagram topologi, tabel alokasi, deskripsi kebijakan) sesuai kaidah dokumentasi proyek jaringan.	Dokumentasi tidak disusun.
Kerja Sama Tim	20%	Seluruh anggota kelompok berkontribusi aktif dan merata sesuai pembagian tugas yang jelas.	Tidak terdapat kerja sama tim yang efektif.

Nilai Pertemuan 14 berkontribusi 2% terhadap komponen Tugas Praktikum (30%) pada nilai akhir mata kuliah, serta mendukung capaian CPL-9 dan CPL-10 sesuai Peta Kompetensi. Modul ini membuka CPMK-5, merupakan bagian pertama dari dua bagian proyek kelompok integratif (dilanjutkan pada Modul 15 untuk implementasi dan presentasi).

MODUL 15

IMPLEMENTASI, PRESENTASI HASIL RANCANGAN, DAN JALUR SERTIFIKASI PROFESI (PROYEK KELOMPOK, BAGIAN 2)

A. Identitas Modul

Modul / Pertemuan	Modul 15 / Pertemuan ke-15 (Proyek Kelompok, Bagian 2)
Judul Modul	Implementasi, Presentasi Hasil Rancangan, dan Jalur Sertifikasi Profesi
Sub-CPMK	Sub-CPMK-5.2 — Mampu mempresentasikan hasil rancangan jaringan secara profesional dan menjelaskan jalur sertifikasi kompetensi terkait (CCNA/MTCNA).
CPL Terkait	CPL-9, CPL-10, CPL-12
Metode Pembelajaran	Presentasi kelompok, demonstrasi konfigurasi, diskusi tanya-jawab
Alokasi Waktu	170 menit (1 sks praktik)
Bobot Nilai	Kontribusi 3% dari komponen Tugas Praktikum (30%)

B. Tujuan Praktikum

Setelah mengikuti praktikum ini, mahasiswa diharapkan mampu:

1. Mengimplementasikan rancangan topologi dari Modul 14 pada simulator/perangkat sesuai dokumentasi teknis yang telah disusun.
2. Mempresentasikan hasil rancangan dan implementasi jaringan secara jelas, terstruktur, dan profesional.
3. Menjawab pertanyaan terkait rancangan dengan tepat, menunjukkan penguasaan penuh atas pekerjaan kelompok.
4. Menjelaskan keterkaitan materi praktikum dengan skema sertifikasi kompetensi profesi jaringan (CCNA/MTCNA).

C. Dasar Teori Ringkas

1. Dari Rancangan Menuju Implementasi

Tahap implementasi menerjemahkan dokumentasi teknis (diagram topologi, skema IP/VLAN, kebijakan keamanan) yang disusun pada Modul 14 menjadi konfigurasi nyata pada simulator atau perangkat laboratorium. Proses ini menuntut ketelitian agar hasil implementasi benar-benar sesuai dengan rancangan, sekaligus melatih kemampuan mengidentifikasi dan menyesuaikan rancangan apabila ditemukan kendala teknis saat implementasi.

2. Komunikasi Teknis dan Presentasi Profesional

Kemampuan menyampaikan hasil kerja teknis secara lisan merupakan kompetensi penting bagi praktisi jaringan, khususnya saat berkomunikasi dengan atasan, klien, atau tim lain yang tidak selalu memiliki latar belakang teknis mendalam. Presentasi teknis yang efektif menyampaikan konteks kebutuhan, keputusan desain, hasil implementasi, dan kendala secara ringkas dan terstruktur, didukung alat bantu visual (diagram, tangkapan layar hasil verifikasi) yang relevan.

3. Jalur Sertifikasi Kompetensi Profesi Jaringan

Sertifikasi kompetensi merupakan pengakuan formal atas keterampilan teknis seseorang di bidang jaringan, yang umum menjadi persyaratan atau nilai tambah dalam dunia kerja industri jaringan dan telekomunikasi.

- CCNA (Cisco Certified Network Associate) — sertifikasi tingkat associate dari Cisco yang mencakup fondasi jaringan, termasuk topik-topik yang telah dipraktikkan sepanjang mata kuliah ini seperti VLAN, routing, keamanan dasar, dan otomasi jaringan.
- MTCNA (MikroTik Certified Network Associate) — sertifikasi dasar dari MikroTik yang berfokus pada konfigurasi dan manajemen perangkat RouterOS, relevan bagi lulusan yang bekerja dengan perangkat berbasis MikroTik di industri.

Pemahaman atas jalur sertifikasi ini membantu mahasiswa merencanakan pengembangan kompetensi berkelanjutan setelah menyelesaikan mata kuliah, sejalan dengan capaian CPL-10.

D. Alat dan Bahan

Komponen	Keterangan
Perangkat Lunak	Cisco Packet Tracer (versi terbaru), aplikasi presentasi (mis. PowerPoint/Google Slides)
Perangkat Pendukung	Laptop/komputer kelompok, proyektor/layar presentasi
Dokumen Pendukung	Dokumentasi Teknis Proyek (hasil Modul 14), Rubrik Penilaian Proyek Kelompok (Lampiran 3), Ringkasan Jalur Sertifikasi CCNA/MTCNA

E. Langkah Kerja / Prosedur

Tahap 1 — Implementasi Rancangan (± 50 menit)

1. Setiap kelompok mengimplementasikan topologi, VLAN, routing, redundansi gateway, dan kebijakan keamanan sesuai dokumentasi teknis Modul 14 pada Cisco Packet Tracer.
2. Melakukan verifikasi menyeluruh atas hasil implementasi (konektivitas antar-segmen, status redundansi, efektivitas kebijakan ACL) dan menyesuaikan rancangan apabila ditemukan kendala teknis.

Tahap 2 — Persiapan Materi Presentasi (± 25 menit)

1. Menyusun bahan presentasi ringkas (slide atau media visual lain) yang mencakup: konteks studi kasus, ringkasan rancangan, hasil implementasi, dan kendala/solusi yang dihadapi.
2. Menyiapkan pembagian peran presentasi antar-anggota kelompok.

Tahap 3 — Presentasi dan Demonstrasi (± 15 menit per kelompok, menyesuaikan jumlah kelompok)

1. Setiap kelompok mempresentasikan hasil rancangan dan implementasi secara bergiliran di hadapan instruktur dan/atau kelompok lain.
2. Melakukan demonstrasi langsung sebagian konfigurasi kunci (mis. pengujian failover redundansi gateway atau verifikasi kebijakan ACL) sebagai bukti implementasi berfungsi.

Tahap 4 — Sesi Tanya-Jawab dan Diskusi Jalur Sertifikasi (± 40 menit)

1. Menjawab pertanyaan dari instruktur/kelompok lain terkait keputusan desain dan hasil implementasi.
2. Menjelaskan keterkaitan kompetensi yang dipraktikkan sepanjang mata kuliah dengan skema sertifikasi CCNA/MTCNA.

Tahap 5 — Penutupan Sesi (± 20 menit)

1. Menyimpan file topologi final dan bahan presentasi sesuai konvensi penamaan file yang berlaku.
2. Merapikan area kerja dan mengembalikan perangkat sesuai prosedur K3.

F. Tugas Praktikum

Melanjutkan proyek kelompok dari Modul 14, setiap kelompok bertindak sebagai konsultan jaringan yang mempresentasikan hasil implementasi kepada 'manajemen perusahaan' (diperankan oleh instruktur) untuk memperoleh persetujuan akhir.

Ketentuan tugas:

1. Mengimplementasikan seluruh elemen rancangan Modul 14 pada Cisco Packet Tracer dan memverifikasi fungsinya sesuai dokumentasi teknis.
2. Menyusun dan menyampaikan presentasi kelompok (maksimal 15 menit) yang mencakup ringkasan rancangan, hasil implementasi, dan kendala/solusi.
3. Melakukan minimal satu demonstrasi langsung (live demo) atas konfigurasi kunci hasil implementasi.
4. Menjawab pertanyaan dari instruktur terkait rancangan, implementasi, maupun keterkaitannya dengan jalur sertifikasi profesi.
5. Menyerahkan file topologi final (.pkt) dan bahan presentasi sesuai konvensi penamaan yang berlaku.

G. Format Penyerahan Hasil Proyek

Hasil akhir proyek kelompok diserahkan dalam bentuk:

1. File topologi final (.pkt) dengan nama file: Kelompok[X]_Modul15_TopologiFinal.pkt
2. Bahan presentasi (slide/media visual) dengan nama file: Kelompok[X]_Modul15_Presentasi
3. Dokumentasi teknis final (revisi dari Modul 14 berdasarkan hasil implementasi dan umpan balik) dengan nama file: Kelompok[X]_Modul15_DokumentasiFinal

Seluruh berkas dikumpulkan sesuai mekanisme dan tenggat waktu yang ditentukan instruktur.

H. Rubrik Penilaian Ringkas

Penilaian menggunakan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55). Deskriptor lengkap keempat kategori untuk setiap aspek tersedia pada Rubrik Penilaian Praktikum per Pertemuan (Lampiran 3).

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Kesesuaian Implementasi dengan Rancangan	30%	Implementasi pada simulator/perangkat sepenuhnya	Implementasi tidak sesuai rancangan atau tidak berfungsi.

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
		sesuai rancangan topologi dan kebijakan yang telah disusun, serta berfungsi sesuai ekspektasi.	
Kualitas Presentasi & Komunikasi	25%	Presentasi disampaikan secara jelas, terstruktur, dan profesional dengan alat bantu visual yang efektif.	Presentasi tidak disampaikan dengan baik atau tidak dilakukan.
Penguasaan Materi (Tanya-Jawab)	25%	Mampu menjawab seluruh pertanyaan dengan tepat dan menunjukkan penguasaan penuh atas rancangan yang dibuat.	Tidak mampu menjawab pertanyaan dengan memadai.
Pemahaman Jalur Sertifikasi Profesi	20%	Mampu menjelaskan keterkaitan materi praktikum dengan skema sertifikasi (CCNA/MTCNA) secara tepat dan relevan.	Tidak mampu menjelaskan keterkaitan dengan jalur sertifikasi profesi.

Nilai Pertemuan 15 berkontribusi 3% terhadap komponen Tugas Praktikum (30%) pada nilai akhir mata kuliah, serta mendukung capaian CPL-9, CPL-10, dan CPL-12 sesuai Peta Kompetensi. Modul ini menutup CPMK-5 sekaligus menjadi materi terakhir sebelum UAS (Modul 16).

MODUL 16

UJIAN AKHIR SEMESTER (UAS) — UJIAN PRAKTIK KOMPREHENSIF DAN PRESENTASI PROYEK AKHIR

A. Identitas Modul

Modul / Pertemuan	Modul 16 / Pertemuan ke-16 (Evaluasi Akhir Semester)
Judul Modul	Ujian Akhir Semester (UAS) — Ujian Praktik Komprehensif dan Presentasi Proyek Akhir
Cakupan Sub-CPMK	Sub-CPMK-3.1 s.d. Sub-CPMK-5.2 (Modul 9–15), terintegrasi dengan Modul 1–8
CPL Terkait	CPL-5, CPL-8, CPL-9, CPL-10, CPL-12
Metode Ujian	Ujian praktik individual/kelompok, presentasi akhir
Alokasi Waktu	170 menit (1 sks praktik)
Bobot Nilai	30% dari nilai akhir mata kuliah (komponen UAS)

B. Tujuan Ujian

Ujian Akhir Semester (UAS) bertujuan mengevaluasi ketercapaian Sub-CPMK-3.1 hingga Sub-CPMK-5.2 secara komprehensif, sekaligus mengevaluasi keseluruhan kompetensi mata kuliah secara terintegrasi bersama capaian Modul 1–8 (yang telah dievaluasi pada UTS). Secara spesifik, UAS mengevaluasi kemampuan mahasiswa dalam:

1. Mengonfigurasi redundansi gateway (HSRP/VRRP) dan VPN site-to-site berbasis IPSec (Modul 9 –10).
2. Menerapkan ACL, firewall, segmentasi zona keamanan, serta monitoring dan troubleshooting jaringan (Modul 11–13).
3. Merevisi dan memfinalisasi rancangan proyek kelompok berdasarkan umpan balik dari Modul 14–15.
4. Mempresentasikan dan mempertanggungjawabkan seluruh hasil kerja secara jelas dan profesional.

C. Cakupan Materi Ujian

Cakupan materi ujian merangkum seluruh Sub-CPMK yang telah dipraktikkan pada Modul 9–15, tanpa memuat materi baru, dan terintegrasi dengan capaian Modul 1–8 yang telah dievaluasi pada UTS.

Modul	Materi	Sub-CPMK Diujikan
9	Redundansi Gateway (HSRP/VRRP)	Sub-CPMK-3.1
10	VPN Site-to-Site Berbasis IPSec	Sub-CPMK-3.2
11	Access Control List (ACL)	Sub-CPMK-4.1
12	Firewall dan Segmentasi Zona Keamanan	Sub-CPMK-4.2
13	Monitoring Jaringan dan Troubleshooting	Sub-CPMK-4.3

Modul	Materi	Sub-CPMK Diujikan
14–15	Proyek Kelompok: Perancangan, Implementasi, Presentasi	Sub-CPMK-5.1, 5.2

D. Ketentuan dan Tata Tertib Ujian

1. UAS terdiri atas dua komponen: (1) ujian praktik konfigurasi komprehensif bersifat individual, dan (2) presentasi/revisi akhir proyek kelompok (kelanjutan Modul 14–15).
2. Untuk komponen ujian praktik individual, mahasiswa dilarang bekerja sama atau berbagi jawaban dengan mahasiswa lain.
3. Untuk komponen presentasi proyek kelompok, seluruh anggota kelompok wajib hadir dan berperan aktif dalam sesi presentasi/tanya-jawab.
4. Mahasiswa wajib menerapkan prosedur K3 laboratorium selama ujian berlangsung, mendukung penilaian CPL-12.
5. Setiap mahasiswa/kelompok dapat memperoleh variasi skenario/pertanyaan yang berbeda untuk mencegah kecurangan.
6. Segala bentuk kecurangan akan ditindak sesuai kode etik akademik yang berlaku.

E. Alat dan Bahan Ujian

Komponen	Keterangan
Perangkat Lunak	Cisco Packet Tracer (versi terbaru), file topologi ujian (.pkt) yang dibagikan instruktur
Perangkat Presentasi	Aplikasi presentasi (PowerPoint/Google Slides), proyektor/layar presentasi
Dokumen Pendukung	Lembar Soal Ujian Praktik, Dokumentasi Teknis Proyek (revisi dari Modul 14–15), Rubrik Penilaian UAS

F. Gambaran Umum Skenario Ujian

Skenario ujian praktik individual bersifat komprehensif, mengintegrasikan topik Modul 9–13 dalam satu topologi enterprise. Parameter spesifik ditentukan instruktur dan dapat bervariasi antar-mahasiswa. Contoh cakupan skenario meliputi:

1. Konfigurasi HSRP/VRRP untuk redundansi gateway pada segmen yang ditentukan (Sub-CPMK-3.1).
2. Konfigurasi tunnel VPN IPSec site-to-site antar-lokasi (Sub-CPMK-3.2).
3. Penerapan ACL standar/extended sesuai kebijakan akses yang ditentukan (Sub-CPMK-4.1).
4. Konfigurasi firewall dan segmentasi zona keamanan (Sub-CPMK-4.2).
5. Konfigurasi monitoring (SNMP/syslog) serta troubleshooting skenario gangguan yang disisipkan (Sub-CPMK-4.3).

Untuk komponen proyek kelompok, setiap kelompok diminta memfinalisasi rancangan berdasarkan umpan balik Modul 14–15, kemudian mempresentasikan revisi akhir beserta pertanggungjawaban hasil kerja secara keseluruhan.

G. Prosedur Pelaksanaan Ujian

Tahap 1 — Ujian Praktik Konfigurasi Komprehensif (± 100 menit)

1. Instruktur membagikan lembar soal dan file topologi ujian kepada masing-masing mahasiswa.
2. Mahasiswa mengerjakan seluruh skenario ujian (redundansi, VPN, ACL, firewall, monitoring) secara mandiri.
3. Mahasiswa melakukan verifikasi dan troubleshooting mandiri atas seluruh hasil konfigurasi, serta memastikan kebijakan keamanan diterapkan konsisten.
4. Mahasiswa menyimpan file topologi akhir dan lembar jawaban (screenshot verifikasi) sesuai format yang ditentukan.

Tahap 2 — Finalisasi Proyek Kelompok (± 30 menit)

1. Setiap kelompok menyelesaikan revisi akhir dokumentasi dan/atau implementasi proyek berdasarkan umpan balik Modul 14–15.
2. Kelompok memastikan seluruh elemen proyek (topologi, dokumentasi, implementasi) telah konsisten dan siap dipresentasikan.

Tahap 3 — Presentasi dan Pertanggungjawaban Hasil (± 40 menit, menyesuaikan jumlah kelompok)

1. Setiap kelompok mempresentasikan revisi akhir proyek secara ringkas, menekankan penyempurnaan dari umpan balik sebelumnya.
2. Instruktur/audiens mengajukan pertanyaan terkait keseluruhan hasil kerja kelompok maupun kontribusi individual.
3. Mahasiswa/kelompok mempertanggungjawabkan hasil kerja secara jelas dan sesuai kaidah komunikasi teknis profesional.

H. Format Pengumpulan Hasil Ujian

Hasil UAS dikumpulkan dalam bentuk:

1. File topologi ujian praktik individual (.pkt) dengan nama file: NIM_NamaMahasiswa_UAS.pkt
2. Lembar Jawaban ujian praktik individual berisi tangkapan layar hasil verifikasi setiap bagian skenario.
3. Dokumentasi teknis final dan file topologi final proyek kelompok (revisi dari Modul 14–15) dengan nama file: Kelompok[X]_UAS_DokumentasiFinal dan Kelompok[X]_UAS_TopologiFinal.pkt
4. Bahan presentasi revisi akhir proyek kelompok.

I. Rubrik Penilaian UAS

Penilaian menggunakan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55). Deskriptor lengkap keempat kategori untuk setiap aspek tersedia pada Rubrik Penilaian Praktikum per Pertemuan (Lampiran 3).

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
Kelengkapan & Ketepatan Konfigurasi Komprehensif	30%	Seluruh elemen ujian (redundansi gateway, VPN, ACL, firewall, monitoring) dikonfigurasi lengkap	Sebagian besar elemen ujian tidak dikonfigurasi atau salah total.

Aspek Penilaian	Bobot	Kriteria Sangat Baik (85–100)	Kriteria Kurang (< 55)
		dan benar sesuai skenario komprehensif.	
Kualitas Revisi/Finalisasi Proyek Akhir	25%	Revisi akhir rancangan proyek menunjukkan penyempurnaan signifikan dari umpan balik pertemuan sebelumnya dan siap diimplementasikan.	Tidak dilakukan revisi/finalisasi terhadap proyek.
Verifikasi, Troubleshooting & Keamanan	25%	Mampu memverifikasi seluruh hasil konfigurasi, mengatasi gangguan yang muncul, dan memastikan kebijakan keamanan diterapkan konsisten.	Tidak mampu memverifikasi maupun mengatasi gangguan yang muncul.
Presentasi & Pertanggungjawaban Hasil	20%	Mampu mempresentasikan dan mempertanggungjawabkan seluruh hasil kerja (individual/kelompok) secara jelas, meyakinkan, dan sesuai kaidah komunikasi teknis profesional.	Tidak mampu mempresentasikan atau mempertanggungjawabkan hasil kerja.

Nilai UAS berkontribusi 30% terhadap nilai akhir mata kuliah dan menjadi dasar perhitungan Nilai CPMK-3, CPMK-4, dan CPMK-5 (bersama rerata Tugas Praktikum Modul 9–15 dengan proporsi 70% tugas : 30% UAS), yang selanjutnya berkontribusi pada perhitungan capaian seluruh CPL mata kuliah sesuai Rubrik Penilaian CPL. Modul ini menutup seluruh 16 modul praktikum Enterprise Networking.

DAFTAR PUSTAKA

Daftar pustaka berikut merangkum seluruh referensi yang digunakan dalam penyusunan Modul Praktikum Enterprise Networking, sesuai Daftar Referensi pada dokumen RPS mata kuliah ini.

Cisco Networking Academy. (2023). CCNA: Switching, Routing, and Wireless Essentials v7 Companion Guide. Cisco Press.

Cisco Networking Academy. (2023). CCNA: Enterprise Networking, Security, and Automation v7 Companion Guide. Cisco Press.

Empson, S. (2022). CCNA Routing and Switching Portable Command Guide (4th ed.). Cisco Press.

Lammle, T. (2023). CCNA Certification Study Guide: Exam 200-301 (2nd ed.). Sybex.

MikroTik Certified Training Partner. (2022). MTCNA Course Outline and Lab Guide. MikroTik Academy.

Odom, W. (2024). CCNA 200-301 Official Cert Guide, Volume 2 (2nd ed.). Cisco Press.

Sari, R. P., & Hidayat, T. (2023). Implementasi VLAN dan Routing OSPF Multi-Area pada Jaringan Kampus Berbasis Cisco Packet Tracer. Jurnal Teknik Informatika dan Sistem Informasi, 9(2), 145 –156.

GLOSARIUM

Glosarium berikut merangkum istilah teknis kunci yang digunakan sepanjang 16 modul praktikum, disusun berdasarkan urutan abjad.

Access Control List (ACL) — Kumpulan aturan berurutan pada router/switch untuk menyaring trafik berdasarkan kriteria tertentu (alamat, protokol, port).

Area Border Router (ABR) — Router OSPF yang memiliki interface pada lebih dari satu area, bertugas meneruskan informasi rute antar-area.

Backbone Area — Area pusat (Area 0) pada OSPF yang menghubungkan seluruh area lain dalam topologi multi-area.

Command Line Interface (CLI) — Antarmuka baris perintah untuk mengonfigurasi dan mengelola perangkat jaringan Cisco IOS.

Demilitarized Zone (DMZ) — Zona jaringan perantara yang menampung layanan/server yang perlu diakses dari luar, terisolasi dari zona internal.

EtherChannel — Teknologi yang menggabungkan beberapa tautan fisik antar-switch menjadi satu tautan logis untuk agregasi bandwidth dan redundansi.

Failover — Proses pengalihan otomatis fungsi/peran dari perangkat yang gagal ke perangkat cadangan.

Firewall — Perangkat/fungsi keamanan yang mengendalikan aliran trafik antar-jaringan berdasarkan kebijakan keamanan.

Hot Standby Router Protocol (HSRP) — Protokol milik Cisco yang menyediakan redundansi default gateway melalui virtual IP bersama pada dua router atau lebih.

Interesting Traffic — Trafik yang didefinisikan (melalui ACL) untuk dienkapsulasi dan dilindungi melalui tunnel VPN IPSec.

Internet Key Exchange (IKE)/ISAKMP — Protokol negosiasi yang digunakan untuk membentuk secure channel (Fase 1) dan IPSec SA (Fase 2) pada VPN IPSec.

Link Aggregation Control Protocol (LACP) — Protokol standar terbuka (IEEE 802.3ad) untuk negosiasi pembentukan EtherChannel.

Link State Advertisement (LSA) — Paket informasi topologi yang dipertukarkan antar-router OSPF untuk membangun link-state database.

Management Information Base (MIB) — Struktur data pada perangkat jaringan yang menyimpan informasi status yang dapat diakses melalui SNMP.

Open Shortest Path First (OSPF) — Protokol routing dinamis berbasis link-state yang menghitung jalur terpendek menggunakan algoritma Dijkstra.

Port Aggregation Protocol (PAgP) — Protokol milik Cisco (proprietary) untuk negosiasi pembentukan EtherChannel.

Preempt — Opsi pada HSRP/VRRP yang memungkinkan router prioritas lebih tinggi merebut kembali peran aktif setelah kembali online.

Priority — Nilai yang menentukan router mana yang menjadi Active/Master pada HSRP/VRRP; nilai tertinggi terpilih sebagai router aktif.

Router-on-a-Stick — Metode routing antar-VLAN menggunakan sub-interface logis pada satu interface fisik router yang terhubung ke trunk switch.

Security Zoning — Pengelompokan segmen jaringan ke dalam zona dengan tingkat kepercayaan berbeda (internal, DMZ, eksternal) untuk tujuan keamanan.

Simple Network Management Protocol (SNMP) — Protokol standar untuk memantau dan mengelola perangkat jaringan dari satu titik terpusat (NMS).

Switch Virtual Interface (SVI) — Interface virtual pada switch Layer-3 yang berfungsi sebagai gateway untuk VLAN tertentu.

Syslog — Standar protokol pencatatan log yang mengirimkan pesan log perangkat ke server terpusat.

Transform-Set — Kumpulan algoritma enkripsi dan hashing yang digunakan untuk melindungi trafik data pada Fase 2 IPSec.

Trunk Port — Jenis port switch yang membawa trafik dari beberapa VLAN sekaligus melalui satu tautan fisik menggunakan tagging 802.1Q.

Virtual LAN (VLAN) — Teknik segmentasi jaringan logis pada lapisan data link yang membagi satu switch fisik menjadi beberapa broadcast domain independen.

Virtual Router Redundancy Protocol (VRRP) — Protokol standar terbuka (RFC 5798) yang menyediakan redundansi default gateway, setara HSRP namun bukan proprietary Cisco.

VLAN Trunking Protocol (VTP) — Protokol Cisco yang memungkinkan propagasi otomatis informasi VLAN antar-switch dalam satu domain.

Wildcard Mask — Notasi yang digunakan ACL untuk menentukan rentang alamat IP yang dicocokkan, kebalikan logika dari subnet mask biasa.

LAMPIRAN 1 — TEMPLATE LAPORAN PRAKTIKUM

Template berikut digunakan sebagai acuan format laporan praktikum individual (Modul 1–13) sebagaimana dirujuk pada bagian G setiap modul.

Halaman Judul

- Judul Modul dan Nomor Pertemuan
- Nama dan NIM Mahasiswa
- Program Studi, Jurusan, dan Institusi
- Tanggal Pelaksanaan Praktikum

Isi Laporan

1. Tujuan Praktikum — disalin dari bagian B modul terkait.
2. Alat dan Bahan yang Digunakan.
3. Skema/Rancangan Terkait (topologi, skema IP/VLAN, atau kebijakan, sesuai modul).
4. Langkah Kerja beserta Bukti Pelaksanaan — setiap tahap disertai tangkapan layar (screenshot) konfigurasi dan hasil verifikasi CLI.
5. Hasil Pengujian/Verifikasi — merangkum hasil akhir pengujian sesuai tugas praktikum modul terkait.
6. Kendala dan Solusi — kendala teknis yang dihadapi selama praktikum beserta solusi yang diterapkan (jika ada).
7. Kesimpulan — rangkuman singkat capaian dan pembelajaran dari sesi praktikum.

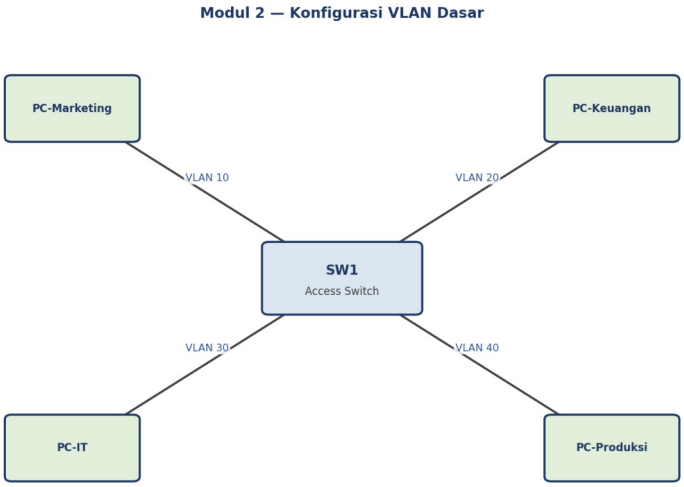
Ketentuan Format

- Nama file: NIM_NamaMahasiswa_ModulXX_Laporan (format PDF/DOCX).
- Font Calibri/Times New Roman 11–12pt, spasi 1,15.
- Setiap tangkapan layar diberi nomor dan keterangan (caption) yang jelas.

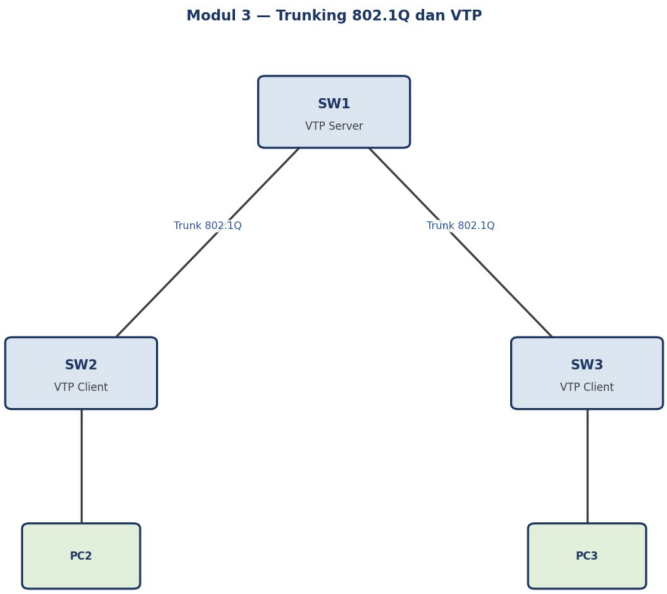
LAMPIRAN 2 — TOPOLOGI REFERENSI TIAP MODUL

Diagram berikut menggambarkan topologi referensi yang digunakan pada setiap modul praktikum (Modul 1–13; Modul 8 dan 16 bersifat evaluasi dengan skenario yang bervariasi sehingga tidak memiliki satu topologi tetap). Diagram bersifat ilustratif — parameter rinci (alamat IP, VLAN ID, dan sejenisnya) mengikuti ketentuan pada setiap modul atau instruksi instruktur. File topologi (.pkt) rinci disediakan secara terpisah oleh instruktur/pengelola laboratorium.

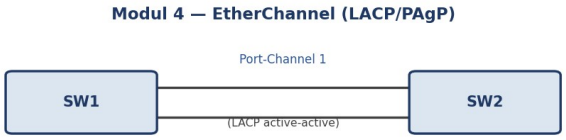
Gambar L2.1 — Modul 1: Orientasi Praktikum, K3, dan Dasar CLI



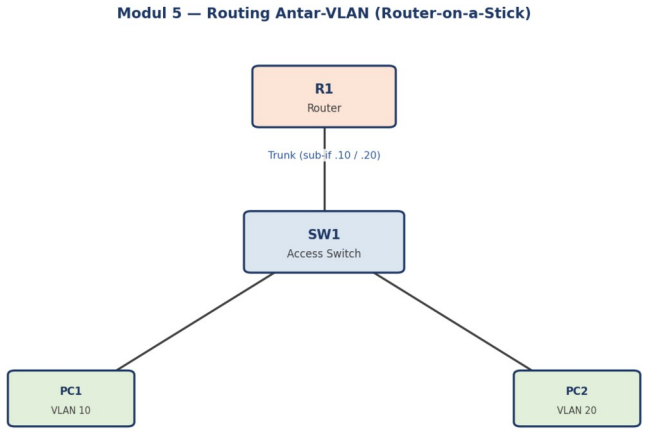
Gambar L2.2 — Modul 2: Konfigurasi VLAN Dasar



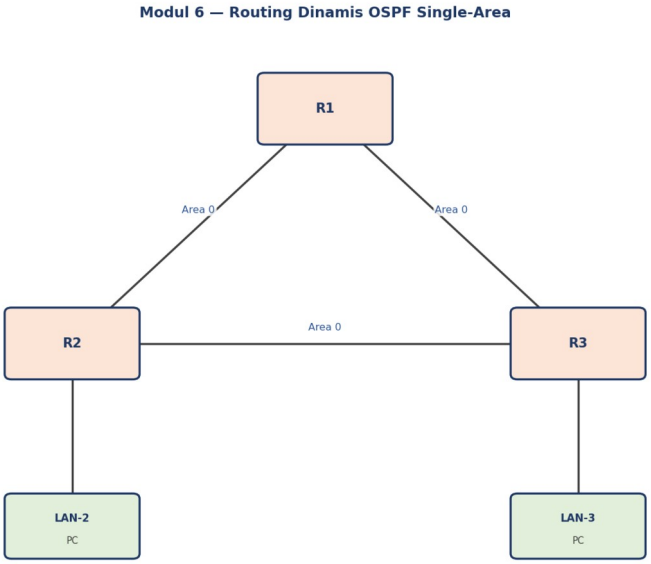
Gambar L2.3 — Modul 3: Trunking 802.1Q dan VTP



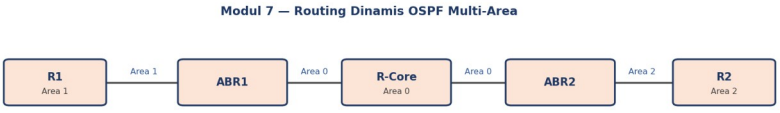
Gambar L2.4 — Modul 4: EtherChannel (LACP/PAgP)



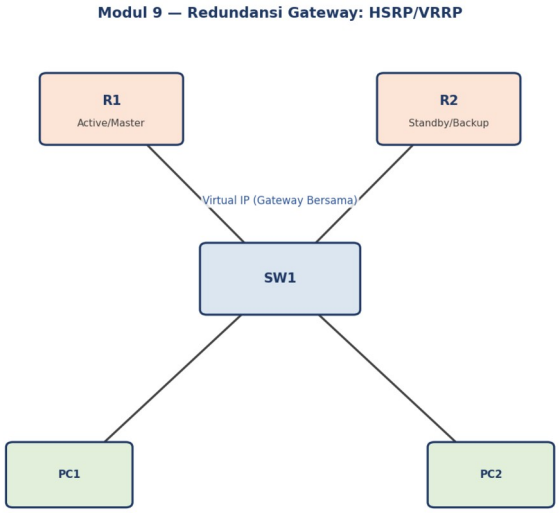
Gambar L2.5 — Modul 5: Routing Antar-VLAN (Router-on-a-Stick)



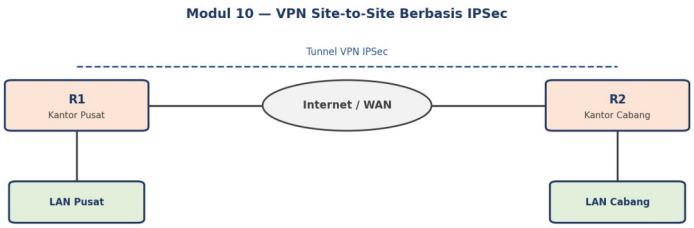
Gambar L2.6 — Modul 6: Routing Dinamis OSPF Single-Area



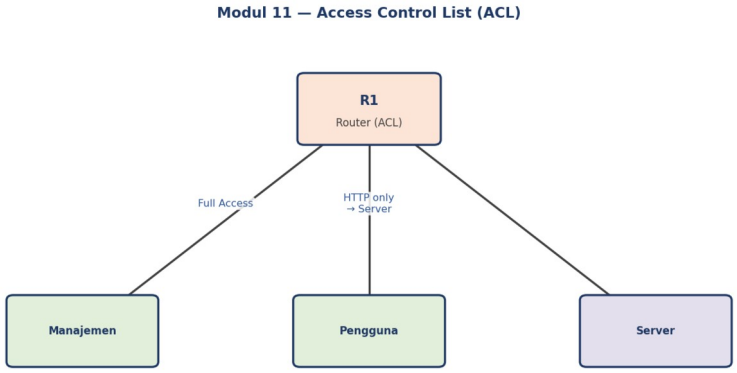
Gambar L2.7 — Modul 7: Routing Dinamis OSPF Multi-Area



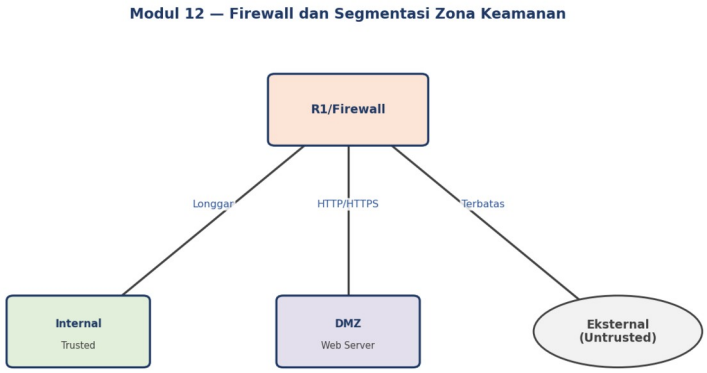
Gambar L2.8 — Modul 9: Redundansi Gateway (HSRP/VRRP)



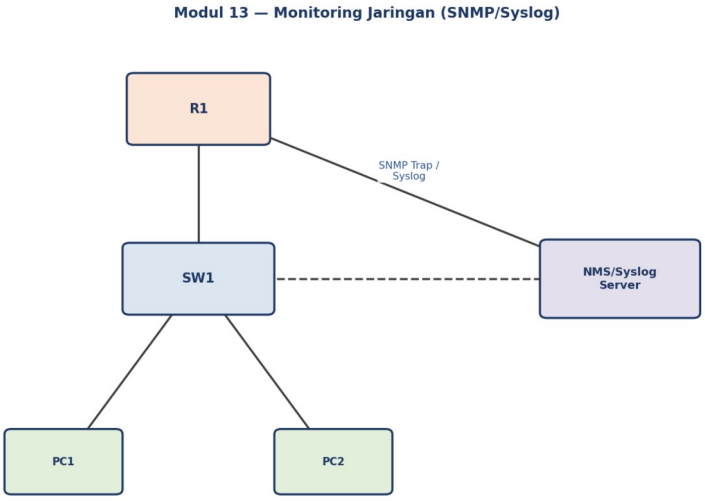
Gambar L2.9 — Modul 10: VPN Site-to-Site Berbasis IPSec



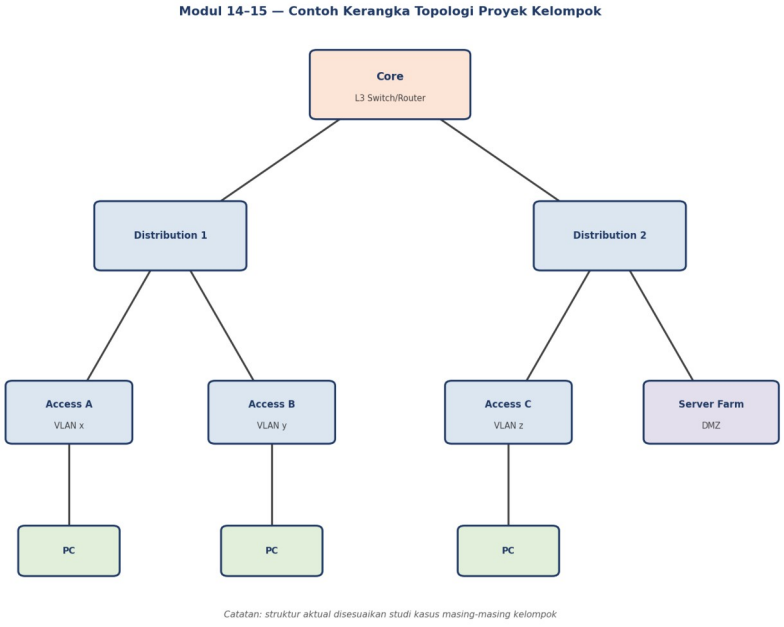
Gambar L2.10 — Modul 11: Access Control List (ACL)



Gambar L2.11 — Modul 12: Firewall dan Segmentasi Zona Keamanan



Gambar L2.12 — Modul 13: Monitoring Jaringan (SNMP/Syslog)



Gambar L2.13 — Modul 14–15: Contoh Kerangka Topologi Proyek Kelompok

LAMPIRAN 3 — LEMBAR PENILAIAN/REKAPITULASI PER PERTEMUAN

Lembar berikut digunakan instruktur sebagai rekapitulasi nilai mahasiswa per pertemuan sepanjang semester. Rubrik penilaian analitik (multi-aspek) lengkap untuk setiap modul mengikuti deskriptor pada dokumen Rubrik Penilaian Praktikum per Pertemuan (bagian H setiap modul), dengan empat kategori: Sangat Baik (85–100), Baik (70–84), Cukup (55–69), dan Kurang (< 55).

Nama Mahasiswa: _____ NIM: _____

Modul	Topik	Bobot	Nilai
1	Orientasi K3 & CLI	1%	
2	VLAN Dasar	2%	
3	Trunking & VTP	2%	
4	EtherChannel	2%	
5	Routing Antar-VLAN	2%	
6	OSPF Single-Area	2%	
7	OSPF Multi-Area	3%	
8	UTS	30%	
9	HSRP/VRRP	2%	
10	VPN IPSec	3%	
11	ACL	2%	
12	Firewall & Segmentasi	2%	
13	Monitoring & Troubleshooting	2%	
14	Proyek Kelompok (Bagian 1)	2%	
15	Proyek Kelompok (Bagian 2)	3%	
16	UAS	30%	

LAMPIRAN 4 — CHECKLIST K3 LABORATORIUM

Checklist berikut diisi oleh mahasiswa pada setiap awal sesi praktikum sebagai penerapan prosedur K3 sebagaimana diuraikan pada bagian Tata Tertib dan Prosedur K3 Laboratorium.

Modul: _____ Nama/NIM: _____ Tanggal: _____

Sebelum Praktikum

- ☐ Mengenakan pakaian praktik sesuai ketentuan program studi.
- ☐ Memeriksa kondisi kabel daya dan kabel jaringan sebelum digunakan.
- ☐ Memeriksa kondisi fisik perangkat (switch/router) sebelum digunakan.
- ☐ Menata area kerja dan kabel agar tidak mengganggu akses/keselamatan kerja.

Selama Praktikum

- ☐ Menghindari kontak langsung dengan konektor logam saat perangkat menyala.
- ☐ Menggunakan gelang antistatis saat menangani komponen internal (jika tersedia).
- ☐ Menggunakan perangkat laboratorium sesuai penugasan instruktur.
- ☐ Tidak membawa makanan/minuman ke area kerja perangkat aktif.

Setelah Praktikum

- ☐ Mematikan dan mencabut perangkat sesuai prosedur (bukan langsung mencabut kabel daya).
- ☐ Mengembalikan kabel dan perangkat pada kondisi rapi.
- ☐ Melaporkan kerusakan/insiden (jika ada) kepada instruktur.

Paraf Mahasiswa: _____ Paraf Instruktur: _____

LAMPIRAN 5 — PANDUAN INSTALASI DAN PENGGUNAAN SIMULATOR

A. Instalasi Cisco Packet Tracer

8. Membuat akun pada Cisco Networking Academy (NetAcad) melalui laman resmi Cisco.
9. Mendaftar pada kursus 'Getting Started with Cisco Packet Tracer' (gratis) untuk memperoleh akses unduhan resmi.
10. Mengunduh installer Cisco Packet Tracer sesuai sistem operasi (Windows/Linux/macOS).
11. Menjalankan installer dan mengikuti petunjuk instalasi hingga selesai.
12. Masuk (login) menggunakan akun NetAcad saat pertama kali membuka aplikasi.

B. Pengenalan Antarmuka Dasar

- Panel perangkat (device panel) — memilih jenis perangkat (switch, router, PC, kabel) untuk diletakkan pada area kerja.
- Area kerja (workspace) — kanvas utama untuk menyusun topologi jaringan.
- Mode CLI/Config/Physical pada setiap perangkat — mengakses command line, konfigurasi GUI, atau tampilan fisik perangkat.
- Mode simulasi (Simulation Mode) — memvisualisasikan pergerakan paket data pada topologi secara langkah-demi-langkah.

C. Praktik Terbaik Penggunaan Simulator

13. Menyimpan file topologi secara berkala selama sesi praktikum berlangsung.
14. Menggunakan penamaan perangkat (hostname) yang deskriptif agar topologi mudah dibaca.
15. Memanfaatkan mode simulasi untuk memverifikasi pergerakan paket saat troubleshooting.
16. Melakukan pencadangan (backup) file topologi pada folder kerja terstruktur sesuai konvensi penamaan (Bagian Awal modul, subbab Panduan Perangkat dan Simulator).

D. Sumber Daya Tambahan

Dokumentasi resmi, tutorial, dan forum diskusi Cisco Packet Tracer tersedia melalui platform Cisco Networking Academy (NetAcad) bagi mahasiswa yang memerlukan referensi tambahan di luar sesi praktikum terjadwal.

INDEKS

Indeks berikut memuat istilah kunci beserta rentang halaman kemunculannya pada dokumen modul lengkap. Rentang halaman mengacu pada penomoran final setelah seluruh bagian modul disusun menjadi satu dokumen utuh.