BUKU BAHAN AJAR GURU

PERENCANAAN DAN PENGALAMATAN JARINGAN

Kelas XI — Program Keahlian TJKT

Disusun berdasarkan Naskah Soal LKS SMK Tingkat Kabupaten Tasikmalaya Tahun 2026
(Bidang IT Network System Administration — Modul A: Linux Environment & Modul B: Cisco Packet Tracer)
Mengacu pada dokumen Target Pembelajaran Kelas XI (Porsi 80%)

Fokus: Perencanaan berbasis praktik dengan Cisco Packet Tracer

Kata Pengantar

Buku ini disusun sebagai bahan ajar bagi guru mata pelajaran Perencanaan dan Pengalamatan Jaringan pada Program Keahlian Teknik Jaringan Komputer dan Telekomunikasi (TJKT) Kelas XI Sekolah Menengah Kejuruan. Materi disusun berdasarkan dokumen "Target Pembelajaran Kelas XI" yang memuat 20 target kompetensi (80% dari keseluruhan target) tersebar pada 7 elemen: analisis kebutuhan jaringan, perencanaan pengalamatan IP, perencanaan VLAN, perencanaan routing, perencanaan redundansi, perencanaan layanan pendukung, serta dokumentasi dan visualisasi desain jaringan.

Lima target lanjutan yang bersifat lebih spesifik — pengalamatan IPv6 dual-stack, pengalamatan VPN, distribusi VLAN melalui VTP, redundansi Virtual IP berbasis Keepalived, dan integrasi DNS forward/reverse zone — sengaja tidak dibahas mendalam pada buku ini karena telah dipetakan sebagai materi pendalaman Kelas XII. Dengan demikian, buku ini murni berfokus pada penguatan fondasi perencanaan jaringan yang tuntas dan matang di Kelas XI, sebelum siswa melanjutkan ke materi yang lebih kompleks.

Seluruh materi disusun dengan filosofi belajar melalui praktik langsung (practice-based learning). Setiap konsep perencanaan selalu diikuti contoh perhitungan atau skema nyata, kemudian dipraktikkan langsung menggunakan Cisco Packet Tracer — alat yang menjadi acuan Modul B pada naskah soal LKS. Studi kasus utama yang dipakai secara konsisten dari awal hingga akhir buku adalah perusahaan multi-cabang ITNSA.ID Corp, sehingga siswa mengalami sendiri bagaimana sebuah rancangan jaringan tumbuh secara bertahap dari analisis kebutuhan hingga dokumentasi akhir.

Setiap bab disusun dengan struktur konsisten: tujuan pembelajaran, uraian materi dengan contoh, praktik/aktivitas di Packet Tracer, rangkuman, dan soal latihan/refleksi — memudahkan guru mengelola alokasi waktu dan asesmen di kelas. Semoga buku ini bermanfaat sebagai pegangan guru dalam menyampaikan materi Perencanaan dan Pengalamatan Jaringan secara sistematis, aplikatif, dan membangun fondasi kuat bagi siswa TJKT.

Penyusun

Daftar Isi

Peta Kompetensi Buku

Tabel berikut memetakan setiap elemen pada dokumen Target Pembelajaran Kelas XI ke bab pembahasan dalam buku ini, sekaligus jumlah target kompetensi dan alat praktik utama yang digunakan.

Bab	Elemen Target	Jumlah Target	Alat Praktik Utama
Bab 2	Analisis Kebutuhan Jaringan	3	Diagram / Packet Tracer (Logical Workspace)
Bab 3	Perencanaan Skema Pengalamatan IP	3	Kalkulasi VLSM + Packet Tracer
Bab 4	Perencanaan VLAN dan Segmentasi Layer 2	2	Packet Tracer (Switch IOS)
Bab 5	Perencanaan Routing	4	Packet Tracer (Router IOS)
Bab 6	Perencanaan Redundansi dan High Availability	2	Packet Tracer (EtherChannel & HSRP)
Bab 7	Perencanaan Layanan Pendukung Jaringan	3	Packet Tracer (DHCP, NAT, NTP)
Bab 8	Dokumentasi dan Visualisasi Desain Jaringan	3	Packet Tracer (Physical Workspace) + dokumen
Bab 9	Proyek Akhir Terintegrasi	(gabungan 20 target)	Packet Tracer — Studi Kasus ITNSA.ID Corp

BAB 1 — Pendahuluan

1.1 Kedudukan Mata Pelajaran

Perencanaan dan Pengalamatan Jaringan adalah mata pelajaran kejuruan pada Program Keahlian TJKT Kelas XI yang menjembatani pengetahuan dasar jaringan komputer (yang telah dipelajari di Kelas X) dengan kemampuan konfigurasi teknis lanjutan (yang akan dipelajari di mapel Administrasi Infrastruktur Jaringan dan Teknologi Jaringan Berbasis Luas). Posisinya bersifat khas: siswa dilatih untuk berpikir dan merancang terlebih dahulu — menentukan skema IP, VLAN, jalur routing, dan redundansi di atas kertas/dokumen — sebelum menyentuh konfigurasi perangkat secara mendalam.

1.2 Dasar Penyusunan Materi

Materi buku ini disusun berdasarkan dokumen "Target Pembelajaran Kelas XI (Porsi 80%)", yang merupakan hasil pemecahan target kompetensi perencanaan jaringan menjadi dua tingkat: 80% target inti untuk Kelas XI dan 20% target pendalaman untuk Kelas XII. Dasar penyusunan target itu sendiri mengacu pada studi kasus nyata Lomba Kompetensi Siswa (LKS) SMK Bidang IT Network System Administration, khususnya topologi perusahaan multi-cabang (ITNSA.ID Corp) dan jaringan internal-DMZ.

Karena target IPv6 dual-stack, VPN, VTP, Keepalived, dan integrasi DNS zone dipindahkan ke Kelas XII, seluruh materi dan praktik dalam buku ini dapat dituntaskan menggunakan satu alat saja: Cisco Packet Tracer. Hal ini sengaja dipilih agar guru dan siswa dapat fokus membangun kebiasaan kerja yang rapi dan konsisten pada satu tools sebelum diperkenalkan pada tools yang lebih kompleks (GNS3) di Kelas XII.

1.3 Capaian Pembelajaran Umum

Setelah menyelesaikan seluruh materi pada buku ini, siswa diharapkan mampu:

- Menganalisis kebutuhan jaringan dari sebuah skenario bisnis dan menuliskannya sebagai dokumen requirement yang jelas.
- Merancang skema pengalamatan IPv4 (VLSM) untuk jaringan skala menengah, termasuk segmen LAN dan WAN point-to-point antar cabang.
- Merancang struktur VLAN serta jalur trunk/native VLAN sesuai kebutuhan organisasi.
- Merencanakan dan menerapkan protokol routing statis maupun dinamis (EIGRP/OSPF) beserta parameter pendukungnya.
- Merancang redundansi jaringan menggunakan EtherChannel dan HSRP.
- Merencanakan layanan pendukung jaringan: DHCP, NAT/PAT, dan sinkronisasi waktu (NTP).
- Mendokumentasikan dan mempresentasikan hasil rancangan jaringan secara logis maupun fisik.

1.4 Struktur Buku

Buku ini terdiri atas 10 bab. Bab 1 berisi pendahuluan dan petunjuk penggunaan. Bab 2 hingga Bab 8 membahas satu elemen target per bab, mengikuti urutan logis proses perencanaan jaringan: mulai dari analisis kebutuhan, pengalamatan IP, VLAN, routing, redundansi, layanan pendukung, hingga dokumentasi. Bab 9 merupakan proyek akhir terintegrasi yang menggabungkan seluruh elemen dalam satu studi kasus besar. Bab 10 berisi penutup dan kaitan dengan Kelas XII.

Setiap bab (2-8) memiliki struktur yang konsisten:

- Tujuan Pembelajaran — target kompetensi dan indikator capaian yang dirujuk dari dokumen target.
- Uraian Materi — konsep, rumus, dan contoh perhitungan/skema yang dijelaskan langkah demi langkah.
- Praktik/Aktivitas Pembelajaran — instruksi hands-on di Cisco Packet Tracer beserta contoh perintah CLI.
- Rangkuman — poin-poin kunci yang wajib dikuasai siswa.
- Soal Latihan/Refleksi — pertanyaan pemantik diskusi dan latihan mandiri.

1.5 Petunjuk Penggunaan bagi Guru

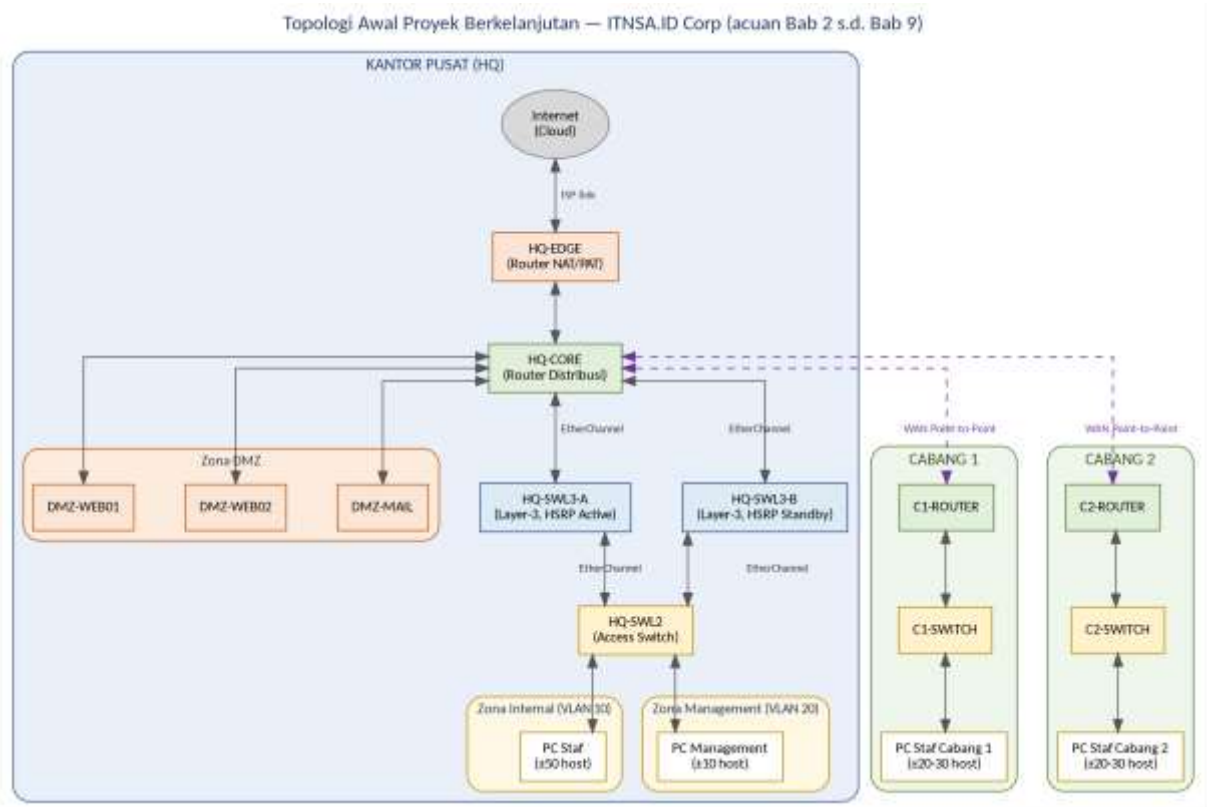
- Gunakan studi kasus ITNSA.ID Corp secara konsisten di setiap bab agar siswa merasakan kesinambungan rancangan, bukan latihan-latihan terpisah.
- Alokasikan waktu lebih banyak pada Bab 3 (Pengalamatan IP) dan Bab 5 (Routing) karena keduanya menjadi fondasi bab-bab berikutnya.
- Selalu minta siswa menuliskan hasil rancangan di atas kertas/dokumen (tabel IP, tabel VLAN) sebelum membuka Packet Tracer — sesuai filosofi "rencanakan dulu, baru implementasikan".
- Gunakan file proyek Packet Tracer (.pkt) yang sama dari Bab 2 hingga Bab 9 sebagai satu proyek berkelanjutan (living project), bukan file terpisah per bab.
- Penilaian sebaiknya menimbang dokumen perencanaan (tabel IP, diagram, justifikasi desain) setara atau lebih besar bobotnya dibanding hasil akhir konfigurasi.

1.6 Kaitan dengan Kelas XII dan Kompetisi Keahlian

Dua puluh target pada buku ini adalah fondasi yang wajib tuntas sebelum siswa mempelajari lima target pendalaman di Kelas XII (IPv6 dual-stack, VPN, VTP, Keepalived, dan DNS zone) yang dibahas pada buku "Target Perencanaan dan Pengalamatan Jaringan Kelas XII". Penguasaan materi buku ini secara langsung juga mempersiapkan siswa menghadapi Modul B (Cisco Packet Tracer) pada Lomba Kompetensi Siswa Bidang IT Network System Administration.

1.7 Topologi Awal Proyek Berkelanjutan (Gambaran Umum)

Sebelum siswa membuka Packet Tracer di Bab 2, guru disarankan menunjukkan lebih dahulu gambaran topologi akhir yang akan dituju sepanjang buku ini. Tujuannya bukan agar siswa langsung meniru topologi ini, melainkan agar mereka memahami arah dan skala proyek yang sedang dibangun secara bertahap — sehingga setiap keputusan kecil di tiap bab (penempatan perangkat, pengalamatan, VLAN, routing, dst.) terasa punya tujuan yang jelas, bukan latihan yang berdiri sendiri.



Gambar 1.1 — Topologi akhir proyek berkelanjutan ITNSA.ID Corp yang menjadi acuan dari Bab 2 hingga Bab 9. Pada Bab 2, siswa baru menempatkan kerangka perangkat per zona (INT, DMZ, Management, WAN) tanpa kabel dan tanpa IP; seluruh elemen lain pada gambar ini (pengalamatan, EtherChannel, HSRP, dan seterusnya) ditambahkan bertahap pada bab-bab berikutnya.

Tabel berikut merangkum bagaimana satu file proyek Packet Tracer (.pkt) yang sama ini berkembang dari bab ke bab — gunakan tabel ini sebagai peta alur pembelajaran sebelum memulai Bab 2:

Bab	Yang Ditambahkan ke File .pkt yang Sama
Bab 2	Kerangka topologi awal — perangkat ditempatkan per zona (INT/DMZ/WAN), belum dikabel, belum ada IP.
Bab 3	Kabel dipasang, IP address diisi sesuai hasil perhitungan VLSM.
Bab 4	VLAN, trunk, dan native VLAN dikonfigurasi di switch.
Bab 5	Routing OSPF dikonfigurasi — titik pertama koneksi antar-subnet mulai berhasil.
Bab 6	EtherChannel dan HSRP ditambahkan di atas topologi yang sudah berjalan.
Bab 7	DHCP, NAT, dan NTP dikonfigurasi.
Bab 8	Physical Workspace ditata dan screenshot diambil untuk dokumentasi.
Bab 9	Proyek akhir — penyempurnaan file yang sama, dinilai sebagai satu kesatuan.

Mengapa Satu File Proyek yang Sama?

Siswa merasakan bagaimana sebuah rancangan jaringan tumbuh bertahap — persis seperti proyek nyata — bukan mengerjakan latihan-latihan terputus yang tidak saling berhubungan. Pola ini juga meniru format soal LKS Modul B, yang biasanya berupa satu topologi besar dikerjakan bertahap sesuai instruksi soal.

Siswa/kelompok perlu menyimpan file .pkt mereka sendiri dan membawanya (atau menyimpannya di folder kerja bersama) dari pertemuan ke pertemuan.

Jika ada kesalahan konfigurasi di bab awal, kesalahan itu akan terbawa ke bab berikutnya — sehingga proyek ini sekaligus melatih kebiasaan verifikasi tiap tahap sebelum lanjut. Gunakan Lembar Checkpoint yang tersedia di akhir setiap bab (Bab 2–9) sebagai alat bantu verifikasi tersebut.

Untuk penilaian portofolio, guru dapat meminta siswa submit file .pkt di akhir tiap bab sebagai checkpoint, atau cukup di akhir Bab 9 sebagai proyek akhir.

Cara Menggunakan Checklist Verifikasi per Bab

Checklist berikut muncul di akhir setiap bab (Bab 2–9) sebagai alat kontrol progres bagi guru, untuk memastikan file proyek Packet Tracer (.pkt) setiap kelompok benar-benar layak dilanjutkan ke bab berikutnya. Karena proyek ini bersifat berkelanjutan (living project) dari Bab 2 hingga Bab 9, kesalahan yang tidak terdeteksi di satu bab akan terbawa dan menyulitkan bab-bab selanjutnya. Gunakan satu lembar per kelompok per bab; guru cukup membubuhkan tanda centang dan paraf setelah memverifikasi hasil kerja kelompok secara langsung di Packet Tracer.

Cara Pakai Lembar Ini

Fotokopi/cetak (atau salin ke lembar terpisah) satu set lembar checkpoint per kelompok, atau isi secara digital.

Isi kolom ‘Status’ setelah guru mengecek langsung file .pkt kelompok — bukan hanya berdasarkan pengakuan siswa.

Kelompok yang belum mencentang seluruh item pada satu bab sebaiknya menuntaskannya terlebih dahulu sebelum melanjutkan konfigurasi di bab berikutnya, agar kesalahan tidak menumpuk.

BAB 2 — Analisis Kebutuhan Jaringan

Tujuan Pembelajaran

Bab ini merujuk pada Elemen 1 dokumen target, dengan tiga target kompetensi: menganalisis kebutuhan jaringan dari skenario bisnis, menentukan segmentasi jaringan berdasarkan fungsi dan keamanan, serta menyusun dokumen kebutuhan jaringan. Setelah mempelajari bab ini, siswa mampu membaca sebuah skenario bisnis dan menerjemahkannya menjadi kerangka kebutuhan jaringan yang terstruktur.

2.1 Studi Kasus Utama: ITNSA.ID Corp

Sepanjang buku ini, seluruh latihan menggunakan satu studi kasus besar yang berkembang bertahap: ITNSA.ID Corp, sebuah perusahaan dengan kantor pusat dan beberapa cabang, memiliki kebutuhan konektivitas antar cabang (WAN), zona internal (INT) untuk karyawan, serta zona publik/DMZ untuk server yang diakses dari luar (web, mail). Topologi inti kantor pusat menggunakan pola CORE-DIST-ACCESS (perangkat CORE, switch layer-3/SWL3, dan switch layer-2/SWL2).

Skenario Bisnis (Ringkas)

ITNSA.ID Corp memiliki 1 kantor pusat (HQ) dan 2 kantor cabang.

Setiap cabang memiliki jaringan LAN untuk staf (VLAN Internal) dan perangkat manajemen (VLAN Management).

Kantor pusat memiliki zona DMZ berisi web server dan mail server yang dapat diakses dari internet.

Seluruh kantor terhubung melalui WAN link point-to-point ke kantor pusat.

Langkah pertama analisis kebutuhan adalah mengidentifikasi entitas: siapa saja pengguna jaringan (staf, tamu, admin), perangkat apa yang perlu terhubung (PC, printer, server, access point), dan layanan apa yang harus tersedia (akses internet, akses file server, akses web/mail dari luar).

2.2 Segmentasi Jaringan: INT, DMZ, dan WAN

Segmentasi adalah pembagian jaringan menjadi zona-zona berdasarkan fungsi dan tingkat kepercayaan (trust level). Tiga zona yang wajib dipahami siswa pada tahap ini:

Zona	Fungsi	Tingkat Keamanan
INT (Internal)	Jaringan staf/karyawan, perangkat kerja sehari-hari	Tinggi — hanya dapat diakses dari dalam, dibatasi firewall ke luar
DMZ (Demilitarized Zone)	Menempatkan server publik (web, mail) yang perlu diakses dari internet	Menengah — dapat diakses terbatas dari luar, tetap dipisah dari INT
WAN	Jalur penghubung antar kantor/cabang dan ke internet	Bergantung pada jalur; titik masuk utama yang harus dijaga oleh firewall/edge router

Prinsip dasar yang perlu ditanamkan ke siswa: server yang diakses publik TIDAK BOLEH diletakkan di zona INT, karena jika server tersebut disusupi maka penyerang akan mendapat pijakan langsung ke jaringan internal. DMZ berfungsi sebagai zona penyangga sehingga trafik dari internet ke server publik tidak pernah menyentuh segmen INT secara langsung.

2.3 Menyusun Dokumen Kebutuhan Jaringan (Requirement)

Dokumen kebutuhan jaringan adalah keluaran (output) dari elemen ini. Dokumen tersebut minimal memuat: daftar lokasi/cabang, jumlah perkiraan pengguna dan perangkat per lokasi, daftar layanan yang dibutuhkan, dan zona keamanan yang diperlukan. Contoh format sederhana:

Lokasi	Perkiraan Host	Zona	Layanan Dibutuhkan
HQ - Internal	50 host	INT	Akses internet, file sharing, akses ke DMZ terbatas
HQ - DMZ	4 server	DMZ	Web (HTTP/HTTPS), Mail (SMTP), diakses dari internet
HQ - Management	10 host	INT (Management VLAN)	Akses konfigurasi perangkat jaringan
Cabang 1	20 host	INT (remote)	Akses ke HQ via WAN, akses internet
Cabang 2	20 host	INT (remote)	Akses ke HQ via WAN, akses internet

Praktik/Aktivitas Pembelajaran

Aktivitas 2.1 — Membaca Skenario dan Menyusun Requirement (individu/kelompok, 30 menit): Berikan siswa satu paragraf skenario bisnis (boleh memodifikasi ITNSA.ID Corp), lalu minta mereka mengisi tabel requirement seperti contoh di atas.

Aktivitas 2.2 — Kerangka Awal di Packet Tracer (30 menit): Buka Packet Tracer, buat file proyek baru (ini akan menjadi file proyek berkelanjutan hingga Bab 9). Tempatkan perangkat sesuai hasil analisis: router (1 per lokasi), switch, PC/laptop, dan server, dikelompokkan visual per zona (INT, DMZ) menggunakan kotak teks/anotasi pada Logical Workspace. Jangan sambungkan kabel dan jangan isi IP terlebih dahulu — fokus tahap ini hanya kerangka dan penempatan perangkat.

> **Tips Guru**
>
> Gunakan fitur 'Add Simple PDU' hanya di bab-bab berikutnya; pada bab ini siswa cukup menata perangkat.
>
> Dorong siswa memberi nama perangkat yang deskriptif (mis. HQ-CORE, DMZ-WEB01) — kebiasaan ini akan sangat membantu di bab dokumentasi.

Rangkuman

- Analisis kebutuhan jaringan dimulai dari memahami skenario bisnis: siapa penggunanya, perangkat apa saja, dan layanan apa yang dibutuhkan.
- Segmentasi jaringan membagi jaringan menjadi zona INT, DMZ, dan WAN berdasarkan fungsi dan tingkat keamanan.
- Server publik selalu ditempatkan di DMZ, terpisah dari zona INT, untuk mencegah eksposur langsung ke jaringan internal.
- Dokumen kebutuhan jaringan menjadi acuan dasar bagi seluruh tahap perencanaan berikutnya (pengalamatan, VLAN, routing, dst.).

Soal Latihan/Refleksi

- 1. Mengapa server web dan mail sebaiknya tidak diletakkan pada zona internal (INT)? Jelaskan risikonya.

- 2. Sebutkan tiga contoh layanan yang menurutmu wajib ada pada zona INT sebuah kantor kecil, dan tiga layanan yang wajib ada di DMZ.
- 3. Sebuah sekolah memiliki lab komputer, ruang guru, dan server nilai online yang diakses siswa dari rumah. Susunlah tabel requirement seperti contoh pada bab ini untuk skenario tersebut.
- 4. Apa perbedaan mendasar antara zona DMZ dan zona WAN dari sisi fungsi dan tingkat keamanannya?

Checkpoint Bab 2 — Analisis Kebutuhan Jaringan

Sebelum kelompok melanjutkan ke bab berikutnya, pastikan seluruh item di bawah ini sudah terverifikasi langsung oleh guru pada file proyek .pkt kelompok tersebut:

No	Item Verifikasi	Status
1	Dokumen requirement (lokasi, perkiraan host, zona, layanan) sudah diisi lengkap sesuai skenario.	☐ Sudah ☐ Belum
2	Seluruh perangkat (router, switch, PC/laptop, server) sudah ditempatkan di Logical Workspace, satu per lokasi/fungsi sesuai hasil analisis.	☐ Sudah ☐ Belum
3	Perangkat dikelompokkan secara visual per zona (INT, DMZ, Management) menggunakan kotak teks/anotasi.	☐ Sudah ☐ Belum
4	Setiap perangkat sudah diberi nama deskriptif (mis. HQ-CORE, DMZ-WEB01), bukan nama bawaan (Router0, Switch0).	☐ Sudah ☐ Belum
5	Belum ada kabel yang dipasang dan belum ada IP address yang diisi (sesuai batasan tahap ini).	☐ Sudah ☐ Belum

Nama Kelompok: _____ Tanggal Verifikasi: _____
Catatan Guru: _____
Paraf Guru: _____

BAB 3 — Perencanaan Skema Pengalamatan IP (IP Addressing Plan)

Tujuan Pembelajaran

Bab ini merujuk pada Elemen 2 dokumen target dengan tiga target kompetensi: merancang skema subnetting/VLSM sesuai kebutuhan host, menyusun tabel pengalamatan IPv4 untuk jaringan skala menengah, dan merencanakan pengalamatan untuk jaringan multi-cabang/WAN. Bab ini adalah fondasi teknis terpenting sebelum siswa masuk ke VLAN dan routing.

3.1 Konsep Subnetting dan VLSM

VLSM (Variable Length Subnet Mask) memungkinkan satu blok alamat IP dipecah menjadi beberapa subnet dengan ukuran berbeda-beda, disesuaikan dengan jumlah host yang dibutuhkan tiap segmen — berbeda dengan subnetting biasa yang membagi rata. Prinsip VLSM: alokasikan subnet terbesar (kebutuhan host terbanyak) terlebih dahulu, baru subnet yang lebih kecil.

Rumus dasar yang wajib dikuasai siswa: jumlah host yang dapat digunakan dalam sebuah subnet dihitung dengan 2 pangkat n dikurangi 2, di mana n adalah jumlah bit host yang tersisa (dikurangi 2 karena network address dan broadcast address tidak dapat dipakai host).

Prefix (CIDR)	Subnet Mask	Jumlah Host Usable	Contoh Penggunaan
/24	255.255.255.0	254	LAN kantor/cabang berukuran sedang (puluhan host)
/27	255.255.255.224	30	LAN departemen kecil / VLAN Management
/29	255.255.255.248	6	Segmen server DMZ berisi beberapa server
/30	255.255.255.252	2	Link point-to-point antar router (WAN)

Contoh Perhitungan VLSM

Misalkan ITNSA.ID Corp mendapat alokasi blok 192.168.10.0/24 untuk kantor pusat, dengan kebutuhan: LAN Internal 50 host, DMZ 4 host, LAN Management 10 host, dan 1 link WAN ke Cabang 1. Langkah pengerjaan VLSM:

- 1. Urutkan kebutuhan dari terbesar ke terkecil: Internal (50) → Management (10) → DMZ (4) → WAN (2).
- 2. Internal butuh 50 host → subnet terkecil yang muat adalah /26 (62 host usable). Alokasikan 192.168.10.0/26 (range .1-.62).
- 3. Management butuh 10 host → /28 (14 host usable). Alokasikan subnet berikutnya: 192.168.10.64/28 (range .65-.78).
- 4. DMZ butuh 4 host → /29 (6 host usable). Alokasikan 192.168.10.80/29 (range .81-.86).
- 5. WAN link butuh 2 host → /30 (2 host usable). Alokasikan 192.168.10.88/30 (range .89-.90).

Kesalahan Umum Siswa

Lupa mengurutkan dari kebutuhan terbesar ke terkecil — menyebabkan subnet besar tidak muat di sisa blok. Menghitung host usable tanpa mengurangi 2 (network & broadcast address).

Menempatkan alamat network/broadcast sebagai alamat host pada perangkat.

3.2 Menyusun Tabel Pengalamatan (Addressing Table)

Tabel pengalamatan adalah dokumen wajib yang memetakan setiap interface perangkat ke alamat IP, subnet mask, dan gateway-nya. Tabel ini menjadi rujukan tunggal (single source of truth) sebelum konfigurasi dilakukan di Packet Tracer. Contoh tabel pengalamatan untuk hasil VLSM di atas:

Perangkat	Interface	Alamat IP	Subnet Mask	Keterangan
HQ-CORE	G0/0 (Internal)	192.168.10.1	255.255.255.192	Gateway VLAN Internal
HQ-CORE	G0/1 (Management)	192.168.10.65	255.255.255.240	Gateway VLAN Management
HQ-CORE	G0/2 (DMZ)	192.168.10.81	255.255.255.248	Gateway segmen DMZ
HQ-CORE	S0/0/0 (WAN ke Cabang 1)	192.168.10.89	255.255.255.252	Link point-to-point
CBG1-RTR	S0/0/0 (WAN ke HQ)	192.168.10.90	255.255.255.252	Link point-to-point

Ajarkan siswa membuat tabel ini dalam bentuk spreadsheet/tabel dokumen sebelum menyentuh Packet Tracer, sehingga proses input IP di simulator tinggal 'menyalin' dari dokumen yang sudah matang.

3.3 Pengalamatan Multi-Cabang/WAN

Untuk jaringan multi-cabang, setiap link WAN point-to-point antar router idealnya menggunakan subnet /30 tersendiri (hanya butuh 2 alamat host). Susun blok alamat WAN secara terpisah dari blok LAN agar mudah didokumentasikan dan diperluas. Contoh alokasi untuk ITNSA.ID Corp dengan 2 cabang:

Link WAN	Subnet	IP Ujung HQ	IP Ujung Cabang
HQ – Cabang 1	192.168.10.88/30	192.168.10.89	192.168.10.90
HQ – Cabang 2	192.168.10.92/30	192.168.10.93	192.168.10.94

Setiap cabang kemudian memiliki blok LAN tersendiri, misalnya Cabang 1 mendapat 192.168.11.0/24 dan Cabang 2 mendapat 192.168.12.0/24, sehingga penomoran antar lokasi tidak tumpang tindih dan mudah diringkas (summarized) saat routing nanti.

Praktik/Aktivitas Pembelajaran

Aktivitas 3.1 — Latihan VLSM Berbasis Kasus (individu, 40 menit): Berikan siswa kebutuhan host berbeda dari contoh (mis. blok 172.16.0.0/23 dengan 4 segmen kebutuhan berbeda), minta mereka melakukan VLSM dan menyusun tabel pengalamatan lengkap.

Aktivitas 3.2 — Implementasi di Packet Tracer (60 menit): Lanjutkan file proyek dari Bab 2. Hubungkan seluruh perangkat dengan kabel yang sesuai (copper straight-through untuk PC-switch, copper cross-over/otomatis untuk switch-router, serial DCE/DTE untuk link WAN antar router). Isi IP address pada

setiap interface PC dan router melalui tab Desktop > IP Configuration (PC) atau CLI (router), sesuai tabel pengalamatan yang telah disusun. Verifikasi dengan perintah berikut pada router:

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip address 192.168.10.1 255.255.255.192
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface Serial0/0/0
Router(config-if)# ip address 192.168.10.89 255.255.255.252
Router(config-if)# clock rate 64000
Router(config-if)# no shutdown
```

Setelah seluruh interface terisi, uji konektivitas antar perangkat yang berada pada subnet yang sama menggunakan PDU Simple (klik ikon amplop lalu klik dua perangkat) atau perintah ping dari Command Prompt PC/router. Catatan: konektivitas ANTAR subnet berbeda baru akan berhasil setelah routing dikonfigurasi di Bab 5 — pada tahap ini cukup pastikan status link menyala hijau.

Rangkuman

- VLSM membagi satu blok alamat menjadi subnet dengan ukuran berbeda sesuai kebutuhan host, dialokasikan dari kebutuhan terbesar ke terkecil.
- Jumlah host usable = 2 pangkat n dikurangi 2 (n = jumlah bit host).
- Tabel pengalamatan (addressing table) adalah dokumen rujukan wajib sebelum konfigurasi dilakukan.
- Link WAN point-to-point idealnya menggunakan subnet /30 tersendiri, terpisah dari blok alamat LAN.

Soal Latihan/Refleksi

- 1. Sebuah segmen jaringan membutuhkan 25 host. Tentukan prefix (CIDR) minimum yang mencukupi beserta jumlah host usable-nya.
- 2. Lakukan VLSM untuk blok 10.10.0.0/24 dengan kebutuhan: LAN A 60 host, LAN B 28 host, LAN C 12 host, dan 2 link WAN /30. Susun tabel pengalamatan lengkap.
- 3. Mengapa link WAN point-to-point sebaiknya menggunakan /30 dan bukan /24?
- 4. Jelaskan risiko yang terjadi jika dua cabang berbeda menggunakan blok alamat IP yang sama (tumpang tindih).

Checkpoint Bab 3 — Perencanaan Skema Pengalamatan IP (VLSM)

Sebelum kelompok melanjutkan ke bab berikutnya, pastikan seluruh item di bawah ini sudah terverifikasi langsung oleh guru pada file proyek .pkt kelompok tersebut:

No	Item Verifikasi	Status
1	Perhitungan VLSM sudah dituliskan di atas kertas/dokumen sebelum dipindahkan ke Packet Tracer.	☐ Sudah ☐ Belum
2	Tabel pengalamatan (perangkat, interface, IP, subnet mask, keterangan) sudah lengkap dan konsisten dengan hasil VLSM.	☐ Sudah ☐ Belum
3	Seluruh perangkat sudah terhubung dengan jenis kabel yang sesuai (copper untuk PC-switch/switch-router, serial DCE/DTE untuk WAN).	☐ Sudah ☐ Belum

4	IP address pada setiap interface PC dan router sudah diisi sesuai tabel pengalamatan.	☐ Sudah ☐ Belum
5	Status link antar perangkat pada subnet yang sama sudah hijau; ping ANTAR subnet berbeda memang belum berhasil (wajar, karena routing belum dikonfigurasi).	☐ Sudah ☐ Belum
6	Alokasi subnet WAN point-to-point (/30) sudah terpisah dari blok alamat LAN.	☐ Sudah ☐ Belum

Nama Kelompok: _____ Tanggal Verifikasi: _____
Catatan Guru: _____
Paraf Guru: _____

BAB 4 — Perencanaan VLAN dan Segmentasi Layer 2

Tujuan Pembelajaran

Bab ini merujuk pada Elemen 3 dokumen target dengan dua target kompetensi: merancang struktur VLAN berdasarkan fungsi/departemen, dan merencanakan alokasi Native VLAN serta trunking. Bab ini melatih siswa memisahkan trafik secara logis pada Layer 2 sebelum trafik tersebut dirutekan pada Layer 3.

4.1 Struktur VLAN Berdasarkan Fungsi/Departemen

VLAN (Virtual Local Area Network) memungkinkan satu switch fisik dipecah menjadi beberapa jaringan logis yang saling terisolasi, meski perangkatnya terhubung pada switch yang sama. Pembagian VLAN idealnya mengikuti fungsi/departemen, bukan lokasi fisik semata, karena mempermudah penerapan kebijakan keamanan per kelompok pengguna.

Melanjutkan studi kasus ITNSA.ID Corp, kebutuhan VLAN kantor pusat dapat dirancang sebagai berikut:

VLAN ID	Nama VLAN	Fungsi	Subnet Terkait
10	VLAN_INTERNAL	Jaringan staf/karyawan	192.168.10.0/26
20	VLAN_MANAGEMENT	Manajemen perangkat jaringan (switch, router)	192.168.10.64/28
30	VLAN_DMZ	Segmen server publik (web, mail)	192.168.10.80/29
1	default (Native)	VLAN bawaan, tidak dipakai untuk data produksi	-
99	VLAN_NATIVE (jika dikustomisasi)	Trafik untagged pada trunk, dipisah dari VLAN 1 untuk keamanan	-

Praktik terbaik yang perlu ditanamkan ke siswa: jangan pernah menggunakan VLAN 1 (default) untuk trafik data produksi, karena VLAN 1 memiliki banyak trafik kontrol bawaan (CDP, VTP, STP) yang membuatnya rentan dijadikan target serangan VLAN hopping.

4.2 Native VLAN dan Trunking

Trunk adalah jalur antar switch (atau antara switch dan router) yang membawa trafik dari banyak VLAN sekaligus, dengan setiap frame diberi tag 802.1Q berisi nomor VLAN asal. Native VLAN adalah satu-satunya VLAN pada jalur trunk yang frame-nya dikirim TANPA tag (untagged) — biasanya digunakan untuk kompatibilitas perangkat lama, namun praktik yang lebih aman adalah mengalihkan Native VLAN ke VLAN yang tidak dipakai (mis. VLAN 99) alih-alih VLAN 1 default.

Aturan Penting Trunking

Kedua ujung link trunk harus memiliki Native VLAN yang sama, jika tidak maka switch akan mencatat peringatan 'native VLAN mismatch'.

Access port (port ke PC/printer) hanya membawa satu VLAN dan tidak memerlukan tagging.

Trunk port hanya digunakan antar switch, atau antara switch dan router (untuk router-on-a-stick) — bukan ke PC biasa.

Praktik/Aktivitas Pembelajaran

Aktivitas 4.1 — Merancang Tabel VLAN (20 menit): Siswa menyusun tabel VLAN seperti contoh di atas untuk topologi ITNSA.ID Corp yang sedang dikerjakan, termasuk menentukan port mana saja yang menjadi access port dan mana yang trunk.

Aktivitas 4.2 — Konfigurasi VLAN dan Trunk di Packet Tracer (60 menit): Pada switch HQ, buat VLAN sesuai tabel, tetapkan access port ke PC, dan konfigurasi trunk antar switch/ke router:

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name VLAN_INTERNAL
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name VLAN_MANAGEMENT
Switch(config-vlan)# exit
Switch(config)# vlan 30
Switch(config-vlan)# name VLAN_DMZ
Switch(config-vlan)# exit
Switch(config)# vlan 99
Switch(config-vlan)# name NATIVE_UNUSED
Switch(config-vlan)# exit
! Access port ke PC staf
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
! Trunk port ke switch/router lain
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 99
Switch(config-if)# switchport trunk allowed vlan 10,20,30,99
```

Verifikasi hasil konfigurasi dengan perintah show vlan brief dan show interfaces trunk, lalu minta siswa menjelaskan output tersebut untuk memastikan pemahaman, bukan sekadar menyalin perintah.

Rangkuman

- VLAN memisahkan trafik secara logis pada satu switch fisik, idealnya dikelompokkan berdasarkan fungsi/departemen.
- Hindari penggunaan VLAN 1 (default) untuk trafik data produksi karena alasan keamanan.
- Trunk membawa banyak VLAN sekaligus dengan tagging 802.1Q; Native VLAN adalah satu-satunya VLAN yang untagged pada trunk tersebut.
- Kedua ujung trunk wajib memiliki Native VLAN yang sama untuk menghindari mismatch.

Soal Latihan/Refleksi

- 1. Mengapa VLAN 1 sebaiknya tidak digunakan untuk trafik data produksi?
- 2. Sebuah sekolah ingin memisahkan jaringan Lab Komputer, Ruang Guru, dan Perpustakaan menjadi VLAN berbeda. Rancang tabel VLAN (ID, nama, fungsi) untuk kebutuhan tersebut.
- 3. Apa yang terjadi jika Native VLAN pada kedua ujung sebuah trunk berbeda?
- 4. Jelaskan perbedaan access port dan trunk port, beserta contoh penggunaannya masing-masing.

Checkpoint Bab 4 — Perencanaan VLAN dan Segmentasi Layer 2

Sebelum kelompok melanjutkan ke bab berikutnya, pastikan seluruh item di bawah ini sudah terverifikasi langsung oleh guru pada file proyek .pkt kelompok tersebut:

No	Item Verifikasi	Status
1	Tabel VLAN (ID, nama, fungsi, subnet terkait) sudah disusun sesuai kebutuhan topologi.	☐ Sudah ☐ Belum
2	VLAN sudah dibuat di switch sesuai tabel, dan VLAN 1 (default) tidak dipakai untuk trafik data produksi.	☐ Sudah ☐ Belum
3	Access port ke PC/server sudah diarahkan ke VLAN yang benar (switchport mode access + switchport access vlan).	☐ Sudah ☐ Belum
4	Trunk port antar switch/ke router sudah dikonfigurasi dengan Native VLAN yang konsisten di kedua ujung.	☐ Sudah ☐ Belum
5	Output show vlan brief dan show interfaces trunk sudah diperiksa dan sesuai rencana.	☐ Sudah ☐ Belum

Nama Kelompok: _____ Tanggal Verifikasi: _____

Catatan Guru: _____

Paraf Guru: _____

BAB 5 — Perencanaan Routing

Tujuan Pembelajaran

Bab ini merujuk pada Elemen 4 dokumen target dengan empat target kompetensi: memilih protokol routing sesuai kebutuhan topologi, merencanakan Router ID dan AS/Process ID, merencanakan jaringan yang diadvertise dan passive interface, serta merencanakan default route. Bab ini adalah bab dengan bobot terbesar karena routing menghubungkan seluruh segmen yang telah direncanakan pada bab-bab sebelumnya.

5.1 Memilih Protokol Routing

Routing statis cocok untuk jaringan kecil dengan jalur yang jarang berubah — konfigurasinya sederhana namun tidak otomatis menyesuaikan bila ada perubahan topologi. Routing dinamis (EIGRP atau OSPF) lebih cocok untuk jaringan skala menengah-besar dengan banyak jalur alternatif, karena router saling bertukar informasi rute secara otomatis.

Kriteria	Routing Statis	EIGRP	OSPF
Kompleksitas konfigurasi	Sangat sederhana	Sedang	Sedang-Tinggi
Skalabilitas	Rendah (manual per rute)	Tinggi	Tinggi
Vendor	Universal	Cisco (proprietary, kini terbuka sebagian)	Standar terbuka (multi-vendor)
Kebutuhan konfigurasi tambahan	Tidak ada	AS Number	Process ID, Area (mis. Area 0)
Cocok untuk	Jaringan sangat kecil / stub network	Jaringan Cisco menengah dengan banyak link	Jaringan menengah-besar, multi-vendor

Untuk topologi ITNSA.ID Corp dengan 3 lokasi (HQ dan 2 cabang) yang saling terhubung, OSPF dipilih sebagai contoh utama pada buku ini karena sifatnya standar terbuka dan paling umum diujikan pada Modul B LKS, namun guru dapat pula melatih siswa dengan EIGRP sebagai pembanding menggunakan topologi yang sama.

5.2 Router ID dan Process ID/AS Number

Router ID adalah identitas unik 32-bit (format seperti alamat IP) yang membedakan satu router dari router lain dalam proses pertukaran rute OSPF/EIGRP. Jika tidak ditentukan manual, router akan memilih otomatis dari alamat IP tertinggi pada interface loopback atau interface aktifnya — praktik yang kurang dapat diprediksi, sehingga sebaiknya direncanakan dan ditentukan manual.

Process ID (OSPF) bersifat lokal per router dan hanya perlu konsisten pada router yang sama (boleh berbeda antar router, meski disarankan disamakan untuk kerapian dokumentasi). Sebaliknya, AS Number (EIGRP) WAJIB sama persis pada seluruh router yang ingin saling bertukar rute — jika berbeda, router tidak akan membentuk relasi tetangga (neighbor).

Router	Router ID (direncanakan)	OSPF Process ID	OSPF Area
HQ-CORE	1.1.1.1	1	Area 0

Router	Router ID (direncanakan)	OSPF Process ID	OSPF Area
CBG1-RTR	2.2.2.2	1	Area 0
CBG2-RTR	3.3.3.3	1	Area 0

5.3 Advertised Network dan Passive Interface

Jaringan yang diadvertise adalah daftar subnet yang diumumkan router ke tetangganya agar dapat dijangkau dari router lain. Prinsip perencanaan: advertise SEMUA subnet yang terhubung langsung ke router (LAN maupun WAN), kecuali subnet yang memang tidak perlu diketahui router lain.

Passive interface adalah interface yang tetap diadvertise subnetnya, namun TIDAK mengirim paket update routing melalui interface tersebut — cocok diterapkan pada interface yang mengarah ke LAN (berisi PC/server, bukan router lain), karena PC/server tidak perlu dan tidak akan memproses paket update routing. Menerapkan passive interface pada interface LAN mengurangi trafik broadcast/multicast yang tidak perlu dan menutup celah keamanan (mencegah perangkat asing di LAN ikut mengirim update routing palsu).

Aturan Perencanaan Passive Interface

Interface ke arah LAN (menuju switch berisi PC/server) → dijadikan passive interface.

Interface ke arah router lain (WAN point-to-point antar cabang) → TIDAK passive, karena harus saling bertukar update routing.

5.4 Default Route

Default route (0.0.0.0/0) digunakan agar router mengetahui ke mana harus meneruskan paket yang tujuannya tidak ada pada tabel routing spesifik — biasanya menuju jaringan luar/internet. Pada topologi multi-cabang, default route umumnya dikonfigurasi di router edge/HQ yang terhubung ke ISP, kemudian disebarkan (redistribusi sederhana) ke router cabang melalui protokol routing dinamis, sehingga cabang tidak perlu dikonfigurasi default route manual satu per satu.

Praktik/Aktivitas Pembelajaran

Aktivitas 5.1 — Merancang Tabel Routing Plan (20 menit): Siswa melengkapi tabel Router ID/Process ID dan menentukan interface mana yang perlu passive pada topologi ITNSA.ID Corp yang sedang dikerjakan.

Aktivitas 5.2 — Konfigurasi OSPF di Packet Tracer (60 menit): Lanjutkan proyek dari bab sebelumnya. Konfigurasi OSPF pada HQ-CORE:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 1
Router(config-router)# router-id 1.1.1.1
Router(config-router)# network 192.168.10.0 0.0.0.63 area 0
Router(config-router)# network 192.168.10.64 0.0.0.15 area 0
Router(config-router)# network 192.168.10.88 0.0.0.3 area 0
Router(config-router)# passive-interface GigabitEthernet0/0
Router(config-router)# passive-interface GigabitEthernet0/1
Router(config-router)# default-information originate
```

```
Router(config-router)# exit
Router(config)# ip route 0.0.0.0 0.0.0.0 <IP next-hop ISP>
```

Ulangi konfigurasi serupa (tanpa default-information originate dan ip route default) pada router tiap cabang, menyesuaikan router-id dan network sesuai tabel pengalamatan masing-masing. Verifikasi dengan show ip route, show ip ospf neighbor, dan uji ping antar segmen yang sebelumnya belum terhubung (mis. PC di Cabang 1 ke server DMZ di HQ) — inilah momen di mana koneksi antar subnet mulai berhasil untuk pertama kalinya.

Rangkuman

- Routing statis cocok untuk jaringan kecil/stabil; routing dinamis (EIGRP/OSPF) cocok untuk jaringan menengah-besar dengan banyak perubahan.
- Router ID harus direncanakan manual dan unik per router; AS Number (EIGRP) wajib sama di seluruh router, Process ID (OSPF) bersifat lokal.
- Semua subnet terhubung langsung wajib diadvertise; interface ke arah LAN dijadikan passive interface.
- Default route pada router edge/HQ disebarkan ke cabang melalui redistribusi sederhana agar seluruh jaringan memiliki jalur ke internet.

Soal Latihan/Refleksi

- 1. Jelaskan perbedaan mendasar antara Process ID pada OSPF dan AS Number pada EIGRP dari sisi konsistensi antar router.
- 2. Mengapa interface yang mengarah ke LAN sebaiknya dijadikan passive interface, sedangkan interface ke arah router lain tidak?
- 3. Sebuah router HQ memiliki 2 interface LAN dan 3 interface WAN ke cabang berbeda. Tentukan interface mana yang passive dan buat perintah network OSPF untuk seluruh subnet yang terhubung.
- 4. Jelaskan mengapa default route biasanya dikonfigurasi di router edge/HQ, bukan di setiap router cabang.

Checkpoint Bab 5 — Perencanaan Routing

Sebelum kelompok melanjutkan ke bab berikutnya, pastikan seluruh item di bawah ini sudah terverifikasi langsung oleh guru pada file proyek .pkt kelompok tersebut:

No	Item Verifikasi	Status
1	Tabel Router ID, Process ID, dan Area sudah direncanakan untuk setiap router sebelum konfigurasi.	☐ Sudah ☐ Belum
2	Router ID sudah ditentukan secara manual (tidak dibiarkan dipilih otomatis oleh router).	☐ Sudah ☐ Belum
3	Seluruh subnet yang terhubung langsung ke tiap router sudah diadvertise melalui OSPF.	☐ Sudah ☐ Belum
4	Interface ke arah LAN (menuju PC/server) sudah dijadikan passive interface.	☐ Sudah ☐ Belum
5	Default route sudah dikonfigurasi di router edge/HQ dan disebarkan ke seluruh cabang.	☐ Sudah ☐ Belum
6	Ping antar-subnet berbeda (mis. PC Cabang 1 ke server DMZ di HQ) sudah berhasil — ini menjadi tanda routing sudah berjalan end-to-end.	☐ Sudah ☐ Belum

7	Output show ip route dan show ip ospf neighbor sudah diperiksa dan sesuai rencana.	☐ Sudah ☐ Belum

Nama Kelompok: _____ Tanggal Verifikasi: _____
Catatan Guru: _____
Paraf Guru: _____

BAB 6 — Perencanaan Redundansi dan High Availability

Tujuan Pembelajaran

Bab ini merujuk pada Elemen 5 dokumen target dengan dua target kompetensi: merencanakan link aggregation (EtherChannel) untuk redundansi, dan merencanakan First Hop Redundancy Protocol (HSRP). Bab ini melatih siswa merancang jaringan yang tetap berjalan meski satu jalur atau satu perangkat gagal.

6.1 EtherChannel (Link Aggregation)

EtherChannel menggabungkan beberapa link fisik antar dua switch (atau switch-router) menjadi satu link logis, memberikan dua manfaat sekaligus: peningkatan bandwidth (total kapasitas gabungan) dan redundansi (jika satu kabel putus, trafik tetap berjalan melalui kabel lain tanpa terputus). Protokol negosiasi yang umum digunakan adalah PAgP (Cisco proprietary) dan LACP (standar terbuka, IEEE 802.3ad).

Mode	Protokol	Perilaku
active	LACP	Aktif menginisiasi negosiasi; port pasangan minimal harus active atau passive
passive	LACP	Menunggu negosiasi dari sisi lain; tidak akan terbentuk jika kedua sisi passive
desirable	PAgP	Aktif menginisiasi negosiasi; port pasangan minimal harus desirable atau auto
auto	PAgP	Menunggu negosiasi dari sisi lain; tidak akan terbentuk jika kedua sisi auto
on	Tidak ada (static)	Paksa EtherChannel tanpa negosiasi protokol — kedua sisi wajib 'on'

Perencanaan penting yang harus disepakati sebelum konfigurasi: kedua switch harus sepakat menggunakan port-port dengan kecepatan dan duplex yang sama, serta konfigurasi VLAN/trunk yang identik pada seluruh port anggota — EtherChannel akan gagal terbentuk (atau berperilaku tidak konsisten) jika port anggotanya tidak seragam.

6.2 HSRP (First Hop Redundancy Protocol)

HSRP menyediakan gateway redundan bagi host di suatu LAN: dua (atau lebih) router/switch layer-3 bekerja sama membentuk satu Virtual IP dan Virtual MAC Address yang digunakan host sebagai default gateway. Salah satu perangkat berperan sebagai Active (menangani trafik) dan yang lain sebagai Standby (siap mengambil alih jika Active gagal). Peran ini ditentukan oleh nilai priority — semakin tinggi priority, semakin besar kemungkinan menjadi Active.

Parameter Perencanaan HSRP

Virtual IP: satu alamat IP tambahan pada subnet LAN yang akan digunakan sebagai default gateway host, terpisah dari IP fisik masing-masing router.

Group Number: identitas grup HSRP (0-255), harus sama pada kedua router yang berpasangan pada subnet yang sama.

> Priority: nilai default 100; router dengan priority lebih tinggi menjadi Active. Naikkan priority pada router yang ingin dijadikan Active utama.
>
> Preempt: opsi agar router dengan priority lebih tinggi otomatis mengambil kembali peran Active begitu ia pulih dari gangguan.

Contoh perencanaan HSRP untuk VLAN Internal (192.168.10.0/26) pada HQ yang memiliki dua switch layer-3 sebagai gateway redundan:

Perangkat	IP Fisik Interface	Priority	Peran
HQ-SWL3-A	192.168.10.2	150	Active
HQ-SWL3-B	192.168.10.3	100 (default)	Standby
Virtual IP (gateway host)	192.168.10.1	-	Digunakan sebagai default gateway seluruh host di VLAN Internal

Praktik/Aktivitas Pembelajaran

Aktivitas 6.1 — Merancang Skema Redundansi (20 menit): Siswa menentukan pasangan switch mana pada topologi ITNSA.ID Corp yang akan digabung dengan EtherChannel, dan segmen LAN mana yang membutuhkan HSRP (biasanya VLAN Internal dengan jumlah host terbanyak).

Aktivitas 6.2 — Konfigurasi EtherChannel di Packet Tracer (30 menit): Pada dua switch yang terhubung dua kabel fisik sekaligus:

```
SwitchA(config)# interface range GigabitEthernet0/1-2
SwitchA(config-if-range)# channel-group 1 mode active
SwitchA(config-if-range)# exit
SwitchA(config)# interface port-channel 1
SwitchA(config-if)# switchport mode trunk
SwitchA(config-if)# switchport trunk allowed vlan 10,20,30,99
! Ulangi konfigurasi channel-group serupa pada SwitchB
```

Aktivitas 6.3 — Konfigurasi HSRP di Packet Tracer (30 menit): Pada dua switch layer-3/router yang menjadi gateway VLAN Internal:

```
HQ-SWL3-A(config)# interface vlan 10
HQ-SWL3-A(config-if)# ip address 192.168.10.2 255.255.255.192
HQ-SWL3-A(config-if)# standby 10 ip 192.168.10.1
HQ-SWL3-A(config-if)# standby 10 priority 150
HQ-SWL3-A(config-if)# standby 10 preempt

HQ-SWL3-B(config)# interface vlan 10
HQ-SWL3-B(config-if)# ip address 192.168.10.3 255.255.255.192
HQ-SWL3-B(config-if)# standby 10 ip 192.168.10.1
HQ-SWL3-B(config-if)# standby 10 priority 100
```

Verifikasi dengan show etherchannel summary dan show standby brief. Sebagai uji redundansi, matikan (shutdown) salah satu port anggota EtherChannel dan pastikan trafik tetap berjalan; matikan router Active HSRP dan amati router Standby mengambil alih peran Active.

Rangkuman

- EtherChannel menggabungkan beberapa link fisik menjadi satu link logis untuk menambah bandwidth sekaligus redundansi.
- Port anggota EtherChannel wajib seragam (kecepatan, duplex, konfigurasi VLAN/trunk) agar terbentuk dengan benar.
- HSRP menyediakan gateway redundan melalui Virtual IP; router dengan priority tertinggi berperan sebagai Active.
- Opsi preempt memastikan router utama otomatis kembali menjadi Active setelah pulih dari gangguan.

Soal Latihan/Refleksi

- 1. Jelaskan dua manfaat utama EtherChannel bagi sebuah jaringan.
- 2. Apa yang terjadi jika kedua ujung EtherChannel menggunakan mode LACP passive?
- 3. Pada HSRP, jelaskan fungsi Virtual IP dan mengapa ia berbeda dari IP fisik masing-masing router.
- 4. Jelaskan skenario nyata mengapa opsi preempt penting diaktifkan pada router dengan priority tertinggi.

Checkpoint Bab 6 — Perencanaan Redundansi dan High Availability

Sebelum kelompok melanjutkan ke bab berikutnya, pastikan seluruh item di bawah ini sudah terverifikasi langsung oleh guru pada file proyek .pkt kelompok tersebut:

No	Item Verifikasi	Status
1	Pasangan switch yang digabung EtherChannel sudah ditentukan, dengan port anggota seragam (kecepatan, duplex, konfigurasi VLAN/trunk).	☐ Sudah ☐ Belum
2	EtherChannel sudah terbentuk dan diverifikasi dengan show etherchannel summary.	☐ Sudah ☐ Belum
3	Segmen LAN yang membutuhkan HSRP (biasanya VLAN Internal) sudah diidentifikasi, lengkap dengan rencana Virtual IP, Group Number, dan Priority.	☐ Sudah ☐ Belum
4	HSRP sudah dikonfigurasi pada kedua router/switch layer-3, dan status Active/Standby sudah sesuai rencana (show standby brief).	☐ Sudah ☐ Belum
5	Uji kegagalan sudah dilakukan: mematikan satu port anggota EtherChannel tidak memutus konektivitas, dan mematikan router Active HSRP membuat router Standby mengambil alih.	☐ Sudah ☐ Belum

Nama Kelompok: _____ Tanggal Verifikasi: _____
Catatan Guru: _____
Paraf Guru: _____

BAB 7 — Perencanaan Layanan Pendukung Jaringan

Tujuan Pembelajaran

Bab ini merujuk pada Elemen 6 dokumen target dengan tiga target kompetensi: merencanakan alokasi pool DHCP, merencanakan skema NAT, dan merencanakan sinkronisasi waktu (NTP). Bab ini melengkapi jaringan yang telah memiliki pengalamatan, VLAN, routing, dan redundansi dengan layanan-layanan pendukung operasional sehari-hari.

7.1 Alokasi Pool DHCP

DHCP (Dynamic Host Configuration Protocol) memberikan alamat IP secara otomatis kepada host, sehingga administrator tidak perlu mengonfigurasi IP satu per satu pada ratusan perangkat. Perencanaan pool DHCP harus menyisihkan sebagian alamat di awal subnet untuk keperluan statis (gateway, server, perangkat manajemen) dan baru mengalokasikan sisanya untuk pool dinamis.

Subnet	Dikecualikan (Statis)	Pool DHCP (Dinamis)	Gateway	DNS
192.168.10.0/26 (Internal)	192.168.10.1 - 192.168.10.10	192.168.10.11 - 192.168.10.62	192.168.10.1	8.8.8.8
192.168.11.0/24 (Cabang 1)	192.168.11.1 - 192.168.11.10	192.168.11.11 - 192.168.11.254	192.168.11.1	8.8.8.8

Prinsip perencanaan: rentang yang dikecualikan (excluded) selalu ditentukan LEBIH DULU sebelum pool dibuat pada router, agar router tidak pernah menyewakan alamat yang sudah dipakai perangkat statis seperti gateway.

7.2 Skema NAT

NAT (Network Address Translation) menerjemahkan alamat IP privat (mis. 192.168.x.x) menjadi alamat IP publik agar perangkat di jaringan internal dapat mengakses internet, karena alamat privat tidak dapat dirutekan langsung di internet. PAT (Port Address Translation), sering disebut NAT Overload, memungkinkan banyak host privat berbagi satu alamat IP publik sekaligus dengan membedakan koneksi melalui nomor port.

Perencanaan Arah NAT

Inside (di dalam): interface yang menghadap ke jaringan privat (LAN/VLAN internal).

Outside (di luar): interface yang menghadap ke jaringan publik/ISP.

Access-list menentukan subnet privat mana saja yang boleh diterjemahkan (biasanya seluruh subnet LAN internal, TIDAK termasuk subnet DMZ yang sudah publik).

7.3 Sinkronisasi Waktu (NTP)

NTP (Network Time Protocol) menyinkronkan jam seluruh perangkat jaringan ke satu sumber waktu terpusat. Sinkronisasi waktu penting agar log dari berbagai perangkat (router, switch, server) dapat dibandingkan secara akurat saat troubleshooting atau investigasi insiden keamanan — log dengan waktu yang tidak sinkron akan sangat menyulitkan analisis urutan kejadian.

Perencanaan NTP sederhana: tentukan satu perangkat (biasanya router HQ/edge) sebagai sumber waktu (NTP server/master), kemudian seluruh perangkat lain (router cabang, switch) dikonfigurasi sebagai NTP client yang menunjuk ke perangkat tersebut.

Praktik/Aktivitas Pembelajaran

Aktivitas 7.1 — Merancang Tabel Pool DHCP (20 menit): Siswa melengkapi tabel pool DHCP untuk seluruh VLAN/subnet pada topologi ITNSA.ID Corp yang sedang dikerjakan.

Aktivitas 7.2 — Konfigurasi DHCP di Packet Tracer (30 menit):

```
Router(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.10
Router(config)# ip dhcp pool POOL_INTERNAL
Router(dhcp-config)# network 192.168.10.0 255.255.255.192
Router(dhcp-config)# default-router 192.168.10.1
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)# exit
```

Aktivitas 7.3 — Konfigurasi NAT/PAT di Packet Tracer (30 menit), pada router edge HQ:

```
Router(config)# access-list 1 permit 192.168.10.0 0.0.0.63
Router(config)# access-list 1 permit 192.168.11.0 0.0.0.255
Router(config)# access-list 1 permit 192.168.12.0 0.0.0.255
Router(config)# interface GigabitEthernet0/3
Router(config-if)# ip nat outside
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# ip nat inside source list 1 interface GigabitEthernet0/3 overload
```

Aktivitas 7.4 — Konfigurasi NTP di Packet Tracer (15 menit), pada router HQ sebagai master dan router cabang sebagai client:

```
! Di router HQ (master)
HQ-CORE(config)# ntp master 3

! Di router cabang (client)
CBG1-RTR(config)# ntp server 192.168.10.89
```

Verifikasi hasil dengan menguji PC client mendapat IP otomatis (ipconfig /all di Command Prompt PC), mengecek tabel translasi NAT dengan show ip nat translations, dan mengecek status sinkronisasi dengan show ntp status/associations pada router cabang.

Rangkuman

- Pool DHCP direncanakan dengan menyisihkan rentang statis lebih dulu sebelum mengalokasikan rentang dinamis.
- NAT/PAT menerjemahkan alamat privat menjadi alamat publik agar jaringan internal dapat mengakses internet; PAT memungkinkan banyak host berbagi satu IP publik.
- Access-list pada NAT menentukan subnet privat mana yang diterjemahkan, biasanya seluruh LAN internal tanpa DMZ.
- NTP menyinkronkan waktu seluruh perangkat ke satu sumber terpusat, penting untuk akurasi log dan troubleshooting.

Soal Latihan/Refleksi

- 1. Mengapa rentang alamat statis (gateway, server) harus dikecualikan (excluded) sebelum pool DHCP dibuat?
- 2. Jelaskan perbedaan NAT biasa dan PAT (NAT Overload) dari sisi jumlah host yang dapat dilayani.
- 3. Mengapa subnet DMZ pada studi kasus ITNSA.ID Corp umumnya TIDAK dimasukkan ke access-list NAT inside seperti subnet LAN internal?
- 4. Jelaskan dampak yang mungkin terjadi pada proses troubleshooting jika seluruh perangkat jaringan memiliki jam yang tidak sinkron.

Checkpoint Bab 7 — Perencanaan Layanan Pendukung Jaringan

Sebelum kelompok melanjutkan ke bab berikutnya, pastikan seluruh item di bawah ini sudah terverifikasi langsung oleh guru pada file proyek .pkt kelompok tersebut:

No	Item Verifikasi	Status
1	Tabel pool DHCP (subnet, rentang excluded, rentang pool, gateway, DNS) sudah lengkap untuk seluruh VLAN/subnet.	☐ Sudah ☐ Belum
2	DHCP pool sudah dikonfigurasi di router, dan PC client berhasil mendapat IP otomatis (diverifikasi lewat ipconfig /all).	☐ Sudah ☐ Belum
3	Arah NAT inside/outside sudah ditentukan dengan benar, dan access-list NAT hanya mencakup subnet LAN internal (tidak termasuk DMZ).	☐ Sudah ☐ Belum
4	NAT/PAT sudah berfungsi — diverifikasi dengan show ip nat translations.	☐ Sudah ☐ Belum
5	NTP sudah dikonfigurasi (router HQ sebagai master, router cabang sebagai client), dan status sinkronisasi sudah diperiksa dengan show ntp status/associations.	☐ Sudah ☐ Belum

Nama Kelompok: _____ Tanggal Verifikasi: _____

Catatan Guru: _____

Paraf Guru: _____

BAB 8 — Dokumentasi dan Visualisasi Desain Jaringan

Tujuan Pembelajaran

Bab ini merujuk pada Elemen 7 dokumen target dengan tiga target kompetensi: membuat diagram topologi logis dan fisik, menyusun dokumentasi tabel pengalamatan dan konfigurasi, serta mempresentasikan dan mengomunikasikan hasil perencanaan. Bab ini menutup siklus perencanaan dengan mengubah seluruh pekerjaan Bab 2-7 menjadi dokumen yang dapat dibaca dan digunakan pihak lain.

8.1 Diagram Topologi Logis dan Fisik

Topologi logis menggambarkan alur data dan pengalamatan IP tanpa memperhatikan lokasi fisik perangkat — fokus pada bagaimana data mengalir dan bagaimana subnet saling terhubung. Topologi fisik menggambarkan lokasi nyata perangkat, jenis kabel, dan tata letak rak/ruangan. Packet Tracer secara unik menyediakan dua tampilan ini sekaligus: Logical Workspace dan Physical Workspace.

Standar Minimum Diagram Logis

Setiap perangkat diberi label nama yang deskriptif (mis. HQ-CORE, bukan Router0).
Setiap link diberi label subnet/IP pada kedua ujungnya.
VLAN pada tiap segmen dicantumkan sebagai anotasi.
Zona (INT/DMZ/WAN) dikelompokkan secara visual, misalnya dengan kotak/warna berbeda.

8.2 Dokumentasi Tabel Pengalamatan dan Konfigurasi

Dokumentasi tertulis melengkapi diagram visual dengan detail yang tidak muat digambarkan. Dokumen lengkap idealnya berisi kumpulan seluruh tabel yang telah disusun sepanjang Bab 2-7 dalam satu berkas: tabel requirement (Bab 2), tabel pengalamatan IP (Bab 3), tabel VLAN (Bab 4), tabel routing plan (Bab 5), tabel redundansi (Bab 6), dan tabel layanan pendukung (Bab 7). Susunan ini sekaligus menjadi bukti proses perencanaan yang runtut, bukan hanya hasil akhir.

Selain tabel, dokumentasi konfigurasi berisi salinan perintah CLI kunci yang telah diterapkan pada tiap perangkat (dapat diambil dari output show running-config), sehingga jika suatu saat perangkat perlu dikonfigurasi ulang dari awal, dokumen ini menjadi rujukan langsung.

8.3 Mempresentasikan Hasil Perencanaan

Kemampuan mengomunikasikan rancangan sama pentingnya dengan kemampuan merancang itu sendiri. Latih siswa menjelaskan alasan (justifikasi) di balik setiap keputusan desain, bukan hanya menyebutkan hasilnya — misalnya, bukan sekadar 'saya pakai OSPF', melainkan 'saya pakai OSPF karena jaringan ini punya banyak jalur alternatif antar cabang dan bersifat multi-vendor'.

Kerangka Presentasi yang Disarankan

1. Ringkasan kebutuhan bisnis dan hasil analisis (Bab 2).
2. Skema pengalamatan dan alasan pembagian VLSM (Bab 3).
3. Struktur VLAN dan trunking (Bab 4).
4. Pilihan protokol routing dan alasan pemilihannya (Bab 5).

5. Mekanisme redundansi yang diterapkan (Bab 6).
6. Layanan pendukung yang disediakan (Bab 7).
7. Demonstrasi singkat konektivitas end-to-end di Packet Tracer.

Praktik/Aktivitas Pembelajaran

Aktivitas 8.1 — Menata Physical Workspace (30 menit): Pada file proyek Packet Tracer yang sama, buka tab Physical Workspace. Tempatkan perangkat pada representasi rak/ruangan sesuai lokasi (HQ, Cabang 1, Cabang 2), lalu ambil screenshot sebagai dokumentasi topologi fisik.

Aktivitas 8.2 — Menyusun Dokumen Perencanaan Lengkap (60 menit): Siswa mengumpulkan seluruh tabel dan diagram dari Bab 2-8 menjadi satu dokumen (Word/PDF) yang rapi dan runtut, dilengkapi screenshot Logical Workspace dan Physical Workspace dari Packet Tracer.

Aktivitas 8.3 — Presentasi Kelompok (sesi terpisah, 10-15 menit per kelompok): Setiap kelompok mempresentasikan dokumen perencanaannya di depan kelas mengikuti kerangka presentasi yang disarankan, dan menjawab pertanyaan dari kelompok lain maupun guru.

Rangkuman

- Topologi logis menekankan alur data dan pengalamatan IP; topologi fisik menekankan lokasi nyata perangkat dan kabel.
- Dokumentasi lengkap adalah kumpulan seluruh tabel perencanaan dari Bab 2-7, bukan hanya hasil akhir konfigurasi.
- Presentasi hasil perencanaan harus menyertakan justifikasi (alasan) di balik setiap keputusan desain, bukan sekadar menyebutkan hasil.

Soal Latihan/Refleksi

- 1. Sebutkan minimal empat informasi yang wajib ada pada sebuah diagram topologi logis yang baik.
- 2. Mengapa dokumentasi tabel pengalamatan tetap penting meski konfigurasi sudah berjalan baik di simulator?
- 3. Susun kerangka presentasi singkat (5 poin) untuk mempresentasikan hasil rancangan VLAN dan trunking pada Bab 4.

Checkpoint Bab 8 — Dokumentasi dan Visualisasi Desain Jaringan

Sebelum kelompok melanjutkan ke bab berikutnya, pastikan seluruh item di bawah ini sudah terverifikasi langsung oleh guru pada file proyek .pkt kelompok tersebut:

No	Item Verifikasi	Status
1	Physical Workspace sudah ditata sesuai lokasi nyata perangkat (HQ, Cabang 1, Cabang 2).	☐ Sudah ☐ Belum
2	Screenshot Logical Workspace dan Physical Workspace sudah diambil untuk dokumentasi.	☐ Sudah ☐ Belum
3	Seluruh tabel dari Bab 2–7 (requirement, pengalamatan, VLAN, routing, redundansi, layanan pendukung) sudah dikumpulkan menjadi satu dokumen.	☐ Sudah ☐ Belum
4	Dokumen sudah mencantumkan justifikasi (alasan) di balik keputusan desain utama, bukan hanya menyebutkan hasil akhirnya.	☐ Sudah ☐ Belum

5	Kerangka presentasi kelompok sudah disiapkan dan latihan presentasi singkat sudah dilakukan.	☐ Sudah ☐ Belum

Nama Kelompok: _____ Tanggal Verifikasi: _____
Catatan Guru: _____
Paraf Guru: _____

BAB 9 — Proyek Akhir Terintegrasi: Studi Kasus ITNSA.ID Corp

Tujuan Proyek

Proyek akhir ini menggabungkan seluruh 20 target kompetensi (Elemen 1-7) dalam satu pengerjaan menyeluruh, menggunakan satu file proyek Packet Tracer yang telah dibangun bertahap sejak Bab 2. Proyek ini berfungsi sebagai asesmen sumatif sekaligus simulasi format Modul B pada Lomba Kompetensi Siswa Bidang IT Network System Administration.

Deskripsi Skenario Lengkap

ITNSA.ID Corp adalah perusahaan dengan kantor pusat (HQ) dan dua kantor cabang. Kantor pusat memiliki: zona internal (staf, 50 host), zona management (10 host), dan zona DMZ (4 server: web01, web02, mail). Kedua cabang masing-masing memiliki 20-30 host dan terhubung ke HQ melalui link WAN point-to-point. HQ memiliki dua switch layer-3 (SWL3) yang berperan sebagai gateway redundan untuk VLAN Internal, terhubung dengan EtherChannel ke switch layer-2 (SWL2) di bawahnya. Seluruh jaringan menggunakan routing OSPF single-area, terhubung ke internet melalui NAT/PAT di router edge HQ.

Tahapan Pengerjaan

Tahap	Elemen	Keluaran yang Dinilai
1	Analisis Kebutuhan (Bab 2)	Dokumen requirement dan kerangka topologi awal
2	Pengalamatan IP (Bab 3)	Perhitungan VLSM dan tabel pengalamatan lengkap
3	VLAN & Trunking (Bab 4)	Tabel VLAN dan konfigurasi trunk/native VLAN
4	Routing (Bab 5)	Tabel Router ID/Process ID dan konfigurasi OSPF berjalan
5	Redundansi (Bab 6)	EtherChannel dan HSRP berfungsi, teruji dengan simulasi kegagalan
6	Layanan Pendukung (Bab 7)	DHCP, NAT/PAT, dan NTP berjalan dan terverifikasi
7	Dokumentasi (Bab 8)	Dokumen perencanaan lengkap dan presentasi hasil

Kriteria Keberhasilan (Definition of Done)

- Seluruh PC pada tiap VLAN mendapat IP otomatis dari DHCP sesuai pool yang direncanakan.
- PC di Cabang 1 dan Cabang 2 dapat melakukan ping ke server DMZ di HQ (menunjukkan routing OSPF berjalan end-to-end).
- PC internal dapat mengakses simulasi internet (mis. server luar) melalui NAT/PAT dari router edge HQ.
- Ketika salah satu port anggota EtherChannel dimatikan, konektivitas antar switch tetap berjalan tanpa terputus.
- Ketika router Active HSRP dimatikan, PC di VLAN Internal tetap dapat terhubung ke gateway (diambil alih router Standby).
- Dokumen perencanaan lengkap (tabel + diagram logis + diagram fisik) telah disusun dan dipresentasikan.

Rubrik Penilaian (Contoh)

Aspek	Bobot	Indikator Penilaian
Ketepatan Pengalamatan IP	20%	VLSM benar, tidak ada tumpang tindih, tabel pengalamatan lengkap dan konsisten dengan konfigurasi
Konfigurasi VLAN & Routing	25%	VLAN, trunk, dan OSPF terkonfigurasi benar; konektivitas end-to-end berhasil
Redundansi	15%	EtherChannel dan HSRP terbukti berfungsi saat diuji skenario kegagalan
Layanan Pendukung	15%	DHCP, NAT, NTP berjalan dan dapat diverifikasi
Dokumentasi & Presentasi	25%	Kelengkapan dokumen, kejelasan diagram, dan kemampuan menjelaskan justifikasi desain

Catatan bagi Guru

Proyek ini sebaiknya dikerjakan berkelompok (2-3 siswa) dengan pembagian peran yang jelas namun seluruh anggota memahami keseluruhan rancangan.

Alokasikan minimal 4-6 pertemuan untuk proyek ini mengingat cakupannya menggabungkan seluruh bab.

File proyek Packet Tracer (.pkt) yang telah dibangun bertahap sejak Bab 2 dapat langsung dilanjutkan dan disempurnakan pada proyek akhir ini.

Checkpoint Bab 9 — Proyek Akhir Terintegrasi

Sebelum kelompok melanjutkan ke bab berikutnya, pastikan seluruh item di bawah ini sudah terverifikasi langsung oleh guru pada file proyek .pkt kelompok tersebut:

No	Item Verifikasi	Status
1	Seluruh PC pada tiap VLAN mendapat IP otomatis dari DHCP sesuai pool yang direncanakan.	☐ Sudah ☐ Belum
2	PC di Cabang 1 dan Cabang 2 dapat melakukan ping ke server DMZ di HQ (routing OSPF berjalan end-to-end).	☐ Sudah ☐ Belum
3	PC internal dapat mengakses simulasi internet (mis. server luar) melalui NAT/PAT dari router edge HQ.	☐ Sudah ☐ Belum
4	Saat salah satu port anggota EtherChannel dimatikan, konektivitas antar switch tetap berjalan tanpa terputus.	☐ Sudah ☐ Belum
5	Saat router Active HSRP dimatikan, PC di VLAN Internal tetap terhubung ke gateway (diambil alih router Standby).	☐ Sudah ☐ Belum
6	Dokumen perencanaan lengkap (tabel + diagram logis + diagram fisik) telah disusun dan dipresentasikan.	☐ Sudah ☐ Belum
7	File proyek .pkt final sudah disimpan dan siap dikumpulkan sebagai bukti asesmen sumatif.	☐ Sudah ☐ Belum

Nama Kelompok: _____ Tanggal Verifikasi: _____

Catatan Guru: _____

Paraf Guru: _____

BAB 10 — Penutup

10.1 Ringkasan Capaian

Setelah menyelesaikan seluruh bab pada buku ini, siswa telah menuntaskan 20 target kompetensi (80% dari keseluruhan target Perencanaan dan Pengalamatan Jaringan), mencakup kemampuan menganalisis kebutuhan, merancang pengalamatan IPv4 dengan VLSM, merancang VLAN dan trunking, merencanakan dan mengimplementasikan routing OSPF, merancang redundansi EtherChannel dan HSRP, merencanakan layanan pendukung (DHCP, NAT, NTP), serta mendokumentasikan dan mempresentasikan hasil rancangan — seluruhnya dilatih melalui praktik langsung di Cisco Packet Tracer dengan satu studi kasus berkelanjutan, ITNSA.ID Corp.

10.2 Kaitan dengan Kelas XII

Lima target pendalaman yang belum dibahas pada buku ini — pengalamatan IPv6 dual-stack, pengalamatan VPN, distribusi VLAN melalui VTP, redundansi Virtual IP berbasis Keepalived, dan integrasi DNS forward/reverse zone — akan dibahas pada dokumen "Target Perencanaan dan Pengalamatan Jaringan Kelas XII". Sebagian materi pendalaman tersebut memerlukan simulasi dengan GNS3 karena melibatkan sistem operasi Linux nyata (Keepalived, DNS server) yang tidak dapat disimulasikan penuh oleh Packet Tracer. Fondasi yang kuat dari buku ini — terutama pemahaman VLSM, routing OSPF, dan kebiasaan mendokumentasikan rancangan secara rapi — akan sangat menentukan kelancaran siswa mempelajari materi pendalaman tersebut.

10.3 Daftar Pustaka dan Referensi

- Naskah Soal LKS SMK Tingkat Kabupaten Tasikmalaya Tahun 2026, Bidang IT Network System Administration (Modul A: Linux Environment & Modul B: Cisco Packet Tracer).
- Dokumen Target Pembelajaran Perencanaan dan Pengalamatan Jaringan Kelas XI (Porsi 80%).
- Capaian Pembelajaran Kurikulum Merdeka, Program Keahlian Teknik Jaringan Komputer dan Telekomunikasi (TJKT).
- Cisco Networking Academy — Packet Tracer Official Documentation.
- Dokumentasi resmi Cisco IOS Command Reference untuk perintah routing, switching, HSRP, dan EtherChannel.

LAMPIRAN — MATERI DAN PRAKTIK LAB MENGGUNAKAN GNS3

Lampiran ini bersifat opsional, ditujukan bagi sekolah yang memiliki akses ke GNS3 selain (atau sebagai pengganti) Cisco Packet Tracer. GNS3 menjalankan image Cisco IOS asli dan dapat menyambungkan node Linux nyata, sehingga cocok digunakan untuk memperdalam proyek ITNSA.ID Corp yang telah dikerjakan pada Bab 2–9, sekaligus membuka target pendalaman yang tidak dapat disimulasikan penuh oleh Packet Tracer (lihat Bab 10.2).

G.1 GNS3 dan Packet Tracer: Kapan Menggunakan yang Mana

Packet Tracer tetap menjadi alat utama buku ini karena ringan dan cukup untuk seluruh target inti Bab 2–9. GNS3 disarankan sebagai pengayaan ketika sekolah memiliki perangkat yang memadai dan ingin memberi siswa pengalaman command line yang identik dengan perangkat asli, atau ingin membuka target pendalaman kelas XII.

Aspek	Packet Tracer	GNS3
Jenis image	Simulasi buatan Cisco (bukan IOS asli)	IOS/IOS-XE asli atau IOU, plus node Linux nyata
Kebutuhan sumber daya	Ringan, berjalan di laptop biasa	Lebih berat (RAM/CPU), terutama untuk banyak router
Dukungan sistem Linux nyata	Tidak ada (hanya PC/simulasi servis)	Ada — bisa memasang Ubuntu/Alpine/Docker sebagai server
Akurasi command line	Mendekati, sejumlah perintah dibatasi	Sama persis dengan perangkat asli
Fitur lanjutan (VTP, Keepalived, DNS zone, IPv6 dual-stack, VPN)	Sebagian besar tidak didukung	Didukung penuh
Paling cocok untuk	Bab 2–9 (pembelajaran inti, kelas besar)	Pengayaan Bab 2–9 + lima target pendalaman kelas XII

G.2 Persiapan Environment GNS3

Sebelum memindahkan proyek ke GNS3, siapkan environment berikut:

- Unduh dan pasang aplikasi GNS3 beserta GNS3 VM (disarankan dijalankan di atas VirtualBox/VMware agar performa lebih stabil).
- Siapkan image Cisco IOS/IOS-XE untuk router dan Cisco IOSvL2 untuk switch layer 2/3.
- Siapkan image Linux ringan (mis. Alpine atau Ubuntu Server) untuk merepresentasikan server DHCP, DNS, NTP, web, dan Keepalived.
- Hubungkan GNS3 Desktop dengan GNS3 VM, lalu uji koneksi dasar antara dua node sederhana sebelum membangun topologi besar.
- Alokasikan RAM secukupnya per node (idealnya 256–512 MB per router IOS) agar topologi 5–7 perangkat tetap responsif.

Catatan Legalitas Image

Image Cisco IOS bersifat berbayar dan berlisensi. Gunakan hanya image yang diperoleh sekolah secara sah, misalnya melalui Cisco Networking Academy atau Cisco Learning Network. Jangan mengunduh atau membagikan image dari sumber tidak resmi.

G.3 Memetakan Proyek ITNSA.ID Corp ke GNS3

Topologi dan skenario ITNSA.ID Corp pada Bab 1.7 tidak perlu diubah — hanya perangkat simulasinya yang disesuaikan. Gunakan padanan berikut saat membangun ulang proyek di GNS3:

Perangkat di Packet Tracer	Padanan di GNS3
Router HQ-CORE / router cabang (mis. 1941, 2911)	Image router Cisco IOSv/IOS-XE dengan jumlah interface serupa
Switch akses/distribusi (mis. 2960)	Image Cisco IOSvL2 (mendukung VLAN, trunk, EtherChannel)
PC/Laptop client	Node VPCS, atau node Linux ringan bila perlu menguji DNS/DHCP client secara nyata
Server (WEB, DNS, NTP)	Container/VM Linux (Alpine/Ubuntu) dengan servis terkait berjalan sungguhan
Kabel tembaga/serial antar perangkat	Link Ethernet/Serial bawaan GNS3 antar node, mengikuti topologi yang sama

G.4 Penyesuaian Praktik per Bab (Bab 2–9) jika Menggunakan GNS3

Seluruh aktivitas pada Bab 2–9 dapat dikerjakan ulang di GNS3 tanpa mengubah tabel perencanaan yang sudah disusun siswa. Berikut penyesuaian utama per bab:

Bab	Penyesuaian Utama di GNS3	Catatan
Bab 2	Penempatan perangkat sama; gunakan node router/switch/Linux sesuai zona (INT, DMZ, WAN).	Segmentasi visual bisa memakai fitur note/rectangle bawaan GNS3.
Bab 3	Perhitungan VLSM dan tabel pengalamatan tidak berubah; verifikasi dengan show ip interface brief pada IOS asli.	Perintah verifikasi persis sama dengan perangkat sungguhan.
Bab 4	VLAN, trunk, dan native VLAN dikonfigurasi di image IOSvL2.	Bisa ditambah VTP untuk sinkronisasi VLAN antar switch (lihat G.5).
Bab 5	Konfigurasi OSPF/EIGRP identik; Router ID diverifikasi dengan show ip ospf/eigrp.	Bisa ditambah IPv6 dual-stack sebagai pengayaan (lihat G.5).

Bab	Penyesuaian Utama di GNS3	Catatan
Bab 6	EtherChannel dan HSRP dikonfigurasi identik di IOSvL2/IOSv.	Sebagai pembanding, coba Keepalived (VRRP) di node Linux (lihat G.5).
Bab 7	DHCP dan NAT bisa memakai IOS asli, atau server Linux (isc-dhcp-server); NTP memakai ntpd/chrony pada node Linux nyata.	Hasil lebih realistis dibanding simulasi Packet Tracer.
Bab 8	Dokumentasi disusun dengan cara yang sama; ambil tangkapan layar topologi GNS3.	Tambahkan hasil show run asli sebagai bukti dokumentasi.
Bab 9	Proyek akhir dapat dikerjakan penuh di GNS3 sebagai versi lanjutan (advanced).	Kombinasikan dengan aktivitas pengayaan pada G.5 bila waktu memungkinkan.

G.5 Aktivitas Praktik Tambahan Khusus GNS3 (Target Pendalaman Kelas XII)

Lima aktivitas berikut memanfaatkan kemampuan GNS3 yang tidak tersedia di Packet Tracer. Aktivitas ini bersifat pengayaan dan berkaitan dengan lima target pendalaman yang disebutkan pada Bab 10.2, dan dapat dikerjakan setelah proyek inti (Bab 2–9) selesai.

Aktivitas G.1 — IPv6 Dual-Stack pada Router Edge (30 menit): Pada router HQ-CORE dan router cabang, aktifkan ipv6 unicast-routing lalu tambahkan alamat IPv6 pada interface yang sudah memiliki alamat IPv4, tanpa menghapus konfigurasi IPv4. Verifikasi dengan show ipv6 interface brief dan uji ping6 antar segmen.

Aktivitas G.2 — VPN Site-to-Site (IPsec) antar Cabang (40 menit): Konfigurasikan tunnel IPsec site-to-site antara router HQ dan salah satu router cabang menggunakan crypto isakmp dan crypto ipsec, lalu uji trafik yang melewati tunnel dengan traceroute.

Aktivitas G.3 — VTP untuk Sinkronisasi VLAN antar Switch (20 menit): Jadikan satu switch sebagai VTP server dan switch lain sebagai VTP client dalam domain yang sama, lalu buktikan bahwa VLAN baru yang dibuat di server otomatis muncul di client tanpa dikonfigurasi manual.

Aktivitas G.4 — Keepalived (VRRP) pada Server Linux (30 menit): Pasang dan konfigurasikan Keepalived pada dua node Linux sebagai gateway redundan untuk satu segmen, sebagai pembanding terhadap HSRP yang telah dikerjakan pada Bab 6. Matikan node master dan amati proses failover ke node backup.

Aktivitas G.5 — DNS Forward/Reverse Zone dengan BIND9 (30 menit): Pasang BIND9 pada node server Linux, buat zone forward (mis. itnsa.id) dan zone reverse untuk subnet DMZ, lalu uji resolusi nama dan resolusi IP-ke-nama dari PC client menggunakan nslookup atau dig.

G.6 Rangkuman

- GNS3 mengemulasikan image Cisco IOS asli dan mendukung node Linux nyata, sehingga cocok digunakan untuk pengayaan proyek ITNSA.ID Corp.
- Seluruh aktivitas Bab 2–9 dapat dipindahkan langsung ke GNS3 dengan topologi dan tabel perencanaan yang sama, tanpa perhitungan ulang.
- GNS3 membuka lima target pendalaman kelas XII yang tidak dapat disimulasikan penuh oleh Packet Tracer: IPv6 dual-stack, VPN, VTP, Keepalived, dan DNS zone.

- Image Cisco IOS wajib diperoleh sekolah secara legal sebelum digunakan dalam pembelajaran.

G.7 Catatan bagi Guru

- GNS3 membutuhkan spesifikasi komputer yang lebih tinggi dibanding Packet Tracer; pertimbangkan lab berkelompok atau bergiliran jika perangkat sekolah terbatas.
- Alokasikan waktu tambahan di luar jadwal reguler, karena environment GNS3 lebih kompleks bagi siswa yang baru pertama kali menggunakannya.
- Gunakan GNS3 sebagai pengayaan opsional, bukan pengganti wajib Packet Tracer — kecuali sekolah memang menargetkan kompetisi keahlian atau kelas XII yang membutuhkan simulasi lebih presisi.

G.8 Langkah Instalasi dan Uji Coba Dasar GNS3 (Step-by-Step)

Bagian G.2 sebelumnya merangkum kebutuhan environment secara umum. Bagian ini memandu guru dan siswa melakukan instalasi hingga uji coba dasar secara berurutan, sehingga proses persiapan lab tidak menebak-nebak langkah.

A. Instalasi GNS3 Desktop dan GNS3 VM

- 1. Unduh GNS3 Desktop dan GNS3 VM dari situs resmi gns3.com (menu Download), pilih versi GNS3 VM yang sesuai hypervisor yang tersedia di lab (VirtualBox, VMware, atau Hyper-V).
- 2. Pasang GNS3 Desktop seperti aplikasi pada umumnya (Next – Next – Finish).
- 3. Impor GNS3 VM ke VirtualBox/VMware melalui menu File > Import Appliance, arahkan ke file .ova hasil unduhan.
- 4. Nyalakan GNS3 VM terlebih dahulu dari VirtualBox/VMware, tunggu hingga layar konsol menampilkan alamat IP VM (mis. 192.168.56.101).
- 5. Buka GNS3 Desktop, masuk ke menu Edit > Preferences > GNS3 VM, centang "Enable the GNS3 VM", pilih hypervisor yang digunakan.
- 6. Klik tombol Apply, lalu perhatikan indikator status di pojok kanan bawah jendela GNS3 Desktop — status berwarna hijau bertuliskan "GNS3 VM (…) running" menandakan environment siap dipakai.

> **Tips Guru**
>
> Jika status tidak kunjung hijau, periksa pengaturan jaringan VirtualBox untuk GNS3 VM: adapter pertama sebaiknya bertipe NAT (untuk update), adapter kedua bertipe Host-only (untuk komunikasi dengan GNS3 Desktop).
>
> Untuk laboratorium dengan banyak siswa, GNS3 VM dapat dijalankan di satu server lab yang lebih kuat, sementara GNS3 Desktop tiap siswa terhubung ke server tersebut melalui jaringan lokal.

B. Mengimpor Image Cisco IOS

- 1. Buka menu Edit > Preferences > IOS Routers, klik New.
- 2. Pilih lokasi menjalankan image: "Run this IOS on the GNS3 VM" (disarankan) atau pada komputer lokal bila GNS3 VM tidak digunakan.
- 3. Klik Browse, arahkan ke file image IOS (.bin) yang telah diperoleh sekolah secara legal, lalu klik Next.

- 4. Beri nama template yang deskriptif (mis. "Router-1941"), sesuaikan alokasi RAM mengikuti rekomendasi bawaan (umumnya 256–512 MB sudah cukup untuk topologi kecil-menengah), klik Next hingga Finish.
- 5. Ulangi proses yang sama untuk image switch layer-3 (IOSvL2) yang akan mewakili peran HQ-SWL3-A/B, HQ-ACCESS-SWL2, dan switch cabang.

C. Menyiapkan Node Server Linux

- 1. Buka menu Edit > Preferences > VirtualBox VMs (atau Qemu VMs), klik New.
- 2. Pilih image Linux ringan yang telah dipasang di VirtualBox — dapat diunduh siap pakai dari GNS3 Marketplace (mis. template "Alpine Linux").
- 3. Tentukan jumlah adapter jaringan sesuai kebutuhan node (minimal 1 untuk server biasa).
- 4. Simpan template. Node inilah yang nantinya berperan sebagai server DMZ (web, DNS, NTP) atau node Keepalived pada aktivitas pengayaan (lihat G.10).

D. Uji Coba Topologi Sederhana (2 Router)

Sebelum membangun ulang topologi ITNSA.ID Corp secara penuh, lakukan uji coba kecil ini untuk memastikan environment benar-benar siap:

- 1. Seret dua node router ke kanvas, hubungkan kabel antar interface GigabitEthernet0/0 kedua router.
- 2. Klik tombol Start All (ikon segitiga hijau) pada toolbar untuk menjalankan seluruh node.
- 3. Klik kanan salah satu router, pilih Console, tunggu hingga jendela terminal CLI terbuka.
- 4. Konfigurasikan IP dasar pada kedua router dan uji ping seperti contoh berikut:

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# end
Router# ping 10.0.0.2
```

Jika balasan ping berhasil (ditandai tanda seru berulang, mis. !!!!!), environment GNS3 dinyatakan siap digunakan untuk membangun ulang topologi ITNSA.ID Corp secara penuh sesuai padanan perangkat pada Tabel G.3.

> **Tips Guru**
>
> Jika console tidak dapat terbuka atau macet, periksa Edit > Preferences > General > Console applications, arahkan aplikasi terminal yang benar-benar terpasang di komputer (mis. SolarPuTTY, atau Windows Terminal).
>
> Simpan hasil uji coba ini sebagai baseline: jika suatu saat topologi besar bermasalah, guru dapat membandingkan dengan kondisi topologi 2-router sederhana ini untuk mengisolasi penyebab (lihat juga G.11 Troubleshooting).

G.9 Panduan Dasar Berinteraksi dengan Node

Sebelum mengerjakan ulang praktik Bab 2–9 di GNS3, siswa perlu terbiasa dengan dua jenis node yang paling sering dipakai sebagai pengganti PC/perangkat pada Packet Tracer: VPCS (Virtual PC Simulator) dan node Cisco IOS asli. Perintah dasar berikut berlaku umum di seluruh bab.

A. Perintah Dasar CLI IOS (Router/Switch)

Karena GNS3 menjalankan image IOS asli, seluruh perintah CLI pada Bab 2–9 buku ini berlaku identik tanpa penyesuaian. Dua perintah tambahan yang penting diketahui siswa:

```
! Melihat konfigurasi yang sedang berjalan
Router# show running-config

! Menyimpan konfigurasi agar tidak hilang saat node dimatikan/restart
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Perbedaan Penting dari Packet Tracer

Packet Tracer otomatis menyimpan status konfigurasi bersama file .pkt. Pada GNS3, konfigurasi HARUS disimpan manual dengan copy running-config startup-config sebelum node dimatikan, atau seluruh konfigurasi akan hilang.

B. Perintah Dasar VPCS (Pengganti PC Sederhana)

VPCS adalah node ringan bawaan GNS3 yang mewakili PC/klien sederhana — cocok untuk menguji IP, ping, dan DHCP, namun tidak dapat menjalankan aplikasi sungguhan seperti browser. Gunakan node Linux penuh (lihat bagian C di G.8) bila aktivitas memerlukan aplikasi nyata, misalnya resolusi DNS pada G.10.

```
VPCS> ip 192.168.11.11/24 192.168.11.1
Checking for duplicate address...
PC1 : 192.168.11.11 255.255.255.0 gateway 192.168.11.1

VPCS> show ip
VPCS> ping 192.168.11.1
VPCS> dhcp
VPCS> save
```

C. Menata Ulang Topologi ITNSA.ID Corp di GNS3

Gunakan diagram Gambar 1.1 (Bab 1.7) sebagai acuan tata letak — susunan zona (HQ, DMZ, Cabang 1, Cabang 2) dan hubungan antar perangkat TIDAK berubah, hanya jenis node yang disesuaikan mengikuti padanan pada Tabel G.3. Tempatkan node sesuai zona secara visual, gunakan fitur "Add a note" atau "Draw a rectangle" pada toolbar kiri GNS3 untuk mengelompokkan zona secara visual — setara dengan anotasi kotak teks yang telah dibuat siswa di Logical Workspace Packet Tracer pada Bab 2.

G.10 Panduan Lengkap Aktivitas Pengayaan (Langkah dan Perintah CLI)

Bagian G.5 sebelumnya memperkenalkan lima aktivitas pengayaan secara ringkas. Bagian ini menguraikannya menjadi langkah konfigurasi dan perintah verifikasi yang lengkap, agar siswa dapat mempraktikkannya tanpa perlu menebak sintaks.

Detail Aktivitas G.1 — IPv6 Dual-Stack pada Router Edge

Tujuan: menyertakan alamat IPv6 berdampingan dengan IPv4 pada interface yang sama, tanpa mengganggu konfigurasi IPv4 yang sudah berjalan sejak Bab 3. Topologi tambahan: tidak diperlukan — gunakan topologi HQ-EDGE-RTR yang sudah ada.

```
HQ-EDGE-RTR(config)# ipv6 unicast-routing
HQ-EDGE-RTR(config)# interface GigabitEthernet0/0
HQ-EDGE-RTR(config-if)# ipv6 address 2001:DB8:10::1/64
HQ-EDGE-RTR(config-if)# ipv6 enable
HQ-EDGE-RTR(config-if)# exit
```

Verifikasi:

```
HQ-EDGE-RTR# show ipv6 interface brief
HQ-EDGE-RTR# ping ipv6 2001:DB8:10::2
```

Catatan: pastikan alamat IPv4 pada interface yang sama tetap ada dan tidak terhapus — itulah inti dual-stack, kedua protokol berjalan berdampingan pada satu interface fisik.

Detail Aktivitas G.2 — VPN Site-to-Site (IPsec) antar Cabang

Tujuan: mengenkripsi trafik antara LAN Internal HQ dan LAN Cabang 1 yang melewati jaringan WAN. Topologi tambahan: tidak diperlukan — gunakan link WAN HQ-EDGE-RTR ke CBG1-RTR yang sudah ada. Konfigurasi berikut diterapkan pada KEDUA ujung (HQ-EDGE-RTR dan CBG1-RTR), dengan menyesuaikan alamat IP peer satu sama lain:

```
crypto isakmp policy 10
 encryption aes 256
 hash sha256
 authentication pre-share
 group 14
crypto isakmp key CiscoVPN123 address <IP-WAN-lawan>
!
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
access-list 101 permit ip 192.168.10.0 0.0.0.63 192.168.11.0 0.0.0.255
!
crypto map VPNMAP 10 ipsec-isakmp
 set peer <IP-WAN-lawan>
 set transform-set TSET
 match address 101
!
interface Serial0/0/0
 crypto map VPNMAP
```

Verifikasi:

```
show crypto isakmp sa
show crypto ipsec sa
traceroute 192.168.11.11
```

Catatan: access-list menentukan trafik "interesting" mana yang wajib dienkripsi — pada contoh ini trafik dari subnet LAN Internal HQ menuju subnet LAN Cabang 1. Trafik lain tetap berjalan sebagai teks biasa (tidak dienkripsi).

Detail Aktivitas G.3 — VTP untuk Sinkronisasi VLAN

Tujuan: membuktikan bahwa VLAN yang dibuat pada satu switch (server) otomatis tersebar ke switch lain (client) dalam satu domain, tanpa perlu mengetik perintah vlan berulang di setiap switch. Langkah pada switch yang berperan sebagai VTP server:

```
SW-SERVER(config)# vtp domain ITNSACORP
SW-SERVER(config)# vtp mode server
SW-SERVER(config)# vtp password itnsa123
SW-SERVER(config)# vlan 40
SW-SERVER(config-vlan)# name VLAN_TEST
SW-SERVER(config-vlan)# exit
```

Langkah pada switch yang berperan sebagai VTP client:

```
SW-CLIENT(config)# vtp domain ITNSACORP
SW-CLIENT(config)# vtp mode client
SW-CLIENT(config)# vtp password itnsa123
```

Verifikasi (dijalankan pada switch client):

```
SW-CLIENT# show vtp status
SW-CLIENT# show vlan brief
```

Catatan: VLAN 40 yang dibuat di SW-SERVER akan otomatis muncul pada output show vlan brief di SW-CLIENT. Tunjukkan perbandingan ini langsung di depan kelas sebagai bukti kerja VTP — sekaligus mengingatkan siswa bahwa domain dan password HARUS identik pada seluruh switch anggota.

Detail Aktivitas G.4 — Keepalived (VRRP) pada Server Linux

Tujuan: membandingkan mekanisme redundansi gateway pada platform Linux (Keepalived/VRRP) dengan HSRP pada Cisco IOS yang telah dipraktikkan di Bab 6. Langkah berikut dijalankan pada KEDUA node Linux (MASTER dan BACKUP):

```
# Pasang paket keepalived
apt-get update && apt-get install -y keepalived

# Isi /etc/keepalived/keepalived.conf pada node MASTER
vrrp_instance VI_1 {
    state MASTER
    interface eth0
    virtual_router_id 51
    priority 150
    virtual_ipaddress {
        192.168.10.1/26
    }
}

systemctl restart keepalived
```

Pada node BACKUP, gunakan berkas konfigurasi yang sama persis, hanya ubah state menjadi BACKUP dan priority menjadi 100 (lebih rendah dari MASTER). Verifikasi:

```
ip addr show eth0        # Virtual IP hanya muncul di node yang sedang MASTER
systemctl status keepalived
# Matikan service keepalived di node MASTER, lalu amati:
```

```
# Virtual IP akan berpindah otomatis ke node BACKUP dalam hitungan detik
```

Catatan: konsepnya identik dengan HSRP pada Bab 6 — Virtual IP, nilai priority, dan failover otomatis — hanya berbeda platform (Cisco IOS vs Linux). Diskusikan dengan siswa: layanan/perangkat seperti apa yang lebih cocok memakai HSRP dan yang lebih cocok memakai Keepalived pada jaringan nyata.

Detail Aktivitas G.5 — DNS Forward/Reverse Zone dengan BIND9

Tujuan: menyediakan resolusi nama domain internal (forward zone) sekaligus resolusi IP-ke-nama (reverse zone) untuk server pada segmen DMZ. Langkah pada node server Linux DMZ:

```
apt-get install -y bind9

# Tambahkan pada /etc/bind/named.conf.local
zone "itnsa.id" {
    type master;
    file "/etc/bind/db.itnsa.id";
};
zone "10.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192.168.10";
};

# Isi /etc/bind/db.itnsa.id (forward zone)
web01   IN  A   192.168.10.81
mail    IN  A   192.168.10.83

# Isi /etc/bind/db.192.168.10 (reverse zone)
81  IN  PTR  web01.itnsa.id.
83  IN  PTR  mail.itnsa.id.

systemctl restart bind9
```

Verifikasi (dijalankan dari PC/node client, dengan DNS server diarahkan ke IP node BIND9 ini):

```
nslookup web01.itnsa.id 192.168.10.83
dig -x 192.168.10.81 @192.168.10.83
```

Catatan: pastikan PC client menunjuk DNS server ke IP node BIND9 ini, baik diisi manual maupun disebarkan lewat DHCP (dns-server pada Bab 7), agar resolusi nama dapat diuji end-to-end dari sisi pengguna, bukan hanya dari server itu sendiri.

G.11 Troubleshooting Umum di GNS3

Tabel berikut merangkum kendala yang paling sering dijumpai siswa/guru saat pertama kali menggunakan GNS3, beserta penyebab yang paling mungkin dan langkah penyelesaiannya.

Gejala	Kemungkinan Penyebab	Solusi
Node tidak mau menyala (ikon tetap merah/tanda seru)	Alokasi RAM tidak cukup, atau file image korup/salah	Kurangi RAM node lain yang sedang tidak dipakai, atau impor ulang image dari sumber yang sah
Console tidak bisa terbuka saat diklik	Aplikasi konsol default belum diarahkan dengan benar	Buka Edit > Preferences > General > Console applications, arahkan ke

Gejala	Kemungkinan Penyebab	Solusi
		aplikasi terminal yang benar-benar terpasang
Indikator GNS3 VM tetap merah (not running)	VM belum dinyalakan, atau adapter jaringan salah	Nyalakan GNS3 VM terlebih dahulu di VirtualBox/VMware; periksa adapter Host-only pada pengaturan VM
Ping antar node gagal padahal IP sudah sesuai	Interface belum diaktifkan (no shutdown), atau kabel terpasang di slot yang salah	Jalankan show ip interface brief pada kedua ujung, pastikan status up/up dan port fisik sesuai rencana
Topologi terasa sangat lambat saat banyak node aktif	RAM/CPU komputer host tidak mencukupi	Matikan (Stop) node yang sedang tidak digunakan; kerjakan topologi secara bertahap per zona
Konfigurasi VLAN/trunk tidak berjalan pada switch	Image yang dipakai adalah router biasa, bukan image switch layer 2/3	Gunakan template image khusus IOSvL2 untuk kebutuhan VLAN/trunk/EtherChannel
Konfigurasi hilang setelah node di-restart	Belum disimpan ke startup-config	Jalankan copy running-config startup-config sebelum menutup/mematikan node (lihat G.9.A)

G.12 Lembar Checkpoint Praktik GNS3

Gunakan lembar ini sebagai gerbang verifikasi sebelum kelompok dinyatakan tuntas mengerjakan pengayaan GNS3, sejalan dengan lembar checkpoint Bab 2–9 pada bagian utama buku ini.

No	Item Verifikasi	Status
1	GNS3 Desktop dan GNS3 VM sudah terpasang, status GNS3 VM "running" (hijau).	☐ Sudah ☐ Belum
2	Image Cisco IOS Router dan IOSvL2 sudah berhasil diimpor dan diuji pada topologi 2-router sederhana (G.8.D).	☐ Sudah ☐ Belum
3	Topologi ITNSA.ID Corp sudah dibangun ulang di GNS3 sesuai padanan perangkat pada Tabel G.3.	☐ Sudah ☐ Belum
4	Konfigurasi inti Bab 2–9 (pengalamatan, VLAN, routing, redundansi, layanan pendukung) sudah diverifikasi berjalan sama seperti di Packet Tracer.	☐ Sudah ☐ Belum
5	Minimal satu aktivitas pengayaan (G.1–G.5 pada G.10) sudah dicoba dan diverifikasi berhasil.	☐ Sudah ☐ Belum
6	Konfigurasi setiap node sudah disimpan (copy running-config startup-config) agar tidak hilang.	☐ Sudah ☐ Belum
7	Dokumentasi tambahan (screenshot topologi GNS3 + output show run terkait) sudah disimpan sebagai bukti pengayaan.	☐ Sudah ☐ Belum

Catatan Guru:

_____

Paraf Guru: _____