BUKU BAHAN AJAR GURU

PERENCANAAN DAN PENGALAMATAN JARINGAN

Kelas XII — Program Keahlian TJKT (Porsi 20%, Pendalaman)

Edisi Khusus: Implementasi Penuh GNS3

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 XII (Porsi 20%, Pendalaman)
Fokus: Seluruh perencanaan dan praktik dikerjakan di GNS3 — tanpa 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 XII Sekolah Menengah Kejuruan. Materi disusun berdasarkan dokumen “Target Pembelajaran Kelas XII” yang memuat 5 target kompetensi (20% dari keseluruhan target, sebagai pendalaman dari 80% target Kelas XI) tersebar pada 4 elemen: perencanaan skema pengalamatan IP lanjutan, perencanaan VLAN dan segmentasi Layer 2 lanjutan, perencanaan redundansi dan ketersediaan tinggi lanjutan, serta perencanaan layanan pendukung jaringan lanjutan.

Berbeda dari buku Kelas XI yang seluruh materinya dapat dituntaskan dengan Cisco Packet Tracer, kelima target pada buku ini — dual-stack IPv6, VPN, distribusi VLAN melalui VTP, redundansi Virtual IP berbasis Keepalived, dan integrasi DNS forward/reverse zone — memerlukan perilaku IOS dan Linux yang presisi dan tidak dapat disederhanakan. Oleh karena itu, buku ini disusun dengan pendekatan berbeda: seluruh perencanaan, konfigurasi, dan verifikasi dikerjakan sepenuhnya di GNS3, tanpa menggunakan Packet Tracer sama sekali. Keputusan ini konsisten dengan hasil analisis kelayakan tools yang mendasari penyusunan buku ini (lihat Bab 1.6).

Studi kasus utama yang dipakai tetap sama dengan Kelas XI, yaitu perusahaan multi-cabang ITNSA.ID Corp, sehingga siswa melanjutkan satu proyek jaringan yang sama alih-alih memulai dari nol. Topologi dasar yang telah dibangun di Kelas XI (pengalamatan IPv4/VLSM, VLAN, routing OSPF, HSRP, DHCP/NAT/NTP) menjadi fondasi yang di atasnya kelima kompetensi lanjutan ini ditambahkan secara bertahap.

Setiap bab disusun dengan struktur konsisten: tujuan pembelajaran, uraian materi dengan contoh perhitungan/skema, praktik/aktivitas di GNS3 lengkap dengan perintah CLI, rangkuman, dan soal latihan/refleksi — memudahkan guru mengelola alokasi waktu dan asesmen di kelas. Semoga buku ini bermanfaat sebagai pegangan guru dalam menyampaikan materi pendalaman Perencanaan dan Pengalamatan Jaringan Kelas XII secara sistematis, aplikatif, dan mempersiapkan siswa menghadapi tantangan jaringan skala nyata maupun kompetisi keahlian.

Penyusun

Daftar Isi

Peta Kompetensi Buku

Tabel berikut memetakan setiap bab pada buku ini terhadap elemen dan target kompetensi pada dokumen Target Pembelajaran Kelas XII, sehingga guru dapat langsung melihat cakupan asesmen per bab.

Bab	Elemen (Kelas XII)	Target Kompetensi	Tools
Bab 2	Persiapan	Environment GNS3 siap dipakai	GNS3
Bab 3	Elemen 2 — Pengalamatan IP Lanjutan	Dual-stack IPv6 berdampingan dengan IPv4	GNS3 (IOS)
Bab 4	Elemen 2 — Pengalamatan IP Lanjutan	Pengalamatan untuk kebutuhan VPN	GNS3 (IOS)
Bab 5	Elemen 3 — VLAN & Segmentasi L2 Lanjutan	Distribusi VLAN via VTP	GNS3 (IOSvL2)
Bab 6	Elemen 5 — Redundansi & HA Lanjutan	Virtual IP / Keepalived pada server	GNS3 (Linux)
Bab 7	Elemen 6 — Layanan Pendukung Lanjutan	Integrasi DNS forward/reverse zone	GNS3 (Linux/BIND9)
Bab 8	Proyek Akhir	Integrasi seluruh target di satu topologi	GNS3

Total: 5 target kompetensi wajib (100% dari target Kelas XII), tersebar pada 4 elemen lanjutan, seluruhnya diverifikasi melalui praktik langsung di GNS3.

BAB 1 — Pendahuluan

1.1 Kedudukan Mata Pelajaran di Kelas XII

Pada Kelas XI, mata pelajaran Perencanaan dan Pengalamatan Jaringan membangun fondasi perencanaan jaringan skala menengah: analisis kebutuhan, pengalamatan IPv4 (VLSM), VLAN, routing, redundansi dasar (EtherChannel/HSRP), dan layanan pendukung dasar (DHCP/NAT/NTP), seluruhnya dikerjakan dengan Cisco Packet Tracer. Pada Kelas XII, mata pelajaran ini memasuki tahap pendalaman: siswa dituntut merancang skema yang lebih kompleks dan mendekati kondisi jaringan produksi sesungguhnya — dual-stack IPv6, konektivitas aman antar-cabang melalui VPN, distribusi konfigurasi VLAN berskala melalui VTP, redundansi tingkat server melalui Keepalived, dan integrasi layanan nama domain melalui DNS forward/reverse zone.

Kedudukan buku ini bersifat lanjutan langsung (extension) dari buku Kelas XI: topologi, skema pengalamatan, dan studi kasus yang sama (ITNSA.ID Corp) tetap dipakai, namun perangkat simulasi berpindah sepenuhnya ke GNS3 karena kelima target kompetensi ini menuntut perilaku sistem operasi (Cisco IOS dan Linux) yang presisi dan tidak dapat disederhanakan oleh simulator ringan.

1.2 Dasar Penyusunan Materi

Materi buku ini disusun berdasarkan dokumen “Target Pembelajaran Kelas XII (Porsi 20%, Pendalaman)”, yang merupakan lanjutan langsung dari dokumen “Target Pembelajaran Kelas XI (Porsi 80%)”. Kelima target pada dokumen tersebut — dual-stack IPv6, pengalamatan VPN, VTP, Keepalived, dan DNS forward/reverse zone — sengaja dipisahkan dari Kelas XI karena masing-masing memerlukan environment yang tidak tersedia atau tidak presisi di Cisco Packet Tracer.

Sebagai dasar keputusan tools, berikut ringkasan kelayakan setiap target apabila dikerjakan di Packet Tracer dibanding GNS3:

Target	Di Packet Tracer	Di GNS3
Dual-stack IPv6	Terbatas: IPv6 dasar & OSPFv3/RIPng tersedia, cukup untuk desain skema alamat saja	Penuh: perilaku IOS asli, seluruh command IPv6 tersedia
Pengalamatan VPN	Sebagian: fitur IPsec/GRE tersedia namun disederhanakan dan tidak selalu konsisten dengan IOS asli	Penuh: crypto isakmp/ipsec/GRE berjalan identik dengan perangkat nyata
VTP	Bisa, relatif matang di switch PT	Penuh, dengan image IOSvL2 identik switch nyata
Keepalived (Virtual IP)	Tidak bisa — server PT tidak memiliki shell/OS nyata	Wajib GNS3 — daemon Linux nyata (VRRP) di node Linux/container
DNS forward/reverse zone	Tidak bisa — DNS Server PT hanya mapping nama↔IP sederhana tanpa zone file	Wajib GNS3 — BIND9 nyata dengan zone file, SOA, dan PTR record

Karena 2 dari 5 target (Keepalived dan DNS zone) sama sekali tidak dapat dikerjakan di Packet Tracer, dan 3 target lainnya hanya dapat dikerjakan secara terbatas atau kurang presisi, buku ini memutuskan untuk konsisten menggunakan satu alat saja pada Kelas XII: GNS3. Pendekatan ini menghindari kebingungan berpindah-pindah tools untuk target yang berbeda, dan sekaligus mempersiapkan siswa pada environment yang lebih dekat dengan praktik jaringan profesional maupun Modul A (Linux Environment) pada LKS.

1.3 Capaian Pembelajaran Umum

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

- Merancang skema pengalamatan IPv6 yang berdampingan (dual-stack) dengan skema IPv4 yang telah dibuat di Kelas XI, tanpa mengubah alokasi IPv4 yang sudah berjalan.
- Merancang skema pengalamatan untuk kebutuhan VPN, termasuk menentukan rentang alamat tunnel yang terpisah dari alamat LAN/WAN produksi.
- Merancang strategi distribusi konfigurasi VLAN antar-switch menggunakan VTP dalam satu domain, lengkap dengan pertimbangan revision number dan mode VTP.
- Merancang skema Virtual IP dengan mekanisme MASTER-BACKUP pada server menggunakan Keepalived, sebagai padanan HSRP pada level server/Linux.
- Merencanakan integrasi layanan DNS forward dan reverse zone sesuai desain alamat dan penamaan domain yang telah dibuat.
- Mengoperasikan GNS3 secara mandiri: instalasi, impor image, membangun topologi, serta melakukan verifikasi konfigurasi menggunakan perintah CLI IOS dan Linux yang sesungguhnya.

1.4 Struktur Buku

Buku ini terdiri atas 9 bab. Bab 1 berisi pendahuluan dan petunjuk penggunaan. Bab 2 membahas persiapan environment GNS3 sebagai prasyarat teknis sebelum masuk ke materi inti. Bab 3 hingga Bab 7 membahas satu target kompetensi per bab, mengikuti urutan pada dokumen Target Kelas XII: pengalamatan IPv6, pengalamatan VPN, VTP, Keepalived, dan DNS forward/reverse zone. Bab 8 merupakan proyek akhir terintegrasi yang menggabungkan seluruh target dalam satu topologi ITNSA.ID Corp lanjutan. Bab 9 berisi penutup.

Setiap bab inti (3–7) memiliki struktur yang konsisten:

- Tujuan Pembelajaran — target kompetensi dan indikator capaian yang dirujuk langsung dari dokumen Target Kelas XII.
- Uraian Materi — konsep, perhitungan, dan skema yang dijelaskan langkah demi langkah, melanjutkan skema Kelas XI.
- Praktik/Aktivitas Pembelajaran — instruksi hands-on di GNS3 beserta perintah CLI IOS/Linux yang sesungguhnya.
- Rangkuman — poin-poin kunci yang wajib dikuasai siswa.
- Soal Latihan/Refleksi — pertanyaan pemantik diskusi dan latihan mandiri.
- Checkpoint — lembar verifikasi ketuntasan praktik sebelum lanjut ke bab berikutnya.

1.5 Petunjuk Penggunaan bagi Guru

- Pastikan Bab 2 (Persiapan Environment GNS3) benar-benar tuntas — termasuk uji ping dua node sederhana — sebelum siswa masuk ke Bab 3, karena seluruh bab berikutnya bergantung pada environment yang sudah berjalan stabil.
- Gunakan file proyek GNS3 (.gns3) yang sama dari Bab 2 hingga Bab 8 sebagai satu proyek berkelanjutan (living project), melanjutkan filosofi yang sama seperti file .pkt pada buku Kelas XI.
- Bila memungkinkan, minta siswa mengekspor topologi Kelas XI (Packet Tracer) ke bentuk dokumentasi (tabel IP, tabel VLAN) terlebih dahulu, lalu membangun ulang secara manual di GNS3 mengikuti tabel padanan pada Bab 2.3 — proses membangun ulang ini sendiri adalah latihan pemahaman topologi yang berharga.
- Alokasikan waktu ekstra pada Bab 6 dan Bab 7 (Keepalived dan DNS) karena keduanya melibatkan konfigurasi berbasis file teks Linux (bukan CLI interaktif seperti IOS) yang biasanya baru pertama kali ditemui siswa.

- Penilaian sebaiknya menimbang dokumen perencanaan (tabel alamat, skema tunnel, rancangan zone) setara atau lebih besar bobotnya dibanding hasil akhir konfigurasi, konsisten dengan filosofi "rencanakan dulu, baru implementasikan" pada buku Kelas XI.
- RAM dan CPU laptop/komputer siswa perlu diperhatikan — GNS3 dengan banyak node aktif (khususnya node Linux) jauh lebih berat dibanding Packet Tracer. Lihat Bab 2.4 dan Lampiran A untuk strategi mitigasi.

1.6 Perbedaan Pendekatan dengan Kelas XI: Mengapa Full GNS3?

Buku Kelas XI secara sadar membatasi diri pada satu alat (Packet Tracer) agar siswa membangun kebiasaan kerja yang rapi sebelum berpindah ke tools yang lebih kompleks. Buku ini melanjutkan filosofi "satu tools yang konsisten" tersebut, namun dengan alat yang berbeda: GNS3 dipilih secara penuh, bukan sebagai lampiran pengayaan opsional seperti pada buku Kelas XI, karena pada Kelas XII kelayakan Packet Tracer justru berbalik — dua dari lima target sama sekali mustahil dikerjakan dengannya (lihat tabel pada Bab 1.2).

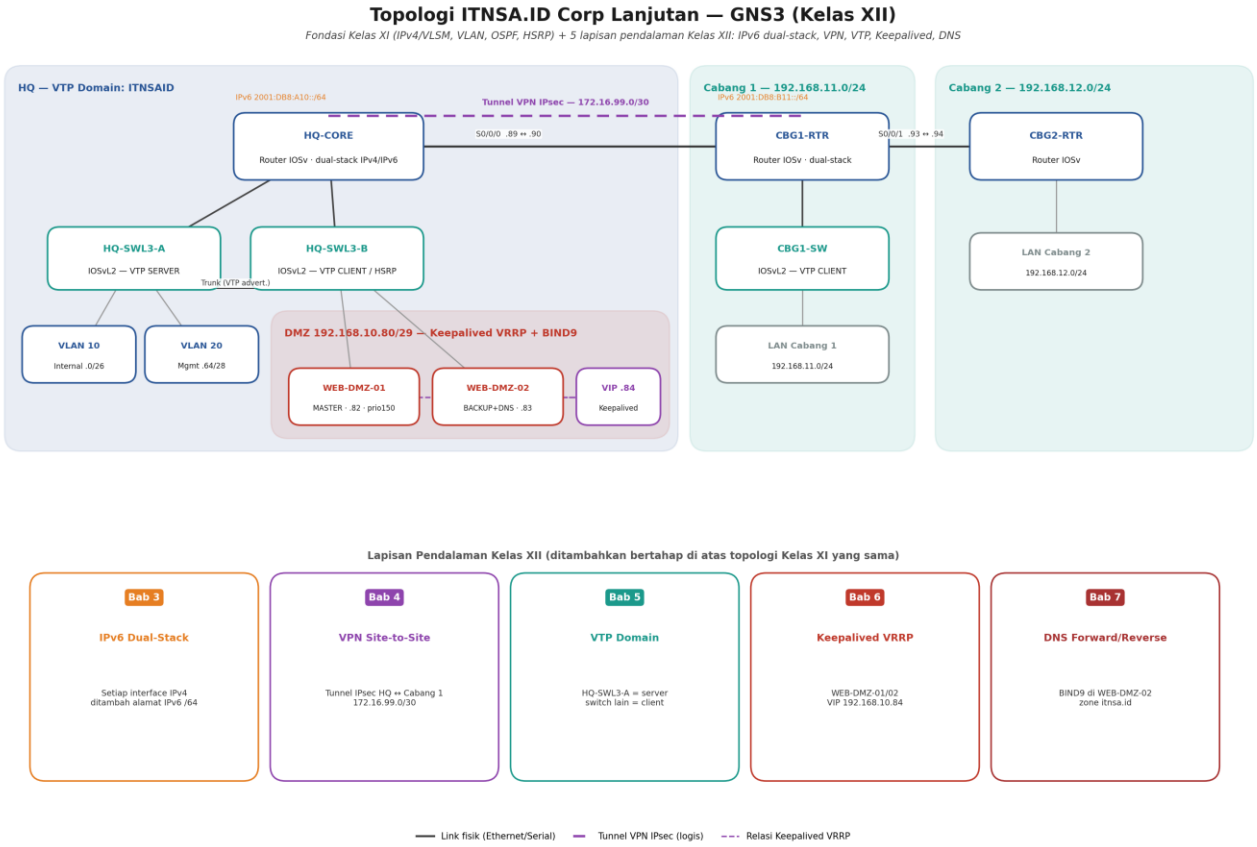
Konsekuensinya, guru tidak perlu lagi menjelaskan dua tools sekaligus pada Kelas XII. Namun perlu diperhatikan bahwa GNS3 menuntut spesifikasi komputer yang lebih tinggi dan proses instalasi awal yang lebih rumit dibanding Packet Tracer — inilah alasan Bab 2 dialokasikan khusus untuk persiapan environment sebelum masuk ke materi inti.

1.7 Topologi Lanjutan Proyek Berkelanjutan (Gambaran Umum)

Topologi yang dipakai pada buku ini adalah kelanjutan langsung dari topologi ITNSA.ID Corp pada Kelas XI (HQ dengan VLAN Internal/Management/DMZ, dua kantor cabang, routing OSPF, HSRP). Tidak ada perubahan pada kerangka topologi maupun skema IPv4 yang sudah ada — kelima target Kelas XII ditambahkan sebagai lapisan baru di atas topologi yang sama, sesuai tabel berikut:

Bab	Yang Ditambahkan ke Topologi ITNSA.ID Corp yang Sama
Bab 2	Topologi Kelas XI dibangun ulang di GNS3 memakai image IOSv/IOSvL2/Linux — skema IPv4 dan VLAN tidak berubah.
Bab 3	Alamat IPv6 ditambahkan berdampingan di setiap interface yang sudah memiliki IPv4 (dual-stack).
Bab 4	Tunnel VPN site-to-site ditambahkan antara HQ dan salah satu cabang, dengan rentang alamat tunnel tersendiri.
Bab 5	VTP domain dikonfigurasi antar switch akses/distribusi — VLAN yang sudah ada didistribusikan otomatis.
Bab 6	Dua node server Linux ditambahkan pada segmen DMZ sebagai pasangan MASTER-BACKUP Keepalived.
Bab 7	Layanan BIND9 ditambahkan pada salah satu node server DMZ, dengan forward dan reverse zone.
Bab 8	Seluruh lapisan di atas diintegrasikan dan diverifikasi sebagai satu topologi utuh — proyek akhir.

Guru disarankan menunjukkan gambaran topologi akhir ini di awal, sama seperti pendekatan pada Bab 1.7 buku Kelas XI, agar siswa memahami bahwa kelima target ini bukan latihan lepas, melainkan penyempurnaan bertahap dari satu proyek jaringan yang sama sejak Kelas XI.



Gambar 1.1 — Topologi ITNSA.ID Corp Lanjutan di GNS3: fondasi Kelas XI (HQ, dua cabang, VLAN, WAN) dengan lima lapisan pendalaman Kelas XII (IPv6 dual-stack, VPN, VTP, Keepalived, DNS) ditandai pada kartu di bagian bawah.

BAB 2 — Persiapan Environment GNS3

Tujuan Pembelajaran

Bab ini bersifat prasyarat teknis: siswa mampu memasang GNS3 Desktop dan GNS3 VM, mengimpor image yang dibutuhkan, serta membangun ulang topologi ITNSA.ID Corp dari Kelas XI di GNS3 dan memverifikasinya dengan uji konektivitas dasar, sebelum masuk ke lima target kompetensi pendalaman pada Bab 3–7.

2.1 Instalasi GNS3 Desktop dan GNS3 VM

GNS3 terdiri atas dua komponen: GNS3 Desktop (aplikasi antarmuka untuk merancang topologi) dan GNS3 VM (mesin virtual tempat node-node benar-benar dijalankan, agar performa tidak membebani sistem operasi utama secara langsung). Langkah instalasi ringkas:

1. Unduh GNS3 Desktop dan GNS3 VM (format OVA untuk VirtualBox/VMware) dari situs resmi GNS3.
2. Pasang GNS3 Desktop seperti aplikasi pada umumnya di sistem operasi guru/siswa.
3. Impor GNS3 VM ke VirtualBox atau VMware, alokasikan RAM minimal 2–4 GB dan 2 vCPU (sesuaikan dengan jumlah node yang akan dijalankan bersamaan).
4. Jalankan GNS3 VM, catat alamat IP yang muncul di layar konsol (mis. 192.168.56.101) untuk dihubungkan dari GNS3 Desktop.
5. Pada GNS3 Desktop, buka menu Edit > Preferences > GNS3 VM, aktifkan “Enable the GNS3 VM” dan pilih virtualization engine yang sesuai, lalu uji koneksi.

Catatan keamanan jaringan: pastikan adapter jaringan pada VirtualBox/VMware diatur ke mode Host-only atau NAT agar traffic node-node lab tidak bocor ke jaringan sekolah yang sesungguhnya.

2.2 Image yang Dibutuhkan

Berbeda dari Packet Tracer yang perangkatnya sudah tersedia bawaan, GNS3 memerlukan image sistem operasi yang diimpor secara terpisah. Berikut kebutuhan image untuk buku ini:

Kebutuhan	Image yang Digunakan	Catatan Lisensi
Router (HQ-CORE, CBG1-RTR, CBG2-RTR)	Cisco IOSv atau IOS-XE (format .qcow2/.bin sesuai platform)	Berlisensi — gunakan hanya image yang diperoleh sekolah secara sah, mis. Cisco Networking Academy/Cisco Learning Network.
Switch akses/distribusi (HQ-SWL3-A/B, CBG-SW)	Cisco IOSvL2 (mendukung VLAN, trunk, EtherChannel, VTP)	Berlisensi, sumber sama seperti di atas.
Server Linux (DMZ, DNS, Keepalived)	Ubuntu Server / Alpine Linux (image ringan)	Open source, dapat diunduh bebas dari situs resmi distro.
Client uji cepat	Node VPCS (bawaan GNS3, tanpa OS penuh)	Bawaan GNS3, tidak perlu image tambahan.

Import image dilakukan melalui menu Edit > Preferences > pilih kategori perangkat (Dynamips/IOS, IOSv, Qemu VMs), lalu New Template dan mengikuti wizard yang meminta lokasi file image.

2.3 Memetakan Ulang Topologi ITNSA.ID Corp dari Kelas XI ke GNS3

Topologi dan skenario ITNSA.ID Corp yang telah dibangun siswa di Packet Tracer pada Kelas XI tidak perlu dirancang ulang dari nol — hanya perangkat simulasinya yang disesuaikan. Gunakan padanan berikut:

Perangkat di Packet Tracer (Kelas XI)	Padanan di GNS3
Router HQ-CORE / router cabang (mis. tipe 1941, 2911)	Image router Cisco IOSv dengan jumlah interface serupa
Switch akses/distribusi (mis. tipe 2960, switch Layer 3)	Image Cisco IOSvL2
PC/laptop client	Node VPCS, atau node Linux ringan bila perlu menguji DNS/DHCP client secara nyata
Server (WEB, DNS, NTP)	Node/VM Linux (Ubuntu/Alpine) dengan servis terkait berjalan sungguhan
Kabel tembaga/serial antar perangkat	Link Ethernet/Serial bawaan GNS3 antar node, mengikuti topologi yang sama

Skema pengalamatan IPv4, VLAN, dan hasil perhitungan VLSM yang sudah disusun di Kelas XI tidak berubah sama sekali — cukup dipindahkan konfigurasinya ke perintah CLI IOS yang sesungguhnya di GNS3. Sebagai pengingat, skema inti yang dipakai sepanjang buku ini:

Segmen	Alokasi	Keterangan
VLAN 10 — Internal (HQ)	192.168.10.0/26	Gateway 192.168.10.1
VLAN 20 — Management (HQ)	192.168.10.64/28	Gateway 192.168.10.65
VLAN 30 — DMZ (HQ)	192.168.10.80/29	Gateway 192.168.10.81
WAN HQ ↔ Cabang 1	192.168.10.88/30	HQ: .89, Cabang 1: .90
WAN HQ ↔ Cabang 2	192.168.10.92/30	HQ: .93, Cabang 2: .94
LAN Cabang 1	192.168.11.0/24	Gateway 192.168.11.1
LAN Cabang 2	192.168.12.0/24	Gateway 192.168.12.1

2.4 Uji Coba Dasar (Sebelum Topologi Penuh Dibangun)

Sebelum membangun ulang topologi ITNSA.ID Corp secara penuh, sangat disarankan menguji dua node sederhana terlebih dahulu untuk memastikan environment GNS3 sudah berjalan stabil:

```
! Pada Router1
Router1(config)# interface g0/0
Router1(config-if)# ip address 10.0.0.1 255.255.255.0
Router1(config-if)# no shutdown

! Pada Router2
Router2(config)# interface g0/0
Router2(config-if)# ip address 10.0.0.2 255.255.255.0
Router2(config-if)# no shutdown

! Uji dari Router1
Router1# ping 10.0.0.2
```

Bila ping berhasil, environment GNS3 sudah siap dan siswa dapat melanjutkan membangun ulang topologi ITNSA.ID Corp secara penuh sesuai padanan perangkat pada Tabel 2.3.

Praktik/Aktivitas Pembelajaran

Ceklis Praktik — Persiapan Environment GNS3 (Bab 2)

No	Langkah Praktik yang Harus Dilakukan Siswa	Ceklis
1	Unduh dan pasang GNS3 Desktop.	☐ Selesai
2	Impor GNS3 VM ke VirtualBox/VMware, alokasikan RAM dan vCPU sesuai kebutuhan.	☐ Selesai
3	Nyalakan GNS3 VM dan hubungkan dari GNS3 Desktop (Edit > Preferences > GNS3 VM).	☐ Selesai
4	Impor image router (IOSv), switch (IOSvL2), dan Linux sesuai Tabel 2.2.	☐ Selesai
5	Bangun topologi 2 node sederhana dan uji ping antar-node.	☐ Selesai
6	Bangun ulang kerangka topologi ITNSA.ID Corp (perangkat dan zona INT/DMZ/Management/WAN).	☐ Selesai
7	Isi ulang alamat IPv4 dan VLAN dari tabel Kelas XI ke perangkat GNS3.	☐ Selesai
8	Verifikasi dengan show ip interface brief dan show vlan brief pada seluruh perangkat.	☐ Selesai

6. Pasang GNS3 Desktop dan GNS3 VM, lakukan uji koneksi antara keduanya.
7. Impor image router (IOSv), switch (IOSvL2), dan Linux sesuai Tabel 2.2.
8. Bangun topologi 2 node sederhana dan uji ping sesuai contoh di atas.
9. Bangun ulang kerangka topologi ITNSA.ID Corp (perangkat dan zona INT/DMZ/Management/WAN) sesuai hasil Kelas XI, lalu isi ulang alamat IPv4 dan VLAN dari tabel yang sudah ada.
10. Verifikasi dengan show ip interface brief dan show vlan brief pada seluruh perangkat, bandingkan hasilnya dengan dokumentasi Kelas XI.

Rangkuman

- GNS3 terdiri atas GNS3 Desktop dan GNS3 VM, dan memerlukan image OS yang diimpor terpisah — tidak seperti Packet Tracer yang perangkatnya sudah tersedia bawaan.
- Topologi dan skema pengalamatan ITNSA.ID Corp dari Kelas XI tidak berubah; hanya perangkat simulasinya yang dipetakan ulang ke image GNS3 (IOSv, IOSvL2, Linux).
- Uji coba dua node sederhana sebaiknya dilakukan lebih dulu sebelum membangun topologi penuh, untuk memastikan environment sudah stabil.

Soal Latihan/Refleksi

11. Jelaskan perbedaan peran GNS3 Desktop dan GNS3 VM.
12. Mengapa image Cisco IOS tidak boleh diunduh dari sumber tidak resmi?
13. Sebutkan tiga kemungkinan penyebab jika sebuah node di GNS3 tidak mau menyala.

Checkpoint Bab 2 — Persiapan Environment GNS3

No	Item Verifikasi	Status
1	GNS3 Desktop dan GNS3 VM sudah terpasang dan status GNS3 VM “running” (hijau).	☐ Sudah ☐ Belum
2	Image router (IOSv), switch (IOSvL2), dan Linux sudah berhasil diimpor.	☐ Sudah ☐ Belum

No	Item Verifikasi	Status
3	Uji ping 2 node sederhana berhasil.	☐ Sudah ☐ Belum
4	Topologi ITNSA.ID Corp sudah dibangun ulang di GNS3 sesuai padanan perangkat pada Tabel 2.3, dengan alamat IPv4 dan VLAN yang identik dengan hasil Kelas XI.	☐ Sudah ☐ Belum

BAB 3 — Perencanaan Pengalamatan IPv6 Dual-Stack

Tujuan Pembelajaran

Elemen 2: Perencanaan Skema Pengalamatan IP (Lanjutan) — mengacu pada dokumen Target Pembelajaran Kelas XII.

No	Target Kompetensi	Indikator Capaian
1	Merencanakan pengalamatan IPv6 berdampingan dengan IPv4 (dual-stack)	Siswa mampu menyertakan alokasi IPv6 pada perencanaan pengalamatan bersamaan dengan IPv4

3.1 Konsep Dual-Stack IPv4/IPv6

Dual-stack adalah pendekatan di mana sebuah perangkat jaringan menjalankan IPv4 dan IPv6 secara bersamaan pada interface yang sama, tanpa salah satu menggantikan yang lain. Pendekatan ini dipilih pada ITNSA.ID Corp karena bersifat paling aman untuk migrasi bertahap: seluruh layanan dan skema IPv4 yang sudah berjalan sejak Kelas XI tetap berfungsi seperti biasa, sementara IPv6 ditambahkan sebagai lapisan paralel yang dapat diuji dan disempurnakan tanpa risiko mengganggu produksi.

Pada Cisco IOS, dual-stack diaktifkan dengan mengaktifkan proses routing IPv6 secara global (ipv6 unicast-routing), kemudian menambahkan alamat IPv6 pada interface yang sudah memiliki alamat IPv4, menggunakan perintah ipv6 address yang berdiri sendiri di samping ip address yang sudah ada.

3.2 Skema Pengalamatan IPv6 untuk ITNSA.ID Corp

Untuk memudahkan siswa mengingat pemetaan antara segmen IPv4 dan IPv6-nya, buku ini menggunakan konvensi penamaan prefix IPv6 yang mencerminkan nomor VLAN/segmen IPv4 terkait. Setiap segmen mendapat prefix /64 sesuai praktik umum alokasi IPv6 per subnet:

Segmen	Alokasi IPv4 (Kelas XI)	Alokasi IPv6 (Baru, Kelas XII)
VLAN 10 — Internal (HQ)	192.168.10.0/26	2001:DB8:A10::/64
VLAN 20 — Management (HQ)	192.168.10.64/28	2001:DB8:A20::/64
VLAN 30 — DMZ (HQ)	192.168.10.80/29	2001:DB8:A30::/64
WAN HQ ↔ Cabang 1	192.168.10.88/30	2001:DB8:10::/64
WAN HQ ↔ Cabang 2	192.168.10.92/30	2001:DB8:20::/64
LAN Cabang 1	192.168.11.0/24	2001:DB8:B11::/64
LAN Cabang 2	192.168.12.0/24	2001:DB8:B12::/64

Prinsip penomoran: dua digit terakhir prefix mengikuti oktet ketiga alamat IPv4 (mis. VLAN Internal HQ = 192.168.10.x → prefix 2001:DB8:A10::/64), sehingga guru dan siswa dapat langsung mengenali pasangan IPv4-IPv6 sebuah segmen tanpa membuka tabel referensi terpisah. Konvensi seperti ini umum dipakai di lapangan agar dokumentasi dual-stack tetap mudah dibaca.

3.3 Tabel Pengalamatan Dual-Stack Lengkap

Melanjutkan tabel pengalamatan IPv4 pada Bab 3 buku Kelas XI, berikut tabel dual-stack lengkap yang ditambahkan untuk interface router utama:

Perangkat	Interface	IPv4	IPv6
HQ-CORE	G0/0 (Internal)	192.168.10.1/26	2001:DB8:A10::1/64
HQ-CORE	G0/1 (Management)	192.168.10.65/28	2001:DB8:A20::1/64
HQ-CORE	G0/2 (DMZ)	192.168.10.81/29	2001:DB8:A30::1/64
HQ-CORE	S0/0/0 (WAN ke Cabang 1)	192.168.10.89/30	2001:DB8:10::1/64
CBG1-RTR	S0/0/0 (WAN ke HQ)	192.168.10.90/30	2001:DB8:10::2/64
CBG1-RTR	G0/0 (LAN Cabang 1)	192.168.11.1/24	2001:DB8:B11::1/64

Praktik/Aktivitas Pembelajaran

Ceklis Praktik — IPv6 Dual-Stack (Bab 3)

No	Langkah Praktik yang Harus Dilakukan Siswa	Ceklis
1	Aktifkan ipv6 unicast-routing pada HQ-CORE dan CBG1-RTR.	☐ Selesai
2	Tambahkan alamat ipv6 address pada interface yang sudah memiliki IPv4 sesuai Tabel 3.3, tanpa menghapus konfigurasi IPv4.	☐ Selesai
3	Aktifkan ipv6 ospf 1 area 0 pada interface yang sama di kedua router.	☐ Selesai
4	Jalankan show ipv6 interface brief dan pastikan status up/up.	☐ Selesai
5	Uji ping ipv6 dari HQ-CORE ke CBG1-RTR.	☐ Selesai
6	Jalankan show ipv6 ospf neighbor dan pastikan neighbor sudah terbentuk.	☐ Selesai

Aktivitas GNS3 — IPv6 Dual-Stack pada Router Edge (± 30 menit): pada HQ-CORE dan CBG1-RTR, aktifkan routing IPv6 lalu tambahkan alamat IPv6 pada interface yang sudah memiliki IPv4, tanpa menghapus konfigurasi IPv4 yang sudah ada.

```
! Pada HQ-CORE
HQ-CORE(config)# ipv6 unicast-routing
HQ-CORE(config)# interface g0/0
HQ-CORE(config-if)# ipv6 address 2001:DB8:A10::1/64
HQ-CORE(config-if)# exit
HQ-CORE(config)# interface s0/0/0
HQ-CORE(config-if)# ipv6 address 2001:DB8:10::1/64
HQ-CORE(config-if)# exit

! Pada CBG1-RTR
CBG1-RTR(config)# ipv6 unicast-routing
CBG1-RTR(config)# interface s0/0/0
CBG1-RTR(config-if)# ipv6 address 2001:DB8:10::2/64
CBG1-RTR(config-if)# exit
CBG1-RTR(config)# interface g0/0
CBG1-RTR(config-if)# ipv6 address 2001:DB8:B11::1/64

! Verifikasi
```

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

Untuk routing antar-segmen IPv6, tambahkan OSPFv3 sebagai padanan OSPF yang sudah dikonfigurasi untuk IPv4 di Kelas XI:

```
HQ-CORE(config)# interface g0/0
HQ-CORE(config-if)# ipv6 ospf 1 area 0
HQ-CORE(config-if)# exit
HQ-CORE(config)# interface s0/0/0
HQ-CORE(config-if)# ipv6 ospf 1 area 0

CBG1-RTR(config)# interface s0/0/0
CBG1-RTR(config-if)# ipv6 ospf 1 area 0
CBG1-RTR(config)# interface g0/0
CBG1-RTR(config-if)# ipv6 ospf 1 area 0

HQ-CORE# show ipv6 ospf neighbor
```

Rangkuman

- Dual-stack menjalankan IPv4 dan IPv6 bersamaan pada interface yang sama, tanpa mengubah konfigurasi IPv4 yang sudah ada.
- Setiap segmen IPv4 pada ITNSA.ID Corp dipetakan ke satu prefix IPv6 /64 dengan konvensi penomoran yang mengikuti oktet ketiga IPv4-nya.
- OSPFv3 digunakan sebagai padanan OSPF untuk routing dinamis antar-segmen IPv6.

Soal Latihan/Refleksi

14. Mengapa dual-stack dianggap pendekatan migrasi yang lebih aman dibanding langsung berpindah penuh ke IPv6?
15. Tentukan alamat IPv6 yang konsisten dengan konvensi Tabel 3.2 untuk segmen WAN HQ ↔ Cabang 2 (IPv4: 192.168.10.92/30).
16. Perintah apa yang digunakan untuk memverifikasi bahwa OSPFv3 sudah membentuk hubungan tetangga (neighbor) antar router?

Checkpoint Bab 3 — Pengalamatan IPv6 Dual-Stack

No	Item Verifikasi	Status
1	ipv6 unicast-routing sudah diaktifkan pada seluruh router.	☐ Sudah ☐ Belum
2	Alamat IPv6 sudah ditambahkan berdampingan dengan IPv4 pada interface sesuai Tabel 3.3, tanpa mengubah IPv4 yang sudah ada.	☐ Sudah ☐ Belum
3	show ipv6 interface brief menunjukkan status up/up pada interface yang direncanakan.	☐ Sudah ☐ Belum
4	ping ipv6 antar segmen berhasil, dan OSPFv3 sudah membentuk neighbor (bila dikonfigurasi).	☐ Sudah ☐ Belum

BAB 4 — Perencanaan Pengalamatan untuk VPN

Tujuan Pembelajaran

Elemen 2: Perencanaan Skema Pengalamatan IP (Lanjutan) — mengacu pada dokumen Target Pembelajaran Kelas XII.

No	Target Kompetensi	Indikator Capaian
1	Merencanakan pengalamatan untuk kebutuhan VPN	Siswa mampu merancang skema pengalamatan pada tunnel VPN (mis. rentang khusus terpisah dari LAN/WAN) untuk client remote

4.1 Konsep VPN Site-to-Site dan Remote Access

VPN (Virtual Private Network) membangun jalur komunikasi terenkripsi di atas jaringan publik yang tidak dipercaya (mis. internet), sehingga dua lokasi atau sebuah client remote dapat saling terhubung seolah berada pada satu jaringan privat. Terdapat dua model utama yang relevan untuk ITNSA.ID Corp:

- Site-to-site VPN — menghubungkan dua kantor secara permanen (mis. HQ dengan Cabang 1) melalui tunnel terenkripsi, biasanya menggunakan IPsec di atas internet sebagai pengganti atau pelengkap link WAN privat.
- Remote access VPN — menghubungkan client individu (mis. karyawan yang bekerja dari luar kantor) ke jaringan HQ melalui tunnel terenkripsi yang dibentuk sesuai kebutuhan (on-demand).

Buku ini berfokus pada site-to-site VPN antara HQ dan Cabang 1 menggunakan IPsec, karena skenario ini paling relevan dengan topologi multi-cabang ITNSA.ID Corp yang sudah dibangun sejak Kelas XI, dan merupakan kasus yang paling sering diujikan pada kompetisi keahlian jaringan.

4.2 Prinsip Perencanaan Alamat Tunnel

Prinsip utama perencanaan pengalamatan VPN adalah memisahkan rentang alamat tunnel dari alamat LAN/WAN produksi yang sudah ada, agar tidak terjadi tumpang tindih (overlap) dan agar trafik tunnel mudah dikenali serta difilter melalui access-list bila diperlukan. Rentang khusus ini idealnya dialokasikan dari blok privat yang belum dipakai di skema ITNSA.ID Corp manapun.

Karena skema IPv4 ITNSA.ID Corp sejauh ini memakai blok 192.168.10.0/24 (HQ), 192.168.11.0/24 (Cabang 1), dan 192.168.12.0/24 (Cabang 2), buku ini mengalokasikan blok baru 172.16.99.0/30 khusus untuk alamat ujung tunnel (tunnel endpoint) antara HQ dan Cabang 1, agar terpisah tegas dari ketiga blok tersebut.

4.3 Perhitungan dan Tabel Alamat Tunnel

Parameter	Nilai
Blok alamat tunnel	172.16.99.0/30
Tunnel interface HQ-CORE	172.16.99.1/30
Tunnel interface CBG1-RTR	172.16.99.2/30
Trafik yang dienkripsi (interesting traffic)	192.168.10.0/26 (VLAN Internal HQ) ↔ 192.168.11.0/24 (LAN Cabang 1)
Alamat publik ujung tunnel (peer)	Alamat interface WAN yang sudah ada: 192.168.10.89 (HQ) ↔ 192.168.10.90 (Cabang 1)

Perhatikan bahwa alamat peer VPN memanfaatkan alamat WAN yang sudah direncanakan sejak Kelas XI (Bab 3, tabel WAN point-to-point) — pengalamatan VPN tidak menciptakan kebutuhan alamat WAN baru, hanya menambahkan lapisan tunnel logis di atasnya.

Praktik/Aktivitas Pembelajaran

Ceklis Praktik — VPN Site-to-Site (Bab 4)

No	Langkah Praktik yang Harus Dilakukan Siswa	Ceklis
1	Konfigurasi crypto isakmp policy (encryption, authentication, group) di HQ-CORE dan CBG1-RTR.	☐ Selesai
2	Tetapkan crypto isakmp key yang identik di kedua router, mengarah ke IP peer yang benar.	☐ Selesai
3	Buat crypto ipsec transform-set yang sama di kedua sisi.	☐ Selesai
4	Buat access-list interesting traffic yang saling mencerminkan (source/destination dibalik).	☐ Selesai
5	Buat crypto map dan terapkan pada interface WAN (S0/0/0) di kedua router.	☐ Selesai
6	Jalankan show crypto isakmp sa dan show crypto ipsec sa, pastikan security association aktif.	☐ Selesai
7	Uji traceroute dari LAN Internal HQ ke LAN Cabang 1 dan pastikan trafik melewati tunnel.	☐ Selesai

Aktivitas GNS3 — VPN Site-to-Site (IPsec) antar Cabang (± 40 menit): konfigurasikan tunnel IPsec site-to-site antara HQ-CORE dan CBG1-RTR menggunakan crypto isakmp dan crypto ipsec, lalu uji trafik yang melewati tunnel.

```
! === Pada HQ-CORE ===
! Tahap 1 - ISAKMP (IKE Phase 1)
HQ-CORE(config)# crypto isakmp policy 10
HQ-CORE(config-isakmp)# encryption aes 256
HQ-CORE(config-isakmp)# authentication pre-share
HQ-CORE(config-isakmp)# group 14
HQ-CORE(config-isakmp)# exit
HQ-CORE(config)# crypto isakmp key ITNSA@VPN2026 address 192.168.10.90

! Tahap 2 - IPsec Transform Set (IKE Phase 2)
HQ-CORE(config)# crypto ipsec transform-set ITNSA-TS esp-aes esp-sha-hmac

! Access-list untuk trafik yang dienkripsi
HQ-CORE(config)# access-list 101 permit ip 192.168.10.0 0.0.0.63 192.168.11.0 0.0.0.255

! Crypto map
HQ-CORE(config)# crypto map ITNSA-MAP 10 ipsec-isakmp
HQ-CORE(config-crypto-map)# set peer 192.168.10.90
HQ-CORE(config-crypto-map)# set transform-set ITNSA-TS
HQ-CORE(config-crypto-map)# match address 101
HQ-CORE(config-crypto-map)# exit
HQ-CORE(config)# interface s0/0/0
HQ-CORE(config-if)# crypto map ITNSA-MAP
```

```
! === Pada CBG1-RTR (konfigurasi cerminan) ===
```

```
CBG1-RTR(config)# crypto isakmp policy 10
CBG1-RTR(config-isakmp)# encryption aes 256
CBG1-RTR(config-isakmp)# authentication pre-share
CBG1-RTR(config-isakmp)# group 14
CBG1-RTR(config-isakmp)# exit
CBG1-RTR(config)# crypto isakmp key ITNSA@VPN2026 address 192.168.10.89

CBG1-RTR(config)# crypto ipsec transform-set ITNSA-TS esp-aes esp-sha-hmac
CBG1-RTR(config)# access-list 101 permit ip 192.168.11.0 0.0.0.255 192.168.10.0 0.0.0.63

CBG1-RTR(config)# crypto map ITNSA-MAP 10 ipsec-isakmp
CBG1-RTR(config-crypto-map)# set peer 192.168.10.89
CBG1-RTR(config-crypto-map)# set transform-set ITNSA-TS
CBG1-RTR(config-crypto-map)# match address 101
CBG1-RTR(config-crypto-map)# exit
CBG1-RTR(config)# interface s0/0/0
CBG1-RTR(config-if)# crypto map ITNSA-MAP

! Verifikasi dari kedua sisi
HQ-CORE# show crypto isakmp sa
HQ-CORE# show crypto ipsec sa
HQ-CORE# traceroute 192.168.11.11
```

Catatan guru: pastikan interesting traffic (access-list 101) benar-benar mencerminkan satu sama lain di kedua sisi (source dan destination dibalik), karena kesalahan umum siswa pemula adalah menyalin access-list yang sama persis tanpa membalik urutannya.

Rangkuman

- Site-to-site VPN menghubungkan dua kantor secara permanen melalui tunnel terenkripsi di atas jaringan publik/WAN yang sudah ada.
- Alamat tunnel VPN sebaiknya dialokasikan dari blok terpisah agar tidak tumpang tindih dengan alamat LAN/WAN produksi.
- Konfigurasi IPsec terdiri atas ISAKMP (IKE Phase 1), transform set (IKE Phase 2), access-list interesting traffic, dan crypto map yang diterapkan pada interface WAN.

Soal Latihan/Refleksi

17. Mengapa alamat tunnel VPN sebaiknya tidak menggunakan blok yang sama dengan LAN produksi?
18. Jelaskan perbedaan peran access-list interesting traffic di sisi HQ dibanding di sisi Cabang 1.
19. Perintah apa yang digunakan untuk memverifikasi bahwa security association (SA) IPsec sudah terbentuk?

Checkpoint Bab 4 — Pengalamatan VPN

No	Item Verifikasi	Status
1	Blok alamat tunnel sudah dialokasikan terpisah dari LAN/WAN produksi.	☐ Sudah ☐ Belum
2	crypto isakmp dan crypto ipsec sudah dikonfigurasi cerminan di kedua router (HQ-CORE dan CBG1-RTR).	☐ Sudah ☐ Belum
3	show crypto isakmp sa dan show crypto ipsec sa menunjukkan security association aktif.	☐ Sudah ☐ Belum
4	traceroute dari LAN Internal HQ ke LAN Cabang 1 menunjukkan trafik melewati tunnel VPN.	☐ Sudah ☐ Belum

BAB 5 — Perencanaan Distribusi VLAN dengan VTP

Tujuan Pembelajaran

Elemen 3: Perencanaan VLAN dan Segmentasi Layer 2 (Lanjutan) — mengacu pada dokumen Target Pembelajaran Kelas XII.

No	Target Kompetensi	Indikator Capaian
1	Merencanakan strategi distribusi VLAN (VTP)	Siswa mampu merancang skema distribusi konfigurasi VLAN dari switch pusat (server) ke switch lain (client) dalam satu domain

5.1 Konsep VTP: Server, Client, dan Transparent

VTP (VLAN Trunking Protocol) memungkinkan konfigurasi VLAN dibuat satu kali pada satu switch, lalu didistribusikan otomatis ke seluruh switch lain dalam satu domain VTP yang sama melalui link trunk, tanpa perlu mengetik ulang perintah vlan di setiap switch. Terdapat tiga mode VTP:

- Server — dapat membuat, mengubah, dan menghapus VLAN; perubahan disebarkan ke seluruh switch lain dalam domain. Mode ini adalah default pabrik pada sebagian besar switch Cisco.
- Client — menerima dan menerapkan VLAN yang disebarkan oleh server, tetapi tidak dapat membuat VLAN secara lokal.
- Transparent — tidak berpartisipasi dalam distribusi VTP; dapat membuat VLAN lokal sendiri, dan hanya meneruskan (forward) advertisement VTP yang lewat tanpa memprosesnya.

Elemen kunci lain yang wajib dipahami siswa adalah configuration revision number: setiap kali VTP server membuat perubahan VLAN, angka ini bertambah satu. Switch yang bergabung ke domain akan menerima konfigurasi manapun yang memiliki revision number lebih tinggi — termasuk dari switch client/server “asing” yang baru dipasang. Kesalahan umum di lapangan adalah memasang switch bekas dengan revision number tinggi namun VLAN yang salah, sehingga tanpa sengaja menghapus seluruh VLAN yang benar di domain produksi.

5.2 Perencanaan Domain VTP untuk ITNSA.ID Corp

Pada topologi ITNSA.ID Corp, HQ-SWL3-A ditetapkan sebagai VTP server karena merupakan switch distribusi pusat tempat VLAN 10/20/30 pertama kali dibuat pada Kelas XI. HQ-SWL3-B dan switch cabang ditetapkan sebagai VTP client, sehingga VLAN yang sama otomatis tersedia tanpa dikonfigurasi manual satu per satu.

Switch	Mode VTP	Peran
HQ-SWL3-A	Server	Sumber tunggal pembuatan/perubahan VLAN 10, 20, 30
HQ-SWL3-B	Client	Menerima VLAN dari HQ-SWL3-A, berpasangan HSRP dengannya
CBG1-SW	Client	Menerima VLAN yang relevan untuk LAN Cabang 1

Parameter VTP	Nilai yang Direncanakan
Domain VTP	ITNSAID
Password domain	Vtp@ITNSA2026
Versi VTP	2 (kompatibilitas luas pada IOSvL2)

Parameter VTP	Nilai yang Direncanakan
Pruning	Dinonaktifkan pada tahap awal (diaktifkan bila trafik trunk perlu dioptimalkan)

Praktik/Aktivitas Pembelajaran

Ceklis Praktik — Distribusi VLAN dengan VTP (Bab 5)

No	Langkah Praktik yang Harus Dilakukan Siswa	Ceklis
1	Tetapkan HQ-SWL3-A sebagai vtp mode server.	☐ Selesai
2	Tetapkan HQ-SWL3-B dan CBG1-SW sebagai vtp mode client.	☐ Selesai
3	Samakan vtp domain dan vtp password di seluruh switch dalam domain.	☐ Selesai
4	Samakan vtp version di seluruh switch (versi 2).	☐ Selesai
5	Pastikan link antar-switch sudah switchport mode trunk.	☐ Selesai
6	Buat VLAN baru hanya di HQ-SWL3-A, lalu verifikasi VLAN otomatis muncul di switch client (show vlan brief).	☐ Selesai
7	Bandingkan configuration revision number di seluruh switch melalui show vtp status.	☐ Selesai

Aktivitas GNS3 — VTP untuk Sinkronisasi VLAN antar Switch (± 20 menit): jadikan HQ-SWL3-A sebagai VTP server dan HQ-SWL3-B/CBG1-SW sebagai VTP client dalam domain yang sama, lalu buktikan VLAN baru yang dibuat di server otomatis muncul di client.

```
! === Pada HQ-SWL3-A (VTP Server) ===
HQ-SWL3-A(config)# vtp domain ITNSAID
HQ-SWL3-A(config)# vtp password Vtp@ITNSA2026
HQ-SWL3-A(config)# vtp version 2
HQ-SWL3-A(config)# vtp mode server

! Pastikan trunk ke switch lain sudah aktif
HQ-SWL3-A(config)# interface g0/1
HQ-SWL3-A(config-if)# switchport mode trunk

! === Pada HQ-SWL3-B dan CBG1-SW (VTP Client) ===
HQ-SWL3-B(config)# vtp domain ITNSAID
HQ-SWL3-B(config)# vtp password Vtp@ITNSA2026
HQ-SWL3-B(config)# vtp version 2
HQ-SWL3-B(config)# vtp mode client
HQ-SWL3-B(config)# interface g0/1
HQ-SWL3-B(config-if)# switchport mode trunk
```

```
! Uji: buat VLAN baru HANYA di HQ-SWL3-A (server)
HQ-SWL3-A(config)# vlan 40
HQ-SWL3-A(config-vlan)# name VLAN_GUEST
HQ-SWL3-A(config-vlan)# exit

! Verifikasi di HQ-SWL3-B - VLAN 40 harus sudah muncul TANPA dikonfigurasi manual
HQ-SWL3-B# show vlan brief
HQ-SWL3-B# show vtp status
```

```
! Bandingkan configuration revision number di kedua switch - harus sama
HQ-SWL3-A# show vtp status
```

Diskusikan dengan siswa: apa yang terjadi bila sebuah switch client dengan revision number lebih tinggi namun VLAN yang salah dipasang ke domain ini? Ini adalah skenario risiko nyata yang wajib dipahami sebelum siswa bekerja di jaringan produksi.

Rangkuman

- VTP mendistribusikan konfigurasi VLAN dari satu switch server ke switch client lain dalam satu domain, tanpa perlu konfigurasi manual berulang.
- Configuration revision number menentukan konfigurasi VLAN mana yang dianggap paling baru dan akan diterapkan oleh switch lain — nilai yang tidak dipahami dengan baik dapat berisiko menghapus VLAN produksi.
- Pada ITNSA.ID Corp, HQ-SWL3-A berperan sebagai VTP server, sementara HQ-SWL3-B dan switch cabang berperan sebagai VTP client.

Soal Latihan/Refleksi

20. Jelaskan risiko yang dapat terjadi bila sebuah switch bekas dengan revision number tinggi dipasang ke domain VTP produksi.
21. Kapan sebuah switch sebaiknya diatur ke mode VTP transparent, bukan server atau client?
22. Perintah apa yang digunakan untuk memverifikasi mode dan domain VTP sebuah switch?

Checkpoint Bab 5 — Distribusi VLAN dengan VTP

No	Item Verifikasi	Status
1	Domain, password, dan versi VTP sudah dikonfigurasi identik di seluruh switch dalam domain.	☐ Sudah ☐ Belum
2	HQ-SWL3-A berperan sebagai VTP server, switch lain berperan sebagai VTP client.	☐ Sudah ☐ Belum
3	VLAN baru yang dibuat di server terbukti otomatis muncul di client tanpa konfigurasi manual (show vlan brief).	☐ Sudah ☐ Belum
4	show vtp status menunjukkan configuration revision number yang sama di seluruh switch dalam domain.	☐ Sudah ☐ Belum

BAB 6 — Perencanaan Redundansi Virtual IP dengan Keepalived

Tujuan Pembelajaran

Elemen 5: Perencanaan Redundansi dan Ketersediaan Tinggi (Lanjutan) — mengacu pada dokumen Target Pembelajaran Kelas XII.

No	Target Kompetensi	Indikator Capaian
1	Merencanakan redundansi pada layer server (Virtual IP/Keepalived)	Siswa mampu merancang skema virtual IP dengan mekanisme MASTER-BACKUP pada server agar layanan tetap tersedia saat salah satu server gagal

6.1 Keepalived dan VRRP: Padanan HSRP pada Level Server

Pada Kelas XI, redundansi gateway di level jaringan (Layer 3) sudah dipelajari melalui HSRP (Bab 6 buku Kelas XI): dua switch/router berbagi satu virtual IP, salah satunya berperan Active dan yang lain Standby. Keepalived membawa konsep yang sama ke level server: dua server Linux berbagi satu virtual IP, salah satunya berperan MASTER dan yang lain BACKUP, menggunakan protokol VRRP (Virtual Router Redundancy Protocol) sebagai mekanisme di baliknya.

Perbedaan utama dengan HSRP bukan pada konsepnya — keduanya sama-sama redundansi berbasis virtual IP dan priority — melainkan pada platform: HSRP adalah fitur bawaan Cisco IOS, sementara Keepalived adalah daemon (layanan latar belakang) yang berjalan di sistem operasi Linux dan dikonfigurasi melalui file teks, bukan CLI interaktif.

6.2 Perencanaan Skema Virtual IP MASTER-BACKUP untuk Server

Pada ITNSA.ID Corp, dua server web ditempatkan pada segmen DMZ untuk menyediakan layanan yang sama (redundan). Kedua server berbagi satu virtual IP yang akan diiklankan sebagai IP layanan utama; hanya node MASTER yang secara aktif menjawab pada IP tersebut hingga terjadi kegagalan.

Peran	Node	IP Fisik (DMZ)	Priority	Status Normal
MASTER	WEB-DMZ-01	192.168.10.82/29	150	Aktif melayani Virtual IP
BACKUP	WEB-DMZ-02	192.168.10.83/29	100 (default)	Siaga, mengambil alih bila MASTER gagal
Virtual IP (layanan)	—	192.168.10.84/29	—	Diiklankan oleh node yang sedang MASTER

Perhatikan bahwa alamat fisik kedua node dan virtual IP dialokasikan dari blok DMZ yang sama (192.168.10.80/29) yang sudah direncanakan sejak Kelas XI — Keepalived tidak menciptakan kebutuhan subnet baru, hanya menambahkan satu alamat virtual di dalam subnet yang sudah ada.

Praktik/Aktivitas Pembelajaran

Ceklis Praktik — Keepalived (VRRP) pada Server Linux (Bab 6)

No	Langkah Praktik yang Harus Dilakukan Siswa	Ceklis
1	Pasang paket keepalived pada kedua node Linux DMZ (WEB-DMZ-01 dan WEB-DMZ-02).	☐ Selesai
2	Isi /etc/keepalived/keepalived.conf pada WEB-DMZ-01 dengan state MASTER dan priority 150.	☐ Selesai
3	Isi /etc/keepalived/keepalived.conf pada WEB-DMZ-02 dengan state BACKUP dan priority 100.	☐ Selesai
4	Samakan virtual_router_id dan auth_pass di kedua node.	☐ Selesai
5	Jalankan systemctl restart keepalived pada kedua node, lalu periksa systemctl status keepalived.	☐ Selesai
6	Verifikasi virtual IP 192.168.10.84 aktif di node MASTER melalui ip addr show eth0.	☐ Selesai
7	Uji failover: matikan systemctl stop keepalived di MASTER, amati virtual IP berpindah ke BACKUP.	☐ Selesai

Aktivitas GNS3 — Keepalived (VRRP) pada Server Linux (± 30 menit): pasang dan konfigurasikan Keepalived pada dua node Linux sebagai gateway/layanan redundan, lalu matikan node MASTER dan amati proses failover ke node BACKUP.

```
! Pasang Keepalived pada kedua node Linux
apt-get update && apt-get install -y keepalived

! === Konfigurasi pada WEB-DMZ-01 (MASTER) ===
! Isi /etc/keepalived/keepalived.conf

vrrp_instance VI_DMZ {
    state MASTER
    interface eth0
    virtual_router_id 30
    priority 150
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass itnsa30
    }
    virtual_ipaddress {
        192.168.10.84/29
    }
}
```

```
! === Konfigurasi pada WEB-DMZ-02 (BACKUP) ===
! Isi /etc/keepalived/keepalived.conf

vrrp_instance VI_DMZ {
    state BACKUP
    interface eth0
    virtual_router_id 30
    priority 100
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass itnsa30
```

```
    }
    virtual_ipaddress {
        192.168.10.84/29
    }
}

! Jalankan servis di kedua node
systemctl restart keepalived
systemctl status keepalived
```

```
! Verifikasi virtual IP aktif di node MASTER
ip addr show eth0

! Uji failover: matikan servis keepalived di node MASTER
systemctl stop keepalived

! Amati di node BACKUP: virtual IP berpindah otomatis
! dalam hitungan detik (sesuai advert_int)
ip addr show eth0
```

Catatan guru: konsepnya identik dengan HSRP pada Kelas XI — virtual IP, nilai priority, dan failover otomatis — hanya berbeda platform (Cisco IOS vs Linux). Diskusikan dengan siswa: layanan atau perangkat seperti apa yang lebih cocok memakai HSRP dibanding Keepalived pada jaringan nyata, dan mengapa virtual_router_id harus unik di segmen yang sama (untuk menghindari konflik dengan instance VRRP/HSRP lain).

Rangkuman

- Keepalived membawa konsep redundansi virtual IP berbasis VRRP ke level server Linux, sebagai padanan HSRP yang sudah dipelajari di level router/switch pada Kelas XI.
- Peran MASTER dan BACKUP ditentukan oleh nilai priority; node dengan priority lebih tinggi menjadi MASTER dan mengiklankan virtual IP.
- Virtual IP Keepalived dialokasikan dari subnet yang sudah ada (DMZ), bukan subnet baru, sehingga tidak mengubah skema pengalamatan yang sudah direncanakan sejak Kelas XI.

Soal Latihan/Refleksi

23. Jelaskan persamaan dan perbedaan mendasar antara HSRP dan Keepalived.
24. Mengapa virtual_router_id pada Keepalived harus unik di dalam satu segmen jaringan?
25. Apa yang akan terjadi pada layanan bila node MASTER dan BACKUP memiliki priority yang sama persis?

Checkpoint Bab 6 — Redundansi Virtual IP dengan Keepalived

No	Item Verifikasi	Status
1	Keepalived sudah terpasang dan dikonfigurasi pada kedua node server (MASTER dan BACKUP) dengan virtual_router_id yang sama.	☐ Sudah ☐ Belum
2	Virtual IP terbukti aktif di node MASTER dalam kondisi normal (ip addr show).	☐ Sudah ☐ Belum
3	Uji failover (mematikan servis di node MASTER) menunjukkan virtual IP berpindah otomatis ke node BACKUP.	☐ Sudah ☐ Belum
4	Priority dan alamat virtual IP sesuai dengan tabel perencanaan (Tabel 6.2).	☐ Sudah ☐ Belum

BAB 7 — Perencanaan Integrasi DNS Forward/Reverse Zone

Tujuan Pembelajaran

Elemen 6: Perencanaan Layanan Pendukung Jaringan (Lanjutan) — mengacu pada dokumen Target Pembelajaran Kelas XII.

No	Target Kompetensi	Indikator Capaian
1	Merencanakan integrasi layanan DNS dalam skema jaringan	Siswa mampu merencanakan pemetaan nama domain internal dan publik (forward/reverse zone) sesuai desain alamat yang telah dibuat

7.1 Konsep Forward Zone dan Reverse Zone

Forward zone memetakan nama domain ke alamat IP (mis. web01.itnsa.id → 192.168.10.82), sedangkan reverse zone memetakan arah sebaliknya, alamat IP ke nama domain (mis. 192.168.10.82 → web01.itnsa.id). Keduanya sama-sama diperlukan pada jaringan produksi: forward zone dipakai pengguna sehari-hari untuk mengakses layanan dengan nama yang mudah diingat, sedangkan reverse zone dipakai oleh berbagai layanan verifikasi (mis. mail server, logging, audit keamanan) untuk memastikan sebuah alamat IP benar-benar terasosiasi dengan nama domain yang diklaim.

Konfigurasi DNS pada Kelas XI (Bab 7, sub-bab layanan pendukung) hanya mencakup DHCP dan NAT; layanan DNS server penuh dengan forward/reverse zone sengaja tidak dibahas di Kelas XI karena DNS Server bawaan Packet Tracer hanya menyediakan mapping nama↔IP sederhana tanpa konsep zone file, SOA, maupun PTR record. BIND9 pada GNS3 menyediakan seluruh konsep tersebut secara nyata.

7.2 Perencanaan Pemetaan Nama Domain Internal dan Publik

Layanan DNS ditempatkan pada node WEB-DMZ-02 (server yang sama dengan node BACKUP Keepalived pada Bab 6, untuk efisiensi jumlah node lab), melayani domain internal itnsa.id untuk seluruh perangkat di jaringan ITNSA.ID Corp. Berikut pemetaan yang direncanakan:

Nama Domain (Forward)	Alamat IP	Keterangan
web01.itnsa.id	192.168.10.82	Server web DMZ (WEB-DMZ-01 / node MASTER Keepalived)
web02.itnsa.id	192.168.10.83	Server web DMZ cadangan (WEB-DMZ-02 / node BACKUP Keepalived)
www.itnsa.id	192.168.10.84	Virtual IP layanan web (hasil Bab 6) — nama yang dipakai pengguna
mail.itnsa.id	192.168.10.85	Server mail DMZ
ns1.itnsa.id	192.168.10.83	Server DNS itu sendiri (self-reference)

Zone reverse dibuat untuk blok DMZ yang sudah dialokasikan sejak Kelas XI (192.168.10.80/29), menghasilkan pemetaan PTR sebagai cerminan tabel forward di atas.

7.3 Tabel Perencanaan Zone

Parameter	Nilai
Nama zone forward	itnsa.id
File zone forward	/etc/bind/db.itnsa.id
Nama zone reverse	10.168.192.in-addr.arpa
File zone reverse	/etc/bind/db.192.168.10
Server otoritatif (SOA/NS)	ns1.itnsa.id (192.168.10.83)
Type zone	master (server ini adalah sumber utama, bukan salinan/slave)

Praktik/Aktivitas Pembelajaran

Ceklis Praktik — DNS Forward/Reverse Zone dengan BIND9 (Bab 7)

No	Langkah Praktik yang Harus Dilakukan Siswa	Ceklis
1	Pasang paket bind9 pada node server DNS (WEB-DMZ-02).	☐ Selesai
2	Daftarkan zone “itnsa.id” (forward) dan “10.168.192.in-addr.arpa” (reverse) pada named.conf.local.	☐ Selesai
3	Isi zone file forward /etc/bind/db.itnsa.id sesuai Tabel 7.2 (SOA, NS, dan A record).	☐ Selesai
4	Isi zone file reverse /etc/bind/db.192.168.10 sebagai cerminan PTR dari zone forward.	☐ Selesai
5	Jalankan systemctl restart bind9 setelah setiap perubahan zone file.	☐ Selesai
6	Arahkan DNS server pada node client ke IP node BIND9 (manual atau via DHCP).	☐ Selesai
7	Uji nslookup dari node client dan dig -x untuk resolusi reverse, pastikan keduanya berhasil.	☐ Selesai

Aktivitas GNS3 — DNS Forward/Reverse Zone dengan BIND9 (± 30 menit): sediakan resolusi nama domain internal (forward zone) sekaligus resolusi IP-ke-nama (reverse zone) untuk server pada segmen 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)
$TTL 604800
@   IN  SOA  ns1.itnsa.id. admin.itnsa.id. (
            2026080401 ; serial
            3600       ; refresh
            1800       ; retry
```

```
            604800     ; expire
            86400 )    ; minimum TTL
    IN  NS   ns1.itnsa.id.

ns1   IN  A  192.168.10.83
web01 IN  A  192.168.10.82
web02 IN  A  192.168.10.83
www   IN  A  192.168.10.84
mail  IN  A  192.168.10.85
```

```
! Isi /etc/bind/db.192.168.10 (reverse zone)
$TTL 604800
@   IN  SOA  ns1.itnsa.id. admin.itnsa.id. (
            2026080401 ; serial
            3600 1800 604800 86400 )
    IN  NS   ns1.itnsa.id.

82  IN  PTR web01.itnsa.id.
83  IN  PTR web02.itnsa.id.
84  IN  PTR www.itnsa.id.
85  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 192.168.10.82 @192.168.10.83
```

Catatan guru: pastikan PC client menunjuk DNS server ke IP node BIND9 ini, baik diisi manual maupun disebarkan lewat DHCP (server DHCP yang sudah dikonfigurasi di Kelas XI), agar resolusi nama dapat diuji end-to-end dari sisi pengguna, bukan hanya dari server itu sendiri. Perhatikan pula bahwa nilai serial pada SOA record wajib dinaikkan setiap kali zone file diedit, agar perubahan dikenali oleh proses reload/transfer zone.

Rangkuman

- Forward zone memetakan nama ke IP; reverse zone memetakan IP ke nama — keduanya diperlukan untuk operasi jaringan yang lengkap dan tidak dapat disimulasikan secara presisi di Packet Tracer.
- BIND9 pada node Linux GNS3 menyediakan konsep zone file, SOA record, dan PTR record secara nyata, sesuai perilaku DNS server produksi.
- Pemetaan nama domain pada ITNSA.ID Corp mengikuti alokasi IP yang sudah direncanakan sejak Kelas XI, termasuk virtual IP hasil Keepalived pada Bab 6.

Soal Latihan/Refleksi

26. Jelaskan mengapa reverse zone tetap diperlukan meskipun forward zone sudah berfungsi dengan baik.
27. Apa fungsi nilai serial pada SOA record, dan apa yang terjadi bila nilai ini lupa dinaikkan setelah zone file diedit?
28. Mengapa nama www.itnsa.id pada Tabel 7.2 diarahkan ke virtual IP Keepalived, bukan ke salah satu IP fisik server?

Checkpoint Bab 7 — Integrasi DNS Forward/Reverse Zone

No	Item Verifikasi	Status
1	BIND9 sudah terpasang dan zone forward (itnsa.id) serta reverse (10.168.192.in-addr.arpa) sudah dikonfigurasi pada named.conf.local.	☐ Sudah ☐ Belum
2	Zone file forward dan reverse sudah diisi sesuai Tabel 7.2, termasuk SOA dan NS record.	☐ Sudah ☐ Belum
3	nslookup/dig dari node client menunjukkan resolusi forward dan reverse berhasil.	☐ Sudah ☐ Belum
4	PC client sudah diarahkan ke DNS server ini (manual atau via DHCP) dan resolusi nama berhasil diuji end-to-end.	☐ Sudah ☐ Belum

BAB 8 — Proyek Akhir Terintegrasi: ITNSA.ID Corp Lanjutan

Tujuan Proyek

Menggabungkan kelima target kompetensi Kelas XII (dual-stack IPv6, VPN, VTP, Keepalived, dan DNS forward/reverse zone) menjadi satu topologi GNS3 yang utuh dan konsisten, di atas fondasi ITNSA.ID Corp yang telah dibangun sejak Kelas XI, sebagai bukti penguasaan menyeluruh siswa terhadap materi pendalaman kelas ini.

Deskripsi Skenario Lengkap

ITNSA.ID Corp telah tumbuh: manajemen memutuskan bahwa jaringan perusahaan harus siap menghadapi kebutuhan masa depan (IPv6), konektivitas antar-cabang yang lebih aman melalui internet publik (VPN), pengelolaan VLAN yang lebih efisien seiring bertambahnya switch (VTP), layanan web yang tidak boleh mati meski satu server gagal (Keepalived), dan sistem penamaan domain internal yang profesional (DNS zone). Siswa berperan sebagai tim jaringan yang ditugaskan menuntaskan seluruh permintaan ini pada satu topologi GNS3 yang sama, tanpa mengubah skema IPv4/VLAN yang sudah berjalan sejak Kelas XI.

Tahapan Pengerjaan

29. Pastikan topologi ITNSA.ID Corp hasil Bab 2 sudah berjalan stabil di GNS3, dengan skema IPv4 dan VLAN identik dengan hasil Kelas XI.
30. Tambahkan dual-stack IPv6 pada seluruh interface router utama sesuai skema Bab 3, lalu verifikasi routing OSPFv3 antar segmen.
31. Bangun tunnel VPN site-to-site antara HQ-CORE dan CBG1-RTR sesuai skema Bab 4, lalu verifikasi trafik LAN Internal HQ ke LAN Cabang 1 melewati tunnel.
32. Konfigurasikan domain VTP pada seluruh switch sesuai skema Bab 5, lalu buktikan VLAN baru pada server otomatis tersebar ke seluruh client.
33. Tambahkan dua node server DMZ dengan Keepalived sesuai skema Bab 6, lalu uji failover virtual IP dari MASTER ke BACKUP.
34. Pasang BIND9 pada salah satu node server DMZ sesuai skema Bab 7, lalu verifikasi resolusi forward dan reverse dari node client.
35. Susun dokumentasi akhir: topologi lengkap (screenshot GNS3), seluruh tabel pengalamatan (IPv4, IPv6, VPN, VTP, Keepalived, DNS), dan hasil verifikasi (output show/CLI) sebagai bukti setiap target tuntas.

Ceklis Praktik — Proyek Akhir Terintegrasi (Bab 8)

No	Langkah Praktik yang Harus Dilakukan Siswa	Ceklis
1	Topologi ITNSA.ID Corp hasil Bab 2 berjalan stabil, skema IPv4/VLAN identik Kelas XI.	☐ Selesai
2	Dual-stack IPv6 aktif pada seluruh interface router utama, OSPFv3 sudah neighbor.	☐ Selesai
3	Tunnel VPN site-to-site HQ-CORE ↔ CBG1-RTR terbentuk dan trafik LAN-ke-LAN diverifikasi.	☐ Selesai
4	Domain VTP berjalan (server + minimal dua client), VLAN baru tersebar otomatis.	☐ Selesai
5	Dua node server DMZ dengan Keepalived aktif, failover MASTER → BACKUP terverifikasi.	☐ Selesai
6	BIND9 terpasang, resolusi forward dan reverse berhasil diuji dari node client.	☐ Selesai

No	Langkah Praktik yang Harus Dilakukan Siswa	Ceklis
7	Dokumentasi akhir (topologi, seluruh tabel pengalamatan, bukti verifikasi CLI) tersusun.	☐ Selesai

Kriteria Keberhasilan (Definition of Done)

- Seluruh interface router utama memiliki alamat IPv4 dan IPv6 aktif, dengan ping/ping6 berhasil antar segmen.
- Tunnel VPN antara HQ dan Cabang 1 terbentuk (security association aktif) dan traceroute LAN-ke-LAN menunjukkan trafik melewati tunnel.
- Domain VTP berjalan dengan minimal satu switch server dan dua switch client, dibuktikan dengan VLAN baru yang tersebar otomatis.
- Virtual IP Keepalived aktif pada node MASTER dan terbukti berpindah ke node BACKUP saat diuji failover.
- Resolusi DNS forward dan reverse berhasil diuji dari node client, bukan hanya dari server DNS itu sendiri.
- Skema IPv4 dan VLAN Kelas XI tidak berubah/rusak akibat penambahan kelima target di atas.

Rubrik Penilaian (Contoh)

Aspek	Bobot	Indikator
Dokumen perencanaan (tabel alamat, skema tunnel/zone)	30%	Lengkap, konsisten dengan skema Kelas XI, dan dapat dijelaskan alasan setiap keputusan desain
Implementasi IPv6 & VPN	20%	Dual-stack dan tunnel VPN berfungsi serta terverifikasi dengan perintah CLI yang sesuai
Implementasi VTP & Keepalived	20%	Distribusi VLAN dan failover virtual IP terbukti berjalan sesuai skenario uji
Implementasi DNS zone	15%	Forward dan reverse zone terverifikasi berhasil dari sisi client
Dokumentasi akhir & presentasi	15%	Topologi, tabel, dan bukti verifikasi tersusun rapi dan dapat dipresentasikan

Checkpoint Bab 8 — Proyek Akhir Terintegrasi

No	Item Verifikasi	Status
1	Checkpoint Bab 2–7 seluruhnya sudah dinyatakan tuntas sebelum memulai integrasi akhir.	☐ Sudah ☐ Belum
2	Seluruh lima target berjalan bersamaan pada satu topologi GNS3 yang sama, tanpa saling mengganggu.	☐ Sudah ☐ Belum
3	Dokumentasi akhir (topologi, tabel pengalamatan lengkap, bukti verifikasi CLI) sudah disusun.	☐ Sudah ☐ Belum
4	Skema IPv4/VLAN Kelas XI dipastikan tetap utuh dan tidak berubah setelah seluruh target Kelas XII ditambahkan.	☐ Sudah ☐ Belum

BAB 9 — Penutup

9.1 Ringkasan Capaian

Buku ini telah membawa siswa menuntaskan 5 target kompetensi pendalaman Kelas XII (20% dari keseluruhan target perencanaan dan pengalamatan jaringan), melanjutkan langsung 20 target inti yang telah dikuasai di Kelas XI. Kelima target — dual-stack IPv6, pengalamatan VPN, distribusi VLAN via VTP, redundansi Virtual IP via Keepalived, dan integrasi DNS forward/reverse zone — seluruhnya dikerjakan penuh di GNS3, mempertemukan siswa dengan perilaku sistem operasi Cisco IOS dan Linux yang presisi dan mendekati kondisi jaringan produksi sesungguhnya.

Dengan tuntasnya buku ini, siswa telah menguasai seluruh 25 target kompetensi (100%) pada mata pelajaran Perencanaan dan Pengalamatan Jaringan Program Keahlian TJKT, tersebar pada 7 elemen, mulai dari analisis kebutuhan jaringan hingga integrasi layanan DNS lanjutan, dengan satu studi kasus berkelanjutan: ITNSA.ID Corp.

9.2 Kaitan dengan Kompetisi Keahlian

Penguasaan materi buku ini secara langsung mempersiapkan siswa menghadapi Modul A (Linux Environment) dan memperdalam Modul B (Cisco Packet Tracer/GNS3) pada Lomba Kompetensi Siswa Bidang IT Network System Administration, khususnya soal-soal yang melibatkan layanan berbasis Linux (BIND9, Keepalived), keamanan konektivitas antar-lokasi (VPN), serta skalabilitas pengelolaan VLAN (VTP) — topik-topik yang jarang diujikan pada tingkat Kelas XI namun umum muncul pada tingkat kompetisi yang lebih tinggi.

9.3 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 Kelas XI (Porsi 80%) dan Target Pembelajaran Kelas XII (Porsi 20%, Pendalaman).
- Dokumentasi resmi GNS3 (gns3.com) untuk instalasi, pengelolaan image, dan praktik terbaik penggunaan GNS3 VM.
- Dokumentasi resmi Cisco IOS untuk perintah IPv6, IPsec (crypto isakmp/ipsec), dan VTP.
- Dokumentasi resmi Keepalived (keepalived.org) untuk konfigurasi VRRP pada Linux.
- Dokumentasi resmi ISC BIND9 untuk konfigurasi zone forward dan reverse.

LAMPIRAN

A. Troubleshooting Umum di GNS3

Tabel berikut merangkum kendala yang paling sering dijumpai siswa/guru selama mengerjakan buku ini, 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 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
ping6 gagal padahal ipv6 address sudah diisi	ipv6 unicast-routing belum diaktifkan secara global	Jalankan ipv6 unicast-routing pada mode global configuration di setiap router
Tunnel VPN tidak terbentuk (SA kosong)	Access-list interesting traffic tidak simetris antar kedua sisi, atau pre-shared key tidak sama	Periksa access-list di kedua router harus saling mencerminkan (source/destination dibalik); pastikan crypto isakmp key identik
VLAN baru di server VTP tidak muncul di client	Password/domain VTP tidak identik, atau link antar-switch bukan trunk	Samakan vtp domain dan vtp password di seluruh switch; pastikan switchport mode trunk aktif pada link yang menghubungkan
Virtual IP Keepalived tidak pernah berpindah saat MASTER dimatikan	virtual_router_id berbeda antar node, atau advert_int/firewall memblokir paket VRRP	Samakan virtual_router_id di kedua node; pastikan tidak ada aturan firewall yang memblokir multicast VRRP (224.0.0.18)
nslookup gagal dari node client	Node client belum menunjuk DNS server yang benar, atau bind9 belum di-restart setelah edit zone file	Set DNS server pada client secara manual atau via DHCP; jalankan systemctl restart bind9 setelah setiap perubahan zone file
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 bab, bukan seluruhnya sekaligus
Konfigurasi hilang setelah node di-restart	Belum disimpan ke startup-config (IOS) atau file konfigurasi belum permanen (Linux)	IOS: copy running-config startup-config. Linux: pastikan systemctl enable dijalankan agar servis aktif otomatis saat boot

B. Lembar Checkpoint Rekap Seluruh Target Kelas XII

Gunakan lembar ini sebagai gerbang verifikasi akhir sebelum siswa dinyatakan tuntas seluruh materi pendalaman Kelas XII, merangkum checkpoint Bab 2–8 pada buku ini.

No	Item Verifikasi	Status
1	Environment GNS3 (Desktop + VM + image) sudah terpasang dan topologi dasar ITNSA.ID Corp berjalan stabil (Bab 2).	☐ Sudah ☐ Belum
2	Dual-stack IPv6 aktif pada seluruh interface router utama dan OSPFv3 sudah membentuk neighbor (Bab 3).	☐ Sudah ☐ Belum
3	Tunnel VPN site-to-site HQ ↔ Cabang 1 terbentuk dan trafik LAN-ke-LAN terverifikasi melewati tunnel (Bab 4).	☐ Sudah ☐ Belum
4	Domain VTP berjalan dengan satu server dan minimal dua client, VLAN baru terbukti tersebar otomatis (Bab 5).	☐ Sudah ☐ Belum
5	Virtual IP Keepalived aktif pada node MASTER dan failover ke BACKUP terverifikasi (Bab 6).	☐ Sudah ☐ Belum
6	Zone forward dan reverse DNS terverifikasi berhasil dari node client (Bab 7).	☐ Sudah ☐ Belum
7	Dokumentasi akhir proyek terintegrasi (topologi, tabel pengalamatan lengkap, bukti verifikasi CLI) sudah disusun (Bab 8).	☐ Sudah ☐ Belum

Catatan Guru:

Paraf Guru: _____