BUKU BAHAN AJAR GURU

TEKNOLOGI JARINGAN KABEL DAN NIRKABEL

Program Keahlian Teknik Jaringan Komputer dan Telekomunikasi (TJKT)

Disusun berdasarkan Capaian Pembelajaran Kurikulum Merdeka SMK
dan Naskah Soal LKS SMK Bidang IT Network System Administration (Modul B: Cisco Packet Tracer)

Jilid 2 - Untuk Kelas XII SMK

Yusuf Burhani, S.Pd., S.Kom

Kata Pengantar

Buku ini disusun sebagai bahan ajar bagi guru mata pelajaran Teknologi Jaringan Kabel dan Nirkabel pada Program Keahlian Teknik Jaringan Komputer dan Telekomunikasi (TJKT) kelas XI dan XII Sekolah Menengah Kejuruan. Penyusunan materi mengacu pada Capaian Pembelajaran (CP) mata pelajaran ini dalam kerangka Kurikulum Merdeka, serta diperkaya dengan kebutuhan kompetensi jaringan kabel yang bersumber dari naskah soal Lomba Kompetensi Siswa (LKS) SMK Bidang IT Network System Administration, khususnya Modul B (Cisco Packet Tracer).

Materi dalam buku ini disusun dalam dua kelompok besar sesuai sumbernya. Target A merupakan kompetensi jaringan kabel (wired) yang tersirat langsung dari topologi dan konfigurasi interface pada soal LKS, meliputi media dan interface Ethernet, teknologi WAN berbasis kabel (koneksi serial), serta agregasi dan redundansi jalur kabel. Target B merupakan materi instalasi fisik kabel dan jaringan nirkabel (wireless) yang menjadi bagian standar mata pelajaran ini namun tidak tercakup pada soal LKS yang dijadikan acuan, sehingga disusun mandiri mengacu pada Capaian Pembelajaran nasional, mencakup terminasi kabel tembaga dan fiber optik, structured cabling, pengujian kabel, standar WLAN, instalasi access point, keamanan nirkabel, site survey, tautan nirkabel outdoor, hingga troubleshooting jaringan kabel dan nirkabel.

Urutan bab dalam buku ini mengikuti rekomendasi urutan pembelajaran pada dokumen target, yaitu dimulai dari dasar instalasi fisik kabel (Target B.1), dilanjutkan konsep dan konfigurasi logis jaringan kabel/WAN menggunakan Cisco Packet Tracer (Target A), kemudian jaringan nirkabel (Target B.2), dan ditutup dengan troubleshooting gabungan kabel dan nirkabel (Target B.3). Setiap bab disusun dengan struktur konsisten: tujuan pembelajaran, uraian materi, praktik/aktivitas pembelajaran, rangkuman, serta soal latihan/refleksi.

Karena sumber soal LKS yang dijadikan acuan tidak mencakup praktik wireless dan instalasi fisik kabel secara eksplisit, guru disarankan melengkapi praktik Target B menggunakan perangkat fisik yang tersedia di sekolah (access point, tang crimping, kabel UTP, alat terminasi fiber, cable tester), termasuk proyek nyata pemasangan access point di lingkungan sekolah untuk melengkapi pengalaman simulasi yang diperoleh dari Target A.

Semoga buku ini bermanfaat sebagai pegangan guru dalam menyampaikan materi Teknologi Jaringan Kabel dan Nirkabel secara sistematis, aplikatif, dan relevan dengan kebutuhan dunia kerja serta persiapan kompetisi keahlian.

Penyusun

Daftar Isi

Peta Kompetensi Buku

Tabel berikut memetakan setiap bab terhadap kelompok target pembelajaran (Target A: bersumber langsung dari kebutuhan soal LKS; Target B: materi prasyarat/fondasi di luar cakupan soal LKS) sebagaimana termuat dalam dokumen Target Pembelajaran Teknologi Jaringan Kabel dan Nirkabel. Urutan bab mengikuti rekomendasi urutan pembelajaran: B.1 → A.1–A.3 → B.2 → B.3.

Bab	Judul	Kelompok Target	Fokus Utama
1	Pendahuluan	-	Orientasi mata pelajaran
2	Terminasi Kabel Tembaga (UTP/STP)	Target B.1	Standar TIA/EIA-568, konektor RJ45
3	Instalasi dan Terminasi Kabel Fiber Optik	Target B.1	Jenis fiber, splicing, konektorisasi
4	Structured Cabling	Target B.1	Pengkabelan horizontal & backbone
5	Pengujian Kabel dengan Alat Ukur	Target B.1	Cable tester, OTDR sederhana
6	Media dan Interface Ethernet	Target A.1	FastEthernet, GigabitEthernet
7	Perancangan Koneksi Fisik sesuai Topologi	Target A.1	Router-switch, switch-switch, end device
8	Verifikasi Status Interface	Target A.1	Status up/down, protocol up/down
9	Teknologi WAN Berbasis Kabel: Koneksi Serial	Target A.2	Leased line point-to-point
10	Konfigurasi Interface Serial pada Router	Target A.2	IP address, clock rate, bandwidth
11	Topologi Multi-Cabang melalui Jalur WAN	Target A.2	Router CORE, BRT, TMT
12	Agregasi Jalur Kabel: EtherChannel	Target A.3	PAgP, LACP, mode konfigurasi
13	Redundansi Jalur Kabel Jaringan Enterprise	Target A.3	Keandalan, load balancing
14	Konsep Dasar dan Standar WLAN (802.11)	Target B.2	Evolusi standar, frekuensi, kecepatan
15	Instalasi dan Konfigurasi Access Point	Target B.2	SSID, channel, mode keamanan
16	Keamanan Jaringan Nirkabel	Target B.2	WPA2, WPA3, risiko keamanan
17	Perencanaan Cakupan Sinyal (Site Survey)	Target B.2	Faktor cakupan, redaman, interferensi

Bab	Judul	Kelompok Target	Fokus Utama
18	Koneksi Nirkabel Point-to-Point/Multipoint	Target B.2	Antena outdoor sebagai alternatif WAN
19	Troubleshooting Jaringan Kabel	Target B.3	Kabel putus, konektor rusak, mis-wiring
20	Troubleshooting Jaringan Nirkabel	Target B.3	Interferensi, jangkauan, kesalahan konfigurasi
21	Rangkuman dan Evaluasi Akhir	-	Konsolidasi & asesmen
22	Materi Praktik MikroTik	-	

CATATAN: Bagian Daftar Isi dan Peta Kompetensi Buku di atas mengikuti buku aslinya secara utuh (Bab 1-21). Jilid ini (Jilid 2 - Kelas XII) hanya memuat Bab 14 sampai Bab 21 (beserta lampiran dan daftar pustaka).

BAB 14 — Konsep Dasar dan Standar WLAN (802.11)

Tujuan Pembelajaran

- Peserta didik mampu menjelaskan konsep dasar jaringan nirkabel (WLAN).
- Peserta didik mampu menjelaskan perkembangan standar WLAN 802.11 beserta karakteristiknya.
- Peserta didik mampu menjelaskan konsep frekuensi dan channel pada jaringan nirkabel.

14.1 Konsep Dasar Jaringan Nirkabel

Wireless Local Area Network (WLAN) adalah jaringan lokal yang menghubungkan perangkat menggunakan gelombang radio sebagai media transmisi, tanpa memerlukan kabel fisik antar perangkat dan titik akses. WLAN memberikan fleksibilitas mobilitas bagi pengguna, memudahkan instalasi pada area yang sulit dijangkau kabel, namun memiliki keterbatasan berupa jangkauan sinyal terbatas, rentan terhadap interferensi, dan pada umumnya menawarkan keamanan yang memerlukan konfigurasi lebih cermat dibandingkan jaringan kabel.

14.2 Perkembangan Standar IEEE 802.11

Standar	Nama Pemasaran (Wi-Fi)	Frekuensi	Kecepatan Maksimal Teoretis
802.11b	Wi-Fi 1 (sebutan retroaktif)	2,4 GHz	11 Mbps
802.11g	Wi-Fi 3 (sebutan retroaktif)	2,4 GHz	54 Mbps
802.11n	Wi-Fi 4	2,4 GHz / 5 GHz	600 Mbps
802.11ac	Wi-Fi 5	5 GHz	hingga beberapa Gbps
802.11ax	Wi-Fi 6 / Wi-Fi 6E	2,4 GHz / 5 GHz / 6 GHz	hingga puluhan Gbps (teoretis)

14.3 Frekuensi 2,4 GHz vs 5 GHz

Pita frekuensi 2,4 GHz menawarkan jangkauan sinyal lebih jauh dan kemampuan menembus penghalang (dinding, perabot) lebih baik, namun lebih rentan terhadap interferensi karena banyak digunakan oleh berbagai perangkat rumah tangga (microwave, Bluetooth, telepon nirkabel) dan hanya memiliki jumlah channel non-overlapping (tidak tumpang tindih) yang terbatas. Pita frekuensi 5 GHz menawarkan kecepatan lebih tinggi dan lebih banyak channel non-overlapping sehingga lebih minim interferensi, namun jangkauan sinyalnya lebih pendek dan kemampuan menembus penghalang lebih lemah dibandingkan 2,4 GHz.

14.4 Konsep Channel pada WLAN

Channel adalah pembagian sub-frekuensi di dalam satu pita frekuensi yang digunakan access point untuk mentransmisikan sinyal. Pada pita 2,4 GHz, channel 1, 6, dan 11 umum dipilih karena merupakan tiga channel non-overlapping yang tersedia (tidak saling tumpang tindih spektrumnya),

sehingga penempatan access point yang berdekatan sebaiknya menggunakan kombinasi channel tersebut untuk meminimalkan interferensi co-channel.

14.5 Studi Kasus: Memilih Standar WLAN untuk Kebutuhan Sekolah

Sebuah sekolah berencana memperbarui jaringan Wi-Fi lamanya yang masih menggunakan access point berstandar 802.11n untuk mendukung kebutuhan pembelajaran digital dengan banyak perangkat terhubung bersamaan (laptop, tablet, smartphone). Pertimbangan pemilihan standar baru perlu mempertimbangkan jumlah perangkat, jenis aktivitas (streaming video pembelajaran memerlukan bandwidth lebih besar dibanding sekadar browsing), serta anggaran yang tersedia, karena standar terbaru (802.11ax/Wi-Fi 6) menawarkan efisiensi lebih baik untuk banyak perangkat namun dengan harga perangkat yang lebih tinggi dibandingkan 802.11ac/Wi-Fi 5.

Skenario Kebutuhan	Rekomendasi Standar
Laboratorium komputer, kepadatan tinggi, banyak perangkat	802.11ax (Wi-Fi 6) — efisiensi tinggi untuk banyak perangkat
Ruang kelas umum, kebutuhan standar	802.11ac (Wi-Fi 5) — keseimbangan biaya dan performa
Area terbuka/luar ruangan, cakupan lebih diutamakan	802.11n pada 2,4 GHz — jangkauan lebih jauh

Praktik / Aktivitas Pembelajaran

1. Peserta didik menyusun tabel perbandingan standar 802.11 (b/g/n/ac/ax) berdasarkan tahun kemunculan, frekuensi, dan kecepatan maksimal, dipresentasikan dalam bentuk infografis sederhana.
2. Diskusi kelompok: jelaskan skenario kapan sebaiknya memilih frekuensi 2,4 GHz dan kapan sebaiknya memilih 5 GHz berdasarkan kebutuhan jangkauan dan kecepatan.
3. Praktik menggunakan aplikasi Wi-Fi analyzer pada smartphone/laptop (bila tersedia) untuk memindai access point di sekitar lingkungan sekolah, mengidentifikasi channel yang digunakan masing-masing dan channel mana yang paling ramai (berpotensi interferensi).

Rangkuman

WLAN memungkinkan konektivitas jaringan tanpa kabel menggunakan gelombang radio, dengan standar 802.11 yang terus berkembang (b, g, n, ac, ax) menawarkan peningkatan kecepatan dan efisiensi. Pita frekuensi 2,4 GHz menawarkan jangkauan lebih jauh namun rentan interferensi, sedangkan 5 GHz menawarkan kecepatan lebih tinggi dengan jangkauan lebih pendek. Pemilihan channel yang tepat (mis. 1, 6, 11 pada 2,4 GHz) membantu meminimalkan interferensi antar access point. Pemahaman ini menjadi dasar sebelum mempelajari instalasi dan konfigurasi access point pada bab berikutnya.

Catatan Praktis

Selain praktik terbaik teknis, kebijakan keamanan wireless yang baik juga perlu diimbangi edukasi pengguna, misalnya mengingatkan siswa dan staf untuk tidak membagikan passphrase Wi-Fi sekolah kepada pihak luar, serta melaporkan segera apabila menemukan SSID mencurigakan yang menyerupai nama jaringan sekolah (indikasi kemungkinan serangan evil twin) di lingkungan sekolah.

Soal Latihan / Refleksi

1. Jelaskan perbedaan karakteristik jangkauan dan kecepatan antara frekuensi 2,4 GHz dan 5 GHz.
2. Jelaskan mengapa channel 1, 6, dan 11 disarankan digunakan pada pita frekuensi 2,4 GHz.
3. Sebutkan tiga standar 802.11 beserta kecepatan maksimal teoretisnya.

BAB 15 — Instalasi dan Konfigurasi Access Point

Tujuan Pembelajaran

- Peserta didik mampu memasang access point sesuai kebutuhan topologi jaringan.
- Peserta didik mampu mengonfigurasi SSID dan channel pada access point.
- Peserta didik mampu mengonfigurasi mode keamanan dasar pada access point.

15.1 Persiapan Instalasi Fisik Access Point

Sebelum konfigurasi, access point perlu dipasang secara fisik pada lokasi yang strategis, mempertimbangkan cakupan area yang ingin dilayani, minimnya penghalang fisik (dinding tebal, logam), serta ketersediaan sumber daya (power) dan koneksi ke jaringan kabel melalui port Ethernet (atau Power over Ethernet/PoE apabila didukung, yang menyalurkan daya listrik dan data melalui satu kabel yang sama).

15.2 Konfigurasi SSID

Service Set Identifier (SSID) adalah nama jaringan nirkabel yang akan terlihat oleh perangkat pengguna saat mencari jaringan Wi-Fi yang tersedia. Praktik terbaik dalam penamaan SSID adalah menghindari penggunaan informasi sensitif (mis. nama pemilik, alamat lengkap) dan mempertimbangkan opsi menyembunyikan SSID (hidden SSID) untuk jaringan yang memerlukan tingkat kerahasiaan tambahan, meskipun opsi ini bukan merupakan metode keamanan utama dan tidak menggantikan enkripsi yang kuat.

15.3 Konfigurasi Channel dan Parameter Radio

Pemilihan channel pada access point sebaiknya mempertimbangkan hasil pemindaian channel yang telah digunakan access point lain di sekitarnya (sebagaimana dibahas pada Bab 14), untuk meminimalkan interferensi co-channel. Sebagian besar access point modern menawarkan mode Auto Channel Selection yang secara otomatis memilih channel dengan tingkat interferensi terendah, meskipun konfigurasi manual tetap dimungkinkan untuk kontrol yang lebih presisi pada lingkungan dengan kepadatan access point tinggi.

15.4 Konfigurasi Mode Keamanan Dasar

Setiap access point perlu dikonfigurasi dengan mode keamanan untuk mencegah akses tidak sah, dibahas lebih mendalam pada Bab 16. Pada tahap instalasi awal, administrator perlu menentukan mode keamanan yang akan digunakan (umumnya WPA2-Personal untuk jaringan skala kecil-menengah), menetapkan passphrase yang kuat, serta mengubah kredensial administratif default (username dan password bawaan pabrik) pada antarmuka manajemen access point untuk mencegah akses konfigurasi oleh pihak tidak berwenang.

15.5 Verifikasi Pasca-Instalasi Access Point

Setelah seluruh konfigurasi access point selesai, langkah verifikasi perlu dilakukan untuk memastikan access point berfungsi sesuai rencana sebelum dianggap selesai. Verifikasi mencakup pengecekan

bahwa SSID terlihat oleh perangkat client, perangkat dapat terhubung menggunakan passphrase yang telah ditetapkan, perangkat memperoleh alamat IP (baik melalui DHCP dari jaringan kabel maupun dari access point itu sendiri jika berfungsi sebagai DHCP server), serta perangkat dapat mengakses jaringan/internet melalui uplink kabel access point.

Item Verifikasi	Cara Memeriksa
SSID terlihat	Pindai jaringan Wi-Fi yang tersedia dari perangkat client
Autentikasi berhasil	Masukkan passphrase dan pastikan status koneksi 'terhubung'
Perangkat memperoleh IP	Periksa pengaturan jaringan pada perangkat client (ipconfig/ifconfig)
Akses ke jaringan/internet	Uji ping ke gateway dan browsing ke situs web

Praktik / Aktivitas Pembelajaran

1. Praktik (bila tersedia perangkat fisik) memasang access point pada lokasi yang ditentukan, menghubungkannya ke jaringan kabel sekolah, dan mengakses antarmuka manajemen melalui browser.
2. Praktik mengonfigurasi SSID sesuai penamaan yang ditentukan guru (mis. mencerminkan nama kelompok/kelas), memilih channel secara manual berdasarkan hasil pemindaian pada Bab 14.
3. Praktik mengubah kredensial administratif default access point dan mengonfigurasi mode keamanan dasar (WPA2-Personal) dengan passphrase yang kuat.
4. Praktik menghubungkan perangkat (smartphone/laptop) ke SSID yang telah dikonfigurasi, memverifikasi bahwa perangkat memperoleh alamat IP dan dapat mengakses jaringan.

Rangkuman

Instalasi access point mencakup persiapan fisik (lokasi, sumber daya, koneksi ke jaringan kabel), konfigurasi SSID sebagai identitas jaringan nirkabel, pemilihan channel untuk meminimalkan interferensi, serta konfigurasi mode keamanan dasar dan penggantian kredensial administratif default. Kompetensi ini menjadi dasar praktis sebelum mempelajari keamanan jaringan nirkabel secara lebih mendalam pada bab berikutnya.

Catatan Praktis

Hasil site survey sebaiknya didokumentasikan dalam bentuk peta cakupan sinyal (heatmap) yang diperbarui secara berkala, terutama setelah ada perubahan tata ruang (penambahan sekat, perubahan fungsi ruangan) yang berpotensi memengaruhi propagasi sinyal wireless. Dokumentasi ini menjadi rujukan penting saat sekolah berencana menambah atau memindahkan access point di masa depan.

Soal Latihan / Refleksi

1. Jelaskan pertimbangan utama dalam menentukan lokasi pemasangan access point.
2. Jelaskan fungsi Power over Ethernet (PoE) pada instalasi access point.
3. Jelaskan mengapa mengubah kredensial administratif default access point merupakan langkah keamanan penting.

BAB 16 — Keamanan Jaringan Nirkabel

Tujuan Pembelajaran

- Peserta didik mampu menjelaskan berbagai metode keamanan jaringan nirkabel.
- Peserta didik mampu menerapkan metode keamanan WPA2/WPA3 pada access point.
- Peserta didik mampu menjelaskan risiko keamanan yang umum terjadi pada jaringan nirkabel.

16.1 Evolusi Protokol Keamanan Wireless

Protokol	Tahun Perkenalan (perkiraan)	Tingkat Keamanan	Catatan
WEP (Wired Equivalent Privacy)	1997	Sangat lemah	Mudah dibobol dengan alat modern, tidak disarankan digunakan lagi
WPA (Wi-Fi Protected Access)	2003	Lemah–sedang	Perbaikan sementara dari WEP, sudah dianggap usang
WPA2	2004	Baik	Menggunakan enkripsi AES, standar minimum yang masih layak digunakan saat ini
WPA3	2018	Sangat baik	Perlindungan tambahan terhadap serangan brute-force offline dan enkripsi individual per sesi

16.2 Mode Autentikasi WPA2/WPA3

WPA2/WPA3 menawarkan dua mode autentikasi utama. Mode Personal (PSK/Pre-Shared Key) menggunakan satu passphrase yang sama untuk seluruh pengguna, cocok untuk jaringan rumahan atau sekolah skala kecil-menengah karena kemudahan konfigurasinya. Mode Enterprise menggunakan server autentikasi terpusat (RADIUS) yang memberikan kredensial unik untuk setiap pengguna, menawarkan kontrol akses dan audit yang jauh lebih baik, cocok untuk organisasi berskala besar meskipun memerlukan infrastruktur tambahan (server RADIUS).

16.3 Risiko Keamanan Umum pada Jaringan Nirkabel

Jenis Risiko	Penjelasan
Rogue Access Point	Access point tidak sah yang dipasang oleh pihak tidak berwenang untuk menyusup ke jaringan atau memancing korban terhubung ke jaringan palsu
Evil Twin	Access point palsu yang meniru SSID jaringan sah untuk menipu pengguna agar terhubung dan menyadap lalu lintas datanya

Jenis Risiko	Penjelasan
Brute-force / Dictionary Attack	Upaya menebak passphrase Wi-Fi secara berulang menggunakan daftar kata sandi umum atau kombinasi acak
Deauthentication Attack	Serangan yang memaksa perangkat terputus dari access point sah, sering digunakan sebagai langkah awal serangan lain
Interferensi/Jamming	Gangguan sinyal yang disengaja untuk mengganggu ketersediaan (availability) jaringan nirkabel

16.4 Praktik Terbaik Keamanan Access Point

Beberapa praktik terbaik untuk meningkatkan keamanan jaringan nirkabel meliputi: menggunakan WPA2 atau WPA3 dengan passphrase yang kuat dan unik, mengganti kredensial administratif default, memperbarui firmware access point secara berkala untuk menutup celah keamanan yang ditemukan, menonaktifkan fitur WPS (Wi-Fi Protected Setup) yang rentan terhadap serangan brute-force, serta memisahkan jaringan tamu (guest network) dari jaringan utama menggunakan VLAN agar tamu tidak dapat mengakses sumber daya internal.

16.5 Studi Kasus: Menyusun Kebijakan Keamanan Wireless Sekolah

Tim TIK sebuah sekolah diminta menyusun kebijakan keamanan jaringan Wi-Fi yang akan diterapkan di seluruh area sekolah. Kebijakan tersebut perlu mempertimbangkan pemisahan akses antara staf pengajar (yang memerlukan akses ke sistem administrasi sekolah) dan siswa (yang hanya memerlukan akses internet untuk pembelajaran), serta tamu yang berkunjung sesekali.

Segmen Pengguna	SSID Terpisah	Rekomendasi Keamanan
Staf/Guru	Wifi-Staf	WPA2/WPA3-Personal dengan passphrase kuat, akses ke server internal
Siswa	Wifi-Siswa	WPA2/WPA3-Personal, hanya akses internet, tanpa akses ke sistem internal
Tamu	Wifi-Tamu	Jaringan terisolasi (VLAN terpisah), passphrase berbeda dan diganti berkala

Praktik / Aktivitas Pembelajaran

1. Diskusi kelompok: bandingkan tingkat keamanan WEP, WPA, WPA2, dan WPA3 dalam bentuk tabel, jelaskan mengapa WEP tidak lagi disarankan digunakan.
2. Praktik (bila tersedia perangkat fisik) mengonfigurasi mode keamanan WPA2-Personal dengan passphrase kuat pada access point, kemudian menguji koneksi dari perangkat client.
3. Diskusi kelompok: jelaskan skenario serangan evil twin dan langkah-langkah yang dapat dilakukan pengguna maupun administrator jaringan untuk mencegahnya.
4. Diskusi kelompok: rancang kebijakan keamanan wireless sederhana untuk jaringan Wi-Fi sekolah, mencakup pemisahan jaringan guru/siswa dan jaringan tamu.

Rangkuman

Keamanan jaringan nirkabel telah berkembang dari WEP yang sangat lemah hingga WPA3 yang menawarkan perlindungan terkini, dengan mode autentikasi Personal (PSK) untuk jaringan skala kecil dan Enterprise (RADIUS) untuk organisasi besar. Berbagai risiko keamanan seperti rogue access point, evil twin, dan serangan brute-force perlu diwaspadai, dengan mitigasi melalui praktik terbaik seperti penggunaan WPA2/WPA3, passphrase kuat, pembaruan firmware, dan pemisahan jaringan tamu. Pemahaman ini menjadi dasar sebelum mempelajari perencanaan cakupan sinyal pada bab berikutnya.

Catatan Praktis

Sebelum memutuskan investasi tautan nirkabel outdoor, sebaiknya dilakukan uji coba awal (proof of concept) menggunakan perangkat sederhana untuk memverifikasi kualitas sinyal aktual pada lokasi yang direncanakan, mengingat faktor lingkungan seperti pepohonan yang tumbuh seiring waktu atau bangunan baru dapat memengaruhi line-of-sight yang sebelumnya diperkirakan bebas penghalang berdasarkan pengamatan visual maupun peta satelit.

Soal Latihan / Refleksi

1. Jelaskan perbedaan tingkat keamanan antara WPA2 dan WPA3.
2. Jelaskan perbedaan mode autentikasi Personal dan Enterprise pada WPA2/WPA3.
3. Jelaskan apa yang dimaksud dengan serangan evil twin dan bagaimana cara mencegahnya.
4. Sebutkan empat praktik terbaik dalam mengamankan access point.

BAB 17 — Perencanaan Cakupan Sinyal (Site Survey)

Tujuan Pembelajaran

- Peserta didik mampu menjelaskan faktor-faktor yang memengaruhi kekuatan dan cakupan sinyal wireless.
- Peserta didik mampu menjelaskan konsep dasar site survey sederhana.
- Peserta didik mampu merencanakan penempatan access point pada suatu area berdasarkan hasil analisis cakupan.

17.1 Faktor yang Memengaruhi Cakupan Sinyal

Faktor	Pengaruh terhadap Sinyal
Jarak dari access point	Semakin jauh jarak, semakin lemah kekuatan sinyal yang diterima (path loss)
Material penghalang	Dinding beton/logam meredam sinyal lebih besar dibandingkan dinding gypsum/kayu atau kaca
Interferensi frekuensi	Perangkat lain yang menggunakan frekuensi sama (microwave, Bluetooth, access point tetangga) dapat mengganggu sinyal
Jumlah pengguna aktif	Semakin banyak perangkat terhubung pada satu access point, semakin terbagi kapasitas bandwidth yang tersedia
Ketinggian dan posisi antena	Penempatan access point yang tidak strategis (mis. di sudut ruangan, terlalu rendah) dapat mengurangi cakupan efektif

17.2 Konsep Site Survey

Site survey adalah proses pemetaan dan analisis kondisi sinyal wireless pada suatu area sebelum atau setelah instalasi access point, bertujuan menentukan jumlah dan penempatan access point yang optimal untuk mencapai cakupan sinyal yang merata dengan kualitas yang memadai. Site survey sederhana dapat dilakukan secara manual menggunakan aplikasi pengukur kekuatan sinyal (Wi-Fi analyzer) pada smartphone/laptop yang dibawa berkeliling area yang akan dicakup, mencatat kekuatan sinyal (dBm) pada berbagai titik untuk mengidentifikasi area dengan sinyal lemah (dead zone).

17.3 Indikator Kekuatan Sinyal (RSSI)

Kekuatan Sinyal (dBm)	Kualitas	Keterangan
-30 dBm hingga -50 dBm	Sangat baik	Sinyal maksimal, umumnya hanya terjadi sangat dekat access point
-50 dBm hingga -60 dBm	Baik	Kualitas sangat baik untuk streaming dan transfer data
-60 dBm hingga -70 dBm	Cukup	Masih dapat digunakan untuk browsing dan email, mungkin tersendat untuk streaming
-70 dBm hingga -80 dBm	Lemah	Koneksi tidak stabil, kecepatan menurun signifikan

Kekuatan Sinyal (dBm)	Kualitas	Keterangan
Di bawah -80 dBm	Sangat lemah/tidak terjangkau	Koneksi sering terputus atau tidak terdeteksi sama sekali

17.4 Strategi Penempatan Access Point

Berdasarkan hasil site survey, penempatan access point sebaiknya mempertimbangkan pemerataan cakupan (menghindari tumpang tindih berlebihan yang memboroskan biaya, namun cukup untuk menghindari dead zone), penempatan pada posisi sentral dan cukup tinggi (mis. di langit-langit) untuk memaksimalkan cakupan ke segala arah, serta mempertimbangkan kepadatan pengguna pada suatu area (mis. aula pertemuan mungkin memerlukan lebih dari satu access point meski luasnya tidak terlalu besar, karena banyaknya perangkat yang akan terhubung bersamaan).

17.5 Studi Kasus: Merancang Site Survey untuk Gedung Bertingkat

Sebuah gedung sekolah tiga lantai berencana memasang jaringan Wi-Fi menyeluruh. Tim TIK perlu melakukan site survey pada setiap lantai secara terpisah, mengingat lantai beton antar tingkat merupakan penghalang signifikan bagi sinyal wireless, sehingga access point pada satu lantai umumnya tidak dapat diandalkan untuk mencakup lantai di atas atau di bawahnya secara memadai, dan setiap lantai perlu direncanakan memiliki access point tersendiri.

Lantai	Perkiraan Kebutuhan Access Point	Catatan
Lantai 1 (aula, ruang tamu, TU)	2 unit	Aula memerlukan cakupan lebih luas dan kapasitas pengguna lebih tinggi
Lantai 2 (ruang kelas)	3 unit	Disesuaikan jumlah dan luas ruang kelas
Lantai 3 (laboratorium)	2 unit	Kepadatan perangkat tinggi memerlukan cakupan lebih rapat

Praktik / Aktivitas Pembelajaran

1. Praktik menggunakan aplikasi Wi-Fi analyzer pada smartphone untuk mengukur kekuatan sinyal (RSSI) di beberapa titik pada satu lantai gedung sekolah, mencatat hasilnya dalam bentuk tabel atau peta sederhana (heatmap manual).
2. Diskusi kelompok: berdasarkan hasil pengukuran, identifikasi area dengan sinyal lemah (dead zone) dan usulkan rekomendasi penempatan access point tambahan.
3. Diskusi kelompok: analisis studi kasus sebuah aula pertemuan sekolah dengan kapasitas 200 orang, rancang jumlah dan penempatan access point yang disarankan beserta alasannya.

Rangkuman

Cakupan sinyal wireless dipengaruhi oleh jarak, material penghalang, interferensi, jumlah pengguna, dan penempatan antena. Site survey adalah proses sistematis untuk memetakan kekuatan sinyal (RSSI) pada suatu area guna menentukan jumlah dan penempatan access point yang optimal, dengan indikator kekuatan sinyal yang dapat diklasifikasikan dari sangat baik hingga tidak terjangkau.

Perencanaan cakupan sinyal yang baik menyeimbangkan pemerataan area dan kapasitas pengguna. Pemahaman ini menjadi dasar sebelum mempelajari koneksi nirkabel jarak jauh pada bab berikutnya.

Catatan Praktis

Peserta didik yang terbiasa melakukan troubleshooting secara terstruktur dan mendokumentasikannya akan lebih siap menghadapi soal-soal praktik kompetisi keahlian yang sering menyisipkan kesalahan tersembunyi pada topologi yang harus ditemukan dan diperbaiki dalam waktu terbatas, sebagaimana pola soal yang umum dijumpai pada LKS Bidang IT Network System Administration.

Soal Latihan / Refleksi

1. Sebutkan tiga faktor utama yang memengaruhi cakupan sinyal wireless.
2. Jelaskan tujuan dilakukannya site survey sebelum instalasi access point.
3. Sebuah area menunjukkan kekuatan sinyal -75 dBm. Jelaskan kualitas koneksi yang dapat diharapkan pada area tersebut beserta rekomendasi perbaikannya.

BAB 18 — Koneksi Nirkabel Point-to-Point/Point-to-Multipoint

Tujuan Pembelajaran

- Peserta didik mampu menjelaskan prinsip kerja tautan nirkabel jarak jauh menggunakan antena outdoor.
- Peserta didik mampu membedakan konfigurasi point-to-point dan point-to-multipoint.
- Peserta didik mampu menjelaskan kelebihan tautan nirkabel outdoor sebagai alternatif WAN kabel.

18.1 Konsep Tautan Nirkabel Jarak Jauh

Selain digunakan untuk jaringan lokal dalam gedung, teknologi nirkabel juga dapat diterapkan untuk menghubungkan dua lokasi yang berjauhan (mis. antar gedung atau antar area yang sulit dijangkau kabel fiber) menggunakan antena outdoor berdaya pancar dan penerimaan lebih tinggi dibandingkan access point indoor biasa. Tautan ini menjadi alternatif media WAN selain koneksi kabel Serial yang telah dipelajari pada Bab 9-11, terutama untuk lokasi yang secara geografis sulit atau mahal dijangkau kabel fisik.

18.2 Konfigurasi Point-to-Point (PtP)

Konfigurasi point-to-point menghubungkan tepat dua lokasi menggunakan sepasang antena outdoor yang saling diarahkan (aligned) satu sama lain, umumnya menggunakan antena directional (terarah) berdaya pancar tinggi ke satu arah tertentu untuk memaksimalkan jarak jangkauan dan kekuatan sinyal antar dua titik tersebut. Konfigurasi ini cocok digunakan untuk menghubungkan dua kantor cabang secara langsung tanpa melalui titik perantara.

18.3 Konfigurasi Point-to-Multipoint (PtMP)

Konfigurasi point-to-multipoint menghubungkan satu lokasi pusat dengan beberapa lokasi lain sekaligus, menggunakan antena omnidirectional atau sectoral pada titik pusat yang memancarkan sinyal ke berbagai arah, sementara setiap lokasi cabang menggunakan antena directional yang diarahkan ke titik pusat tersebut. Konfigurasi ini menyerupai arsitektur hub-and-spoke yang telah dipelajari pada Bab 11, namun menggunakan media nirkabel alih-alih kabel serial, cocok untuk menghubungkan satu kantor pusat dengan banyak kantor cabang dalam radius jangkauan tertentu tanpa perlu menyewa leased line kabel yang mahal.

Aspek	Point-to-Point (PtP)	Point-to-Multipoint (PtMP)
Jumlah lokasi terhubung	Dua lokasi	Satu lokasi pusat dengan banyak lokasi cabang
Jenis antena di titik pusat	Directional (terarah)	Omnidirectional atau sectoral
Kesesuaian topologi	Menghubungkan dua kantor secara langsung	Menyerupai arsitektur hub-and-spoke nirkabel

18.4 Kelebihan dan Pertimbangan Tautan Nirkabel Outdoor

Kelebihan tautan nirkabel outdoor dibandingkan kabel fisik (Serial/leased line ataupun fiber optik) meliputi biaya instalasi yang umumnya lebih rendah untuk jarak menengah karena tidak memerlukan penggalian/pemasangan kabel fisik sepanjang rute, waktu instalasi yang lebih cepat, serta fleksibilitas untuk direlokasi jika diperlukan. Namun perlu dipertimbangkan pula keterbatasannya, yaitu memerlukan garis pandang langsung (line-of-sight) tanpa penghalang antara kedua antena, rentan terhadap gangguan cuaca (hujan lebat, kabut tebal) yang dapat melemahkan sinyal, serta bandwidth yang umumnya lebih terbatas dibandingkan fiber optik untuk jarak yang sama.

18.5 Studi Kasus: Menghitung Kebutuhan Line-of-Sight

Dua gedung sekolah yang berjarak 500 meter berencana dihubungkan menggunakan tautan point-to-point. Sebelum instalasi, tim teknis perlu memastikan tidak ada penghalang (pohon tinggi, bangunan lain) di antara kedua titik pemasangan antena, termasuk mempertimbangkan zona Fresnel — area berbentuk elips di sekitar garis lurus penghubung kedua antena yang juga perlu bebas dari penghalang agar sinyal tidak mengalami redaman signifikan, meskipun garis pandang langsung (line-of-sight) tampak bebas penghalang secara kasat mata.

Faktor Perencanaan	Pertimbangan
Jarak antar titik	Menentukan spesifikasi antena (gain) yang diperlukan agar sinyal cukup kuat
Ketinggian pemasangan	Antena perlu dipasang cukup tinggi agar zona Fresnel bebas dari penghalang di antara kedua titik
Kondisi cuaca setempat	Daerah dengan curah hujan tinggi memerlukan margin daya sinyal (fade margin) lebih besar

Praktik / Aktivitas Pembelajaran

1. Diskusi kelompok: rancang skenario penggunaan tautan point-to-point untuk menghubungkan dua gedung sekolah yang terpisah jalan raya, jelaskan pertimbangan line-of-sight yang perlu diperhatikan.
2. Diskusi kelompok: rancang skenario penggunaan tautan point-to-multipoint untuk menghubungkan satu kantor dinas pendidikan dengan lima sekolah di sekitarnya, bandingkan dengan alternatif menyewa leased line kabel untuk kelima lokasi tersebut dari sisi biaya dan kompleksitas instalasi.
3. Peserta didik mencari dan mempresentasikan satu contoh produk antena outdoor point-to-point yang beredar di pasaran (spesifikasi jarak jangkau dan frekuensi kerja), sebagai pengenalan terhadap perangkat nyata di lapangan.

Rangkuman

Tautan nirkabel outdoor menggunakan antena berdaya tinggi menjadi alternatif media WAN selain kabel Serial atau fiber optik, dengan dua konfigurasi utama: point-to-point (menghubungkan dua lokasi) dan point-to-multipoint (menghubungkan satu pusat dengan banyak cabang, menyerupai arsitektur hub-and-spoke nirkabel). Kelebihan utamanya adalah biaya dan kecepatan instalasi, dengan pertimbangan keterbatasan line-of-sight dan gangguan cuaca. Bab ini menutup rangkaian materi Target B.2 (jaringan nirkabel), sebelum peserta didik mempelajari troubleshooting jaringan kabel dan nirkabel pada bab-bab penutup.

Catatan Praktis

Kombinasi troubleshooting jaringan kabel dan nirkabel di lapangan sering kali memerlukan koordinasi antara tim yang menangani infrastruktur fisik (kabel, switch, router) dan tim yang menangani konfigurasi wireless, terutama pada organisasi besar yang membagi tanggung jawab tersebut ke tim berbeda. Kemampuan berkomunikasi dan mendokumentasikan temuan secara jelas antar tim menjadi keterampilan tambahan yang sama pentingnya dengan keterampilan teknis itu sendiri.

Soal Latihan / Refleksi

1. Jelaskan perbedaan konfigurasi point-to-point dan point-to-multipoint pada tautan nirkabel outdoor.
2. Jelaskan syarat line-of-sight dan mengapa hal ini penting bagi tautan nirkabel outdoor.
3. Bandingkan kelebihan dan keterbatasan tautan nirkabel outdoor dibandingkan kabel fiber optik sebagai media WAN.

BAB 19 — Troubleshooting Jaringan Kabel

Tujuan Pembelajaran

- Peserta didik mampu mengidentifikasi penyebab umum gangguan koneksi kabel.
- Peserta didik mampu menerapkan metode troubleshooting sistematis pada jaringan kabel.
- Peserta didik mampu menggunakan alat ukur dan perintah CLI untuk mendiagnosis gangguan.

19.1 Penyebab Umum Gangguan Jaringan Kabel

Gejala	Kemungkinan Penyebab	Cara Verifikasi
Interface down total	Kabel putus, konektor lepas/rusak, port perangkat mati	Pemeriksaan fisik, cable tester, show ip interface brief
Koneksi tidak stabil (intermittent)	Konektor longgar, kabel tertekuk tajam, crimping kurang presisi	Cable tester, pemeriksaan fisik jalur kabel
Kecepatan jauh di bawah normal	Kesalahan kategori kabel (mis. Cat5 untuk kebutuhan Gigabit), mismatch duplex/speed	show interfaces (cek counter error/collision), verifikasi kategori kabel
Interface up namun tidak dapat ping	Kesalahan pengalamatan IP, VLAN tidak sesuai, masalah pada Layer 3	show ip interface brief, show vlan brief, show ip route
Kabel fiber tidak terdeteksi	Konektor kotor/tergores, kabel tertekuk melebihi batas radius, urutan TX/RX tertukar	Pembersihan konektor, power meter/OTDR, penukaran ulang urutan TX/RX

19.2 Metode Troubleshooting Sistematis

Pendekatan troubleshooting yang disarankan mengikuti model lapisan OSI secara bertahap (bottom-up), dimulai dari Layer 1 (Physical): periksa kabel, konektor, dan indikator LED perangkat; dilanjutkan Layer 2 (Data Link): periksa status line protocol, VLAN, dan konfigurasi trunk; kemudian Layer 3 (Network): periksa alamat IP, subnet mask, dan tabel routing. Pendekatan bottom-up ini efektif untuk masalah fisik yang jelas, sementara pendekatan top-down (mulai dari Layer 3 turun ke Layer 1) lebih efisien digunakan ketika masalah lebih mengarah pada kesalahan konfigurasi logis.

19.3 Perangkat dan Perintah Bantu Troubleshooting

Alat/Perintah	Fungsi dalam Troubleshooting
Cable tester	Memverifikasi kontinuitas dan urutan kabel tembaga (open, short, miswire)
Power meter / OTDR	Memverifikasi kualitas dan menemukan titik masalah pada kabel fiber optik
show interfaces	Memeriksa counter error, collision, CRC error yang mengindikasikan masalah fisik/kualitas kabel
show cdp neighbors	Memverifikasi topologi fisik aktual sesuai dengan diagram yang direncanakan

Alat/Perintah	Fungsi dalam Troubleshooting
ping / traceroute	Menguji konektivitas end-to-end dan menemukan titik kegagalan pada jalur data

19.4 Dokumentasi sebagai Bagian dari Troubleshooting

Dokumentasi jaringan yang baik (diagram topologi, tabel pengalamatan, catatan riwayat perubahan konfigurasi) sangat membantu proses troubleshooting karena memungkinkan teknisi membandingkan kondisi aktual dengan kondisi yang seharusnya (baseline). Tanpa dokumentasi yang memadai, proses troubleshooting menjadi lebih lambat karena teknisi harus menelusuri kondisi jaringan dari awal tanpa acuan yang jelas.

19.5 Studi Kasus: Menyusun Laporan Troubleshooting

Setelah berhasil menyelesaikan sebuah kasus troubleshooting, teknisi jaringan yang baik akan mendokumentasikan proses dan solusi yang telah dilakukan dalam bentuk laporan singkat, mencakup gejala awal yang dilaporkan, langkah diagnosis yang dilakukan, akar masalah yang ditemukan, solusi yang diterapkan, serta rekomendasi pencegahan agar masalah serupa tidak terulang. Kebiasaan mendokumentasikan proses troubleshooting ini membangun basis pengetahuan (knowledge base) yang bermanfaat bagi tim teknis di masa depan.

Praktik / Aktivitas Pembelajaran

1. Praktik pada Cisco Packet Tracer: guru menyiapkan topologi dengan kesalahan tersembunyi (mis. kabel salah jenis, interface shutdown, alamat IP salah subnet), peserta didik diminta mendiagnosis dan memperbaiki menggunakan pendekatan bottom-up.
2. Praktik fisik: menguji beberapa kabel UTP buatan sendiri dari bab-bab sebelumnya menggunakan cable tester, mengidentifikasi dan memperbaiki kabel yang menunjukkan hasil gagal.
3. Diskusi kelompok: susun daftar periksa (checklist) troubleshooting berurutan dari Layer 1 hingga Layer 3 yang dapat digunakan sebagai panduan standar saat menghadapi keluhan 'jaringan tidak bisa terhubung'.
4. Simulasi studi kasus: peserta didik diberikan gejala 'interface up, tetapi ping gagal ke jaringan tujuan' pada sebuah topologi, diminta menelusuri kemungkinan penyebab pada Layer 2 dan Layer 3 secara berurutan.

Rangkuman

Troubleshooting jaringan kabel memerlukan pemahaman gejala dan kemungkinan penyebab pada setiap layer, mulai dari masalah fisik (kabel putus, konektor rusak) hingga kesalahan konfigurasi logis (VLAN, IP address, routing). Pendekatan sistematis bottom-up atau top-down, dibantu alat ukur (cable tester, power meter/OTDR) dan perintah CLI (show interfaces, show cdp neighbors, ping, traceroute), serta dokumentasi jaringan yang baik, menjadi kunci efisiensi proses troubleshooting. Kompetensi ini menjadi dasar sebelum mempelajari troubleshooting jaringan nirkabel pada bab berikutnya.

Soal Latihan / Refleksi

1. Jelaskan perbedaan pendekatan troubleshooting bottom-up dan top-down beserta kapan masing-masing lebih efektif digunakan.
2. Jelaskan tiga kemungkinan penyebab interface yang menunjukkan status up namun tidak dapat melakukan ping ke jaringan tujuan.
3. Jelaskan pentingnya dokumentasi jaringan dalam mendukung proses troubleshooting yang efisien.

BAB 20 — Troubleshooting Jaringan Nirkabel

Tujuan Pembelajaran

- Peserta didik mampu mengidentifikasi penyebab umum gangguan koneksi jaringan nirkabel.
- Peserta didik mampu membedakan masalah interferensi, jangkauan, dan kesalahan konfigurasi pada WLAN.
- Peserta didik mampu menerapkan langkah troubleshooting sistematis pada jaringan nirkabel.

20.1 Penyebab Umum Gangguan Jaringan Nirkabel

Gejala	Kemungkinan Penyebab	Cara Verifikasi/Penanganan
SSID tidak terlihat oleh perangkat client	Access point mati/rusak, SSID disembunyikan (hidden), perangkat client di luar jangkauan	Periksa status daya access point, cek pengaturan hidden SSID, ukur RSSI menggunakan Wi-Fi analyzer
Koneksi terputus-putus (intermittent)	Interferensi frekuensi, jangkauan sinyal lemah, terlalu banyak perangkat terhubung	Analisis channel yang digunakan sekitar, site survey ulang, pertimbangkan penambahan access point
Kecepatan sangat lambat meski sinyal kuat	Kepadatan pengguna tinggi, interferensi co-channel dari access point tetangga, standar 802.11 lama yang membatasi kecepatan seluruh jaringan	Cek jumlah perangkat terhubung, ubah channel, evaluasi standar 802.11 yang didukung
Perangkat tidak dapat terhubung meski passphrase benar	Mode keamanan tidak didukung perangkat client, MAC filtering aktif dan menolak perangkat, batas maksimal koneksi tercapai	Cek kompatibilitas standar keamanan, cek daftar MAC filtering, cek jumlah koneksi aktif
Sinyal terdeteksi namun tidak dapat browsing	Access point terhubung namun uplink ke jaringan kabel/internet bermasalah (masalah Layer 3 ke atas)	Periksa koneksi kabel access point ke switch/router, cek konfigurasi DHCP/gateway

20.2 Diagnosis Interferensi vs Jangkauan vs Konfigurasi

Langkah awal troubleshooting wireless adalah membedakan tiga kategori masalah utama. Masalah interferensi umumnya ditandai sinyal kuat namun koneksi tidak stabil, dapat diverifikasi dengan mengecek channel yang digunakan access point sekitar menggunakan Wi-Fi analyzer. Masalah jangkauan ditandai sinyal lemah (RSSI rendah) yang konsisten pada area tertentu, memerlukan solusi berupa relokasi/penambahan access point sebagaimana dibahas pada Bab 17. Masalah konfigurasi umumnya ditandai kegagalan koneksi yang konsisten terlepas dari kekuatan sinyal (mis. passphrase salah, mode keamanan tidak cocok, MAC filtering), memerlukan pemeriksaan pengaturan pada access point maupun perangkat client.

20.3 Perangkat dan Aplikasi Bantu Troubleshooting Wireless

Alat/Aplikasi	Fungsi
Wi-Fi Analyzer (aplikasi smartphone/laptop)	Memindai SSID, channel, dan kekuatan sinyal (RSSI) access point di sekitar
Spectrum Analyzer	Mendeteksi sumber interferensi non-Wi-Fi (mis. microwave, perangkat Bluetooth) pada pita frekuensi yang sama
Antarmuka manajemen access point	Memeriksa log koneksi, daftar perangkat terhubung, dan status konfigurasi keamanan
ping / speed test	Menguji konektivitas dan kecepatan aktual setelah perangkat terhubung ke jaringan nirkabel

20.4 Studi Kasus Troubleshooting Gabungan

Pada praktiknya, gangguan jaringan enterprise modern sering melibatkan kombinasi jaringan kabel dan nirkabel yang saling terhubung, misalnya access point yang terhubung ke switch melalui kabel Ethernet. Dalam kasus seperti ini, teknisi perlu menelusuri masalah secara menyeluruh: memverifikasi terlebih dahulu apakah masalah berada pada sisi nirkabel (client ke access point) ataukah pada sisi kabel (access point ke jaringan inti), menggunakan kombinasi teknik troubleshooting yang telah dipelajari pada Bab 19 dan bab ini.

20.5 Studi Kasus: Menyusun Laporan Troubleshooting Wireless

Sama halnya dengan troubleshooting jaringan kabel, setiap penyelesaian kasus gangguan jaringan nirkabel sebaiknya didokumentasikan, mencakup gejala yang dilaporkan pengguna, hasil pemindaian Wi-Fi analyzer (channel dan RSSI sekitar), langkah perbaikan yang diambil, serta rekomendasi jangka panjang seperti penambahan access point atau perubahan channel secara permanen, agar tim TIK sekolah memiliki basis data kondisi jaringan yang terus diperbarui dari waktu ke waktu.

Praktik / Aktivitas Pembelajaran

1. Praktik menggunakan Wi-Fi analyzer untuk mengidentifikasi access point dengan channel yang saling tumpang tindih di lingkungan sekolah, mengusulkan perubahan channel untuk mengurangi interferensi.
2. Simulasi studi kasus: guru memberikan skenario 'beberapa siswa mengeluh Wi-Fi lambat di aula saat acara sekolah, padahal sinyal terlihat penuh', peserta didik menganalisis kemungkinan penyebab (kepadatan pengguna) dan solusinya.
3. Diskusi kelompok: susun daftar periksa (checklist) troubleshooting wireless yang membedakan gejala interferensi, jangkauan, dan kesalahan konfigurasi.
4. Diskusi kelompok/simulasi: analisis studi kasus gabungan di mana access point kehilangan koneksi ke jaringan kabel (kemungkinan masalah pada Bab 19), namun gejala yang dilaporkan pengguna adalah 'Wi-Fi tidak berfungsi' — jelaskan langkah penelusuran menyeluruh yang perlu dilakukan.

Rangkuman

Troubleshooting jaringan nirkabel memerlukan kemampuan membedakan tiga kategori masalah utama: interferensi, jangkauan sinyal, dan kesalahan konfigurasi, masing-masing dengan gejala dan metode verifikasi yang berbeda. Alat bantu seperti Wi-Fi analyzer dan spectrum analyzer membantu

mendiagnosis sumber masalah secara lebih presisi. Pada jaringan modern yang menggabungkan kabel dan nirkabel, troubleshooting menyeluruh perlu mempertimbangkan kedua sisi media transmisi. Bab ini menutup seluruh rangkaian materi Target B.3 sekaligus keseluruhan buku, sebelum konsolidasi akhir pada bab penutup.

Soal Latihan / Refleksi

1. Jelaskan perbedaan gejala antara masalah interferensi dan masalah jangkauan sinyal pada jaringan nirkabel.
2. Jelaskan tiga kemungkinan penyebab perangkat client gagal terhubung meski passphrase yang dimasukkan sudah benar.
3. Jelaskan langkah troubleshooting menyeluruh yang perlu dilakukan ketika access point kehilangan koneksi internet meski sinyal Wi-Fi tetap terpancar dengan baik.

BAB 21 — Rangkuman dan Evaluasi Akhir

Tujuan Pembelajaran

- Guru dan peserta didik mampu mengaitkan keterkaitan antar bab yang telah dipelajari.
- Peserta didik mampu mengerjakan evaluasi akhir sebagai bentuk asesmen sumatif materi Teknologi Jaringan Kabel dan Nirkabel.

21.1 Keterkaitan Antar Bab

Materi dalam buku ini disusun mengikuti urutan pembelajaran yang direkomendasikan pada dokumen target. Keterampilan dasar instalasi fisik kabel (Bab 2-5: terminasi tembaga, fiber optik, structured cabling, dan pengujian kabel) menjadi fondasi praktis sebelum peserta didik mempelajari konfigurasi logis jaringan kabel (Bab 6-13), dimulai dari interface Ethernet dan perancangan koneksi fisik, dilanjutkan teknologi WAN berbasis kabel Serial untuk topologi multi-cabang, hingga agregasi dan redundansi jalur kabel menggunakan EtherChannel dan STP. Pemahaman jaringan kabel tersebut kemudian diperluas ke ranah nirkabel (Bab 14-18), mencakup standar WLAN, instalasi dan keamanan access point, perencanaan cakupan sinyal, hingga tautan nirkabel jarak jauh sebagai alternatif WAN. Seluruh rangkaian materi kabel dan nirkabel ditutup dengan kompetensi troubleshooting (Bab 19-20) yang menggabungkan seluruh pemahaman sebelumnya untuk mendiagnosis dan menyelesaikan gangguan jaringan secara menyeluruh.

21.2 Rangkuman Keseluruhan Materi

Bab	Inti Materi
2	Terminasi kabel UTP/STP, standar T568A/T568B, kabel straight/cross
3	Jenis fiber optik (single/multi-mode), fusion/mechanical splicing, jenis konektor
4	Structured cabling: komponen, pengkabelan horizontal dan backbone
5	Pengujian kabel: cable tester, OTDR, power meter, visual fault locator
6	Jenis interface Ethernet dan konfigurasi dasar sesuai tabel pengalamatan
7	Perancangan koneksi fisik sesuai topologi dan jenis kabel yang tepat
8	Verifikasi status interface (Layer 1/Layer 2) dan strategi diagnosis bertahap
9	Konsep koneksi Serial sebagai media WAN point-to-point, leased line, DCE/DTE
10	Konfigurasi interface serial: IP address, clock rate, verifikasi
11	Topologi multi-cabang hub-and-spoke dan static routing antar cabang
12	EtherChannel: link aggregation, protokol PAgP/LACP
13	Redundansi jalur kabel dan peran Spanning Tree Protocol (STP)
14	Konsep WLAN, standar 802.11, frekuensi dan channel
15	Instalasi access point: SSID, channel, mode keamanan dasar
16	Keamanan wireless: evolusi protokol, mode autentikasi, risiko keamanan

Bab	Inti Materi
17	Site survey: faktor cakupan sinyal, RSSI, strategi penempatan access point
18	Tautan nirkabel point-to-point dan point-to-multipoint sebagai alternatif WAN
19	Troubleshooting jaringan kabel: gejala, penyebab, metode sistematis
20	Troubleshooting jaringan nirkabel: interferensi, jangkauan, konfigurasi

21.3 Soal Evaluasi Akhir

Soal berikut dapat digunakan guru sebagai bahan asesmen sumatif atau latihan persiapan kompetisi keahlian, mencakup seluruh bab dalam buku ini.

1. Jelaskan perbedaan standar pengkabelan T568A dan T568B beserta kapan masing-masing dikombinasikan untuk menghasilkan kabel straight-through dan cross-over.
2. Jelaskan perbedaan kabel fiber optik single-mode dan multi-mode beserta metode penyambungannya.
3. Jelaskan konsep structured cabling beserta perbedaan pengkabelan horizontal dan backbone.
4. Jelaskan fungsi cable tester dan OTDR dalam pengujian kualitas kabel.
5. Jelaskan perbedaan interface FastEthernet dan GigabitEthernet.
6. Jelaskan makna status interface 'up, line protocol down' beserta kemungkinan penyebabnya.
7. Jelaskan konsep leased line dan peran perangkat DCE/DTE pada koneksi Serial.
8. Tuliskan urutan perintah dasar untuk mengonfigurasi interface serial sebagai sisi DCE dengan alamat IP dan clock rate tertentu.
9. Jelaskan arsitektur hub-and-spoke pada topologi multi-cabang beserta cara kerjanya.
10. Jelaskan tujuan dan protokol negosiasi pada konfigurasi EtherChannel.
11. Jelaskan bagaimana Spanning Tree Protocol mencegah loop pada jaringan redundan.
12. Jelaskan perkembangan standar WLAN 802.11 beserta karakteristik frekuensi 2,4 GHz dan 5 GHz.
13. Jelaskan langkah-langkah dasar instalasi dan konfigurasi access point.
14. Jelaskan evolusi protokol keamanan wireless dari WEP hingga WPA3.
15. Jelaskan konsep site survey dan faktor yang memengaruhi cakupan sinyal wireless.
16. Jelaskan perbedaan konfigurasi tautan nirkabel point-to-point dan point-to-multipoint.
17. Jelaskan metode troubleshooting sistematis (bottom-up/top-down) pada jaringan kabel.
18. Jelaskan cara membedakan masalah interferensi, jangkauan, dan konfigurasi pada troubleshooting jaringan nirkabel.

21.4 Glosarium Istilah

Glosarium berikut merangkum istilah-istilah teknis penting yang digunakan sepanjang buku ini, disusun sebagai rujukan cepat bagi guru maupun peserta didik.

Istilah	Penjelasan Singkat
Access Point (AP)	Perangkat yang menghubungkan perangkat nirkabel ke jaringan kabel menggunakan gelombang radio
Backbone Cabling	Kabel yang menghubungkan Equipment Room dengan Telecommunications Room antar lantai/gedung
Bandwidth	Kapasitas maksimal data yang dapat ditransmisikan melalui suatu media dalam satuan waktu tertentu
Cable Tester	Alat ukur untuk menguji kontinuitas dan urutan pemasangan kabel tembaga
Cladding	Lapisan kaca di sekeliling core pada kabel fiber optik yang memantulkan cahaya secara total
Cleaver	Alat presisi untuk memotong ujung serat fiber optik agar rata dan tegak lurus
Core	Inti kaca/plastik tempat cahaya merambat pada kabel fiber optik
Crosstalk	Interferensi sinyal antar pasangan kabel yang berdekatan dalam satu kabel
DCE (Data Communication Equipment)	Perangkat pada koneksi Serial yang menyediakan sinyal clock
DTE (Data Terminal Equipment)	Perangkat pada koneksi Serial yang mengikuti sinyal clock dari sisi DCE
DMZ (Demilitarized Zone)	Segmen jaringan perantara yang menampung server yang perlu diakses dari luar, terisolasi dari jaringan internal
EtherChannel	Teknik Cisco untuk menggabungkan beberapa link fisik menjadi satu link logis
Fusion Splicing	Metode penyambungan fiber optik dengan melelehkan ujung serat menggunakan busur listrik
Hub-and-Spoke	Arsitektur jaringan dengan satu titik pusat terhubung ke beberapa titik cabang
LACP (Link Aggregation Control Protocol)	Protokol standar terbuka IEEE 802.3ad untuk negosiasi EtherChannel
Leased Line	Jalur komunikasi yang disewa secara eksklusif dari penyedia layanan telekomunikasi
Line-of-Sight	Garis pandang langsung tanpa penghalang antara dua titik, disyaratkan pada tautan nirkabel outdoor
Mechanical Splicing	Metode penyambungan fiber optik menggunakan penjepit mekanis tanpa peleburan
OTDR (Optical Time Domain Reflectometer)	Alat ukur untuk menguji kualitas dan menemukan titik masalah pada kabel fiber optik
PAgP (Port Aggregation Protocol)	Protokol proprietary Cisco untuk negosiasi EtherChannel

Istilah	Penjelasan Singkat
Point-to-Multipoint (PtMP)	Konfigurasi tautan nirkabel yang menghubungkan satu titik pusat dengan banyak titik cabang
Point-to-Point (PtP)	Konfigurasi tautan yang menghubungkan tepat dua lokasi secara langsung
Port Security	Fitur switch yang membatasi jumlah/jenis MAC address yang diizinkan pada suatu port
RJ45	Jenis konektor standar yang digunakan pada kabel UTP/STP untuk jaringan Ethernet
Rogue Access Point	Access point tidak sah yang dipasang tanpa izin untuk menyusup ke jaringan
RSSI (Received Signal Strength Indicator)	Indikator kekuatan sinyal yang diterima, diukur dalam satuan dBm
SSID (Service Set Identifier)	Nama jaringan nirkabel yang terlihat oleh perangkat pengguna
Site Survey	Proses pemetaan dan analisis kondisi sinyal wireless pada suatu area
Spanning Tree Protocol (STP)	Protokol layer 2 yang mencegah loop pada jaringan switch dengan jalur redundan
Splicing	Proses penyambungan dua ujung serat fiber optik
Structured Cabling	Pendekatan standar merancang infrastruktur pengkabelan gedung yang terorganisasi
T568A / T568B	Dua standar urutan warna kabel UTP pada konektor RJ45 menurut TIA/EIA-568
Telecommunications Room (TR)	Ruangan pada tiap lantai/area yang menampung perangkat distribusi jaringan
WPA2 / WPA3	Protokol keamanan jaringan nirkabel yang digunakan untuk mengenkripsi lalu lintas Wi-Fi

21.5 Lampiran: Ringkasan Perintah CLI Cisco IOS

Lampiran berikut merangkum perintah-perintah CLI Cisco IOS yang paling sering digunakan sepanjang buku ini, disusun sebagai lembar rujukan cepat (quick reference) bagi peserta didik saat praktik maupun menghadapi kompetisi keahlian.

Kategori	Perintah	Fungsi Singkat
Mode Dasar	enable	Masuk ke mode privileged EXEC
Mode Dasar	configure terminal	Masuk ke mode global configuration
Identitas	hostname <nama>	Mengatur nama perangkat
Interface	interface <nama>	Masuk ke mode konfigurasi interface

Kategori	Perintah	Fungsi Singkat
Interface	ip address <ip> <mask>	Menetapkan alamat IP pada interface
Interface	no shutdown	Mengaktifkan interface
Interface Serial	clock rate <angka>	Menetapkan clock pada sisi DCE
Routing	ip route <network> <mask> <next-hop>	Menambahkan rute statis
VLAN	vlan <nomor>	Membuat VLAN baru
VLAN	switchport mode access/trunk	Mengatur mode port switch
EtherChannel	channel-group <nomor> mode active	Menggabungkan interface ke EtherChannel (LACP)
Keamanan	crypto key generate rsa	Membuat kunci enkripsi untuk SSH
Keamanan	switchport port-security	Mengaktifkan port security
Verifikasi	show ip interface brief	Menampilkan ringkasan status interface
Verifikasi	show interfaces	Menampilkan detail status dan statistik interface
Verifikasi	show cdp neighbors	Menampilkan perangkat Cisco tetangga
Verifikasi	show ip route	Menampilkan tabel routing
Verifikasi	show vlan brief	Menampilkan ringkasan VLAN pada switch
Verifikasi	show etherchannel summary	Menampilkan ringkasan status EtherChannel
Verifikasi	show running-config	Menampilkan konfigurasi yang sedang berjalan

21.6 Lampiran: Daftar Singkatan

Singkatan	Kepanjangan
AP	Access Point
DCE	Data Communication Equipment
DTE	Data Terminal Equipment
EF	Entrance Facility
ER	Equipment Room
IEEE	Institute of Electrical and Electronics Engineers
LACP	Link Aggregation Control Protocol
LC	Lucent Connector
MMF	Multi-Mode Fiber

Singkatan	Kepanjangan
OTDR	Optical Time Domain Reflectometer
PAgP	Port Aggregation Protocol
PoE	Power over Ethernet
PtMP	Point-to-Multipoint
PtP	Point-to-Point
RSSI	Received Signal Strength Indicator
SC	Subscriber Connector
SMF	Single-Mode Fiber
SSID	Service Set Identifier
STP (protokol)	Spanning Tree Protocol
STP (kabel)	Shielded Twisted Pair
TIA/EIA	Telecommunications Industry Association / Electronic Industries Alliance
TR	Telecommunications Room
UTP	Unshielded Twisted Pair
VFL	Visual Fault Locator
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

21.7 Lampiran: Checklist Instalasi dan Troubleshooting

Checklist berikut dapat digunakan peserta didik maupun guru sebagai panduan langkah demi langkah saat melakukan praktik instalasi maupun troubleshooting, memastikan tidak ada tahapan penting yang terlewat.

Checklist Instalasi Kabel Tembaga

No	Item Pemeriksaan
1	Kategori kabel sesuai kebutuhan (mis. Cat6 untuk Gigabit)
2	Urutan warna kabel sesuai standar T568A/T568B yang dipilih
3	Panjang kupasan jaket sesuai (tidak berlebihan)
4	Seluruh kabel menyentuh ujung konektor sebelum crimping
5	Hasil crimping diuji dengan cable tester (tidak ada open/short/miswire)

Checklist Konfigurasi Perangkat Jaringan (Cisco IOS)

No	Item Pemeriksaan
1	Hostname dan domain-name telah dikonfigurasi
2	Password enable secret, console, dan vty telah diatur
3	Alamat IP dan subnet mask sesuai tabel pengalamatan
4	Interface telah diaktifkan (no shutdown)
5	Status interface terverifikasi up/up (show ip interface brief)
6	Konektivitas end-to-end terverifikasi (ping/traceroute)
7	Konfigurasi telah disimpan (copy running-config startup-config)

Checklist Instalasi dan Keamanan Access Point

No	Item Pemeriksaan
1	Lokasi pemasangan mempertimbangkan cakupan dan penghalang
2	SSID telah dikonfigurasi sesuai penamaan yang ditentukan
3	Channel dipilih berdasarkan hasil pemindaian (minim interferensi)
4	Mode keamanan WPA2/WPA3 telah diaktifkan dengan passphrase kuat
5	Kredensial administratif default telah diganti
6	Perangkat client berhasil terhubung dan memperoleh alamat IP

21.8 Lampiran: Konvensi Penamaan Perangkat pada Topologi LKS

Naskah soal LKS Bidang IT Network System Administration umumnya menggunakan konvensi penamaan perangkat yang konsisten untuk memudahkan peserta memahami peran setiap perangkat dalam topologi multi-cabang. Pemahaman konvensi ini membantu peserta didik lebih cepat beradaptasi saat membaca topologi soal kompetisi yang sesungguhnya.

Pola Penamaan	Arti	Contoh
R-CORE / R-HQ	Router pada kantor pusat (Head Quarter/Core)	R-CORE
R-BRT, R-TMT, dsb.	Router pada kantor cabang, disingkat dari nama arah/lokasi (Barat, Timur)	R-BRT (cabang Barat), R-TMT (cabang Timur)
SW-<lokasi>	Switch pada suatu lokasi/segmen jaringan	SW-CORE, SW-BRT
PC-<kode>	Perangkat end-device (client) pada suatu segmen	PC-A, PC-B1
Se0/0/0, Se0/0/1	Interface Serial pada router, umumnya digunakan untuk link WAN	Se0/0/0 (link ke cabang pertama)

Pola Penamaan	Arti	Contoh
Gi0/0, Fa0/0	Interface GigabitEthernet/FastEthernet, umumnya digunakan untuk LAN	Gi0/0 (uplink ke switch LAN)

Membiasakan diri membaca dan menginterpretasikan konvensi penamaan seperti ini sejak awal pembelajaran akan sangat membantu peserta didik saat menghadapi tekanan waktu pada kompetisi keahlian, karena tidak perlu lagi menerka-nerka peran setiap perangkat dari nolnya.

21.9 Daftar Pustaka

Materi dalam buku ini disusun dan dikembangkan mengacu pada Capaian Pembelajaran mata pelajaran Teknologi Jaringan Kabel dan Nirkabel Kurikulum Merdeka untuk SMK Program Keahlian Teknik Jaringan Komputer dan Telekomunikasi kelas XI-XII, serta Naskah Soal Lomba Kompetensi Siswa (LKS) SMK Tingkat Kabupaten Tasikmalaya Tahun 2026 Bidang IT Network System Administration (Modul B: Cisco Packet Tracer).

- Cisco Networking Academy. Introduction to Networks (ITN) & Connecting Networks Companion Guide. Cisco Press.
- Cisco Systems. Cisco IOS Command Reference. Dokumentasi resmi Cisco (cisco.com).
- TIA/EIA-568 Commercial Building Telecommunications Cabling Standard. Telecommunications Industry Association.
- IEEE 802.11 Working Group. Wireless LAN Standards Documentation. Institute of Electrical and Electronics Engineers.
- Sofana, Iwan. CISCO CCNA & Jaringan Komputer. Bandung: Informatika, 2017.
- Wi-Fi Alliance. WPA3 Specification Overview. Dokumentasi resmi Wi-Fi Alliance (wi-fi.org).

Guru disarankan melengkapi referensi dengan dokumentasi resmi Cisco Packet Tracer, standar TIA/EIA terbaru, serta perangkat access point yang tersedia di sekolah untuk memastikan materi tetap relevan dengan perkembangan teknologi terbaru.

MODUL TAMBAHAN TJKT — KELAS XII

Simulasi MikroTik dengan GNS3

Panduan Instalasi GNS3 (Windows & Ubuntu) dan Praktik Terpadu Berbasis Materi Buku MTCNA & MTCRE

Pendamping Praktik untuk Mata Pelajaran Administrasi Sistem Jaringan & Keamanan Jaringan

Kompetensi Keahlian Teknik Jaringan Komputer dan Telekomunikasi (TJKT)

Kata Pengantar

Modul ini adalah pendamping praktik dari Buku MTCRE, disusun khusus untuk mengatasi keterbatasan jumlah RouterBOARD fisik yang umum dihadapi sekolah. Menggunakan GNS3 (network emulator gratis dan open-source) yang menjalankan RouterOS asli melalui image CHR (Cloud Hosted Router), peserta didik dapat membangun topologi dengan banyak router MikroTik sekaligus hanya menggunakan satu unit laptop/PC.

Modul dibuka dengan panduan instalasi GNS3 lengkap untuk Windows maupun Ubuntu Linux, dilanjutkan dengan rangkaian lab praktik yang disusun mengikuti urutan Buku MTCRE untuk Kelas XII. Setiap bab praktik diawali kotak "Pengenalan Awal MikroTik" yang menyegarkan kembali konsep terkait sebelum masuk ke langkah teknis GNS3.

Penting dipahami sejak awal: GNS3 BUKAN pengganti hardware fisik sepenuhnya. Topik Wireless (802.11) tetap wajib dipraktikkan menggunakan RouterBOARD fisik sungguhan karena keterbatasan virtual machine yang tidak memiliki perangkat radio. Modul ini dirancang sebagai PENGALI kesempatan praktik untuk materi routing, firewall, VPN, VLAN, dan OSPF/BGP/MPLS — bukan pengganti seluruh praktik hardware.

Selamat membangun topologi jaringan tanpa batas, dan semoga modul ini mempercepat penguasaan kompetensi MTCRE peserta didik Kelas XII.

Daftar Isi

Catatan: nomor halaman rinci per sub-bab dapat ditampilkan otomatis melalui menu References > Table of Contents > Update Table apabila dokumen dibuka di Microsoft Word.

BAB 1

Mengapa Simulasi GNS3 untuk Belajar MikroTik

Memahami posisi GNS3 sebagai jembatan antara teori dan praktik saat perangkat RouterBOARD fisik terbatas jumlahnya di sekolah.

Tujuan Pembelajaran

Peserta memahami konsep dasar network simulator/emulator, mengapa GNS3 dipilih untuk simulasi MikroTik, serta topik mana saja dari Buku MTCNA dan MTCRE yang cocok dan tidak cocok disimulasikan di GNS3.

1.1 Masalah Klasik: Perangkat Fisik Terbatas

Salah satu tantangan terbesar pembelajaran jaringan di SMK adalah keterbatasan jumlah RouterBOARD fisik. Banyak lab pada Buku MTCNA dan MTCRE membutuhkan 3-4 router sekaligus (misalnya lab OSPF multi-area atau SuperLab multi-cabang), sementara sekolah mungkin hanya memiliki beberapa unit RouterBOARD untuk digunakan bergantian oleh puluhan siswa. Simulasi jaringan hadir sebagai solusi: siswa dapat membangun topologi kompleks dengan banyak "router" sekaligus, menggunakan satu laptop/PC saja.

1.2 Emulator vs Simulator vs Cloud Testing

Pendekatan	Penjelasan	Contoh
Simulator murni	Meniru perilaku perangkat tanpa menjalankan OS sungguhan — terbatas fitur, cocok untuk konsep dasar saja	Cisco Packet Tracer
Emulator	Menjalankan OS/firmware ASLI (image sungguhan) di dalam virtual machine — perilaku identik dengan perangkat fisik	GNS3 + MikroTik CHR, GNS3 + Cisco IOS
Cloud/Virtual Lab	Menyewa akses ke perangkat virtual di server pihak ketiga	MikroTik Cloud Lab, EVE-NG Cloud

GNS3 termasuk kategori emulator: ia tidak "berpura-pura" menjadi MikroTik, melainkan benar-benar menjalankan RouterOS asli (dalam bentuk image CHR) di dalam virtual machine. Ini berarti SELURUH perintah, perilaku, bahkan bug sekalipun akan identik persis dengan RouterBOARD fisik sungguhan — berbeda dengan simulator seperti Packet Tracer yang hanya meniru sebagian perilaku dan sering tidak mendukung fitur RouterOS versi terbaru.

1.3 Apa itu MikroTik CHR (Cloud Hosted Router)?

CHR adalah versi RouterOS yang dikemas khusus untuk dijalankan sebagai virtual machine (bukan pada RouterBOARD fisik) — dapat berjalan di VMware, VirtualBox, Proxmox, Hyper-V, cloud provider, dan tentu saja GNS3. CHR inilah yang akan kita gunakan sepanjang modul ini sebagai "router MikroTik virtual" di dalam GNS3. Seperti dibahas pada Buku MTCNA Bab 1, CHR menggunakan sistem lisensi yang sama dengan RouterOS pada umumnya — versi gratis (tanpa lisensi berbayar) memiliki batasan throughput (dibatasi sekitar 1 Mbps setelah reboot) namun tetap penuh dari sisi fitur,

sehingga sangat cukup untuk kebutuhan pembelajaran karena kita tidak menguji kecepatan transfer data sungguhan, melainkan mempelajari logika konfigurasi.

1.4 Peta Kompatibilitas: Materi Mana yang Cocok di GNS3?

Karena CHR berjalan sebagai virtual machine tanpa perangkat keras wireless fisik, TIDAK SEMUA materi pada kedua buku dapat disimulasikan di GNS3. Berikut peta kompatibilitasnya:

Sumber	Topik	Kompatibel GNS3?
MTCNA Bab 3	Konfigurasi Dasar Router & NAT	✅ Sangat cocok
MTCNA Bab 4	DHCP Server & Client	✅ Sangat cocok
MTCNA Bab 7	Routing Dasar & Failover	✅ Sangat cocok
MTCNA Bab 8	Bridging & Switching	✅ Cocok
MTCNA Bab 9	Wireless 802.11	❌ TIDAK cocok — CHR tidak memiliki interface wireless
MTCNA Bab 10	Firewall dan NAT	✅ Sangat cocok
MTCNA Bab 11	QoS (Simple Queue, Queue Tree)	✅ Cocok (throughput terbatas lisensi gratis, namun logika konfigurasi tetap valid)
MTCNA Bab 12	VPN Dasar (PPTP/SSTP/PPPoE)	✅ Sangat cocok
MTCRE Bab 2-3	Policy Routing & Load Balancing	✅ Sangat cocok — justru topik terbaik untuk GNS3 karena butuh banyak router
MTCRE Bab 4-5	Tunnel & VPN Lanjutan (IPSec)	✅ Sangat cocok
MTCRE Bab 6	VLAN & QinQ	✅ Cocok
MTCRE Bab 7-8	OSPF Fundamentals & Lanjutan	✅ SANGAT cocok — topik paling ideal untuk GNS3
MTCRE Bab 9-10	BGP & MPLS (pengayaan)	✅ Cocok

Catatan Penting

Karena keterbatasan wireless, modul ini TIDAK menyertakan lab GNS3 untuk topik Wireless (MTCNA Bab 9). Topik tersebut tetap wajib dipraktikkan menggunakan RouterBOARD wireless fisik sungguhan. Sebaliknya, hampir seluruh materi MTCRE justru LEBIH IDEAL dipelajari lewat GNS3 dibanding hardware fisik, karena kebutuhan jumlah router yang banyak untuk topologi multi-cabang/multi-area.

Penerapan di Industri — GNS3 sebagai Standar Latihan Calon Network Engineer

Sebelum terjun ke proyek nyata di client, hampir seluruh Network Engineer profesional membiasakan diri merancang dan menguji topologi kompleks terlebih dahulu di GNS3 atau EVE-NG, karena jauh lebih murah dan cepat dibanding membeli/menyewa banyak perangkat fisik hanya untuk uji coba. Kemampuan menggunakan GNS3 secara mahir menjadi nilai tambah tersendiri saat

wawancara kerja di perusahaan System Integrator atau ISP, karena menunjukkan kebiasaan kerja yang efisien dan terbiasa dengan tooling standar industri.

☑ Uji Pemahaman

1. Jelaskan perbedaan mendasar antara simulator (seperti Packet Tracer) dan emulator (seperti GNS3).

2. Apa itu MikroTik CHR dan mengapa image ini yang dipakai di GNS3, bukan image RouterBOARD biasa?

3. Sebutkan minimal 3 topik dari Buku MTCNA/MTCRE yang PALING cocok disimulasikan di GNS3, dan jelaskan alasannya.

4. Mengapa topik Wireless (Bab 9 MTCNA) tidak dapat disimulasikan di GNS3?

BAB 2

Instalasi GNS3 di Windows

Langkah lengkap memasang GNS3 pada sistem operasi Windows, termasuk komponen pendukung yang sering terlewat oleh pemula.

Tujuan Pembelajaran

Peserta mampu memasang GNS3 Desktop beserta GNS3 VM di Windows, dan memahami mengapa GNS3 VM diperlukan untuk performa emulasi yang optimal.

2.1 Kebutuhan Sistem (Persyaratan Minimum)

Komponen	Minimum yang Disarankan
Sistem Operasi	Windows 10/11 64-bit
RAM	Minimal 8 GB (16 GB lebih nyaman untuk topologi banyak router)
Virtualisasi CPU (VT-x/AMD-V)	WAJIB aktif di BIOS/UEFI
Software Virtualisasi	VMware Workstation Player/Pro ATAU VirtualBox (salah satu)
Ruang Penyimpanan	Minimal 10 GB kosong untuk GNS3 VM + image CHR

Mengapa Virtualisasi CPU Wajib Aktif?

GNS3 VM dan MikroTik CHR sama-sama berjalan sebagai virtual machine yang membutuhkan dukungan virtualisasi hardware (Intel VT-x atau AMD-V) dari prosesor. Jika fitur ini tidak aktif di BIOS, proses emulasi akan sangat lambat atau bahkan gagal total. Pengaturan ini biasanya ditemukan di menu BIOS/UEFI dengan nama "Virtualization Technology", "VT-x", "SVM Mode", atau "AMD-V", tergantung merek motherboard.

2.2 Dua Komponen Utama: GNS3 GUI dan GNS3 VM

Pemula sering mengira GNS3 hanya satu aplikasi tunggal, padahal instalasi GNS3 yang optimal di Windows terdiri dari dua bagian terpisah:

- GNS3 GUI (GNS3 Desktop) — aplikasi utama tempat kita menggambar topologi, menghubungkan perangkat, dan membuka console. Berjalan langsung di Windows.
- GNS3 VM — sebuah virtual machine terpisah (berbasis Linux) yang sebenarnya menjalankan seluruh proses emulasi (termasuk CHR MikroTik) di baliknya. GNS3 GUI di Windows hanya "mengendalikan" GNS3 VM ini dari jarak dekat.

Alasan pemisahan ini adalah karena teknologi virtualisasi hardware (KVM) yang dibutuhkan untuk performa emulasi terbaik bekerja jauh lebih baik di lingkungan Linux dibanding native Windows — sehingga GNS3 "menitipkan" seluruh beban emulasi ke GNS3 VM berbasis Linux tersebut, sementara Windows hanya menjadi tampilan (GUI) pengendalinya.

2.3 Langkah Instalasi

1. Unduh installer GNS3 untuk Windows dari situs resmi https://www.gns3.com/software/download (perlu membuat akun gratis terlebih dahulu).
2. Unduh juga file GNS3 VM (dalam format .ova) dari halaman unduhan yang sama, pilih versi sesuai software virtualisasi yang akan dipakai (VMware atau VirtualBox).
3. Jalankan installer GNS3 GUI, ikuti wizard instalasi standar (Next-Next-Finish). Saat diminta memilih komponen tambahan, centang Wireshark jika ingin mampu menangkap paket data langsung dari GNS3.
4. Instal VMware Workstation Player (gratis untuk penggunaan non-komersial) atau VirtualBox, pilih salah satu saja.
5. Import file GNS3 VM (.ova) ke dalam VMware/VirtualBox: buka VMware/VirtualBox, pilih menu Import/Open, arahkan ke file .ova yang telah diunduh.
6. Nyalakan GNS3 VM tersebut, biarkan proses booting selesai hingga menampilkan layar dengan informasi IP address GNS3 VM.
7. Buka aplikasi GNS3 GUI di Windows, pada wizard awal pilih "Run appliances in a virtual machine", lalu pilih GNS3 VM yang baru saja dijalankan.
8. GNS3 GUI akan otomatis terhubung ke GNS3 VM. Jika berhasil, indikator koneksi di pojok kanan bawah GNS3 GUI akan berwarna hijau.

Alternatif: Local Server (Tanpa GNS3 VM)

Bagi laptop dengan RAM terbatas, GNS3 juga bisa dijalankan menggunakan "Local Server" (menjalankan emulasi langsung di Windows tanpa GNS3 VM terpisah), namun mode ini membutuhkan instalasi tambahan seperti Npcap dan sedikit lebih rumit untuk dikonfigurasi, serta performa emulasi router non-MikroTik seperti Cisco IOS bisa kurang stabil. Untuk pemula, menggunakan GNS3 VM tetap menjadi pilihan yang lebih direkomendasikan.

LAB: Verifikasi Instalasi GNS3 di Windows

1. Pastikan GNS3 VM menyala dan GNS3 GUI menunjukkan indikator koneksi hijau di pojok kanan bawah.

2. Buat proyek baru melalui menu File > New Blank Project, beri nama "TesInstalasi".

3. Seret (drag) ikon Cloud dari panel kiri ke kanvas kerja — ini mewakili koneksi ke jaringan fisik/internet laptop Anda.

4. Klik kanan pada kanvas kosong, pilih "Show/Hide interface labels" untuk memastikan tampilan topologi berjalan normal.

5. Simpan proyek, tutup dan buka kembali GNS3 untuk memastikan proyek tersimpan dengan benar.

Uji Pemahaman

1. Mengapa GNS3 di Windows umumnya membutuhkan dua komponen terpisah: GNS3 GUI dan GNS3 VM?

2. Apa yang terjadi jika Virtualisasi CPU (VT-x/AMD-V) tidak diaktifkan di BIOS sebelum menjalankan GNS3?

3. Sebutkan dua pilihan software virtualisasi yang dapat dipasangkan dengan GNS3 VM di Windows.

BAB 3

Instalasi GNS3 di Ubuntu Linux

Memasang GNS3 secara native di Ubuntu, memanfaatkan dukungan KVM langsung tanpa memerlukan GNS3 VM terpisah seperti di Windows.

Tujuan Pembelajaran

Peserta mampu memasang GNS3 di Ubuntu Linux menggunakan repository resmi, mengaktifkan dukungan KVM, dan memahami keunggulan performa dibanding instalasi di Windows.

3.1 Keunggulan GNS3 di Linux

Berbeda dengan Windows yang memerlukan GNS3 VM terpisah untuk performa optimal, di Ubuntu Linux, GNS3 dapat langsung memanfaatkan KVM (Kernel-based Virtual Machine) yang tertanam di kernel Linux itu sendiri — sehingga tidak diperlukan lagi virtual machine tambahan hanya untuk menjalankan mesin emulasi. Ini membuat instalasi lebih ringan dan performa emulasi CHR MikroTik biasanya terasa lebih responsif dibanding di Windows dengan spesifikasi laptop yang sama.

3.2 Kebutuhan Sistem

Komponen	Minimum yang Disarankan
Sistem Operasi	Ubuntu 22.04 LTS atau lebih baru (64-bit)
RAM	Minimal 8 GB
Dukungan KVM	Prosesor mendukung virtualisasi (Intel VT-x / AMD-V), diaktifkan di BIOS
Hak akses	Akun dengan akses sudo untuk instalasi paket

3.3 Langkah Instalasi

```
# 1. Tambahkan repository resmi GNS3 (PPA)
sudo add-apt-repository ppa:gns3/ppa
sudo apt update

# 2. Instal GNS3 GUI dan GNS3 Server sekaligus
sudo apt install gns3-gui gns3-server

# 3. Tambahkan user Anda ke group "kvm" dan "wireshark" agar punya izin akses
sudo usermod -aG kvm $USER
sudo usermod -aG wireshark $USER
sudo usermod -aG ubridge $USER

# 4. Logout lalu login kembali (atau restart) agar perubahan group berlaku
reboot
```

3.4 Verifikasi Dukungan KVM

Sebelum menjalankan GNS3, pastikan dahulu KVM benar-benar aktif dan dapat diakses oleh user Anda, karena tanpa KVM, CHR MikroTik tidak akan bisa dijalankan sama sekali (atau berjalan sangat lambat menggunakan emulasi software murni).

```
kvm-ok
# Output yang diharapkan:
# INFO: /dev/kvm exists
# KVM acceleration can be used

# Jika perintah kvm-ok tidak ditemukan, instal terlebih dahulu:
sudo apt install cpu-checker
```

Jika KVM Tidak Terdeteksi

Jika "kvm-ok" menunjukkan KVM tidak dapat digunakan, penyebab paling umum adalah Virtualisasi CPU belum diaktifkan di BIOS/UEFI, atau — pada kasus laptop yang menjalankan Ubuntu di dalam virtual machine lain (misalnya VMware di atas Windows) — virtualisasi bersarang (nested virtualization) belum diaktifkan pada VM tersebut.

3.5 Menjalankan GNS3 Pertama Kali

9. Buka aplikasi GNS3 dari menu aplikasi Ubuntu, atau ketik "gns3" di terminal.
10. Pada wizard konfigurasi awal (Setup Wizard), pilih opsi "Run appliances on my local computer" karena kita akan memanfaatkan KVM lokal, BUKAN GNS3 VM seperti di Windows.
11. GNS3 akan otomatis mendeteksi GNS3 Server lokal yang telah terpasang, klik Next hingga wizard selesai.
12. Pastikan indikator koneksi server di pojok kanan bawah aplikasi GNS3 berwarna hijau, menandakan GNS3 Server berjalan normal.

LAB: Verifikasi Instalasi GNS3 di Ubuntu

1. Jalankan "kvm-ok" di terminal, pastikan hasilnya menunjukkan KVM acceleration dapat digunakan.

2. Buka GNS3, buat proyek baru bernama "TesInstalasiUbuntu".

3. Periksa menu Edit > Preferences > Local Server, pastikan path server dan konfigurasi lain menunjuk ke instalasi lokal Ubuntu Anda.

4. Seret ikon Cloud ke kanvas kerja, verifikasi tidak ada pesan error yang muncul.

5. Simpan proyek untuk memastikan seluruh komponen bekerja normal sebelum lanjut ke Bab 4 (setup CHR).

Penerapan di Industri — Linux sebagai Standar Lab Jaringan Profesional

Banyak Network Engineer dan instruktur pelatihan jaringan profesional lebih memilih menjalankan GNS3/EVE-NG di atas server Linux (baik lokal maupun cloud) dibanding Windows, karena performa KVM native jauh lebih efisien saat menjalankan puluhan router virtual sekaligus untuk topologi skala

besar — sesuatu yang sering dibutuhkan saat merancang jaringan enterprise kompleks sebelum benar-benar diimplementasikan di lapangan.

☑ Uji Pemahaman

1. Mengapa instalasi GNS3 di Ubuntu tidak memerlukan GNS3 VM terpisah seperti di Windows?

2. Perintah apa yang digunakan untuk memverifikasi dukungan KVM di Ubuntu sebelum menjalankan GNS3?

3. Mengapa user perlu ditambahkan ke group "kvm" setelah instalasi GNS3 di Ubuntu?

BAB 4

Menyiapkan MikroTik CHR di GNS3 & Topologi Pertama

Mengimpor image RouterOS CHR ke dalam GNS3 sebagai template perangkat yang siap dipakai berulang kali di seluruh lab modul ini.

Tujuan Pembelajaran

Peserta mampu mengunduh dan mengimpor image CHR ke GNS3, membuat template MikroTik reusable, serta membangun dan menguji topologi GNS3 pertama dengan dua router MikroTik.

4.1 Mengunduh Image CHR

13. Kunjungi halaman resmi https://mikrotik.com/download.
14. Pada bagian "Cloud Hosted Router (CHR)", unduh file dengan format RAW disk image (.img.zip) — format ini yang paling universal untuk diimpor ke GNS3/QEMU.
15. Ekstrak file .zip tersebut hingga mendapatkan file .img mentah.

Lisensi CHR untuk Simulasi

Seperti dibahas di Bab 1, CHR tanpa lisensi berbayar tetap dapat digunakan penuh untuk kebutuhan pembelajaran, hanya dibatasi throughput sekitar 1 Mbps setelah reboot pertama. Karena tujuan modul ini adalah mempelajari LOGIKA konfigurasi (routing, firewall, VPN, dsb) dan bukan menguji kecepatan transfer data sungguhan, batasan ini tidak mengganggu proses pembelajaran sama sekali.

4.2 Mengimpor CHR sebagai Template GNS3

16. Di GNS3 GUI, buka menu Edit > Preferences > QEMU VMs, klik "New".
17. Beri nama template, misalnya "MikroTik CHR 7.x".
18. Pada pengaturan RAM, cukup alokasikan 128 MB per instance (CHR sangat ringan, cukup untuk kebutuhan lab pembelajaran meski topologi terdiri dari banyak router sekaligus).
19. Pada tahap pemilihan disk image, arahkan ke file .img CHR yang sudah diekstrak sebelumnya sebagai HDA disk image.
20. Pada bagian Network, atur jumlah adapter sesuai kebutuhan maksimal topologi Anda (disarankan minimal 4-8 adapter agar fleksibel untuk lab dengan banyak koneksi), dan pastikan tipe adapter diset ke "virtio-net-pci" untuk performa jaringan terbaik.
21. Simpan template. Template ini kini dapat di-drag berkali-kali ke kanvas kerja GNS3 untuk mewakili banyak router MikroTik sekaligus, tanpa perlu mengulang proses impor setiap kali.

4.3 Membangun Topologi Pertama: Dua Router Terhubung

22. Buat proyek baru, beri nama "Lab-Pertama-GNS3".
23. Seret dua node "MikroTik CHR" dari panel kiri ke kanvas, beri nama R1 dan R2.
24. Hubungkan kedua router dengan mengklik ikon kabel, lalu klik pada R1 (pilih interface ether1), lanjutkan klik ke R2 (pilih interface ether1) untuk membentuk link antar keduanya.
25. Klik kanan pada R1, pilih "Start" (atau start seluruh topologi sekaligus melalui tombol Play di

toolbar atas).

26. Tunggu proses booting CHR selesai (ditandai ikon node berubah menjadi hijau).
27. Klik kanan pada R1, pilih "Console" untuk membuka terminal CLI RouterOS — inilah console yang akan dipakai sepanjang modul ini untuk mengetik perintah, identik dengan New Terminal di Winbox.

```
; Di console R1:
/ip address add address=10.0.0.1/30 interface=ether1
/ping 10.0.0.2 count=1     ; pastikan belum berhasil, karena R2 belum dikonfigurasi

; Di console R2:
/ip address add address=10.0.0.2/30 interface=ether1

; Kembali ke R1, uji ulang:
/ping 10.0.0.2 count=4     ; sekarang harus berhasil
```

4.4 Menghubungkan GNS3 ke Winbox (Opsional)

Meski console bawaan GNS3 sudah cukup untuk mengetik perintah CLI, banyak siswa lebih nyaman menggunakan Winbox seperti pada praktik dengan hardware fisik. GNS3 mendukung ini melalui node "Cloud" yang dijembatani ke adapter jaringan lokal komputer, atau melalui fitur NAT node bawaan GNS3, sehingga Winbox di komputer host dapat terhubung langsung ke router CHR di dalam topologi GNS3.

```
; Tambahkan node "NAT" dari panel kiri GNS3, hubungkan ke salah satu router,
; lalu set IP address dengan DHCP client pada interface yang terhubung ke NAT
tersebut:
/ip dhcp-client add interface=ether2 disabled=no
/ip dhcp-client print   ; catat IP address yang didapat
; IP tersebut dapat langsung diakses dari Winbox di komputer host seperti biasa
```

LAB: Membangun dan Menguji Topologi 2 Router

1. Ikuti seluruh langkah 4.3 untuk membangun topologi R1-R2.

2. Tambahkan node "NAT" dari GNS3, hubungkan ke R1 melalui interface ether2.

3. Konfigurasikan DHCP client pada ether2 di R1, catat IP yang didapat.

4. Buka Winbox di komputer host, hubungkan ke IP tersebut, verifikasi Anda dapat login dan melihat konfigurasi R1 melalui GUI Winbox seperti biasa.

5. Simpan topologi ini sebagai template dasar — seluruh lab pada bab-bab berikutnya akan menggunakan pola serupa (beberapa router MikroTik + node NAT untuk akses Winbox).

Uji Pemahaman

1. Mengapa alokasi RAM 128MB per instance CHR sudah cukup untuk kebutuhan pembelajaran, berbeda dengan router fisik yang biasanya memiliki RAM lebih besar?

2. Apa fungsi node "NAT" pada topologi GNS3 dalam konteks mengakses router CHR melalui

Winbox?

3. Mengapa tipe adapter jaringan "virtio-net-pci" disarankan dibanding tipe adapter standar lain saat membuat template CHR?

BAB 11

GNS3 Lab — Policy Routing & Load Balancing (PCC)

Membangun topologi 2-ISP dari Buku MTCRE Bab 2-3 sepenuhnya di GNS3 — topik yang justru LEBIH mudah diuji di simulator dibanding hardware fisik karena kebutuhan banyak router sekaligus.

Tujuan Pembelajaran

Peserta mampu mengimplementasikan policy routing dan load balancing PCC di GNS3, serta menguji failover multi-ISP secara langsung.

Pengenalan Awal MikroTik

Ingat kembali Buku MTCRE Bab 2 (mangle mark-routing) dan Bab 3 (PCC dengan per-connection-classifier). Lab multi-ISP seperti ini sering sulit diuji dengan hardware fisik di sekolah (butuh 2 koneksi internet sungguhan), namun di GNS3 kita bisa membuat dua "ISP" virtual sekaligus tanpa biaya tambahan apa pun.

11.1 Topologi Lab

R-Client memiliki dua koneksi WAN menuju R-ISP1 dan R-ISP2 (masing-masing mensimulasikan ISP berbeda dengan subnet publik simulasi sendiri), serta satu interface LAN menuju beberapa VPCS.

11.2 Konfigurasi Dasar Kedua ISP

```
; R-Client:
/ip address add address=10.0.1.2/30 interface=ether1   ; ke ISP1
/ip address add address=10.0.2.2/30 interface=ether2   ; ke ISP2
/ip address add address=192.168.10.1/24 interface=ether3  ; LAN

/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
/ip firewall nat add chain=srcnat out-interface=ether2 action=masquerade
```

11.3 Konfigurasi PCC (Persis Buku MTCRE Bab 3)

```
/ip firewall mangle add chain=prerouting in-interface=ether3 dst-address-type=!local
per-connection-classifier=both-addresses:2/0 action=mark-connection new-connection-
mark=isp1-conn passthrough=yes
/ip firewall mangle add chain=prerouting in-interface=ether3 dst-address-type=!local
per-connection-classifier=both-addresses:2/1 action=mark-connection new-connection-
mark=isp2-conn passthrough=yes
/ip firewall mangle add chain=prerouting connection-mark=isp1-conn action=mark-routing
new-routing-mark=isp1-route passthrough=no
/ip firewall mangle add chain=prerouting connection-mark=isp2-conn action=mark-routing
new-routing-mark=isp2-route passthrough=no

/ip route add dst-address=0.0.0.0/0 gateway=10.0.1.1 routing-mark=isp1-route check-
```

```
gateway=ping
/ip route add dst-address=0.0.0.0/0 gateway=10.0.2.1 routing-mark=isp2-route check-
gateway=ping
/ip route add dst-address=0.0.0.0/0 gateway=10.0.1.1 distance=1 check-gateway=ping
/ip route add dst-address=0.0.0.0/0 gateway=10.0.2.1 distance=2 check-gateway=ping
```

🔧 LAB: Verifikasi Load Balancing dan Failover Multi-ISP

1. Bangun topologi 3 router + beberapa VPCS sesuai 11.1, konfigurasikan R-ISP1 dan R-ISP2 sebagai jaringan sederhana yang masing-masing memiliki "internet" simulasi sendiri (subnet berbeda mewakili tujuan eksternal).

2. Terapkan konfigurasi 11.2 dan 11.3 di R-Client.

3. Dari beberapa VPC berbeda, lakukan traceroute ke tujuan simulasi di jaringan ISP1 dan ISP2, verifikasi trafik terbagi sesuai algoritma PCC (kombinasi source-destination tertentu konsisten memilih jalur yang sama).

4. Matikan (stop) node R-ISP1 untuk mensimulasikan ISP1 down, verifikasi via "/ip route print" bahwa rute isp1-route menjadi tidak aktif, namun trafik yang tadinya lewat ISP1 kini gagal dialihkan otomatis KECUALI tabel main fallback (distance based) turut dikonfigurasi dengan benar — diskusikan bersama instruktur mengapa policy routing murni TIDAK otomatis failover tanpa rule tambahan di tabel main.

5. Nyalakan kembali R-ISP1, verifikasi trafik kembali normal.

🏭 Penerapan di Industri — GNS3 sebagai Sarana Latihan Sebelum Beli 2 Koneksi Internet Sungguhan

Banyak pemilik usaha kecil-menengah di Indonesia yang berencana menggabungkan dua langganan internet ragu berinvestasi sebelum yakin skema load balancing benar-benar berfungsi sesuai harapan. Teknisi yang mampu mendemonstrasikan simulasi PCC di GNS3 terlebih dahulu — menunjukkan bagaimana trafik akan terbagi dan bagaimana failover bekerja — dapat meyakinkan klien dengan bukti konkret sebelum klien mengeluarkan biaya berlangganan ISP kedua.

✓ Uji Pemahaman

1. Mengapa lab multi-ISP seperti ini justru lebih mudah dilakukan di GNS3 dibanding hardware fisik di banyak sekolah?

2. Jelaskan mengapa policy routing murni (berbasis routing-mark) tidak secara otomatis mendukung failover tanpa rute tambahan di tabel main.

3. Bagaimana PCC memastikan satu klien yang sama konsisten menggunakan jalur ISP yang sama?

BAB 12

GNS3 Lab — Tunnel (EoIP/GRE) dan VPN Lanjutan (IPSec)

Membangun tunnel Layer 2 dan Layer 3 dari Buku MTCRE Bab 4-5, lengkap dengan enkripsi IPSec, sepenuhnya disimulasikan tanpa perlu dua lokasi fisik terpisah.

Tujuan Pembelajaran

Peserta mampu membangun dan memverifikasi tunnel EoIP/GRE serta mengamankannya dengan IPSec di lingkungan GNS3.

Pengenalan Awal MikroTik

Ingat kembali Buku MTCRE Bab 4 (EoIP untuk penggabungan Layer 2, GRE untuk interoperabilitas dan dukungan multicast) dan Bab 5 (IPSec Phase 1/Phase 2 untuk enkripsi). GNS3 sangat ideal untuk lab ini karena "internet" penghubung kedua kantor dapat disimulasikan dengan router perantara sederhana, memungkinkan kita benar-benar MELIHAT paket GRE/ESP mengalir melalui Wireshark bawaan GNS3.

12.1 Topologi Lab

R-Kantor1 dan R-Kantor2 masing-masing memiliki LAN sendiri, terhubung melalui R-Internet (mewakili internet publik) di tengah. Tunnel EoIP/GRE akan dibangun melalui R-Internet ini, seolah kedua kantor berjauhan secara geografis.

12.2 Tunnel GRE dengan IPSec

```
; R-Kantor1 (IP publik simulasi: 100.64.0.1):
/interface gre add name=gre-ke-kantor2 local-address=100.64.0.1 remote-
address=100.64.0.2
/ip address add address=10.200.0.1/30 interface=gre-ke-kantor2

/ip ipsec profile add name=profile-kantor dh-group=modp2048 enc-algorithm=aes-256
/ip ipsec peer add name=peer-kantor2 address=100.64.0.2/32 profile=profile-kantor
/ip ipsec identity add peer=peer-kantor2 secret=RahasiaGNS3Lab
/ip ipsec proposal add name=proposal-kantor enc-algorithms=aes-256-cbc auth-
algorithms=sha256
/ip ipsec policy add src-address=100.64.0.1/32 dst-address=100.64.0.2/32 protocol=gre
peer=peer-kantor2 proposal=proposal-kantor

; R-Kantor2 (IP publik simulasi: 100.64.0.2) — konfigurasi cermin dari R-Kantor1
```

12.3 Verifikasi dengan Wireshark Bawaan GNS3

Salah satu fitur unggulan GNS3 adalah kemampuan "menyadap" (capture) trafik pada link mana pun dalam topologi hanya dengan klik kanan pada link tersebut, tanpa perlu port mirroring seperti pada jaringan fisik.

28. Klik kanan pada link antara R-Kantor1 dan R-Internet, pilih "Start capture".
29. GNS3 akan otomatis membuka Wireshark menampilkan trafik real-time pada link tersebut.
30. Kirim ping dari LAN Kantor1 menuju LAN Kantor2 melalui tunnel, amati di Wireshark bahwa paket yang lewat di link publik (menuju R-Internet) muncul sebagai paket ESP (terenkripsi) — BUKAN paket ICMP biasa yang bisa dibaca isinya, membuktikan IPSec benar-benar mengenkripsi trafik tunnel.

LAB: Membangun Tunnel Aman Antar 2 Kantor Simulasi

1. Bangun topologi 3 router (Kantor1, Internet, Kantor2) + LAN masing-masing kantor dengan 1 VPCS per lokasi.

2. Konfigurasikan IP publik simulasi pada interface yang menghadap R-Internet.

3. Terapkan konfigurasi GRE dan IPSec sesuai 12.2 pada kedua router kantor (cermin satu sama lain).

4. Tambahkan static route agar LAN kedua kantor saling mengenal melalui tunnel GRE.

5. Uji ping dari VPC Kantor1 ke VPC Kantor2, verifikasi berhasil.

6. Lakukan capture Wireshark sesuai 12.3, konfirmasi trafik pada link publik benar-benar terenkripsi (ESP), bukan GRE polos yang bisa dibaca isinya.

Studi Kasus Nyata — Membuktikan Enkripsi Bekerja, Bukan Sekadar Asumsi

Banyak admin jaringan pemula mengaktifkan IPSec dan berasumsi trafik otomatis aman tanpa pernah benar-benar memverifikasi menggunakan packet capture. Kemampuan menyadap trafik sendiri dan MELIHAT LANGSUNG bahwa paket benar-benar berbentuk ESP terenkripsi (bukan payload GRE polos) adalah keterampilan validasi yang membedakan admin yang benar-benar paham keamanan jaringan dengan yang hanya "asal ikuti tutorial" tanpa verifikasi.

Uji Pemahaman

1. Mengapa GRE dipilih dibanding EoIP untuk tunnel pada lab ini?

2. Bagaimana cara memverifikasi bahwa trafik tunnel benar-benar terenkripsi menggunakan fitur bawaan GNS3?

3. Apa yang akan terlihat di Wireshark pada link publik jika IPSec BELUM dikonfigurasi dengan benar?

BAB 13

GNS3 Lab — VLAN dan Inter-VLAN Routing

Mereplikasi segmentasi VLAN dari Buku MTCRE Bab 6, memanfaatkan node "Ethernet Switch" bawaan GNS3 yang mendukung VLAN tagging sederhana sebagai pelengkap CHR.

Tujuan Pembelajaran

Peserta mampu membangun topologi VLAN trunk/access menggunakan kombinasi CHR dan Ethernet Switch GNS3, serta mengimplementasikan inter-VLAN routing.

Pengenalan Awal MikroTik

Ingat kembali Buku MTCRE Bab 6: access port (untagged) untuk perangkat akhir, trunk port (tagged) untuk antar-perangkat jaringan, dan PVID untuk menentukan VLAN default suatu port. GNS3 menyediakan node "Ethernet Switch" bawaan yang mendukung VLAN access/trunk sederhana — bisa dikombinasikan dengan Bridge VLAN Filtering di CHR untuk topologi yang lebih realistis.

13.1 Topologi Lab

Satu router R1 sebagai gerbang inter-VLAN routing, terhubung via trunk ke node "Ethernet Switch" GNS3, yang kemudian memiliki beberapa port access menuju VPC1 (VLAN 10) dan VPC2 (VLAN 20).

13.2 Konfigurasi Ethernet Switch GNS3 (VLAN Access/Trunk)

Node Ethernet Switch dikonfigurasi langsung melalui GUI GNS3 (klik kanan node > Configure), bukan melalui CLI seperti RouterOS:

- Port menuju R1: set type "trunk", VLAN ID sesuai kebutuhan (bawaan biasanya 1 sebagai native, tambahkan konfigurasi trunk membawa VLAN 10 dan 20).
- Port menuju VPC1: set type "access", VLAN ID 10.
- Port menuju VPC2: set type "access", VLAN ID 20.

13.3 Konfigurasi VLAN dan Inter-VLAN Routing di R1

```
/interface vlan add name=vlan10 interface=ether1 vlan-id=10
/interface vlan add name=vlan20 interface=ether1 vlan-id=20
/ip address add address=192.168.10.1/24 interface=vlan10
/ip address add address=192.168.20.1/24 interface=vlan20
```

Alternatif: Bridge VLAN Filtering Penuh

Untuk latihan yang lebih mendalam mendekati Buku MTCRE Bab 6, seluruh proses VLAN tagging juga bisa dilakukan murni menggunakan 2-3 router CHR dengan Bridge VLAN Filtering (tanpa node Ethernet Switch sama sekali) — silakan ulangi lab ini menggunakan pendekatan tersebut sebagai latihan tambahan, persis seperti lab pada buku utama.

LAB: Verifikasi Isolasi VLAN dan Inter-VLAN Routing

1. Bangun topologi 13.1, konfigurasikan Ethernet Switch sesuai 13.2 dan R1 sesuai 13.3.

2. Set IP VPC1 di 192.168.10.10/24 (gateway 192.168.10.1) dan VPC2 di 192.168.20.10/24 (gateway 192.168.20.1).

3. Uji ping antar VPC1 dan VPC2 SEBELUM rute inter-VLAN aktif (harus gagal jika VLAN benar-benar terisolasi Layer 2).

4. Verifikasi ping dari VPC1 ke gateway-nya sendiri (192.168.10.1) dan dari VPC2 ke gateway-nya (192.168.20.1) berhasil.

5. Uji ping dari VPC1 ke VPC2 — kini harus berhasil melalui proses inter-VLAN routing di R1 (karena kedua VLAN sama-sama diarahkan melalui router yang sama).

Studi Kasus Nyata — Menguji Desain VLAN Sebelum Beli Switch Managed

Sekolah/perusahaan kecil yang berencana membeli switch managed untuk pertama kalinya (investasi cukup mahal) sering menggunakan GNS3 untuk menguji dahulu rencana pembagian VLAN mereka — memastikan skema VLAN ID, trunk, dan access port yang direncanakan benar-benar akan berfungsi seperti yang diharapkan, sebelum benar-benar menghabiskan anggaran untuk membeli perangkat.

Uji Pemahaman

1. Mengapa VPC1 dan VPC2 pada lab ini tidak bisa saling ping sebelum inter-VLAN routing dikonfigurasi?

2. Apa perbedaan cara konfigurasi VLAN pada node Ethernet Switch GNS3 dibanding pada Bridge VLAN Filtering CHR?

3. Jelaskan mengapa trunk port harus membawa kedua VLAN ID (10 dan 20) menuju R1.

BAB 14

GNS3 Lab — OSPF Single & Multi-Area

Topik paling ideal untuk GNS3: mereplikasi lab OSPF dari Buku MTCRE Bab 7-8 dengan leluasa menggunakan banyak router sekaligus, sesuatu yang hampir mustahil dilakukan dengan hardware fisik terbatas di kebanyakan sekolah.

Tujuan Pembelajaran

Peserta mampu membangun topologi OSPF single-area dan multi-area lengkap di GNS3, serta menguji konvergensi dan perilaku Stub Area secara langsung.

Pengenalan Awal MikroTik

Ingat kembali Buku MTCRE Bab 7 (neighbor adjacency, DR/BDR, konfigurasi single-area) dan Bab 8 (ABR, Stub Area, redistribusi). OSPF adalah topik yang PALING diuntungkan oleh simulasi GNS3 — lab multi-area yang butuh 4-6 router sekaligus sangat sulit direplikasi dengan hardware fisik terbatas, namun sangat mudah dan cepat dibangun di GNS3.

14.1 Topologi Lab Single-Area (3 Router Segitiga)

```
; Router A, B, C saling terhubung membentuk segitiga (persis Buku MTCRE Bab 7)
; Setelah IP address point-to-point dikonfigurasi pada tiap link:

; Di setiap router (ganti router-id sesuai masing-masing):
/routing ospf instance add name=default-instance router-id=1.1.1.1
/routing ospf area add name=backbone instance=default-instance area-id=0.0.0.0
/routing ospf interface-template add interfaces=ether1,ether2 area=backbone
```

LAB: Verifikasi Neighbor dan Konvergensi Single-Area

1. Bangun topologi segitiga 3 router di GNS3, konfigurasikan IP point-to-point pada tiap link.

2. Terapkan konfigurasi OSPF di atas pada ketiga router dengan router-id unik masing-masing.

3. Jalankan "/routing ospf neighbor print" di setiap router, verifikasi status "Full" pada seluruh pasangan neighbor.

4. Tambahkan loopback dengan IP unik pada tiap router, sertakan ke dalam OSPF, verifikasi ketiga router saling ping ke loopback satu sama lain.

5. Klik kanan pada salah satu LINK di GNS3, pilih Suspend untuk mensimulasikan kegagalan, ukur berapa detik yang dibutuhkan hingga "/ip route print" di router lain menunjukkan rute alternatif melalui router ketiga.

14.2 Topologi Lab Multi-Area (4 Router, 2 Area)

Router A-B di Area 0 (backbone), Router B-C di Area 1, Router C-D di Area 1 — persis skenario Buku MTCRE Bab 8, kini dibangun dalam hitungan menit di GNS3 tanpa perlu mengumpulkan 4 unit

RouterBOARD fisik sekaligus.

```
; Router B (berperan sebagai ABR):
/routing ospf area add name=area1 instance=default-instance area-id=0.0.0.1
/routing ospf interface-template add interfaces=ether-ke-A area=backbone
/routing ospf interface-template add interfaces=ether-ke-C area=area1

; Mengubah Area 1 menjadi Stub (dilakukan di SEMUA anggota Area 1, termasuk Router B
sebagai ABR):
/routing ospf area set area1 type=stub
```

LAB: Verifikasi Perilaku Stub Area

1. Bangun topologi 4 router sesuai 14.2, konfigurasikan pembagian area seperti dijelaskan.

2. Verifikasi seluruh neighbor Full dan seluruh router dapat saling ping ke seluruh subnet SEBELUM Area 1 diubah menjadi Stub.

3. Tambahkan satu static route percobaan di Router A (mewakili "rute dari luar OSPF"), lakukan redistribusi static di Router A, verifikasi rute tersebut muncul di Router C dan D (yang berada di Area 1).

4. Ubah Area 1 menjadi Stub Area di SELURUH router anggotanya (Router B, C, D), amati "/ip route print" di Router C dan D — rute static hasil redistribusi tadi HARUS MENGHILANG, digantikan satu default route menuju Router B.

5. Verifikasi Router C dan D tetap bisa mencapai tujuan static route tersebut MESKI rutenya tidak lagi terlihat detail, murni mengandalkan default route hasil Stub Area.

6. Diskusikan hasil pengamatan bersama kelompok: apa untung-rugi menerapkan Stub Area dalam skenario ini?

Penerapan di Industri — Merancang Arsitektur OSPF Sebelum Implementasi Nyata

Network Engineer yang merancang jaringan OSPF untuk klien dengan belasan cabang HAMPIR SELALU membangun terlebih dahulu model lengkap topologi tersebut di GNS3 untuk menguji pembagian area yang optimal, memprediksi perilaku konvergensi, dan memastikan desain Stub Area tidak menimbulkan masalah reachability yang tidak terduga — jauh lebih murah memperbaiki kesalahan desain di simulator dibanding setelah puluhan router fisik sudah terpasang di lapangan.

Uji Pemahaman

1. Mengapa lab OSPF multi-area sangat diuntungkan oleh simulasi GNS3 dibanding lab lain yang mungkin bisa memakai lebih sedikit router?

2. Apa yang terjadi pada rute hasil redistribusi static setelah Area 1 diubah menjadi Stub Area?

3. Bagaimana cara mensimulasikan kegagalan link di GNS3 untuk menguji kecepatan konvergensi OSPF?

BAB 15

GNS3 Lab — Pengenalan BGP dan MPLS

Menutup rangkaian lab Kelas XII dengan simulasi BGP dan MPLS dari Buku MTCRE Bab 9-10 (materi pengayaan), memanfaatkan kemudahan GNS3 dalam membangun topologi multi-AS.

Tujuan Pembelajaran

Peserta mampu membangun sesi eBGP sederhana dan mengaktifkan MPLS/LDP dasar di GNS3 sebagai bekal menuju jenjang MTCINE.

Pengenalan Awal MikroTik

Ingat kembali Buku MTCRE Bab 9 (eBGP, Private ASN, AS-Path) dan Bab 10 (LSR, LER, LDP). Kedua topik ini bersifat pengayaan, namun sangat cocok dipelajari lewat GNS3 karena topologi multi-AS/multi-LSR yang representatif membutuhkan cukup banyak router — persis kekuatan utama simulasi dibanding hardware fisik terbatas.

15.1 Lab eBGP: 2 AS Terhubung Langsung

```
; Router A (AS 65001):
/ip address add address=10.0.0.1/30 interface=ether1
/routing bgp connection add name=peer-b remote.address=10.0.0.2 remote.as=65002
local.as=65001

; Router B (AS 65002):
/ip address add address=10.0.0.2/30 interface=ether1
/routing bgp connection add name=peer-a remote.address=10.0.0.1 remote.as=65001
local.as=65002
```

LAB: Verifikasi Sesi eBGP dan Pertukaran Rute

1. Bangun topologi 2 router terhubung langsung, konfigurasikan sesuai 15.1.

2. Verifikasi status sesi melalui "/routing bgp connection print", pastikan menunjukkan "established".

3. Tambahkan loopback dengan IP berbeda di masing-masing router, redistribusikan ke BGP, verifikasi rute loopback Router A muncul di tabel routing Router B (dan sebaliknya).

4. Perluas topologi menjadi 3 AS berantai (A-B-C) untuk melihat bagaimana AS-Path bertambah panjang seiring rute "melompat" dari satu AS ke AS lain — amati melalui "/routing bgp advertisements print".

15.2 Lab MPLS Dasar dengan LDP

Gunakan kembali topologi OSPF single-area 3 router dari Bab 14 (karena MPLS selalu membutuhkan IGP yang sudah berjalan sebagai fondasinya).

```
; Di setiap router (yang sudah menjalankan OSPF dari Bab 14):
/mpls interface add interface=ether1
/mpls interface add interface=ether2
/mpls ldp set enabled=yes lsr-id=1.1.1.1 transport-address=1.1.1.1
/mpls ldp interface add interface=ether1
/mpls ldp interface add interface=ether2
```

LAB: Verifikasi LDP Neighbor dan Label Forwarding

1. Aktifkan MPLS dan LDP pada ketiga router topologi OSPF dari Bab 14 sesuai 15.2.

2. Verifikasi sesi LDP neighbor terbentuk melalui "/mpls ldp neighbor print".

3. Amati "/mpls forwarding-table print", identifikasi label yang otomatis terbentuk untuk rute-rute OSPF yang sudah ada.

4. Lakukan capture Wireshark pada salah satu link (seperti pada Bab 12) saat melakukan ping antar loopback router, coba identifikasi header MPLS label yang menyelimuti paket IP di dalamnya.

Studi Kasus Nyata — Simulasi Sebelum Ambil Sertifikasi MTCINE

Siswa yang berencana melanjutkan ke sertifikasi MTCINE setelah lulus MTCRE sering menggunakan GNS3 sebagai sarana latihan mandiri di rumah, karena topik BGP dan MPLS yang mendalam nyaris mustahil dipraktikkan dengan hardware fisik mengingat kebutuhan koneksi ke ASN publik sungguhan. Kebiasaan membangun topologi multi-AS di GNS3 sejak Kelas XII menjadi modal berharga bagi siswa yang ingin serius mendalami jenjang karier Internetworking Engineer.

Uji Pemahaman

1. Mengapa topologi 3-AS berantai lebih informatif untuk memahami AS-Path dibanding topologi 2-AS langsung?

2. Mengapa lab MPLS pada bab ini memanfaatkan ulang topologi OSPF dari Bab 14, bukan topologi baru?

3. Bagaimana cara memverifikasi keberadaan header MPLS label pada paket yang lewat menggunakan fitur bawaan GNS3?

BAB 16

Penutup — Materi yang Tetap Butuh Hardware Fisik & Ringkasan Modul

Menutup modul dengan kejujuran penting: GNS3 luar biasa untuk routing, namun bukan pengganti sepenuhnya untuk hardware fisik — terutama untuk topik Wireless.

Tujuan Pembelajaran

Peserta memahami batasan simulasi GNS3 secara utuh, mengetahui solusi alternatif untuk materi Wireless, serta memiliki peta jalan belajar gabungan GNS3 + hardware fisik yang seimbang.

16.1 Mengapa Wireless Tidak Bisa Disimulasikan di GNS3

CHR (Cloud Hosted Router) yang digunakan sepanjang modul ini adalah versi RouterOS untuk virtual machine, yang secara desain TIDAK memiliki driver maupun interface wireless sama sekali — karena virtual machine tidak memiliki radio/antena fisik untuk dijalankan wireless-nya. Ini berbeda total dengan topik routing/firewall/VPN yang murni bersifat "logika perangkat lunak" dan bisa berjalan identik baik di hardware fisik maupun virtual machine.

Aspek Wireless	Bisa Disimulasikan di GNS3?
Konfigurasi Security Profile (WPA2 dsb)	❌ Tidak — perintah ada, namun tidak ada radio untuk benar-benar mengujinya
Site survey (Scan, Snooper)	❌ Tidak — membutuhkan penerimaan sinyal RF sungguhan
Registration Table dengan client asli	❌ Tidak — tidak ada perangkat wireless yang benar-benar terhubung
NV2/TDMA behavior	❌ Tidak — perilaku timing sinyal radio tidak dapat disimulasikan software murni

16.2 Solusi: Kombinasi GNS3 + Hardware Fisik Bergantian

Pendekatan paling realistis untuk sekolah dengan keterbatasan RouterBOARD fisik adalah kombinasi strategis: gunakan GNS3 untuk SELURUH materi routing, firewall, VPN, VLAN, dan OSPF/BGP (yang jumlahnya jauh lebih banyak dan butuh banyak router sekaligus), lalu fokuskan RouterBOARD fisik yang terbatas jumlahnya KHUSUS untuk sesi praktik Wireless — di mana jumlah router yang dibutuhkan biasanya hanya 2 unit per kelompok (1 AP + 1 Station), jauh lebih hemat dibanding kebutuhan 4-6 router untuk lab OSPF multi-area.

Kebutuhan Praktik	Jumlah Router Dibutuhkan	Rekomendasi Platform
Lab OSPF Multi-Area (Bab 14)	4-6 router	GNS3 (mustahil pakai hardware terbatas)
Lab SuperLab Multi-Cabang	3+ router	GNS3
Lab Wireless PTP (Buku MTCNA Bab 9)	2 router wireless	Hardware fisik (wajib)

Kebutuhan Praktik	Jumlah Router Dibutuhkan	Rekomendasi Platform
Lab Firewall/NAT/VPN dasar	1-2 router	Boleh GNS3 ATAU hardware, keduanya setara

16.3 Alternatif Lain untuk Wireless: Simulator Khusus RF (Opsional)

Bagi sekolah yang ingin memperkenalkan konsep propagasi sinyal wireless secara visual sebelum praktik hardware, tersedia tools terpisah di luar GNS3 seperti aplikasi perencanaan wireless (contoh: Ubiquiti ISP Design Center atau software pemetaan RF lainnya) yang dapat memvisualisasikan cakupan sinyal berdasarkan parameter seperti tinggi antena dan daya pancar — namun ini bersifat pelengkap konsep, bukan pengganti praktik konfigurasi RouterOS wireless yang sesungguhnya, dan tidak dibahas mendalam dalam modul ini.

16.4 Ringkasan Peta Modul GNS3 Keseluruhan

Bab	Judul	Kelas	Sumber Materi Utama
1	Mengapa Simulasi GNS3	-	Pengantar
2-3	Instalasi Windows & Ubuntu	-	Pengantar
4	Setup CHR & Topologi Pertama	-	Pengantar
11	Policy Routing & Load Balancing	XII	MTCRE Bab 2-3
12	Tunnel & IPSec	XII	MTCRE Bab 4-5
13	VLAN & Inter-VLAN Routing	XII	MTCRE Bab 6
14	OSPF Single & Multi-Area	XII	MTCRE Bab 7-8
15	Pengenalan BGP & MPLS	XII	MTCRE Bab 9-10

Penerapan di Industri — Kombinasi Simulasi dan Hardware adalah Standar Industri

Bahkan di perusahaan besar sekalipun, Network Engineer profesional tidak pernah sepenuhnya meninggalkan pengujian hardware fisik — simulasi seperti GNS3 dipakai untuk memvalidasi logika desain dengan cepat dan murah, namun pengujian akhir (terutama untuk hal yang melibatkan sinyal fisik seperti wireless, kualitas kabel, atau interferensi elektromagnetik) tetap wajib dilakukan di hardware sungguhan sebelum sistem benar-benar dinyatakan siap produksi. Pola pikir "simulasi dulu, validasi hardware kemudian" inilah yang coba dibiasakan sejak dini melalui modul ini.

16.5 Rekomendasi Alur Belajar Gabungan

31. Kelas X: Pelajari Buku MTCNA Bab 1-4 dan Bab 8 menggunakan hardware fisik RouterBOARD (kelompok kecil bergantian), sambil mengenalkan instalasi GNS3 (Modul Bab 1-4) sebagai keterampilan tambahan.

32. Kelas XI Semester 1: Materi MTCNA Bab 5-7, 9-13 — KHUSUS Bab 9 (Wireless) tetap wajib hardware fisik, sisanya bisa memakai kombinasi GNS3 (Modul Bab 5-10) dan hardware bergantian.
33. Kelas XI Semester 2: Materi MTCRE Bab 1-8 — mayoritas menggunakan GNS3 (Modul Bab 11, 13-14) karena kebutuhan banyak router.
34. Kelas XII (3 bulan): Review cepat + Modul GNS3 Bab 12, 15 (Tunnel/IPSec, BGP/MPLS) + SuperLab MTCRE (dari Buku MTCRE Bab 11) dikerjakan penuh di GNS3 sebagai simulasi UKK, ditutup dengan uji sertifikasi.

Pesan Penutup

GNS3 bukan pengganti hardware fisik, melainkan PENGALI kesempatan praktik. Dengan satu laptop dan modul ini, seorang siswa kini dapat membangun dan menguji ulang topologi 6 router OSPF multi-area sebanyak yang ia mau, kapan pun ia mau — sesuatu yang mustahil dilakukan hanya dengan 2-3 unit RouterBOARD sekolah yang harus bergantian dengan puluhan siswa lain. Manfaatkan kombinasi keduanya secara bijak: GNS3 untuk eksplorasi dan pengulangan tanpa batas, hardware fisik untuk validasi akhir dan topik yang memang membutuhkannya seperti wireless.