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 1 - Untuk Kelas XI 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 MikroTik	-	Praktik GNS3

CATATAN: Bagian Daftar Isi dan Peta Kompetensi Buku di atas mengikuti buku aslinya secara utuh (Bab 1-21). Jilid ini (Jilid 1 - Kelas XI) hanya memuat Bab 1 sampai Bab 13.

BAB 1 — Pendahuluan

Tujuan Pembelajaran

- Guru memahami ruang lingkup dan kedudukan mata pelajaran Teknologi Jaringan Kabel dan Nirkabel dalam struktur kurikulum Program Keahlian TJKT.
- Guru memahami capaian pembelajaran (CP) mata pelajaran ini secara umum untuk kelas XI dan XII.
- Guru memahami cara menggunakan buku ini sebagai bahan ajar di kelas maupun laboratorium.

1.1 Kedudukan Mata Pelajaran

Teknologi Jaringan Kabel dan Nirkabel merupakan mata pelajaran lanjutan pada Program Keahlian TJKT kelas XI-XII yang membekali peserta didik dengan keterampilan instalasi fisik media transmisi (kabel tembaga dan fiber optik), konfigurasi logis perangkat jaringan kabel berskala menengah (termasuk koneksi WAN), serta perencanaan dan pengamanan jaringan nirkabel. Mata pelajaran ini melanjutkan fondasi yang telah dibangun pada mata pelajaran Jaringan Dasar di kelas X, dan menjadi jembatan menuju mata pelajaran Administrasi Infrastruktur Jaringan serta Perencanaan dan Pengalamatan Jaringan.

Berbeda dengan Jaringan Dasar yang berfokus pada konsep pengantar, mata pelajaran ini menuntut peserta didik menguasai keterampilan praktik fisik (memotong, mengupas, dan mengoneksikan kabel) sekaligus keterampilan konfigurasi perangkat jaringan berskala lebih kompleks, termasuk topologi multi-cabang yang menghubungkan kantor pusat dan kantor cabang melalui jalur WAN.

1.2 Dasar Penyusunan Materi

Naskah soal LKS SMK Bidang IT Network System Administration Modul B (Cisco Packet Tracer) memuat topologi jaringan multi-cabang dengan berbagai jenis koneksi fisik, yaitu Ethernet/Gigabit Ethernet untuk jaringan LAN dan Serial untuk jaringan WAN point-to-point. Namun karena simulasi Cisco Packet Tracer berfokus pada konfigurasi logis perangkat dan tidak mencakup praktik instalasi fisik kabel maupun jaringan nirkabel, materi buku ini disusun dalam dua kelompok: Target A (kompetensi jaringan kabel yang tersirat langsung dari soal LKS) dan Target B (materi instalasi fisik kabel serta jaringan nirkabel yang menjadi bagian standar mata pelajaran namun disusun mandiri mengacu pada Capaian Pembelajaran nasional).

1.3 Capaian Pembelajaran Umum

Pada akhir fase pembelajaran, peserta didik diharapkan mampu melakukan terminasi kabel tembaga dan fiber optik sesuai standar, menjelaskan konsep structured cabling, menguji kualitas kabel menggunakan alat ukur, mengonfigurasi interface Ethernet dan Serial pada perangkat jaringan, merancang topologi multi-cabang melalui jalur WAN, mengonfigurasi agregasi dan redundansi jalur kabel, memahami standar dan konsep jaringan nirkabel, memasang dan mengamankan access point, merencanakan cakupan sinyal, memahami tautan nirkabel outdoor, serta melakukan troubleshooting dasar pada jaringan kabel dan nirkabel.

1.4 Struktur Buku

Buku ini terdiri atas 21 bab yang disusun mengikuti urutan pembelajaran yang direkomendasikan pada dokumen target: dimulai dari dasar instalasi fisik kabel, dilanjutkan konsep dan konfigurasi logis kabel/WAN, kemudian jaringan nirkabel, dan ditutup dengan troubleshooting gabungan. Setiap bab memuat komponen berikut:

- Tujuan Pembelajaran — kompetensi yang ingin dicapai pada bab tersebut.
- Uraian Materi — penjelasan konsep dilengkapi tabel, spesifikasi teknis, dan contoh perintah CLI.
- Praktik/Aktivitas Pembelajaran — kegiatan praktik fisik (kabel, access point) maupun simulasi Cisco Packet Tracer.
- Rangkuman — inti sari materi untuk memudahkan review.
- Soal Latihan/Refleksi — bahan evaluasi formatif bagi peserta didik.

1.5 Petunjuk Penggunaan bagi Guru

1. Ajarkan Target B.1 (Bab 2–5) terlebih dahulu sebagai dasar keterampilan fisik instalasi kabel, karena keterampilan ini menjadi prasyarat praktis sebelum masuk ke konfigurasi logis.
2. Lanjutkan dengan Target A Elemen 1–3 (Bab 6–13): media dan interface Ethernet, teknologi WAN berbasis kabel, serta agregasi dan redundansi jalur kabel, seluruhnya dipraktikkan menggunakan Cisco Packet Tracer sesuai media yang digunakan pada LKS.
3. Lanjutkan dengan Target B.2 (Bab 14–18): konsep, instalasi, keamanan, perencanaan cakupan, dan tautan outdoor jaringan nirkabel. Integrasikan dengan proyek nyata pemasangan access point di lingkungan sekolah bila memungkinkan.
4. Tutup dengan Target B.3 (Bab 19–20): troubleshooting gabungan jaringan kabel dan nirkabel, menggabungkan seluruh kompetensi yang telah dipelajari.
5. Lengkapi praktik Target B menggunakan perangkat fisik yang tersedia di sekolah (access point, tang crimping, kabel UTP, alat terminasi fiber, cable tester), karena materi ini tidak tercakup pada simulasi Cisco Packet Tracer.
6. Manfaatkan Bab 21 sebagai bahan konsolidasi menjelang asesmen sumatif atau persiapan kompetisi keahlian.

Rangkuman

Teknologi Jaringan Kabel dan Nirkabel merupakan mata pelajaran lanjutan TJKT kelas XI-XII yang memadukan keterampilan instalasi fisik kabel, konfigurasi logis jaringan kabel/WAN, serta perencanaan dan pengamanan jaringan nirkabel. Buku disusun dengan urutan B.1 → A.1-A.3 → B.2 → B.3 sesuai rekomendasi dokumen target, dengan struktur bab yang konsisten agar memudahkan guru merancang pembelajaran bertahap dari keterampilan fisik menuju konfigurasi logis dan troubleshooting.

1.6 Kaitan dengan Asesmen dan Kompetisi Keahlian

Struktur kompetensi pada buku ini dirancang selaras dengan pola penilaian yang umum digunakan pada asesmen sekolah maupun kompetisi keahlian seperti LKS. Penilaian pengetahuan dapat memanfaatkan soal latihan/refleksi pada setiap bab maupun soal evaluasi akhir pada Bab 21. Penilaian keterampilan sebaiknya menggabungkan penilaian proses (ketepatan langkah kerja saat praktik terminasi kabel maupun konfigurasi perangkat) dan penilaian hasil (fungsi akhir kabel/topologi yang

dibangun), sejalan dengan pola penilaian unjuk kerja yang umum diterapkan pada mata pelajaran produktif TJKT.

Aspek Penilaian	Contoh Bentuk Asesmen	Bab Terkait
Pengetahuan (kognitif)	Soal pilihan ganda/esai tentang konsep OSI, standar kabel, protokol keamanan	Seluruh bab
Keterampilan fisik	Unjuk kerja terminasi kabel UTP/fiber, penggunaan cable tester	Bab 2-5
Keterampilan konfigurasi	Unjuk kerja konfigurasi topologi pada Cisco Packet Tracer	Bab 6-13
Keterampilan instalasi nirkabel	Unjuk kerja instalasi dan pengamanan access point	Bab 14-18
Pemecahan masalah	Studi kasus troubleshooting dengan kesalahan tersembunyi	Bab 19-20

Guru disarankan mengalokasikan waktu tambahan untuk simulasi kompetisi (mock competition) menjelang persiapan LKS, menggabungkan beberapa kompetensi dari berbagai bab sekaligus dalam satu topologi kompleks bertenggat waktu, sebagaimana pola soal yang biasa dijumpai pada kompetisi keahlian sesungguhnya.

BAB 2 — Terminasi Kabel Tembaga (UTP/STP)

Tujuan Pembelajaran

- Peserta didik mampu menjelaskan struktur dan kategori kabel UTP/STP.
- Peserta didik mampu melakukan pemasangan konektor RJ45 sesuai standar TIA/EIA-568 (T568A dan T568B).
- Peserta didik mampu membuat kabel straight-through dan cross-over serta mengujinya.

2.1 Struktur Kabel UTP dan STP

Kabel Unshielded Twisted Pair (UTP) terdiri atas empat pasang kabel tembaga yang dipilin (twisted pair) tanpa pelindung tambahan, sedangkan Shielded Twisted Pair (STP) memiliki lapisan pelindung logam (shield) di sekeliling pasangan kabel untuk mengurangi interferensi elektromagnetik. Pemilinan setiap pasang kabel bertujuan mengurangi crosstalk (interferensi antar pasangan kabel di dalam kabel yang sama) melalui prinsip pembatalan medan elektromagnetik (cancellation).

Kategori Kabel	Bandwidth Maksimal	Kecepatan Umum	Jarak Maksimal (umum)
Cat5e	100 MHz	1 Gbps	100 meter
Cat6	250 MHz	10 Gbps (jarak terbatas ±55m)	100 meter (1 Gbps), 55 meter (10 Gbps)
Cat6a	500 MHz	10 Gbps	100 meter
Cat7	600 MHz	10 Gbps ke atas	100 meter

2.2 Standar Pengkabelan T568A dan T568B

TIA/EIA-568 menetapkan dua standar urutan warna kabel pada konektor RJ45, yaitu T568A dan T568B, yang berbeda hanya pada posisi pasangan warna hijau dan oranye.

Pin	T568A	T568B
1	Putih-Hijau	Putih-Oranye
2	Hijau	Oranye
3	Putih-Oranye	Putih-Hijau
4	Biru	Biru
5	Putih-Biru	Putih-Biru
6	Oranye	Hijau
7	Putih-Cokelat	Putih-Cokelat
8	Cokelat	Cokelat

2.3 Kabel Straight-Through dan Cross-Over

Kombinasi kedua standar pada masing-masing ujung kabel menentukan jenis kabel yang dihasilkan: kabel straight-through menggunakan standar yang sama pada kedua ujung (T568B–T568B) dan digunakan untuk menghubungkan perangkat berbeda jenis (mis. PC ke switch), sedangkan kabel cross-over menggunakan standar berbeda pada tiap ujung (T568A–T568B) dan digunakan untuk menghubungkan perangkat sejenis (mis. switch ke switch, PC ke PC).

2.4 Prosedur Terminasi Konektor RJ45

Prosedur umum pemasangan konektor RJ45 pada kabel UTP meliputi: mengupas jaket luar kabel sepanjang kurang lebih 2-3 cm menggunakan cable stripper, meluruskan dan mengurutkan keempat pasang kabel sesuai standar T568A/T568B yang dipilih, memotong ujung kabel rata menggunakan gunting/cutter agar semua kabel memiliki panjang sama, memasukkan kabel ke dalam konektor RJ45 hingga seluruh kabel menyentuh ujung konektor, kemudian mengunci konektor menggunakan crimping tool sehingga pin tembaga pada konektor menembus dan mengunci setiap kabel.

2.5 Studi Kasus: Diagnosis Kegagalan Instalasi Kabel

Sebuah laboratorium komputer mengalami keluhan salah satu titik jaringan tidak berfungsi meski kabel terlihat terpasang rapi. Teknisi memeriksa menggunakan cable tester dan menemukan bahwa lampu indikator pin 3 dan 6 tidak menyala pada kedua ujung kabel, sementara pin lainnya menyala normal. Kasus ini menggambarkan pentingnya pengujian sistematis setelah instalasi, karena kerusakan visual pada jaket kabel tidak selalu mencerminkan kondisi konduktor di dalamnya.

Langkah Diagnosis	Tindakan
1. Identifikasi pola kegagalan	Catat pin mana saja yang tidak menyala pada cable tester
2. Periksa ujung konektor	Buka housing konektor RJ45, periksa apakah pin tembaga menembus inti kabel dengan sempurna
3. Potong ulang dan pasang ulang	Jika ditemukan pin tidak menembus sempurna, potong konektor lama dan pasang konektor baru
4. Uji ulang	Verifikasi kembali menggunakan cable tester hingga seluruh pin menyala sesuai standar

Praktik / Aktivitas Pembelajaran

1. Praktik membuat kabel straight-through menggunakan kabel UTP Cat5e/Cat6, konektor RJ45, dan crimping tool, mengikuti standar T568B pada kedua ujung.
2. Praktik membuat kabel cross-over menggunakan standar T568A pada satu ujung dan T568B pada ujung lainnya.
3. Praktik menguji kedua kabel yang telah dibuat menggunakan cable tester, memastikan seluruh delapan pin menyala berurutan (straight) atau berpasangan silang (cross) sesuai jenis kabelnya.
4. Diskusi kelompok: identifikasi kesalahan umum yang menyebabkan kabel gagal berfungsi (mis. urutan kabel tertukar, kabel tidak rata, crimping kurang kuat) berdasarkan hasil pengujian yang tidak sempurna.

Rangkuman

Kabel UTP/STP tersusun atas empat pasang kabel terpilin dengan berbagai kategori (Cat5e hingga Cat7) yang menentukan bandwidth dan kecepatan maksimalnya. Standar TIA/EIA-568 menetapkan urutan warna T568A dan T568B, di mana kombinasi keduanya menghasilkan kabel straight-through (perangkat berbeda jenis) atau cross-over (perangkat sejenis). Keterampilan terminasi konektor RJ45 menjadi dasar praktis sebelum mempelajari terminasi fiber optik pada bab berikutnya.

Catatan Praktis

Sebagai catatan praktis di lapangan, teknisi jaringan berpengalaman umumnya membawa beberapa kabel patch cord jadi (straight dan cross) dengan panjang bervariasi sebagai cadangan siap pakai, mengingat waktu pembuatan kabel secara manual di lokasi kerja tidak selalu memungkinkan saat terjadi gangguan mendesak. Kebiasaan menandai/label setiap kabel buatan sendiri dengan tanggal dan jenis (straight/cross) juga membantu manajemen inventaris peralatan praktik di sekolah.

Soal Latihan / Refleksi

1. Jelaskan perbedaan struktur kabel UTP dan STP beserta kegunaannya masing-masing.
2. Tuliskan urutan warna kabel standar T568B dari pin 1 hingga pin 8.
3. Jelaskan kapan sebaiknya digunakan kabel straight-through dan kapan kabel cross-over.
4. Jelaskan tiga kemungkinan penyebab kegagalan pengujian kabel UTP menggunakan cable tester.

BAB 3 — Instalasi dan Terminasi Kabel Fiber Optik

Tujuan Pembelajaran

- Peserta didik mampu menjelaskan jenis dan karakteristik kabel fiber optik (single-mode dan multi-mode).
- Peserta didik mampu menjelaskan prinsip dasar penyambungan (splicing) dan konektorisasi kabel fiber optik.
- Peserta didik mampu mengenal jenis konektor fiber optik yang umum digunakan.

3.1 Prinsip Kerja Fiber Optik

Kabel fiber optik mentransmisikan data dalam bentuk pulsa cahaya yang merambat melalui inti kaca atau plastik (core) yang sangat tipis, memantul secara total di dalam lapisan cladding yang mengelilinginya akibat perbedaan indeks bias. Karena menggunakan cahaya alih-alih sinyal listrik, fiber optik tidak terpengaruh interferensi elektromagnetik, mampu mentransmisikan data dengan kecepatan sangat tinggi, dan dapat menempuh jarak jauh tanpa penurunan sinyal yang signifikan dibandingkan kabel tembaga.

3.2 Jenis Kabel Fiber Optik

Jenis	Diameter Core	Sumber Cahaya	Jarak Tempuh	Kegunaan Umum
Single-Mode (SMF)	±9 mikron	Laser	Puluhan kilometer	Backbone jarak jauh, antar kota/gedung
Multi-Mode (MMF)	±50-62,5 mikron	LED/VCSEL	Ratusan meter	Jaringan lokal dalam gedung/kampus

3.3 Metode Penyambungan (Splicing) Fiber Optik

Penyambungan kabel fiber optik dapat dilakukan dengan dua metode utama. Fusion splicing menyambung dua ujung serat kaca dengan cara melelehkan (fusi) menggunakan busur listrik pada alat fusion splicer, menghasilkan sambungan dengan redaman (loss) sangat rendah dan umum digunakan untuk instalasi permanen berskala besar. Mechanical splicing menyambung dua ujung serat menggunakan penjepit mekanis tanpa proses peleburan, lebih cepat dan tidak memerlukan alat semahal fusion splicer, namun menghasilkan redaman yang sedikit lebih tinggi dan umum digunakan untuk perbaikan cepat atau instalasi berskala kecil.

3.4 Jenis Konektor Fiber Optik

Jenis Konektor	Karakteristik
SC (Subscriber Connector)	Bentuk persegi, mekanisme push-pull, umum digunakan pada peralatan jaringan

Jenis Konektor	Karakteristik
LC (Lucent Connector)	Bentuk lebih kecil dari SC, umum digunakan pada perangkat dengan port padat (mis. SFP module)
FC (Ferrule Connector)	Menggunakan mekanisme ulir (screw-on), umum pada peralatan telekomunikasi presisi tinggi
ST (Straight Tip)	Mekanisme bayonet (twist-lock), umum pada instalasi fiber lama

3.5 Prosedur Dasar Terminasi/Konektorisasi Fiber Optik

Prosedur umum konektorisasi fiber optik meliputi: mengupas lapisan pelindung luar kabel fiber, membersihkan serat kaca menggunakan alcohol wipe khusus, memotong ujung serat menggunakan cleaver presisi agar permukaannya rata dan tegak lurus, memasukkan serat ke dalam konektor (SC/LC/FC/ST) sesuai jenis yang digunakan, kemudian melakukan pengujian akhir menggunakan power meter atau visual fault locator untuk memastikan sambungan berkualitas baik dengan redaman minimal.

3.6 Keselamatan Kerja dalam Instalasi Fiber Optik

Pekerjaan terminasi fiber optik memiliki risiko keselamatan kerja tersendiri yang perlu diperhatikan secara ketat. Serpihan serat kaca hasil pemotongan (cleaving) berukuran sangat kecil dan tajam, dapat menembus kulit tanpa terasa dan sangat berbahaya bila mengenai mata. Selain itu, cahaya laser yang digunakan pada beberapa peralatan uji fiber optik (mis. visual fault locator) tidak boleh diarahkan langsung ke mata meskipun tampak sebagai sinar berwarna biasa.

Aspek K3	Praktik yang Wajib Diterapkan
Penanganan serpihan serat	Gunakan alas kerja gelap (dark mat) agar serpihan mudah terlihat, buang pada wadah tertutup khusus
Pelindung diri	Gunakan kacamata pelindung selama proses pemotongan dan penyambungan fiber
Sumber cahaya laser	Jangan pernah mengarahkan ujung konektor/adapter fiber langsung ke mata saat menguji sumber cahaya
Area kerja	Pastikan area kerja bersih dan bebas dari makanan/minuman untuk mencegah serpihan tertelan

Praktik / Aktivitas Pembelajaran

1. Peserta didik mengamati dan mengidentifikasi contoh kabel fiber optik single-mode dan multi-mode (bila tersedia di sekolah), membandingkan perbedaan warna jaket kabel sebagai penanda jenisnya (umumnya kuning untuk single-mode, oranye/aqua untuk multi-mode).
2. Peserta didik mengidentifikasi berbagai jenis konektor fiber optik (SC, LC, FC, ST) dari contoh fisik atau gambar, dan menjodohkan dengan perangkat yang umum menggunakannya.
3. Simulasi/demonstrasi (bila tersedia alat) prosedur dasar pengupasan dan pemotongan serat fiber menggunakan cleaver, dengan pengawasan ketat guru karena serat kaca yang terpotong berbahaya bagi kulit dan mata.

4. Diskusi kelompok: bandingkan kelebihan dan kekurangan fusion splicing dan mechanical splicing dari sisi biaya, kecepatan, dan kualitas sambungan.

Rangkuman

Kabel fiber optik mentransmisikan data melalui pulsa cahaya, terbagi menjadi single-mode (jarak jauh) dan multi-mode (jarak dekat). Penyambungan fiber dilakukan melalui fusion splicing (redaman rendah, instalasi permanen) atau mechanical splicing (cepat, instalasi kecil), dengan berbagai jenis konektor seperti SC, LC, FC, dan ST. Prosedur terminasi fiber memerlukan ketelitian dan alat khusus karena serat kaca sangat rapuh dan berbahaya bila tidak ditangani dengan hati-hati. Pemahaman ini menjadi dasar sebelum mempelajari structured cabling pada bab berikutnya.

Catatan Praktis

Karena biaya peralatan fusion splicer yang cukup mahal, banyak sekolah menengah kejuruan memperkenalkan konsep terminasi fiber optik melalui video demonstrasi atau kunjungan industri, dilengkapi praktik terbatas menggunakan peralatan mechanical splice yang lebih terjangkau. Penting bagi peserta didik untuk setidaknya memahami konsep dan prosedurnya secara teoritis meski praktik langsung terbatas, sehingga siap beradaptasi ketika bekerja di industri yang memiliki peralatan lengkap.

Soal Latihan / Refleksi

1. Jelaskan perbedaan karakteristik kabel fiber optik single-mode dan multi-mode.
2. Jelaskan perbedaan metode fusion splicing dan mechanical splicing.
3. Sebutkan empat jenis konektor fiber optik yang umum digunakan beserta karakteristik singkatnya.
4. Jelaskan mengapa fiber optik tidak terpengaruh interferensi elektromagnetik, berbeda dengan kabel tembaga.

BAB 4 — Structured Cabling

Tujuan Pembelajaran

- Peserta didik mampu menjelaskan konsep pengkabelan terstruktur (structured cabling) pada gedung/ruangan.
- Peserta didik mampu membedakan pengkabelan horizontal dan backbone.
- Peserta didik mampu menjelaskan komponen utama sistem structured cabling.

4.1 Konsep Structured Cabling

Structured cabling adalah pendekatan standar dalam merancang infrastruktur pengkabelan gedung yang terorganisasi, terdokumentasi, dan mengikuti standar industri (mis. TIA/EIA-568), sehingga memudahkan instalasi, perawatan, dan pengembangan jaringan di masa depan tanpa perlu merombak seluruh infrastruktur kabel. Pendekatan ini berbeda dengan pengkabelan point-to-point yang dipasang secara ad-hoc tanpa perencanaan standar, yang cenderung sulit ditelusuri dan dirawat seiring bertambahnya jumlah perangkat.

4.2 Komponen Utama Structured Cabling

Komponen	Fungsi
Entrance Facility (EF)	Titik masuk kabel dari luar gedung (mis. dari penyedia layanan) ke dalam gedung
Equipment Room (ER)	Ruangan pusat yang menampung perangkat jaringan utama (server, router inti, MDF)
Telecommunications Room (TR)	Ruangan pada tiap lantai/area yang menampung perangkat distribusi (IDF)
Backbone Cabling	Kabel yang menghubungkan Equipment Room dengan Telecommunications Room antar lantai/gedung
Horizontal Cabling	Kabel yang menghubungkan Telecommunications Room dengan titik outlet/perangkat pengguna pada satu lantai
Work Area	Area tempat pengguna akhir mengakses jaringan melalui outlet/wall-plate

4.3 Pengkabelan Horizontal

Pengkabelan horizontal menghubungkan Telecommunications Room (TR) pada suatu lantai dengan titik outlet di ruang kerja (work area), umumnya menggunakan kabel UTP dengan panjang maksimal 90 meter (ditambah maksimal 10 meter untuk patch cord di kedua ujung, sehingga total maksimal 100 meter sesuai batas jarak kabel UTP). Topologi pengkabelan horizontal umumnya berbentuk star, dengan setiap outlet terhubung langsung ke TR terdekat.

4.4 Pengkabelan Backbone

Pengkabelan backbone (juga disebut vertical cabling) menghubungkan Equipment Room (ER) dengan Telecommunications Room (TR) di setiap lantai, atau menghubungkan antar gedung dalam satu kompleks. Karena menempuh jarak lebih jauh dan menampung lalu lintas data dari banyak lantai/area sekaligus, pengkabelan backbone umumnya menggunakan kabel fiber optik yang mampu mentransmisikan data lebih jauh dan lebih cepat dibandingkan kabel tembaga.

4.5 Standar Pelabelan dan Dokumentasi Structured Cabling

Selain aspek fisik pengkabelan, structured cabling yang baik juga memerlukan sistem pelabelan dan dokumentasi yang konsisten pada setiap titik kabel (outlet, patch panel, dan ujung kabel di Telecommunications Room), sehingga memudahkan identifikasi dan penelusuran saat instalasi tambahan maupun troubleshooting di masa depan. Standar pelabelan umumnya mencantumkan kode ruangan, nomor outlet, dan nomor port pada patch panel yang berkorespondensi.

Elemen Label	Contoh Format	Keterangan
Kode ruangan/lantai	L2-R05	Lantai 2, Ruang 05
Nomor outlet	L2-R05-01	Outlet pertama pada ruang tersebut
Port patch panel korespondensi	PP-A-24	Patch panel A, port ke-24, harus sama dengan label pada outlet

Praktik / Aktivitas Pembelajaran

1. Peserta didik menggambar diagram sederhana structured cabling untuk sebuah gedung sekolah tiga lantai, menandai lokasi Equipment Room, Telecommunications Room di tiap lantai, jalur backbone, dan jalur horizontal menuju beberapa ruang kelas.
2. Diskusi kelompok: jelaskan alasan pengkabelan backbone lebih disarankan menggunakan fiber optik dibandingkan kabel tembaga.
3. Kunjungan/observasi (bila memungkinkan) ke ruang server atau ruang jaringan sekolah untuk mengidentifikasi komponen structured cabling yang benar-benar diterapkan.

Rangkuman

Structured cabling adalah pendekatan standar merancang infrastruktur pengkabelan gedung yang terorganisasi dan mudah dirawat, terdiri atas komponen Entrance Facility, Equipment Room, Telecommunications Room, backbone cabling, horizontal cabling, dan work area. Pengkabelan horizontal menghubungkan TR dengan outlet pengguna menggunakan kabel tembaga (maksimal 90 meter), sedangkan pengkabelan backbone menghubungkan ER dengan TR antar lantai/gedung, umumnya menggunakan fiber optik. Pemahaman ini menjadi dasar sebelum mempelajari pengujian kabel pada bab berikutnya.

Catatan Praktis

Dalam praktik structured cabling di gedung nyata, dokumentasi as-built (dokumentasi kondisi akhir instalasi setelah seluruh pekerjaan selesai, yang mungkin berbeda dari rancangan awal akibat penyesuaian di lapangan) menjadi rujukan penting bagi tim pemeliharaan di masa depan. Banyak proyek instalasi jaringan mensyaratkan penyerahan dokumentasi as-built sebagai bagian dari serah terima pekerjaan kepada pemilik gedung.

Soal Latihan / Refleksi

1. Jelaskan perbedaan fungsi Equipment Room dan Telecommunications Room dalam structured cabling.
2. Jelaskan perbedaan pengkabelan horizontal dan pengkabelan backbone.
3. Jelaskan mengapa panjang maksimal kabel UTP pada pengkabelan horizontal dibatasi hingga 90-100 meter.

BAB 5 — Pengujian Kabel dengan Alat Ukur

Tujuan Pembelajaran

- Peserta didik mampu menguji kontinuitas kabel UTP menggunakan cable tester.
- Peserta didik mampu menjelaskan fungsi dan prinsip kerja OTDR sederhana untuk pengujian fiber optik.
- Peserta didik mampu menginterpretasikan hasil pengujian kabel untuk mendeteksi kesalahan pemasangan.

5.1 Cable Tester untuk Kabel Tembaga

Cable tester adalah alat ukur yang digunakan untuk menguji kontinuitas dan urutan pemasangan kabel UTP/STP. Alat ini umumnya terdiri atas dua unit (main unit dan remote unit) yang dihubungkan pada kedua ujung kabel yang diuji. Cable tester akan mengirimkan sinyal listrik secara berurutan pada setiap pin dan menampilkan hasilnya melalui lampu indikator LED, sehingga teknisi dapat memastikan apakah kabel terpasang dengan benar (straight atau cross sesuai kebutuhan), tidak ada kabel yang terputus (open), tidak ada kabel yang terhubung ke pin yang salah (miswire), dan tidak ada dua kabel yang saling terhubung tidak sengaja (short).

Jenis Kesalahan	Ciri pada Cable Tester	Penyebab Umum
Open	Salah satu lampu LED tidak menyala pada kedua unit	Kabel putus atau tidak menempel sempurna pada pin konektor
Short	Dua lampu LED menyala bersamaan pada nomor pin yang seharusnya berbeda	Dua kabel bersentuhan akibat kupasan berlebih atau crimping tidak presisi
Miswire	Urutan lampu menyala tidak sesuai standar yang diharapkan (straight/cross)	Urutan warna kabel tertukar saat pemasangan pada konektor
Split Pair	Kontinuitas normal namun kinerja transmisi menurun (perlu alat lebih presisi untuk deteksi)	Pasangan kabel yang dipilin tertukar dengan kabel dari pasangan lain

5.2 OTDR (Optical Time Domain Reflectometer)

OTDR adalah alat ukur yang digunakan untuk menguji kualitas dan menemukan titik masalah pada kabel fiber optik. Prinsip kerjanya adalah mengirimkan pulsa cahaya ke dalam serat fiber dan mengukur cahaya yang dipantulkan kembali (backscatter) akibat adanya sambungan, konektor, tekukan berlebih, atau titik putus pada kabel. Hasil pengukuran ditampilkan dalam bentuk grafik yang menunjukkan besarnya redaman (loss) sepanjang kabel, sehingga teknisi dapat mengidentifikasi lokasi dan tingkat keparahan masalah tanpa harus menelusuri kabel secara fisik dari ujung ke ujung, terutama pada instalasi backbone yang menempuh jarak jauh.

5.3 Power Meter dan Visual Fault Locator

Selain OTDR, pengujian fiber optik sederhana dapat dilakukan menggunakan optical power meter untuk mengukur daya sinyal yang diterima pada ujung kabel dan membandingkannya dengan ambang batas redaman yang wajar, serta visual fault locator (VFL) yang memancarkan sinar laser merah tampak mata untuk membantu menemukan titik patah atau bengkok tajam pada kabel fiber secara visual, cocok untuk pengujian cepat pada instalasi berskala kecil.

5.4 Interpretasi Hasil Pengujian dan Tindak Lanjut

Hasil pengujian kabel perlu diinterpretasikan dengan tepat agar tindak lanjut yang diambil sesuai dengan akar masalah. Pada pengujian kabel tembaga, hasil 'open' pada pin tertentu umumnya mengharuskan pemasangan ulang konektor, sedangkan hasil 'split pair' memerlukan pemeriksaan urutan pasangan kabel yang mungkin tertukar meski secara kontinuitas tetap terhubung. Pada pengujian fiber optik menggunakan OTDR, redaman yang melebihi ambang batas standar pada suatu titik tertentu mengindikasikan perlunya penyambungan ulang (re-splice) pada lokasi tersebut, sedangkan redaman yang merata tinggi di sepanjang kabel dapat mengindikasikan kualitas kabel itu sendiri yang kurang baik.

Hasil Pengujian	Tindak Lanjut yang Disarankan
Cable tester: open/short/miswire	Pasang ulang konektor RJ45 dengan urutan warna yang benar
Cable tester: split pair	Periksa dan perbaiki urutan pasangan kabel sesuai standar T568A/B
OTDR: redaman tinggi pada satu titik	Lakukan penyambungan ulang (re-splice) pada lokasi yang teridentifikasi
OTDR: redaman merata tinggi	Evaluasi kualitas kabel, pertimbangkan penggantian jika di luar spesifikasi

Praktik / Aktivitas Pembelajaran

1. Praktik menguji kabel straight-through dan cross-over yang telah dibuat pada Bab 2 menggunakan cable tester, mencatat dan menginterpretasikan hasil tampilan LED.
2. Praktik sengaja membuat kabel dengan kesalahan (mis. dua pin tertukar), kemudian menguji dengan cable tester untuk mengenali pola tampilan kesalahan miswire.
3. Diskusi kelompok/demonstrasi: jika tersedia OTDR atau simulasinya, amati bagaimana grafik OTDR menunjukkan titik-titik sambungan dan potensi masalah pada kabel fiber optik.
4. Diskusi kelompok: jelaskan kapan sebaiknya teknisi menggunakan cable tester sederhana dibandingkan OTDR yang lebih kompleks dan mahal.

Rangkuman

Pengujian kabel merupakan langkah penting untuk memastikan kualitas instalasi jaringan. Cable tester digunakan untuk menguji kontinuitas dan urutan kabel UTP/STP, mendeteksi kesalahan seperti open, short, dan miswire. OTDR digunakan untuk menguji kualitas kabel fiber optik dengan mengukur redaman sepanjang kabel dan menemukan lokasi masalah, dilengkapi power meter dan visual fault locator untuk pengujian sederhana. Kompetensi pengujian kabel ini menutup rangkaian materi Target B.1 (instalasi fisik kabel), sebelum peserta didik mempelajari konfigurasi logis jaringan kabel pada bab berikutnya.

Catatan Praktis

Selain cable tester dan OTDR, teknisi jaringan profesional juga mengenal istilah certification tester, yaitu alat ukur kelas industri yang tidak hanya menguji kontinuitas namun juga mengukur parameter kualitas transmisi secara menyeluruh (attenuation, crosstalk, return loss) untuk memastikan kabel yang terpasang benar-benar memenuhi spesifikasi kategori yang diklaim (mis. benar-benar mampu Cat6a). Alat ini umum digunakan pada proyek instalasi berskala besar yang mensyaratkan sertifikasi kualitas kabel secara formal.

Soal Latihan / Refleksi

1. Jelaskan fungsi cable tester dan tiga jenis kesalahan umum yang dapat dideteksinya.
2. Jelaskan prinsip kerja OTDR dalam menemukan titik masalah pada kabel fiber optik.
3. Jelaskan perbedaan penggunaan power meter dan visual fault locator dalam pengujian fiber optik.

BAB 6 — Media dan Interface Ethernet

Tujuan Pembelajaran

- Peserta didik mampu mengidentifikasi jenis interface Ethernet pada perangkat jaringan.
- Peserta didik mampu membedakan FastEthernet dan GigabitEthernet dari sisi kecepatan dan penamaan interface.
- Peserta didik mampu mengonfigurasi interface Ethernet sesuai topologi yang diberikan.

6.1 Jenis Interface Ethernet pada Perangkat Cisco

Perangkat router dan switch Cisco memiliki berbagai jenis interface Ethernet yang penamaannya mencerminkan kecepatan maksimal yang didukung. Penamaan interface pada perangkat Cisco umumnya mengikuti format <jenis interface><slot>/<port>, misalnya FastEthernet0/1 atau GigabitEthernet0/0.

Jenis Interface	Kecepatan Maksimal	Penamaan Umum pada Cisco IOS
Ethernet	10 Mbps	Ethernet0/0
FastEthernet	100 Mbps	FastEthernet0/0, disingkat Fa0/0
GigabitEthernet	1000 Mbps (1 Gbps)	GigabitEthernet0/0, disingkat Gi0/0
TenGigabitEthernet	10 Gbps	TenGigabitEthernet0/0, disingkat Te0/0

6.2 Mengidentifikasi Interface pada Topologi

Sebelum melakukan konfigurasi, teknisi jaringan perlu membaca tabel pengalamatan (addressing table) yang menyertai desain topologi untuk mengetahui interface mana pada setiap perangkat yang harus dikonfigurasi, beserta alamat IP dan subnet mask yang harus diterapkan. Tabel pengalamatan umumnya mencantumkan nama perangkat, nama interface, alamat IP, dan subnet mask secara terstruktur.

Perangkat	Interface	Alamat IP	Subnet Mask
R-CORE	GigabitEthernet0/0	192.168.1.1	255.255.255.0
SW-LAN1	VLAN 1	192.168.1.2	255.255.255.0
PC-A	NIC	192.168.1.10	255.255.255.0

6.3 Konfigurasi Dasar Interface Ethernet

Perintah CLI	Fungsi
interface GigabitEthernet0/0	Masuk ke mode konfigurasi interface tertentu
ip address 192.168.1.1 255.255.255.0	Menetapkan alamat IPv4 dan subnet mask pada interface
description <keterangan>	Memberi keterangan/label pada interface untuk memudahkan dokumentasi

Perintah CLI	Fungsi
no shutdown	Mengaktifkan interface yang sedang dalam kondisi nonaktif (administratively down)
duplex auto	Mengatur mode duplex interface secara otomatis (auto-negotiation)
speed auto	Mengatur kecepatan interface secara otomatis (auto-negotiation)

6.4 Studi Kasus: Memilih Interface yang Tepat

Sebuah sekolah merancang jaringan baru dengan kebutuhan menghubungkan server utama ke switch inti dengan kecepatan tinggi, sementara koneksi ke ruang kelas cukup menggunakan kecepatan standar. Perancang jaringan perlu mempertimbangkan ketersediaan interface pada perangkat yang dimiliki serta kebutuhan bandwidth pada setiap segmen, agar investasi perangkat sesuai kebutuhan tanpa pemborosan biaya pada interface berkecepatan tinggi yang tidak diperlukan.

Segmen Jaringan	Kebutuhan	Rekomendasi Interface
Server utama — Switch inti	Transfer data besar, banyak pengguna bersamaan	GigabitEthernet
Switch inti — Switch ruang kelas	Distribusi ke banyak titik akhir	GigabitEthernet atau FastEthernet (sesuai anggaran)
Switch ruang kelas — PC siswa	Kebutuhan standar (browsing, dokumen)	FastEthernet cukup memadai

Praktik / Aktivitas Pembelajaran

1. Praktik pada Cisco Packet Tracer: mengidentifikasi jenis dan jumlah interface Ethernet yang tersedia pada beberapa model router dan switch yang berbeda melalui tampilan fisik perangkat (Physical tab).
2. Praktik mengonfigurasi alamat IP pada interface GigabitEthernet sebuah router sesuai tabel pengalamatan yang diberikan guru, kemudian memverifikasi dengan show ip interface brief.
3. Diskusi kelompok: jelaskan pentingnya membaca tabel pengalamatan sebelum memulai konfigurasi pada topologi yang kompleks.

Rangkuman

Interface Ethernet pada perangkat Cisco terdiri atas beberapa jenis dengan kecepatan berbeda (Ethernet, FastEthernet, GigabitEthernet, TenGigabitEthernet), dengan penamaan interface yang mencerminkan jenis dan kecepatannya. Konfigurasi interface dilakukan berdasarkan tabel pengalamatan yang menyertai desain topologi, menggunakan perintah dasar interface, ip address, dan no shutdown. Kompetensi ini menjadi dasar sebelum mempelajari perancangan koneksi fisik sesuai topologi pada bab berikutnya.

Catatan Praktis

Penamaan interface pada perangkat Cisco generasi terbaru dapat sedikit bervariasi (mis. TwoGigabitEthernet, TenGigabitEthernet pada perangkat access point atau switch kelas atas), namun prinsip penamaan <jenis interface><slot>/<port> tetap konsisten diterapkan, sehingga pemahaman konsep penamaan ini akan tetap relevan meski peserta didik kelak bekerja dengan perangkat model lebih baru yang belum dibahas secara spesifik dalam buku ini.

Soal Latihan / Refleksi

1. Jelaskan perbedaan kecepatan maksimal antara FastEthernet dan GigabitEthernet.
2. Tuliskan urutan perintah CLI untuk mengonfigurasi alamat IP 10.10.10.1/24 pada interface FastEthernet0/1 sebuah router.
3. Jelaskan fungsi tabel pengalamatan (addressing table) dalam proses konfigurasi jaringan.

BAB 7 — Perancangan Koneksi Fisik sesuai Topologi

Tujuan Pembelajaran

- Peserta didik mampu merancang koneksi fisik antar perangkat sesuai diagram topologi.
- Peserta didik mampu menentukan jenis kabel yang tepat untuk setiap jenis koneksi (router-switch, switch-switch, switch-end device).
- Peserta didik mampu mengimplementasikan rancangan koneksi fisik pada Cisco Packet Tracer.

7.1 Membaca Diagram Topologi sebagai Acuan Perancangan

Sebelum melakukan koneksi fisik, teknisi jaringan perlu membaca dan memahami diagram topologi yang menggambarkan seluruh perangkat beserta keterhubungannya. Diagram topologi umumnya mencantumkan nama perangkat, jenis perangkat (router/switch/end device), serta garis penghubung yang merepresentasikan jenis media (kabel Ethernet, Serial, atau nirkabel) yang digunakan antar perangkat.

7.2 Menentukan Jenis Kabel sesuai Jenis Koneksi

Pada perangkat jaringan modern yang telah mendukung fitur Auto-MDIX, pemilihan kabel straight-through atau cross-over tidak lagi menjadi masalah kritis karena perangkat dapat mendeteksi secara otomatis. Namun, pemahaman standar tradisional tetap penting sebagai kompetensi dasar dan digunakan secara konsisten pada perangkat/simulasi yang belum mendukung Auto-MDIX.

Jenis Koneksi	Jenis Kabel (Standar Tradisional)	Keterangan
Router — Switch	Straight-through	Perangkat berbeda jenis
Switch — Switch	Cross-over	Perangkat sejenis
Switch — End Device (PC/Server)	Straight-through	Perangkat berbeda jenis
Router — Router (langsung)	Cross-over	Perangkat sejenis
Router — PC (langsung, tanpa switch)	Cross-over	Perangkat sejenis

7.3 Prosedur Perancangan Koneksi Fisik pada Cisco Packet Tracer

Pada Cisco Packet Tracer, perancangan koneksi fisik dilakukan dengan memilih jenis kabel yang sesuai dari palet Connections, kemudian menghubungkan port pada perangkat sumber ke port pada perangkat tujuan. Packet Tracer akan menampilkan indikator status koneksi berupa titik hijau (interface aktif dan terhubung dengan benar), titik kuning/oranye (interface aktif namun sedang dalam proses negosiasi, seperti spanning-tree), atau titik merah (interface tidak aktif atau terjadi kesalahan konfigurasi/pengkabelan).

7.4 Studi Kasus: Menyusun Rancangan Kabel untuk Topologi Baru

Seorang teknisi diberi tugas merancang koneksi fisik untuk sebuah topologi baru terdiri atas satu router, dua switch yang saling terhubung, dan delapan PC yang tersebar pada kedua switch tersebut. Sebelum mulai memasang kabel secara fisik, teknisi perlu menyusun daftar kebutuhan kabel beserta jenisnya agar proses instalasi berjalan efisien dan tidak ada kesalahan jenis kabel yang terpasang.

No	Koneksi	Jenis Kabel
1	Router — Switch 1	Straight-through
2	Switch 1 — Switch 2	Cross-over (atau straight-through bila mendukung Auto-MDIX)
3	Switch 1/2 — masing-masing PC (8 unit)	Straight-through

Praktik / Aktivitas Pembelajaran

1. Praktik pada Cisco Packet Tracer: membangun topologi terdiri atas satu router, satu switch, dan tiga PC, menghubungkan seluruh perangkat menggunakan jenis kabel yang tepat sesuai tabel pada bagian 7.2.
2. Praktik mengamati indikator status koneksi (warna titik) pada setiap ujung kabel setelah seluruh interface diaktifkan dengan no shutdown, dan memperbaiki koneksi yang menunjukkan status bermasalah.
3. Diskusi kelompok: berikan sebuah diagram topologi kompleks dengan minimal dua router, tiga switch, dan lima end device, minta peserta didik menentukan jenis kabel yang tepat untuk setiap koneksi.

Rangkuman

Perancangan koneksi fisik memerlukan kemampuan membaca diagram topologi dan menentukan jenis kabel yang tepat sesuai jenis perangkat yang dihubungkan (straight-through untuk perangkat berbeda jenis, cross-over untuk perangkat sejenis). Pada Cisco Packet Tracer, status koneksi dapat dipantau melalui indikator warna pada kedua ujung kabel. Kompetensi ini menjadi dasar sebelum mempelajari verifikasi status interface pada bab berikutnya.

Catatan Praktis

Pada praktik dunia nyata, indikator LED fisik pada port perangkat (menyala hijau solid, berkedip, atau mati) memberikan informasi awal yang cepat tentang status koneksi tanpa perlu mengakses CLI terlebih dahulu. Teknisi lapangan yang berpengalaman terbiasa melakukan pemeriksaan visual cepat terhadap LED port sebagai langkah pertama sebelum masuk ke pemeriksaan CLI yang lebih mendalam.

Soal Latihan / Refleksi

1. Jelaskan jenis kabel yang tepat untuk menghubungkan dua switch secara langsung.
2. Jelaskan arti indikator titik merah pada koneksi kabel di Cisco Packet Tracer.
3. Jelaskan fungsi fitur Auto-MDIX pada perangkat jaringan modern.

BAB 8 — Verifikasi Status Interface

Tujuan Pembelajaran

- Peserta didik mampu memeriksa status interface (up/down, protocol up/down) pada perangkat jaringan.
- Peserta didik mampu menginterpretasikan kombinasi status interface untuk mendiagnosis masalah koneksi.
- Peserta didik mampu menggunakan perintah verifikasi CLI yang tepat sesuai kebutuhan.

8.1 Dua Lapis Status pada Setiap Interface

Setiap interface pada perangkat Cisco IOS memiliki dua lapis status yang ditampilkan secara terpisah: status Layer 1 (Physical), yang menunjukkan apakah koneksi fisik/kabel terdeteksi dengan benar, dan status Layer 2 (Line Protocol), yang menunjukkan apakah protokol data link berjalan dengan benar di atas koneksi fisik tersebut. Kedua status ini ditampilkan dalam format 'interface is [status1], line protocol is [status2]'.

Status Interface	Status Line Protocol	Kemungkinan Penyebab
up	up	Interface berfungsi normal, koneksi fisik dan logis keduanya baik
down	down	Kabel tidak terhubung, port nonaktif di sisi lain, atau kerusakan fisik
up	down	Koneksi fisik baik namun ada masalah konfigurasi (mis. encapsulation tidak cocok, keepalive tidak diterima)
administratively down	down	Interface sengaja dinonaktifkan oleh administrator melalui perintah shutdown

8.2 Perintah Verifikasi Status Interface

Perintah CLI	Fungsi
show ip interface brief	Menampilkan ringkasan status seluruh interface beserta alamat IP dalam satu tabel singkat
show interfaces <nama-interface>	Menampilkan detail status, statistik paket, dan konfigurasi sebuah interface tertentu
show interfaces status	Menampilkan ringkasan status interface pada switch, termasuk VLAN dan mode duplex/speed
show cdp neighbors	Menampilkan perangkat Cisco tetangga yang terhubung langsung, membantu verifikasi topologi fisik

8.3 Strategi Diagnosis Bertahap

Ketika menemukan interface bermasalah, teknisi disarankan melakukan diagnosis secara bertahap dari layer terendah: pertama periksa status Layer 1 (apakah kabel terpasang dengan benar dan

interface tidak dalam kondisi administratively down), kemudian periksa status Layer 2 (apakah ada kecocokan protokol/enkapsulasi dengan perangkat di seberang), dan terakhir periksa konfigurasi Layer 3 (apakah alamat IP dan subnet mask sudah benar) menggunakan perintah ping dan show ip route. Strategi bertahap ini mencegah teknisi salah fokus pada konfigurasi logis padahal akar masalah ada pada koneksi fisik.

8.4 Studi Kasus: Menelusuri Interface yang Tidak Kunjung Up

Seorang siswa melaporkan bahwa setelah mengonfigurasi alamat IP pada sebuah interface router dan menjalankan no shutdown, status interface pada show ip interface brief tetap menunjukkan 'down/down', bukan 'up/up' seperti yang diharapkan. Kasus ini menuntut penelusuran berurutan mulai dari hal paling mendasar sebelum menduga kesalahan konfigurasi logis.

Kemungkinan Penyebab	Langkah Verifikasi
Kabel belum benar-benar terhubung pada topologi Packet Tracer	Periksa ulang kedua ujung kabel pada diagram topologi
Interface pada perangkat seberang belum diaktifkan (masih shutdown)	Periksa status interface pada perangkat di ujung lain koneksi
Interface yang dikonfigurasi salah (mis. salah nomor slot/port)	Bandingkan nama interface yang dikonfigurasi dengan yang ditunjukkan diagram fisik

Praktik / Aktivitas Pembelajaran

1. Praktik pada Cisco Packet Tracer: menjalankan show ip interface brief pada router dan switch dalam topologi yang telah dibangun pada Bab 7, mengidentifikasi interface mana yang belum aktif.
2. Praktik sengaja menonaktifkan sebuah interface menggunakan shutdown, kemudian mengamati perubahan status pada show ip interface brief, lalu mengaktifkannya kembali dengan no shutdown.
3. Praktik menggunakan show cdp neighbors untuk memverifikasi bahwa perangkat yang terhubung sesuai dengan diagram topologi yang direncanakan.
4. Diskusi kelompok: berikan skenario status interface 'up, line protocol down' pada sebuah koneksi serial, minta peserta didik menganalisis kemungkinan penyebabnya.

Rangkuman

Verifikasi status interface melibatkan pemeriksaan dua lapis status: Layer 1 (Physical) dan Layer 2 (Line Protocol), yang kombinasinya membantu mendiagnosis letak masalah koneksi. Perintah show ip interface brief, show interfaces, dan show cdp neighbors menjadi alat verifikasi utama pada Cisco IOS. Strategi diagnosis bertahap dari layer terendah membantu teknisi menemukan akar masalah secara efisien. Kompetensi ini menutup rangkaian materi Target A.1 (media dan interface LAN), sebelum peserta didik mempelajari teknologi WAN berbasis kabel pada bab berikutnya.

Catatan Praktis

Meskipun koneksi Serial secara tradisional identik dengan leased line fisik, dalam praktik modern banyak penyedia layanan juga menawarkan simulasi koneksi serial melalui teknologi lain (mis. circuit emulation atas jaringan MPLS) yang tetap tampil sebagai interface serial dari sudut pandang

konfigurasi router pelanggan, meski secara fisik telah bertransformasi. Hal ini menunjukkan bahwa konsep dan keterampilan konfigurasi interface serial tetap relevan meski teknologi dasar di baliknya terus berkembang.

Soal Latihan / Refleksi

1. Jelaskan perbedaan makna status 'up/up' dan 'up/down' pada sebuah interface.
2. Jelaskan fungsi perintah show cdp neighbors dalam verifikasi topologi fisik.
3. Jelaskan strategi diagnosis bertahap yang disarankan ketika menemukan interface bermasalah.

BAB 9 — Teknologi WAN Berbasis Kabel: Koneksi Serial

Tujuan Pembelajaran

- Peserta didik mampu menjelaskan karakteristik koneksi Serial sebagai media WAN point-to-point.
- Peserta didik mampu menjelaskan konsep leased line dan perannya menghubungkan site yang berjauhan.
- Peserta didik mampu membedakan koneksi WAN dan koneksi LAN dari sisi jangkauan dan media.

9.1 Perbedaan Jaringan LAN dan WAN

Local Area Network (LAN) mencakup jaringan pada area terbatas seperti satu gedung atau kampus, umumnya menggunakan kabel Ethernet dengan kecepatan tinggi dan biaya relatif rendah. Wide Area Network (WAN) menghubungkan jaringan yang secara geografis terpisah jauh (antar kota, antar pulau, bahkan antar negara), umumnya disewa dari penyedia layanan telekomunikasi karena infrastrukturnya melintasi area publik yang tidak dimiliki organisasi secara langsung.

9.2 Koneksi Serial sebagai Media WAN Point-to-Point

Koneksi Serial merupakan salah satu jenis koneksi WAN yang menghubungkan dua perangkat secara langsung (point-to-point) melalui jalur sewa (leased line) dari penyedia layanan telekomunikasi. Berbeda dengan Ethernet yang mentransmisikan data secara paralel pada jaringan lokal, koneksi Serial mentransmisikan data secara berurutan (serial) satu bit pada satu waktu, cocok untuk jalur WAN yang menempuh jarak jauh dengan bandwidth yang lebih terbatas dibandingkan Ethernet lokal.

9.3 Konsep Leased Line

Leased line adalah jalur komunikasi yang disewa secara eksklusif dari penyedia layanan telekomunikasi untuk menghubungkan dua lokasi secara permanen, berbeda dengan jalur publik yang digunakan bersama banyak pelanggan. Karena sifatnya yang eksklusif dan didedikasikan (dedicated), leased line menawarkan keandalan dan konsistensi bandwidth yang lebih terjamin dibandingkan koneksi internet publik biasa, meskipun dengan biaya sewa yang lebih tinggi. Leased line umum digunakan perusahaan untuk menghubungkan kantor pusat dengan kantor cabang yang membutuhkan konektivitas stabil untuk aplikasi bisnis kritikal.

9.4 Peran Perangkat DCE dan DTE

Pada koneksi Serial point-to-point, salah satu perangkat berperan sebagai Data Communication Equipment (DCE) yang menyediakan sinyal clock untuk sinkronisasi transmisi data, sedangkan perangkat di sisi lain berperan sebagai Data Terminal Equipment (DTE) yang mengikuti clock dari sisi DCE. Pada simulasi Cisco Packet Tracer, kabel serial memiliki penanda visual (ikon jam) pada ujung yang berperan sebagai DCE, menandakan bahwa perintah clock rate perlu dikonfigurasi pada sisi tersebut.

9.5 Perbandingan Serial dengan Media WAN Lain

Selain koneksi Serial, terdapat beberapa media WAN lain yang berkembang seiring waktu, seperti Frame Relay, MPLS (Multiprotocol Label Switching), dan koneksi berbasis internet (VPN over broadband). Meskipun materi ini secara mendalam berada di luar cakupan mata pelajaran, pemahaman perbandingan singkat membantu peserta didik memahami posisi koneksi Serial dalam evolusi teknologi WAN.

Media WAN	Karakteristik Singkat
Serial (Leased Line)	Koneksi dedicated point-to-point, keandalan tinggi, biaya sewa tetap
Frame Relay	Berbagi jalur (packet-switched) antar banyak pelanggan, lebih ekonomis namun kurang dedicated
MPLS	Solusi WAN modern berbasis label switching, mendukung banyak titik dan prioritas trafik
VPN over Broadband	Memanfaatkan koneksi internet umum dengan enkripsi, biaya rendah namun bergantung kualitas internet publik

Praktik / Aktivitas Pembelajaran

1. Diskusi kelompok: bandingkan karakteristik LAN dan WAN dari sisi jangkauan, kecepatan, biaya, dan kepemilikan infrastruktur, dituliskan dalam bentuk tabel perbandingan.
2. Praktik pada Cisco Packet Tracer: mengamati kabel Serial DCE pada palet Connections, menghubungkan dua router menggunakan kabel tersebut, dan mengidentifikasi sisi mana yang berperan sebagai DCE melalui ikon jam pada koneksi.
3. Diskusi kelompok: jelaskan mengapa perusahaan dengan banyak kantor cabang memilih menyewa leased line dibandingkan menggunakan koneksi internet publik biasa untuk komunikasi antar kantor.

Rangkuman

Koneksi Serial merupakan media WAN point-to-point yang menghubungkan dua lokasi berjauhan melalui jalur sewa (leased line) dari penyedia layanan telekomunikasi, berbeda dengan Ethernet yang digunakan pada jaringan LAN lokal. Pada koneksi Serial, salah satu perangkat berperan sebagai DCE (menyediakan clock) dan yang lain sebagai DTE (mengikuti clock). Pemahaman konsep ini menjadi dasar sebelum mempelajari konfigurasi interface serial pada bab berikutnya.

Catatan Praktis

Dalam ujian praktik maupun kompetisi keahlian, kesalahan pengetikan kecil pada perintah konfigurasi interface serial (mis. subnet mask yang salah ketik) merupakan penyebab kegagalan paling sering dijumpai. Membiasakan diri memverifikasi hasil konfigurasi segera setelah setiap langkah menggunakan show ip interface brief, alih-alih menunggu hingga seluruh topologi selesai dikonfigurasi, sangat membantu mempercepat proses identifikasi kesalahan.

Soal Latihan / Refleksi

1. Jelaskan perbedaan mendasar antara jaringan LAN dan WAN.
2. Jelaskan konsep leased line dan alasan perusahaan bersedia membayar biaya sewa yang lebih tinggi untuk menggunakannya.
3. Jelaskan perbedaan peran perangkat DCE dan DTE pada koneksi Serial point-to-point.

BAB 10 — Konfigurasi Interface Serial pada Router

Tujuan Pembelajaran

- Peserta didik mampu mengonfigurasi alamat IP pada interface serial router sesuai tabel pengalamatan.
- Peserta didik mampu mengonfigurasi parameter clock rate pada sisi DCE.
- Peserta didik mampu memverifikasi konfigurasi dan konektivitas interface serial.

10.1 Perintah Dasar Konfigurasi Interface Serial

Perintah CLI	Fungsi
interface Serial0/0/0	Masuk ke mode konfigurasi interface serial tertentu
ip address <alamat-ip> <subnet-mask>	Menetapkan alamat IPv4 dan subnet mask pada interface serial
clock rate <angka>	Menetapkan kecepatan clock pada sisi DCE, mis. clock rate 64000 (dalam bit per second)
bandwidth <angka>	Menetapkan nilai bandwidth interface untuk keperluan perhitungan metric routing (dalam kbps)
no shutdown	Mengaktifkan interface serial yang sedang nonaktif
show controllers serial <nama-interface>	Memeriksa sisi mana (DCE/DTE) pada interface serial tersebut

10.2 Menentukan Sisi DCE dan Konfigurasi Clock Rate

Perintah clock rate hanya perlu dan hanya dapat dikonfigurasi pada sisi yang berperan sebagai DCE. Pada Cisco Packet Tracer, sisi DCE dapat diidentifikasi secara visual melalui ikon jam pada kabel koneksi, atau secara CLI melalui perintah show controllers serial yang akan menampilkan keterangan 'DCE cable' atau 'DTE cable'. Konfigurasi clock rate yang keliru (dikonfigurasi pada sisi DTE, atau tidak dikonfigurasi sama sekali pada sisi DCE) akan menyebabkan interface tidak dapat mencapai status 'up/up' meskipun kabel telah terpasang dengan benar.

10.3 Contoh Konfigurasi Lengkap

Berikut contoh konfigurasi interface serial pada router yang berperan sebagai sisi DCE, menghubungkan jaringan 10.0.0.0/30 antara Router A dan Router B:

Langkah	Perintah
1	Router(config)# interface Serial0/0/0
2	Router(config-if)# ip address 10.0.0.1 255.255.255.252
3	Router(config-if)# clock rate 64000
4	Router(config-if)# no shutdown

Langkah	Perintah
5	Router(config-if)# end
6	Router# show ip interface brief

10.4 Studi Kasus: Kesalahan Umum Konfigurasi Interface Serial

Pada praktik konfigurasi interface serial, beberapa kesalahan umum sering dijumpai peserta didik pemula, yang perlu dikenali agar dapat segera diperbaiki secara mandiri tanpa selalu bergantung pada bantuan guru.

Kesalahan Umum	Dampak	Solusi
Clock rate dikonfigurasi pada sisi DTE, bukan DCE	Interface tidak mencapai status up/up	Verifikasi sisi DCE dengan show controllers serial, pindahkan konfigurasi clock rate
Subnet mask tidak konsisten antar kedua ujung	Kedua interface up namun tidak dapat saling ping	Samakan subnet mask pada kedua ujung sesuai tabel pengalamatan
Lupa menjalankan no shutdown	Interface tetap administratively down	Jalankan no shutdown pada kedua sisi interface

Praktik / Aktivitas Pembelajaran

1. Praktik pada Cisco Packet Tracer: menghubungkan dua router menggunakan kabel Serial DCE, kemudian mengonfigurasi alamat IP pada kedua sisi interface serial sesuai tabel pengalamatan yang diberikan guru.
2. Praktik mengonfigurasi clock rate pada sisi DCE (diverifikasi terlebih dahulu menggunakan show controllers serial), kemudian mengaktifkan kedua interface dengan no shutdown dan memastikan status menjadi up/up.
3. Praktik menguji konektivitas antar kedua router menggunakan perintah ping melalui interface serial yang telah dikonfigurasi.
4. Diskusi kelompok: jelaskan apa yang akan terjadi pada status interface apabila clock rate tidak dikonfigurasi sama sekali pada topologi tersebut.

Rangkuman

Konfigurasi interface serial melibatkan penetapan alamat IP seperti pada interface Ethernet, ditambah konfigurasi khusus clock rate yang hanya diperlukan pada sisi DCE. Identifikasi sisi DCE dapat dilakukan secara visual (ikon jam pada Packet Tracer) maupun melalui perintah show controllers serial. Kesalahan umum seperti clock rate yang tidak dikonfigurasi akan menyebabkan interface gagal mencapai status up/up. Kompetensi ini menjadi dasar sebelum membangun topologi multi-cabang melalui jalur WAN pada bab berikutnya.

Catatan Praktis

Pada kompetisi keahlian seperti LKS, topologi multi-cabang dengan static routing sederhana sering menjadi bagian awal dari rangkaian soal yang lebih kompleks, sebelum peserta diminta menerapkan routing dinamis maupun fitur lanjutan lainnya. Menguasai static routing dengan cermat, termasuk

kemampuan memverifikasi tabel routing menggunakan show ip route, menjadi fondasi penting yang akan terus digunakan pada tahapan konfigurasi berikutnya.

Soal Latihan / Refleksi

1. Jelaskan fungsi perintah clock rate dan pada sisi mana perintah tersebut perlu dikonfigurasi.
2. Tuliskan urutan lengkap perintah untuk mengonfigurasi interface Serial0/0/0 dengan alamat IP 172.16.0.1/30 sebagai sisi DCE dengan clock rate 64000.
3. Jelaskan akibat yang mungkin terjadi apabila clock rate tidak dikonfigurasi pada sisi DCE.

BAB 11 — Topologi Multi-Cabang melalui Jalur WAN

Tujuan Pembelajaran

- Peserta didik mampu merancang topologi jaringan multi-cabang yang menghubungkan router pusat dan router cabang.
- Peserta didik mampu mengonfigurasi dan menguji konektivitas antar router melalui jalur serial.
- Peserta didik mampu menerapkan static routing sederhana untuk menghubungkan jaringan antar cabang.

11.1 Arsitektur Jaringan Multi-Cabang (Hub-and-Spoke)

Arsitektur jaringan multi-cabang yang umum diterapkan pada topologi soal LKS adalah model hub-and-spoke, di mana satu router pusat (CORE) terhubung langsung ke beberapa router cabang (mis. BRT untuk cabang Barat, TMT untuk cabang Timur) melalui jalur WAN serial point-to-point. Model ini memusatkan kendali dan lalu lintas data melalui kantor pusat, memudahkan pengelolaan kebijakan jaringan secara terpusat, meskipun menciptakan ketergantungan tinggi terhadap ketersediaan router pusat.

11.2 Perancangan Tabel Pengalamatan Multi-Cabang

Perancangan topologi multi-cabang memerlukan perencanaan alamat IP yang cermat agar setiap segmen jaringan (LAN pada setiap cabang, serta setiap link WAN point-to-point) memiliki alokasi subnet yang tidak tumpang tindih. Umumnya digunakan subnet kecil (mis. /30) untuk link WAN point-to-point karena hanya membutuhkan dua alamat host, dan subnet lebih besar (mis. /24) untuk jaringan LAN pada setiap cabang.

Segmen	Network	Perangkat	Alamat IP
WAN CORE-BRT	10.0.0.0/30	R-CORE (Se0/0/0)	10.0.0.1
WAN CORE-BRT	10.0.0.0/30	R-BRT (Se0/0/0)	10.0.0.2
WAN CORE-TMT	10.0.0.4/30	R-CORE (Se0/0/1)	10.0.0.5
WAN CORE-TMT	10.0.0.4/30	R-TMT (Se0/0/0)	10.0.0.6
LAN BRT	192.168.10.0/24	R-BRT (Gi0/0)	192.168.10.1
LAN TMT	192.168.20.0/24	R-TMT (Gi0/0)	192.168.20.1

11.3 Konfigurasi Static Routing Antar Cabang

Setelah seluruh interface dikonfigurasi dan koneksi fisik/logis antar router terverifikasi (status up/up), langkah selanjutnya adalah mengonfigurasi static routing agar setiap router mengetahui cara mencapai jaringan LAN pada cabang lainnya yang tidak terhubung langsung. Pada router CORE, diperlukan rute menuju LAN BRT dan LAN TMT; pada router BRT, diperlukan rute menuju LAN TMT melalui CORE (dan sebaliknya).

Router	Perintah Static Routing
R-CORE	ip route 192.168.10.0 255.255.255.0 10.0.0.2
R-CORE	ip route 192.168.20.0 255.255.255.0 10.0.0.6
R-BRT	ip route 192.168.20.0 255.255.255.0 10.0.0.1
R-BRT	ip route 0.0.0.0 0.0.0.0 10.0.0.1 (alternatif: default route ke CORE)
R-TMT	ip route 192.168.10.0 255.255.255.0 10.0.0.5

11.4 Studi Kasus: Menambahkan Cabang Baru pada Topologi

Sebuah organisasi yang telah memiliki topologi hub-and-spoke dengan router CORE dan dua cabang (BRT dan TMT) berencana menambahkan satu cabang baru (Cabang Selatan/SEL). Perancangan penambahan cabang baru memerlukan alokasi subnet baru untuk link WAN dan LAN cabang tersebut, tanpa mengganggu subnet yang telah dialokasikan sebelumnya, serta penambahan entri static routing pada router CORE dan router cabang lainnya agar seluruh cabang tetap dapat saling terhubung.

Segmen Baru	Alokasi Subnet	Perintah Static Routing Tambahan
WAN CORE-SEL	10.0.0.8/30	-
LAN SEL	192.168.30.0/24	Pada R-CORE: ip route 192.168.30.0 255.255.255.0 10.0.0.10
Update di R-BRT & R-TMT	-	Tambahkan ip route 192.168.30.0 255.255.255.0 <next-hop ke CORE> pada masing-masing router cabang

Praktik / Aktivitas Pembelajaran

1. Praktik pada Cisco Packet Tracer: membangun topologi hub-and-spoke terdiri atas satu router CORE dan dua router cabang (BRT dan TMT), masing-masing cabang memiliki satu jaringan LAN dengan minimal satu PC, menggunakan tabel pengalamatan pada bagian 11.2 sebagai acuan.
2. Praktik mengonfigurasi seluruh interface (Ethernet dan Serial) sesuai tabel pengalamatan, memastikan seluruh link WAN mencapai status up/up.
3. Praktik mengonfigurasi static routing pada ketiga router sesuai tabel pada bagian 11.3, kemudian menguji konektivitas end-to-end dari PC di cabang BRT ke PC di cabang TMT menggunakan ping dan traceroute.
4. Diskusi kelompok: jelaskan mengapa arsitektur hub-and-spoke menciptakan ketergantungan tinggi terhadap router pusat, dan diskusikan dampaknya apabila router CORE mengalami gangguan.

Rangkuman

Topologi multi-cabang umumnya menerapkan arsitektur hub-and-spoke dengan router pusat (CORE) terhubung ke beberapa router cabang melalui jalur WAN serial. Perancangan memerlukan tabel pengalamatan yang cermat, umumnya subnet /30 untuk link WAN dan subnet lebih besar untuk LAN setiap cabang, dilengkapi konfigurasi static routing agar seluruh jaringan dapat saling terhubung. Kompetensi ini menutup rangkaian materi Target A.2 (teknologi WAN berbasis kabel), sebelum peserta didik mempelajari agregasi jalur kabel pada bab berikutnya.

Catatan Praktis

Pada perangkat Cisco kelas menengah ke atas, EtherChannel juga sering dikombinasikan dengan load balancing berdasarkan algoritma tertentu (mis. berdasarkan alamat MAC atau alamat IP sumber-tujuan) untuk mendistribusikan lalu lintas data secara merata di antara link fisik yang tergabung, bukan sekadar menyediakan cadangan pasif. Pembahasan algoritma load balancing EtherChannel secara mendalam berada di luar cakupan buku ini, namun penting diketahui sebagai wawasan tambahan.

Soal Latihan / Refleksi

1. Jelaskan karakteristik arsitektur jaringan hub-and-spoke.
2. Mengapa subnet /30 umum digunakan untuk link WAN point-to-point? Jelaskan alasannya.
3. Sebuah topologi memiliki router CORE terhubung ke router cabang X (WAN 172.16.0.0/30) dengan LAN cabang X berupa 192.168.5.0/24. Tuliskan perintah static routing pada router CORE agar dapat mencapai LAN cabang X.

BAB 12 — Agregasi Jalur Kabel: EtherChannel

Tujuan Pembelajaran

- Peserta didik mampu menjelaskan konsep dan tujuan link aggregation (EtherChannel).
- Peserta didik mampu membedakan protokol negosiasi PAgP dan LACP.
- Peserta didik mampu mengonfigurasi EtherChannel dasar antar switch pada Cisco Packet Tracer.

12.1 Konsep Link Aggregation

Link aggregation (dikenal sebagai EtherChannel pada perangkat Cisco) adalah teknik menggabungkan beberapa link fisik antar dua perangkat menjadi satu link logis tunggal, dengan tujuan meningkatkan total bandwidth yang tersedia (agregasi kapasitas) sekaligus menyediakan redundansi (apabila salah satu link fisik terputus, lalu lintas data tetap mengalir melalui link fisik lainnya tanpa mengganggu koneksi secara keseluruhan). Dari sudut pandang protokol spanning-tree, seluruh link fisik yang tergabung dalam satu EtherChannel diperlakukan sebagai satu port logis, sehingga tidak ada link yang diblokir akibat mencegah loop, dan total bandwidth dari seluruh link fisik dapat dimanfaatkan sepenuhnya.

12.2 Protokol Negosiasi EtherChannel

Protokol	Kepemilikan	Mode Konfigurasi Terkait
PAgP (Port Aggregation Protocol)	Proprietary Cisco	desirable (aktif menegosiasikan), auto (menunggu ajakan dari sisi lain)
LACP (Link Aggregation Control Protocol)	Standar terbuka IEEE 802.3ad	active (aktif menegosiasikan), passive (menunggu ajakan dari sisi lain)
On (statis, tanpa negosiasi)	-	Mengaktifkan EtherChannel langsung tanpa protokol negosiasi (harus dikonfigurasi sama pada kedua sisi)

LACP sebagai standar terbuka lebih disarankan untuk digunakan pada jaringan yang menggabungkan perangkat dari berbagai vendor, sedangkan PAgP hanya kompatibel antar perangkat Cisco. Mode konfigurasi pada kedua ujung link harus kompatibel: desirable dapat berpasangan dengan desirable atau auto (PAgP); active dapat berpasangan dengan active atau passive (LACP); namun auto tidak dapat berpasangan dengan auto, dan passive tidak dapat berpasangan dengan passive, karena keduanya sama-sama pasif menunggu ajakan negosiasi.

12.3 Prosedur Konfigurasi EtherChannel pada Cisco IOS

Perintah CLI	Fungsi
interface range FastEthernet0/1-2	Memilih rentang beberapa interface sekaligus untuk dikonfigurasi bersamaan
channel-group 1 mode active	Menggabungkan interface terpilih ke dalam EtherChannel nomor 1 menggunakan LACP mode active

Perintah CLI	Fungsi
interface port-channel 1	Masuk ke mode konfigurasi interface logis EtherChannel yang telah terbentuk
switchport mode trunk	Mengonfigurasi EtherChannel sebagai trunk (dapat pula dikonfigurasi sebagai access, sesuai kebutuhan)
show etherchannel summary	Menampilkan ringkasan status EtherChannel yang telah dikonfigurasi

12.4 Studi Kasus: Troubleshooting EtherChannel yang Gagal Terbentuk

Dua switch yang dihubungkan dengan dua kabel fisik dan telah dikonfigurasi channel-group tetap menunjukkan status EtherChannel yang gagal terbentuk (individual, bukan bundled) pada show etherchannel summary. Kasus ini umum terjadi akibat inkonsistensi parameter pada interface yang digabungkan.

Kemungkinan Penyebab Kegagalan	Solusi
Mode PAgP/LACP tidak kompatibel antar kedua sisi (mis. auto-auto)	Ubah salah satu sisi menjadi mode aktif (desirable/active)
Kecepatan atau mode duplex interface yang digabungkan tidak seragam	Samakan speed dan duplex pada seluruh interface yang tergabung dalam channel-group
Konfigurasi VLAN/trunk pada interface yang digabungkan berbeda-beda	Samakan konfigurasi switchport (access/trunk, VLAN) pada seluruh interface sebelum digabungkan

Praktik / Aktivitas Pembelajaran

1. Praktik pada Cisco Packet Tracer: menghubungkan dua switch menggunakan dua kabel fisik sekaligus (mis. FastEthernet0/1 dan FastEthernet0/2), kemudian mengonfigurasi EtherChannel menggunakan LACP mode active pada kedua sisi.
2. Praktik memverifikasi hasil konfigurasi menggunakan show etherchannel summary, memastikan status port-channel menunjukkan kondisi aktif (bundled).
3. Praktik menguji redundansi: memutuskan salah satu dari dua kabel fisik yang tergabung dalam EtherChannel, kemudian mengamati apakah konektivitas jaringan tetap berjalan melalui kabel yang tersisa.
4. Diskusi kelompok: jelaskan perbedaan konsekuensi jika mode konfigurasi pada kedua sisi EtherChannel tidak kompatibel (mis. satu sisi active, sisi lain on).

Rangkuman

EtherChannel menggabungkan beberapa link fisik menjadi satu link logis untuk meningkatkan bandwidth dan menyediakan redundansi, menggunakan protokol negosiasi PAgP (proprietary Cisco) atau LACP (standar terbuka IEEE 802.3ad). Konfigurasi EtherChannel memerlukan kompatibilitas mode pada kedua sisi link serta memerlukan konfigurasi yang konsisten (jenis interface, kecepatan, mode trunk/access) pada seluruh interface yang digabungkan. Kompetensi ini menjadi dasar sebelum mempelajari konsep redundansi jalur kabel secara lebih luas pada bab berikutnya.

Catatan Praktis

Sebagai perbandingan dengan materi Bab 11 (arsitektur hub-and-spoke jaringan kabel), penting dipahami bahwa jaringan nirkabel modern pada skala enterprise umumnya dikelola melalui sistem terpusat (Wireless LAN Controller/WLC) yang mengatur banyak access point sekaligus, berbeda dengan pengelolaan access point mandiri (standalone) yang dibahas pada buku ini untuk kebutuhan skala kecil-menengah. Konsep WLC akan diperluas pada mata pelajaran Administrasi Infrastruktur Jaringan.

Soal Latihan / Refleksi

1. Jelaskan tujuan utama penggunaan EtherChannel pada jaringan enterprise.
2. Jelaskan perbedaan protokol PAgP dan LACP.
3. Tuliskan urutan perintah dasar untuk menggabungkan interface FastEthernet0/1 dan FastEthernet0/2 ke dalam EtherChannel menggunakan LACP mode active.

BAB 13 — Redundansi Jalur Kabel Jaringan Enterprise

Tujuan Pembelajaran

- Peserta didik mampu menjelaskan manfaat redundansi jalur kabel pada jaringan enterprise.
- Peserta didik mampu menjelaskan konsep dasar Spanning Tree Protocol (STP) dalam mencegah loop pada jalur redundan.
- Peserta didik mampu menjelaskan hubungan antara redundansi, keandalan, dan kapasitas jaringan.

13.1 Manfaat Redundansi Jalur Kabel

Redundansi jalur kabel berarti menyediakan lebih dari satu jalur fisik antar perangkat jaringan, sehingga apabila satu jalur mengalami gangguan (kabel putus, port rusak, perangkat mati), lalu lintas data dapat dialihkan melalui jalur alternatif tanpa menghentikan operasional jaringan secara keseluruhan. Pada jaringan enterprise yang menuntut ketersediaan tinggi (high availability), redundansi menjadi strategi utama untuk meminimalkan dampak gangguan (downtime) terhadap operasional bisnis, selain juga dapat meningkatkan kapasitas total jaringan apabila jalur redundan tersebut dikombinasikan dengan EtherChannel.

13.2 Masalah Loop pada Jaringan Redundan

Meskipun bermanfaat, penambahan jalur redundan pada jaringan switch (layer 2) tanpa pengendalian yang tepat dapat menimbulkan masalah loop, yaitu perputaran frame data tanpa henti antar switch yang saling terhubung dalam jalur melingkar. Loop dapat menyebabkan broadcast storm (lonjakan lalu lintas broadcast yang membanjiri jaringan), duplikasi frame, serta ketidakstabilan tabel MAC address, yang pada akhirnya dapat melumpuhkan seluruh jaringan.

13.3 Spanning Tree Protocol (STP) sebagai Solusi

Spanning Tree Protocol (STP) adalah protokol pada layer 2 yang secara otomatis mendeteksi topologi redundan dan memblokir sebagian port secara logis untuk mencegah terjadinya loop, sambil tetap mempertahankan jalur fisik redundan sebagai cadangan. Ketika jalur aktif mengalami gangguan, STP akan secara otomatis mengaktifkan kembali port yang tadinya diblokir untuk menggantikan jalur yang terputus, sehingga konektivitas jaringan tetap terjaga meskipun dengan sedikit jeda waktu selama proses konvergensi ulang topologi. Pembahasan konfigurasi STP secara mendalam (termasuk penentuan root bridge, port role, dan variannya seperti Rapid STP) akan diperluas pada mata pelajaran Administrasi Infrastruktur Jaringan; pada tahap ini peserta didik cukup memahami konsep dan tujuannya sebagai pelengkap pemahaman redundansi jaringan.

13.4 Kombinasi Redundansi dan Agregasi

Pada praktiknya, jaringan enterprise sering mengombinasikan redundansi jalur dengan EtherChannel yang telah dipelajari pada bab sebelumnya: dua atau lebih link fisik antar switch digabungkan menjadi satu EtherChannel logis, yang dari sudut pandang STP diperlakukan sebagai satu port tunggal, sehingga seluruh kapasitas link fisik dapat dimanfaatkan sepenuhnya tanpa ada yang diblokir,

sekaligus tetap menyediakan redundansi di dalam EtherChannel itu sendiri (apabila satu link fisik dalam grup terputus, link fisik lainnya dalam grup yang sama tetap berfungsi).

13.5 Studi Kasus: Dampak Kegagalan Root Bridge terhadap Jaringan

Pada jaringan dengan spanning-tree aktif, salah satu switch berperan sebagai root bridge yang menjadi titik acuan seluruh perhitungan jalur STP. Apabila switch yang berperan sebagai root bridge mengalami gangguan atau dimatikan, seluruh switch lain dalam domain STP akan melakukan pemilihan root bridge baru dan menghitung ulang topologi (proses konvergensi), yang untuk sesaat dapat menyebabkan gangguan lalu lintas data hingga topologi baru stabil kembali. Memahami dampak ini membantu peserta didik menyadari pentingnya perencanaan redundansi yang matang, bukan sekadar menambahkan kabel cadangan tanpa mempertimbangkan peran setiap perangkat dalam topologi logis.

Peran Port STP	Penjelasan
Root Port	Port pada switch non-root yang memiliki jalur terbaik menuju root bridge
Designated Port	Port yang bertugas meneruskan lalu lintas data pada suatu segmen jaringan
Blocking Port	Port yang diblokir secara logis untuk mencegah loop, namun tetap dipantau sebagai jalur cadangan

Praktik / Aktivitas Pembelajaran

1. Diskusi kelompok: jelaskan dengan ilustrasi sederhana bagaimana loop dapat terjadi pada tiga switch yang saling terhubung membentuk segitiga tanpa pengendalian STP.
2. Praktik pada Cisco Packet Tracer: membangun topologi tiga switch yang saling terhubung (segitiga), mengamati melalui mode Simulation bagaimana STP secara otomatis memblokir salah satu port untuk mencegah loop, ditandai indikator warna oranye/blocking pada Packet Tracer.
3. Praktik memutuskan salah satu link aktif pada topologi tersebut, kemudian mengamati bagaimana STP mengaktifkan kembali port yang tadinya diblokir untuk memulihkan konektivitas.
4. Diskusi kelompok: jelaskan bagaimana kombinasi EtherChannel dan redundansi jalur dapat memaksimalkan pemanfaatan kapasitas jaringan tanpa mengorbankan keandalan.

Rangkuman

Redundansi jalur kabel meningkatkan keandalan jaringan enterprise dengan menyediakan jalur alternatif saat terjadi gangguan, namun berisiko menimbulkan loop pada jaringan switch tanpa pengendalian yang tepat. Spanning Tree Protocol (STP) mengatasi masalah ini dengan memblokir sebagian port secara logis untuk mencegah loop, sambil mempertahankan jalur fisik sebagai cadangan otomatis. Kombinasi redundansi dengan EtherChannel memungkinkan pemanfaatan kapasitas jaringan secara maksimal tanpa mengorbankan keandalan. Bab ini menutup rangkaian materi Target A (jaringan kabel dari soal LKS), sebelum peserta didik mempelajari jaringan nirkabel pada bab berikutnya.

Catatan Praktis

Selain SSID dan channel, access point modern umumnya menawarkan fitur band steering yang secara otomatis mengarahkan perangkat client yang mendukung dual-band ke frekuensi 5 GHz yang lebih minim interferensi, sambil tetap menyediakan frekuensi 2,4 GHz untuk perangkat lama yang hanya mendukung single-band. Fitur ini membantu mengoptimalkan kinerja jaringan tanpa memerlukan konfigurasi manual dari pengguna.

Soal Latihan / Refleksi

1. Jelaskan manfaat utama redundansi jalur kabel pada jaringan enterprise.
2. Jelaskan apa yang dimaksud dengan loop pada jaringan switch dan dampak negatifnya.
3. Jelaskan bagaimana Spanning Tree Protocol mencegah terjadinya loop tanpa menghilangkan manfaat redundansi.

BAB 14 — Materi Tambahan: Simulasi MikroTik dengan GNS3

Bab ini merupakan modul pendamping praktik yang membahas penggunaan GNS3 sebagai emulator jaringan untuk mensimulasikan perangkat MikroTik (RouterOS/CHR), mendukung materi Administrasi Sistem Jaringan dan Keamanan Jaringan pada kompetensi keahlian TJKT.

MODUL TAMBAHAN TJKT — KELAS XI

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 MTCNA, 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 MTCNA untuk Kelas XI. 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 MTCNA peserta didik Kelas XI.

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 5

GNS3 Lab — Konfigurasi Dasar Router & NAT

Mensimulasikan skenario WAN-LAN-NAT dari Buku MTCNA Bab 3, kini menggunakan dua router MikroTik CHR di GNS3 (satu berperan sebagai "ISP", satu sebagai router pelanggan).

Tujuan Pembelajaran

Peserta mampu mereplikasi konfigurasi IP address, default gateway, DNS, dan NAT masquerade sepenuhnya di lingkungan GNS3.

Pengenalan Awal MikroTik

Sebelum masuk ke lab ini, ingat kembali konsep dari Buku MTCNA Bab 3: setiap router butuh IP address per interface, default route menuju gateway ISP, DNS agar nama domain bisa diterjemahkan, dan NAT masquerade agar IP privat di jaringan lokal dapat "menumpang" IP publik router saat keluar ke internet. Di dunia nyata, "ISP" adalah pihak eksternal; pada lab GNS3 ini, kita akan MEMBUAT ISP kita sendiri menggunakan router CHR kedua, sehingga seluruh skenario dapat diuji tanpa koneksi internet sungguhan.

5.1 Topologi Lab

Topologi terdiri dari 3 node: R-ISP (mensimulasikan jaringan ISP, terhubung ke node NAT/Cloud GNS3 agar punya akses internet sungguhan opsional), R-Client (router yang akan dikonfigurasi persis seperti skenario Buku MTCNA Bab 3), dan satu node VPCS (Virtual PC Simulator, bawaan GNS3, sangat ringan untuk mensimulasikan komputer klien).

- R-ISP: ether1 ke Cloud/NAT (opsional internet asli), ether2 ke R-Client (mewakili "jalur ISP")
- R-Client: ether1 ke R-ISP (WAN), ether2 ke VPC1 (LAN)
- VPC1: perangkat klien virtual super ringan bawaan GNS3

5.2 Konfigurasi R-ISP (Mensimulasikan DHCP dari ISP)

```
/ip address add address=192.168.1.1/24 interface=ether2
/ip pool add name=pool-isp ranges=192.168.1.10-192.168.1.100
/ip dhcp-server add name=dhcp-isp interface=ether2 address-pool=pool-isp disabled=no
/ip dhcp-server network add address=192.168.1.0/24 gateway=192.168.1.1 dns-
server=8.8.8.8
```

5.3 Konfigurasi R-Client (Persis seperti Buku MTCNA Bab 3)

```
/ip dhcp-client add interface=ether1 disabled=no    ; WAN menerima IP dari R-ISP
/ip address add address=192.168.10.1/24 interface=ether2   ; LAN
/ip dns set servers=8.8.8.8 allow-remote-requests=yes
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
```

5.4 Konfigurasi VPC1

```
; Di console VPC1 (bukan RouterOS, melainkan CLI ringan bawaan VPCS):
ip 192.168.10.10/24 192.168.10.1
save
ping 192.168.10.1
```

LAB: Verifikasi End-to-End

1. Bangun topologi sesuai 5.1, konfigurasikan ketiga node sesuai 5.2-5.4.

2. Dari VPC1, ping ke gateway (192.168.10.1) — harus berhasil.

3. Dari VPC1, ping ke R-ISP (192.168.1.1) — harus berhasil (melewati NAT masquerade di R-Client).

4. Dari R-Client, jalankan "/ip dhcp-client print", pastikan status "bound" dan IP address dari R-ISP berhasil didapat.

5. Jika node R-ISP dihubungkan ke Cloud GNS3 dengan akses internet asli, uji ping dari VPC1 ke 8.8.8.8 — jika berhasil, seluruh rantai NAT bertingkat (VPC1 → R-Client NAT → R-ISP → internet asli) bekerja sempurna.

Studi Kasus Nyata — Simulasi Sebelum Deploy ke Lapangan

Seorang teknisi WISP yang akan memasang router baru di rumah pelanggan sering menguji dahulu seluruh rencana konfigurasi (WAN DHCP client, LAN, NAT) di GNS3 menggunakan topologi serupa lab ini sebelum benar-benar berangkat ke lokasi pelanggan — memastikan tidak ada kesalahan sintaks perintah yang bisa memperlambat proses instalasi di lapangan, terutama saat lokasi pelanggan jauh dan kunjungan ulang akan memakan waktu dan biaya perjalanan tambahan.

Uji Pemahaman

1. Mengapa pada lab ini digunakan dua router CHR (R-ISP dan R-Client) alih-alih hanya satu router?

2. Apa fungsi node VPCS dalam topologi GNS3, dan mengapa dipilih dibanding menggunakan router CHR ketiga sebagai "klien"?

3. Jelaskan alur NAT bertingkat yang terjadi ketika VPC1 mengakses internet asli melalui R-Client dan R-ISP.

BAB 6

GNS3 Lab — DHCP Server Multi-Segmen

Membangun beberapa DHCP Server sekaligus dalam satu topologi GNS3, mereplikasi skenario multi-VLAN/multi-ruangan dari Buku MTCNA Bab 4.

Tujuan Pembelajaran

Peserta mampu mengonfigurasi DHCP Server untuk lebih dari satu segmen jaringan sekaligus di GNS3, lengkap dengan static lease.

Pengenalan Awal MikroTik

Ingat kembali tiga komponen inti DHCP Server dari Buku MTCNA Bab 4: IP Pool (rentang IP yang dibagikan), DHCP Server (objek yang mengaktifkan layanan pada interface tertentu), dan DHCP Network (mendefinisikan gateway dan DNS untuk subnet tersebut). Pada lab ini kita akan membuat DUA DHCP Server sekaligus dalam satu router, masing-masing untuk segmen jaringan berbeda — skenario umum saat satu router melayani beberapa ruangan/departemen.

6.1 Topologi Lab

Satu router R-Utama dengan tiga interface LAN (ether2, ether3, ether4), masing-masing terhubung ke satu VPCS berbeda, mewakili 3 ruangan berbeda yang masing-masing memiliki subnet DHCP tersendiri.

6.2 Konfigurasi 3 DHCP Server Sekaligus

```
/ip address add address=192.168.10.1/24 interface=ether2
/ip address add address=192.168.20.1/24 interface=ether3
/ip address add address=192.168.30.1/24 interface=ether4

/ip pool add name=pool-r1 ranges=192.168.10.10-192.168.10.50
/ip pool add name=pool-r2 ranges=192.168.20.10-192.168.20.50
/ip pool add name=pool-r3 ranges=192.168.30.10-192.168.30.50

/ip dhcp-server add name=dhcp-r1 interface=ether2 address-pool=pool-r1 disabled=no
/ip dhcp-server add name=dhcp-r2 interface=ether3 address-pool=pool-r2 disabled=no
/ip dhcp-server add name=dhcp-r3 interface=ether4 address-pool=pool-r3 disabled=no

/ip dhcp-server network add address=192.168.10.0/24 gateway=192.168.10.1 dns-
server=8.8.8.8
/ip dhcp-server network add address=192.168.20.0/24 gateway=192.168.20.1 dns-
server=8.8.8.8
/ip dhcp-server network add address=192.168.30.0/24 gateway=192.168.30.1 dns-
server=8.8.8.8
```

6.3 Menguji DHCP dari VPCS

```
; Di console masing-masing VPC (VPC1, VPC2, VPC3):
ip dhcp
show ip     ; verifikasi IP yang didapat sesuai subnet masing-masing
```

Kelebihan VPCS untuk Lab DHCP

Berbeda dengan console RouterOS yang perlu diketik manual, VPCS mendukung perintah "ip dhcp" yang langsung mensimulasikan proses DHCP discover-offer-request-ack persis seperti komputer sungguhan — sangat memudahkan verifikasi cepat tanpa perlu menyiapkan VM Windows/Linux penuh hanya untuk menguji DHCP.

6.4 Menambahkan Static Lease

```
; Catat MAC address VPC1 terlebih dahulu (tampil di "show ip" pada VPCS)
/ip dhcp-server lease add address=192.168.10.99 mac-address=<MAC_VPC1> server=dhcp-r1
```

LAB: Simulasi 3 Ruangan dengan DHCP Terpisah

1. Bangun topologi 1 router + 3 VPCS sesuai 6.1.

2. Terapkan seluruh konfigurasi 6.2.

3. Jalankan "ip dhcp" pada ketiga VPCS, verifikasi masing-masing mendapat IP sesuai subnet ruangannya.

4. Buat static lease untuk salah satu VPC, lepas dan sambungkan kembali (release/renew) menggunakan perintah VPCS, verifikasi IP yang didapat tetap sama.

5. Diskusikan: mengapa ketiga DHCP Server ini tidak saling "bentrok" meski berjalan bersamaan dalam satu router yang sama?

Uji Pemahaman

1. Mengapa diperlukan IP Pool terpisah untuk masing-masing DHCP Server pada satu router yang sama?

2. Apa keuntungan menggunakan VPCS dibanding VM sungguhan untuk menguji fungsi DHCP di GNS3?

3. Jelaskan proses yang terjadi saat perintah "ip dhcp" dijalankan di VPCS.

BAB 7

GNS3 Lab — Routing Dasar & Failover

Mereplikasi lab static routing dengan check-gateway dari Buku MTCNA Bab 7, kini dengan leluasa menggunakan 3 router sekaligus tanpa batasan jumlah hardware fisik.

Tujuan Pembelajaran

Peserta mampu membangun topologi routing dengan jalur ganda dan menguji mekanisme failover secara langsung di GNS3.

Pengenalan Awal MikroTik

Ingat kembali dari Buku MTCNA Bab 7: static route dengan check-gateway=ping memungkinkan router mendeteksi kematian sebuah gateway dan otomatis beralih ke rute cadangan dengan distance lebih besar. GNS3 sangat ideal untuk lab ini karena kita bisa "mematikan" sebuah link hanya dengan klik kanan > Stop pada kabel/node, jauh lebih cepat dibanding mencabut kabel fisik sungguhan.

7.1 Topologi Lab

Router A (client) terhubung ke Router B dan Router C melalui dua jalur terpisah, sementara Router B dan Router C sama-sama terhubung ke Router D (mewakili "internet"). Ini persis skenario failover pada Buku MTCNA Bab 7, namun kini dapat diuji berulang kali tanpa perlu mencabut-pasang kabel fisik.

7.2 Konfigurasi IP Address (Point-to-Point)

```
; Router A:
/ip address add address=10.0.12.1/30 interface=ether1   ; ke Router B
/ip address add address=10.0.13.1/30 interface=ether2   ; ke Router C

; Router B:
/ip address add address=10.0.12.2/30 interface=ether1   ; ke Router A
/ip address add address=10.0.24.1/30 interface=ether2   ; ke Router D

; Router C:
/ip address add address=10.0.13.2/30 interface=ether1   ; ke Router A
/ip address add address=10.0.34.1/30 interface=ether2   ; ke Router D

; Router D ("internet"):
/ip address add address=10.0.24.2/30 interface=ether1   ; ke Router B
/ip address add address=10.0.34.2/30 interface=ether2   ; ke Router C
/ip address add address=100.64.0.1/24 interface=ether3  ; mewakili "internet"
```

7.3 Static Route dengan Failover

```
; Router B dan C perlu rute menuju "internet" (100.64.0.0/24) di Router D — tidak
dibahas detail di sini, fokus pada Router A
```

```
; Router A:
/ip route add dst-address=100.64.0.0/24 gateway=10.0.12.2 distance=1 check-
gateway=ping
/ip route add dst-address=100.64.0.0/24 gateway=10.0.13.2 distance=2 check-
gateway=ping
```

LAB: Uji Failover Langsung di GNS3

1. Bangun topologi 4 router sesuai 7.1, konfigurasikan seluruh IP address sesuai 7.2.

2. Tambahkan static route di Router B dan C menuju subnet "internet" (100.64.0.0/24) di Router D, serta rute kembali di Router D menuju Router A melalui Router B dan C.

3. Terapkan static route dengan failover di Router A sesuai 7.3.

4. Dari Router A, jalankan "/tool traceroute 100.64.0.1", pastikan jalur melewati Router B (jalur distance=1).

5. Klik kanan pada LINK antara Router A dan Router B di kanvas GNS3, pilih "Suspend" atau langsung stop node Router B untuk mensimulasikan kegagalan link.

6. Jalankan ulang traceroute dari Router A, verifikasi jalur kini melewati Router C, dan amati "/ip route print" untuk melihat perubahan flag Active pada kedua rute.

7. Aktifkan kembali Router B, verifikasi trafik kembali otomatis melalui jalur utama (Router B).

Penerapan di Industri — Keunggulan GNS3 untuk Uji Skenario Kegagalan

Menguji skenario kegagalan jaringan (disaster testing) jauh lebih aman dan cepat dilakukan di GNS3 dibanding hardware produksi sungguhan. Network Engineer sering membangun ulang topologi jaringan kantor/klien mereka di GNS3 terlebih dahulu untuk menguji "apa yang terjadi jika link ini putus" atau "apa yang terjadi jika router ini mati", sebelum akhirnya menerapkan desain redundansi yang telah teruji tersebut ke infrastruktur fisik sungguhan.

Uji Pemahaman

1. Bagaimana cara mensimulasikan kegagalan link di GNS3 tanpa mencabut kabel fisik?

2. Mengapa distance yang lebih kecil pada static route dianggap sebagai jalur "utama" oleh RouterOS?

3. Jelaskan mengapa GNS3 sangat cocok untuk menguji skenario failover berulang kali dibanding hardware fisik.

BAB 8

GNS3 Lab — Bridging Antar Router

Mereplikasi konsep bridge dari Buku MTCNA Bab 8 menggunakan CHR di GNS3, memahami keterbatasan emulasi bridge dibanding hardware offload sungguhan.

Tujuan Pembelajaran

Peserta mampu membangun bridge di GNS3 dan memahami perbedaan performa bridge software (yang selalu terjadi di GNS3) dengan hardware offload pada RouterBOARD fisik.

Pengenalan Awal MikroTik

Ingat kembali dari Buku MTCNA Bab 8: bridge menggabungkan beberapa interface menjadi satu broadcast domain Layer 2. Penting dipahami: karena CHR berjalan sebagai virtual machine murni tanpa switch chip fisik, SELURUH bridge di GNS3 otomatis berjalan sebagai bridge software — konsep hardware offload yang dibahas di buku utama TIDAK dapat diuji performanya di GNS3, hanya logika konfigurasinya saja yang identik.

8.1 Topologi Lab

Satu router R1 dengan tiga interface (ether2, ether3, ether4) digabungkan ke dalam satu bridge, masing-masing terhubung ke VPC1, VPC2, dan VPC3 — mensimulasikan penggabungan beberapa "port switch".

8.2 Konfigurasi Bridge

```
/interface bridge add name=bridge-lab
/interface bridge port add bridge=bridge-lab interface=ether2
/interface bridge port add bridge=bridge-lab interface=ether3
/interface bridge port add bridge=bridge-lab interface=ether4
/ip address add address=192.168.50.1/24 interface=bridge-lab
/interface bridge set bridge-lab protocol-mode=rstp
```

8.3 Menguji Loop dan RSTP

Salah satu keunggulan GNS3 adalah kita bisa dengan sengaja membuat kesalahan topologi (seperti loop) tanpa risiko melumpuhkan jaringan sungguhan — sangat berguna untuk benar-benar MELIHAT bagaimana RSTP bereaksi.

LAB: Membuat dan Mengatasi Loop dengan RSTP

1. Bangun topologi 8.1, konfigurasikan bridge sesuai 8.2, set IP pada VPC1-3 dalam subnet 192.168.50.0/24.

2. Verifikasi VPC1, VPC2, VPC3 dapat saling ping (satu broadcast domain).

3. Tambahkan SATU LAGI kabel penghubung langsung antara ether3 dan ether4 di R1 melalui sebuah SWITCH virtual GNS3 (node Ethernet Switch bawaan) — ini sengaja menciptakan loop

redundan.

4. Amati menu Bridge > STP di console R1 ("/interface bridge port print" dengan kolom role), identifikasi port mana yang otomatis diblokir RSTP untuk mencegah loop.

5. Putuskan salah satu link utama secara sengaja, amati port yang tadinya diblokir kini berubah menjadi forwarding untuk mengambil alih jalur yang terputus.

📌 Studi Kasus Nyata — Melatih Insting Sebelum Pegang Hardware Sungguhan

Sekolah yang membiarkan siswa sengaja membuat loop di GNS3 (sesuatu yang berisiko jika dilakukan sembarangan di jaringan sekolah sungguhan) membantu siswa benar-benar memahami DAMPAK sebuah broadcast storm dan bagaimana RSTP menyelamatkan situasi tersebut — pemahaman yang jauh lebih dalam dibanding sekadar membaca teori, tanpa risiko melumpuhkan jaringan produksi sekolah yang sesungguhnya.

☑ Uji Pemahaman

1. Mengapa konsep hardware offload dari Buku MTCNA Bab 8 tidak dapat diuji performanya di GNS3?

2. Bagaimana cara sengaja menciptakan loop pada topologi GNS3 untuk keperluan pembelajaran RSTP?

3. Apa risiko yang dihindari dengan menguji skenario loop di GNS3 dibanding di jaringan sekolah yang sesungguhnya?

BAB 9

GNS3 Lab — Firewall, NAT Lanjutan & Raw

Membangun dan menguji rule firewall filter, DSTNAT (port forwarding), serta Firewall Raw dari Buku MTCNA Bab 10 di lingkungan GNS3 yang aman untuk bereksperimen.

Tujuan Pembelajaran

Peserta mampu menguji efektivitas rule firewall secara terkontrol, termasuk simulasi serangan sederhana untuk menguji rule Raw.

Pengenalan Awal MikroTik

Ingat kembali dari Buku MTCNA Bab 10: firewall bekerja berdasarkan chain (input/forward/output) yang diperiksa berurutan, sementara tabel Raw diproses lebih awal (sebelum connection tracking) sehingga lebih ringan untuk memblokir trafik berbahaya. GNS3 memungkinkan kita mensimulasikan "penyerang" menggunakan VPCS atau router tambahan tanpa risiko menyerang jaringan sungguhan.

9.1 Topologi Lab: Server, Client, dan "Penyerang"

Router R1 sebagai target, terhubung ke VPC-Server (mensimulasikan web server internal), VPC-Client (pengguna sah), dan VPC-Attacker (mensimulasikan sumber trafik mencurigakan) — ketiganya berada di jaringan luar (WAN) R1 melalui sebuah switch bersama, sementara VPC-Server sebenarnya berada di LAN R1 dan diakses dari luar melalui DSTNAT.

9.2 Konfigurasi Dasar & DSTNAT

```
/ip address add address=203.0.113.1/24 interface=ether1   ; WAN, terhubung ke switch
bersama
/ip address add address=192.168.100.1/24 interface=ether2  ; LAN, ke VPC-Server
/ip firewall nat add chain=dstnat protocol=tcp dst-port=80 in-interface=ether1
action=dst-nat to-addresses=192.168.100.10 to-ports=80
/ip firewall nat add chain=srcnat out-interface=ether2 action=masquerade
```

9.3 Firewall Filter Chain Input

```
/ip firewall filter add chain=input connection-state=established,related action=accept
/ip firewall filter add chain=input connection-state=invalid action=drop
/ip firewall filter add chain=input protocol=icmp action=accept
/ip firewall filter add chain=input in-interface=ether1 action=drop
```

9.4 Simulasi Port Scan Sederhana dan Firewall Raw

VPCS memiliki keterbatasan (tidak mendukung tool port-scan sungguhan), sehingga untuk mensimulasikan trafik "mencurigakan", kita dapat memanfaatkan router CHR tambahan sebagai "attacker" yang mengirim banyak paket ping/traceroute beruntun, cukup untuk mendemonstrasikan cara kerja address-list dan Raw secara konseptual.

```
/ip firewall raw add chain=prerouting src-address-list=blocked-attacker action=drop
/ip firewall filter add chain=input protocol=icmp limit=5,5:packet action=add-src-to-address-list address-list=blocked-attacker address-list-timeout=1m
```

LAB: Menguji Isolasi dan Pemblokiran Otomatis

1. Bangun topologi 9.1, terapkan seluruh konfigurasi 9.2-9.3.

2. Dari VPC-Client, akses simulasi web server melalui "curl 203.0.113.1:80" (VPCS mendukung perintah dasar semacam ini) atau uji dengan ping biasa ke 203.0.113.1 lalu verifikasi trafik diteruskan ke VPC-Server melalui DSTNAT.

3. Dari VPC-Attacker (atau router CHR tambahan berperan sebagai attacker), kirim ping beruntun ke R1 melebihi limit 5 paket per 5 detik yang sudah diatur.

4. Verifikasi IP attacker otomatis masuk ke address-list "blocked-attacker" melalui "/ip firewall address-list print".

5. Verifikasi ping selanjutnya dari attacker benar-benar diblokir (timeout) karena kini ditangani oleh rule Raw.

6. Tunggu 1 menit (sesuai address-list-timeout), verifikasi IP tersebut otomatis hilang dari address-list dan ping kembali berhasil.

Penerapan di Industri — Lab Keamanan Tanpa Risiko

GNS3 menjadi tempat ideal untuk siswa maupun profesional mempelajari teknik mitigasi serangan dasar (seperti rate-limiting dan auto-blocking berbasis address-list) tanpa risiko hukum atau etika yang muncul jika mencoba teknik serupa di jaringan sungguhan tanpa izin. Banyak pelatihan keamanan siber profesional menggunakan pendekatan lab virtual serupa sebelum peserta diizinkan menyentuh sistem produksi.

Uji Pemahaman

1. Mengapa VPC-Server pada lab ini ditempatkan di LAN, bukan langsung di WAN R1?

2. Jelaskan alur kerja rule yang menambahkan IP ke address-list secara otomatis berdasarkan limit paket ICMP.

3. Mengapa pemblokiran otomatis ini diletakkan di tabel Raw, bukan tabel Filter biasa?

BAB 10

GNS3 Lab — QoS dan VPN Dasar

Menutup rangkaian lab Kelas XI dengan simulasi Simple Queue/PCQ dan VPN PPTP/SSTP dari Buku MTCNA Bab 11-12, sekaligus memahami keterbatasan pengujian bandwidth di lingkungan virtual.

Tujuan Pembelajaran

Peserta mampu mereplikasi konfigurasi QoS dan VPN dasar di GNS3, serta memahami mengapa pengujian throughput sesungguhnya tetap memerlukan hardware fisik.

Pengenalan Awal MikroTik

Ingat kembali Buku MTCNA Bab 11 (Simple Queue, PCQ) dan Bab 12 (PPTP/SSTP/PPPoE, PPP Profile & Secret). Penting dipahami: karena CHR tanpa lisensi dibatasi throughput sekitar 1 Mbps, LOGIKA konfigurasi queue tetap bisa diuji dan dipahami sepenuhnya di GNS3, namun untuk benar-benar merasakan efek pembagian bandwidth pada kecepatan tinggi (puluhan/ratusan Mbps), pengujian akhir tetap perlu dilakukan di RouterBOARD fisik.

10.1 Lab QoS: Simple Queue dan PCQ

```
/queue type add name=pcq-up kind=pcq pcq-classifier=src-address pcq-rate=0
/queue type add name=pcq-down kind=pcq pcq-classifier=dst-address pcq-rate=0
/queue simple add name=lan-pcq target=192.168.10.0/24 queue=pcq-up/pcq-down max-
limit=1M/1M
```

LAB: Verifikasi Logika PCQ (Bukan Kecepatan)

1. Bangun topologi 1 router dengan 2-3 VPCS di LAN yang sama.

2. Terapkan konfigurasi PCQ di atas.

3. Dari masing-masing VPC, jalankan ping beruntun panjang secara bersamaan ke arah WAN/internet.

4. Amati tab Traffic pada Simple Queue di Winbox (terhubung melalui node NAT seperti Bab 4) — meski kecepatan absolutnya kecil (dibatasi lisensi CHR), perhatikan bahwa distribusi PROPORSI bandwidth antar klien tetap terlihat merata, membuktikan LOGIKA PCQ bekerja benar meski angka mutlaknya tidak merepresentasikan performa hardware asli.

10.2 Lab VPN: PPTP Server-Client Antar Dua CHR

```
; Router Server:
/interface pptp-server server set enabled=yes
/ppp profile add name=profile-vpn local-address=10.99.0.1 remote-address=pool-vpn
/ip pool add name=pool-vpn ranges=10.99.0.10-10.99.0.20
/ppp secret add name=siswa01 password=Passw0rd! service=pptp profile=profile-vpn
```

```
; Router Client:
/interface pptp-client add name=vpn-out1 connect-to=<IP_WAN_Server> user=siswa01
password=Passw0rd!
```

LAB: Membangun VPN PPTP Antar Dua Lokasi Simulasi

1. Bangun topologi 2 router (Server dan Client) terhubung melalui router ketiga yang berperan sebagai "internet" (mirip topologi Bab 7).

2. Konfigurasikan PPTP Server pada Router Server sesuai 10.2.

3. Konfigurasikan PPTP Client pada Router Client, arahkan ke IP WAN Router Server (melalui jalur "internet" simulasi).

4. Verifikasi status interface pptp-out1 di Router Client menunjukkan status "R" (running/connected).

5. Dari Router Client, ping menuju local-address Router Server (10.99.0.1) melalui tunnel yang baru terbentuk.

6. Bandingkan hasil traceroute sebelum dan sesudah VPN terbentuk — amati bagaimana trafik kini "seolah-olah" langsung terhubung meski secara fisik melewati router "internet" perantara.

Penerapan di Industri — GNS3 sebagai Sandbox VPN Sebelum Produksi

Sebelum mengaktifkan VPN Server sungguhan di router produksi kantor, banyak admin IT menguji terlebih dahulu seluruh alur PPP Profile, PPP Secret, dan pool address di GNS3 untuk memastikan tidak ada konflik subnet dengan jaringan yang sudah berjalan — kesalahan konfigurasi pool VPN yang tumpang tindih dengan subnet LAN yang sudah ada adalah salah satu penyebab umum masalah VPN di dunia nyata, dan jauh lebih murah diperbaiki saat masih di tahap simulasi.

Uji Pemahaman

1. Mengapa hasil pengujian bandwidth di GNS3 tidak dapat dijadikan acuan performa RouterBOARD fisik sesungguhnya?

2. Apa yang tetap valid diuji dari konfigurasi PCQ meski dijalankan di lingkungan dengan throughput terbatas seperti CHR tanpa lisensi?

3. Jelaskan alur singkat bagaimana Router Client "seolah-olah terhubung langsung" ke Router Server setelah tunnel PPTP terbentuk.

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
5	Konfigurasi Dasar & NAT	XI	MTCNA Bab 3
6	DHCP Multi-Segmen	XI	MTCNA Bab 4
7	Routing Dasar & Failover	XI	MTCNA Bab 7
8	Bridging Antar Router	XI	MTCNA Bab 8
9	Firewall, NAT & Raw	XI	MTCNA Bab 10
10	QoS & VPN Dasar	XI	MTCNA Bab 11-12

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

28. 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.
29. 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.

30. Kelas XI Semester 2: Materi MTCRE Bab 1-8 — mayoritas menggunakan GNS3 (Modul Bab 11, 13-14) karena kebutuhan banyak router.
31. 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.