BUKU BAHAN AJAR SISWA

JARINGAN DASAR

Program Keahlian Teknik Jaringan Komputer dan Telekomunikasi (TJKT)

Disusun berdasarkan Capaian Pembelajaran Kurikulum Merdeka SMK
dan Naskah Soal LKS SMK Tingkat Kabupaten Tasikmalaya Tahun 2026
Bidang IT Network System Administration — Modul A: Linux Environment & Modul B: Cisco Packet Tracer

Untuk Jenjang Kelas X SMK

Yusuf Burhani, S.Pd., S.Kom

Kata Pengantar

Buku ini disusun sebagai bahan ajar bagi peserta didik mata pelajaran Jaringan Dasar pada Program Keahlian Teknik Jaringan Komputer dan Telekomunikasi (TJKT) di Sekolah Menengah Kejuruan kelas X. Penyusunan materi mengacu pada Capaian Pembelajaran (CP) mata pelajaran Jaringan Dasar dalam kerangka Kurikulum Merdeka, serta diperkaya dengan kebutuhan kompetensi terapan yang bersumber dari Naskah Soal Lomba Kompetensi Siswa (LKS) SMK Tingkat Kabupaten Tasikmalaya Tahun 2026 Bidang IT Network System Administration.

Materi dalam buku ini dibagi menjadi dua kelompok besar. Target B merupakan materi prasyarat konsep jaringan yang menjadi fondasi awal, meliputi model referensi OSI dan TCP/IP, media transmisi, topologi fisik, protokol dan port, serta perangkat jaringan dasar. Target A merupakan kompetensi wajib yang bersumber langsung dari kebutuhan soal LKS, meliputi pengalamatan IP, desain topologi, konfigurasi dasar perangkat menggunakan Cisco Packet Tracer, konsep switching dan routing dasar, layanan jaringan, hingga keamanan jaringan tingkat dasar.

Setiap bab disusun dengan struktur yang konsisten, yaitu tujuan pembelajaran, uraian materi, aktivitas pembelajaran, rangkuman, serta soal latihan/refleksi. Struktur ini dimaksudkan untuk memudahkan peserta didik dalam memahami konsep secara bertahap sekaligus mempersiapkan diri menghadapi praktik konfigurasi jaringan nyata maupun kompetisi keahlian seperti LKS.

Semoga buku ini bermanfaat sebagai pegangan belajar yang sistematis, aplikatif, dan relevan dengan kebutuhan dunia kerja serta perkembangan teknologi jaringan komputer.

Penyusun

Daftar Isi

Contents

Contents

Kata Pengantar 2
Daftar Isi 3
Peta Kompetensi Buku 7
BAB 1 — Pendahuluan 9
Kedudukan Mata Pelajaran Jaringan Dasar 9
Dasar Penyusunan Target Pembelajaran 9
Struktur Buku 10
Petunjuk Penggunaan bagi Guru dan Peserta Didik 10
BAB 2 — Model Referensi OSI 7 Layer 13
Pengertian dan Tujuan Model OSI 13
Tujuh Lapisan OSI dan Fungsinya 13
Enkapsulasi dan Dekapsulasi Data 14
Komunikasi Peer-to-Peer Antar Layer 14
Pendekatan Troubleshooting Berlapis (Layered Troubleshooting) 14
BAB 3 — Model TCP/IP 16
Latar Belakang Model TCP/IP 16
Empat Lapisan TCP/IP 16
Pemetaan TCP/IP terhadap Model OSI 16
Protocol Data Unit pada Model TCP/IP 17
Studi Kasus: Mengikuti Perjalanan Satu Permintaan Web 17
BAB 4 — Media Transmisi dan Pengkabelan 18
Media Kabel Tembaga: UTP dan STP 18
Konektor RJ-45 dan Standar Pengkabelan 18
Kabel Straight-Through dan Cross-Over 19
Media Fiber Optik 19
Media Transmisi Nirkabel 19
Perbandingan Jarak dan Kecepatan Antar Media Transmisi 19
BAB 5 — Topologi Fisik Jaringan 21
Pengertian Topologi Jaringan 21
Topologi Bus 21
Topologi Star 21
Topologi Ring 21
Topologi Mesh 21
Topologi Tree (Hierarkis) 22

Perbandingan Topologi Jaringan **22**
BAB 6 — Protokol dan Port Dasar **24**
Pengertian Protokol Jaringan **24**
TCP vs UDP **24**
Konsep Port dan Well-Known Ports **24**
Protokol Aplikasi yang Sering Ditemui **25**
BAB 7 — Perangkat Jaringan Dasar **27**
Hub **27**
Switch **27**
Router **27**
Access Point **27**
Perbandingan Perangkat Jaringan Dasar **28**
Kriteria Praktis Pemilihan Perangkat **28**
BAB 8 — Pengantar MikroTik & RouterOS ***29***
BAB 9 — Instalasi & Manajemen RouterOS ***31***
BAB 10 — Konfigurasi Dasar Router ***33***
BAB 11 — DHCP Server & Client ***35***
BAB 12 — Bridging & Switching ***37***
BAB 13 — Pengalamatan IPv4 dan Subnetting ***39***
Struktur Alamat IPv4 ..... **39**
Kelas Alamat IPv4 ..... **40**
Subnet Mask dan Notasi CIDR **40**
Perhitungan Subnetting Sederhana **41**
Menentukan Network Address, Broadcast Address, dan Rentang Host **41**
Latihan Terpandu: Membagi Jaringan dengan VLSM **41**
BAB 14 — Pengalamatan IPv6 Dasar ***43***
Latar Belakang IPv6 ..... **43**
Format Penulisan Alamat IPv6 ..... **43**
Jenis Alamat IPv6 ..... **43**
Konfigurasi Alamat IPv6 pada Interface **44**
Konsep Dual-Stack (IPv4 dan IPv6 Berdampingan) **44**
BAB 15 — Topologi dan Perangkat dalam Desain Jaringan ***46***
Membaca Diagram Topologi Fisik dan Logis **46**
Simbol Standar dalam Diagram Topologi **46**
Fungsi Perangkat dalam Topologi Jaringan Nyata **46**
Segmentasi Jaringan: Internal, DMZ, dan Branch-Core **46**
Checklist Praktis Merancang Topologi Jaringan Sederhana **47**
BAB 16 — Konfigurasi Dasar Perangkat Jaringan dengan Cisco Packet Tracer ***49***
Mengenal Cisco Packet Tracer **49**

Mode Command Line Interface **49**
Konfigurasi Hostname dan Domain-name **49**
Konfigurasi Password dan User Administratif **50**
Konfigurasi Banner Login (MOTD) **50**
Menyimpan Konfigurasi Perangkat **50**
Perintah Verifikasi Dasar **51**
BAB 17 — Konsep Switching Dasar ***53***
Konsep VLAN dan Tujuannya **53**
Access Port dan Trunk Port **53**
VLAN Tagging (Pengantar 802.1Q) **54**
Konsep Link Aggregation (EtherChannel) **54**
Manfaat VLAN dalam Konteks Keamanan dan Manajemen **54**
BAB 18 — Konsep Routing Dasar ***56***
Fungsi dan Cara Kerja Routing **56**
Tabel Routing **56**
Static Routing **56**
Pengantar Routing Dinamis **57**
Pengantar Administrative Distance **57**
BAB 19 — Layanan Jaringan Dasar ***59***
Domain Name System (DNS) **59**
Dynamic Host Configuration Protocol (DHCP) **59**
Network Address Translation (NAT) **60**
Network Time Protocol (NTP) **60**
BAB 20 — Keamanan Jaringan Tingkat Dasar ***62***
SSH vs Telnet **62**
Konfigurasi Akses SSH Dasar **62**
Port Security pada Switch **63**
Prinsip Defense in Depth pada Jaringan **63**
BAB 21 — Rangkuman dan Evaluasi Akhir ***65***
12.26 Peta Keterkaitan Antar Bab **65**
12.27 Rekapitulasi Capaian Target Pembelajaran **65**
12.28 Arah Pembelajaran Lanjutan **66**
Glosarium **68**
Lampiran: Ringkasan Perintah CLI Cisco **70**
Lampiran: Latihan Komprehensif Persiapan LKS **71**
Studi Kasus 1: Desain Jaringan Kantor Cabang Kecil **71**
Studi Kasus 2: Verifikasi dan Troubleshooting **71**
Studi Kasus 3: Pengamanan Akses Perangkat **71**
Daftar Pustaka **72**

BAB 22 — Pengantar MikroTik & RouterOS 74
Apa itu MikroTik? 74
Lini Produk RouterBOARD 74
Level Lisensi RouterOS 74
Jalur Sertifikasi MikroTik 75
BAB 23 — Instalasi dan Akses Perangkat MikroTik 76
Metode Instalasi RouterOS 76
Proses Netinstall 76
Mengakses Router: Winbox, WebFig, SSH, Telnet 76
Dasar Command Line Interface (CLI) 76
Upgrade dan Downgrade RouterOS 77
RouterBOOT Firmware Upgrade 77
BAB 24 — Konfigurasi Dasar Jaringan MikroTik 78
Topologi Dasar Jaringan MikroTik 78
Konfigurasi IP Address 78
Default Gateway & DNS 78
Koneksi WAN via DHCP Client 78
NAT Masquerade — Menghubungkan LAN ke Internet 78
Troubleshooting Konektivitas Dasar 79
BAB 25 — Layanan DHCP dan ARP pada MikroTik 80
Konsep DHCP 80
Konfigurasi DHCP Server 80
DHCP Lease dan Static Lease 80
Address Resolution Protocol (ARP) 80
BAB 26 — Bridging pada MikroTik 82
Konsep Bridging 82
Membuat Bridge 82
Bridge Software vs Hardware Offload 82
Spanning Tree Protocol (STP/RSTP) 82
Bridge Firewall dan Switch Chip 82

Peta Kompetensi Buku

Tabel berikut memetakan setiap bab terhadap kelompok target pembelajaran sebagaimana termuat dalam dokumen Target Pembelajaran Jaringan Dasar. Target B merupakan materi prasyarat/fondasi, sedangkan Target A bersumber langsung dari kebutuhan soal LKS.

Bab	Judul	Kelompok Target	Fokus Utama
1	Pendahuluan	-	Orientasi mata pelajaran
2	Model Referensi OSI 7 Layer	Target B	Tujuh lapisan OSI, enkapsulasi data
3	Model TCP/IP	Target B	Empat lapisan TCP/IP, pemetaan terhadap OSI
4	Media Transmisi dan Pengkabelan	Target B	UTP/STP, fiber optik, standar T568A/B
5	Topologi Fisik Jaringan	Target B	Bus, star, ring, mesh, tree
6	Protokol dan Port Dasar	Target B	TCP vs UDP, well-known ports
7	Perangkat Jaringan Dasar	Target B	Hub, switch, router, access point
8	Pengantar MikroTik & RouterOS	Target A.0	Ekosistem MikroTik, RouterOS, RouterBOARD, jalur sertifikasi
9	Instalasi dan Akses Perangkat MikroTik	Target A.0	Netinstall, Winbox/WebFig/SSH, dasar CLI, upgrade RouterOS
10	Konfigurasi Dasar Jaringan MikroTik	Target A.0	IP address, gateway/DNS, DHCP client, NAT masquerade
11	Layanan DHCP dan ARP pada MikroTik	Target A.0	DHCP server, static lease, Address Resolution Protocol
12	Bridging pada MikroTik	Target A.0	Konsep bridge, STP/RSTP, bridge firewall
13	Pengalamatan IPv4 dan Subnetting	Target A.1	Kelas IP, CIDR, perhitungan subnetting
14	Pengalamatan IPv6 Dasar	Target A.1	Format alamat, jenis alamat, konfigurasi CLI
15	Topologi dan Perangkat dalam Desain Jaringan	Target A.2	Membaca diagram, segmentasi, DMZ
16	Konfigurasi Dasar Perangkat dengan Packet Tracer	Target A.3	Mode CLI, hostname, password, banner
17	Konsep Switching Dasar	Target A.4	VLAN, access/trunk port, EtherChannel
18	Konsep Routing Dasar	Target A.5	Tabel routing, static routing, pengantar dinamis
19	Layanan Jaringan Dasar	Target A.6	DNS, DHCP, NAT, NTP
20	Keamanan Jaringan Tingkat Dasar	Target A.7	SSH vs Telnet, port security

21	Rangkuman dan Evaluasi Akhir	-	Konsolidasi dan evaluasi sumatif

BAB 1 — Pendahuluan

Jaringan Dasar merupakan mata pelajaran fondasi pada Program Keahlian Teknik Jaringan Komputer dan Telekomunikasi (TJKT) yang membekali peserta didik dengan pemahaman tentang konsep, arsitektur, dan praktik dasar jaringan komputer. Mata pelajaran ini menjadi landasan bagi mata pelajaran lanjutan seperti Administrasi Infrastruktur Jaringan, Teknologi Jaringan Berbasis Luas, dan Keamanan Jaringan.

Buku ini disusun dengan mengacu pada dua sumber utama. Sumber pertama adalah Capaian Pembelajaran (CP) mata pelajaran Jaringan Dasar dalam kerangka Kurikulum Merdeka SMK. Sumber kedua adalah Naskah Soal Lomba Kompetensi Siswa (LKS) SMK Tingkat Kabupaten Tasikmalaya Tahun 2026 Bidang IT Network System Administration, khususnya Modul B (Cisco Packet Tracer) dan Modul A (Linux Environment), yang memuat kompetensi konfigurasi jaringan tingkat lanjut sebagai indikasi kebutuhan kompetensi dasar yang harus dikuasai lebih dahulu.

Tujuan Pembelajaran

Peserta didik memahami kedudukan mata pelajaran Jaringan Dasar dalam struktur kurikulum Program Keahlian TJKT.

Peserta didik memahami dasar penyusunan target pembelajaran yang digunakan dalam buku ini.

Peserta didik memahami cara menggunakan buku ini sebagai bahan belajar, baik teori maupun praktik.

Kedudukan Mata Pelajaran Jaringan Dasar

Jaringan Dasar mengajarkan konsep dan keterampilan dasar jaringan komputer yang menjadi prasyarat bagi seluruh kompetensi jaringan tingkat lanjut. Materi mencakup konsep referensi jaringan (model OSI dan TCP/IP), media transmisi dan topologi, pengalamatan IP, perangkat jaringan, konfigurasi dasar perangkat menggunakan simulator, konsep switching dan routing tingkat pengantar, layanan jaringan dasar, hingga keamanan jaringan tingkat dasar.

Kompetensi yang diujikan pada LKS Bidang IT Network System Administration sesungguhnya bertumpu pada penguasaan dasar-dasar ini. Materi seperti routing dinamis (EIGRP, OSPF), VTP, FHRP/HSRP, dan high-availability yang muncul pada soal LKS tidak dapat dikuasai tanpa fondasi kompetensi dasar yang kuat, sehingga Jaringan Dasar berperan sebagai gerbang masuk menuju kompetensi tersebut pada mata pelajaran lanjutan.

Dasar Penyusunan Target Pembelajaran

Target pembelajaran dalam buku ini disusun dalam dua kelompok besar. **Target A** merupakan kompetensi dasar jaringan yang secara eksplisit tersirat atau menjadi fondasi wajib dari soal LKS, meliputi pengalamatan IP, topologi dan perangkat, layanan dasar, serta konfigurasi awal perangkat. **Target B** merupakan materi prasyarat konsep jaringan yang lazim diajarkan di kelas X sebagai fondasi — model OSI/TCP-IP, media transmisi, dan topologi fisik — namun tidak tercantum eksplisit pada soal LKS karena soal tersebut mengasumsikan peserta sudah menguasainya.

Pembagian ini menjaga agar mata pelajaran Jaringan Dasar tetap fokus pada level pengenalan dan dasar, sementara topik lanjutan seperti EIGRP, OSPF, VTP, dan high-availability diarahkan ke mata pelajaran Administrasi Infrastruktur Jaringan atau Teknologi Jaringan Berbasis Luas pada tingkat berikutnya.

Kelompok	Cakupan	Jumlah Elemen
Target B	Prasyarat konsep: OSI, TCP/IP, media transmisi, topologi fisik, protokol/port, perangkat dasar	6 topik
Target A	Fondasi wajib dari soal LKS: pengalamatan, topologi & perangkat, konfigurasi dasar, switching, routing, layanan, keamanan dasar	7 elemen

Struktur Buku

Buku ini terdiri atas 21 bab yang disusun secara berjenjang, dimulai dari materi prasyarat konsep (Target B) pada Bab 2 sampai Bab 7, dilanjutkan praktik perangkat MikroTik RouterOS (Target A.0) pada Bab 8 sampai Bab 12, kemudian materi fondasi dari soal LKS berbasis Cisco Packet Tracer (Target A) pada Bab 13 sampai Bab 20, dan diakhiri dengan rangkuman serta evaluasi akhir pada Bab 21. Setiap bab memuat komponen yang konsisten sebagai berikut.

Tujuan Pembelajaran — kompetensi yang ingin dicapai peserta didik pada bab tersebut.

Uraian Materi — penjelasan konsep dilengkapi contoh, ilustrasi, dan tabel perbandingan.

Aktivitas Pembelajaran — kegiatan praktik, simulasi, atau diskusi yang dapat diterapkan di kelas maupun laboratorium.

Rangkuman — inti sari materi untuk memudahkan review sebelum evaluasi.

Soal Latihan/Refleksi — bahan evaluasi formatif bagi peserta didik.

Petunjuk Penggunaan bagi Guru dan Peserta Didik

Gunakan Bab 2–7 (Target B) sebagai materi pengantar pada awal semester untuk membangun fondasi konsep sebelum masuk ke praktik konfigurasi.

Gunakan Bab 8–12 (Target A.0) sebagai pengenalan praktik konfigurasi perangkat MikroTik RouterOS, sebagai pelengkap di luar ekosistem Cisco Packet Tracer, sebelum masuk ke Bab 13–20.

Gunakan Bab 13–20 (Target A) sebagai materi inti yang disampaikan secara bertahap, idealnya disertai praktik langsung menggunakan Cisco Packet Tracer.

Urutan pembelajaran yang disarankan mengikuti urutan bab dalam buku ini: prasyarat konsep terlebih dahulu, kemudian pengalamatan dan topologi, dilanjutkan konfigurasi dasar, switching, routing, layanan, dan keamanan dasar.

Manfaatkan Bab 21 sebagai bahan konsolidasi menjelang asesmen sumatif maupun persiapan kompetisi keahlian seperti LKS.

Topik lanjutan yang berada di luar cakupan dasar (VTP, EIGRP, OSPF, FHRP/HSRP, EtherChannel tingkat lanjut) sengaja tidak dibahas mendalam pada buku ini agar tidak tumpang tindih dengan mata pelajaran Administrasi Infrastruktur Jaringan.

Rangkuman

Jaringan Dasar merupakan fondasi kompetensi TJKT yang disusun dalam dua kelompok target: Target B sebagai prasyarat konsep dan Target A sebagai kompetensi wajib yang bersumber dari kebutuhan soal LKS. Buku ini disusun berjenjang dari konsep dasar menuju praktik konfigurasi agar peserta didik siap menghadapi materi lanjutan maupun kompetisi keahlian.

BAB 2 — Model Referensi OSI 7 Layer

Tujuan Pembelajaran

Peserta didik mampu menjelaskan tujuan dan manfaat model referensi OSI dalam komunikasi jaringan.

Peserta didik mampu menjelaskan fungsi masing-masing dari tujuh lapisan OSI.

Peserta didik mampu mengaitkan setiap lapisan OSI dengan perangkat dan protokol jaringan yang relevan.

Pengertian dan Tujuan Model OSI

Open Systems Interconnection (OSI) adalah model referensi konseptual yang dikembangkan oleh International Organization for Standardization (ISO) untuk menstandarkan fungsi-fungsi komunikasi data ke dalam tujuh lapisan (layer). Model ini tidak mendefinisikan protokol secara spesifik, melainkan kerangka kerja yang membagi proses komunikasi jaringan menjadi bagian-bagian yang lebih kecil dan mudah dipahami.

Tujuan utama model OSI adalah memudahkan interoperabilitas antar perangkat dan sistem dari vendor berbeda, mempermudah proses troubleshooting dengan mengisolasi masalah pada lapisan tertentu, serta menjadi bahasa umum bagi para praktisi jaringan dalam mendiskusikan arsitektur dan permasalahan jaringan.

Tujuh Lapisan OSI dan Fungsinya

Model OSI membagi komunikasi jaringan menjadi tujuh lapisan yang bekerja secara berurutan, dari lapisan aplikasi yang paling dekat dengan pengguna hingga lapisan fisik yang berhubungan langsung dengan media transmisi.

Layer	Nama	Fungsi Utama	Contoh
7	Application	Antarmuka layanan jaringan untuk aplikasi pengguna	HTTP, FTP, DNS, SMTP
6	Presentation	Translasi, enkripsi, dan kompresi data	SSL/TLS, JPEG, ASCII
5	Session	Membuka, mengelola, dan menutup sesi komunikasi	NetBIOS, RPC
4	Transport	Pengiriman data end-to-end, kontrol aliran dan error	TCP, UDP
3	Network	Pengalamatan logis dan routing antar jaringan	IP, ICMP, Router
2	Data Link	Pengalamatan fisik (MAC) dan deteksi error pada segmen lokal	Ethernet, Switch
1	Physical	Transmisi bit mentah melalui media fisik	Kabel, konektor, sinyal

Layer Atas (Upper Layer)

Layer 5 sampai 7 (Session, Presentation, Application) sering disebut upper layer karena berkaitan langsung dengan interaksi perangkat lunak dan pengguna. Ketiga layer ini umumnya diimplementasikan dalam perangkat lunak pada sistem operasi atau aplikasi.

Layer Bawah (Lower Layer)

Layer 1 sampai 4 (Physical, Data Link, Network, Transport) berkaitan dengan pergerakan data yang sesungguhnya melalui jaringan, dan sebagian besar diimplementasikan pada perangkat keras jaringan seperti kartu jaringan (NIC), switch, dan router.

Enkapsulasi dan Dekapsulasi Data

Ketika data dikirim dari satu perangkat ke perangkat lain, data tersebut melewati proses enkapsulasi, yaitu penambahan header (dan pada layer 2 juga trailer) pada setiap lapisan saat data bergerak dari layer atas ke layer bawah pada sisi pengirim. Sebaliknya, pada sisi penerima terjadi proses dekapsulasi, yaitu pelepasan header pada setiap lapisan saat data bergerak dari layer bawah ke layer atas.

Setiap lapisan memiliki istilah tersendiri untuk satuan data yang diprosesnya, yang dikenal sebagai Protocol Data Unit (PDU): Data pada layer Application-Presentation-Session, Segment pada layer Transport, Packet pada layer Network, Frame pada layer Data Link, dan Bit pada layer Physical.

Komunikasi Peer-to-Peer Antar Layer

Model OSI menerapkan konsep komunikasi peer-to-peer, yaitu setiap layer pada perangkat pengirim secara logis 'berkomunikasi' dengan layer yang sama pada perangkat penerima, meskipun secara fisik data harus melewati seluruh lapisan di bawahnya terlebih dahulu. Misalnya, layer Transport pada pengirim menambahkan informasi yang hanya akan dibaca dan diproses oleh layer Transport pada penerima.

Pendekatan Troubleshooting Berlapis (Layered Troubleshooting)

Salah satu manfaat praktis terbesar model OSI adalah memudahkan proses pelacakan gangguan jaringan (troubleshooting) secara sistematis. Teknisi dapat menelusuri masalah mulai dari layer terendah (bottom-up) maupun layer tertinggi (top-down) untuk mempersempit kemungkinan penyebab gangguan.

Layer Dicurigai	Contoh Gejala	Langkah Pemeriksaan
Physical	Lampu indikator port mati, tidak ada koneksi sama sekali	Periksa kabel, konektor, dan port fisik perangkat
Data Link	Koneksi ada namun tidak stabil, salah VLAN	Periksa konfigurasi switchport dan tabel MAC address
Network	Tidak dapat ping ke jaringan lain	Periksa alamat IP, subnet mask, dan tabel routing
Transport hingga Application	Ping berhasil namun aplikasi tidak dapat diakses	Periksa status layanan/aplikasi dan port yang digunakan

Pendekatan bottom-up dimulai dari pemeriksaan layer Physical (misalnya memastikan kabel benar-benar terpasang) sebelum naik ke layer yang lebih tinggi, sedangkan pendekatan top-down dimulai dari aplikasi

yang bermasalah lalu turun ke layer yang lebih rendah. Pemilihan pendekatan bergantung pada gejala awal yang teramati dan pengalaman teknisi.

Aktivitas Pembelajaran

Peserta didik menggambar diagram tujuh lapisan OSI beserta contoh protokol/perangkat pada setiap lapisan menggunakan kertas kerja atau aplikasi diagram sederhana.

Peserta didik melakukan simulasi proses enkapsulasi data mulai dari layer Application hingga Physical menggunakan studi kasus pengiriman e-mail.

Diskusi kelompok: mengapa troubleshooting jaringan lebih mudah dilakukan dengan memahami model OSI dibanding menganggap jaringan sebagai satu proses tunggal?

Rangkuman

Model OSI membagi komunikasi jaringan menjadi tujuh lapisan (Physical, Data Link, Network, Transport, Session, Presentation, Application) yang masing-masing memiliki fungsi spesifik. Proses enkapsulasi dan dekapsulasi data melalui PDU pada setiap layer menjadi dasar pemahaman bagaimana data bergerak dari aplikasi pengirim hingga aplikasi penerima, dan menjadi prasyarat penting sebelum mempelajari model TCP/IP pada bab berikutnya.

Soal Latihan / Refleksi

Sebutkan tujuh lapisan model OSI beserta urutannya dari layer 7 hingga layer 1.

Jelaskan perbedaan fungsi antara layer Network dan layer Transport.

Apa yang dimaksud dengan PDU, dan sebutkan nama PDU pada layer Data Link serta layer Network.

Jelaskan proses enkapsulasi data secara singkat menggunakan contoh pengiriman pesan melalui aplikasi chatting.

BAB 3 — Model TCP/IP

Tujuan Pembelajaran

Peserta didik mampu menjelaskan latar belakang dan tujuan pengembangan model TCP/IP.

Peserta didik mampu menjelaskan fungsi masing-masing dari empat lapisan TCP/IP.

Peserta didik mampu memetakan lapisan TCP/IP terhadap model OSI.

Latar Belakang Model TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) adalah kumpulan protokol komunikasi yang menjadi dasar operasional jaringan internet saat ini. Berbeda dengan OSI yang bersifat konseptual dan dikembangkan sebagai standar internasional, TCP/IP dikembangkan oleh Departemen Pertahanan Amerika Serikat (DARPA) dan telah diimplementasikan secara luas jauh sebelum OSI diformalkan, sehingga TCP/IP menjadi standar de facto jaringan modern.

Empat Lapisan TCP/IP

Model TCP/IP menyederhanakan tujuh lapisan OSI menjadi empat lapisan yang lebih ringkas namun tetap mencakup seluruh fungsi komunikasi jaringan.

Layer TCP/IP	Fungsi	Contoh Protokol
Application	Menggabungkan fungsi Application, Presentation, dan Session OSI	HTTP, FTP, DNS, DHCP, SMTP
Transport	Pengiriman data end-to-end, sama seperti layer Transport OSI	TCP, UDP
Internet	Pengalamatan logis dan routing, setara layer Network OSI	IP, ICMP, ARP
Network Access	Menggabungkan fungsi Data Link dan Physical OSI	Ethernet, Wi-Fi

Pemetaan TCP/IP terhadap Model OSI

Meskipun jumlah lapisannya berbeda, kedua model memiliki fungsi yang saling berkesesuaian. Pemahaman pemetaan ini penting agar peserta didik tidak keliru ketika literatur atau perangkat lunak jaringan menggunakan istilah dari model yang berbeda untuk merujuk pada fungsi yang sama.

Model OSI	Model TCP/IP
Application, Presentation, Session	Application
Transport	Transport
Network	Internet
Data Link, Physical	Network Access

Protocol Data Unit pada Model TCP/IP

Sama seperti model OSI, model TCP/IP juga mengenal satuan data pada tiap lapisan: Data pada layer Application, Segment (untuk TCP) atau Datagram (untuk UDP) pada layer Transport, Packet pada layer Internet, dan Frame pada layer Network Access. Pemahaman PDU ini penting ketika menganalisis lalu lintas jaringan menggunakan aplikasi capture paket seperti Wireshark.

Studi Kasus: Mengikuti Perjalanan Satu Permintaan Web

Untuk memperkuat pemahaman, perhatikan studi kasus sederhana berikut: seorang siswa membuka alamat web sekolahnya melalui browser pada laptop yang terhubung ke jaringan sekolah. Proses ini melibatkan seluruh lapisan TCP/IP secara berurutan.

Application — browser membentuk permintaan HTTP GET menuju server web sekolah.

Transport — permintaan tersebut dibungkus dalam segment TCP, lengkap dengan proses three-way handshake terlebih dahulu ke port 80/443 server tujuan.

Internet — segment TCP dibungkus menjadi packet dengan alamat IP sumber (laptop siswa) dan alamat IP tujuan (server web).

Network Access — packet dibungkus menjadi frame dengan alamat MAC tujuan berupa default gateway (router sekolah), karena server web berada di luar jaringan lokal.

Proses ini kemudian berulang secara terbalik (dekapsulasi) di setiap perangkat perantara hingga mencapai server tujuan, dan kembali terulang untuk paket balasan dari server menuju laptop siswa. Studi kasus semacam ini membantu peserta didik memahami bahwa satu aktivitas sederhana seperti membuka halaman web sesungguhnya melibatkan proses berlapis yang kompleks namun terstruktur.

Aktivitas Pembelajaran

Peserta didik membuat tabel pemetaan mandiri antara tujuh lapisan OSI dan empat lapisan TCP/IP tanpa melihat buku, kemudian mencocokkan dengan kunci jawaban.

Diskusi kelompok mengenai alasan model TCP/IP lebih banyak digunakan secara praktik dibanding model OSI, meskipun OSI tetap menjadi acuan pembelajaran.

Rangkuman

Model TCP/IP terdiri atas empat lapisan (Application, Transport, Internet, Network Access) yang merupakan penyederhanaan dari tujuh lapisan OSI, dan menjadi standar operasional jaringan internet saat ini. Pemahaman pemetaan antara kedua model menjadi dasar penting sebelum mempelajari protokol dan pengalamatan IP secara lebih mendalam.

Soal Latihan / Refleksi

Jelaskan perbedaan mendasar antara latar belakang pengembangan model OSI dan model TCP/IP.

Sebutkan layer OSI mana saja yang tergabung menjadi layer Application pada model TCP/IP.

Jelaskan perbedaan istilah PDU pada layer Transport TCP/IP antara protokol TCP dan UDP.

BAB 4 — Media Transmisi dan Pengkabelan

Tujuan Pembelajaran

Peserta didik mampu mengidentifikasi jenis-jenis media transmisi jaringan kabel (UTP, STP, fiber optik).

Peserta didik mampu menjelaskan standar pengkabelan T568A dan T568B.

Peserta didik mampu mempraktikkan pembuatan kabel straight dan cross menggunakan konektor RJ-45.

Media Kabel Tembaga: UTP dan STP

Unshielded Twisted Pair (UTP) adalah jenis kabel tembaga yang paling umum digunakan pada jaringan lokal (LAN) karena harganya terjangkau dan mudah dipasang. Kabel ini terdiri atas empat pasang kawat tembaga yang dipilin (twisted pair) tanpa pelindung tambahan, di mana proses pemilinan berfungsi mengurangi interferensi elektromagnetik antar pasangan kabel.

Shielded Twisted Pair (STP) memiliki struktur serupa UTP namun dilengkapi lapisan pelindung logam (shield) untuk mengurangi interferensi elektromagnetik dari luar, sehingga lebih sesuai digunakan pada lingkungan dengan gangguan elektromagnetik tinggi, seperti area dekat mesin industri, meskipun harganya lebih mahal dan pemasangannya lebih rumit dibanding UTP.

Kategori	Kecepatan Maksimum	Penggunaan Umum
Cat 5	100 Mbps	Jaringan lama, sudah jarang digunakan
Cat 5e	1 Gbps	Jaringan LAN kantor/sekolah umum
Cat 6	1–10 Gbps (tergantung jarak)	Jaringan modern kecepatan tinggi
Cat 6a	10 Gbps	Data center dan backbone jaringan
Cat 7	10 Gbps ke atas	Instalasi kelas enterprise

Konektor RJ-45 dan Standar Pengkabelan

RJ-45 (Registered Jack 45) adalah konektor standar untuk kabel UTP/STP pada jaringan Ethernet, memiliki 8 pin yang harus dipasang sesuai urutan warna kabel tertentu. Terdapat dua standar urutan warna yang diakui secara internasional, yaitu T568A dan T568B.

Pin	T568A	T568B
1	Hijau Putih	Oranye Putih
2	Hijau	Oranye
3	Oranye Putih	Hijau Putih
4	Biru	Biru
5	Biru Putih	Biru Putih

Pin	T568A	T568B
6	Oranye	Hijau
7	Coklat Putih	Coklat Putih
8	Coklat	Coklat

Kabel Straight-Through dan Cross-Over

Kabel **straight-through** menggunakan standar pengkabelan yang sama (T568B-T568B atau T568A-T568A) pada kedua ujungnya, dan digunakan untuk menghubungkan perangkat yang berbeda jenis, misalnya PC ke switch, atau switch ke router.

Kabel **cross-over** menggunakan standar berbeda pada tiap ujungnya (satu ujung T568A, ujung lain T568B), dan secara tradisional digunakan untuk menghubungkan perangkat sejenis, misalnya PC ke PC, atau switch ke switch. Perlu dicatat bahwa perangkat jaringan modern umumnya sudah mendukung fitur Auto-MDIX yang secara otomatis mendeteksi jenis kabel yang terpasang, sehingga perbedaan straight dan cross menjadi kurang kritikal pada peralatan generasi terbaru, namun pemahaman konsepnya tetap penting sebagai dasar troubleshooting.

Media Fiber Optik

Kabel fiber optik mengirimkan data dalam bentuk pulsa cahaya melalui inti serat kaca atau plastik, sehingga kebal terhadap interferensi elektromagnetik dan mampu menempuh jarak jauh dengan kecepatan sangat tinggi. Terdapat dua jenis utama: **Single-mode fiber (SMF)** yang menggunakan inti serat sangat kecil untuk transmisi jarak sangat jauh (puluhan kilometer) dengan sumber cahaya laser, dan **Multi-mode fiber (MMF)** yang menggunakan inti serat lebih besar untuk jarak menengah (ratusan meter) dengan sumber cahaya LED, umumnya digunakan pada jaringan backbone di dalam gedung atau data center.

Media Transmisi Nirkabel

Selain media kabel, jaringan juga dapat menggunakan media nirkabel (wireless) yang memanfaatkan gelombang radio untuk mengirimkan data tanpa kabel fisik. Standar yang umum digunakan pada jaringan lokal nirkabel adalah IEEE 802.11 (Wi-Fi) dengan berbagai varian seperti 802.11ac dan 802.11ax (Wi-Fi 6) yang menawarkan kecepatan dan efisiensi lebih tinggi dibanding standar sebelumnya.

Perbandingan Jarak dan Kecepatan Antar Media Transmisi

Pemilihan media transmisi yang tepat pada sebuah proyek instalasi jaringan sangat bergantung pada kebutuhan jarak, kecepatan, anggaran, dan lingkungan pemasangan. Tabel berikut merangkum karakteristik umum tiap jenis media sebagai bahan pertimbangan praktis.

Media	Jarak Maksimum Umum	Kecepatan Umum	Ketahanan Interferensi
UTP Cat 6	100 meter	Hingga 10 Gbps (jarak pendek)	Rendah–sedang
STP	100 meter	Setara UTP	Sedang–tinggi

Media	Jarak Maksimum Umum	Kecepatan Umum	Ketahanan Interferensi
Multi-mode Fiber	±550 meter	10 Gbps ke atas	Sangat tinggi
Single-mode Fiber	Puluhan kilometer	10 Gbps ke atas	Sangat tinggi
Wi-Fi (802.11ac/ax)	±30–50 meter indoor	Ratusan Mbps – beberapa Gbps	Rendah (rentan interferensi)

Sebagai aturan praktis di lapangan, kabel UTP dipilih untuk instalasi jaringan gedung standar dengan jarak pendek, fiber optik dipilih untuk koneksi antar gedung atau backbone jarak jauh, dan media nirkabel dipilih untuk fleksibilitas mobilitas pengguna meskipun dengan kompromi pada kestabilan dan keamanan dibanding media kabel.

Aktivitas Pembelajaran

Peserta didik mempraktikkan pembuatan kabel straight-through menggunakan kabel UTP, konektor RJ-45, dan crimping tool, kemudian menguji konektivitas menggunakan cable tester.

Peserta didik mempraktikkan pembuatan kabel cross-over dan membandingkan urutan warna dengan kabel straight-through yang telah dibuat sebelumnya.

Peserta didik mengamati dan mengidentifikasi jenis media transmisi yang digunakan pada jaringan di laboratorium sekolah.

Rangkuman

Media transmisi jaringan terdiri atas media kabel (UTP, STP, fiber optik) dan media nirkabel. Pemilihan jenis kabel UTP/STP mengacu pada kategori (Cat 5e hingga Cat 7) sesuai kebutuhan kecepatan, sementara pemasangan konektor RJ-45 mengikuti standar T568A atau T568B yang menentukan jenis kabel straight-through atau cross-over. Pemahaman media transmisi menjadi dasar sebelum mempelajari topologi fisik jaringan pada bab berikutnya.

Soal Latihan / Refleksi

Jelaskan perbedaan utama antara kabel UTP dan STP beserta konteks penggunaannya masing-masing.

Sebutkan urutan warna kabel pada standar T568B dari pin 1 sampai pin 8.

Kapan sebuah kabel jaringan disebut sebagai kabel cross-over, dan pada kondisi apa kabel jenis ini secara tradisional digunakan?

Jelaskan perbedaan single-mode fiber dan multi-mode fiber.

BAB 5 — Topologi Fisik Jaringan

Tujuan Pembelajaran

Peserta didik mampu menjelaskan pengertian topologi jaringan.

Peserta didik mampu membedakan jenis-jenis topologi fisik jaringan (bus, star, ring, mesh, tree).

Peserta didik mampu menganalisis kelebihan dan kekurangan masing-masing topologi.

Pengertian Topologi Jaringan

Topologi jaringan adalah susunan atau pola keterhubungan antar perangkat dalam sebuah jaringan komputer. Topologi dapat dibedakan menjadi topologi fisik, yaitu tata letak nyata kabel dan perangkat, serta topologi logis, yaitu pola aliran data yang sesungguhnya terjadi tanpa memandang tata letak fisiknya. Bab ini berfokus pada topologi fisik sebagai fondasi sebelum mempelajari desain jaringan yang lebih kompleks.

Topologi Bus

Topologi bus menghubungkan seluruh perangkat pada satu jalur kabel utama (backbone) secara linear. Topologi ini sederhana dan hemat kabel, namun memiliki kelemahan signifikan: jika kabel utama terputus di satu titik, seluruh segmen jaringan akan terganggu, dan kinerja jaringan menurun drastis seiring bertambahnya jumlah perangkat karena terjadinya collision domain yang besar. Topologi ini sudah jarang digunakan pada jaringan modern.

Topologi Star

Topologi star menghubungkan setiap perangkat secara langsung ke satu titik pusat, umumnya berupa switch atau hub. Topologi ini menjadi standar paling umum digunakan pada jaringan LAN modern karena kegagalan pada satu kabel hanya memengaruhi satu perangkat, memudahkan proses troubleshooting, dan mendukung penambahan perangkat baru dengan mudah. Kelemahan utamanya adalah ketergantungan pada titik pusat — jika perangkat pusat (switch) mengalami kegagalan, seluruh jaringan pada segmen tersebut akan terputus.

Topologi Ring

Topologi ring menghubungkan setiap perangkat ke dua perangkat tetangganya sehingga membentuk lingkaran tertutup, dan data mengalir dalam satu arah (atau dua arah pada dual-ring) melalui setiap perangkat secara berurutan. Topologi ini pernah populer pada jaringan Token Ring dan FDDI, dengan kelebihan performa yang lebih stabil dibanding bus karena tidak ada collision, namun kegagalan pada satu titik dapat mengganggu keseluruhan jaringan kecuali menggunakan konfigurasi dual-ring untuk redundansi.

Topologi Mesh

Topologi mesh menghubungkan setiap perangkat secara langsung ke beberapa atau seluruh perangkat lainnya. Pada **full mesh**, setiap perangkat terhubung ke seluruh perangkat lain, memberikan redundansi maksimal dan keandalan tinggi, namun membutuhkan jumlah kabel yang sangat banyak sehingga biaya

implementasi tinggi. Pada **partial mesh**, hanya sebagian perangkat penting yang saling terhubung langsung, menjadi kompromi antara keandalan dan biaya. Topologi ini umum digunakan pada jaringan backbone inti (core) yang menuntut keandalan tinggi.

Topologi Tree (Hierarkis)

Topologi tree merupakan gabungan beberapa topologi star yang dihubungkan melalui satu jalur backbone, membentuk struktur hierarkis bertingkat. Topologi ini umum digunakan pada jaringan skala menengah hingga besar seperti jaringan kampus atau kantor bercabang, karena memudahkan manajemen jaringan secara terstruktur berdasarkan lapisan (misalnya lapisan core, distribution, dan access), meskipun ketergantungan pada node di lapisan atas tetap menjadi titik kegagalan potensial.

Perbandingan Topologi Jaringan

Topologi	Kelebihan	Kekurangan
Bus	Hemat kabel, instalasi sederhana	Rentan gangguan total, performa menurun saat perangkat bertambah
Star	Mudah dikelola, kegagalan satu titik tidak mengganggu lainnya	Bergantung pada perangkat pusat (switch)
Ring	Performa stabil tanpa collision	Kegagalan satu titik mengganggu jaringan (kecuali dual-ring)
Mesh	Redundansi dan keandalan tinggi	Biaya dan kompleksitas kabel tinggi
Tree	Terstruktur, cocok jaringan skala besar	Ketergantungan pada node lapisan atas

Aktivitas Pembelajaran

Peserta didik menggambar kelima jenis topologi jaringan pada kertas kerja atau aplikasi diagram, lengkap dengan simbol perangkat.

Peserta didik melakukan studi kasus: menentukan topologi paling sesuai untuk tiga skenario berbeda (laboratorium sekolah, kantor cabang kecil, dan data center perusahaan) beserta alasannya.

Simulasi sederhana menggunakan Cisco Packet Tracer untuk membangun topologi star dengan satu switch dan empat PC.

Rangkuman

Topologi jaringan menggambarkan pola keterhubungan perangkat, dengan lima jenis utama yaitu bus, star, ring, mesh, dan tree, masing-masing memiliki kelebihan dan kekurangan tersendiri. Topologi star merupakan standar paling umum pada jaringan LAN modern, sementara topologi mesh sering digunakan pada jaringan backbone yang menuntut keandalan tinggi. Pemahaman topologi menjadi dasar penting sebelum mempelajari desain dan implementasi jaringan pada bab-bab selanjutnya.

Soal Latihan / Refleksi

Jelaskan perbedaan antara topologi fisik dan topologi logis.

Mengapa topologi star menjadi pilihan paling umum pada jaringan LAN modern dibanding topologi bus?

Jelaskan perbedaan full mesh dan partial mesh beserta konteks penggunaannya.

Berikan satu contoh skenario nyata yang paling sesuai menggunakan topologi tree, beserta alasannya.

BAB 6 — Protokol dan Port Dasar

Tujuan Pembelajaran

Peserta didik mampu menjelaskan pengertian dan fungsi protokol jaringan.

Peserta didik mampu membedakan karakteristik protokol TCP dan UDP.

Peserta didik mampu menjelaskan konsep port dan menyebutkan well-known port dari protokol umum.

Pengertian Protokol Jaringan

Protokol jaringan adalah seperangkat aturan yang mengatur bagaimana data diformat, dikirim, diterima, dan diinterpretasikan oleh perangkat-perangkat dalam jaringan. Tanpa protokol yang disepakati bersama, perangkat dari vendor berbeda tidak akan mampu saling berkomunikasi. Protokol beroperasi pada lapisan yang berbeda-beda sesuai model OSI maupun TCP/IP, mulai dari protokol pada layer Application seperti HTTP hingga protokol pada layer Internet seperti IP.

TCP vs UDP

Transmission Control Protocol (TCP) dan User Datagram Protocol (UDP) merupakan dua protokol utama pada layer Transport yang memiliki karakteristik sangat berbeda.

Karakteristik	TCP	UDP
Sifat koneksi	Connection-oriented (perlu handshake)	Connectionless (tanpa handshake)
Keandalan	Andal — ada acknowledgment & retransmisi	Tidak andal — tanpa jaminan pengiriman
Urutan data	Terjamin urut	Tidak terjamin urut
Kecepatan	Lebih lambat (overhead lebih besar)	Lebih cepat (overhead minimal)
Contoh penggunaan	HTTP/HTTPS, FTP, email (SMTP)	DNS, DHCP, streaming video, VoIP

TCP melakukan proses **three-way handshake** (SYN, SYN-ACK, ACK) sebelum pengiriman data dimulai untuk memastikan kedua pihak siap berkomunikasi, sedangkan UDP langsung mengirimkan data tanpa proses negosiasi tersebut, sehingga lebih cocok untuk aplikasi yang mengutamakan kecepatan dibanding keandalan penuh, seperti panggilan video atau game daring.

Konsep Port dan Well-Known Ports

Port adalah nomor identifikasi logis (0–65535) yang digunakan untuk membedakan berbagai layanan atau aplikasi yang berjalan pada satu alamat IP yang sama. Ketika sebuah perangkat menerima data, nomor port pada header TCP/UDP menentukan aplikasi mana yang harus memproses data tersebut. Port dibagi menjadi tiga kategori: **Well-known ports** (0–1023) yang dialokasikan untuk layanan standar, **Registered ports** (1024–49151) untuk aplikasi terdaftar, dan **Dynamic/Private ports** (49152–65535) yang digunakan sementara oleh aplikasi client.

Port	Protokol Transport	Layanan
20/21	TCP	FTP (Data/Control)
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP (pengiriman email)
53	TCP/UDP	DNS
67/68	UDP	DHCP (Server/Client)
80	TCP	HTTP
110	TCP	POP3
123	UDP	NTP
143	TCP	IMAP
443	TCP	HTTPS

Protokol Aplikasi yang Sering Ditemui

Selain memahami nomor port, teknisi jaringan perlu mengenal fungsi protokol pada layer Application yang paling sering ditemui dalam operasional sehari-hari.

Protokol	Fungsi Singkat
HTTP/HTTPS	Transfer halaman web; HTTPS menambahkan enkripsi TLS/SSL
FTP	Transfer berkas antar client dan server
SMTP/POP3/IMAP	Pengiriman dan pengambilan email
DNS	Penerjemah nama domain ke alamat IP
DHCP	Pemberian alamat IP otomatis kepada client
SSH/Telnet	Akses remote command line ke perangkat

Aktivitas Pembelajaran

Peserta didik menggunakan perintah `netstat` atau aplikasi sejenis pada komputer laboratorium untuk mengamati port-port yang sedang aktif digunakan.

Diskusi kelompok: mengapa DNS menggunakan UDP untuk query biasa namun dapat menggunakan TCP untuk transfer zona (zone transfer)?

Peserta didik membuat kartu hafalan (flashcard) berisi pasangan nomor port dan layanan untuk sepuluh protokol yang paling umum digunakan.

Rangkuman

Protokol jaringan mengatur aturan komunikasi antar perangkat, dengan TCP dan UDP sebagai dua protokol utama pada layer Transport yang memiliki karakteristik keandalan dan kecepatan berbeda. Port berfungsi membedakan layanan pada satu alamat IP yang sama, dengan well-known port seperti 80 (HTTP), 443 (HTTPS), 22 (SSH), dan 53 (DNS) menjadi pengetahuan dasar wajib bagi teknisi jaringan.

Soal Latihan / Refleksi

Jelaskan perbedaan utama antara protokol TCP dan UDP beserta contoh aplikasi yang menggunakan masing-masing protokol.

Apa fungsi nomor port dalam komunikasi jaringan?

Sebutkan nomor port default untuk layanan HTTP, HTTPS, SSH, dan DNS.

Jelaskan secara singkat proses three-way handshake pada protokol TCP.

BAB 7 — Perangkat Jaringan Dasar

Tujuan Pembelajaran

Peserta didik mampu membedakan fungsi hub, switch, router, dan access point dalam jaringan sederhana.

Peserta didik mampu menjelaskan pada layer OSI mana masing-masing perangkat beroperasi.

Peserta didik mampu memilih perangkat yang sesuai untuk kebutuhan jaringan sederhana.

Hub

Hub adalah perangkat jaringan sederhana yang beroperasi pada layer Physical (layer 1) dan berfungsi menghubungkan beberapa perangkat dalam satu jaringan LAN. Hub bekerja dengan cara meneruskan (broadcast) setiap data yang diterima ke seluruh port lainnya tanpa mekanisme penyaringan (filtering), sehingga seluruh perangkat yang terhubung ke hub berada dalam satu collision domain yang sama. Keterbatasan ini menyebabkan hub sudah sangat jarang digunakan pada jaringan modern dan telah digantikan oleh switch.

Switch

Switch adalah perangkat yang beroperasi pada layer Data Link (layer 2) dan menghubungkan beberapa perangkat dalam satu jaringan LAN secara lebih cerdas dibanding hub. Switch mempelajari alamat MAC setiap perangkat yang terhubung pada setiap portnya dan menyimpannya dalam tabel MAC address, sehingga data hanya diteruskan ke port tujuan yang sesuai, bukan disiarkan ke seluruh port. Hal ini membuat setiap port pada switch menjadi collision domain tersendiri, sehingga meningkatkan efisiensi dan performa jaringan secara signifikan dibanding hub.

Terdapat pula **switch layer 3** yang menggabungkan fungsi switching dengan kemampuan routing dasar, memungkinkan perangkat ini melakukan routing antar VLAN tanpa memerlukan router terpisah — topik ini akan dibahas lebih lanjut pada bab mengenai konsep switching dan routing.

Router

Router adalah perangkat yang beroperasi pada layer Network (layer 3) dan berfungsi menghubungkan dua atau lebih jaringan yang berbeda, serta menentukan jalur terbaik (routing) untuk meneruskan paket data antar jaringan tersebut berdasarkan alamat IP tujuan. Router menggunakan tabel routing yang berisi informasi jalur menuju berbagai jaringan tujuan, baik yang dipelajari secara manual (static routing) maupun otomatis melalui protokol routing dinamis.

Access Point

Access Point (AP) adalah perangkat yang memungkinkan perangkat nirkabel (wireless) terhubung ke jaringan kabel yang sudah ada, berfungsi sebagai jembatan antara media transmisi nirkabel dan media transmisi kabel. Access Point umumnya beroperasi pada layer Data Link, memancarkan sinyal Wi-Fi menggunakan Service Set Identifier (SSID) tertentu agar perangkat klien dapat menemukan dan terhubung ke jaringan tersebut.

Perbandingan Perangkat Jaringan Dasar

Perangkat	Layer OSI	Fungsi Utama
Hub	1 (Physical)	Menghubungkan perangkat, broadcast ke semua port
Switch	2 (Data Link)	Menghubungkan perangkat secara cerdas berdasarkan MAC address
Router	3 (Network)	Menghubungkan jaringan berbeda, menentukan jalur routing
Access Point	1–2 (Physical/Data Link)	Menjembatani perangkat nirkabel ke jaringan kabel

Kriteria Praktis Pemilihan Perangkat

Dalam merancang jaringan sederhana, teknisi perlu mempertimbangkan beberapa faktor praktis saat memilih perangkat: jumlah perangkat yang perlu terhubung (menentukan jumlah port switch yang dibutuhkan), kebutuhan menghubungkan ke jaringan berbeda atau internet (menentukan kebutuhan router), kebutuhan akses nirkabel (menentukan kebutuhan access point), serta anggaran dan skalabilitas di masa depan. Sekolah dengan laboratorium komputer misalnya umumnya memerlukan minimal satu switch untuk menghubungkan seluruh PC, satu router sebagai gateway ke internet, dan satu atau lebih access point apabila mendukung akses Wi-Fi bagi peserta didik dan tenaga pendidik.

Aktivitas Pembelajaran

Peserta didik mengamati dan mengidentifikasi perangkat jaringan yang tersedia di laboratorium sekolah (switch, router, access point) beserta spesifikasi dasarnya.

Peserta didik membangun topologi sederhana pada Cisco Packet Tracer menggunakan satu router, satu switch, dan beberapa PC untuk memahami peran masing-masing perangkat.

Diskusi kelompok: dalam skenario apa sebuah jaringan cukup menggunakan switch saja tanpa router, dan dalam skenario apa router menjadi wajib?

Rangkuman

Perangkat jaringan dasar terdiri atas hub, switch, router, dan access point, yang masing-masing beroperasi pada layer OSI berbeda dan memiliki fungsi spesifik. Switch menjadi perangkat sentral pada jaringan LAN modern karena efisiensinya, sementara router menjadi wajib ketika menghubungkan jaringan yang berbeda. Pemahaman ini menjadi fondasi sebelum mempelajari konfigurasi dan desain jaringan pada bab-bab selanjutnya.

Soal Latihan / Refleksi

Jelaskan perbedaan cara kerja hub dan switch dalam meneruskan data.

Pada layer OSI berapa router beroperasi, dan apa fungsi utamanya?

Jelaskan fungsi access point dalam sebuah jaringan yang menggabungkan perangkat kabel dan nirkabel.

Mengapa switch dianggap lebih efisien dibanding hub dalam hal collision domain?

BAB 8 — Pengantar MikroTik & RouterOS

Mengenal ekosistem MikroTik, RouterOS, dan RouterBOARD sebagai fondasi sebelum masuk ke konfigurasi teknis.

Tujuan Pembelajaran

Peserta didik memahami apa itu MikroTik, RouterOS, dan RouterBOARD.

Peserta didik mampu membedakan lini produk RouterBOARD dan jenjang lisensi RouterOS.

Peserta didik memahami jalur sertifikasi resmi MikroTik dan kedudukannya di dunia kerja.

12.1 Apa itu MikroTik?

MikroTik adalah perusahaan asal Latvia yang memproduksi perangkat keras jaringan (router, switch, access point) dan mengembangkan sistem operasi jaringan bernama RouterOS. MikroTik dikenal luas di kalangan ISP kecil-menengah, WISP (Wireless ISP), sekolah, dan perusahaan karena menawarkan fitur jaringan kelas enterprise dengan harga perangkat yang jauh lebih terjangkau dibanding vendor besar seperti Cisco atau Juniper.

Terdapat dua produk inti MikroTik yang perlu dipahami sejak awal. RouterOS adalah sistem operasi (mirip Linux) yang menjalankan fungsi routing, firewall, bridging, wireless, VPN, QoS, dan berbagai layanan jaringan lainnya. RouterBOARD (RB) adalah perangkat keras buatan MikroTik yang sudah terpasang RouterOS di dalamnya, siap pakai layaknya router pada umumnya.

Perlu diketahui: *RouterOS tidak selalu terikat pada RouterBOARD. RouterOS juga dapat diinstal di PC/server biasa (x86) maupun dijalankan sebagai virtual machine melalui image Cloud Hosted Router (CHR).*

12.2 Lini Produk RouterBOARD

RouterBOARD hadir dalam berbagai bentuk sesuai kebutuhan penggunaan, mulai dari perangkat wireless outdoor untuk koneksi jarak jauh hingga router performa tinggi untuk jaringan skala besar.

Kategori	Contoh Seri	Kegunaan Utama
Wireless Outdoor	SXT, LHG, Groove	Point-to-Point / Point-to-Multipoint jarak jauh
Wireless Indoor	hAP, cAP	Access point rumah/kantor
Router Indoor	RB750, RB951, RB4011	Router kantor/rumah dengan port Ethernet
Cloud Core Router (CCR)	CCR1036, CCR2004	Router performa tinggi berbasis multi-core CPU
Cloud Router Switch (CRS)	CRS326, CRS328	Switch layer 2/3 dengan kemampuan RouterOS penuh
Embedded RB	RB912, RB912UAG	Board tertanam untuk perangkat custom/outdoor

12.3 Level Lisensi RouterOS

RouterOS menggunakan sistem lisensi berjenjang (level) yang membatasi fitur dan jumlah pengguna

simultan yang dapat memakai fitur tertentu, misalnya jumlah user Hotspot atau PPPoE. Pada RouterBOARD, lisensi biasanya sudah tertanam (built-in) sesuai model perangkat.

Level	Karakteristik Utama
Level 0 (Trial)	Gratis, berlaku 24 jam, untuk uji coba instalasi baru
Level 1 (Demo)	Terbatas, biasanya untuk perangkat SOHO ringan (hanya WiFi client tanpa AP)
Level 3	Umum ditemukan di RouterBOARD kelas SOHO, mendukung fitur routing dasar
Level 4	Lisensi standar untuk sebagian besar RouterBOARD wireless
Level 5	Menambah kapasitas jumlah user Hotspot/PPPoE dibanding Level 4
Level 6	Lisensi penuh tanpa batasan, umum dipakai di CCR dan CHR produksi

12.4 Jalur Sertifikasi MikroTik

MikroTik menyediakan jalur sertifikasi resmi berjenjang. MTCNA (MikroTik Certified Network Associate) adalah sertifikasi level dasar dan menjadi syarat wajib sebelum mengambil sertifikasi tingkat lanjut apa pun, seperti MTCRE (Routing Engineer), MTCWE (Wireless Engineer), MTCTCE (Traffic Control Engineer), MTCUME (User Management Engine), hingga MTCINE (Internetworking Engineer) sebagai jenjang tertinggi.

Format Ujian MTCNA: *Ujian sertifikasi dilakukan secara daring di situs resmi MikroTik, terdiri dari 25 soal pilihan ganda dalam waktu 60 menit, dengan nilai minimum kelulusan umumnya 60%.*

Banyak WISP dan penyedia jaringan skala kecil-menengah di Indonesia mensyaratkan MTCNA sebagai standar minimum bagi teknisi lapangan, karena sertifikasi ini membuktikan kompetensi dasar yang terukur dan diakui secara internasional. Banyak pula NOC (Network Operations Center) perusahaan menggunakan RouterOS sebagai edge router karena rasio harga terhadap fitur yang kompetitif, sehingga kompetensi MikroTik menjadi nilai tambah tersendiri bagi lulusan TJKT saat memasuki dunia kerja.

Aktivitas Pembelajaran

Peserta didik mencari dan membandingkan spesifikasi tiga seri RouterBOARD berbeda (misalnya hAP lite, RB750, dan CCR1009) melalui situs resmi MikroTik, lalu mendiskusikan kegunaan masing-masing.

Peserta didik membuat peta jalur sertifikasi MikroTik dalam bentuk diagram sederhana, mulai dari MTCNA hingga MTCINE.

Diskusi kelompok: mengapa banyak WISP di Indonesia lebih memilih perangkat MikroTik dibanding vendor enterprise seperti Cisco untuk jaringan skala kecil-menengah?

Rangkuman

MikroTik adalah vendor perangkat jaringan yang mengembangkan sistem operasi RouterOS dan perangkat keras RouterBOARD. RouterBOARD hadir dalam berbagai lini sesuai kebutuhan, sementara

RouterOS menggunakan sistem lisensi berjenjang dari Level 0 hingga Level 6. MTCNA menjadi sertifikasi dasar wajib sebagai gerbang menuju jenjang sertifikasi MikroTik lanjutan, dan menjadi bekal penting sebelum mempelajari instalasi dan konfigurasi RouterOS pada bab berikutnya.

Soal Latihan / Refleksi

Jelaskan perbedaan mendasar antara RouterOS dan RouterBOARD.

Sebutkan minimal tiga lini produk RouterBOARD beserta kegunaannya masing-masing.

Mengapa MTCNA menjadi syarat wajib sebelum mengambil sertifikasi MikroTik lainnya?

Jelaskan perbedaan antara lisensi Level 4 dan Level 6 pada RouterOS.

BAB 9 — Instalasi & Manajemen RouterOS

Mempelajari metode instalasi RouterOS dan cara mengakses router untuk pertama kali menggunakan Winbox, WebFig, maupun CLI.

Tujuan Pembelajaran

Peserta didik mampu menjelaskan berbagai metode instalasi/reinstalasi RouterOS.

Peserta didik mampu mengakses router melalui Winbox, WebFig, SSH, dan Telnet.

Peserta didik memahami dasar navigasi CLI RouterOS serta proses upgrade/downgrade yang aman.

12.5 Metode Instalasi RouterOS

RouterOS dapat dipasang melalui beberapa jalur tergantung jenis perangkat yang digunakan. Pada RouterBOARD bawaan, RouterOS sudah terpasang dari pabrik dan tinggal dikonfigurasi. Netinstall adalah alat instalasi ulang RouterOS dari nol melalui jaringan Ethernet, umum dipakai saat perangkat gagal boot atau ingin mengganti versi secara bersih. CHR (Cloud Hosted Router) adalah image RouterOS untuk dijalankan sebagai virtual machine, sementara instalasi di PC/x86 memungkinkan RouterOS dipasang langsung pada perangkat PC atau server biasa dari media instalasi.

12.6 Proses Netinstall

Netinstall adalah tool berbasis Windows yang memungkinkan instalasi ulang RouterOS ke RouterBOARD melalui jaringan, tanpa perlu kartu memori tambahan. Langkah umum penggunaannya meliputi: mengunduh paket Netinstall dan file RouterOS (.npk) sesuai arsitektur perangkat dari situs resmi MikroTik; menghubungkan PC dan RouterBOARD dalam satu jaringan Ethernet lalu menyesuaikan IP address Netinstall; menyalakan ulang RouterBOARD sambil menahan tombol reset agar masuk ke mode Netinstall/Etherboot; memilih perangkat yang terdeteksi dan paket RouterOS yang ingin dipasang; dan menunggu proses selesai hingga router reboot otomatis dalam kondisi default.

Kapan Netinstall dibutuhkan?: *Netinstall paling sering dipakai ketika router lupa password total tanpa akses backup, RouterOS mengalami corrupt, atau ingin melakukan downgrade ke versi RouterOS yang jauh lebih lama secara bersih.*

12.7 Mengakses Router: Winbox, WebFig, SSH, Telnet

Metode	Karakteristik
Winbox	Aplikasi desktop berbasis GUI, paling umum dipakai,

	terhubung via IP atau MAC address
WebFig	Antarmuka konfigurasi berbasis browser web, cocok untuk akses cepat tanpa instal aplikasi
SSH	Akses command line terenkripsi, aman untuk manajemen jarak jauh
Telnet	Akses command line tanpa enkripsi, tidak disarankan untuk jaringan publik
MAC-Winbox	Koneksi ke router menggunakan MAC address, berguna saat router belum punya IP address

Winbox mendukung dua metode koneksi: melalui IP address, jika router sudah memiliki alamat IP dan dapat dijangkau, atau melalui MAC address, yang memanfaatkan broadcast Layer 2 dan berguna saat konfigurasi awal sebelum IP diset.

12.8 Dasar Command Line Interface (CLI)

RouterOS memiliki struktur perintah CLI berbasis menu bertingkat, mirip struktur direktori. Tombol Tab digunakan untuk melengkapi otomatis nama menu atau parameter, tanda tanya (?) menampilkan daftar perintah yang tersedia pada level menu saat itu, tanda garis miring (/) mengembalikan ke menu root, dan tanda titik dua kali (..) mengembalikan satu level ke menu sebelumnya. Command history dapat diakses dengan tombol panah atas/bawah untuk mengulang perintah sebelumnya.

```
/ip address print
/interface print
/system identity set name=Router-Sekolah
/ip service print
```

12.9 Upgrade dan Downgrade RouterOS

RouterOS memiliki dua jenis paket, yaitu paket utama (routeros) dan paket tambahan seperti wireless, ipv6, atau dude yang dapat dipasang terpisah sesuai kebutuhan. Cara termudah melakukan upgrade adalah melalui menu System > Packages > Check for Updates pada Winbox. Cara manual dilakukan dengan mengunduh file paket .npk sesuai arsitektur perangkat, mengunggahnya ke router melalui menu Files, lalu me-reboot router untuk memicu instalasi otomatis. Downgrade dilakukan dengan cara serupa menggunakan file paket versi lebih lama.

Perhatian: *Selalu lakukan backup konfigurasi sebelum melakukan upgrade/downgrade RouterOS, terutama pada perangkat produksi, untuk menghindari kehilangan konfigurasi akibat kegagalan proses update.*

12.10 RouterBOOT Firmware Upgrade

Selain paket RouterOS itu sendiri, setiap RouterBOARD memiliki firmware tingkat rendah bernama RouterBOOT, setara BIOS/UEFI pada PC, yang bertanggung jawab pada proses boot awal perangkat sebelum RouterOS dimuat. RouterBOOT dan RouterOS adalah dua komponen terpisah yang di-upgrade secara independen.

```
/system routerboard print
/system routerboard upgrade
/system reboot
```

Perbedaan penting: *Meng-upgrade paket RouterOS tidak secara otomatis meng-upgrade RouterBOOT. Banyak kasus router berjalan tidak stabil setelah update besar RouterOS disebabkan oleh RouterBOOT yang tertinggal jauh dari versi RouterOS yang berjalan di atasnya, sehingga upgrade RouterBOOT harus dilakukan sebagai langkah terpisah.*

Aktivitas Pembelajaran

Peserta didik menghubungkan laptop ke router MikroTik menggunakan kabel LAN, membuka Winbox, dan login menggunakan koneksi MAC address ke perangkat dalam kondisi default pabrik.

Peserta didik mengganti nama identitas router melalui menu System > Identity, kemudian memeriksa versi RouterOS dan RouterBOOT yang terpasang melalui menu System > Packages dan System > RouterBOARD.

Peserta didik membuka New Terminal dan menjalankan perintah "/system resource print" untuk mengamati informasi CPU, memori, serta versi RouterOS yang aktif.

Rangkuman

RouterOS dapat diinstal melalui berbagai metode sesuai jenis perangkat, dengan Netinstall sebagai solusi utama untuk reinstalasi bersih melalui jaringan. Router dapat diakses melalui Winbox, WebFig, SSH, atau Telnet, dengan SSH menjadi pilihan paling aman untuk manajemen jarak jauh. Proses upgrade RouterOS dan RouterBOOT bersifat terpisah dan keduanya perlu dilakukan secara disiplin agar perangkat tetap stabil, menjadi dasar sebelum mempelajari konfigurasi jaringan pada bab berikutnya.

Soal Latihan / Refleksi

Sebutkan tiga metode instalasi RouterOS beserta situasi yang tepat untuk masing-masing metode.

Kapan sebaiknya Netinstall digunakan dibanding proses upgrade biasa?

Jelaskan perbedaan koneksi Winbox melalui IP address dan melalui MAC address.

Mengapa Telnet dianggap kurang aman dibanding SSH untuk manajemen jarak jauh?

Jelaskan perbedaan antara upgrade paket RouterOS dan upgrade RouterBOOT, dan mengapa keduanya perlu dilakukan terpisah.

BAB 10 — Konfigurasi Dasar Router

Membangun konfigurasi jaringan dasar: pengalamatan IP, default gateway, DNS, hingga koneksi internet pertama melalui NAT masquerade.

Tujuan Pembelajaran

Peserta didik mampu mengonfigurasi IP address pada interface RouterOS.

Peserta didik mampu mengonfigurasi default gateway dan DNS pada router.

Peserta didik mampu menghubungkan jaringan lokal ke internet menggunakan NAT masquerade serta melakukan troubleshooting dasar.

12.11 Topologi Dasar Jaringan MikroTik

Skenario paling umum dalam praktik konfigurasi MikroTik adalah router yang memiliki dua sisi jaringan: sisi WAN yang terhubung ke internet/ISP, dan sisi LAN yang terhubung ke jaringan lokal atau klien. Konsep dasar yang wajib dipahami sebelum mengonfigurasi adalah membedakan interface mana yang berfungsi sebagai WAN dan mana yang berfungsi sebagai LAN, sebagaimana telah diperkenalkan pada pembahasan router dan topologi jaringan di bab-bab sebelumnya.

12.12 Konfigurasi IP Address

IP address di RouterOS diikatkan pada sebuah interface, misalnya ether1, ether2, atau wlan1. Format penulisan menggunakan notasi CIDR (Classless Inter-Domain Routing), sebagaimana telah dipelajari pada konsep subnetting, misalnya 192.168.1.1/24.

```
/ip address add address=192.168.1.1/24 interface=ether2
/ip address print
```

Prefix (CIDR)	Subnet Mask	Jumlah Host Usable
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14
/30	255.255.255.252	2 (umum untuk link point-to-point)

12.13 Default Gateway & DNS

Default gateway adalah rute yang digunakan router saat tidak ada rute spesifik lain yang cocok dengan tujuan paket, biasanya mengarah ke perangkat ISP. DNS diperlukan agar router, dan klien di baliknya jika DNS diaktifkan sebagai cache, dapat menerjemahkan nama domain menjadi IP address.

```
/ip route add dst-address=0.0.0.0/0 gateway=192.168.1.254
/ip dns set servers=8.8.8.8,1.1.1.1 allow-remote-requests=yes
```

allow-remote-requests: *Parameter ini membuat router berfungsi sebagai DNS cache/relay untuk klien di jaringan lokal, sehingga klien cukup mengarahkan DNS mereka ke IP router, bukan langsung ke DNS publik.*

12.14 Koneksi WAN via DHCP Client

Jika ISP menyediakan IP secara dinamis, sebagaimana umum ditemui pada koneksi rumahan, interface WAN router cukup diset sebagai DHCP client agar otomatis menerima IP address, gateway, dan DNS dari ISP.

```
/ip dhcp-client add interface=ether1 disabled=no
/ip dhcp-client print
```

12.15 NAT Masquerade — Menghubungkan LAN ke Internet

Karena IP address di jaringan lokal umumnya bersifat privat dan tidak dapat dirutekan langsung di internet, diperlukan NAT (Network Address Translation) tipe masquerade agar seluruh trafik dari LAN keluar menggunakan IP publik router saat menuju internet.

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

Rule ini berarti setiap paket yang keluar melalui interface ether1 (WAN) akan diubah source IP-nya menjadi IP address ether1 itu sendiri, sehingga balasan dari internet dapat kembali dengan benar ke router dan diteruskan ke klien yang bersangkutan.

12.16 Troubleshooting Konektivitas Dasar

Perintah ping digunakan untuk menguji konektivitas dasar ke gateway, DNS, atau internet, sedangkan perintah "/tool traceroute" digunakan untuk melihat jalur yang dilalui paket menuju tujuan. Perintah "/ip route print" memastikan default route sudah ada dan berstatus aktif, sementara "/ip firewall nat print" memastikan rule masquerade sudah terpasang dengan urutan yang benar.

Metodologi troubleshooting yang disiplin sangat penting di dunia kerja: dimulai dari lapisan terendah (fisik/link, apakah lampu interface menyala dan kabel tersambung), lanjut ke lapisan IP (apakah IP address dan gateway benar), lalu ke lapisan aplikasi (apakah DNS resolve, apakah port yang dituju terbuka). Pendekatan bottom-up seperti ini sejalan dengan pendekatan troubleshooting berlapis yang telah dipelajari pada Bab 2 tentang model OSI.

Aktivitas Pembelajaran

Peserta didik mengatur ether1 sebagai interface WAN dengan DHCP client aktif, dan ether2 sebagai interface LAN dengan IP statis 192.168.10.1/24.

Peserta didik menambahkan rule NAT masquerade untuk interface WAN, menghubungkan laptop ke ether2, dan menguji ping berjenjang dari gateway, ke DNS publik (8.8.8.8), hingga ke nama domain (google.com).

Jika ping ke domain gagal namun ping ke 8.8.8.8 berhasil, peserta didik memeriksa kembali konfigurasi DNS pada router sebagai latihan troubleshooting.

Rangkuman

Konfigurasi dasar router MikroTik meliputi pemasangan IP address pada interface, penetapan default gateway dan DNS, serta penggunaan NAT masquerade agar jaringan lokal dapat mengakses internet. Pendekatan troubleshooting berlapis, dimulai dari lapisan fisik hingga aplikasi, menjadi keterampilan wajib untuk mengisolasi gangguan jaringan secara sistematis, dan menjadi dasar sebelum mempelajari konfigurasi DHCP server pada bab berikutnya.

Soal Latihan / Refleksi

Jelaskan fungsi default gateway pada tabel routing.

Mengapa diperlukan NAT masquerade agar jaringan lokal dapat mengakses internet?

Apa perbedaan antara mengatur IP WAN secara statis dan menggunakan DHCP client?

Sebutkan langkah troubleshooting jika klien tidak bisa browsing meski ping ke IP publik berhasil.

BAB 11 — DHCP Server & Client

Memahami cara kerja DHCP pada RouterOS, baik sebagai client yang menerima IP dari jaringan atas, maupun sebagai server yang membagikan IP ke klien di bawahnya.

Tujuan Pembelajaran

Peserta didik mampu mengonfigurasi DHCP server lengkap dengan pool, network, dan lease.

Peserta didik mampu membedakan dynamic lease dan static lease serta manfaat keamanannya.

Peserta didik memahami mekanisme ARP yang mendukung proses DHCP dalam jaringan Layer 2.

12.17 Konsep DHCP

DHCP (Dynamic Host Configuration Protocol) adalah protokol yang memungkinkan perangkat klien memperoleh konfigurasi IP address, subnet mask, gateway, dan DNS secara otomatis dari sebuah server, tanpa perlu dikonfigurasi manual satu per satu — konsep yang sama seperti telah dipelajari pada pembahasan layanan jaringan dasar.

RouterOS dapat berperan sebagai dua sisi sekaligus dalam jaringan berbeda: sebagai DHCP client di sisi WAN untuk menerima IP dari ISP, dan sebagai DHCP server di sisi LAN untuk membagikan IP ke perangkat klien.

12.18 Konfigurasi DHCP Server

RouterOS menyediakan wizard “DHCP Setup” yang mempercepat proses konfigurasi, namun pemahaman komponen manualnya tetap penting bagi teknisi jaringan.

Komponen	Fungsi
DHCP Server	Objek utama yang mengaktifkan layanan DHCP pada sebuah interface
IP Pool	Rentang IP address yang akan dibagikan ke klien
DHCP Network	Mendefinisikan gateway, DNS, dan parameter jaringan untuk subnet tertentu
Lease	Catatan IP yang sedang/pernah dipinjamkan ke klien tertentu berdasarkan MAC address

```
/ip pool add name=pool-lan ranges=192.168.10.10-192.168.10.200
/ip dhcp-server add name=dhcp-lan interface=ether2 address-pool=pool-lan disabled=no
/ip dhcp-server network add address=192.168.10.0/24 gateway=192.168.10.1 dns-
server=8.8.8.8
```

12.19 DHCP Lease dan Static Lease

Setiap kali klien menerima IP dari DHCP server, informasi tersebut tercatat di menu Leases, yang berguna untuk memantau perangkat mana saja yang aktif di jaringan. Untuk perangkat yang memerlukan IP tetap, misalnya printer, server, atau access point, administrator dapat membuat static lease yang mengikat MAC address tertentu agar selalu mendapat IP address yang sama.

```
/ip dhcp-server lease add address=192.168.10.50 mac-address=AA:BB:CC:DD:EE:FF
server=dhcp-lan
```

Tips Keamanan DHCP: *Fitur “DHCP Static Only” dapat mengunci server sehingga hanya perangkat dengan static lease terdaftar yang bisa mendapat IP, sementara perangkat asing otomatis ditolak — salah satu bentuk keamanan dasar pada jaringan yang membutuhkan kontrol ketat terhadap perangkat yang terhubung.*

12.20 Address Resolution Protocol (ARP)

ARP adalah protokol yang menerjemahkan IP address menjadi MAC address dalam jaringan Layer 2, sehingga paket data dapat dikirim ke perangkat yang tepat pada level fisik. RouterOS mendukung beberapa mode ARP pada interface.

Mode ARP	Perilaku
enabled	Mode default, ARP bekerja normal (otomatis belajar dan merespons)
disabled	ARP dimatikan sepenuhnya pada interface tersebut, komunikasi memerlukan entry ARP statis
proxy-arp	Router menjawab ARP request atas nama perangkat lain di jaringan berbeda
reply-only	Router hanya menjawab ARP request untuk entry yang sudah didaftarkan secara statis, kombinasi keamanan populer dengan static lease DHCP

Aktivitas Pembelajaran

Peserta didik membuat IP Pool dengan rentang 192.168.20.10 sampai 192.168.20.100, kemudian membuat DHCP Server pada interface ether3 menggunakan pool tersebut beserta DHCP Network-nya.

Peserta didik menghubungkan laptop ke ether3, memverifikasi laptop menerima IP otomatis, lalu mencatat MAC address yang muncul pada menu DHCP Server > Leases.

Peserta didik membuat static lease untuk MAC address laptop tersebut agar selalu mendapat IP 192.168.20.50, kemudian memutus dan menyambungkan kembali koneksi untuk memverifikasi hasilnya.

Rangkuman

DHCP pada RouterOS memungkinkan perangkat berperan sebagai client maupun server sekaligus dalam jaringan yang berbeda. Konfigurasi DHCP server terdiri atas komponen pool, network, dan lease, dengan static lease menjadi solusi bagi perangkat yang membutuhkan IP tetap. Pemahaman ARP melengkapi konsep ini sebagai mekanisme dasar penerjemahan IP ke MAC address, dan menjadi dasar sebelum mempelajari konsep bridging dan switching pada bab berikutnya.

Soal Latihan / Refleksi

Jelaskan tiga komponen utama yang membentuk sebuah DHCP server pada RouterOS.

Apa perbedaan antara dynamic lease dan static lease?

Bagaimana fitur “DHCP Static Only” dapat meningkatkan keamanan jaringan?

Jelaskan fungsi mode ARP “reply-only” dan kapan sebaiknya digunakan.

BAB 12 — Bridging & Switching

Memahami konsep penggabungan beberapa interface menjadi satu segmen jaringan Layer 2 menggunakan bridge, serta pengenalan Spanning Tree Protocol.

Tujuan Pembelajaran

Peserta didik mampu menjelaskan konsep bridging dan perbedaannya dengan routing.

Peserta didik mampu membuat dan mengonfigurasi bridge pada RouterOS.

Peserta didik memahami dasar STP/RSTP untuk mencegah loop jaringan.

12.21 Konsep Bridging

Bridge adalah fitur yang menggabungkan dua atau lebih interface fisik, baik Ethernet maupun wireless, menjadi satu segmen jaringan Layer 2 yang sama, seolah-olah seluruh perangkat yang terhubung berada dalam satu switch. Ini berbeda dengan routing, yang bekerja di Layer 3 dan memisahkan jaringan menjadi subnet-subnet berbeda, sebagaimana telah dibedakan pada pembahasan perangkat jaringan dasar.

Kapan menggunakan Bridge?: *Bridge umum digunakan saat ingin menggabungkan beberapa port Ethernet menjadi satu jaringan LAN yang sama, menghubungkan segmen wireless dan wired dalam satu broadcast domain, atau membuat access point transparan tanpa perlu routing/NAT tambahan.*

12.22 Membuat Bridge

```
/interface bridge add name=bridge-lan
/interface bridge port add bridge=bridge-lan interface=ether2
/interface bridge port add bridge=bridge-lan interface=ether3
/ip address add address=192.168.10.1/24 interface=bridge-lan
```

Setelah interface digabungkan ke dalam bridge, IP address sebaiknya dipasang pada interface bridge itu sendiri, bukan pada masing-masing port fisik, karena bridge kini merepresentasikan keseluruhan segmen jaringan tersebut.

12.23 Bridge Software vs Hardware Offload

Pada perangkat MikroTik dengan switch chip khusus, bridge dapat memanfaatkan hardware offload, yaitu proses forwarding paket yang ditangani langsung oleh chip switch, bukan oleh CPU utama, sehingga performa jauh lebih tinggi (mendekati kecepatan wire-speed) dan beban CPU jauh berkurang dibanding bridge software murni.

Aspek	Bridge Software	Hardware Offload
Pemrosesan	Ditangani CPU	Ditangani switch chip khusus
Performa	Terbatas oleh kemampuan CPU	Mendekati wire-speed, jauh lebih tinggi
Fleksibilitas fitur	Mendukung semua fitur RouterOS	Beberapa fitur lanjutan mungkin tidak didukung penuh

12.24 Spanning Tree Protocol (STP/RSTP)

Ketika terdapat lebih dari satu jalur fisik yang saling terhubung antar switch atau bridge, misalnya untuk redundansi, berpotensi terjadi loop Layer 2 yang menyebabkan broadcast storm dan melumpuhkan jaringan. STP (Spanning Tree Protocol) dan versi yang lebih cepat, RSTP (Rapid STP), bekerja mendeteksi loop tersebut dan secara otomatis memblokir salah satu jalur redundan sampai dibutuhkan, misalnya saat jalur utama terputus.

```
/interface bridge set bridge-lan protocol-mode=rstp
```

12.25 Bridge Firewall dan Switch Chip

RouterOS menyediakan firewall khusus untuk trafik yang melewati bridge, terpisah dari firewall IP biasa, karena trafik pada bridge beroperasi di Layer 2 dan bisa saja berupa paket non-IP. Pada perangkat dengan lebih dari satu switch chip, penting pula memahami switch chip group — port-port yang berada pada chip fisik yang sama dapat memanfaatkan hardware offload penuh, sedangkan penggabungan lintas chip mungkin memerlukan penanganan khusus.

Sebagai ilustrasi penerapan di lapangan, WISP sering menggunakan bridge, bukan routing, pada perangkat CPE pelanggan agar pelanggan menerima IP publik langsung dari core network ISP. Pada topologi menara BTS dengan banyak sektor antena, hardware offload bridge menjadi krusial karena volume trafik yang melewati satu RouterBOARD dapat mencapai ratusan Mbps hingga beberapa Gbps.

Aktivitas Pembelajaran

Peserta didik membuat interface bridge baru bernama “bridge-lab”, menambahkan ether2 dan ether3 sebagai port bridge tersebut, lalu memasang IP address 192.168.30.1/24 pada interface bridge-lab.

Peserta didik menghubungkan dua laptop ke ether2 dan ether3 dengan IP manual pada subnet yang sama, lalu menguji ping antar keduanya untuk memverifikasi bahwa keduanya berada dalam satu broadcast domain meski terhubung ke port fisik berbeda.

Peserta didik mengaktifkan RSTP pada bridge tersebut dan mengamati menu Bridge > STP untuk melihat status tiap port.

Rangkuman

Bridging pada RouterOS menggabungkan beberapa interface fisik menjadi satu segmen jaringan Layer 2, berbeda dengan routing yang bekerja pada Layer 3. Hardware offload meningkatkan performa bridge secara signifikan pada perangkat yang mendukungnya, sementara STP/RSTP mencegah terjadinya loop dan broadcast storm pada jaringan dengan jalur redundan. Pemahaman konsep Layer 2 ini melengkapi kompetensi dasar sebelum peserta didik melanjutkan ke pembahasan pengalamatan IP dan subnetting secara lebih mendalam pada bab berikutnya.

Soal Latihan / Refleksi

Jelaskan perbedaan mendasar antara bridging (Layer 2) dan routing (Layer 3).

Mengapa IP address sebaiknya dipasang pada interface bridge, bukan pada port fisik individual?

Apa fungsi utama STP/RSTP dalam sebuah jaringan dengan jalur redundan?

Jelaskan keuntungan performa dari hardware offload dibanding bridge software murni.

BAB 13 — Pengalamatan IPv4 dan Subnetting

Tujuan Pembelajaran

Peserta didik mampu menjelaskan struktur dan kelas alamat IPv4.

Peserta didik mampu menjelaskan fungsi subnet mask dan notasi CIDR.

Peserta didik mampu melakukan perhitungan subnetting sederhana untuk kebutuhan segmentasi jaringan.

Struktur Alamat IPv4

Alamat IP versi 4 (IPv4) terdiri atas 32 bit yang ditulis dalam empat oktet berformat desimal bertitik (dotted decimal notation), misalnya 192.168.1.1. Setiap oktet merepresentasikan 8 bit biner dengan rentang nilai desimal 0 hingga 255. Sebuah alamat IP terdiri atas dua bagian: **network ID** yang mengidentifikasi jaringan tempat perangkat berada, dan **host ID** yang mengidentifikasi perangkat spesifik dalam jaringan tersebut.

Kelas Alamat IPv4

Alamat IPv4 secara historis dibagi menjadi lima kelas berdasarkan nilai oktet pertamanya, meskipun pada praktik jaringan modern pembagian kelas sudah banyak digantikan oleh pendekatan classless (CIDR) yang lebih fleksibel.

Kelas	Rentang Oktet Pertama	Default Subnet Mask	Penggunaan
A	1–126	255.0.0.0 (/8)	Jaringan skala sangat besar
B	128–191	255.255.0.0 (/16)	Jaringan skala menengah–besar
C	192–223	255.255.255.0 (/24)	Jaringan skala kecil
D	224–239	—	Multicast
E	240–255	—	Eksperimental/riset

Perlu dicatat bahwa oktet pertama 127 dicadangkan untuk alamat loopback (127.0.0.1), dan terdapat rentang alamat privat yang tidak dirutekan di internet publik: 10.0.0.0/8, 172.16.0.0/12, dan 192.168.0.0/16, yang lazim digunakan pada jaringan lokal seperti laboratorium sekolah atau kantor.

Subnet Mask dan Notasi CIDR

Subnet mask adalah rangkaian 32 bit yang menentukan bagian mana dari alamat IP yang merupakan network ID dan bagian mana yang merupakan host ID. Classless Inter-Domain Routing (CIDR) memperkenalkan notasi ringkas dengan menuliskan jumlah bit network setelah tanda garis miring, misalnya /24 yang setara dengan subnet mask 255.255.255.0.

Notasi CIDR	Subnet Mask	Jumlah Host Usable
/24	255.255.255.0	254
/25	255.255.255.128	126

Notasi CIDR	Subnet Mask	Jumlah Host Usable
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14
/30	255.255.255.252	2

Perhitungan Subnetting Sederhana

Subnetting adalah proses membagi sebuah jaringan besar menjadi beberapa jaringan yang lebih kecil (subnet) untuk efisiensi pengalamatan dan segmentasi jaringan. Jumlah host yang dapat digunakan pada sebuah subnet dihitung dengan rumus 2 pangkat (jumlah bit host) dikurangi 2, karena alamat pertama dicadangkan sebagai network address dan alamat terakhir sebagai broadcast address.

Contoh perhitungan /27: Subnet mask /27 memiliki 5 bit host (32−27=5), sehingga jumlah total alamat adalah 2^5=32, dan jumlah host usable adalah 32−2=30. Blok subnet dihitung dari 256 dikurangi nilai oktet terakhir subnet mask (256−224=32), sehingga rentang subnet pertama pada jaringan 192.168.1.0/27 adalah 192.168.1.0 hingga 192.168.1.31, dengan network address 192.168.1.0, broadcast address 192.168.1.31, dan rentang host usable 192.168.1.1 sampai 192.168.1.30.

Contoh perhitungan /30: Subnet /30 hanya memiliki 2 bit host (32−30=2), menghasilkan total 4 alamat dengan 2 host usable. Subnet ini umum digunakan pada koneksi point-to-point antar router, misalnya jaringan 192.168.1.0/30 memiliki network address 192.168.1.0, host usable 192.168.1.1 dan 192.168.1.2, serta broadcast address 192.168.1.3.

Menentukan Network Address, Broadcast Address, dan Rentang Host

Untuk menentukan network address dari sebuah alamat IP dan subnet mask tertentu, dilakukan operasi AND biner antara alamat IP dan subnet mask. Broadcast address diperoleh dengan mengubah seluruh bit host menjadi 1. Langkah-langkah ini menjadi keterampilan wajib bagi teknisi jaringan dalam merancang dan mengonfigurasi pengalamatan IP pada perangkat jaringan maupun host.

Komponen	Contoh (192.168.1.0/27)
Network Address	192.168.1.0
Rentang Host Usable	192.168.1.1 – 192.168.1.30
Broadcast Address	192.168.1.31
Jumlah Host Usable	30

Latihan Terpandu: Membagi Jaringan dengan VLSM

Sebagai latihan terpandu, perhatikan studi kasus berikut. Sebuah sekolah memperoleh alokasi jaringan 192.168.20.0/24 dan perlu membaginya untuk tiga ruangan: Laboratorium Komputer (butuh 50 host), Ruang Guru (butuh 20 host), dan Ruang Tata Usaha (butuh 10 host). Prinsip yang digunakan adalah **VLSM**

(Variable Length Subnet Mask), yaitu membagi jaringan dengan ukuran subnet berbeda-beda sesuai kebutuhan masing-masing segmen, dimulai dari kebutuhan host terbesar agar alokasi alamat lebih efisien.

Segmen	Kebutuhan Host	Prefix Terpilih	Alokasi Subnet	Host Usable
Lab Komputer	50	/26 (62 host)	192.168.20.0/26	192.168.20.1–192.168.20.62
Ruang Guru	20	/27 (30 host)	192.168.20.64/27	192.168.20.65–192.168.20.94
Ruang TU	10	/28 (14 host)	192.168.20.96/28	192.168.20.97–192.168.20.110

Pendekatan VLSM ini jauh lebih efisien dibanding membagi rata ketiga ruangan dengan prefix /26 yang sama, karena Ruang TU yang hanya membutuhkan 10 host tidak perlu dialokasikan 62 alamat yang sebagian besar akan terbuang percuma. Efisiensi alokasi alamat seperti ini menjadi keterampilan penting dalam merancang jaringan skala menengah, dan menjadi materi pengantar bagi teknik subnetting lanjutan yang akan diperdalam pada mata pelajaran Administrasi Infrastruktur Jaringan.

Aktivitas Pembelajaran

Peserta didik berlatih menghitung network address, broadcast address, dan rentang host usable untuk lima soal subnetting dengan prefix bervariasi (/26, /27, /28, /29, /30).

Peserta didik memverifikasi hasil perhitungan manual menggunakan kalkulator subnetting daring atau aplikasi sejenis.

Praktik pada Cisco Packet Tracer: mengonfigurasi alamat IP statis dengan subnet mask tertentu pada beberapa PC dan menguji konektivitas antar host dalam subnet yang sama maupun berbeda.

Rangkuman

Pengalamatan IPv4 terdiri atas 32 bit yang dibagi menjadi network ID dan host ID, dengan subnet mask dan notasi CIDR menentukan pembagian tersebut. Subnetting memungkinkan sebuah jaringan besar dibagi menjadi beberapa subnet lebih kecil untuk efisiensi pengalamatan, dengan perhitungan network address, broadcast address, dan rentang host usable menjadi keterampilan dasar wajib bagi teknisi jaringan.

Soal Latihan / Refleksi

Sebuah jaringan menggunakan alamat 192.168.10.0/26. Tentukan network address, broadcast address, rentang host usable, dan jumlah host usable.

Jelaskan perbedaan penggunaan subnet /30 dibanding /24 dalam konteks jaringan nyata.

Mengapa alamat pertama dan terakhir pada sebuah subnet tidak dapat digunakan sebagai alamat host?

Sebutkan tiga rentang alamat IP privat yang didefinisikan untuk jaringan lokal.

BAB 14 — Pengalamatan IPv6 Dasar

Tujuan Pembelajaran

Peserta didik mampu menjelaskan latar belakang pengembangan IPv6.

Peserta didik mampu membaca dan menuliskan format alamat IPv6 termasuk bentuk penyingkatannya.

Peserta didik mampu mengonfigurasi alamat IPv6 dasar pada interface perangkat jaringan.

Latar Belakang IPv6

Internet Protocol version 6 (IPv6) dikembangkan sebagai solusi atas keterbatasan jumlah alamat pada IPv4, yang hanya menyediakan sekitar 4,3 miliar alamat unik — jumlah yang semakin tidak mencukupi seiring pertumbuhan pesat perangkat yang terhubung ke internet. IPv6 menggunakan alamat 128 bit, jauh lebih besar dibanding 32 bit pada IPv4, sehingga mampu menyediakan jumlah alamat yang praktis tidak akan habis dalam waktu dekat.

Format Penulisan Alamat IPv6

Alamat IPv6 ditulis dalam delapan kelompok bilangan heksadesimal 16-bit yang dipisahkan oleh tanda titik dua, misalnya 2001:0db8:0000:0000:0000:ff00:0042:8329. Untuk mempermudah penulisan, terdapat dua aturan penyingkatan yang dapat diterapkan.

Penghilangan angka nol di depan setiap kelompok — misalnya 0db8 dapat ditulis menjadi db8.

Penyingkatan kelompok nol berurutan dengan tanda :: (dua titik dua) — hanya boleh digunakan satu kali dalam satu alamat untuk menghindari ambiguitas. Contoh: 2001:0db8:0000:0000:0000:ff00:0042:8329 dapat disingkat menjadi 2001:db8::ff00:42:8329.

Jenis Alamat IPv6

IPv6 mengenal tiga jenis alamat utama yang menggantikan konsep broadcast pada IPv4 (yang ditiadakan pada IPv6).

Jenis Alamat	Deskripsi
Unicast	Alamat untuk satu interface tunggal, data dikirim ke satu tujuan spesifik
Multicast	Alamat untuk sekelompok interface, data dikirim ke seluruh anggota grup
Anycast	Alamat yang dapat dimiliki banyak interface, data dikirim ke interface terdekat

Alamat unicast sendiri terbagi menjadi beberapa tipe, di antaranya **Global Unicast Address** (dapat dirutekan di internet publik, analog dengan alamat publik pada IPv4), **Link-Local Address** (hanya berlaku pada segmen jaringan lokal, diawali dengan fe80::/10, dan dibuat otomatis pada setiap interface yang aktif), serta **Unique Local Address** (analog dengan alamat privat pada IPv4, diawali dengan fc00::/7).

Konfigurasi Alamat IPv6 pada Interface

Konfigurasi alamat IPv6 pada perangkat Cisco dilakukan melalui mode konfigurasi interface menggunakan perintah dasar berikut, yang dapat dipraktikkan langsung pada Cisco Packet Tracer.

Perintah	Fungsi
Router(config)# ipv6 unicast-routing	Mengaktifkan proses routing IPv6 pada router
Router(config-if)# ipv6 address 2001:db8:1::1/64	Menetapkan alamat IPv6 statis pada interface
Router(config-if)# ipv6 enable	Mengaktifkan IPv6 pada interface tanpa alamat statis (link-local otomatis)
Router# show ipv6 interface brief	Menampilkan ringkasan status dan alamat IPv6 tiap interface

Konsep Dual-Stack (IPv4 dan IPv6 Berdampingan)

Mengingat migrasi penuh dari IPv4 ke IPv6 membutuhkan waktu yang panjang, sebagian besar jaringan modern saat ini menerapkan pendekatan **dual-stack**, yaitu mengaktifkan IPv4 dan IPv6 secara bersamaan pada perangkat dan interface yang sama. Dengan pendekatan ini, perangkat dapat berkomunikasi menggunakan IPv4 dengan sistem yang belum mendukung IPv6, sekaligus menggunakan IPv6 dengan sistem yang sudah mendukungnya, memberikan masa transisi yang mulus tanpa mengganggu layanan yang sudah berjalan.

Pada perangkat Cisco, konfigurasi dual-stack cukup dilakukan dengan menetapkan alamat IPv4 dan IPv6 sekaligus pada interface yang sama menggunakan perintah `ip address` dan `ipv6 address` secara berurutan, tanpa saling mengganggu satu sama lain.

Aktivitas Pembelajaran

Peserta didik berlatih menyingkat lima alamat IPv6 penuh menjadi bentuk singkatnya, dan sebaliknya menuliskan kembali bentuk penuh dari alamat yang telah disingkat.

Praktik pada Cisco Packet Tracer: mengonfigurasi alamat IPv6 statis pada interface router dan menguji konektivitas menggunakan perintah ping ke alamat IPv6 tujuan.

Diskusi kelompok: mengapa migrasi penuh dari IPv4 ke IPv6 berjalan lambat meskipun IPv6 telah tersedia sejak lama?

Rangkuman

IPv6 dikembangkan untuk mengatasi keterbatasan jumlah alamat IPv4 dengan menggunakan format 128 bit yang ditulis dalam notasi heksadesimal. Pemahaman format penulisan, aturan penyingkatan, jenis alamat (unicast, multicast, anycast), serta konfigurasi dasar pada interface perangkat menjadi bekal penting bagi peserta didik menghadapi jaringan masa depan yang semakin mengadopsi IPv6.

Soal Latihan / Refleksi

Singkat alamat IPv6 berikut sesuai aturan penyingkatan: 2001:0db8:0000:0000:0000:0000:0000:0001.

Jelaskan perbedaan alamat unicast, multicast, dan anycast pada IPv6.

Apa fungsi alamat link-local pada IPv6, dan bagaimana cara alamat tersebut terbentuk secara otomatis?

Tuliskan perintah dasar untuk menetapkan alamat IPv6 2001:db8:a::1/64 pada sebuah interface router Cisco.

BAB 15 — Topologi dan Perangkat dalam Desain Jaringan

Tujuan Pembelajaran

Peserta didik mampu membaca dan menginterpretasikan diagram topologi jaringan fisik maupun logis.

Peserta didik mampu menjelaskan fungsi perangkat jaringan dalam konteks sebuah topologi nyata.

Peserta didik mampu menjelaskan konsep segmentasi jaringan seperti zona internal, DMZ, dan jaringan antar cabang.

Membaca Diagram Topologi Fisik dan Logis

Diagram topologi jaringan merupakan representasi visual yang menggambarkan keterhubungan antar perangkat dalam sebuah jaringan. Diagram topologi fisik menunjukkan lokasi nyata perangkat dan jalur kabel, sedangkan diagram topologi logis menunjukkan aliran data dan pengalamatan IP tanpa memandang lokasi fisik. Kemampuan membaca kedua jenis diagram ini menjadi keterampilan wajib bagi teknisi jaringan, terutama dalam konteks kompetisi seperti LKS yang mengharuskan peserta membangun jaringan sesuai skema topologi yang diberikan pada soal.

Simbol Standar dalam Diagram Topologi

Simbol	Perangkat	Keterangan
Kotak dengan panah melingkar	Router	Menghubungkan jaringan berbeda
Kotak dengan garis horizontal	Switch	Menghubungkan perangkat dalam satu LAN
Layar monitor	PC/Host/Client	Perangkat pengguna akhir
Kotak server dengan garis rak	Server	Menyediakan layanan (web, DNS, DHCP, dll.)
Bentuk perisai/tembok bata	Firewall	Menyaring lalu lintas jaringan untuk keamanan
Awan (cloud)	Internet/WAN	Representasi jaringan luas yang tidak digambarkan detail

Fungsi Perangkat dalam Topologi Jaringan Nyata

Dalam sebuah topologi jaringan nyata, setiap perangkat memiliki peran yang saling melengkapi. **Router** berperan sebagai gerbang (gateway) yang menghubungkan jaringan lokal dengan jaringan luar atau menghubungkan beberapa segmen jaringan internal yang berbeda. **Switch layer 2** mengelola konektivitas dalam satu segmen LAN, sementara **switch layer 3** dapat berperan ganda melakukan routing antar VLAN tanpa memerlukan router terpisah. **Firewall** ditempatkan pada titik masuk jaringan (perimeter) untuk menyaring lalu lintas berdasarkan kebijakan keamanan, dan **server** menyediakan layanan tertentu seperti web, DNS, atau file sharing kepada client dalam jaringan.

Segmentasi Jaringan: Internal, DMZ, dan Branch-Core

Segmentasi jaringan adalah praktik membagi jaringan menjadi beberapa zona dengan tingkat kepercayaan (trust level) berbeda untuk meningkatkan keamanan dan manajemen. **Zona internal** merupakan jaringan privat tempat perangkat dan pengguna organisasi berada, dengan tingkat kepercayaan tertinggi dan akses terbatas dari luar.

Demilitarized Zone (DMZ) adalah segmen jaringan perantara yang ditempatkan di antara jaringan internal dan jaringan luar (internet), digunakan untuk menempatkan server yang perlu diakses dari luar seperti web server atau mail server, sehingga jika server tersebut diretas, penyerang tidak langsung mendapatkan akses ke jaringan internal yang lebih sensitif.

Konsep **branch-core** menggambarkan arsitektur jaringan organisasi dengan banyak lokasi, di mana **core** merupakan jaringan pusat yang menyimpan sumber daya utama (server, database), sedangkan **branch** merupakan jaringan kantor cabang yang terhubung ke core melalui jaringan WAN (Wide Area Network), baik menggunakan koneksi privat (leased line, MPLS) maupun VPN melalui internet publik.

Checklist Praktis Merancang Topologi Jaringan Sederhana

Sebelum membangun sebuah jaringan, baik dalam simulasi Cisco Packet Tracer maupun implementasi nyata, teknisi sebaiknya melalui beberapa langkah perencanaan berikut agar desain yang dihasilkan efisien dan mudah dikelola.

Identifikasi jumlah dan jenis perangkat yang akan terhubung (PC, server, printer, access point).

Tentukan kebutuhan segmentasi (apakah diperlukan VLAN terpisah untuk keamanan atau manajemen).

Rancang skema pengalamatan IP menggunakan subnetting/VLSM sesuai kebutuhan tiap segmen.

Tentukan lokasi penempatan perangkat kritikal seperti firewall dan server publik (apakah memerlukan DMZ).

Gambarkan diagram topologi fisik dan logis sebelum melakukan konfigurasi aktual pada perangkat.

Aktivitas Pembelajaran

Peserta didik diberikan sebuah diagram topologi jaringan sederhana dan diminta mengidentifikasi seluruh perangkat, jenis koneksi, serta menjelaskan fungsi masing-masing perangkat dalam topologi tersebut.

Peserta didik menggambar topologi jaringan sekolah versi sederhana yang mencakup zona internal dan DMZ (misalnya server web sekolah), lengkap dengan penempatan firewall.

Simulasi pada Cisco Packet Tracer: membangun topologi dengan dua segmen jaringan (branch dan core) yang dihubungkan melalui router, kemudian menguji konektivitas antar segmen.

Rangkuman

Kemampuan membaca dan menginterpretasikan topologi jaringan, baik fisik maupun logis, menjadi keterampilan penting bagi teknisi jaringan. Pemahaman fungsi perangkat dalam konteks topologi nyata serta konsep segmentasi jaringan seperti zona internal, DMZ, dan arsitektur branch-core menjadi dasar sebelum mempelajari konfigurasi perangkat secara langsung pada bab berikutnya.

Soal Latihan / Refleksi

Jelaskan perbedaan antara topologi fisik dan topologi logis dalam sebuah diagram jaringan.

Apa fungsi DMZ dalam sebuah arsitektur jaringan, dan mengapa server publik sebaiknya tidak ditempatkan langsung di zona internal?

Jelaskan konsep arsitektur branch-core beserta jenis koneksi yang lazim digunakan untuk menghubungkan keduanya.

Sebutkan tiga simbol standar yang umum digunakan dalam diagram topologi jaringan beserta perangkat yang direpresentasikannya.

BAB 16 — Konfigurasi Dasar Perangkat Jaringan dengan Cisco Packet Tracer

Tujuan Pembelajaran

Peserta didik mampu mengoperasikan Cisco Packet Tracer untuk membangun dan mengonfigurasi topologi jaringan sederhana.

Peserta didik mampu melakukan konfigurasi awal perangkat meliputi hostname, domain-name, password, dan banner login.

Peserta didik mampu menyimpan konfigurasi perangkat agar tidak hilang ketika perangkat dinyalakan ulang.

Mengenal Cisco Packet Tracer

Cisco Packet Tracer adalah perangkat lunak simulasi jaringan yang dikembangkan oleh Cisco Systems untuk keperluan pembelajaran, memungkinkan pengguna merancang, mengonfigurasi, dan menguji topologi jaringan secara virtual tanpa memerlukan perangkat keras fisik. Perangkat lunak ini menjadi media utama pembelajaran dan kompetisi LKS Bidang IT Network System Administration karena mendukung simulasi perangkat Cisco dengan antarmuka command line interface (CLI) yang identik dengan perangkat aslinya.

Mode Command Line Interface

Perangkat Cisco (router dan switch) memiliki beberapa mode akses CLI yang bertingkat, masing-masing dengan cakupan perintah yang berbeda.

Mode	Prompt	Keterangan
User EXEC	Router>	Mode dasar dengan akses terbatas, hanya perintah monitoring dasar
Privileged EXEC	Router#	Akses penuh untuk melihat konfigurasi dan menjalankan perintah debug
Global Configuration	Router(config)#	Mode untuk melakukan perubahan konfigurasi perangkat secara global
Interface Configuration	Router(config-if)#	Mode untuk konfigurasi spesifik pada satu interface
Line Configuration	Router(config-line)#	Mode untuk konfigurasi jalur akses seperti console dan vty

Perpindahan antar mode dilakukan dengan perintah tertentu: dari User EXEC ke Privileged EXEC menggunakan perintah `enable`, dari Privileged EXEC ke Global Configuration menggunakan perintah `configure terminal`, dan untuk kembali ke mode sebelumnya menggunakan perintah `exit`, atau langsung ke Privileged EXEC dari mode manapun menggunakan `end`.

Konfigurasi Hostname dan Domain-name

Hostname digunakan untuk memberikan nama identitas pada perangkat agar mudah dikenali, sedangkan domain-name digunakan sebagai bagian dari proses pembuatan kunci keamanan (misalnya untuk SSH) dan pengelolaan DNS. Kedua konfigurasi ini dilakukan pada mode Global Configuration.

Perintah	Fungsi
Router(config)# hostname R1-CORE	Mengubah nama perangkat menjadi R1-CORE
R1-CORE(config)# ip domain-name tjkt.sch.id	Menetapkan nama domain perangkat

Konfigurasi Password dan User Administratif

Keamanan akses perangkat dimulai dari konfigurasi password pada berbagai jalur akses, meliputi console, vty (untuk akses remote seperti Telnet/SSH), dan mode privileged.

Perintah	Fungsi
Router(config)# enable secret Cisco123	Menetapkan password terenkripsi untuk masuk ke Privileged EXEC
Router(config)# line console 0	Masuk ke mode konfigurasi jalur console
Router(config-line)# password Cisco123	Menetapkan password pada jalur console
Router(config-line)# login	Mengaktifkan permintaan password saat login
Router(config)# username admin secret Admin123	Membuat user administratif dengan password terenkripsi

Penggunaan perintah `enable secret` lebih disarankan dibanding `enable password` karena `enable secret` mengenkripsi password menggunakan algoritma yang lebih kuat, sementara `enable password` menyimpan password dalam bentuk teks biasa pada file konfigurasi kecuali dienkripsi tambahan menggunakan perintah `service password-encryption`.

Konfigurasi Banner Login (MOTD)

Banner Message of the Day (MOTD) adalah pesan yang ditampilkan kepada pengguna sebelum proses autentikasi, umumnya berisi peringatan hukum bahwa akses tanpa izin dilarang. Banner ini dikonfigurasi menggunakan perintah berikut, di mana karakter pembatas (delimiter) seperti tanda pagar (#) menandai awal dan akhir pesan.

Perintah	Fungsi
Router(config)# banner motd # PERINGATAN: Akses tanpa izin dilarang! #	Menampilkan pesan peringatan sebelum login

Menyimpan Konfigurasi Perangkat

Konfigurasi yang telah dibuat tersimpan sementara pada running-config (memori RAM) dan akan hilang jika perangkat dimatikan atau dinyalakan ulang tanpa disimpan. Untuk menyimpan konfigurasi secara permanen ke startup-config (NVRAM), digunakan perintah berikut pada mode Privileged EXEC.

Perintah	Fungsi
Router# copy running-config startup-config	Menyimpan konfigurasi aktif ke memori permanen
Router# show running-config	Menampilkan konfigurasi yang sedang aktif
Router# show startup-config	Menampilkan konfigurasi tersimpan yang akan dimuat saat boot

Perintah Verifikasi Dasar

Selain perintah konfigurasi, teknisi jaringan perlu menguasai perintah verifikasi untuk memastikan konfigurasi berjalan sebagaimana mestinya dan untuk keperluan troubleshooting sehari-hari.

Perintah	Fungsi
Router# show ip interface brief	Menampilkan ringkasan status dan alamat IP setiap interface
Router(config-if)# no shutdown	Mengaktifkan interface yang secara default dalam kondisi mati (administratively down)
Router# show interfaces g0/0	Menampilkan detail status, statistik, dan konfigurasi sebuah interface
Router# show version	Menampilkan informasi versi IOS, model perangkat, dan register konfigurasi
PC> ipconfig /all	Menampilkan konfigurasi IP lengkap pada PC dalam simulasi Packet Tracer
PC> ping 192.168.1.1	Menguji konektivitas ke alamat IP tujuan
PC> tracert 192.168.1.1	Menampilkan jalur (hop) yang dilalui paket menuju alamat tujuan

Interface pada perangkat Cisco secara default berada dalam kondisi administratively down setelah pemasangan awal, sehingga perintah `no shutdown` pada mode Interface Configuration menjadi langkah wajib yang sering terlewat oleh pemula namun krusial agar interface dapat mulai meneruskan lalu lintas data.

Aktivitas Pembelajaran

Peserta didik membangun topologi sederhana pada Cisco Packet Tracer terdiri atas satu router dan satu switch, kemudian mempraktikkan konfigurasi hostname, domain-name, enable secret, password console, dan banner motd secara berurutan.

Peserta didik mempraktikkan penyimpanan konfigurasi menggunakan `copy running-config startup-config`, kemudian menguji dengan mematikan dan menyalakan ulang perangkat untuk memverifikasi konfigurasi tersimpan.

Peserta didik saling menukar file topologi Packet Tracer dengan rekan sekelas untuk saling memeriksa hasil konfigurasi dasar yang telah dibuat.

Rangkuman

Cisco Packet Tracer menjadi media utama praktik konfigurasi perangkat jaringan, dimulai dari pemahaman mode CLI bertingkat (User EXEC, Privileged EXEC, Global Configuration) hingga konfigurasi dasar seperti hostname, domain-name, password, dan banner login. Penyimpanan konfigurasi menggunakan copy running-config startup-config menjadi langkah wajib agar konfigurasi tidak hilang, dan menjadi dasar sebelum mempelajari konfigurasi switching dan routing pada bab selanjutnya.

Soal Latihan / Refleksi

Jelaskan urutan mode CLI pada perangkat Cisco dari User EXEC hingga Interface Configuration beserta prompt masing-masing.

Tuliskan perintah untuk mengubah hostname perangkat menjadi SW1-ACCESS.

Mengapa `enable secret` lebih disarankan dibanding `enable password`?

Jelaskan perbedaan antara running-config dan startup-config, serta perintah untuk menyimpan konfigurasi secara permanen.

BAB 17 — Konsep Switching Dasar

Tujuan Pembelajaran

Peserta didik mampu menjelaskan tujuan pembuatan VLAN untuk segmentasi jaringan.

Peserta didik mampu membedakan access port dan trunk port beserta konsep native VLAN.

Peserta didik mampu menjelaskan tujuan link aggregation (EtherChannel) pada jaringan switch.

Konsep VLAN dan Tujuannya

Virtual Local Area Network (VLAN) adalah teknik segmentasi jaringan yang memungkinkan sebuah switch fisik dibagi menjadi beberapa jaringan logis yang terpisah, meskipun perangkat-perangkat tersebut terhubung secara fisik pada switch yang sama. Setiap VLAN merupakan broadcast domain tersendiri, sehingga lalu lintas broadcast pada satu VLAN tidak akan diteruskan ke VLAN lain kecuali melalui perangkat routing.

Tujuan utama penggunaan VLAN meliputi peningkatan keamanan dengan memisahkan lalu lintas antar departemen atau fungsi (misalnya VLAN untuk staf administrasi terpisah dari VLAN untuk laboratorium siswa), pengurangan ukuran broadcast domain untuk meningkatkan performa jaringan, serta fleksibilitas pengelompokan perangkat berdasarkan fungsi tanpa terikat lokasi fisik.

Access Port dan Trunk Port

Port pada switch dapat dikonfigurasi dalam dua mode utama terkait VLAN. **Access port** hanya membawa lalu lintas untuk satu VLAN tertentu dan digunakan untuk menghubungkan perangkat pengguna akhir seperti PC atau printer ke switch. **Trunk port** dapat membawa lalu lintas dari beberapa VLAN sekaligus melalui satu tautan fisik, dan umumnya digunakan untuk menghubungkan antar switch atau antara switch dengan router, agar VLAN yang sama dapat diperluas ke berbagai bagian jaringan tanpa memerlukan kabel terpisah untuk setiap VLAN.

Trunk port menggunakan mekanisme **VLAN tagging** sesuai standar IEEE 802.1Q untuk menandai setiap frame dengan ID VLAN asalnya, sehingga switch penerima dapat mengetahui frame tersebut milik VLAN mana. **Native VLAN** adalah satu-satunya VLAN pada trunk port yang framenya dikirim tanpa tag 802.1Q; secara default VLAN 1 berperan sebagai native VLAN, meskipun dapat diubah sesuai kebutuhan keamanan jaringan.

Perintah	Fungsi
Switch(config)# vlan 10	Membuat VLAN dengan ID 10
Switch(config-vlan)# name STAF	Memberi nama pada VLAN 10
Switch(config)# interface fa0/1	Masuk ke konfigurasi interface fa0/1
Switch(config-if)# switchport mode access	Menetapkan port sebagai access port
Switch(config-if)# switchport access vlan 10	Menetapkan port fa0/1 sebagai anggota VLAN 10
Switch(config-if)# switchport mode trunk	Menetapkan port sebagai trunk port

VLAN Tagging (Pengantar 802.1Q)

Standar IEEE 802.1Q menambahkan 4 byte tag pada header frame Ethernet yang berisi informasi VLAN ID (mendukung hingga 4094 VLAN), memungkinkan satu trunk port membawa lalu lintas banyak VLAN sekaligus sambil tetap menjaga isolasi antar VLAN. Ketika frame keluar melalui trunk port, switch menambahkan tag sesuai VLAN asalnya; ketika frame diterima oleh switch tujuan, tag tersebut dibaca untuk menentukan VLAN mana yang berhak menerima frame tersebut, lalu tag dilepas kembali sebelum diteruskan ke access port tujuan.

Konsep Link Aggregation (EtherChannel)

Link aggregation, yang pada perangkat Cisco dikenal dengan istilah EtherChannel, adalah teknik menggabungkan beberapa tautan fisik antar switch (atau antara switch dan perangkat lain) menjadi satu tautan logis tunggal. Tujuan utamanya adalah meningkatkan total bandwidth yang tersedia antar perangkat serta menyediakan redundansi — apabila salah satu kabel fisik dalam kelompok tersebut terputus, lalu lintas akan tetap mengalir melalui kabel lain tanpa mengganggu konektivitas secara keseluruhan. Konfigurasi EtherChannel tingkat lanjut menggunakan protokol seperti PAgP atau LACP akan dibahas lebih mendalam pada mata pelajaran Administrasi Infrastruktur Jaringan.

Manfaat VLAN dalam Konteks Keamanan dan Manajemen

Selain manfaat performa, VLAN memberikan manfaat signifikan dalam hal keamanan dan kemudahan manajemen jaringan skala menengah. Sebagai ilustrasi, sebuah sekolah dapat memisahkan VLAN untuk jaringan tata usaha (data administratif sensitif), VLAN untuk laboratorium siswa (akses terbatas), dan VLAN untuk jaringan tamu/Wi-Fi publik, sehingga lalu lintas dari satu segmen tidak dapat diakses langsung oleh segmen lain tanpa melalui kontrol routing dan firewall yang eksplisit.

VLAN ID	Nama VLAN	Peruntukan
10	STAF	Jaringan tata usaha dan administrasi
20	LAB	Jaringan laboratorium komputer siswa
30	GUEST	Jaringan tamu/Wi-Fi publik
99	MGMT	Jaringan manajemen perangkat (switch/router)

Aktivitas Pembelajaran

Peserta didik membangun topologi pada Cisco Packet Tracer dengan satu switch dan empat PC, membuat dua VLAN berbeda, dan menguji bahwa PC pada VLAN berbeda tidak dapat saling terhubung tanpa routing.

Peserta didik mengonfigurasi trunk port antara dua switch yang membawa dua VLAN sekaligus, kemudian memverifikasi menggunakan perintah `show vlan brief` dan `show interfaces trunk`.

Diskusi kelompok: mengapa penggunaan VLAN dianggap meningkatkan keamanan jaringan dibanding menempatkan seluruh perangkat pada satu jaringan datar (flat network)?

Rangkuman

VLAN memungkinkan segmentasi jaringan logis pada satu switch fisik untuk meningkatkan keamanan dan performa, dengan access port membawa satu VLAN dan trunk port membawa banyak VLAN menggunakan tagging 802.1Q. Konsep link aggregation (EtherChannel) menggabungkan beberapa tautan fisik menjadi satu tautan logis untuk meningkatkan bandwidth dan redundansi. Pemahaman ini menjadi dasar sebelum mempelajari konsep routing pada bab berikutnya.

Soal Latihan / Refleksi

Jelaskan tujuan utama penggunaan VLAN dalam sebuah jaringan.

Apa perbedaan antara access port dan trunk port?

Jelaskan fungsi native VLAN pada sebuah trunk port.

Mengapa link aggregation (EtherChannel) dapat meningkatkan keandalan jaringan selain meningkatkan bandwidth?

BAB 18 — Konsep Routing Dasar

Tujuan Pembelajaran

Peserta didik mampu menjelaskan fungsi dan cara kerja routing dalam meneruskan paket antar jaringan.

Peserta didik mampu mengonfigurasi static routing menggunakan exit interface maupun next-hop.

Peserta didik mampu menjelaskan perbedaan routing statis dan routing dinamis secara konseptual.

Fungsi dan Cara Kerja Routing

Routing adalah proses menentukan jalur terbaik yang harus dilalui sebuah paket data untuk mencapai jaringan tujuan yang berbeda dari jaringan asalnya. Router melakukan proses ini dengan memeriksa alamat IP tujuan pada setiap paket yang diterima, kemudian mencocokkannya dengan entri pada tabel routing untuk menentukan interface keluar (exit interface) yang harus digunakan untuk meneruskan paket tersebut.

Tabel Routing

Tabel routing adalah basis data yang disimpan pada setiap router, berisi daftar jaringan tujuan yang diketahui beserta informasi jalur untuk mencapainya. Setiap entri pada tabel routing umumnya memuat informasi jaringan tujuan (network address dan subnet mask), interface keluar, alamat next-hop (router berikutnya), serta sumber informasi rute (langsung terhubung, statis, atau dinamis). Perintah `show ip route` digunakan untuk menampilkan tabel routing pada perangkat Cisco.

Static Routing

Static routing adalah metode routing di mana administrator jaringan secara manual menentukan rute menuju jaringan tujuan tertentu. Static routing cocok digunakan pada jaringan kecil dengan topologi sederhana dan jarang berubah, karena tidak membebani perangkat dengan proses komputasi routing dinamis, namun menjadi tidak praktis pada jaringan besar yang sering berubah karena setiap perubahan topologi memerlukan konfigurasi ulang secara manual pada setiap router.

Konfigurasi static routing dapat dilakukan dengan dua pendekatan: menggunakan **exit interface** (menentukan interface lokal tempat paket akan dikeluarkan) atau menggunakan **next-hop** (menentukan alamat IP router berikutnya yang akan menerima paket).

Perintah	Pendekatan	Keterangan
Router(config)# ip route 192.168.2.0 255.255.255.0 g0/1	Exit interface	Paket menuju 192.168.2.0/24 dikeluarkan melalui interface g0/1
Router(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2	Next-hop	Paket menuju 192.168.2.0/24 diteruskan ke router dengan IP 10.0.0.2

Selain itu dikenal pula konsep **default route** yang berfungsi sebagai jalur cadangan untuk seluruh paket yang tujuannya tidak ditemukan pada tabel routing, dikonfigurasi menggunakan `ip route 0.0.0.0 0.0.0.0 [next-hop/exit-interface]`, umum digunakan pada router yang terhubung ke internet.

Pengantar Routing Dinamis

Routing dinamis adalah metode di mana router secara otomatis saling bertukar informasi routing menggunakan protokol tertentu, sehingga tabel routing dapat diperbarui secara otomatis ketika terjadi perubahan topologi jaringan, tanpa memerlukan intervensi manual dari administrator. Kelebihan ini menjadikan routing dinamis lebih sesuai untuk jaringan berskala besar dan kompleks, meskipun membutuhkan sumber daya komputasi dan konfigurasi awal yang lebih rumit dibanding routing statis.

Beberapa contoh protokol routing dinamis yang umum digunakan pada jaringan enterprise antara lain **EIGRP** (Enhanced Interior Gateway Routing Protocol), protokol milik Cisco yang menggunakan algoritma hybrid, dan **OSPF** (Open Shortest Path First), protokol standar terbuka yang menggunakan algoritma link-state. Konfigurasi mendalam kedua protokol ini, termasuk topik terkait seperti pembentukan neighbor, metric, dan area, akan dipelajari secara khusus pada mata pelajaran Administrasi Infrastruktur Jaringan sebagai kelanjutan dari pengenalan konsep pada bab ini.

Pengantar Administrative Distance

Ketika sebuah router mempelajari lebih dari satu jalur menuju jaringan tujuan yang sama dari sumber berbeda (misalnya static routing dan routing dinamis sekaligus), router perlu menentukan sumber mana yang lebih dipercaya. Nilai ini disebut **administrative distance (AD)**, yaitu nilai kepercayaan yang diberikan pada sebuah sumber informasi routing, di mana semakin kecil nilainya semakin tinggi prioritasnya.

Sumber Rute	Administrative Distance
Directly Connected (jaringan terhubung langsung)	0
Static Route	1
EIGRP	90
OSPF	110
Rute tidak dikenal (unreachable)	255

Sebagai contoh, apabila sebuah router memiliki rute statis dan rute EIGRP menuju jaringan tujuan yang sama, router akan memprioritaskan rute statis karena nilai AD-nya lebih kecil (1) dibanding EIGRP (90), sehingga rute EIGRP hanya akan digunakan sebagai cadangan (floating static route) apabila rute statis tersebut tidak tersedia. Konsep ini menjadi dasar penting yang akan diperdalam ketika mempelajari kombinasi routing statis dan dinamis pada mata pelajaran lanjutan.

Aktivitas Pembelajaran

Peserta didik membangun topologi pada Cisco Packet Tracer dengan dua router dan dua jaringan LAN berbeda, kemudian mengonfigurasi static routing menggunakan pendekatan next-hop agar kedua LAN dapat saling terhubung.

Peserta didik mengulangi aktivitas serupa menggunakan pendekatan exit interface, kemudian membandingkan hasil `show ip route` dari kedua pendekatan tersebut.

Diskusi kelompok: dalam skenario jaringan seperti apa static routing masih menjadi pilihan yang tepat meskipun routing dinamis tersedia?

Rangkuman

Routing memungkinkan paket data diteruskan antar jaringan berbeda berdasarkan tabel routing pada router. Static routing dikonfigurasi secara manual menggunakan exit interface atau next-hop dan cocok untuk jaringan kecil, sementara routing dinamis seperti EIGRP dan OSPF memungkinkan pembaruan otomatis pada jaringan berskala besar. Pemahaman konsep routing dasar ini menjadi fondasi sebelum mempelajari topik routing lanjutan pada mata pelajaran berikutnya.

Soal Latihan / Refleksi

Jelaskan fungsi tabel routing pada sebuah router.

Tuliskan perintah static routing menggunakan pendekatan next-hop untuk mencapai jaringan 172.16.1.0/24 melalui router dengan IP 10.1.1.1.

Jelaskan perbedaan mendasar antara routing statis dan routing dinamis.

Apa fungsi default route, dan kapan sebaiknya digunakan?

BAB 19 — Layanan Jaringan Dasar

Tujuan Pembelajaran

Peserta didik mampu menjelaskan konsep dan cara kerja DNS termasuk forward dan reverse zone.

Peserta didik mampu menjelaskan proses pemberian alamat IP otomatis melalui DHCP.

Peserta didik mampu menjelaskan konsep NAT dan sinkronisasi waktu jaringan melalui NTP.

Domain Name System (DNS)

Domain Name System (DNS) adalah layanan yang menerjemahkan nama domain yang mudah diingat manusia (misalnya www.contoh.sch.id) menjadi alamat IP yang digunakan perangkat untuk saling berkomunikasi. Proses ini dikenal sebagai **forward lookup**. Sebaliknya, **reverse lookup** (atau reverse zone) melakukan proses kebalikannya, yaitu menerjemahkan alamat IP menjadi nama domain, yang sering digunakan untuk keperluan verifikasi keamanan dan pencatatan log jaringan.

DNS bekerja secara hierarkis dan terdistribusi melalui berbagai jenis server: **root server** di puncak hierarki, **TLD server** (Top-Level Domain, seperti .com atau .id) di bawahnya, dan **authoritative name server** yang menyimpan data resmi untuk domain tertentu. DNS menggunakan protokol UDP pada port 53 untuk query standar karena membutuhkan respons cepat, namun dapat menggunakan TCP pada port 53 untuk transfer zona antar server DNS yang membutuhkan keandalan lebih tinggi.

Data pada server DNS disimpan dalam bentuk **resource record** dengan beberapa jenis utama yang perlu dipahami peserta didik.

Jenis Record	Fungsi
A	Memetakan nama domain ke alamat IPv4
AAAA	Memetakan nama domain ke alamat IPv6
CNAME	Alias/nama alternatif yang mengarah ke nama domain lain
MX	Menunjuk server yang menangani email untuk domain tersebut
PTR	Digunakan untuk reverse lookup, memetakan alamat IP ke nama domain
NS	Menunjuk authoritative name server untuk sebuah domain

Dynamic Host Configuration Protocol (DHCP)

DHCP adalah layanan yang secara otomatis memberikan konfigurasi alamat IP (beserta subnet mask, default gateway, dan DNS server) kepada perangkat client tanpa perlu konfigurasi manual, sangat memudahkan pengelolaan jaringan berskala besar dengan banyak perangkat. Proses pemberian alamat IP melalui DHCP dikenal dengan istilah **DORA**.

Tahap	Nama	Deskripsi
1	Discover	Client menyiarkan permintaan mencari server DHCP yang tersedia
2	Offer	Server DHCP menawarkan alamat IP yang tersedia kepada client
3	Request	Client meminta secara resmi alamat IP yang ditawarkan tersebut
4	Acknowledge	Server DHCP mengonfirmasi dan menyelesaikan proses pemberian alamat

DHCP menggunakan protokol UDP dengan port 67 untuk server dan port 68 untuk client. Alamat IP yang diberikan melalui DHCP bersifat sementara (lease), dengan masa berlaku tertentu yang dapat diperpanjang (renew) oleh client sebelum masa berlakunya habis.

Network Address Translation (NAT)

Network Address Translation (NAT) adalah teknik yang menerjemahkan alamat IP privat pada jaringan internal menjadi alamat IP publik agar perangkat dapat mengakses internet, sekaligus menyembunyikan struktur alamat internal dari jaringan luar sebagai lapisan keamanan tambahan. NAT menjadi solusi penting mengingat keterbatasan jumlah alamat IPv4 publik yang tersedia.

Jenis NAT	Deskripsi
Static NAT	Pemetaan satu alamat privat ke satu alamat publik secara tetap
Dynamic NAT	Pemetaan alamat privat ke salah satu alamat publik dari kumpulan (pool) yang tersedia
PAT (Port Address Translation)	Banyak alamat privat berbagi satu alamat publik dengan nomor port berbeda, juga dikenal sebagai NAT Overload

PAT merupakan jenis NAT yang paling umum digunakan pada jaringan rumah maupun kantor kecil, karena memungkinkan banyak perangkat internal berbagi satu alamat IP publik tunggal secara efisien.

Network Time Protocol (NTP)

Network Time Protocol (NTP) adalah protokol yang digunakan untuk menyinkronkan waktu antar perangkat dalam jaringan dengan sumber waktu acuan yang akurat. Sinkronisasi waktu yang konsisten sangat penting dalam operasional jaringan, terutama untuk keperluan pencatatan log (logging) yang akurat guna keperluan troubleshooting dan investigasi keamanan, validitas sertifikat digital yang bergantung pada waktu, serta koordinasi proses terjadwal antar sistem. NTP menggunakan protokol UDP pada port 123.

Aktivitas Pembelajaran

Peserta didik membangun topologi pada Cisco Packet Tracer dengan satu server DHCP dan beberapa PC, kemudian mengonfigurasi server tersebut dan memverifikasi PC menerima alamat IP secara otomatis.

Peserta didik mengonfigurasi server DNS sederhana pada Cisco Packet Tracer untuk menerjemahkan satu nama domain menjadi alamat IP server web pada topologi yang sama.

Diskusi kelompok bergambar: menjelaskan urutan proses DORA pada DHCP menggunakan diagram alur sederhana.

Rangkuman

Layanan jaringan dasar seperti DNS, DHCP, NAT, dan NTP memainkan peran penting dalam operasional jaringan sehari-hari. DNS menerjemahkan nama domain menjadi alamat IP, DHCP mengotomatisasi pemberian alamat IP melalui proses DORA, NAT memungkinkan banyak perangkat privat mengakses internet melalui alamat publik terbatas, dan NTP menjaga sinkronisasi waktu antar perangkat jaringan. Pemahaman layanan-layanan ini menjadi dasar sebelum mempelajari aspek keamanan jaringan pada bab berikutnya.

Soal Latihan / Refleksi

Jelaskan perbedaan antara forward lookup dan reverse lookup pada DNS.

Sebutkan dan jelaskan urutan empat tahap proses DORA pada DHCP.

Jelaskan perbedaan Static NAT, Dynamic NAT, dan PAT (NAT Overload).

Mengapa sinkronisasi waktu melalui NTP penting bagi keamanan dan pencatatan log jaringan?

BAB 20 — Keamanan Jaringan Tingkat Dasar

Tujuan Pembelajaran

Peserta didik mampu menjelaskan kelebihan SSH dibanding Telnet untuk akses remote perangkat.

Peserta didik mampu mengonfigurasi akses SSH dasar pada perangkat jaringan.

Peserta didik mampu menjelaskan dan mengonfigurasi konsep port security pada switch.

SSH vs Telnet

Telnet dan Secure Shell (SSH) adalah dua protokol yang digunakan untuk mengakses perangkat jaringan secara remote melalui command line interface. Telnet, yang beroperasi pada port TCP 23, mengirimkan seluruh data termasuk username dan password dalam bentuk teks polos (plaintext) tanpa enkripsi, sehingga sangat rentan disadap oleh pihak yang tidak berwenang menggunakan teknik packet sniffing.

SSH, yang beroperasi pada port TCP 22, mengenkripsi seluruh data yang dikirimkan antara client dan perangkat, termasuk kredensial login, sehingga jauh lebih aman digunakan untuk akses remote pada jaringan produksi. Oleh karena keunggulan keamanannya, SSH menjadi standar industri untuk akses remote perangkat jaringan, dan penggunaan Telnet pada jaringan produksi modern sangat tidak disarankan.

Aspek	Telnet	SSH
Port	TCP 23	TCP 22
Enkripsi	Tidak ada (plaintext)	Ada (terenkripsi penuh)
Keamanan	Rentan disadap	Aman terhadap penyadapan
Rekomendasi penggunaan	Tidak disarankan	Standar industri

Konfigurasi Akses SSH Dasar

Konfigurasi SSH pada perangkat Cisco memerlukan beberapa langkah persiapan sebelum SSH dapat diaktifkan, meliputi penetapan hostname dan domain-name (sebagaimana telah dipelajari pada Bab 11), pembuatan kunci enkripsi RSA, serta pembuatan akun pengguna.

Perintah	Fungsi
Router(config)# ip domain-name tjkt.sch.id	Prasyarat pembuatan kunci RSA (domain-name harus sudah ditetapkan)
Router(config)# crypto key generate rsa	Membuat pasangan kunci enkripsi RSA (disarankan modulus 1024 bit ke atas)
Router(config)# username admin secret Admin123	Membuat akun pengguna untuk autentikasi SSH
Router(config)# line vty 0 4	Masuk ke konfigurasi jalur vty (akses remote)
Router(config-line)# transport input ssh	Membatasi akses vty hanya melalui SSH (menonaktifkan Telnet)

Perintah	Fungsi
Router(config-line)# login local	Menetapkan autentikasi menggunakan akun lokal yang telah dibuat

Port Security pada Switch

Port security adalah fitur keamanan pada switch yang membatasi jumlah dan/atau jenis alamat MAC yang diperbolehkan terhubung pada sebuah port, bertujuan mencegah akses tidak sah dari perangkat yang tidak dikenal, termasuk mencegah serangan seperti MAC flooding yang dapat membanjiri tabel MAC address switch.

Perintah	Fungsi
Switch(config-if)# switchport mode access	Prasyarat wajib — port security hanya berlaku pada access port
Switch(config-if)# switchport port-security	Mengaktifkan fitur port security pada interface
Switch(config-if)# switchport port-security maximum 2	Membatasi maksimal 2 alamat MAC yang diperbolehkan pada port tersebut
Switch(config-if)# switchport port-security violation shutdown	Menetapkan port akan dinonaktifkan otomatis jika terjadi pelanggaran
Switch(config-if)# switchport port-security mac-address sticky	Mempelajari dan menyimpan alamat MAC secara otomatis ke dalam konfigurasi

Terdapat tiga mode tindakan (violation mode) yang dapat diterapkan ketika pelanggaran port security terdeteksi: **protect** (paket dari MAC tidak sah ditolak tanpa pemberitahuan), **restrict** (paket ditolak dan dicatat sebagai log, disertai penghitung pelanggaran), dan **shutdown** (port dinonaktifkan sepenuhnya dan memerlukan intervensi manual administrator untuk mengaktifkannya kembali) — mode shutdown merupakan mode default dan paling ketat di antara ketiganya.

Prinsip Defense in Depth pada Jaringan

SSH dan port security yang dipelajari pada bab ini merupakan dua contoh penerapan prinsip **defense in depth**, yaitu strategi keamanan yang menerapkan berbagai lapisan pengamanan sekaligus, sehingga apabila satu lapisan berhasil ditembus, lapisan lain tetap dapat mencegah atau memperlambat serangan. Prinsip ini akan terus dikembangkan secara lebih mendalam pada mata pelajaran Keamanan Jaringan, yang mencakup topik seperti firewall tingkat lanjut, deteksi intrusi (IDS/IPS), serta kriptografi terapan.

Aktivitas Pembelajaran

Peserta didik mempraktikkan konfigurasi SSH pada router dalam topologi Cisco Packet Tracer, kemudian menguji akses remote menggunakan PC client melalui aplikasi terminal SSH yang tersedia pada Packet Tracer.

Peserta didik mengonfigurasi port security pada sebuah interface switch dengan maksimal satu alamat MAC dan mode violation shutdown, kemudian menguji pelanggaran dengan

menghubungkan perangkat berbeda pada port yang sama untuk mengamati port menjadi nonaktif (err-disabled).

Diskusi kelompok: mengapa Telnet masih ditemukan digunakan pada beberapa jaringan lama meskipun risikonya sudah diketahui secara luas?

Rangkuman

Keamanan jaringan tingkat dasar mencakup penggunaan SSH sebagai pengganti Telnet untuk akses remote yang aman melalui enkripsi, serta port security pada switch untuk membatasi akses berdasarkan alamat MAC guna mencegah perangkat tidak sah terhubung ke jaringan. Kedua kompetensi ini menjadi bekal dasar sebelum peserta didik mempelajari topik keamanan jaringan yang lebih mendalam pada mata pelajaran Keamanan Jaringan.

Soal Latihan / Refleksi

Jelaskan mengapa SSH dianggap lebih aman dibanding Telnet untuk akses remote perangkat jaringan.

Sebutkan langkah-langkah prasyarat yang harus dipenuhi sebelum SSH dapat diaktifkan pada perangkat Cisco.

Jelaskan tujuan fitur port security pada switch beserta salah satu contoh serangan yang dapat dicegahnya.

Jelaskan perbedaan mode violation restrict dan shutdown pada konfigurasi port security.

BAB 21 — Rangkuman dan Evaluasi Akhir

Bab ini menjadi bahan konsolidasi menyeluruh atas seluruh materi Jaringan Dasar yang telah dipelajari, mencakup Target B (materi prasyarat konsep) pada Bab 2 hingga Bab 7, Target A.0 (praktik perangkat MikroTik RouterOS) pada Bab 8 hingga Bab 12, serta Target A (fondasi wajib dari soal LKS berbasis Cisco Packet Tracer) pada Bab 13 hingga Bab 20. Bab ini dapat digunakan sebagai bahan review menjelang asesmen sumatif maupun persiapan kompetisi keahlian seperti LKS Bidang IT Network System Administration.

12.26 Peta Keterkaitan Antar Bab

Materi dalam buku ini disusun secara berjenjang, di mana penguasaan bab sebelumnya menjadi prasyarat bagi bab berikutnya. Model OSI dan TCP/IP (Bab 2–3) mendasari pemahaman mengenai bagaimana data bergerak dalam jaringan, yang kemudian diterapkan pada pemahaman media transmisi dan topologi (Bab 4–5). Protokol, port, dan perangkat jaringan dasar (Bab 6–7) menjadi jembatan menuju praktik konfigurasi perangkat MikroTik RouterOS (Bab 8–12) sebagai pengenalan platform kedua di luar Cisco Packet Tracer, sebelum peserta didik masuk ke kompetensi praktik pengalamatan IP (Bab 13–14) dan desain topologi nyata (Bab 15).

Kompetensi praktik konfigurasi dimulai pada Bab 16 dengan dasar-dasar CLI Cisco, kemudian diperdalam melalui konsep switching (Bab 17) dan routing (Bab 18) yang menjadi fondasi wajib bagi kompetisi LKS. Layanan jaringan dasar (Bab 19) dan keamanan tingkat dasar (Bab 20) melengkapi kompetensi akhir sebelum peserta didik siap melanjutkan ke mata pelajaran Administrasi Infrastruktur Jaringan maupun Teknologi Jaringan Berbasis Luas yang membahas topik lanjutan seperti VTP, EIGRP, OSPF, dan FHRP/HSRP secara mendalam.

12.27 Rekapitulasi Capaian Target Pembelajaran

Kelompok	Elemen/Topik	Bab Terkait
Target B	Model OSI 7 Layer	Bab 2
Target B	Model TCP/IP	Bab 3
Target B	Media Transmisi & Pengkabelan	Bab 4
Target B	Topologi Fisik Jaringan	Bab 5
Target B	Protokol dan Port Dasar	Bab 6
Target B	Perangkat Jaringan Dasar	Bab 7
Target A.0	Praktik Perangkat MikroTik RouterOS	Bab 8–12
Target A.1	Pengalamatan Jaringan (IPv4/IPv6)	Bab 13–14
Target A.2	Topologi & Perangkat Jaringan	Bab 15
Target A.3	Konfigurasi Dasar Perangkat	Bab 16
Target A.4	Konsep Switching Dasar	Bab 17
Target A.5	Konsep Routing Dasar	Bab 18
Target A.6	Layanan Jaringan Dasar	Bab 19

Target A.7	Keamanan Jaringan Tingkat Dasar	Bab 20

12.28 Arah Pembelajaran Lanjutan

Setelah menuntaskan seluruh materi dalam buku ini, peserta didik diharapkan telah memiliki fondasi yang cukup kuat untuk melanjutkan ke mata pelajaran yang membahas topik jaringan tingkat lanjut. Topik seperti routing dinamis (EIGRP, OSPF), VLAN Trunking Protocol (VTP), First Hop Redundancy Protocol (FHRP/HSRP), EtherChannel tingkat lanjut menggunakan LACP/PAgP, hingga konsep high-availability pada layanan web, akan menjadi fokus pembelajaran pada mata pelajaran Administrasi Infrastruktur Jaringan dan Teknologi Jaringan Berbasis Luas.

Peserta didik yang berminat mengikuti kompetisi keahlian seperti LKS Bidang IT Network System Administration & Cloud Computing disarankan untuk memperdalam praktik konfigurasi menggunakan Cisco Packet Tracer secara mandiri, serta mempelajari dasar-dasar lingkungan Linux (Modul A LKS) sebagai pelengkap kompetensi jaringan berbasis Cisco (Modul B LKS).

Soal Latihan / Refleksi

Jelaskan keterkaitan antara model OSI/TCP-IP dengan kemampuan melakukan troubleshooting jaringan menggunakan pendekatan per-layer.

Sebuah kantor cabang kecil memerlukan desain jaringan sederhana dengan satu router, satu switch, dan sepuluh PC, menggunakan subnet /27. Rancanglah skema pengalamatan IP beserta konfigurasi dasar (hostname, password, VLAN) yang sesuai.

Jelaskan mengapa static routing dianggap tidak praktis untuk jaringan skala besar, dan sebutkan dua protokol routing dinamis yang menjadi materi lanjutan.

Rancang sebuah skenario topologi jaringan sekolah sederhana yang menerapkan konsep VLAN, SSH untuk akses remote, dan port security, lengkap dengan penjelasan alasan setiap keputusan desain yang diambil.

Jelaskan hubungan antara Target A dan Target B dalam struktur pembelajaran buku ini, dan mengapa urutan pembelajaran keduanya penting diperhatikan.

Glosarium

Access Point (AP) — perangkat yang menjembatani perangkat nirkabel dengan jaringan kabel.

Administrative Distance (AD) — nilai kepercayaan sebuah sumber informasi routing; semakin kecil nilainya semakin diprioritaskan.

Bandwidth — kapasitas maksimum data yang dapat dikirimkan melalui sebuah media dalam satuan waktu tertentu.

Broadcast Domain — kumpulan perangkat yang menerima lalu lintas broadcast yang sama.

CIDR (Classless Inter-Domain Routing) — notasi ringkas subnet mask yang menuliskan jumlah bit network, misalnya /24.

Collision Domain — segmen jaringan tempat terjadinya potensi tabrakan (collision) antar sinyal data.

DHCP (Dynamic Host Configuration Protocol) — protokol pemberian alamat IP otomatis kepada client.

DMZ (Demilitarized Zone) — segmen jaringan perantara antara jaringan internal dan jaringan luar untuk menempatkan server publik.

DNS (Domain Name System) — layanan penerjemah nama domain menjadi alamat IP.

Enkapsulasi — proses penambahan header pada data di setiap lapisan model OSI/TCP-IP saat data dikirim.

EtherChannel — teknik link aggregation milik Cisco untuk menggabungkan beberapa tautan fisik menjadi satu tautan logis.

Firewall — perangkat/perangkat lunak yang menyaring lalu lintas jaringan berdasarkan kebijakan keamanan.

Frame — satuan data (PDU) pada layer Data Link.

Host ID — bagian dari alamat IP yang mengidentifikasi perangkat spesifik dalam sebuah jaringan.

IPv4/IPv6 — Internet Protocol versi 4 (32 bit) dan versi 6 (128 bit).

MAC Address — alamat fisik unik 48 bit yang melekat pada kartu jaringan (NIC) suatu perangkat.

NAT (Network Address Translation) — teknik penerjemahan alamat IP privat menjadi alamat IP publik.

Native VLAN — satu-satunya VLAN pada trunk port yang framenya dikirim tanpa tag 802.1Q.

Network ID — bagian dari alamat IP yang mengidentifikasi jaringan tempat sebuah perangkat berada.

NTP (Network Time Protocol) — protokol sinkronisasi waktu antar perangkat jaringan.

OSI (Open Systems Interconnection) — model referensi tujuh lapisan untuk komunikasi jaringan.

Packet — satuan data (PDU) pada layer Network/Internet.

PAT (Port Address Translation) — jenis NAT di mana banyak alamat privat berbagi satu alamat publik melalui perbedaan nomor port.

PDU (Protocol Data Unit) — satuan data pada setiap lapisan model OSI/TCP-IP.

Port Security — fitur switch yang membatasi jumlah/jenis alamat MAC yang diperbolehkan pada sebuah port.

Routing Table — basis data pada router berisi informasi jalur menuju berbagai jaringan tujuan.

SSH (Secure Shell) — protokol akses remote terenkripsi, pengganti Telnet yang lebih aman.

Subnet Mask — rangkaian bit yang menentukan bagian network ID dan host ID pada sebuah alamat IP.

Topologi — pola keterhubungan antar perangkat dalam sebuah jaringan.

Trunk Port — port switch yang dapat membawa lalu lintas beberapa VLAN sekaligus.

VLAN (Virtual Local Area Network) — teknik segmentasi jaringan logis pada satu switch fisik.

VLSM (Variable Length Subnet Mask) — teknik subnetting dengan ukuran subnet berbeda-beda sesuai kebutuhan host tiap segmen.

Lampiran: Ringkasan Perintah CLI Cisco

Lampiran ini merangkum perintah-perintah dasar Cisco IOS yang telah dipelajari sepanjang buku ini, disusun sebagai referensi cepat bagi peserta didik saat praktik maupun menghadapi kompetisi keahlian.

Kategori	Perintah	Fungsi Singkat
Mode Dasar	enable	Masuk ke Privileged EXEC
Mode Dasar	configure terminal	Masuk ke Global Configuration
Mode Dasar	end	Kembali ke Privileged EXEC dari mode manapun
Identitas	hostname [nama]	Mengubah nama perangkat
Identitas	ip domain-name [domain]	Menetapkan nama domain perangkat
Keamanan	enable secret [password]	Password terenkripsi mode privileged
Keamanan	username [nama] secret [password]	Membuat akun pengguna lokal
Keamanan	crypto key generate rsa	Membuat kunci RSA untuk SSH
Keamanan	transport input ssh	Membatasi akses vty hanya melalui SSH
Keamanan	switchport port-security	Mengaktifkan port security pada interface
Antarmuka	interface [nama]	Masuk ke konfigurasi sebuah interface
Antarmuka	ip address [ip] [mask]	Menetapkan alamat IPv4 pada interface
Antarmuka	ipv6 address [alamat]/[prefix]	Menetapkan alamat IPv6 pada interface
Antarmuka	no shutdown	Mengaktifkan interface
VLAN	vlan [id]	Membuat VLAN baru
VLAN	switchport mode access / trunk	Menetapkan mode port
VLAN	switchport access vlan [id]	Menetapkan VLAN pada access port
Routing	ip route [network] [mask] [next-hop/exit-if]	Menambahkan static route
Penyimpanan	copy running-config startup-config	Menyimpan konfigurasi permanen
Verifikasi	show ip interface brief	Ringkasan status & IP tiap interface
Verifikasi	show ip route	Menampilkan tabel routing
Verifikasi	show vlan brief	Menampilkan daftar VLAN
Verifikasi	show running-config	Menampilkan konfigurasi aktif

Lampiran: Latihan Komprehensif Persiapan LKS

Lampiran ini memuat kumpulan soal komprehensif yang menggabungkan beberapa Target A dan Target B sekaligus, sebagai simulasi format soal yang lazim ditemui pada Lomba Kompetensi Siswa (LKS) Bidang IT Network System Administration Modul B.

Studi Kasus 1: Desain Jaringan Kantor Cabang Kecil

Sebuah kantor cabang memiliki satu router, satu switch, dan 25 PC yang perlu dibagi ke dalam dua VLAN: VLAN 10 (Staf, 15 PC) dan VLAN 20 (Tamu, 10 PC). Kantor pusat berada pada jaringan 10.0.0.0/24 dan terhubung melalui link WAN point-to-point. Tugas: (a) tentukan alokasi subnet untuk VLAN 10 dan VLAN 20 menggunakan VLSM dari blok 192.168.100.0/24, (b) tuliskan konfigurasi dasar hostname, VLAN, dan access port untuk switch, (c) tuliskan konfigurasi static route dari router cabang menuju jaringan kantor pusat.

Studi Kasus 2: Verifikasi dan Troubleshooting

Sebuah PC pada VLAN 20 tidak dapat melakukan ping ke default gateway-nya. Tugas: susun urutan langkah troubleshooting berlapis (mengacu pada model OSI) yang harus dilakukan, mulai dari pemeriksaan fisik hingga pemeriksaan konfigurasi logis, beserta perintah verifikasi Cisco IOS yang relevan pada setiap langkah.

Studi Kasus 3: Pengamanan Akses Perangkat

Sebuah router baru perlu dikonfigurasi agar hanya dapat diakses secara remote melalui SSH (bukan Telnet), dengan akun administratif bernama 'teknisi' dan password terenkripsi. Tugas: tuliskan seluruh perintah konfigurasi yang diperlukan secara berurutan, mulai dari penetapan hostname dan domain-name hingga pengujian akses SSH berhasil.

Daftar Pustaka

Cisco Networking Academy. Introduction to Networks Companion Guide. Cisco Press.

International Organization for Standardization. ISO/IEC 7498-1: Open Systems Interconnection — Basic Reference Model.

Naskah Soal Lomba Kompetensi Siswa (LKS) SMK Tingkat Kabupaten Tasikmalaya Tahun 2026, Bidang IT Network System Administration, Modul A: Linux Environment dan Modul B: Cisco Packet Tracer.

Purbo, Onno W. (2026). Buku Pegangan Teknik Jaringan Menggunakan MikroTik.

Kemdikbudristek. Capaian Pembelajaran Mata Pelajaran Jaringan Dasar, Kurikulum Merdeka SMK Program Keahlian TJKT.

MATERI TAMBAHAN: PRAKTIK MIKROTIK ROUTEROS

Lima bab berikut merupakan materi tambahan yang melengkapi kompetensi praktik jaringan pada buku ini, dengan fokus pada perangkat dan platform MikroTik RouterOS yang banyak digunakan pada dunia kerja Teknik Jaringan Komputer dan Telekomunikasi (TJKT).

BAB 22 — Pengantar MikroTik & RouterOS

Mengenal ekosistem MikroTik, RouterOS, dan RouterBOARD sebagai fondasi sebelum masuk ke konfigurasi teknis.

Tujuan Pembelajaran

1. Peserta didik memahami apa itu MikroTik, RouterOS, dan RouterBOARD.
2. Peserta didik mampu membedakan lini produk RouterBOARD dan jenjang lisensi RouterOS.
3. Peserta didik memahami jalur sertifikasi resmi MikroTik dan kedudukannya di dunia kerja.

Apa itu MikroTik?

MikroTik adalah perusahaan asal Latvia yang memproduksi perangkat keras jaringan (router, switch, access point) dan mengembangkan sistem operasi jaringan bernama RouterOS. MikroTik dikenal luas di kalangan ISP kecil-menengah, WISP (Wireless ISP), sekolah, dan perusahaan karena menawarkan fitur jaringan kelas enterprise dengan harga perangkat yang jauh lebih terjangkau dibanding vendor besar seperti Cisco atau Juniper.

Terdapat dua produk inti MikroTik yang perlu dipahami sejak awal. RouterOS adalah sistem operasi (mirip Linux) yang menjalankan fungsi routing, firewall, bridging, wireless, VPN, QoS, dan berbagai layanan jaringan lainnya. RouterBOARD (RB) adalah perangkat keras buatan MikroTik yang sudah terpasang RouterOS di dalamnya, siap pakai layaknya router pada umumnya.

Perlu diketahui

RouterOS tidak selalu terikat pada RouterBOARD. RouterOS juga dapat diinstal di PC/server biasa (x86) maupun dijalankan sebagai virtual machine melalui image Cloud Hosted Router (CHR).

Lini Produk RouterBOARD

RouterBOARD hadir dalam berbagai bentuk sesuai kebutuhan penggunaan, mulai dari perangkat wireless outdoor untuk koneksi jarak jauh hingga router performa tinggi untuk jaringan skala besar.

Kategori	Contoh Seri	Kegunaan Utama
Wireless Outdoor	SXT, LHG, Groove	Point-to-Point / Point-to-Multipoint jarak jauh
Wireless Indoor	hAP, cAP	Access point rumah/kantor
Router Indoor	RB750, RB951, RB4011	Router kantor/rumah dengan port Ethernet
Cloud Core Router (CCR)	CCR1036, CCR2004	Router performa tinggi berbasis multi-core CPU
Cloud Router Switch (CRS)	CRS326, CRS328	Switch layer 2/3 dengan kemampuan RouterOS penuh
Embedded RB	RB912, RB912UAG	Board tertanam untuk perangkat custom/outdoor

Level Lisensi RouterOS

RouterOS menggunakan sistem lisensi berjenjang (level) yang membatasi fitur dan jumlah pengguna simultan yang dapat memakai fitur tertentu, misalnya jumlah user Hotspot atau PPPoE. Pada RouterBOARD, lisensi biasanya sudah tertanam (built-in) sesuai model perangkat.

Level	Karakteristik Utama
Level 0 (Trial)	Gratis, berlaku 24 jam, untuk uji coba instalasi baru
Level 1 (Demo)	Terbatas, biasanya untuk perangkat SOHO ringan (hanya WiFi client tanpa AP)
Level 3	Umum ditemukan di RouterBOARD kelas SOHO, mendukung fitur routing dasar
Level 4	Lisensi standar untuk sebagian besar RouterBOARD wireless

Level 5	Menambah kapasitas jumlah user Hotspot/PPPoE dibanding Level 4
Level 6	Lisensi penuh tanpa batasan, umum dipakai di CCR dan CHR produksi

Jalur Sertifikasi MikroTik

MikroTik menyediakan jalur sertifikasi resmi berjenjang. MTCNA (MikroTik Certified Network Associate) adalah sertifikasi level dasar dan menjadi syarat wajib sebelum mengambil sertifikasi tingkat lanjut apa pun, seperti MTCRE (Routing Engineer), MTCWE (Wireless Engineer), MTCTCE (Traffic Control Engineer), MTCUME (User Management Engine), hingga MTCINE (Internetworking Engineer) sebagai jenjang tertinggi.

Format Ujian MTCNA

Ujian sertifikasi dilakukan secara daring di situs resmi MikroTik, terdiri dari 25 soal pilihan ganda dalam waktu 60 menit, dengan nilai minimum kelulusan umumnya 60%.

Banyak WISP dan penyedia jaringan skala kecil-menengah di Indonesia mensyaratkan MTCNA sebagai standar minimum bagi teknisi lapangan, karena sertifikasi ini membuktikan kompetensi dasar yang terukur dan diakui secara internasional. Banyak pula NOC (Network Operations Center) perusahaan menggunakan RouterOS sebagai edge router karena rasio harga terhadap fitur yang kompetitif, sehingga kompetensi MikroTik menjadi nilai tambah tersendiri bagi lulusan TJKT saat memasuki dunia kerja.

Aktivitas Pembelajaran

4. Peserta didik mencari dan membandingkan spesifikasi tiga seri RouterBOARD berbeda (misalnya hAP lite, RB750, dan CCR1009) melalui situs resmi MikroTik, lalu mendiskusikan kegunaan masing-masing.
5. Peserta didik membuat peta jalur sertifikasi MikroTik dalam bentuk diagram sederhana, mulai dari MTCNA hingga MTCINE.
6. Diskusi kelompok: mengapa banyak WISP di Indonesia lebih memilih perangkat MikroTik dibanding vendor enterprise seperti Cisco untuk jaringan skala kecil-menengah?

Rangkuman

MikroTik adalah vendor perangkat jaringan yang mengembangkan sistem operasi RouterOS dan perangkat keras RouterBOARD. RouterBOARD hadir dalam berbagai lini sesuai kebutuhan, sementara RouterOS menggunakan sistem lisensi berjenjang dari Level 0 hingga Level 6. MTCNA menjadi sertifikasi dasar wajib sebagai gerbang menuju jenjang sertifikasi MikroTik lanjutan, dan menjadi bekal penting sebelum mempelajari instalasi dan konfigurasi RouterOS pada bab berikutnya.

Soal Latihan / Refleksi

7. Jelaskan perbedaan mendasar antara RouterOS dan RouterBOARD.
8. Sebutkan minimal tiga lini produk RouterBOARD beserta kegunaannya masing-masing.
9. Mengapa MTCNA menjadi syarat wajib sebelum mengambil sertifikasi MikroTik lainnya?
10. Jelaskan perbedaan antara lisensi Level 4 dan Level 6 pada RouterOS.

BAB 23 — Instalasi dan Akses Perangkat MikroTik

Mempelajari metode instalasi RouterOS dan cara mengakses router untuk pertama kali menggunakan Winbox, WebFig, maupun CLI.

Tujuan Pembelajaran

11. Peserta didik mampu menjelaskan berbagai metode instalasi/reinstalasi RouterOS.
12. Peserta didik mampu mengakses router melalui Winbox, WebFig, SSH, dan Telnet.
13. Peserta didik memahami dasar navigasi CLI RouterOS serta proses upgrade/downgrade yang aman.

Metode Instalasi RouterOS

RouterOS dapat dipasang melalui beberapa jalur tergantung jenis perangkat yang digunakan. Pada RouterBOARD bawaan, RouterOS sudah terpasang dari pabrik dan tinggal dikonfigurasi. Netinstall adalah alat instalasi ulang RouterOS dari nol melalui jaringan Ethernet, umum dipakai saat perangkat gagal boot atau ingin mengganti versi secara bersih. CHR (Cloud Hosted Router) adalah image RouterOS untuk dijalankan sebagai virtual machine, sementara instalasi di PC/x86 memungkinkan RouterOS dipasang langsung pada perangkat PC atau server biasa dari media instalasi.

Proses Netinstall

Netinstall adalah tool berbasis Windows yang memungkinkan instalasi ulang RouterOS ke RouterBOARD melalui jaringan, tanpa perlu kartu memori tambahan. Langkah umum penggunaannya meliputi: mengunduh paket Netinstall dan file RouterOS (.npk) sesuai arsitektur perangkat dari situs resmi MikroTik; menghubungkan PC dan RouterBOARD dalam satu jaringan Ethernet lalu menyesuaikan IP address Netinstall; menyalakan ulang RouterBOARD sambil menahan tombol reset agar masuk ke mode Netinstall/Etherboot; memilih perangkat yang terdeteksi dan paket RouterOS yang ingin dipasang; dan menunggu proses selesai hingga router reboot otomatis dalam kondisi default.

Kapan Netinstall dibutuhkan?

Netinstall paling sering dipakai ketika router lupa password total tanpa akses backup, RouterOS mengalami corrupt, atau ingin melakukan downgrade ke versi RouterOS yang jauh lebih lama secara bersih.

Mengakses Router: Winbox, WebFig, SSH, Telnet

Metode	Karakteristik
Winbox	Aplikasi desktop berbasis GUI, paling umum dipakai, terhubung via IP atau MAC address
WebFig	Antarmuka konfigurasi berbasis browser web, cocok untuk akses cepat tanpa instal aplikasi
SSH	Akses command line terenkripsi, aman untuk manajemen jarak jauh
Telnet	Akses command line tanpa enkripsi, tidak disarankan untuk jaringan publik
MAC-Winbox	Koneksi ke router menggunakan MAC address, berguna saat router belum punya IP address

Winbox mendukung dua metode koneksi: melalui IP address, jika router sudah memiliki alamat IP dan dapat dijangkau, atau melalui MAC address, yang memanfaatkan broadcast Layer 2 dan berguna saat konfigurasi awal sebelum IP diset.

Dasar Command Line Interface (CLI)

RouterOS memiliki struktur perintah CLI berbasis menu bertingkat, mirip struktur direktori. Tombol Tab digunakan untuk melengkapi otomatis nama menu atau parameter, tanda tanya (?) menampilkan daftar perintah yang tersedia pada level menu saat itu, tanda garis miring (/) mengembalikan ke menu root, dan tanda titik dua kali (..) mengembalikan satu level ke menu sebelumnya. Command history dapat diakses dengan tombol panah atas/bawah untuk mengulang perintah sebelumnya.

```
/ip address print
/interface print
```

```
/system identity set name=Router-Sekolah
/ip service print
```

Upgrade dan Downgrade RouterOS

RouterOS memiliki dua jenis paket, yaitu paket utama (routeros) dan paket tambahan seperti wireless, ipv6, atau dude yang dapat dipasang terpisah sesuai kebutuhan. Cara termudah melakukan upgrade adalah melalui menu System > Packages > Check for Updates pada Winbox. Cara manual dilakukan dengan mengunduh file paket .npk sesuai arsitektur perangkat, mengunggahnya ke router melalui menu Files, lalu me-reboot router untuk memicu instalasi otomatis. Downgrade dilakukan dengan cara serupa menggunakan file paket versi lebih lama.

Perhatian

Selalu lakukan backup konfigurasi sebelum melakukan upgrade/downgrade RouterOS, terutama pada perangkat produksi, untuk menghindari kehilangan konfigurasi akibat kegagalan proses update.

RouterBOOT Firmware Upgrade

Selain paket RouterOS itu sendiri, setiap RouterBOARD memiliki firmware tingkat rendah bernama RouterBOOT, setara BIOS/UEFI pada PC, yang bertanggung jawab pada proses boot awal perangkat sebelum RouterOS dimuat. RouterBOOT dan RouterOS adalah dua komponen terpisah yang di-upgrade secara independen.

```
/system routerboard print
/system routerboard upgrade
/system reboot
```

Perbedaan penting

Meng-upgrade paket RouterOS tidak secara otomatis meng-upgrade RouterBOOT. Banyak kasus router berjalan tidak stabil setelah update besar RouterOS disebabkan oleh RouterBOOT yang tertinggal jauh dari versi RouterOS yang berjalan di atasnya, sehingga upgrade RouterBOOT harus dilakukan sebagai langkah terpisah.

Aktivitas Pembelajaran

14. Peserta didik menghubungkan laptop ke router MikroTik menggunakan kabel LAN, membuka Winbox, dan login menggunakan koneksi MAC address ke perangkat dalam kondisi default pabrik.
15. Peserta didik mengganti nama identitas router melalui menu System > Identity, kemudian memeriksa versi RouterOS dan RouterBOOT yang terpasang melalui menu System > Packages dan System > RouterBOARD.
16. Peserta didik membuka New Terminal dan menjalankan perintah “/system resource print” untuk mengamati informasi CPU, memori, serta versi RouterOS yang aktif.

Rangkuman

RouterOS dapat diinstal melalui berbagai metode sesuai jenis perangkat, dengan Netinstall sebagai solusi utama untuk reinstalasi bersih melalui jaringan. Router dapat diakses melalui Winbox, WebFig, SSH, atau Telnet, dengan SSH menjadi pilihan paling aman untuk manajemen jarak jauh. Proses upgrade RouterOS dan RouterBOOT bersifat terpisah dan keduanya perlu dilakukan secara disiplin agar perangkat tetap stabil, menjadi dasar sebelum mempelajari konfigurasi jaringan pada bab berikutnya.

Soal Latihan / Refleksi

17. Sebutkan tiga metode instalasi RouterOS beserta situasi yang tepat untuk masing-masing metode.
18. Kapan sebaiknya Netinstall digunakan dibanding proses upgrade biasa?
19. Jelaskan perbedaan koneksi Winbox melalui IP address dan melalui MAC address.
20. Mengapa Telnet dianggap kurang aman dibanding SSH untuk manajemen jarak jauh?
21. Jelaskan perbedaan antara upgrade paket RouterOS dan upgrade RouterBOOT, dan mengapa keduanya perlu dilakukan terpisah.

BAB 24 — Konfigurasi Dasar Jaringan MikroTik

Membangun konfigurasi jaringan dasar: pengalamatan IP, default gateway, DNS, hingga koneksi internet pertama melalui NAT masquerade.

Tujuan Pembelajaran

22. Peserta didik mampu mengonfigurasi IP address pada interface RouterOS.
23. Peserta didik mampu mengonfigurasi default gateway dan DNS pada router.
24. Peserta didik mampu menghubungkan jaringan lokal ke internet menggunakan NAT masquerade serta melakukan troubleshooting dasar.

Topologi Dasar Jaringan MikroTik

Skenario paling umum dalam praktik konfigurasi MikroTik adalah router yang memiliki dua sisi jaringan: sisi WAN yang terhubung ke internet/ISP, dan sisi LAN yang terhubung ke jaringan lokal atau klien. Konsep dasar yang wajib dipahami sebelum mengonfigurasi adalah membedakan interface mana yang berfungsi sebagai WAN dan mana yang berfungsi sebagai LAN, sebagaimana telah diperkenalkan pada pembahasan router dan topologi jaringan di bab-bab sebelumnya.

Konfigurasi IP Address

IP address di RouterOS diikatkan pada sebuah interface, misalnya ether1, ether2, atau wlan1. Format penulisan menggunakan notasi CIDR (Classless Inter-Domain Routing), sebagaimana telah dipelajari pada konsep subnetting, misalnya 192.168.1.1/24.

```
/ip address add address=192.168.1.1/24 interface=ether2
/ip address print
```

Prefix (CIDR)	Subnet Mask	Jumlah Host Usable
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14
/30	255.255.255.252	2 (umum untuk link point-to-point)

Default Gateway & DNS

Default gateway adalah rute yang digunakan router saat tidak ada rute spesifik lain yang cocok dengan tujuan paket, biasanya mengarah ke perangkat ISP. DNS diperlukan agar router, dan klien di baliknya jika DNS diaktifkan sebagai cache, dapat menerjemahkan nama domain menjadi IP address.

```
/ip route add dst-address=0.0.0.0/0 gateway=192.168.1.254
/ip dns set servers=8.8.8.8,1.1.1.1 allow-remote-requests=yes
```

allow-remote-requests

Parameter ini membuat router berfungsi sebagai DNS cache/relay untuk klien di jaringan lokal, sehingga klien cukup mengarahkan DNS mereka ke IP router, bukan langsung ke DNS publik.

Koneksi WAN via DHCP Client

Jika ISP menyediakan IP secara dinamis, sebagaimana umum ditemui pada koneksi rumahan, interface WAN router cukup diset sebagai DHCP client agar otomatis menerima IP address, gateway, dan DNS dari ISP.

```
/ip dhcp-client add interface=ether1 disabled=no
/ip dhcp-client print
```

NAT Masquerade — Menghubungkan LAN ke Internet

Karena IP address di jaringan lokal umumnya bersifat privat dan tidak dapat dirutekan langsung di internet, diperlukan NAT (Network Address Translation) tipe masquerade agar seluruh trafik dari LAN keluar menggunakan IP publik router saat menuju internet.

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

Rule ini berarti setiap paket yang keluar melalui interface ether1 (WAN) akan diubah source IP-nya menjadi IP

address ether1 itu sendiri, sehingga balasan dari internet dapat kembali dengan benar ke router dan diteruskan ke klien yang bersangkutan.

Troubleshooting Konektivitas Dasar

Perintah ping digunakan untuk menguji konektivitas dasar ke gateway, DNS, atau internet, sedangkan perintah "/tool traceroute" digunakan untuk melihat jalur yang dilalui paket menuju tujuan. Perintah "/ip route print" memastikan default route sudah ada dan berstatus aktif, sementara "/ip firewall nat print" memastikan rule masquerade sudah terpasang dengan urutan yang benar.

Metodologi troubleshooting yang disiplin sangat penting di dunia kerja: dimulai dari lapisan terendah (fisik/link, apakah lampu interface menyala dan kabel tersambung), lanjut ke lapisan IP (apakah IP address dan gateway benar), lalu ke lapisan aplikasi (apakah DNS resolve, apakah port yang dituju terbuka). Pendekatan bottom-up seperti ini sejalan dengan pendekatan troubleshooting berlapis yang telah dipelajari pada Bab 2 tentang model OSI.

Aktivitas Pembelajaran

25. Peserta didik mengatur ether1 sebagai interface WAN dengan DHCP client aktif, dan ether2 sebagai interface LAN dengan IP statis 192.168.10.1/24.
26. Peserta didik menambahkan rule NAT masquerade untuk interface WAN, menghubungkan laptop ke ether2, dan menguji ping berjenjang dari gateway, ke DNS publik (8.8.8.8), hingga ke nama domain (google.com).
27. Jika ping ke domain gagal namun ping ke 8.8.8.8 berhasil, peserta didik memeriksa kembali konfigurasi DNS pada router sebagai latihan troubleshooting.

Rangkuman

Konfigurasi dasar router MikroTik meliputi pemasangan IP address pada interface, penetapan default gateway dan DNS, serta penggunaan NAT masquerade agar jaringan lokal dapat mengakses internet. Pendekatan troubleshooting berlapis, dimulai dari lapisan fisik hingga aplikasi, menjadi keterampilan wajib untuk mengisolasi gangguan jaringan secara sistematis, dan menjadi dasar sebelum mempelajari konfigurasi DHCP server pada bab berikutnya.

Soal Latihan / Refleksi

28. Jelaskan fungsi default gateway pada tabel routing.
29. Mengapa diperlukan NAT masquerade agar jaringan lokal dapat mengakses internet?
30. Apa perbedaan antara mengatur IP WAN secara statis dan menggunakan DHCP client?
31. Sebutkan langkah troubleshooting jika klien tidak bisa browsing meski ping ke IP publik berhasil.

BAB 25 — Layanan DHCP dan ARP pada MikroTik

Memahami cara kerja DHCP pada RouterOS, baik sebagai client yang menerima IP dari jaringan atas, maupun sebagai server yang membagikan IP ke klien di bawahnya.

Tujuan Pembelajaran

32. Peserta didik mampu mengonfigurasi DHCP server lengkap dengan pool, network, dan lease.
33. Peserta didik mampu membedakan dynamic lease dan static lease serta manfaat keamanannya.
34. Peserta didik memahami mekanisme ARP yang mendukung proses DHCP dalam jaringan Layer 2.

Konsep DHCP

DHCP (Dynamic Host Configuration Protocol) adalah protokol yang memungkinkan perangkat klien memperoleh konfigurasi IP address, subnet mask, gateway, dan DNS secara otomatis dari sebuah server, tanpa perlu dikonfigurasi manual satu per satu — konsep yang sama seperti telah dipelajari pada pembahasan layanan jaringan dasar.

RouterOS dapat berperan sebagai dua sisi sekaligus dalam jaringan berbeda: sebagai DHCP client di sisi WAN untuk menerima IP dari ISP, dan sebagai DHCP server di sisi LAN untuk membagikan IP ke perangkat klien.

Konfigurasi DHCP Server

RouterOS menyediakan wizard “DHCP Setup” yang mempercepat proses konfigurasi, namun pemahaman komponen manualnya tetap penting bagi teknisi jaringan.

Komponen	Fungsi
DHCP Server	Objek utama yang mengaktifkan layanan DHCP pada sebuah interface
IP Pool	Rentang IP address yang akan dibagikan ke klien
DHCP Network	Mendefinisikan gateway, DNS, dan parameter jaringan untuk subnet tertentu
Lease	Catatan IP yang sedang/pernah dipinjamkan ke klien tertentu berdasarkan MAC address

```
/ip pool add name=pool-lan ranges=192.168.10.10-192.168.10.200
/ip dhcp-server add name=dhcp-lan interface=ether2 address-pool=pool-lan disabled=no
/ip dhcp-server network add address=192.168.10.0/24 gateway=192.168.10.1 dns-
server=8.8.8.8
```

DHCP Lease dan Static Lease

Setiap kali klien menerima IP dari DHCP server, informasi tersebut tercatat di menu Leases, yang berguna untuk memantau perangkat mana saja yang aktif di jaringan. Untuk perangkat yang memerlukan IP tetap, misalnya printer, server, atau access point, administrator dapat membuat static lease yang mengikat MAC address tertentu agar selalu mendapat IP address yang sama.

```
/ip dhcp-server lease add address=192.168.10.50 mac-address=AA:BB:CC:DD:EE:FF server=dhcp-
lan
```

Tips Keamanan DHCP

Fitur “DHCP Static Only” dapat mengunci server sehingga hanya perangkat dengan static lease terdaftar yang bisa mendapat IP, sementara perangkat asing otomatis ditolak — salah satu bentuk keamanan dasar pada jaringan yang membutuhkan kontrol ketat terhadap perangkat yang terhubung.

Address Resolution Protocol (ARP)

ARP adalah protokol yang menerjemahkan IP address menjadi MAC address dalam jaringan Layer 2, sehingga paket data dapat dikirim ke perangkat yang tepat pada level fisik. RouterOS mendukung beberapa mode ARP pada interface.

Mode ARP	Perilaku
enabled	Mode default, ARP bekerja normal (otomatis belajar dan merespons)

disabled	ARP dimatikan sepenuhnya pada interface tersebut, komunikasi memerlukan entry ARP statis
proxy-arp	Router menjawab ARP request atas nama perangkat lain di jaringan berbeda
reply-only	Router hanya menjawab ARP request untuk entry yang sudah didaftarkan secara statis, kombinasi keamanan populer dengan static lease DHCP

Aktivitas Pembelajaran

35. Peserta didik membuat IP Pool dengan rentang 192.168.20.10 sampai 192.168.20.100, kemudian membuat DHCP Server pada interface ether3 menggunakan pool tersebut beserta DHCP Network-nya.
36. Peserta didik menghubungkan laptop ke ether3, memverifikasi laptop menerima IP otomatis, lalu mencatat MAC address yang muncul pada menu DHCP Server > Leases.
37. Peserta didik membuat static lease untuk MAC address laptop tersebut agar selalu mendapat IP 192.168.20.50, kemudian memutus dan menyambungkan kembali koneksi untuk memverifikasi hasilnya.

Rangkuman

DHCP pada RouterOS memungkinkan perangkat berperan sebagai client maupun server sekaligus dalam jaringan yang berbeda. Konfigurasi DHCP server terdiri atas komponen pool, network, dan lease, dengan static lease menjadi solusi bagi perangkat yang membutuhkan IP tetap. Pemahaman ARP melengkapi konsep ini sebagai mekanisme dasar penerjemahan IP ke MAC address, dan menjadi dasar sebelum mempelajari konsep bridging dan switching pada bab berikutnya.

Soal Latihan / Refleksi

38. Jelaskan tiga komponen utama yang membentuk sebuah DHCP server pada RouterOS.
39. Apa perbedaan antara dynamic lease dan static lease?
40. Bagaimana fitur “DHCP Static Only” dapat meningkatkan keamanan jaringan?
41. Jelaskan fungsi mode ARP “reply-only” dan kapan sebaiknya digunakan.

BAB 26 — Bridging pada MikroTik

Memahami konsep penggabungan beberapa interface menjadi satu segmen jaringan Layer 2 menggunakan bridge, serta pengenalan Spanning Tree Protocol.

Tujuan Pembelajaran

42. Peserta didik mampu menjelaskan konsep bridging dan perbedaannya dengan routing.
43. Peserta didik mampu membuat dan mengonfigurasi bridge pada RouterOS.
44. Peserta didik memahami dasar STP/RSTP untuk mencegah loop jaringan.

Konsep Bridging

Bridge adalah fitur yang menggabungkan dua atau lebih interface fisik, baik Ethernet maupun wireless, menjadi satu segmen jaringan Layer 2 yang sama, seolah-olah seluruh perangkat yang terhubung berada dalam satu switch. Ini berbeda dengan routing, yang bekerja di Layer 3 dan memisahkan jaringan menjadi subnet-subnet berbeda, sebagaimana telah dibedakan pada pembahasan perangkat jaringan dasar.

Kapan menggunakan Bridge?

Bridge umum digunakan saat ingin menggabungkan beberapa port Ethernet menjadi satu jaringan LAN yang sama, menghubungkan segmen wireless dan wired dalam satu broadcast domain, atau membuat access point transparan tanpa perlu routing/NAT tambahan.

Membuat Bridge

```
/interface bridge add name=bridge-lan
/interface bridge port add bridge=bridge-lan interface=ether2
/interface bridge port add bridge=bridge-lan interface=ether3
/ip address add address=192.168.10.1/24 interface=bridge-lan
```

Setelah interface digabungkan ke dalam bridge, IP address sebaiknya dipasang pada interface bridge itu sendiri, bukan pada masing-masing port fisik, karena bridge kini merepresentasikan keseluruhan segmen jaringan tersebut.

Bridge Software vs Hardware Offload

Pada perangkat MikroTik dengan switch chip khusus, bridge dapat memanfaatkan hardware offload, yaitu proses forwarding paket yang ditangani langsung oleh chip switch, bukan oleh CPU utama, sehingga performa jauh lebih tinggi (mendekati kecepatan wire-speed) dan beban CPU jauh berkurang dibanding bridge software murni.

Aspek	Bridge Software	Hardware Offload
Pemrosesan	Ditangani CPU	Ditangani switch chip khusus
Performa	Terbatas oleh kemampuan CPU	Mendekati wire-speed, jauh lebih tinggi
Fleksibilitas fitur	Mendukung semua fitur RouterOS	Beberapa fitur lanjutan mungkin tidak didukung penuh

Spanning Tree Protocol (STP/RSTP)

Ketika terdapat lebih dari satu jalur fisik yang saling terhubung antar switch atau bridge, misalnya untuk redundansi, berpotensi terjadi loop Layer 2 yang menyebabkan broadcast storm dan melumpuhkan jaringan. STP (Spanning Tree Protocol) dan versi yang lebih cepat, RSTP (Rapid STP), bekerja mendeteksi loop tersebut dan secara otomatis memblokir salah satu jalur redundan sampai dibutuhkan, misalnya saat jalur utama terputus.

```
/interface bridge set bridge-lan protocol-mode=rstp
```

Bridge Firewall dan Switch Chip

RouterOS menyediakan firewall khusus untuk trafik yang melewati bridge, terpisah dari firewall IP biasa, karena trafik pada bridge beroperasi di Layer 2 dan bisa saja berupa paket non-IP. Pada perangkat dengan lebih dari satu switch chip, penting pula memahami switch chip group — port-port yang berada pada chip fisik yang sama dapat memanfaatkan hardware offload penuh, sedangkan penggabungan lintas chip mungkin memerlukan penanganan khusus.

Sebagai ilustrasi penerapan di lapangan, WISP sering menggunakan bridge, bukan routing, pada perangkat CPE

pelanggan agar pelanggan menerima IP publik langsung dari core network ISP. Pada topologi menara BTS dengan banyak sektor antena, hardware offload bridge menjadi krusial karena volume trafik yang melewati satu RouterBOARD dapat mencapai ratusan Mbps hingga beberapa Gbps.

Aktivitas Pembelajaran

45. Peserta didik membuat interface bridge baru bernama “bridge-lab”, menambahkan ether2 dan ether3 sebagai port bridge tersebut, lalu memasang IP address 192.168.30.1/24 pada interface bridge-lab.
46. Peserta didik menghubungkan dua laptop ke ether2 dan ether3 dengan IP manual pada subnet yang sama, lalu menguji ping antar keduanya untuk memverifikasi bahwa keduanya berada dalam satu broadcast domain meski terhubung ke port fisik berbeda.
47. Peserta didik mengaktifkan RSTP pada bridge tersebut dan mengamati menu Bridge > STP untuk melihat status tiap port.

Rangkuman

Bridging pada RouterOS menggabungkan beberapa interface fisik menjadi satu segmen jaringan Layer 2, berbeda dengan routing yang bekerja pada Layer 3. Hardware offload meningkatkan performa bridge secara signifikan pada perangkat yang mendukungnya, sementara STP/RSTP mencegah terjadinya loop dan broadcast storm pada jaringan dengan jalur redundan. Pemahaman konsep Layer 2 ini melengkapi kompetensi dasar sebelum peserta didik melanjutkan ke pembahasan pengalamatan IP dan subnetting secara lebih mendalam pada bab berikutnya.

Soal Latihan / Refleksi

48. Jelaskan perbedaan mendasar antara bridging (Layer 2) dan routing (Layer 3).
49. Mengapa IP address sebaiknya dipasang pada interface bridge, bukan pada port fisik individual?
50. Apa fungsi utama STP/RSTP dalam sebuah jaringan dengan jalur redundan?
51. Jelaskan keuntungan performa dari hardware offload dibanding bridge software murni.