BUKU MATERI TJKT — KELAS X/XI

MTCNA

MikroTik Certified Network Associate Konsep, Konfigurasi Praktis & Persiapan Sertifikasi

Disusun untuk Mata Pelajaran Jaringan Dasar & Administrasi Sistem Jaringan
Kompetensi Keahlian Teknik Jaringan Komputer dan Telekomunikasi (TJKT)

Yusuf Burhani, S.Pd., S.Kom

Kata Pengantar

Buku ini disusun sebagai materi ajar bagi peserta didik Kompetensi Keahlian Teknik Jaringan Komputer dan Telekomunikasi (TJKT), dengan fokus pada penguasaan konsep dan praktik jaringan MikroTik setara jenjang sertifikasi MTCNA (MikroTik Certified Network Associate).

Materi disusun secara bertahap mulai dari pengenalan ekosistem MikroTik, instalasi RouterOS, konfigurasi jaringan dasar, keamanan router, routing, bridging, wireless, firewall, quality of service, hingga VPN dasar. Setiap bab dilengkapi dengan kotak LAB berisi praktikum langkah-demi-langkah serta soal uji pemahaman di akhir bab.

Buku ini disusun berdasarkan sintesis dari materi resmi pelatihan MikroTik serta praktik terbaik yang berlaku di industri, dan diharapkan dapat menjadi bekal yang kuat bagi peserta didik baik untuk kebutuhan praktik di dunia kerja maupun sebagai persiapan menempuh ujian sertifikasi MTCNA secara resmi.

Selamat belajar dan semoga sukses menempuh jenjang karier di bidang jaringan komputer.

Daftar Isi

BAB 1

Pengantar MikroTik & RouterOS

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

Tujuan Pembelajaran

Peserta memahami apa itu MikroTik, RouterOS, RouterBOARD, jenis-jenis lisensi RouterOS, dan jalur sertifikasi resmi MikroTik mulai dari MTCNA.

1.1 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.

Dua produk inti MikroTik yang perlu dipahami sejak awal:

- RouterOS — sistem operasi (mirip Linux) yang menjalankan fungsi routing, firewall, bridging, wireless, VPN, QoS, dan berbagai layanan jaringan lainnya.
- RouterBOARD (RB) — perangkat keras (hardware) buatan MikroTik yang sudah terpasang RouterOS di dalamnya, siap pakai layaknya router pada umumnya.

Perlu diketahui

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

1.2 Lini Produk RouterBOARD

RouterBOARD hadir dalam berbagai bentuk sesuai kebutuhan penggunaan:

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 (Tile/ARM)
Cloud Router Switch (CRS)	CRS326, CRS328	Switch layer 2/3 dengan kemampuan RouterOS penuh
Embedded RB	RB912, RB912UAG	Board tertanam untuk perangkat custom/outdoor

1.3 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 yang umum ditemui:

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/dsb dibanding Level 4
Level 6	Lisensi penuh tanpa batasan, umum dipakai di CCR dan CHR produksi

📌 Studi Kasus Nyata — Warnet Beralih ke MikroTik

Sebuah warnet di Yogyakarta pada 2015 menggunakan router pabrikan biasa yang sering hang saat 20+ komputer mengakses game online bersamaan, memaksa admin me-restart router manual setiap beberapa jam. Setelah beralih ke RouterBOARD RB750 (lisensi Level 4) dengan RouterOS, admin dapat menerapkan queue per-komputer dan firewall yang jauh lebih stabil, sekaligus mendapat fitur monitoring yang sebelumnya tidak tersedia di router konsumen biasa — downtime bulanan turun drastis dari puluhan kali menjadi hampir nol, dengan biaya investasi hardware yang jauh lebih murah dibanding solusi enterprise sekelas Cisco.

1.4 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.

- MTCNA — Network Associate (dasar, wajib sebagai gerbang ke semua sertifikasi lain)
- MTCRE — Routing Engineer (routing lanjutan, OSPF, VPN, VLAN)
- MTCWE — Wireless Engineer
- MTCTCE — Traffic Control Engineer (firewall & QoS lanjutan)
- MTCUME — User Management Engine (PPP, RADIUS, Hotspot)
- MTCINE — Internetworking Engineer (BGP, MPLS — level tertinggi, butuh MTCNA + MTCRE)

Format Ujian MTCNA

Ujian sertifikasi dilakukan online di www.mikrotik.com, terdiri dari 25 soal pilihan ganda dalam waktu 60 menit. Nilai minimum kelulusan umumnya 60%, dengan kesempatan mengulang (second chance) pada hari yang sama jika nilai berada di rentang 50-59%.

Penerapan di Industri — Mengapa Sertifikasi Ini Dicari Industri

Banyak WISP (Wireless ISP) 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. Di sisi industri korporat, banyak NOC (Network Operations Center) perusahaan menggunakan RouterOS sebagai edge router karena rasio harga-terhadap-fitur yang tidak tertandingi vendor besar, sehingga tenaga kerja bersertifikat MikroTik menjadi nilai jual tersendiri saat melamar posisi Network Engineer maupun Technical Support di perusahaan ISP.

Uji Pemahaman

1. Sebutkan minimal 3 lini produk RouterBOARD beserta kegunaannya masing-masing.

2. Mengapa MTCNA menjadi syarat wajib sebelum mengambil sertifikasi MikroTik lainnya?

3. Apa perbedaan antara lisensi Level 4 dan Level 6 pada RouterOS?

BAB 2

Instalasi & Manajemen RouterOS

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

Tujuan Pembelajaran

Peserta mampu melakukan instalasi/reinstalasi RouterOS, mengakses router melalui berbagai metode, serta melakukan upgrade dan downgrade versi RouterOS dengan aman.

2.1 Metode Instalasi RouterOS

RouterOS dapat dipasang melalui beberapa jalur tergantung jenis perangkat yang digunakan:

- RouterBOARD bawaan — RouterOS sudah terpasang dari pabrik, tinggal dikonfigurasi.
- Netinstall — 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) — image RouterOS untuk dijalankan sebagai virtual machine (VMware, VirtualBox, Proxmox, Hyper-V, atau cloud provider).
- Instalasi di PC/x86 — RouterOS dapat dipasang langsung di perangkat PC/server biasa dari media instalasi (USB/CD).

2.2 Proses Netinstall

Netinstall adalah tool berbasis Windows yang memungkinkan instalasi ulang RouterOS ke RouterBOARD melalui jaringan, tanpa perlu kartu memori tambahan. Langkah umum penggunaannya:

1. Unduh paket Netinstall dan file RouterOS (.npk) sesuai arsitektur perangkat (mipsbe, arm, tile, x86, dsb) dari situs resmi MikroTik.
2. Hubungkan PC dan RouterBOARD dalam satu jaringan Ethernet, lalu set IP address netinstall sesuai subnet perangkat.
3. Nyalakan ulang RouterBOARD sambil menahan tombol reset agar masuk ke mode Netinstall/Etherboot.
4. Pada aplikasi Netinstall, pilih perangkat yang terdeteksi, tandai paket RouterOS yang ingin dipasang, lalu klik Install.
5. Tunggu proses selesai, router akan reboot otomatis dengan RouterOS baru dalam kondisi default.

Kapan Netinstall dibutuhkan?

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

📌 Studi Kasus Nyata — Router "Terkunci" karena Lupa Password

Seorang teknisi lapangan WISP menerima laporan sebuah RouterBOARD di menara pelanggan tidak bisa diakses sama sekali — password admin hilang bersamaan dengan resign-nya teknisi sebelumnya tanpa dokumentasi serah terima. Alih-alih mengganti seluruh unit (yang berarti downtime lama dan biaya hardware baru), teknisi membawa laptop dengan Netinstall, menghubungkannya langsung ke

router via kabel Ethernet, dan melakukan reinstall bersih RouterOS dalam waktu kurang dari 15 menit — router kembali normal dengan konfigurasi default, tinggal dikonfigurasi ulang sesuai kebutuhan pelanggan tersebut.

2.3 Mengakses Router: Winbox, WebFig, SSH, Telnet

Metode	Karakteristik
Winbox	Aplikasi desktop (Windows/Wine) 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 (memanfaatkan broadcast Layer 2, berguna saat konfigurasi awal sebelum IP diset).

2.4 Dasar Command Line Interface (CLI)

RouterOS memiliki struktur perintah CLI berbasis menu bertingkat (mirip direktori). Beberapa prinsip navigasi dasar:

- Gunakan tombol Tab untuk melengkapi otomatis (auto-complete) nama menu/parameter.
- Tanda "?" menampilkan daftar perintah/parameter yang tersedia pada level menu saat itu.
- Perintah "/" mengembalikan ke menu root/utama.
- Perintah ".." mengembalikan satu level ke menu sebelumnya.
- Command history dapat diakses dengan tombol panah atas/bawah untuk mengulang perintah sebelumnya.

```
/ip address print              ; menampilkan seluruh IP address
/interface print               ; menampilkan seluruh interface
/system identity set name=Router-Sekolah
/ip service print              ; menampilkan status layanan (winbox, ssh, dsb)
```

2.5 Upgrade dan Downgrade RouterOS

RouterOS memiliki dua jenis paket: paket utama (routeros) dan paket tambahan (misalnya wireless, ipv6, dude, dsb) yang bisa dipasang terpisah sesuai kebutuhan.

6. Cara termudah: menu System > Packages > Check For Updates di Winbox, lalu klik Download & Install.

7. Cara manual: unduh file paket .npk sesuai arsitektur perangkat, unggah ke router melalui menu Files, lalu reboot router untuk memicu instalasi otomatis.
8. Downgrade dilakukan dengan cara serupa namun menggunakan file paket versi lebih lama, atau melalui perintah "/system package downgrade" jika paket versi lama tersedia di penyimpanan router.

Perhatian

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

LAB: Instalasi & Akses Awal Router

1. Hubungkan laptop ke port Ethernet router MikroTik menggunakan kabel LAN.

2. Buka aplikasi Winbox, klik tombol "..." pada kolom Connect To untuk mencari router melalui broadcast MAC address.

3. Login menggunakan username default "admin" tanpa password (kondisi default pabrik).

4. Buka menu System > Identity, ubah nama router sesuai nama laboratorium/kelas Anda.

5. Buka menu System > Packages, catat versi RouterOS yang terpasang saat ini.

6. Buka New Terminal, jalankan perintah "/system resource print" dan amati informasi CPU, memori, serta versi RouterOS.

2.6 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                ; menampilkan versi RouterBOOT saat ini dan
versi terbaru yang tersedia
/system routerboard upgrade               ; memulai proses upgrade RouterBOOT ke versi
terbaru
; setelah upgrade, WAJIB reboot manual agar firmware baru benar-benar aktif
/system reboot
```

Perbedaan penting

Meng-upgrade paket RouterOS TIDAK secara otomatis meng-upgrade RouterBOOT. Banyak kasus router "berjalan tidak stabil" setelah update besar RouterOS (misalnya lompat dari v6 ke v7) disebabkan oleh RouterBOOT yang tertinggal jauh dari versi RouterOS yang berjalan di atasnya — sehingga upgrade RouterBOOT harus dilakukan sebagai langkah terpisah dan tidak boleh dilewatkan.

Penerapan di Industri — Downgrade & RouterBOOT di Lapangan

Teknisi WISP yang mengelola ratusan perangkat di menara BTS pelanggan biasanya menstandarkan satu versi RouterOS dan RouterBOOT tertentu yang sudah terbukti stabil (bukan selalu versi terbaru), lalu melakukan mass-deployment versi yang sama ke seluruh perangkat menggunakan Netinstall agar

konsisten. Ini mengurangi risiko downtime akibat bug pada versi baru yang belum teruji di lapangan, sekaligus memudahkan troubleshooting karena seluruh perangkat berperilaku sama.

✓ Uji Pemahaman

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

2. Kapan sebaiknya kita menggunakan Netinstall dibanding upgrade biasa?

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

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

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

BAB 3

Konfigurasi Dasar Router

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

Tujuan Pembelajaran

Peserta mampu mengonfigurasi IP address, default gateway, DNS, serta menghubungkan jaringan lokal ke internet menggunakan firewall NAT masquerade.

3.1 Topologi Dasar Jaringan MikroTik

Skenario paling umum dalam praktik MTCNA adalah router MikroTik yang memiliki dua sisi jaringan: sisi WAN (terhubung ke internet/ISP) dan sisi LAN (terhubung ke jaringan lokal/klien). Konsep dasar yang wajib dipahami sebelum mengonfigurasi adalah membedakan interface mana yang berfungsi sebagai WAN dan mana yang berfungsi sebagai LAN.

3.2 Konfigurasi IP Address

IP address di RouterOS diikatkan pada sebuah interface (misalnya ether1, ether2, wlan1). Format penulisan menggunakan notasi CIDR (Classless Inter-Domain Routing), 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)

3.3 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 (Domain Name System) 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.

Studi Kasus Nyata — Internet Kantor "Lambat" Ternyata Salah DNS

Karyawan sebuah kantor kecil mengeluhkan browsing terasa lambat meski hasil speedtest menunjukkan bandwidth normal. Setelah ditelusuri, admin menemukan router hanya diarahkan ke satu DNS server yang sering timeout, sehingga setiap kali klien membuka website baru, terjadi jeda lama sebelum nama domain berhasil diterjemahkan ke IP address — padahal koneksi data sesungguhnya sudah cepat begitu terhubung. Solusinya sederhana: menambahkan DNS sekunder (misalnya 1.1.1.1 sebagai cadangan dari 8.8.8.8) dan mengaktifkan DNS caching di router, sehingga permintaan DNS yang berulang tidak perlu keluar ke internet lagi. Keluhan lambat hilang tanpa perlu upgrade bandwidth sama sekali.

3.4 Koneksi WAN via DHCP Client

Jika ISP menyediakan IP secara dinamis (umum 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
```

3.5 NAT Masquerade — Menghubungkan LAN ke Internet

Karena IP address di jaringan lokal (LAN) umumnya bersifat private (misalnya 192.168.x.x) dan tidak dapat diroutingkan 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.

3.6 Troubleshooting Konektivitas Dasar

- Gunakan "ping" untuk menguji konektivitas dasar ke gateway, DNS, atau internet.
- Gunakan "/tool traceroute" untuk melihat jalur yang dilalui paket menuju tujuan.
- Periksa "/ip route print" untuk memastikan default route sudah ada dan berstatus aktif (flag A).
- Periksa "/ip firewall nat print" untuk memastikan rule masquerade sudah terpasang dan urutannya benar.

Metodologi troubleshooting yang disiplin sangat penting di dunia kerja: mulai dari lapisan terendah (fisik/link — apakah lampu interface menyala, apakah 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 mencegah teknisi menebak-nebak dan mempercepat proses isolasi masalah, terutama saat menangani laporan gangguan dari banyak pelanggan sekaligus.

Penerapan di Industri — Studi Kasus ISP/WISP

Pada ISP rumahan, skema WAN-LAN-NAT seperti pada bab ini adalah konfigurasi paling dasar yang dijalankan di CPE (Customer Premises Equipment) pelanggan. Namun pada praktiknya, banyak ISP tidak memberi IP publik langsung ke tiap pelanggan (karena keterbatasan IPv4), melainkan menerapkan CGNAT (Carrier-Grade NAT) di sisi core network — pelanggan tetap mendapat IP privat dari DHCP/PPPoE ISP, lalu NAT dilakukan berlapis di beberapa titik sebelum benar-benar keluar ke internet publik. Memahami NAT masquerade dasar di bab ini adalah fondasi wajib sebelum memahami skema CGNAT yang lebih kompleks tersebut.

LAB: Konfigurasi Internet Dasar (WAN-LAN-NAT)

1. Set ether1 sebagai interface WAN, aktifkan DHCP client pada ether1.

2. Set IP address statis 192.168.10.1/24 pada ether2 sebagai interface LAN.

3. Tambahkan rule NAT masquerade untuk interface WAN (ether1).

4. Hubungkan laptop ke ether2, set IP laptop secara manual di subnet yang sama (misal 192.168.10.10/24) dengan gateway 192.168.10.1.

5. Uji ping dari laptop ke gateway router (192.168.10.1), lalu ke DNS publik (8.8.8.8), lalu ke domain (google.com).

6. Jika ping ke domain gagal namun ping ke 8.8.8.8 berhasil, periksa kembali konfigurasi DNS pada router.

Uji Pemahaman

1. Jelaskan fungsi default gateway pada tabel routing.

2. Mengapa diperlukan NAT masquerade agar jaringan lokal dapat mengakses internet?

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

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

BAB 4

DHCP Server & Client

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

Tujuan Pembelajaran

Peserta mampu mengonfigurasi DHCP server lengkap dengan pool, lease, static binding, serta memahami mekanisme ARP yang mendukung proses tersebut.

4.1 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.

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

4.2 Konfigurasi DHCP Server

RouterOS menyediakan wizard "DHCP Setup" yang mempercepat proses konfigurasi, namun pemahaman komponen manualnya tetap penting:

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
```

4.3 DHCP Lease dan Static Lease

Setiap kali klien menerima IP dari DHCP server, informasi tersebut tercatat di menu Leases. Ini 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 — 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 — perangkat asing otomatis ditolak. Ini merupakan salah satu bentuk keamanan dasar pada jaringan yang membutuhkan kontrol ketat terhadap perangkat yang terhubung.

Studi Kasus Nyata — Printer Kantor Selalu "Hilang" Setiap Pagi

Staf administrasi sebuah sekolah rutin mengeluh printer jaringan tidak terdeteksi setiap pagi, padahal sore harinya berfungsi normal. Setelah diselidiki, IT menemukan printer tersebut mendapat IP address dinamis dari DHCP, dan setiap kali printer dimatikan semalaman lalu dinyalakan kembali paginya, ada kemungkinan IP yang didapat berbeda dari hari sebelumnya (karena lease sebelumnya sudah diklaim perangkat lain semalaman) — sementara komputer staf sudah terlanjur menyimpan IP lama di driver printer mereka. Solusi permanennya adalah membuat static lease untuk MAC address printer tersebut, memastikan IP-nya selalu sama kapan pun dinyalakan, sehingga tidak perlu lagi mengatur ulang driver printer di puluhan komputer setiap kali masalah muncul.

4.4 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 (berguna untuk skenario bridging tertentu)
reply-only	Router hanya menjawab ARP request untuk entry yang sudah didaftarkan secara statis, tidak belajar otomatis — kombinasi keamanan populer dengan static lease DHCP

LAB: Konfigurasi DHCP Server & Static Lease

1. Buat IP Pool dengan rentang 192.168.20.10 sampai 192.168.20.100.

2. Buat DHCP Server pada interface ether3 menggunakan pool tersebut.

3. Definisikan DHCP Network dengan gateway 192.168.20.1 dan DNS 8.8.8.8.

4. Hubungkan laptop ke ether3, pastikan laptop menerima IP otomatis, cek melalui "ipconfig" (Windows) atau "ifconfig" (Linux/Mac).

5. Di router, buka menu DHCP Server > Leases, catat MAC address laptop yang muncul.

6. Buat static lease untuk MAC address laptop tersebut agar selalu mendapat IP 192.168.20.50.

7. Putuskan dan sambungkan kembali koneksi laptop, verifikasi IP yang didapat tetap 192.168.20.50.

Penerapan di Industri — DHCP di Jaringan Skala Besar

Pada jaringan kampus atau perkantoran dengan ratusan klien, DHCP static-only dan static lease adalah praktik standar untuk perangkat kritis seperti server, printer jaringan, access point, dan kamera CCTV — sehingga perangkat IT dapat memantau dan memfilter berdasarkan IP yang konsisten. Sebaliknya, untuk jaringan BYOD (Bring Your Own Device) seperti WiFi tamu di kantor/kampus, dynamic lease dengan masa sewa (lease time) pendek justru lebih disukai agar IP address yang tidak lagi dipakai (perangkat yang sudah pergi) cepat kembali ke pool dan dapat dipakai ulang oleh klien baru.

☑ Uji Pemahaman

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

2. Apa perbedaan antara dynamic lease dan static lease?

3. Bagaimana fitur "DHCP Static Only" dapat meningkatkan keamanan jaringan?

4. Jelaskan fungsi mode ARP "reply-only" dan kapan sebaiknya digunakan.

BAB 5

Backup, Restore, Export & Import Konfigurasi

Mempelajari cara mengamankan konfigurasi router agar dapat dipulihkan dengan cepat saat terjadi kegagalan perangkat atau kesalahan konfigurasi.

Tujuan Pembelajaran

Peserta memahami perbedaan backup dan export, mampu melakukan backup/restore, export/import, serta melakukan reset konfigurasi dengan aman.

5.1 Backup vs Export — Apa Bedanya?

RouterOS menyediakan dua mekanisme berbeda untuk menyimpan konfigurasi, dan keduanya sering tertukar oleh pemula:

Aspek	Backup (.backup)	Export (.rsc)
Format file	Biner, tidak bisa dibaca manusia	Teks, berupa daftar perintah CLI, bisa dibaca dan diedit
Isi	Seluruh konfigurasi termasuk user & password	Konfigurasi dalam bentuk skrip perintah
Kompatibilitas	Hanya bisa direstore ke RouterOS dengan versi & arsitektur yang kompatibel	Fleksibel, bisa diedit lalu dijalankan ulang (import) di router lain
Kegunaan umum	Pemulihan cepat router yang sama persis	Dokumentasi, migrasi konfigurasi, templating

5.2 Melakukan Backup dan Restore

```
/system backup save name=backup-router-2026
/system backup load name=backup-router-2026
```

Perhatian saat restore

Proses restore backup akan menggantikan seluruh konfigurasi router dan memicu reboot otomatis. Pastikan file backup berasal dari perangkat dengan versi RouterOS dan arsitektur (mipsbe, arm, x86, dsb) yang sesuai.

5.3 Export dan Import Konfigurasi

Perintah export menghasilkan file berisi rangkaian perintah CLI yang, jika dijalankan kembali (import), akan membentuk ulang konfigurasi yang sama. File export sangat berguna karena bisa dibuka dengan text editor, diedit sebagian (misalnya mengganti IP address sebelum diterapkan ke router lain), dan didokumentasikan.

```
/export file=konfigurasi-lengkap
```

```
/ip firewall export file=konfigurasi-firewall   ; export hanya bagian firewall
/import file-name=konfigurasi-lengkap.rsc
```

Studi Kasus Nyata — Router Rusak Saat Petir, Bisnis Tetap Jalan

Sebuah toko retail mengalami router utamanya rusak total akibat sambaran petir yang merambat lewat kabel listrik, padahal toko tersebut sangat bergantung pada koneksi internet untuk sistem kasir online. Karena admin IT rutin melakukan export konfigurasi mingguan yang disimpan di cloud storage terpisah, mereka hanya perlu membeli RouterBOARD pengganti dengan model serupa, meng-import file export terakhir, dan toko kembali online dalam waktu kurang dari satu jam — dibandingkan tanpa backup yang bisa memakan waktu berhari-hari untuk mengingat dan mengetik ulang seluruh konfigurasi dari nol.

5.4 Reset Konfigurasi

Reset mengembalikan router ke kondisi konfigurasi kosong (atau default pabrik). Terdapat pilihan untuk tetap menyimpan akses (no-defaults) atau langsung memuat konfigurasi default RouterBOARD setelah reset.

```
/system reset-configuration no-defaults=yes
/system reset-configuration keep-users=yes
```

LAB: Backup, Export, dan Simulasi Restore

1. Lakukan konfigurasi dasar router (IP address, DHCP server) seperti pada bab sebelumnya.

2. Jalankan perintah backup dan simpan dengan nama yang jelas (contoh: backup-sebelum-uji).

3. Jalankan perintah export ke file terpisah, lalu buka file .rsc tersebut melalui menu Files dan amati isinya.

4. Ubah salah satu konfigurasi (misal ganti IP address LAN).

5. Lakukan restore menggunakan file backup yang telah dibuat sebelumnya, amati apakah konfigurasi kembali seperti semula.

6. Diskusikan: dalam kondisi apa Anda akan memilih export dibanding backup, dan sebaliknya?

Penerapan di Industri — Standar Operasional Backup di Perusahaan

Perusahaan dengan banyak perangkat jaringan biasanya menjadwalkan backup otomatis (menggunakan scheduler RouterOS atau sistem monitoring eksternal) yang mengirim salinan file export/backup ke server terpusat setiap malam. Ini krusial saat terjadi kerusakan hardware mendadak — teknisi cukup memasang router pengganti dan mengimpor konfigurasi terakhir, memangkas downtime dari berjam-jam menjadi hitungan menit. File export (.rsc) juga sering dijadikan template konfigurasi standar (golden config) yang di-deploy ke banyak cabang sekaligus, dengan bagian IP address diedit sesuai lokasi masing-masing.

Uji Pemahaman

1. Jelaskan perbedaan mendasar antara file backup (.backup) dan file export (.rsc).

2. Mengapa file backup tidak selalu bisa dipindahkan begitu saja ke perangkat MikroTik lain?

3. Kapan sebaiknya kita menggunakan export dibanding backup?

4. Apa risiko yang perlu diperhatikan sebelum melakukan restore konfigurasi?

BAB 6

Keamanan Dasar Router

Mengamankan router itu sendiri sebelum mengamankan jaringan di baliknya — mulai dari manajemen user, pembatasan layanan, hingga monitoring dasar.

Tujuan Pembelajaran

Peserta mampu mengelola user & group RouterOS, membatasi layanan yang tidak diperlukan, serta menggunakan tools monitoring dasar seperti Neighbor Discovery dan SNMP.

6.1 Mengapa Router Perlu Diamankan Dahulu

Sebelum berbicara tentang firewall untuk melindungi jaringan klien, langkah pertama yang sering terlupakan adalah mengamankan router itu sendiri sebagai perangkat. Router yang tidak aman berisiko diakses pihak tak berwenang, yang bisa mengubah seluruh konfigurasi jaringan.

6.2 User dan Group RouterOS

RouterOS mendukung banyak akun user dengan hak akses (permission) berbeda melalui sistem group. Tiga group bawaan yang tersedia:

Group	Hak Akses
full	Akses penuh ke seluruh konfigurasi router
write	Dapat mengubah konfigurasi, namun tidak dapat mengelola user lain
read	Hanya dapat melihat konfigurasi tanpa mengubah apa pun

```
/user add name=operator password=Passw0rd! group=write
/user print
/user disable admin   ; menonaktifkan (bukan menghapus) user default
```

Praktik terbaik

Buat akun administrator dengan nama unik (bukan "admin" default) dan password yang kuat, lalu nonaktifkan atau hapus akun admin default untuk mengurangi risiko serangan brute-force yang menyasar username umum.

6.3 Membatasi IP Service

Menu IP Service mengatur layanan manajemen apa saja yang aktif di router (Winbox, WWW, SSH, Telnet, FTP, API, dsb) beserta port dan sumber IP yang diizinkan mengaksesnya.

```
/ip service disable telnet,ftp,www
/ip service set winbox address=192.168.10.0/24
```

```
/ip service set ssh port=2222
```

Menonaktifkan layanan yang tidak digunakan (misalnya Telnet dan FTP yang tidak terenkripsi) serta membatasi service hanya dapat diakses dari subnet manajemen tertentu adalah praktik keamanan dasar yang sangat efektif.

6.4 Neighbor Discovery (MNDP/CDP)

Fitur Neighbor Discovery memungkinkan perangkat MikroTik saling mengenali perangkat MikroTik lain (dan perangkat yang mendukung protokol CDP seperti Cisco) di jaringan Layer 2 yang sama — berguna untuk topology discovery, namun juga dapat membocorkan informasi perangkat ke pihak yang tidak berwenang jika dibiarkan aktif di semua interface, termasuk interface WAN.

```
/ip neighbor print
/ip neighbor discovery-settings set discover-interface-list=LAN-only
```

6.5 Tools Monitoring Dasar

- MAC Server — mengatur apakah router dapat diakses melalui Winbox/Telnet berbasis MAC address, dan dari interface mana saja.
- Tools > Email — memungkinkan router mengirim notifikasi otomatis (misalnya alert) melalui email.
- Tools > Profile — menampilkan penggunaan CPU per proses/fitur pada router, berguna untuk troubleshooting performa.
- SNMP — protokol standar industri untuk memonitor perangkat jaringan dari sistem monitoring eksternal (Zabbix, PRTG, Cacti, dsb).
- The Dude — aplikasi monitoring jaringan buatan MikroTik untuk visualisasi topologi dan status perangkat secara real-time.

SNMP bekerja dengan model client-server: router bertindak sebagai SNMP agent yang menyediakan data (misalnya penggunaan CPU, trafik interface, suhu perangkat) melalui OID (Object Identifier) tertentu, sementara sistem monitoring eksternal (SNMP manager) secara berkala melakukan polling data tersebut untuk ditampilkan dalam dashboard atau memicu alert otomatis jika suatu ambang batas (threshold) terlampaui. Di lingkungan produksi, SNMP selalu diaktifkan dengan community string yang tidak mudah ditebak (bukan "public" default) atau menggunakan SNMPv3 yang mendukung autentikasi dan enkripsi, karena SNMP versi lama (v1/v2c) mengirim data dalam bentuk plain-text.

Penerapan di Industri — NOC dan Monitoring 24/7

Perusahaan ISP dan WISP skala menengah-besar biasanya mengoperasikan NOC (Network Operations Center) yang memantau ratusan hingga ribuan perangkat MikroTik secara bersamaan menggunakan kombinasi SNMP dan sistem monitoring seperti Zabbix, PRTG, LibreNMS, atau The Dude. Ketika satu perangkat down atau CPU melonjak abnormal, sistem monitoring otomatis mengirim notifikasi ke tim on-call melalui Telegram/WhatsApp/email — jauh lebih efisien dibanding menunggu laporan keluhan pelanggan. Praktik hardening seperti menonaktifkan layanan tak terpakai dan membatasi akses manajemen per-subnet (seperti dipelajari di bab ini) menjadi baseline keamanan wajib sebelum perangkat "go-live" di jaringan produksi.

Studi Kasus Nyata — Router Publik Kena Brute-Force

Sebuah RT/RW-net di pinggiran kota membiarkan port Winbox default (8291) terbuka ke internet tanpa pembatasan IP, dengan alasan agar admin bisa mengelola router dari mana saja. Beberapa bulan kemudian, router tiba-tiba mengalami CPU 100% dan seluruh pelanggan mengeluh internet mati — investigasi menunjukkan router terkena serangan brute-force otomatis yang mencoba ribuan kombinasi password per menit, membebani CPU hingga router tidak sanggup lagi memproses trafik normal. Setelah membatasi akses Winbox hanya dari IP tertentu (menggunakan VPN untuk akses remote) dan mengganti seluruh password default, serangan berhenti total dan performa router kembali normal.

LAB: Hardening Keamanan Dasar Router

1. Buat user baru dengan group "full" menggunakan nama unik dan password kuat.

2. Login menggunakan user baru tersebut untuk memastikan berfungsi.

3. Nonaktifkan user "admin" default.

4. Nonaktifkan layanan Telnet dan FTP melalui menu IP Service.

5. Batasi akses Winbox hanya dari subnet LAN Anda (misal 192.168.10.0/24).

6. Periksa menu IP > Neighbors, identifikasi perangkat lain yang terdeteksi di jaringan lab.

Uji Pemahaman

1. Mengapa menonaktifkan user "admin" default dianggap praktik keamanan yang baik?

2. Jelaskan tiga group user bawaan RouterOS beserta perbedaan hak aksesnya.

3. Mengapa Telnet sebaiknya dinonaktifkan pada router produksi?

4. Apa risiko membiarkan Neighbor Discovery aktif di interface WAN?

BAB 7

Routing Dasar

Memahami cara router MikroTik menentukan jalur pengiriman paket melalui static routing, serta tools untuk memantau kualitas rute tersebut.

Tujuan Pembelajaran

Peserta mampu memahami komponen tabel routing, mengonfigurasi static route termasuk multiple gateway dan check-gateway, serta menggunakan tools Netwatch dan Traceroute.

7.1 Konsep Dasar Routing

Routing adalah proses menentukan jalur terbaik yang harus dilalui sebuah paket data untuk mencapai tujuannya. Setiap router menyimpan informasi ini dalam tabel routing, yang berisi daftar rute beserta interface/gateway yang harus dilalui.

Tipe Rute	Sumber
Connected	Terbentuk otomatis dari IP address yang dikonfigurasi langsung pada interface
Static	Ditambahkan manual oleh administrator
Dynamic	Dipelajari otomatis melalui protokol routing seperti OSPF atau BGP (dibahas di buku MTCRE)

7.2 Parameter Static Route

```
/ip route add dst-address=10.10.10.0/24 gateway=192.168.1.254 distance=1
```

Parameter	Fungsi
dst-address	Jaringan tujuan yang ingin dicapai
gateway	Alamat next-hop atau nama interface yang harus dilalui
distance	Administrative distance — menentukan prioritas jika ada beberapa rute menuju tujuan yang sama (nilai lebih kecil = prioritas lebih tinggi)

7.3 Membaca Flags pada Routing Table

Flag	Arti
A	Active — rute sedang aktif digunakan
S	Static — rute ditambahkan manual

Flag	Arti
C	Connected — rute otomatis dari IP address interface
D	Dynamic — rute dipelajari dari protokol routing dinamis
X	Disabled — rute dinonaktifkan
U	Unreachable — tujuan tidak dapat dicapai

7.4 Multiple Gateway dan Pemilihan Rute

RouterOS mendukung penambahan beberapa gateway sekaligus menuju satu tujuan yang sama, baik untuk keperluan load balancing sederhana maupun failover. Pemilihan rute aktif ditentukan oleh distance terkecil; jika distance sama, RouterOS akan melakukan pembagian trafik secara round-robin sederhana (bukan load balancing sejati — untuk load balancing yang tepat, ECMP dibahas lebih lanjut di buku MTCRE).

7.5 Check-Gateway — Deteksi Kegagalan Rute

Parameter check-gateway memungkinkan router secara aktif memeriksa apakah gateway masih dapat dijangkau (melalui ping atau ARP). Jika gateway utama tidak merespons, router otomatis menonaktifkan rute tersebut dan beralih ke rute cadangan dengan distance lebih besar — inilah dasar mekanisme failover sederhana di RouterOS.

```
/ip route add dst-address=0.0.0.0/0 gateway=192.168.1.254 distance=1 check-gateway=ping
/ip route add dst-address=0.0.0.0/0 gateway=192.168.2.254 distance=2 check-gateway=ping
```

Di luar ping, check-gateway juga mendukung metode "arp" — memeriksa keberadaan gateway melalui ARP request/reply, berguna pada skenario di mana perangkat gateway dikonfigurasi untuk tidak merespons ICMP ping (sering dilakukan sebagai langkah keamanan) namun tetap merespons ARP karena berada di segmen Layer 2 yang sama.

Penerapan di Industri — Failover Internet di Kantor/Sekolah

Skema static route dengan check-gateway seperti pada bab ini adalah solusi failover paling umum diterapkan di kantor kecil-menengah maupun sekolah yang tidak memiliki tim IT khusus untuk mengelola protokol routing dinamis yang lebih kompleks (seperti BGP). Banyak instansi menggabungkan satu koneksi ISP fiber sebagai jalur utama dan satu modem 4G/5G sebagai cadangan, sehingga saat fiber terputus (misalnya akibat galian kabel), layanan internet tetap berjalan otomatis melalui jalur seluler tanpa campur tangan manual — krusial bagi bisnis yang bergantung pada koneksi internet stabil seperti kasir online, absensi digital, atau sistem pembelajaran daring.

Studi Kasus Nyata — Toko Online Selamat dari Putusnya Fiber

Sebuah UMKM yang berjualan online mengandalkan satu koneksi fiber sebagai satu-satunya akses internet. Suatu hari terjadi galian proyek di dekat toko yang memutus kabel fiber tersebut, dan tanpa jalur cadangan, seluruh operasional toko online (chat pelanggan, update stok, konfirmasi pembayaran) lumpuh selama lebih dari 6 jam hingga teknisi ISP memperbaiki kabel. Setelah kejadian tersebut, pemilik toko berinvestasi pada modem 4G sebagai jalur kedua dan meminta teknisi mengonfigurasi

static route dengan check-gateway seperti dipelajari di bab ini — kejadian serupa berikutnya tidak lagi berdampak sama sekali karena trafik otomatis berpindah ke jalur 4G dalam hitungan detik.

7.6 Tools Pendukung: Netwatch dan Traceroute

- Netwatch — memantau status up/down suatu host secara berkala, dan dapat menjalankan skrip otomatis (misalnya kirim notifikasi) saat status berubah.
- Traceroute — menampilkan setiap hop (titik lompatan) yang dilalui paket menuju tujuan, membantu mengidentifikasi di titik mana sebuah koneksi mengalami gangguan.

```
/tool netwatch add host=8.8.8.8 interval=10s
/tool traceroute 8.8.8.8
```

🔗 LAB: Static Route dengan Failover Sederhana

1. Siapkan topologi dua router: Router A (client) terhubung ke Router B dan Router C sebagai dua jalur berbeda menuju internet simulasi.

2. Tambahkan static route default (0.0.0.0/0) mengarah ke Router B dengan distance=1 dan check-gateway=ping.

3. Tambahkan static route default kedua mengarah ke Router C dengan distance=2 dan check-gateway=ping.

4. Uji koneksi dari Router A, pastikan trafik melewati Router B (cek dengan traceroute).

5. Matikan interface menuju Router B secara sengaja, amati apakah trafik otomatis berpindah ke Router C.

6. Jalankan "/ip route print" untuk mengamati perubahan flag Active (A) pada kedua rute selama pengujian.

☑ Uji Pemahaman

1. Jelaskan tiga sumber rute yang bisa muncul pada tabel routing RouterOS.

2. Bagaimana RouterOS menentukan rute mana yang aktif jika ada dua rute menuju tujuan yang sama?

3. Jelaskan cara kerja parameter check-gateway dalam mekanisme failover.

4. Apa perbedaan fungsi antara tool Netwatch dan Traceroute?

BAB 8

Bridging & Switching

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

Tujuan Pembelajaran

Peserta mampu membuat dan mengonfigurasi bridge, memahami perbedaan bridge software dan hardware offload, serta memahami dasar STP/RSTP untuk mencegah loop jaringan.

8.1 Konsep Bridging

Bridge adalah fitur yang menggabungkan dua atau lebih interface fisik (Ethernet, wireless) menjadi satu segmen jaringan Layer 2 yang sama, seolah-olah semua perangkat yang terhubung berada dalam satu switch. Ini berbeda dengan routing, yang bekerja di Layer 3 dan memisahkan jaringan menjadi subnet-subnet berbeda.

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).

8.2 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 yang kini merepresentasikan keseluruhan segmen jaringan tersebut.

8.3 Bridge Software vs Hardware Offload

Pada perangkat MikroTik dengan switch chip khusus, bridge dapat memanfaatkan hardware offload — proses forwarding paket 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

Aspek	Bridge Software	Hardware Offload
Fleksibilitas fitur	Mendukung semua fitur RouterOS (firewall bridge, dsb)	Beberapa fitur lanjutan mungkin tidak didukung penuh

8.4 Spanning Tree Protocol (STP/RSTP)

Ketika terdapat lebih dari satu jalur fisik yang saling terhubung antar switch/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 putus).

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

8.5 Bridge Firewall dan Switch Chip

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

Penerapan di Industri — Bridging di Jaringan WISP

WISP sering menggunakan bridge (bukan routing) pada perangkat CPE pelanggan agar pelanggan menerima IP publik langsung dari core network ISP, bukan IP privat hasil NAT di CPE — memudahkan ISP memberikan layanan seperti IP static atau port forwarding tanpa perlu konfigurasi tambahan di sisi pelanggan. Pada topologi menara BTS dengan banyak sektor antena, hardware offload bridge menjadi krusial karena volume trafik yang melewati satu RouterBOARD bisa mencapai ratusan Mbps hingga beberapa Gbps — jika bridge diproses murni oleh CPU (software), perangkat akan cepat mengalami bottleneck performa.

Studi Kasus Nyata — Broadcast Storm Melumpuhkan Lab Komputer

Sebuah lab komputer sekolah mendadak mengalami jaringan sangat lambat setelah siswa magang menambahkan satu kabel tambahan antar-switch untuk "memastikan koneksi lebih stabil", tanpa menyadari ini menciptakan loop fisik antara dua switch yang sudah terhubung lewat jalur lain. Loop tersebut menyebabkan broadcast storm yang membanjiri seluruh jaringan dengan trafik duplikat hingga hampir seluruh bandwidth habis hanya untuk trafik broadcast yang berputar-putar. Setelah mengaktifkan RSTP pada bridge MikroTik yang menjadi titik pusat jaringan, insiden serupa yang terjadi kembali (siswa lain melakukan kesalahan sama) tidak lagi berdampak — RSTP otomatis mendeteksi loop dan memblokir salah satu jalur redundan tanpa memengaruhi konektivitas lab sama sekali.

LAB: Membuat Bridge dan Menguji Broadcast Domain

1. Buat interface bridge baru bernama "bridge-lab".

2. Tambahkan ether2 dan ether3 sebagai port dari bridge tersebut.

3. Pasang IP address 192.168.30.1/24 pada interface bridge-lab (bukan pada ether2/ether3 secara individu).

4. Hubungkan dua laptop ke ether2 dan ether3, set IP manual pada subnet yang sama.

5. Uji ping antar kedua laptop, verifikasi keduanya dapat saling berkomunikasi meski terhubung ke port fisik berbeda.

6. Aktifkan RSTP pada bridge tersebut dan amati menu Bridge > STP untuk melihat status port.

✓ Uji Pemahaman

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

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

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

4. Jelaskan keuntungan performa dari hardware offload dibanding bridge software murni.

BAB 9

Wireless 802.11

Mempelajari konsep dasar jaringan nirkabel berbasis standar 802.11, konfigurasi Point-to-Point, Point-to-MultiPoint, hingga pengamanan jaringan wireless.

Tujuan Pembelajaran

Peserta memahami standar wireless, mampu mengonfigurasi mode Access Point maupun Station, menerapkan keamanan WPA2, serta menggunakan tools monitoring sinyal.

9.1 Standar Wireless IEEE 802.11

Standar	Frekuensi	Kecepatan Maksimum (teoretis)
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4/5 GHz	hingga 600 Mbps (MIMO)
802.11ac	5 GHz	hingga beberapa Gbps (MU-MIMO)

Frekuensi 2.4 GHz memiliki jangkauan lebih jauh dan lebih baik menembus penghalang, namun lebih rentan interferensi karena dipakai banyak perangkat (WiFi rumahan, Bluetooth, microwave). Frekuensi 5 GHz menyediakan lebih banyak channel bersih dan kecepatan lebih tinggi, namun jangkauannya lebih pendek dan lebih mudah terhalang. Penggunaan frekuensi juga tunduk pada regulasi masing-masing negara.

9.2 Mode Wireless: AP Bridge vs Station

Mode	Fungsi
ap bridge	Perangkat berfungsi sebagai Access Point, menerima koneksi dari klien/station
station	Perangkat berfungsi sebagai klien yang terhubung ke sebuah Access Point
station bridge	Mode station khusus MikroTik yang mendukung bridging Layer 2 penuh ke sisi AP (umum dipakai pada link PTP)
bridge	Mode PTP murni antara dua perangkat MikroTik

9.3 Konfigurasi Point-to-Point (PTP)

Link PTP menghubungkan dua titik secara langsung menggunakan antena directional, umum digunakan untuk menjangkau lokasi yang jauh dari jaringan utama (misalnya menghubungkan gedung berbeda).

9. Pada sisi Access Point: set mode=ap bridge, tentukan SSID dan frequency/band.

10. Pada sisi Station: set mode=station (atau station bridge), pastikan band dan SSID sama dengan AP.
11. Setelah terhubung, gabungkan interface wireless ke dalam bridge pada masing-masing sisi jika ingin trafik Layer 2 transparan.
12. Pasang IP address pada bridge (bukan pada interface wireless langsung) sesuai kebutuhan jaringan.

9.4 Point-to-MultiPoint (PTMP)

Berbeda dengan PTP, PTMP memungkinkan satu Access Point melayani banyak klien station sekaligus — skema umum pada jaringan WISP (Wireless ISP) untuk melayani banyak pelanggan dari satu tower/menara.

Sebelum memasang PTMP, teknisi biasanya melakukan site survey menggunakan fitur Scanner (untuk melihat SSID dan sinyal AP lain di sekitar) dan Frequency Usage (untuk memeriksa channel mana yang paling bersih dari interferensi sebelum menentukan frekuensi operasional).

Studi Kasus Nyata — Sinyal WiFi Kuat Tapi Internet Tetap Lambat

Sebuah kafe menerima keluhan pelanggan bahwa sinyal WiFi tampak penuh (full bar) di HP mereka, namun browsing tetap sangat lambat terutama saat jam ramai. Setelah dicek menggunakan Registration Table, admin menemukan puluhan perangkat terhubung ke satu Access Point yang sama pada frekuensi 2.4GHz yang sudah sangat padat oleh interferensi dari kafe dan rumah tetangga di sekitarnya — sinyal kuat tidak berarti kualitas koneksi baik jika channel yang dipakai penuh gangguan. Solusinya adalah memindahkan sebagian beban ke Access Point tambahan di frekuensi 5GHz (yang jauh lebih bersih dari interferensi) serta melakukan channel scan ulang untuk memilih channel 2.4GHz yang paling sedikit dipakai jaringan tetangga.

9.5 Keamanan Jaringan Wireless

Mekanisme	Fungsi
Security Profile (WPA/WPA2 PSK)	Enkripsi dan autentikasi menggunakan passphrase bersama
Access List	Mengizinkan/menolak koneksi berdasarkan MAC address tertentu (dikonfigurasi di sisi AP)
Connect List	Menentukan AP mana yang boleh dihubungi oleh station (dikonfigurasi di sisi client)
WPS (WiFi Protected Setup)	Metode pairing cepat, namun secara umum dianggap kurang aman untuk lingkungan produksi

```
/interface wireless security-profiles add name=wpa2-lab mode=dynamic-keys
authentication-types=wpa2-psk wpa2-pre-shared-key=SekolahTJKT2026
/interface wireless set wlan1 security-profile=wpa2-lab
```

Access List vs Security Profile

Security Profile mengatur "bagaimana" koneksi dienkripsi (passphrase), sedangkan Access List mengatur "siapa" (MAC address mana) yang diizinkan terhubung — keduanya bisa dipakai bersamaan untuk lapisan keamanan berlapis.

9.6 Tx-Power, Rx-Sensitivity, dan Data Rate

Tx-Power menentukan daya pancar sinyal wireless — semakin tinggi, jangkauan makin jauh namun berisiko interferensi ke perangkat lain dan melanggar regulasi daya pancar setempat. Rx-Sensitivity menunjukkan seberapa lemah sinyal yang masih bisa diterima dengan baik oleh perangkat penerima. Data Rate menentukan kecepatan modulasi yang dipakai — semakin tinggi data rate yang dipilih, semakin sensitif terhadap kualitas sinyal (mudah drop jika sinyal lemah).

9.7 NV2 — Protokol Wireless Proprietary MikroTik

Standar 802.11 pada dasarnya menggunakan mekanisme CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), di mana setiap perangkat "mendengarkan" dulu sebelum mengirim data untuk menghindari tabrakan (collision). Mekanisme ini bekerja baik untuk jaringan WiFi indoor biasa, namun kurang efisien untuk skenario PTMP outdoor dengan banyak client jarak jauh, karena rentan terhadap masalah hidden node (dua client tidak saling mendengar satu sama lain, namun sama-sama mengirim ke AP yang sama, menyebabkan tabrakan di sisi AP).

NV2 adalah protokol proprietary MikroTik berbasis TDMA (Time Division Multiple Access) yang mengatasi masalah ini dengan cara AP membagikan slot waktu (time slot) khusus kepada setiap client secara terjadwal — setiap client hanya boleh mengirim pada slotnya masing-masing, sehingga tabrakan akibat hidden node dapat dihindari sepenuhnya. Hasilnya adalah throughput yang jauh lebih stabil dan predictable pada jaringan PTMP dengan banyak client dibanding protokol 802.11 standar.

```
/interface wireless set wlan1 mode=ap-bridge wireless-protocol=nv2 nv2-qos=default
```

> **Catatan Kompatibilitas**
> Karena NV2 adalah protokol proprietary, seluruh perangkat dalam satu jaringan PTMP (baik AP maupun seluruh client-nya) harus sama-sama perangkat MikroTik yang mendukung NV2 — tidak dapat digunakan untuk menghubungkan MikroTik dengan perangkat wireless vendor lain.

9.8 Monitoring Tools: Scan, Snooper, dan Registration Table

Tool	Fungsi
Scan (Wireless Scan)	Memindai dan menampilkan seluruh SSID/AP yang terdeteksi di sekitar beserta kekuatan sinyal — dipakai saat site survey awal sebelum menentukan channel operasional
Snooper	Memindai dan menampilkan tingkat pemakaian (utilization) tiap channel/frekuensi secara real-time dari seluruh jaringan wireless di sekitar (bukan hanya SSID MikroTik), membantu mengidentifikasi channel mana yang paling "sepi" dari interferensi sebelum instalasi
Registration Table	Menampilkan daftar client yang sedang terhubung ke Access Point beserta detail kualitas koneksi masing-masing (signal strength, CCQ, tx/rx rate)

Penerapan di Industri — Site Survey Sebelum Instalasi Tower

Sebelum memasang perangkat PTMP baru di sebuah menara, teknisi WISP profesional selalu melakukan site survey menggunakan Snooper untuk memetakan tingkat kepadatan penggunaan spektrum 2.4GHz/5GHz di lokasi tersebut — terutama di area perkotaan padat di mana puluhan RT/RW-net dan ISP kecil beroperasi di frekuensi yang sama. Hasil survey ini menentukan pemilihan channel dan lebar pita (channel width) yang optimal, serta menjadi dasar pertimbangan apakah perlu migrasi ke NV2 atau bahkan ke frekuensi lisensi (licensed spectrum) jika interferensi 2.4/5GHz sudah terlalu parah.

LAB: Point-to-Point Wireless dengan Keamanan WPA2

1. Siapkan dua RouterBOARD wireless (Router A sebagai AP, Router B sebagai Station).

2. Pada Router A, set wlan1 mode=ap bridge, tentukan SSID "LAB-PTP", pilih band dan frequency.

3. Pada Router B, set wlan1 mode=station, pastikan band sama, lalu scan dan connect ke SSID "LAB-PTP".

4. Verifikasi koneksi melalui menu Wireless > Registration Table di sisi AP.

5. Buat Security Profile WPA2-PSK pada kedua router dengan passphrase yang sama, terapkan ke wlan1 masing-masing.

6. Gabungkan wlan1 ke dalam bridge pada masing-masing router, pasang IP address pada bridge.

7. Uji konektivitas end-to-end dengan ping antar kedua router.

Uji Pemahaman

1. Jelaskan perbedaan karakteristik frekuensi 2.4 GHz dan 5 GHz.

2. Apa perbedaan mode "station" dan "station bridge" pada RouterOS?

3. Mengapa site survey penting dilakukan sebelum memasang jaringan PTMP?

4. Jelaskan perbedaan fungsi Access List dan Connect List.

5. Mengapa protokol NV2 lebih unggul dibanding 802.11 standar untuk skenario PTMP dengan banyak client outdoor?

6. Apa perbedaan fungsi antara tool Scan dan Snooper dalam proses site survey wireless?

BAB 10

Firewall dan NAT

Membangun lapisan pertahanan jaringan menggunakan Firewall Filter, memahami connection tracking, serta memahami dua jenis NAT: Source NAT dan Destination NAT.

Tujuan Pembelajaran

Peserta mampu merancang rule firewall filter untuk mengamankan router dan jaringan, memahami connection state, serta mengimplementasikan SRCNAT dan DSTNAT.

10.1 Konsep Firewall RouterOS

Firewall RouterOS bekerja berdasarkan chain (rantai) yang merepresentasikan titik pemeriksaan paket dalam alur trafik jaringan.

Chain	Digunakan untuk trafik
input	Paket yang tujuannya adalah router itu sendiri (misalnya akses Winbox, ping ke router)
forward	Paket yang melewati router menuju perangkat lain (misalnya trafik dari klien LAN ke internet)
output	Paket yang dihasilkan oleh router itu sendiri menuju luar

Setiap rule dievaluasi berurutan dari atas ke bawah. Begitu sebuah paket cocok dengan kondisi suatu rule dan rule tersebut memiliki action yang bersifat final (seperti accept atau drop), proses evaluasi berhenti — rule di bawahnya tidak lagi diperiksa untuk paket tersebut.

10.2 Action Firewall Filter

Action	Perilaku
accept	Mengizinkan paket lewat dan menghentikan pemeriksaan rule berikutnya
drop	Membuang paket tanpa pemberitahuan ke pengirim
reject	Membuang paket dan mengirim pesan penolakan ke pengirim
log	Mencatat informasi paket ke log, lalu tetap melanjutkan ke rule berikutnya
jump	Mengalihkan pemeriksaan ke chain kustom lain

10.3 Mengamankan Router (Chain Input)

```
/ip firewall filter add chain=input connection-state=established,related action=accept
/ip firewall filter add chain=input connection-state=invalid action=drop
```

```
/ip firewall filter add chain=input protocol=icmp action=accept
/ip firewall filter add chain=input in-interface=ether1 action=drop
```

Pola umum firewall input yang baik: izinkan trafik yang sudah dikenal (established/related), buang trafik tidak valid, izinkan ICMP untuk keperluan diagnosa (ping), lalu blokir semua akses masuk lain dari interface publik/WAN sebagai baris terakhir.

10.4 Connection State dan Connection Tracking

RouterOS melacak status setiap koneksi melalui mekanisme connection tracking, yang mengklasifikasikan paket ke dalam beberapa status:

Connection State	Arti
new	Paket pertama dari sebuah koneksi baru
established	Bagian dari koneksi yang sudah terbentuk sebelumnya
related	Terkait dengan koneksi lain yang sudah ada (misalnya paket error ICMP terkait sesi FTP)
invalid	Paket tidak dikenali/tidak sesuai dengan koneksi manapun, umumnya dicurigai berbahaya

FastTrack — Percepatan Trafik

FastTrack adalah mekanisme yang memungkinkan paket dari koneksi yang sudah established/related dilewatkan langsung tanpa perlu diproses ulang oleh seluruh firewall dan connection tracking, sehingga secara signifikan meningkatkan throughput router — terutama penting pada perangkat dengan CPU terbatas.

```
/ip firewall filter add chain=forward connection-state=established,related
action=fasttrack-connection
/ip firewall filter add chain=forward connection-state=established,related action=accept
```

📌 Studi Kasus Nyata — Server Internal "Bocor" ke Internet

Sebuah perusahaan menemukan bahwa server database internal mereka ternyata bisa diakses langsung dari internet oleh siapa saja yang mengetahui IP publiknya — celah ini ditemukan oleh tim keamanan eksternal saat melakukan penetration testing rutin. Investigasi menunjukkan router tidak pernah memiliki rule firewall input yang eksplisit memblokir akses dari luar; router hanya mengandalkan NAT sebagai satu-satunya lapisan pertahanan, padahal untuk trafik yang ditujukan langsung ke router itu sendiri (bukan diteruskan ke klien), NAT tidak relevan. Setelah menerapkan firewall filter chain=input yang eksplisit memblokir seluruh akses dari WAN kecuali yang benar-benar diperlukan, celah tersebut tertutup total tanpa mengganggu layanan yang memang seharusnya publik.

10.5 NAT: Source NAT (SRCNAT) dan Destination NAT (DSTNAT)

Jenis NAT	Fungsi	Contoh Penggunaan
SRCNAT (chain=srcnat)	Mengubah source IP paket saat keluar	Masquerade: LAN privat mengakses internet menggunakan IP publik router
DSTNAT (chain=dstnat)	Mengubah destination IP/port paket saat masuk	Port forwarding: mengarahkan akses dari internet ke server internal (misalnya web server di LAN)

```
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
/ip firewall nat add chain=dstnat protocol=tcp dst-port=80 action=dst-nat to-
addresses=192.168.10.100 to-ports=80
```

10.6 Address List

Address List memungkinkan pengelompokan beberapa IP address ke dalam satu label, yang kemudian dapat dirujuk oleh banyak rule firewall sekaligus — memudahkan pengelolaan dibanding menulis IP satu per satu di setiap rule. Address list juga bisa terbentuk secara dinamis (misalnya menandai IP yang mencoba melakukan serangan berulang) menggunakan parameter address-list dan address-list-timeout pada rule firewall.

```
/ip firewall address-list add list=blocked-ip address=203.0.113.5
/ip firewall filter add chain=input src-address-list=blocked-ip action=drop
```

10.7 Firewall Raw — Filtering Sebelum Connection Tracking

Selain tabel Filter dan NAT, RouterOS menyediakan satu tabel firewall lagi bernama Raw, yang bekerja pada tahap paling awal alur pemrosesan paket — bahkan sebelum proses connection tracking dimulai. Ini membuat Raw sangat efisien untuk dua tujuan utama: mempercepat performa router secara drastis, dan sebagai lapisan pertahanan pertama terhadap serangan volumetrik.

Chain pada Raw	Digunakan untuk
prerouting	Paket yang baru masuk ke router, sebelum routing decision dan sebelum connection tracking
output	Paket yang dihasilkan router itu sendiri, sebelum connection tracking

```
/ip firewall raw add chain=prerouting src-address-list=blocked-ip action=drop
/ip firewall raw add chain=prerouting protocol=tcp psd=21,3s,3,1 action=drop   ; deteksi
port scan sederhana
/ip firewall raw add chain=prerouting connection-state=new connection-state=invalid
action=drop
```

Karena rule di Raw diproses sebelum connection tracking, paket yang di-drop di sini tidak pernah "tercatat" oleh conntrack sama sekali — beban CPU router menjadi jauh lebih ringan dibanding jika paket berbahaya

tersebut baru diblokir di chain Filter biasa (yang berarti paket tersebut sudah sempat diproses connection tracking terlebih dahulu). Inilah sebabnya Raw sangat direkomendasikan untuk memblokir sumber-sumber yang sudah pasti berbahaya (misalnya address-list hasil deteksi serangan) sedini mungkin.

notrack — Mengecualikan dari Connection Tracking

Action "notrack" pada tabel Raw membuat suatu trafik tertentu (misalnya trafik VoIP volume tinggi yang tidak memerlukan NAT/firewall filter kompleks) dilewatkan tanpa dicatat oleh connection tracking sama sekali, mengurangi beban memori dan CPU router pada trafik volume sangat tinggi. Namun perlu diperhatikan bahwa trafik yang di-notrack tidak dapat lagi diproses oleh NAT maupun firewall filter berbasis connection-state.

Penerapan di Industri — Mitigasi DDoS Ringan dengan Raw

ISP dan penyedia hosting skala kecil-menengah sering menggunakan kombinasi Firewall Raw dan address-list dinamis sebagai lini pertahanan pertama terhadap serangan DDoS volumetrik skala kecil-menengah (misalnya SYN flood dari segelintir sumber). Karena diproses sebelum connection tracking, rule Raw mampu menangani volume paket jauh lebih tinggi dibanding rule Filter biasa sebelum CPU router kewalahan — meski untuk serangan DDoS skala besar, mitigasi tetap perlu dilakukan di level upstream/ISP menggunakan layanan scrubbing khusus, bukan hanya mengandalkan router pelanggan.

LAB: Firewall Dasar dan Port Forwarding

1. Buat rule firewall input untuk mengizinkan established/related dan ICMP, lalu blokir sisanya dari interface WAN.

2. Tambahkan rule fasttrack-connection sebelum rule accept established/related di chain forward.

3. Simulasikan sebuah web server sederhana di salah satu klien LAN (bisa menggunakan Python simple HTTP server pada port 8080).

4. Buat rule DSTNAT untuk meneruskan akses dari port 80 di interface WAN menuju port 8080 klien tersebut.

5. Uji akses dari luar (atau simulasikan dari router lain) menuju IP WAN port 80, verifikasi trafik diteruskan ke server internal.

6. Buat address-list berisi satu IP percobaan, lalu buat rule yang memblokir seluruh akses dari IP dalam address-list tersebut. Uji hasilnya.

7. Pindahkan rule pemblokiran address-list tersebut ke tabel Raw (chain=prerouting), bandingkan hasilnya dengan versi di tabel Filter — fungsinya sama, namun jelaskan mengapa versi Raw lebih ringan bagi CPU router.

Uji Pemahaman

1. Jelaskan perbedaan fungsi chain input, forward, dan output pada firewall filter.

2. Mengapa urutan rule firewall sangat menentukan hasil akhir dari pemrosesan paket?

3. Jelaskan perbedaan SRCNAT dan DSTNAT beserta contoh penggunaan masing-masing.

4. Apa manfaat FastTrack terhadap performa router?

5. Jelaskan mengapa rule pada tabel Firewall Raw diproses lebih ringan bagi CPU dibanding rule pada tabel Filter untuk tujuan yang sama.

BAB 11

Quality of Service (QoS)

Mengelola alokasi bandwidth menggunakan Simple Queue dan Queue Tree agar trafik jaringan terdistribusi adil dan sesuai prioritas.

Tujuan Pembelajaran

Peserta mampu mengonfigurasi pembatasan bandwidth dasar, memahami staged limitation, serta menerapkan PCQ untuk pembagian bandwidth yang adil antar pengguna.

11.1 Mengapa QoS Diperlukan

Tanpa pengaturan trafik, satu perangkat dapat menghabiskan seluruh bandwidth yang tersedia (misalnya melalui aktivitas download besar), sehingga mengganggu pengguna lain di jaringan yang sama. QoS (Quality of Service) memastikan bandwidth teralokasi secara terkendali dan adil sesuai kebijakan yang ditetapkan administrator.

11.2 Simple Queue

Simple Queue adalah cara termudah membatasi bandwidth per IP address atau per subnet, mendukung pembatasan terpisah untuk arah upload (target-upload) dan download (target-download).

```
/queue simple add name=limit-klien-01 target=192.168.10.50/32 max-limit=2M/5M
```

Pada contoh di atas, klien dengan IP 192.168.10.50 dibatasi maksimum 2 Mbps untuk upload dan 5 Mbps untuk download (format penulisan: upload/download).

11.3 Custom Destination dan Staged Limitation

Simple Queue juga mendukung target berdasarkan tujuan tertentu (custom destination), misalnya membatasi bandwidth khusus menuju layanan streaming tertentu. Untuk skenario lebih kompleks, staged limitation memungkinkan pembuatan queue bertingkat (parent-child), di mana sebuah "parent queue" membatasi total bandwidth suatu grup, sementara "child queue" di bawahnya membagi alokasi tersebut ke masing-masing anggota grup — sering dipakai untuk membagi bandwidth per divisi/kelas sekaligus membatasi total pemakaian keseluruhan.

11.4 Priority pada Queue

Setiap queue dapat diberi nilai priority (1 = prioritas tertinggi, 8 = terendah). Saat bandwidth mendekati batas total yang tersedia, queue dengan priority lebih tinggi akan diistimewakan mendapat alokasi sisa bandwidth (burst) dibanding queue dengan priority lebih rendah.

11.5 PCQ (Per Connection Queue)

PCQ adalah metode antrian yang membagi bandwidth secara otomatis dan adil di antara banyak koneksi/klien tanpa perlu membuat rule Simple Queue satu per satu untuk tiap klien. PCQ mengklasifikasikan trafik berdasarkan sub-stream (misalnya berdasarkan src-address untuk arah upload, atau dst-address untuk arah download), lalu membagi bandwidth yang tersedia secara merata di antara

sub-stream aktif — jika hanya ada satu klien aktif, klien tersebut mendapat seluruh bandwidth; begitu klien lain aktif, bandwidth otomatis terbagi secara adil.

```
/queue type add name=pcq-upload kind=pcq pcq-classifier=src-address pcq-rate=0
/queue type add name=pcq-download kind=pcq pcq-classifier=dst-address pcq-rate=0
/queue simple add name=pcq-semua-klien target=192.168.10.0/24 queue=pcq-upload/pcq-
download max-limit=10M/20M
```

Kunci PCQ

pcq-rate=0 berarti tidak ada batas per klien secara individual — bandwidth dibagi secara dinamis dan proporsional tergantung jumlah klien yang sedang aktif menggunakan jaringan pada saat itu.

11.6 Tools Monitoring: Graph dan Bandwidth Test

- Tools > Graphing — menyimpan riwayat penggunaan trafik interface dan queue dalam bentuk grafik yang dapat diakses melalui web.
- Bandwidth Test (Btest) — mengukur kapasitas throughput riil antar dua perangkat MikroTik, berguna untuk menguji kapasitas link sebelum menentukan batas queue yang realistis.

11.6 Queue Tree — Kontrol Bandwidth Tingkat Lanjut

Jika Simple Queue cukup untuk kebutuhan pembatasan per-IP yang sederhana, Queue Tree menawarkan kontrol jauh lebih fleksibel dan powerful, terutama untuk skenario hierarki bandwidth yang kompleks (misalnya membagi total bandwidth ke banyak level: per gedung, per lantai, per divisi, per user) atau saat perlu memisahkan prioritas berdasarkan jenis trafik (misalnya trafik VoIP diprioritaskan di atas trafik browsing biasa) lintas banyak klien sekaligus.

Aspek	Simple Queue	Queue Tree
Kemudahan konfigurasi	Sangat mudah, satu rule mencakup upload & download sekaligus	Lebih kompleks, perlu memisahkan arah upload dan download ke tree terpisah
Fleksibilitas hierarki	Terbatas (parent-child sederhana)	Sangat fleksibel, mendukung hierarki bertingkat-tingkat
Kebutuhan mangle	Umumnya tidak wajib	Wajib menandai trafik dengan mangle (packet-mark) terlebih dahulu sebelum bisa di-queue
Kasus penggunaan umum	Pembatasan sederhana per klien/subnet	ISP/WISP skala besar, prioritas jenis trafik, QoS kompleks

Karena Queue Tree hanya bekerja pada satu arah (searah dengan posisinya pada chain global-in atau global-out), penerapannya selalu diawali dengan menandai paket menggunakan mangle terlebih dahulu.

```
; Langkah 1: Tandai trafik dengan mangle
/ip firewall mangle add chain=forward src-address=192.168.10.0/24 action=mark-packet
new-packet-mark=upload-lan passthrough=yes
/ip firewall mangle add chain=forward dst-address=192.168.10.0/24 action=mark-packet
new-packet-mark=download-lan passthrough=yes
```

```
; Langkah 2: Buat Queue Tree berdasarkan packet-mark
/queue tree add name=total-upload parent=ether1 max-limit=10M
/queue tree add name=lan-upload parent=total-upload packet-mark=upload-lan max-limit=10M
/queue tree add name=total-download parent=ether2 max-limit=50M
/queue tree add name=lan-download parent=total-download packet-mark=download-lan max-
limit=50M
```

Konsep parent pada Queue Tree

Parameter "parent" pada Queue Tree bisa merujuk ke sebuah interface fisik (sebagai batas total keluar/masuk interface tersebut) atau merujuk ke queue lain yang sudah dibuat sebelumnya (membentuk hierarki bertingkat). Total limit pada child queue tidak boleh melebihi limit milik parent-nya, karena parent berfungsi sebagai "wadah" pembatas keseluruhan.

Penerapan di Industri — Queue Tree di ISP/WISP Produksi

ISP dan WISP hampir selalu menggunakan Queue Tree (bukan Simple Queue) di router core/distribusi mereka, karena perlu mengatur hierarki bandwidth bertingkat: total bandwidth upstream dari NAP/IIX, dibagi per OLT/sektor, dibagi lagi per paket layanan pelanggan (misalnya paket 10Mbps vs 50Mbps), dengan prioritas tambahan untuk trafik real-time seperti VoIP dan gaming di atas trafik download/streaming biasa. Kombinasi mangle + Queue Tree + PCQ inilah yang menjadi fondasi sistem billing dan bandwidth management di hampir seluruh ISP berbasis MikroTik di Indonesia.

Studi Kasus Nyata — Satu Pengguna "Menyedot" Seluruh Bandwidth Kos

Sebuah rumah kos dengan 15 kamar berbagi satu koneksi internet 50Mbps tanpa pembatasan bandwidth apa pun. Salah satu penghuni yang gemar mengunduh file torrent berukuran besar tanpa disadari menghabiskan hampir seluruh bandwidth setiap malam, membuat penghuni lain tidak bisa video call atau streaming sama sekali di jam tersebut, memicu keluhan berulang ke pemilik kos. Setelah pemilik memasang RouterBOARD dan menerapkan PCQ agar bandwidth otomatis terbagi rata di antara seluruh IP aktif, keluhan tersebut langsung hilang — penghuni yang mengunduh besar tetap bisa berjalan, namun kini dibatasi otomatis begitu penghuni lain mulai menggunakan jaringan, tanpa perlu pemilik kos memantau atau menegur siapa pun secara manual.

LAB: Pembatasan Bandwidth dengan Simple Queue dan PCQ

1. Buat Simple Queue untuk satu IP klien tertentu dengan batas 1M/2M (upload/download), uji menggunakan speedtest atau download file besar.

2. Hapus rule tersebut, lalu buat dua Queue Type PCQ (upload berbasis src-address, download berbasis dst-address).

3. Terapkan kedua Queue Type PCQ tersebut pada satu Simple Queue yang menargetkan seluruh subnet LAN dengan total limit 10M/20M.

4. Hubungkan minimal dua klien, uji unduhan bersamaan, amati apakah bandwidth terbagi secara adil melalui menu Queue > Simple Queue (lihat statistik tab).

5. Diskusikan: apa yang terjadi pada alokasi bandwidth tiap klien saat jumlah klien aktif bertambah?

6. Sebagai perbandingan, buat versi Queue Tree untuk skenario yang sama: tandai trafik LAN dengan mangle packet-mark, lalu buat queue tree dengan parent=ether1 (upload) dan parent=ether2 (download). Bandingkan kompleksitas konfigurasi antara Simple Queue dan Queue Tree untuk hasil akhir yang serupa.

☑ Uji Pemahaman

1. Jelaskan perbedaan antara parent queue dan child queue pada staged limitation.

2. Bagaimana priority memengaruhi alokasi bandwidth saat kondisi jaringan padat?

3. Jelaskan cara kerja PCQ dalam membagi bandwidth secara adil antar klien.

4. Mengapa pcq-rate=0 sering digunakan dalam skenario pembagian bandwidth publik/umum?

5. Jelaskan mengapa Queue Tree wajib didahului oleh rule mangle, berbeda dengan Simple Queue.

BAB 12

VPN Dasar (PPTP, SSTP, PPPoE)

Mempelajari konsep tunneling dasar dan implementasi tiga jenis VPN paling umum di level MTCNA: PPTP, SSTP, dan PPPoE.

Tujuan Pembelajaran

Peserta memahami konsep dasar VPN, mampu mengonfigurasi server dan client PPTP serta SSTP, serta memahami penggunaan PPPoE sebagai metode autentikasi koneksi pelanggan.

12.1 Apa itu VPN?

VPN (Virtual Private Network) membentuk jalur komunikasi terenkripsi (tunnel) antara dua titik melalui jaringan publik seperti internet, seolah-olah kedua titik tersebut terhubung langsung dalam jaringan privat yang sama. VPN umum digunakan untuk menghubungkan kantor cabang, mengakses jaringan kantor dari luar secara aman, atau menyediakan layanan koneksi pelanggan (seperti PPPoE pada ISP).

12.2 PPTP (Point-to-Point Tunneling Protocol)

PPTP adalah salah satu protokol VPN tertua dan paling ringan secara komputasi, mudah dikonfigurasi, namun dianggap memiliki tingkat keamanan enkripsi yang lebih lemah dibanding protokol VPN modern seperti SSTP atau IPSec. PPTP tetap relevan dipelajari di MTCNA karena kesederhanaannya sebagai pengantar konsep tunneling.

```
/interface pptp-server server set enabled=yes
/ppp secret add name=user1 password=Passw0rd! service=pptp local-address=10.10.10.1
remote-address=10.10.10.2

; Sisi Client:
/interface pptp-client add name=pptp-out1 connect-to=203.0.113.1 user=user1
password=Passw0rd!
```

12.3 SSTP (Secure Socket Tunneling Protocol)

SSTP membungkus trafik VPN melalui koneksi HTTPS (port 443), sehingga cenderung lebih mudah menembus firewall/NAT restriktif dibanding PPTP, sekaligus menawarkan enkripsi yang lebih kuat berbasis SSL/TLS.

```
/interface sstp-server server set enabled=yes certificate=cert-router
/ppp secret add name=user2 password=Passw0rd! service=sstp

; Sisi Client:
/interface sstp-client add name=sstp-out1 connect-to=203.0.113.1 user=user2
password=Passw0rd!
```

12.4 PPPoE (Point-to-Point Protocol over Ethernet)

PPPoE banyak digunakan oleh ISP untuk mengautentikasi pelanggan sebelum memberikan akses internet — pelanggan memasukkan username dan password pada perangkat mereka (router rumahan atau langsung di komputer) untuk membentuk sesi PPPoE menuju server ISP.

```
/interface pppoe-server server add interface=ether2 service-name=internet-sekolah
disabled=no
/ppp secret add name=siswa01 password=Passw0rd! service=pppoe local-address=10.20.20.1
remote-address=10.20.20.2

; Sisi Client:
/interface pppoe-client add interface=ether1 user=siswa01 password=Passw0rd!
```

📌 Studi Kasus Nyata — Kerja Remote Aman Saat Pandemi

Ketika sebuah perusahaan diharuskan menerapkan kerja dari rumah secara mendadak, tim IT mereka perlu memberikan akses aman ke server internal (database, file share, aplikasi internal) tanpa mengekspos server tersebut langsung ke internet. Dengan mengaktifkan PPTP Server (kemudian ditingkatkan ke SSTP karena lebih aman) di router kantor dan membuat akun PPP Secret untuk tiap karyawan, seluruh staf dapat "seolah-olah" berada di jaringan kantor begitu terhubung VPN dari rumah masing-masing — mengakses seluruh resource internal dengan aman tanpa perlu membuka satu pun port berbahaya ke internet publik.

12.5 PPP Profile dan PPP Secret

Baik PPTP, SSTP, maupun PPPoE sama-sama memanfaatkan sistem PPP (Point-to-Point Protocol) di baliknya, sehingga pengaturan user (PPP Secret) dan kebijakan koneksi (PPP Profile) bersifat terpusat dan dapat dipakai bersama oleh ketiga jenis VPN tersebut.

Komponen	Fungsi
PPP Profile	Menentukan kebijakan koneksi: rentang IP lokal/remote, DNS yang diberikan, batas kecepatan (rate-limit), dsb
PPP Secret	Menyimpan kredensial (username/password) tiap pengguna beserta profile yang digunakan
IP Pool untuk VPN	Rentang IP address yang dialokasikan secara dinamis ke client yang terhubung, mirip konsep IP Pool pada DHCP

```
/ppp profile add name=profile-siswa local-address=10.20.20.1 remote-address=pool-vpn-
siswa dns-server=8.8.8.8 rate-limit=1M/2M
```

🔧 LAB: Membangun PPTP Server dan Client

1. Pada Router Server, aktifkan PPTP server melalui menu Interface > PPTP Server.

2. Buat PPP Profile dengan local-address dan pool remote-address tersendiri.

3. Buat PPP Secret untuk satu user percobaan, kaitkan dengan profile yang telah dibuat, dan tentukan service=pptp.

4. Pada Router Client, buat interface PPTP Client mengarah ke IP publik/WAN Router Server, isi user dan password yang sesuai.

5. Verifikasi status koneksi melalui menu Interface (pastikan status "R" — running) pada kedua sisi.

6. Uji ping dari Client menuju local-address Server melalui tunnel PPTP yang baru terbentuk, dan amati tabel routing untuk melihat rute otomatis yang terbentuk.

Penerapan di Industri — PPPoE sebagai Tulang Punggung ISP Fiber/Kabel

Hampir seluruh ISP fiber-to-the-home (FTTH) dan ISP kabel di Indonesia menggunakan PPPoE sebagai metode autentikasi pelanggan standar, karena memudahkan kontrol akses (memutus layanan otomatis saat tagihan menunggak, cukup menonaktifkan PPP Secret pelanggan bersangkutan) dan memungkinkan pelanggan berpindah lokasi fisik tanpa mengubah kredensial. Untuk skala ribuan pelanggan, PPP Secret hampir selalu diintegrasikan dengan server RADIUS eksternal (bukan disimpan lokal di router) agar dapat terhubung langsung ke sistem billing ISP — begitu pelanggan bayar, sistem billing otomatis mengaktifkan kembali akun via API RADIUS tanpa perlu login manual ke router.

Uji Pemahaman

1. Jelaskan konsep dasar VPN dan mengapa enkripsi menjadi bagian pentingnya.

2. Apa kelebihan SSTP dibanding PPTP dalam hal menembus firewall/NAT?

3. Jelaskan mengapa PPPoE umum dipakai oleh ISP untuk autentikasi pelanggan.

4. Bagaimana hubungan antara PPP Profile dan PPP Secret dalam konfigurasi VPN berbasis PPP?

BAB 13

SuperLab MTCNA — Proyek Akhir Terintegrasi

Satu skenario jaringan utuh yang menggabungkan LITERALLY seluruh materi Bab 1-12 secara bertahap (multi-fase), dirancang agar peserta benar-benar merasakan bagaimana seluruh fitur RouterOS bekerja bersama dalam satu sistem nyata — bukan sekadar latihan terpisah per topik.

Tujuan Pembelajaran

Peserta mampu merancang, membangun, mengamankan, dan mendokumentasikan sebuah jaringan kantor/sekolah kecil secara end-to-end menggunakan seluruh kompetensi MTCNA, serta siap menghadapi ujian sertifikasi MTCNA (25 soal pilihan ganda, 60 menit).

13.1 Latar Belakang SuperLab

SMK Teknik Jaringan "Nusantara Digital" baru saja membangun gedung baru dengan 3 lantai: Lantai 1 (Ruang Guru & TU), Lantai 2 (Lab Komputer TJKT), dan Lantai 3 (Area WiFi Tamu/Perpustakaan). Sekolah memiliki satu koneksi internet dari ISP, dan menunjuk Anda sebagai teknisi jaringan untuk merancang seluruh infrastruktur dari nol. Kepala sekolah memberikan daftar kebutuhan yang harus dipenuhi — inilah yang akan Anda kerjakan sepanjang SuperLab ini.

No	Kebutuhan Kepala Sekolah	Bab Terkait
1	Router harus terpasang dengan RouterOS versi terbaru dan diberi nama identitas sekolah	Bab 2
2	Koneksi ke ISP otomatis (DHCP Client) dan seluruh ruangan bisa akses internet	Bab 3
3	Tiap lantai punya jaringan sendiri dengan DHCP Server otomatis	Bab 4
4	Ada backup konfigurasi terjadwal agar tidak kehilangan setting jika router rusak	Bab 5
5	Router harus aman dari akses tidak sah, terutama karena terpasang di ruangan yang bisa diakses siapa saja	Bab 6
6	Jika koneksi ISP utama mati, harus ada jalur cadangan otomatis (sekolah punya modem 4G cadangan)	Bab 7
7	Lab Komputer perlu 2 switch tambahan yang digabung jadi satu jaringan tanpa masalah loop	Bab 8
8	Area Perpustakaan perlu WiFi dengan keamanan WPA2, terpisah dari jaringan guru	Bab 9

No	Kebutuhan Kepala Sekolah	Bab Terkait
9	WiFi Tamu tidak boleh bisa mengakses jaringan Ruang Guru maupun server sekolah	Bab 10
10	Lab Komputer sering dipakai untuk download tugas besar — jangan sampai menghabiskan seluruh bandwidth sekolah	Bab 11
11	Guru piket kadang perlu akses ke sistem sekolah dari rumah pada malam hari	Bab 12

13.2 Denah Alamat IP (IP Addressing Plan)

Sebelum mengetik satu perintah pun, rancang dahulu denah pengalamatan IP di atas kertas/spreadsheet — kebiasaan ini adalah standar profesional yang mencegah kekacauan saat jaringan mulai kompleks.

Segmen	Subnet	Gateway	Keterangan
WAN (ISP)	DHCP Client	-	Interface ether1
WAN Cadangan (4G)	DHCP Client	-	Interface ether2, distance=2
LAN Ruang Guru	192.168.10.0/24	192.168.10.1	Interface ether3 / bridge-guru
LAN Lab Komputer	192.168.20.0/24	192.168.20.1	Interface bridge-lab (ether4+ether5, hasil gabungan 2 switch)
WiFi Tamu/Perpustakaan	192.168.30.0/24	192.168.30.1	Interface wlan1 + bridge-tamu
VPN Guru Piket	192.168.40.0/24	192.168.40.1	PPTP/SSTP Server, pool 192.168.40.10-40.50

13.3 Fase Pengerjaan SuperLab

SuperLab dikerjakan dalam 8 fase berurutan. Setiap fase HARUS diverifikasi berhasil sebelum lanjut ke fase berikutnya — ini melatih kebiasaan validasi bertahap yang sangat penting dalam pekerjaan nyata, di mana kesalahan pada fase awal dapat menyebabkan efek berantai yang sulit dilacak di fase-fase selanjutnya.

LAB: FASE 1 — Instalasi & Fondasi Router (Bab 2)

1. Lakukan Netinstall pada RouterBOARD untuk memastikan kondisi bersih (default), catat versi RouterOS yang terpasang.

2. Set identity router menjadi "SMK-NusantaraDigital-Core".

3. Buat user administrator baru dengan nama unik dan password kuat, group=full.

4. Verifikasi: login menggunakan user baru berhasil, dan "/system resource print" menampilkan versi RouterOS serta arsitektur perangkat.

LAB: FASE 2 — Koneksi Internet Dasar & NAT (Bab 3)

1. Set ether1 sebagai DHCP Client (WAN utama dari ISP).

2. Pasang IP address 192.168.10.1/24 pada interface LAN Ruang Guru (sementara langsung di ether3 dahulu, akan disesuaikan setelah bridge dibuat di Fase 5).

3. Set DNS server 8.8.8.8 dan 1.1.1.1 dengan allow-remote-requests=yes.

4. Tambahkan rule NAT masquerade untuk ether1.

5. Verifikasi: dari laptop yang terhubung ke ether3, ping ke 8.8.8.8 dan ke google.com berhasil.

LAB: FASE 3 — DHCP Server per Segmen (Bab 4)

1. Buat IP Pool dan DHCP Server untuk Ruang Guru (192.168.10.0/24), Lab Komputer (192.168.20.0/24), dan WiFi Tamu (192.168.30.0/24) — meski interface fisiknya baru benar-benar terpasang di fase berikutnya, konfigurasikan objeknya terlebih dahulu.

2. Buat static lease untuk satu perangkat "server" simulasi di Ruang Guru (misalnya sebuah laptop yang akan berperan sebagai server aplikasi sekolah) agar selalu mendapat IP 192.168.10.50.

3. Verifikasi: "/ip dhcp-server print" menampilkan tiga DHCP server berbeda, masing-masing berstatus aktif.

LAB: FASE 4 — Backup Awal Sebagai Titik Aman (Bab 5)

1. Lakukan backup dan export konfigurasi saat ini, beri nama "superlab-fase4-selesai".

2. Simpan file tersebut di luar router (unduh ke laptop Anda) sebagai titik pemulihan jika terjadi kesalahan fatal di fase-fase berikutnya.

3. Diskusikan dengan instruktur: mengapa kebiasaan backup bertahap seperti ini penting dalam pekerjaan nyata, bukan hanya backup di akhir proyek?

LAB: FASE 5 — Bridging Lab Komputer & Keamanan Router (Bab 6, Bab 8)

1. Buat bridge-lab, gabungkan ether4 dan ether5 ke dalamnya (mensimulasikan 2 switch yang digabung).

2. Aktifkan RSTP pada bridge-lab untuk mencegah masalah loop.

3. Pasang IP address 192.168.20.1/24 pada bridge-lab (bukan pada ether4/ether5 individual).

4. Buat bridge-guru, gabungkan ether3, pasang IP 192.168.10.1/24 di sana (pindahkan dari Fase 2).

5. Terapkan hardening keamanan: nonaktifkan user admin default, matikan Telnet/FTP, batasi Winbox hanya dari 192.168.10.0/24 (subnet Ruang Guru, dianggap sebagai jaringan admin).

6. Verifikasi: laptop di ether4 dan ether5 saling ping (satu broadcast domain), dan winbox tidak lagi bisa diakses dari subnet lain.

LAB: FASE 6 — Failover Internet & Wireless Tamu (Bab 7, Bab 9)

1. Set ether2 sebagai DHCP Client kedua (mensimulasikan modem 4G), tambahkan static route default distance=2 dengan check-gateway=ping (distance=1 pada rute dari ether1 DHCP Client sudah otomatis).

2. Konfigurasikan wlan1 sebagai Access Point, SSID "SMK-NusantaraDigital-Tamu", buat Security Profile WPA2-PSK.

3. Buat bridge-tamu, gabungkan wlan1 ke dalamnya, pasang IP 192.168.30.1/24.

4. Verifikasi failover: putuskan ether1 secara sengaja, amati "/ip route print" — rute default harus berpindah otomatis ke ether2.

5. Verifikasi WiFi: hubungkan HP ke SSID tamu, pastikan mendapat IP dari DHCP Server WiFi Tamu (dari Fase 3) dan bisa browsing internet.

LAB: FASE 7 — Isolasi Firewall & Kontrol Bandwidth (Bab 10, Bab 11)

1. Buat firewall filter chain=forward yang memblokir trafik dari 192.168.30.0/24 (WiFi Tamu) menuju 192.168.10.0/24 dan 192.168.20.0/24 (isolasi jaringan internal).

2. Pastikan rule isolasi tersebut diletakkan SEBELUM rule accept umum lainnya di chain forward (ingat: urutan rule menentukan hasil).

3. Buat Queue Type PCQ untuk upload dan download, terapkan pada Simple Queue yang menargetkan 192.168.20.0/24 (Lab Komputer) dengan total limit 20M/40M.

4. Verifikasi isolasi: dari HP yang terhubung ke WiFi Tamu, coba ping ke 192.168.10.50 (server simulasi) — harus gagal/timeout.

5. Verifikasi queue: unduh file besar dari dua laptop berbeda di Lab Komputer secara bersamaan, amati pembagian bandwidth melalui tab Traffic pada Simple Queue.

LAB: FASE 8 — VPN Akses Malam Hari & Dokumentasi Akhir (Bab 12)

1. Aktifkan PPTP Server, buat PPP Profile dengan local-address 192.168.40.1 dan pool remote-address 192.168.40.10-192.168.40.50.

2. Buat PPP Secret untuk akun "guru_piket" dengan service=pptp.

3. Dari perangkat di luar jaringan sekolah (simulasikan dengan hotspot HP terpisah), hubungkan VPN PPTP menggunakan akun tersebut, verifikasi dapat ping ke server simulasi di 192.168.10.50 melalui tunnel.

4. Lakukan backup dan export final, beri nama "superlab-final-selesai".

5. Susun dokumentasi akhir berisi: topologi jaringan (gambar), IP addressing plan, daftar seluruh rule firewall beserta alasannya, dan hasil pengujian tiap fase — inilah yang di dunia kerja disebut Network Documentation, dokumen wajib yang harus diserahkan setelah proyek instalasi jaringan selesai.

13.4 Checklist Verifikasi Akhir SuperLab

Verifikasi	Status yang Diharapkan
Ping dari Ruang Guru ke internet	Berhasil
Ping dari Lab Komputer ke internet	Berhasil, bandwidth otomatis terbagi jika ada >1 klien aktif
Ping dari WiFi Tamu ke internet	Berhasil
Ping dari WiFi Tamu ke server Ruang Guru (192.168.10.50)	GAGAL (terisolasi oleh firewall)
Winbox diakses dari subnet Lab Komputer/Tamu	GAGAL (dibatasi hanya dari Ruang Guru)
Internet tetap jalan saat ether1 diputus	Berhasil (failover ke ether2)
VPN PPTP dari luar jaringan berhasil terhubung dan ping ke server internal	Berhasil
File backup & export tersimpan di luar router	Tersedia dan dapat di-restore

Penerapan di Industri — SuperLab sebagai Simulasi Proyek Nyata

Struktur SuperLab ini sengaja meniru alur kerja nyata seorang Network Engineer/Technician: menerima daftar kebutuhan dari klien (bukan spesifikasi teknis siap pakai), merancang IP addressing plan sebelum eksekusi, mengerjakan bertahap dengan validasi tiap tahap, dan menutup proyek dengan dokumentasi lengkap. Kemampuan menerjemahkan kebutuhan bisnis/non-teknis (seperti permintaan kepala sekolah) menjadi konfigurasi teknis yang tepat adalah keterampilan yang membedakan teknisi junior dengan teknisi yang benar-benar siap kerja — dan inilah yang coba dilatih melalui SuperLab ini, bukan sekadar menghafal perintah CLI secara terpisah-pisah.

13.5 Ringkasan Perintah Penting per Bab

Bab	Perintah Kunci
2 - Instalasi & Manajemen	/system identity, /system package, /system resource print, /system routerboard upgrade
3 - Konfigurasi Dasar	/ip address, /ip route, /ip dns, /ip firewall nat (masquerade)
4 - DHCP	/ip pool, /ip dhcp-server, /ip dhcp-server lease
5 - Backup/Export	/system backup save|load, /export, /import
6 - Keamanan Dasar	/user, /ip service, /ip neighbor
7 - Routing Dasar	/ip route (dengan check-gateway), /tool netwatch, /tool traceroute
8 - Bridging	/interface bridge, /interface bridge port
9 - Wireless	/interface wireless, /interface wireless security-profiles, wireless-protocol=nv2

Bab	Perintah Kunci
10 - Firewall & NAT	/ip firewall filter, /ip firewall nat, /ip firewall raw, /ip firewall address-list
11 - QoS	/queue simple, /queue type (pcq), /queue tree
12 - VPN Dasar	/interface pptp-server, /interface sstp-server, /ppp secret, /ppp profile

13.6 Latihan Soal Bergaya Ujian MTCNA

✓ Uji Pemahaman

1. Sebuah router memiliki dua rute default dengan distance 1 dan distance 2 menuju gateway berbeda. Rute manakah yang akan digunakan router selama gateway distance 1 tersedia?

2. Manakah action firewall yang membuang paket TANPA mengirimkan notifikasi apa pun ke pengirim: accept, drop, atau reject?

3. Pada konfigurasi NAT, chain apa yang digunakan untuk membuat rule masquerade?

4. Jika sebuah interface digabungkan ke dalam bridge, di manakah sebaiknya IP address dipasang: pada interface fisik atau pada interface bridge?

5. Apa perbedaan mendasar antara Security Profile dan Access List pada konfigurasi wireless?

6. Fitur apa yang digunakan agar router secara otomatis berpindah ke gateway cadangan saat gateway utama tidak merespons ping?

7. Manakah connection-state yang menunjukkan paket pertama dari sebuah koneksi baru: new, established, atau related?

8. Pada Queue Type PCQ, apa arti dari pcq-rate=0?

9. Layanan manajemen apa yang sebaiknya dinonaktifkan karena tidak mengenkripsi trafiknya: SSH atau Telnet?

10. Protokol VPN mana yang membungkus trafik melalui port 443 (HTTPS) sehingga lebih mudah menembus firewall restriktif: PPTP atau SSTP?

11. Rule pada tabel firewall manakah yang diproses paling awal, sebelum connection tracking dimulai: Filter atau Raw?

12. Pada Queue Tree, komponen apa yang wajib dikonfigurasi terlebih dahulu sebelum queue dapat mengenali trafik yang harus dibatasi?

13. Protokol wireless proprietary MikroTik berbasis TDMA yang mengatasi masalah hidden node pada jaringan PTMP disebut apa?

14. Apa perbedaan antara upgrade paket RouterOS dan upgrade RouterBOOT?

15. Dalam SuperLab, mengapa rule isolasi WiFi Tamu harus diletakkan sebelum rule accept umum lainnya di chain forward?

Tips Menghadapi Ujian Resmi

Ujian MTCNA berupa 25 soal pilihan ganda dalam 60 menit dengan nilai kelulusan minimum sekitar 60%. Fokuskan belajar pada pemahaman konsep "mengapa" suatu fitur bekerja, bukan sekadar menghafal perintah CLI, karena soal ujian sering menguji pemahaman skenario (studi kasus singkat)

dibanding sekadar sintaks perintah. Mengerjakan ulang SuperLab dari nol tanpa melihat catatan adalah cara terbaik menguji kesiapan Anda sebelum ujian sesungguhnya.

13.7 Langkah Selanjutnya

Setelah menguasai seluruh materi buku ini, lulus SuperLab, dan lulus sertifikasi MTCNA, jalur belajar berikutnya yang paling relevan adalah MTCRE (MikroTik Certified Routing Engineer), yang membahas routing lanjutan, OSPF, VPN tingkat lanjut, VLAN, hingga pengantar BGP dan MPLS — dibahas secara mendalam pada buku kedua dari seri ini, lengkap dengan SuperLab tersendiri yang menyatukan seluruh materi routing lanjutan tersebut.