BUKU MATERI TJKT — KELAS XI

MTCRE

MikroTik Certified Routing Engineer Routing Lanjutan, OSPF, VPN & Pengantar BGP/MPLS

Disusun untuk Mata Pelajaran Administrasi Sistem Jaringan & Keamanan Jaringan

Kompetensi Keahlian Teknik Jaringan Komputer dan Telekomunikasi (TJKT)

Yusuf Burhani, S.Kom., S.Pd

Kata Pengantar

Buku ini merupakan kelanjutan dari Buku MTCNA, disusun bagi peserta didik yang telah menguasai konsep jaringan dasar MikroTik dan siap mendalami routing tingkat lanjut setara jenjang sertifikasi MTCRE (MikroTik Certified Routing Engineer).

Materi disusun mulai dari static routing lanjutan dan policy routing, load balancing multi-ISP, tunneling (IPIP/EoIP/GRE), VPN lanjutan (L2TP/IPSec), VLAN, hingga protokol routing dinamis OSPF secara mendalam mulai dari konsep dasar hingga multi-area. Sebagai pengayaan, buku ini juga menyertakan pengantar BGP dan MPLS sebagai jembatan menuju jenjang sertifikasi MTCINE.

Setiap bab dilengkapi kotak LAB berisi praktikum langkah-demi-langkah yang dapat disimulasikan menggunakan RouterBOARD fisik maupun virtual (CHR) di laboratorium sekolah, serta soal uji pemahaman untuk mengukur penguasaan materi.

Buku ini disusun berdasarkan sintesis dari materi resmi pelatihan MikroTik serta praktik industri jaringan skala menengah-besar. Selamat mendalami dunia routing, dan semoga sukses menempuh sertifikasi MTCRE.

Daftar Isi

BAB 1

Pengantar Routing Lanjutan

Menjembatani pemahaman routing dasar (MTCNA) menuju konsep routing lanjutan yang menjadi fondasi materi MTCRE.

Tujuan Pembelajaran

Peserta memahami komponen RIB/FIB, konsep routing table lanjutan, serta gambaran umum materi yang akan dipelajari sepanjang buku MTCRE ini.

1.1 Dari MTCNA ke MTCRE

Buku MTCNA telah membahas static routing dasar: menambahkan rute manual, memahami flag pada tabel routing, serta mekanisme failover sederhana melalui check-gateway. Buku MTCRE (MikroTik Certified Routing Engineer) ini melanjutkan pembahasan tersebut ke tingkat yang jauh lebih dalam: routing policy, load balancing sejati, tunneling, VLAN, hingga protokol routing dinamis OSPF — dengan pengantar BGP dan MPLS sebagai bab pengayaan.

1.2 RIB dan FIB

Dua istilah penting yang mendasari cara kerja router modern:

Istilah	Kepanjangan	Fungsi
RIB	Routing Information Base	Basis data seluruh rute yang diketahui router — dari static, connected, maupun dinamis (OSPF, BGP) — sebelum proses seleksi rute terbaik
FIB	Forwarding Information Base	Rute-rute terbaik yang telah dipilih dari RIB dan benar-benar digunakan router untuk meneruskan paket (inilah yang tampil pada /ip route print dengan flag Active)

Sebuah router bisa saja memiliki banyak entri RIB menuju tujuan yang sama (misalnya dari static route dan OSPF sekaligus), namun hanya satu (atau beberapa jika ECMP) yang akhirnya masuk ke FIB dan benar-benar dipakai, berdasarkan nilai distance dan metric terbaik.

1.3 Routing Mark dan Routing Table Tambahan

RouterOS mendukung pembuatan routing table tambahan di luar tabel utama (main), memungkinkan sekelompok trafik tertentu memiliki jalur routing sendiri yang terpisah dari trafik lainnya — konsep inilah yang menjadi dasar Policy Based Routing yang dibahas mendalam pada bab berikutnya.

Studi Kasus Nyata — Rute "Hantu" yang Bikin Bingung Tim IT

Tim IT sebuah perusahaan multi-cabang kebingungan karena trafik ke salah satu cabang terkadang lewat jalur cepat (link fiber langsung), namun sesekali malah lewat jalur lambat (backup VPN) padahal

link fiber terlihat baik-baik saja di monitoring. Setelah diselidiki menggunakan "/ip route print" dan memeriksa RIB secara detail, ditemukan ada static route lama dengan distance lebih kecil yang sengaja dibuat teknisi sebelumnya untuk keperluan testing sementara, namun tidak pernah dihapus — rute tersebut sesekali "menang" di FIB saat kondisi tertentu terpenuhi. Kejadian ini menjadi pengingat penting bahwa memahami perbedaan RIB (semua kemungkinan rute) dan FIB (rute yang benar-benar dipakai) sangat krusial untuk troubleshooting masalah routing yang tampak "acak".

1.4 Peta Materi Buku MTCRE

Bab	Topik
2	Static Routing Lanjutan & Policy Routing
3	Load Balancing (ECMP, PCC, NTH)
4	Tunnel Dasar (IPIP, EoIP, GRE)
5	VPN Lanjutan (L2TP, PPPoE mendalam, IPSec)
6	VLAN & 802.1Q, QinQ
7	OSPF Fundamentals
8	OSPF Lanjutan (area types, redistribusi, filtering)
9	Pengenalan BGP (pengayaan)
10	Pengenalan MPLS (pengayaan)
11	Lab Komprehensif & Persiapan Ujian MTCRE

Penerapan di Industri — Dari MTCNA ke Dunia Kerja Routing

Posisi Network Engineer di ISP menengah-besar, Data Center, maupun perusahaan multi-cabang hampir selalu mensyaratkan pemahaman mendalam tentang RIB/FIB dan cara kerja route selection, karena troubleshooting masalah konektivitas skala besar sering kali berakar dari kesalahpahaman tentang rute mana yang sebenarnya aktif di FIB versus yang hanya tersimpan di RIB. Sertifikasi MTCRE menjadi pembeda signifikan antara level "network technician" (mampu instalasi & konfigurasi dasar) dengan level "network engineer" (mampu merancang arsitektur routing kompleks) di banyak struktur organisasi IT.

Uji Pemahaman

1. Jelaskan perbedaan antara RIB dan FIB.

2. Mengapa sebuah router bisa memiliki banyak entri di RIB namun hanya sedikit yang aktif di FIB?

3. Apa yang dimaksud dengan routing table tambahan (selain tabel main) pada RouterOS?

BAB 2

Static Routing Lanjutan & Policy Routing

Mendalami parameter-parameter lanjutan pada static route serta menerapkan Policy Based Routing menggunakan routing mark dan mangle.

Tujuan Pembelajaran

Peserta mampu mengonfigurasi static route dengan parameter lanjutan (scope, target-scope, pref-src), serta merancang policy routing untuk mengarahkan trafik tertentu melalui jalur berbeda.

2.1 Parameter Lanjutan Static Route

Parameter	Fungsi
scope	Nilai yang menentukan apakah suatu rute layak dipakai sebagai gateway untuk rute lain (rute dengan scope lebih tinggi dari target-scope rute lain tidak akan dipakai sebagai gateway)
target-scope	Nilai maksimum scope gateway yang masih dianggap valid/reachable oleh rute ini
pref-src	Menentukan source IP address yang dipakai router saat menghasilkan paket menuju tujuan rute tersebut (berguna saat router memiliki banyak IP address)
routing-mark	Menandai rute agar hanya berlaku pada routing table tertentu (bukan tabel main), menjadi dasar policy routing
type=blackhole	Membuang seluruh paket menuju tujuan rute tanpa mengirim notifikasi apa pun — sering dipakai untuk mencegah routing loop atau memblokir suatu subnet secara routing-level
type=unreachable	Membuang paket dan mengirimkan pesan ICMP unreachable ke pengirim

Konsep scope dan target-scope sering membingungkan pemula. Intuisi sederhananya: sebuah rute hanya dianggap "hidup" (dapat dipakai) jika gateway-nya sendiri dapat dijangkau melalui rute lain yang memiliki nilai scope lebih kecil atau sama dengan target-scope rute tersebut — ini mencegah terjadinya rute yang bergantung pada dirinya sendiri secara melingkar (recursive routing loop).

2.2 Recursive Routing (Gateway via Rute Lain)

Berbeda dengan gateway langsung (directly connected), sebuah static route juga bisa menunjuk ke gateway yang hanya dapat dijangkau melalui rute lain (bukan terhubung langsung secara fisik) — dikenal sebagai recursive routing atau gateway indirect. RouterOS akan terus menelusuri (recursive lookup) rute demi rute hingga menemukan gateway yang benar-benar dapat dijangkau secara langsung.

```
/ip route add dst-address=172.16.0.0/24 gateway=10.0.0.2  ; 10.0.0.2 dijangkau via rute
lain, bukan langsung
```

2.3 Mangle — Menandai Trafik untuk Policy Routing

Firewall Mangle digunakan untuk menandai paket (bukan memfilter/memblokir) berdasarkan berbagai kriteria (IP asal, protokol, port, dsb), yang kemudian dapat dimanfaatkan oleh fitur lain seperti policy routing maupun queue.

```
/ip firewall mangle add chain=prerouting src-address=192.168.10.100 action=mark-routing
new-routing-mark=jalur-vip passthrough=no
/ip route add dst-address=0.0.0.0/0 gateway=192.168.1.254 routing-mark=jalur-vip
```

Contoh di atas menandai seluruh trafik dari IP 192.168.10.100 dengan routing-mark "jalur-vip", lalu membuat static route default yang hanya berlaku pada routing-mark tersebut — sehingga klien 192.168.10.100 akan keluar melalui gateway yang berbeda dari klien lain di jaringan yang sama.

2.4 Skenario Umum Policy Routing

- Mengarahkan trafik dari subnet/departemen tertentu melalui ISP berbeda (misalnya divisi keuangan memakai jalur ISP khusus yang lebih stabil).
- Memisahkan trafik game/streaming melalui jalur dengan latency rendah, sementara trafik download besar melalui jalur lain.
- Mengarahkan trafik VPN atau tunnel tertentu melalui gateway spesifik agar tidak tercampur dengan trafik internet biasa.

Parameter "passthrough" pada mangle menentukan apakah paket yang sudah cocok dengan satu rule tetap dilanjutkan ke rule mangle berikutnya (passthrough=yes) atau berhenti di situ (passthrough=no). Untuk mark-routing, passthrough umumnya diset "no" karena satu paket cukup memiliki satu routing-mark saja; namun untuk mark-connection yang nantinya akan dipakai lagi oleh rule mark-routing terpisah (seperti pada teknik PCC di Bab 3), passthrough diset "yes" agar paket dapat terus diproses oleh rule-rule berikutnya.

Penerapan di Industri — Multi-WAN untuk Bisnis Kritis

Perusahaan dengan kebutuhan uptime tinggi (fintech, e-commerce, rumah sakit) hampir selalu berlangganan lebih dari satu ISP sekaligus dan menerapkan policy routing agar trafik kritis (misalnya transaksi ke gateway pembayaran) selalu melalui ISP dengan SLA (Service Level Agreement) terbaik, sementara trafik non-kritis (browsing karyawan, update software) dialihkan ke ISP sekunder yang lebih murah — mengoptimalkan biaya sekaligus menjaga keandalan layanan inti bisnis.

Studi Kasus Nyata — Divisi Keuangan Butuh Jalur Internet Terpisah

Sebuah perusahaan manufaktur menerapkan kebijakan bahwa divisi keuangan harus mengakses internet melalui ISP dengan sertifikasi keamanan lebih baik (meski lebih mahal), sementara divisi lain memakai ISP reguler yang lebih murah untuk efisiensi biaya. Tanpa policy routing, opsi yang tersedia hanya memasang router fisik terpisah untuk tiap divisi — mahal dan merepotkan. Dengan menandai trafik dari subnet divisi keuangan menggunakan mangle dan mengarahkannya ke ISP premium melalui

routing-mark, perusahaan berhasil memenuhi kebijakan tersebut hanya dengan satu router, menghemat biaya hardware sekaligus mempermudah manajemen jaringan secara keseluruhan.

LAB: Policy Routing Berdasarkan Subnet

1. Siapkan router dengan dua koneksi WAN (dua ISP simulasi, misal ether1 dan ether2).

2. Buat dua rule mangle: satu menandai trafik dari 192.168.10.0/25 dengan routing-mark "jalur-A", satu lagi menandai 192.168.10.128/25 dengan routing-mark "jalur-B".

3. Buat dua static route default masing-masing dengan routing-mark yang sesuai, mengarah ke gateway ISP berbeda.

4. Tetap sediakan satu static route default tanpa routing-mark (di tabel main) sebagai jalur fallback umum.

5. Uji dari dua klien pada masing-masing sub-subnet, verifikasi dengan traceroute bahwa keduanya keluar melalui gateway ISP yang berbeda.

Uji Pemahaman

1. Jelaskan perbedaan konsep scope dan target-scope pada static route.

2. Apa fungsi parameter pref-src dan kapan parameter ini relevan digunakan?

3. Bagaimana firewall mangle berperan dalam mekanisme policy routing?

4. Sebutkan minimal dua skenario nyata di mana policy routing bermanfaat.

BAB 3

Load Balancing (ECMP, PCC, NTH)

Mempelajari berbagai teknik load balancing pada RouterOS untuk mendistribusikan trafik ke lebih dari satu jalur/ISP secara efektif.

Tujuan Pembelajaran

Peserta memahami perbedaan ECMP, PCC, dan NTH, serta mampu mengimplementasikan load balancing dua ISP dengan mekanisme failover.

3.1 Load Balancing vs Failover

Penting membedakan dua konsep yang sering tertukar: failover memastikan jalur cadangan hanya aktif ketika jalur utama mati (hanya satu jalur dipakai pada satu waktu), sedangkan load balancing mendistribusikan trafik ke beberapa jalur secara bersamaan untuk memaksimalkan total bandwidth yang tersedia.

3.2 ECMP (Equal Cost Multi Path)

ECMP adalah metode load balancing paling sederhana: menambahkan beberapa gateway sekaligus dalam satu baris static route dengan distance yang sama. RouterOS akan mendistribusikan koneksi baru ke gateway-gateway tersebut menggunakan algoritma round-robin berbasis hash (bukan per paket, melainkan per koneksi), sehingga satu sesi/koneksi tetap konsisten melalui satu jalur yang sama.

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

Keterbatasan ECMP murni

ECMP membagi trafik cukup merata untuk skenario dengan banyak koneksi kecil, namun tidak ideal jika ada satu koneksi berukuran sangat besar (misalnya satu sesi download besar) karena satu koneksi tersebut tetap hanya melalui satu jalur saja, tidak terpecah.

3.3 NTH — Load Balancing Berbasis Rasio

Fitur NTH pada firewall mangle memungkinkan pembagian trafik berdasarkan rasio setiap paket/koneksi ke-N, sehingga administrator dapat mengatur pembagian yang tidak harus 50:50 — misalnya 2:1 jika kapasitas satu ISP dua kali lipat ISP lainnya.

```
/ip firewall mangle add chain=prerouting dst-address-type=!local in-interface=bridge-lan
nth=2,1 action=mark-connection new-connection-mark=isp1-conn
/ip firewall mangle add chain=prerouting dst-address-type=!local in-interface=bridge-lan
nth=2,2 action=mark-connection new-connection-mark=isp2-conn
```

3.4 PCC — Per Connection Classifier

PCC adalah metode load balancing paling populer untuk skenario dua-ISP karena kesederhanaannya: PCC mengelompokkan koneksi berdasarkan kombinasi tertentu (misalnya src-address dan dst-address) ke dalam

beberapa "kelompok" menggunakan operasi hash modulo, lalu setiap kelompok diarahkan ke jalur ISP yang berbeda secara konsisten — satu klien yang sama akan cenderung selalu melalui jalur ISP yang sama untuk kombinasi sumber-tujuan tertentu, menjaga konsistensi sesi (penting untuk aplikasi yang sensitif terhadap perubahan IP publik, seperti perbankan online).

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


/ip route add dst-address=0.0.0.0/0 gateway=192.168.1.254 routing-mark=isp1-route
/ip route add dst-address=0.0.0.0/0 gateway=192.168.2.254 routing-mark=isp2-route
/ip route add dst-address=0.0.0.0/0 gateway=192.168.1.254 distance=1  ; fallback tabel
main
/ip route add dst-address=0.0.0.0/0 gateway=192.168.2.254 distance=2  ; fallback tabel
main
```

3.5 Menggabungkan Load Balancing dengan Failover

Load balancing dan failover bukan konsep yang saling eksklusif — keduanya justru sering digabungkan. Setiap rute pada routing-mark tertentu tetap dapat diberi check-gateway, sehingga jika salah satu ISP mati, trafik yang seharusnya melalui ISP tersebut dapat dialihkan sepenuhnya ke ISP yang masih hidup melalui rute fallback di tabel main.

Penerapan di Industri — PCC — Standar Industri Warnet & Kantor Kecil-Menengah

PCC adalah teknik load balancing paling banyak diadopsi di Indonesia untuk warnet, kantor kecil-menengah, hingga kos-kosan/apartemen yang menggabungkan beberapa langganan internet rumahan menjadi satu jaringan gabungan berkapasitas lebih besar. Popularitasnya karena tidak memerlukan lisensi khusus, cukup satu RouterBOARD kelas menengah, dan konfigurasinya sudah terstandarisasi luas di komunitas MikroTik Indonesia — banyak tutorial dan template konfigurasi PCC yang beredar didasarkan pada pola dasar yang persis seperti dipelajari di bab ini.

Studi Kasus Nyata — Aplikasi Perbankan Selalu Logout Sendiri

Sebuah kos-kosan menggabungkan dua langganan internet rumahan menggunakan ECMP murni untuk menambah kapasitas total. Penghuni kemudian mengeluh aplikasi mobile banking mereka terus-menerus meminta login ulang di tengah transaksi. Setelah diselidiki, penyebabnya adalah ECMP yang membagi ulang koneksi antar dua ISP secara tidak konsisten, menyebabkan IP publik yang terlihat oleh server bank berubah-ubah di tengah sesi yang sama — bank mendeteksi ini sebagai potensi pembajakan sesi dan otomatis logout demi keamanan. Setelah beralih ke PCC yang menjaga konsistensi jalur per kombinasi source-destination, masalah logout mendadak tersebut hilang sepenuhnya karena IP publik yang terlihat bank kini konsisten sepanjang sesi.

LAB: Load Balancing 2 ISP dengan PCC

1. Siapkan topologi router dengan dua koneksi WAN (ether1 ke ISP-1, ether2 ke ISP-2) dan satu jaringan LAN.

2. Buat empat rule mangle PCC sesuai contoh (per-connection-classifier=both-addresses:2/0 dan 2/1) untuk menandai connection-mark.

3. Buat dua rule mangle tambahan untuk mengubah connection-mark menjadi routing-mark (mark-routing berdasarkan connection-mark).

4. Buat static route dengan routing-mark sesuai menuju masing-masing gateway ISP, tambahkan check-gateway=ping.

5. Buat NAT masquerade terpisah untuk masing-masing interface WAN.

6. Uji dari beberapa klien berbeda, verifikasi dengan traceroute bahwa trafik terbagi ke kedua ISP, lalu putuskan salah satu ISP dan amati apakah trafik yang tadinya lewat jalur tersebut berhasil failover ke ISP yang masih hidup.

Uji Pemahaman

1. Jelaskan perbedaan mendasar antara load balancing dan failover.

2. Mengapa ECMP murni kurang ideal untuk trafik dengan satu koneksi berukuran sangat besar?

3. Jelaskan cara kerja PCC dalam menjaga konsistensi jalur untuk klien yang sama.

4. Bagaimana check-gateway dapat dikombinasikan dengan policy routing untuk menghasilkan load balancing sekaligus failover?

BAB 4

Tunnel Dasar (IPIP, EoIP, GRE)

Mempelajari konsep tunneling Layer 3 dan Layer 2 dasar sebagai fondasi sebelum masuk ke VPN yang lebih kompleks.

Tujuan Pembelajaran

Peserta memahami perbedaan tunnel IPIP, EoIP, dan GRE, serta mampu mengonfigurasi masing-masing untuk menghubungkan dua jaringan melalui internet.

4.1 Konsep Dasar Tunneling

Tunneling adalah teknik membungkus (encapsulate) satu jenis paket data di dalam paket data jenis lain, sehingga dapat dikirim melalui jaringan yang mungkin tidak secara native mendukung jenis paket aslinya. Berbeda dengan VPN berbasis PPP (PPTP, SSTP) yang dibahas di buku MTCNA, tunnel di bab ini bekerja langsung di level IP tanpa proses autentikasi user/password.

4.2 IPIP Tunnel

IPIP (IP-in-IP) adalah tunnel paling sederhana, membungkus paket IP di dalam paket IP lain. IPIP hanya mendukung trafik IPv4/IPv6 murni (Layer 3), tidak dapat membawa trafik Layer 2 seperti broadcast ARP atau paket non-IP.

```
/interface ipip add name=ipip-ke-cabang local-address=203.0.113.1 remote-
address=203.0.113.2
/ip address add address=10.100.0.1/30 interface=ipip-ke-cabang
/ip route add dst-address=192.168.99.0/24 gateway=10.100.0.2
```

4.3 EoIP Tunnel (Ethernet over IP)

EoIP adalah tunnel proprietary buatan MikroTik yang membungkus trafik Ethernet (Layer 2) di dalam paket GRE/IP, sehingga mampu membawa seluruh jenis trafik termasuk broadcast, ARP, dan protokol non-IP — menjadikannya seolah-olah dua jaringan di lokasi berbeda tergabung dalam satu segmen Layer 2 yang sama melalui internet.

```
/interface eoip add name=eoip-ke-cabang local-address=203.0.113.1 remote-
address=203.0.113.2 tunnel-id=1
/interface bridge port add bridge=bridge-lan interface=eoip-ke-cabang
```

EoIP dan Bridge

EoIP paling sering digabungkan langsung ke dalam bridge (bukan diberi IP address sendiri), sehingga perangkat di kedua lokasi benar-benar berada dalam satu broadcast domain Layer 2 yang sama — berguna misalnya untuk menyatukan jaringan CCTV atau VoIP antar cabang.

4.4 GRE Tunnel

GRE (Generic Routing Encapsulation) adalah protokol tunneling standar industri (bukan proprietary MikroTik), sehingga kompatibel untuk menghubungkan RouterOS dengan perangkat vendor lain seperti Cisco atau Juniper. Secara fungsi, GRE mirip IPIP namun mendukung lebih banyak jenis protokol yang dibungkus di dalamnya, termasuk mendukung multicast — penting jika tunnel tersebut nantinya akan menjalankan protokol routing dinamis seperti OSPF di atasnya.

```
/interface gre add name=gre-ke-cabang local-address=203.0.113.1 remote-
address=203.0.113.2
```

4.5 Perbandingan Tunnel Dasar

Tunnel	Layer	Multicast	Interoperabilitas Vendor Lain
IPIP	Layer 3	Tidak	Cukup luas (standar)
EoIP	Layer 2	Ya (karena membawa Ethernet penuh)	Proprietary MikroTik (terbatas)
GRE	Layer 3 (mendukung banyak protokol)	Ya	Luas (standar industri)

Pemilihan jenis tunnel tergantung kebutuhan: gunakan EoIP jika membutuhkan penggabungan Layer 2 penuh antar-MikroTik, gunakan GRE jika perlu interoperabilitas dengan vendor lain atau perlu membawa multicast (misalnya untuk OSPF over tunnel), dan gunakan IPIP untuk kebutuhan tunneling IP sederhana dengan overhead paling minim.

Penerapan di Industri — Menghubungkan Cabang Toko/Restoran

Bisnis waralaba (franchise) dengan puluhan hingga ratusan cabang sering menggunakan kombinasi EoIP/GRE untuk menyatukan sistem kasir (POS), CCTV, dan absensi karyawan seluruh cabang ke dalam satu jaringan terpusat yang dapat dimonitor dari kantor pusat, tanpa perlu menyewa jalur leased-line mahal — cukup memanfaatkan koneksi internet biasa di tiap cabang. Pendekatan ini jauh lebih murah dibanding MPLS VPN dari operator telekomunikasi, meski dengan trade-off keandalan yang bergantung pada kualitas internet publik masing-masing cabang.

Studi Kasus Nyata — CCTV Cabang Tidak Bisa Diakses dari Pusat

Sebuah bisnis retail dengan 5 cabang memasang CCTV berbasis IP di tiap toko, namun tim keamanan di kantor pusat tidak bisa mengakses CCTV cabang karena masing-masing CCTV memiliki IP privat lokal yang tidak dapat dijangkau dari luar jaringan cabang tersebut, dan membeli DVR cloud berbayar dianggap terlalu mahal untuk 5 cabang sekaligus. Solusinya, teknisi memasang EoIP dari tiap router cabang menuju router pusat, menggabungkannya ke bridge yang sama dengan jaringan CCTV di pusat — hasilnya seluruh CCTV cabang kini "terlihat" seolah berada dalam satu jaringan lokal yang sama dengan kantor pusat, dan tim keamanan bisa mengaksesnya langsung melalui IP lokal seperti biasa tanpa biaya layanan cloud tambahan.

LAB: Menghubungkan Dua Kantor dengan EoIP

1. Simulasikan dua router yang terhubung melalui jaringan "internet" (bisa berupa router ketiga sebagai perantara).

2. Buat interface EoIP pada Router A menuju IP publik Router B, dan sebaliknya pada Router B menuju Router A, gunakan tunnel-id yang sama.

3. Gabungkan masing-masing interface EoIP ke dalam bridge LAN pada kedua router.

4. Hubungkan satu klien ke LAN Router A dan satu klien lain ke LAN Router B, pastikan keduanya berada dalam subnet IP yang sama.

5. Uji ping antar kedua klien tersebut, verifikasi bahwa mereka dapat berkomunikasi seolah berada dalam satu jaringan lokal yang sama.

6. Bandingkan dengan mencoba pendekatan IPIP: buat interface IPIP antar kedua router, beri IP address pada masing-masing sisi tunnel, lalu tambahkan static route agar kedua subnet LAN saling terhubung tanpa bridging Layer 2.

✓ Uji Pemahaman

1. Jelaskan perbedaan mendasar antara tunnel Layer 2 (EoIP) dan Layer 3 (IPIP).

2. Mengapa GRE lebih cocok dipakai saat menghubungkan RouterOS dengan perangkat vendor lain dibanding EoIP?

3. Dalam skenario apa EoIP lebih dipilih dibanding IPIP?

4. Mengapa dukungan multicast pada tunnel menjadi penting jika di atasnya akan dijalankan OSPF?

BAB 5

VPN Lanjutan (L2TP, PPPoE Mendalam, IPSec)

Melanjutkan pembahasan VPN dari buku MTCNA dengan protokol yang lebih kompleks, termasuk kombinasi L2TP dengan IPSec untuk keamanan tingkat enterprise.

Tujuan Pembelajaran

Peserta mampu mengonfigurasi L2TP/IPSec, memahami parameter keamanan IPSec (Phase 1 dan Phase 2), serta mendalami skenario PPPoE untuk lingkungan ISP.

5.1 L2TP (Layer 2 Tunneling Protocol)

L2TP membentuk tunnel Layer 2 melalui jaringan IP, namun secara default tidak menyediakan enkripsi sendiri — L2TP hanya menangani pembentukan tunnel, sementara keamanan/enkripsi biasanya diserahkan pada IPSec yang berjalan bersamanya, membentuk kombinasi populer bernama L2TP/IPSec.

```
/interface l2tp-server server set enabled=yes use-ipsec=yes ipsec-
secret=RahasiaBersama123
/ppp secret add name=cabang01 password=Passw0rd! service=l2tp local-address=10.50.0.1
remote-address=10.50.0.2
```

5.2 Konsep Dasar IPSec

IPSec (Internet Protocol Security) adalah kerangka kerja standar industri untuk mengamankan trafik IP melalui autentikasi dan enkripsi. IPSec bekerja dalam dua fase negosiasi:

Fase	Fungsi
Phase 1 (IKE)	Membentuk kanal aman awal antar dua peer untuk saling autentikasi (biasanya menggunakan pre-shared key atau sertifikat) dan menyepakati parameter enkripsi
Phase 2 (IPSec SA)	Menggunakan kanal aman dari Phase 1 untuk menyepakati parameter enkripsi trafik data sesungguhnya (algoritma enkripsi, lifetime, dsb)

Komponen penting dalam konfigurasi IPSec di RouterOS meliputi Peer (menentukan siapa lawan bicara dan parameter Phase 1), Proposal (algoritma enkripsi/autentikasi yang ditawarkan), dan Policy (menentukan trafik/subnet mana saja yang harus dilewatkan melalui tunnel terenkripsi ini).

```
/ip ipsec profile add name=profile-cabang dh-group=modp2048 enc-algorithm=aes-256
/ip ipsec peer add name=peer-cabang address=203.0.113.2/32 profile=profile-cabang
/ip ipsec identity add peer=peer-cabang secret=RahasiaBersama123
/ip ipsec proposal add name=proposal-cabang enc-algorithms=aes-256-cbc auth-
algorithms=sha256
/ip ipsec policy add src-address=192.168.10.0/24 dst-address=192.168.20.0/24 peer=peer-
cabang proposal=proposal-cabang tunnel=yes
```

5.3 Site-to-Site VPN vs Remote Access VPN

Jenis	Karakteristik	Contoh Protokol
Site-to-Site	Menghubungkan dua jaringan/kantor secara permanen, biasanya tanpa interaksi user (always-on)	IPSec Site-to-Site, EoIP+IPSec, GRE+IPSec
Remote Access	Pengguna individual terhubung ke jaringan kantor dari lokasi mana pun, memerlukan proses login	PPTP, SSTP, L2TP/IPSec, OpenVPN

5.4 PPPoE Mendalam untuk Lingkungan ISP

Buku MTCNA telah membahas PPPoE secara dasar. Pada skala ISP dengan ratusan/ribuan pelanggan, beberapa pertimbangan tambahan menjadi penting: penggunaan RADIUS sebagai basis data user terpusat (dibanding menyimpan seluruh PPP Secret secara lokal di router), rate-limit per profile untuk membedakan paket layanan pelanggan, serta pemantauan resource CPU karena setiap sesi PPPoE membutuhkan pemrosesan enkapsulasi tersendiri.

Penerapan di Industri — IPSec di Perbankan dan Fintech

Industri perbankan dan fintech di Indonesia diwajibkan regulator (OJK) menerapkan standar keamanan data yang ketat, sehingga koneksi antar kantor cabang atau antara kantor dengan penyedia layanan pihak ketiga (misalnya switching pembayaran) hampir selalu menggunakan IPSec dengan algoritma enkripsi kuat (AES-256) dan proses audit keamanan berkala. Meski RouterOS mendukung IPSec dengan baik untuk skala menengah, perusahaan skala enterprise besar biasanya tetap menggunakan perangkat firewall dedicated (Fortinet, Palo Alto, Cisco ASA) untuk kebutuhan compliance yang lebih ketat — namun prinsip dasar Phase 1/Phase 2 yang dipelajari di sini tetap sama persis di seluruh platform tersebut.

Studi Kasus Nyata — Staf Lapangan Butuh Akses Aman Tanpa Laptop Khusus

Sebuah perusahaan konstruksi memiliki staf lapangan yang perlu mengakses sistem ERP internal dari lokasi proyek yang berbeda-beda setiap minggu, namun perusahaan tidak ingin repot menginstal software VPN pihak ketiga di puluhan laptop dan HP staf. Dengan mengaktifkan L2TP/IPSec di router kantor, staf cukup menggunakan fitur VPN bawaan yang sudah tersedia di Windows, macOS, iOS, maupun Android tanpa instalasi tambahan apa pun — cukup memasukkan alamat server, pre-shared key, dan kredensial masing-masing. Ini secara signifikan mengurangi beban dukungan teknis dibanding harus mengelola aplikasi VPN pihak ketiga di berbagai jenis perangkat.

LAB: L2TP/IPSec Remote Access VPN

1. Aktifkan L2TP Server pada router, aktifkan use-ipsec=yes dengan sebuah ipsec-secret.

2. Buat PPP Profile khusus untuk L2TP dengan local-address dan pool remote-address tersendiri.

3. Buat PPP Secret untuk satu user percobaan dengan service=l2tp.

4. Dari perangkat client (bisa laptop dengan built-in L2TP/IPSec VPN client), konfigurasikan koneksi VPN menuju IP publik router dengan pre-shared key dan kredensial user yang sesuai.

5. Setelah terhubung, verifikasi status koneksi pada menu PPP > Active Connections di router.

6. Uji ping dari client menuju IP LAN router melalui tunnel, konfirmasikan trafik benar-benar terenkripsi dengan memeriksa Torch pada interface WAN (trafik tampak sebagai paket IPSec/ESP, bukan trafik biasa).

☑ Uji Pemahaman

1. Jelaskan perbedaan fungsi Phase 1 dan Phase 2 pada negosiasi IPSec.

2. Mengapa L2TP sering dikombinasikan dengan IPSec, padahal keduanya adalah protokol berbeda?

3. Jelaskan perbedaan mendasar antara Site-to-Site VPN dan Remote Access VPN.

4. Mengapa ISP skala besar cenderung memakai RADIUS dibanding menyimpan seluruh kredensial PPPoE secara lokal di router?

BAB 6

VLAN & 802.1Q, QinQ

Memahami segmentasi jaringan Layer 2 menggunakan VLAN, konfigurasi trunk/access port, serta pengenalan QinQ untuk skenario multi-tenant.

Tujuan Pembelajaran

Peserta mampu merancang dan mengonfigurasi VLAN pada RouterOS, memahami perbedaan tagged dan untagged port, serta memahami konsep dasar QinQ.

6.1 Mengapa VLAN Diperlukan

VLAN (Virtual Local Area Network) memungkinkan satu infrastruktur fisik (switch/bridge yang sama) dipecah menjadi beberapa broadcast domain logis yang terpisah, tanpa memerlukan perangkat fisik terpisah untuk masing-masing segmen. Ini sangat efisien dari sisi biaya sekaligus meningkatkan keamanan (memisahkan trafik antar departemen) dan mengurangi ukuran broadcast domain (meningkatkan performa jaringan).

6.2 Tagged vs Untagged Port

Istilah	Penjelasan
Access Port (Untagged)	Port yang terhubung ke perangkat akhir (PC, printer) yang tidak memahami VLAN tag — port ini hanya menjadi anggota satu VLAN tertentu tanpa perlu tagging
Trunk Port (Tagged)	Port yang menghubungkan antar-switch/router, membawa trafik dari banyak VLAN sekaligus dengan menambahkan tag 802.1Q pada setiap frame untuk menandai VLAN asalnya

6.3 Konfigurasi VLAN pada RouterOS

RouterOS mengimplementasikan VLAN sebagai interface virtual yang dipasang di atas interface fisik atau bridge. Terdapat dua pendekatan umum: VLAN interface langsung di atas interface fisik (untuk router dengan trunk sederhana), atau VLAN filtering pada bridge (pendekatan modern yang lebih powerful, mendekati cara kerja switch VLAN pada umumnya).

```
; Pendekatan sederhana: VLAN interface di atas ether1 (trunk)
/interface vlan add name=vlan10-staf interface=ether1 vlan-id=10
/interface vlan add name=vlan20-tamu interface=ether1 vlan-id=20
/ip address add address=192.168.10.1/24 interface=vlan10-staf
/ip address add address=192.168.20.1/24 interface=vlan20-tamu
```

```
; Pendekatan modern: Bridge VLAN Filtering
/interface bridge add name=br1 vlan-filtering=no  ; aktifkan filtering setelah semua
port ditambahkan
```

```
/interface bridge port add bridge=br1 interface=ether2 pvid=10
/interface bridge port add bridge=br1 interface=ether3 pvid=20
/interface bridge port add bridge=br1 interface=ether1 frame-types=admit-only-vlan-
tagged
/interface bridge vlan add bridge=br1 vlan-ids=10 tagged=br1,ether1 untagged=ether2
/interface bridge vlan add bridge=br1 vlan-ids=20 tagged=br1,ether1 untagged=ether3
/interface bridge set br1 vlan-filtering=yes
```

PVID (Port VLAN ID)

PVID menentukan VLAN mana yang akan "diasumsikan" untuk frame yang masuk tanpa tag (untagged) pada suatu port — inilah yang membuat port tersebut berfungsi sebagai access port untuk VLAN yang bersangkutan.

6.4 Inter-VLAN Routing

Karena VLAN memisahkan trafik menjadi broadcast domain berbeda (setara subnet berbeda), komunikasi antar VLAN memerlukan proses routing (Layer 3) — dapat dilakukan oleh router MikroTik itu sendiri (router-on-a-stick, menggunakan satu interface trunk) atau melalui router/Layer 3 switch terpisah.

6.5 QinQ (802.1ad) — Pengantar

QinQ adalah teknik "VLAN di dalam VLAN" — membungkus tag VLAN pelanggan (customer VLAN/C-VLAN) di dalam tag VLAN penyedia layanan (service VLAN/S-VLAN). Ini umum dipakai oleh ISP/penyedia layanan Metro Ethernet untuk memisahkan trafik banyak pelanggan (yang masing-masing sudah memakai VLAN internal mereka sendiri) di atas satu infrastruktur bersama, tanpa perlu khawatir tabrakan VLAN ID antar pelanggan karena keduanya berada di "lapisan" tagging yang berbeda.

Penerapan di Industri — VLAN sebagai Standar Wajib Jaringan Korporat

Hampir tanpa kecuali, setiap perusahaan menengah-besar menyegmentasi jaringannya menggunakan VLAN: VLAN terpisah untuk staf, tamu, perangkat IoT/CCTV, server, dan manajemen perangkat jaringan itu sendiri. Selain alasan keamanan (mencegah tamu WiFi mengakses server internal), segmentasi ini juga menjadi syarat kepatuhan pada banyak standar keamanan seperti ISO 27001 dan PCI-DSS (untuk bisnis yang memproses data kartu kredit). Auditor keamanan IT hampir selalu memeriksa desain VLAN sebagai salah satu item checklist utama saat melakukan audit infrastruktur jaringan perusahaan.

Studi Kasus Nyata — Magang IT Tanpa Sengaja Akses Server Produksi

Sebuah perusahaan startup awalnya menghubungkan seluruh perangkat (laptop staf, server produksi, printer, WiFi tamu) ke satu switch/bridge yang sama tanpa segmentasi apa pun. Suatu hari, anak magang yang baru bergabung tanpa sengaja menemukan server database produksi dapat diakses langsung dari laptop pribadinya yang terhubung ke WiFi kantor biasa — celah yang sebenarnya sangat berbahaya jika laptop tersebut terinfeksi malware. Setelah menerapkan VLAN yang memisahkan jaringan Server, Staf, dan Tamu/Magang secara tegas, insiden serupa tidak mungkin terjadi lagi karena secara desain jaringan, ketiga segmen tersebut kini benar-benar terisolasi kecuali melalui jalur routing yang sudah dikontrol firewall.

LAB: Segmentasi VLAN dengan Bridge VLAN Filtering

1. Buat bridge baru, tambahkan tiga port: satu untuk trunk (menuju switch/router lain) dan dua untuk access port (VLAN 10 dan VLAN 20).

2. Set PVID masing-masing access port sesuai VLAN yang diinginkan.

3. Definisikan Bridge VLAN untuk VLAN 10 dan VLAN 20, tentukan port mana saja yang tagged (trunk) dan untagged (access) untuk masing-masing VLAN.

4. Aktifkan vlan-filtering=yes pada bridge.

5. Hubungkan dua klien ke dua access port berbeda (VLAN 10 dan VLAN 20), pastikan keduanya TIDAK dapat saling ping secara langsung (karena berbeda broadcast domain).

6. Tambahkan IP address dan static route pada router untuk masing-masing VLAN, lalu verifikasi kedua klien kini dapat saling ping melalui proses inter-VLAN routing.

Uji Pemahaman

1. Jelaskan perbedaan access port dan trunk port dalam konteks VLAN.

2. Apa fungsi PVID pada konfigurasi Bridge VLAN Filtering?

3. Mengapa komunikasi antar VLAN memerlukan proses routing, bukan sekadar bridging?

4. Jelaskan secara singkat konsep QinQ dan mengapa ISP membutuhkannya.

BAB 7

OSPF Fundamentals

Memasuki inti materi MTCRE: protokol routing dinamis OSPF, mulai dari konsep area, neighbor adjacency, hingga konfigurasi dasar di RouterOS.

Tujuan Pembelajaran

Peserta memahami konsep dasar link-state routing, mampu mengonfigurasi OSPF single-area, serta memahami proses pembentukan neighbor dan pemilihan DR/BDR.

7.1 Mengapa Routing Dinamis?

Static routing yang dipelajari di buku MTCNA cukup untuk jaringan kecil dengan sedikit rute, namun menjadi sangat merepotkan dikelola secara manual pada jaringan besar dengan banyak router dan rute yang sering berubah. Routing dinamis memungkinkan router-router saling bertukar informasi rute secara otomatis dan beradaptasi terhadap perubahan topologi (misalnya link putus) tanpa campur tangan manual administrator.

7.2 OSPF sebagai Protokol Link-State

OSPF (Open Shortest Path First) adalah protokol routing dinamis berbasis link-state, artinya setiap router membangun "peta" lengkap topologi jaringan (bukan sekadar tabel rute tetangga seperti protokol distance-vector), lalu menghitung jalur terpendek menuju setiap tujuan menggunakan algoritma Dijkstra (Shortest Path First).

Istilah	Penjelasan
LSA (Link State Advertisement)	Paket informasi yang berisi status link suatu router, disebarkan ke seluruh router dalam area yang sama
LSDB (Link State Database)	Basis data hasil kumpulan seluruh LSA yang diterima — pada dasarnya adalah "peta" topologi jaringan versi router tersebut
Area	Pengelompokan router OSPF untuk membatasi ukuran LSDB dan mengurangi beban komputasi SPF, terutama pada jaringan besar
Router ID	Identitas unik 32-bit (format mirip IP address) yang membedakan setiap router OSPF, biasanya diambil dari salah satu IP address loopback

7.3 Pembentukan Neighbor Adjacency

Sebelum dua router OSPF dapat bertukar informasi rute, mereka harus terlebih dahulu membentuk hubungan tetangga (neighbor adjacency) melalui pertukaran paket Hello secara berkala. Proses ini melalui beberapa tahapan status (state): Down, Init, 2-Way, ExStart, Exchange, Loading, hingga Full (adjacency terbentuk sepenuhnya).

Syarat pembentukan neighbor

Dua router hanya dapat menjadi neighbor jika berada pada area OSPF yang sama, memiliki interval Hello dan Dead yang sama, subnet yang sama (untuk jaringan broadcast), serta autentikasi yang sesuai jika diaktifkan.

7.4 DR dan BDR pada Jaringan Broadcast

Pada jaringan broadcast multi-access (misalnya segmen Ethernet dengan lebih dari dua router OSPF), jika setiap router membentuk adjacency penuh dengan semua router lain, jumlah adjacency akan tumbuh secara kuadratik dan sangat tidak efisien. OSPF mengatasi ini dengan memilih satu Designated Router (DR) dan satu Backup Designated Router (BDR) pada segmen tersebut — seluruh router lain hanya membentuk adjacency penuh dengan DR dan BDR, bukan dengan satu sama lain, sehingga jumlah pertukaran informasi jauh berkurang.

Pemilihan DR/BDR ditentukan oleh nilai OSPF Priority tertinggi pada interface (nilai 0 berarti router tersebut tidak akan pernah menjadi DR/BDR); jika priority sama, Router ID tertinggi yang menjadi penentu.

Setiap kali terjadi perubahan pada suatu link (misalnya interface down/up, atau penambahan rute baru), router yang mendeteksi perubahan tersebut segera menyebarkan LSA terbaru ke seluruh router lain dalam area yang sama (dikenal sebagai flooding). Setiap router yang menerima update tersebut memperbarui LSDB miliknya dan menjalankan ulang algoritma SPF untuk menghitung ulang jalur terpendek — proses inilah yang disebut konvergensi (convergence). Kecepatan konvergensi OSPF (umumnya hanya membutuhkan waktu beberapa detik) menjadi salah satu keunggulan utama dibanding routing statis yang memerlukan intervensi manual saat terjadi perubahan topologi.

Penerapan di Industri — OSPF di Data Center dan Jaringan Kampus

OSPF adalah pilihan IGP (Interior Gateway Protocol) paling populer untuk jaringan internal perusahaan skala menengah-besar, kampus universitas, dan data center karena bersifat open-standard (tidak terikat satu vendor, sehingga bisa menghubungkan MikroTik dengan Cisco, Juniper, atau Huawei sekaligus dalam satu domain routing) serta konvergensinya sangat cepat. Perusahaan multi-cabang dengan lebih dari 5-10 router biasanya beralih dari static routing ke OSPF tepat pada titik ketika pengelolaan rute manual sudah mulai tidak terkendali dan rawan human error saat terjadi perubahan topologi.

Studi Kasus Nyata — Static Route Manual Bikin Downtime Berulang

Sebuah perusahaan dengan 8 cabang selama bertahun-tahun mengelola konektivitas antar-cabang menggunakan static route yang diketik manual di setiap router. Setiap kali ada penambahan subnet baru di salah satu cabang, admin harus mengingat untuk menambahkan rute yang sesuai di ketujuh router lainnya secara manual — proses yang rawan lupa dan sering menyebabkan cabang tertentu tidak bisa saling terhubung selama berhari-hari tanpa disadari, karena baru ketahuan setelah ada keluhan pengguna. Setelah bermigrasi ke OSPF, penambahan subnet baru di satu cabang otomatis diketahui oleh seluruh router lain dalam hitungan detik tanpa campur tangan manual sama sekali, menghilangkan kelas masalah ini sepenuhnya.

7.5 Konfigurasi OSPF Dasar (Single Area)

```
/routing ospf instance add name=default-instance router-id=1.1.1.1
/routing ospf area add name=backbone instance=default-instance area-id=0.0.0.0
```

```
/routing ospf interface-template add interfaces=ether1,ether2 area=backbone
```

Pada RouterOS versi terbaru (v7+), konfigurasi OSPF berbasis interface-template yang menentukan interface mana saja yang ikut serta menjalankan OSPF pada area tertentu — sedikit berbeda dari pendekatan berbasis network statement pada versi RouterOS lama (v6), namun konsep dasarnya tetap sama.

7.6 Verifikasi dan Troubleshooting OSPF

```
/routing ospf neighbor print   ; melihat status neighbor (harus "Full" untuk adjacency
sempurna)
/routing ospf lsa print        ; melihat isi Link State Database
/ip route print where ospf     ; melihat rute yang dipelajari dari OSPF (flag "o")
```

🔧 LAB: OSPF Single Area dengan 3 Router

1. Siapkan topologi segitiga: Router A - Router B - Router C, masing-masing terhubung langsung satu sama lain (3 link).

2. Konfigurasikan IP address point-to-point pada setiap link (gunakan subnet /30 seperti dipelajari di buku MTCNA).

3. Pada ketiga router, buat OSPF instance dengan router-id unik masing-masing (misal 1.1.1.1, 2.2.2.2, 3.3.3.3).

4. Buat OSPF area backbone (area-id=0.0.0.0) pada ketiga router, daftarkan seluruh interface yang terhubung ke router lain.

5. Verifikasi neighbor adjacency terbentuk penuh (status Full) di ketiga router menggunakan "/routing ospf neighbor print".

6. Tambahkan satu loopback interface dengan IP unik pada masing-masing router, sertakan ke dalam OSPF, lalu verifikasi ketiga router dapat saling ping ke loopback satu sama lain melalui rute OSPF (bukan static).

7. Putuskan salah satu link secara sengaja, amati proses reconvergence — seberapa cepat trafik menemukan jalur alternatif melalui router ketiga.

✓ Uji Pemahaman

1. Jelaskan perbedaan mendasar antara protokol routing link-state dan distance-vector.

2. Apa fungsi Router ID dalam OSPF dan bagaimana biasanya nilai tersebut ditentukan?

3. Mengapa OSPF memerlukan pemilihan DR dan BDR pada jaringan broadcast multi-access?

4. Sebutkan syarat-syarat yang harus terpenuhi agar dua router OSPF dapat membentuk neighbor adjacency.

BAB 8

OSPF Lanjutan

Mendalami OSPF multi-area, jenis-jenis area khusus, redistribusi rute dari luar OSPF, serta filtering dan tuning cost.

Tujuan Pembelajaran

Peserta mampu merancang OSPF multi-area, memahami perbedaan stub/totally stub/NSSA, serta mampu melakukan redistribusi dan filtering rute OSPF.

8.1 Mengapa Multi-Area?

Pada jaringan besar dengan banyak router, menjalankan OSPF dalam satu area tunggal (area 0 / backbone) menyebabkan LSDB tumbuh sangat besar dan proses SPF menjadi berat secara komputasi. OSPF mengatasi ini dengan membagi jaringan menjadi beberapa area, di mana detail topologi suatu area disembunyikan (disederhanakan menjadi ringkasan) saat diteruskan ke area lain — mengurangi ukuran LSDB dan mempercepat konvergensi.

Aturan Backbone Area

Dalam desain OSPF multi-area, seluruh area non-backbone wajib terhubung langsung ke Area 0 (backbone area) — baik secara fisik maupun melalui virtual link — karena seluruh trafik antar-area harus melewati backbone.

8.2 Jenis-Jenis Area Khusus

Jenis Area	Karakteristik
Standard Area	Menerima seluruh jenis LSA termasuk rute eksternal dari luar OSPF (redistribusi)
Stub Area	Memblokir rute eksternal (Type 5 LSA) dari luar OSPF, digantikan default route tunggal menuju backbone — mengurangi ukuran LSDB pada area ini
Totally Stub Area	Lebih ketat dari Stub: selain memblokir rute eksternal, juga memblokir rute antar-area (Type 3 LSA), hanya menyisakan default route — fitur khas MikroTik/Cisco untuk area yang benar-benar hanya sebagai "ranting" jaringan
NSSA (Not-So-Stubby-Area)	Mirip Stub Area, namun tetap mengizinkan area tersebut menyuntikkan rute eksternal miliknya sendiri ke dalam OSPF (melalui LSA Type 7 yang dikonversi menjadi Type 5 di ABR)

8.3 Router Role dalam OSPF Multi-Area

- Internal Router — seluruh interface-nya berada dalam satu area yang sama.

- ABR (Area Border Router) — memiliki interface pada lebih dari satu area, termasuk minimal satu terhubung ke backbone; bertugas meringkas dan meneruskan informasi rute antar-area.
- Backbone Router — memiliki minimal satu interface pada Area 0.
- ASBR (Autonomous System Boundary Router) — menjadi gerbang redistribusi rute dari luar OSPF (misalnya dari static route atau protokol BGP) ke dalam domain OSPF.

8.4 Redistribusi Rute ke dalam OSPF

Redistribusi memungkinkan rute yang berasal dari luar OSPF (misalnya static route atau rute dari protokol lain seperti BGP) turut disebarkan ke seluruh router OSPF, dengan router yang melakukannya berperan sebagai ASBR.

```
/routing ospf instance set default-instance redistribute=static
```

> **Hati-hati saat redistribusi**
> Redistribusi yang tidak direncanakan dengan baik (misalnya me-redistribute seluruh static route tanpa filter) dapat menyebabkan rute yang tidak diinginkan tersebar ke seluruh jaringan, bahkan berpotensi menimbulkan routing loop. Sebaiknya gunakan filter atau route-map untuk mengontrol rute spesifik mana saja yang di-redistribute.

8.5 Filtering Rute OSPF

RouterOS menyediakan mekanisme filter (melalui routing filter chain) untuk mengontrol rute OSPF mana saja yang diterima ke dalam tabel routing, maupun rute mana yang diizinkan untuk di-advertise keluar — berguna untuk menyembunyikan subnet tertentu dari sebagian jaringan atau mencegah rute yang tidak diinginkan masuk ke tabel routing lokal.

8.6 OSPF Cost dan Load Balancing

Setiap interface OSPF memiliki nilai cost, yang secara default dihitung berdasarkan bandwidth interface tersebut (semakin tinggi bandwidth, semakin rendah cost). OSPF memilih jalur dengan total cost terendah menuju tujuan. Jika terdapat dua jalur dengan total cost yang identik, OSPF secara otomatis melakukan ECMP di antara jalur-jalur tersebut.

```
/routing ospf interface-template set [find interfaces~"ether2"] cost=20
```

> **Penerapan di Industri — Desain Multi-Area di ISP Regional**
> ISP regional yang memiliki banyak POP (Point of Presence) tersebar di berbagai kota biasanya merancang setiap kota/wilayah sebagai OSPF area tersendiri yang terhubung ke Area 0 (backbone) di data center pusat. Desain Stub Area sering diterapkan pada area cabang yang hanya memiliki satu jalur keluar menuju backbone, karena area tersebut tidak memerlukan detail rute eksternal lengkap — cukup mengetahui bahwa "segala sesuatu di luar area ini" dapat dicapai melalui satu default route ke arah backbone, sehingga mengurangi beban memori router-router kecil di POP cabang yang biasanya memiliki spesifikasi hardware lebih rendah dibanding router core.

Studi Kasus Nyata — Kantor Cabang Kecil "Kebanjiran" Update Rute

Sebuah perusahaan menjalankan OSPF single-area untuk seluruh 15 cabangnya, termasuk cabang-cabang kecil yang hanya memiliki router entry-level dengan RAM terbatas. Router-router kecil tersebut mulai sering hang dan restart sendiri, terutama saat ada perubahan topologi di cabang besar yang menyebabkan flooding LSA ke seluruh jaringan, termasuk ke router-router kecil yang sebenarnya tidak perlu tahu detail topologi cabang lain. Setelah admin merancang ulang jaringan menjadi multi-area dengan cabang-cabang kecil dikelompokkan sebagai Totally Stub Area, beban LSDB pada router-router tersebut turun drastis (hanya menyimpan satu default route), dan masalah hang/restart tidak pernah terjadi lagi.

LAB: OSPF Multi-Area dengan Stub Area

1. Rancang topologi 4 router: Router A dan B berada di Area 0 (backbone), Router B dan C terhubung ke Area 1, Router C dan D berada dalam Area 1.

2. Konfigurasikan OSPF pada seluruh router sesuai pembagian area tersebut, pastikan Router B berperan sebagai ABR (memiliki interface di Area 0 dan Area 1).

3. Verifikasi seluruh neighbor adjacency terbentuk penuh, dan seluruh router dapat saling ping ke seluruh subnet.

4. Ubah Area 1 menjadi Stub Area pada seluruh router yang menjadi anggotanya (termasuk Router B sebagai ABR), amati bagaimana routing table pada Router C dan D berubah (rute eksternal digantikan default route).

5. Tambahkan satu static route percobaan pada Router A (mewakili rute dari "luar" jaringan OSPF), lakukan redistribusi static pada Router A, amati apakah rute tersebut muncul di Router C/D sebelum dan sesudah Area 1 dijadikan Stub Area.

6. Diskusikan hasil pengamatan: mengapa rute eksternal tersebut tidak muncul di Stub Area, dan bagaimana Router C/D tetap bisa mencapai tujuan tersebut?

Uji Pemahaman

1. Mengapa seluruh area non-backbone wajib terhubung ke Area 0 dalam desain OSPF multi-area?

2. Jelaskan perbedaan antara Stub Area dan Totally Stub Area.

3. Apa perbedaan peran ABR dan ASBR dalam topologi OSPF?

4. Mengapa redistribusi rute perlu dilakukan secara hati-hati dan idealnya disertai filtering?

BAB 9

Pengenalan BGP (Bab Pengayaan)

Bab pengayaan di luar cakupan inti ujian MTCRE, memberikan gambaran awal BGP sebagai jembatan menuju sertifikasi MTCINE (Internetworking Engineer).

Tujuan Pembelajaran

Peserta memahami konsep dasar BGP sebagai protokol routing antar-Autonomous System, perbedaannya dengan OSPF, serta mampu membangun sesi eBGP sederhana.

Catatan Cakupan Materi

BGP mendalam merupakan materi inti sertifikasi MTCINE, bukan MTCRE. Bab ini disertakan sebagai pengayaan/pengantar agar peserta memiliki gambaran awal sebelum melanjutkan ke jenjang sertifikasi berikutnya.

9.1 Apa itu BGP dan Mengapa Berbeda dari OSPF

BGP (Border Gateway Protocol) adalah protokol routing yang dirancang untuk pertukaran rute antar Autonomous System (AS) — kumpulan jaringan yang berada di bawah satu kendali administratif, misalnya satu ISP atau satu perusahaan besar. Jika OSPF dirancang untuk routing di dalam satu jaringan (Interior Gateway Protocol/IGP), BGP dirancang sebagai Exterior Gateway Protocol (EGP) yang menjadi tulang punggung routing internet global itu sendiri.

Aspek	OSPF	BGP
Kategori	Interior Gateway Protocol (IGP)	Exterior Gateway Protocol (EGP)
Algoritma	Link-state (Dijkstra/SPF)	Path-vector
Metrik pemilihan rute	Cost berbasis bandwidth	Kombinasi banyak atribut (AS-Path, Local Preference, MED, dsb)
Skala penggunaan	Jaringan internal organisasi	Antar-organisasi/ISP, termasuk internet global

9.2 Autonomous System (AS) dan AS Number

Setiap organisasi yang menjalankan BGP secara mandiri di internet publik memerlukan AS Number (ASN) yang unik secara global, didaftarkan melalui Regional Internet Registry (RIR) seperti APNIC untuk kawasan Asia-Pasifik. Untuk keperluan pembelajaran/lab internal, dapat digunakan Private AS Number (umumnya pada rentang 64512-65534) yang tidak memerlukan pendaftaran resmi.

9.3 eBGP vs iBGP

Jenis	Penjelasan
eBGP (External BGP)	Sesi BGP antara dua router yang berada pada AS Number berbeda — umum dipakai untuk peering

Jenis	Penjelasan
	antar-ISP atau menghubungkan jaringan perusahaan ke ISP
iBGP (Internal BGP)	Sesi BGP antara router-router yang berada dalam AS Number yang sama — biasanya dipakai bersamaan dengan IGP (seperti OSPF) di dalam AS tersebut

9.4 Konfigurasi eBGP Dasar di RouterOS

```
/routing bgp connection add name=peer-isp remote.address=203.0.113.2 remote.as=65001
local.as=65002 as-override=no
/routing bgp connection print
/routing bgp advertisements print   ; melihat rute yang diadvertise ke peer
```

Setelah sesi BGP terbentuk (status Established), router akan saling bertukar rute dan menambahkannya ke tabel routing sesuai kebijakan yang diatur (misalnya melalui network statement atau redistribusi dari rute lain).

9.5 Atribut Dasar BGP

- AS-Path — daftar AS yang telah dilalui suatu rute, juga berfungsi mencegah routing loop (rute ditolak jika AS sendiri sudah muncul di dalam AS-Path).
- Local Preference — menentukan preferensi keluar (outbound) trafik ke arah AS tertentu, dibagikan hanya di dalam iBGP.
- MED (Multi-Exit Discriminator) — memberi saran kepada AS tetangga mengenai jalur masuk (inbound) mana yang lebih disukai jika ada beberapa titik koneksi.
- Next-Hop — alamat IP router selanjutnya yang harus dilalui untuk mencapai suatu rute.

Penerapan di Industri — BGP — Tulang Punggung Internet Global

Setiap kali Anda mengakses sebuah website, paket data yang dikirim kemungkinan besar melewati puluhan Autonomous System berbeda yang saling bertukar rute melalui BGP — inilah yang membuat internet global bisa berfungsi sebagai satu jaringan besar meski dikelola oleh ribuan organisasi independen. Di Indonesia, ISP menengah-besar dan perusahaan dengan kebutuhan multihoming (berlangganan ke lebih dari satu upstream provider sekaligus demi redundansi) wajib memiliki ASN resmi dari APNIC dan menjalankan BGP agar dapat mengumumkan (announce) blok IP publik mereka sendiri ke internet global — pengetahuan BGP inilah yang menjadi pembeda antara level MTCRE dan level MTCINE dalam jenjang karier Network Engineer.

Studi Kasus Nyata — ISP Kecil "Lumpuh" Saat Salah Satu Upstream Down

Sebuah ISP kecil hanya berlangganan ke satu upstream provider besar tanpa BGP, sehingga saat provider tersebut mengalami gangguan regional selama beberapa jam, seluruh pelanggan ISP kecil tersebut ikut terputus total dari internet tanpa ada jalur alternatif apa pun. Setelah ISP tersebut mendaftarkan ASN sendiri dan berlangganan ke dua upstream provider berbeda sambil menjalankan eBGP ke keduanya, kejadian serupa di kemudian hari tidak lagi berdampak — begitu satu upstream

down, BGP secara otomatis mengalihkan seluruh trafik pelanggan melalui upstream kedua dalam hitungan detik, jauh lebih andal dibanding hanya mengandalkan satu provider saja.

LAB: Membangun Sesi eBGP Sederhana

1. Siapkan dua router yang saling terhubung langsung, masing-masing mewakili AS berbeda (misal AS 65001 dan AS 65002, gunakan Private ASN untuk lab).

2. Konfigurasikan IP address pada link penghubung kedua router.

3. Pada masing-masing router, buat BGP connection menuju IP tetangga dengan remote.as dan local.as yang sesuai.

4. Verifikasi status sesi BGP menggunakan "/routing bgp connection print", pastikan status menunjukkan "established".

5. Tambahkan satu network/rute percobaan pada salah satu router (misalnya melalui static route dan redistribusi, atau melalui BGP network statement), amati apakah rute tersebut muncul di tabel routing router tetangga.

6. Diskusikan: apa yang membedakan proses ini dengan pembentukan neighbor OSPF yang telah dipelajari sebelumnya?

☑ Uji Pemahaman

1. Jelaskan perbedaan mendasar antara eBGP dan iBGP.

2. Mengapa BGP dikategorikan sebagai Exterior Gateway Protocol, berbeda dari OSPF?

3. Apa fungsi atribut AS-Path dalam mencegah routing loop pada BGP?

4. Mengapa organisasi yang hanya melakukan lab internal dapat menggunakan Private AS Number?

BAB 10

Pengenalan MPLS (Bab Pengayaan)

Bab pengayaan memperkenalkan konsep dasar MPLS sebagai teknologi forwarding berbasis label yang sering menjadi pelengkap arsitektur BGP pada jaringan skala besar.

Tujuan Pembelajaran

Peserta memahami konsep dasar label switching pada MPLS, perbedaannya dengan routing IP konvensional, serta gambaran umum implementasi dasarnya di RouterOS.

Catatan Cakupan Materi

Seperti BGP, MPLS mendalam merupakan materi lanjutan yang lebih relevan untuk MTCINE. Bab ini memberikan pengantar konsep dasar sebagai bekal awal.

10.1 Apa itu MPLS?

MPLS (Multi Protocol Label Switching) adalah teknologi forwarding paket yang tidak mengandalkan pencarian rute berbasis IP address tujuan pada setiap hop (seperti routing IP konvensional), melainkan menggunakan label pendek yang disisipkan di antara header Layer 2 dan Layer 3. Router di sepanjang jalur (disebut Label Switch Router/LSR) cukup melihat label tersebut untuk menentukan ke mana paket harus diteruskan, tanpa perlu melakukan pencarian tabel routing IP yang lebih kompleks pada setiap hop.

10.2 Mengapa MPLS Diperlukan?

- Forwarding lebih cepat — pencarian berbasis label lebih sederhana dibanding longest-prefix-match pada routing IP biasa (meski pada perangkat modern, keunggulan kecepatan ini semakin tidak signifikan berkat hardware yang semakin cepat).
- Traffic Engineering — memungkinkan penyedia jaringan mengarahkan trafik melalui jalur spesifik yang telah direncanakan, bukan hanya jalur terpendek default hasil perhitungan routing.
- VPN berbasis MPLS (L3VPN/L2VPN) — memungkinkan penyedia layanan menghadirkan jaringan privat virtual bagi banyak pelanggan berbeda di atas satu infrastruktur fisik bersama, dengan isolasi trafik antar pelanggan.

10.3 Istilah Dasar MPLS

Istilah	Penjelasan
LSR (Label Switch Router)	Router yang mampu memproses forwarding berbasis label MPLS
LER (Label Edge Router)	Router di tepi domain MPLS, bertugas menambahkan label pertama kali (ingress) atau melepas label terakhir kali (egress)
LDP (Label Distribution Protocol)	Protokol yang digunakan antar-LSR untuk saling bertukar informasi pemetaan label secara otomatis
LSP (Label Switched Path)	Jalur yang dilalui suatu paket berdasarkan urutan label sepanjang domain MPLS, mirip konsep "tunnel" logis

10.4 Gambaran Umum Konfigurasi MPLS di RouterOS

```
/mpls interface add interface=ether1
/mpls ldp set enabled=yes lsr-id=1.1.1.1 transport-address=1.1.1.1
/mpls ldp interface add interface=ether1
```

Setelah LDP aktif dan berhasil membentuk sesi dengan LSR tetangga, label akan otomatis dipertukarkan dan LSP mulai terbentuk mengikuti rute IGP (seperti OSPF) yang sudah berjalan di jaringan tersebut — inilah sebabnya MPLS pada praktiknya selalu berjalan berdampingan dengan sebuah IGP, bukan berdiri sendiri.

10.5 Hubungan MPLS dengan OSPF dan BGP

Dalam arsitektur jaringan skala besar (umumnya di ISP), ketiga teknologi yang telah dipelajari saling melengkapi: OSPF (atau IGP lain) menyediakan jalur dasar dan reachability antar-LSR di dalam jaringan inti (core), MPLS menyediakan mekanisme forwarding berbasis label di sepanjang jalur tersebut, sementara BGP (khususnya MP-BGP) digunakan untuk membawa informasi rute pelanggan/VPN di atas infrastruktur MPLS tersebut — kombinasi yang sering disebut sebagai arsitektur MPLS L3VPN.

Penerapan di Industri — MPLS pada Layanan Metro Ethernet Operator

Ketika sebuah perusahaan berlangganan layanan "VPN IP" atau "Metro Ethernet" dari operator telekomunikasi besar (Telkom, Indosat, dsb) untuk menghubungkan kantor-kantor cabangnya, di balik layar operator tersebut menjalankan arsitektur MPLS L3VPN persis seperti konsep yang dipelajari di bab ini — pelanggan cukup menerima "jalur privat" yang tampak seolah terhubung langsung, tanpa perlu tahu bahwa di infrastruktur operator, trafik mereka sebenarnya melewati puluhan router MPLS yang menangani ribuan pelanggan lain secara bersamaan dengan isolasi penuh antar pelanggan.

Studi Kasus Nyata — Memilih Antara VPN Internet Biasa dan Layanan MPLS Operator

Sebuah perusahaan multi-cabang awalnya menghubungkan seluruh cabangnya menggunakan EoIP/IPSec melalui internet biasa (seperti dipelajari di Bab 4-5), namun mulai mengalami masalah latency tidak stabil dan packet loss saat volume trafik antar-cabang meningkat pesat, terutama untuk aplikasi VoIP internal yang sangat sensitif terhadap jitter. Setelah membandingkan biaya, perusahaan memutuskan bermigrasi sebagian trafik kritis (VoIP dan ERP real-time) ke layanan Metro Ethernet berbasis MPLS dari operator telekomunikasi, sementara trafik non-kritis tetap menggunakan VPN internet biasa yang jauh lebih murah — sebuah keputusan arsitektur yang mengharuskan pemahaman trade-off antara biaya dan kualitas layanan (SLA) seperti yang dibahas di bab ini.

LAB: Eksplorasi MPLS Dasar dengan LDP

1. Gunakan topologi 3 router dari lab OSPF multi-area sebelumnya (Bab 8) yang sudah memiliki OSPF berjalan sebagai IGP.

2. Aktifkan MPLS pada interface yang menghubungkan ketiga router.

3. Aktifkan LDP pada ketiga router dengan lsr-id unik masing-masing (dapat memanfaatkan IP loopback yang sudah dibuat sebelumnya).

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

5. Amati tabel forwarding MPLS melalui "/mpls forwarding-table print", identifikasi label yang terbentuk otomatis untuk rute-rute OSPF yang telah ada.

6. Diskusikan: pada titik mana konsep "label switching" ini berbeda dari proses lookup routing table IP biasa yang telah dipelajari sepanjang buku ini?

✓ Uji Pemahaman

1. Jelaskan perbedaan mendasar antara forwarding berbasis label (MPLS) dan forwarding berbasis IP routing konvensional.

2. Apa perbedaan peran LSR dan LER dalam domain MPLS?

3. Mengapa MPLS pada praktiknya selalu memerlukan sebuah IGP (seperti OSPF) yang berjalan bersamaan?

4. Jelaskan secara singkat bagaimana OSPF, MPLS, dan BGP saling melengkapi dalam arsitektur MPLS L3VPN.

BAB 11

SuperLab MTCRE — Proyek Akhir Terintegrasi

Satu skenario jaringan multi-cabang utuh yang menyatukan LITERALLY seluruh materi Bab 1-10 secara bertahap (multi-fase): policy routing, load balancing, tunneling, VPN, VLAN, dan OSPF multi-area — bahkan menyentuh BGP sebagai pengayaan akhir.

Tujuan Pembelajaran

Peserta mampu merancang, membangun, dan mendokumentasikan jaringan multi-cabang dengan routing dinamis dan keamanan berlapis menggunakan seluruh kompetensi MTCRE, serta siap menghadapi ujian sertifikasi MTCRE.

11.1 Latar Belakang SuperLab

PT Nusantara Digital Group adalah perusahaan retail yang berkembang pesat, kini memiliki Kantor Pusat di Jakarta dan dua Kantor Cabang di Bandung dan Surabaya. Direktur IT menunjuk Anda sebagai Network Engineer untuk merancang ulang seluruh infrastruktur jaringan perusahaan yang sebelumnya masih menggunakan static route manual yang mulai sulit dikelola. Berikut daftar kebutuhan yang harus Anda penuhi.

No	Kebutuhan Direktur IT	Bab Terkait
1	Kantor Pusat berlangganan 2 ISP — trafik divisi Keuangan harus lewat ISP premium, divisi lain via ISP reguler	Bab 2
2	Jika salah satu ISP Kantor Pusat mati, seluruh trafik otomatis pindah ke ISP yang masih hidup	Bab 3
3	Kantor Cabang Bandung dan Surabaya terhubung ke Pusat melalui internet secara aman (bukan sewa leased-line mahal)	Bab 4, Bab 5
4	Staf yang bekerja dari rumah/perjalanan dinas tetap bisa akses sistem internal secara aman	Bab 5
5	Tiap kantor memisahkan jaringan Staf, Server, dan Tamu agar tidak saling mengganggu/membahayakan	Bab 6
6	Seluruh subnet di ketiga lokasi harus saling terhubung otomatis tanpa static route manual yang merepotkan	Bab 7, Bab 8
7	(Opsional/Pengayaan) Ke depan perusahaan berencana punya koneksi langsung ke upstream ISP sendiri	Bab 9

11.2 Rancangan Topologi & OSPF Area

Lokasi	Peran OSPF	Subnet Utama
Kantor Pusat (Jakarta)	ABR — Area 0 (backbone) + gerbang ke Area 1 & Area 2 via tunnel	192.168.0.0/16 (dipecah per VLAN)
Cabang Bandung	Area 1 (Stub Area)	192.168.101.0/24 (Staf), 192.168.102.0/24 (Server)
Cabang Surabaya	Area 2 (Stub Area)	192.168.201.0/24 (Staf), 192.168.202.0/24 (Server)

VLAN di Kantor Pusat	VLAN ID	Subnet
Staf Umum	10	192.168.10.0/24
Divisi Keuangan (jalur ISP premium)	11	192.168.11.0/24
Server Internal	20	192.168.20.0/24
Tamu	30	192.168.30.0/24

11.3 Fase Pengerjaan SuperLab

SuperLab dikerjakan dalam 7 fase berurutan, disimulasikan menggunakan 3 RouterBOARD/CHR yang mewakili Kantor Pusat, Cabang Bandung, dan Cabang Surabaya. Setiap fase harus diverifikasi sebelum melanjutkan ke fase berikutnya.

LAB: FASE 1 — VLAN & Policy Routing di Kantor Pusat (Bab 2, Bab 6)

1. Buat 4 VLAN di Kantor Pusat sesuai tabel: Staf (10), Keuangan (11), Server (20), Tamu (30) menggunakan Bridge VLAN Filtering.

2. Pasang IP address pada masing-masing interface VLAN sesuai denah subnet.

3. Buat rule mangle yang menandai trafik dari VLAN Keuangan (192.168.11.0/24) dengan routing-mark "isp-premium".

4. Buat static route default dengan routing-mark "isp-premium" mengarah ke ISP premium (ether1), dan static route default umum (tabel main) mengarah ke ISP reguler (ether2).

5. Verifikasi: traceroute dari klien VLAN Keuangan menunjukkan keluar via ether1, sementara traceroute dari VLAN Staf keluar via ether2.

LAB: FASE 2 — Load Balancing & Failover 2 ISP (Bab 3)

1. Modifikasi konfigurasi Fase 1: tambahkan check-gateway=ping pada kedua static route default (baik yang routing-mark maupun tabel main).

2. Tambahkan static route default cadangan dengan distance lebih besar pada tabel main, mengarah ke ISP yang berlawanan (sebagai fallback jika salah satu ISP mati) — pastikan trafik Keuangan tetap punya jalur keluar meski ISP premium sedang down.

3. Verifikasi failover: putuskan interface ISP premium (ether1), amati apakah trafik VLAN Keuangan tetap bisa keluar internet (melalui rute fallback), meski kini lewat ISP reguler.

4. Sambungkan kembali ether1, verifikasi trafik Keuangan kembali otomatis lewat ISP premium.

🔗 LAB: FASE 3 — Tunnel Aman ke Kedua Cabang (Bab 4, Bab 5)

1. Dari Kantor Pusat, buat interface GRE menuju Cabang Bandung dan interface GRE terpisah menuju Cabang Surabaya (gunakan GRE agar mendukung multicast, dibutuhkan untuk OSPF di Fase 6).

2. Amankan kedua tunnel tersebut dengan IPSec policy (Phase 1 dan Phase 2) menggunakan pre-shared key berbeda untuk masing-masing cabang.

3. Pasang IP address point-to-point pada masing-masing ujung tunnel GRE (baik di Pusat maupun di kedua cabang).

4. Verifikasi: dari Kantor Pusat, ping ke IP tunnel di kedua cabang berhasil, dan trafik tersebut benar-benar terenkripsi (periksa melalui Torch di interface WAN, harus tampak sebagai paket ESP/IPSec).

🔗 LAB: FASE 4 — VPN Remote Access untuk Staf Mobile (Bab 5)

1. Aktifkan L2TP Server dengan use-ipsec=yes di Kantor Pusat.

2. Buat PPP Profile khusus VPN staf dengan local-address dan pool remote-address tersendiri (terpisah dari pool VLAN manapun).

3. Buat beberapa PPP Secret untuk staf percobaan.

4. Verifikasi dari perangkat "luar jaringan" (simulasikan dengan hotspot terpisah), hubungkan VPN L2TP/IPSec, pastikan berhasil ping ke subnet Server (192.168.20.0/24) di Kantor Pusat.

🔗 LAB: FASE 5 — Segmentasi VLAN di Kedua Cabang (Bab 6)

1. Ulangi konsep Bridge VLAN Filtering di Cabang Bandung dan Cabang Surabaya, masing-masing dipecah menjadi VLAN Staf dan VLAN Server sesuai denah subnet.

2. Pastikan penamaan dan penomoran VLAN konsisten dengan dokumentasi agar tidak membingungkan saat troubleshooting di kemudian hari.

3. Verifikasi: klien di VLAN Staf dan VLAN Server pada masing-masing cabang berada di broadcast domain terpisah (tidak bisa saling ping tanpa routing).

🔗 LAB: FASE 6 — OSPF Multi-Area Menyatukan Seluruh Lokasi (Bab 7, Bab 8)

1. Di Kantor Pusat, buat OSPF instance, definisikan Area 0 (backbone) mencakup seluruh VLAN internal Pusat, serta Area 1 dan Area 2 pada interface tunnel GRE menuju Bandung dan Surabaya.

2. Di Cabang Bandung, buat OSPF instance dengan seluruh interface (VLAN lokal + tunnel GRE ke Pusat) sebagai anggota Area 1.

3. Di Cabang Surabaya, lakukan hal serupa untuk Area 2.

4. Ubah Area 1 dan Area 2 menjadi Stub Area (karena kedua cabang hanya memiliki satu jalur keluar yaitu melalui Kantor Pusat).

5. Verifikasi neighbor adjacency Full terbentuk antara Pusat-Bandung dan Pusat-Surabaya melalui "/routing ospf neighbor print".

6. Verifikasi akhir yang PALING PENTING: dari klien VLAN Staf di Cabang Bandung, ping ke klien VLAN Server di Cabang Surabaya — trafik ini harus berhasil secara OTOMATIS mengalir melalui Kantor Pusat tanpa satupun static route manual, murni hasil kalkulasi OSPF.

7. Uji resiliensi: putuskan tunnel GRE ke Cabang Bandung, amati reconvergence OSPF dan pastikan seluruh lokasi lain tidak terganggu (hanya Cabang Bandung yang terisolasi, sesuai desain karena tidak ada jalur cadangan ke cabang tersebut).

🔗 LAB: FASE 7 — Pengayaan BGP & Dokumentasi Akhir (Bab 9)

1. Sebagai simulasi rencana masa depan, bangun sesi eBGP percobaan antara Kantor Pusat (mewakili AS perusahaan, gunakan Private ASN) dengan satu router tambahan yang mewakili "upstream ISP".

2. Verifikasi sesi BGP berhasil established, dan lakukan redistribusi satu rute percobaan dari OSPF ke BGP (mensimulasikan perusahaan mengumumkan blok IP mereka sendiri ke upstream).

3. Lakukan backup dan export konfigurasi final dari ketiga router (Pusat, Bandung, Surabaya).

4. Susun dokumentasi akhir: topologi lengkap (gambar), tabel OSPF area & VLAN, seluruh IP addressing plan, serta hasil pengujian tiap fase termasuk skenario failover dan resiliensi yang sudah diuji.

11.4 Checklist Verifikasi Akhir SuperLab

Verifikasi	Status yang Diharapkan
Trafik VLAN Keuangan keluar via ISP premium	Berhasil
Trafik VLAN Keuangan tetap jalan saat ISP premium mati	Berhasil (failover ke ISP reguler)
Tunnel ke Bandung & Surabaya terenkripsi IPSec	Terverifikasi via Torch (paket ESP)
VPN L2TP staf mobile berhasil akses subnet Server Pusat	Berhasil
VLAN Staf dan Server terisolasi dalam satu lokasi yang sama	Terisolasi (butuh routing untuk saling akses)
Klien Bandung ping ke klien Surabaya TANPA static route manual	Berhasil murni via OSPF
Salah satu cabang terputus tidak mengganggu cabang lain	Terverifikasi (isolasi sesuai desain)
Sesi eBGP percobaan established dan redistribusi rute berhasil	Berhasil

Penerapan di Industri — SuperLab sebagai Simulasi Proyek Network Engineer Sungguhan

Skenario multi-cabang dengan kombinasi policy routing, load balancing, VPN, VLAN, dan OSPF multi-area seperti pada SuperLab ini adalah representasi hampir persis dari proyek nyata yang dikerjakan Network Engineer di perusahaan System Integrator saat menangani klien korporat multi-cabang. Kemampuan merancang OSPF area boundary yang tepat (mana yang backbone, mana yang stub), memutuskan kapan memakai tunnel biasa versus IPSec, serta mendokumentasikan seluruh keputusan desain, adalah kompetensi inti yang diuji dalam sertifikasi MTCRE sekaligus yang paling dicari di dunia kerja jaringan enterprise.

11.5 Ringkasan Perintah Penting per Bab

Bab	Perintah Kunci
2 - Policy Routing	/ip firewall mangle (mark-routing), /ip route (routing-mark)
3 - Load Balancing	/ip firewall mangle (per-connection-classifier, nth), routing-mark ganda
4 - Tunnel Dasar	/interface eoip, /interface ipip, /interface gre
5 - VPN Lanjutan	/interface l2tp-server, /ip ipsec peer|proposal|policy|identity
6 - VLAN	/interface bridge vlan, /interface bridge port (pvid, frame-types)
7-8 - OSPF	/routing ospf instance|area|interface-template, /routing ospf neighbor print
9 - BGP (pengayaan)	/routing bgp connection
10 - MPLS (pengayaan)	/mpls interface, /mpls ldp

11.6 Latihan Soal Bergaya Ujian MTCRE

Uji Pemahaman

1. Sebuah static route memiliki gateway yang hanya dapat dijangkau melalui rute lain, bukan terhubung langsung. Apa istilah untuk jenis routing ini?

2. Pada konfigurasi PCC, parameter apa yang digunakan untuk mengklasifikasikan koneksi berdasarkan kombinasi source dan destination address?

3. Manakah tunnel yang mampu membawa trafik broadcast dan ARP karena beroperasi di Layer 2: IPIP atau EoIP?

4. Dalam negosiasi IPSec, fase manakah yang bertugas menyepakati parameter enkripsi untuk trafik data sesungguhnya: Phase 1 atau Phase 2?

5. Apa fungsi PVID pada sebuah access port dalam konfigurasi Bridge VLAN Filtering?

6. Pada OSPF, status neighbor apa yang menandakan adjacency telah terbentuk sepenuhnya?

7. Jenis area OSPF manakah yang memblokir baik rute eksternal maupun rute antar-area, hanya menyisakan default route?

8. Router dengan interface di lebih dari satu area OSPF, termasuk terhubung ke backbone, disebut sebagai apa?

9. Dalam BGP, atribut apa yang mencegah terjadinya routing loop dengan menolak rute yang sudah memuat AS milik sendiri?

10. Apa istilah untuk router di tepi domain MPLS yang bertugas menambahkan atau melepas label pertama/terakhir kali?

11. Dalam SuperLab, mengapa tunnel antar-kantor dipilih menggunakan GRE dibanding IPIP?

12. Mengapa Cabang Bandung dan Surabaya pada SuperLab dirancang sebagai Stub Area, bukan Standard Area?

Tips Menghadapi Ujian Resmi MTCRE

Selain memahami konsep dan sintaks konfigurasi, ujian MTCRE sering menyajikan skenario topologi yang perlu dianalisis (misalnya menentukan jalur mana yang dipilih OSPF berdasarkan cost, atau memprediksi hasil policy routing). Mengerjakan ulang SuperLab dari nol tanpa melihat catatan, lalu mencoba menjelaskan setiap keputusan desain (mengapa Area ini Stub, mengapa tunnel ini pakai GRE bukan EoIP) kepada rekan belajar, adalah cara terbaik menguji kesiapan konseptual sebelum ujian sesungguhnya.

11.7 Langkah Selanjutnya Setelah MTCRE

Setelah menguasai materi buku ini dan lulus SuperLab, peserta yang ingin mendalami jaringan skala ISP/enterprise dapat melanjutkan ke sertifikasi MTCINE (Internetworking Engineer) yang membahas BGP dan MPLS secara mendalam, atau memilih jalur spesialisasi lain sesuai minat: MTCWE (Wireless Engineer) untuk pendalaman wireless, MTCTCE (Traffic Control Engineer) untuk pendalaman firewall dan QoS, atau MTCUME (User Management Engineer) untuk pendalaman manajemen pengguna berbasis RADIUS dan Hotspot.