

Advanced MikroTik Training

Routing (MTCRE)

Rofiq Fauzi, MTCNA, MTCRE, MTCWE, MTCINE, Cert. Trainer

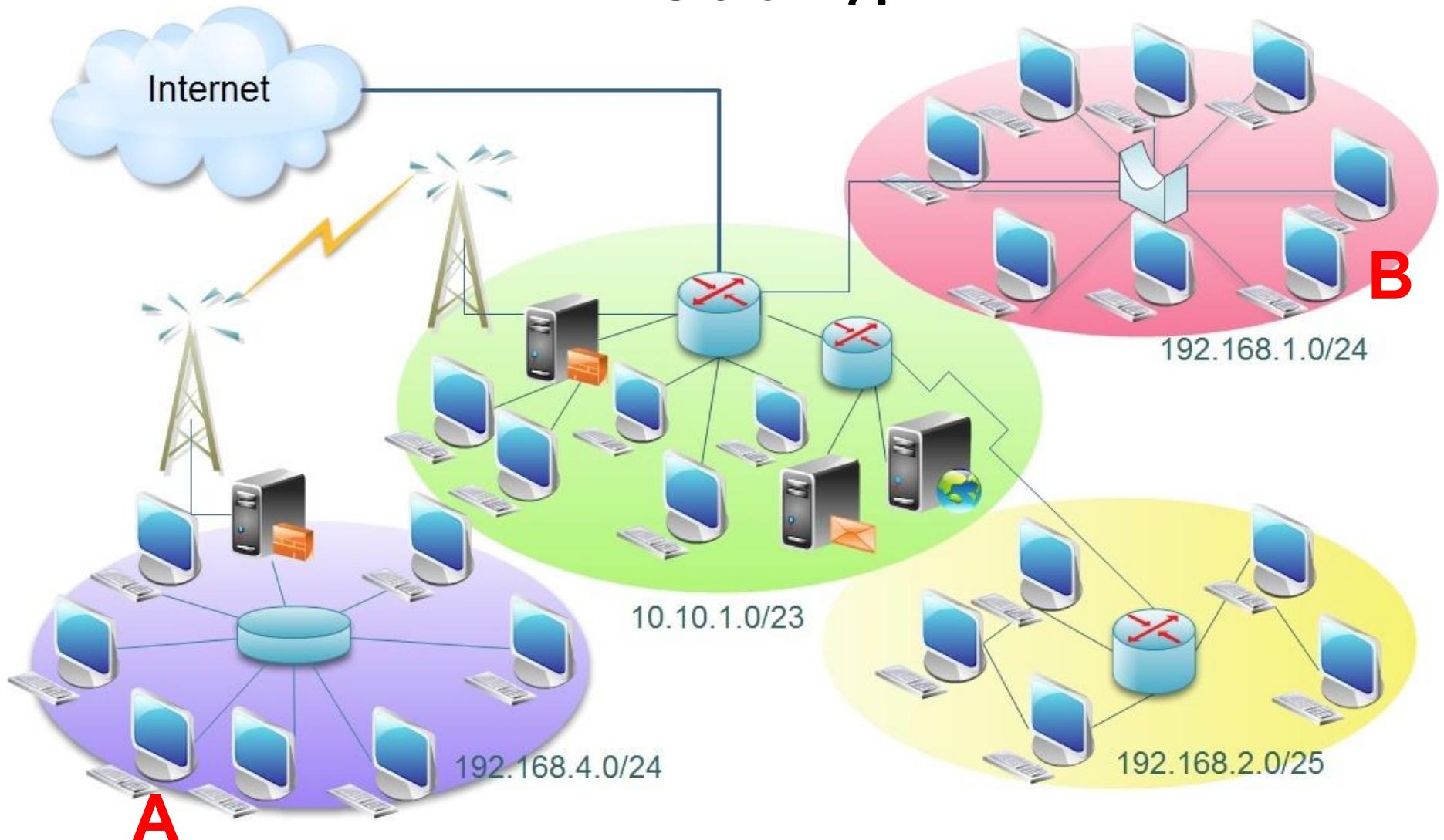
ID-Networkers

www.training-mikrotik.com

Materi

- Static & Dynamic Routing
- ECMP
- OSPF
- VLAN
- Point to Point Addressing
- Tunneling
- MME Wireless Protocol (introduction)

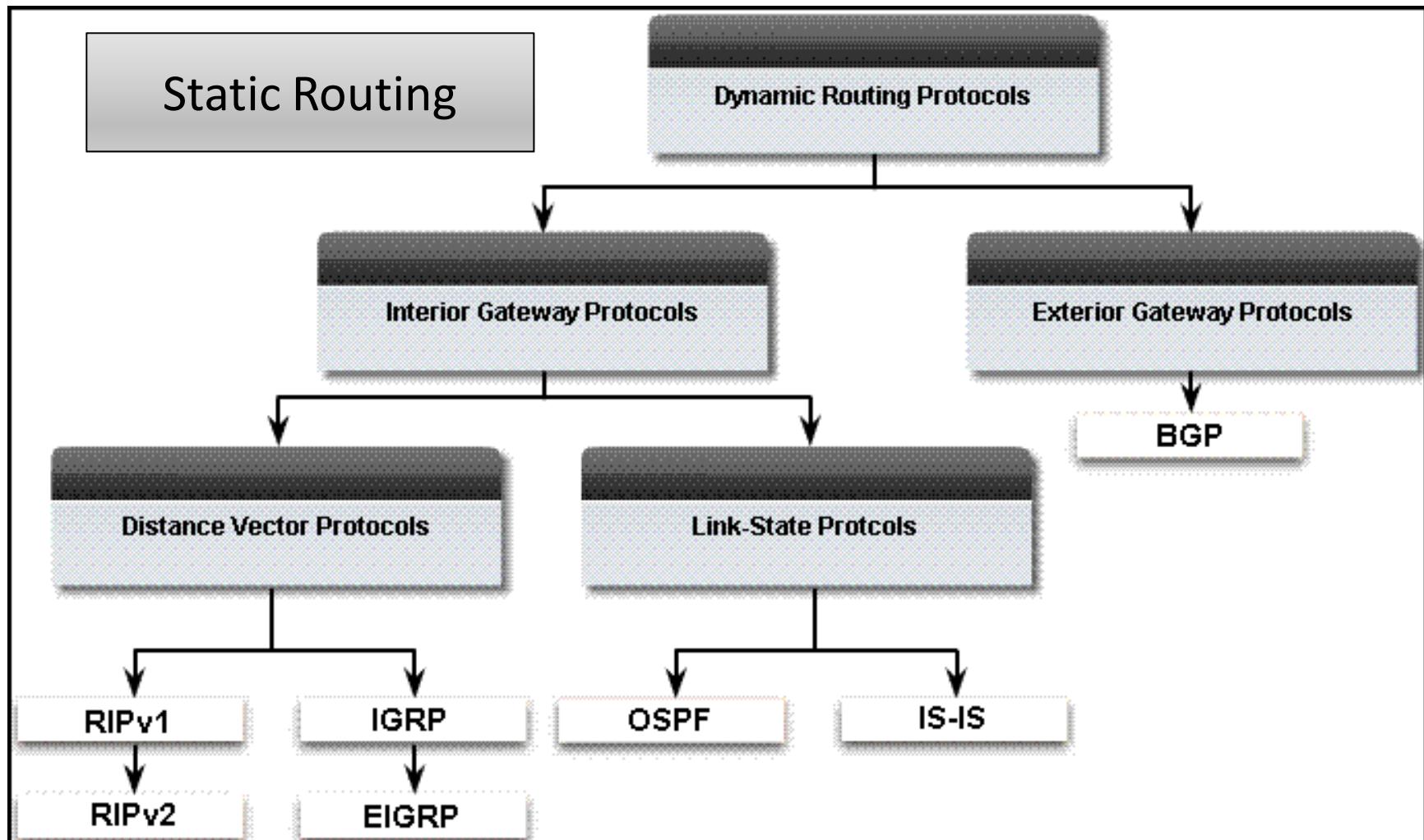
Routing



Routing

- Ketika jaringan lokal sudah mulai komplek.
- Jika kita menginginkan pemantauan dan pengelolaan jaringan yang lebih baik
- Lebih aman (firewall filtering lebih mudah dan lengkap)
- Trafik broadcast hanya terkonsentrasi di setiap subnet/network.
- Koneksi antar public IP network.
- Koneksi antar Wide Area Network (company, Provider, dll)

Klasifikasi Routing

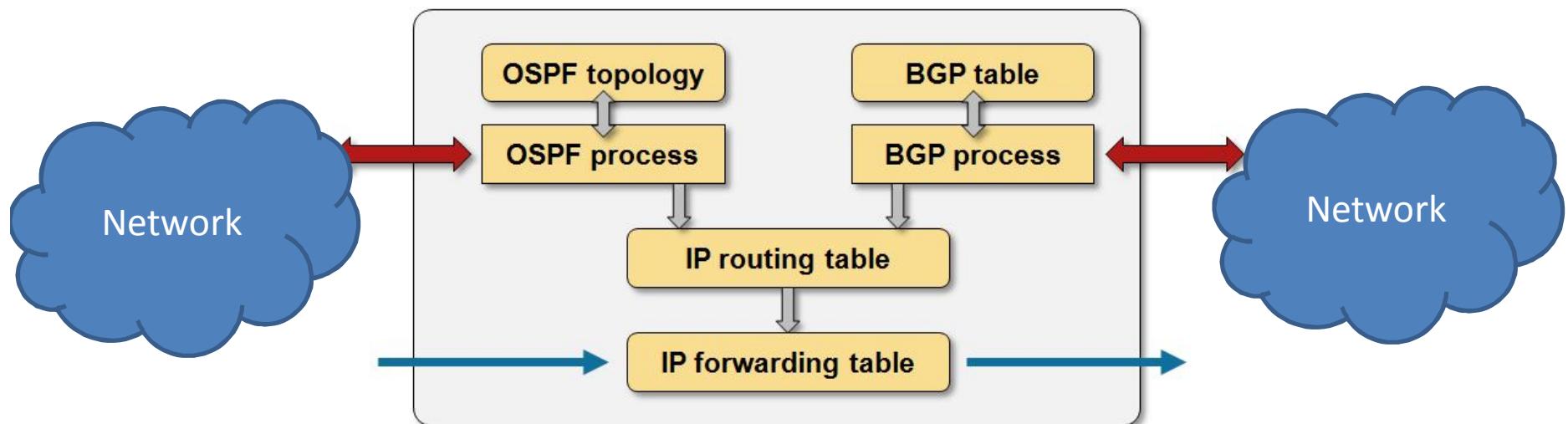


Routing

- **Routing** → proses untuk meneruskan paket-paket dari sebuah jaringan ke jaringan lainnya melalui internetwork device (router).
- **Static routing** → administrator melakukan routing secara manual. Mendefenisikan setiap network tujuan dan gateway yang dilaluinya pada setiap router-router yang akan digunakan.
- **Dinamic routing** → administrator hanya melakukan sedikit konfigurasi (mengaktifkan fungsi dinamic routing) pada setiap router, router-router tersebut otomatis mencari route dan gateway terbaik dari semua network yang terhubung.

Komponen Routing

- RIB (Routing Information Base) / Routing Table
- FIB (Forwarding Information Base) / Forwarding Table



Router Information Base (RIB)

- RIB/Tabel Routing adalah tabel data dalam router yang berisi daftar rute ke jaringan/network tertentu
- RIB juga berisi metric (nilai/prioritas) dari masing-masing rute.
- RIB terbentuk dari:
 - Semua rute yang terbentuk dari dynamic routing protocol
 - Semua rute untuk connected network, dan
 - Setiap konfigurasi rute tambahan seperti static route

RIB / Routing Table

- IP>Route>List

The screenshot shows the 'Route List' window from the Winbox interface. The window has a blue header bar with the title 'Route List'. Below the header is a navigation bar with tabs: 'Routes' (selected), 'Nexthops', 'Rules', and 'VRF'. To the right of the tabs are buttons for 'Find' and 'all'. The main area is a table with columns: 'Dst. Address', 'Gateway', and 'Distance'. The table contains 14 rows of route entries. Most entries have a red arrow icon next to the destination address. Some entries show 'reachable' or 'etherX' status. The 'Distance' column shows values like 0, 110, 120, and 1.

	Dst. Address	Gateway	Distance
DAC	▶ 1.1.1.1	bridge1 reachable	0
DAo	▶ 2.2.2.2	12.12.12.2 reachable ether2	110
DAo	▶ 3.3.3.3	12.12.12.2 reachable ether2	110
AS	▶ 10.10.10.0/24	192.168.0.2 reachable ether1	1
DAC	▶ 11.11.11.0/24	ether5 reachable	0
DAC	▶ 12.12.12.0/24	ether2 reachable	0
DAr	▶ 14.0.0.0/8	11.11.11.2 reachable ether5	120
DAr	▶ 14.14.14.0/24	11.11.11.2 reachable ether5	120
DAo	▶ 23.23.23.0/24	12.12.12.2 reachable ether2	110
DAC	▶ 192.168.0.0/24	ether1 reachable	0
DAo	▶ 192.168.2.0/24	12.12.12.2 reachable ether2	110
DAo	▶ 192.168.3.0/24	12.12.12.2 reachable ether2	110

Fungsi RIB

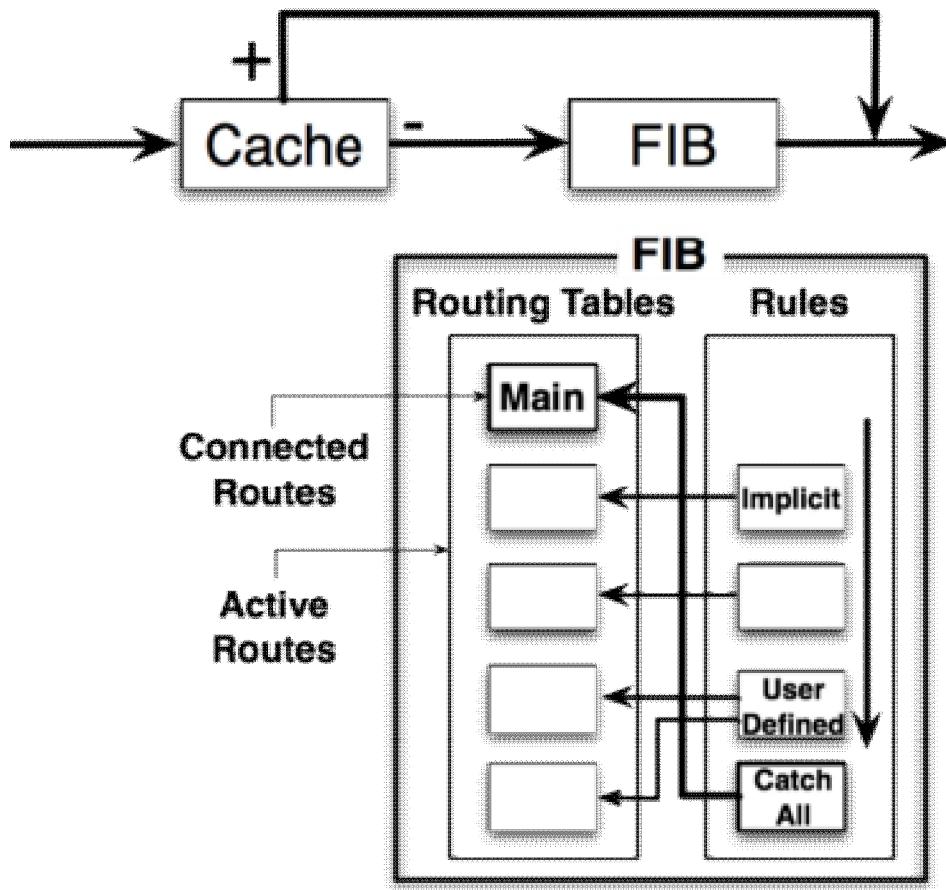
RIB digunakan untuk:

- Memfilter informasi routing dari semua jenis routing protocol
- Mengkalkulasi dan memilih route terbaik ke network tertentu.
- Membuat dan mengupdate Forwarding Information Base (FIB)
- Mendistribusikan informasi routing ke routing protokol lainnya

Forwarding Information Base (FIB)

- RIB/Tabel routing umumnya tidak digunakan secara langsung untuk forwarding/meneruskan paket di router arsitektur modern.
- RIB digunakan untuk menghasilkan informasi untuk tabel forwarding yang lebih kecil.
- Sebuah tabel forwarding hanya berisi rute yang dipilih oleh algoritma routing sebagai jalur pilihan untuk meneruskan paket, atau route yang sering digunakan.
- Hal ini sering dalam bentuk cache format terkompresi atau pre-compiled yang dioptimalkan untuk perangkat keras penyimpanan dan pencarian.

Forwarding Information Base (FIB)

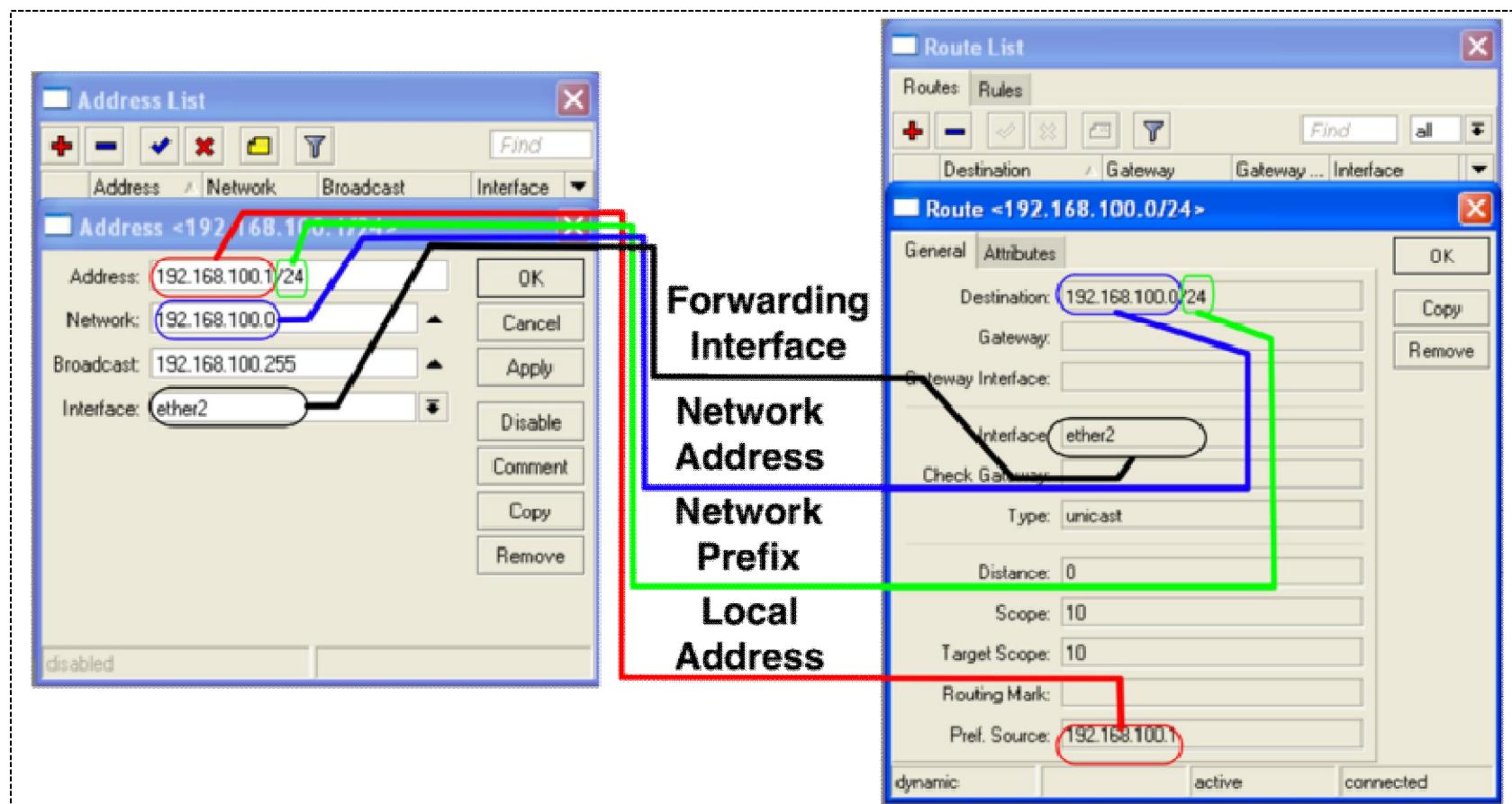


- FIB adalah hasil olahan dari RIB yang telah terfilter
- Merupakan informasi routing yang disimpan dalam cache
- Secara default (bila tidak ada “routing mark” yang digunakan) semua rute aktif akan ada pada tabel routing utama (main).
- Hanya ada satu rule implisit yang tersembunyi (rule “catch all”) yang menggunakan tabel utama untuk semua pencarian routing.

Connected Route

- Dibuat secara otomatis setiap kali kita menambahkan sebuah IP Address pada interface yang valid (interface yang aktif).
- Jika terdapat **dua buah IP Address** yang berasal dari subnet yang sama pada **sebuah interface**, hanya akan ada **1 connected route**.
- Jangan menempatkan **dua ip address** dari **subnet yang sama** pada **dua interface yang berbeda**, karena akan membingungkan tabel dan logika routing di router.

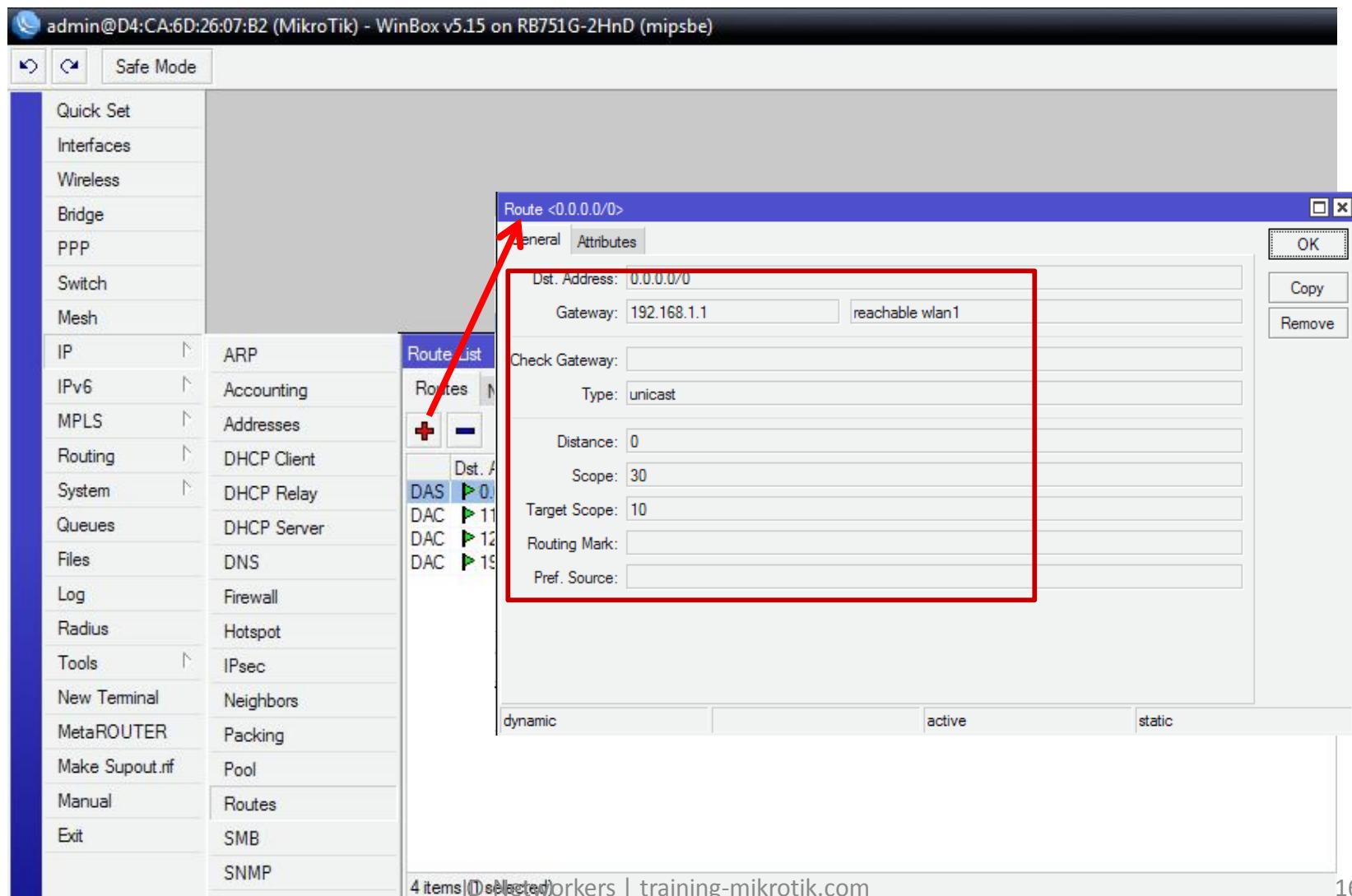
Connected Route



Static Route

- Static route dibuat dengan menambahkan route secara manual pada routing table.
- Pada static route yang ditambahkan adalah network tujuan dan gatewaynya.
- Dapat dikatakan kita mendefinisikan route mau ke network yang mana, lewat gateway mana.

Menambahkan Routing



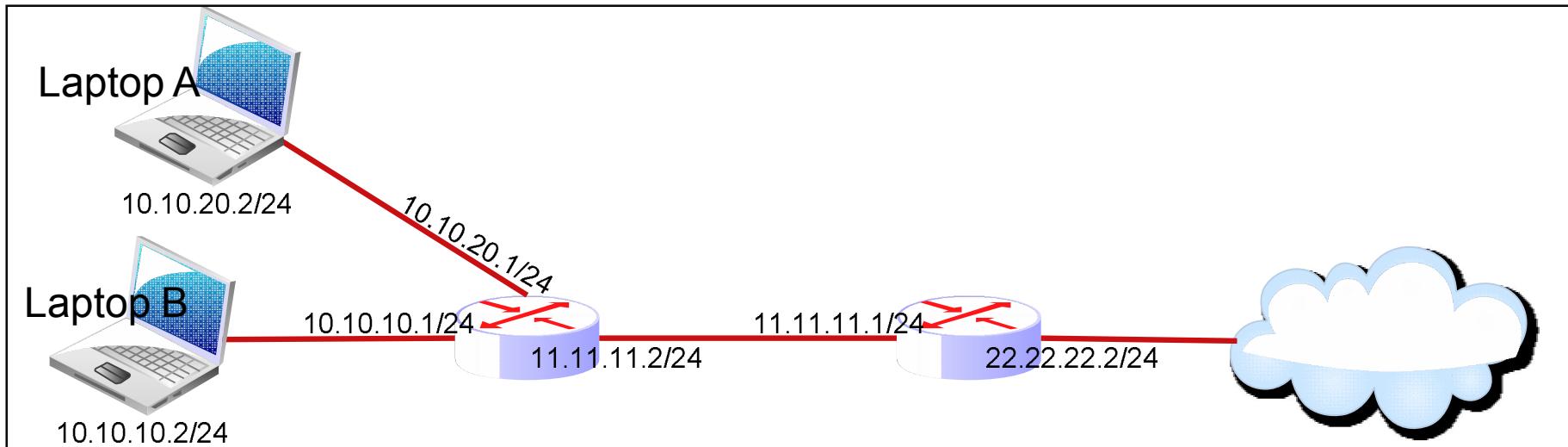
Route Parameter

- Destination
 - ✓ Destination address & network mask
 - ✓ 0.0.0.0/0 -> ke semua network
- Gateway
 - ✓ IP Address gateway, harus merupakan IP address yang satu subnet dengan IP yang terpasang pada salah satu interface router
 - ✓ Gateway berupa Interface digunakan apabila IP gateway tidak diketahui dan bersifat dinamik (hanya point to point/serial connection).
- Pref Source
 - ✓ source IP address dari paket yang akan meninggalkan router,
 - ✓ Biasanya adalah ip address yang terpasang di interface yang menjadi gateway.
- Distance
 - ✓ Jarak, digunakan perhitungan pemilihan route.
- Scope & Target Scope
 - ✓ Digunakan untuk recursive nexthoplookup

Gateway & Default Gateway

- Static Routing dilakukan dengan pengaturan arah paket data yang melalui router, dengan menentukan **gateway** untuk **dst-address/network** tertentu
- Gateway bisa berupa : **IP Address** atau **Interface**
- **IP Gateway** router harus **satu subnet** dengan **salah satu IP interface router**
- Hanya ada 1 gateway untuk suatu network tujuan
- Router akan memilih gateway untuk network tujuan yang lebih spesifik (netmask lebih besar)
- **Default gateway** adalah pengaturan untuk dst-address 0.0.0.0/0, karena ip 0.0.0.0/0 menggantikan semua ip yang ada di internet.

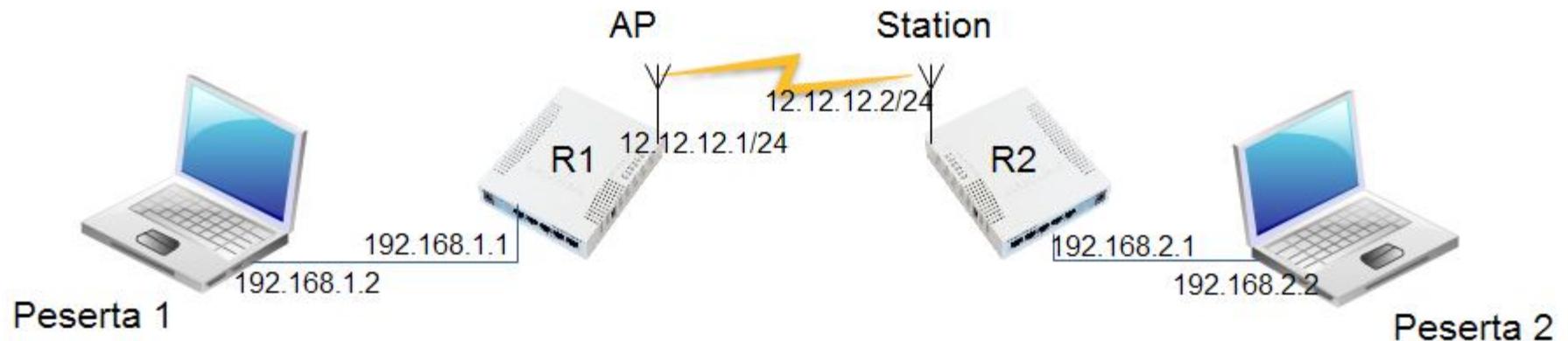
Latihan



IP Gateway router **HARUS SATU SUBNET** dengan **salah satu IP interface router**

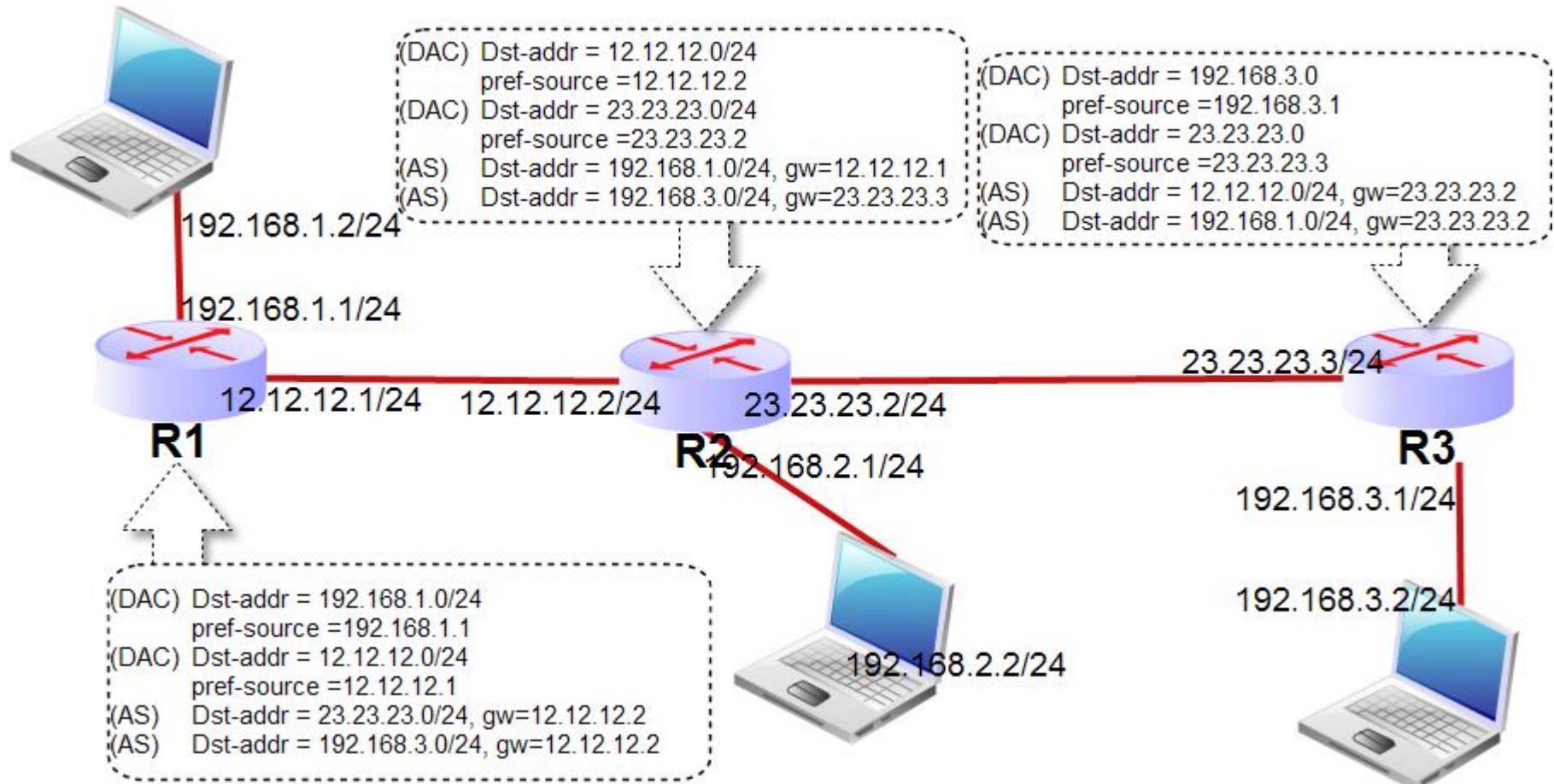
- Pada Laptop A , IP gateway ke network 11.11.11.0/24 berapa?
- Pada Laptop A, IP gateway ke network 22.22.22.0/24 berapa?
- Pada Laptop A, IP default gateway berapa?
- Pada R1, IP gateway ke network 22.22.22.0/24 berapa?
- Pada R1, IP Default Gateway adalah ?
- Pada R2, IP gateway ke network Laptop A berapa?

LAB I – Static Routing



- Reset konfigurasi router (no default)
- Koneksikan laptop antar peserta sesuai dengan topologi diatas
- Buatlah static routing di masing-masing router & laptop.
- Ping antar laptop.

LAB I – Static Routing



Load Balancing & Fail Over

- **Load Balancing** adalah teknik untuk mendistribusikan beban kerja di dua atau lebih link jaringan untuk memaksimalkan throughput, meminimalisasi response time, dan menghindari overload.
- **Fail Over** adalah sistem proteksi untuk menjaga apabila link utama terganggu, secara otomatis akan memfungsikan jalur cadangan (link kedua, ketiga, dst)

Jenis Load Balancing

- Per Packet Load Balancing
 - Pada MikroTik menggunakan fitur bernama Interface Bonding
 - Pembagian beban berdasarkan packet-packet (packet 1 lewat gateway a, packet 2 lewat gateway b)
- Per Connection Load Balancing
 - Menggunakan fitur Mikrotik Bernama NTH di IP mangle
 - Pembagian beban berdasarkan koneksi (koneksi 1 lewat gateway a, koneksi ke 2 lewat gateway b)
- Per address-pair connection Load Balancing
 - Fitur ECMP dan PCC (Peer Connection Classified)
 - Pebagian traffik berdasarkan koneksi dan IP address asal dan tujuan dari koneksi tersebut
- Custom Load Balancing (Policy Routing -> route mark)

Equal Cost Multi Path (ECMP)

Route <0.0.0.0/0>

General Attributes

Dst. Address: 0.0.0.0/0

Gateway: 13.13.13.10 reachable ether3
12.12.12.10 reachable ether2
12.12.12.10 reachable ether2

Check Gateway:

Type: unicast

Distance: 1

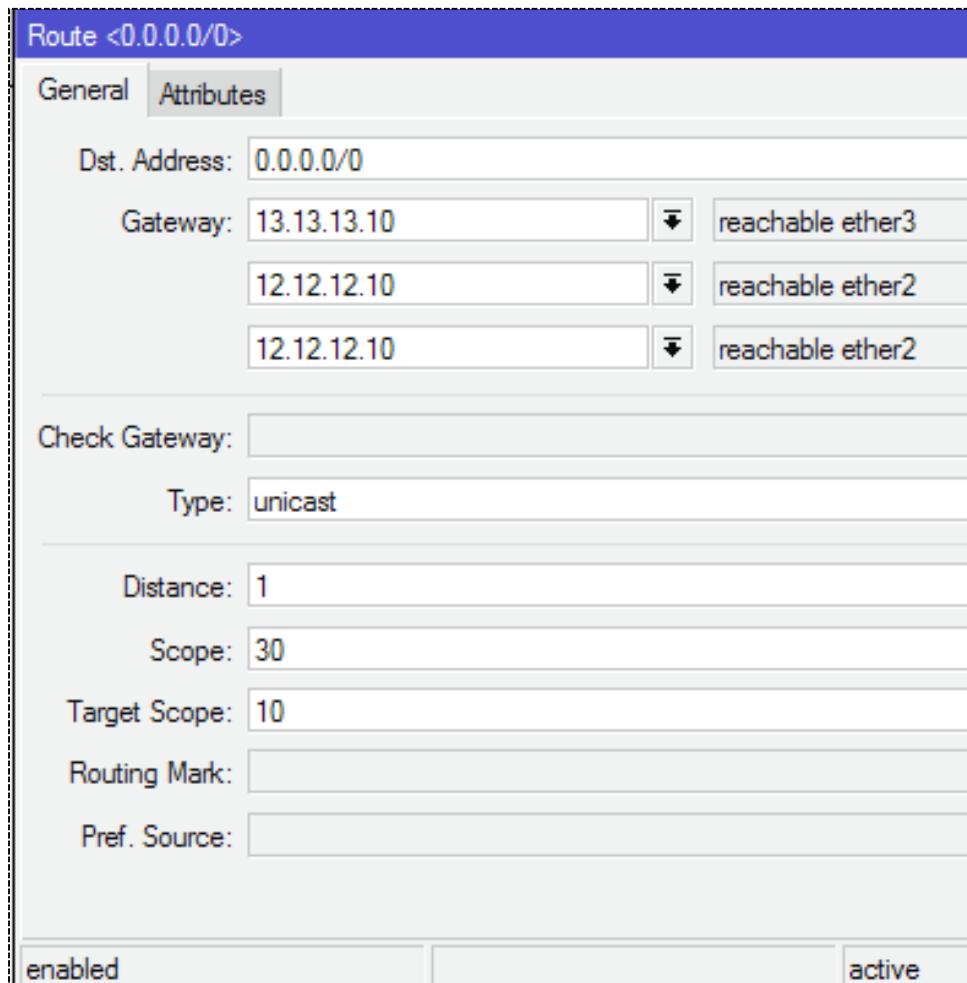
Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

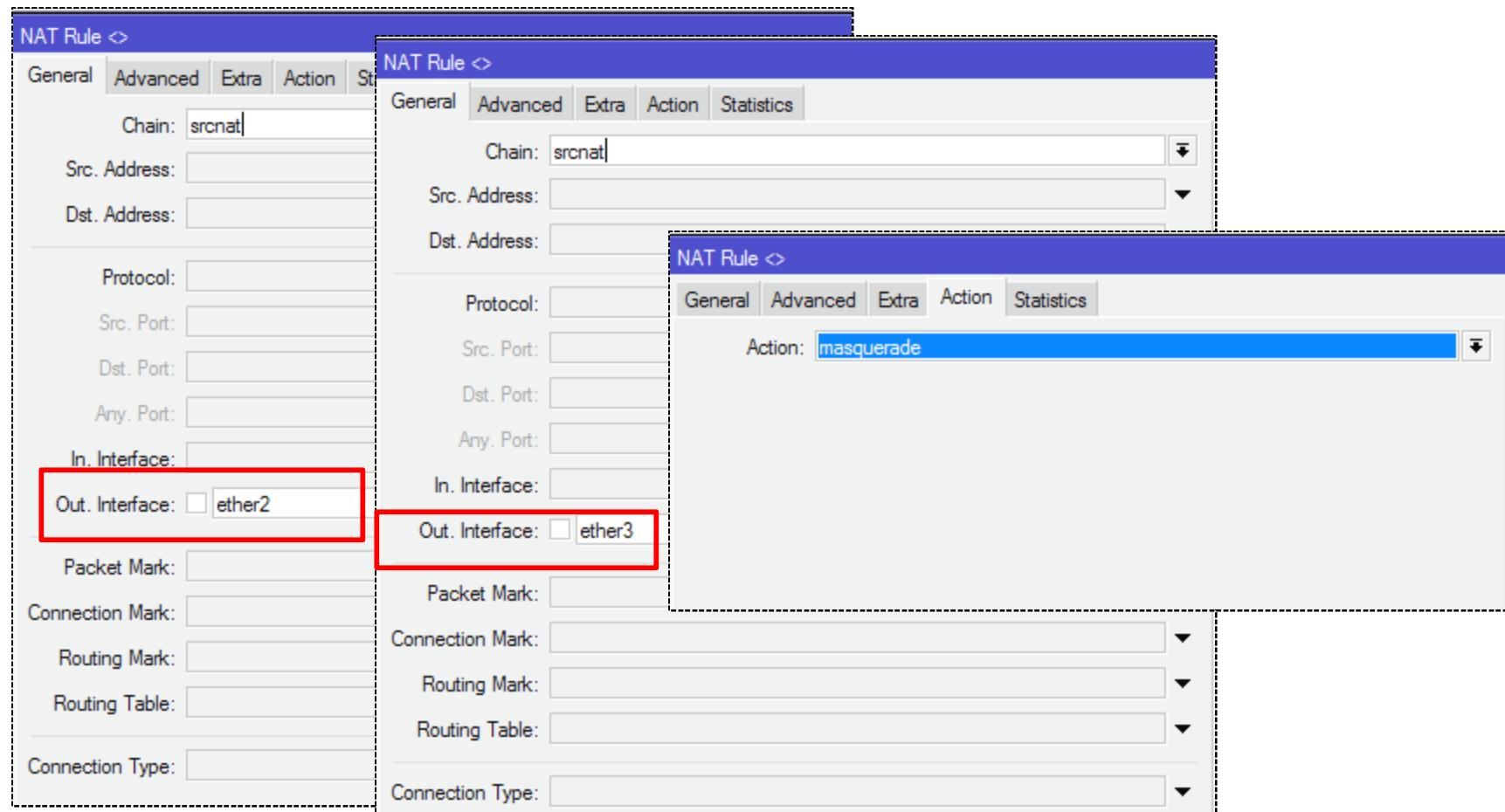
enabled active



- ECMP memungkinkan router memiliki lebih dari 1 gateway untuk 1 network tujuan.
- Masing-masing gateway pada ECMP akan dipilih berdasarkan algoritma Round Robin dari kombinasi SRC/DST address
- Gateway yang sama dapat ditulis berulang-ulang

ECMP Load Balancing

- Konfigurasi router ECMP (NAT Masquerade)



ECMP Load Balancing

- Konfigurasi router ECMP (IP Route)

The screenshot shows the Winbox interface for managing routes on a MikroTik router. A red arrow points from the 'Route List' window to the 'Route <0.0.0.0/0>' details window.

Route List (Left):

- Shows a list of routes:

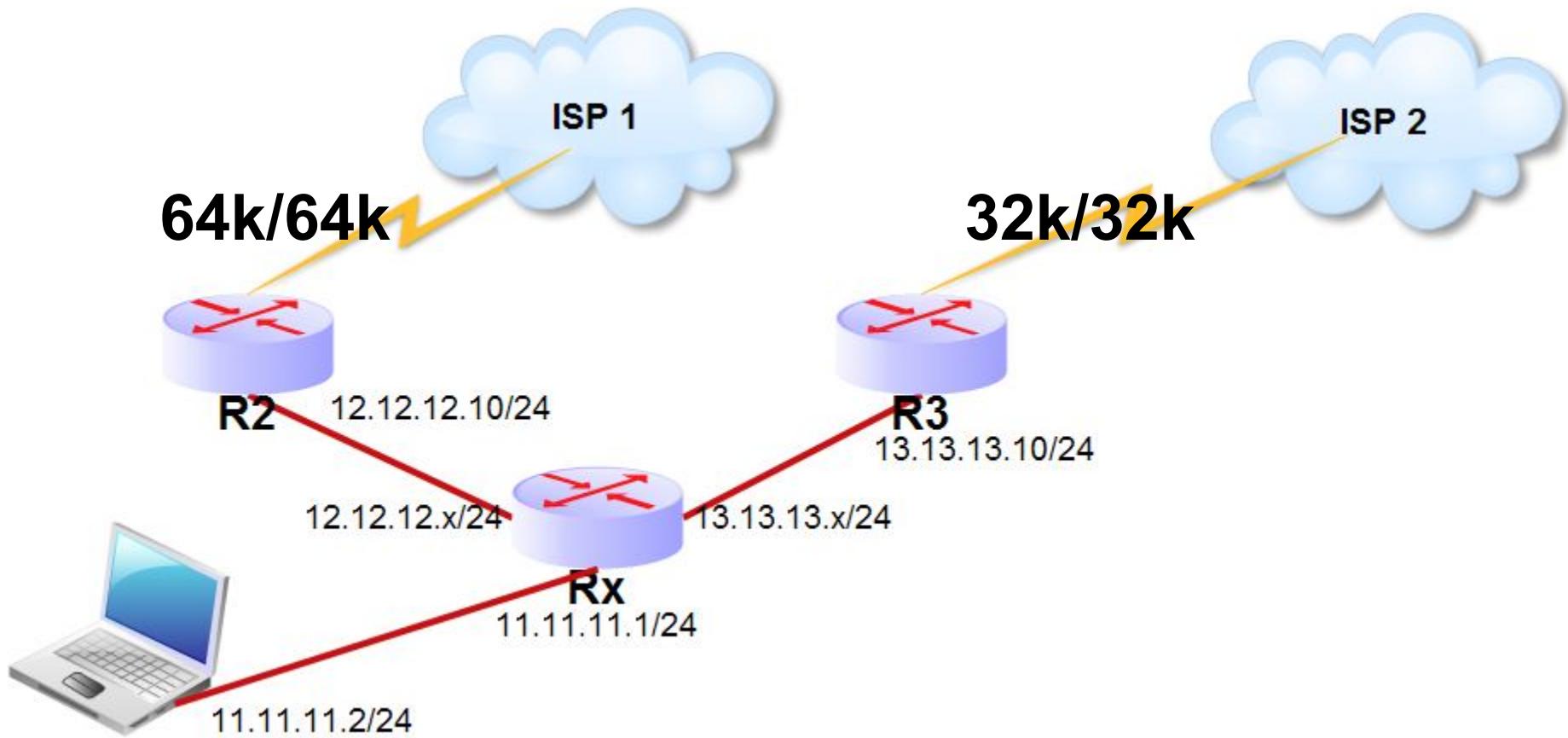
 - AS (0.0.0.0/0) via 13.13.13.10 (reachable via ether3) and 12.12.12.10 (reachable via ether2).
 - DAC (12.12.12.0/24) via ether2 (reachable).
 - DAC (13.13.13.0/24) via ether3 (reachable).
 - DAC (192.168.1.0/24) via ether1 (reachable).

Route <0.0.0.0/0> (Right):

- General Tab:**
 - Dst. Address: 0.0.0.0/0
 - Gateway: 13.13.13.10 (reachable via ether3)
 - Gateway: 12.12.12.10 (reachable via ether2)
 - Check Gateway: (empty)
 - Type: unicast
 - Distance: 1
 - Scope: 30
 - Target Scope: 10
 - Routing Mark: (empty)
 - Pref. Source: (empty)
- Attributes Tab:**
 - enabled
 - active

ECMP-Load Balancing

- Link ISP 1 = 64k/64k, Link ISP 2 =32k/32k



ECMP Load Balancing

- Status Link 1 dan Link 2 saat peak traffik

The image displays two separate WinBox windows, each showing the 'Queue List' configuration for a specific router.

Router ISP 1 (Top Window):

- Queue List: Simple Queues tab selected.
- Buttons: +, -, ✓, ✘, ⚡, ⚡, Find.
- Counters: 00 Reset Counters, 00 Reset All Counters.
- Table:

#	Name	Target Address	Rx Max Limit	Tx Max Limit	Packet ...
0	queue1	12.12.12.200	64k	64k	

Router ISP 2 (Bottom Window):

- Queue List: Simple Queues tab selected.
- Buttons: +, -, ✓, ✘, ⚡, ⚡, Find.
- Counters: 00 Reset Counters, 00 Reset All Counters.
- Table:

#	Name	Target Ad...	Rx Max Limit	Tx Max Limit	Packet ...
0	queue1	13.13.13.2...	32k	32k	

ECMP Load Balancing

- Apabila ada dua gateway, Link A (64k) dua kali lebih besar dari Link B (32k), A:B = 64k:32k, atau 2:1, total A+B=3
- Gateway ditulis 3 kali = dengan perbandingan 2x untuk gateway A + 1x untuk gateway B

Route <0.0.0.0/0>

General	Attributes
Dst. Address:	0.0.0.0/0
Gateway:	13.13.13.10 reachable ether3
	12.12.12.10 reachable ether2
	12.12.12.10 reachable ether2
Check Gateway:	

ECMP Load Balancing

- Bagaimana kalau salah satu gatewaynya putus? Apakah koneksi dari laptop ke internet masih bisa?

Administrative Distance

- Administrative Distance (Distance) digunakan untuk memilih jalur terbaik ketika terdapat dua atau lebih rute/routing protocol yang berbeda ke tujuan yang sama.
- Nilai dari distance adalah (0-255) dan secara default telah tersetting pada setiap protocol routing yang digunakan.
- Distance yang lebih kecil akan lebih diprioritaskan dalam pemilihan tabel routing
 - Connected routes : 0
 - Static Routes : 1
 - eBGP: 20
 - OSPF: 110
 - RIP : 120
 - MME : 130
 - iBGP: 200
- Route dengan distance 255 adalah route yang direject oleh route filter

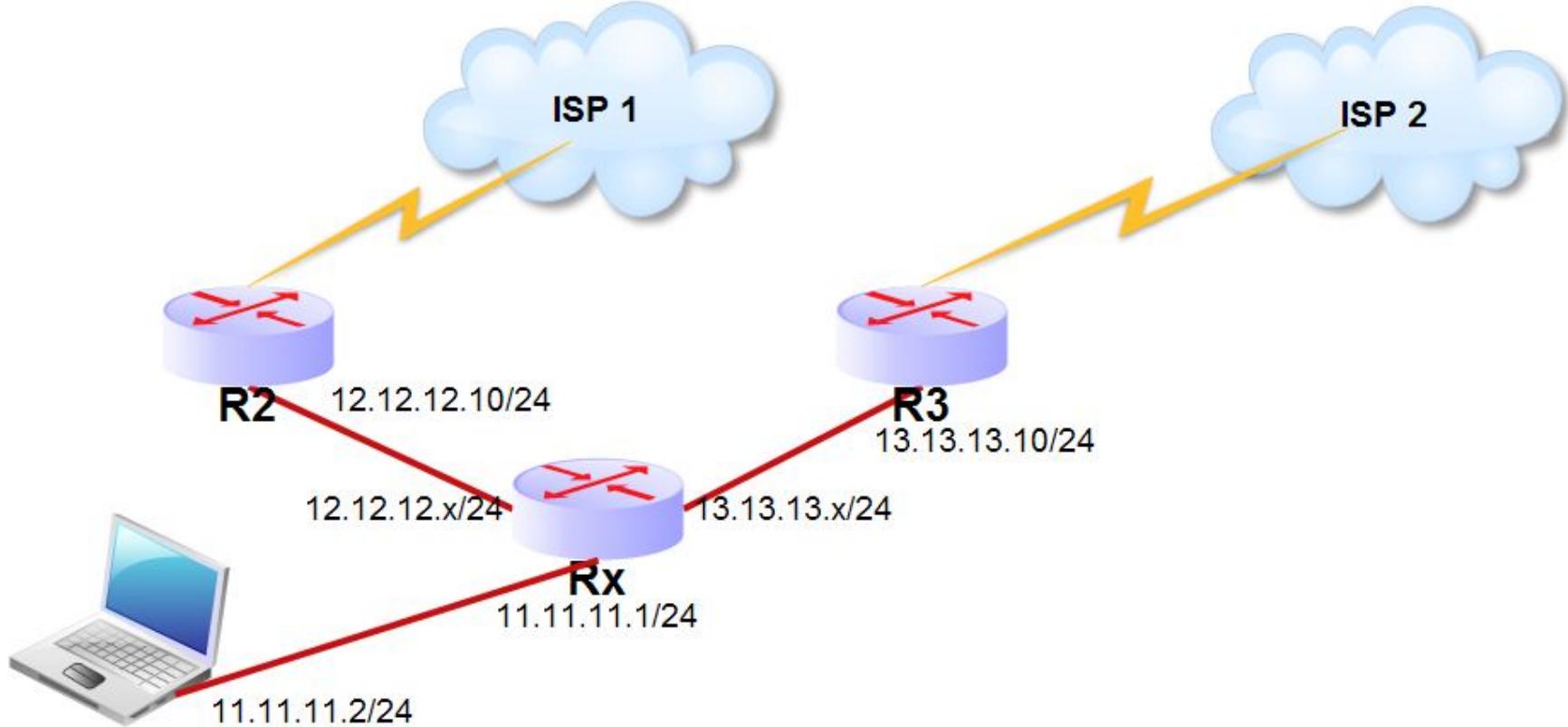
Route “Distance” Option

• Lihatnya di IP>Routes

The image shows the Winbox interface for managing routes. On the left, the 'Route <0.0.0.0/0>' dialog is open, showing settings for a default route: Dst. Address: 0.0.0.0/0, Gateway: 192.168.1.1, Type: unicast, and Distance: 1. The 'Distance' field is highlighted with a red box. On the right, the 'Route List' window displays a list of routes, also highlighting the 'Distance' column with a red box. The routes listed are:

	Dst. Address	Gateway	Distance
DAC	► 1.1.1.1	bridge1 reachable	0
DAo	► 2.2.2.2	12.12.12.2 reachable ether2	110
DAo	► 3.3.3.3	12.12.12.2 reachable ether2	110
AS	► 10.10.10.0/24	192.168.0.2 reachable ether1	1
DAC	► 11.11.11.0/24	ether5 reachable	0
DAC	► 12.12.12.0/24	ether2 reachable	0
DAr	► 14.0.0.0/8	11.11.11.2 reachable ether5	120
DAr	► 14.14.14.0/24	11.11.11.2 reachable ether5	120
DAo	► 23.23.23.0/24	12.12.12.2 reachable ether2	110
DAC	► 192.168.0.0/24	ether1 reachable	0
DAo	► 192.168.2.0/24	12.12.12.2 reachable ether2	110
DAo	► 192.168.3.0/24	12.12.12.2 reachable ether2	110

LAB III, Distance



- Coba ubahlah pada salah satu router distance dari default routing aktif / yang sedang digunakan menjadi bernilai “2” dan untuk route yang non aktif tetap bernilai 1.

Option “Check-gateway”

- Adalah sebuah mekanisme pengecekan gateway yang dapat dilakukan oleh router mikrotik.
- Dikirimkan setiap 10 detik, menggunakan ARP request atau ICMP ping.
- Dianggap “Gateway time-out” jika tidak menerima respon dalam 10 detik dari mesin Gateway.
- Gateway dianggap “unreachable” jika terjadi 2 kali Gateway time-out berurutan.
- Jika mengaktifkan fitur check gateway untuk sebuah rule, maka akan berpengaruh juga untuk semua rule dengan gateway yang sama

Property	Description
<code>check-gateway (arp ping; Default: "")</code>	Periodically (every 10 seconds) check gateway by sending either ICMP echo request (<i>ping</i>) or ARP request (<i>arp</i>). If no response from gateway is received for 10 seconds, request times out. After two timeouts gateway is considered unreachable. After receiving reply from gateway it is considered reachable and timeout counter is reset.

Lab- ECMP Fail Over

- Pada IP route, tiap gateway dibuatkan route sendiri-sendiri
- Buat salah satu **distance** route lebih besar.
- Aktifkan option Check gateway hanya pada route dengan distance terkecil

Route <0.0.0.0/0>	
General Attributes	
Dst. Address:	0.0.0.0/0
Gateway:	12.12.12.10 reachable ether2
Check Gateway:	ping
Type:	unicast
Distance:	1
Scope:	30
Target Scope:	10
Routing Mark:	
Pref. Source:	

Route <0.0.0.0/0>	
General Attributes	
Dst. Address:	0.0.0.0/0
Gateway:	13.13.13.10 reachable ether3
Check Gateway:	
Type:	unicast
Distance:	2
Scope:	30
Target Scope:	10
Routing Mark:	
Pref. Source:	

Lab- ECMP Fail Over

- Check gateway hanya pada distance terkecil (active route)

Route List						
	Routes	Nexthops	Rules	VRF		
AS	► 0.0.0.0/0	12.12.12.10 reachable ether2	ping	1		
S	► 0.0.0.0/0	13.13.13.10 reachable ether3		2		
DAC	► 12.12.12.0/24	ether2 reachable		0		12.12.12.200
DAC	► 13.13.13.0/24	ether3 reachable		0		13.13.13.200
DAC	► 192.168.1.0/24	ether1 reachable		0		192.168.1.1

5 items (1 selected) ID-Networkers | training-mikrotik.com

Routing Policy

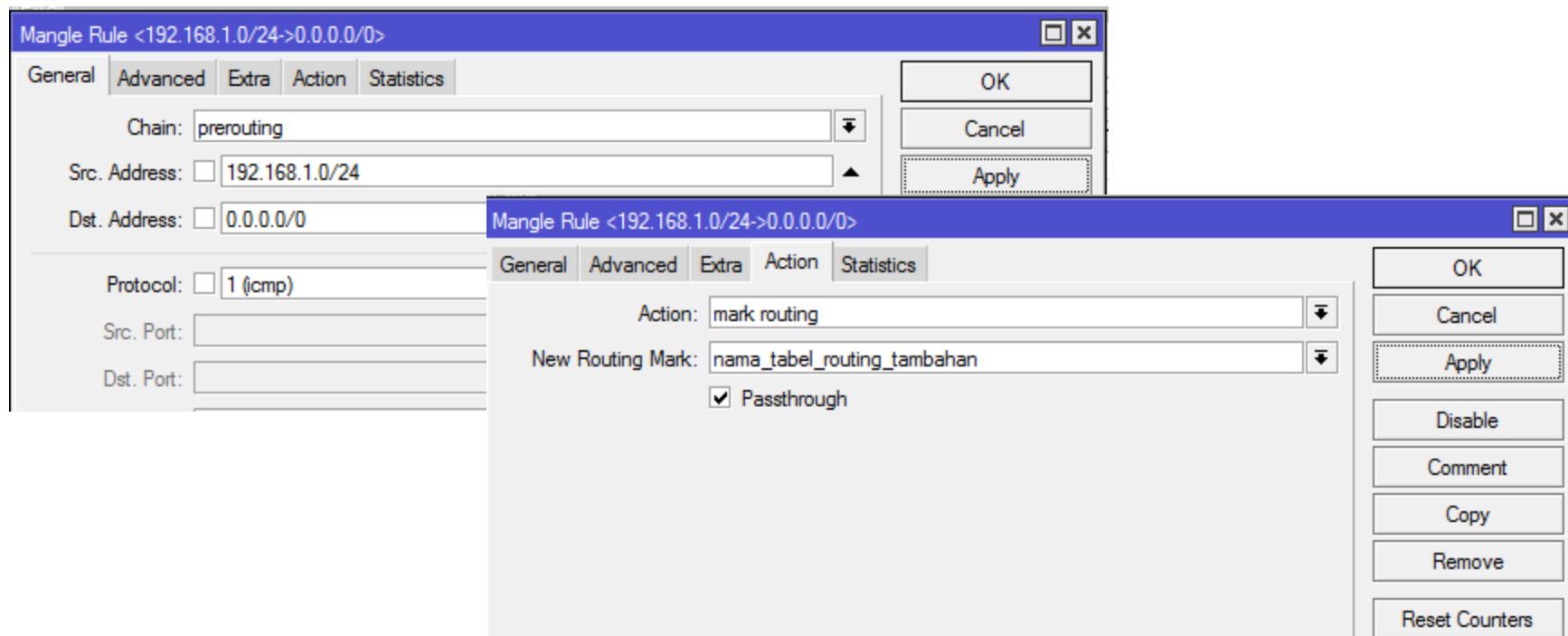
- Secara default, router akan menggunakan table routing “main” (utama)
- Kita bisa membuat table routing tambahan dan mengarahkan router menggunakan tabel tersebut dengan menggunakan:
 1. IP > Route > Rules
 2. IP > Firewall > Mangle > Route-mark
- Setiap routing mark yang dibuat membentuk routing table sendiri memiliki nama sama dengan nama routing marknya.

Routing Mark

- Untuk mengarahkan traffic yang lebih spesifik ke sebuah route, traffik tersebut harus diidentifikasi terlebih dahulu melalui routing mark (ada di IP Firewall Mangle)
- Untuk trafik yang melalui router menggunakan chain: **prerouting**
- Untuk trafik yang berasal dari/keluar router menggunakan mangle chain: **output**
- Setiap packet hanya dapat memiliki **satu routing mark**.
- Apabila (ada setidaknya 1) route yang memakai **routing mark** maka **traffik dengan routing mark tersebut akan diabaikan oleh routing table utama.**

Routing Mark

- IP>Firewall>Mangle



IP Route Rules

The screenshot shows two windows from the Winbox interface of a MikroTik router. The top window is titled "Route List" and has tabs for Routes, Nexthops, Rules, and VRF. The Rules tab is selected, showing a table with one rule entry:

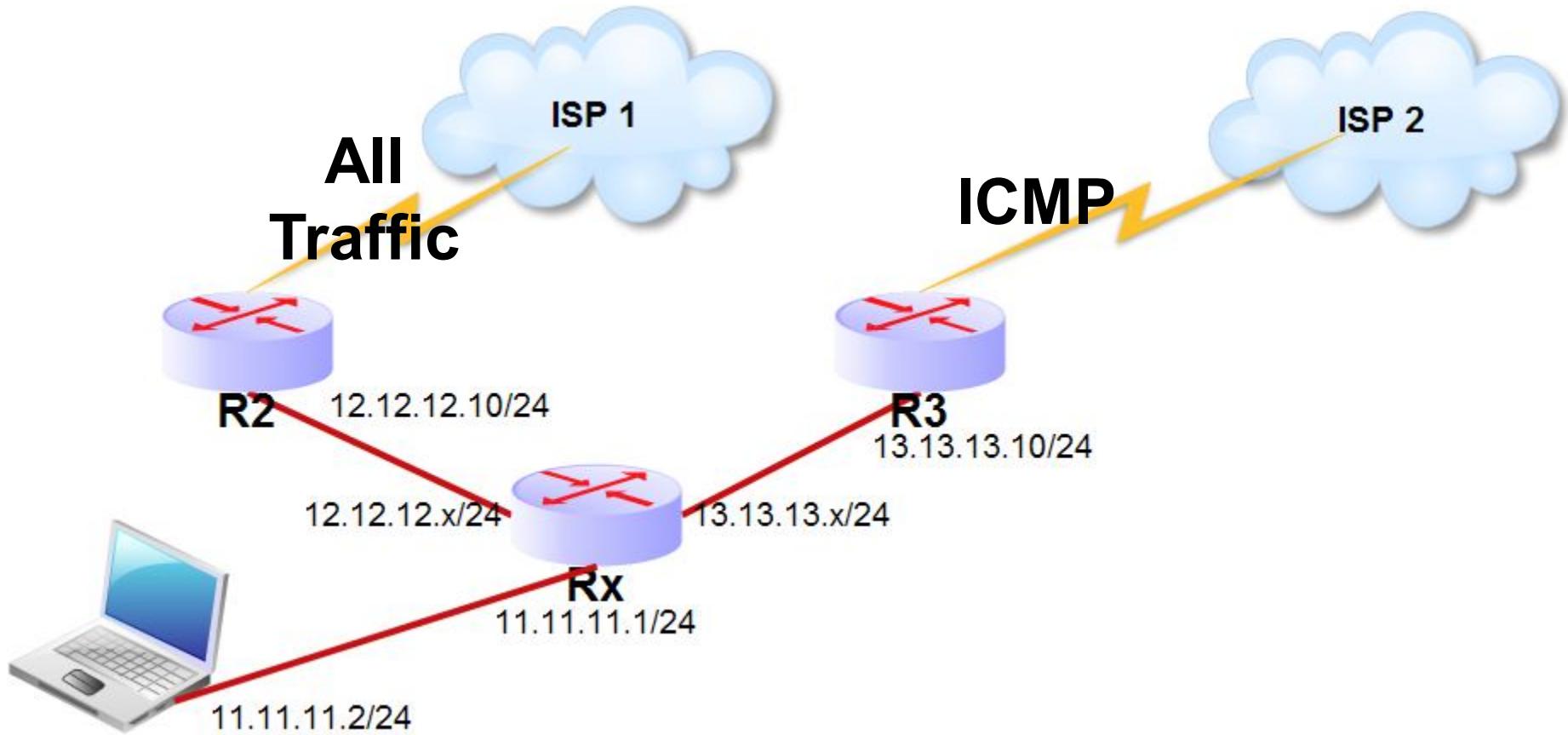
#	Src. Address	Dst. Address	Routing Mark	Interface	Action	Table
0	192.168.0.0...				lookup	table_1

A red arrow points from the "New Policy Routing Rule" button in the "Route List" window down to the "New Policy Routing Rule" dialog box. This dialog box is titled "New Policy Routing Rule" and contains fields for Src. Address (192.168.0.0/24), Dst. Address, Routing Mark, Interface, Action (lookup), and Table. The Table dropdown menu lists several options: main, non_main_routing_table, bukan_tabel_routing_main, and nama_tabel_routing_tambahan. The "bukan_tabel_routing_main" option is highlighted with a blue selection bar. The dialog box also includes OK, Cancel, Apply, Disable, Comment, Copy, and Remove buttons.

- Route rules mendefinisikan routing IP yang lebih spesifik dari network asal dan atau network tujuan.
- Dapat menggunakan mangle routing mark
- Tidak dilengkapi parameter routing lengkap (distance, pref.source dll).

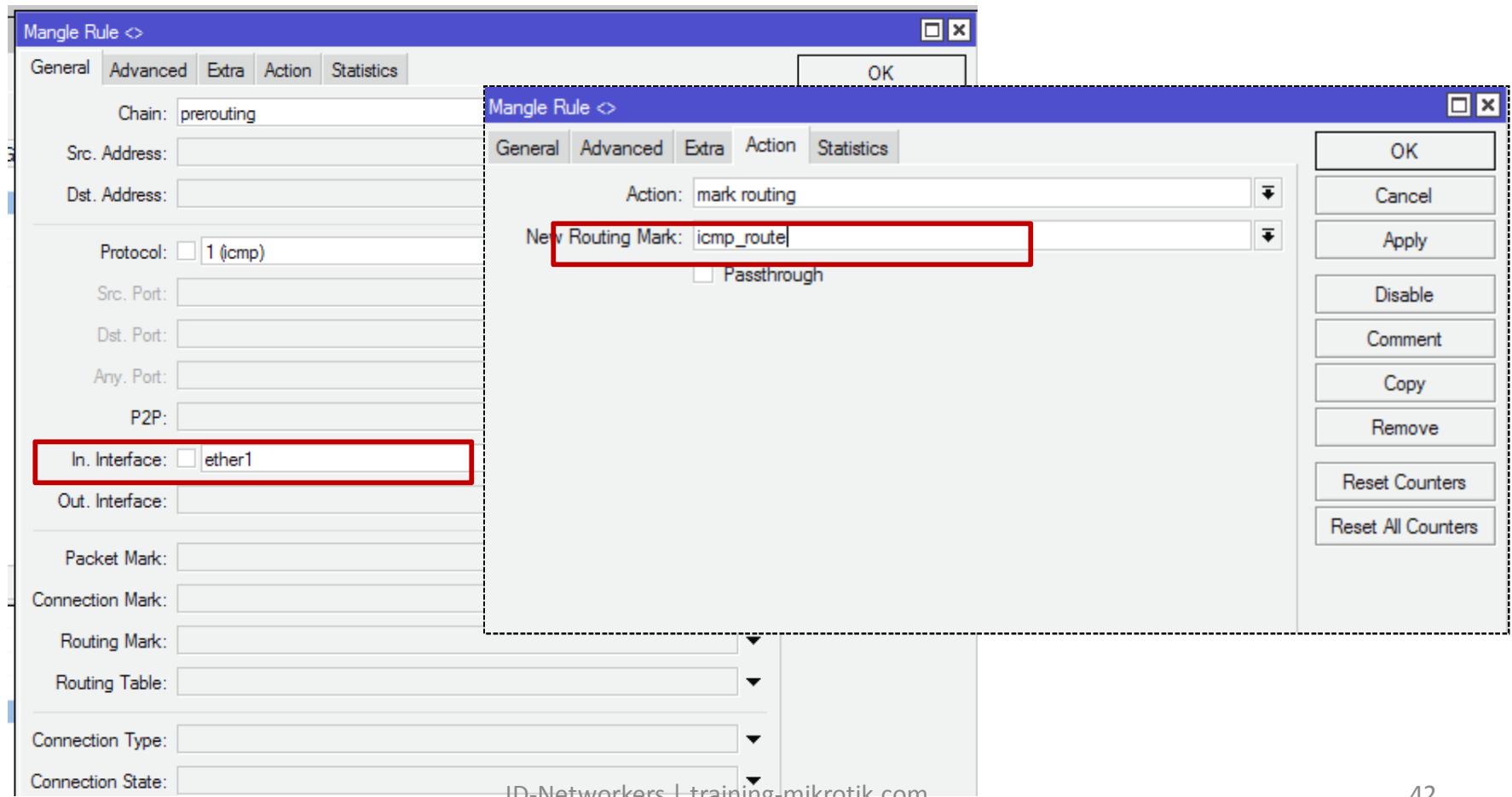
LAB ECMP-Routing Mark

- Paket ICMP (ping & traceroute) akan dilewatkan ISP 2



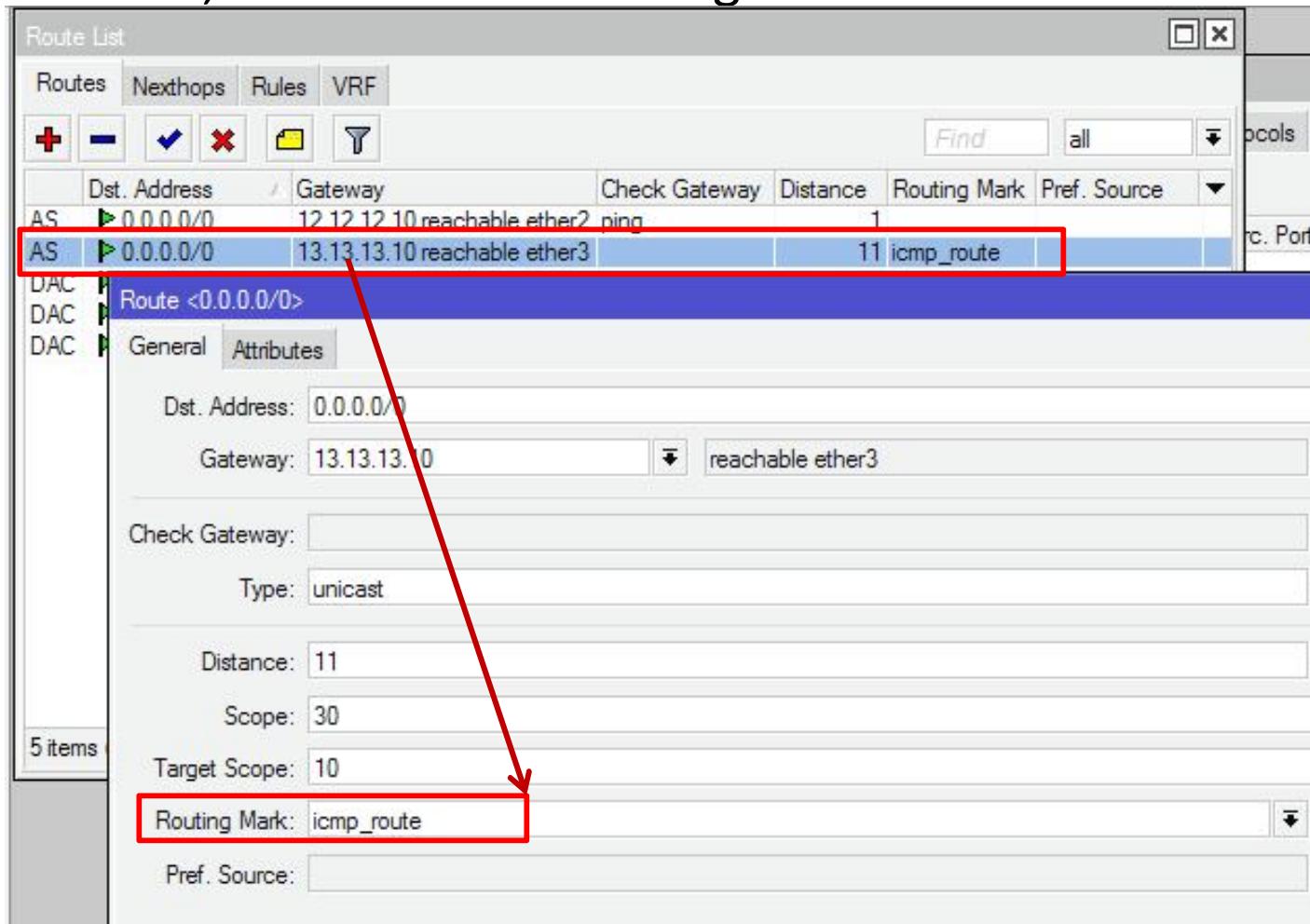
Lab- ECMP Routing Mark

- IP Firewall Mangle, membuat routing mark untuk ICMP packet



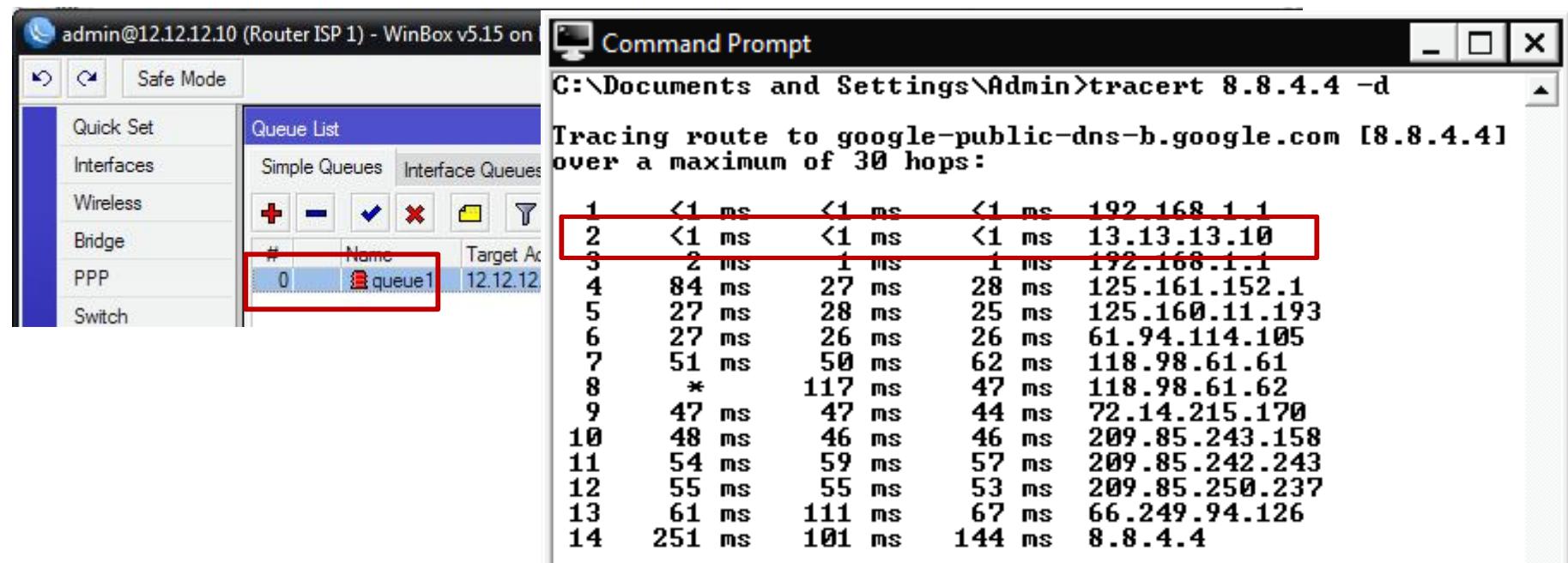
Lab- ECMP Routing Mark

- IP Route, memasukkan routing mark dalam route inactive



Super Lab- ECMP Routing Mark

- All traffic melewati link 1 (termasuk traffic web). Hanya paket icmp (traceroute & ping) akan dilewatkan link ke 2
- Cobalah lakukan ping keluar saat traffic full.



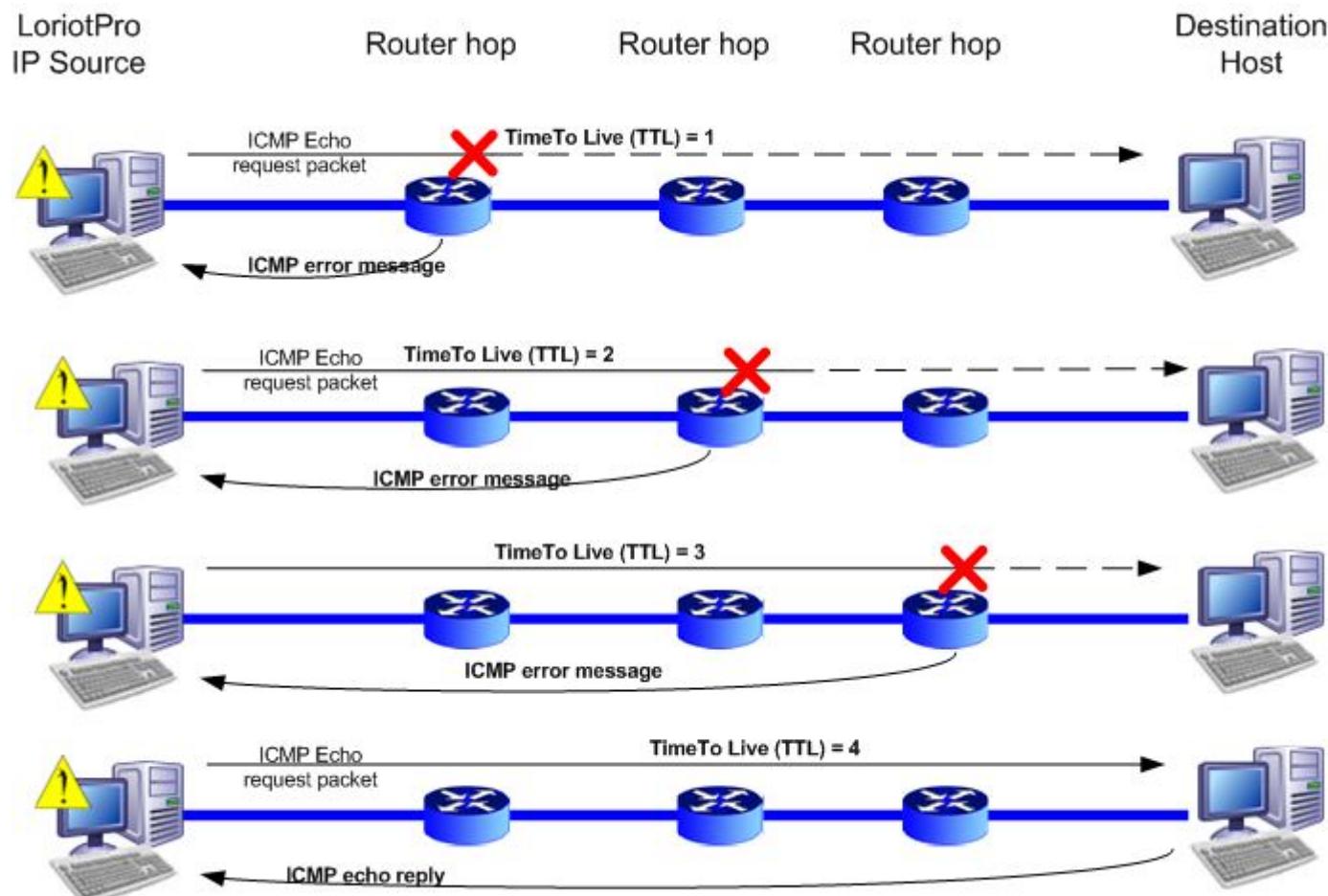
Kelemahan ECMP

- Forwarding table di Linux Kernel secara otomatis akan refresh setiap 10 menit
- Hal ini menyebabkan ada kemungkinan paket data untuk suatu aplikasi berganti koneksi sehingga mendapatkan masquerade address yang berbeda. Koneksi bisa terputus.

TTL (Time To Live)

- TTL adalah suatu nilai pada paket data (header IP) yang menyatakan berapa lama paket tersebut bisa beredar/berjalan -jalan dalam jaringan.
- Nilai tersebut akan memberitahukan kepada router apakah paket tersebut harus diteruskan ke router selanjutnya (next hop router) atau di-*discard*.
- Nilai default TTL adalah 64 (8bits) dan nilainya akan berkurang 1 setiap paket data melewati router (layer 3), beberapa saat sebelum *forwarded decision*.
- Router tidak akan melewaskan traffik ke route selanjutnya apabila TTL yang dia terima bernilai 1

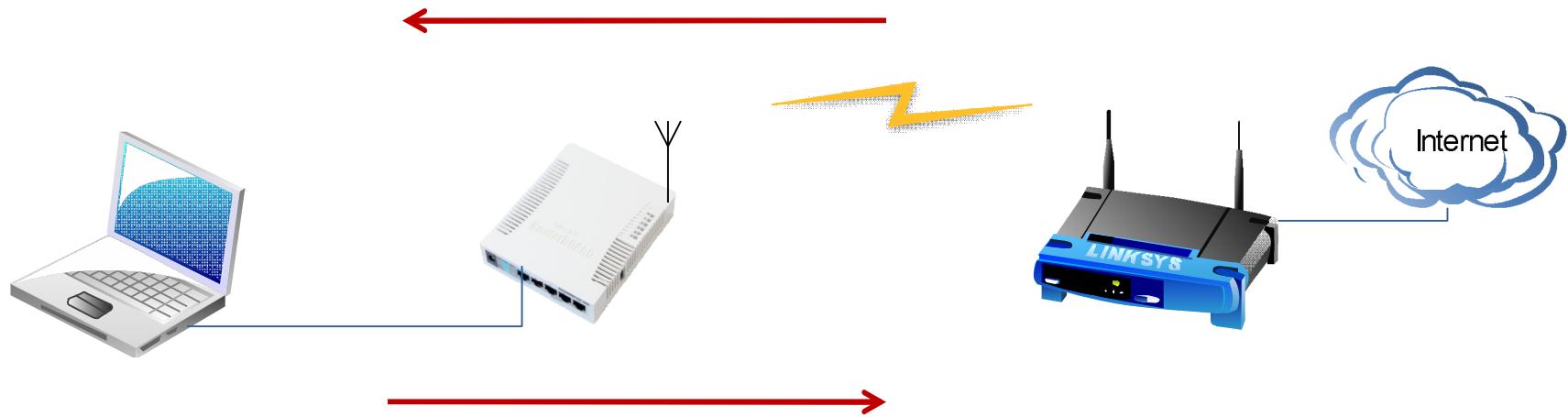
TTL (Time To Live)



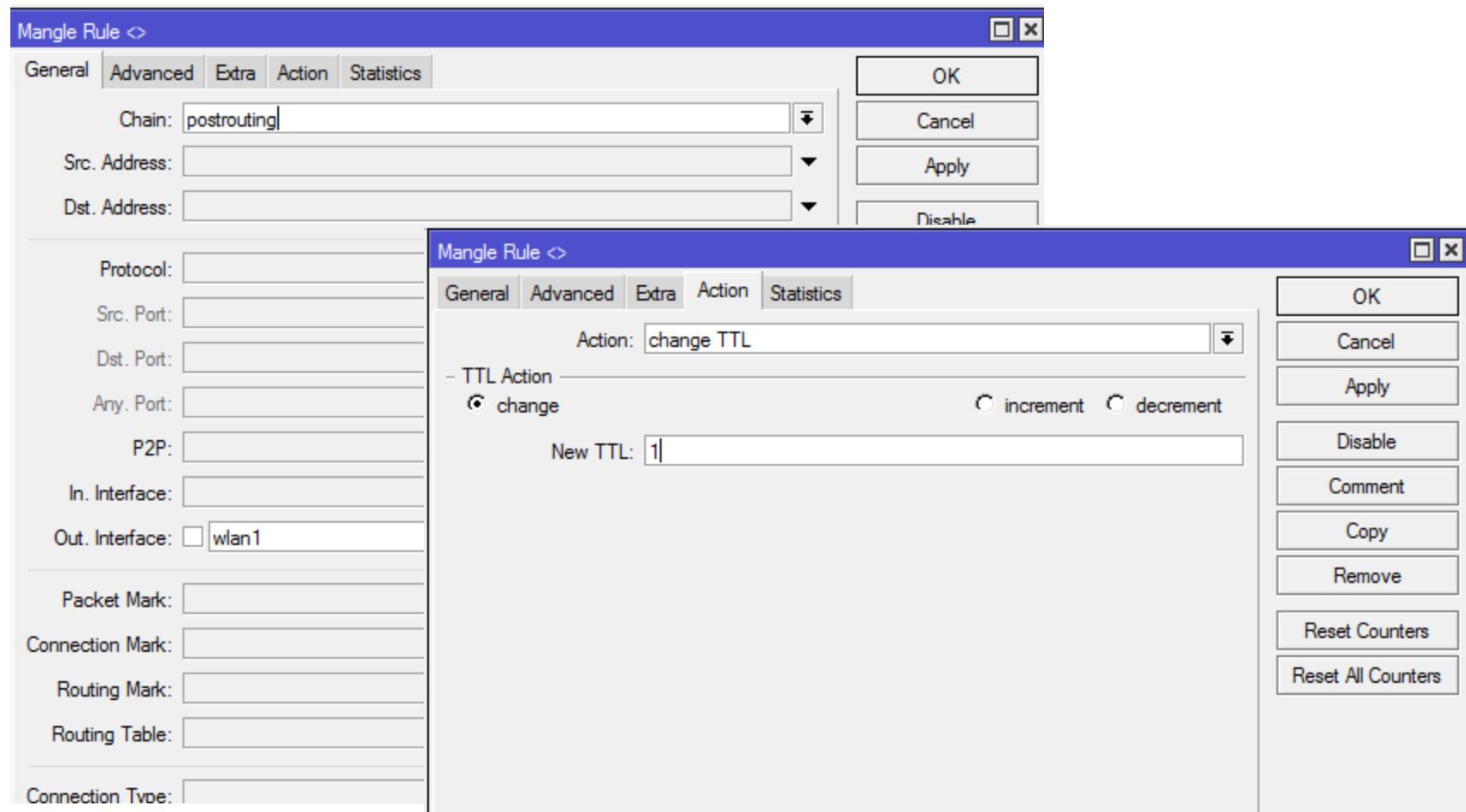
LUTEUS Copyrights 2008

LAB VI – Change TTL

- Kita bisa merubah nilai TTL kearah laptop maupun merubah nilai TTL yang kearah internet (IP 8.8.8.8)



LAB – Change TTL



LAB – Change TTL

- Menghitung jumlah hop dari nilai TTL reply

The image shows two Command Prompt windows side-by-side. The left window displays the output of a 'ping' command to 8.8.8.8. The right window displays the output of a 'tracert' command to google-public-dns-a.google.com (8.8.8.8) with the '-d' option.

Left Window (Ping Output):

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=88ms TTL=50
Reply from 8.8.8.8: bytes=32 time=63ms TTL=50
Reply from 8.8.8.8: bytes=32 time=64ms TTL=50
Reply from 8.8.8.8: bytes=32 time=57ms TTL=50

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 57ms, Maximum = 88ms, Average = 68ms

C:\>
```

Right Window (Tracert Output):

```
Command Prompt
Minimum = 57ms, Maximum = 88ms, Average = 68ms
C:\>tracert 8.8.8.8 -d

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:
1     1 ms      <1 ms      <1 ms      192.168.1.1
2     <1 ms      <1 ms      <1 ms      13.13.13.10
3      2 ms      2 ms      1 ms      192.168.1.1
4     30 ms      42 ms      39 ms      125.161.152.1
5     29 ms      30 ms      27 ms      125.160.11.193
6     33 ms      27 ms      26 ms      61.94.114.105
7     49 ms      51 ms      47 ms      118.98.61.61
8      *         45 ms      74 ms      118.98.61.62
9     47 ms      47 ms      46 ms      72.14.214.45
10    69 ms     145 ms      80 ms      209.85.243.158
11    57 ms      58 ms      58 ms      209.85.242.243
12    54 ms      55 ms      53 ms      209.85.250.237
13    66 ms      57 ms      67 ms      66.249.94.126
14    60 ms      54 ms      55 ms      8.8.8.8

Trace complete.

C:\>
```

A red box highlights the TTL values (50) in the ping reply section of the left window. A red arrow points from this box to a callout box containing the text: "Saat dikirim TTL nya 64, sisa TTL=50 Jumlah hop 64-50=14".

Scope & Target Scope

- Mekanisme Check gateway yang kita gunakan hanya bisa mendeteksi problem koneksi pada hoop (gateway) terdekat.
- Jika problem terjadi setelah gateway terdekat (nexthoop), check gateway tidak bisa mendeteksinya.
- Untuk mendeteksi problem koneksi yang terjadi setelah gateway terdekat, bisa digunakan teknik scope/target scope.

Scope & Target Scope

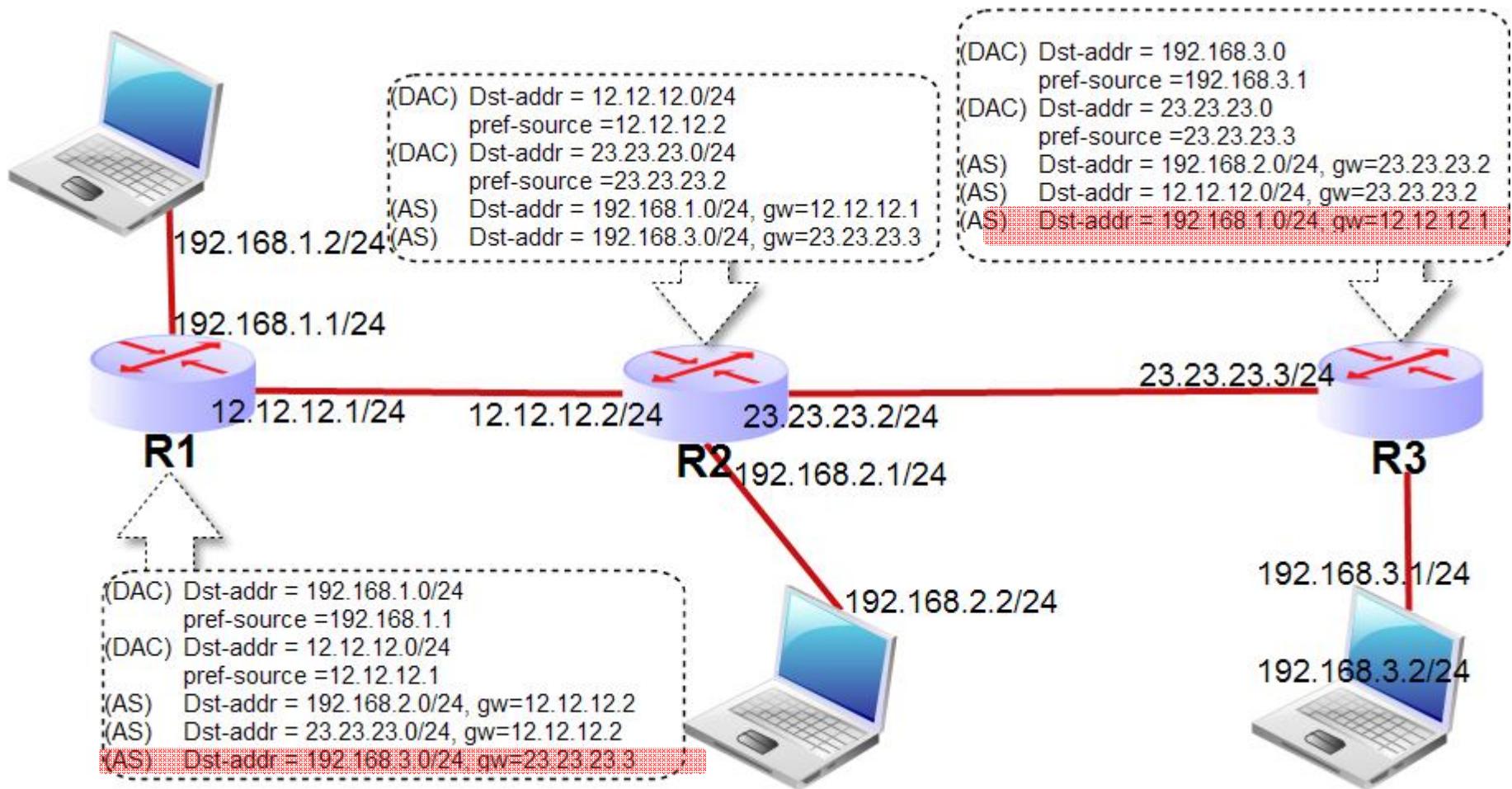
- Pada FIB router melakukan nexthop lookup, yaitu gateway (nexthop) yang dituju ada di interface yang mana.
- Route dapat meresolve nexthopnya hanya melalui rute lain yang memiliki scope lebih kecil atau sama dengan target scope dari rute tersebut.
- Target scope digunakan untuk static route yang dibuat recursive (gateway tidak terkoneksi langsung).
- Target Scope adalah nilai scope maksimum dari semua rute lainnya yang reachable.
- Kegunaan:
 - Bisa melakukan pemantauan check gateway ping untuk gateway yang tidak terhubung langsung
 - Dikombinasikan dengan iBGP (gateway tidak terhubung langsung)

Scope & Target Scope

- Nilai default scope & target scope

Scope	Route type	Target Scope
0		
10	Connected (running)	10
20	OSPF, R.P., MME	10
30	Static	10
40	eBGP	10
40	iBGP	30
200	Connected (not active)	

LAB VII – Recursive Next Hop



Route Type

Kita bisa melakukan blocking untuk network/dst-address tertentu menggunakan static route :

- Blackhole
 - Memblok dengan diam-diam
- Prohibit
 - Memblok dan mengirimkan pesan error ICMP administratively prohibited" (type 3 code 13)
- Unreachable
 - Memblok dan mengirimkan pesan error ICMP host unreachable" (type 3 code 1)

Ketiga tipe di atas tidak membutuhkan IP Address gateway.

Other Options

Route <0.0.0.0/0>

General Attributes

Dst. Address: 0.0.0.0/0

Gateway: 192.168.1.1 ↴ reachable ether1 ↴

Check Gateway:

Type: unicast ↴ blackhole ↴ prohibit ↴ unicast ↴ unreachable ↴

Distance:

Scope: 30

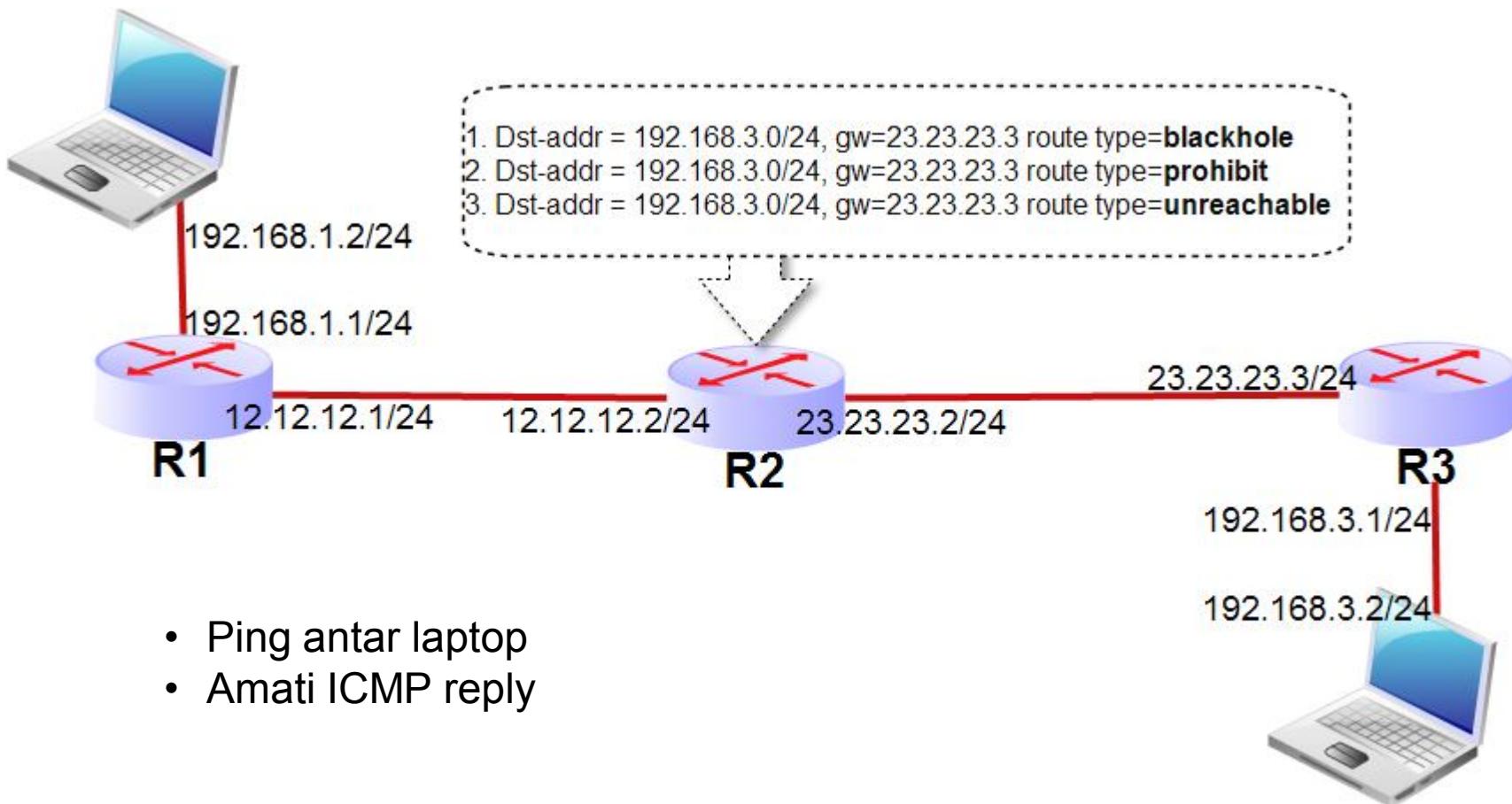
Target Scope: 10

Routing Mark:

Pref. Source:

The screenshot shows the 'Route' configuration window for a route with destination 0.0.0.0/0. The 'General' tab is selected. In the 'Type' field, 'unicast' is selected and highlighted with a red border. A dropdown menu is open, showing other options: 'blackhole', 'prohibit', 'unicast', and 'unreachable'. The 'blackhole' option is currently selected and highlighted with a blue background. Other fields include 'Gateway' (192.168.1.1), 'Check Gateway', 'Distance', 'Scope' (30), 'Target Scope' (10), 'Routing Mark', and 'Pref. Source'.

LAB VIII - Other Route Option



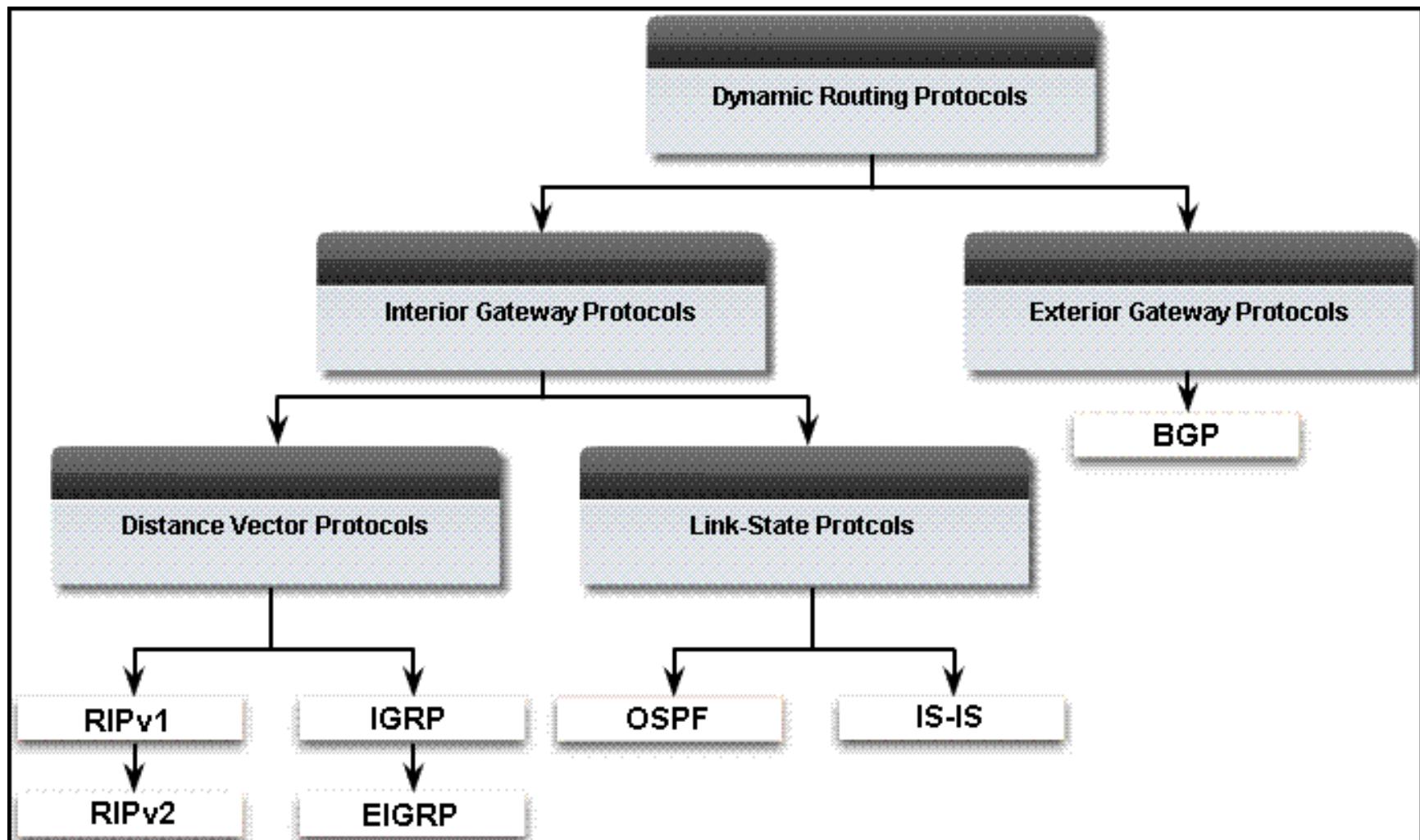
- Ping antar laptop
- Amati ICMP reply

Preferred Source

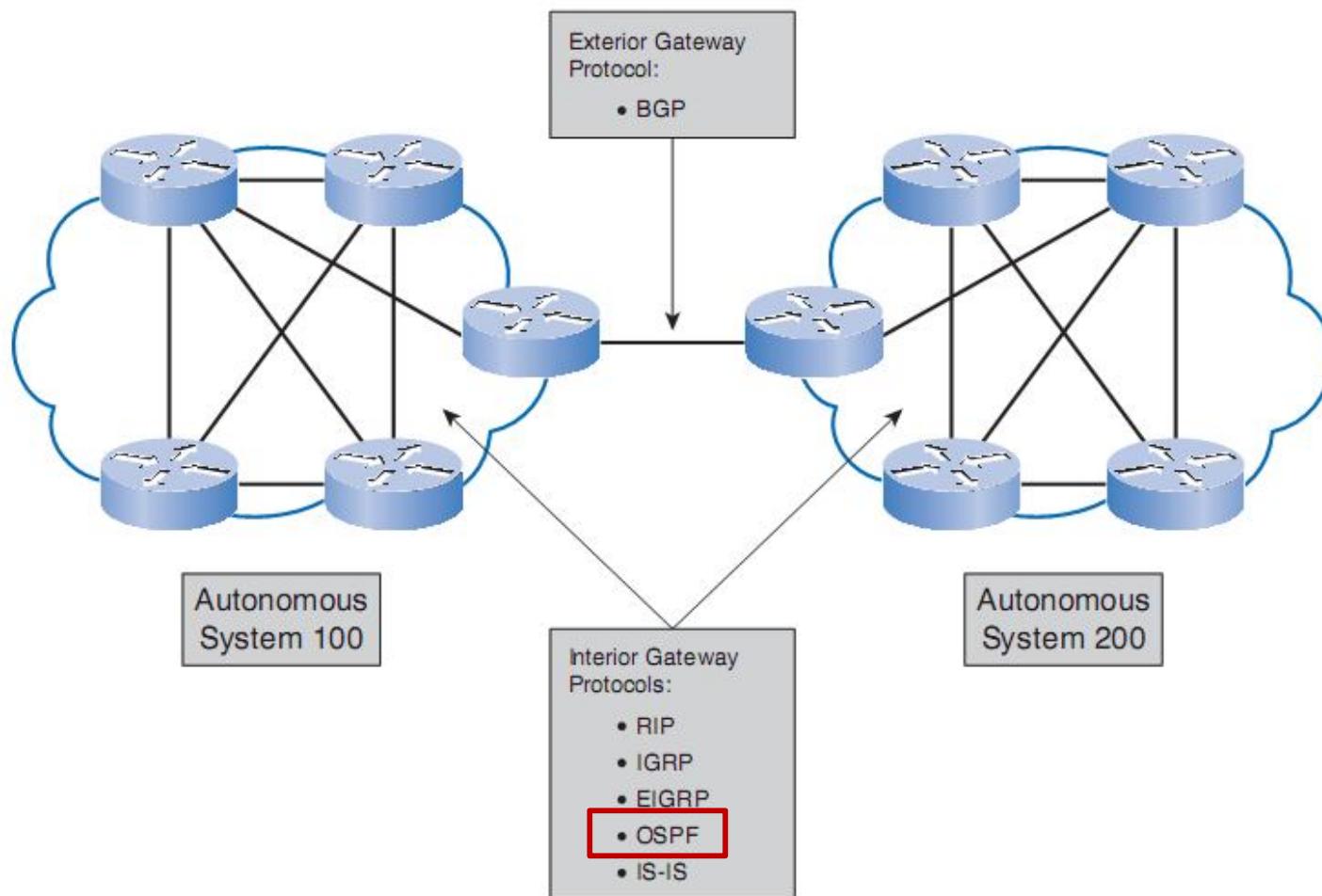
- Default nilai Pref-source bernilai kosong, kecuali untuk connected routes akan berisi IP address interfacenya.
- Fungsi :
 - IP Address asal untuk paket data yang berasal dari router
 - IP Address src-address-to untuk paket data yang terkena action NAT – masquerade
- Jika tidak ditentukan, secara otomatis akan menggunakan salah satu IP Address yang ada pada output interface dari packet.
- Jika isian pref-src adalah IP Address yang tidak terpasang pada router, rule ini akan non-aktif.
- Implementasinya biasanya ketika kita ingin memanipulasi traffik uplink lewat IP A dengan prefered source IP B, maka downlink akan menuju IP B.

OSPF

Dynamic Routing Protocol



IGP & EGP



IGP & EGP

Berdasarkan jenisnya dynamic routing dibedakan menjadi 2 yaitu:

- IGP → Interior Gateway Protocol menghandle routing di dalam suatu Autonomous System (satu routing domain). Dapat dikatakan bahwa IGP adalah routing yang bekerja pada jaringan milik kita atau antar router yang masih milik kita.
- EGP → Exterior Gateway Protocol menghandle routing antar Autonomous System (antar domain routing). Dapat dikatakan bahwa EGP adalah routing yang bekerja atau antara jaringan kita dengan jaringan orang lain.

Autonomous System (AS)

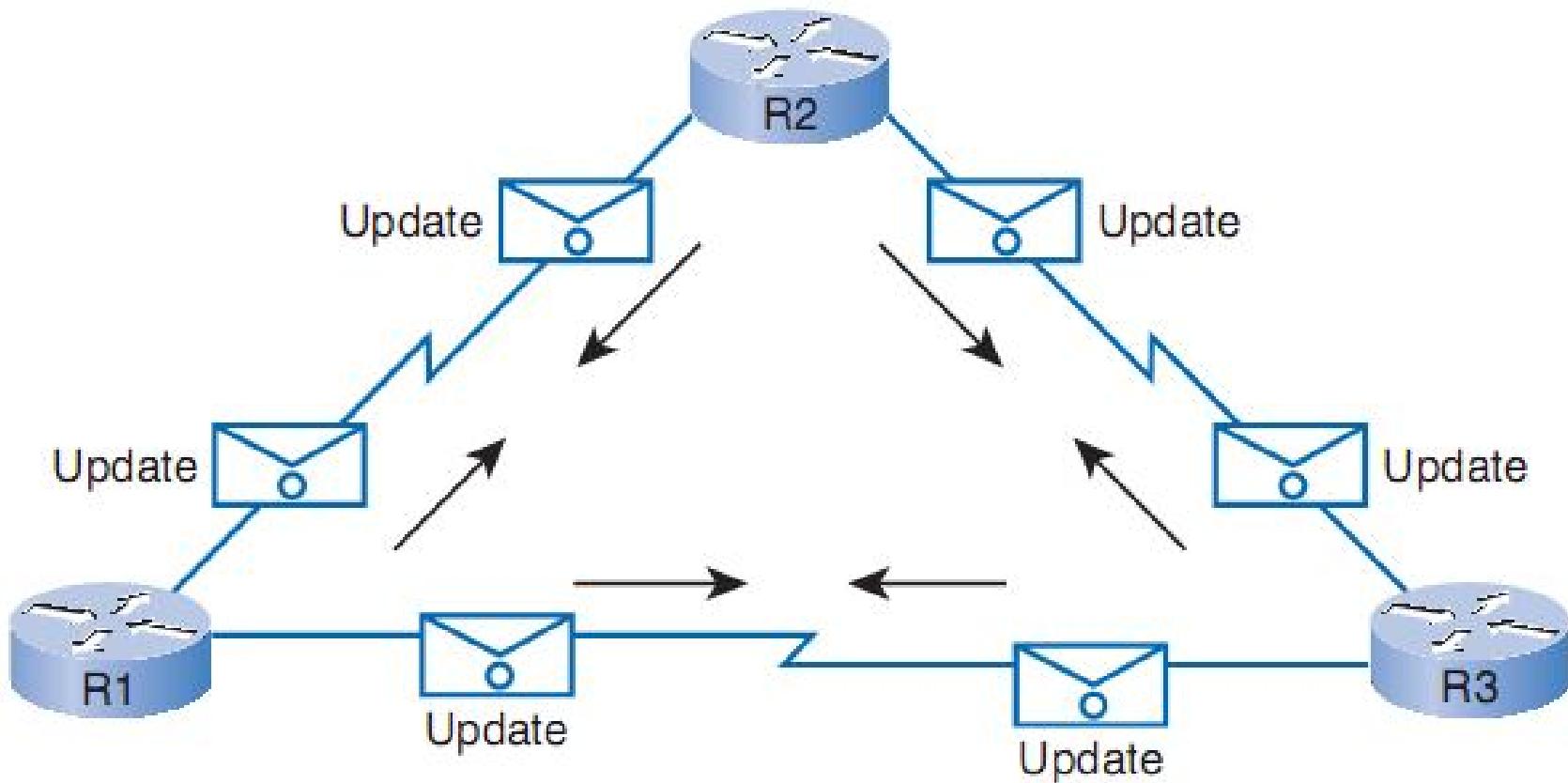
- AS merupakan gabungan dari jaringan / router yang biasanya masih dalam satu kepemilikan atau kontrol yang memiliki sistem routing yang serupa.
- AS diidentifikasi dalam 16 bit number (0 - 65535)
 - ✓ Range dari 1 - 64511 untuk digunakan untuk Internet
 - ✓ Range dari 64512 - 65535 untuk privat

OSPF Protocol

- Open Shortest Path First (OSPF) adalah dynamic routing protocol yang termasuk dalam kategori IGP (Interior Gateway Protocol)
- OSPF memiliki kemampuan Link-state (melakukan deteksi status link) dan algoritma Dijkstra (algoritma pencarian jarak terpendek)
- OSPF mampu menjaga, mengatur dan mendistribusikan informasi routing antar network walaupun topologi network tersebut berubah-ubah secara dinamis.
- Menggunakan IP protocol (layer3) nomor 89.

Routing Distribution

Routers Dynamically Pass Updates

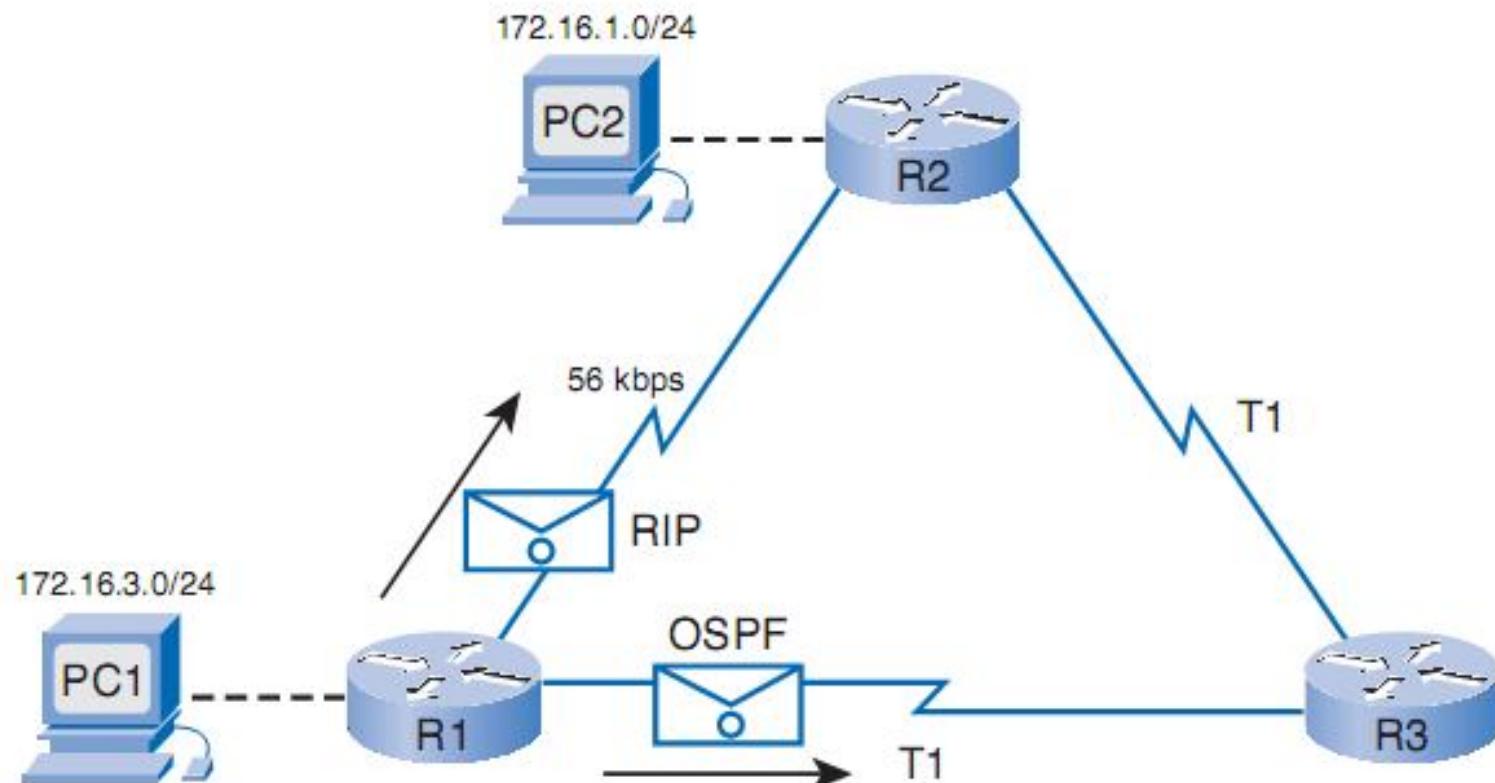


Metrics

- Metric adalah properti dari rute jaringan, terdiri dari berbagai nilai yang digunakan oleh Routing Protocol untuk menentukan apakah suatu rute lebih baik dari route lainnya.
- Metrik bisa berupa:
 - measuring link utilization (using SNMP)
 - number of hops (hop count)
 - speed of the path
 - packet loss (router congestion/conditions)
 - latency (delay)
 - path reliability
 - path bandwidth
 - throughput [SNMP - query routers]
 - load
 - MTU

OSPF VS RIP Metric

Hop Count Versus Bandwidth

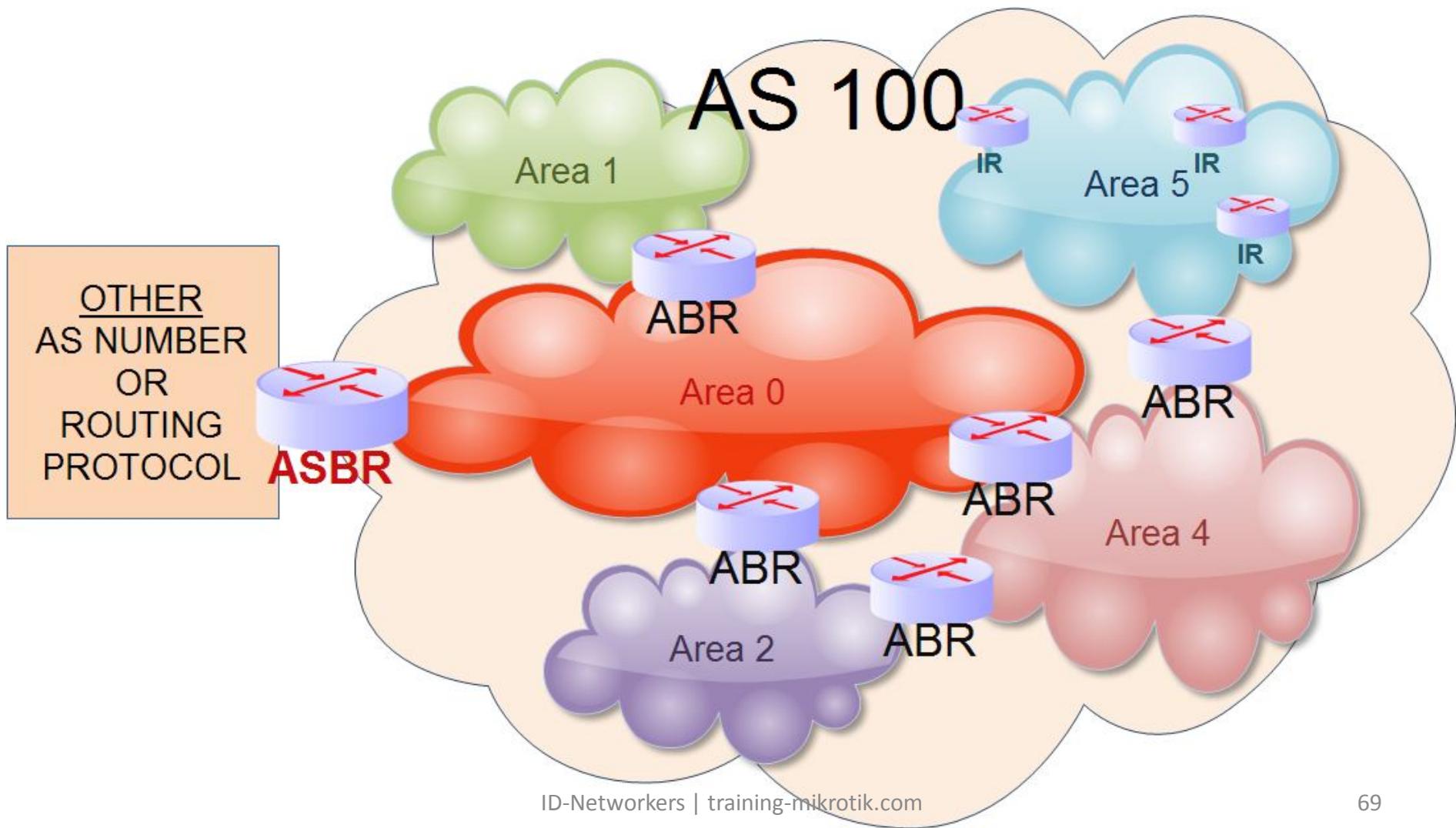


RIP chooses shortest path based on hop count.
OSPF chooses shortest path based on bandwidth.

OSPF Areas

- Suatu AS terdiri dari satu atau beberapa Area.
- Area adalah system grouping yang digunakan di protocol OSPF yaitu gabungan dari beberapa router IR (Internal Routing).
- Area memudahkan dalam manajemen jaringan besar OSPF.
- Struktur satu area tidak terlihat dari area lainnya.
- OSPF areas ditulis dalam 32-bit / seperti IP address (0.0.0 – 255.255.255.255)
- Dalam satu AS, area ID harus unik

OSPF Areas



IR, ABR and ASBR

- IR adalah router yang tergabung dalam sebuah area, jumlah maksimal IR dalam satu area adalah 80 router.
- ABR adalah router yang menjembatani area satu dengan area yang lain.
- ASBR adalah sebuah router yang terletak di perbatasan sebuah AS (Router terluar dari sebuah AS) dan bertugas untuk menjembatani antara router yang ada di dalam AS dengan Network lain (Berbeda AS).
- ASBR juga bisa berarti sebuah router anggota OSPF yang menjembatani routing OSPF dengan Routing protocol yang lain (RIP, BGP dll).

Cara Kerja OSPF(1)

1. Membentuk adjacency

- Pada saat baru pertama ON, router OSPF tidak tahu apapun tentang tetangganya, router akan mulai mengirimkan paket Hello ke seluruh interface jaringan untuk memperkenalkan diri
- Default nilai hello pada broadcast multi-access adalah 10 detik dan 40 detik jika tidak ada respon akan mati, bila mendapat respon maka router akan melanjutkan hubungan.

2. Pemilihan DR dan BDR

- Dalam jaringan multiaccess router-router akan memilih DR (designated router) dan BDR(Backup designated router) dan berusaha adjencent dengan kedua router tersebut.
- Dalam jaringan broadcast multiaccess, DR dan BDR sangatlah diperlukan. DR dan BDR akan menjadi pusat komunikasi seputar informasi OSPF dalam jaringan tersebut

Cara Kerja OSPF(2)

3. Mengumpulkan State-state dalam Jaringan

- Router mengumpulkan seluruh informasi jalur dalam jaringan dengan bertukar informasi mengenai state-state dan jalur-jalur.
- Pada jaringan broadcast/multiaccess, DR-lah yang akan melayani setiap router yang ingin bertukar informasi OSPF dengannya. DR akan memulai lebih dulu proses pengiriman ini.
- Setelah loading state selesai, maka router-router yang tergabung dalam OSPF akan memiliki informasi state yang lengkap dan penuh dalam database statenya. Fase ini disebut dengan istilah Full state

4. Memilih route terbaik untuk digunakan

- Router akan memilih rute-rute terbaik, parameter yang digunakan oleh OSPF adalah Cost.
- Setelah selesai, maka rute tersebut langsung dimasukkan dalam routing table dan siap digunakan untuk forwarding data.

Cara Kerja OSPF(3)

5. Menjaga Informasi Routing Tetap Up-to-date

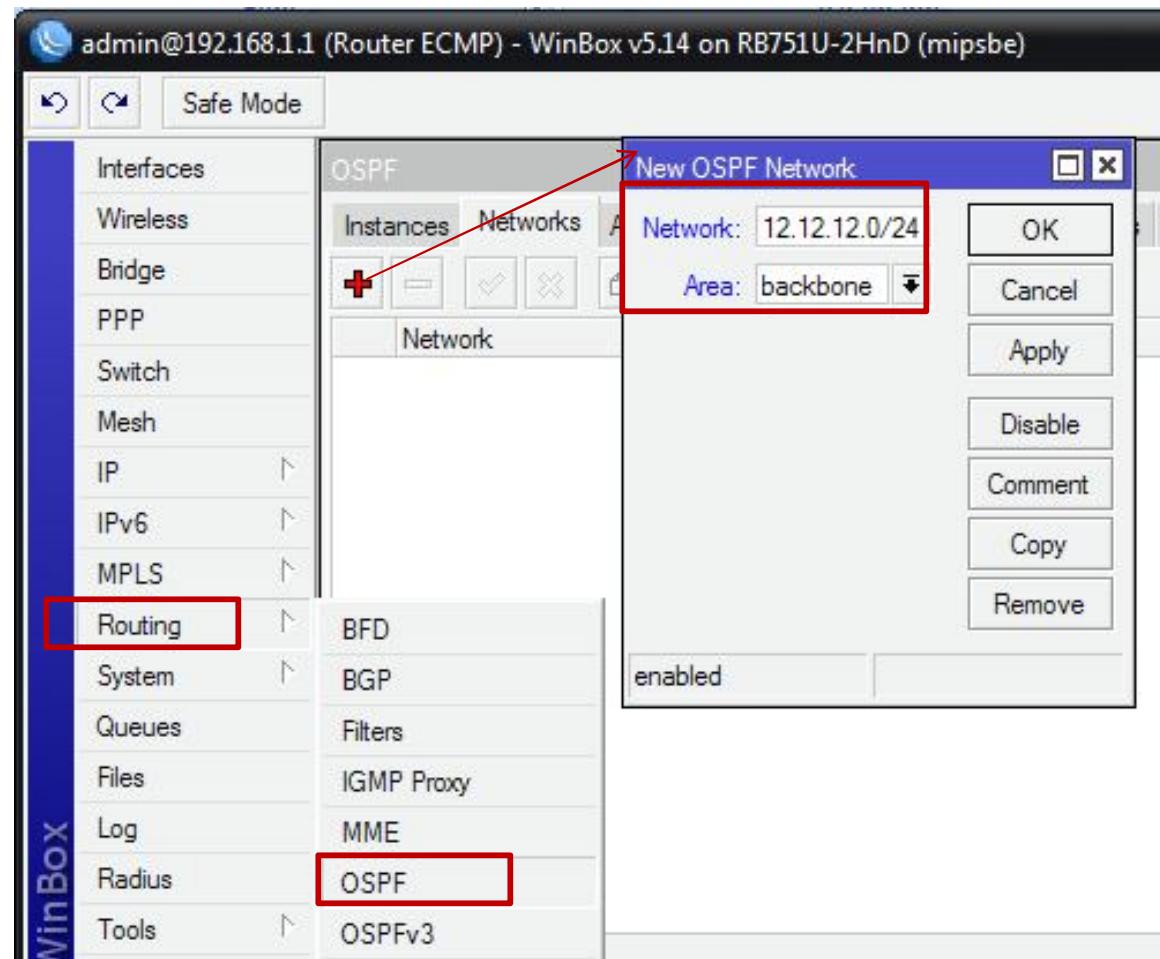
- Ketika sebuah rute sudah masuk ke dalam routing table, router tersebut harus juga me-maintain state database-nya. Hal ini bertujuan kalau ada sebuah rute yang sudah tidak valid, maka router harus tahu dan tidak boleh lagi menggunakannya.
- Ketika ada perubahan link-state dalam jaringan, OSPF router akan melakukan flooding terhadap perubahan ini. Tujuannya adalah agar seluruh router dalam jaringan mengetahui perubahan tersebut.

OSPF Setting

- **Router-id →** Memberi pengenal pada router.
 - Berformat 32bit seperti IP, tidak boleh ada yang sama dalam sebuah jaringan OSPF.
 - Jika diisi 0.0.0.0 maka router akan otomatis menggunakan IP terbesar yang ada pada interface
 - Biasanya router-id diisi alamat loopbacknya (interface bridge)
- **Redistribute Default Route →** Mendistribusikan default route.
Option ini hanya digunakan atau diaktifkan pada router ASBR
- **Redistribute Connected Routes →** Mendistribusikan route yang terpasang dan aktif pada interface
- **Redistribute Static Routes →** Mendistribusikan route static yang ada pada table /ip route
- **Redistribute RIP Routes →** Mendistribusikan route hasil RIP
- **Redistribute BGP Routes →** Mendistribusikan route hasil BGP

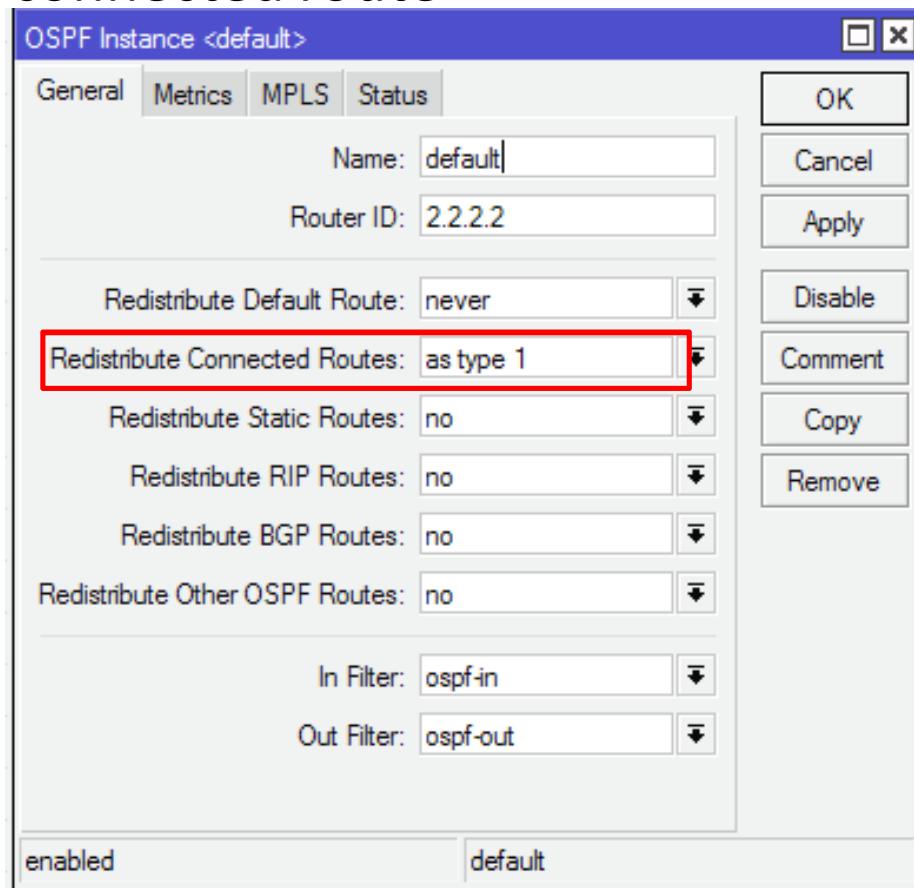
Setting OSPF pada MikroTik

- Add connected network to Area

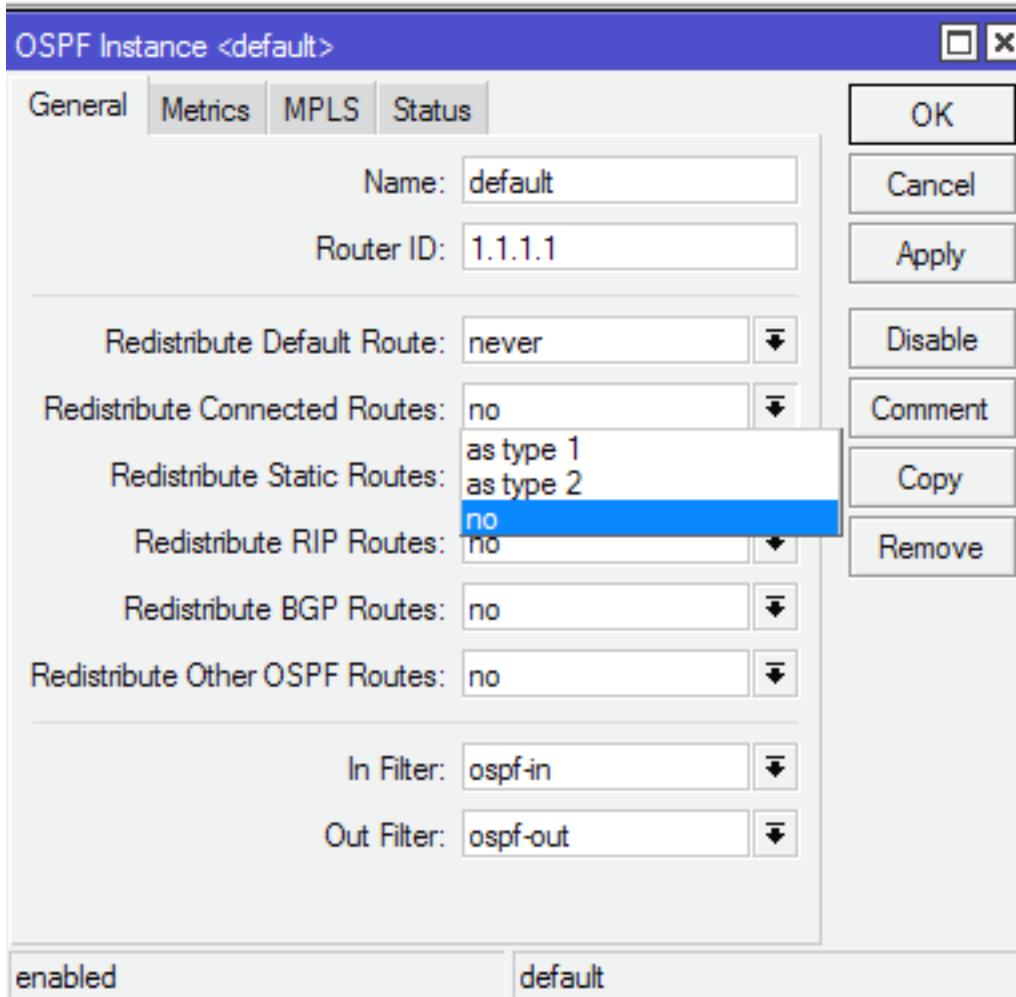


Setting OSPF pada MikroTik

- Routing>OSPF>Instance, setting OSPF Instance, redistribute connected route



OSPF Redistribute Type

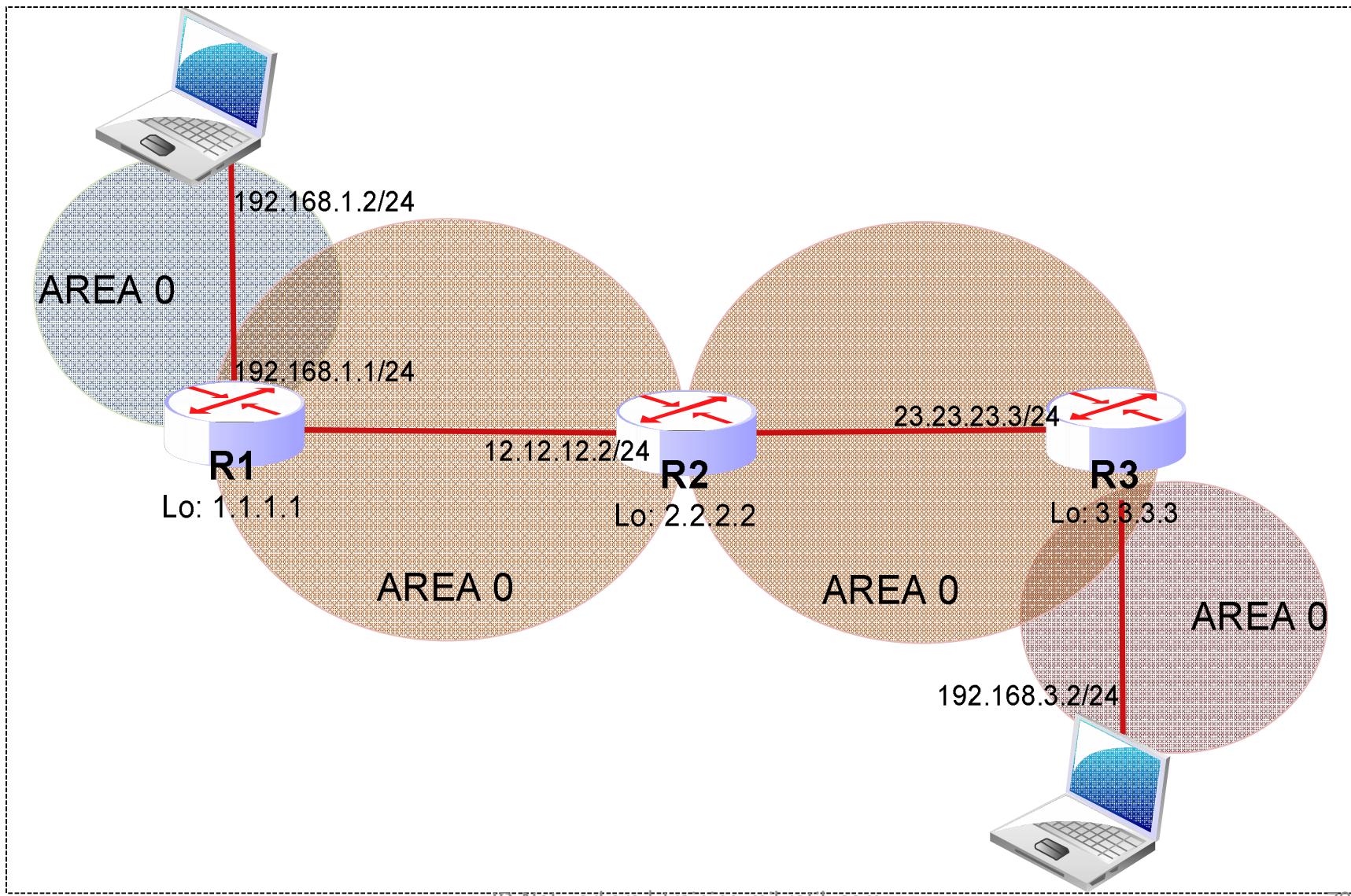


- **as-type-1** – keputusan remote routing network dilakukan berdasarkan **jumlah dari external and internal metrics**
- **as-type-2** – keputusan remote routing network hanya dilakukan berdasarkan **external metrics** (internal metrics tidak diperhitungkan).

Backbone Area

- Area 0 atau Backbone Area merupakan area dimana ABR berkumpul untuk saling menukarkan informasi routing dari area-area yang lain.
- Setiap non Backbone Area harus terhubung langsung dengan Area Bakbone
- Area Backbone juga merupakan Area Transit sebelum traffic keluar atau masuk ke dalam sebuah AS.
- Sebuah area yang tidak terhubung langsung ke area backbone bisa terhubung ke backbone area menggunakan Virtual Link.

LAB IX – Backbone Area (Area 0)

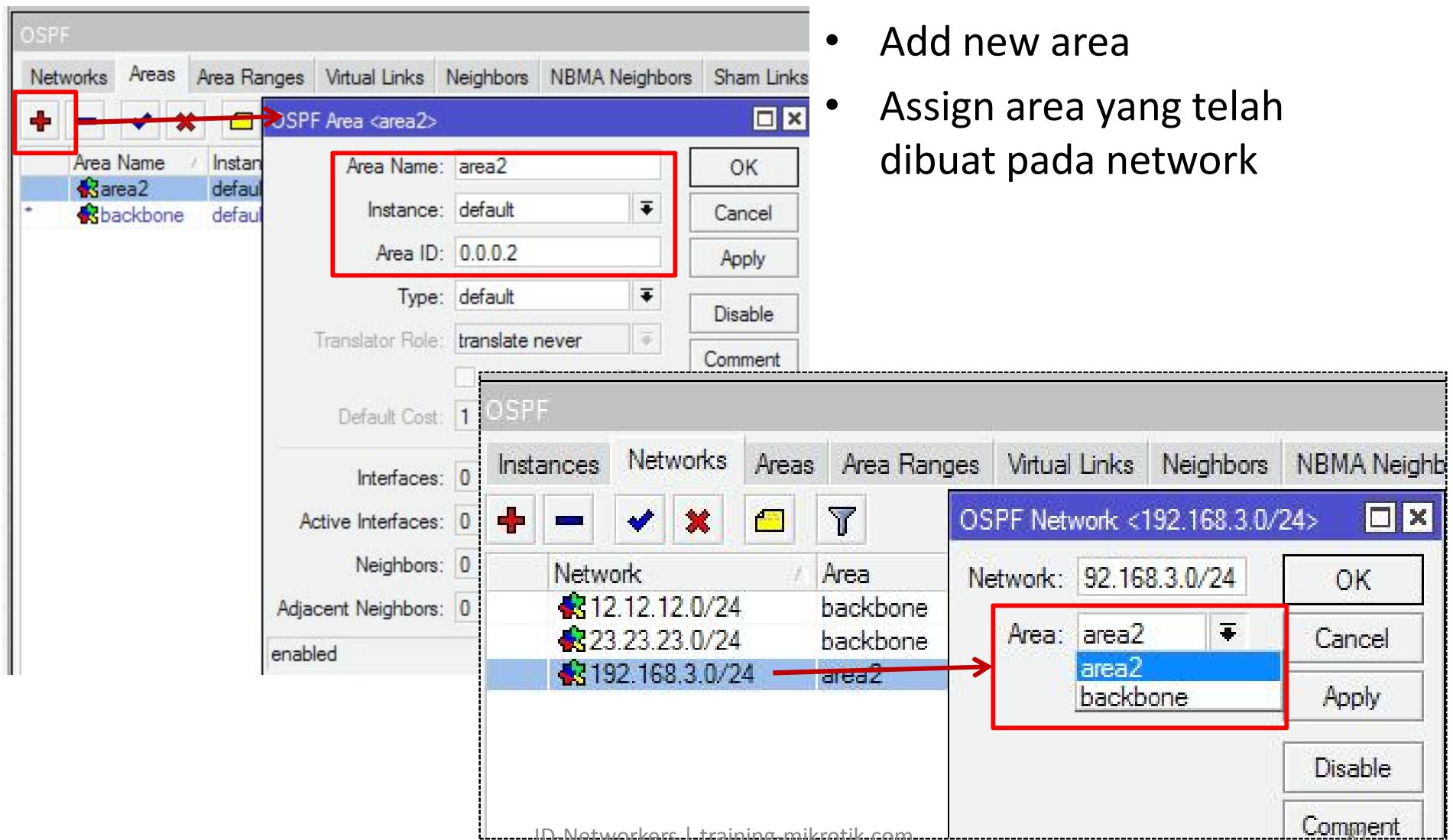


OSPF Area Non Backbone

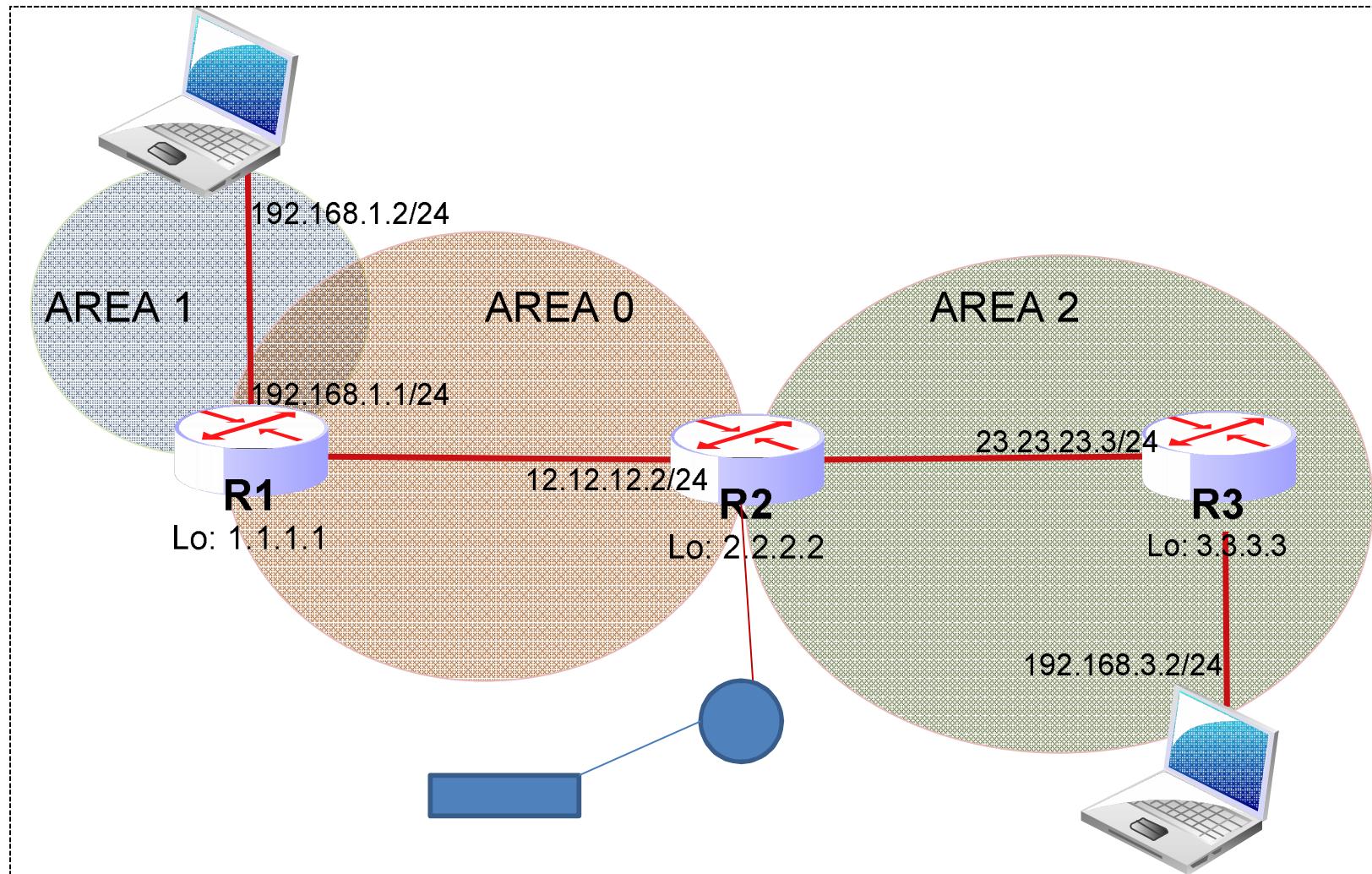
- Sangat memungkinkan jika pada sebuah AS memiliki lebih dari satu area menyesuaikan skala dari jaringan yang dimiliki.
- Semakin banyak router dan jaringan didalamnya, semakin besar ukuran Link State Database (cpu load, memory)
- Internal Router akan mendapat Lin State Advertisement (LSA) hanya dari router lain yang masih dalam satu area
- Area yang ingin mendapatkan informasi LSA secara lengkap dan bisa terkoneksi dengan jaringan yang ada di luar AS maka harus terhubung secara logic dengan Backbone (Area 0).
- Untuk area non backbone yang tidak terhubung langsung ke area backbone harus menggunakan Virtual Link dengan memanfaatkan area lain yang sudah terhubung ke Backbone Area.

Membuat Area Baru

- Add new area
- Assign area yang telah dibuat pada network

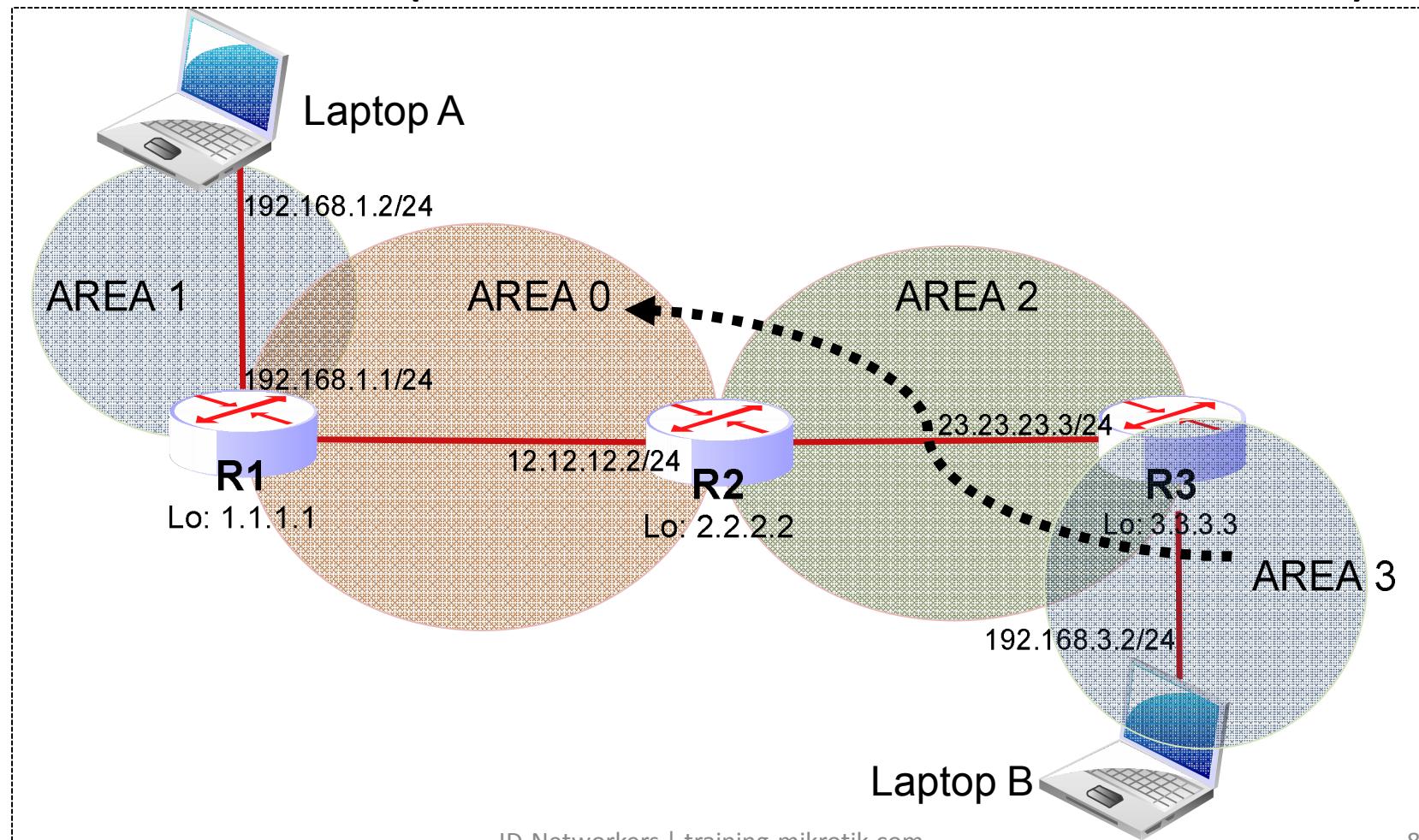


LAB X – Non Backbone Area



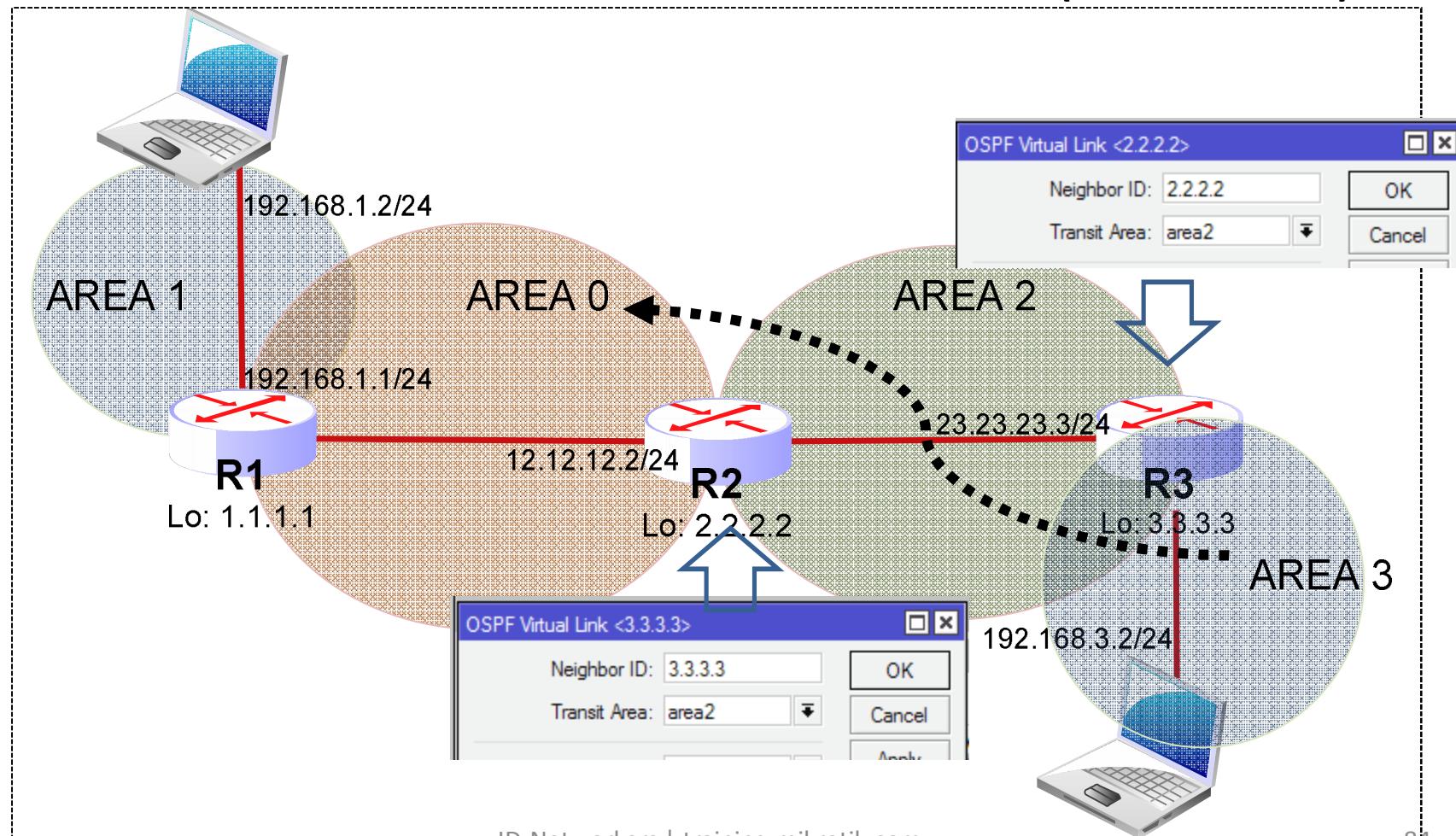
LAB XI – Virtual Link

- Virtual Link (from area 3 to area 0 via area 2)



LAB XI – Virtual Link

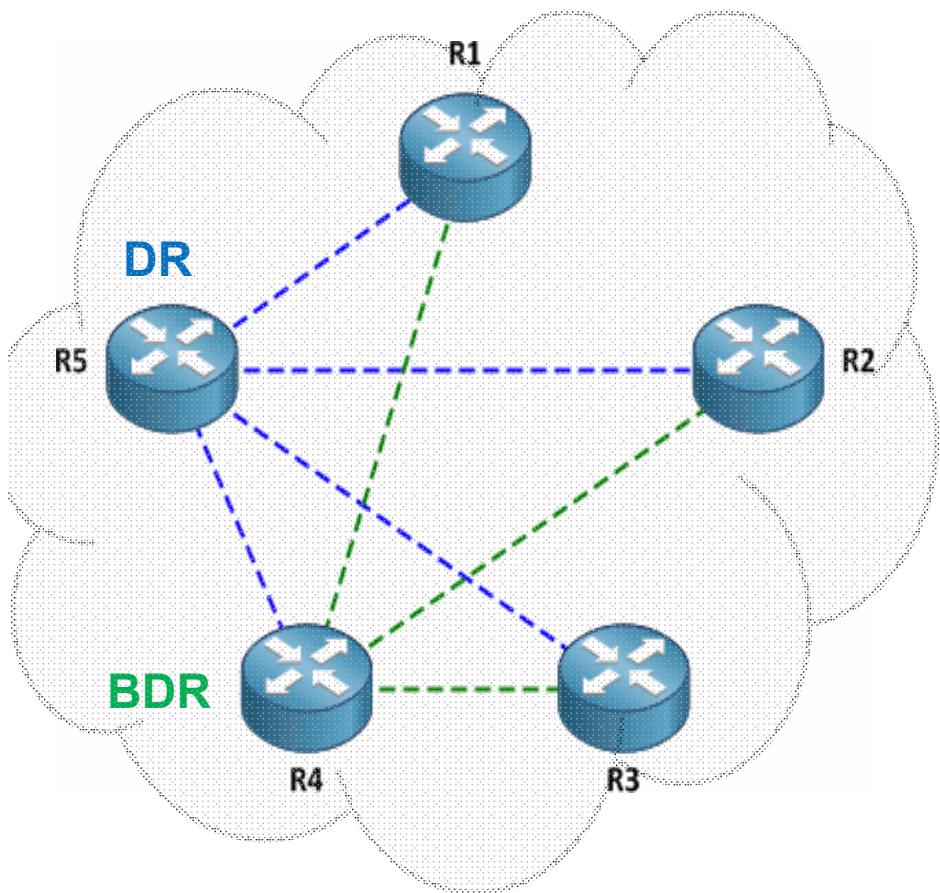
- Virtual Link dibuat di dua sisi ABR (R2 dan R)



DR dan BDR

- Dalam setiap broadcast network pada area, router akan memilih
 - Designated Router (DR) dan
 - Backup Designated Router (BDR) secara otomatis.
- DR berfungsi untuk mengumpulkan dan menyebarkan LSA dalam satu area, sehingga mengurangi traffic dan waktu proses pertukaran LSA antar router
- BDR, akan menggantikan DR jika terjadi error
- DR dan BDR ditentukan oleh priority dari masing-masing router, **priotiry tertinggi (nilainya lebih kecil)** dalam suatu broadcast akan dijadikan DR
- Jika priority sama, DR akan dipilih yang memiliki **router-ID paling tinggi**
- **Jika priority diubah ke 0, dia tidak akan pernah menjadi DR**

DR & BDR



- Dengan adanya BR & BDR, dalam sebuah broadcast network akan mengurangi traffik untuk adjacency.
- Sebuah broadcast network yang terdiri atas 5 router, hanya terjadi 7 adjacency, bukan 9 seperti halnya jaringan mesh.
- Ini berarti pada jaringan broadcast, setiap router hanya perlu melakukan multicast untuk adjacency

DR & BDR

- Designater Router = router dengan OSPF Interfaces semua interfacenya berstatus sebagai designated router

The screenshot shows the Winbox interface for managing OSPF configurations. The window title is "OSPF". The top menu bar includes "Interfaces", "Instances", "Networks", "Areas", "Area Ranges", "Virtual Links", "Neighbors", "NBMA Neighbors", "Sham Links", "LSA", "Routes", and "...". Below the menu is a toolbar with icons for adding (+), deleting (-), checking (✓), unchecking (✗), and filtering (filter icon). A "Find" input field is also present. The main table displays two rows of OSPF interface configurations:

	Interface	Cost	Priority	Authentic...	Authentication Key	Network Type	Instance	Area	Neighbors	State
D	Ether1	10	1	none	*****	broadcast	default	backbone	0	designated router
D	Ether2	10	1	none	*****	broadcast	default	backbone	1	designated router

At the bottom left, it says "2 items out of 0". At the bottom right, it says "ID-Networkers | training-mikrotik.com" and "87".

OSPF-Neighbors State

- Routing>OSPF>Neighbors

The screenshot shows the Winbox interface for managing OSPF neighbors. The window title is "OSPF". The top menu bar includes tabs for "Virtual Links", "Neighbors" (which is selected), "NBMA Neighbors", "Sham Links", "LSA", "Routes", "AS Border Routers", and "...". Below the menu is a search bar with a magnifying glass icon and a "Find" button. The main content area is a table titled "Neighbors" with the following columns: Instance, Router ID, Address, Interface, Designated Router ID, Backup Designat., and State. Two rows of data are listed:

Instance	Router ID	Address	Interface	Designated Router ID	Backup Designat.	State
default	1.1.1.1	12.12.12.1	ether2	12.12.12.2	12.12.12.1	Full
default	3.3.3.3	23.23.23.3	ether3	23.23.23.3	23.23.23.2	Full

OSPF-Neighbors State

1. **down** : router tidak dapat hello packet dari router manapun
2. **attempt** : router mengirimkan hello packet tetapi belum mendapat respon,hanya ada pada tipe NT non broadcast multi-access (NBMA) dan tidak ada respon dari router lain.
3. **Init** : router mendapatkan hello packet dari router lain, tetapi belum terbentukhubungan yang bidirectional (2 way)
4. **2 way** : pada tahap ini hubungan antar router sudah bi-directional, untuk NT broadcast DR & BDR nya akan melanjutkan ke tahap full, router non DR & BDR akan melanjutkan Full hanya dengan DR & BDR saja
5. **Exstart** : terjadi pemilihan Master dan Slave, master adalah router yang memiliki router id tertinggi

OSPF-Neighbors State

6. **Exchange** : terjadi pertukaran Database Descriptor (DBD) paket DBD ini digambarkan dari topologi DB router, proses dimulai oleh master
7. **loading** : router akan memeriksa DBD dari router lain dan apabila ada entry yang tidak diketahui maka router akan mengira link state request (LSR) , LSR akan dibales dengan link state state ACK dan link state reply, diakhir tahap ini semua router yang di adjacent memiliki topologi DB yang sama
8. **Full** : masing-masing router sudah membentuk hubungan yang adjancent.

LSA (Link State Advertisement)

- OSPF adalah type routing jenis Link State (berdasarkan status link)
- Untuk menyebarluaskan informasi Link State ke seluruh router dalam jaringan, OSPF memiliki sebuah sistem khusus disebut dengan istilah Link State Advertisement (LSA).
- Paket LSA akan berisi informasi seputar link-link yang ada dalam sebuah router dan statusnya masing-masing.
- Paket LSA ini kemudian disebarluaskan ke router-router lain yang menjadi neighbour dari router tersebut.
- Setelah informasi LSA sampai ke router lain, maka router tersebut juga akan menyebarluaskan LSA miliknya ke router pengirim dan ke router lain

LSA Type

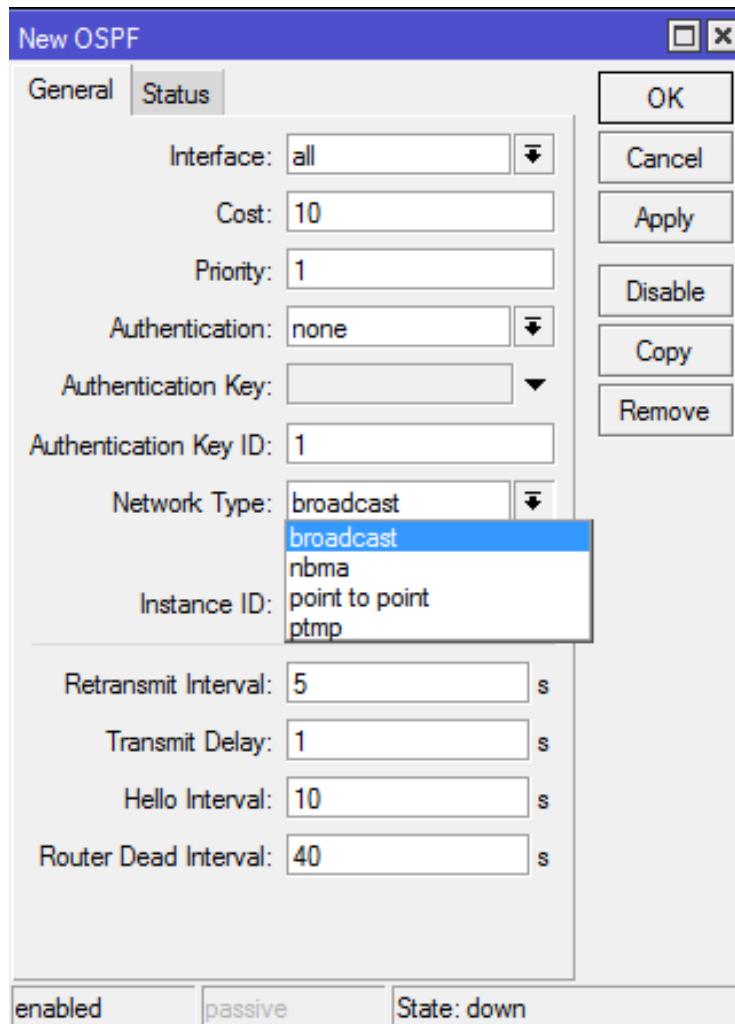
- Type 1 (Router Link) : memberikan informasi router yang terhubung langsung dan kondisi cost interfacenya dalam 1 area
- Type 2 (Network Link) : digenerate oleh DR, memberikan informasi list semua router yang berdekatan, LSA type 2 dibroadcast di dalam satu area.
- Type 3 (Summary Link) : digenerate oleh ABR, memberikan informasi summary jaringan dan link di internal area yang akan di advertise ke area lain dalam satu AS.
- Type 4 (ASBR Summary Link) : dari ABR ke backbone area, memberikan informasi alamat ASBR, menginformasikan ASBR berada di non backbone area , informasi berupa alamat, bukan tabel routing
- Type 5 (AS External Link) : Memberikan informasi routing yang dipelajari dari ASBR. LSAs Eksternal disebarluaskan ke semua area kecuali Stub area. LSA ini membagi dalam dua tipe: eksternal tipe 1 dan type2.
- Type 6 (Group Membership) : digunakan untuk Multicast OSPF (MOSPF), jarang digunakan & tidak disupport oleh MikroTik RouterOS
- Type 7 (NSSA External Link) : diinformasikan oleh ASBR yang berada pada NSSA, LSA type 7 akan berubah ke type 5 setelah meninggalkan areanya melewati ABR

LSA Type

- Route>OSPF>LSA

OSPF							
	Neighbors	NBMA Neighbors	Sham Links	LSA	Routes	AS Border Routers	Area Border Routers
<input type="button" value="Filter"/>						<input type="button" value="Find"/>	
Instance	Area	Type	ID	Originator	Sequence Nu...	Age (s)	
default		as external	2.2.2.2	2.2.2.2	80000001	852	
default		as external	192.168.2.0	2.2.2.2	80000001	852	
default	backbone	network	23.23.23.3	3.3.3.3	80000001	814	
default	backbone	router	2.2.2.2	2.2.2.2	80000004	808	
default		as external	3.3.3.3	3.3.3.3	80000001	854	
default		as external	192.168.3.0	3.3.3.3	80000001	854	
default	backbone	router	1.1.1.1	1.1.1.1	80000003	623	
default	backbone	router	3.3.3.3	3.3.3.3	80000003	814	
default	backbone	network	12.12.12.2	2.2.2.2	80000001	808	

OSPF Network Type



- Default pada interface LAN adalah broadcast

OSPF Network Type

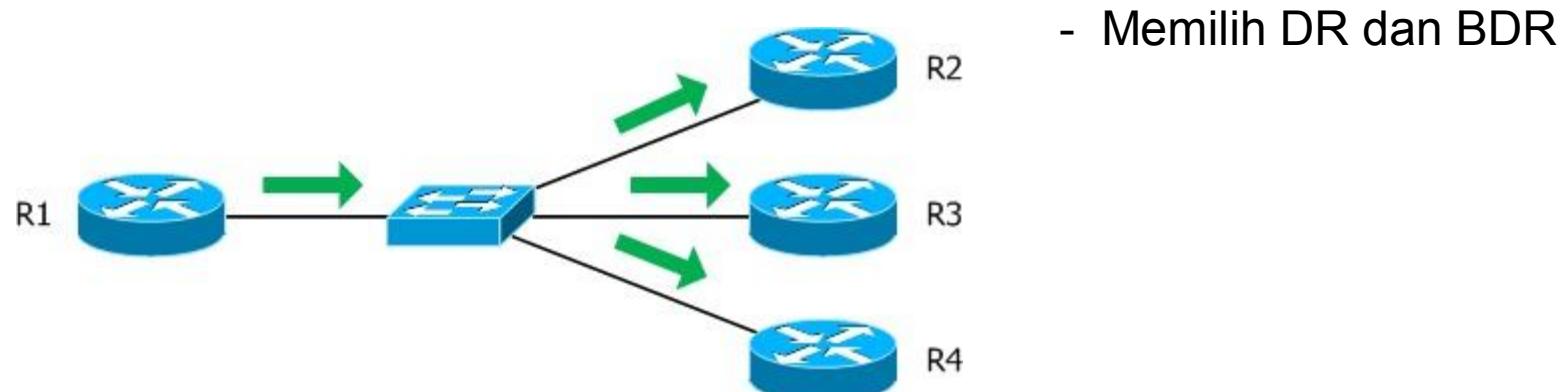
a. Point to Point

- Pada Network point to point, tidak dipilih DR dan BDR



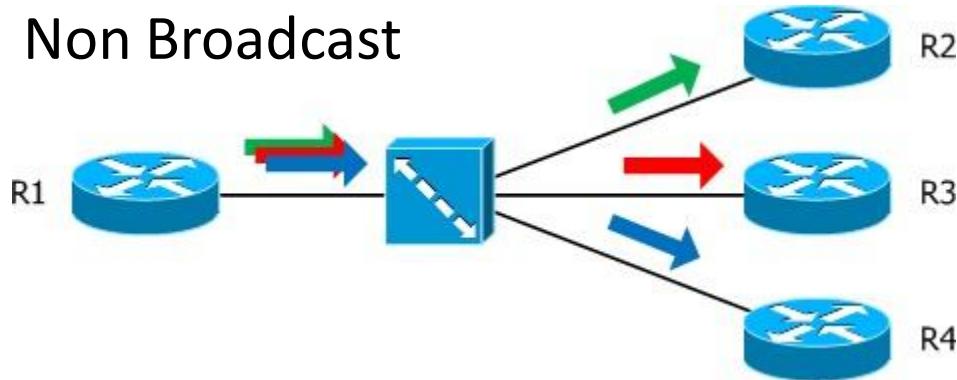
b. Broadcast

- Single packet yang ditransmisikan oleh router dapat digandakan oleh device seperti Ethernet switch) sehingga setiap sisi end pointnya menerima copy dari paket tersebut



OSPF Network Type

c. Non Broadcast



1. Non Broadcast Multiple Access
 - OSPF hello packets masing masing ditransmisikan secara unicast ke masing masing adjacent neighbor.
 - Diperlukan manual konfigurasi pada neighbors
 - Memilih DR dan BDR
2. Point to Multi Point
 - Tidak membutuhkan manual konfigurasi pada neighbors
 - Tidak memilih DR dan BDR
 - Cocok diterapkan pada jaringan wireless, apabila mode “broadcast” tidak bekerja secara maksimal

OSPF Network Type

Interface Type	Uses DR/ BDR?	Default Hello Interval	Requires a neighbor Command?	More than Two Hosts Allowed in the Subnet?
Broadcast	Yes	10	No	Yes
Point-to-point ¹	No	10	No	No
Nonbroadcast ² (NBMA)	Yes	30	Yes	Yes
Point-to-multipoint	No	30	No	Yes
Point-to-multipoint nonbroadcast	No	30	Yes	Yes
Loopback	No	—	—	No

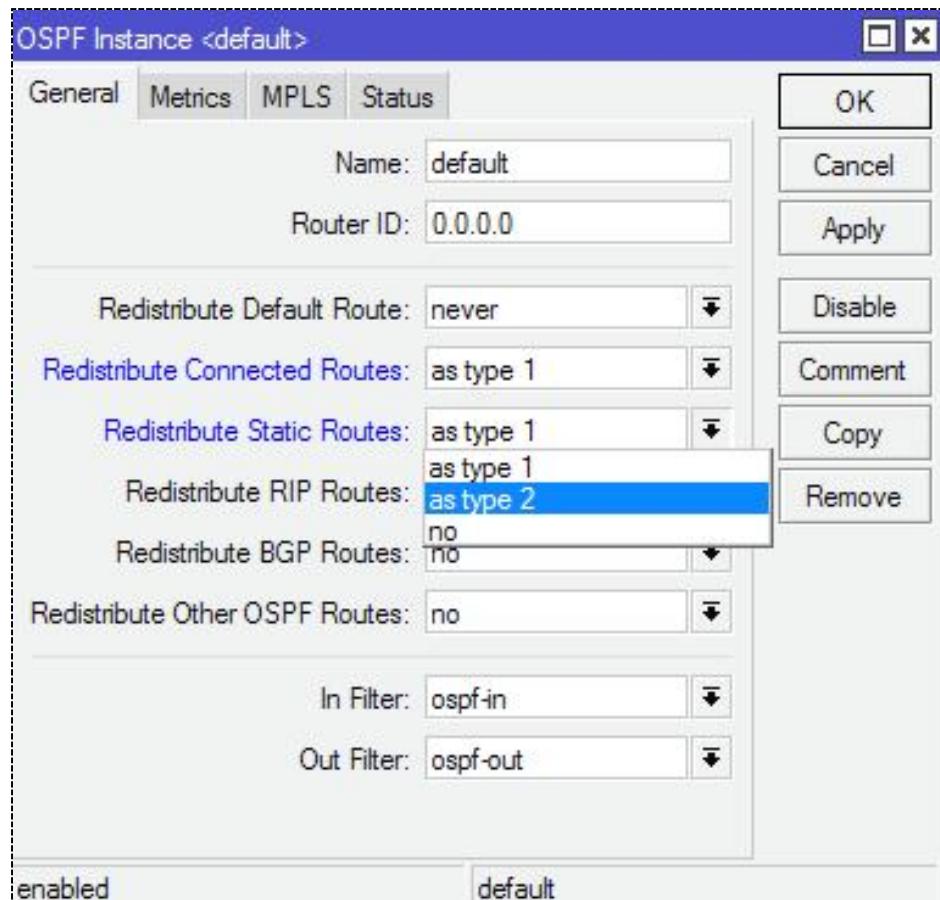
¹ Default on Frame Relay point-to-point subinterfaces.

² Default on Frame Relay physical and multipoint subinterfaces.

Virtual Link

- Setiap non backbone area harus terhubung langsung ke area backbone.
- Virtual link pada OSPF digunakan untuk koneksi non backbone area ke backbone area melewati non backbone area lainnya.
- Virtual link juga digunakan untuk koneksi OSPF antar backbone area melewati non backbone area.

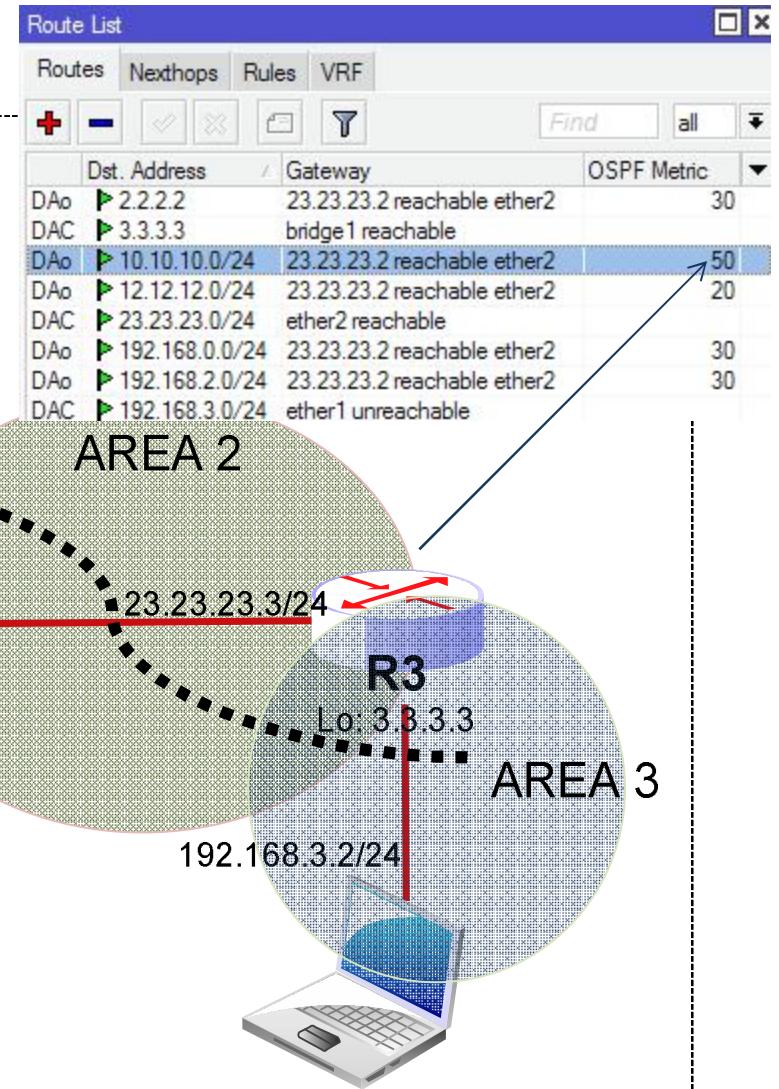
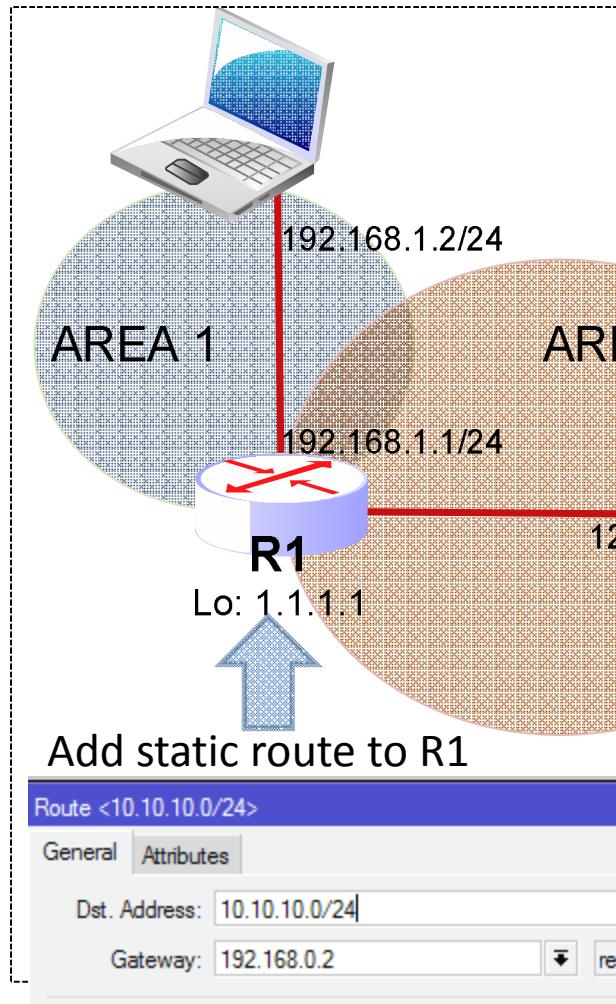
OSPF Redistribute Type



- **as-type-1** – keputusan remote routing network dilakukan berdasarkan **jumlah dari external and internal metrics**
- **as-type-2** – keputusan remote routing network hanya dilakukan berdasarkan **external metrics** (internal metrics tidak diperhitungkan).

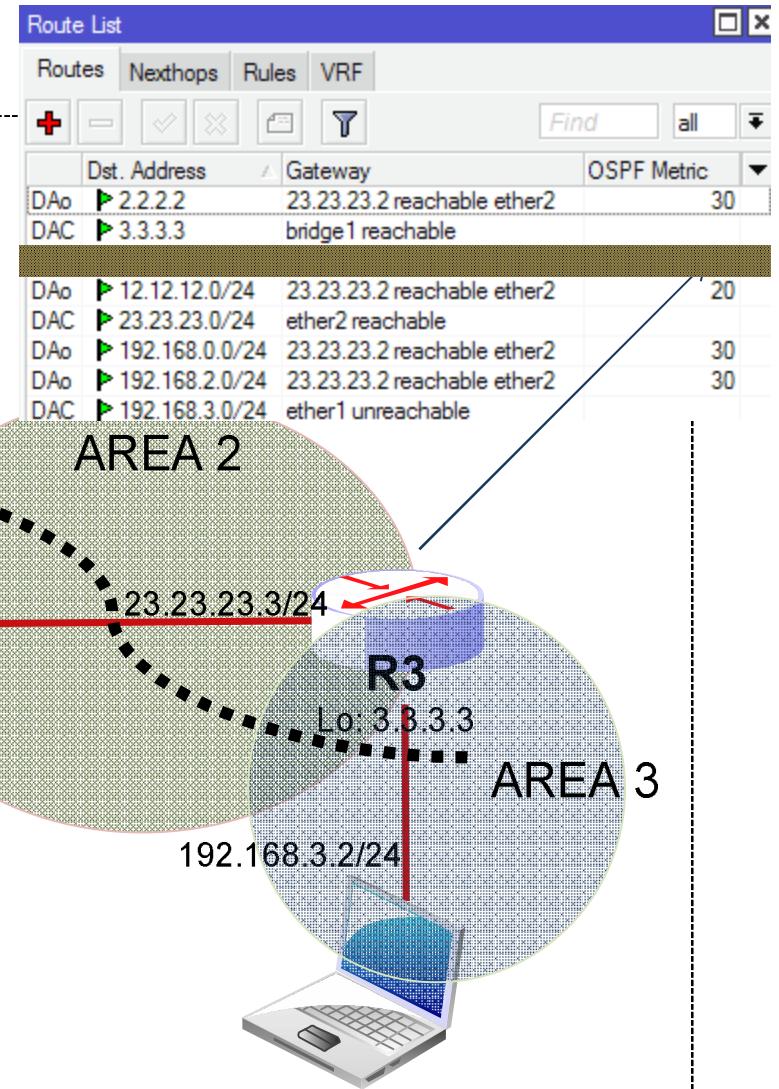
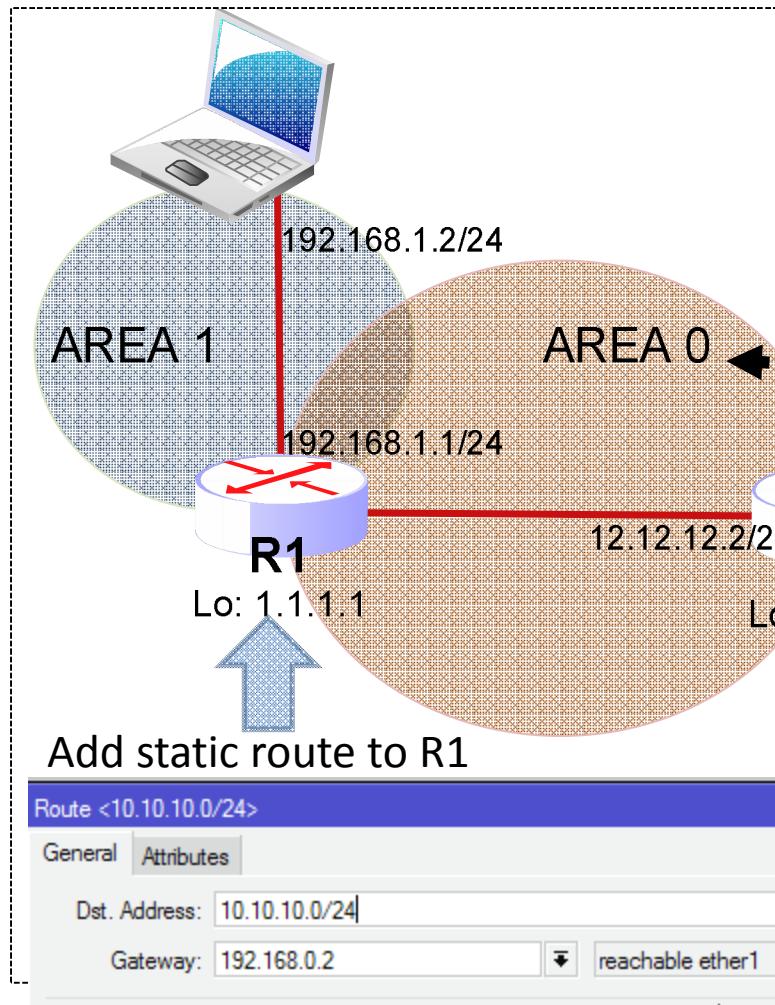
LAB XII-Option Redistribute

Option Redistribute AS-Type1



LAB XII-Option Redistribute

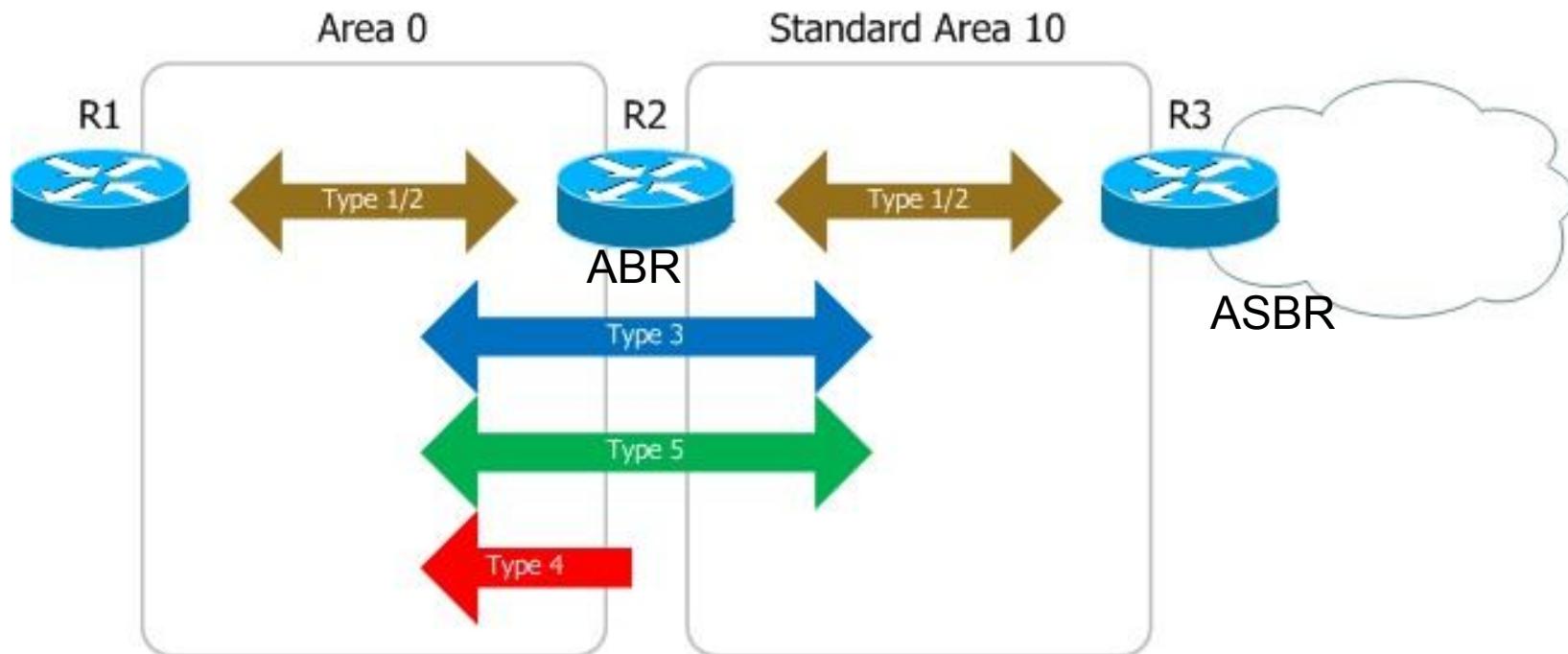
Option Redistribute AS-Type2



Tipe-Tipe Area

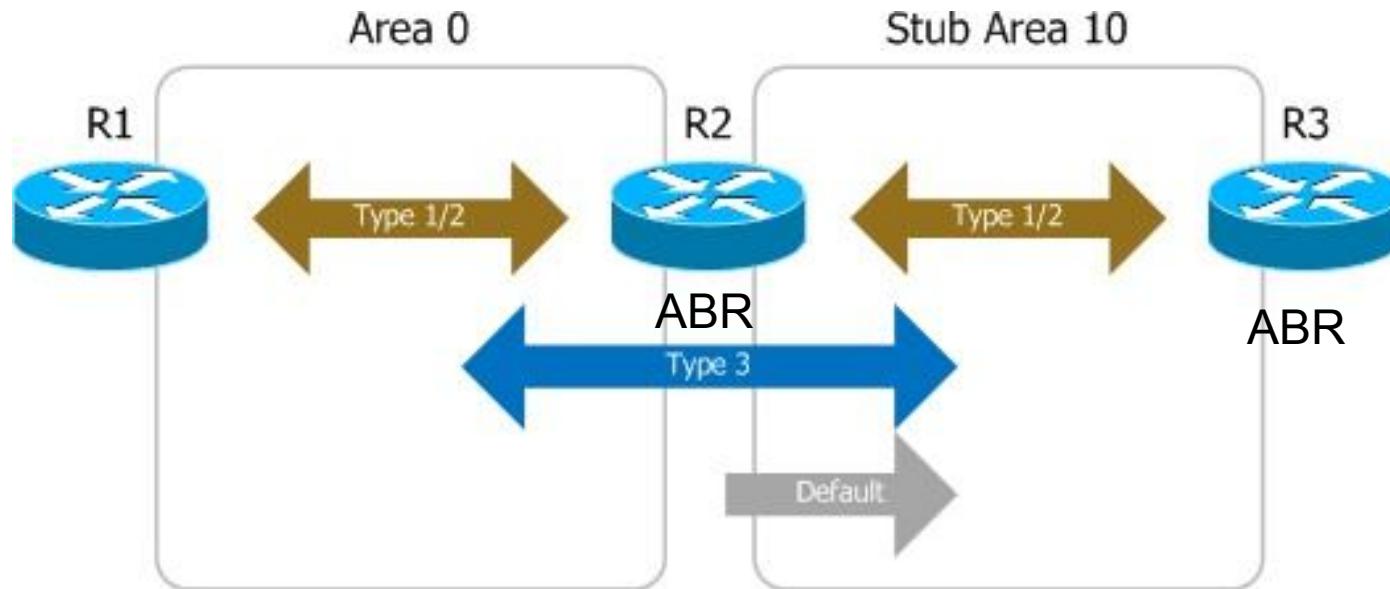
- Backbone – Area 0 (default 0.0.0.0)
 - Bertanggung jawab mendistribusikan informasi routing antara non-Backbone area
 - Semua sub-Area HARUS terhubung dengan backbone secara logikal
- Standar Area
 - Merupakan sub-Area dari Area 0. Area ini menerima LSA intra-area dan inter-area dari ABR yang terhubung dengan area 0
- Stub Area
 - Area yang paling “ujung”. Area ini tidak menerima advertise external route, baik itu dari ABR area lain, ataupun ASBR
- Not So Stubby Area (NSSA)
 - Stub Area yang memiliki external route dan diberikan ke area lain

Standar Area



- **Type 1** - LSA info router yang terhubung langsung (Router)
- **Type 2** – Designated router menginfokan list linkstate pada internal area (Network)
- **Type 3** - Network internal area yg diinfokan ke luar area oleh ABR (link summary)
- **Type 4** – Menginformasikan alamat ASBR
- **Type 5** – Route external (type1/type2) dari ASBR ke semua normal area

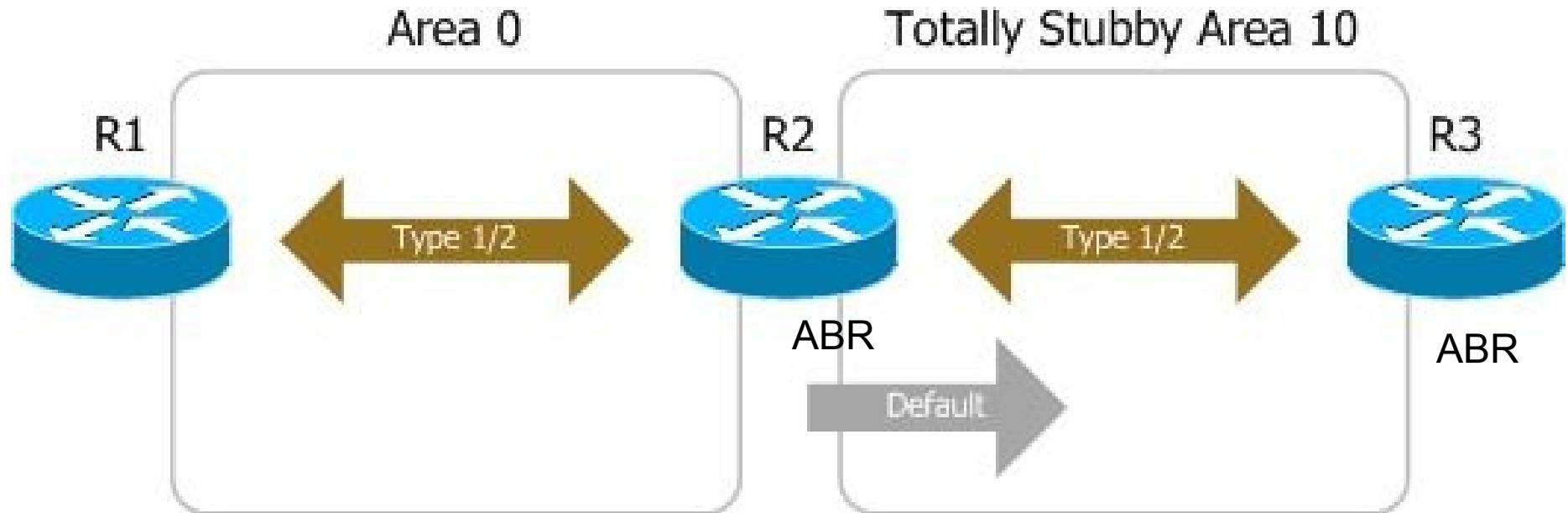
Stub Area



Area yang memiliki batasan khusus , tidak menerima informasi alamat ASBR, tidak mendapatkan external routing diluar AS. Stub area juga tidak dapat melewatkkan virtual link.

- **Type 1** - LSA info router yang terhubung langsung (Router)
- **Type 2** – designated router menginfokan link state pada internal area (Network)
- **Type 3** - Network internal area yg diinfokan ke luar area oleh ABR (link summary)
- **Type 4** – Menginformasikan alamat ASBR
- **Type 5** – Route external (type1/type2) dari ASBR ke semua normal area

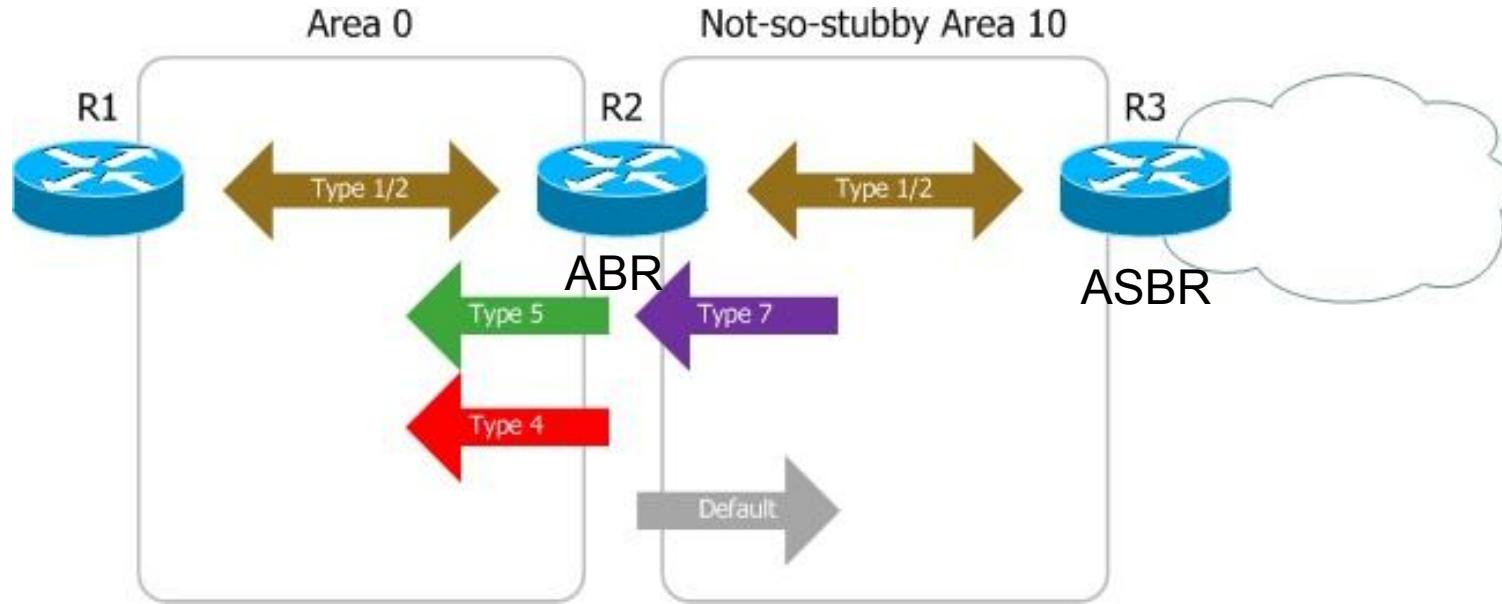
Totally Stub Area



Semua routing yang keluar dari Area tersebut hanya bergantung pada rute default tunggal yang diberikan oleh ABR

- **Type 1** - LSA info router yang terhubung langsung (Router)
- **Type 2** – designated router menginfokan list router pada internal area (Network)
- **Type 3** - Network internal area yg diinfokan ke luar area oleh ABR (link summary)
- **Type 4** – Menginformasikan alamat ASBR
- **Type 5** – Route external (type1/type2) dari ASBR ke semua normal area

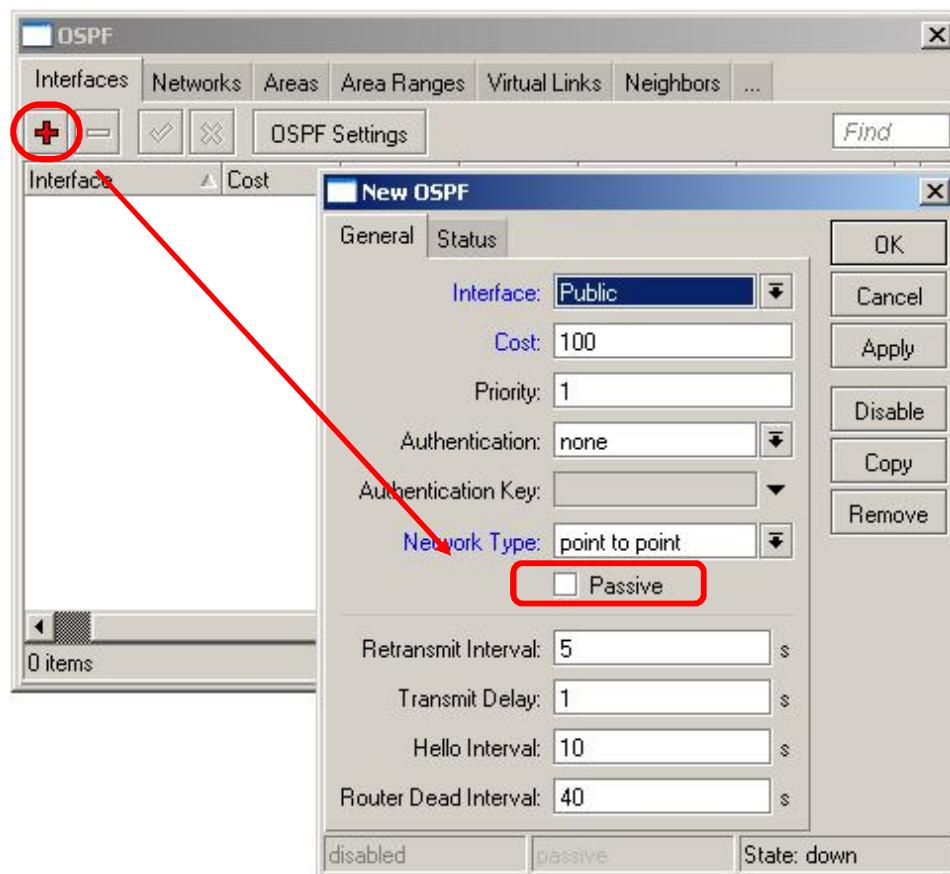
Not-so-Stubby Area



LSA type 7 diinformasikan oleh ASBR yang berada pada NSSA, LSA type 7 akan berubah ke type 5 setelah meninggalkan areanya melewati ABR

- Type 1 - LSA info router yang terhubung langsung (Router)
- Type 2 – designated router menginfokan list router pada internal area (Network)
- ~~Type 3 – Network internal area yg diinfokan ke luar area oleh ABR (link summary)~~
- Type 4 – Menginformasikan alamat ASBR
- Type 5 – Route external (type1/type2) dari ASBR ke semua normal area
- Type 7 – NSSA external link

Passive interface

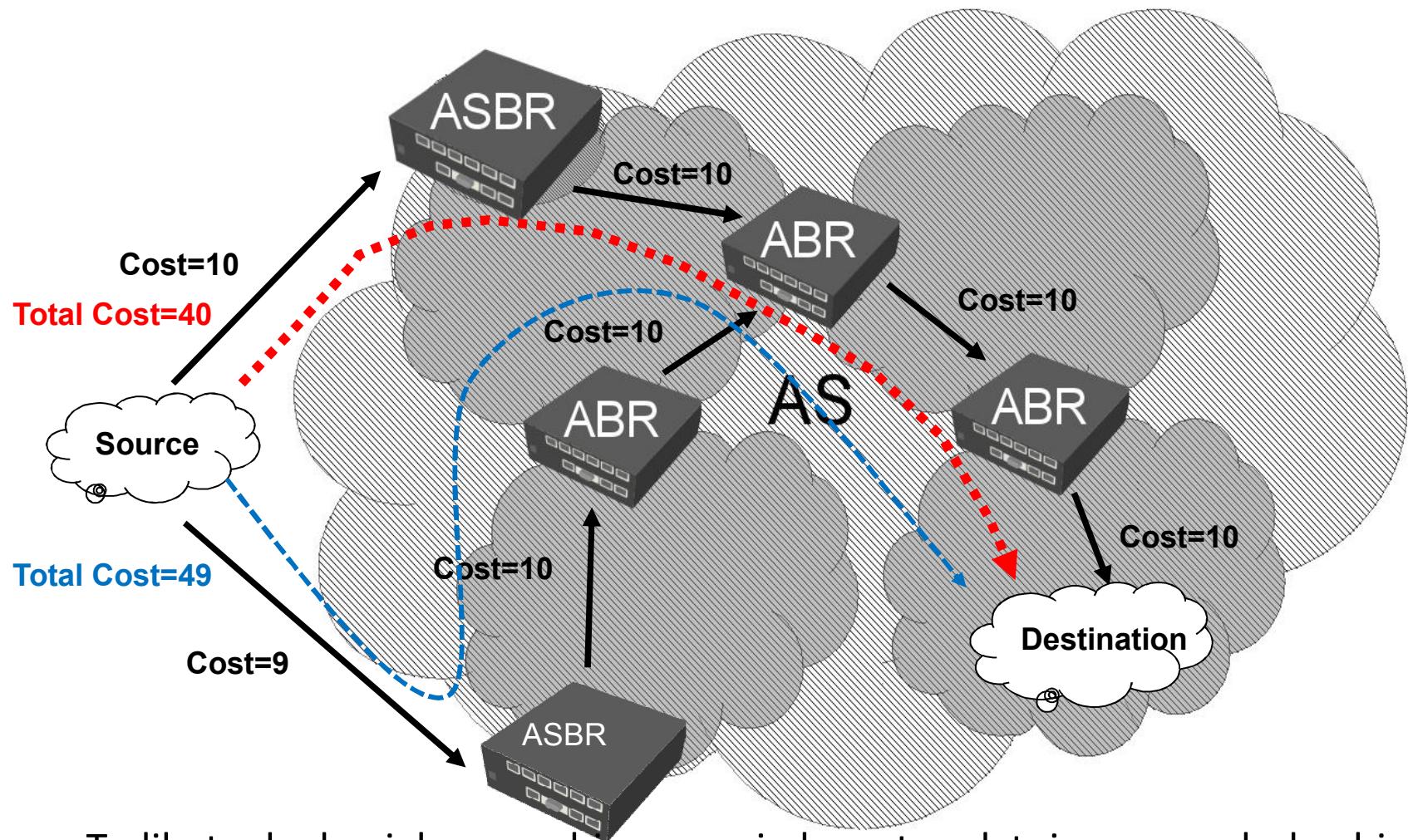


- Apabila kita tidak menginginkan suatu interface untuk menerima dan mengirimkan semua traffik OSPF, Passive interface di-enablekan .
- Ini lebih digunakan untuk alasan keamanan.
- Passive interface di create / di add kemudian diassign pada interface yang ingin diubah.

OSPF Cost

- Untuk menetukan jalur terpendek atau bisa juga diartikan sebagai jalur prioritas, OSPF menggunakan parameter “Cost”.
- OSPF “Cost” akan dijumlahkan di setiap hopnya pada proses Link State / Shortest Path Technology.
- Setelah semua jalur sudah dikalkulasi dan total
- Cost semua jalur sudah dijumlahkan, maka akan dipilih jumlah akumulasi cost yang terkecil

OSPF Cost

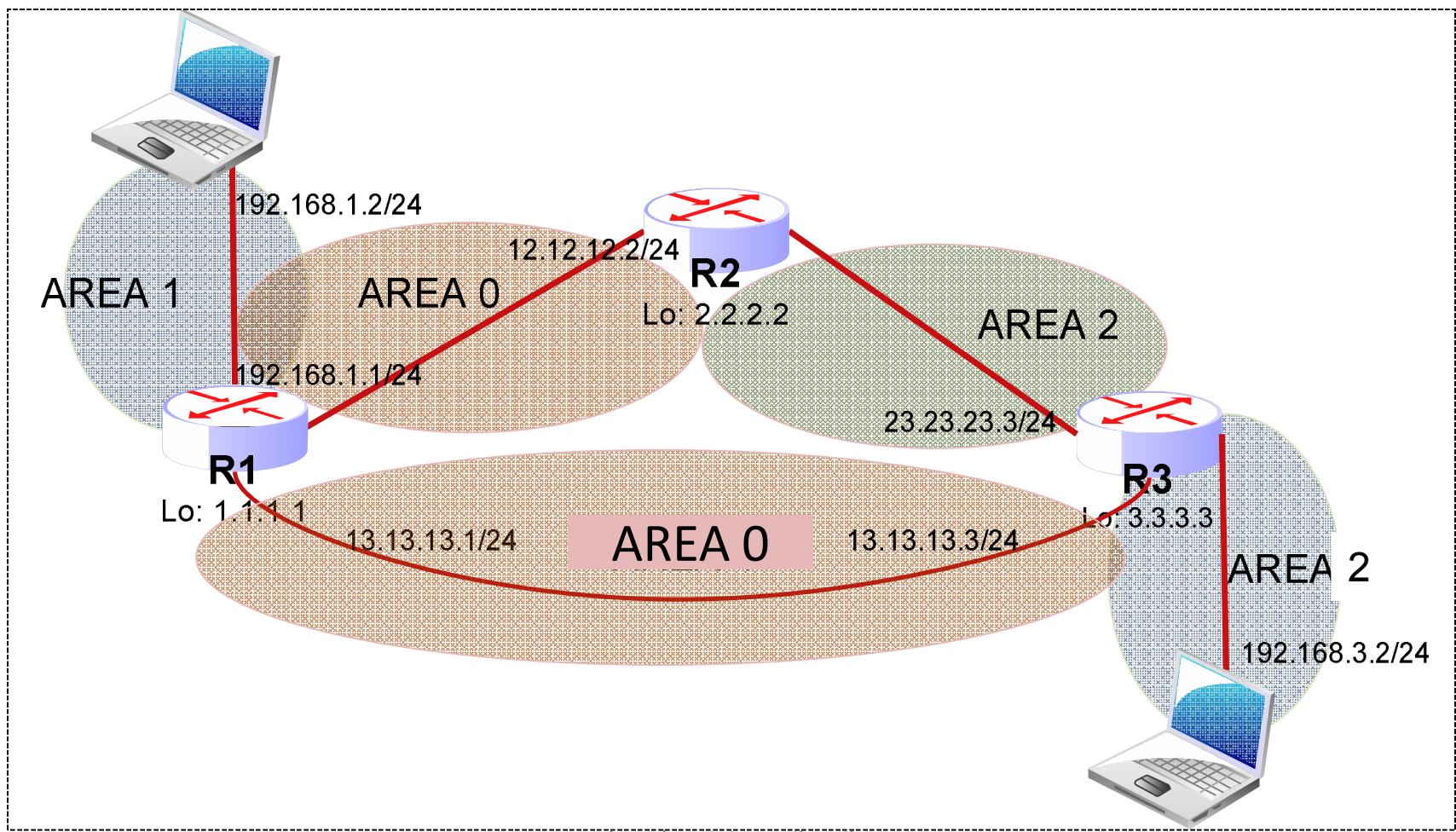


- Terlihat ada dua jalur yang bisa menuju ke network tujuan, merah dan biru.
- Setelah dilakukan perhitungan total Cost, **jalur merah** memiliki total cost terkecil. Maka jalur tersebut yang akan digunakan.

OSPF Redundancy

- Apabila dilakukan penambahan link, OSPF akan mendeteksi dan menambahkan dalam routing tabelnya.
- Apabila ada 1 network dengan 2 gateway yang berbeda namun **cost interface yang sama**, kedua link akan difungikan sebagai **load balancing**.
- Apabila salah satu **cost interfacenya lebih tinggi** maka salah satu link akan dijadikan link utama dan lainnya menjadi **link backup (failover)**

Lab XV – OSPF Redundancy

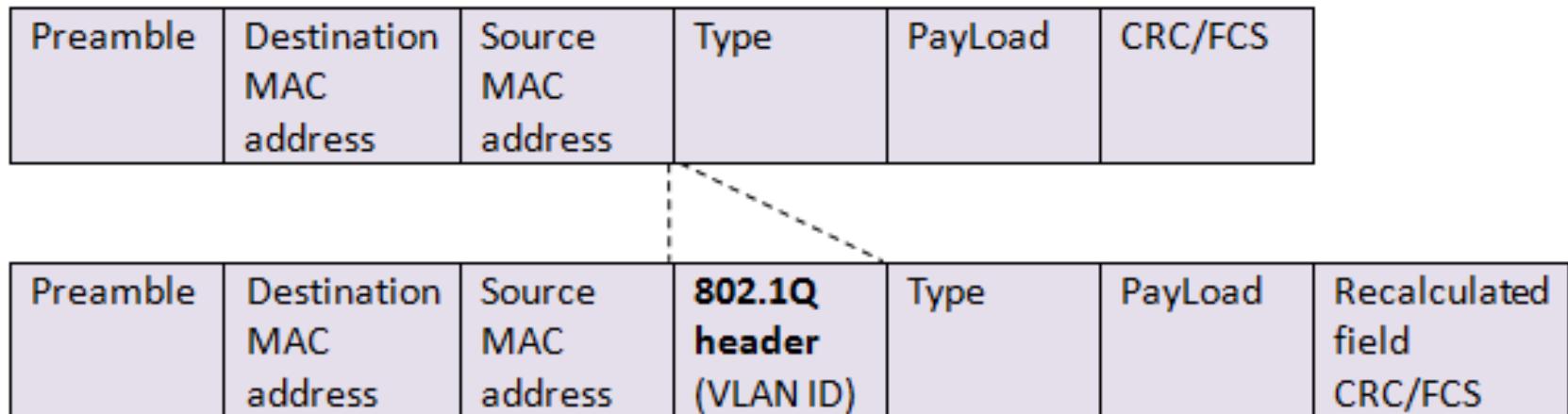


VLAN

- Host dan server yang terhubung ke Layer 2 switch merupakan bagian dari segmen jaringan yang sama. Apabila network sudah menjadi lebar hal ini menimbulkan masalah , yaitu switche terbanjiri traffic broadcast dari dan ke semua port sehingga mengkonsumsi bandwidth yang tidak perlu.
- VLAN dapat membentuk domain broadcast sendiri-sendiri dalam 1 jaringan LAN fisik.
- VLAN adalah sebuah logical group yang memungkinkan user untuk berkomunikasi dengan user yang lain tetapi terisolasi dari user lain yang berbeda group.
- VLAN Bekerja di layer data link dengan standarisasi 802.1Q.
- Mikrotik RouterOS memungkinkan membuat beberapa Virtual LAN untuk memisahkan jaringan (group) di sebuah interface ethernet atau wireless.

802.1Q

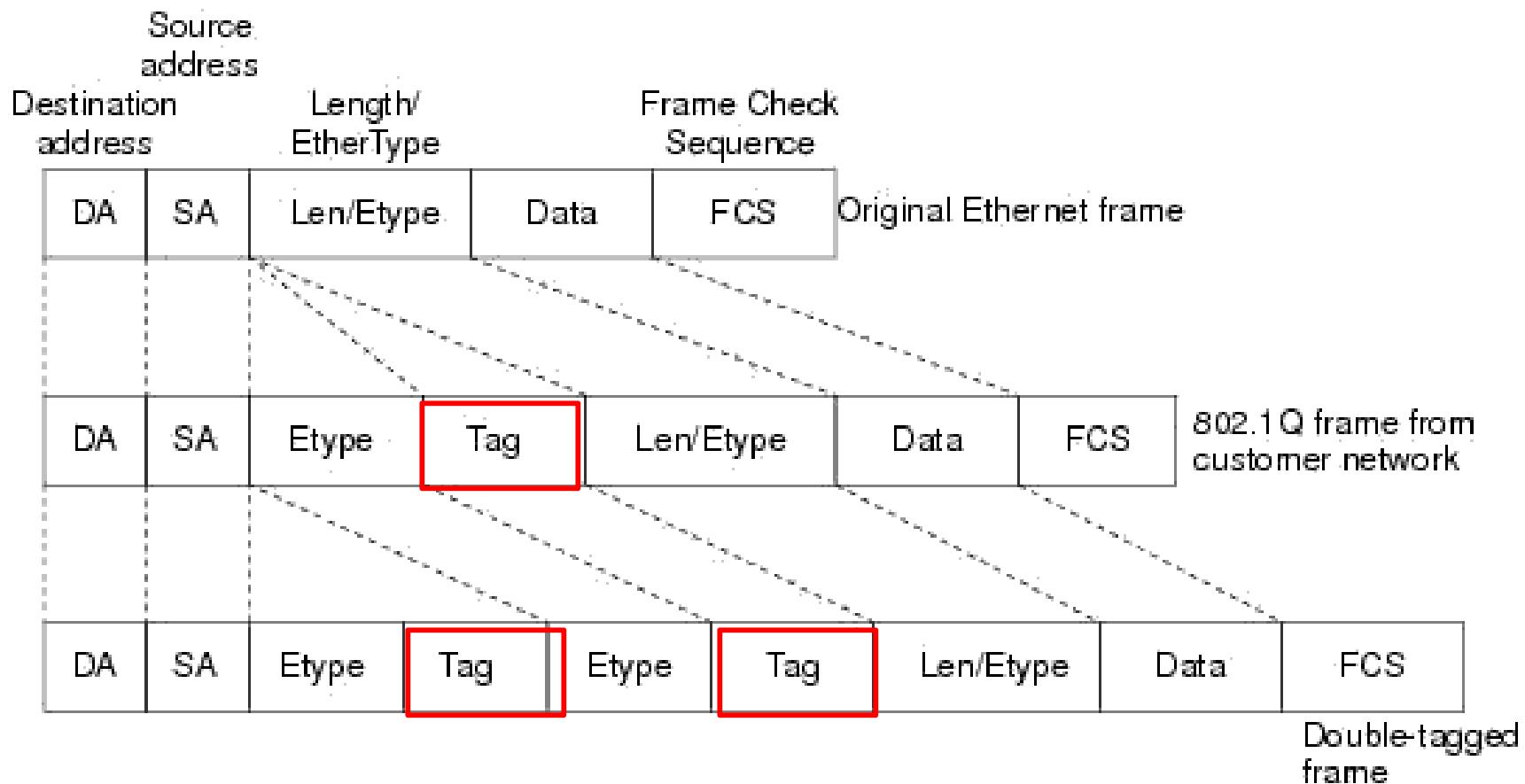
- Ethernet Frame



Insertion of 802.1Q Tag (VLAN ID) in Ethernet-II frame

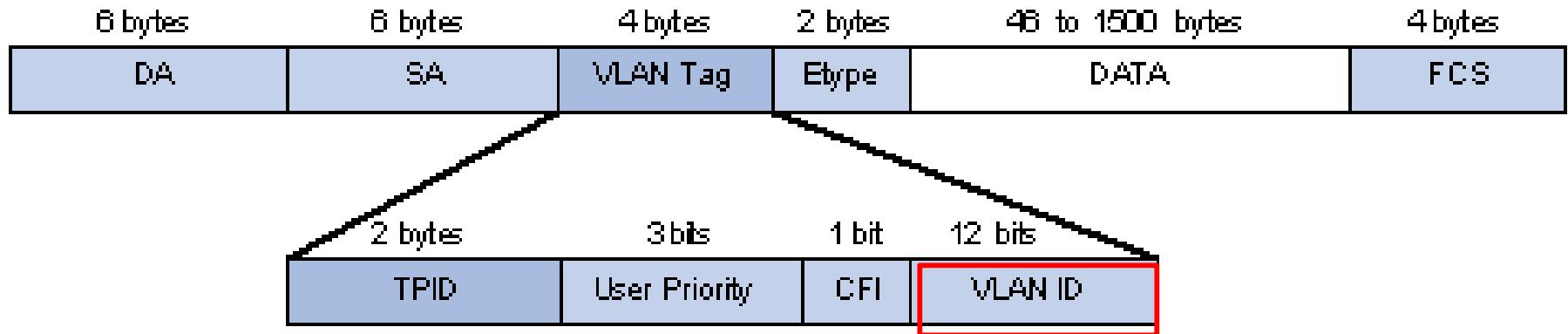
802.1QinQ / IEEE 802.1ad (VLAN over VLAN)

- Ethernet Frame



Frame Format .1Q

Ethernet Frame



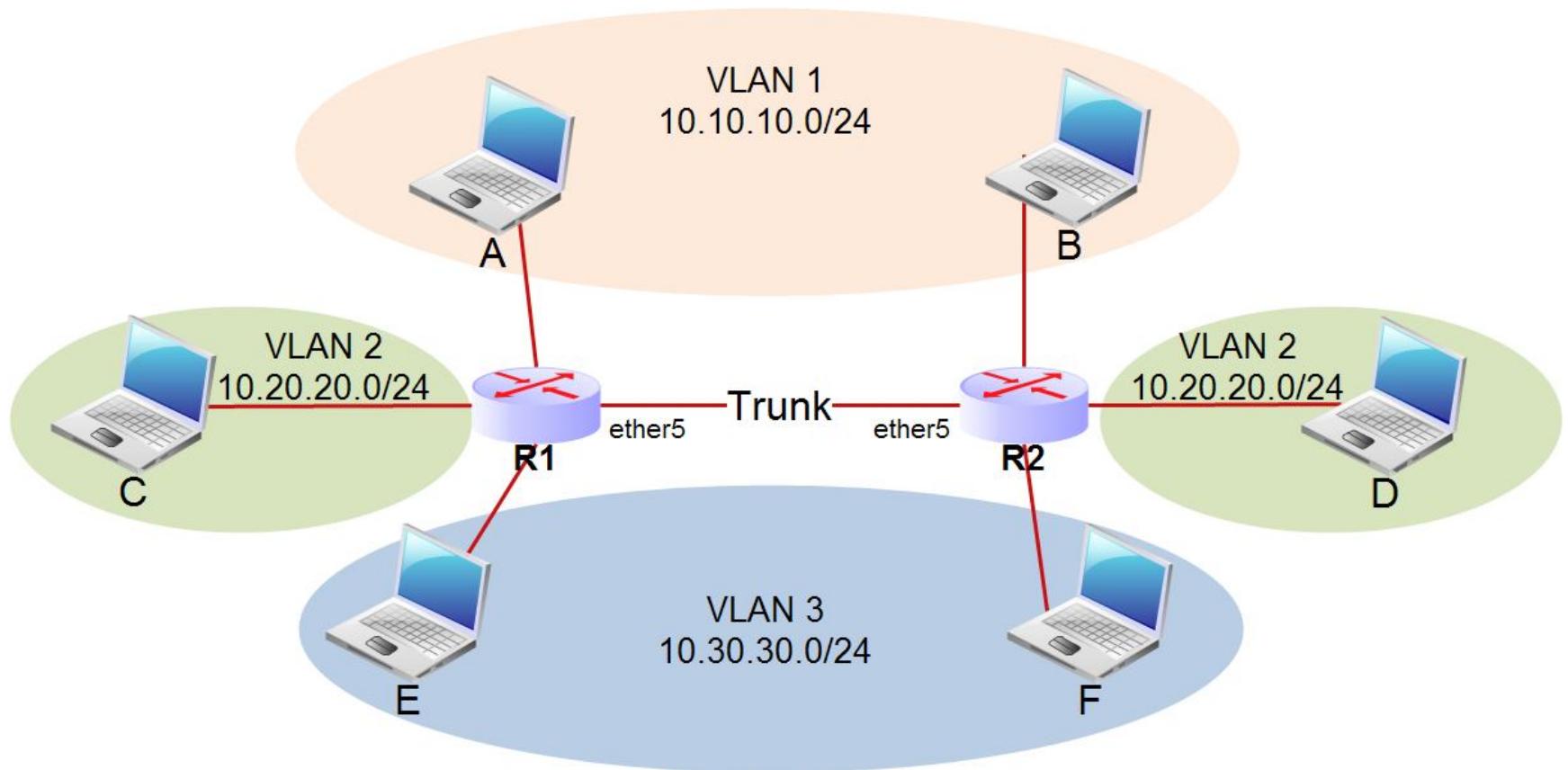
- Panjang total VLAN tag adalah 4 byte (32bit), panjang bit untuk VLAN ID adalah 12bits,
- Jumlah ID/tag yang bisa digunakan adalah 1-4095 (12 bit)
- Standar Maximum Transmission Unit (MTU) untuk ethernet frame adalah 1500 bytes
- Maka MTU untuk VLAN trunk adalah $1500 + 4 = 1504$ bytes
- MTU untuk VLAN over VLAN $1500 + 4 + 4 = 1508$ bytes

Switch port pada VLAN

Ada 2 jenis port /switch port pada VLAN

- Edge ports: (Untagged, pada Cisco: Access Port)
 - Adalah switch port yang dikonfigur sebagai bagian dari sebuah VLAN
 - switchport ini tidak mengirim 4 byte tag. Digunakan oleh device yang tidak melewatkkan VLAN seperti komputer klien, printer, dll.
- Core port: (Tagged, pada Cisco: Trunk Port)
 - Adalah switch port yang diconfigure untuk mengirim 4 byte VLAN tag. Digunakan oleh device yang mensupport VLAN seperti switches,routers and servers.

LAB XVI - VLAN



LAB XVI - VLAN

- Add new interface VLAN

The image shows two windows from the Winbox interface of a MikroTik router.

New Interface Dialog: This window is titled "New Interface". It has tabs for "General" and "Traffic". The "General" tab is selected. The fields are as follows:

- Name: vlan1
- Type: VLAN
- MTU: 1500
- L2 MTU: (empty)
- MAC Address: (empty)
- ARP: enabled
- VLAN ID: 1 (highlighted with a red box)
- Interface: ether5 (highlighted with a red box)
- Use Service Tag

Interface List Window: This window shows a list of all interfaces on the router. The table has columns: Name, Type, L2 MTU, Tx, Rx, and a small icon column.

	Name	Type	L2 MTU	Tx	Rx
R	ether1	Ethernet	1600	76.	
R	ether2	Ethernet	1598		
R	ether3	Ethernet	1598		
R	ether4	Ethernet	1598		
R	ether5	Ethernet	1598		
	vlan1	VLAN	1594		
	vlan2	VLAN	1594		
	vlan3	VLAN	1594		
	vlan4	VLAN	1594		
	vlan5	VLAN	1594		
R	wlan1	Wireless (Atheros 11N)	2290		

Annotations with red arrows point from specific fields in the "New Interface" dialog to their corresponding entries in the "Interface List" window:

- An arrow points from the "VLAN ID: 1" field in the dialog to the "vlan1" entry in the list.
- An arrow points from the "Interface: ether5" field in the dialog to the "ether5" entry in the list.
- A callout box labeled "VLAN ID = unik" points to the "vlan1" entry in the list.
- A callout box labeled "Interface untuk trunk" points to the "ether5" entry in the list.

LAB XVI - VLAN

- Buat bridge untuk membridge vlan dan interface fisik

The screenshot shows the Winbox interface for managing network bridges. At the top, there's a main window titled "Bridge" with tabs for Bridge, Ports, Filters, NAT, and Hosts. The "Bridge" tab is selected. Below the tabs are several icons: a red plus sign for adding, a minus sign for deleting, a checkmark, an X, a folder, a magnifying glass, and a gear icon for settings. To the right of these is a "Find" button. The main area is a table with columns: Name, Type, L2 MTU, Tx, Rx, Tx Pac..., Rx Pac..., and Tx Drops. Three rows are listed:

	Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops
R	bridgeVLAN1	Bridge	65535	0 bps	0 bps	0	0	0
R	bridgeVLAN2	Bridge	65535	0 bps	0 bps	0	0	0
R	bridgeVLAN3	Bridge	65535	0 bps	0 bps	0	0	0

Below this, four smaller windows show the configuration of individual bridge ports. The first two windows are grouped by a red box and apply to bridgeVLAN1. The third and fourth windows are also grouped by a red box and apply to bridgeVLAN2.

New Bridge Port (Top Left):
General tab selected
Interface: ether1
Bridge: bridgeVLAN1

New Bridge Port (Top Right):
General tab selected
Interface: wlan1
Bridge: bridgeVLAN1

New Bridge Port (Bottom Left):
General tab selected
Interface: ether2
Bridge: bridgeVLAN2

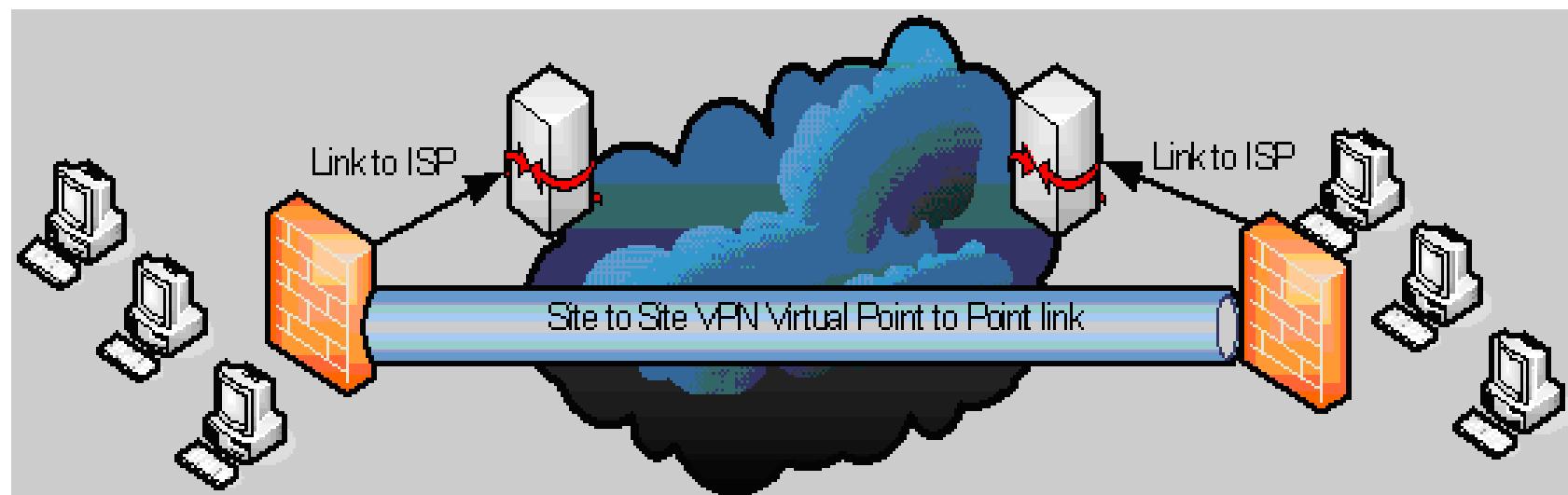
New Bridge Port (Bottom Right):
General tab selected
Interface: wlan2
Bridge: bridgeVLAN2

Tunnel

Tunnel

- Tunnel adalah sebuah metode penyelubungan (encapsulation) paket data di jaringan.
- Paket data mengalami modifikasi sebelum dikirim, yaitu penambahan header dari tunnel
- Ketika data sudah melewati tunnel dan sampai di tujuan (ujung) tunnel, maka header dari paket data akan dikembalikan seperti semula (header tunnel dilepas).

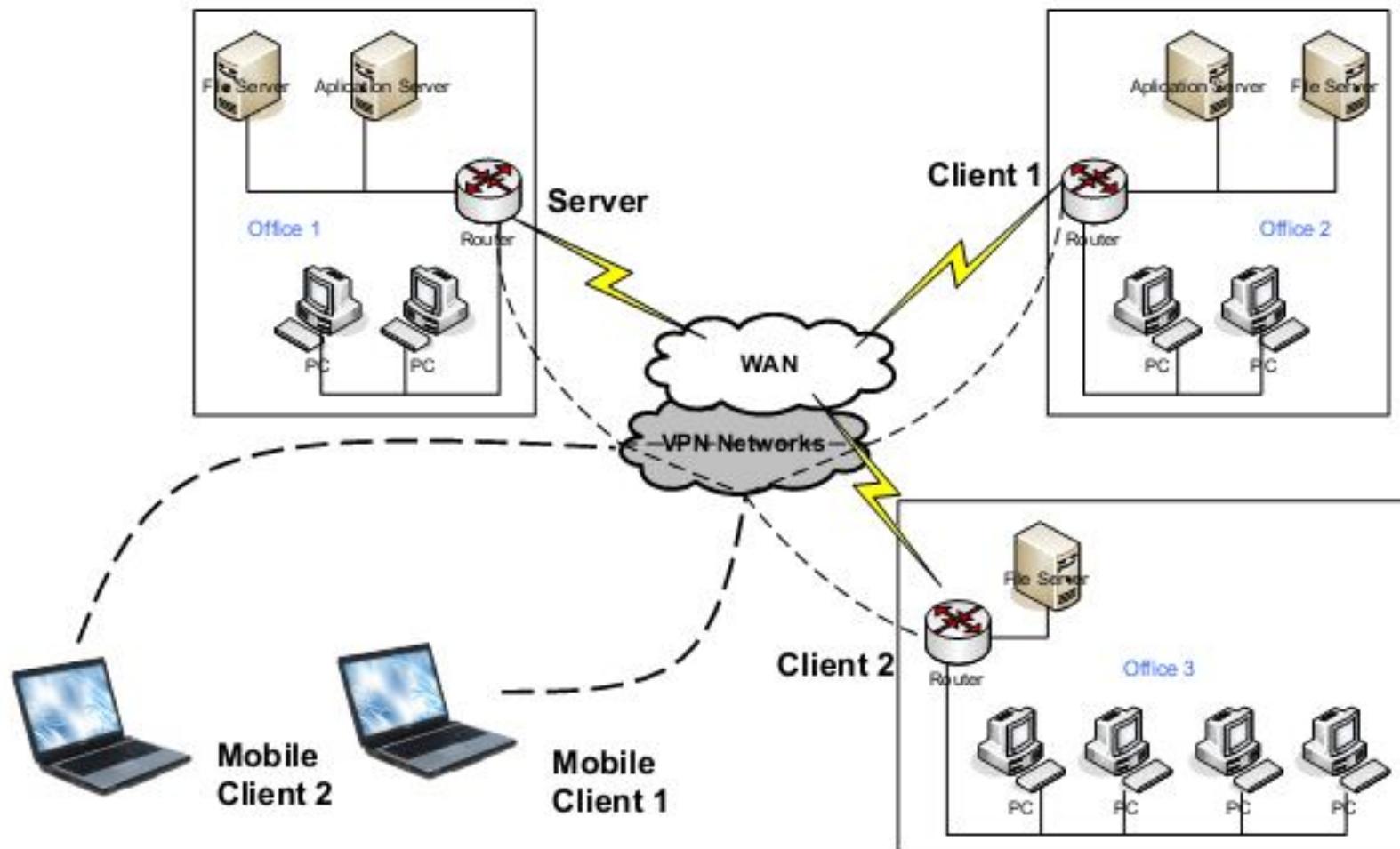
Tunnel



VPN

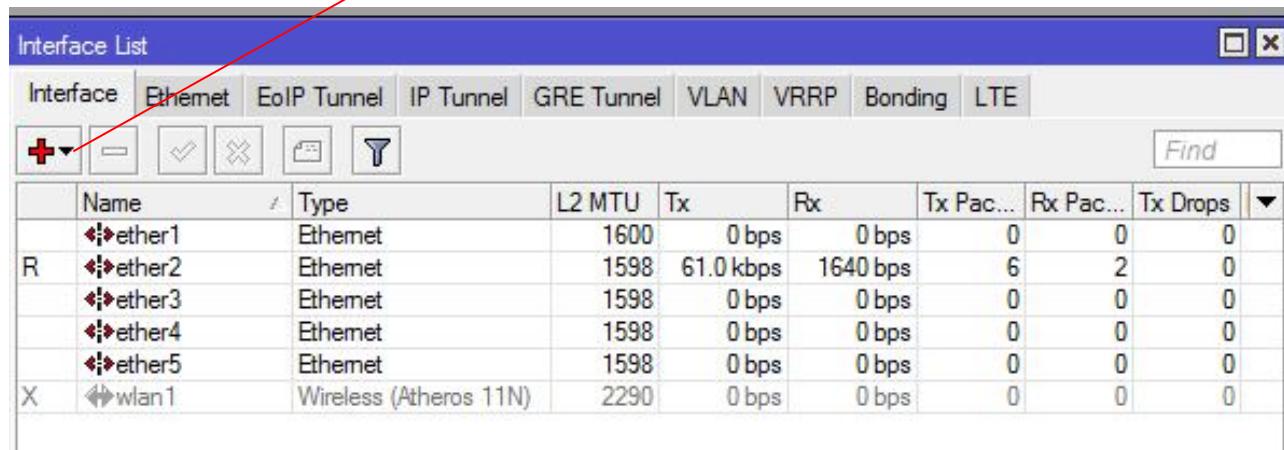
- VPN adalah sebuah cara aman untuk mengakses local area network dengan menggunakan internet atau jaringan publik.
- Tunnel atau terowongan merupakan kunci utama pada VPN, koneksi pribadi dalam VPN dapat terjadi dimana saja selama terdapat tunnel.

VPN



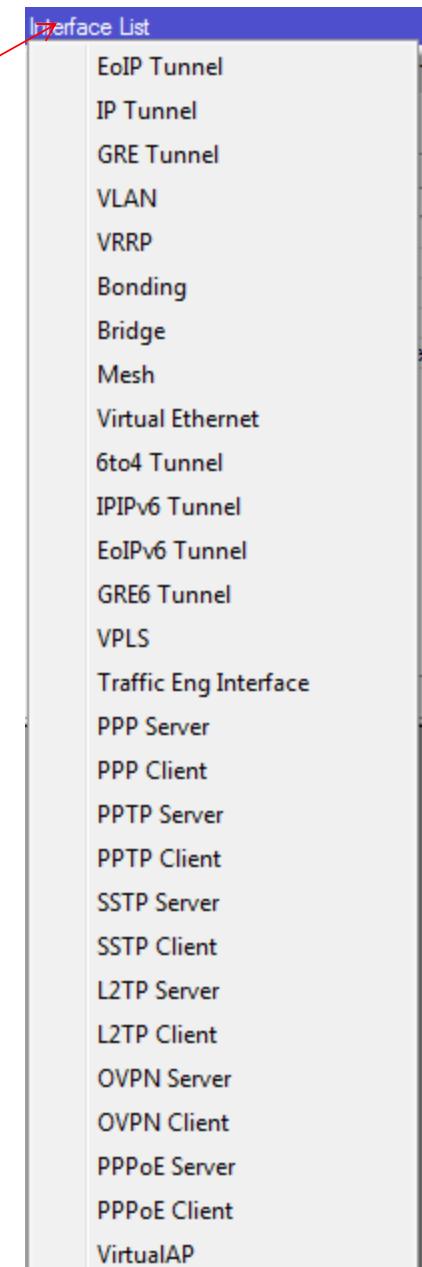
Tunnel Pada MikroTik

- Jenis Tunnel pada Mikrotik : PPTP, L2TP, PPPoE, EoIP, SSTP, OpenVPN, dll
- Jenis-jenis tunnel pada MikroTik dapat dilihat di list virtual interface yang dapat kita add/tambahkan.



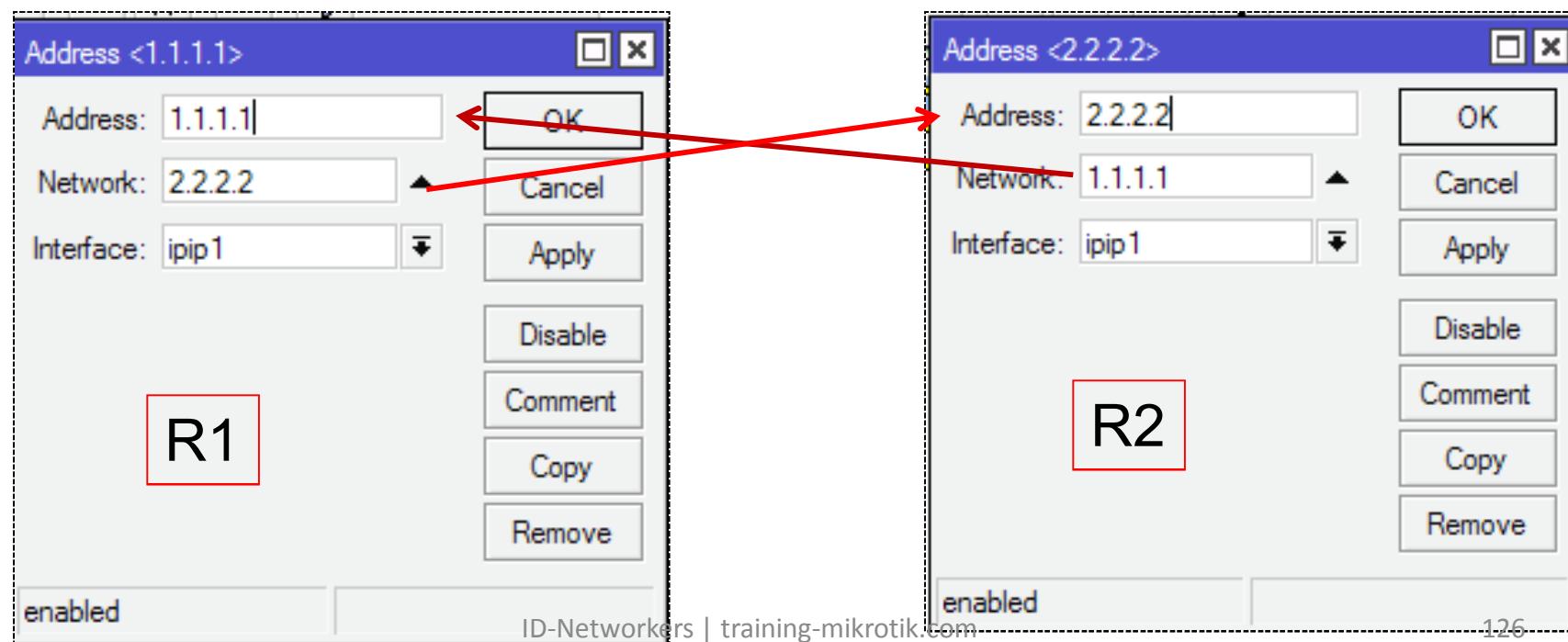
The screenshot shows the 'Interface List' window in MikroTik's Winbox interface. The window title is 'Interface List'. Below the title, there is a toolbar with several icons: a plus sign for adding new interfaces, a minus sign for deleting, a checkmark for selecting, an X for unselecting, a copy icon, and a filter icon. There is also a 'Find' button. The main area is a table with the following columns: Name, Type, L2 MTU, Tx, Rx, Tx Packets, Rx Packets, and Tx Drops. The table lists five physical Ethernet interfaces (ether1-ether5) and one wireless interface (wlan1). The wireless interface (wlan1) is listed as 'Wireless (Atheros 11N)' with an L2 MTU of 2290, 0 bps for both Tx and Rx, and 0 for all packet counts and drops.

	Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops
R	ether1	Ethernet	1600	0 bps	0 bps	0	0	0
R	ether2	Ethernet	1598	61.0 kbps	1640 bps	6	2	0
R	ether3	Ethernet	1598	0 bps	0 bps	0	0	0
R	ether4	Ethernet	1598	0 bps	0 bps	0	0	0
X	ether5	Ethernet	1598	0 bps	0 bps	0	0	0
X	wlan1	Wireless (Atheros 11N)	2290	0 bps	0 bps	0	0	0



Point to Point Addressing

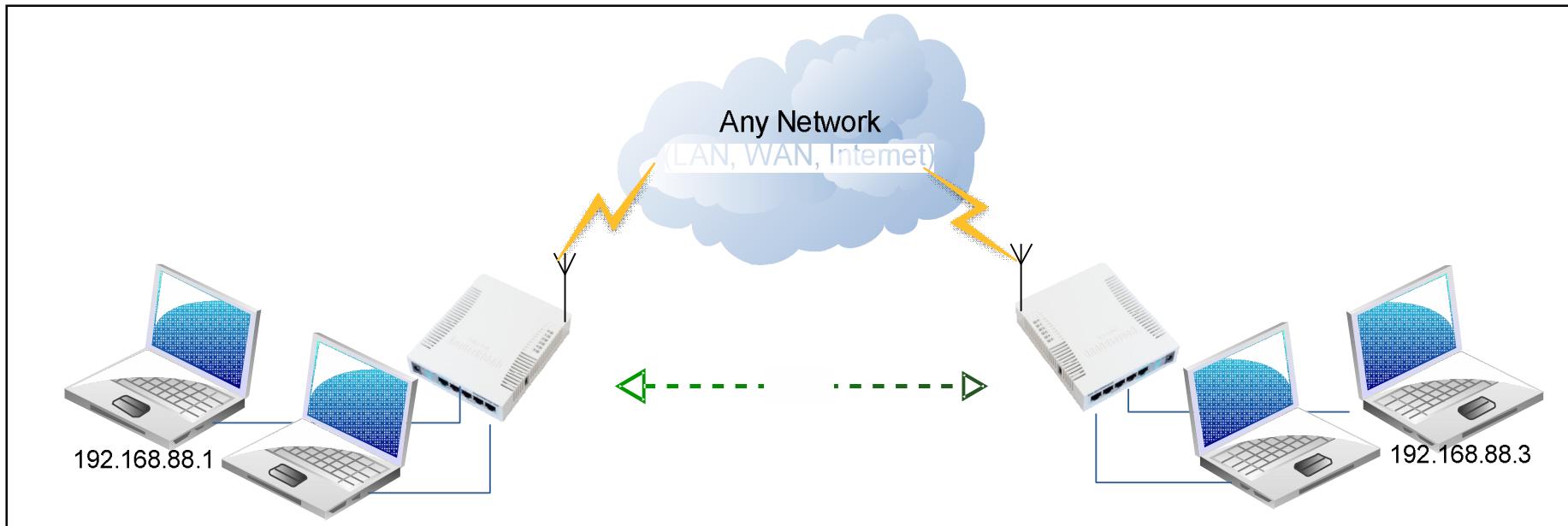
- Adalah sistem pengalamatan IP Address untuk dua buah perangkat yang terkoneksi langsung, menggunakan dua buah IP Address /32.
- Karena hanya menggunakan 2 IP address, tidak ada alamat broadcast, tetapi IP network harus diset secara manual diisi dengan alamat remote IP (opposite)



EoIP Tunnel

- EOIP merupakan protocol proprietary Mikrotik untuk membangun tunnel antar router Mikrotik, dimana interface EOIP akan dianggap sebagai interface ethernet virtual.
- Maksimum jumlah tunnel yang bisa dibuat oleh EoIP di MikroTik adalah 65535
- EoIP berjalan diatas jaringan internet (public), jaringan lokal (LAN) dan diatas tunnel lain (EoIP over IPIP atau EoIP over PPTP).
- MAC Address diantara interface EOIP harus dibedakan.
- EoIP menggunakan encapsulation Generic Routing Encapsulation (IP Protocol No 47). EoIP tidak menggunakan ekripsi, jadi tidak disarankan digunakan untuk transmisi data yang membutuhkan tingkat keamanan yang tinggi.
- Pada konfigurasi EoIP kita hanya mendefinisikan **IP address remote** (lawan) dan tunnel ID (disamakan).

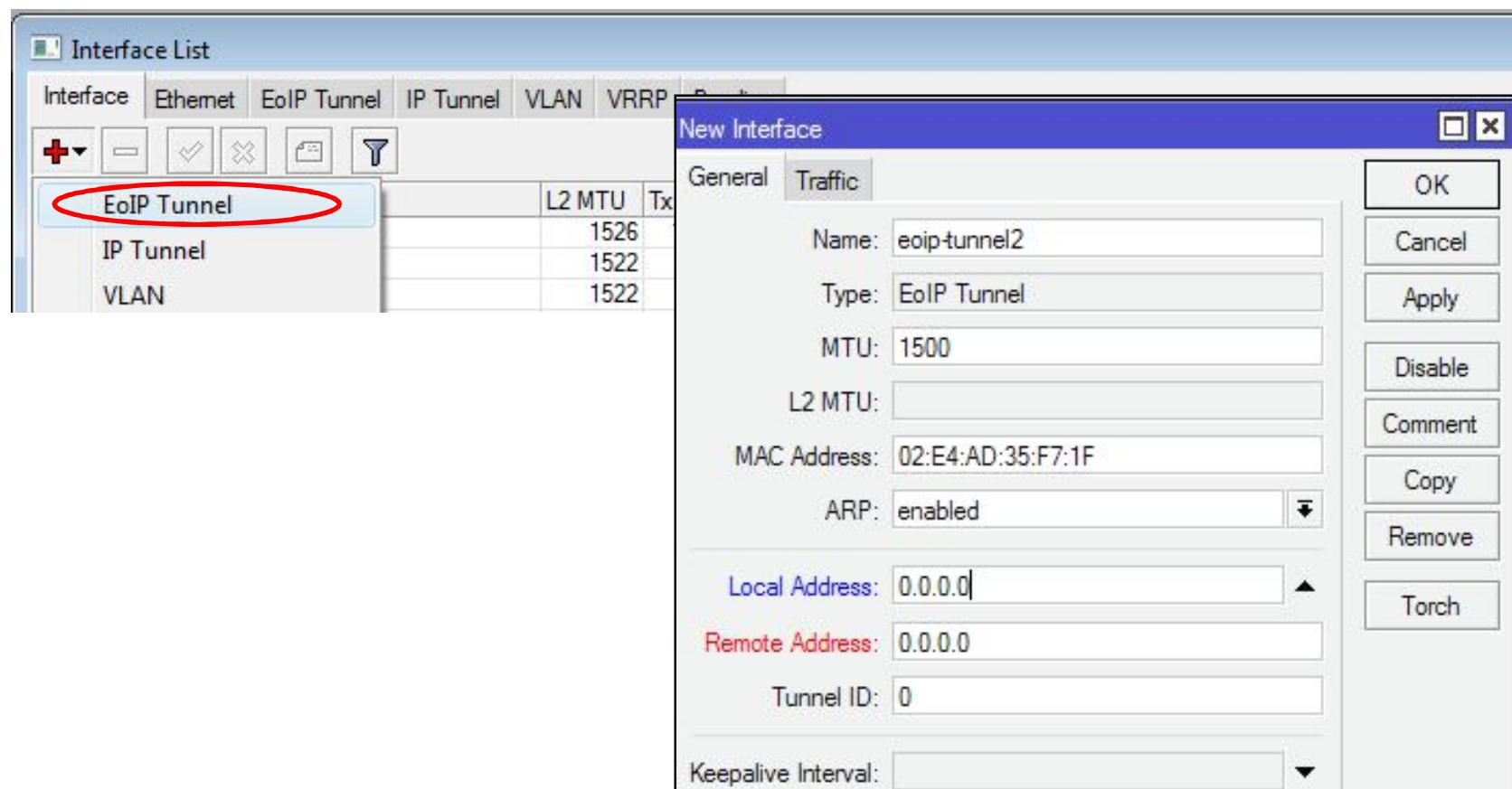
EoIP Tunnel



- Network Lokal (LAN) Office A dapat diakses dari Network Lokal (LAN) Office B.
- LAN Office A satu segmen dengan LAN office B.
- Apabila beda segmen/network, antar IP LAN harus di routing.

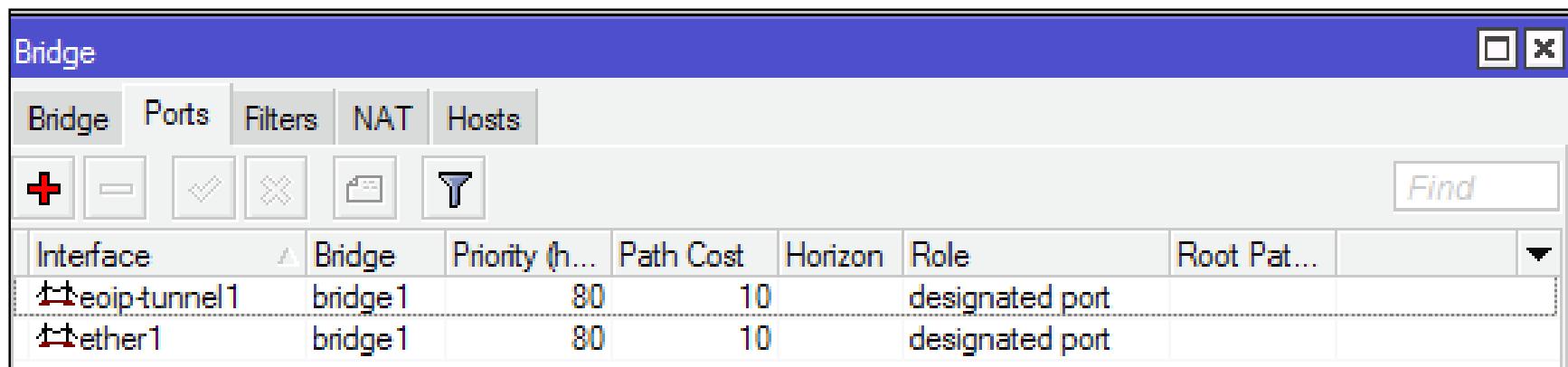
EoIP Tunnel

- Interface>Add>IP>New Interface EOIP Tunnel



EoIP Tunnel

- Interface EoIP yang terbentuk dapat dimasukkan dalam interface bridge.
- Misalkan EoIP di bridge dengan interface yang kearah LAN.



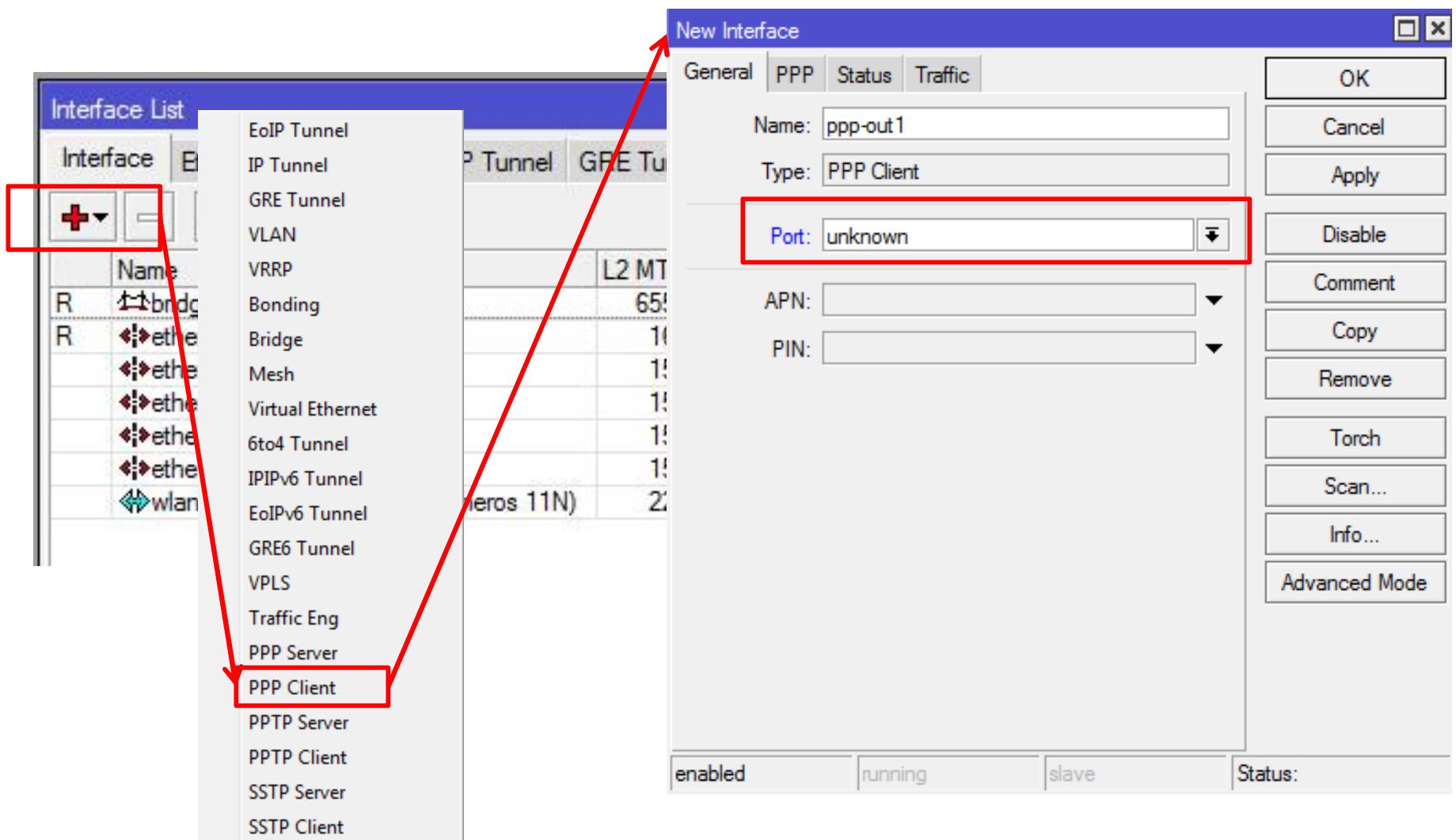
The screenshot shows the 'Bridge' configuration window in Winbox. The 'Bridge' tab is selected. The table lists two interfaces assigned to the bridge:

Interface	Bridge	Priority	Path Cost	Horizon	Role	Root Pat...
eoip-tunnel1	bridge1	80	10		designated port	
ether1	bridge1	80	10		designated port	

PPP

- PPP (Point to Point Protocol) adalah protocol layer 2 yang digunakan untuk komunikasi secara serial.
- Untuk menjalankan koneksi PPP, mikrotik RouterOS harus memiliki port/interface serial, line telephone port berupa RJ11 (PSTN), atau modem seluler (PCI atau PCMCIA)
- Untuk terbentuk koneksi PPP dilakukan melalui dial up nomer telepon tertentu ke ISP (misal nomor *99***1#).
- Kemudian ppp baru mendapatkan IP address untuk koneksi internet.
- MikroTik dapat digunakan sebagai PPP server dan atau PPP client.

Setting PPP Client

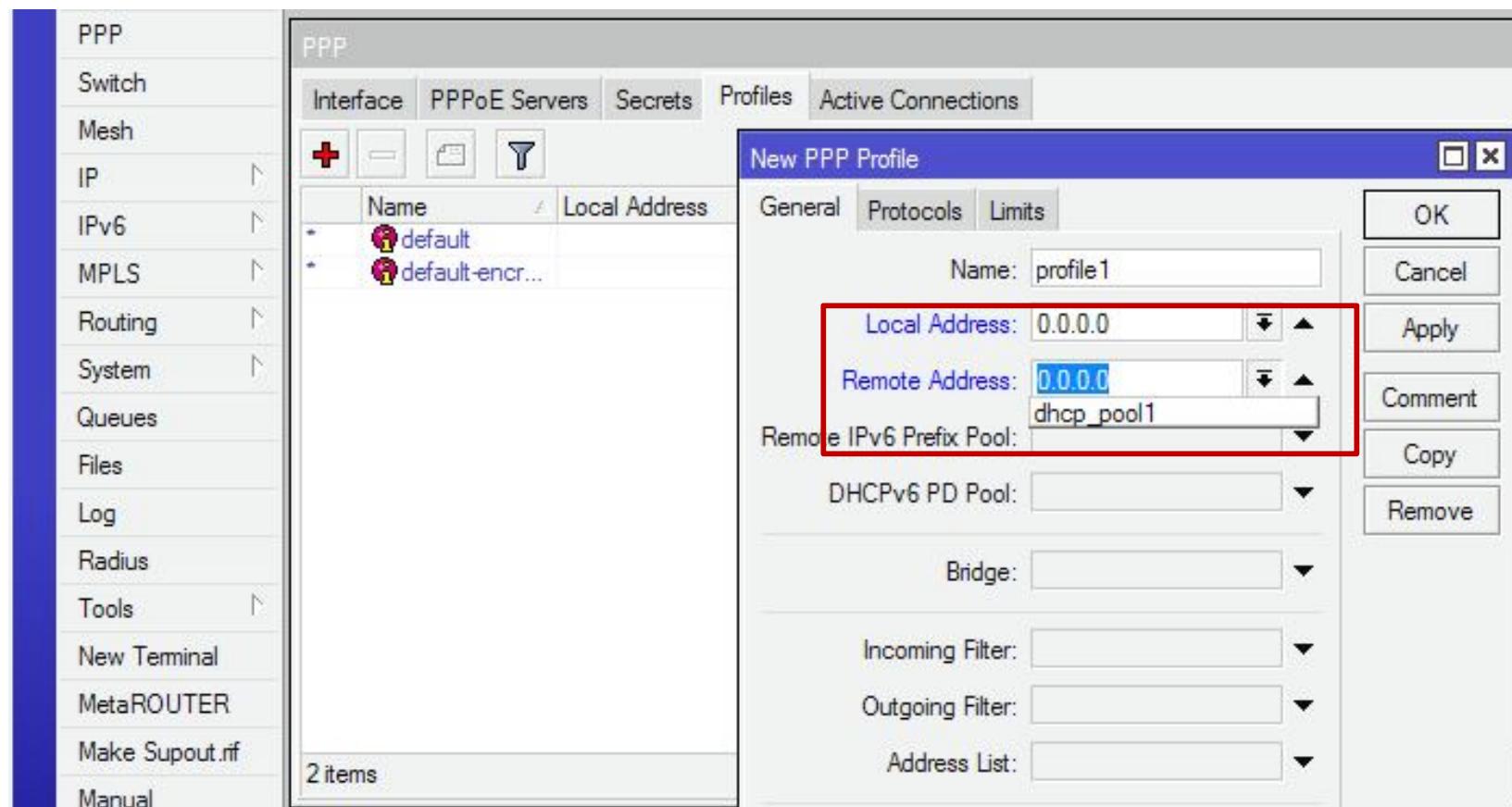


PPTP Tunneling

- PPTP melakukan tunneling packet PPP kedalam IP packet menggunakan protocol TCP dan GRE (Generic Routing Encapsulation)
- PPTP menggunakan port TCP 1723
- PPTP banyak digunakan karena hampir semua OS dapat menjalankan PPTP client.
- Sebelum menjalankan PPTP server, hal yang perlu diperhatikan adalah setting **PPP Secret** dan **PPP Profiles**.

PPP Profile

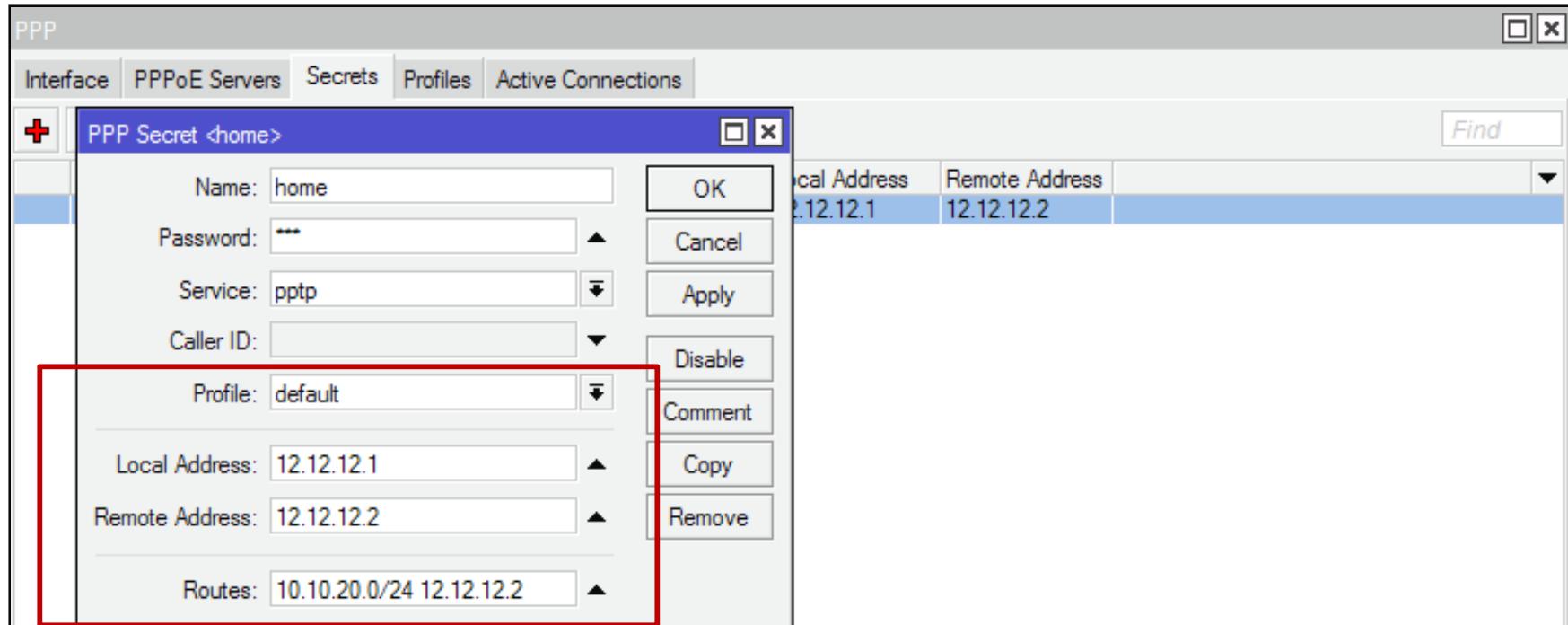
- PPP Profile digunakan untuk setting ip local address dan remote address, remote address dapat menggunakan ip pool.



PPP Secret

- Semua koneksi yang terjadi dalam PPP tunnel selalu melibatkan authentikasi username dan password.
- Secara local, username dan password ini disimpan dan diatur dalam PPP secret.
- Username dan password ini juga dapat disimpan dalam RADIUS server terpisah.
- PPP Secret (database local PPP) menyimpan username dan password yang akan diberikan ke pelanggan/user. PPP secret dipakai untuk koneksi client ; **async, l2tp, openvpn, pppoe, pptp dan sstp.**

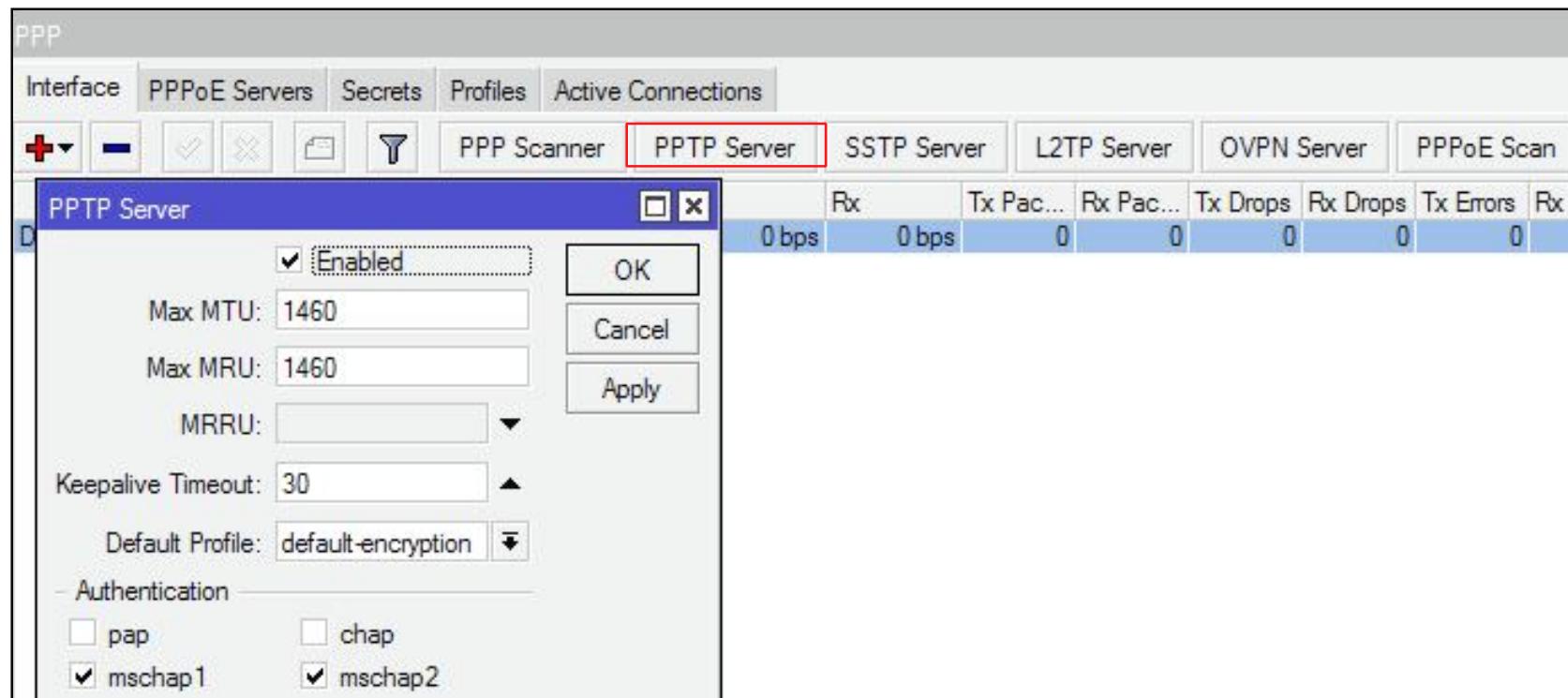
PPP Secret



- Profile = mengambil dari ppp profile
- Local & remote address = diisi IP untuk koneksi PPP
- Routes = Disini kita menambahkan konfigurasi untuk routes 10.10.20.0/24 12.12.12.2 yang akan ditambahkan secara otomatis apabila terbentuk koneksi dari pptp client

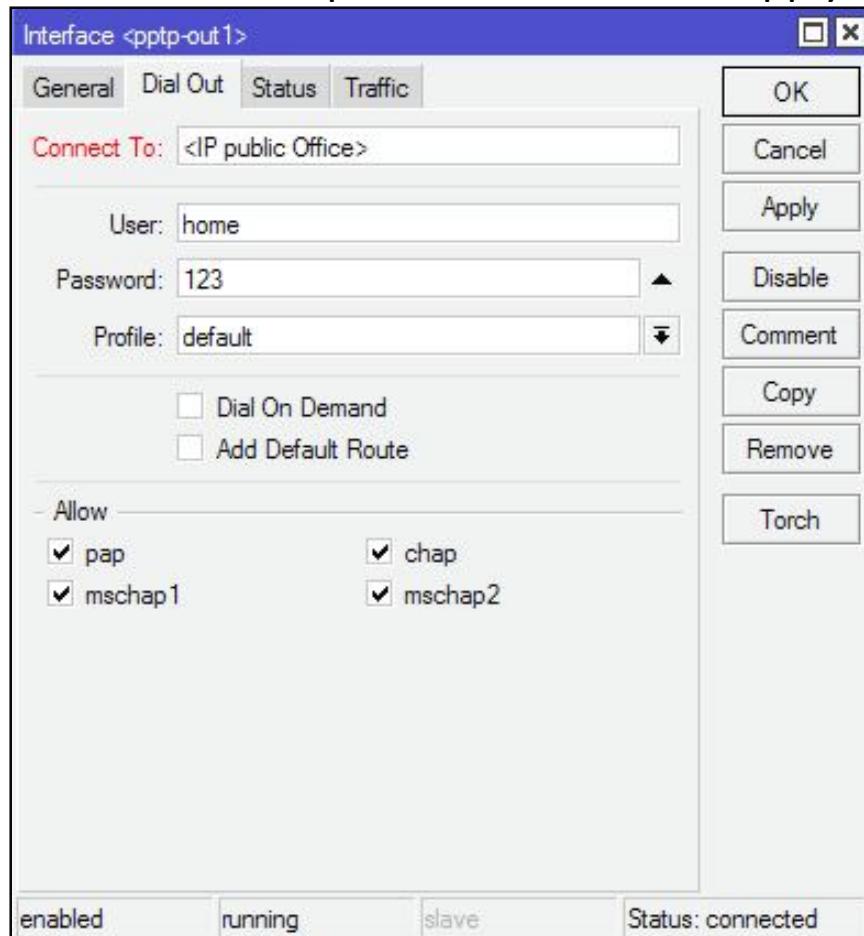
Mengaktifkan PPP Server

- Aktifkan PPTP server pada menu PPP>Interface>PPTP Server



MikroTik PPTP Client

- Add new interface pptp, pada tab Dial Out isikan dengan IP public dari router Office, user dan password, kemudian apply



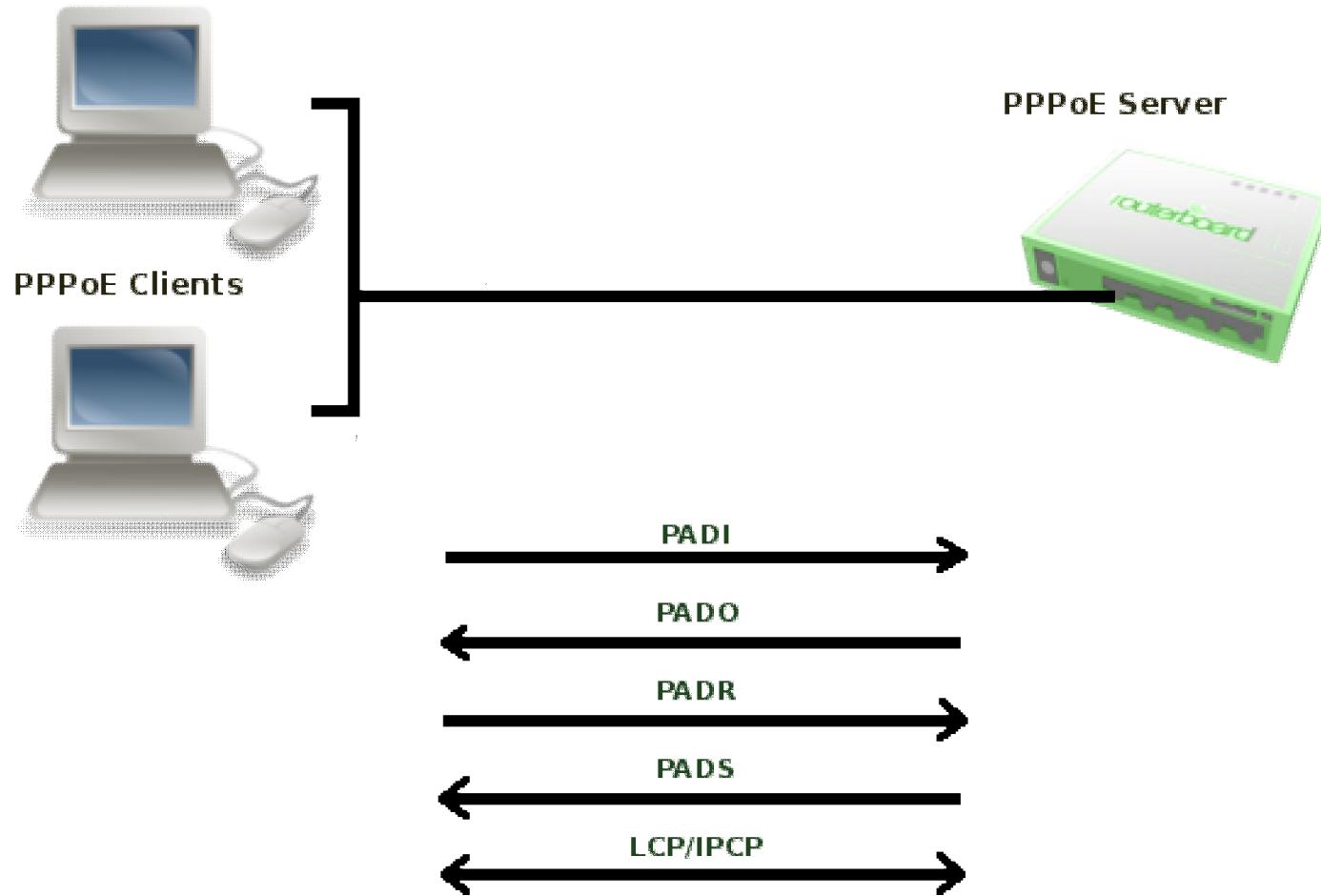
Tunnel

VPN Protocol	Encryption	Ports	Compatible with	Notes
PPTP	MPPE with RC4 128 bit key	1723 TCP	Windows XP, Vista, 7 Mac OS X iPhone OS Android	PPTP is the most widely used VPN protocol today. It is easy to setup and can be used to bypass all Internet restrictions. PPTP is considered less secure.
L2TP	IPsec with 3DES 168 bit key	500 UDP 1701 UDP 5500 UDP	Windows XP, Vista, 7 Mac OS X Android	L2TP is considered more secure than PPTP. If online security is a main concern you should consider using L2TP.
SSTP	SSL with AES 2048 bit key certificate 256 bit key for encryption	443 TCP	Windows 7	SSTP uses a generic port that is never blocked by firewalls. You can use SSTP to bypass corporate or school firewalls. SSTP is considered a very secure protocol.

PPPoE

- PPPoE adalah untuk enkapsulasi frame Point-to-Point Protocol(PPP) di dalam paket Ethernet,
- PPPoE biasanya dipakai untuk jasa layanan ADSL untuk menghubungkan modem ADSL (kabel modem) di dalam jaringan Ethernet (TCP/IP).
- PPPoE, adalah Point-to-Point, di mana harus ada satu point ke satu point lagi. Lalu, apabila point yang pertama adalah router ADSL kita, lalu di mana point satu nya lagi ?
- Tapi, bagaimana si modem ADSL bisa tahu point satunya lagi apabila kita (biasanya) hanya mendapatkan username dan password dari provider?
- Tahap awal dari PPPoE, adalah PADI (PPP Active Discovery Initiation), PADI mengirimkan paket broadcast ke jaringan untuk mencari di mana lokasi Access Concentrator di sisi ISP.

PPPoE



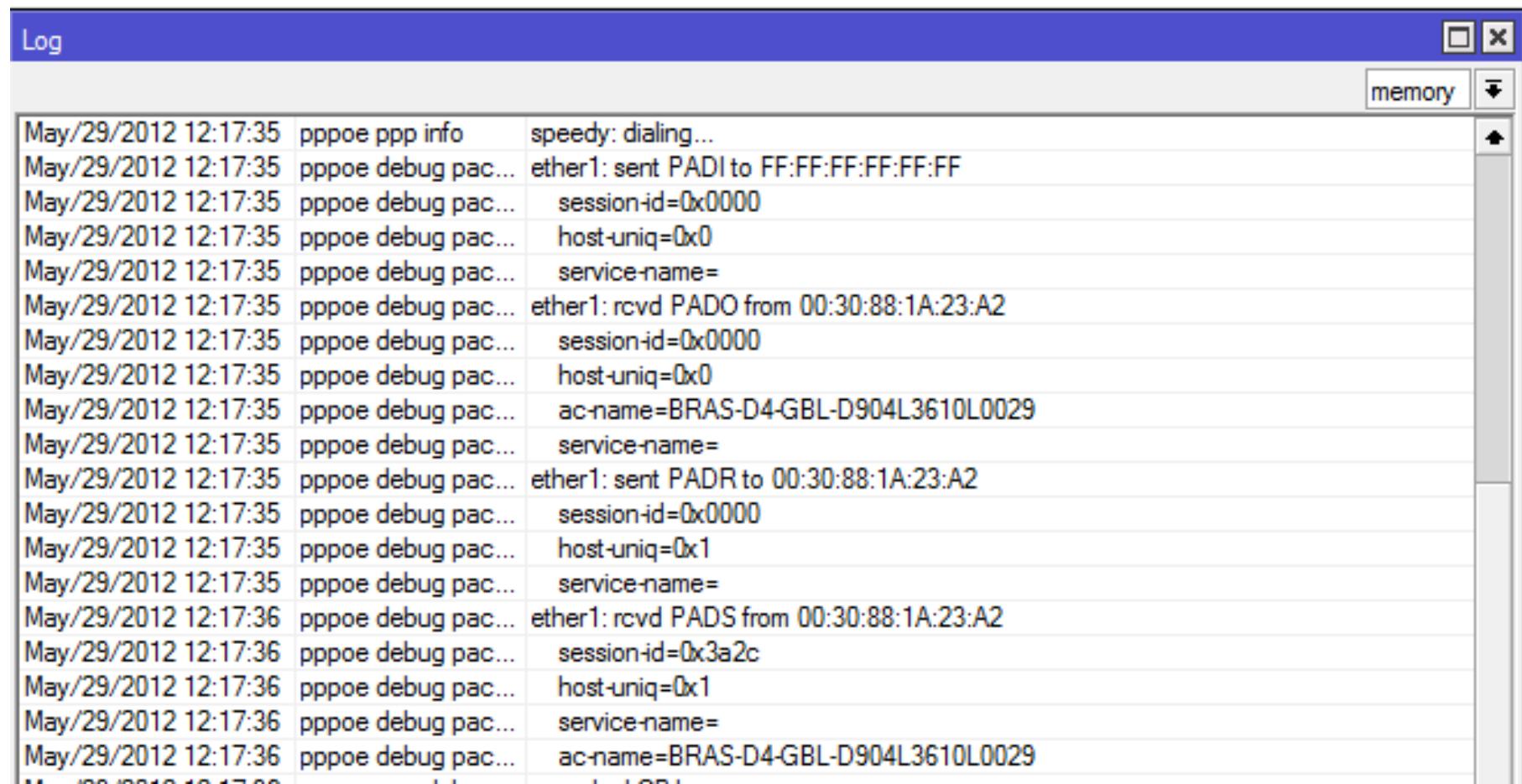
Tahapan Koneksi PPPoE

- PADI (PPP Active Discovery Initiation), Di sini PPoE client mengirimkan paket broadcast ke jaringan dengan alamat pengiriman mac address FF:FF:FF:FF:FF:FF. PPoE client mencari di mana lokasi PPoE server dalam jaringan.
- PADO (PPPoE Active Discovery Offer). PADO ini merupakan jawaban dari PPoE server atas PADI yang didapatkan sebelumnya. PPoE server memberikan identitas berupa MAC addressnya.
- PADR (PPP Active Discovery Request), merupakan konfirmasi dari PPoE client ke server. Disini PPoE client sudah dapat menghubungi PPoE server menggunakan mac addressnya, berbeda dengan paket PADI yang masih berupa broadcast.

Tahapan Koneksi PPPoE

- PADS (PPP Active Discovery Session-confirmation), dari PPoE server ke client. Session-confirmation di sini memang berarti ada session ID yang diberikan oleh server kepada client. Pada tahap ini juga terjadi negosiasi Username, password dan IP address.
- PADT (PPP Active Discovery Terminate), bisa dikirim dari server ataupun client, ketika salah satu ingin mengakhiri koneksi

Tahapan Koneksi PPPoE



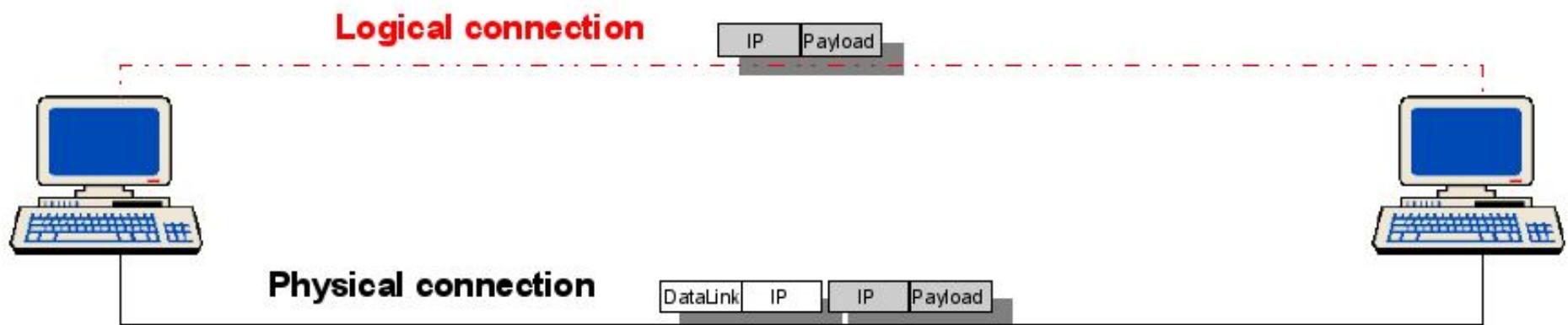
The screenshot shows a Windows-style log window titled "Log". The window has a blue header bar with the title "Log" and standard window controls (minimize, maximize, close). Below the header is a toolbar with a "memory" button and a scroll bar. The main area contains a list of log entries. Each entry consists of a timestamp, a program name, and a message. The log entries are as follows:

Timestamp	Program	Message
May/29/2012 12:17:35	pppoe ppp info	speedy: dialing...
May/29/2012 12:17:35	pppoe debug pac...	ether1: sent PADI to FF:FF:FF:FF:FF:FF
May/29/2012 12:17:35	pppoe debug pac...	session-id=0x0000
May/29/2012 12:17:35	pppoe debug pac...	host-uniq=0x0
May/29/2012 12:17:35	pppoe debug pac...	service-name=
May/29/2012 12:17:35	pppoe debug pac...	ether1: rcvd PADO from 00:30:88:1A:23:A2
May/29/2012 12:17:35	pppoe debug pac...	session-id=0x0000
May/29/2012 12:17:35	pppoe debug pac...	host-uniq=0x0
May/29/2012 12:17:35	pppoe debug pac...	ac-name=BRAS-D4-GBL-D904L3610L0029
May/29/2012 12:17:35	pppoe debug pac...	service-name=
May/29/2012 12:17:35	pppoe debug pac...	ether1: sent PADR to 00:30:88:1A:23:A2
May/29/2012 12:17:35	pppoe debug pac...	session-id=0x0000
May/29/2012 12:17:35	pppoe debug pac...	host-uniq=0x1
May/29/2012 12:17:35	pppoe debug pac...	service-name=
May/29/2012 12:17:36	pppoe debug pac...	ether1: rcvd PADS from 00:30:88:1A:23:A2
May/29/2012 12:17:36	pppoe debug pac...	session-id=0x3a2c
May/29/2012 12:17:36	pppoe debug pac...	host-uniq=0x1
May/29/2012 12:17:36	pppoe debug pac...	service-name=
May/29/2012 12:17:36	pppoe debug pac...	ac-name=BRAS-D4-GBL-D904L3610L0029

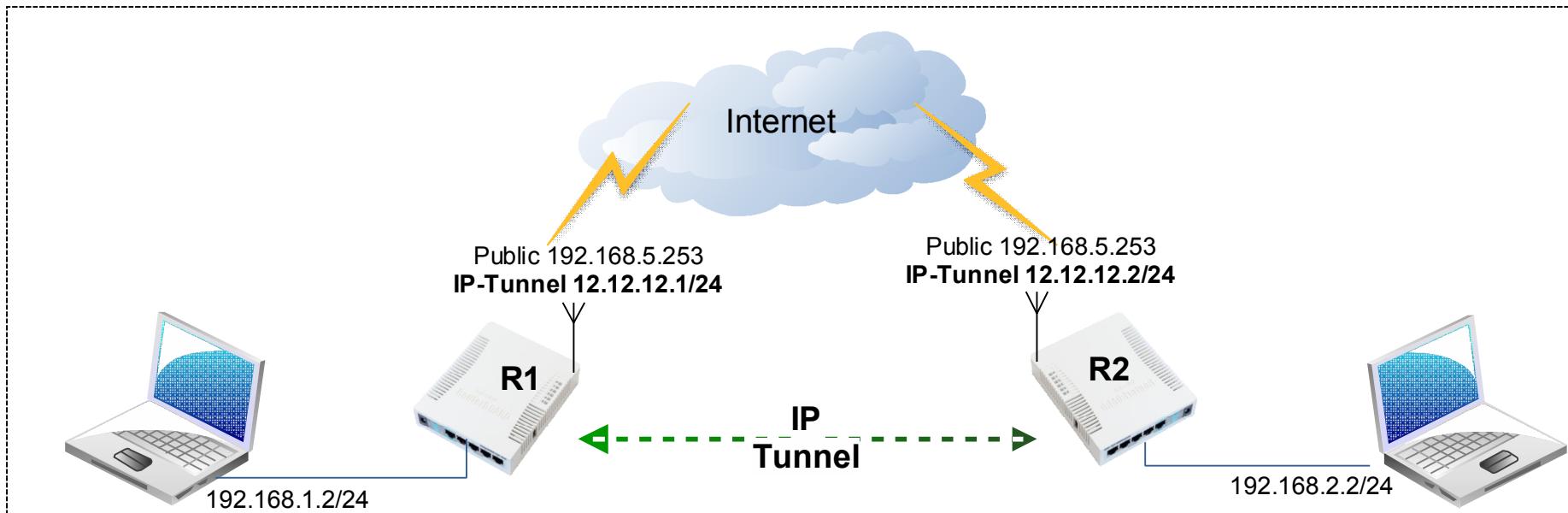
IPIP Tunnel

- IP-in-IP atau IPIP tunnel atau biasa disingkat ip tunnel adalah salah satu bentuk sederhana dari virtual private network/vpn, yaitu mekanisme menyambungkan 2 atau lebih jaringan (umumnya jaringan private/LAN - tapi tidak selalu demikian) melalui jaringan publik (internet).
- IPIP Tunnel bisa dibuat di menu Interface dan dianggap sebagai interface tetapi virtual yang independen.
- Interface IPIP tidak dapat dibridging.
- IPIP juga dapat digunakan untuk IPv6 tunneling pada IPV4

IPIP Tunneling



IPIP Tunnel



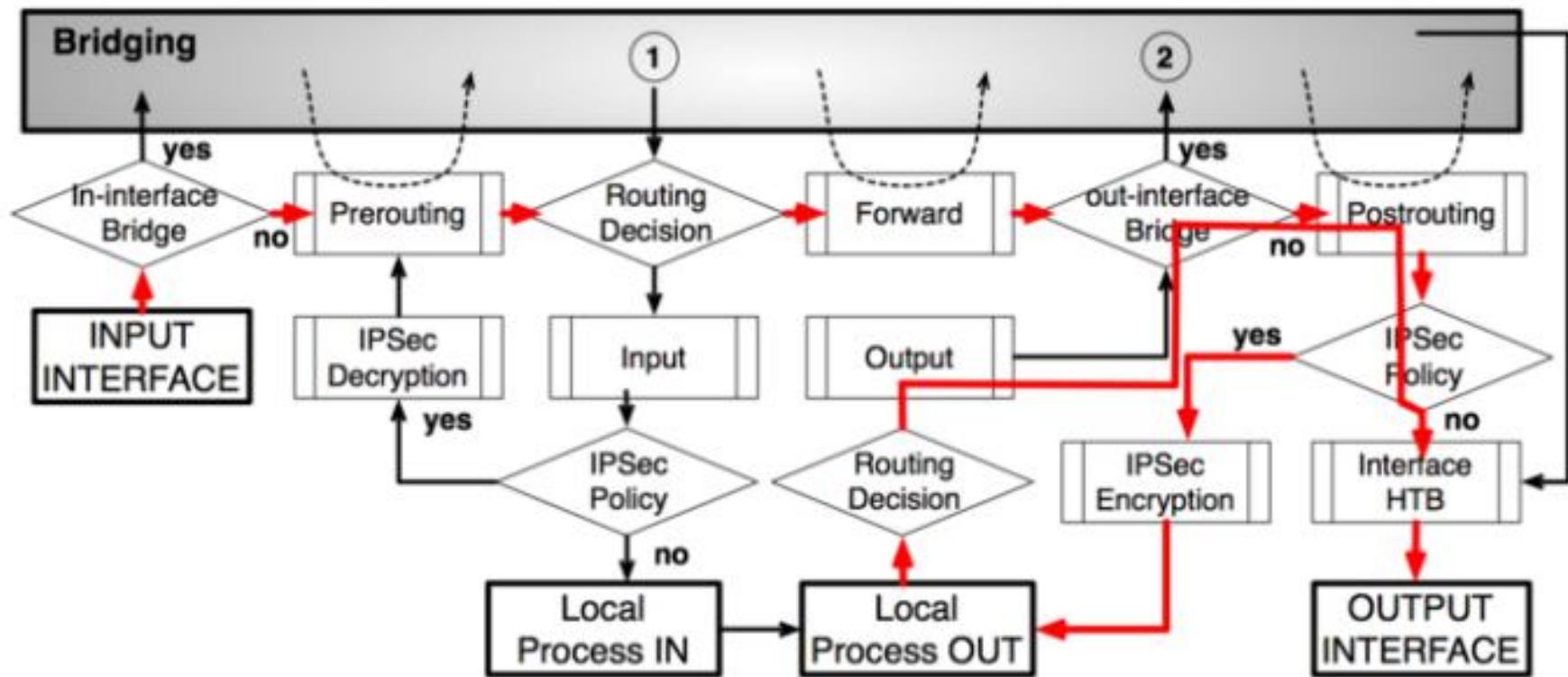
IP Security / VPN (IPSec)

- Protocol IPSec (IP Security) mampu mengimplementasikan security (Enkripsi) di komunikasi jaringan TCP/IP.
- IP Sec bekerja pada layer 4 (transport layer) pada OSI-7
- Pada setiap traffic akan diperlakukan dua fase : Encryption & Decryption
- Pada traffic yang menggunakan IPSec, kedua router akan memiliki peran atau posisi yang berbeda :
 - Initiator – Sebagai router yang menentukan encryption policy (metode autentikasi dan enkripsi yang ada di tawarkan - Proposal).
 - Responder – Router yang menjadi posisi ini akan menyesuaikan metode autentikasi dan enkripsi supaya komunikasi yang terenkripsi dapat dijalankan.
- Selama Router Responder tidak dapat menyamakan metode enkripsi dan autentikasi yang ditawarkan oleh router Initiator maka komunikasi akan di drop

IPSec Encryption

- Setelah paket terkena proses src-nat tetapi sebelum masuk kedalam interface-queue, paket data akan dihadapkan pada pilihan akan dienkripsi atau tidak berdasarkan database policy dari IPsec yaitu berdasarkan SPD (Security Policy Database).
- SPD memiliki dua bagian :
 - Packet Matching – daftar dari src/dst address, protocol dan port (TCP dan UDP) dari traffic yang akan dienkripsi.
 - Action – Jika rule dengan type data mengalami kecocokan maka :
 - Accept – paket akan diteruskan tanpa ada proses enkripsi
 - Drop – paket akan di drop
 - Encrypt – paket data akan dilakukan proses Enkripsi
- Database policy (SPD) bisa berupa kombinasi dari implementasi security yaitu dari beberapa metode enkripsi seperti key, algoritma.

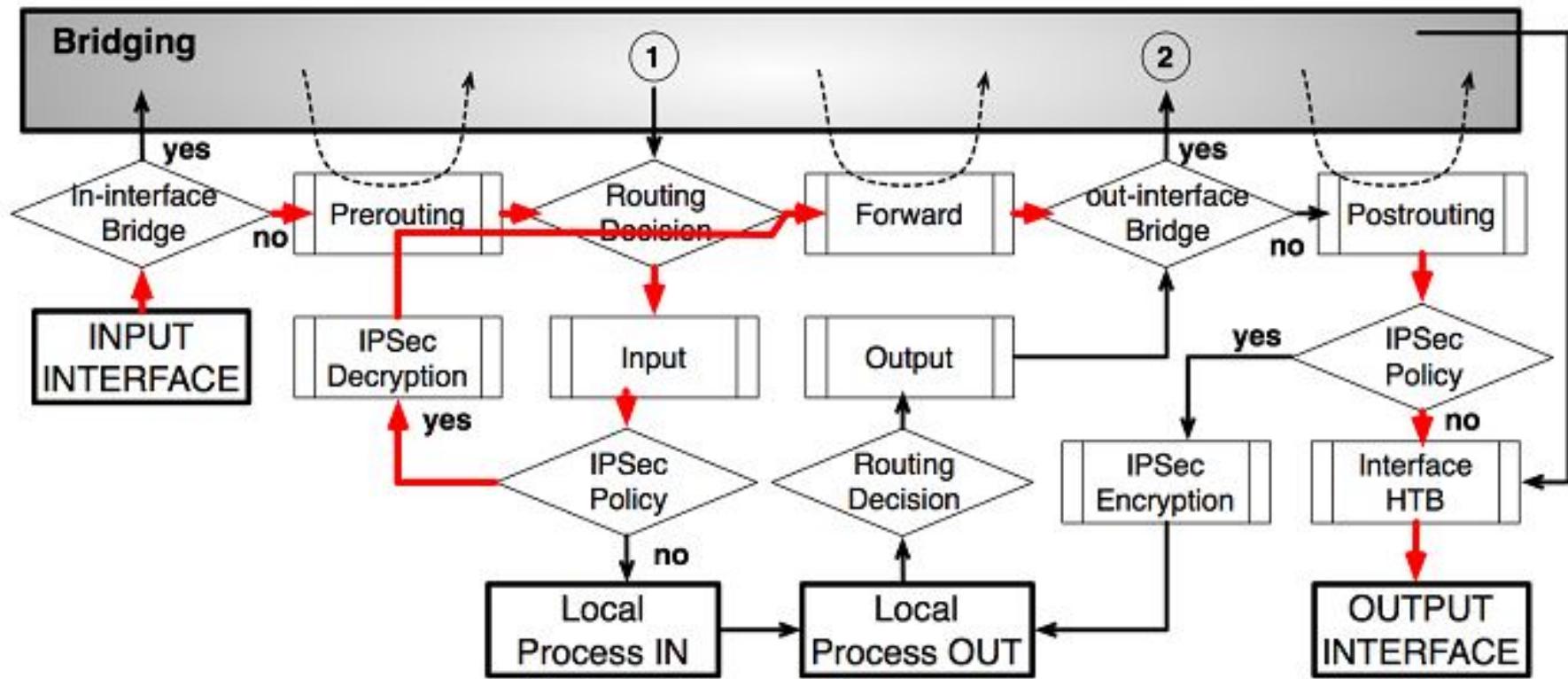
IPSec Encryption Flow



IPSec Description

- Jika paket yang terkena enkripsi diterima oleh router host (setelah dst-nat dan filter Input), maka router akan mencocokkan metode enkripsi dari paket untuk melakukan proses Dekripsi.
- Jika metode tidak ditemukan maka paket akan di drop tetapi jika ditemukan maka paket akan didekripsi.
- Jika proses dekripsi berjalan lancar paket akan kembali dimasukkan melewati dst-nat dan routing table untuk kembali didistribusikan ketujuan yang asli.
- Sedikit catatan dimana paket berada sebelum chain forward dan input paket akan dihadapkan lagi ke SPD dan dicocokkan kembali jika masih memerlukan enkripsi maka paket akan di drop. Proses ini disebut Incoming Policy Check.

IPSec Description Flow



Setting IPSec(1)

- IP Sec diseting berpasangan pada router dengan atau tanpa metode tunnel
- Setting pada IP>IPSec>>Policy>General & action

The image displays four windows from a MikroTik interface, arranged in a 2x2 grid, showing the configuration of IPsec policies between two routers, R1 and R2.

- R1 (Top Left):** Shows the General tab of the IPsec Policy configuration window for the pair 192.168.1.14:0->192.168.1.13:0. The "Src. Address" is 192.168.1.14 and "Dst. Address" is 192.168.1.13. The "Protocol" is set to 255 (all). The "Action" tab shows "Action: encrypt", "Level: require", "IPsec Protocols: esp", and "Tunnel" checked. The "SA Src. Address" is 192.168.1.14 and "SA Dst. Address" is 192.168.1.13. The "Proposal" is default and "Priority" is 0. Both tabs have an "enabled" status at the bottom.
- R2 (Top Right):** Shows the General tab of the IPsec Policy configuration window for the pair 192.168.1.13:0->192.168.1.14:0. The "Src. Address" is 192.168.1.13 and "Dst. Address" is 192.168.1.14. The "Protocol" is set to 255 (all). The "Action" tab shows "Action: encrypt", "Level: require", "IPsec Protocols: esp", and "Tunnel" checked. The "SA Src. Address" is 192.168.1.13 and "SA Dst. Address" is 192.168.1.14. The "Proposal" is default and "Priority" is 0. The "Comment" button is highlighted with a red box.
- R1 (Bottom Left):** Shows the General tab of the IPsec Policy configuration window for the pair 192.168.1.14:0->192.168.1.13:0. This window is identical to the one above it, showing the same settings for R1's perspective.
- R2 (Bottom Right):** Shows the General tab of the IPsec Policy configuration window for the pair 192.168.1.13:0->192.168.1.14:0. This window is identical to the one above it, showing the same settings for R2's perspective.

ID-Networkers | training-mikrotik.com

Setting IPSec(2)

- IP Sec diseting berpasangan pada router yang telah sukses di-tunnel
- Setting pada IP>IPSec>>Policy>peer

The image shows two identical configuration dialogs for 'IPsec Peer <0.0.0.0/0>'. Both dialogs contain the following fields:

- Address: 0.0.0.0/0
- Port: 500
- Auth. Method: pre shared key
- Secret: 123
- Exchange Mode: main
 - Send Initial Contact
 - NAT Traversal
- My ID User FQDN: (empty field)
- Proposal Check: obey
- Hash Algorithm: md5
- Encryption Algorithm: 3des
- DH Group: modp1024
- Generate Policy

R1

R2

Setting IPSec(2)

- IP Sec diseting berpasangan pada router yang telah sukses di-tunnel
- Setting pada IP>IPSec>>Policy>peer

The image shows two identical configuration dialogs for an IPsec peer. Both dialogs have a blue header bar with the title 'IPsec Peer <0.0.0.0/0>' and standard window controls (minimize, maximize, close). The configuration fields are as follows:

- Address:** 0.0.0.0/0
- Port:** 500
- Auth. Method:** pre shared key
- Secret:** 123
- Exchange Mode:** main
 - Send Initial Contact
 - NAT Traversal
- My ID User FQDN:** (empty field)
- Proposal Check:** obey
- Hash Algorithm:** md5
- Encryption Algorithm:** 3des
- DH Group:** modp1024
- Generate Policy

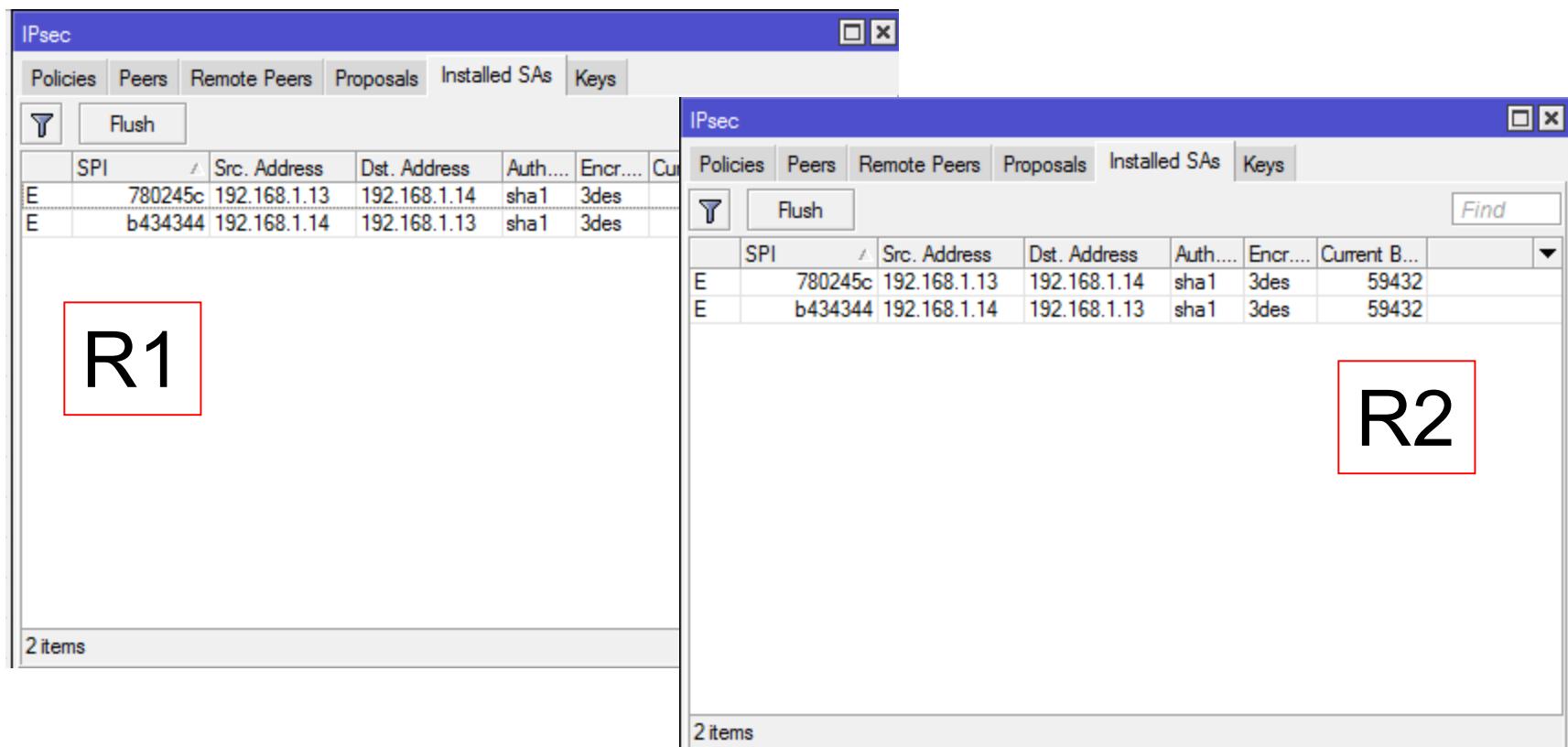
Both dialogs have 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove' buttons in the top right corner.

R1

R2

Setting IPSec(3)

- Apabila telah terjalin koneksi antar router menggunakan IP Sec, maka Security Association (SA) dapat dilihat pada masing masing router di menu IP>IPSec>Installed SAs

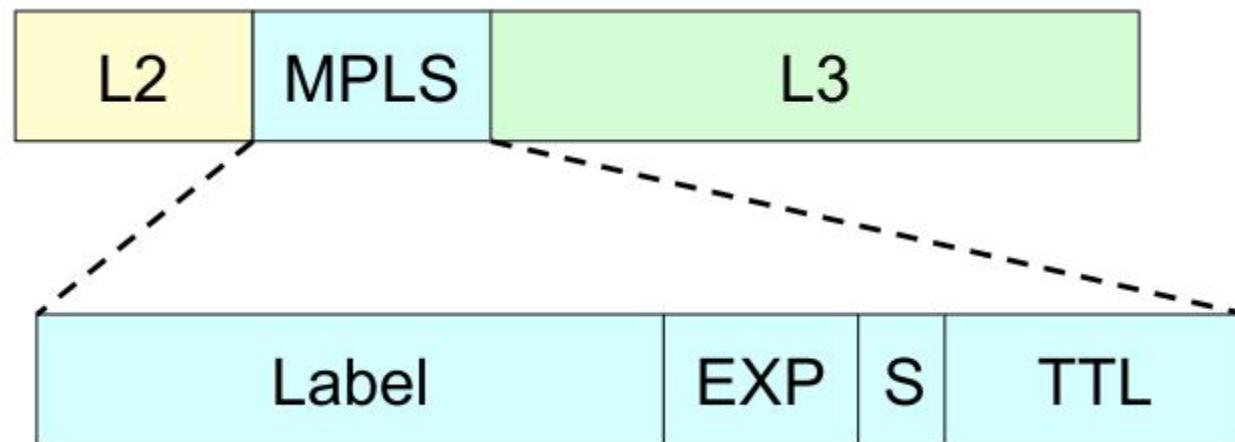


MPLS

- Multiprotocol Label Switching (MPLS) menggantikan IP routing - packet forwarding decision (outgoing interface dan nexthop router) tidak lagi berdasarkan field dalam header IP (dst address) dan tabel routing, tetapi pada label yang melekat pada paket. (seperti layaknya switch)
- MPLS tidak memerlukan packet header dan routing table. Dikenal juga sebagai layer 2,5 (karena terletak antara OSI layer 2 dan layer 3)
- Header dapat mengandung satu atau beberapa shims yang masing2 berukuran 32bit: Label (20bits), EXP (3bits) class of services, End of stack flag (1bit), TTL (8bits)

MPLS

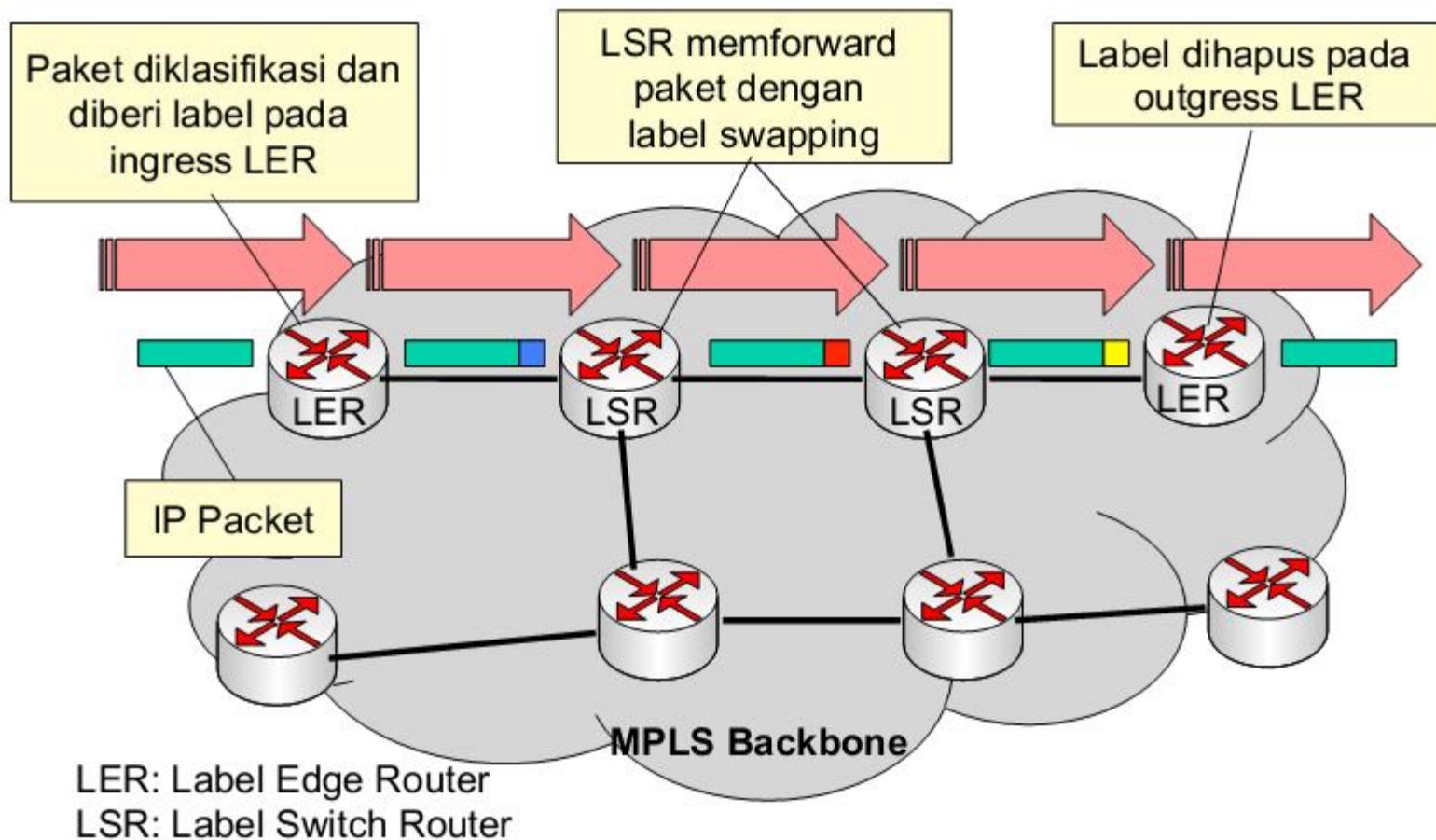
- OSI Layer 2,5



MPLS - LDP

- Label dibuat dan didistribusikan oleh Label Distribution Protocol (LDP)
- Syarat LDP:
 - Konektifitas IP, semua host harus terkoneksi dengan baik (static, OSPF, RIP)
 - Apabila memakai Loopback address / bridge tidak boleh dipasang pada interface fisik
 - Semua perangkat yang dilalui harus mendukung protokol MPLS

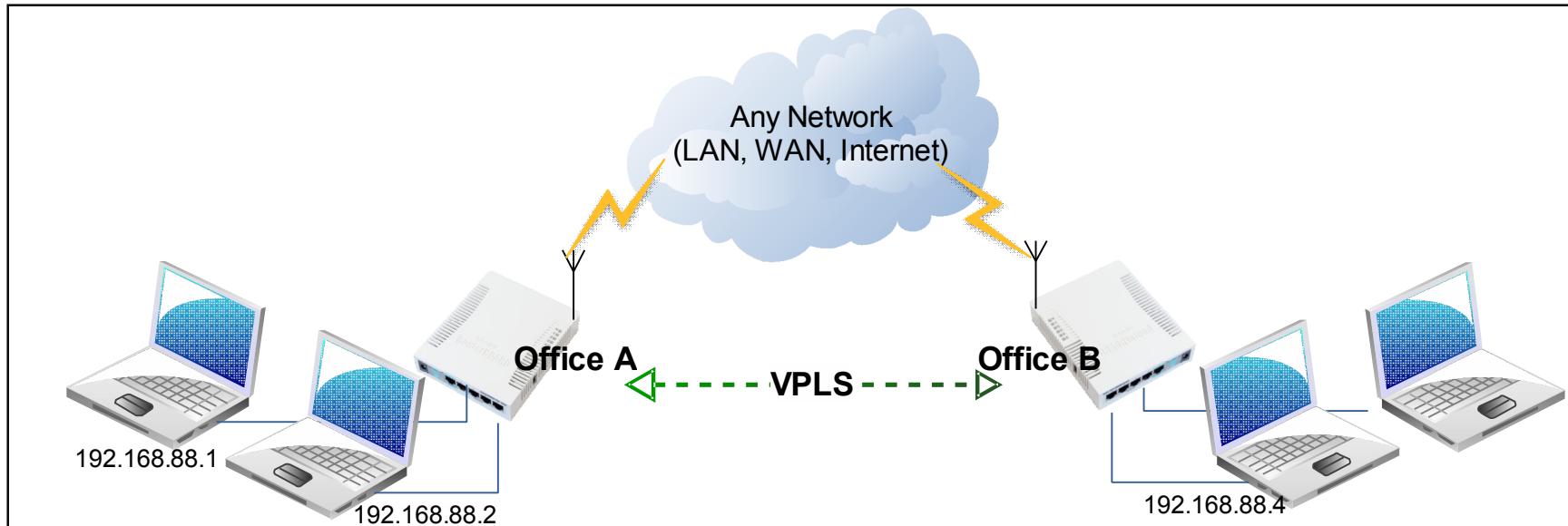
MPLS - LDP



VPLS-MPLS

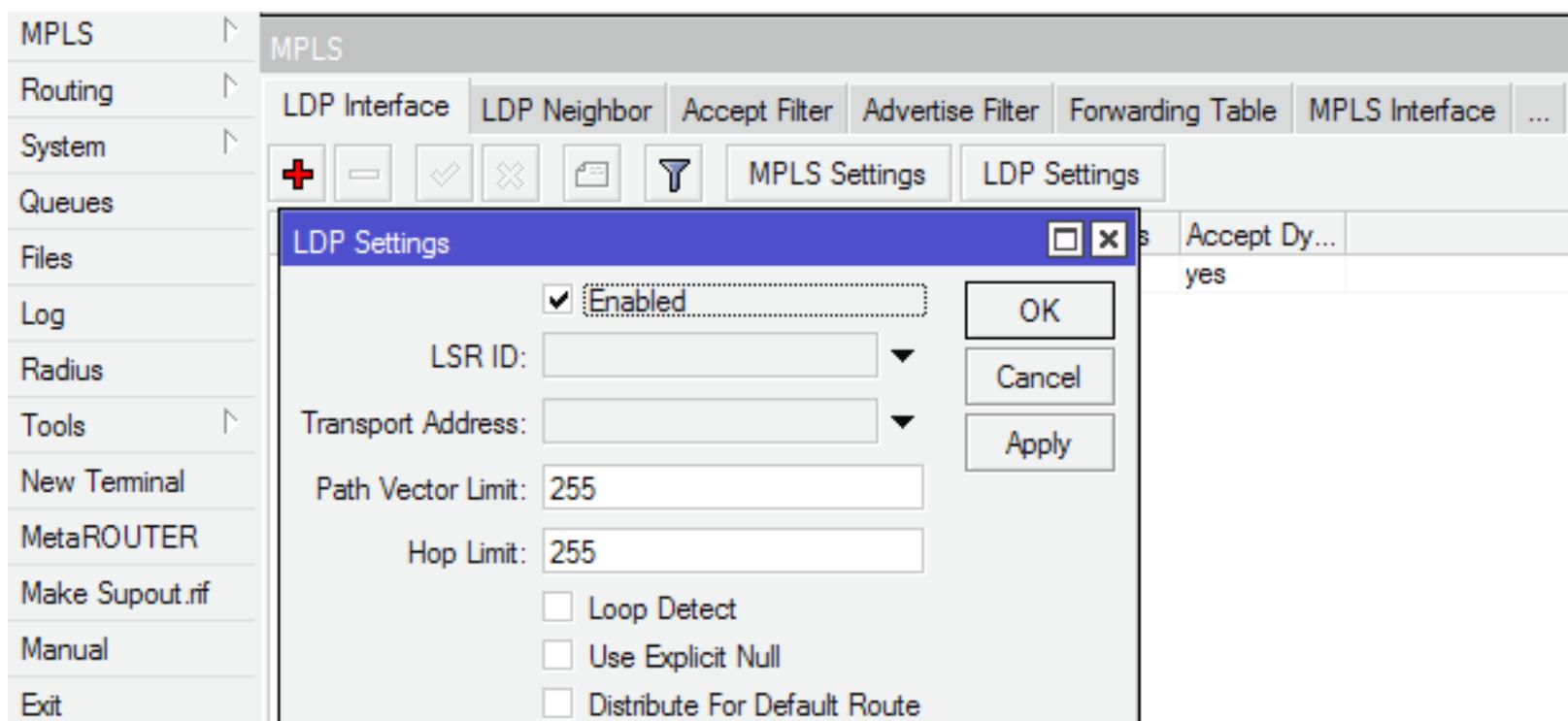
- Virtual Private Lan Layanan (VPLS), adalah tunneling seperti halnya EoIP
- VPLS 60% lebih cepat daripada EOIP dan Resource yang digunakan lebih kecil daripada EOIP
- Negosiasi dari VPLS tunnel dilakukan dengan LDP protokol - kedua endpoint dari VPLS tunnel bertukar label yang ingin digunakan untuk koneksi tunnel.
- Forwarding data dalam tunnel dilakukan dengan menerapkan 2 label pada paket: tunnel label dan transport label - label yang menjamin pengiriman traffic diantara endpoint

LAB-VPLS-MPLS



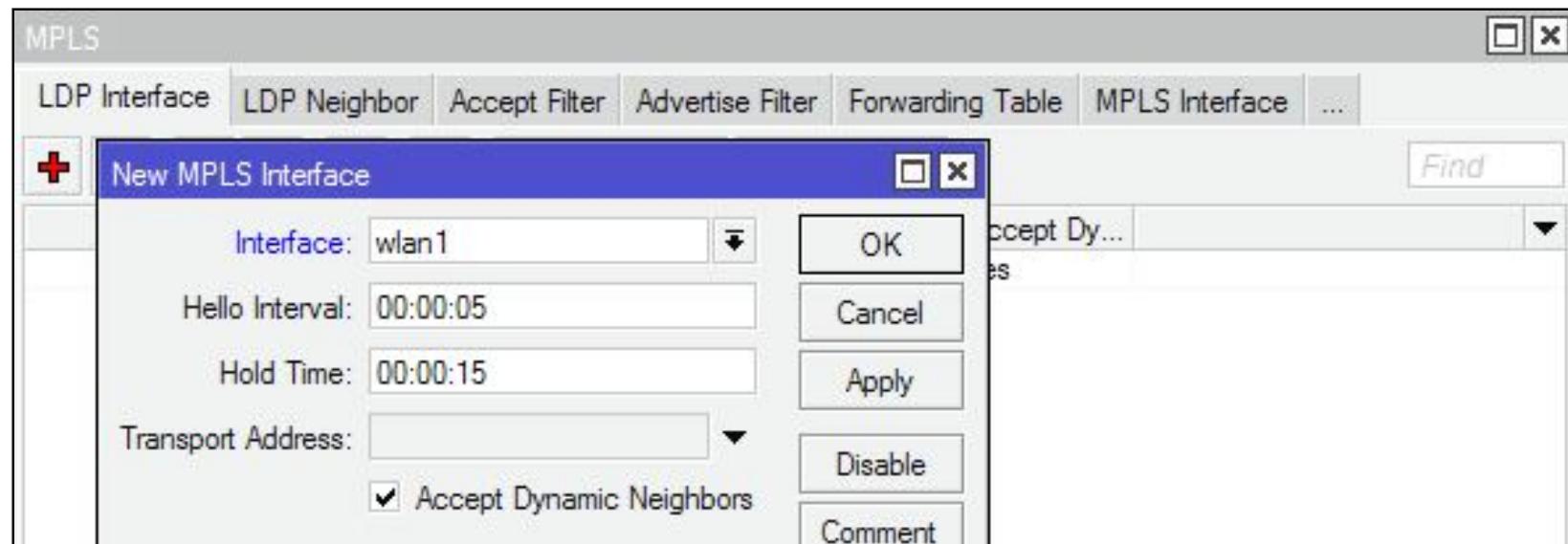
LAB – VPLS-MPLS

- Enable LDP (Label Distribution Protocols) pada menu MPLS>MPLS>LDP Interface>LDP Setting.



LAB – VPLS-MPLS

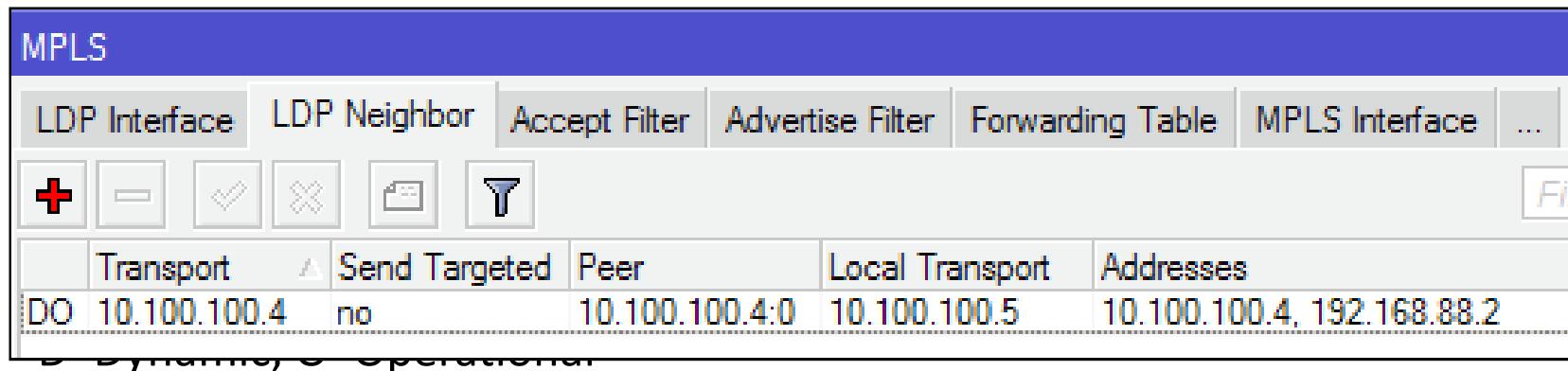
- Add new MPLS interface pada menu pada menu MPLS>MPLS>LDP Interface>klik tanda +, dan definisikan interface yang akan digunakan untuk koneksi VPLS,



- Transport Address boleh dikosongin atau dengan IP address interface MPLS.

LAB – VPLS-MPLS

- Cek status koneksi LDP pada menu MPLS>MPLS>LDP Neighbor

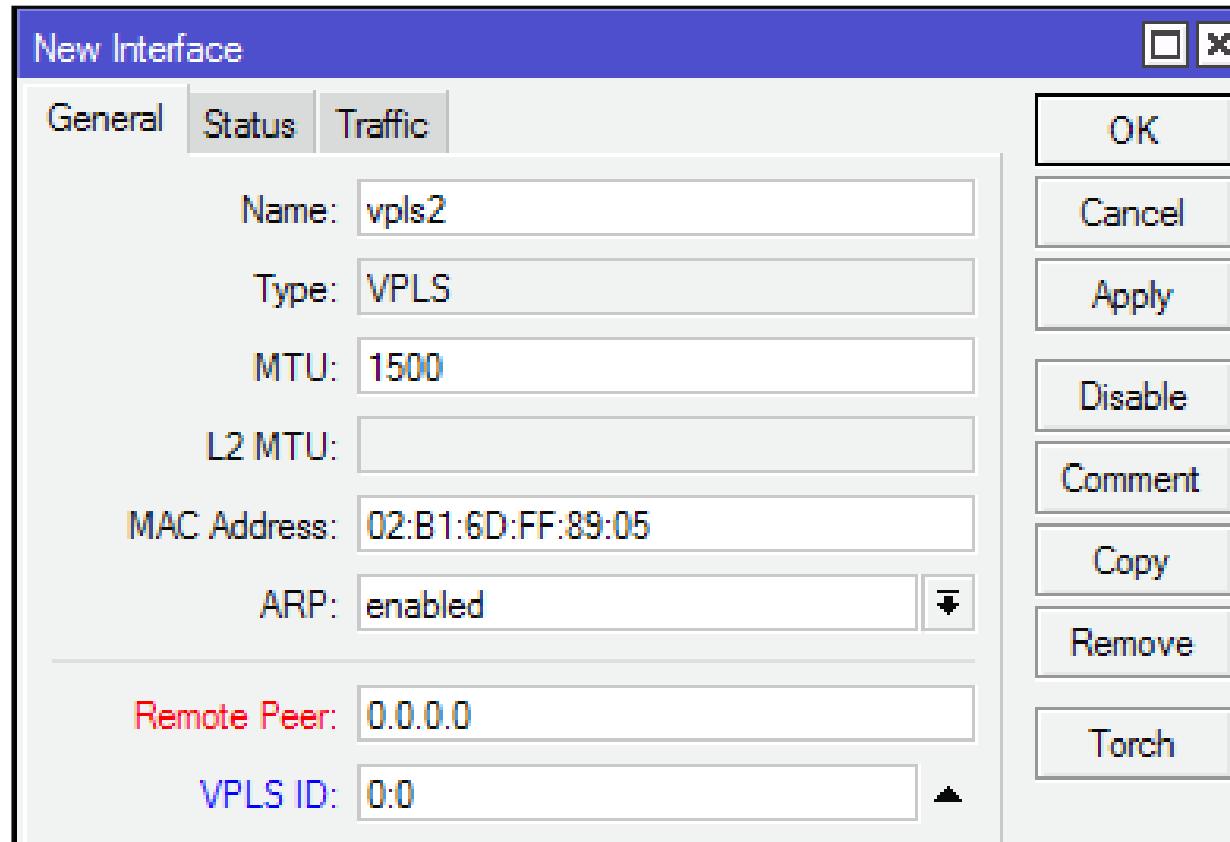


The screenshot shows the Cisco IOS XE CLI interface for managing LDP neighbors. The title bar says "MPLS". Below it is a navigation bar with tabs: LDP Interface, LDP Neighbor (which is selected), Accept Filter, Advertise Filter, Forwarding Table, MPLS Interface, and a "...". Underneath the tabs are several icons: a red plus sign, a minus sign, a checkmark, a crossed-out symbol, a document icon, and a filter icon. To the right of the filter icon is a search bar with the letter "F". The main area is a table with the following columns: Transport, Send Targeted, Peer, Local Transport, and Addresses. A single row is shown with the following values: DO, 10.100.100.4, no, 10.100.100.4:0, 10.100.100.5, and 10.100.100.4, 192.168.88.2.

	Transport	Send Targeted	Peer	Local Transport	Addresses
DO	10.100.100.4	no	10.100.100.4:0	10.100.100.5	10.100.100.4, 192.168.88.2

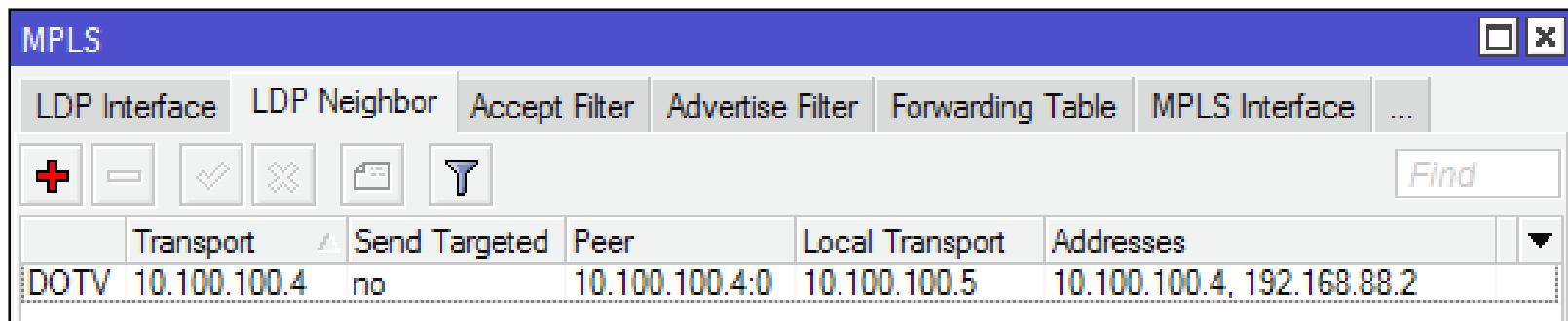
LAB – VPLS-MPLS

- Add New VPLS Interface pada menu Interface, Remote Peer = <IP address remote>
- VPLS ID = <harus sama dengan VPLS ID remotenya>



LAB – VPLS-MPLS

- Cek kembali status konektifitas LDP dan VPLS pada menu MPLS>MPLS>LDP Neighbor



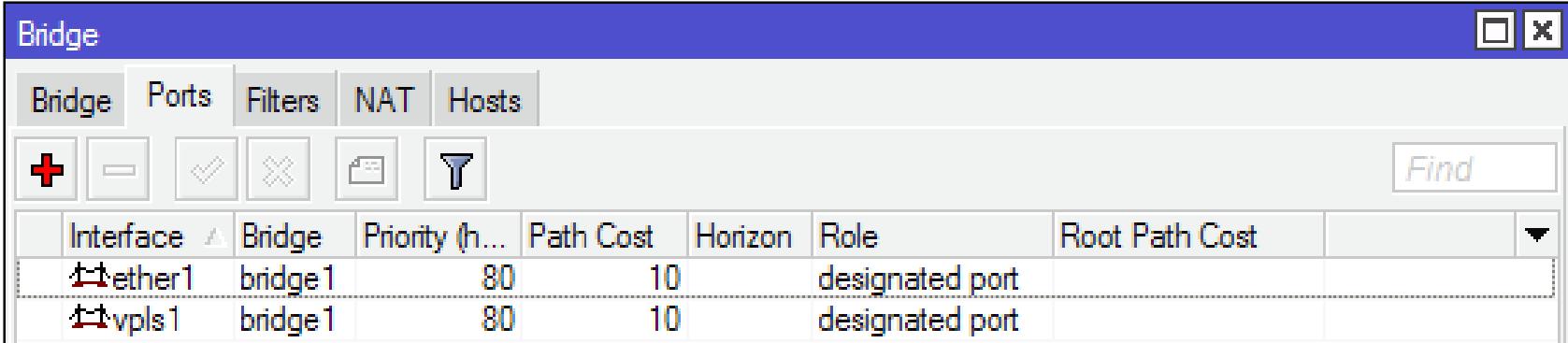
The screenshot shows the Cisco IOS CLI interface with the title bar "MPLS". Below it is a tab bar with "LDP Interface", "LDP Neighbor" (which is selected and highlighted in orange), "Accept Filter", "Advertise Filter", "Forwarding Table", "MPLS Interface", and "...". Below the tabs are several icons: a red plus sign (+), a minus sign (-), a checkmark, a crossed-out symbol, a file icon, and a filter icon. To the right of these icons is a "Find" button. The main area is a table titled "LDP Neighbor". The columns are: Transport, Send Targeted, Peer, Local Transport, and Addresses. A dropdown arrow is positioned above the "Transport" column. The first row of the table contains the values: DOTV, 10.100.100.4, no, 10.100.100.4:0, 10.100.100.5, and 10.100.100.4, 192.168.88.2.

Transport	Send Targeted	Peer	Local Transport	Addresses
DOTV	10.100.100.4	no	10.100.100.4:0	10.100.100.5

- D=Dynamic, O=Operational, T = Transport, V=VPLS Active

LAB – VPLS-MPLS

- Buatlah interface bridge, dan tambahkan interface vpls dan ether1 dalam port



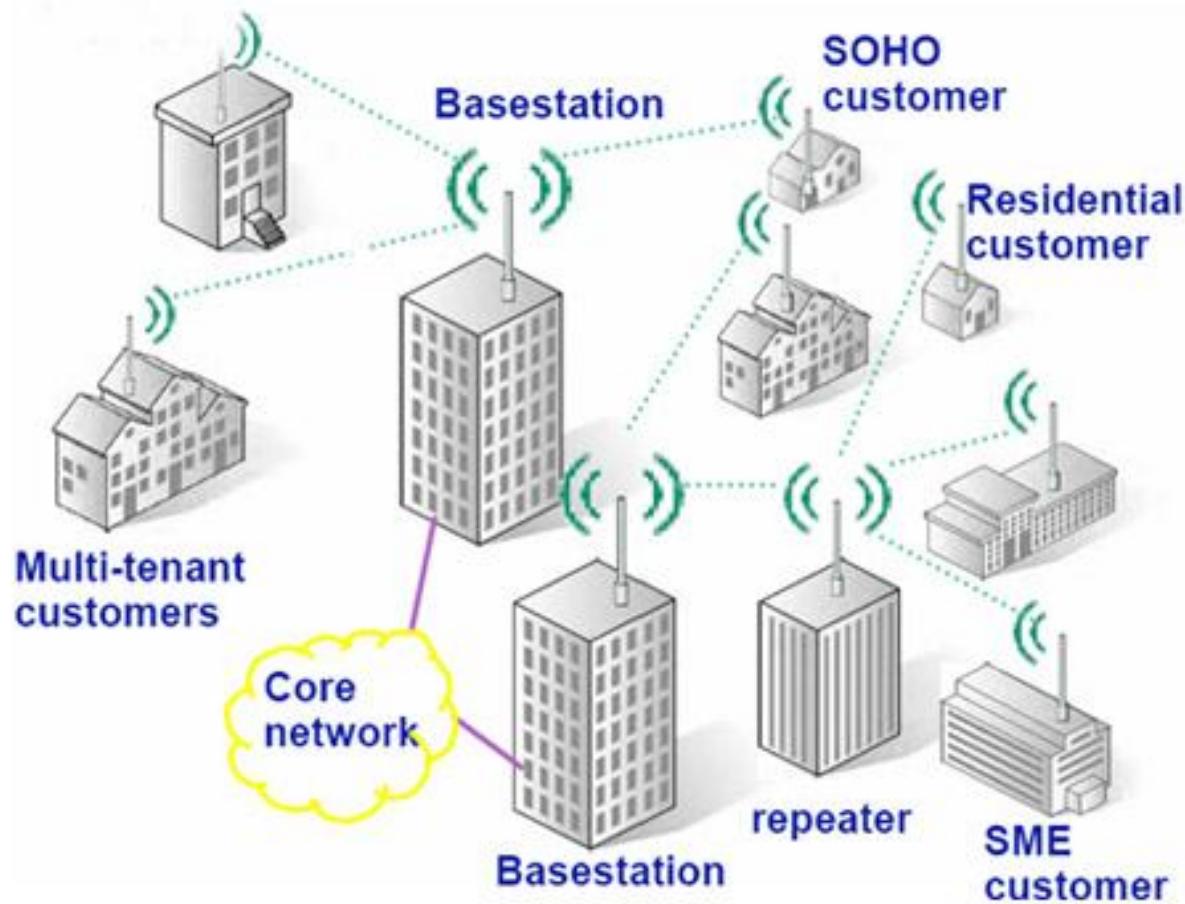
Interface	Bridge	Priority (h...)	Path Cost	Horizon	Role	Root Path Cost	▼
ether1	bridge1	80	10		designated port		
vpls1	bridge1	80	10		designated port		

- Cek dengan ping antar client

MME Wireless Protocol (introduction)

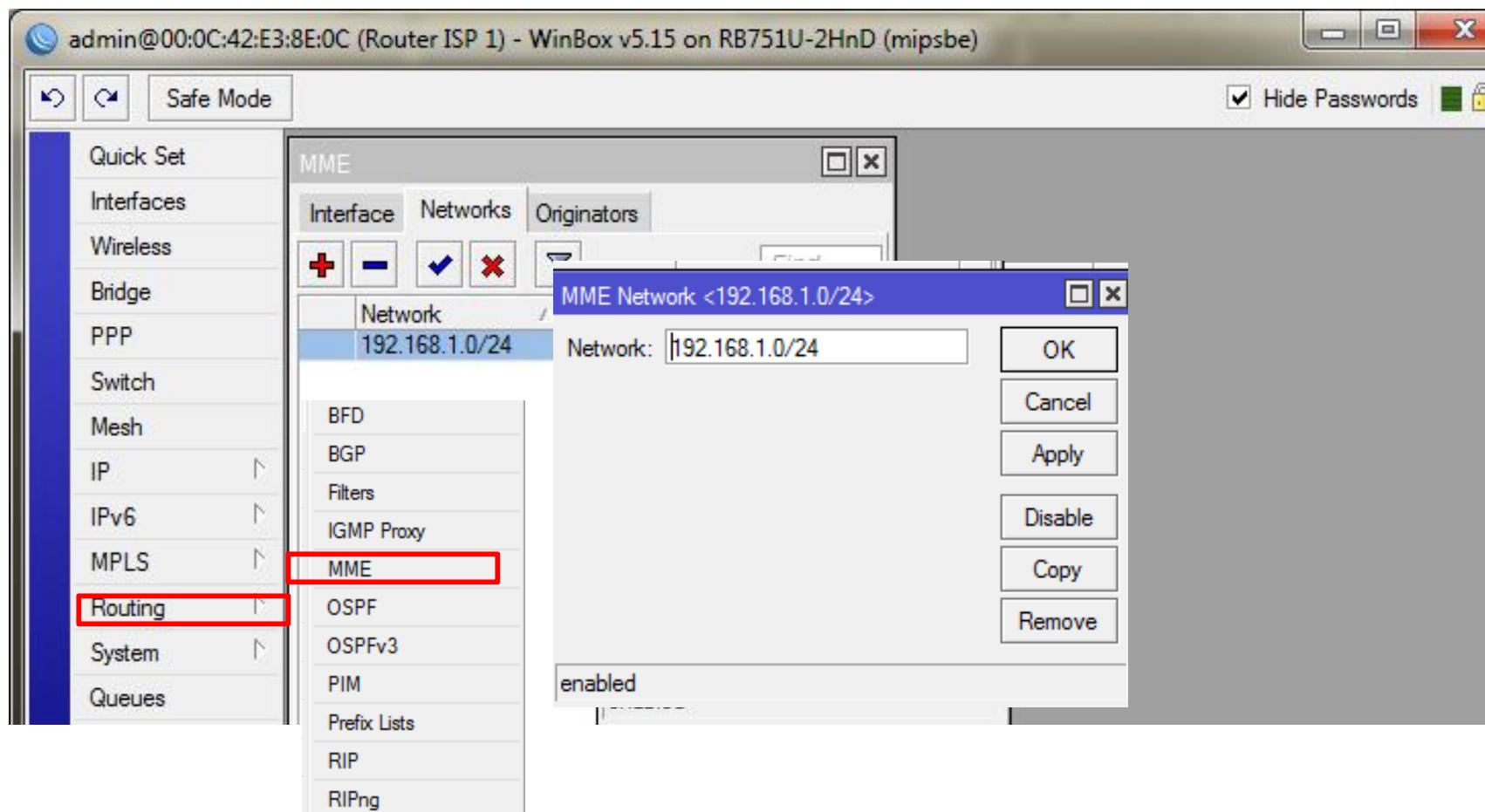
- MME (Mesh Made Easy) adalah protokol routing yang hanya dimiliki oleh MikroTik.
- MME didesain untuk routing dalam jaringan wireless mesh.
- Hal ini didasarkan pada ide dari BATMAN (Better Approach To Mobile Ad-hoc Networking) protokol routing.
- MME digunakan sebagai alternatif OSPF running under wireless network.

MME Routing



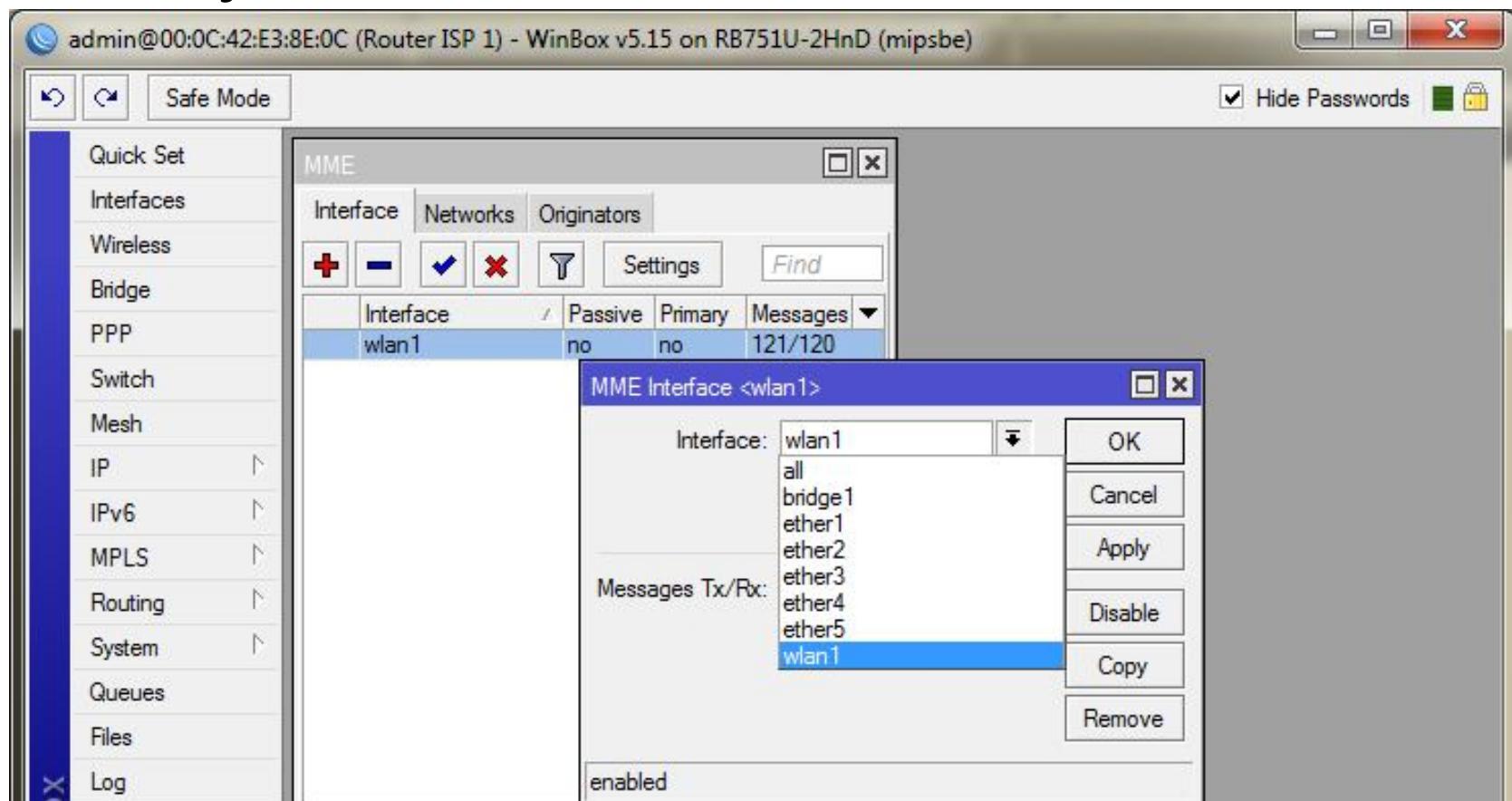
Setting MME

- Add network to MME



Setting MME

- Menjalankan MME ke interface wlan



Setting MME

- Check MME aktif routing di IP>routes

Route List					
Routes		Nexthops	Rules	VRF	
	Dst. Address	Gateway	Distance	Pref. Source	
DAS	► 0.0.0.0/0	192.168.1.1 reachable wlan1	0		
DAC	► 12.12.12.0/24	bridge1 reachable	0	12.12.12.10	
DAC	► 192.168.1.0/24	wlan1 reachable	0	192.168.1.13	
Dm	► 192.168.1.0/24	192.168.1.14 reachable wlan1	130		
DAm	► 192.168.1.14	192.168.1.14 reachable wlan1	130		