



Advanced Mikrotik Training Routing (MTCRE)



Certified Mikrotik Training - Advanced Class (MTCRE)
Organized by: Citraweb Nusa Infomedia
(Mikrotik Certified Training Partner)



Jadwal Training

	Sessi 1 08.30-10.00	Sessi 2 10.30-12.00	Sessi 3 13.00-15.00	Sessi 4 15.30-17.00
Hari 1	Static Route			IP Tunnel
Hari 2			OSPF	
Hari 3	BGP Basic	MPLS Basic		Load Balanced
Hari 4		Lab		Test



New Training Scheme 2010

- **Basic/Essential Training**
 - MikroTik Certified Network Associate (MTCNA)
- **Advanced Training**
 - Certified Wireless Engineer (MTCWE)
 - Certified Routing Engineer (MTCRE)
 - Certified Traffic Control Engineer (MTCTCE)
 - Certified User Managing Engineer (MTCUME)
 - Certified Inter Networking Engineer (MTCINE)

Certification Test

- Diadakan oleh **Mikrotik.com** secara online
- Dilakukan pada sessi terakhir
- Jumlah soal : **25**
- Nilai minimal kelulusan : **60%**
- Yang mendapatkan nilai **50%** hingga **59%** berkesempatan mengambil “**second chance**”
- Yang lulus akan mendapatkan sertifikat yang diakui secara internasional





Trainers

- **Valens Riyadi**
 - MTCNA (2004), Certified Consultant (2005)
 - Certified Trainer (2006), MTCTCE (2009)
 - MTCUME (2009), MTCINE (2010)
- **Novan Chris**
 - MTCNA (2006), Certified Trainer (2008)
 - MTCWE (2008 & 2010), MTCRE (2008)
 - MTCTCE (2011)
- **Pujo Dewobroto**
 - MTCNA (2009), MTCTCE (2009)
 - MTCWE (2010), Certified Trainer (2011)



Perkenalan

- Perkenalkanlah :
 - **Nama Anda :**
 - **Tempat Bekerja :**
 - **Kota / Domisili :**
 - Apa yang Anda kerjakan sehari-hari dan fitur-fitur apa yang ada di Mikrotik yang sudah Anda gunakan.
 - Motivasi mengikuti training.



Static Route & Policy Route



Certified Mikrotik Training Advanced Class (MTCRE)

Organized by: Citraweb Nusa Infomedia

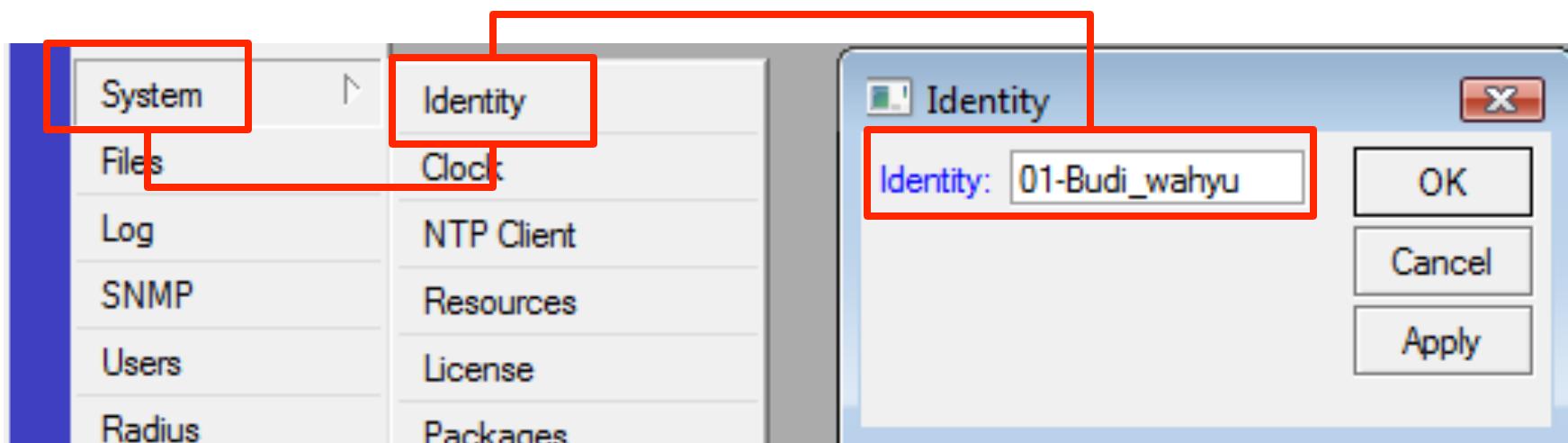
(Mikrotik Certified Training Partner)

Lakukanlah terlebih dahulu!

- Ubahlah nama Router **System Identity** menjadi :
“XX-NAMA ANDA”
- Aktifkan neighbor interface pada WLAN1
- Buatlah username baru dan berilah password (group full)
- Proteksilah user Admin (tanpa password) hanya bisa diakses dari 10.10.10.30/31 (grup full)
- Buatlah user “demo” dengan grup read

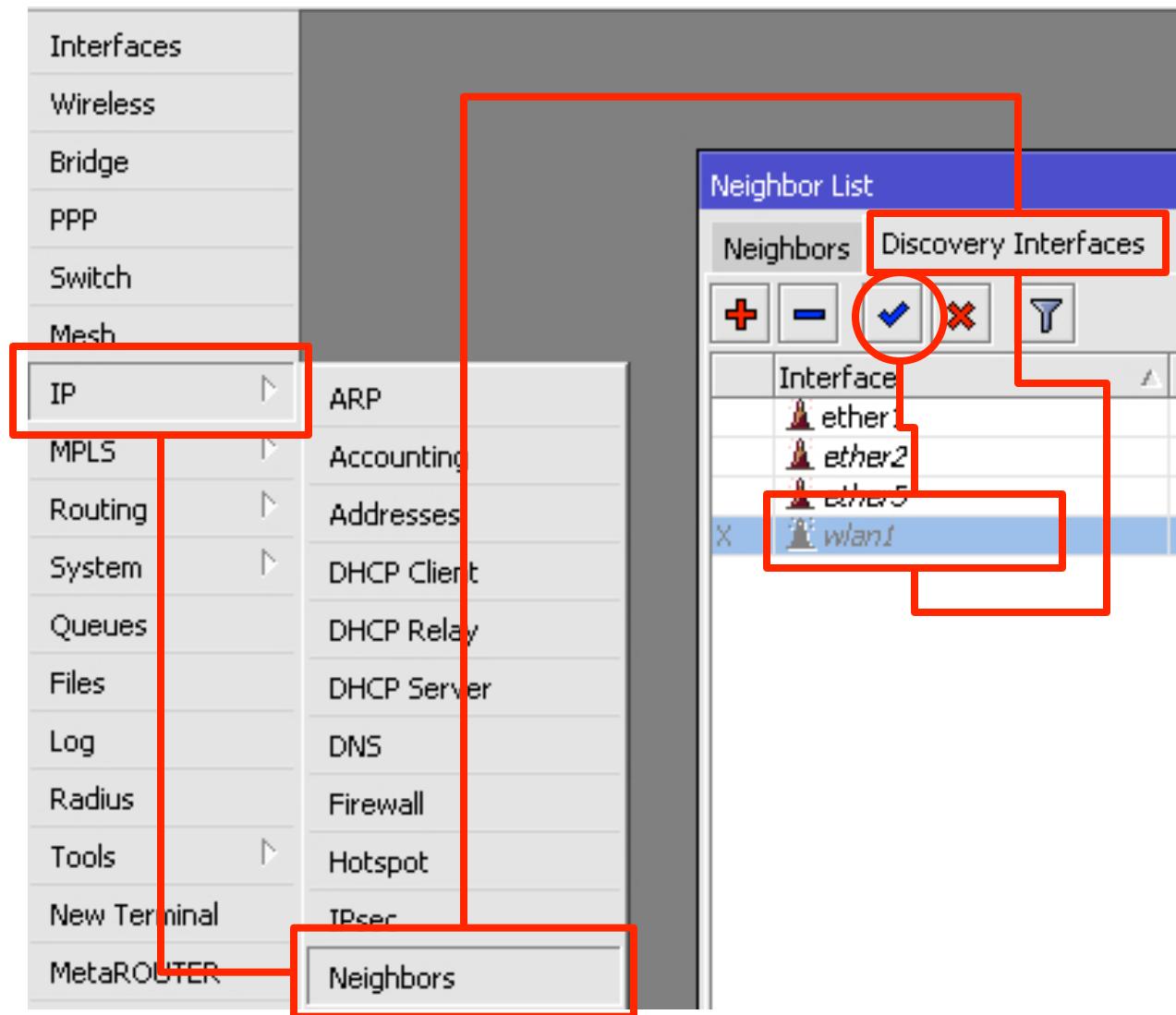
[LAB-1] System Identity

- Supaya tidak membingungkan, ubahlah nama router Anda.
- Format: **xx-NamaAnda**
- Contoh: 01-Budi-Wahyu
- Aktifkan semua interface



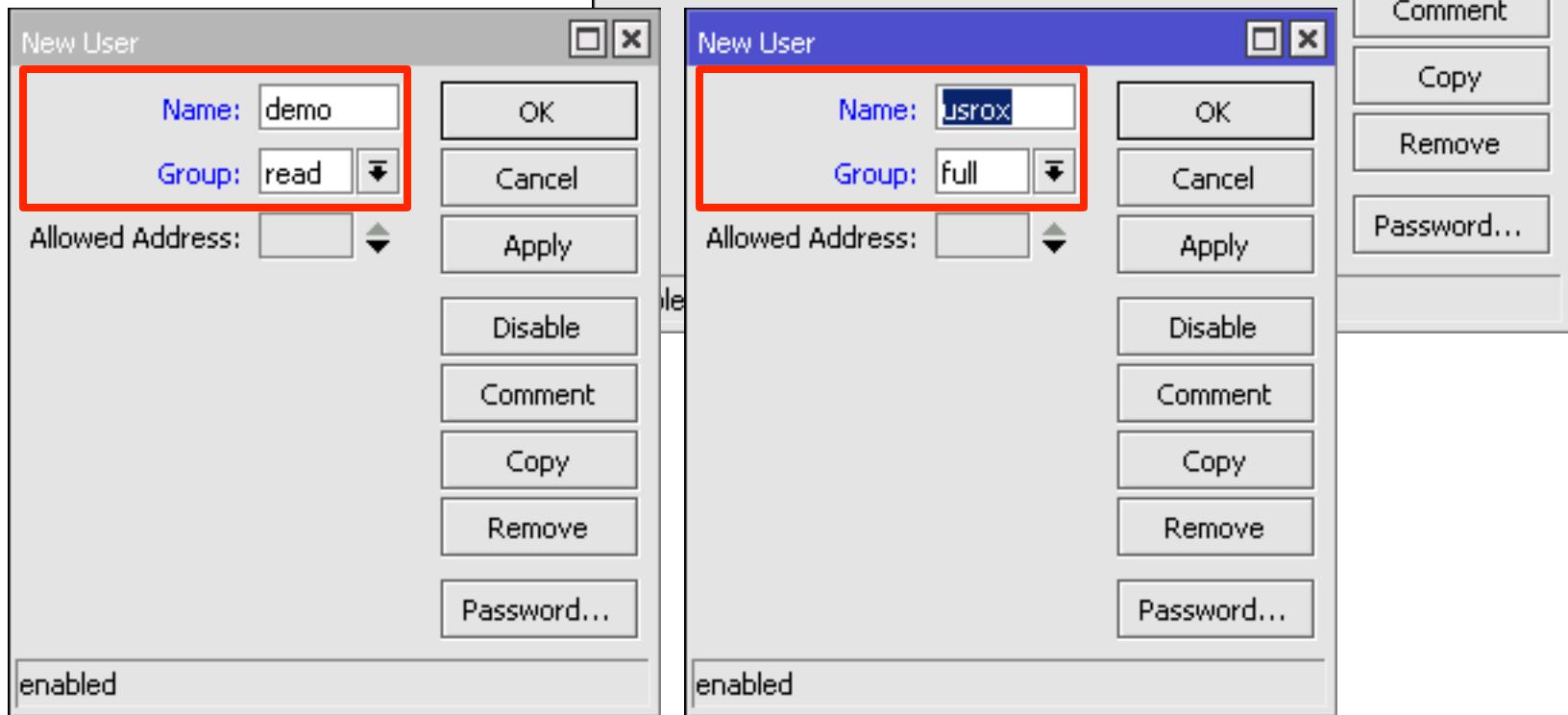
[LAB-2] Activate Neighbour Protocol

- Aktifkan Neighbour Protocol pada wlan1

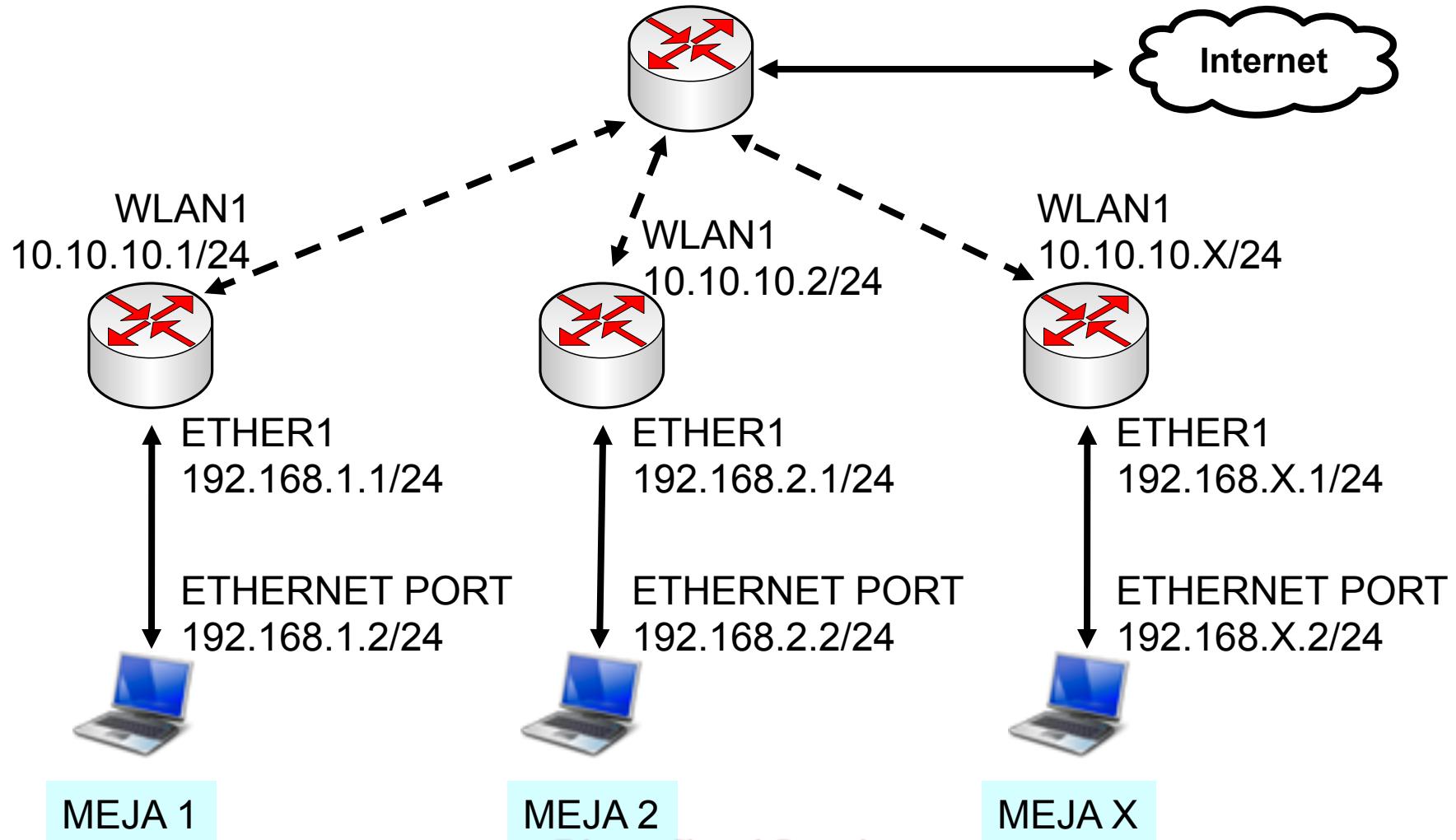


[LAB-3] User Configuration

- Persiapkan User di system mikrotik supaya siap di semua kegiatan training.



[LAB-4] Konfigurasi Dasar



Telegram Channel @nettrain



IP Configuration

- Routerboard Setting
 - WAN IP : 10.10.10.x/24
 - Gateway : 10.10.10.100
 - LAN IP : 192.168.x.1/24
 - DNS : 10.100.100.1
 - Services: Src-NAT and DNS Server
- Laptop Setting
 - IP Address : 192.168.x.2/24
 - Gateway : 192.168.x.1
 - DNS : 192.168.x.1



Configuration

- NTP Server: “id.pool.ntp.org”/ “ntp.nasa.gov”
- Wlan1 SSID : training (WPA=.....)
- Buatlah file backup! Dan simpan juga file tersebut ke laptop



Routed Network

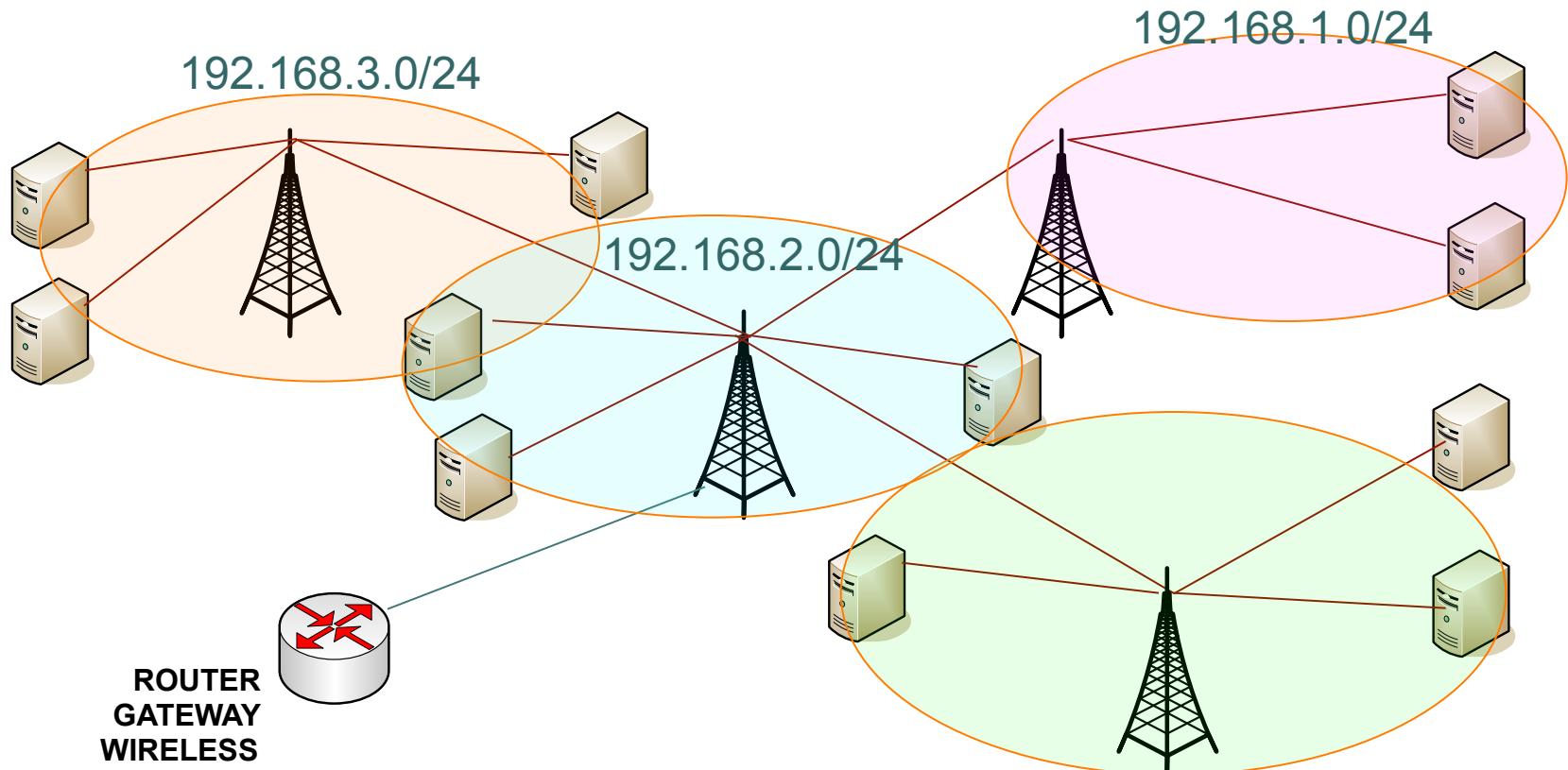
- Pengaturan jalur antar network segment berdasarkan IP Address tujuan (atau juga asal), pada OSI layer **Network**.
- Tiap network segment biasanya memiliki subnet network (IP Address) yang berbeda-beda.



Routing!

- Memungkinkan kita melakukan pemantauan dan pengelolaan jaringan yang lebih baik
- Lebih aman (firewall filtering lebih mudah dan lengkap)
- Trafik broadcast hanya terkonsentrasi di setiap subnet
- Dibutuhkan perangkat wireless yang mampu melakukan full routing, atau menambahkan router di BTS.
- Untuk skala besar, bisa digunakan Dynamic Routing (RIP/OSPF/BGP)

Routing



setiap segment jaringan memiliki subnet IP address yang berbeda.

192.168.0.0/24



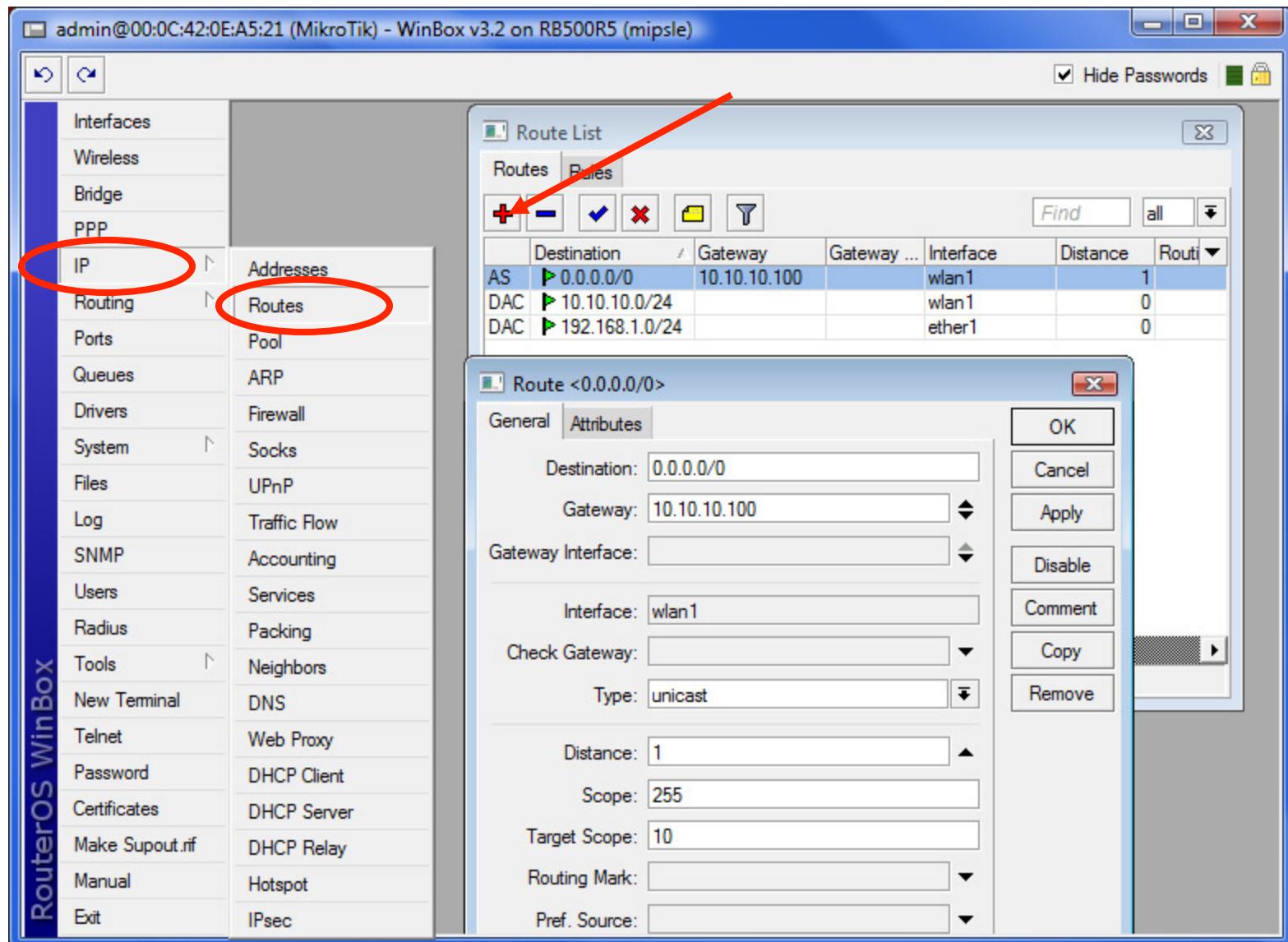
Static Route

- Routing bertujuan untuk melakukan pengaturan arah paket data yang melalui router, dengan menentukan gateway untuk dst-address tertentu
- Gateway bisa berupa :
 - IP Address
 - Interface
- Dst-address 0.0.0.0/0 disebut sebagai default gateway karena ip 0.0.0.0/0 menggantikan semua ip yang ada di internet.

Tipe Informasi Routing

- MikroTik RouterOS tipe routing sbb:
 - **dynamic routes**
yang akan dibuat secara otomatis:
 - saat menambahkan IP Address pada interface
 - informasi routing yang didapat dari protokol routing dinamik seperti RIP, OSPF, dan BGP.
 - **static routes**
adalah informasi routing yang dibuat secara manual oleh user untuk mengatur ke arah mana trafik tertentu akan disalurkan. Default route adalah salah satu contoh static routes.

Menambahkan Routing



Telegram Channel @nettrain

Tipe Routing

A: Active
S: Static

A: Active
D: Dynamic
C: Connected

	Destination	Gateway	Interface	Distance	Routing Mark	Pref. Source
AS	► 0.0.0.0/0	10.10.10.100	wlan1	1		
DAC	► 10.10.10.0/24		wlan1	0		10.10.10.1
DAC	► 192.168.1.0/24		ether1	0		192.168.1.1

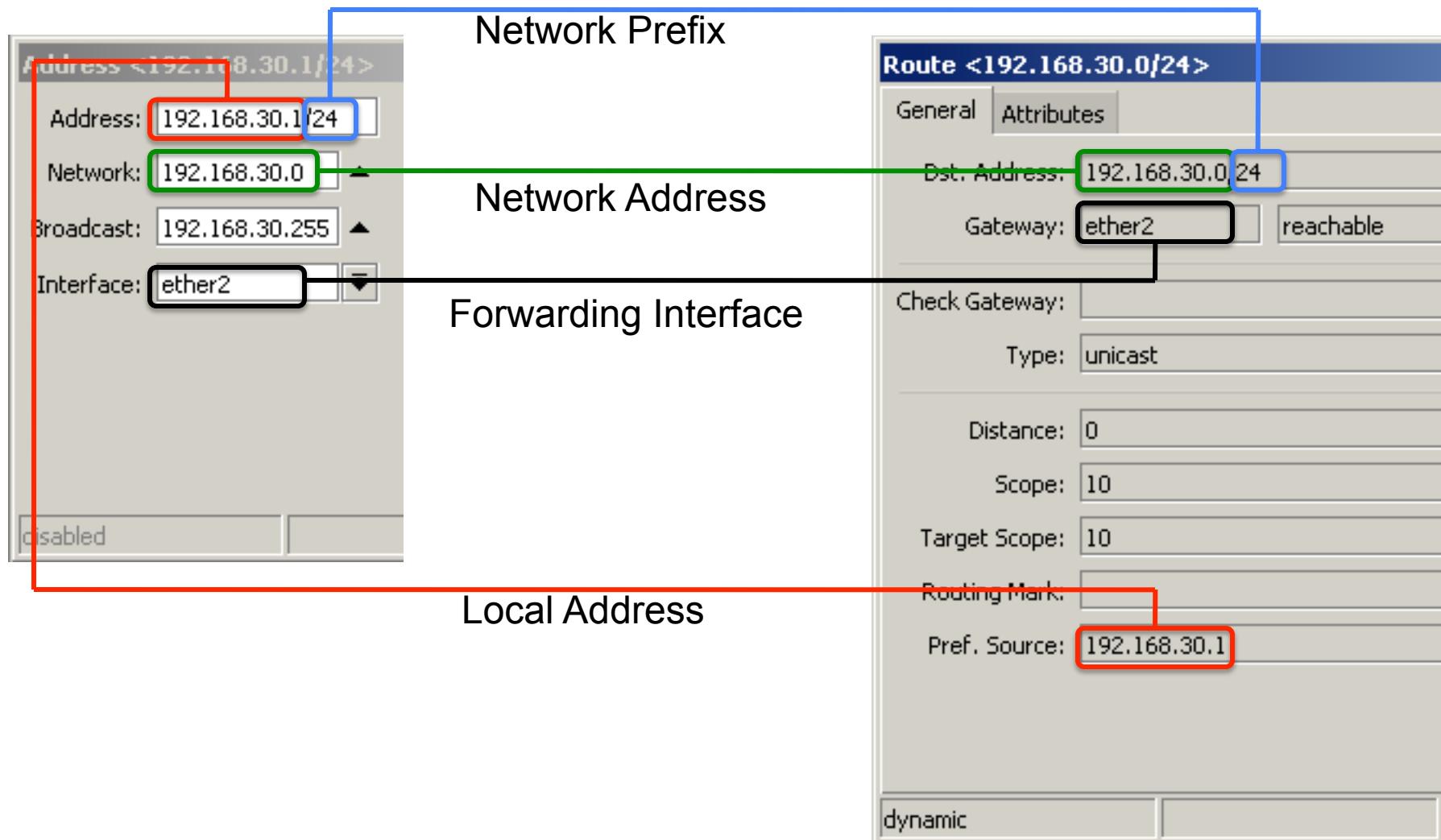
setiap IP Address yang dipasang pada interface di router secara otomatis akan menambahkan DAC Routing dengan pref-source IP Address tersebut.



Connected Routes

- 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 Routes



Static Route

Route <0.0.0.0/0>

General Attributes

Dst. Address:

Gateway: reachable wlan1

Check Gateway:

Type:

Distance:

Scope:

Target Scope:

Routing Mark:

Pref. Source:

**Contoh Implementasi Static Route,
yaitu pemasangan Default Gateway
atau Default Route.**



Parameter Dasar Routing

- **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
 - Gateway Interface, digunakan apabila IP gateway tidak diketahui dan bersifat dinamik.
- **Pref Source**
 - source IP address dari paket yang akan meninggalkan router, Biasanya adalah ip address yang terpasang di interface yang menjadi gateway.
- **Distance**
 - Beban untuk kalkulasi pemilihan rule routing yang akan dijalankan router.

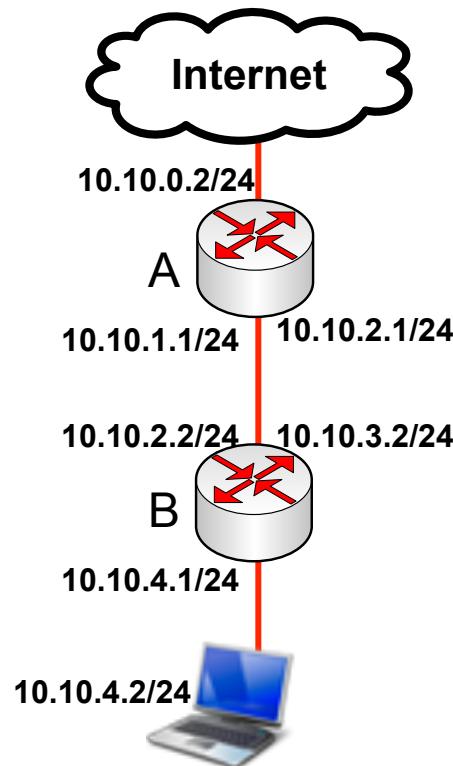
Distance

- Merupakan salah satu parameter yang digunakan untuk pemilihan rule routing, nilainya (0-255) secara default tergantung protocol routing yang digunakan:
 - **Connected routes** : 0
 - **Static Routes** : 1
 - **eBGP** : 20
 - **OSPF** : 110
 - **RIP** : 120
 - **MME** : 130
 - **iBGP** : 200

Note:
Distance=255
berarti “rejected”

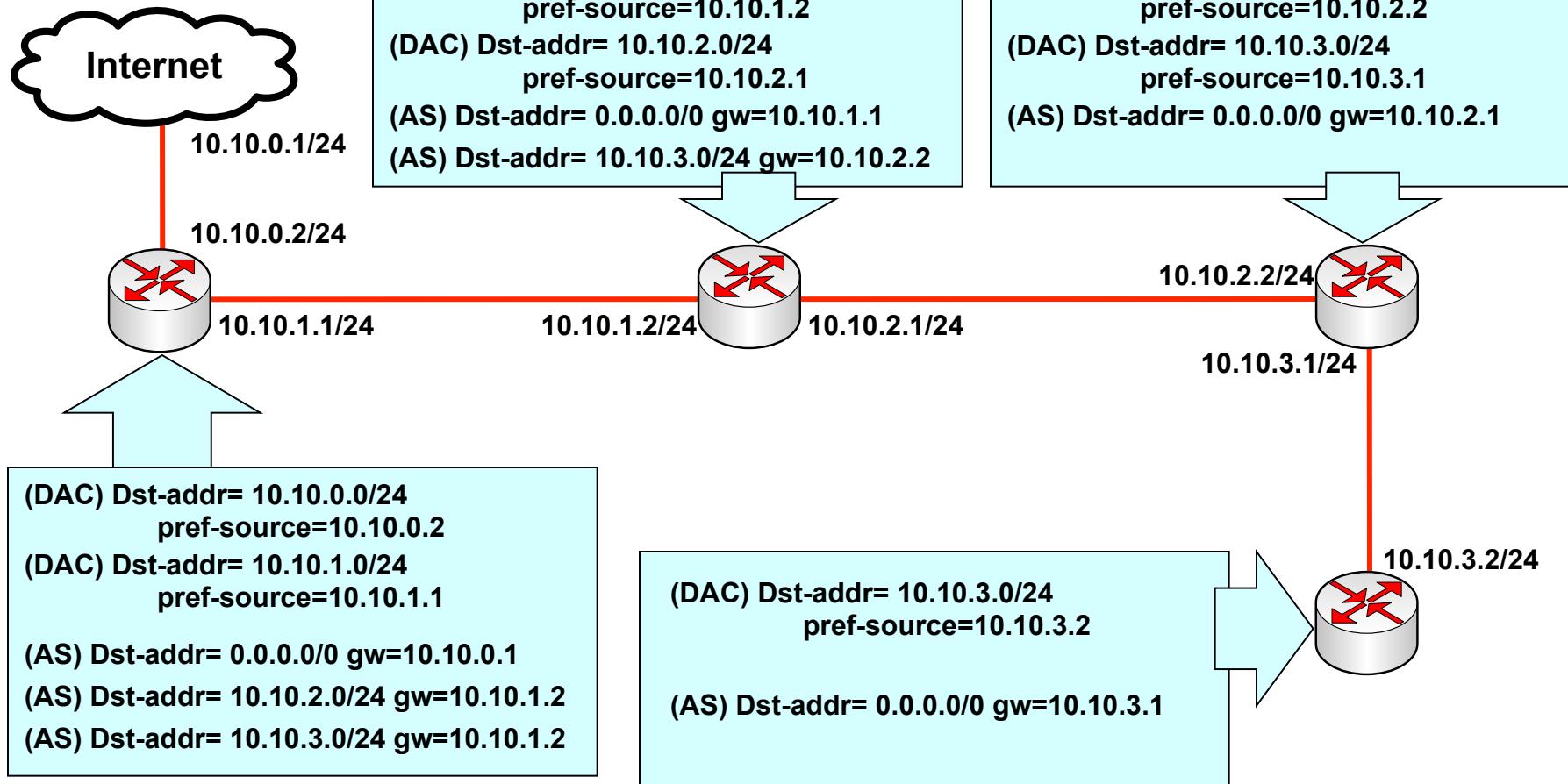
Konsep Dasar Routing

- IP Address Gateway harus merupakan IP Address yang subnetnya sama dengan salah satu IP Address yang terpasang pada router (connect directly).



- Pada interface yang menghubungkan router A dan B, pada masing-masing router terdapat lebih dari 1 buah IP Address.
- Default gateway pada router B adalah router A
- IP Address yang menjadi default gateway router B adalah 10.10.2.1, karena IP Address tersebut berada dalam subnet yang sama dengan salah satu IP Address pada router B (10.10.2.2/24)
- Setting static route default :
 - Dst-address=0.0.0.0/0 gateway=10.10.2.1

Implementasi Konsep Routing



Konsep Dasar Routing

- Untuk pemilihan routing, router akan memilih berdasarkan:
 - Rule routing yang paling spesifik tujuannya
 - Contoh: destination 192.168.0.128/26 lebih spesific dari 192.168.0.0/24
 - Distance
 - Router akan memilih yang distance nya paling kecil
 - Round robin (random)

Contoh Pemilihan

- Untuk koneksi dengan destination **192.168.0.1**, manakah urutan prioritas rule yang digunakan?

Destination	Gateway	Distance	Prioritas
192.168.0.0/27	192.168.1.1	1	2
192.168.0.0/29	192.168.2.1	1	1
192.168.0.0/24	192.168.3.1	5	4
192.168.0.0/24	192.168.4.1	1	3

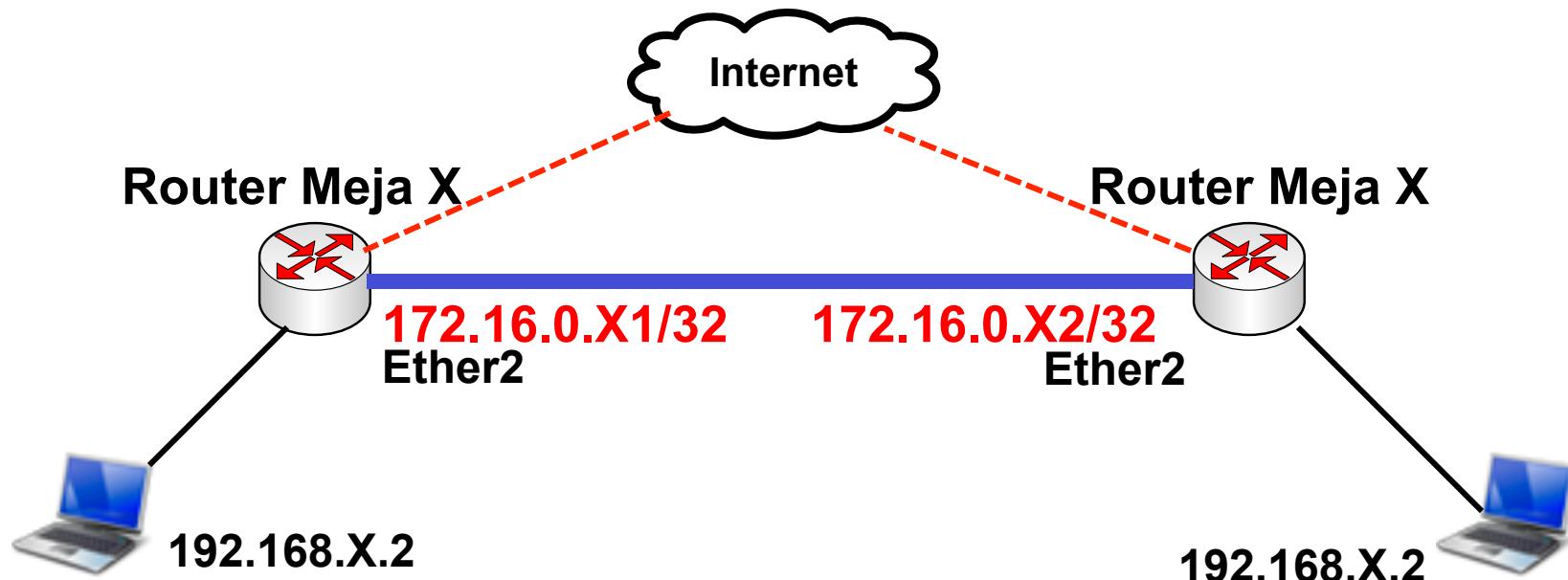
Point to Point Addressing

- Adalah sistem pengalamanan IP Address untuk **dua buah perangkat** yang **terkoneksi langsung**, menggunakan dua buah **IP Address /32**

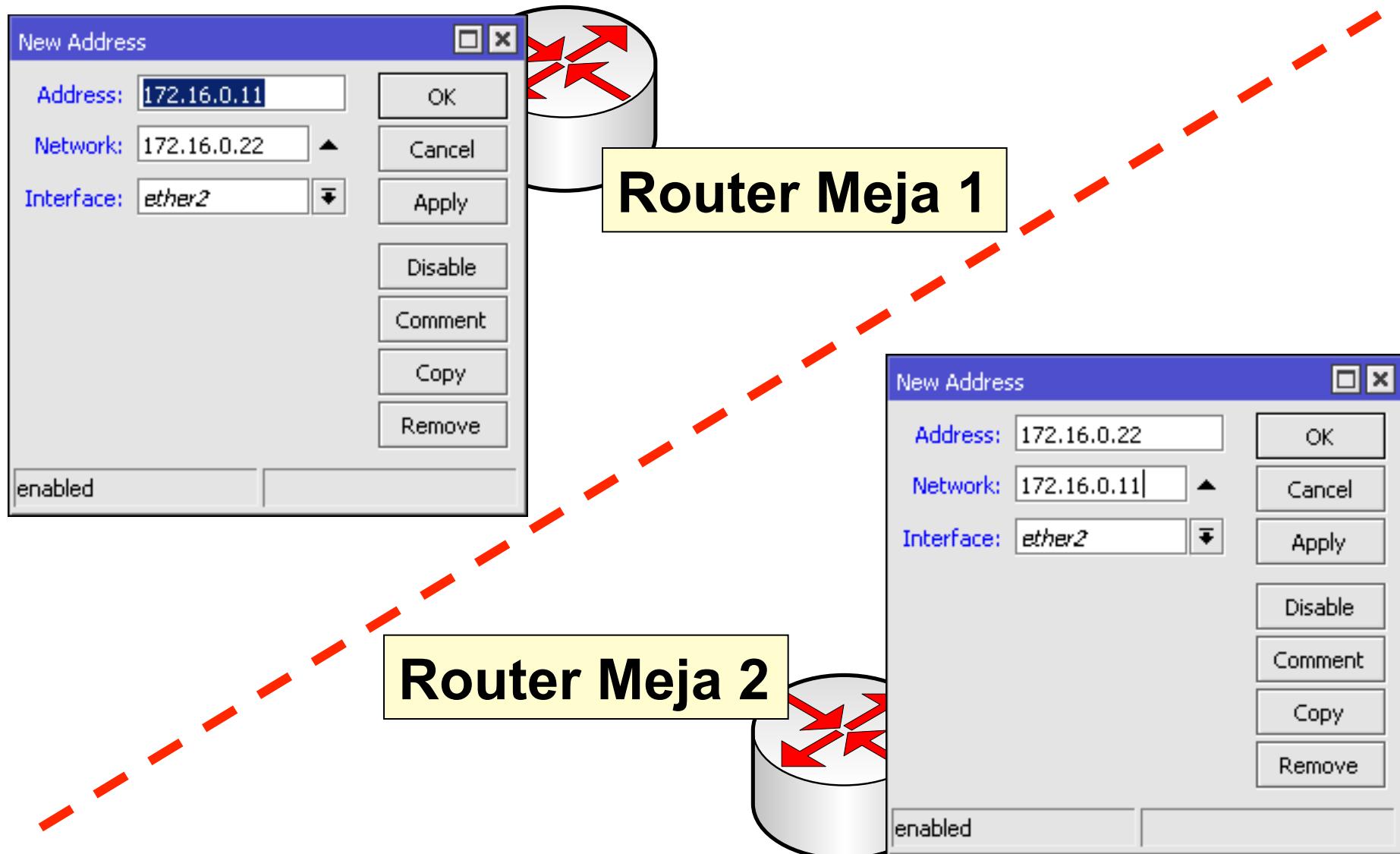
Router 1		Router 2
172.16.0.X1/32	IP Address	172.16.0.X2/32
172.16.0.X2	Network Address	172.16.0.X1
[kosongkan]	Broadcast Address	[kosongkan]
ether2	Interface	ether2

[LAB-5] P2P Addressing

- Hubungkanlah ether2 di router dengan ether2 router rekan sebangku
- Test dengan ping antar router
- Buatlah P2P Addressing dan lakukanlah static route untuk network laptop



Contoh: P2P Addressing

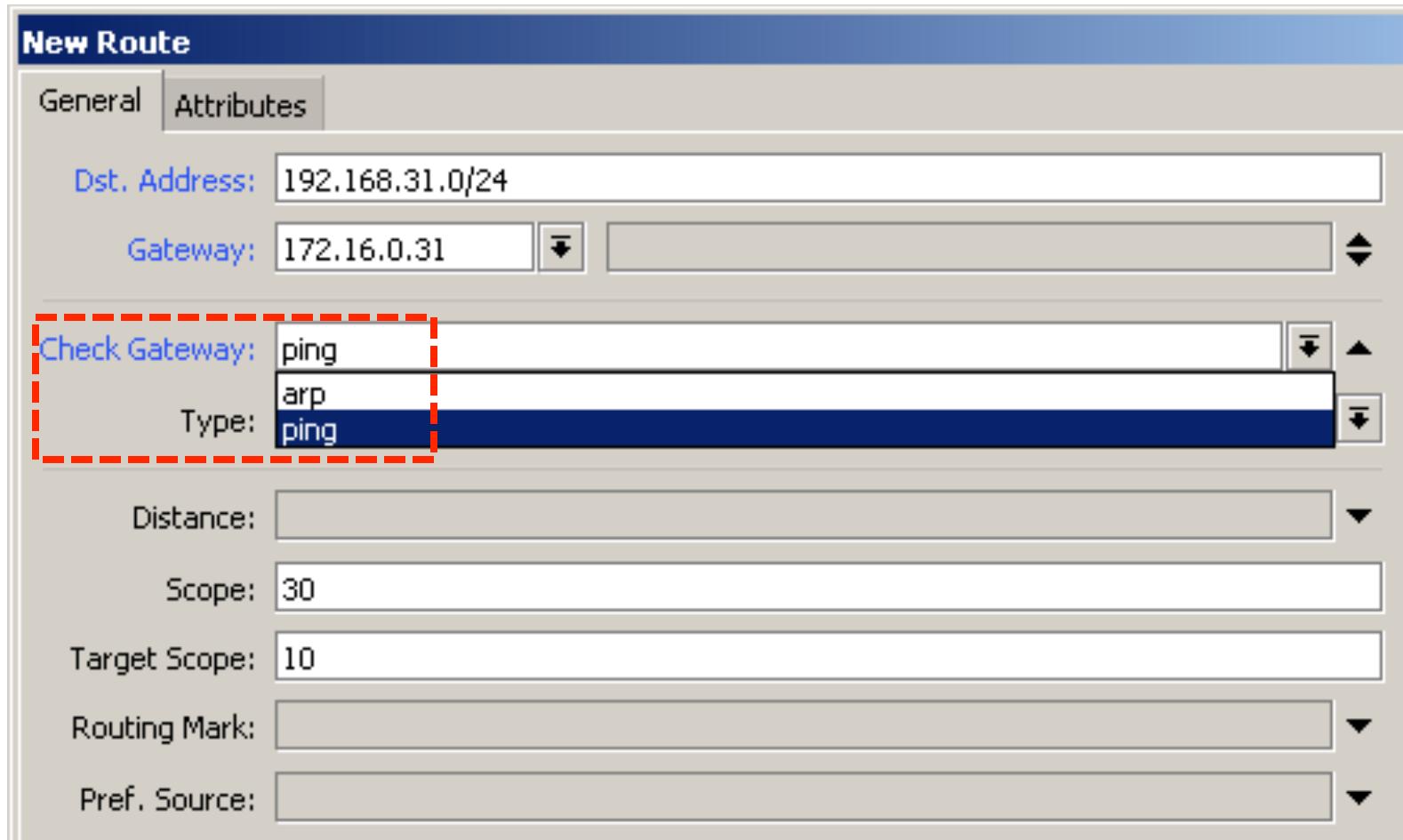




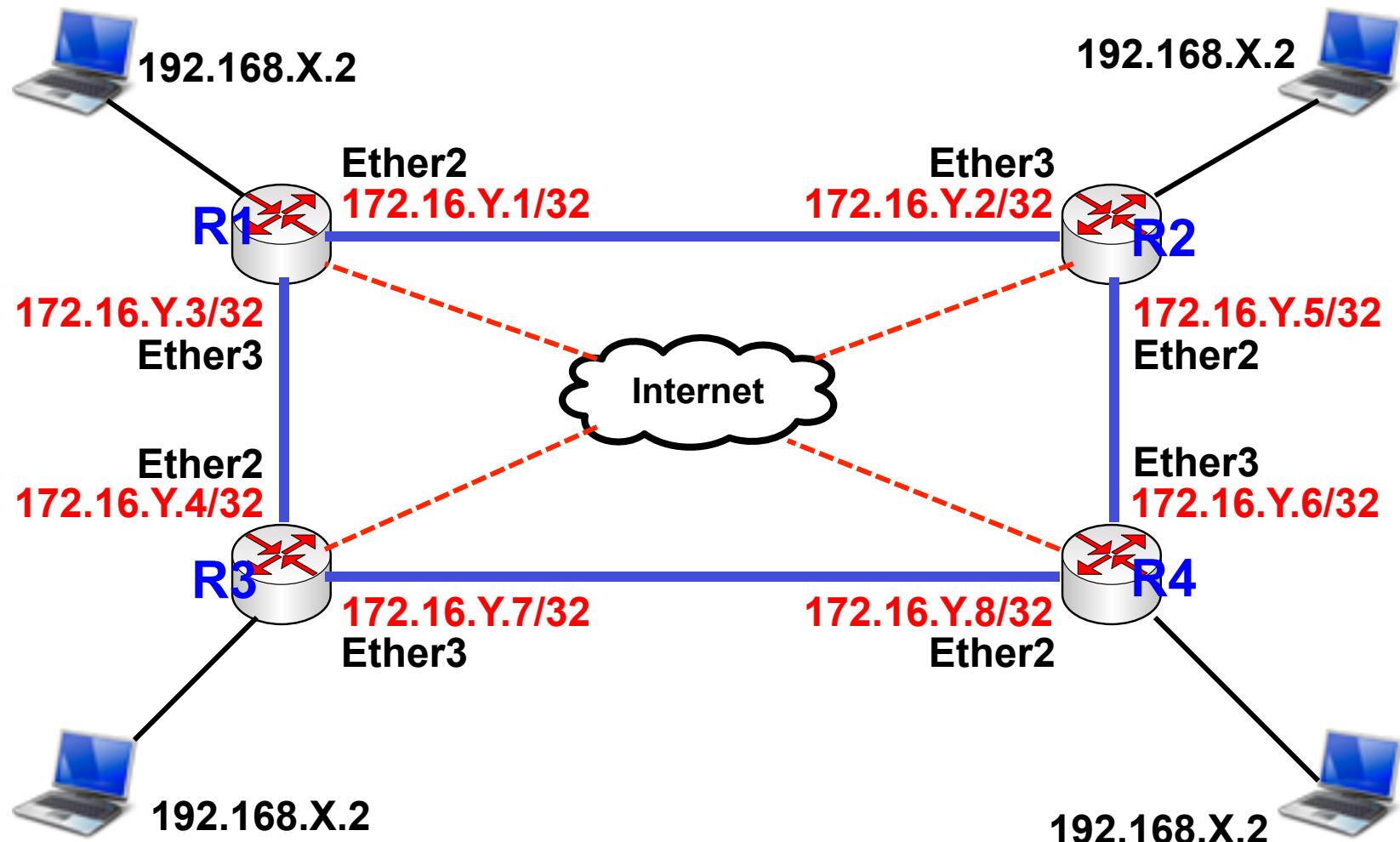
Check Gateway

- Adalah sebuah mekanisme pengecekan gateway yang 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 3 kali Gateway time-out berurutan.
- Jika mengaktifkan fitur check gateway untuk sebuah rule, maka akan berpengaruh juga untuk semua rule dengan gateway yang sama

Check Gateway Option



[LAB-6] Static Route

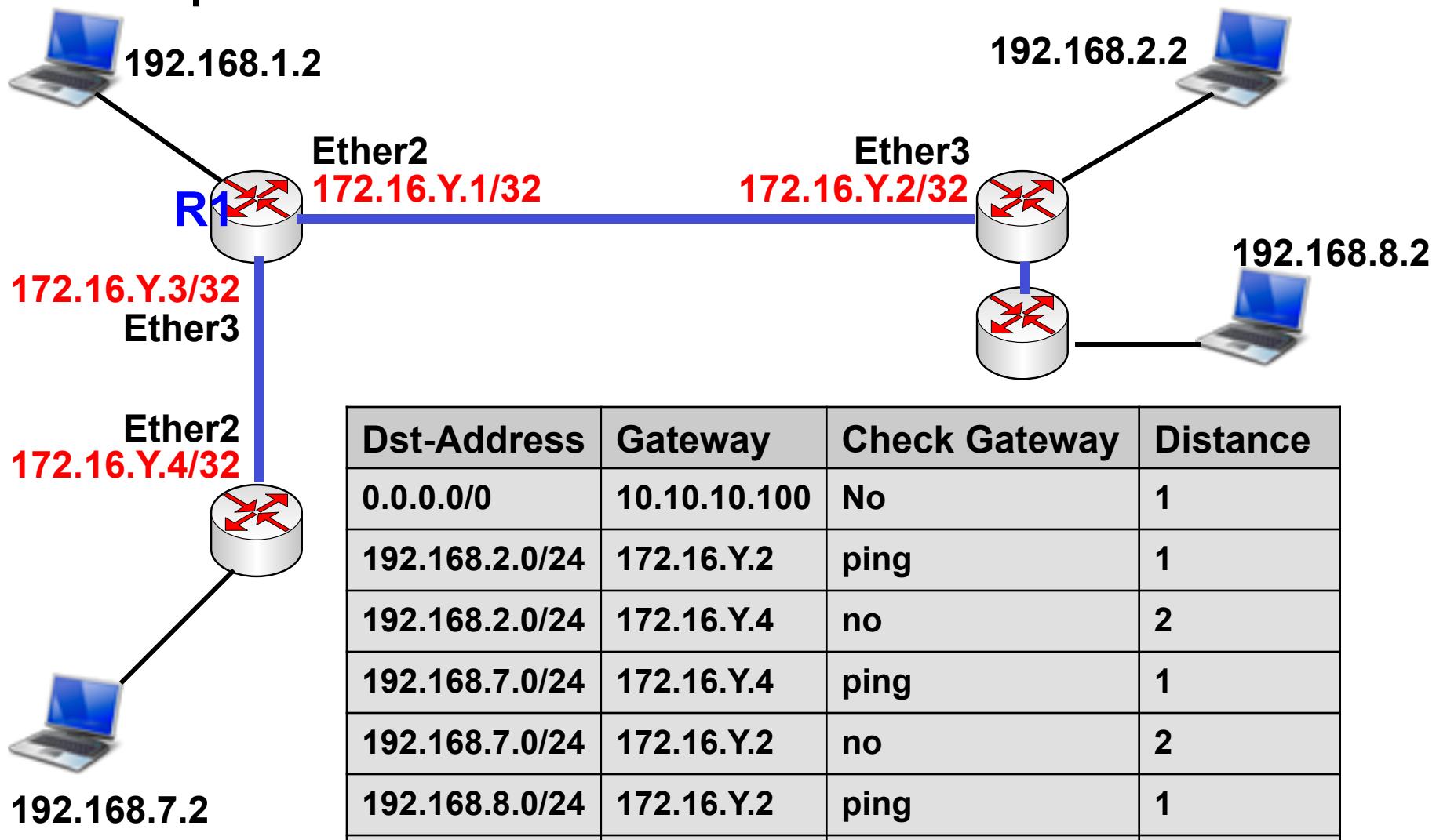




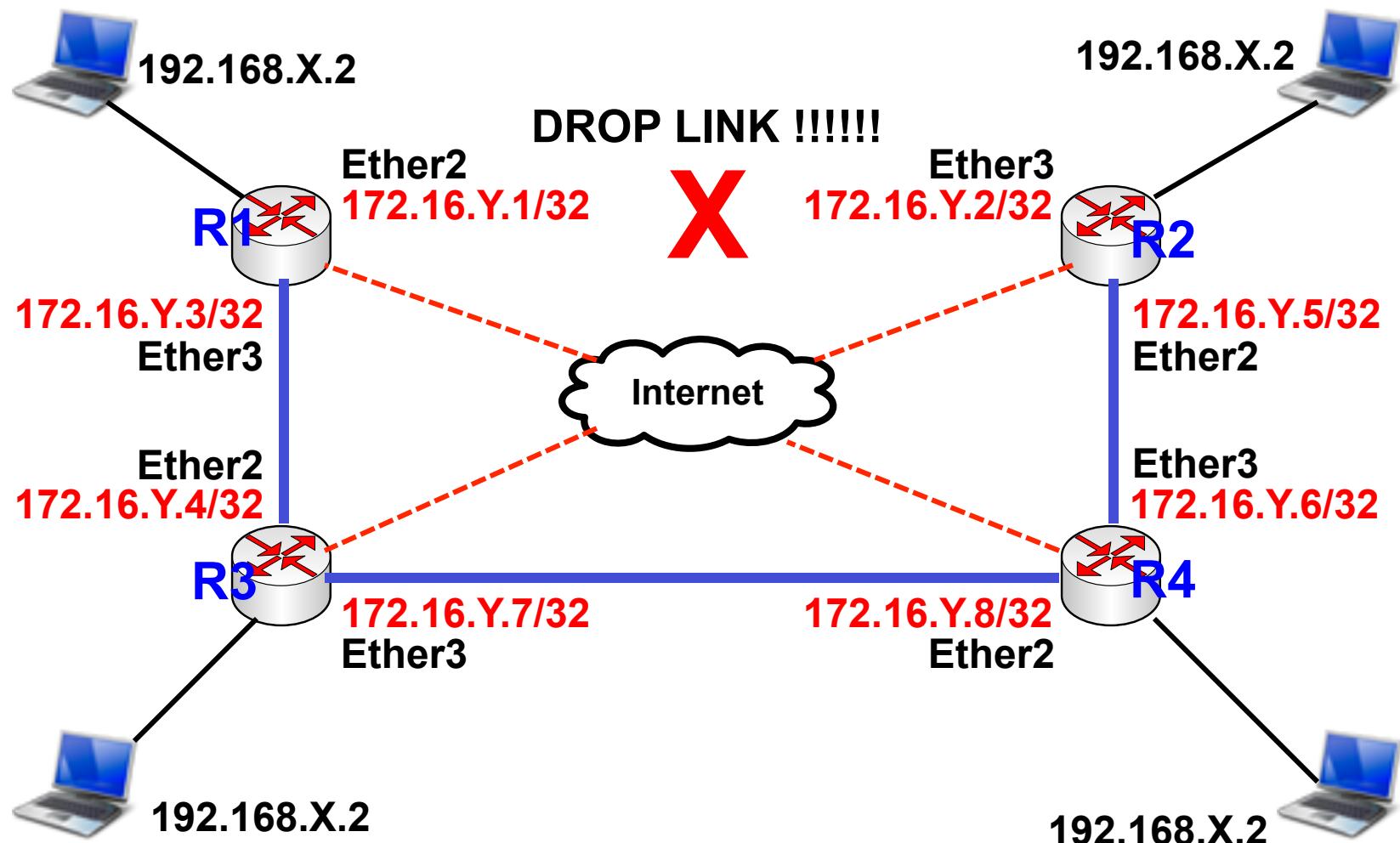
[LAB-6] Static Route 2

- Pasang ip **Point to Point** untuk menghubungkan semua Router dalam kelompok.
- Buatlah static route untuk menjangkau setiap laptop teman sekelompok menggunakan link **Point to Point** address.
- Konfigurasi **Distance** untuk menentukan Prioritas link.
- Link utama adalah melalui jalan terdekat
- Jika ada kondisi jaraknya sama, maka link utama adalah yang searah jarum jam.
- Pantaulah link utama dengan menggunakan **check-gateway**
- Buatlah static route juga untuk back-up link

Example Static route – on R1



[LAB-7] Static Route (Fail Over)





Evaluasi

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



Scope dan Target Scope

- Digunakan untuk static route yang dibuat recursive (tidak terkoneksi langsung).
- Target Scope adalah nilai scope maksimum dari rule lainnya yang reachable.
- Kegunaan:
 - Bisa melakukan pemantauan check gateway ping untuk gateway yang tidak terhubung langsung
 - Dikombinasikan dengan iBGP bila nexthop tidak direct connected

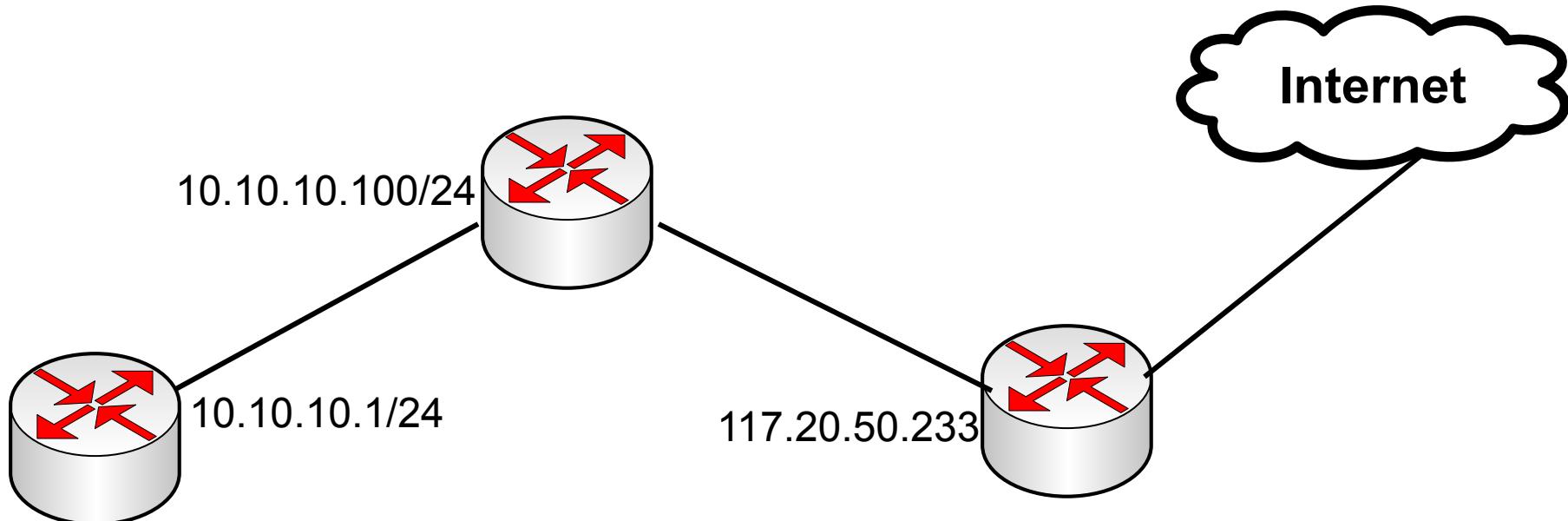
Scope dan Target Scope

- Nilai default scope dan target scope:

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

Scope dan Target Scope

- Contoh: dst-address 0.0.0.0/0 dengan gateway 117.20.50.233, recursive via 10.10.10.100



Dst-Address	Gateway	Scope	Target Scope
0.0.0.0/0	117.20.50.233	30	30
117.20.50.233	10.10.10.100	30	10



[LAB-8] Routing - Scope

- Sesuai dengan diagram network pada **LAB-2** sebelumnya, perbaikilah sistem monitoring link sehingga bisa mendeteksi adanya problem koneksi yang terjadi setelah gateway terdekat.
- Coba cabut salah satu koneksi kabel untuk mensimulasikan terjadinya permasalahan di salah satu link.

Routing Modification

Dst-Address	Gateway	Check Gateway	Distance	Scoop	Target Scoop
0.0.0.0/0	10.10.10.100	no	1	30	10
172.16.Y.5	172.16.Y.2	no	1	30	10
172.16.Y.6	172.16.Y.2	no	1	30	10
172.16.Y.7	172.16.Y.4	no	1	30	10
172.16.Y.8	172.16.Y.4	no	1	30	10
192.168.2.0/24	172.16.Y.2	ping	1	30	10
192.168.2.0/24	172.16.Y.4	no	2	30	10
192.168.7.0/24	172.16.Y.4	ping	1	30	10
192.168.7.0/24	172.16.Y.2	no	2	30	10
192.168.8.0/24	172.16.Y.6	ping	1	30	30
192.168.8.0/24	172.16.Y.4	no	2	30	10

Static Route dgn Scope

	Dst. Address	Gateway	Check ...	Distance	Scope	Target Scope
AS	▶ 0.0.0.0/0	10.10.10.100 reachable wlan1		1	30	10
DAC	▶ 10.10.10.0/24	wlan1 reachable		0	10	10
DAC	▶ 172.16.9.2	ether2 reachable		0	10	10
DAC	▶ 172.16.9.4	ether3 reachable		0	10	10
AS	▶ 172.16.9.5	172.16.9.2 reachable ether2		1	30	10
AS	▶ 172.16.9.6	172.16.9.2 reachable ether2		1	30	10
AS	▶ 172.16.9.7	172.16.9.4 reachable ether3		1	30	10
AS	▶ 172.16.9.8	172.16.9.4 reachable ether3		1	30	10
DAC	▶ 192.168.31.0/24	ether1 reachable		0	10	10
AS	▶ 192.168.32.0/24	172.16.9.2 reachable ether2	ping	1	30	10
S	▶ 192.168.32.0/24	172.16.9.4 reachable ether3		2	30	10
AS	▶ 192.168.33.0/24	172.16.9.4 reachable ether3	ping	1	30	10
S	▶ 192.168.33.0/24	172.16.9.2 reachable ether2		1	30	10
AS	▶ 192.168.34.0/24	172.16.9.6 recursive via 172.16.9.2 ether2	ping	1	30	30
S	▶ 192.168.34.0/24	172.16.9.4 reachable ether3		2	30	10

Static Route dgn Scope

Pada saat terjadi link failure antara R2 dan R4

	Dst. Address	Gateway	Check ...	Distance	Scope	Target Scope	I
AS	▶ 0.0.0.0/0	10.10.10.100 reachable wlan1		1	30	10	
DAC	▶ 10.10.10.0/24	wlan1 reachable		0	10	10	
DAC	▶ 172.16.9.2	ether2 reachable		0	10	10	
DAC	▶ 172.16.9.4	ether3 reachable		0	10	10	
AS	▶ 172.16.9.5	172.16.9.2 reachable ether2		1	30	10	
AS	▶ 172.16.9.6	172.16.9.2 reachable ether2		1	30	10	
AS	▶ 172.16.9.7	172.16.9.4 reachable ether3		1	30	10	
AS	▶ 172.16.9.8	172.16.9.4 reachable ether3		1	30	10	
DAC	▶ 192.168.31.0/24	ether1 reachable		0	10	10	
AS	▶ 192.168.32.0/24	172.16.9.2 reachable ether2	ping	1	30	10	
S	▶ 192.168.32.0/24	172.16.9.4 reachable ether3		2	30	10	
AS	▶ 192.168.33.0/24	172.16.9.4 reachable ether3	ping	1	30	10	
S	▶ 192.168.33.0/24	172.16.9.2 reachable ether2		1	30	10	
S	▶ 192.168.34.0/24	172.16.9.6 recursive via 172.16.9.2 ether2	ping	1	30	30	
AS	▶ 192.168.34.0/24	172.16.9.4 reachable ether3		2	30	10	

Routing Type

- Kita bisa melakukan blok untuk 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.



Pref-source

- By default: null, kecuali untuk connected routes
- 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
- Jika isian pref-src adalah IP Address yang tidak terpasang pada router, rule ini akan non-aktif.

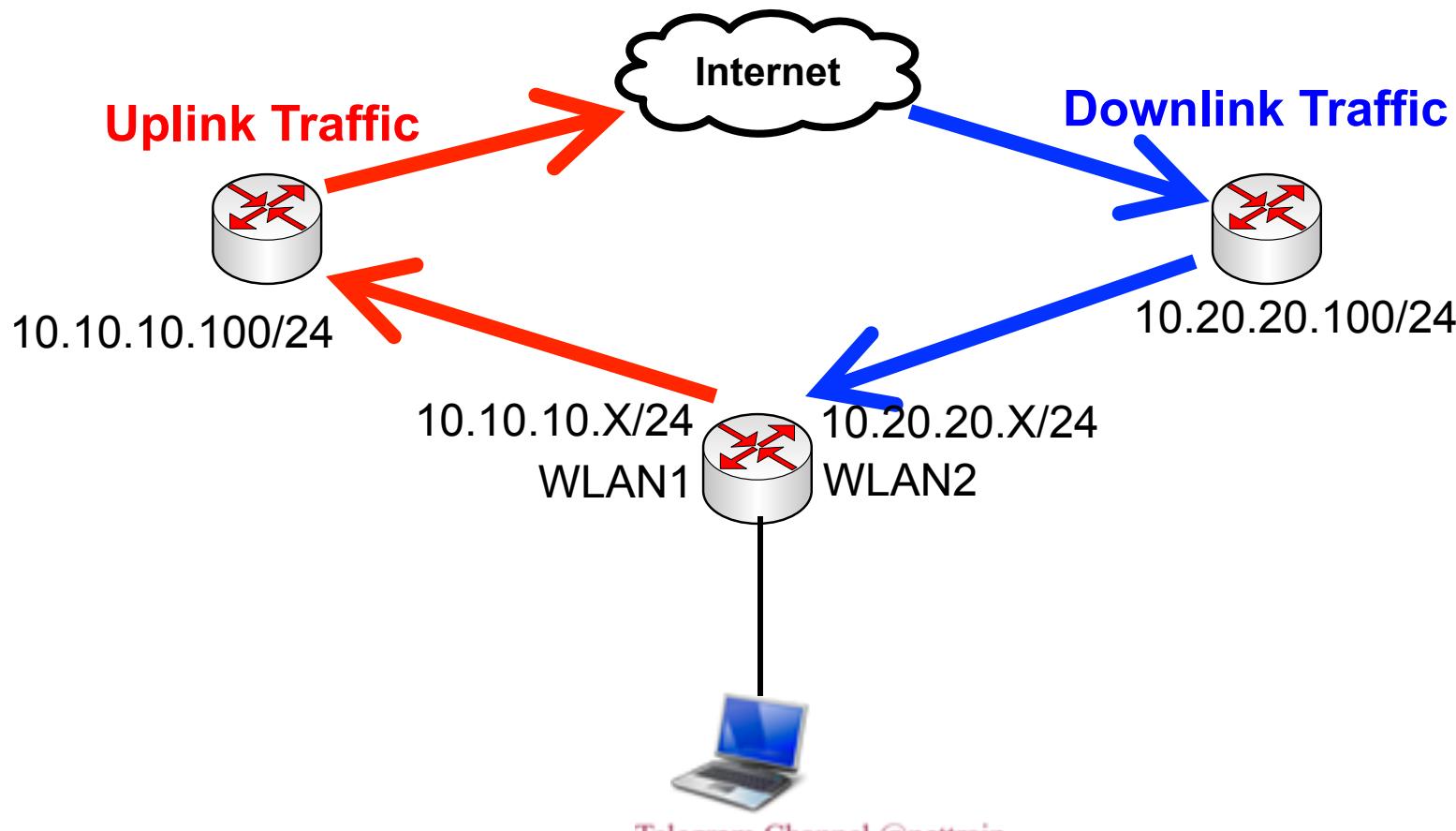


Source Routing

- Source Routing adalah sebuah teknik rotuing yang memungkinkan Administrator jaringan menentukan jalur routing yang akan dilalui oleh paket data.
- Perlu diingat bahwa parameter “dst-address” pada paket header akan selalu diperiksa oleh router yang dilewatinya untuk menentukan hoop selanjutnya.
- Dengan memodifikasi Pref-Source Maka jalur routing balik bisa dimanipulasi sesuai keinginan administrator.

[LAB-9] Pref-Source

- Uplink menggunakan gateway 1
- Downlink menggunakan gateway 2.



Static Route Setting

Route <0.0.0.0/0>

General Attributes

Dst. Address: 0.0.0.0/0

Gateway: 10.10.10.100 ↴ reachable wlan1

Check Gateway:

Type: unicast

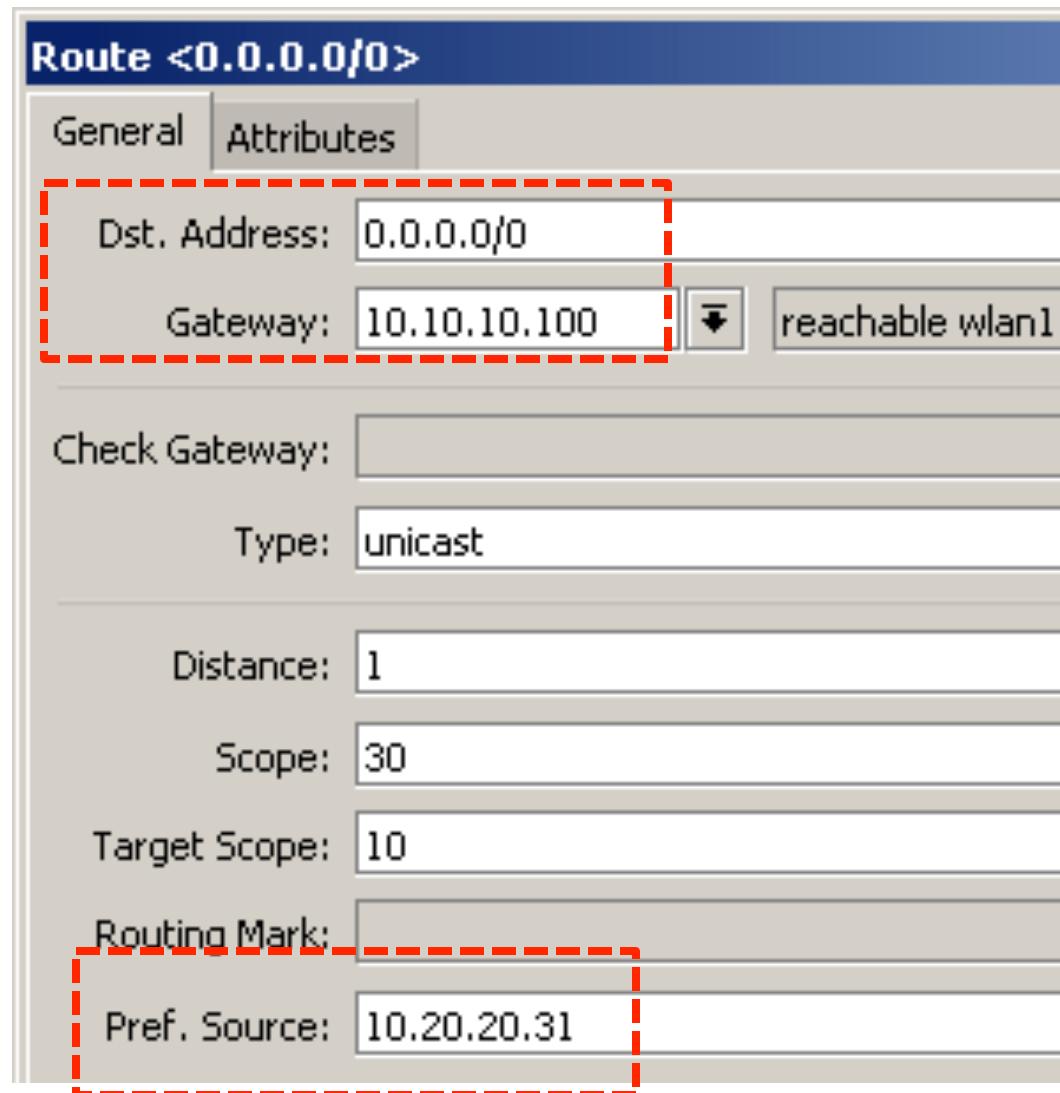
Distance: 1

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source: 10.20.20.31

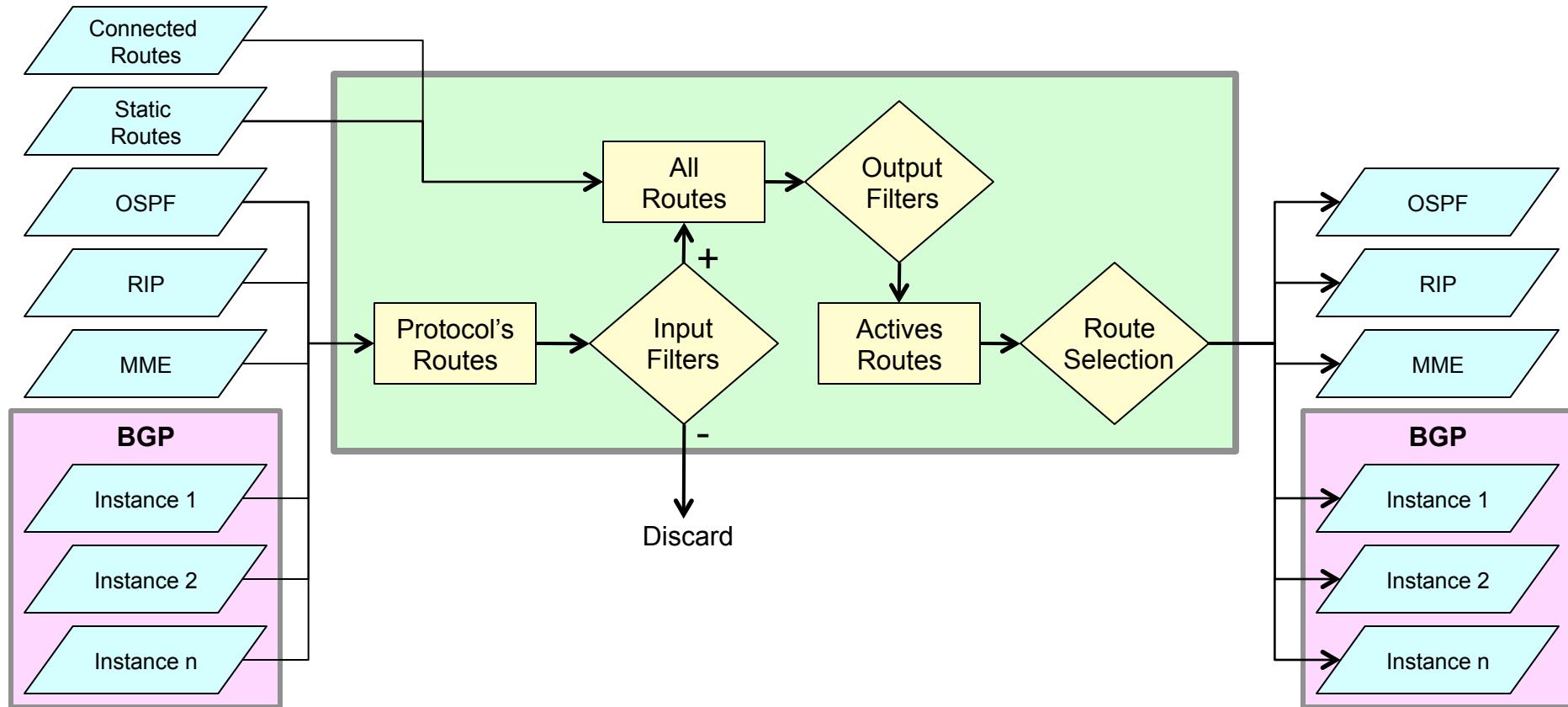


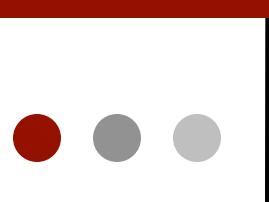
Src-Nat Setting

NAT Rule <>	
General	Advanced
Chain:	srcnat
Src. Address:	
Dst. Address:	
Protocol:	
Src. Port:	
Dst. Port:	
Any. Port:	
In. Interface:	
Out. Interface:	<input type="checkbox"/> wlan1

NAT Rule <>	
General	Advanced
Action:	src-nat
To Addresses:	10.20.20.31
To Ports:	

Routing Information Base





Routing Information Base

- Berisi informasi routing yang lengkap, yang terdiri dari:
 - Static routes dan Policy Routing Rules
 - Informasi routing dari Routing Protocol (OSPF, BGP, etc)
 - Informasi Connected Routes

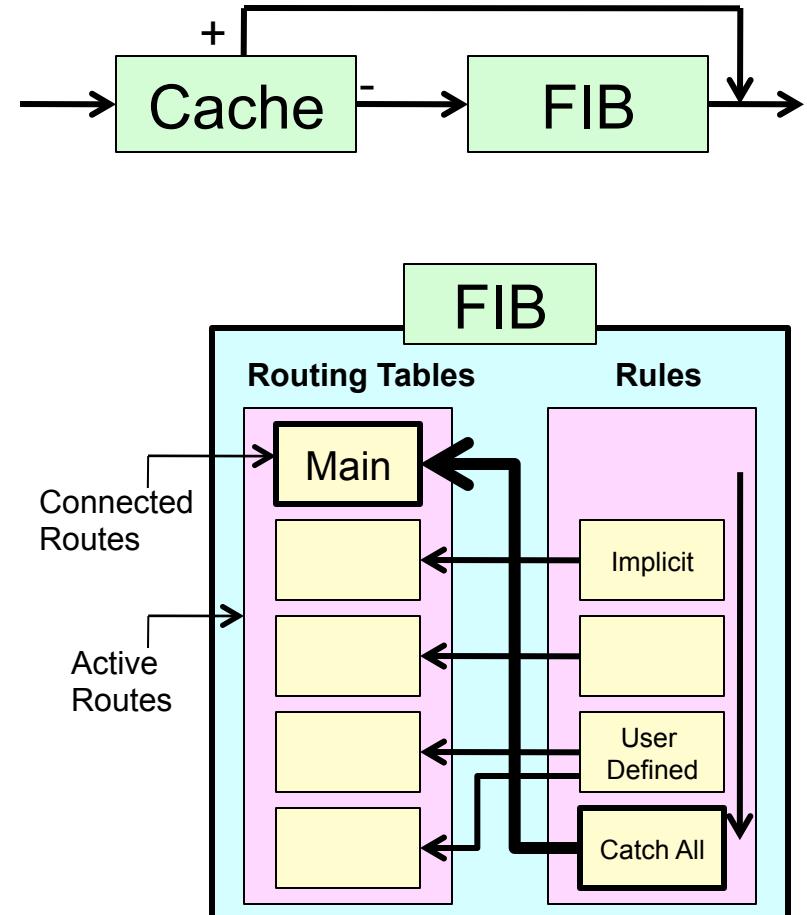


Routing Information Base

- Digunakan untuk:
 - Memfilter informasi routing
 - Mengkalkulasi best route untuk masing-masing dst-address/prefix
 - Membuat dan mengupdate Forwarding Information Base (FIB)
 - Mendistribusikan informasi routing ke routing protokol lainnya

Forwarding Information Base

- Merupakan informasi routing yang disimpan dalam cache, sebagai hasil olahan Routing Information Base yang telah terfilter



Policy Route

- Secara default, router akan menggunakan table routing “main”
- Kita bisa membuat table routing tambahan dan mengarahkan router menggunakan table tersebut dengan menggunakan:
 - **IP - Route – Rules**
 - **IP - Firewall - Mangle – Route-mark**

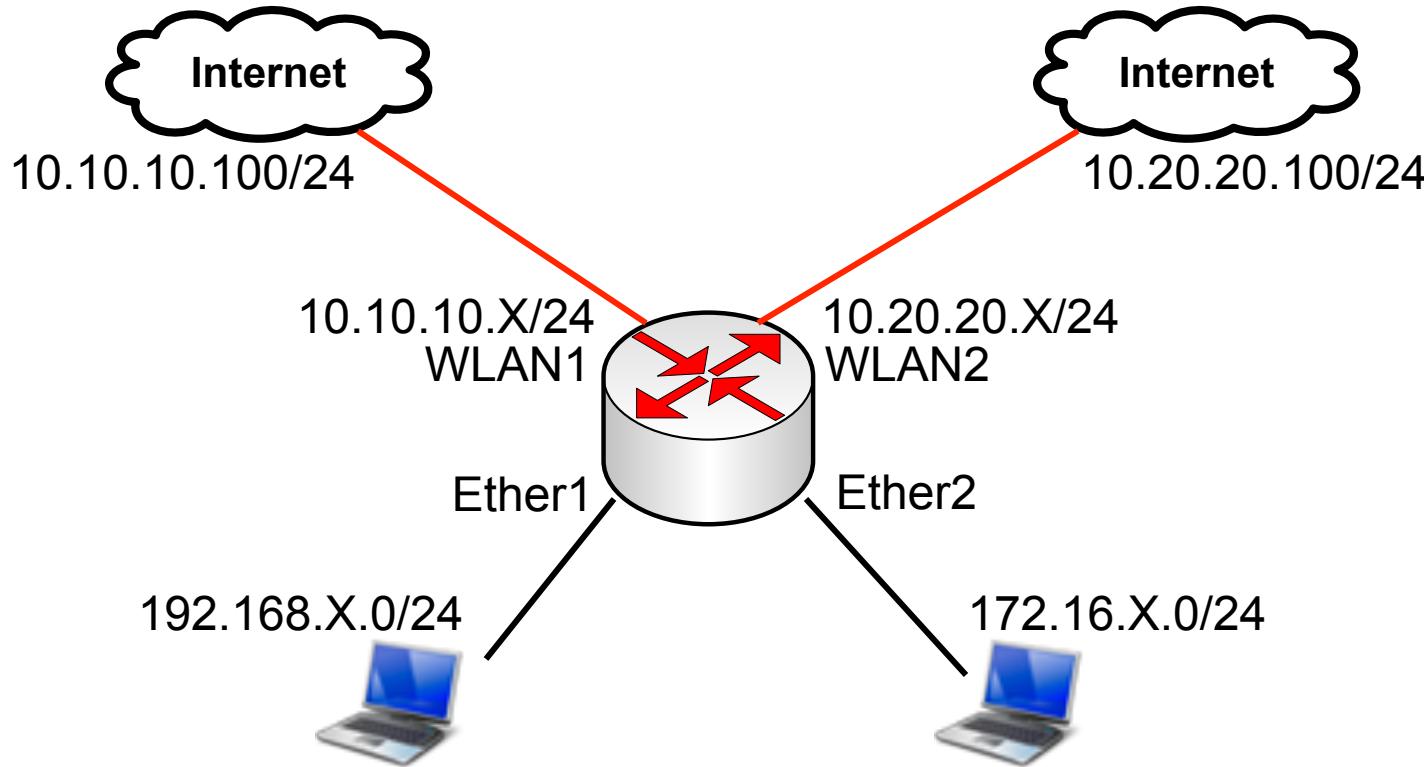
Route Rules

- Route rules hanya dapat melakukan filtering berdasarkan src-address, dst-address, routing-mark, dan interface.
- Untuk filtering yang lebih detail, gunakanlah mangle.

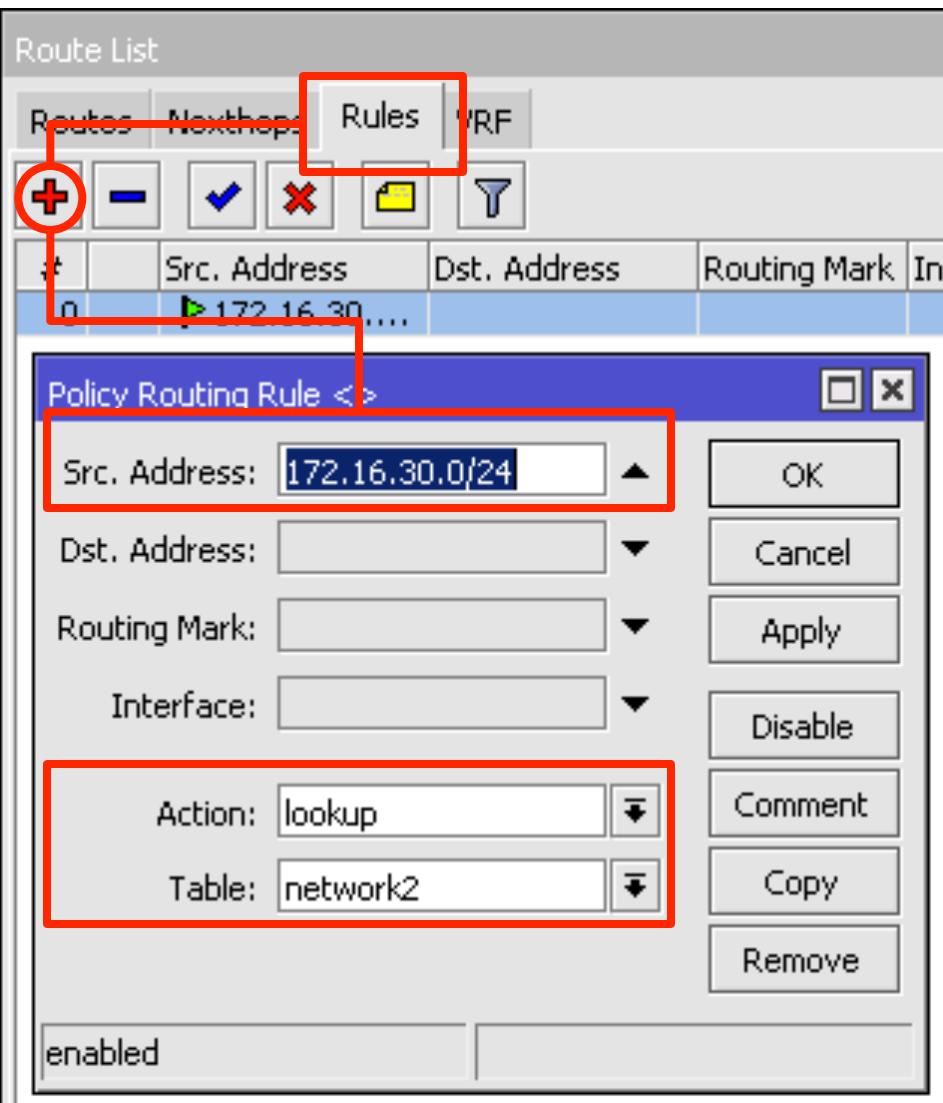


[LAB-10] Route Mark

- WLAN1: Untuk traffic dari 192.168.x.0/24
- WLAN2: Untuk traffic dari 172.16.x.0/24



Route - Rules



- Tambahkan Route – Rules untuk menentukan klasifikasi dari segmen network yang akan menggunakan gateway yang berbeda.

● ● ● | Routing Table - Rules

- Tambahkan rule routing untuk mengarahkan segmen network2 supaya menggunakan gateway lain.

Route <0.0.0.0/0>

General Attributes

Dst. Address: 0.0.0.0/0

Gateway: 10.20.20.100

Check Gateway:

Type: unicast

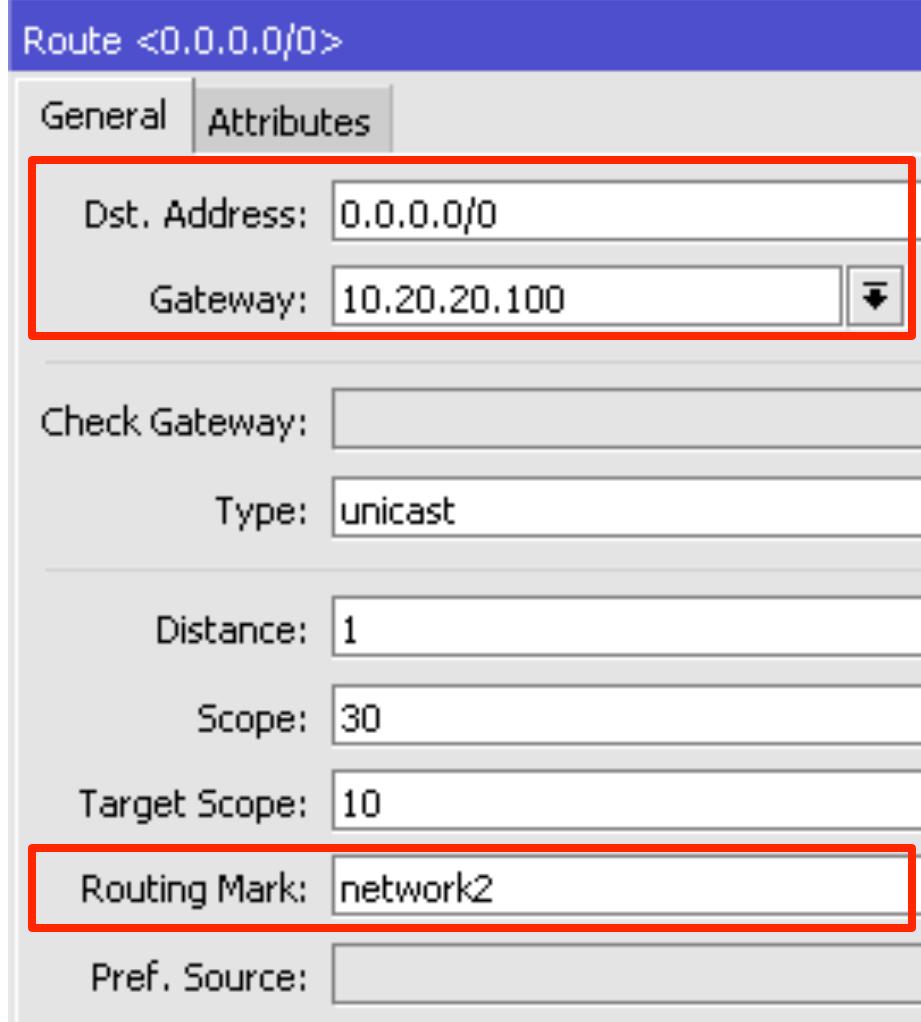
Distance: 1

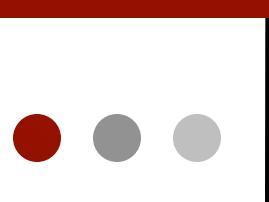
Scope: 30

Target Scope: 10

Routing Mark: network2

Pref. Source:



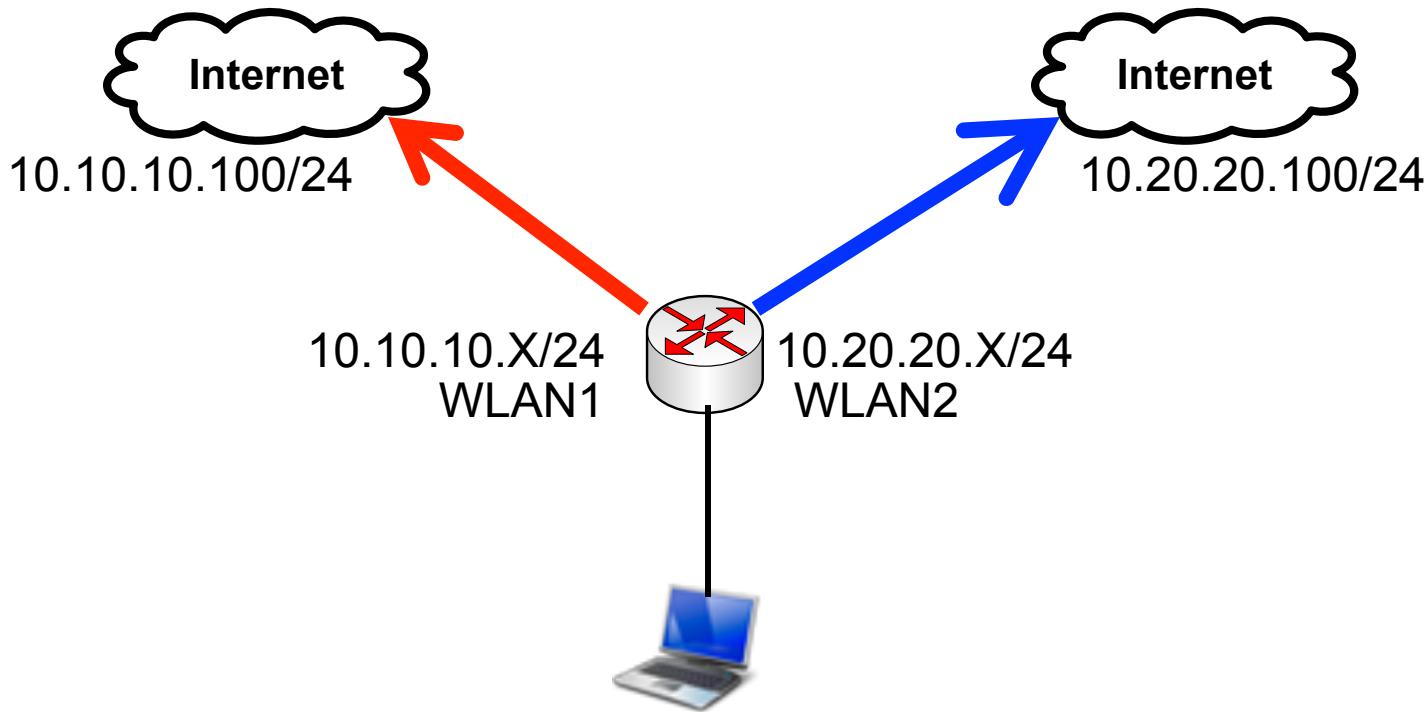


Mangle Route Mark

- Untuk trafik yang melalui router:
 - Mangle chain: prerouting
- Untuk trafik yang berasal dari router, keluar:
 - Mangle chain: output
- Chain lainnya (input, forward, dan postrouting) tidak dapat digunakan untuk melakukan route-mark.

[LAB-11] Route Mark

- WLAN1: **All other traffic**
- WLAN2: **Web only**



Route Mark (client)

Mangle Rule <80>

General Advanced Extra Action Statistics

Chain: (highlighted)

Src. Address:

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port: 80

Any. Port:

P2P:

In. Interface: ether1 (highlighted)

Out. Interface:

Mangle Rule <80>

General Advanced Extra Action Statistics

Action: (highlighted)

New Routing Mark: (highlighted)

Passthrough

Route Mark (local process)

New Mangle Rule

General Advanced Extra Action Statistics

Chain: (highlighted)

Src. Address:

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port: 80

Any. Port:

P2P:

In. Interface:

Out. Interface: wlan1 (highlighted)

Mangle Rule <80>

General Advanced Extra Action Statistics

Action: (highlighted)

New Routing Mark: (highlighted)

Passthrough

Static Route

Trafik Lainnya

Route <0.0.0.0/0>

General	Attributes
Dst. Address:	0.0.0.0/0
Gateway:	10.10.10.100
reachable wlan1	
Check Gateway:	
Type:	unicast
Distance:	1
Scope:	30
Target Scope:	10
Routing Mark:	
Pref. Source:	

Trafik TCP 80

New Route

General	Attributes
Dst. Address:	0.0.0.0/0
Gateway:	10.20.20.100
reachable wlan1	
Check Gateway:	
Type:	unicast
Distance:	
Scope:	30
Target Scope:	10
Routing Mark:	route-web
Pref. Source:	



Tunnel



Certified Mikrotik Training Advanced Class (MTCRE)

Organized by: Citraweb Nusa Infomedia

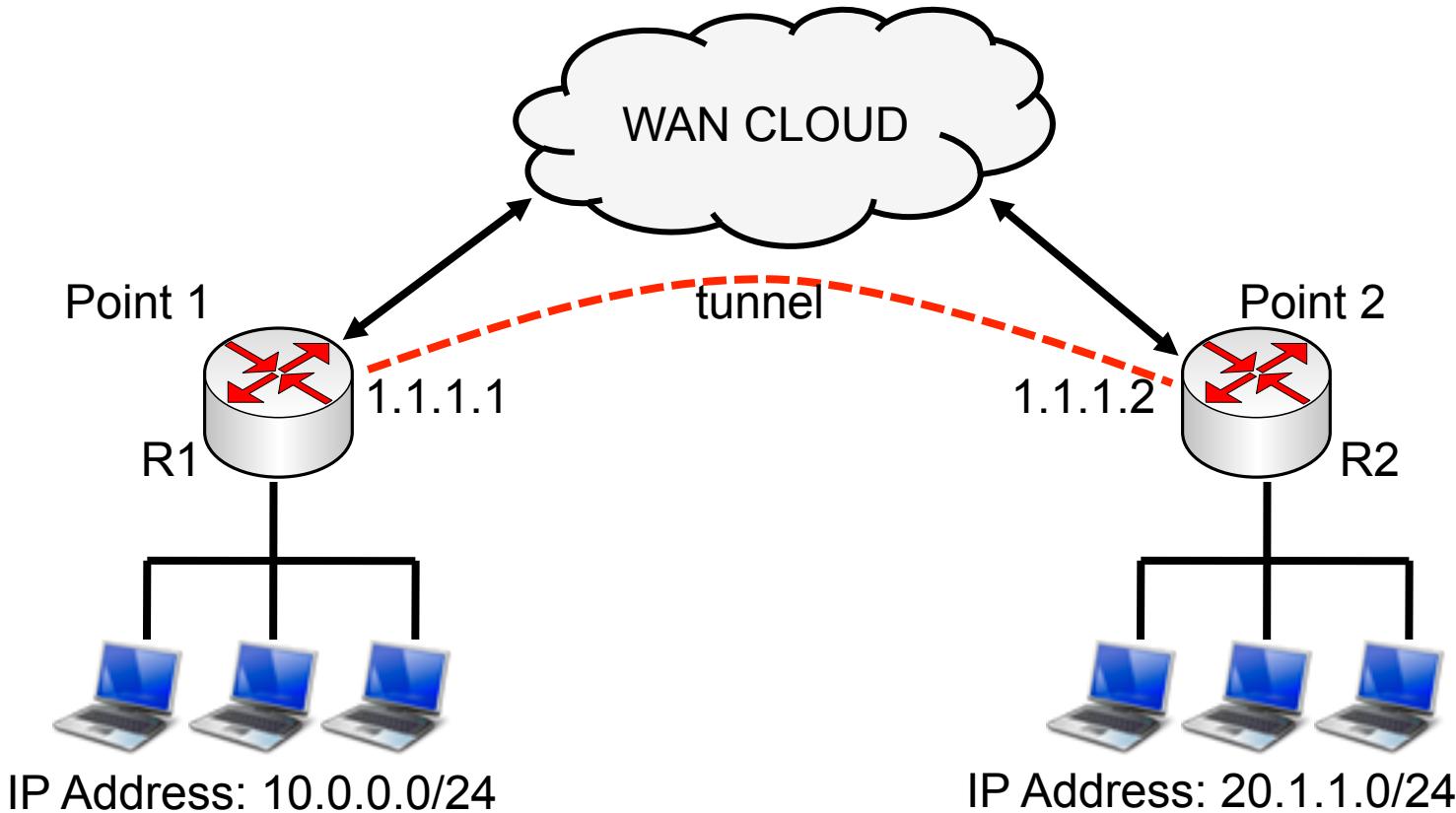
(Mikrotik Certified Training Partner)



IP Tunnel

- Tunnel adalah sebuah metode penyelubungan (encapsulation) paket data di jaringan TCP/IP, yang biasanya digunakan untuk mensimulasikan koneksi fisik antara dua network melewati jaringan yang lebih besar (WAN/Internet).
- Paket data dari aktifitas transfer data di kedua network mengalami sedikit pengubahan atau modifikasi. Yaitu penambahan header dari tunnel di tiap paket data dari traffic yang terjadi di kedua network tersebut. Walupun ada pengubahan pada paket data informasi paket yang asli tetap disertakan (RFC 2003 compliant).
- Ketika data sudah melewati tunnel dan sampai di tujuan (ujung) tunnel, maka header dari paket data akan dikembalikan seperti semula (header tunnel dihilangkan).

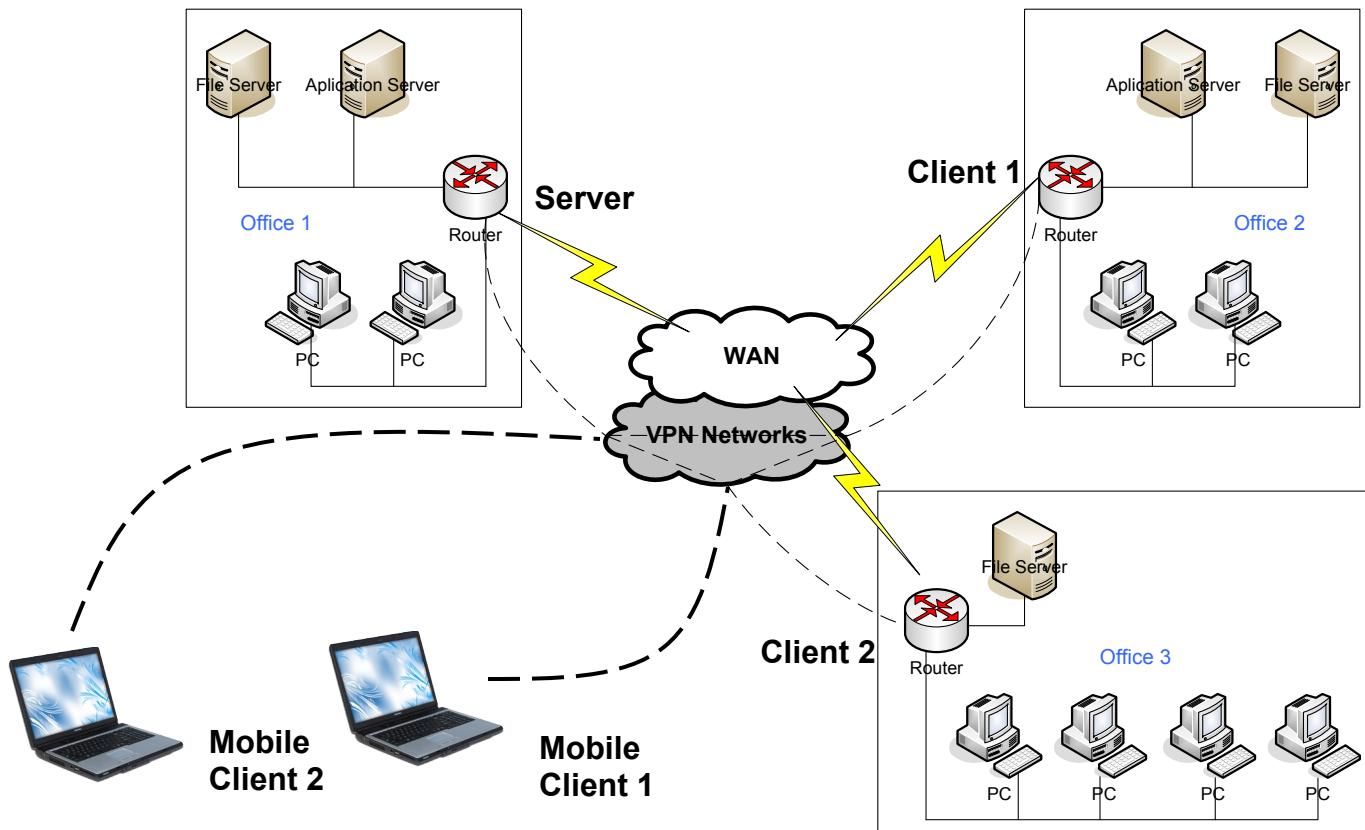
IP Tunnel Network

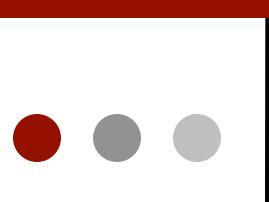


Point to point network encapsulation

VPN Networks

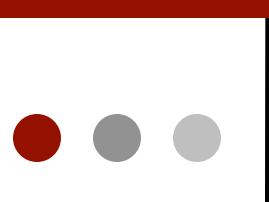
- Virtual private network. A private data network that utilizes a public telecommunication infrastructure.





Tunnel & VPN

- Tunnel
 - IPIP – IP Tunnel
 - EoIP – Ethernet Over IP
 - VLAN – Virtual Lan
 - Gre Tunnel
- VPN
 - PPPoE – PointToPointProtocol Over Ethernet
 - PPTP – PointToPoint Tunnel Protocol
 - L2TP – Layer 2 Tunnel Protocol
 - OpenVPN – Open Virtual Private Network
 - IPSec – IP Security
 - SFTP – Secure Socket Tunnel Protocol



IPIP

- IPIP adalah salah satu protocol tunnel yang paling sederhana dan ringan yang mampu menghubungkan dua router melewati jaringan TCP/IP.
- IPIP Tunnel bisa dibuat di menu Interface dan dianggap sebagai interface (fisik tetapi virtual) yang independen.
- Sudah banyak type router support protocol ini seperti CISCO dan Linux.
- IPIP Tunnel bisa digunakan untuk :
 - Routing antar local network melewati jaringan internet
 - Digunakan untuk menggantikan **Source Routing**
- Interface IPIP tunnel **tidak bisa** dimasukkan dalam bridge network (**bridge port**).

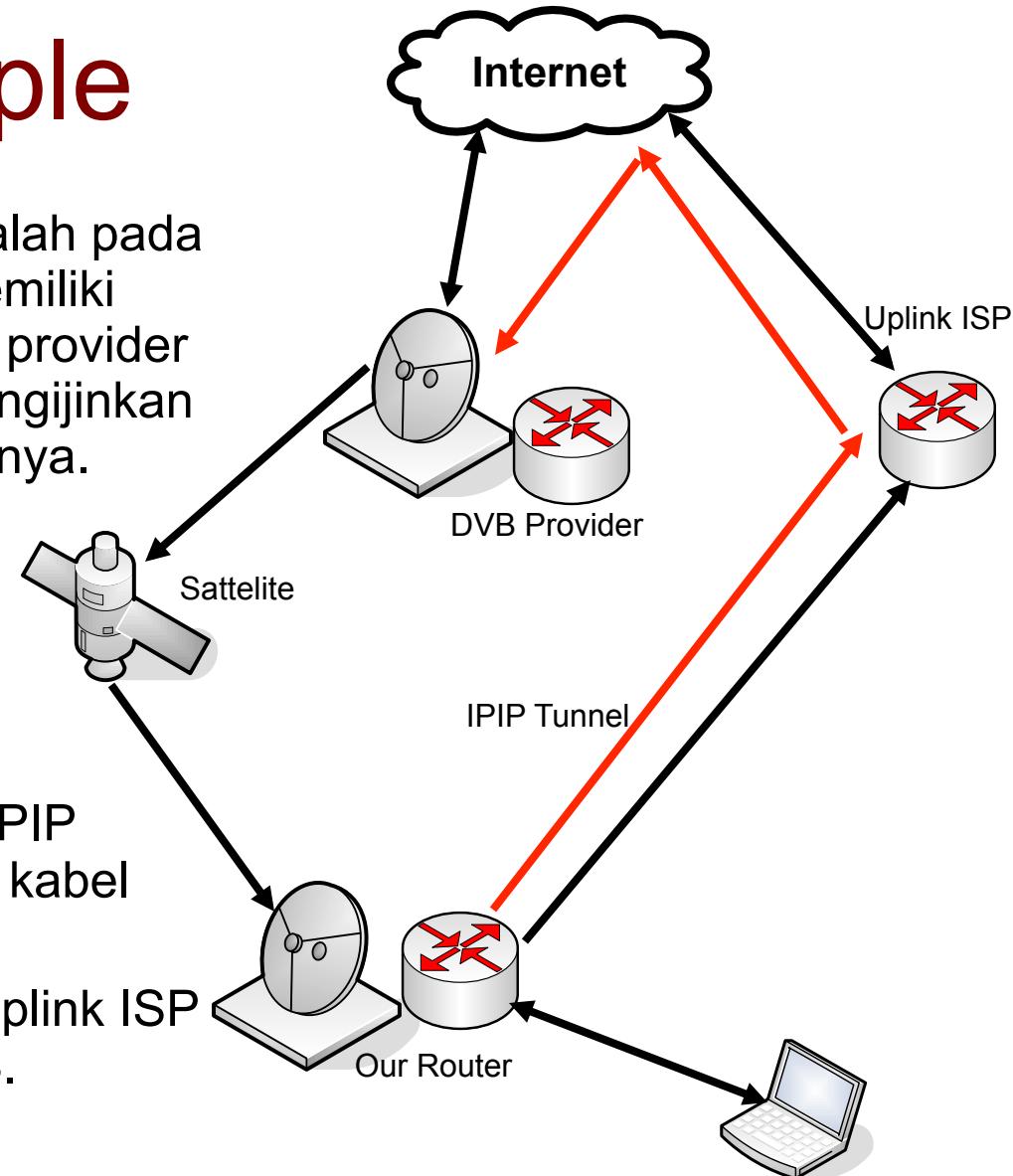
IPIP Packet Header

Packet Sniffer							
Packets	Connections	Hosts	Protocols				
Packet Sniffer Settings							
Time (s)	Interface	Direction	Src. Address	Dst. Address	Protocol	IP Protocol	Size
1.876	ether1	in	192.168.5.1	192.168.5.29	2048 (ip)	4 (ip-encap)	94
2.877	ether1	in	192.168.5.1	192.168.5.29	2048 (ip)	4 (ip-encap)	94
3.879	ether1	in	192.168.5.1	192.168.5.29	2048 (ip)	4 (ip-encap)	94
4.881	ether1	in	192.168.5.1	192.168.5.29	2048 (ip)	4 (ip-encap)	94
0.738	ether1	in	192.168.5.1	192.168.5.29	2048 (ip)	47	60
0.682	ether1	in	192.168.5.23:137	192.168.5.255:137	2048 (ip)	17 (udp)	92
1.865	ether1	out	192.168.5.29	192.168.5.1	2048 (ip)	4 (ip-encap)	94
2.866	ether1	out	192.168.5.29	192.168.5.1	2048 (ip)	4 (ip-encap)	94
3.867	ether1	out	192.168.5.29	192.168.5.1	2048 (ip)	4 (ip-encap)	94
4.869	ether1	out	192.168.5.29	192.168.5.1	2048 (ip)	4 (ip-encap)	94
3.907	ether1	out	192.168.5.29	192.168.5.1	2048 (ip)	47	42

- Test packet sniffer dilakukan untuk mengetahui besar packet header yang digunakan oleh protocol tunnel IPIP.
- Terlihat Tunnel IPIP menggunakan sekitar 20-40 byte pada tiap packet headernya di setiap paket data yang lewat.
- Paket header standardnya adalah 20byte.
- (GRE Protocol Packet size) 42 byte = 20 byte (ip header) + 22 (Encap Header)**

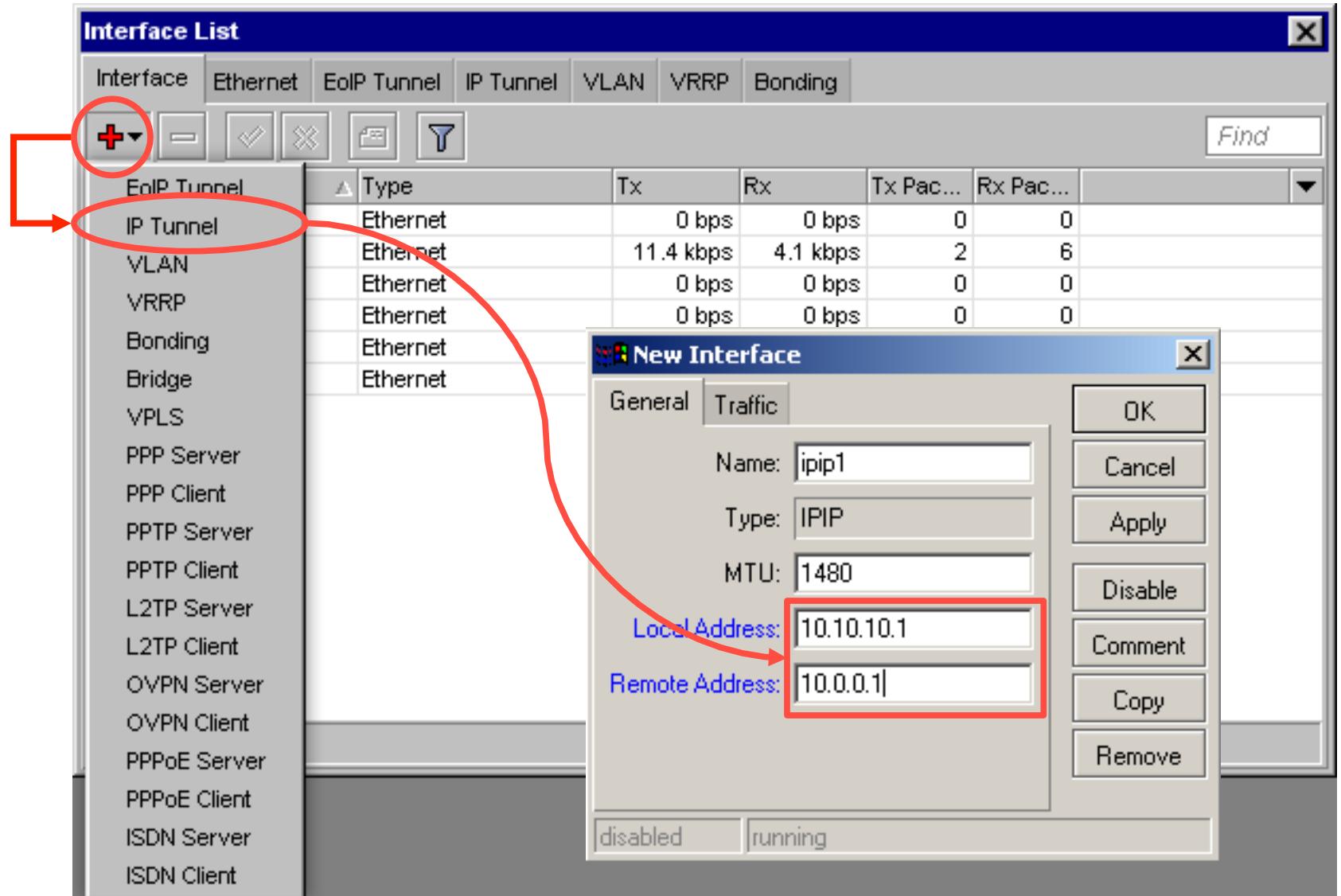
IPIP Example

- Salah satu pengaplikasiannya adalah pada kondisi sebuah network hanya memiliki koneksi VSAT DVB downlink only provider dan uplink provider yang tidak mengijinkan ip ISP lain yang melewati networknya.



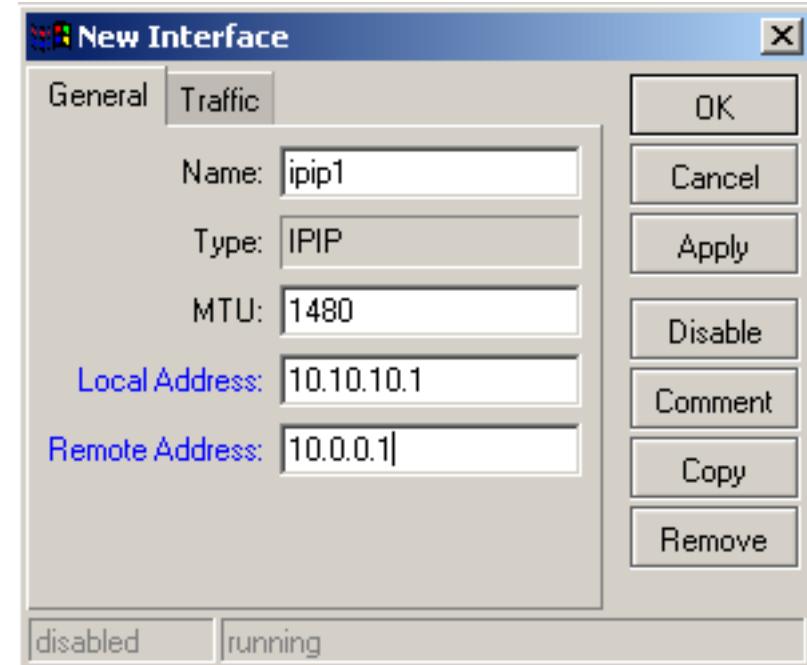
- Maka kita bisa membuat sebuah IPIP tunnel untuk mensimulasi koneksi kabel independen ke DVB provider.
- Sehingga traffic uplink melewati Uplink ISP dan traffic downlink melewati DVB.

IPIP Configuration

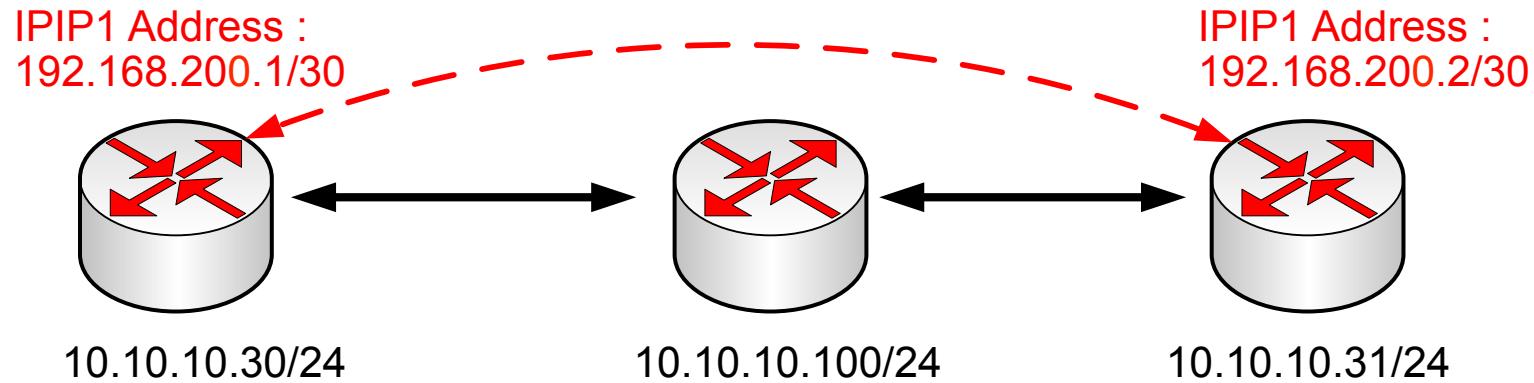


IPIP Configuration

- Parameter **Local Address** adalah parameter untuk ip local router yang digunakan untuk membangun koneksi IPIP tunnel.
- Sedangkan **Remote Address** adalah parameter dari ip address router lawan.
- Gunakan IP public pada kedua parameter ini untuk mebangun sebuah IPIP tunnel melewati jaringan WAN / Internet.



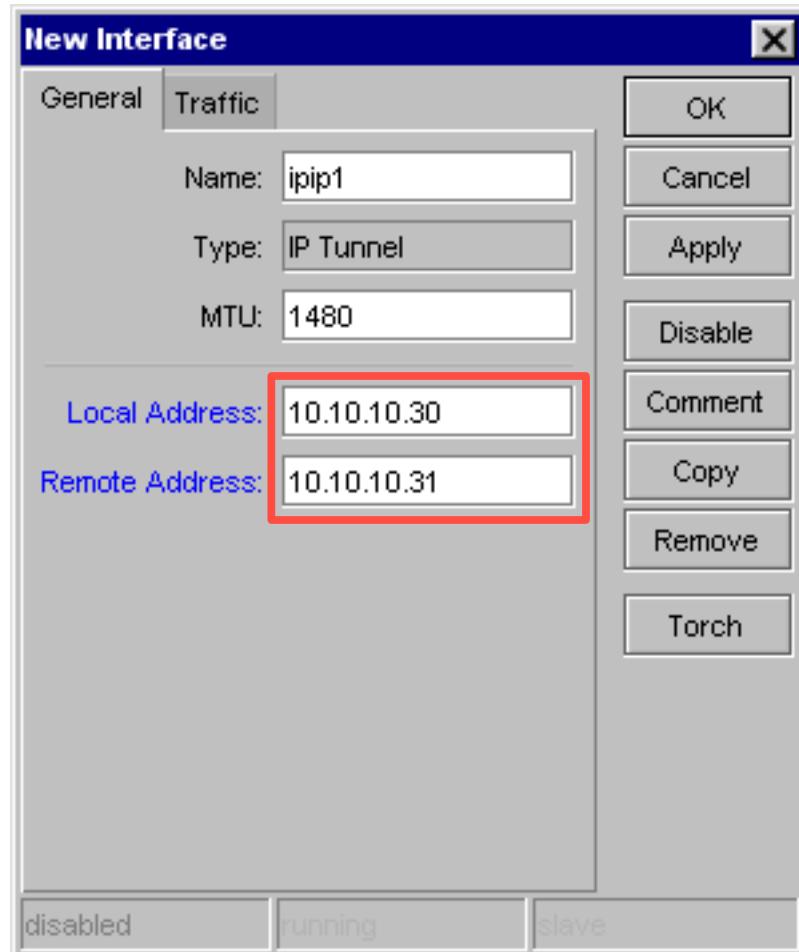
[LAB-1] IPIP Tunnels



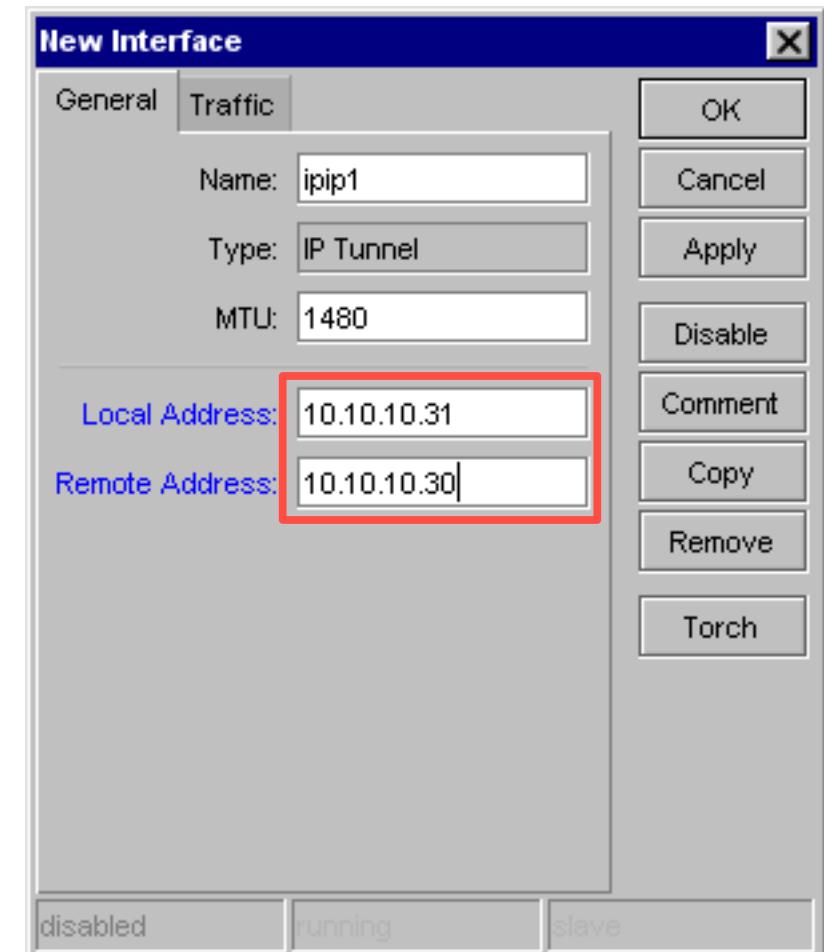
- IPIP Tunnel melewati jaringan WAN.
- Tambahkan ip address untuk menghubungkan kedua interface tunnel.
- Tambahkan rule static routing untuk menghubungkan kedua local network dari masing-masing router.

[LAB-1] IPIP Tunnels

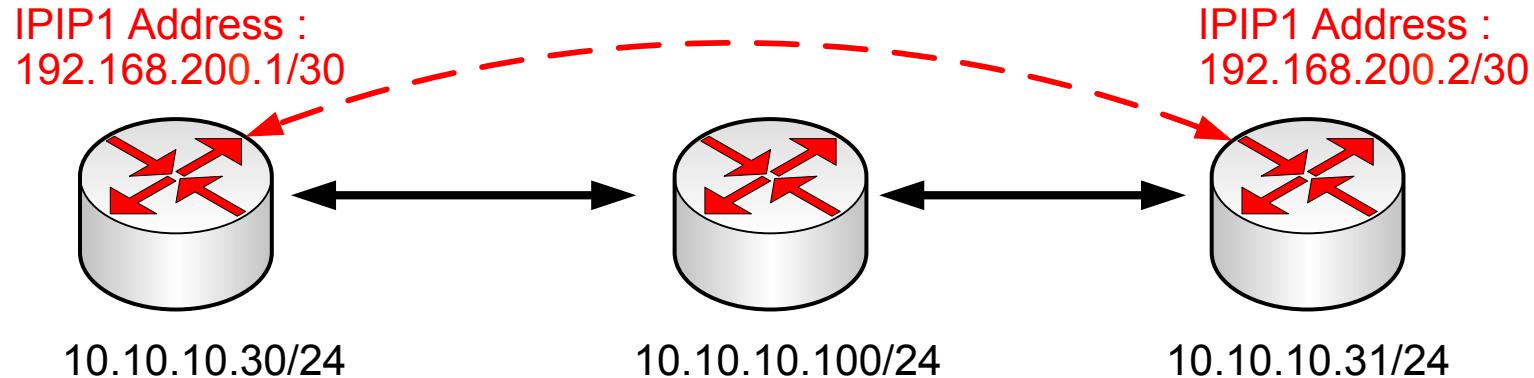
ROUTER A



ROUTER B

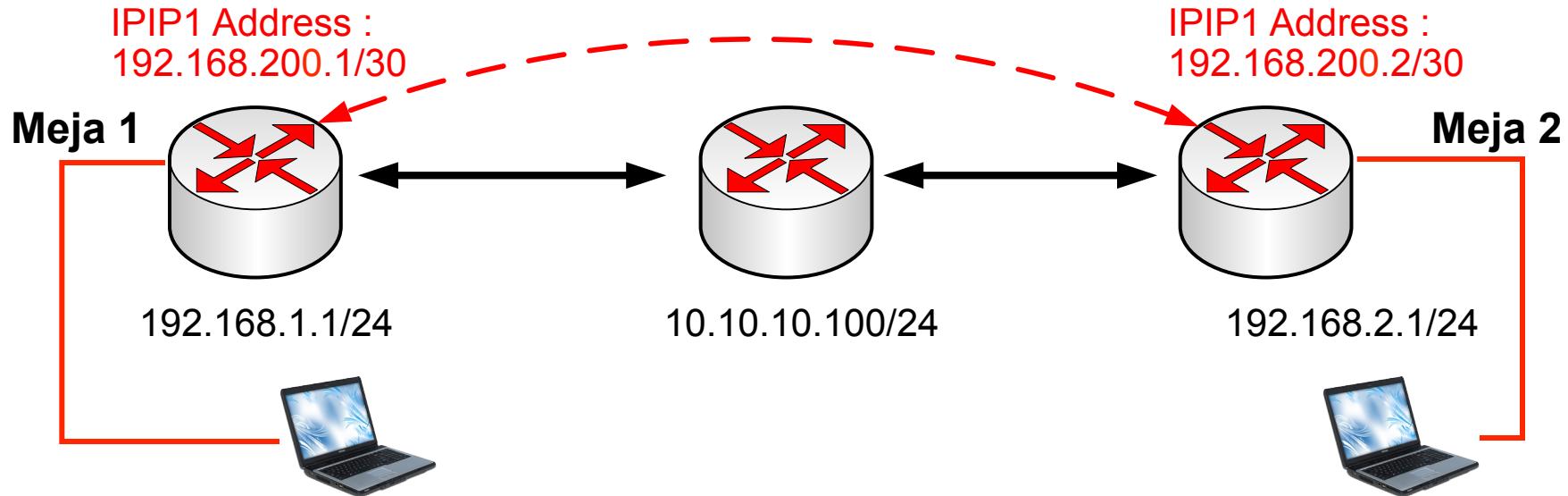


[LAB-1] IPIP Tunnels

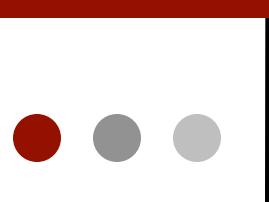


- /interface ipip add name=ipip1 local-address=10.10.10.30 remote-address=10.10.10.31
- /ip address add address=192.168.200.1/30 interface=ipip1
- /interface ipip add name=ipip1 local-address=10.10.10.31 remote-address=10.10.10.30
- /ip address add address=192.168.200.2/30 interface=ipip1

[LAB-1] Routing over Tunnel



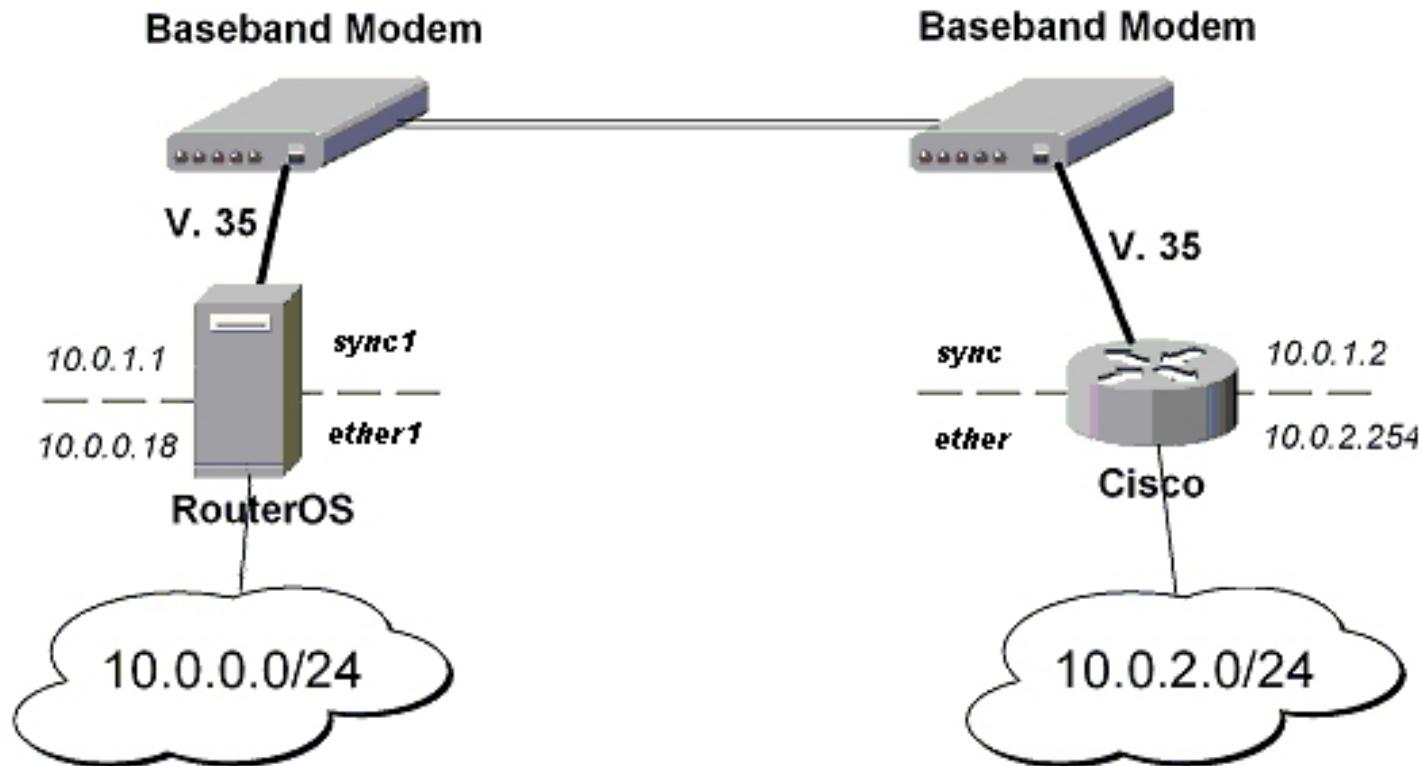
- Static route untuk menghubungkan kedua local network menggunakan tunnel IPIP.
- Routing di Router1 :
 - **/ip route add dst-address=192.168.2.0/24 gateway=192.168.200.2**
- Routing di Router2 :
 - **/ip route add dst-address=192.168.1.0/24 gateway=192.168.200.1**



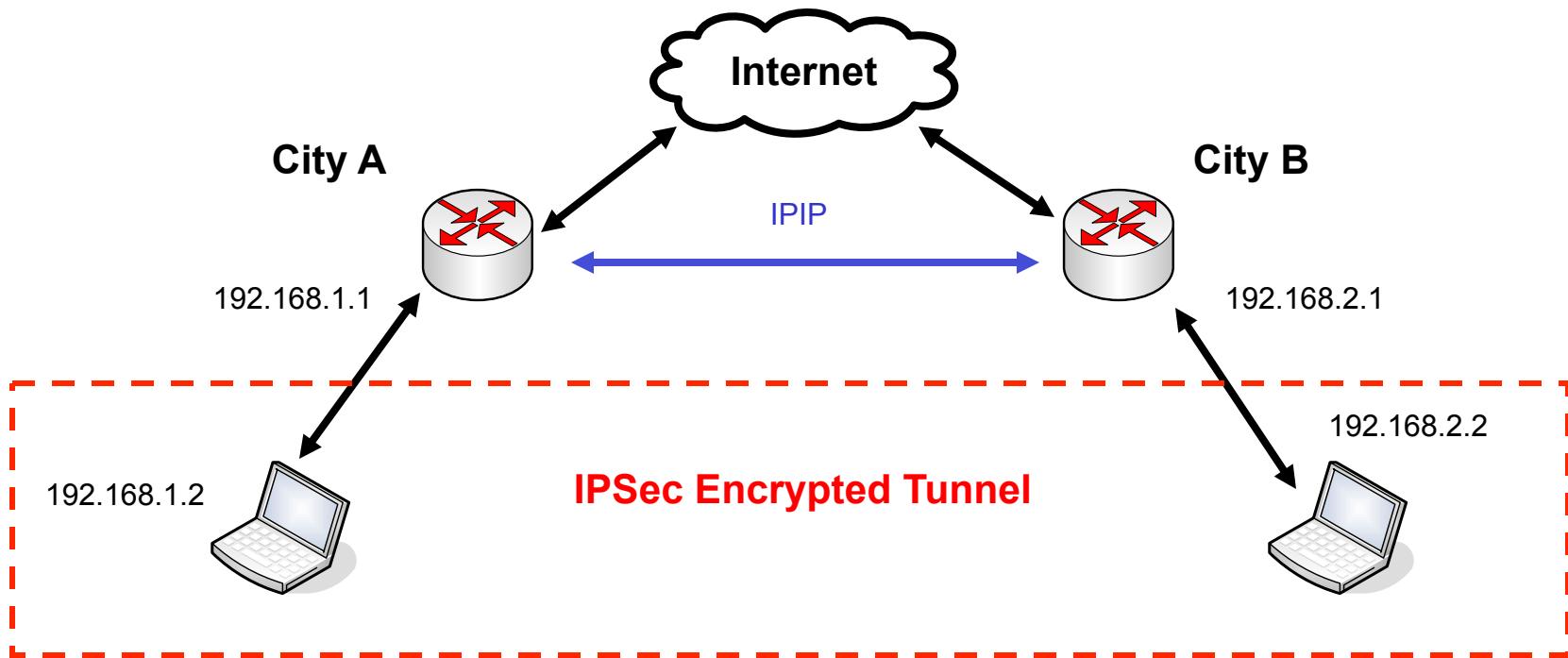
IP Security / VPN (IPSec)

- Protocol IPSec (IP Security) mampu mengimplementasikan security (Enkripsi) di komunikasi jaringan TCP/IP.
- Setiap traffic akan dilakukan 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.

IP Sec Example



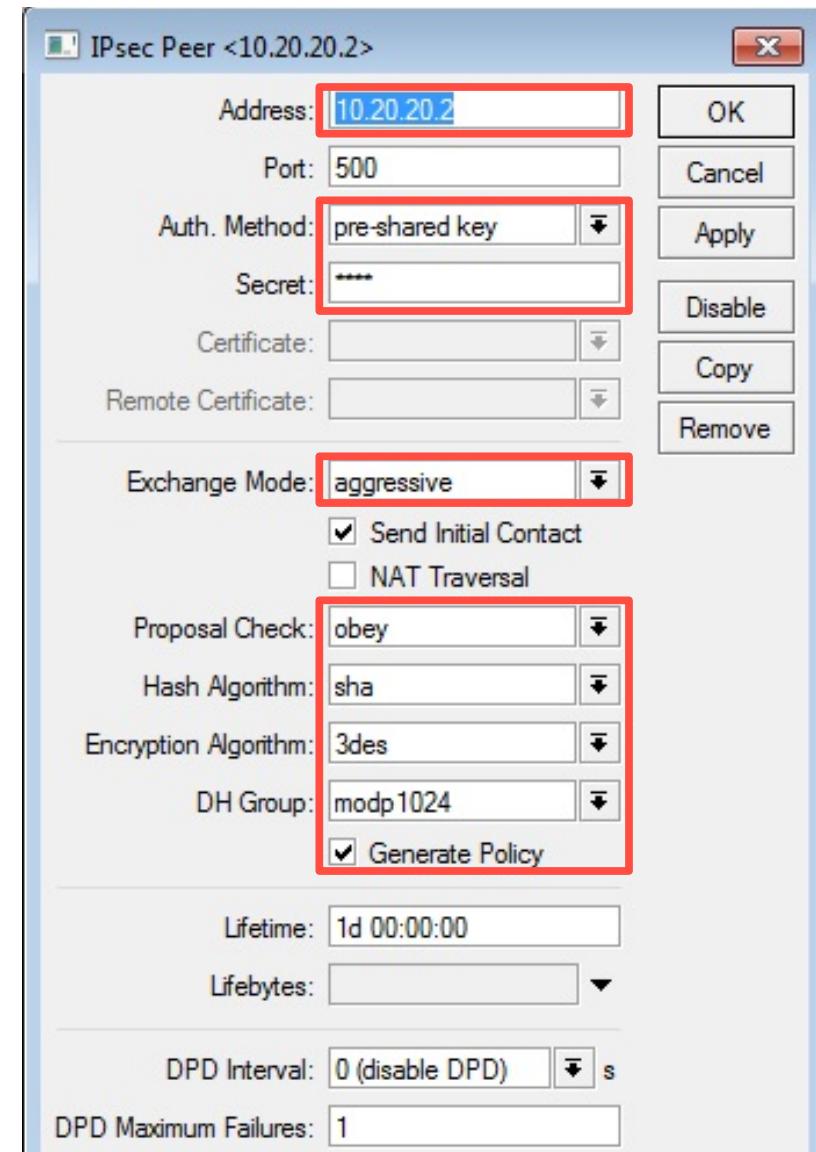
IPSec on Mikrotik



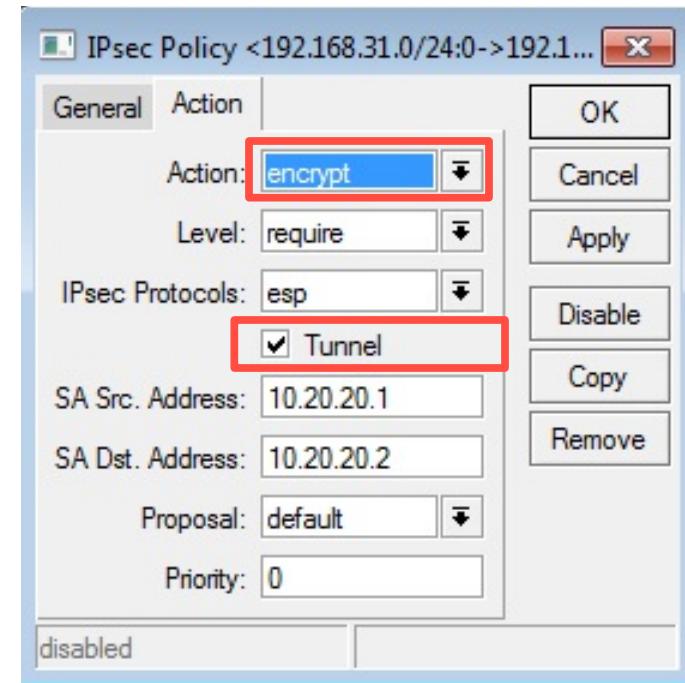
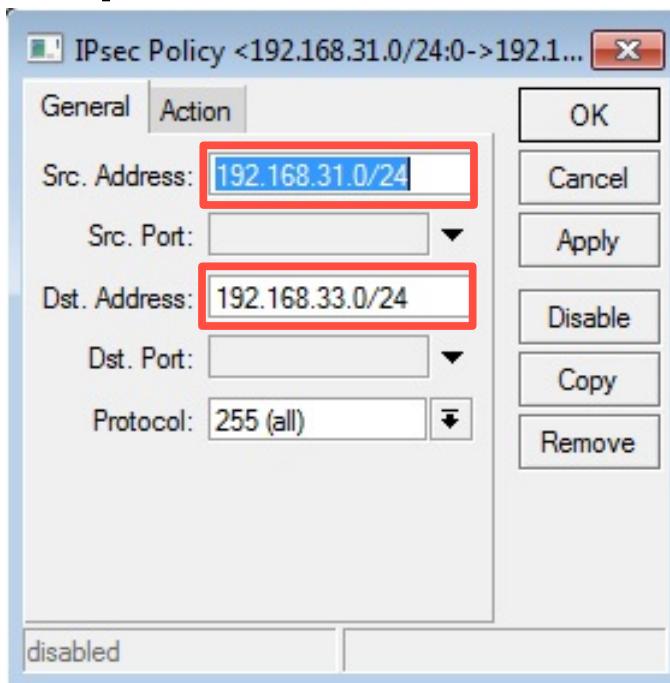
- Karena tunnel IPIP tidak memiliki proses security maka bisa ditambahkan tunnel IPSec untuk membuat tunnel tersebut menjadi secure.

IPSec Peer

- **Address** adalah parameter untuk menentukan peering router yaitu ip dari router lawan.
- **Auth-Method** adalah parameter untuk melakukan autentikasi antar dua router yang ingin meng-implementasikan IPSec.
- Beberapa parameter yang lain digunakan untuk menentukan metode enkripsi yang akan digunakan.

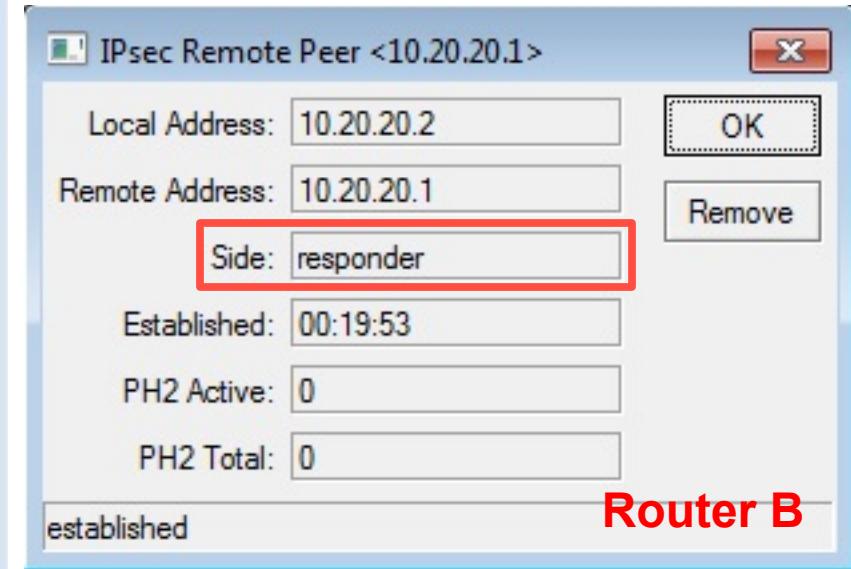
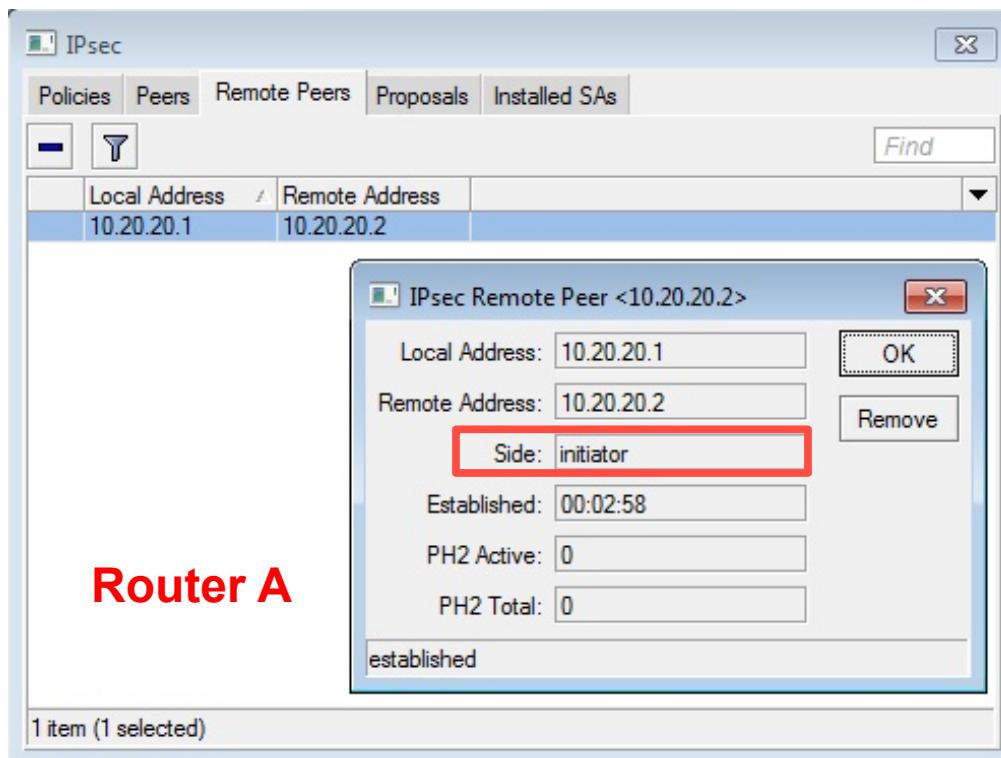


IPSec on Mikrotik



- Pada sisi Initiator akan menentukan traffic apa yang akan diaktifkan security.
- Pada ilustrasi di atas menunjukkan komunikasi dari **src-address=192.168.31.0/24** menuju **dst-address=192.168.33.0/24** akan diaktifkan enkripsi.

IPSec on Mikrotik



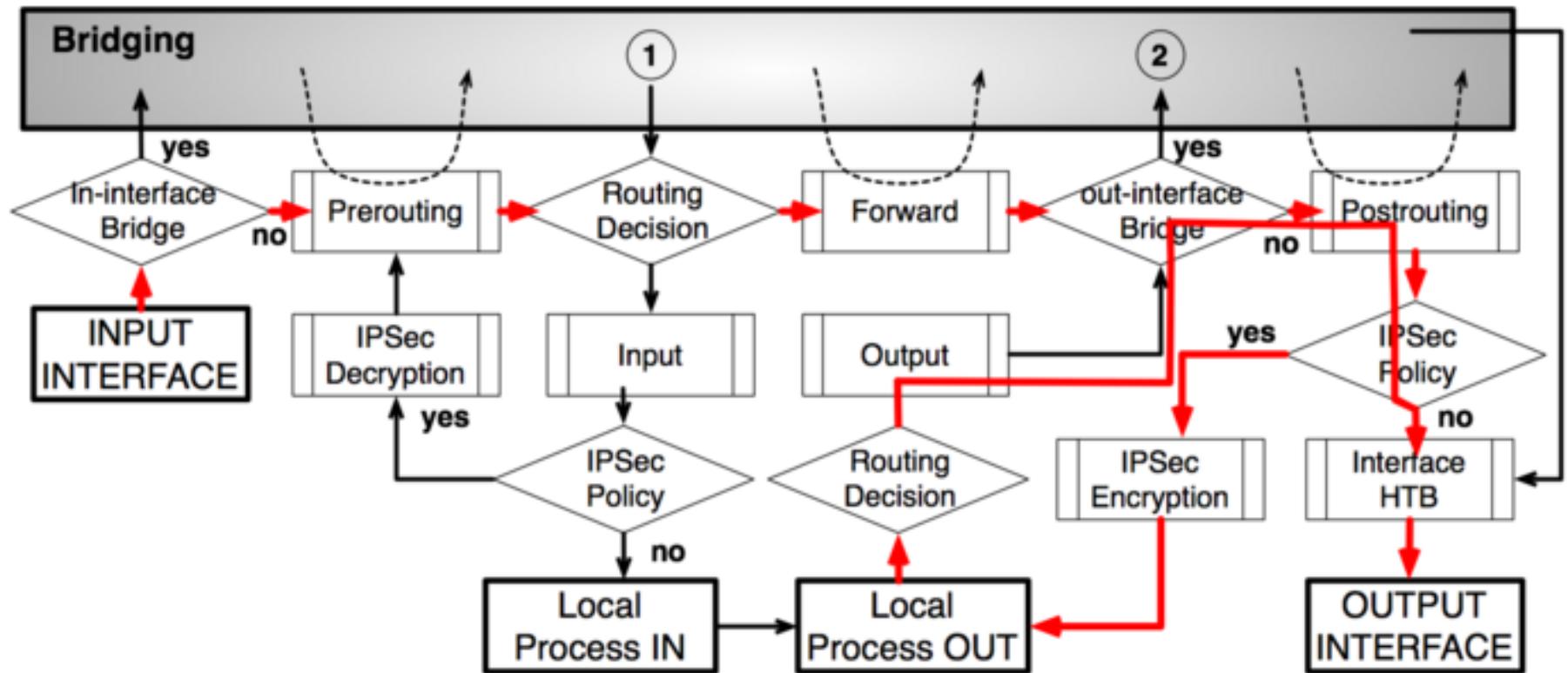
Policies	Peers	Remote Peers	Proposals	Installed SAs	Flush	Find
E	61b4e7b	10.20.20.2	10.20.20.1	Auth. Algorithm: md5	Encr. Algorithm: des	Current Bytes: 48768
E	f914856	10.20.20.1	10.20.20.2	Auth. Algorithm: md5	Encr. Algorithm: des	Current Bytes: 49024



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.

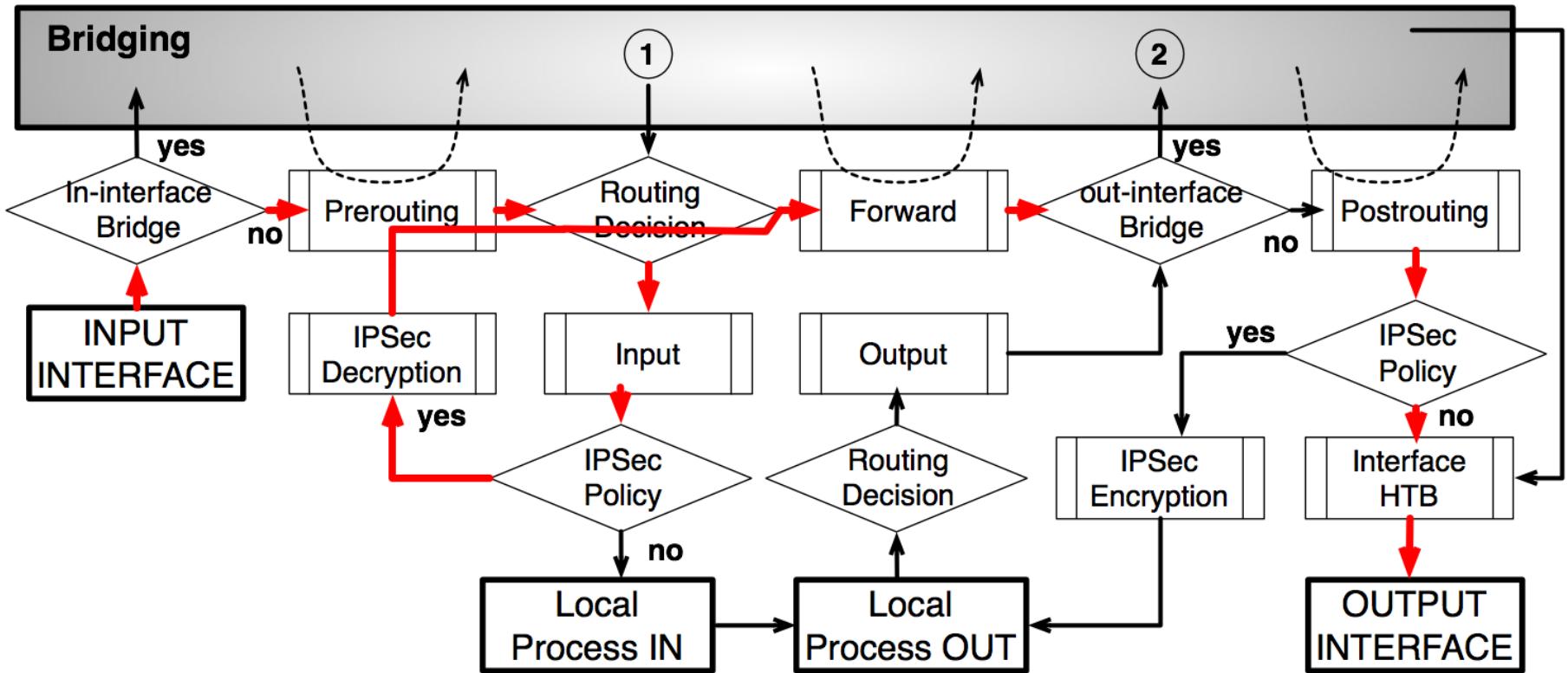
IPSec – Flow (encryption)



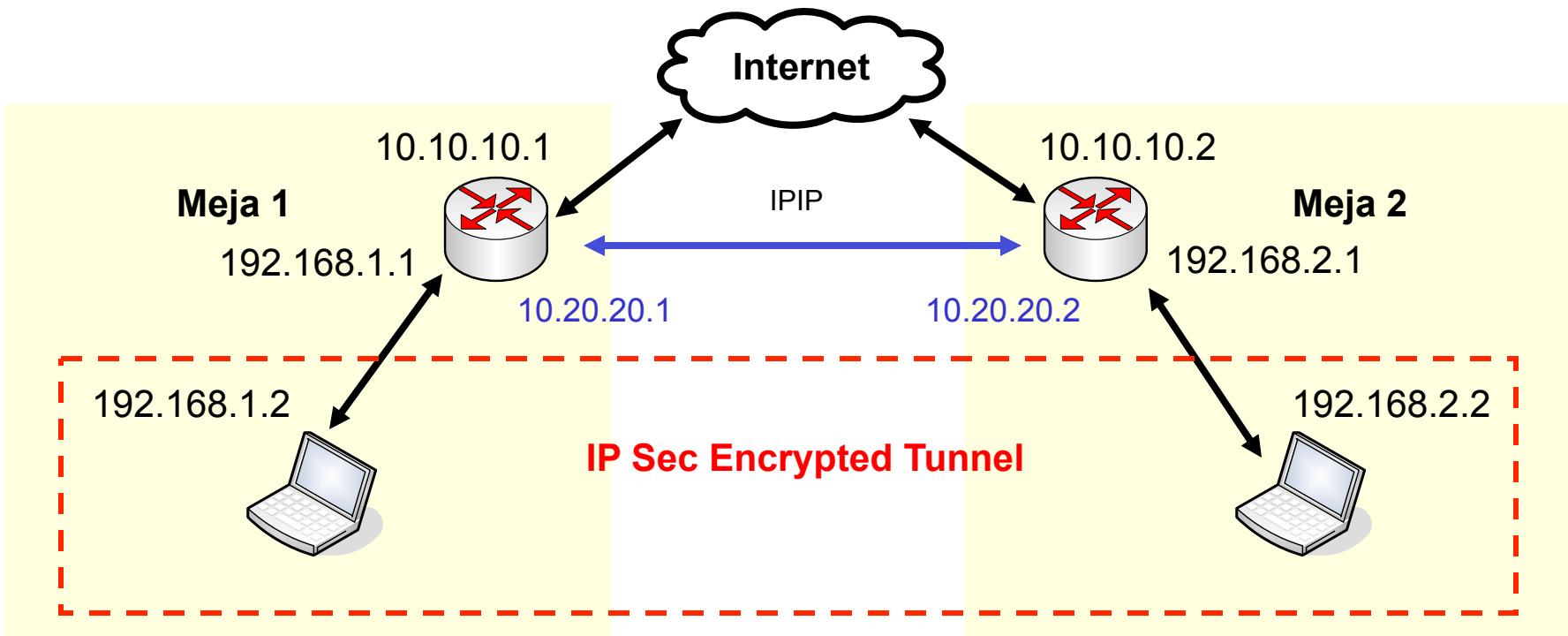
IPSec Decryption

- 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 – Flow (decryption)



[LAB-2] IPSec



- IPIP untuk menghubungkan kedua network
- IPSec untuk mengamankan tunnel IPIP

[LAB-2] IPSec - Peer

IPsec Peer <10.20.20.2>

Address:	10.20.20.2
Port:	500
Auth. Method:	pre-shared key
Secret:	****
Certificate:	
Remote Certificate:	
Exchange Mode:	aggressive
<input checked="" type="checkbox"/> Send Initial Contact	
<input type="checkbox"/> NAT Traversal	
Proposal Check:	obey
Hash Algorithm:	sha
Encryption Algorithm:	3des
DH Group:	modp1024
<input checked="" type="checkbox"/> Generate Policy	
Lifetime:	1d 00:00:00
Lifebytes:	
DPD Interval:	0 (disable DPD)
DPD Maximum Failures:	1
disabled	

Router 1

IPsec Peer <10.20.20.1>

Address:	10.20.20.1
Port:	500
Auth. Method:	pre-shared key
Secret:	test
Certificate:	
Remote Certificate:	
Exchange Mode:	aggressive
<input checked="" type="checkbox"/> Send Initial Contact	
<input type="checkbox"/> NAT Traversal	
Proposal Check:	obey
Hash Algorithm:	sha
Encryption Algorithm:	3des
DH Group:	modp1024
<input checked="" type="checkbox"/> Generate Policy	
Lifetime:	1d 00:00:00
Lifebytes:	
DPD Interval:	0 (disable DPD)
DPD Maximum Failures:	1
disabled	

Router 2

[LAB-2] Policy router Initiator

The image shows two windows for configuring IPsec Policies. Both windows have a title bar 'IPsec Policy <192.168.1.0/24:0->192.16...' and a close button.

Left Window (General Tab):

- Src. Address: 192.168.1.0/24
- Src. Port: (empty)
- Dst. Address: 192.168.2.0/24
- Dst. Port: (empty)
- Protocol: 255 (all)

Right Window (Action Tab):

- Action: encrypt
- Level: require
- IPsec Protocols: esp
- Tunnel
- SA Src. Address: 10.20.20.1
- SA Dst. Address: 10.20.20.2
- Proposal: default
- Priority: 0

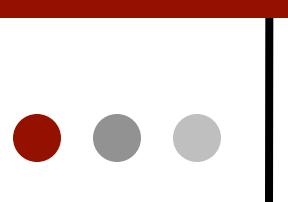
Both windows have 'OK', 'Cancel', 'Apply', 'Disable', 'Copy', and 'Remove' buttons on the right side. A 'disabled' status indicator is at the bottom of each window.

- Router 1 bertugas sebagai Initiator untuk menentukan Metode Enkripsi.



IPSec Performance

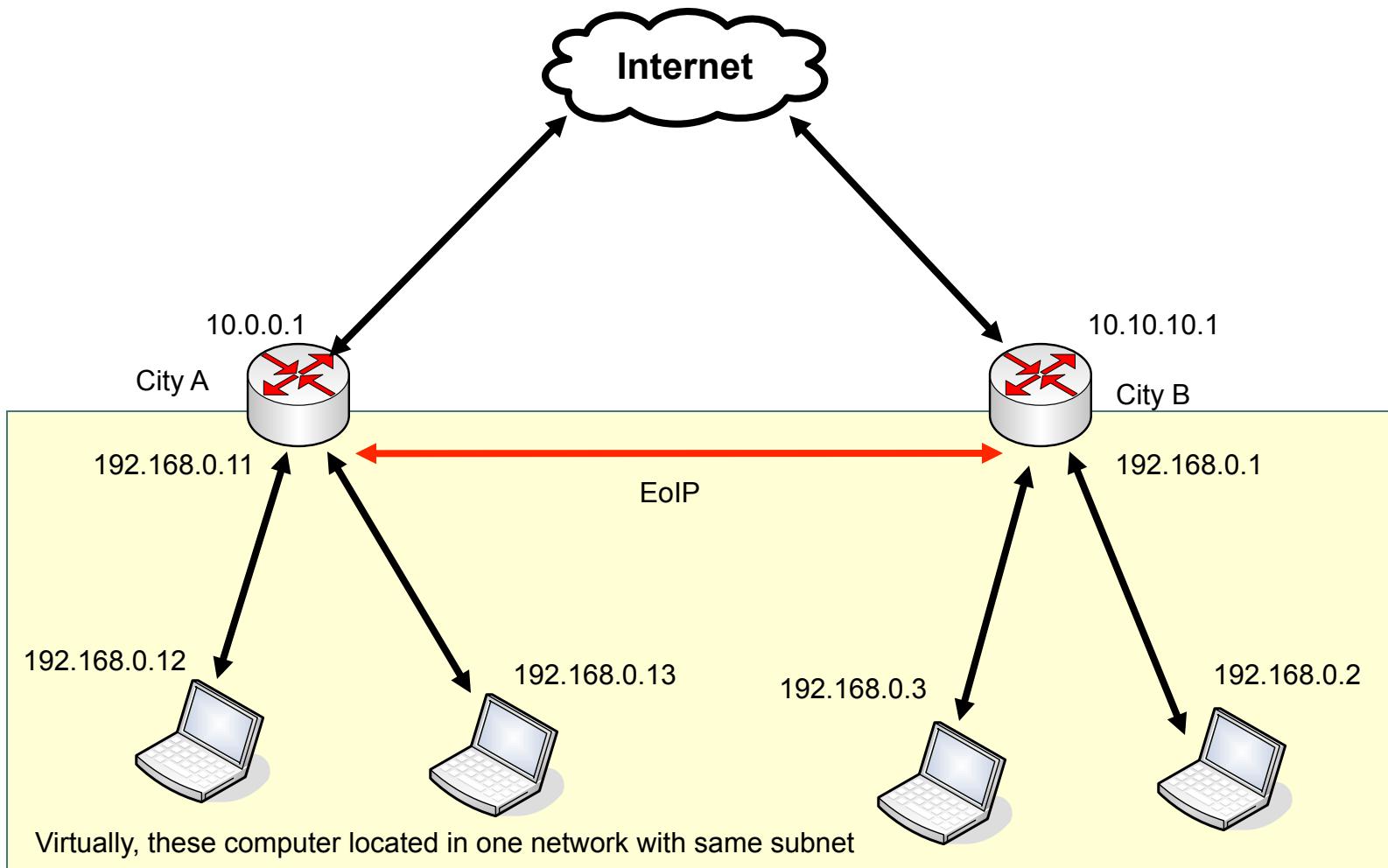
- Semakin besar processor mempengaruhi besar throughput yang bisa dilewatkan oleh IPSec.
- Dengan menggunakan produk Mikrobits, IPSec bisa di digenjot hingga lebih dari 100mbps:
 - Enkripsi **3DES** : 70 ~ 80 Mbps
 - Enkripsi **DES** : 100 ~ 150 Mbps
 - Enkripsi **AES** : 200 ~ 250 Mbps



Ethernet over IP (EoIP)

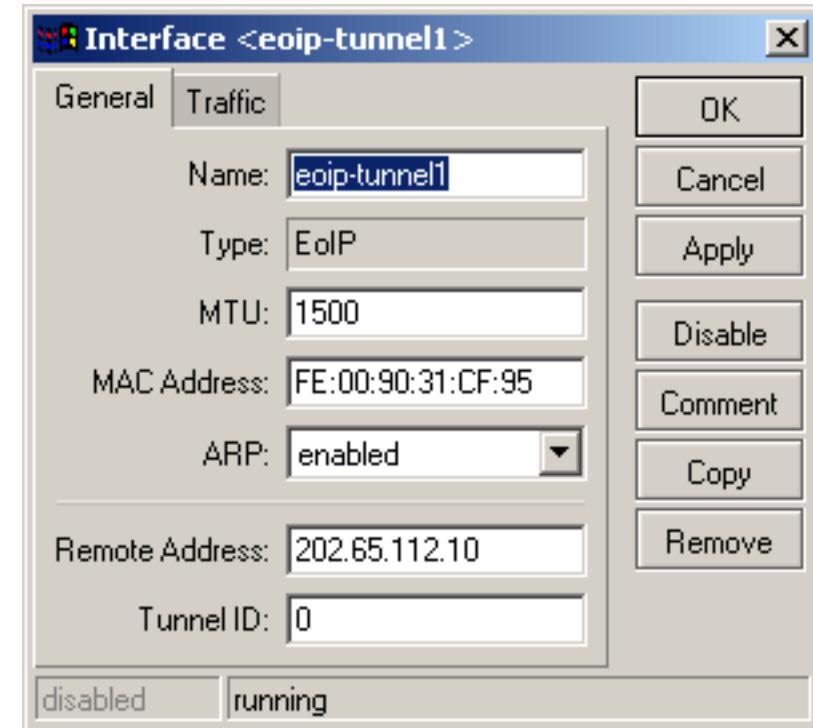
- EoIP Merupakan salah satu implementasi protocol IP Tunneling untuk komunikasi dua router di jaringan TCP/IP.
- Interface EoIP dianggap sebagai sebuah **Ethernet Interface** walaupun sebenarnya adalah Virtual Interface.
- Karena dianggap sebagai Ethernet interface maka Interface EoIP dapat diimplementasikan pada Routed dan **Bridged** network.
- Menggunakan Protocol **GRE/47** (RFC1701).

EoIP Example



EoIP Configuration

- Parameter **Remote-Address** adalah parameter ip address dari Router lawan.
- Tunnel-ID adalah parameter identitas dari koneksi tunnel.
- Jika ingin membangun sebuah tunnel melewati jaringan WAN atau Internet maka gunakan IP public untuk parameter Remote-Address.
- Pastikan Tunnel ID yang berbeda di tiap tunnel interface pada satu router.

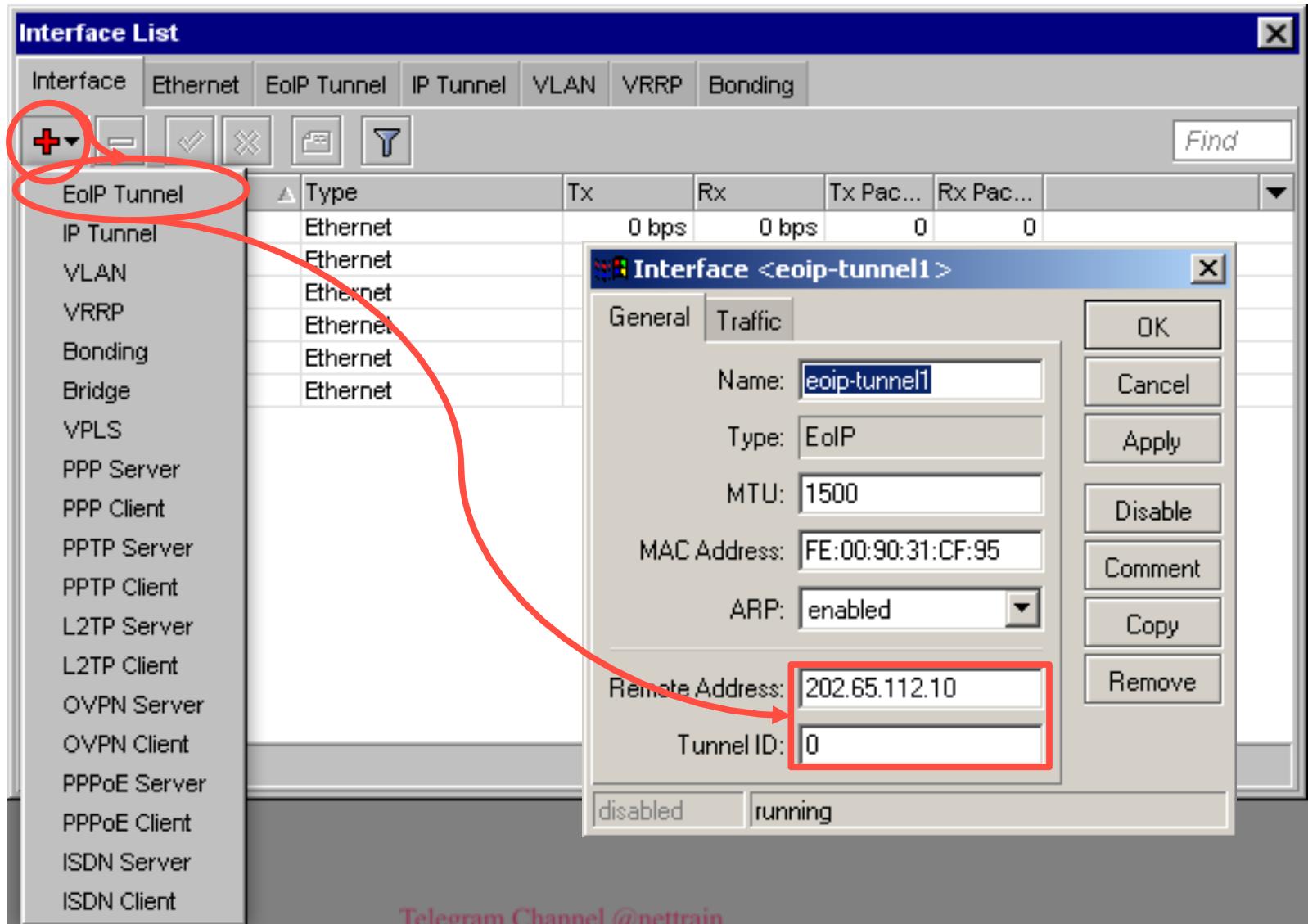


EoIP Packet Header

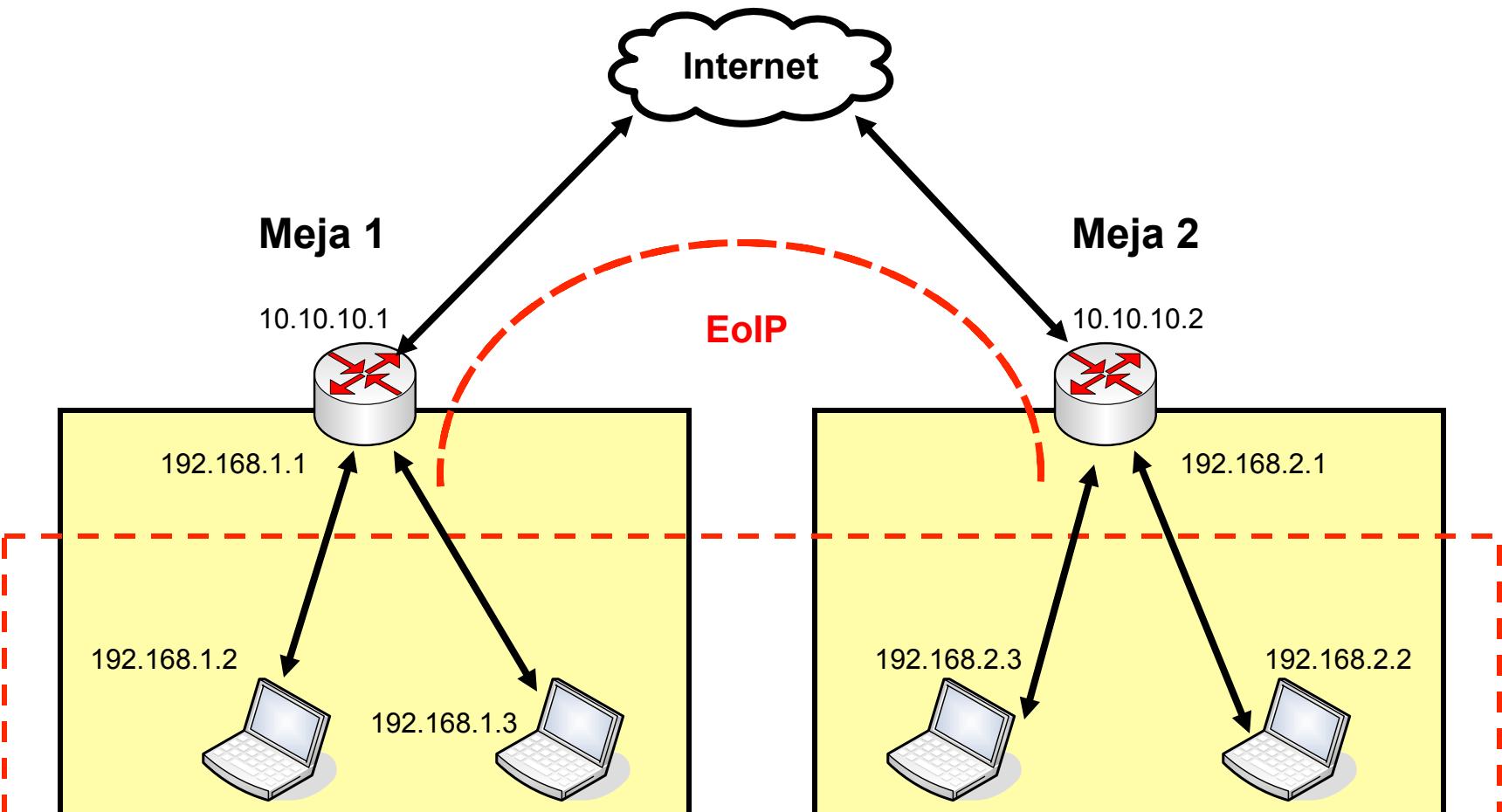
Packet Sniffer								
Packets	Connections	Hosts	Protocols					
Packet Sniffer Settings								
Time (s)	Interface	Direction	Src. Address	▼	Dst. Address	Protocol	IP Protocol	▲ Size
1.137	ether1	in	68.142.233.163:443		192.168.5.29:3662	2048 (ip)	6 (tcp)	60
3.028	ether1	in	192.168.5.1		192.168.5.29	2048 (ip)	47	84
3.041	ether1	in	192.168.5.1		192.168.5.29	2048 (ip)	47	116
4.034	ether1	in	192.168.5.1		192.168.5.29	2048 (ip)	47	116
5.035	ether1	in	192.168.5.1		192.168.5.29	2048 (ip)	47	116
6.036	ether1	in	192.168.5.1		192.168.5.29	2048 (ip)	47	116
3.027	ether1	out	192.168.5.29		192.168.5.1	2048 (ip)	47	84
3.028	ether1	out	192.168.5.29		192.168.5.1	2048 (ip)	47	116
4.023	ether1	out	192.168.5.29		192.168.5.1	2048 (ip)	47	116
5.024	ether1	out	192.168.5.29		192.168.5.1	2048 (ip)	47	116
6.025	ether1	out	192.168.5.29		192.168.5.1	2048 (ip)	47	116
0.718	ether1	out	192.168.5.29:3662		68.142.233.163:443	2048 (ip)	6 (tcp)	138
0.371	ether1	out	192.168.5.29:4021		203.84.158.50:80	2048 (ip)	6 (tcp)	1338
0.514	ether1	out	192.168.5.29:4021		203.84.158.50:80	2048 (ip)	6 (tcp)	54
0.372	ether1	in	203.84.158.50:80		192.168.5.29:4021	2048 (ip)	6 (tcp)	60
0.409	ether1	in	203.84.158.50:80		192.168.5.29:4021	2048 (ip)	6 (tcp)	341

- Test packet sniffer menunjukkan bahwa Tunnel EOIP membutuhkan sekitar 80-116 byte di tiap packet data per traffincnya.

EoIP Configuration

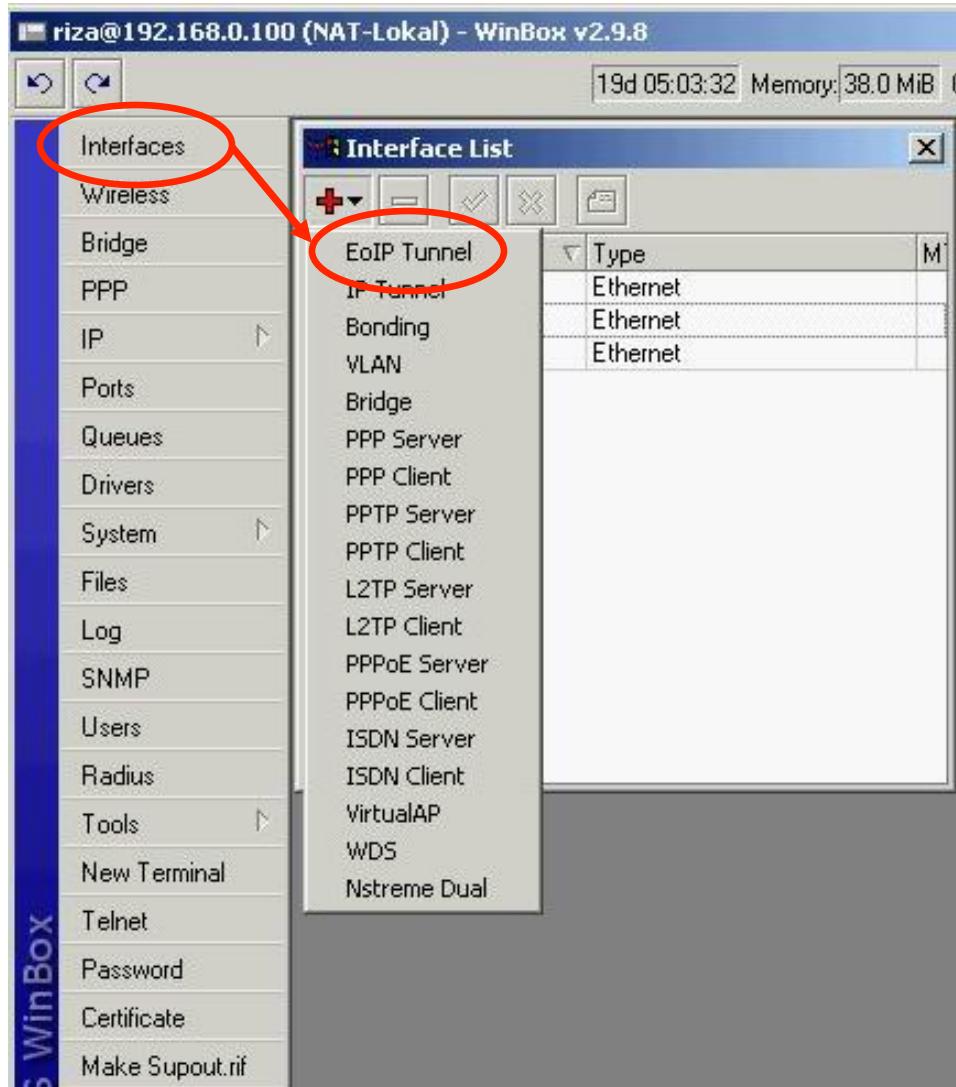


[LAB-3] EoIP Tunnels



Virtually, these computer located in one network with same subnet

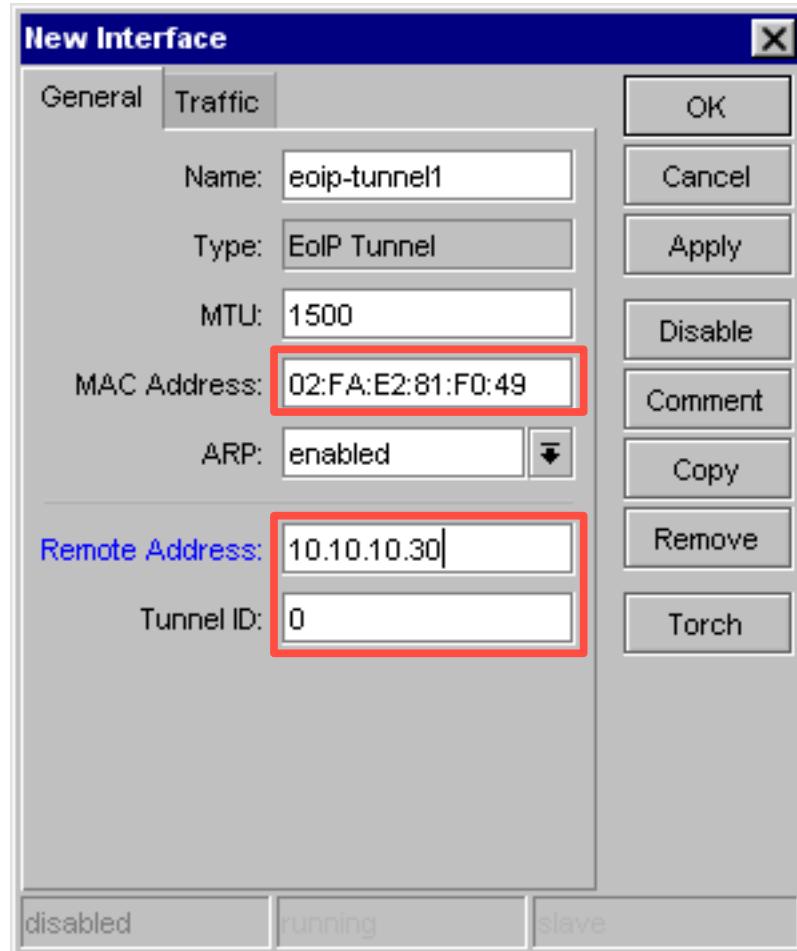
[LAB-3] EoIP Tunnels



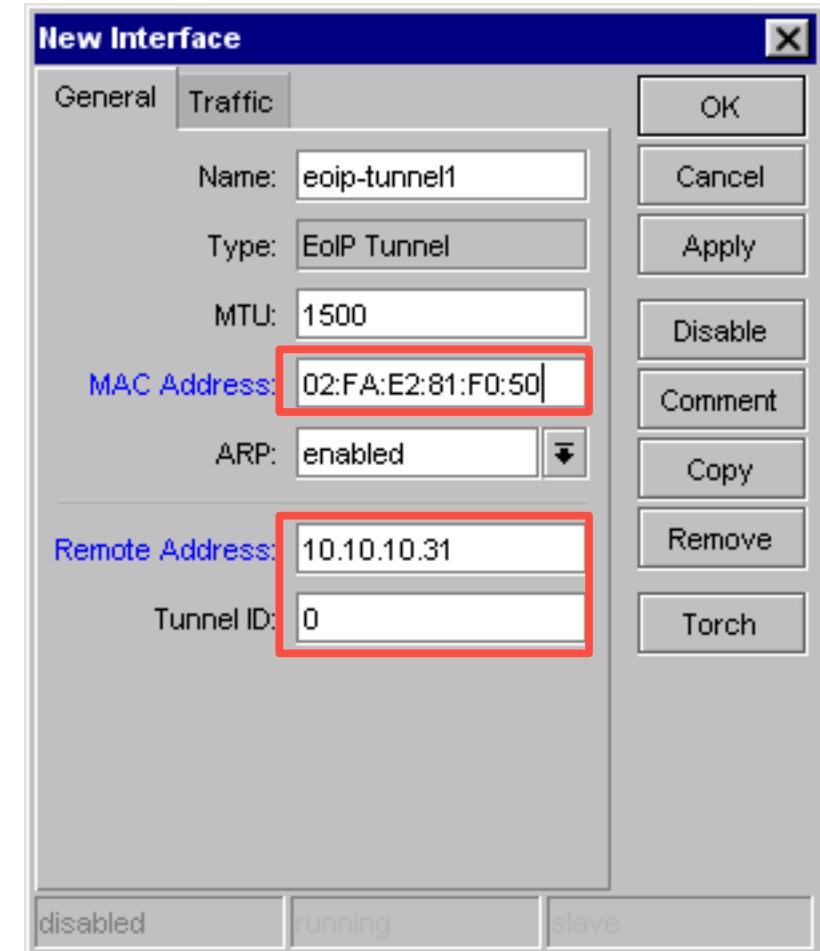
- Buat Interface EoIP baru dari menu interface.
- Buat ip address satu segmen untuk kedua interface EoIP di kedua router.
- Test ping pada kedua router menggunakan ip yang ada di interface EoIP.
- Jika reply maka tunnel EoIP sudah siap untuk digunakan pada routing maupun bridge network.

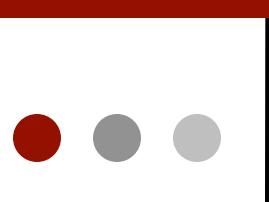
[LAB-3] EoIP Tunnels

ROUTER A



ROUTER B





Virtual LAN (VLAN) 1

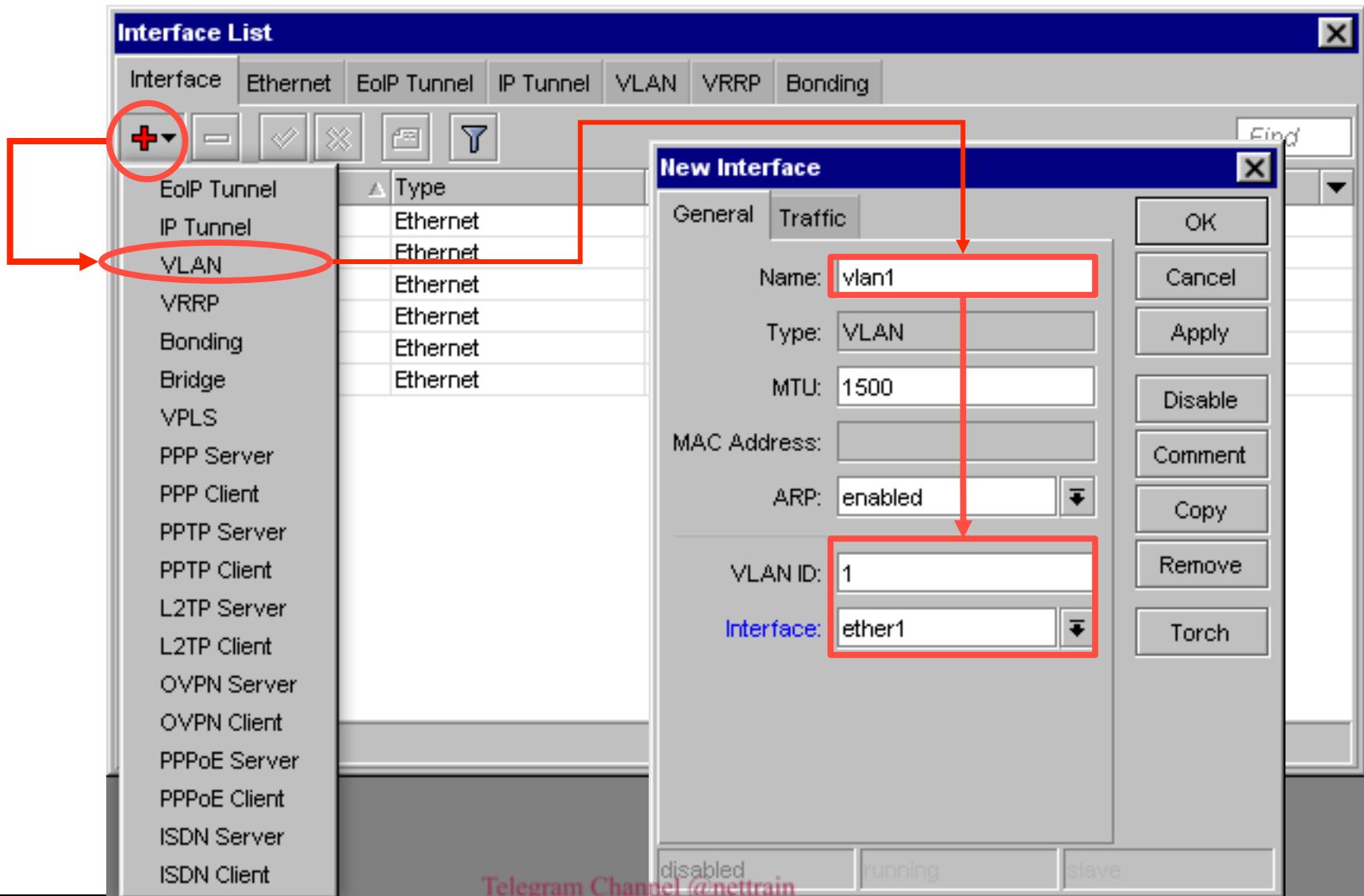
- VLAN adalah sebuah logical group (pengelompokan) yang memungkinkan user untuk berkomunikasi dengan user yang lain tetapi terisolasi dari user lain yang berbeda group walaupun sebenarnya user-user ini masih terhubung secara fisik.
- Dengan menggunakan protocol Vlan Router dapat meningkatkan security dan management yang berbeda terhadap jaringan walaupun masih ada sharing media fisik.
- Bekerja di layer DataLink



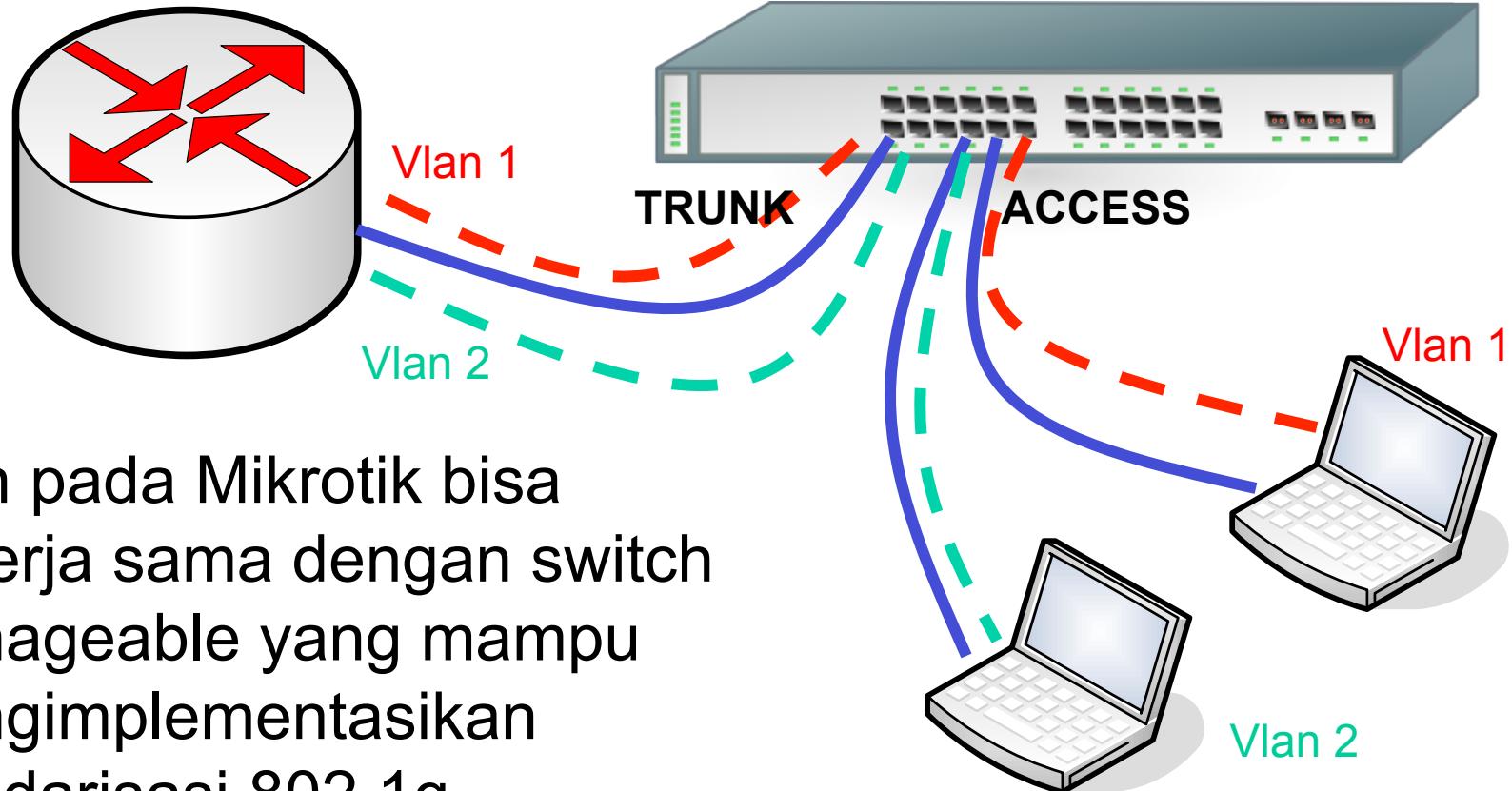
Virtual LAN (VLAN) 2

- VLAN di Mikrotik RouterOS merupakan implementasi dari standarisasi 802.1Q. Dengan menggunakan metode VLAN ini Mikrotik RouterOS memungkinkan membangun beberapa Virtual LAN untuk memisahkan jaringan (group) di sebuah **interface ethernet** atau **wireless**.
- Mikrotik RouterOS mampu membangun **4095** Interface Vlan di sebuah Interface ethernet, banyak router termasuk CISCO, Linux dan Leyer2 Switch yang sudah mendukukng protocol ini.

VLAN Configuration

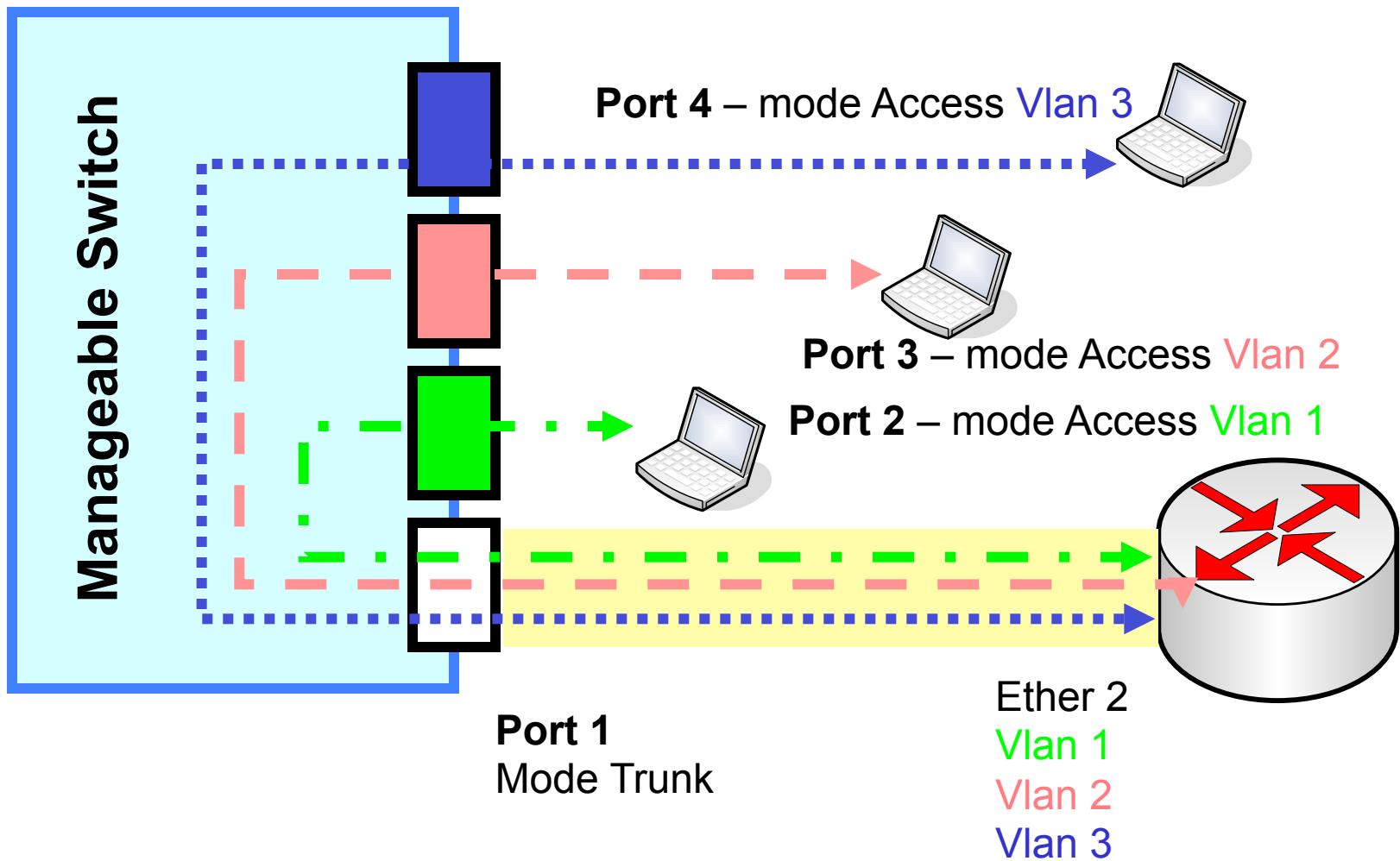


Mikrotik Vlan on Manageable Switch



- Vlan pada Mikrotik bisa bekerja sama dengan switch manageable yang mampu mengimplementasikan standarisasi 802.1q.

Mikrotik Vlan on Manageable Switch



Vlan Implementation using RB250GS



Detail Config : http://www.mikrotik.co.id/artikel_lihat.php?id=36

Mikrotik Vlan on CISCO Switch

The image shows a dual-pane interface. On the left is a terminal window titled '192.168.200.2 - PuTTY' displaying configuration commands for a Mikrotik router. On the right is a 'Interface List' window from a Cisco Switch, showing the status of various ports.

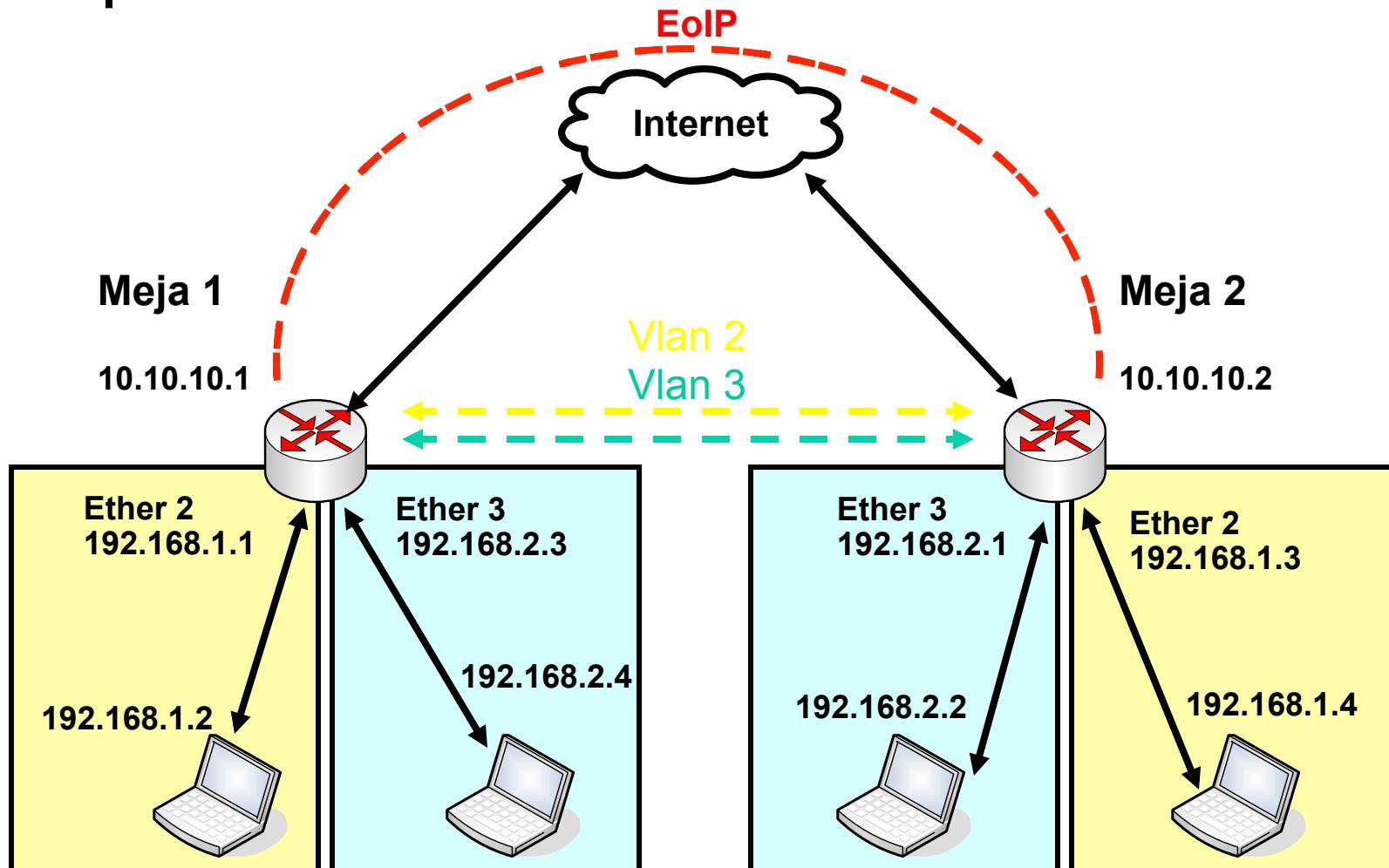
Mikrotik Configuration (Terminal Left):

```
interface FastEthernet0/18
switchport access vlan 3
!
interface FastEthernet0/19
switchport access vlan 3
!
interface FastEthernet0/20
switchport access vlan 3
!
interface FastEthernet0/21
switchport access vlan 2
!
interface FastEthernet0/22
switchport access vlan 2
!
interface FastEthernet0/23
switchport access vlan 2
!
interface FastEthernet0/24
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface VLAN1
ip address 192.168.200.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
!
--More--
```

Cisco Switch Interface List (Window Right):

	Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops
::: local network								
R	ether2	Ethernet	1522	2.1 Mbps	2.0 Mbps	197	199	0
R	vlan1	VLAN	1518	0 bps	0 bps	0	0	0
::: vlan 2 - public network								
R	vlan2	VLAN	1518	0 bps	0 bps	0	0	0
::: vlan local network								
R	vlan3	VLAN	1518	2.1 Mbps	2.0 Mbps	197	199	0
	ether3	Ethernet	1522	0 bps	0 bps	0	0	0
	ether4	Ethernet	1522	0 bps	0 bps	0	0	0
	ether5	Ethernet	1522	0 bps	0 bps	0	0	0
	ether6	Ethernet	1522	0 bps	0 bps	0	0	0
	ether7	Ethernet	1522	0 bps	0 bps	0	0	0
	ether8	Ethernet	1522	0 bps	0 bps	0	0	0
	ether9	Ethernet	1522	0 bps	0 bps	0	0	0

[LAB-4] Mikrotik Vlan Trunking



Bridge 1 port:
Vlan2 & ether 2

Bridge 2 port:
Vlan3 & ether 3

Bridge 1 port:
Vlan3 & ether 3

Bridge 2 port:
Vlan2 & ether 2

[LAB-4] Create VLAN Interface

General | Traffic

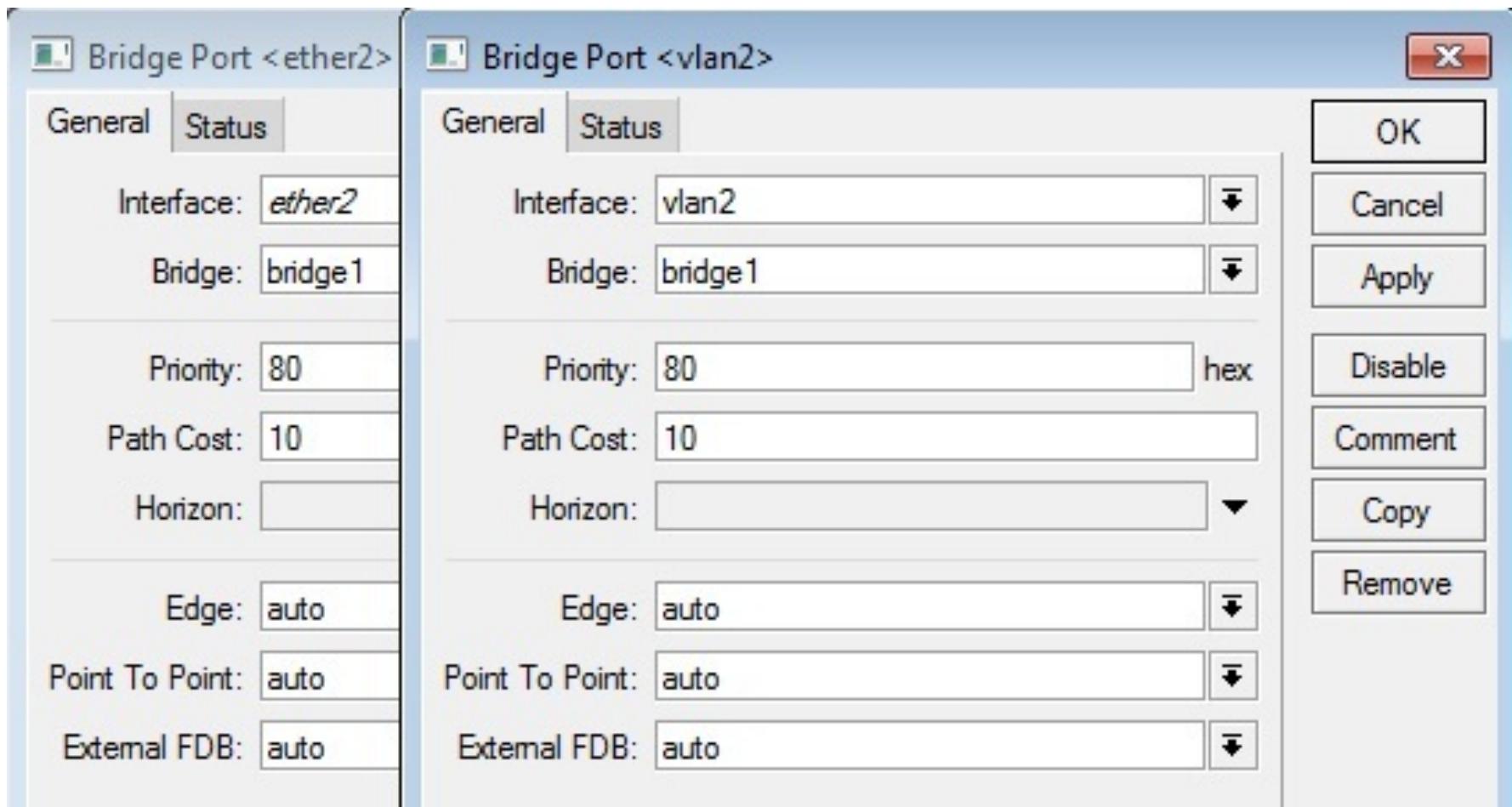
Name:	vlan2
Type:	VLAN
MTU:	1500
L2 MTU:	65531
MAC Address:	02:30:81:24:AA:B8
ARP:	enabled
VLAN ID:	2
Interface:	eoip-tunnel1
<input type="checkbox"/> User Service Tag	

General | Traffic

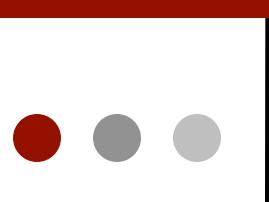
Name:	vlan3
Type:	VLAN
MTU:	1500
L2 MTU:	65531
MAC Address:	02:30:81:24:AA:B8
ARP:	enabled
VLAN ID:	3
Interface:	eoip-tunnel1
<input type="checkbox"/> User Service Tag	

- Membangun vlan interface (trunking) memanfaatkan EoIP Tunnel

[LAB-4] Create VLAN Interface



- Menggabungkan Vlan (Access) antara ether 2 dan 3 dengan vlan 2 dan vlan 3 ke dalam bridge yang terpisah.

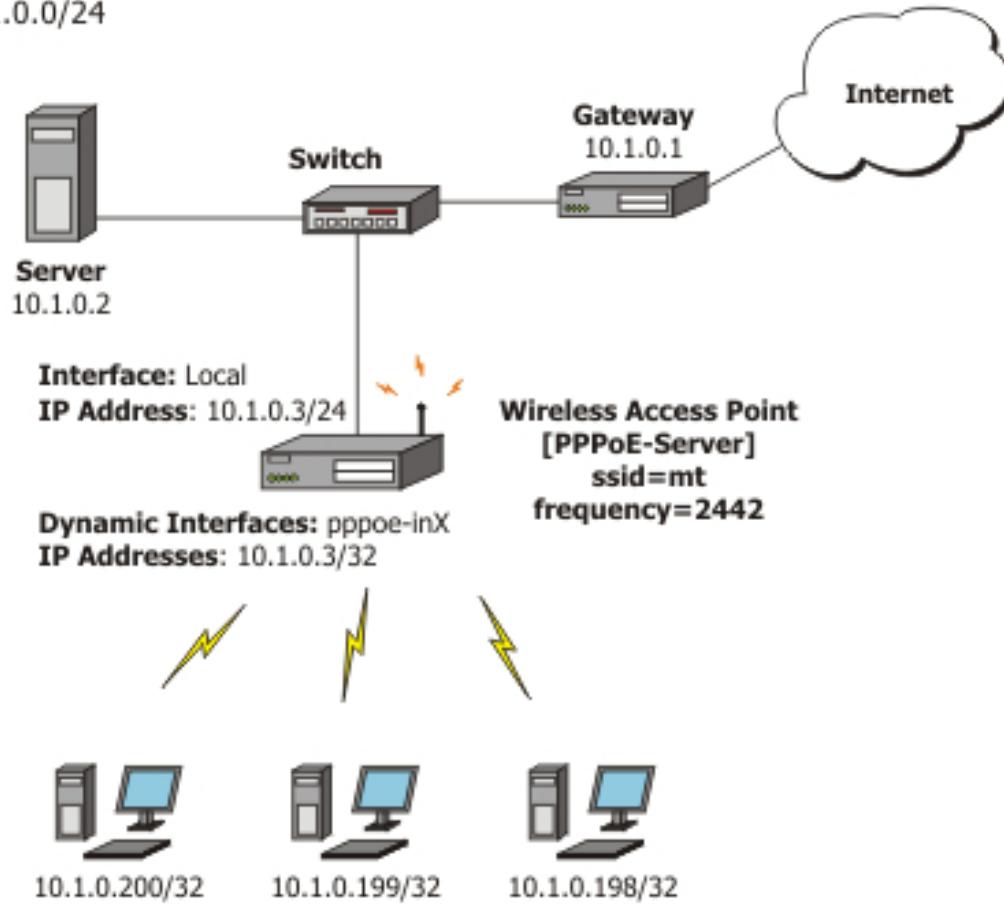


Point to Point Protocol over Ethernet (PPPoE) (1)

- PPPoE adalah salah satu metode implementasi Protocol PPP atau VPN, Hampir sama dengan protocol VPN yang lain (PPTP,L2TP,OpenVPN)
PPPoE menambahkan fungsi accounting dan management user.
- PPPoE biasa digunakan oleh ISP untuk mengontrol koneksi xDSL, cable modem atau bisa juga di Ethernet cable.
- Keunikan dari PPPoE ini adalah menggunakan standard yang berbeda pada protocol PPP yaitu menggunakan metode transport ethernet.
- Support RADIUS authentication.

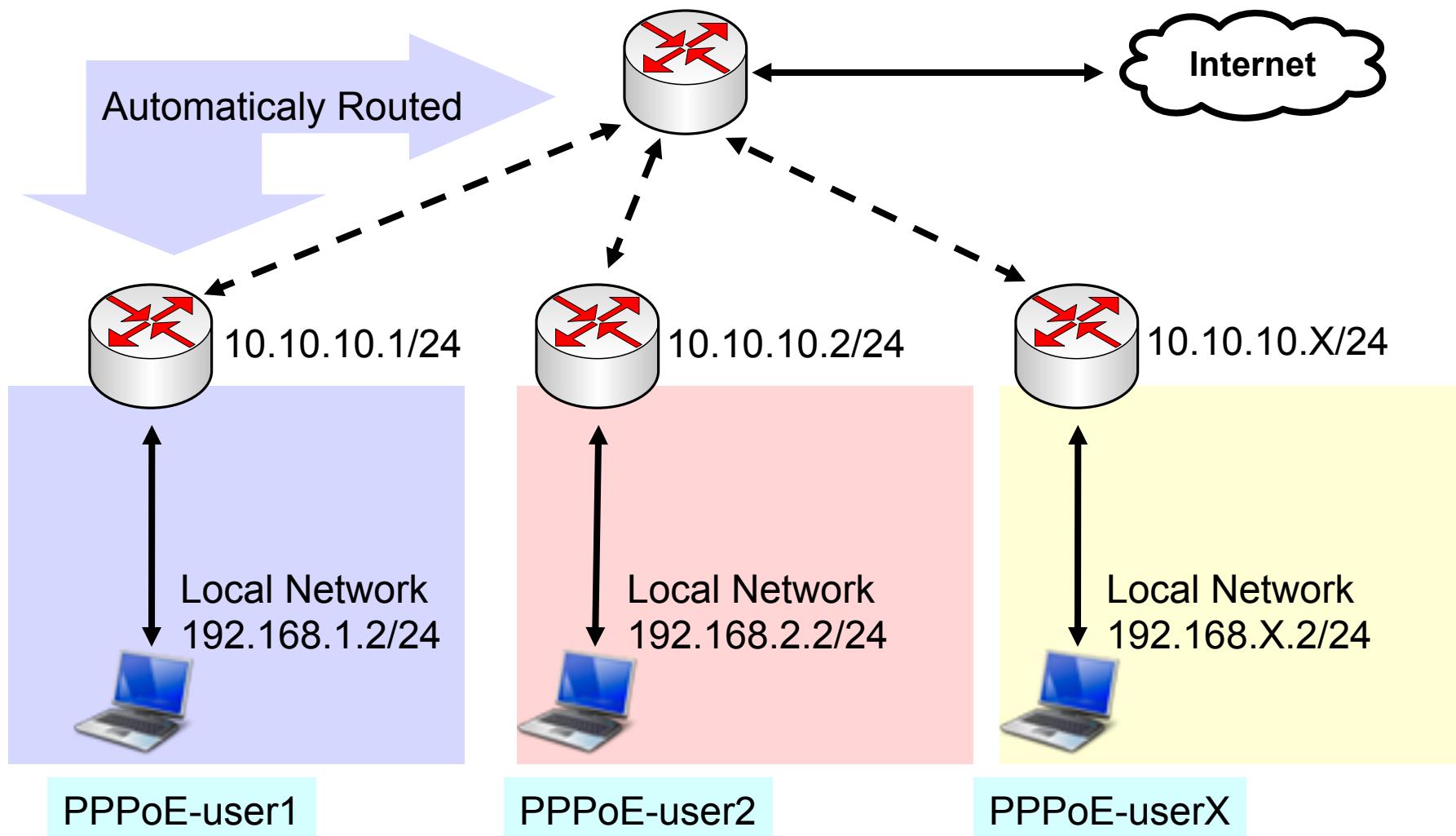
PPPoE Example

Network:
10.1.0.0/24

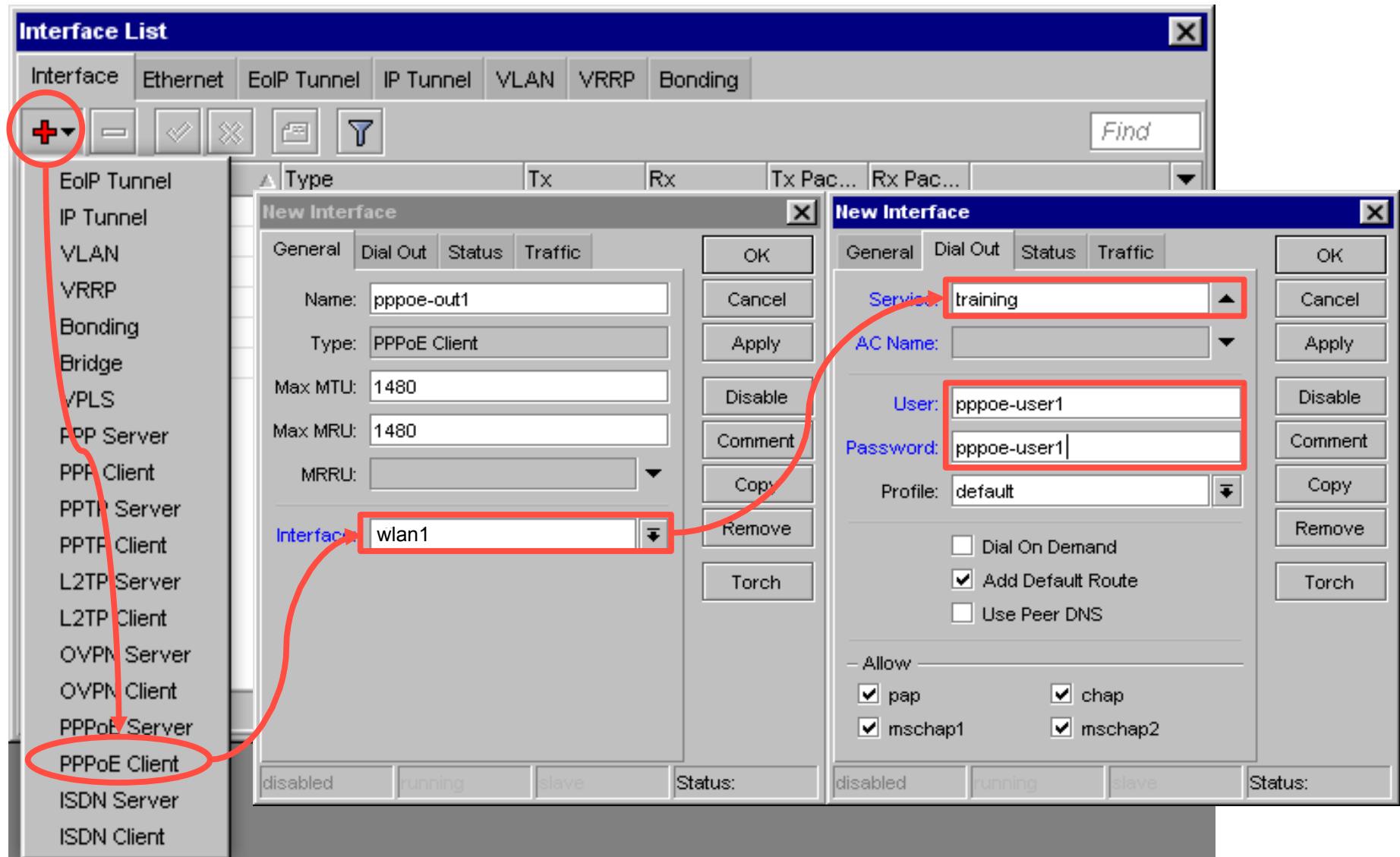


Wireless PPPoE Clients (address range 10.1.0.100-10.1.0.200)

[LAB-5] PPPoE Tunnels - Client

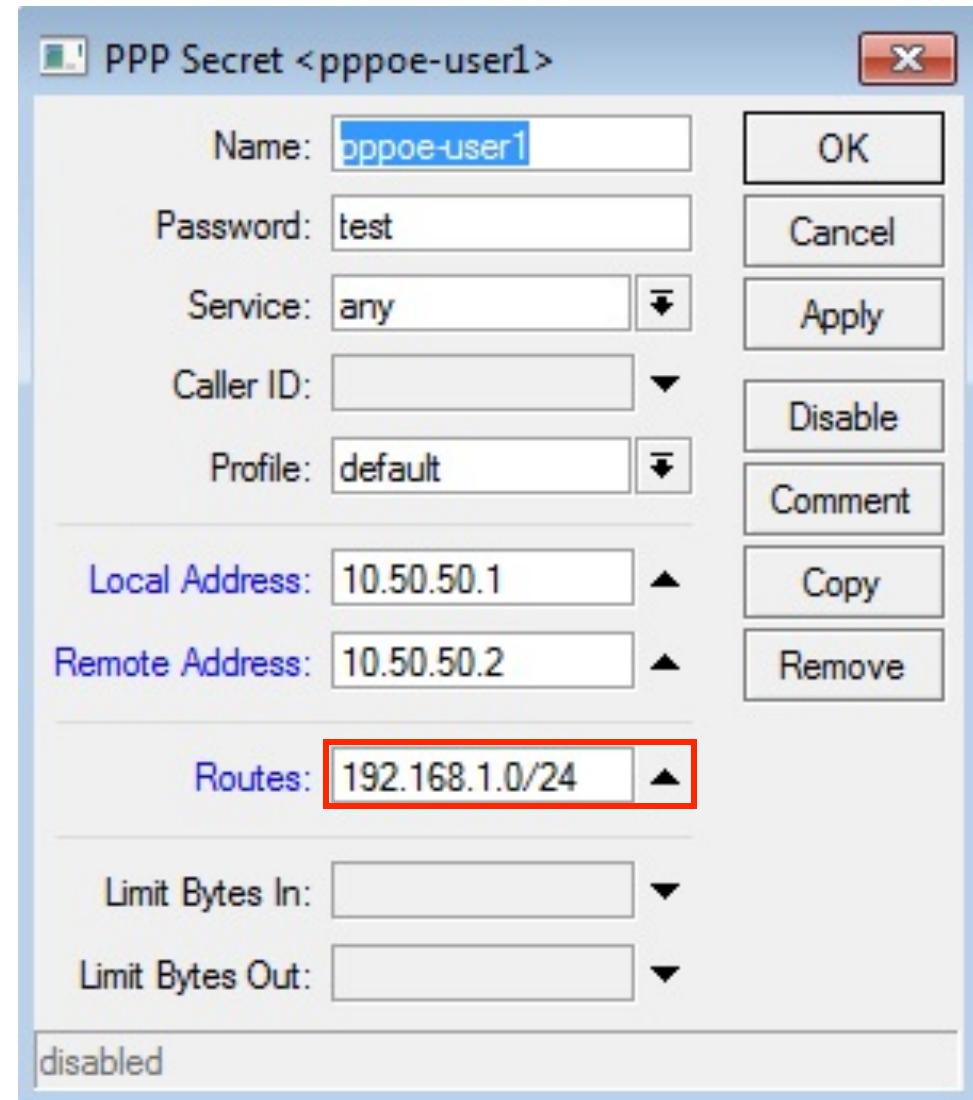


[LAB-5] PPPoE Tunnels - Client



PPP Secret – Routing Injection

- Network yang akan di advertise secara otomatis menggunakan PPP protocol di konfigurasi di parameter **Routes**.
- Network yang diadvertise bisa lebih dari satu network dipisahkan menggunakan tanda koma (,).



● ● ● | PPPoE – Routing Dynamic

The image shows two windows from the MikroTik Winbox interface. On the left is the 'Route List' window, which displays a table of routes. A row for 'DAS' with a destination of '192.168.1.0/24' and a gateway of '10.50.50.2' is selected. On the right is a detailed 'Route <192.168.1.0/24>' configuration window. The 'General' tab is selected. The 'Destination' field is set to '192.168.1.0/24'. The 'Gateway' field is set to '10.50.50.2'. The 'Interface' field is highlighted with a red box and contains the value '<pppoe-pppoe-user1>'. Other fields include 'Check Gateway' (empty), 'Type' (unicast), 'Distance' (1), 'Scope' (30), 'Target Scope' (10), 'Routing Mark' (empty), and 'Pref. Source' (empty). At the bottom, tabs for 'dynamic', 'active', and 'static' are visible.

	Destination	Gateway	Gatew...
DAb	► 192.168.0.0/24	172.16.30.1	
XS	► 0.0.0.0/0	172.16.20.1	
AS	► 239.0.255.9	172.16.20.1	
DAS	► 192.168.1.0/24	10.50.50.2	
XS	► 202.65.114.16	10.10.78.245	
XS	► 0.0.0.0/0	10.10.78.245	
AS	► 0.0.0.0/0	10.10.78.245	
DAC	► 10.50.50.2		
DAC	► 10.10.78.244/30		
DAC	► 192.168.4.0/24		
DAC	► 172.16.20.0/30		
DAC	► 172.16.30.0/30		
DAC	► 117.20.50.240/29		
DAC	► 203.84.154.32/30		
DAC	► 10.5.51.0/24		

Route List

Routes Rules

OK

Copy

Remove

Route <192.168.1.0/24>

General Attributes

Destination: 192.168.1.0/24

Gateway: 10.50.50.2

Gateway Interface:

Interface: <pppoe-pppoe-user1>

Check Gateway:

Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

dynamic active static

24 items (1 selected)



OSPF

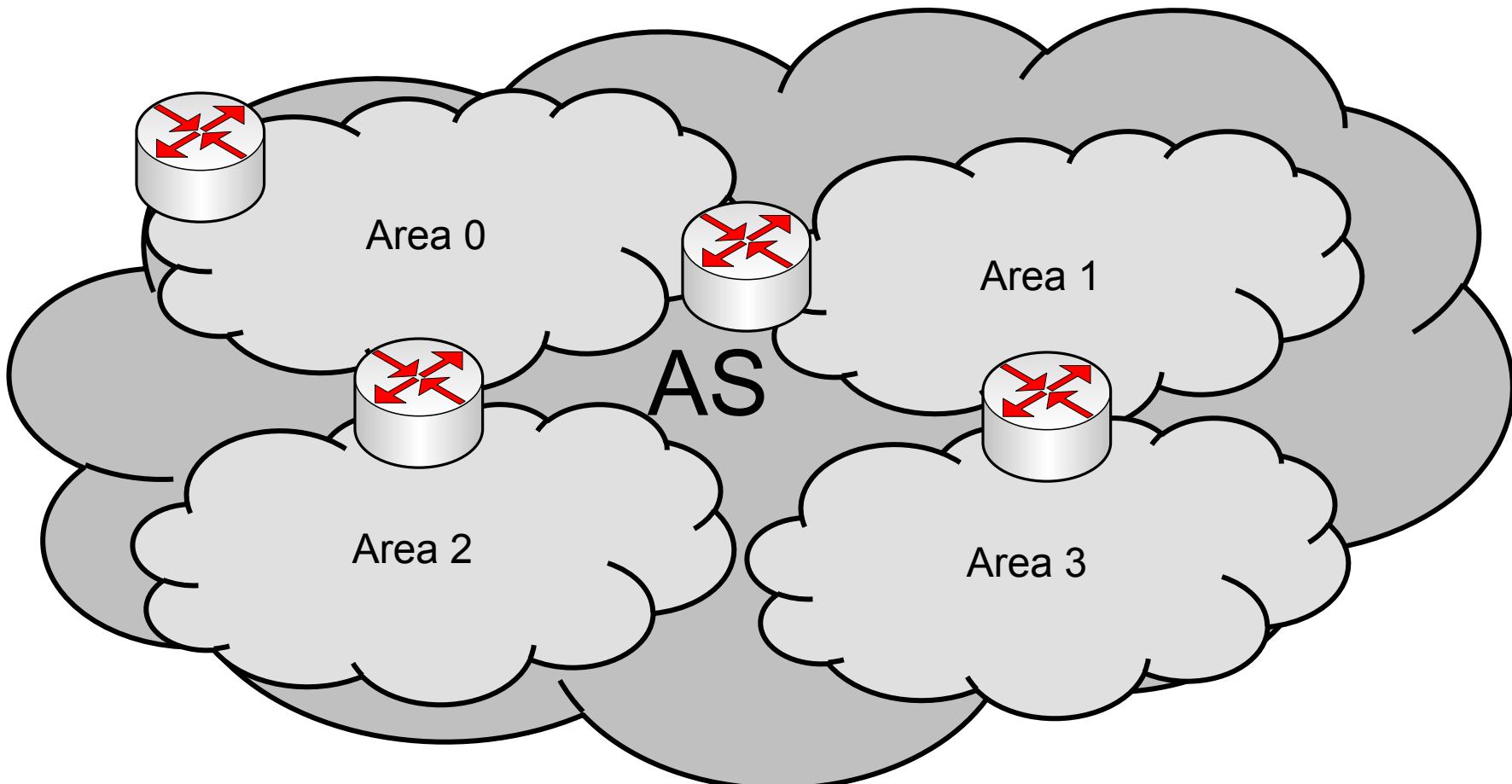


Certified Mikrotik Training Advanced Class (MTCRE)

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner

Autonomous System



Autonomous System (AS) adalah sebuah gabungan dari beberapa jaringan yang sifatnya routing dan memiliki kesamaan metode serta policy pengaturan network, yang semuanya dikendalikan oleh sebuah network operator.

Telegram Channel @nettrain



Background

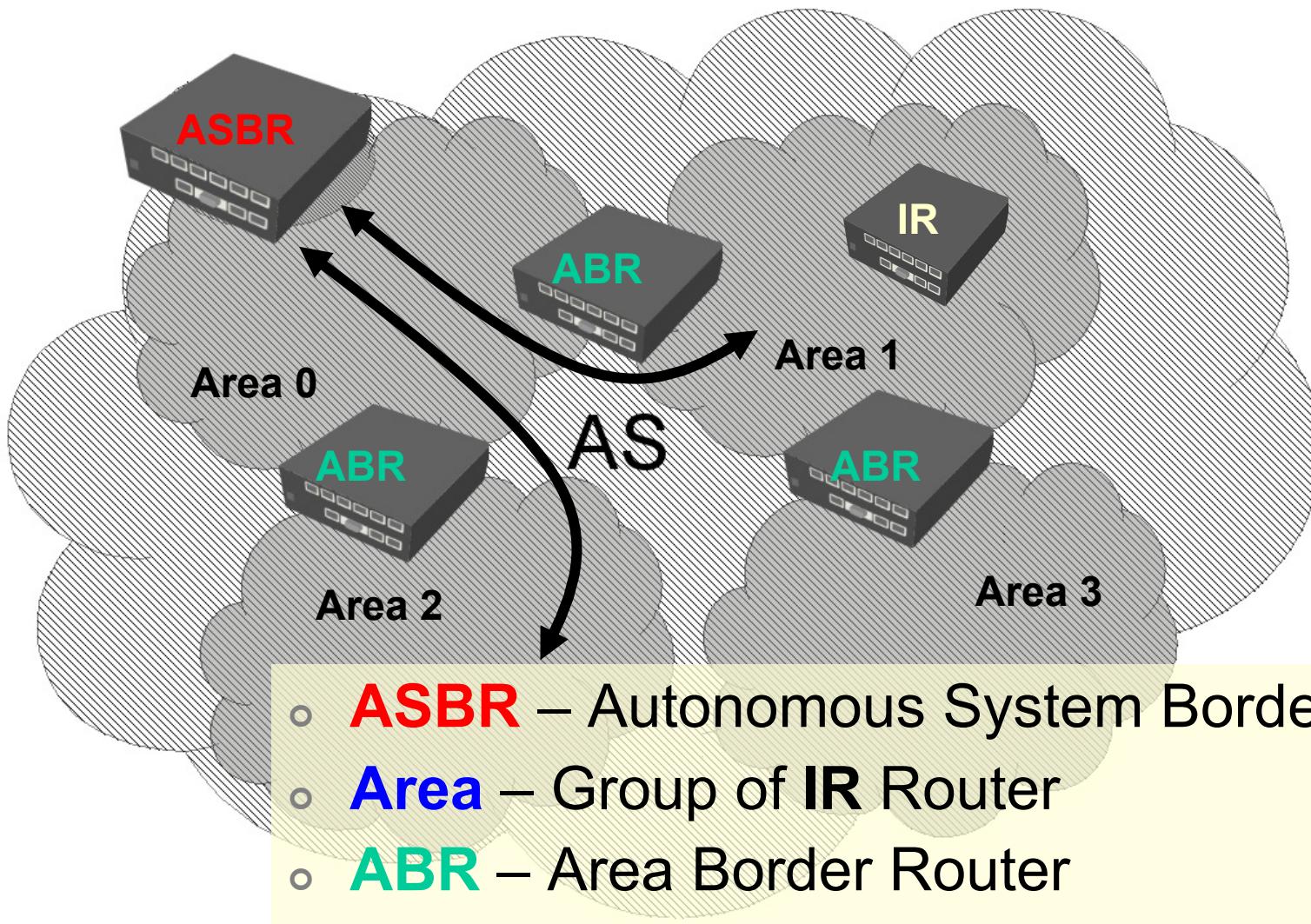
- Karena sebuah Autonomous System (AS) memiliki skala jaringan yang sangat besar maka penggunaan routing menjadi sangat penting dan kritis.
- Informasi routing haruslah tepat dan kesalahan melakukan distribusi informasi routing harus diminimalisasi sedikit mungkin.
- Sangatlah tidak nyaman jika harus menuliskan rule routing untuk puluhan bahkan ratusan router secara static.
- OSPF merupakan sebuah routing protokol yang dapat mendistribusikan informasi routing secara otomatis.
- OSPF juga merupakan *routing* protokol yang menggunakan konsep hirarki *routing*, dengan kata lain OSPF juga mampu membagi-bagi jaringan menjadi beberapa tingkatan. Tingkatan-tingkatan ini diwujudkan dengan menggunakan sistem pengelompokan yaitu **area**.

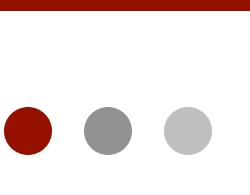


OSPF ?

- **Open Shortest Path First (OSPF)** adalah sebuah protocol routing otomatis (Dynamic Routing) yang mampu menjaga, mengatur dan mendistribusikan informasi routing antar network walaupun jaringan tersebut bisa berubah-ubah secara dinamis.
- OSPF termasuk di dalam kategori IGP (Interior Gateway Protocol) yang memiliki kemampuan **Link-state** dan **Algoritma Dijkstra** yang jauh lebih efisien dibandingkan protocol IGP yang lain.
- Menggunakan protocol tersendiri yaitu **protocol 89**.
- OSPF digunakan untuk management informasi dan distribusi routing di dalam sebuah AS.

Element of OSPF





Area,IR,ABR and ASBR

- **Area** adalah system grouping yang digunakan di protocol OSPF yaitu gabungan dari beberapa router **IR** (Internal Router) yang berjumlah <80 router.
- **IR** adalah router yang tergabung dalam sebuah area OSPF.
- **ABR** adalah router yang menjembatani area satu dengan area yang lain.
- **ASBR** adalah sebuah router yang terletak di perbatasan sebuah **AS (Router Terluar dari 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 protocol Routing yang lain (RIP,BGP dll).

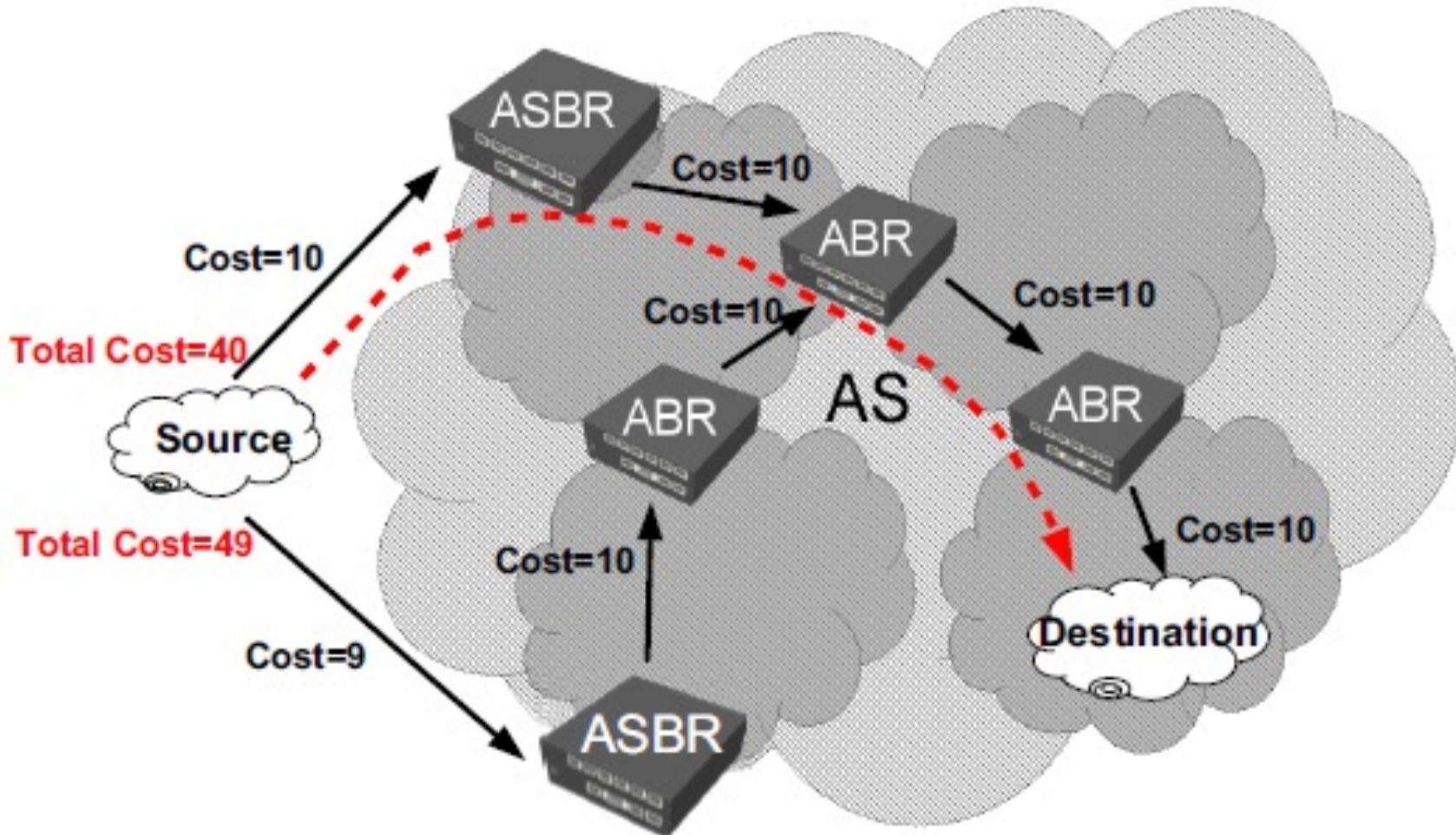


OSPF Feature

OSPF (IPv4 RFC 2838)

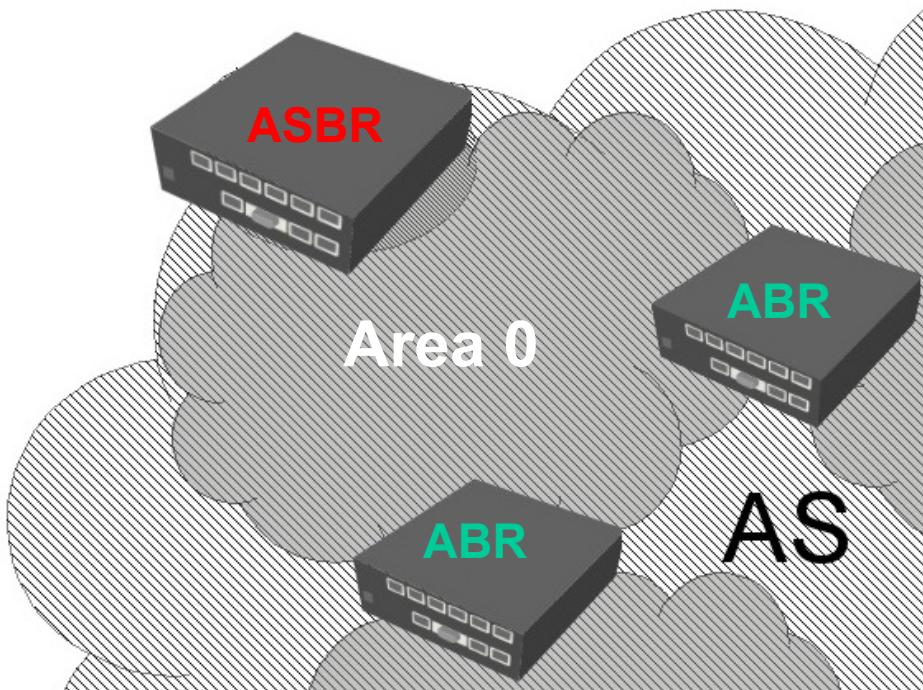
- Dynamic routing
- Interior Gateway Protocol (IGP) didalam sebuah routing domain (AS)
- Proses convergence yang cepat
- Link State / **Shortest Path Technology**
- Route Authentication
- Mendukung sistem pembagian Area
- Mendukung Fail Over

Link State – Based on Routing Cost



- Link State / **Shortest Path Technology** memungkinkan protocol OSPF menentukan jalur terpendek untuk mendistribusikan traffic

OSPF – Backbone Area



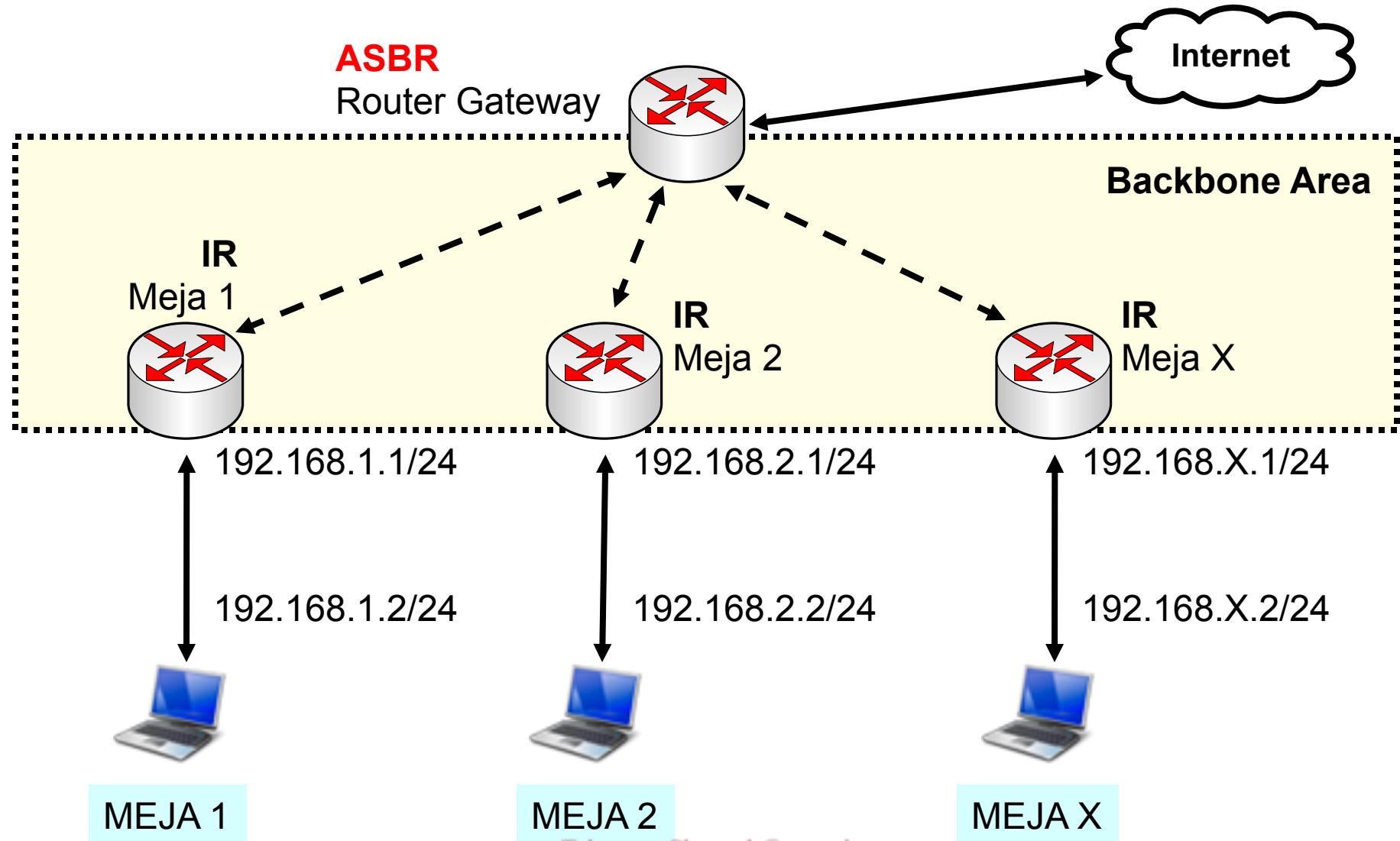
- Area 0 atau sering juga disebut sebagai **Backbone Area** merupakan area dimana Router-Router ABR berkumpul untuk saling menukarkan informasi routing dari area-area yang lain.
- Area Backbone juga merupakan **Area Transit** sebelum traffic keluar atau masuk ke dalam sebuah AS.
- Sebuah area yang tidak terhubung langsung ke area backbone bisa terhubung ke backbone area menggunakan **Virtual Link**.



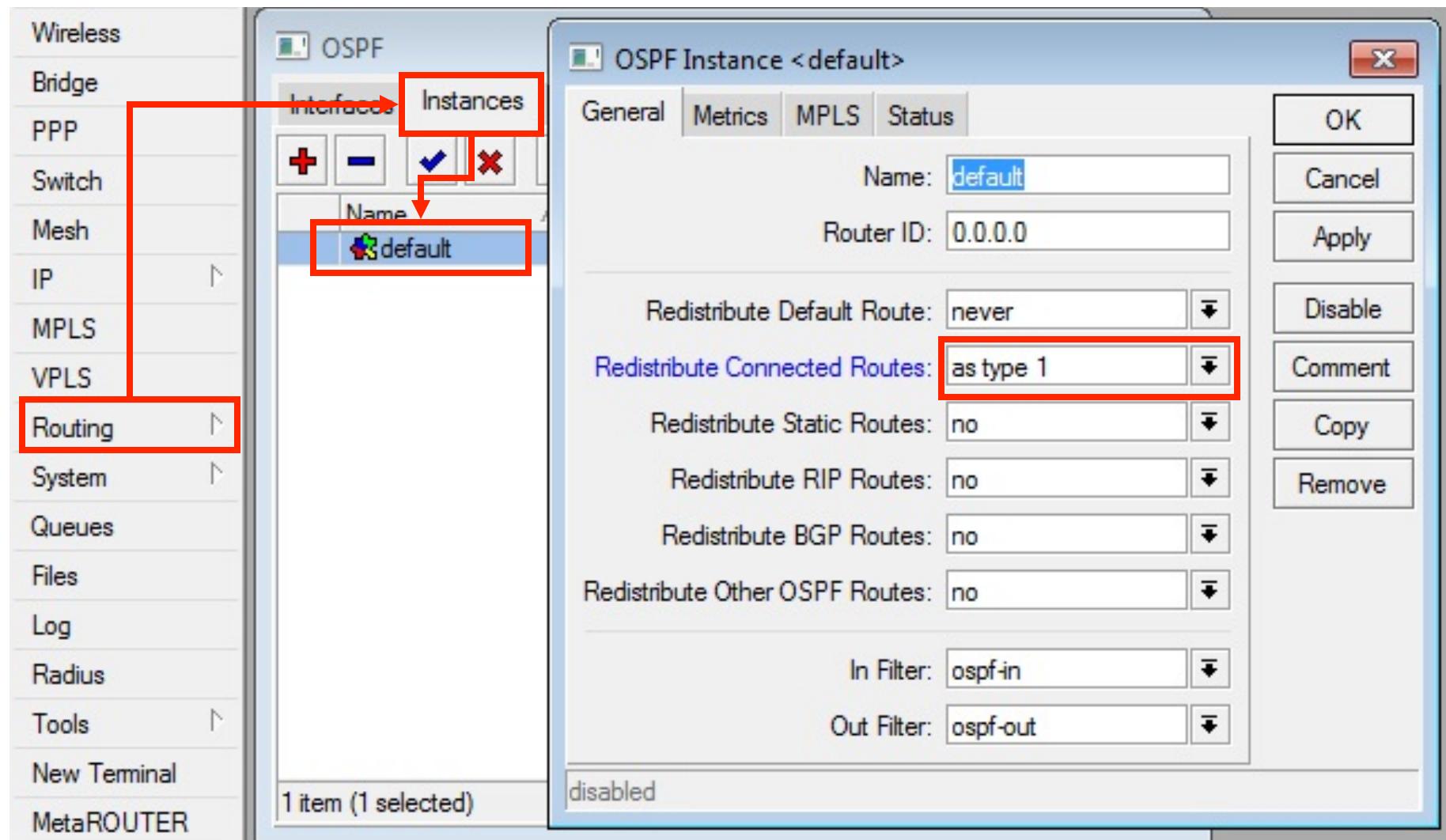
Link State Routing

- OSPF mampu melakukan Pencarian *neighbour router* secara otomatis
 - Yaitu Discovery Router yang terhubung dalam satu area
 - Menggunakan *Hello Packet*
 - Area-ID, authentikasi, Hello dan Dead Interval HARUS SAMA
- Langkah-langkah atau cara kerja OSPF :
 - Setiap router membuat *Link State packet* (LSP)
 - Mendistribusikan LSP ke semua *neighbour* menggunakan *Link State Advertisement* (LSA) dan menentukan DR dan BDR
 - Masing-masing router menghitung jarak terpendek ke semua tujuan berdasarkan cost routing.
 - Jika ada perubahan, LSP akan didistribusi dan dihitung ulang

[LAB-1] Konfigurasi OSPF



[LAB-1] OSPF Instance



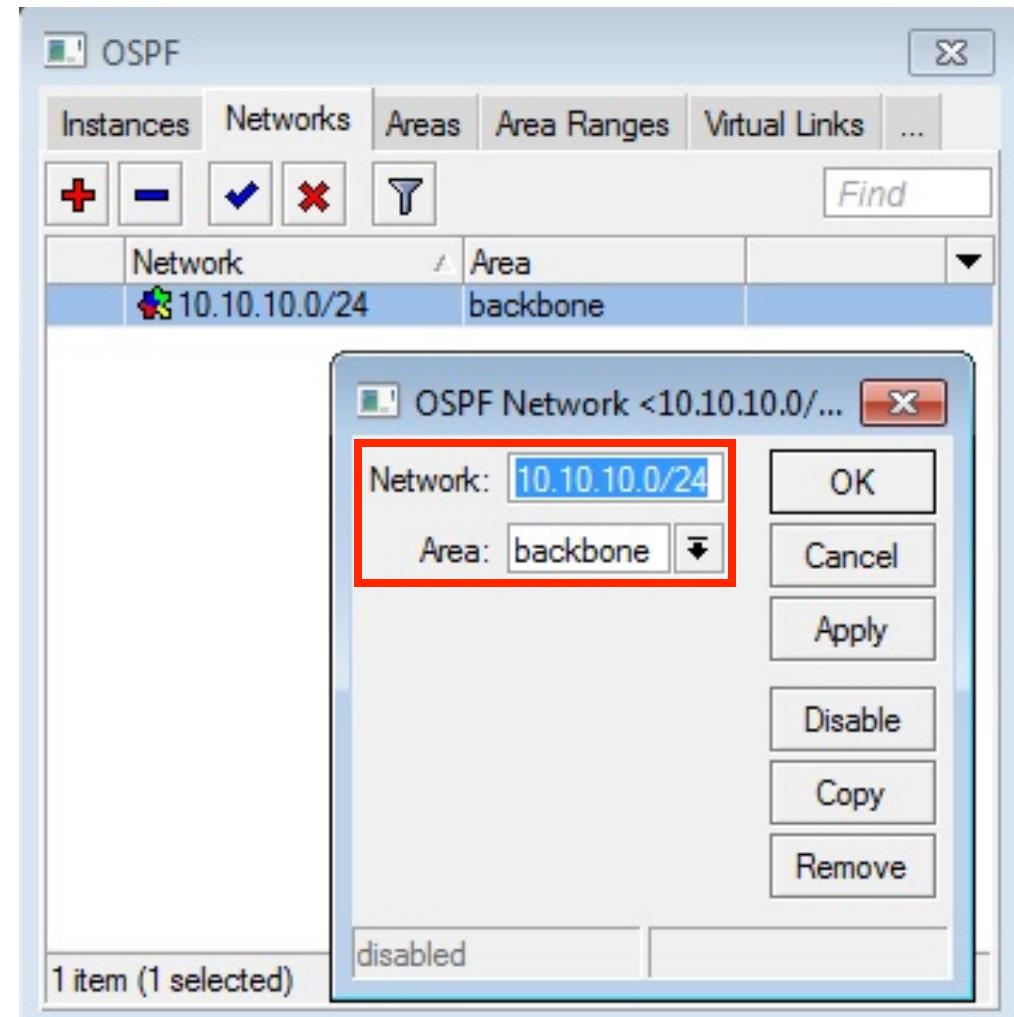


OSPF Setting

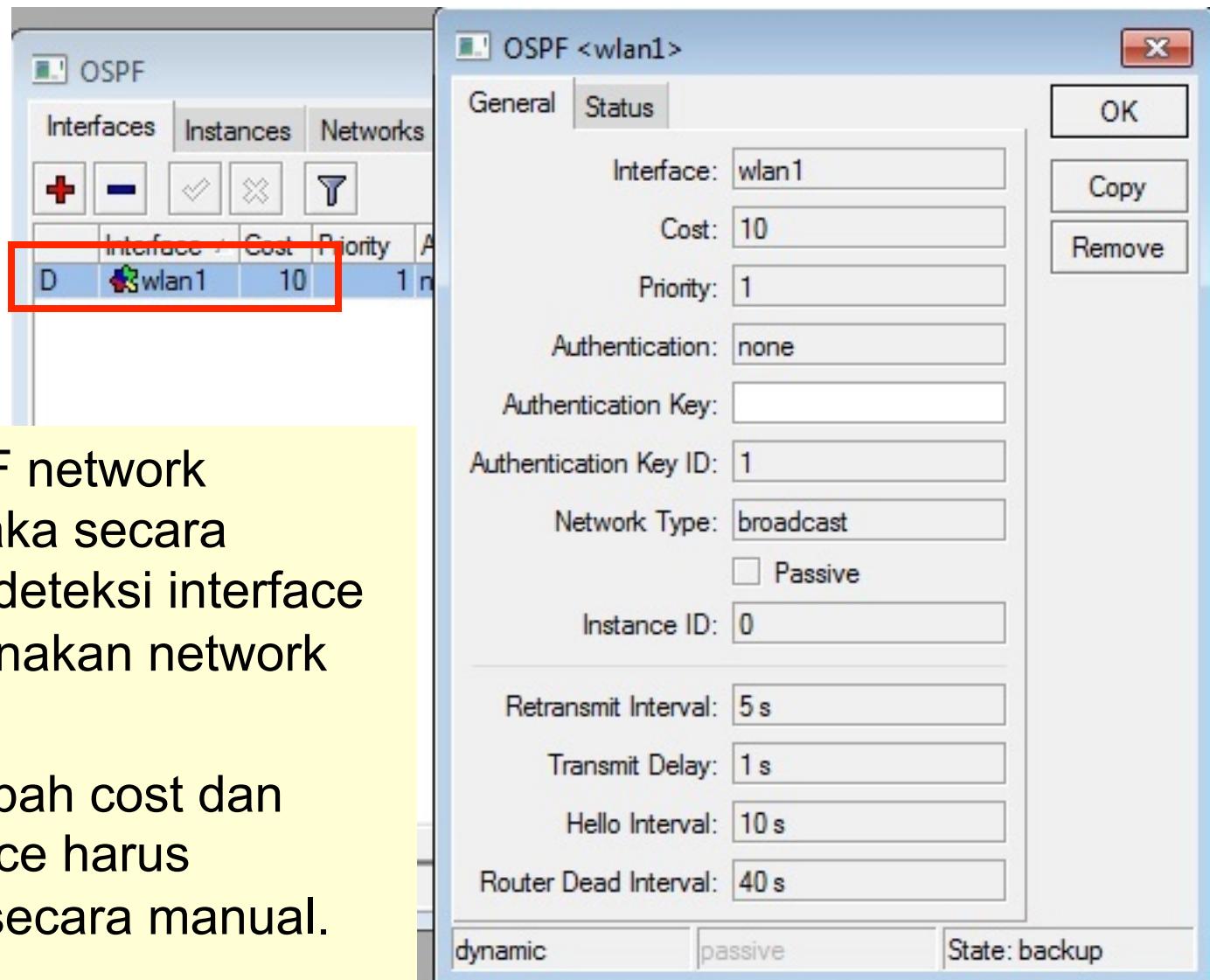
- **Router-id** → Memberi pengenal pada router.
 - Berformat 32bit seperti IP, tidak boleh ada yang sama dalam sebuah jaringan OSPF.
 - Jika diisi 0.0.0.0 maka router akan otomatis menggunakan IP terbesar yang ada pada interface
- **Redistribute Default Route** → Mendistribusikan default route.
 - Option 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

[LAB-1] OSPF Network

- Tambahkan OSPF Network yang terhubung ke area Backbone untuk mendapatkan informasi routing dengan router ABR yang lain.
- Gunakan network 10.10.10.0/24 sebagai network yang ada di backbone area.

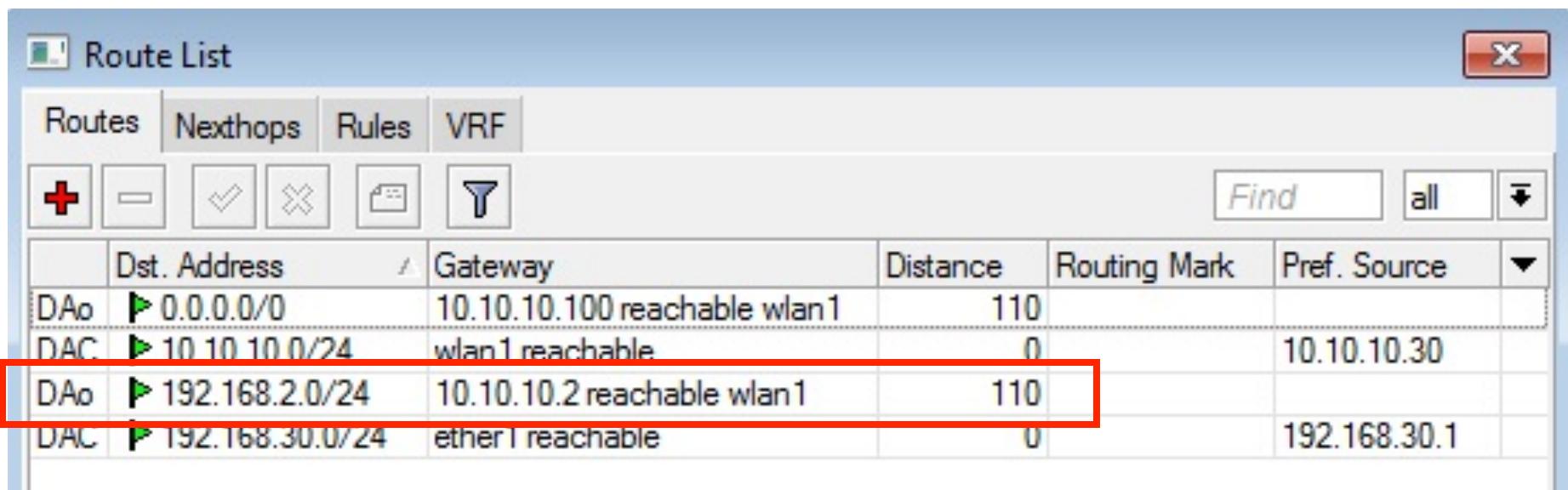


[LAB-1] OSPF Interface



- Setelah OSPF network ditentukan maka secara otomatis mendekripsi interface yang menggunakan network tersebut.
- Untuk mengubah cost dan priority interface harus didefinisikan secara manual.

[LAB-1] OSPF Route



The screenshot shows the 'Route List' window in Winbox. The window has tabs for 'Routes', 'Nexthops', 'Rules', and 'VRF'. The 'Routes' tab is selected. There are several icons at the top: a red plus sign for adding routes, a minus sign for deleting, a checkmark for filtering, an X for clearing filters, a folder for saving, and a magnifying glass for filtering. To the right are buttons for 'Find', 'all', and a dropdown arrow. The main area is a table with columns: 'Dst. Address', 'Gateway', 'Distance', 'Routing Mark', and 'Pref. Source'. The table contains the following data:

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAo	► 0.0.0.0/0	10.10.10.100 reachable wlan1	110		
DAC	► 10.10.10.0/24	wlan1 reachable	0		10.10.10.30
DAo	► 192.168.2.0/24	10.10.10.2 reachable wlan1	110		
DAC	► 192.168.30.0/24	ether1 reachable	0		192.168.30.1

- Cek pada tabel routing, OSPF akan mendistribusikan routing dari network lain yang terhubung ke backbone area.
- Rule routing yang memiliki Flag **DAO** menunjukkan ada rule routing yang didistribusikan menggunakan protocol OSPF.

[LAB-1] OSPF Route Detail

Route <192.168.2.0/24>

General Attributes

Dst. Address: 192.168.2.0/24

Gateway: 10.10.10.2 reachable wlan1

Check Gateway:

Type: unicast

Distance: 110

Scope: 20

Target Scope: 10

Routing Mark:

Pref. Source:

dynamic active dynamic

Route <192.168.2.0/24>

General Attributes

BGP AS Path:

BGP Weight:

BGP Local Pref.:

BGP Prepend:

BGP MED:

BGP Atomic Aggregate:

BGP Origin:

BGP Communities

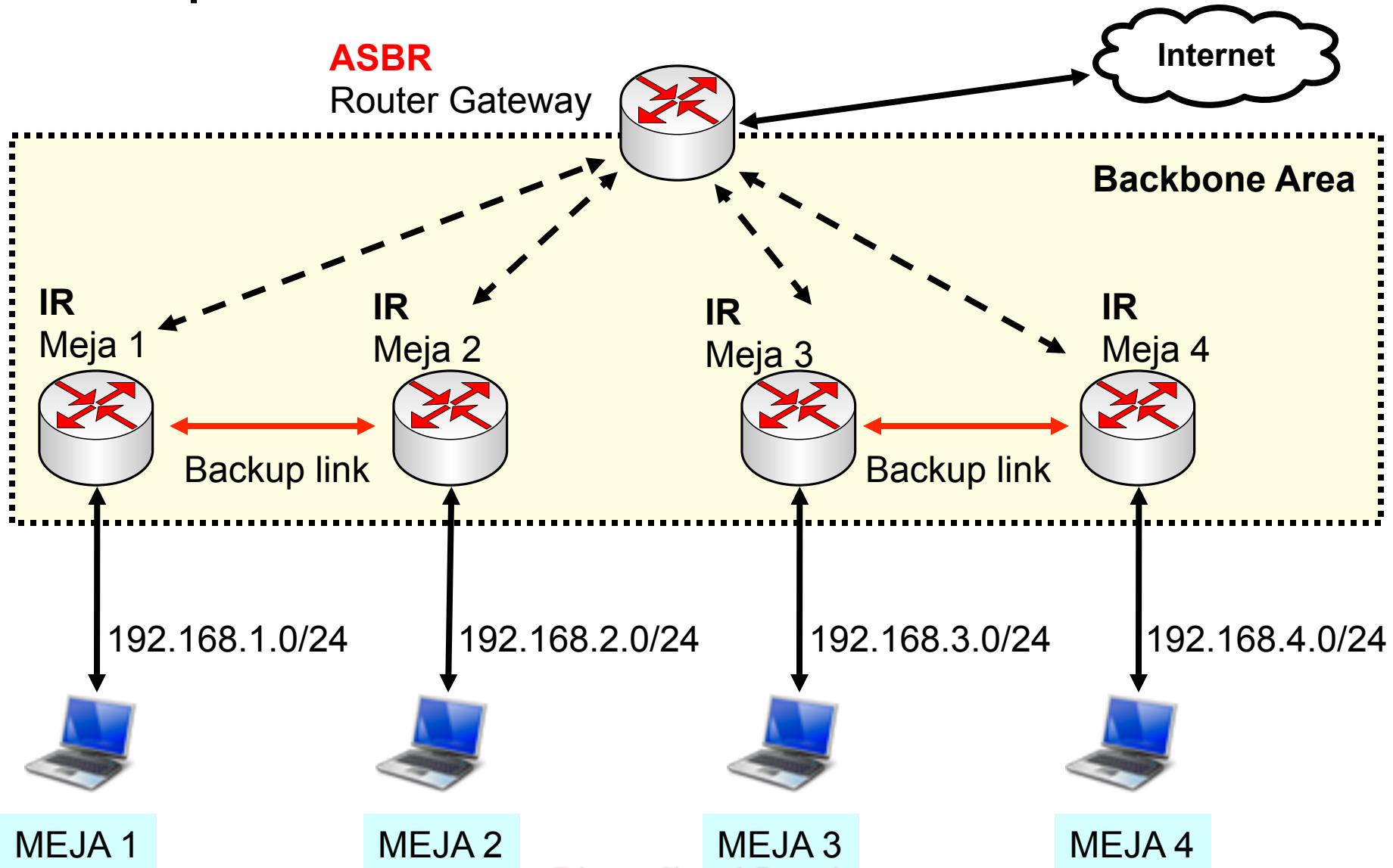
Route Tag:

OSPF Metric: 30

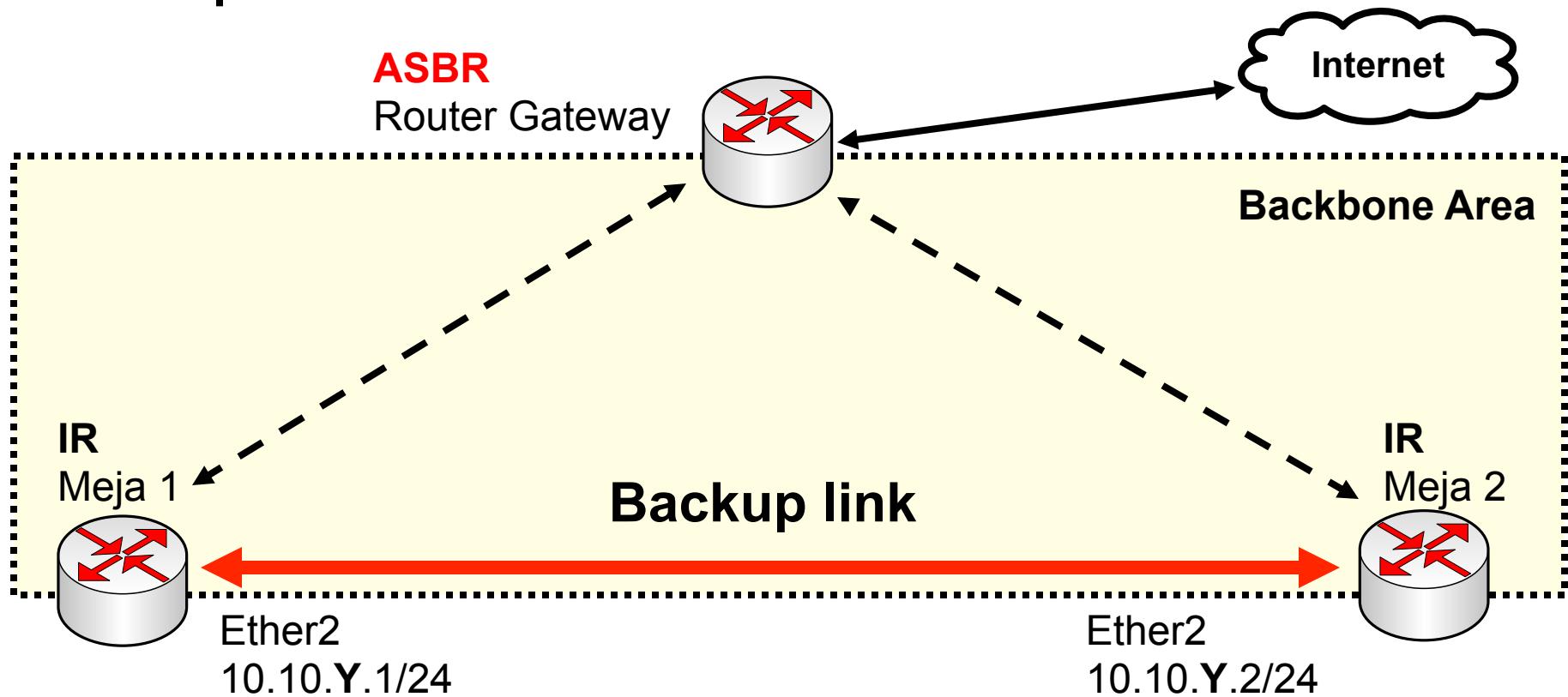
OSPF Type: external type 1

dynamic active dynamic

[LAB-2] OSPF - Fail Over

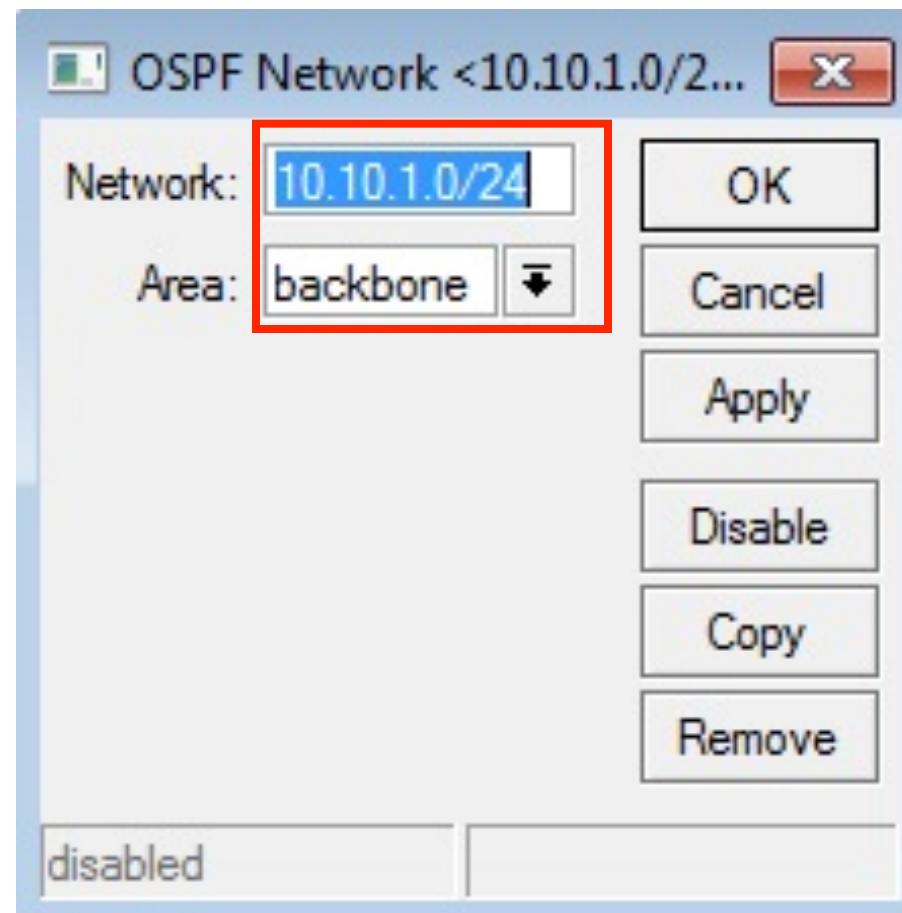


[LAB-2] OSPF - Fail Over detail



- Hubungkan ether2 dari router anda ke ether2 router rekan anda sebagai link backup.
- Pasang ip satu segmen 10.10.Y.0/24 pada link backup tersebut.
- Y adalah nomor kelompok.

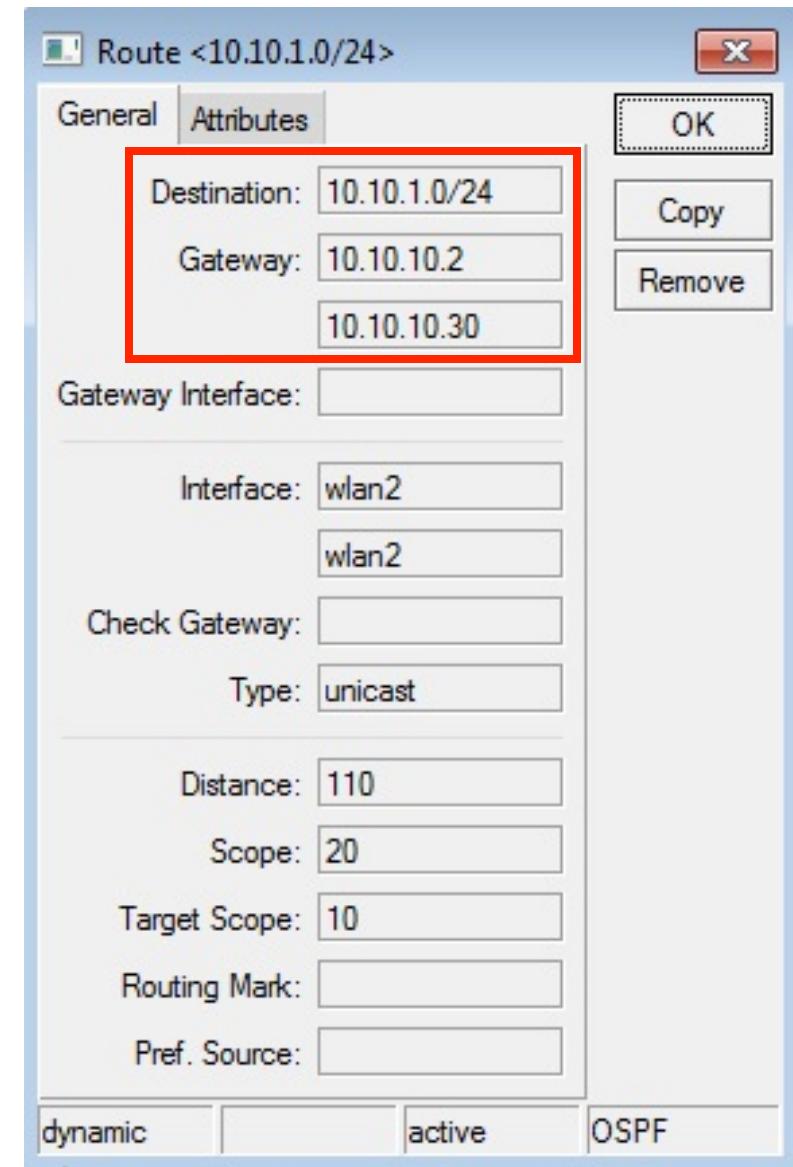
[LAB-2] Interface for Backup



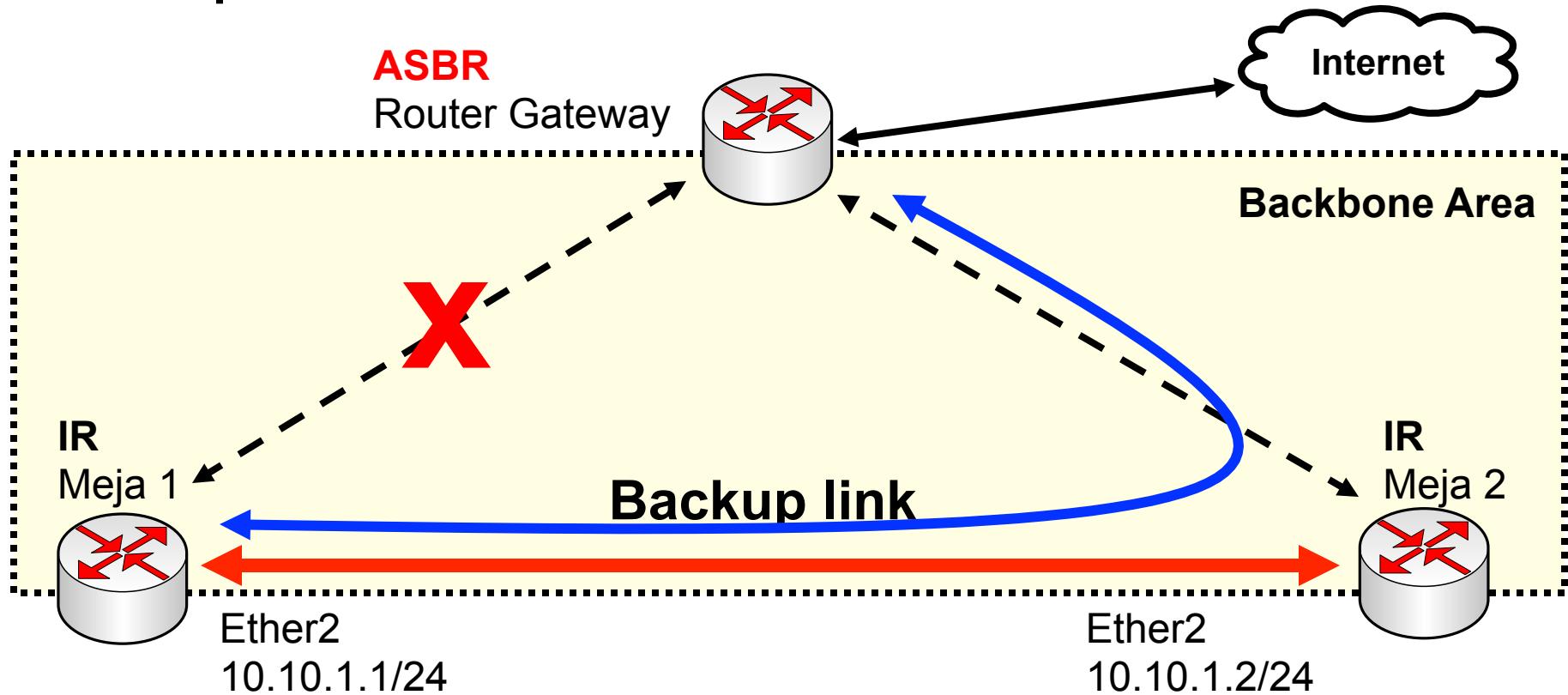
- Tambahkan network baru ke backbone area.

Redundant Detected

- Router Utama (**ASBR**) akan mendekksi ada network baru 10.10.Y.0/24 .
- Network baru tersebut bisa dirouting menggunakan 2 jalur yang berbeda
- Kedua jalur tersebut adalah jalur yang terkoneksi ke 2 router yang berbeda.



[LAB-2] Fail Over Test



- Coba matikan link utama dan test apakah fail over bisa dilakukan otomatis.
- Hidupkan kembali link utama untuk cek terhadap proses failover.

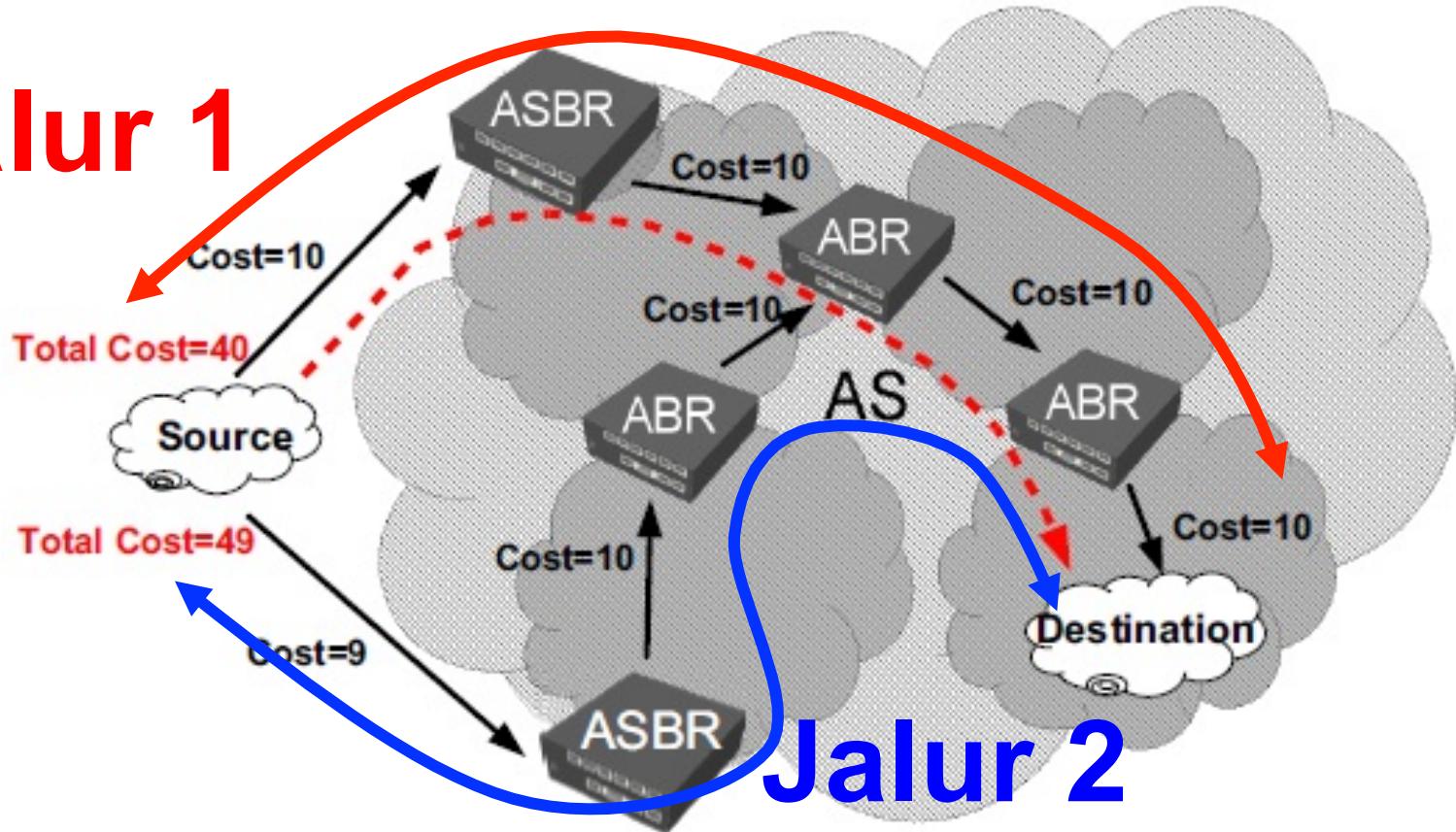


OSPF Cost

- Untuk menetukan jalur terpendek atau bisa juga diartikan sebagai jalur prioritas, OSPF menggunakan parameter “**Cost**”.
- OSPF “Cost” akan dijumlahkan di setiap hoopnya 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

Jalur 1

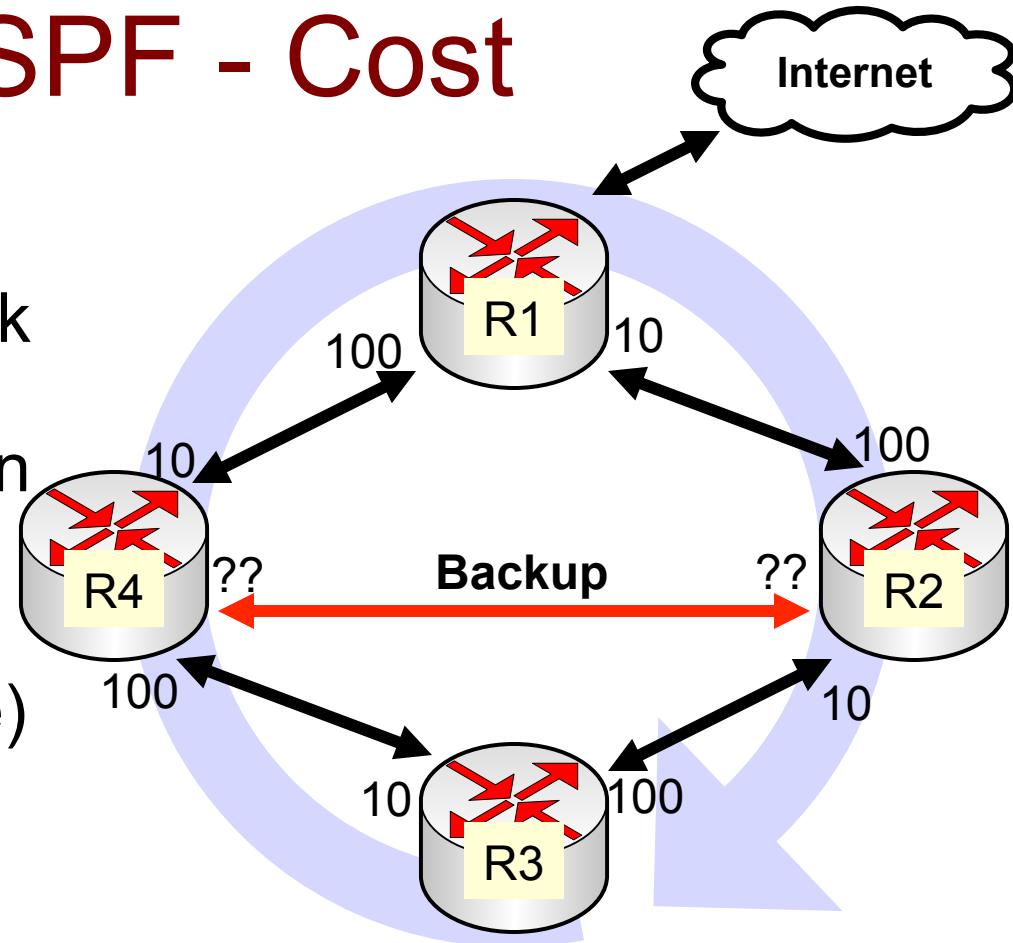


Jalur 2

- Terlihat ada dua jalur yang bisa menuju ke network tujuan.
- Setelah dilakukan perhitungan total **Cost**, jalur 1 memiliki total cost terkecil. Maka jalur tersebut yang akan digunakan.

[LAB-3] OSPF - Cost

- Bangun bagan network berikut dengan kelompok terdiri 4 router dan terkoneksi menggunakan ethernet.
- Gunakan konfigurasi OSPF (manual Interface) sehingga traffic berjalan searah jarum jam.
- Traffic upload melewati router bagian kiri dan download melewati router bagian kanan.



- Gunakan koneksi wireless (Wlan2) sebagai backup link.
- Tentukan cost dari backup link supaya traffic tetap searah jarum jam.

[LAB-3] OSPF - Cost

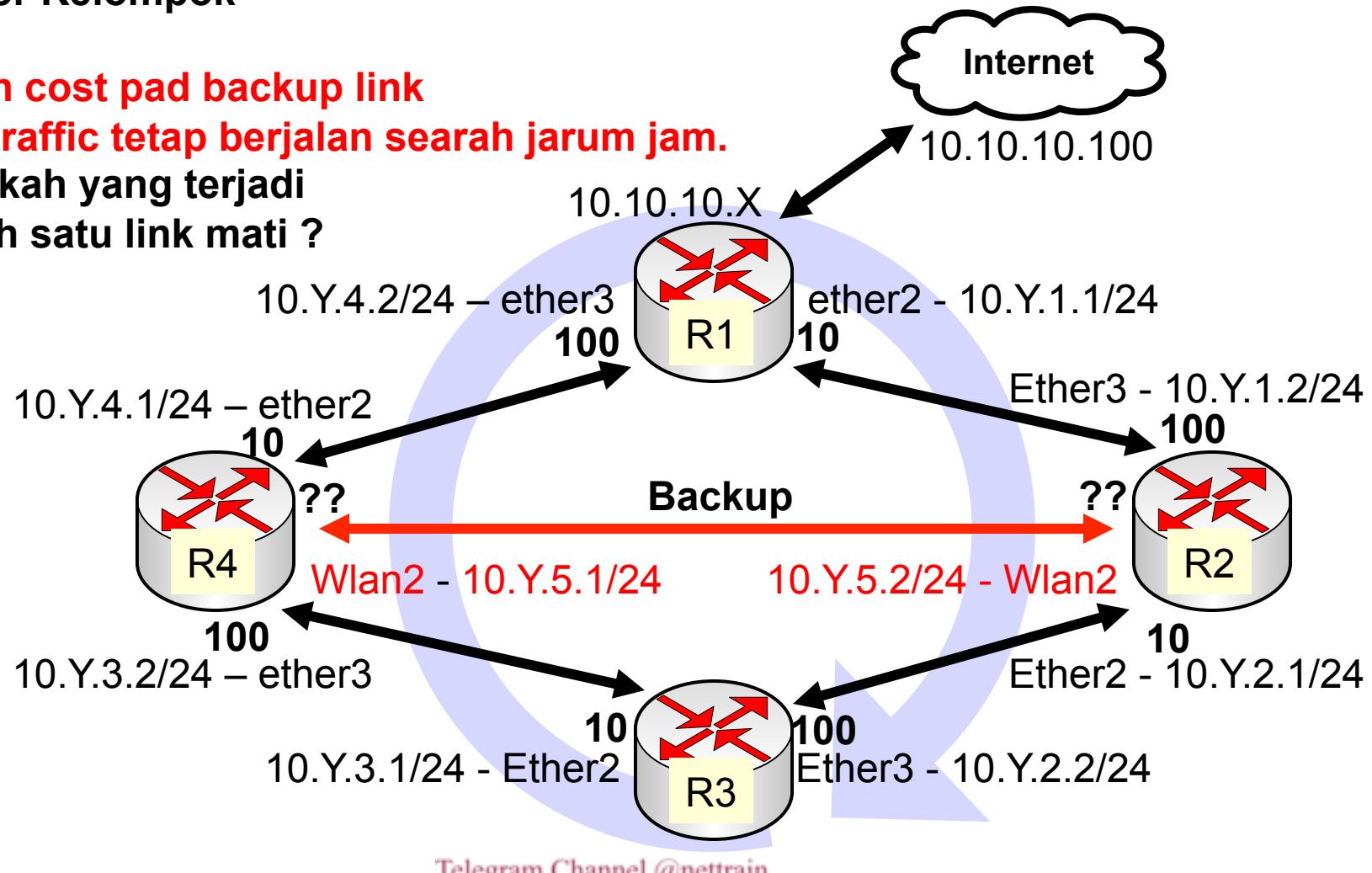
X : Nomor Kursi

Y : Nomor Kelompok

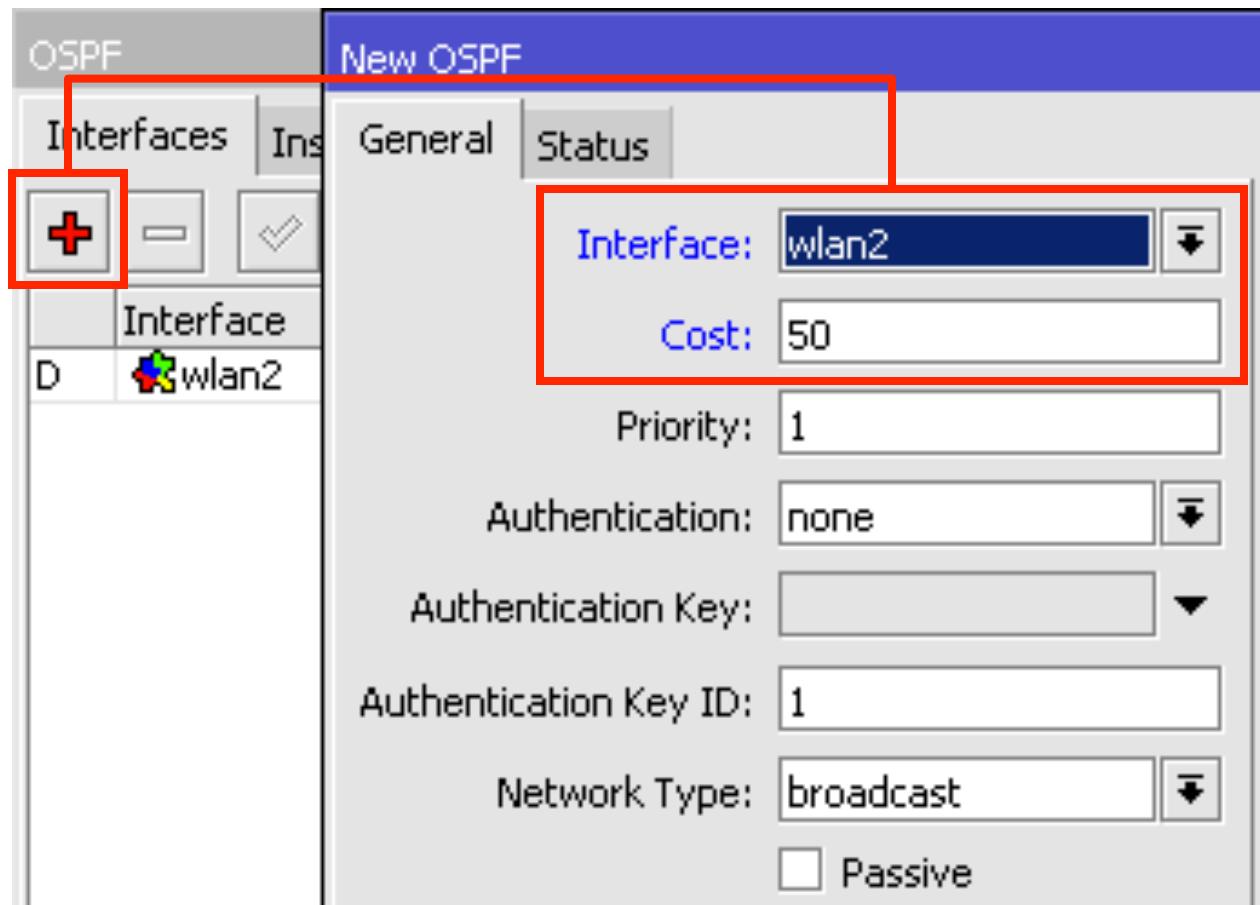
Tentukan cost pad backup link

supaya traffic tetap berjalan searah jarum jam.

Test apakah yang terjadi jika salah satu link mati ?



Cost Overwrite



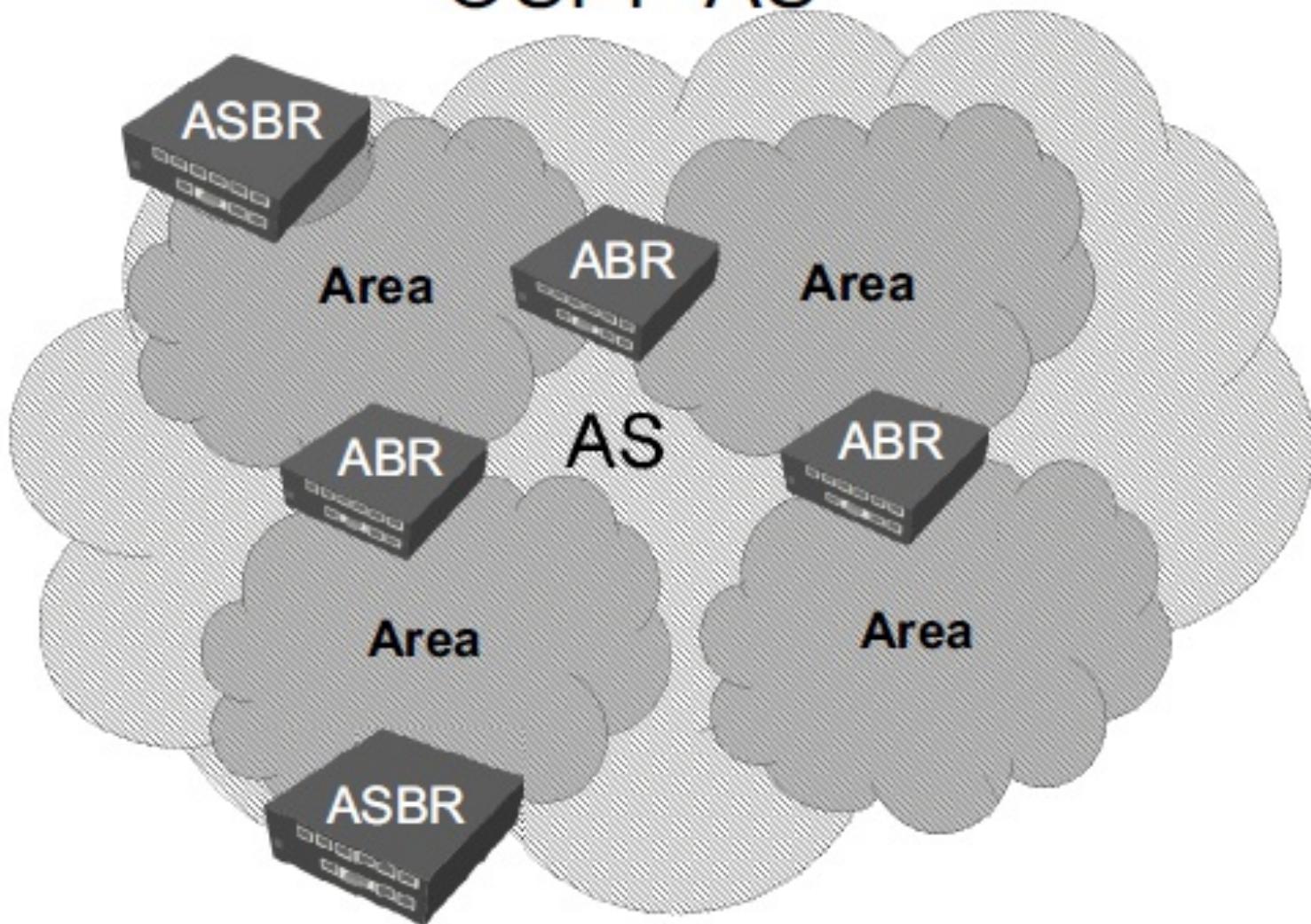
- Tambahkan interface untuk link backup dan ubah “cost” supaya menjadi routing backup.

OSPF-Neighbour State

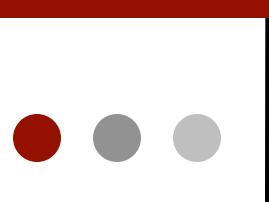
Neighbor State	Description
Down	The initial state. No information has been received from the neighbor router.
Attempt	No information has been received despite attempts to contact the neighbor (for NBMA networks only).
Init	A Hello packet has been received from the neighbor, but the router does not appear in the neighbor list of the neighboring router's Hello packet.
2-Way	A Hello packet has been received from the neighbor, and the router does appear in the neighbor list of the neighboring router's Hello packet.
ExStart	Master and slave roles for the Database Exchange Process are being negotiated. This is the first phase of the adjacency relationship.
Exchange	The router is sending Database Description packets to its neighbor.
Loading	Link State Request packets are being sent to the neighbor requesting missing or more recent LSAs.
Full	The neighboring routers' LSDBs are synchronized, and the two routers are fully adjacent.

OSPF Routing Decision

OSPF AS



Telegram Channel @nettrain



Area DR & BDR

- Dalam setiap segmen 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 proses pertukaran LSA antar router
- BDR, akan menggantikan DR jika terjadi error
- DR dan BDR ditentukan oleh priority dari masing-masing router
- Jika priority sama, akan dipilih yang memiliki router-ID paling tinggi



LSA Type

- **Type 1 (Router Link)** : menginformasikan router yang terhubung langsung dan kondisi interface dalam 1 area
- **Type 2 (Network Link)** : Mengidentifikasi IP semua router DR yang terhubung dengan jaringan
- **Type 3 (Summary Link)** : Meringkaskan kondisi subarea sebelum di advertise ke subarea lain yang masih dalam satu AS
- **Type 4 (ASBR Summary Link)** : Menunjukkan link-state ID dari router ASBR yang mengadvertise LSA type 5
- **Type 5 (AS External Link)** : LSA ini mengandung informasi yang diimpor ke OSPF dari proses routing lainnya dan diadvertise ke semua area (kecuali Stub Area)
- **Type 6 (Group Membership)** : didefinisikan untuk Multicast extensions to OSPF (MOSPF), a multicast routing protocol yang jarang digunakan
- **Type 7 (Group Membership)** : Membawa informasi route yang melewati NSSA Stub Area



OSPF Routing Type

- **Intra-Area routing**

- Menggambarkan route ke tujuan yang masih dalam satu area. (LSA type 1 dan 2)

- **Inter-Area routing**

- Menggambarkan route ke tujuan yang membutuhkan melewati satu atau lebih area OSPF dan masih dalam satu AS. (LSA type 3 dan 4)

- **External Area routing**

- Menggambarkan route keluar jaringan lokal
- Dibedakan menjadi 2 tipe :
 - **E1 → E1** route cost merupakan jumlah dari internal dan external (remote AS) ospf metric.
 - **E2 → E2** route cost merupakan nilai dari cost external saja

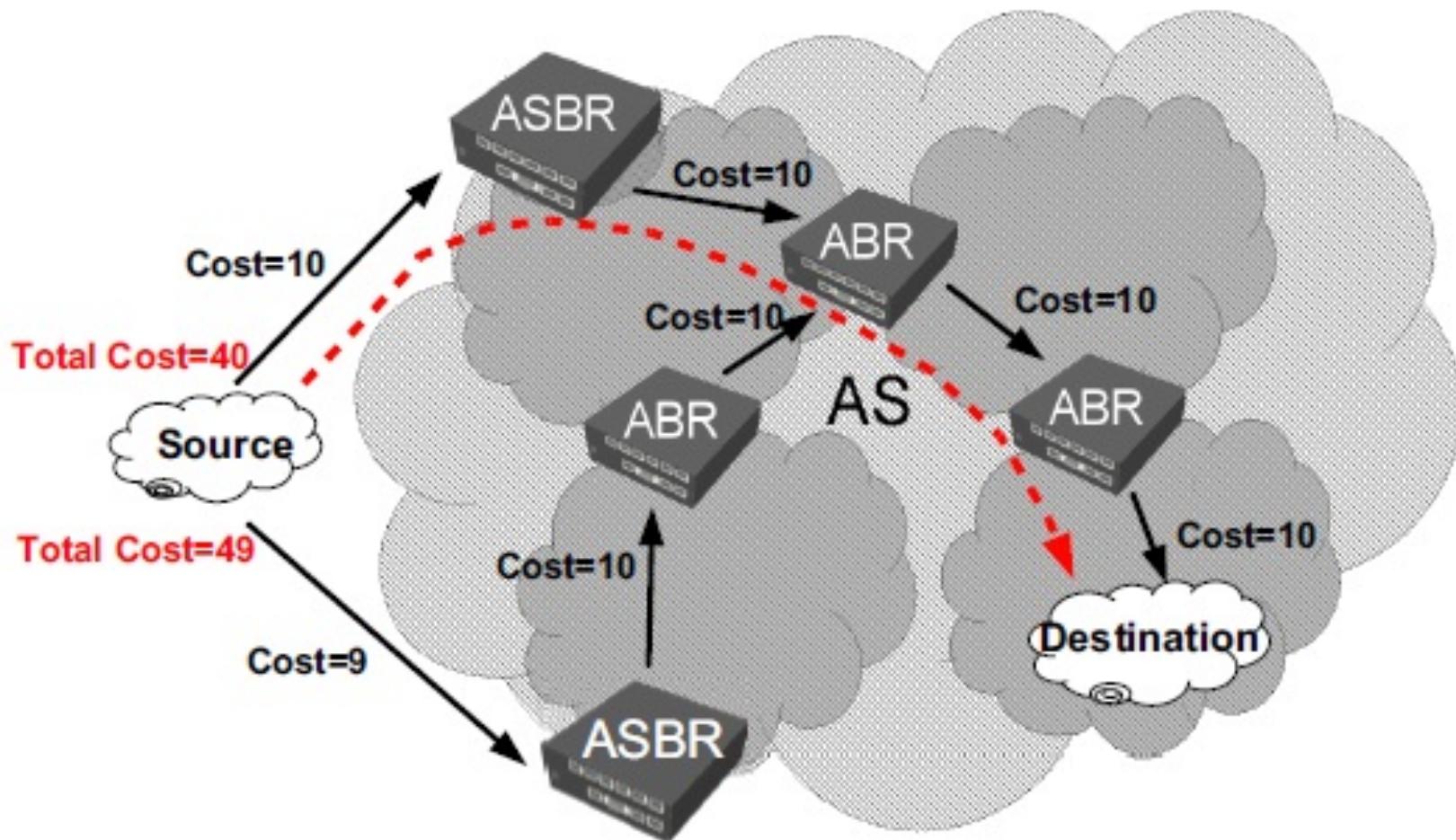


Metric VS Cost?

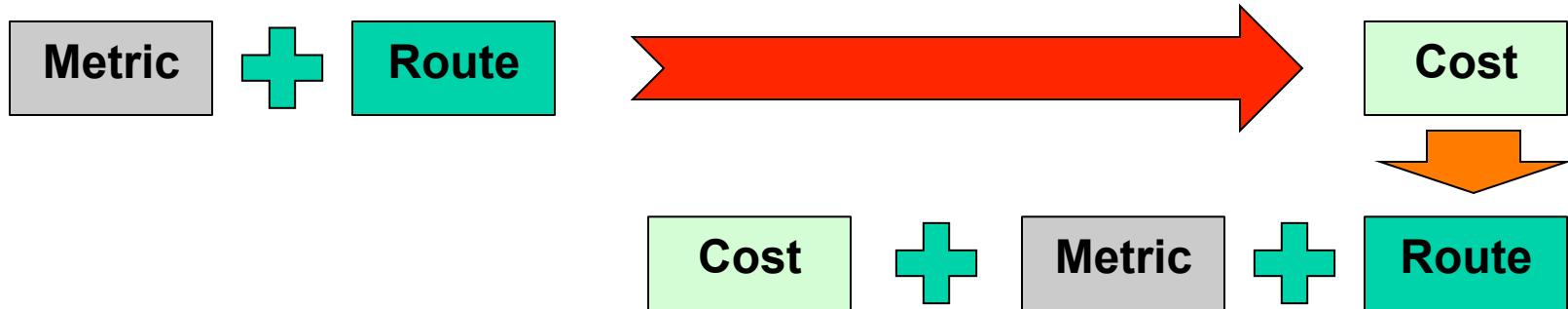
- **Metric** adalah salah satu parameter di routing yang sebenarnya merupakan kumpulan nilai yang digunakan oleh algoritma routing untuk menentukan apakah satu rute lebih baik dari route yang lain
- Nilai Metric bisa terdiri dari :
 - measuring link utilisation (using SNMP)
 - number of hops (hop count)
 - Speed of the path
 - packet loss (router congestion/conditions)
 - latency (delay)
 - path reliability
 - path bandwidth
 - throughput [SNMP - query routers]
 - load
 - MTU
- Pada OSPF, untuk menetukan nilai Metric menggunakan parameter Cost.

Tipe Routing OSPF

External Type 1 Metrics



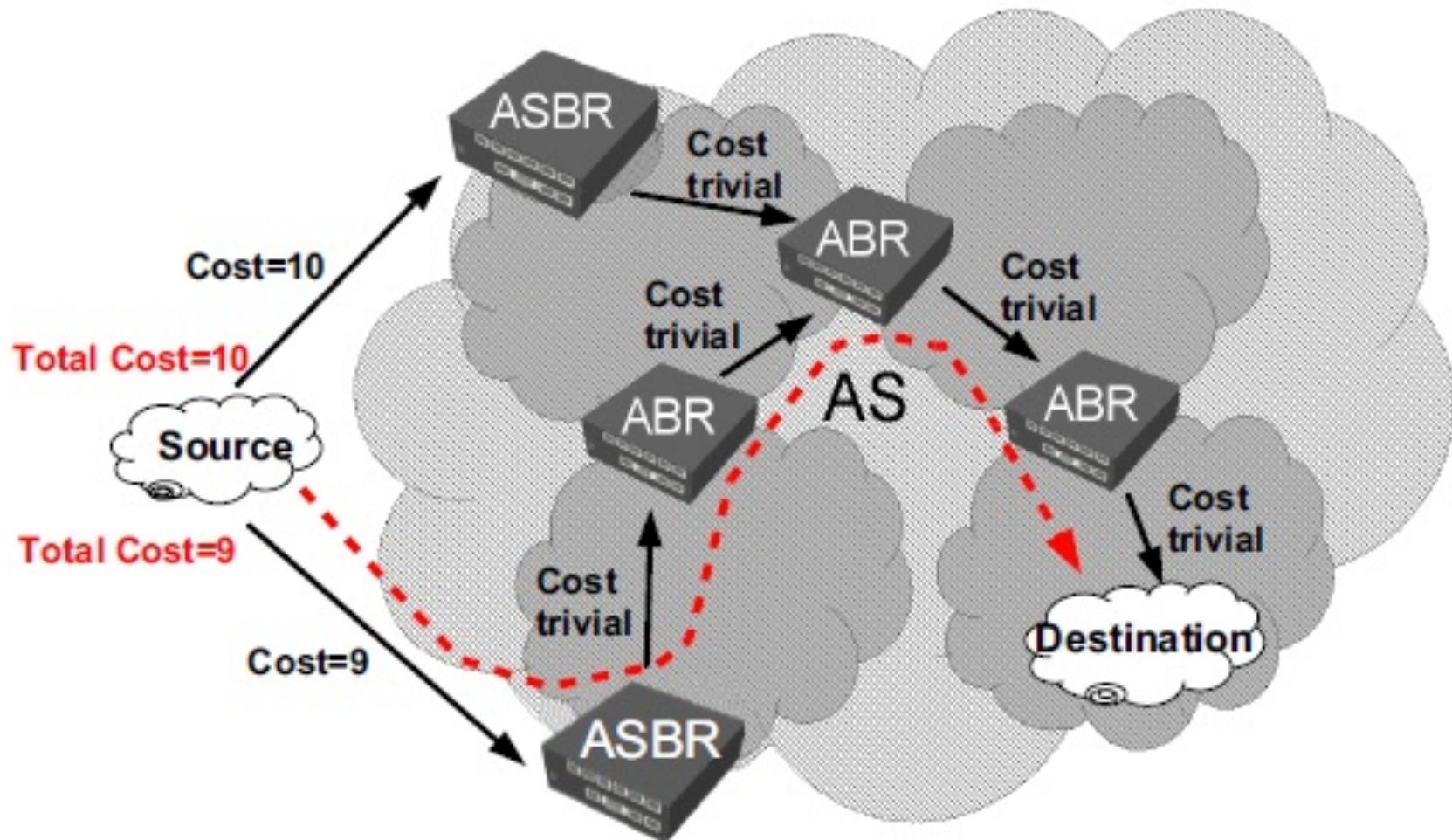
● ● ● | OSPF Metric – as type 1



- Ketika OSPF menggunakan “as-type-1” maka informasi metric akan dibawa bersama dengan informasi routing.
- Sehingga total Metric adalah pejumlahan metric asal dan juga cost.

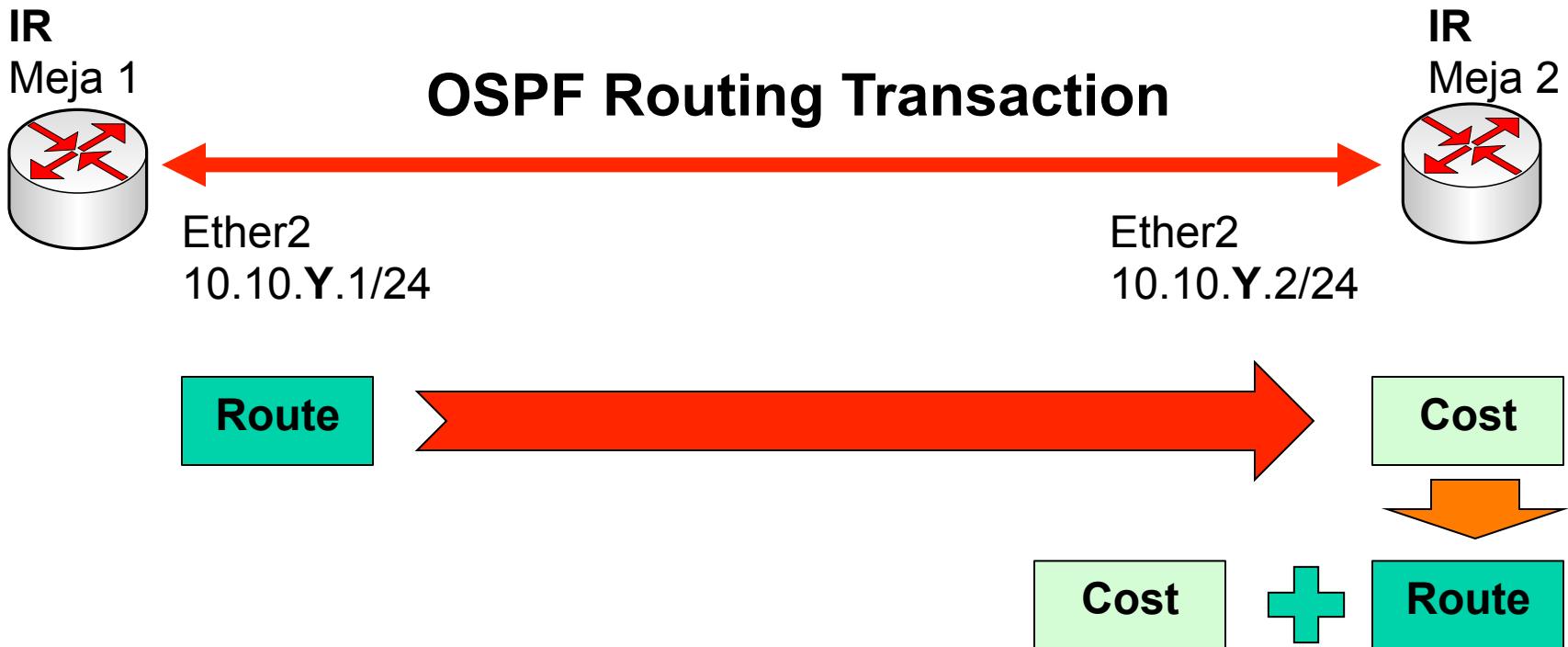
Tipe Routing OSPF

External Type 2 Metrics



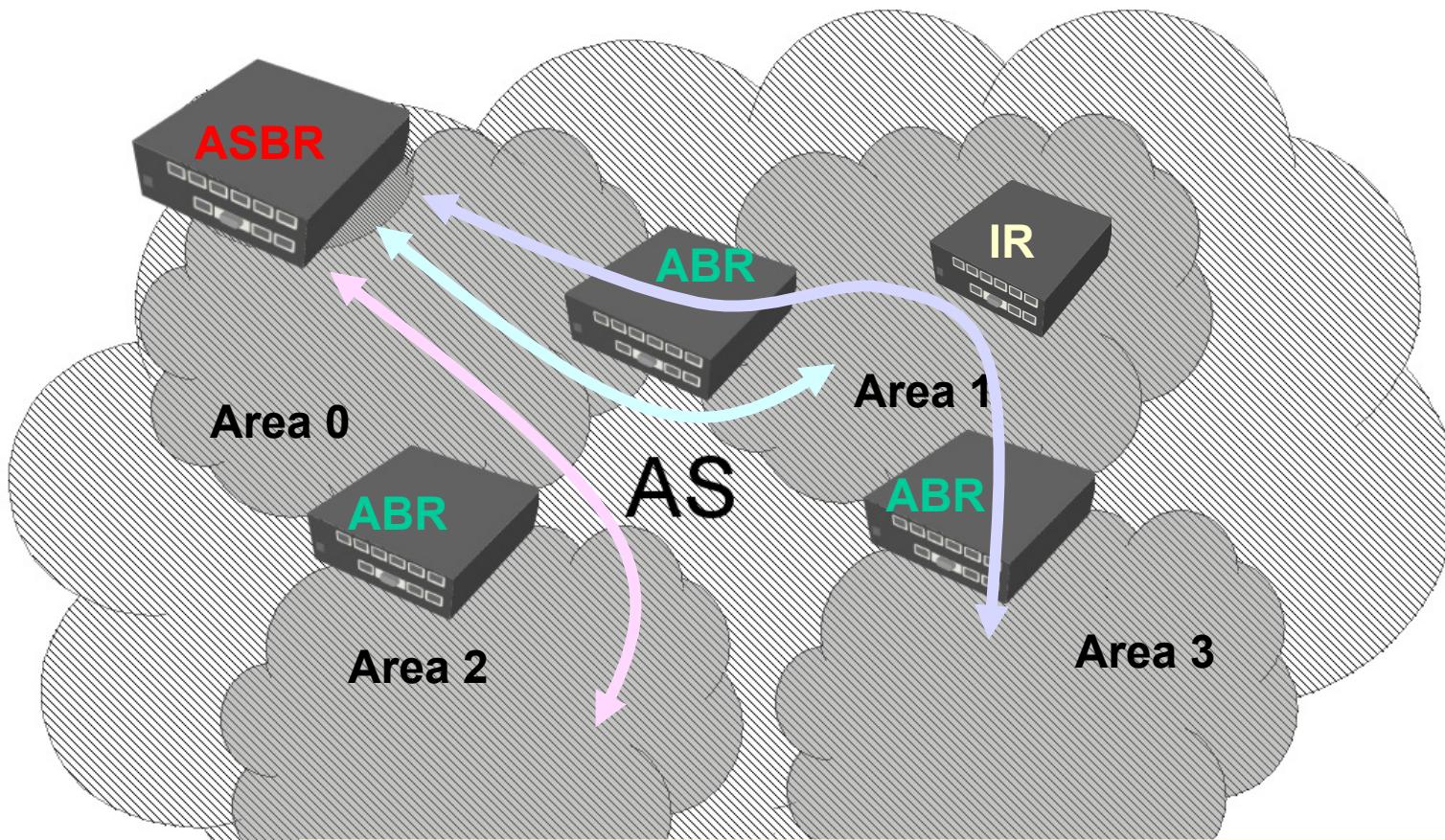
Telegram Channel @nettrain

● ● ● | OSPF Metric – as type 2



- Ketika OSPF menggunakan “as-type-2” maka informasi metric “tidak” akan dibawa bersama dengan informasi routing.
- Sehingga total Metric adalah berdasarkan cost saja.

OSPF Area



- Sangat memungkinkan jika pada sebuah AS memiliki lebih dari satu area menyesuaikan skala dari jaringan yang dimiliki.



OSPF Area

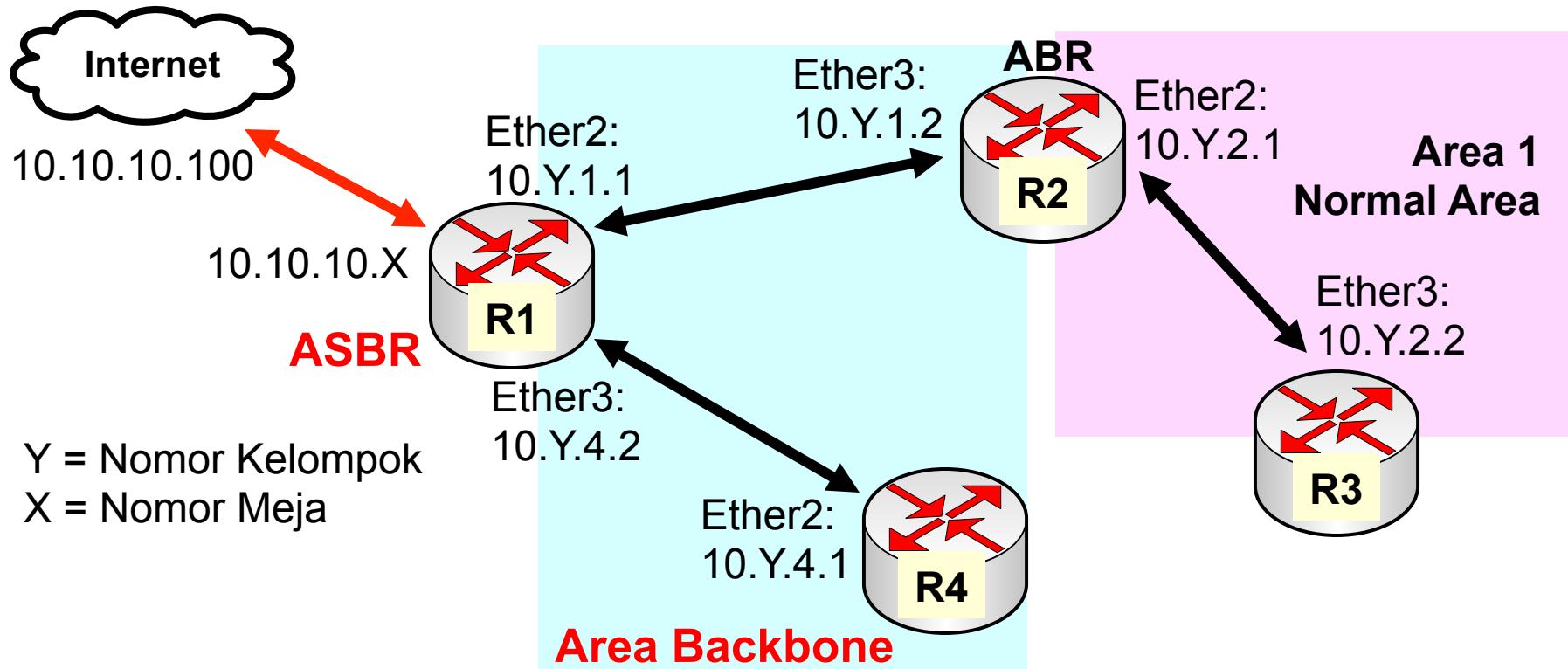
- Semakin banyak router dan jaringan didalamnya, semakin besar ukuran Link State Database → cpu load, memory
- Internal router akan mendapat LSA hanya dari router lain yang masih dalam satu area
- Area yang ingin mendapatkan informasi LSA secara lengkap dan bisa terkoneksi dengan jaringan yang ada di luar AS maka harus terhubung secara logic dengan Backbone (Area 0).
- Untuk area yang tidak secara langsung terhubung ke area backbone bisa menggunakan **Virtual Link** memanfaatkan area lain yang sudah terhubung ke Backbone Area.



Area Type

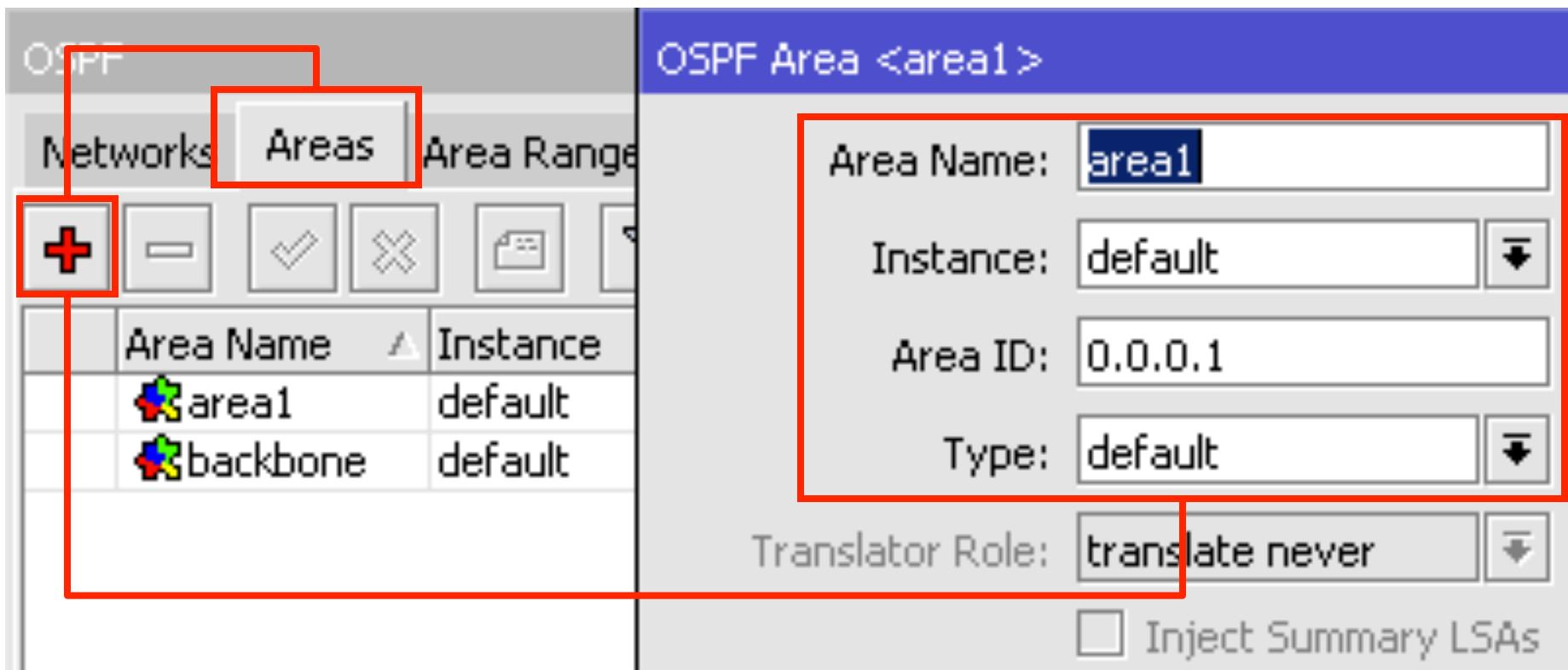
- **Backbone – Area 0** (default mikrotik 0.0.0.0)
 - Bertanggung jawab mendistribusikan informasi routing antara non-Backbone area
 - Semua sub-Area HARUS terhubung dengan backbone secara logikal
- **Standar Area**
 - Merupakan sub-Area dari Area 0. Area ini menerima LSA intra-area dan inter-area dari 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

[LAB-4] OSPF – Normal Area



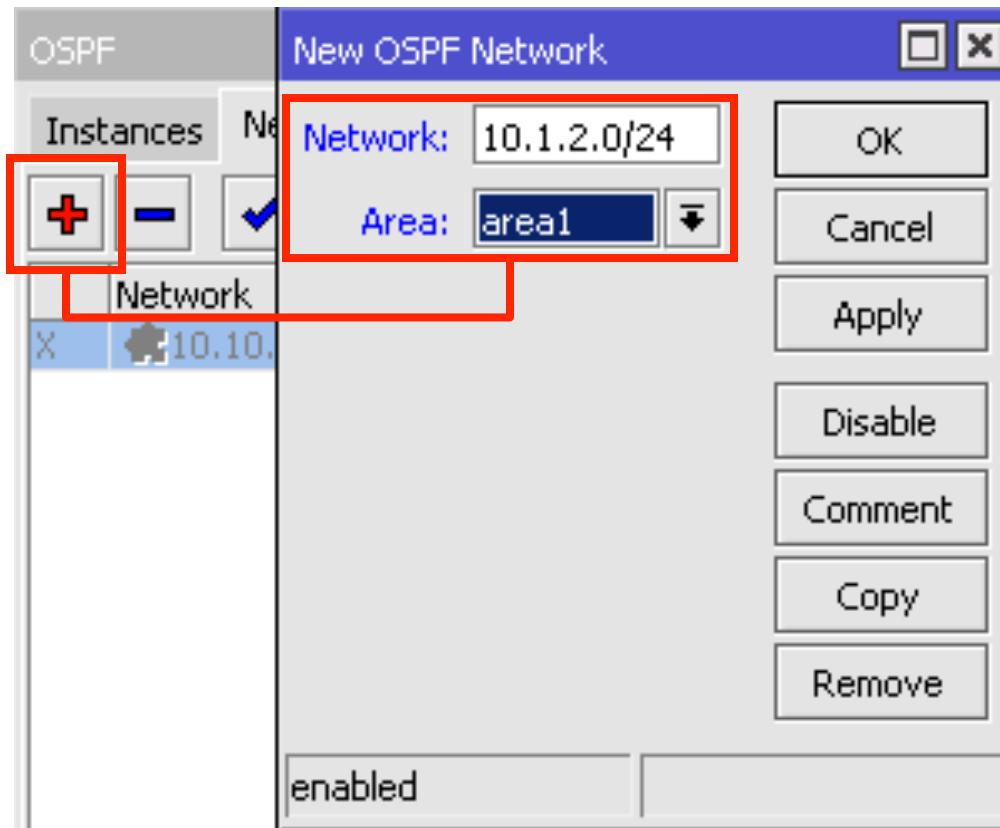
- Bangun network sesuai bagan di atas gunakan dua area yang berbeda (Backbone dan Area1)
- Amati informasi routing di R2 dan R3

Create Area (R2 & R3)



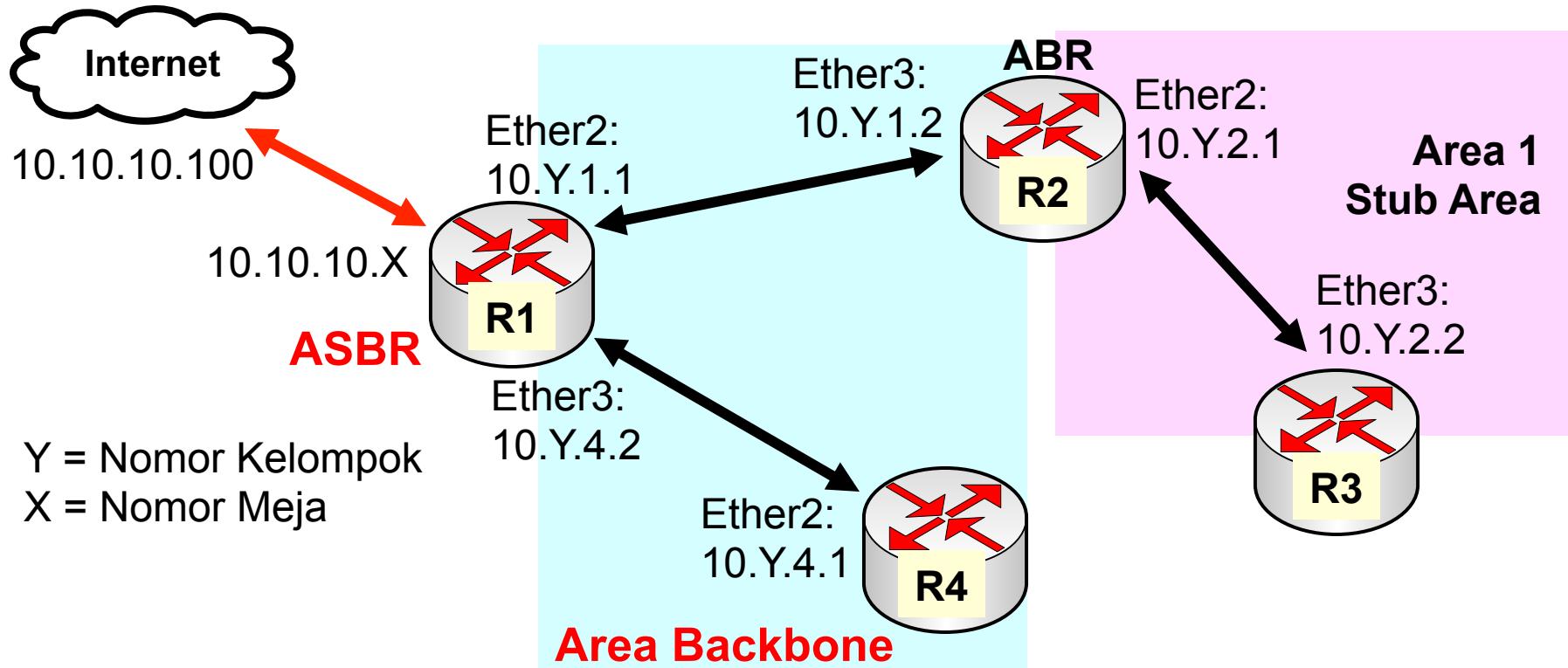
- Tambahkan Area baru yaitu Area1 bertipe "Default" di router R2 dan R3.

Activate OSPF Area1



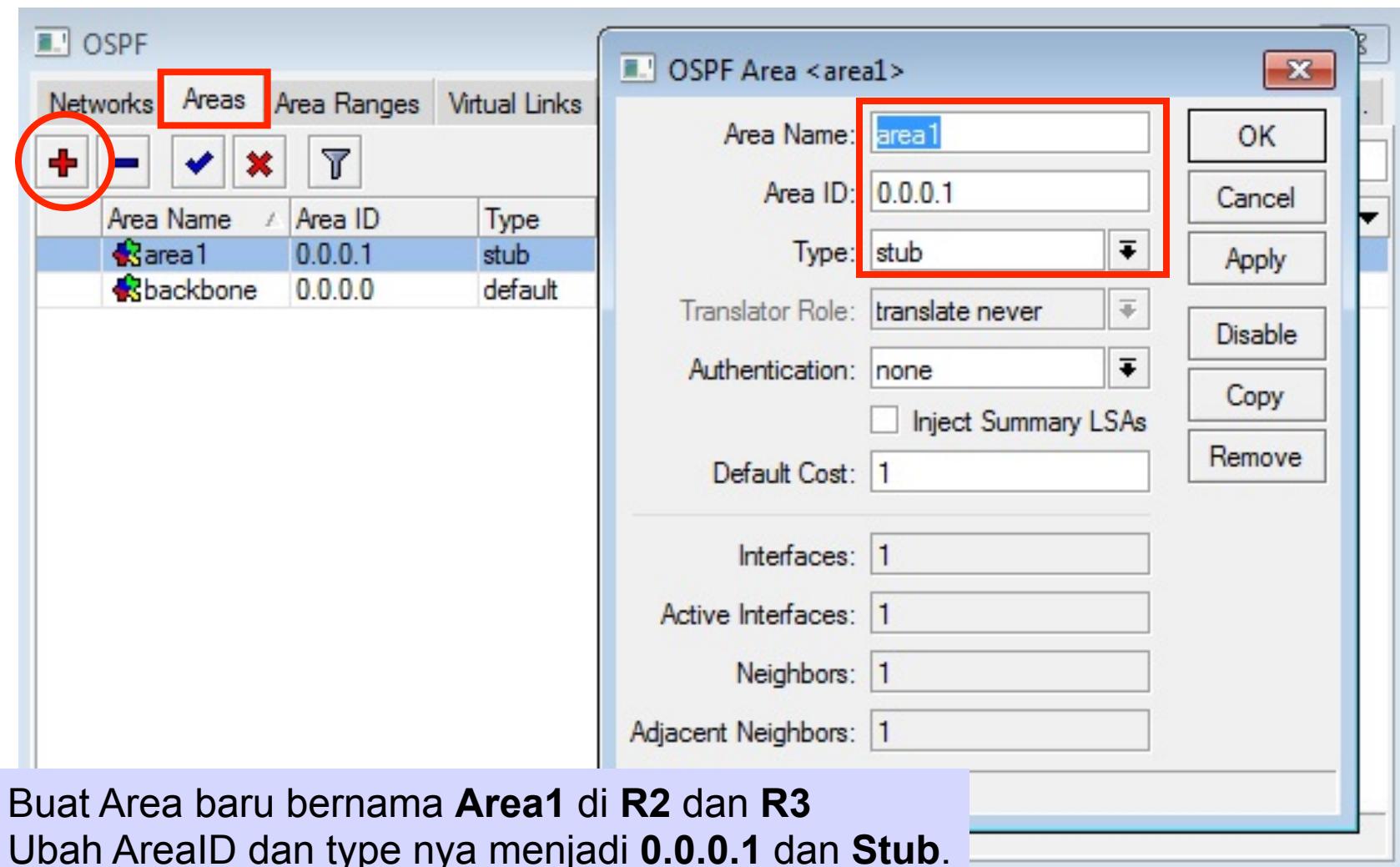
- Aktivkan area1 untuk network 10.Y.2.0/24

[LAB-5] OSPF – Stub Area



- Bangun network sesuai bagan di atas gunakan dua area yang berbeda (Backbone dan Area1)
- Amati informasi routing di R2 dan R3

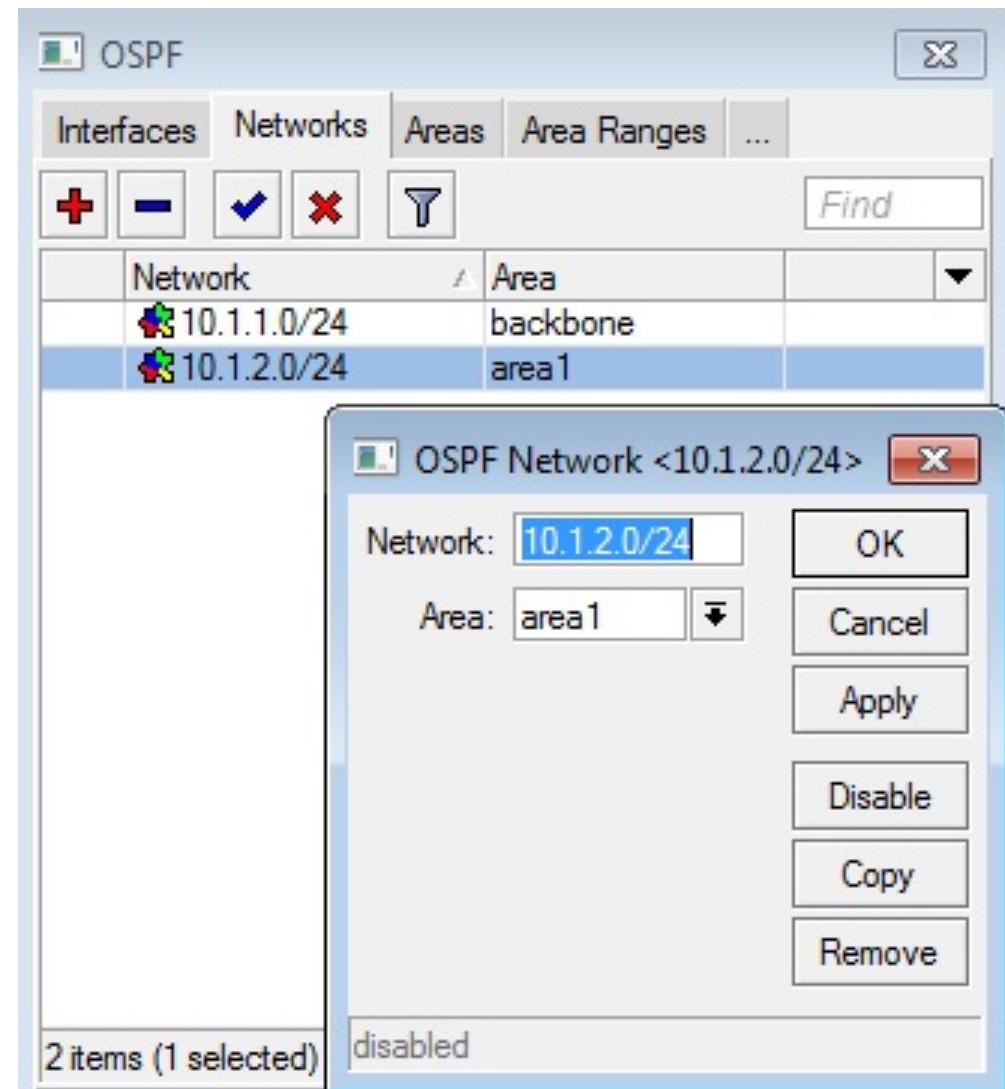
[LAB-5] OSPF Area1 Configuration



Buat Area baru bernama **Area1** di **R2** dan **R3**
Ubah AreaID dan type nya menjadi **0.0.0.1** dan **Stub**.

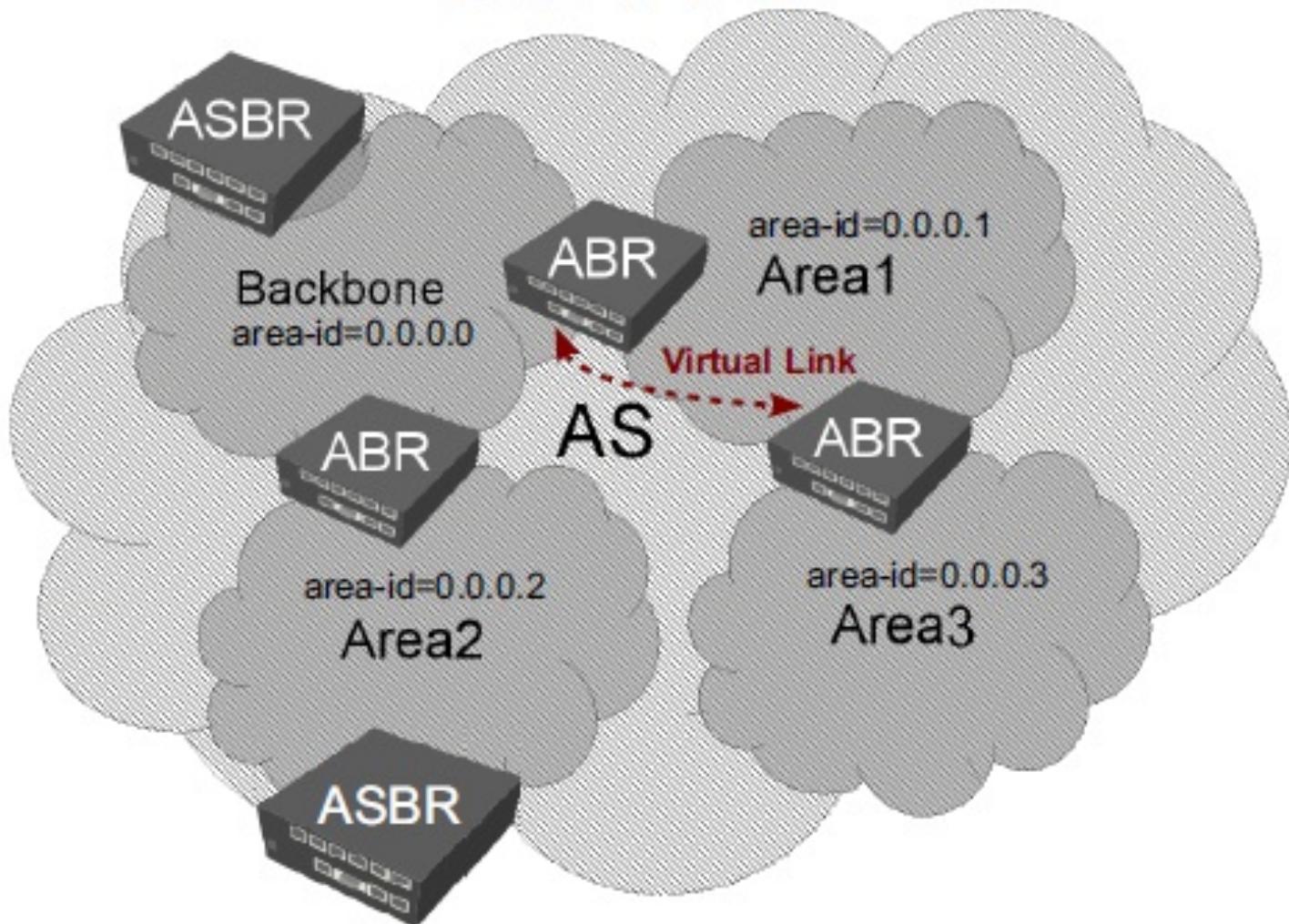
[LAB-5] OSPF Area1 Configuration

- Tambahkan network baru pada **R2** dan **R3** dan gunakan Area1.
- Gunakan interface dynamic untuk network di Area1 kemudian amati perubahan routing di R2 dan R3.



OSPF - Virtual Link

OSPF AS

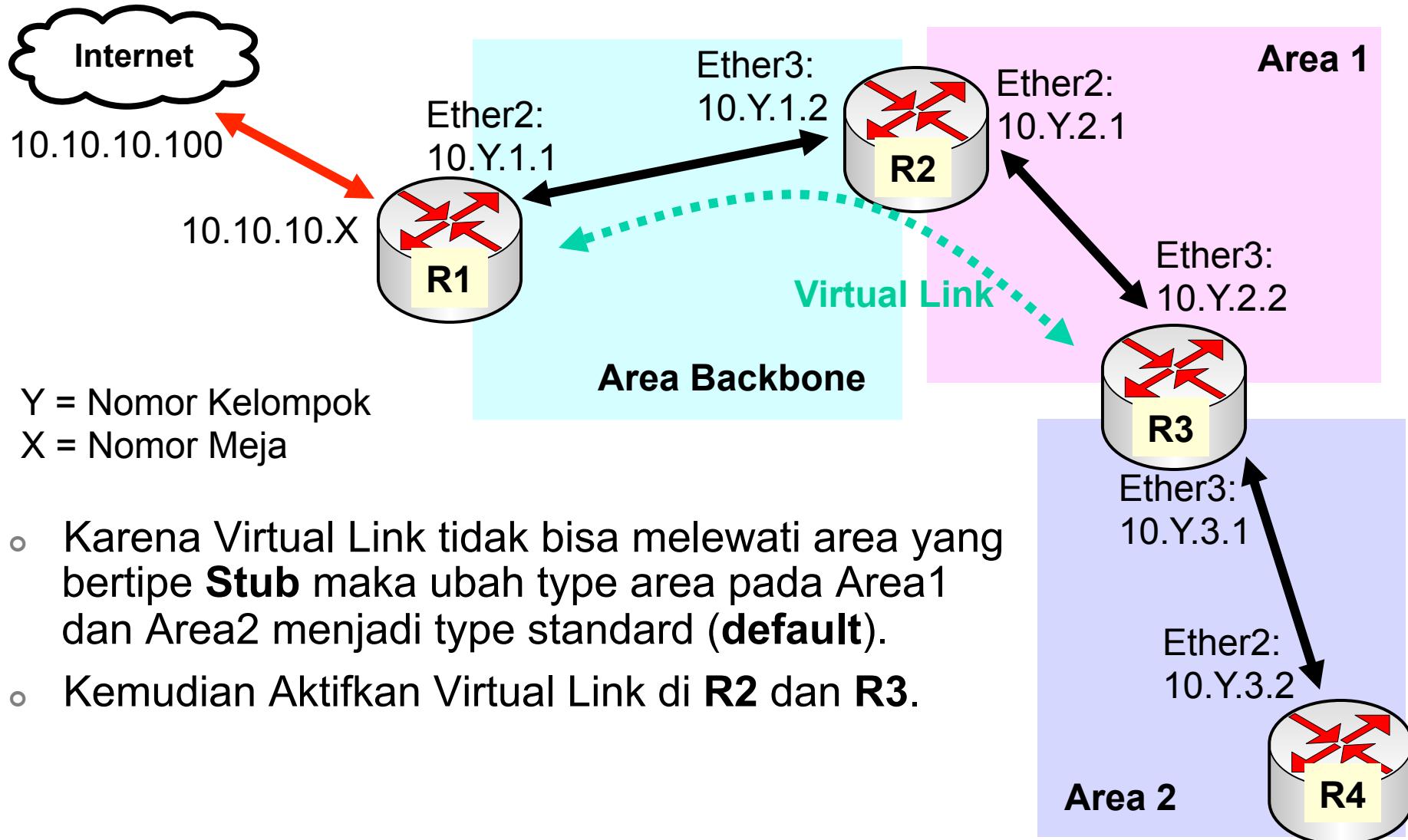




OSPF - Virtual Link

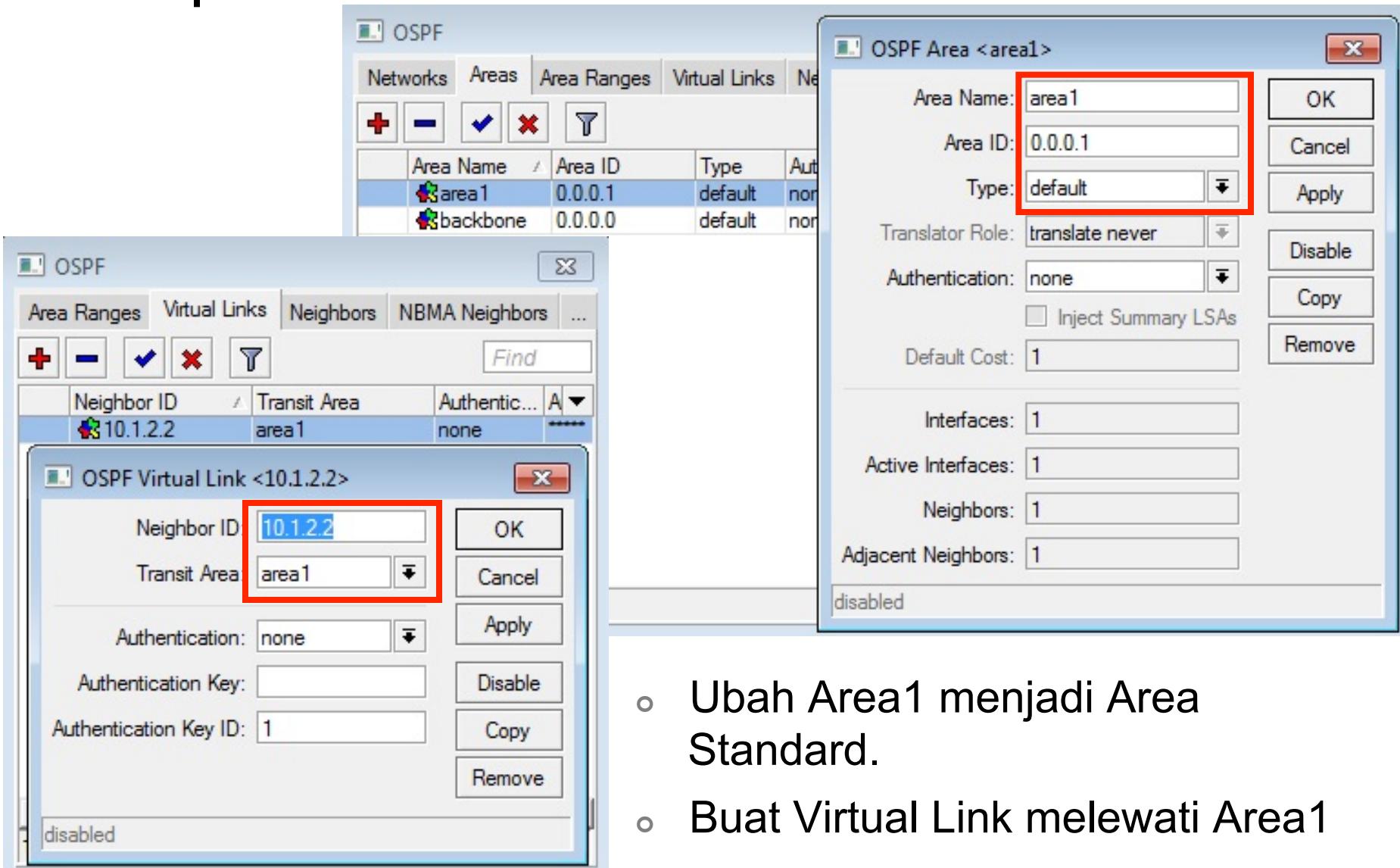
- Virtual Link → digunakan untuk mengatasi koneksi router yang terpisah (secara fisik) dari area backbone
- Juga dapat digunakan untuk menyabung area backbone yang terpisah
- Virtual Link Tidak bisa berjalan sempurna jika melewati stub area.
- Saat ini tidak berfungsi maksimal di RouterOS v4 & v5, akan diperbaiki di versi selanjutnya.

[LAB-6] OSPF – Virtual Link



- Karena Virtual Link tidak bisa melewati area yang bertipe **Stub** maka ubah type area pada Area1 dan Area2 menjadi type standard (**default**).
- Kemudian Aktifkan Virtual Link di **R2** dan **R3**.

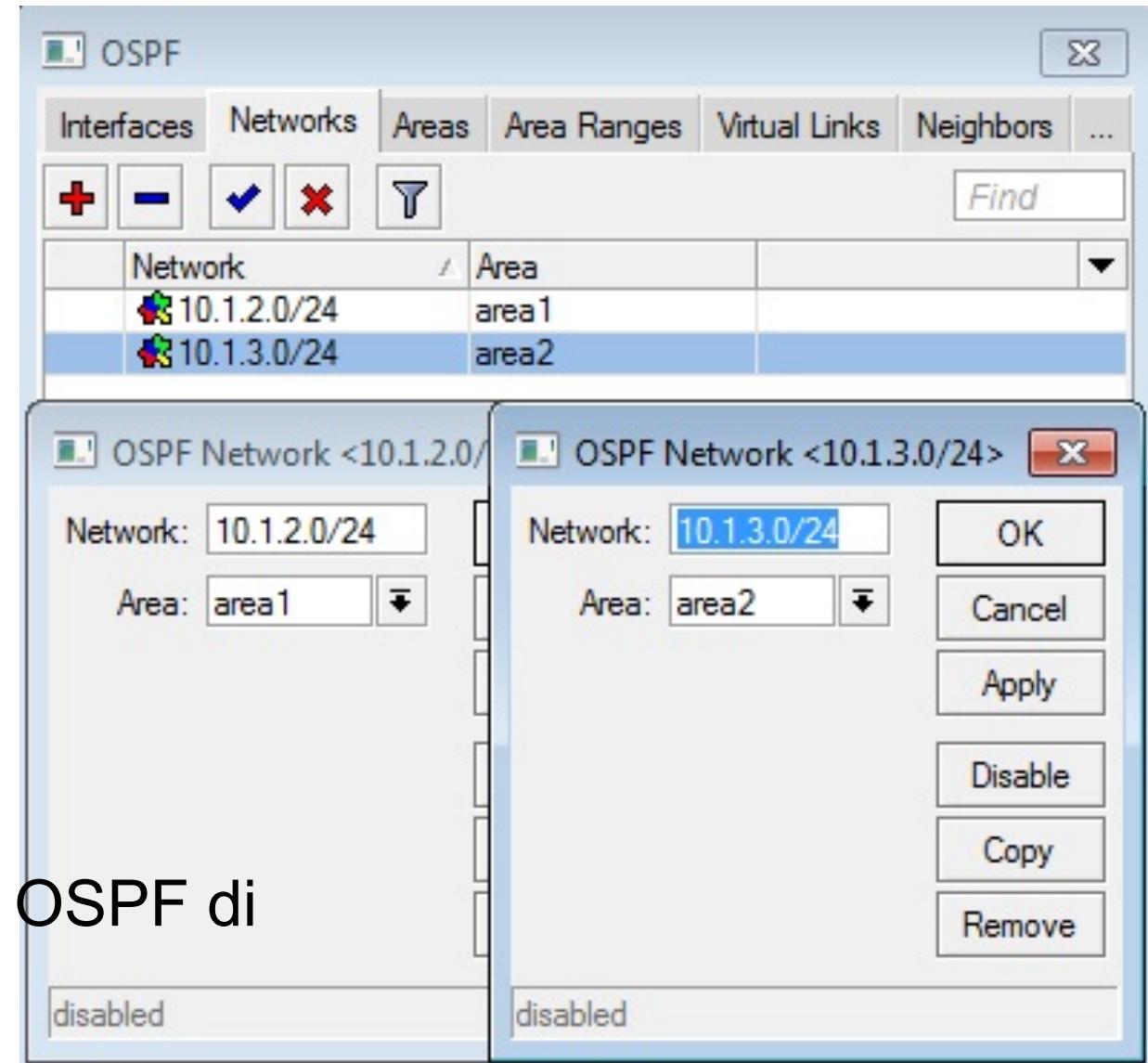
[LAB-6] R2 Configuration



[LAB-6] R3 Configuration

OSPF Area <area1>	OSPF Area <area2>
Area Name: <input type="text" value="area1"/>	Area Name: <input type="text" value="area2"/>
Area ID: <input type="text" value="0.0.0.1"/>	Area ID: <input type="text" value="0.0.0.2"/>
Type: <input type="text" value="default"/>	Type: <input type="text" value="default"/>
Translator Role: <input type="text" value="translate never"/>	Translator Role: <input type="text" value="translate never"/>
Authentication: <input type="text" value="none"/>	Authentication: <input type="text" value="none"/>
<input type="checkbox"/> Inject Summary LSAs	<input type="checkbox"/> Inject Summary LSAs
Default Cost: <input type="text" value="1"/>	Default Cost: <input type="text" value="1"/>
Interfaces: <input type="text" value="1"/>	Interfaces: <input type="text" value="1"/>
Active Interfaces: <input type="text" value="1"/>	Active Interfaces: <input type="text" value="1"/>
Neighbors: <input type="text" value="1"/>	Neighbors: <input type="text" value="1"/>
Adjacent Neighbors: <input type="text" value="1"/>	Adjacent Neighbors: <input type="text" value="1"/>
disabled	
X	
OK	
Cancel	
Apply	
Disable	
Copy	
Remove	

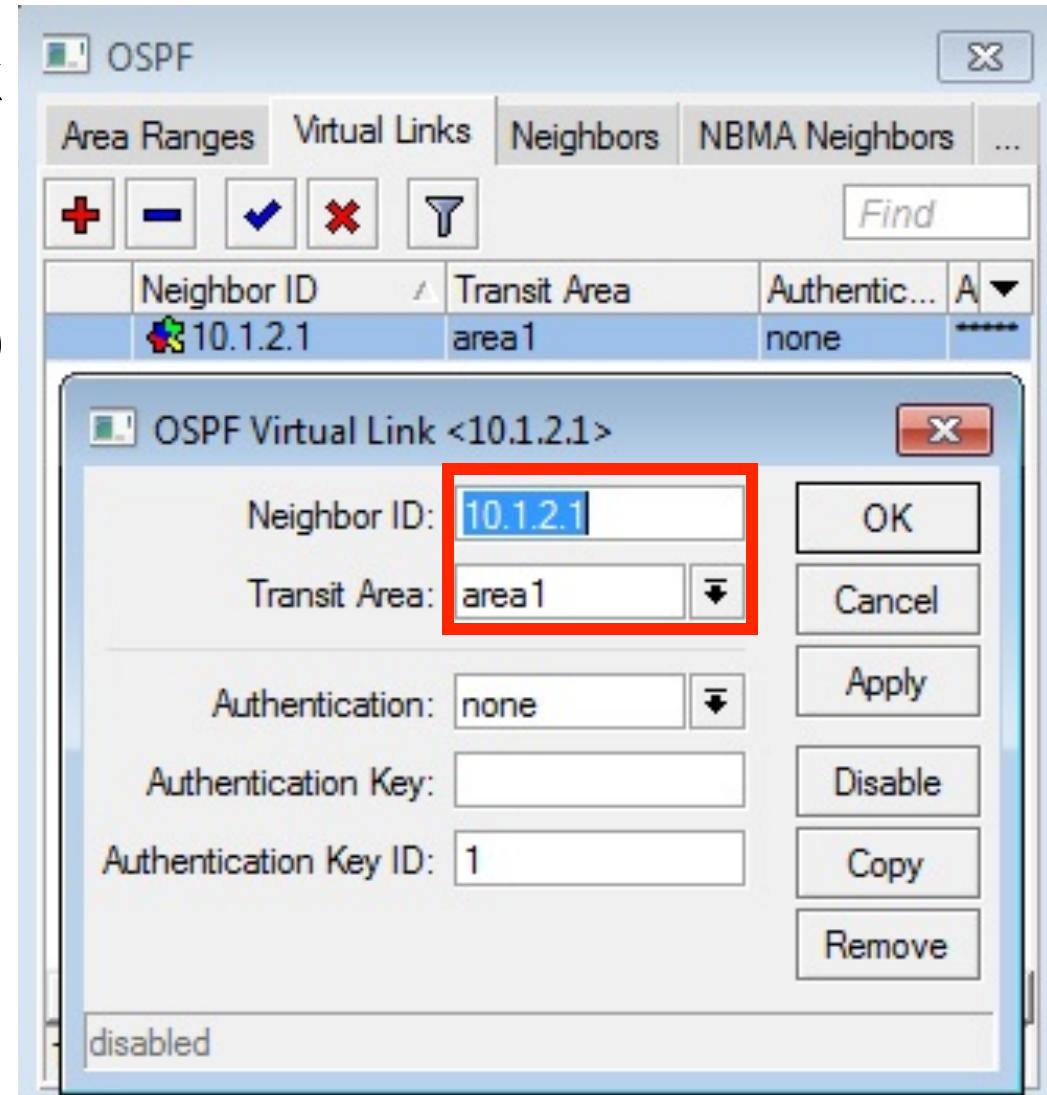
[LAB-6] R3 Configuration



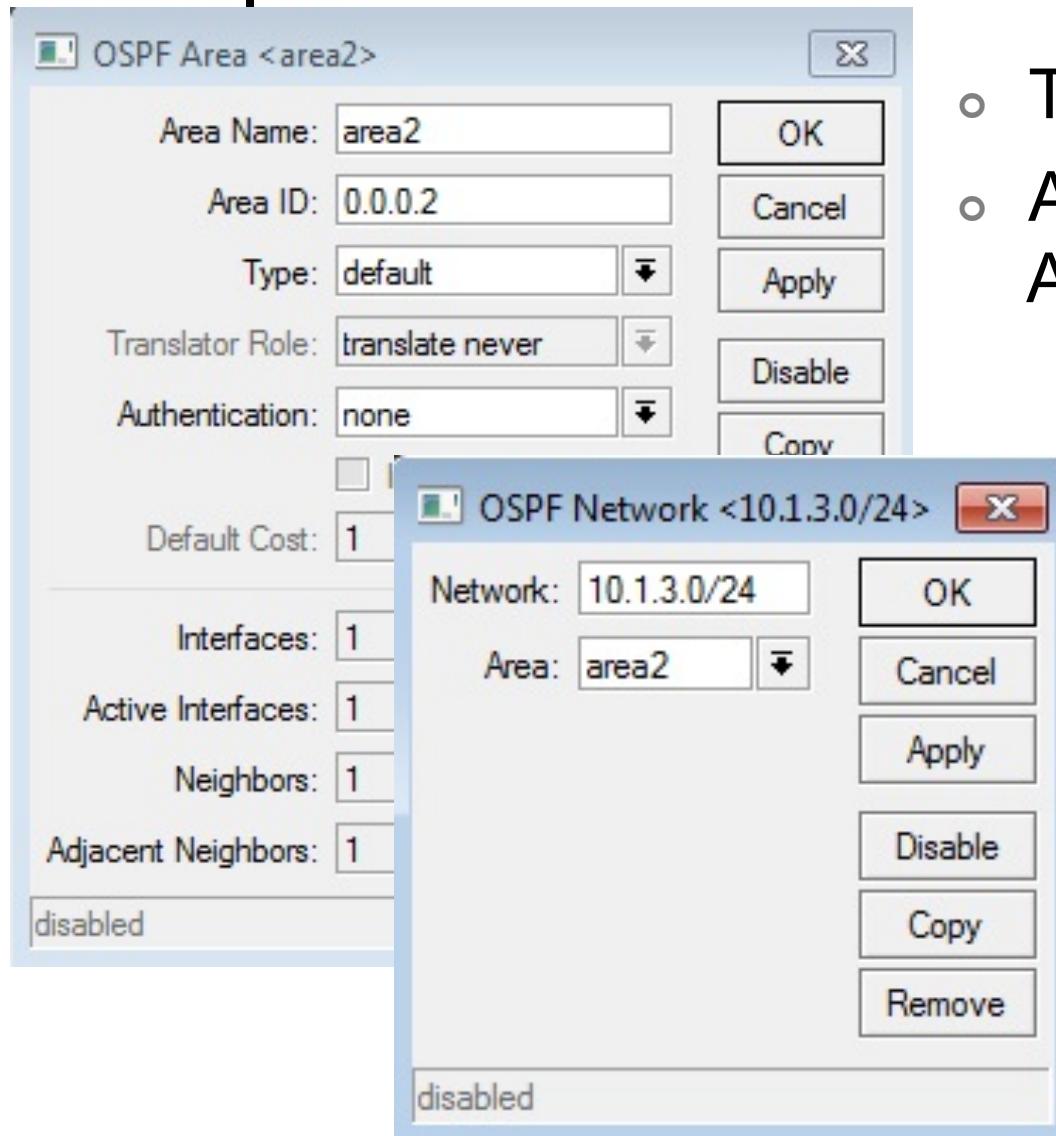
- Aktifkan network OSPF di kedua area.

[LAB-6] R3 Configuration

- Tambahkan Virtual Link memanfaatkan Area1.
- Pastikan **NeighborID** sama dengan **RouterID** yang ada di Area1.



[LAB-6] R4 Configuration



- Tambahkan **Area2** di **R4**.
- Aktifkan Network untuk Area2.



Routing Filter

- Hampir sama dengan IP firewall, routing bisa mengimplementasikan filtering terhadap informasi routing yang didistribusikan di setiap protocolnya.
- Mirip juga dengan IP firewall Urutan penempatan rule sangat berpengaruh.
- OSPF memiliki **chain default** yang digunakan untuk meletakkan filter :
 - Chain built in atau chain default “**OSPF-IN**” adalah chain untuk meletakkan filter informasi routing yang masuk.
 - Chain built in atau chain default “**OSPF-OUT**” adalah chain untuk meletakkan filter informasi routing yang keluar.
- Custom chain juga bisa dibuat sesuai kebutuhan dengan menuliskan nama chain baru secara manual.

OSPF-Filter

Route Filter <192.168.88.0>

Matchers Actions

Chain: ospf-in

Prefix: 192.168.88.0

Prefix Length: 24-32

Match Chain:

Distance:

Scope:

Target Scope:

Pref. Source:

Routing Mark:

Route Comment:

Tag:

Type

BGP

BGP Communities

Invert Match

Route Filter <192.168.88.0>

Matchers Actions

Action: discard

Jump Target:

Set Distance:

Set Scope:

Set Target Scope:

Set Pref. Source:

Set In Nexthop:

Set In Nexthop Direct:

Set Out Nexthop:

Set Routing Mark:

Set Route Comment:

Set Check Gateway:

Set Disabled:

Set Type:

▼ BGP

▼ Set BGP Communities

▼ Append BGP Communities

▼ RIP

disabled

OK Cancel Apply Disable Comment Copy Remove

Routing Filter Chain

- ● ● | ○ Beberapa parameter yang diperlukan untuk melakukan routing filter :
- Chain : Nama chain untuk meletakkan rule filter.
 - **ospf-in** – Letak chain default untuk menempatkan filter routing OSPF (input).
 - **ospf-out** – Letak chain default untuk menempatkan filter routing OSPF (output).
 - **rip-in** – Letak chain default untuk menempatkan filter routing RIP (input).
 - **rip-out** – Letak chain default untuk menempatkan filter routing RIP (output).
 - **mme-in** – Letak chain default untuk menempatkan filter routing MME (input).
 - **connected-in** – Letak chain default untuk menempatkan filter routing Direct Connect (input).
 - **dynamic-in** – Letak chain default untuk routing dynamic yang lain (Selain routing protocol dan connect directly). Biasanya untuk routing yang diinputkan dari **ppp daemon**.

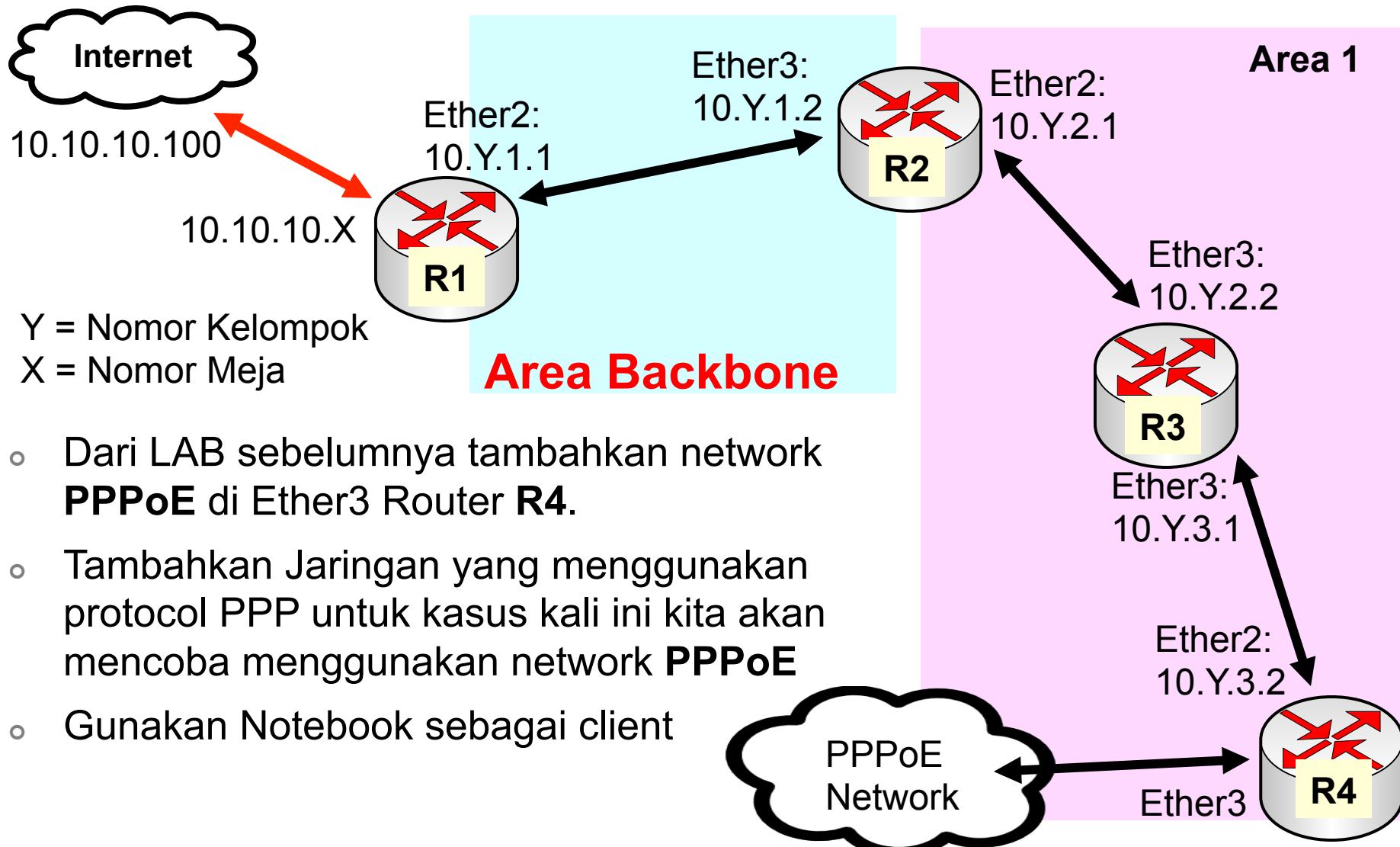
● ● ● | Routing Filter Prefix & Prefix Length

- **Prefix** adalah segmen network yang ingin difilter
 - Contoh :
 - **0.0.0.0/0** – untuk memfilter default route
 - **192.168.0.0/24** – jika tidak ada tambahan setting di **prefix-length** maka akan melakukan filter network tersebut secara spesifik.
 - **192.168.0.0** – jika tidak ada prefix segmen maka dianggap sebagai /32
- **Prefix-Length** adalah filter terhadap prefix-mask dari parameter **Prefix**. Contoh :
 - **prefix=10.0.0.0/8 prefix-length=8-32**
 - Dari rule diatas cocok dengan 10.0.0.0-10.255.255.255
 - **prefix=8.8.0.0/16 prefix-length=16-32**
 - Dari rule diatas cocok dengan 8.8.0.0-8.8.255.255

Routing Filter - Action

- **Accept** – Menerima prefix routing
- **Discard** – tidak memasukkan prefix routing ke proses pengolahan routing di FIB.
- **Jump** – Melemparkan prefix routing ke chain filter routing yang lain.
 - Jump Target – Chain tujuan yang baru.
- **Log** – Memasukkan informasi routing ke pesan Log System.
- **Passthrough** – Meneruskan informasi routing untuk di periksa di rule dibawahnya dalam chain yang sama.
- **Reject** – jika digunakan di Incoming Filter, prefix yang masuk akan disimpan di memory tetapi tidak akan diaktif. Jika Outgoing Filter, prefix tidak akan diproses sama sekali.
- **Return** – Mengembalikan prefix routing yang sebelumnya sudah terkena filter jump.

[LAB-7] OSPF – PPP Network



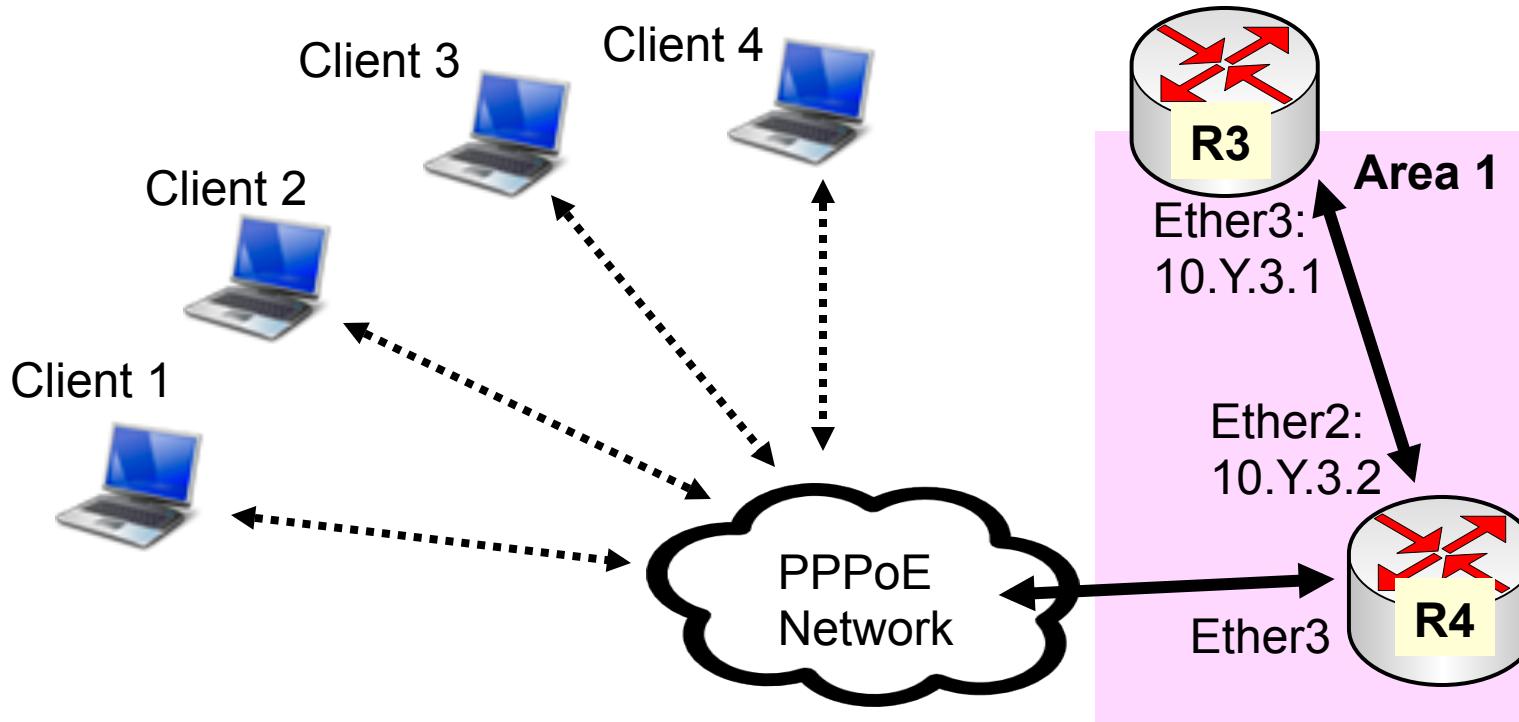
- Dari LAB sebelumnya tambahkan network **PPPoE** di Ether3 Router **R4**.
- Tambahkan Jaringan yang menggunakan protocol PPP untuk kasus kali ini kita akan mencoba menggunakan network **PPPoE**
- Gunakan Notebook sebagai client



OSPF – Filter PPP protocol

- OSPF juga bisa melakukan distribusi routing untuk network point-to-point /32 (VPN / point-to-point addressing).
- Karena sifatnya yang sangat dinamis perubahan struktur jaringan VPN (PPP) akan semakin membebani kerja protocol OSPF.
- Direkomendasikan untuk melakukan filter terhadap network jenis ini.
- Untuk distribusi routing PPPoE di OSPF kita bisa memasang IP Agregasi ke salah satu interface di router, biasanya ip agregasi tersebut dipasang di interface dimana service PPP dipasang.
- Atau bisa juga memasang **static route** dari network VPN (PPP) mengarah ke router itu sendiri.

[LAB-7] OSPF - PPP Filter



- Gunakan routing filter di OSPF untuk menghilangkan advertise network /32 karena akan membebani proses update routing.

[LAB-7] OSPF-Filter

The image displays two side-by-side windows of the 'New Route Filter' configuration in Winbox. Both windows have tabs for 'Matchers' and 'Actions'.
Left Window (Matchers Tab):

- Chain: **ospf-out** (highlighted with a red box)
- Prefix: [empty]
- Prefix Length: **32-32** (highlighted with a red box)
- Match Chain: [empty]
- Distance: [empty]
- Scope: [empty]
- Target Scope: [empty]
- Pref. Source: [empty]
- Routing Mark: [empty]
- Route Comment: [empty]
- Tag: [empty]

Right Window (Actions Tab):

- Action: **discard** (highlighted with a red box)
- Jump Target: [empty]
- Set Distance: [empty]
- Set Scope: [empty]
- Set Target Scope: [empty]
- Set Pref. Source: [empty]
- Set In Nexthop: [empty]
- Set In Nexthop Direct: [empty]
- Set Out Nexthop: [empty]
- Set Routing Mark: [empty]
- Set Route Comment: [empty]
- Set Check Gateway: [empty]
- Set Disabled: [empty]

```
/routing filter add Chain=ospf-out prefix-length=32-32 action=discard
```



Border Gateway Protocol (BGP)



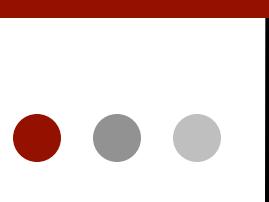
Certified Mikrotik Training Advanced Class (MTCRE)

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

Pendahuluan

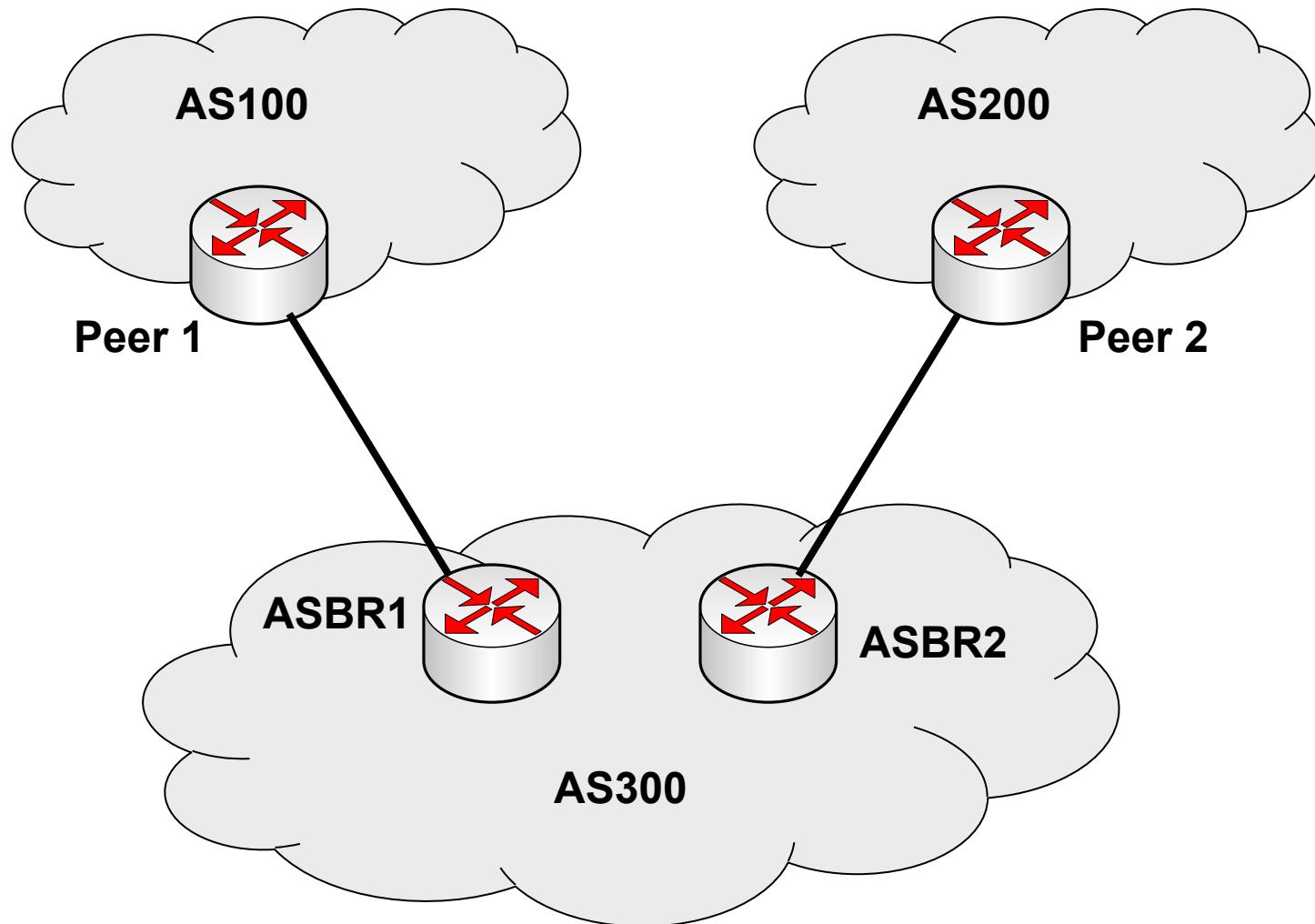
- BGP adalah protokol **routing utama** (satu-satunya) yang saat ini digunakan untuk menjalankan **Internet**.
- Dengan BGP memungkinkan internet diselenggarakan secara **desentralisasi**, sehingga tidak tergantung hanya pada satu node saja.
- BGP hanya mempertukarkan informasi routing, tidak menunjukkan network topology.



BGP

- BGP adalah Protokol Routing yang digunakan untuk bertukar informasi routing antar network yang besar (**AS**).
- Pemilihan routing berdasarkan **prefix yang paling spesifik** dan juga jarak terpendek (**AS path**).
- Mensupport **CIDR** (Classless InterDomain Routing) Routing yang tidak membedakan kelas.
- RouterOS mensupport BGPv4 RFC1771.

BGP Network

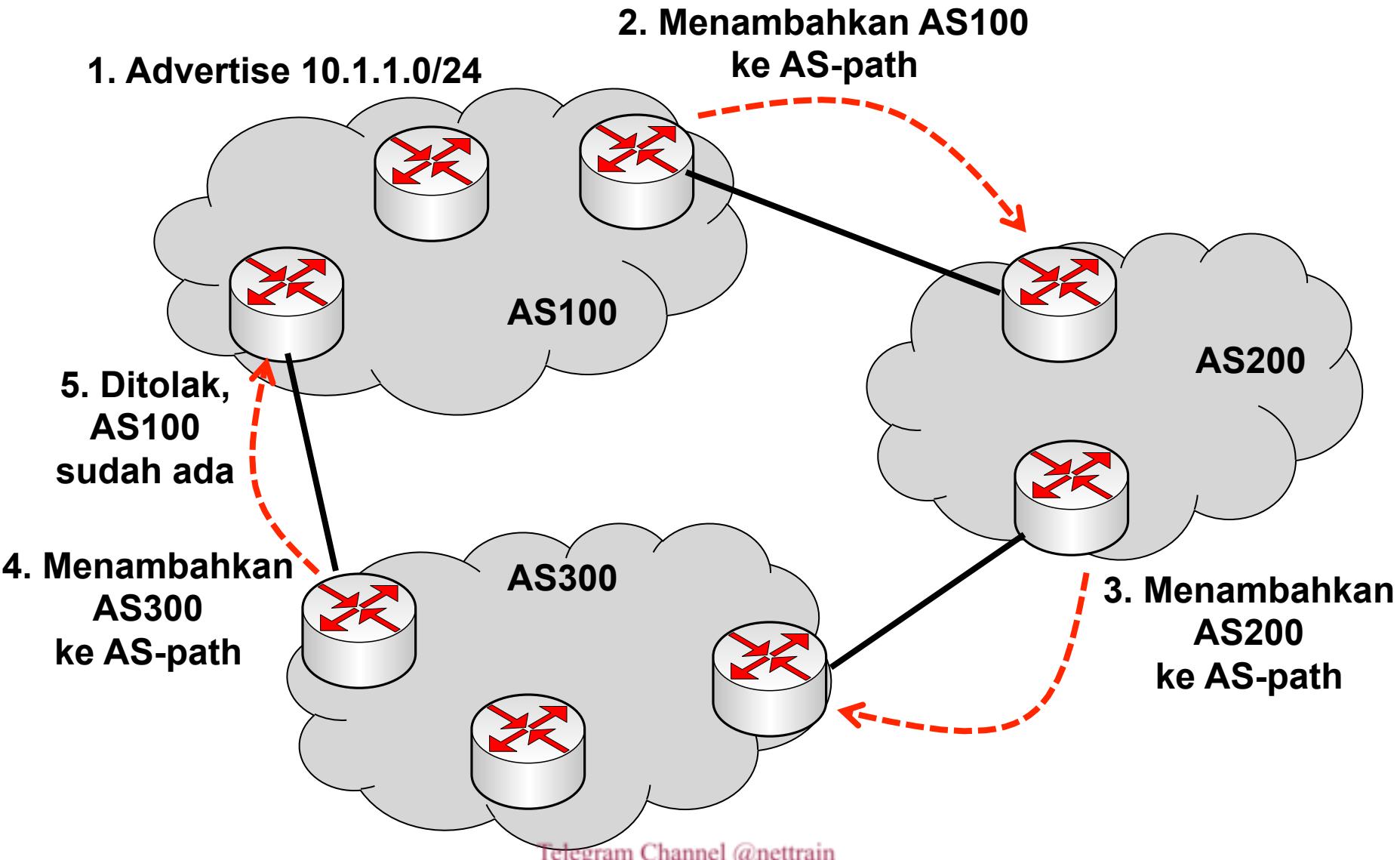




BGP

- Menggunakan protocol TCP port 179.
- Menggunakan sistem “**path vector protocol**” untuk menghitung “jarak/metric” dan menghindari loop.
- **Incremental updates**, jika terjadi perubahan routing, yang dikirimkan hanyalah updatenya saja, bukan keseluruhan informasi routing.

Path Vector Implementation



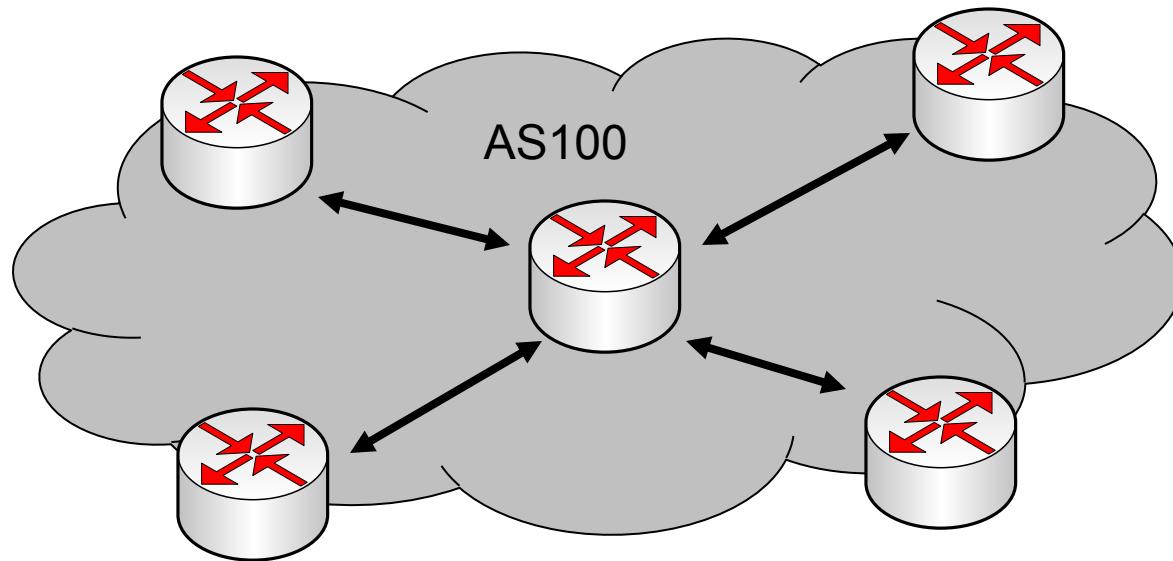
Telegram Channel @nettrain



Kebutuhan BGP

- Kita butuh menggunakan BGP bila:
 - Network dual/multihomed (terkoneksi ke satu atau beberapa AS).
 - Memiliki alokasi IP Address Public sendiri yang akan diadvertised ke Internet.

Autonomous System (AS)



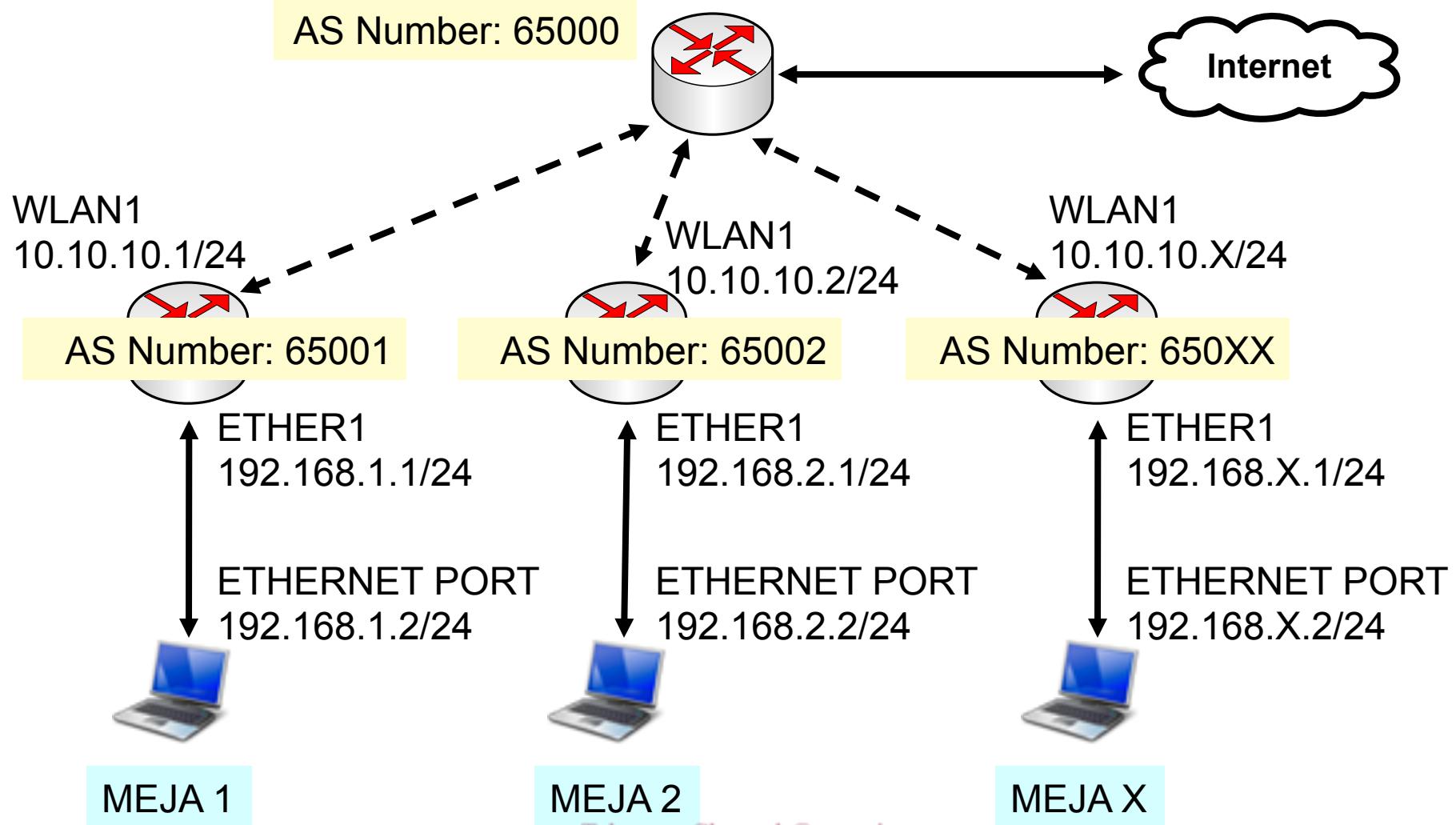
- **AS** Merupakan gabungan dari jaringan yang biasanya dalam satu kepemilikan atau kontrol yang memiliki sistem routing yang serupa.



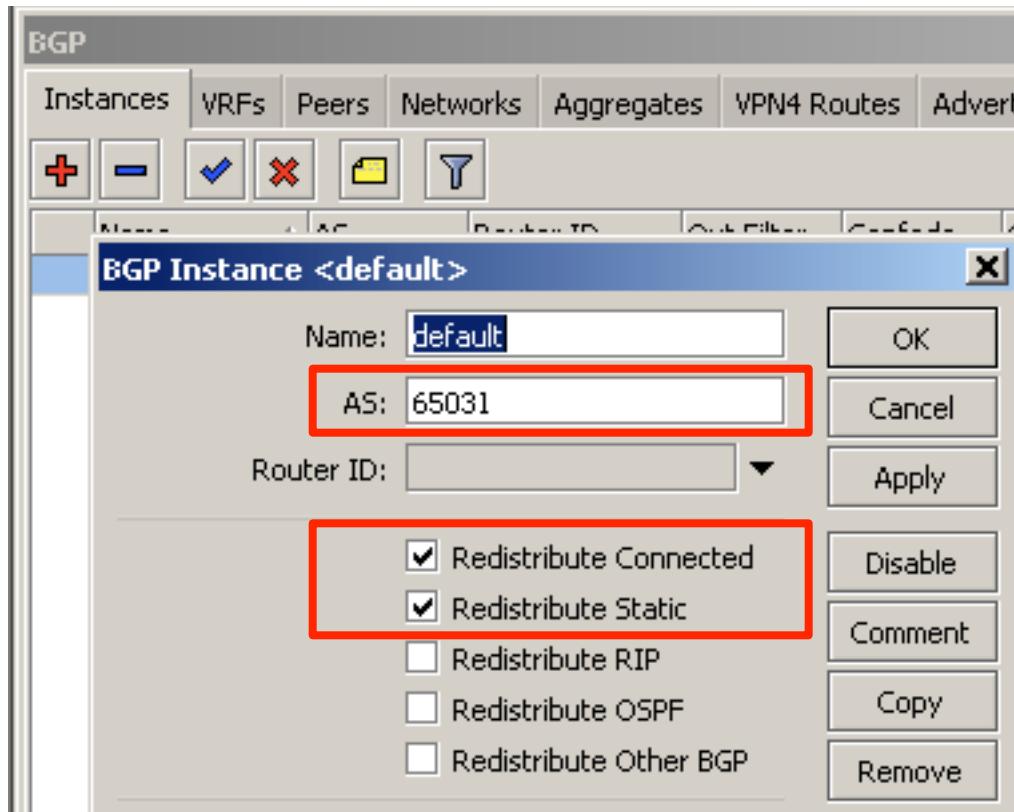
AS Number

- Awalnya, **AS number** menggunakan 2 bit, namun saat ini sedang beralih menjadi 4 bit.
 - 2 bit AS: 0 - 65,535
 - 4 bit AS: 65,536 - 4,294,967,295
- RoS mensupport 2 bit dan 4 bit AS number
- IANA menentukan **AS-64512** sampai **AS-65535** adalah AS private, selain itu adalah AS publik.

[LAB-1] BGP Peer



[LAB-1] BGP Instances



- Ubah AS Number sesuai dengan X urutan meja
- Aktifkan pendistribusian **Connected Route** dan **Static route**

[LAB-1] BGP Peer

BGP

Instances VRFS Peers Networks Aggregates VPN4 Routes Advertisements

+ - ✓ ✗ F Refresh Refresh All Resend Resend All Find

Name	Instance	Remote Address	Remote AS	M...	R...	TTL	Remote ID	Uptime	Prefix Co...	State
peer-to-g...	default	10.10.10.100	65000	no	no	d...	10.10.10.100	00:05:47	5	established

BGP Peer <peer-to-gateway>

General Advanced Status

Name: peer-to-gateway
Instance: default
Remote Address: 10.10.10.100

Remote Port:
Remote AS: 65000
TCP MD5 Key:
Nexthop Choice: default

Multihop
 Route Reflect

OK Cancel Apply Disable Comment Copy Remove Refresh Refresh All

1 item ()

[LAB-1] Routing Table

Route List

	Dst. Address	Gateway	Distance	Pref. Source
AS	0.0.0.0/0	10.10.10.100 reachable wlan1	1	
DAC	10.10.10.0/24	wlan1 reachable	0	10.10.10.31
Db	10.10.10.0/24	10.10.10.100 reachable wlan1	20	
DAC	10.20.20.0/24	wlan2 reachable	0	10.20.20.31
Db	10.20.20.0/24	10.10.10.100 reachable wlan1	20	
DAb	10.100.100.1	10.10.10.100 reachable wlan1	20	
DAb	192.168.0.0/24	10.10.10.100 reachable wlan1	20	
DAC	192.168.31.0/24	ether1 unreachable	0	192.168.31.1
DAb	192.168.32.0/24	10.10.10.32 reachable wlan1	20	

Route <192.168.32.0/24>

General Attributes

BGP AS Path: 65000,65032

BGP Weight:

Menunjukkan asal BGP Router yang mengadvertise prefix tersebut

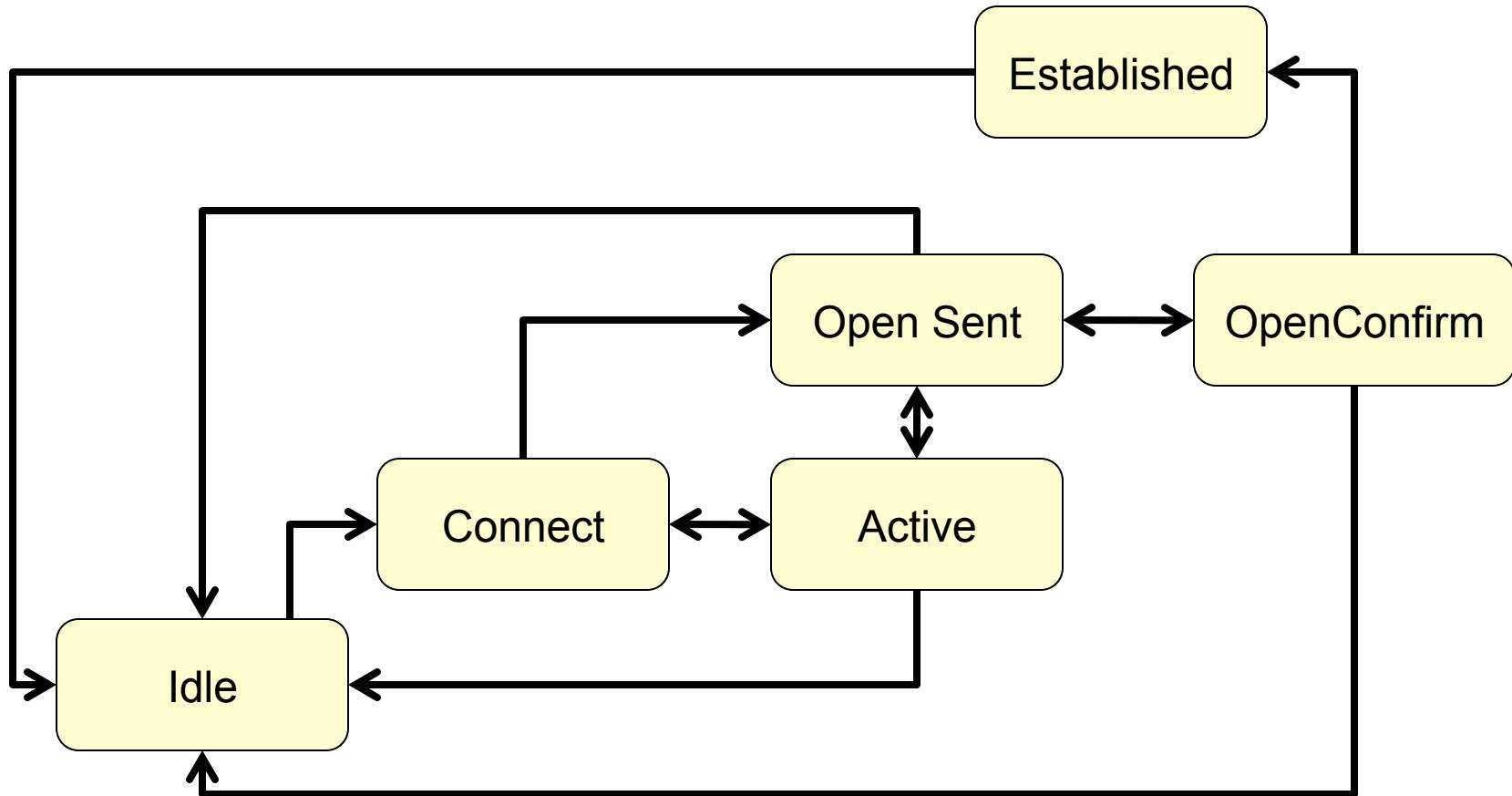
Default Route ?

- By default, kita tidak akan pernah mengadvertisekan default route, ataupun menerima default route via BGP.
- Jika ingin mendistribusikan default gateway bisa diaktifkan option default originate.
- `/routing bgp peer
set peer1 default originate=always`
 - **always** – Router akan menjadi default gateway dari peer yang terkoneksi.
 - **if-installed** – Router akan menjadi default gateway jika ada rule default gateway yang terpasang di tabel routing.
 - **never** – tidak menjadi default gateway.
- Untuk keamanan Lakukanlah filter in/out untuk menolak default route, kecuali memang dibutuhkan.

BGP Finite State Machine

- **Idle**: tidak terhubung, semua koneksi transport (TCP) terputus.
- **Connect**: mulai membuka tcp connection, namun belum terhubung.
- **Active**: tidak berhasil membuat tcp connection, menunggu waktu connect ulang
- **Open Sent**: mengirimkan pesan pembuka, menunggu konfirmasi
- **Open Confirm**: proses saling bertukar keep alive time
- **Established**: terkoneksi dan saling mengirimkan update

BGP Finite State Machine

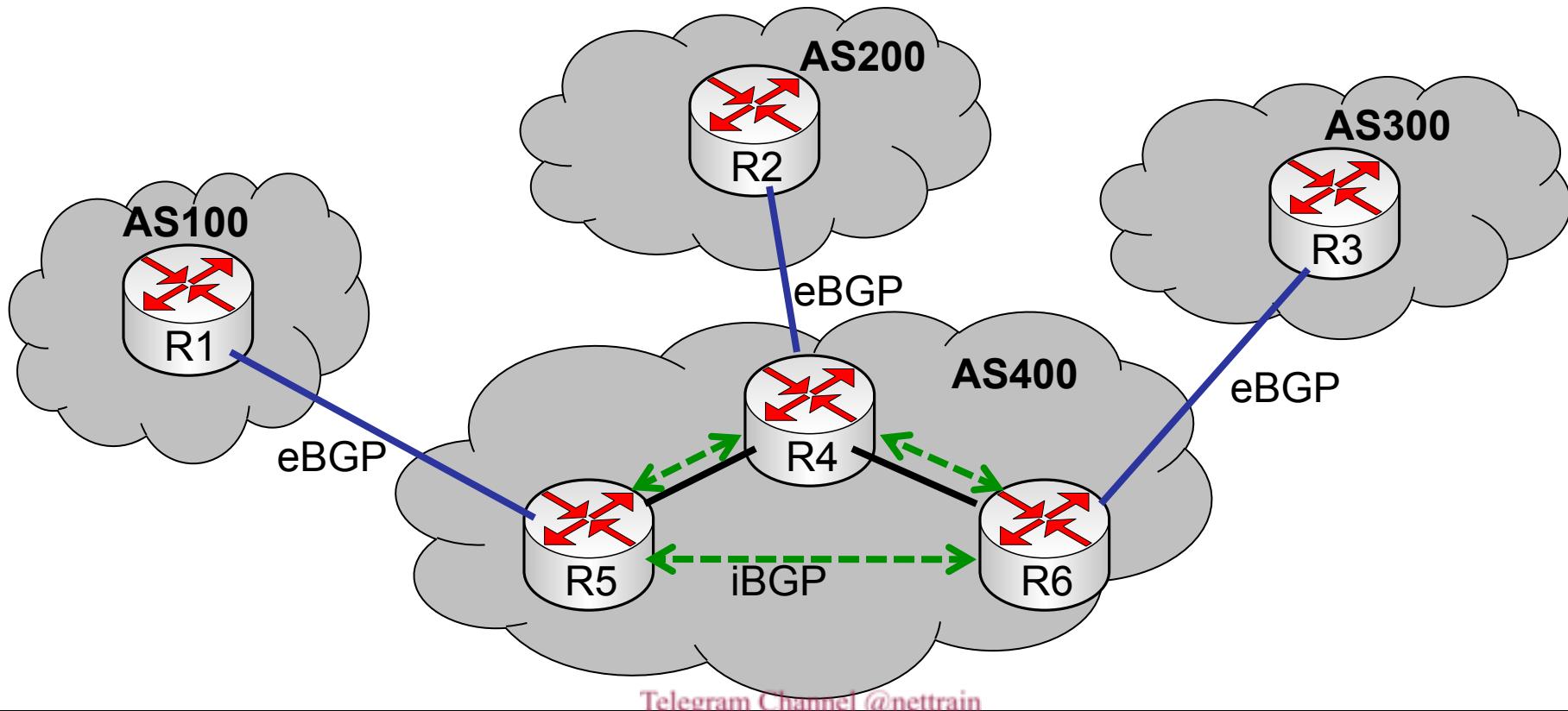


http://en.wikipedia.org/wiki/Border_Gateway_Protocol#Finite-state_machine

Telegram Channel @nettrain

Internal & External BGP

- **iBGP**: peering antar router di dalam AS
- **eBPG**: peering router yg berbeda AS



Telegram Channel @nettrain



External BGP

- Peer dilakukan oleh dua buah router yang berbeda AS.
- AS number akan ditambahkan ke AS path dari routing yang diadvertise.
- By default, next hop akan menggunakan “self”

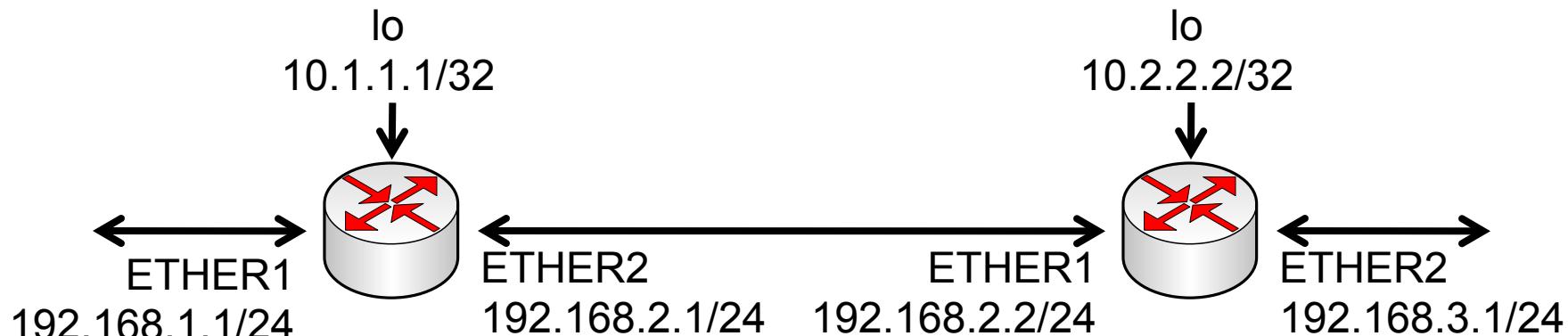


Internal BGP

- Sesama peer tidak harus terkoneksi secara langsung (multi hop).
- iBGP **speaker** (router yang saling melakukan peering) harus terhubung secara **mesh** (terhubung ke lebih dari satu node) dengan penuh.
- Peer dilakukan dengan loopback address
- Jika tidak dapat terhubung dengan full mesh, bisa menggunakan **route-reflect=yes**

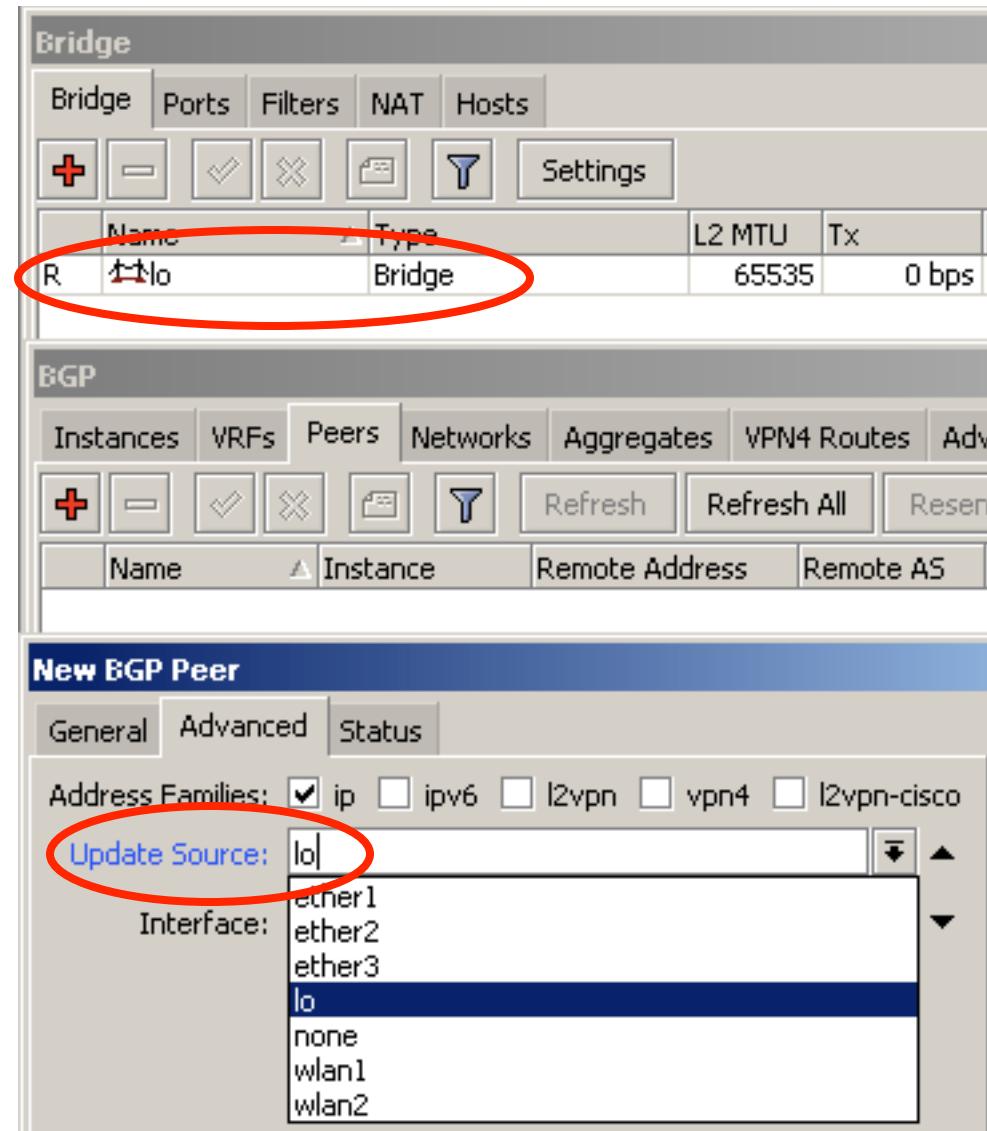
Loopback

- Untuk peer yang tidak terkoneksi langsung (multihops), biasanya kita menggunakan IP BGP pada interface loopback, supaya interkoneksi tidak tergantung pada interface.



Loopback

- Interface loopback di routerOS bisa dibuat menggunakan bridge tanpa port
- Peer “update-source” ke interface loopback



[LAB-2] Loopback Address

- Ubahlah IP BGP Router Anda menggunakan loopback address.
 - Buatlah bridge interface “lo”
 - Pasang IP Address loopback di bridge interface tersebut: 172.16.0.X
 - Buatlah statik route untuk “menjangkau” IP BGP Peer
 - Ubah IP BGP Peer menjadi loopback : 172.16.0.100 dan pilih update-source=“lo”

Bridge & IP loopback

The screenshot shows the Winbox interface for managing network configurations on a MikroTik device. It consists of two main sections: 'Bridge' and 'Address List'.

Bridge Table:

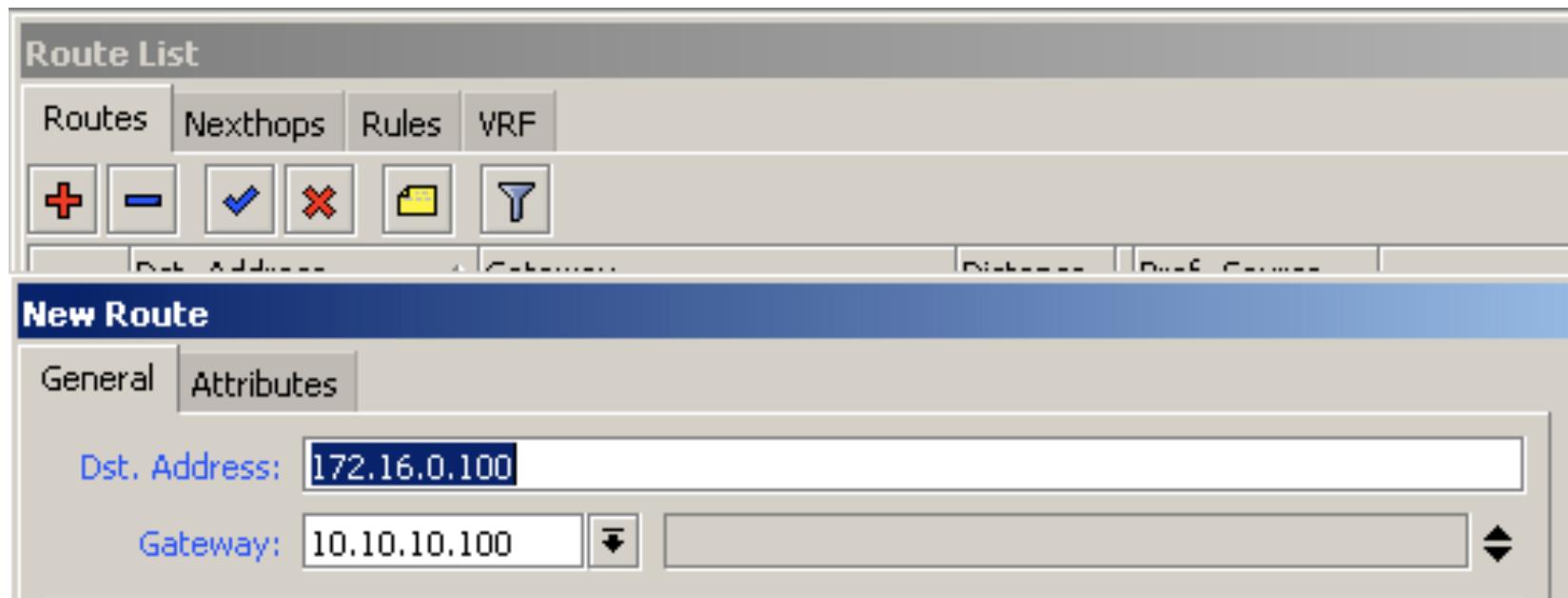
	Name	Type	L2 MTU	Tx	Rx	Tx P
R	1lo	Bridge	65535	0 bps	0 bps	

Address List Table:

	Address	Network	Broadcast	Interface
	10.10.10.31/24	10.10.10.0	10.10.10.255	wlan1
	10.20.20.31/24	10.20.20.0	10.20.20.255	wlan2
	172.16.0.31	172.16.0.31	172.16.0.31	lo
	192.168.31.1/24	192.168.31.0	192.168.31.255	ether1

Menambahkan static route

- /ip route add dst-address=172.16.0.100 gateway=10.10.10.100



Instance & Peer Setting

BGP Peer <peer-to-gateway>	BGP Peer <peer-to-gateway>
General Advanced Status	General Advanced Status
Name: peer-to-gateway	Address Families: <input checked="" type="checkbox"/> ip <input type="checkbox"/> ipv6 <input type="checkbox"/> l2vpn <input type="checkbox"/> vpn4 <input type="checkbox"/> l2vpn-cisco
Instance: default	Update Source: lo
Remote Address: 172.16.0.100	Interface:
Remote Port:	
Remote AS: 65000	
TCP MD5 Key:	
Nexthop Choice: default	
<input checked="" type="checkbox"/> Multihop	
<input type="checkbox"/> Route Reflect	

Routing Table

Route List

Routes Nexthops Rules VRF

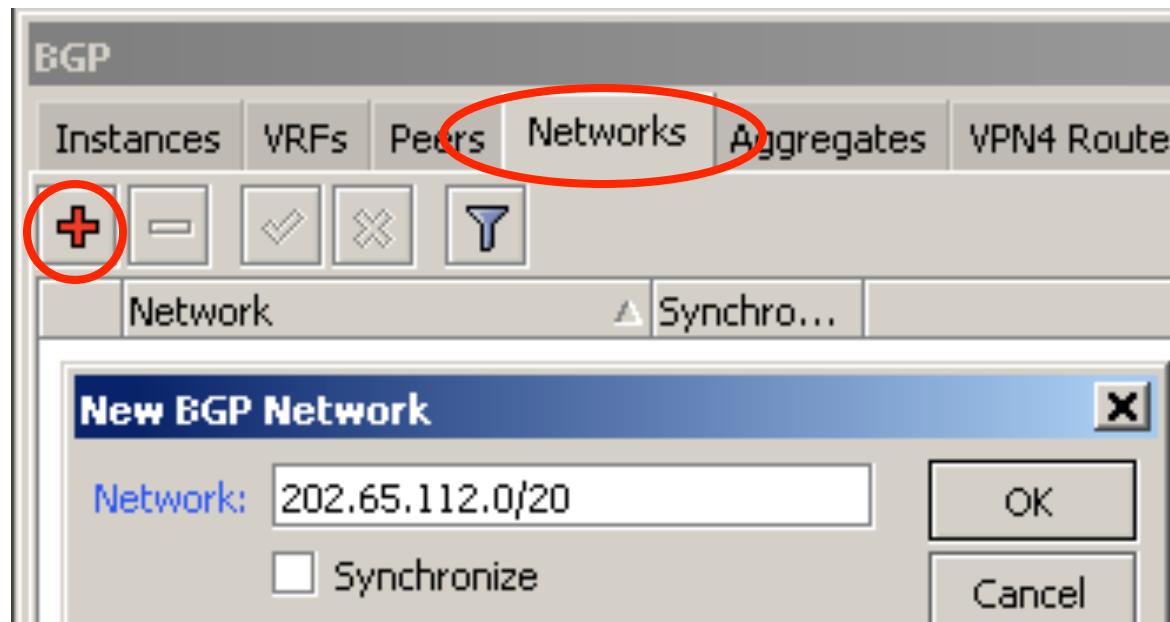
+ - ✓ ✘ Find all

	Dst. Address	Gateway	Distance	Pref. Source
XS	▶ 0.0.0.0/0	10.10.10.100	1	
DAb	▶ 0.0.0.0/0	172.16.0.100 recursive via 10.10.10.100 wlan1	20	
DAC	▶ 10.10.10.0/24	wlan1 reachable	0	10.10.10.31
Db	▶ 10.10.10.0/24	172.16.0.100 recursive via 10.10.10.100 wlan1	20	
DAC	▶ 10.20.20.0/24	wlan2 reachable	0	10.20.20.31
Db	▶ 10.20.20.0/24	172.16.0.100 recursive via 10.10.10.100 wlan1	20	
DAb	▶ 10.100.100.1	172.16.0.100 recursive via 10.10.10.100 wlan1	20	
DAC	▶ 172.16.0.31	lo reachable	0	172.16.0.31
Db	▶ 172.16.0.31	172.16.0.100 recursive via 10.10.10.100 wlan1	20	
DAb	▶ 172.16.0.32	172.16.0.100 recursive via 10.10.10.100 wlan1	20	
AS	▶ 172.16.0.100	10.10.10.100 reachable wlan1	1	
Db	▶ 172.16.0.100	172.16.0.100 recursive via 10.10.10.100 wlan1	20	
DAb	▶ 192.168.0.0/24	172.16.0.100 recursive via 10.10.10.100 wlan1	20	
DAC	▶ 192.168.31.0/24	ether1 unreachable	0	192.168.31.1
Db	▶ 192.168.32.0/24	172.16.0.32 unreachable	20	

15 items (1 selected)

BGP Network

- Dengan BGP, kita bisa mengadvertise kelompok IP Address dan subnet, meskipun IP tersebut tidak terpasang pada router ataupun kita tidak memiliki static route.

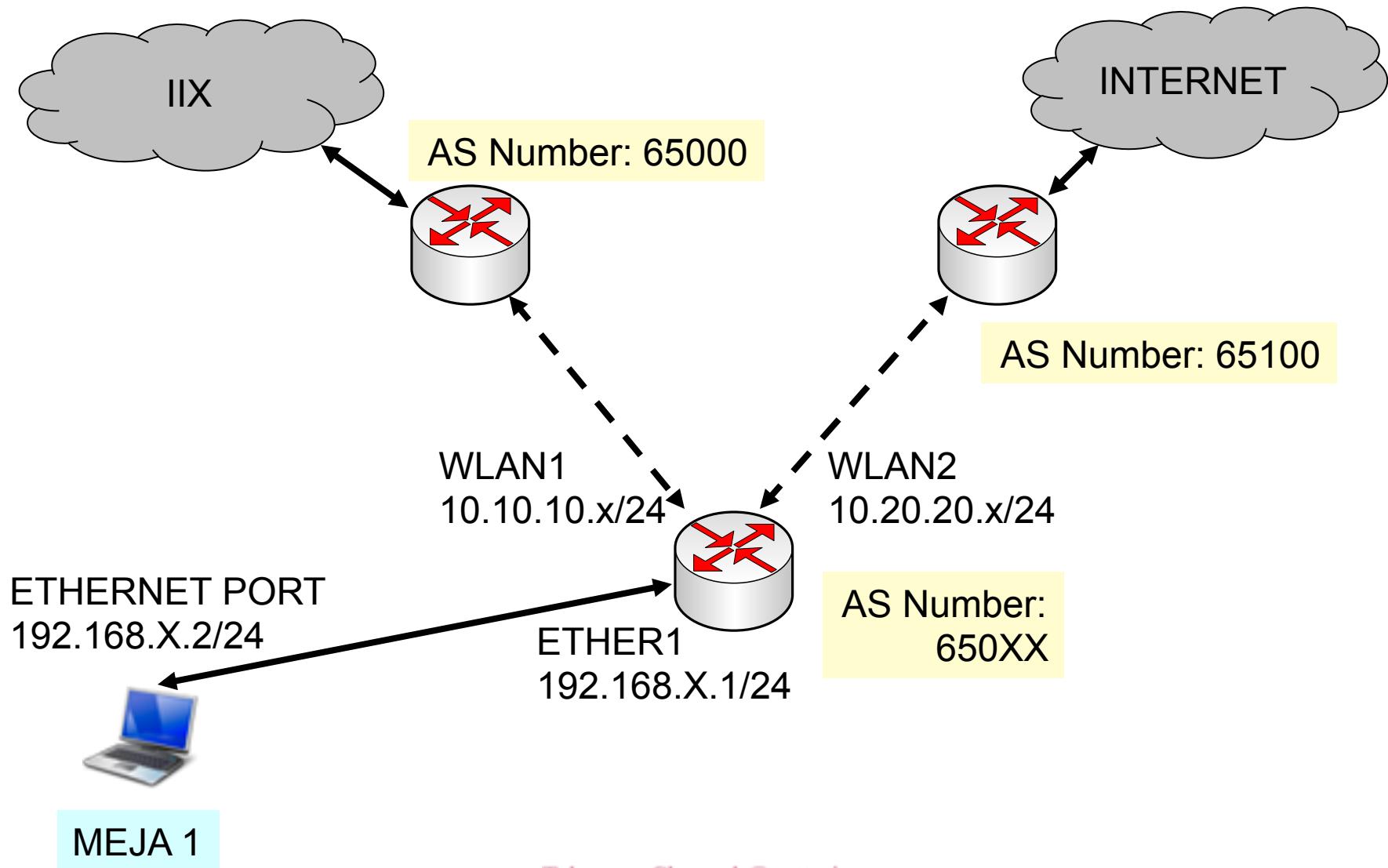


BGP Filter

- Untuk mengatur prefix routing mana saja yang boleh/tidak boleh diterima/diadvertise, kita bisa membuat **Routing Filter**.



[LAB-3] BGP Peer IIX



Static Route

- Aktifkan masquerade pada wlan1 dan wlan2
- Pindahkan Default gateway ke 10.20.20.100 (koneksi wireless wlan2)

Route List						
	Routes	Nexthops	Rules	VRF		
	Dst. Address	Gateway		Distance	Pref.	Source
AS	► 0.0.0.0/0	10.20.20.100 reachable wlan2		1		
DAC	► 10.10.10.0/24	wlan1 reachable		0		10.10.10.31
Db	► 10.10.10.0/24	172.16.0.100 recursive via 10.10.10.100 wlan1		20		
DAC	► 10.20.20.0/24	wlan2 reachable		0		10.20.20.31
Db	► 10.20.20.0/24	172.16.0.100 recursive via 10.10.10.100 wlan1		20		
DAb	► 10.100.100.1	172.16.0.100 recursive via 10.10.10.100 wlan1		20		
DAb	► 27.50.16.0/20	172.16.0.100 recursive via 10.10.10.100 wlan1		20		
DAC	► 10.10.10.0/24	172.16.0.100 recursive via 10.10.10.100 wlan1		20		

Test Traceroute

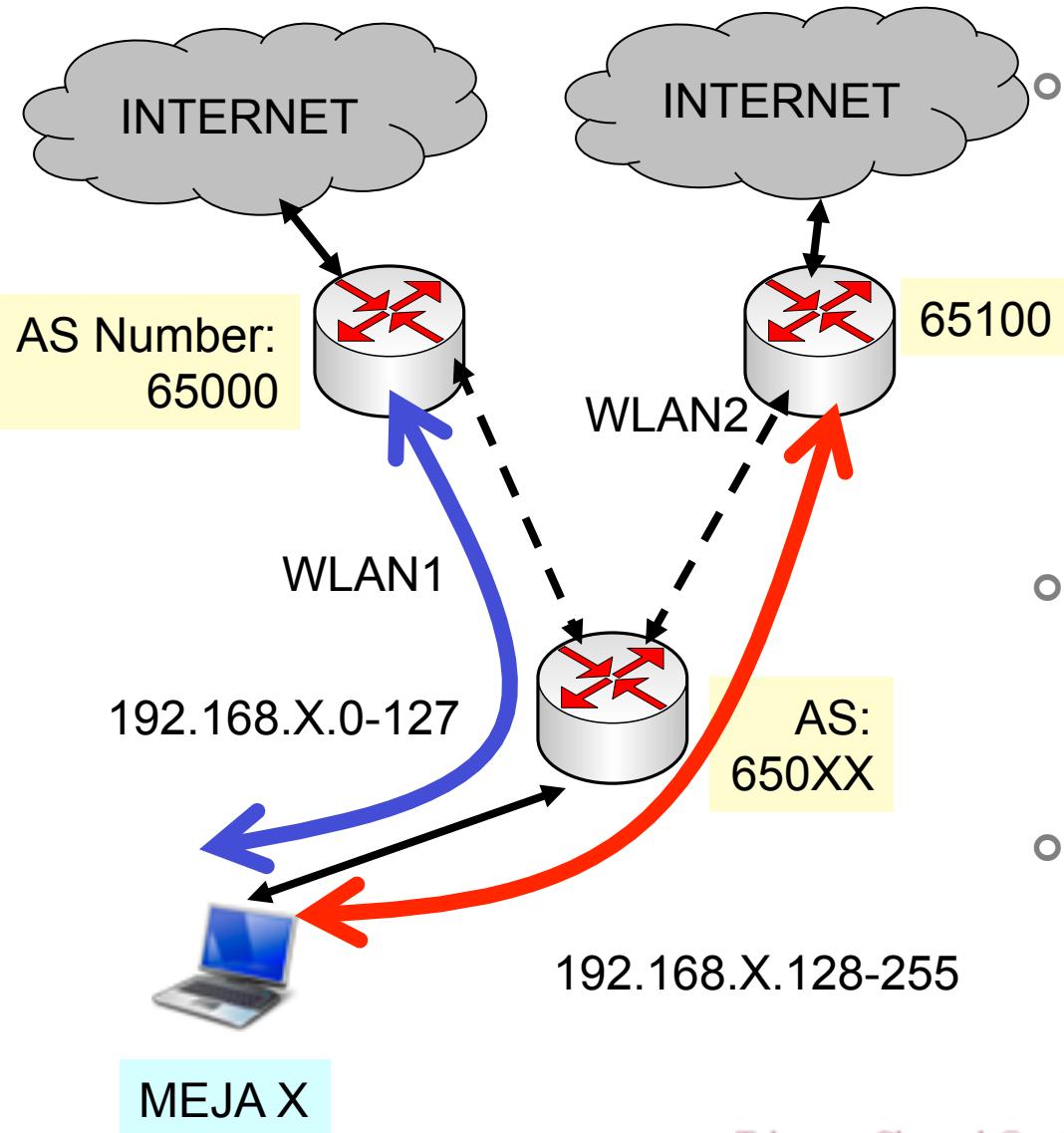
```
[admin@C31] > tool traceroute www.yahoo.com
```

	ADDRESS		STATUS		
1	10.20.20.100	5ms	8ms	9ms	
2	192.168.0.100	3ms	10ms	10ms	
3	202.65.113.1	8ms	15ms	3ms	

```
[admin@C31] > tool traceroute www.mikrotik.co.id
```

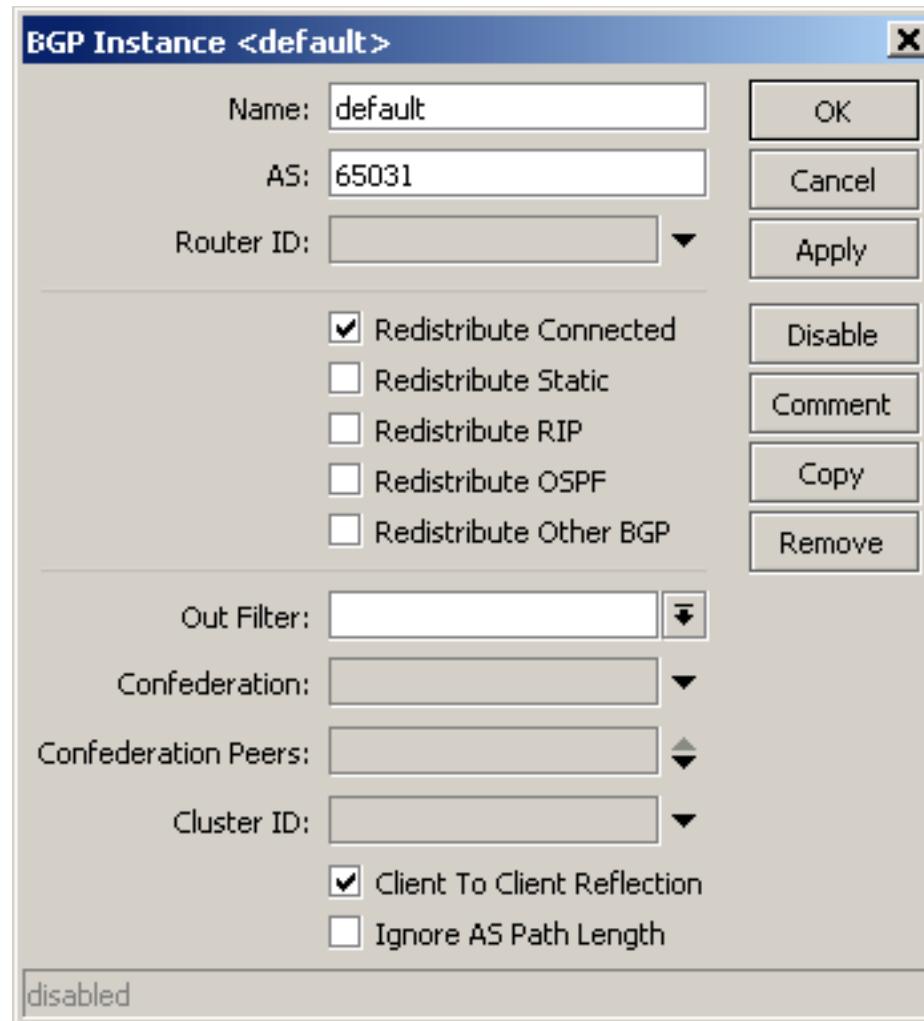
	ADDRESS		STATUS		
1	10.10.10.100	2ms	4ms	7ms	
2	192.168.0.100	1ms	8ms	9ms	
3	202.65.113.1	9ms	12ms	13ms	

[LAB-4] Advertisement



- Buatlah peer di kedua AS 65000 dan 65100 digunakan untuk downstream subnet client yg berbeda.
- Dipermudah dengan menggunakan IP interface
- Buatlah sistem failover antar gateway

BGP Instance



BGP Network

- Untuk memisahkan menjadi 2 subnet, kita menggunakan BGP network (Advertisement)

The screenshot shows the MikroTik BGP configuration interface. The top navigation bar has tabs: Instances, VRFs, Peers, Networks, Aggregates, VPN4 Routes, and Advertisements. The Networks tab is selected. Below the tabs are several icons: a red plus sign (+), a minus sign (-), a checkmark, an X, and a filter icon. A table below lists two network entries:

	Network	Synchro...
	192.168.31.0/25	no
	192.168.31.128/25	no

Routing Filter

- Untuk memilih network prefix mana yang di advertise ke masing-masing gateway, digunakan routing filter.

Route Filters							
#	Chain	Prefix	Prefix Length	Protocol	BGP AS Path	Action	
0	wlan2-out	192.168.31.0/25	25			discard	
1	wlan1-out	192.168.31.128/25	25			discard	

BPG Peer

The screenshot shows the BGP configuration window in Winbox. The title bar says "BGP". The top menu has tabs: Instances, VRFs, Peers (which is selected), Networks, Aggregates, VPN4 Routes, and Advertisements. Below the tabs are several buttons: a red plus sign (+), a minus sign (-), a checkmark, a delete icon (X), a folder icon, a filter icon, Refresh, Refresh All, Resend, Resend All, and a Find button. The main table lists BGP peers:

Name	Instance	Remote Address	Remote AS	Multi...	..	TTL	Remote ID	Uptime	.State
peer-wlan1	default	10.10.10.100	65000	no	no	d...	10.10.10.100	00:09:57	established
peer-wlan2	default	10.20.20.100	65100	no	no	d...	10.20.20.100	00:09:56	established

Routing Table di Gateway

Route List					
	Routes	Nexthops	Rules	VRF	
AS	▶ 0.0.0.0/0	192.168.0.100 reachable ether1			1
DAC	▶ 10.10.10.0/24	wlan1 reachable			0
Db	▶ 10.10.10.0/24	10.10.10.31 reachable wlan1			20
Db	▶ 10.10.10.0/24	10.20.20.31 reachable wlan2			20
Db	▶ 10.20.20.0/24	10.10.10.31 reachable wlan1			20
DAC	▶ 10.20.20.0/24	wlan2 reachable			0
Db	▶ 10.20.20.0/24	10.20.20.31 reachable wlan2			20
DAC	▶ 10.100.100.1	dns-server reachable			0
XS	▶ 172.16.0.31	10.10.10.31			1
DAb	▶ 172.16.0.31	10.10.10.31 reachable wlan1			20
Db	▶ 172.16.0.31	10.20.20.31 reachable wlan2			20
XS	▶ 172.16.0.32	10.10.10.32			1
DAC	▶ 172.16.0.100	lo reachable			0
DAC	▶ 192.168.0.0/24	ether1 reachable			0
DAb	▶ 192.168.31.0/24	10.10.10.31 reachable wlan1			20
Db	▶ 192.168.31.0/24	10.20.20.31 reachable wlan2			20
DAb	▶ 192.168.31.0/25	10.10.10.31 reachable wlan1			20
DAb	▶ 192.168.31.128/25	10.20.20.31 reachable wlan2			20

Route Mark

- BGP Advertisement hanya mengatur jalur downlink saja, untuk mengatur uplink, gunakanlah policy route.

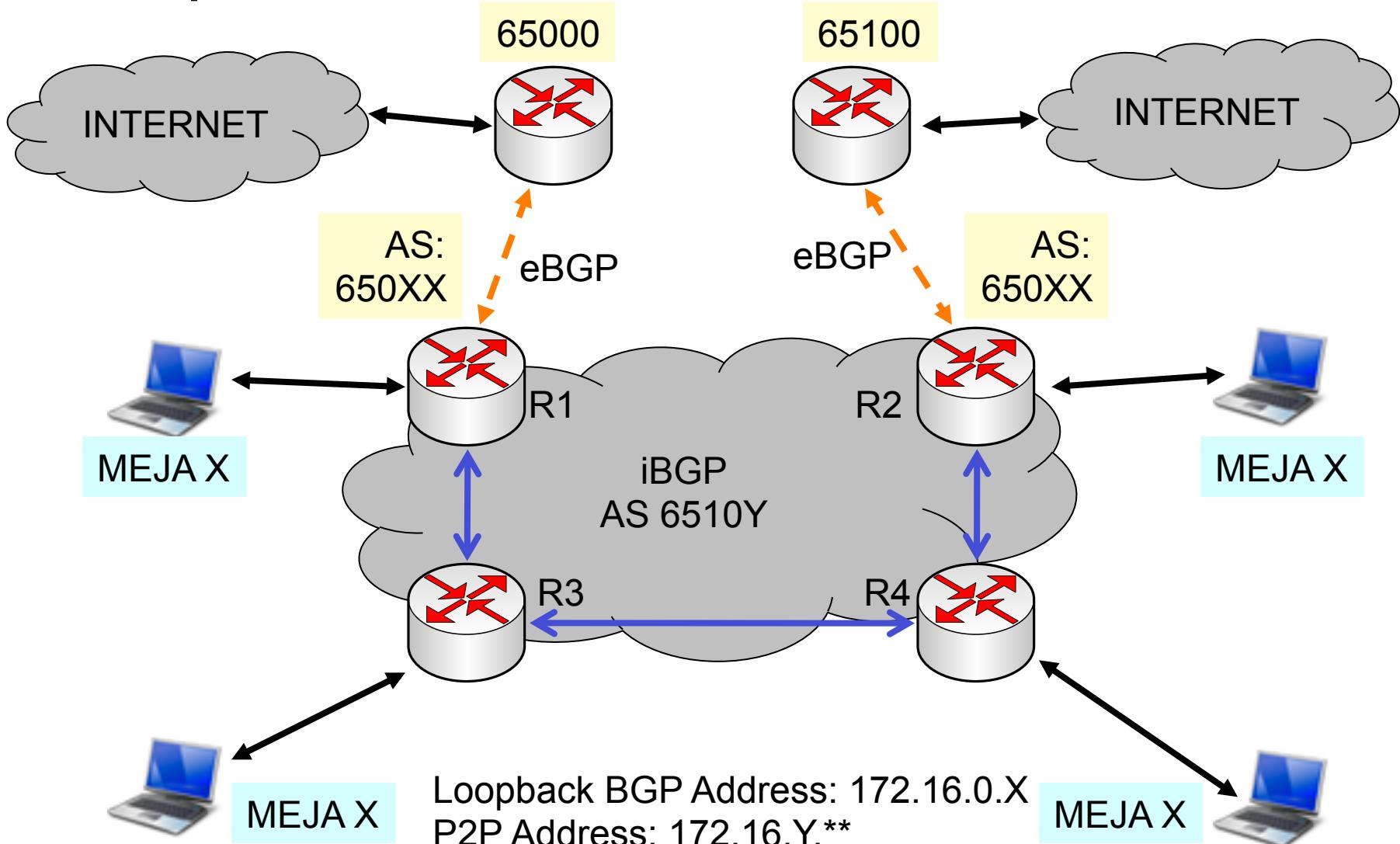
The screenshot shows the 'Route List' window from the Winbox interface. The window has tabs for 'Routes', 'Nexthops', 'Rules', and 'VRF'. The 'Routes' tab is selected. There are several icons at the top: a red plus sign for adding routes, a minus sign for deleting, a checkmark for selecting, an X for unselecting, a folder icon for opening a file, and a magnifying glass for filtering. To the right of these is a 'Find' button. The main area is a table with columns: '#', 'Src. Address', '...', 'Action', and 'Table'. Two rows of data are shown:

#	Src. Address	...	Action	Table
0	▶ 192.168.31.0/25		lookup	route-wlan1
1	▶ 192.168.31.128/25		lookup	route-wlan2

Static Route

Route List						
	Routes	Nexthops	Rules	VRF		
AS	0.0.0.0/0	10.10.10.100 reachable wlan1, ping			1	
	;;; main gateway for 192.168.31.0/25 via wlan1					
AS	0.0.0.0/0	10.10.10.100 reachable wlan1	ping		1	route-wlan1
	;;; main gateway for 192.168.31.128/25 via wlan2					
AS	0.0.0.0/0	10.20.20.100 reachable wlan2	ping		1	route-wlan2
	;;; backup gateway for 192.168.31.0/25 via wlan1					
S	0.0.0.0/0	10.20.20.100 reachable wlan2			2	route-wlan1
	;;; backup gateway for 192.168.31.128/25 via wlan2					
S	0.0.0.0/0	10.10.10.100 reachable wlan1			2	route-wlan2
DAC	10.10.10.0/24	wlan1 reachable			0	10
DAC	10.20.20.0/24	wlan2 reachable			0	10
DAC	172.16.0.31	lo reachable			0	17
AS	172.16.0.100	10.10.10.100 reachable wlan1			1	
DAC	192.168.31.0/24	ether1 reachable			0	19

[LAB-5] iBGP dan eBGP



Langkah

- Pada R1 dan R2, akan memiliki 2 buah instance BGP, masing-masing untuk iBGP dan eBGP
- Pada R3 dan R4, akan memiliki 1 instance BGP (untuk iBGP) dan 2 buah peer
- Untuk iBGP, supaya tidak tergantung pada interface, kita menggunakan loopback address
- Untuk menjamin koneksi antar loopback address, kita menggunakan OSPF yang terfilter (hanya melewatkkan IP loopback saja).

OSPF Setting (R1)

OSPF						
Instances	Networks	Areas	Area Ranges	Virtual Links	Neighbors	NBMA Neighbors
	Network	Area				
	172.16.9.0/24	backbone				

OSPF								
Interfaces	Instances	Networks	Areas	Area Ranges	Virtual Links	Neighbors	NBMA Neighbors	
	Interface	Cost	Priority	Authenti...	Authenticatio...	Network Type		
D	Ether2	10	1	none	*****	broadcast		

OSPF Filter

Route Filter <172.16.0.0/24>

Matchers

- Chain: ospf-in
- Prefix: 172.16.0.0/24
- Prefix Length: 0-32
- Match Chain:
- Protocol:
- Distance:
- Scope:
- Target Scope:
- Pref. Source:
- Routing Mark:
- Route Comment:
- Route Tag:
- Route Targets:
 - Invert Route Targets
- Site Of Origin:
 - Invert Site Of Origin
- Address Family:
- OSPF Type:
 - Invert Match

Actions

- Action: discard
- Jump Target:
- Set Distance:
- Set Scope:
- Set Target Scope:
- Set Pref. Source:
- Set In Nexthop:
- Set In Nexthop Direct:
- Set Out Nexthop:
- Set Routing Mark:
- Set Route Comment:
- Set Check Gateway:
- Set Disabled:
- Set Type:
- Set Route Tag:
- Set Use TE Nexthop:
- Set Route Targets
- Append Route Targets
- Set Site Of Origin

Route Filter <172.16.0.0/24>

Actions

- Action: discard
- Jump Target:
- Set Distance:
- Set Scope:
- Set Target Scope:
- Set Pref. Source:
- Set In Nexthop:
- Set In Nexthop Direct:
- Set Out Nexthop:
- Set Routing Mark:
- Set Route Comment:
- Set Check Gateway:
- Set Disabled:
- Set Type:
- Set Route Tag:
- Set Use TE Nexthop:
- Set Route Targets
- Append Route Targets
- Set Site Of Origin

Buttons (Right Panel):

- OK
- Cancel
- Apply
- Disable
- Comment
- Copy
- Remove

Static Route

- Pastikan di semua router sudah memiliki routing (dari OSPF/DAO) untuk semua IP loopback

Route List						
Routes	Nexthops	Rules	VRF			
	Dst. Address	Gateway		Distance	Routing Mark	Pref. Source
DAC	► 10.10.10.0/24	wlan1 reachable		0		10.10.10.31
DAC	► 172.16.0.31	lo reachable		0		172.16.0.31
DAo	► 172.16.0.32	172.16.9.2 reachable ether2		110		
DAo	► 172.16.0.33	172.16.9.2 reachable ether2		110		
DAo	► 172.16.0.34	172.16.9.2 reachable ether2		110		
DAC	► 172.16.9.2	ether2 reachable		0		172.16.9.1
DAC	► 192.168.31.0/24	ether1 unreachable		0		192.168.31.1

Konfigurasi iBGP

- Pada R3 dan R4 perlu mengaktifkan “route-reflect”, karena merupakan “penghubung” ke R1 dan R2.
- Untuk semua peer iBGP:
 - Remote address peer menggunakan ip loopback
 - Diaktifkan “default-originate” untuk bisa saling memberikan default route di antara iBGP router.
 - Multihop=yes karena menggunakan ip loopback

iBGP Instance

BGP Instance <iBGP>

Name:	iBGP
AS:	65109
Router ID:	172.16.0.31
<input checked="" type="checkbox"/> Redistribute Connected	
<input checked="" type="checkbox"/> Redistribute Static	
<input type="checkbox"/> Redistribute RIP	
<input type="checkbox"/> Redistribute OSPF	
<input checked="" type="checkbox"/> Redistribute Other BGP	
Out Filter:	<input type="text"/>
Confederation:	<input type="text"/>
Confederation Peers:	<input type="text"/>
Cluster ID:	<input type="text"/>
<input type="checkbox"/> Client To Client Reflection	
<input type="checkbox"/> Ignore AS Path Length	

disabled

Peer iBGP

Di R1 ke R3

BGP Peer <peer-to-router-3>

General Advanced Status

Name: peer-to-router-3
Instance: **iBGP**
Remote Address: **172.16.0.33**
Remote Port:
Remote AS: 65109
TCP MD5 Key:
Nexthop Choice: **default**
 Multihop
 Route Reflect
Hold Time: 180 s
TTL: default
Max Prefix Limit:
Max Prefix Restart Time:
In Filter:
Out Filter:
AllowAS In:
 Remove Private AS
 Default Originate

BGP Peer <peer-to-router-3>

General Advanced Status

Address Families: ip ipv6 l2vpn vpn4 l2vpn-cisco
Update Source: **lo**
Interface:

Peer iBGP

Di R4 ke R2

BGP Peer <peer-to-router-2>

General Advanced Status

Name: peer-to-router-2
Instance: default
Remote Address: 172.16.0.32
Remote Port:
Remote AS: 65109
TCP MD5 Key:
Nexthop Choice: default
 Multihop
 Route Reflect
Hold Time: 180 s
TTL: default
Max Prefix Limit:
Max Prefix Restart Time:
In Filter:
Out Filter:
AllowAS In:
 Remove Private AS
 Default Originate

BGP Peer <peer-to-router-2>

General Advanced Status

Address Families: IPv4 IPv6 I2VPN VPN4 I2VPN-CISCO
Update Source: lo
Interface:
ed established

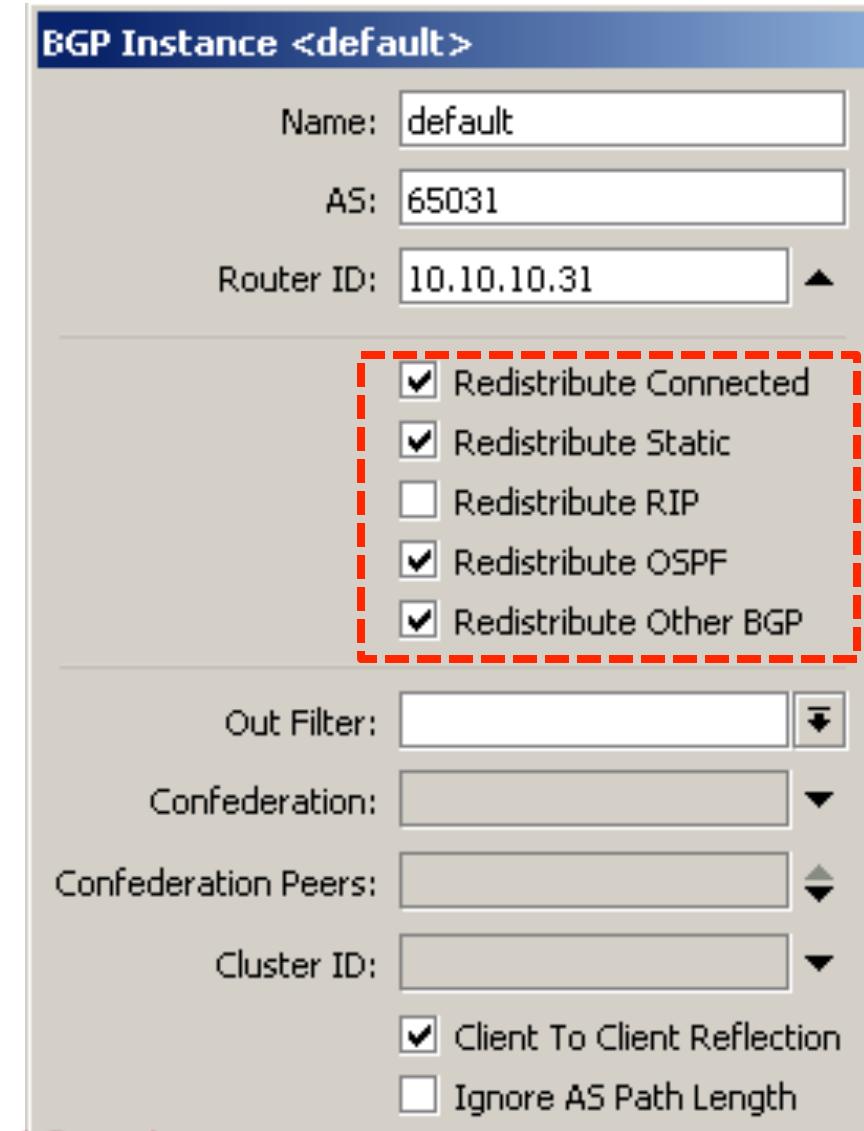
Static Route

- Setelah iBGP terbentuk, pastikan sudah mendapatkan semua network prefix dari semua router. Belum ada “default route”.

Route List					
	Routes	Nexthops	Rules	VRF	
	+	-	✓	✗	
	Dst. Address	Gateway		Distance	Routing Mark
DAC	▶ 10.10.10.0/24	wlan1 reachable		0	10.10.10.31
DAb	▶ 10.20.20.0/24	172.16.0.32 recursive via 17...		200	
DAC	▶ 172.16.0.31	lo reachable		0	172.16.0.31
DAo	▶ 172.16.0.32	172.16.9.2 reachable ether2		110	
DAo	▶ 172.16.0.33	172.16.9.2 reachable ether2		110	
Db	▶ 172.16.0.33	172.16.0.33 recursive via 17...	200		
DAo	▶ 172.16.0.34	172.16.9.2 reachable ether2		110	
DAb	▶ 172.16.9.1	172.16.0.33 recursive via 17...		200	
DAC	▶ 172.16.9.2	ether2 reachable		0	172.16.9.1
DAb	▶ 172.16.9.3	172.16.0.34 recursive via 17...		200	
DAb	▶ 172.16.9.4	172.16.0.33 recursive via 17...		200	
DAb	▶ 172.16.9.5	172.16.0.32 recursive via 17...		200	
DAb	▶ 172.16.9.6	172.16.0.34 recursive via 17...		200	
DAC	▶ 192.168.31.0/24	ether1 unreachable		0	192.168.31.1
DAb	▶ 192.168.32.0/24	172.16.0.32 recursive via 17...		200	
DAb	▶ 192.168.33.0/24	172.16.0.33 recursive via 17...		200	
DAb	▶ 192.168.34.0/24	172.16.0.34 recursive via 17...		200	

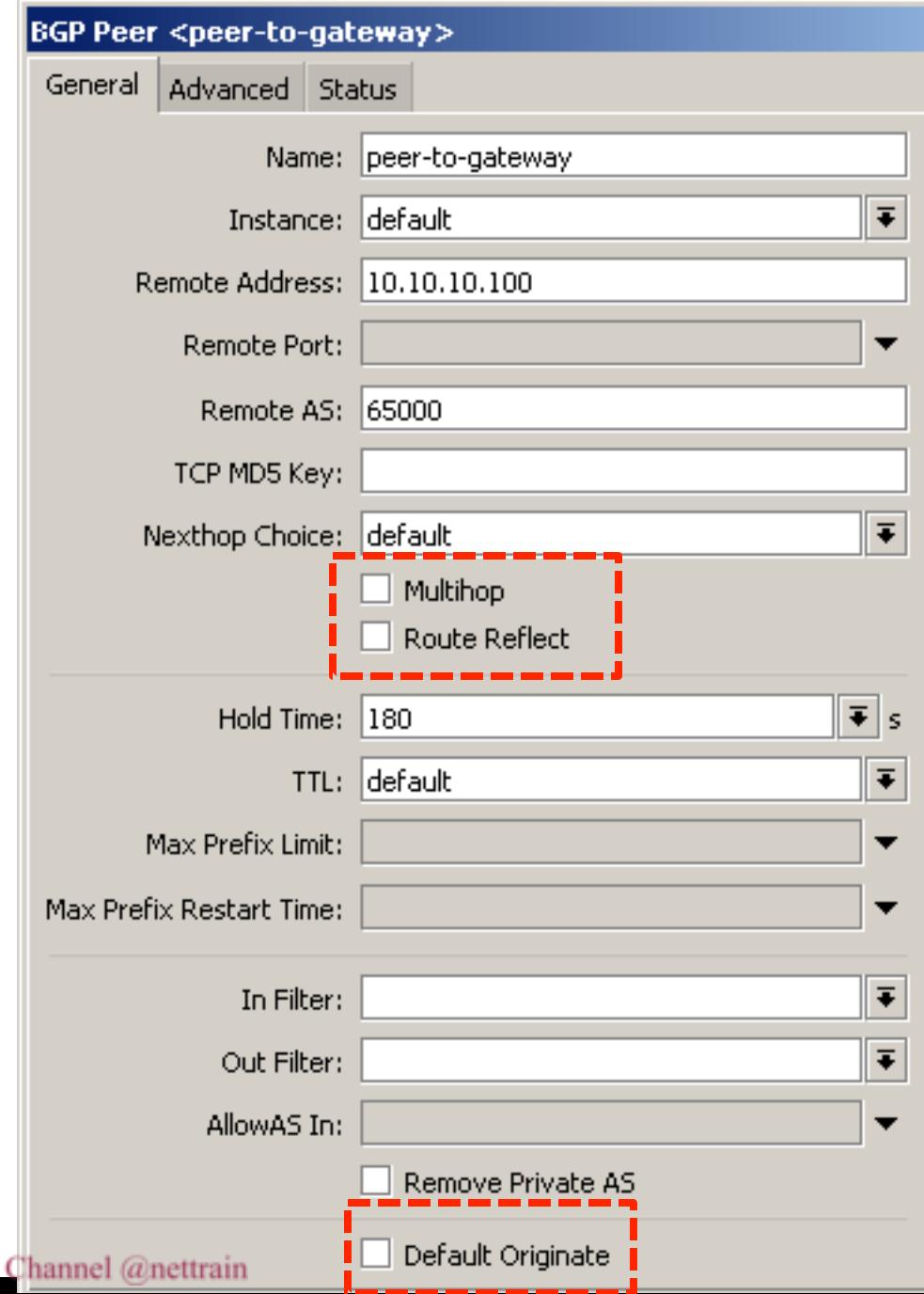
eBGP di R1 dan R2

- BGP Peer menggunakan IP interface
- Aktifkan “redistribute OSPF” untuk mengadvertise routing dari OSPF
- Aktifkan “redistribute other BGP” untuk mengadvertise prefix yang didapat dari BGP instance lain (eBGP)



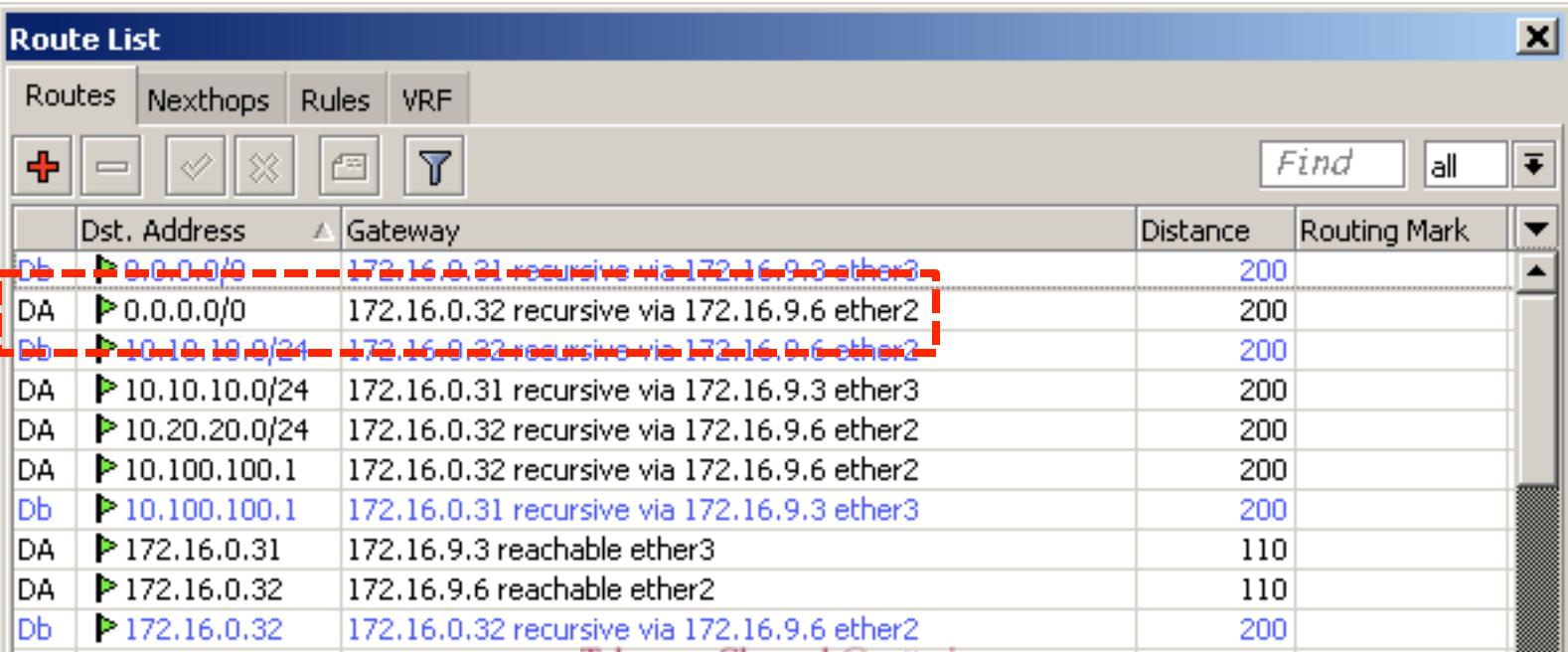
BGP Peer

- Di R1 ke Gateway
- Tidak perlu multihop, karena menggunakan IP interface
- Tidak perlu default originate karena tidak memberikan prefix default route ke gateway



Static Route (normal)

- Pastikan sudah mendapatkan default route ke arah seharusnya.
 $R4 \rightarrow R2, R3 \rightarrow R1, R1 \rightarrow Gw1, R2 \rightarrow Gw2$
- Contoh di R4:



The screenshot shows the 'Route List' window in Winbox. The window has tabs for 'Routes', 'Nexthops', 'Rules', and 'VRF'. The 'Routes' tab is selected. There are buttons for adding (+), deleting (-), and filtering (T). A search bar 'Find' and a 'Find all' button are also present. The table lists routes with columns for Destination Address, Gateway, Distance, and Routing Mark.

	Dst. Address	Gateway	Distance	Routing Mark
Db	► 0.0.0.0/0	172.16.0.21 recursive via 172.16.0.3 ether3	200	
DA	► 0.0.0.0/0	172.16.0.32 recursive via 172.16.9.6 ether2	200	
Db	► 10.10.10.0/24	172.16.0.32 recursive via 172.16.9.6 ether2	200	
DA	► 10.10.10.0/24	172.16.0.31 recursive via 172.16.9.3 ether3	200	
DA	► 10.20.20.0/24	172.16.0.32 recursive via 172.16.9.6 ether2	200	
DA	► 10.100.100.1	172.16.0.32 recursive via 172.16.9.6 ether2	200	
Db	► 10.100.100.1	172.16.0.31 recursive via 172.16.9.3 ether3	200	
DA	► 172.16.0.31	172.16.9.3 reachable ether3	110	
DA	► 172.16.0.32	172.16.9.6 reachable ether2	110	
Db	► 172.16.0.32	172.16.0.32 recursive via 172.16.9.6 ether2	200	

Back Up Link (fail over)

- Pada saat ada link yang putus, akan secara otomatis melalui back up link.
- Contoh di R4, melalui R3, bukan ke R2

Route List			
Routes	Nexthops	Rules	VRF
<input style="width: 20px; height: 20px;" type="button" value="+"/>	<input style="width: 20px; height: 20px;" type="button" value="-"/>	<input type="checkbox"/>	<input style="width: 20px; height: 20px;" type="button" value="X"/>
<input style="width: 20px; height: 20px;" type="button" value="F"/>	<input style="width: 20px; height: 20px;" type="button" value="T"/>	<input type="button" value="Find"/>	<input type="button" value="all"/>
Dst. Address	Gateway	Distance	Routing Mark
DA ► 0.0.0.0/0	172.16.0.31 recursive via 172.16.9.3 ether3	200	
DA ► 10.10.10.0/24	172.16.0.31 recursive via 172.16.9.3 ether3	200	
DA ► 10.20.20.0/24	172.16.0.32 recursive via 172.16.9.6 ether2	200	
DA ► 10.100.100.1	172.16.0.31 recursive via 172.16.9.3 ether3	200	
DA ► 172.16.0.31	172.16.9.3 reachable ether3	110	
DA ► 172.16.0.32	172.16.9.6 reachable ether2	110	
Db ► 172.16.0.32	172.16.0.32 recursive via 172.16.9.6 ether2	200	
DA ► 172.16.0.33	172.16.9.3 reachable ether3	110	



Pengenalan MPLS



Certified Mikrotik Training Advanced Class (MTCRE)

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

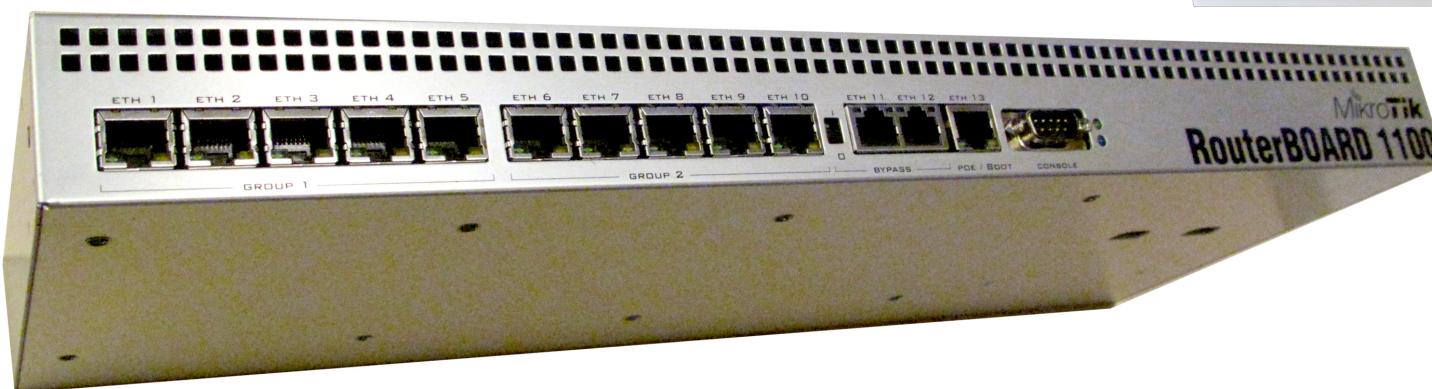
MPLS Jarang Digunakan?

- Ketersediaan perangkat dan/atau harga yang tinggi



MPLS on RouterOS

- Saat ini kita sudah bisa menggunakan fitur MPLS dengan RouterOS. Mulai dari US \$40,- RB750 hingga RouterOS on QuadXeon.





Networking

- 3 metode dalam melakukan networking
 - Routing
 - RIP, OSPF, BGP
 - Bridging
 - STP, RSTP, Mesh
 - Switching
 - MPLS, ATM, Frame Relay

Konsep Switching



Telegram Channel @nettrain

Mikrotik Indonesia <http://www.mikrotik.co.id>



Konsep Switching

- Adalah metode komunikasi jaringan yang melakukan pengiriman data dalam kelompok-kelompok dalam ukuran tertentu
- Setiap kelompok ditransmisikan tidak terkait dengan kelompok lainnya
- Jaringan memiliki kemampuan untuk mengalokasikan kapasitas yang dibutuhkan untuk mengoptimalkan utilisasi dan kualitas transmisi.

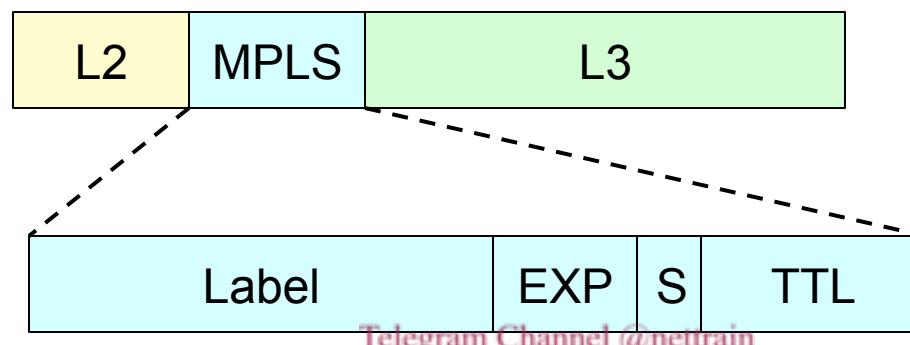


Multi Protocol Label Switching

- Adalah metode transmisi paket data yang berdasarkan label yang melekat pada paket dan “label forwarding table” dengan beban yang minimal.
- MPLS tidak memerlukan packet header dan routing table

MPLS Header

- 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)

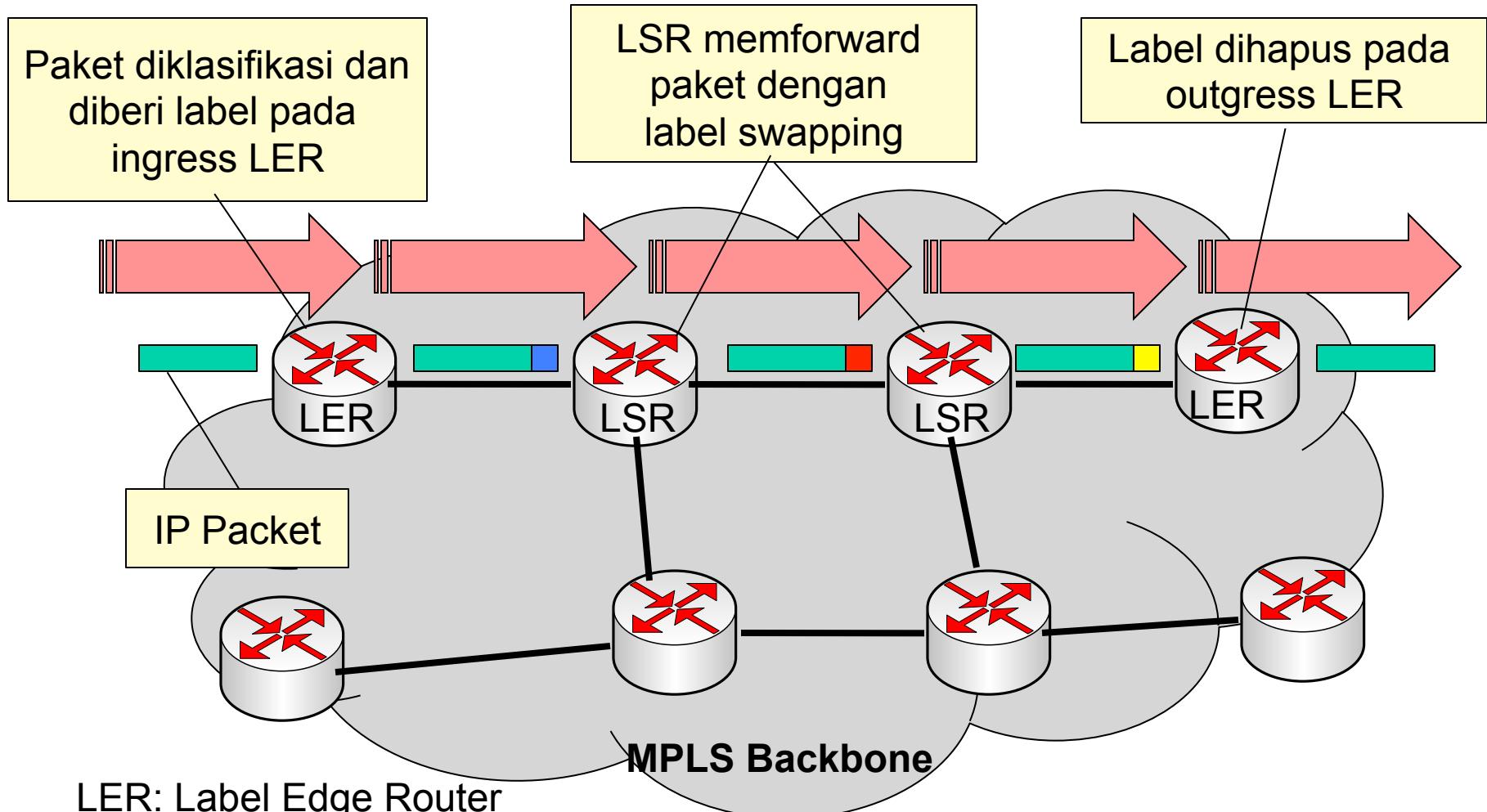




MPLS LDP

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

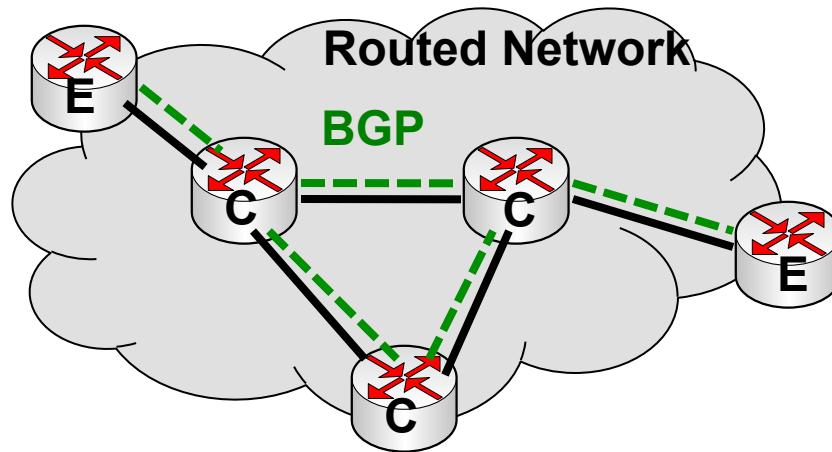
Cara Kerja MPLS



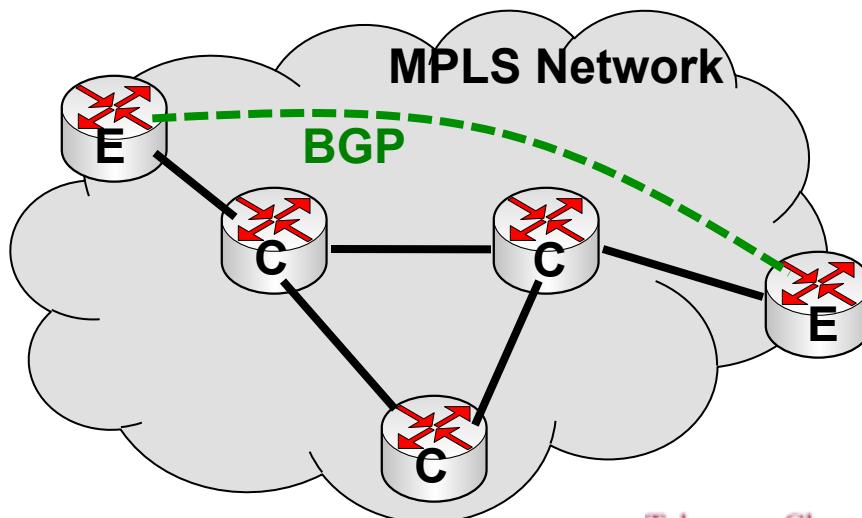
LER: Label Edge Router

LSR: Label Switch Router

Perbandingan BGP

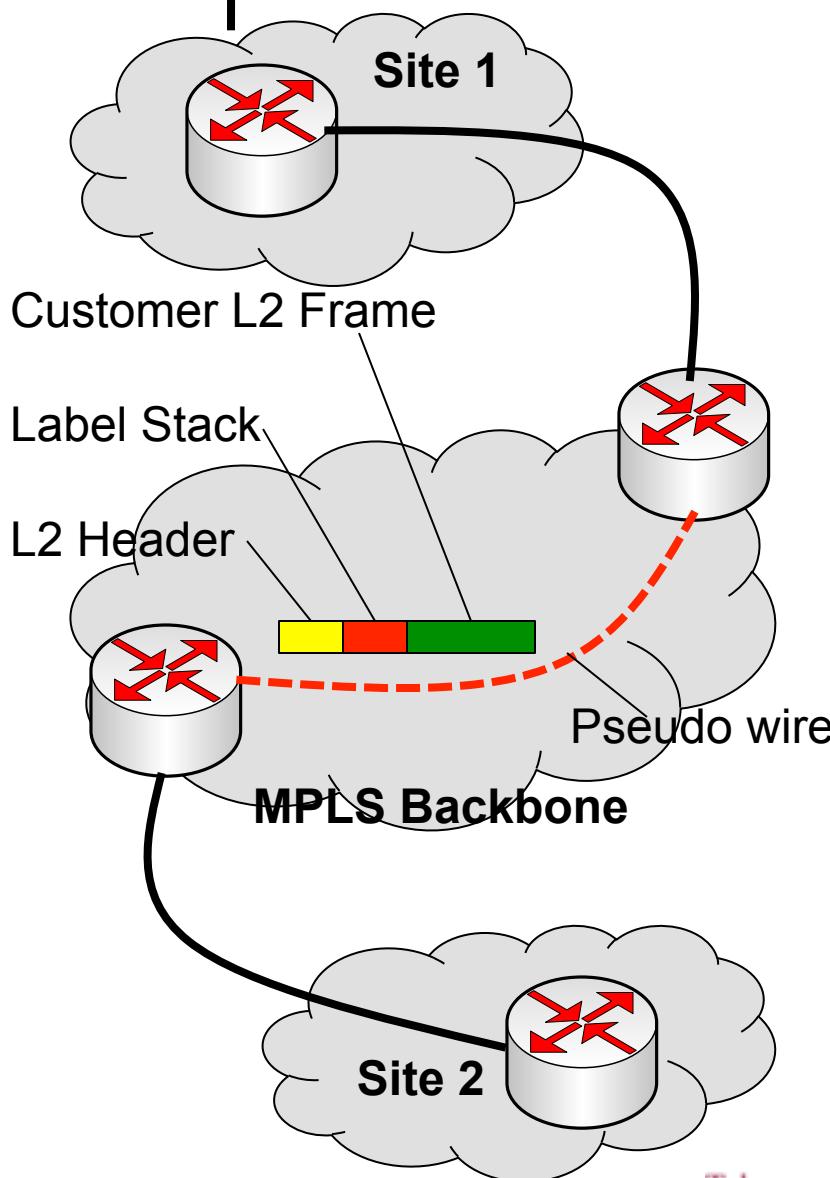


- Biasanya, kita harus menjalankan BGP di semua core router
- Dengan MPLS, BGP dilakukan cukup antar edge router



Telegram Channel @nettrain

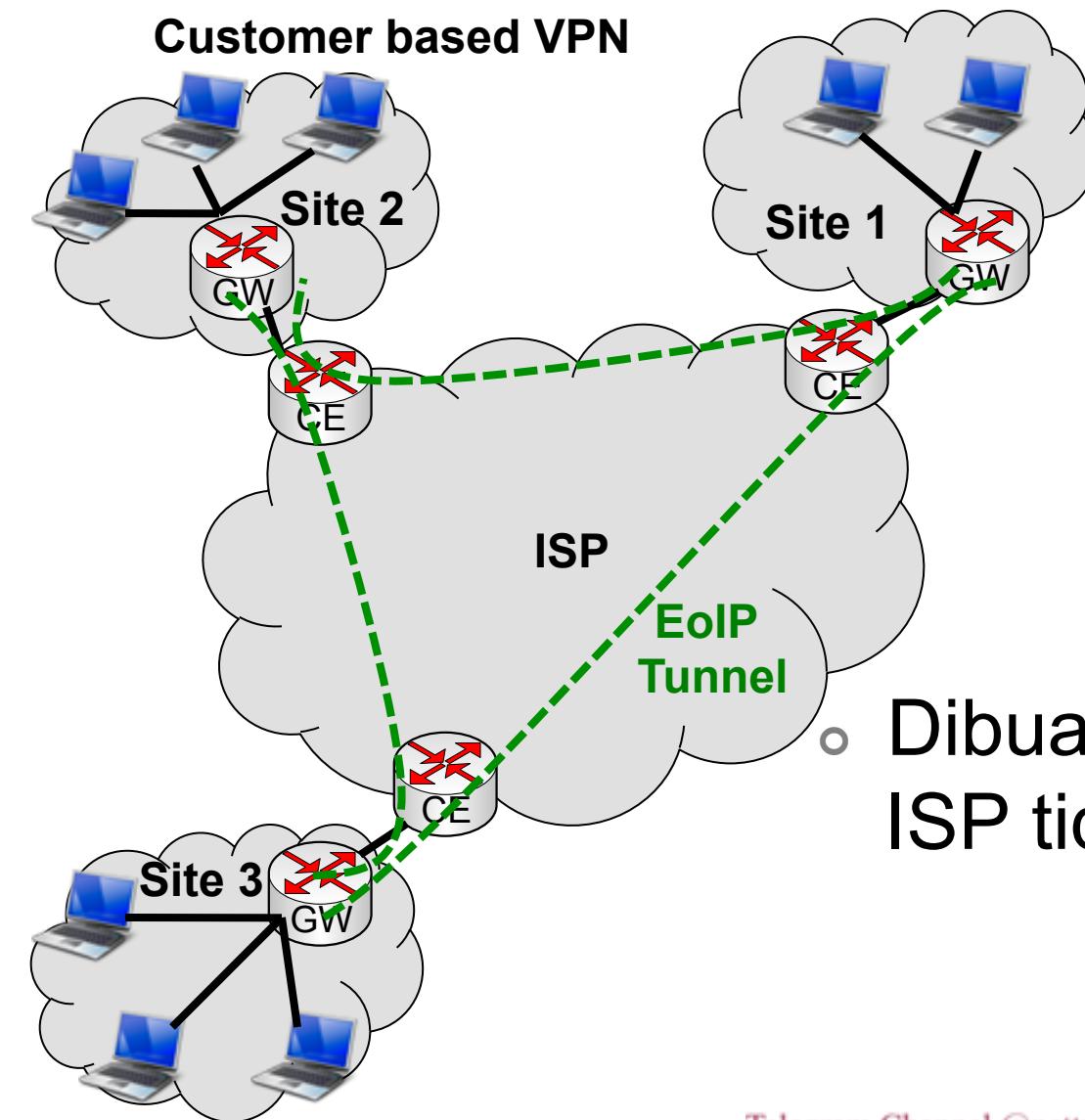
MPLS dan L2VPN



- Layanan L2 tanpa mengurangi kapasitas L2
- Menggunakan split-horizon untuk menghindari loop
- Service dikonfigurasi hanya pada edge router, tidak pada core router
- Pemisahan antara network customer dan infrastruktur

VPN Layer 2 Saat ini

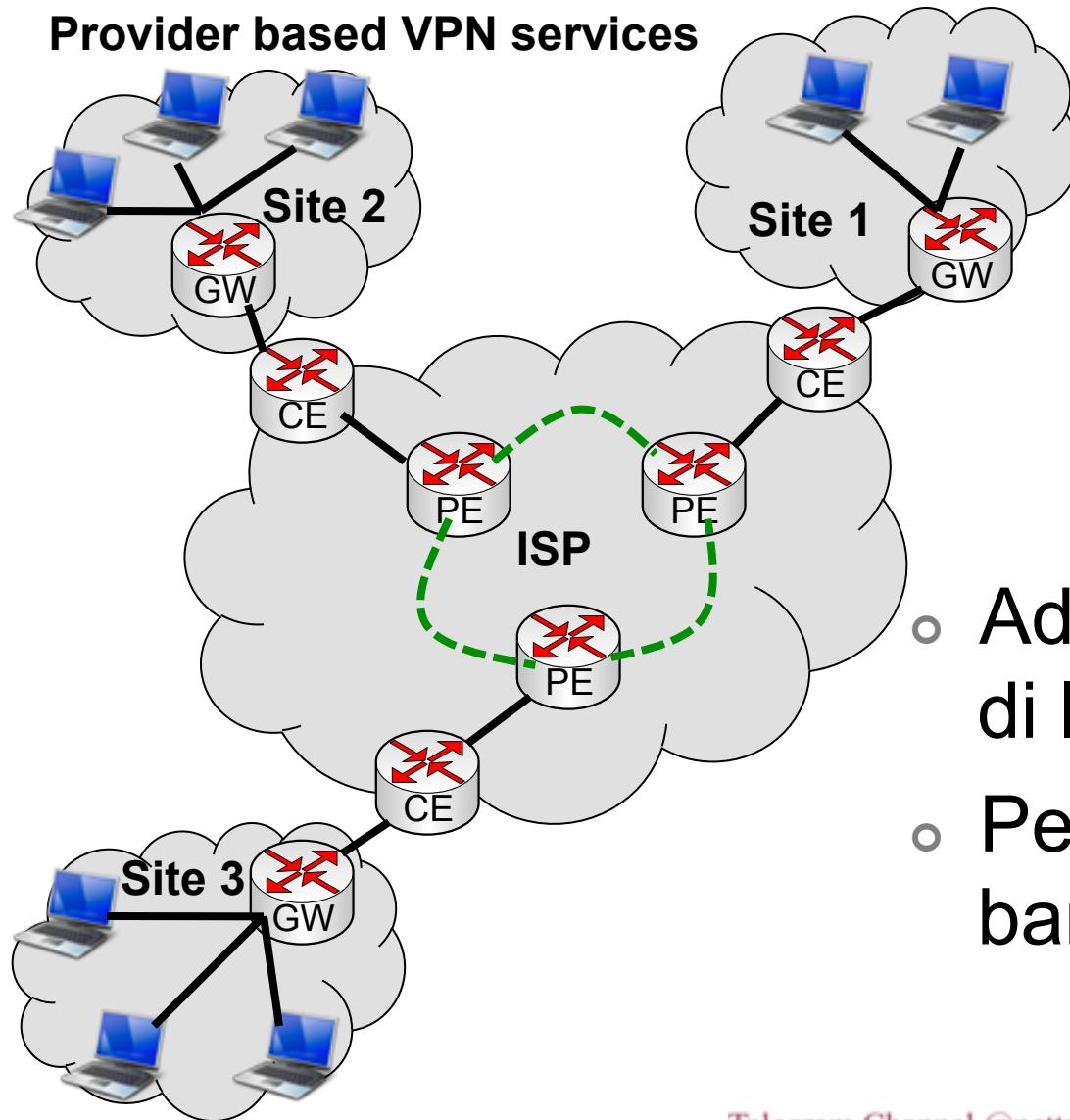
Customer based VPN



- Overhead (IP +GRE+ethernet)
- Tiap ada node baru, harus membuat link baru
- Dibuat di level customer, ISP tidak dilibatkan

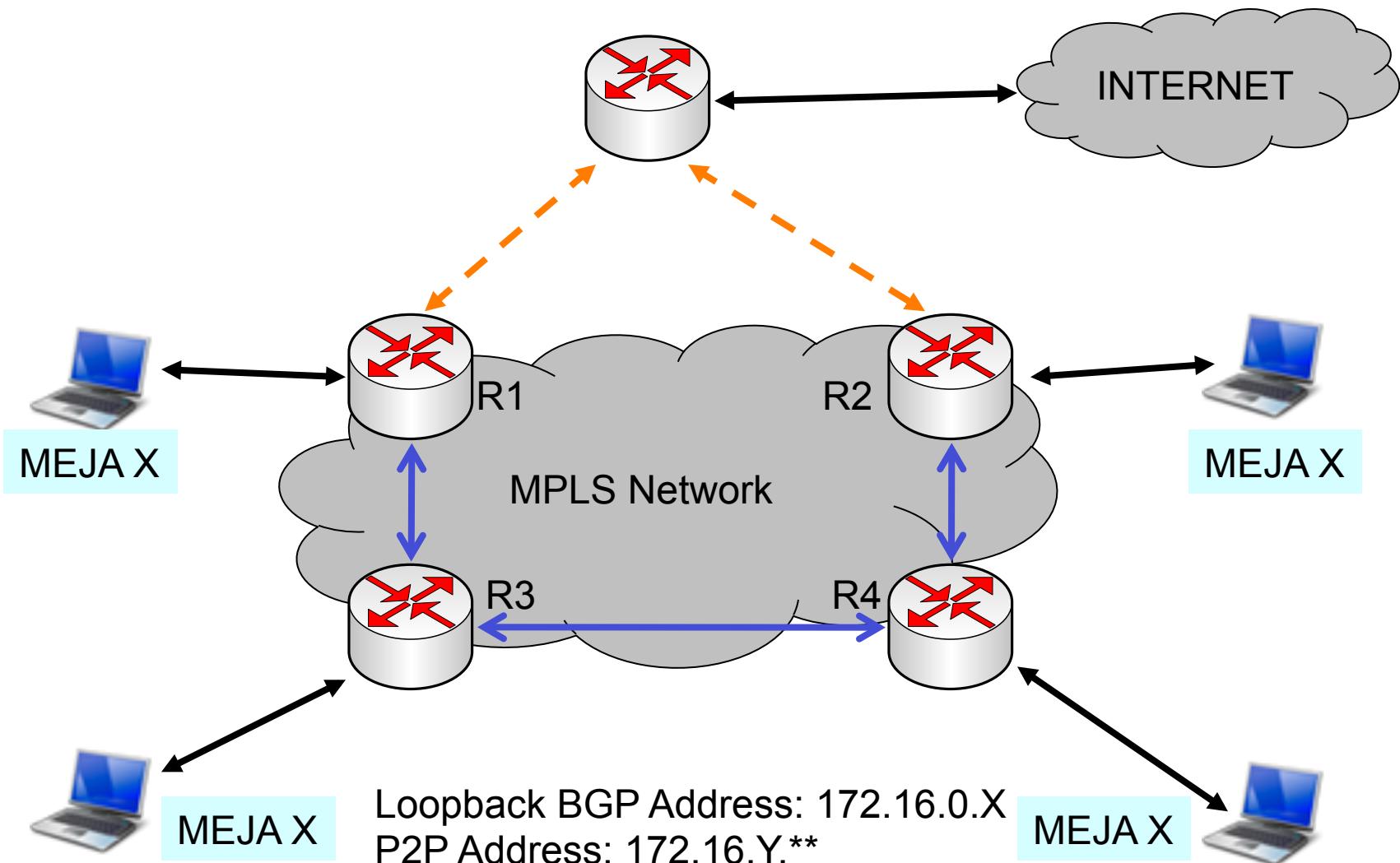
MPLS VPLS

Provider based VPN services



- Overhead lebih kecil (IP+label)
- Bisa diatur garansi bandwidth VPLS
- Administrasi dilakukan di level ISP
- Penambahan node baru tidak sulit

[LAB-1] MPLS & VPLS



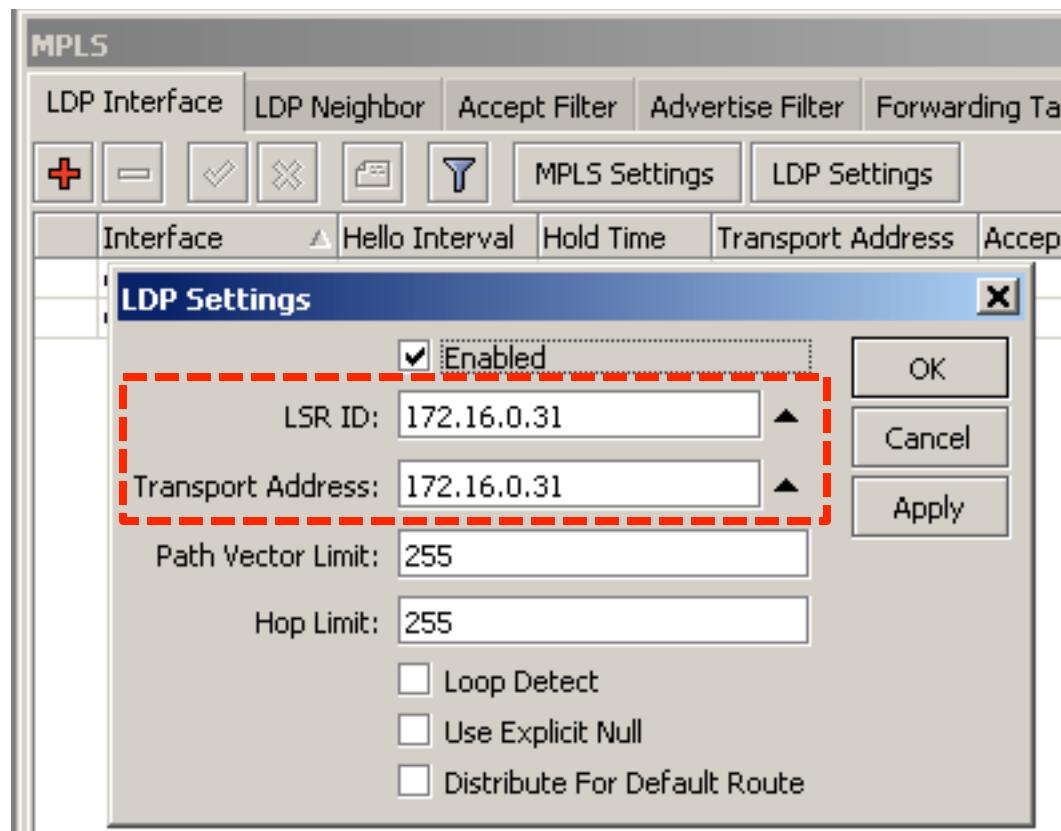


Konfigurasi Awal

- MPLS membutuhkan IP loopback sebagai identitas router dan alamat transport.
- Lakukanlah OSPF sehingga semua IP Address loopback dapat terjangkau

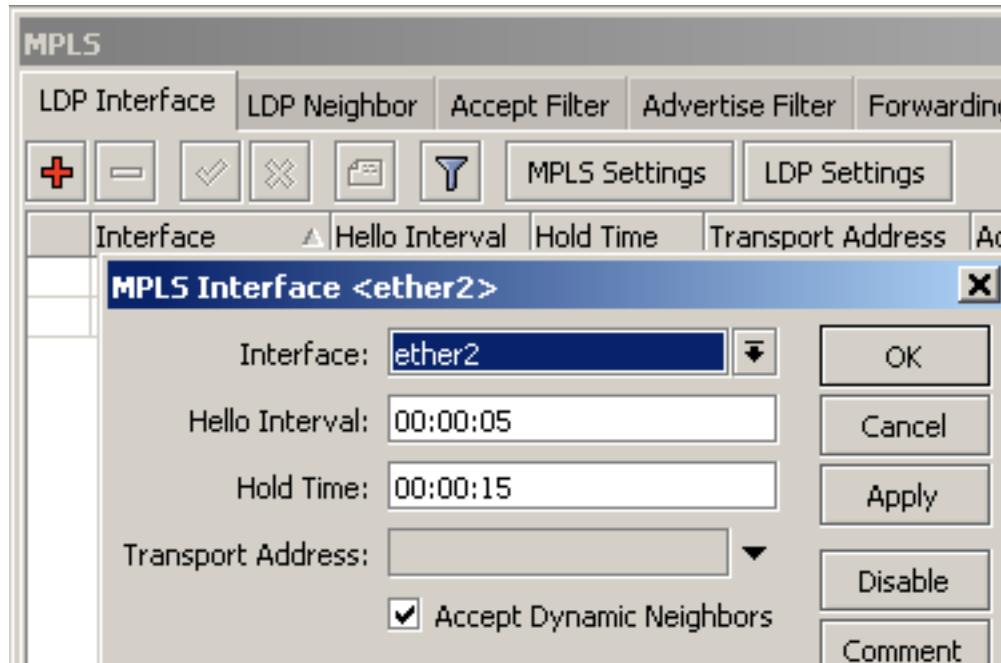
LDP Setting

- Gunakanlah loopback IP untuk LSR ID dan transport address.



LDP Interface

- Buatlah LDP interface yang berhubungan dengan router lainnya



Local Bindings

MPLS

LDP Interface LDP Neighbor Accept Filter Advertise Filter Forwarding Table MPLS Interface Local Bindings Ren

+ - ✓ ✎ ⚡

	Dst. Address	Label	Advertised Path	Peers
DAEL	10.10.10.0/24	impl-null	empty	172.16.0.100:0, 172.16.0.32:0, 172.16.0.33:0
DAG	10.100.100.1	70	hops:2	172.16.0.100:0, 172.16.0.32:0, 172.16.0.33:0
DAEL	172.16.0.31	impl-null	empty	172.16.0.100:0, 172.16.0.32:0, 172.16.0.33:0
DAG	172.16.0.32	67	empty	172.16.0.100:0, 172.16.0.32:0, 172.16.0.33:0
DAG	172.16.0.33	65	empty	172.16.0.100:0, 172.16.0.32:0, 172.16.0.33:0
DAG	172.16.0.34	71	empty	172.16.0.100:0, 172.16.0.32:0, 172.16.0.33:0
DAG	172.16.0.100	61	hops:2	172.16.0.100:0, 172.16.0.32:0, 172.16.0.33:0
DAEL	172.16.9.2	impl-null	empty	172.16.0.100:0, 172.16.0.32:0, 172.16.0.33:0
DAG	172.16.9.4	66	empty	172.16.0.100:0, 172.16.0.32:0, 172.16.0.33:0
DAG	172.16.9.5	69	empty	172.16.0.100:0, 172.16.0.32:0, 172.16.0.33:0
DAG	192.168.0.0/24	62	hops:2	172.16.0.100:0, 172.16.0.32:0, 172.16.0.33:0
DAEL	192.168.31.0/24	impl-null	empty	172.16.0.100:0, 172.16.0.32:0, 172.16.0.33:0
DAG	192.168.32.0/24	68	empty	172.16.0.100:0, 172.16.0.32:0, 172.16.0.33:0
DAG	192.168.33.0/24	63	empty	172.16.0.100:0, 172.16.0.32:0, 172.16.0.33:0
DAG	192.168.34.0/24	64	empty	172.16.0.100:0, 172.16.0.32:0, 172.16.0.33:0

Traceroute

- Lakukanlah test dengan traceroute untuk melihat label yang ada di MPLS

```
[admin@C31] > tool traceroute 172.16.0.34 src-address=172.16.0.31
```

	ADDRESS	STATUS
1	10.10.10.32 1ms 9ms 10ms mpls-label=16	
2	172.16.0.34 6ms 13ms 6ms	

VPLS Tunnel

- Untuk remote peer, gunakanlah IP loopback
- VPLS:ID haruslah unik dalam MPLS

Interface <vpls-R31-to-R34>

General	Status	Traffic
Name: vpls-R31-to-R34		
Type: VPLS		
MTU: 1500		
L2 MTU: 1500		
MAC Address: 02:DC:A9:0C:2E:70		
ARP: enabled		
Remote Peer: 172.16.0.34		
VPLS ID: 1:4		▲
<input type="checkbox"/> Cisco Style		
Cisco Style ID: 0		
Advertised L2MTU: 1500		
PW Type: <input checked="" type="radio"/> tagged ethernet <input type="radio"/> raw ethernet		
disabled	running	slave
BGP signaled		

● ● ● | Interface

- Buatlah tunnel VPLS ke semua router di dalam kelompok

Interface List						
	Interface	Ethernet	EoIP Tunnel	IP Tunnel	VLAN	VRRP
	     					
	Name	Type		L2 MTU	Tx	Rx
	ether1	Ethernet		1526	0 bps	0 bps
R	ether2	Ethernet		1522	0 bps	1188 bps
	ether3	Ethernet		1522	0 bps	0 bps
R	lo	Bridge		65535	0 bps	0 bps
R	vpls-R31-to-R32	VPLS		1500	0 bps	0 bps
R	vpls-R31-to-R33	VPLS		1500	0 bps	0 bps
R	vpls-R31-to-R34	VPLS		1500	0 bps	0 bps
R	wlan1	Wireless (Atheros AR...		2290	43.3 kbps	8.4 kbps
X	wlan2	Wireless (Atheros AR...			0 bps	0 bps

Test

- Masukkan IP Address pada VPLS Tunnel dan lakukan test ping

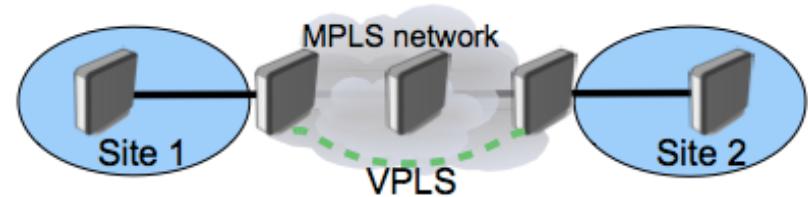
Address List				
	Address	Network	Broadcast	Interface
	10.1.1.1/24	10.1.1.0	10.1.1.255	vpls-R31-to-R34
X	10.10.10.31/24	10.10.10.0	10.10.10.255	wlan1
X	10.20.20.31/24	10.20.20.0	10.20.20.255	wlan2

Pengembangan

- MPLS / VPLS dapat juga diintegrasikan dengan iBGP (I2VPN) untuk membuat VPLS tunnel secara dynamic.
- VPLS tunnel bisa bekerja baik untuk routing maupun untuk bridge.
- Bridge horizon bisa digunakan sebagai alternatif RSTP untuk menghindari bridge loop
- Untuk fungsi yang lebih advanced, bisa dilakukan traffic engineering.

MPLS vs EoIP

- Hampir 2 kali lebih cepat dari IP forwarding
- Sama cepat dengan bridge
- 60% lebih cepat dari EoIP yang melalui network routing



Label switching pada RB1000

	64 byte pps	512 byte pps
Bridge	414.000	359.000
MPLS	410.000	358.000
Routing	236.000	229.700

	64 byte pps	512 byte pps
EoIP	190.000	183.900
VPLS	332.500	301.000



Load Balanced



Certified Mikrotik Training Advanced Class (MTCRE)

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)



Konsep Dasar

- Load Balanced
 - Membagi trafik ke dua atau lebih jalur sehingga setiap jalur bisa digunakan secara optimal
- Fail Over
 - Sistem proteksi untuk menjaga apabila link utama terganggu, secara otomatis akan memfungsikan jalur cadangan

Load Balanced

$$\cancel{1 + 1 = 2}$$

$$1 + 1 = 1 + 1$$

$$1 + 1 = \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2}$$

$$1 + 1 = \frac{1}{4} + \frac{1}{4}$$

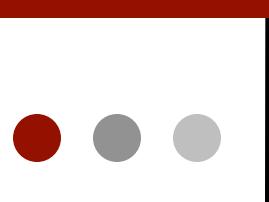
Semakin banyak user, semakin banyak koneksi, pembagian Load balance akan semakin rata dan mudah.

Konsep Load Balanced

- Pembagian trafik dilakukan berdasarkan probabilitas
- Kita harus mengetahui kapasitas masing-masing link dan membagi trafik ke setiap interface sesuai dengan proporsinya
- Misalnya kita memiliki 2 buah gateway, A dengan kapasitas 1 mbps, dan B dengan kapasitas 2 mbps, maka kita akan membagi trafik menjadi $3 = 2:1 = 1$ ke A dan 2 ke B

Penggunaan Fitur

- Untuk bisa melakukan load balance dengan baik, kuasailah fitur-fitur berikut ini:
 - Static route dan policy route
 - Firewall Mangle
 - Firewall src-nat
- Untuk yang lebih advanced, perlu juga menggunakan : OSPF dan BGP



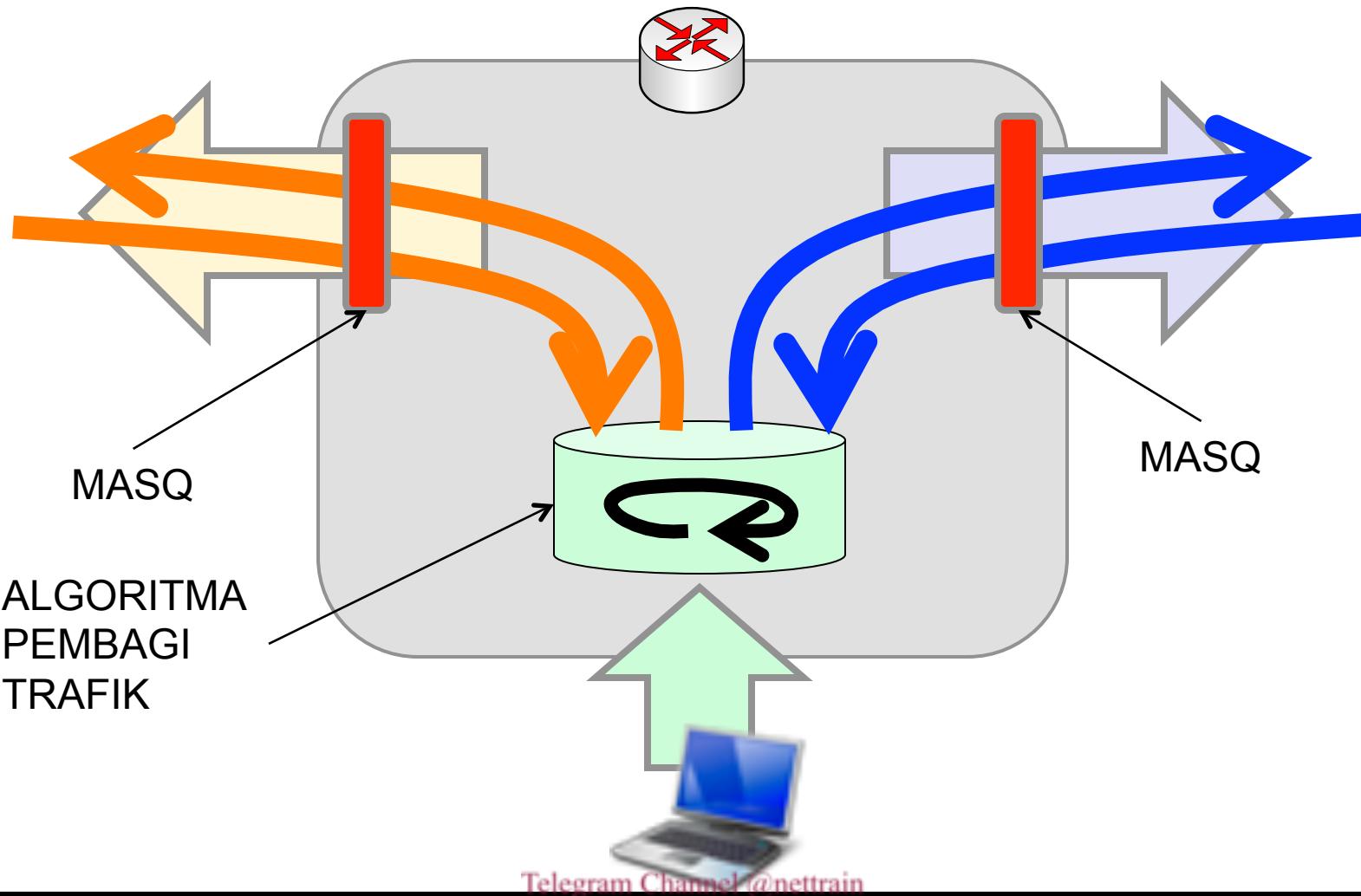
Kunci Load Balanced

- Pada jaringan yang sederhana, kita hanya bisa mengatur jalur uplink. Kita bisa mengatur koneksi mana yang lewat ke jalur yang mana, tetapi kita tidak bisa mengatur lewat mana jalur yang digunakan untuk downlink, karena hal tersebut bergantung pada routing internet secara keseluruhan.

Kunci Load Balanced

- Untuk “mengatur” jalur downlink, kuncinya pada penggunaan src-nat pada tiap gateway, pada saat request dikirimkan ke internet.
- Data yang di NAT dengan IP yang ada pada gateway A, akan kembali melalui gateway A.
- Jika kita hanya menggunakan masquerade untuk tiap interface gateway, maka data akan kembali pada interface yang sama dengan interface uplink.

Skema Kerja Load Balanced



Telegram Channel @nettrain



Metode Load Balanced

- Static Route dengan Address List
- ECMP (Equal Cost Multi Path)
- NTH
- PCC
- BGP



Contoh dgn Static Route

- Berdasarkan Tujuan
 - Gateway A untuk internasional
 - Gateway B untuk trafik lokal
 - Menggunakan address-list NICE



Contoh dgn Static Route

- Berdasarkan source address
 - IP Address client: 192.168.0.0/24
 - 192.168.0.0-127 → gateway A
 - 192.168.0.128-255 → gateway B

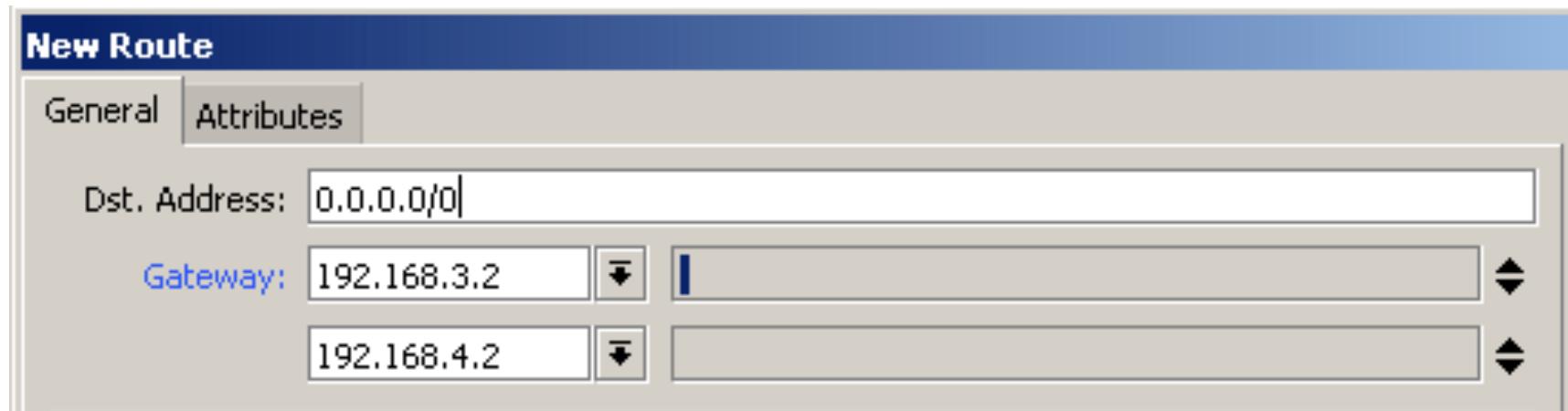


ECMP

- Equal Cost Multi Path
- Pada saat kita memiliki beberapa gateway yang ingin di load balance, metode termudah adalah menggunakan ECMP
- ECMP akan memisahkan trafik per gateway secara random

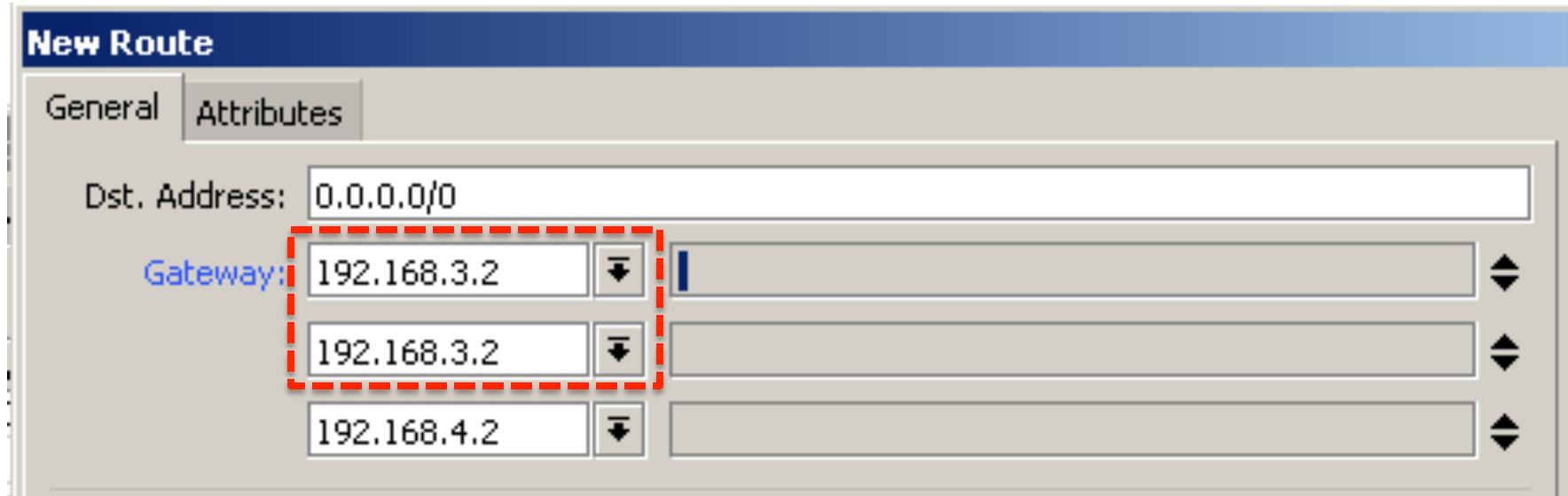
Contoh ECMP (1)

- 2 gateway yang sama besarnya



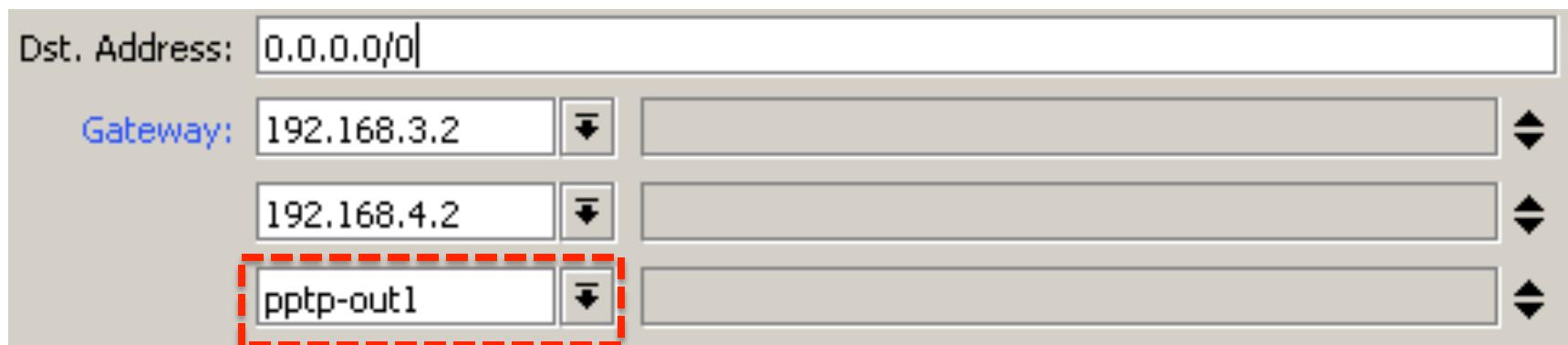
Contoh ECMP (2)

- 2 gateway, A dua kali lebih besar dari B



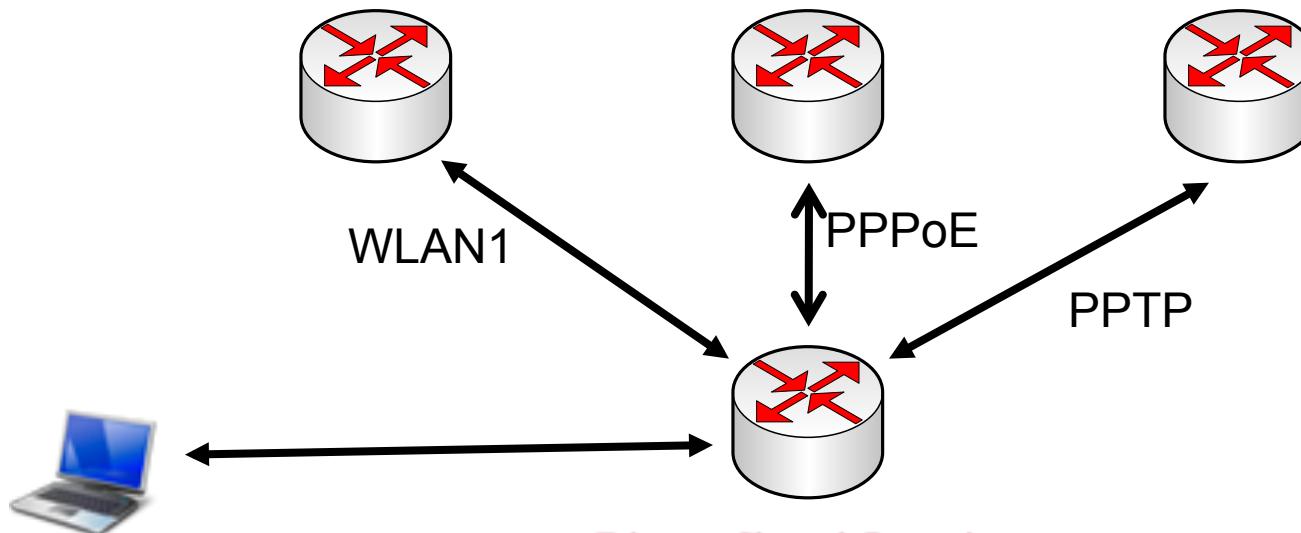
Contoh ECMP (3)

- 3 gateway, gateway A dan B menggunakan gateway IP Address, dan gateway C menggunakan pppoe



[LAB-1] ECMP & Policy Route

- IIX → via WLAN1 dan PPPoE di WLAN2.
- Kapasitas PPPoE 2 x kapasitas WLAN1
- Internasional → PPTP ke IP 10.100.100.1



Telegram Channel @nettrain

Address List

- Download nice.rsc dari server mikrotik.co.id

The screenshot shows the Winbox Firewall Address Lists interface. The window title is "Firewall". The "Address Lists" tab is selected. The table has two columns: "Name" and "Address". The "Name" column contains 760 entries, all labeled "nice", and the "Address" column lists various IP ranges. A vertical scroll bar is visible on the right side of the table.

Name	Address
nice	114.120.0.0/13
nice	120.168.0.0/13
nice	114.56.0.0/14
nice	125.166.0.0/15
nice	125.162.0.0/16
nice	125.163.0.0/16
nice	125.160.0.0/16
nice	125.161.0.0/16
nice	125.164.0.0/16
nice	125.165.0.0/16
nice	120.163.0.0/16
nice	120.162.0.0/16
nice	120.161.0.0/16
nice	120.160.0.0/16
nice	124.81.0.0/16
nice	222.124.0.0/16

760 items

PPTP dan PPPoE Username

- Username dan password:
 - PPTP
 - Username : mikrotik-pptp
 - Password : training
 - PPPoE
 - Username : mikrotik-pppoe
 - Password : training

Static Route untuk PPTP

Route <10.100.100.1>

General	Attributes
Dst. Address:	10.100.100.1
Gateway:	10.10.10.100
	reachable wlan1
Check Gateway:	
Type:	unicast
Distance:	1
Scope:	30
Target Scope:	10
Routing Mark:	
Pref. Source:	

PPTP & PPPoE Setting

Interface <pptp-out1>

General	Dial Out	Status	Traffic
Connect To: 10.100.100.1			
User: mikrotik-pptp			
Password: *****			
Profile: default			
<input type="checkbox"/> Dial On Demand			
<input type="checkbox"/> Add Default Route			
– Allow			
<input checked="" type="checkbox"/> pap	<input checked="" type="checkbox"/> chap		
<input checked="" type="checkbox"/> mschap1	<input checked="" type="checkbox"/> mschap2		

Interface <pppoe-out1>

General	Dial Out	Status	Traffic
Service:			
AC Name:			
User: mikrotik-pppoe			
Password: *****			
Profile: default			
<input type="checkbox"/> Dial On Demand			
<input type="checkbox"/> Add Default Route			
<input type="checkbox"/> Use Peer DNS			
– Allow			
<input checked="" type="checkbox"/> pap	<input checked="" type="checkbox"/> chap		
<input checked="" type="checkbox"/> mschap1	<input checked="" type="checkbox"/> mschap2		

● ● ● | Interface

- Pastikan semua interface sudah bekerja dengan baik

Interface List							
	Interface	Ethernet	EoIP Tunnel	IP Tunnel	VLAN	VRRP	Bonding
R	ether1	Ethernet			1526	51.6 kbps	28.5 kbps
X	ether2	Ethernet			1522	0 bps	0 bps
X	ether3	Ethernet			1522	0 bps	0 bps
R	pppoe-out1	PPPoE Client				0 bps	0 bps
R	pptp-out1	PPTP Client				20.2 kbps	11.0 kbps
R	wlan1	Wireless (Atheros AR...			2290	25.5 kbps	16.4 kbps
R	wlan2	Wireless (Atheros AR...			2290	0 bps	0 bps

IP Address

- Pastikan sudah mendapatkan IP Address dinamik dari PPTP dan PPPoE

Address List				
	Address	Network	Broadcast	Interface
	10.10.10.31/24	10.10.10.0	10.10.10.255	wlan1
D	172.21.1.16	172.21.1.254		pppoe-out1
D	172.21.2.19	172.21.2.254		pptp-out1
	192.168.31.1/24	192.168.31.0	192.168.31.255	ether1

Masquerade Setting

- Buatlah masquerade untuk ketiga gateway

The screenshot shows the Winbox Firewall interface with the NAT tab selected. There are three masquerade rules listed:

#	Action	Chain	Out. Interface	Bytes	Packets
0	masquerade	srcnat	wlan1	37.5 KiB	532
1	masquerade	srcnat	pppoe-out1	0 B	0
2	masquerade	srcnat	pptp-out1	460 B	8

Route-mark Setting

```
[admin@C31] /ip firewall mangle> print
Flags: X - disabled, I - invalid, D - dynamic
0  chain=prerouting action=mark-routing new-routing-mark=route-iix
  passthrough=no dst-address-list=nice in-interface=ether1

1  chain=output action=mark-routing new-routing-mark=route-iix passthrough=no
  dst-address-list=nice out-interface=pptp-out1
```

Rule no 0 untuk trafik dari klien

Rule no 1 untuk trafik dari local process di router

Rule no 1 menggunakan parameter
out-interface=pptp-out1 karena secara default,
routing keluar melalui pptp-out1

Route for IIX & Internasional

New Route

General Attributes

Dst. Address: 0.0.0.0/0

Gateway: 10.10.10.100
pppoe-out1
pppoe-out1

Check Gateway: ping

Type: unicast

Distance:

Scope: 30

Target Scope: 10

Routing Mark: route-iix

Pref. Source:

Route <0.0.0.0/0>

General Attributes

Dst. Address: 0.0.0.0/0

Gateway: pptp-out1

Check Gateway:

Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

● ● ● | Test dengan traceroute

```
valens-riyadis-macbook:~ valens$ traceroute www.yahoo.com
traceroute: Warning: www.yahoo.com has multiple addresses; using 98.137.149.56
traceroute to any-fp.wa1.b.yahoo.com (98.137.149.56), 64 hops max, 52 byte packets
 1  192.168.31.1 (192.168.31.1)  0.921 ms  0.351 ms  0.351 ms
 2  172.21.2.254 (172.21.2.254)  11.141 ms  1.218 ms  0.878 ms
 3  192.168.0.100 (192.168.0.100)  1.771 ms  1.797 ms  1.579 ms
 4  202-65-113-1.jogja.citra.net.id (202.65.113.1)  2.141 ms  3.092 ms  3.566 ms
```

```
valens-riyadis-macbook:~ valens$ traceroute www.mikrotik.co.id
traceroute to www.mikrotik.co.id (202.65.113.16), 64 hops max, 52 byte packets
 1  192.168.31.1 (192.168.31.1)  0.670 ms  0.265 ms  0.180 ms
 2  10.10.10.100 (10.10.10.100)  0.924 ms  0.808 ms  0.745 ms
 3  192.168.0.100 (192.168.0.100)  1.702 ms  1.450 ms  1.268 ms
 4  202-65-113-1.jogja.citra.net.id (202.65.113.1)  2.193 ms  1.852 ms  1.763 ms
```



Kekurangan 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 masq address yang berbeda. Koneksi bisa terputus.
- Info lebih lanjut mengenai hal ini:
 - <http://www.enyo.de/fw/security/notes/linux-dst-cache-dos.html>
 - <http://marc.info/?m=105217616607144>
 - <http://lkml.indiana.edu/hypermail/linux/net/0305.2/index.html#19>



Metode NTH

- NTH dilakukan dengan mengaktifkan counter pada mangle, dan kemudian dinamai (route mark) berdasarkan gatewaynya.
- Route mark kemudian digunakan sebagai dasar untuk membuat policy route.

● ● ● | Proses NTH pada Mangle

- Misalkan kita mempunyai 2 buah gateway (A dan B)
 - Koneksi pertama → route mark “conn-A”
 - Koneksi kedua → route mark “conn-B”
 - Koneksi ketiga → route mark “conn-A”
 - Koneksi keempat → route mark “conn-B”
 - Koneksi kelima → route mark “conn-A”
 - Dst.....

● ● ● | Proses NTH pada Routing

- Setelah ada route-mark, maka kita tinggal mengarahkan route mark tersebut ke gateway yang sesuai.
 - Route-mark “conn-A” ke gateway A
 - Route-mark “conn-B” ke gateway B

● ● ● Proses NTH pada Routing

New Route

General Attributes

Dst. Address: 0.0.0.0/0

Gateway: 192.168.3.2

Check Gateway:

Type: unicast

Distance:

Scope: 30

Target Scope: 10

Routing Mark: conn-A

New Route

General Attributes

Dst. Address: 0.0.0.0/0

Gateway: 192.168.4.2

Check Gateway:

Type: unicast

Distance:

Scope: 30

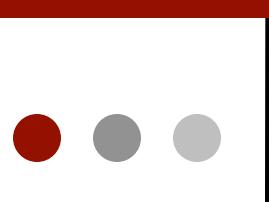
Target Scope: 10

Routing Mark: conn-B



Kelemahan nth

- Nth bekerja berdasarkan “connection tracking”
- Seperti halnya ECMP, nth juga ikut “ter-refresh” setiap 10 menit
- Mikrotik tidak menyarankan penggunaan nth untuk melakukan load balanced
- Untuk “load balanced” yang baik, disarankan menggunakan PCC (Per Connection Classifier)

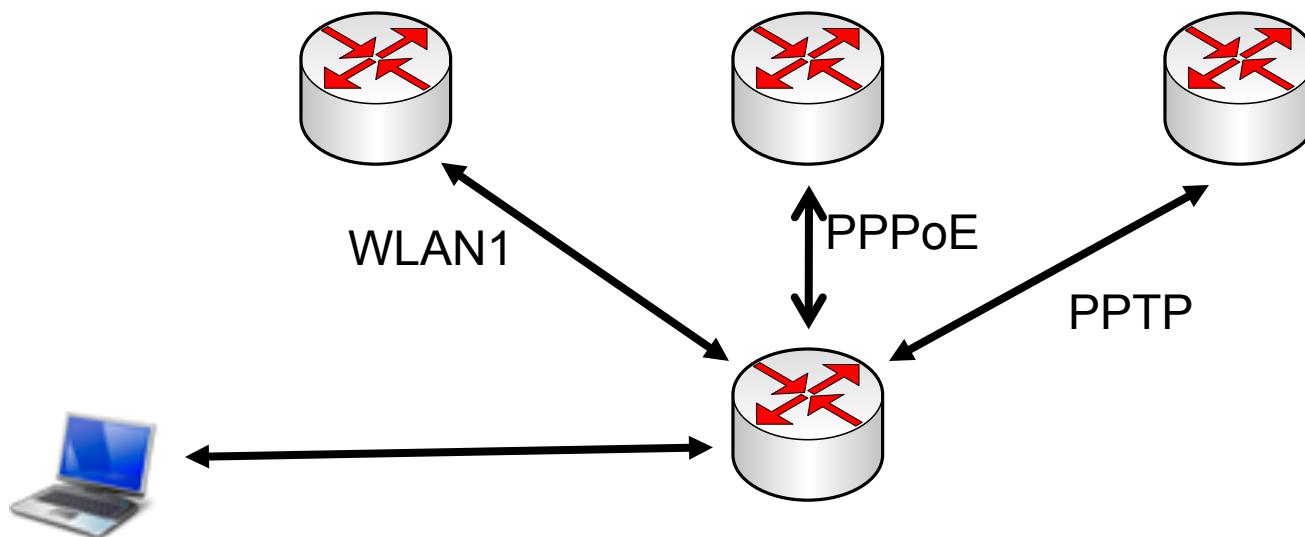


Per Connection Classifier

- Adalah parameter firewall yang memiliki kemampuan untuk membedakan trafik menjadi dua atau lebih stream berdasarkan parameter tetap terjaga, meskipun forwarding table pada kernel ter-refresh
- Option yang bisa digunakan adalah: src-address, src-port, dst-address, dst-port
- Informasi lebih lanjut:
 - <http://wiki.mikrotik.com/wiki/PCC>
- Diperkenalkan mulai RouterOS 3.24

[LAB-2] Load balanced PCC

- Dengan konfigurasi network seperti lab sebelumnya, gunakanlah wlan1, pppoe, dan pptp untuk load balanced dengan PCC



Trafik ke Connected Network

- Routing ke connected route hanya tersedia di routing table “main”
- Kita harus menjaga jangan sampai trafik ke network ini berpindah routing table.
- Kita membuat address-list untuk connected network

Trafik ke Connected Network

Firewall	
Filter Rules	NAT
Mangle	Service Ports
Connections	Address Lists
     	
Name	Address
connected-network	172.21.1.0/24
connected-network	10.10.10.0/24
connected-network	192.168.31.0/24
connected-network	172.21.2.0/24

```
[admin@C31] /ip firewall mangle> pr
```

Flags: X - disabled, I - invalid, D - dynamic

```
0  chain=prerouting action=accept dst-address-list=connected-network  
1  chain=output action=accept dst-address-list=connected-network
```

Koneksi dari luar

- Untuk menjamin bahwa router akan reply setiap connection yang masuk dari luar sesuai dengan jalur masuknya.
- 2 chain=prerouting action=mark-connection new-connection-mark=conn-1
passthrough=yes in-interface=wlan1 connection-mark=no-mark
- 3 chain=prerouting action=mark-connection new-connection-mark=conn-2
passthrough=yes in-interface=pppoe-out1 connection-mark=no-mark
- 4 chain=prerouting action=mark-connection new-connection-mark=conn-3
passthrough=yes in-interface=pptp-out1 connection-mark=no-mark

Custom Route-mark Chain

- Ada dua trafik yang harus di load balanced:
 - Trafik dari client
 - Chain=prerouting
 - In-interface=local (ether1)
 - Connection-mark=no-mark
 - Trafik dari local process
 - Chain=output
 - Connection-mark=no-mark
- Kedua trafik ini akan di jump ke chain baru

Jump to Custom Chain

```
5   ;;; jump to custom chain  
chain=prerouting action=jump jump-target=custom-routing  
in-interface=ether1 connection-mark=no-mark  
  
6   chain=output action=jump jump-target=custom-routing  
connection-mark=no-mark
```

PCC Rules

```
7    ;;; custom chain  
8      chain=custom-routing action=mark-connection new-connection-mark=conn-1  
9      passthrough=yes per-connection-classifier=both-addresses:3/0  
  
8      chain=custom-routing action=mark-connection new-connection-mark=conn-2  
9      passthrough=yes per-connection-classifier=both-addresses:3/1  
  
9      chain=custom-routing action=mark-connection new-connection-mark=conn-3  
9      passthrough=yes per-connection-classifier=both-addresses:3/2
```

Conn-mark → Route Mark

- 10 chain=prerouting action=mark-routing new-routing-mark=route1
passthrough=yes connection-mark=conn-1
- 11 chain=output action=mark-routing new-routing-mark=route1 passthrough=yes
connection-mark=conn-1
- 12 chain=prerouting action=mark-routing new-routing-mark=route2
passthrough=yes connection-mark=conn-2
- 13 chain=output action=mark-routing new-routing-mark=route2 passthrough=yes
connection-mark=conn-2
- 14 chain=prerouting action=mark-routing new-routing-mark=route3
passthrough=yes connection-mark=conn-3
- 15 chain=output action=mark-routing new-routing-mark=route3 passthrough=yes
connection-mark=conn-3

All Mangle

Firewall								
Filter Rules		NAT	Mangle	Service Ports	Connections	Address Lists	Layer7 Protocols	
#	Action	Chain	In. Interface	Connection Mark	Dst. Address List	Per Connection Cla...	New Connection...	New Routing Mark
;;; trafik ke connected network -- ACCEPT								
4	✓ accept	prerouting			connected-network			
5	✓ accept	output			connected-network			
;;; mark new-connection dari interface luar								
6	✓ mark connection	prerouting	wlan1	no-mark			conn-1	
7	✓ mark connection	prerouting	pppoe-out1	no-mark			conn-2	
8	✓ mark connection	prerouting	pptp-out1	no-mark			conn-3	
;;; jump to custom chain								
9	✓ jump	prerouting	ether1	no-mark				
10	✓ jump	output		no-mark				
;;; custom chain								
11	✓ mark connection	custom-routing			both addresses:3/0	conn-1		
12	✓ mark connection	custom-routing			both addresses:3/1	conn-2		
13	✓ mark connection	custom-routing			both addresses:3/2	conn-3		
;;; conn-mark --> route-mark								
14	✓ mark routing	prerouting		conn-1			route1	
15	✓ mark routing	output		conn-1			route1	
16	✓ mark routing	prerouting		conn-2			route2	
17	✓ mark routing	output		conn-2			route2	
18	✓ mark routing	prerouting		conn-3			route3	
19	✓ mark routing	output		conn-3			route3	
16 items out of 20								

Static Route

Route List						
	Routes	Nexthops	Rules	VRF		
	Dst. Address	Gateway	Check ...	Distance	Routing Mark	
AS	▶ 0.0.0.0/0	pppoe-out1 reachable, pptp-out1 reachable		1		
AS	▶ 0.0.0.0/0	10.10.10.100 reachable wlan1		1	route1	
AS	▶ 0.0.0.0/0	pppoe-out1 reachable		1	route2	
AS	▶ 0.0.0.0/0	pptp-out1 reachable		1	route3	
DAC	▶ 10.10.10.0/24	wlan1 reachable		0		10
AS	▶ 10.100.100.1	10.10.10.100 reachable wlan1		1		
DAC	▶ 172.21.1.254	pppoe-out1 reachable		0		17
DAC	▶ 172.21.2.254	pptp-out1 reachable		0		17
DAC	▶ 192.168.31.0/24	ether1 reachable		0		19

Beberapa Problem Lainnya

- Hati-hati untuk penggunaan DNS Server jika kita menggunakan DNS Server ISP dan menggunakan beberapa gateway dari ISP yang berbeda.
- Hal ini bisa diatasi dengan:
 - membuat static route untuk masing-masing DNS dan meng-accept IP DNS sehingga tidak ikut di PCC
 - Menggunakan dns public seperti google-dns