

---

# MTCRE

Mikrotik Certified Routing Engineer

# Selamat Datang

---

- Rekan2 bisa mengkoneksikan perangkat Devicenya ke Akses Point yang ada di ruangan ini dengan SSID dan password

**SSID : gpmnetwork | Password : gpmnetwork**

- Copy File Material training dari Flasdisk Trainer

*Let's Play Together*

*Membiasakan diri berdoa sebelum belajar*

---

اللَّهُمَّ إِنِّي أَسْأَلُكَ عِلْمًا نَافِعًا  
وَرِزْقًا طَيِّبًا وَعَمَلاً مُتَقَبِّلًا

“Allahumma inni as-aluka ‘ilman naafi'a wa rizqon  
thoyyibaa wa ‘amalan mutaqobbalaa”

# Andi Jehan Alhasan

## PENDIDIKAN :

- S1 IST Akprind Jogja, Teknik Informatika
- S2 Binus Jakarta, Magister Teknik Informatika



## BISNIS :

- GPMNETWORK IT Networking Training
- GPMNETWORK IT Consultant

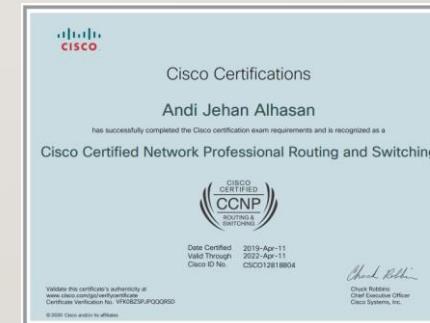


## CSR :

- GPMNETWORK Academy

## SERTIFIKASI :

MIKROTIK TRAINER, MTCNA, MTCRE, MTCINE,  
CCNA R/S, CCNP R/S & CCNP ENTERPRISE



## Social Media :

Instagram @gpmnetwork dan Facebook Andi Jehan

# Tentang GPMNETWORK

---

- Gpm Network** adalah perusahaan IT Network Consultant dan IT Solution yang fokus pada Infrastruktur Jaringan Komputer dan Keamanan Jaringan terletak di Balikpapan, Kalimantan Timur. Layanan kami meliputi, Network, Server, Voice/Voip ,Video surveillance.
- Our Client : Telkom Divre 6, UMKT, PT GAM, Logindo, Modular Mining, Polda Kaltim, Lintasarta, ICONPlus, Pemkot Balikpapan, Diskominfo Kukar, Sucofindo dan lainnya.
- Website : **gpmnetwork.id, drnet.id dan belajarcisco.id**

# Perkenalkan Diri Anda

---

- Nama
- Pekerjaan sehari-hari
- Pengalaman menggunakan Mikrotik
- Pengalaman mengenai jaringan
- Diharapkan dari mengikuti training ini

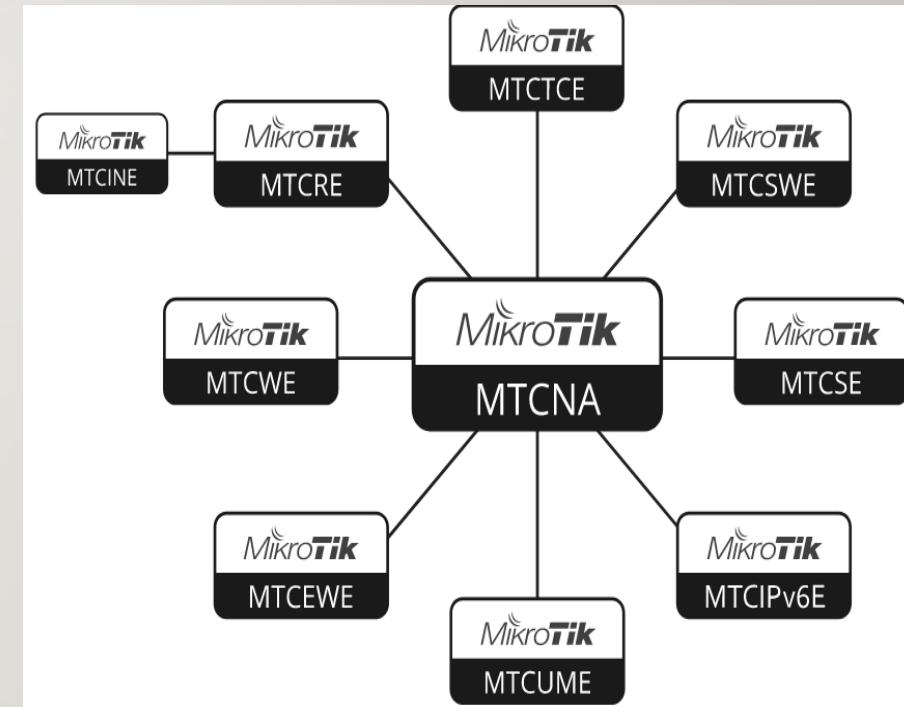
# Tentang Ujian Mikrotik

---

- Ujian dilakukan online melalui mikrotik.com
- Dilakukan pada sesi terakhir training
- Terdapat 25 soal dalam waktu 60 menit
- Nilai minimal kelulusan 60 %
- Nilai antara 50-59 % mendapatkan kesempatan kedua ujian kembali
- Mikrotik academy minimal score 75% (MTCNA dan MTCRE)
- Peserta yang lulus akan mendapatkan sertifikasi MTCRE yang diakui secara international

# SERTIFIKASI MIKROTIK

- A. **MTCNA** - MikroTik Certified Network Associate
- B. **MTCRE** - MikroTik Certified Routing Engineer
- C. **MTCWE** - MikroTik Certified Wireless Engineer
- D. **MTCTCE** - MikroTik Certified Traffic Control Engineer
- E. **MTCUME** - MikroTik Certified User Management Engineer
- F. **MTCINE** - MikroTik Certified Inter-Networking Engineer
- G. **MTCIPv6E** - MikroTik Certified IPv6 Engineer
- H. **MTCSE** - MikroTik Certified Security Engineer
- I. **MTCSWE** - MikroTik Certified Switching Engineer
- J. **MTCEWE** - MikroTik Certified Enterprise Wireless Engineer



# TRAINING MATERIAL

---

1. Connected Route
2. Static Routing
3. Tunnel dan VPN
4. Dynamic Route OSPF
5. VLAN

---

# Pre test

## Jaringan peer to peer

# Pre-test

---

- Buatlah kelompok berisi dua orang
- Config ip address PC seperti di bawah ini
- Tujuannya: ping dari PC 1 ke PC 2 =Reply!!



PC 1

192.168.1.1/24

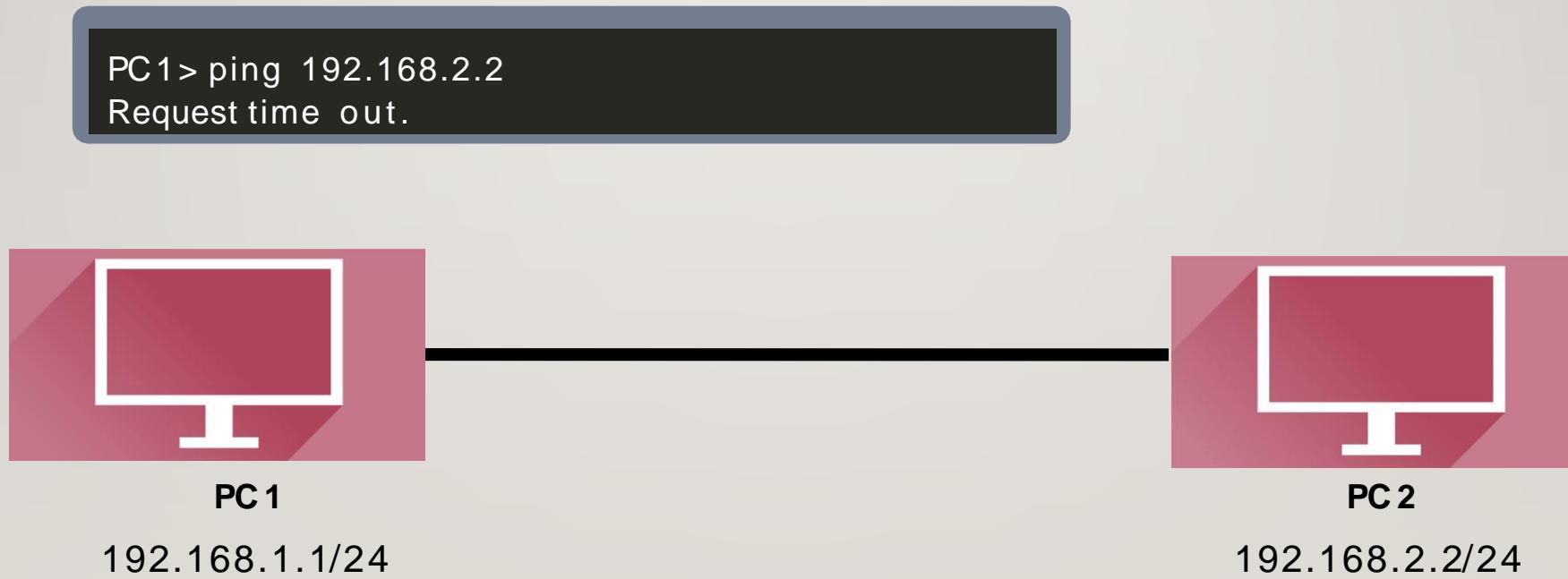


PC 2

192.168.1.2/24

# Gantilah IP seperti di topology bawah ini

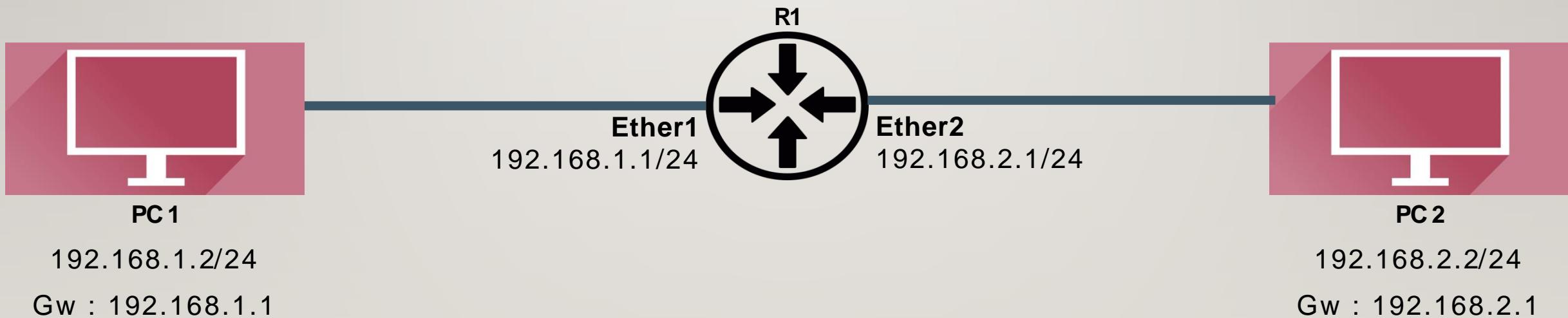
Ping tidak akan terhubung, karena berbeda network IP antar PC



# Diperlukan perangkat router

Router dapat menghubungkan IP Address yang berbeda network

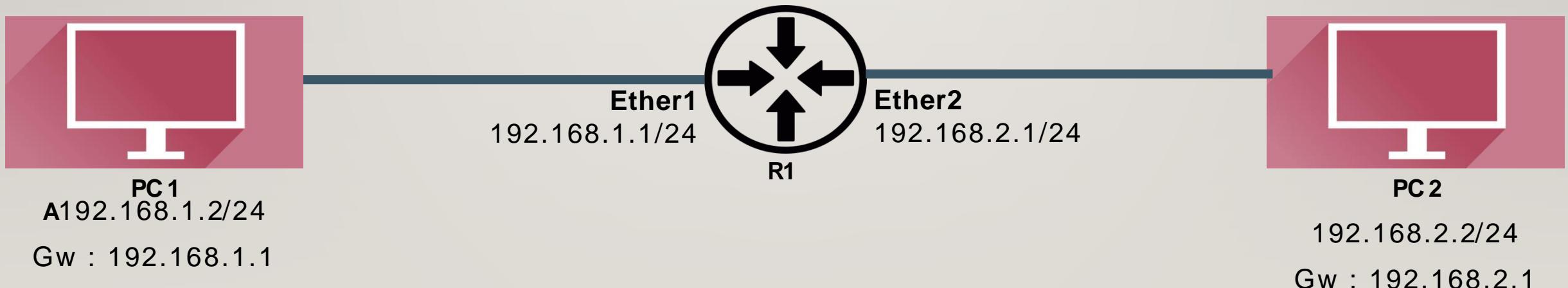
---



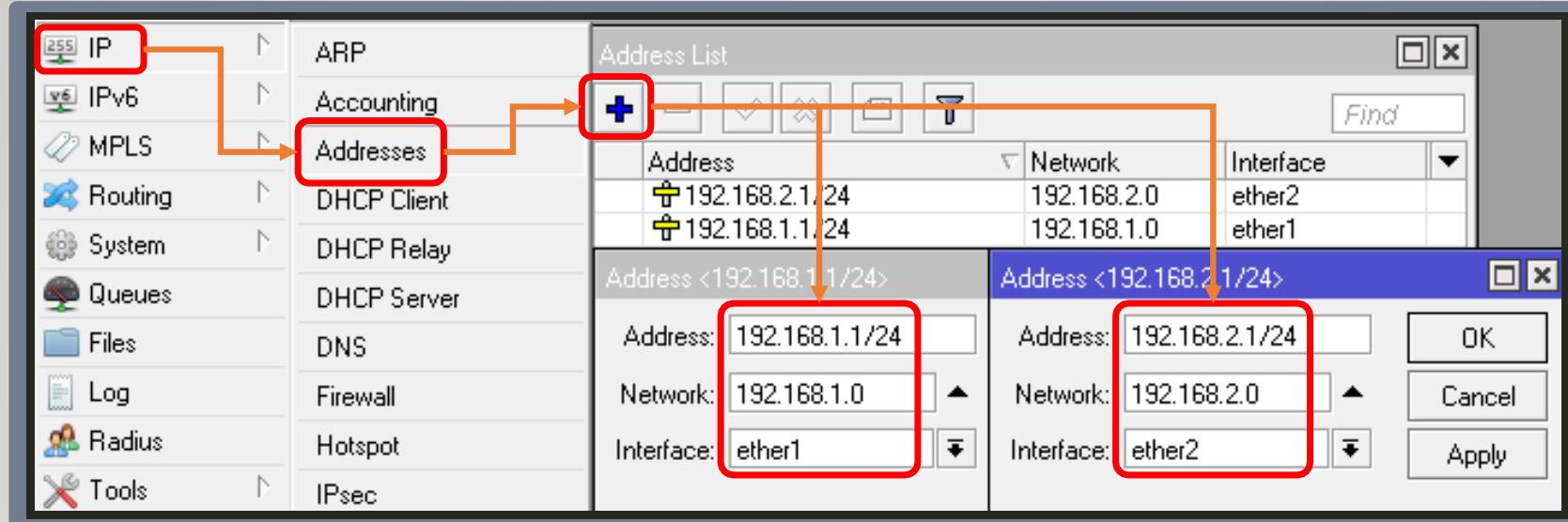
# Menghubungkan Kedua PC yang berbeda network IP

---

- Buatlah topology seperti dibawah ini
- Konfigurasikan IP Address masing-masing PC 1 dan PC 2 sesuai topology, dan jangan lupa konfig IP Gateway di kedua PC
- Cukup tambahkan konfigurasi IP Address di masing-masing interface mikrotik, PC 1 akan dapat berkomunikasi dengan PC 2

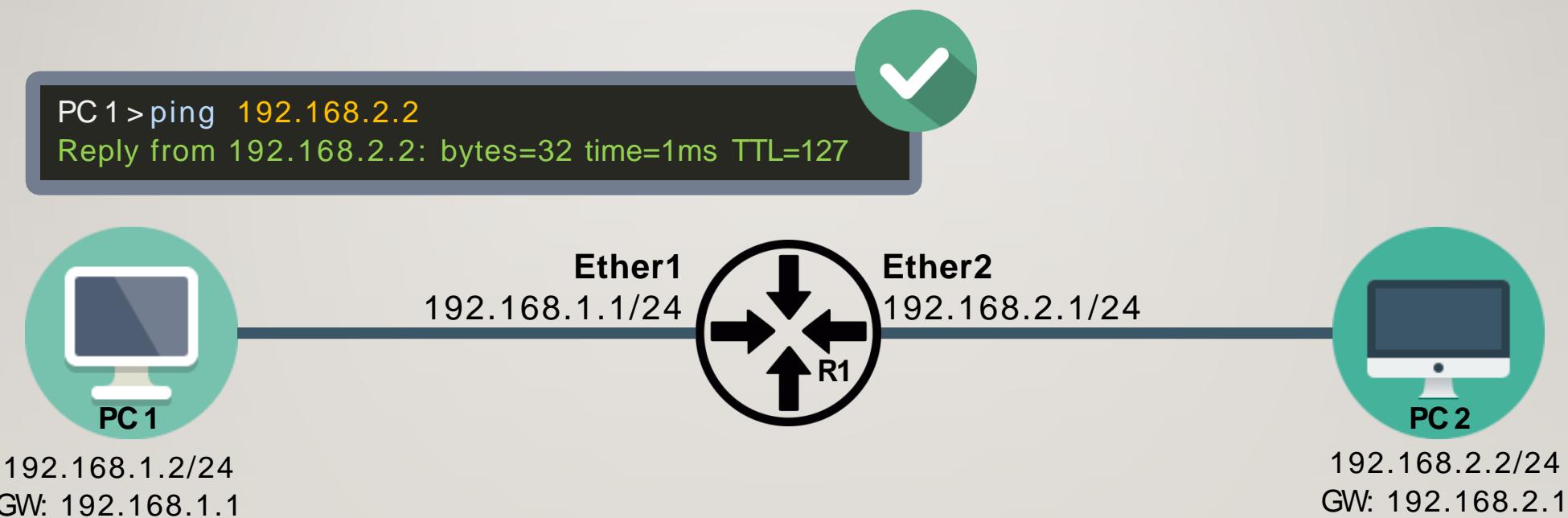


# Konfigurasi IP Address di Router



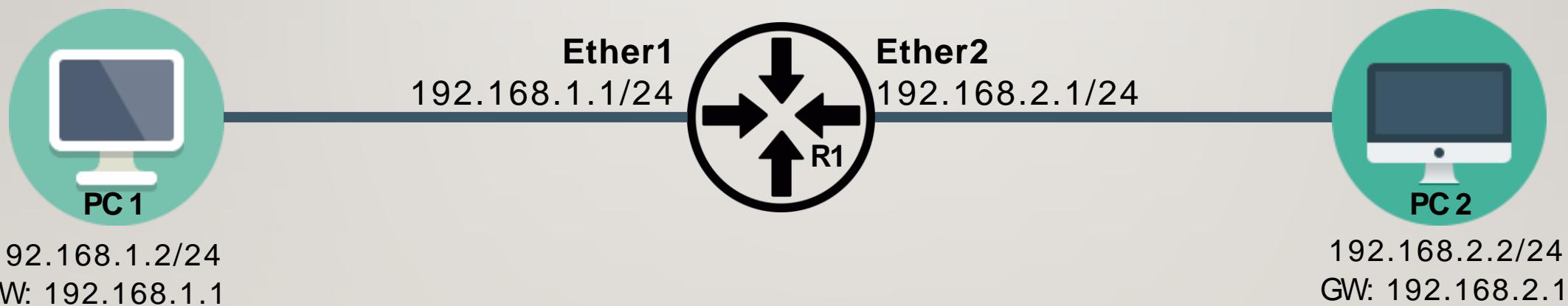
# Test ping dari PC 1 ke PC 2

---



# traceroute dari PC 1 ke PC 2

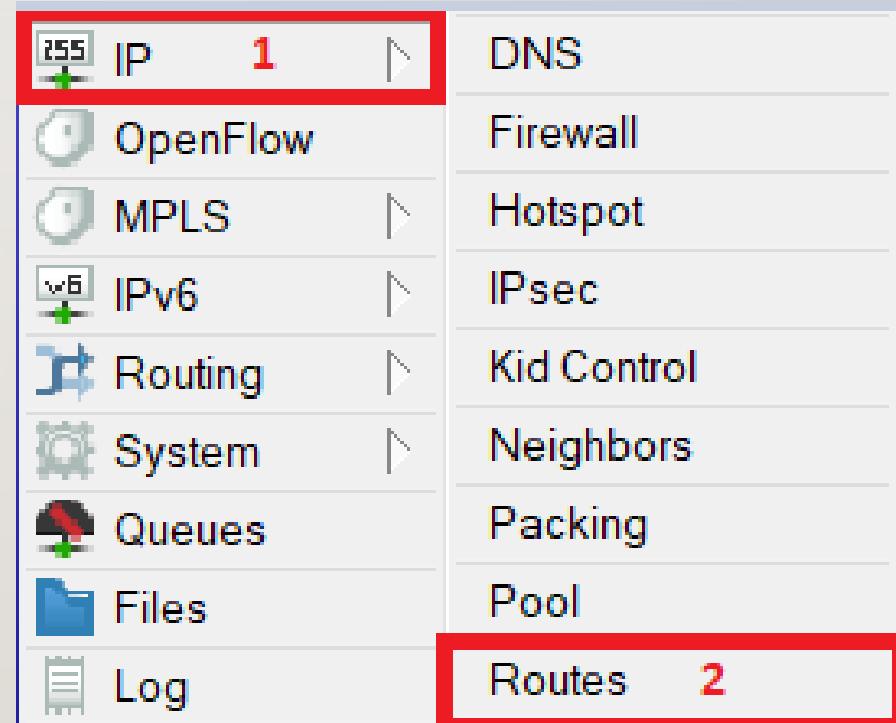
```
PC 1> tracert 192.168.2.2
1 1ms 1ms 1ms 192.168.1.1
2 1ms 1ms 1ms 192.168.2.2
```



---

# **MEMAHAMI CARA KERJA ROUTER**

# Lihat routing table

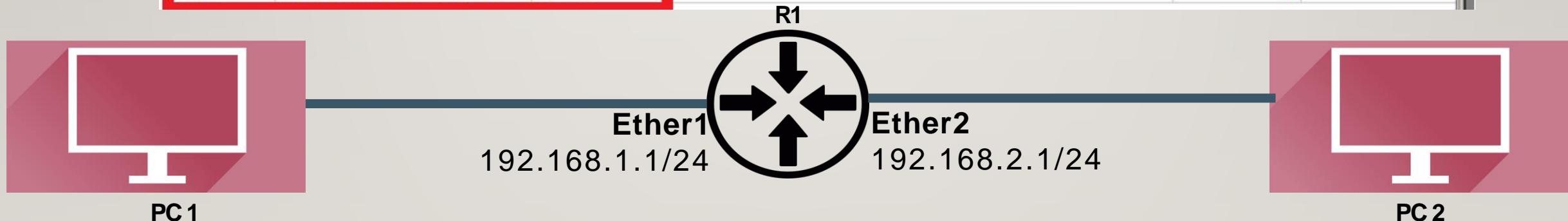


# Connected route

DAC = Dynamic, Active, Connected

Otomatis akan ada setiap menambahkan IPAddress

Route List					
	Routes	Rules			
	+ -	✓ ✗	✖	Filter	Find
	Dst. Address	Gateway	Distance	Pref. Source	
DAd	▶ 0.0.0.0/0	192.168.122.1	1		
DAC	▶ 192.168.100.0/24	ether2	0		
DAC	▶ 192.168.122.0/24	ether1	0		



192.168.1.2/24

Gw : 192.168.1.1

192.168.2.2/24

Gw : 192.168.2.1

# Connected route

---

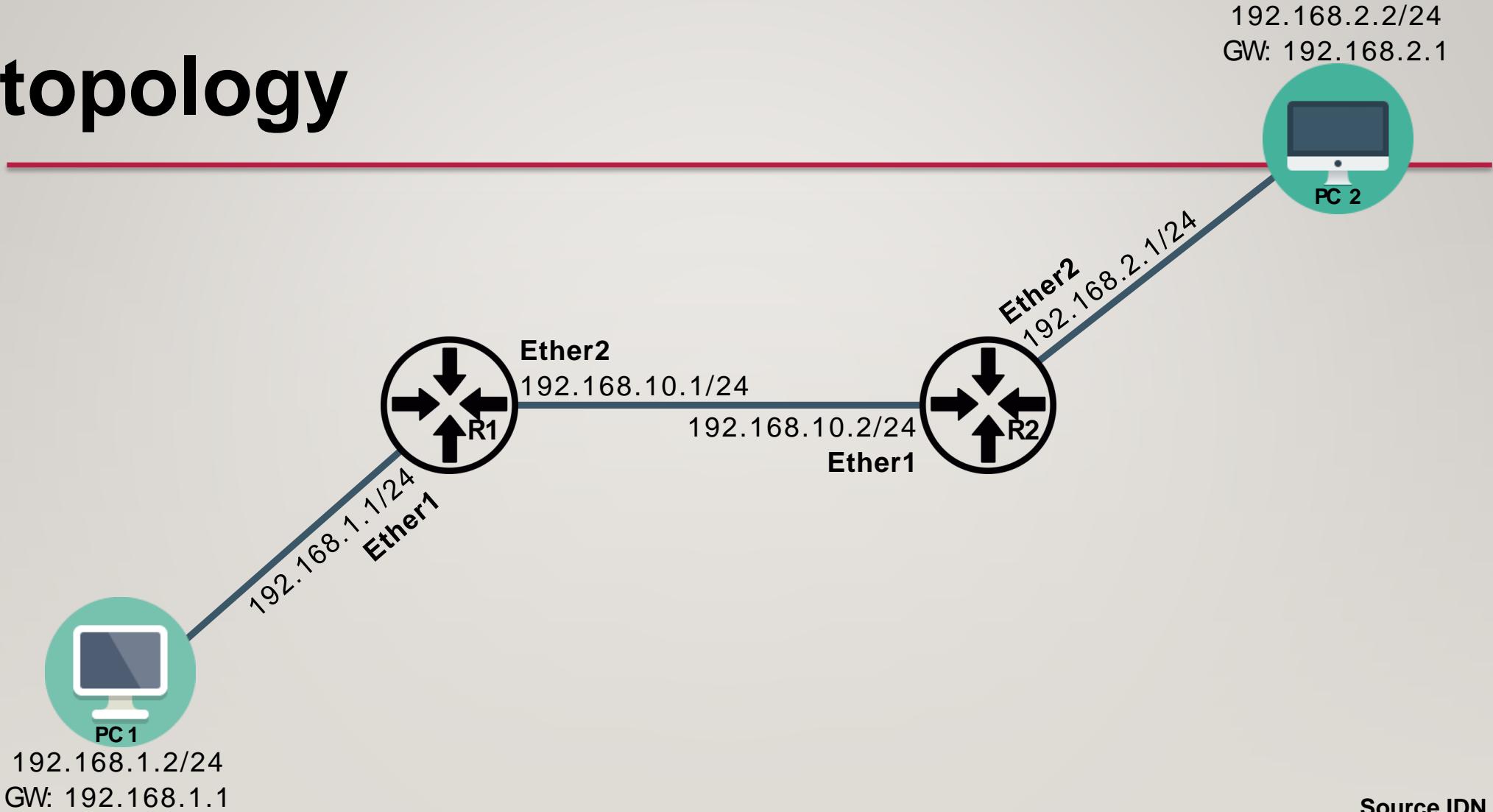
- Route akan muncul secara otomatis pada saat kita menambahkan IP address di router
- Jika terdapat **dua buah IP Address** yang berasal dari subnet yang sama pada **sebuah interface**, hanya akan ada **satu connected route**.
- Jangan menempatkan **dua ip address dari subnet yang sama** pada **dua interface yang berbeda**, karena akan membingungkan tabel dan logika routing di router.

---

**kapan perlu  
menambah route baru di router?**

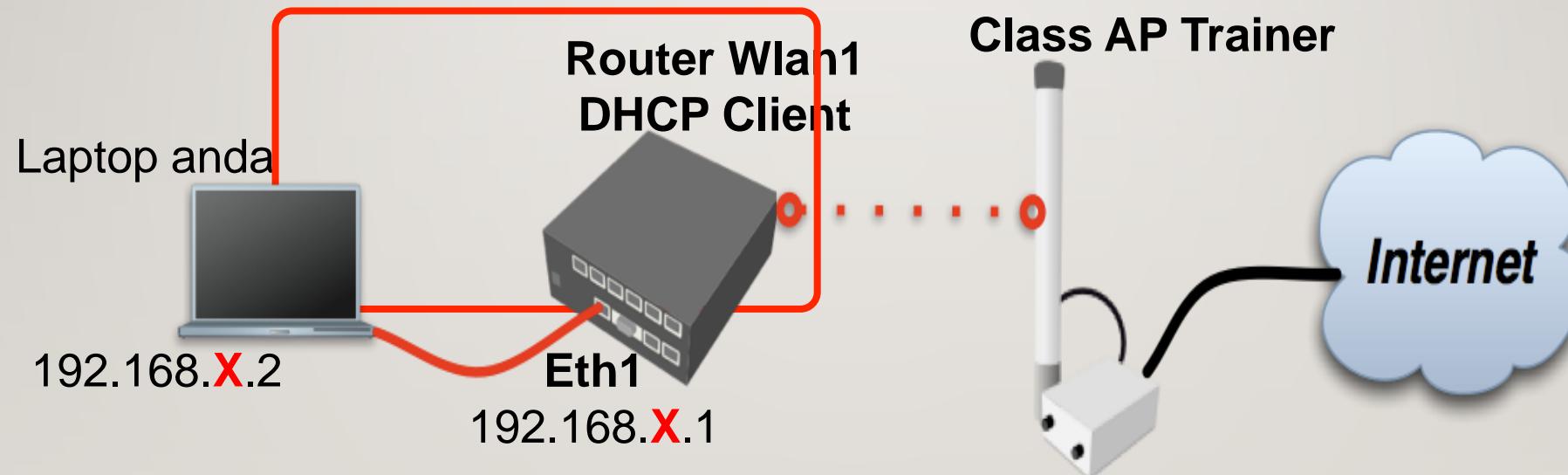
# topology

---



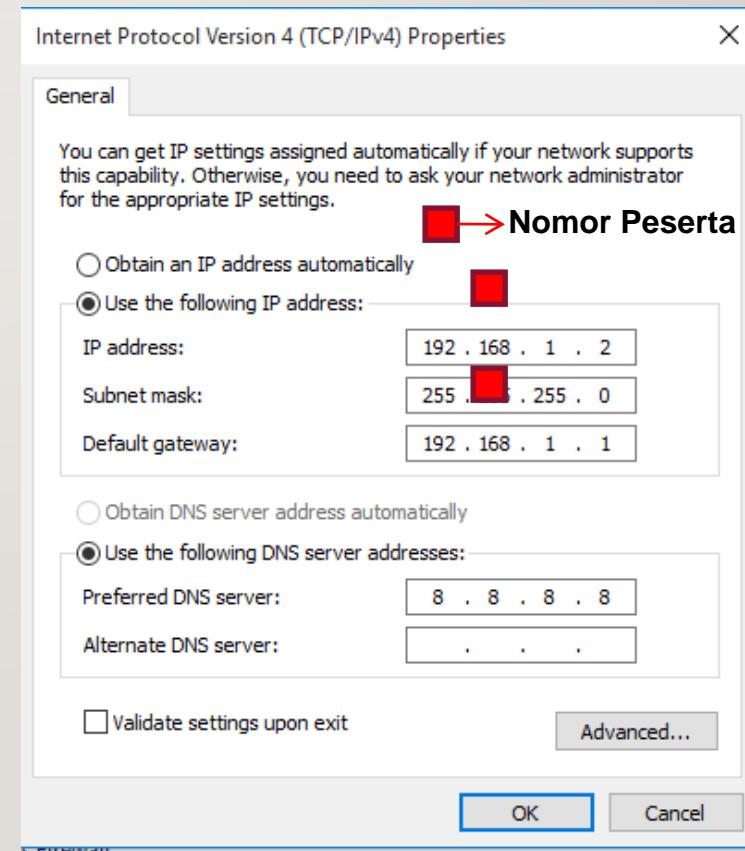
# Setting Router Dalam Kelas Training

**X = Nomer peserta**



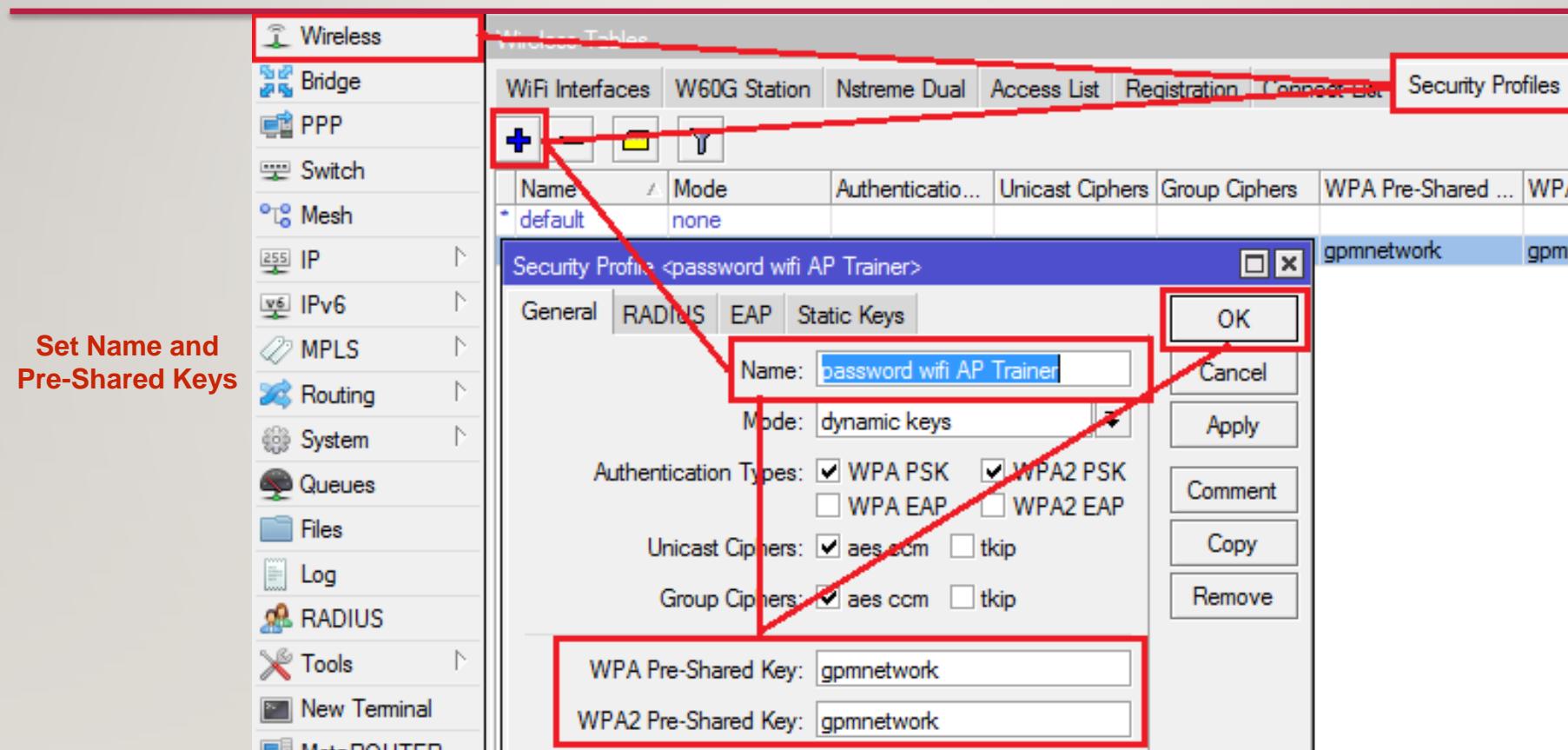
# Setting IP Address Laptop

- **IP address :** 192.168.X.2
- **Subnet Mask :** 255.255.255.0 (/24)
- **Gateway :** 192.168.X.1
- **DNS :** 8.8.8.8

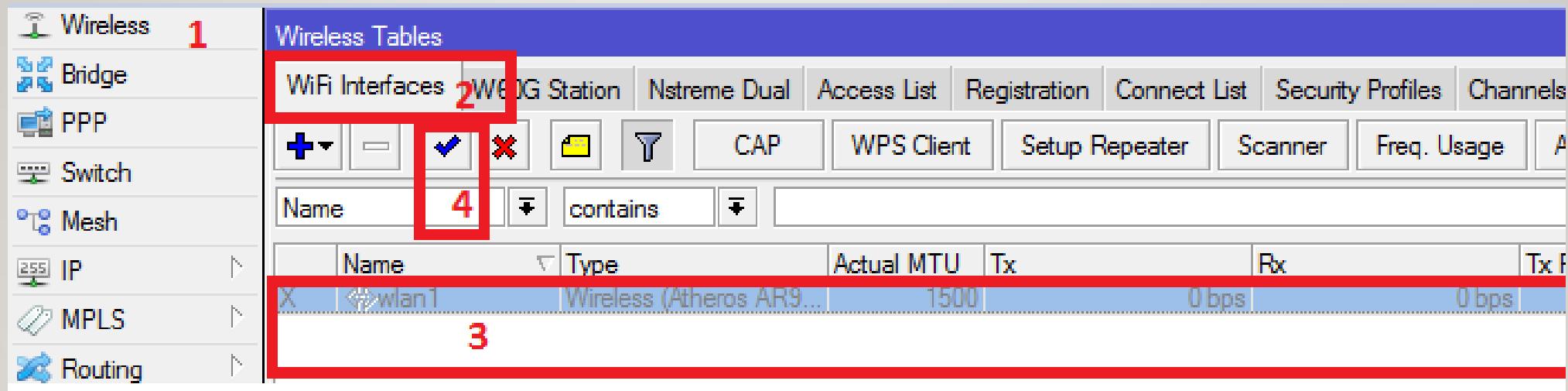


LAB

# Router – Memasukkan Password



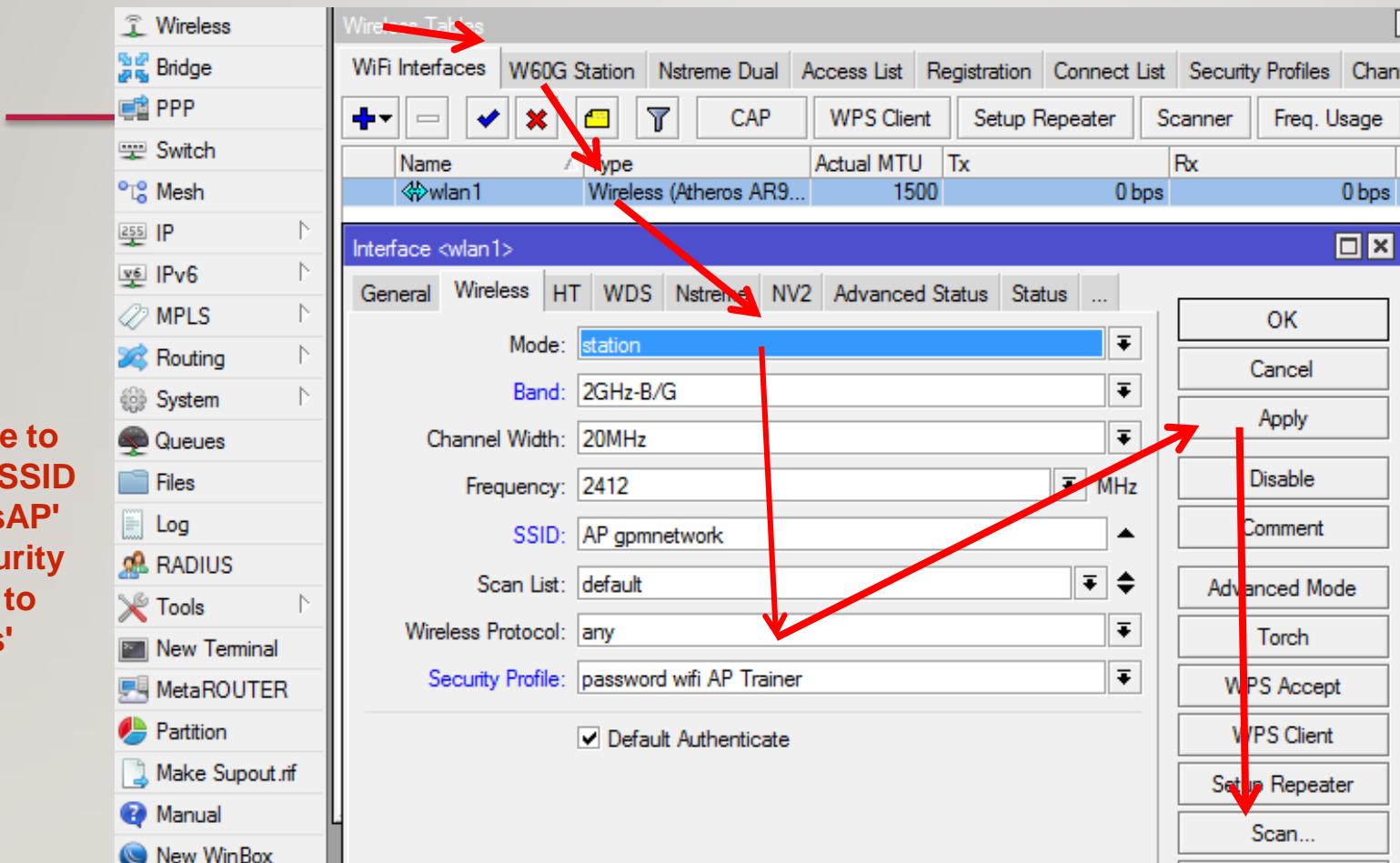
# Enable Wireless Interface



LAB

# Setting RB sebagai wireless Client

Set Mode to  
'station', SSID  
to 'ClassAP'  
and Security  
Profile to  
'class'



Wireless → Interfaces

# Mengkoneksikan ke AP Trainer

The screenshot shows two windows from the NetworkMiner tool. On the left, the 'Scanner' window displays a list of wireless interfaces and nearby access points (APs). An interface named 'wlan1' is selected. A red arrow points from the 'wlan1' selection in the Scanner window to the 'Registration' tab in the Wireless Tables window on the right. Another red arrow points from the 'wlan1' selection in the Scanner window down to the 'Connected to ess' status at the bottom of the Scanner window.

**Scanner**

Interface: wlan1

Background Scan

Address SSID Channel Signal... Noise... Signa...

AP	FC:A6:CD:39:32:E0	tie2nDpurple	2412/2...	-83	-100	11
AP	2C:95:7F:A6:A1:44	alzen	2432/2...	-49	-102	53
AP	AC:64:62:E1:45:1A	JAPON 2	2437/2...	-91	-100	5
A	AC:64:62:E1:45:1B	@wifid	2437/2...	-92	-100	5
AP	C8:3A:35:23:D9:98	Tanda_23D998	2442/2...	-39	-100	6
AP	C8:3A:35:23:D9:A0	GPM	2442/2...	-7	-100	20
AP	72:B5:7E:B1:61:B0	AlzenB6	2452/2...	-94	-100	0

14 items (1 selected)

enabled running slave connected to ess

**Wireless Tables**

Wireless

Bridge PPP Switch Mesh

WiFi Interfaces W60G Station Nstreme Dual Access List Registration Connect List Security Profiles Channels

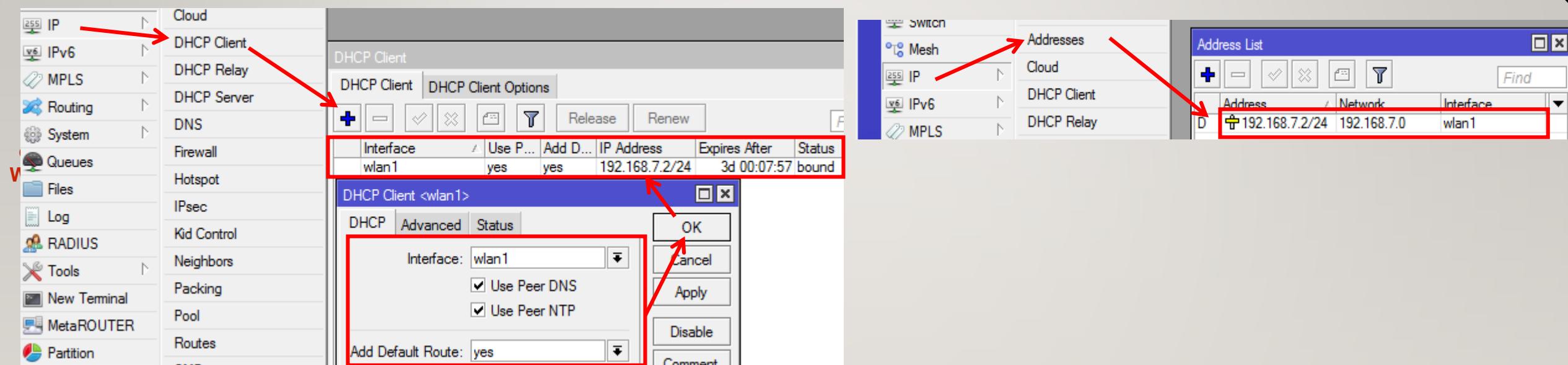
Reset

Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activit...	Tx/Rx Signal ...	Tx Rate	Rx Rate
	C8:3A:35:23:D9:98	wlan1	00:06:30	yes	no	7.680 -40	1Mbps	1Mbps	

**Wireless → Registration**

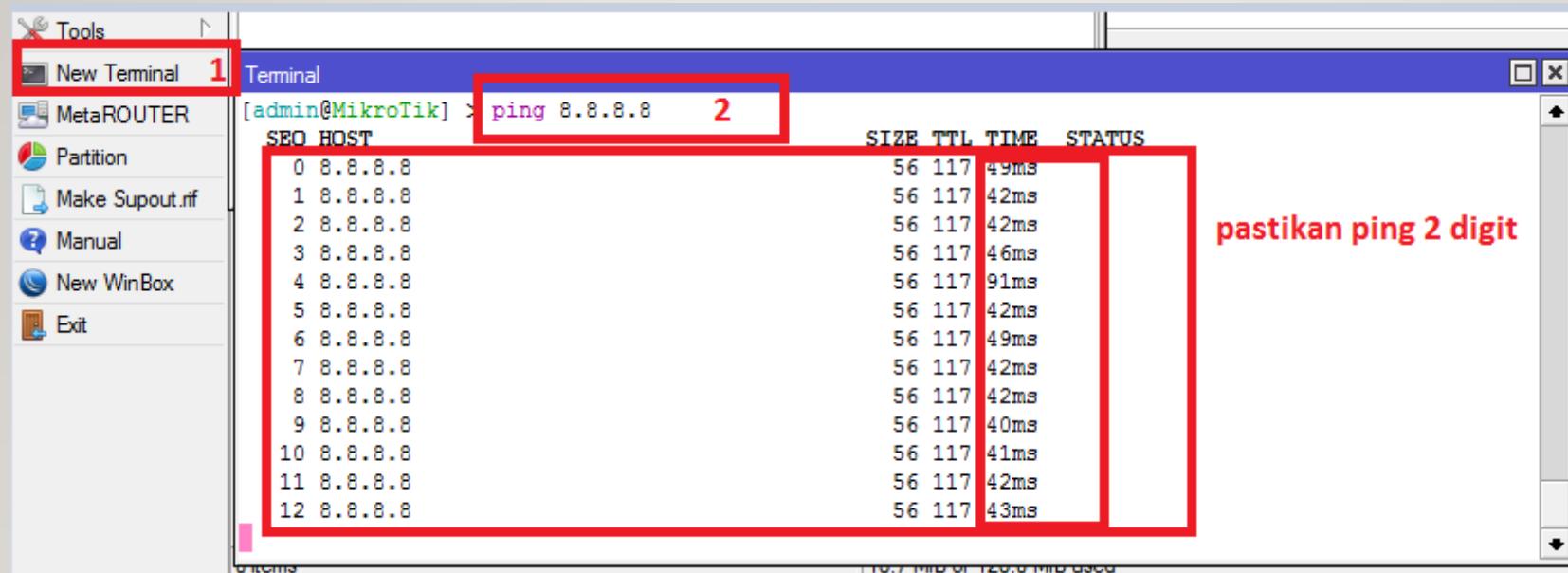
Registration adalah yang digunakan untuk melihat koneksi dan stabilitas point to point wireless

# Meminta IP Address pada AP Trainer

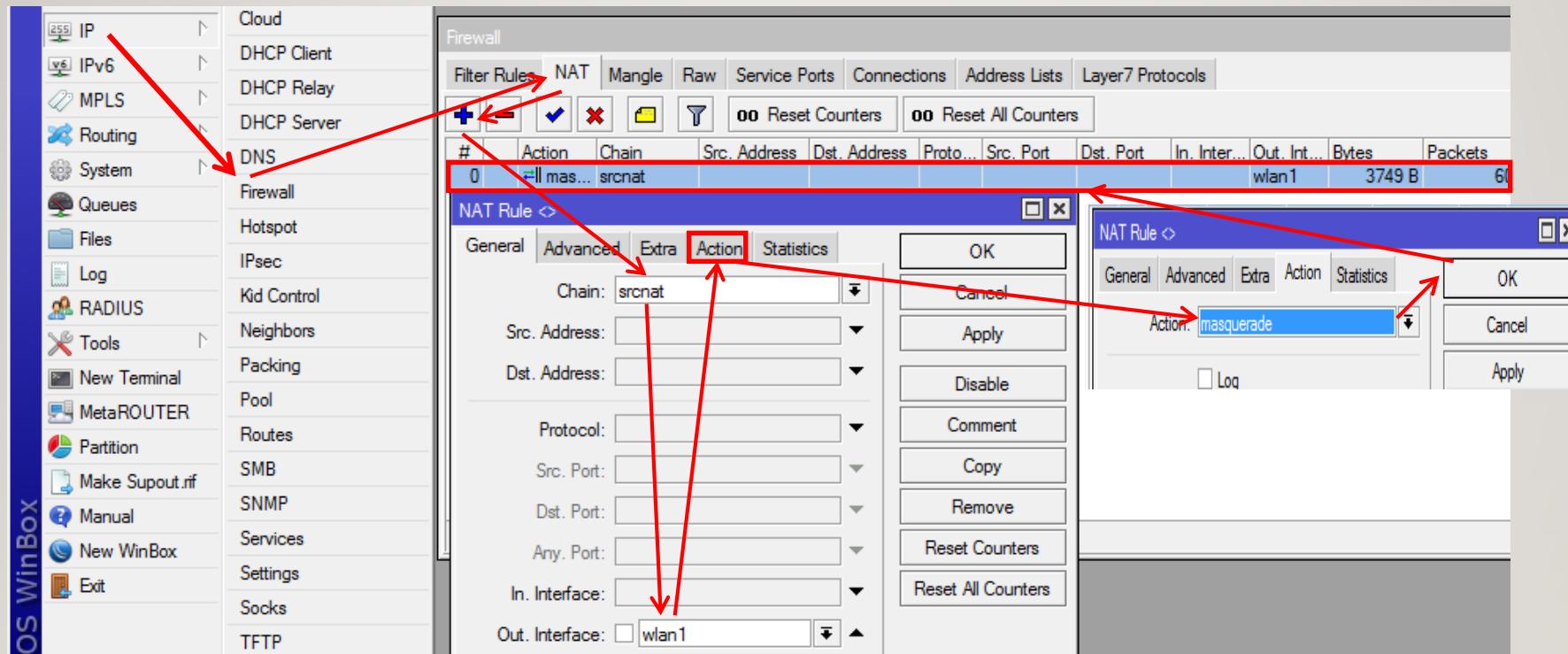


IP → DHCP Client & IP → Address

# Memastikan konektifitas internet dari RB ke internet



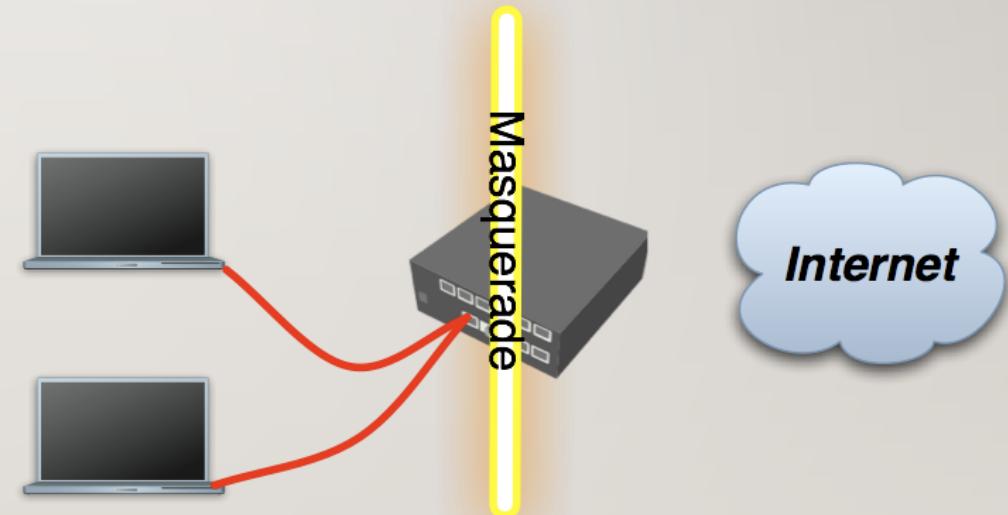
# Setting NAT



IP → Firewall → NAT  
Konfigurasi masquerade pada Wlan Interface

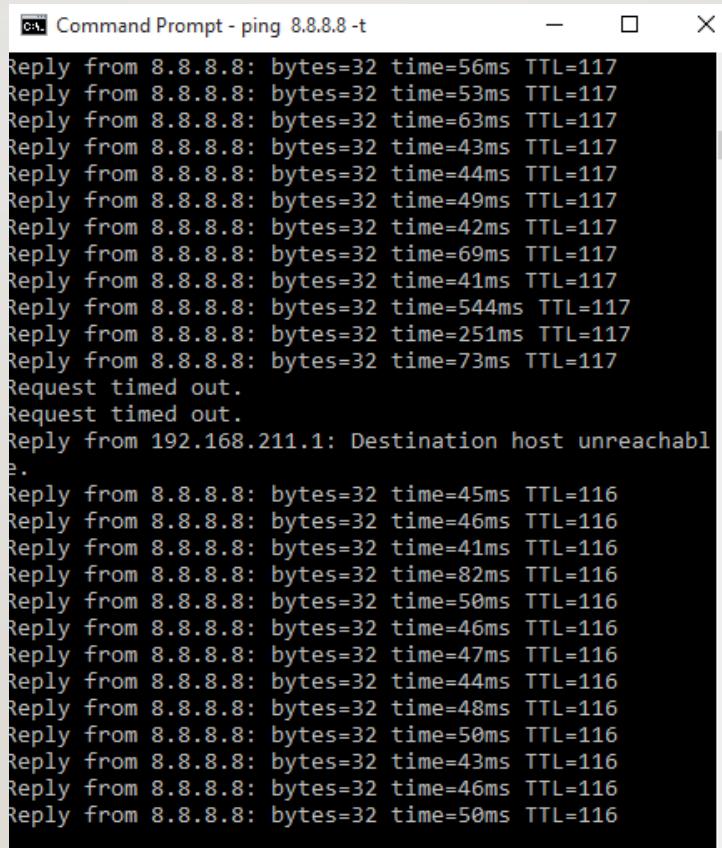
# Private & Public Space

- Dilakukan Masquerade agar jaringan private dapat diketahui oleh jaringan public atau internet
- Termasuk IP Private adalah
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255



# Disable koneksi wireless di Laptop, pastikan akses internet via LAN Ethernet

---



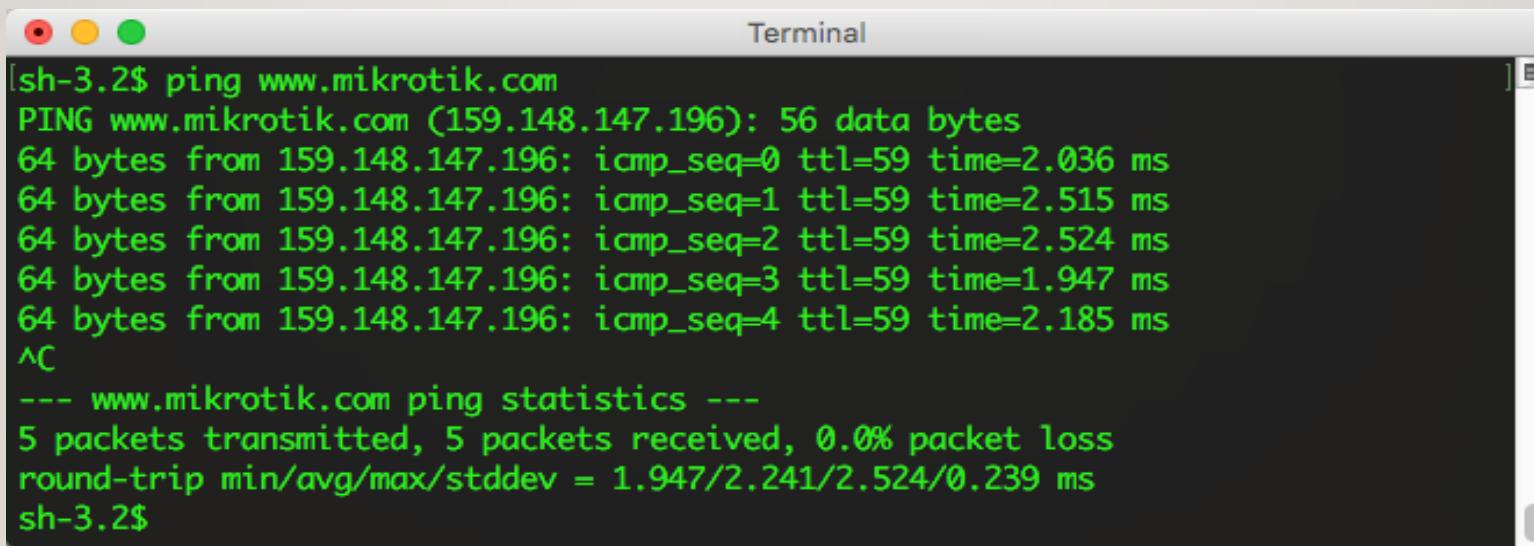
A screenshot of a Windows Command Prompt window titled "Command Prompt - ping 8.8.8.8 -t". The window displays the results of a ping test to the IP address 8.8.8.8. The output shows multiple replies from the destination host, with varying round-trip times (RTTs) and Time-to-Live (TTL) values. The replies are as follows:

```
Reply from 8.8.8.8: bytes=32 time=56ms TTL=117
Reply from 8.8.8.8: bytes=32 time=53ms TTL=117
Reply from 8.8.8.8: bytes=32 time=63ms TTL=117
Reply from 8.8.8.8: bytes=32 time=43ms TTL=117
Reply from 8.8.8.8: bytes=32 time=44ms TTL=117
Reply from 8.8.8.8: bytes=32 time=49ms TTL=117
Reply from 8.8.8.8: bytes=32 time=42ms TTL=117
Reply from 8.8.8.8: bytes=32 time=69ms TTL=117
Reply from 8.8.8.8: bytes=32 time=41ms TTL=117
Reply from 8.8.8.8: bytes=32 time=544ms TTL=117
Reply from 8.8.8.8: bytes=32 time=251ms TTL=117
Reply from 8.8.8.8: bytes=32 time=73ms TTL=117
Request timed out.
Request timed out.
Reply from 192.168.211.1: Destination host unreachable.
Reply from 8.8.8.8: bytes=32 time=45ms TTL=116
Reply from 8.8.8.8: bytes=32 time=46ms TTL=116
Reply from 8.8.8.8: bytes=32 time=41ms TTL=116
Reply from 8.8.8.8: bytes=32 time=82ms TTL=116
Reply from 8.8.8.8: bytes=32 time=50ms TTL=116
Reply from 8.8.8.8: bytes=32 time=46ms TTL=116
Reply from 8.8.8.8: bytes=32 time=47ms TTL=116
Reply from 8.8.8.8: bytes=32 time=44ms TTL=116
Reply from 8.8.8.8: bytes=32 time=48ms TTL=116
Reply from 8.8.8.8: bytes=32 time=50ms TTL=116
Reply from 8.8.8.8: bytes=32 time=43ms TTL=116
Reply from 8.8.8.8: bytes=32 time=46ms TTL=116
Reply from 8.8.8.8: bytes=32 time=50ms TTL=116
```

# Cek Konektifitas ke internet

---

- Lakukan ping atau traceroute untuk windows pc ke webpage mikrotik.com pada menu **new terminal**



The screenshot shows a Mac OS X Terminal window titled "Terminal". The window contains the following text output from a ping command:

```
[sh-3.2$ ping www.mikrotik.com
PING www.mikrotik.com (159.148.147.196): 56 data bytes
64 bytes from 159.148.147.196: icmp_seq=0 ttl=59 time=2.036 ms
64 bytes from 159.148.147.196: icmp_seq=1 ttl=59 time=2.515 ms
64 bytes from 159.148.147.196: icmp_seq=2 ttl=59 time=2.524 ms
64 bytes from 159.148.147.196: icmp_seq=3 ttl=59 time=1.947 ms
64 bytes from 159.148.147.196: icmp_seq=4 ttl=59 time=2.185 ms
^C
--- www.mikrotik.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.947/2.241/2.524/0.239 ms
sh-3.2$
```

# Troubleshooting

---

- Router tidak bisa ping AP ?
- Laptop tidak bisa ping Router ?
- Masquerade tidak berhasil ?

# Mikrotik Certified Routing Engineer (MTCRE)

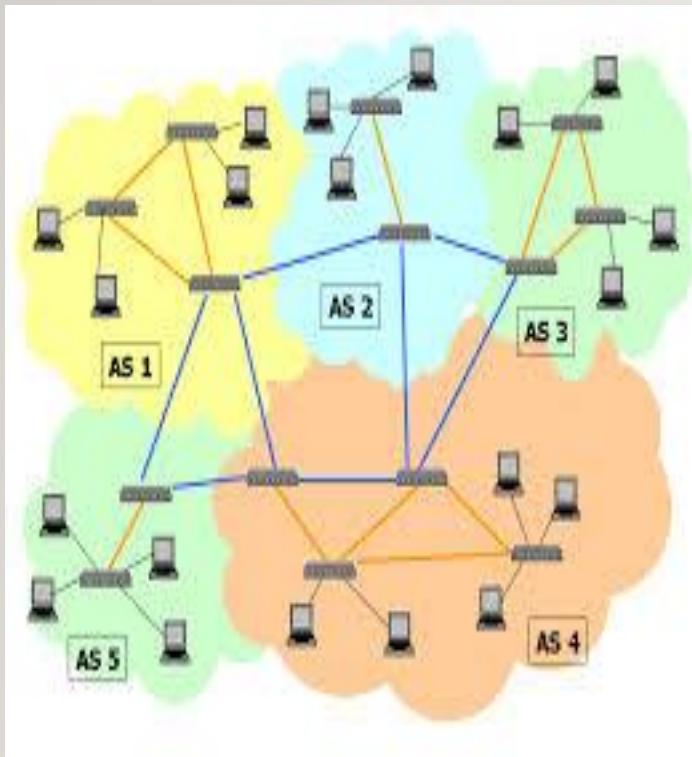
---

## Routing

# Routing

Banyak router di dunia saling terhubung, dengan routing protocol dan membentuk dinamakan internetworking (Internet)

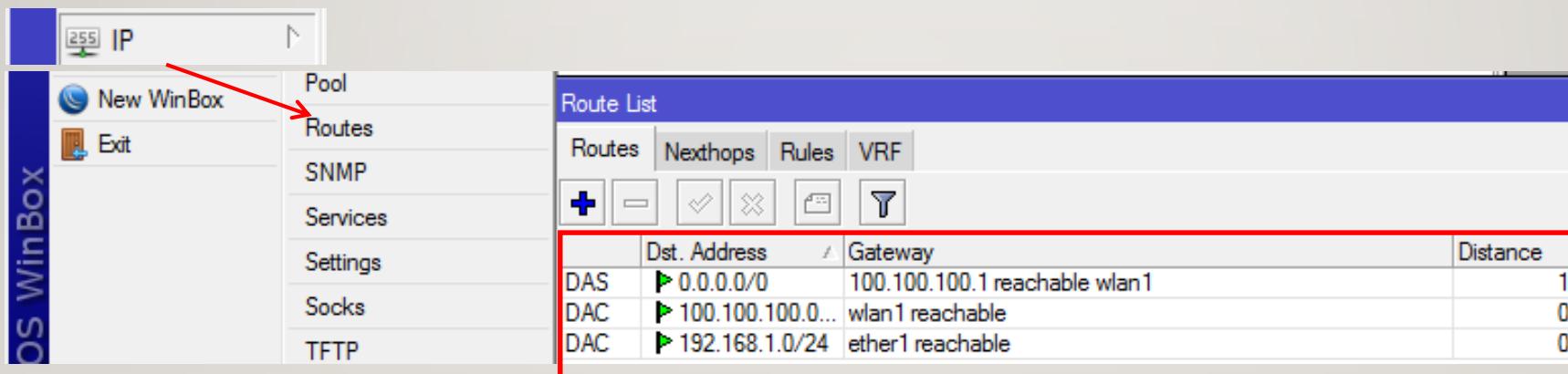
---



# Routing

---

- OSI Layer berkerja pada layer 3
- Fitur routing rules di mikrotik mendefinisikan tujuan packet akan dikirimkan



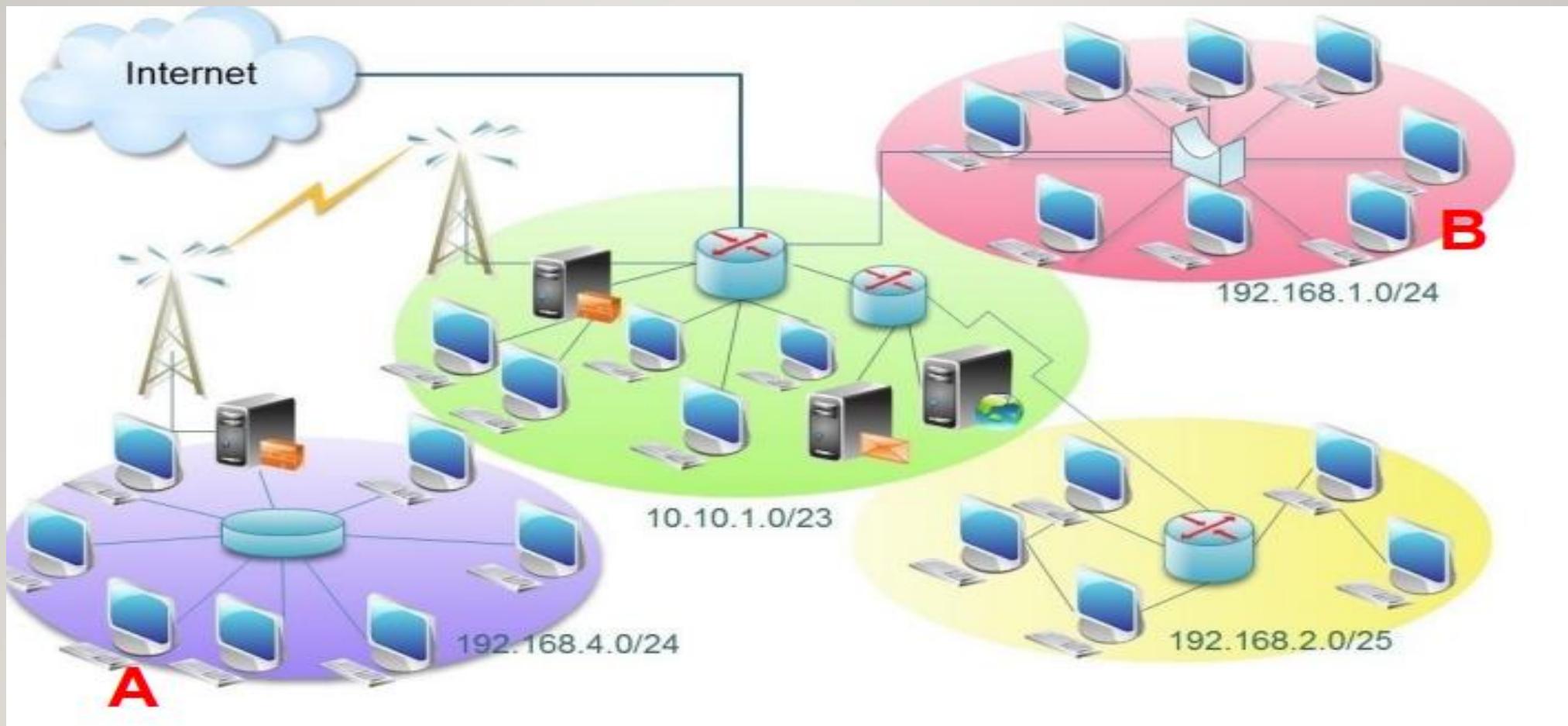
**IP → Routes**

# **Tipe Routing Protocol**

---

- Static Route ( network skala kecil )
- Dynamic Route ( network Skala Besar)
- Default Route ( route untuk terhubung ke Internet)

# Routing



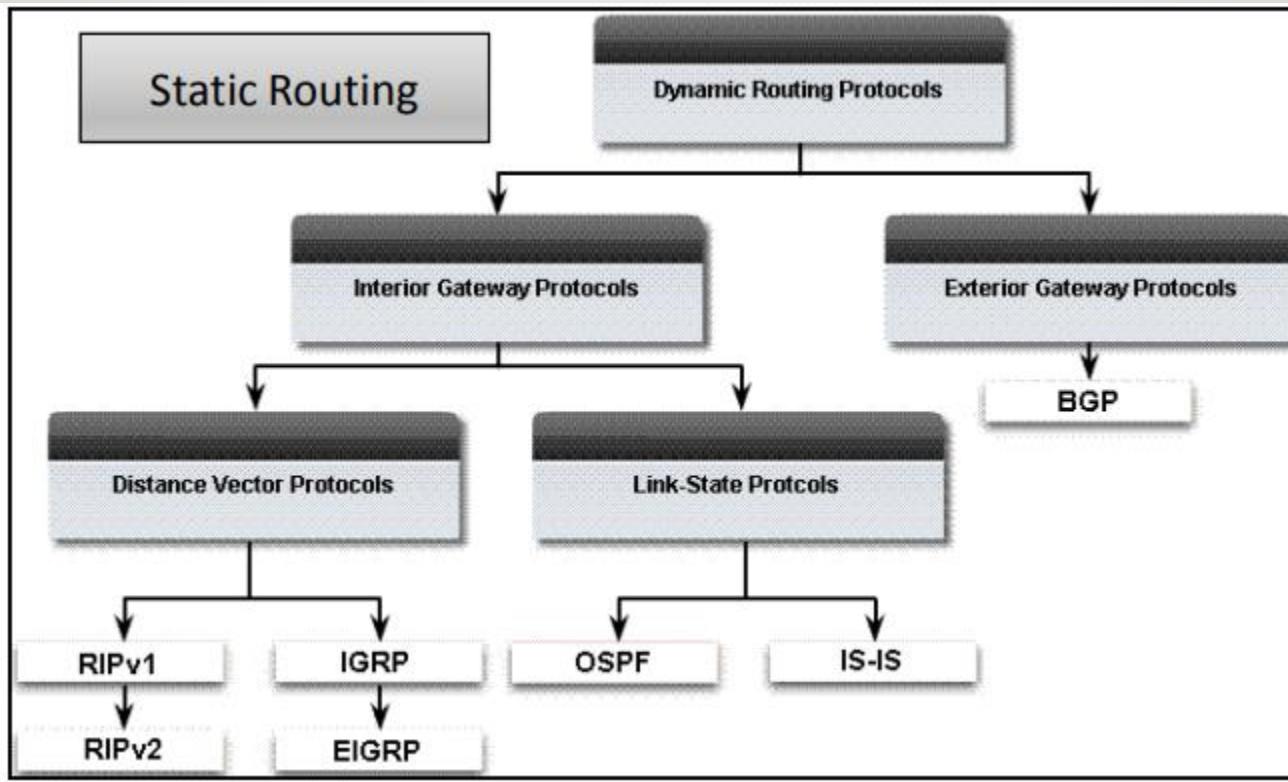
# ROUTING

---

- Routing dibutuhkan ketika jaringan kita berkembang menjadi lebih kompleks
- Untuk pengelolaan jaringan dengan lebih baik
- Lebih aman
- Traffic broadcast hanya disebarluaskan / dikonsentrasi di setiap subnet/ networknya saja
- Koneksi antar public IP
- Memungkinkan kita melakukan pemantauan dan pengelolaan jaringan yang lebih baik
- Untuk network skala besar, bisa digunakan Dynamic Routing (RIP/OSPF/BGP)

# ROUTING (Klasifikasi Routing )

---



# ROUTING

---

## Terminologi Routing

- **Routing** : Proses untuk meneruskan paket-paket antar network yang berbeda
- **Static Routing** : Pemetaan jalur routing yang dilakukan secara manual oleh administrator jaringan dengan cara memetakan setiap jalur/router yang dilalui oleh setiap paket dalam jaringan
- **Dynamic Routing** : Pemetaan konfigurasi yang dilakukan oleh routing protocol dengan hanya melakukan sedikit konfigurasi oleh administrator jaringan

# ROUTING

---

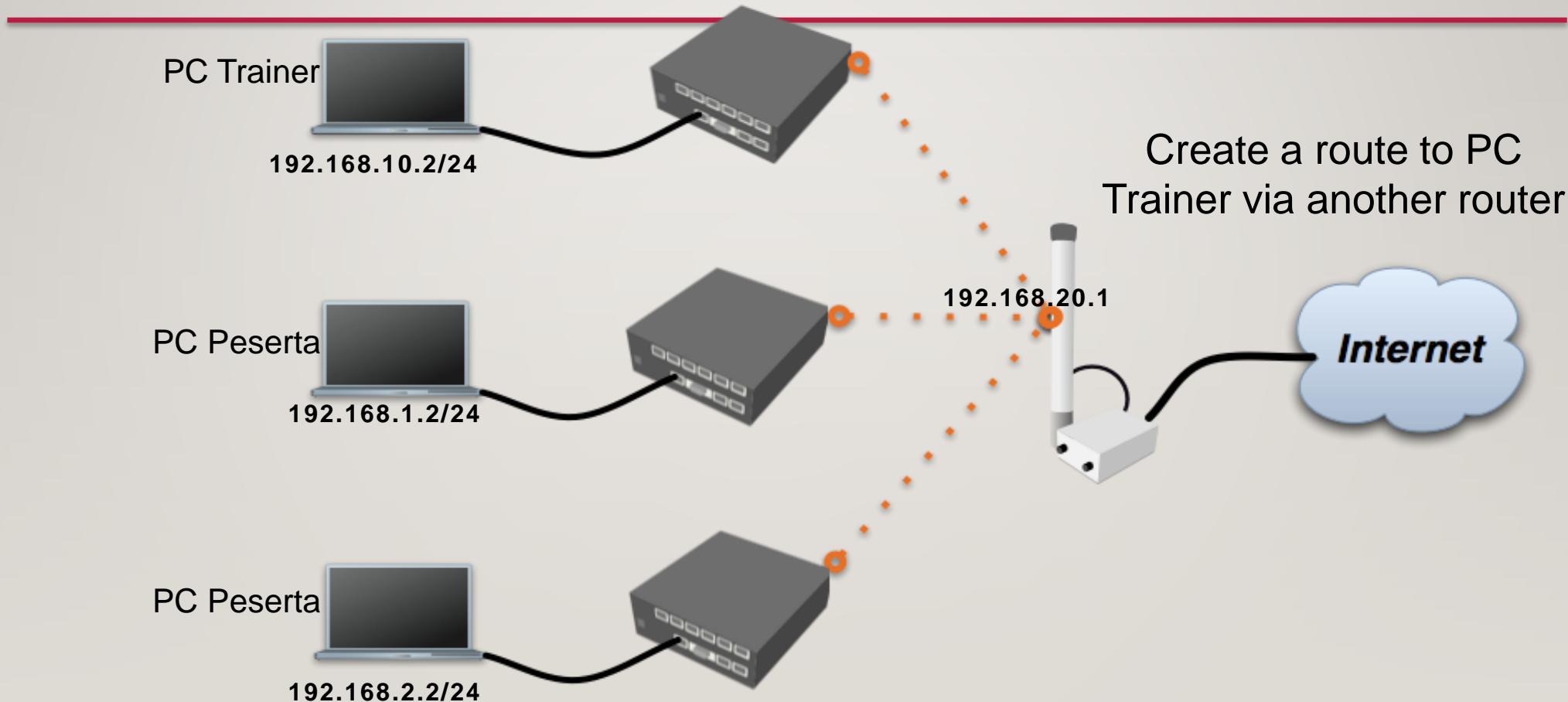
## **Static Routing**

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

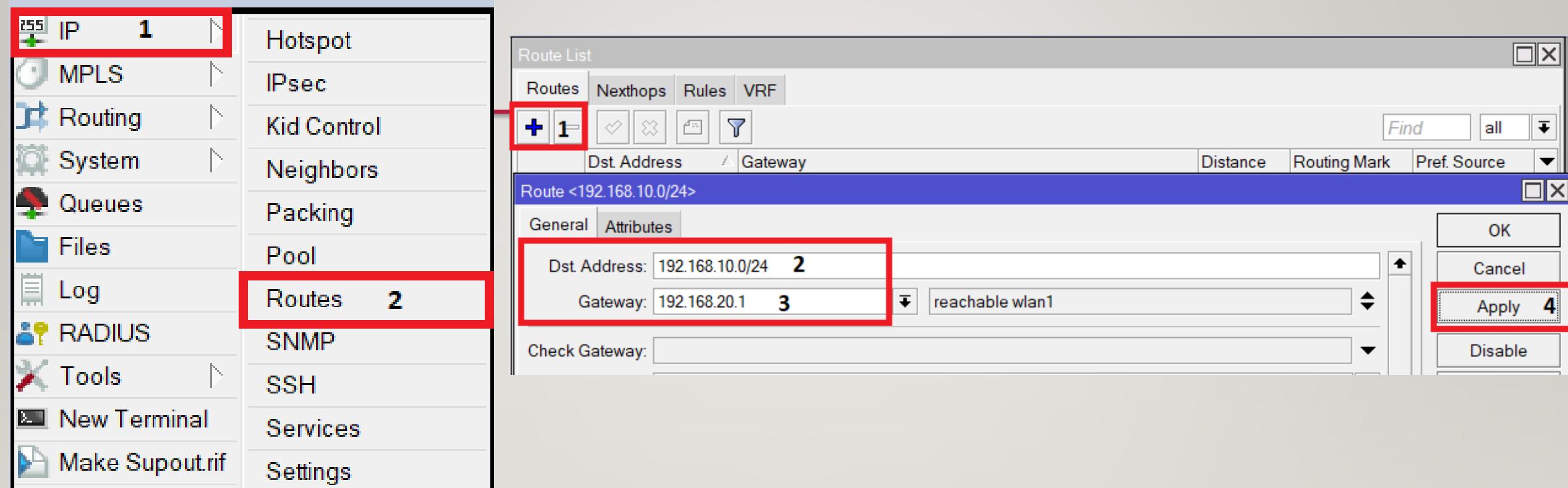
# Topology

Cobalah meroutingkan network di bawah ini.

Tambahkan route baru untuk network yang tidak langsung terhubung



# CONFIG STATIC ROUTE DI ROUTER PESERTA KE ARAH NETWORK TRAINER



# ROUTING ( Gateway & Default Gateway )

---

## Gateway & Default Gateway

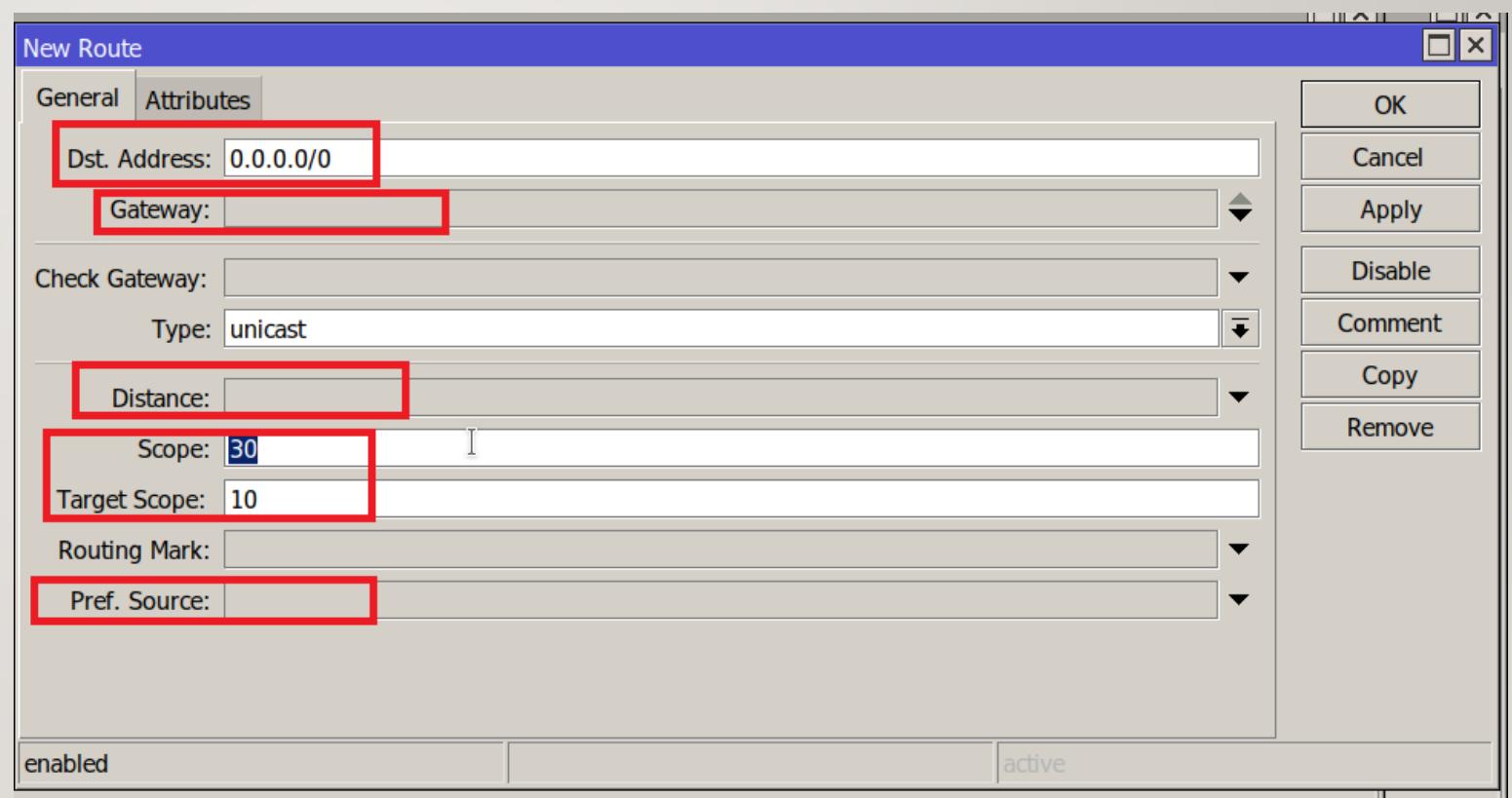
- Gateway bisa berupa IP Address atau Interface
- IP Gateway router harus satu subnet dengan salah satu IP interface router
- Hanya ada 1 gateway untuk suatu network tujuan
- Router akan memilih gateway untuk network tujuan yang lebih spesifik (netmask lebih besar)
- Default gateway adalah pengaturan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

# ROUTING

---

## Parameter

- Destination
- Gateway
- Pref Source
- Distance
- Scope & Target Scope

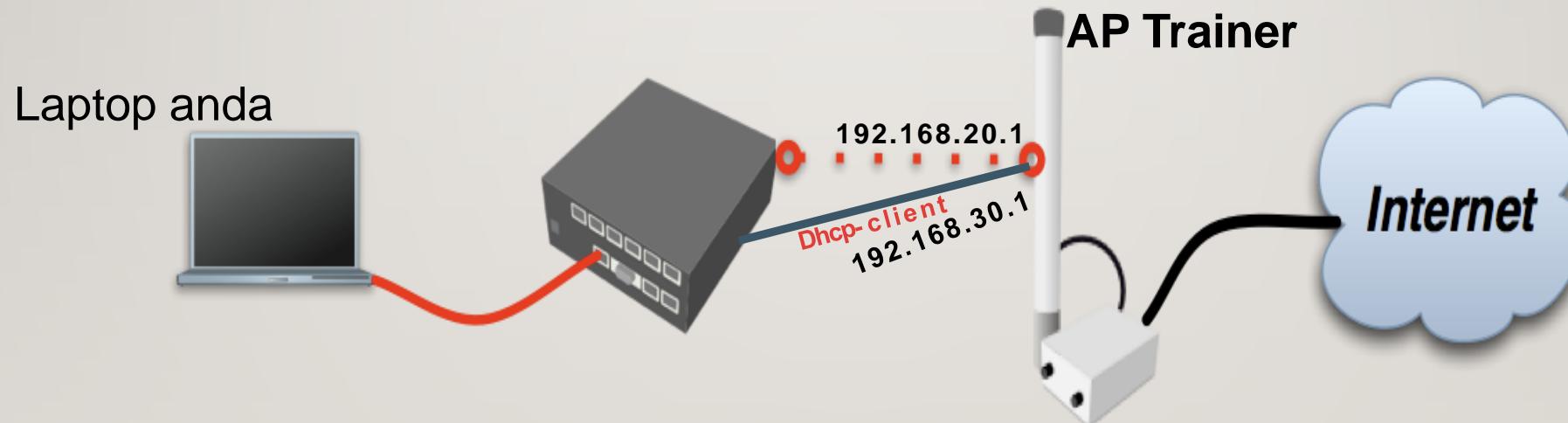


# Kesimpulan - static route

---

- Perlu ditambahkan route baru untuk network IP yang tidak terhubung langsung dengan router.
- Pastikan semua ip address yang ingin dituju, berada di route table.
- Apabila ip address tujuan (destination address) tidak ada di route table, maka data tidak akan diforwardkemanapun.
- Penulisan ip tujuan dapat diringkas dengan cukup menulis ip network dan prefixnya. Sehingga tidak perlu menulis satu-satu IP yang ingin dituju. Contoh: ip 192.168.1.1 - 192.168.1.254 bisa diringkas menjadi 192.168.1.0/24
- Dst-address 0.0.0.0/0 disebut default gateway, mewakili seluruh IP address yang ada (biasa digunakan untuk membuat route menuju ke internet).

Hubungkan RB anda ke internet melalui Wifi dan LAN yang tersedia. Sehingga memiliki 2 link ke internet (lan dan wifi )  
Tambahkan default route dan NAT di kedua link tersebut.



# Konfigurasi IP DHCP Client dan NAT di router peserta

The image shows a screenshot of the WinBox interface on a MikroTik router. It is divided into two main sections: 'DHCP Client' on the left and 'Firewall' on the right.

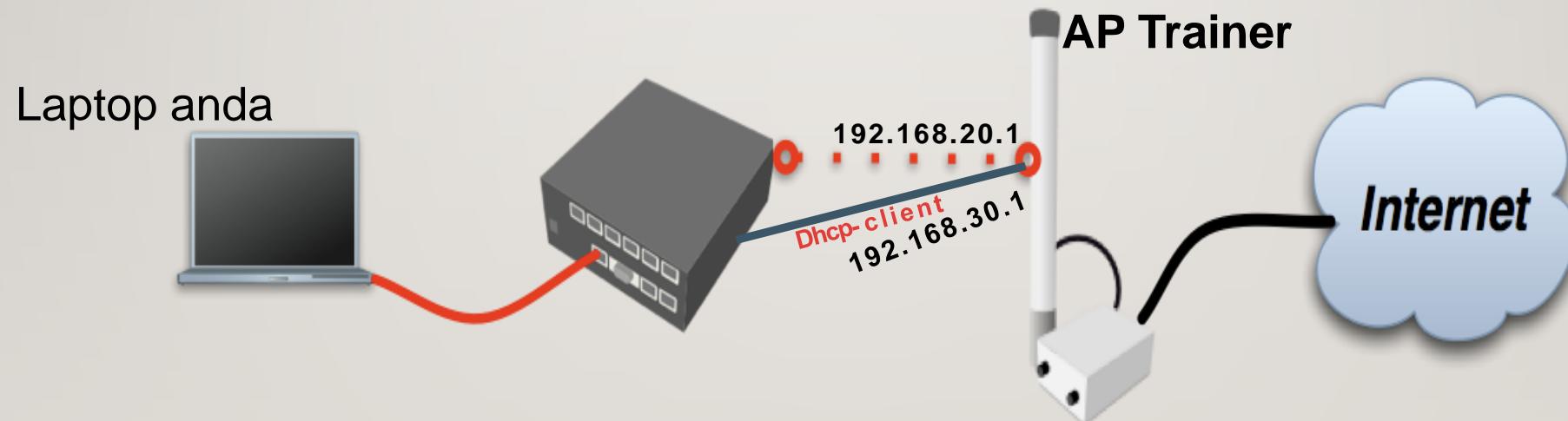
**DHCP Client Configuration (Left Side):**

- Step 1:** In the main menu, click on **IP** (1).
- Step 2:** Click on **DHCP Client** (2).
- Step 3:** Click the **+ Add** button (3+).
- Step 4:** Set the **Interface** to **ether3**. Check the boxes for **Use Peer DNS** and **Use Peer NTP**.
- Step 5:** Click **OK** (5) to save the configuration.
- Step 6:** Verify the status of the interfaces in the list. **ether3** is shown as **bound** with an IP of **192.168.30.254**, and **wlan1** is also listed as bound.

**Firewall Configuration (Right Side):**

- Step 1:** In the main menu, click on **IP** (1).
- Step 2:** Click on **Firewall** (2).
- Step 3:** Click the **NAT** tab (3).
- Step 4:** Click the **+ Add** button (4) to create a new NAT rule.
- Step 5:** Set the **Chain** to **srcnat** (4).
- Step 6:** Set the **Action** to **Masquerade** (6).
- Step 7:** Set the **Out. Interface** to **ether3** (5).
- Step 8:** Click **Apply** (7) to save the rule.

# Topology Best Route ( Distance ) Link aktif/backup



# DISTANCE ROUTE

---

## Administrative Distance

- Administrative Distance (Distance) digunakan untuk memilih jalur terbaik ketika terdapat dua atau lebih rute/routing protocol yang berbeda ke tujuan yang sama.
- Nilai dari distance adalah (0-255) dan secara default telah tersetting pada setiap protocol routing yang digunakan.
- Distance yang lebih kecil akan lebih diprioritaskan dalam pemilihan tabel routing
- Route dengan distance 255 adalah route yang direject oleh route filter

Connected routes : 0

Static Routes : 1

eBGP: 20

OSPF: 110

RIP : 120

MME : 130

iBGP: 200

**Note:**

Distance=255  
berarti “rejected”

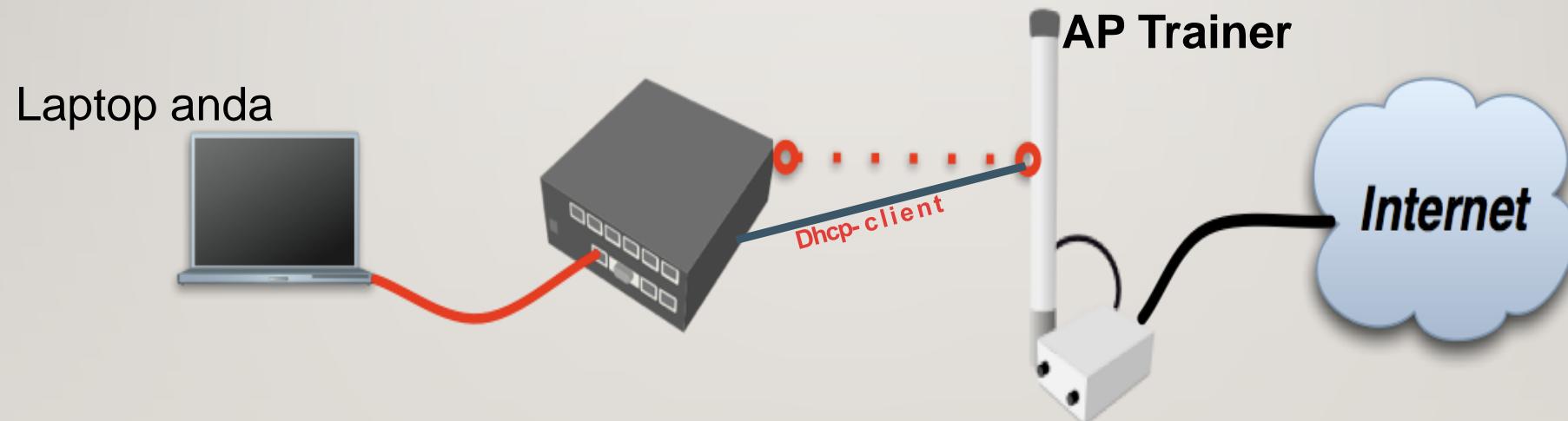
# Distance route

---

Jika ada lebih dari 1 rule route dengan dst-address yang sama, maka yang aktif hanya salah satu. Rule lain akan dijadikan sebagai backup jika route utama mati.

Dst-Address	Gateway	distance	status
0.0.0.0/0	192.168.20.1	1	AS (Active, Static)
0.0.0.0/0	192.168.30.1	2	S (Static) -> nonaktif

# Topology Best Route ( Distance ) Link aktif/backup



# GATEWAY REACHABILITY CHECK

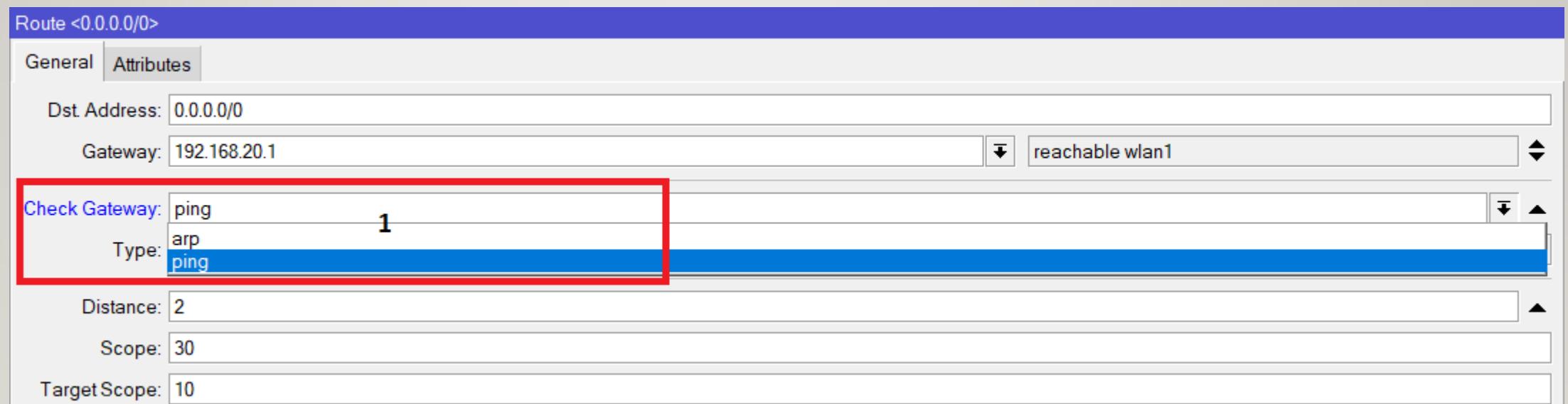
---

- Mekanisme yang digunakan untuk melakukan pengecekan kondisi gateway apakah statusnya reachable atau unreachable
- Check gateway dikirimkan setiap **10 detik** dan dapat menggunakan metode **ARP** atau **ICMP**
- **Gateway dianggap time-out** jika tidak menerima respon selama 10 detik
- Gateway dianggap **unreachable** jika terdapat 2 kali timeout
- Jika mengaktifkan fitur check gateway untuk sebuah rule, maka akan berpengaruh juga untuk semua rule dengan gateway yang sama

# GATEWAY REACHABILITY CHECK

---

Pada menu check gateway kita dapat memilih opsi menggunakan ICMP atau ARP



# Check gateway

---

Tambahkan konfigurasi chek-gateway di route utama

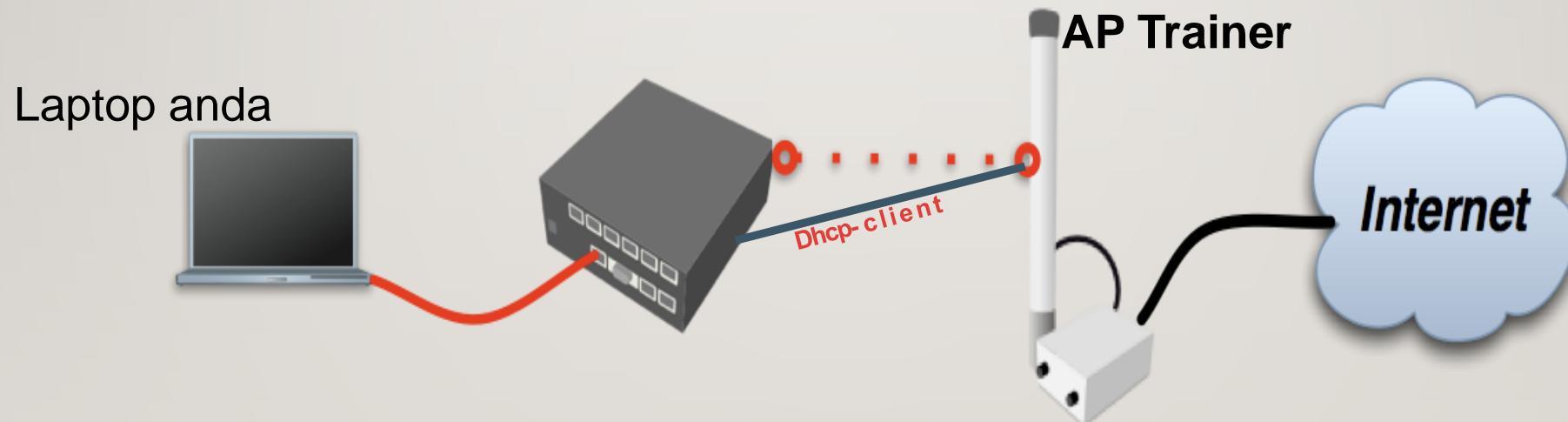
Dst-Address	Gateway	distance	Check-gateway
0.0.0.0/0	192.168.20.1	1	ping
0.0.0.0/0	192.168.30.1	2	none

Silahkan disable IP 192.168.20.1 di perangkat anda, maka route akan berpindah.

Dst-Address	Gateway	distance	status
0.0.0.0/0	192.168.20.1	1	S (Static) -> nonaktif
0.0.0.0/0	192.168.30.1	2	AS (Active, Static)

Gunakan traceroute untuk memastikan link yang dipakai oleh router.

# Topology Equal cost multi path



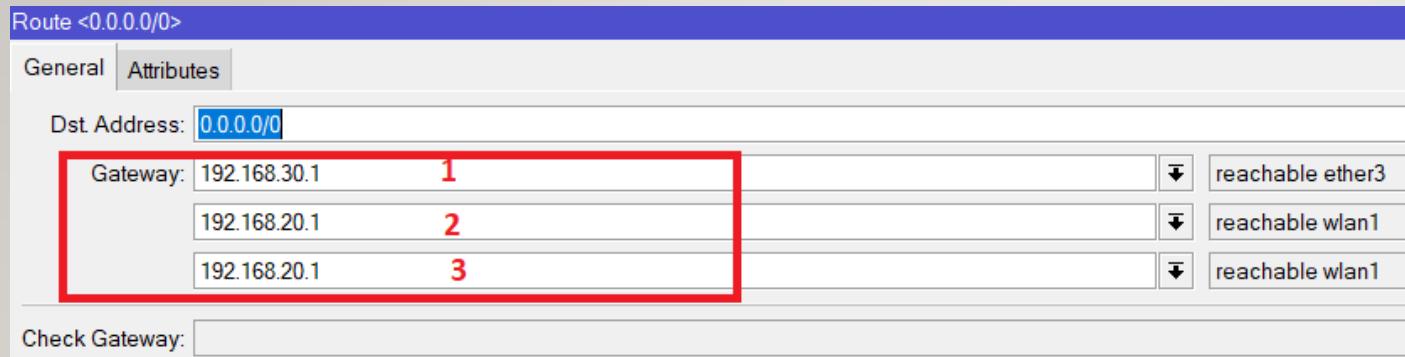
# EQUAL COST MULTI PATH (ECMP)

---

- Salah satu metode Load Balancing
- Load balancing adalah teknik untuk mendistribusikan beban kerja di dua atau lebih link jaringan.
- ECMP memungkinkan router memiliki lebih dari satu gateway untuk satu network tujuan.
- Gateway akan dipilih berdasarkan algoritma Round Robin
- Pada ECMP, pembagian traffik berdasarkan koneksi dan IP address asal dan tujuan (src-address & dst-address pair) dari koneksi tersebut.
- Sebuah Gateway dapat ditulis lebih dari sekali

# EQUAL COST MULTI PATH (ECMP)

---



Pada gambar disamping, gateway 192.168.20.1 di tulis 2 kali, ini mengindikasikan paket yang dilewatkan akan 2 kali lebih banyak ke gateway tersebut dibandingkan dengan gateway 192.168.30.1

# Ecmp–equal cost multi path

---

Lakukan pengetesan menggunakan traceroute dari laptop

```
C:\Users\e1>tracert google.com
Tracing route to google.com [172.217.27.14]
over a maximum of 30 hops:
  1      2 ms      2 ms      2 ms  ^C
```

No.	Src-address	Dst-address	Hop pertama
1	laptop	Facebook.com	192.168.20.1
2	Laptop	Google.com	192.168.20.1
3	Laptop	Detik.com	192.168.20.1
4	Laptop	kompas.com	192.168.20.1
5	Laptop	Twitter.com	192.168.20.1
6	laptop	Gpmnetwork.id	192.168.30.1

# Route type

---

- Kita bisa melakukan blok untuk dst-address tertentu menggunakan static route :

<sup>37</sup>**Blackhole**

Memblok dengan diam-diam

<sup>38</sup>**Prohibit**

Memblok dan mengirimkan pesan error ICMP “administratively prohibited” (type 3 code 13)

<sup>39</sup>**Unreachable**

Memblok dan mengirimkan pesan error ICMP “host unreachable” (type 3 code 1)

- Ketiga tipe di atas **tidak** membutuhkan IP Address gateway.

# Konfigurasi Route type

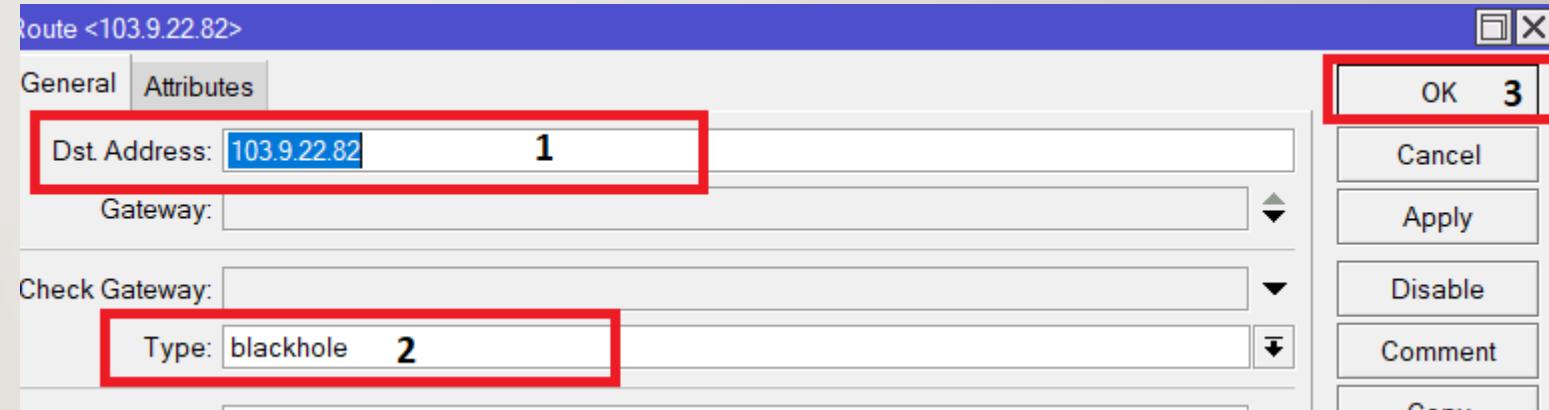
```
C:\ Command Prompt - nslookup
Microsoft Windows [Version 10.0.19043.1889]
(c) Microsoft Corporation. All rights reserved.

C:\Users\andij>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server: UnKnown
Address: 8.8.8.8

> ft.unsoed.ac.id
Server: UnKnown
Address: 8.8.8.8

Non-authoritative answer:
Name: ft.unsoed.ac.id
Address: 103.9.22.82

>
```



# POLICY ROUTING

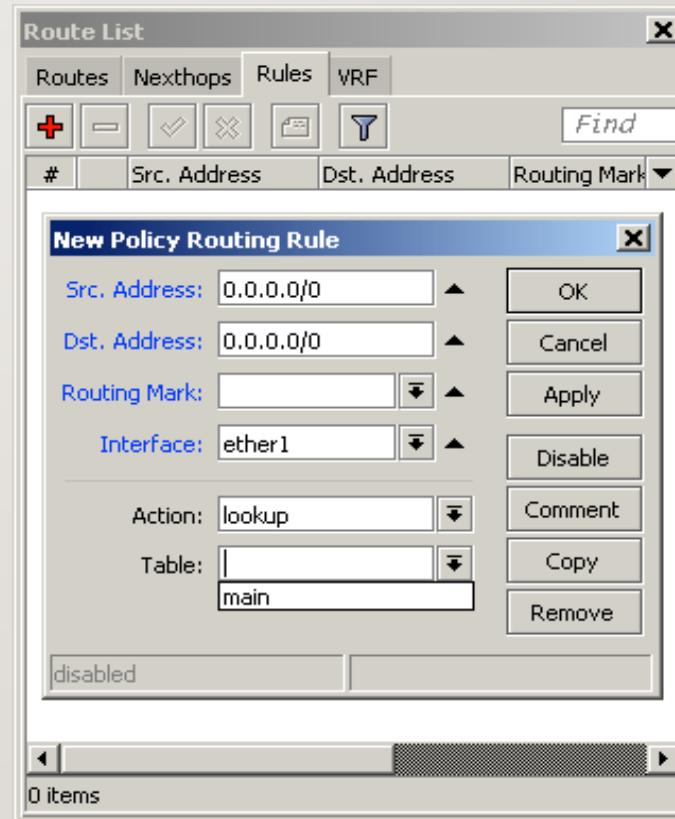
---

- By Default, semua routing akan menggunakan routing table utama
- Untuk membuat routing table tambahan dapat dilakukan dengan cara
  - > IP > Route > Rules
  - > IP > Firewall > Mangle > Route-mark

# Route rules

---

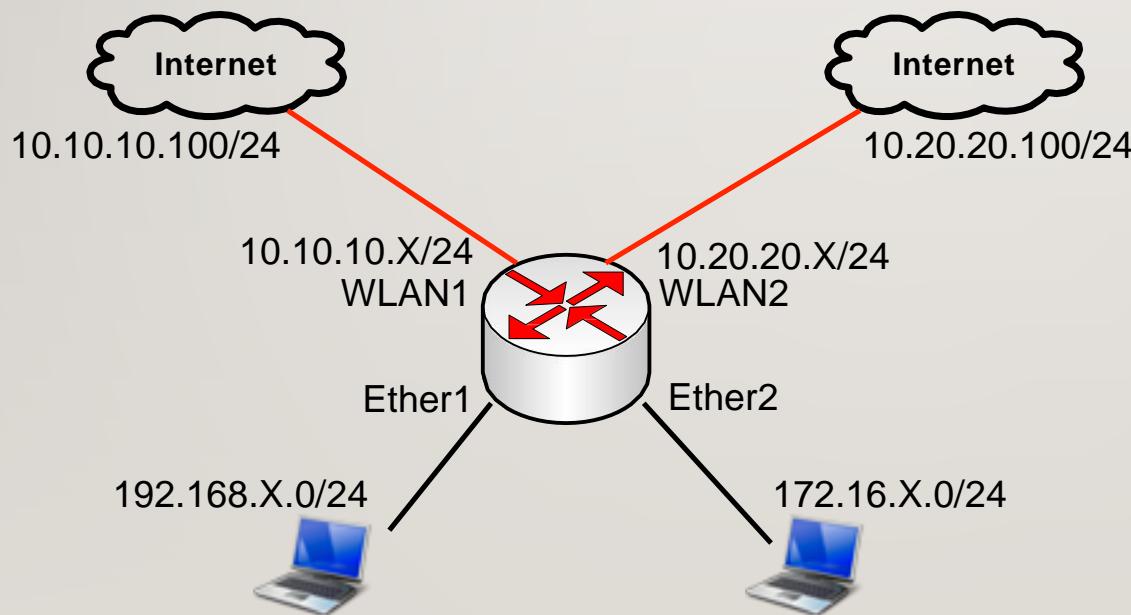
- Route rules hanya dapat melakukan filtering berdasarkan src-address, dst-address, routing-mark, dan interface.
- Untuk filtering yang lebih detail, gunakanlah mangle.



# Route mark

---

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



# ROUTING MARK

---

- Digunakan untuk mengarahkan traffic yang lebih specific ke route tertentu
- Traffic yang akan di arahkan harus diidentifikasi lebih dulu melalui routing mark (Mangle)
- Chain yang dapat di gunakan untuk routing mark adalah Pre Routing (traffic yang melalui routing chain) dan Output (traffic yang keluar dari router)
- Setiap paket hanya boleh memiliki satu routing mark
- Jika sebuah paket memiliki routing mark, maka traffic tersebut akan diabaikan oleh table routing utama

# Route 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

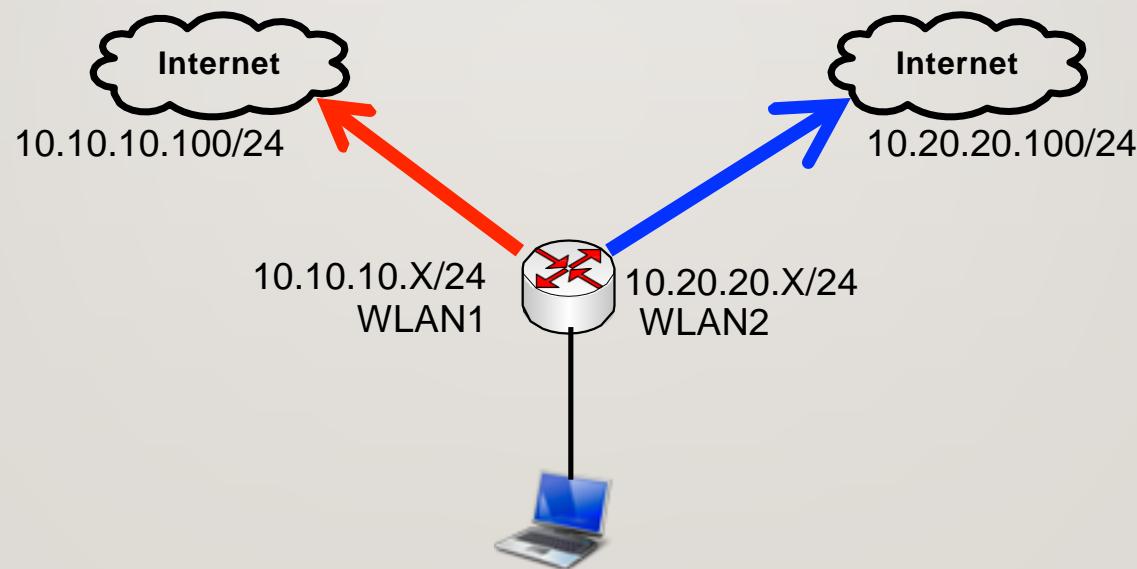
---

- 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.

# Route Mark

---

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



# Route Mark(client)

**Mangle Rule <80>**

General	Advanced	Extra	Action	Statistics
Chain: <input type="text" value="prerouting"/>				
Src. Address:				
Dst. Address:				
Protocol: <input type="checkbox"/> 6 (tcp)				
Src. Port:				
Dst. Port: <input type="checkbox"/> 80				
Any. Port:				
P2P:				
In. Interface: <input type="checkbox"/> ether1				
Out. Interface:				

**Mangle Rule <80>**

General	Advanced	Extra	Action	Statistics
Action: <input type="text" value="mark routing"/>				
New Routing Mark: <input type="text" value="route-web"/>				
<input type="checkbox"/> Passthrough				

# Route Mark(local process)

The image displays two side-by-side screenshots of a network configuration interface, likely from a Linux distribution's packet filtering tool like tc or similar.

**Screenshot 1: New Mangle Rule**

This screenshot shows the configuration of a new mangle rule. The "Chain" field is set to "output", which is highlighted with a red box. Other fields include:

- Src. Address: [empty]
- Dst. Address: [empty]
- Protocol:  6 (tcp)
- Src. Port: [empty]
- Dst. Port:  80
- Any. Port: [empty]
- P2P: [empty]
- In. Interface: [empty]
- Out. Interface:  wlan1

**Screenshot 2: Mangle Rule <80>**

This screenshot shows the configuration of an existing mangle rule with ID 80. The "Action" field is set to "mark routing", and the "New Routing Mark" field is set to "route-web", both of which are highlighted with red boxes. Other fields include:

- General
- Advanced
- Extra
- Action
- Statistics

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
Check Gateway:	reachable wlan1
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
Check Gateway:	
Type:	unicast
Distance:	
Scope:	30
Target Scope:	10
Routing Mark:	route-web
Pref. Source:	

# RECURSIVE NEXT-HOP AND SCOPE/TARGET-SCOPE USAGE

---

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

# Recursive Next Hop

---

- Secara default, gateway yang bisa digunakan di mikrotik adalah IP address router tetangga yang langsung terhubung.
- Jika sumber internet ada di R1, maka gateway untuk R2: 12.12.12.1, gateway untuk R3: 23.23.23.2, dan gateway untuk R4: 34.34.34.3
- Dengan mengubah nilai scope / target scope, maka semua router dapat menggunakan gateway R1 (12.12.12.1) sebagai default route meskipun IP Address tersebut tidak terhubung secara langsung.

# RECURSIVE NEXT-HOP AND SCOPE/TARGET-SCOPE USAGE

---

Berikut ini adalah nilai default scope dan target scope.

Agar recursive jalan, nilai target scope harus sama / lebih besar dari scope route lain yang reachable.

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

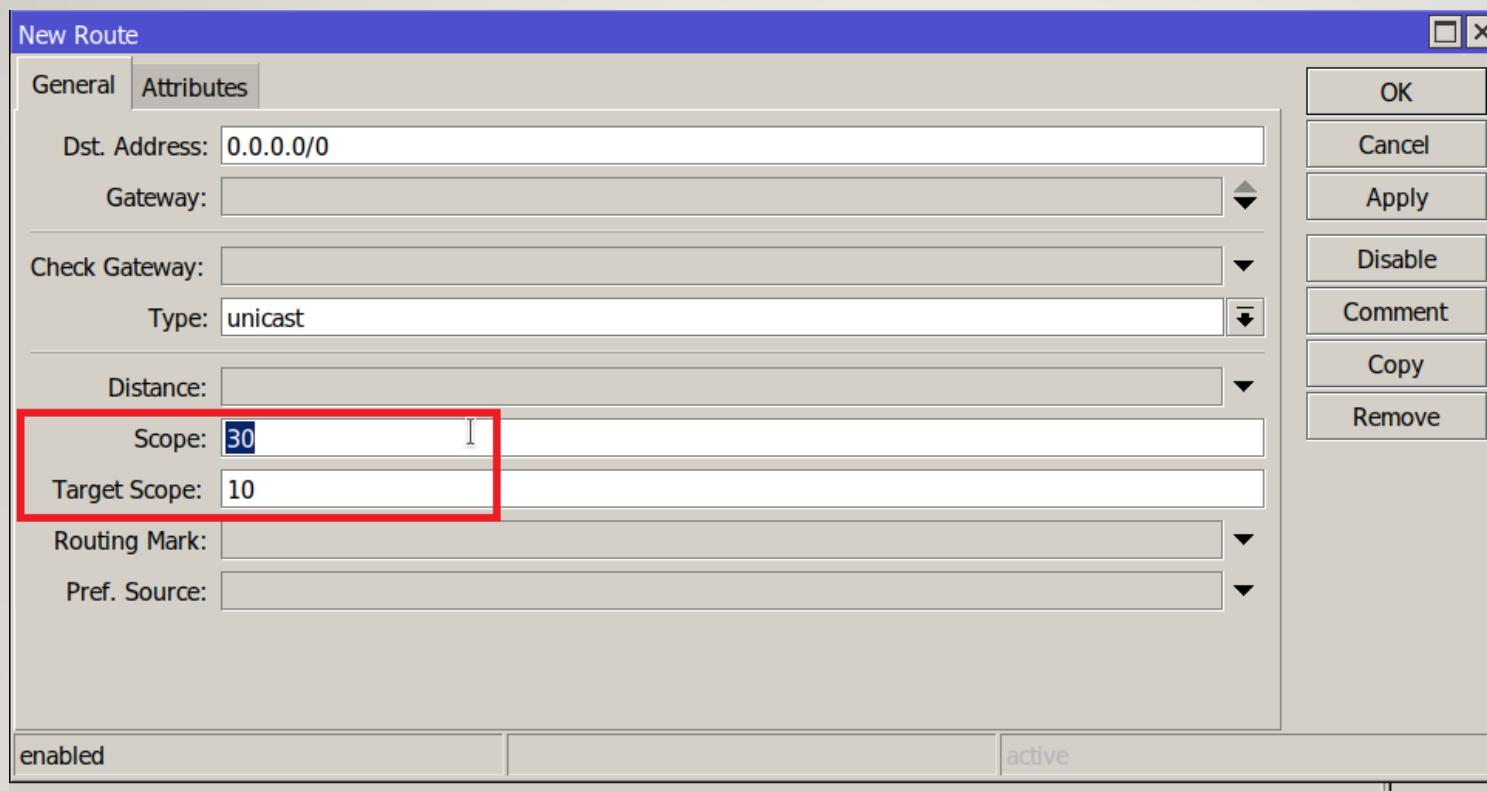
# RECURSIVE NEXT-HOP AND SCOPE/TARGET-SCOPE USAGE

---

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

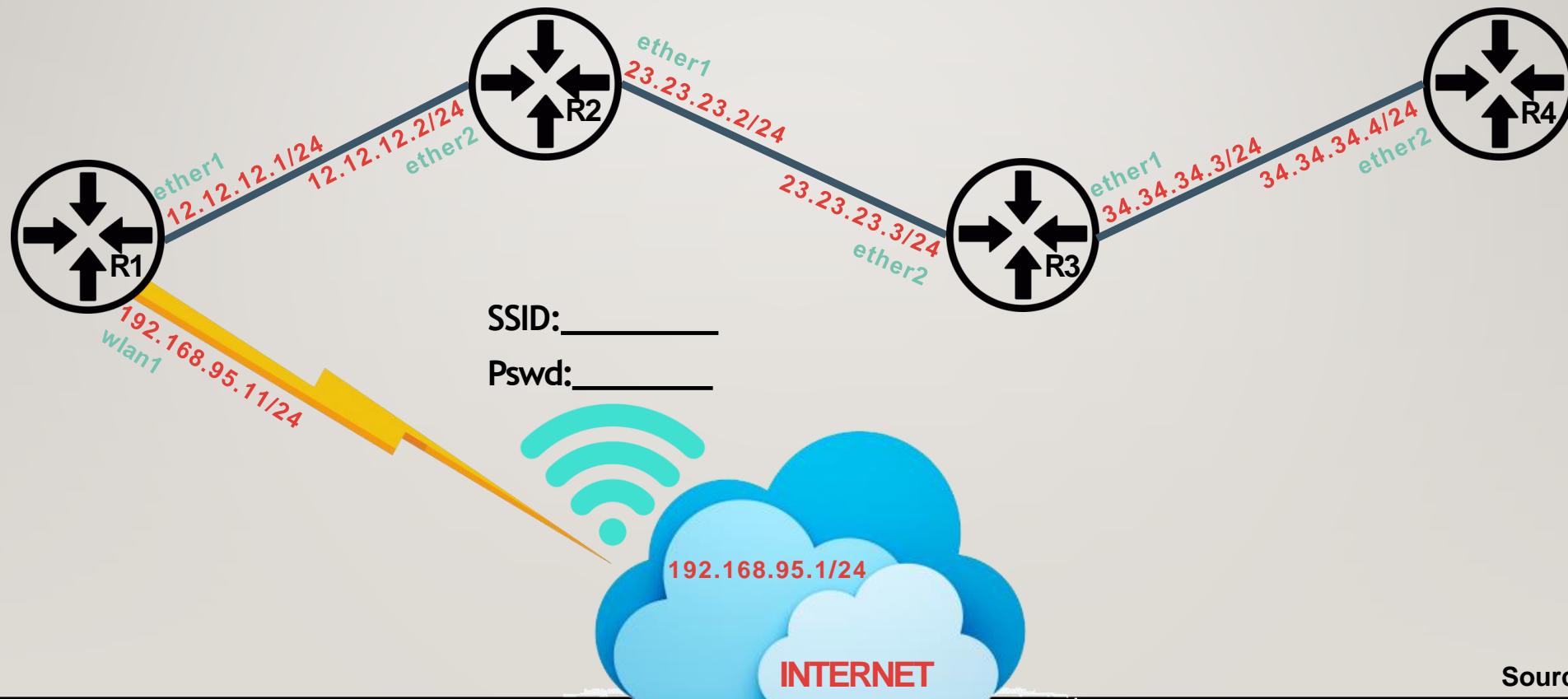
# RECURSIVE NEXT-HOP AND SCOPE/TARGET-SCOPE USAGE

---



## recursive default route di R4

Dst-Address	Gateway	Scope	Target Scope
0.0.0.0/0	12.12.12.1	30	30
12.12.12.0/24	34.34.34.3	30	10

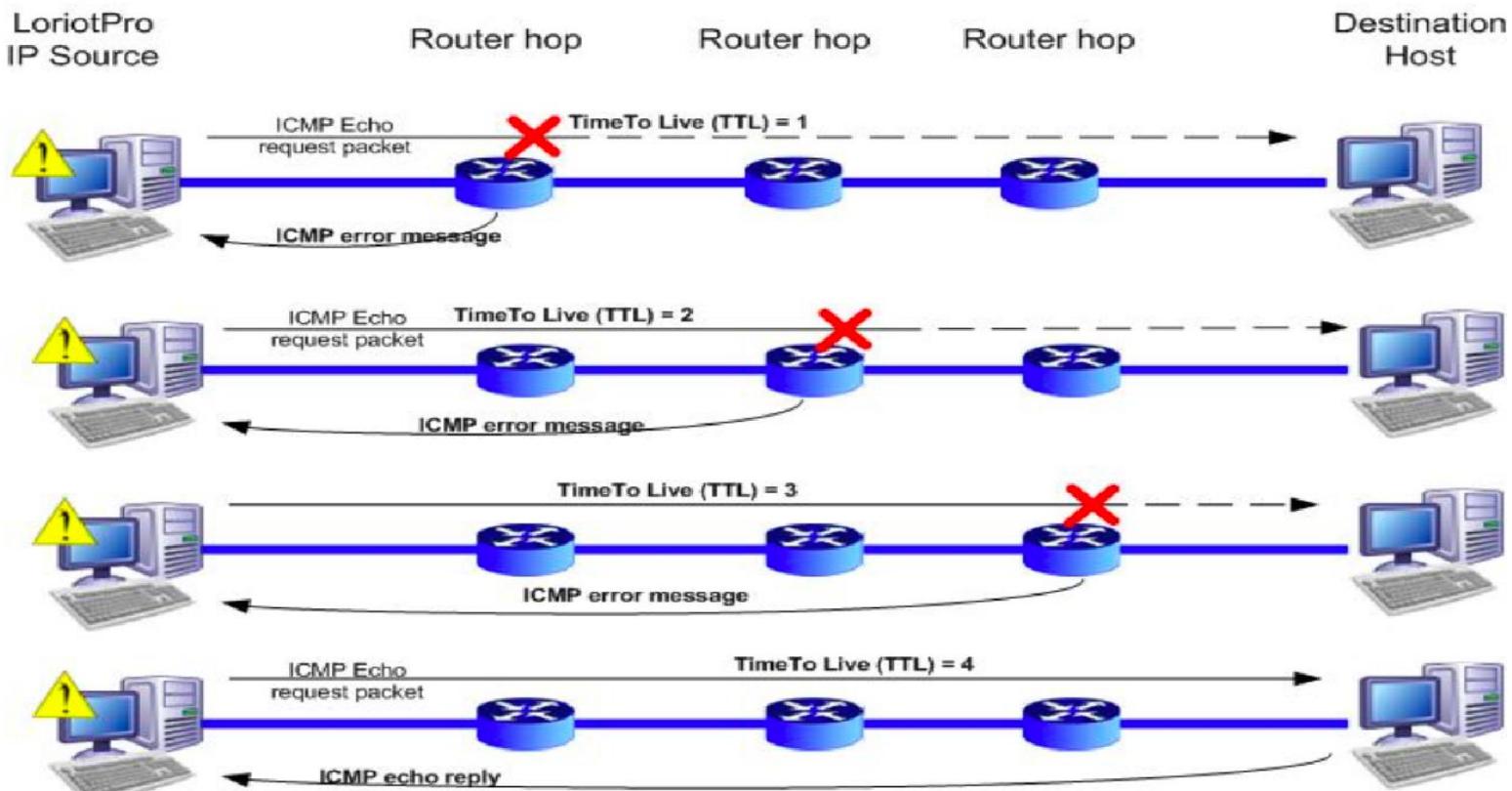


Source IDN MTCRE (idn.id)

# TTL (Time To Live)

- TTL adalah suatu nilai pada paket data (header IP) yang menyatakan berapa lama paket tersebut bisa beredar/berjalan-jalan dalam jaringan.
- Nilai TTL menentukan paket harus diteruskan ke router selanjutnya (next hop router) atau di-*discard*.
- Nilai default TTL adalah 64 maksimum 255(8bits) dan nilainya akan berkurang 1 setiap paket data melewati router (layer 3), beberapa saat sebelum *forwarded decision*.
- Router tidak akan melewatkannya ke route selanjutnya apabila TTL yang dia terima bernilai 1
- Routing loop = paket yang berputar-putar dalam jaringan loop, sampai nilai TTLnya habis

# TTL (Time To Live)



LUTEUS Copyrights 2008

Source IDN MTCRE (idn.id)

# Mikrotik Certified Routing Engineer (MTCRE)

---

## Tunnels dan VPN

# What is VPN?

---

- VPN merupakan sebuah metode untuk membangun jaringan yang menghubungkan antar node jaringan secara aman / terenkripsi dengan memanfaatkan jaringan publik (Internet / WAN).
  - VPN adalah sebuah cara aman untuk mengakses local area network dengan menggunakan internet atau jaringan publik.
  - Tunnel adalah kunci penting dari VPN
- 
- Mikrotik support beberapa metode VPN seperti PPTP, L2TP, SSTP, dan OpenVPN

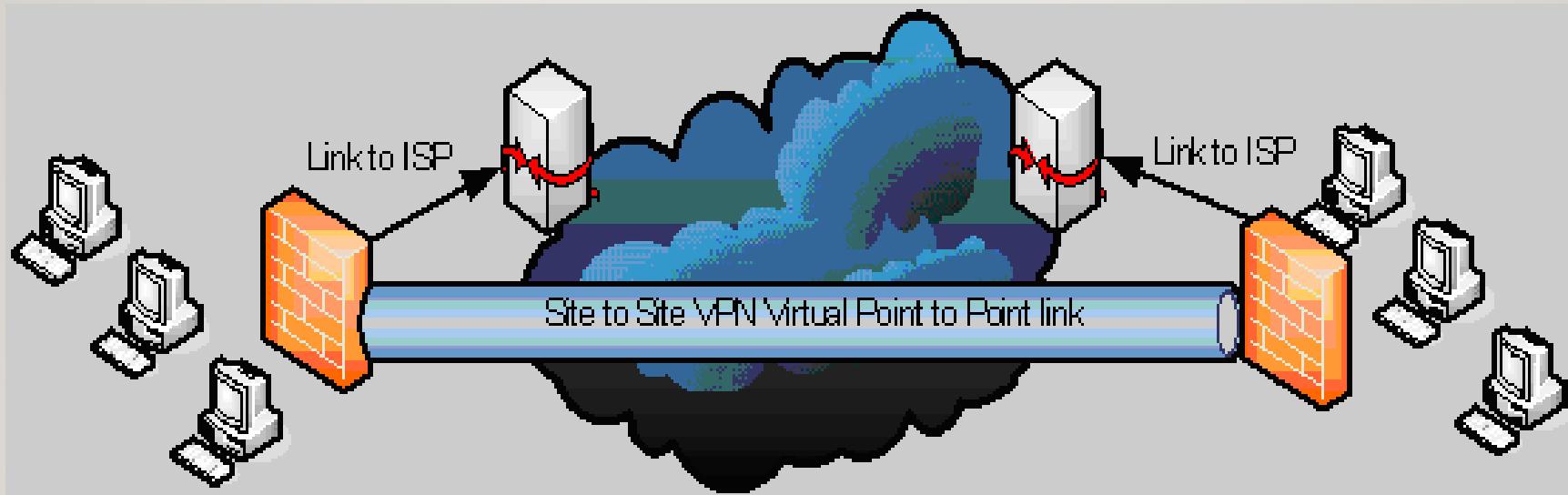
# Tunnel

---

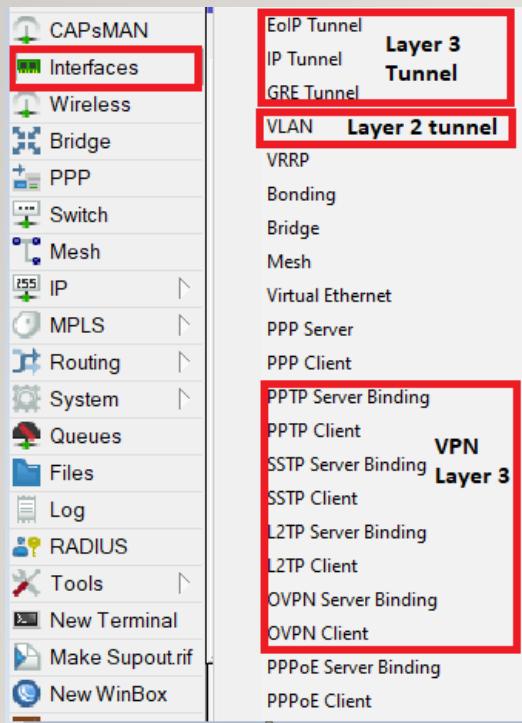
- Tunnel adalah sebuah metode penyelubungan (encapsulation) paket data di jaringan
- Sebelum dikirim, paket data mengalami sedikit pengubahan atau modifikasi, yaitu penambahan header dari tunnel
- Ketika data sudah melewati tunnel dan sampai di tujuan (ujung) tunnel, maka header dari paket data akan dikembalikan seperti semula (header tunnel dilepas).
- Mikrotik support beberapa metode Tunnel seperti EOIP, IPIP, IPSec, dan PPPOe

# Tunnel dan Virtual Private Network

---



# Tunnel dan VPN di Mikrotik



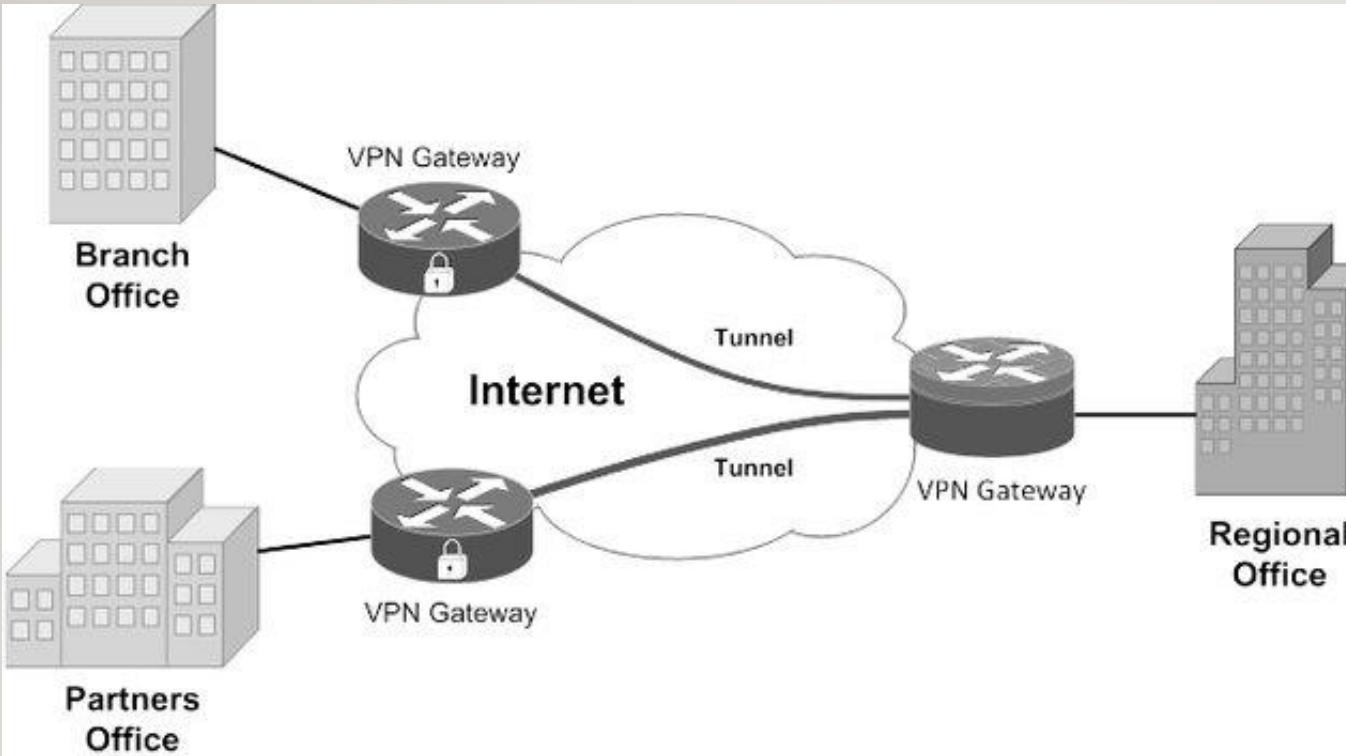
Compare VPN types (RouterOS)

	L2TP	L2TP/IPSEC + psk	OpenVPN	PPTP	SSTP	IPSec IKE2
Protocol	UDP	UDP over UDP/ESP	TCP	GRE	TCP	UDP, ESP
Performance	Fast	Medium	Slow	Fast	Slow	<b>Very fast</b>
Connection establishment	Medium	Slow	Slow	Medium	Medium	<b>Very fast</b>
Requires strong CPU for encryption	No	Yes	Yes	No	Yes	Yes
Multicore CPU load balance	Yes	Yes	No	Yes	Yes	Yes
Security	Low	Strong	Strong	Low	Strong	<b>Very strong</b>
Push routes	No	No	Yes	No	No	Yes
Bypass NAT	Yes	Yes	Yes	Yes	Yes	Yes
Has interface	Yes	Yes	Yes	Yes	Yes	No
OS popularity	High	Very high	High	Very high	Low	High

Nikita Tarikin / nikita@tarikin.com

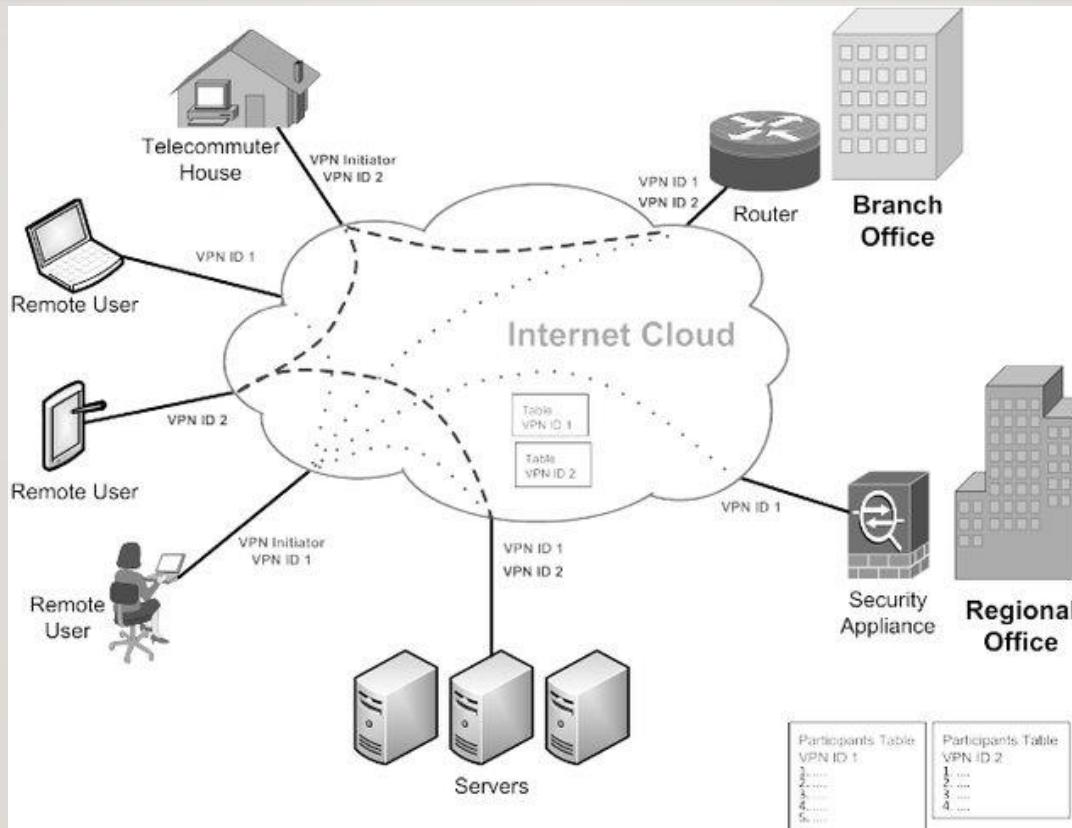
# Site-to-Site VPN/Tunnel

---



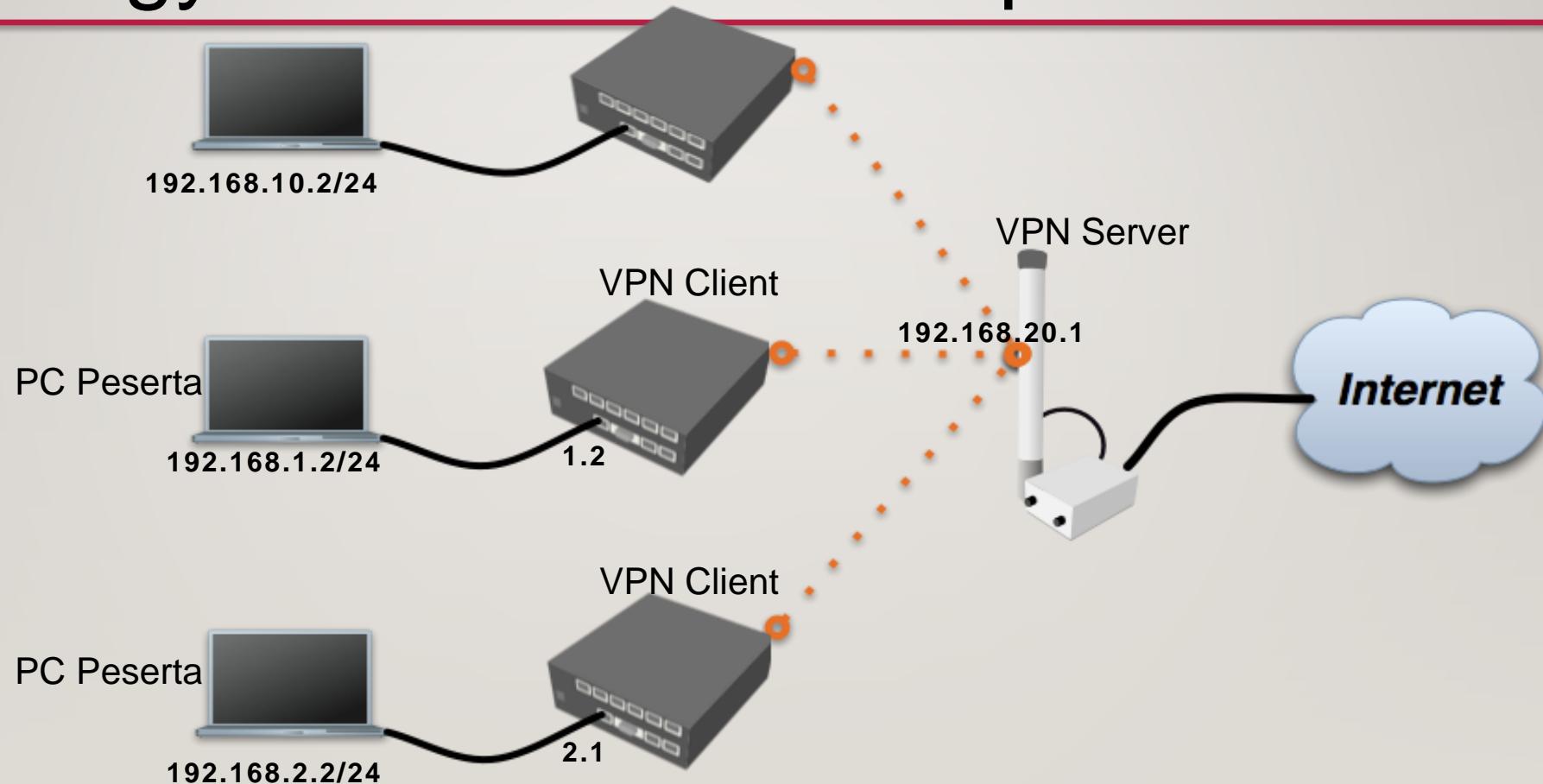
Source Zornitsa Yakova

# A new VPN access model



Source Zornitsa Yakova

# Topology VPN Server dan Vpn Client



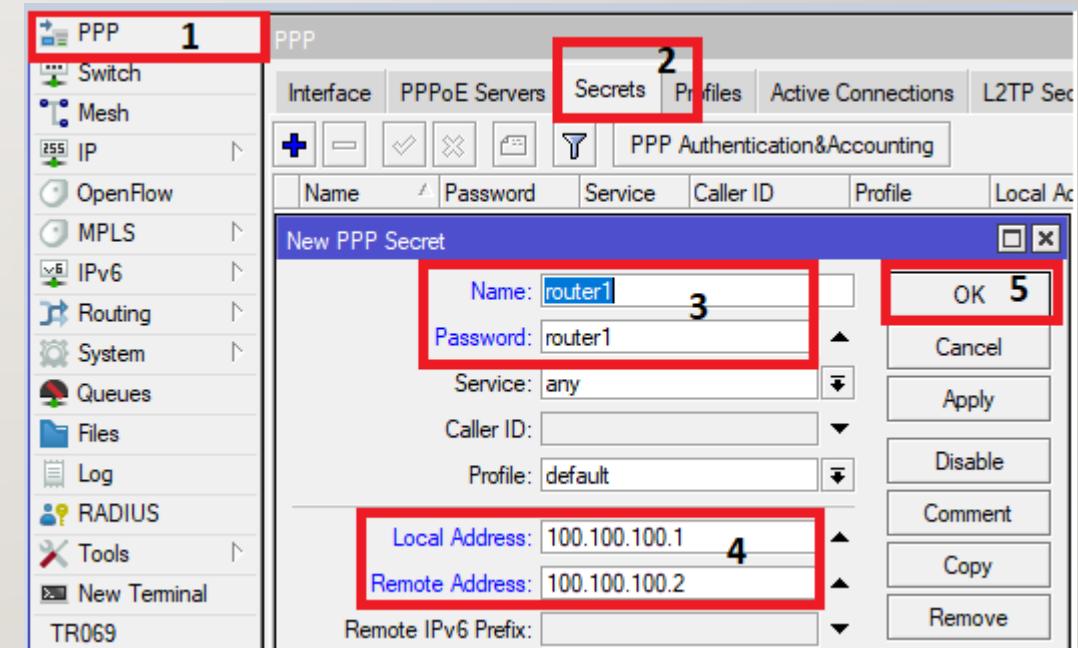
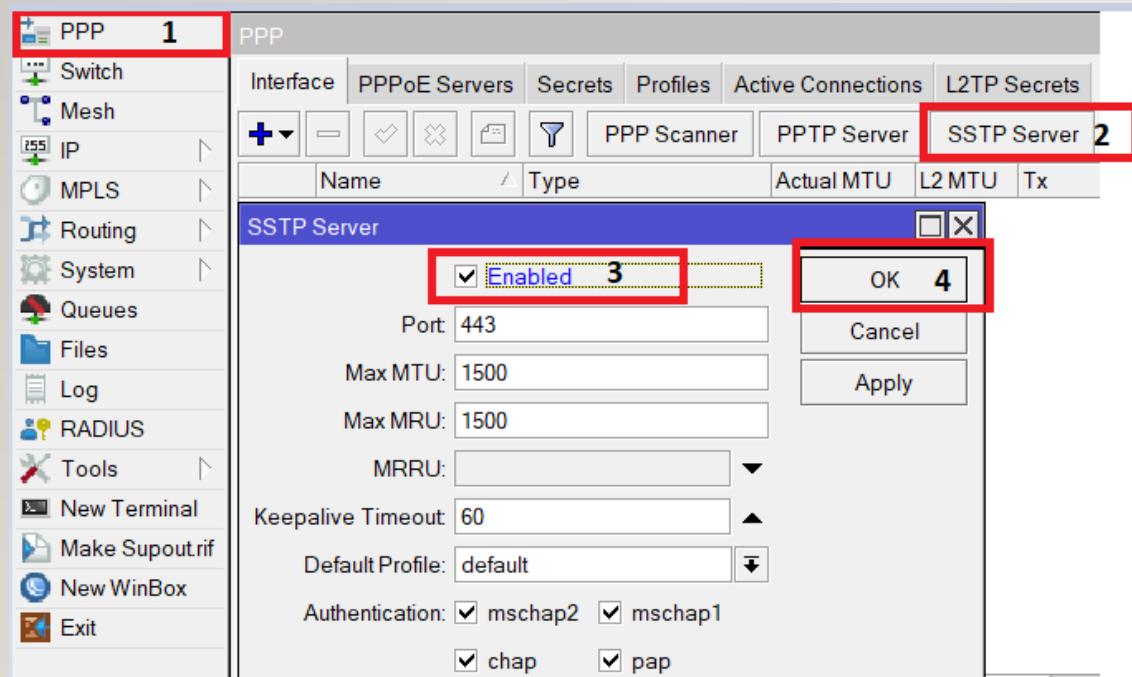
# SSTP

- Secure Socket Tunneling Protocol (SSTP) menggunakan enkripsi tunnel over IP
- port tcp/443
- SSTP client pada OS windows berada di vista SP1 keatas
- RouterOS dapat menjalankan secara bersama antara SSTP client dan server. Since RouterOS 5.0

# LAB

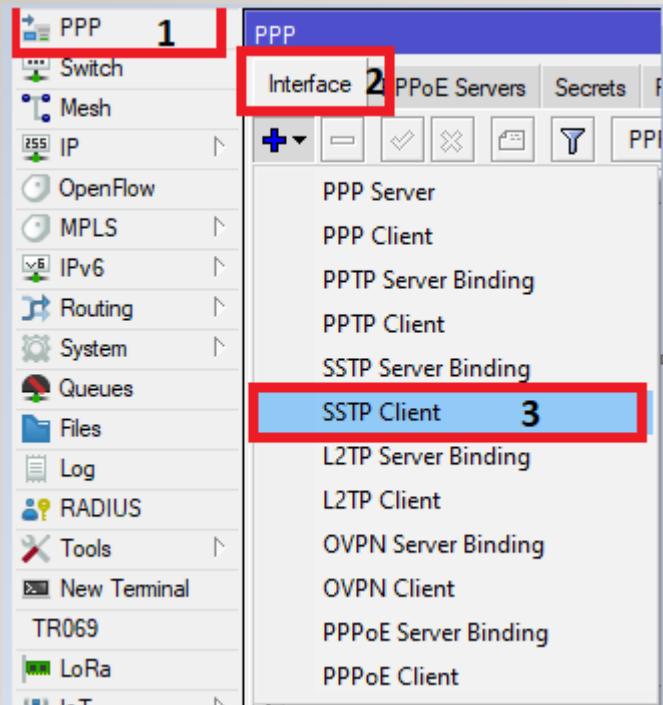
# SSTP Server

## Mengaktifkan SSTP Server pada mikrotik



# LAB

# SSTP Client



**Set name,  
PPTP server  
IP address,  
username,  
password**

The image displays two overlapping windows titled "New Interface". Both windows have tabs for General, Dial Out, Status, and Traffic. The left window's General tab shows fields for Name (set to "VPN Client Router 1" and labeled 1), Type (set to "SSTP Client"), Actual MTU, Max MTU (set to 1500), and MRRU. The right window's General tab shows fields for Connect To (set to "192.168.20.1" and labeled 2), Port (set to 443), Proxy, Proxy Port (set to 443), Certificate (set to "none"), TLS Version (set to "any"), and checkboxes for Verify Server Certificate (unchecked), Verify Server Address From Certificate (checked), and PFS. The right window also shows fields for User (set to "router1" and labeled 3) and Password (set to "router1"). Both windows have standard buttons on the right: OK (labeled 4), Cancel, Apply, Disable, Comment, Copy, Remove, and Torch.

PPP → New PPTP Client(+)

# Sinkronisasi VPN SSTP dari router VPN Client

PPP					
Interface		PPPoE Servers	Secrets	Profiles	Active Connections
+		-	▽	×	File
Name	Type	Actual MTU	L2 MTU	Tx	Rx
R	VPN akses router 1	SSTP Client	1500	0 bps	

Interface <VPN akses router 1>

General Dial Out Status Traffic

Last Link Down Time:

Last Link Up Time: Aug/17/2022 02:55:33

Link Downs: 0

Uptime: 00:02:17

Encoding: AES256-CBC

MTU: 1500

MRU: 1500

Local Address: 100.100.100.2

Remote Address: 100.100.100.1

OK Cancel Apply Disable Comment Copy Remove Torch

# **POINT TO POINT TUNNELING PROTOCOL (PPTP)**

---

- PPTP adalah tunnel yang secure untuk mengirimkan traffic IP menggunakan PPP
- PPTP menggunakan enkripsi MPPE 128 stateless
- PPTP berjalan dengan protocol TCP port 1723 dan menggunakan GRE tunnel dengan port 47
- Mikrotik dapat menjalankan peran sebagai PPTP Server dan PPTP Client

# LAYER 2 TUNNELING PROTOCOL (L2TP)

---

- Layer 2 Tunneling Protocol (L2TP) adalah jenis tunneling & encapsulation lain untuk protocol PPP.
- L2TP support non-TCP/IP protocols (Frame Relay, ATM and SONET).
- L2TP dikembangkan atas kerja sama antara Cisco dan Microsoft untuk menggabungkan fitur dari PPTP dengan protocol proprietary Cisco yaitu protokol Layer 2 Forwarding(L2F).
- L2TP tidak melakukan enkripsi paket, untuk enkripsi biasanya L2TP dikombinasikan dengan IPsec.
- L2TP menggunakan UDP port 1701.

# POINT TO POINT PROTOCOL OVER ETHERNET (PPPOE)

---

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

# Point-to-Point Protocol

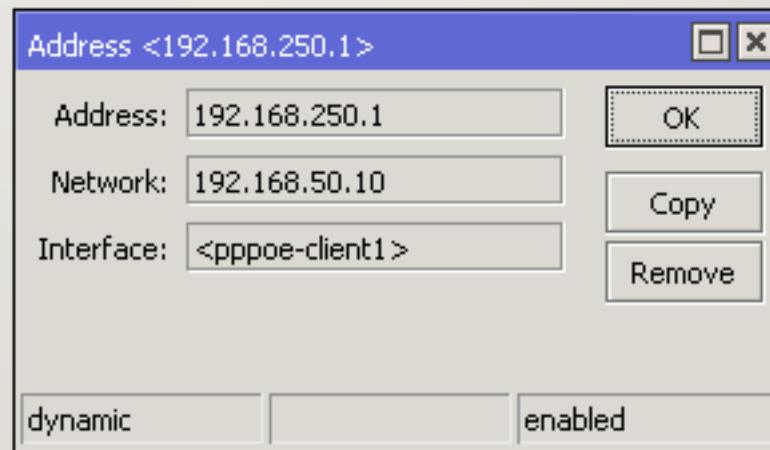
---

- Point to Point Protocol atau PPP biasanya digunakan untuk tunelling (direct connection)
- PPP dapat menggunakan authentication,enkripsi dan kompresi
- Mikrotik RouterOS support PPP tunell contohnya PPPoE, SSTP, PPTP, L2TP dan lainnya

# Point-to-Point Addressing

---

- Apabila koneksi di create diantara PPP client dan server, /32 address yang akan di masukan
- Untuk client network address (gateway) adalah ujung tunnel (router)



# Point-to-Point Addressing

---

- Subnet tidak akan ada hubungannya ketika menggunakan PPP addressing
- PPP addressing menggunakan 2 IP address
- jika PPP addressing tidak support menggunakan device lain, /30 network addressing harus digunakan

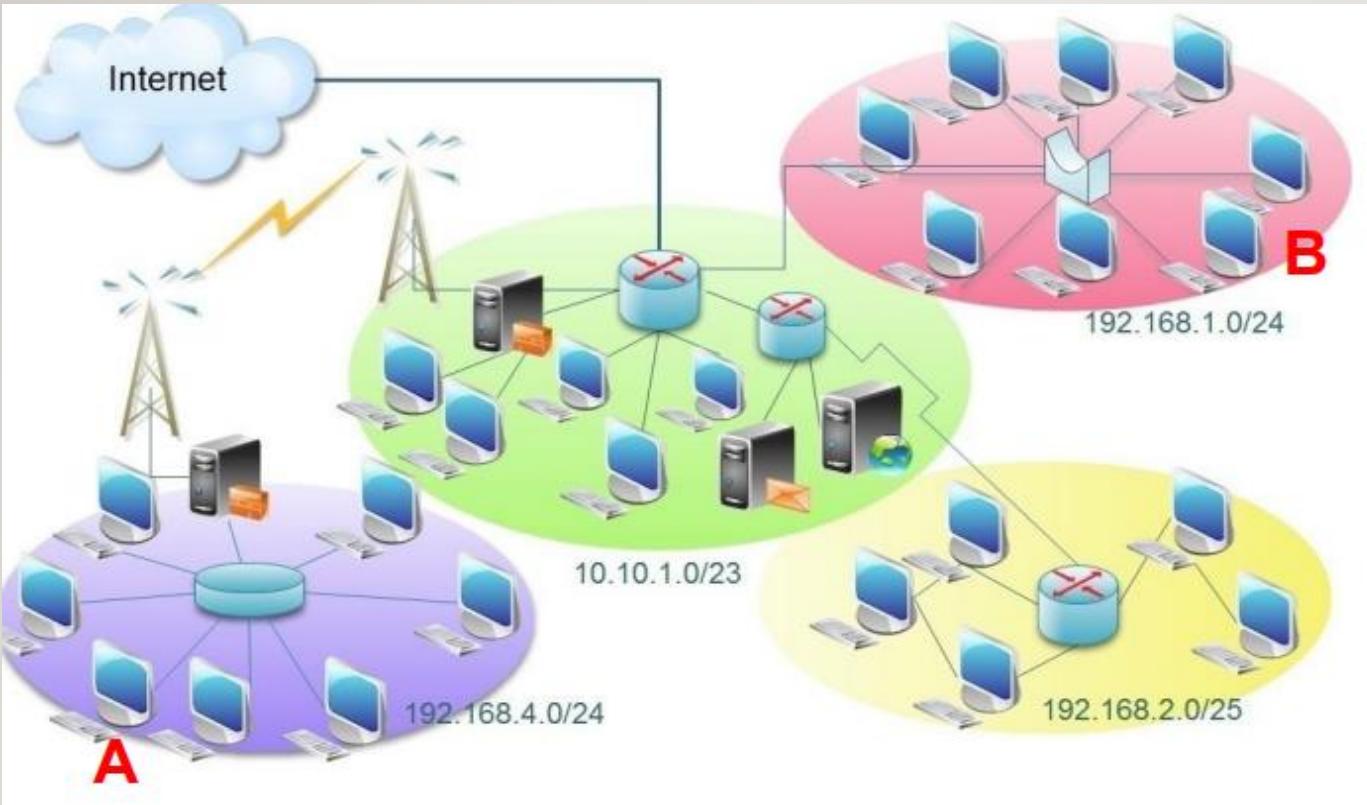
# Mikrotik Certified Routing Engineer (MTCRE)

---

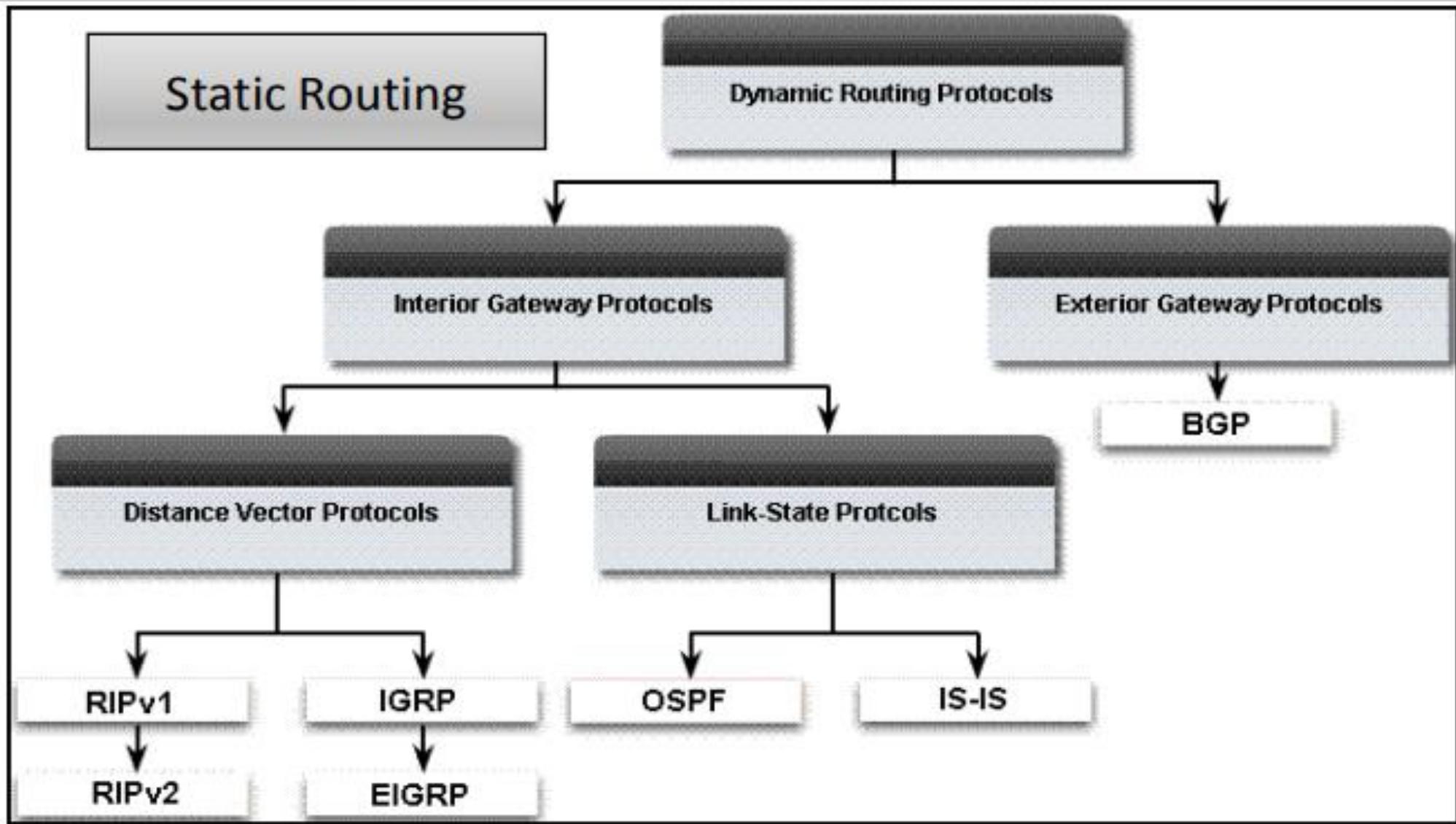
## OSPF

# ROUTING

---

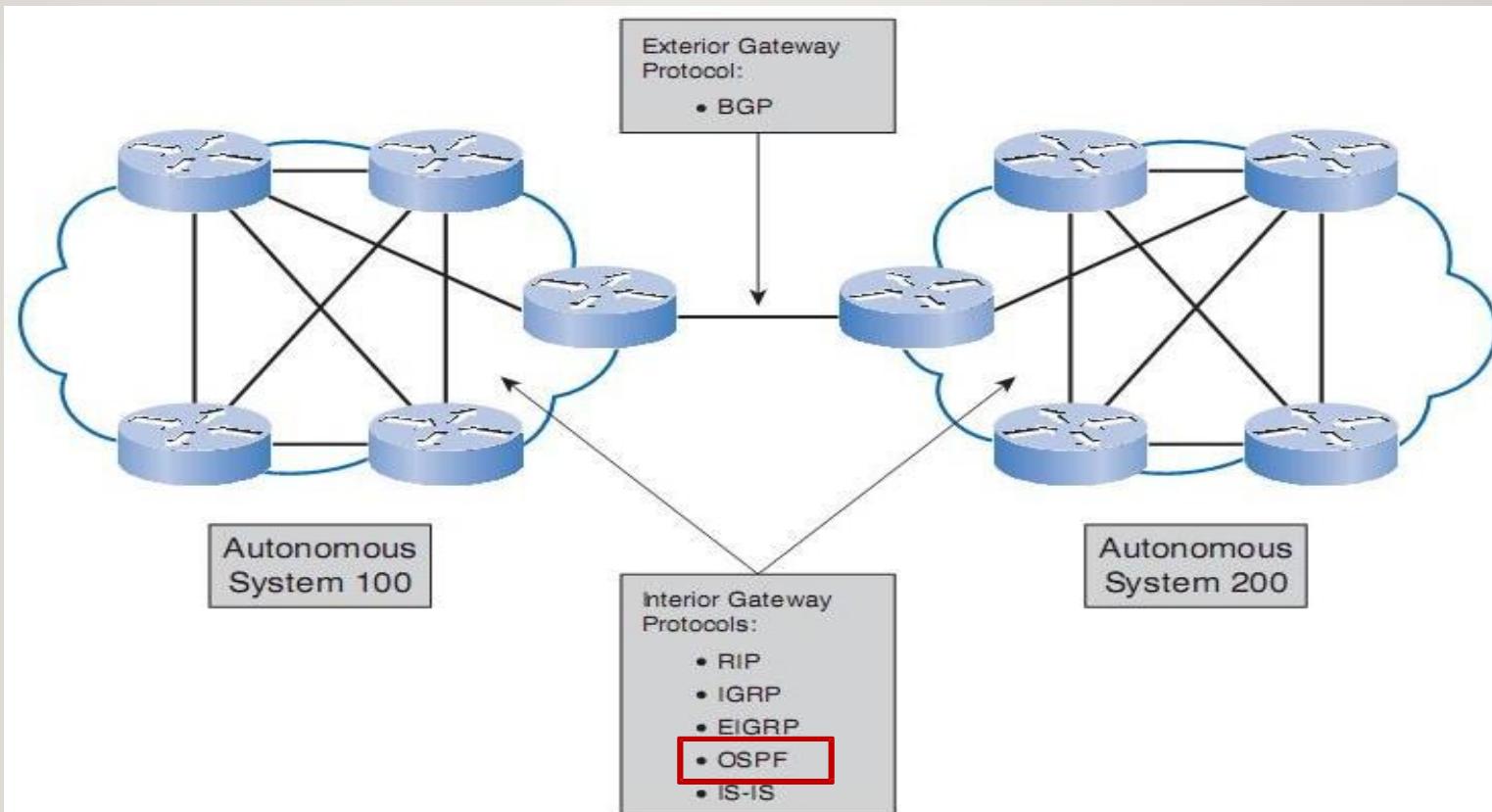


# ROUTING ( KLASIFIKASI ROUTING )



# IGP & EGP

---



# IGP & EGP

---

Berdasarkan jenisnya dynamic routing dibedakan menjadi 2 yaitu:

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

# Autonomous System (AS)

---

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

# WHAT IS OSPF?

---

- Open Shortest Path First (OSPF) adalah dynamic routing protocol yang termasuk dalam kategori IGP (Interior Gateway Protocol)
- OSPF memiliki kemampuan Link-state (melakukan deteksi status link) dan algoritma Dijkstra (algoritma pencarian jarak terpendek)
- OSPF mampu menjaga, mengatur dan mendistribusikan informasi routing antar network walaupun topologi network tersebut berubah-ubah secara dinamis.
- Menggunakan IP protocol (layer3) nomor 89
- OSPF protocol adalah protocol link-state yang menghandle pemetaan jalur routing pada struktur jaringan yang bersifat dinamis
- OSPF dapat memetakan beberapa jalur yang berbeda ke setiap networknya

# CARA KERJA OSPF

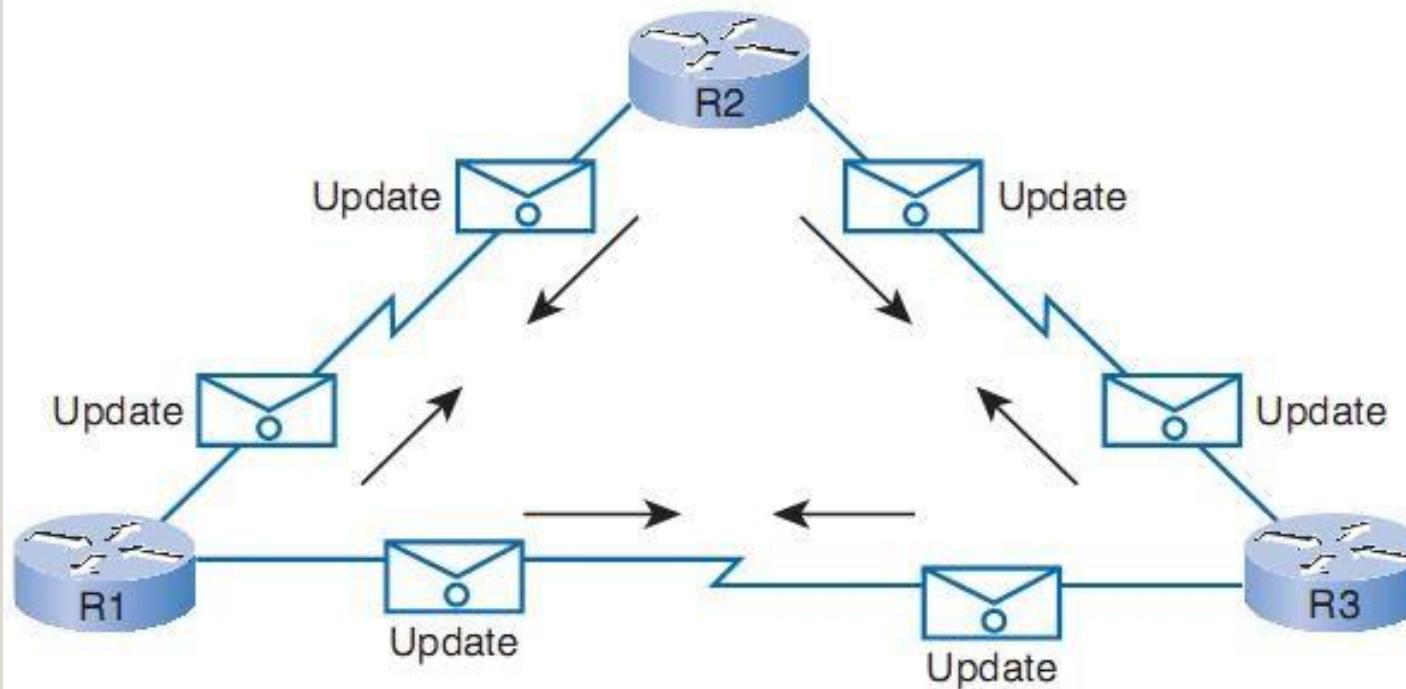
---

1. Membentuk Adjacency
2. Pemilihan DR dan BDR
3. Mengumpulkan state dalam jaringan
4. Memilih Route terbaik yang akan di gunakan
5. Menjaga informasi routing agar tetap up to date

# Routing Distribution

---

Routers Dynamically Pass Updates

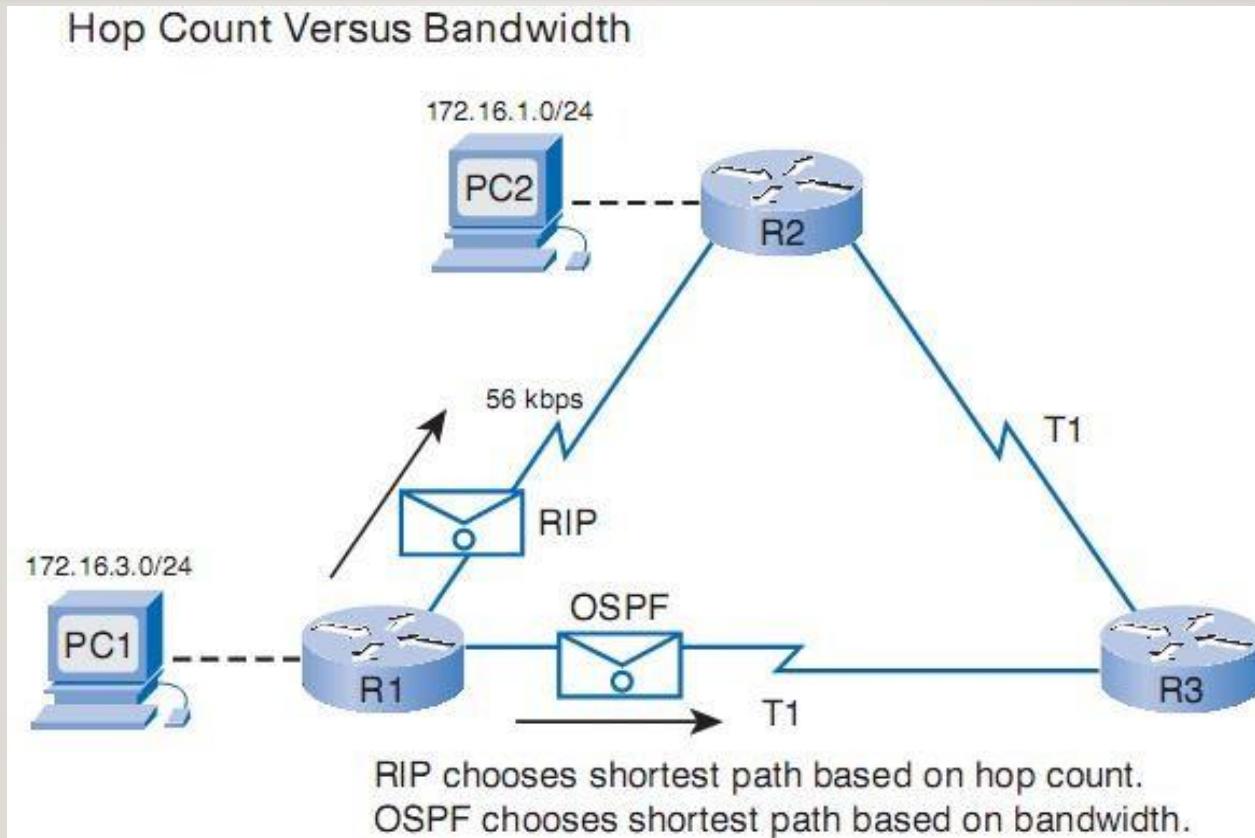


# METRIC

---

- ~ Metric adalah parameter yang digunakan dalam pemetaan jaringan
- ~ Metric digunakan untuk menentukan apakah rute tersebut lebih baik dari yang lainnya.
- ~ Metric dapat berupa :
  - measuring link utilization (using SNMP)
  - number of hops (hop count)
  - speed of the path
  - packet loss (router congestion/conditions)
  - latency (delay)
  - path reliability
  - path bandwidth
  - throughput [SNMP - query routers]
  - load
  - MTU

# OSPF VS RIP Metric

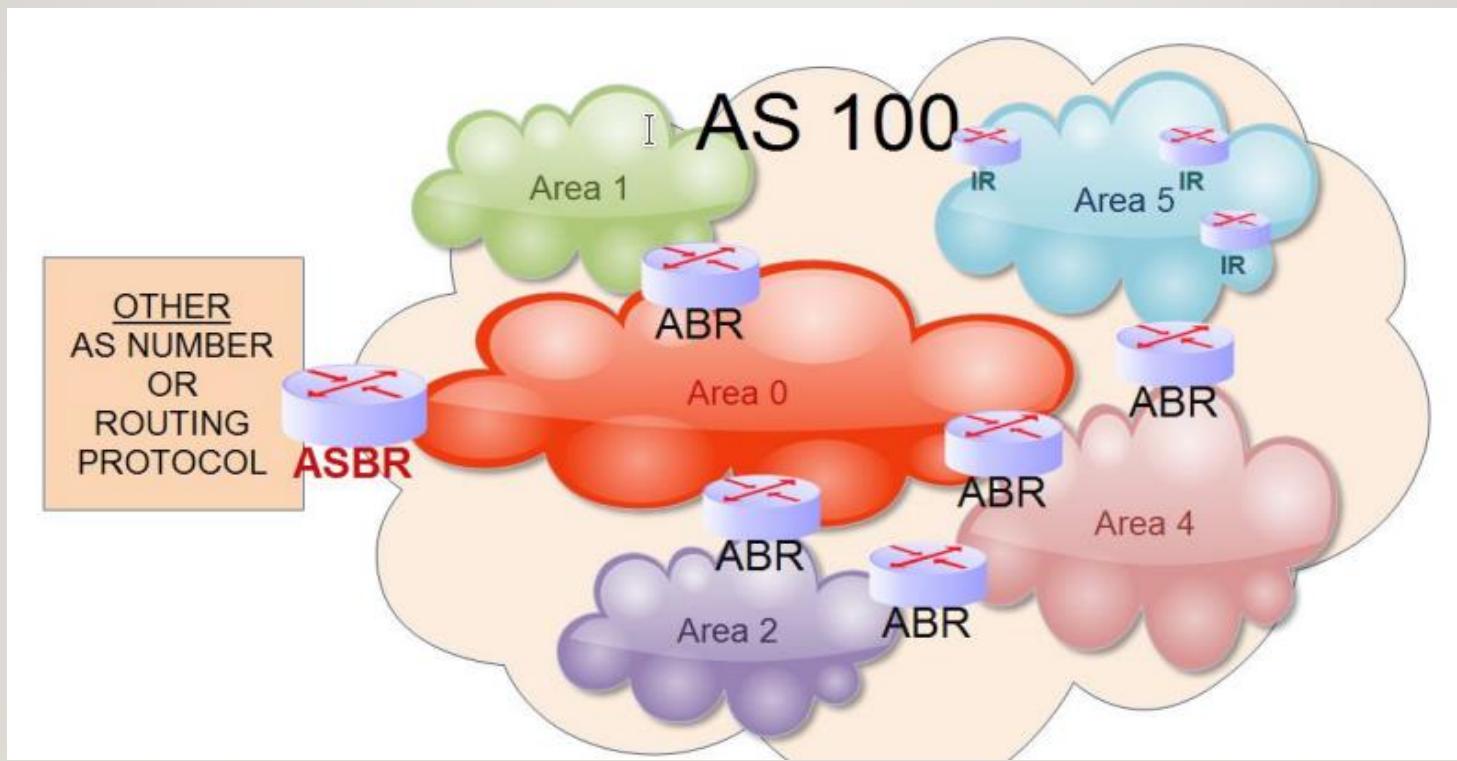


# OSPF AREA

---

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

# OSPF AREA



# IR, ABR, ASBR

---

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

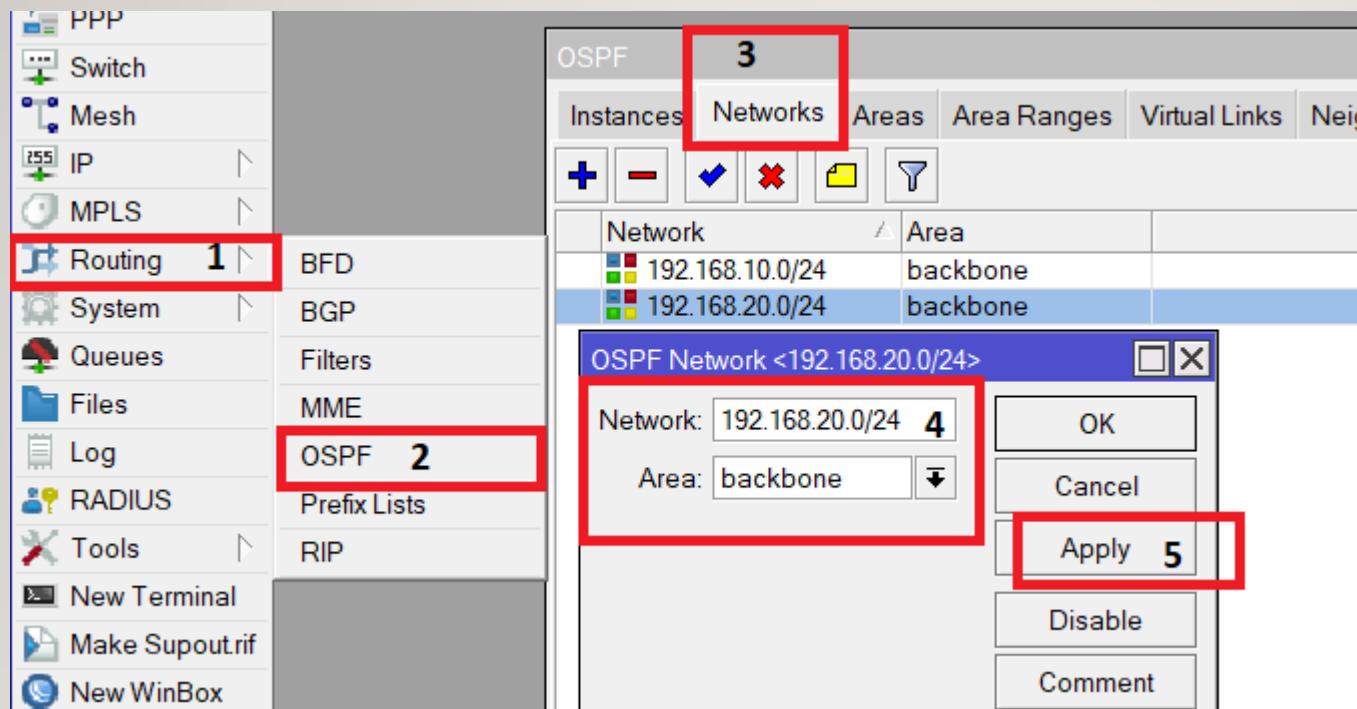
# OSPF SETTING

---

1. 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 terkecil yang terpasang di interface router
    - Biasanya router-id diisi alamat loopbacknya (interface bridge)
2. Redistribute Default Route -> Mendistribusikan default route. Option ini hanya digunakan atau diaktifkan pada router ASBR
3. Redistribute Connected Routes -> Mendistribusikan route yang terpasang dan aktif pada interface
4. Redistribute Static Routes -> Mendistribusikan route static yang ada pada table /ip route
5. Redistribute RIP Routes -> Mendistribusikan route hasil RIP
6. Redistribute BGP Routes -> Mendistribusikan route hasil BGP

# SETTING OSPF PADA MIKROTIK

OSPF akan berjalan ketika sebuah alamat network ditambahkan pada menu **OSPF - network**



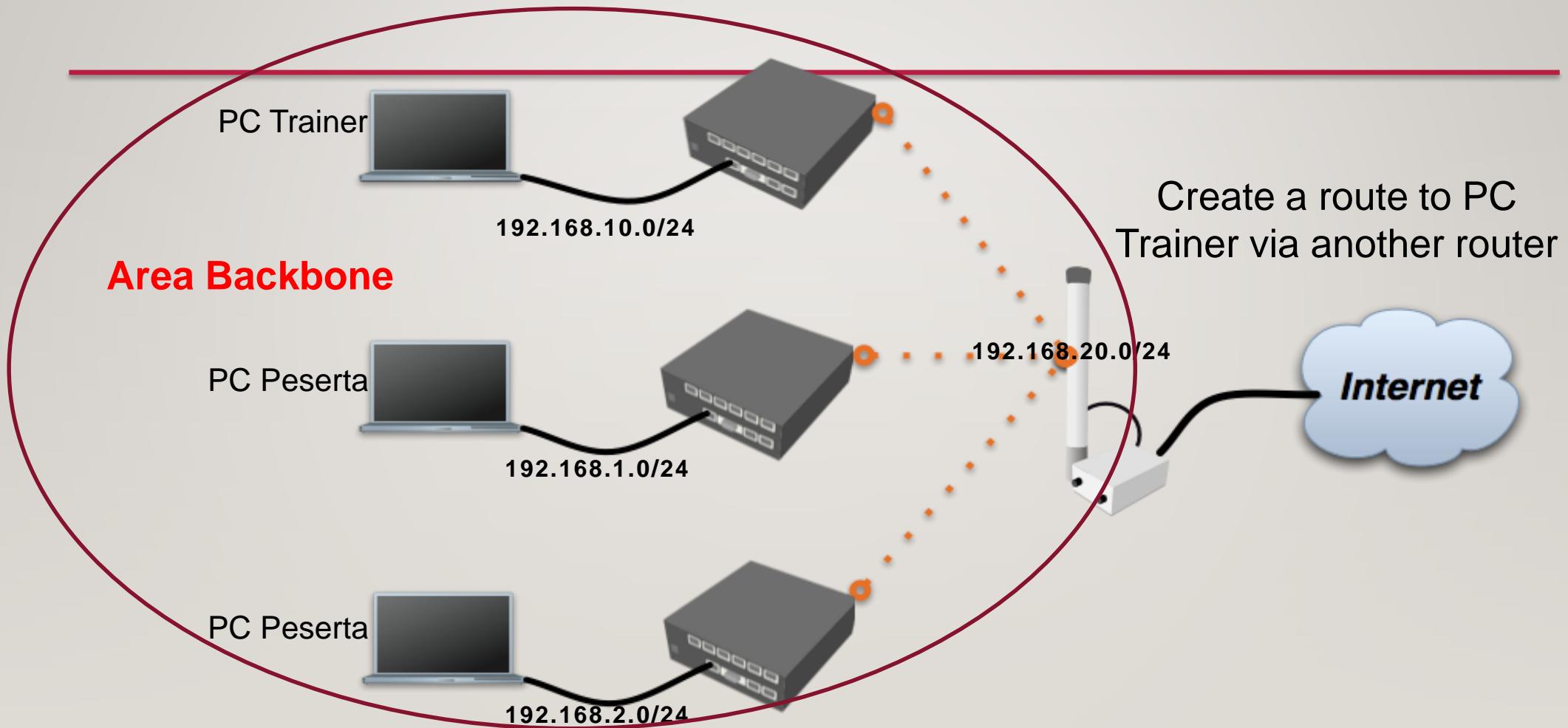
# BACKBONE AREA ( AREA 0 )

---

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

# BACKBONE AREA ( AREA 0 )

LAB



# KONFIGURASI BACKBONE AREA

Berikut adalah konfigurasi pada ROUTER Trainer

The screenshot displays three windows from the Router Trainer software:

- Address List**: Shows IP address assignments. The table has columns: Address, Network, and Interface. Data:

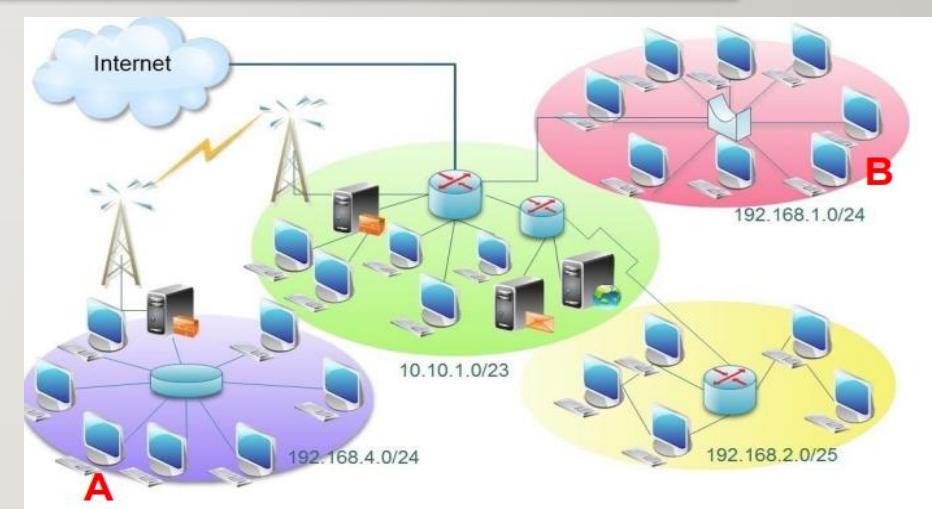
Address	Network	Interface
192.168.10.1/24	192.168.10.0	ether1
D 192.168.20.253/24	192.168.20.0	wlan1
D 192.168.30.254/24	192.168.30.0	ether3
- OSPF**: Shows OSPF configuration. The **Areas** tab is selected. The table has columns: Network and Area. Data:

Network	Area
192.168.10.0/24	backbone
192.168.20.0/24	backbone
- Route List**: Shows the global routing table. The **Routes** tab is selected. The table has columns: Dst. Address, Gateway, Distance, and Routing. Data:

Dst. Address	Gateway	Distance	Routing
AS 0.0.0.0/0	192.168.30.1 reachable ether3, 192.168.20.1 reachable wlan1, 192.168.20.1 reachable...	1	
S 0.0.0.0/0	192.168.30.1 reachable ether3	2	
DAo 192.168.1.0/24	192.168.20.1 reachable wlan1	110	
DAC 192.168.10.0/24	ether1 reachable	0	
DAC 192.168.20.0/24	wlan1 reachable	0	
DAC 192.168.30.0/24	ether3 reachable	0	

# OSPF Area Non Backbone

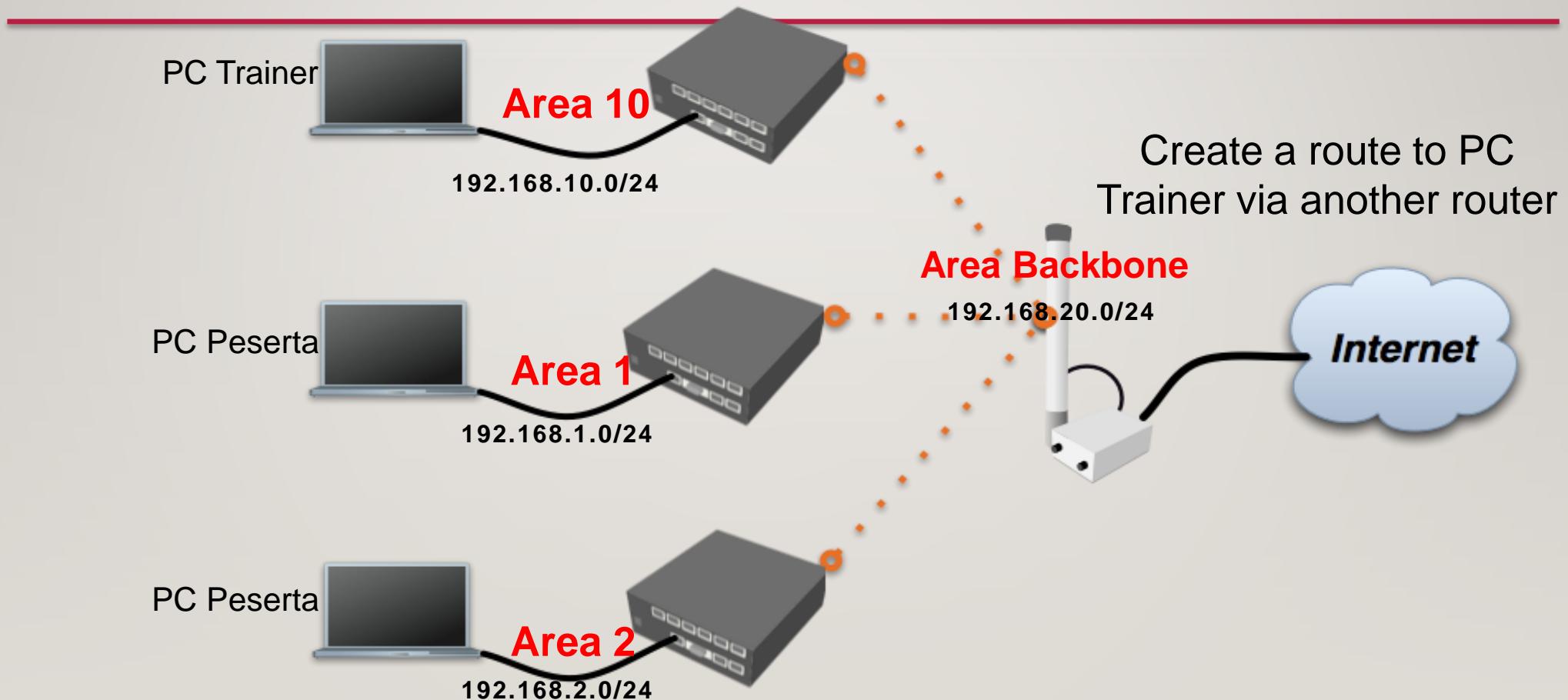
- Sangat memungkinkan jika pada sebuah AS memiliki lebih dari satu area menyesuaikan skala dari jaringan yang dimiliki.
- Semakin banyak router dan jaringan didalamnya, semakin besar ukuran Link State Database (cpu load, memory)
- Internal Router akan mendapat Link State Advertisement (LSA) hanya dari router lain yang masih dalam satu area
- Area yang ingin mendapatkan informasi LSA secara lengkap dan bisa terkoneksi dengan jaringan yang ada di luar AS maka harus terhubung secara logic dengan Backbone (Area0).
- Untuk area non backbone yang tidak terhubung langsung ke area backbone harus menggunakan Virtual Link dengan memanfaatkan area lain yang sudah terhubung ke BackboneArea.



Source IDN MTCRE (idn.id)

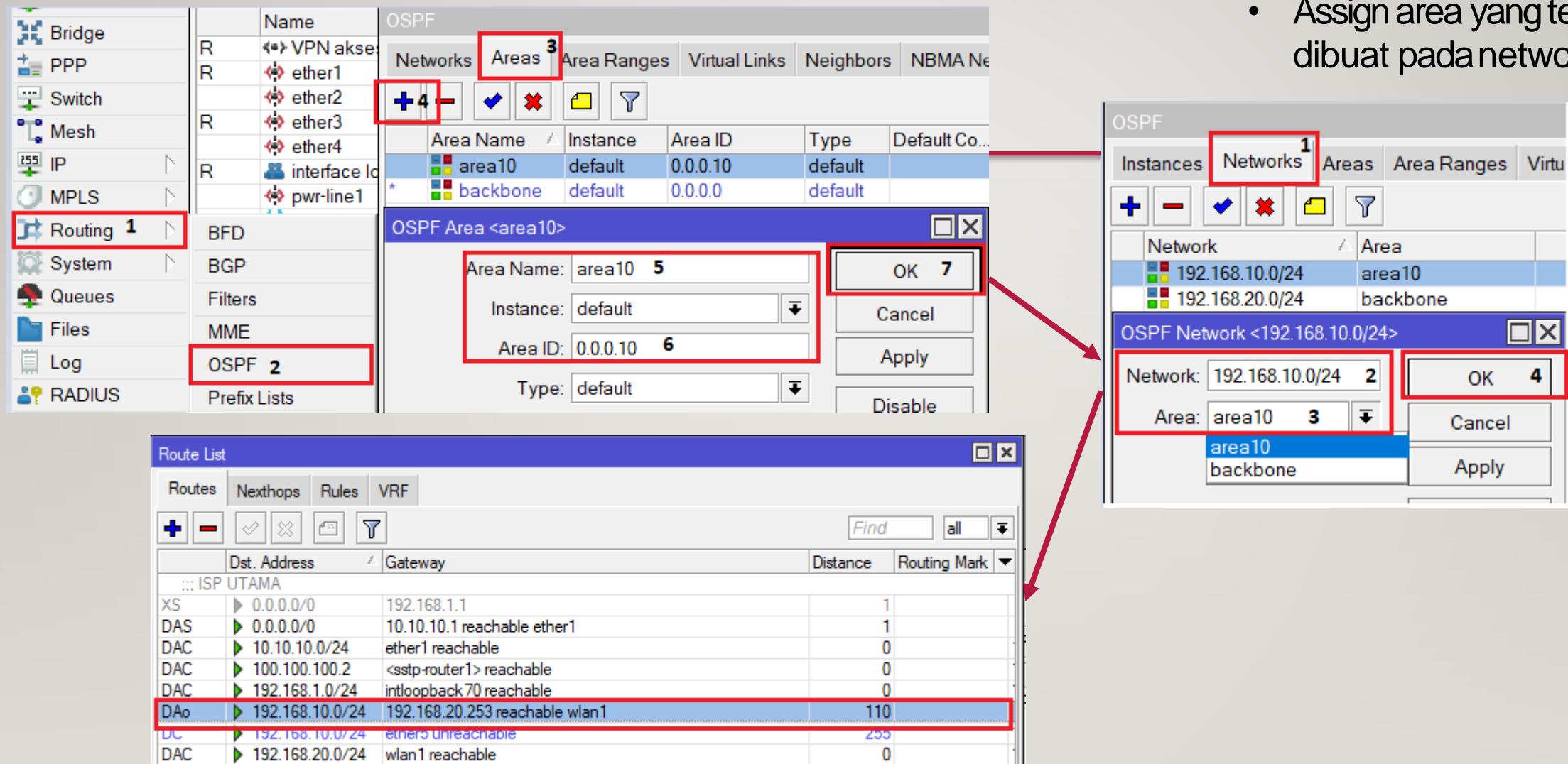
LAB

# BACKBONE AREA ( AREA 0 )



# Membuat Area Baru

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



# Virtual Link

---

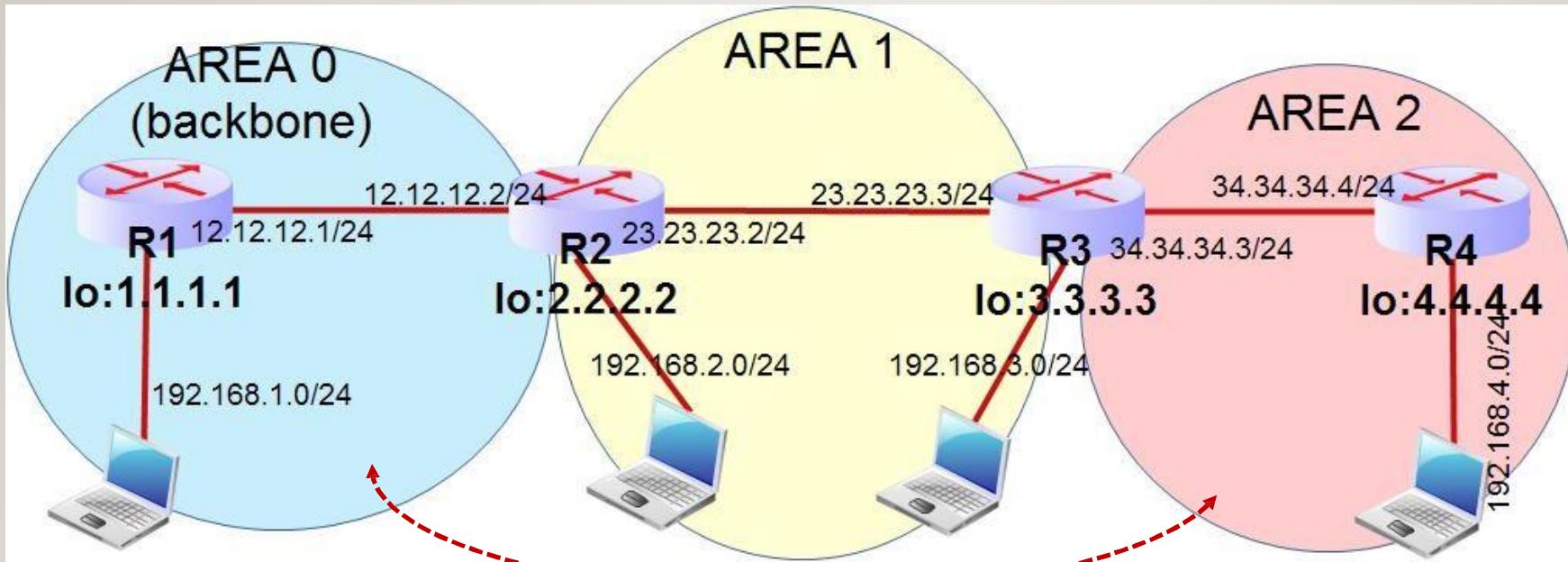
- Setiap non backbone area harus terhubung langsung ke area backbone.
- Virtual link pada OSPF digunakan untuk koneksi non backbone area ke backbone area melewati non backbone area lainnya.
- Virtual link juga digunakan untuk koneksi OSPF antar backbone area melewati non backbone area.

# Virtual Link

Virtual Link (from area 3 to area 0 via area2)

Virtual Link dibuat di dua sisi ABR (R2 dan R3)

---



Source IDN MTCRE (idn.id)

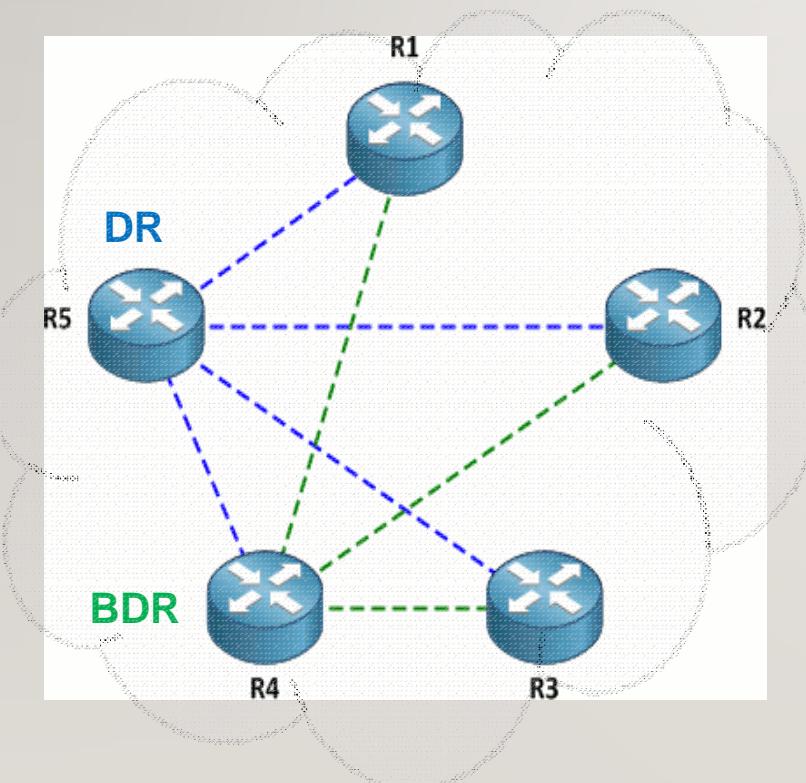
# DR dan BDR

---

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

# DR & BDR

---

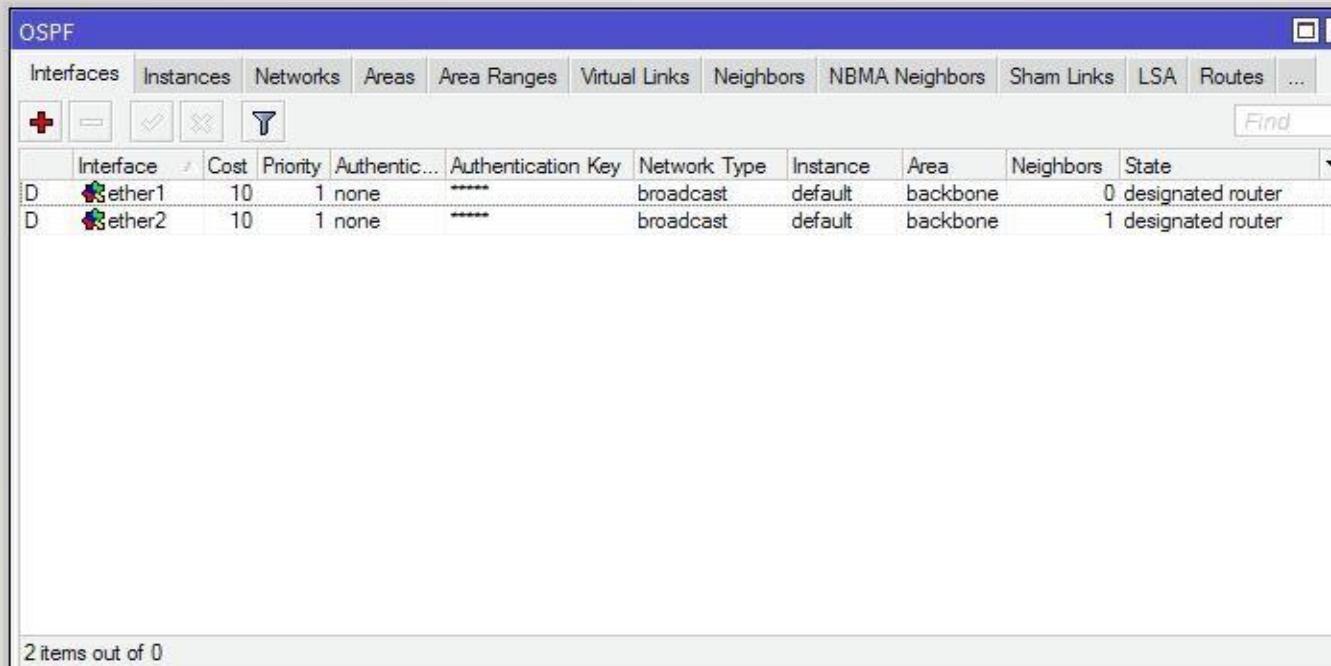


- Dengan adanya BR & BDR, dalam sebuah broadcast network akan mengurangi traffik untuk adjacency.
- Sebuah broadcast network yang terdiri atas 5 router, hanya terjadi 7 adjacency, bukan 9 seperti halnya jaringan mesh.
- Ini berarti pada jaringan broadcast, setiap router hanya perlu melakukan multicast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

Source IDN MTCRE (idn.id)

# DR& BDR

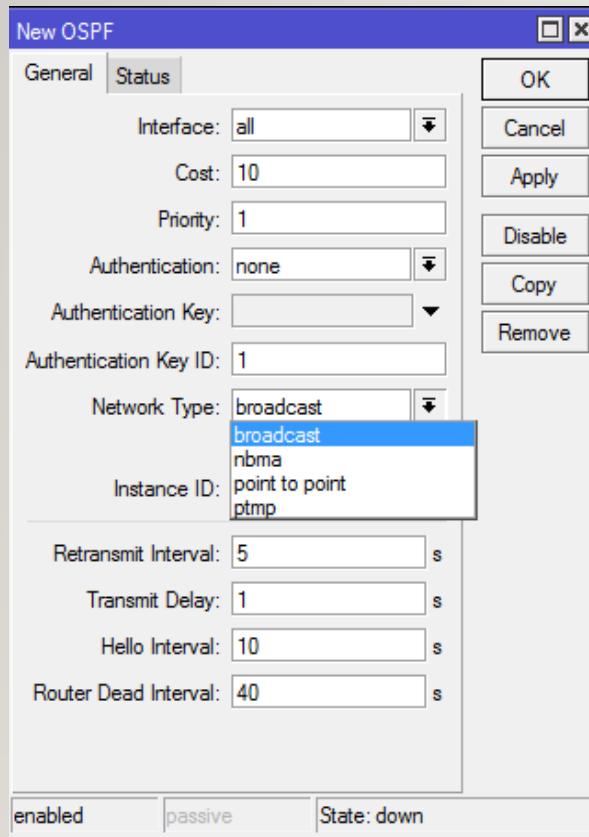
- Designater Router = router dengan OSPF Interfaces semua interfacenya berstatus sebagai designated router



	Interface	Cost	Priority	Authentic...	Authentication Key	Network Type	Instance	Area	Neighbors	State
D	ether1	10	1	none	****	broadcast	default	backbone	0	designated router
D	ether2	10	1	none	****	broadcast	default	backbone	1	designated router

Source IDN MTCRE (idn.id)

# OSPF Network Type



- Default pada interface LAN adalah broadcast

Source IDN MTCRE (idn.id)

# OSPF Network Type

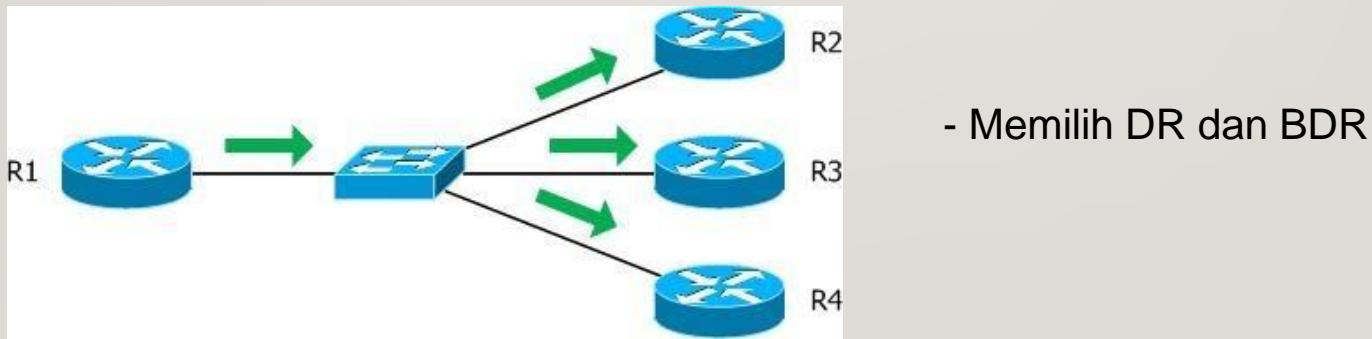
## a. Point to Point

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



## b. Broadcast

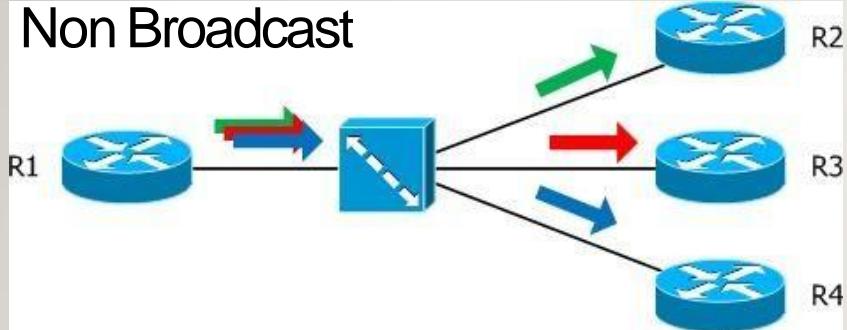
- Single packet yang ditransmisikan oleh router dapat digandakan oleh device seperti Ethernet switch) sehingga setiap sisi end pointnya menerima copy dari paket tersebut



Source IDN MTCRE (idn.id)

# OSPF Network Type

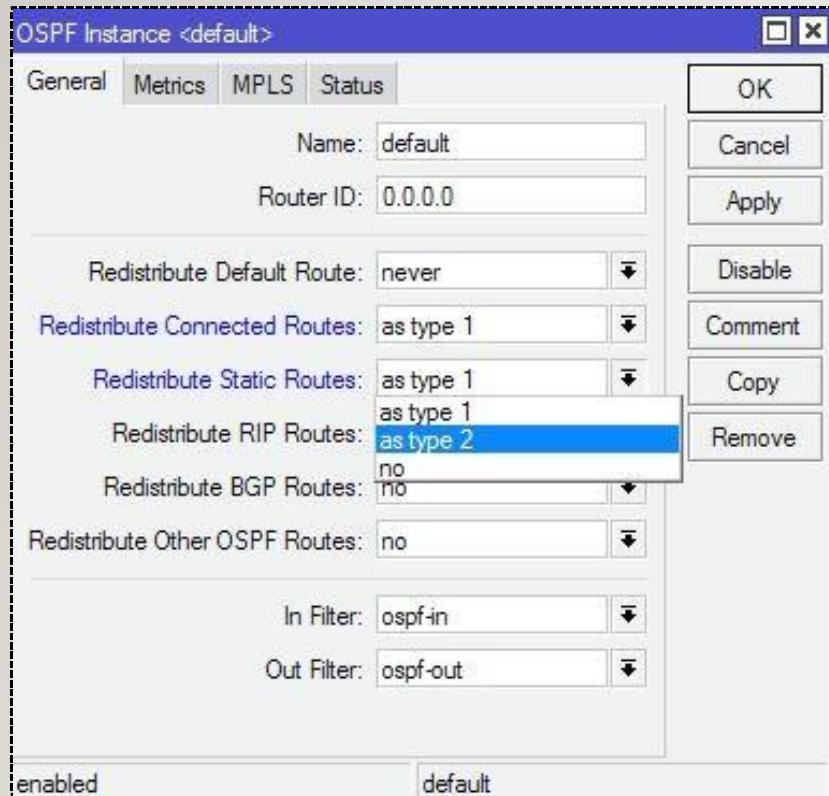
## c. Non Broadcast



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

Source IDN MTCRE (idn.id)

# OSPF Redistribute Type



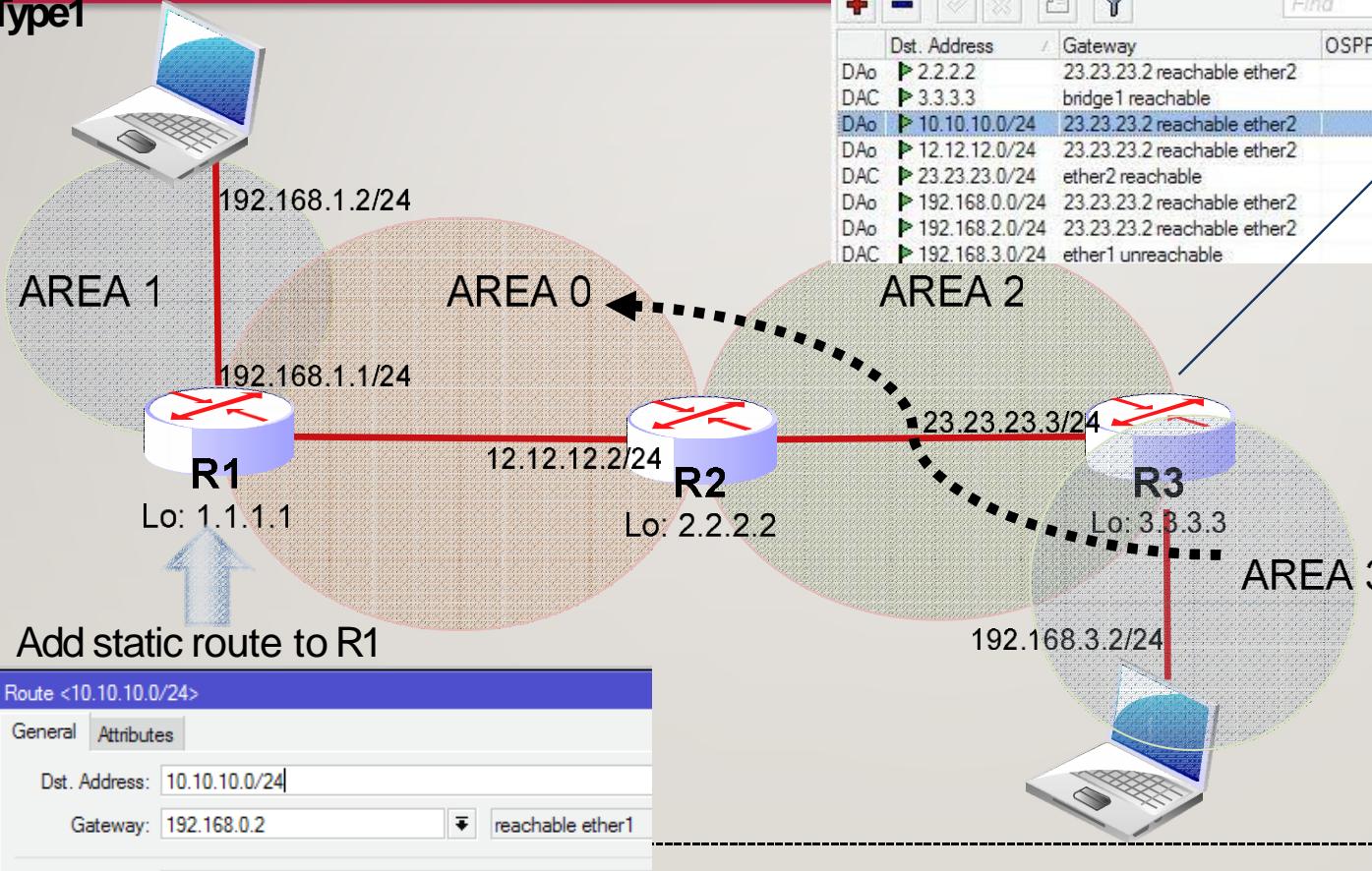
- **as-type-1** – keputusan remote routing network dilakukan berdasarkan **jumlah dari external and internal metrics**
- **as-type-2** – keputusan remote routing network hanya dilakukan berdasarkan **external metrics** (internal metrics tidak diperhitungkan).

Source IDN MTCRE (idn.id)

# Option Redistribute

## Option Redistribute AS-

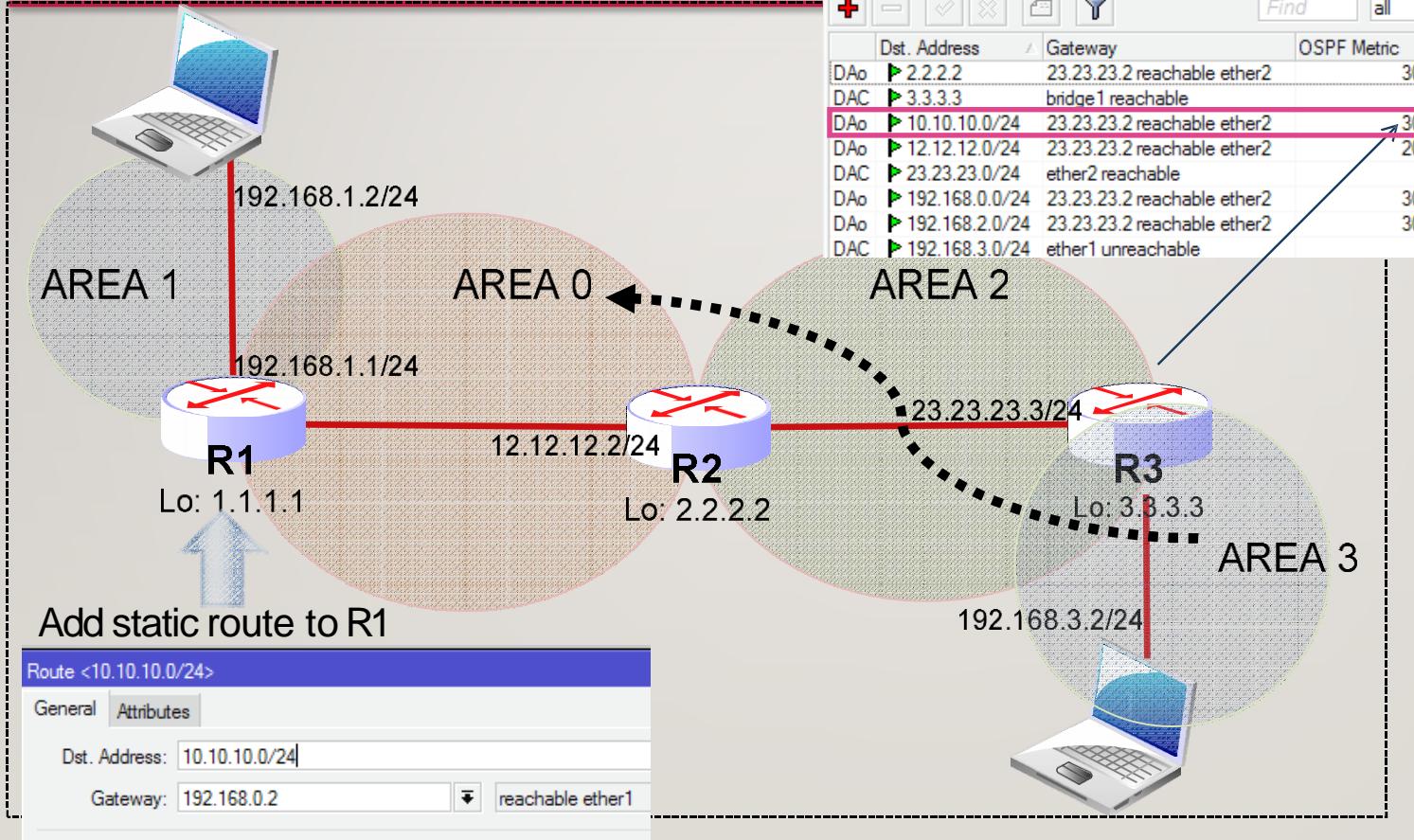
Type1



Source IDN MTCRE (idn.id)

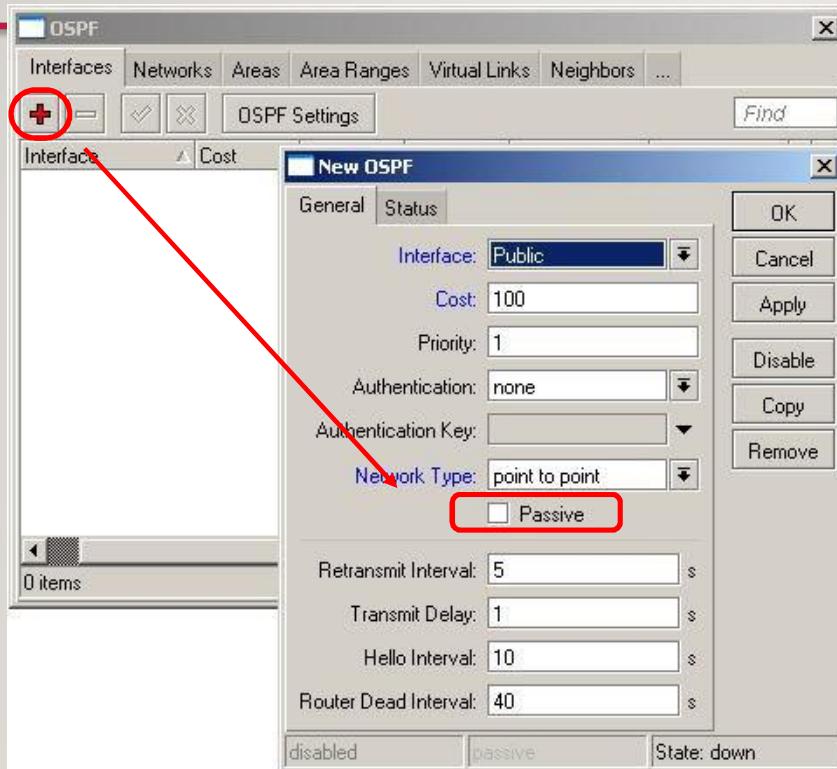
# Option Redistribute

Option Redistribute AS-Type2



Source IDN MTCRE (idn.id)

# Passive interface



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

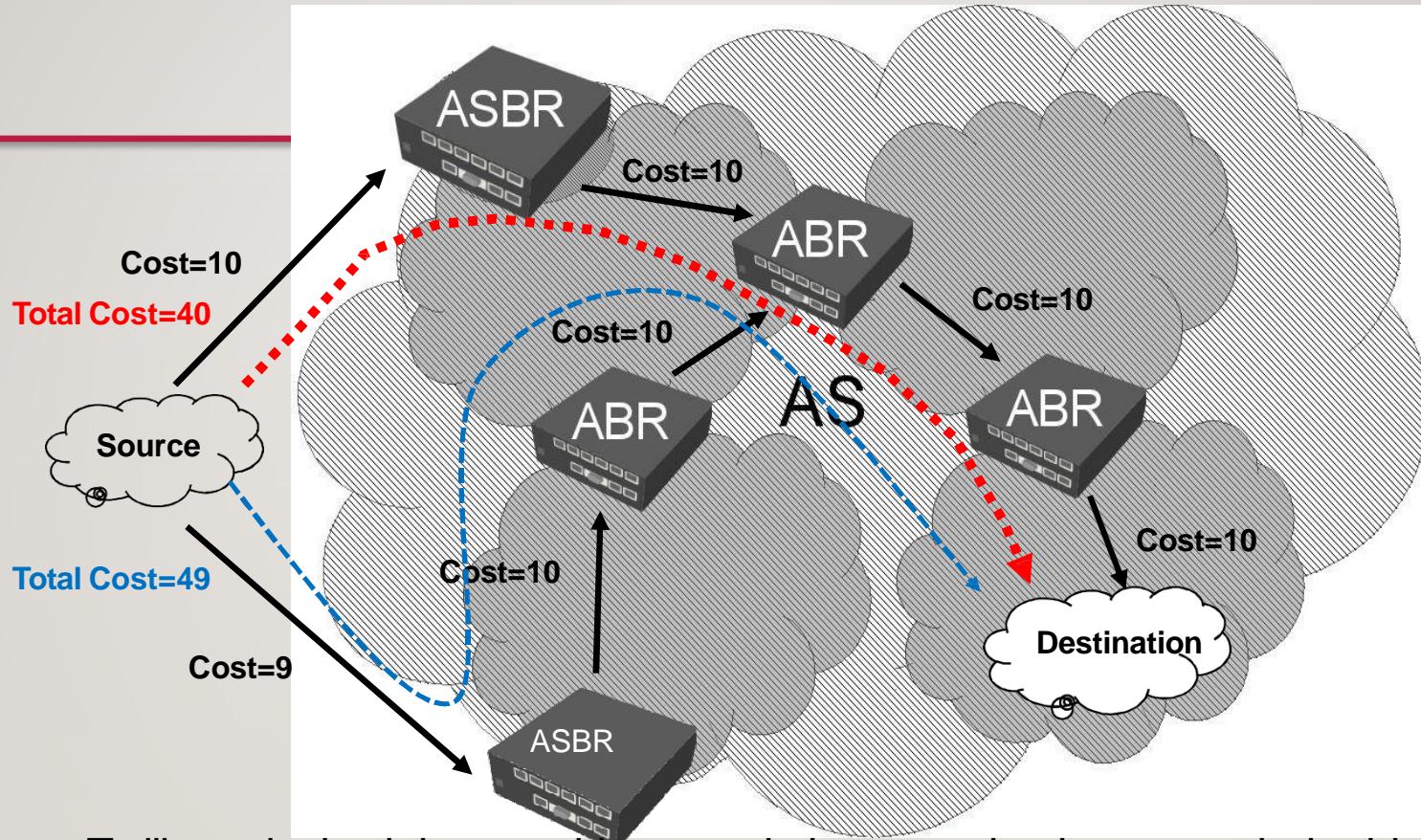
Source IDN MTCRE (idn.id)

# OSPF Cost

---

- Untuk menentukan jalur terpendek atau bisa juga diartikan sebagai jalur prioritas, OSPF menggunakan parameter “Cost”.
- Nilai cost adalah  $10^8/\text{bandwidth}$
- OSPF “Cost” akan dijumlahkan di setiap loopnya pada proses Link State / Shortest Path Technology.
- Setelah semua jalur sudah dikalkulasi dan total
- Cost semua jalur sudah dijumlahkan, maka akan dipilih jumlah akumulasi cost yang terkecil

# OSPF Cost



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

Source IDN MTCRE (idn.id)

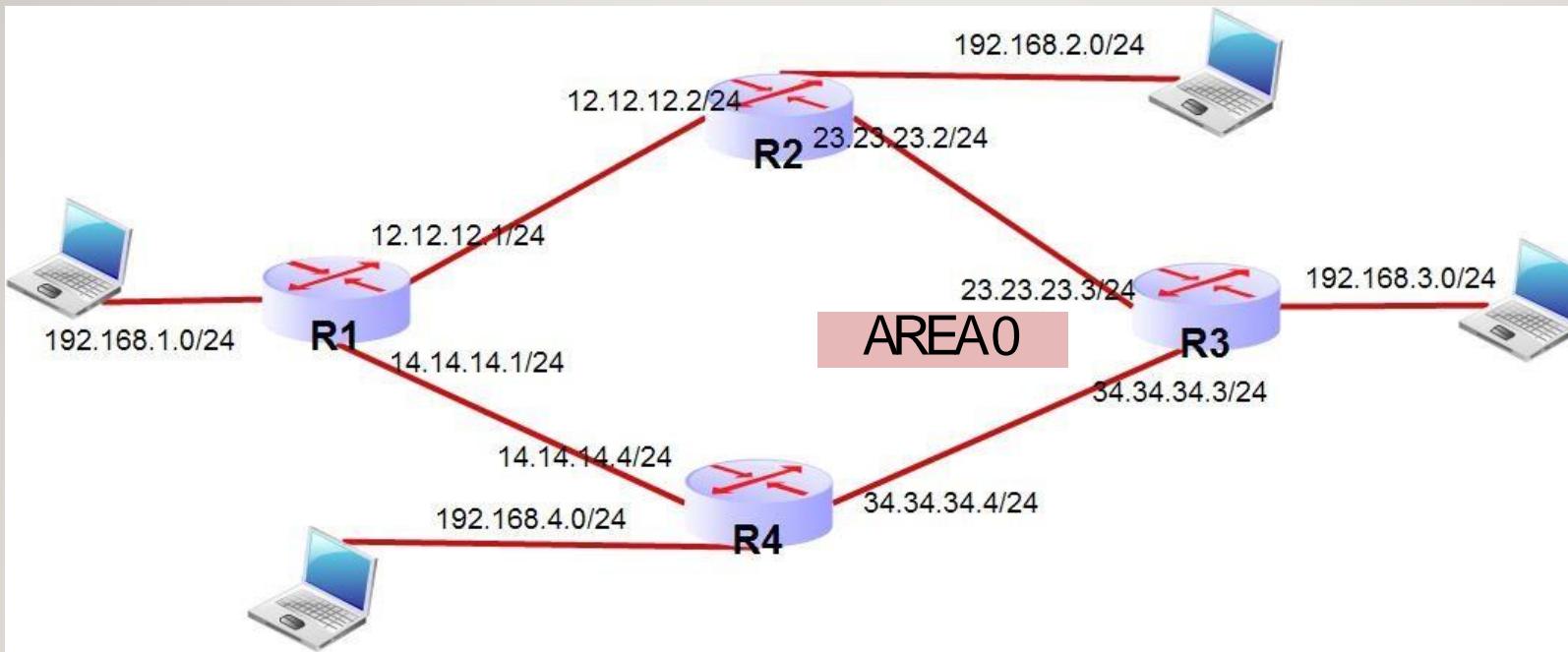
# OSPF Redundancy

---

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

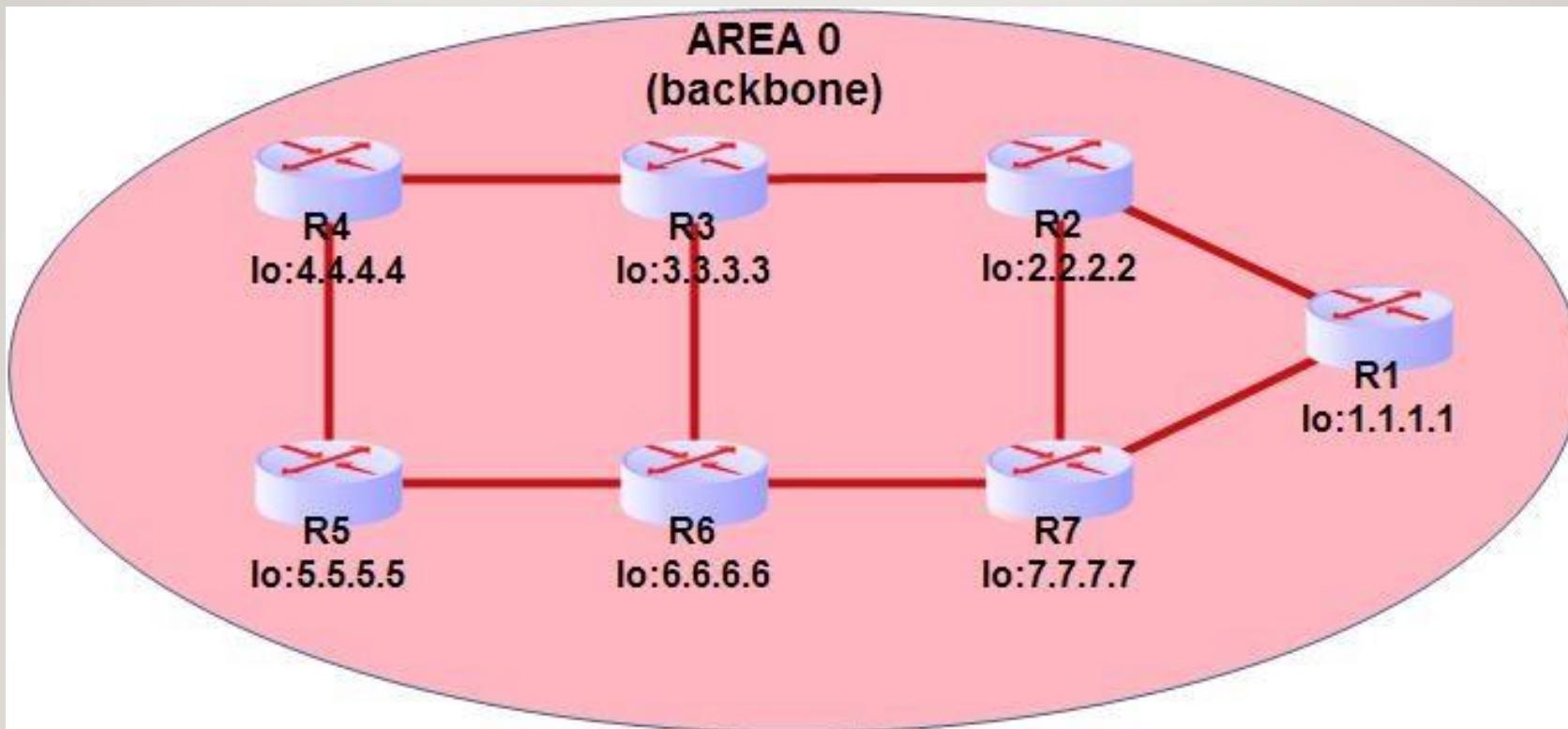
# OSPF Redundancy

- Buat topologi untuk test load balancing dan fail over pada OSPF



Source IDN MTCRE (idn.id)

# OSPF Redundancy



Source IDN MTCRE (idn.id)

# Routing Filter

---

Fungsi routing filter:

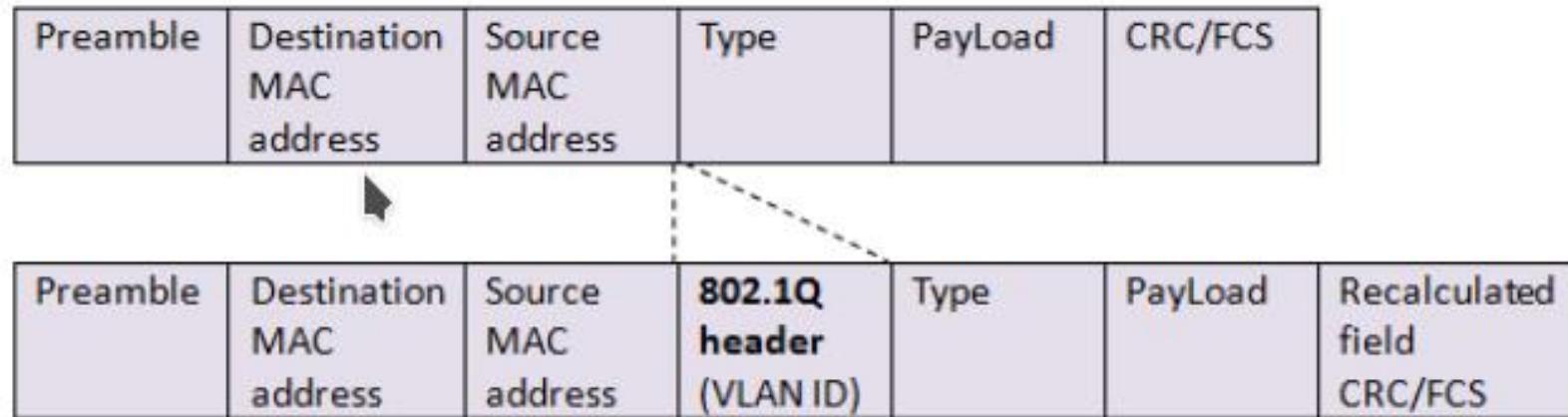
- Memfilter prefix atau route yang masuk ke tabel routing.
- Memfilter prefix atau route yang akan didistribusikan ke router lainnya
- Mengubah nilai parameter route

# VLAN (VIRTUAL LOCAL AREA NETWORK)

---

- VLAN adalah metode pada layer 2 yang dapat mengizinkan beberapa vlan pada sebuah interface fisik (Ethernet, wireless dan lain-lain)
- Karena VLAN bekerja pada layer 2 OSI, VLAN dapat digunakan sebagaimana network interface lainnya tanpa ada batasan apapun
- Protokol yang umumnya digunakan untuk VLAN adalah IEEE 802.1Q
- Ini adalah protocol enkapsulasi standar untuk mendefinisikan cara untuk memasukan 4 byte VLAN identifier ke Ethernet header

# 802.1Q



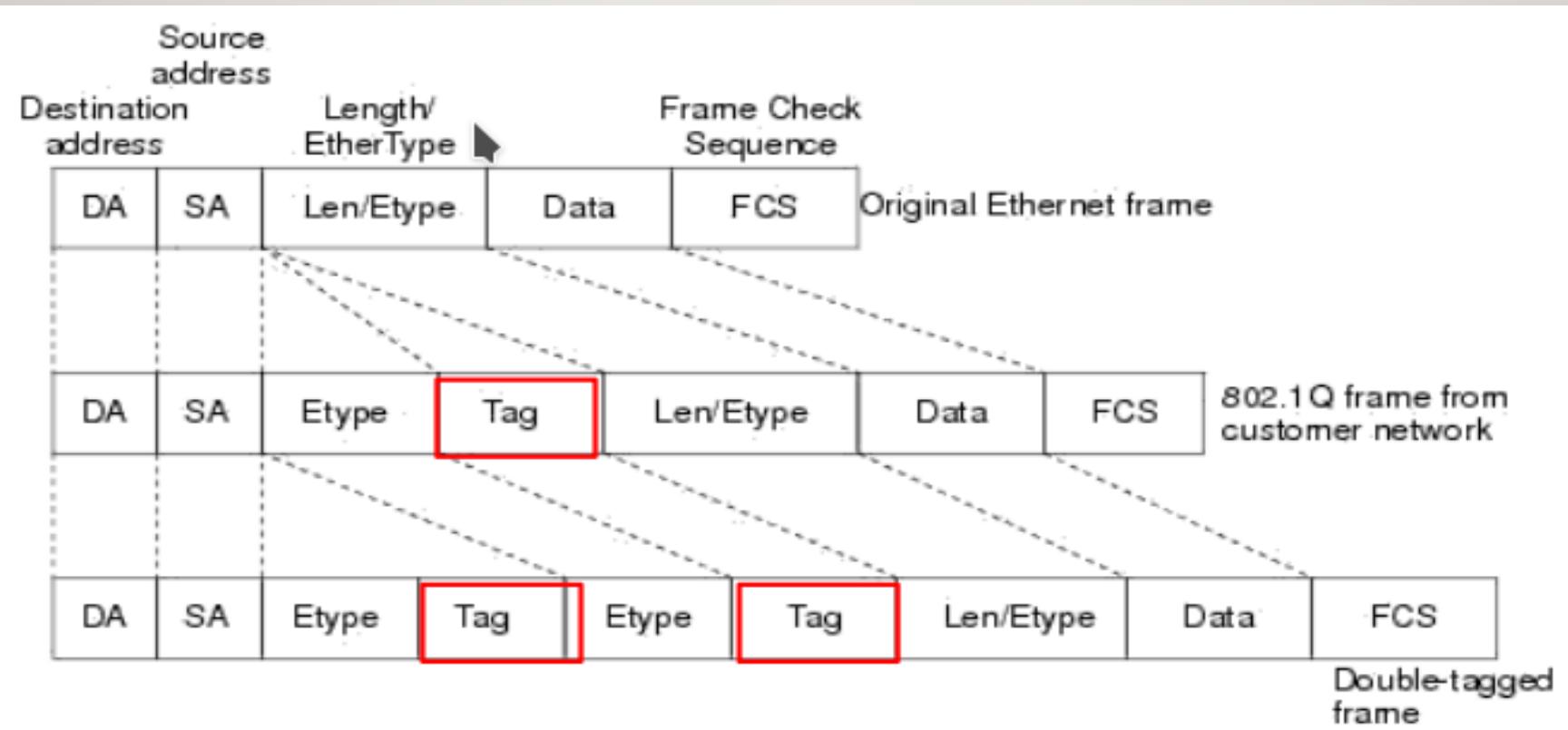
Insertion of 802.1Q Tag (VLAN ID) in Ethernet-II frame

# Q-IN-Q IMPLEMENTATION

---

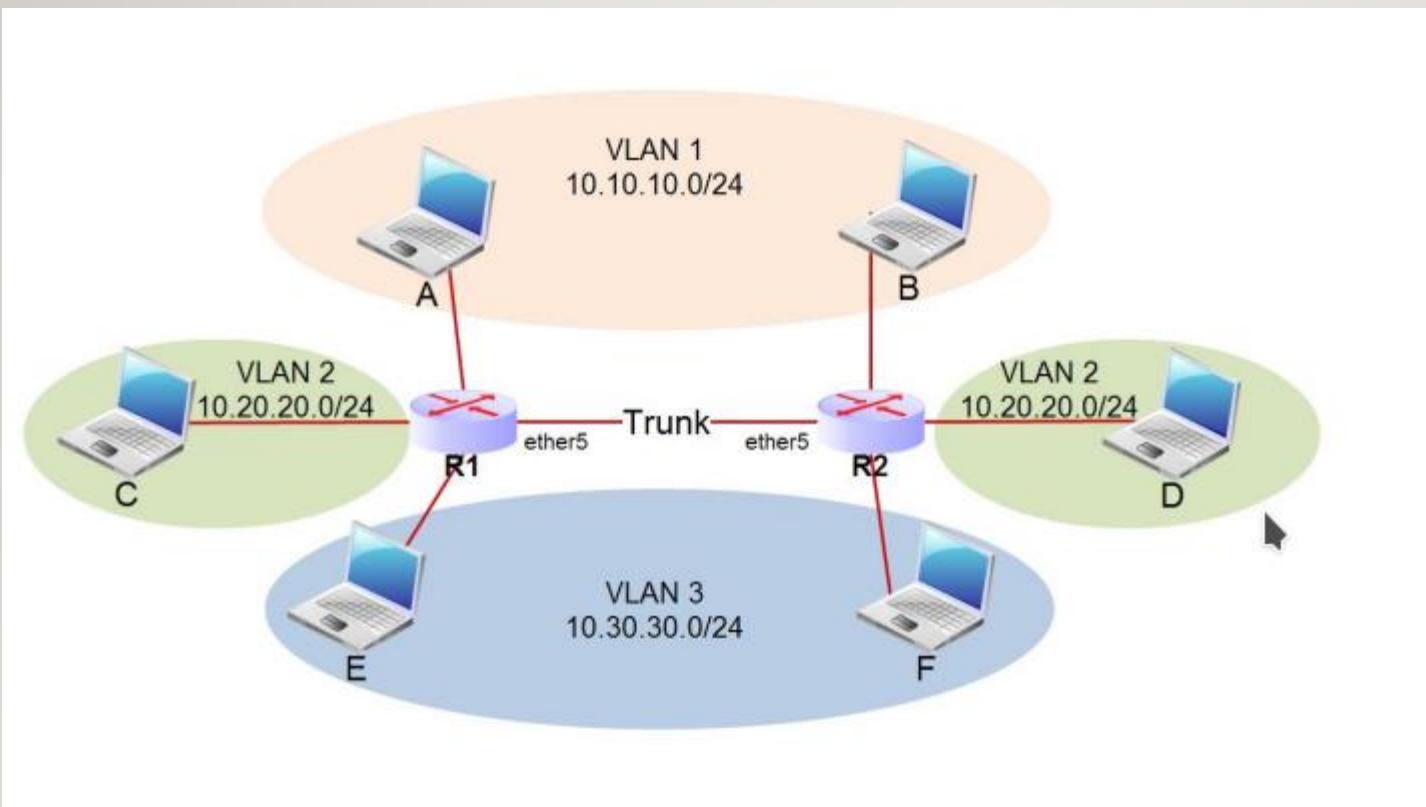
- Pada dasarnya protocol 802.1Q hanya mengijinkan 1 VLAN header
- Pada metode Q-in-Q dapat mengijinkan 2 atau lebih vlan header
- Pada RouterOS, konfigurasi Q-in-Q dapat dilakukan dengan menambahkan 1 atau beberapa interface VLAN diatas VLAN lain

# Q-IN-Q IMPLEMENTATION



# VLAN (VIRTUAL LOCAL AREA NETWORK)

---



# VLAN (VIRTUAL LOCAL AREA NETWORK)

- Add new interface VLAN

The image shows two windows from a network configuration tool. The left window is a 'New Interface' dialog for creating a 'VLAN' type interface. It has fields for Name (vlan1), Type (VLAN), MTU (1500), L2 MTU, MAC Address, ARP (enabled), VLAN ID (1), and Interface (ether5). A red box highlights the 'VLAN ID: 1' field. The right window is an 'Interface List' table showing existing interfaces and the newly created VLAN1 interface.

VLAN ID = unik

Interface untuk trunk

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

# SWITCH PORT PADA VLAN

---

- Ada 2 jenis port /switch port pada VLAN
- • Edge ports: (Untagged, pada Cisco:Access Port)
  - Adalah switch port yang dikonfigur sebagai bagian dari sebuah VLAN
  - switchport ini tidak mengirim 4 byte tag. Digunakan oleh device yang tidak melewaskan VLAN seperti komputer klien, printer, dll.
- • Core port: (Tagged, pada Cisco:Trunk Port)
  - Adalah switch port yang diconfigure untuk mengirim 4 byte VLAN tag. Digunakan oleh device yang mensupport VLAN seperti switches,routers and servers.

# SOURCE MATERI

---

- gpmnetwork team ( gpmnetwork.id)
- IDN IT training dan Consultant ( idn.id )