

INTRA Training Center

PRE-MTCNA

21 - 23 April 2017



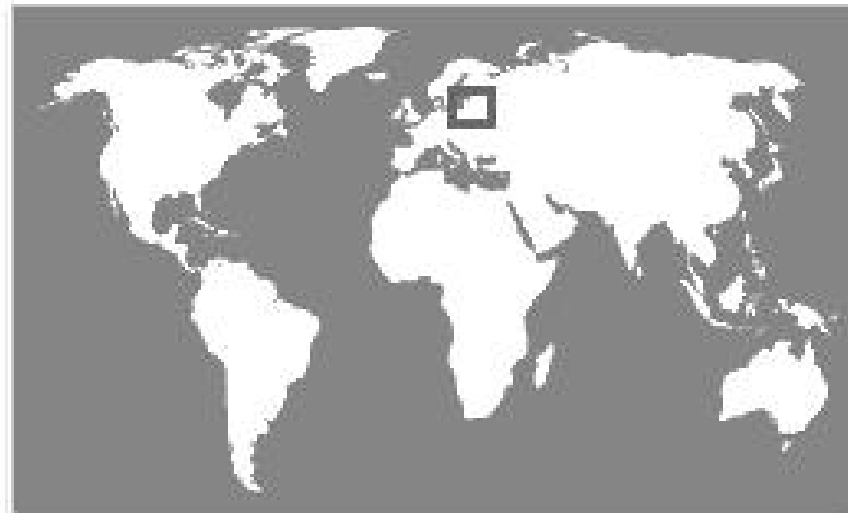
SMK-Net
INDONESIA

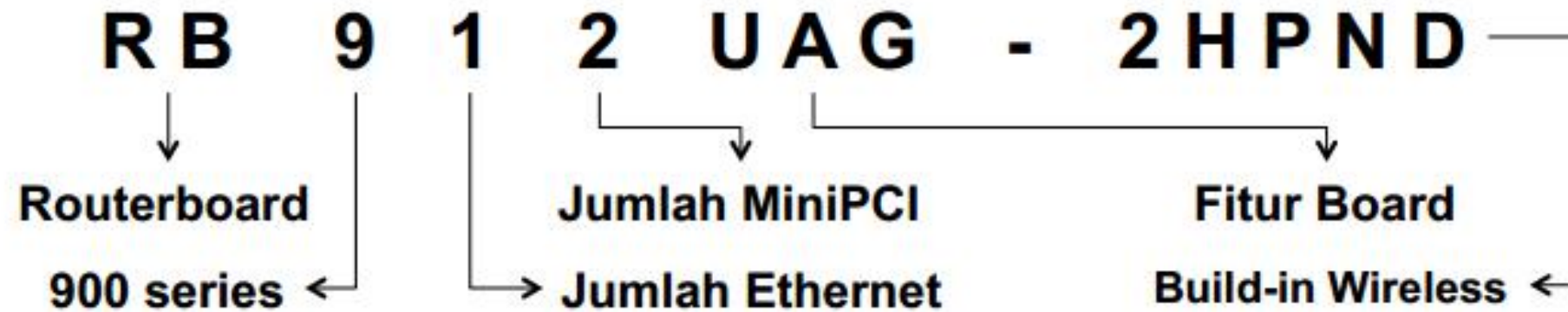
Persembahkan
BLC TELKOM **BLC**
Broadband
Learning Center
Untukmu INDONESIA

- **RouterOS** > Software Router untuk PC (x86, AMD, DLL).
 - Menjadikan PC biasa memiliki fungsi router yang lengkap
 - Diinstall sebagai Operating System, Tidak membutuhkan operating system lainnya.
- **Routerboard** > Hardware untuk jaringan (terutama wireless)
 - Wireless board(Contoh : RB400, RB600, RB750, RB1000,dll)
 - Wireless Interface(R52, R52H, R5H, R52N, R2N,dll)
 - Menggunakan RouterOS sebagai software

Introduction About MikroTik

- MikroTik adalah kependekan dari "**mikrotikls**"
- Artinya : "network kecil" dalam bahasa Latvia





Fitur Board Code :

U : USB

P : PoE out

i : single PoE out

A : RAM besar (bisa juga lisensi)

H : CPU besar

G : Gigabit

L : Light Edition

S : SFP Port

e : PCIe Extension Card

X : Jumlah CPU Core

- RouterOS adalah sistem operasi dan perangkat lunak yang mampu membuat PC berbasis Intel/AMD mampu melakukan fungsi **Router, Bridge, Firewall, Bandwidth Management, Proxy, Hotspot**, dan masih banyak lagi.
- RouterOS dapat melakukan hampir semua fungsi networking dan juga beberapa fungsi server.

- IP Routing
 - Static route & Policy route
 - Dynamic Routing (RIP, OSPF, BGP)
 - Multicast Routing
- Interface
 - Ethernet, V35, G703, ISDN, Dial Up Modem
 - Wireless : PTP, PTMP, Nstream, WDS, Mesh
 - Bridge, Bonding, STP, RSTP
 - Tunnel : EoIP, IPSec, IPIP, L2TP, PPPoE, PPTP, VLAN, MPLS, OpenVPN, SSTP
- Firewall
 - Mangle, NAT, Address List, Filter Rules, L7 Protocol
- Bandwidth Managemen
 - HTB, PFIFO, BFIFO, SFQ, PCQ, RED

- **Services (Server)**
 - Proxy(cache), Hotspot, DHCP, IP Pool, DNS, NTP, Radius Server(User-Manager), Samba(v6.xx)
- **AAA**
 - PPP, Radius Client
 - IP Accounting, Traffic Flow
- **Monitoring**
 - Graphs, Watchdog, Tournch, Custom Log, SNMP, The Dude Monitoring Tools
- **Diagnostic Tools & Scripting**
 - Ping, TCP Ping, Tracert, Network Monitoring, Traffic Monitoring, Scheduller, Scripting
- **VRRP**

License Level

Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key ↗	registration required ↗	volume only ↗	\$45	\$95	\$250
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h trial	-	yes(+)	yes	yes	yes
EoIP tunnels	24h trial	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited
L2TP tunnels	24h trial	1	200	200	500	unlimited
OVPN tunnels	24h trial	1	200	200	unlimited	unlimited
VLAN interfaces	24h trial	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h trial	1	1	200	500	unlimited
RADIUS client	24h trial	-	yes	yes	yes	yes
Queues	24h trial	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h trial	-	yes	yes	yes	yes
User manager active sessions	24h trial	1	10	20	50	Unlimited
Number of KVM guests	none	1	Unlimited	Unlimited	Unlimited	Unlimited

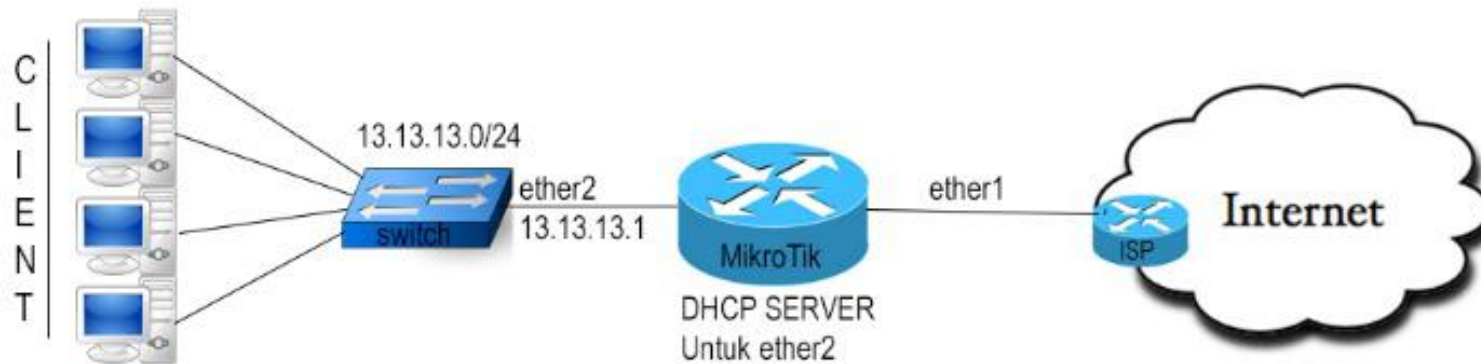
Produk mana yang dipilih?

- Kenalilah kebutuhan Anda :
 - Fungsi perangkat (Router, Server, dll)
 - Jumlah trafik (Real Troughput)
 - Fitur yang dibutuhkan (Proxy, Hotspot, Radius)
 - Interface yang dibutuhkan
- Baik menggunakan PC ataupun menggunakan Routerboard, fitur MikroTik ROuterOS selalu sama (tergantung pada level yang digunakan)

- 300/400 Mhz Processor (< **5Mbps** Traffic)
 - RB450, RB750, RB433, RB493
- 680 Mhz Processor (**5 - 20 Mbps** Traffic)
 - RB450G, RB433AH, RB493G
- 1Ghz Processor (**20 - 100 Mbps** Traffic)
 - RBB1200, RB1100AH
- 1Ghz Dual Core Processor (> **100 Mbps** Traffic)
 - RB1100AHx2
- Multi Core x86 Processor (> **1 Gbps** Traffic)
 - Mikrobits : Aneto, Ainos, Dinara
- Xeon Processor (> **10 Gbps** Traffic)
 - Mikrobits : Dinara

www.routerboard.co.id

- DHCP atau Dynamic Host Control Protocol berfungsi untuk memberikan IP Address, DNS , Gateway otomatis dari Server kepada Client.
- Pada MikroTik sendiri, kita dapat membuat router menjadi DHCP Server untuk para Client, dan bisa juga Router MikroTik menjadi DHCP Client dan meminta IP , DNS , Gateway dari ISP atau dari router lain yang terhubung melalui jaringan Ethernet atau pun Wireless.



DHCP Server biasanya digunakan untuk ke client yang lebih dari 10 PC

(LAB)DHCP Server

The screenshot displays a network configuration interface. On the left, a tree view shows the following structure:

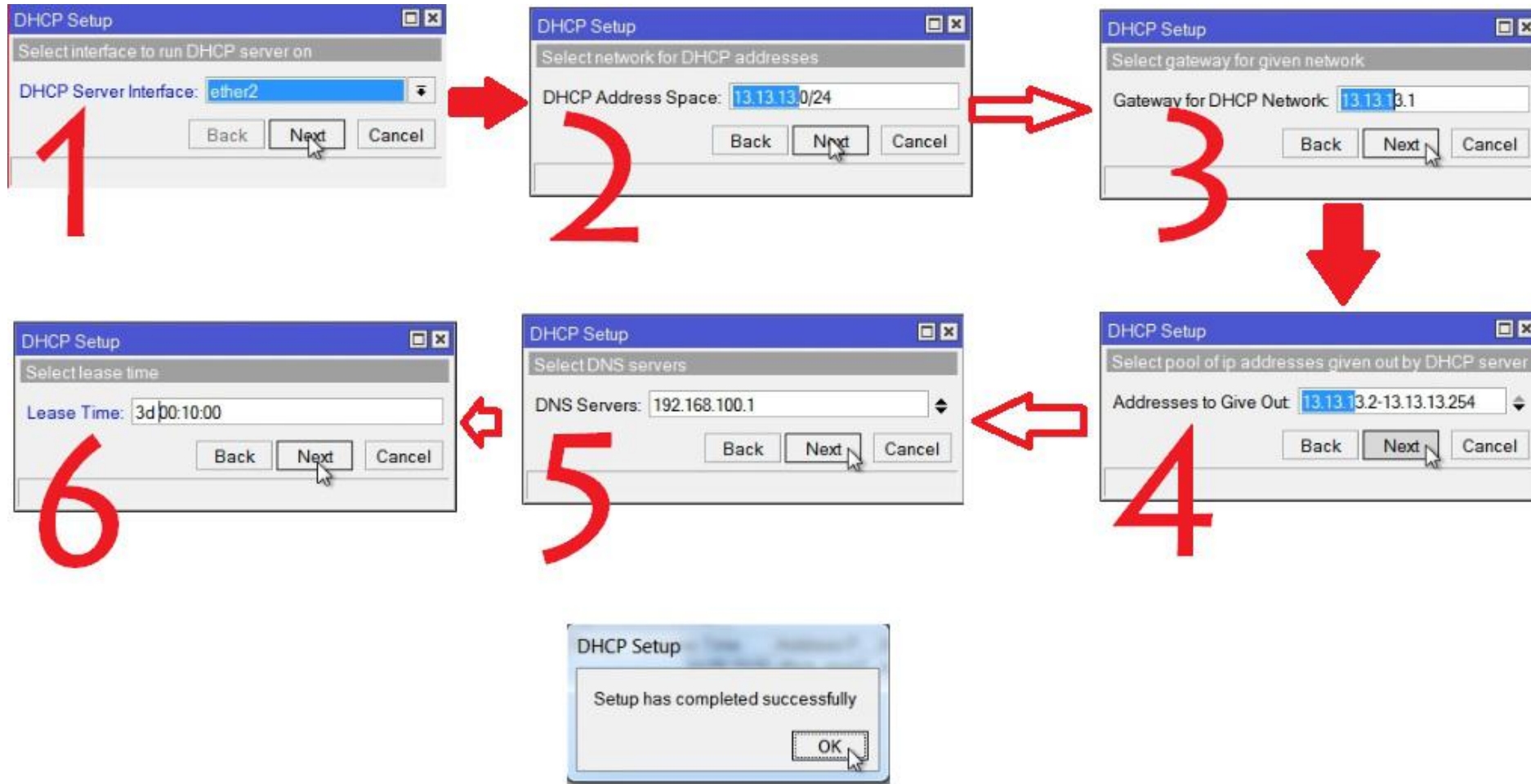
- IP (highlighted with a red box)
- MPLS
- Routing
- System
- Queues
- Files
- Log

Under the 'IP' folder, the 'DHCP Server' option is selected and highlighted with a red box. A red line connects this selection to the 'DHCP' tab in the main configuration area.

The main configuration area is titled 'DHCP Server' and contains the following elements:

- A 'DHCP' tab (highlighted with a red box) is selected.
- Sub-tabs include 'Networks', 'Leases', 'Options', 'Option Sets', and 'Alerts'.
- Buttons for '+', '-', '✓', '✗', and a funnel icon are present.
- 'DHCP Config' and 'DHCP Setup' buttons are visible, with 'DHCP Setup' highlighted by a red box.
- A table with columns 'Name', 'Interface', 'Relay', and 'Lease Time' is shown at the bottom.

(LAB)DHCP Server



Terminal DHCP Server Wizard

```
[admin@Rangga] > ip dhcp-server setup
Select interface to run DHCP server on

dhcp server interface: ether2
Select network for DHCP addresses

dhcp address space: 13.13.13.0/24
Select gateway for given network

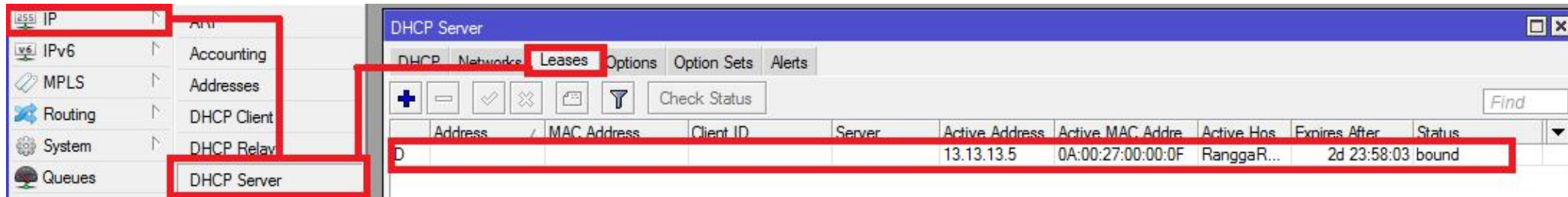
gateway for dhcp network: 13.13.13.1
Select pool of ip addresses given out by DHCP server

addresses to give out: 13.13.13.2-13.13.13.5
Select DNS servers

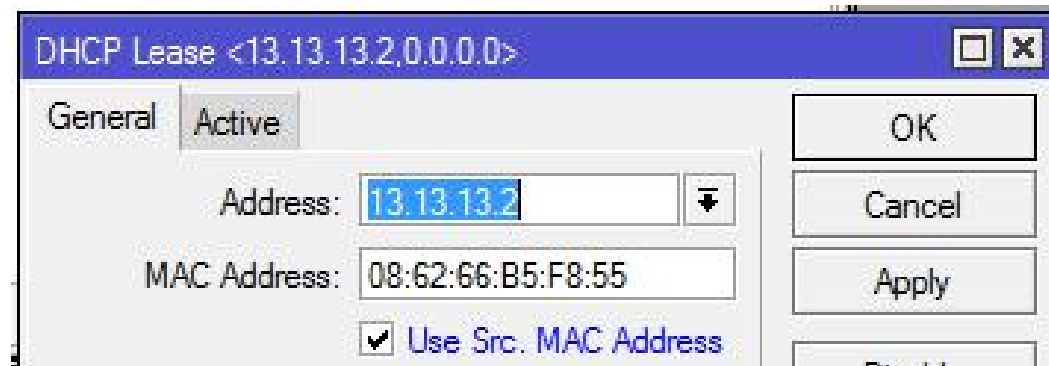
dns servers: 192.168.100.1
Select lease time
```

- Ubahlah konfigurasi IP Address dan DNS pada laptop client menjadi otomatis
- Cek pada laptop apakah sudah mendapatkan alokasi IP Address dari DHCP
 - **C:\ipconfig** lalu tekan **enter**
- Cobalah melakukan koneksi ke Internet

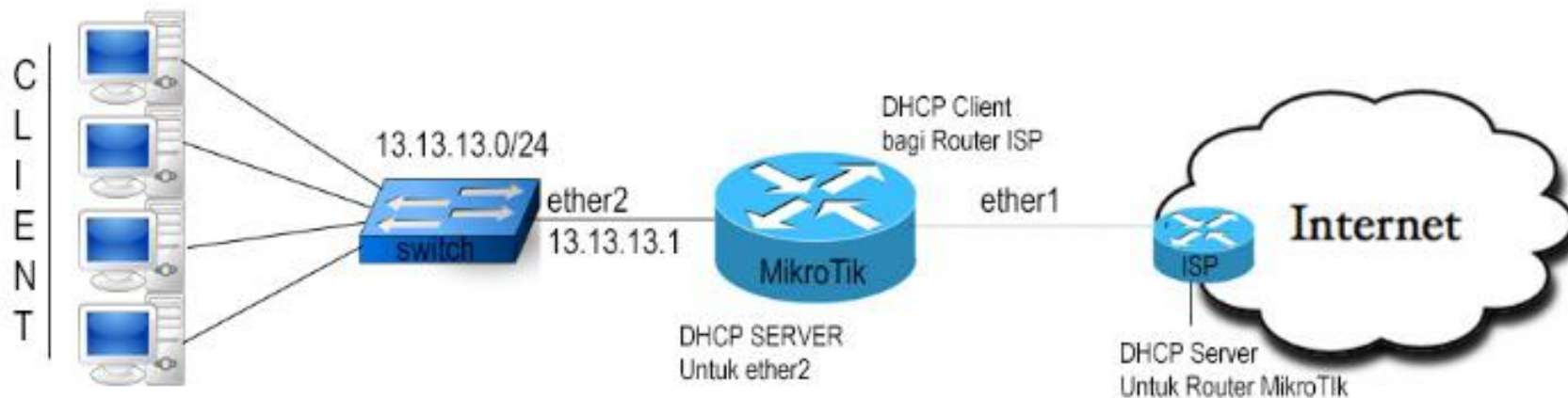
DHCP Management



- Daftar DHCP yang aktif terlihat pada menu **DHCP Server > Leases**
- Untuk membuat IP Address tertentu hanya digunakan oleh Mac Address tertentu, bisa menggunakan **DHCP-Static**



- Dalam kondisi tertentu, IP Address yang diberikan oleh ISP yang akan dipasang pada router bukanlah IP Address statik, melainkan IP Address dinamis yang didapatkan melalui DHCP.
- Dalam kasus ini kita bisa menggunakan fitur **DHCP Client**



(LAB)DHCP Client

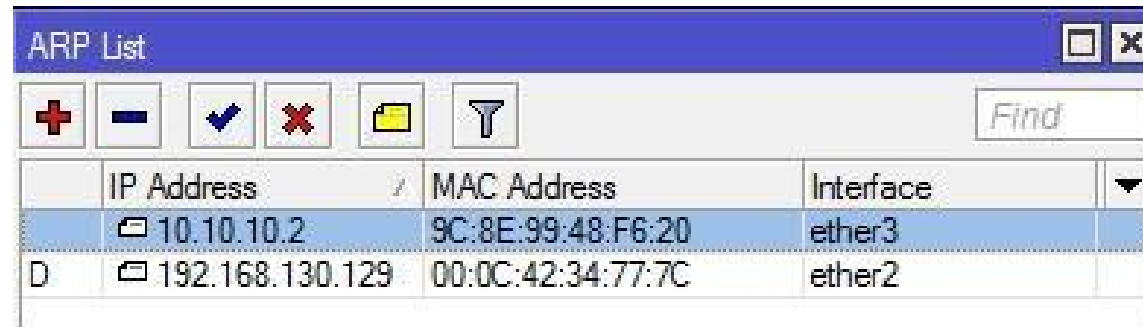
The screenshot displays the Mikrotik WinBox interface for configuring a DHCP Client. The left sidebar shows a tree view with 'IP' and 'DHCP Client' highlighted in red. The main window is titled 'DHCP Client' and contains a configuration form for the 'wlan1' interface. The form includes fields for 'Interface' (wlan1), 'Use Peer DNS' (checked), 'Use Peer NTP' (checked), 'DHCP Options' (hostname and clientid), 'Add Default Route' (yes), and 'Default Route Distance' (0). A table below the form shows the DHCP Client status for 'wlan1' as 'bound' with an expiration time of '2:37:01'. The status bar at the bottom indicates 'enabled' and 'Status: bound'. A terminal window in the background shows the command 'show ip dhcp client status wlan1' and its output.

Interface	Use Peer DNS	Add D...	IP Address	Expires After	Status
wlan1	<input checked="" type="checkbox"/>			2:37:01	bound

```
show ip dhcp client status wlan1
DHCP Client Status for wlan1:
  Enabled: yes
  Status: bound
  Expires: 2:37:01
  Mikrotik] >
```

- **Interface**
 - Pilihlah interface sesuai yang terkoneksi ke DHCP Server
- **Hostname (tidak harus diisi)**
 - Nama DHCP client yang akan dikenali oleh DHCP Server
- **Client ID (tidak harus diisi)**
 - Biasanya merupakan mac-address interface yang kita gunakan, apabila proses DHCP di server menggunakan sistem radius
- **Add default route**
 - Bila kita menginginkan default route kita mengarah sesuai dengan informasi DHCP
- **Use Peer DNS**
 - Bila kita hendak menggunakan DNS server sesuai dengan informasi DHCP
- **Use Peer NTP**
 - Bila kita hendak menggunakan informasi pengaturan waktu di router(NTP) sesuai dengan informasi dari DHCP
- **Default route distance**
 - Menentukan prioritas routing jika terdapat lebih dari satu DHCP Server yang digunakan. Routing akan melakukan distance yang lebih kecil

- Merupakan protokol penghubung antara **layer 2 data-link** dan **layer 3 network**.
- ARP Table di router merupakan daftar **host yang terhubung langsung** berisi informasi pasangan **mac address** dan **ip address**
- Di **IPv6** arp digantikan dengan NDP(Network Discovery Protocol)

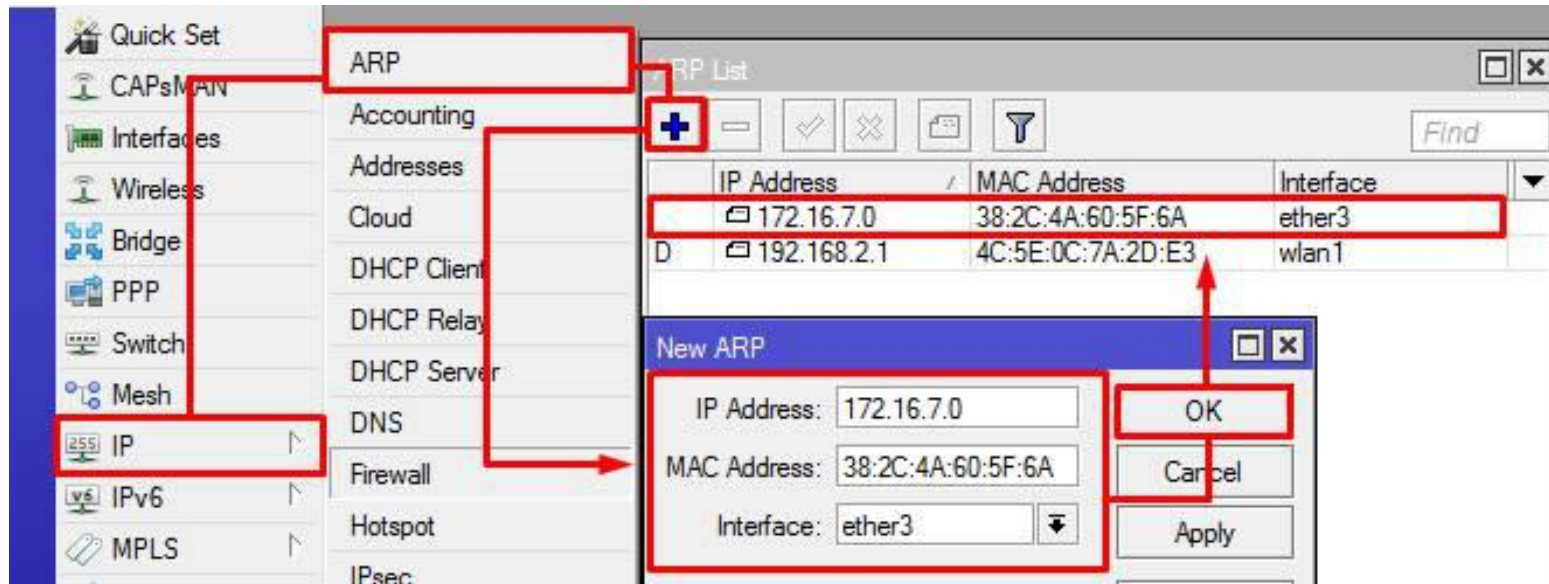


The screenshot shows a window titled "ARP List" with a toolbar containing icons for adding (+), deleting (-), checking (✓), unchecking (✗), refreshing (F5), and filtering (funnel). A search box labeled "Find" is also present. The table below contains the following data:

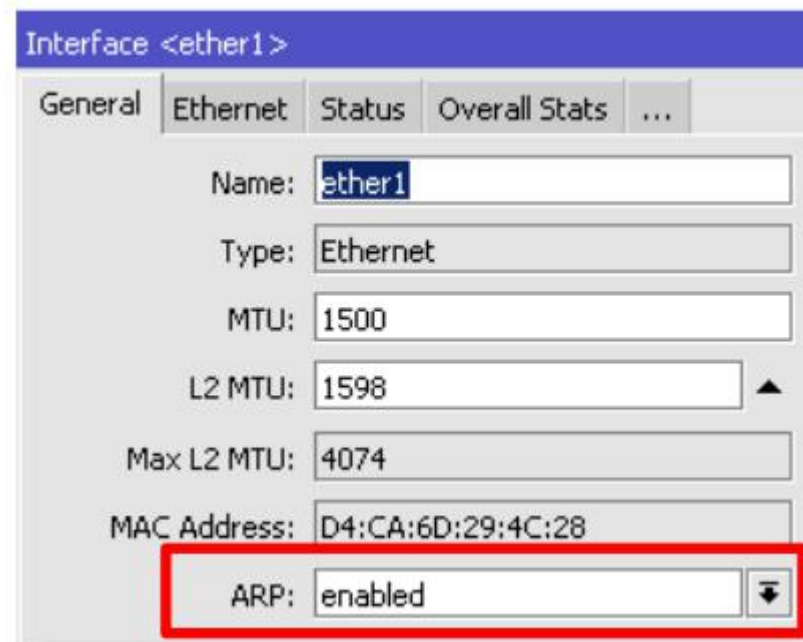
	IP Address	MAC Address	Interface
	10.10.10.2	9C:8E:99:48:F6:20	ether3
D	192.168.130.129	00:0C:42:34:77:7C	ether2

Address Resolution Protocol

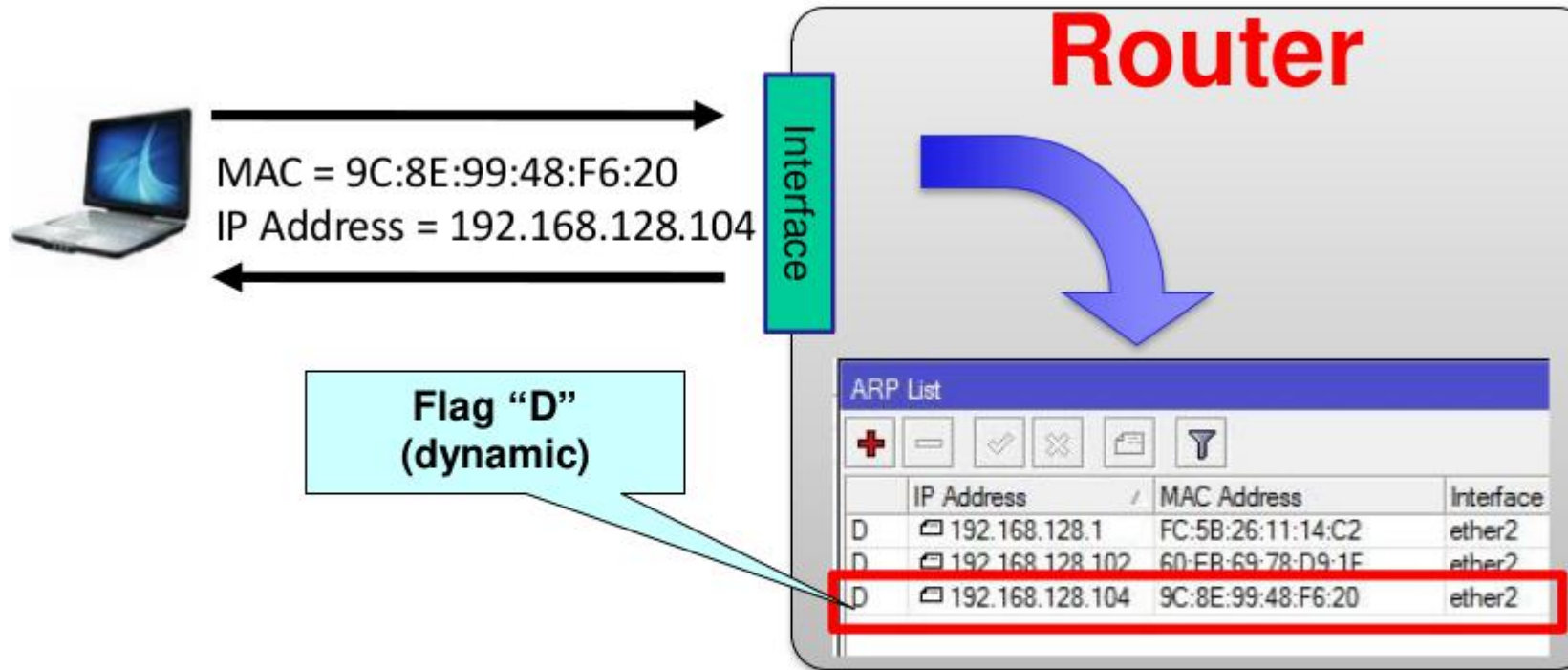
- Untuk memetakan OSI level 3 IP Address ke OSI level 2 MAC Address
- Digunakan dalam transport data antara host dengan router



- ARP protocol secara "default" aktif di setiap interface
- ARP = Enabled artinya menandakan Interface akan mengupdate tabel ARP secara otomatis

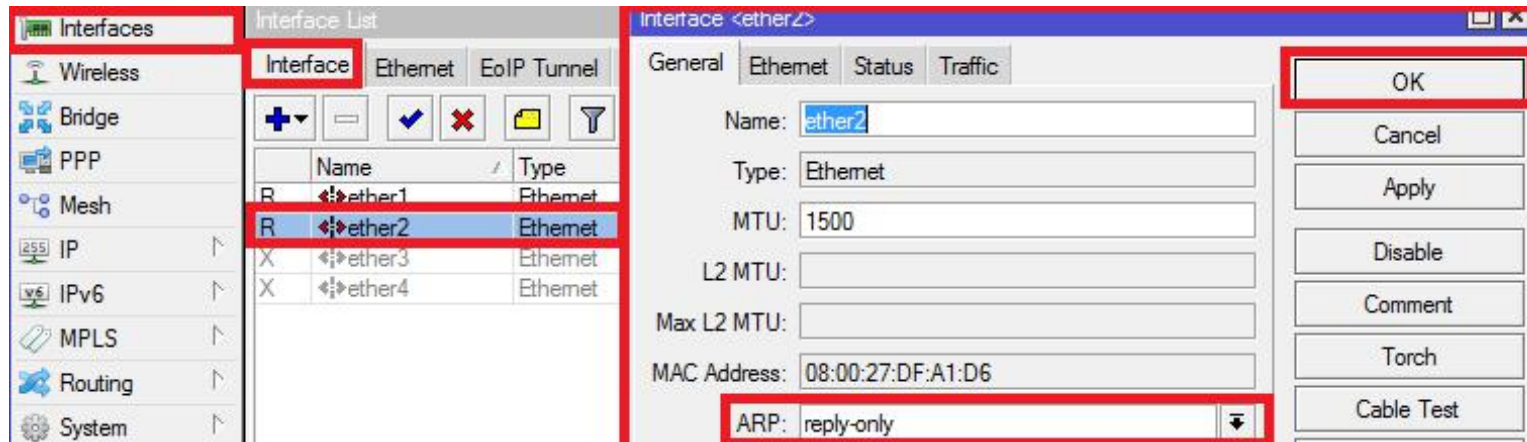


Interface ARP = Enabled

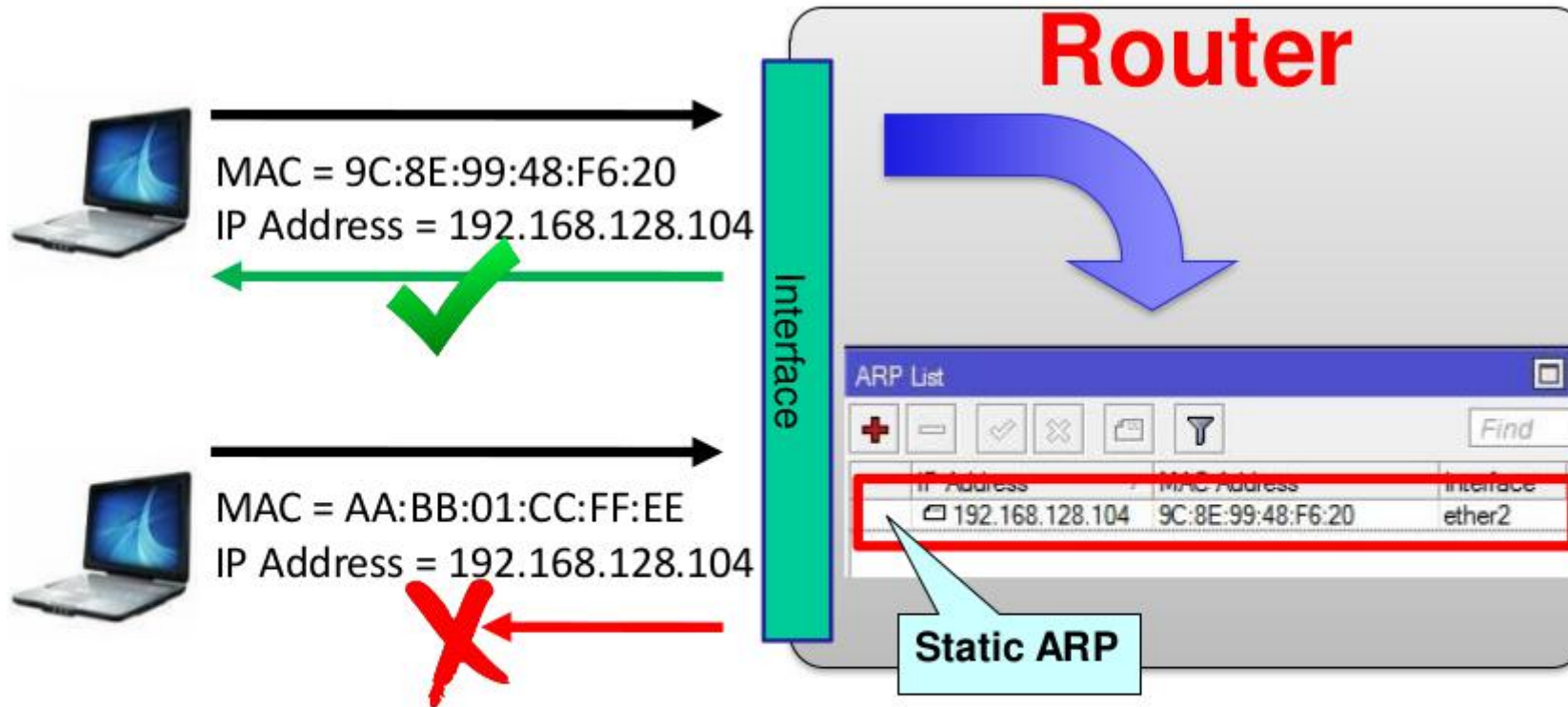


Interface melakukan update tabel ARP dengan kombinasi MAC Address dan IP Address host secara otomatis

- **ARP = reply-only** artinya menandakan ARP protocol pada interface tidak mengupdate data di ARP table secara otomatis



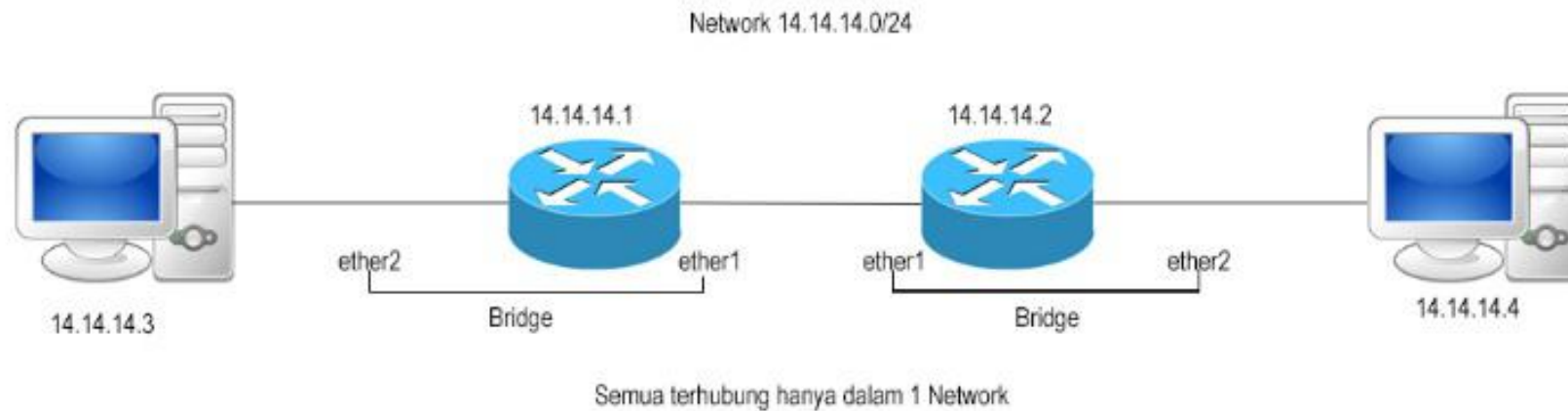
Interface ARP = reply-only



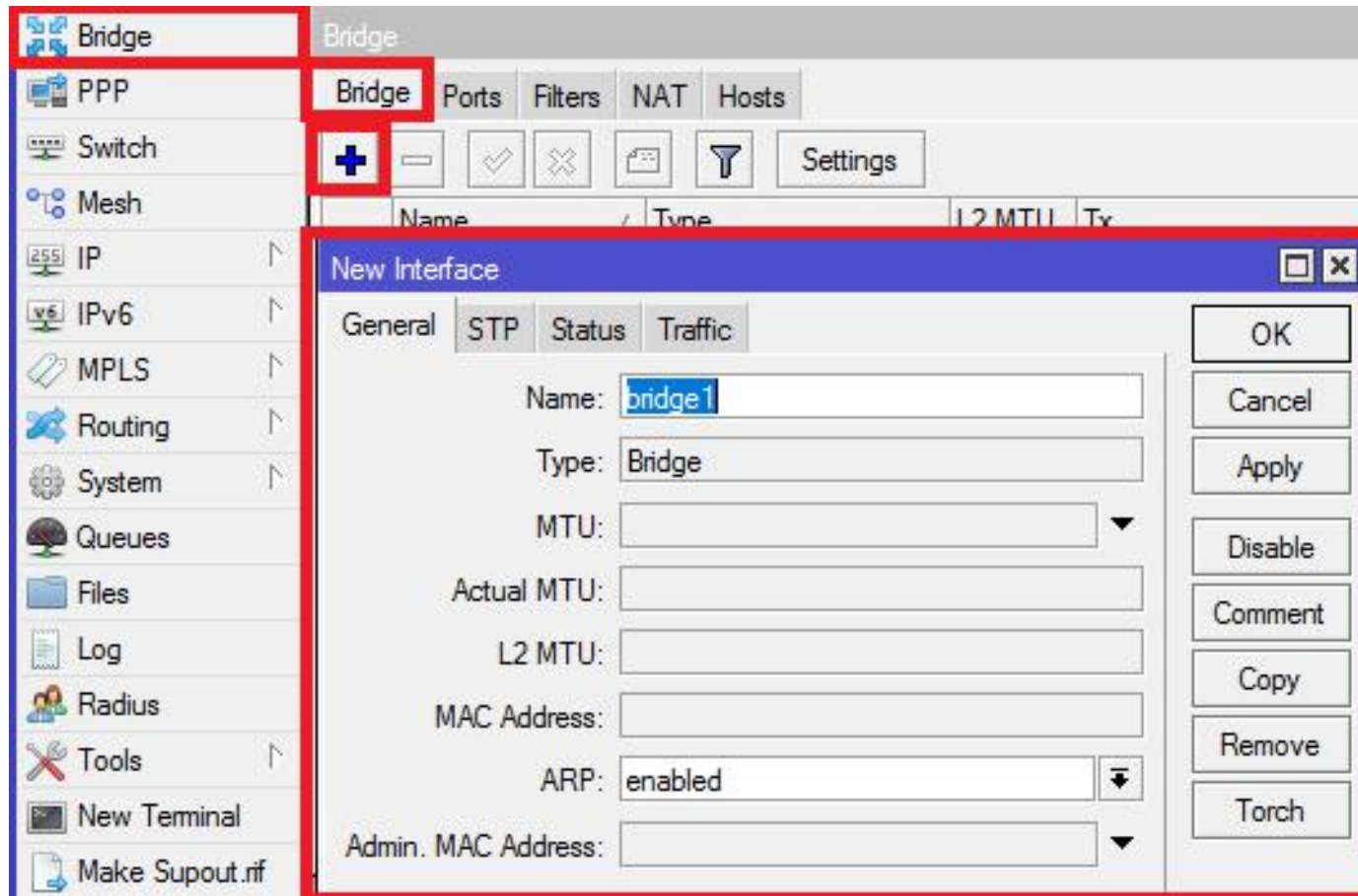
- Interface tidak melakukan update tabel ARP secara otomatis
- Interface hanya akan meresponse request dari host dengan kombinasi MAC Address dan IP Address yang sesuai dengan tabel ARP

- Menggabungkan **dua atau lebih interface** yang bertipe ethernet, atau sejenisnya, seolah-olah berada dalam **satu segmen network yang sama**
- Proses penggabungan ini terjadi pada layer data-link
- Mengaktifkan bridge pada dua buah interface akan menonaktifkan fungsi routing di antara kedua interface tersebut
- Mengemulasi mode **switch** secara software pada dua atau lebih interface

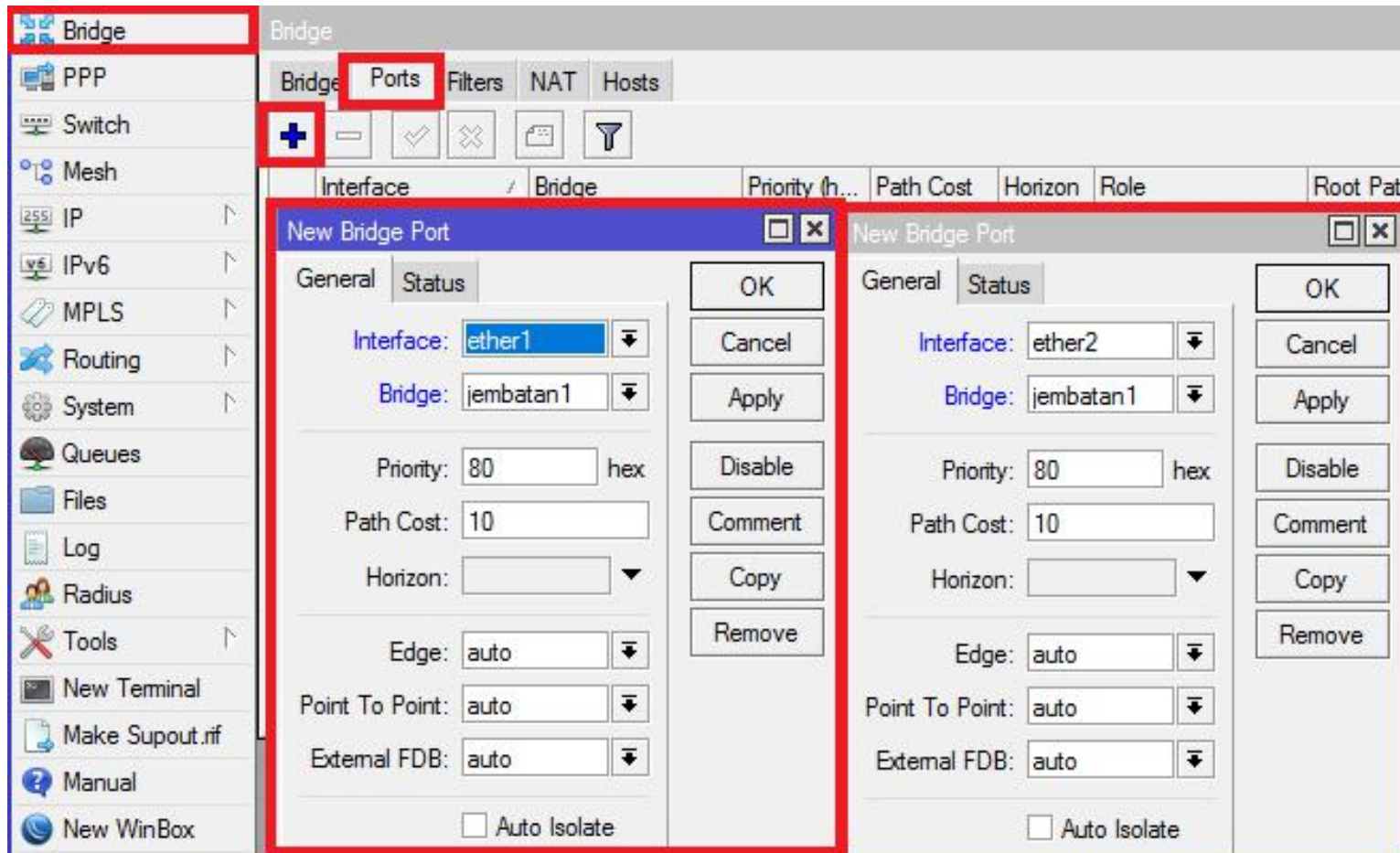
- Berpasangan dengan teman semeja, buatlah konfigurasi bridge berikut ini, sehingga dari PC A bisa melakukan ping ke PC B



- Membuat Interface bridge



- Memasukkan interface ethernet ke interface bridge



- Membuat Bridge

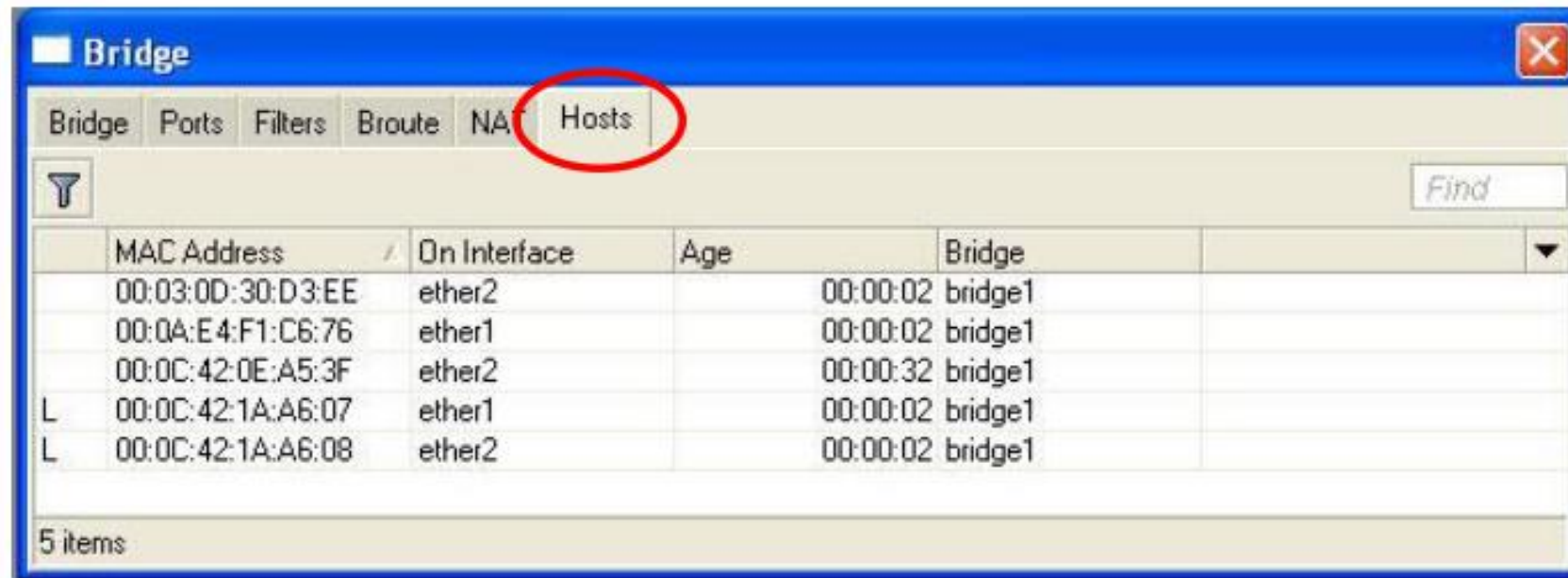
```
[admin@Mikrotik1] > interface bridge add name=jembatan1
[admin@Mikrotik1] > interface bridge print
Flags: X - disabled, R - running
0 R name="jembatan1" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled mac-address=00:00:00:00:00:00
  protocol-mode=rstp priority=0x8000 auto-mac=yes admin-mac=00:00:00:00:00:00 max-message-age=20s
  forward-delay=15s transmit-hold-count=6 ageing-time=5m
```

- Menambahkan Bridge Port

```
[admin@Mikrotik1] > interface bridge port add interface=ether1 bridge=jembatan1
[admin@Mikrotik1] > interface bridge port add interface=ether2 bridge=jembatan1
[admin@Mikrotik1] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic
```

#	INTERFACE	BRIDGE	PRIORITY	PATH-COST	HORIZON
0	ether1	jembatan1	0x80	10	none
1	ether2	jembatan1	0x80	10	none

- Untuk melihat MAC Address host yang terkoneksi dengan bridge tersebut



The screenshot shows a window titled "Bridge" with several tabs: "Bridge", "Ports", "Filters", "Broute", "NA", and "Hosts". The "Hosts" tab is selected and circled in red. Below the tabs is a search bar labeled "Find" and a filter icon. The main area contains a table with the following data:

	MAC Address	On Interface	Age	Bridge
	00:03:0D:30:D3:EE	ether2	00:00:02	bridge1
	00:0A:E4:F1:C6:76	ether1	00:00:02	bridge1
	00:0C:42:0E:A5:3F	ether2	00:00:32	bridge1
L	00:0C:42:1A:A6:07	ether1	00:00:02	bridge1
L	00:0C:42:1A:A6:08	ether2	00:00:02	bridge1

5 items

- Konsekuensi pengguna System Bridge
 - Sulit untuk mengatur trafik broadcast(misalnya akibat virus,dll)
 - Permasalahan pada satu segment akan membuat masalah di semua segment pada bridge yang sama
 - Sulit untuk membuat fail over system
 - Sulit untuk melihat kualitas link pada setiap segment
 - Beban trafik pada setiap perangkat yang dilalui akan berat, karena terjadi akumulasi trafik

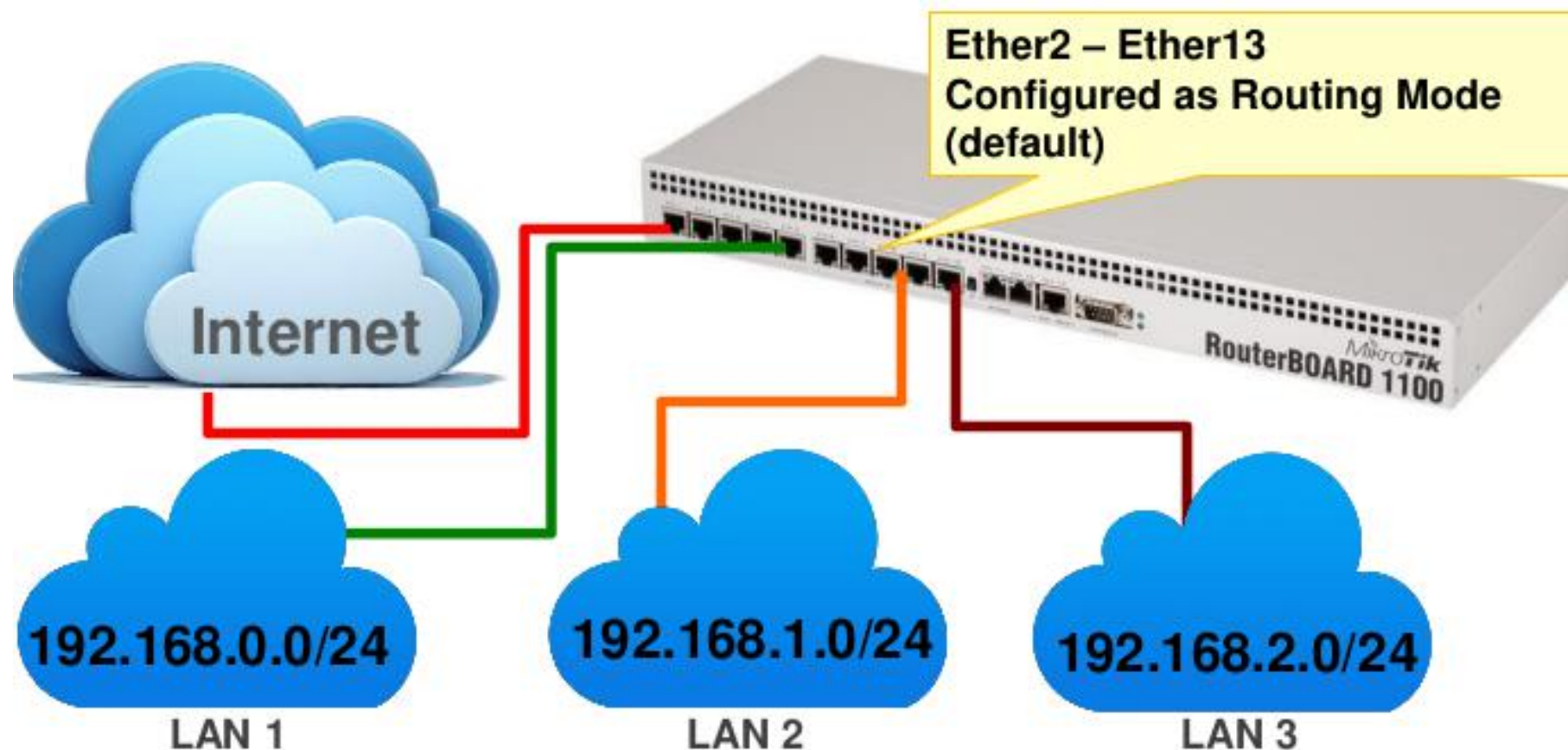
- Berikut ini jenis-jenis interface yang dapat dijadikan Bridge Port :
 - **Ethernet**
 - **VLAN**
 - Merupakan bagian dari ethernet atau wireless interface
 - Jangan melakukan bridge sebuah VLAN dengan interface induknya
 - **Wireless AP, WDS, dan custom station mode**
 - Note : mode "**station**" tidak bisa digunakan untuk bridge
 - **EoIP(Ethernet over IP)**
 - Tunnel proprietary Mikrotik RouterOS
 - **PPTP**
 - Selama bridge dilakukan baik di sisi server maupun client

- Kita tidak harus memasang IP Address pada sebuah bridge interface
- Jika kita menonaktifkan bridge, pada IP Address yang terpasang pada bridge akan menjadi invalid
- Kita tidak bisa membuat bridge dengan interface yang bukan bertipe ethernet seperti synchronous(serial), IPIP, PPPoE, dll.

- **Routing** artinya menentukan jalur yang akan dilewati oleh sebuah traffic
- Bekerja pada OSI Layer 3 (Network)
- Untuk menghubungkan network yang berbeda segment (subnet) memerlukan sebuah perangkat yang mampu melakukan proses routing yang disebut dengan Rrouter

Routing Example

- Routerboard yang berfungsi sebagai router akan menjembatani komunikasi antar network yang berbeda



- Memungkinkan kita melakukan pemantauan dan pengelolaan jaringan yang lebih baik
- Lebih aman (firewall filtering lebih mudah)
- Traffik broadcast(virus) hanya terkonsentrasi di local network seggmen yang sama
- Untuk network skala besar, Routing bisa diimplementasikan menggunakan Dynamic Routing Protocol (RIP/OSPF/BGP)

- **Dynamic Routes** artinya routing 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

The screenshot illustrates the process of adding a new route in Mikrotik WinBox. The 'Mesh' menu is open, and the 'Routes' option is selected. The 'Route List' window is open, and the 'New Route' dialog is displayed. The 'Dst. Address' field is set to 0.0.0.0/0, and the 'Type' is set to unicast.

Route List

Routes	Nexthops	Rules	VRF
AS	▶ 0.0.0.0/0	10.10.10.100 reachable wlan1	Distance: 1
DAC	▶ 10.10.10.0/24	reachable	0.10.10.00
DAC	▶ 192.168.30.0/24		

New Route

General | Attributes

Dst. Address: 0.0.0.0/0

Gateway: [Dropdown]

Check Gateway: [Dropdown]

Type: unicast

Distance: [Dropdown]

Scope: 30

Target Scope: 10

Routing Mark: [Dropdown]

Pref. Source: [Dropdown]

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

Type Routing

The screenshot shows a 'Route List' window with a table of routing entries. A yellow callout box points to the 'A' flag in the first entry, explaining that 'A' stands for Active and 'S' for Static. Another yellow callout box points to the 'A', 'D', and 'C' flags in the first entry, explaining that 'A' is Active, 'D' is Dynamic, and 'C' is Connected. Below the table, a text box explains that when an IP is installed on an interface, a DAC routing entry is automatically created with the preferred source IP. At the bottom, a terminal window shows the command 'ip route print' and its output, which lists various routing flags and their meanings.

	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	10.10.10.30
DAC	▶ 192.168.30.0/24	ether1 reachable	0	192.168.30.1

A: Active
S: Static

A: Active
D: Dynamic
C: Connected

Setiap memasang IP disebuah interface, secara otomatis akan dibuatkan routing DAC untuk networknya dengan prefered source IP tersebut

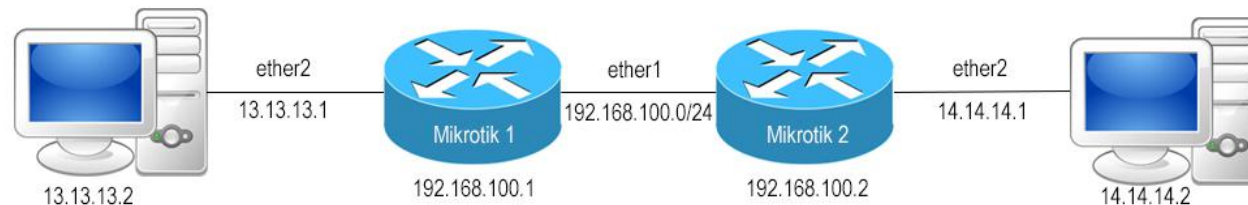
```
Terminal
[admin@30-Pujo-Dewobroto] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
```

Parameter Dasar Routing

- Destination
 - Destination address : 222.162.115.10
 - Network mask : 202.134.1.0/24
 - 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 (biasanya digunakan di **ppp** interface)
- Pref Source
 - source IP address dari paket yang akan meninggalkan router
- Distance
 - Beban untuk kalkulasi pemilihan routing

Konsep Dasar Routing

- IP Address Gateway harus merupakan IP Address dari router lawannya yang subnetnya sama dengan salah satu IP Address yang terpasang pada router kita (connect directly)
- Pada interface yang menghubungkan router 1 dan 2, pada masing-masing router terdapat lebih dari 1 buah IP Address
- Default gateway pada router 2 adalah router 1
- IP address yang menjadi default gateway router 2 adalah 192.168.100.1, karena IP Address tersebut berada dalam subnet yang sama dengan salah satu IP Address pada router B (192.168.100.2/24)
- Setting static route default :
 - Dst-address=0.0.0.0/0 gateway192.168.100.1



(LAB)Static Route

The screenshot displays the Mikrotik WinBox interface for configuring static routes. The left sidebar shows the 'IP' menu expanded, with 'Routes' selected. The main window is divided into three panes:

- Route List:** Shows a table with columns for 'Dst. Address', 'Gateway', 'Distance', 'Routing Mark', and 'Pref. Source'. A '+' icon is visible in the top-left corner of this pane.
- New Route Router2:** A configuration dialog for Router2 with the following fields:
 - Dst. Address: 13.13.13.0/24
 - Gateway: 192.168.100.1
 - Type: unicast
 - Distance: (empty)
 - Scope: 30
 - Target Scope: 10
 - Routing Mark: (empty)
 - Pref. Source: 0.0.0.0
- New Route Router1:** A configuration dialog for Router1 with the following fields:
 - Dst. Address: 14.14.14.0/24
 - Gateway: 192.168.100.2
 - Type: unicast
 - Distance: (empty)
 - Scope: 30
 - Target Scope: 10
 - Routing Mark: (empty)
 - Pref. Source: (empty)

Buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove' are visible on the right side of the configuration panes.

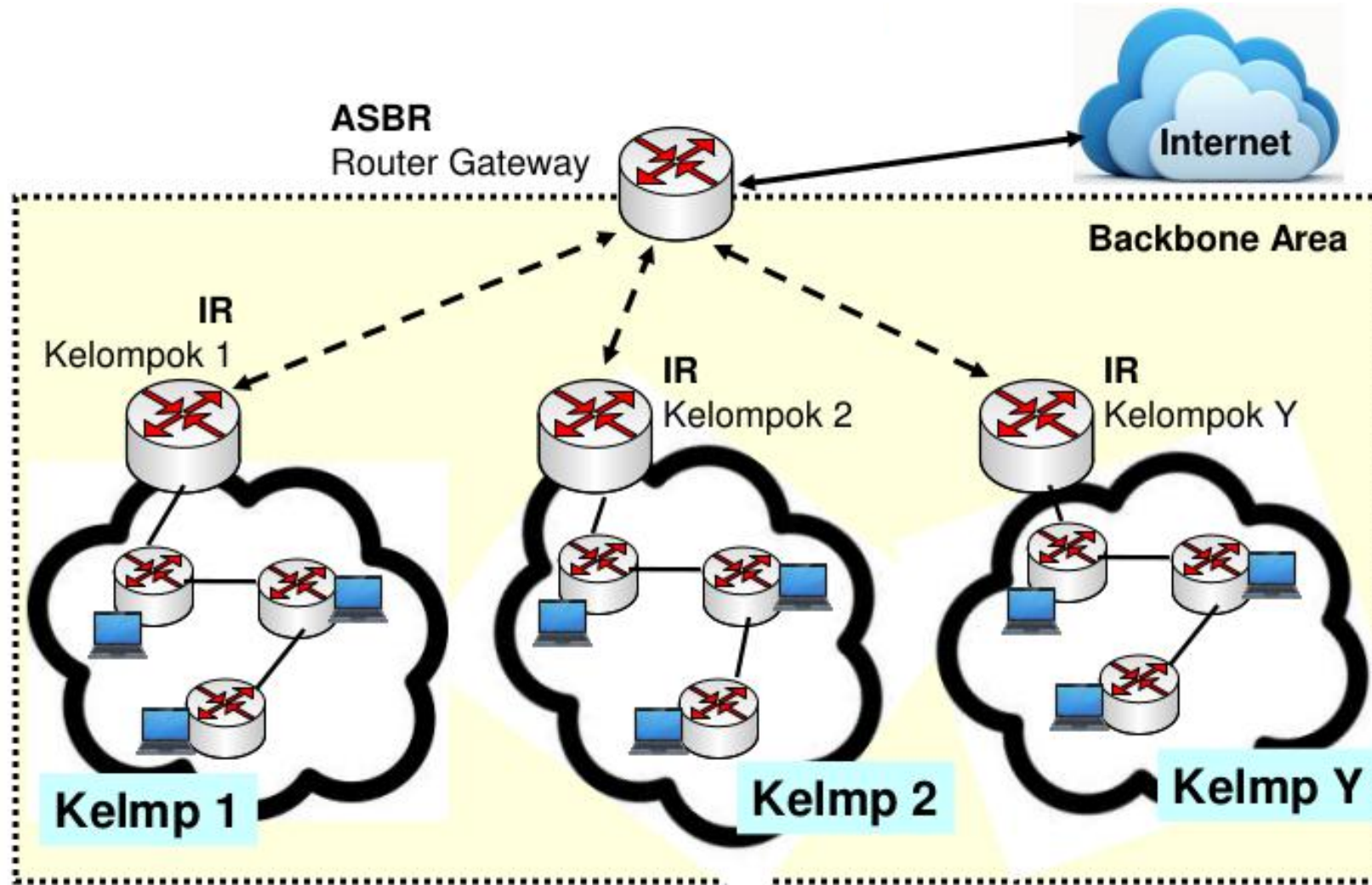
Dasar Pemilihan Routing

- Untuk pemilihan routing, router akan memilih berdasarkan :
 - Rule routing yang paling spesifik tujuannya
 - Contoh : destination 192.168.10.1/28 lebih spesifik dibanding 192.168.100.1/25
 - Distance
 - Router akan memilih distance routing protokol nya paling kecil
 - Round robin

- Karena sebuah jaringan memiliki skala yang berbeda satu sama lain, maka sangat memungkinkan jika jaringan tersebut berkembang menjadi 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

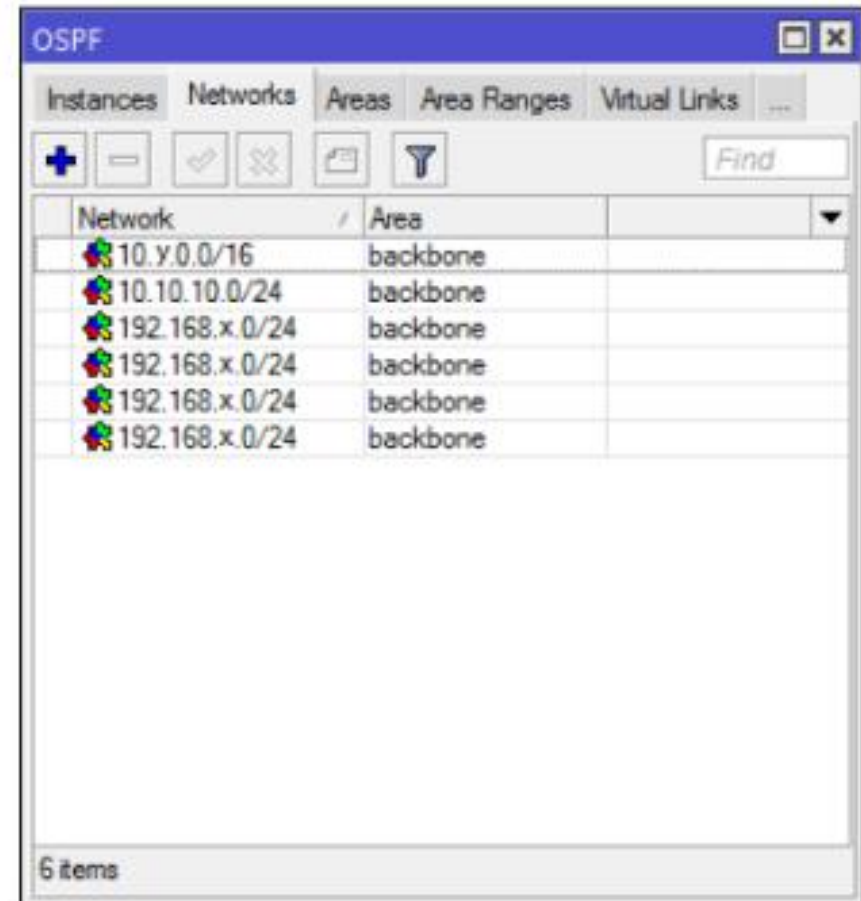
- **OSPF** merupakan sebuah routing protokol yang dapat mendistribusikan informasi routing secara otomatis
- OSPF juga merupakan routing protokol yang menggunakan konsep hirarki routing, dengan kata lain OSPF juga mampu membagi-bagi jaringan menjadi beberapa tingkatan. Tingkatan-tingkatan ini diwujudkan dengan menggunakan sistem pengelompokan yaitu **area**

(LAB) Topologi OSPF



(LAB)Konfigurasi OSPF

- Tambahkan network yang akan saling bertukar informasi routing :
 - Network antar IR
 - Network antar router
 - Network Client dibawah router



- **Band 2.4Ghz**

- 802.11 b : Wireless Lan yang menggunakan Frequency 2.4Ghz berkecepatan transfer data **11Mbps**
- 802.11 b/g : Wireless Lan yang menggunakan Frequency 2.4Ghz berkecepatan transfer data **54Mbps**
- 802.11 b/g/n : Wireless Lan yang menggunakan Frequency 2.4Ghz berkecepatan transfer data **300Mbps**

- **Band 5Ghz**

- 802.11 a/g : Wireless Lan yang menggunakan Frequency 5Ghz berkecepatan transfer data **54Mbps**
- 802.11 a/g/n : Wireless Lan yang menggunakan Frequency 5Ghz berkecepatan transfer data **300Mbps**

- Wireless Menu :
 - **Interface** > Daftar Interface wireless yang terpasang
 - **Access List** > Security MAC Address Client (AP Mode)
 - **Registration** > Daftar Wireless yang terkoneksi
 - **Connect List** > Security MAC Address AP (Station Mode)
 - **Security Profile** > Konfigurasi Wireless Security (WPA/WEPA)



Wireless Tables

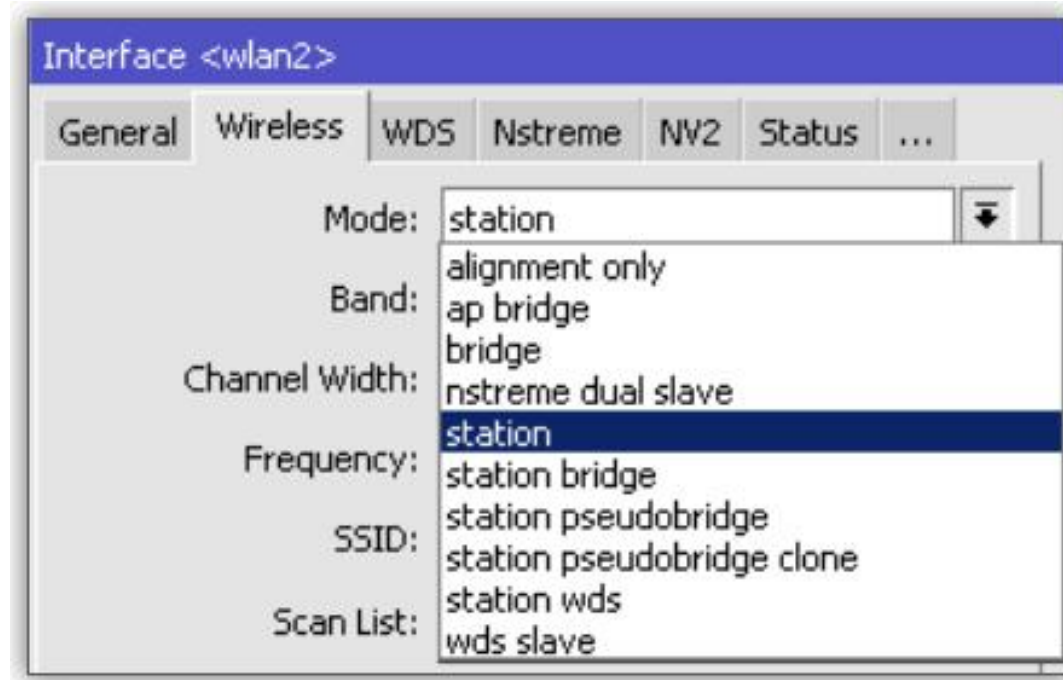
Interfaces | Nstreme Dual | Access List | Registration | Connect List | Security Profiles | Channels

+ - ✓ ✗ 📁 📏 CAP Scanner Freq. Usage Alignment Wireless Sniffer Wireless Snooper

Name	Type	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx
wlan1	Wireless (Atheros AR9...	0 bps	0 bps	0	0	0 bps	0 bps

Wireless Mode List

- Wireless Mode :
 - alignment-only
 - ap-bridge
 - bridge
 - nstreme-dual-slave
 - station
 - station-wds
 - wds-slave
 - station-pseudobridge
 - station-pseudobridge-clone
 - station-bridge



- alignment-only : Digunakan untuk melakukan pointing dengan bantuan "**Beeper**" pada Routerboard.
- ap-bridge : Mode wireless sebagai Access Point untuk topologi **Point-to-Multipoint**
- bridge : Mode wireless sebagai Access Point untuk topologi **Point-to-Point** (hanya bisa menerima satu client)
- nstreme-dualslave : Mode wireless untuk mengaktifkan topologi Nstreme-dual (Wireless Full Duplex)
- station : Mode Wireless sebagai Client untuk topologi **Point-to-Point** dan juga **Point-to-Multipoint**

- station-wds : Mode wireless sebagai client tetapi mengaktifkan protocol WDS (Digunakan untuk wireless WDS client)
- wds-slave : Mode wireless sebagai Access Point dan juga mengaktifkan protocol WDS (Digunakan untuk wireless WDS repeater)
- station-pseudobridge : Mode wireless sebagai client yang bisa mengaktifkan bridge pada "**station**" tanpa harus menggunakan protocol WDS
- station-pseudobridge-clone : Mode wireless sama seperti **station-pseudobridge** yang dilengkapi dengan fungsi cloning mac-address dari interface ethernet
- station-bridge : Mode wireless client untuk bridge network sesama perangkat MikroTik

AP Side

- Mikrotik Minimum Licence Level 3
- Set mode, ssid, band, frequency
- mode=bridge
 - **Hanya menerima 1 station**

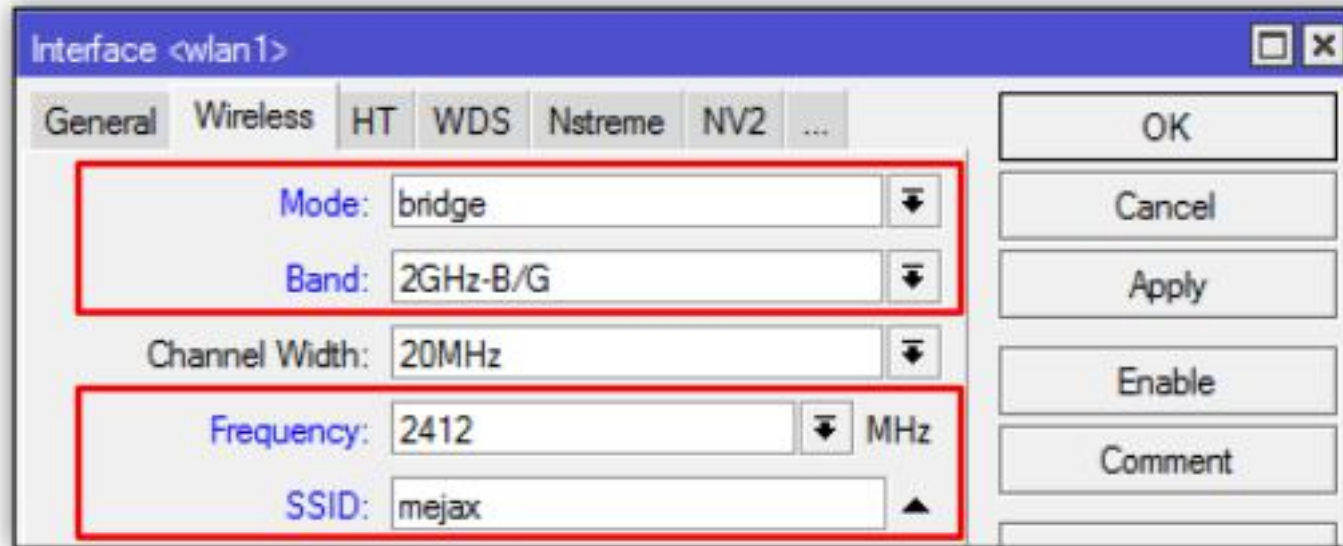


Client Side

- Mikrotik Minimum Licence Level 3
 - Set mode, ssid, band, scan-list
 - mode=station
- Make sure frequency is in scan-list

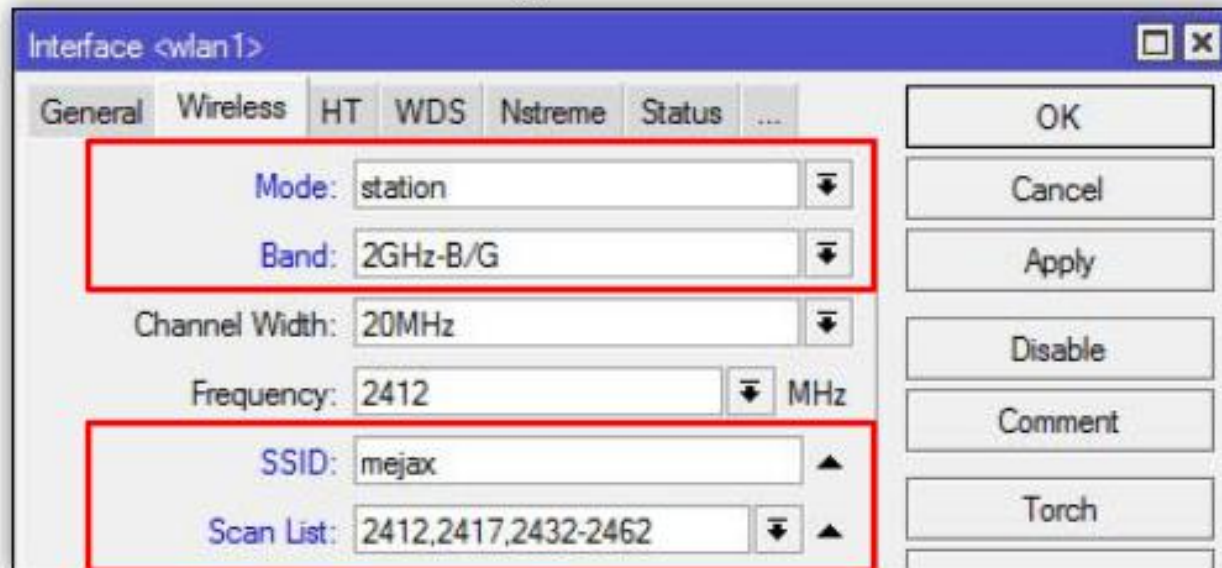
(LAB)Point to Point AP Side

- Konfigurasi :
 - Set **mode, ssid, band, dan frequency**
 - mode = **bridge**
 - Hanya bisa terkoneksi dengan satu station (1 client)



(LAB) Point to Point Client Side

- Konfigurasi :
 - Set **mode**, **ssid**, **band**, dan **scan-list**
 - mode **station**
 - Pastikan frequency yang dipilih oleh
 - AP masuk dalam range scan-list



Monitoring Wireless Interface

The screenshot shows the Mikrotik WinBox interface. The 'Registration' tab is highlighted with a red box. The 'AP Client <4E:5E:0C:27:D8:54>' window is open, displaying the following details:

- Radio Name: 4C5E0C27D853
- MAC Address: 4E:5E:0C:27:D8:54
- Interface: wlan1
- Uptime: 00:09:41
- Distance: 1 km
- RouterOS Version: 6.11

The 'Signal' tab in the AP Client window shows the following signal strength details:

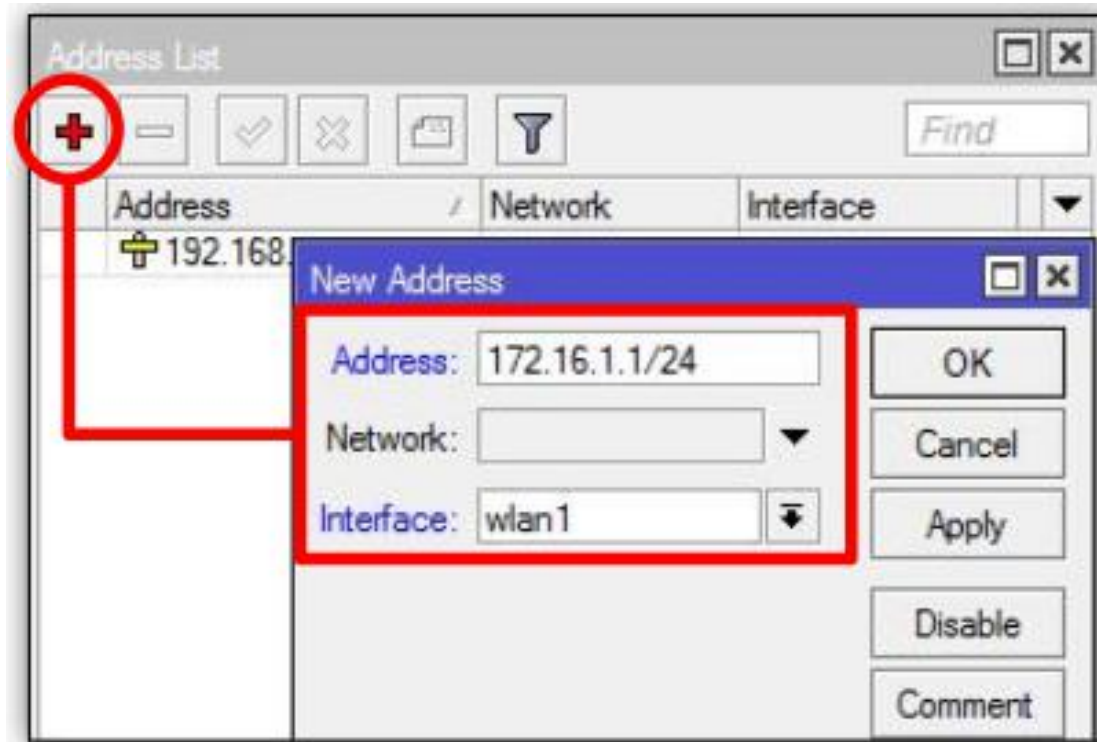
- Last Activity: 0.010 s
- Tx/Rx Signal Strength: -42/-26 dBm
- Tx/Rx Signal Strength Ch0: -45/-26 dBm
- Tx/Rx Signal Strength Ch1: -46 dBm
- Tx/Rx Signal Strength Ch2: -74 dBm
- Signal To Noise: 81 dB
- Tx/Rx CCG: 65/60 %
- P Throughput: 32391 kbps

The 'Signal Strengths' table shows the following data:

Rate	Strength	Last Measure
HT20-7	-34	00:00:00
5.5Mbps	-31	00:05:20
54Mbps	-31	00:02:27
2Mbps	-30	00:05:32
11Mbps	-29	00:05:09
48Mbps	-29	00:03:14
HT20-6	-29	00:02:06
6Mbps	-28	00:06:14
9Mbps	-28	00:05:19
18Mbps	-28	00:04:36
36Mbps	-28	00:03:50

(LAB)Point to Point Test

- Tambahkan IP Address di interface **Wlan1**
- Test koneksi wireless kedua router dengan tool Ping
- Setelah test ping berhasil maka wireless Point-to-Point sudah selesai



- Country : membatasi channel yang bisa digunakan sesuai dengan regulasi sebuah Negara
- Jika di set "*no_country_set*" maka akan menggunakan standard channel FCC compliant



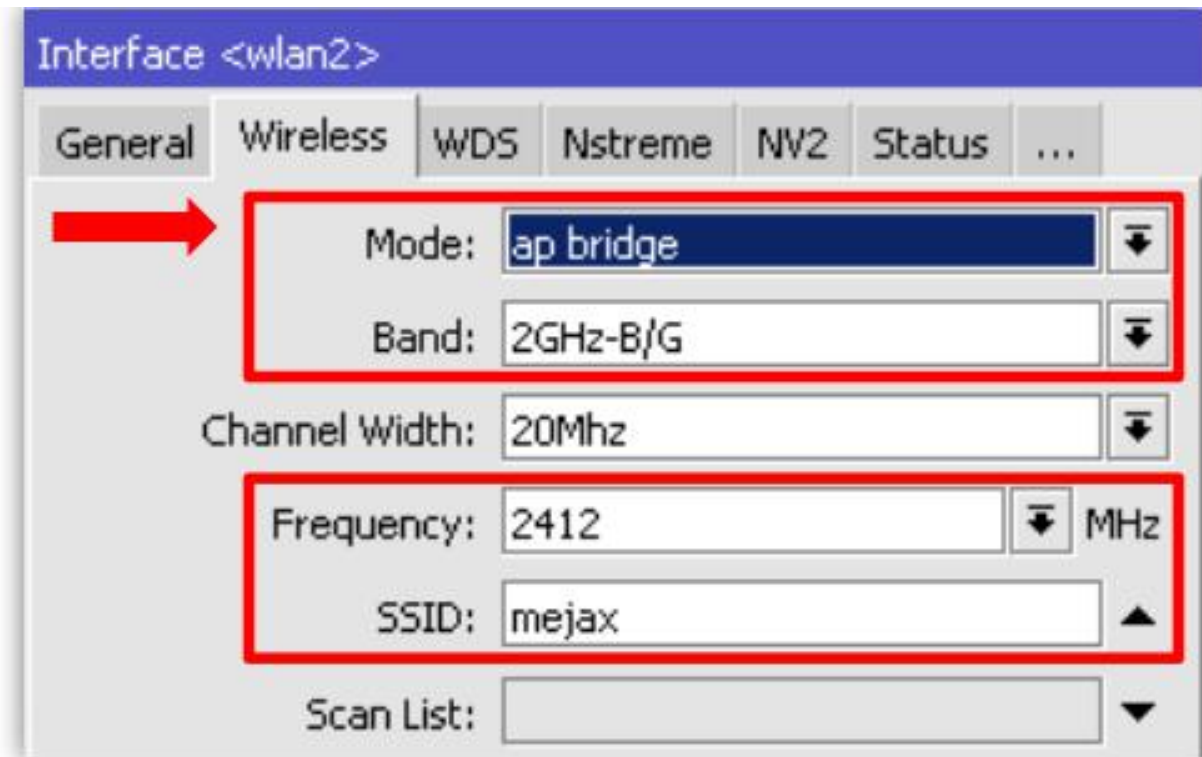
(LAB)Point to Multipoint

- MikroTik difungsikan sebagai Access Point. Digunakan standard 802.11 b atau 802.11 b/g sehingga semua client (berbagai vendor dan berbagai tipe) dapat terkoneksi.



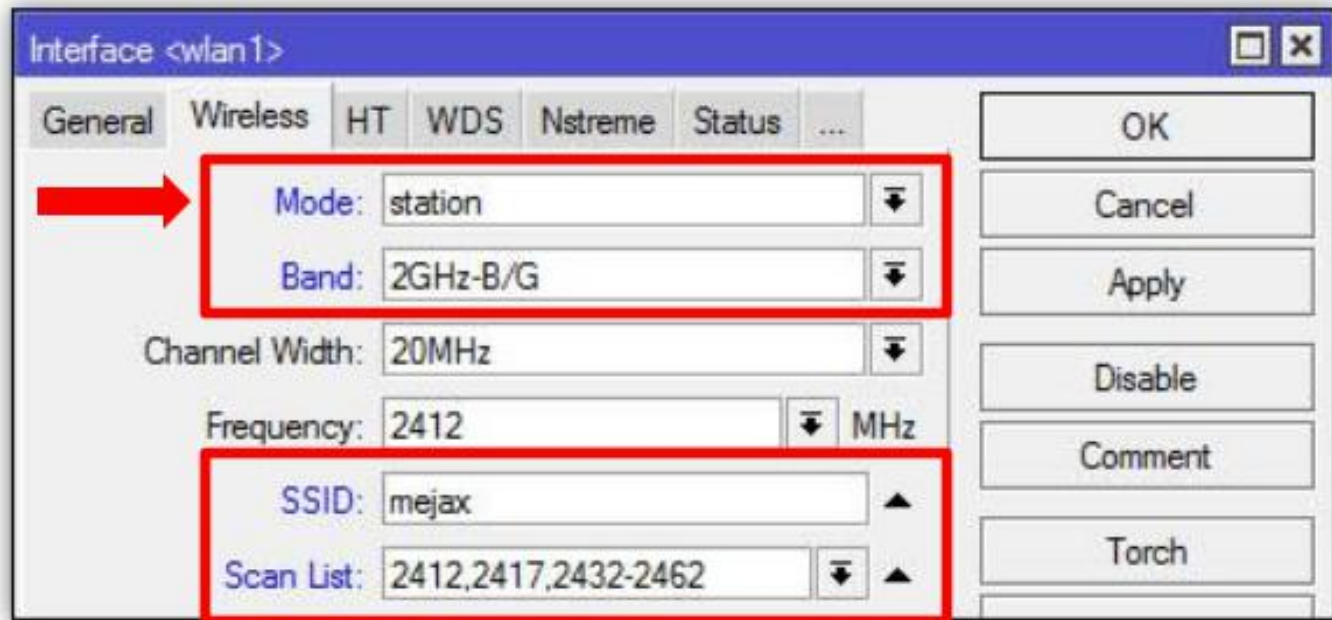
(LAB) Point to Multipoint AP Side

- Membutuhkan minimal lisensi level 4
- Set mode=ap-bridge
- Konfigurasi lainnya sama dengan konfigurasi point-to-multipoint



(LAB) Point to Multipoint Station Side

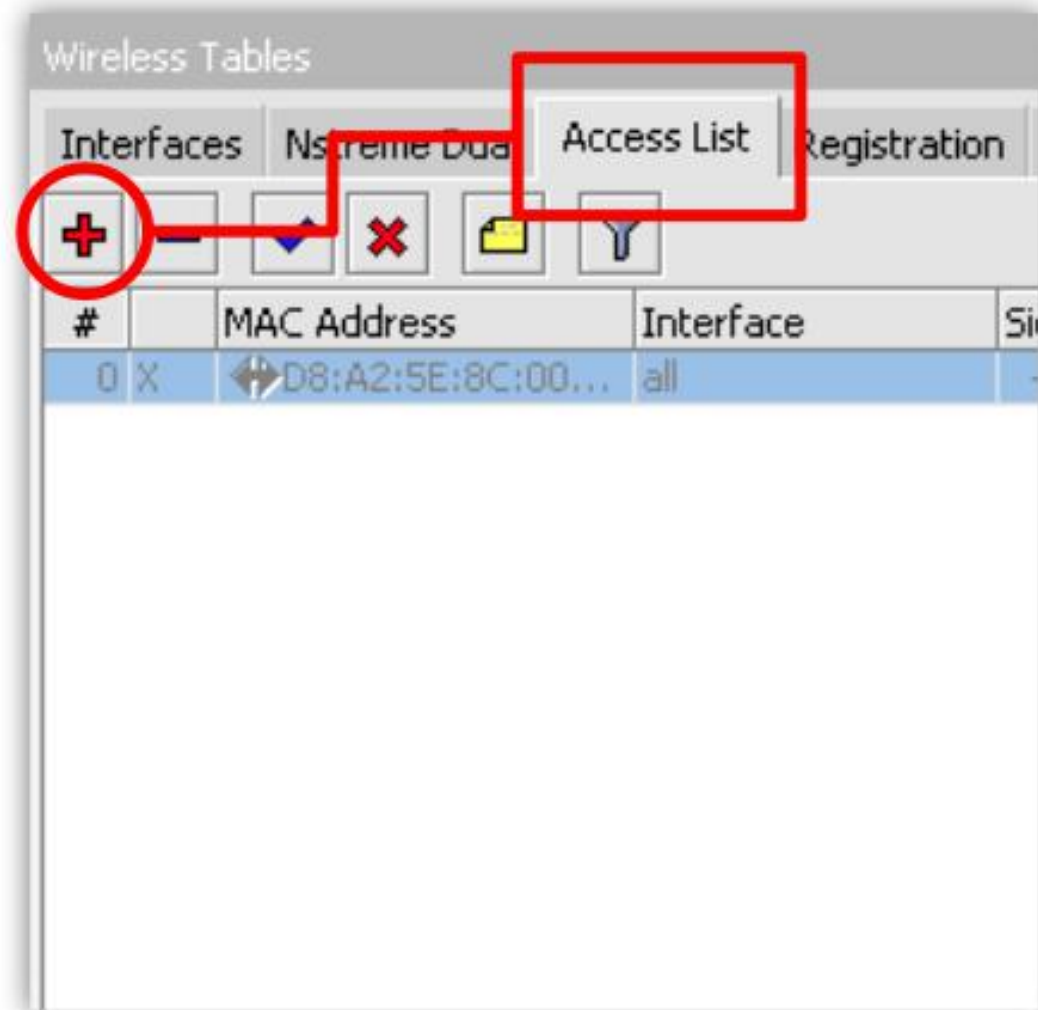
- Dapat menggunakan lisensi level 3
- Set mode, ssid, band, scan-list
- Set mode=station



Wireless Access Management

- **Access list** : adalah filter autentikasi sebuah AP (AP Side) terhadap client yang terkoneksi
- **Connect List** : adalah filter autentikasi sebuah wireless station (Client Side) terhadap AP mana yang ingin terkoneksi
- Rule autentikasi atau filter autentikasi dibaca secara terurut dari atas ke bawah seperti halnya sebuah filter firewall sampai request autentikasi mencapai kecocokan
- Sangat dimungkiinkan untuk memasang beberapa filter untuk mac-address yang sama dan juga satu rule untuk semua mac-address
- sebuah rule filter mac-address bisa diterapkan pada sebuah interface wireless saja atau bisa juga untuk semua interface
- Jika tidak ada rule yang sesuai maka akan digunakan default policy (**default authentication & default forward**) dari wireless interface tersebut

- Kita dapat melakukan pengaturan untuk setiap client menggunakan :
 - Access list :
 - MAC Address
 - Signal Strength
 - Time



Client Management

The screenshot shows the configuration page for an AP Access Rule with the MAC address <D8:A2:5E:8C:00:B9>. The interface includes several fields and options:

- MAC Address:** D8:A2:5E:8C:00:B9 (highlighted with a red box)
- Interface:** all
- Signal Strength Range:** -120..120
- AP Tx Limit:** (empty field)
- AP Rx Limit:** (empty field)
- Authentication:** (checked)
- Forwarding:** (checked)
- WPA State Key:** none
- WPA Red Key:** (empty field)
- WPA Management Protection Key:** (empty field)
- Time:** 00:00:00 - 1d 00:00:00 (highlighted with a red box)
- Days:** sun, mon, tue, wed, thu, fri, sat

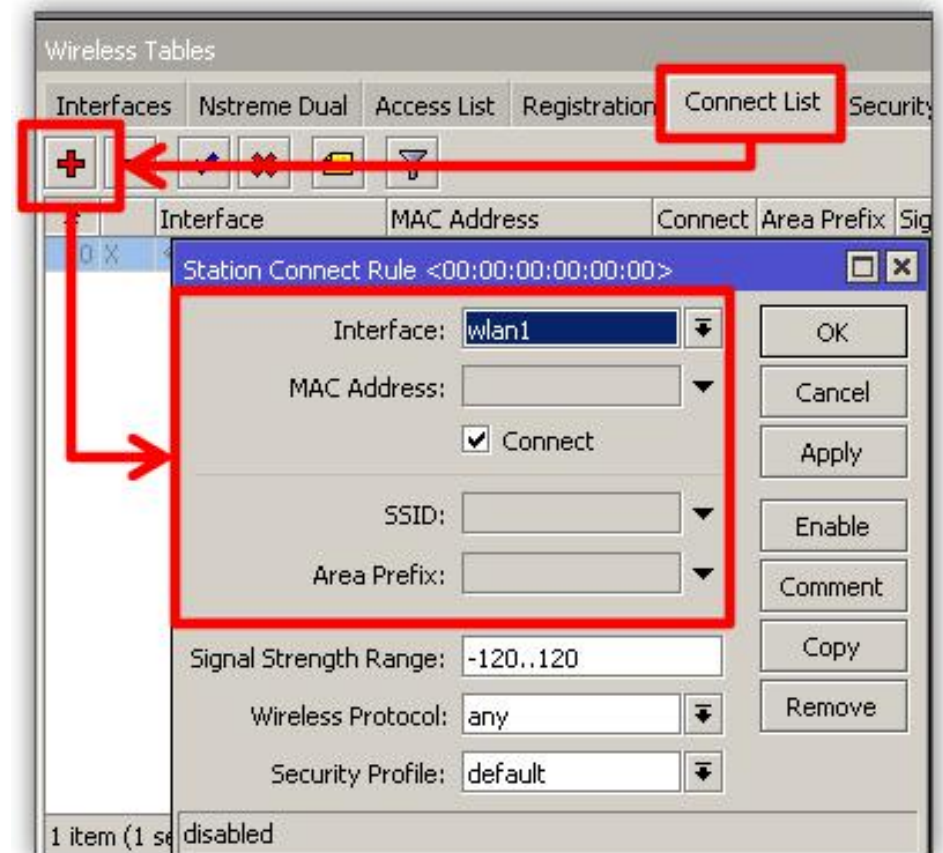
Three callout boxes provide additional information:

- Klasifikasi mac-address dari client** (Classification of mac-address from client) - points to the MAC Address field.
- Option policy boleh terkoneksi atau tidak** (Option policy can be connected or not) - points to the Authentication and Forwarding checkboxes.
- Option waktu untuk mengaktifkan rule access list** (Option time for activating rule access list) - points to the Time and Days fields.

- Kita dapat melakukan pengaturan untuk AP yang akan kita hubungkan menggunakan

- Connect List :

- MAC Address
- SSID
- Area



- Karena sifat dari wireless yang "open access" maka sebuah Access Point akan rentan terhadap serangan dari pihak yang tidak bertanggung jawab
- Sudah saatnya untuk mengimplementasikan Wireless Security untuk menjaga AP tersebut dari berbagai serangan



Wireless Tables

Interfaces | Nstreme Dual | Access List | Registration | Connect List | **Security Profiles**

+ [Filter Icon]

Name	Mode	Authenticatio...	Unicast Ciphers	Group Ciphers	WPA Pre-Shared ...	WPA2 Pre-Share...
default	none				*****	*****
profile1	dy			tkip aes ccm	*****	*****
profile2	dy			tkip aes ccm	*****	*****

Tambahkan Security Profile

(LAB) Create Wireless Security

The screenshot shows the configuration for a Security Profile named 'profile1'. The 'General' tab is active, showing the 'Name' as 'profile1' and 'Mode' as 'dynamic keys'. Under 'Authentication Types', 'WPA PSK' and 'WPA2 PSK' are selected. Under 'Unicast Ciphers', 'aes ccm' is selected. Under 'Group Ciphers', 'tkip' and 'aes ccm' are selected. The 'WPA Pre-Shared Key' is set to 'mikrotik1' and the 'WPA2 Pre-Shared Key' is set to 'mikrotik2'. Two callout boxes provide instructions: 'Tentukan metode securitynya' (Determine the security method) points to the 'WPA PSK' and 'WPA2 PSK' checkboxes, and 'Tentukan passwordnya' (Determine the password) points to the 'WPA Pre-Shared Key' and 'WPA2 Pre-Shared Key' text boxes.

Security Profile <profile1 >

General | RADIUS | EAP | Static Keys

Name: profile1

Mode: dynamic keys

- Authentication Types

- WPA PSK
- WPA EAP
- WPA2 PSK
- WPA2 EAP

- Unicast Ciphers

- aes ccm

- Group Ciphers

- tkip
- aes ccm

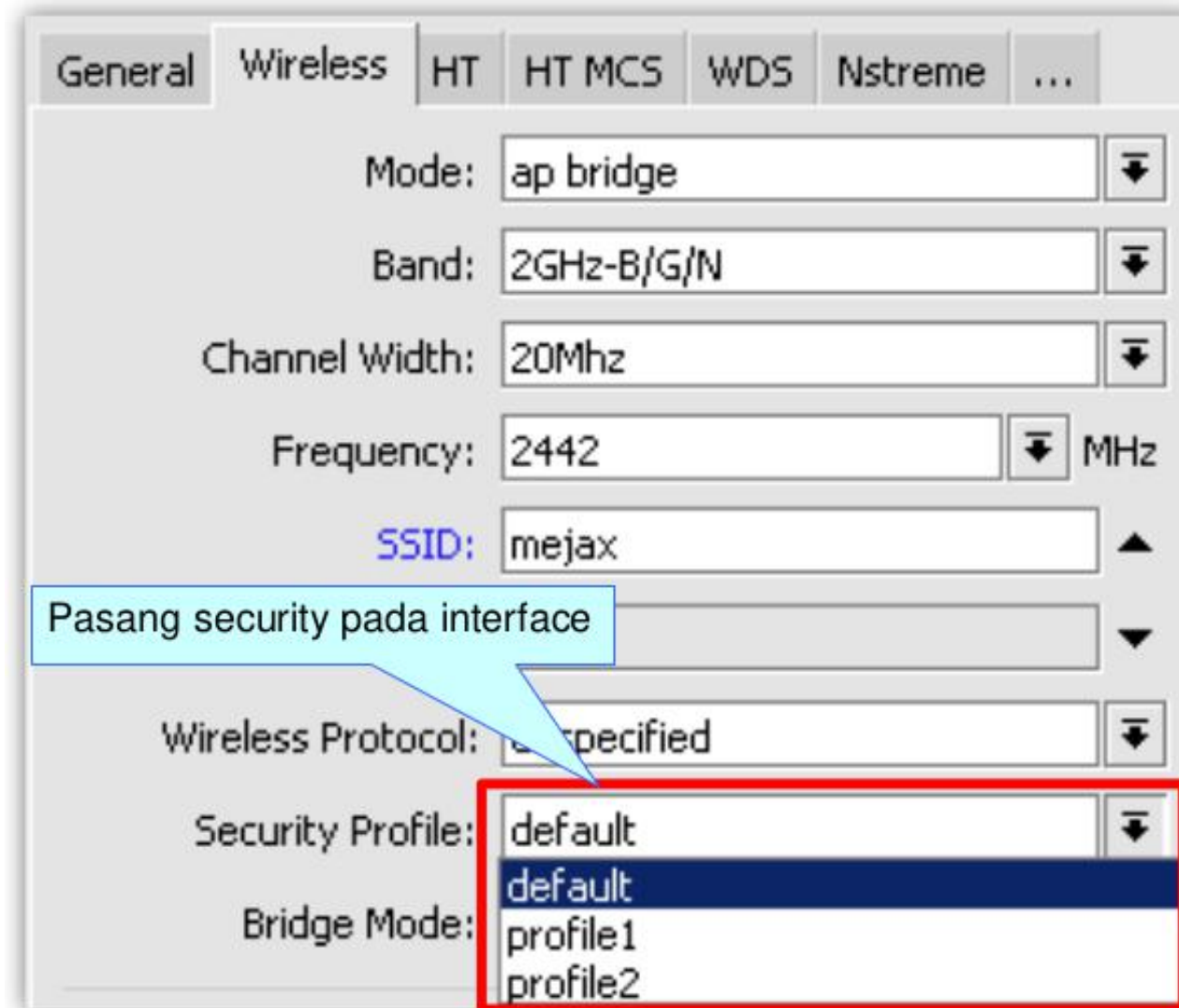
WPA Pre-Shared Key: mikrotik1

WPA2 Pre-Shared Key: mikrotik2

Tentukan metode securitynya

Tentukan passwordnya

(LAB) Create Wireless Security



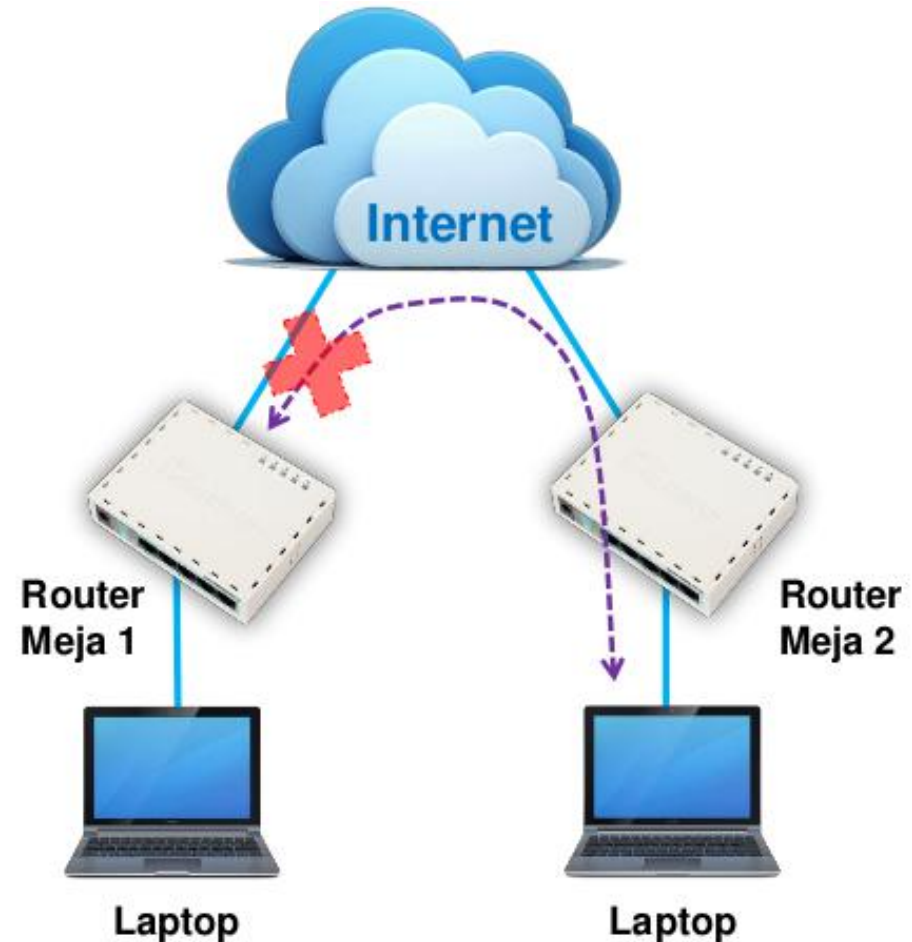
- Service yang melakukan management paket data yang menuju/melewati router berdasarkan rule yang didefinisikan oleh admin jaringan
- Bertindak sebagai pengaman
- Contoh real, perangkat firewall di antara Internet dan LAN



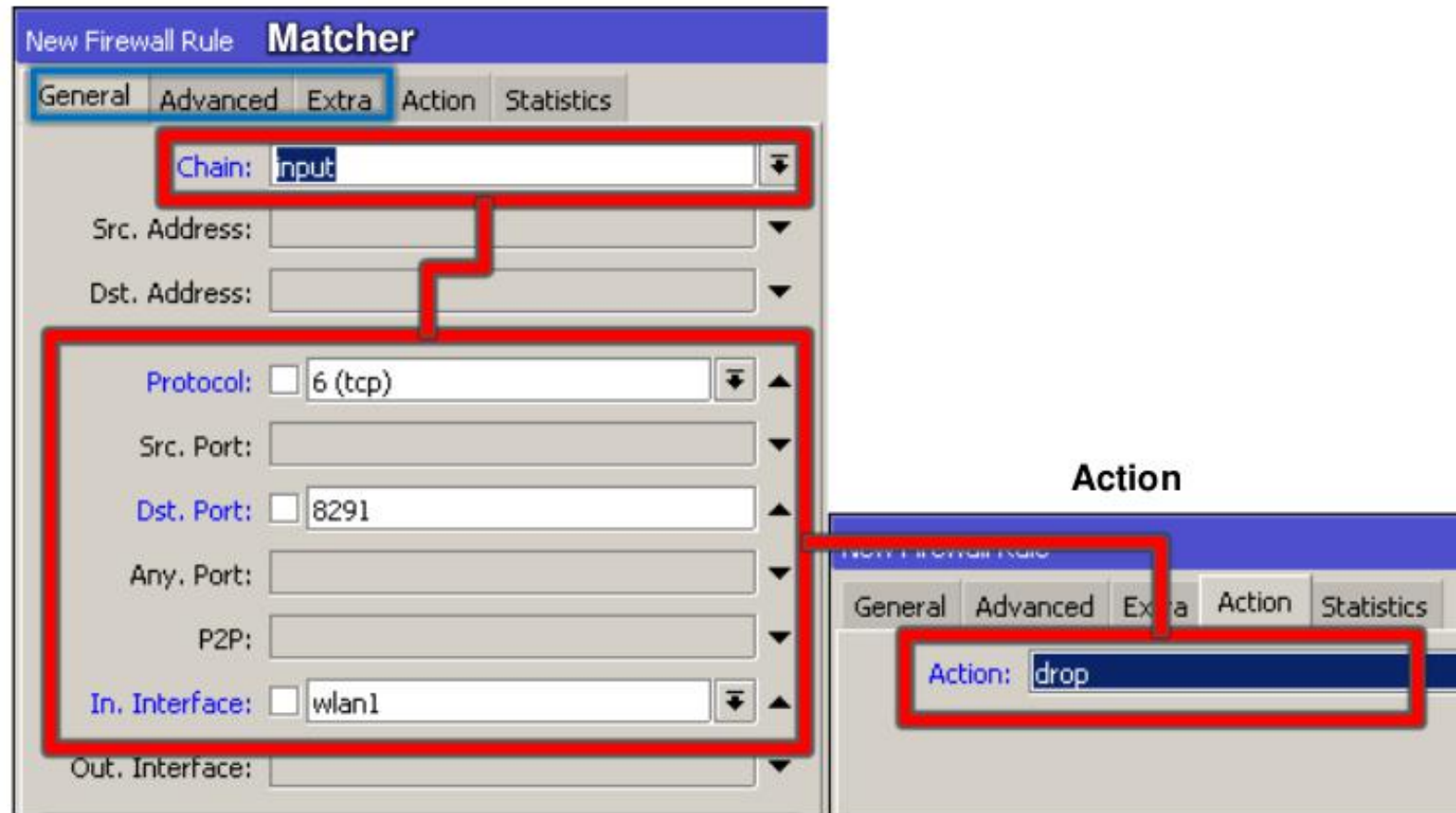
- Rules
- NAT (source-nat and destination-nat)
- Mangle
- Address List
- Layer 7 Protocol (baru di versi 3)
- Service Ports
- Connections
 - For monitoring only

(LAB) Firewall Filter

- Blok koneksi winbox ke router yang masuk melalui interface public(wlan)



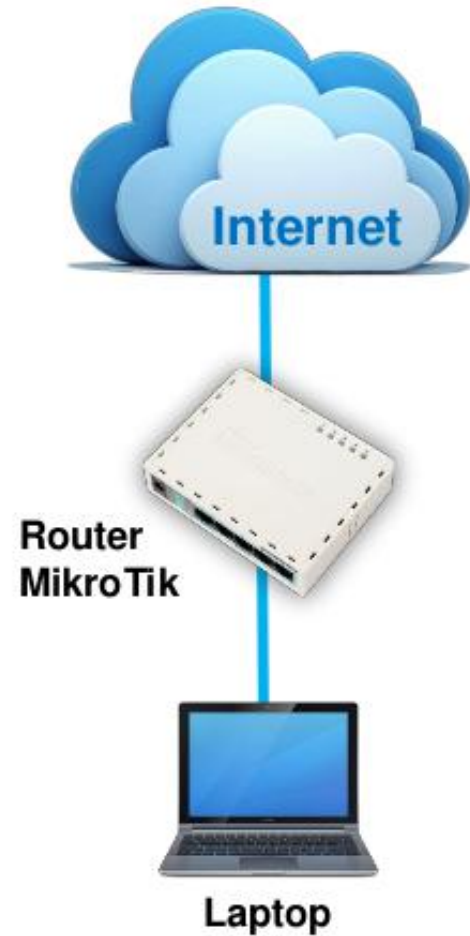
- Blok koneksi Winbox ke Router dari interface publik(wlan)



Prinsip Kerja MikroTik Firewall

- Bekerja menggunakan rules yang terdiri dari 2 bagian :
 - Matcher : Melakukan pengecekan kriteria paket data
 - Action : Perlakuan jika kriteria sesuai
- Pengecekan paket data bisa berdasarkan :
 - Source MAC Address
 - IP Addresses (network atau list) & address types (broadcast, local, multicast, unicast)
 - Port atau port range
 - Protocol
 - Dan masih banyak lagi parameter yang bisa digunakan

(LAB)Firewall Filter



PING






**Router
FTP Router**

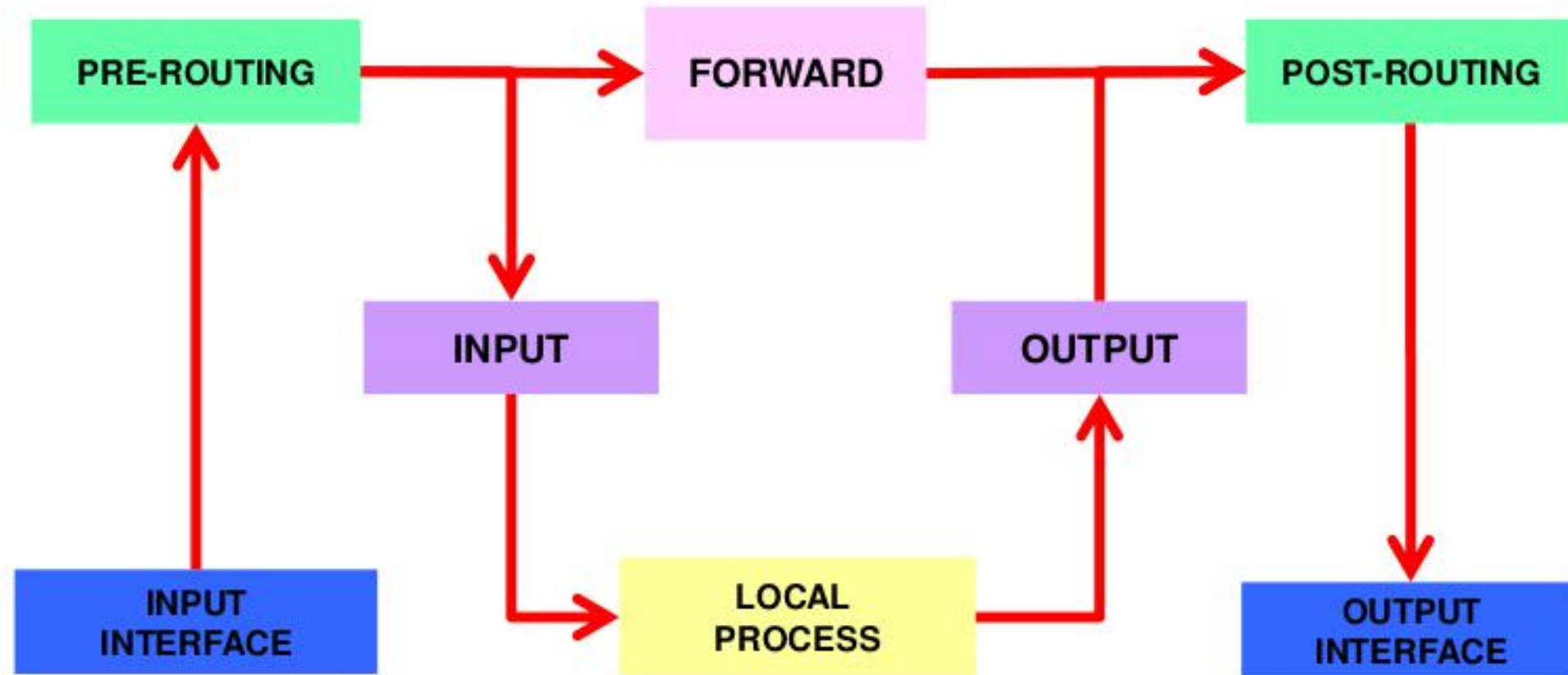


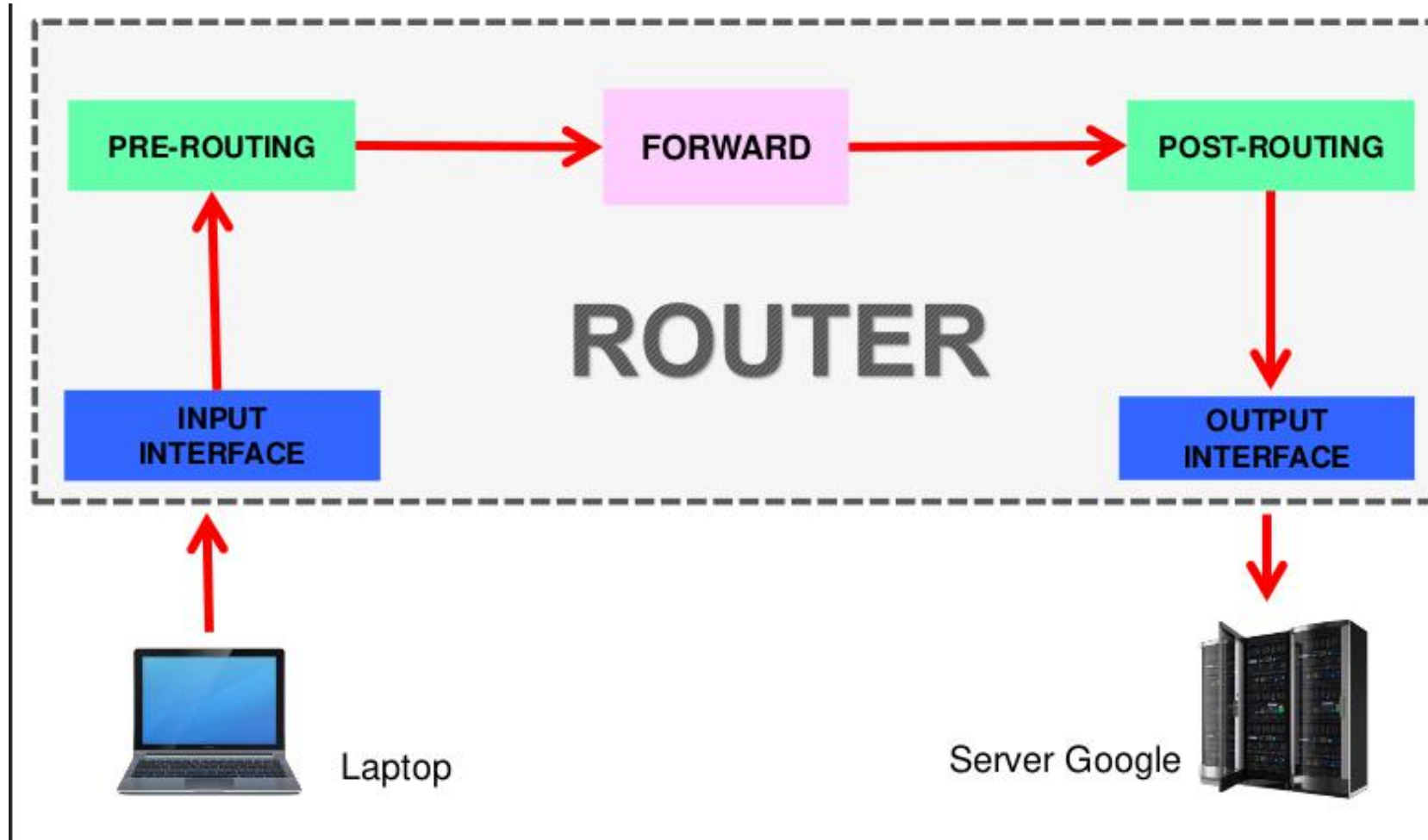
HTTP Router

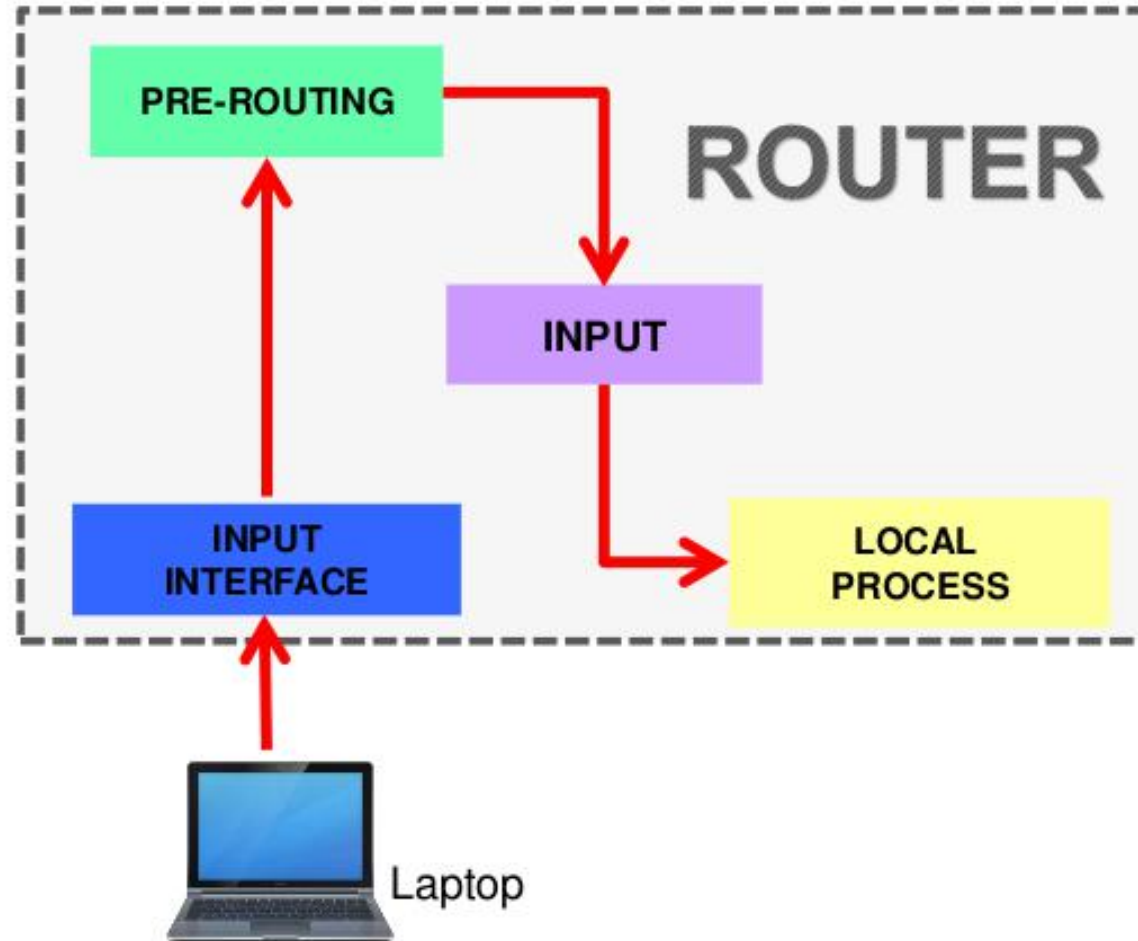
Chain pada Filter

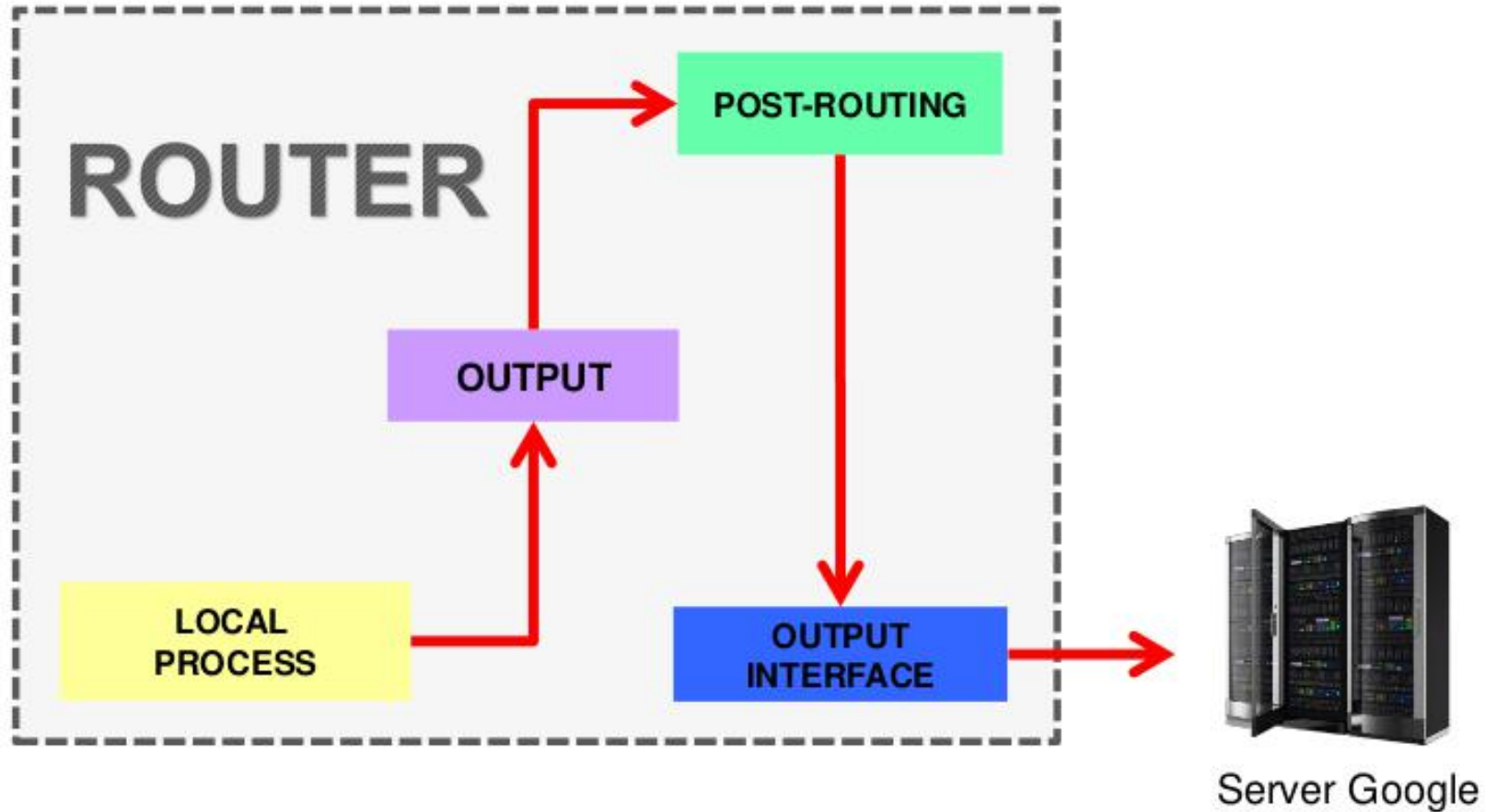
			
Prerouting	not implemented	not implemented	not implemented
Input	yes	no	no
Forward	no	yes	no
Output	no	no	yes
Postrouting	not implemented	not implemented	not implemented

Simple Packet Flow

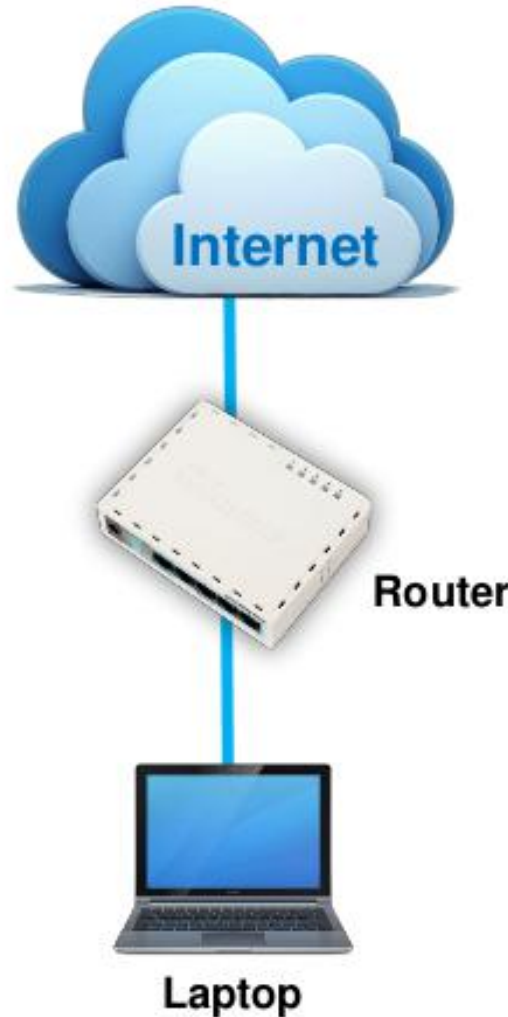








- User dapat membuat chain sendiri dengan kriteria sesuai kebutuhan
- Pilihan Action "**Jump**" dan isi nama custom chain pada opsi "**Jump Target**"
- Selanjutnya, kita bisa buat rule firewall dengan chain yang sudah dibuat



Batasi akses client ke internet



HTTP



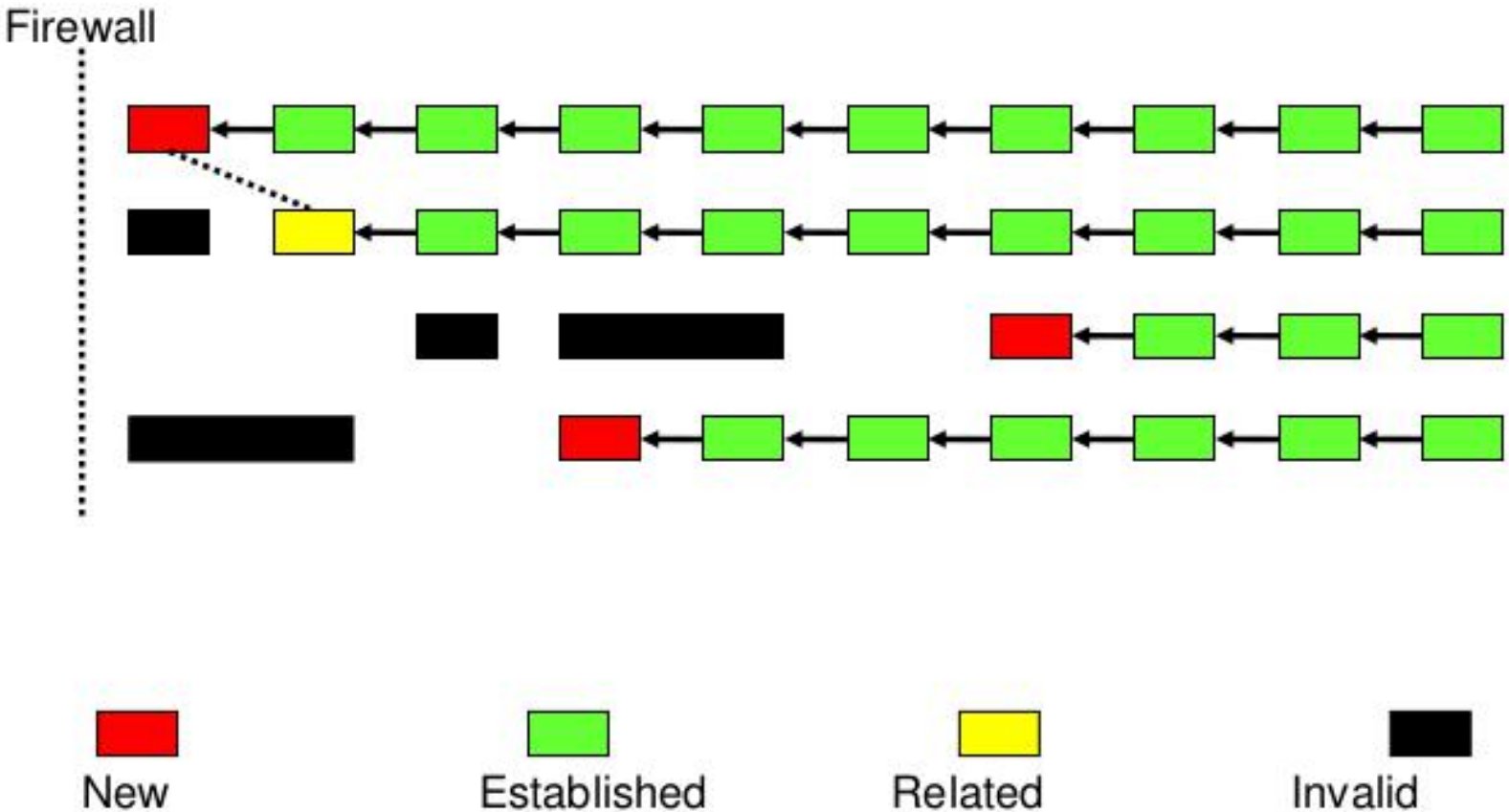
**Drop semua, kecuali
HTTP**

Firewall Filters Blocking Rules

- Pembacaan rule filter dilakukan dari atas ke bawah secara berurutan. Jika melewati rule yang kriteianya sesuai akan dilakukan action yang ditentukan, jika tidak sesuai, akan dianalisa ke baris selanjutnya.

- Setiap paket data yang lewat memiliki status :
 - **Invalid** : Paket tidak dimiliki oleh koneksi apapun, tidak berguna
 - **New** : Paket yang merupakkan pembuka sebuah koneksi/paket pertama dari sebuah koneksi
 - **Established** : Merupakan paket kelanjutan dari paket dengan status **New**
 - **Related** : Paket pembuka sebuah koneksi baru, tetapi masih berhubungan dengan koneksi sebelumnya

Connection State



Connection Tracking

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

Tracking Find

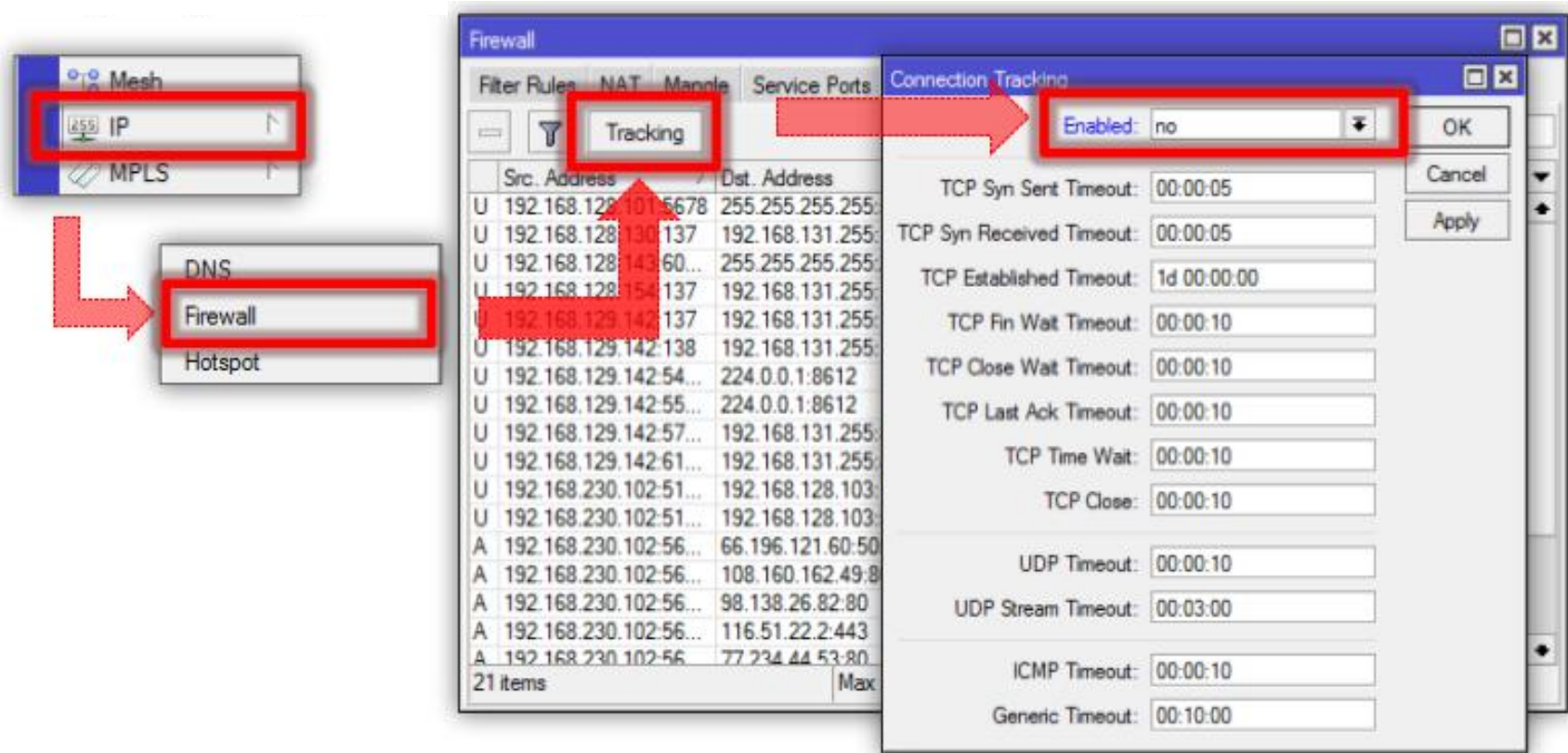
	Src. Address	Dst. Address	Reply Src. Address	Reply Dst. Address	Protocol	Connection ..
U	192.168.130.141:5...	69.25.24.26:80	69.25.24.26:80	192.168.130.141:59518	6 (tcp)	conn-penjaha
A	192.168.130.182:5...	69.171.233.33:443	69.171.233.33:443	192.168.130.182:59565	6 (tcp)	tso-con
A	192.168.130.177:5...	69.171.235.16:443	69.171.235.16:443	192.168.130.177:50146	6 (tcp)	spv-con
A	192.168.130.178:5...	69.171.235.16:443	69.171.235.16:443	192.168.130.178:53346	6 (tcp)	spv-con
A	192.168.130.177:5...	69.171.235.16:443	69.171.235.16:443	192.168.130.177:50144	6 (tcp)	spv-con
A	192.168.130.174:5...	69.171.245.49:443	69.171.245.49:443	192.168.130.174:51976	6 (tcp)	tso-con
A	192.168.130.168:5...	69.171.245.49:443	69.171.245.49:443	192.168.130.168:56507	6 (tcp)	tso-con
A	192.168.130.105:5...	69.171.245.49:443	69.171.245.49:443	192.168.130.105:50942	6 (tcp)	tso-con
A	192.168.130.83:64...	69.171.248.16:443	69.171.248.16:443	192.168.130.83:64766	6 (tcp)	tso-con
U	192.168.130.56:1527	70.33.182.206:80	70.33.182.206:80	192.168.130.56:1527	6 (tcp)	tso-con
A	192.168.130.80:54...	74.6.166.159:80	74.6.166.159:80	192.168.130.80:51919	6 (tcp)	tso-con
U	39.219.230.75:44367	74.82.91.47:443	74.82.91.47:443	192.168.130.80:51919	6 (tcp)	tso-con
A	192.168.130.173:4...	74.82.91.59:443	74.82.91.59:443	192.168.130.173:44367	6 (tcp)	tso-con
A	192.168.130.182:3...	74.82.91.66:443	74.82.91.66:443	192.168.130.182:3...	6 (tcp)	tso-con
A	192.168.130.168:4...	74.82.91.90:443	74.82.91.90:443	192.168.130.168:4...	6 (tcp)	tso-con
U	192.168.130.141:5...	74.125.96.141:80	74.125.96.141:80	192.168.130.141:56998	6 (tcp)	conn-penjaha

1052 items Max Entries: 524288

Maximum Connection yang bisa dihandle

(LAB)Connection Tracking

- Matikan **Connection Tracking**, kemudian amati apa yang terjadi?



- Memungkinkan tracking koneksi UDP, TCP, ICMP, dll walaupun UDP bersifat "stateless"
- Connection tracking bisa saja didisable untuk meningkatkan performance Router
- Akan tetapi ada konsekuensinya

- Dengan mematikan Connection Tracking, maka fungsi berikut tidak bisa digunakan :
 - NAT
 - Parameter Point to Point pada Simple Queue
 - Firewall dengan parameter :
 - connection-bytes
 - connection-mark
 - connection-type
 - connection-state
 - connection-limit
 - connection-rate
 - layer7-protocol
 - point-to-point
 - new-connection-mark
 - tarpit

- **accept** : paket diterima dan tidak melanjutkan membaca baris berikutnya
- **drop** : menolak paket secara diam-diam (tidak mengirimkan pesan penolakan ICMP)
- **reject** : menolak paket dan mengirimkan pesan penolakan ICMP
- **tarbit** : menolak, tetapi tetap menjaga TCP connections yang masuk (membalas dengan SYN/ACK untuk paket TCP SYN yang masuk)
- **log** : menambahkan informasi paket data ke log

IP Address List

Kita dapat melakukan pengelompokan IP Address dengan Address List

Address List bisa digunakan sebagai src. Address atau dst. Address pada Firewall Filter, Mangle dan NAT

The screenshot shows the Mikrotik WinBox Firewall configuration interface. The 'Address Lists' tab is selected and highlighted with a red box. Below the tab, there is a table of existing address lists:

Name	Address	Timeout
● nakal	10.0.0.2-10.0.0.5	
D ● nakal	192.168.128.102	
D ● nakal	192.168.128.102	
D ● nakal	172.16.1.1	
D ● nakal	192.168.128.102	

Two dialog boxes are overlaid on the interface:

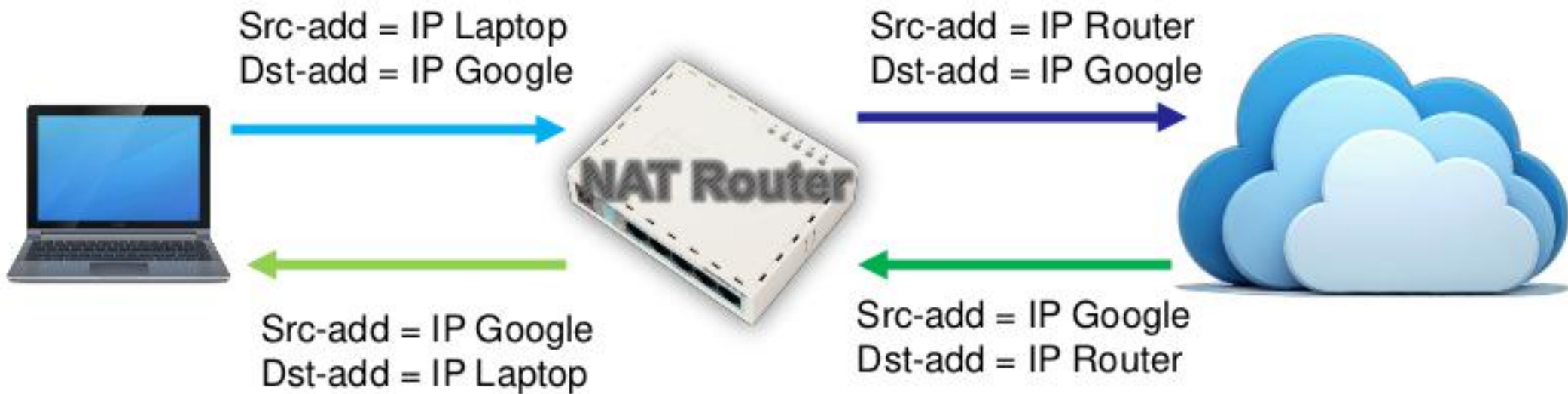
- New Firewall Address List:** This dialog is used to create a new address list. It shows 'Name' set to 'nakal' and 'Address' set to '192.168.30.0/24'. There is a 'Dynamic' checkbox which is currently unchecked.
- New Firewall Rule:** This dialog is used to configure a firewall rule. The 'Advanced' tab is selected and highlighted with a red box. It shows 'Src. Address List' set to 'nakal' and 'Dst. Address List' set to an empty field.

A red arrow points from the text box on the left to the 'Advanced' tab in the 'New Firewall Rule' dialog.

Network Address Translation (NAT)

- NAT digunakan untuk melakukan pengubahan baik **src-address** ataupun **dst-address**
- Setelah paket data pertama dari sebuah koneksi terkena NAT, maka paket berikutnya pada koneksi tersebut juga akan terkena NAT
- NAT akan diproses terurut mulai baris paling atas hingga ke bawah

- Cara kerja NAT ketika client mencoba mengakses google



(LAB) Firewall NAT

The image illustrates the configuration of a NAT rule in Mikrotik WinBox. It shows three main windows with red boxes and arrows highlighting the configuration steps:

- Mesh Window:** The 'IP' menu item is highlighted with a red box.
- DNS Window:** The 'Firewall' menu item is highlighted with a red box.
- Firewall Window:** The 'NAT' tab is selected and highlighted with a red box. A red box around the '+' icon indicates the 'Add' button.
- New NAT Rule Window:** This window shows the configuration for a new NAT rule. The 'Chain' dropdown is set to 'srcnat' and highlighted with a red box. The 'Out. Interface' dropdown is set to 'wlan1' and highlighted with a red box.
- NAT Rule Window:** This window shows the configuration for the selected NAT rule. The 'Action' dropdown is set to 'masquerade' and highlighted with a red box.

Red arrows indicate the flow of configuration: from the 'IP' menu to 'Firewall', then to the 'NAT' tab, then to the 'Add' button, then to the 'New NAT Rule' window, and finally to the 'NAT Rule' window.

Untuk menyembunyikan IP Address lokal dan menggantikannya dengan IP Address publik yang sudah terpasang pada router

- **src-nat**
 - Kita bisa memilih IP Address publik yang digunakan untuk menggantikan
- **masquerade**
 - Secara otomatis akan menggunakan IP Address pada interface publik
 - Digunakan untuk mempermudah instalasi dan bila IP Address publik pada interface publik menggunakan IP Address yang dinamik (misalnya DHCP, PPTP, atau EoIP)

Untuk melakukan penggantian IP Address tujuan, atau mengarahkan koneksi ke localhost

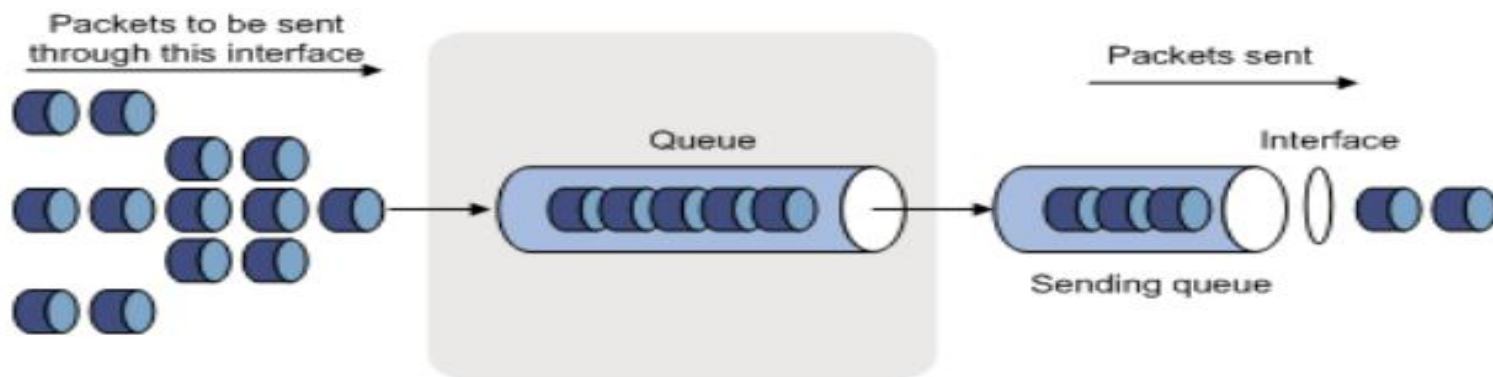
- **dst-nat**

- Kita bisa mengganti IP Address dan port tujuan dari suatu koneksi

- **redirect**

- Untuk mengalihkan koneksi yang tadinya melewati Router, dan dialihkan menuju ke localhost

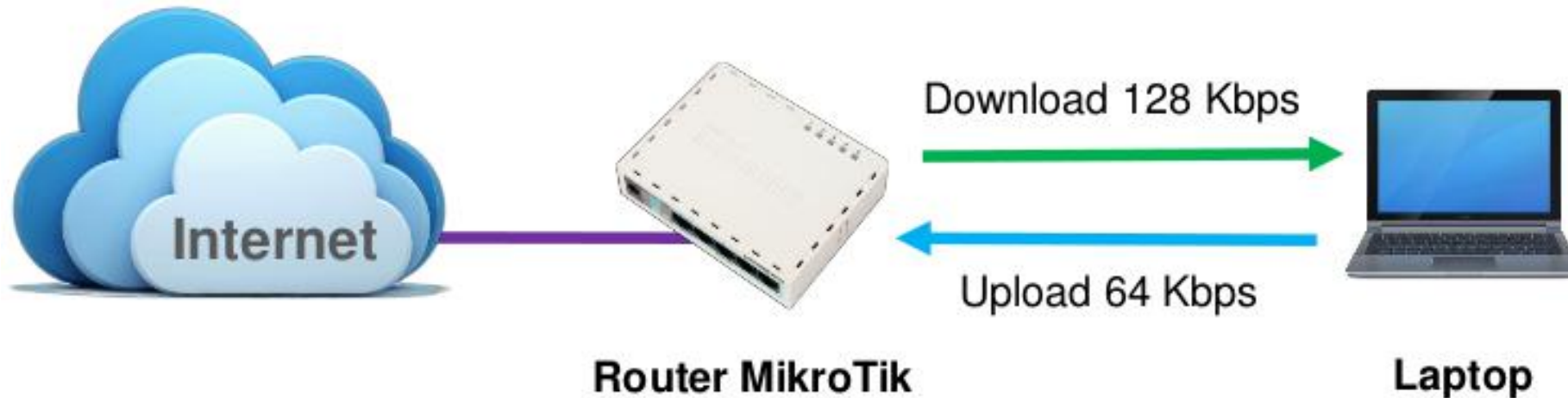
- **QoS** tidak selalu berarti pembatasan bandwidth, dan tidak bisa memperbesar bandwidth
- Adalah cara yang digunakan untuk **mengatur penggunaan bandwidth yang ada secara rasional**
- **QoS** bisa digunakan juga untuk mengatur prioritas berdasarkan parameter yang diberikan, menghindari terjadinya trafik yang memonopoli seluruh bandwidth yang tersedia



- Dengan simple queue, kita dapat melakukan :
 - Melimit tx-rate client (upload)
 - Melimit rx-rate client (download)
 - Melimit tx+rx-rate client (akumulasi)

Make a simple queue for your laptop

- Downstream : 128 kbps
- Upstream : 64 kbps



(LAB)Simple Queue

New Simple Queue

General | Advanced | Statistics | Traffic | Total | Total Statistics

Name: queue-simple

Target: 192.168.x.2

Dst.:

	Target Upload	Target Download
Max Limit:	64k	128k
Burst Limit:	unlimited	unlimited
Burst Threshold:	unlimited	unlimited
Burst Time:	0	0

Time

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Torch

- Target Address harus diisi
- Parameter target address bisa berupa IP Address, Interface, dan Network
- Multiple Target Address untuk target yang lebih dari satu

- Sebaiknya harus ditentukan, karena di kondisi nyata tidak ada bandwidth unlimited
- Jika max limit tidak ditentukan, bandwidth management tidak dapat berjalan sempurna

- Kita tidak dapat melakukan pembatasan trafik yang masuk ke suatu interface
- Satu-satunya cara untuk mengontrol adalah dengan buffering(menahan sementara), atau kalau melampaui limit buffer, akan dilakukan drop pada paket tersebut
- Pada TCP, paket yang didrop akan dikirimkan ulang sehingga tidak ada kehilangan paket data
- Cara termudah melakukan queue di RouterOS adalah menggunakan **Simple Queue**

Akumulasi Upload dan Download

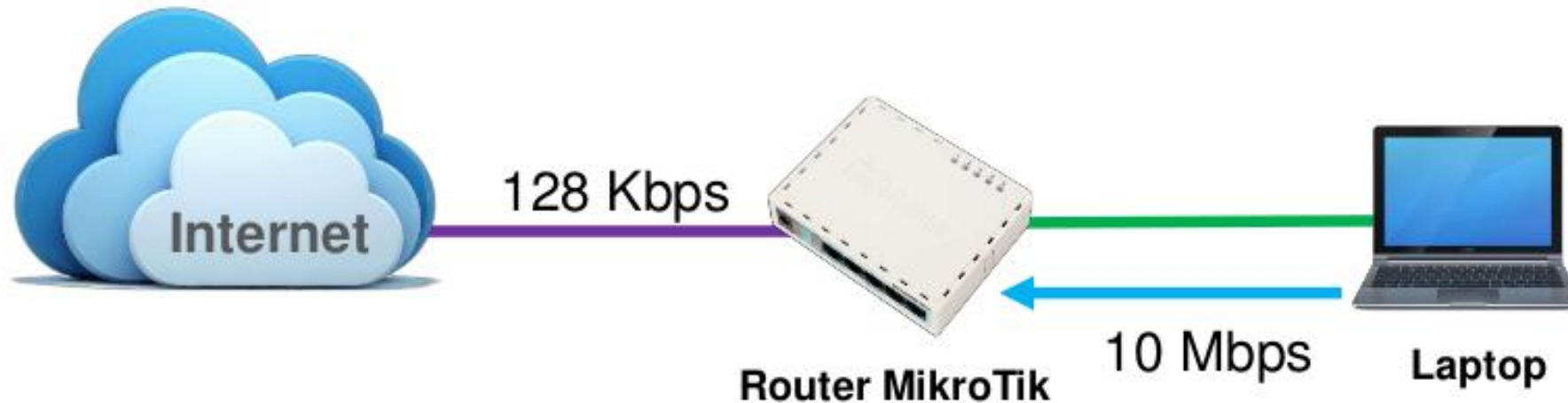
The screenshot shows the 'New Simple Queue' dialog box with the 'Total Statistics' tab selected. The dialog has a title bar with a close button. The tabs are 'General', 'Advanced', 'Statistics', 'Traffic', 'Total', and 'Total Statistics'. The 'Total Statistics' tab contains the following fields and controls:

- Total Limit At: ▼ bits/s
- Total Max Limit: ▲ bits/s
- Total Priority: ▼
- Total Burst Limit: ▼ bits/s
- Total Burst Threshold: ▼ bits/s
- Total Burst Time: ▼ s
- Total Queue Type: ▼

On the right side of the dialog, there is a vertical stack of buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters, and Torch. At the bottom left of the dialog, the text 'enabled' is displayed.

- Jika kita perhatikan, ada perubahan warna pada icon Queue rule. Maksud masing-masing warna adalah sebagai berikut :
 - **Hijau** : 0 – 50% bandwidth digunakan.
 - **Kuning** : 51 – 75% bandwidth digunakan
 - **Merah** : 76 – 100% bandwidth digunakan

- Limit download laptop maksimal 128 Kbps
- Khusus koneksi ke router, boleh menggunakan bandwidth sampai 10 Mbps



Simple Queue Destination

New Simple Queue

General | Advanced | Statistics | Traffic | Total | ...

Name: queue-ke-router

Target: 192.168.x.2

Dst.: 10.10.10.x

	Target Upload	Target Download	
Max Limit:	10M	10M	bits/s
Burst Limit:	unlimited	unlimited	bits/s
Burst Threshold:	unlimited	unlimited	bits/s
Burst Time:	0	0	s

Time

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Torch

- Menentukan queue untuk trafik dengan tujuan tertentu
- Bisa diisi dengan IP Address atau Network

- Limit bandwidth pada jam 09:00 - 17:00 di hari kerja dengan bandwidth 128 Kbps
- Kemudian limit bandwidth pada jam 17:00 - 09:00 di hari kerja dengan bandwidth 512 Kbps
- Untuk sabtu - minggu boleh menggunakan bandwidth sampai 1 Mbps

(LAB) Simple Queue Time

Simple Queue <queue2>

General Advanced Statistics Traffic Total Total Statistics

Name: queue-simple

Target: 192.168.x.2

Dst.:

Target Upload Target Download

Max Limit: 128k 128k bits/s

Burst

Time

Time: 09:00:00 - 17:00:00

sun mon tue wed thu fri sat

Simple Queue <queue2>

General Advanced Statistics Traffic Total Total Statistics

Name: queue-simple 2

Target: 192.168.x.2

Det.:

Target Upload Target Download

Max Limit: 512k 512k bits/s

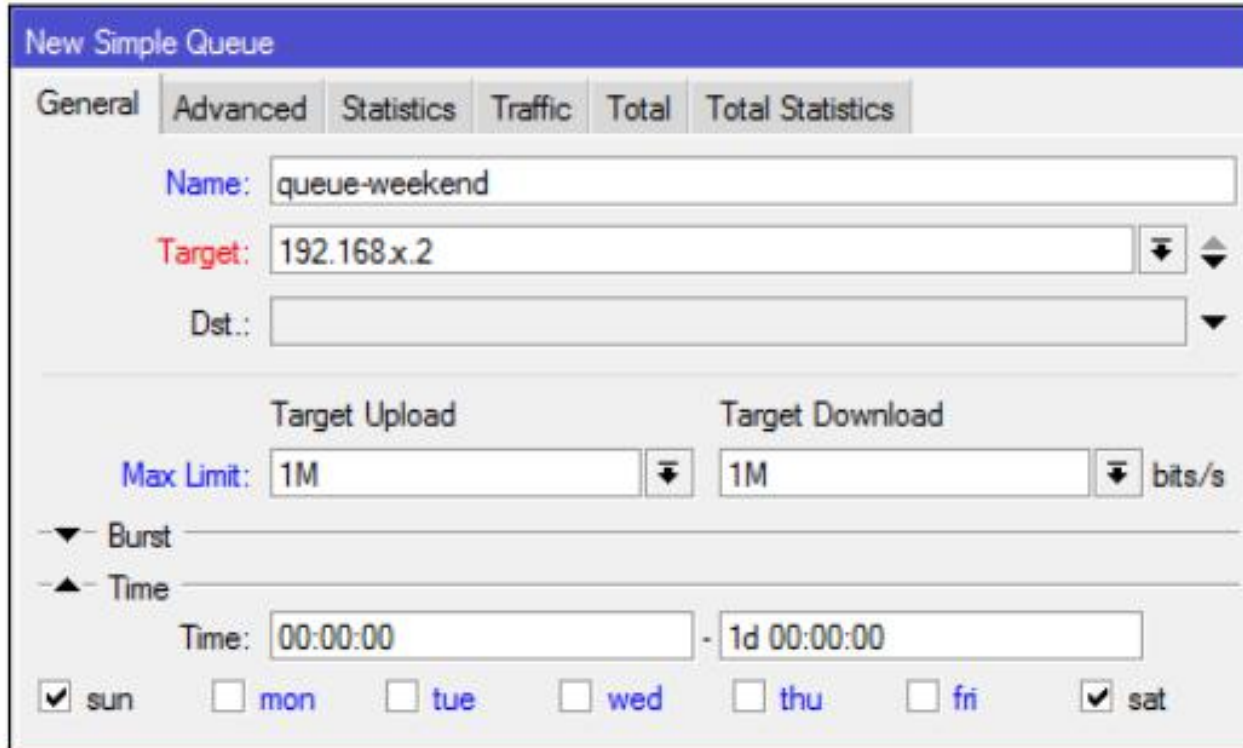
Burst

Time

Time: 17:00:01 - 08:59:59

sun mon tue wed thu fri sat

(LAB) Simple Queue Time



New Simple Queue

General Advanced Statistics Traffic Total Total Statistics

Name: queue-weekend

Target: 192.168.x.2

Dst.:

Target Upload Target Download

Max Limit: 1M 1M bits/s

Burst

Time

Time: 00:00:00 - 1d 00:00:00

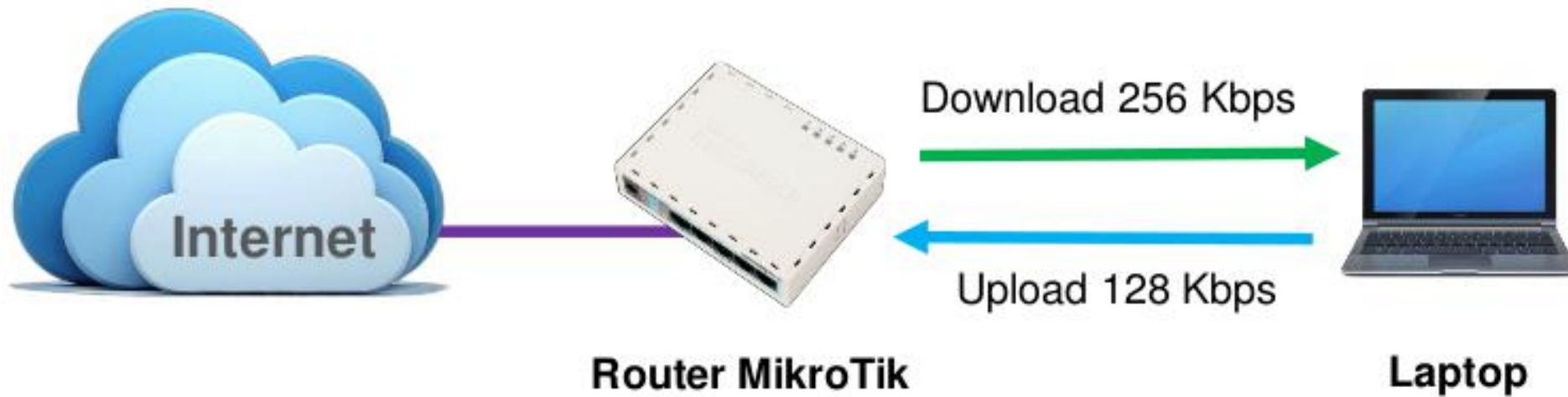
sun mon tue wed thu fri sat

Sebelum setting parameter Time, pastikan sudah setting NTP Client dan clock router sudah sesuai dengan kondisi real

- **Burst** adalah salah satu cara menjalankan **QoS**
- **Burst** memungkinkan penggunaan data-rate yang melebihi max-limit untuk periode waktu tertentu
- Jika data-rate lebih kecil dari **burst-threshold**, burst dapat dilakukan hingga data-rate mencapai **burst-limit**
- Setiap detik, router mengkalkulasi data-rate rata-rata pada suatu kelas queue untuk periode waktu terakhir sesuai dengan **burst-time**
- **Burst-time** tidak sama dengan waktu yang dijalankan untuk melakukan burst

Topologi Simple Queue Burst

- Pada kondisi tertentu, user diijinkan untuk menggunakan bandwidth melebihi max limit



- Make a simple queue for your laptop
 - Downstream max-limit=256k
 - Upstream max-limit=128k
- Try Using Burst
 - Burst-limit=1M
 - Burst-treshold=512K
 - Burst-time=30s

(LAB) Simple Queue Burst

New Simple Queue

General | Advanced | Statistics | Traffic | Total | Total Statistics

Name:

Target Address:

Target Upload Target Download

Max Limit: bits/s

-▲- Burst

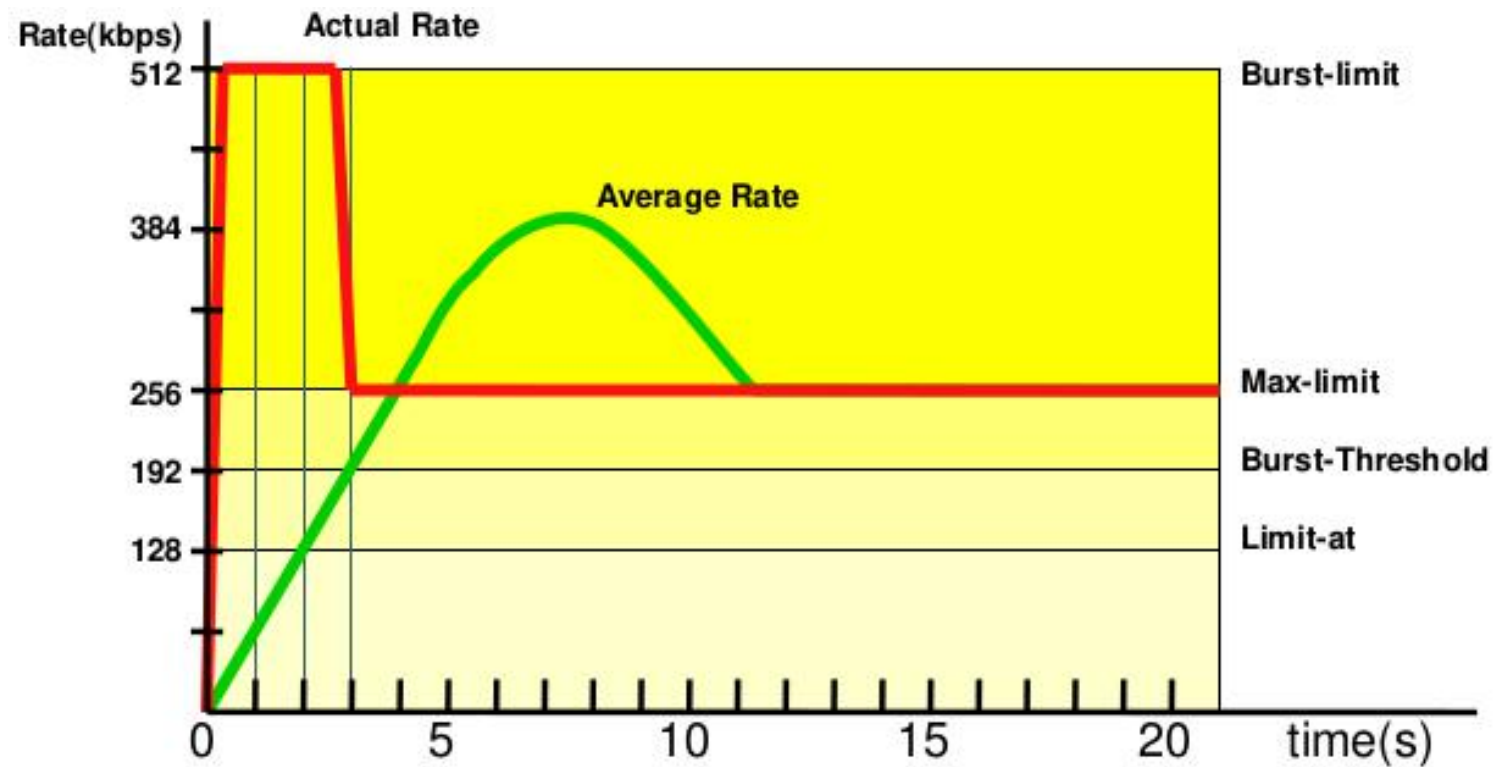
Burst Limit: bits/s

Burst Threshold: bits/s

Burst Time: s

-▼- Time

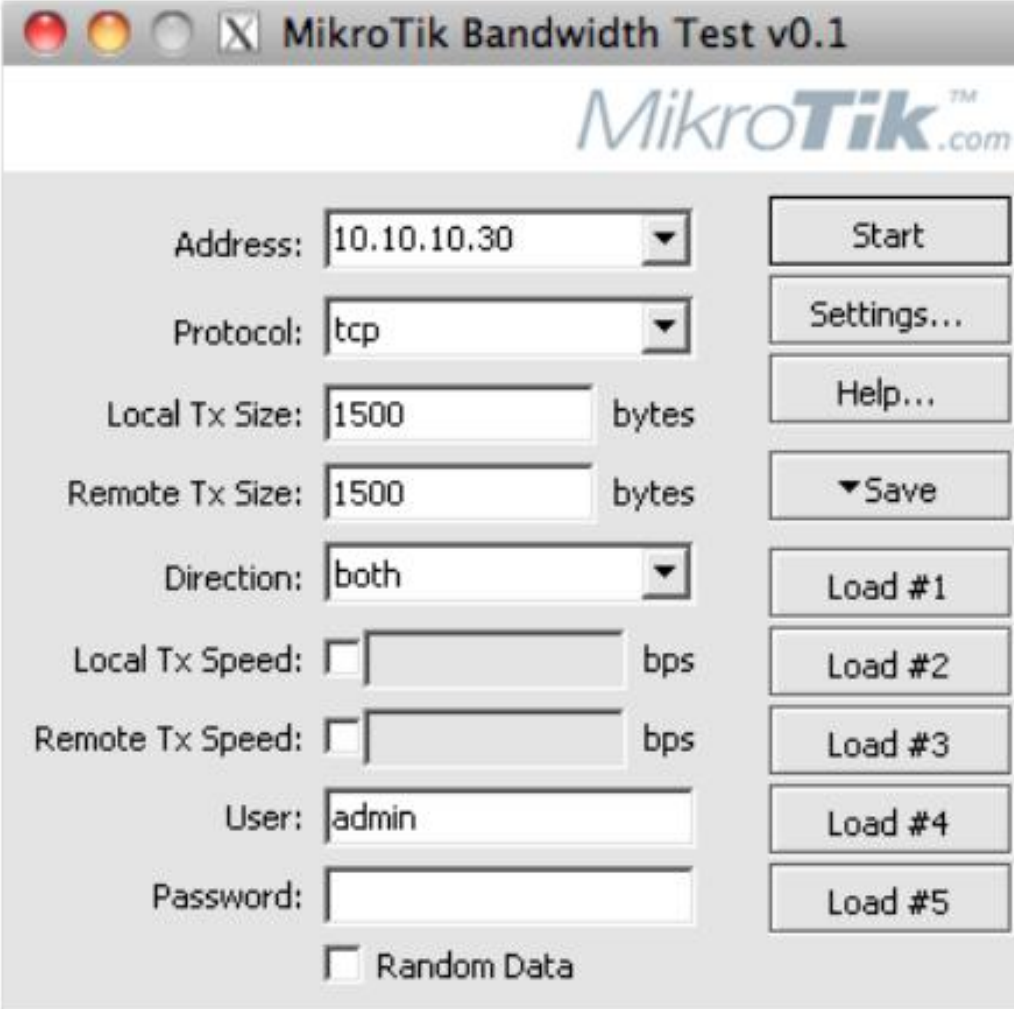
Max-limit=256kbps, burst-time=8,
burst-threshold=192kbps, burst-limit=512kbps.



- Pada awalnya, data rate rata-rata dalam 8 detik terakhir adalah 0 kbps. Karena data rate rata-rata ini lebih kecil dari burst-threshold, maka burst dapat dilakukan
- Setelah 1 detik, data rate rata-rata adalah $(0+0+0+0+0+0+0+512)/8=64\text{kbps}$, masih lebih kecil dari **burst-threshold**. Burst dapat dilakukan
- Demikian pula untuk detik kedua, data rate rata-rata adalah $(0+0+0+0+0+0+512+512)/8=128\text{kbps}$
- Setelah 3 detik, tibalah pada saat dimana data rate rata-rata lebih besar dari **burst-threshold**. Burst tidak dapat lagi dilakukan, dan data rate turun menjadi **max-limit** (256kbps)

Simple Queue Bandwidth Test

- **Address :**
 - IP Address test serve
- **Direction :**
 - Upload
 - Download
 - Upload & Download
- **Protocol :**
 - TCP / UDP
- **User & Password :**
 - Autentikasi



The screenshot shows the MikroTik Bandwidth Test v0.1 application window. The title bar reads "MikroTik Bandwidth Test v0.1". The MikroTik logo is visible in the top right. The interface contains several input fields and buttons:

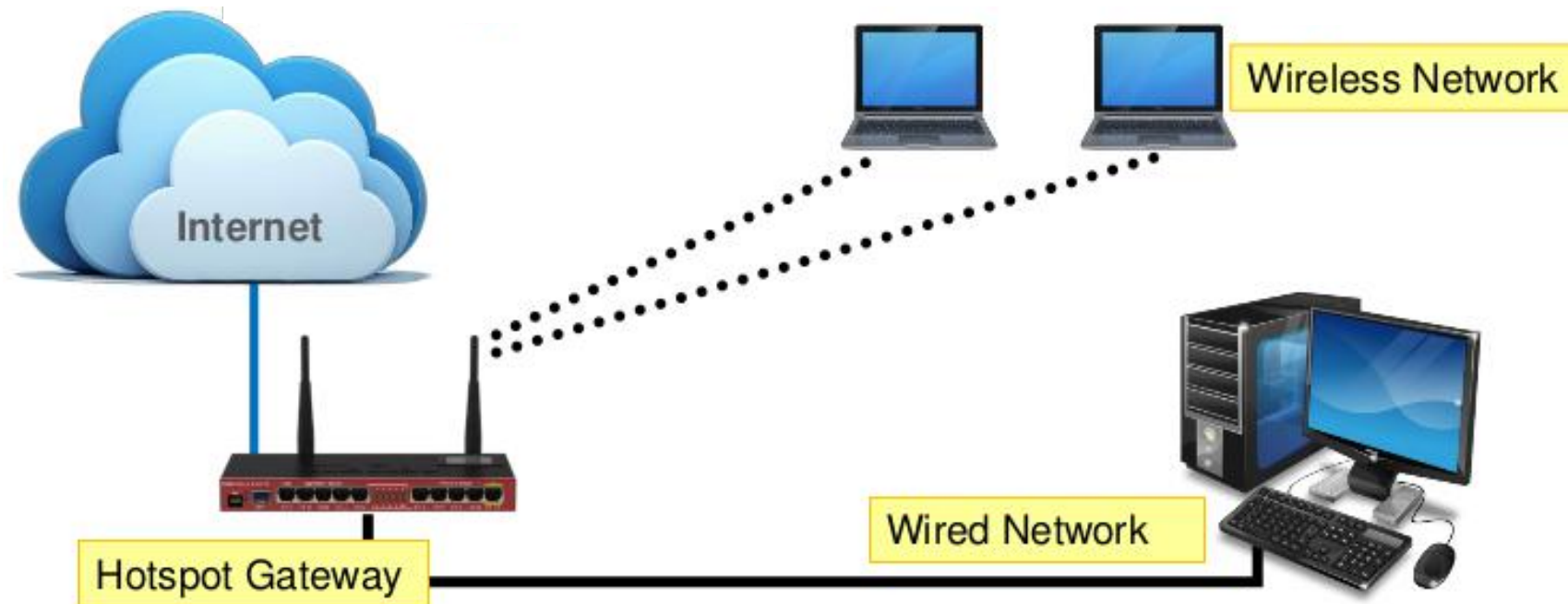
- Address:** 10.10.10.30
- Protocol:** tcp
- Local Tx Size:** 1500 bytes
- Remote Tx Size:** 1500 bytes
- Direction:** both
- Local Tx Speed:** [] bps
- Remote Tx Speed:** [] bps
- User:** admin
- Password:** []
- Random Data

Buttons on the right side include: Start, Settings..., Help..., Save (with a dropdown arrow), Load #1, Load #2, Load #3, Load #4, and Load #5.

- Hotspot System digunakan untuk memberikan layanan akses jaringan (Internet/Intranet) di Public Area dengan media kabel maupun wireless
- Hotspot menggunakan Autentikasi untuk menjaga Jaringan tetap dapat dijaga walaupun bersifat Publik
- Proses Autentikasi menggunakan protokol HTTP/HTTPS yang bisa dilakukan oleh semua web-browser
- Hotspot System ini merupakan gabungan atau kombinasi dari beberapa fungsi dan fitur RouterOS menjadi sebuah system yang sering disebut "Plug-n-Play" Access

Example Hotspot Network

- Hotspot System bisa digunakan pada jaringan Wireless maupun jaringan Kabel bahkan kombinasi dari keduanya
- Jaringan Hotspot bersifat **Bridge Network**



- Autentikasi User
- Perhitungan
 - Waktu akses
 - Data dikirim atau diterima
- Limitasi Data
 - Berdasarkan data rate (kecepatan akses)
 - Berdasarkan jumlah data
- Limitasi Akses User berdasarkan waktu
- Support RADIUS
- Bypass !

(LAB) Hotspot Setup Wizard

- RouterOS sudah menyediakan Wizard untuk melakukan setup Hotspot System
- Wizard ini berupa menu interaktif yang terdiri dari beberapa pertanyaan mengenai parameter setting hotspot
- Wizard bisa dipanggil atau dieksekusi menggunakan perintah **"/ip hotspot setup"**
- Jika anda mengalami kegagalan dalam konfigurasi hotspot direkomendasikan reset kembali router dan konfigurasi ulang dari awal

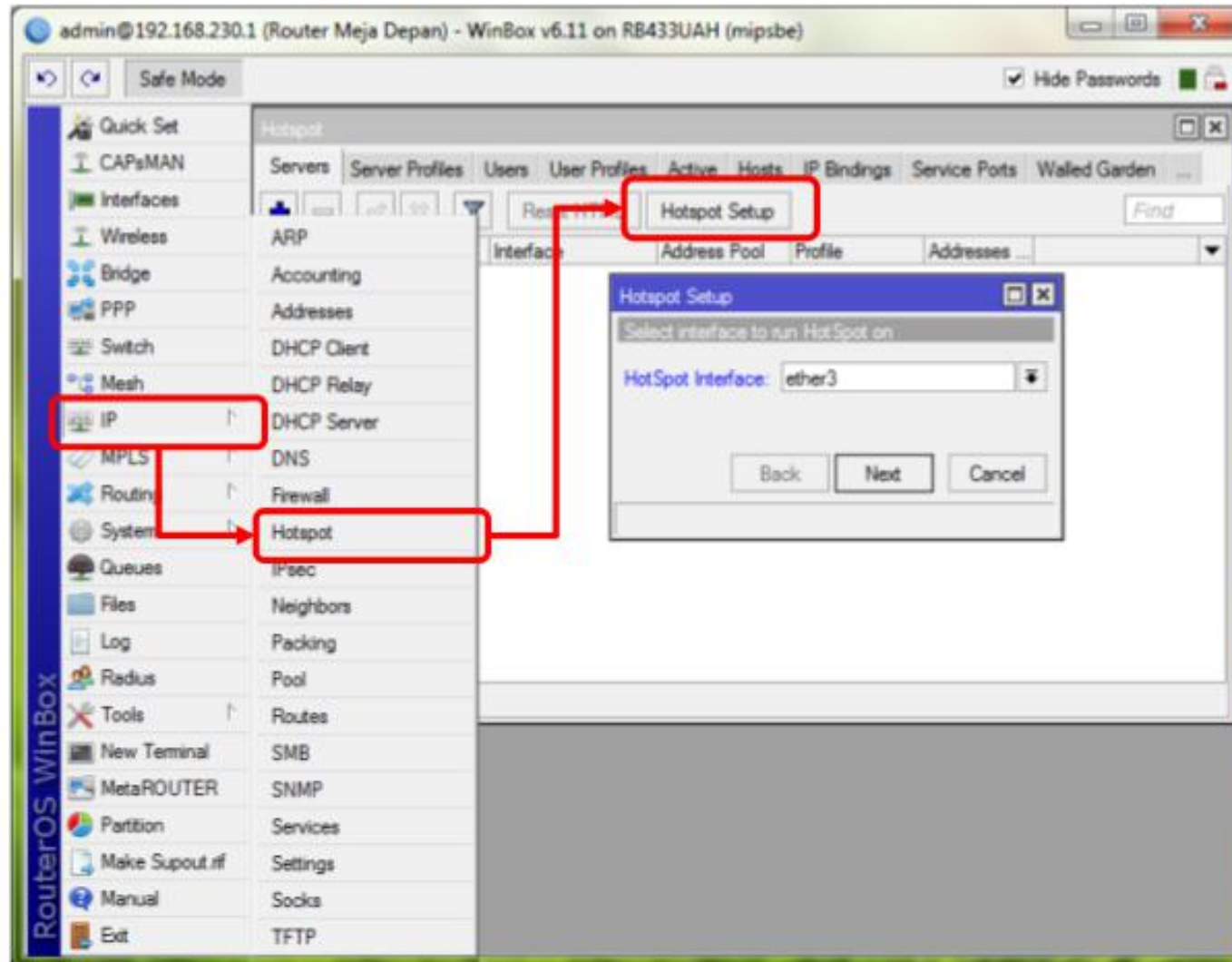
(LAB) Hotspot Setup Wizard

- Pada Langkah awal Tentukan Interface mana yang akan digunakan untuk menjalankan Hotspot System :
 - *hotspot interface : (ex:ether1,wlan1,bridge1,vlan1)*
- Tentukan Alamat IP untuk Interface Hotspot :
 - *Local address of hotspot network : (ex:10.10.10.1/24)*
- Opsi Hotspot Network akan NAT atau Routing :
 - *masquerade hotspot network : yes*
- Tentukan IP-Pool untuk jaringan Hotspot :
 - *address pool of hotspot network : 10.10.10.50-10.10.10.254*
- Menggunakan SSL-Certificate jika ingin menggunakan Login-By HTTPS :
 - *select certificate : none*

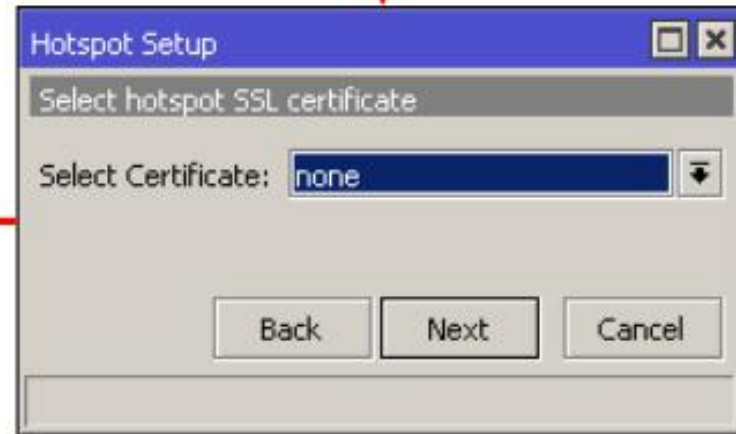
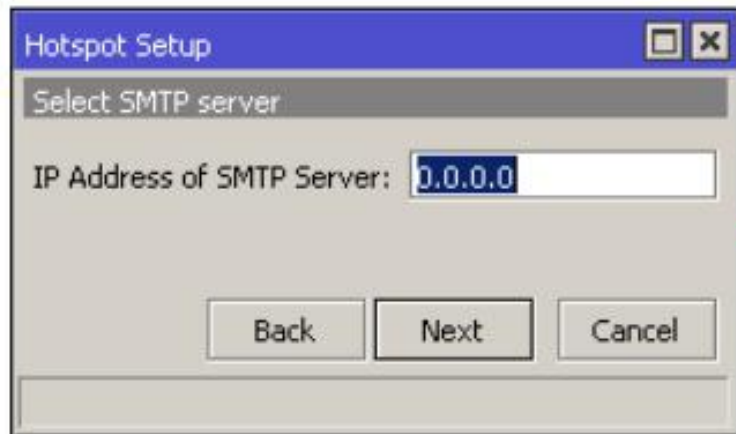
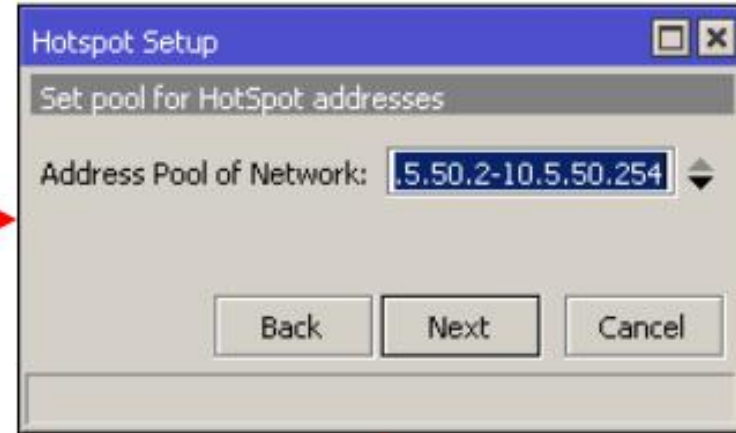
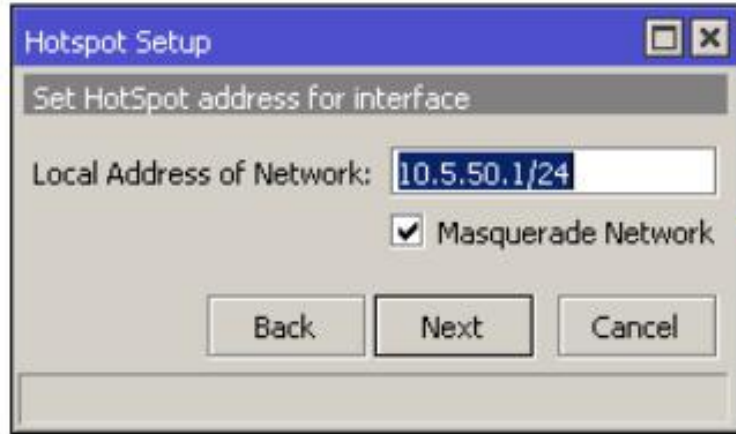
(LAB) Hotspot Setup Wizard

- Jika diperlukan SMTP Server khusus untuk Server hotspot bisa ditentukan, sehingga Server bisa mengirimkan email (misal email notifikasi). Konfigurasi SMTP Server :
 - *Ip address of smtp server : 0.0.0.0 (ex : 168.125.154.190)*
- Konfigurasi DNS Server yang akan digunakan oleh user Hotspot :
 - *dns server : 158.149.180.192, 185.154.85.23*
- Konfigurasi DNS-name dari router Hotspot. Hal ini digunakan jika Router memiliki DNS-Name yang valid (FQDN), Jika tidak ada biarkan kosong
- Langkah terakhir dari wizard adalah pembuatan sebuah user hotspot :
 - *name of local hotspot user : admin*
 - *password for the user : admin*

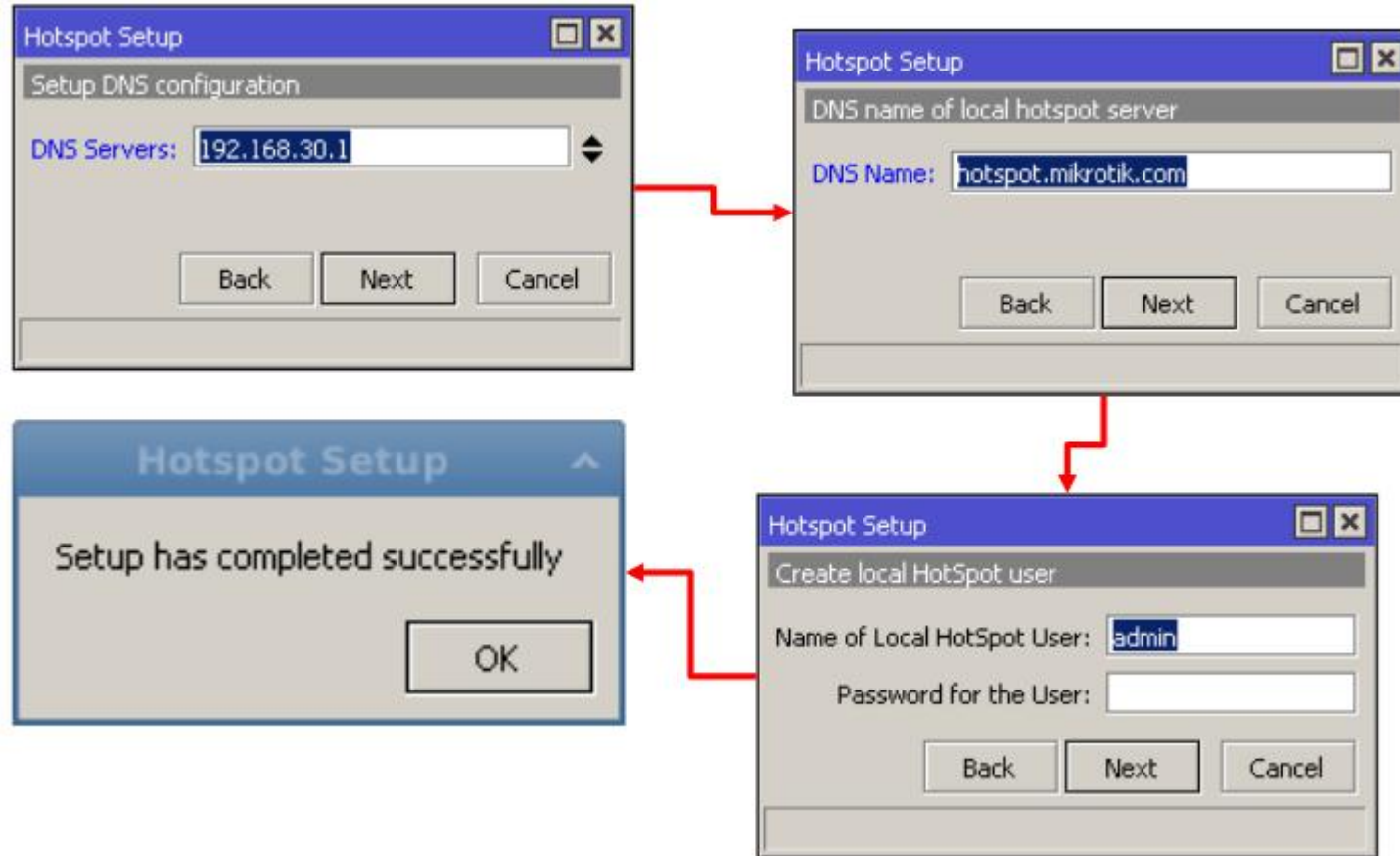
(LAB) Hotspot Setup Wizard (Step 1)



(LAB) Hotspot Setup Wizard (Step 2-5)



(LAB) Hotspot Setup Wizard (Step 6-9)



How does it work?

- User mencoba membuka halaman web
- Authentication Check dilakukan oleh router pada Hotspot System
- Jika belum ter-autentikasi, router akan mengalihkan ke halaman login
- User memasukkan informasi login

Please log on to use the mikrotik hotspot service



A screenshot of a Mikrotik Hotspot login page. The page has a white background with a thin border. At the top, it says "Please log on to use the mikrotik hotspot service". Below this, there are two input fields: "login" with the text "anyuser" and "password" with a series of asterisks. Below the password field is an "OK" button. At the bottom of the page is the Mikrotik logo.

Powered by mikrotik routers © 2005 mikrotik

How does it work?

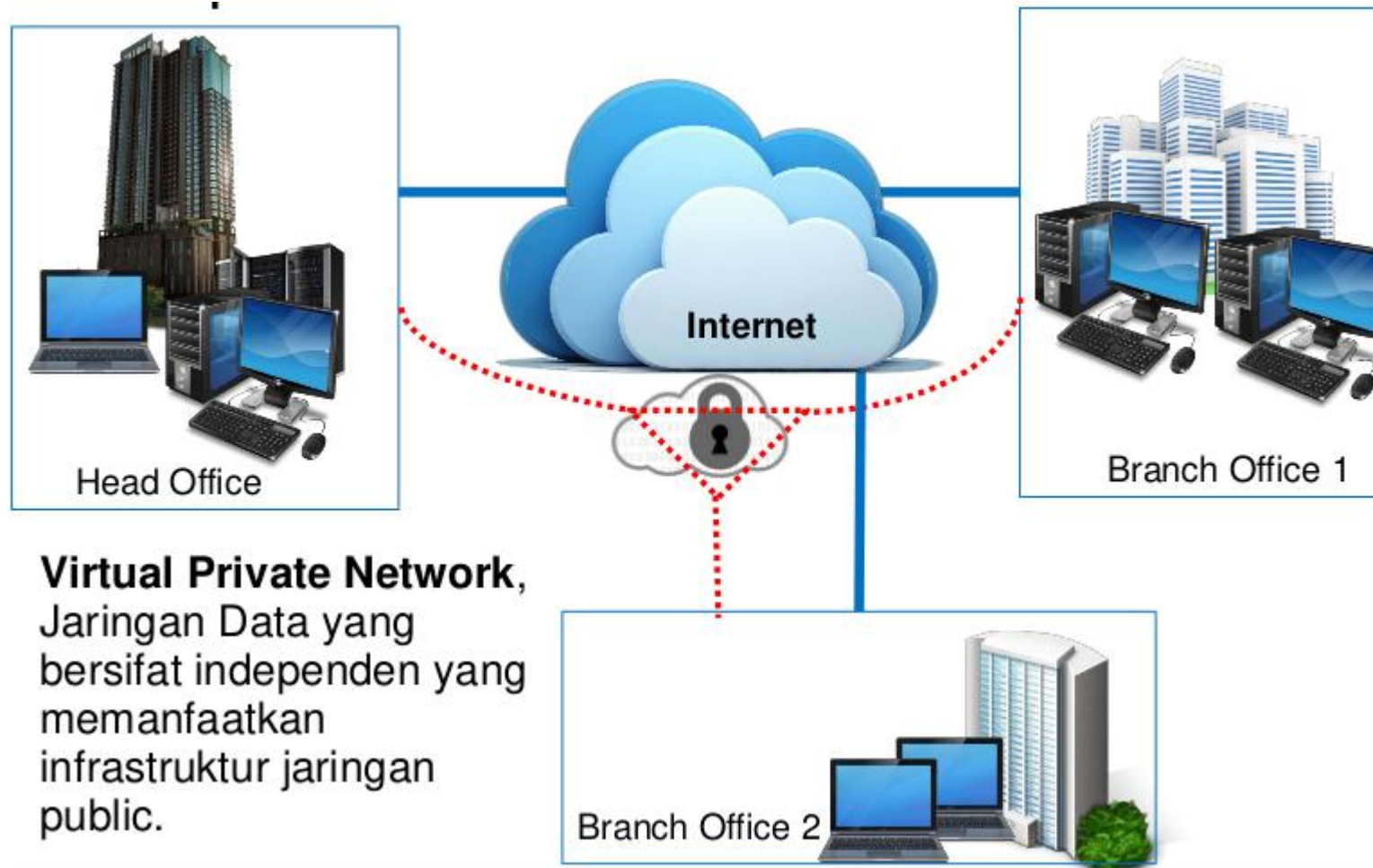
- Jika informasi login sudah tepat, router akan :
 - Mengautentikasi client di Hotspot System
 - Membuka halaman web yang diminta sebelumnya
 - Membuka pop-up halaman status
- User dapat menggunakan akses jaringan

Welcome anyuser!

IP address:	10.1.100.1
bytes up/down:	23.1 KiB / 43.5 KiB
connected:	40s
status refresh:	1m

log off

- Virtual Private Network(VPN) adalah sebuah jaringan komputer dimana koneksi antar nodenya **memanfaatkan jaringan publik** (Internet/WAN) karena mungkin dalam kondisi atau kasus tertentu tidak memungkinkan untuk membangun infrastruktur jaringan sendiri
- **Interkoneksi** antar node seperti memiliki jaringan yang **independen** yang sebenarnya dibuatkan koneksi atau jalur khusus melewati jaringan publik
- Pada implementasinya biasa digunakan untuk membuat **komunikasi yang bersifat secure** melalui jaringan Internet, tetapi VPN tidak harus menggunakan standard keamanan yang baku seperti Autentikasi dan Enkripsi
- Salah satu contohnya adalah penggunaan VPN untuk akses network dengan tingkat security yang tinggi di system reservasi ticket



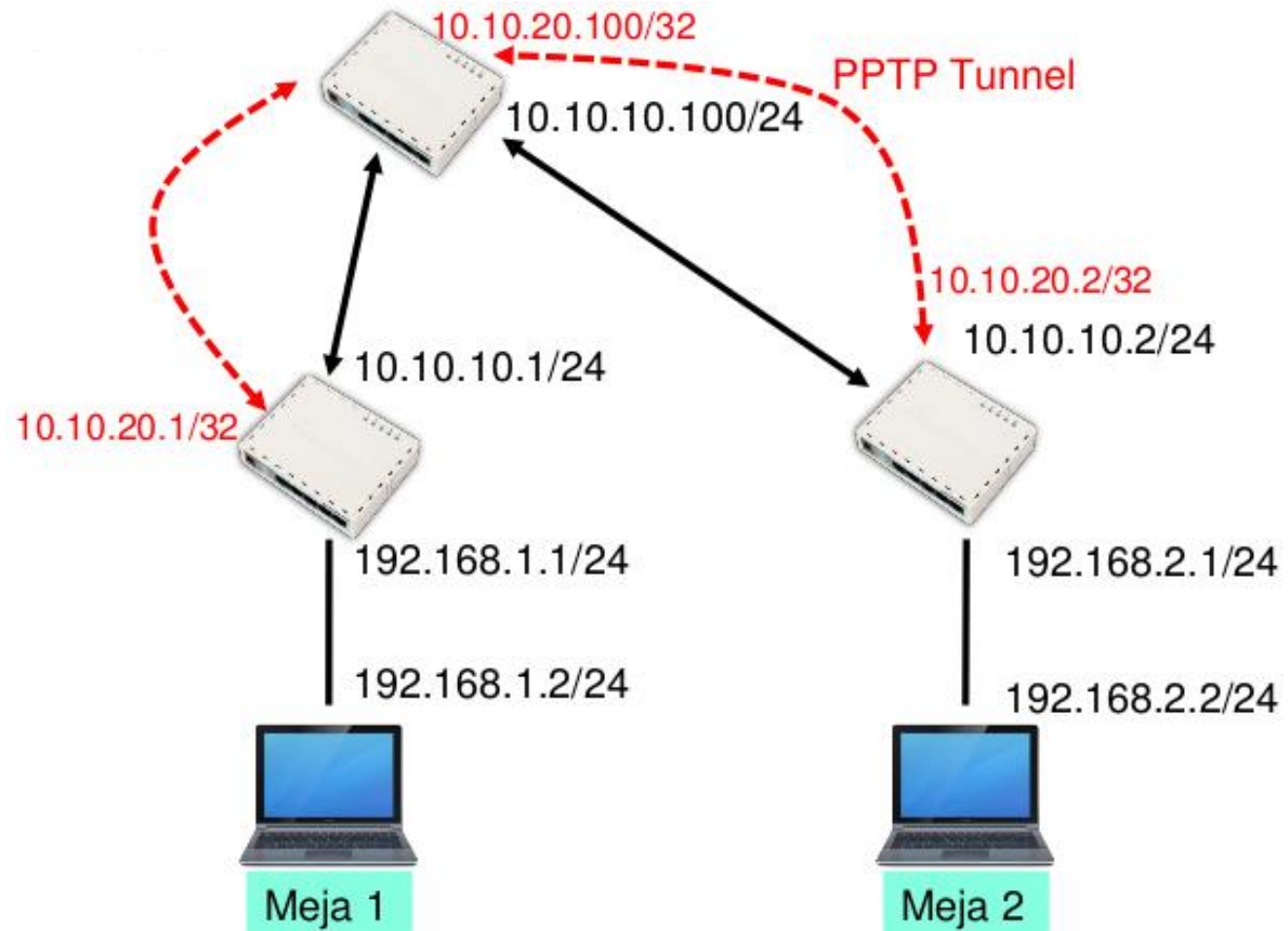
Virtual Private Network,
Jaringan Data yang bersifat independen yang memanfaatkan infrastruktur jaringan public.

VPN bisa diimplementasikan di berbagai tipe network :

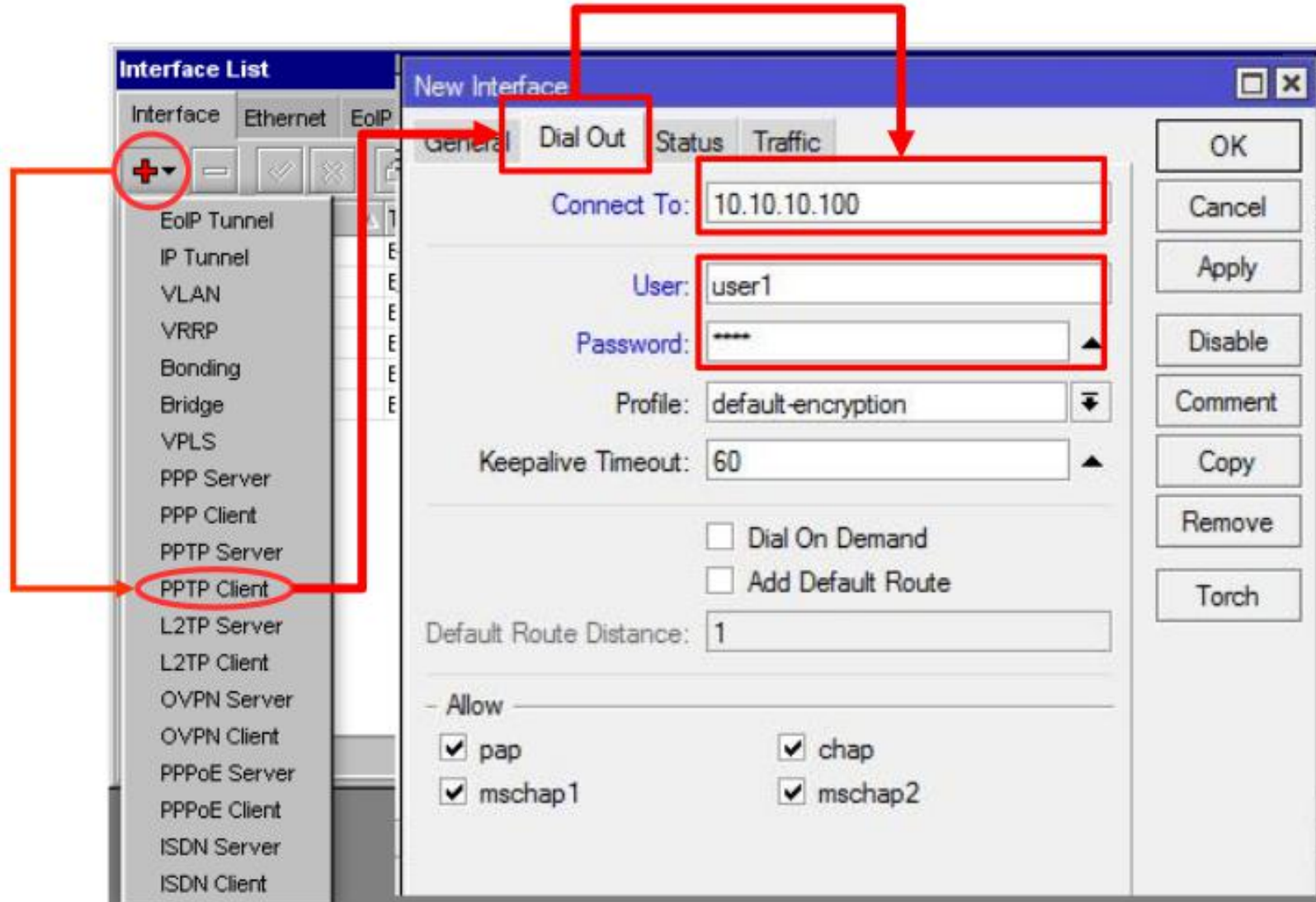
- Routed Network :
 - VPN yang dilakukan di network yang sudah melewati multi hop router atau melewati internet. Contohnya menggunakan **PPTP**
- Bridge Network :
 - VPN yang diimplementasikan di network yang masih satu switch (satu network bridge). Contohnya penggunaan **PPPoE**

(LAB)PPTP Tunnels Client

- Contoh Topologi



(LAB)PPTP Tunnels Client



(LAB)PPTP Tunnels Client

Membuat PPTP-Client :

- **Username** dan **Password** : Sesuaikan dengan konfigurasi server
- **Connect-to** : Parameter Alamat IP dari PPTP-Server
- **Add-Default-Route** : Jika akan menggunakan koneksi PPTP sebagai gateway utama
- **Dial on Demand** : Jika diaktifkan(centang), koneksi PPTP hanya akan aktif ketika digunakan(terdapat trafik)

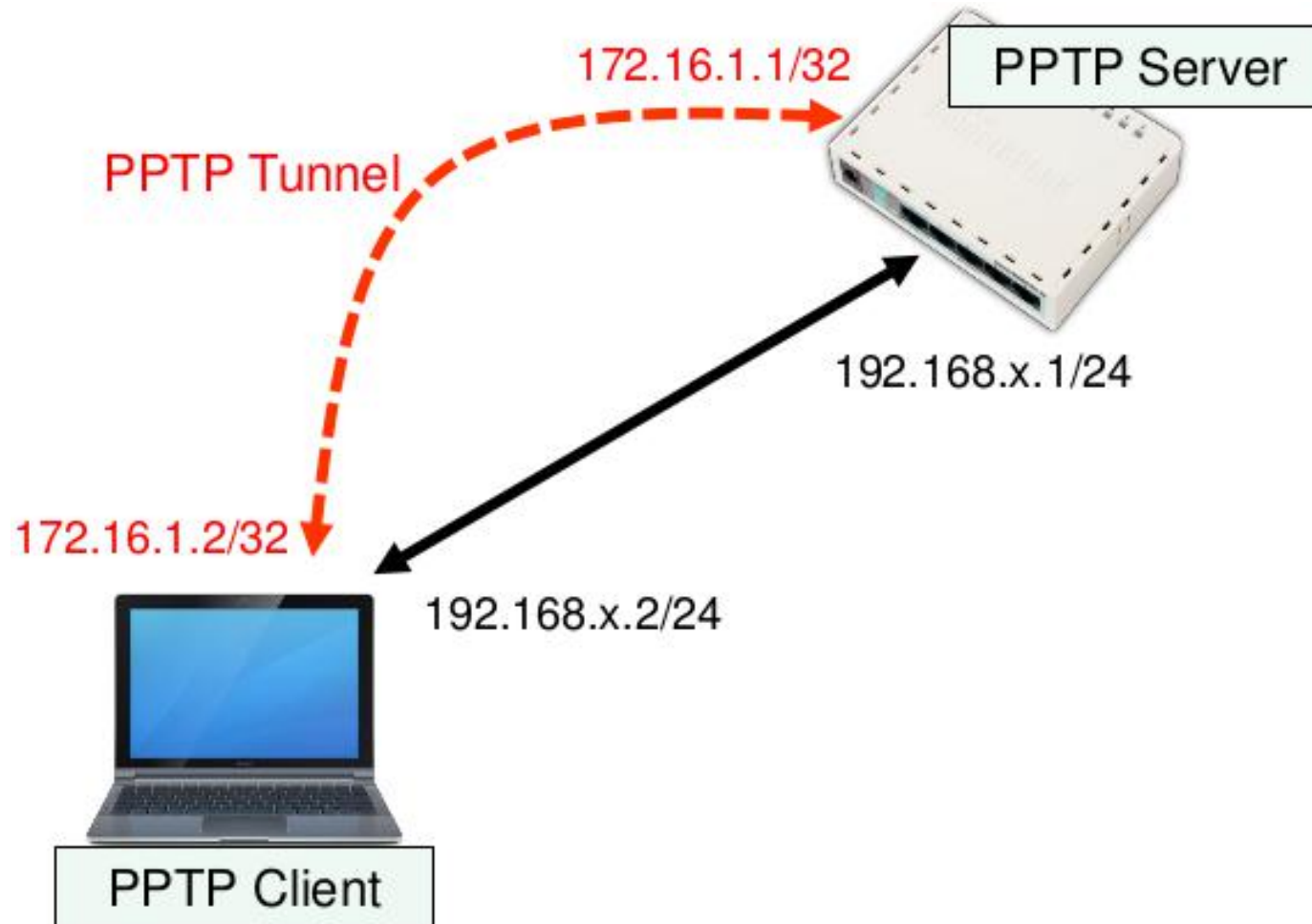
Membuat PPTP-Client Interface :

```
/interface pptp-client add name=pptp-out1 connect-to=10.10.10.100  
user=user1 password=test
```

Point to Point Tunnel Protocol

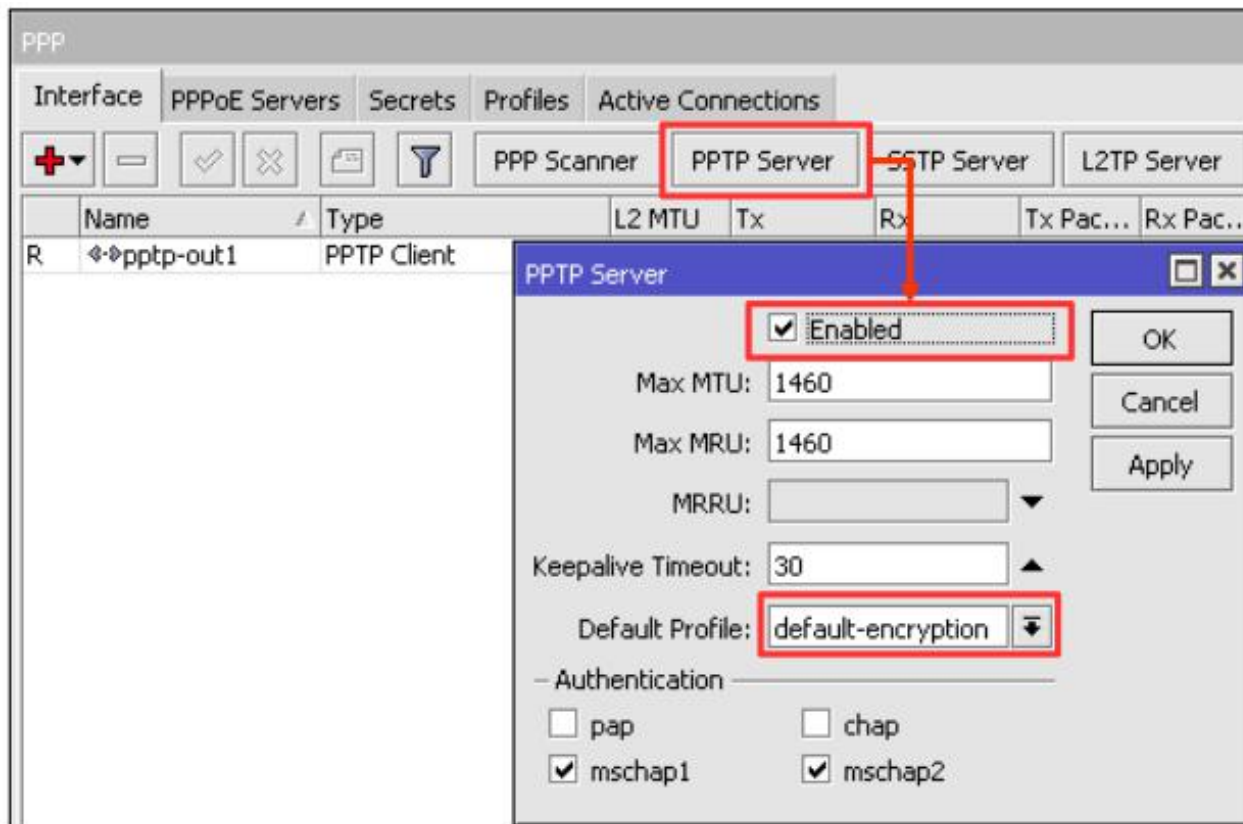
- Penggunaan PPTP Tunnel :
 - Koneksi antar router over Internet yang bersifat secure
 - Untuk menghubungkan jaringan local over WAN
 - Untuk digunakan sebagai mobile client atau remote client yang ingin melakukan akses ke network local(Intranet) sebuah perusahaan
- Sebuah koneksi PPTP terdiri dari Server dan Client
 - MikroTik RouterOS bisa berfungsi sebagai PPTP Server maupun PPTP Client atau gabungan dari keduanya
- Koneksi PPTP menggunakan TCP port 1723 dan IP protocol 47/GRE
- Fungsi PPTP Client sudah tersedia atau termasuk dalam sebagian besar Sistem Operasi

Laptop dial PPTP ke router



(LAB)PPTP Tunnels Server

Aktifkan PPTP Server, pastikan menggunakan profile "default-encryption" supaya link VPN terenkripsi



PPTP Server Configuration

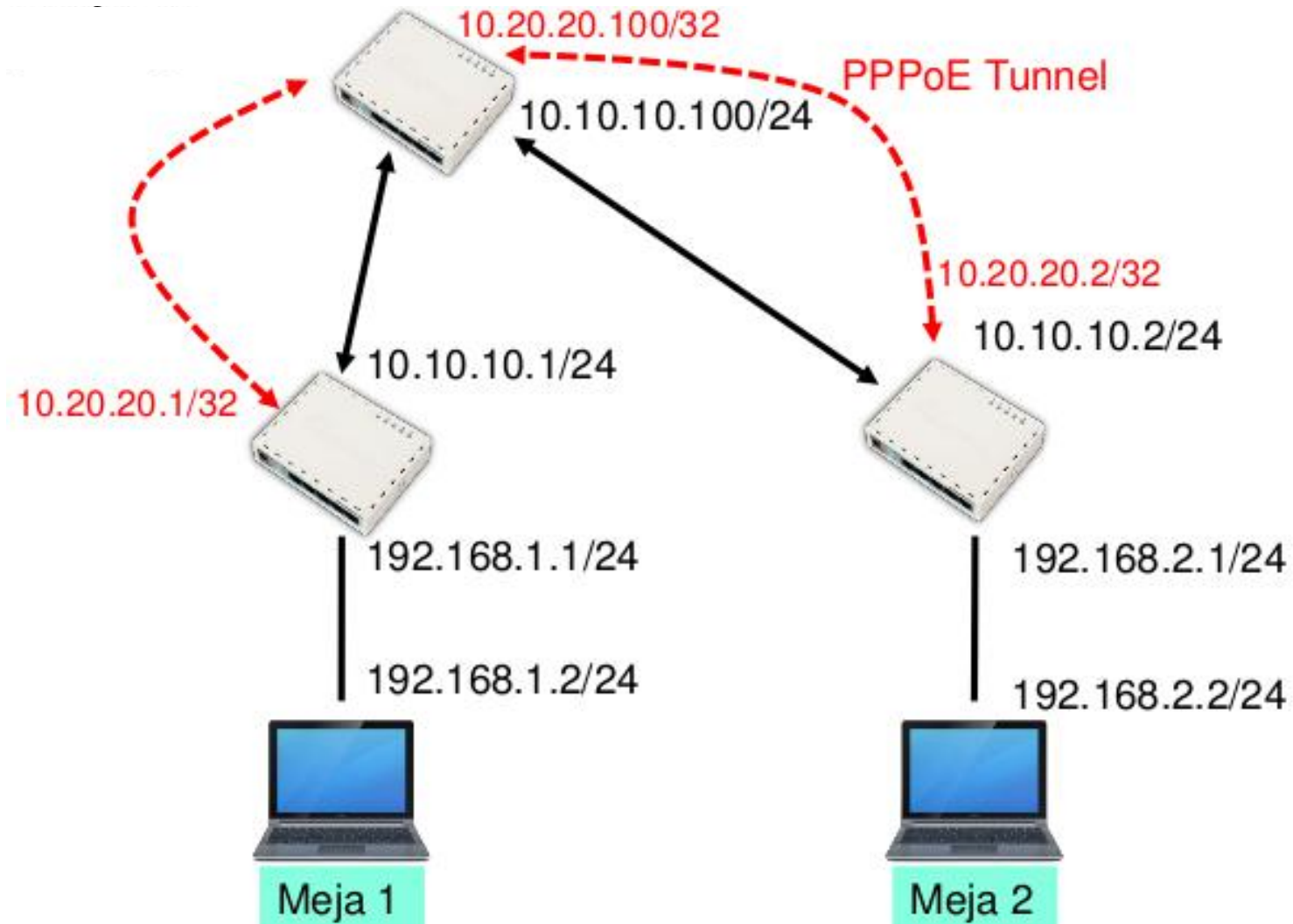
- **Service** PPTP Server bisa diaktifkan pada PPP Configuration
- **Default Profile** digunakan untuk menentukan group dan memberikan konfigurasi dasar seperti IP Address, penggunaan enkripsi, dan juga limitasi user
- Default Profile digunakan untuk user-user yang tidak terdapat di database local router contohnya jika autentikasi user menggunakan Radius

- PPP Secret adalah data user untuk Service VPN (PPTP, PPPoE, OpenVPN, dll) yang ada di local database router, semua konfigurasi user seperti username, password, alokasi IP Address, profile, dan limitasi bisa dilakukan disini
- Ada dua pilihan melakukan assign IP ke user yaitu menggunakan setting di secret (fix IP) atau menggunakan profile (IP Pool)
- VPN User juga bisa menggunakan database user external yaitu menggunakan Radius seperti UserManager atau FreeRadius

Point to Point Protocol over Ethernet

- Penggunaan PPPoE Tunnel :
 - Koneksi antar Client dan Router yang bersifat secure
 - Untuk digunakan sebagai koneksi internet bersifat secure di jaringan local (LAN)
- Sebuah Koneksi PPPoE
 - MikroTik RouterOS bisa berfungsi sebagai PPPoE Server maupun PPPoE Client atau gabungan dari keduanya
- Koneksi PPPoE menggunakan Ethernet frame sebagai protokol transportnya
- Fungsi PPPoE Clients sudah tersedia atau termasuk dalam sebagian besar Sistem Operasi

Topologi



(LAB)PPPoE Client Configuration

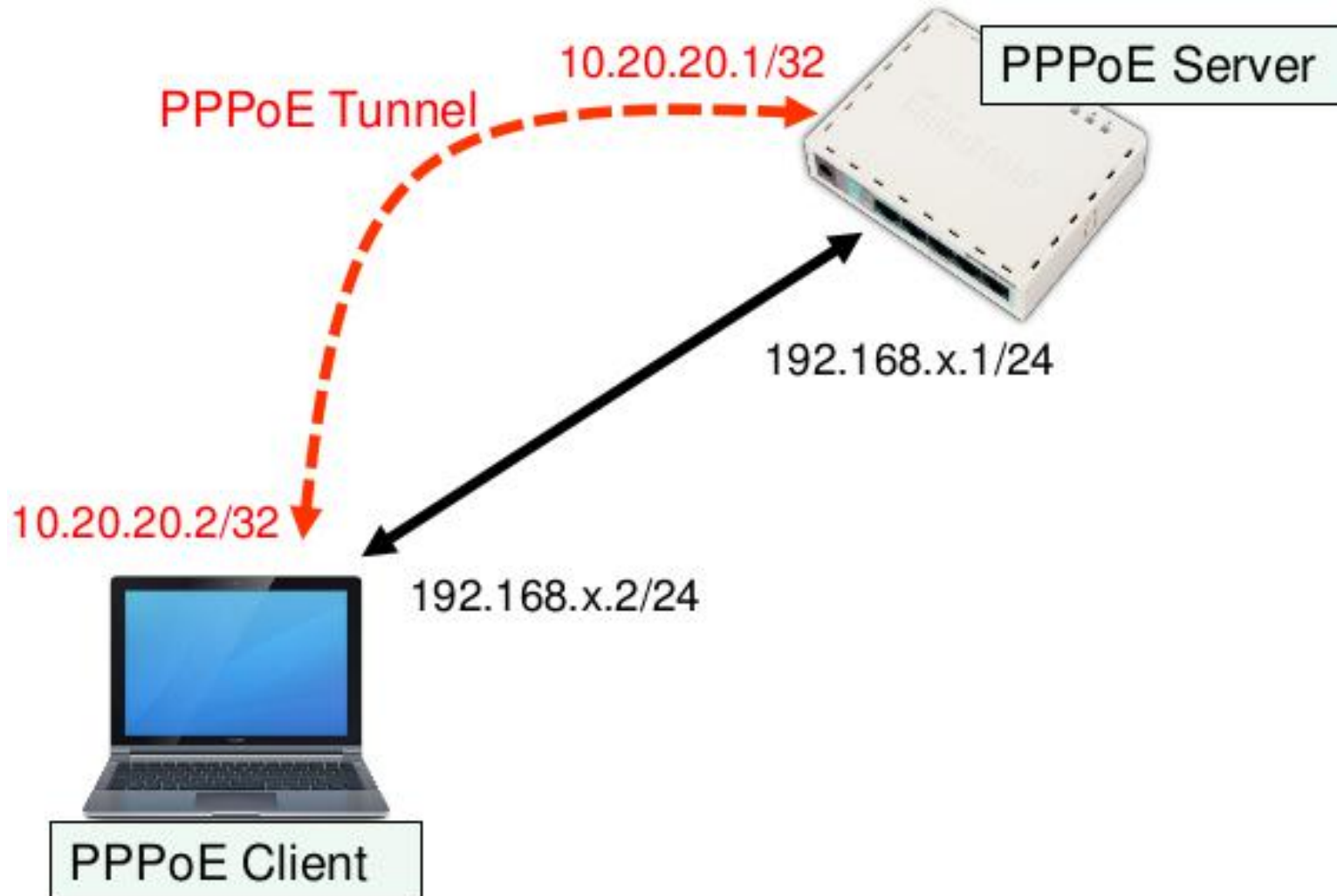
The image displays a network configuration interface with three main panels. The left panel, titled 'PPP', shows a tree view of configuration options. A red box highlights the '+' icon, and another red box highlights 'PPPoE Client' in the list. A red arrow points from 'PPPoE Client' to the 'General' tab of the 'New Interface' configuration window. The middle panel, 'New Interface', has the 'General' tab selected. A red box highlights the 'Name' field containing 'pppoe-out1', and another red box highlights the 'Interfaces' field containing 'wlan1'. A red arrow points from 'wlan1' to the 'Dial Out' tab of the second 'New Interface' configuration window. The right panel, 'New Interface', has the 'Dial Out' tab selected. A red box highlights the 'User' field containing 'user1', and another red box highlights the 'Password' field containing '****'. A red arrow points from 'user1' to the 'Password' field. At the bottom of the configuration windows, there are status indicators: 'enabled' and 'running' for the first window, and 'enabled', 'running', 'slave', and 'Statu' for the second window.

(LAB)PPPoE Client Configuration

Membuat PPPoE-Client pada RouterOS :

- **Interface** : Interface yang terhubung langsung dengan PPPoE Server
- **Username** dan **Password** : Sesuaikan dengan konfigurasi Server
- **Add Default Route** : Aktifkan jika akan menggunakan koneksi PPPoE sebagai Gateway utama
- **Dial on Demand** : Jika diaktifkan, koneksi PPPoE hanya akan aktif ketika digunakan (ada trafik)
- **Use Peer DNS** : Jika akan menggunakan DNS sesuai informasi pada PPPoE Server

Topologi



(LAB)PPPoE Server Configuration

- Aktifkan PPPoE Server pada Interface
- Buat PPP Secret untuk PPPoE Client(Langkahnya hampir sama dengan konfigurasi pada Lab PPTP)
- Dial PPPoE dari Laptop

(LAB)PPPoE Server Configuration

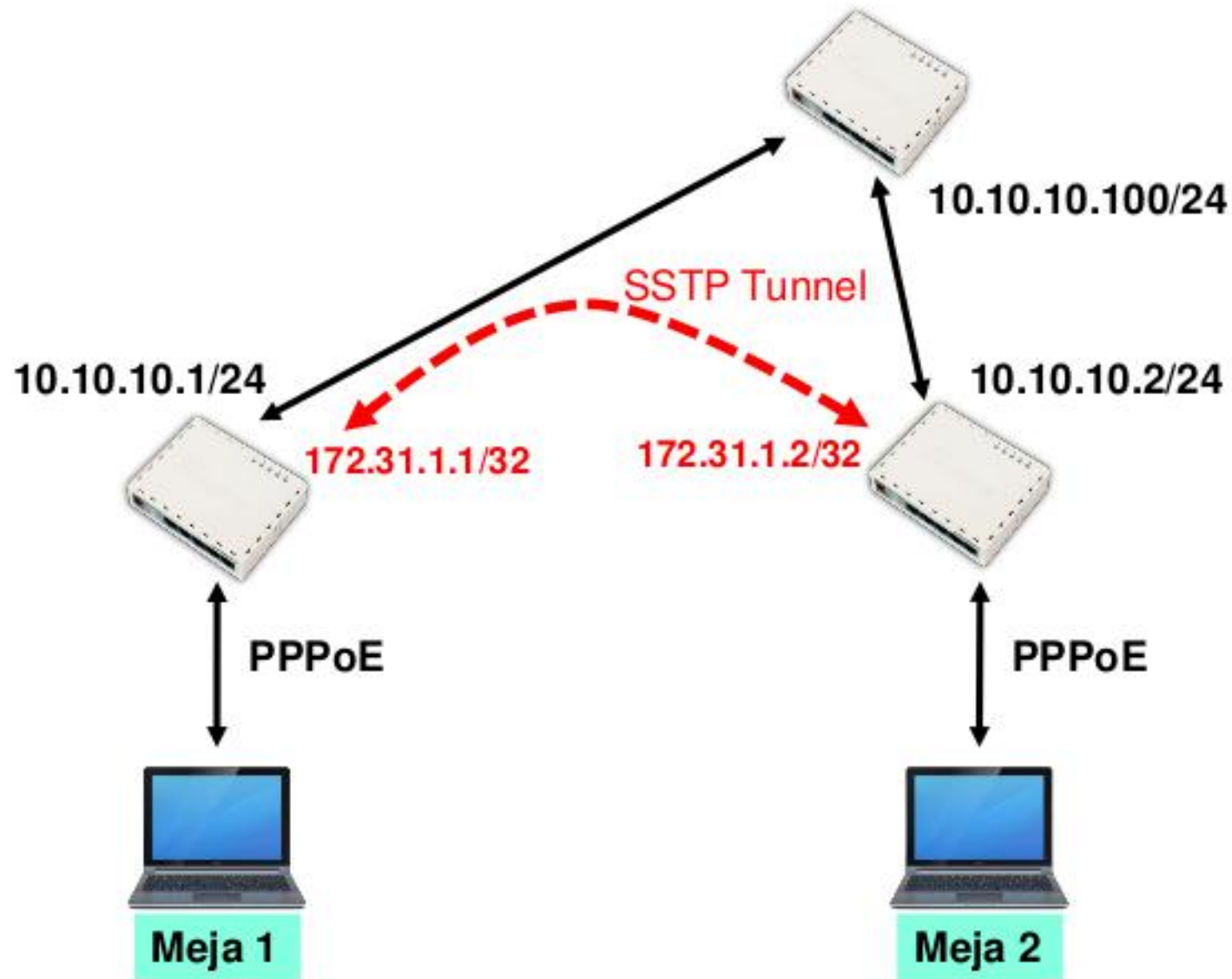
The screenshot displays a network configuration interface with two main panels. The left panel, titled 'ppp', contains a tabbed interface with 'Interface', 'PPPoE Servers', 'Secrets', 'Profiles', and 'Active'. The 'PPPoE Servers' tab is active, showing a table with columns for 'Service ...', 'Interface', 'Max MTU', and 'Max MRU'. A red circle highlights a '+' button in the toolbar above the table. A red box highlights the 'PPPoE Servers' tab, and a red arrow points from this box to the 'Service Name' field in the right panel. The right panel, titled 'New PPPoE Service', contains the following configuration fields:

- Service Name:
- Interface:
- Max MTU:
- Max MRU:
- MRRU:
- Keepalive Timeout:
- Default Profile:
- One Session Per Host
- Max Sessions:

Below these fields is an 'Authentication' section with the following options:

- pap
- chap
- mschap1
- mschap2

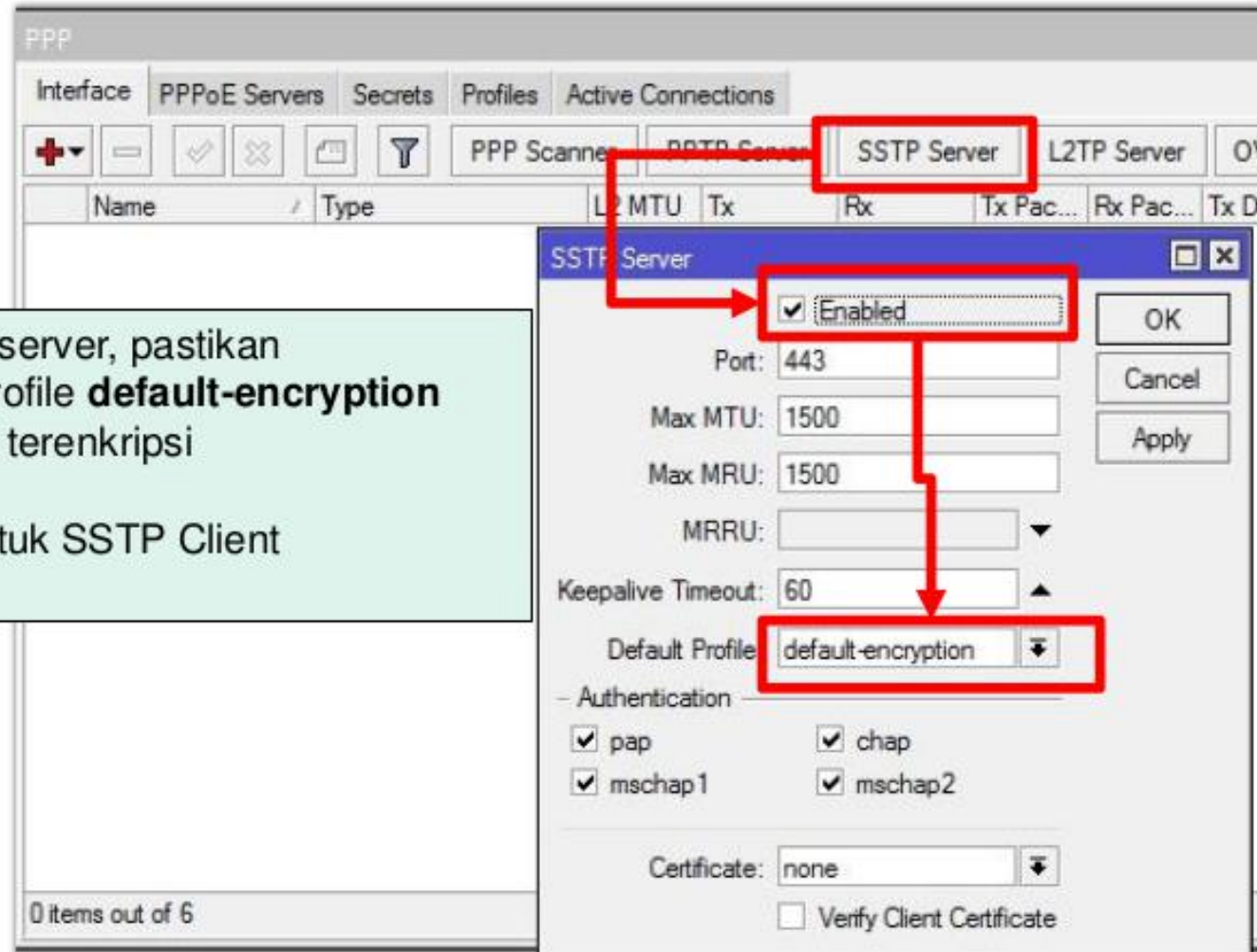
Topologi



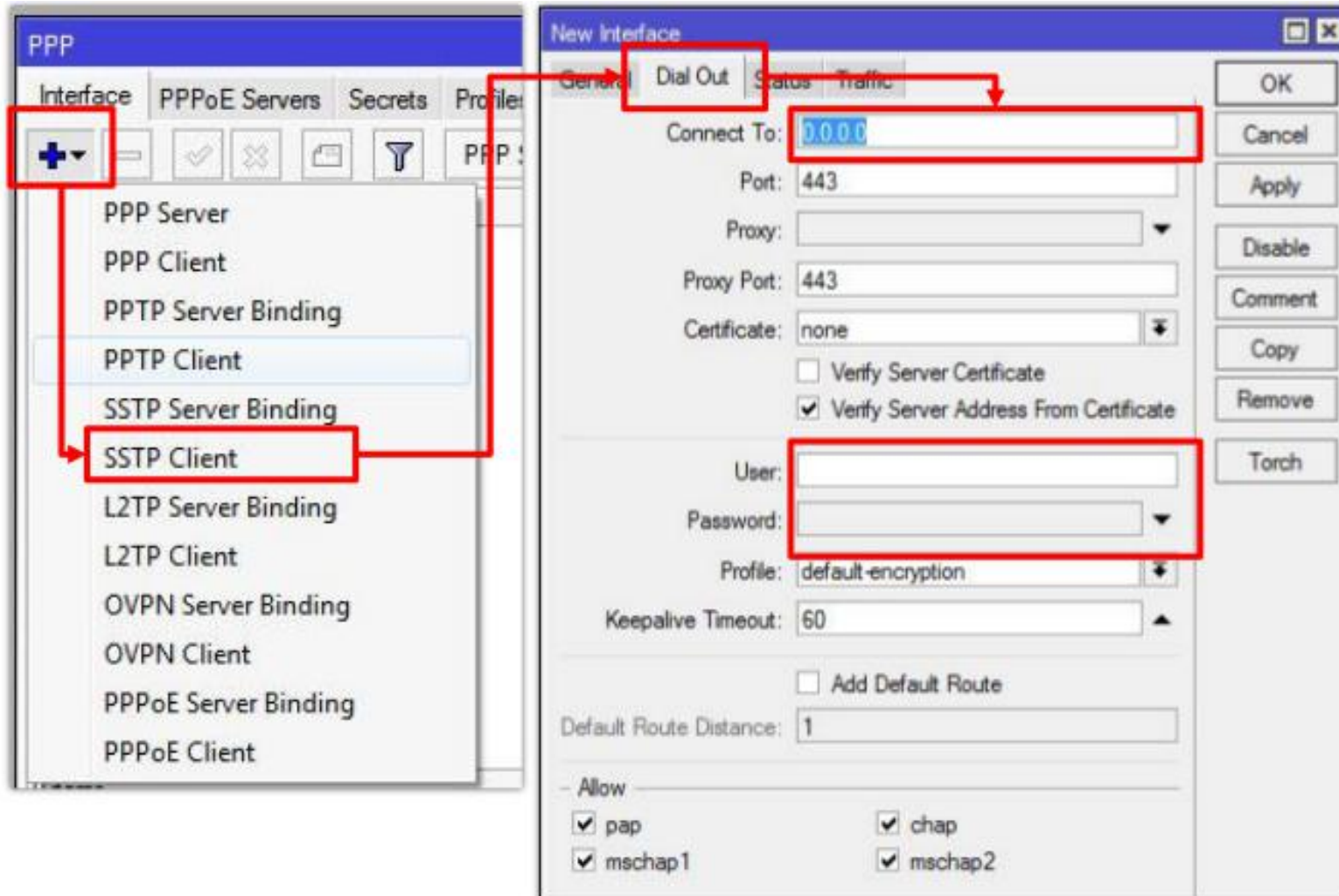
- Buatlah SSTP Tunnel tanpa certificate antar Router, bekerja sama dengan rekan semeja
- Koneksikan laptop dengan Router menggunakan service PPPoE pada masing-masing meja
- Buatlah Static Route agar laptop bisa saling berkomunikasi

(LAB)SSTP Server

- Aktifkan SSTP server, pastikan menggunakan profile **default-encryption** supaya link VPN terenkripsi
- Buat Secret untuk SSTP Client



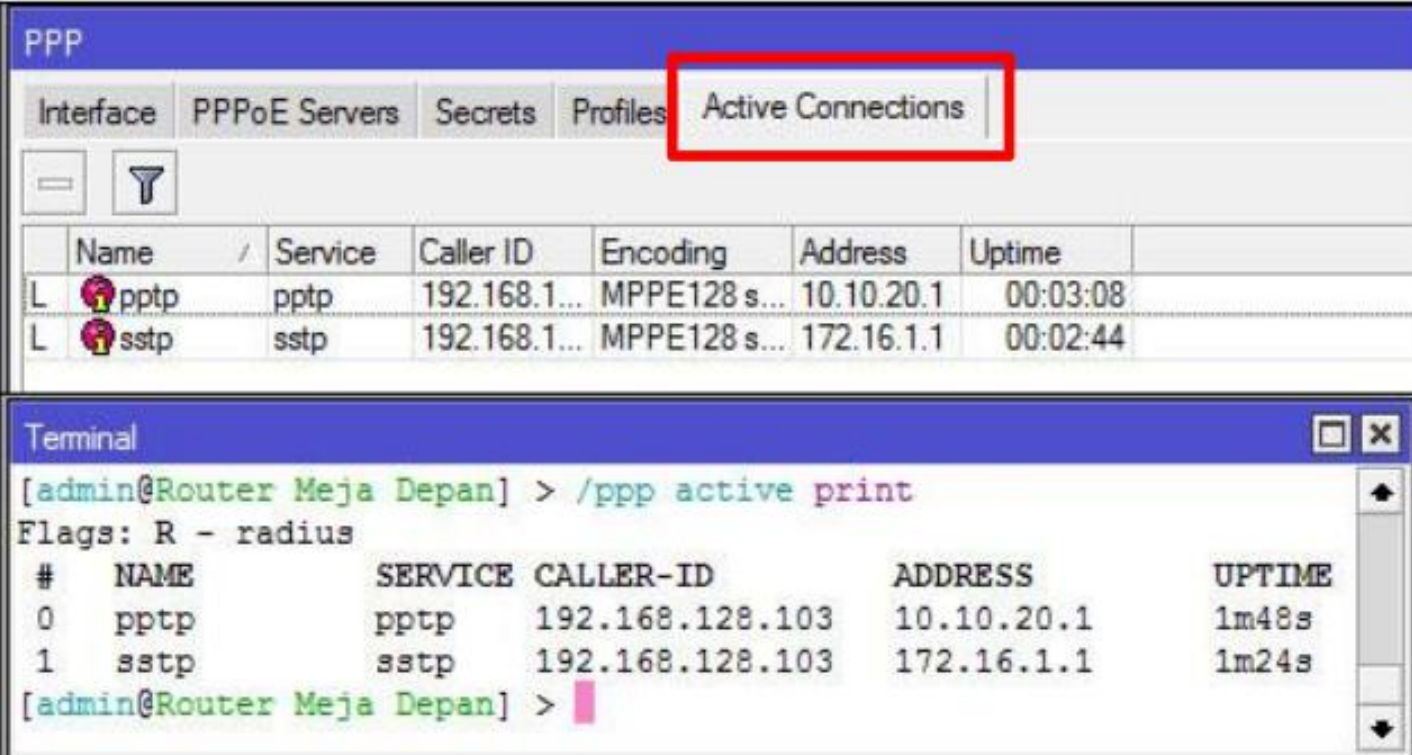
(LAB)SSTP Client



Secure Socket Tunneling Protocol

- PPP Tunnel over SSL
- MikroTik RouterOS bisa berfungsi sebagai SSTP Server maupun SSTP Client atau gabungan dari keduanya
- Dibutuhkan SSL Certificate untuk dapat terkoneksi, baik ada Server maupun Client(tidak berlaku jika keduanya MikroTik RouterOS)
- Koneksi SSTP menggunakan TCP port 443

- Pada sisi Server bisa dilihat berapa banyak koneksi VPN yang terbentuk (aktif)



The image shows a network management interface with a 'PPP' section and a 'Terminal' window. The 'Active Connections' tab is highlighted with a red box. The terminal window shows the command `/ppp active print` and its output, which lists active connections with columns for #, NAME, SERVICE, CALLER-ID, ADDRESS, and UPTIME.

#	NAME	SERVICE	CALLER-ID	ADDRESS	UPTIME
0	pptp	pptp	192.168.128.103	10.10.20.1	1m48s
1	sstp	sstp	192.168.128.103	172.16.1.1	1m24s