MikroTik
ROUTING THE WORLD

IDN.ID
INDONESIAN EXPERT FACTORY

MIKROTIK CERTIFIED NETWORK ASSOCIATE (MTCNA) TRAINING

Presented by: ID-Networkers (IDN.ID)

PERKENALAN

- Nama :
- Asal dari :
- Saat ini kerja di :
- Posisi sebagai :
- Pengalaman di dunia network :
- Pengalaman di MikroTik :
- Harapan :

PREPARATION BEFORE TRAINING

REGISTRASI ACCOUNT DI MIKROTIK.COM

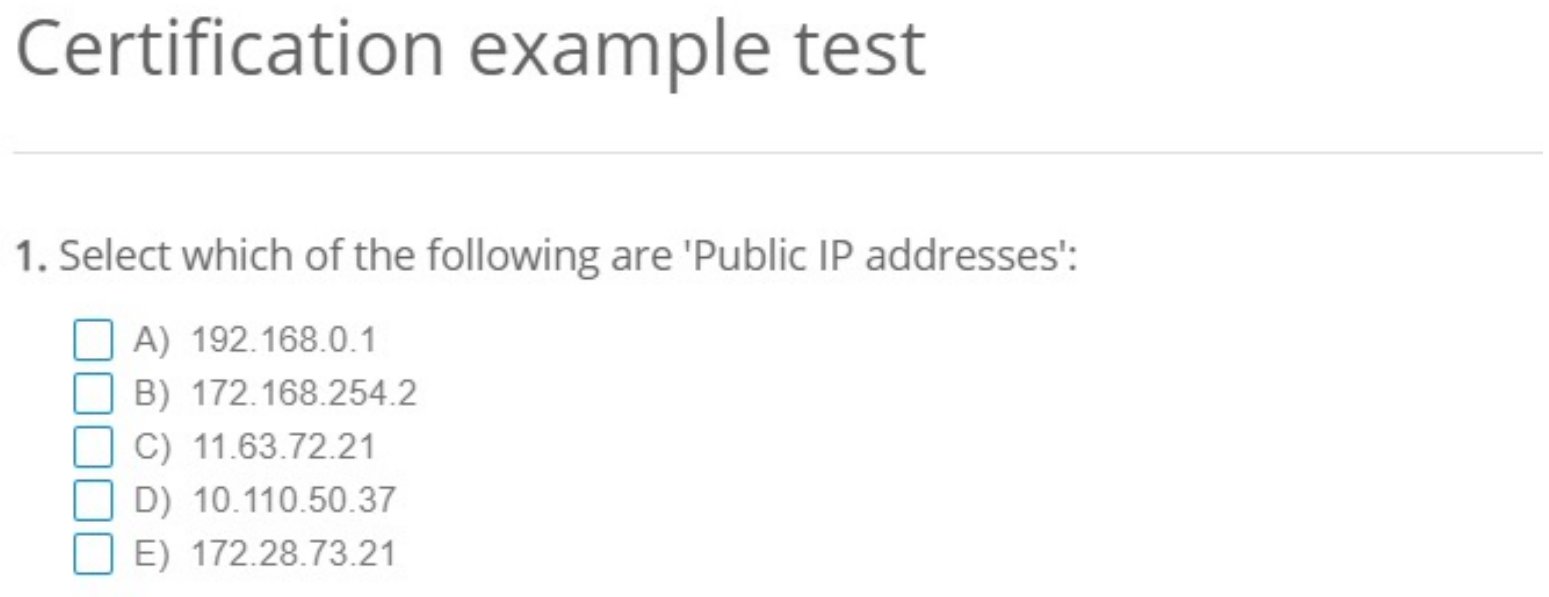
- Untuk training dan ujian MTCNA peserta harus teregistrasi di official web mikrotik
- Register account di www.mikrotik.com, pada menu account isi semua form yang disediakan
- Pastikan nama anda ditulis lengkap dalam profil,karena otomatis akan tercetak dalam sertifikat.

TENTANG UJIAN MTCNA

- **Online test** terdiri atas **25 soal** dalam waktu **1 jam.**
- Sistem Penjawaban **Pilihan Ganda** (*Single, Multiple, True/False*), tidak ada **LAB dan Esai**.
- Soal setiap **test random**, dengan beberapa soal mungkin ada yang sama dengan soal sebelumnya.
- Passing grade **60%,** nilai **50%-59%** bisa test ulang (*Second Chance*).
- **Hati-hati membaca soal**, disamping bahasa inggris dari soal yang kadang-kadang kurang mudah dipahami, juga banyak jebakan batman .
- Syarat Mikrotik Academy, Mikrotik Consultant, Trainer nilai harus minimal 75% untuk Associate level (MTCNA) dan engineer level (MTC*E).

LATIHAN TEST

- Latihan ujian MTCNA ada di menu Account -> My training session ->Try example test



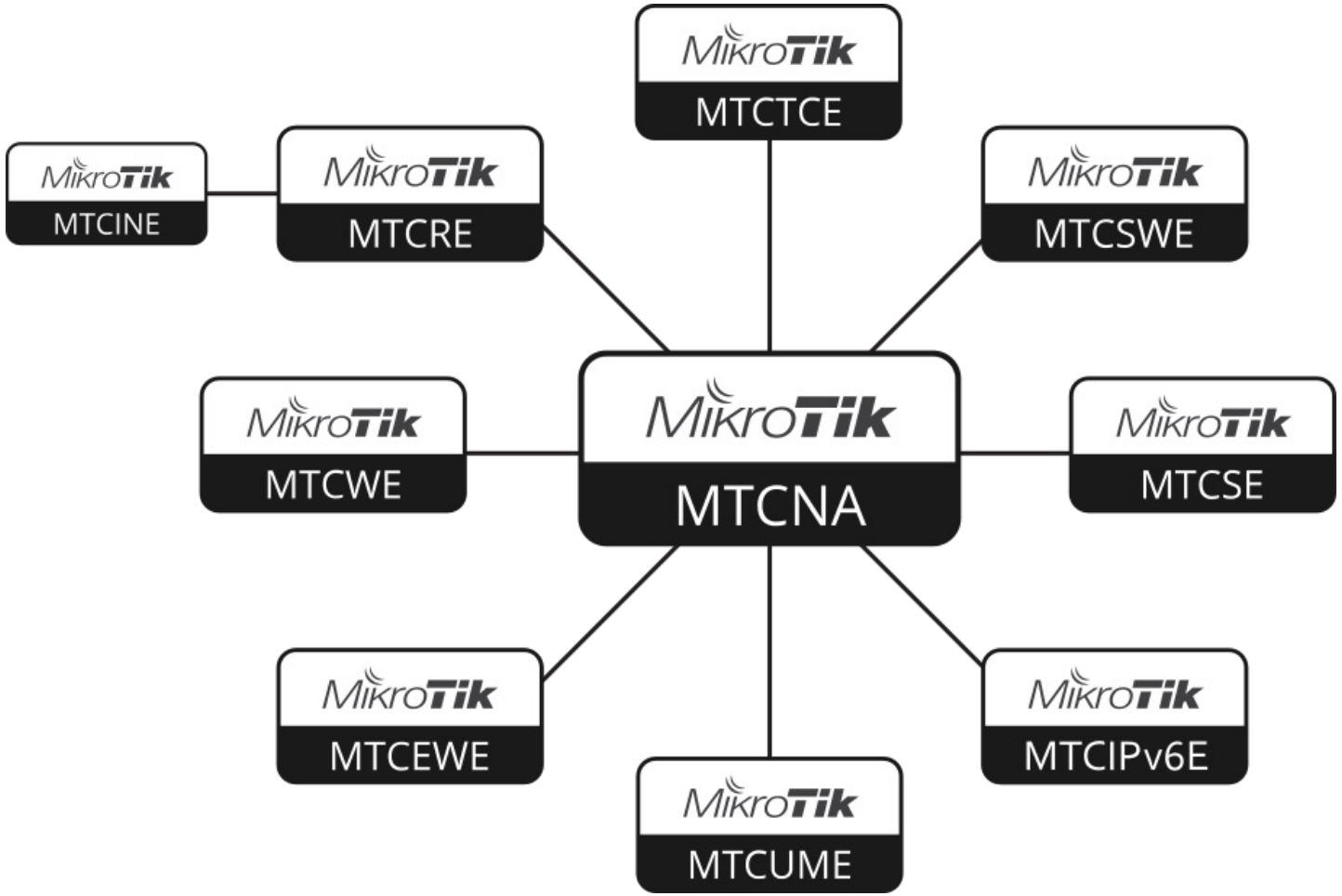
- NB : Soal pada Example Test, tidak akan ada yang keluar pada Exam Mikrotik

TUJUAN TRAINING MTCNA

- Mempelajari karakteristik, fitur-fitur dan kemampuan MikroTik RouterOS.
- Mempelajari cara instalasi, konfigurasi, fungsi, maintenance dan troubleshooting dasar MikroTik RouterOS.
- Mendapatkan kualifikasi sebagai MikroTik Certified Network Associate.

SERTIFIKASI MIKROTIK

- Sertifikasi berjenjang, kalau belum lulus MTCNA belum bisa ikut ujian level engineer
- Masa berlaku sertifikat selama 3 tahun, setelah itu bisa diperpanjang dengan cara ujian lagi
- Jika Sertifikasi Expired, tetap bisa mengikuti Sertifikasi Next Level



SERTIFIKASI MIKROTIK

MikroTik certified training programs

- **MTCNA** - MikroTik Certified Network Associate (view outline)
- **MTCRE** - MikroTik Certified Routing Engineer (view outline)
- **MTCWE** - MikroTik Certified Wireless Engineer (view outline)
- **MTCTCE** - MikroTik Certified Traffic Control Engineer (view outline)
- **MTCUME** - MikroTik Certified User Management Engineer (view outline)
- **MTCINE** - MikroTik Certified Inter-Networking Engineer (view outline)
- **MTCIPv6E** - MikroTik Certified IPv6 Engineer (view outline)
- **MTCSE** - MikroTik Certified Security Engineer (view outline)
- **MTCSWE** - MikroTik Certified Switching Engineer (view outline)
- **MTCEWE** - MikroTik Certified Enterprise Wireless Engineer (view outline)

- NB : Link untuk melihat lebih lengkap Serifikasi Mikrotik
www.mikrotik.com/training/about

MTCNA–OUTLINE

- Modul 1 – Introduction
- Modul 2 - DHCP dan ARP
- Modul 3 - Bridge
- Modul 4 - Routing
- Modul 5 - Wireless
- Modul 6 - Firewall
- Modul 7 - QoS
- Modul 8 - Tunnel
- Modul 9 - Misc

MODUL 1
INTRODUCTION MIKROTIK

SEJARAH MIKROTIK

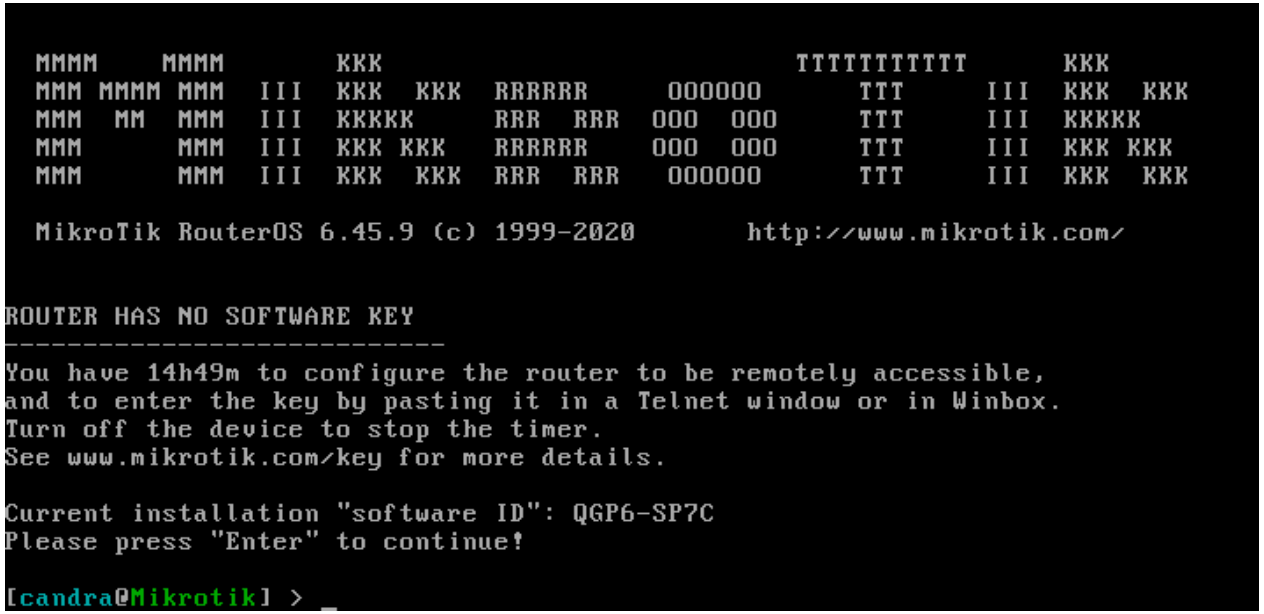
- Founder (1996) : **John Trully & Arnis Reikstins.**
- Lokasi : Riga, Latvia (Eropa Utara)
- Produsen Software dan Hardware Router.
- Menjadikan teknologi internet lebih murah, cepat, handal dan terjangkau luas.
- Motto Mikrotik : **Routing the World.**

MIKROTIK TIMELINE

- 1996 : Founded
- 1997 : RouterOS software x86 (PC)
- 2002 : Perangkat RouterBOARD pertama
- 2006 : MikroTik User Meeting (MUM) pertama Prague, Czech Republic
- 2015 : MUM terbesar : Indonesia, 2500+

MIKROTIK ROUTEROS

- System Operasi yang digunakan oleh perangkat Mikrotik RouterBOARD.
- Dapat diinstall di PC atau sebagai VM (Virtual Machine).
- Stand-alone operating system berbasis Linux v3.3.5 kernel.



MIKROTIK ROUTERBOARD

- Built in hardware (board).
- Dibuat untuk menjalankan sistem operasi RouterOS.
- Tersedia mulai dari low-end s/d high-end router.

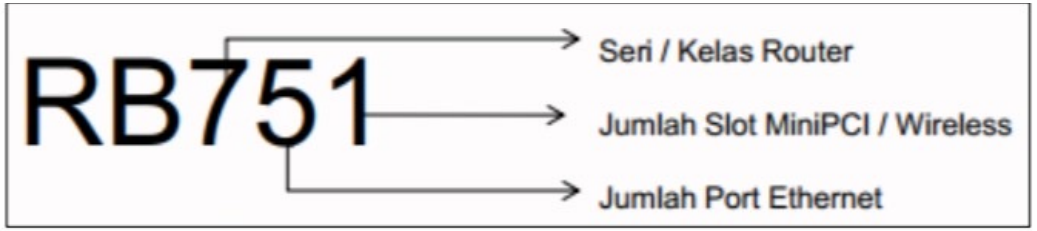
ROUTEROS FEATURES

- Support 802.11 a/b/g/n/ac wireless network.
- Routing (RIP, OSPF, BGP, RIPng, OSPFv3).
- Firewall & NAT (Fully-customized, linux based).
- QoS / Bandwidth (Fully-customized, linux based).
- Point to point tunneling (PPTP, PPPoE, SSTP, OpenVPN).
- User Management (DHCP / Proxy / Hotspot / Radius, dll).
- Tools (Bandwidth test, torch, mac-ping, MRTG, dll)

https://wiki.mikrotik.com/wiki/Manual:RouterOS_features

ROUTERBOARDNAME

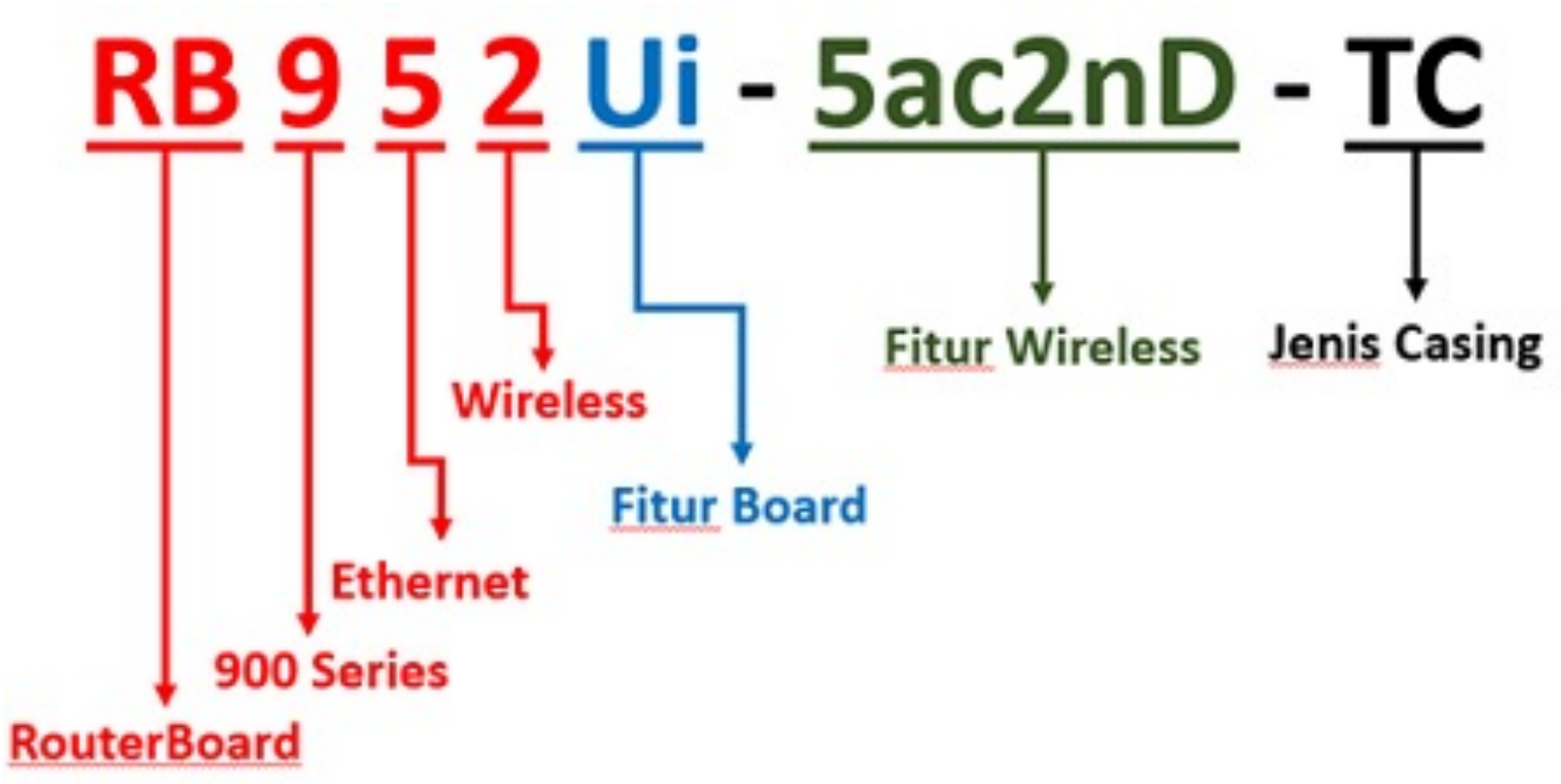
- 3-symbol name



- Word
  - OmniTIK, Groove, SXT, LHG, DynaDish, cAP, wAP, hAP, hEX

- Exceptional naming
  - Nama disederhanakan dan disesuaikan dengan tahun pengembangan, dan biasanya ethernet nya lebih dari 9 port.
  - Contoh : RB600, 800, 1000, 1100, 1200, 2011, 3011, 4011

ROUTERBOARD-TYPE



ROUTERBOARD-TYPE

Kode lain yang ada pada RouterBOARD :

- U – Support port USB
- A – Memory lebih tinggi dan dan level lisensi lebih tinggi
- H – more powerfull CPU
- G – Support port Gigabit
- S – Support port SFP
- 5 – Support frekuensi 5Ghz
- 2 – Support frekuensi 2,4Ghz
- 52 – dual band 5Ghz dan 2,4Ghz
- TC – Tower (vertical) case

- NB : Link untuk melihat Product Naming Mikrotik lebih lengkap
www.wiki.mikrotik.com/wiki/Manual:Product_Naming

ARSITEKTUR ROUTERBOARD

- Arsitektur RouterBoard dibedakan berdasarkan jenis dan kinerja processor.
- software/OS untuk setiap arsitektur berbeda

mipsbe	BaseBox, CRS series, NetBox, NetMetal, PowerBox, QRT, RB4xx series, RB7xx series, RB9xx series, cAP, mAP, hEX, DynaDish, RB2011 series, SXT, OmniTik, Groove, Metal, Sextant
ppc	RB3xx series, RB600 series, RB800 series, RB1100, RB1000
x86	PC / X86, RB230 series
mipsle	RB1xx series, RB5xx series, Crossroads
tile	CCR series
smips	hAP lite

- NB : Link untuk melihat Arsitektur Mikrotik lebih lengkap

www.mikrotik.com/download

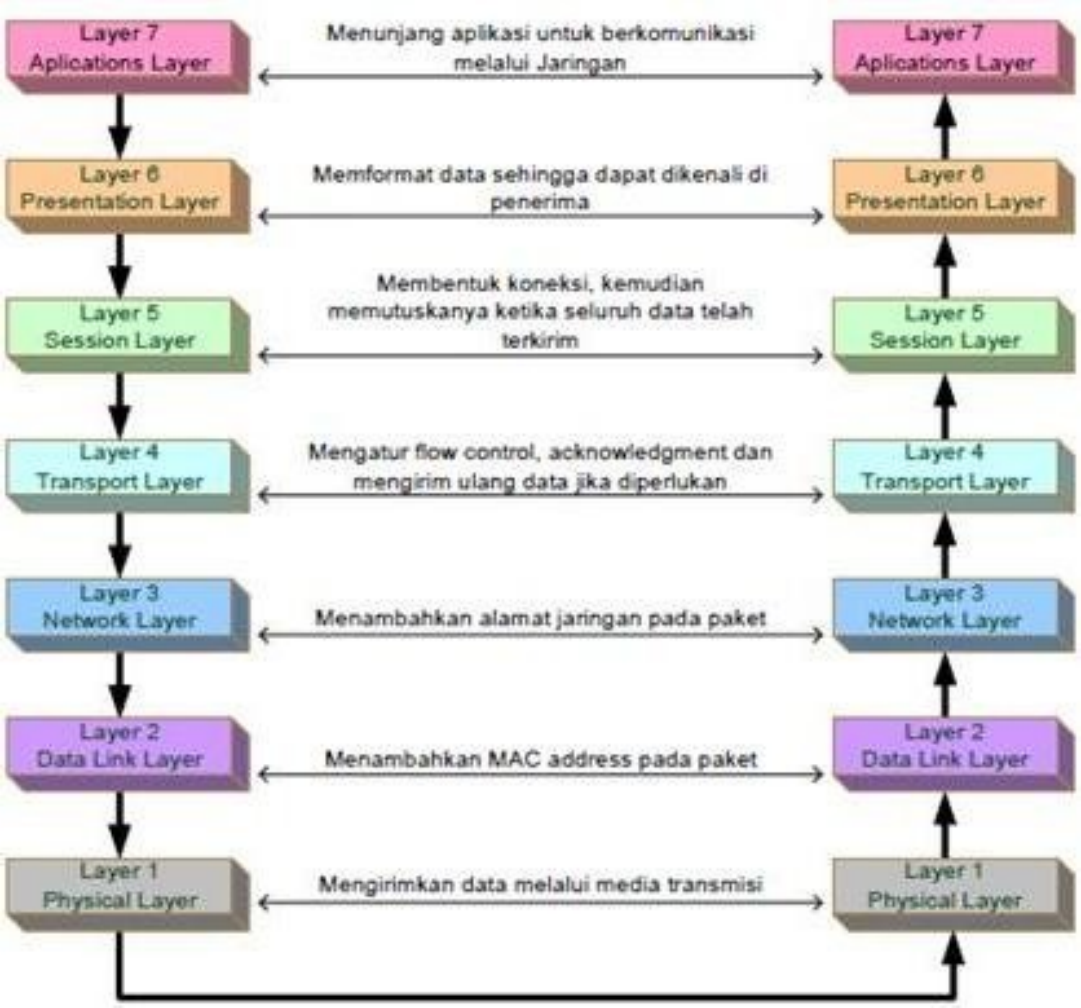
PREREQUISITES MTCNA TRAINING

TCP/IP BASIC

OSI LAYER MODEL

- Tidak adanya suatu protokol yang sama, membuat banyak perangkat tidak bisa saling berkomunikasi.
- ***Open System Interconnection*** atau OSI layer 7 *adalah model* arsitektural jaringan yang dikembangkan oleh International Organization for Standardization (ISO) di Eropa tahun1977.
- Sebelum ada OSI, sistem jaringan **sangat tergantung kepada vendor** pemasok perangkat jaringan yang berbeda-beda.
- Model Osi layer 7 merupakan koneksi logis yang harus terjadi agar terjadi komunikasi data dalam jaringan.

OSI LAYER MODEL



OSI LAYER MODEL

Layer	Name	Device	Data Unit	Addressing
Layer 3	Network	Router	Paket	IP Address
Layer 2	Data Link	Switch	Frame	MAC Address
Layer 1	Physical	Hub	Bit	0111001110

PROTOCOL – TCP & UDP

- TCP is more reliable.
- TCP digunakan untuk IP karena support Error Checking.

- UDP is more faster.
- UDP digunakan untuk video streaming, games, dan aplikasi lain yang membutuhkan kecepatan data.

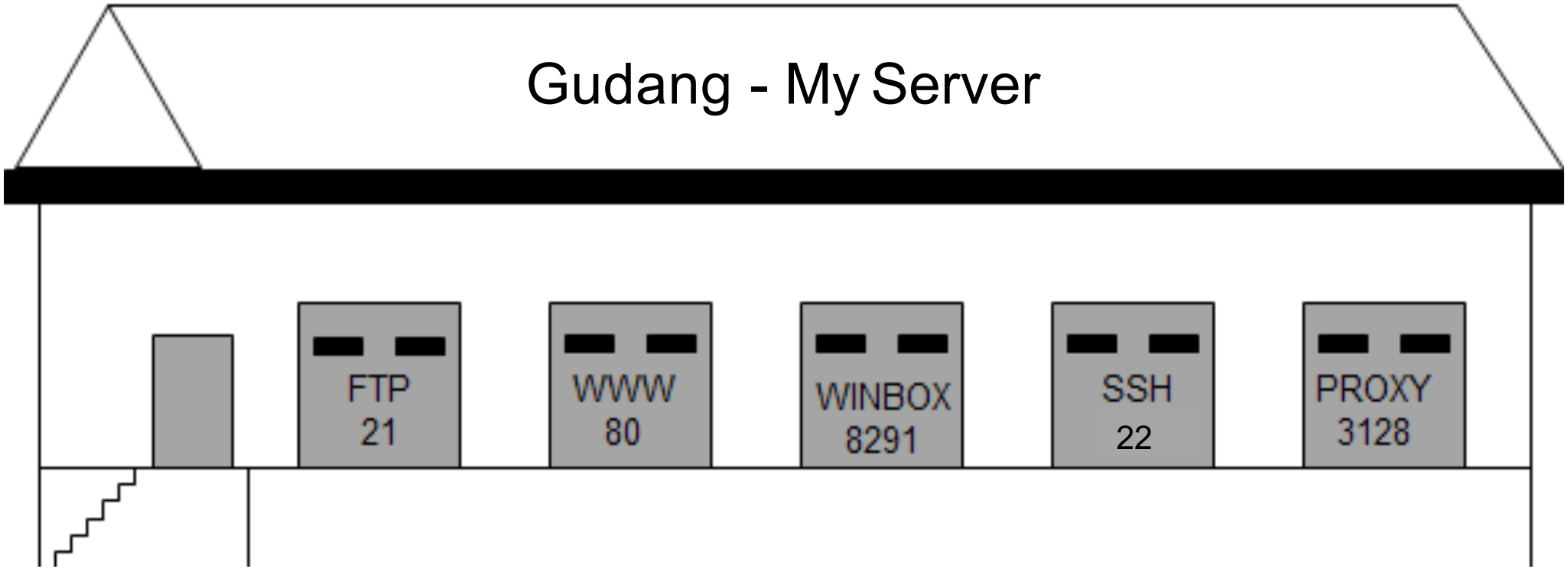
PORT

- Pintu Masuk.
- Digunakan untuk menjalankan service pada komunikasi jaringan.
- Terdapat total 65535, dengan klasifikasi sebagai berikut :
  - 0 - 1023 (well known ports),
  - 1024 – 49151 (registered ports),
  - 49152 – 65535 (unregistered / dynamic, private or ephemeral ports)

PORT YANG BIASA DIGUNAKAN

Port No	Protocol	Service	Remark
21	TCP	FTP	File Transfer Protocol
23	TCP	Telnet	Remote access
25	TCP	SMTP	Simple Mail Transfer Protocol
53	UDP	DNS	Domain Name Server
80	TCP	HTTP	Hypertext Transfer Protocol
110	TCP	POP3	Post Office Protocol v3
123	UDP	NTP	Network Time Protocol
137	TCP	NetBIOS-ns	NetBIOS – Name Service
161	UDP	SNMP	Simple Network Monitoring Protocol
3128	TCP	HTTP - Proxy	Web-Cache (default by Squid)
8080	TCP	HTTP - Proxy	Web-Cache (customized)

PORT ANALOGI



MAC ADDRESS

- MAC Address (Media Access Control Address) adalah alamat jaringan pada lapisan data-link (layer 2) dalam OSI 7 Layer Model.
- Dalam sebuah komputer, MAC address ditetapkan ke sebuah kartu jaringan (network interface card/NIC).
- MAC address merupakan alamat yang unik yang memiliki panjang 48-bit.
- MAC terdiri atas 16 digit bilangan heksadesimal (0 s/d F),
- **6 digit pertama** merepresentasikan **vendor pembuat kartu jaringan**.
- Contoh MAC Address : **02-00-4C**-4F-05-50.

IP ADDRESS

- IP (Internet Protocol) terdapat dalam Network Layer (layer 3) OSI.
- Digunaddressakan untuk komunikasi antar perangkat jaringan.
- Terdapat 2 jenis IP Address
  - IPv4

    Pengalamatan 32 bit,

    IPv4 terbagi menjadi 4 blok (setiap blok ada 8 bit) X.X.X.X

    Jumlah max host 4,294,967,296
  - IPv6

    Pengalamatan 128 bit,

    IPv4 terbagi menjadi 8 blok (setiap blok ada 16 bit) X.X.X.X.X.X.X.X

    Jumlah max host 340,282,366,920,938,463,463,374,607,431,768,211,456

IPV4 – PEMBAGIAN KELAS

- **Kelas A**

- **Kelas B**

- **Kelas C**

IP PRIVAT

- Berdasarkan jenisnya IP address dibedakan menjadi IP Public dan IP Private.
- IP Public adalah IP addres yang digunakan untuk koneksi jaringan global (internet) secara langsung dan bersifat unik.
- IP Private digunakan untuk jaringan lokal (LAN)
- Alokasi IP Privat adalah sbb:

RFC1918 name	IP address range	number of addresses
24-bit block	10.0.0.0 – 10.255.255.255	16,777,216
20-bit block	172.16.0.0 – 172.31.255.255	1,048,576
16-bit block	192.168.0.0 – 192.168.255.255	65,536

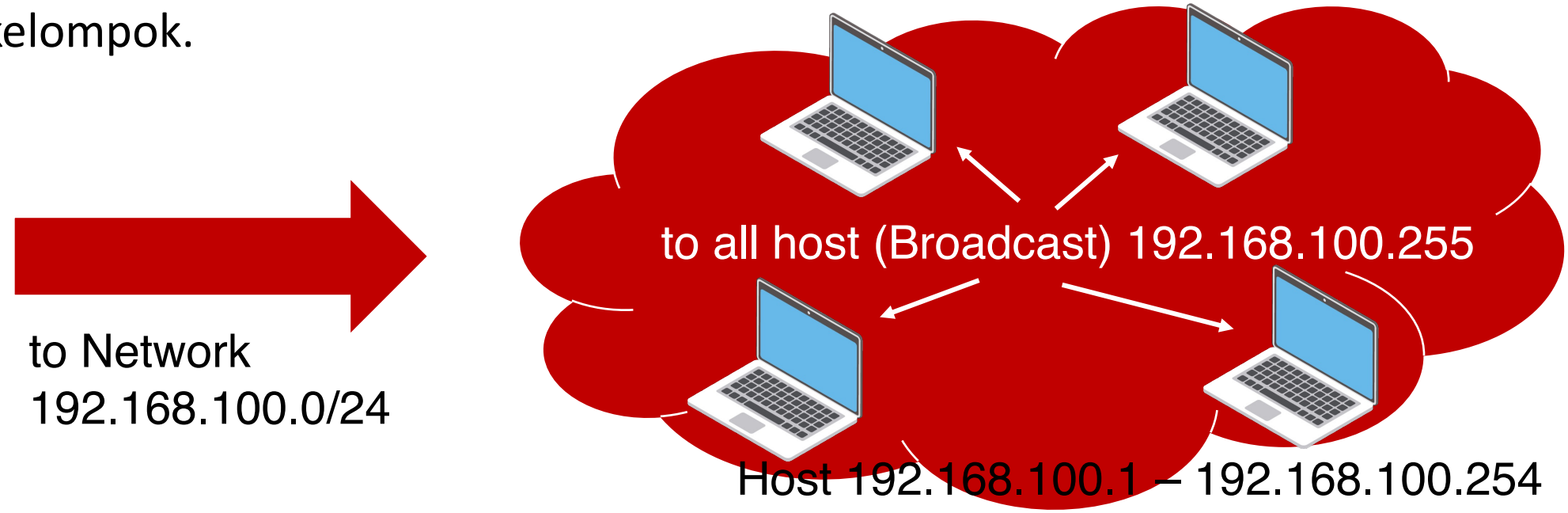
SUBNETTING

- Subnetting adalah cara untuk memisah dan mendistribusikan beberapa IP address.
- Host / Perangkat yang terletak pada subnet yang sama dapat berkomunikasi satu sama lain secara langsung (tanpa router/routing).
- Subnet ditulis dalam format 32 bit (seperti IP) atau dalam bentuk decimal (prefix lenght)

Kelas	Subnet mask (binner)	Subnet	Prefix Length
A	11111111.00000000.00000000.00000000	255.0.0.0	/8
B	11111111. 11111111.00000000.00000000	255.255.0.0	/16
C	11111111. 11111111. 11111111.00000000	255.255.255.0	/24

NETWORK ID DAN BROADCAST

- Dalam kelompok IP address atau satu subnet ada 2 IP yang sifatnya khusus
  - Network ID : identitas suatu kelompok IP / Subnet.
  - Broadcast : alamat IP yang digunakan untuk memanggil semua IP dalam satu kelompok.



PERHITUNGAN IP SUBNET

Tabel Subnetting

Prefix	Subnet Mask 255.255.255.(256-jml IP)	Jumlah IP	Jumlah Host (Jml IP – 2)
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2
/31	255.255.255.254	2	-
/32	255.255.255.255	1	-

LATIHAN

- 103.120.130.10/29
- 202.130.140.20/28
- 192.168.100.1/27
- 172.16.200.1/25

AKSES ROUTEROS

AKSES KE MIKROTIK ROUTEROS

Akses Via	Koneksi	Text Base	GUI	Need IP
Keyboard	Langsung di PC	Yes	-	-
Serial Console	Konektor Kabel Serial	Yes	-	-
Remote Server (Telnet / SSH)	Layer 3	yes	-	yes
Winbox	Layer 2	yes	yes	-
FTP	Layer 3	yes	-	yes
API	Socket Programming	-	-	yes
Quick Set & WebFig (HTTP)	Layer 3	Yes	yes	yes
MAC-Telnet	Layer 2	Yes	-	no
Local (Winbox Terminal Menu)	Terminal winbox	Yes	-	-
Mikrotik TikAPP	Android / iOS	Yes	yes	yes

MENGAKSES MIKROTIK

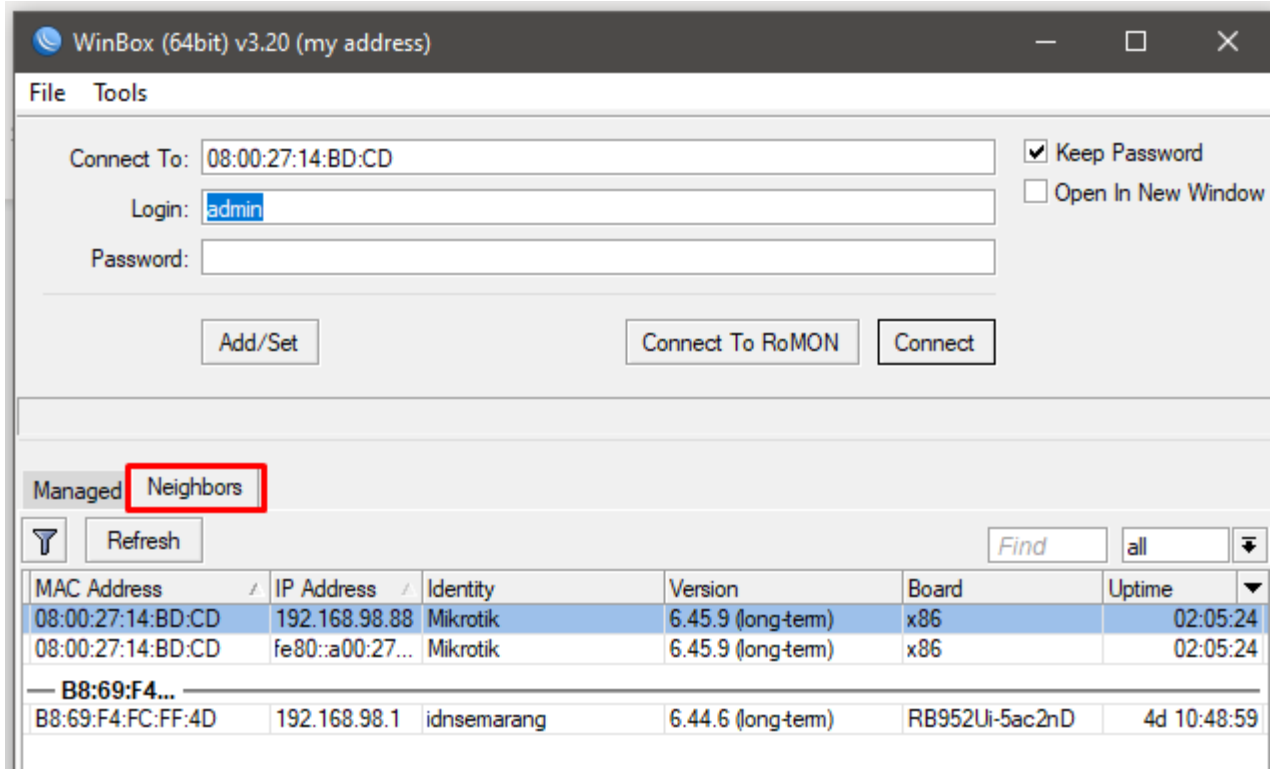
LAB

- Belajar cara akses mikrotik
- Topologi

WINBOX

LAB

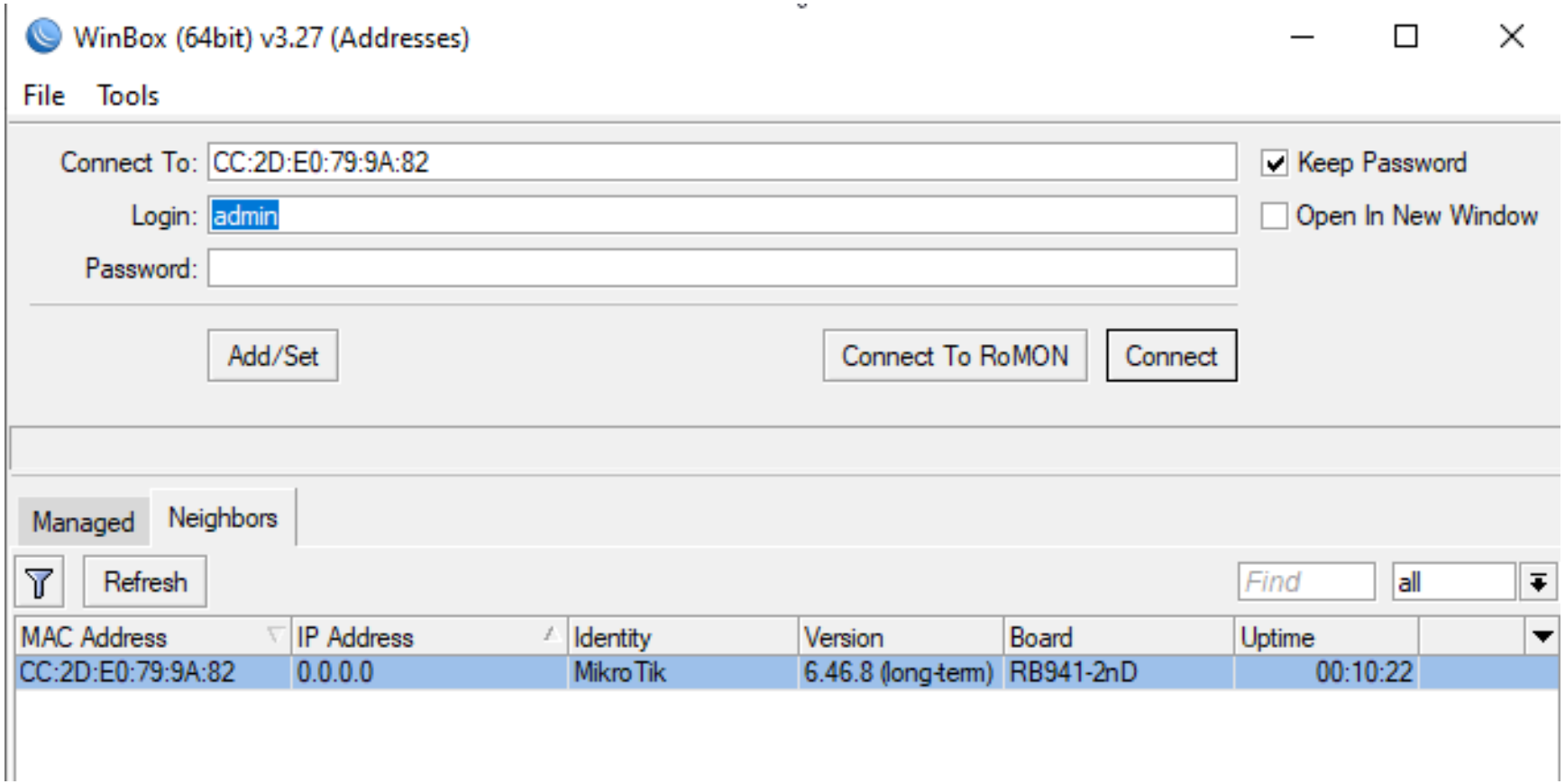
- Cara paling mudah dalam mengakses dan mengkonfigurasi MikroTik adalah menggunakan winbox
  - Available access by MAC and IP address
  - Default IP Address : 192.168.88.1/24
  - User : admin
  - Password : (blank)



WINBOX LOGIN

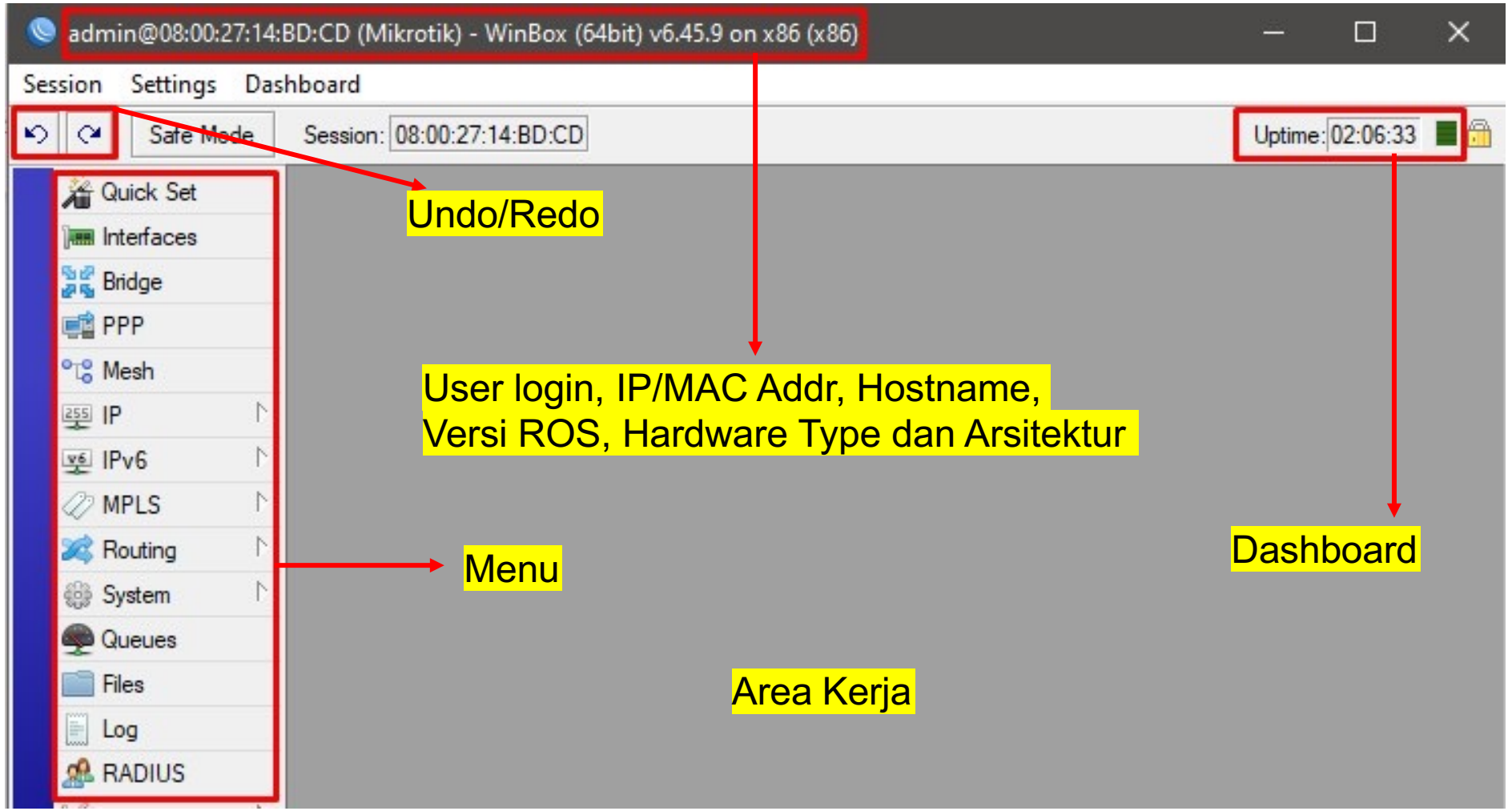
LAB

Apabila tidak tahu ip address router gunakan fitur discovery dan mac winbox



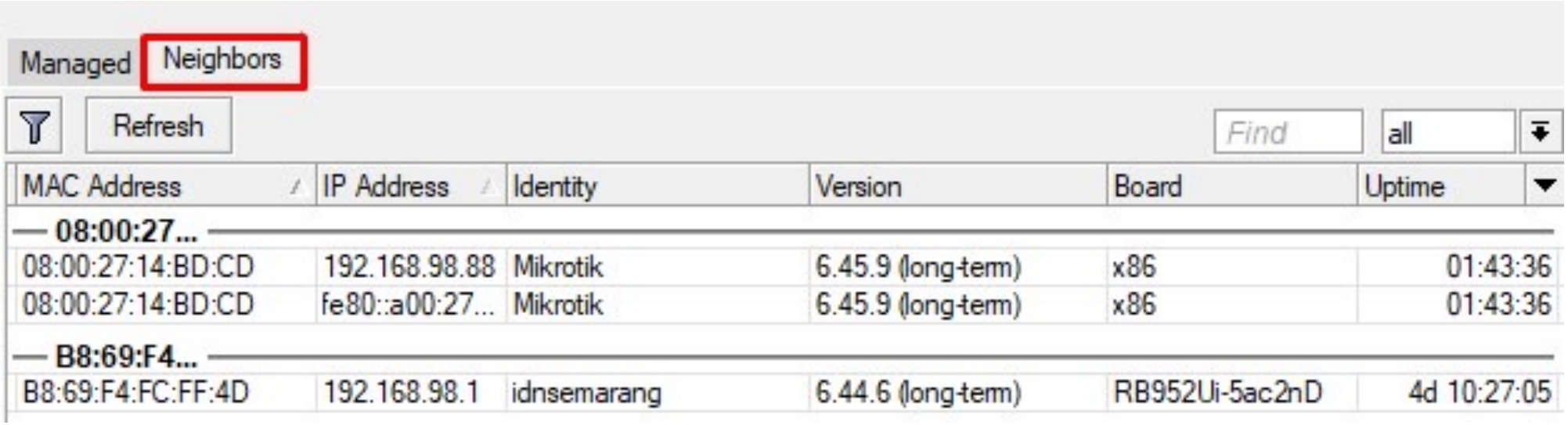
TAMPILAN MIKROTIK – PADA WINBOX

LAB



ROUTER IDENTITY (HOSTNAME)

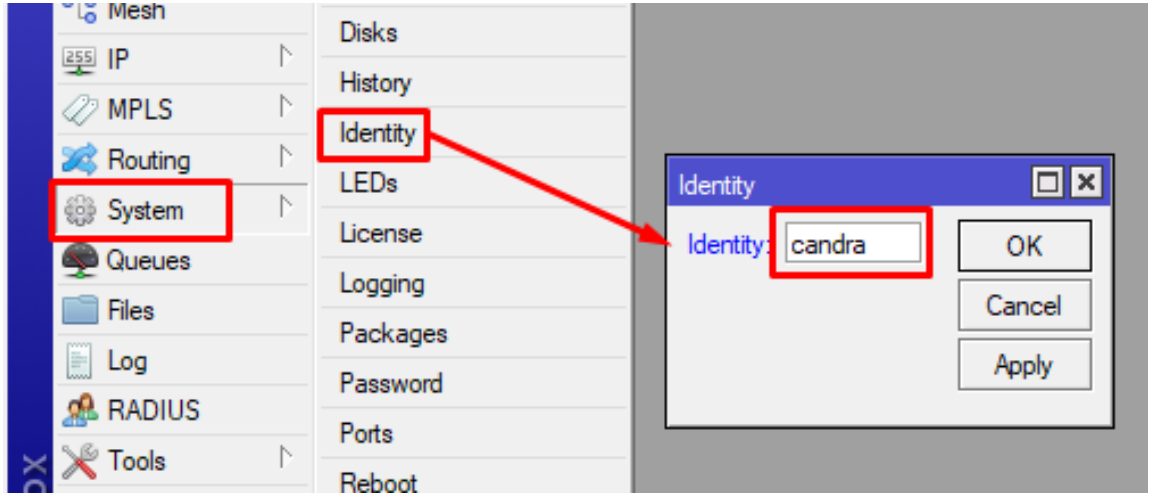
Router Identity (hostname) digunakan sebagai pengenal / identitas mengenai router itu sendiri.



ROUTER IDENTITY (HOSTNAME)

LAB

- System > Identity

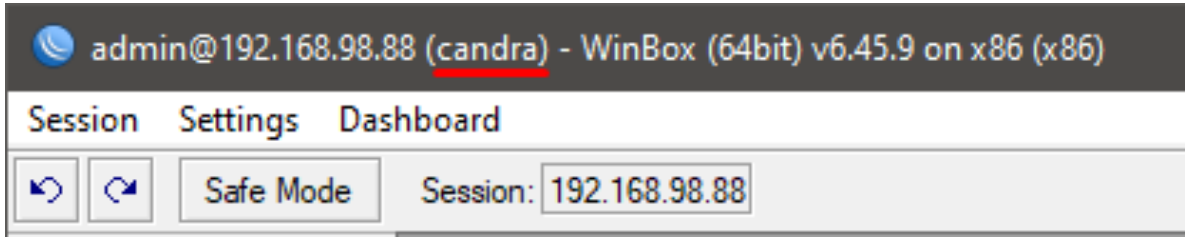


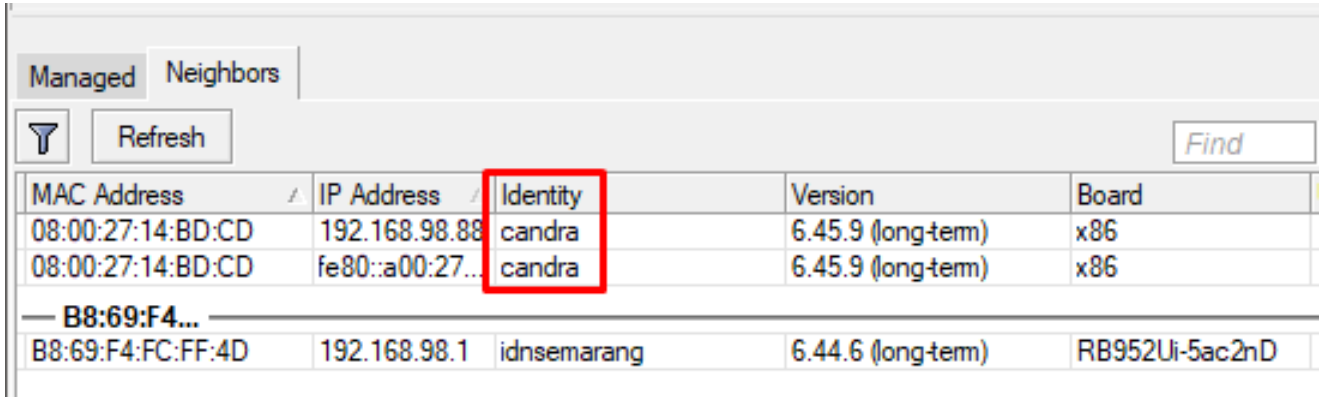

```
[admin@Mikrotik] > system identity set name=candra
[admin@candra] >
```

ROUTER IDENTITY (HOSTNAME)

LAB

- Verifikasi

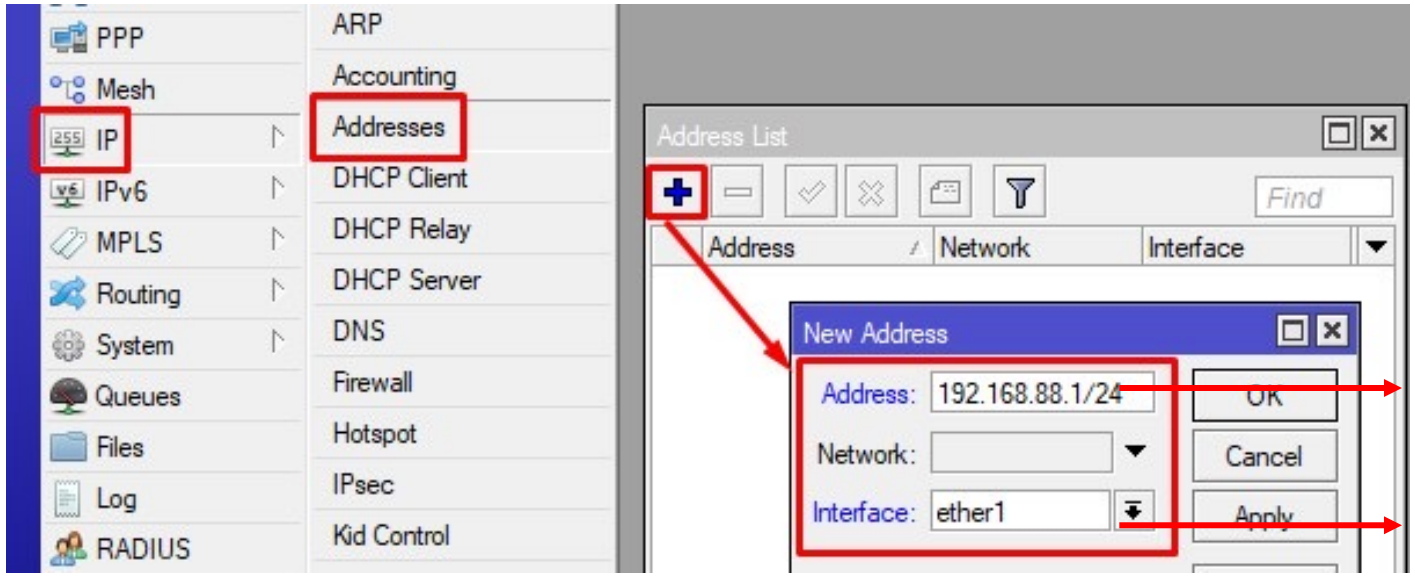




IP ADDRESS

LAB

- Belajar membuat IP address pada Router Mikrotik
- IP > Address



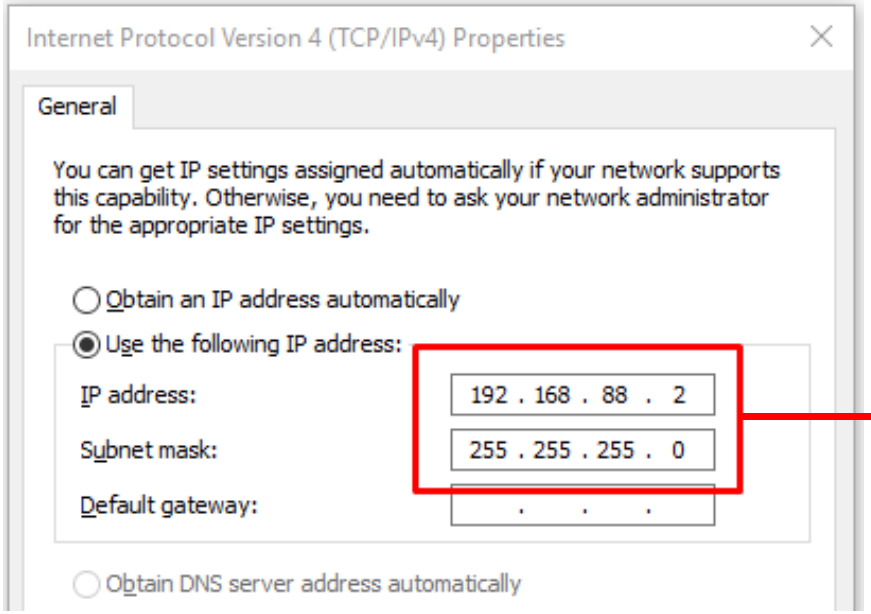
IP address/prefix

Interface yang akan di pasang IP tersebut

IP ADDRESS LAPTOP

LAB

- Setting IP address supaya laptop dapat komunikasi secara langsung dengan router



IP address dan subnetmask satu jaringan dengan router

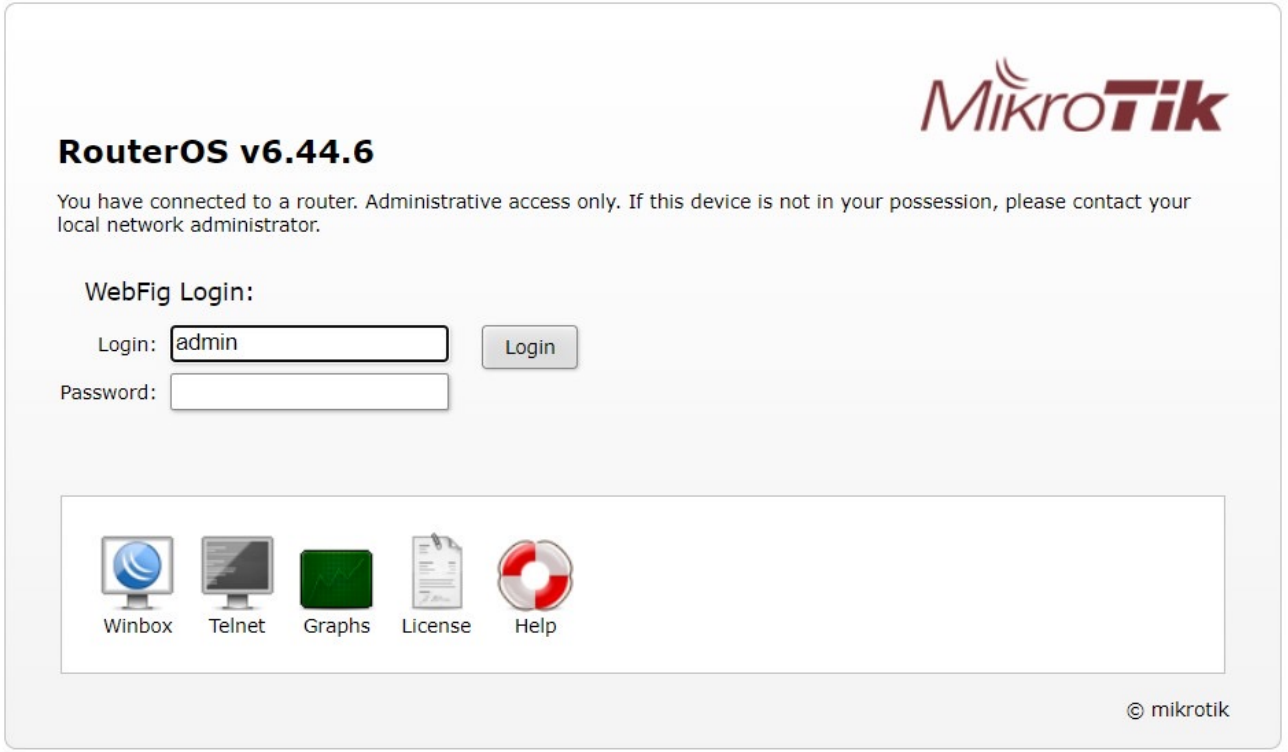
- Test Ping dari laptop ke router, pastikan reply

MENGAKSES MIKROTIK – WEBFIG

LAB

- Diperkenalkan sejak ROSv5.0 dengan fungsi yang sama dengan winbox
- Support IPv4 dan IPv6
- Support HTTP dan HTTPS
- Alternatif winbox

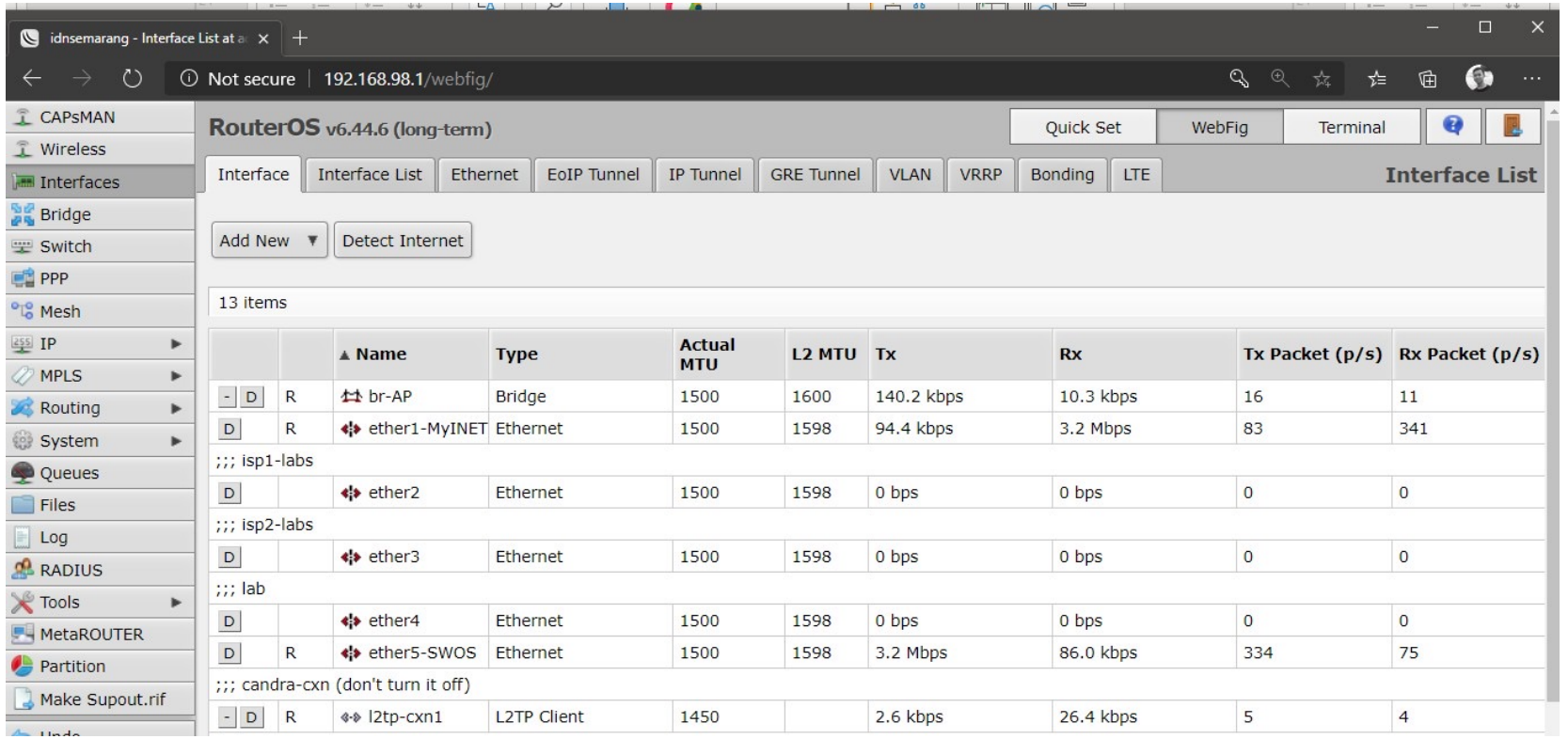
- Akses via browser :
- http://<ip_router>



MENGAKSES MIKROTIK – WEBFIG

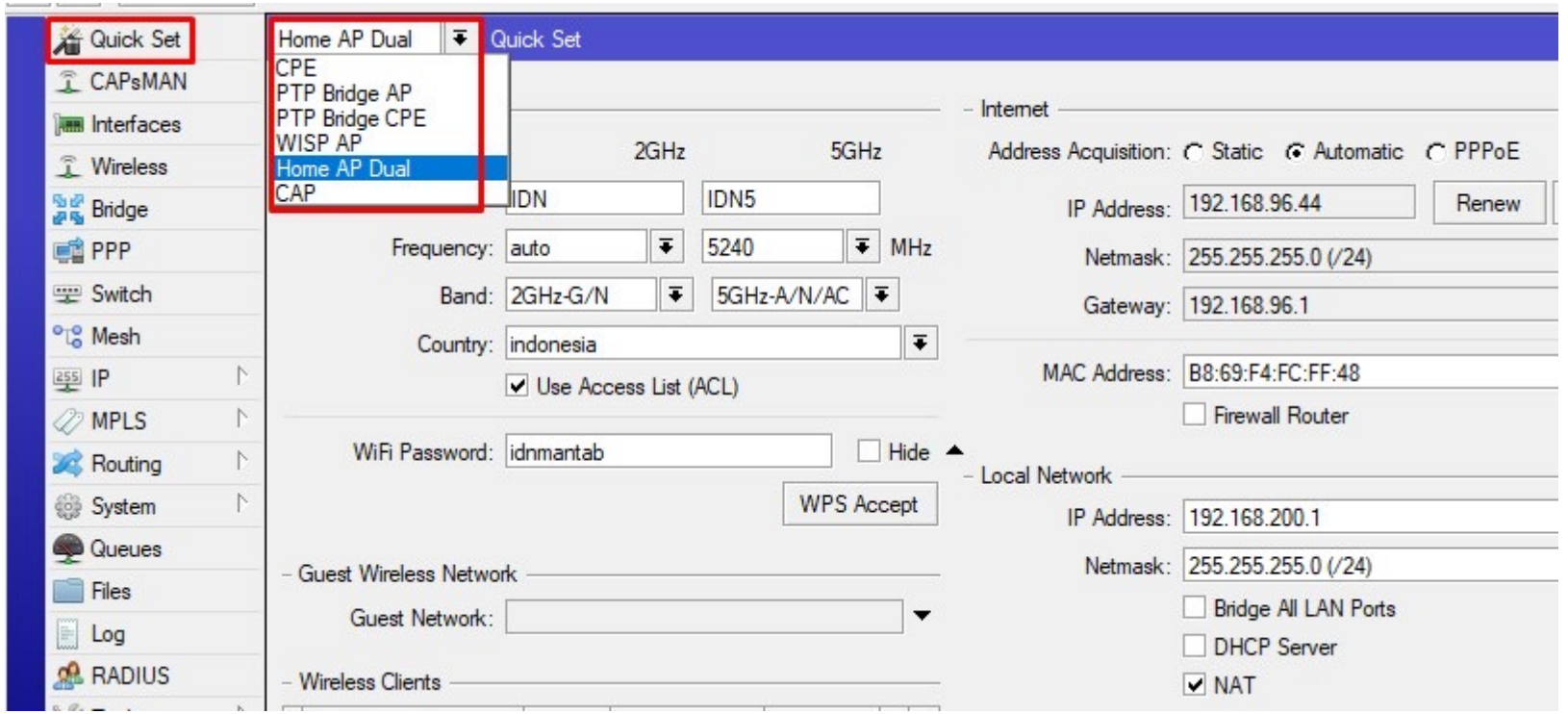
LAB

- Setting IP address pada router dan laptop (satu jaringan)
- Ketikan IP address router dibrowser



QUICK SET

- Settingan dasar router dalam satu tampilan.
- Dapat di akses melalui winbox atau webfig

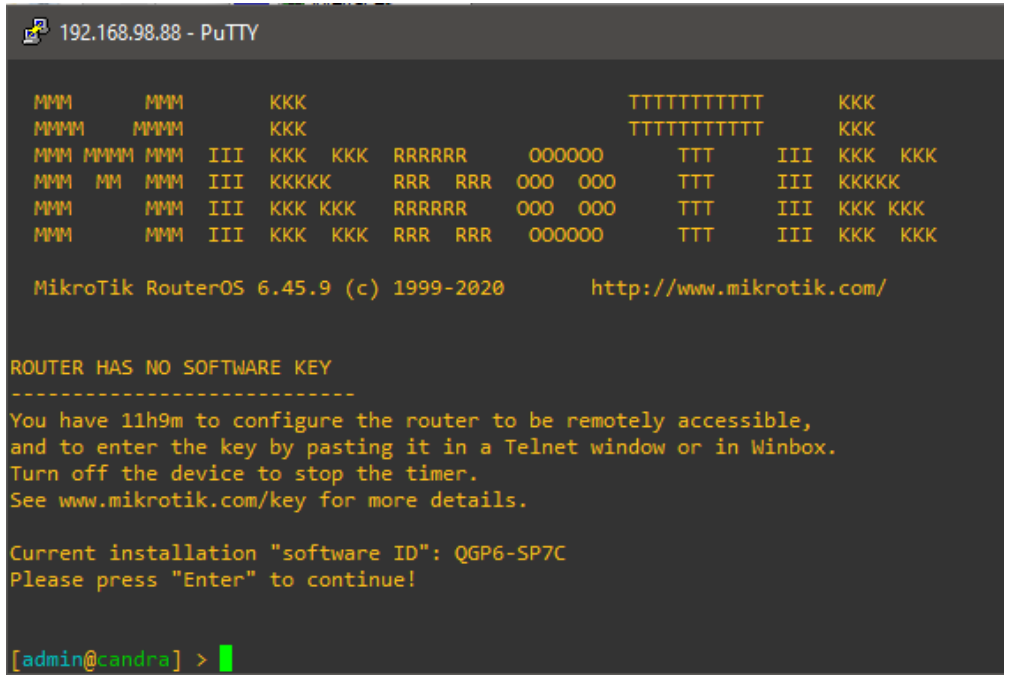


DEFAULT CONFIGURATION

- Terdapat beberapa perbedaan di default configuration tiap device.
- Untuk selengkapnya dapat dilihat pada default configuration di wiki mikrotik https://wiki.mikrotik.com/wiki/Manual:Default_Configurations
- Contohnya : pada SOHO routers – secara default ether1 sudah terdapat settingan DHCP Client, DHCP Server pada port lain dan Wireless yang sudah enable.
- Namun dapat juga di set “blank” sehingga kita dapat membangun konfigurasi dari awal.

COMMAND LINE INTERFACE

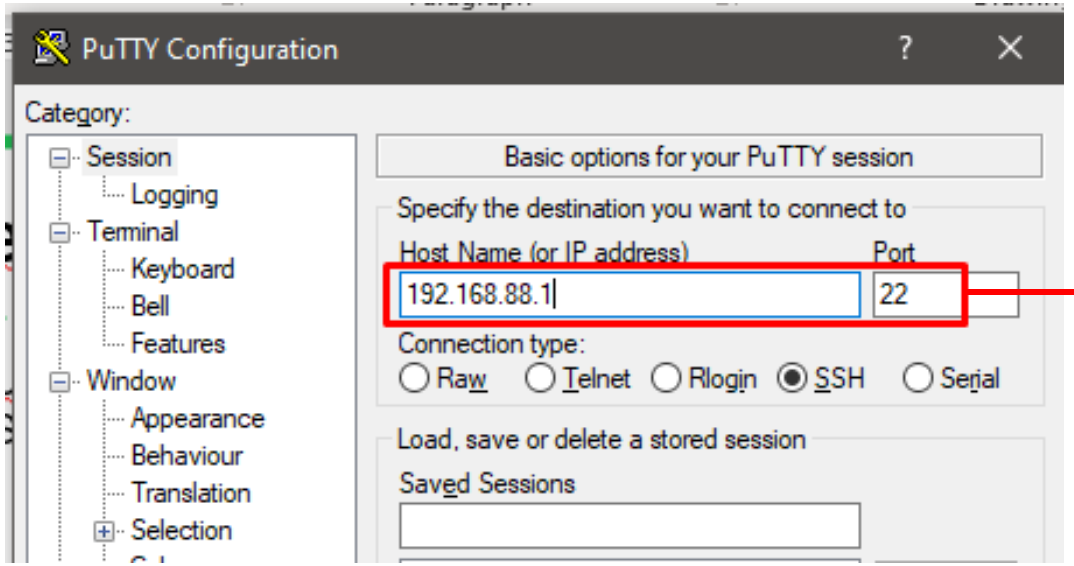
- Akses router via text / CLI dapat dilakukan melalui SSH, Telnet, Console, New Terminal (winbox) dan Terminal (WebFig).
- Digunakan untuk merunning script atau ketika akan mengakses router dengan keterbatasan bandwidth.



COMMAND LINE INTERFACE

LAB

- Untuk mengakses router via SSH/Telnet, bias menggunakan program
- SSH/Telnet client seperti putty, WinSCP dll.



IP Address router dan port

- Link download Putty https://www.putty.org/

COMMAND LINE INTERFACE

- Hierarchial Structure (sama seperti menu pada winbox)
- <tab> completes command
- Double <tab> untuk melihat ketersediaan command
- “?” untuk menampilkan bantuan command disertai keterangan
- Untuk navigasi command bisa menggunakan tombol ← ↑ → ↓ di keyboard

- Informasi selengkapnya bisa di lihat pada wiki mikrotik
  https://wiki.mikrotik.com/wiki/Manual:Console

COMMAND LINE INTERFACE

LAB

- Perintah masuk ke suatu menu (IP address)

[admin@idn] > /ip address

[admin@idn] /ip address >

- Perintah Kembali ke directory sebelumnya (IP address)

[admin@idn] /ip address > ..

[admin@idn] /ip >

- Perintah Kembali ke directory awal (Root)

[admin@idn] /ip > /
[admin@idn] >

COMMAND LINE INTERFACE

LAB

Perintah masuk ke konfigurasi IP Address

[admin@idn] > /ip address

Perintah melihat konfigurasi IP Address

[admin@idn] > /ip address print

Perintah lain di konfigurasi IP address

add – menambah IP address

remove – menghapus IP address

disable – mematikan IP address

set / edit – memodifikasi IP address

COMMAND LINE INTERFACE

LAB

Perintah menambahkan konfigurasi (IP Address)

```
[admin@idn] > /ip address          [Enter]
[admin@idn] /ip address > add address=192.168.100.1/24 interface=ether5
```

Verifikasi

```
[admin@idn] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
      #   ADDRESS            NETWORK         INTERFACE
      0   192.168.88.1/24    192.168.88.0    ether2
      1   192.168.100.1/24   192.168.100.0   ether5
```

COMMAND LINE INTERFACE

LAB

Perintah menghapus konfigurasi (IP Address)

Sebelum menghapus IP address lakukan pengecekan list nomor urut IP dulu.

[admin@idn] > /ip address print

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

#	ADDRESS	NETWORK	INTERFACE
0	192.168.88.1/24	192.168.88.0	ether2
1	**192.168.100.1/24**	**192.168.100.0**	**ether5**

Tujuan kali ini akan menghapus IP address 192.168.100.1/24 karena IP address tersebut berada pada nomor urut 1 maka perintahnya adalah

[admin@idn] /ip address > remove number=1

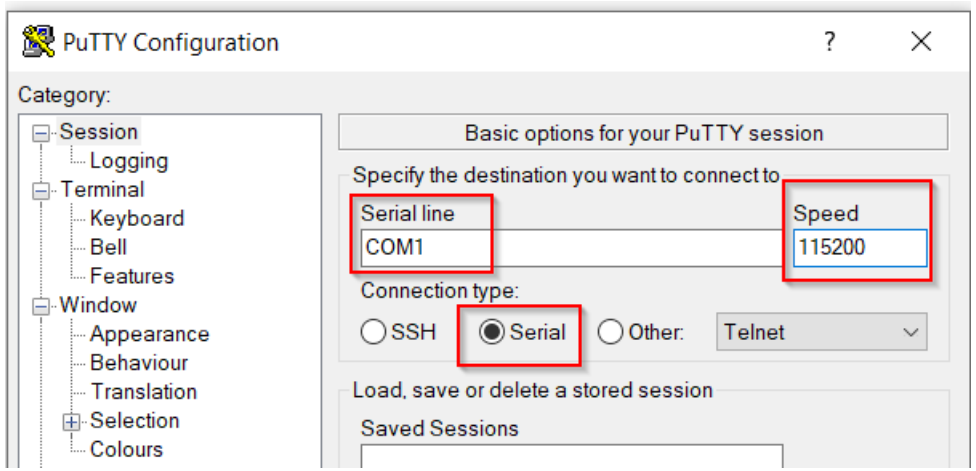
SERIAL CONSOLE

- Serial Console digunakan apabila kita lupa/salah telah mendisable semua interface pada MikroTik.
- Serial Console dibutuhkan juga saat kita menggunakan Netinstall.
- Remote via serial console membutuhkan kabel DB-9 (atau converter USB ke DB-9).
- Menggunakan program HyperTerminal. Baud rate 115200, Data bits 8, Parity None, Stop bits 1,dan Flow Control None.

SERIAL CONSOLE

LAB

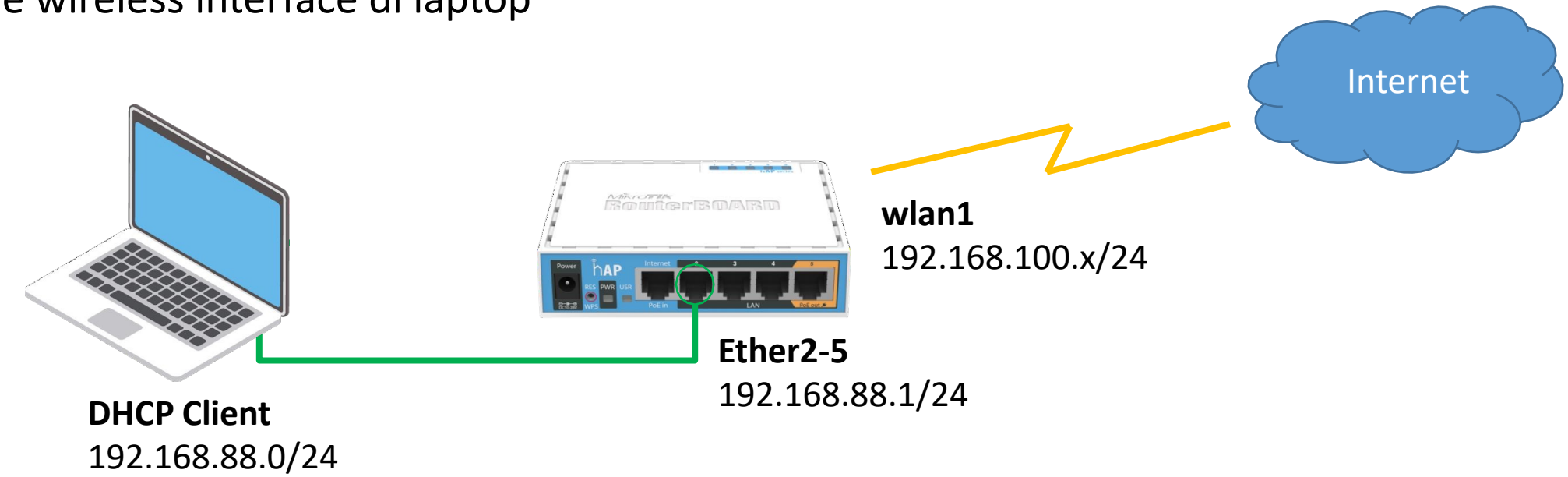
- Masuk Terminal, seperti Putty.
  Pilih Connection Type Serial dan Sesuaikan serial line COM(x) dilihat dalam device manager.
- Lalu spees baudrate 115200 khusus perangkat mikrotik.



MENGKONEKSIKAN MIKROTIK KE INTERNET

LAB

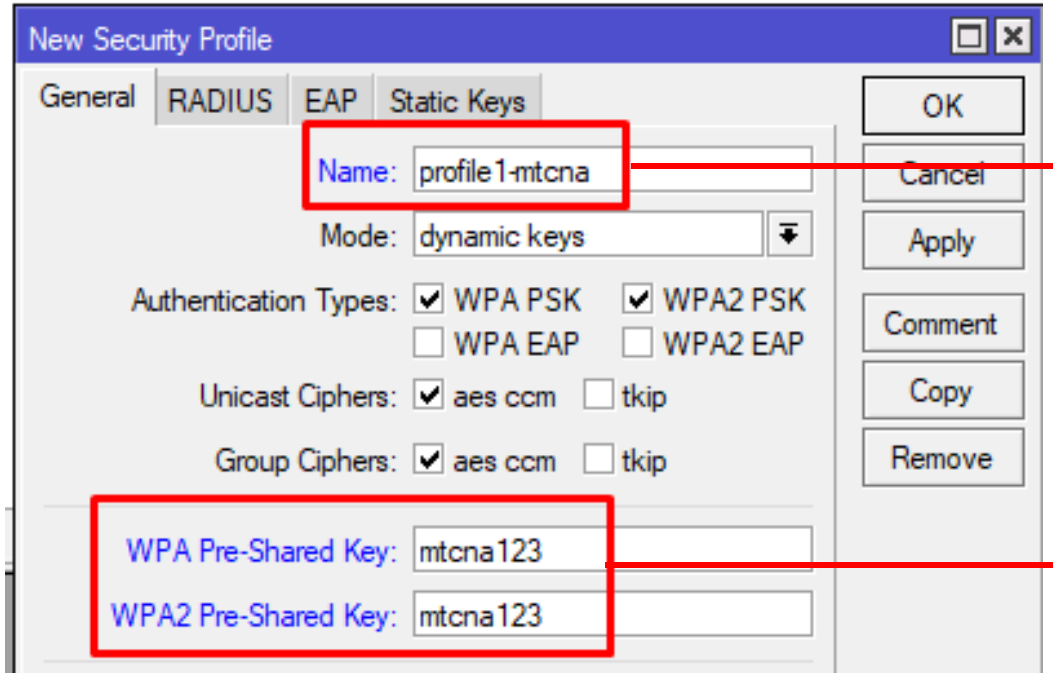
- Belajar mengkoneksikan Leptop ke internet via Mikrotik
- Buat topologi seperti pada gambar di bawah
- Koneksikan port LAN laptop ke ether (2-5)
- Disable wireless interface di laptop



KONFIGURASI WAN – SECURITY PROFILE

LAB

- Wireless Security Profile merupakan tempat untuk menyimpan password yang nantinya digunakan untuk konek ke suatu SSID AP.
- Buat password di **Wireless > Security profile** untuk konek ke AP yang akan di koneksikan.



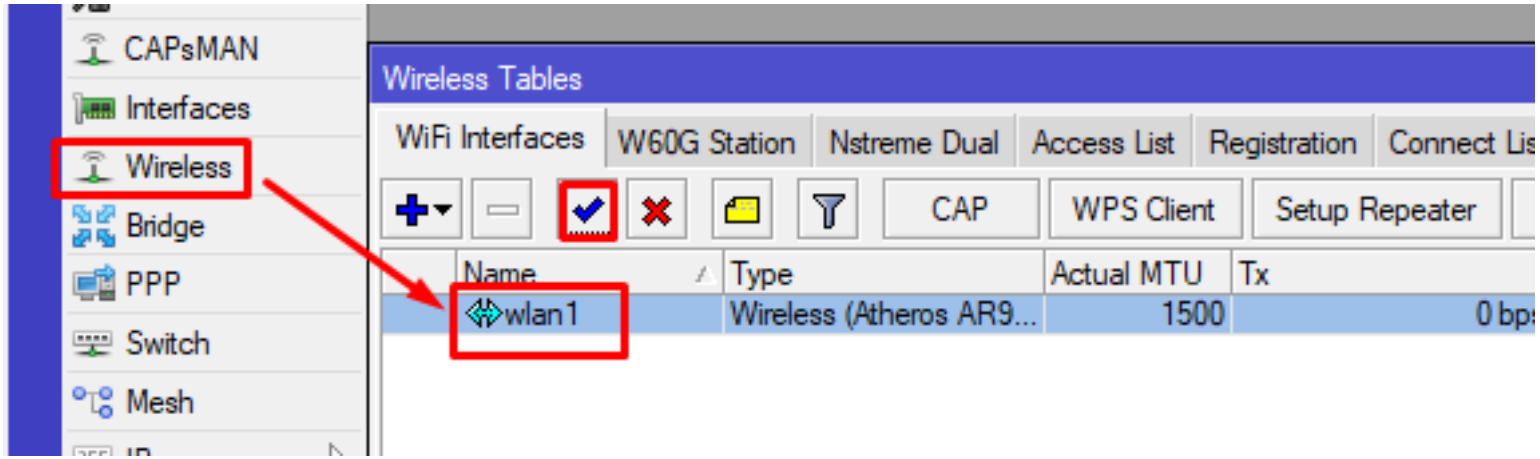
Nama Security Profile yang akan di buat.

Password dari SSID yang akan di koneksikan.

KONFIGURASI WAN

LAB

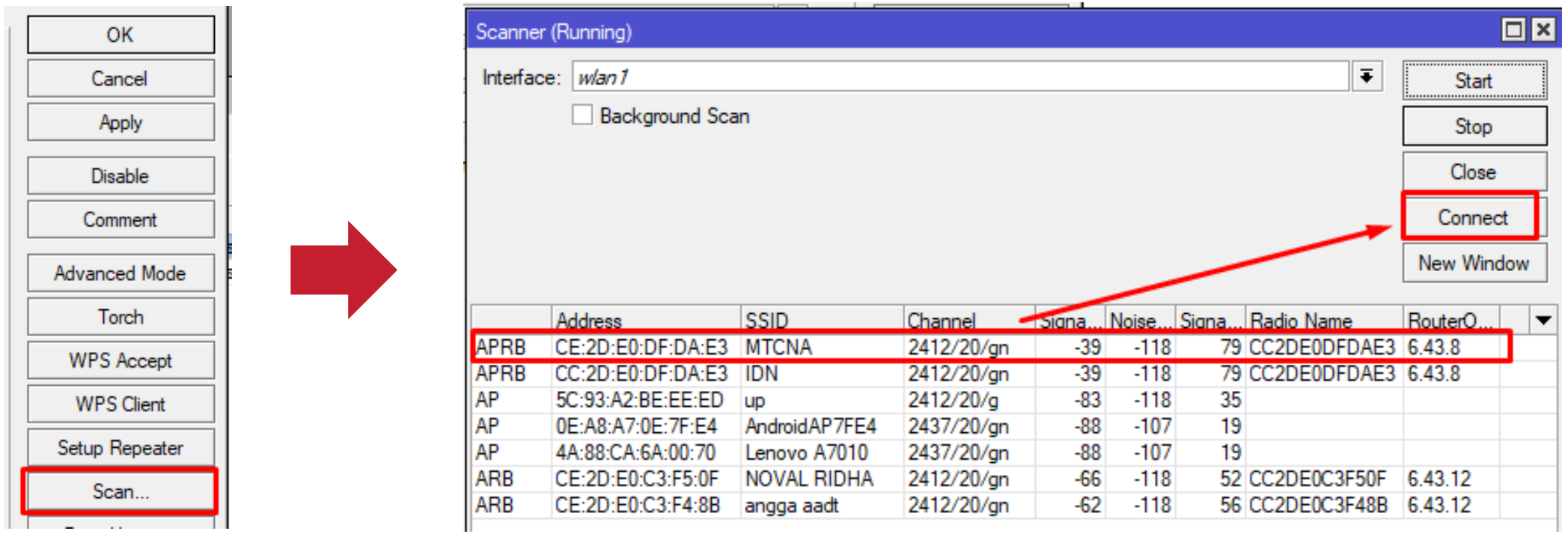
- Interface wireless di mikrotik diberi nama wlan1 (Wireless LAN Interface)
- By default setelah router di reset interface tersebut dalam keadaan disable
- Enable interface tersebut melalui menu **Wireless > checklist wlan1**



KONFIGURASI WAN – MODE STATION (1)

LAB

- Untuk mempermudah konek ke AP bisa menggunakan tool scan



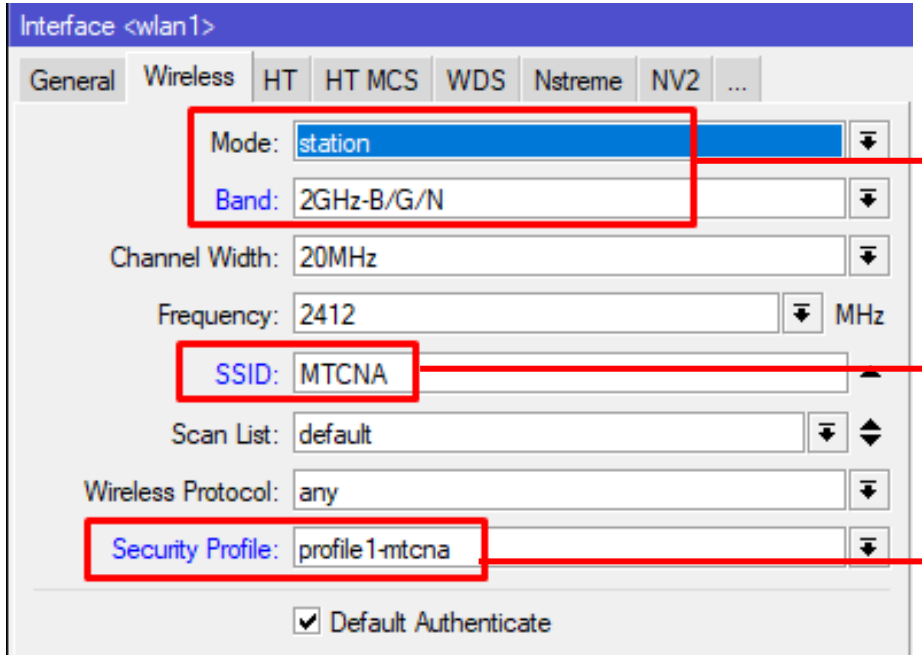
- Pilih SSID yang akan di koneksikan kemudian klik tombol Connect

KONFIGURASI WAN – MODE STATION (2)

LAB

- Wireless mikrotik bisa kita fungsikan sebagai station (penerima sinyal) dengan merubah parameter mode di menu wireless.
- Sesuakan parameter lainnya (band, frekuensi, security profile sesuai AP).

Double klik wlan1 > Wireless Tab



Mode = Station (penerima)
Band = sesuai band AP

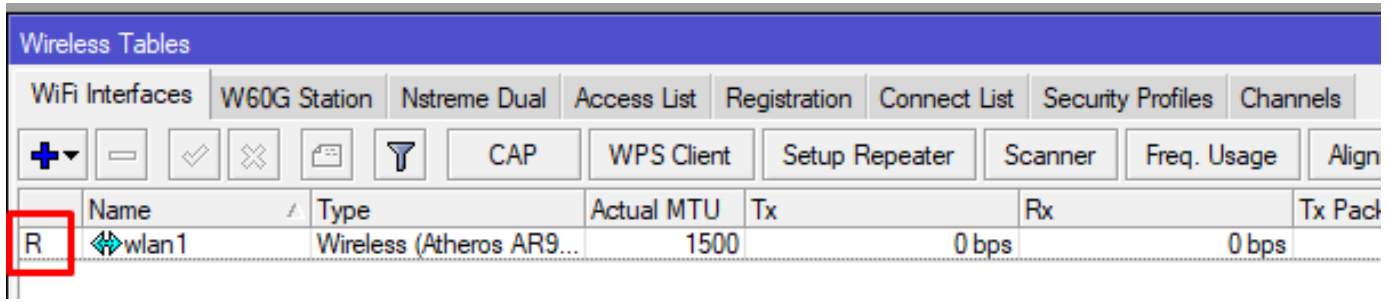
SSID = menyesuaikan dengan SSID AP

Pasang Security Profile yang sebelumnya dibuat

KONFIGURASI WAN – STATION MODE (VERIFIKASI)

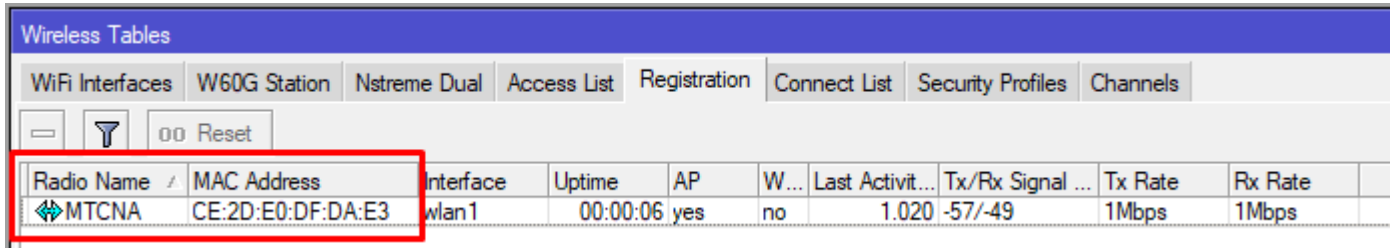
LAB

- Pastikan Wireless sudah terkoneksi



Huruf **R** (Running), menandakan wireless telah terkoneksi.

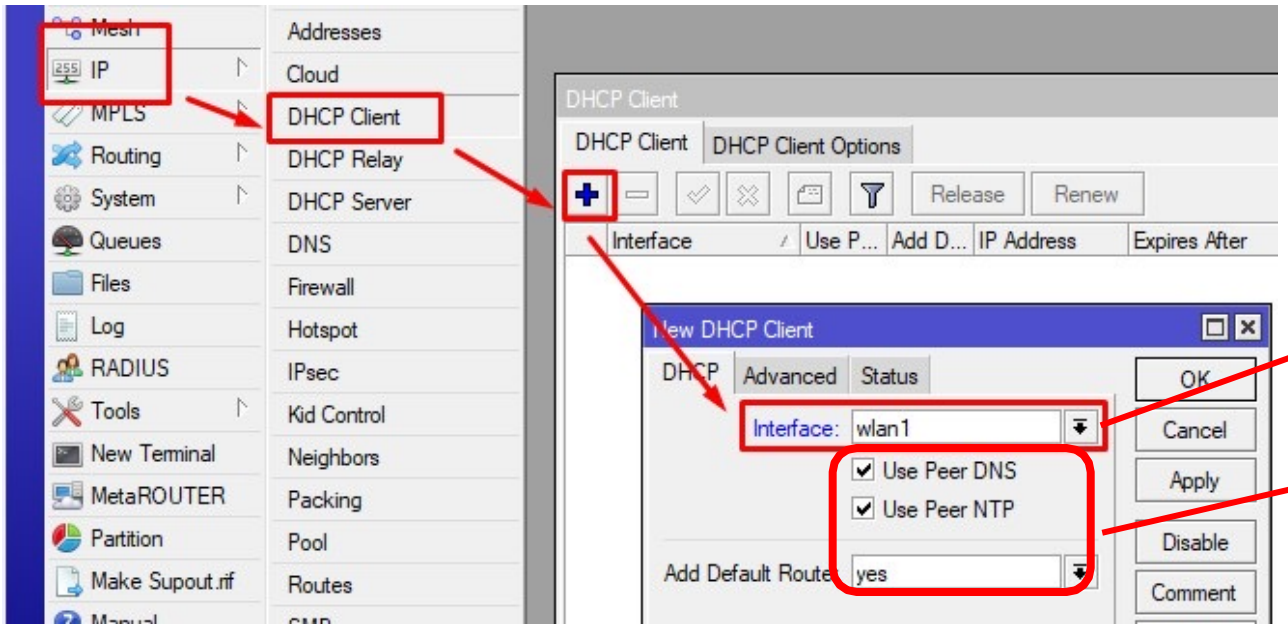
- AP yang terkoneksi akan terdaftar di menu **Registration**



KONFIGURASI WAN – REQUEST DHCP CLIENT (1)

LAB

- Walaupun wireless sudah terkoneksi ke AP, router belum dapat akses ke internet. Hal ini di karenakan router belum mendapat IP secara otomatis dari AP.
- Sehingga kita perlu request IP address dari AP melalui menu IP > DHCP Client.



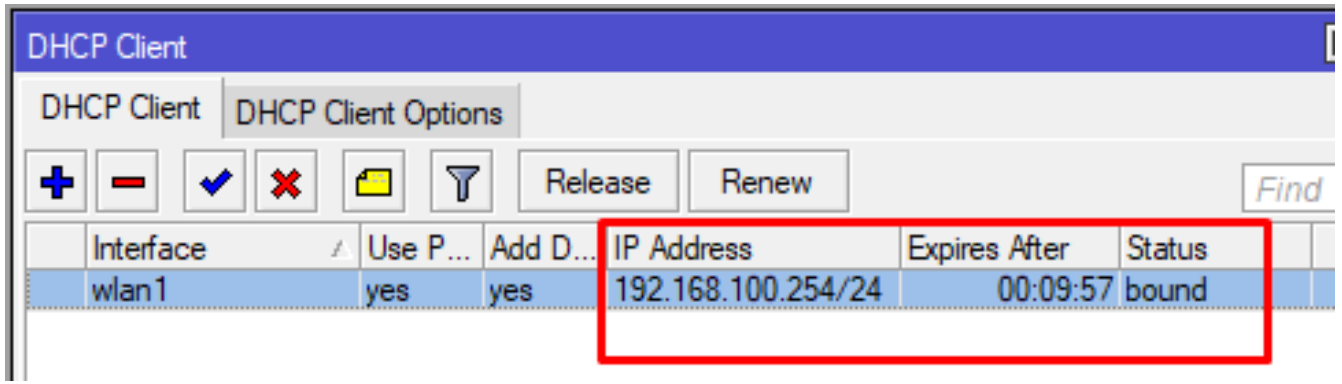
Interface ke WAN (Internet)

Set agar DNS, NTP dan default route otomatis didapatkan dari server

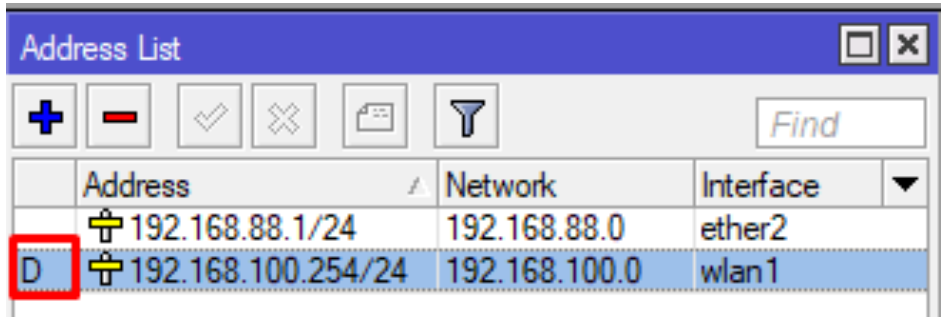
KONFIGURASI WAN – REQUEST DHCP CLIENT (2)

LAB

- Pastikan mendapat status bound, menandakan bahwa wlan1 sudah mendapatkan IP address dari AP



- Pada menu IP Address terdapat dynamic IP address ada wlan1



VERIFIKASI PING KE INTERNET MELALUI ROUTER

LAB

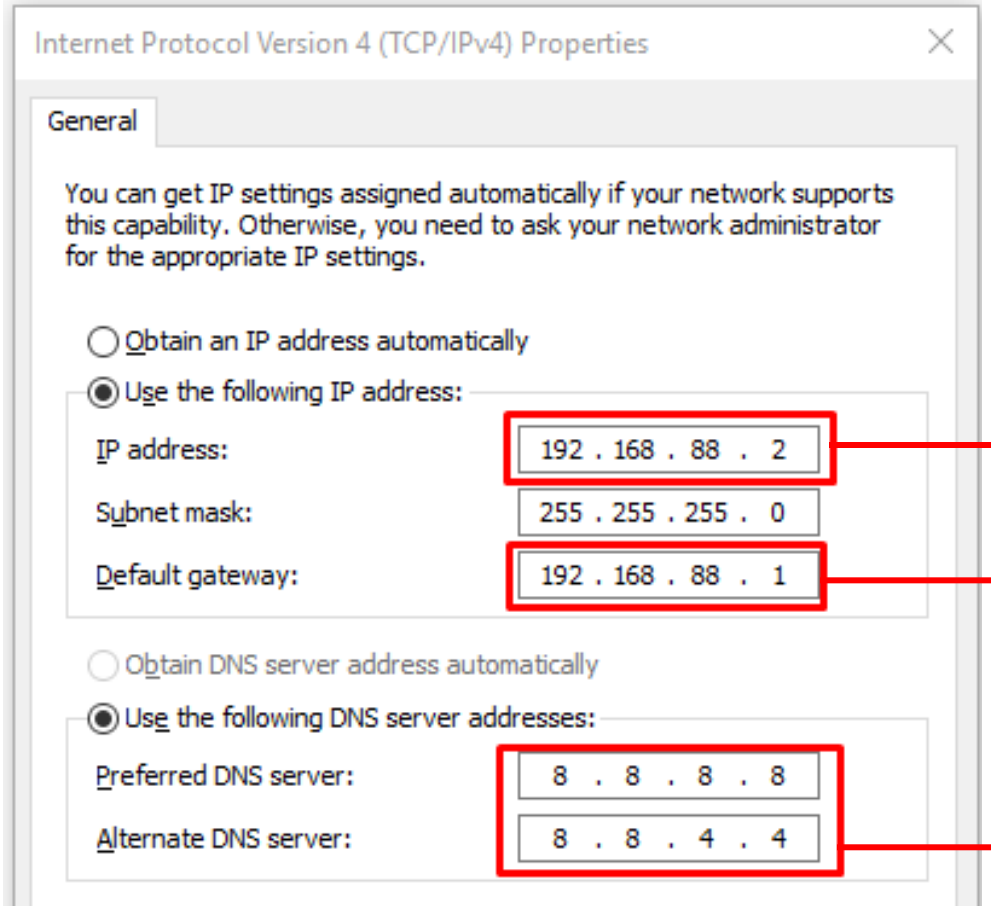
- Ping dari Router ke Internet
- New Terminal

```
[admin@candra] > ping google.com
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 74.125.68.100                              56  40 32ms
    1 74.125.68.100                              56  40 124ms
    2 74.125.68.100                              56  40 207ms
    3 74.125.68.100                              56  40 150ms
    4 74.125.68.100                              56  40 72ms
    5 74.125.68.100                              56  40 175ms
    6 74.125.68.100                              56  40 32ms
    7 74.125.68.100                              56  40 40ms
    8 74.125.68.100                              56  40 61ms
```

KONFIGURASILAN-LAPTOP

LAB

- Setting IP address pada laptop



IP Laptop satu jaringan dengan IP interface Mikrotik

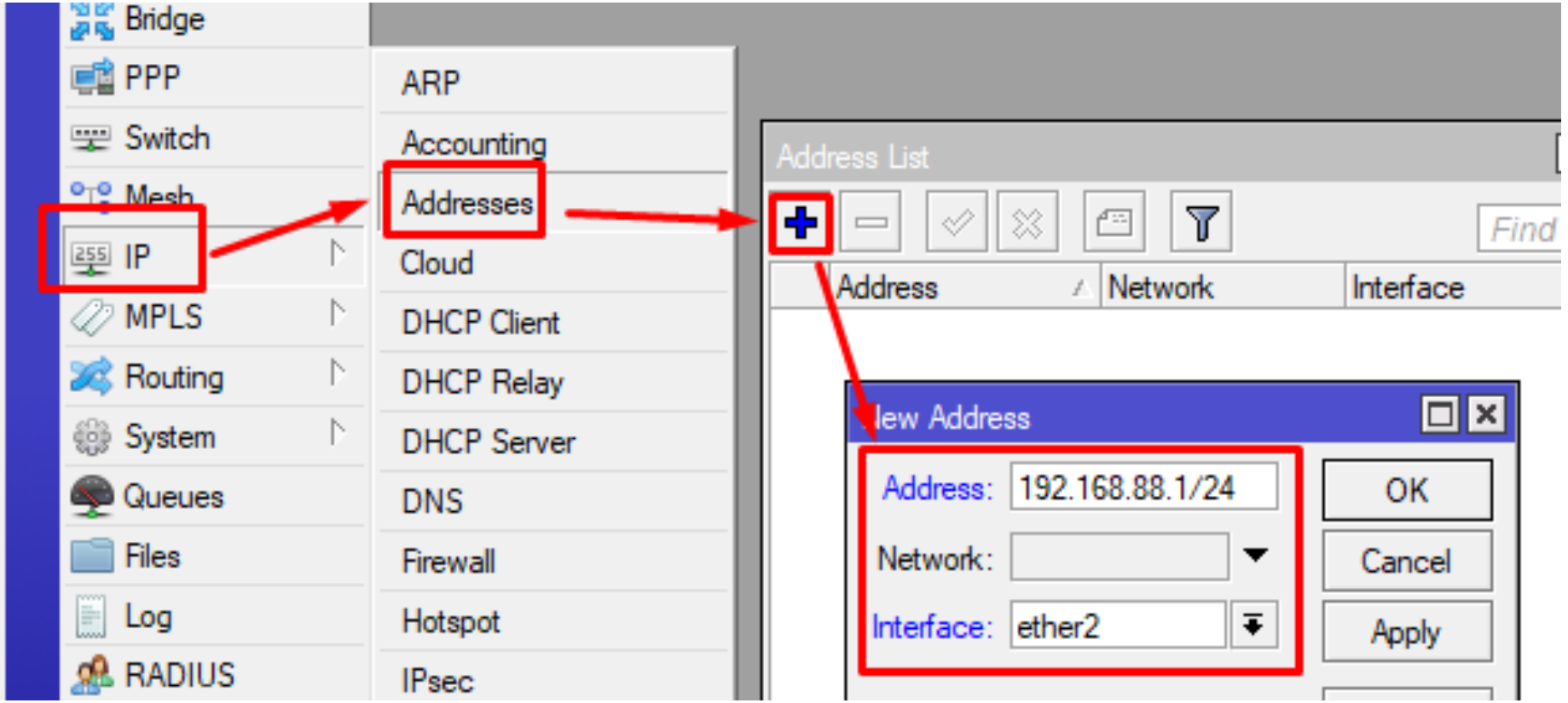
Gateway Leptop adalah IP interface Mikrotik

DNS Public google

KONFIGURASILAN-ROUTER

LAB

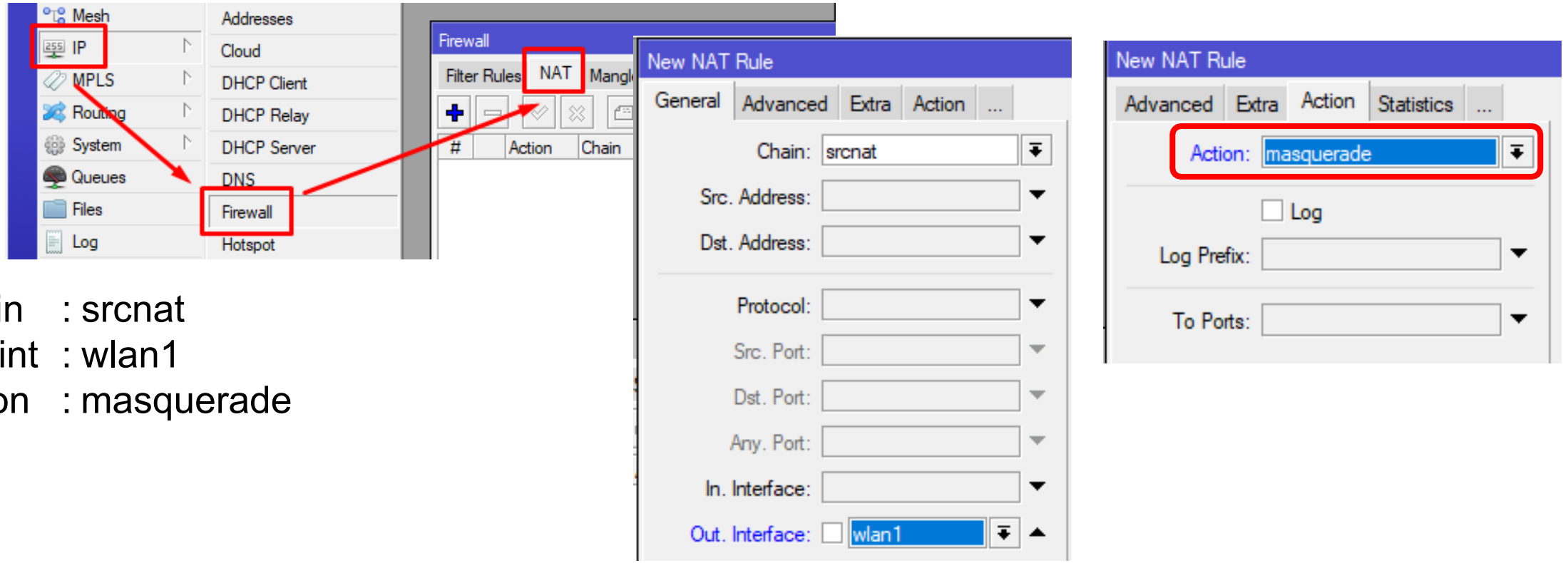
- Setting IP address pada router



KONFIGURASI WAN – NAT

LAB

- NAT (Network Address Translation) digunakan supaya client yang ada di Jaringan lokal agar dapat mengakses jaringan public (internet)



Chain : srcnat
Out-int : wlan1
Action : masquerade

LISENSI MIKROTIK

- Ketika membeli semua type RouterBOARD sudah include lisensi didalamnya.
- Lisensi melakat pada media penyimpanan **(NAND).**
- Lisensi menentukan fitur-fitur yang dimiliki oleh setiap router.
- Lisensi terdiri dari **level 0-6**
- Level lisensi juga menentukan Batasan upgrade packet.
- Lisensi akan hilang jika di uninstall menggunakan non mikrotik.
- Khusus untuk x86 harus membeli license di mikrotik.com atau bisa melalui distributor.

LISENSIMIKROTIK

Level	Type	Typical Use
0	Trial Mode	24h trial
1	Free Demo	Limited RouterOS features
3	CPE	Wireless client (station), wireless bridge (AP PTP)
4	AP	Wireless AP : WISP, HOME, Office
5	ISP	Support more tunnels than L4
6	Controller	Unlimited RouterOS features

LISENSI MIKROTIK – ROUTERBOARD

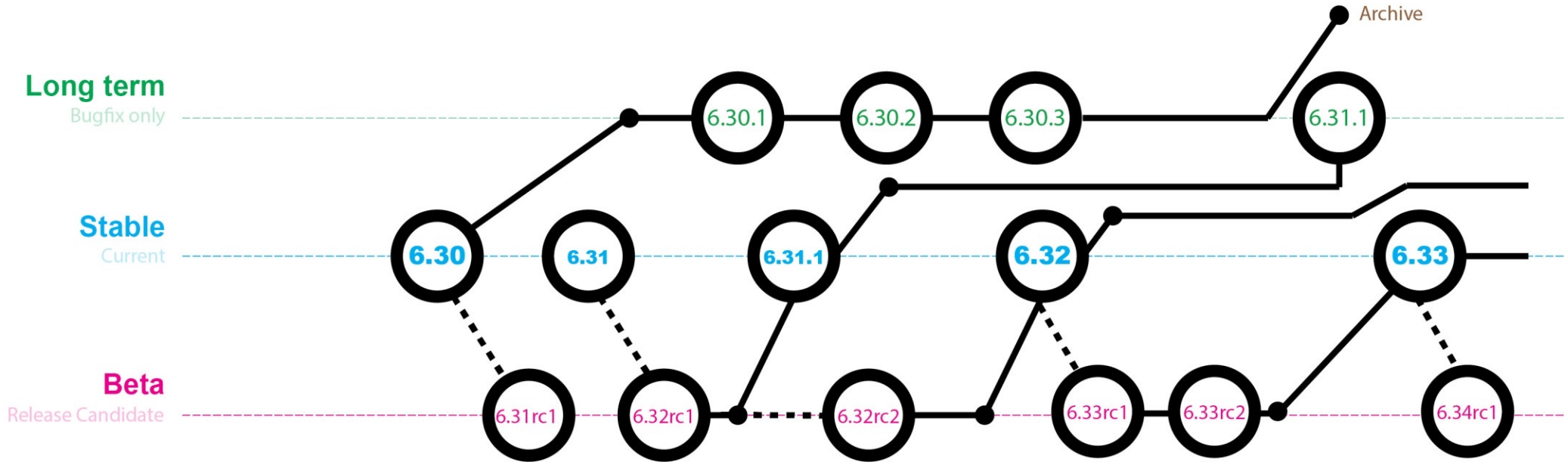
Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key	registration required	do not sell	$45	$95	$250
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, 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

LISENSI MIKROTIK – CHR (CLOUD HOSTED ROUTER)

License	Speed limit	Price
Free	1Mbit	FREE
P1	1Gbit	45 US$
P10	10Gbit	95 US$
P-Unlimited	Unlimited	250 US$

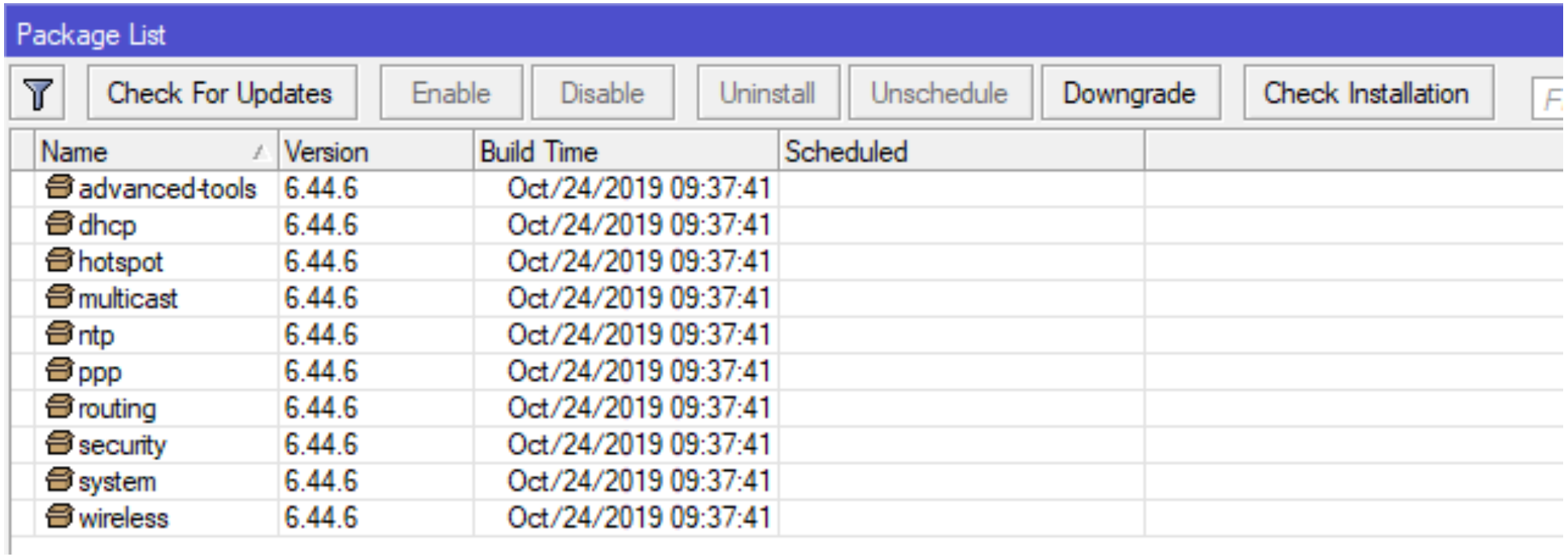
ROUTEROS RELEASES

- Long term (Bugfix Only) : most stable version, update without new features
- Stable (Current) : same fixes and new features release
- Beta (Release Candidate) : consider as a “nightly build”, not recommended for production



MANAGEMENT PACKAGES

- Fitur-fitur routerOS tergantung dari packages yang di install
- Setiap packages memiliki fitur yang berbeda-beda
  - System > Packages



MANAGEMENT PACKAGES

Package	Features
advanced-tools (*mipsle, mipsbe, ppc, x86*)	advanced ping tools. netwatch, ip-scan, sms tool, wake-on-LAN
calea (*mipsle, mipsbe, ppc, x86*)	data gathering tool for specific use due to "Communications Assistance for Law Enforcement Act" in USA
dhcp (*mipsle, mipsbe, ppc, x86*)	Dynamic Host Control Protocol client and server
gps (*mipsle, mipsbe, ppc, x86*)	Global Positioning System devices support
hotspot (*mipsle, mipsbe, ppc, x86*)	HotSpot user management
ipv6 (*mipsle, mipsbe, ppc, x86*)	IPv6 addressing support
mpls (*mipsle, mipsbe, ppc, x86*)	Multi Protocol Labels Switching support
multicast (*mipsle, mipsbe, ppc, x86*)	Protocol Independent Multicast - Sparse Mode; Internet Group Managing Protocol - Proxy
ntp (*mipsle, mipsbe, ppc, x86*)	Network protocol client and service
ppp (*mipsle, mipsbe, ppc, x86*)	MlPPP client, PPP, PPTP, L2TP, PPPoE, ISDN PPP clients and servers
routerboard (*mipsle, mipsbe, ppc, x86*)	accessing and managing RouterBOOT. RouterBOARD specific imformation.
routing (*mipsle, mipsbe, ppc, x86*)	dynamic routing protocols like RIP, BGP, OSPF and routing utilities like BFD, filters for routes.
security (*mipsle, mipsbe, ppc, x86*)	IPSEC, SSH, Secure WinBox
system (*mipsle, mipsbe, ppc, x86*)	basic router features like *static routing, ip addresses, sNTP, telnet, API, queues, firewall, web proxy, DNS cache, TFTP, IP pool, SNMP, packet sniffer, e-mail send tool, graphing, bandwidth-test, torch, EoIP, IPIP, bridging, VLAN, VRRP etc.). Also, for RouterBOARD platform - MetaROUTER | Virtualization*
ups (*mipsle, mipsbe, ppc, x86*)	APC ups
user-manager (*mipsle, mipsbe, ppc, x86*)	MikroTik User Manager
wireless (*mipsle, mipsbe, ppc, x86*)	wireless interface support

https://wiki.mikrotik.com/wiki/Manual:System/Packages

MANAGEMENT PACKAGES – MAIN PACKAGE

- Setiap arsitektur RouterOS mempunyai kombinasi paket yang berbeda-beda.
- Contoh ‘routeros-mipsbe’ ‘routeros-tile’
- Berisi fitur standard RouterOS (wireless, dhcp, ppp, router, etc.)
- Biasanya digunakan untuk kebutuhan Install Ulang router.
- Untuk mendownload Main Packages bisa melalui link berikut : www.mikrotik.com/download

MANAGEMENT PACKAGES – EXTRA PACKAGES

- Berisi fitur-fitur tambahan untuk router (user-manager, gps, ntp, ups, dll)
- Untuk menambahkan extra packages ke dalam router, caranya download extra packages, kemudian ekstrak dan upload salah satu packages ke dalam router. Terakhir reboot router

RouterOS

	6.44.6 (Long-term)	6.45.7 (Stable)	6.46beta59 (Testing)	7.0beta3 (Development)
MIPSBE	CRS1xx, CRS2xx, CRS312-4C+8XG, CRS326-24S+2Q+, DISC, FiberBox, hAP, hAP ac, hAP ac lite, LDF, LHG, ltAP mini, mANTBox, mAP, NetBox, NetMetal, PowerBox PWR-Line, QRT, RB9xx, SXTsq, cAP, hEX Lite, RB4xx, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx, hEX PoE			
Main package	💾	💾	💾	💾
Extra packages	💾	💾	💾	-
SMIPS	hAP mini, hAP lite			

MANAGEMENT PACKAGES

LAB

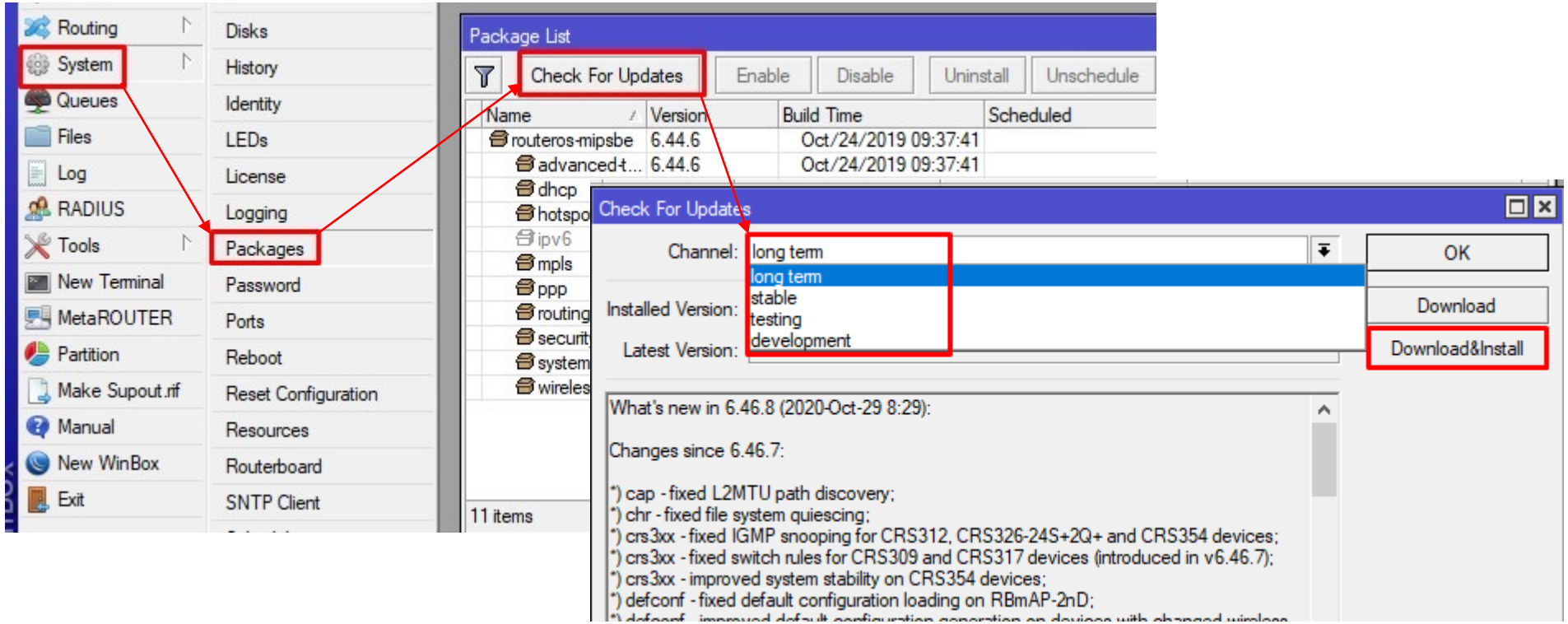
- Perhatikan list menu yang ada di winbox
- Buka System Packages
- Disable MPLS Package
- Enable IPv6 Package
- Reboot router
- Check list menu yang ada di Winbox kembali.

UPGRADE ROUTEROS

- Upgrade digunakan untuk fix bugs, security, new feature dll.
- Untuk alasan security Mikrotik menyarankan agar selalu melakukan upgrade router ke versi terbaru.
- Upgrade harus memperhatikan aturan level dan lisensi yang berlaku
- Selain itu juga harus memperhatikan kompatibilitas terhadap jenis arsitektur hardware.
- Upgrade ada 2 cara :
  - Upgrade packages from router (internet required)
  - Manual Upload packages

UPGRADE ROUTEROS – UPGRADE FROM ROUTER

- Pastikan router sudah punya akses internet.
- Upgrade melalui menu



UPGRADE ROUTEROS – MANUAL UPLOAD PACKAGES

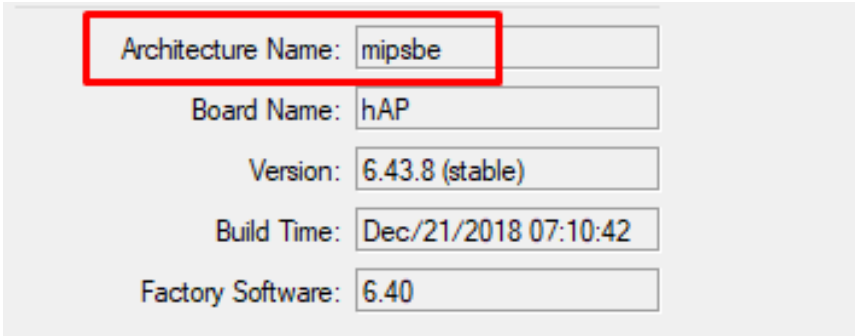
- Upgrade ini di lakukan dengan mengupload beberapa packages ke router.
- **Upload packages tinggal drag n drop** dari komputer ke router melalui winbox menggunakan protocol **TCP port 8291**.
- Selain drag n drop melalui winbox, bisa menggunakan FTP Client dan packages harus diupload di bagian **root.**
- Untuk packages bisa di download di situs mikrotik **mikrotik.com/download.**
- Pemilihan paket sangat penting dalam melakukan upgrade **jenis & arsitektur** hardware memiliki software yang berbeda.
- Untuk kebutuhan upgrade gunakan **“extra packages”** dan disarankan untuk mendownload yang versi **Long Term / Stable.**

UPGRADE ROUTEROS – MANUAL UPLOAD PACKAGES

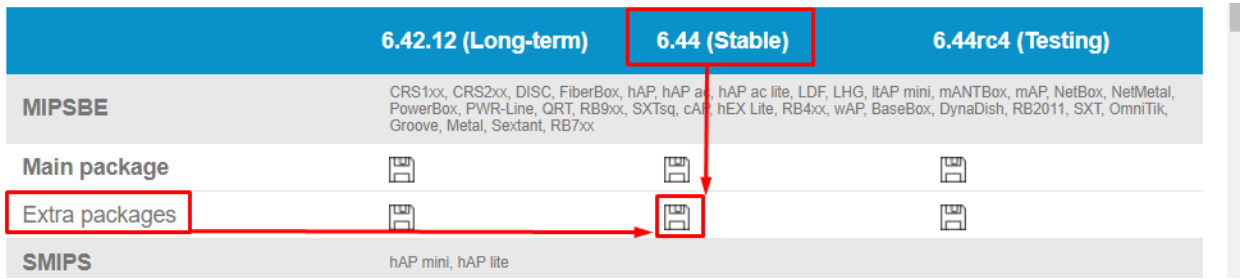
LAB

- Check type arsitektur di router.

  System > Resources



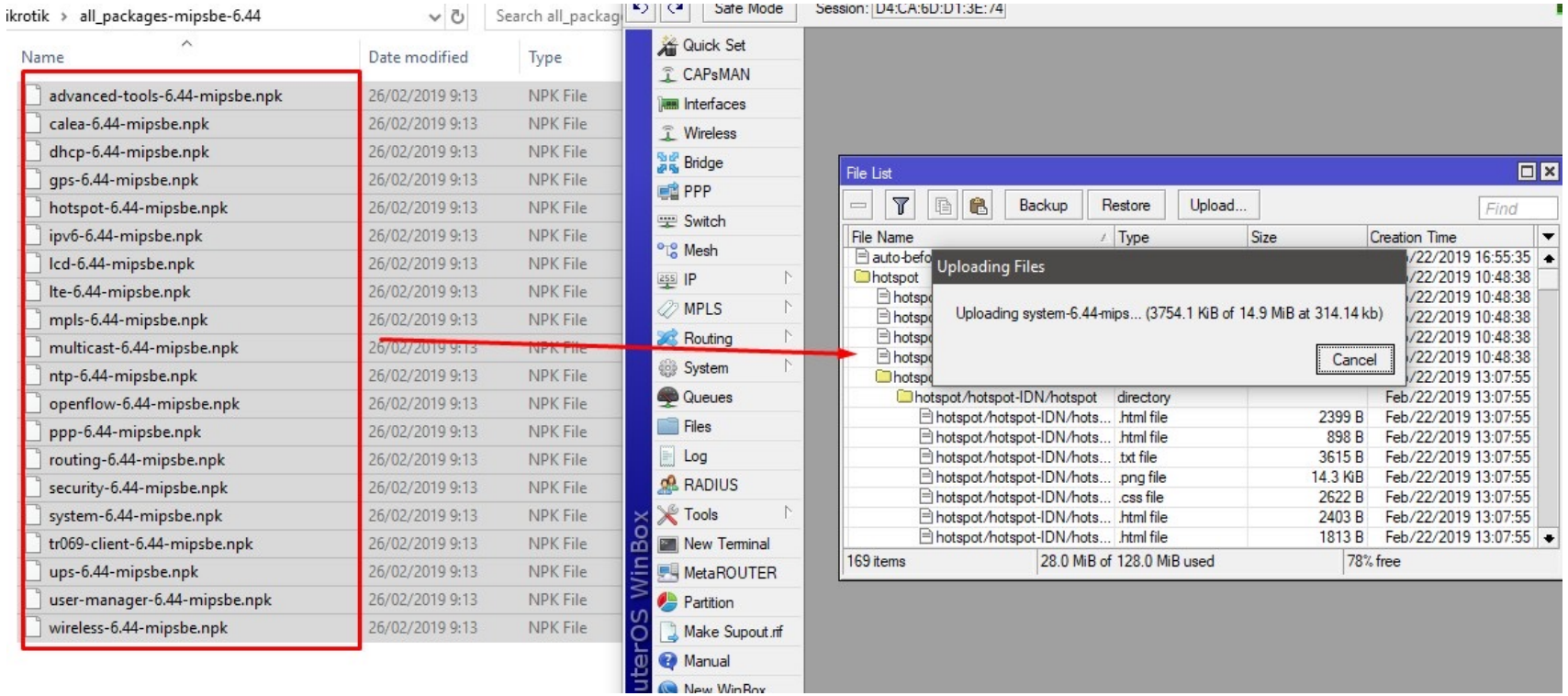
- Download extra packages di situs mikrotik.com/download sesuai type arsitektur. (misal arsitektur yang digunakan MIPSBE).



UPGRADE ROUTEROS – MANUAL UPLOAD PACKAGES

LAB

- Ekstrak packages yang tadi di download, dan hasilnya di drag n drop ke router

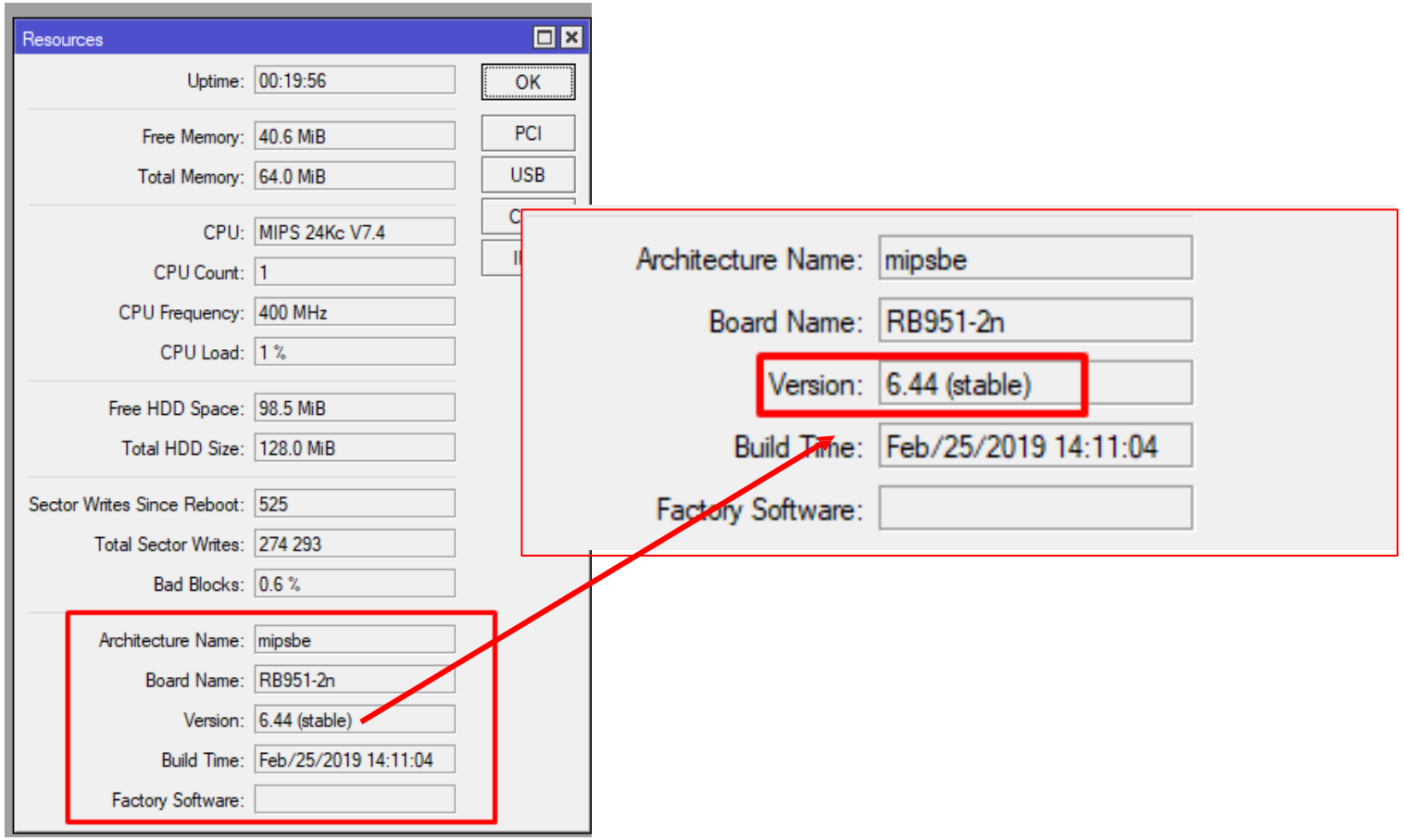


- Reboot Router (System > Reboot)

UPGRADE ROUTEROS – MANUAL UPLOAD PACKAGES

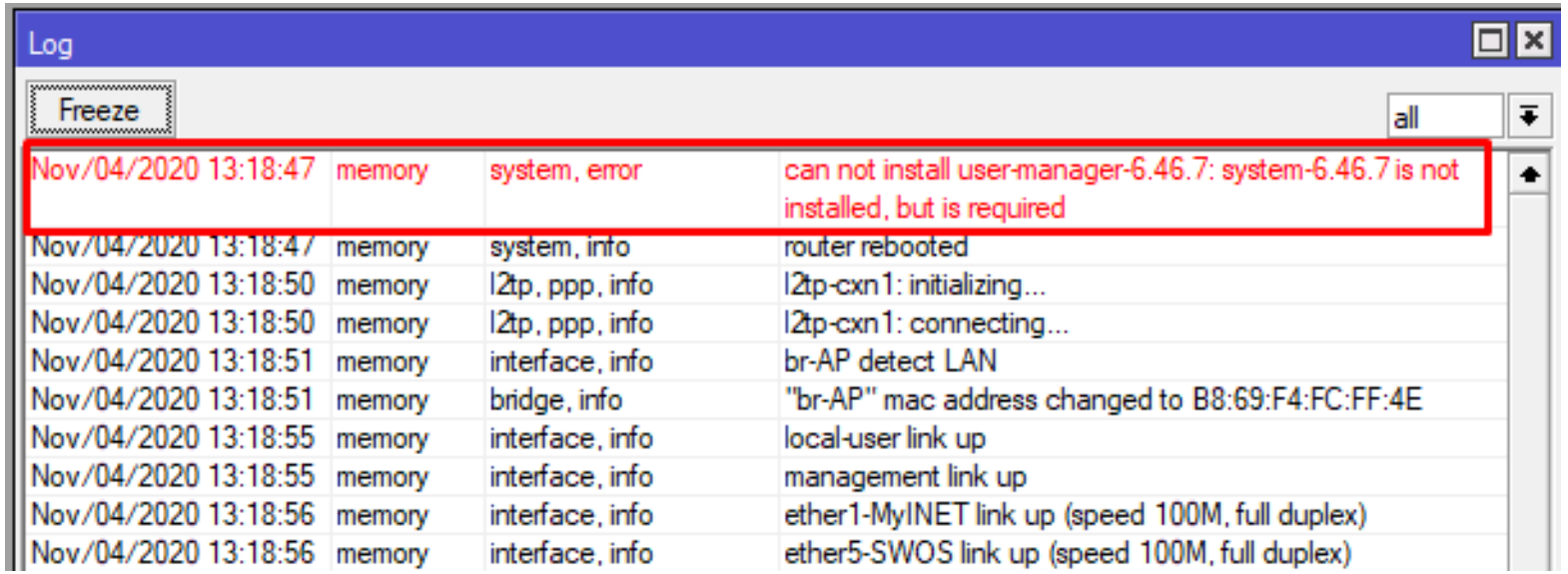
LAB

- Check Versi router
- System > Resources



TROUBLESHOOTING – UPGRADE ROUTER

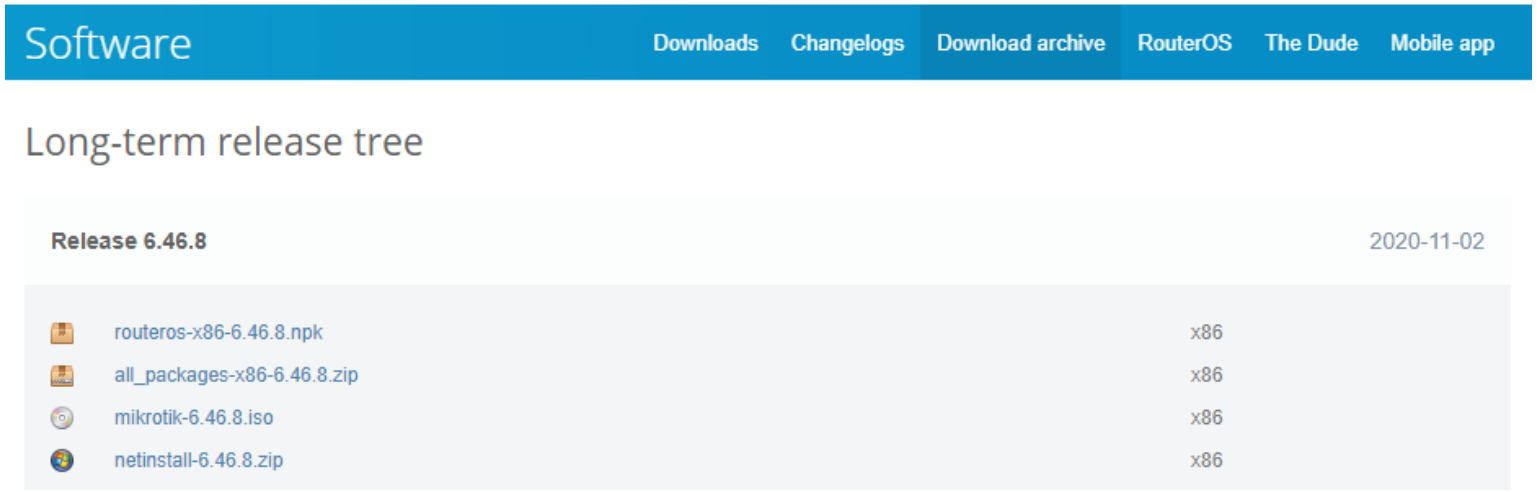
- Versi masih sama
- Upload diskonek
- Packages tidak terinstall



DOWNGRADE ROUTER OS

LAB

- Downgrade dilakukan apabila hardware kurang mendukung terhadap versi
- baru atau terdapat bug pada versi aktifnya.
- Downgrade harus memperhatikan kompatibilitas terhadap jenis arsitektur hardware.
- Untuk mendownload packages versi lama bisa melalui menu **Download archive**



DOWNGRADE ROUTER OS

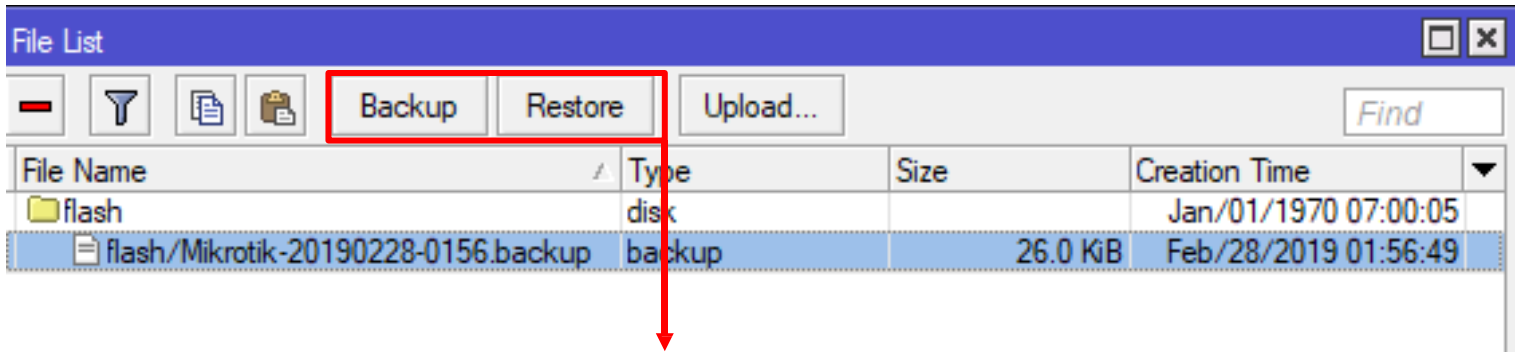
- Downgrade from router
  - System Packages > Check for Updates
  - Pilih channel yang berbeda (bug-fix only/Long term)
  - Klik download
  - Klik downgrade di “Packages List” window
- Manual Downgrade
  - Download packages versi sebelumnya dari web mikrotik.com/download
  - Ekstrak kemudian upload ke dalam router
  - Masuk ke system Packages
  - Klik downgrade

BACKUP DAN RESTORE

- Konfigurasi di router bisa di simpan, kemudian bisa digunakan juga di kemudian hari.
  - **Di Mikrotik terdapat 2 jenis Backup**
    - **Binary File (.backup) – restoring config on same router**
      - Tidak dapat dibaca text editor
      - Membackup semua konfigurasi router
      - Create return point (kembali seperti semula)
    - **Script File (.rsc) – moving config and restoring to another router**
      - Berupa script, dapat dibaca oleh text editor
      - Dapat membackup sebagian konfigurasi router
      - Dapat digunakan untuk menambahkan konfig baru atau script terbaru pada mikrotik

BACKUP DAN RESTORE – BINARY FILE

- Backup file dapat dibuat melalui menu Files
- Backup file adalah binary, **secara default terkenkripsi dengan user password**.
- Berisi seluruh konfigurasi yang terdapat pada router (**termasuk username dan password)**

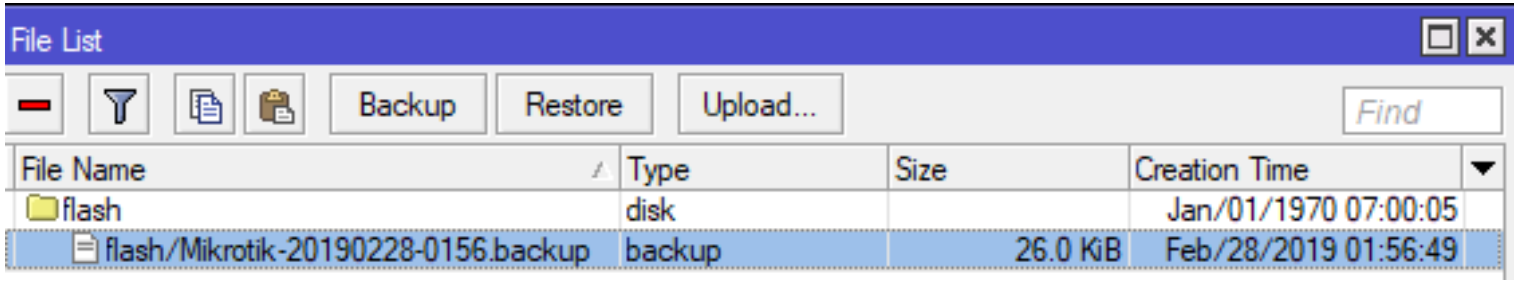


Tombol **backup** digunakan untuk membackup konfigurasi pada Mikrotik.
Tombol **restore** digunakan untuk mengembalikan konfigurasi.

BACKUP – BINARY FILE

- By default ketika membackup tanpa mengisi parameter name, maka secara
- otomatis router akan menggunakan format sebagai berikut:

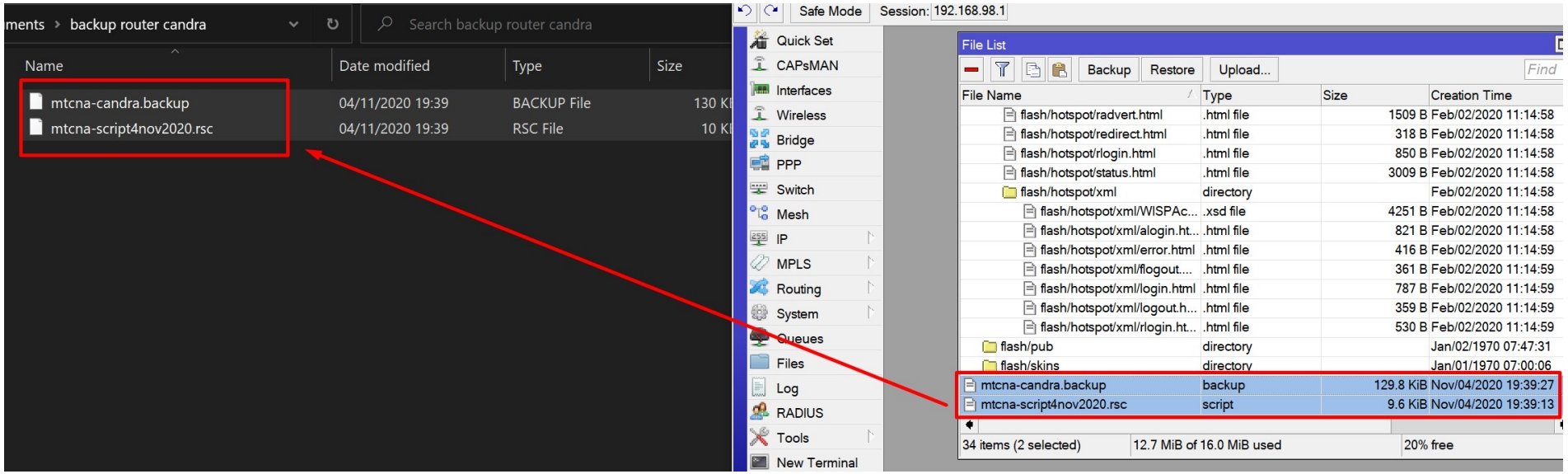
```
HOSTNAME-[tahun][bulan][tanggal]-[jam][menit]
```



- Waktu dan tanggal akan menyesuaikan saat kita melakukan backup.
- Selain itu juga dapat mengcustom nama file backup dan manambahkan password yang dapat digunakan ketika akan merestore.

RESTORE – BINARY FILE

- File Binnary dan Script dapat disimpan kedalam komputer/laptop menggunakan WinBox (drag & drop), FTP atau melalui WebFig.
- Tidak direcomendasikan menyimpan file backup hanya pada router.



BACKUP DAN RESTORE – SCRIPT FILE

- File export (.rsc) merupakan salah satu jenis file backup yang berupa script.
- File export menggunakan **type Plain Text (dapat di edit).**
- Berisi beberapa konfigurasi yang ada pada router.
- **Script tidak akan membackup settingan username dan password router.**
- Dapat juga membackup **sebagian konfigurasi** yang ada pada router.
- Untuk membuat File export harus menggunakan terminal/CLI.
- Konfigurasi dapat dipindahkan ke RouterBOARD yang berbeda.
- Restore harus menggunakan perintah **'/import'**

BACKUP – SCRIPT FILE

- Backup dan restore dengan menggunakan mode script dilakukan dengan
- perintah :
- **EXPORT**, akan menyimpan konfigurasi dengan bentuk script yang dapat di olah.
- **IMPORT**, akan menjalankan perintah yang terdapat dalam script.

- Perintah Export

```
[admin@idn] > export file=backup-all
```

- Export sebagian config (IP Address)

```
[admin@idn] > /ip address export file=cuma-ip
```

RESTORE–SCRIPT FILE

- Import digunakan untuk mengembalikan konfigurasi yang sudah di export
- Perintah import hanya tersedia di menu root (/).
- Bila konfigurasi yang sebelumnya sudah ada, maka tidak bisa di import kembali

- Perintah Import

```
[admin@idn] > import file-name=backup-all.rsc
```

PERBEDAAN BINNARY DAN SCRIPT FILE

Perbedaan	Script Backup	Binnary Backup
Command	Export / Import	Backup / Restore
Bisa dengan menu klik	No	Yes
Backup all config	No (user&Pass)	Yes
Need reboot to restore	No	Yes
Backup sebagian config	Yes	No
Bisa dibaca test editor	Yes	No

BACKUP DAN RESTORE

LAB

- Backup konfigurasi menggunakan binary (backup) dan script (export).
- Pindah kedua file tersebut ke leptop.
- Buka menggunakan text editor.
- Manakah dari kedua file tersebut yang bisa di edit (konfigurasi bisa dibaca melalui text editor).

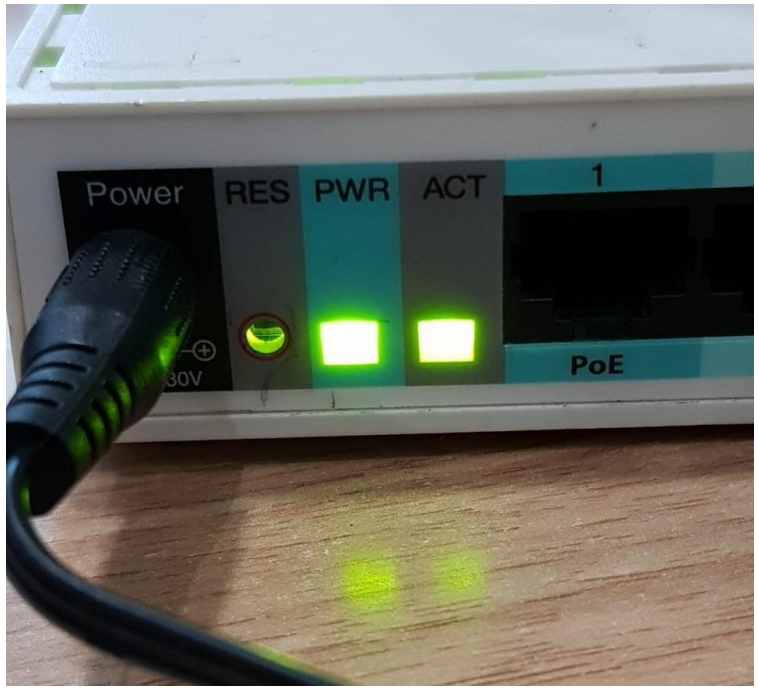
RESET KONFIGURASI

- Reset konfigurasi digunakan untuk mengembalikan setting ke default/settingan pabrik.
- Reset Konfigurasi Mikrotik di perlukan jika:
  - Lupa username atau password ketika akan login
  - Perlu menata dari nol, konfigurasi yang sudah komplek

- Reset Konfigurasi dapat dilakukan dengan cara:
  - **Hard Reset** (reset secara fisik).
  - **Soft Reset** (reset secara software).
  - **Install Ulang**.

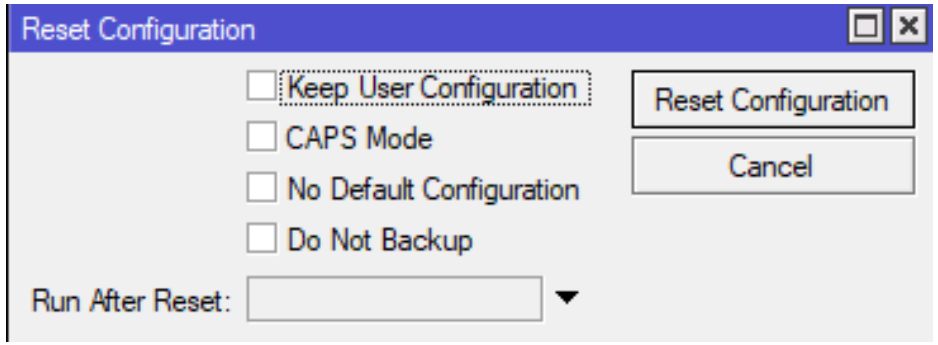
RESET KONFIGURASI – HARD RESET

- Reset dengan menjumper atau menggunakan tombol fisik yang ada dibagian belakang router



RESET KONFIGURASI – SOFT RESET

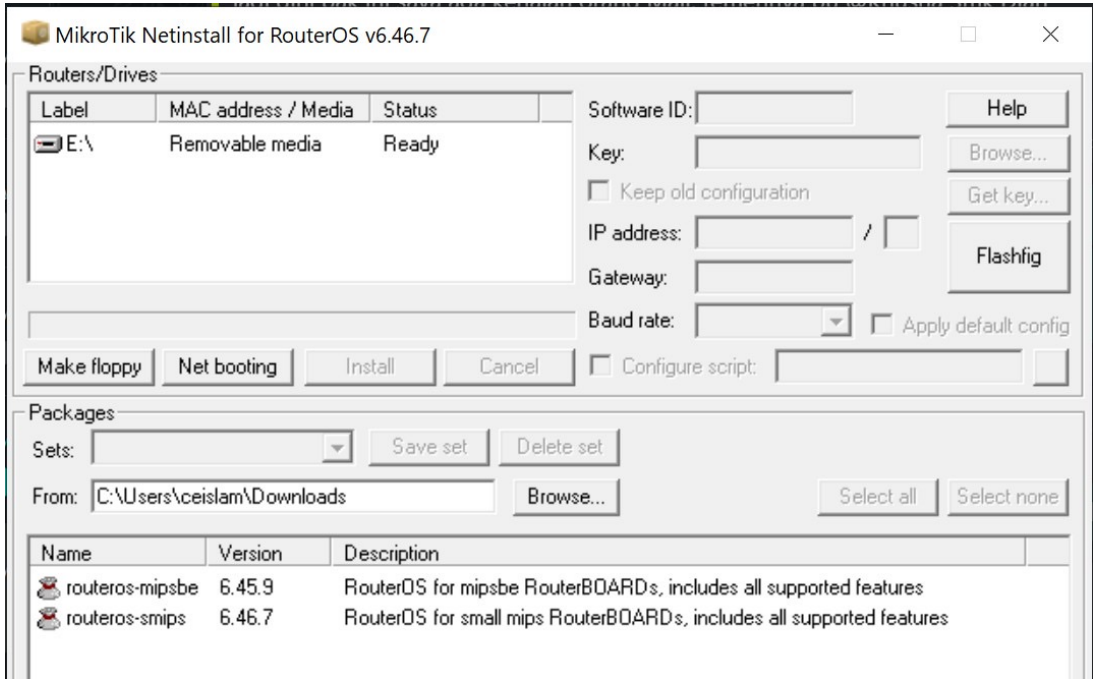
- Soft reset, reset by software (bila masih bisa akses ke Mikrotik)
  - **System > Reset Configuraton**



  - **Keep User Configuration**, reset semua konfigurasi kecuali user dan password.
  - **CAPS Mode,** setting mode CAPs (mode AP yang dimanage oleh CAPsMAN).
  - **No Default Configuration**, menghapus semua settingan yang ada di router.
  - **Do Not Backup**, ketika di reset RouterOS tidak akan melakukan backup file.
  - *) Apabila semua parameter tidak di pilih maka router akan kembali ke factory default

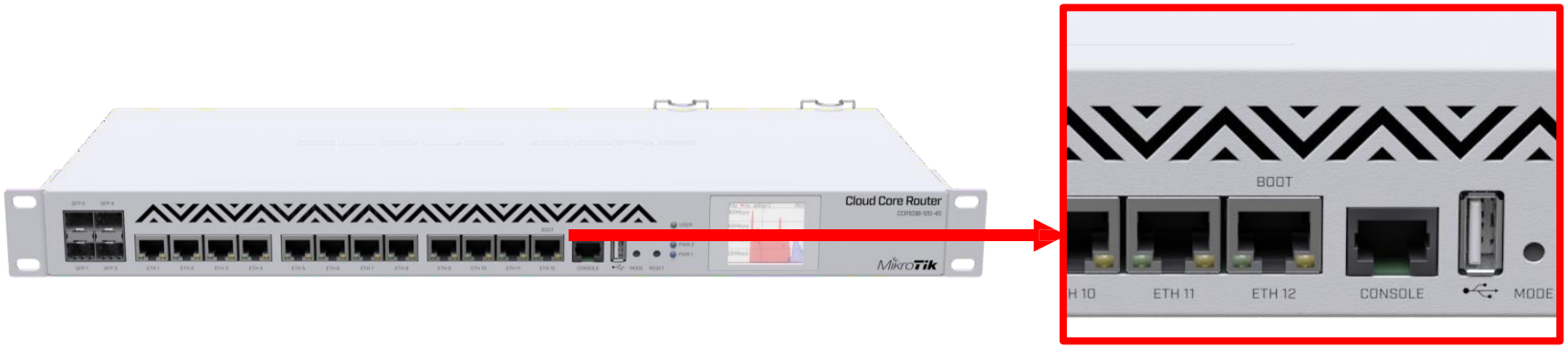
RESET KONFIGURASI – INSTALL ULANG

- Mikrotik dapat di install ulang layaknya system operasi lain.
- Install ulang dapat mengembalikan mikrotik ke posisi awal/default
- Disarankan ketika install ulang harus menggunakan aplikasi **Netinstall**.



NETINSTALL

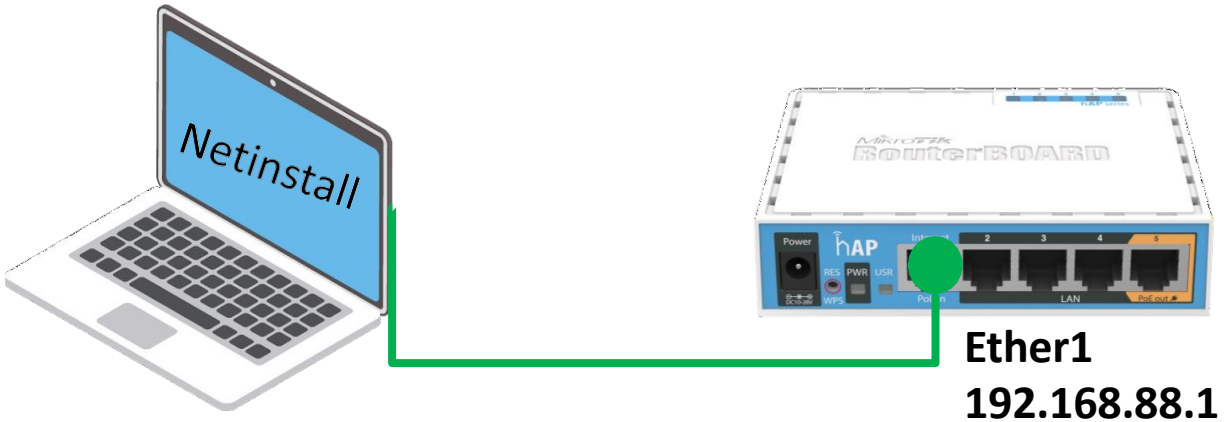
- Software yang di sediakan oleh Mikrotik untuk install ulang RouterOS.
- Netinstall dapat di download di situs resmi Mikrotik.
- Netinstall running under Windows.
- PC/Komputer yang menjalankan netinstall harus terhubung langsung dengan router melalui UTP atau LAN dan harus menggunakan ether1 (kecuali CCR dan RB1xxx harus menggunakan port terakhir)



INSTALL ULANG – NETINSTALL (1)

LAB

- Buat topologi seperti berikut:

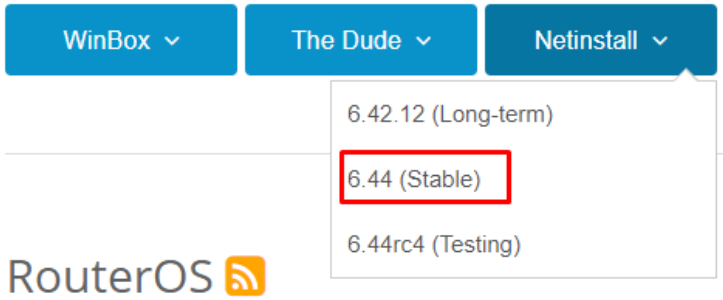


- Pastikan router terkoneksi ke leptop (boot server) menggunakan ether1

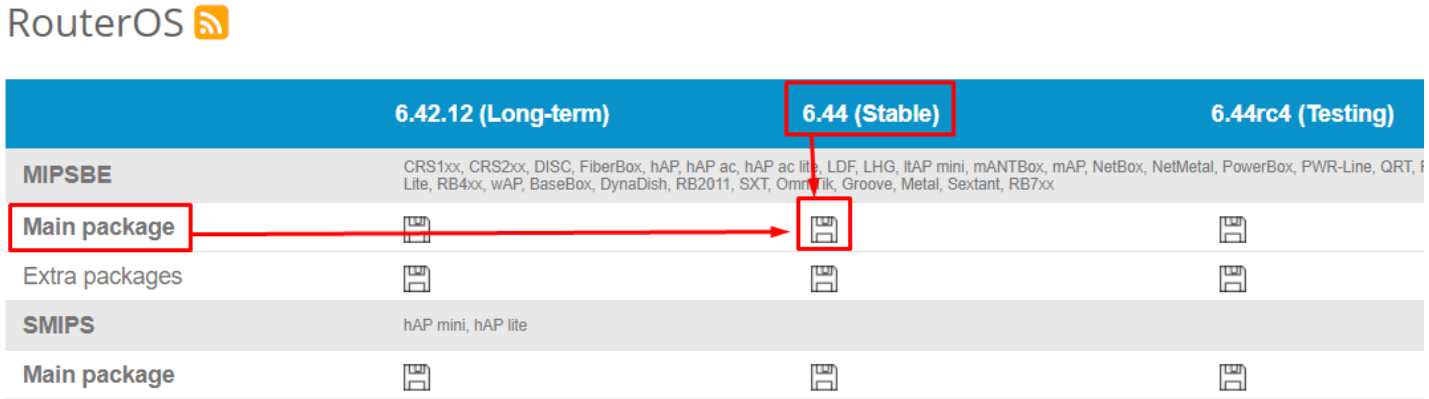
INSTALL ULANG – NETINSTALL (2)

LAB

- Download beberapa tool yang perlu dipersiapkan untuk install ulang router.
  - Netinstall



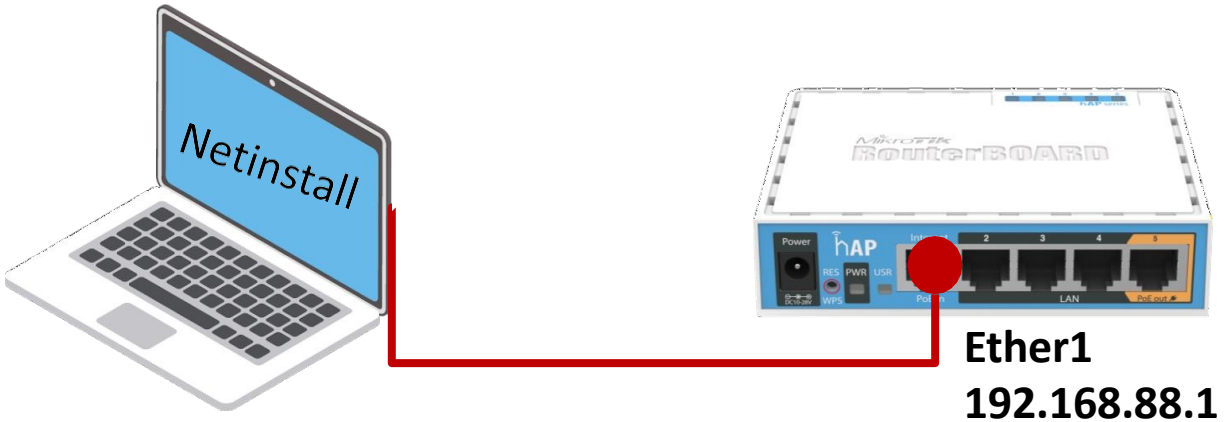
  - Main packages (type arsitektur di sesuaikan)



INSTALL ULANG – NETINSTALL (3)

LAB

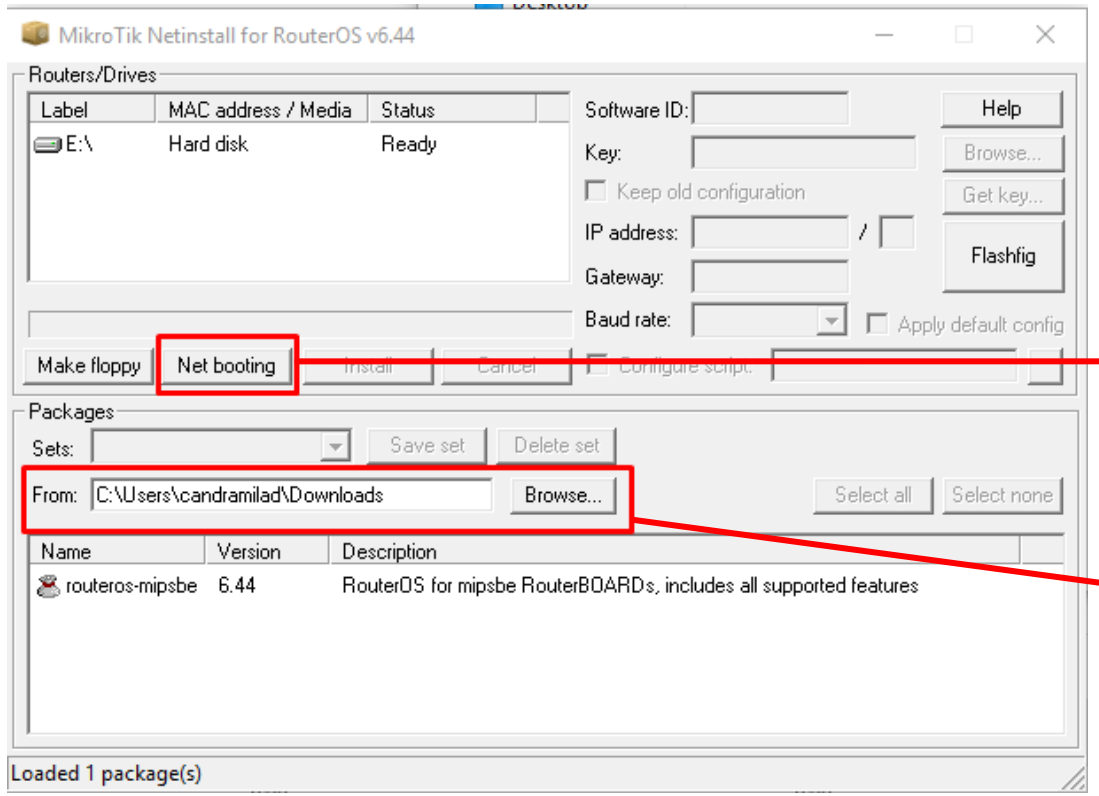
- Disable beberapa security di windows :
- Windows defender off
- Windows firewall off
- Antivirus off
- Adapter Virtual off



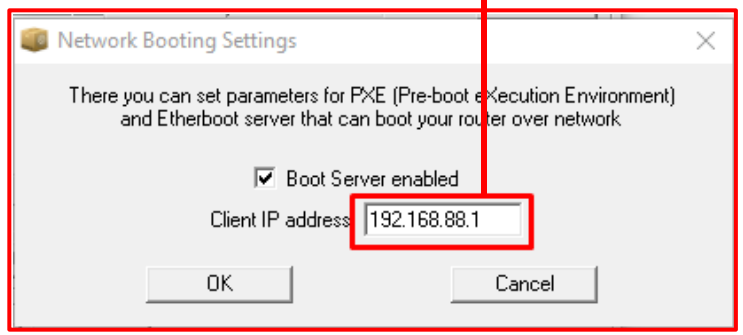
INSTALL ULANG – NETINSTALL (4)

LAB

- Jalankan Netinstall



IP RouterOS

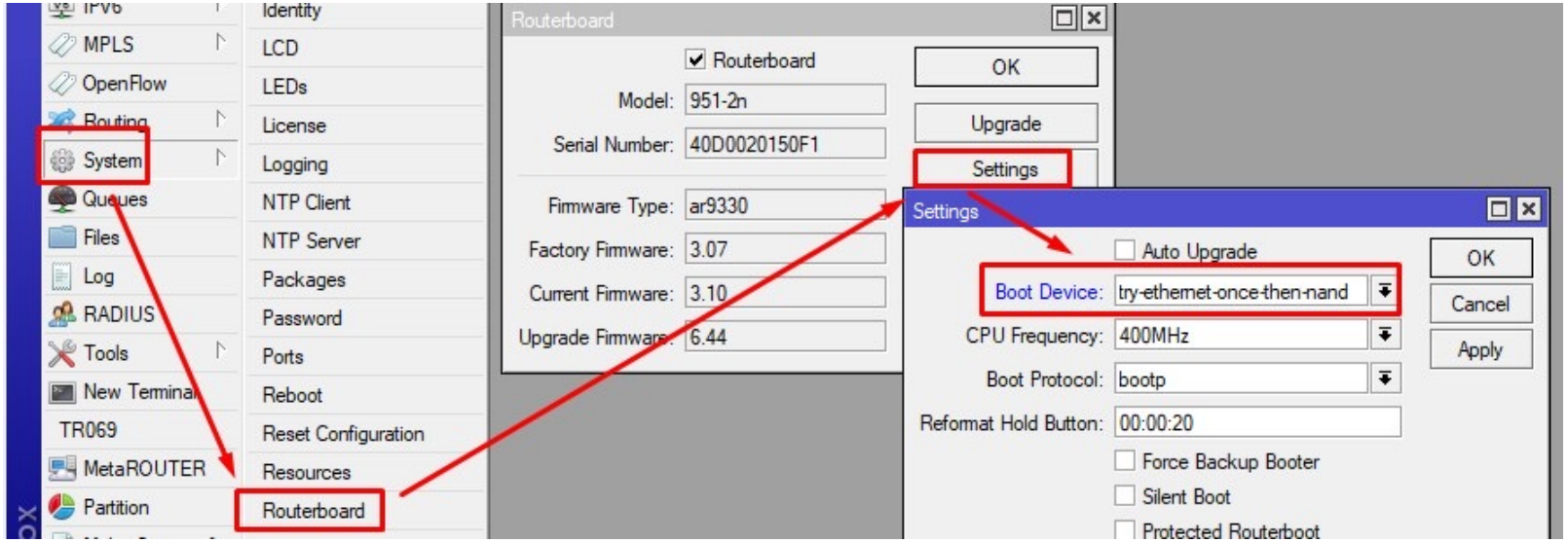


Arahkan ke folder dimana main paket (.npk) routerOS tersimpan di laptop.

INSTALL ULANG – NETINSTALL (OTOMATIS) (5)

LAB

- Setting RouterBOOT, supaya ketika device booting akan memilih ethernet dulu
  - **System > Routerboard > Setting**



  - Reboot router (**system > reboot**)

INSTALL ULANG – NETINSTALL (MANUAL) (6)

LAB

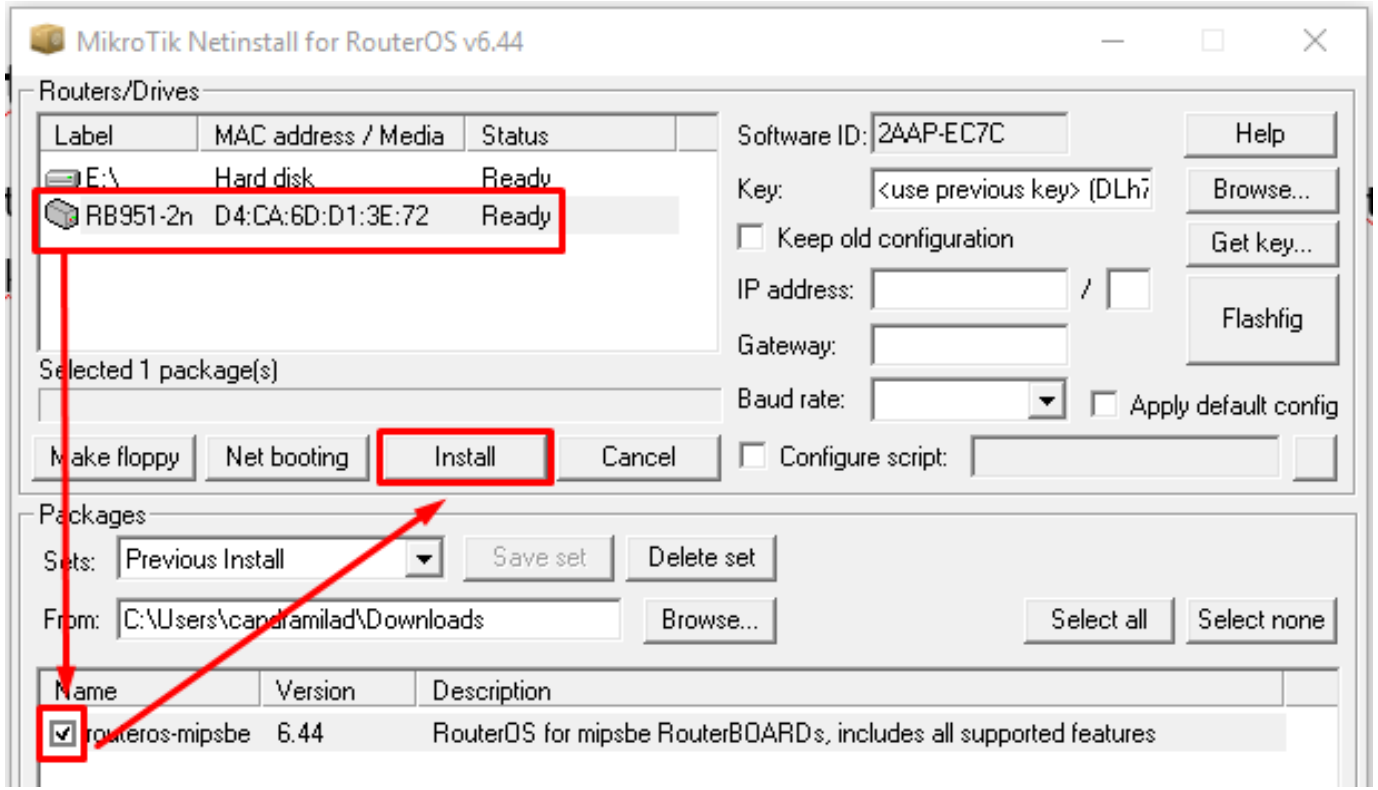
- Melalui Tombol Reset :
    1. lepas kabel power
    2. tekan tombol reset lalu colokan kabel power
    3. Indikator lampu "usr" / "act"

        nyala - kedap kedip - nyala - redup
    4. lepas tombol reset

INSTALL ULANG – NETINSTALL (6)

LAB

- Setelah device di reboot, pastikan terdeteksi 1 device mikrotik di netinstall
- Klik install, untuk memulai installasi

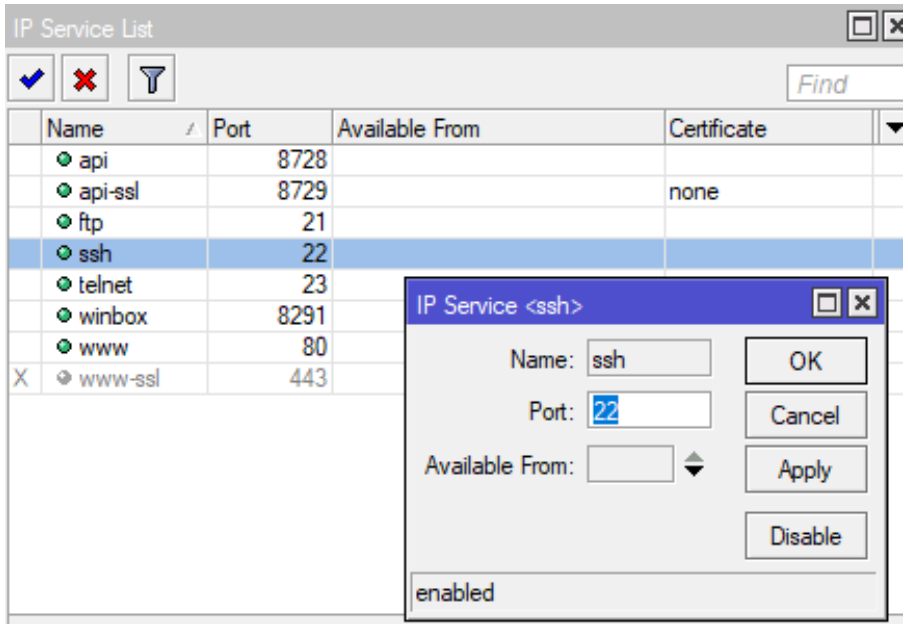


TROUBLESHOOTING – INSTALL ULANG

- RouterBOARD tidak terbaca di Netinstall.
- Packages List tidak bisa dipilih (dicentang).

IP SERVICES

- IP services merupakan berbagai cara untuk masuk/login kedalam RouterOS
- Dapat juga digunakan untuk membatasi user untuk login dari salah satu service dengan cara mematikan atau merubah nilai port pada service tersebut.



IP SERVICES

LAB

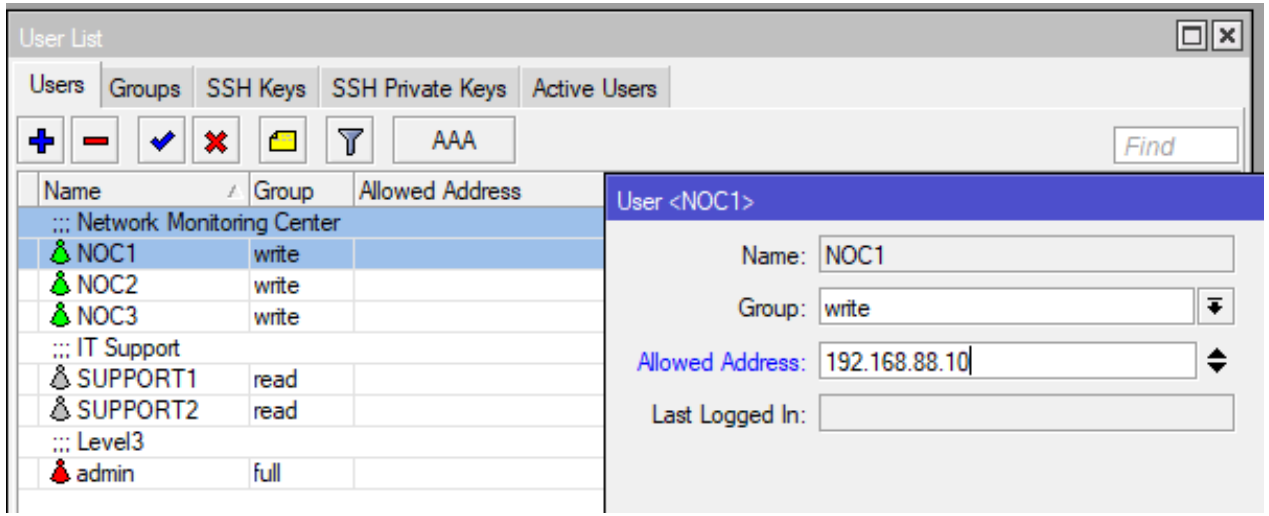
- Disable semua service **kecuali SSH dan Winbox.**
- Rubah port SSH **menjadi 9022 dan winbox menjadi 3000**.
- Login kembali ke router menggunakan default port.
- Login kembali ke router menggunakan port yang sudah di rubah.

ROUTEROS LOGIN MANAGEMENT

- RouterOS Login Management digunakan untuk mengatur siapa saja yang diijinkan masuk kedalam router (Console, Serial terminal, Telnet, SSH, WebFig, Winbox.
- Untuk mengatur dan mambuat siapa saja yang boleh masuk ke dalam router terdapat 2 option : lokal database dan RADIUS server.
- Manajemen user dilakukan dengan:
  - **GROUP** – profile pengelompokan user, menentukan previlage yang bisa diperoleh suatu user
  - **USER** – merupakan login (username & password dari suatu user)

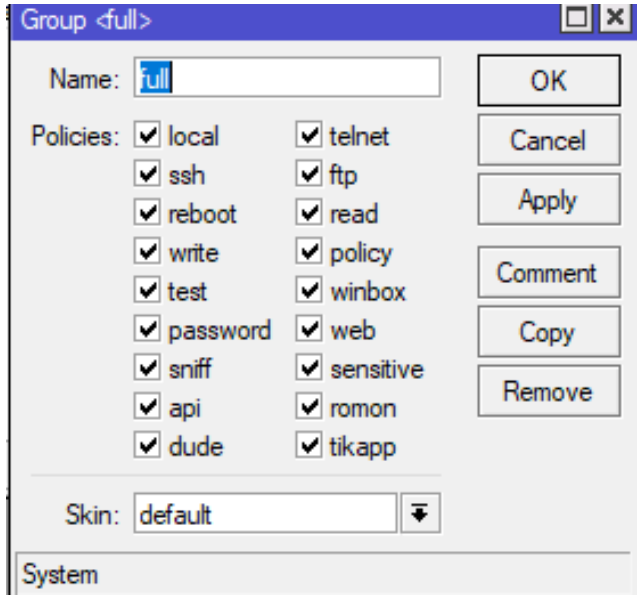
ROUTEROS LOGIN MANAGEMENT – USER

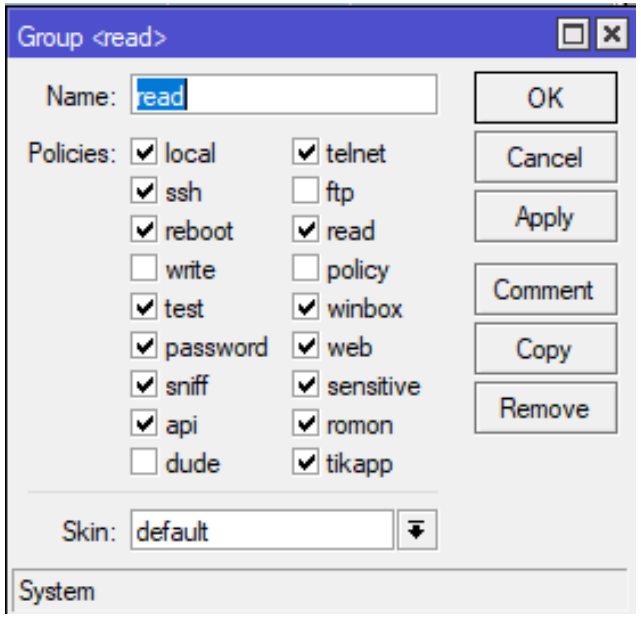
- By default mikrotik menggunakan **user admin tanpa password untuk login**.
- Selain itu kita bisa membuat user baru dan memberikan hak akses yang berbeda terhadap user tersebut.
- Dapat juga melakukan pembatasan berdasarkan IP address yang digunakannya.

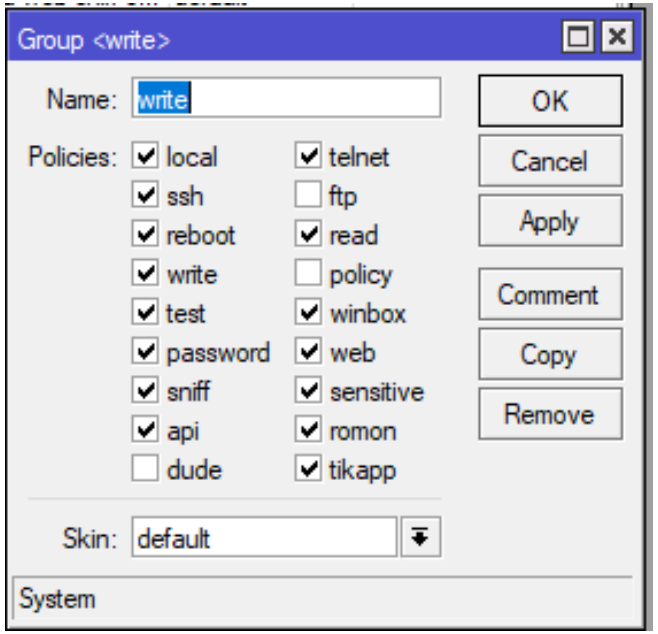


ROUTEROS LOGIN MANAGEMENT – GROUP

- Group digunakan untuk memberikan hak akses terhadap user.
- By default terdapat 3 Group di mikrotik : **full, write dan read.**





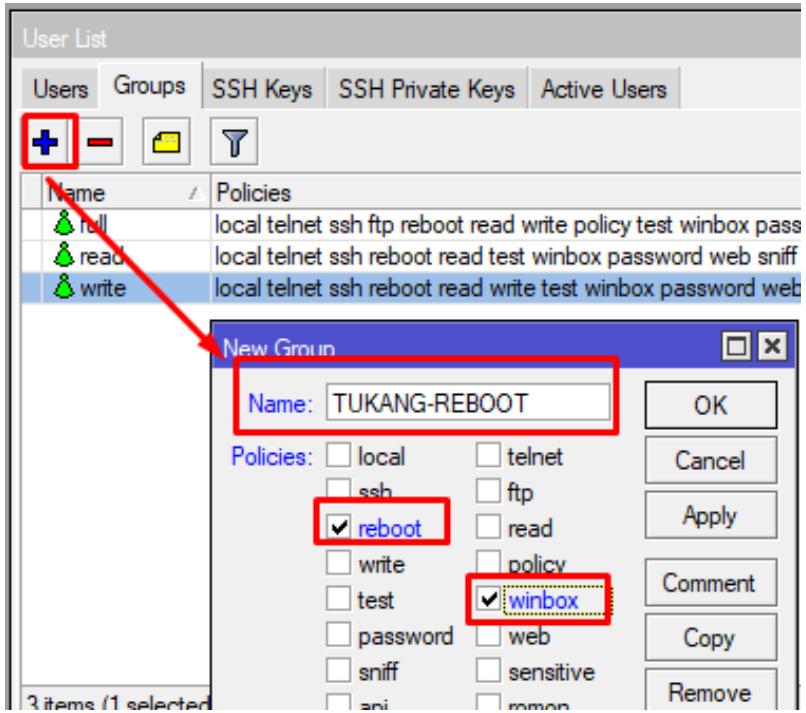


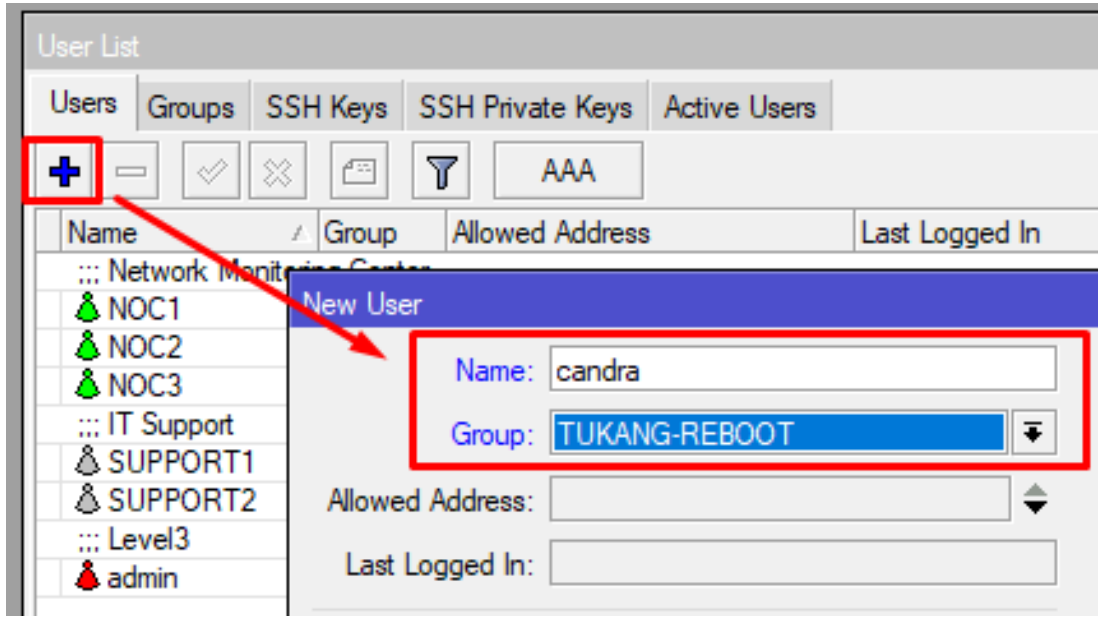
- kita juga bisa membuat custom group baru sesuai dengan aturan yang kita inginkan.

USER LOGIN MANAGEMENT

LAB

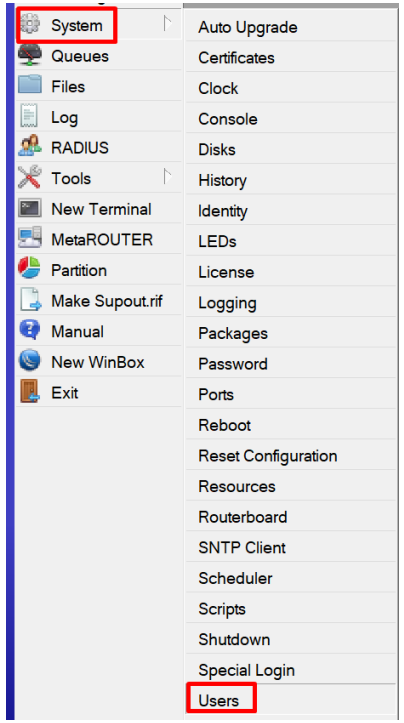
- Buatlah sebuah user dengan nama “Tojeh”
- Berikan privilege agar user tersebut hanya bisa melakukan reboot via winbox.

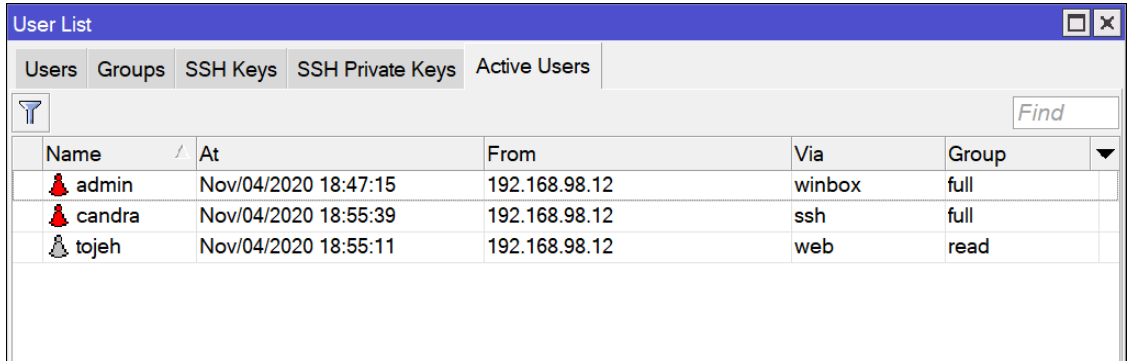




ACTIVE USERS

- Untuk melihat sesi user yang sedang melakukan koneksi ke Router
- Cara checknya melalui menu **System > Users > Active Users**





INFORMASI TAMBAHAN

- wiki.mikrotik.com – Dokumentasi dan artikel mengenai RouterOS.
- forum.mikrotik.com – forum komunikasi antar pengguna RouterOS.
- mum.mikrotik.com – Mikrotik User Meeting
- Distributor and consultant support
  support@mikrotik.com

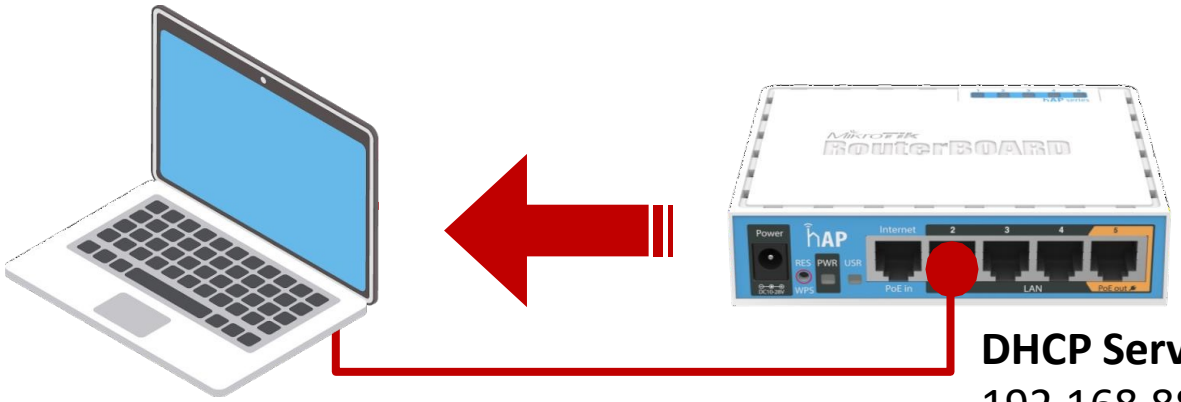
MODUL 2
DHCP DAN ARP

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

- DHCP merupakan service yang digunakan untuk mempermudah distribusi IP address dalam suatu jaringan.
- DHCP running dalam satu broadcast domain (satu jaringan)
- Terdapat 3 type DHCP :
  - **DHCP Server** : sebagai **penyedia** layanan DHCP ke client
  - **DHCP Client** : sebagai **penerima** layanan DHCP dari server
  - **DHCP Relay** : **penghubung** layanan DHCP Server ke Client

DHCP SERVER DAN DHCP CLIENT

- DHCP Server : **penyedia** layanan pool IP
- DHCP Client : **penerima** layanan IP dari DHCP Server



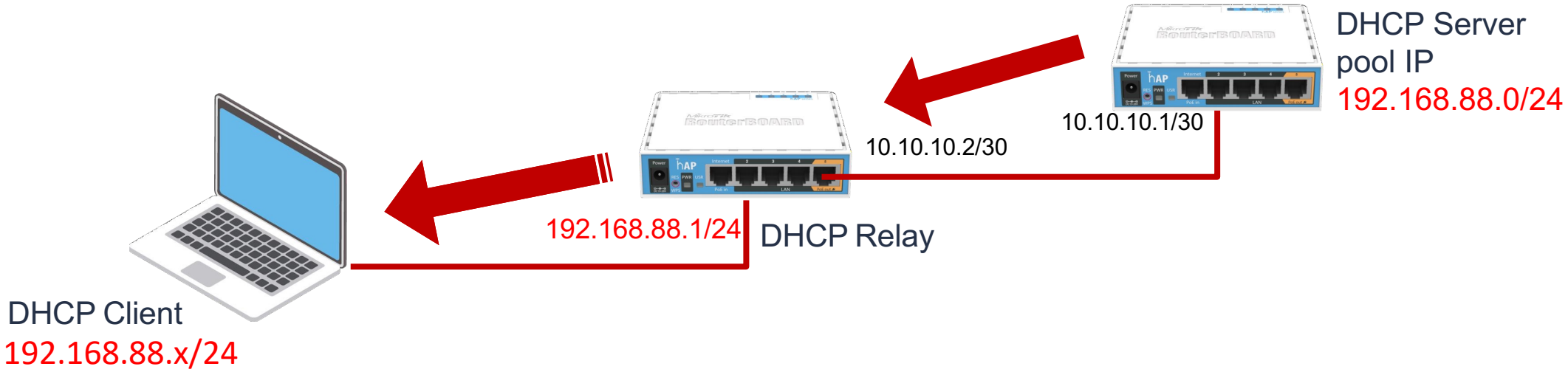
DHCP Client
192.168.88.X/24 (DHCP)

DHCP Server
192.168.88.1/24

Pool IP 192.168.88.2 – 192.168.88.254

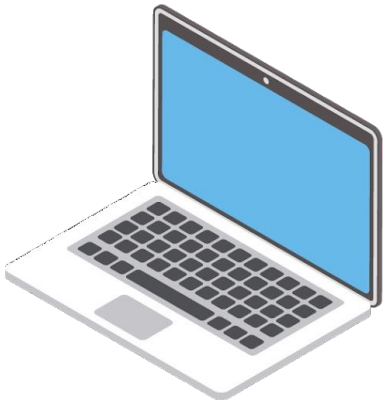
DHCP RELAY

- DHCP Relay : penerus layanan dari server ke client



- DHCP Relay memanfaatkan DHCP server yang terpusat di router lain

DHCP PROCESS – D.O.R.A



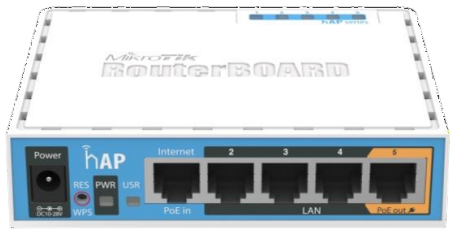
DHCP Client

(1) **D**iscover (Broadcast : server dimana ya?)

(2) **O**ffer (Unicast : aku punya address ***a.b.c.d*** mau engga?)

(3) **R**equest (Broadcast : mau, minta address lengkapnya dong)

(4) **A**ck (Unicast : OK, silahkan)



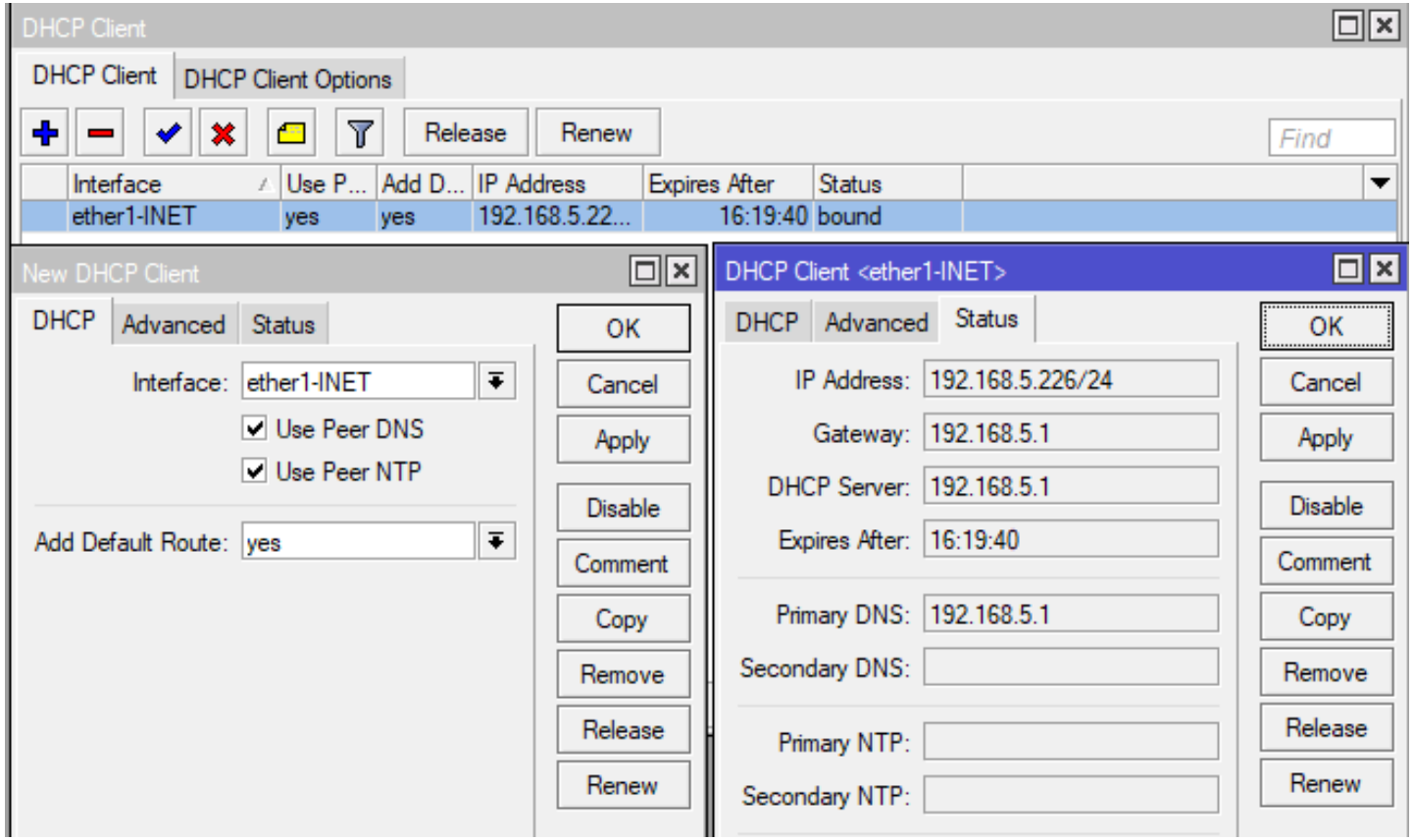
DHCP Server

DHCP CLIENT

- DHCP Client digunakan untuk merequest address secara otomatis ke penyedia (server).
- Parameter yang didapat ketika request DHCP Client :
  - IP Address
  - Subnet mask
  - Default gateway
  - DNS Server, dan informasi tambahan lain.
- Mikrotik SOHO router by default mempunyai settingan DHCP client pada interface ether1 (WAN).

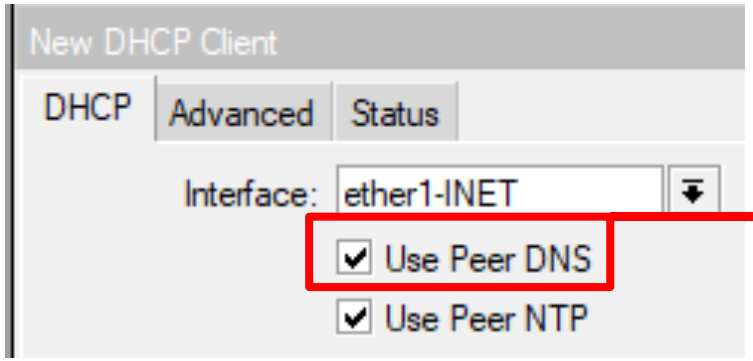
DHCP CLIENT

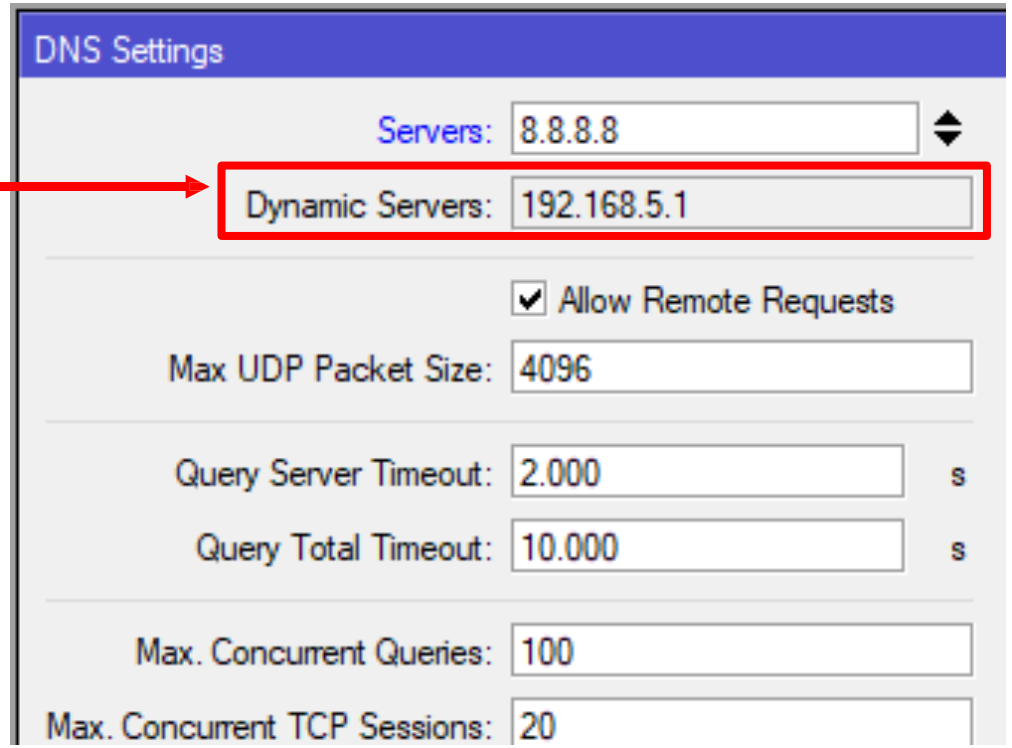
- **IP > DHCP Client**



DHCP CLIENT – USE PEER DNS

- By default DHCP client juga akan meminta IP DNS Server. Ketika Use Peer DNS enable





- Walaupun dapat juga DNS kita definisikan secara manual.

DHCP SERVER

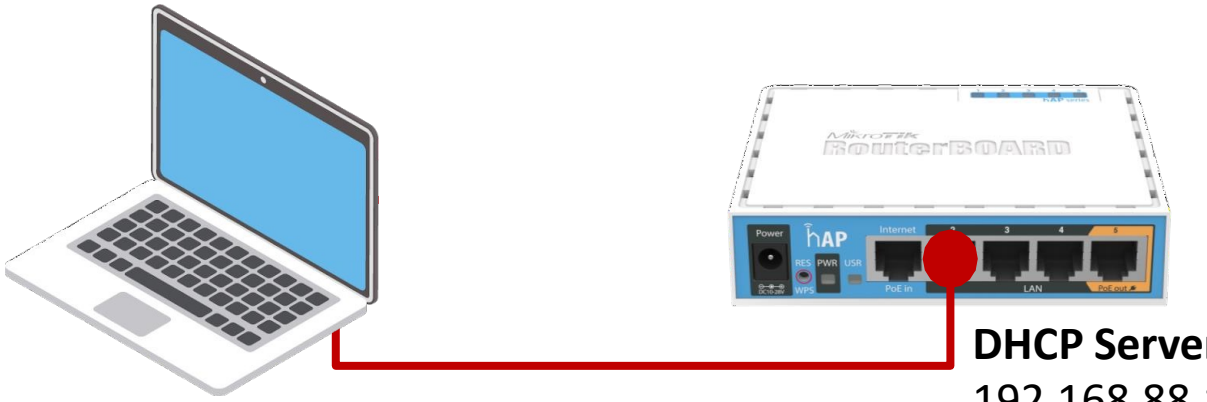
- Secara otomatis akan memberikan alokasi range IP ke host yang merequest IP.
- Sebelum setting DHCP server, pastikan interface tersebut sudah tersetting IP Address.
- Untuk mengkonfigurasikan DHCP server gunakan perintah “**DHCP Setup**”

pada menu **IP > DHCP-Server.**

DHCP SERVER (1)

LAB

- Setting DHCP server pada router, sehingga leptop dapat IP secara otomatis melalui router



DHCP Client
192.168.88.X/24 (DHCP)

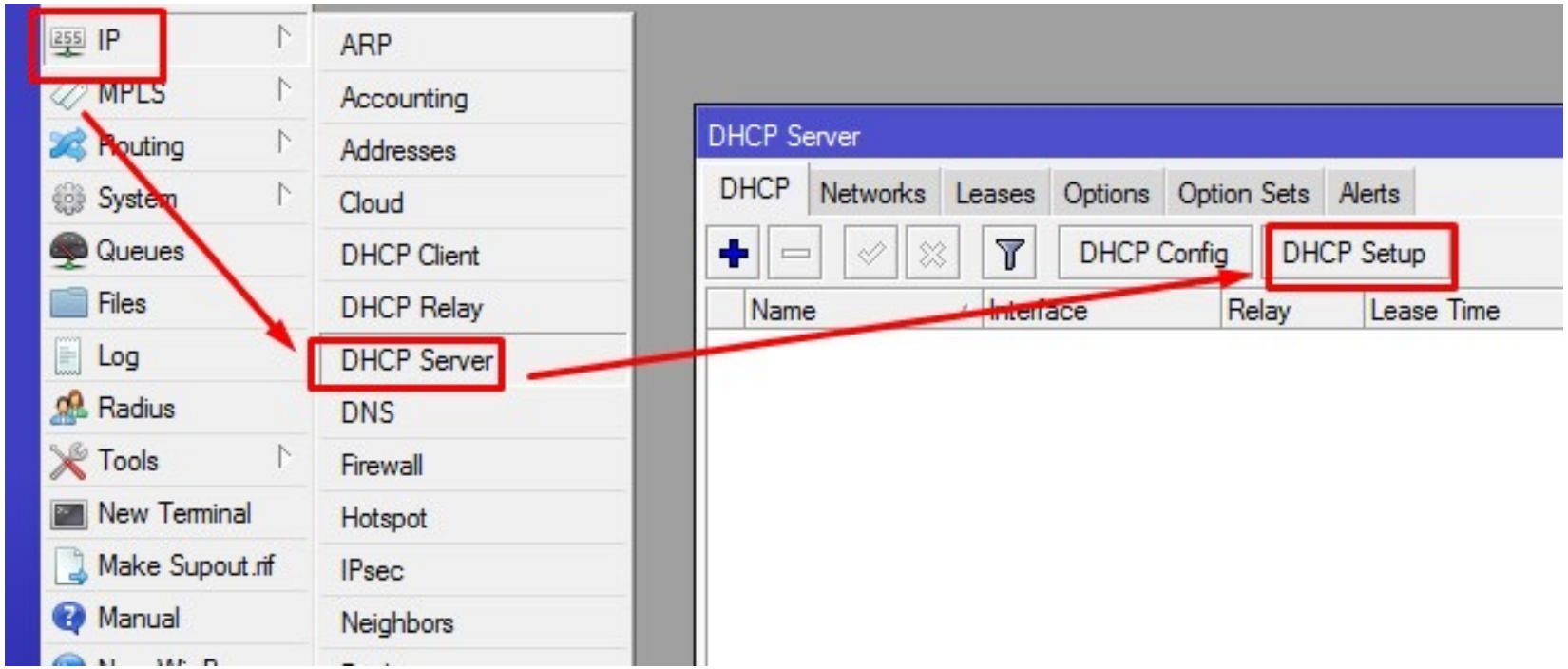
DHCP Server
192.168.88.1/24

Pool IP 192.168.88.2 – 192.168.88.254

DHCP SERVER (2)

LAB

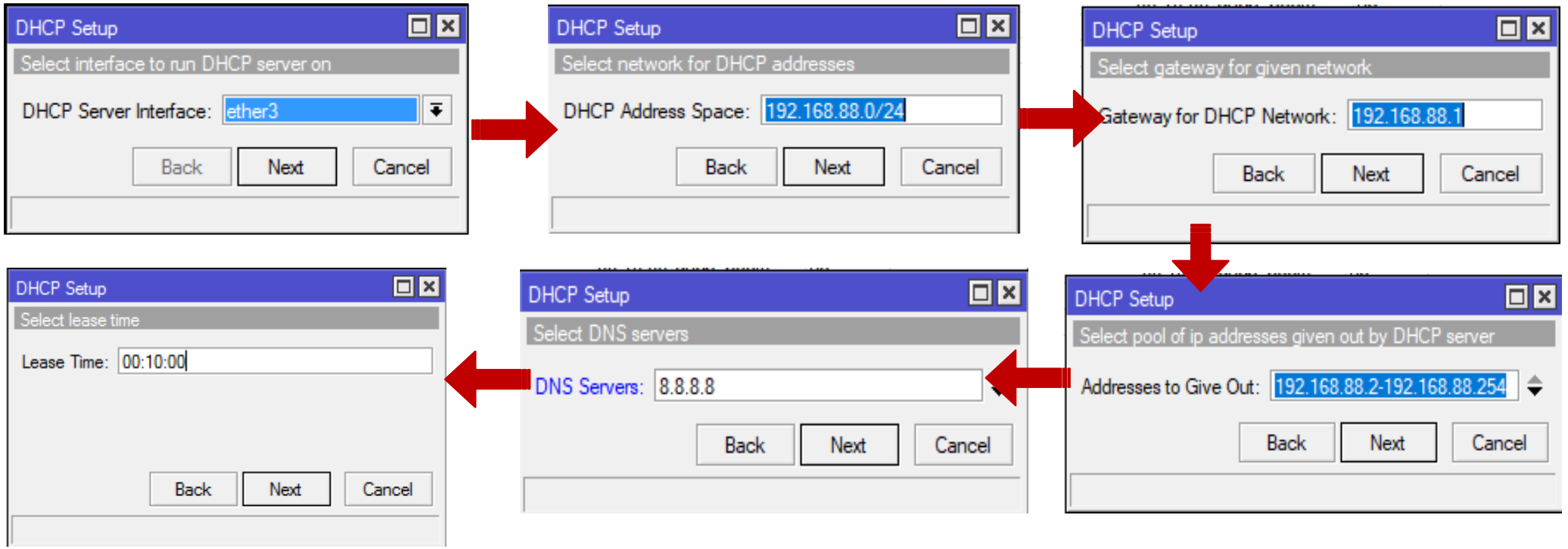
- **IP > DHCP Server > Setup**



DHCP SERVER (3)

LAB

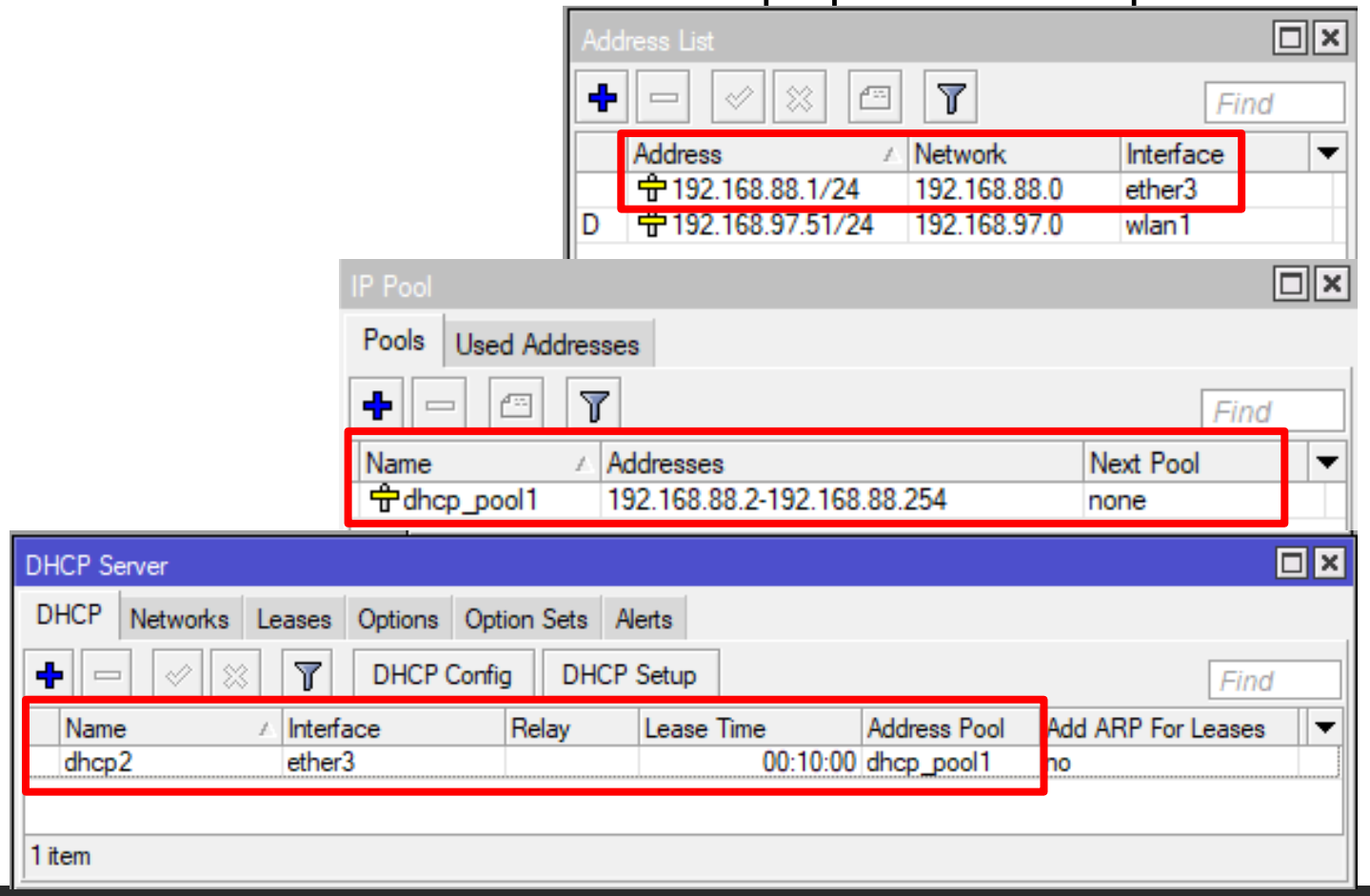
- **IP > DHCP Server > Setup**



- Lakukan verifikasi dari laptop masing-masing dan pastikan mendapatkan IP secara otomatis.

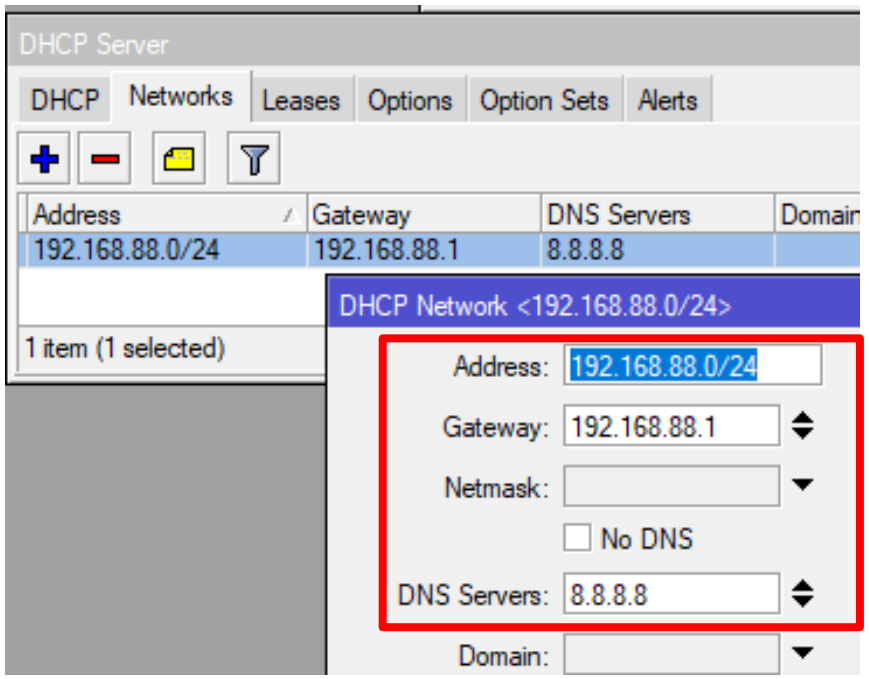
DHCP SERVER – SETUP WIZARD

- DHCP setup wizard secara otomatis akan membuatkan beberapa parameter seperti :
  - Dynamic IP pool
  - DHCP server setting
  - DHCP Network



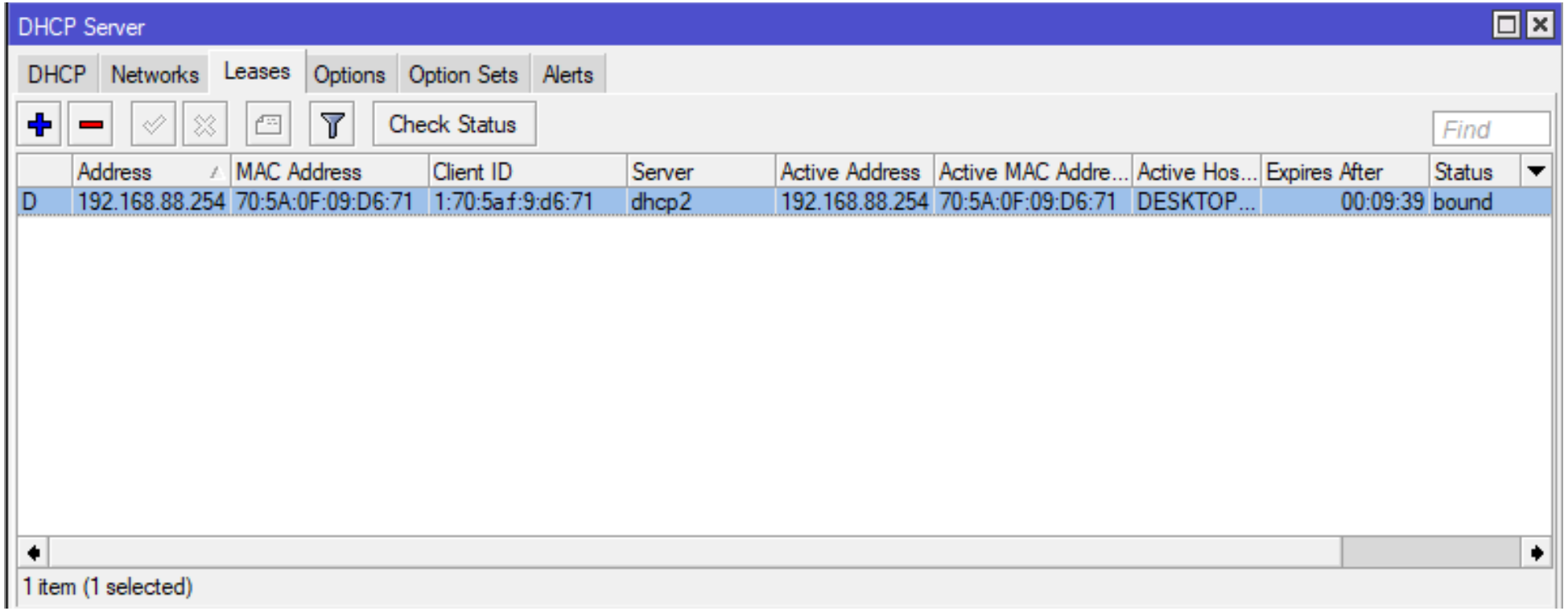
DHCP SERVER – SETUP WIZARD

- DHCP setup wizard secara otomatis akan membuatkan beberapa parameter seperti :
  - Dynamic IP pool
  - DHCP server setting
  - DHCP Network



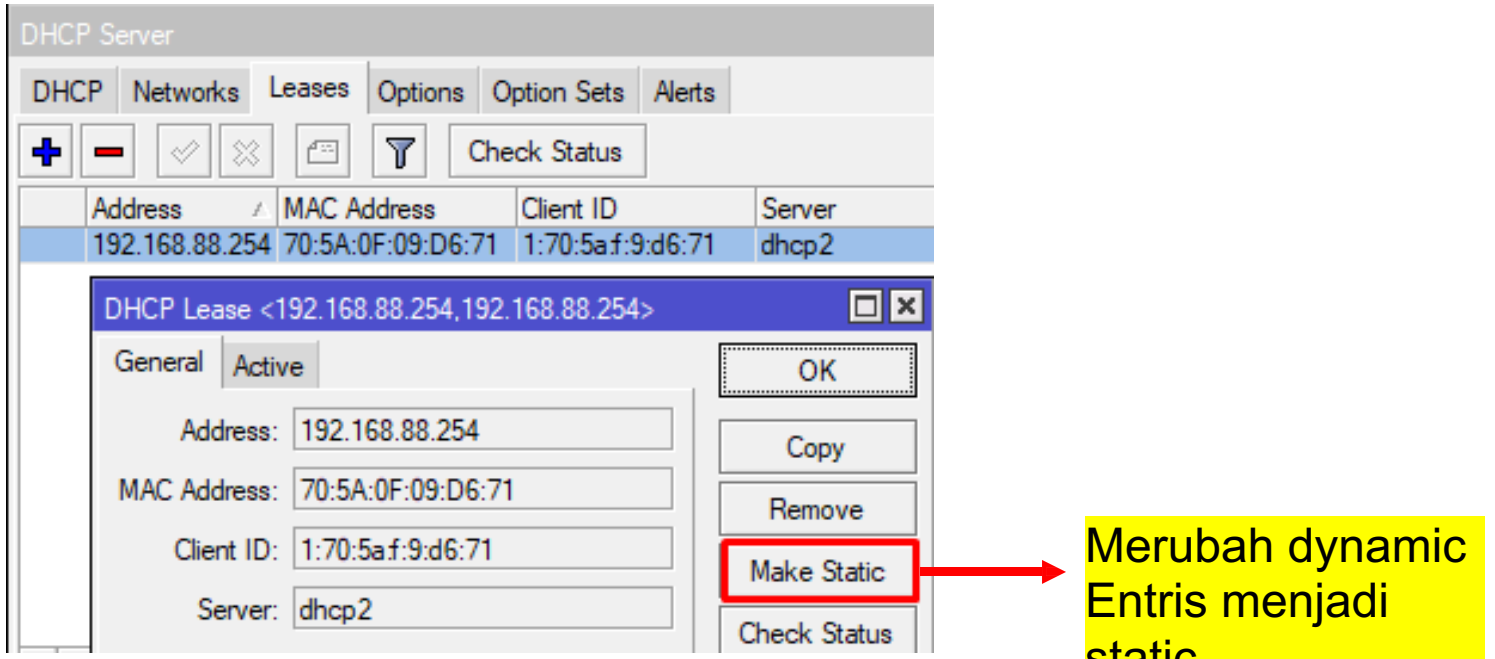
DHCP LEASES

- Untuk melihat list client yang mendapatkan IP DHCP secara otomatis bisa melalui menu **IP > DHCP Server > Leases.**



DHCP STATIC

- Dapat memungkinan untuk memberikan alamat IP address yang sama pada device yang sama berdasarkan MAC Address.
- DHCP Server dapat di gunakan tanpa Dynamic IP pool dan hanya menetapkan alamat yang telah dikonfigurasikan.
- **IP > DHCP Server > Leases**



Merubah dynamic Entris menjadi static

DHCP STATIC

LAB

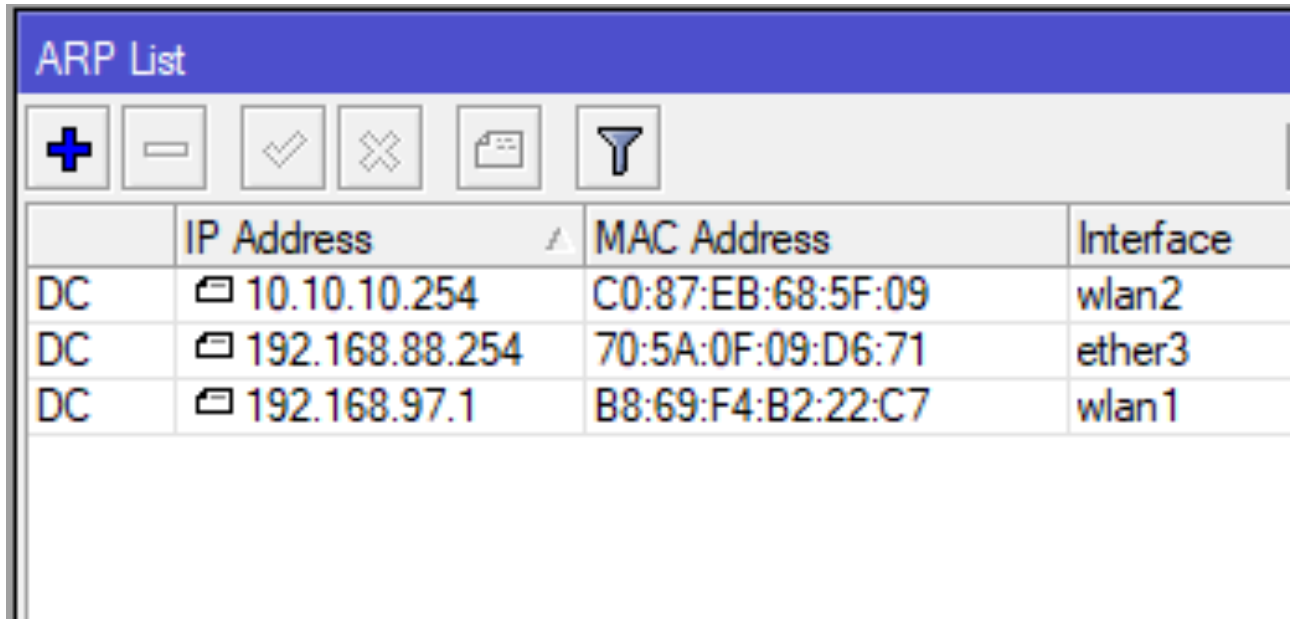
- Buat static leases untuk laptop.
- Rubah IP address leases untuk laptop menjadi 192.168.88.123.
- Renew IP address di laptop.
- Check kembali IP address di laptop

ARP

- Address Resolution Protocol.
- Digunakan untuk mapping IP address (Layer 3) dengan MAC address (Layer 2).
- Untuk menghubungkan kedua device informasi ARP keduanya harus saling memiliki.
- ARP bekerja secara dynamic (otomatis).
- Semua interface memancarkan ARP (enable).
- Dapat juga dikonfigurasikan secara manual (Static ARP).

ARP TABLE

- Berisi informasi mengenai IP address, MAC address dan interface yang terkoneksi ke router.
  - **IP > ARP**



STATIC ARP

- Mencatat informasi ARP client secara static/manual.
- Digunakan untuk masalah security.
- Untuk static ARP, ARP mode di interface harus di konfigurasikan menjadi **“Reply-only”.**
- **Reply-only** hanya dapat membaca kombinasi IP dan MAC address pada ARP Table secara static.
- Device hanya bisa konek ke router, apabila informasinya (IP dan MAC address) terdaftar di ARP.

ARP STATIC

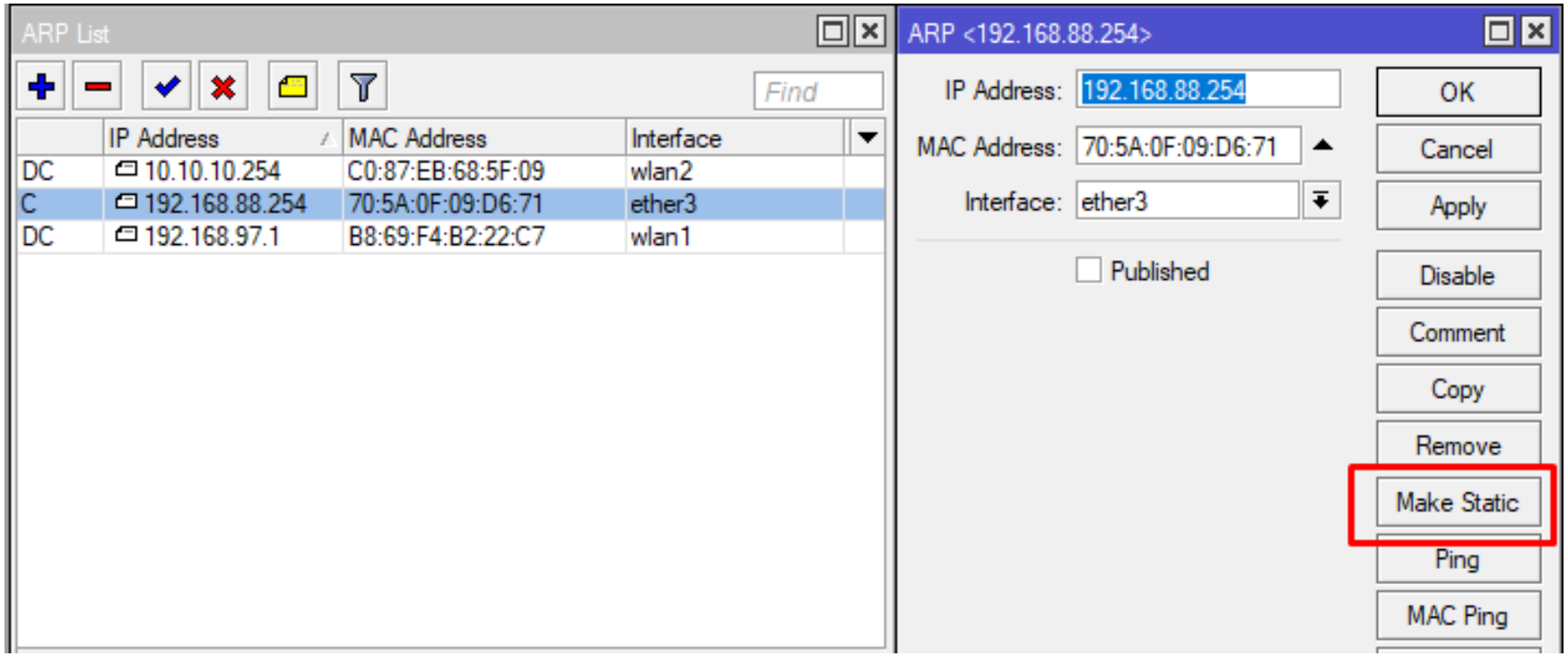
LAB

- Rubah ARP entries untuk laptop menjadi static.
- Rubah arp mode di interface yang mengarah ke laptop menjadi Reply-only.
- Pastikan laptop masih bisa terkoneksi ke jaringan dan ke internet.
- Rubah informasi MAC address laptop di ARP table.
- Test ping ke jaringan dan test koneksi internet.

ARP STATIC (1)

LAB

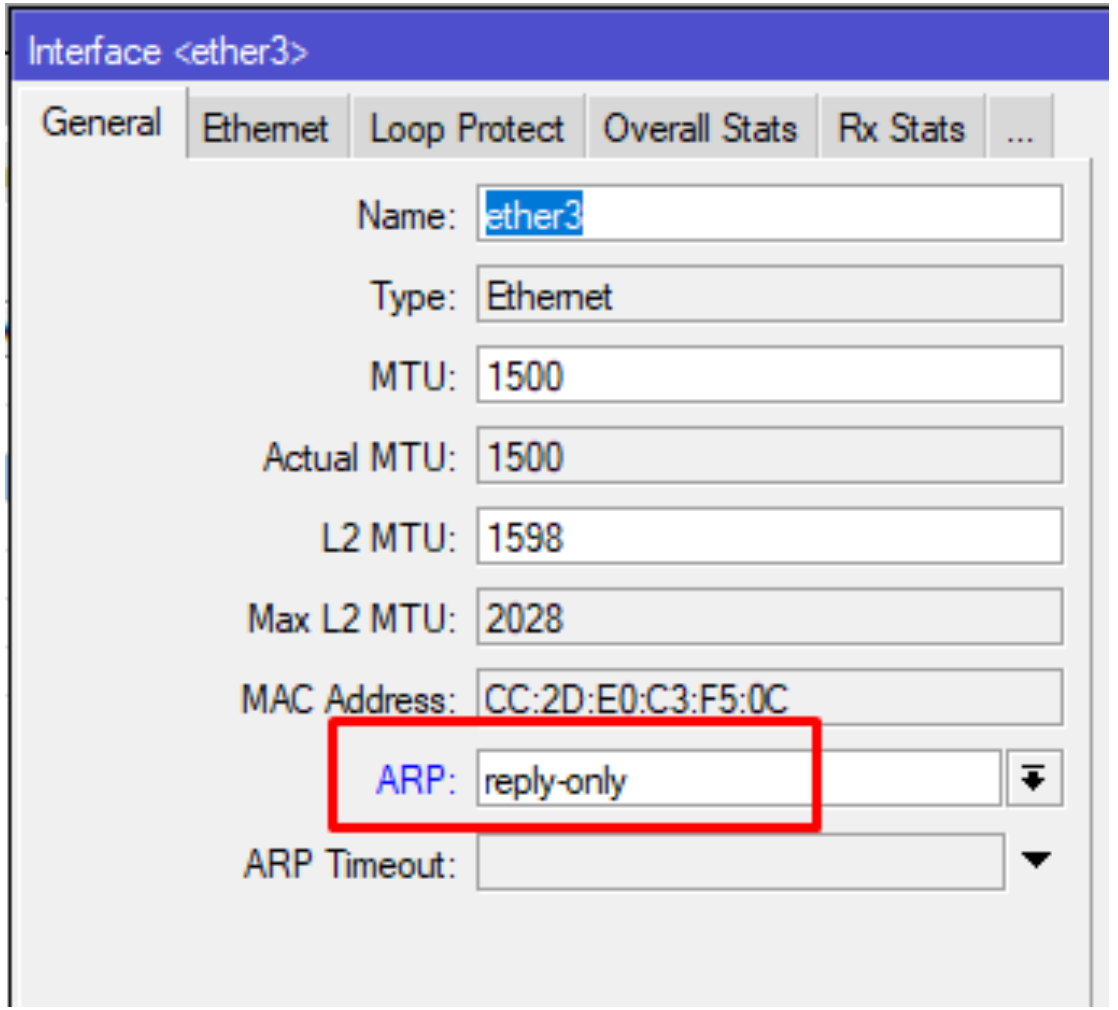
- **IP > ARP**



ARP STATIC (2)

LAB

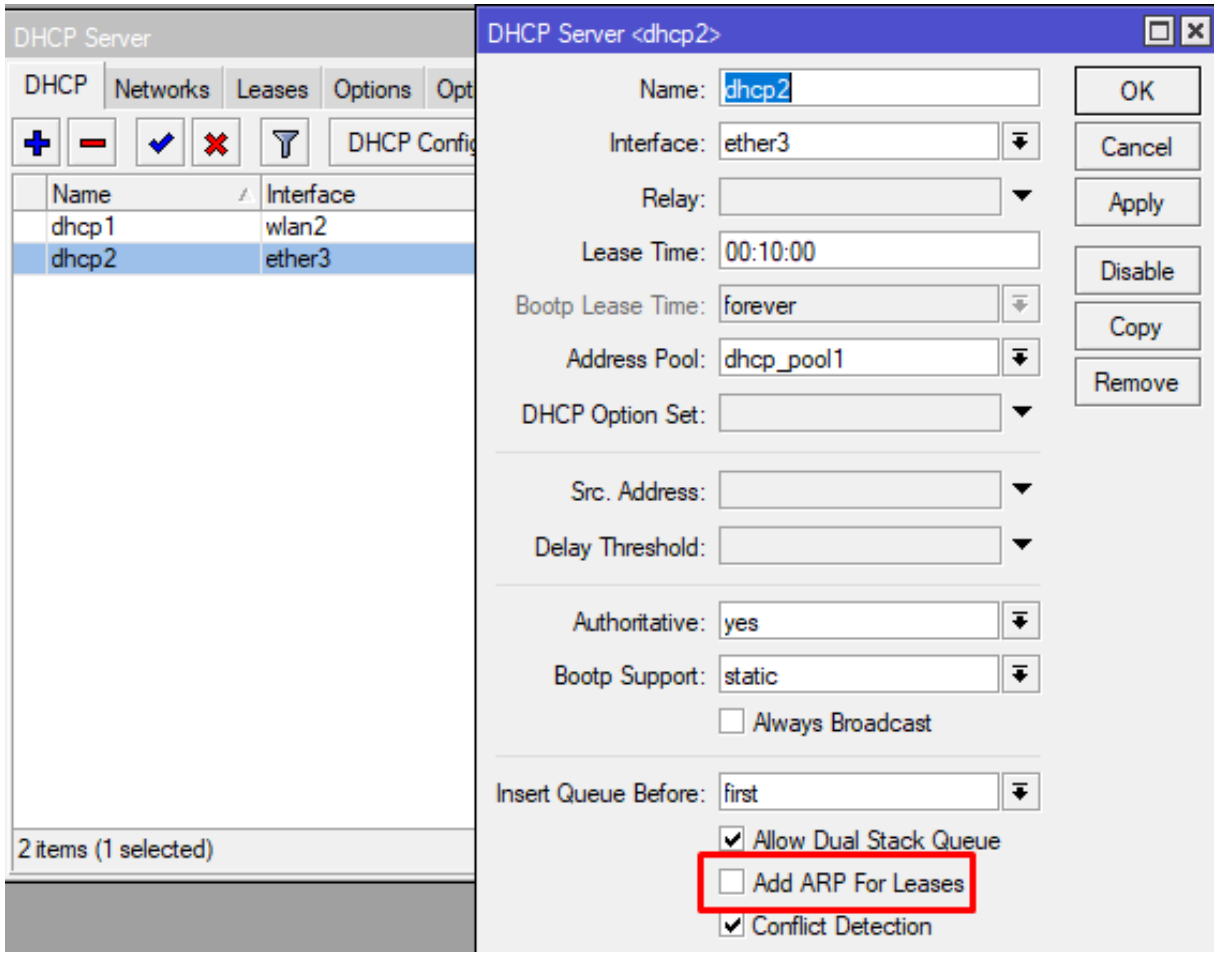
- **Interface > ether3**



DHCP DAN ARP

- DHCP Server dapat manambahkan ARP entri secara otomatis.
- Dengan mengkombinasikan static leases dan reply-only pada interface DHCP server.
- Fungsinya untuk alasan security, device yang sudah mandapatkan DHCP
- address tidak dapat mengganti addressnya ke alamat yang lain.

DHCP DAN ARP


DHCP Server
DHCP
Networks
Leases
Options
Opt
DHCP Config
Name
Interface
dhcp1
wlan2
dhcp2
ether3
2 items (1 selected)
DHCP Server <dhcp2>
Name: dhcp2
Interface: ether3
Relay:
Lease Time: 00:10:00
Bootp Lease Time: forever
Address Pool: dhcp_pool1
DHCP Option Set:
Src. Address:
Delay Threshold:
Authoritative: yes
Bootp Support: static
Always Broadcast
Insert Queue Before: first
Allow Dual Stack Queue
Add ARP For Leases
Conflict Detection
OK
Cancel
Apply
Disable
Copy
Remove

LAB DHCP STATIC LEASES WITH ARP

LAB

- Melanjutakan lab sebelumnya
- Pastikan laptop konek ke router dan mendapatkan IP DHCP server secara otomatis.
- Aktifkan ‘Add ARP for Leases’ pada DHCP server.
- Hapus static entri untuk laptop di ARP Table.
- Pastikan laptop tidak bisa akses internet.
- Renew IP address laptop
- Check kembali koneksi Internet, pastikan laptop bisa akses internet
- Perhatikan ARP Table.

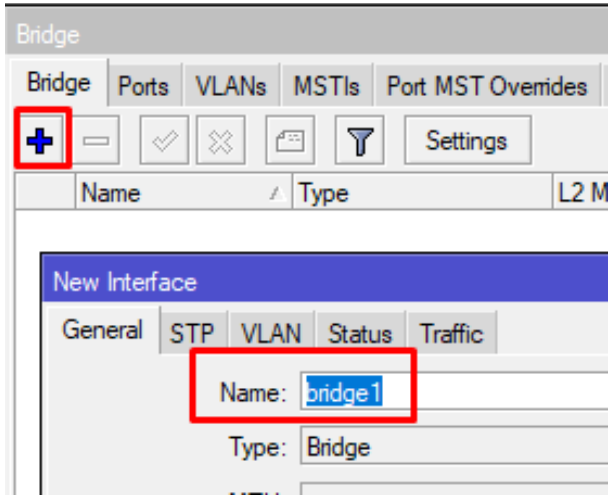
MODUL 3
BRIDGE

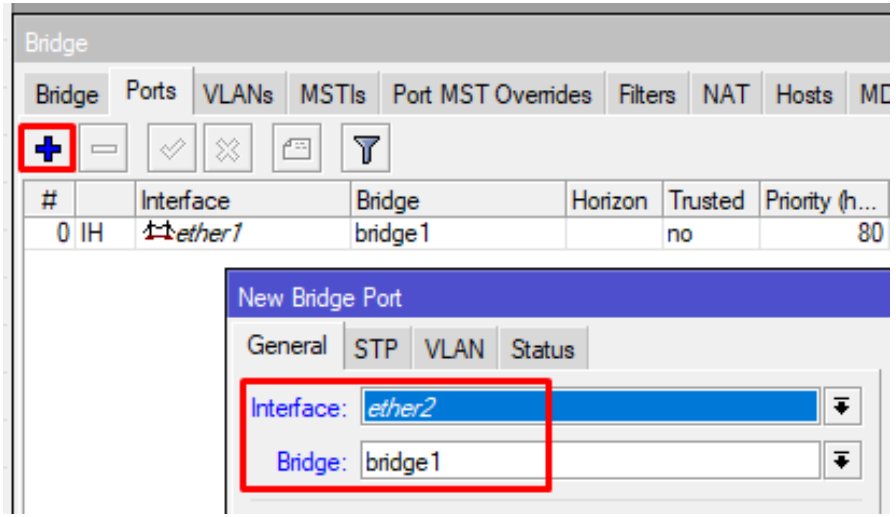
BRIDGING

- Bridge adalah mengabungkan beberapa interface menjadi satu interface virtual (satu jaringan).
- Bridge bekerja pada Layer 2
- Bridge memisahkan collision domain menjadi 2 bagian.
- Semua type interface (Ethernet, Wireless, SFP, tunnel) bisa di bridge.
- By default untuk Router SOHO sudah tersetting bridge (ether2-ether5).
- Ether2-5 tergabung dalam satu switch chip, ether2 master, ether3-5 slave.

BRIDGING

- Tahap pembuatan bridge adalah membuat interface bridge baru dan menambahkan interface fisik kedalam port bridge.



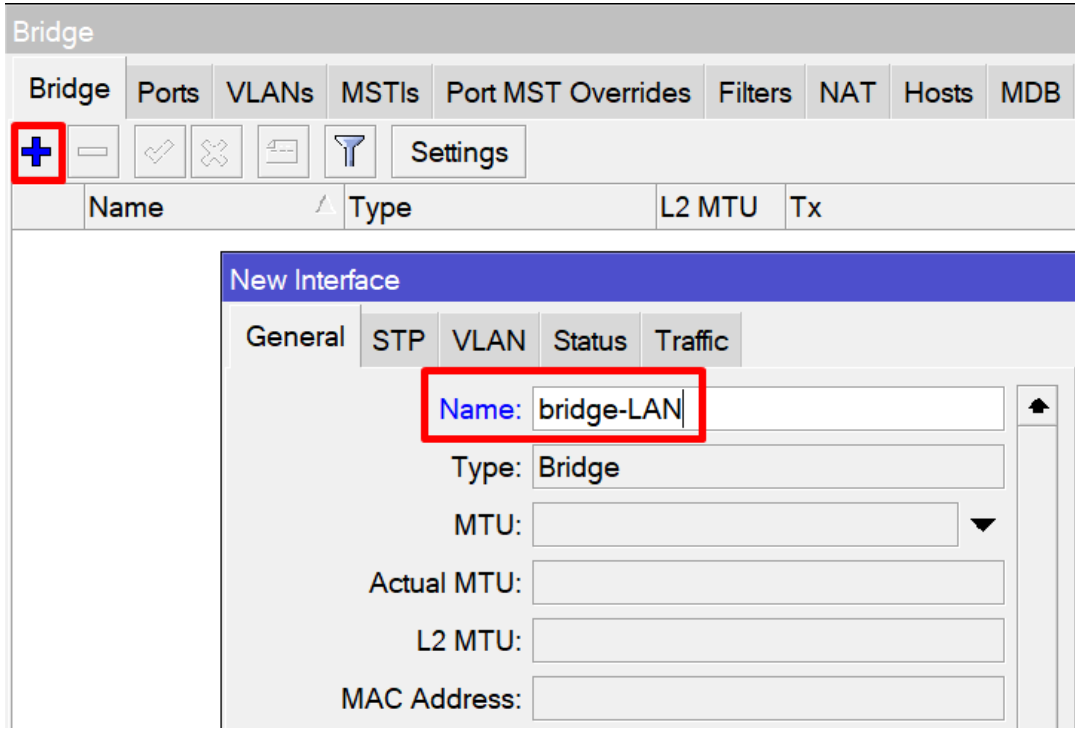


- Bila hanya membuat interface bridge tanpa menambahkan port, maka bridge tersebut disebut sebagai interface **loopback.**

BRIDGING (1)

LAB

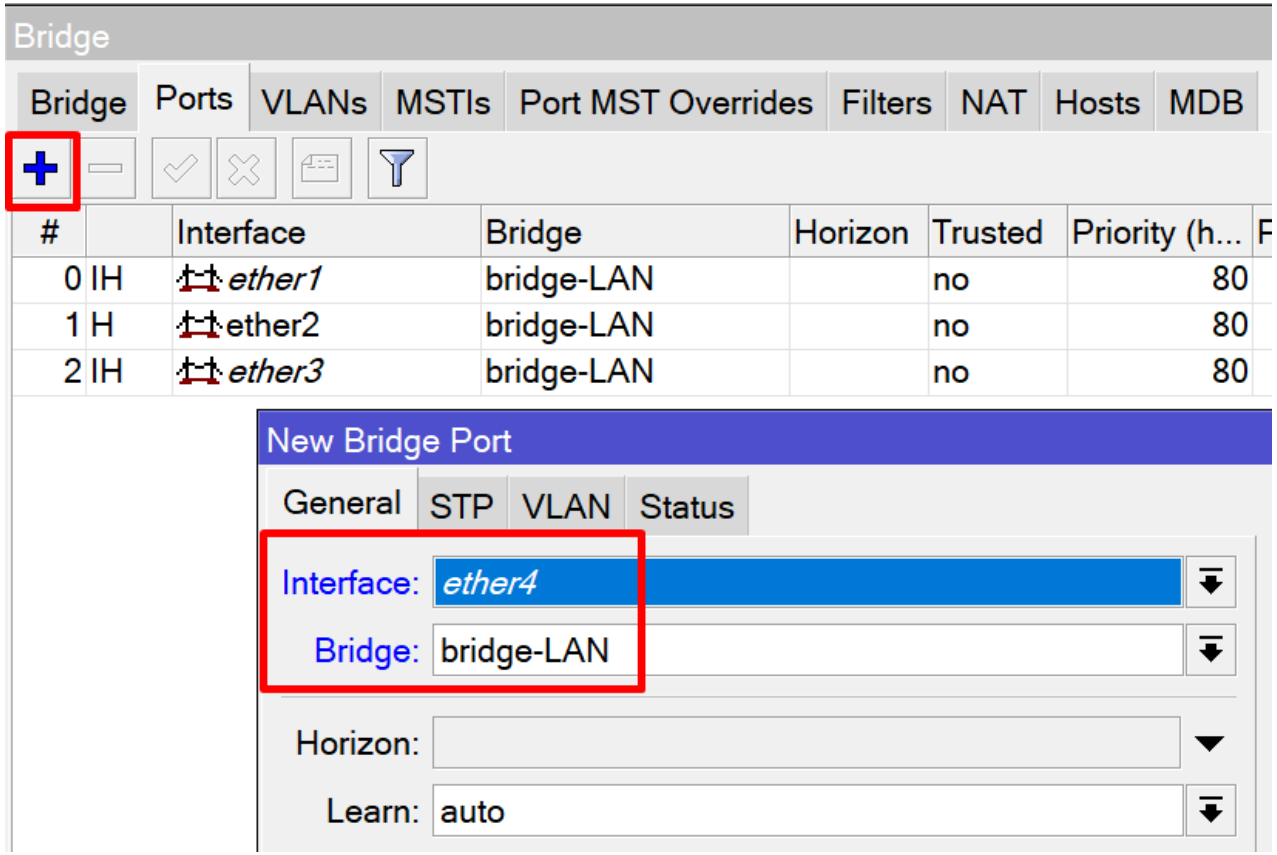
- Bridge semua interface supaya berada pada satu jaringan yang sama.
- Buat Interface bridge (Bridge-LAN)
  - **Bridge > add**



BRIDGING (2)

LAB

- Buat bridge port untuk membridge semua interface
  - **Bridge > Port > add**

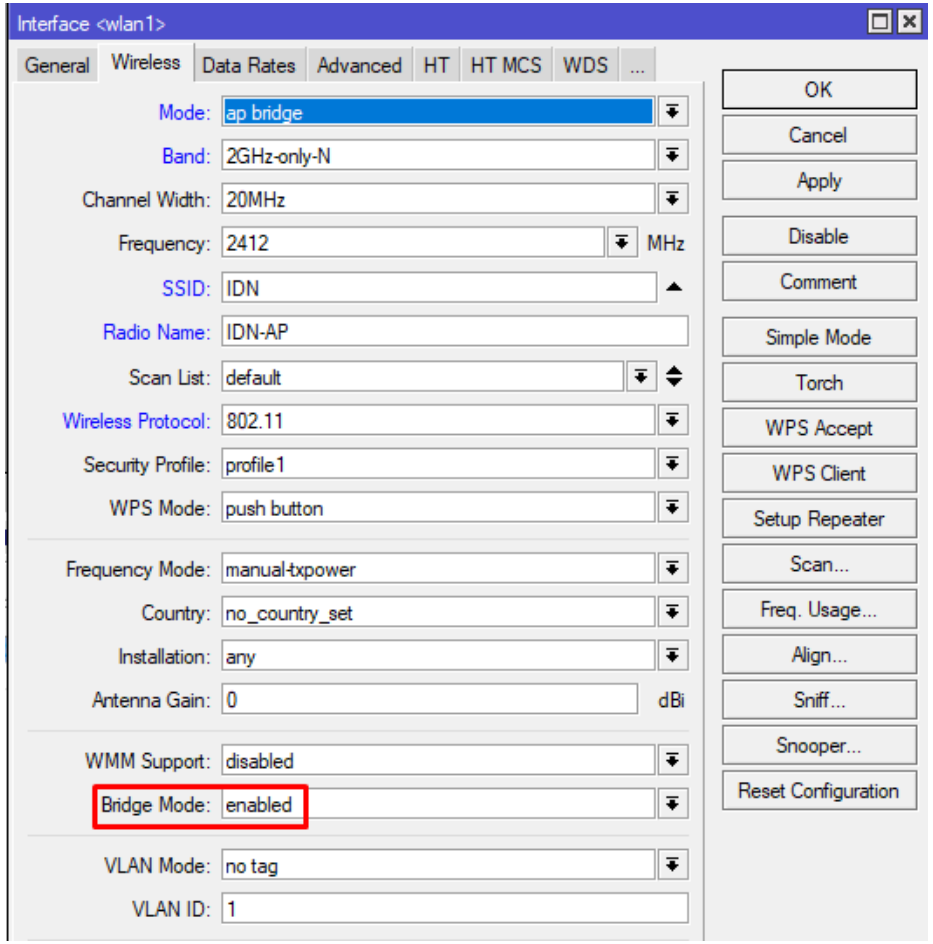


WIRELESS BRIDGING

- Karena ada batasan dari standar wireless 802.11, wireless client (mode: station) tidak bisa dibridge.
- Mode station tidak bisa dibridged sehingga RouterOS membuat mode lain yang bisa dibridging.
- Mode tersebut diciptakan sejak ROS v5.
  - Station Bridge - RouterOS to RouterOS.
  - Station Pseudobridge - RouterOS to non-RouterOS.
  - Station WDS (Wireless Distribution System) - RouterOS to RouterOS.

WIRELESS BRIDGING

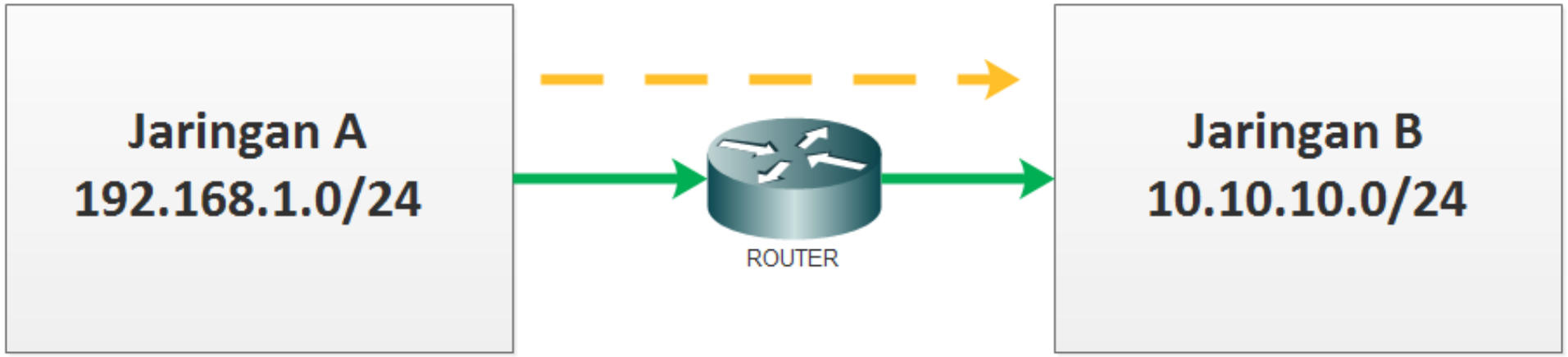
- Untuk menggunakan station bridge, bridge mode pada AP harus diaktifkan terlebih dahulu.



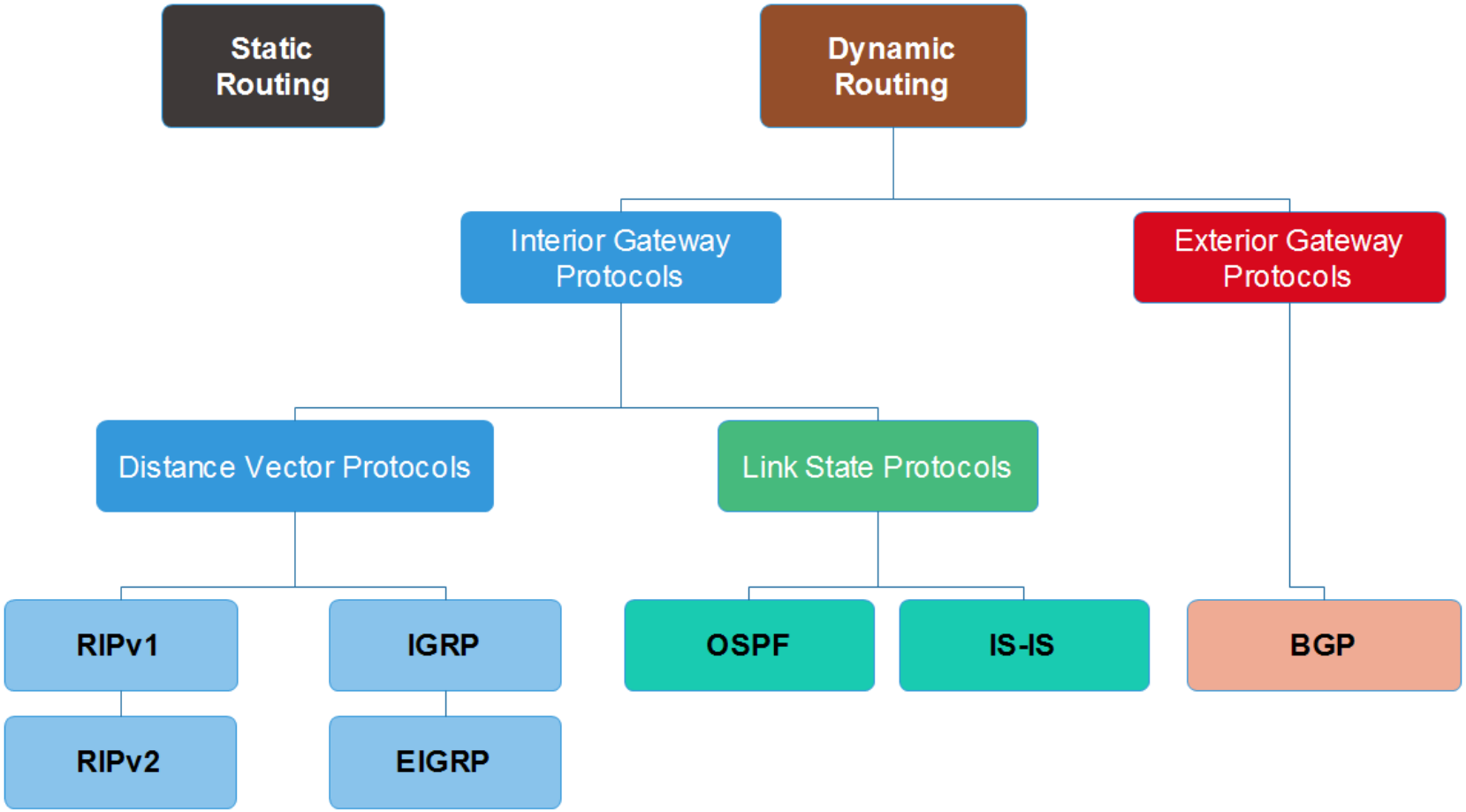
MODUL 4
ROUTING

ROUTING

- Proses melewatkan data dari satu jaringan ke jaringan lain melalui router.
- Routing bekerja pada OSI layer 3.



KLASIFIKASIROUTING



KLASIFIKASIROUTING

- **Static Routing**

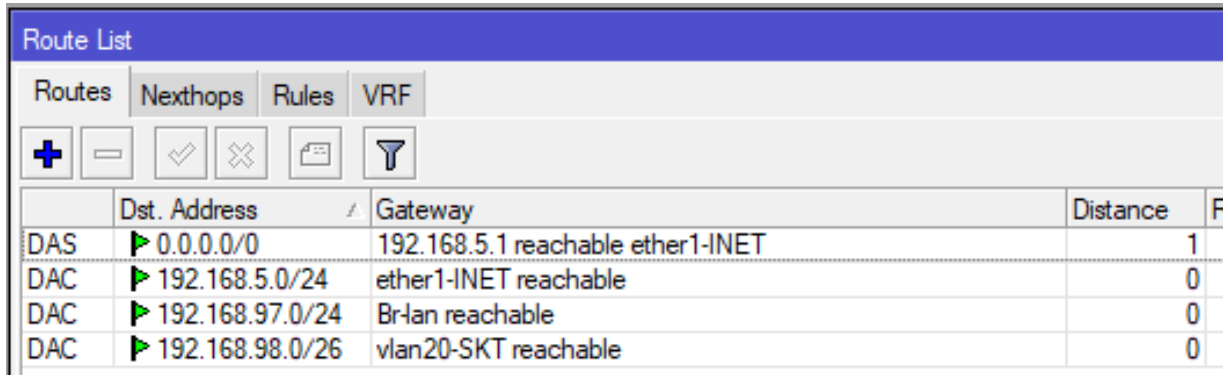
Routing yang dibuat dengan menambahkan secara manual kedalam routing table.

- **Dynamic Routing**

Routing yang dibuat dengan melakukan enable fungsi protocol pada router tersebut. Maka secara otimatis router akan mecari jalurnya sendiri.

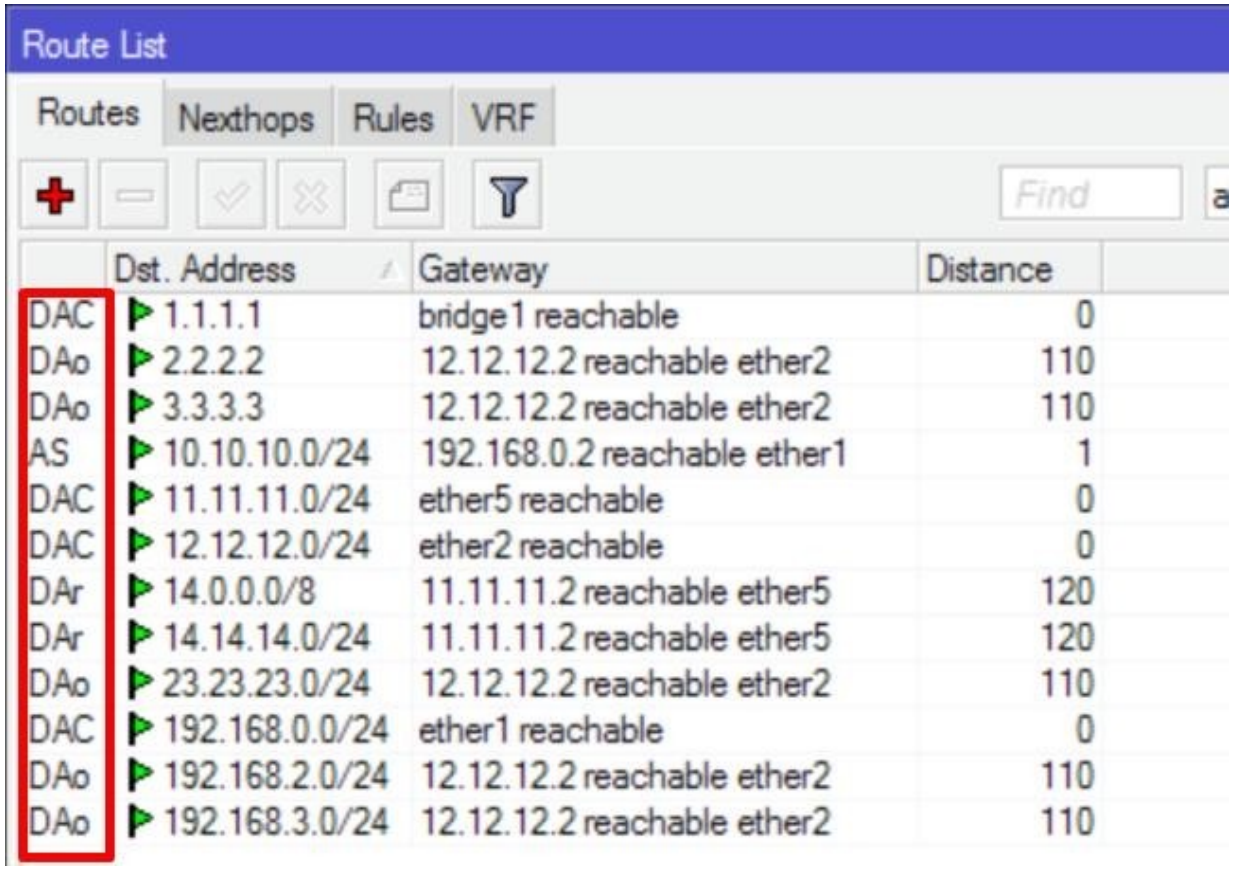
ROUTING TABLE

- Berisi informasi mengenai rute ke jaringan/network tertentu.
- Berisi nilai prioritas/metric dari masing-masing rute.



- Routing Table terbentuk dari:
  - Semua rute yang berasal dari dynamic routing protocol.
  - Semua rute untuk network yang directly connected ke router.
  - Konfigurasi tambahan (static route).

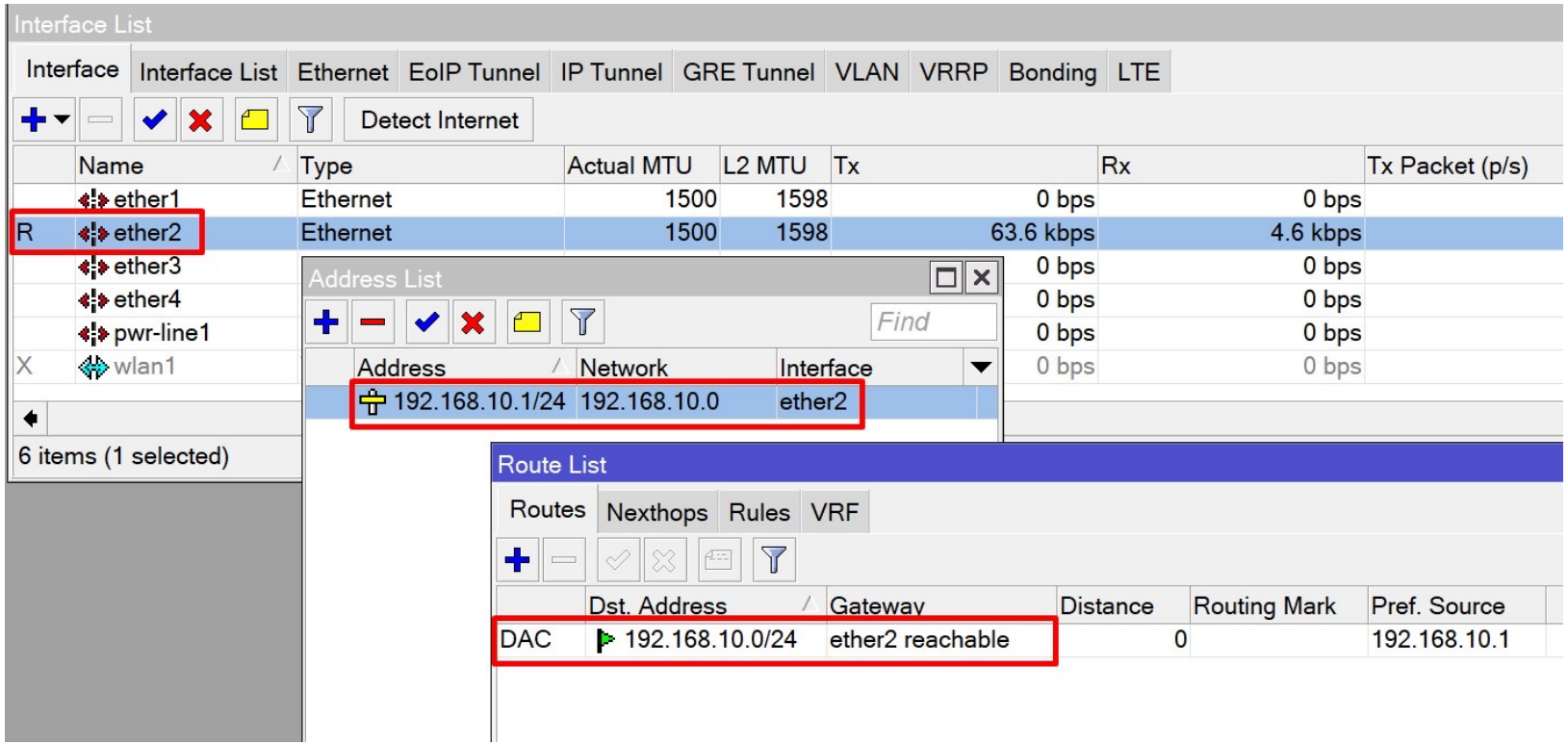
ROUTE FLAGS



- D = Dynamic
- A = Active
- C = Connected
- S = Static
- o = OSPF
- r = RIP
- b = BGP
- m = MME
- B = Blackhole
- P = Prohibit
- U = Unreachable
- X = Disable

CONNECTED ROUTE

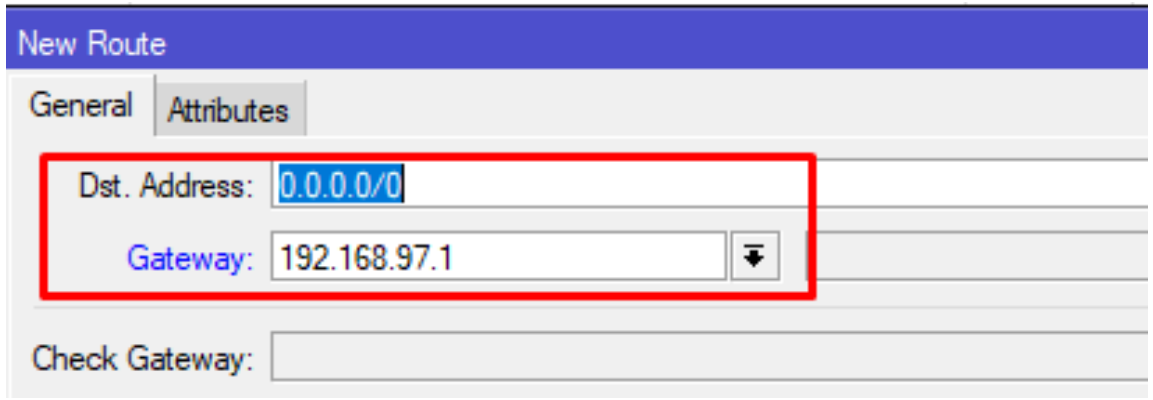
- Dibuat secara otomatis setiap menambahkan sebuah IP pada interface yang aktif



STATIC ROUTE

- Static routing dibuat dengan cara menambahkan jalur manual ke routing table.
- Pada static route yang perlu menambahkah parameter routing (Dst. Address dan Gateway) secara manual kedalam routing table.

IP > Routes > add



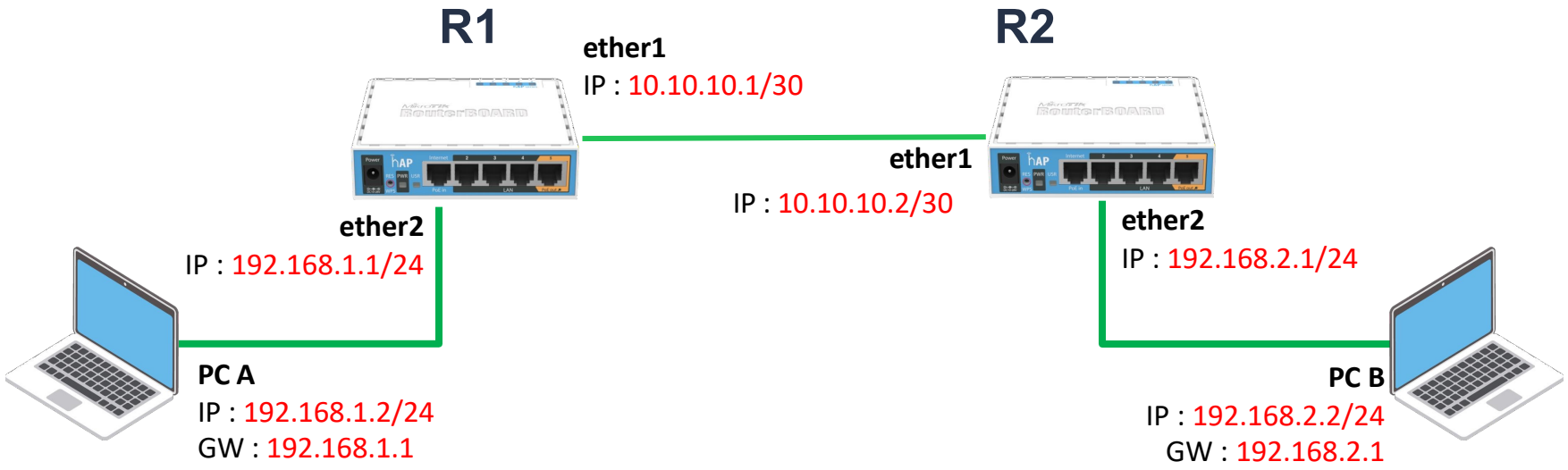
STATIC ROUTE

- Mudah dikonfigurasikan pada jaringan skala kecil.
- Membutuhkan resource yang ringan.
- Tidak cocok digunakan untuk jaringan skala besar.
- Manual konfigurasi setiap penambahan jaringan baru.

STATIC ROUTE

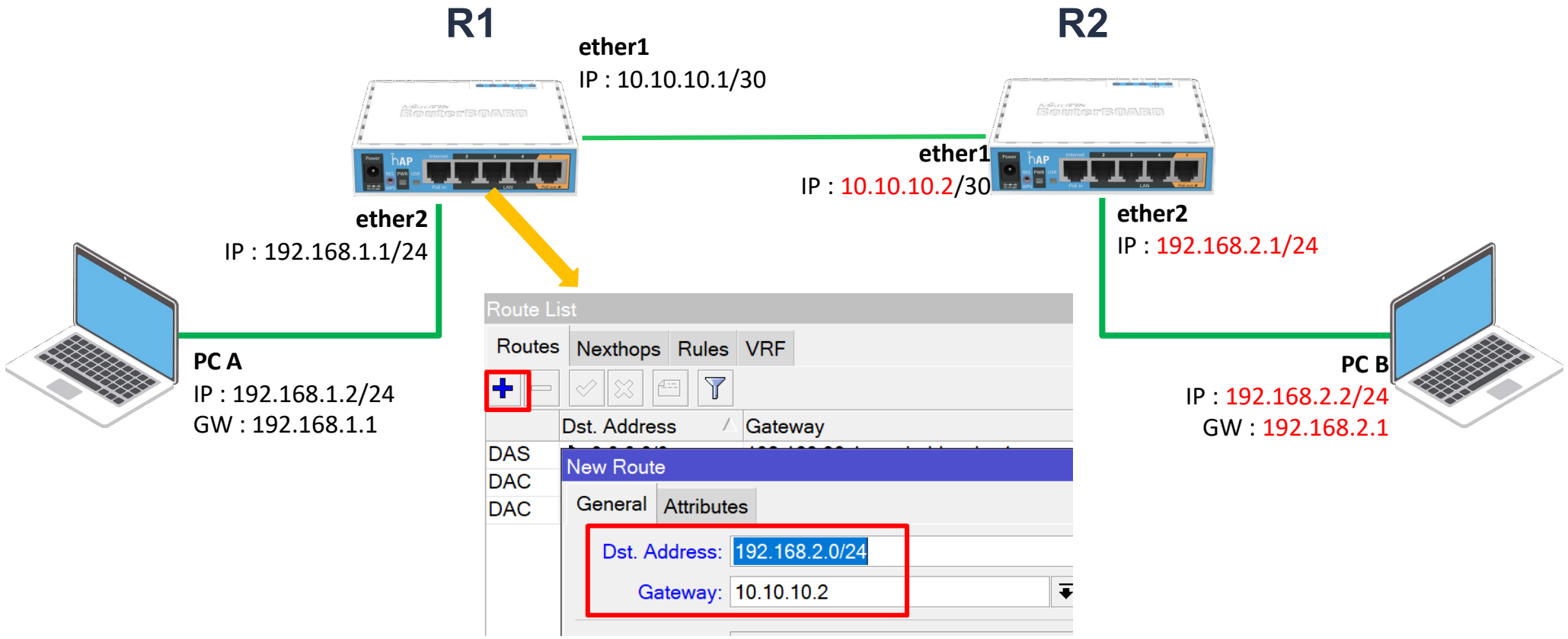
LAB

- Buat topologi seperti dibawah ini.
- Setting IP address dan pastikan link peer to peernya reachable dengan cara di PING.
- Konfigurasikan static route agar PC A bisa berkomunikasi dengan PC B.



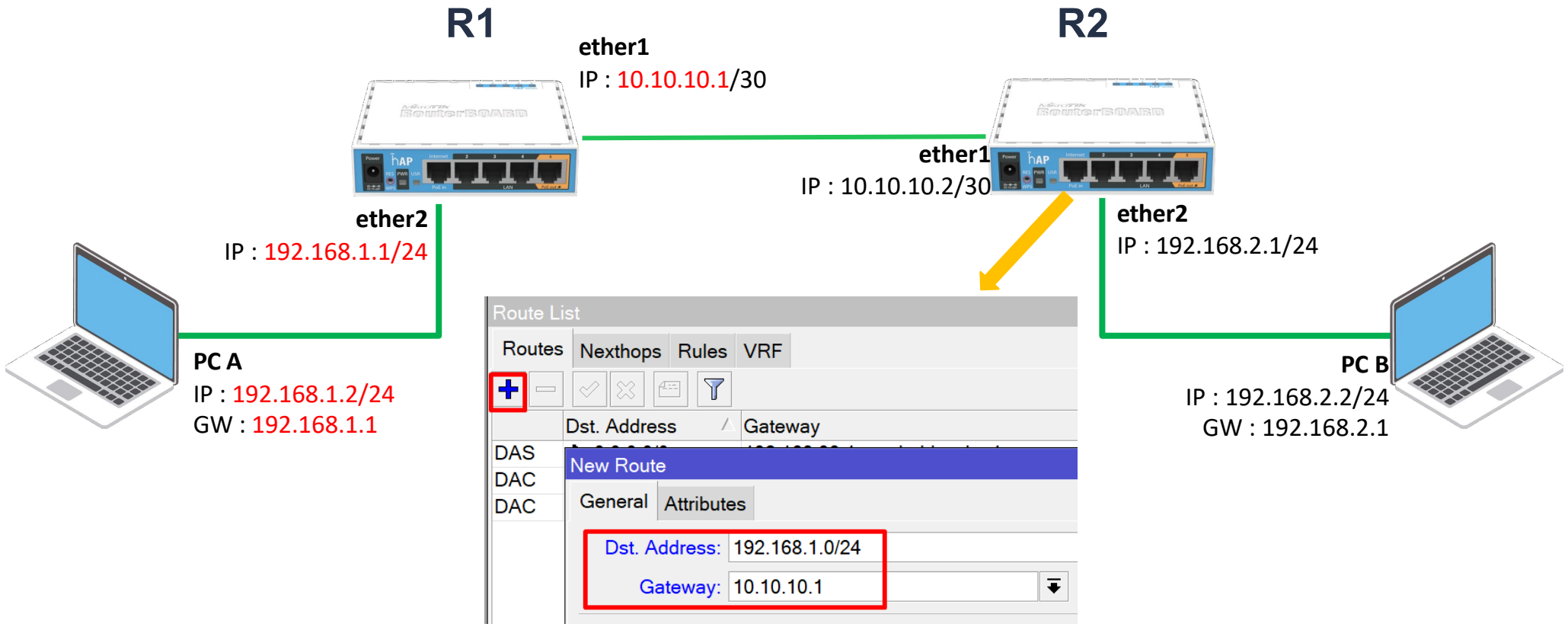
STATIC ROUTE – R1

LAB



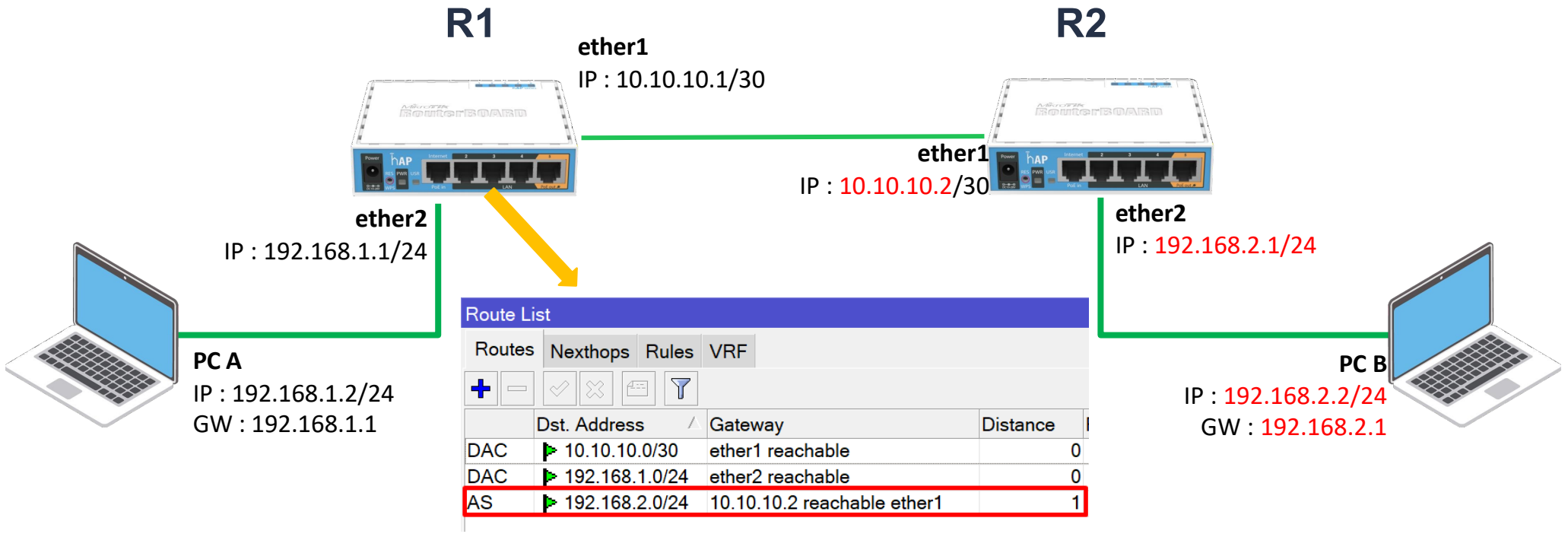
STATIC ROUTE – R2

LAB



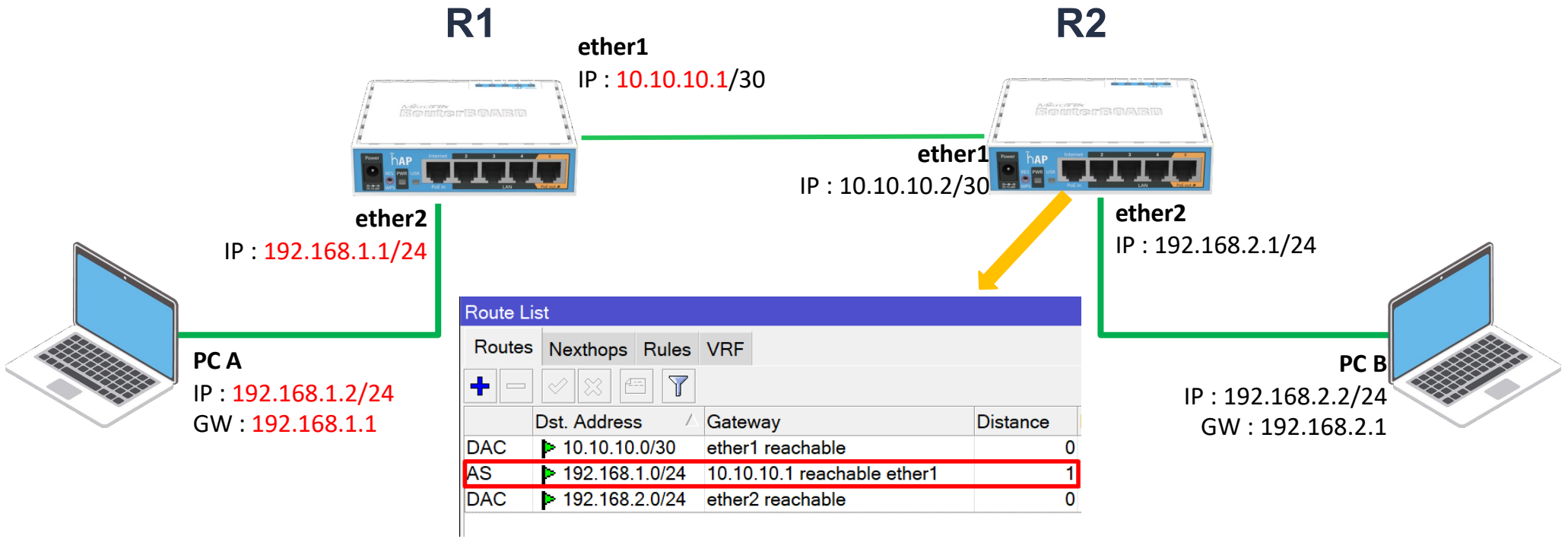
VERIFIKASI–R1

LAB



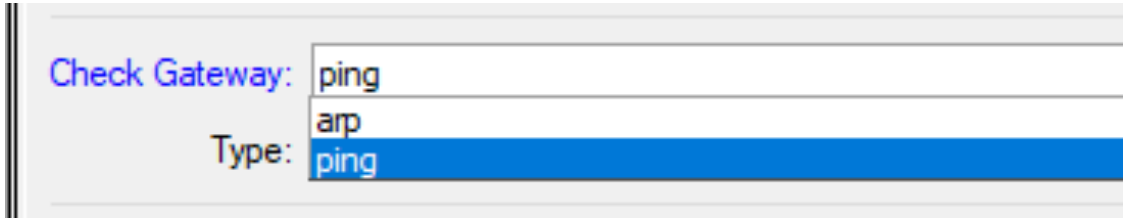
VERIFIKASI–R2

LAB



CHECK GATEWAY

- Check Gateway adalah pengecekan gateway oleh router melalui Layer 3 setiap interval 10 detik sekali.
- Request Time Out bila dalam 10 detik tidak menerima respon dari gateway.
- Unreachable bila 2x 10 detik tidak menerima respon dari gateway.
- Check gateway bisa berupa ICMP echo request (PING) dan ARP request.



- Semua route akan terkena efek check gateway bila menggunakan gateway yang sama, bila gateway tersebut diaktifkan check gateway.

ROUTING – BEST SELECTION ROUTE

- Untuk pemilihan route / jalur terbaik secara otomatis router akan melihat beberapa parameter sebagai berikut :
  - Network (pastikan dst-address dengan yang akan dituju sama)
  - Prefix (spesifik prefix)
  - Distance (semakin kecil distance, semakin prioritas)

ROUTING – BEST SELECTION ROUTE

- Network (pastikan dst-address dengan yang akan dituju sama)

Contoh :

Bila ada paket yang akan dikirimkan ke tujuan 192.168.97.190, terdapat 2 buah gateway sebagai berikut:

#1 dst-address=192.168.97.0/25	gateway=192.168.1.1
#2 dst-address=192.168.97.128/25	gateway=192.168.2.1

- Manakah gateway yang akan digunakan?
- Paket akan dikirimkan melalui 192.168.2.1, karena 192.168.97.190 masuk ke dalam range network 192.168.97.128

ROUTING – BEST SELECTION ROUTE

- Prefix (semakin spesifik, semakin di pilih)

Contoh :

Bila ada paket yang akan dikirimkan ke tujuan 192.168.88.10, terdapat 2 buah gateway sebagai berikut:

#1 dst-address=192.168.88.0/28	gateway=192.168.3.1
#2 dst-address=192.168.88.0/26	gateway=192.168.4.1

- Manakah gateway yang akan digunakan?
- Paket akan dikirimkan melalui 192.168.3.1, karena prefix yang digunakan lebih spesifik.
- /28 = 16 address sedangkan /26 = 64 address

ROUTING – BEST SELECTION ROUTE

- Distance (semakin kecil, semakin prioritas)

Contoh :

Bila ada paket yang akan dikirimkan ke tujuan 192.168.100.20, terdapat 2 buah gateway sebagai berikut:

#1 dst-address=192.168.100.0/27 distance=1 gateway=192.168.5.1

#2 dst-address=192.168.100.0/27 distance=2 gateway=192.168.6.1

- Manakah gateway yang akan digunakan?
- Paket akan dikirimkan melalui 192.168.5.1, karena distance terkecil.

ROUTING – BEST SELECTION ROUTE

- Contoh :

Bila ada paket yang akan dikirimkan ke tujuan 192.168.200.3, terdapat 2 buah gateway sebagai berikut:

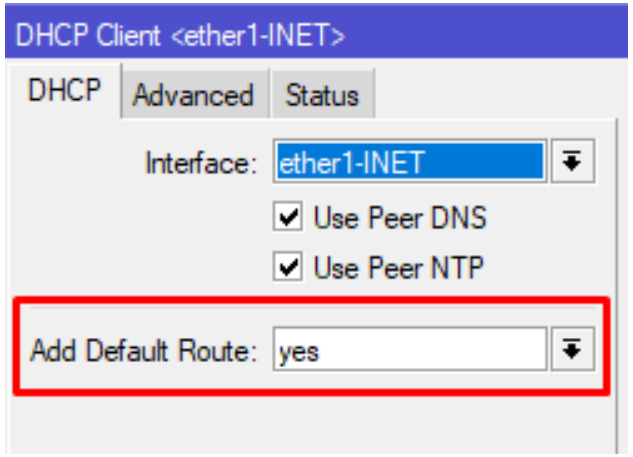
#1 dst-address=192.168.200.0/29 distance=5 gateway=192.168.7.1

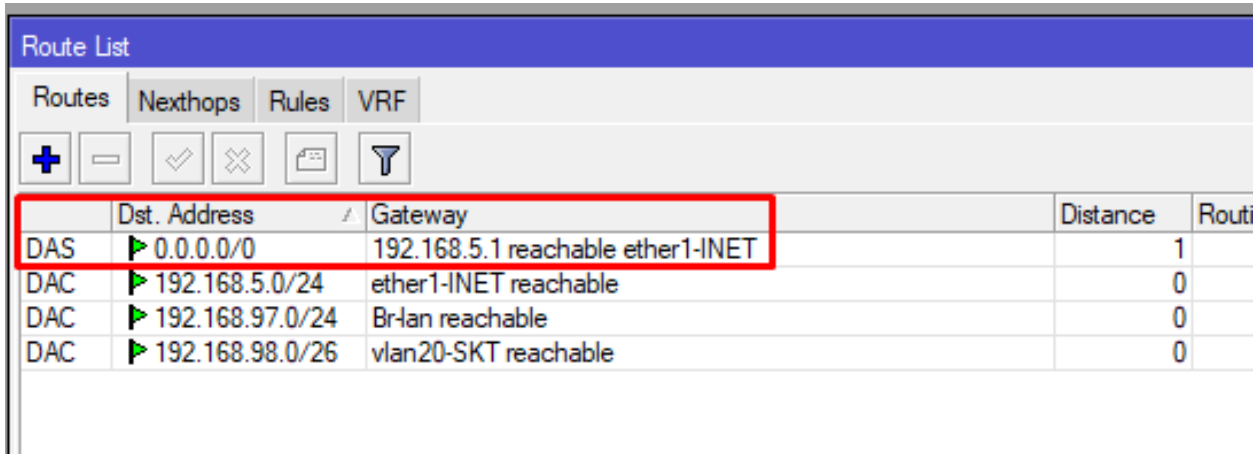
#2 dst-address=192.168.200.0/28 distance=3 gateway=192.168.8.1

- Manakah gateway yang akan digunakan?

DEFAULT GATEWAY

- Default Gateway : rute yang mewakili semua address ketika akan dikirimkan.
- Menggunakan alamat 0.0.0.0/0.
- 0.0.0.0/0 mewakili semua alamat di IP Address.
- By default ketika request DHCP Client secara otomatis defaut gateway akan
- dikonfigurasikan dan ditambahkan ke dalam routing table (DAS)





DEFAULT GATEWAY

LAB

- Disable ‘Add Default Route’ di DHCP Client setting.
- Pastikan router tidak bisa mengakses internet.
- Tambahkan default gateway secara manual.
- Check koneksi internet kembali.

MODUL 5
WIRELESS

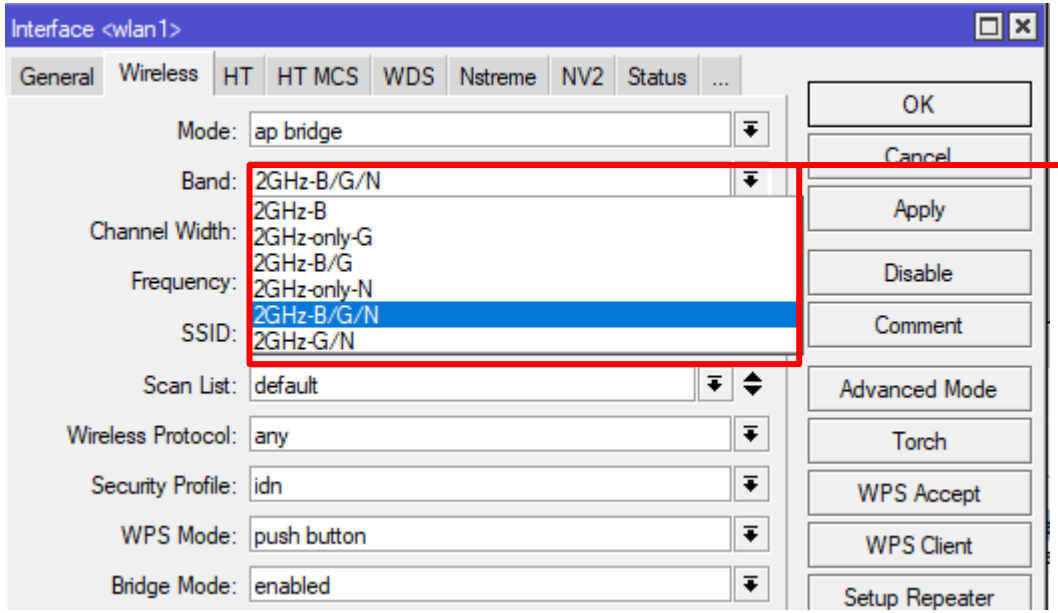
WIRELESS PADA MIKROTIK

- Wireless memiliki standard & spesifikasi IEEE 802.11 dan menggunakan frekuensi 2,4 GHZ dan 5,8 GHz
- RouterOS mendukung protocol standard & spesifikasi IEEE 802.11 a/n/ac (5Ghz) dan 802.11 b/g/n (2,4 Ghz).

IEEE Standard	Frequency	Speed
802.11a	5 GHz	54Mbps
802.11b	2,4 GHz	11Mbps
802.11g	2,4 GHz	54Mbps
802.11n	2,4 GHz dan 5Ghz	Up to 450 Mbps*
802.11ac	5 GHz	Up to 1300 Mbps *

WIRELESS BAND

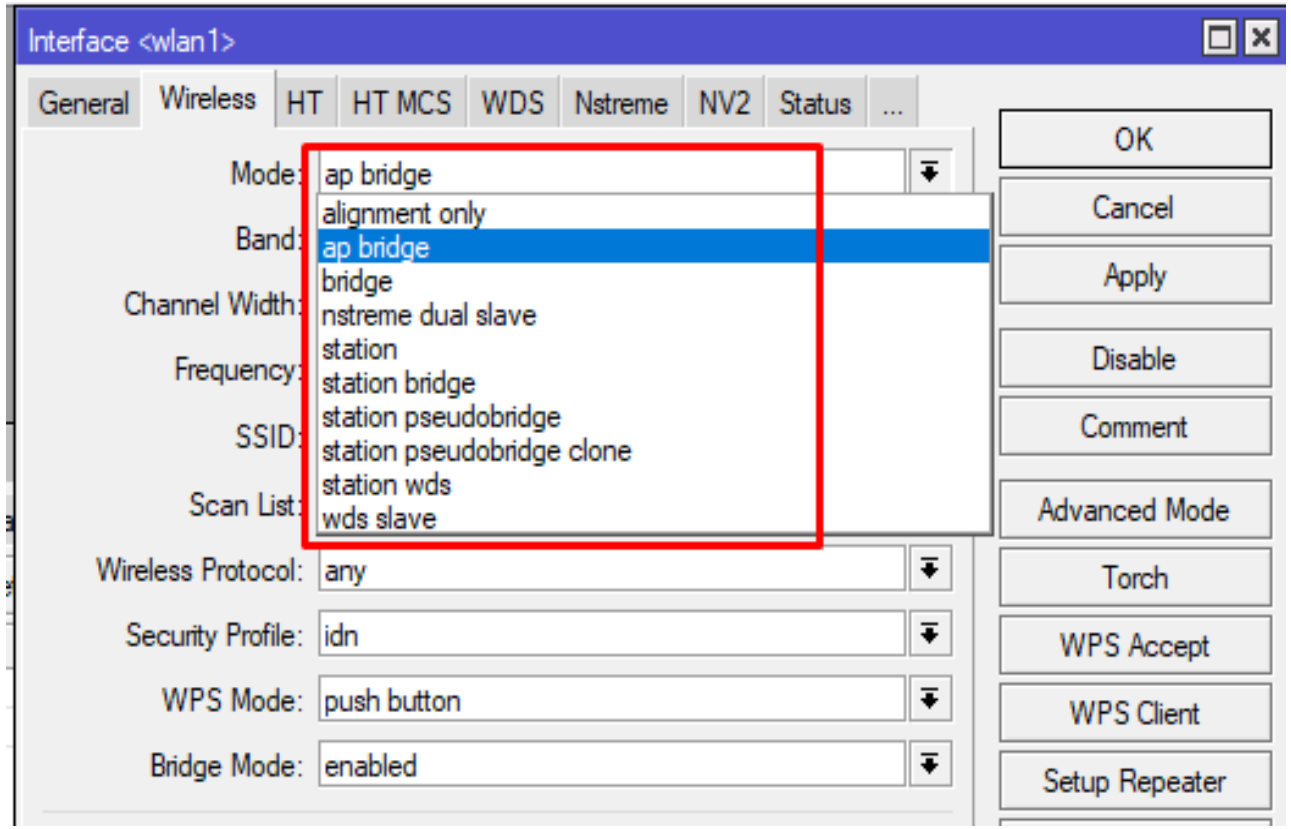
- Band merupakan standard protocol yang akan digunakan oleh jaringan wireless yang akan kita buat.
- Untuk menghubungkan 2 perangkat, keduanya harus bekerja pada protocol dan band yang sama.



Band yang ada pada list, tergantung pada jenis wireless card yang digunakan.

WIRELESS MODE

- Wireless Mode menentukan fungsi suatu wireless tersebut.



WIRELESS MODE

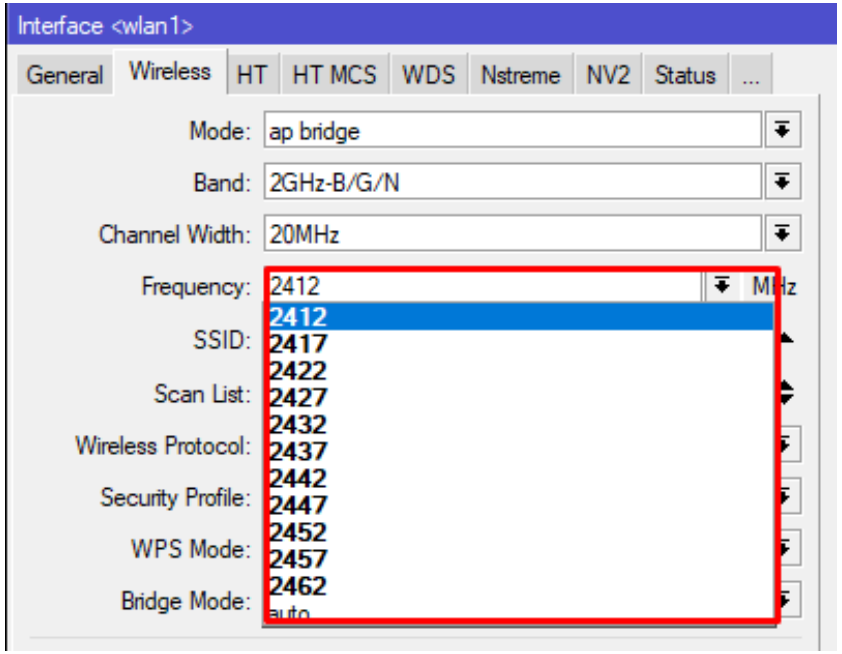
- **AP Mode**
  - **AP Bridge** merupakan mode pemancar yang bisa melayani banyak client (PTMP).
  - **Bridge** merupakan mode pemancar yang hanya bisa melayani satu client (PTP).
- **Station Mode**
  - **Station** merupakan mode penerima yang bersifat routing.
  - **Station Bridge** merupakan mode penerima yang support bridge.
  - **Station Psudobridge** merupakan mode penerima yang digunakan untuk menghubungkan mikrotik dengan non mikrotik secara bridging.
  - **Station Psudobridge Clone** merupakan mode yang sama dengan station Psudobridge yang harus melakukan cloning MAC address ketika akan konek.
  - **Station WDS** berfungsi sebagai penerima untuk AP yang mengaktifkan fitur WDS.

WIRELESS MODE

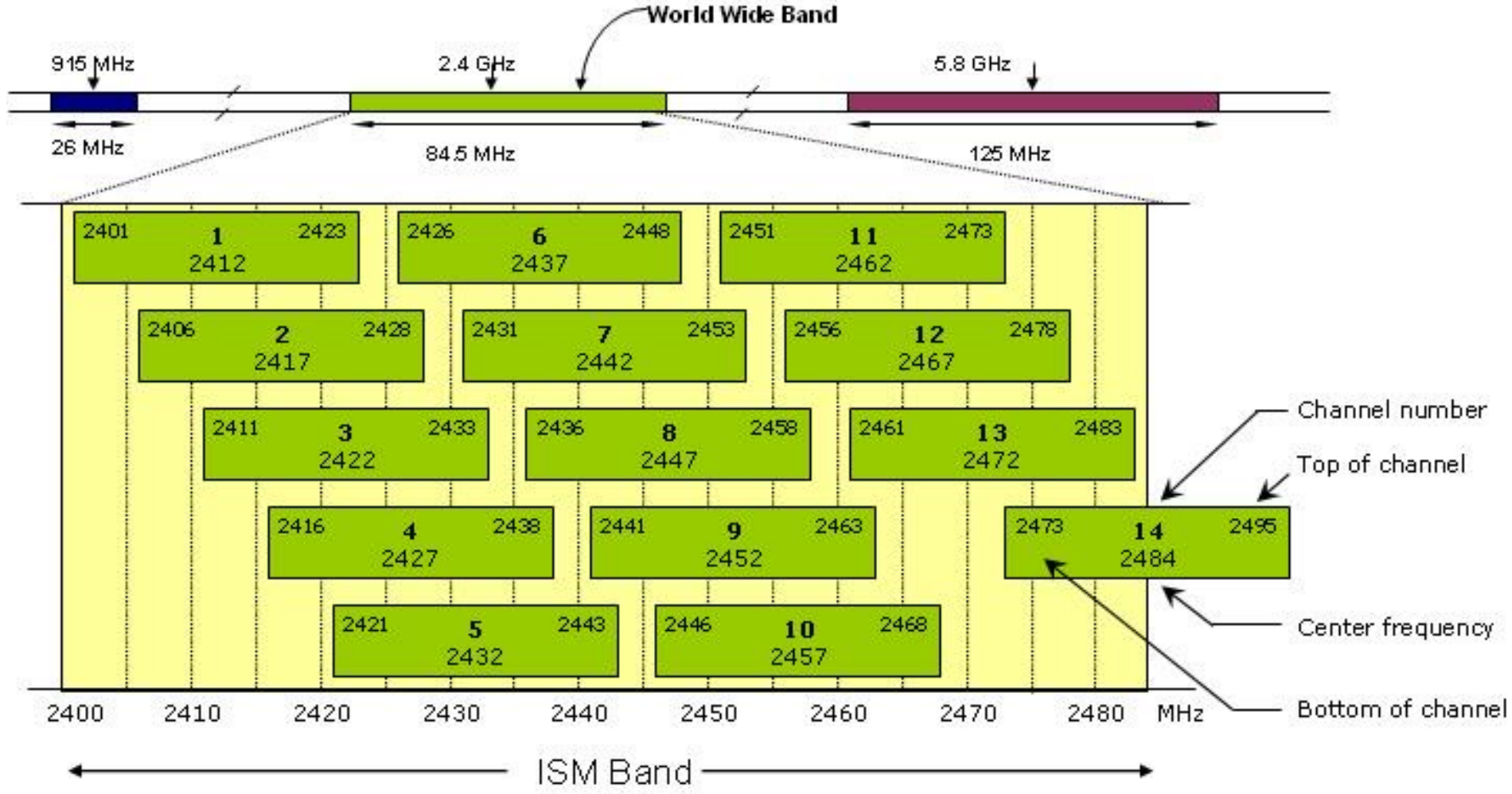
- **Special Mode**
  - **Alignment Only** merupakan mode yang biasanya digunakan untuk pointing. Hasil outputnya dapat berupa suara beep. Semakin kencang suara semakin bagus sinyal yang di dapat.
  - **Nstreme-Dual-Slave** mode untuk membuat jaringan wireless jadi full duplex. Karena pada dasarnya jaringan wireless itu adalah half duplex. Untuk membuat mode ini diperlukan 2 wireless card dan 2 antenna pada kedua radio.
  - **WDS-Slave** merupakan mode untuk membuat repeater.

FREQUENCY

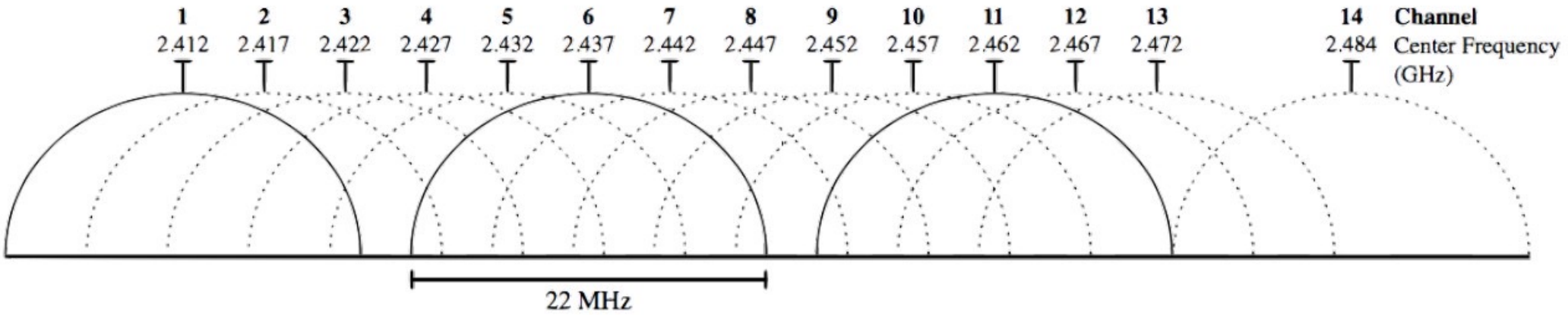
- Merupakan pembagian dari frekuensi dalam suatu band dimana jaringan wireless beroperasi.
- Pentingnya pemilihan frekuensi adalah untuk mencegah terjadinya interferensi.



WIRELESS – 2,4GHZ CHANNELS



WIRELESS – 2,4GHZ CHANNELS



- Setiap negara mempunyai regulasi channel yang berbeda-beda, contohnya US punya 11 channels. Sedangkan Jepang punya 14 channels.
- Channel width :
  - 802.11b 22Mhz, 802.11g 20MHz, 802.11n 20/40Mhz

WIRELESS – 5GHZ CHANNELS

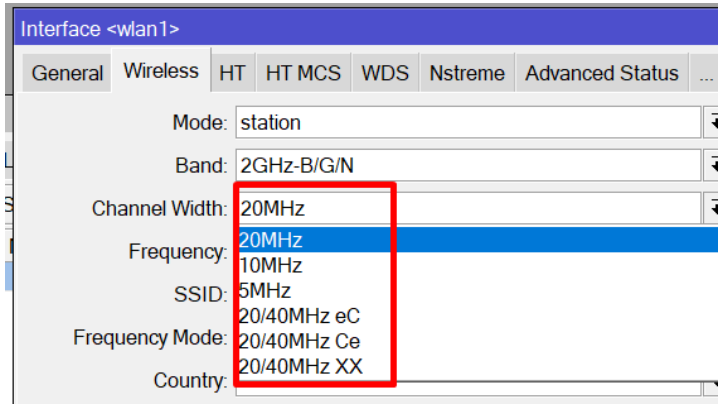
- RouterOS juga telah mendukung frekuensi 5Ghz.
- 5180-5320 Mhz (channel 36-64)
- 5500-5720 Mhz (channel 100-144)
- 5747-5825 Mhz (channel 149-165)
- Tergantung juga pada regulasi di setiap negara.

WIRELESS – 5GHZ CHANNELS

IEEE Standard	Channel Width
802.11a	20MHz
802.11n	20MHz
	40MHz
802.11ac	20MHz
	40MHz
	80MHz
	160MHz

CHANNEL WIDTH

- Channel Width (lebar channel) merupakan lebar jalur yang digunakan untuk melewatkan data di Jaringan Wireless.
- Default Channel width 22MHz (ditulis 20MHz)
- Lebar channel dapat dikecilkan (5 MHz) untuk meminimalkan frequensi atau dibesarkan (40 MHz) untuk mendapatkan troughput yang lebih besar.
- Semaki besar CW semakin besar juga kemungkinan terjadi interferensi di jaringan wireless.

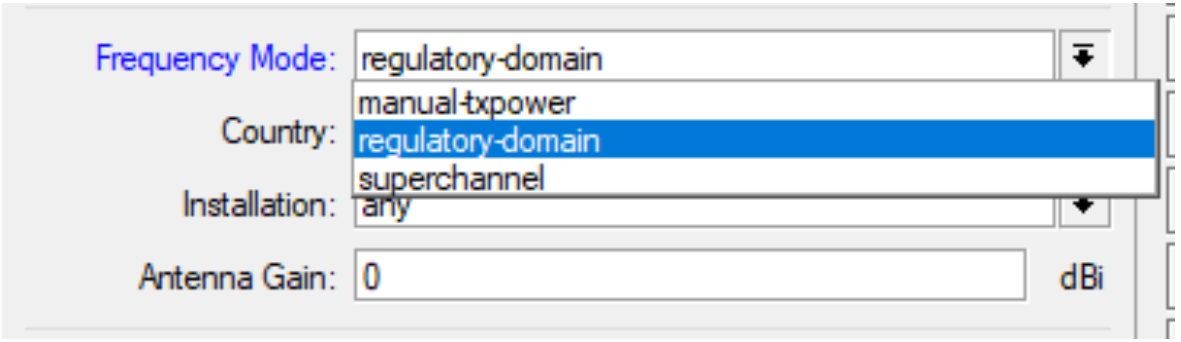


- 20/40MHz eC (HT-Bellow) 20MHz frequensi normal dan 20MHz di bawahnya.
- 20/40MHz Ce (HT-Above) 20MHz frequensi normal dan 20MHz di atasnya.
- 20/30MHz XX (Otomatis Scan channel)

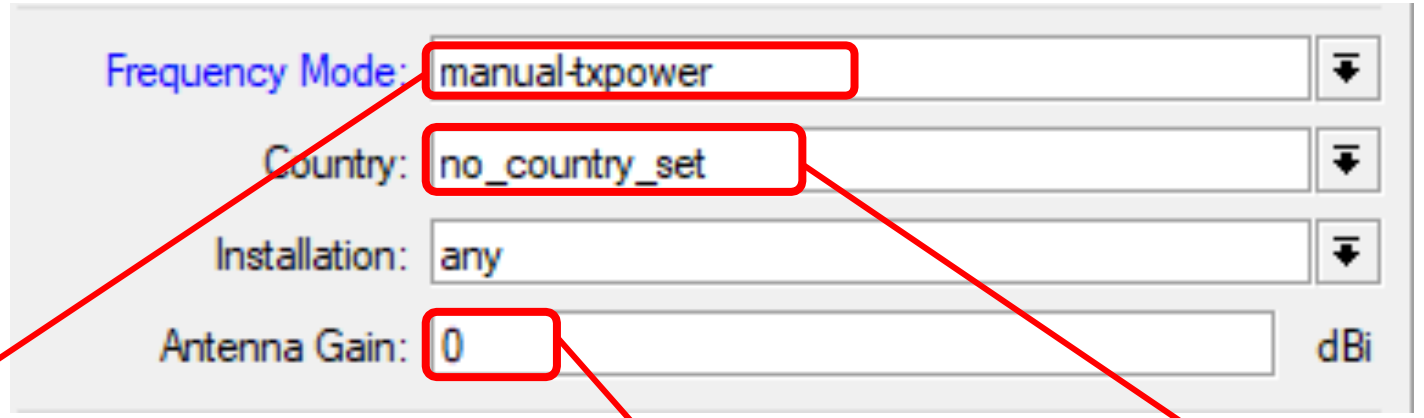
Ketiga channel width di atas bekerja di band N

COUNTRY REGULATIONS

- Regulatory-domain digunakan untuk menyesuaikan regulasi di suatu negara.
- Setiap negara memiliki regulasi tertentu dalam hal frekuensi wireless untuk internet carrier.
- Regulasi tersebut dalam mikrotik didefinisikan pada parameter wireless advanced frequency mode = regulatory-domain, kemudian tinggal di arahkan ke suatu negara.
- Namun apabila ingin membuka semua frekuensi yang dapat digunakan oleh wireless card, dapat menggunakan pilihan **superchannel**



COUNTRY REGULATIONS



Frequency Mode

1. Manual-txpower

frekuensi default mikrotik.

2. Regulatory-domain

frekuensi sesuai regulasi disuatu negara

3. Superchannel

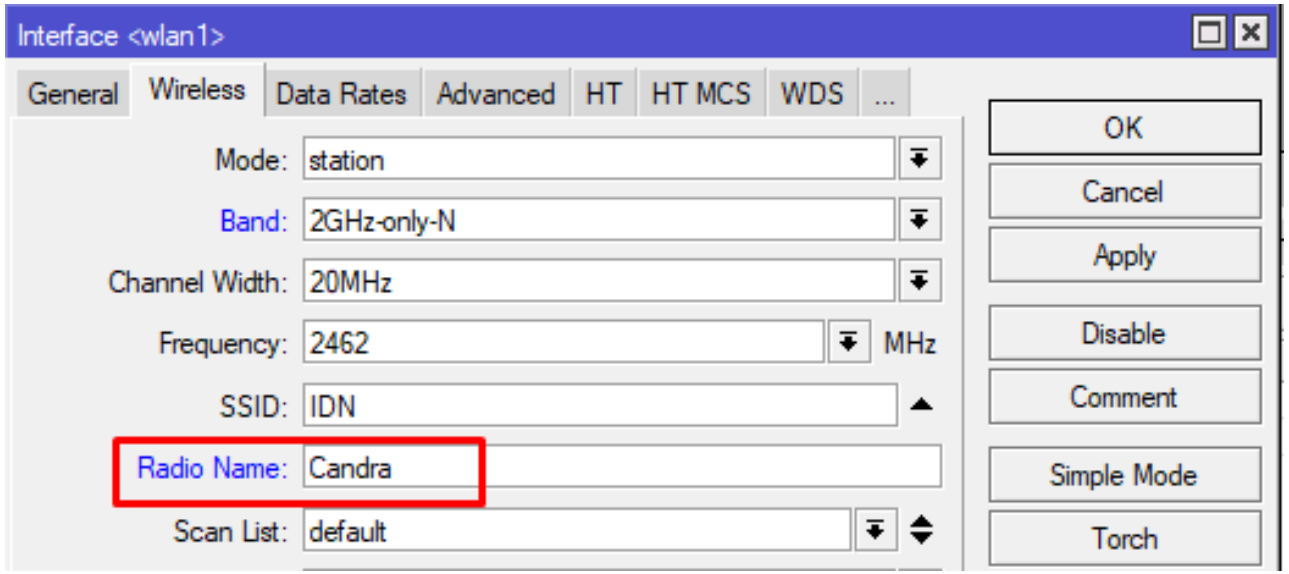
membuka semua frekuensi yang di support oleh wireless card

Pemilihan Country / Negara

Default 0, akan otomatis menyesuaikan agar tidak melebihi EIRP country regulation

RADIONAME

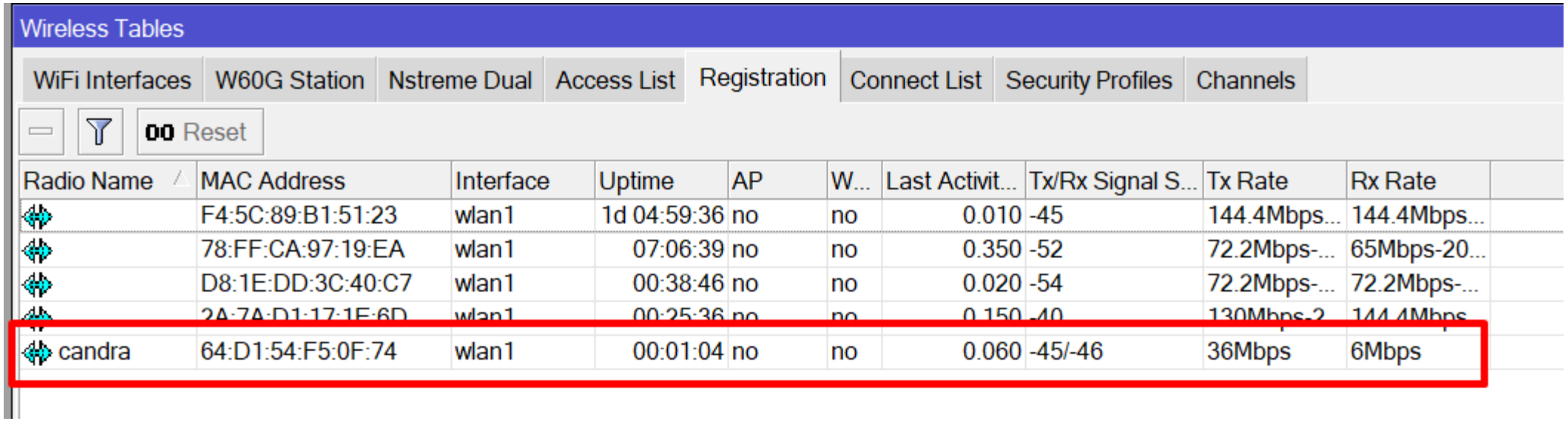
- Radio Name merupakan hostname dari radio itu sendiri.
- Hanya akan terlihat apabila sama-sama menggunakan RouterOS.
- Untuk mengetahui radio name lawan bias di cek di Registration table.



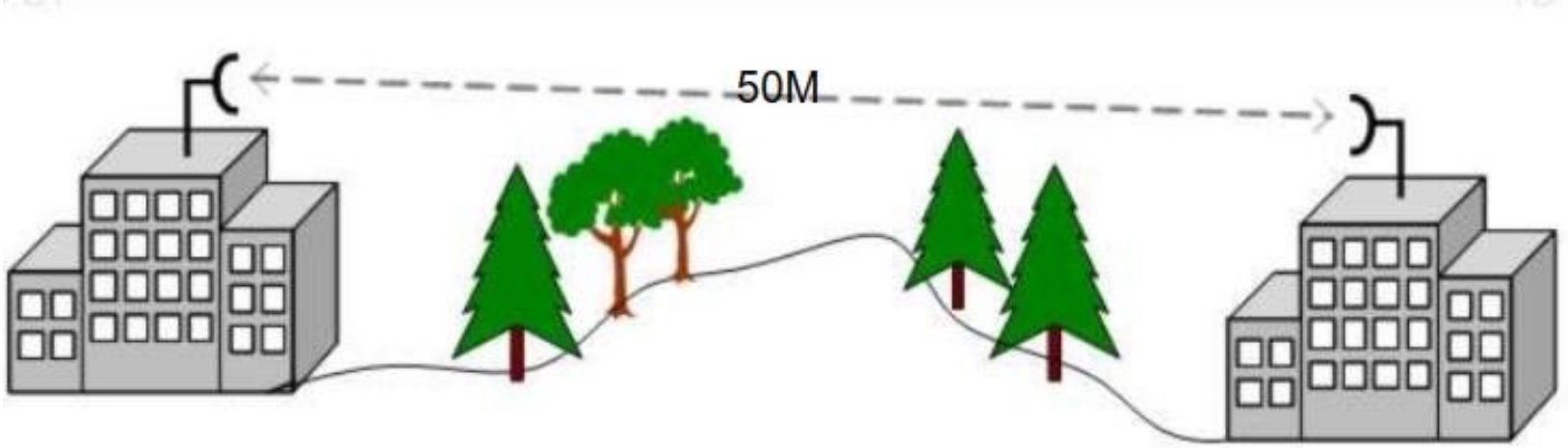
RADIONAME

LAB

- Wireless > Registration



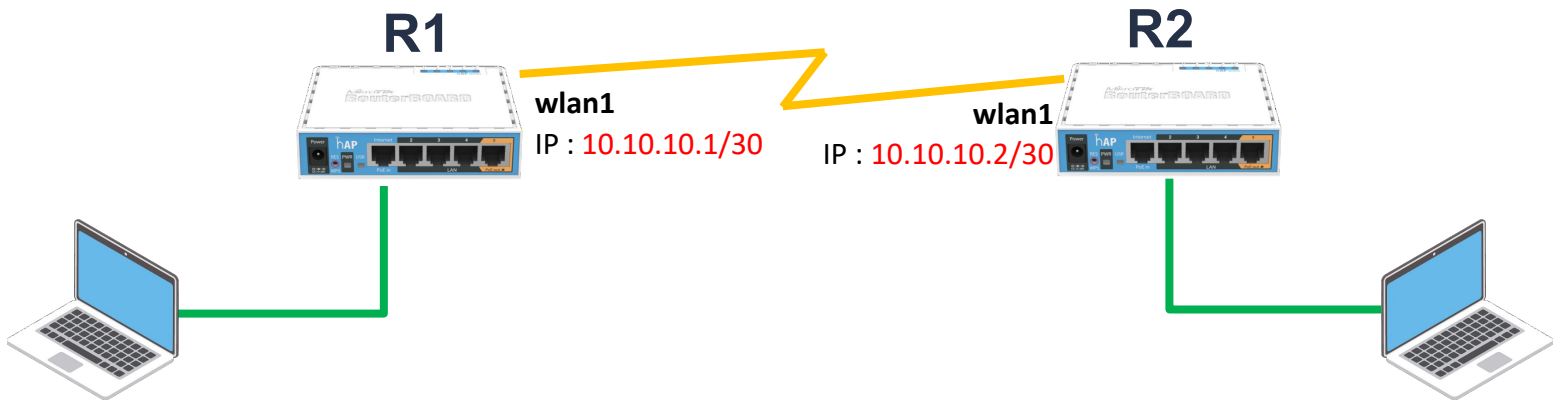
KONSEP KONEKSI WIRELESS



- Kesesuaian Mode : (AP-Station, AP-Repeater, Repeater-repeater)
- Kesesuaian BAND
- Kesesuaian SSID
- Kesesuaian enkripsi dan authentikasi
- Frekuensi channel tidak perlu sama, station secara otomatis akan mengikuti channel frekuensi pada AP.

KONEKSI WIRELESS

LAB

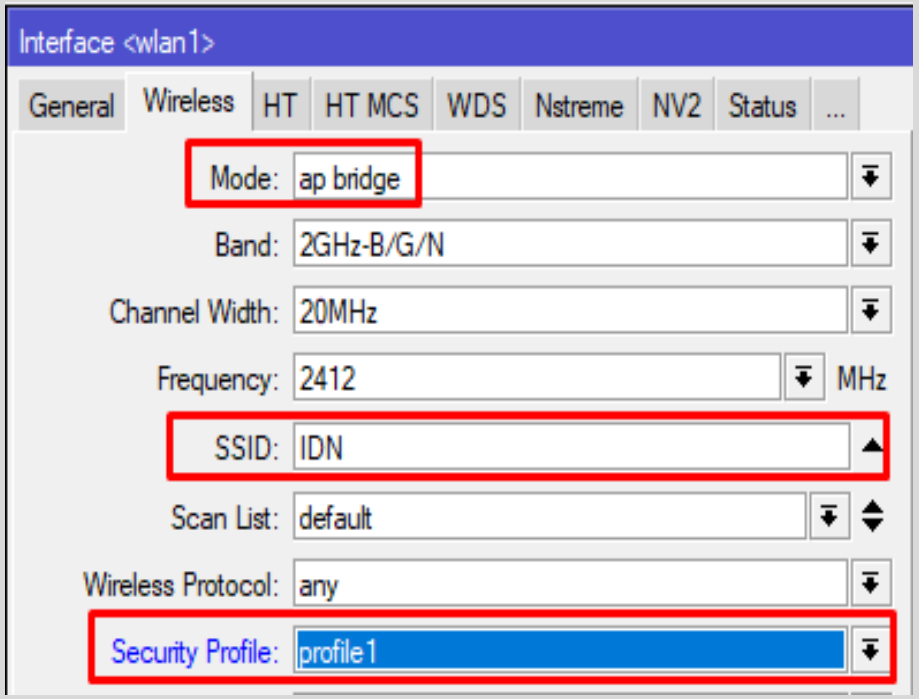


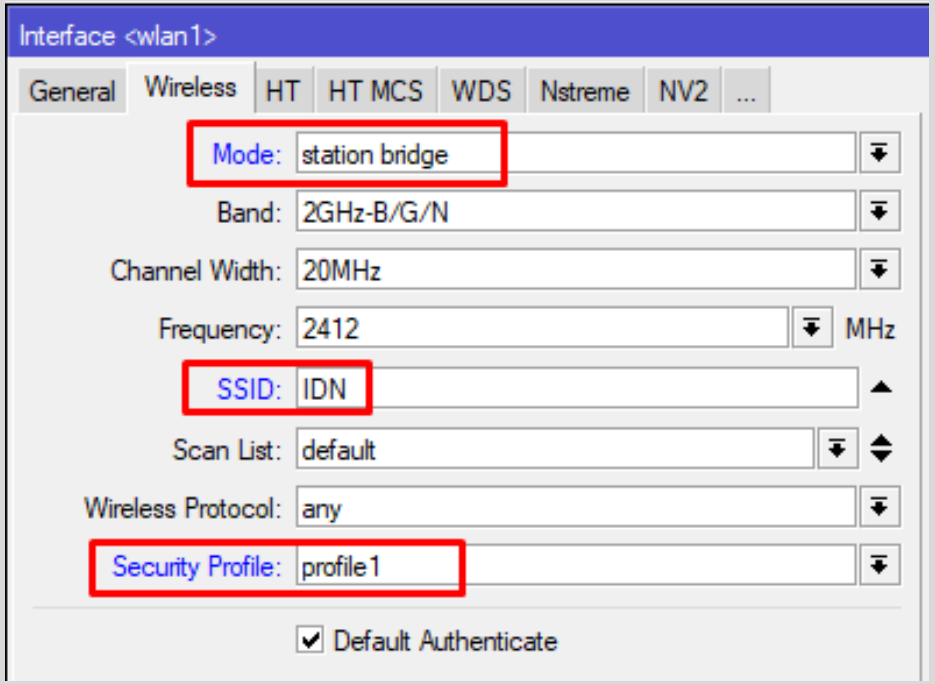
Konfigurasi	Peserta I	Peserta II
Mode	AP-Bridge/Bridge	Station/Station-Bridge
Band	Samakan	
SSID	Samakan (Unik untuk tiap pasangan)	
Frequensi	Pilih	Tidak harus sama
Security Profile	Samakan	
IP address wlan1	10.10.10.1/30	10.10.10.2/30

KONEKSI WIRELESS

LAB

Peserta 1 (Access Point)	Peserta 2 (Station)

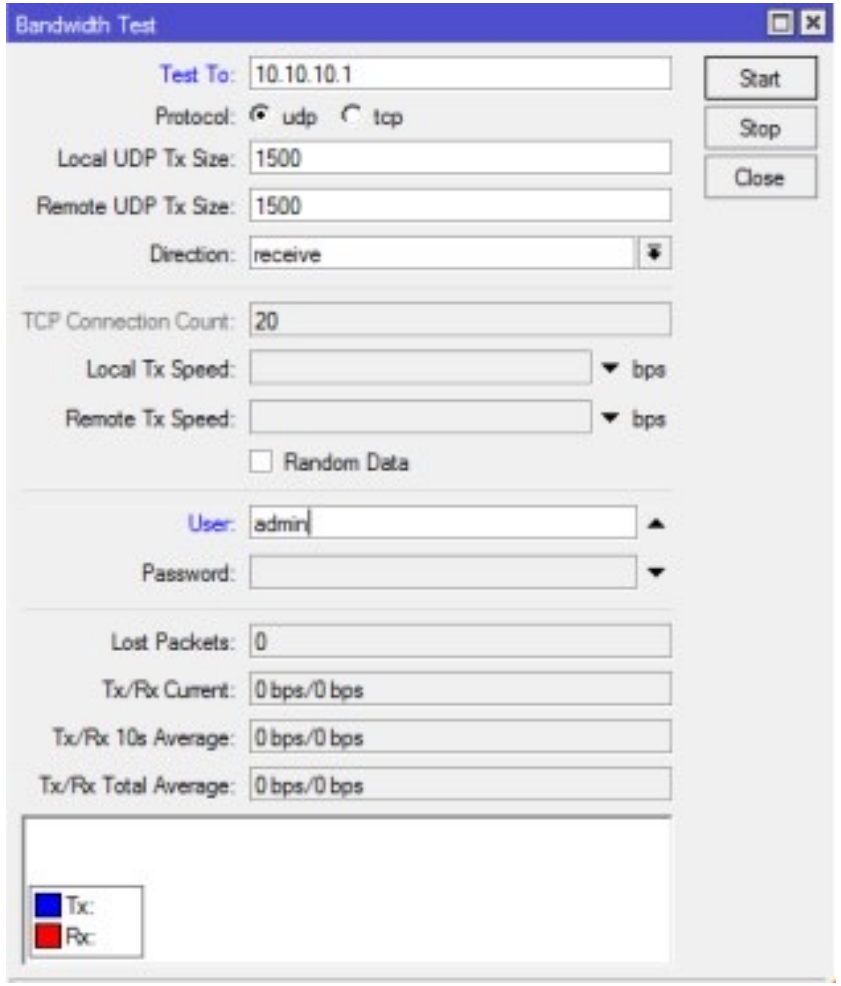




- Check pastikan muncul R (Running) di interface wlan1 / check di registration Setting IP address sesuai topologi, pastikan antar router bisa saling ping

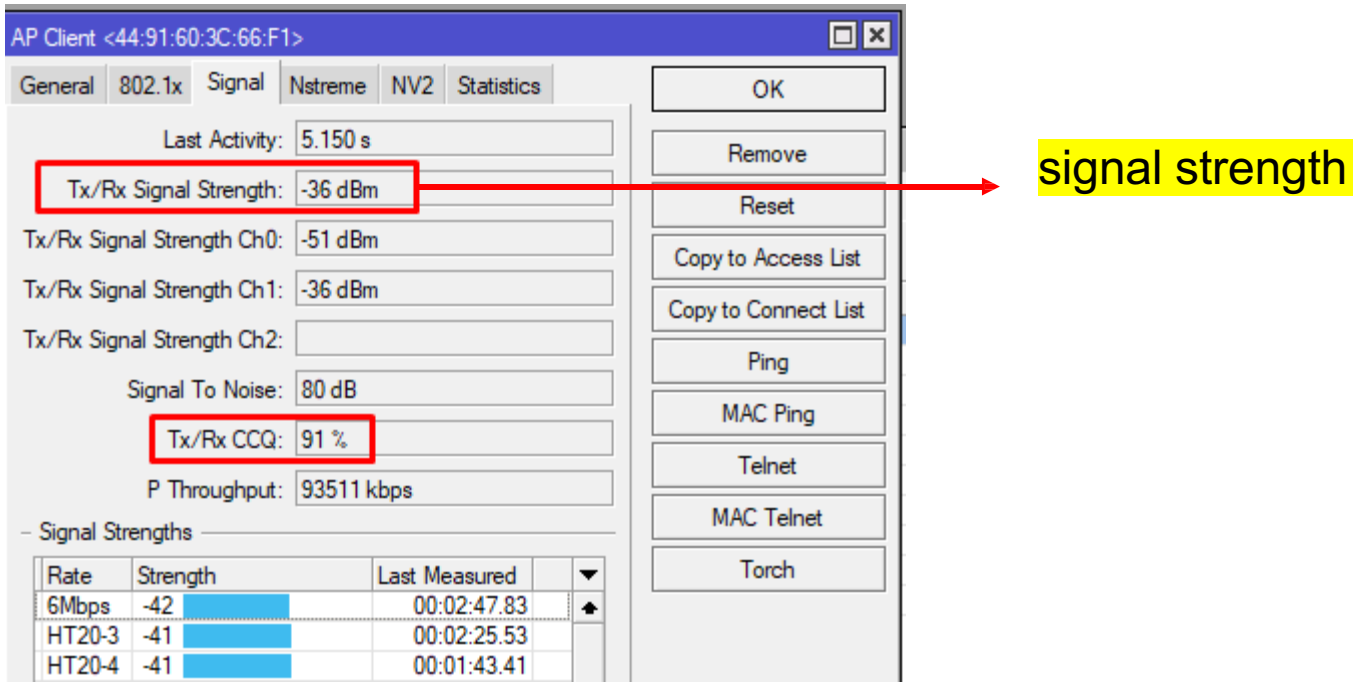
BANDWIDTH TEST

- Bandwidht test digunakan untuk mengukur seberapa besar link dapat mendeliver bandwidth.
- Untuk menjamin keakuratan, bandwidth test hanya dijalankan di salah satu sisi.
- Tool > Bandwidth Test
  - Test to = IP lawan
  - User & password = user password
  - router lawan



CCQ (CLIENT CONNECTION QUALITY)

- CCQ merupakan nilai yang menyatakan seberapa efektifkah bandwidth yang dapat digunakan.
- Untuk mengetahui CCQ bias melalui menu **Wireless > Registration** klik MAC Address

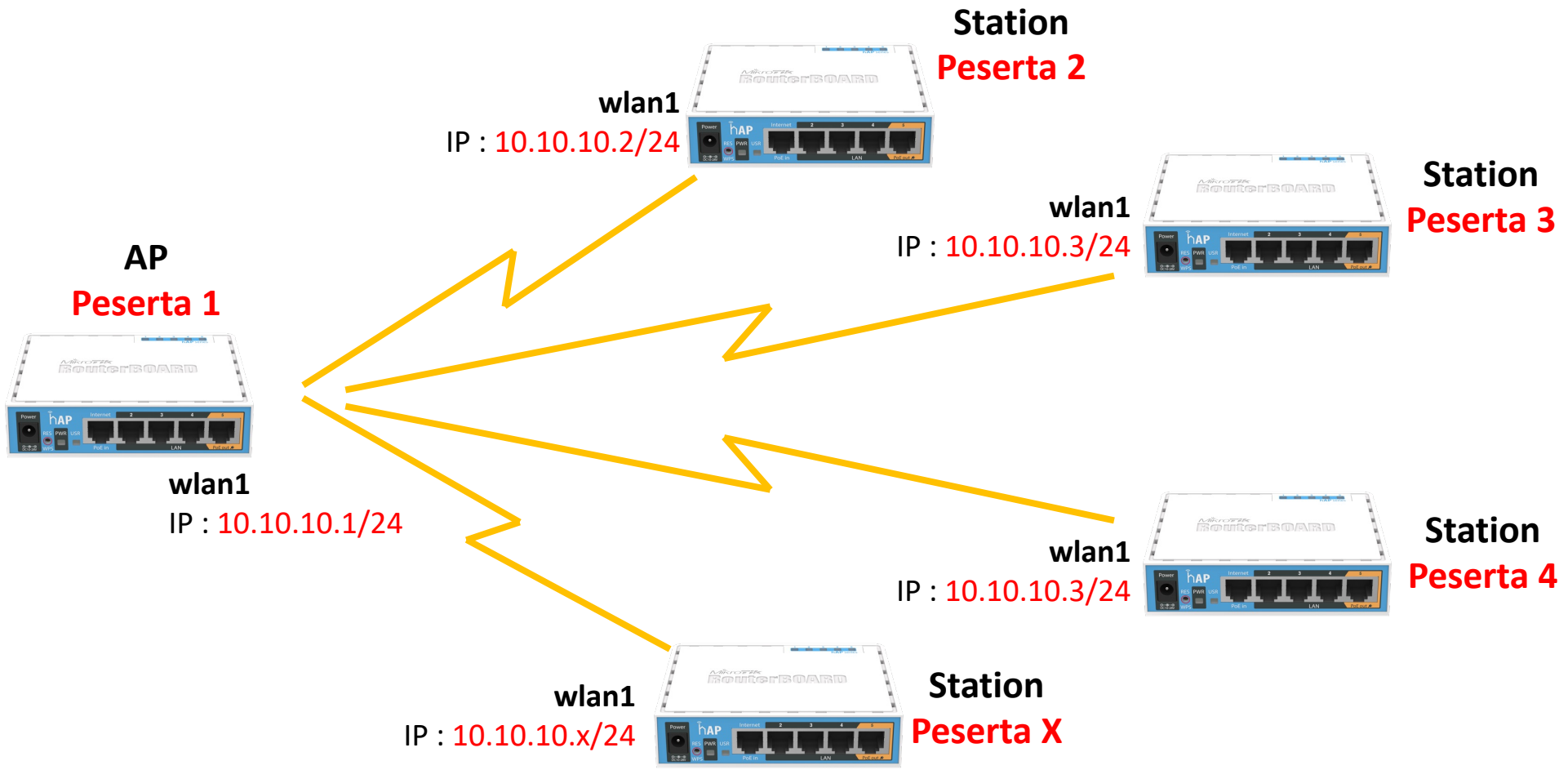


WIRELESS MAC FILTERING

- Salah satu keamanan di Wireless menggunakan fitur MAC Filtering.
- MAC Filtering bisa diterapkan di AP dan Station.
- MAC Filtering disisi **AP** bisa menggunakan **Access List.**
- MAC Filtering disisi **Station** bisa menggunakan **Connect List.**

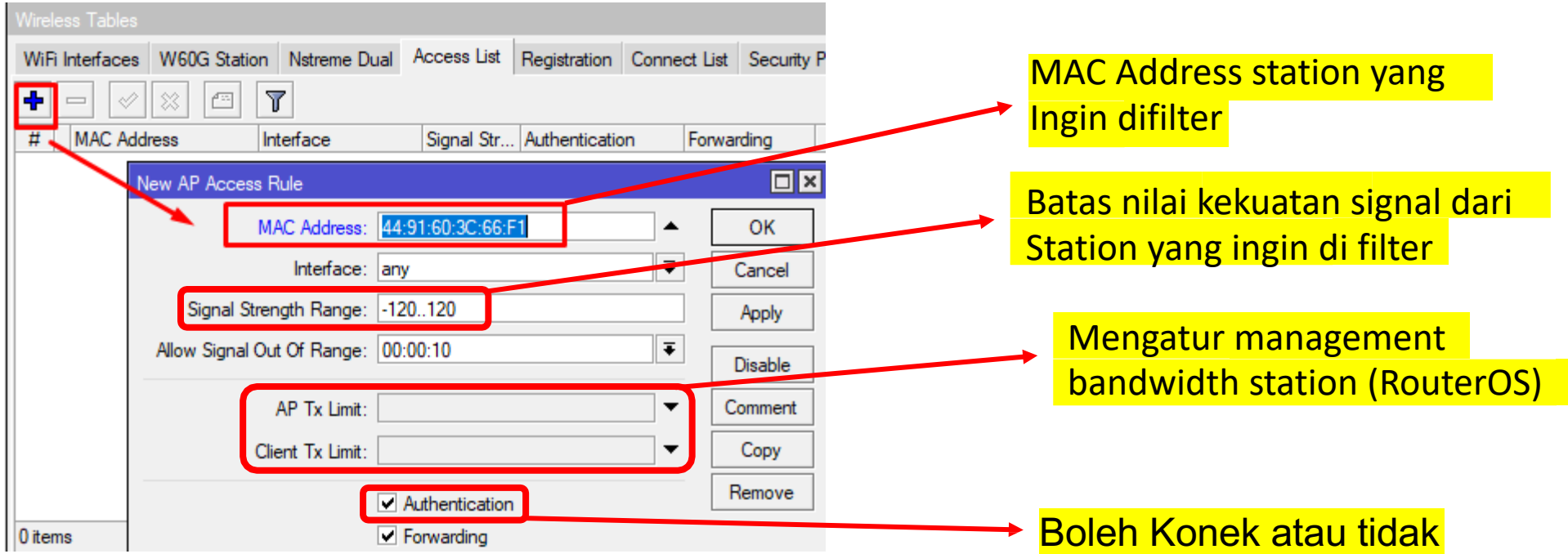
WIRELESS MAC FILTERING – ACCESS LIST

LAB



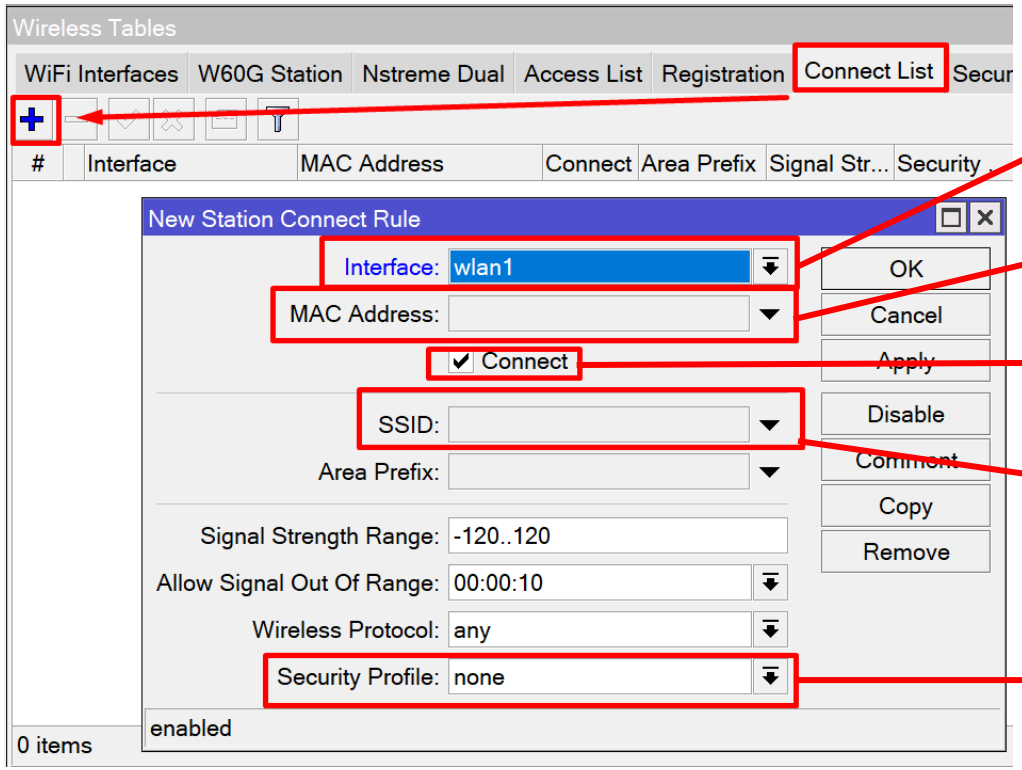
WIRELESS MAC FILTERING – ACCESS LIST

- Access List (Wireless > Access List) digunakan untuk memfilter station mana saja yang boleh terkoneksi ke AP dengan mendaftarkan informasi MAC Address Station



WIRELESS MAC FILTERING – CONNECT LIST

- Connect List (Wireless > Connect List) digunakan untuk membatasi AP mana saja yang boleh / tidak boleh terkoneksi oleh station.



Interface radio yang difungsikan sebagai client

MAC Address AP

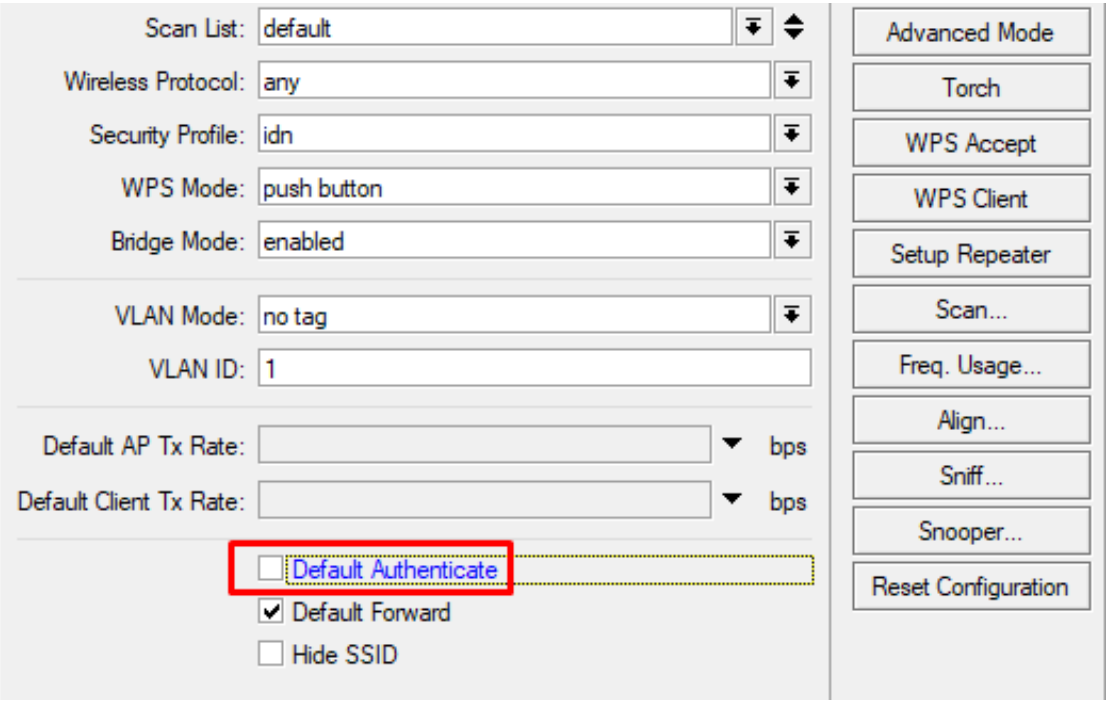
Boleh / tidak boleh konek dengan MAC Addrss diatas

SSID yang akan dikoneksikan. Bila kosong berarti any AP

Bisa menambahkan security profile yang dibuat sebelumnya

DEFAULT AUTHENTICATE

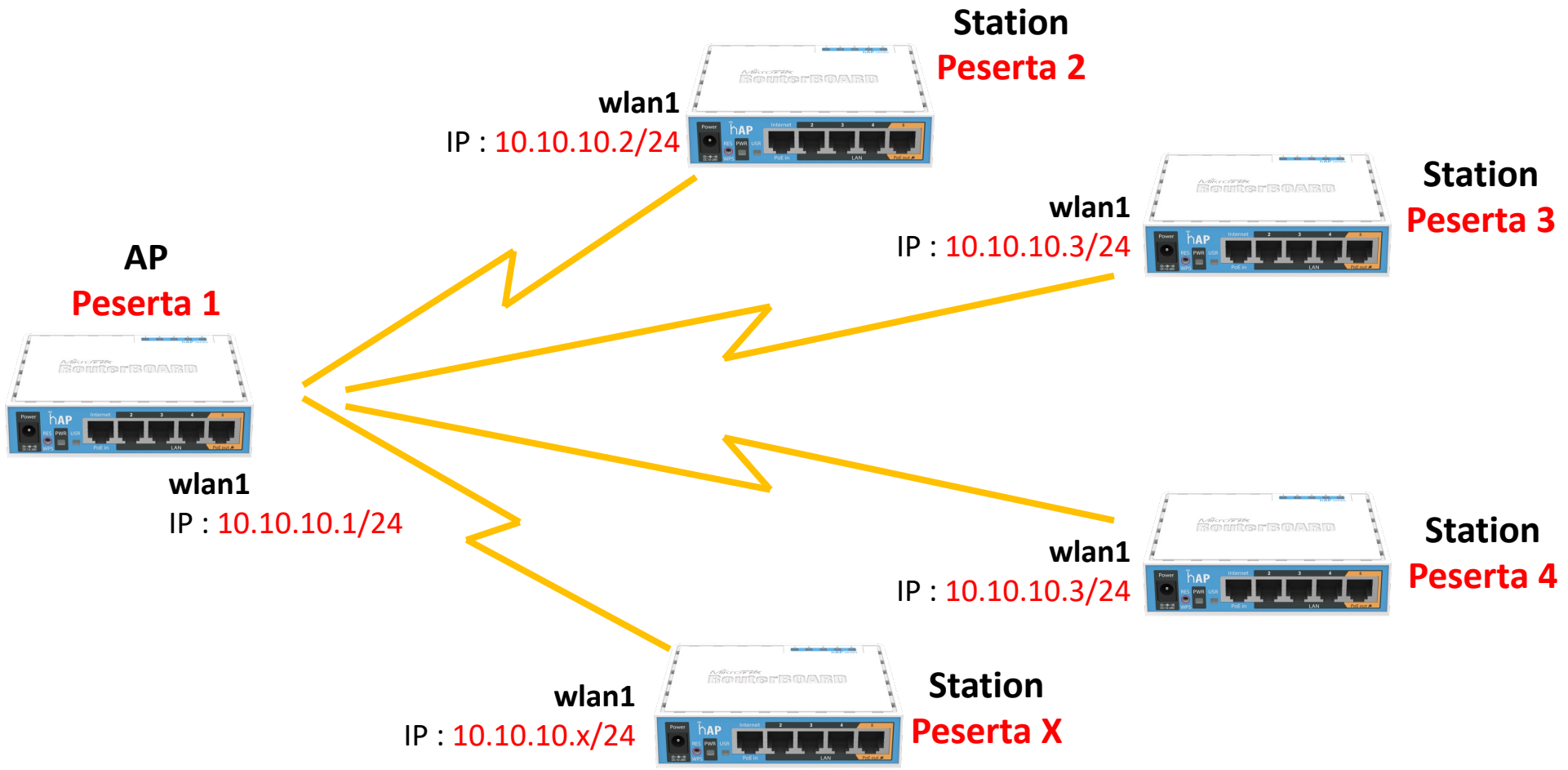
- Digunakan untuk mengijinkan semua station terkonkesi ke AP (Baik yang sudah terfilter ataupun belum bisa konek)
- **Wifi Interface > wlan1 > Wireless Tab**



Bila diuncheck, hanya station yang sudah terdaftar (terfilter di MAC Filtering) saja yang bias konek ke AP

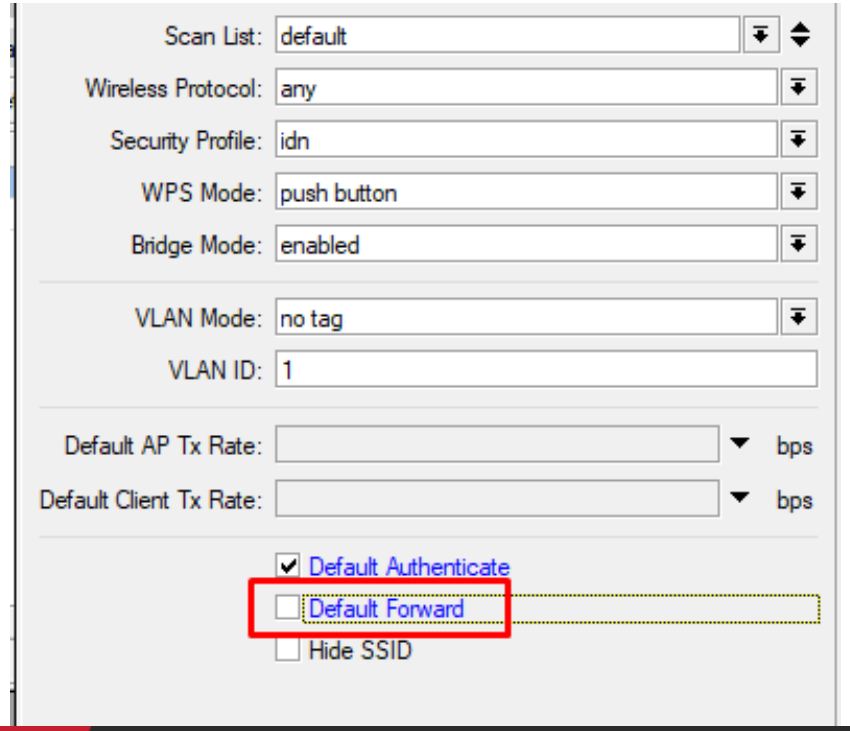
DEFAULT FORWARD

LAB



DEFAULT FORWARD

- Digunakan untuk mengijinkan komunikasi antar station yang terkoneksi dalam satu AP (default = enable).
- Fitur ini cuman ada di sisi AP. **(Wireless Interface > wlan1 > Wireless Tab)**



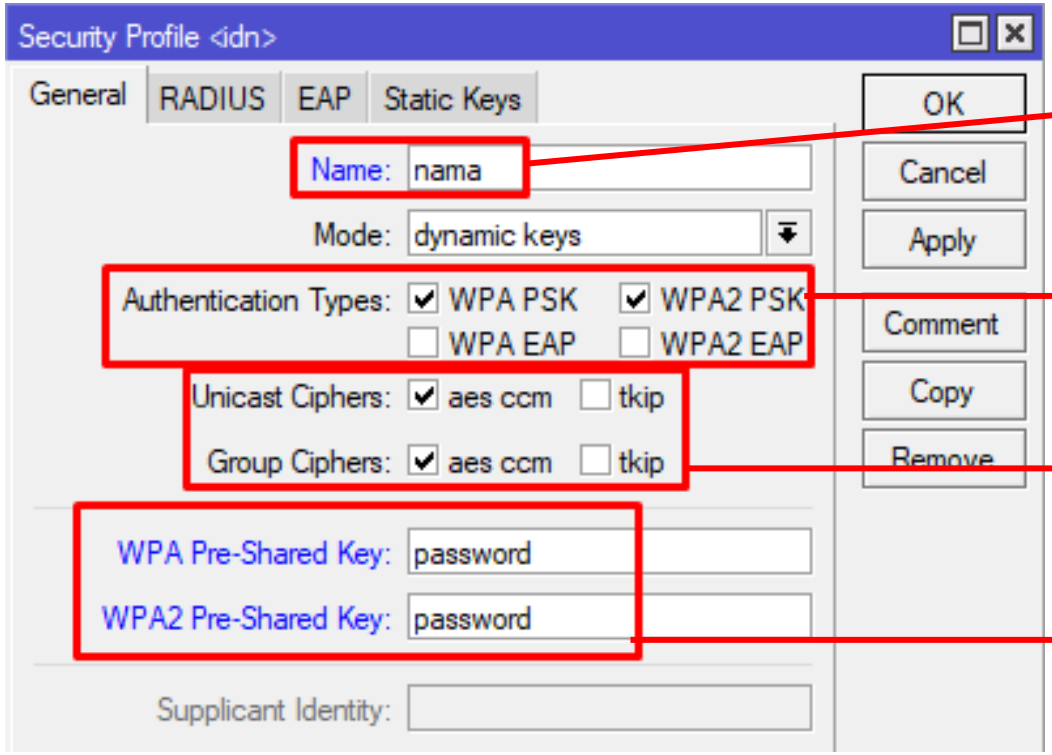
Bila diuncheck, maka antar station tidak akan bisa saling komunikasi.

WIRELESS SECURITY

- Untuk pengamanan koneksi wireless, tidah hanya dengan MAC-Filtering saja, karena masih ada cara untuk melakukan cloning MAC Address.
- Selain itu, data yang dilewatkan dijaringan bias di ambil dan dianalisa.
- Terdapat metode keamanan lain yang dapat digunakan yaitu:
  - Authentikasi (WPA-PSK, WPA-EAP)
  - Enkripsi (AES, TKIP, WEP)
- Kedua metode keamanan tersebut ada di menu **Wireless > Security Profile.**
- Mode wireless security profile :
  - None : mode tanpa authentikasi dan enkripsi (open wireless)
  - Dynamic : mode yang hanya support enkripsi (WPA)
  - Static : mode yang hanya support enkripsi (WEP)

WIRELESS SECURITY

- Wireless > Security Profile



Nama Security Profile

Jenis Authentikasi

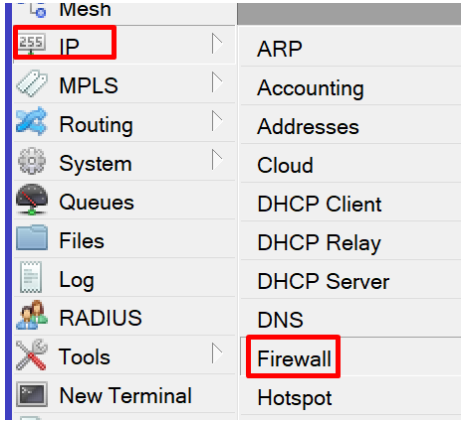
Model Enkripsi

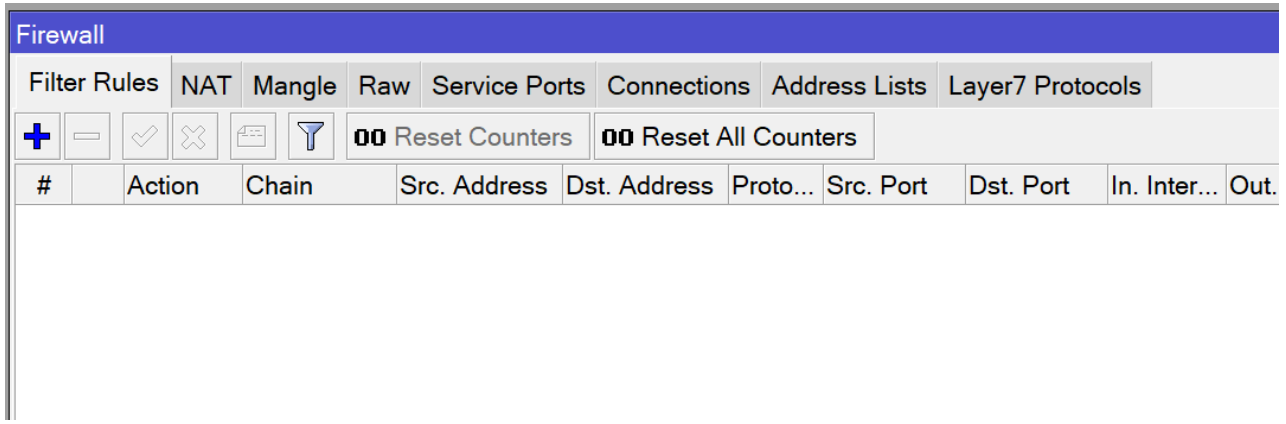
Key authentikasi/password

MODUL 6
FIREWALL

FIREWALL

- Firewall digunakan sebagai pelindung jaringan, baik yang berasal dari WAN (Internet) maupun dari LAN (Local).
- Melindungi dari network lain yang melewati router.
- Fitur firewall pada RouterOS ada pada menu **IP > Firewall.**
- Basic Firewall ada di **IP > Firewall > Filter Rules**



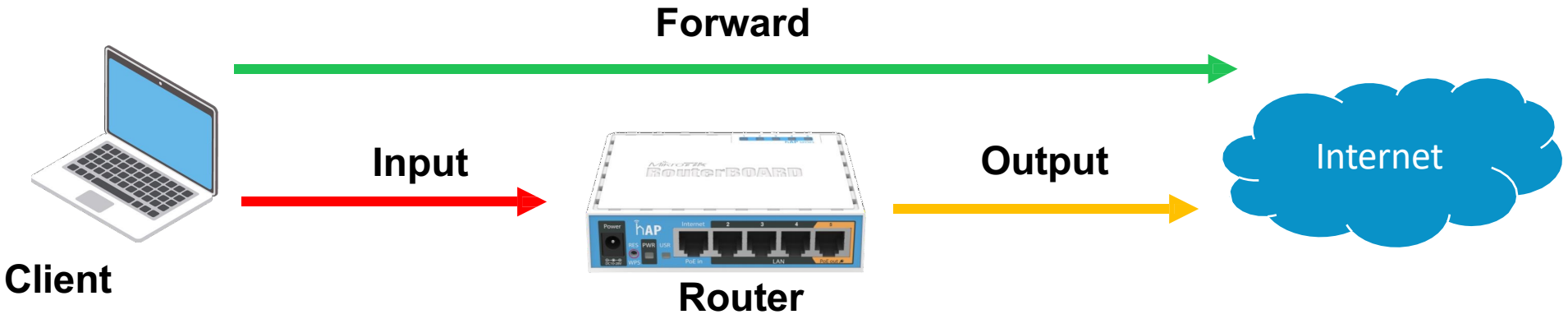


FIREWALL – FILTER RULES

- Firewall filter rule merupakan basic firewall di RouterOS.
- Setiap firewall filter rule **di organisir dalam chain (rantai)** yang berurutan.
- Setiap chain yang dibuat akan **dibaca** oleh router dari **atas ke bawah**.
- **Paket dicocokan** dengan kriteria/persyaratan dalam suatu chain, apabila cocok paket **akan dieksekusi**. Namun apabila paket yang masuk ke firewall **tidak cocok** makan akan **dilarikan ke rule dibawahnya sampai dia match.**
- Terdapat **3 default chain (input, output, forward).**
- Dimungkinkan juga kita dapat membuat custom chain sesuai dengan yang diinginkan.
- **By default** jika di **Filter Rules tidak ada settingan sama sekali,** artinya **semua traffic yang masuk atau melewati router akan diijinkan** baik itu yang aman atau yang tidak aman.

FIREWALL – SIMPLE PACKET FLOW

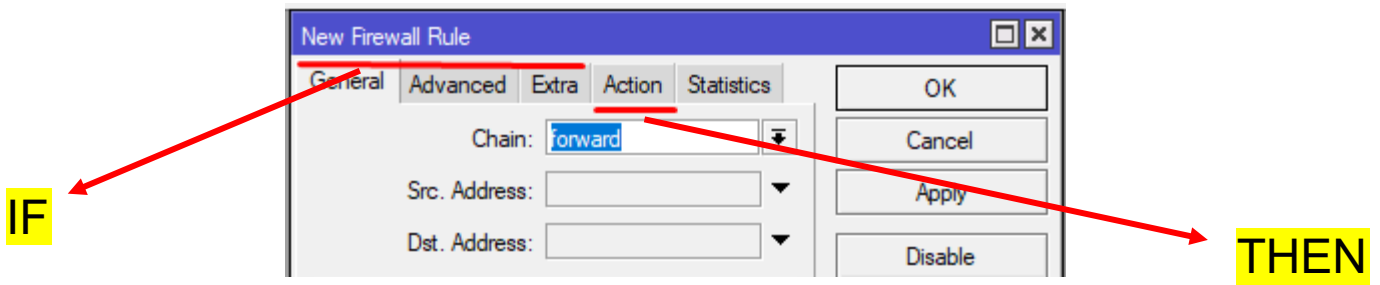
- Tiga aturan dasar packet flow:
  - Input – ke router
  - Output – dari router
  - Forward – melewati router



FIREWALL – IF (CONDITION)

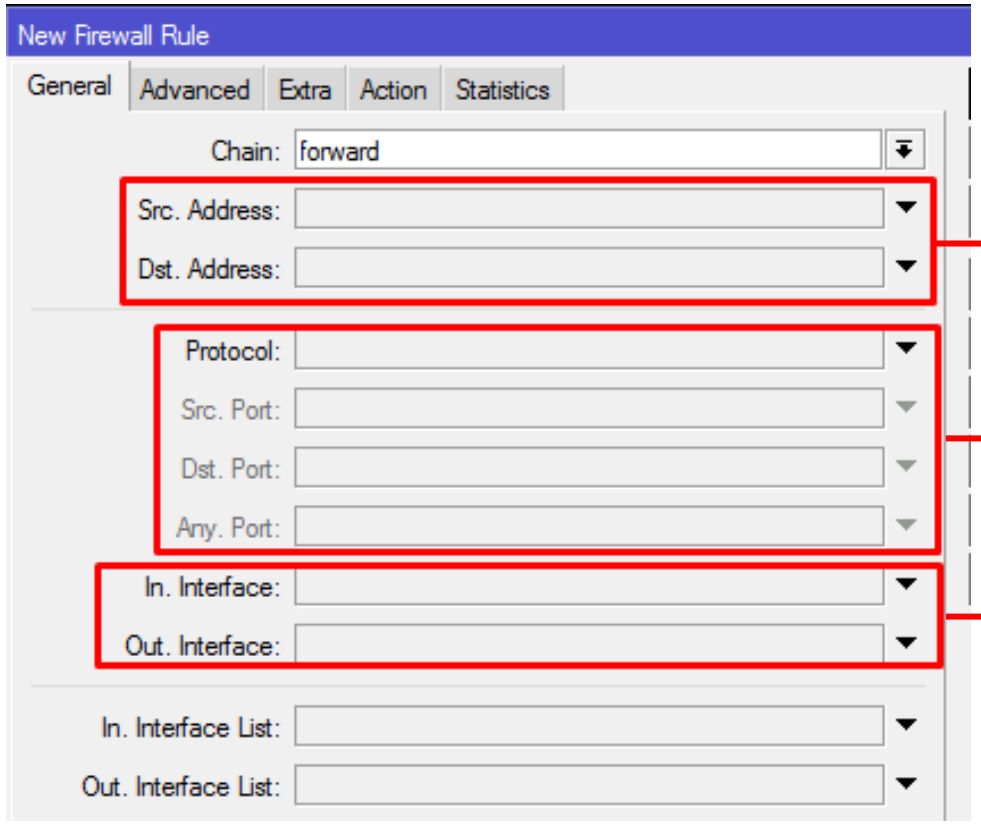
- Prinsip IF …. Then ….
  - IF (Jika) paket memenuhi syarat kriteria yang kita buat.
  - Then (maka) action apa yang akan kita berikan ke paket tersebut.

- Di firewall Filter Rule **IF condition** ada dimenu **(General, Advanced dan Extra)** sedangkan **Then condition** ada dimenu **action**



FIREWALL FILTER – IF (GENERAL)

- IP > Firewall Filter > General

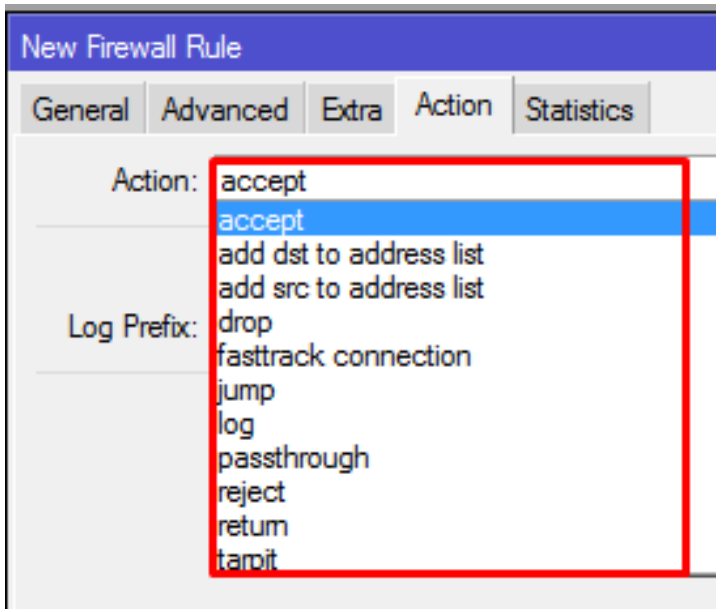


Source address (alamat sumber), Destination address (alamat tujuan) format bisa spesifik IP, spesifik network atau semua network (any).

Protocol (TCP/UDP/ICMP, dll)
Source Port (port sumber/ dari client)
Destination port (port tujuan)

Interface (traffic masuk atau keluar)

FIREWALL FILTER – THEN (ACTION)



- **IP > Firewall Filter > Action**
- **accept** – paket akan di terima (di ijinkan)
- **add-dst-to address-list** – alamat tujuan akan di tambahkan ke dalam address list (grup ip address)
- **add-src-to address-list** – alamat source akan di tambahkan ke dalam address list
- **drop** – paket akan di tolak (tidak di ijinkan)
- **fasttrack connection** – fitur alternative untuk speedboost traffic data.
- **jump** - paket akan di lempar ke spesifik custom chain yang kita buat
- **log** – paket akan dibuatkan sebuah catatan atau log khusus. Passtrough – paket akan di biarkan (di eksekusi) dan di ijinkan membaca rule selanjutnya
- **reject** - sama kayak drop, cuman nanti keluar pesan ICMP reject. return – paket akan dikembalikan dimana lokasi action jump di buat. tarpit - membuka port bayangan yang ada di router, seolah-olah semua port di router aktif, tetapi tidak akan pernah bisa di akses.

FREQUENTLY USED PORTS

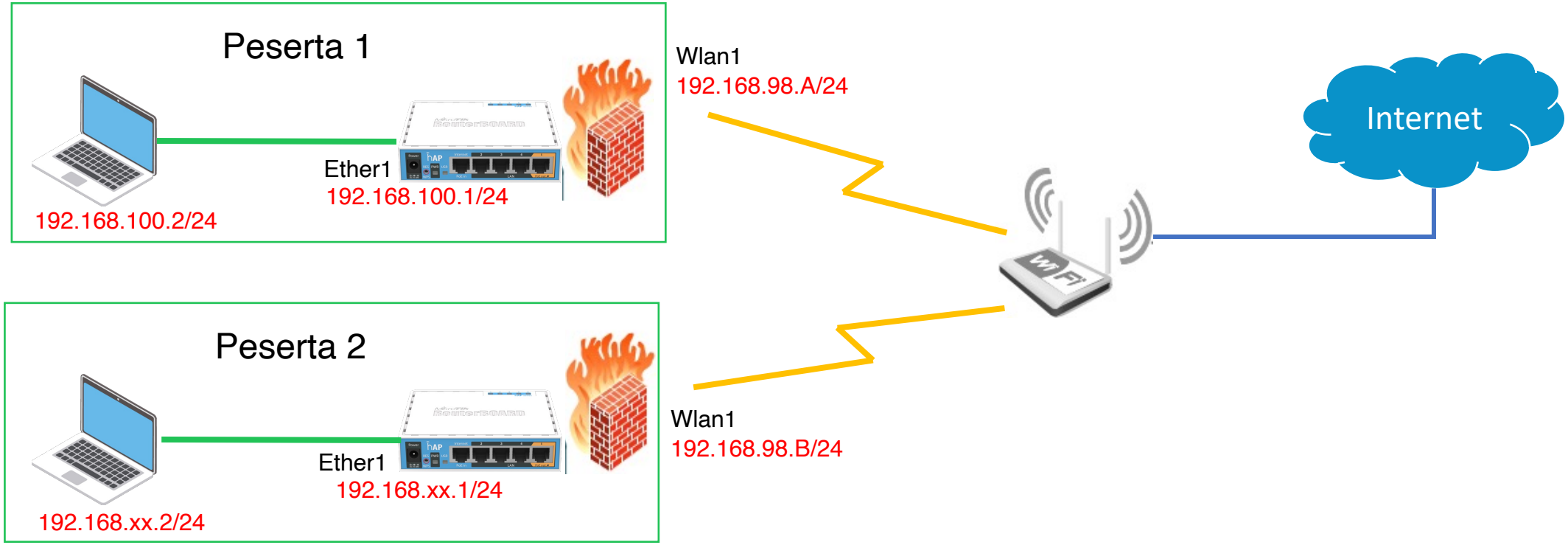
- **Beberapa port yang biasanya sering digunakan pada Firewall**

Port/protocol	Service
80/tcp	HTTP
443/tcp	HTTPS
22/tcp	SSH
23/tcp	Telnet
20,21/tcp	FTP
8291/tcp	Winbox
5678/udp	MNDP
20561/udp	MAC Winbox

FIREWALL – PROTECTING OUR ROUTER (1)

LAB

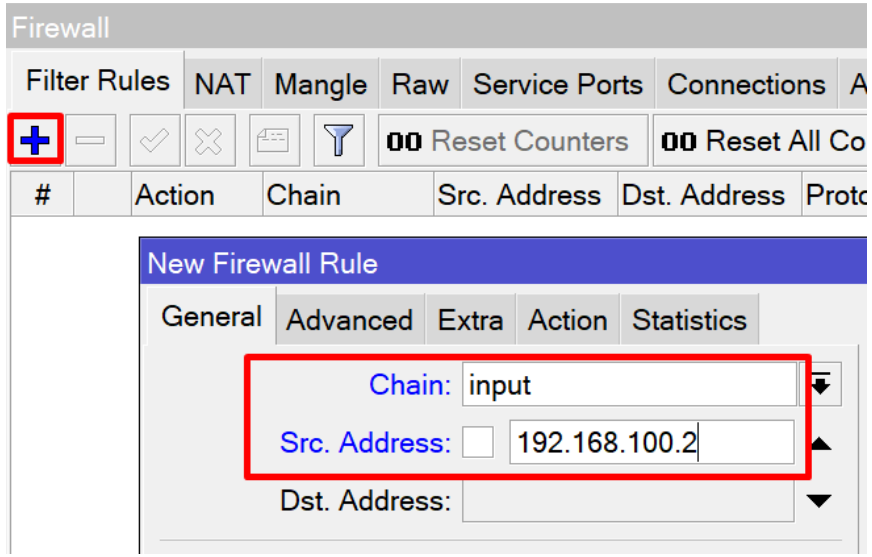
- Buatlah firewall untuk mengijinkan hanya IP laptop saja yang bisa akses router.



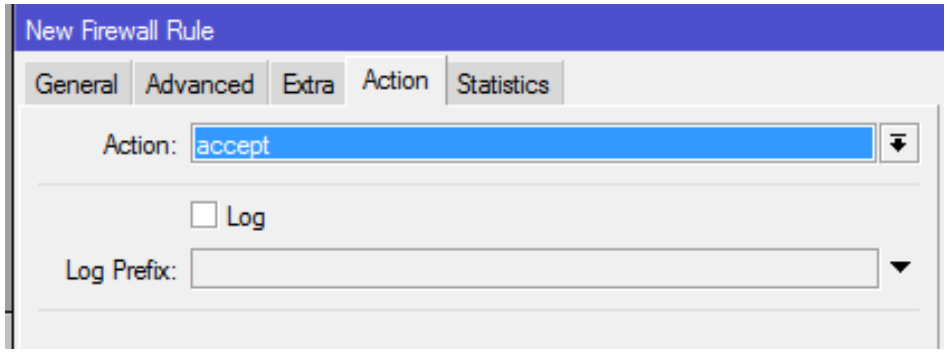
FIREWALL – PROTECTING OUR ROUTER (2)

LAB

- IF ada traffic **input** yang berasal dari IP laptop **(192.168.100.2)**



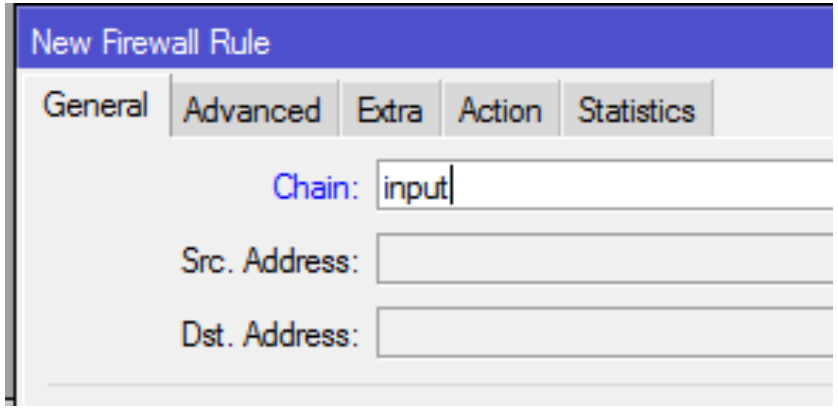
- THEN tentukan action > **accept**



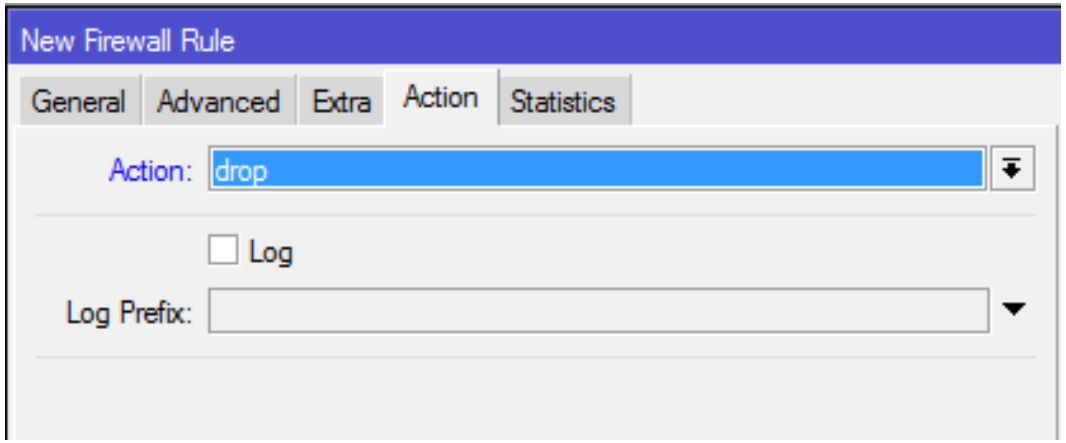
FIREWALL – PROTECTING OUR ROUTER (3)

LAB

- IF ada traffic **input** yang berasal dari <kosong> atau “any address/network”



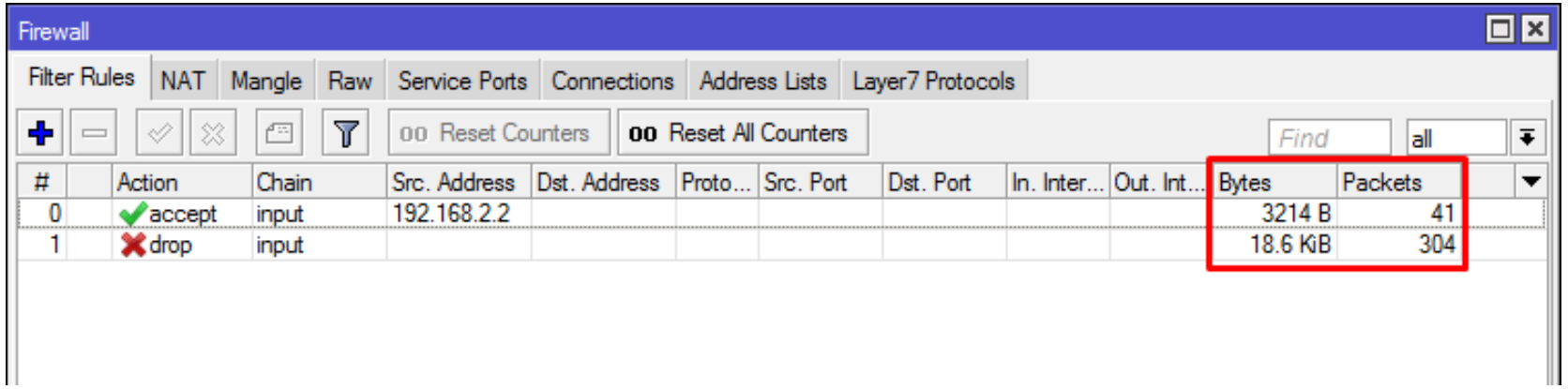
- THEN tentukan action > **drop**



FIREWALL – PROTECTING OUR ROUTER (4)

LAB

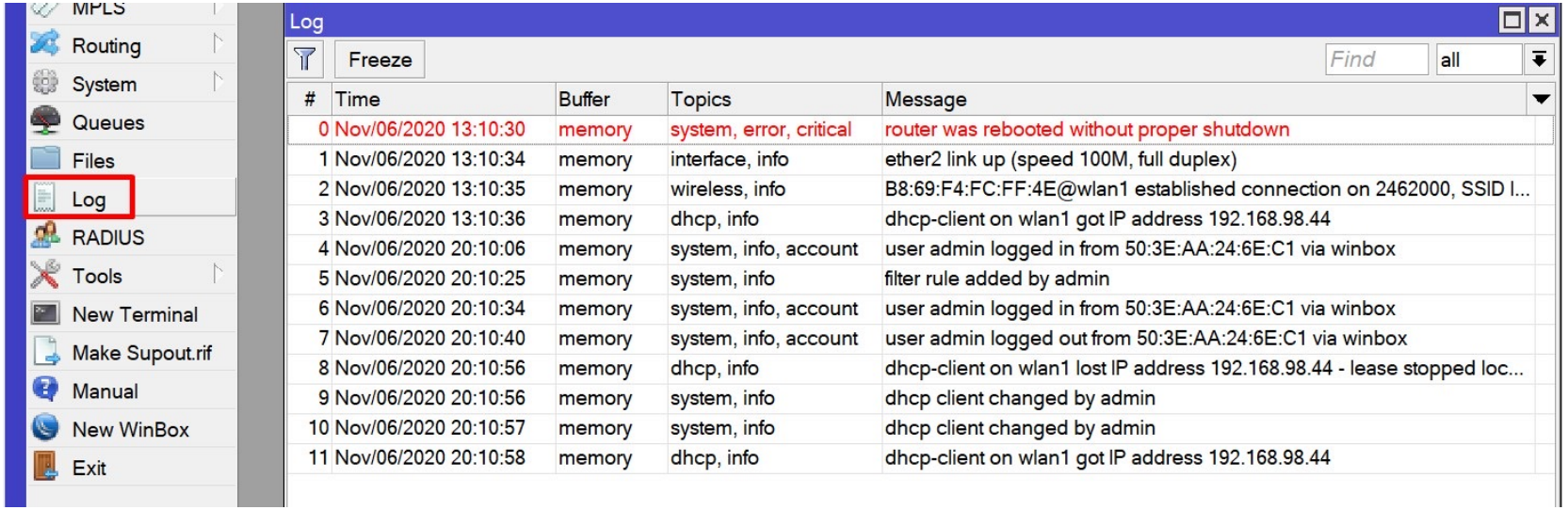
- Akan ada 2 chain rules



- Perhatikan jumlah bytes di setiap chain rule, tetap ataukah bertambah Ketika kita melakukan akses ke router
- Coba masing-masing peserta untuk melakukan ping, akses web, dan remote winbox ke router peserta lain.

FIREWALL – LOG

- Log merupakan fitur yang digunakan untuk menampilkan beberapa informasi / aktivitas yang ada pada router.

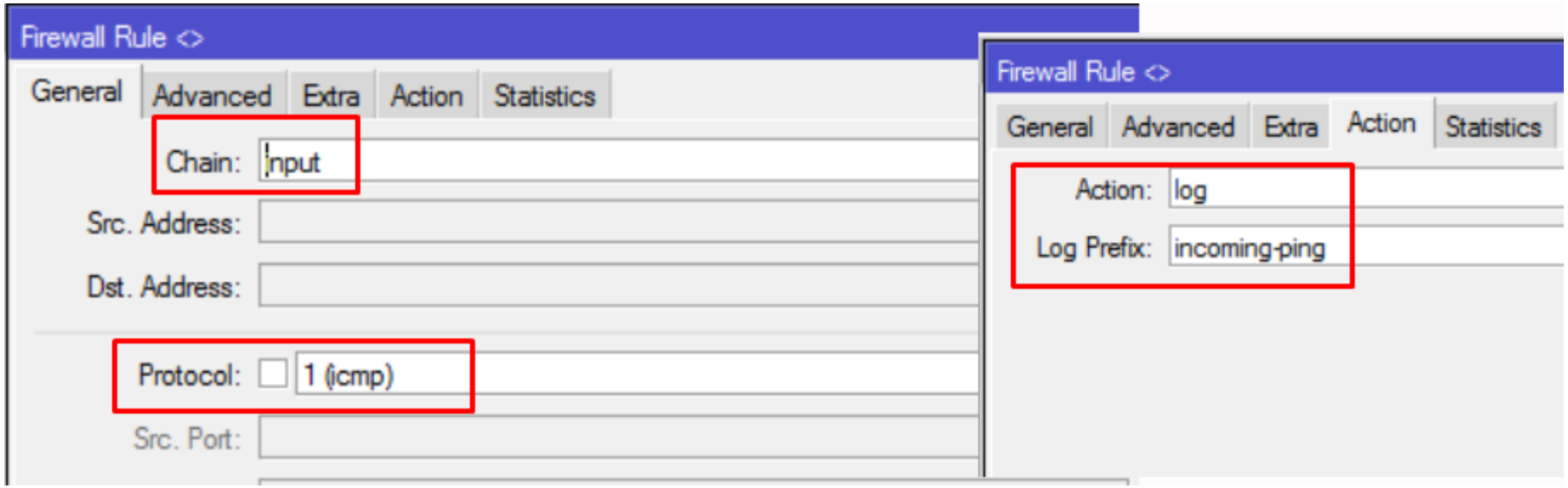


- Kita dapat membuat atau menambahkan catatan aktivitas apa saja sesuai yang diinginkan melalui firewall filter dengan menggunakan action **log.**

FIREWALL – LOG

LAB

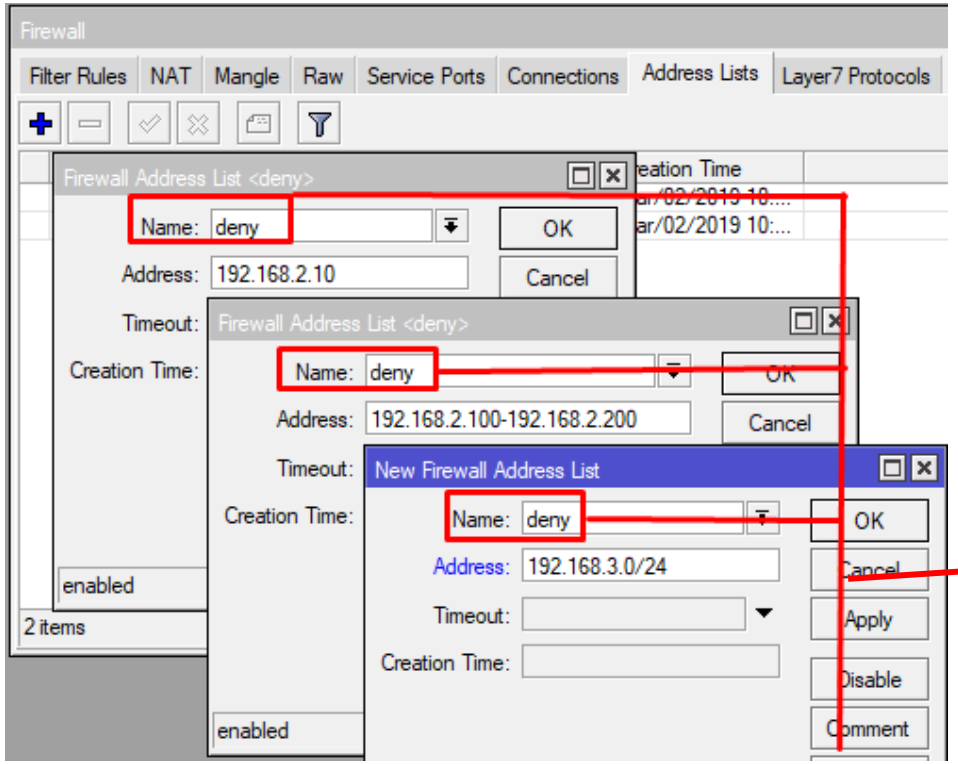
- Buatlah log untuk mencatat aktivitas ping yang masuk ke router.
- Caranya buat rule baru pada IP > Firewall > Filter Rules.



- Ping IP router dari laptop atau dari peserta lain, amati log pada router.

FIREWALL – ADDRESS LIST

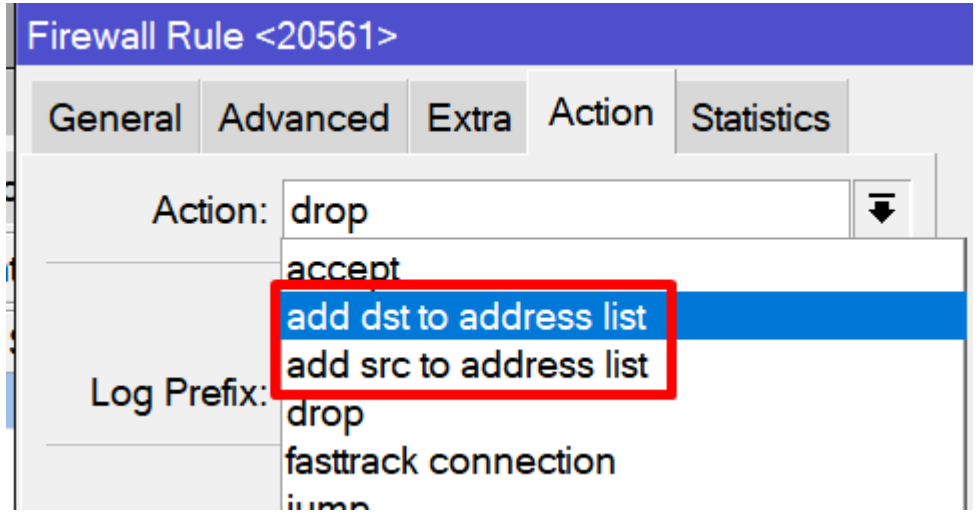
- Address list digunakan untuk memfilter berdasarkan group IP.
- Satu line address-list dapat berupa subnet, range IP atau spesifik IP.

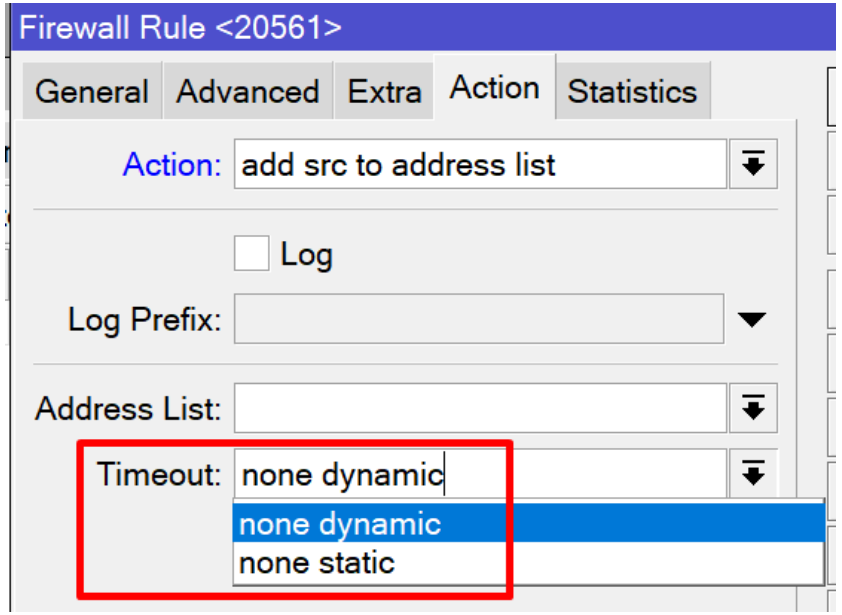


Beberapa address dengan nama grup yang sama.

FIREWALL – ADDRESS LIST

- Address list dapat dibuat juga secara otomatis dengan memanfaatkan action “add-to-address list”.
- Kita juga dapat mengatur apakah address-list yang dibua secara permanen atau sementara dengan mengatur timeout





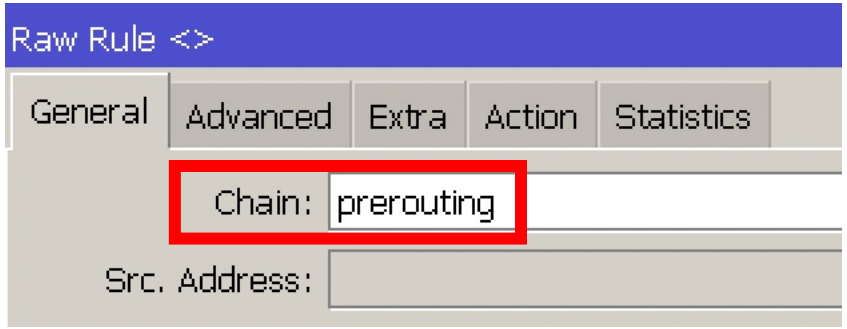
FIREWALL – ADDRESS LIST

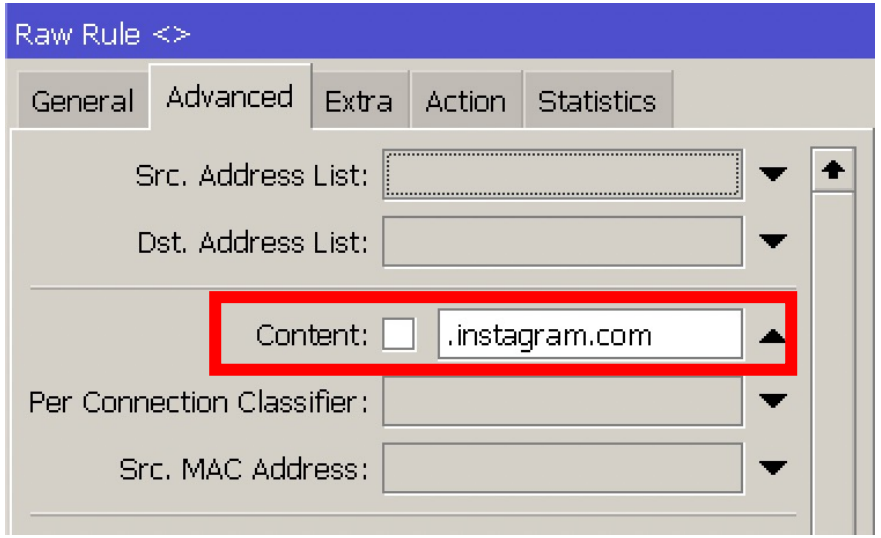
- Kita akan coba block facebook dan Instagram dengan MikroTik
- Ada 2 step untuk melakukan nya :
  - Setiap user akses facebook dan Instagram, akan dicatat IP Instagram/fb ke dalam Address List
  - IP yang tercatat di address list akan kita block.

	Name	Address	Timeout
D	ip-instagram	157.240.208.9	23:59:11
D	ip-instagram	157.240.208.63	23:59:15
D	ip-instagram	157.240.235.63	23:59:15

FIREWALL – ADDRESS LIST

- Kita akan gunakan content untuk mencatat IP Instagram / Facebook nya.
- Menggunakan IP – Firewall – RAW untuk mencatat IP nya (lebih ringan dibanding firewall filter)
- Instagram :
  - .instagram.com
  - .cdninstagram.com
- Facebook
  - .facebook.com
  - .facebook.net
  - .fbcdn.net

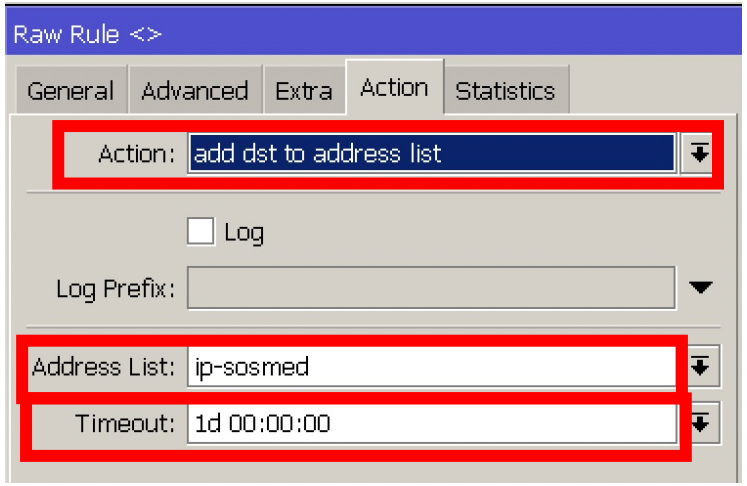




- Menggunakan “PREROUTING” untuk mencatat IP dari Laptop - Internet

FIREWALL – ADDRESS LIST

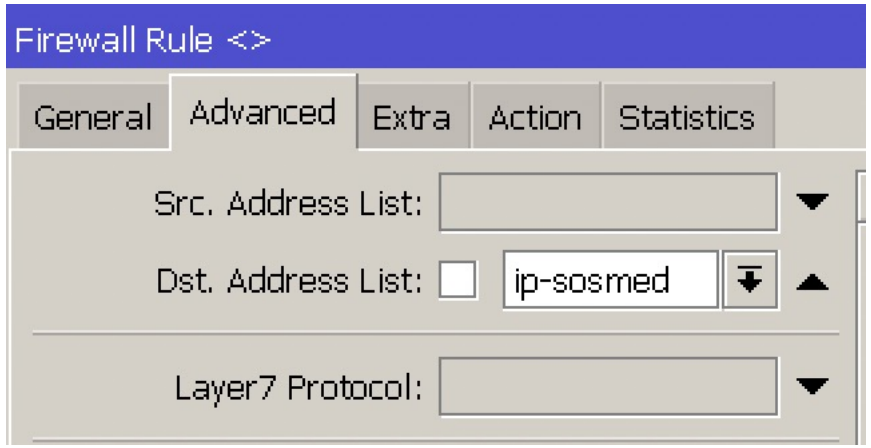
- Pada bagian action, gunakan “ADD DST TO ADDRESS LIST”
- Lalu ketik manual pada bagian Address List, misal nya IP Sosmed
- Untuk waktu nya kita isi 1d = 1hari karena IP social media sering berubah.
- Lalu cek hasil nya di IP – Firewall – Address List

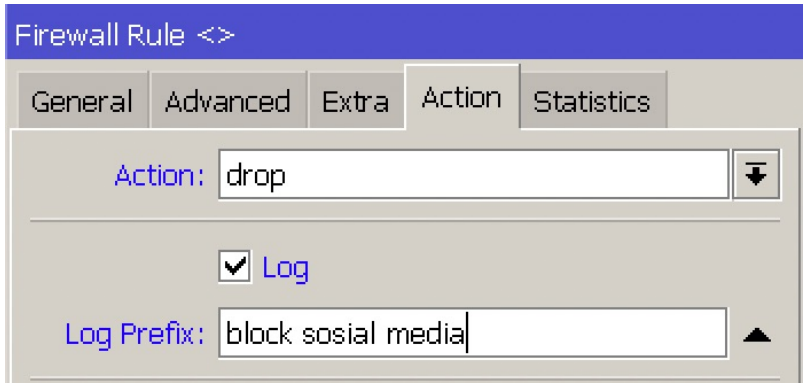


	Name	Address
D	ip-sosmed	31.13.95.1
D	ip-sosmed	31.13.95.13
D	ip-sosmed	31.13.95.19
D	ip-sosmed	31.13.95.34
D	ip-sosmed	31.13.95.35
D	ip-sosmed	31.13.95.63
D	ip-sosmed	112.78.129.210
D	ip-sosmed	112.78.129.211
D	ip-sosmed	112.78.129.225
D	ip-sosmed	114.121.226.81
D	ip-sosmed	114.124.224.209
D	ip-sosmed	157.240.208.9
D	ip-sosmed	157.240.208.14
D	ip-sosmed	157.240.208.16
D	ip-sosmed	157.240.208.23
D	ip-sosmed	157.240.208.34

FIREWALL – ADDRESS LIST

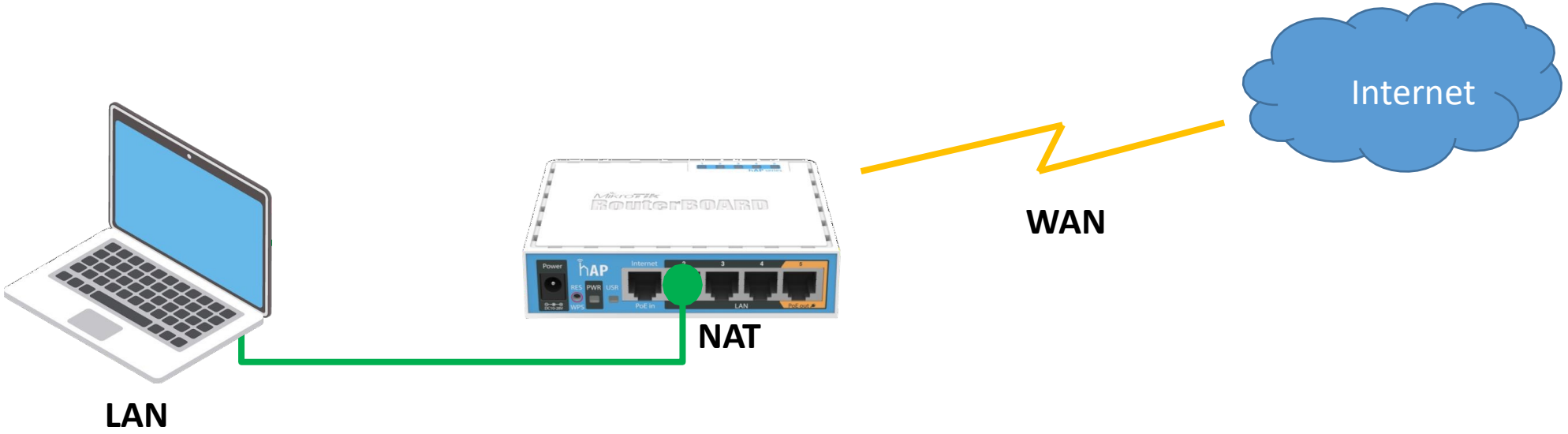
- Kalau sudah ada IP nya, setelah itu kita buatkan rule Firewall – Filter
- **IP – Firewall – Filter**





FIREWALL – NAT

- NAT (Network Address Translation) merupakan metode yang digunakan untuk menghubungkan banyak computer ke jaringan Internet dengan menggunakan satu / lebih alamat IP.
- NAT digunakan untuk ketersediaan alamat IP Public
- Prinsip NAT sama seperti Filter Rule, bekerja dengan “IF-THEN”.



FIREWALL – NAT

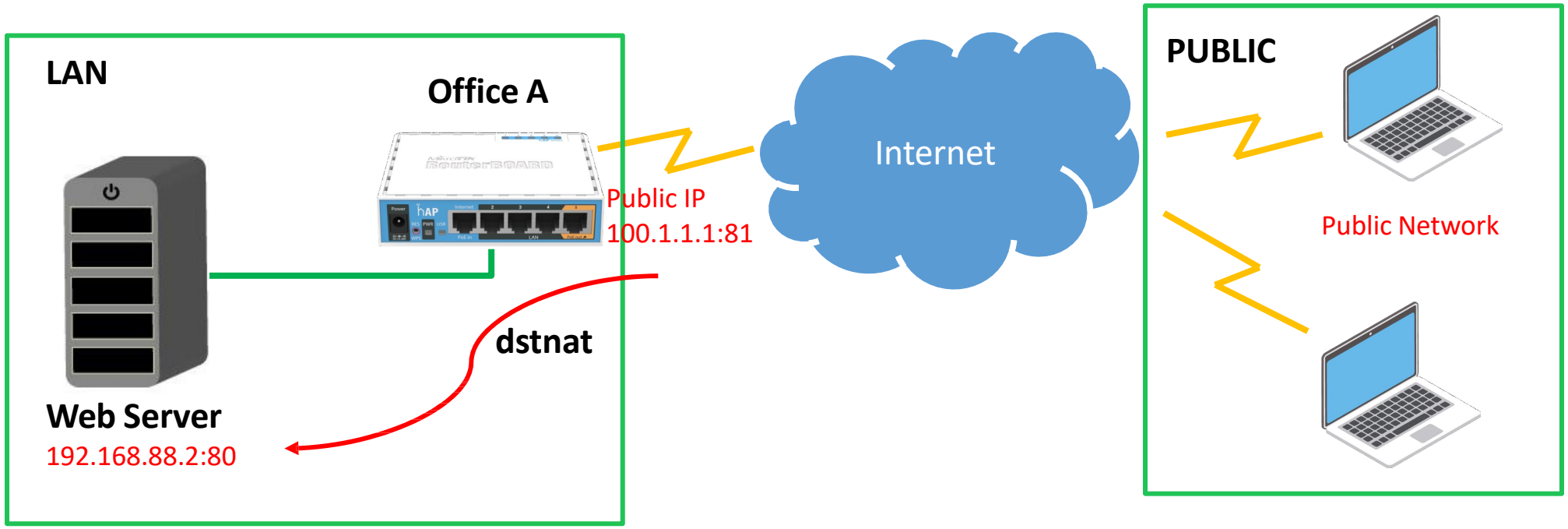
Di Mikrotik terdapat 2 type NAT :

- **Srcnat,** digunakan ketika client yang ada di dalam router ingin keluar (Internet).
  - Masquerade : digunakan untuk menghubungkan jaringan lokal ke internet menggunakan IP public dynamic.
  - Src-nat : digunakan untuk menghubungkan jaringan lokal ke internet menggunakan IP public static.
- **Dstnat,** digunakan ketika client di internet ingin mengakses jaringan local dari internet
  - Dst-nat : digunakan ketika akan mengakses jaringan lokal melalui internet (port forwarding). → melempar traffik ke luar router.
  - Redirect : digunakan ketika akan membelokan traffic ke router itu sendiri. contoh : hotspot, webproxy, dns server router dll

FIREWALL – DSTNAT

LAB

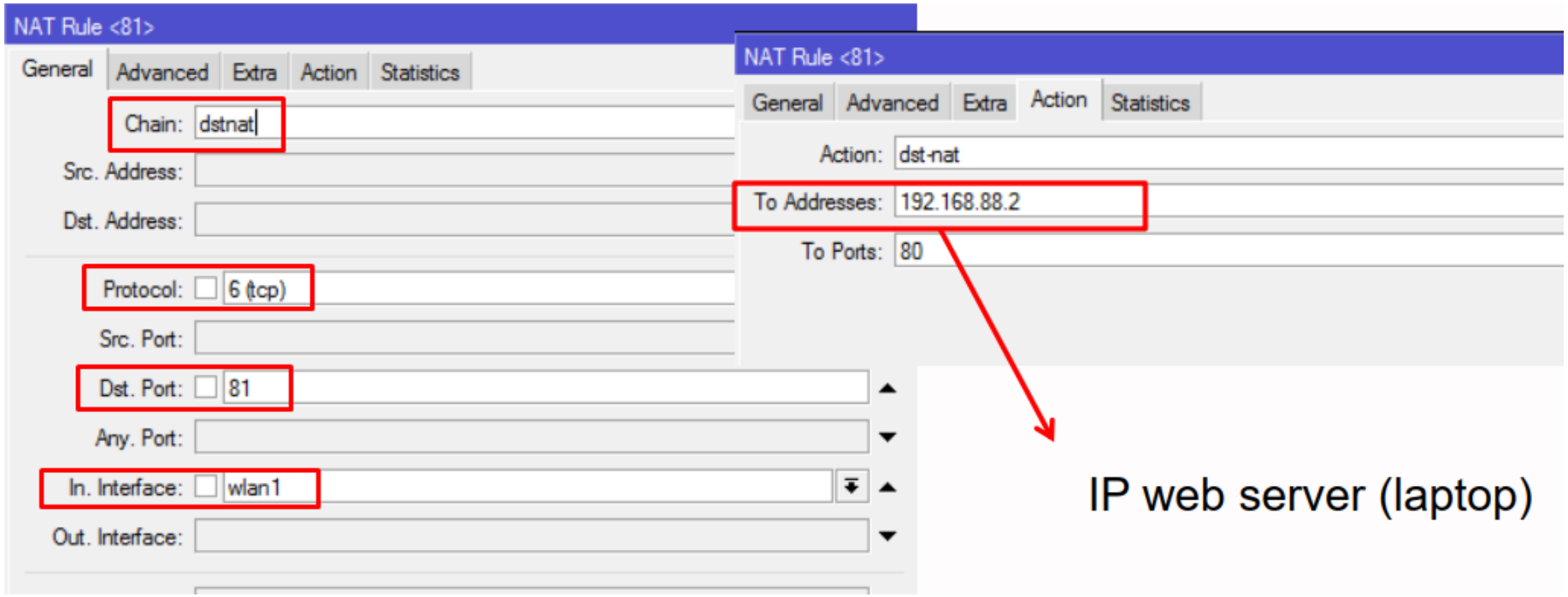
- DSTNAT digunakan untuk mengakses host/service yang ada di Lokal melalui Public Internet.



FIREWALL – DSTNAT

LAB

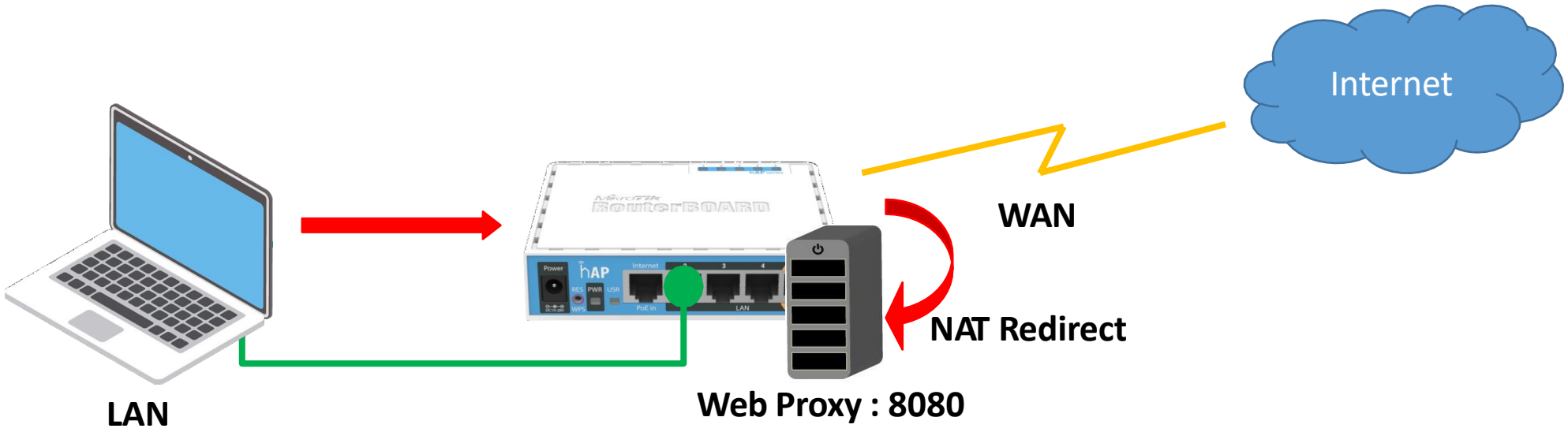
- Buat rule pada IP > Firewall > NAT untuk redirect port 81 router ke IP laptop dan port 80.



- Akses IP Public router **http://<ip wlan1 router>:81** dari laptop peserta lain.

FIREWALL – REDIRECT

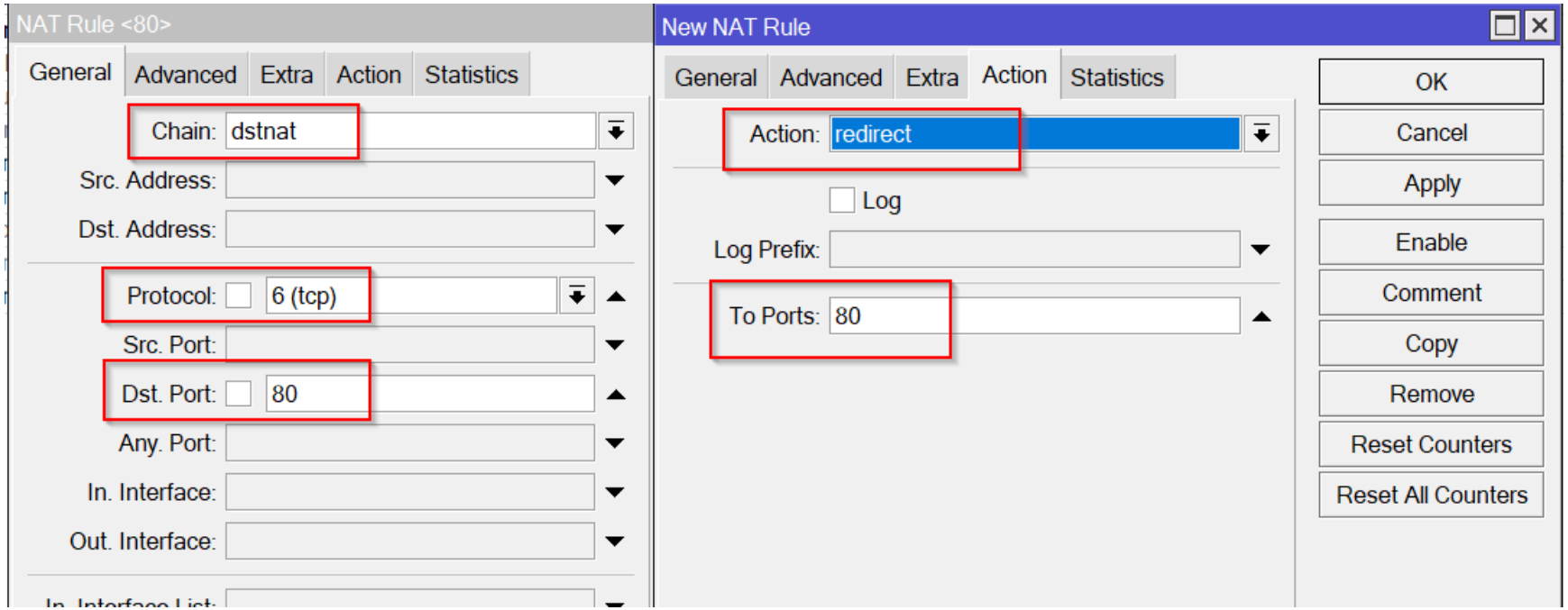
- Merupakan action yang digunakan untuk mengarahkan suatu paket kedalam spesifik servis / port yang ada pada router. (DNS, Web Proxy).
- Redirect hanya bisa digunakan apabila kita menggunakan chain dstnat



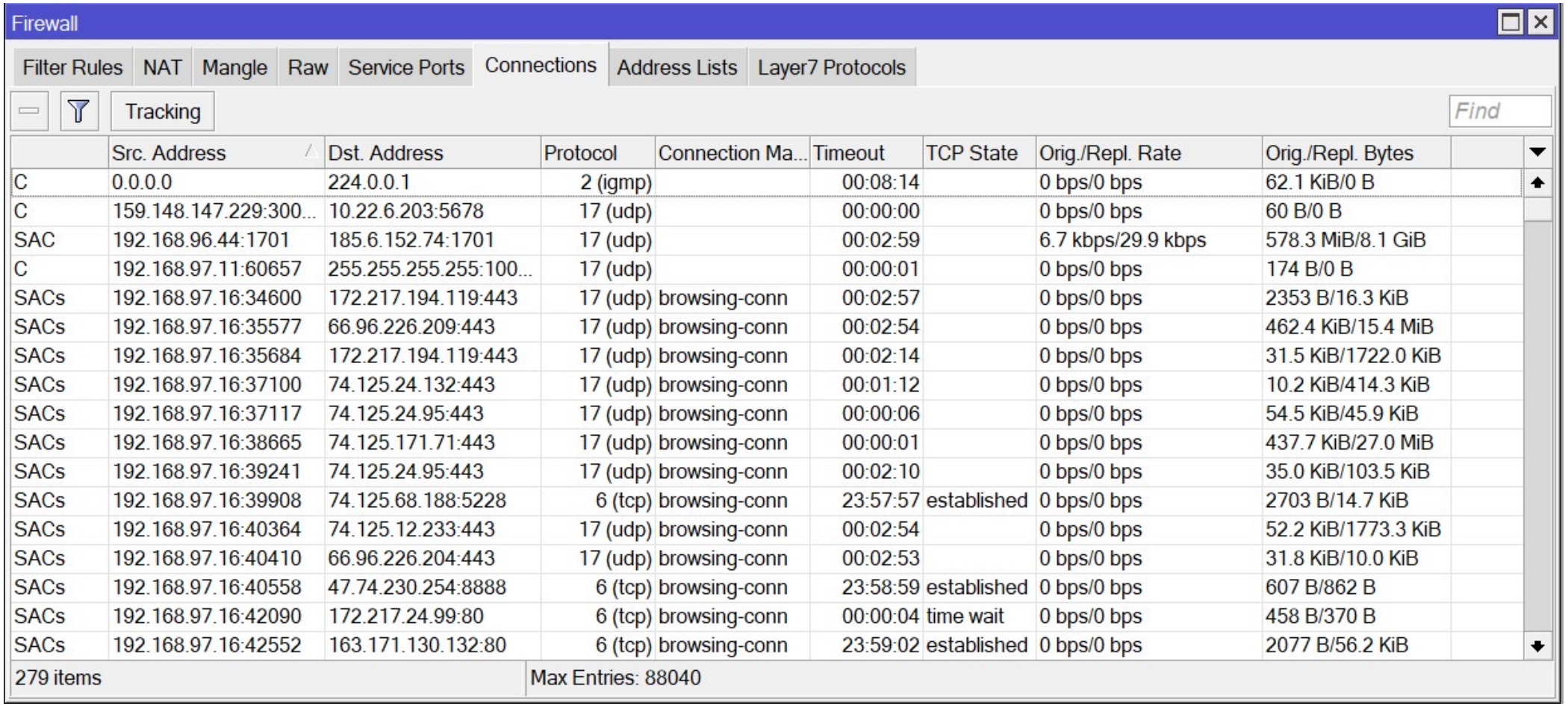
FIREWALL – REDIRECT

LAB

- Buat rule redirect, Ketika ada paket TCP/80 ke tujuan public maka akan dibelokan ke router port 80.



FIREWALL – CONNECTION TRACKING

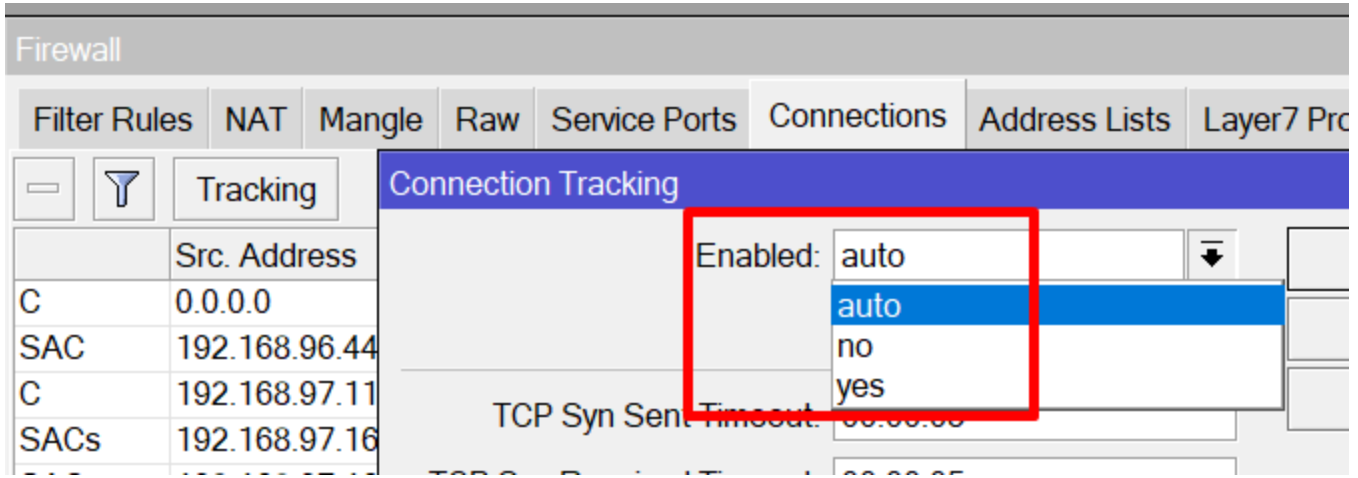


	Src. Address	Dst. Address	Protocol	Connection Ma...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
C	0.0.0.0	224.0.0.1	2 (igmp)		00:08:14		0 bps/0 bps	62.1 KiB/0 B
C	159.148.147.229:300...	10.22.6.203:5678	17 (udp)		00:00:00		0 bps/0 bps	60 B/0 B
SAC	192.168.96.44:1701	185.6.152.74:1701	17 (udp)		00:02:59		6.7 kbps/29.9 kbps	578.3 MiB/8.1 GiB
C	192.168.97.11:60657	255.255.255.255:100...	17 (udp)		00:00:01		0 bps/0 bps	174 B/0 B
SACs	192.168.97.16:34600	172.217.194.119:443	17 (udp)	browsing-conn	00:02:57		0 bps/0 bps	2353 B/16.3 KiB
SACs	192.168.97.16:35577	66.96.226.209:443	17 (udp)	browsing-conn	00:02:54		0 bps/0 bps	462.4 KiB/15.4 MiB
SACs	192.168.97.16:35684	172.217.194.119:443	17 (udp)	browsing-conn	00:02:14		0 bps/0 bps	31.5 KiB/1722.0 KiB
SACs	192.168.97.16:37100	74.125.24.132:443	17 (udp)	browsing-conn	00:01:12		0 bps/0 bps	10.2 KiB/414.3 KiB
SACs	192.168.97.16:37117	74.125.24.95:443	17 (udp)	browsing-conn	00:00:06		0 bps/0 bps	54.5 KiB/45.9 KiB
SACs	192.168.97.16:38665	74.125.171.71:443	17 (udp)	browsing-conn	00:00:01		0 bps/0 bps	437.7 KiB/27.0 MiB
SACs	192.168.97.16:39241	74.125.24.95:443	17 (udp)	browsing-conn	00:02:10		0 bps/0 bps	35.0 KiB/103.5 KiB
SACs	192.168.97.16:39908	74.125.68.188:5228	6 (tcp)	browsing-conn	23:57:57	established	0 bps/0 bps	2703 B/14.7 KiB
SACs	192.168.97.16:40364	74.125.12.233:443	17 (udp)	browsing-conn	00:02:54		0 bps/0 bps	52.2 KiB/1773.3 KiB
SACs	192.168.97.16:40410	66.96.226.204:443	17 (udp)	browsing-conn	00:02:53		0 bps/0 bps	31.8 KiB/10.0 KiB
SACs	192.168.97.16:40558	47.74.230.254:8888	6 (tcp)	browsing-conn	23:58:59	established	0 bps/0 bps	607 B/862 B
SACs	192.168.97.16:42090	172.217.24.99:80	6 (tcp)	browsing-conn	00:00:04	time wait	0 bps/0 bps	458 B/370 B
SACs	192.168.97.16:42552	163.171.130.132:80	6 (tcp)	browsing-conn	23:59:02	established	0 bps/0 bps	2077 B/56.2 KiB

279 items | Max Entries: 88040

FIREWALL – CONNECTION TRACKING

- Connection Tracking berisi informasi koneksi (source, destination IP, port,protocol yang sedang digunakan)
- Harus diaktifkan bila kita akan menggunakan beberapa service Firewall.
- **IP > Firewall > Connections > Tracking**



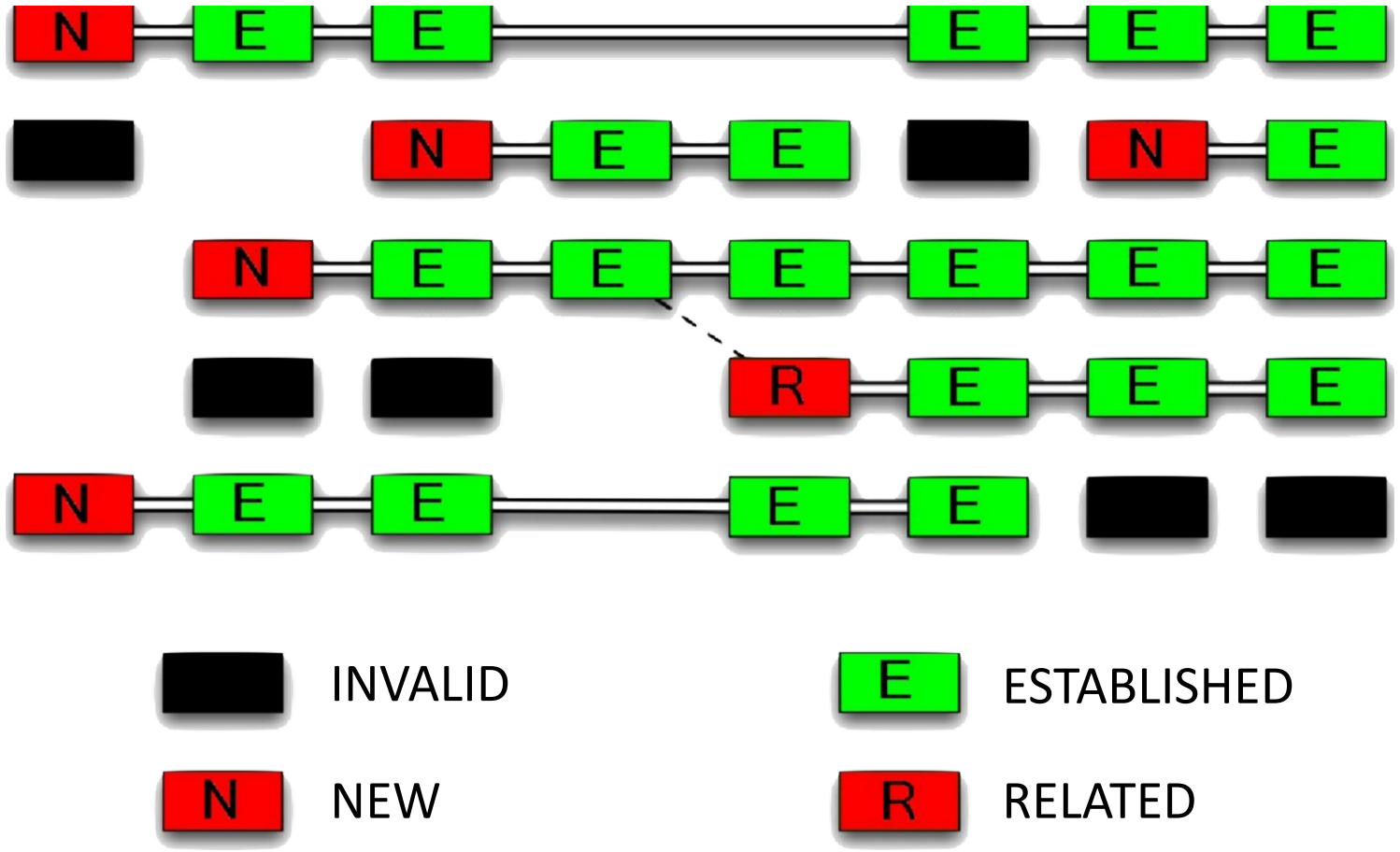
FIREWALL – CONNECTION TRACKING

- Bila connection tracking mati, beberapa fitur firewall tidak akan berfungsi sebagai berikut :
- NAT
- Firewall :
  - connection-bytes
  - connection-mark
  - connection-type
  - connection-state
  - connection-limit
  - connection-rate
  - layer7-protocol
  - new-connection-mark
  - tarpit

FIREWALL – CONNECTION TRACKING

- Status koneksi pada connection tracking :
  - **New** : membuka koneksi baru
  - **Established** : memiliki koneksi yang sudah dikenal
  - **Related** : paket membuka koneksi baru tetapi memiliki hubungan dengan koneksi yang sudah diketahui
  - **Invalid** : paket tidak termasuk koneksi yang diketahui.

FIREWALL – CONNECTION TRACKING

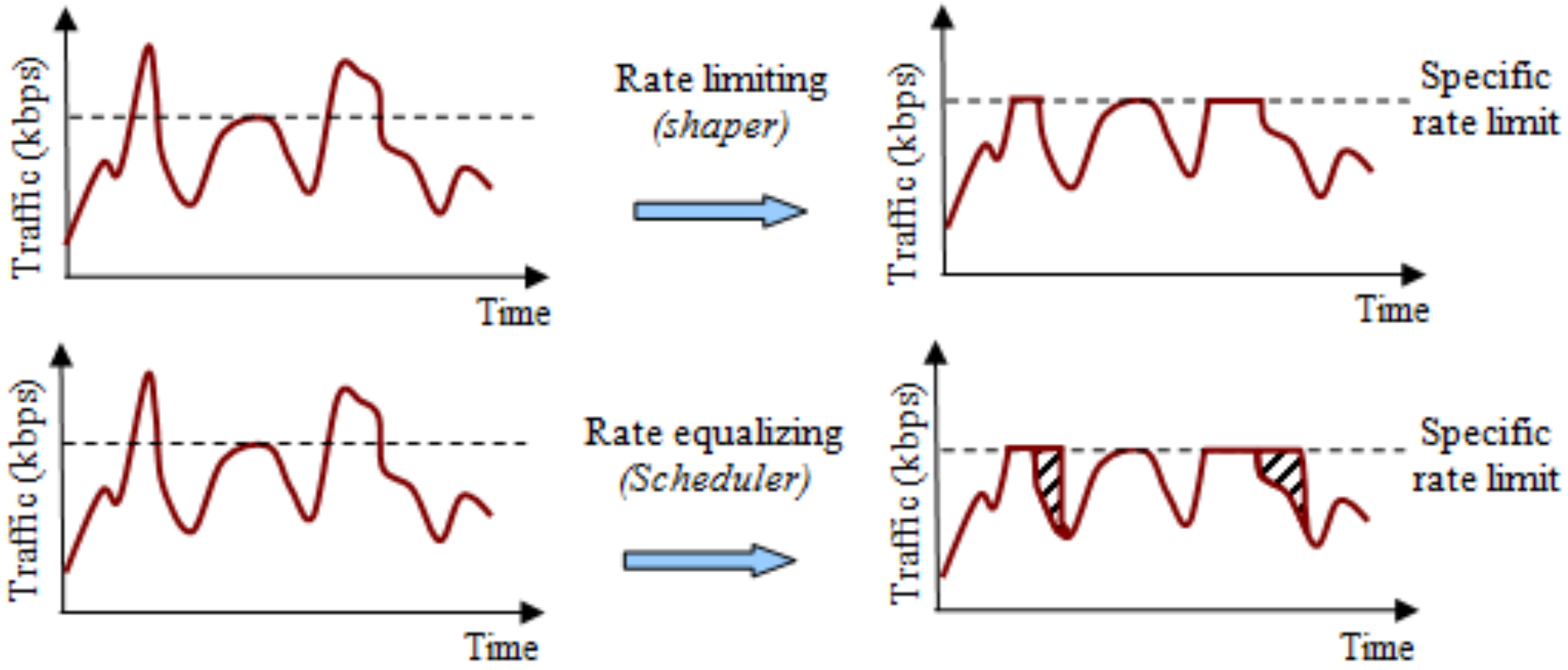


MODUL 7
QOS

QOS

- Quality of Service merupakan mekanisme pengaturan bandwidth dengan tujuan mencegah terjadinya monopoli penggunaan sehingga semua client mendapat jatah bandwidth yang sesuai.
- Managemen bandwidth di RouterOS dapat dilakukan melalui :
- Simple queue (pengaturan bandwidth secara simple)
  - Single client upload/download
  - Limitasi p2p traffic
- Queue tree (pengaturan bandwidth tingkat lanjut)
  - Global prioritization policy
  - User group limitation
  - Membutuhkan settingan mangle untuk menandai paket.

QOS – RATE LIMITATION



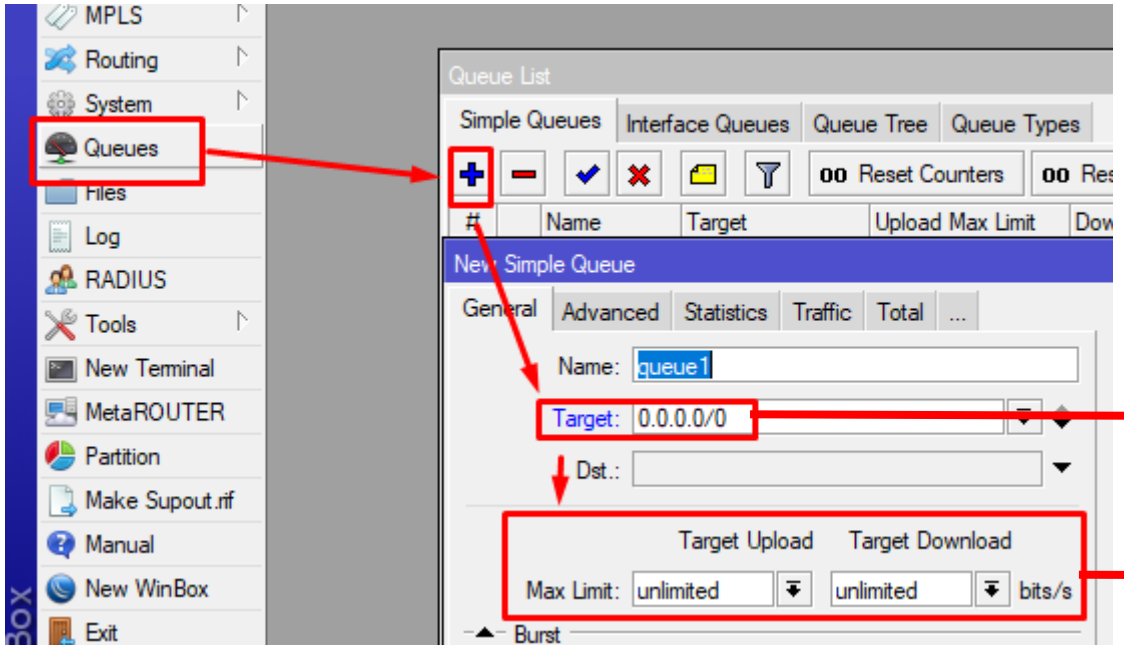
QOS – RATE LIMITATION

- Pada RouterOS, dikenal 2 jenis Batasan rate limit :
- CIR (Committed Information Rate)
  - Limit-at
  - Pada keadaan terburuk, client akan mendapatkan bandwidth sesuai dengan limit-at. (asumsi bandwidth yang tersedia cukup untuk semua client).

- MIR (Maximum Information Rate)
  - Max-limit
  - Sisa bandiwdht yang diberikan ketika semua client sudah mencapai “limit-at”, maka client bisa mendapatkan bandwidth tambahan hingga “max-limit”.

QOS – SIMPLE QUEUE

- Pembagian bandwidth yang paling sederhana pada RouterOS
- Simple queue mendefinisikan parameter address (target address) dari host/koneksi yang dilimit.



- Target address bisa berupa spesifik client/host, alamat server, network, interface
- Total = Upload + Download

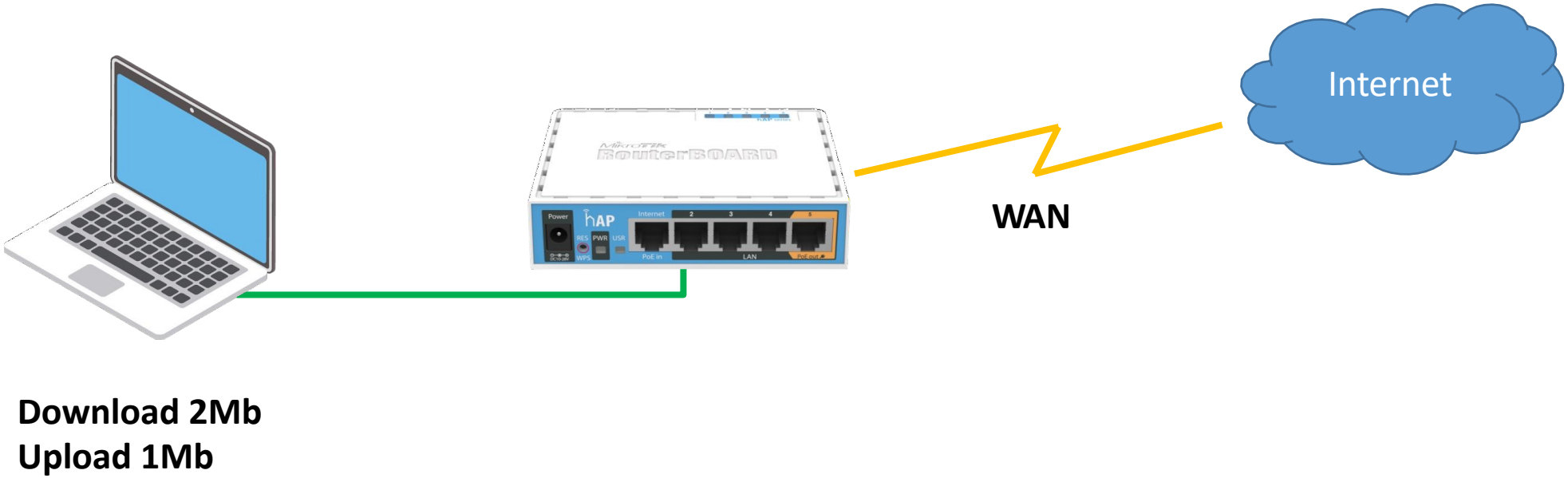
Target address yang akan di limit

Target upload dan download

QOS – SIMPLE QUEUE (1)

LAB

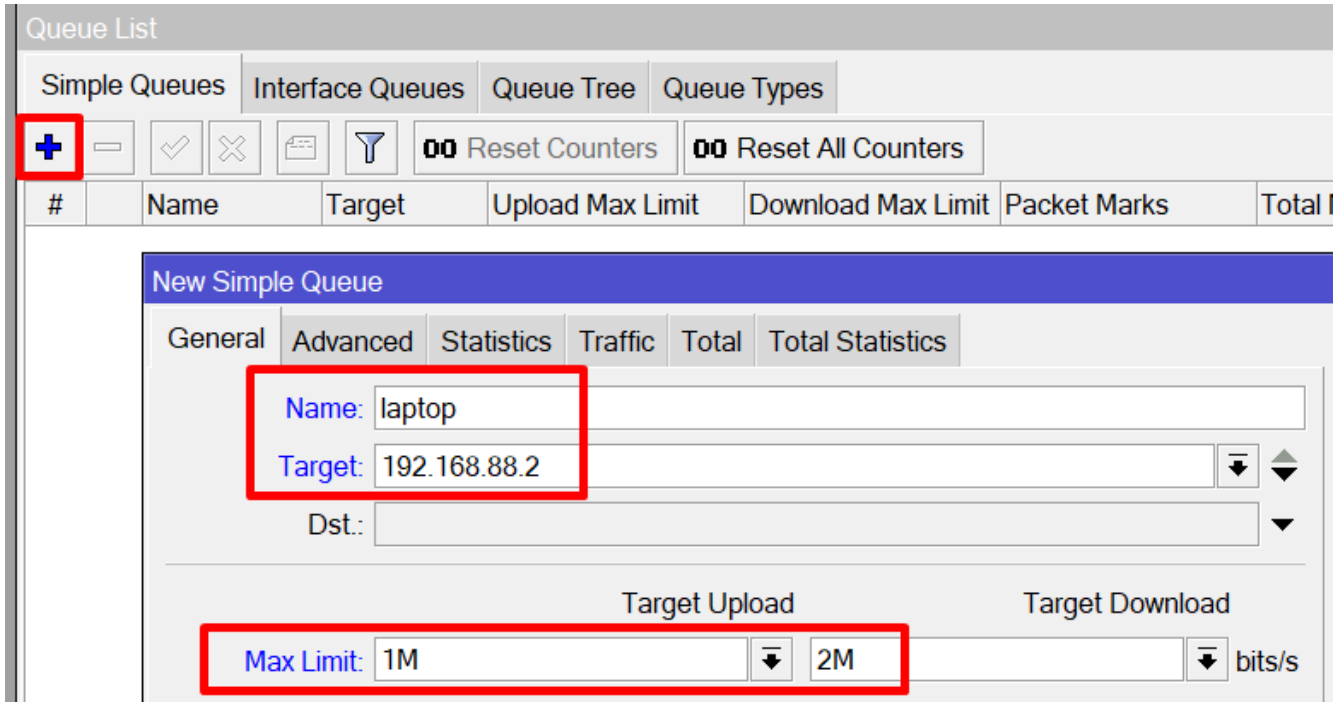
- Limit bandwidth laptop dengan ketentuan sebagai berikut:
  - Download =2MB
  - Upload =2MB
- Lakukan speedtest dari laptop dan amati.



QOS – SIMPLE QUEUE (2)

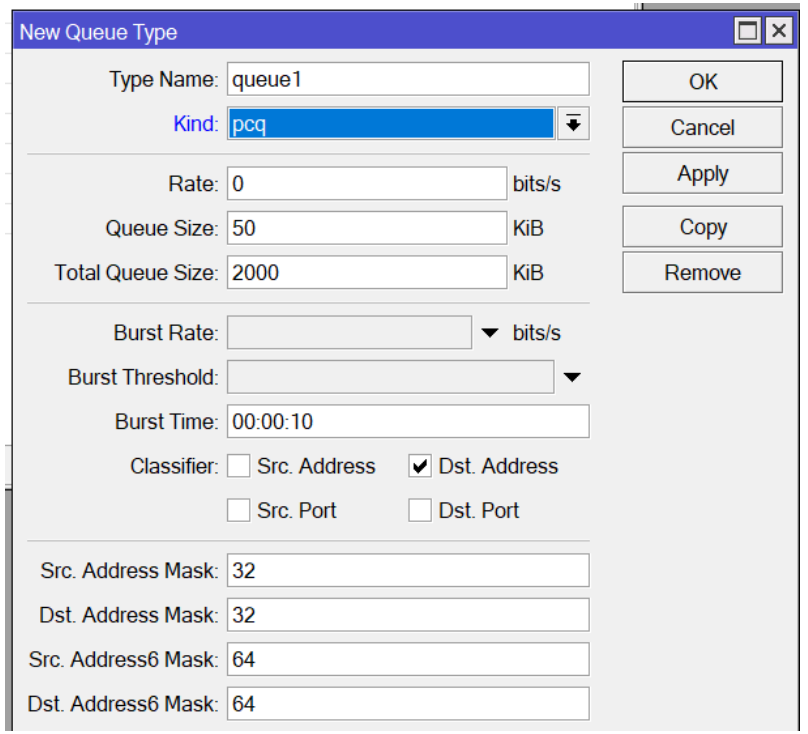
LAB

- Limit bandwidth laptop dengan ketentuan sebagai berikut:
  - Download =2MB
  - Upload =1MB



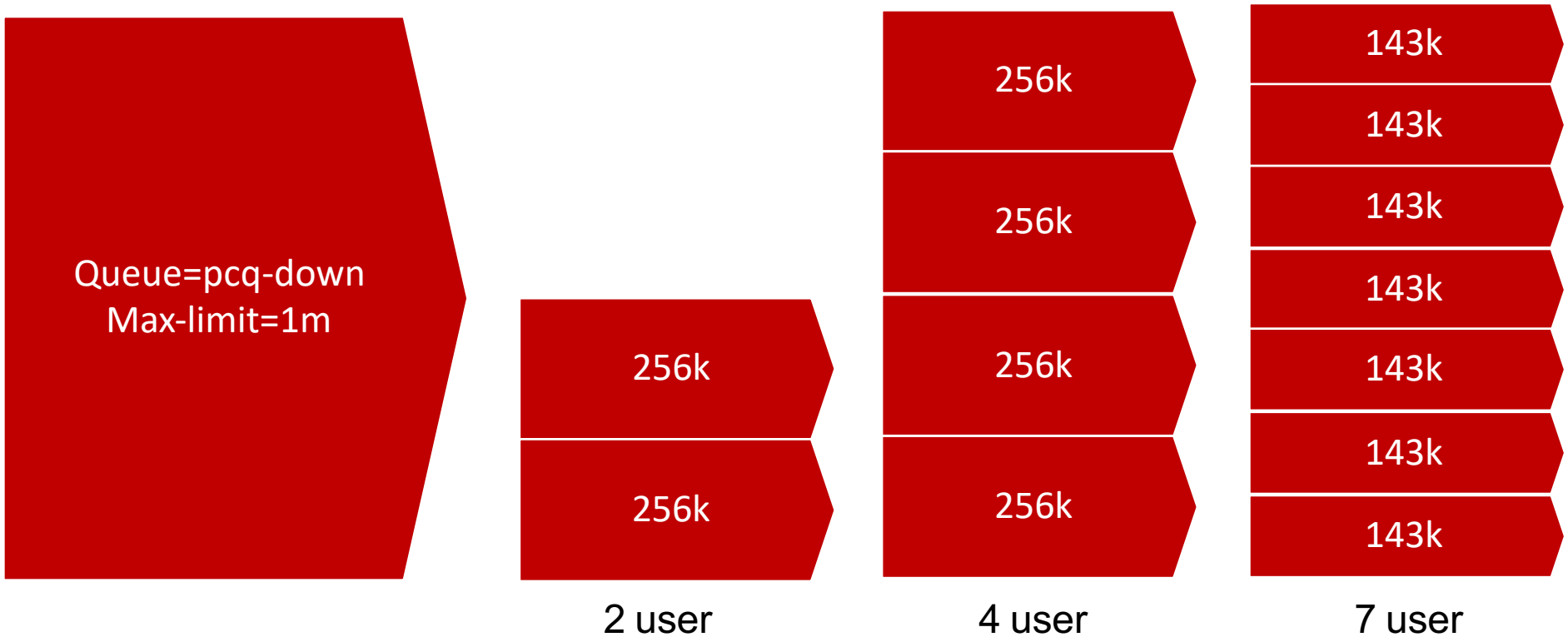
QOS–PCQ

- Dimungkinkan untuk melakukan pembagian bandwidth rata menggunakan PCQ.
- Dengan PCQ dapat membatasi maksimal data rate untuk setiap sub-queue dan jumlah paket data (pcq limit)
- Beberapa klasifikasi yang digunakan:
  - Source/destination address
  - Source/destination port



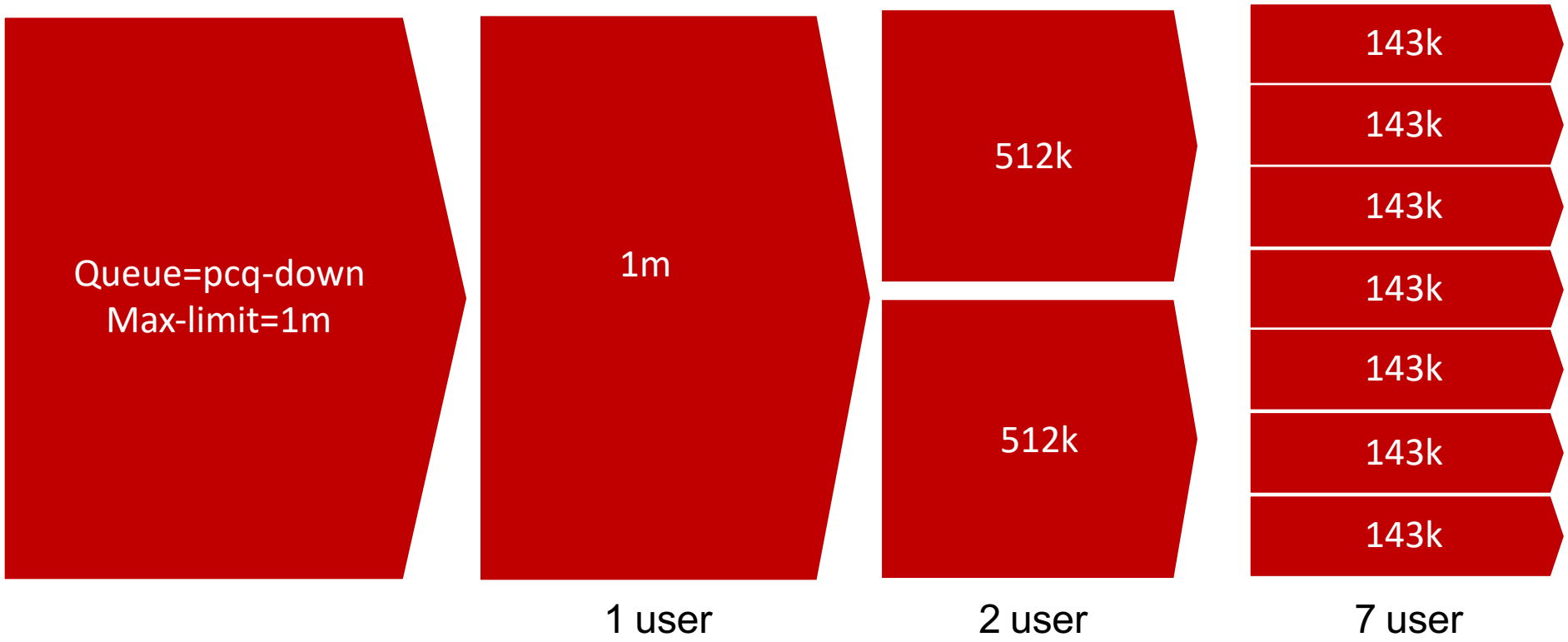
QOS–PCQ

- PCQ Rate = 256k



QOS–PCQ

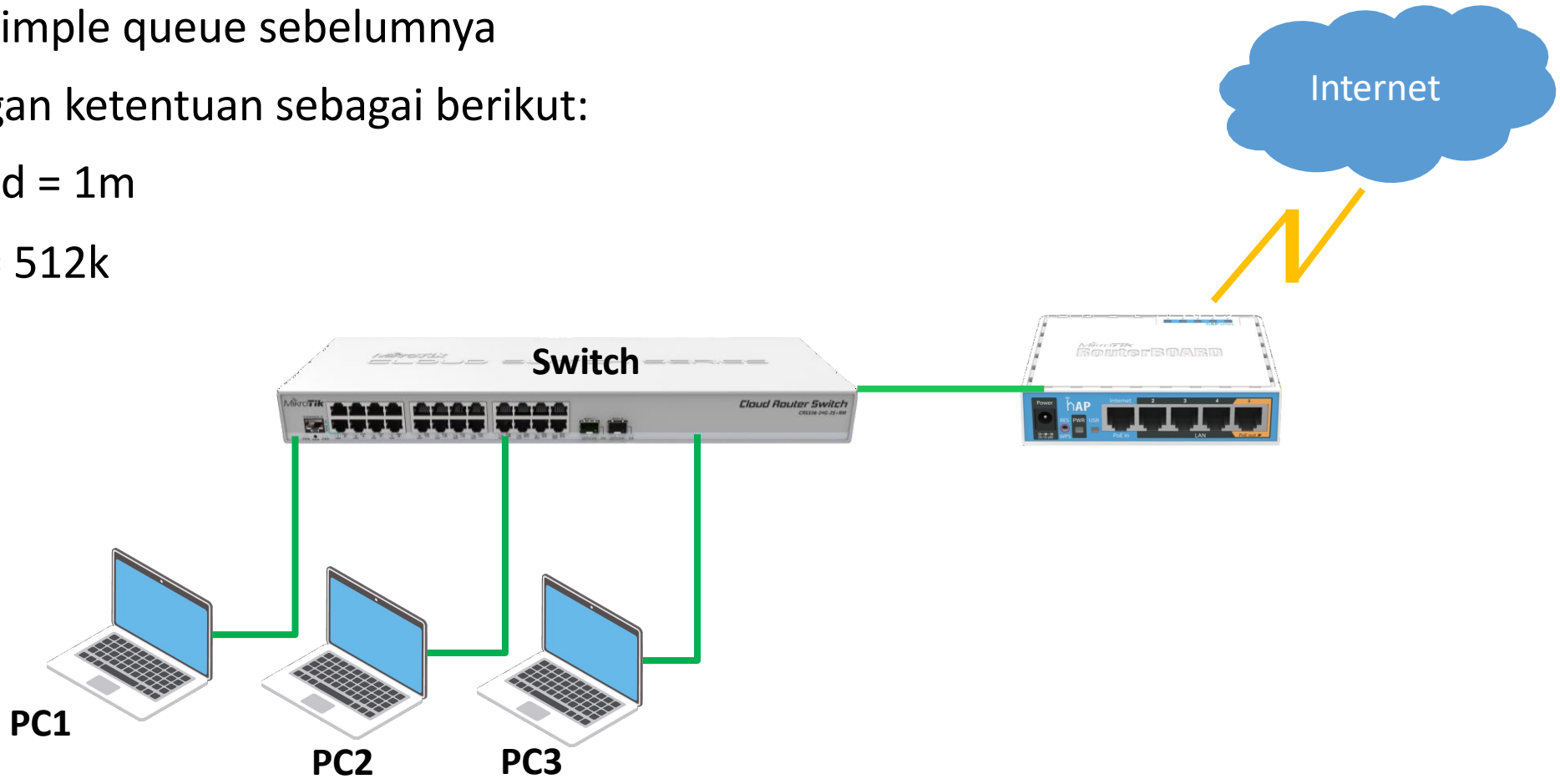
- PCQ Rate = 0



QOS–PCQ

LAB

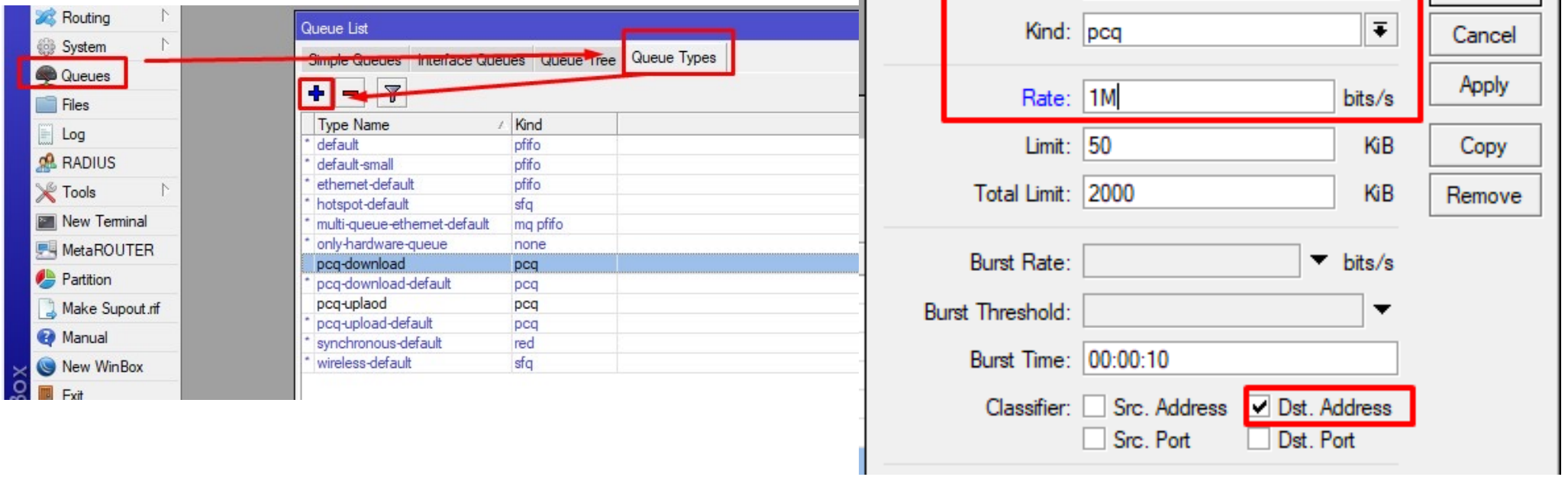
- Melanjutkan lab simple queue sebelumnya
- Buatlah PCQ dengan ketentuan sebagai berikut:
  - PCQ Download = 1m
  - PCQ Upload = 512k
  - Rate = 0
  - Rate = 512



QOS – PCQ (2)

LAB

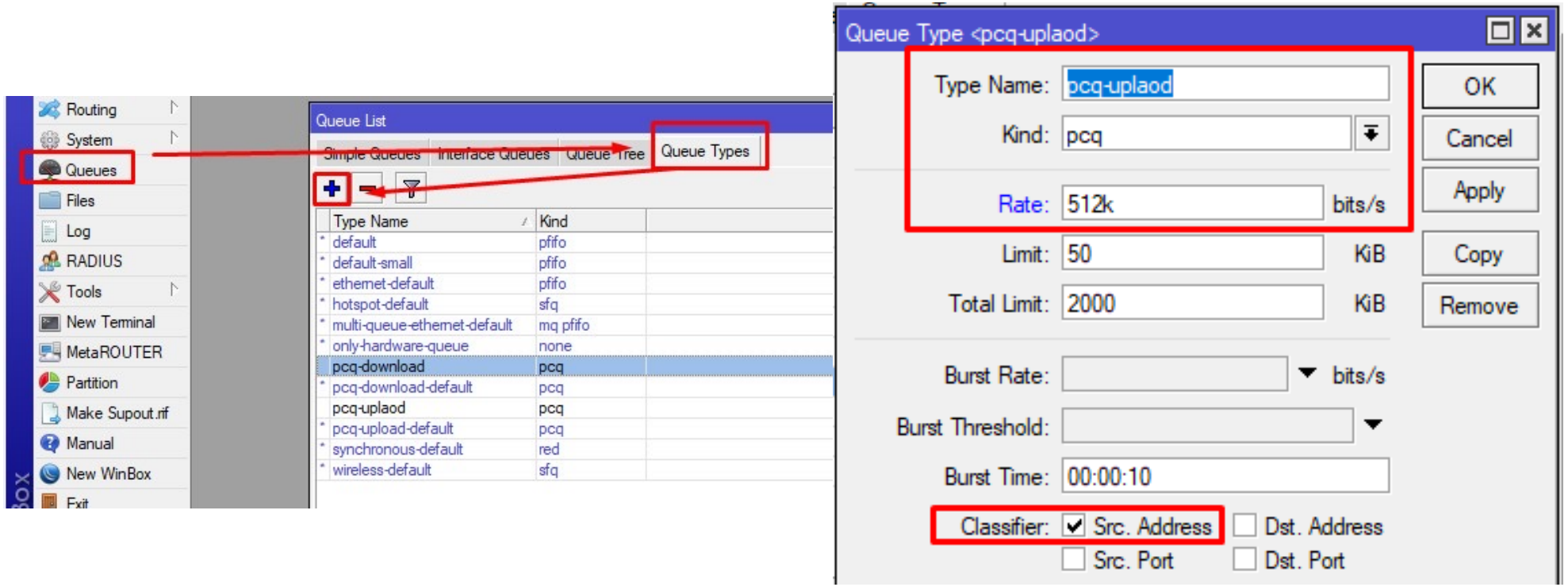
- PCQ Download
- Queue > Queue Types > add



QOS – PCQ (3)

LAB

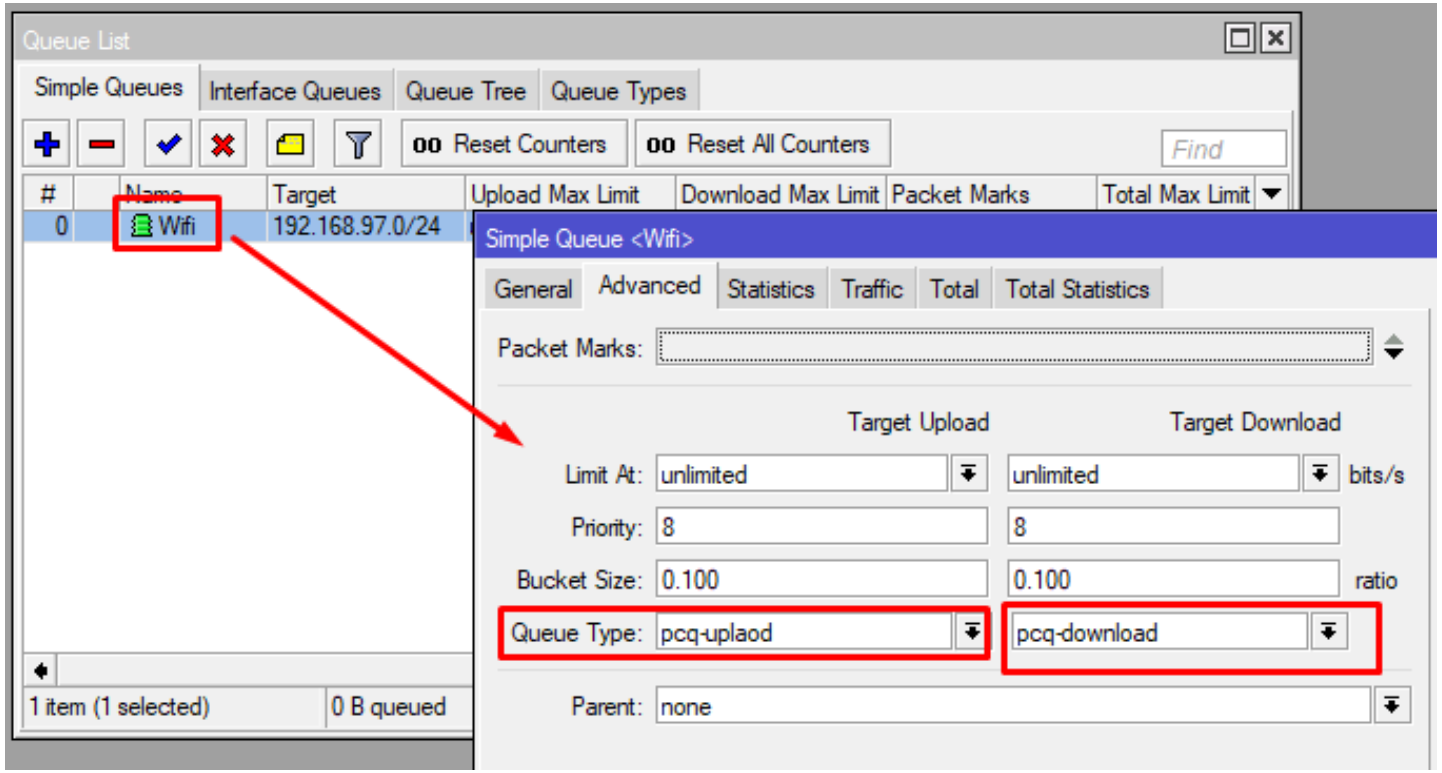
- PCQ Upload
- Queue > Queue Types > add



QOS–PCQ(4)

LAB

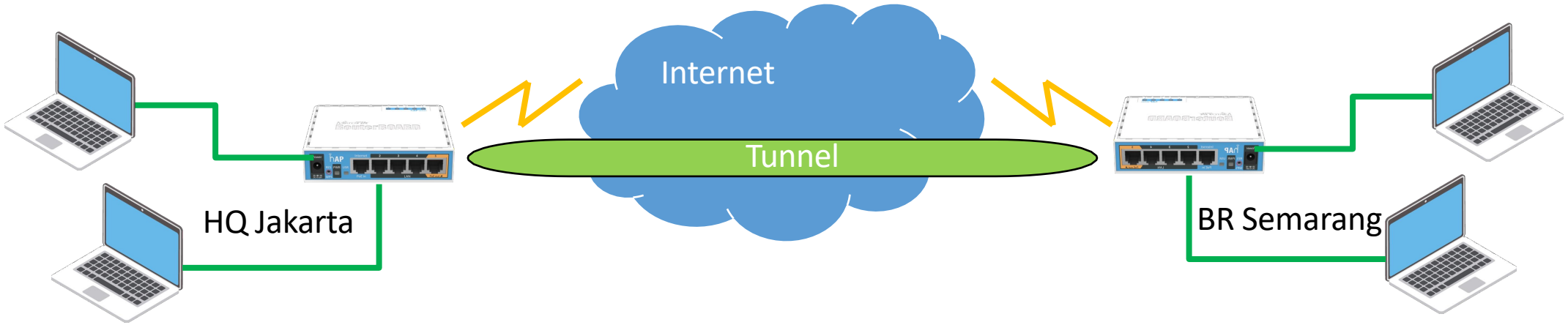
- Simple Queue Advanced



MODUL 8
TUNNEL

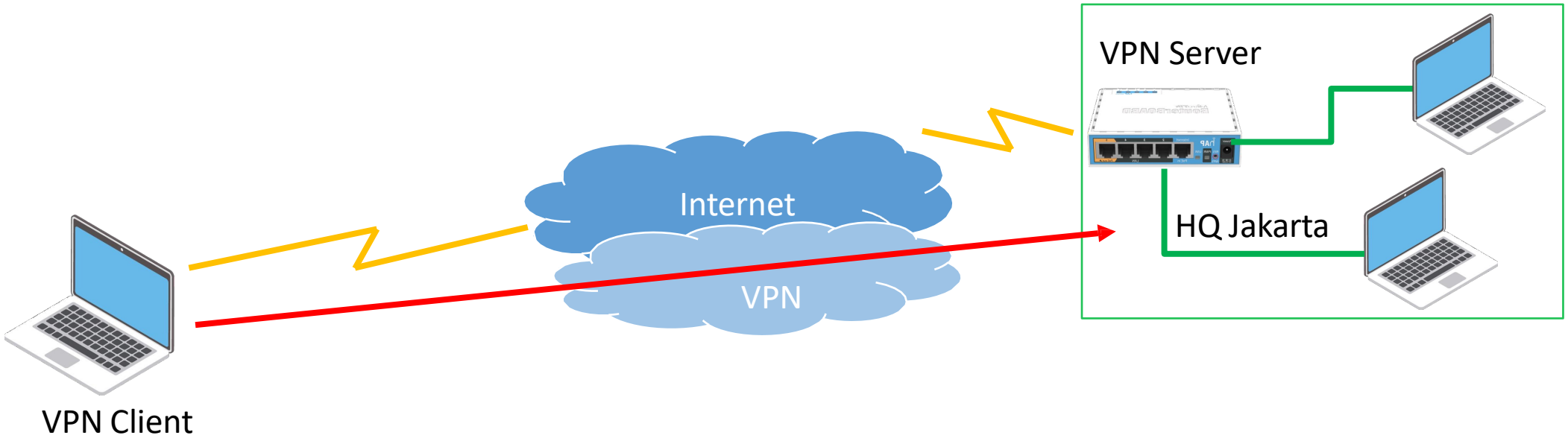
TUNNEL

- Tunnel merupakan metode menghubungkan jaringan yang berbeda lokasi menggunakan sebuah jalur khusus di internet.
- Paket akan mengalamai modifikasi atau perubahan (penambahan header) selama paket dikirimkan.
- Ketika paket sudah melewati tunnel dan sampai tujuan, maka header paket akan dikembalikan seperti semula (header dilepas).



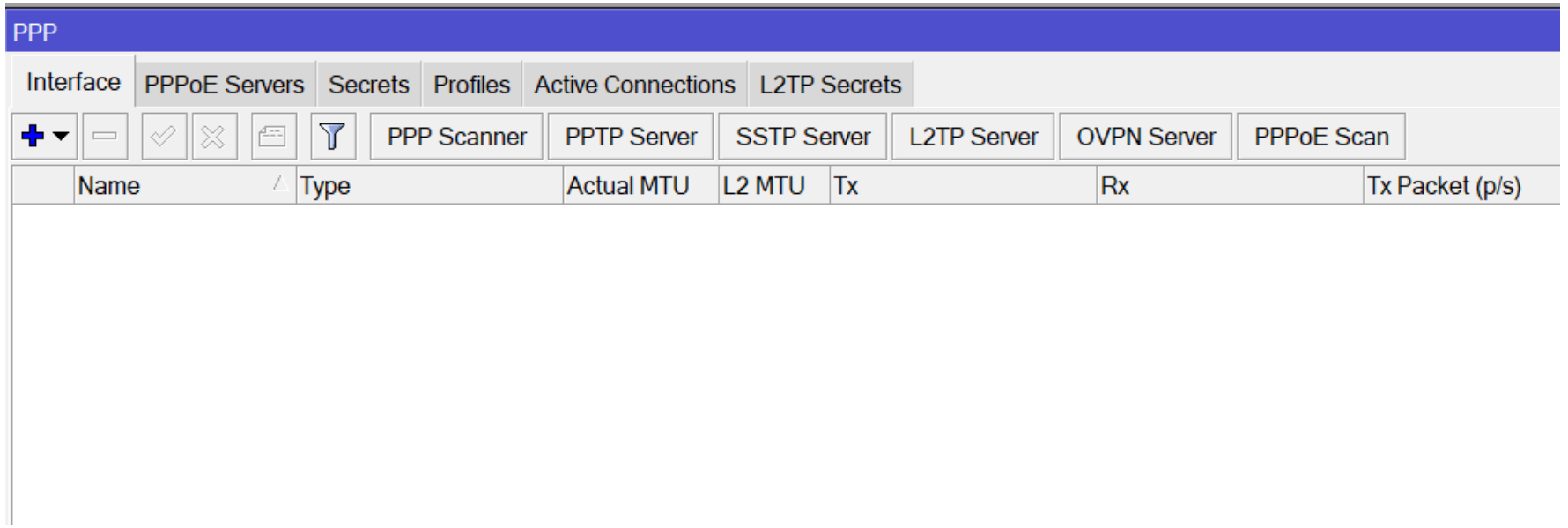
VPN

- VPN (Virtual Private Network) cara aman untuk mengakses jaringan LAN melalui internet dengan tunnel.
- VPN terbentuk dari beberapa tunnel yang digabung.



POINT-TO-POINT PROTOCOL

- Point to Point Protocol (PPP) digunakan untuk membangun tunnel (koneksi langsung) antara dua lokasi yang berbeda melalui internet.
- PPP dapat menyediakan authentikasi koneksi, ekripsi dan kompresi.
- RouterOS mendukung berbagai tunnel PPP seperti PPPoE, SSTP, PPTP dll.



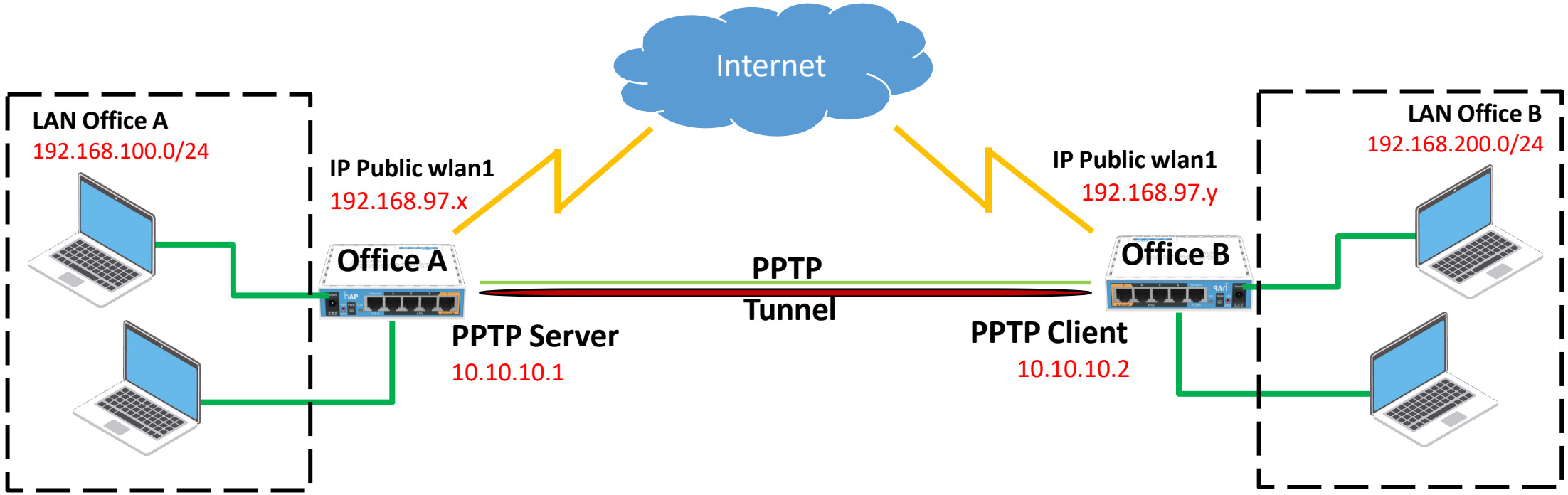
PPTP TUNNELING

- Point-to-Point Tunnelling Protocol (PPTP) merupakan salah satu tunnel yang menyediakan enkripsi melalui IP.
- Merupakan tunnel yang banyak digunakan karena hamper semua OS support PPTP client.
- Dapat digunakan untuk membuat koneksi aman antara jaringan local melalui internet.
- RouterOS mendukung PPTP client dan PPTP Server.
- PPTP menggunakan port TCP 1723 dan IP protocol 47 GRE (Generic Routing Encapsulation).
- NAT helpers digunakan untuk mendukung PPTP dijaringan NAT.

PPTP SITE TO SITE (MIKROTIK – MIKROTIK)

LAB

- Buatlah topologi seperti berikut

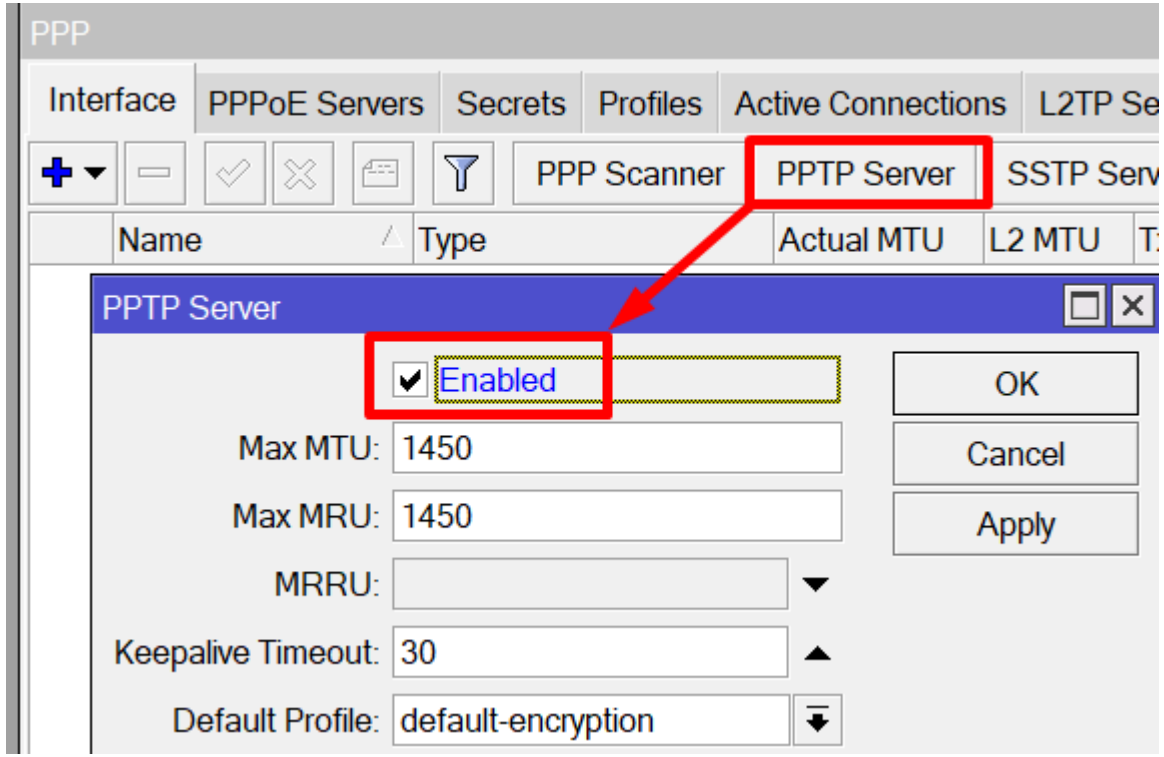


- Gunakan static route untuk menghubungkan antar client

PPTP SERVER

LAB

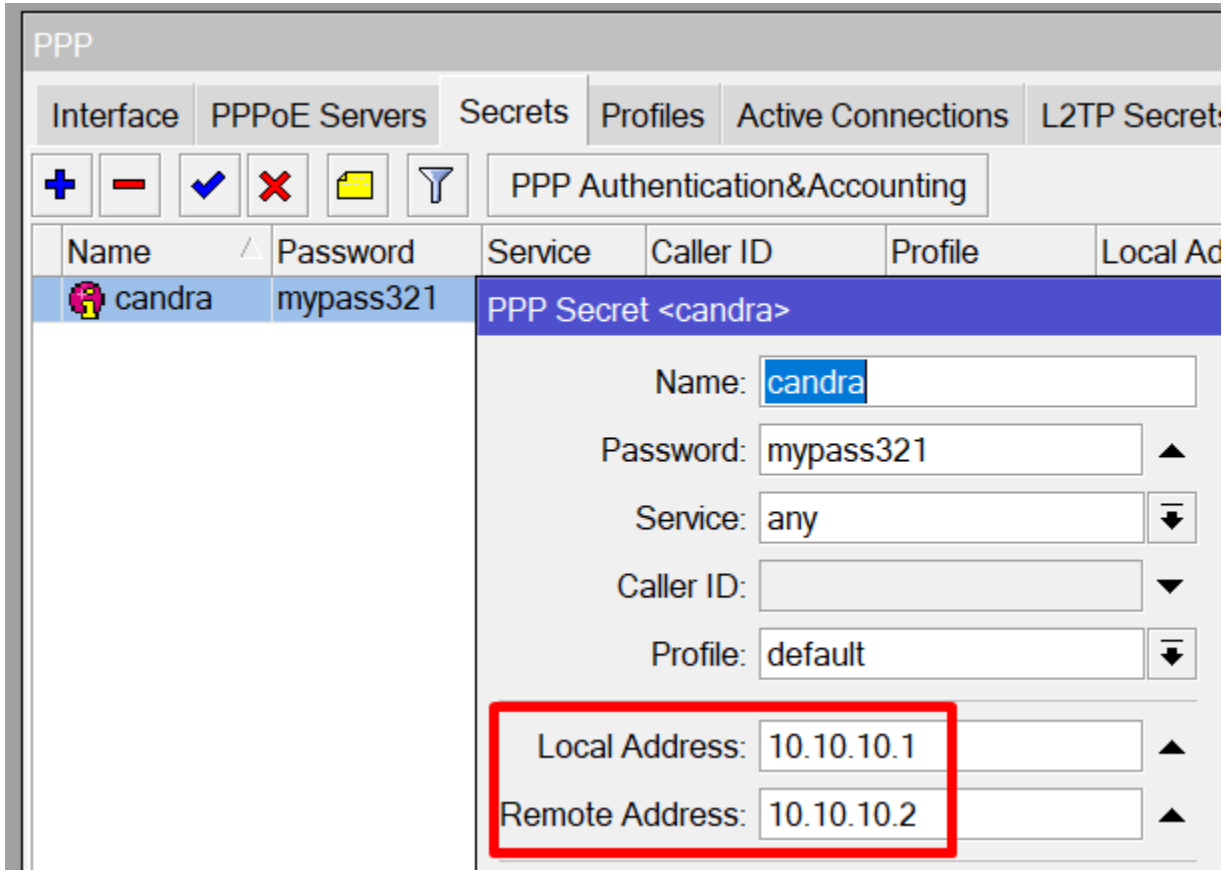
- Untuk mengaktifkan PPTP sebagai server, yang harus dilakukan adalah enable service pada **menu PPP > Interface > PPTP Server.**



PPTP SERVER

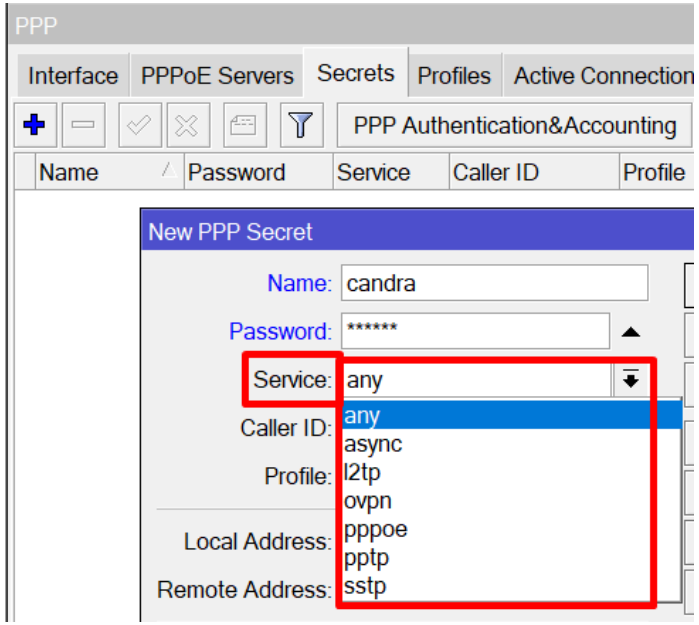
LAB

- Membuat authentikasi username dan password pada database (PPP Secret)



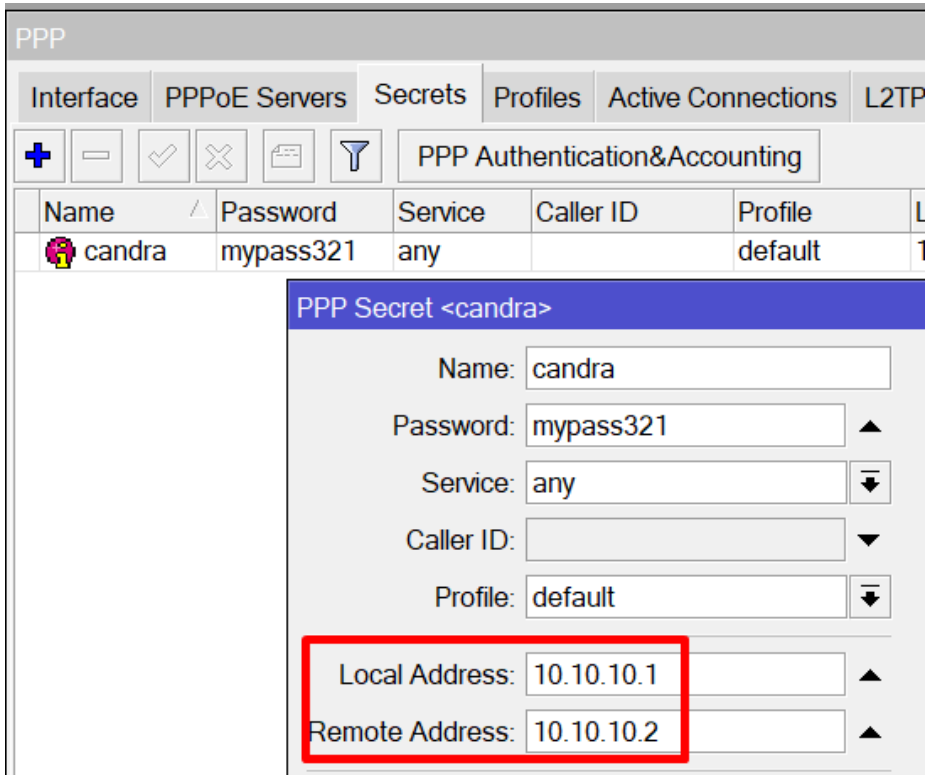
PPP USER DATABASE

- Digunakan sebagai authentikasi username password di Tunnel.
- By default username password tunnel di simpan di menu PPP > Secret
- Selain itu juga dapat disimpan di Radius Server terpisah.
- PPP Secret dapat digunakan untuk beberapa service seperti berikut :
  - Async
  - L2TP
  - PPTP
  - OVPN
  - PPPoE
  - SSTP



PPP SECRET

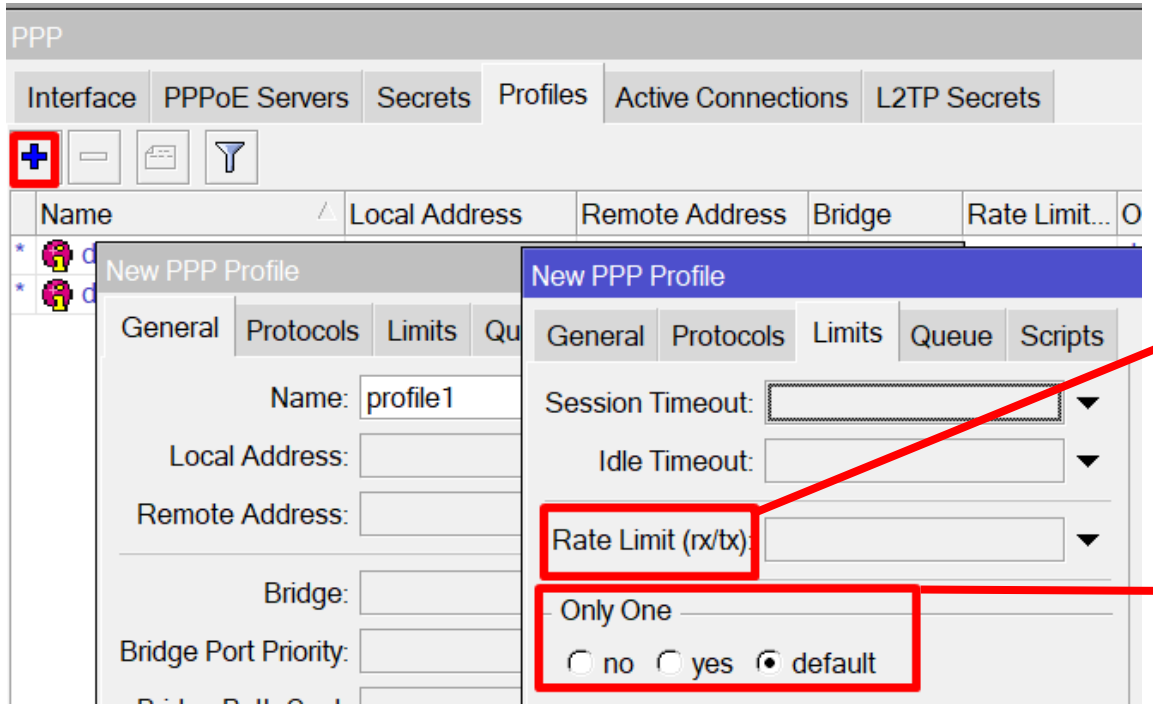
- Local Address (alamat IP tunnel server)
- Remote Address (alamat IP tunnel client)



PPP PROFILE

LAB

- PPP Profile menentukan aturan yang digunakan oleh server PPP untuk clientnya.
- Bisa digunakan untuk mengatur pengaturan yang sama untuk banyak client.



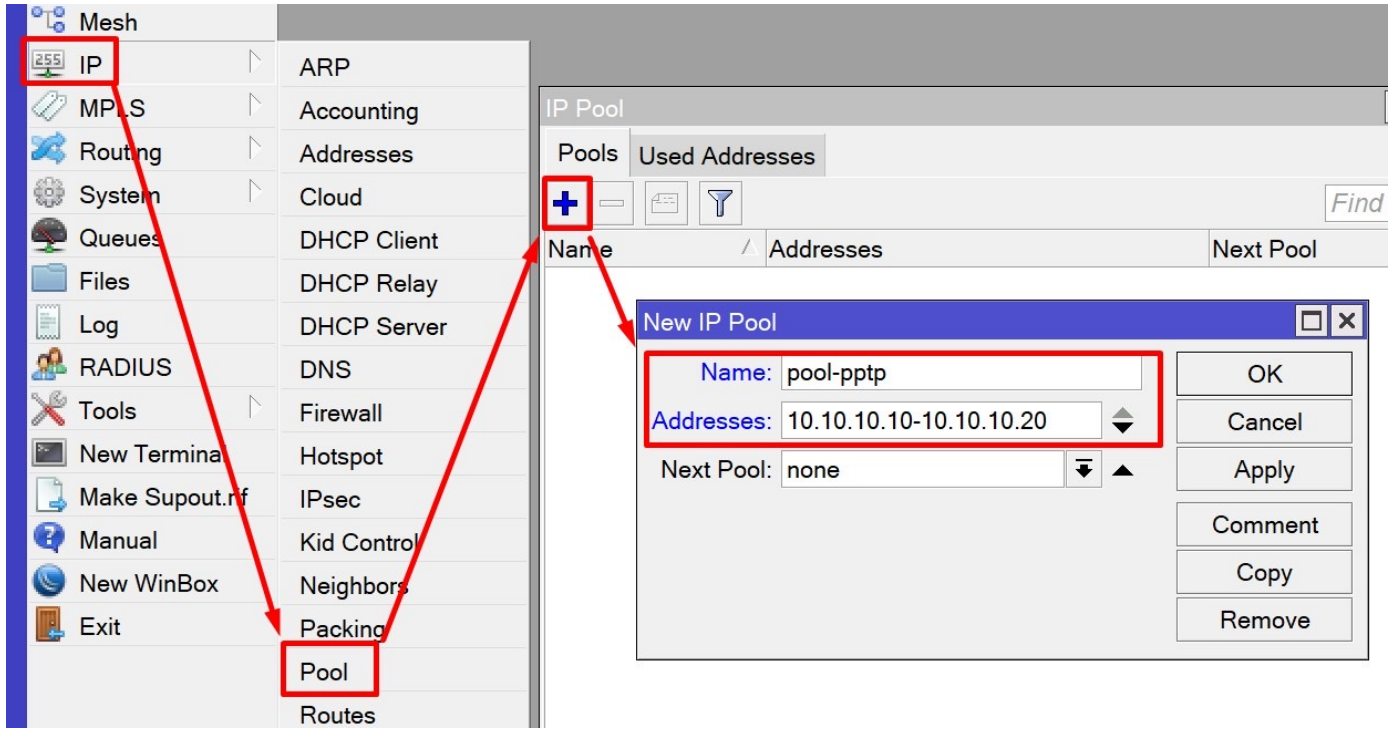
digunakan untuk membatasi bandwidth

digunakan untuk membatasi jumlah session client yang konek

IP POOL

LAB

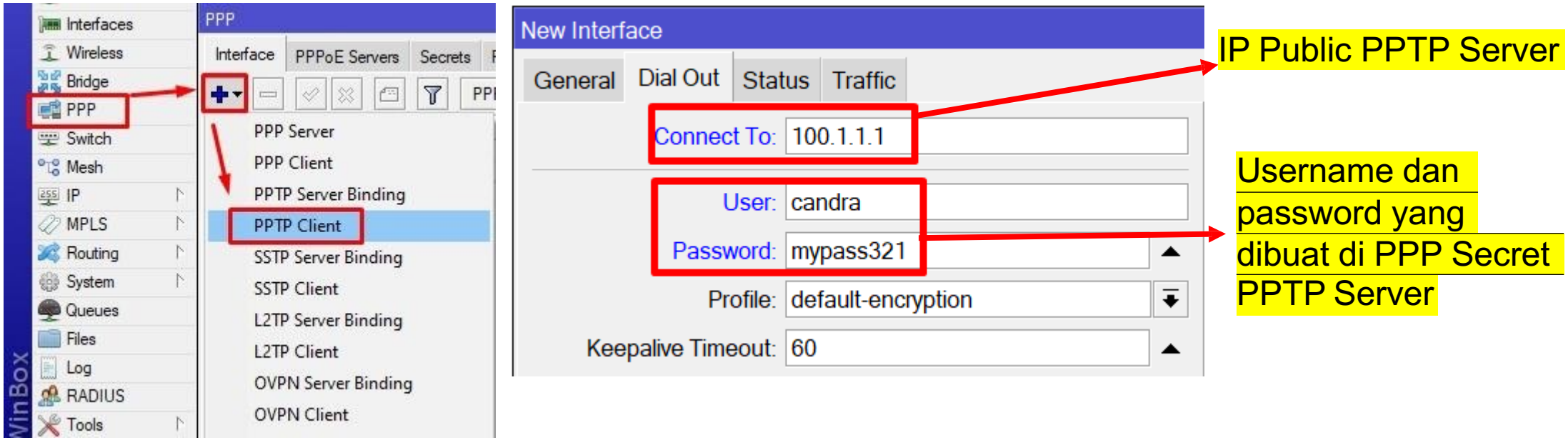
- Menentukan range alamat IP yang bisa digunakan untuk service pada RouterOS (DHCP, PPP, Hotspot, dll).
- Address diambil dari pool secara otomatis



PPTP CLIENT

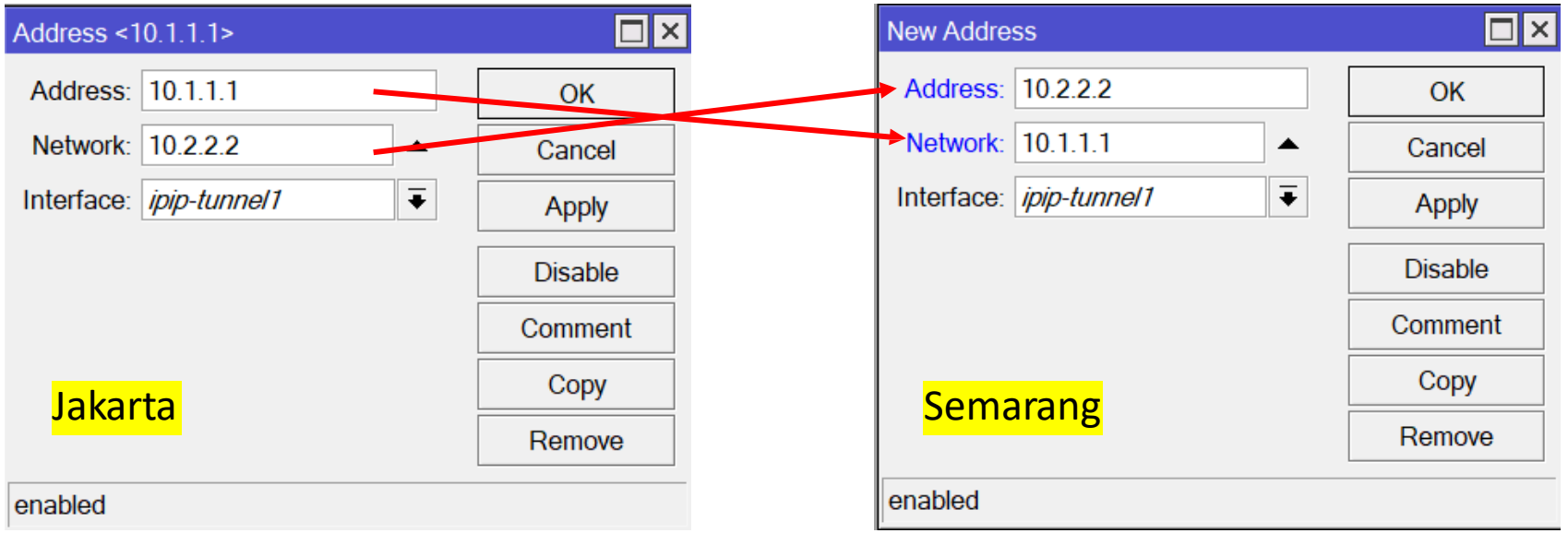
LAB

- Digunakan untuk melakukan Dial Out dari client ke server.
- Untuk pembuatan PPTP Client melalui menu **PPP > Interface > Add > PPTP Client.**



POINT-TO-POINT ADDRESSING

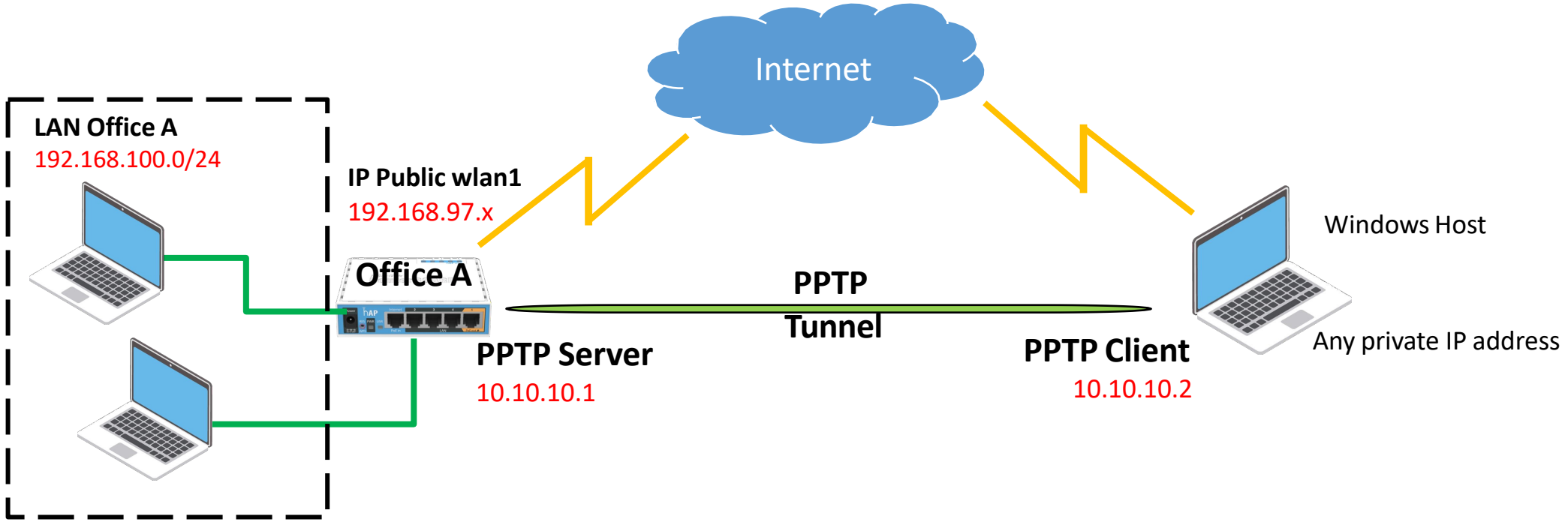
- Merupakan tipe addressing yang digunakan untuk pengalamatan di jaringan tunnel.
- Biasanya menggunakan pengalamatan IP /32, bisa menggunakan /30 sebagai alternative bila ada perangkat yang tidak support /32



PPTP VPN (MIKROTIK – WINDOWS)

LAB

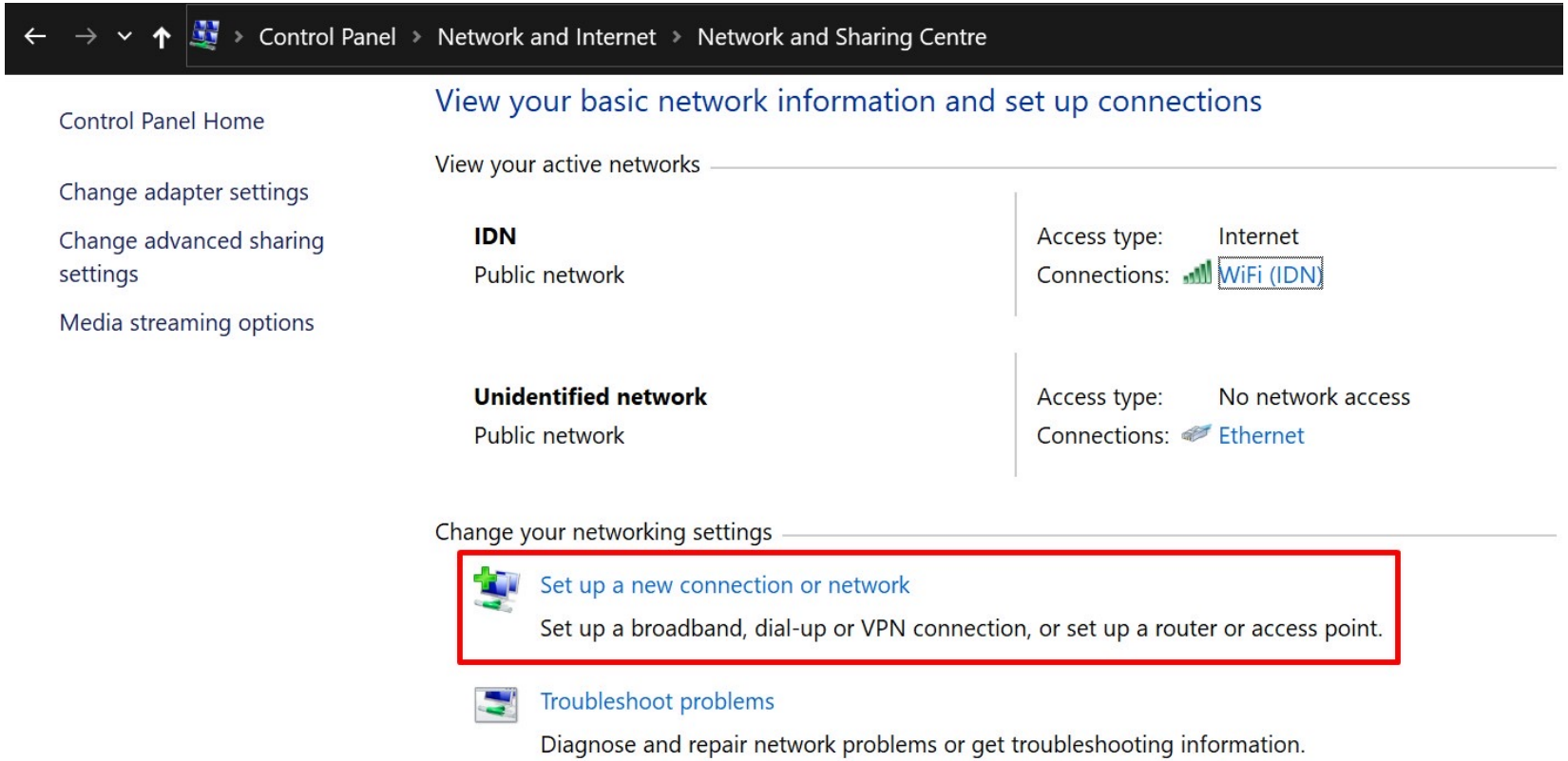
- Buatlah topologi seperti berikut



PPTP VPN (MIKROTIK – WINDOWS)

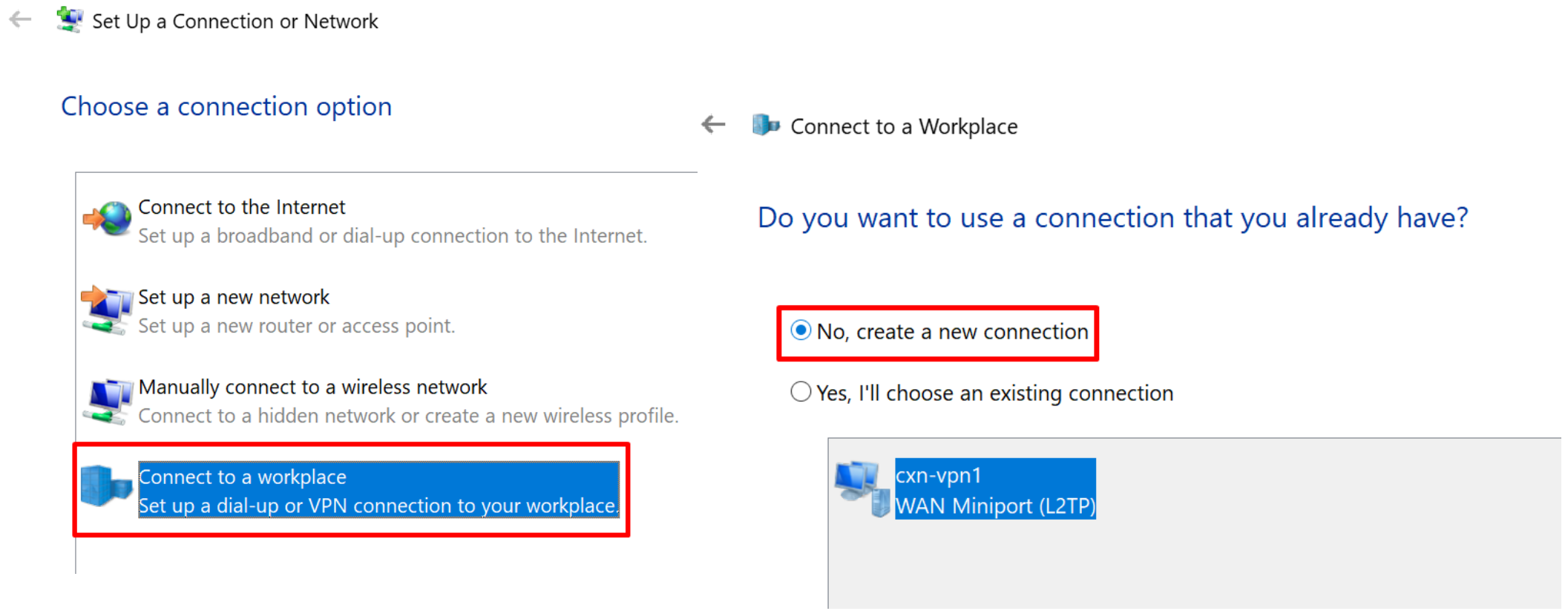
LAB

- Windows Setup



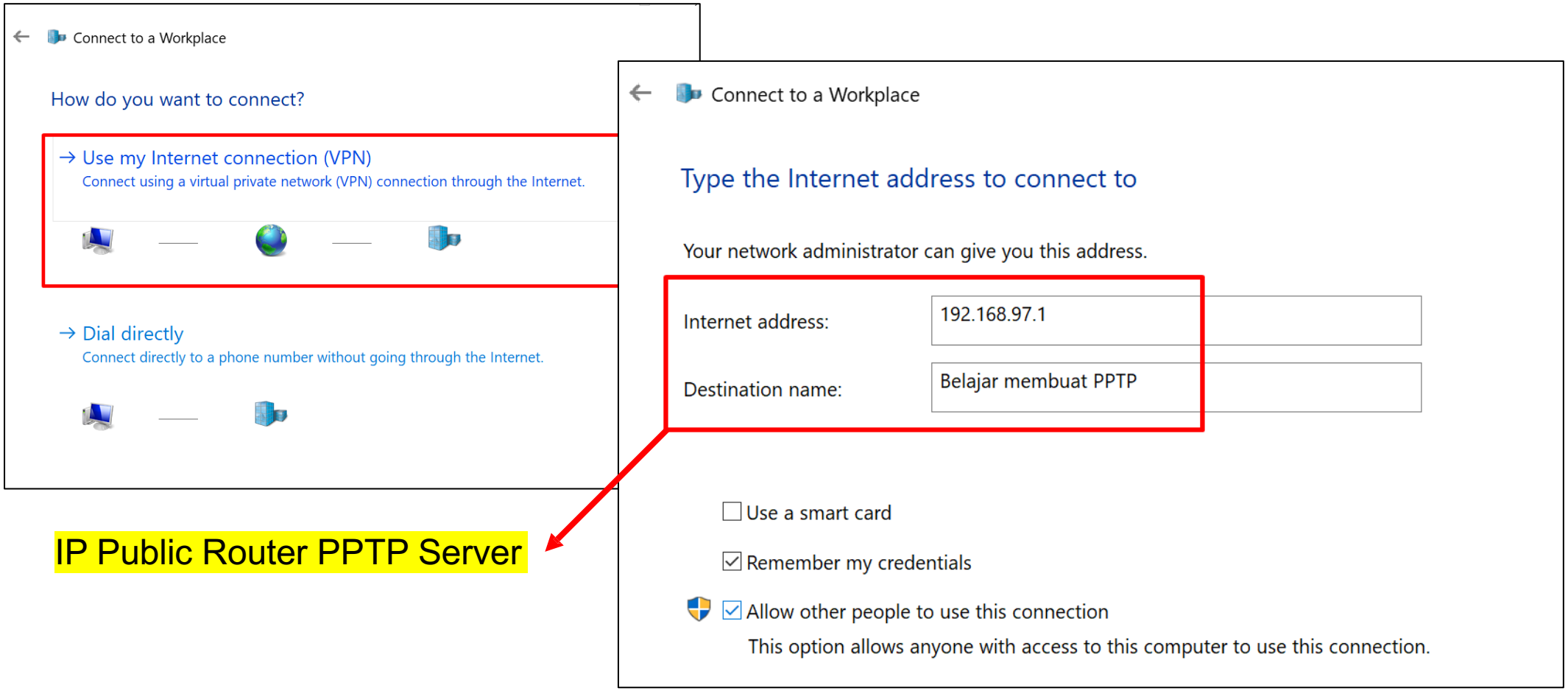
PPTP VPN (MIKROTIK – WINDOWS)

LAB



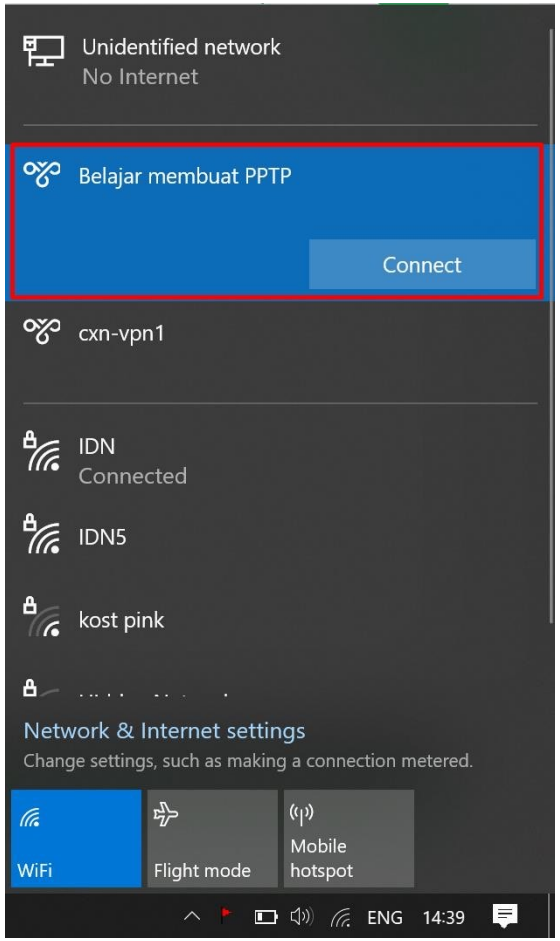
PPTP VPN (MIKROTIK – WINDOWS)

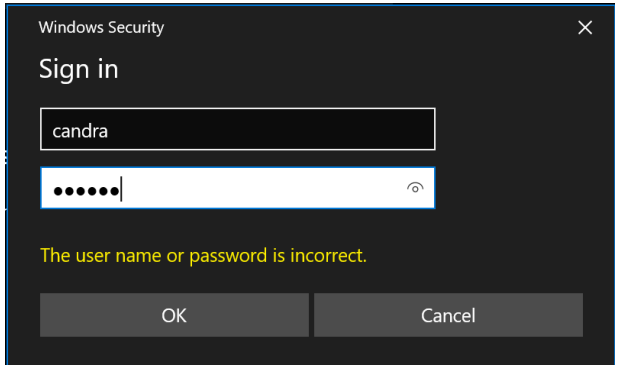
LAB



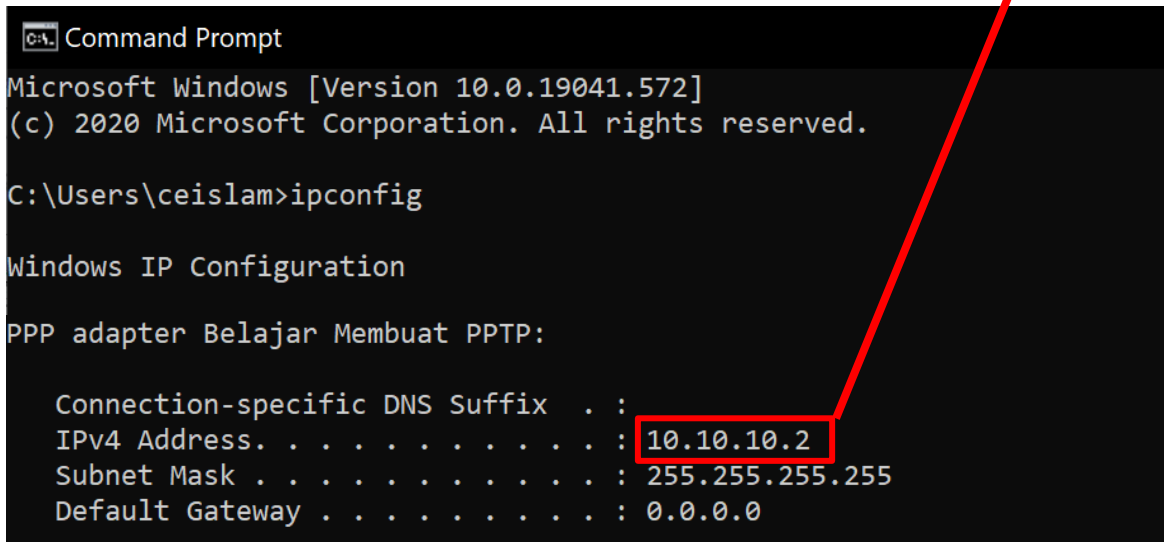
PPTP VPN (MIKROTIK – WINDOWS)

LAB



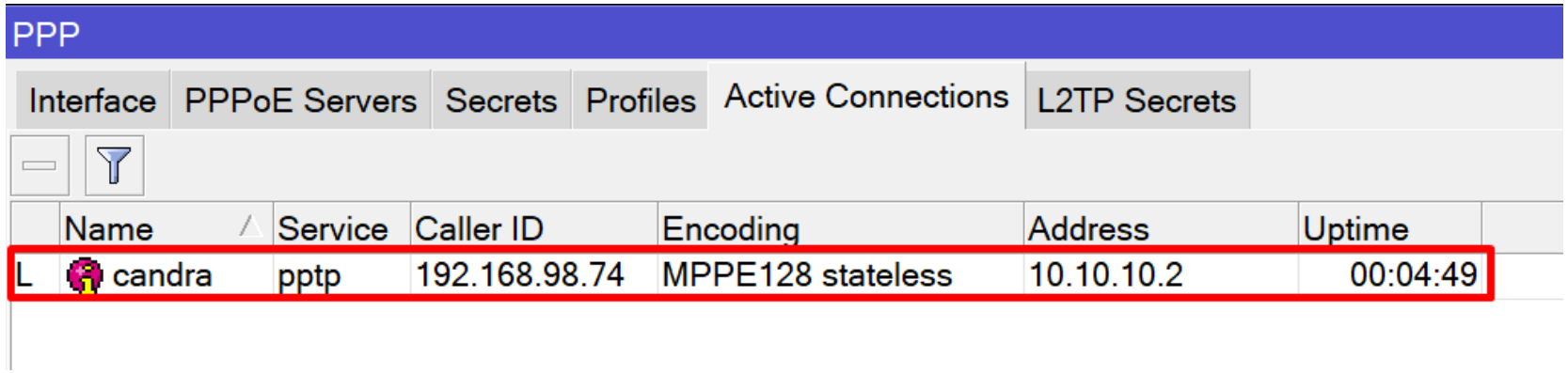


IP PPTP Client yang didapat dari remote address PPP > Secret



PPP ACTIVE CONNECTIONS

- PPP Active connections digunakan untuk melihat list session client yang sedang melakukan koneksi ke PPTP Server.
- Terdapat 2 flags :
  - **L** = Local (username dan password yang digunakan berasal dari PPP Secret).
  - **R** = Radius (username dan password yang digunakan untuk login berasal dari radius server).



SSTP

- Secure Socket Tunneling Protocol (SSTP) merupakan jenis tunnel yang menyediakan enkripsi melalui IP.
- Menggunakan port TCP 443 (sama seperti HTTPS).
- RouterOS support SSTP client dan SSTP Server
- SSTP Client mulai tersedia di Windows Vista SP1 sampai windows yang ada pada sekarang.
- SSTP dapat melewati firewall tanpa konfigurasi, karena trafficnya melalui https.

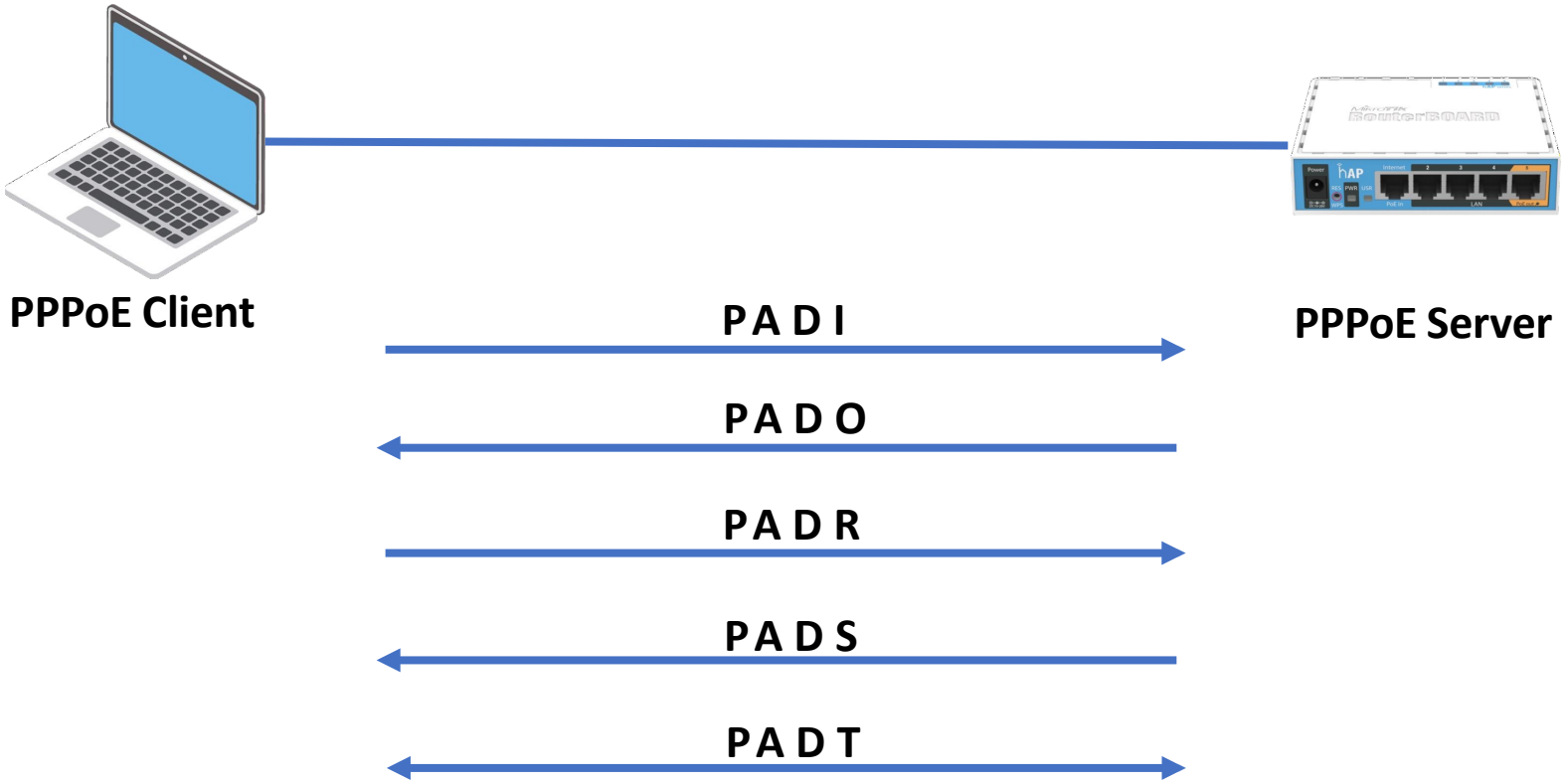
PPPOE

- Point-to-Point Protocol over Ethernet merupakan jenis protocol tunnel layer 2 yang digunakan untuk mengontrol akses ke jaringan.
- Salah satu jenis protocol tunnel yang banyak digunakan di ISP, karena dapat dengan mudah melakukan management banyak client tanpa menggunakan IP Public.
- Memberikan authentikasi, enkripsi dan kompresi.
- PPPoE hanya bekerja pada satu jaringan (one broadcast domain).

PPPOE

- PPPoE mempunyai 2 tahapan
- Discovery Stages
  - Sebelum konek ke server, client akan melakukan pencarian dengan cara melakukan discovery stage untuk membuat sebuah koneksi yang established.
- Session
  - Kondisi dimana PPPoE client sudah terkoneksi ke server (established).

PPPOE DISCOVERY STAGES



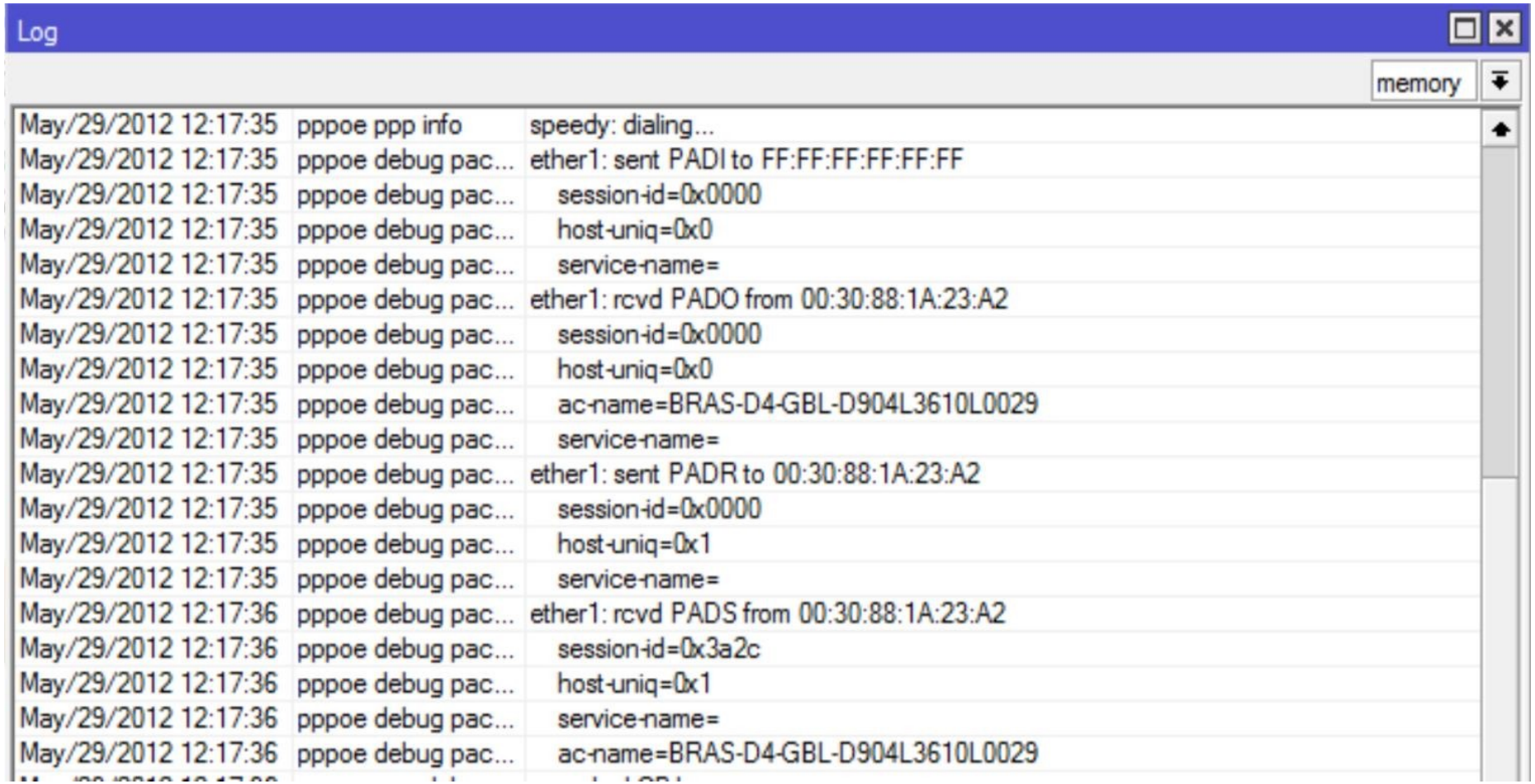
PPPOE DISCOVERY STAGES

- PADI (PPP Active Discovery Initiation), PPPoE Client mengirimkan paket broadcast ke jaringan dengan alamat pengiriman MAC Address FF:FF:FF:FF:FF:FF:FF:FF untuk mencari di mana lokasi PPPoE server dalam jaringan.
- PADO (PPP Active Discovery Offer). Merupakan jawaban dari PPPoE Server atas PADI yang didapatkan sebelumnya, dengan memberikan identitas berupa MAC Addressnya.
- PADR (PPP Active Discovery Request), merupakan informasi dari PPPoE client ke server dengan menghubungi ulang server melalui MAC address yang diberikan sebelumnya.

PPPOE DISCOVERY STAGES

- PADS (PPP Active Discovery Session-confirmation) dari PPPoE Server ke Client, isinya mengenai session ID dan pada tahap ini akan terjadi negosiasi username, password dan IP address.
- PADT (PPP Active Discovery Terminate) digunakan untuk mengakhiri session. Bisa dikirim dari Server atau dari Client.

PPPOE DISCOVERY STAGES

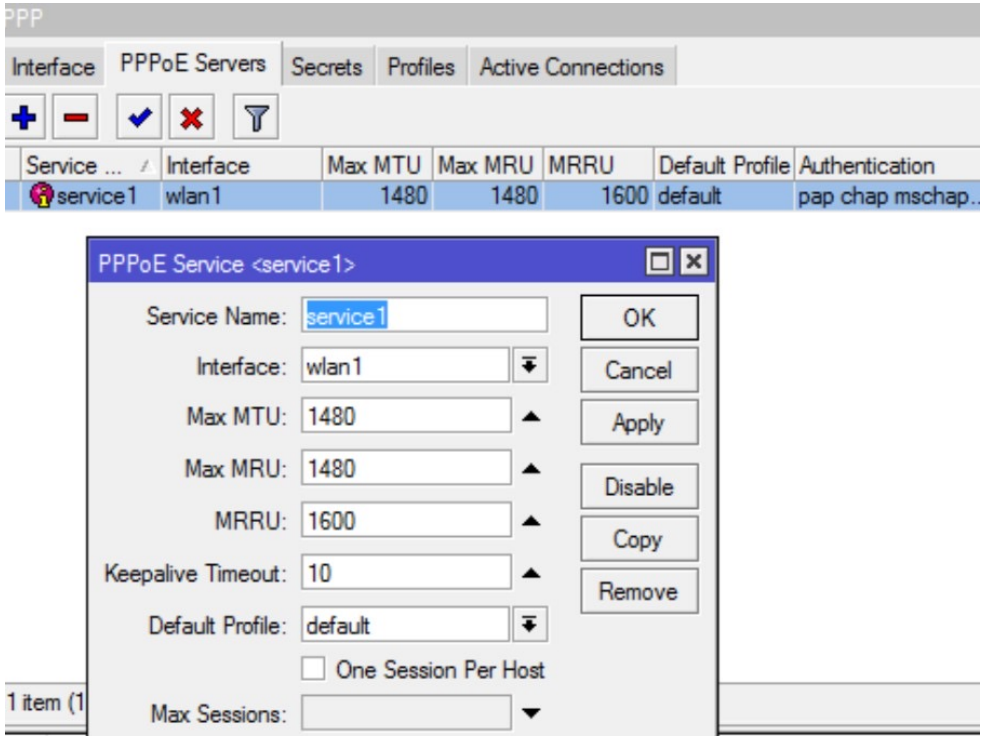


PPPOE SESSION STAGE

- LCP Negotiation
- Authentication
- IPCP Negotiation (Pembagian IP address ke client)

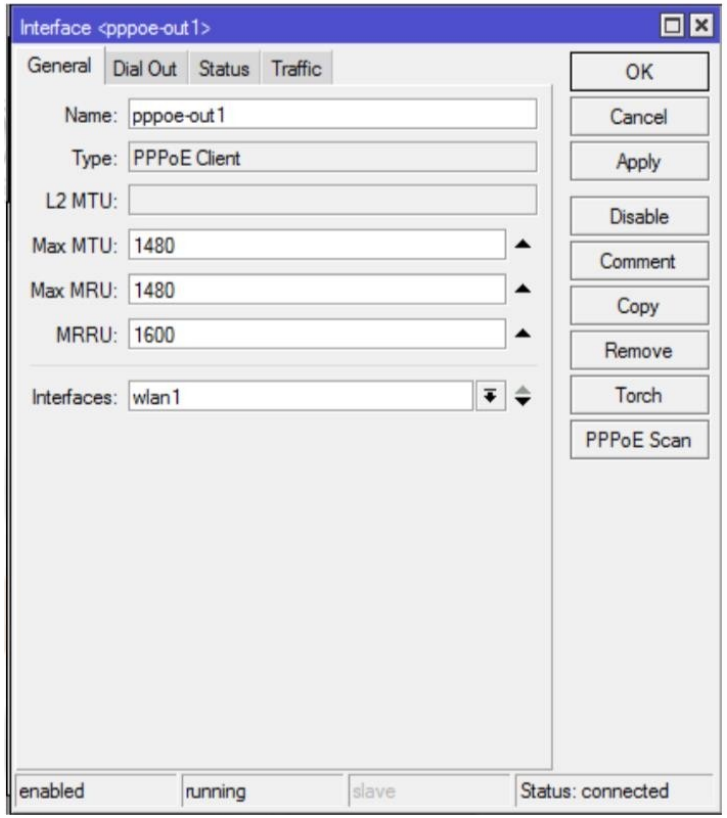
PPPOE SERVER

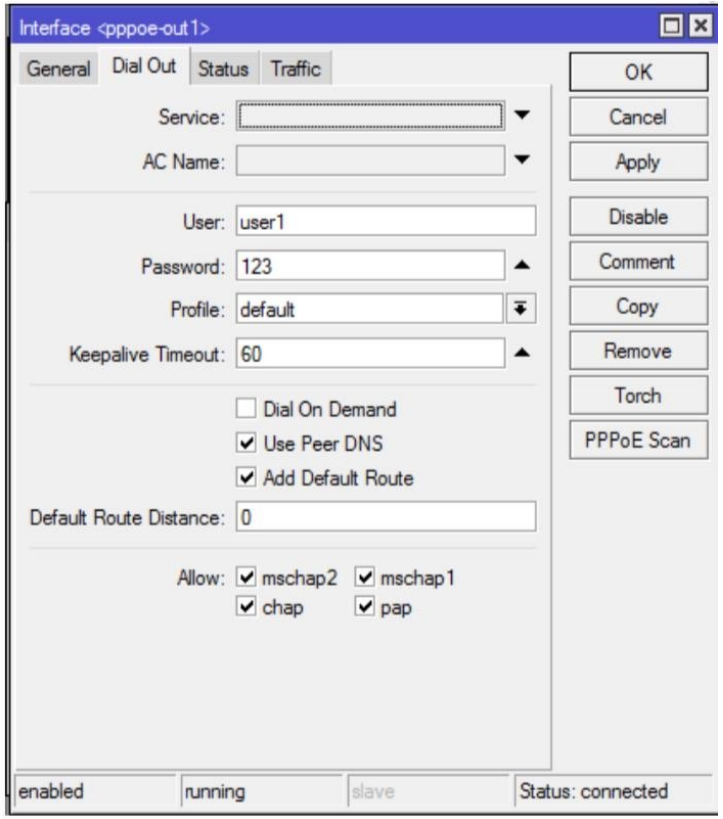
- PPPoE Server support beberapa type interface.
- Tidak bisa dikonfigurasikan pada interface yang merupakan bagian dari bridge



PPPOE CLIENT

- PPPoE Client digunakan untuk melakukan dial out PPPoE Server

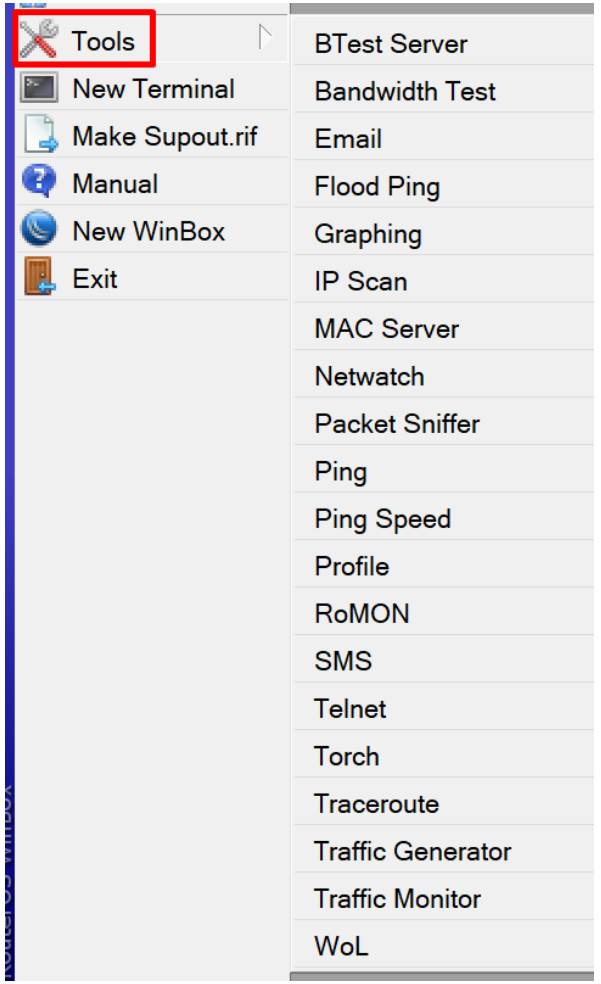




MODUL 9
MISC

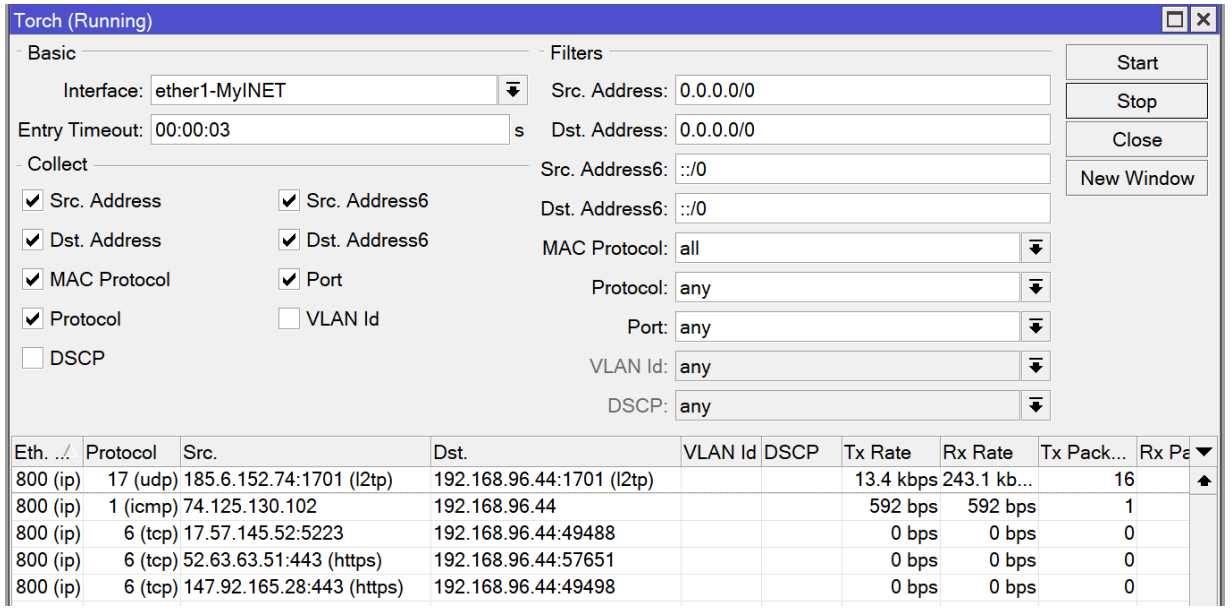
ROUTEROS TOOLS

- RouterOS menyediakan berbagai utilitas yang membantu mengelola dan memanatu router dengan lebih efisien.



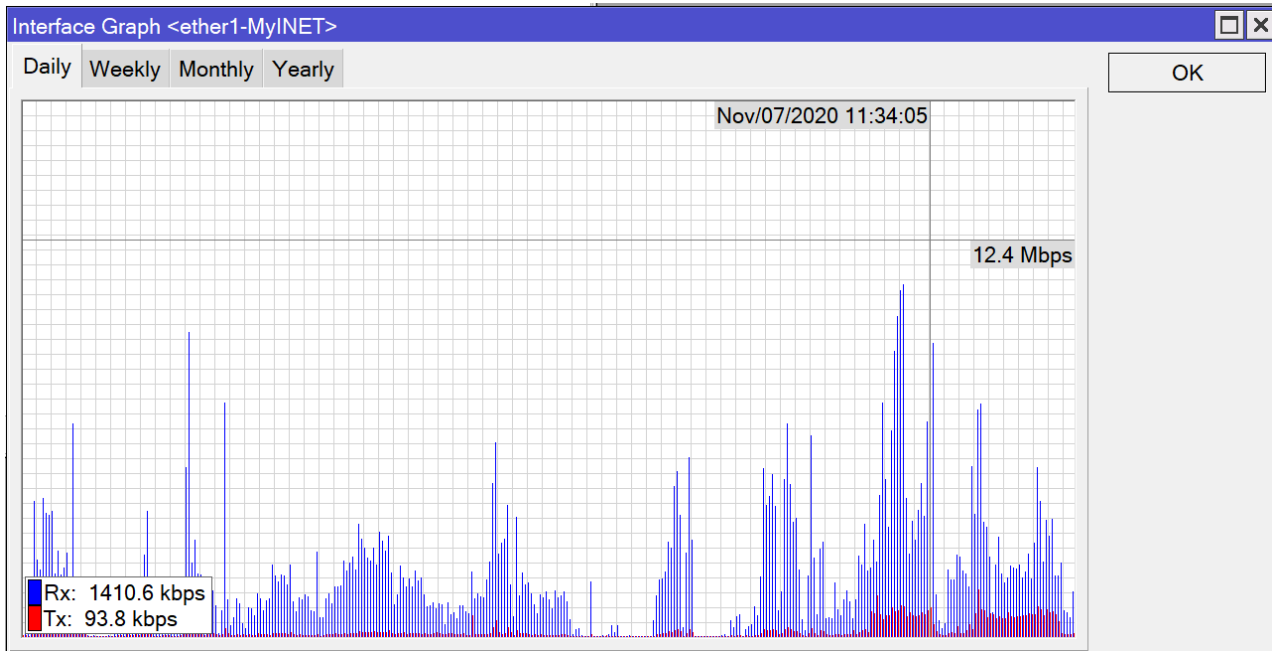
TORCH

- Digunakan untuk memantau traffic dari sebuah paket melalui interface.
- Real-time monitoring tool
- Dapat memantau lalu lintas yang diklasifikasikan berdasarkan nama protocol IP, sumber / alamat tujuan (IPv4 / IPv6), dan port.



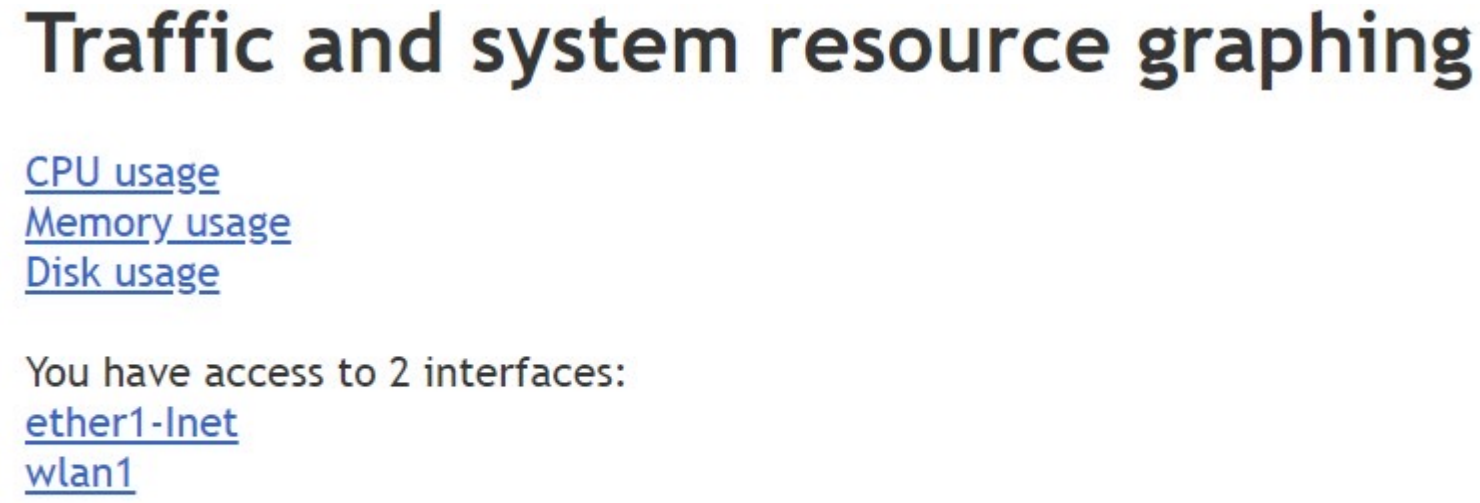
GRAPHS

- Digunakan untuk memonitoring traffic yang melewati interface dalam waktu tertentu.
- Traffic rata-rata diambil tiap interval 5 menit sekali.
- Dapat digunakan untuk memonitoring penggunaan CPU, memory dan disk



GRAPHS

- Untuk melihat hasil monitoring graphs bisa melalui 2 cara :
- Winbox : Tool > Graphing > Interface Graphs
- WebFig : http://router_ip/graphs

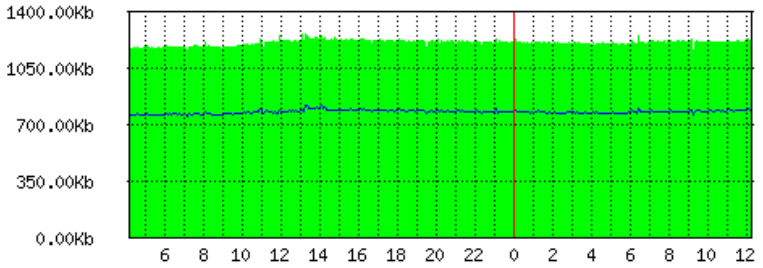


GRAPHS

Interface <ether1-gateway> Statistics

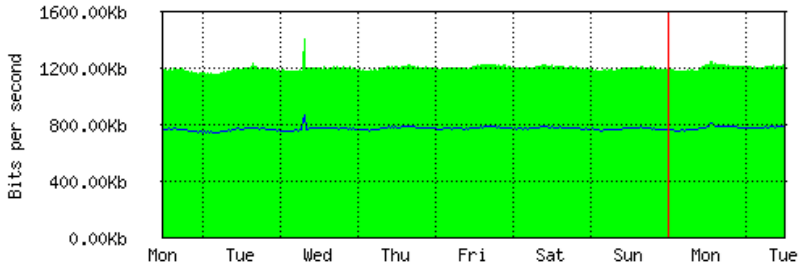
- Last update: Wed Dec 31 23:59:59 2015

"Daily" Graph (5 Minute Average)



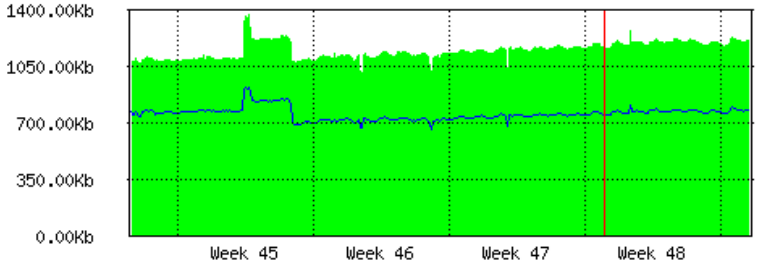
Max In: 1.26Mb; Average In: 1.21Mb; Current In: 1.22Mb;
Max Out: 821.58Kb; Average Out: 780.56Kb; Current Out: 793.75Kb;

"Weekly" Graph (30 Minute Average)



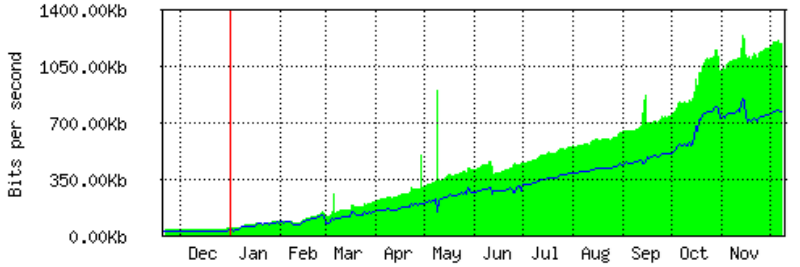
Max In: 1.41Mb; Average In: 1.20Mb; Current In: 1.22Mb;
Max Out: 872.20Kb; Average Out: 772.71Kb; Current Out: 792.54Kb;

"Monthly" Graph (2 Hour Average)



Max In: 1.37Mb; Average In: 1.15Mb; Current In: 1.21Mb;
Max Out: 922.93Kb; Average Out: 757.19Kb; Current Out: 786.12Kb;

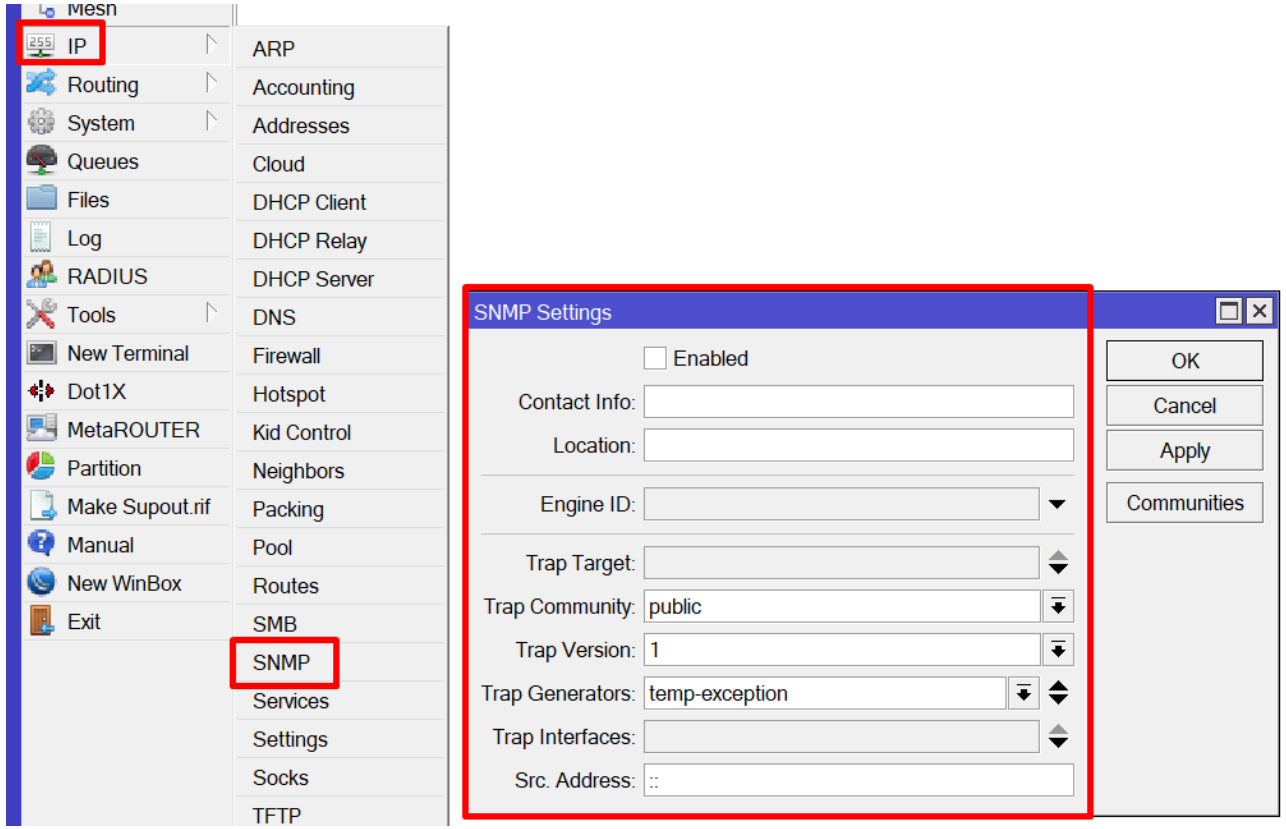
"Yearly" Graph (1 Day Average)



Max In: 1.24Mb; Average In: 445.51Kb; Current In: 1.20Mb;
Max Out: 850.52Kb; Average Out: 303.36Kb; Current Out: 772.42Kb;

SNMP

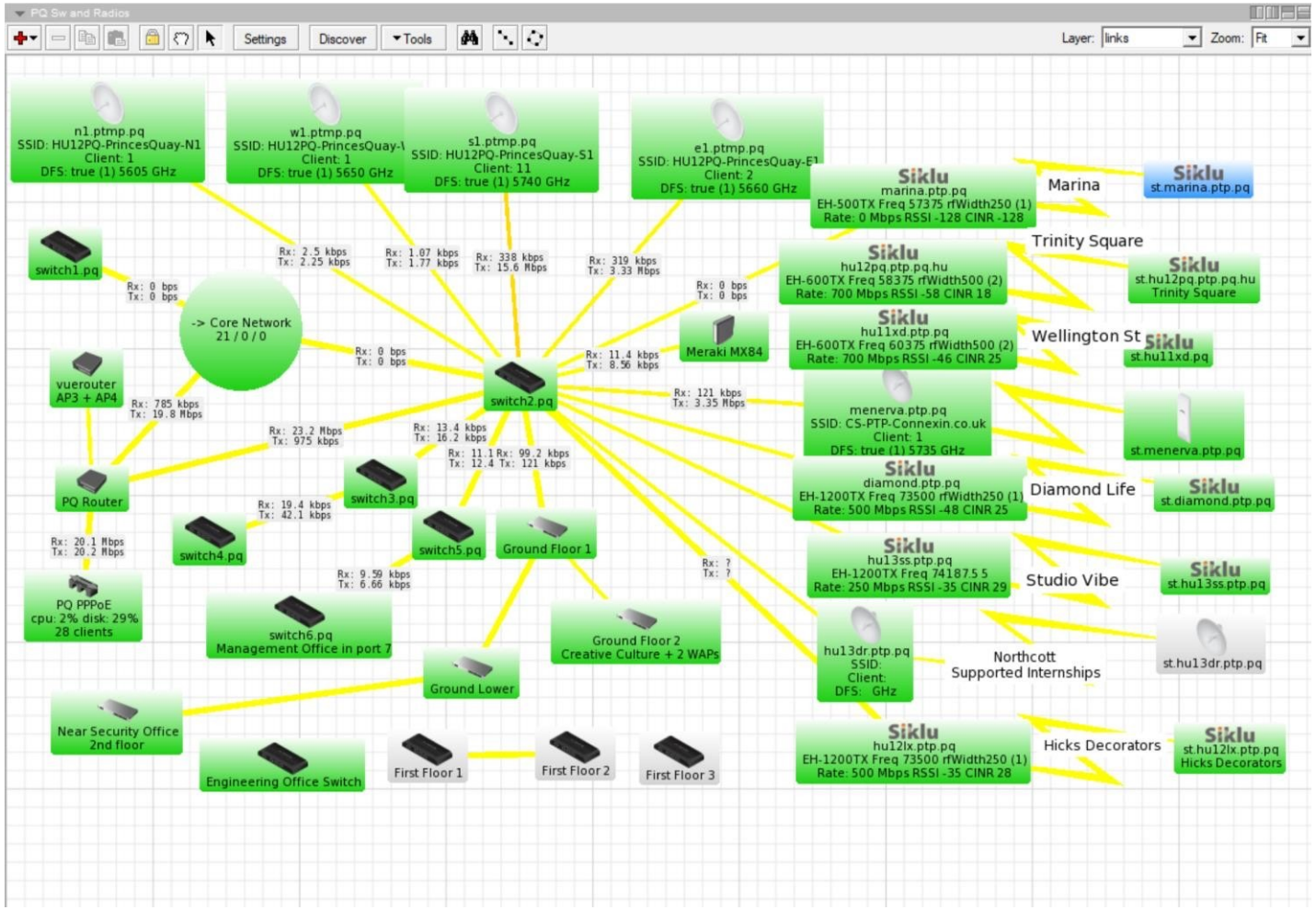
- Simpe Network Management Protocol (SNMP)
- Digunakan untuk memonitor dan mengelola perangkat.
- RouterOS mendukung SNMP v1, v2 dan v3
- **IP > SNMP**



THE DUDE

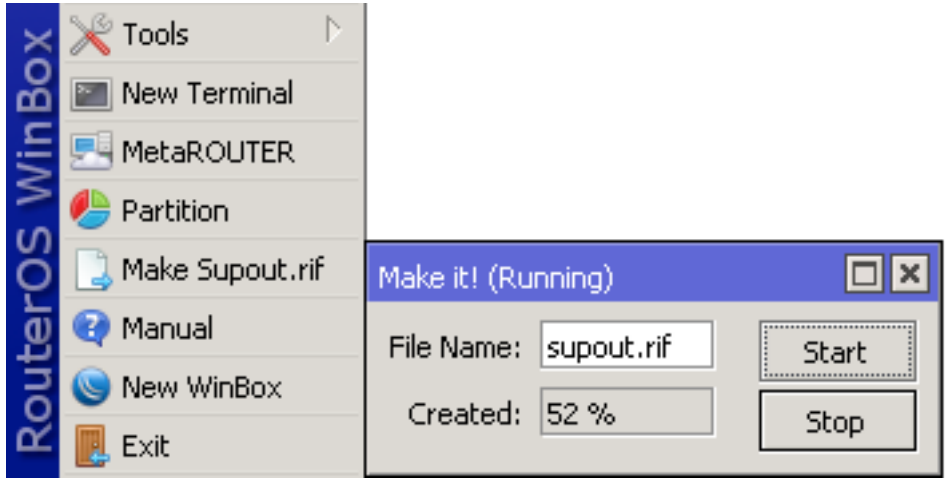
- Aplikasi bawaan Mikrotik yang digunakan untuk memonitoring jaringan secara realtime.
- Device yang akan dimonitoring bisa ditambahkan secara manual kedalam The Dude atau secara otomatis menggunakan fitur Discovery.
- Monitoring services dan alerting.
- Free
- Mendukung SNMP, ICMP, DNS dan TCP monitoring.
- Terdapat 2 tipe The Dude :
  - The Dude Server (digunakan sebagai SNMP master untuk menjalankan service The Dude -> CCR, CHR, or x86)
  - The Dude Client (digunakan sebagai SNMP Agent menampilkan device yang sedang dimonitoring -> windows, linux dan OS X menggunakan aplikasi pihak ketiga)

THE DUDE


PQ Sw and Radios
Settings
Discover
Tools
Layer: links
Zoom: Fit
n1.ptmp.pq
SSID: HU12PQ-PrincesQuay-N1
Client: 1
DFS: true (1) 5605 GHz
w1.ptmp.pq
Client: 1
DFS: true (1) 5650 GHz
s1.ptmp.pq
SSID: HU12PQ-PrincesQuay-S1
Client: 11
DFS: true (1) 5740 GHz
e1.ptmp.pq
SSID: HU12PQ-PrincesQuay-E1
Client: 2
DFS: true (1) 5660 GHz
Siklu
marina.ptp.pq
EH-500TX Freq 57375 rfWidth250 (1)
Rate: 0 Mbps RSSI -128 CINR -128
Marina
Siklu
st.marina.ptp.pq
switch1.pq
Rx: 2.5 kbps
Tx: 2.25 kbps
Rx: 1.07 kbps
Tx: 1.77 kbps
Rx: 338 kbps
Tx: 15.6 Mbps
Rx: 319 kbps
Tx: 3.33 Mbps
Rx: 0 bps
Tx: 0 bps
Siklu
hu12pq.ptp.pq.hu
EH-600TX Freq 58375 rfWidth500 (2)
Rate: 700 Mbps RSSI -58 CINR 18
Trinity Square
Siklu
st.hu12pq.ptp.pq.hu
Trinity Square
Rx: 0 bps
Tx: 0 bps
-> Core Network
21 / 0 / 0
Meraki MX84
Siklu
hu11xd.ptp.pq
EH-600TX Freq 60375 rfWidth500 (2)
Rate: 700 Mbps RSSI -46 CINR 25
Wellington St
Siklu
st.hu11xd.pq
Rx: 0 bps
Tx: 0 bps
Rx: 11.4 kbps
Tx: 8.56 kbps
vuerouter
AP3 + AP4
switch2.pq
Rx: 121 kbps
Tx: 3.35 Mbps
Rx: 785 kbps
Tx: 19.8 Mbps
menerva.ptp.pq
SSID: CS-PTP-Connexin.co.uk
Client: 1
DFS: true (1) 5735 GHz
st.menerva.ptp.pq
Rx: 23.2 Mbps
Tx: 975 kbps
Rx: 13.4 kbps
Tx: 16.2 kbps
Rx: 11.1 Rx: 99.2 kbps
Tx: 12.4 Tx: 121 kbps
Siklu
diamond.ptp.pq
EH-1200TX Freq 73500 rfWidth250 (1)
Rate: 500 Mbps RSSI -48 CINR 25
Diamond Life
Siklu
st.diamond.ptp.pq
PQ Router
switch3.pq
Rx: 19.4 kbps
Tx: 42.1 kbps
switch4.pq
switch5.pq
Ground Floor 1
Rx: 20.1 Mbps
Tx: 20.2 Mbps
Rx: 9.59 kbps
Tx: 6.66 kbps
Rx: ?
Tx: ?
Siklu
hu13ss.ptp.pq
EH-1200TX Freq 74187.5 5
Rate: 250 Mbps RSSI -35 CINR 29
Studio Vibe
Siklu
st.hu13ss.ptp.pq
PQ PPPoE
cpu: 2% disk: 29%
28 clients
switch6.pq
Management Office in port 7
Ground Floor 2
Creative Culture + 2 WAPs
hu13dr.ptp.pq
SSID:
Client:
DFS: GHz
Northcott
Supported Internships
st.hu13dr.ptp.pq
Ground Lower
Near Security Office
2nd floor
Engineering Office Switch
First Floor 1
First Floor 2
First Floor 3
Siklu
hu12lx.ptp.pq
EH-1200TX Freq 73500 rfWidth250 (1)
Rate: 500 Mbps RSSI -35 CINR 28
Hicks Decorators
Siklu
st.hu12lx.ptp.pq
Hicks Decorators

CONTACTING SUPPORT

- autosupout.rif akan dibuat secara otomatis apabila terjadi kerusakan perangkat keras.
- Dimanage oleh proses watchdog.
- Sebelum mengirim ke Mikrotik, konten file output support dapat dilihat di mikrotik.com/account



CONTACTING SUPPORT

- Sebelum mengontak support@mikrotik.com check resources pada router.
- Disarankan untuk memberikan note pada setiap support yang kita report.
- Jelaskan serinci mungkin sehingga dapat memudahkan tim Mikrotik
- Sertakan diagram jaringan anda
- Untuk selengkapnya bisa dilihat di link berikut https://mikrotik.com/support

TERIMAKASIH

www.idn.id