MTCNA

MikroTik Certified Network Associate Training

Rofiq Fauzi, MTCNA, MTCRE, MTCWE, MTCTCE, MTCUME, MTCINE, Trainer
ID-Networkers | www.Training-MikroTik.com

ID NETWORKERS
Expert Trainer & Consultant

Rofiq Fauzi

- Using MikroTik (v.2.97) since 2005, as Network Engineer at WISP company
- 2007, Network & Wireless Engineer at INDOSAT Central Java Area
- 2008, Network & Telco Procurement at INDOSAT Head Quarter
- 2012-Now, MikroTik Consultant & Certified Trainer (MTCNA, MTCRE, MTCTCE, MTCWE, MTCINE, Certified Trainer) at ID-Networkers.
- Training & Consultant in Asia Pacific (Cambodia, Thailand, Philippine, Nepal, Malaysia

CONSULTANT	http://www.mikrotik.com/consultants/asia/indonesia
CERTIFIED TRAINER	http://www.mikrotik.com/training/partners/asia/indonesia

ID NETWORKERS
Expert Trainer & Consultant

ID-NETWORKERS

EXPERT LEVEL TRAINERS & CONSULTANS

In the Most Prestigious Networking Certification

OVERVIEW

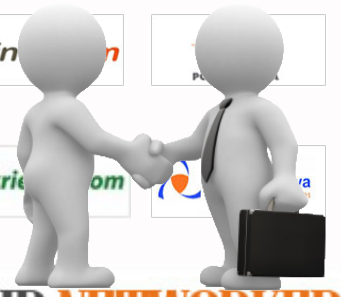
We are young entrepreneurs, we are only one training partner & consultant who has expert level trainers in the most prestigious networking certification, CCIE Guru , JNCIE Guru and MTCINE guru, which very limited number in Indonesia even Asia. Proven that hundred of our students pass the certification exam every year. We are the biggest certification factory in Indonesia.

WEBSITE
www.id-networkers.com
www.idn.id

ID NETWORKERS
Expert Trainer & Consultant

Our Clients

Prasmanindo Boga Utama
Fondaco Mitratama
PrawedaNET Aliansi Teknologi
Sentranet multimedia
metra
SCBDnet
PSN
BERCA
IBM Jasa Teknologi Informasi
JGC
HIMALAYA
Colliers International
BAHANA
TERA
SNS
Alcatel-Lucent
PACKET SYSTEMS
CIMB NIAGA
SPOTELINDO MITRA UTAMA
Bata
telkomsigma
tokobagus.com
ERICSSON
APJII
Deloitte.
ASIATECHBIZ
AXIS
lintasarta
PATRAKOM
netsphere
Aerofood ACS
icon+
HUAWEI
indosat
FUJITSU
KINGSLAM soft
PT. MUSTIKA MEMADATA
INOV
alita
Manulife
MNC insurance
ASIATECHBIZ
Telkom Indonesia
Nokia Siemens Networks
BANK KALBAR
INDOSATM2 connected anywhere
Moratelindo creative telecom innovation
Telin
EPSON
PRIMA BANK
KALBE
MITRA INTEGRASI INFORMATIKA



ID NETWORKERS
Expert Trainer & Consultant

Perkenalkan Diri Anda

- Silahkan perkenalkan diri anda:
  - Nama?
  - Dari Perusahaan apa?/pekerjaan sehari-hari?
  - Pengalaman menggunakan MikroTik?
  - Pengalaman tentang jaringan?
  - Apa yang diharapkan dari training ini?

Connect Internet

- Wifi = IDN-TRAINING
- Password = idnmantab

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.

User Information	
Company Name (or person name):	Rofiq Fauzi, ID-Networkers *
Authorised Person *(Firstname Lastname)* or Purchaser (for ordering):	Rofiq Fauzi *
E-mail (License key will be sent here):	rofiq.fauzi@gmail.com *

- Informasikan email anda ke instruktur (rofiq.fauzi@gmail.com), peserta harus mendapat invitation dari instruktur.

Tentang Ujian MTCNA

- Online test terdiri atas 25 soal dalam waktu 1 jam.
- Soal setiap test random, dengan beberapa soal mungkin ada yang sama dengan soal sebelumnya.
- Passing grade **60%,** nilai 50%-59% bisa test ulang.
- Hati-hati membaca soal, disamping bahasa inggris dari soal yang kadang-kadang kurang mudah dipahami, juga banyak jebakan batman ☺.
- **Silahkan melakukan latihan test training di web mikrotik, dan lihat scorenya.**

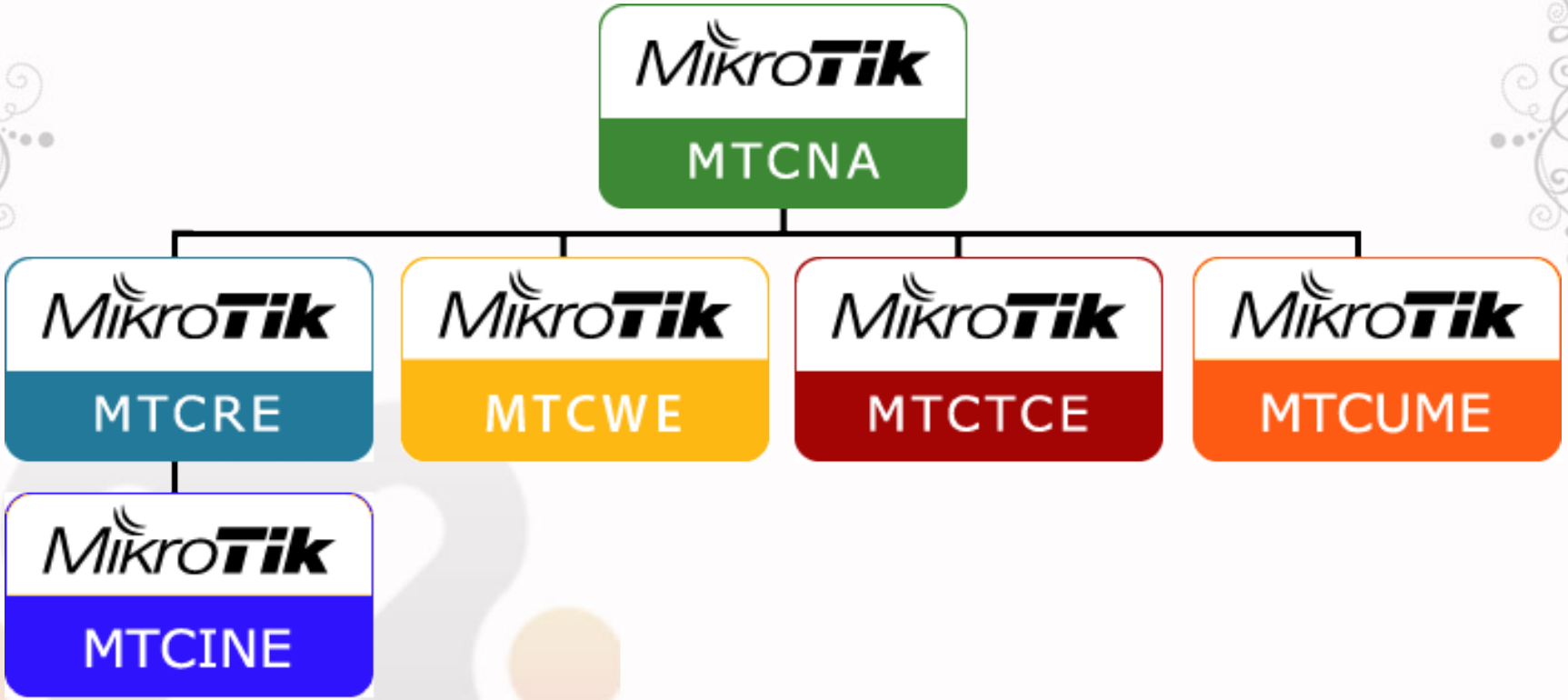
Latihan Test

- Setelah mendapatkan invitation dari trainer, peserta dapat melakukan latihan ujian MTCNA di website mikrotik.com
- Latihan ujian MTCNA ada di menu Account , My training session, Try example test

Tujuan Training MTCNA

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

Sertifikasi MikroTik

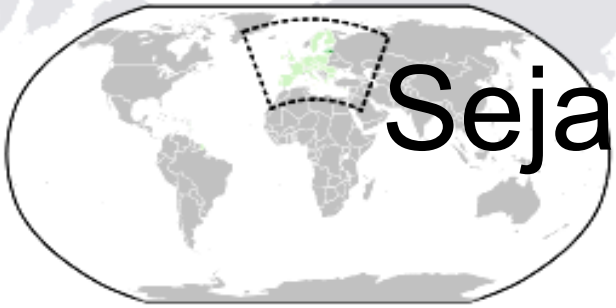


- Sertifikasi berjenjang, kalau belum lulus MTCNA belum bisa ikut ujianlevel engineer
- Masa berlaku sertifikat selama 3 tahun, setelah itu bisa diperpanjang dengan cara ujian lagi

MTCNA – Outline

- Module 1 – Introduction of MikroTik RouterOS
  – TCP/IP Review
- Module 2 – Firewall
- Module 3 – Wireless
- Module 4 – Bridging
- Module 5 – Routing
- Module 6 – Tunnel
- Module 7 – QoS
- Module 8 – Network Management

BAB I
Introduction MikroTik RouterOS & RouterBOARD



Sejarah MikroTik

- 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.
- Founder (1996): John Trully & Arnis Reikstins.

Jenis MikroTik

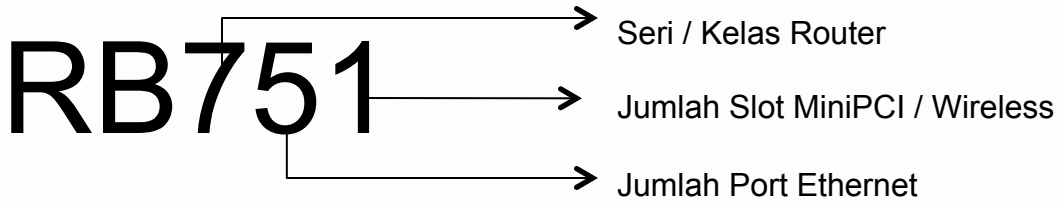
- MikroTik RouterOS™
  - ✓Operating sistem yang bisa diinstall di PC dan menjadikannya sebuah Router yang handal.
  - ✓Berbasis Linux
  - ✓Diinstall sebagai Sistem Operasi
  - ✓Biasanya diinstall pada power PC
- MikroTik RouterBOARD
  - ✓Built in hardware (board) yang menggunakan RouterOS sebagai Operating Sistemnya.
  - ✓Tersedia mulai low-end s/d high-end Router.

Fitur-Fitur Mikrotik

- Router OS apabila diinstall pada PC/Virtual machine, akan support driver perangkat
  - ✓ Ethernet, Wireless Card, V35, ISDN, USB Mass Storage, USB 3G Modem, E1/T1.
- Memiliki fitur yang melebihi sebuah “router”
  - ✓ User Management (DHCP, Hotspot, Radius, dll).
  - ✓ Routing (RIP, OSPF, BGP, RIPng, OSPF V3).
  - ✓ Firewall & NAT (fully-customized, linux based).
  - ✓ QoS/Bandwidth limiter (fully customized, linux based).
  - ✓ Tunnel (EoIP, PPTP, L2TP, PPPoE, SSTP, OpenVPN).
  - ✓ Real-time Tools (Torch, watchdog, mac-ping, MRTG, sniffer).

RouterBOARD - Type

- RouterBoard memiliki sistem kode tertentu



- Kode Lain ada di belakang tipe
  - ✓ U - dilengkapi port USB
  - ✓ A - Advanced, biasanya diatas lisensi level 4
  - ✓ H - Hight Performance, processor lebih tinggi
  - ✓ R - dilengkapi wireless card embedded.
  - ✓ G - dilengkapi port ethernet Gigabit
  - ✓ 2nD – dual channel

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

- Secara lengkap dapat dilihat di www.mikrotik.com/download

MikroTik VS Cisco

source: http://wiki.MikroTik.com/wiki/Manual:RouterOS_FAQ

How does this software compare to using a Cisco router?

*You can **do almost everything** that a proprietary router does at a fraction of the **cost** of such a router and have flexibility in upgrading, **ease of management and maintenance**.*

Anda dapat melakukan **hampir semua** yang dilakukan proprietary router tersebut (Cisco) dengan hanya sebagian kecil dari biaya router tersebut dan memiliki **fleksibilitas dalam mengupgrade, kemudahan manajemen dan pemeliharaan**.

Prerequisites MTCNA Training
TCP / IP Basic

Internet Protocol

Internet Protocol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer.

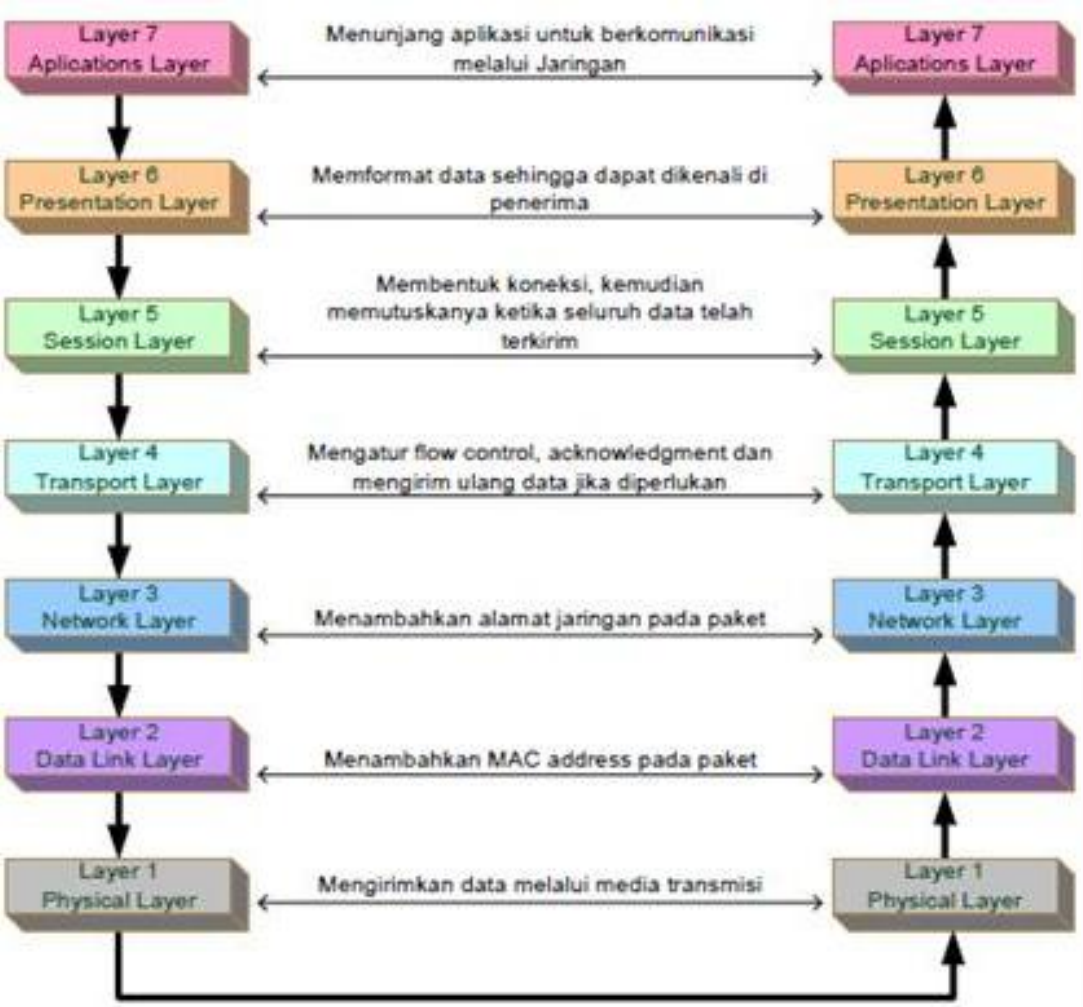
Tugas Internet Protocol

- Melakukan deteksi koneksi fisik.
- Melakukan metode “jabat-tangan” (handshaking).
- Negosiasi berbagai macam karakteristik hubungan.
- Mengawali dan mengakhiri suatu pesan/session.
- Bagaimana format pesan yang digunakan.
- Apa yang dilakukan apabila terjadi error pengiriman?.
- Mengkalkulasi dan menentukan jalur pengiriman.
- Mengakhiri suatu koneksi.

OSI Layer Model

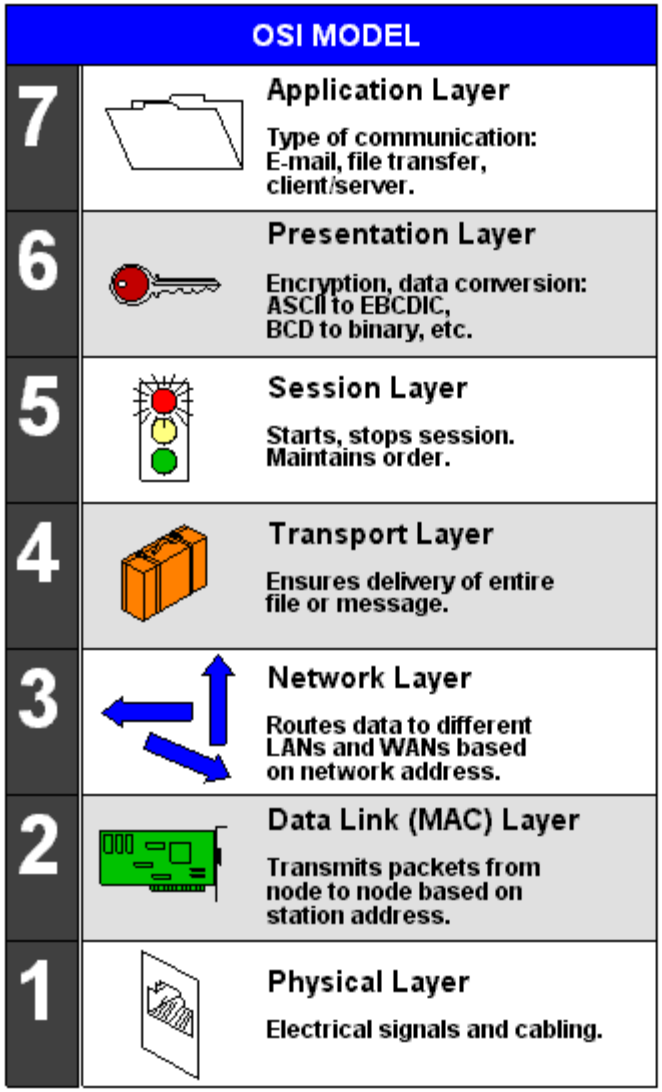
- Tidak adanya suatu protokol yang sama, membuat banyak perangkat tidak bisa saling berkomunikasi.
- ***Open System Interconnection*** atau OSI layer 7 *adalah m*odel arsitektural jaringan yang dikembangkan oleh International Organization for Standardization (ISO) di Eropa tahun1977.
- Sebelum ada OSI, 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 7 Leyer - Koneksi Antar Host



ID NETWORKERS
Expert Trainer & Consultant

OSI Layer



- Apabila 7 OSI Layer susah untuk dihafal, maka Layer 1, Layer 2 dan Layer 3 adalah suatu keharusan, karena dapat menunjukkan bedanya antara Hub/bridge, Switch dan Router
- Ketiganya berada di layer yang berbeda sehingga memiliki cara kerja yang berbeda tentunya

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

Device	Connectivity	Data Transfer	Memory
Router	Antar network yang berbeda	Destination IP Address	Routing Table
Switch	Antar network yang sama	Berdasar MAC Address Tujuan	MAC Address Table
Hub	Antar network yang sama	Broadcast ke semua port	none

Protocol

- Protocol menentukan prosedur pengiriman data.
- Protocol yang sering digunakan:
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP) → DNS
  - Internet Control Message Protocol (ICMP) →ping traceroute
  - Hypertext Transfer Protocol (HTTP) →web
  - Post Office Protocol (POP3)→email
  - File Transfer Protocol (FTP)
  - Internet Message Access Protocol (IMAP)→email
  - dll

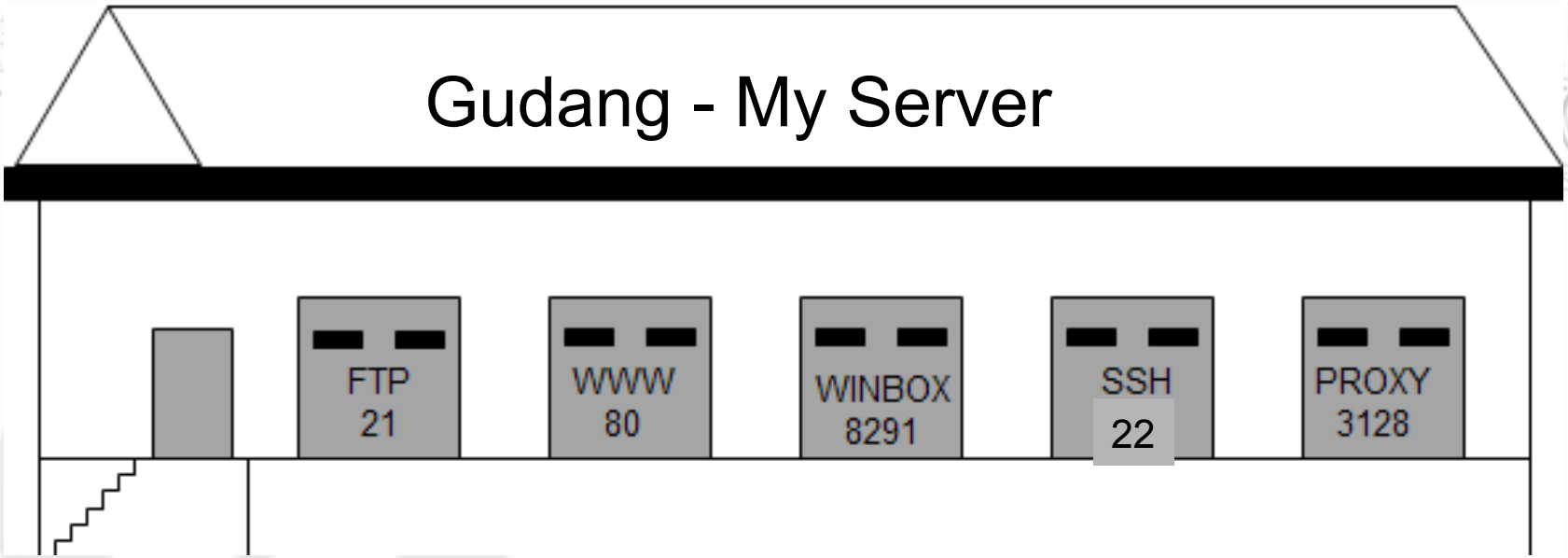
Port

- Port adalah sebuah aplikasi-spesifik atau proses software spesifik pada Komputer/host yang **menjalankan servise** untuk komunikasi jaringan.
- Jumlah total port Host adalah 65535, dengan klasifikasi penomoran sebagai berikut:
  1. Dari 0 s/d 1023 (*well-known ports),*
  2. Dari 1024 s/d 49151 (*registered port*),
  3. Dari 49152 s/d 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



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 12 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.
- IP address digunakan untuk pengalamatan suatu PC / host secara logic
- Terdapat 2 jenis IP Address
  - ✓ IPv4
    - ✓Pengalamatan 32 bit
    - ✓Jumlah max host 4,294,967,296
  - ✓ IPv6
    - ✓Pengalamatan 128 bit
    - ✓Jumlah max host 340,282,366,920,938,463,374,607,431,768,211,456

IPv4

- IPv4 diekspresikan dalam notasi desimal bertitik, yang dibagi ke dalam 4 buah oktet berukuran 8-bit.
- Karena setiap oktet berukuran 8-bit, maka nilainya berkisar antara 0 hingga 255 (2^0 s/d 2^7)
- Aturan pengalamatan IPv4, misal IP 192.148.41.1

11000000.10010100.00101111.00000001

$1x2^7 + 0x2^6 + 0x2^5 + 1x2^4 + 0x2^3 + 1x2^2 + 0x2^1 + 0x2^0$

1x128 + 0x64 + 0x32 + 1x16 + 0x8 + 1 x4 + 0x2 + 0x1

128 + 0 + 0 + 16 + 0 + 4 + 0 + 0 = 148

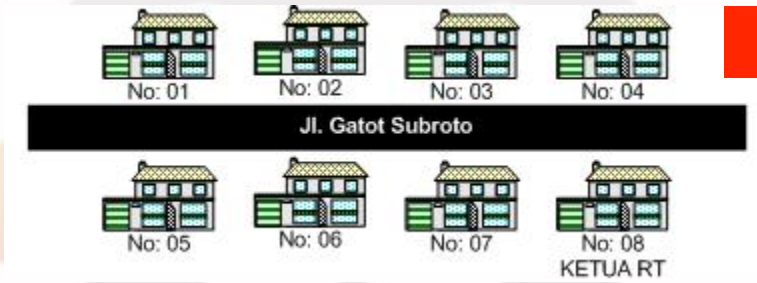
192 . 148 . 41 . 1

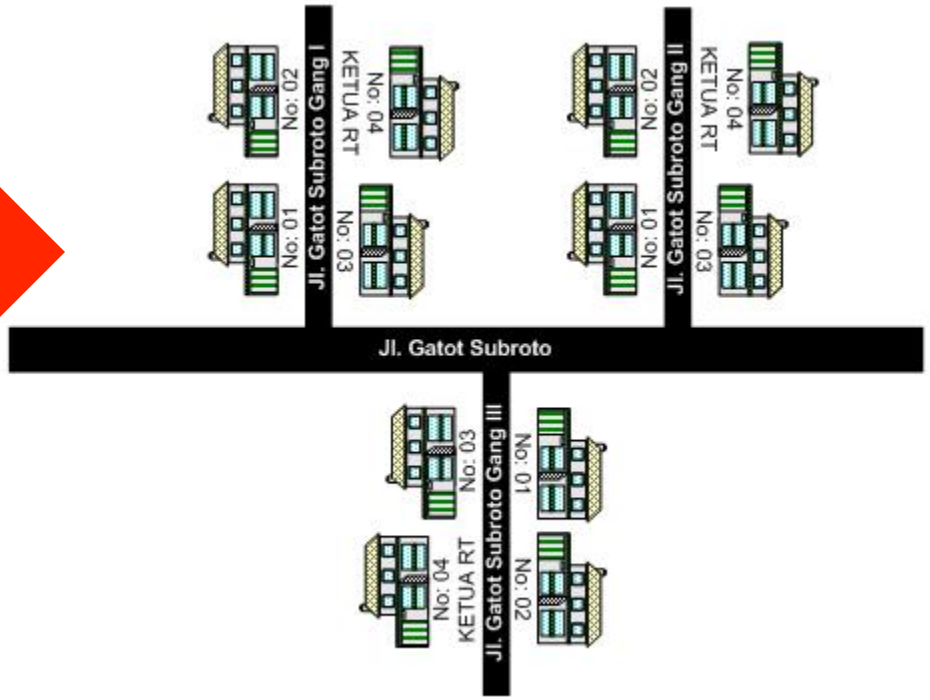
Subneting

- Dari 4 milyar IP address, tidak mungkin diberikan ke satu internet provider saja.
- Alamat IP didesain untuk digunakan secara berkelompok (sub-jaringan/subnet).
- Subneting adalah cara untuk memisahkan dan mendistribusikan beberapa IP address.
- Host/perangkat yang terletak pada subnet yang sama dapat berkomunikasi satu sama lain secara langsung (tanpa melibatkan router/ routing).

Subneting

- Apabila jaringan dianalogikan sebuah jalan, apabila disepanjang jalan cuma ada 8 rumah, ketua RT mengumumkan sesuatu dari rumah ke rumah lewat jalan itu.
- Apabila sepanjang jalan sudah penuh rumah butuh ada gang-gang . Butuh ada ketua RT tiap gang untuk meminimalis transportasi saat pengumuman dan mengatur urusan RTnya sendiri





Notasi Subnet

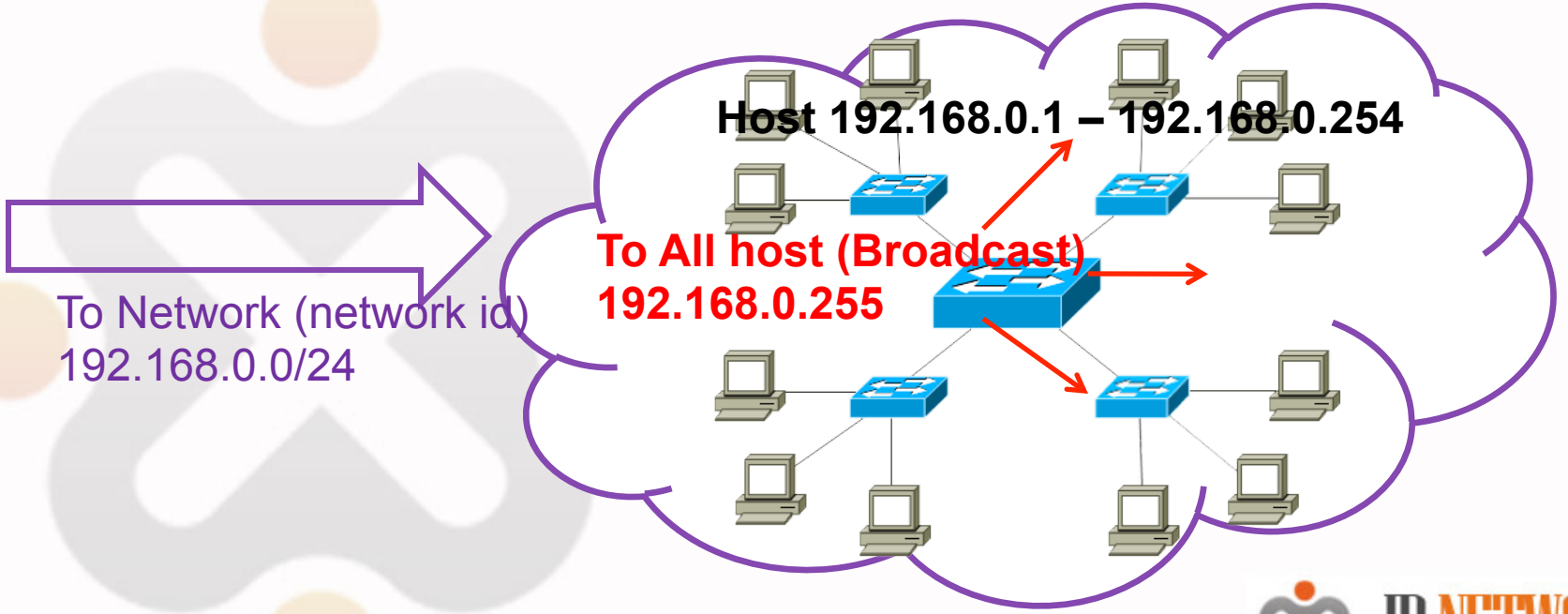
- Subnet ditulis dalam format 32 bit (seperti IP), atau dalam bentuk desimal (prefix Length)

Subnet mask (biner)	Subnet mask (desimal)	Prefix Length
11111111.00000000.00000000.00000000	255.0.0.0	/8
11111111.11111111.00000000.00000000	255.255.0.0	/16
11111111.11111111.11111111.00000000	255.255.255.0	/24

- Sebagai contoh, network 192.168.1.0 yang memiliki subnet mask 255.255.255.0 dapat direpresentasikan di dalam notasi prefix length sebagai **192.168.1.0/24.**

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

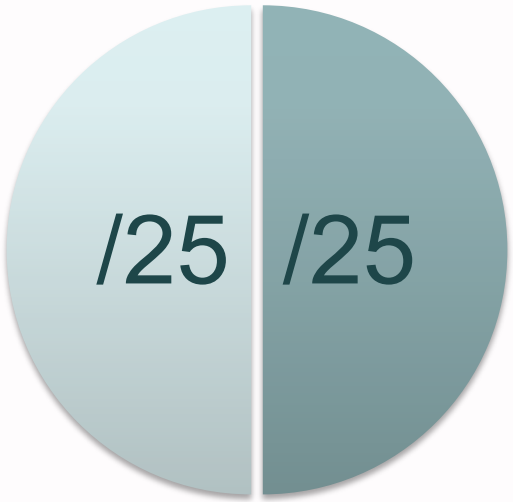
Tabel Subnetting

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	-

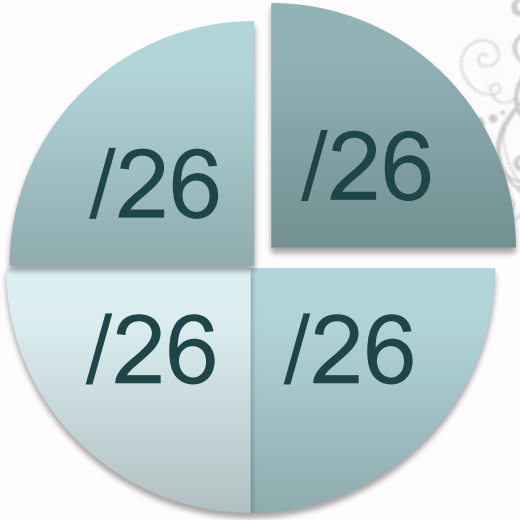
Subneting

256 IP Address

128 IP / Subnet



64 IP / Subnet



192.168.0.0/24
(192.168.0.0-192.168.0.255)

- 192.168.0.0/25 (192.168.0.0-192.168.0.127)
  - 192.168.0.0/26 (192.168.0.0-192.168.0.63)
  - 192.168.0.64/26 (192.168.0.64-192.168.0.127)
- 192.168.0.128/25 (192.168.0.128-192.168.0.255)
  - 192.168.0.128/26 (192.168.0.128-192.168.0.191)
  - 192.168.0.192/26 (192.168.0.192-192.168.0.255)

Perhitungan Subnet

Rumus menghitung Jumlah IP address dalam subnetmask:

$2^{(32-n)}$, dimana n=prefix subnet

Contoh, IP kelas C: 20.20.20.20/30,

Tentukan Range IP, IP Host , Network ID, Broadcast dan Subnet Masknya:

- Jumlah IP dalam subnet:
  Gunakan Rumus $2^{(32-30)} = 2^2 = 4$
- Range IP
  Range IP dicari berdasarkan kelipatan Jumlah IPnya (kelipatan 4):
  20.20.20.0 s/d 20.20.20.3
  20.20.20.4 s/d 20.20.20.7, (8-11),(12-15)…terus sampai (252-255)
  IP address pada soal (20.20.20.20) ada pada range:
  20.20.20.20 s/d 20.20.20.23

Perhitungan Subnet

IP kelas C: 20.20.20.20/30,

Tentukan Range IP, IP Host , Network ID, Broadcast dan Subnet Masknya :

- Network ID dan Boradcast:

  Dari range IP yang telah ditemukan (20.20.20.20 s/d 20.20.20.23)

  IP terkecil digunakan untuk network ID, terbesar untuk Broadcast

  Network ID → 20.20.20.20, Broadcast →20.20.20.23
- IP Host → Range IP dikurangi Network ID dan broadcast

  IP host → 20.20.20.21 s/d 20.20.20.22

  Jumlah IP host →jumlah IP dalam subnet dikurangi dua
- Subnet mask → 255.255.255.(256 – jumlah IP)

  Subnet mask → 255.255.255.252

Kerjakan Soal Berikut

Tentukan jumlah IP, network id & broadcast, IP Host, dan subnet mask dari IP address berikut:

1. 11.11.11.11/26
2. 22.22.22.22/28
3. 33.33.33.33/25
4. 44.44.44.44/29
5. 55.55.55.55/27
6. 66.66.66.66/28
7. 77.77.77.77/30
8. 88.88.88.88/31
9. 99.99.99.99/25
10. 100.100.100.100/27

11.111.111.111.111/30

12. 122.122.122.122/25
13. 133.133.133.133/28

14.144.144.144.144/24

15.155.155.155.155/26

16.166.166.166.166/29

IP Address Kelas B

IP address 12.12.12.12/**22**, Tentukan Range IP, IP Host , Network ID, Broadcast dan Subnet Masknya :

- Translate prefix netmask menjadi kelas C dengan ditambah 8, menjadi (**22**+8)=30
- Jumlah IP prefix /30 dalam kelas C adalah $\mathbf{2^{(32-30)} = 4}$
- Jumlah IP dalam kelas B = **4** x 256 = 1024

Range IP Address

- Jumlah IP kelas C nya, yaitu 4, Range IP diimplementasikan pada oktet ke 3

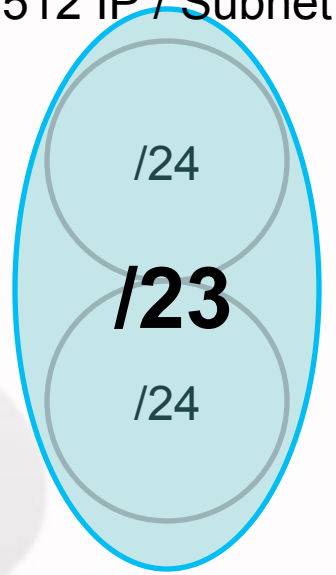
  12.12.**0**.0 – 12.12.**3**.255, 12.12.4.0 – 12.12.7.255, 8 – 11, **12 -15**, dan seterusnya
- Range IP → 12.12.**12**.0 s/d 12.12.15.255
- Network ID →12.12.**12**.0, broadcast 12.12.**15**.255
- Jumlah host yg dapat digunakan →12.12.**12**.1 – 12.12.**15**.254

  Netmask = 255.255.(256-4).0 = 255.255.252.0

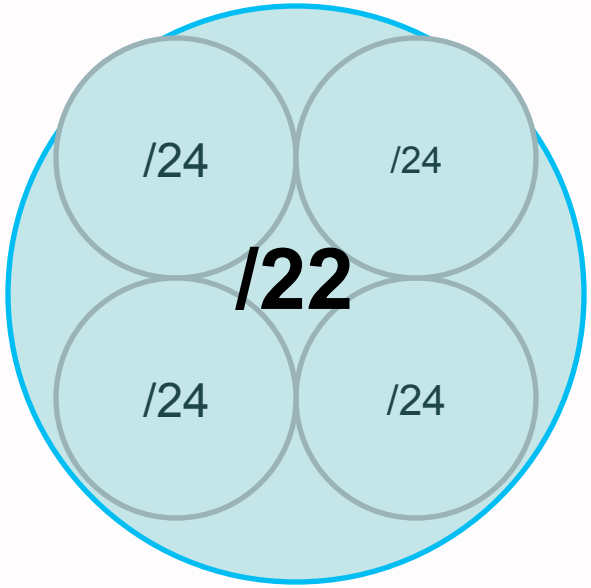
IP Address class B

256 IP Address

512 IP / Subnet



1024 IP / Subnet



Kerjakan Soal Berikut

1. 11.11.11.11/23
2. 22.22.22.22/21
3. 33.33.33.33/20
4. 44.44.44.44/22
5. 55.55.55.55/18

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

- 127.0.0.0 – 127.255.255.255 (loopback address)
- 224.0.0.0 – 239.255.255.255 (multicast)
- 169.254.0.0 - 169.254.255.255 ("link local" addresses)

Modul 1
Mengkases MikroTik RouterOS

Akses ke MikroTik RouterOS

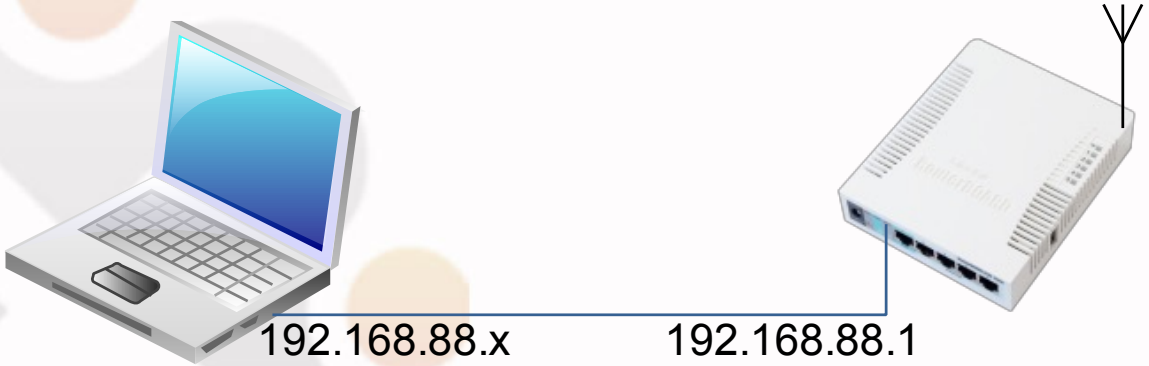
Akses Via	Koneksi	Text Base	GUI	Need IP
Keyboard	Langsung di PC	yes		
Serial Console	Konektor Kabel Serial	yes		
Telnet & SSH	Layer 3	yes		yes
Winbox	Menggunakan OS Windows	yes	yes	
FTP	Layer 3	yes		yes
API	Socket Programing			yes
Web (HTTP)	Layer 3		yes	yes
MAC-Telnet	Layer 2	yes		

Winbox

- Cara paling mudah dalam mengakses dan mengkonfigurasi MikroTik adalah menggunakan winbox.
- Winbox dapat didapatkan dari:
  - Web www.mikrotik.com
  - Via http/web IP atau domain Router MikroTik
  - Copy dari media penyimpanan

Default Setting RouterBoard

- RouterBoard (RB) baru, atau setelah di reset defualt , memiliki default konfigurasi dari pabrikannya yaitu:
  - IP Address Ether 2-5 : 192.168.88.1/24
  - Username “admin” password blank.
- Untuk meremote, Laptop/PC dihubungkan dengan ether1 dan diset dengan IP 192.168.88.xxx/24.



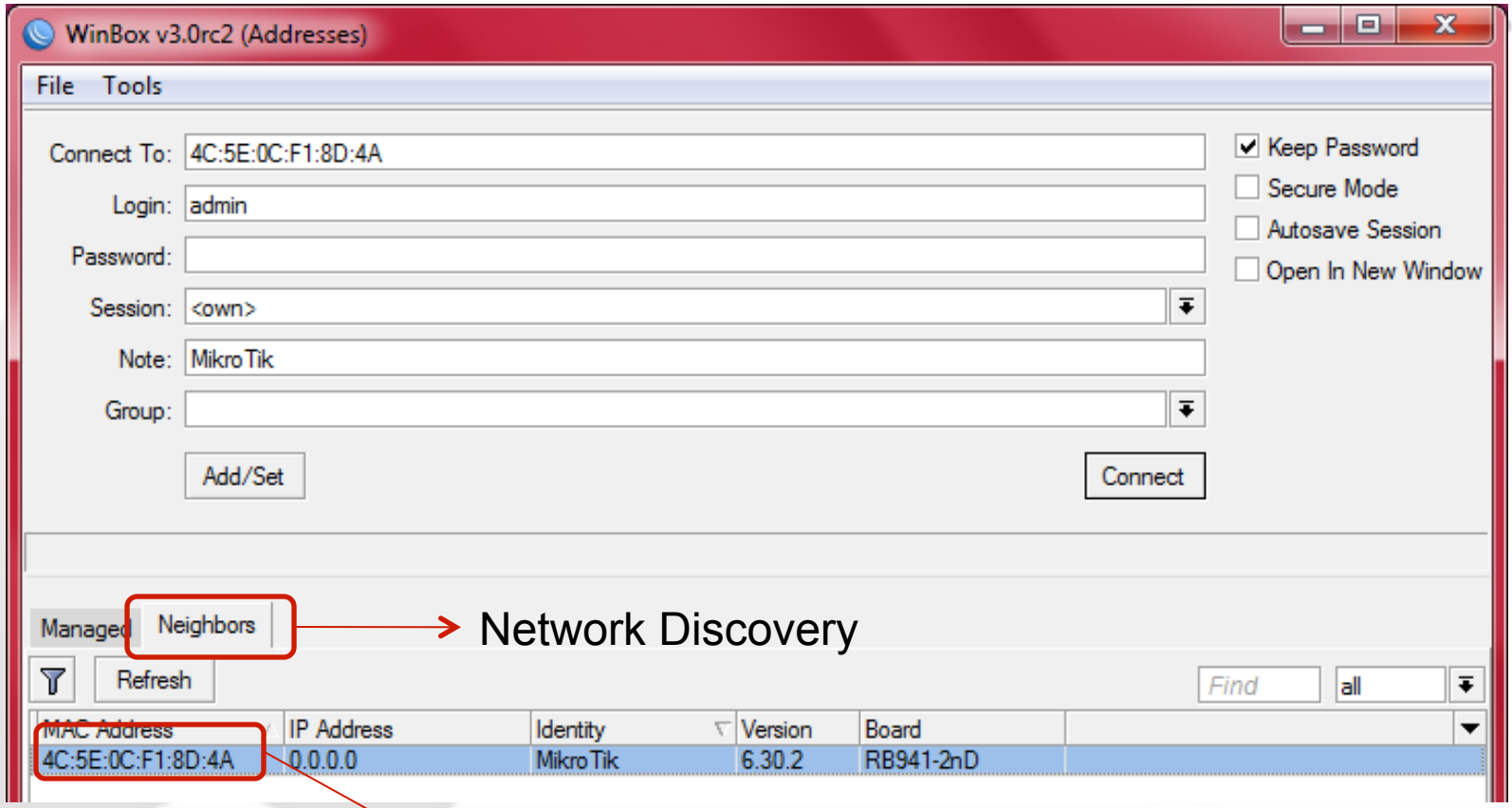
LAB – Konek Router

Apabila router baru (default) untuk remote menggunakan winbox dengan cara:

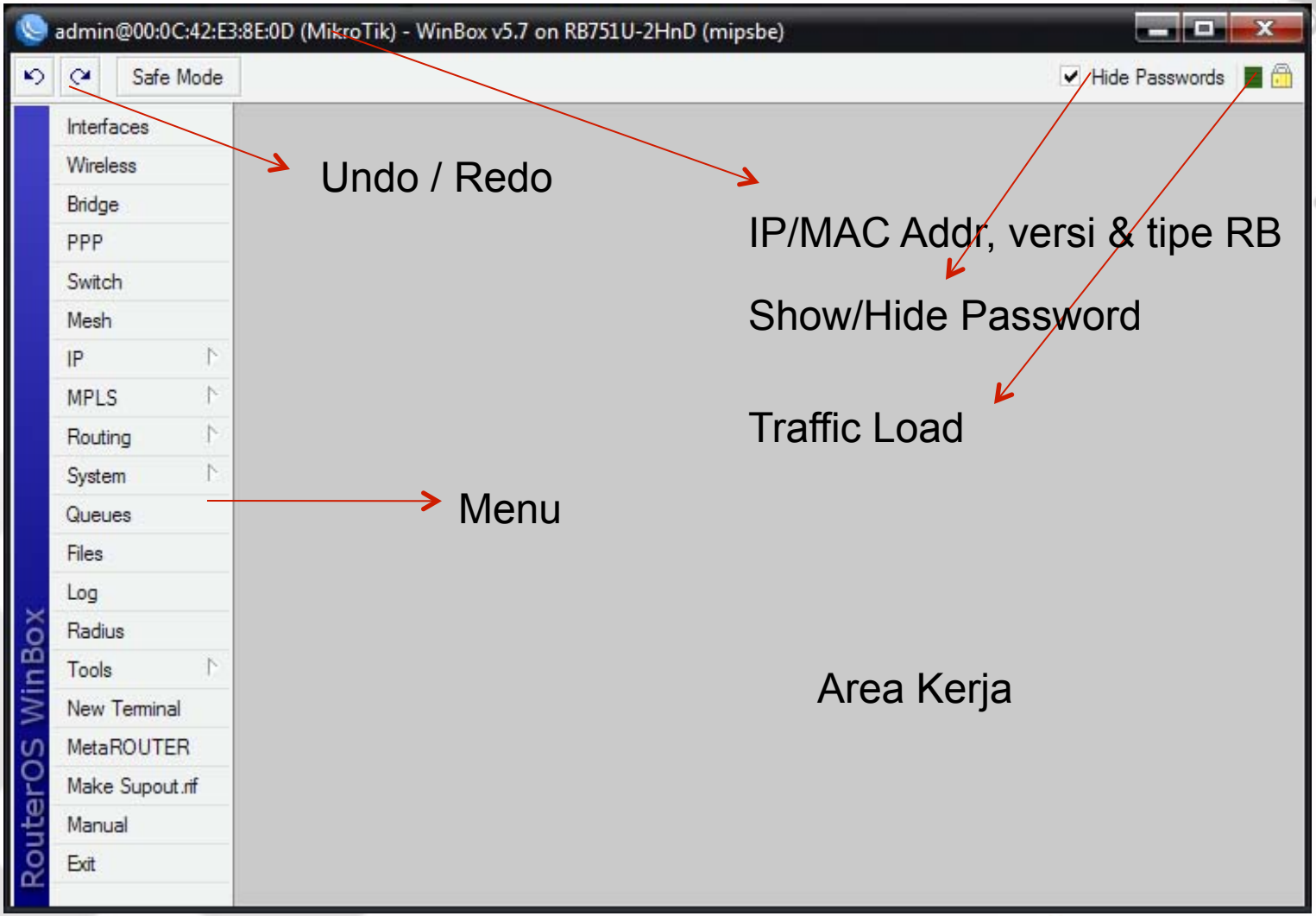
- Ubah IP Komputer anda menjadi:
  - IP Address 192.168.88.x
  - Netmask 255.255.255.0
- Ping ke RouterBOARD (192.168.88.1)
- Buka URL RouterBOARD (http://192.168.88.1)
- Download winbox dari halaman tersebut.

Winbox Login

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



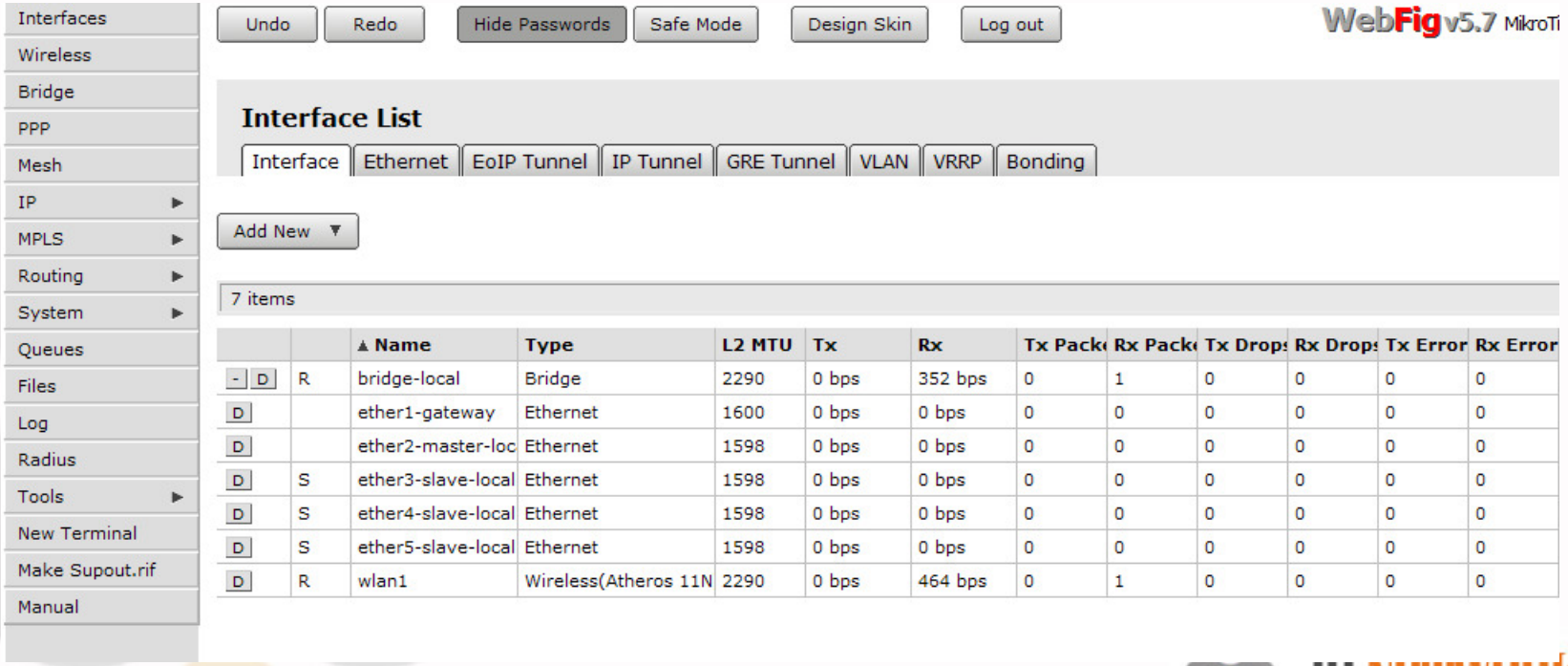
Tampilan MikroTik – pada Winbox



WebFig

Sejak versi 5.0, interface via web diperkenalkan, dengan fungsi-fungsi yang sama dengan Winbox.

- Tambahkan IP pada router pada menu IP Address
- Coba akses webfig mikrotik router anda dengan browser.
- http://<ip router>

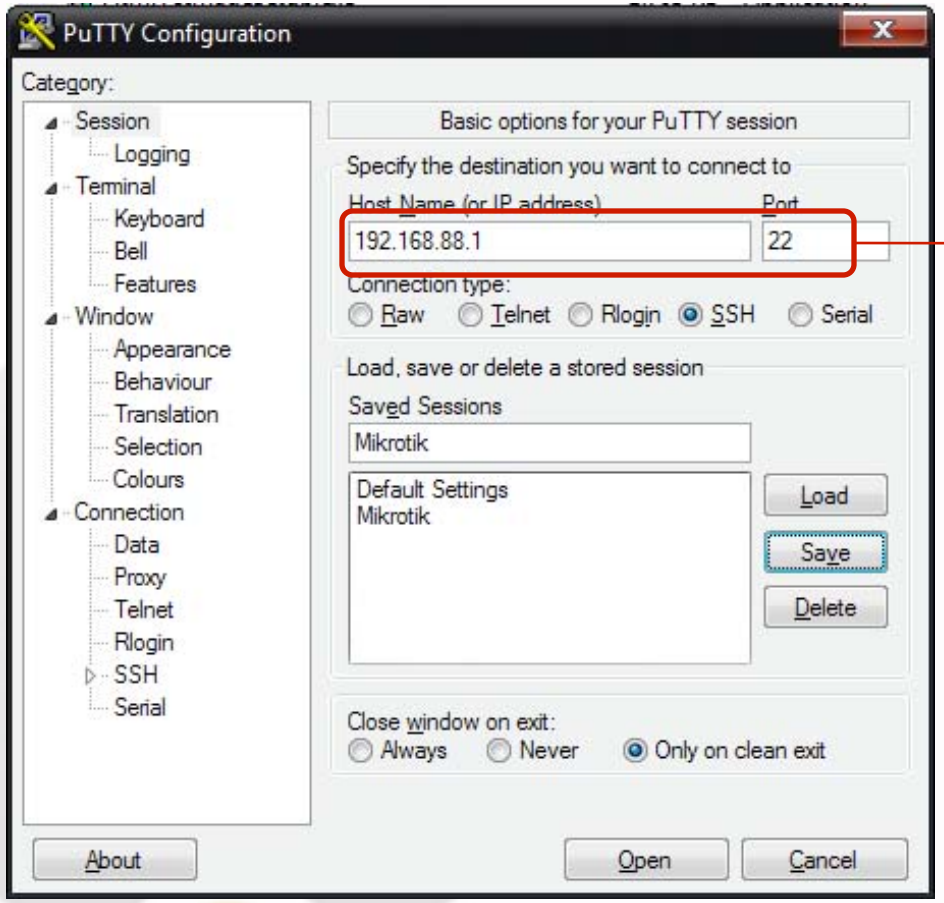


Konfigurasi Via Terminal

- Dalam kondisi tertentu remote dan konfigurasi via GUI tidak memungkinkan dikarenakan hal-hal seperti; keterbatasan bandwidth, kebutuhan untuk running script, remote via ..x console, dll.
- Remote & konfigurasi terminal bisa dilakukan dengan cara:
  - Telnet (via IP port 23, non secure connection)
  - SSH (via IP Port 22, lebih secure dari telnet)
  - Serial console (kabel serial)

LAB-Telnet & SSH

- Gunakan MsDOS prompt (telnet), atau program SSH/Telnet client lainnya, seperti putty, winSCP untuk remote mikrotik.



IP MikroTik dan Port

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.

Versi dan Lisensi Mikrotik

Lisensi MikroTik

- Fitur-fitur RouterOS ditentukan oleh level lisensi yang melekat pada perangkat.
- Level dari lisensi juga menentukan batasan upgrade packet.
- Lisensi melekat pada storage/media penyimpanan (ex. Hardisk, NAND, USB, Compact Flash).
- Bila media penyimpanan diformat dengan non MikroTik, maka lisensi akan hilang.

Level Lisensi MikroTik

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

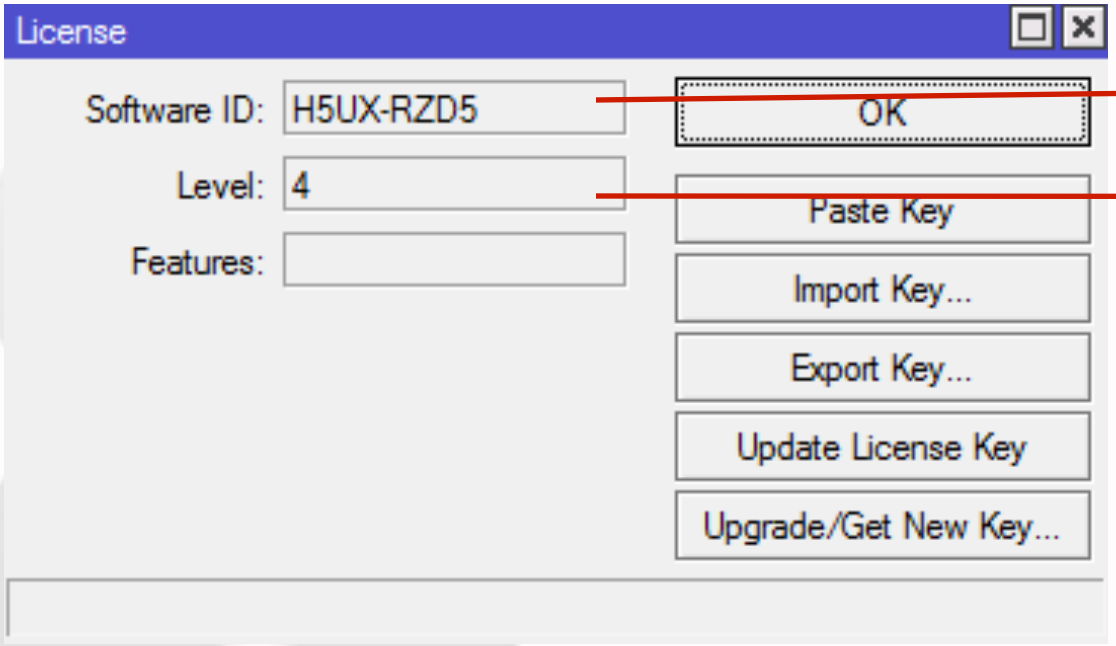
http://wiki.**mikrotik**.com/wiki/Manual:**License**

Coba lihat lisensi router pada menu System license

ID NETWORKERS
Expert Trainer & Consultant

Lisensi dan Batasan Upgrade Versi

- Lisensi menentukan versi berapa dari MikroTikOS yang dapat diinstall/ diupgrade di suatu hardware.
- L1 dan 2 mengijinkan upgrade 1 versi, L5 dan L6 mengijinkan upgrade sampai 2 versi.
- Silahkan lihat di menu System License



Software ID => unik hardware ID untuk saat membeli lisensi

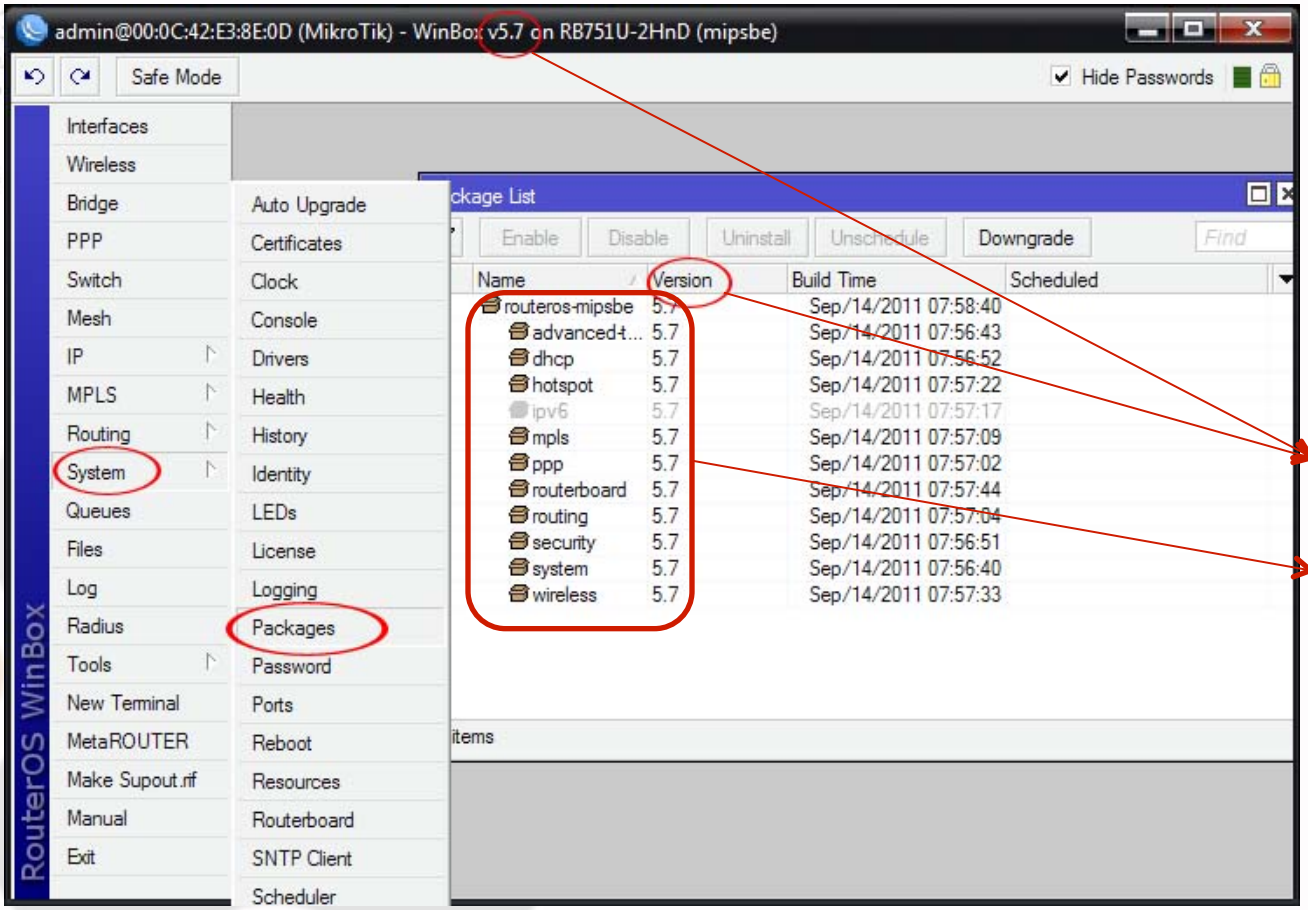
Lisensi Level

Versi MikroTik

- Fitur-fitur MikroTik selain ditentukan oleh lisensi yang digunakan, juga ditentukan oleh versi dari MikroTik yang terinstall.
- Pada RouterOS, versi MikroTik dapat dilihat dari paket yang terinstall.
- Paket yang terinstall menunjukkan fitur apa saja yang didukung oleh RouterOS.

Melihat Versi MikroTik

System>Packages



Versi MikroTik

Paket

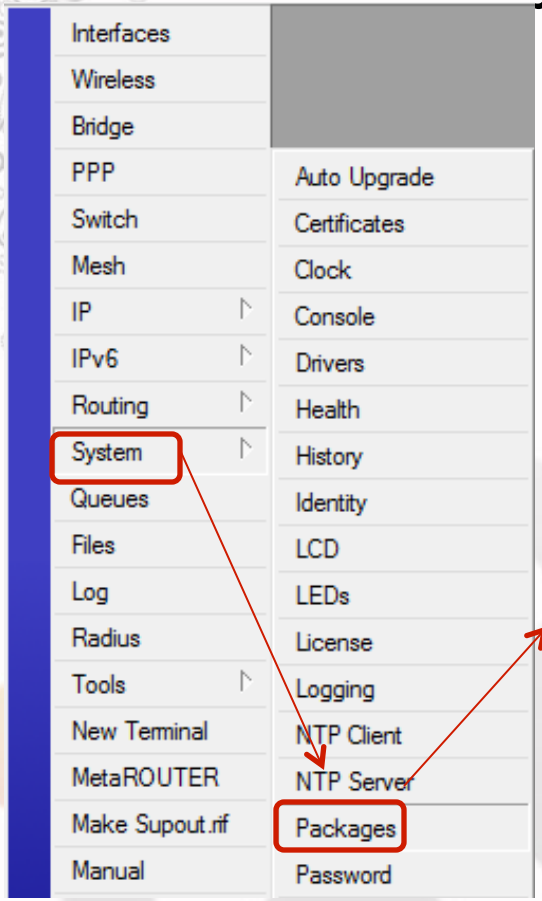
Paket – Fitur Paket

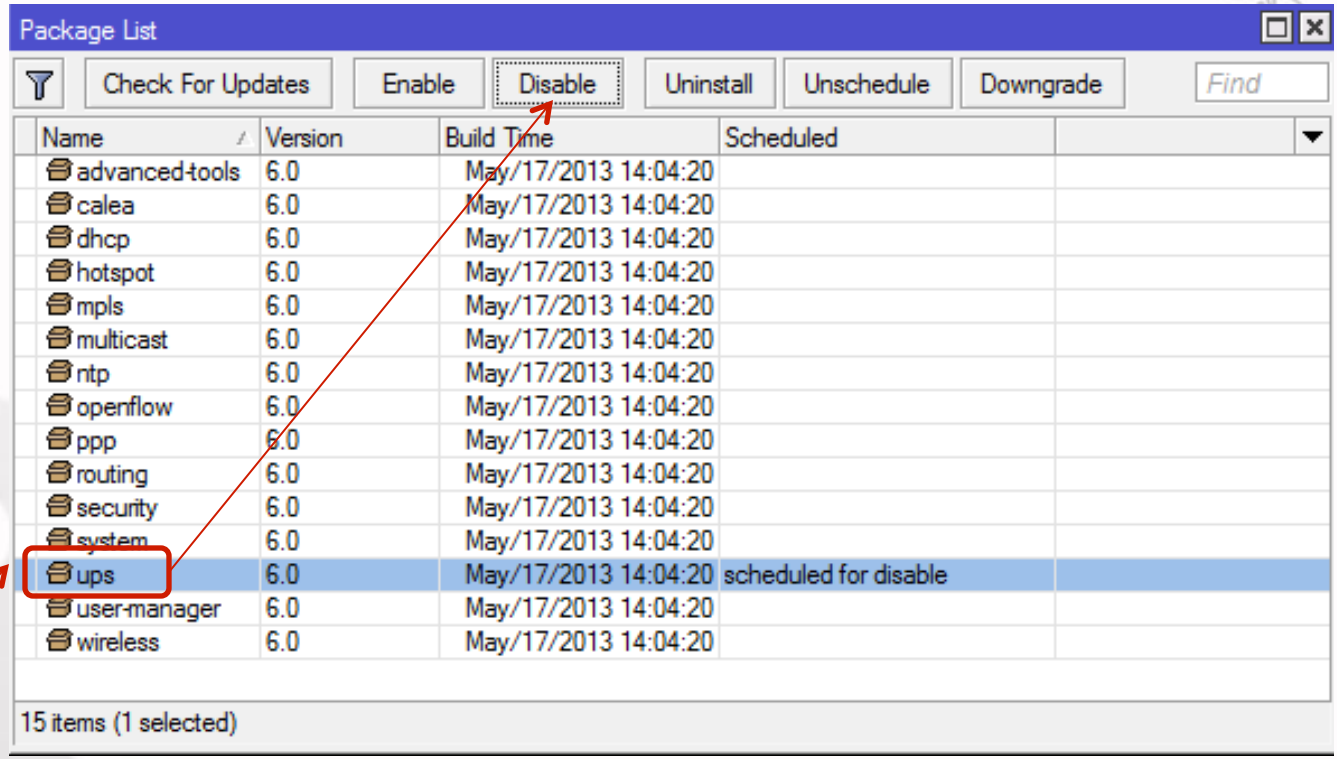
Package	Features
advanced-tools (*mipsle, mipsbe, ppc, x86*)	advanced ping tools. netwatch, ip-scan, sms tool, wake-on-LAN
calea (*mipsle, mipsbe, ppc, x86*)	data gathering tool for specific use due to "Communications Assistance for Law Enforcement Act" in USA
dhcp (*mipsle, mipsbe, ppc, x86*)	Dynamic 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

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

Package – Enable/Disable

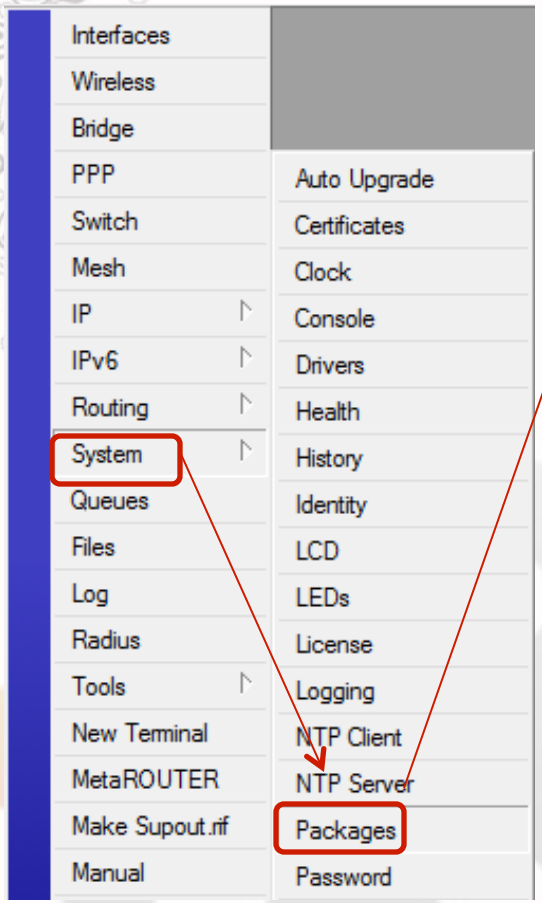
- Pada menu System> Package

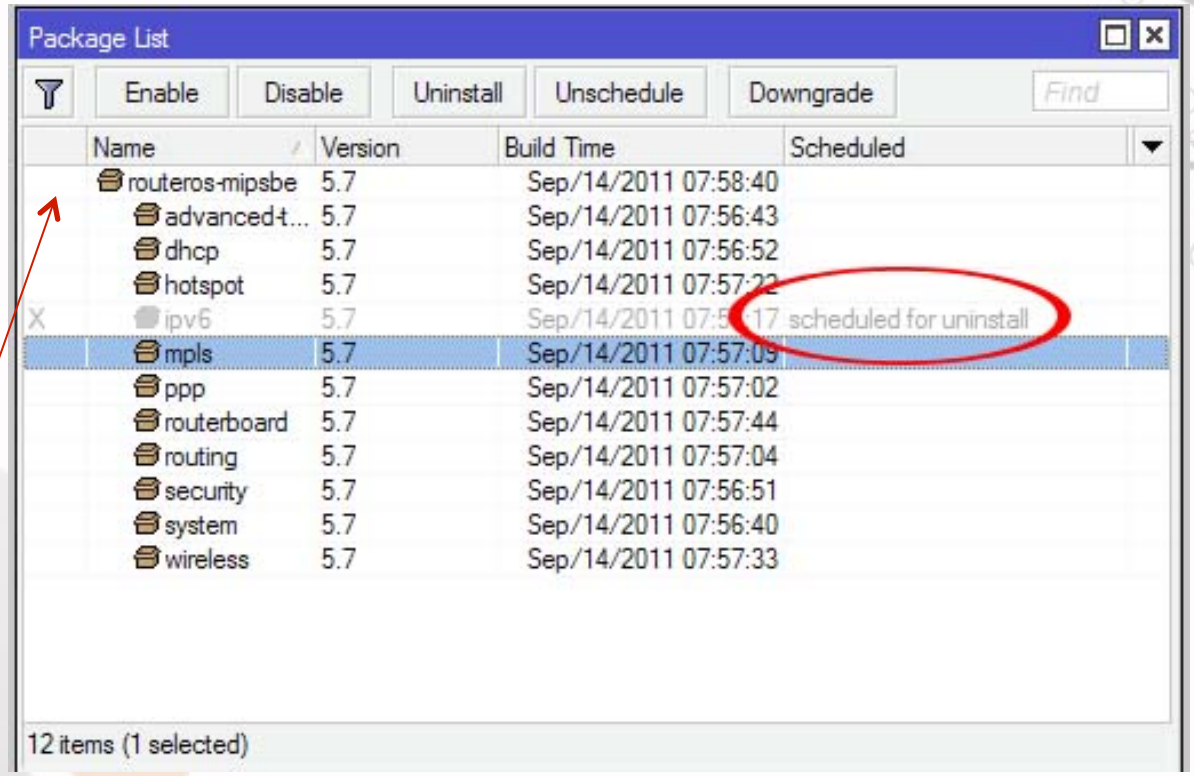




Package akan di disable setelah router di reboot

Paket – Uninstall

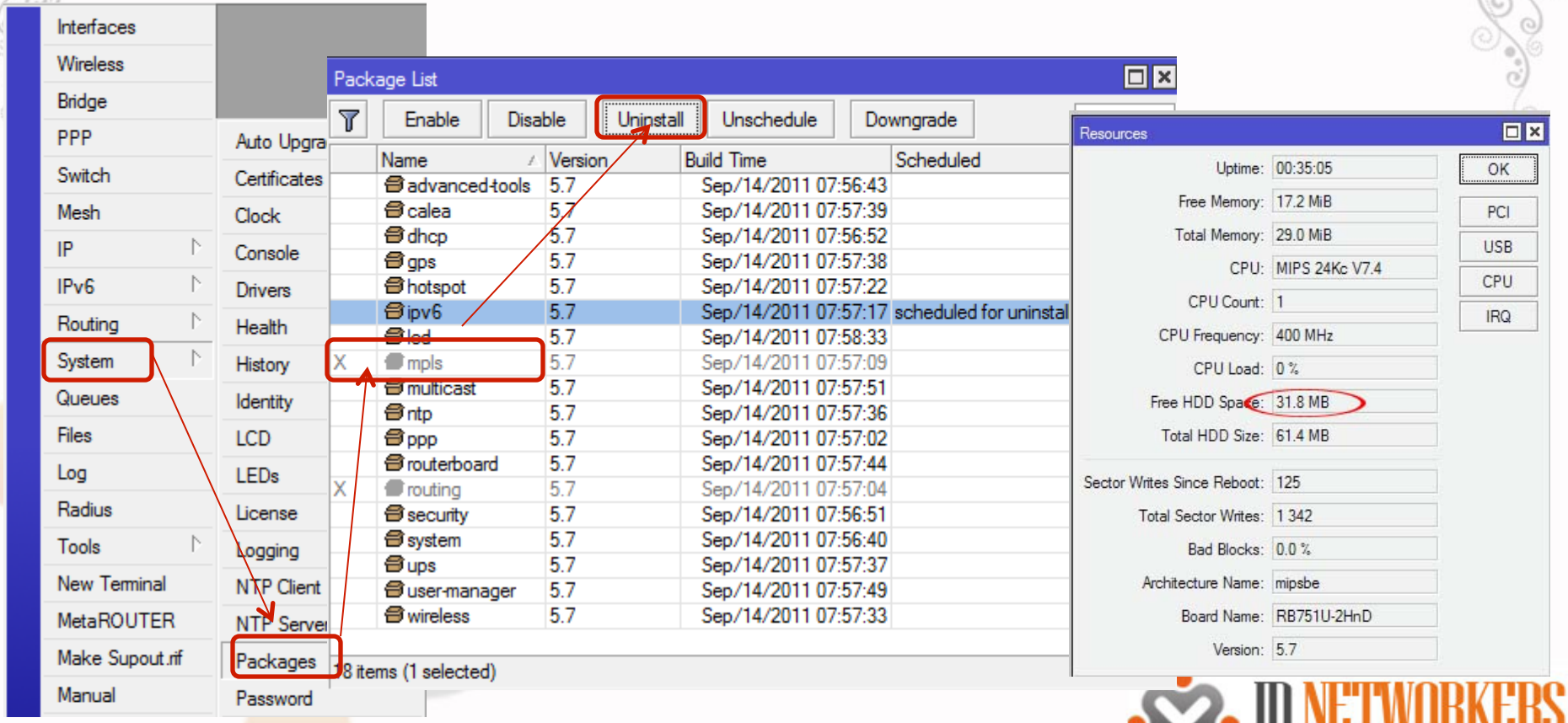




Package akan hilang setelah reboot router

LAB- Paket

- Uninstall mpls packets.
- Lihat kapasitas NAND (mendia penyimpanan) sebelum dan sesudah uninstall.

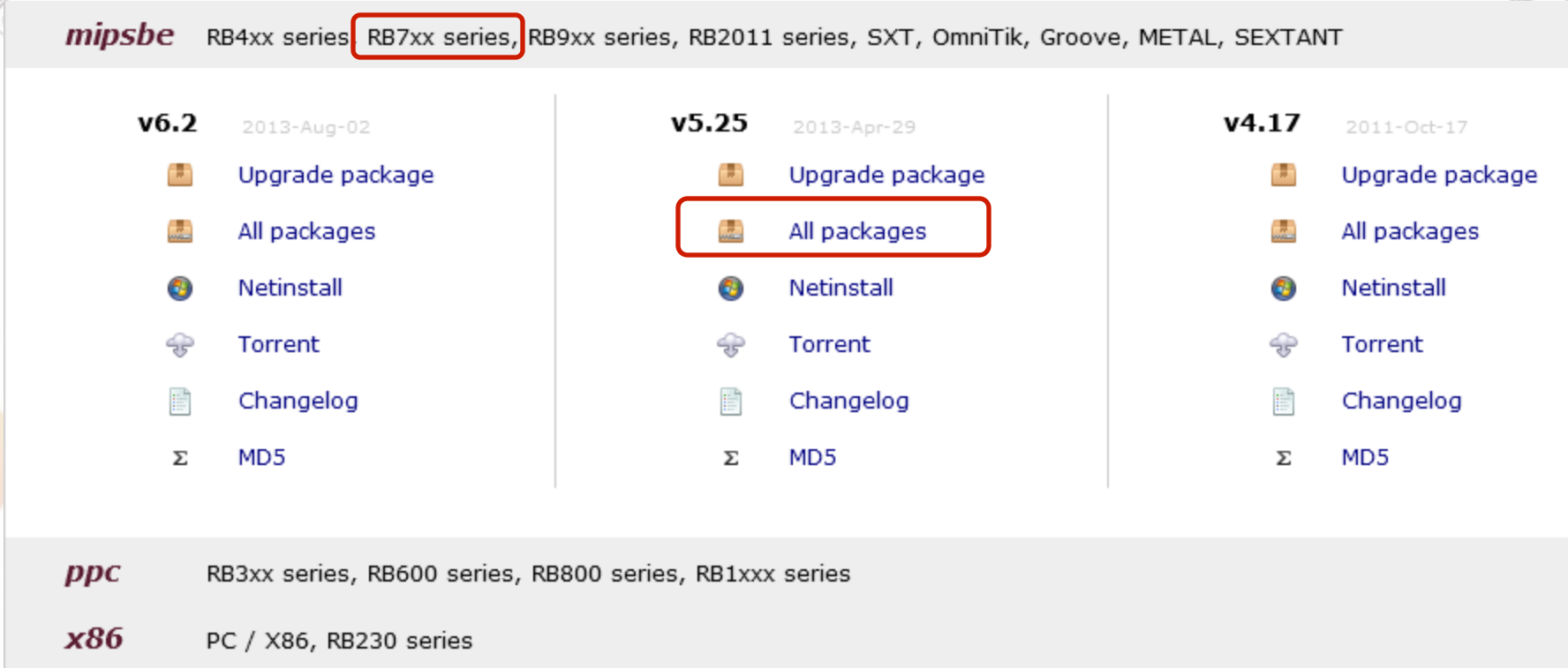


Paket – Upgrade / Downgrade

- Usahakan selalu upgrade versi terbaru, untuk fix bugs, new feature dll.
- Downgrade dilakukan apabila hardware kurang mendukung terhadap versi baru atau terdapat bug pada versi aktifnya.
- Upgrade paket harus memperhatikan aturan level dan lisensi yang berlaku.
- Upgrade dan downgrade juga harus memperhatikan kompatibilitas terhadap jenis arsitektur hardware.

LAB – Upgrade / Downgrade

- Pemilihan paket sangat penting dalam melakukan upgrade / downgrade, **jenis & arsitektur hardware** memiliki software yang berbeda.
- Bila ragu, dapat di crosschek dan didownload di www.mikrotik.com/download.html

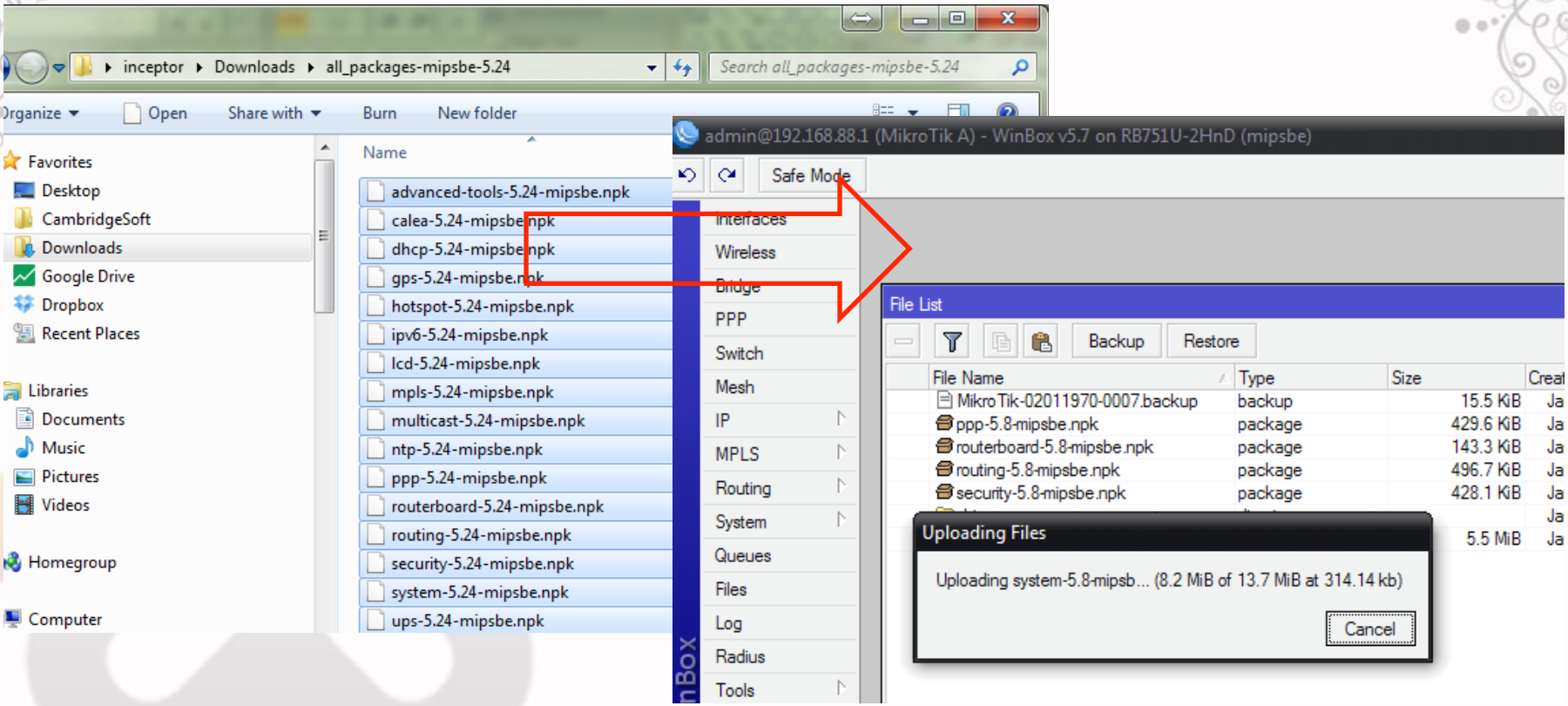


LAB – Mengupload Paket

- Paket yang akan diinstall (versi lama/baru) harus diupload terlebih dahulu ke router pada bagian file.
- Upload dapat dilakukan dengan **drag-and drop** (via winbox), ataupun via FTP client.
- Drag and drop menggunakan protocol winbox (tcp port 8291) untuk koneksi IP dan menggunakan frame untuk koneksi mac address.
- Apabila upload menggunakan FTP, pastikan semua packet terupload di folder utama, bukan di sub folder
- Untuk mengeksekusi upgrade, router harus direboot.

LAB – Mengupload Paket Baru

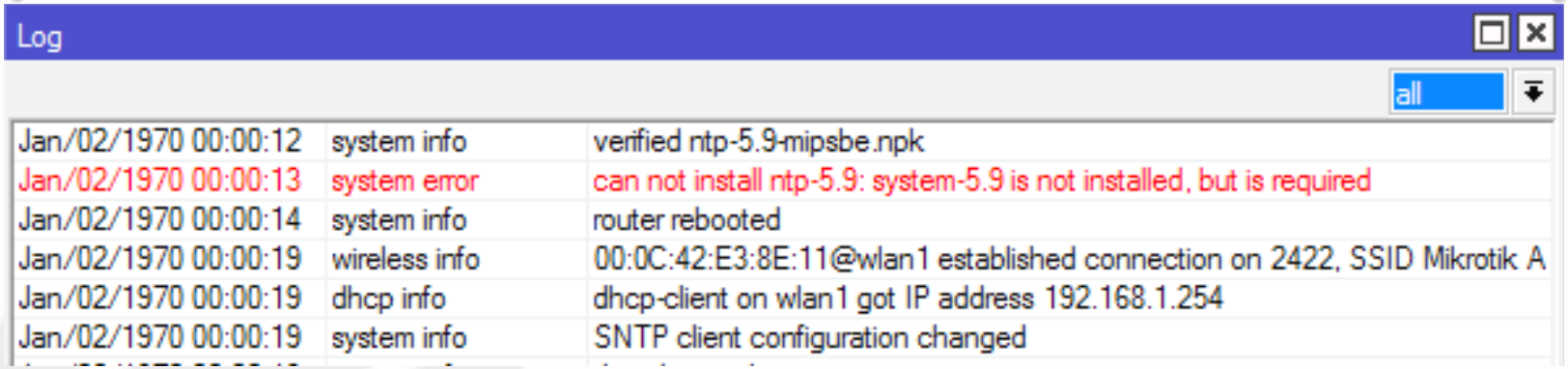
- Upgrade router anda ke versi terbaru.
- Download versi terbaru dari web mikrotik.com
- Drag and drop file-file *.npk ke jendela winbox.



- Reboot setelah selesai upload, dan lihat hasilnya.

LAB – Mengupload Paket Baru

Cek log untuk melihat apabila ada error, berikut adalah contoh apabila ada error



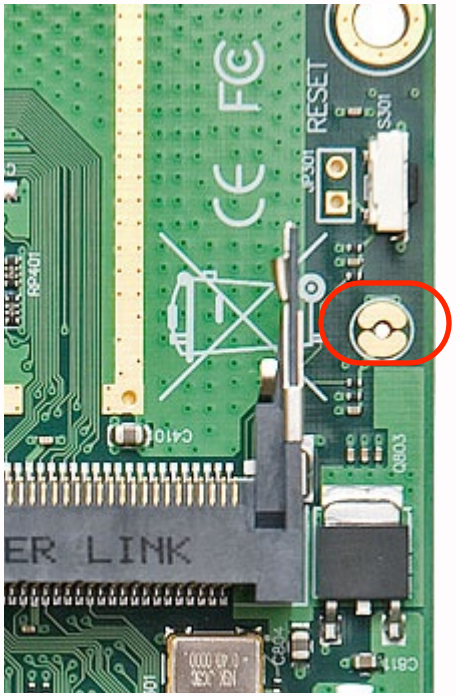
Cek kembali pada menu System>package untuk melihat update pacet yang telah kita lakukan

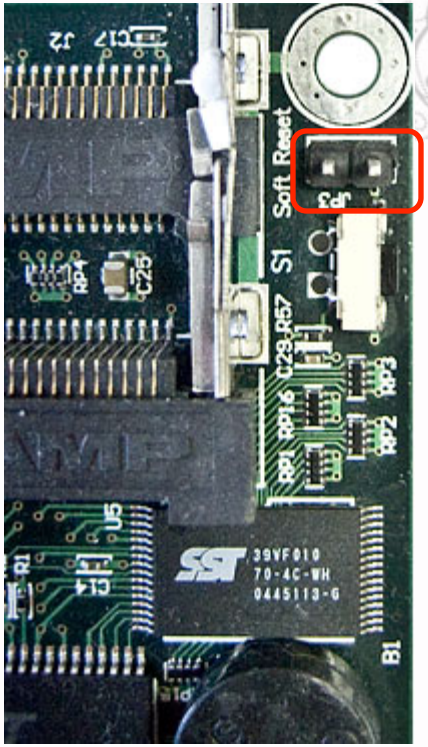
Reset Konfigurasi

- Reset konfigurasi MikroTik diperlukan jika:
  - Saat lupa username dan atau password
  - Saat konfigurasi terlalu komplek dan perlu ditata dari nol.
- Reset konfigurasi dapat dilakukan dengan cara:
  - Hard Reset, reset secara fisik.
  - Soft reset, reset secara software.
  - Install ulang.

Hard Reset

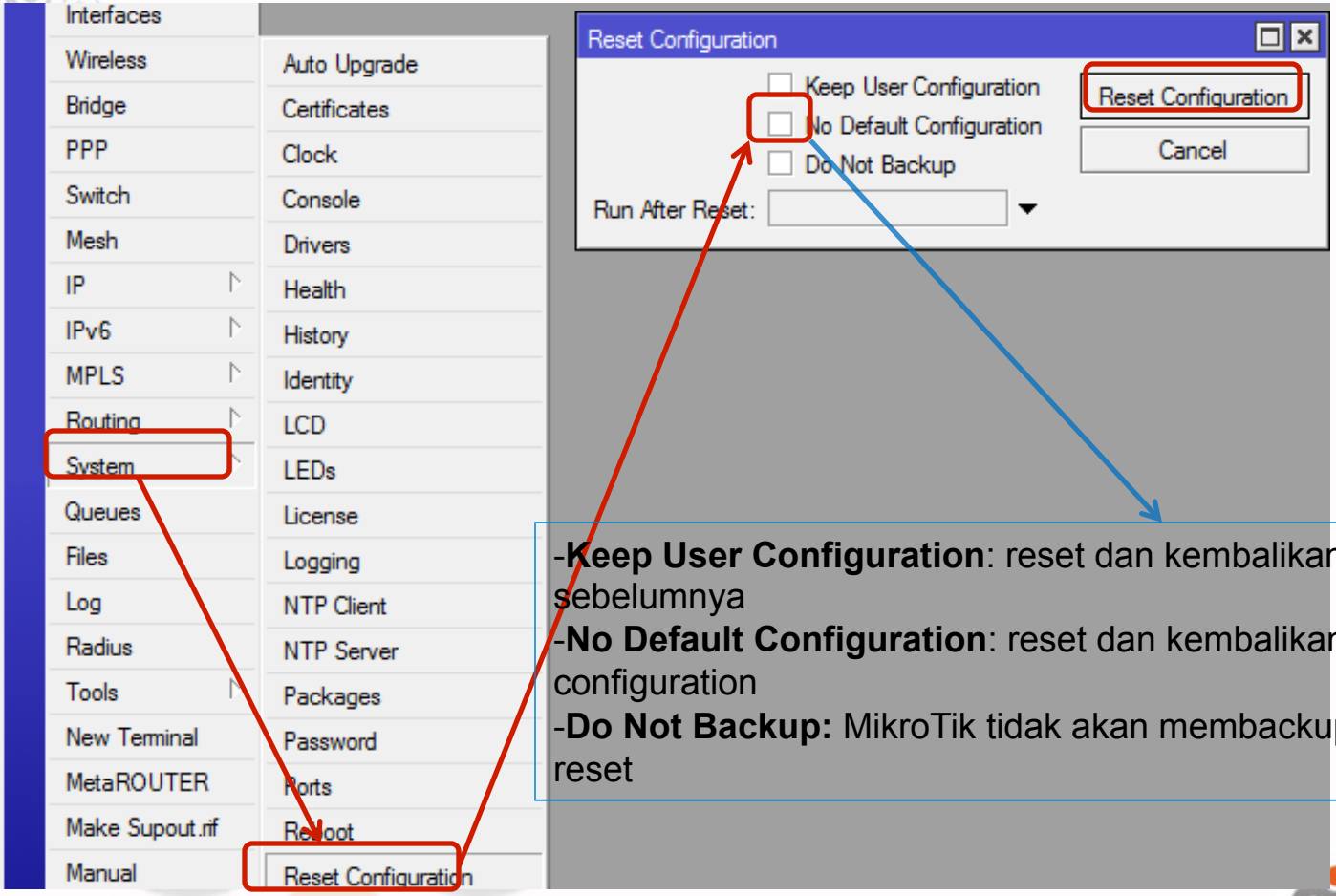
- Khusus RouterBoard memiliki rangkaian untuk reset pada board dengan cara menjumper sambil menyalakan RB, RB akan kembali ke konfigurasi awal/default.





Soft Reset

- Jika kita masih bisa akses ke MikroTik, lakukan reset lewat reset menu

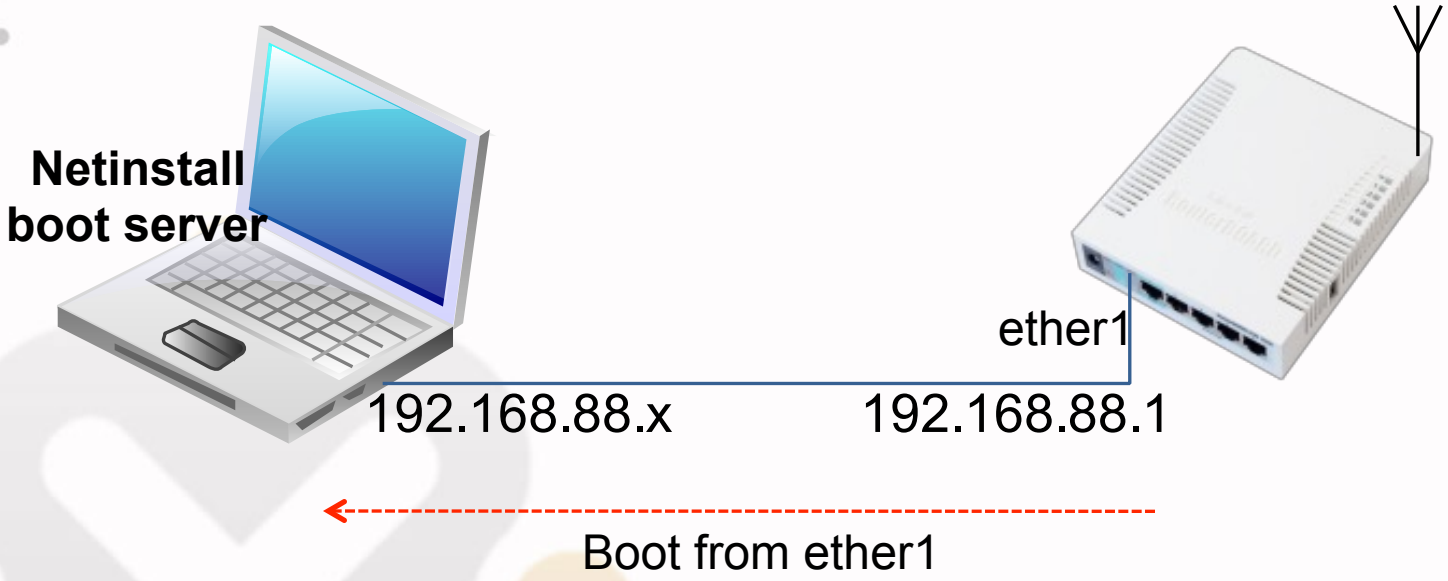


-**Keep User Configuration**: reset dan kembalikan ke konfigurasi sebelumnya
-**No Default Configuration**: reset dan kembalikan ke factory default configuration
-**Do Not Backup:** MikroTik tidak akan membackup configurasi pada proses reset

Install Ulang

- Mikrotik dapat di install ulaang lyaknya operating system yang lain
- Install ulang dapat mengembalikan mikrotik ke posisi awal/default.
- Install dapat dilakukan menggunakan media CD dan software Netinstall.
- RouterBOARD hanya dapat diinstall ulang menggunakan software Netinstall.

Install Ulang



Install Ulang via Netinstall

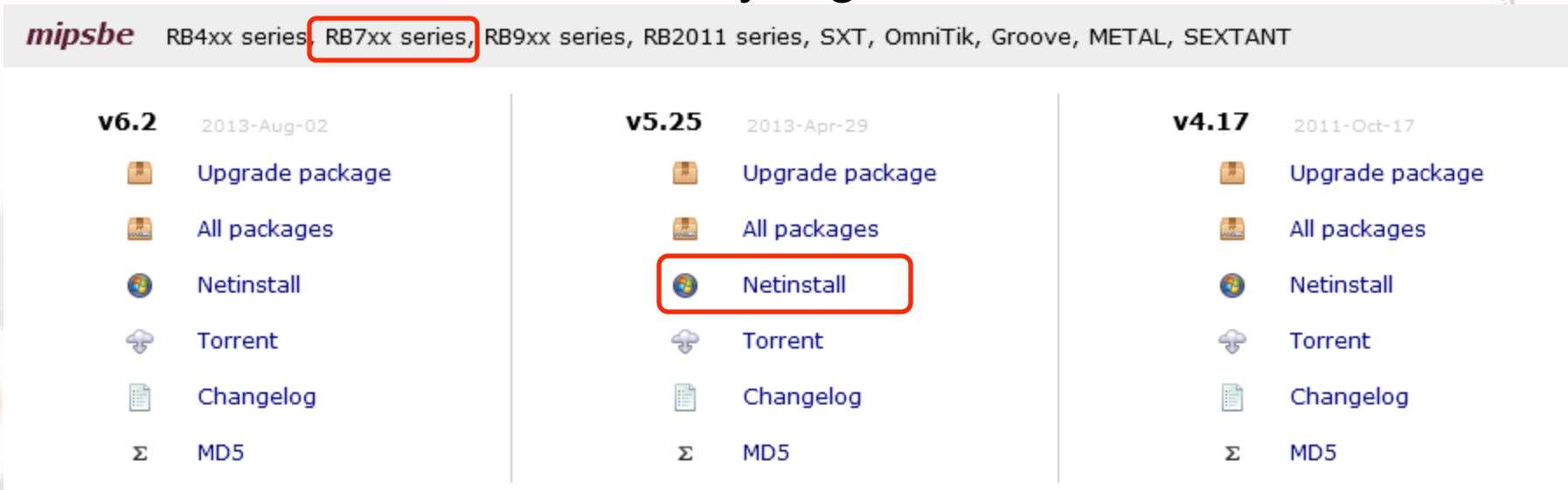
- RB harus dikoneksikan dengan laptop/PC melalui primary ethernetnya (ether1)
- Laptop/PC harus menjalankan program netinstall
- RB harus disetting agar booting dari network/ jaringan (ether1), dengan cara:
  - Setting via serial console
  - Setting via terminal console
  - Winbox
  - Tekan tombol reset

NetInstall

- Software yang running under windows.
- Digunakan untuk install dan reinstall RouterOS
- Digunakan untuk reset password.
- PC/Laptop yang menjalankan netinstall harus terhubung langsung dengan router melalui kabel UTP atau LAN.
- Software netinstall dapat didownload di web resmi MikroTik.

LAB – Reinstall RB 751

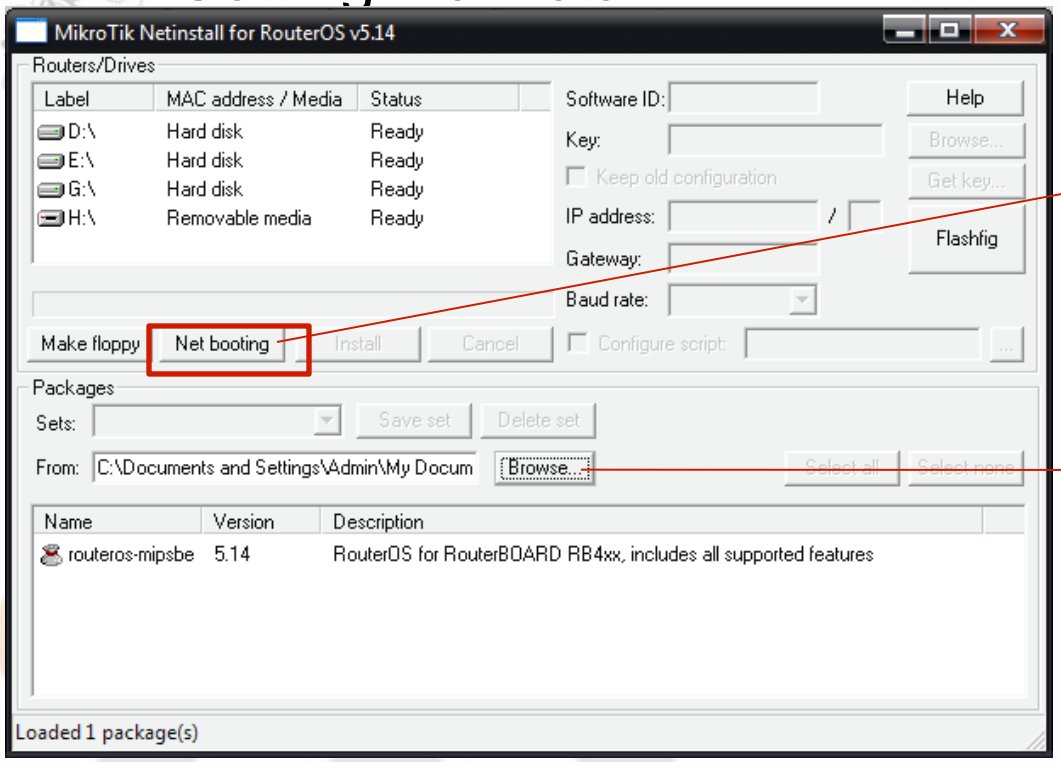
- Download RouterOS dan Software Netinstall terbaru di http://www.mikrotik.com/download.html
- Pilih untuk seri routerboard yang sesuai

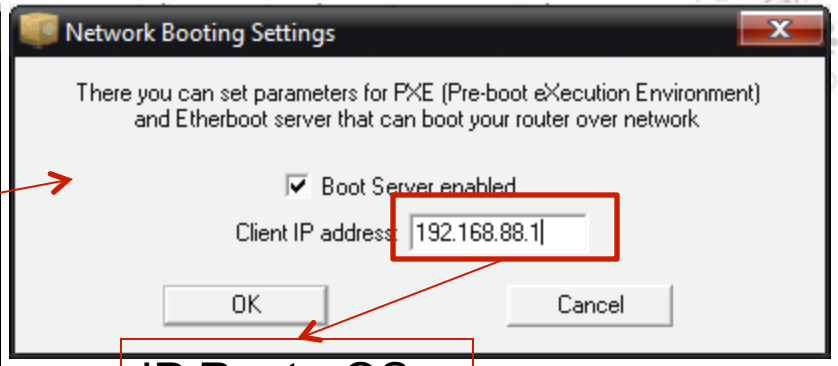


- Koneksikan laptop dengan Routerboard di ether1 dan pastikan bisa ping

LAB – Reinstall RB 751

- Setting Netinstall



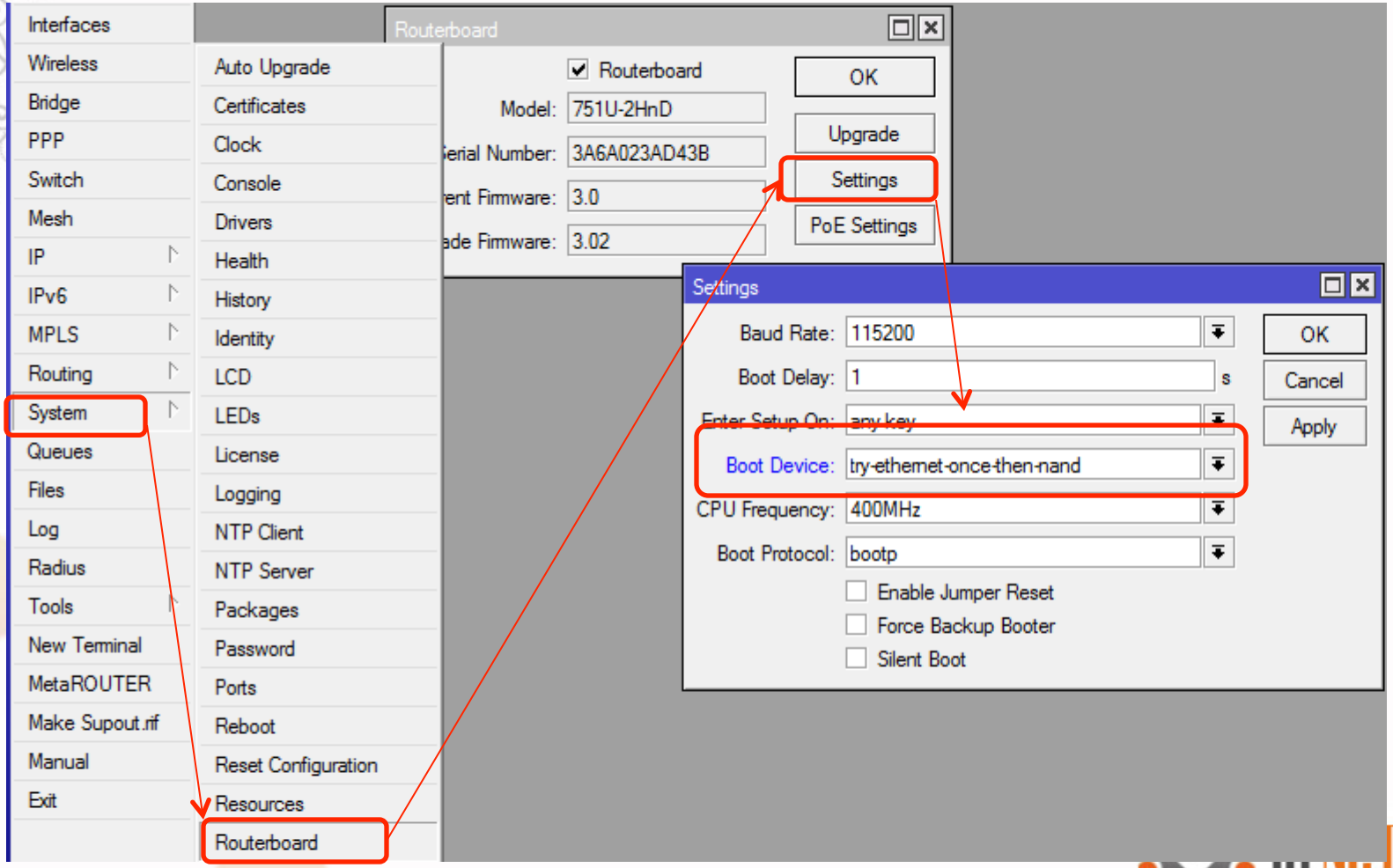


IP RouterOS

Arahkan ke folder dimana paket (file npk) routeros disimpan di laptop kita

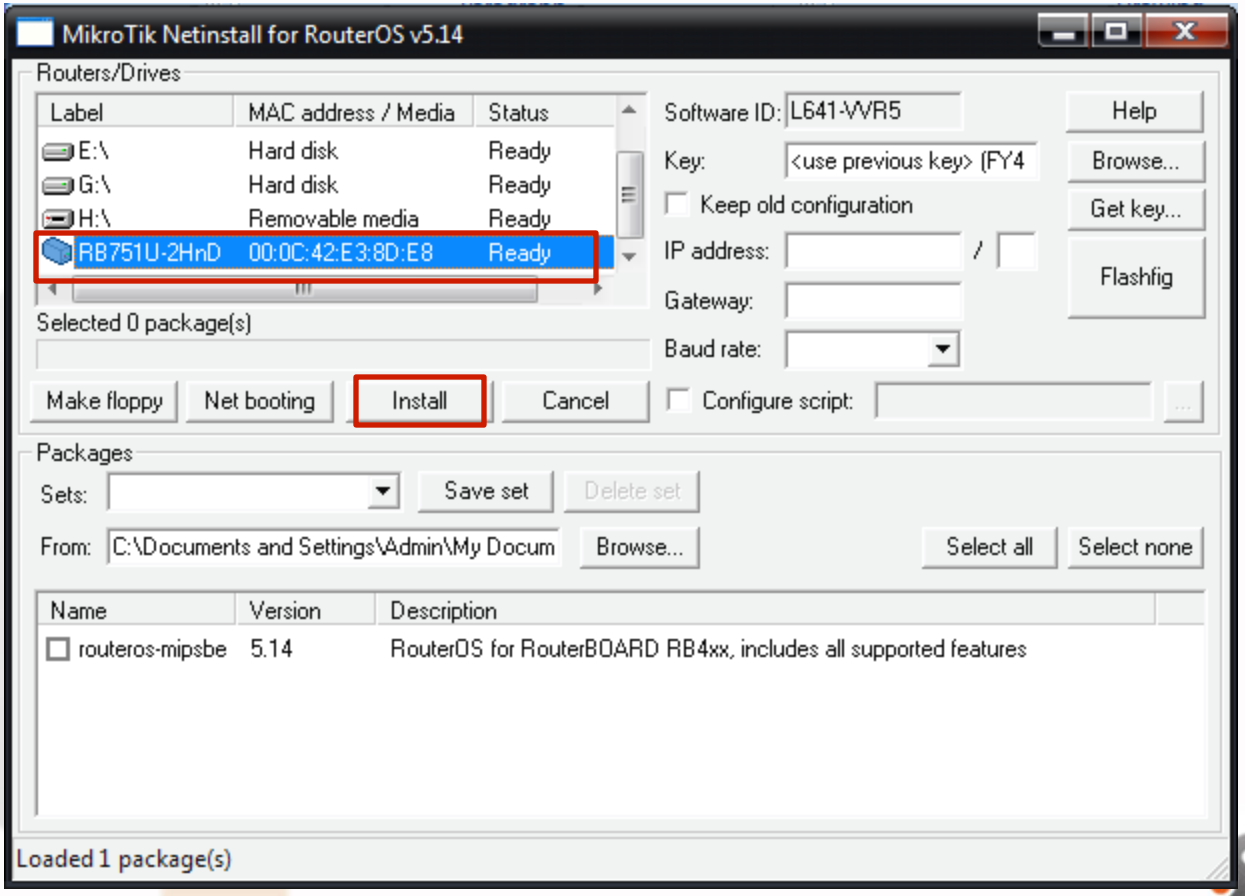
Setting BIOS via winbox

Seting boot device MikroTik ada di menu System>Routerboard>Setting>Boot Device (Try-ethernet-once-then-nand)



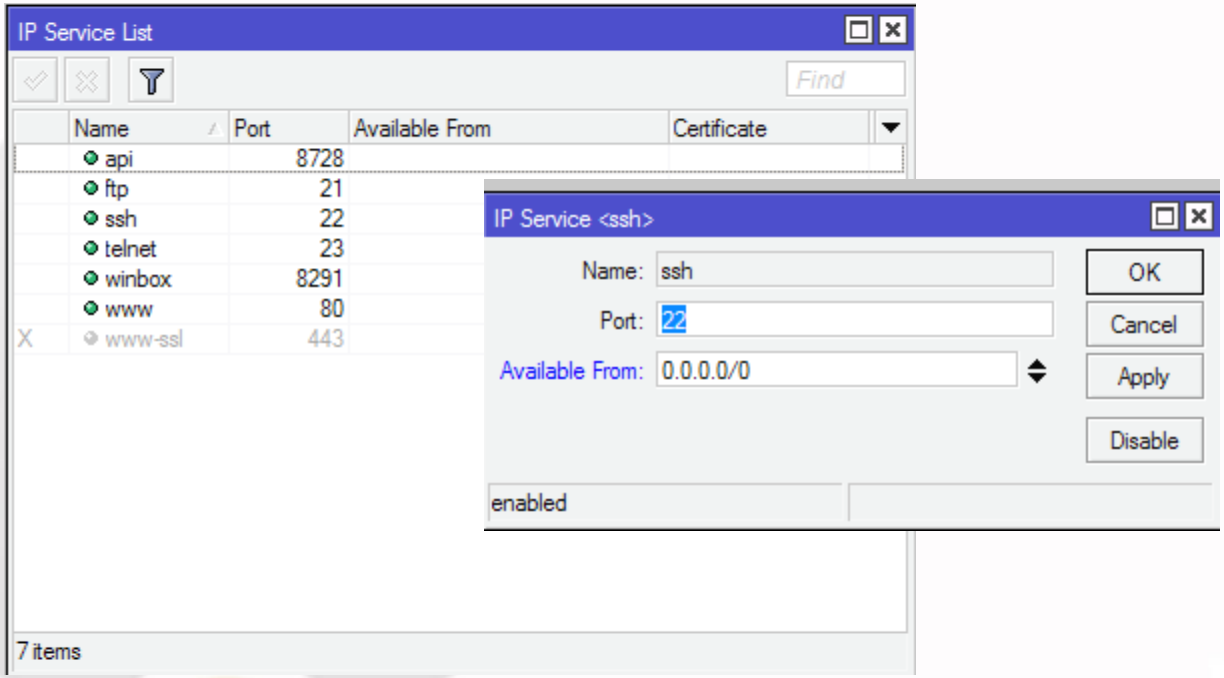
LAB – Reinstall RB 751

- Reboot router melalui system reboot, sampai terdeteksi 1 device mikrotik di netinstallnya
- Klik install, untuk memulai installasi



IP Services

- Menghidukan/mematikan service yang dijalankan oleh Router.
- Setting konfigurasinya ada di menu IP>Services
- Untuk keamanan kita juga dapat mengganti/mengubah default port pada masing-masing services

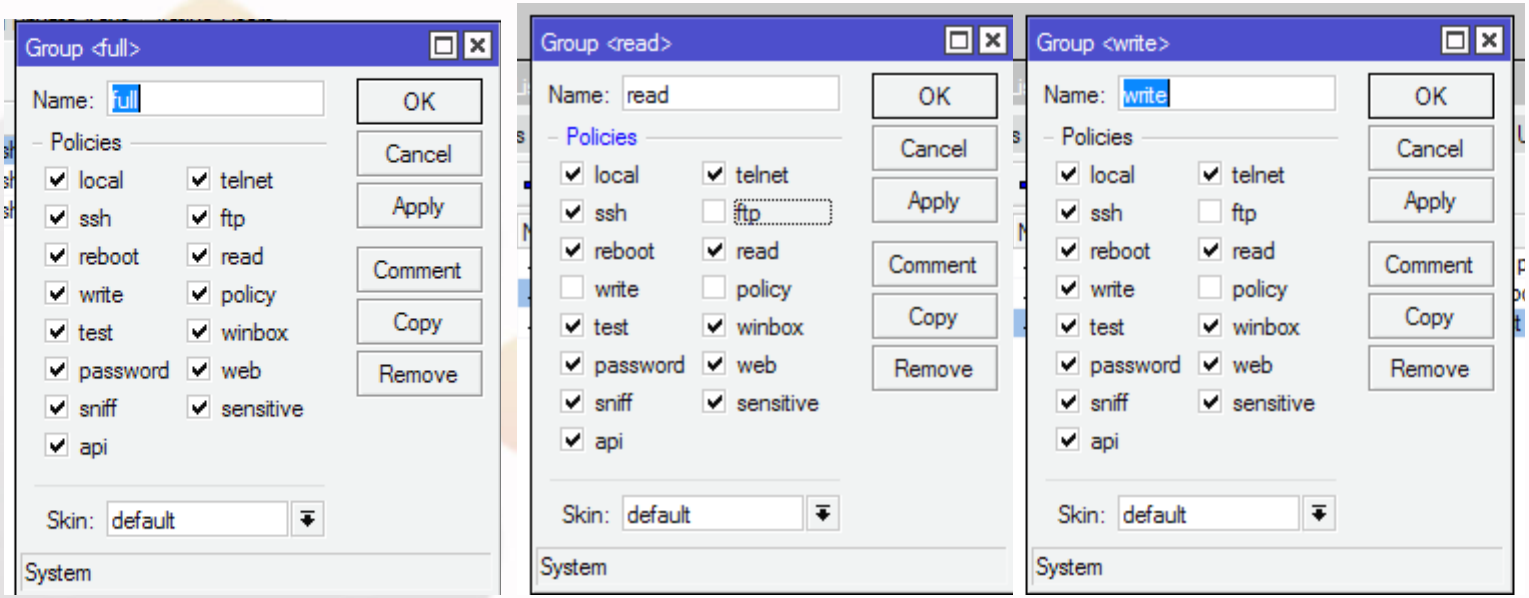


User Login Management

- Akses ke router ditentukan oleh menu user.
- Manajemen user dilakukan dengan
  - GROUP – profil pengelompokan user, menentukan previlage yang bisa diperoleh suatu user.
  - USER – merupakan login (username & password dari suatu user.
- Sesi user yang sedang melakukan koneksi ke router dapat dilihat pada menu System>Users>Active Users

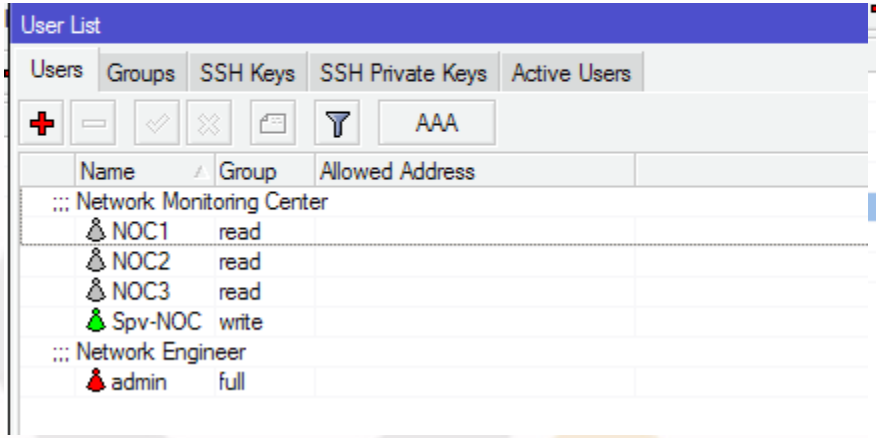
User Login Management - Group

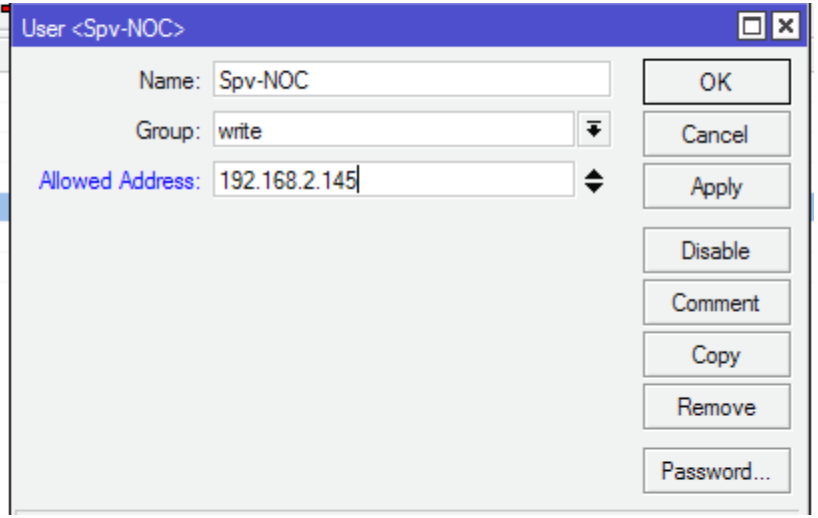
- Group merupakan pengelompokan previlage/hak akses yang akan diberikan pada user.
- Ada 3 default previlage yang ada di MikroTik yaitu full, read dan write, namun diperbolehkan untuk customize sendiri.



User Login Management - Akses

- Masing-masing user dapat dibatasi hak aksesnya berdasarkan group.
- Masing-masing user juga dapat dibatasi berdasarkan IP address yang digunakannya.
- Misalkan si A hanya boleh login dengan IP A, atau hanya boleh dari network A.

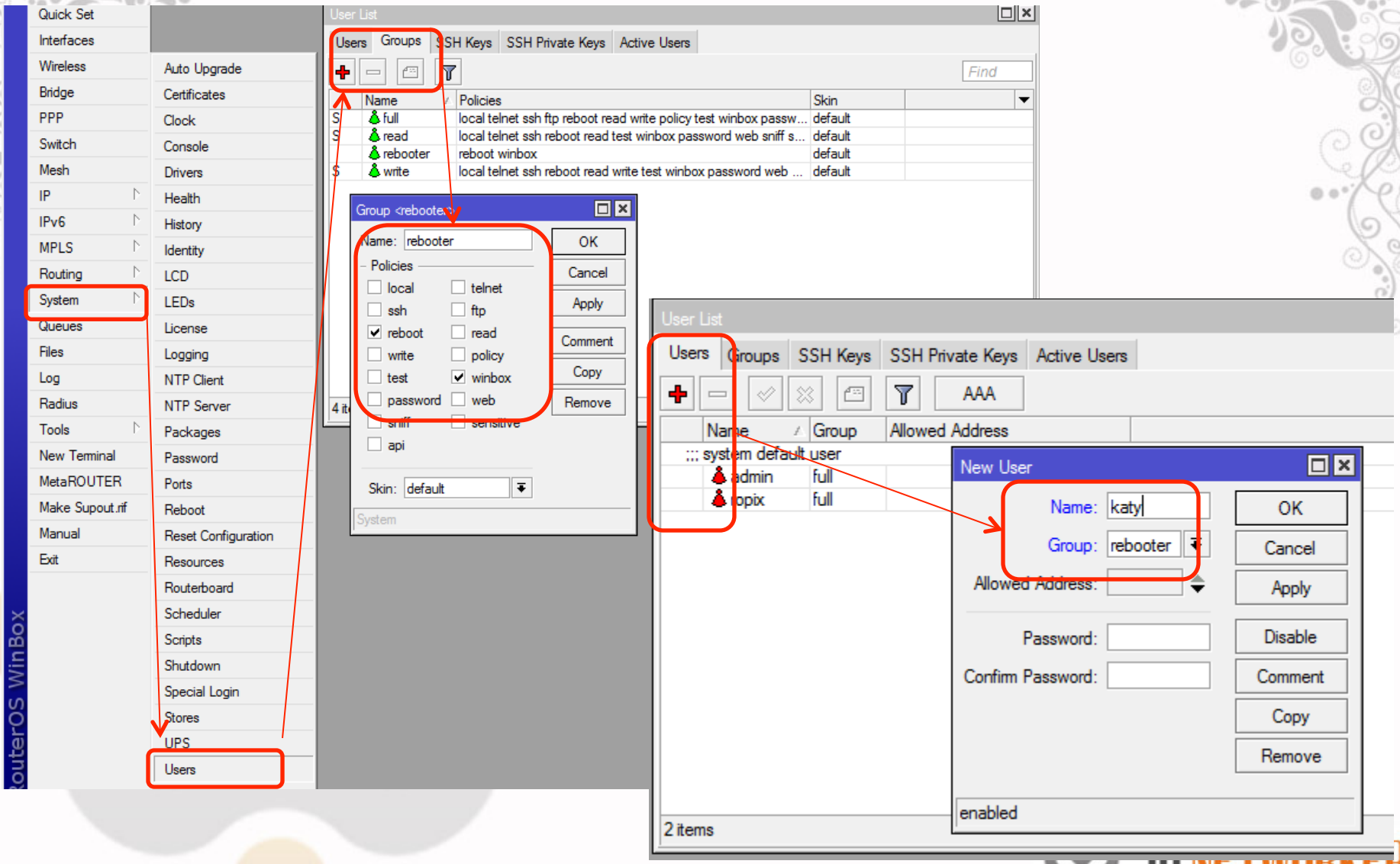




LAB - User Login Management

- Buatlah satu user dengan nama “katy”
- Berikan previlage agar user katy hanya bisa melakukan reboot router via winbox
- Caranya adalah, buat group dulu dengan previlage reboot dan winbox, baru setelah itu buat user katy dengan group reboot.

LAB - User Login Management



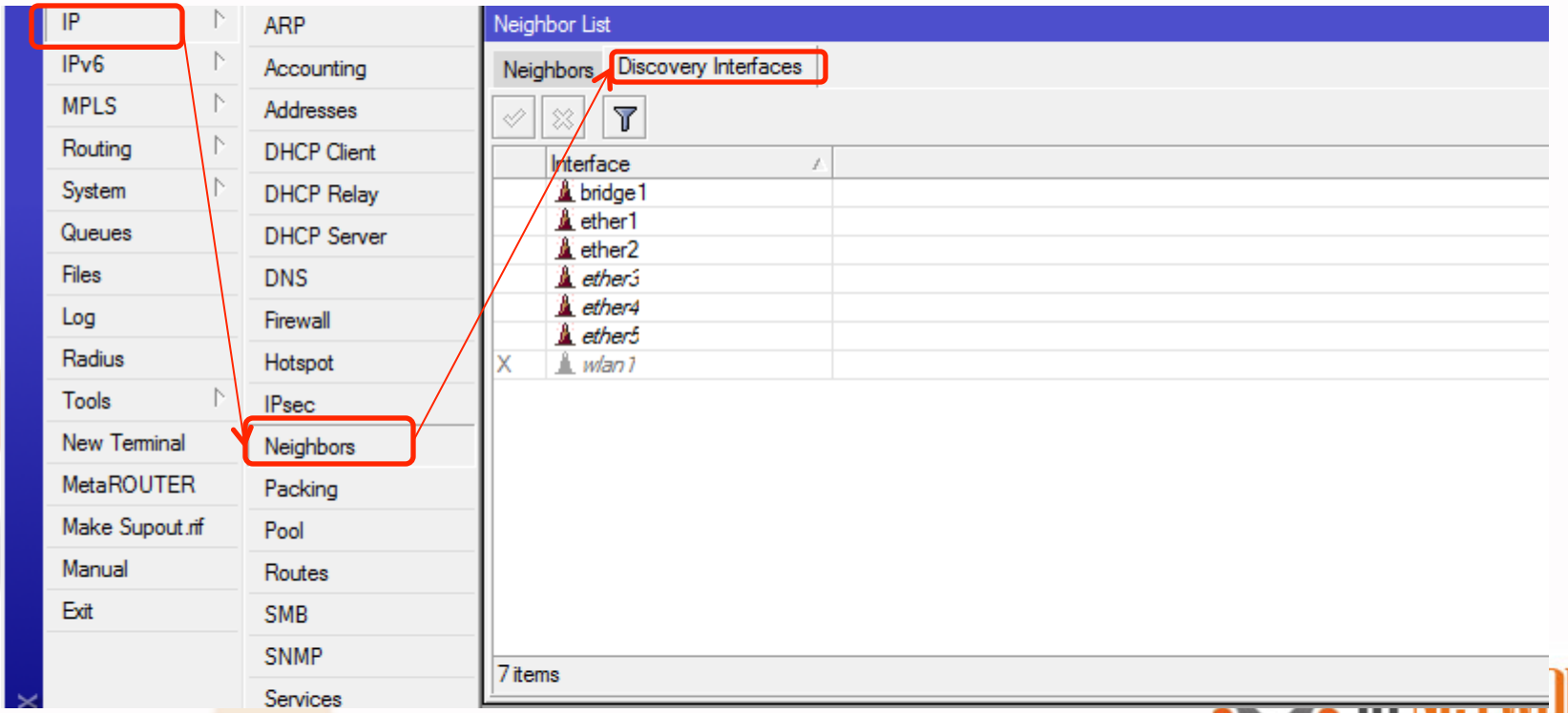
MikroTik Neighbor Discovery Protocol (MNDP)

- MNDP memudahkan konfigurasi dan manajemen jaringan dengan memungkinkan setiap router MikroTik untuk mendeteksi MikroTik lainnya yang terhubung langsung
- MNDP fitur:
  - bekerja pada layer 2
  - bekerja pada semua non-dinamic interface
  - mendistribusikan informasi dasar
- MNDP dapat berkomunikasi dengan CDP (Cisco Discovery Protocol).
- Disarankan untuk tidak memancarkan MNDP ke interface yang mengarah ke jaringan public.

Block MNDP

Untuk menyembunyikan mikrotik anda agar tidak muncul pada Winbox MNDP scan, atau muncul pada neigbors:

1. Disable MNDP pada menu **IP Neighbors Discovery**
2. Block Port UDP protocol port 5678 (port untuk komunikasi MNDP) menggunakan **IP Firewall Filter Rule**



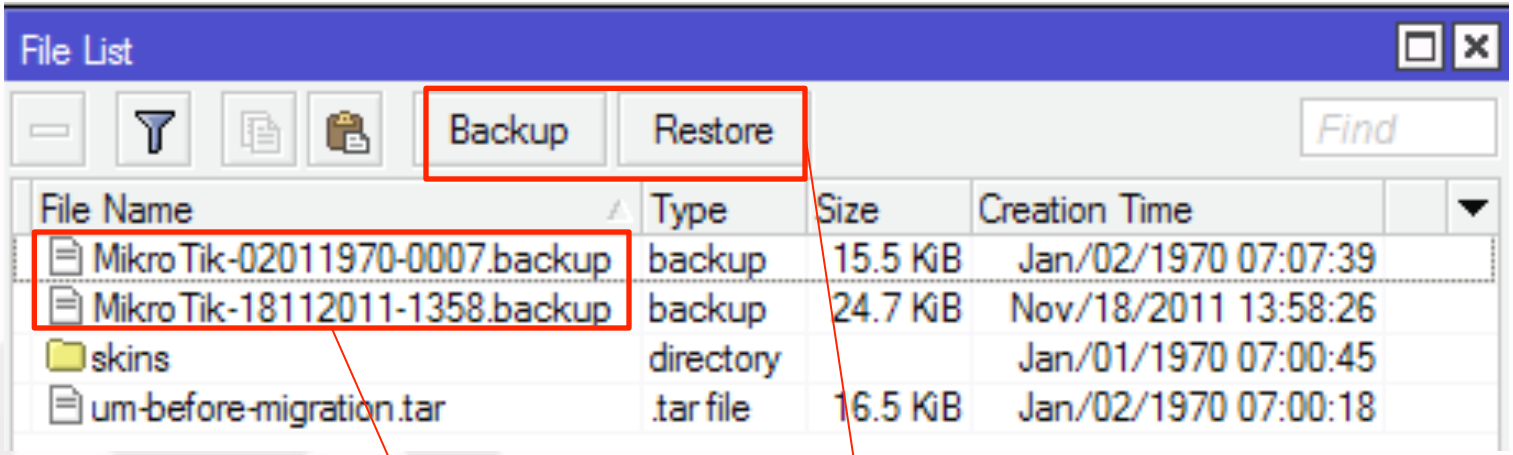
Backup dan Restore

- Konfigurasi dalam router dapat dibackup dan disimpan untuk digunakan di kemudian hari. Ada 2 jenis backup yaitu

1. **Binary file (.backup)**
   - ✓ **Tidak dapat dibaca** text editor.
   - ✓ Membackup **keseluruhan konfigurasi** router
   - ✓ Create return point (dapat kembali seperti semula)
2. **Script file (.rsc)**
   - ✓ Berupa script, **dapat dibaca** dengan text editor.
   - ✓ Dapat membackup **sebagian atau keseluruhan konfigurasi** router.
   - ✓ Tidak mengembalikan ke konfigurasi seperti semula, melainkan menambahkan script tertentu pada konfigurasi utama.

Binary – Backup & Restore

- Backup ada pada menu File>backup



Format backup file:
MikroTik-[tanggal][bulan][tahun]-[jam][menit]
File dapat disimpan di PC dengan cara drag-and-drop atau FTP

1. Tombol backup digunakan untuk backup konfigurasi router aktual.
2. Tombol restore digunakan untuk mengembalikan konfigurasi sesuai dengan file yang dipilih.

Binary – Backup & Restore

- Binary backup dan restore juga dapat dilakukan menggunakan terminal.
- Backup via teminal kelebihanya adalah dapat memberi nama file backup sesuai dengan keinginan kita

```
[admin@MikroTik A] > system backup save name=bakup_18_nov_11
Saving system configuration
Configuration backup saved
[admin@MikroTik A] > file print
 # NAME            TYPE                                SIZE CREATION-TIME
 0 um-before-mi... .tar file                         16 896 jan/02/1970 07:00:18
 1 skins           directory                                jan/01/1970 07:00:45
 2 MikroTik-181... backup                            25 338 nov/18/2011 13:58:26
 3 MikroTik-020... backup                            15 865 jan/02/1970 07:07:39
 4 bakup_18_nov... backup                            25 338 nov/18/2011 14:10:52
[admin@MikroTik A] >
```

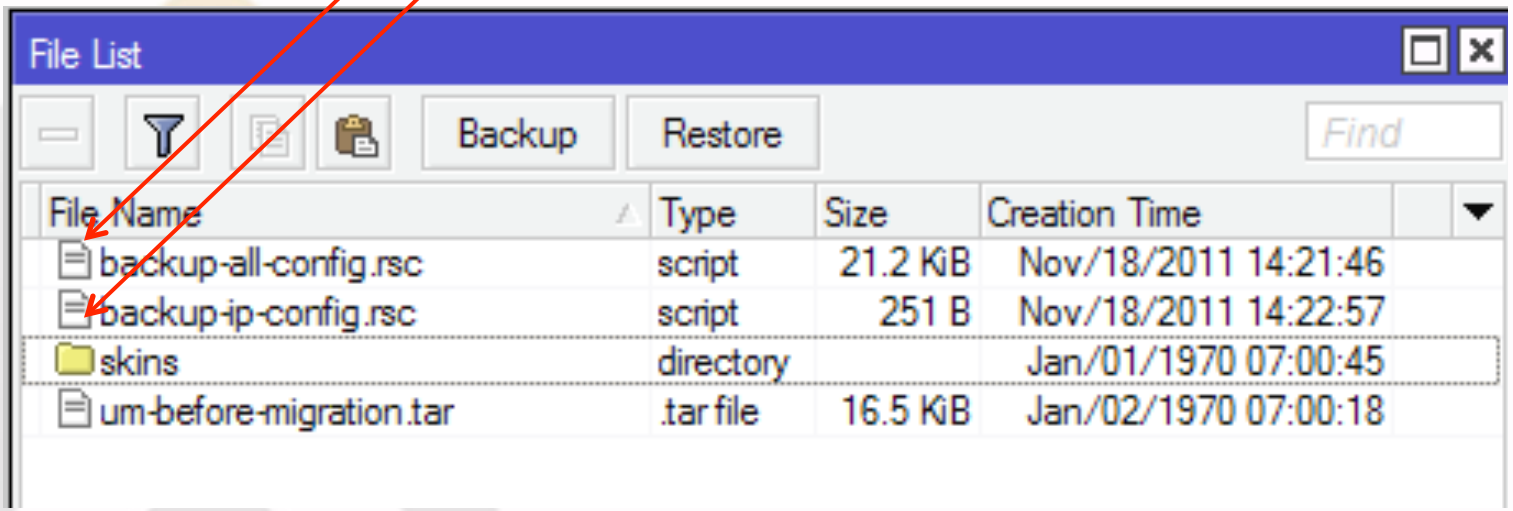
Script – Backup & Restore

- Backup dan restore dengan mode script dilakukan dengan perintah:
  - EXPORT akan menyimpan konfigurasi dengan bentuk script yang dapat dibaca dan diolah.
  - IMPORT akan menjalankan perintah yang terdapat dalam script.
- IMPORT/EXPORT dapat digunakan untuk membackup sebagian konfigurasi.
- IMPORT/EXPORT harus dilakukan melalui terminal.
- EXPORT tidak menyimpan username password

Script – Backup & Restore

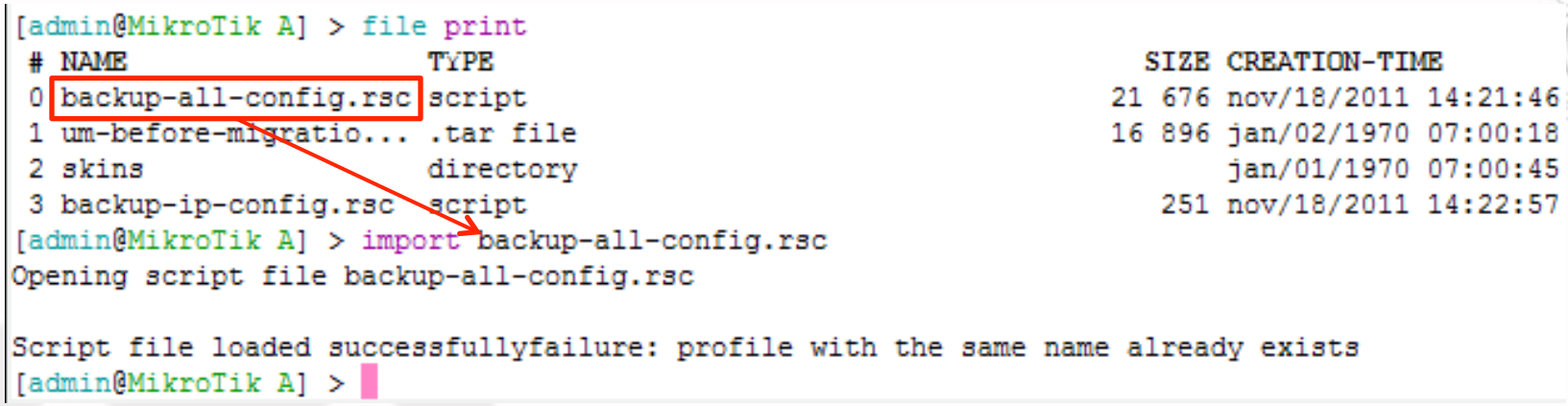
- Perintah EXPORT

```
[admin@MikroTik A] > export file=backup-all-config
[admin@MikroTik A] > /ip address export file=backup-ip-config
[admin@MikroTik A] >
```



Script – Backup & Restore

- Perintah IMPORT



Perbedaan Export & Backup

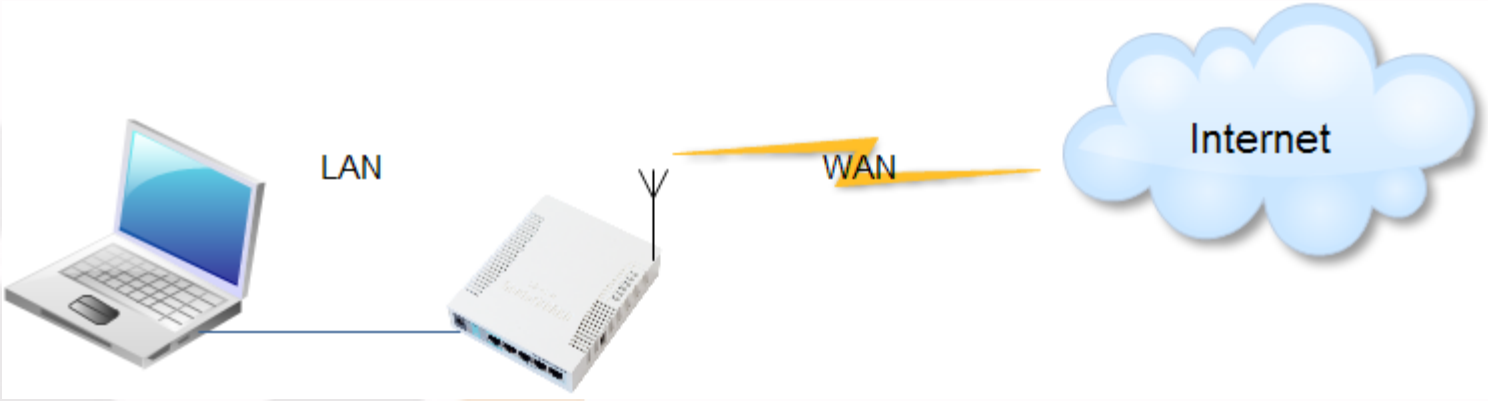
Perbedaan	Script Backup	Binnary Backup
Command	Export / Import	Backup / Restore
Bisa dengan menu klik	No	Yes
Backup all config	No (user&Pass)	Yes
Need reboot to restore	No	Yes
Backup sebagian config	Yes	No
Bisa dibaca test editor	Yes	No

LAB - Backup & Restore

- Buatlah backup konfigurasi dengan perintah backup dan export.
- Pindahkan file backup dan rsc ke komputer/ laptop.
- Coba buka dan edit file backup dan file rsc tersebut

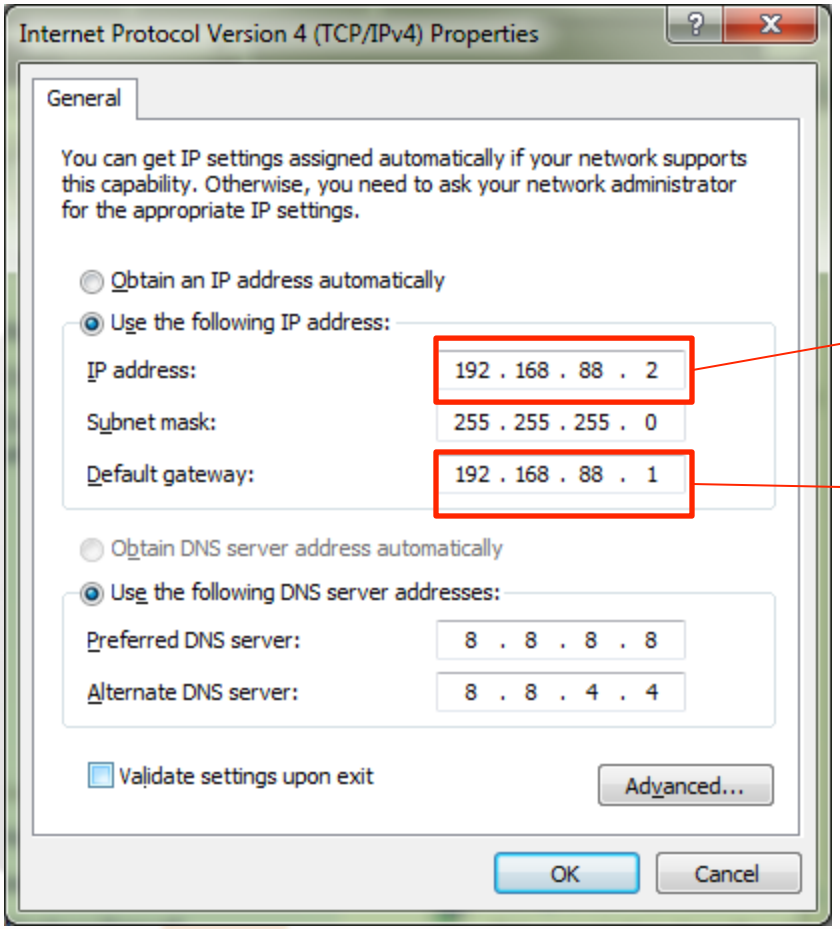
LAB – Koneksi Internet

- Ini adalah simulasi jaringan dasar untuk koneksi internet
- Setting koneksi internet menggunakan mikrotik sebagai Network Address Translation (NAT).



Konfigurasi LAN

- Setting IP pada Ethernet Laptop

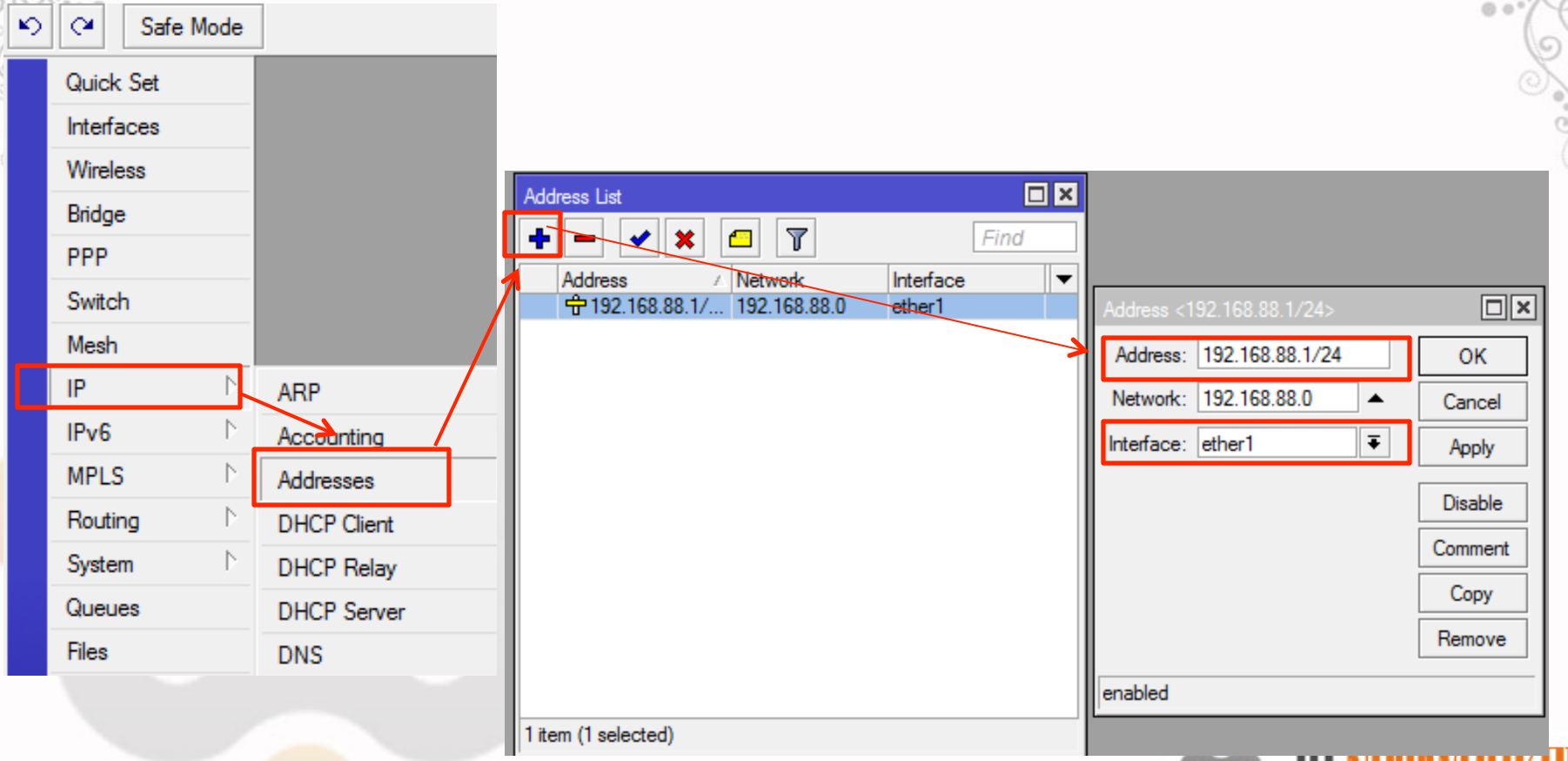


IP Laptop satu network dengan IP Mikrotik LAN

Gateway Laptop adalah IP interface mikrotik LAN

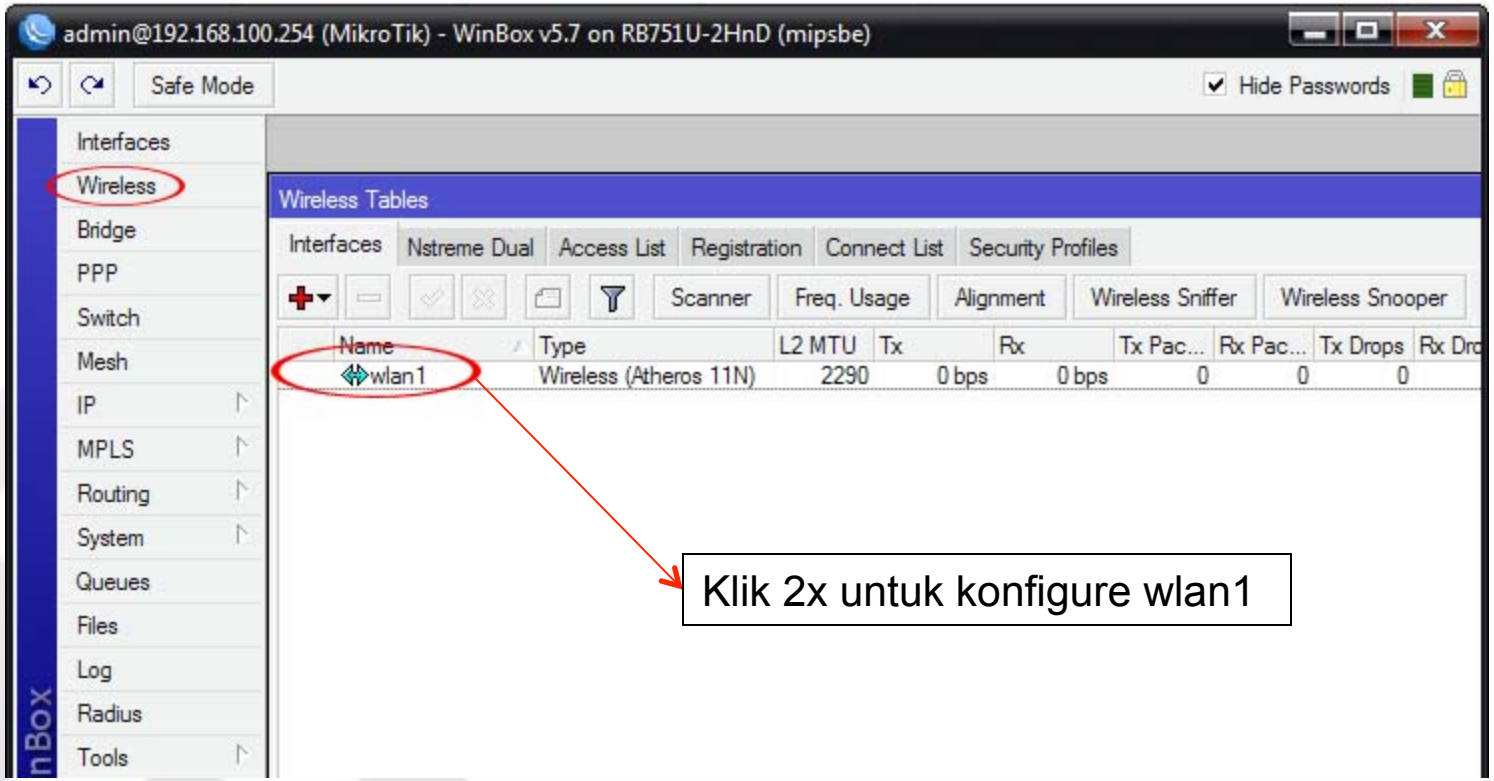
Konfigurasi LAN

- Setting IP pada Ether1 (ether yang terhubung dengan laptop)



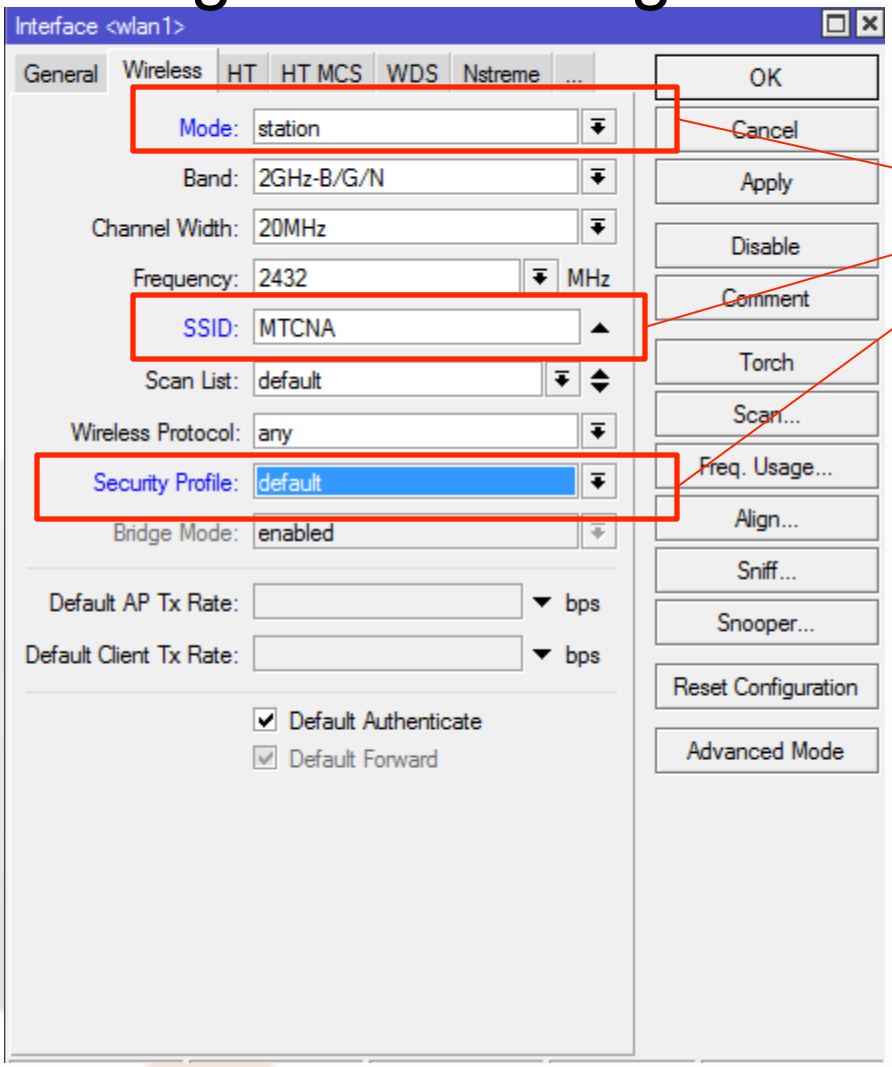
Konfigurasi WAN

- Setting wlan pada MikroTik sebagai station.



Konfigurasi WAN

- Setting wlan1 sebagai station

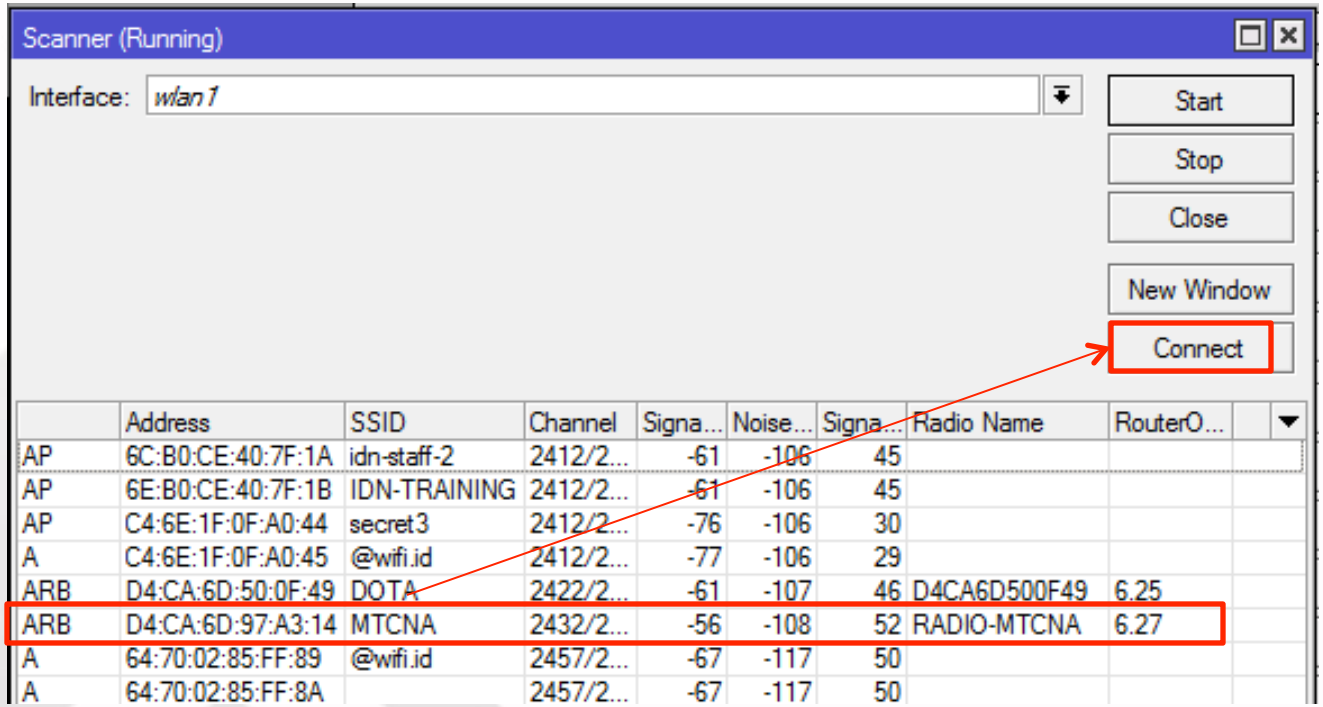


- Setting wireless mode
- Setting SSID
- Security Profile (yang sudah dibuat sebelumnya)

Klik Apply untuk mengeksekusi hasil konfigurasi

Konfigurasi WAN

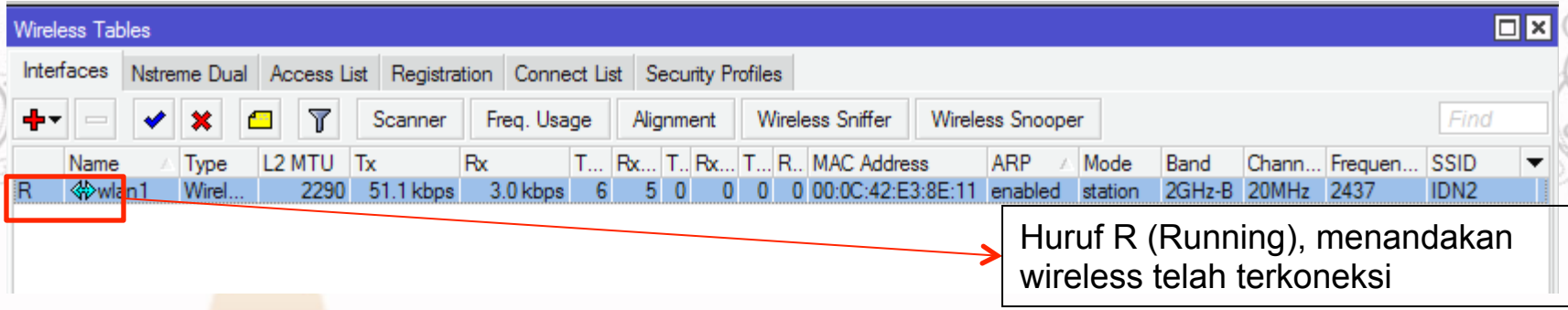
- Mode station juga dapat digunakan untuk scan network untuk mempermudah konek ke sebuah AP.

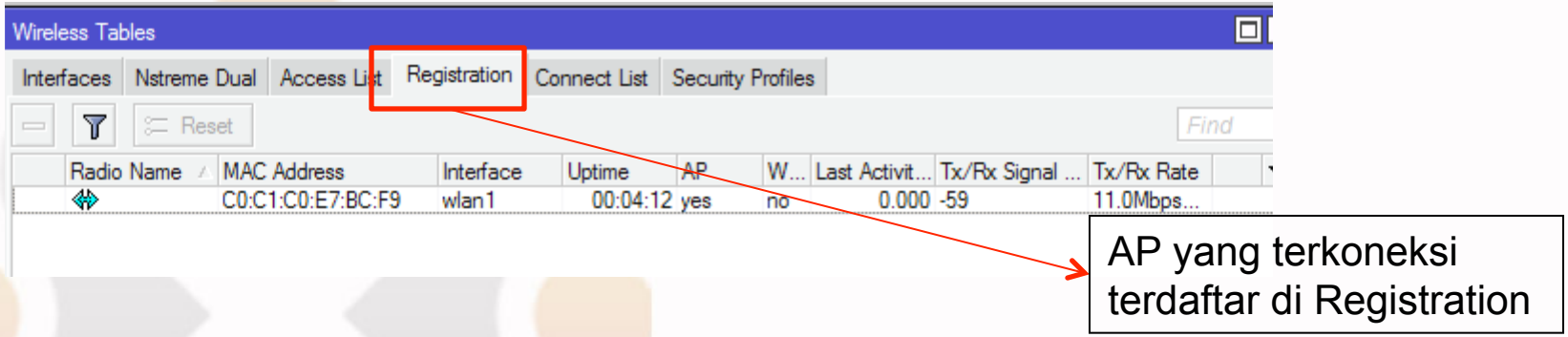


- Pilih AP yang ingin dikoneksikan dan klik tombol connect

Konfigurasi WAN

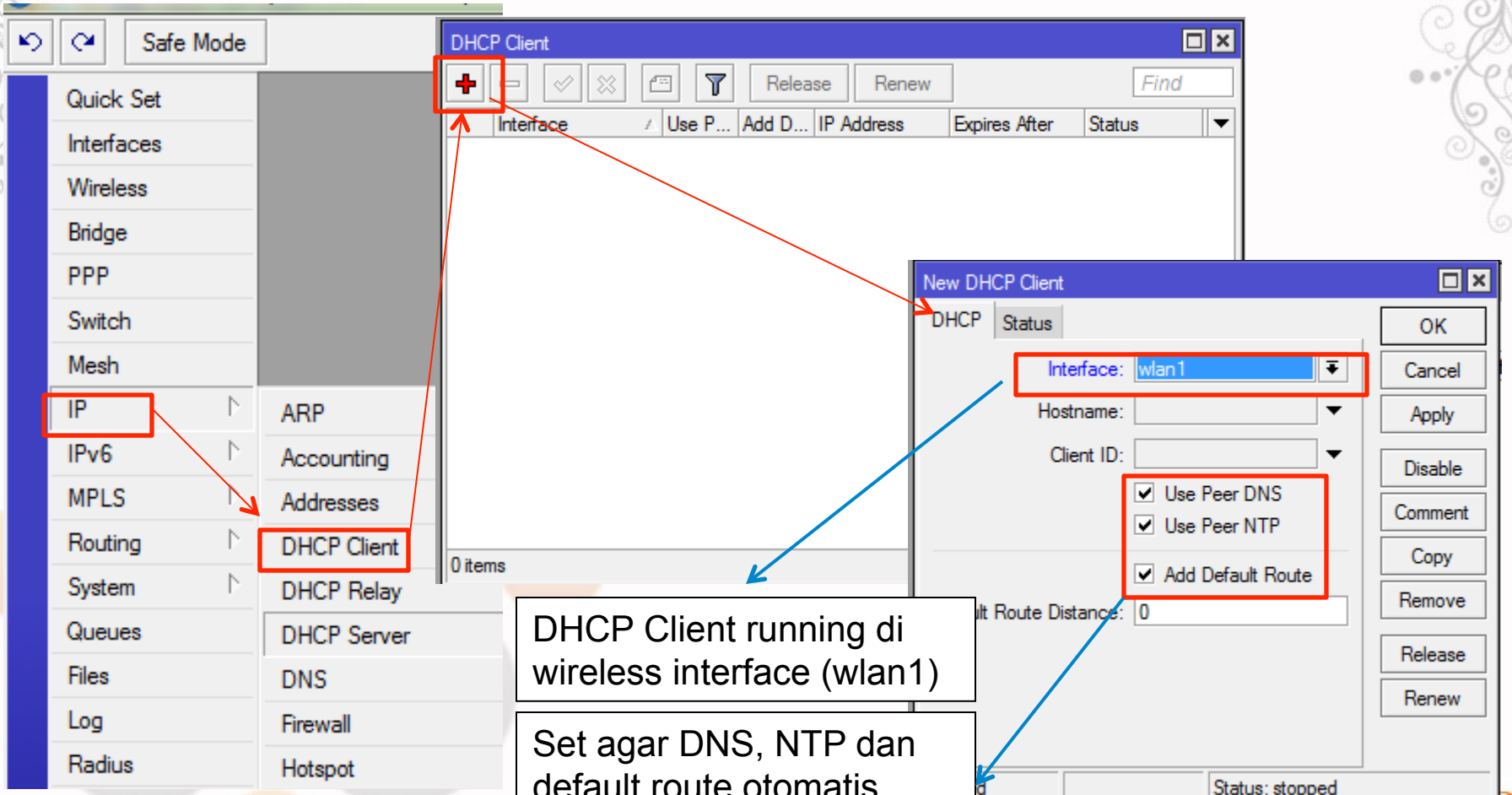
- Wireless telah terkoneksi





Konfigurasi WAN

- Setting DHCP client

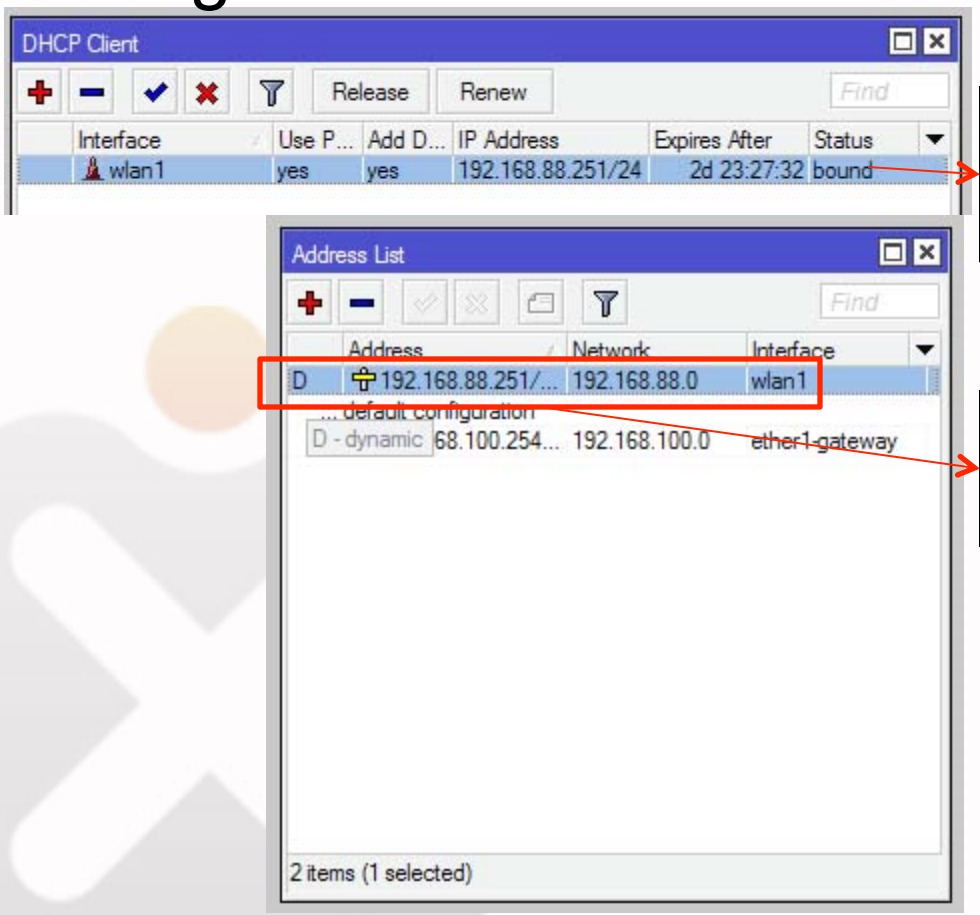


DHCP Client running di wireless interface (wlan1)

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

Seting DHCP Client

- Setting DHCP client

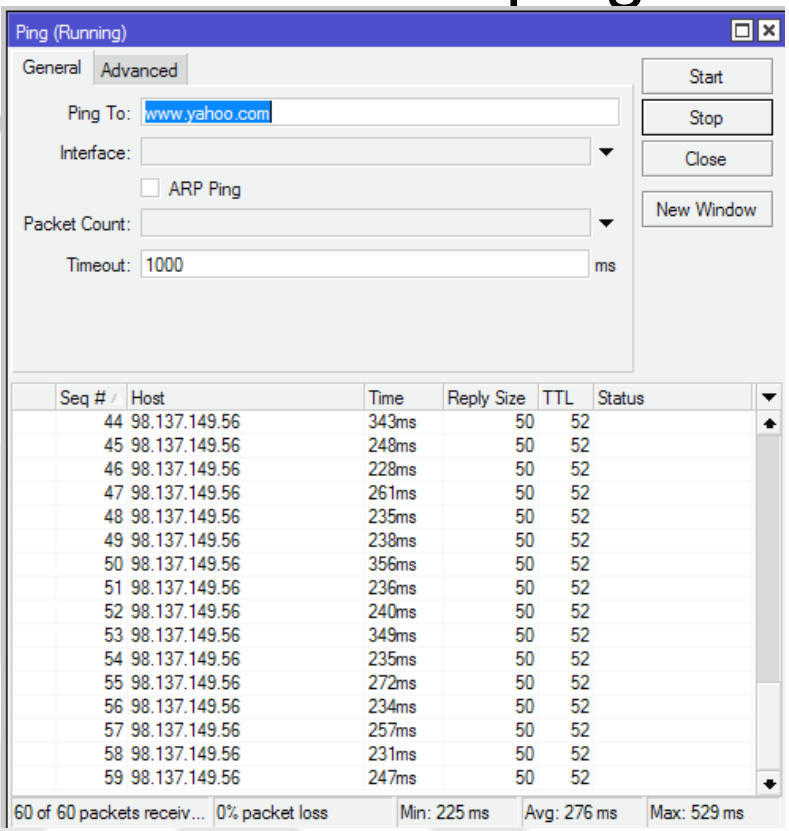


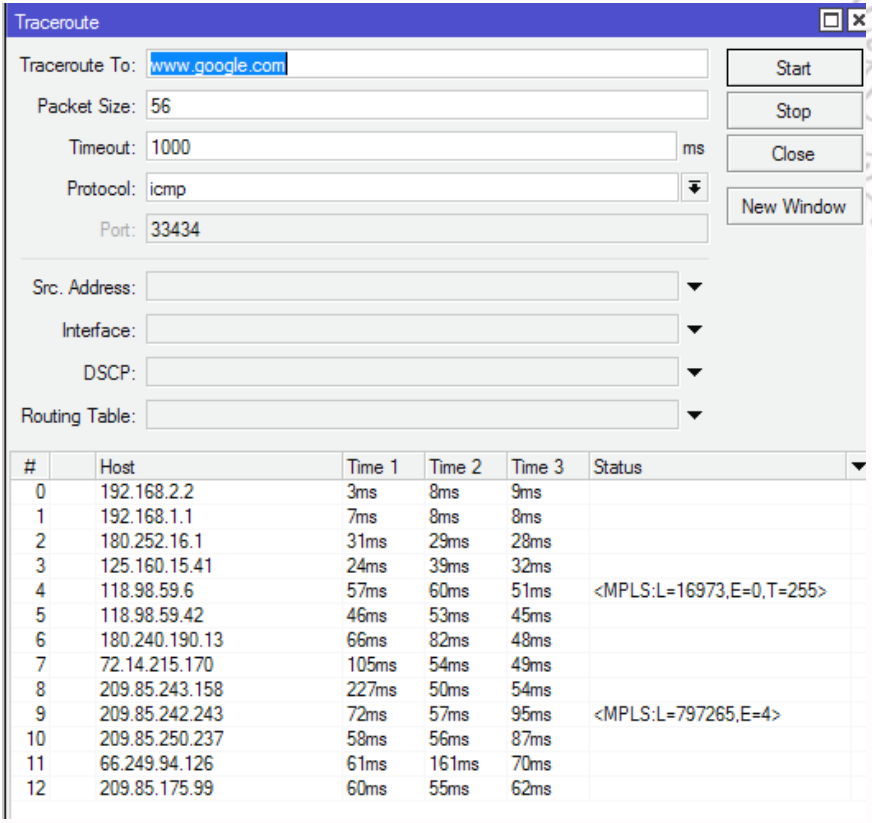
Status bound menandakan bahwa wlan1 sudah mendapatkan IP address dari AP

Pada IP>address>interface terdapat dynamic IP addres pada wlan1

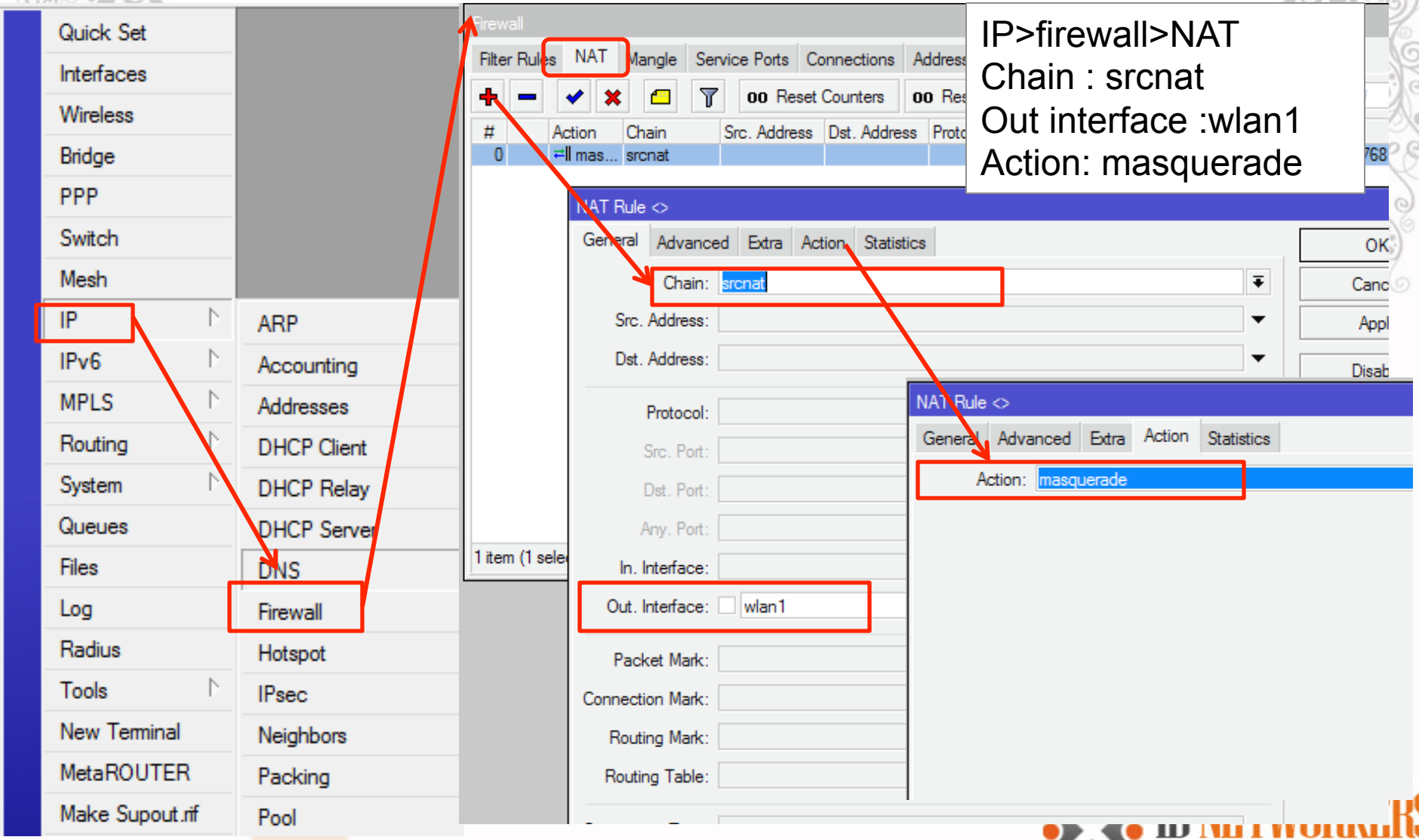
Testing

- Coba lakukan ping dan traceroute dari MikroTik





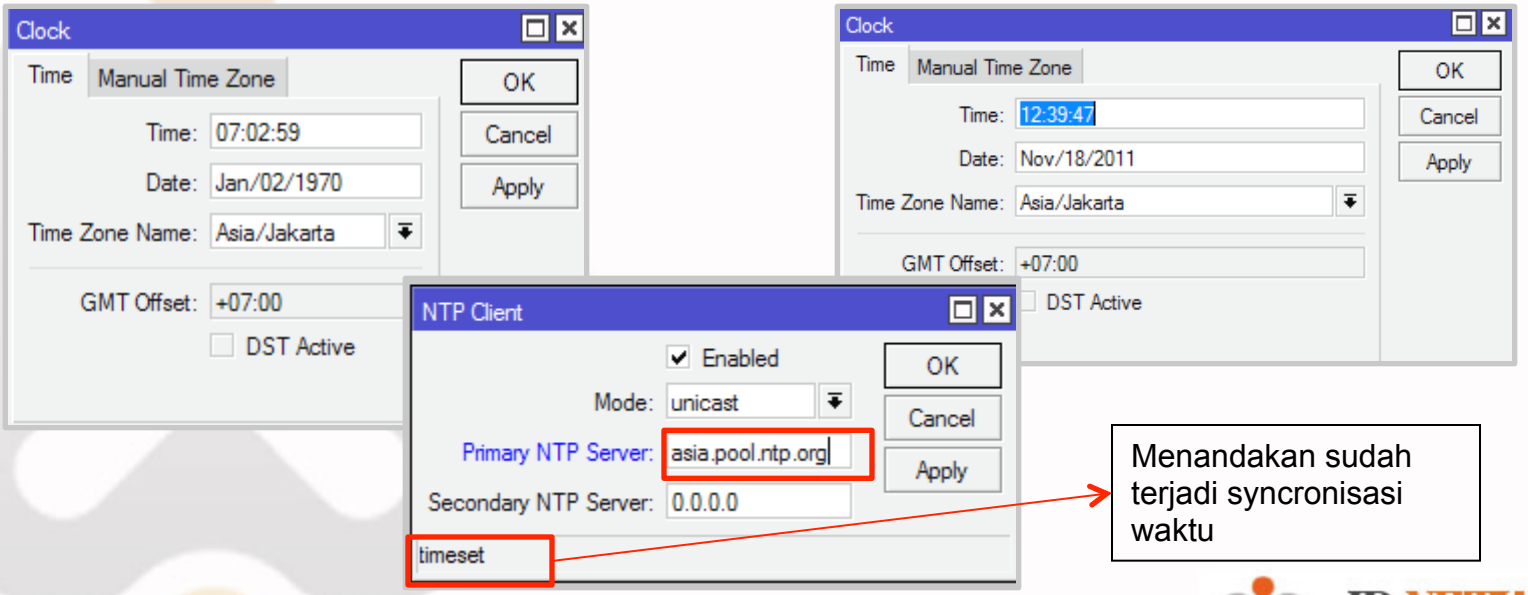
Setting NAT



IP>firewall>NAT
Chain : srcnat
Out interface :wlan1
Action: masquerade

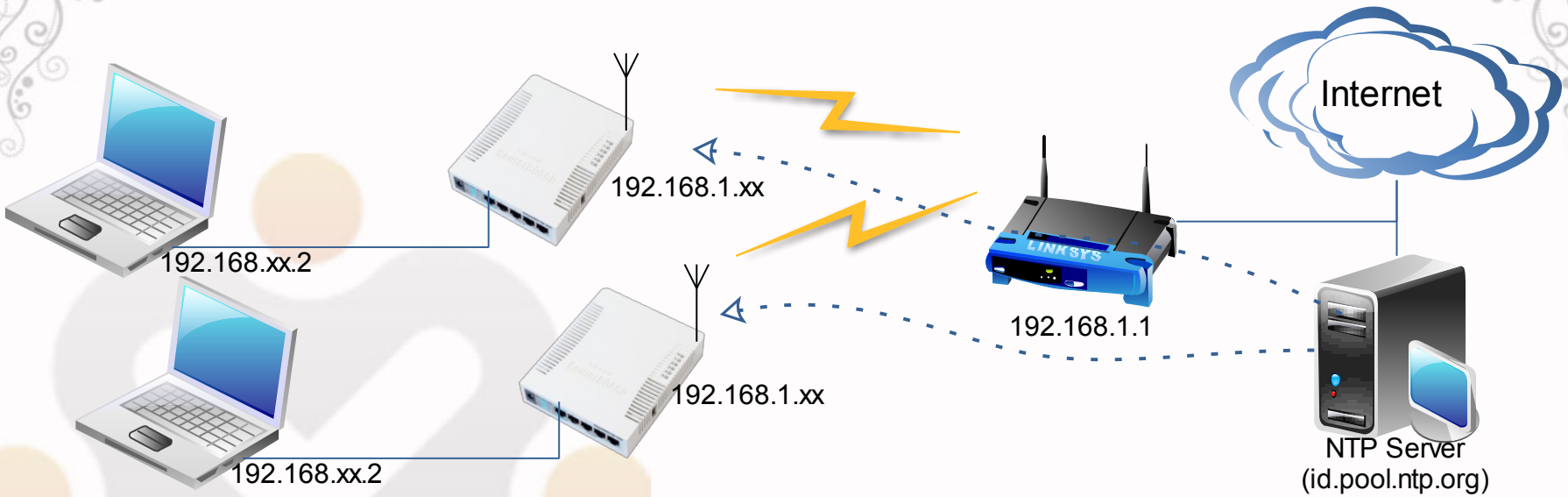
Network Time Protocol

- Kebanyakan RB mikrotik tidak memiliki battery untuk clock internal (kecuali RB230 dan powerpc)
- NTP untuk sinkronisasi waktu antar router/server lainnya.
- NTP juga bisa diarahkan ke public NTP server seperti **asia.pool.ntp.org**, atau **id.pool.ntp.org**
- Konfigurasinya ada di menu **system ntp client**



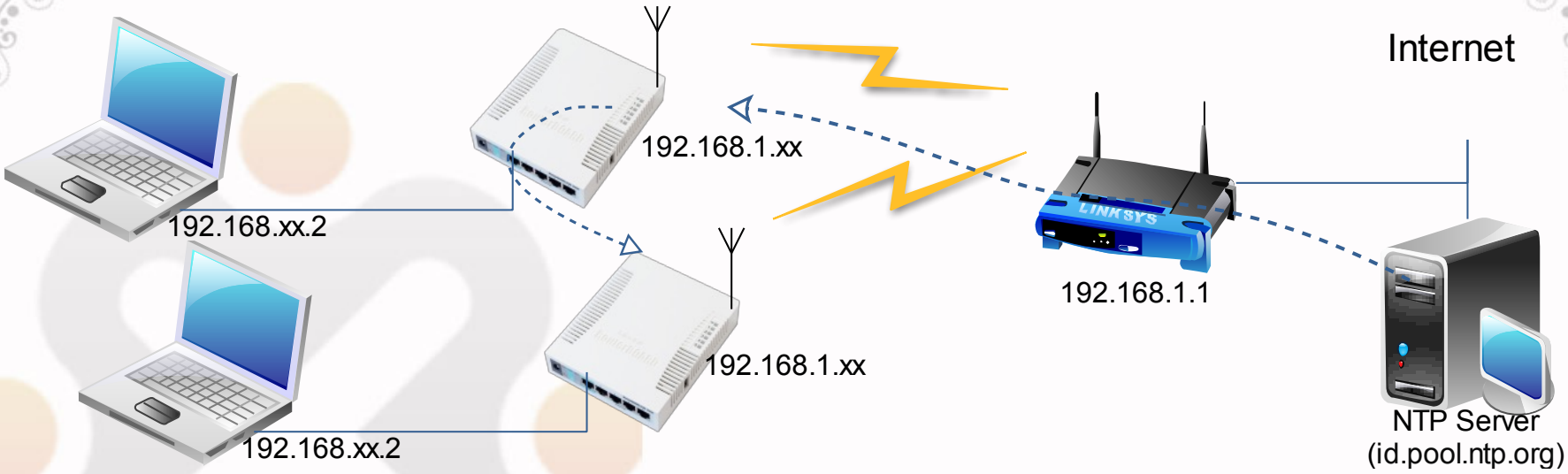
LAB- Network Time Protocol (NTP)

- Cobalah seting Mikrotik menggunakan NTP public service id.pool.ntp.org



LAB- Network Time Protocol (NTP)

- Peserta 1 menggunakan NTP public service id.pool.ntp.org, peserta yang lain NTP server diarahkan ke peserta 1



NTP Client

Fase sinkronisasi NTP Client

- **Started** : start service NTP
- **Reached** : terkoneksi dengan NTP server
- **Synchronized** :sinkronisasi waktu dengan NTP server
- **Timeset** : mengganti waktu/tanggal lokal sesuai waktu NTP server

Module 2 - Firewall

Firewall – Overview

- Untuk melindungi router dari luar, baik dari berasal dari WAN (internet) maupun dari client (local).
- Untuk melindungi netwok dari netwok lain yang melewati router.
- Dalam MikroTik, firewall ada banyak fitur yang semuanya dimasukkan dalam menu IP Firewall.
- Firewall basic di MikroTik ada di IP Firewall Filter Rule.

Firewall Filter Rule

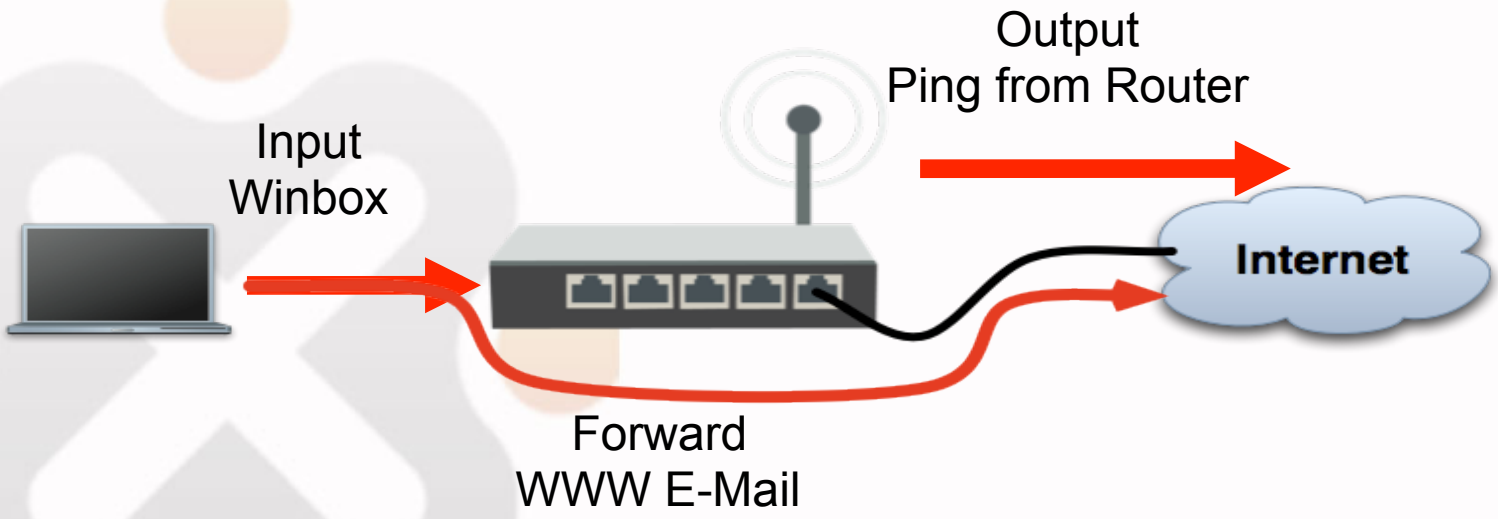
- Setiap Firewall Filter rule diorganisir dalam chain (rantai) yang berurutan.
- Setiap aturan chain yang dibuat akan dibaca oleh router dari atas ke bawah.
- Di Firewall Filter Rule ada 3 default chain (input, forward, output).
- Kita juga boleh membuat nama chain sesuai dengan keinginan kita
- Paket dicocokkan dengan kriteria/persyaratan dalam suatu chain, apabila cocok paket akan melalui kriteria/ persyaratan chain berikutnya/ di bawahnya.

.

Packet Flow

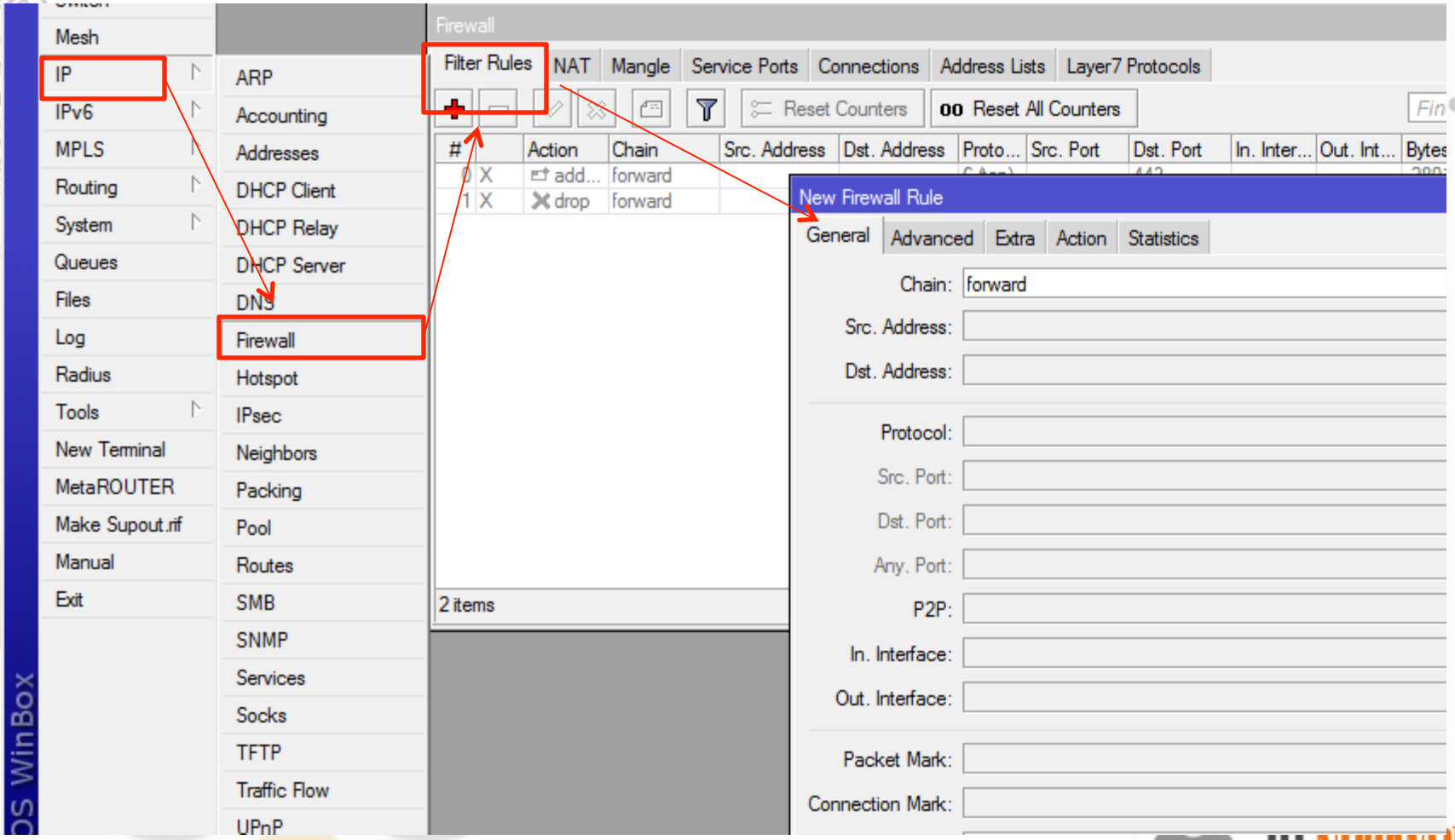
Tiga aturan dasar packet flow

- INPUT – **ke** router
- OUTPUT – **dari** router
- FORWARD – **melewati** router



Firewall Filter Rule

- IP Firewall Filter Rule

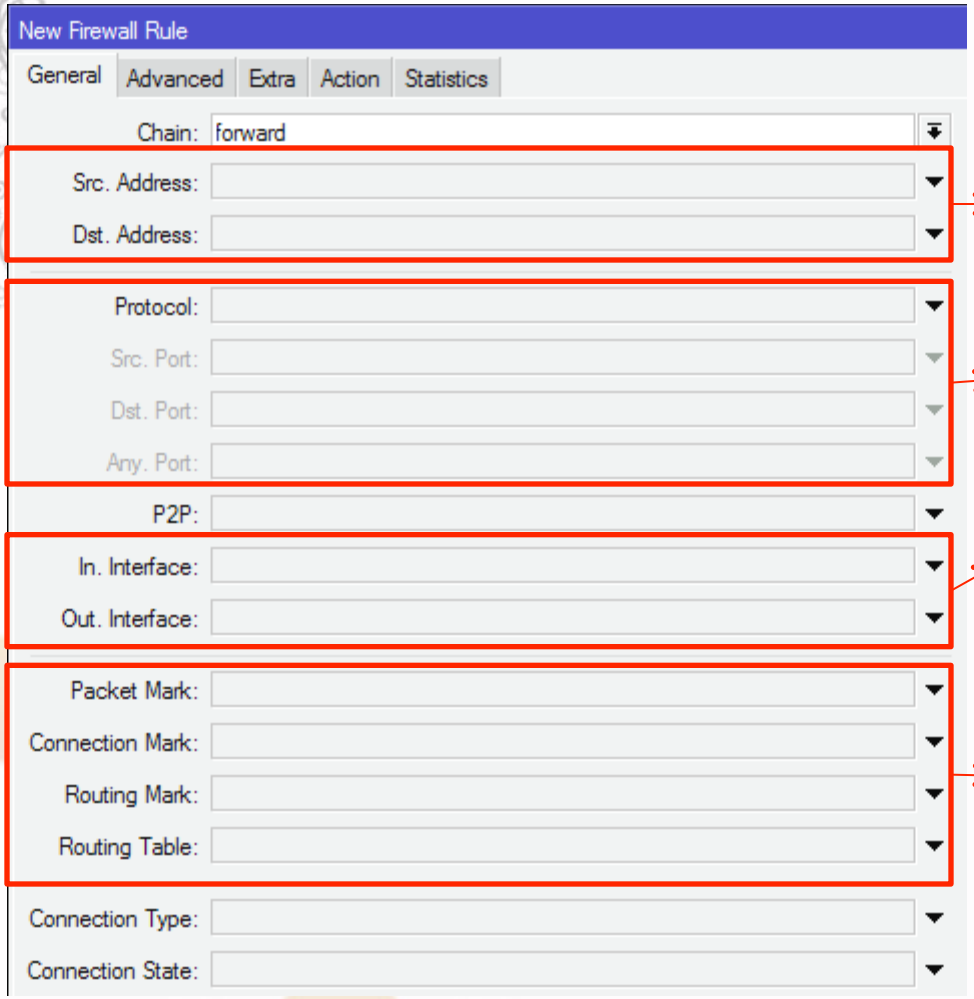


Firewall Filter Rule

- Prinsip IF….THEN….
- IF (jika) packet memenuhi syarat kriteria yang kita buat.
- THEN (maka) action apa yang akan dilakukan pada packet tersebut

Firewall – IF (Condition)

IP>Firewall>Filter Rules>General



Source IP (IP client)
Destination IP (IP internet)

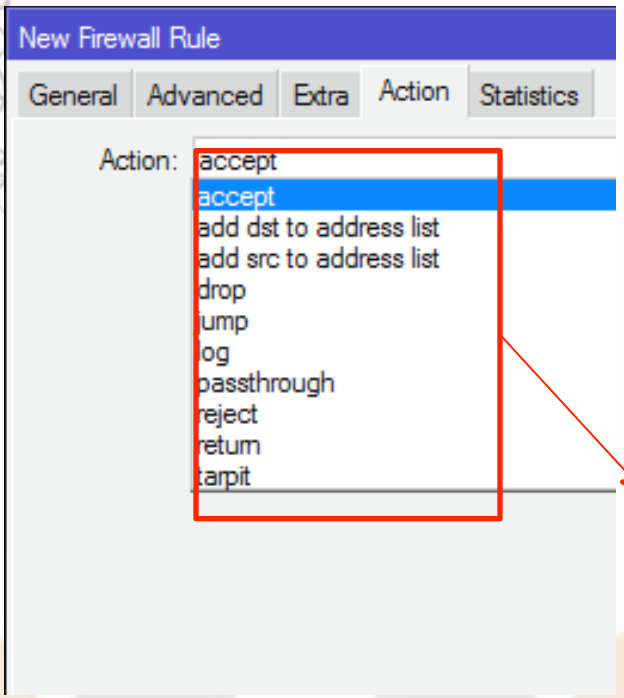
Protocol (TCP/UDP/ICMP, dll)
Source port (biasanya port dari client)
Destination port (service port tujuan)

Interface (traffik masuk atau keluar)

Paket yang sebelumnya telah ditandai

Firewall – THEN (Action)

IP>Firewall>Filter Rules>Action



accept - accept the packet. Packet is not passed to next firewall rule.

add-dst-to-address-list - add destination address to address list specified by address-list parameter

add-src-to-address-list - add source address to address list specified by address-list parameter

drop - silently drop the packet

jump - jump to the user defined chain specified by the value of jump-target parameter

log - add a message to the system log containing following data: in-interface, out-interface, src-mac, protocol, src-ip:port->dst-ip:port and length of the packet. After packet is matched it is passed to next rule in the list, similar as passthrough

passthrough - ignore this rule and go to next one (useful for statistics).

reject - drop the packet and send an ICMP reject message

return - passes control back to the chain from where the jump took place

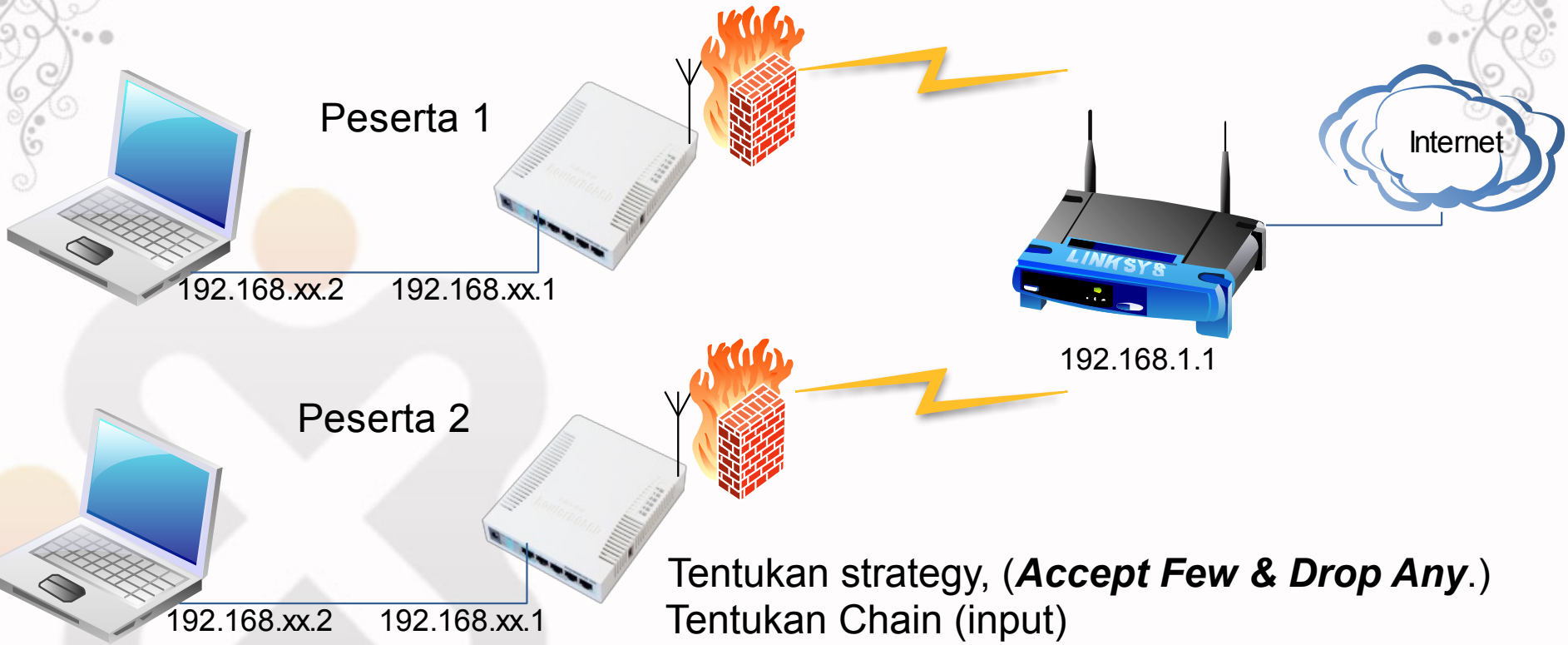
tarpit - captures and holds TCP connections (replies with SYN/ACK to the inbound TCP SYN packet)

Firewall Strategy

- Banyak traffik yang harus difilter dan dipilah mana yang harus di perbolehkan (accept) dan mana yang harus di buang (drop)
- Ada 2 metode untuk menyederhanakan rule firewall yang kita buat:
  - Drop beberapa, lainya diterima (*drop few, accept any*)
  - Terima beberapa, lainya dibuang (*accept few, drop any*)
- By default bila tidak ada rule apapun di firewall, semua traffik akan di accept oleh router.

LAB – Protecting Our Router

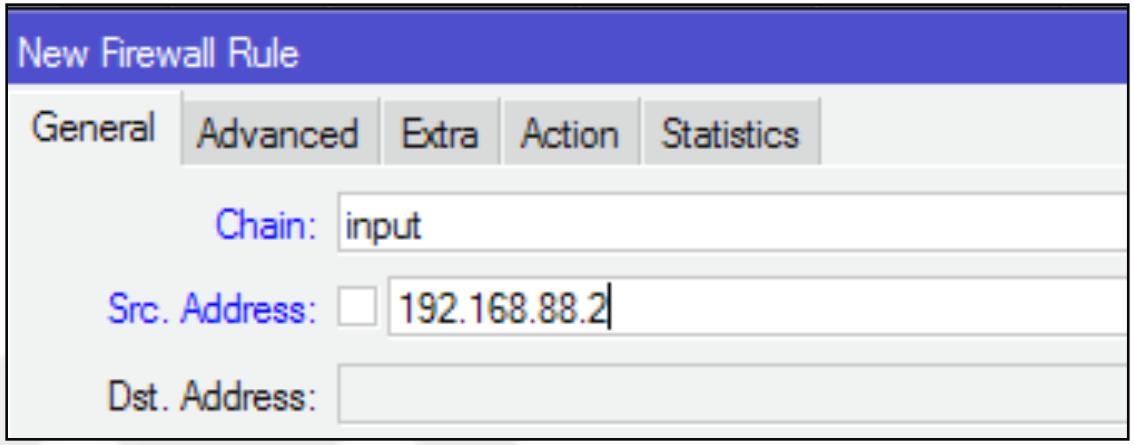
Cobalah buat firewall hanya memperbolehkan IP laptop sendiri yang hanya bisa akses router



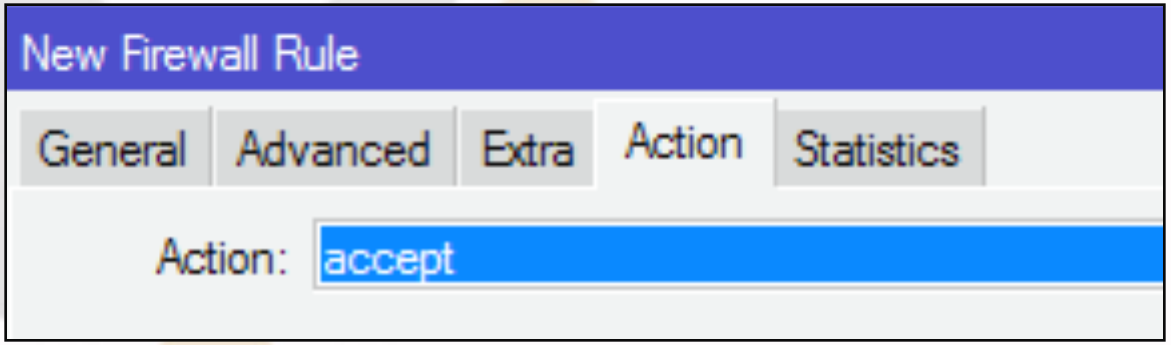
Tentukan strategy, (***Accept Few & Drop Any***.)
Tentukan Chain (input)

LAB – Protecting Our Router

- IF ada traffic **input** yang berasal dari IP Laptop (**192.168.88.2**)

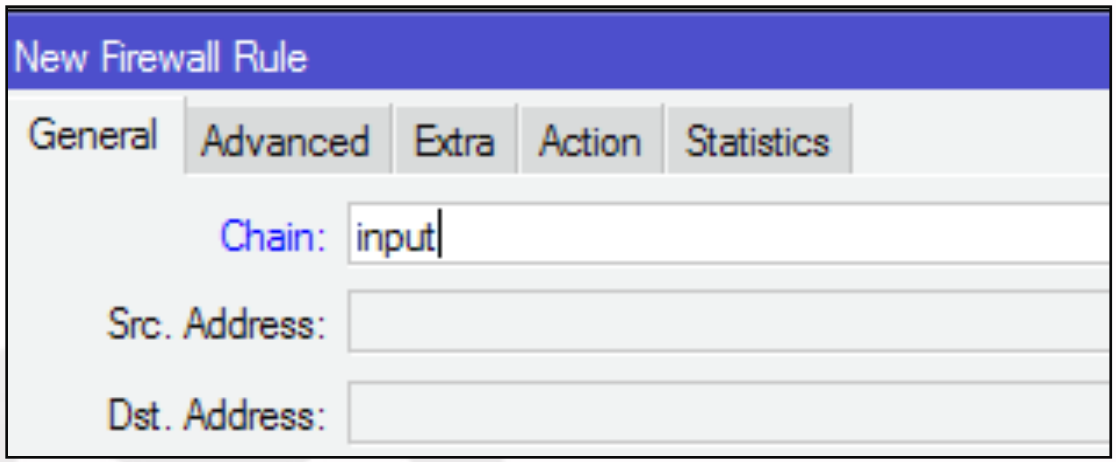


- Then tentukan action → **accept**

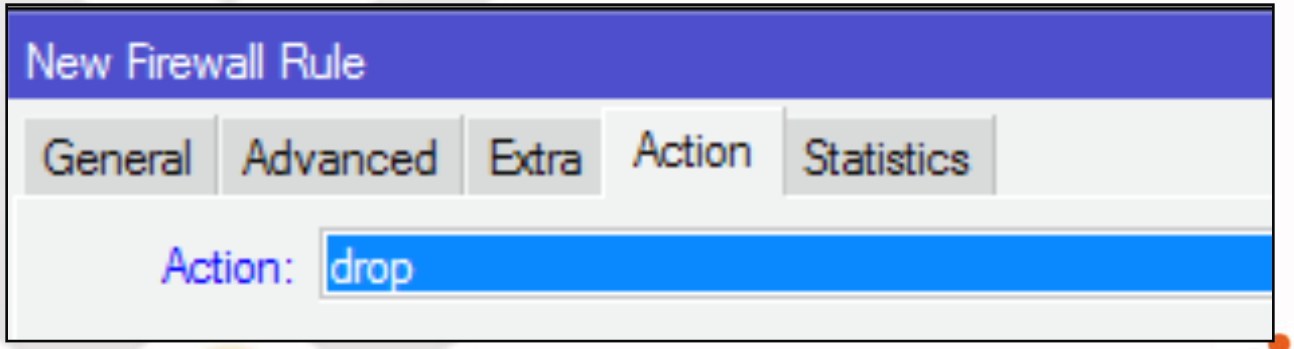


LAB – Protecting Our Router

- IF ada traffic yang berasal dari <kosong> atau “all”

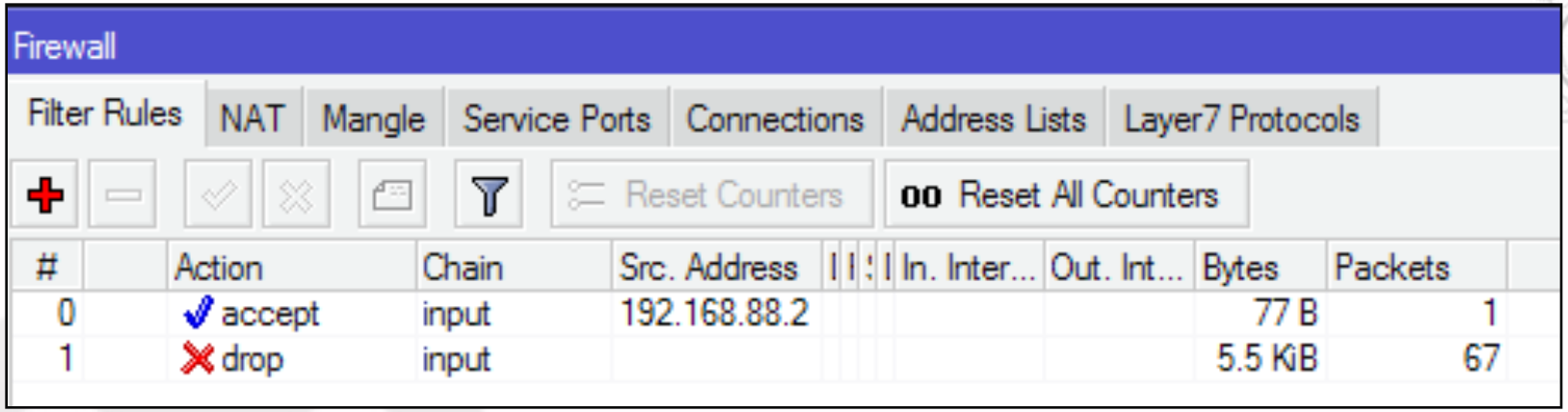


- Then tentukan action drop



LAB – Protecting Our Router

- Akan ada 2 chain rules.

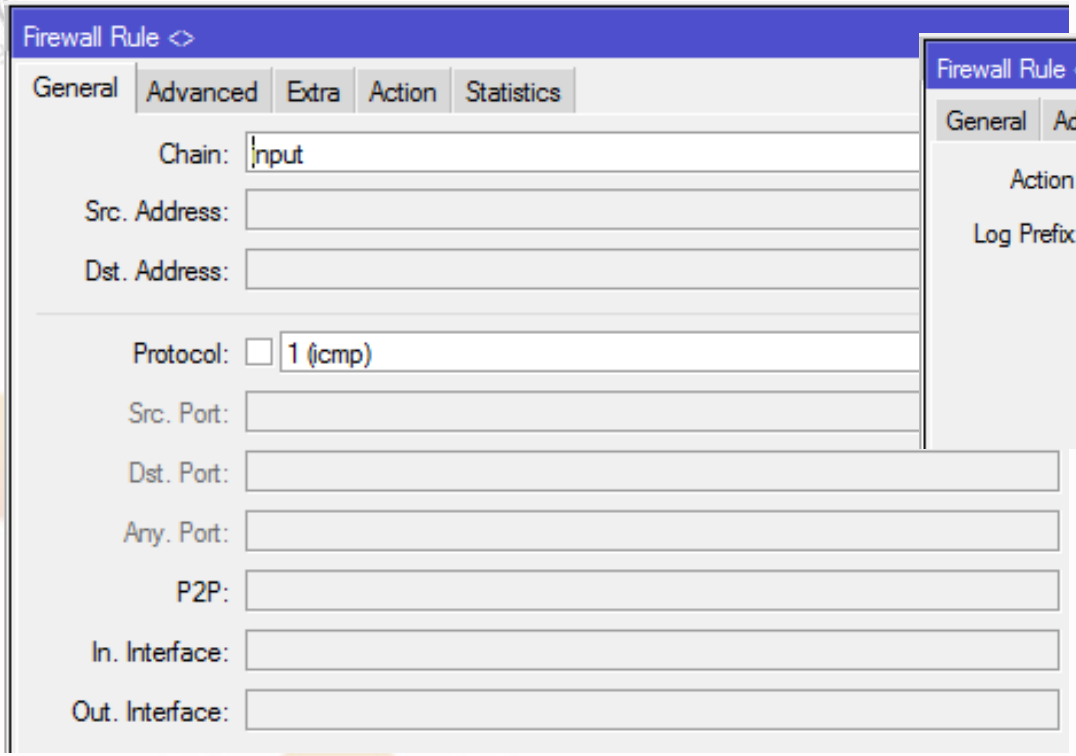


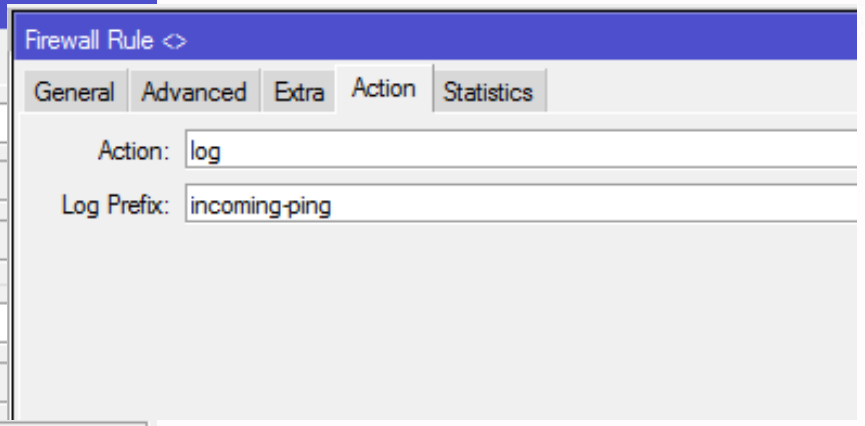
- Perhatikan jumlah bytes pada setiap chain rule, tetap ataukah bertambah ketika kita melakukan akses ke router?
- Cobalah masing-masing peserta untuk melakukan ping, akses web, dan remote winbox ke router peserta lain.

LAB – Firewall Loging

Firewall Logging adalah fitur untuk mencatat (menampilkan pada log) aktifitas yang jaringan yang kita inginkan.

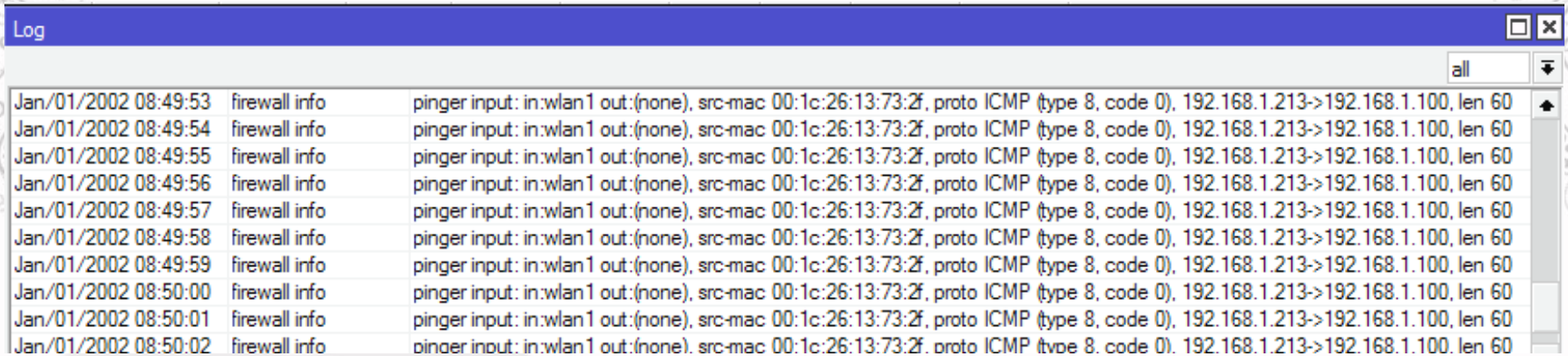
- Buat filter rule pada menu IP>Firewall>Filter Rules, untuk logging semua yang ping router kita





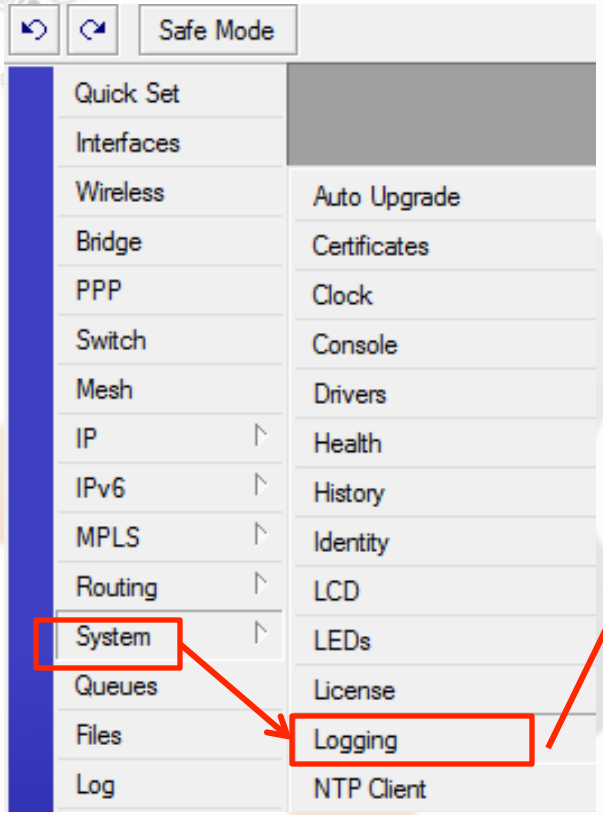
LAB – Firewall Loging

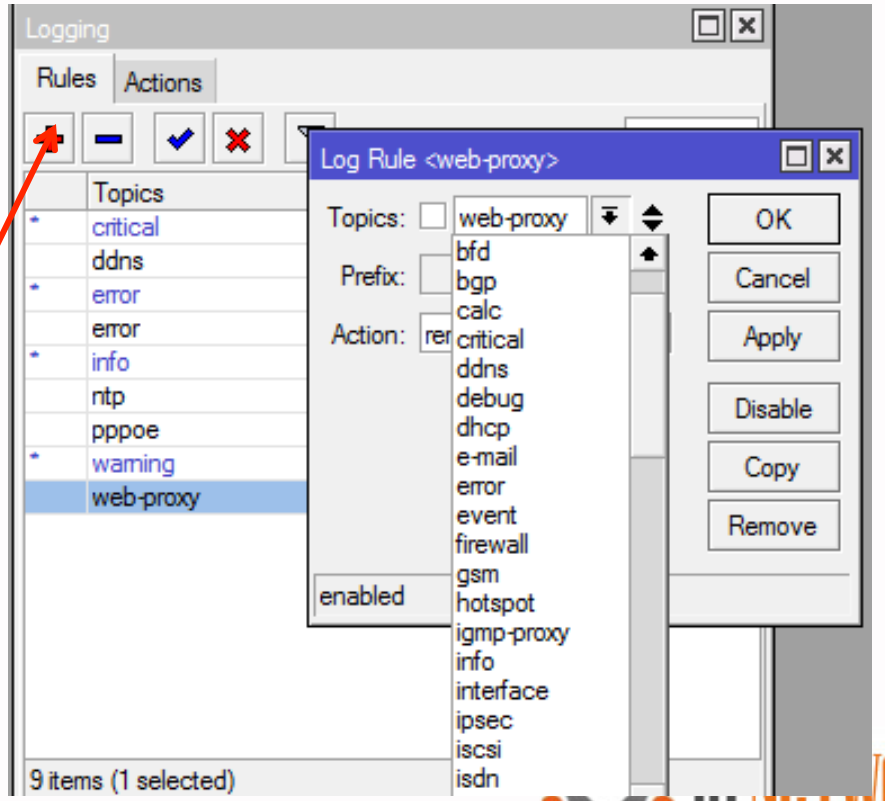
Ping dari laptop IP interface wlan1 dan amati log pada router:



Logging

- Kita dapat mengatur aktivitas atau fitur apa yang akan ditampilkan dalam log.
- Kita juga dapat mengirimkan log ke syslog server tententu menggunakan default protocol UDP port 514.
- Pengaturan logging ada dalam menu System Logging



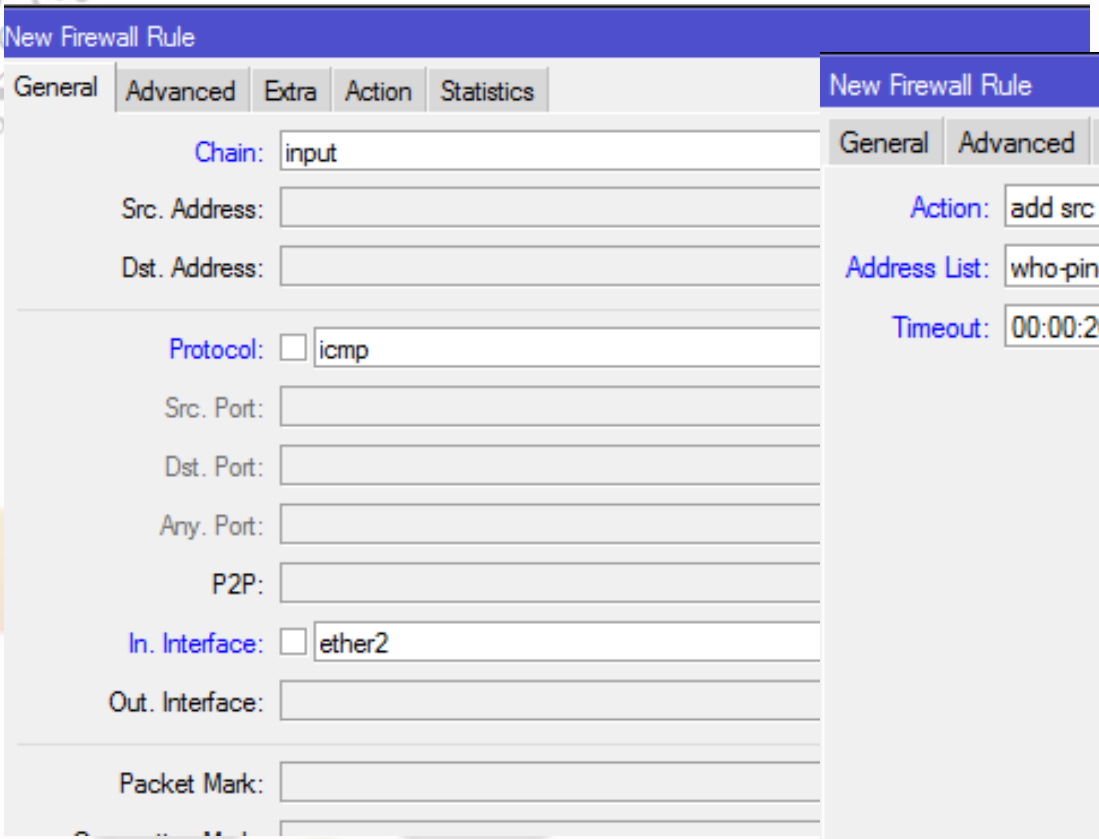


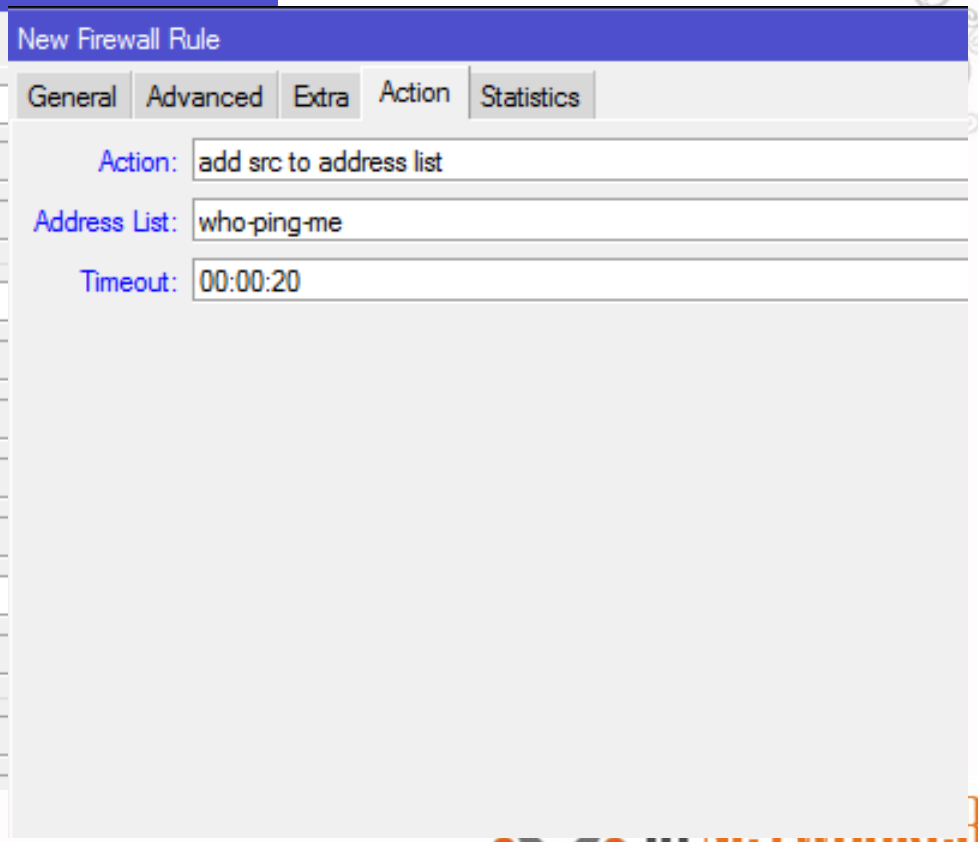
Firewall – Address List

- Address-list digunakan untuk memfilter group IP address dengan 1 rule firewall.
- Address-list juga bisa merupakan list IP hasil dari rule firewall yang memiliki action “add to address list”
- Satu line address-list dapat berupa subnet, range, atau 1 host IP address

LAB– Address List

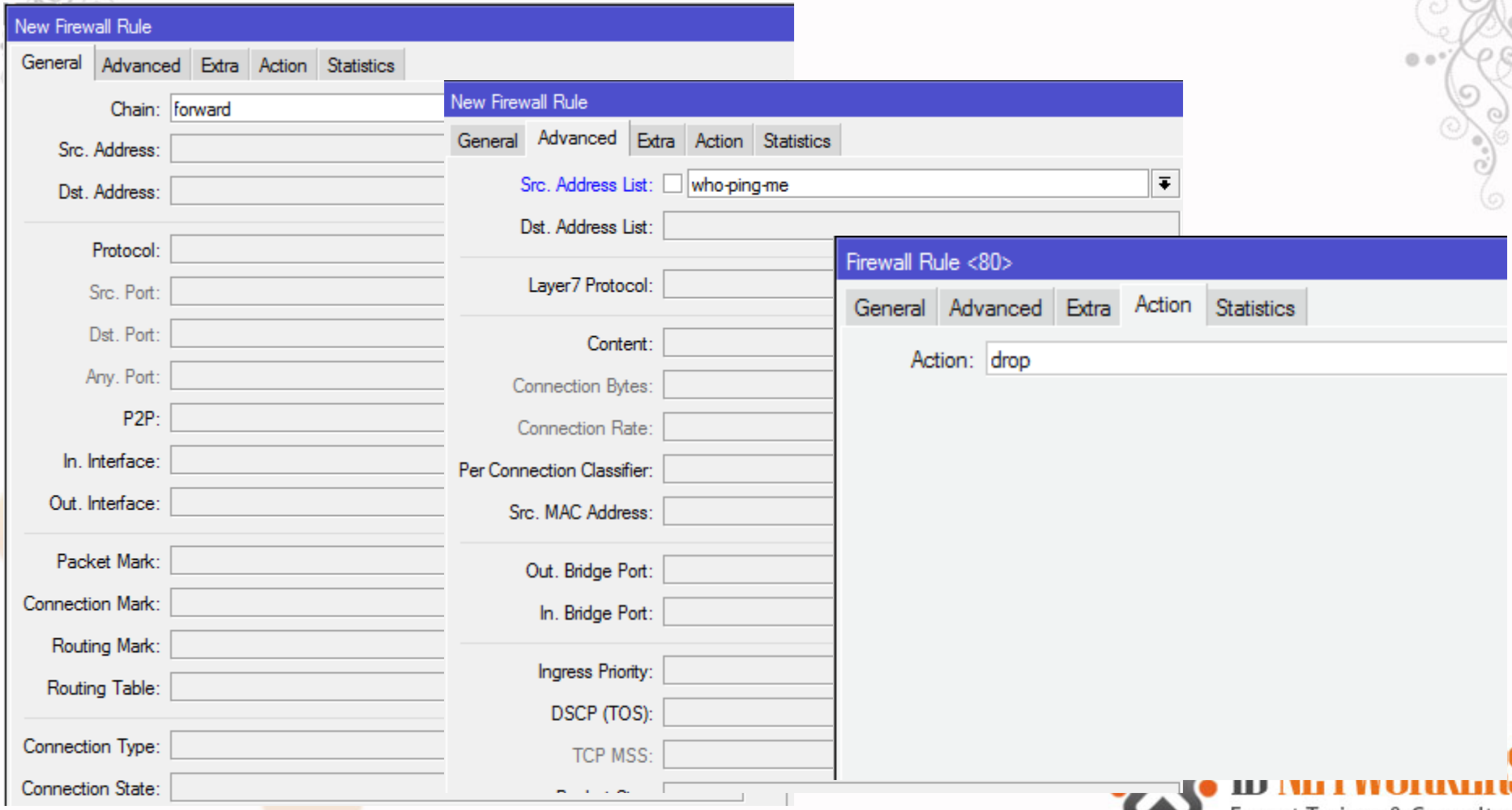
- Siapa dari lokal kita yang ping ke router, dia tidak bisa akses internet selama 20 detik
- Buat rule firewall untuk memasukkan setiap IP yang melakukan ping ke dalam address-list dan beri nama address list “who-ping-me”.





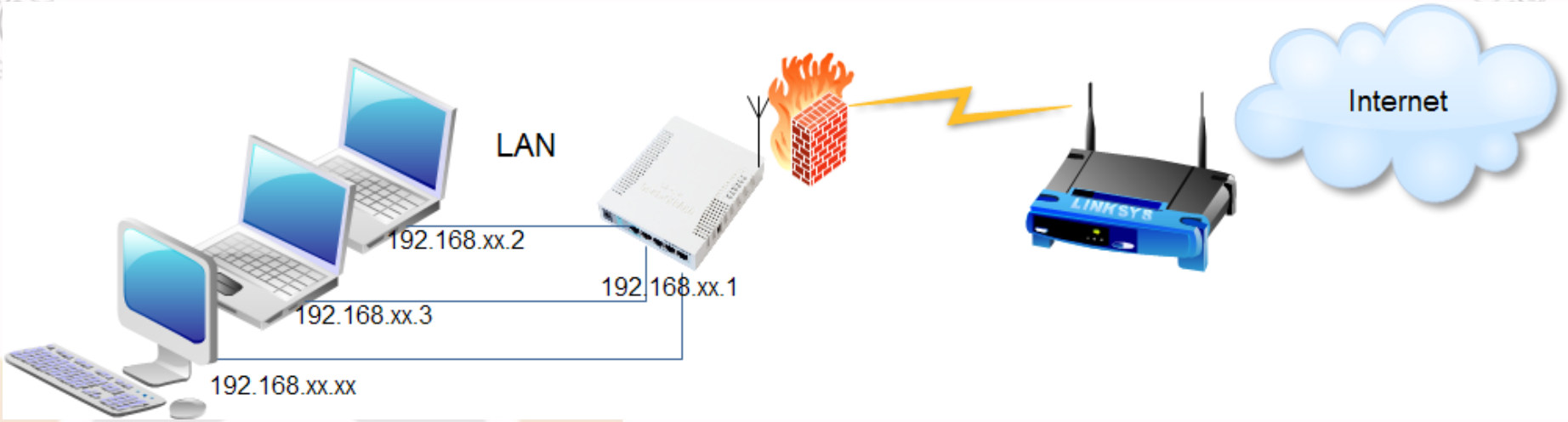
LAB– Address List

- Buat rule drop untuk address-list “who-ping-me”
- Rule ini akan bekerja jika ada yang ping ke router saja



LAB – Block content

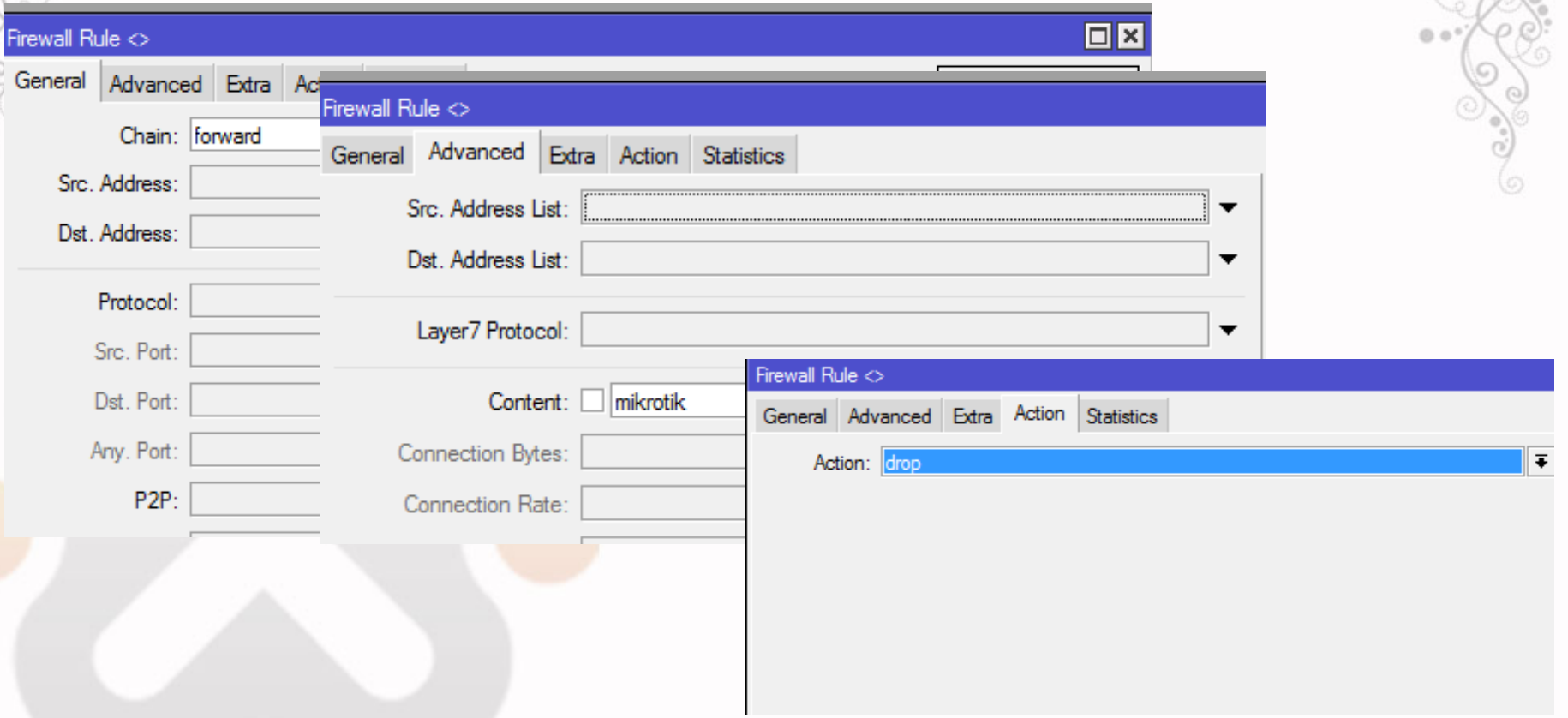
Kita akan block akses dari LAN ke situs tertentu, misalnya situs yang mengandung kata “porno”, tapi porno dalam hal ini kita ganti kata “mikrotik”



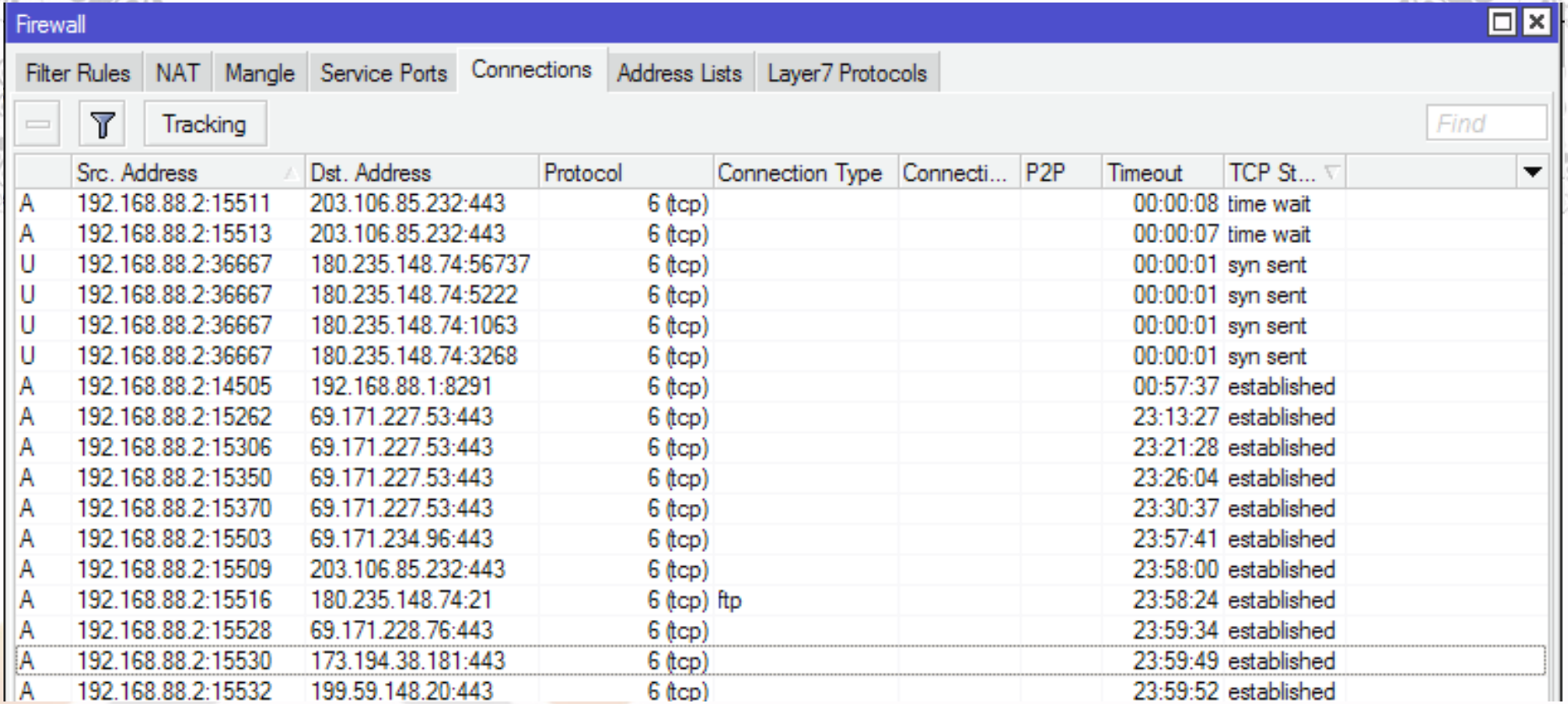
LAB – Block content

IP Firewall Filter Rule

Add chain=forward content=mikrotik action=drop



Connection Tracking

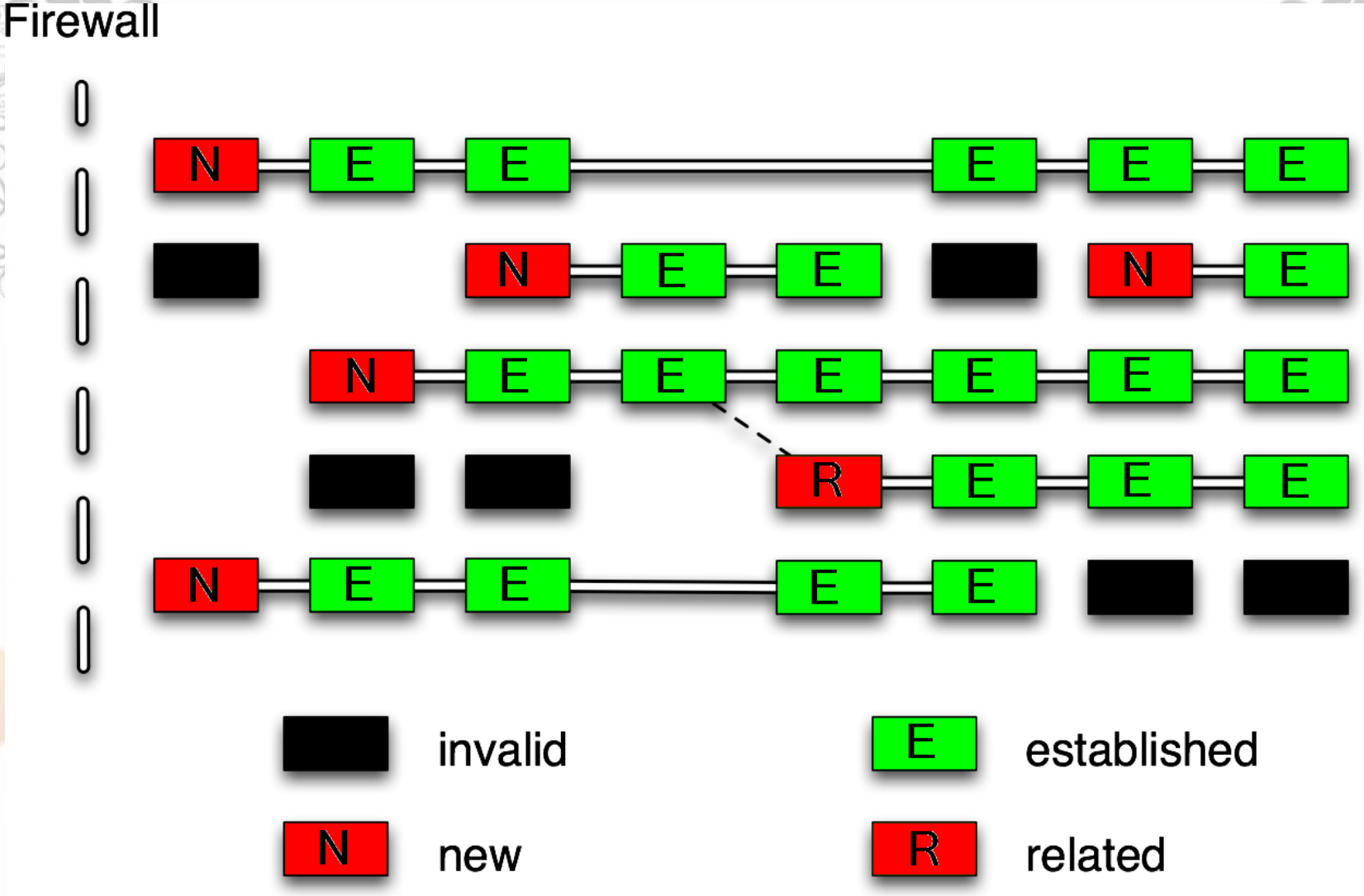


	Src. Address	Dst. Address	Protocol	Connection Type	Connecti...	P2P	Timeout	TCP St...
A	192.168.88.2:15511	203.106.85.232:443	6 (tcp)				00:00:08	time wait
A	192.168.88.2:15513	203.106.85.232:443	6 (tcp)				00:00:07	time wait
U	192.168.88.2:36667	180.235.148.74:56737	6 (tcp)				00:00:01	syn sent
U	192.168.88.2:36667	180.235.148.74:5222	6 (tcp)				00:00:01	syn sent
U	192.168.88.2:36667	180.235.148.74:1063	6 (tcp)				00:00:01	syn sent
U	192.168.88.2:36667	180.235.148.74:3268	6 (tcp)				00:00:01	syn sent
A	192.168.88.2:14505	192.168.88.1:8291	6 (tcp)				00:57:37	established
A	192.168.88.2:15262	69.171.227.53:443	6 (tcp)				23:13:27	established
A	192.168.88.2:15306	69.171.227.53:443	6 (tcp)				23:21:28	established
A	192.168.88.2:15350	69.171.227.53:443	6 (tcp)				23:26:04	established
A	192.168.88.2:15370	69.171.227.53:443	6 (tcp)				23:30:37	established
A	192.168.88.2:15503	69.171.234.96:443	6 (tcp)				23:57:41	established
A	192.168.88.2:15509	203.106.85.232:443	6 (tcp)				23:58:00	established
A	192.168.88.2:15516	180.235.148.74:21	6 (tcp)	ftp			23:58:24	established
A	192.168.88.2:15528	69.171.228.76:443	6 (tcp)				23:59:34	established
A	192.168.88.2:15530	173.194.38.181:443	6 (tcp)				23:59:49	established
A	192.168.88.2:15532	199.59.148.20:443	6 (tcp)				23:59:52	established

Connection Tracking

- Connection Tracking dapat dilihat pada menu IP>firewall>connection.
- Connection tracking mempunyai kemampuan untuk melihat informasi koneksi seperti source dan destinition IP dan port yang sedang digunakan, status koneksi, tipe protocol, dll.
- Status koneksi pada connection tracking:
  - **established** = *the packet is part of already known connection,*
  - **new** = *the packet starts a new connection or belongs to a connection that has not seen packets in both directions yet*,
  - **related** = *the packet starts a new connection, but is associated with an existing connection, such as FTP data transfer or ICMP error message.*
  - **invalid** = *the packet does not belong to any known connection and, at the same time, does not open a valid new connection.*

Connection Tracking

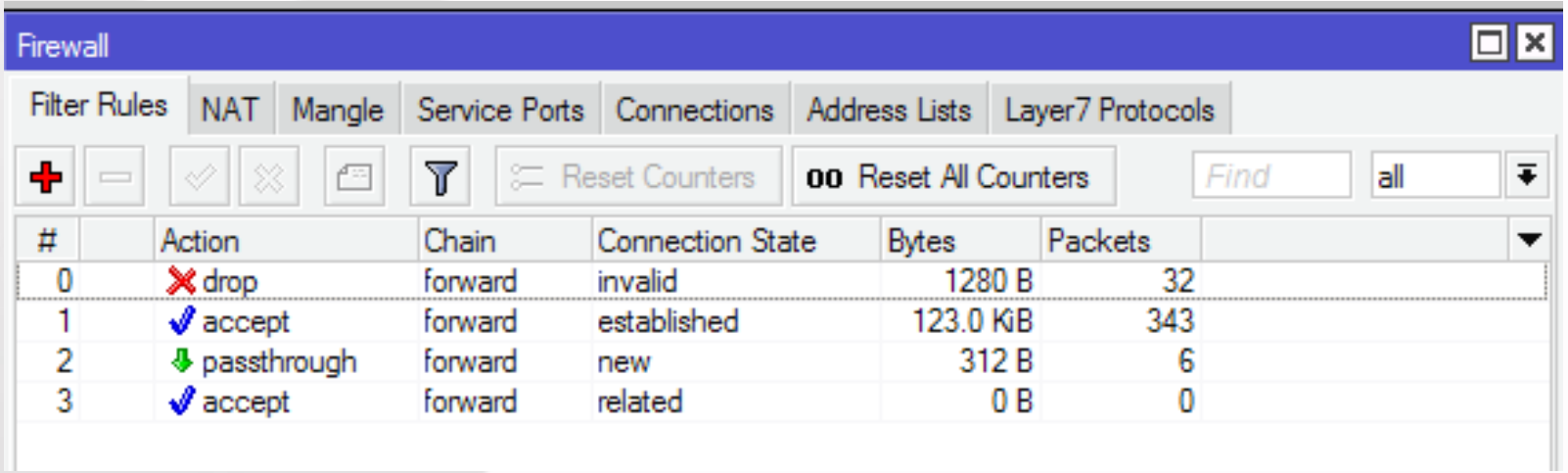


Implementasi Connection Tracking

- Pada saat membuat firewall, pada baris paling atas umumnya akan dibuat rule sebagai berikut:
  - Connection state invalid → Drop
  - Connection state established → Accept
  - Connection state related → Accept
  - Connection state new → Diproses ke rule berikutnya
- System rule ini akan sangat menghemat resource router, karena proses filtering selanjutnya akan dilakukan ketika koneksi dimulai (connection state = new)

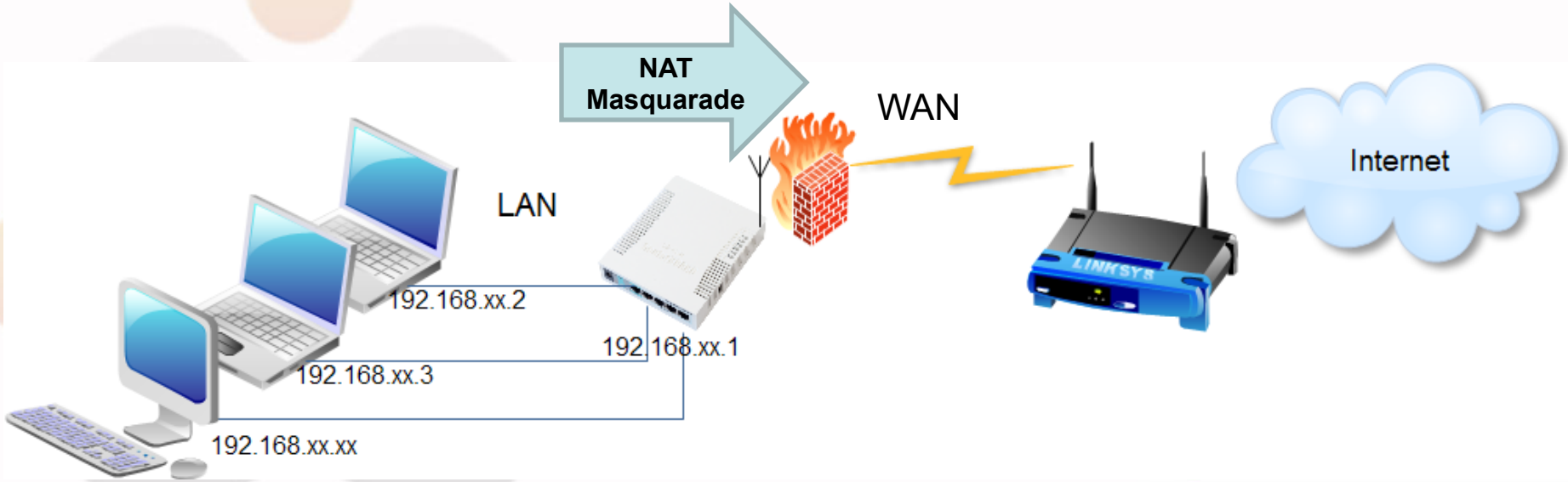
LAB – Buatlah Firewall untuk Connection State

- Pada IP>Firewall>Filter Rule buat chain
- Chain Foward
  - Connection state invalid → action Drop
  - Connection state established → action Accept
  - Connection state related → action Accept
  - Connection state new → action pass-through



NAT - Masquarade

- NAT adalah suatu metode untuk menghubungkan banyak komputer ke jaringan internet dengan menggunakan satu atau lebih alamat IP.
- NAT digunakan karena ketersediaan alamat IP public.
- NAT juga digunakan untuk alasan keamanan (security), kemudahan dan fleksibilitas dalam administrasi jaringan.



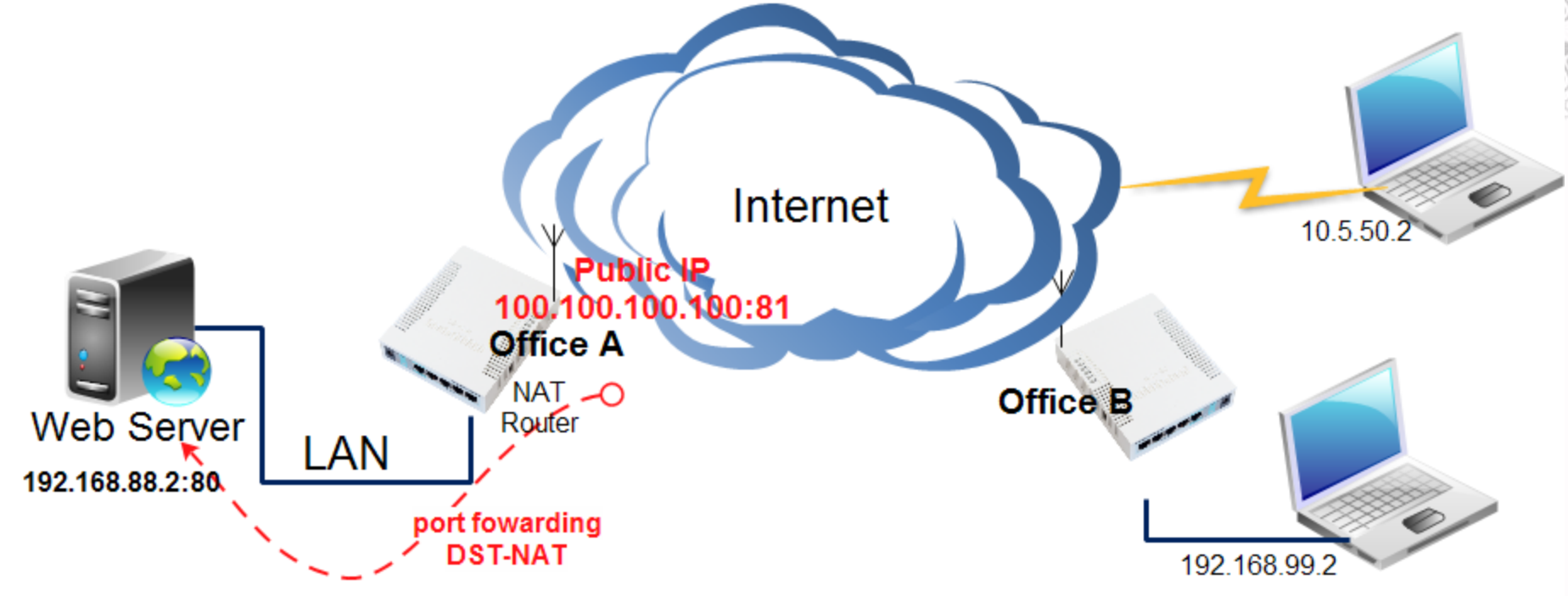
NAT

Chain pada IP Firewall NAT

1. **srcnat**, dengan action yang diperbolehkan:
    1. Masquarade – subnet LAN to 1 dinamic IP WAN
    2. Src-nat – subnet LAN to 1 static IP WAN

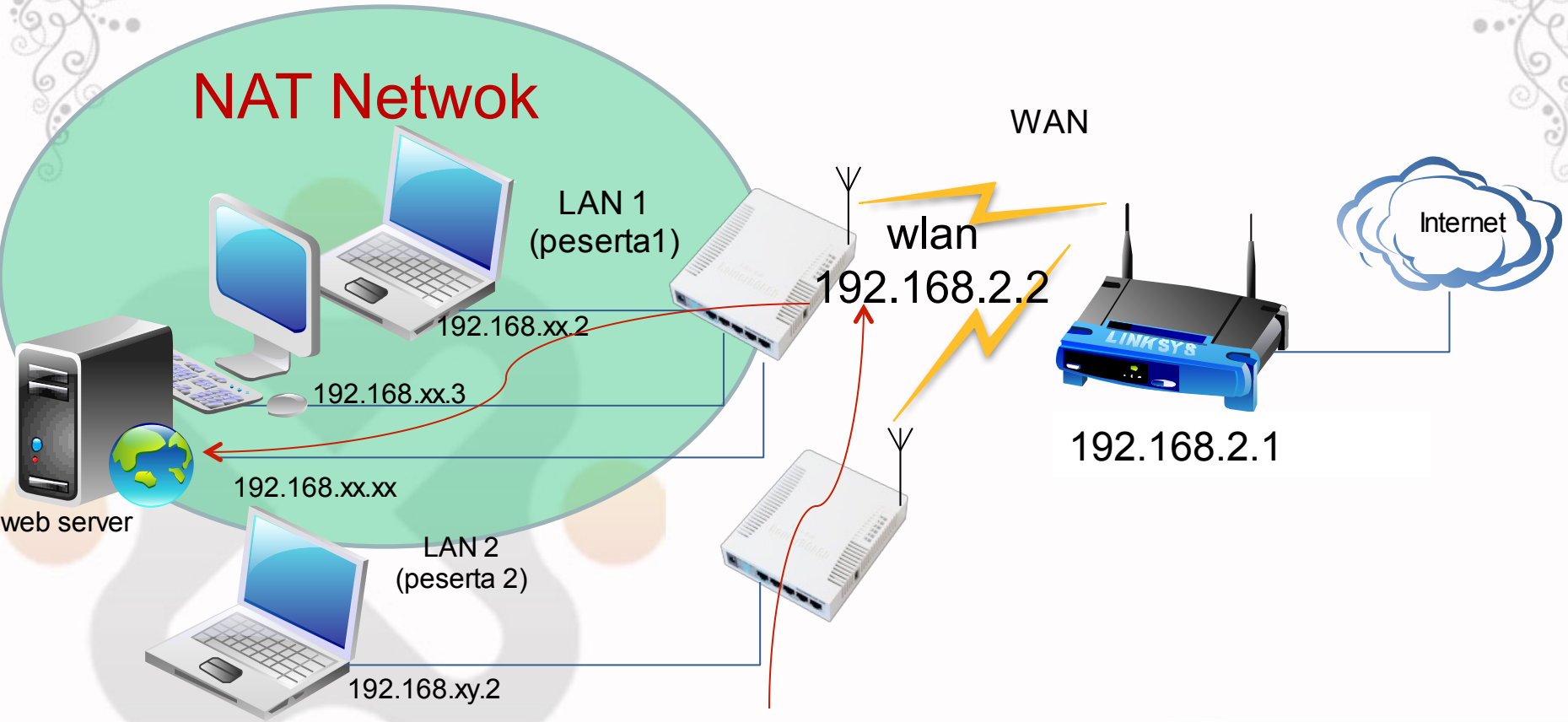
2. **dsnat** (port fowarding), dengan action yang diperbolehkan:
    1. Dst-nat – membelokkan traffik ke luar router
    2. Redirect – membelokkan traffik ke router sendiri

DSTNAT



LAB- DstNAT

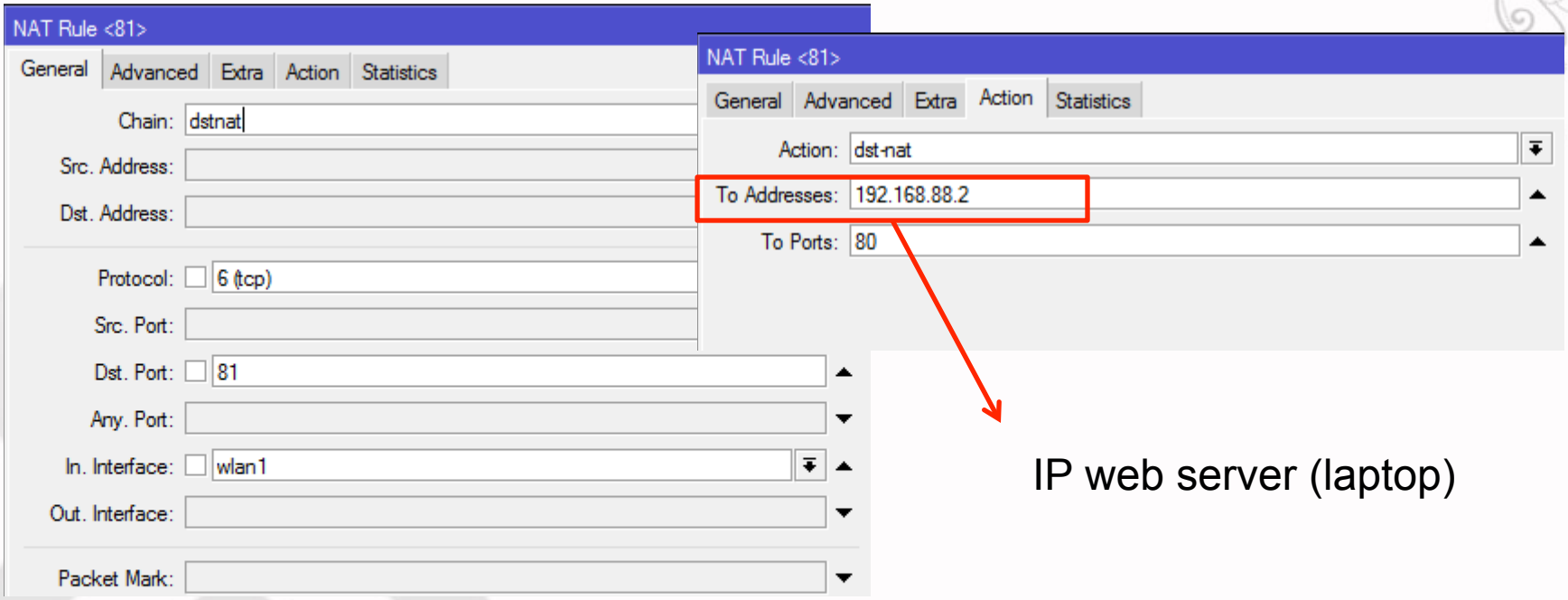
Redirect port http IP WAN router ke IP web server lokal (LAN)



http://192.168.2.2:81

LAB – Dst-nat Web Server

- Install dan Jalankan program web server di laptop
- Buat rule pada IP>Firewall>NAT untuk redirect port 81 router ke IP laptop dan port 80.



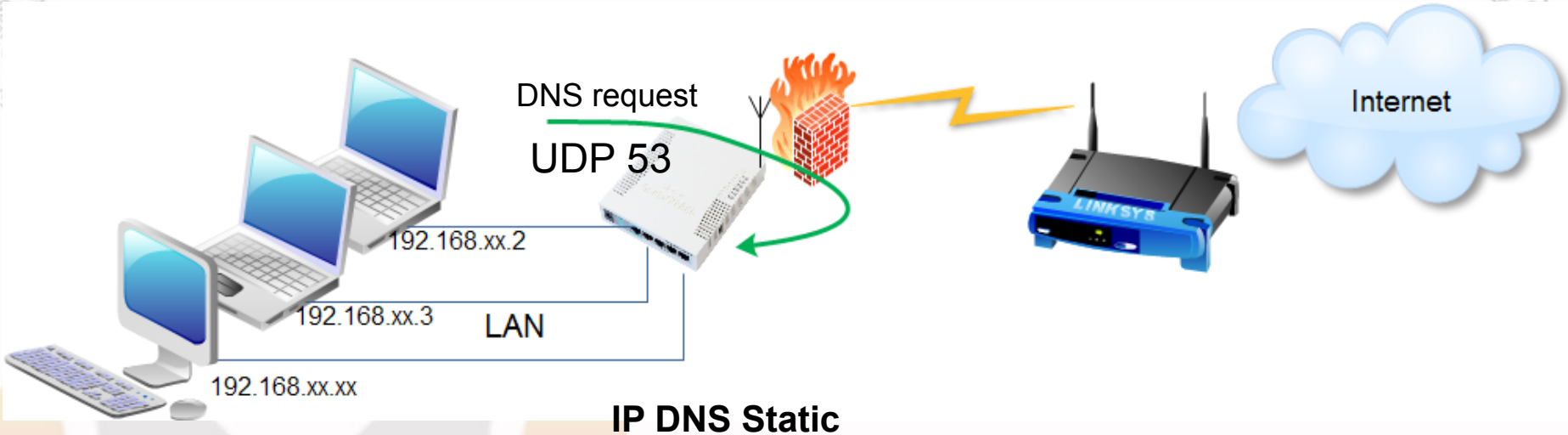
- Coba dengan http://<ip wlan router>:81 dari laptop peserta lain

DNS

- DNS (Domain Name System) berfungsi untuk menterjemahkan nama domain menjadi IP address.
- Kita lebih mudah mengingat nama domain (detik.com) dibanding dengan IP addressnya (203.190.241.43).
- DNS memiliki database/cache alamat domain dan IP address yang diperoleh dari primary DNS diatasnya.
- Client yang menggunakan DNS server akan menggunakan cache tersebut.
- Pada periode tertentu chache akan diperbaharui mengambil dari DNS server diatasnya.

LAB - Static DNS

- Paksa semua client menggunakan DNS pada router dengan port fowarding (dst-nat)
- Siapkan content warning (web server dengan tampilan index warning)
- Tambahkan static DNS yang ingin difilter



IP DNS Static

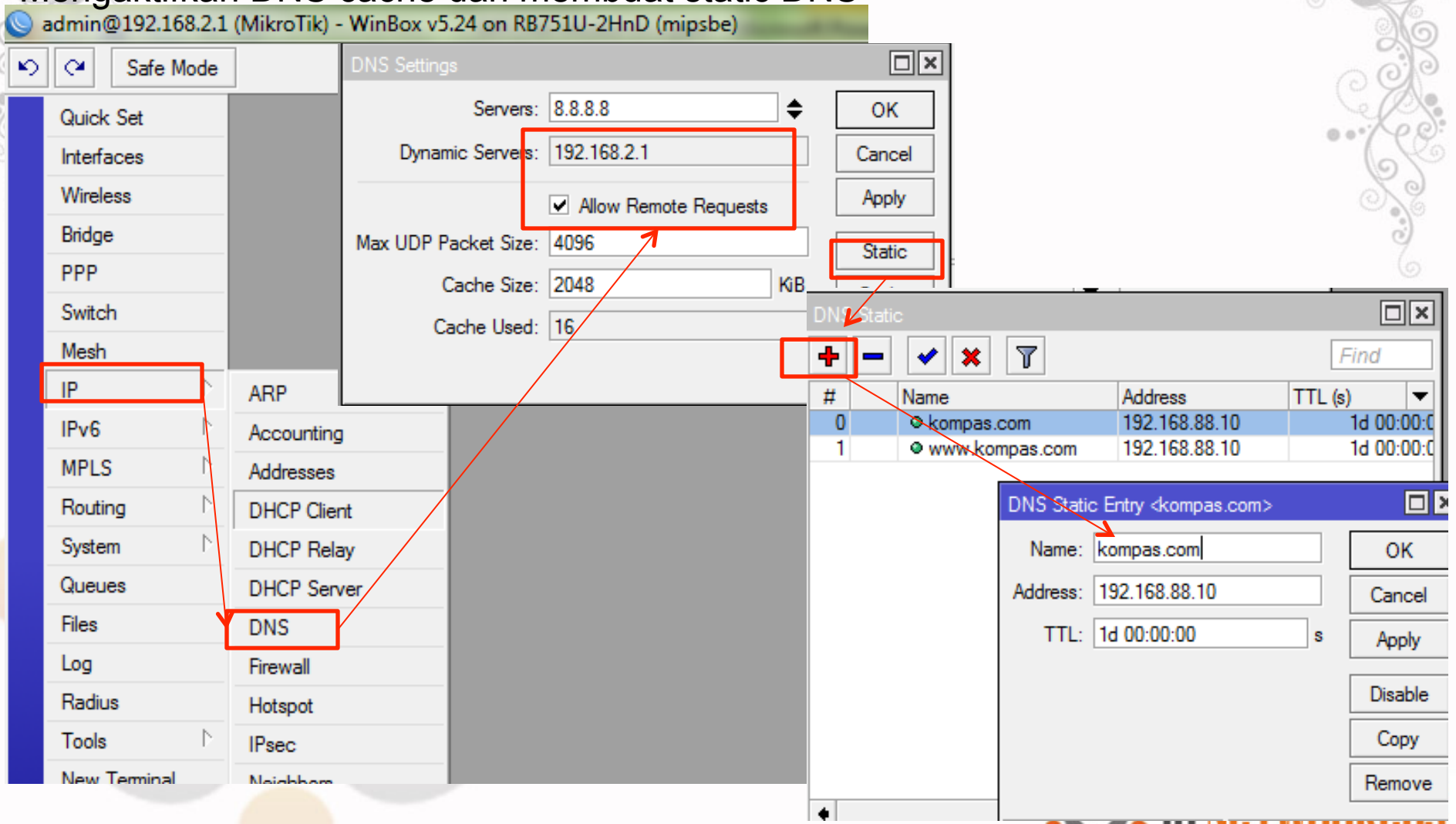
Domain	IP
Kompas.com	192.168.88.10
www.kompas.com	192.168.88.10

LAB – Transparent Static DNS

- Kita dapat memanipulasi cache DNS yang ada dengan static entry pada tabel DNS.
- Misal apabila kita ping atau akses domain kompas.com maka akan direply oleh IP address yang bukan milik kompas, diubah dengan IP yang kita tentukan sendiri
- Caranya adalah sebagai berikut:
  - Set agar router kita menjadi DNS server
  - Set Primary DNS di router kita
  - Set static DNS untuk domain yang ingin kita buat static
  - Buat rule dst-nat agar setiap traffik DNS dibelokkan ke router kita

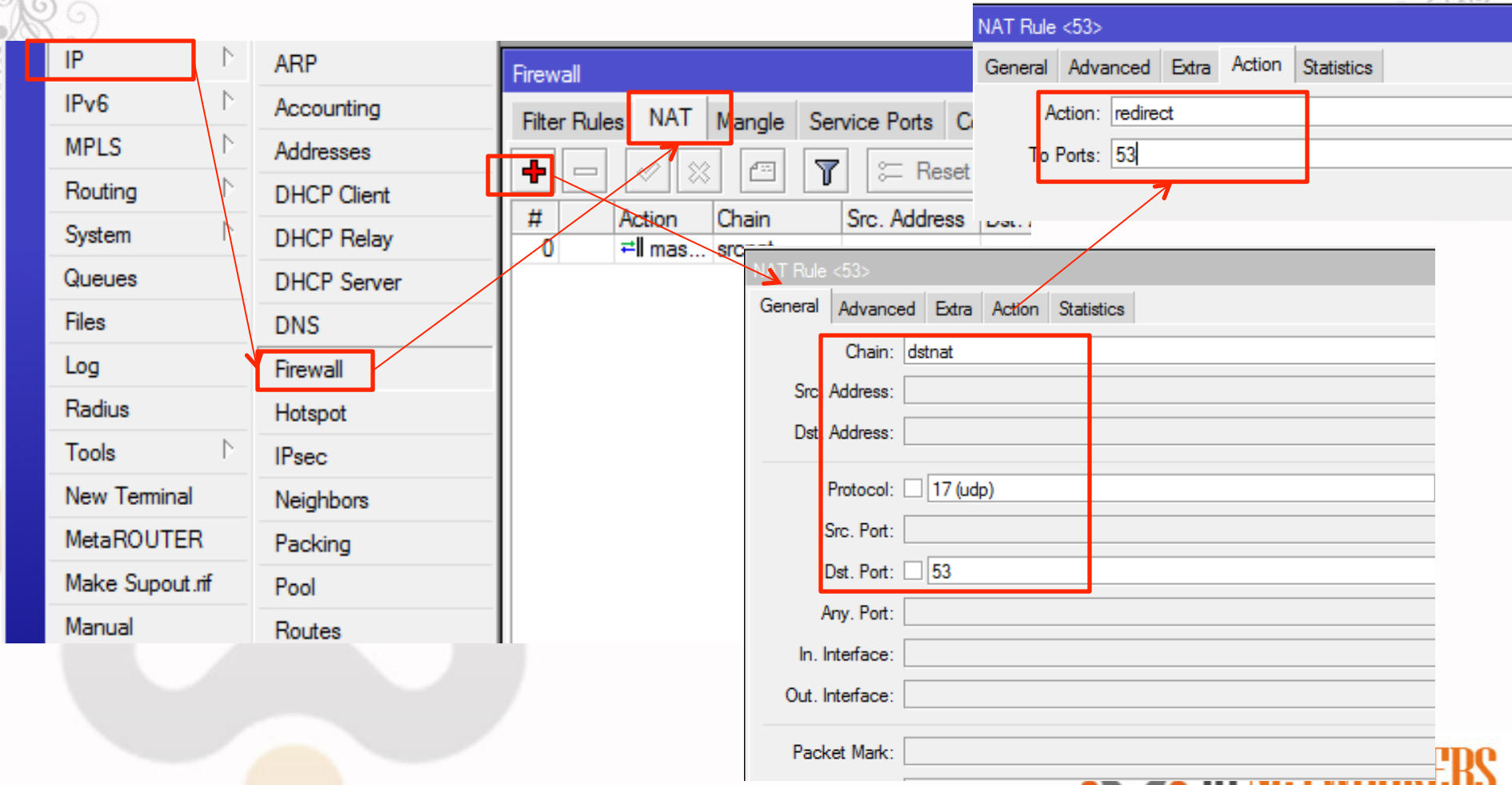
LAB - Static DNS

Mengaktifkan DNS cache dan membuat static DNS



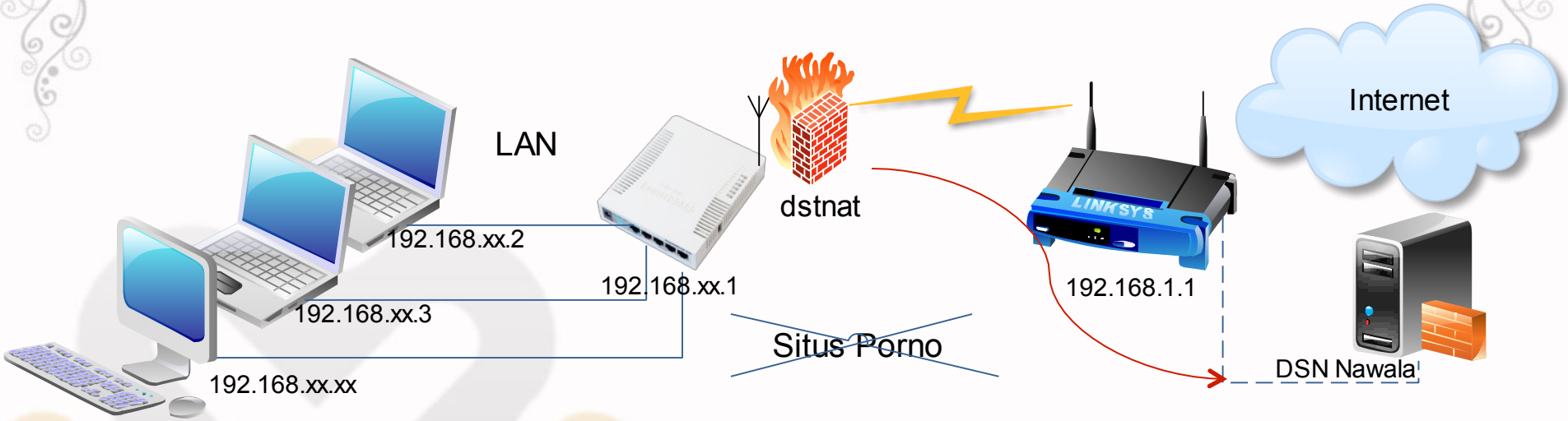
LAB - Static DNS

- Memaksa traffic dns request dari client untuk ke router



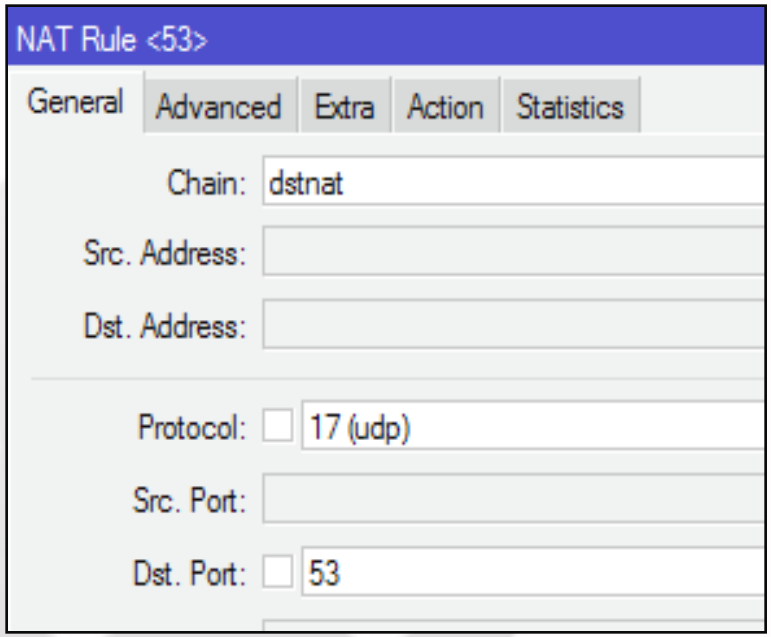
LAB-Transparent DNS Nawala

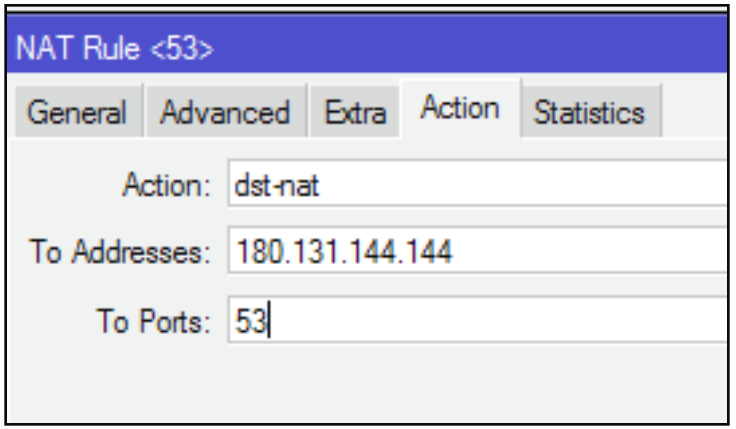
- Kita akan melakukan block situs porno dengan transparent DNS Nawala



LAB – Transparent DNS Nawala

- Transparent DNS memaksa user untuk akses DNS server tertentu
- Buatlah rule baru pada menu IP>Firewall>NAT , redirect protocol TCP dan UDP port 53 ke IP port DNS Nawala **180.131.144.144**, atau bisa juga ke DNS Norton **199.85.127.30**





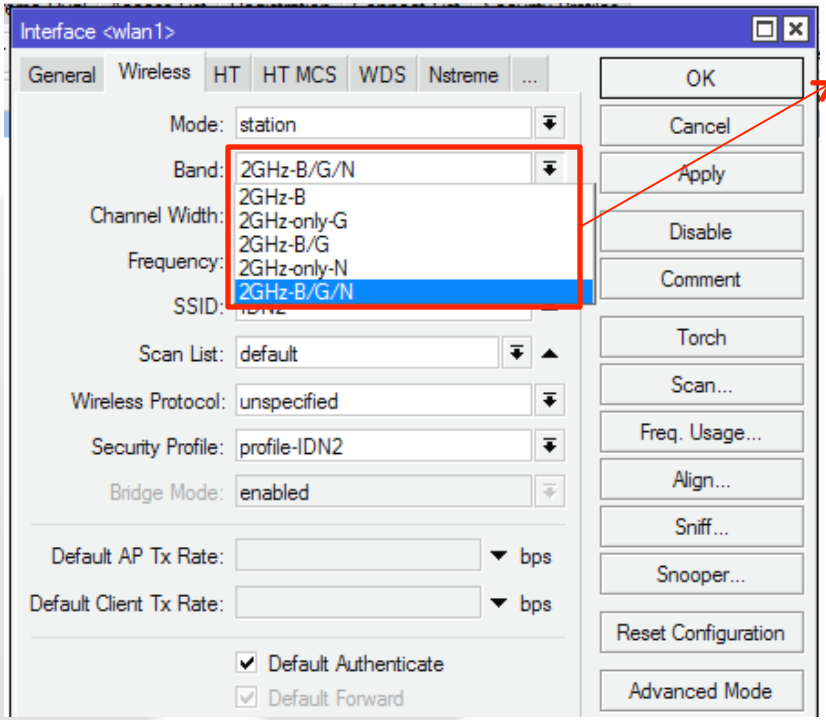
Module 3 - Wireless

Wireless pada Mikrotik

- RouterOS mendukung beberapa modul radio (wireless card) untuk jaringan WLAN atau Wi-Fi (Wireless Fidelity).
- Wi-Fi memiliki standar & spesifikasi IEEE 802.11 dan menggunakan frekuensi 2,4GHz dan 5,8GHz.
- MikroTik mendukung standar IEEE 802.11a/b/g/n
  - 802.11a – frekuensi 5GHz, 54Mbps.
  - 802.11b – frekuensi 2,4GHz, 11 Mbps.
  - 802.11g – frekuensi 2,4GHz, 54Mbps.
  - 802.11n (Level 4 keatas) – frekuensi 2,4GHz atau 5GHz, 300Mbps

Wireless Band

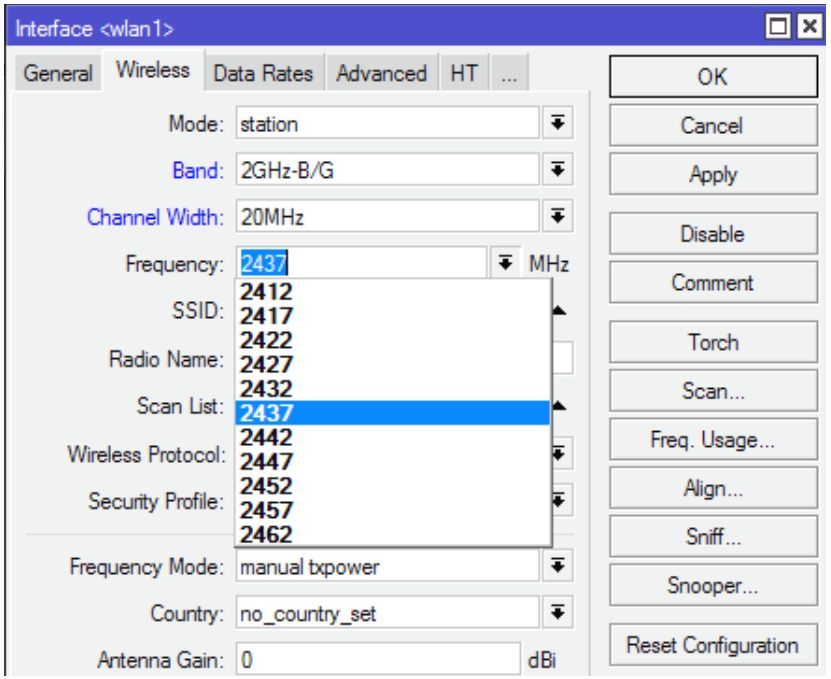
- Band merupakan mode kerja frekuensi dari suatu perangkat wireless.
- Untuk menghubungkan 2 perangkat, keduanya harus bekerja pada band frekuensi yang sama



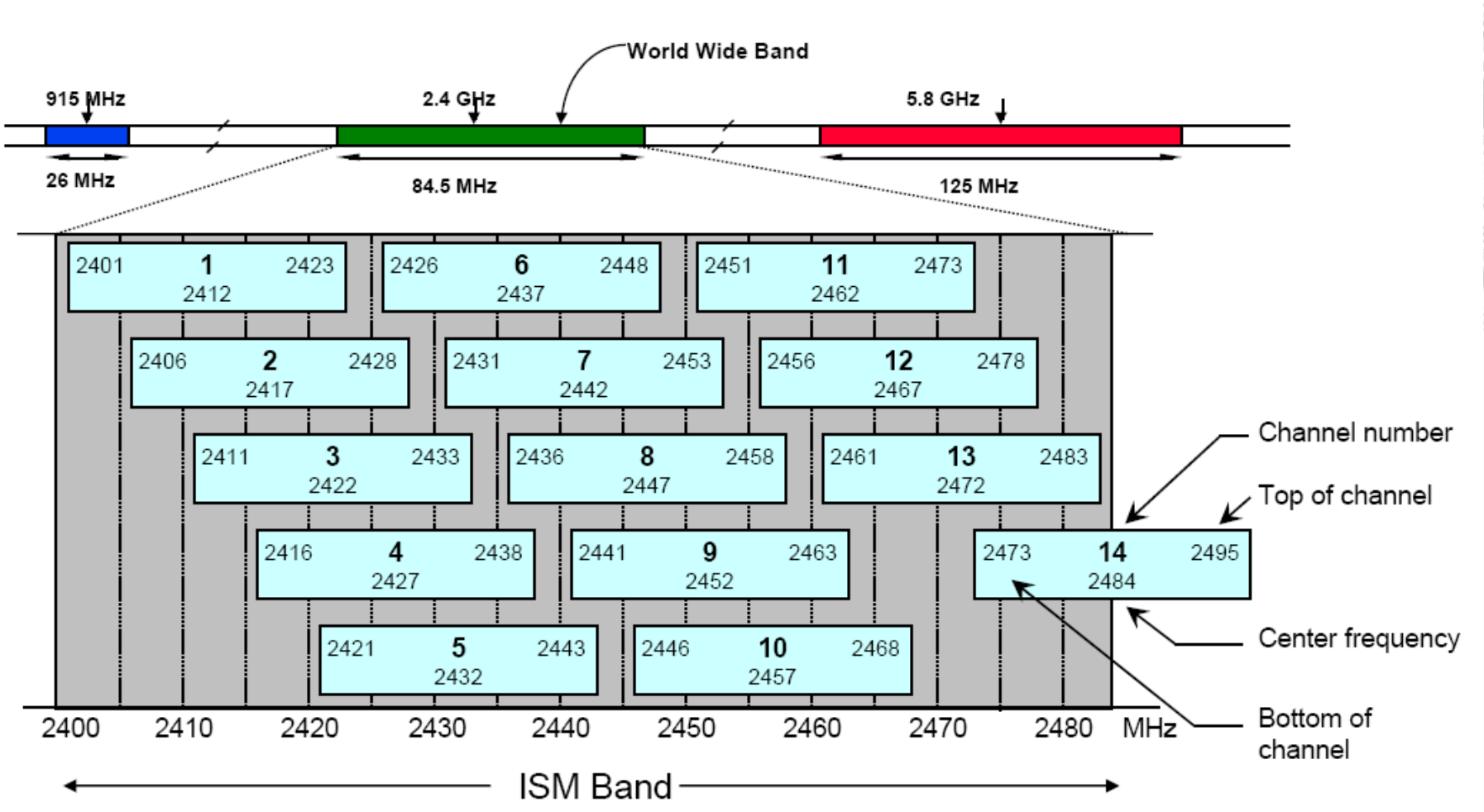
Band yang ada di list, bergantung pada jenis wireless card yang digunakan.

Wireless – Frequency Channel

- Frequency channel adalah pembagian frekuensi dalam suatu band dimana Access Point (AP) beroperasi.
- Nilai-nilai channel bergantung pada band yang dipilih**, kemampuan wireless card**, dan **aturan/regulasi frekuensi suatu negara**.
- Range frequency channel untuk masing-masing band adalah sbb:
  - 2,4Ghz = 2412 s/d 2499MHz
  - 5GHz = 4920 s/d 6100MHz

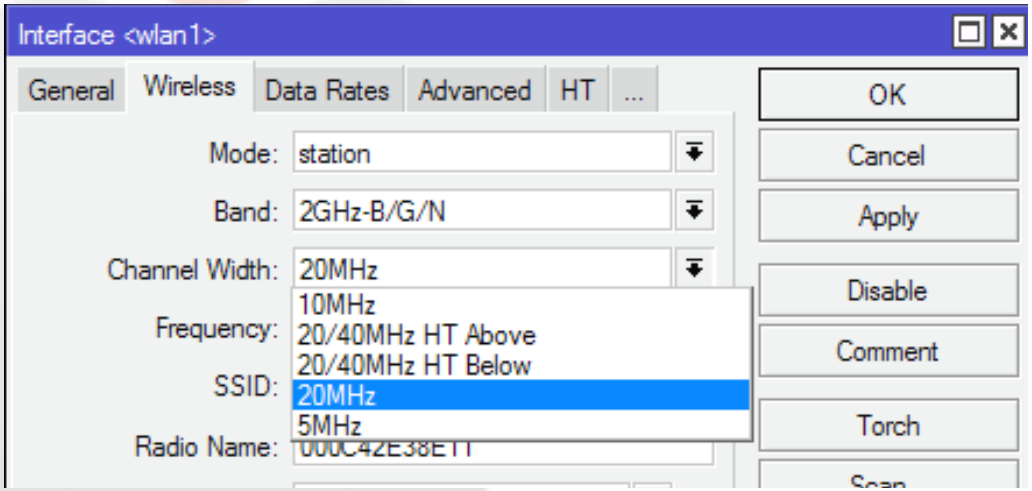


802.11 b/g Channels



Wireless – Lebar Channel

- Lebar channel adalah rentang frekuensi batas bawah dan batas atas dalam 1 channel.
- MikroTIk dapat mengatur berapa lebar channel yang akan digunakan.
- Default lebar channel yang digunakan adalah 22Mhz (ditulis 20MHz).
- Lebar channel dapat dikecilkan (5MHz) untuk meminimasil frekuensi, atau dibesarkan (40MHz) untuk mendapatkan troughtput yang lebih besar.

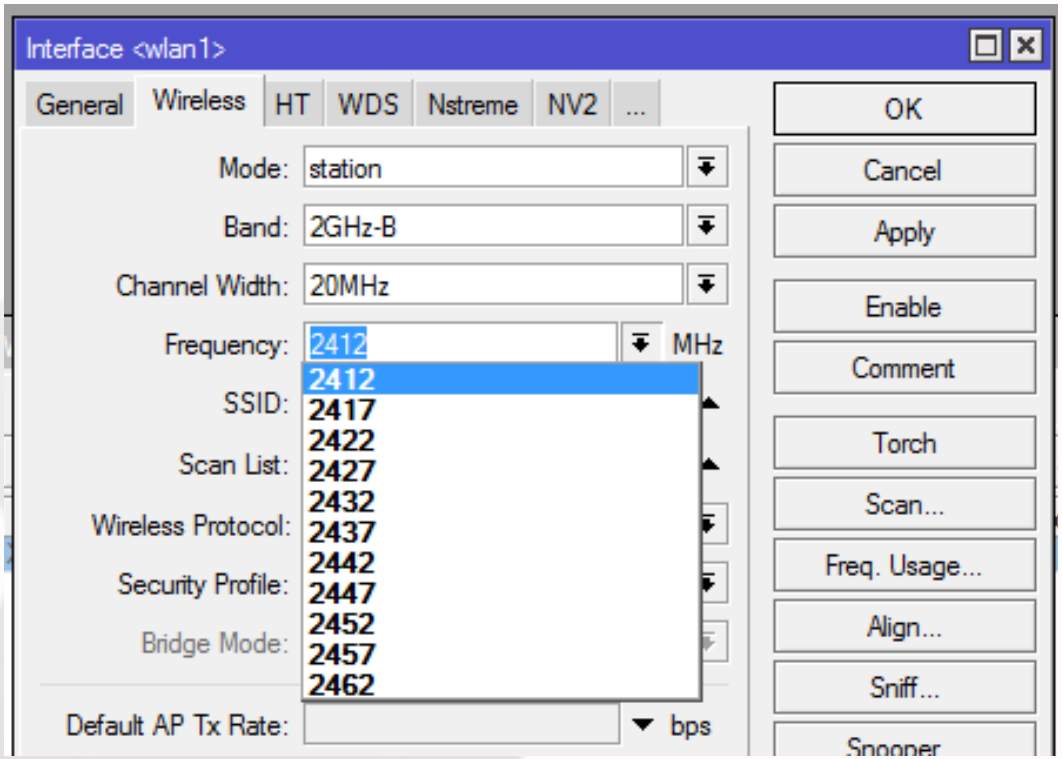


Wireless – Regulasi Frekuensi

- Setiap negara memiliki regulasi tertentu dalam hal frekuensi wireless untuk internet carrier.
- Indonesia telah merdeka untuk menggunakan frekuensi 2.4GHz berdasarkan KEPMENHUB No. 2/2005 berkat perjuangan para penggerak internet sejak tahun 2001
- Regulasi tersebut dalam mikrotik didefinisikan pada bagian Wireless “country-regulation”.
- Namun apabila diinginkan untuk membuka semua frekuensi yang dapat digunakan oleh wireless card, dapat menggunakan pilihan “**superchanne**l”.

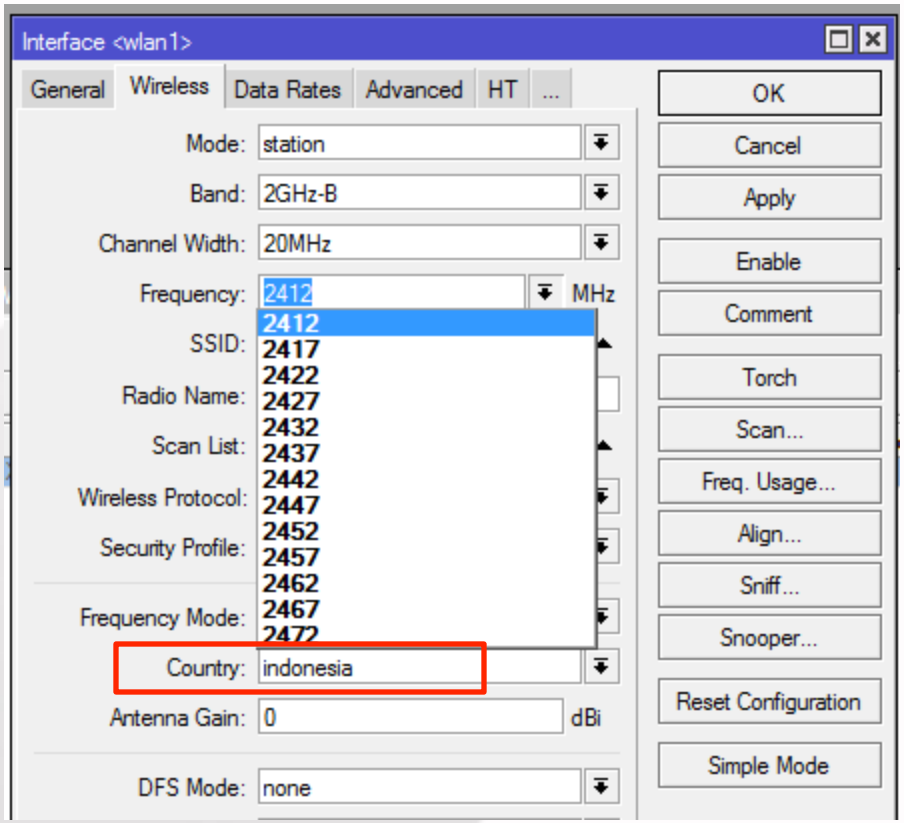
LAB-Regulasi Frekuensi

- Ada berapa channel frekuensi default MikroTik?
- Lihatnya di menu Wireless Wlan1 Wireless



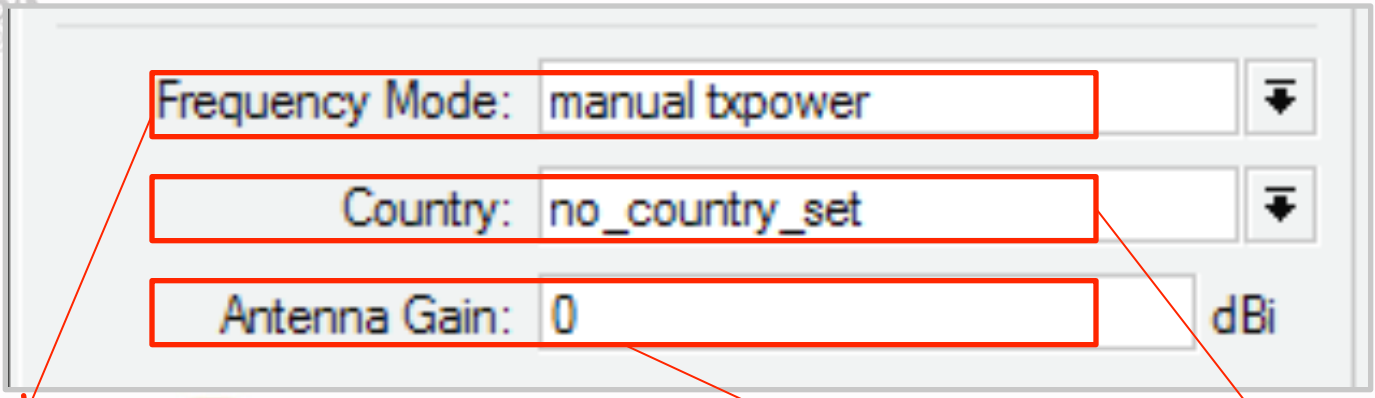
LAB-Regulasi Frekuensi

- Ada berapa channel frekuensi untuk country regulation Indonesia?
- Lihatnya di menu Wireless Wlan1 Wireless Advanced Mode



Coba ganti Frekuensi
Mode = Superchannel

LAB-Regulasi Frekuensi



Frequency Mode

1. manual-tx-power

   Transmit power diatur manual (tidak menyesuaikan dengan negara tertentu).

2. regulation-domain

   Frekuensi channel disesuaikan dengan frekuensi-frekuensi yang diijinkan di suatu negara.

3. Superchannel

   Membuka semua frekuensi yang bisa disupport oleh wireless card

Pemilihan Country / Negara

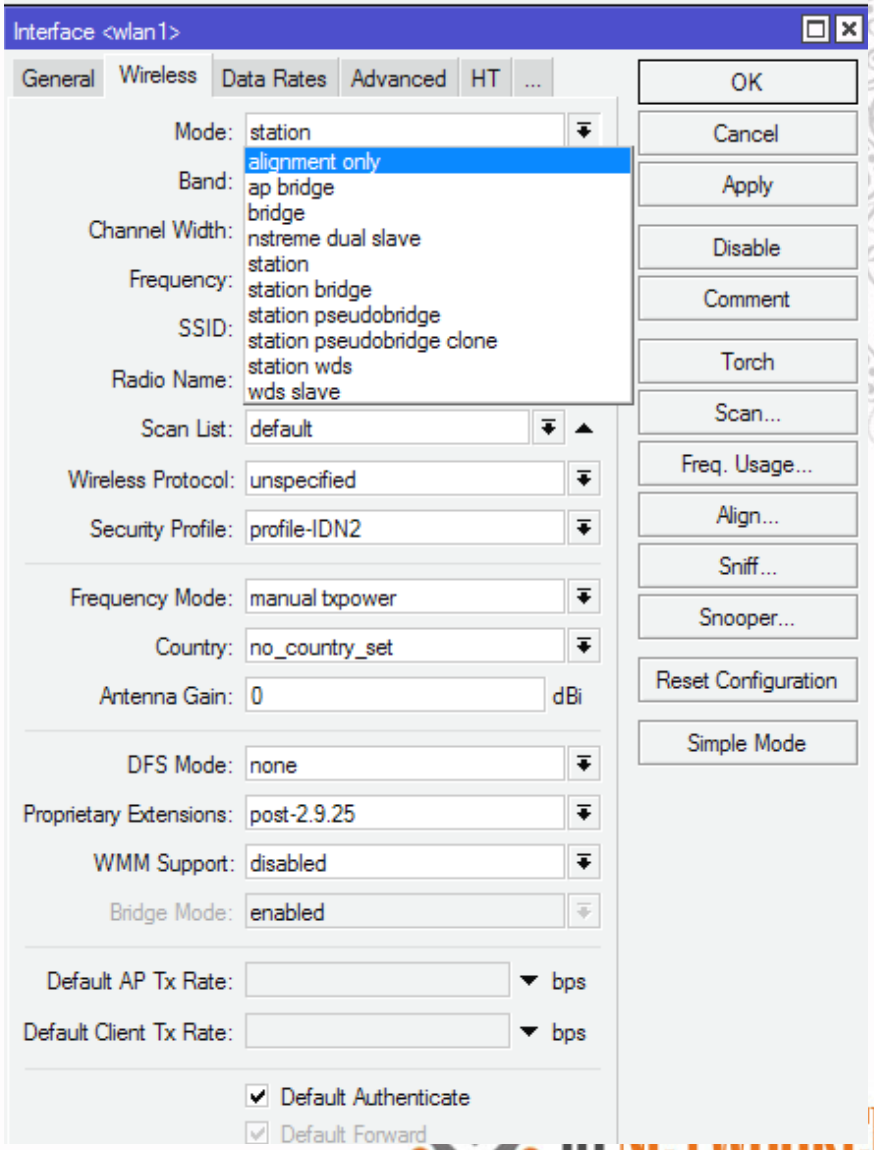
Default 0, akan otomais menyesuaikan agar tidak melebihi EIRP country regulation

Konsep Koneksi Wireless

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

Mode Interface Wireless

- Aligement Only
- AP Bridge
- Bridge
- Nstream dual slave
- Station
- Station bridge
- Station pseudobridge
- Station pseudobridge clone
- Station wds
- Wds slave



Mode Interface Wireless

AP Mode

- **AP-bridge** – wireless difungsikan sebagai Akses Poin.
- **Bridge** - hampir sama dengan AP-bridge, namun hanya bisa dikoneksi oleh 1 station/client, mode ini biasanya digunakan untuk point-to-point.

Station Mode

- **Station –** scan dan conent AP dengan frekuensi & SSID yang sama, mode ini TIDAK DAPAT di BRIDGE
- **Station-bridge** – sama seperti station, mode ini adalah MikroTik proprietary. Mode untuk L2 bridging, selain wds.
- **Station-wds** – sama seperti station, namum membentuk koneksi WDS dengan AP yang menjalankan WDS.
- **station-pseudobridge** – sama seperti *station*, dengan tambahan MAC address translation untuk bridge.
- ***station-pseudobridge-clone*** – Sama seperti *station-pseudobridge*, menggunakan **station-bridge-clone-mac** address untuk konek ke AP.

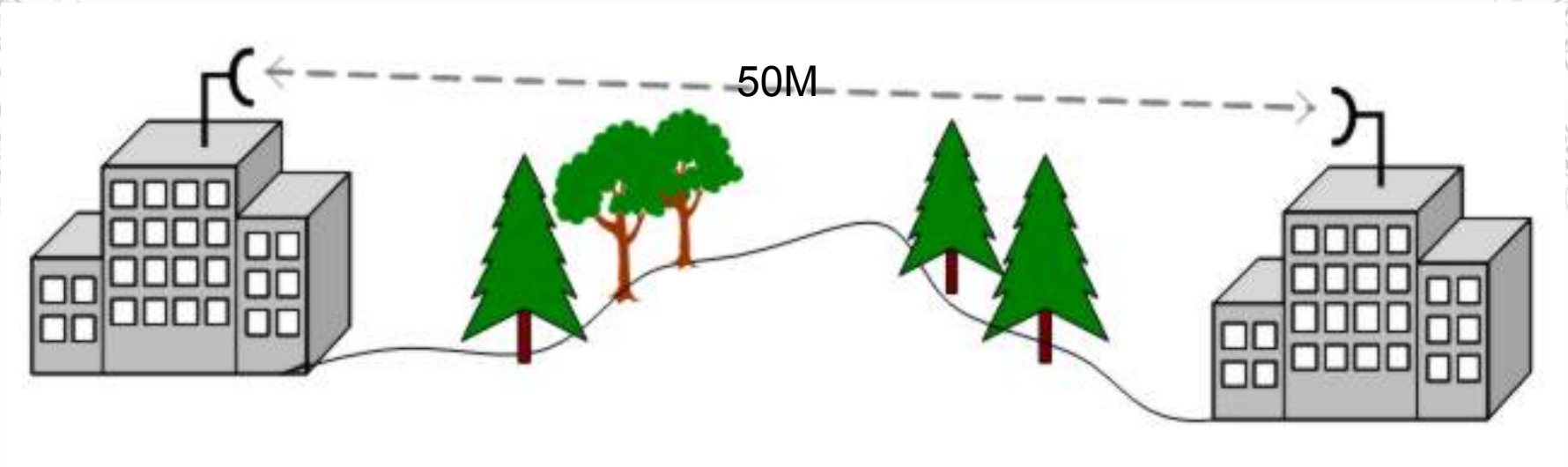
Interface Wireless Mode

Special Mode

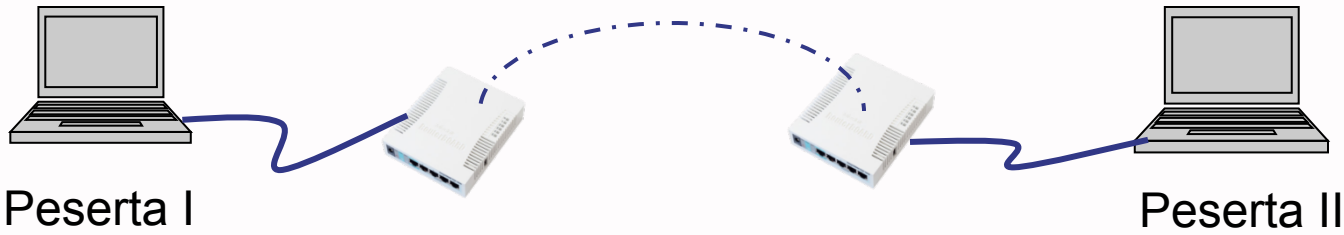
- **alignment-only** – mode transmit secara terus-menerus digunakan untuk positioning antena jarak jauh.
- **nstreme-dual-slave** – digunakan untuk sistem nstreme-dual.
- **WDS-slave** - Sama seperti ap-bridge, namun melakukan scan ke AP dengan SSID yang sama dan melakukan koneksi dengan WDS. Apabila link terputus, akan melanjutkan scanning.

LAB – Wireless AP & Station

- Buatlah link point to point untuk melewatkan bandwith minimal 10M



LAB – Wireless AP & Station



Konfigurasi	Peserta I	Peserta II
Mode	AP-Bridge/Bridge	Station
Band	Samakan	
SSID	Samakan (unik untuk tiap pasangan)	
Frequensi	Pilih	Tidak harus sama
Security Profile	Samakan	
IP address wlan1	10.10.10.1/24	10.10.10.2/24

LAB – Wireless AP & Station

- Satu peserta manjadi Acess Point, satunya menjadi Station (wireless mode)
- Samakan SSID, band dan security profile.
- Setting IP Address interface wlan:

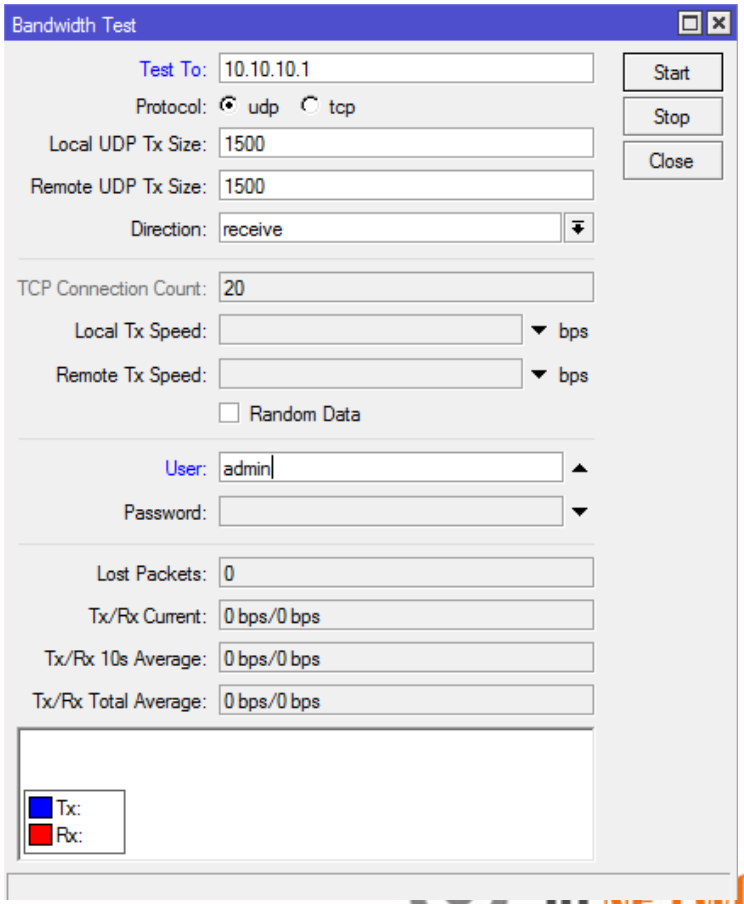
  IP AP= 10.10.10.1/24

  IP station = 10.10.10.2/24
- Pastikan koneksi wireless (layer 1) terhubung, baru dapat dilakukan ping antar IP (layer 3)
- Lakukan ping dari masing-masing MikroTik.
- Lakukan bandwidth test antar Mikrotik

Bandwidth Test

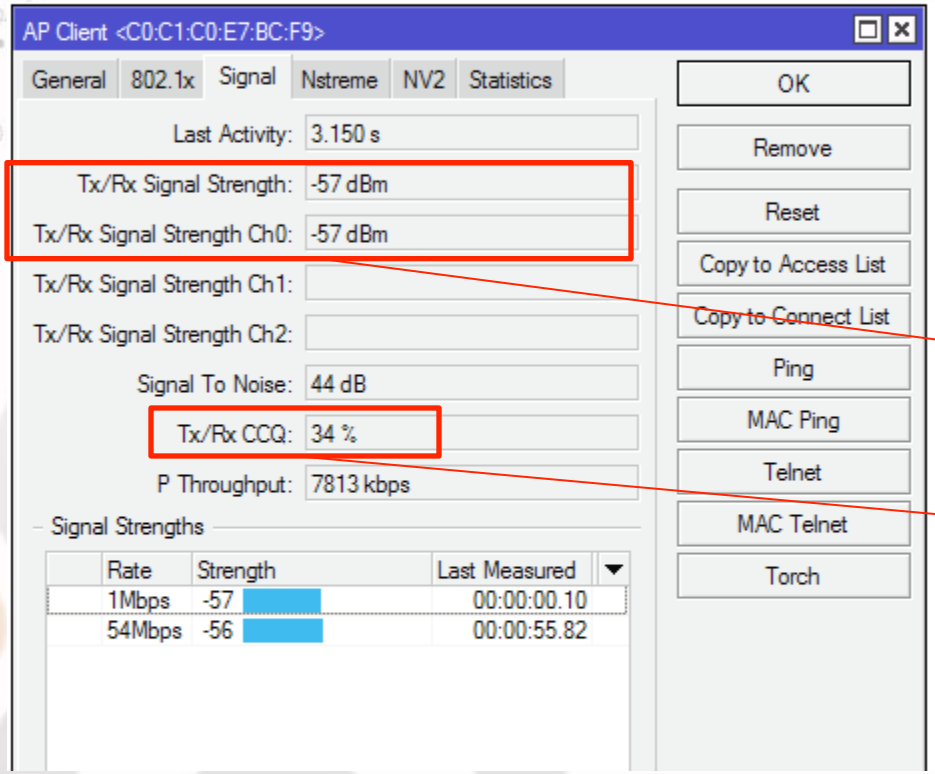
- Bandwidth test digunakan untuk mengukur seberapa besar link dapat mendeliver bandwidth

- Untuk menjamin keakuratan, Bandwidth test hanya dijalankan disatu sisi
- Test to = IP lawan kita
- User & password = user password router yang kita test



LAB – Wireless AP & Station

- Coba gantilah frekuensi untuk mendapatkan signal terbaik.



Signal yang dikirim dan diterima oleh antena

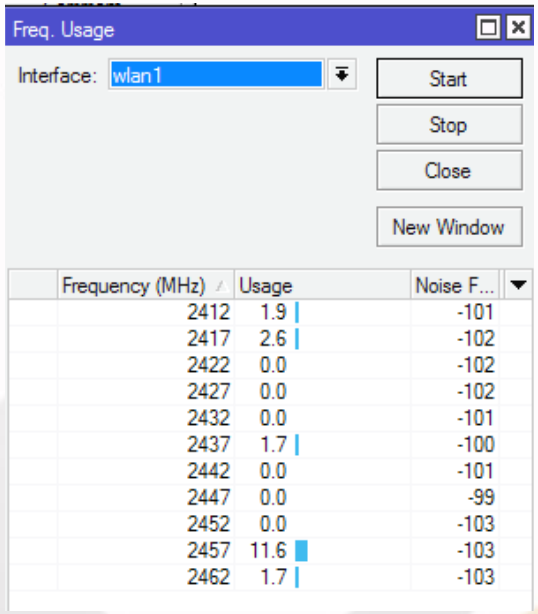
Client Connection Quality (CCQ) yaitu nilai yang menyatakan seberapa efektifkah kapasitas bandwidth yang dapat digunakan

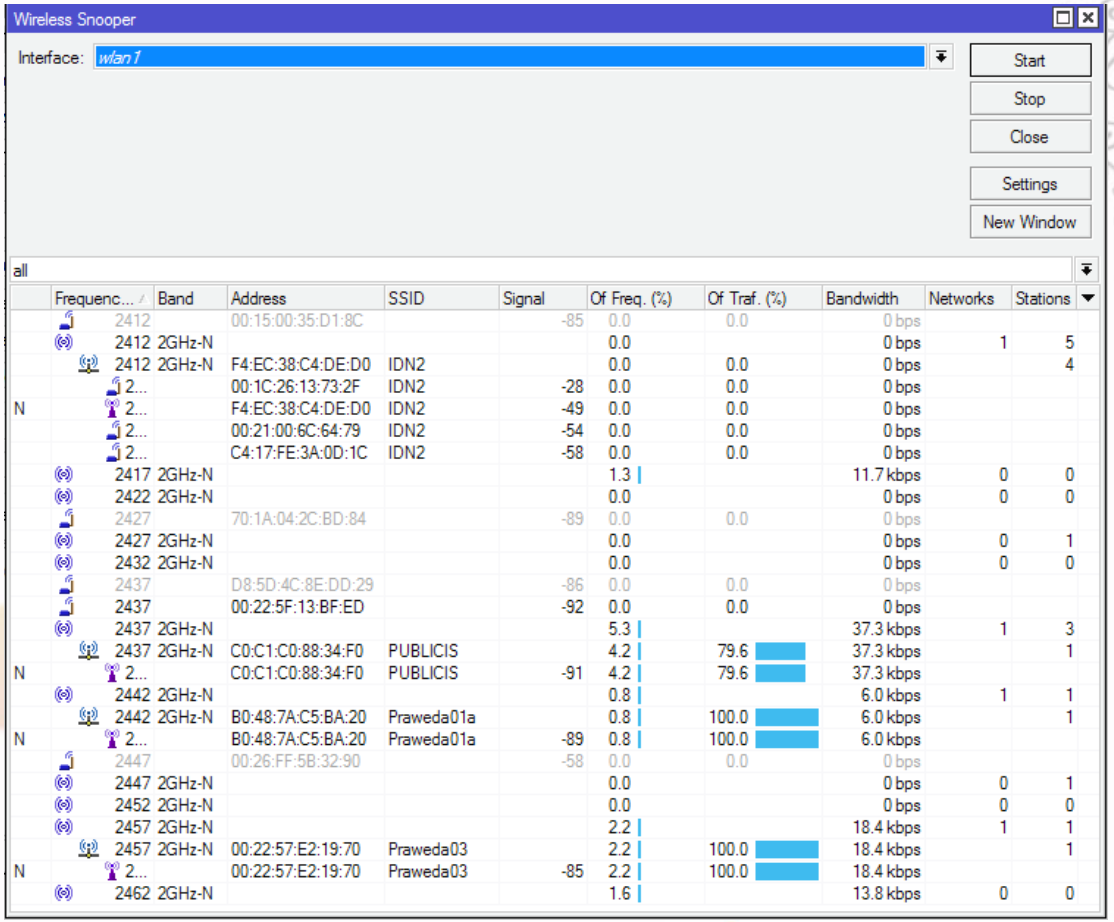
Wireless Tools

- Ada beberapa tool dalam wireless MikroTik yang dapat digunakan untuk optimasi link.
  - **Scan** – untuk melihat informasi AP yang aktif, beserta SSID dan memudahkan untuk membuat koneksi ke AP aktif tersebut.
  - **Align** – untuk pointing antenna.
  - **Sniff** – untuk melihat lalu lintas paket data di jaringan.
  - **Snooper** – seperti tool scan, informasi AP yang aktif secara lengkap, SSID, channel yang digunakan, signal strength, utilisasi/traffic load dan jumlah station pada masing-masing AP.
  - **Bw Test** – digunakan untuk test bandwidth khusus untuk MikroTik, bw test dapat didownload di web resmi MikroTik.

LAB – Wireless Tools

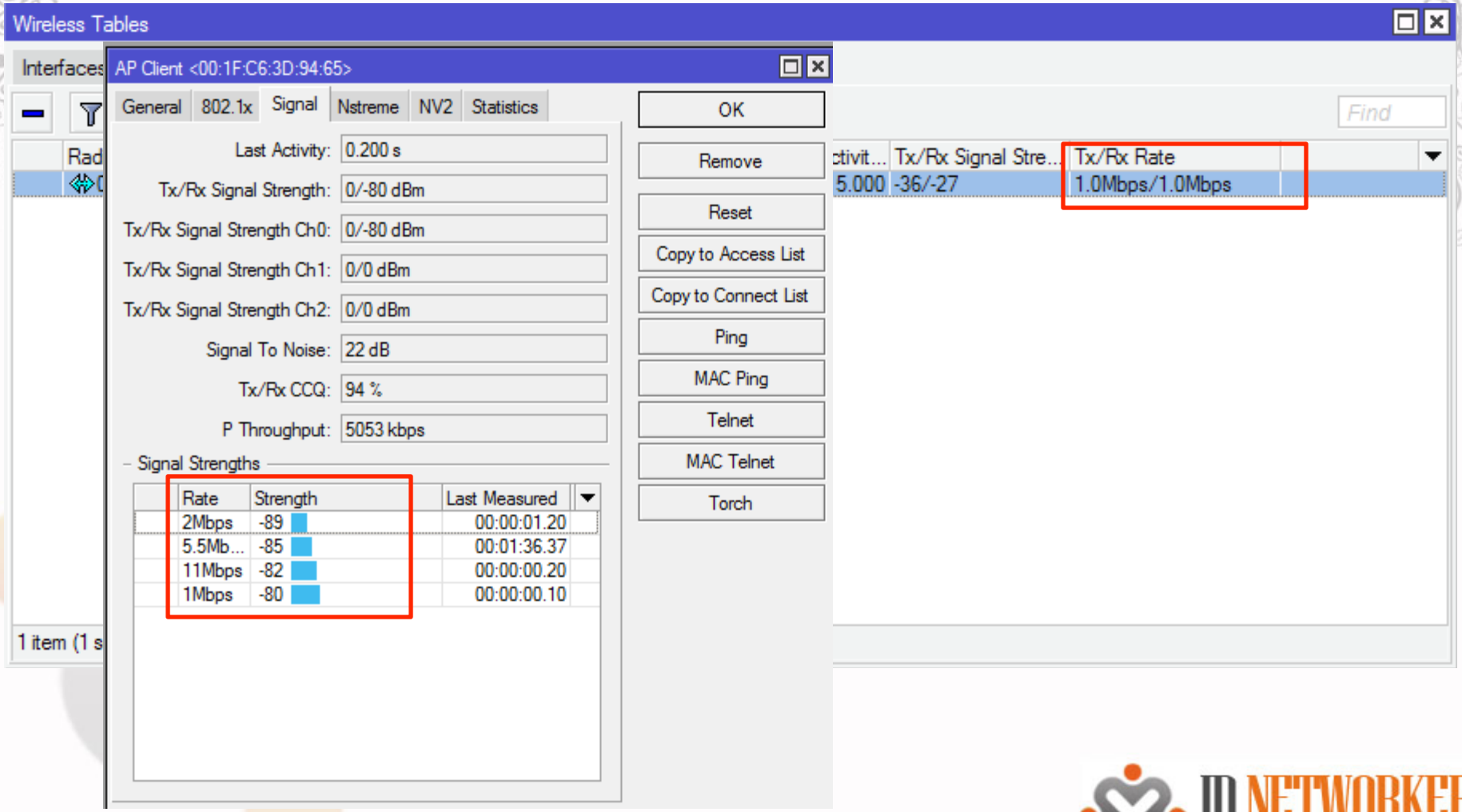
- Gunakan tool Frequency Use dan Snooper untuk pemilihan channel yang optimum, serta lakukan bandwidth test.





LAB-Rate flapping

- Max data rate dapat dilihat di Wireless>Registration

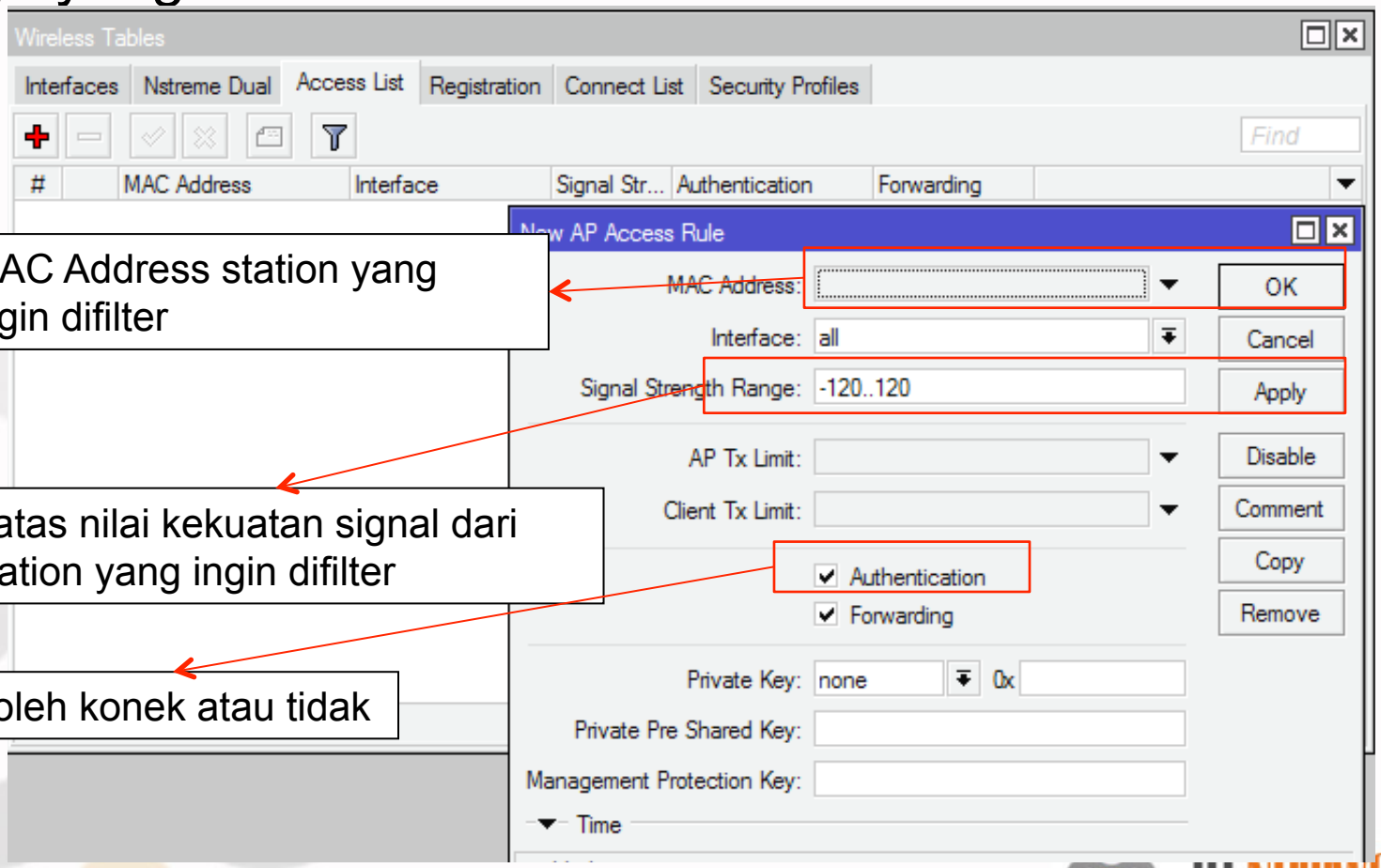


Wireless MAC Filtering

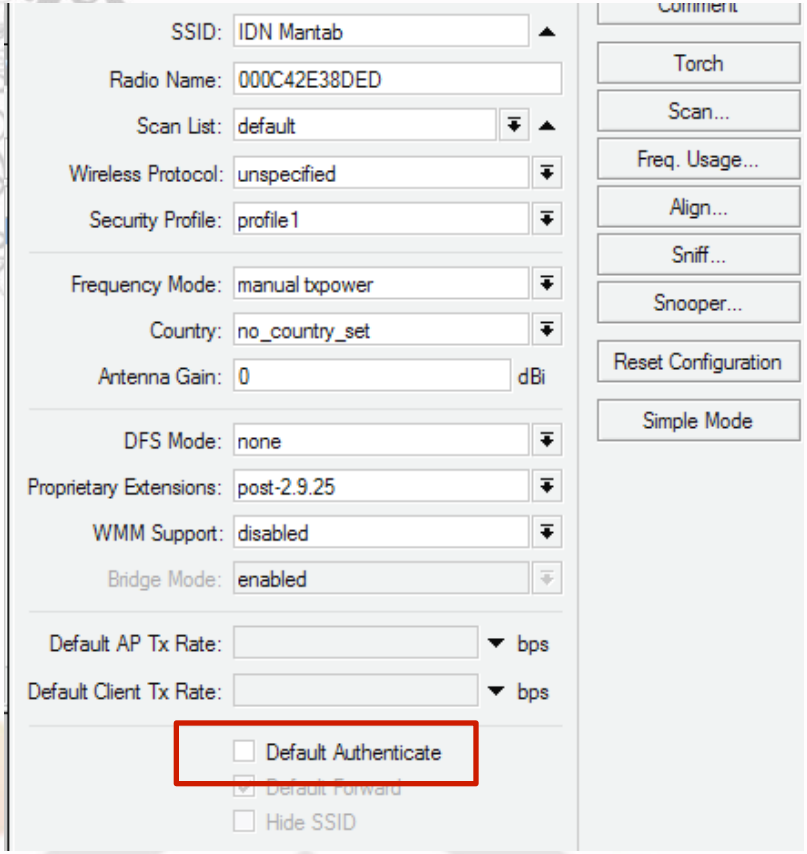
- **Access Point**, dapat dilakukan pembatasan hak akses dimana AP hanya dapat dikonek oleh station yang sudah kita tentukan.
- **Station**, juga dapat dilock agar terkoneksi dengan AP yg sudah ditentukan.
- Mac filtering AP ada di Access List
- Mac filtering Station ada di Connect List.

Access Point – Access List

- Access List pada Access Point, memfilter station mana saja yang boleh terkoneksi



Access Point – Default Authenticate

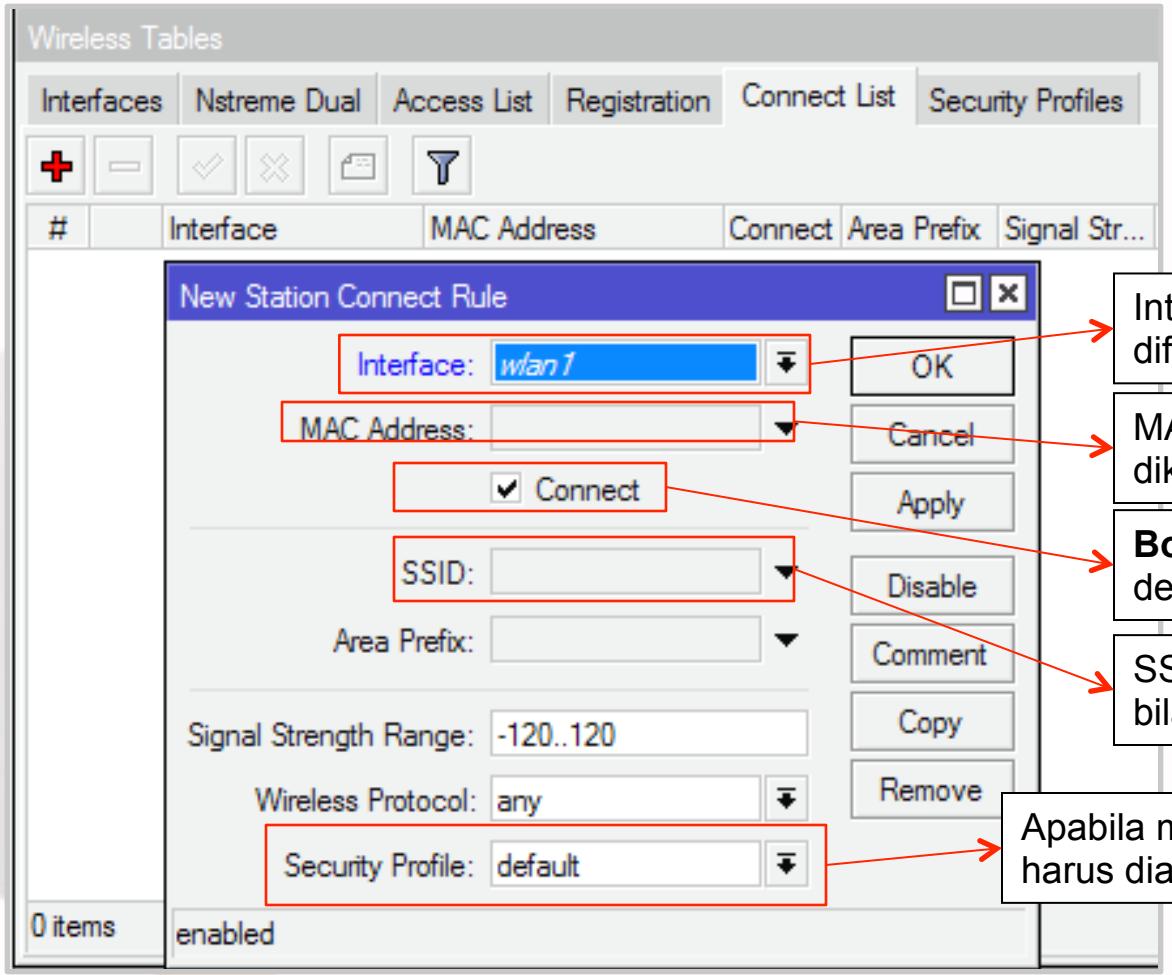


Access List dapat berfungsi apabila wireless default authenticate di non aktifkan (uncheck).

Artinya by default station tidak akan bisa konek ke AP apabila tidak di allow di Access List

Station – Connection List

- Pada wireless Station, Connect List membatasi AP mana saja yang boleh/tidak boleh terkoneksi



Interface radio yang difungsikan sebagai client

MAC address AP yang akan dikoneksikan.

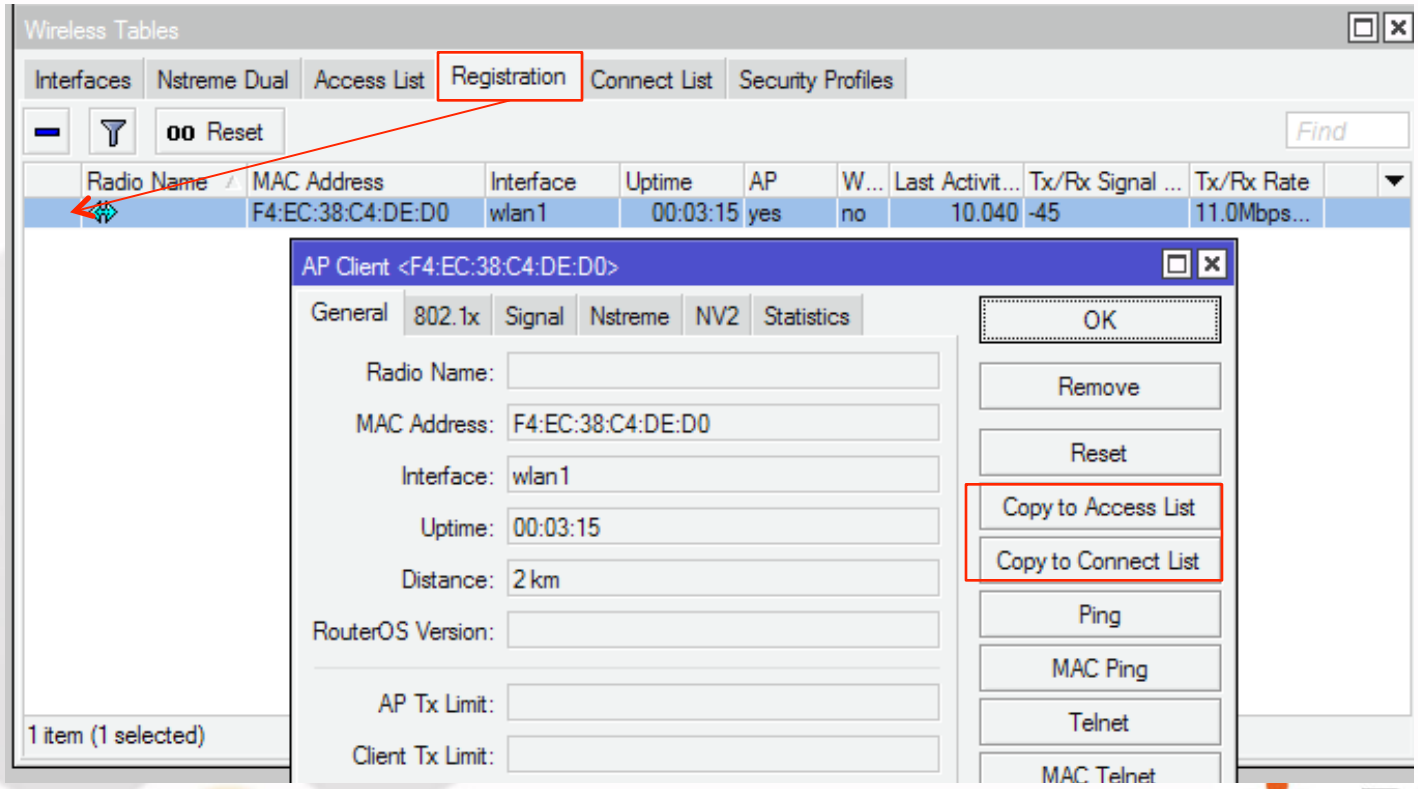
Boleh / tidak boleh konek dengan MAC diatas

SSID yang ingin dikoneksikan, bila kosong berarti any AP.

Apabila menggunakan security profile, harus diapply di ruleConnect List

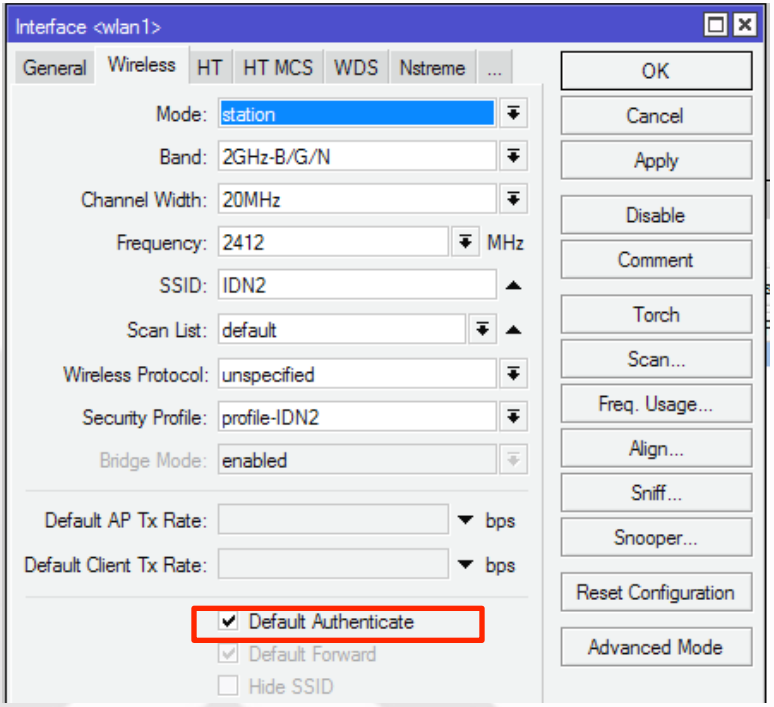
Registration List

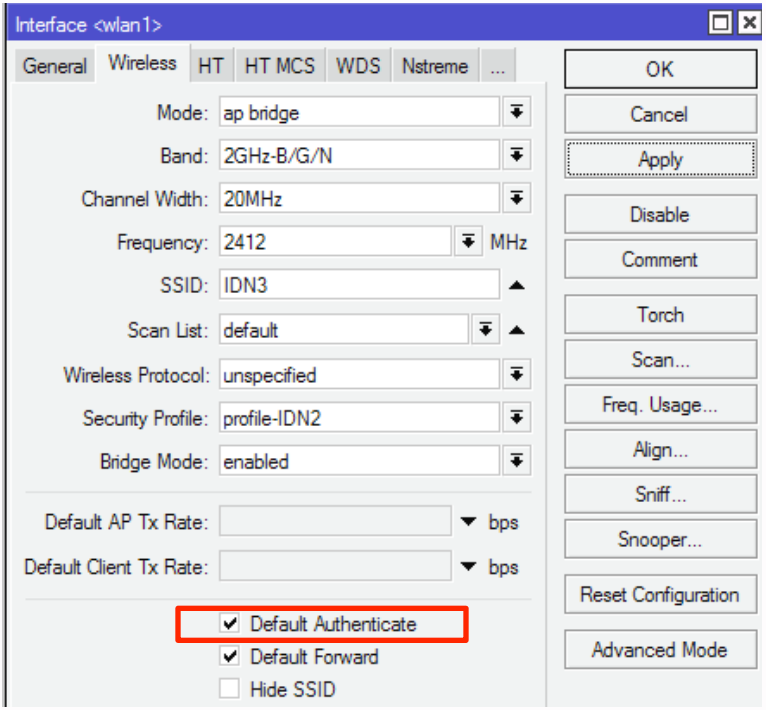
- Pada Access Point dan Station, Registered List berisi data AP/station yang sedang terkoneksi.
- Untuk memudahkan filtering pada Access List dan Connection List, menggunakan menu “Copy to Access/Connect List”



Default Authenticated

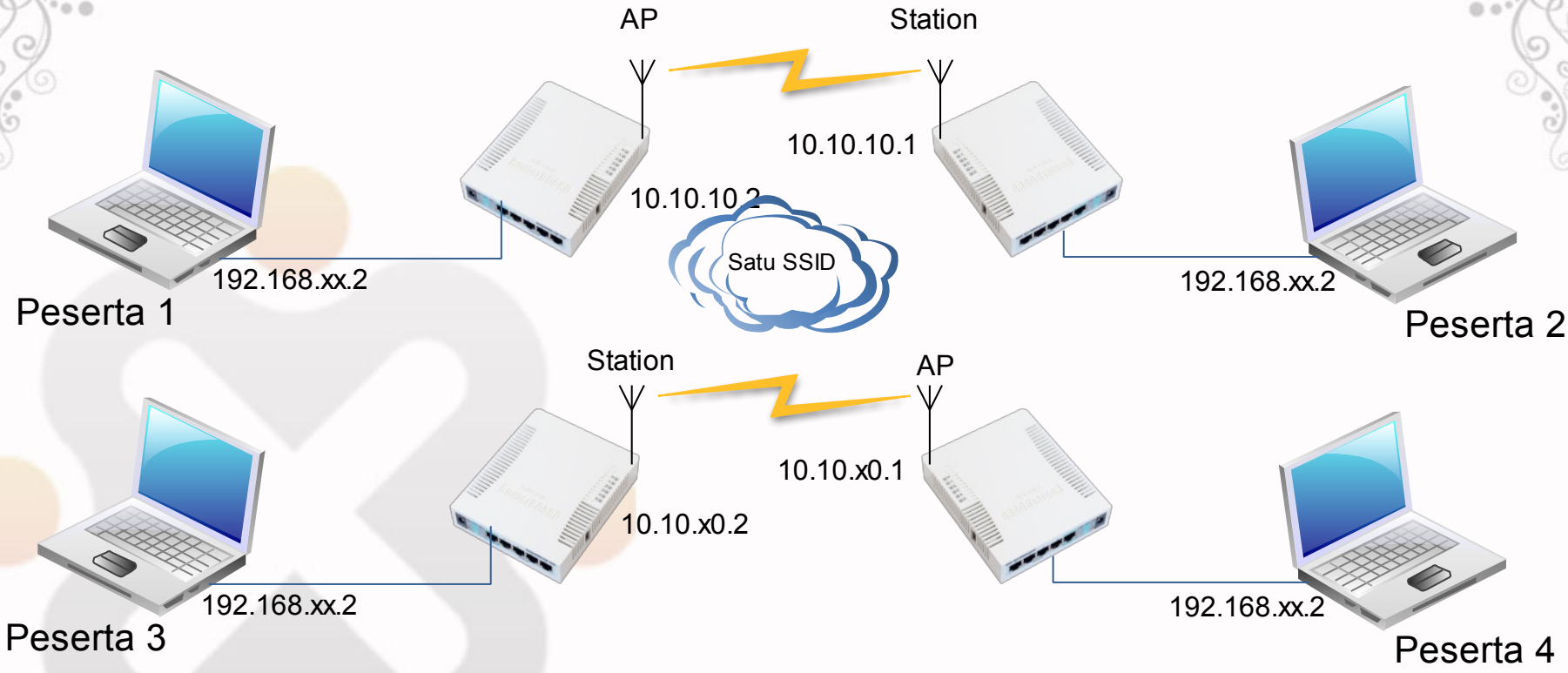
- Untuk menggunakan pilihan Connection List atau Access List baik pada AP atau Station Default Authenticated harus di uncheck.





LAB-Wireless Mac Filtering

Buatlah topologi AP-Station dengan SSID yang sama.

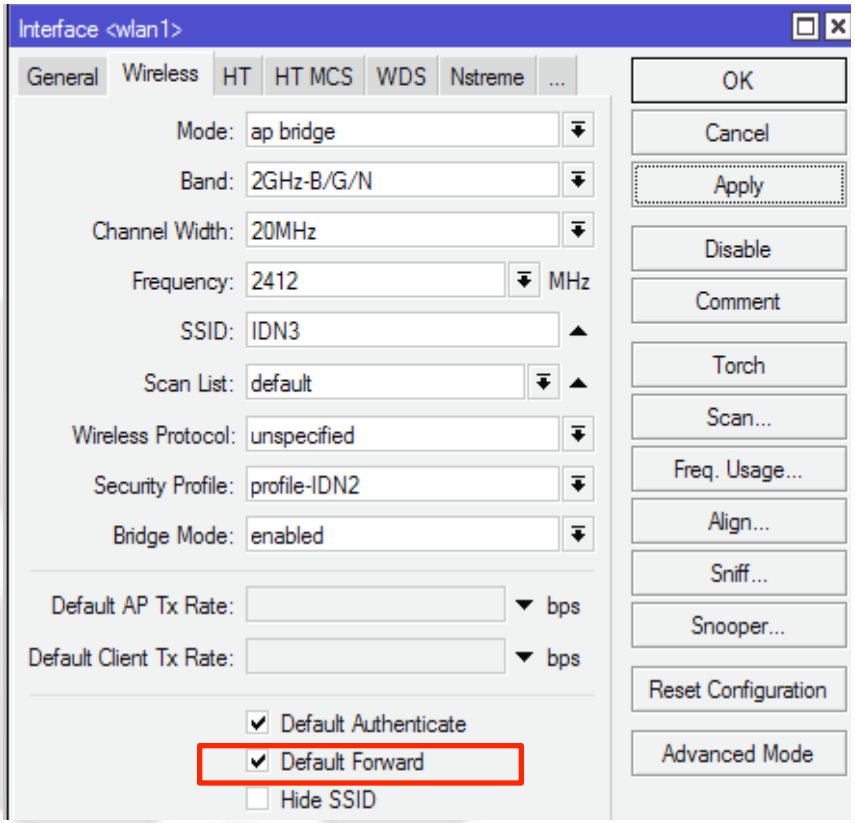


LAB – MAC Filtering

- Filter mac address agar koneksi point to point anda dengan partner tidak mudah dikacaukan oleh koneksi lain.
- Masukkan data mac address wireless partner ke list yang benar.
- Jika sebagai Station masukkan kedalam Connect-List, apabila sebagai AP masukkan dalam Access-List.
- Untuk setting wireless pada AP, default authenticate harus di-uncheck, agar tidak semua client bisa teraouthentikasi secara otomatis.
- Coba untuk konek ke AP yang bukan pasangan

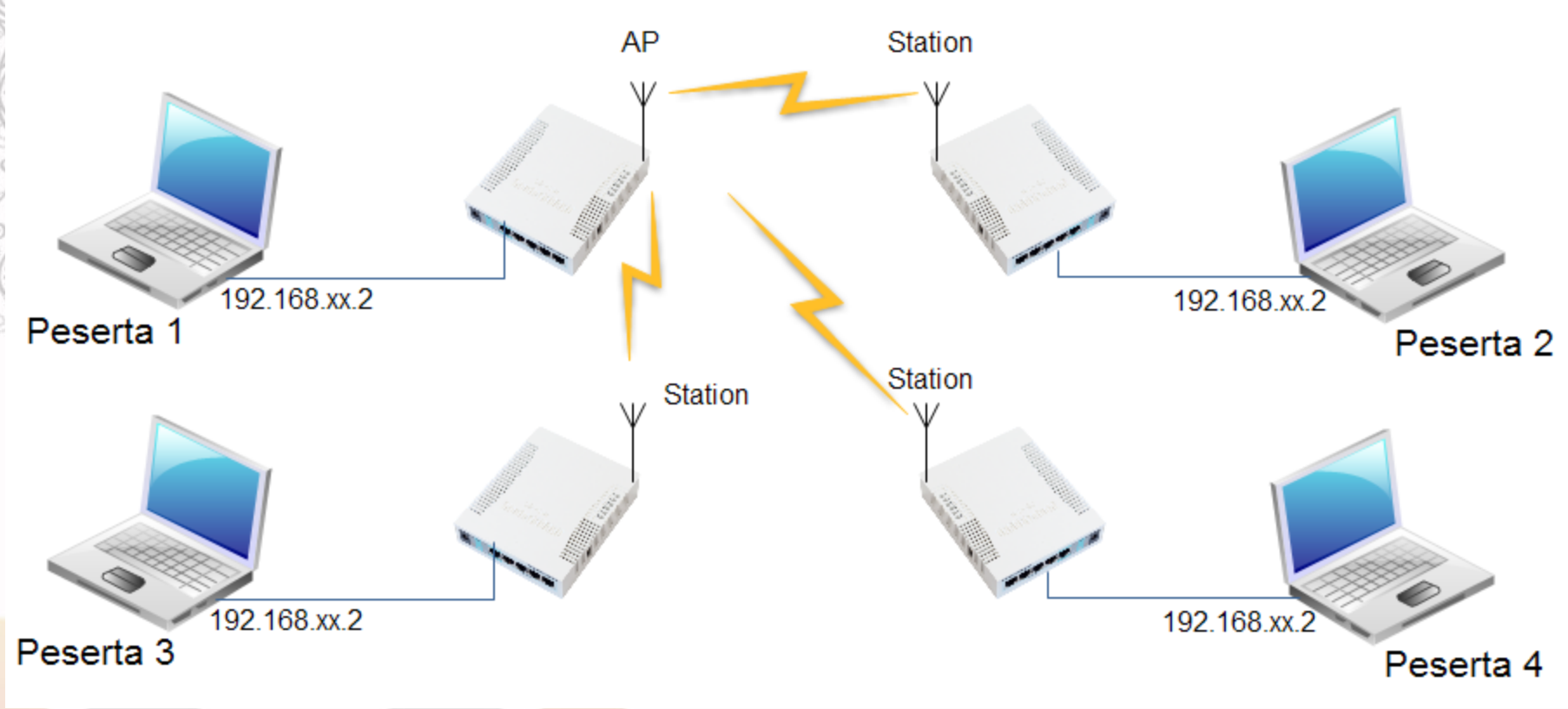
Drop Koneksi Antar Client

- Default forward (hanya dapat diseting pada Access Point).
- Digunakan untuk mengijinkan/tidak komunikasi antar client/station yang terkoneksi dalam 1 Access Point.



- Default forward biasanya didisable untuk alasan keamanan.
- Sesama station tidak dapat berkomunikasi, apabila default forward di uncheck

LAB – Default Fowarding



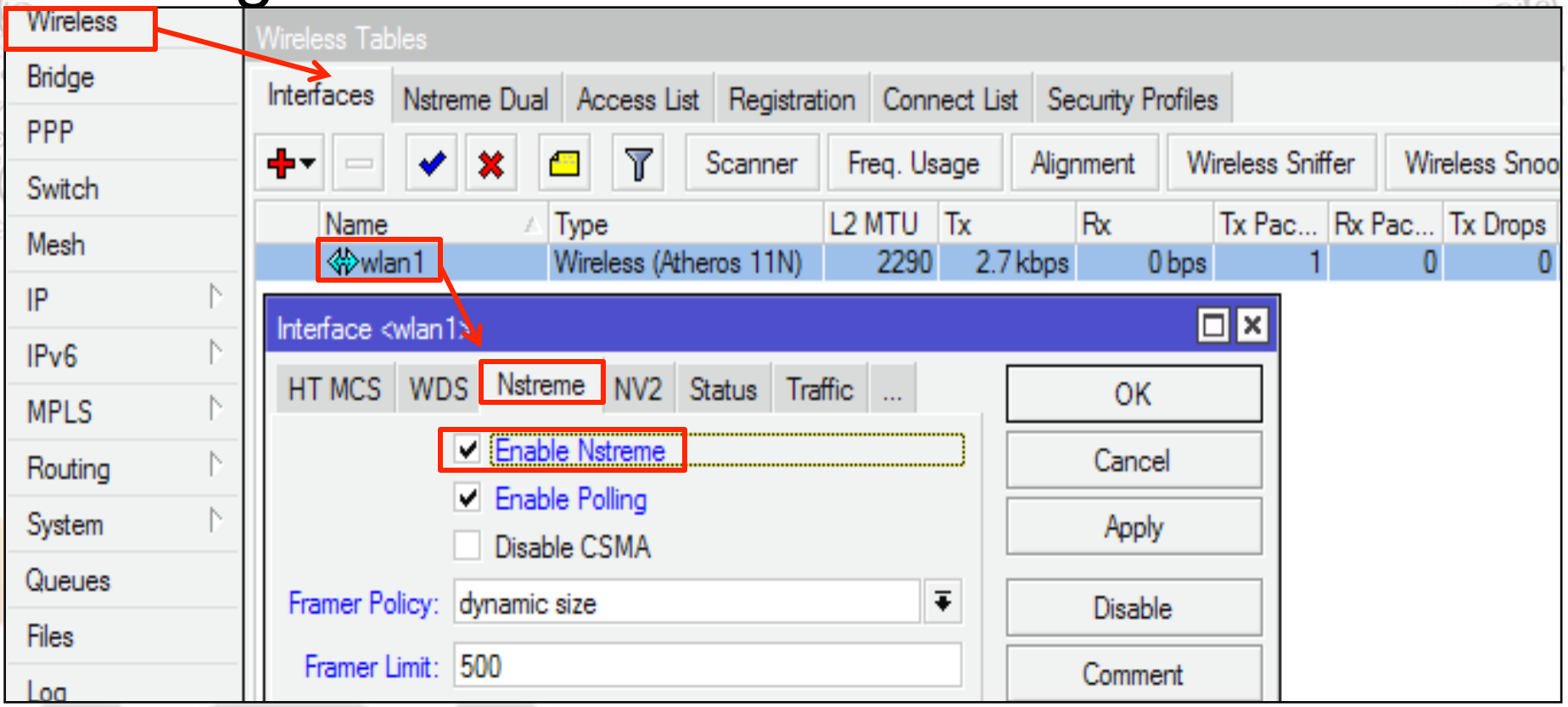
- Cobalah ping antar peserta ketika default fowarding check dan uncheck

Nstreme

- Nstreme adalah protocol wireless proprietary Mikrotik
- Meningkatkan perfomance link wireless jarak jauh.
- Untuk konek fitur Nstreme harus diaktifkan baik di sisi AP maupun station
- Konfigurasi Nstreme hanya di sisi AP, client hanya meng-enable-kan saja

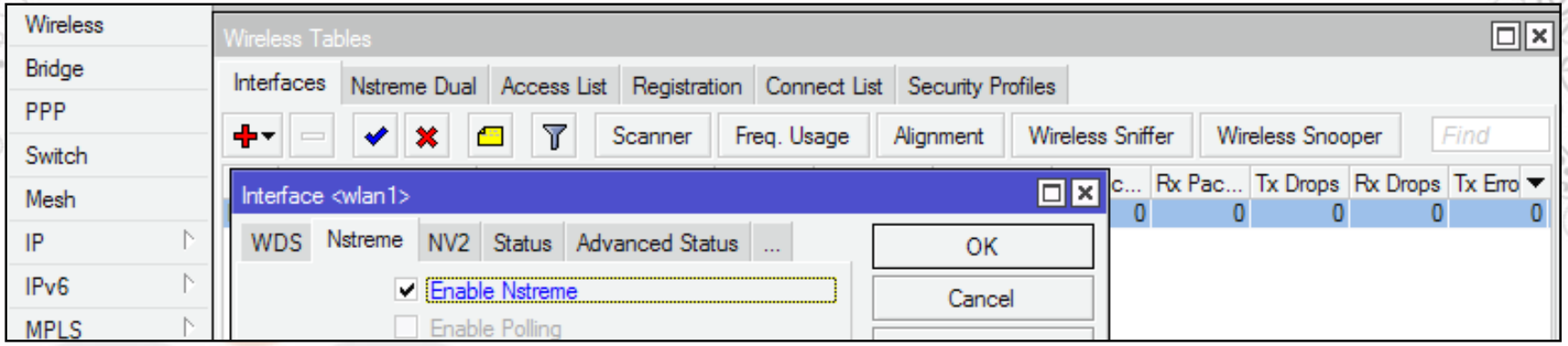
LAB - Wireless Nstreme

Setting di AP



LAB - Wireless Nstreme

Setting di Station

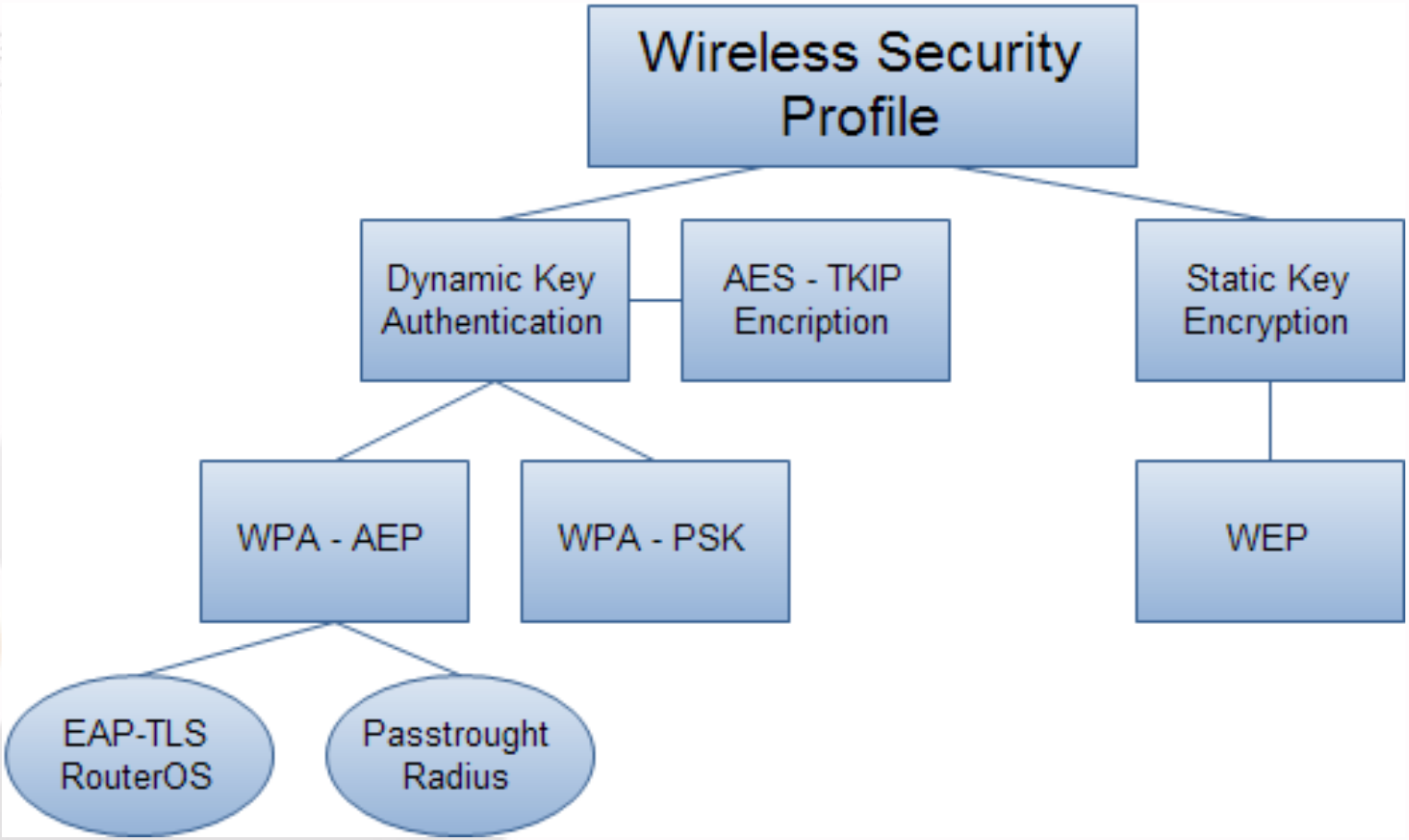


Cobalah konek dengan Laptop ke AP yang mengaktifkan feature nstream

Wireless Security

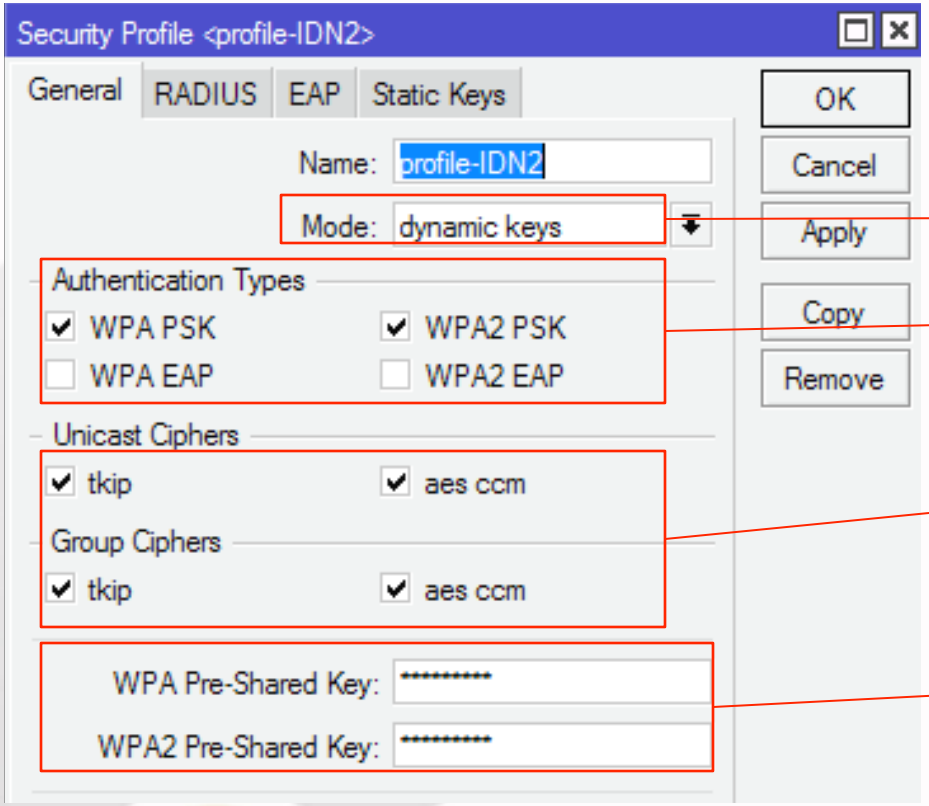
- Untuk pengamanan koneksi wireless, tidak hanya cukup dengan MAC-Filtering, karena data yang lewat ke jaringan bisa diambil dan dianalisa.
- Terdapat metode keamanan lain yang dapat digunakan yaitu:
  - Authentication (WPA-PSK, WPA-AEP)
  - Enkripsi (AES, TKIP, WEP)

Wireless Security



Wireless Encryption - WPA

- Pilihan wireless encryption terdapat pada menu Wireless>Security Profile.
- Security profile diberi nama tertentu untuk diimplementasikan dalam interface wireless.



Dynamic key = WPA
Static Key = WEP (lama)

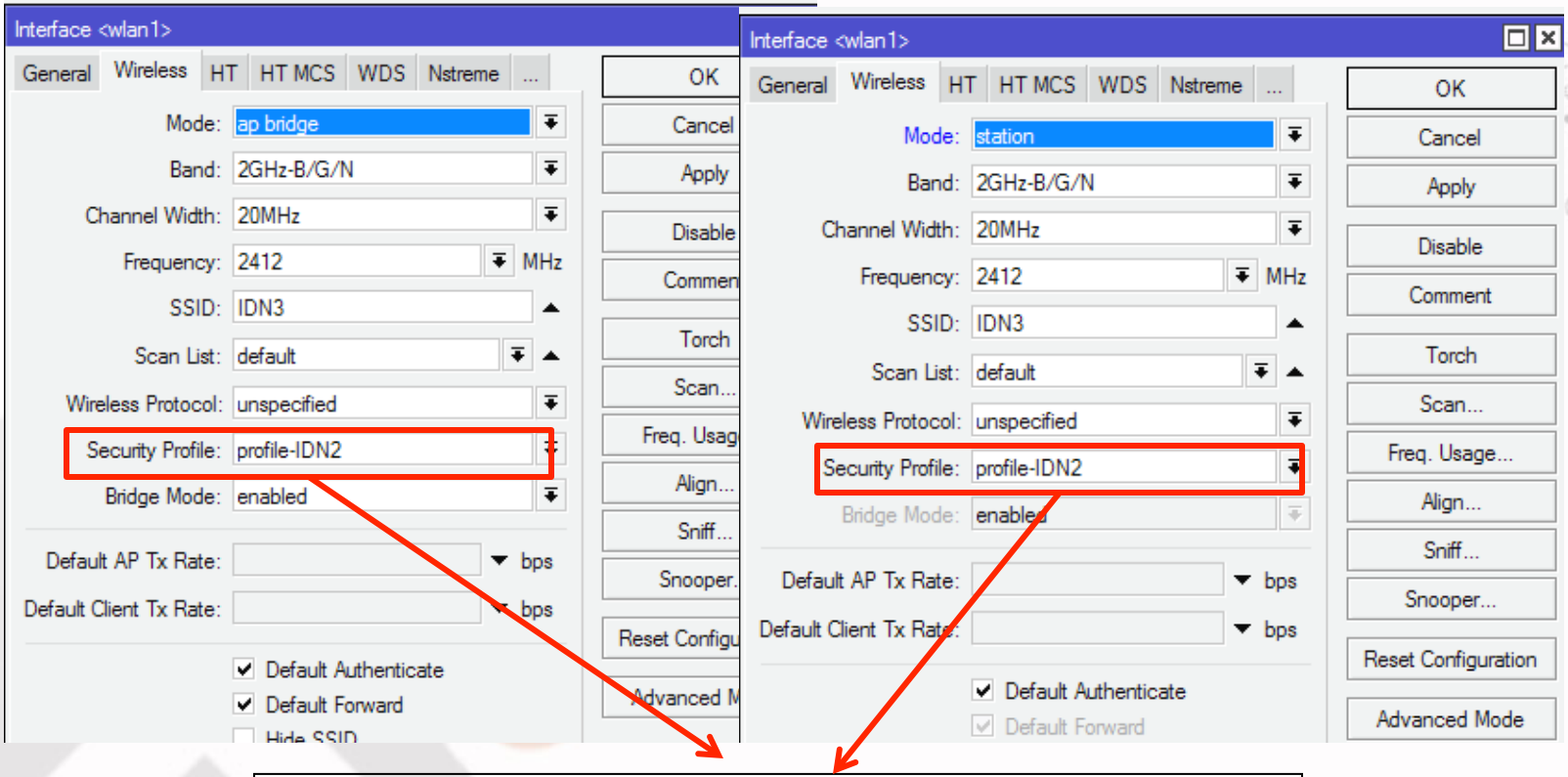
Jenis Authentifikasi

Model Enkripsi

Key Authentifikasi / password

Wireless Encryption

- Implementasi security profile



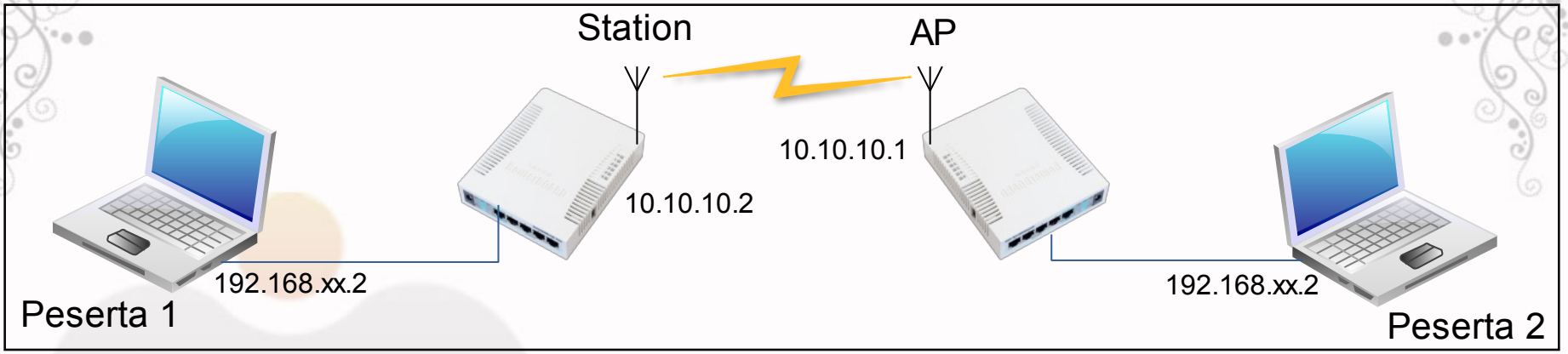
Pilih security profil yang telah kita buat sebelumnya baik di AP maupun Station

WEP Encryption

- WEP (Wired Equivalent Privacy) tipe wireless security yang pertama kali muncul dan masih sangat sederhana
- Tidak mempunyai authenticate method
- Not recommended as it is vulnerable to wireless hacking tools

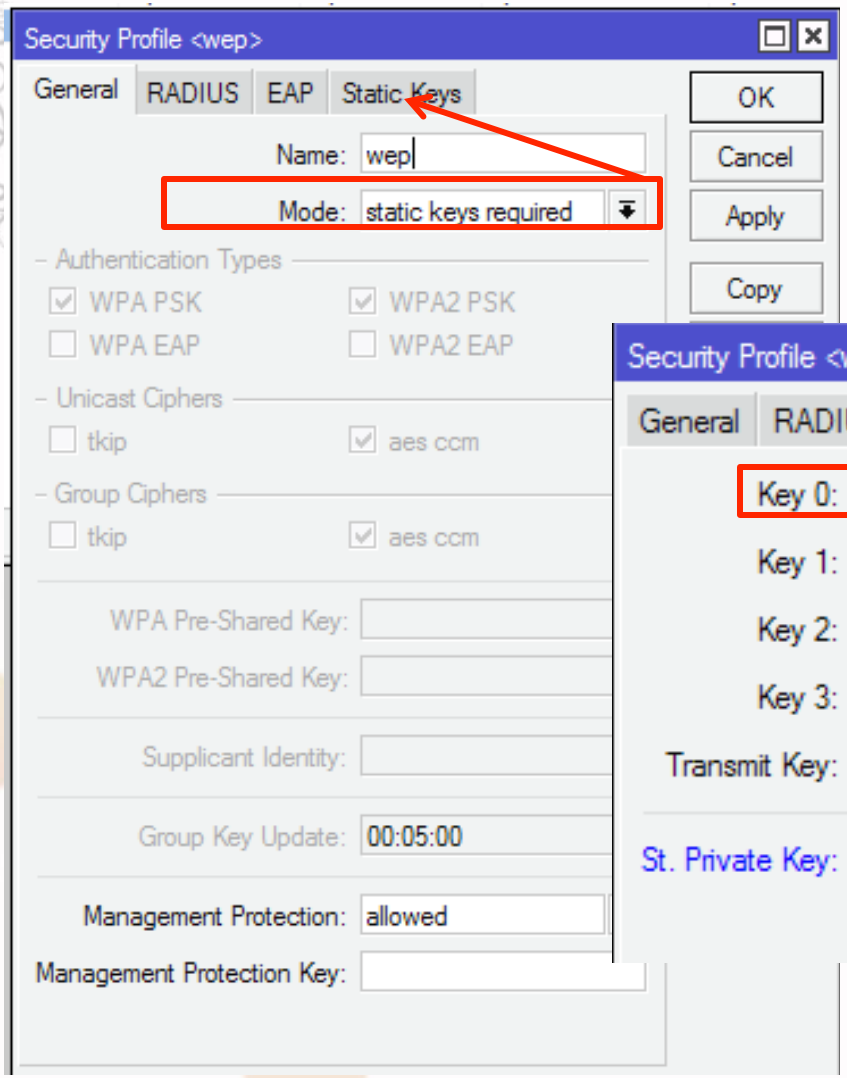
LAB-WEP Encryption

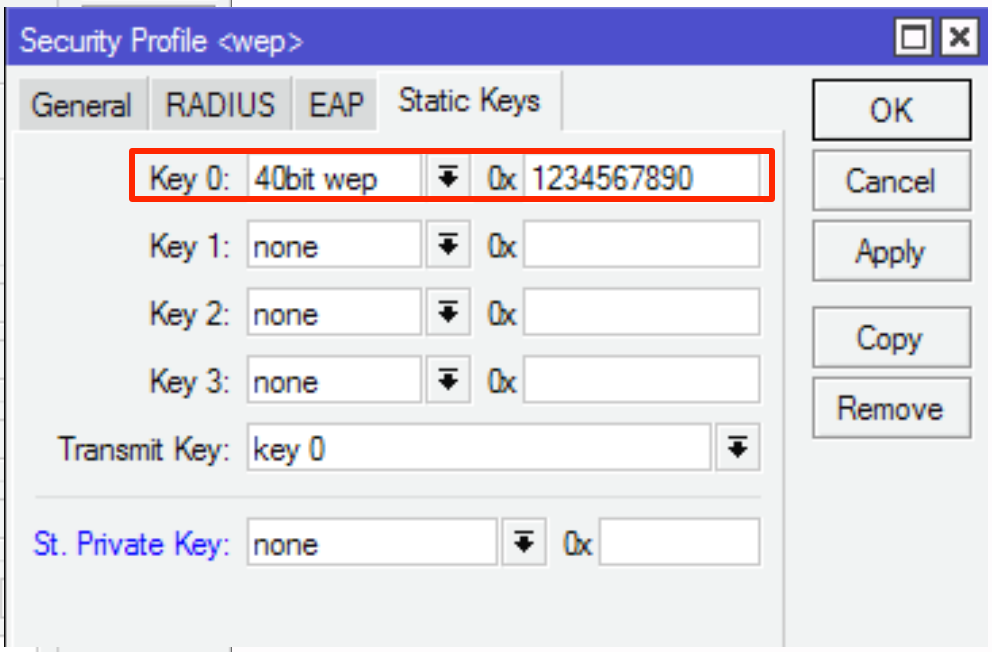
- Buat koneksi AP-Station dengan pasangan anda.



- Create WEP security profile pada kedua sisi wlan (AP & station), samakan static keynya.
- Apply security profile tersebut pada interface wireless wlan1

LAB-WEP Encryption

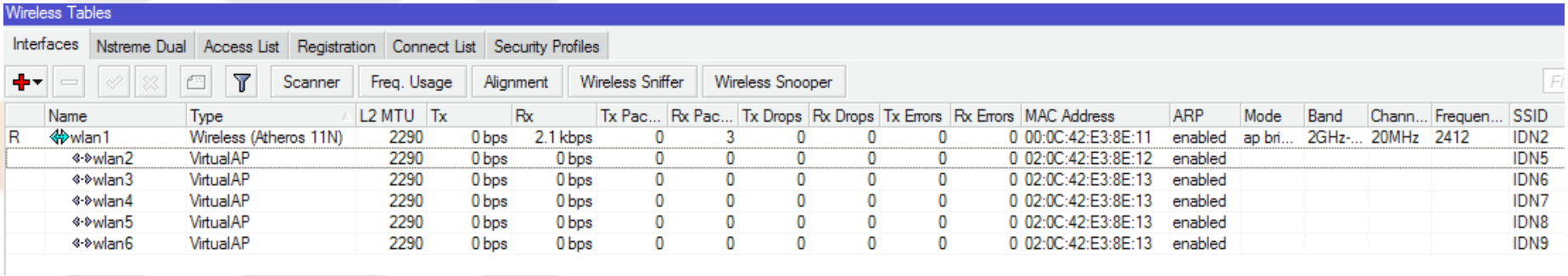




Wireless Security Profile:
-Mode: static keys required
-Key 0 : 40 bit
-0x : 1234567890

LAB - Virtual Access Point

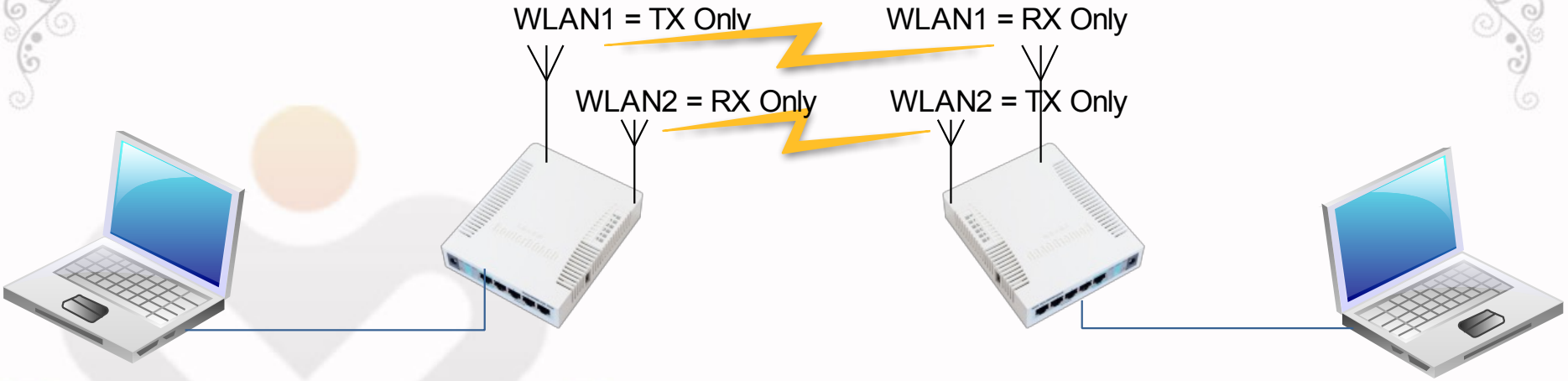
- Virtual AP akan menjadi child dari wlan (interface real).
- Satu interface dapat memiliki banyak virtual AP (maksimum 128)
- Virtual AP dapat diset **dengan SSID, security profile dan access list** yang berbeda, namun menggunakan **frekuensi** dan **band yang sama** dengan wlan induk.
- Virtual AP bersifat sama seperti AP:
  - Dapat dikoneksikan dengan station / client.
  - Dapat difungsikan sebagai DHCP server.
  - Dapat difungsikan sebagai Hotspot server.



	Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops	Rx Drops	Tx Errors	Rx Errors	MAC Address	ARP	Mode	Band	Chann...	Frequen...	SSID
R	wlan1	Wireless (Atheros 11N)	2290	0 bps	2.1 kbps	0	3	0	0	0	0	00:0C:42:E3:8E:11	enabled	ap bri...	2GHz-...	20MHz	2412	IDN2
	wlan2	VirtualAP	2290	0 bps	0 bps	0	0	0	0	0	0	02:0C:42:E3:8E:12	enabled					IDN5
	wlan3	VirtualAP	2290	0 bps	0 bps	0	0	0	0	0	0	02:0C:42:E3:8E:13	enabled					IDN6
	wlan4	VirtualAP	2290	0 bps	0 bps	0	0	0	0	0	0	02:0C:42:E3:8E:13	enabled					IDN7
	wlan5	VirtualAP	2290	0 bps	0 bps	0	0	0	0	0	0	02:0C:42:E3:8E:13	enabled					IDN8
	wlan6	VirtualAP	2290	0 bps	0 bps	0	0	0	0	0	0	02:0C:42:E3:8E:13	enabled					IDN9

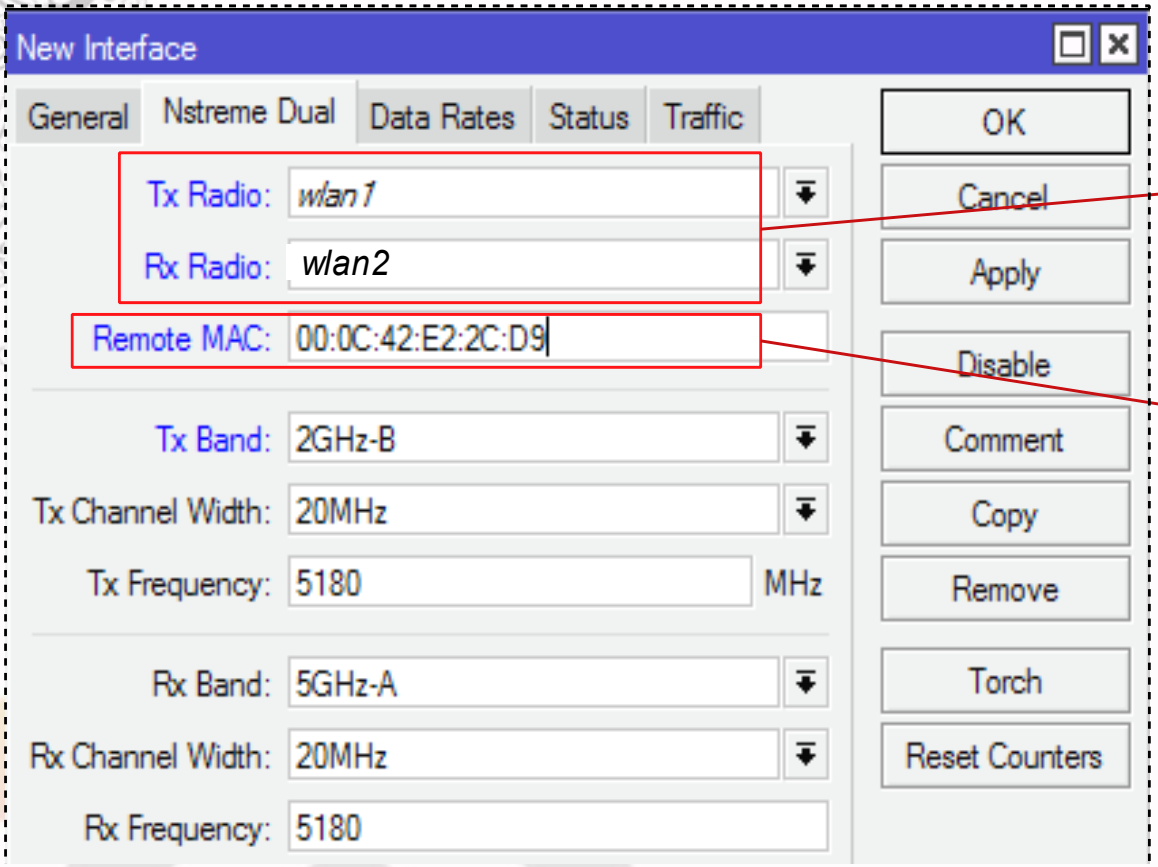
Nstreme Dual

Nstreme dual memanfaatkan keunggulan Nstreame (polling based) namun menggunakan 2 interface sekaligus yaitu 1 sebagai TX dan satu lagi sebagai RX.



Untuk menjalankan nstreme dual Mikrotik harus mempunyai 2 interface wireless.

Nstreme Dual



Pemilihan interface wlan sebagai RX atau TX

Mac-address interface nstream-dual disisi remote

- Untuk konfigurasi Mikrotik lawannya frekuensi untuk TX dan Rxnya dibalik

Bridge (Layer 2 Connection)

Bridge

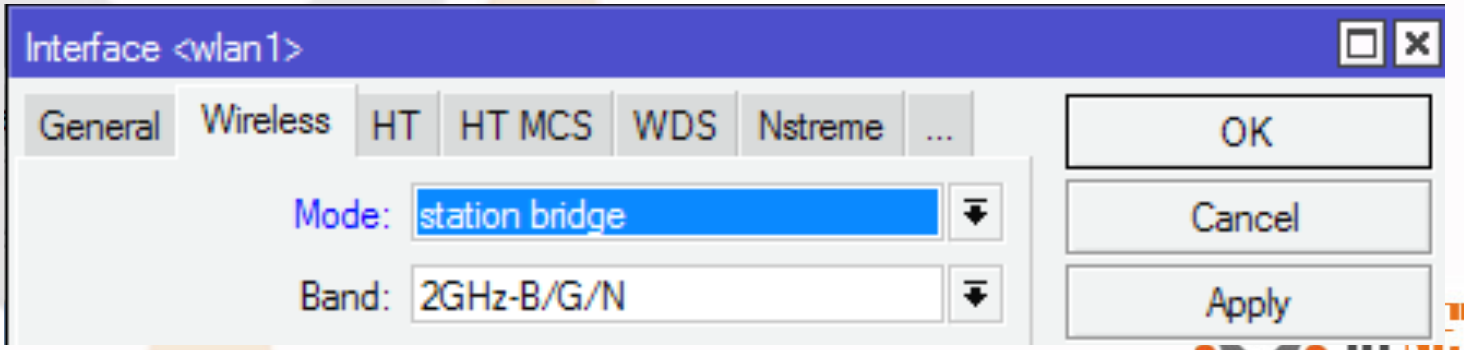
- Menggabungkan 2 atau lebih interface seolah-olah berada dalam 1 segmen network yang sama,
- Bridge juga dapat berjalan pada jaringan wireless
- Proses bridge berjalan pada layer data link (layer 2)
- Interface bridge adalah interface virtual, dimana kita dapat membuat sebanyak yang kita inginkan.
- Tahap pembuatan bridge adalah, membuat bridge baru dan menambahkan interface fisik kedalam port bridge.
- Jika kita membuat interface bride tanpa menambahkan interface fisik pada portnya, maka bridge tersebut dianggap sebagai interface loopback.

Bridge

- Kelemahan dari Bridge adalah:
  - Sulit untuk mengatur trafik broadcast (misalnya akibat virus, dll)
  - Permasalahan pada satu port/segmen akan membuat masalah di port/segmen pada bridge yang sama
  - Peningkatan beban trafik akibat terjadinya akumulasi traffic broadcast

Wireless Bridging

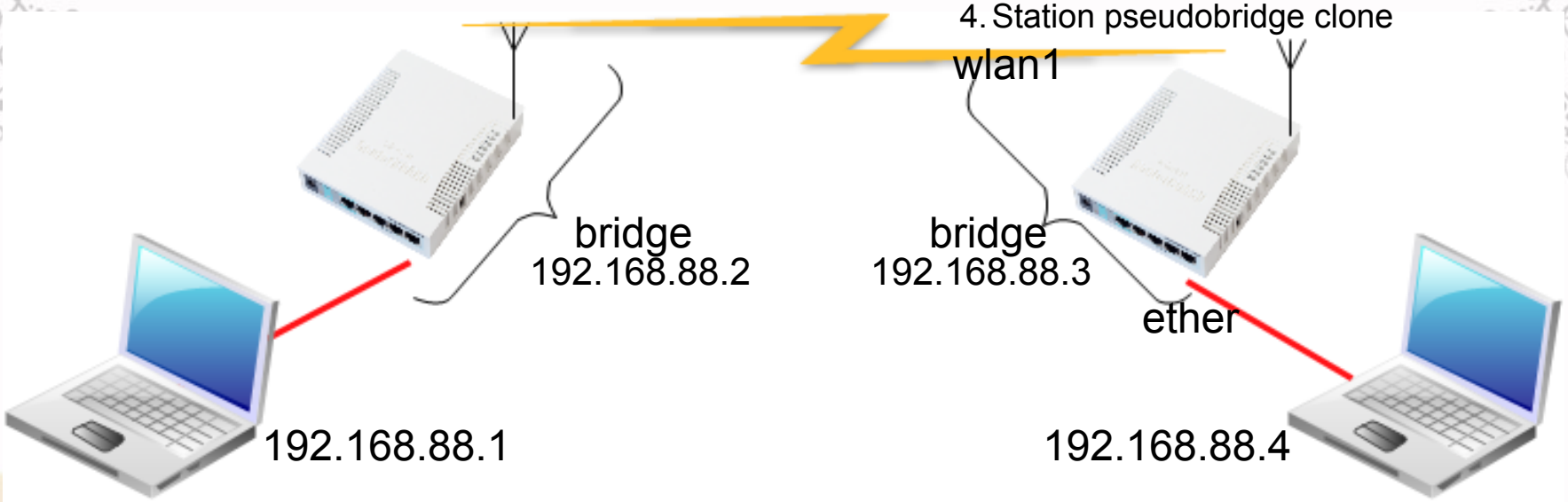
- Semua mode wireless bisa dibridging, kecuali mode station.
- Mode station tidak dapat di bridging, sehingga diciptakan mode station dengan type lain.
- Station bridge adalah fitur MikroTik sejak v5 yang memungkinkan station untuk dibridge.
- Station bridge hanya akan berjalan pada koneksi antar MikroTik (versi 5 keatas).



Lab - Bridging

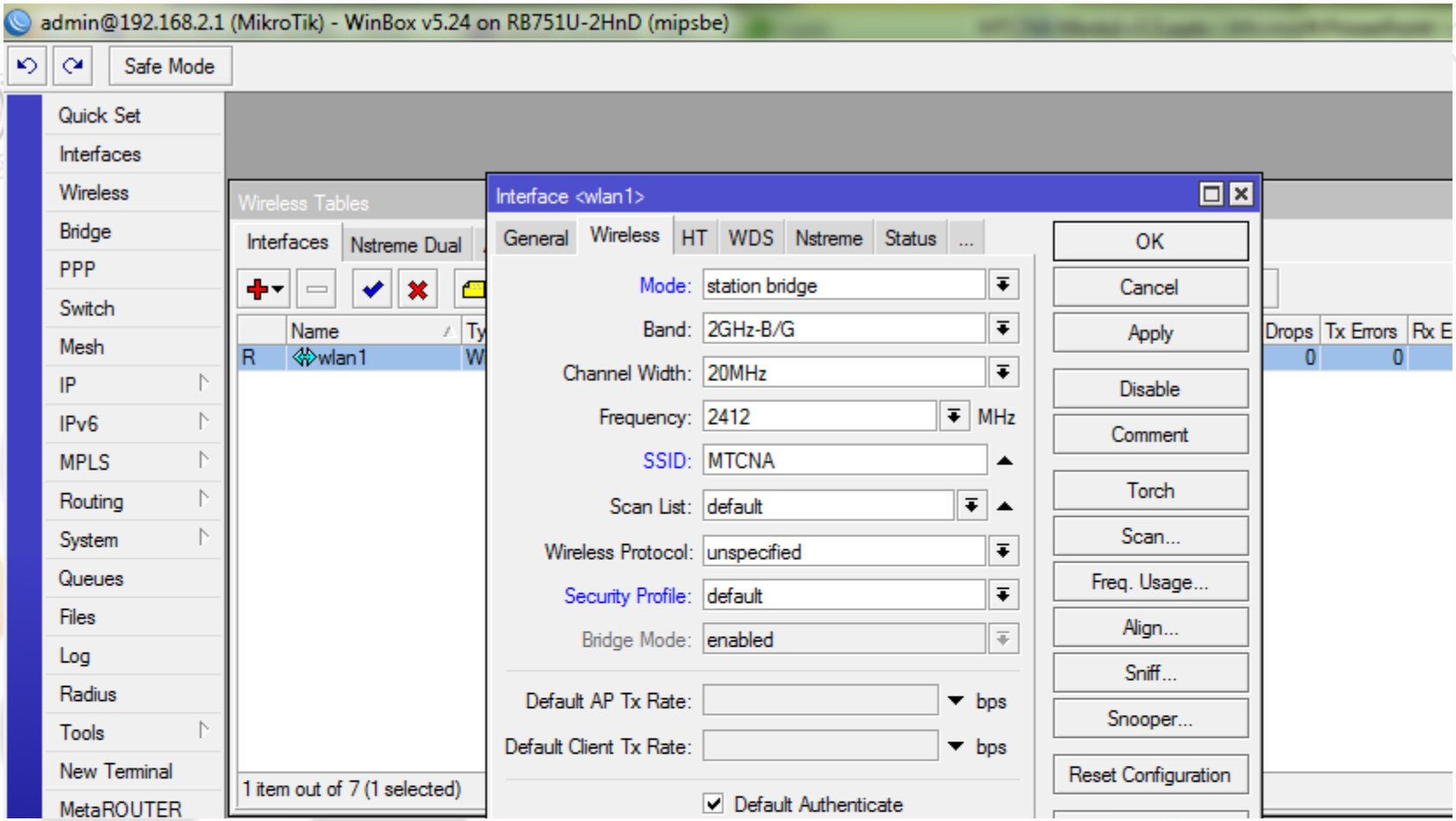
Wireless mode:
AP-bridge

Wireless mode:
1. Station bridge
2. Station
3. Station pseudobridge
4. Station pseudobridge clone



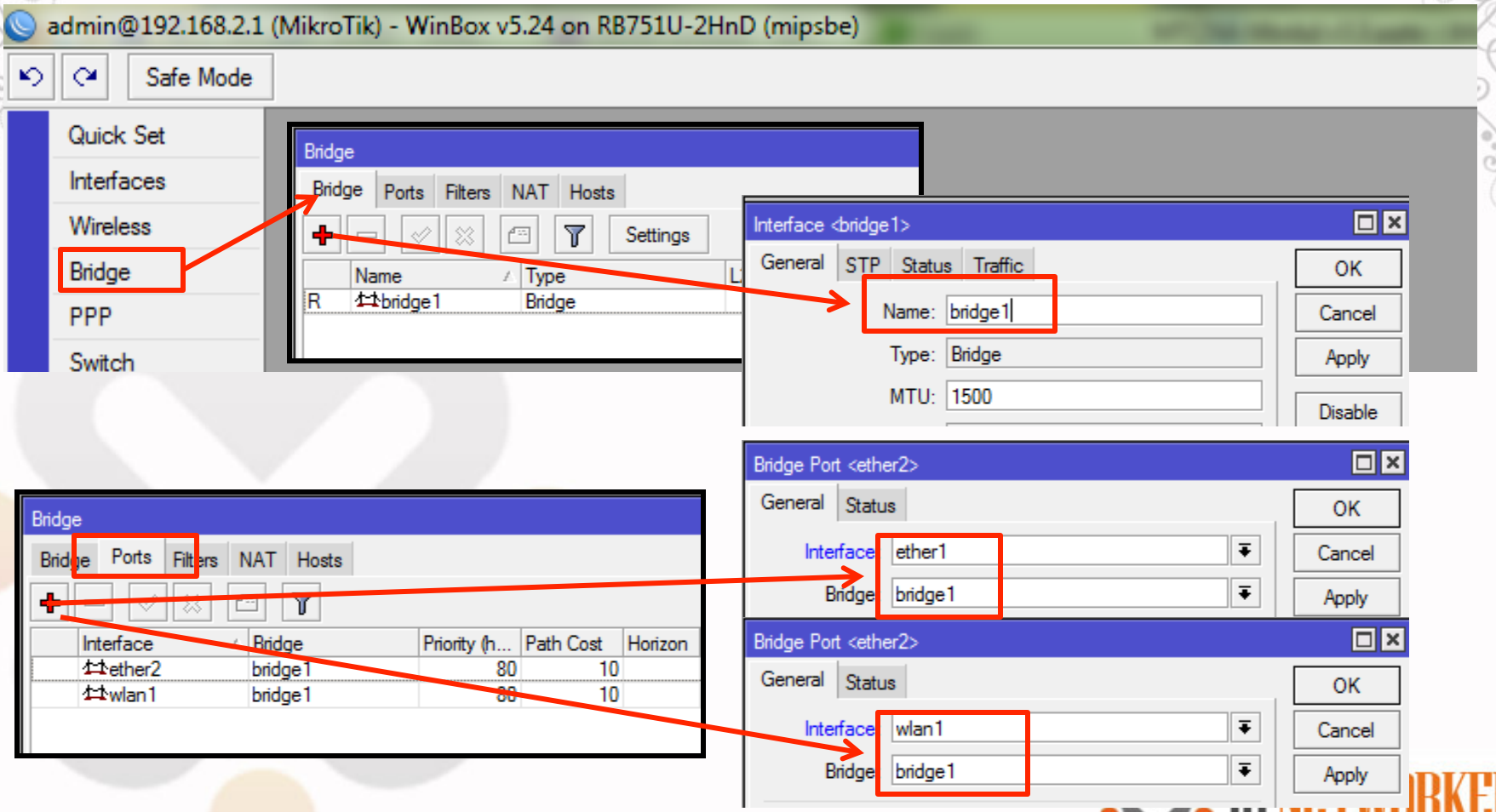
LAB-Simple Wireless Bridge

- Set wireless mode ke station bridge atau pseudobridge



LAB - Simple Wireless Bridge

- Pada menu Bridge, buatlah satu interface bride dan tambahkan interface ether1 dan wlan1 pada portsnya.

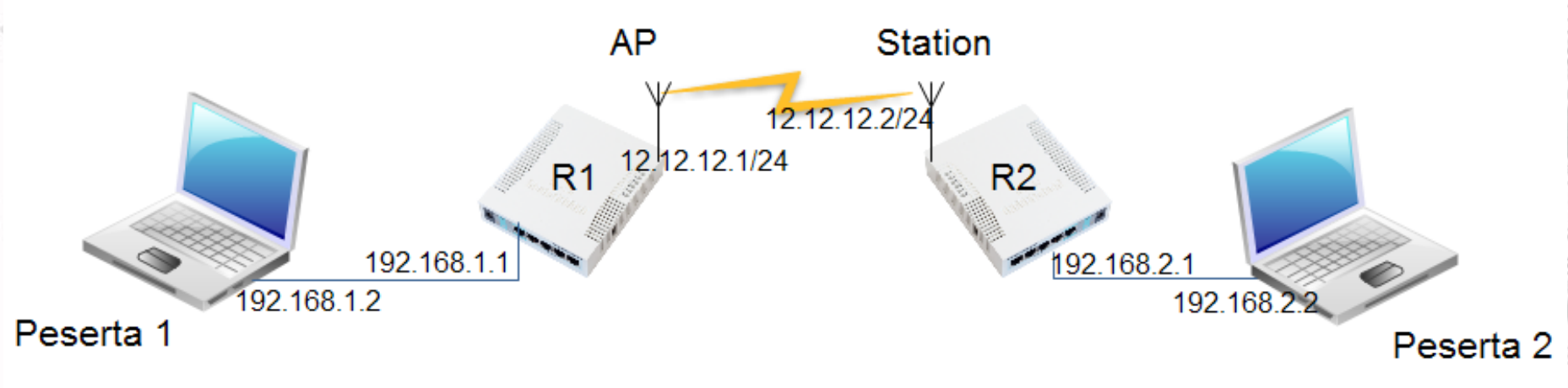


LAB - Simple Wireless Bridge

- Sambil terus di ping antar laptop, ubahlah mode wireless station menjadi tipe:
  1. Station
  2. Station bridge
  3. Station pseudobridge
  4. Station pseudobridge clone
- Amati ping antar laptop
- Manakah diantara mode tersebut yang tidak bisa di bridging

Routing

Static Routing

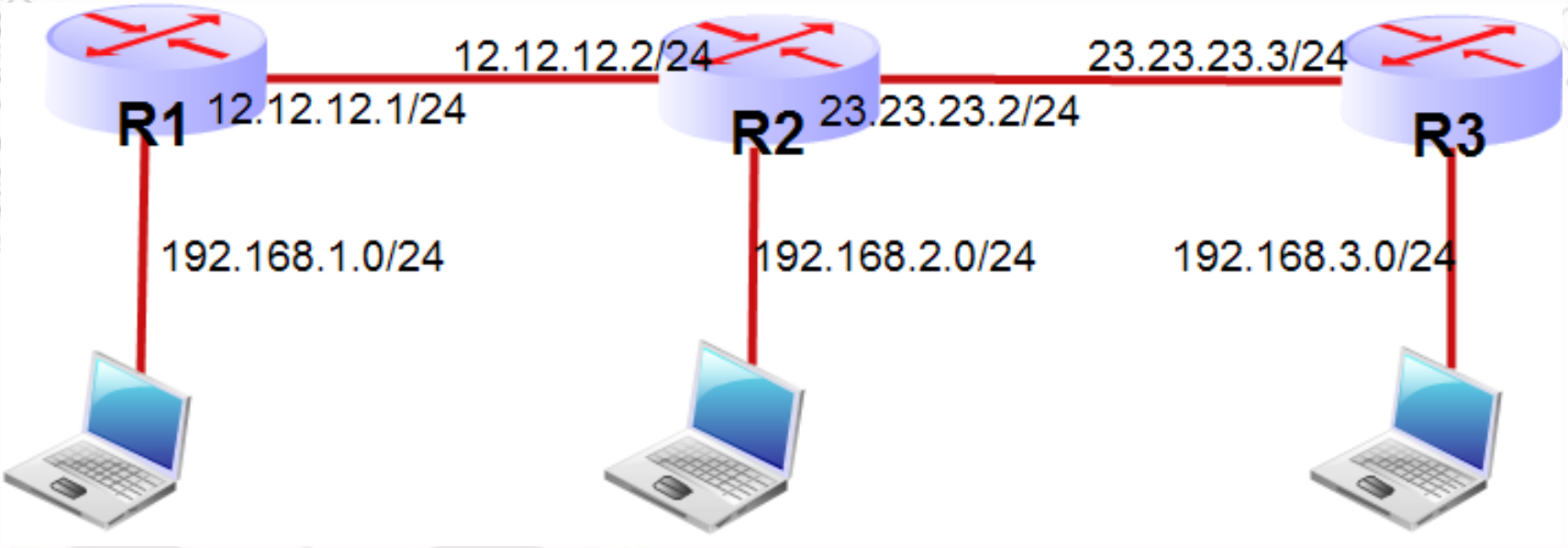


- Buat konfigurasi seperti diatas, IP addressnya disesuaikan
- Laptop di set default gatewaynya
- Laptop1, default gateway: 192.168.1.1, Laptop 2, 192.168.2.1
- Buat static routing di R1 dan R1 kearah network yg tidak terhubung langsung.
- Konfigurasi R1:

  IP > Route, add dst-address=192.168.2.0/24, gateway = 12.12.12.2
- Konfigurasi R2:

  IP> Route, add dst-address=192.168.1.0/24, gateway=12.12.12.1
- Ping dari laptop ke laptop

Static Routing



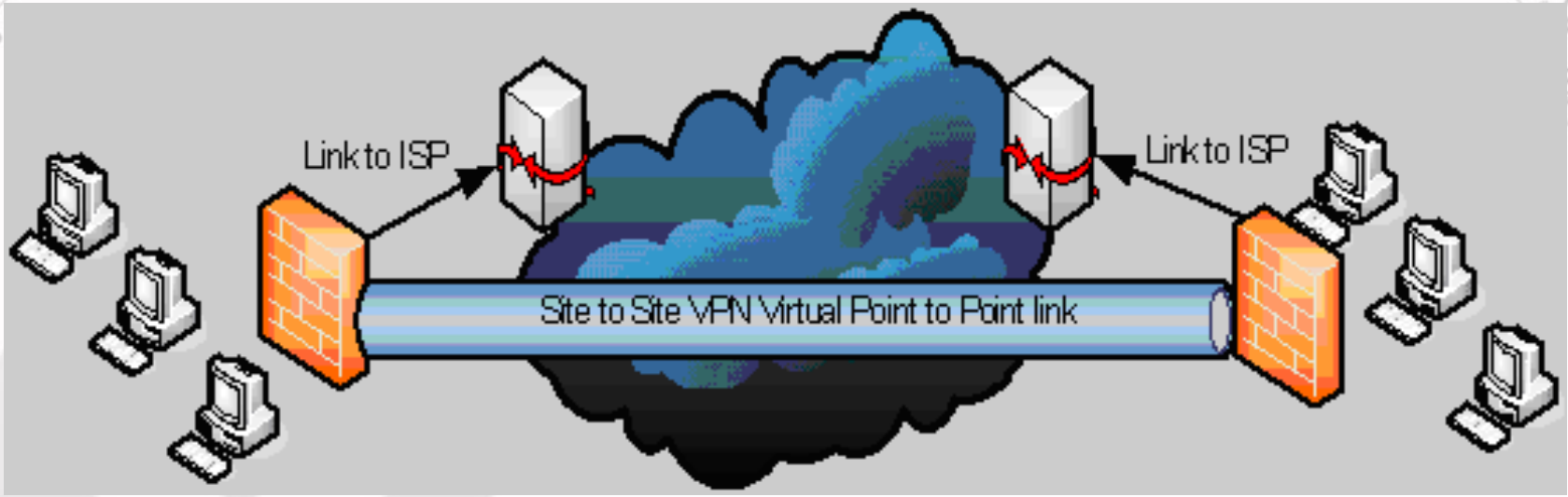
- Buatkan routing ke semua network yang tidak direct connected dengan router kita

Tunnel

Tunnel

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

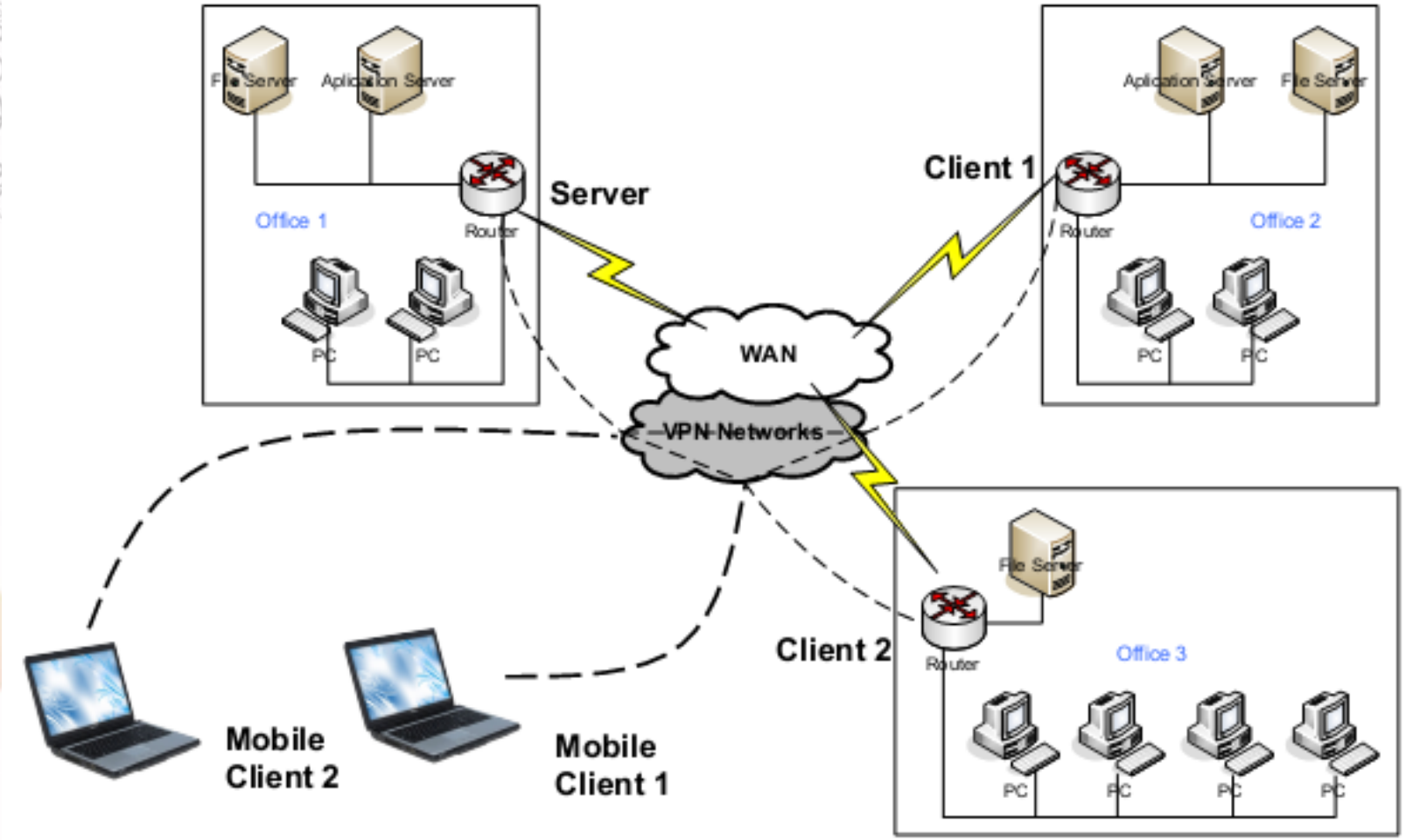
Tunnel



VPN

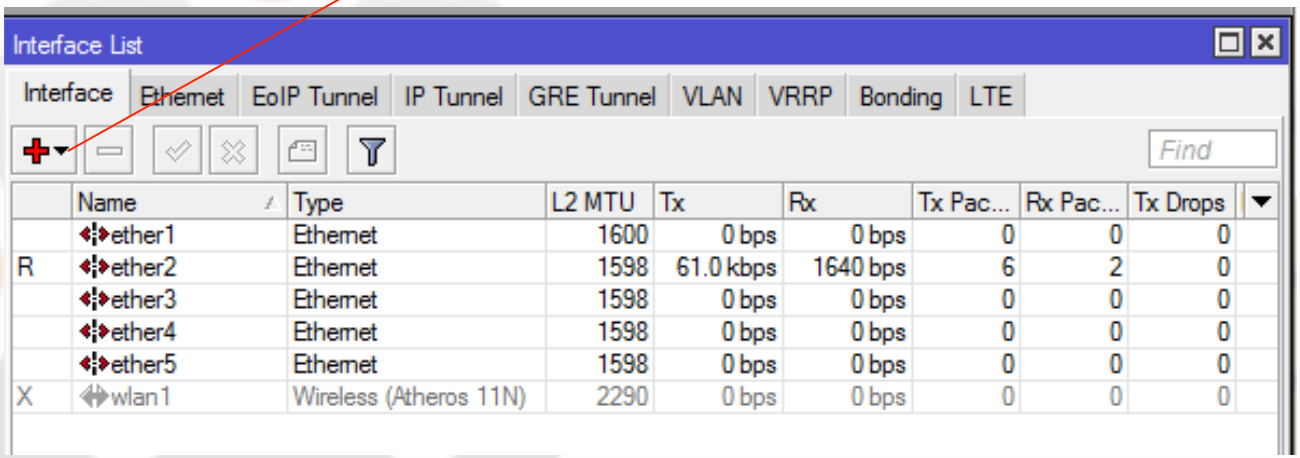
- VPN dibentuk dari beberapa tunnel yang digabung
- VPN adalah sebuah cara aman untuk mengakses local area network dengan menggunakan internet atau jaringan publik.
- Tunnel atau terowongan merupakan kunci utama pada VPN, koneksi pribadi dalam VPN dapat terjadi dimana saja selama terdapat tunnel.

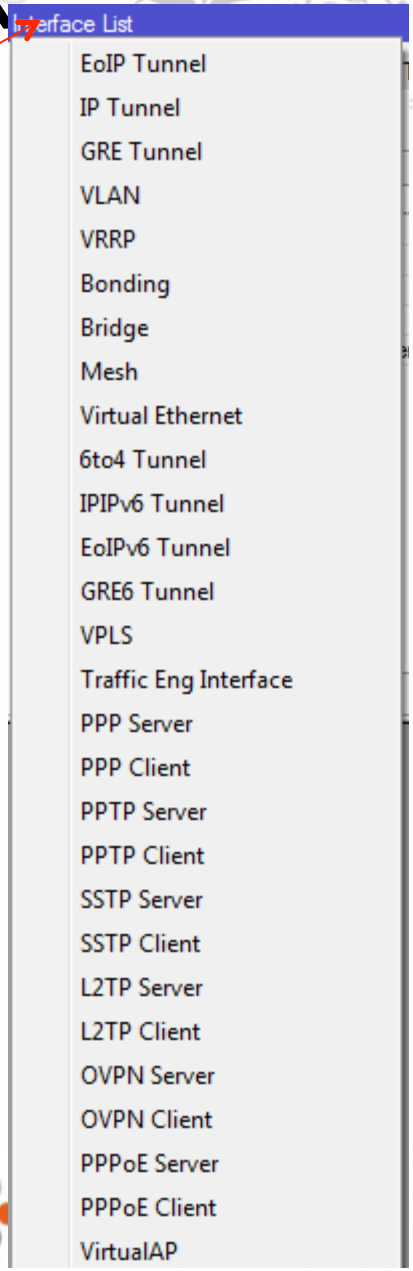
VPN



Tunnel Pada Mikrotik

- There are so many tunnel type in Mikrotik : PPTP, L2TP, PPPoE, EoIP, SSTP, OpenVPN, dll
- We can see that in virtual interface that we can add them

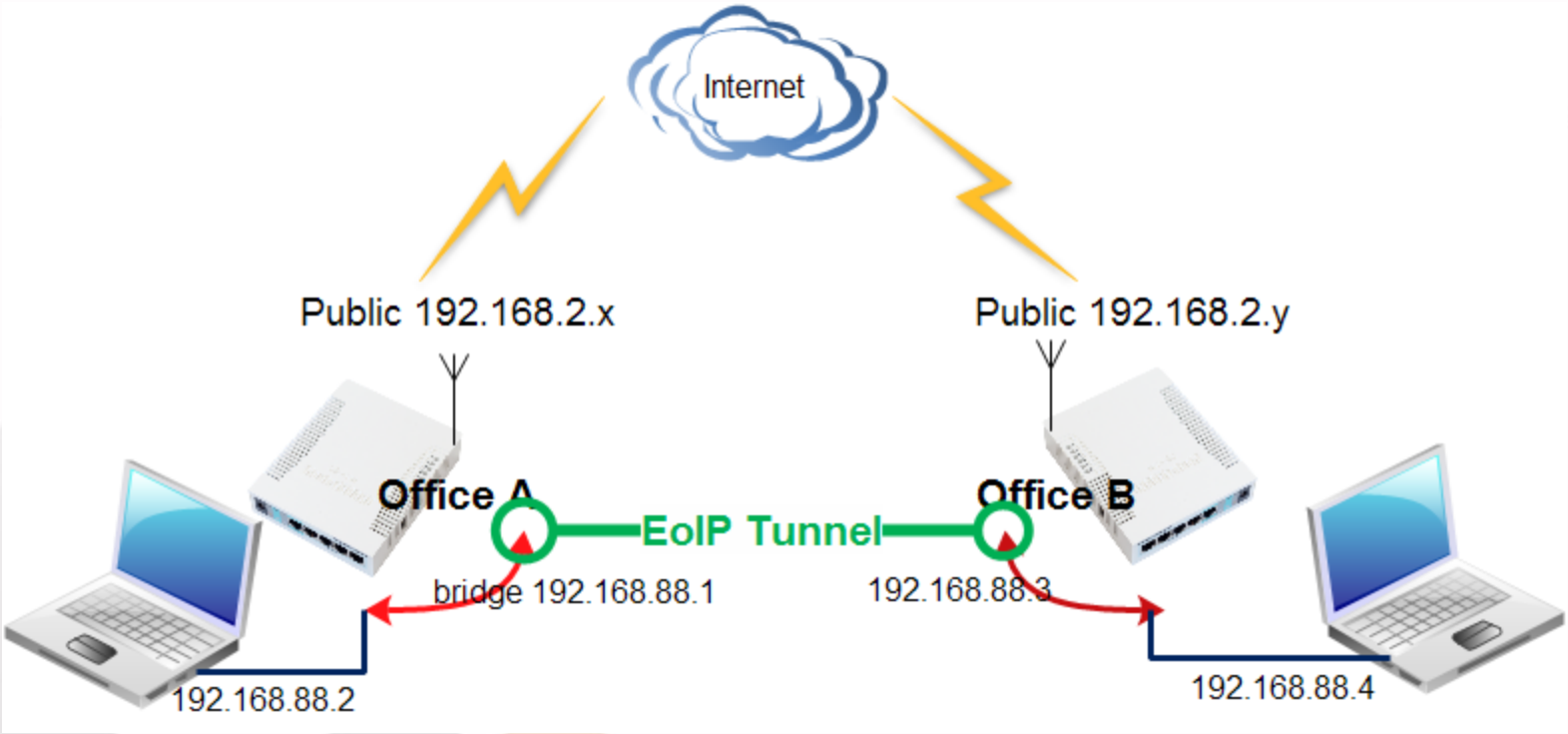




EOIP

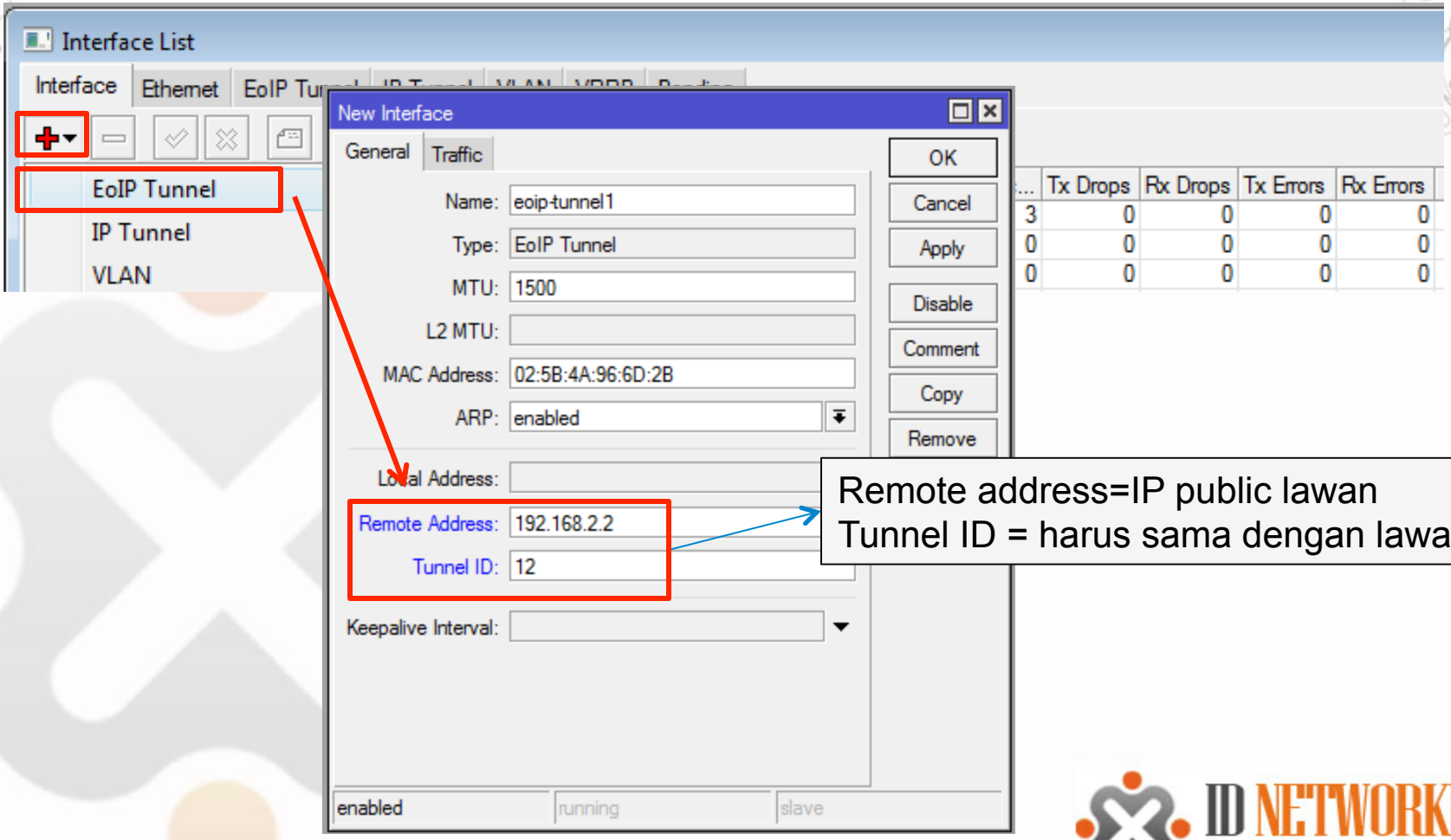
- Tunnel yang paling sederhana di MikroTik adalah EoIP (Ethetnet over IP)
- EOIP merupakan protocol proprietary untuk membangun bridge dan tunnel antar router Mikrotik, dimana interface EOIP akan dianggap sebagai ethernet.
- EoIP menggunakan encapsulation Generic Routing Encapsulation (IP Protocol No 47).
- EoIP tidak menggunakan ekripsi, jadi tidak disarankan digunakan untuk transmisi data yang membutuhkan tingkat keamanan yang tinggi.
- Identifikasi tunnel menggunakan Tunnel ID
- MAC Address diantara interface EOIP harus berbeda

LAB –EOIP -Bridging



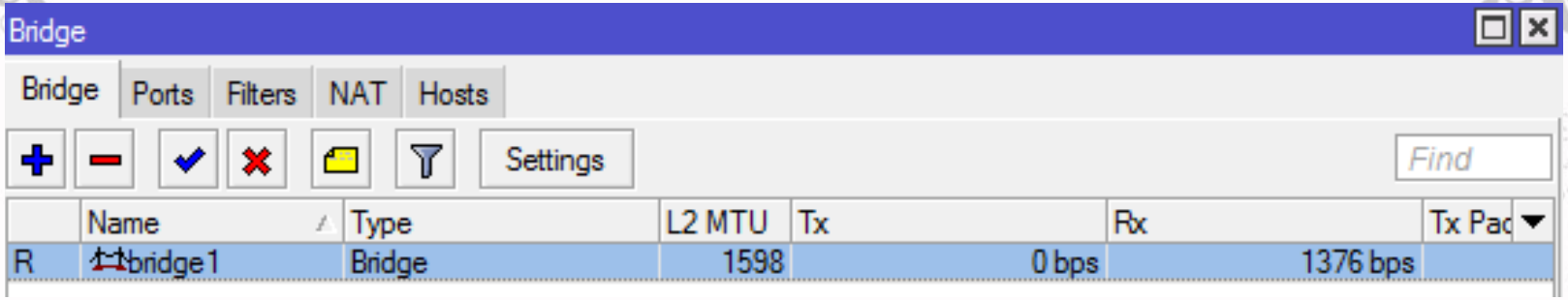
EOIP Tunnel

- New Interface EOIP Tunnel

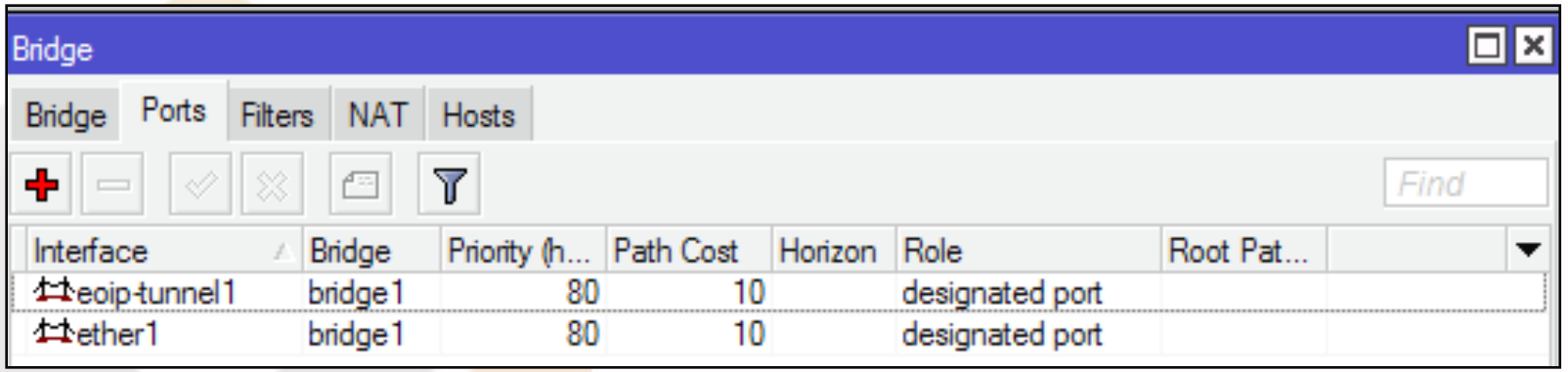


EoIP Tunnel

- Bridge add name=bridge1

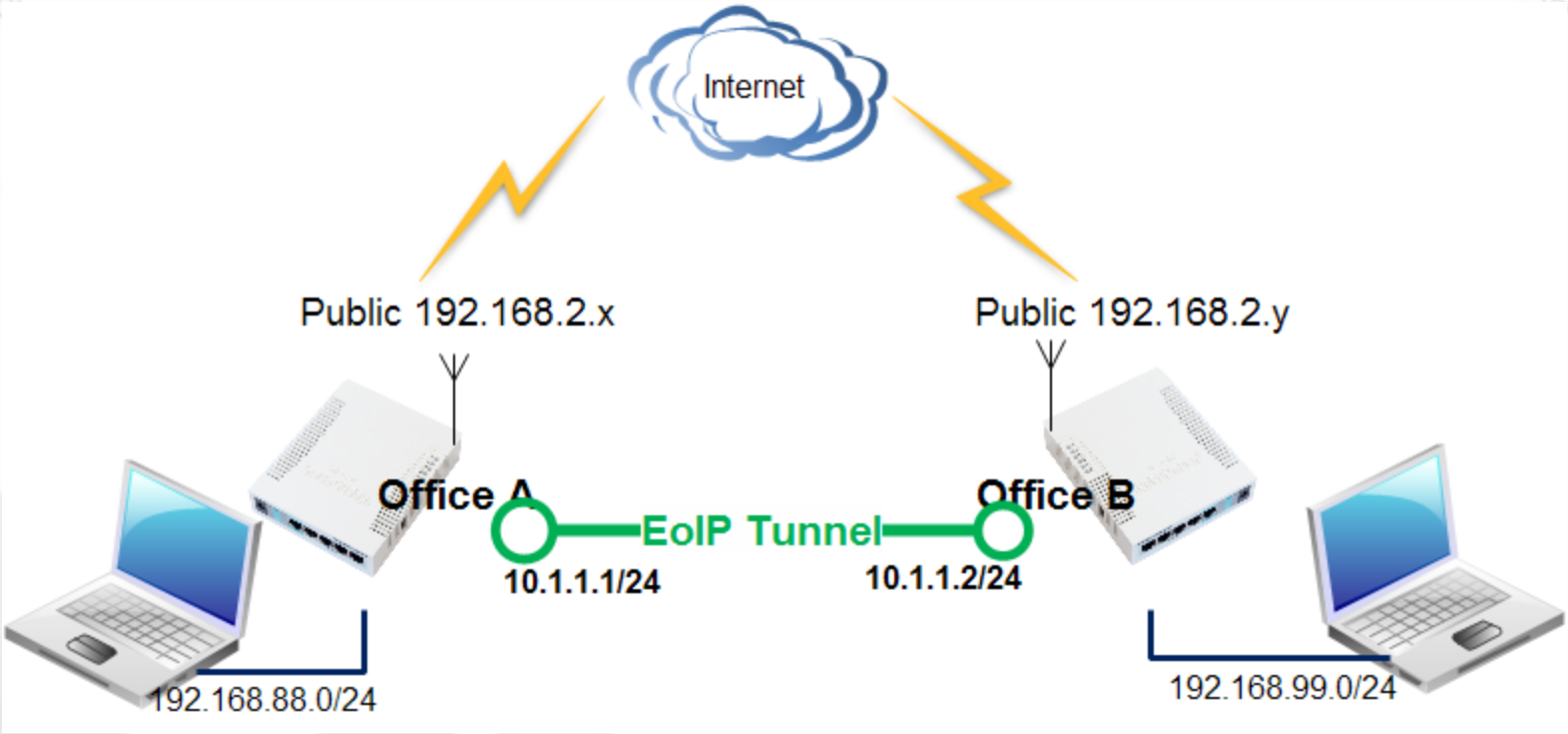


- Masukkan dalam interface bride interface EoIP dan ether1



- Tambahkan IP address pada interface bridge

LAB –EOIP- Routing



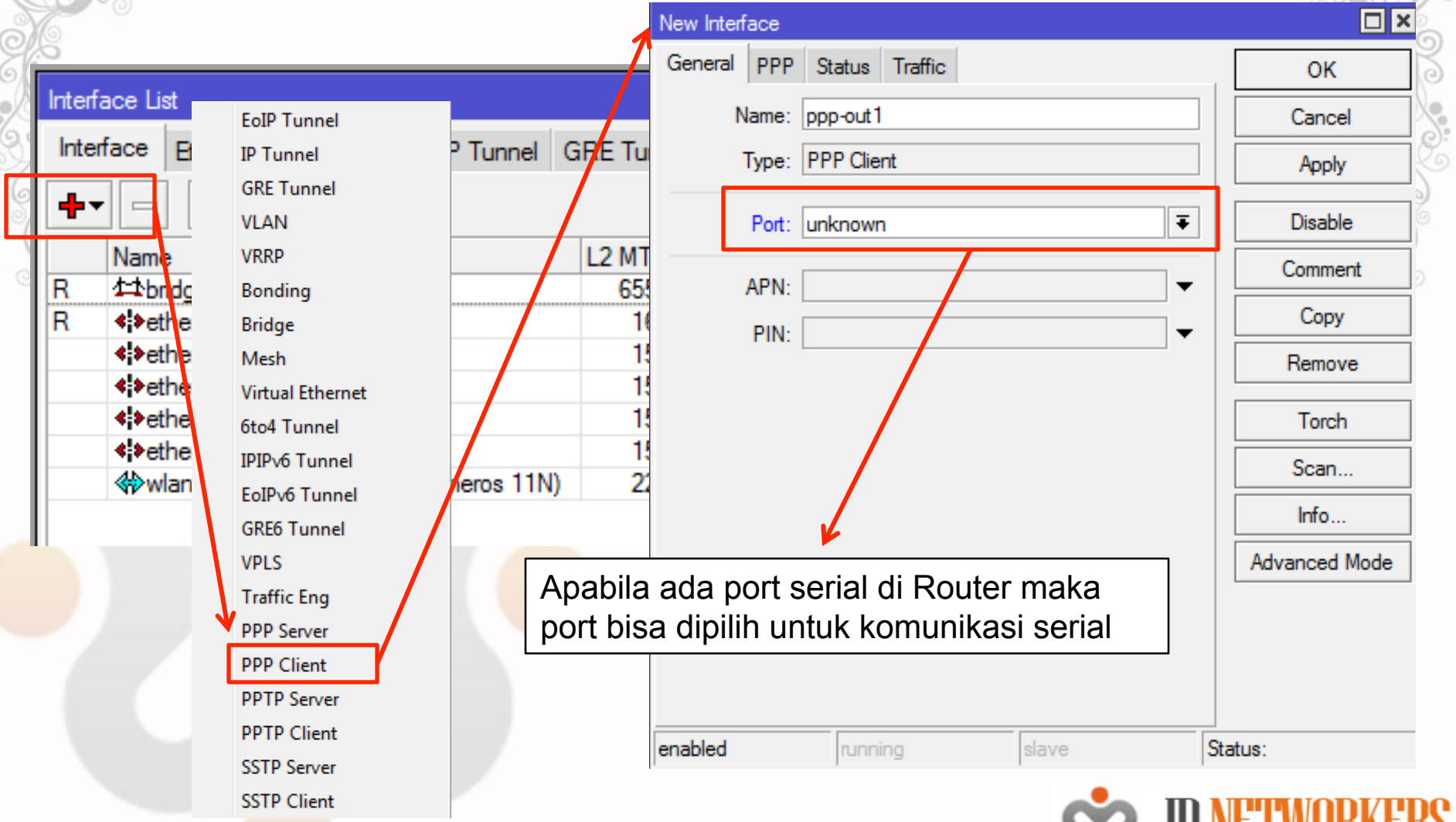
Office A:
IP route add dst-address=192.168.99.0/24 gateway 10.1.1.2

Office B:
IP route add dst-address=192.168.88.0/24 gateway 10.1.1.1

PPP

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

Setting PPP Client

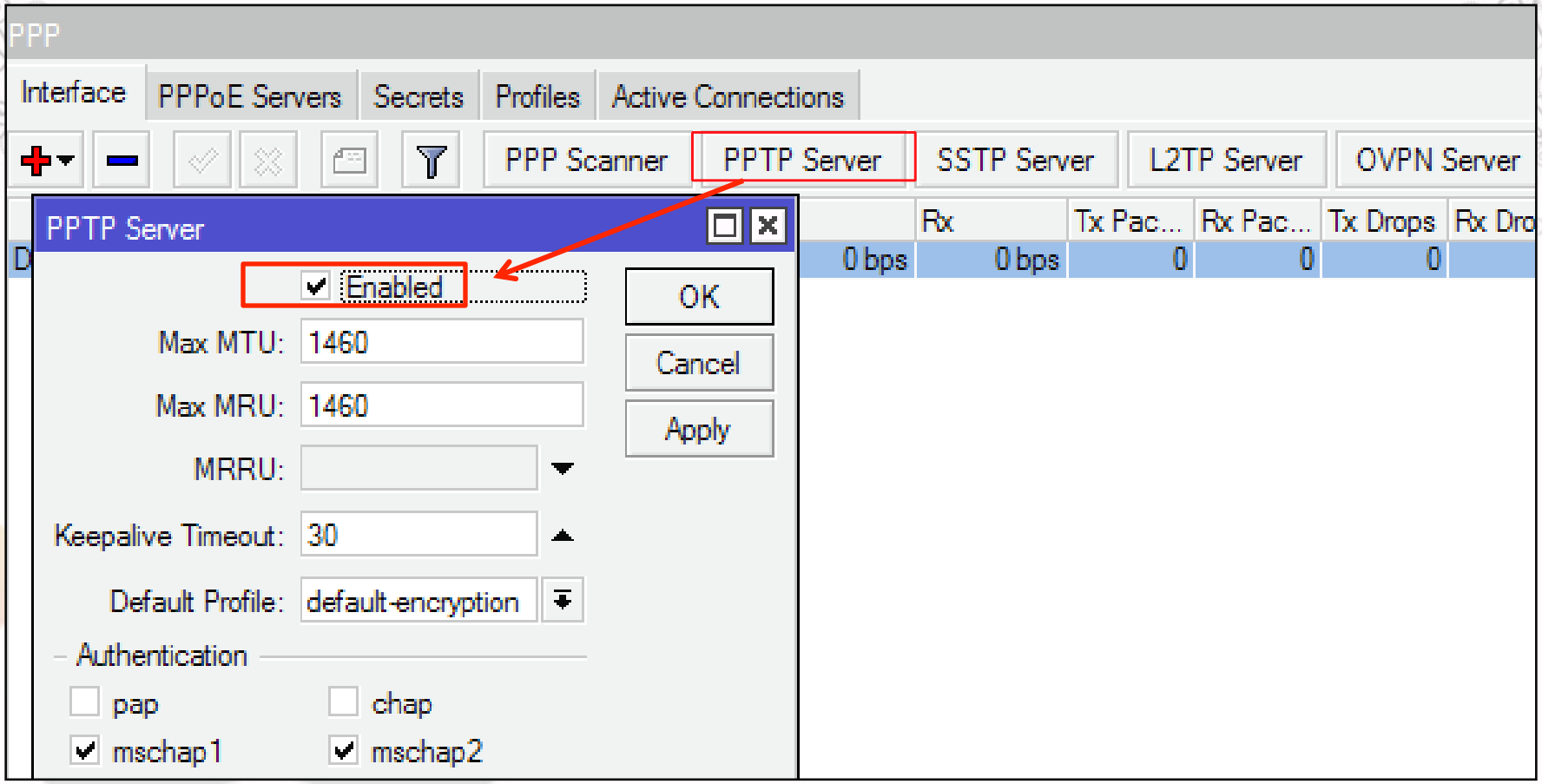


PPTP Tunneling

- PPTP melakukan membentuk tunnel PPP antar IP mengunakan protocol TCP dan GRE (Generic Routing Encapsulation).
- PPTP secure, karena menggunakan enkripsi MPPE (Microsoft Point-to-Point Encryption) panjang 40 dan 128 bit encrypts
- PPTP menggunakan port TCP 1723
- PPTP banyak digunakan karena hampir semua OS dapat menjalankan PPTP client.
- PPTP adalah tunnel tipe client server, dimana PPTP server lebih banyak melalukan konfgurasi untuk setiap client yang ingin konek

Mengaktifkan PPTP Server

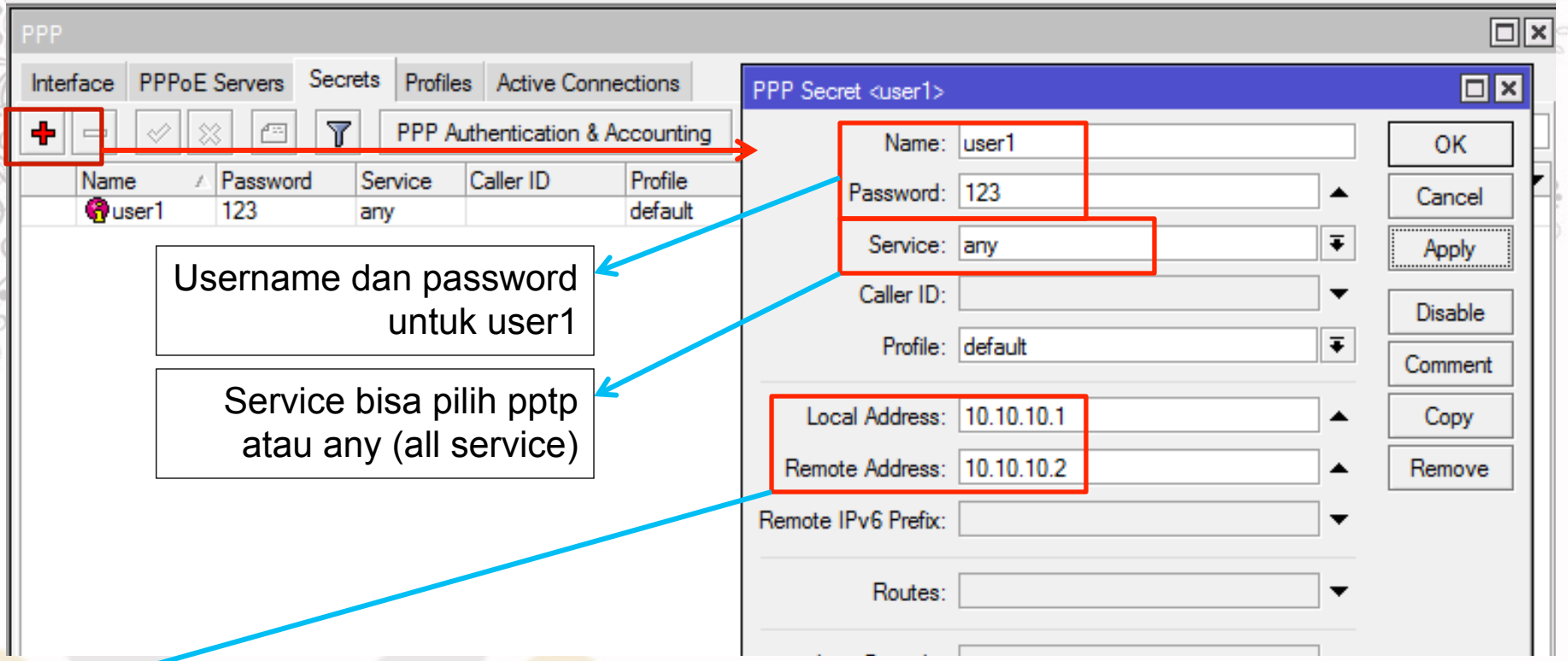
- Aktifkan PPTP server pada menu PPP>Interface>PPTP Server



PPP Secret

- Semua koneksi yang menggunkan protocol PPP selalu melibatkan authentikasi username dan password.
- Secara local, username dan password ini disimpan dan diatur dalam bagian **PPP secret**.
- Username dan password ini juga dapat disimpan dalam RADIUS server terpisah.
- PPP Secret (database local PPP) menyimpan username dan password yang akan digunakan oleh semua pptp clientnya.
- Selain dipakai untuk PPTP client, PPP secret juga dipakai untuk protocol ppp lainya seperti; **async, l2tp, openvpn, pppoe, pptp dan sstp.**

PPP Secret



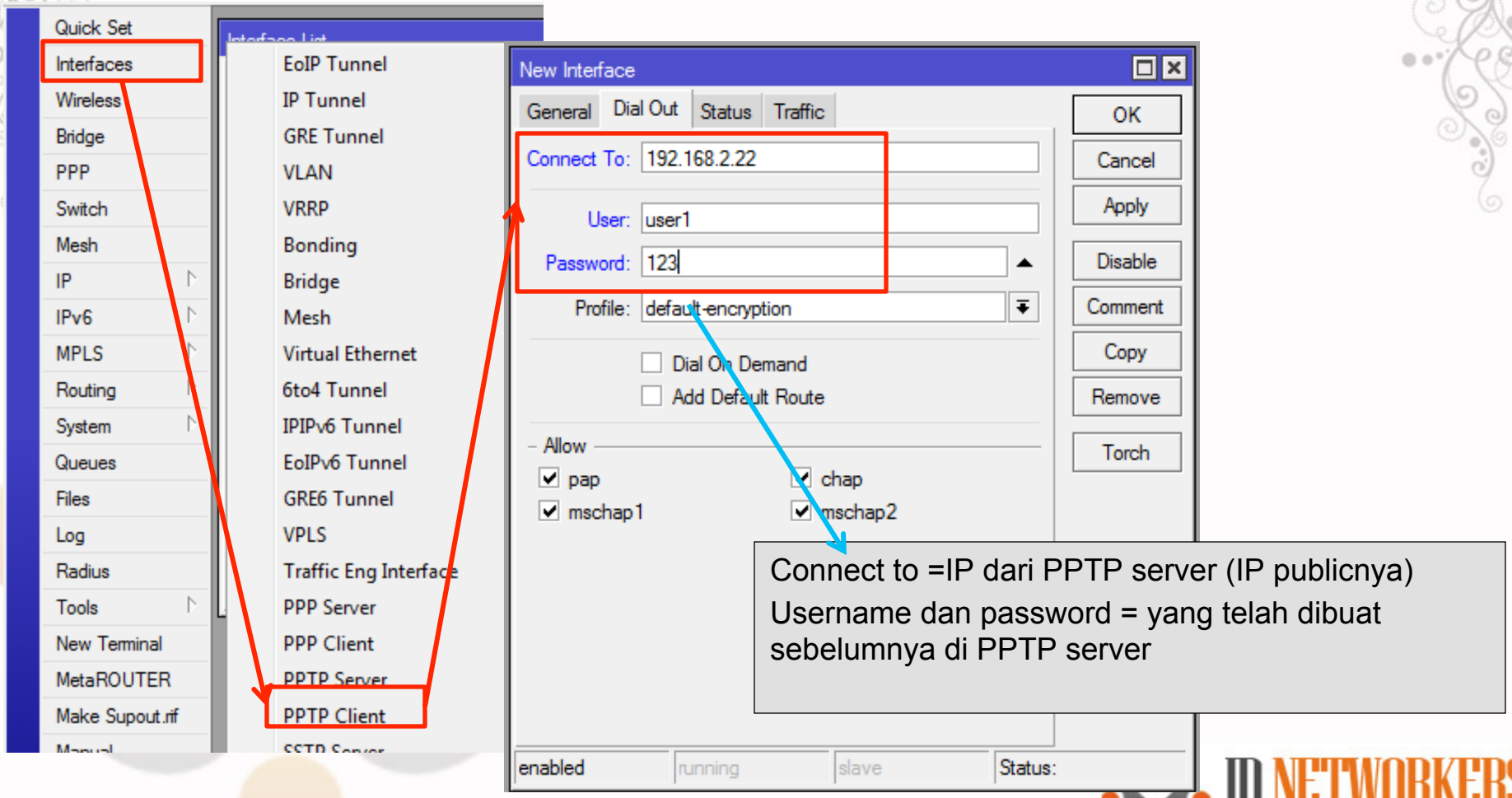
IP yang nantinya akan dibuat untuk komunikasi tunnel point to point antara server dan client user1

Local address=IP yang akan dipakai server

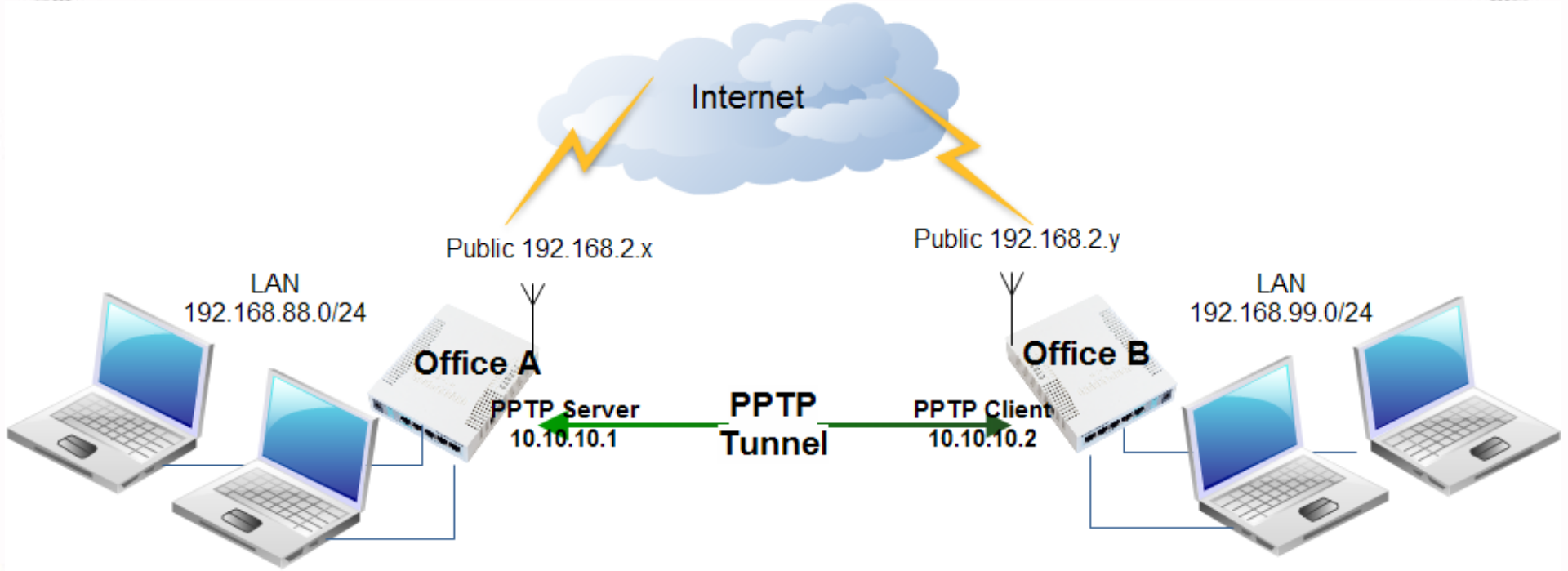
Remote address=IP yang diberikan ke client

MikroTik PPTP Client

- Pada menu Interface add new PPTP client, pada tab Dial Out isikan dengan IP public dari PPTP server, user dan password, kemudian apply



LAB PPTP Tunneling (Mikrotik to Mikrotik)



Buat Static Routing

Office A (PPTP Server)

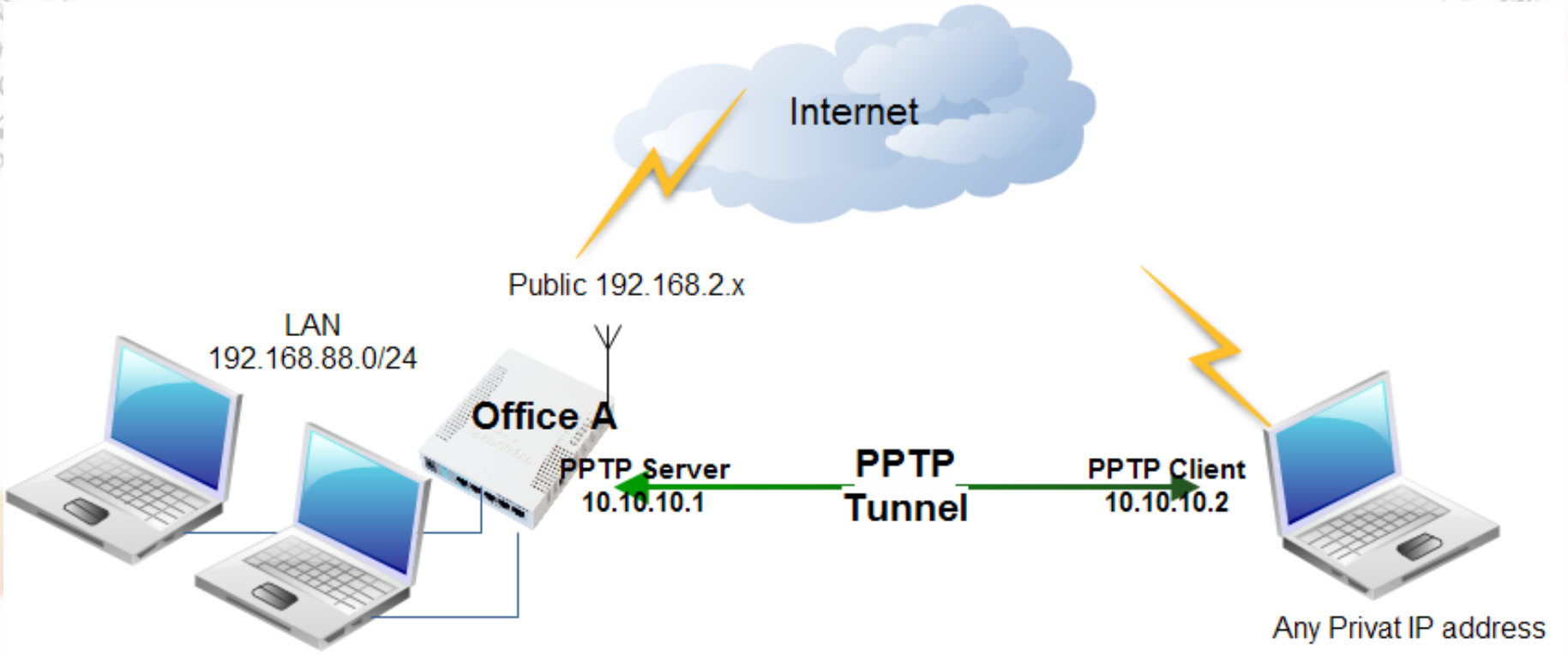
```
IP Route
add dst-address=192.168.99.0/24
gateway=10.10.10.2
```

Office B (PPTP Client)

```
IP Route
add dst-address=192.168.88.0/24
gateway=10.10.10.1
```

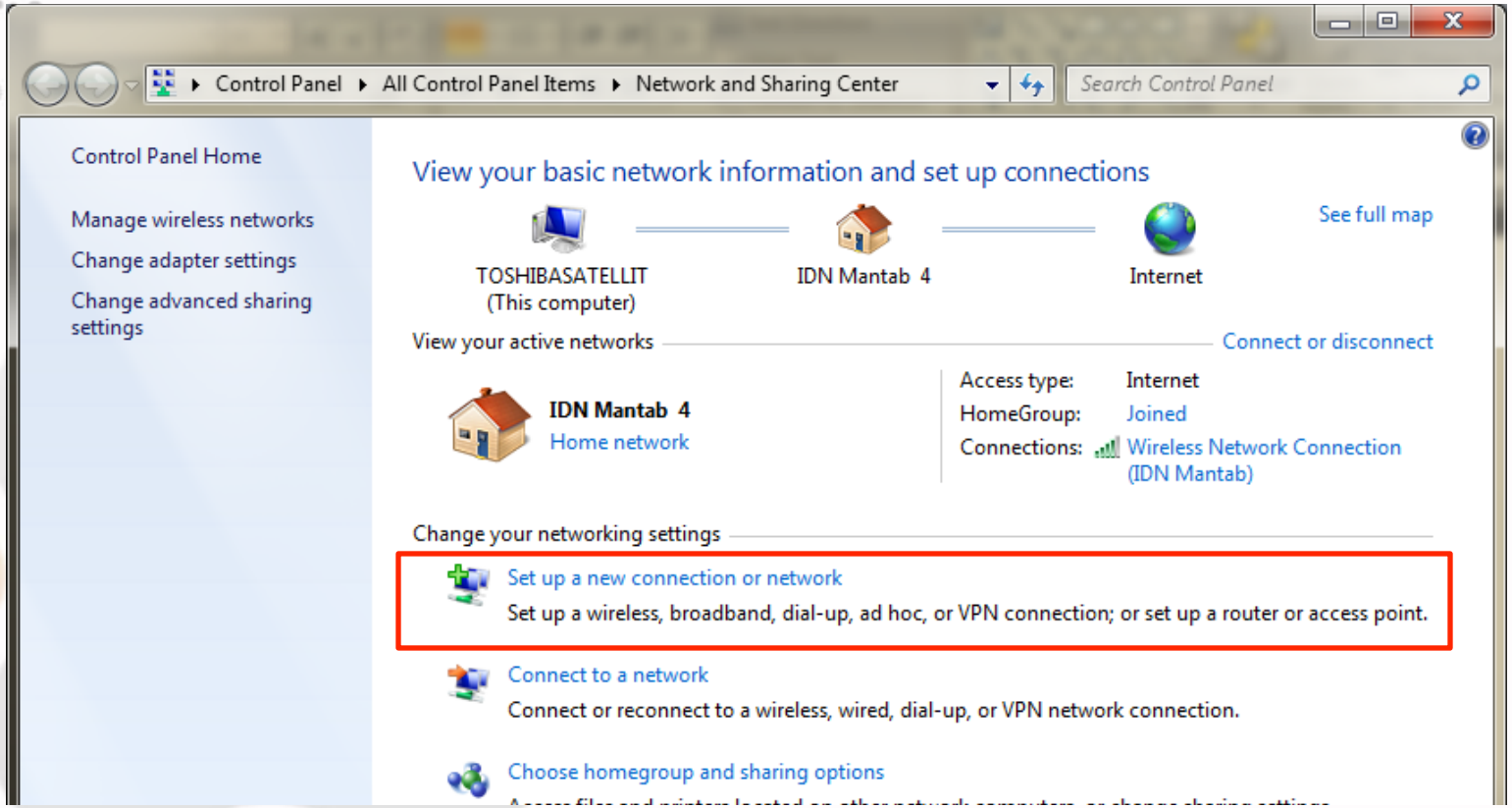
LAB Tunneling (MK-Laptop/PC)

- Koneksi PPTT client dengan Windows



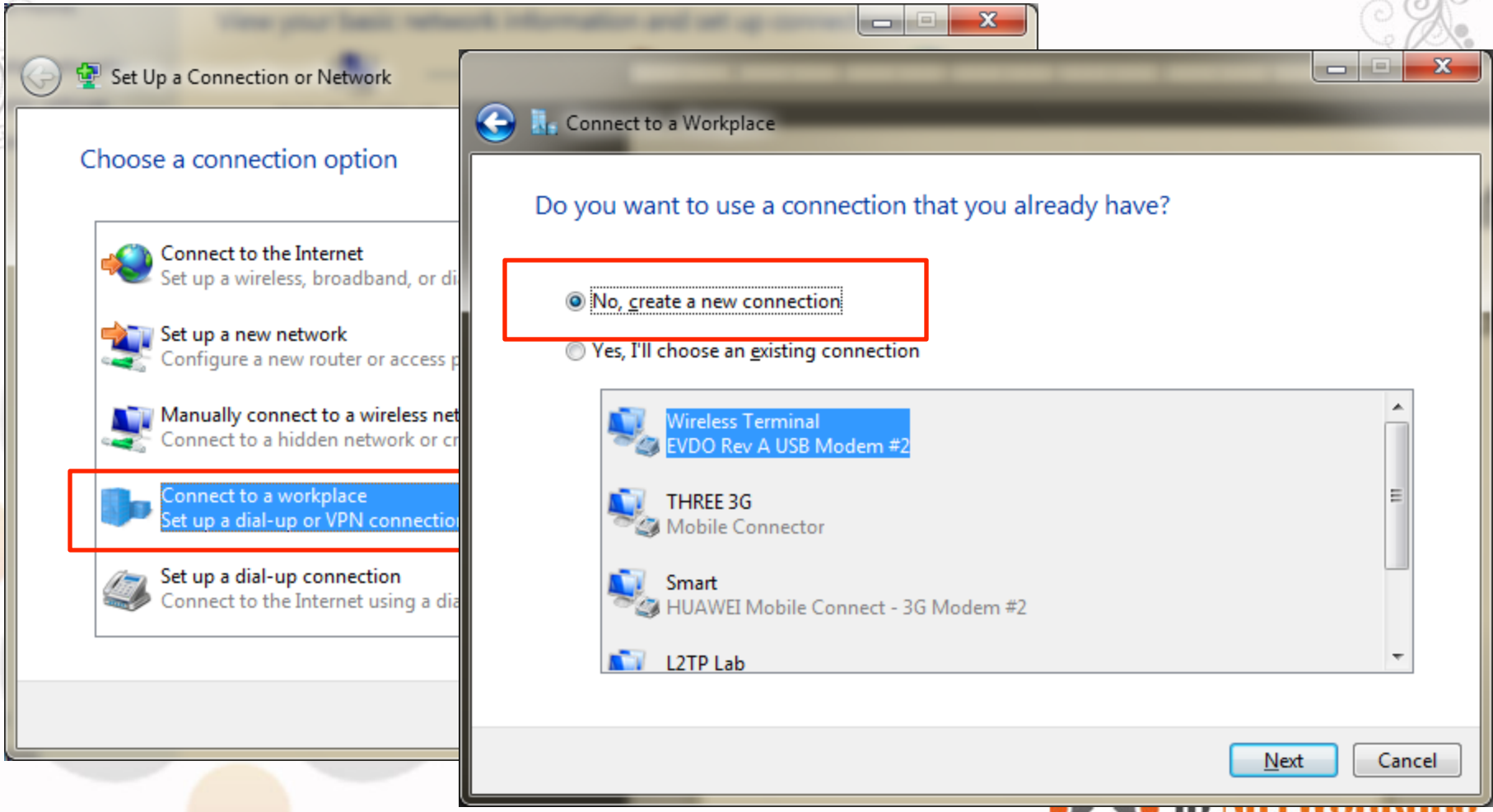
(Windows) PPTP Client

- PPTP server masih menggunakan configurasi sebelumnya
- Setup New Connection di Network Connection



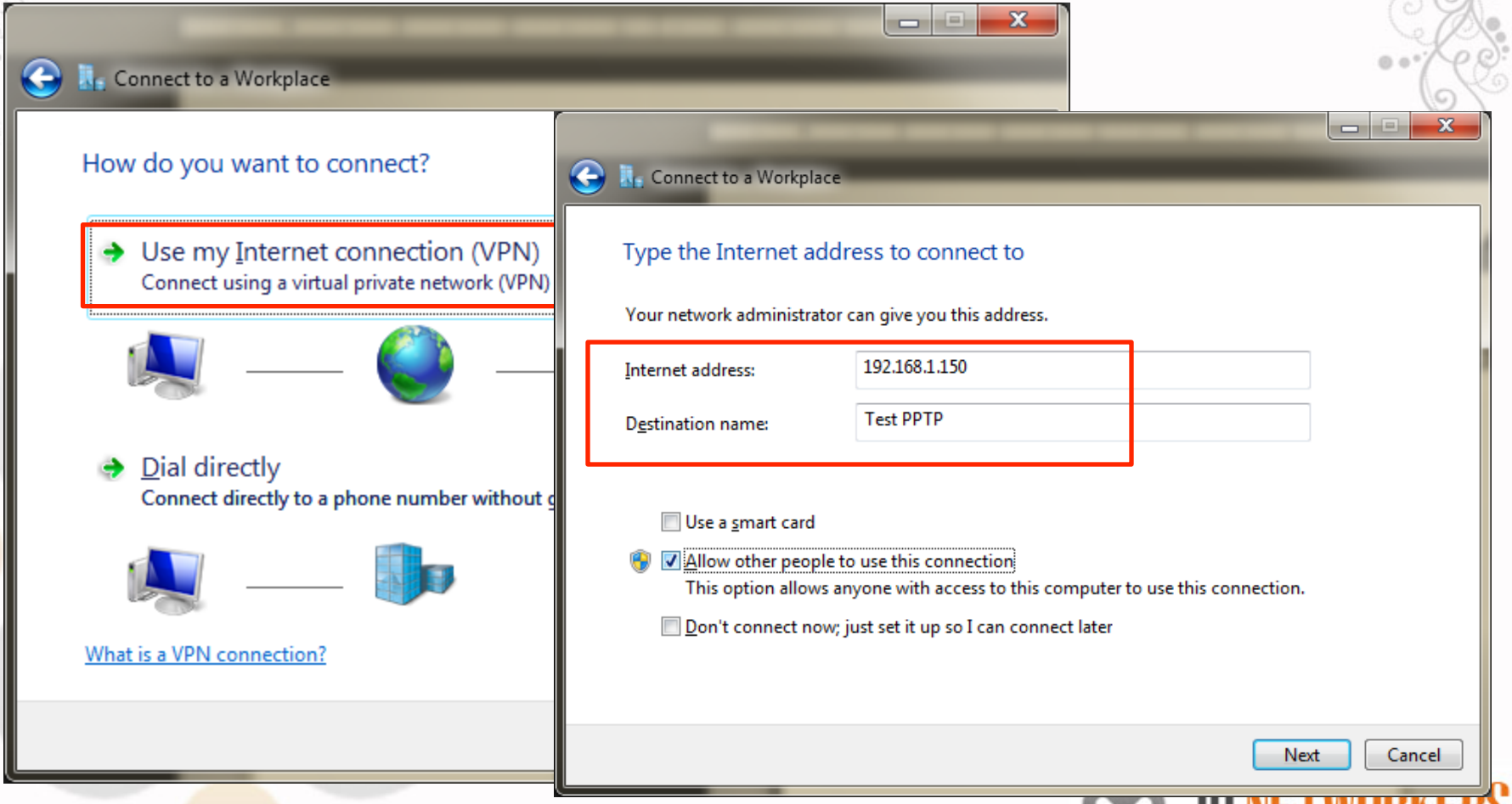
(Windows) PPTP Client

- Setup New Connection di Network Connection



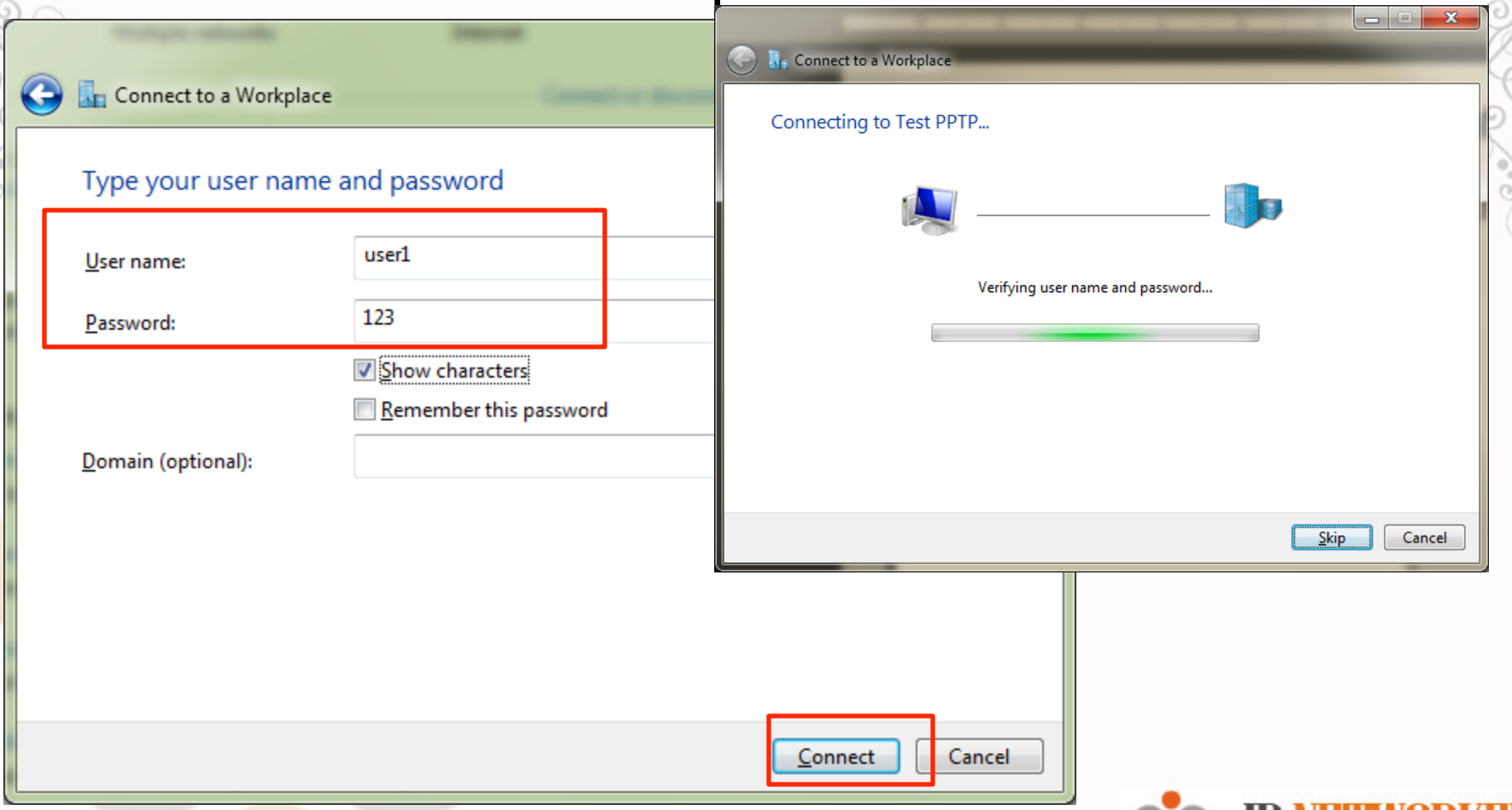
(Windows) PPTP Client

- Pilih Connect Using VPN & Isikan IP PPTP Server



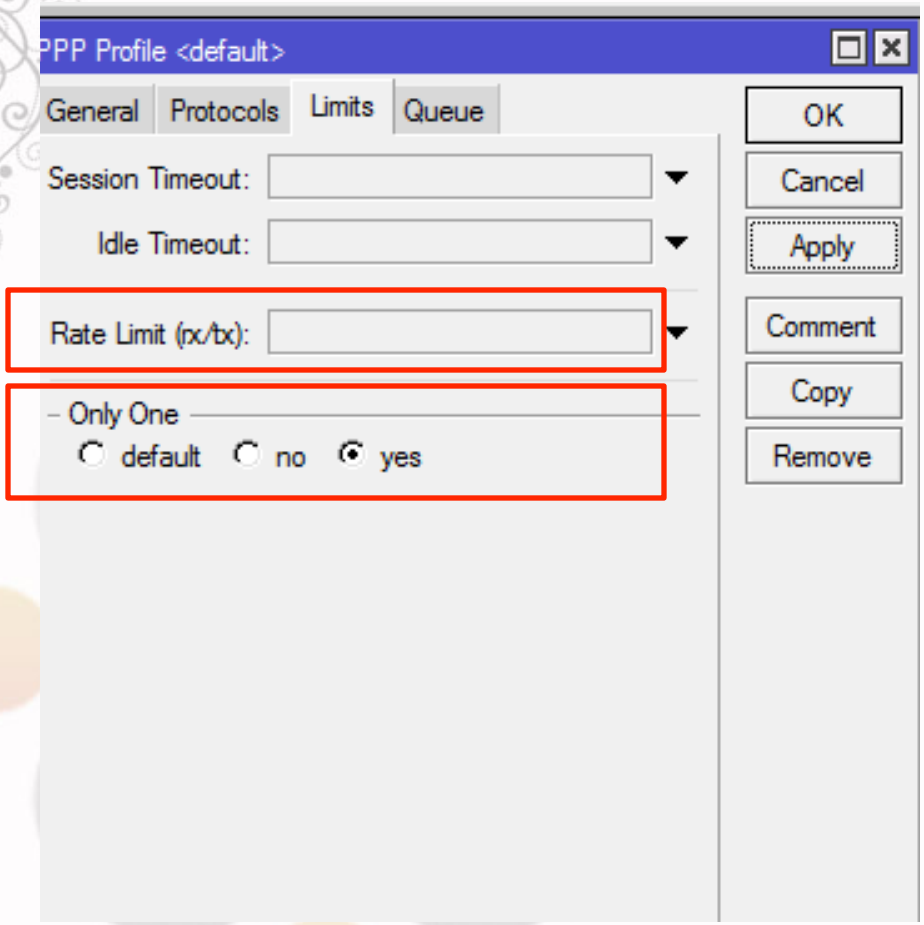
(Windows) PPTP Client

- Masukkan username & password PPTP-Client



Fitur pada PPTP

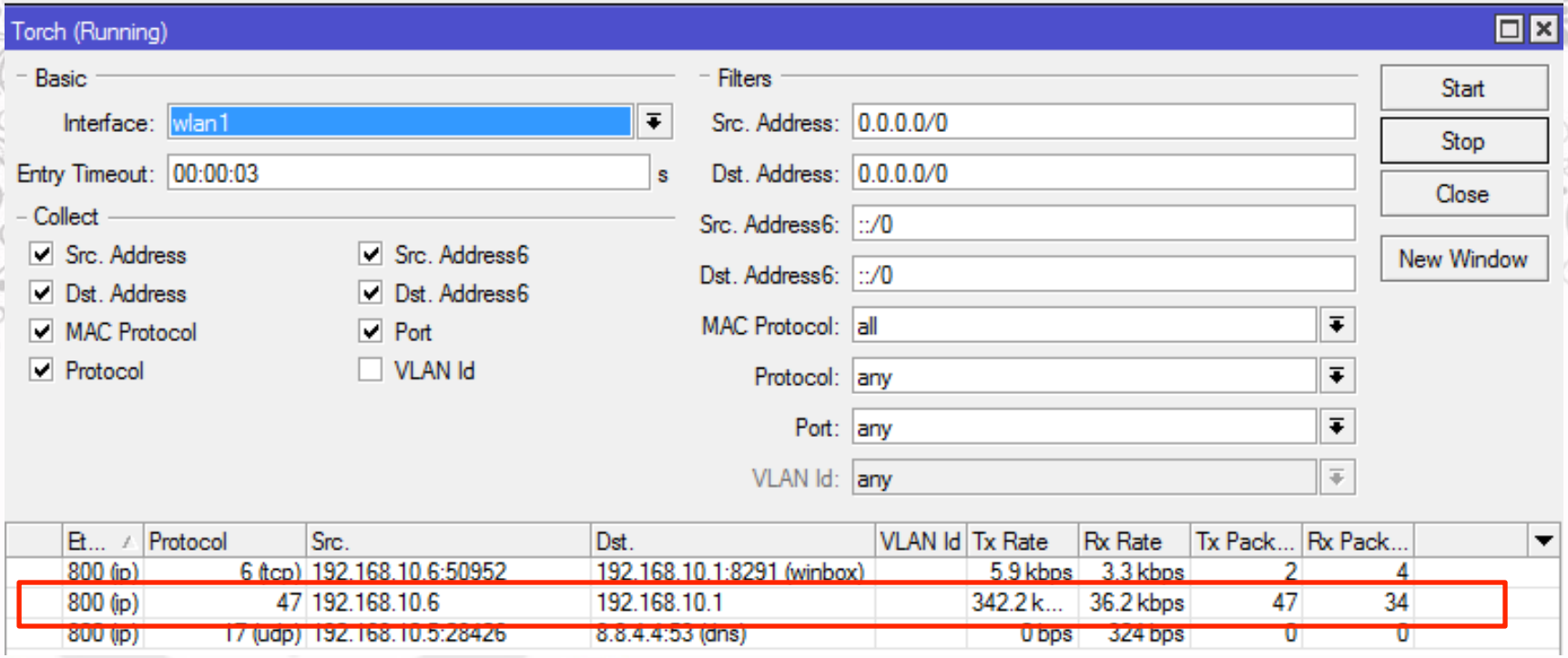
- PPP Profile Limit



Limit bandwidth

Satu user 1 session

PPTP Traffic Analyze

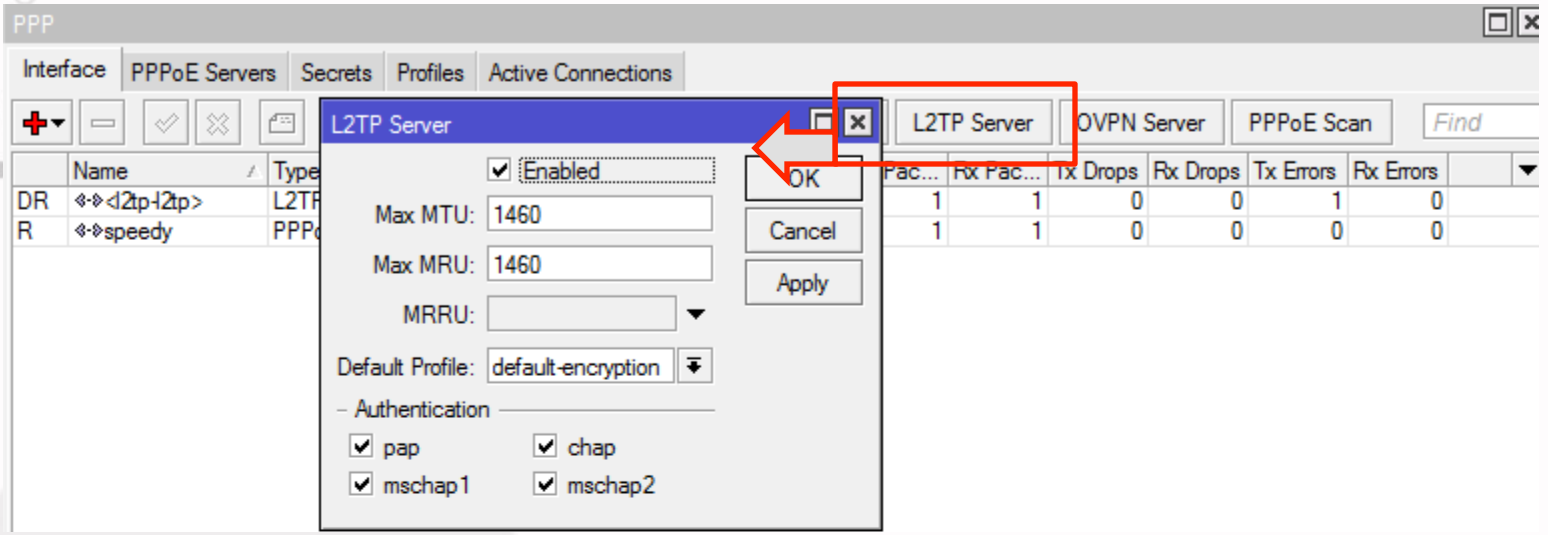


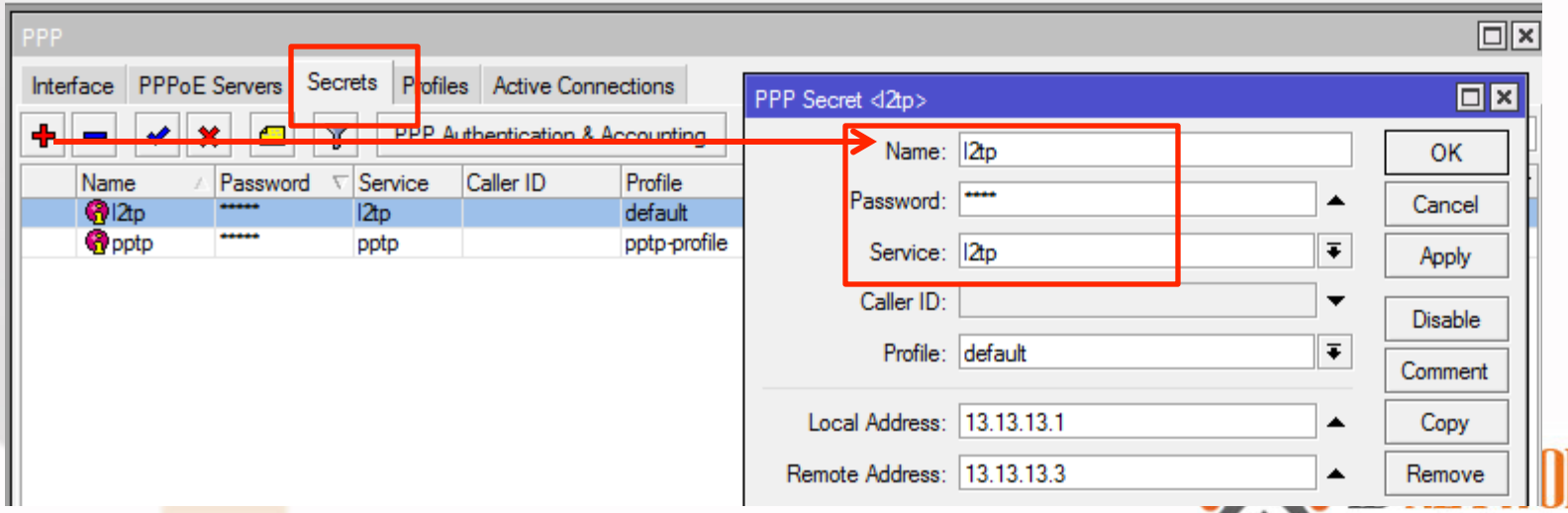
- Apabila kita browsing di internet tidak, traffik aktual tidak terdeteksi.
- Koneksi yang terdeteksi adalah koneksi tunnel PPTP dengan Protocol 47 (GRE)

L2TP

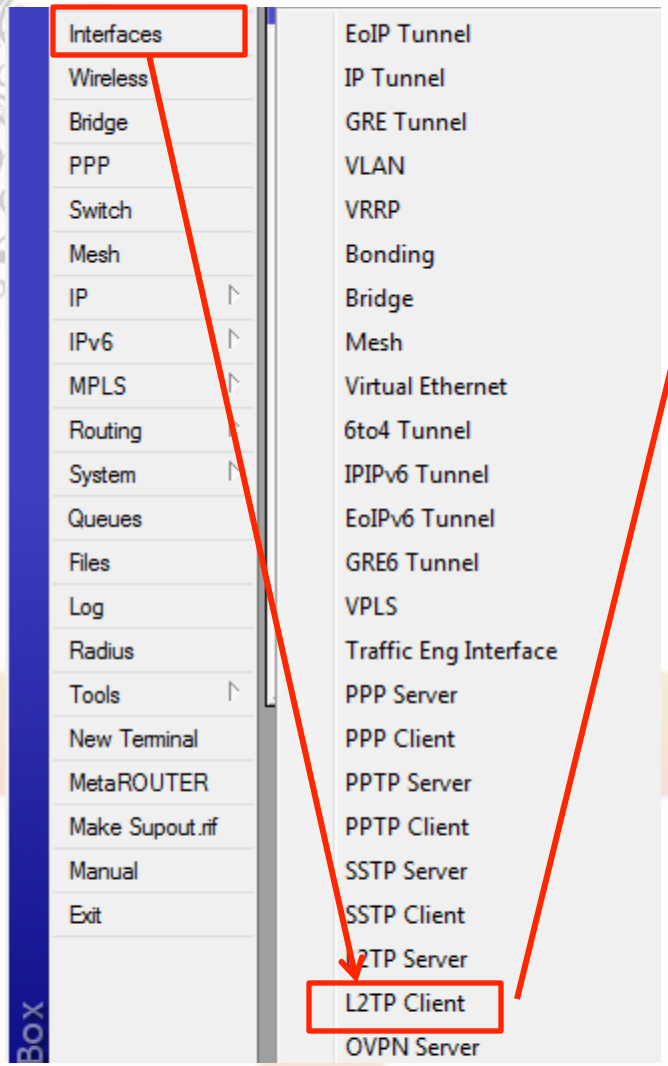
- Layer 2 Tunneling Protocol (L2TP) adalah jenis tunneling & encapsulation lain untuk protocol PPP.
- L2TP mensupport non-TCP/IP protocols (Frame Relay, ATM and SONET).
- L2TP dikembangkan atas kerja sama antara Cisco dan Microsoft untuk menggabungkan fitur dari PPTP dengan protocol proprietary Cisco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

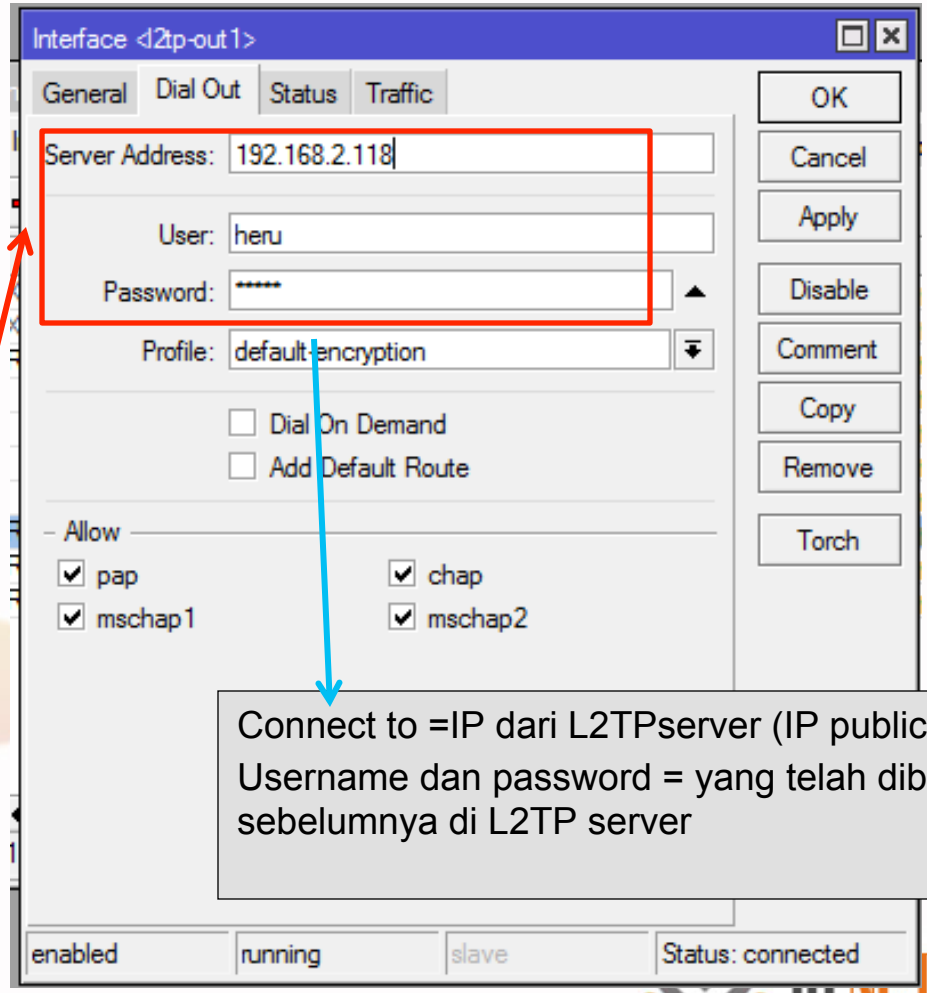
L2TP Server





MikroTik L2TP Client

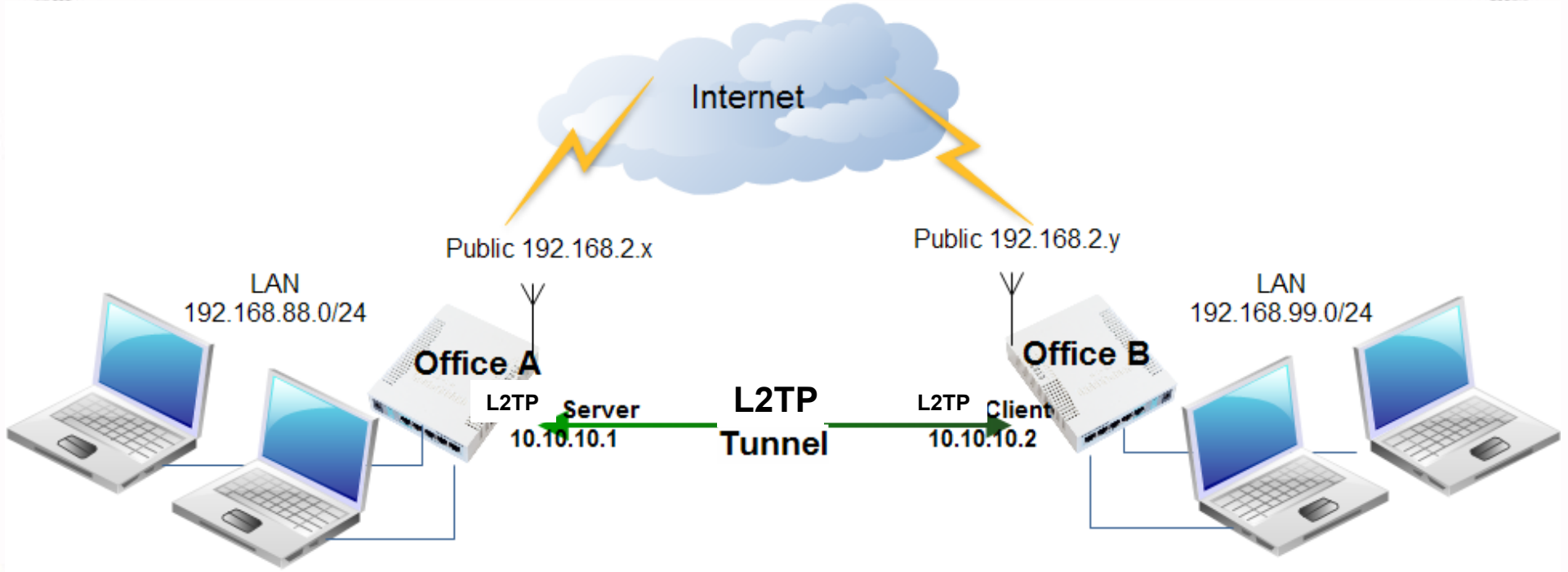




Connect to =IP dari L2TPserver (IP publicnya)

Username dan password = yang telah dibuat sebelumnya di L2TP server

LAB L2TP Tunneling (Mikrotik to Mikrotik)



Buat Static Routing

Office A (PPTP Server)

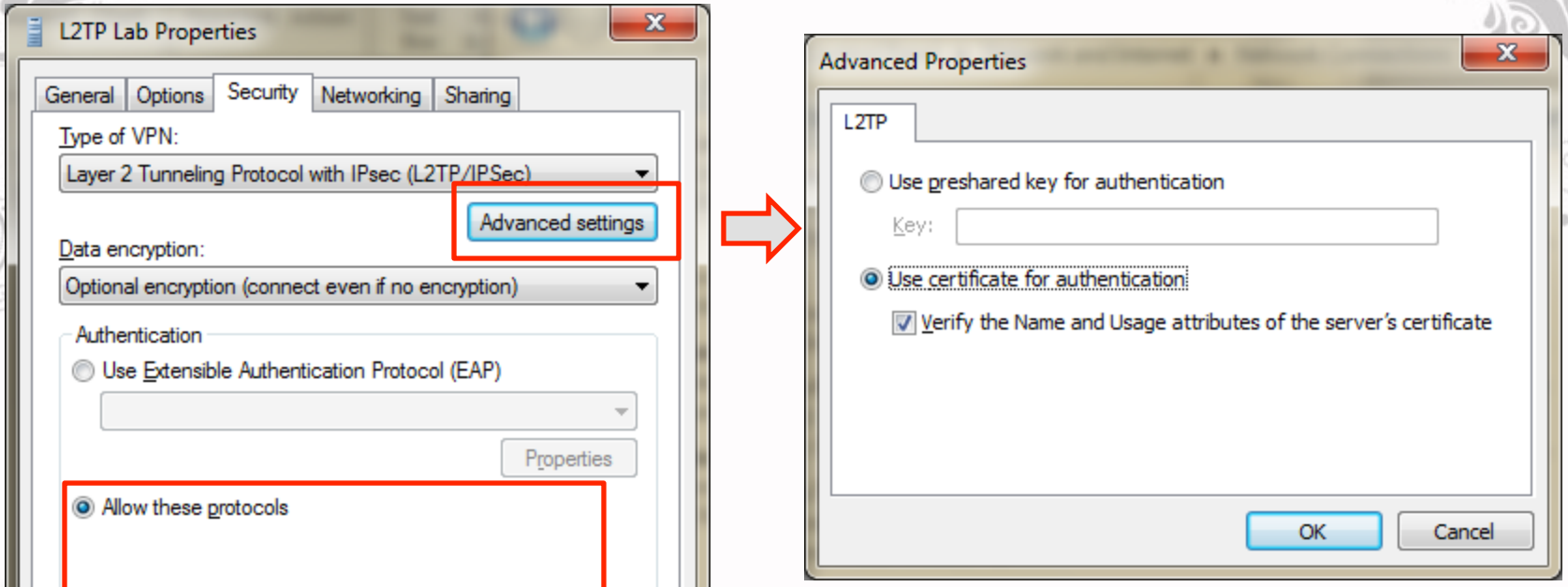
```
IP Route
add dst-address=192.168.99.0/24
gateway=10.10.10.2
```

Office B (PPTP Client)

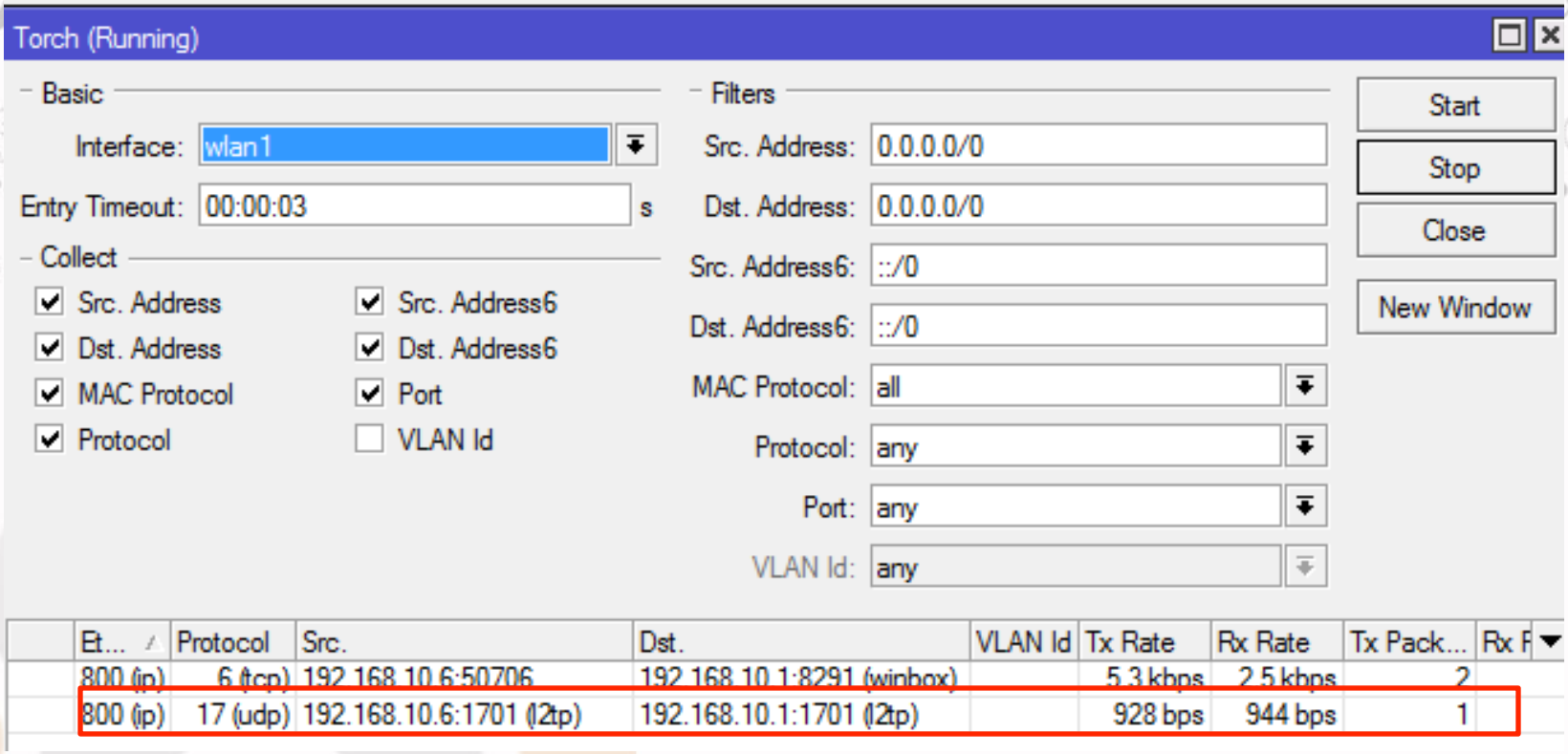
```
IP Route
add dst-address=192.168.88.0/24
gateway=10.10.10.1
```

ID NETWORKERS
Expert Trainer & Consultant

Windows L2TP Client



L2TP – Traffic Analyze

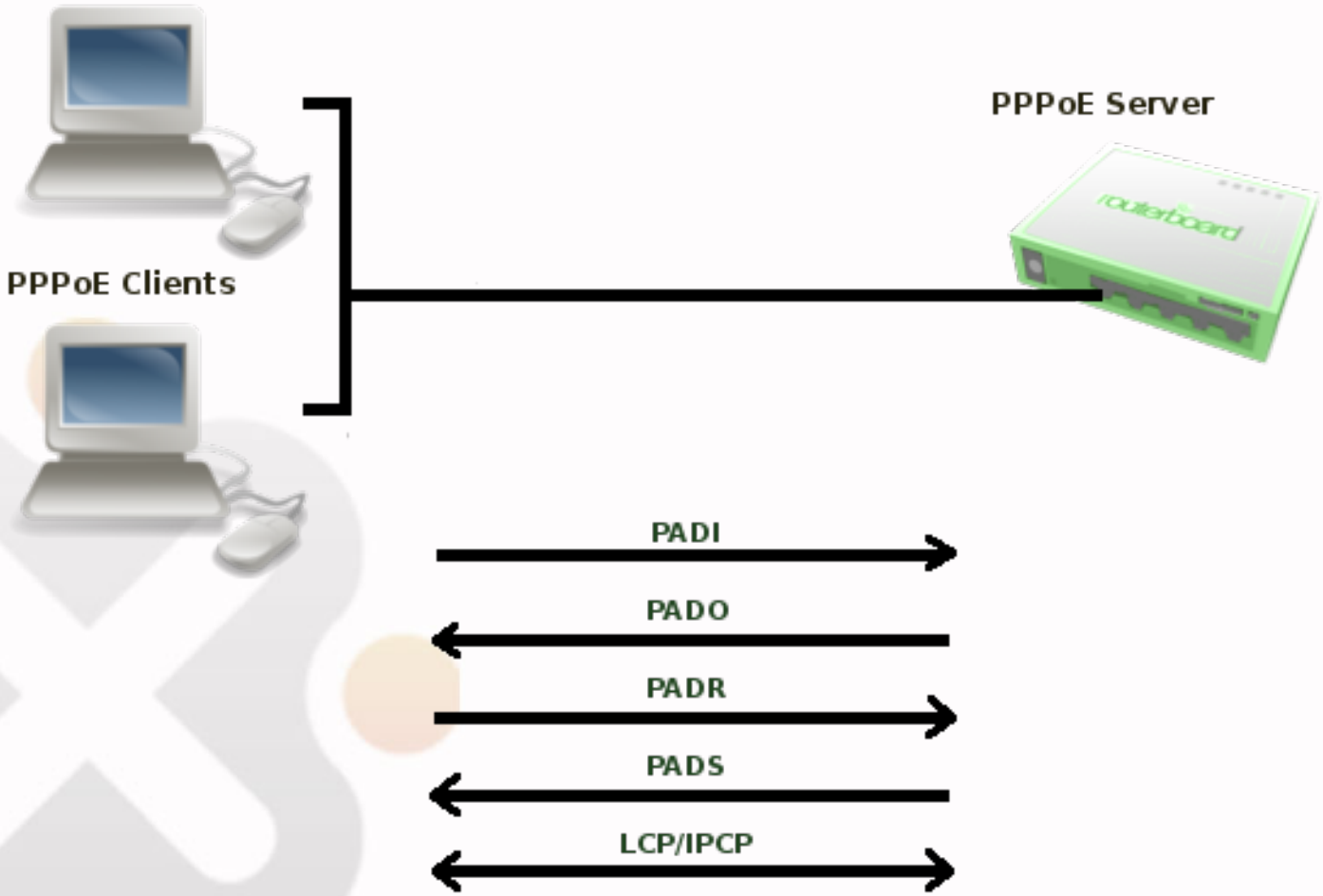


- Setelah menggunakan L2TP tunnel, traffik pada wlan1 merupakan traffic L2TP
- Hanya menggunakan protocol UDP

PPPoE

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

PPPoE



Tahapan Koneksi PPPoE

- PADI (PPP Active Discovery Initiation), Di sini PPoE client mengirimkan paket broadcast ke jaringan dengan alamat pengiriman mac address FF:FF:FF:FF:FF:FF. PPPoE client mencari di mana lokasi PPoE server dalam jaringan.

- PADO (PPPoE Active Discovery Offer). PADO ini merupakan jawaban dari PPoE server atas PADI yang didapatkan sebelumnya. PPPoE server memberikan identitas berupa MAC addressnya.

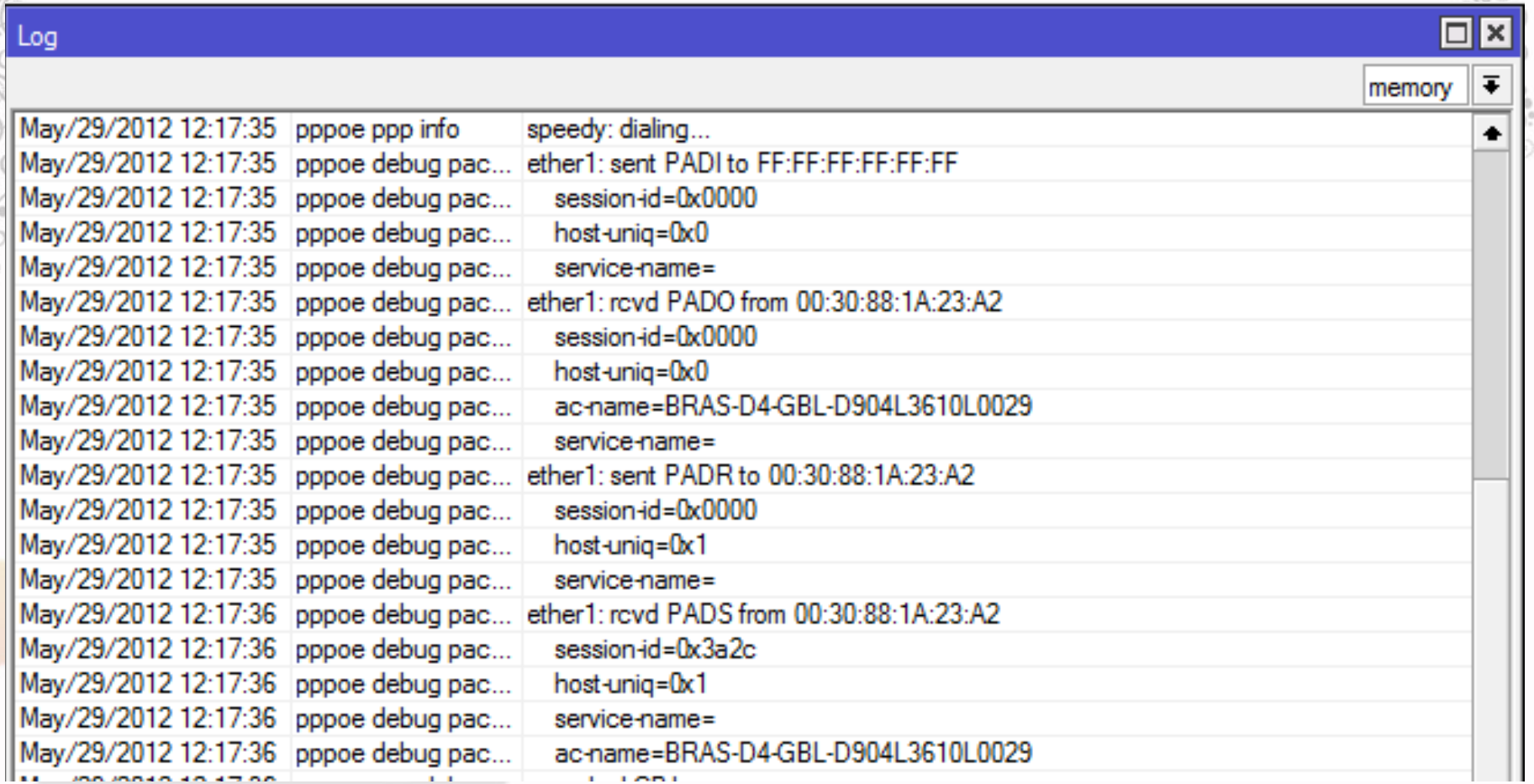
- PADR (PPP Active Discovery Request), merupakan konfirmasi dari PPoE client ke server. Disini PPoE client sudah dapat menghubungi PPoE server menggunakan mac addressnya, berbeda dengan paket PADI yang masih berupa broadcast.

Tahapan Koneksi PPPoE

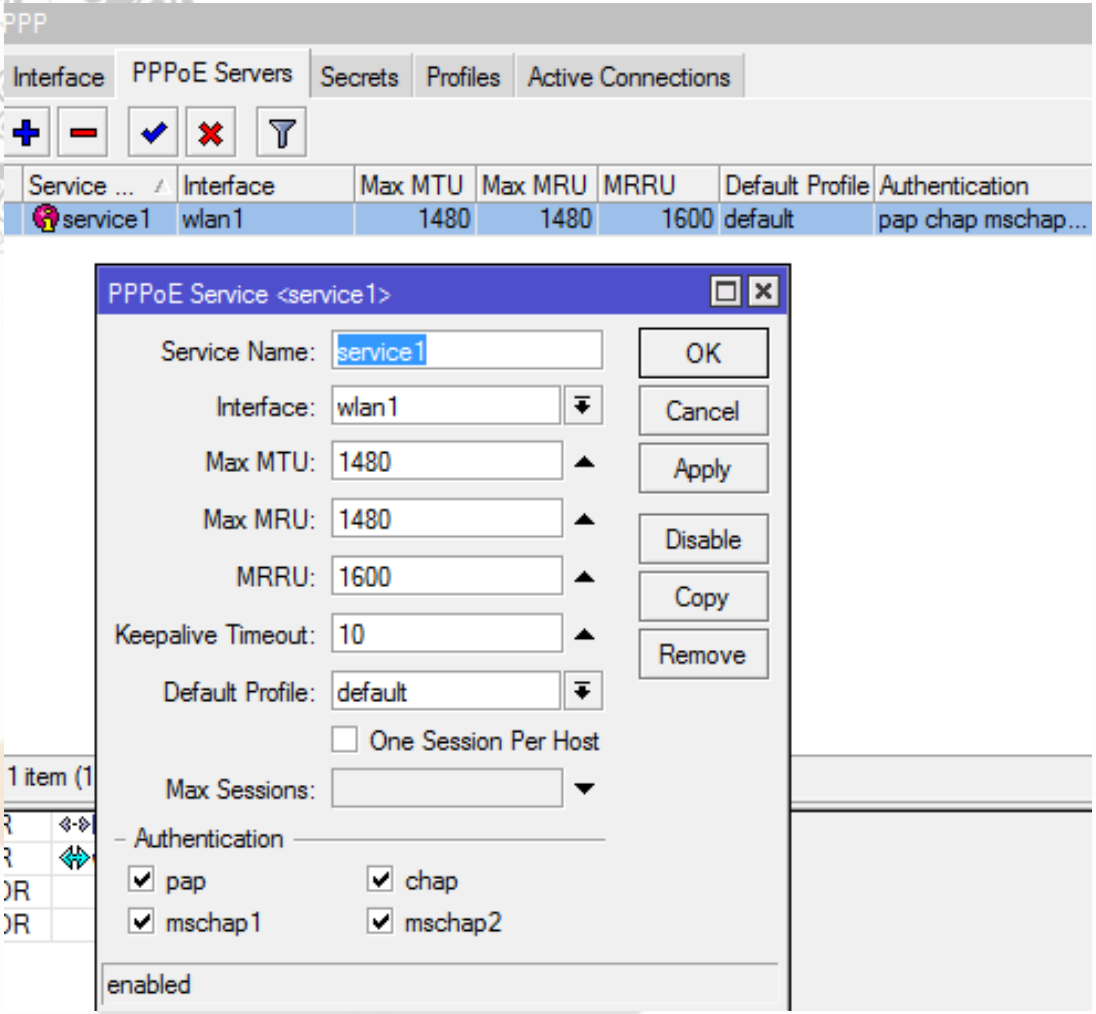
- PADS (PPP Active Discovery Session-confirmation), dari PPoE server ke client. Session-confirmation di sini memang berarti ada session ID yang diberikan oleh server kepada client. Pada tahap ini juga terjadi negosiasi Username, password dan IP address.

- PADT (PPP Active Discovery Terminate), bisa dikirim dari server ataupun client, ketika salah satu ingin mengakhiri koneksinya

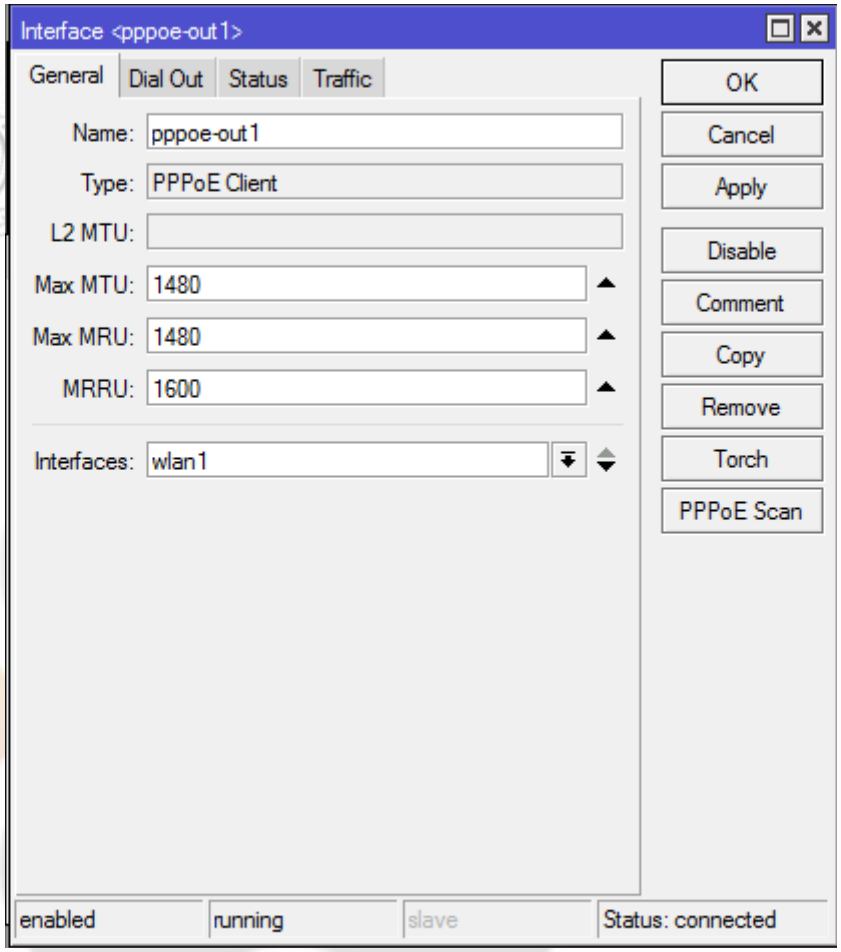
Tahapan Koneksi PPPoE

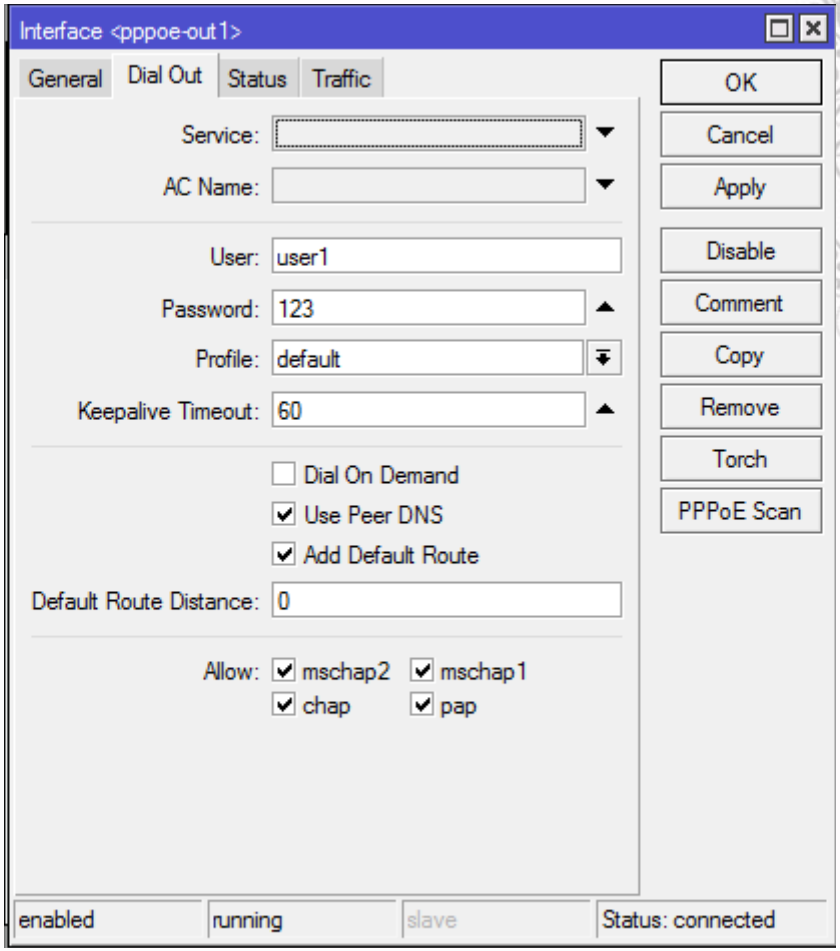


PPPOE SERVER



PPOE Client

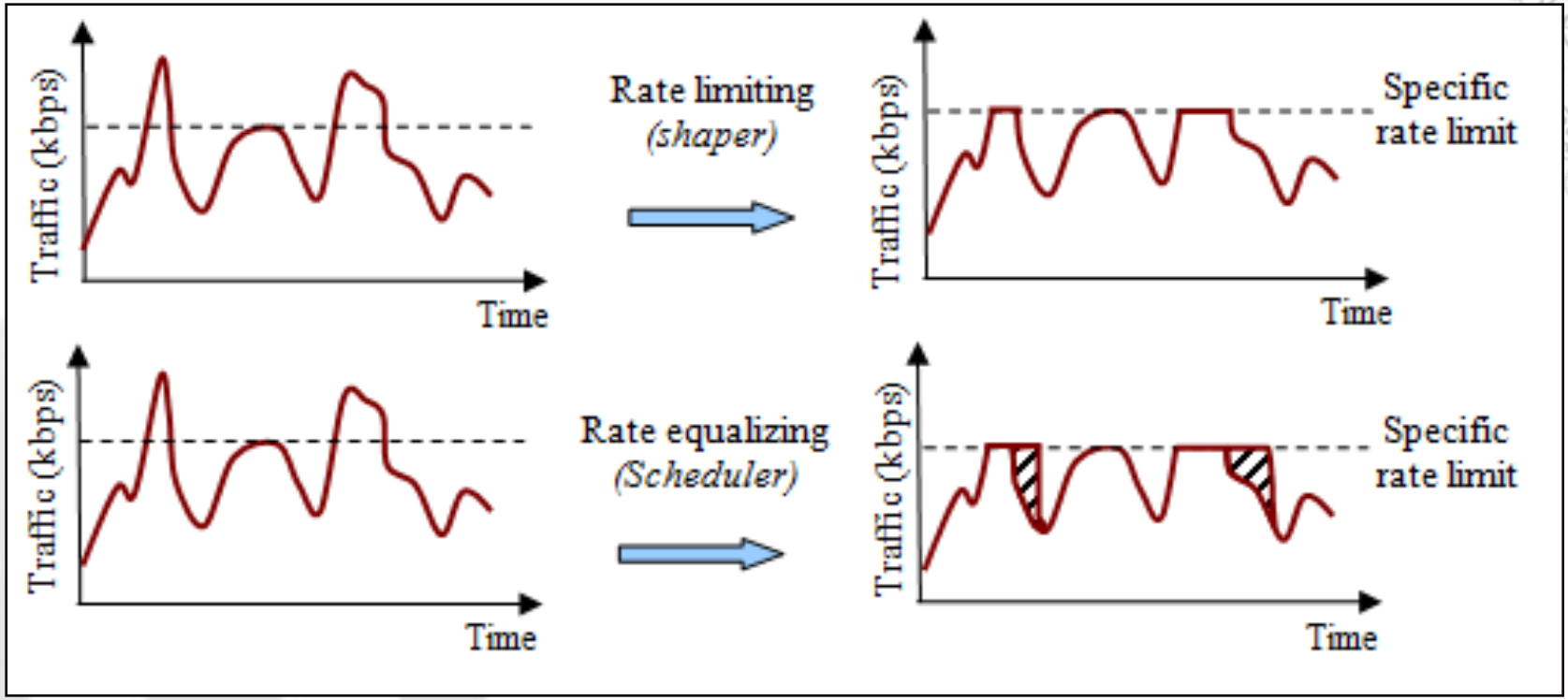




QoS

QoS

- Bandwidth Limiter



Rate Limit

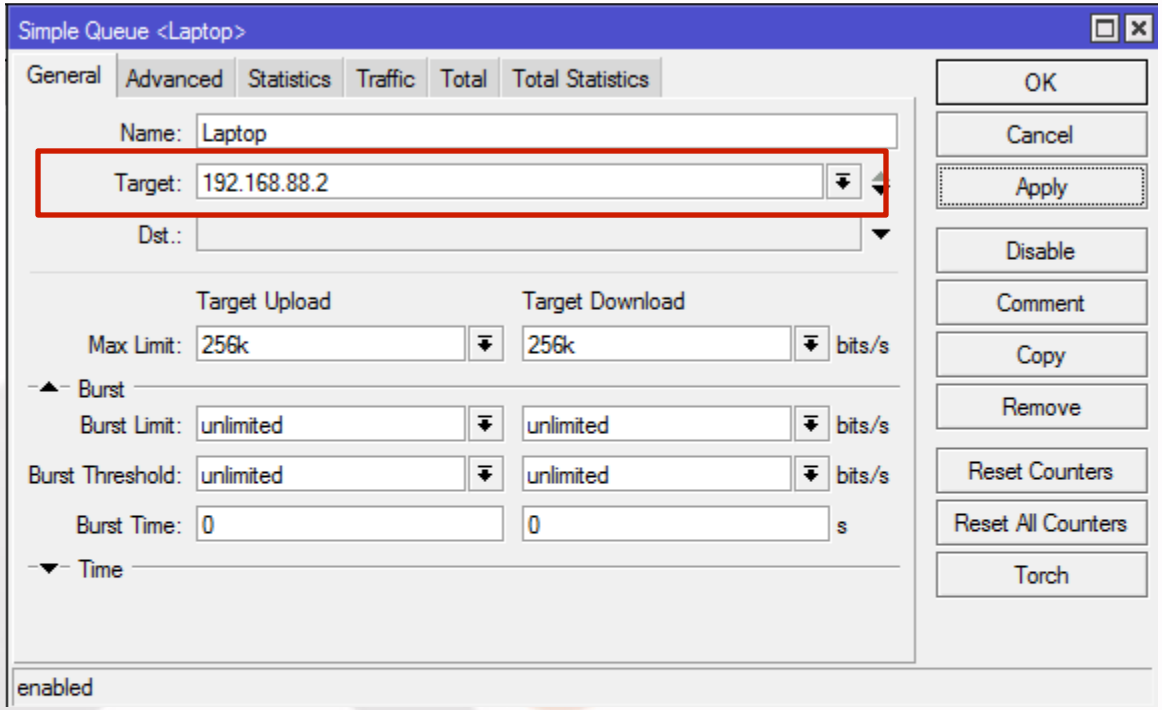
- Pada RouterOS, dikenal 2 jenis batasan rate limit:
- **CIR** (Committed Information Rate) - dalam keadaan terburuk, client akan mendapatkan bandwidth sesuai dengan "**limit-at**" (dengan asumsi bandwidth yang tersedia cukup untuk CIR semua client).
- **MIR** (Maximal Information Rate)- jika masih ada bandwidth yang tersisa setelah semua client mencapai "limit-at", maka client bisa mendapatkan bandwidth tambahan hingga "**max-limit**".

Simple Queue

- Pada RouterOS, Bandwidth Limit dapat dilakukan dengan berbagi cara (wireless access list, ppp secret dan hotspot user)
- Simple queue mengatur pembatasan bandwidth dengan hanya mendefinisikan parameter IP address (target address) dari host/koneksi yang dilimit.
- Simple queue paling sederhana hanya melakukan pembatasan bandwidth max-limit (MIR)

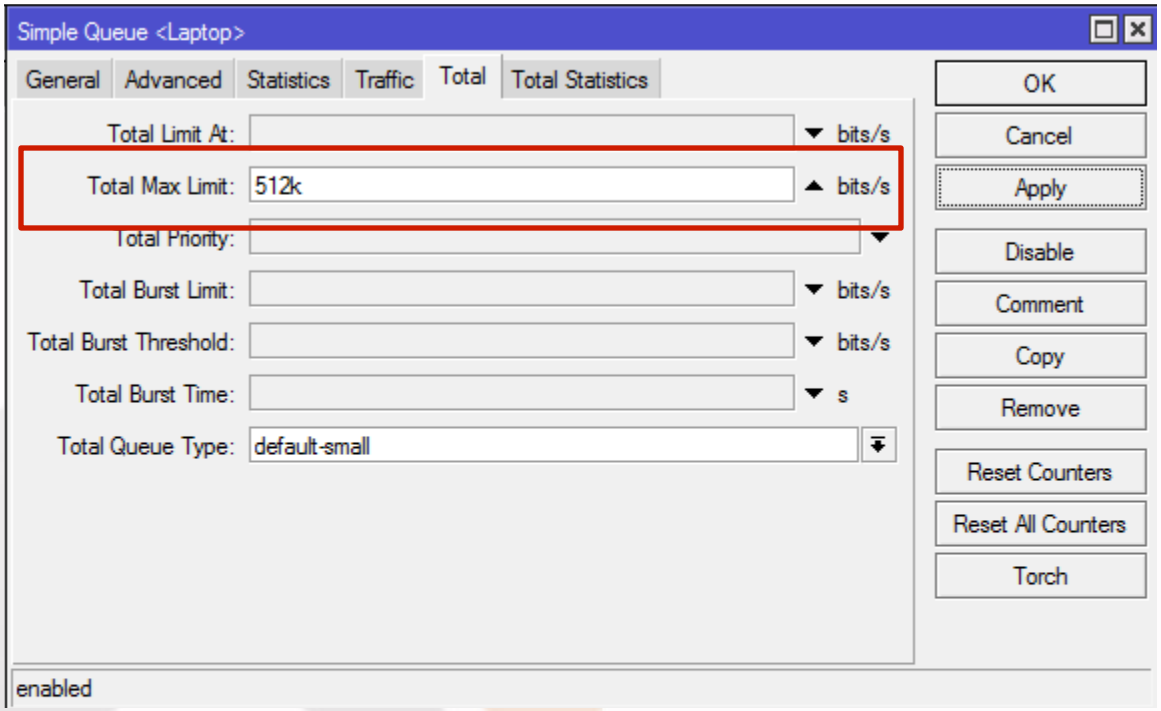
LAB - Simple Queue

Batasi bandwidth Laptop anda 256k Upload, 256k Download



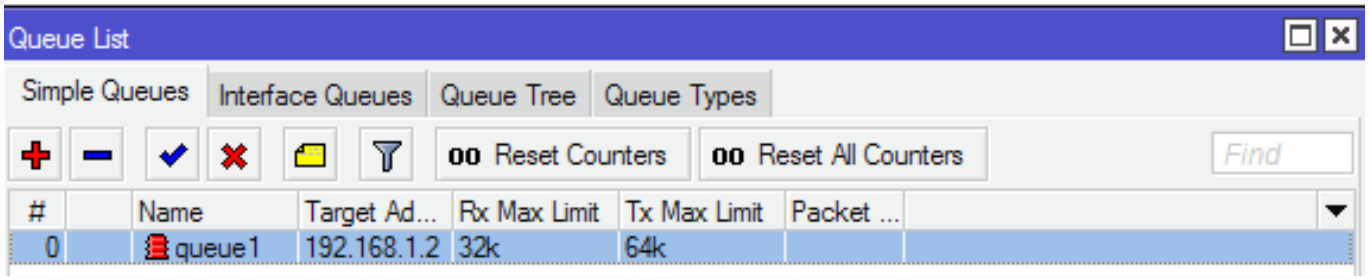
LAB - Simple Queue

Total adalah penjumlahan upload dan download

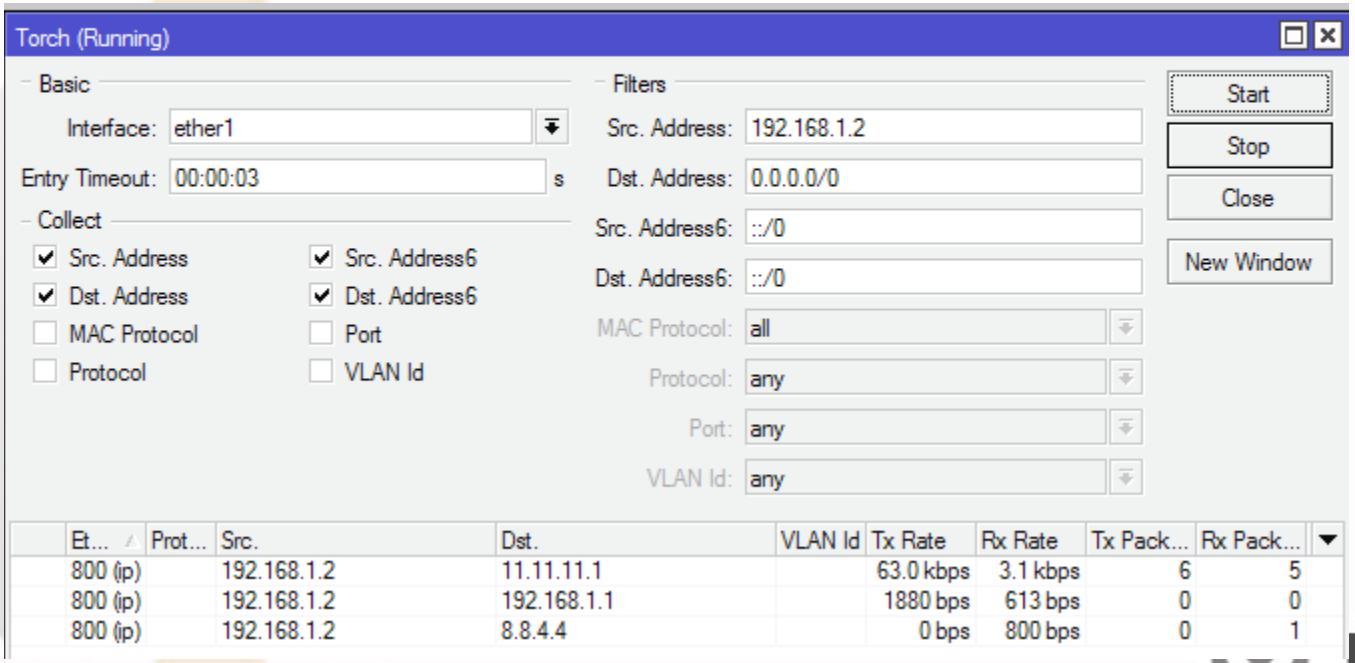


LAB-Cek Bandwidth Status

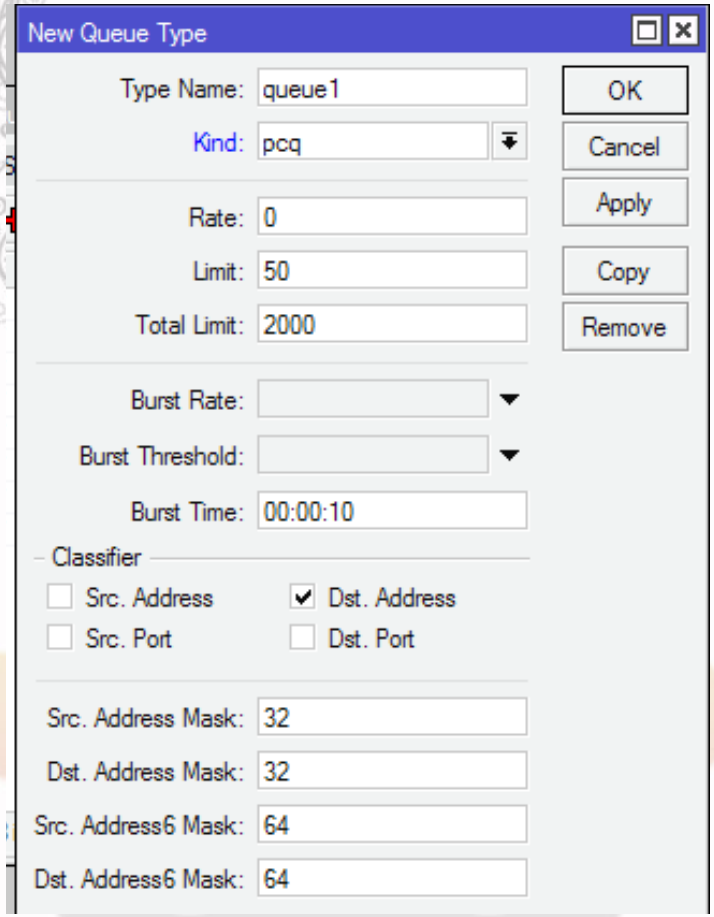
Simple Queue status



Toot Torch status



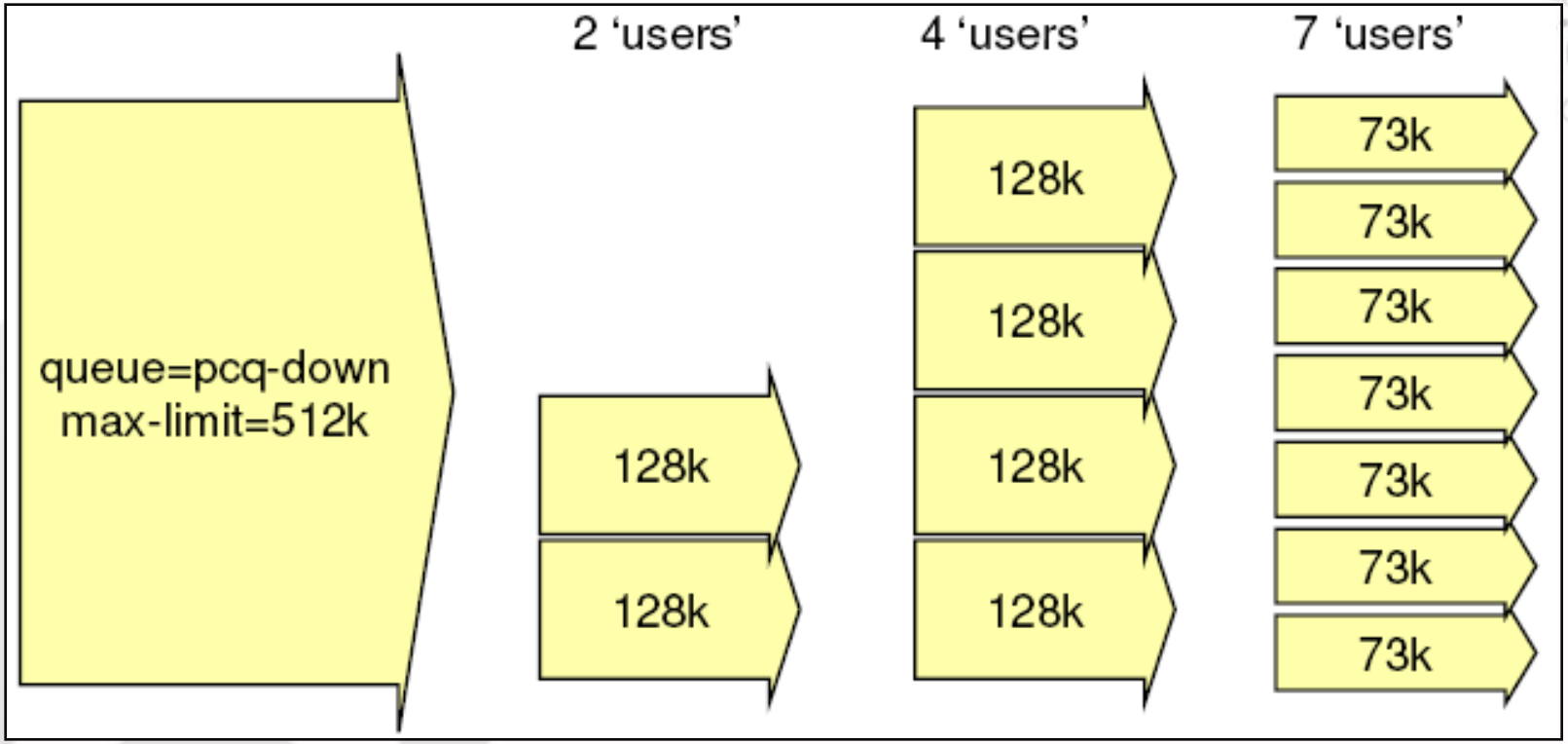
PCQ



- PCQ akan membuat sub-queue, berdasarkan parameter pcq-classifier (src-address, dst-address, src-port, dst-port)
- Dimungkinkan untuk membatasi maksimal data rate untuk setiap sub-queue (pcq-rate) dan jumlah paket data (pcq-limit)
- Total ukuran queue pada PCQ-sub-queue tidak bisa melebihi jumlah paket sesuai pcq-total-limit

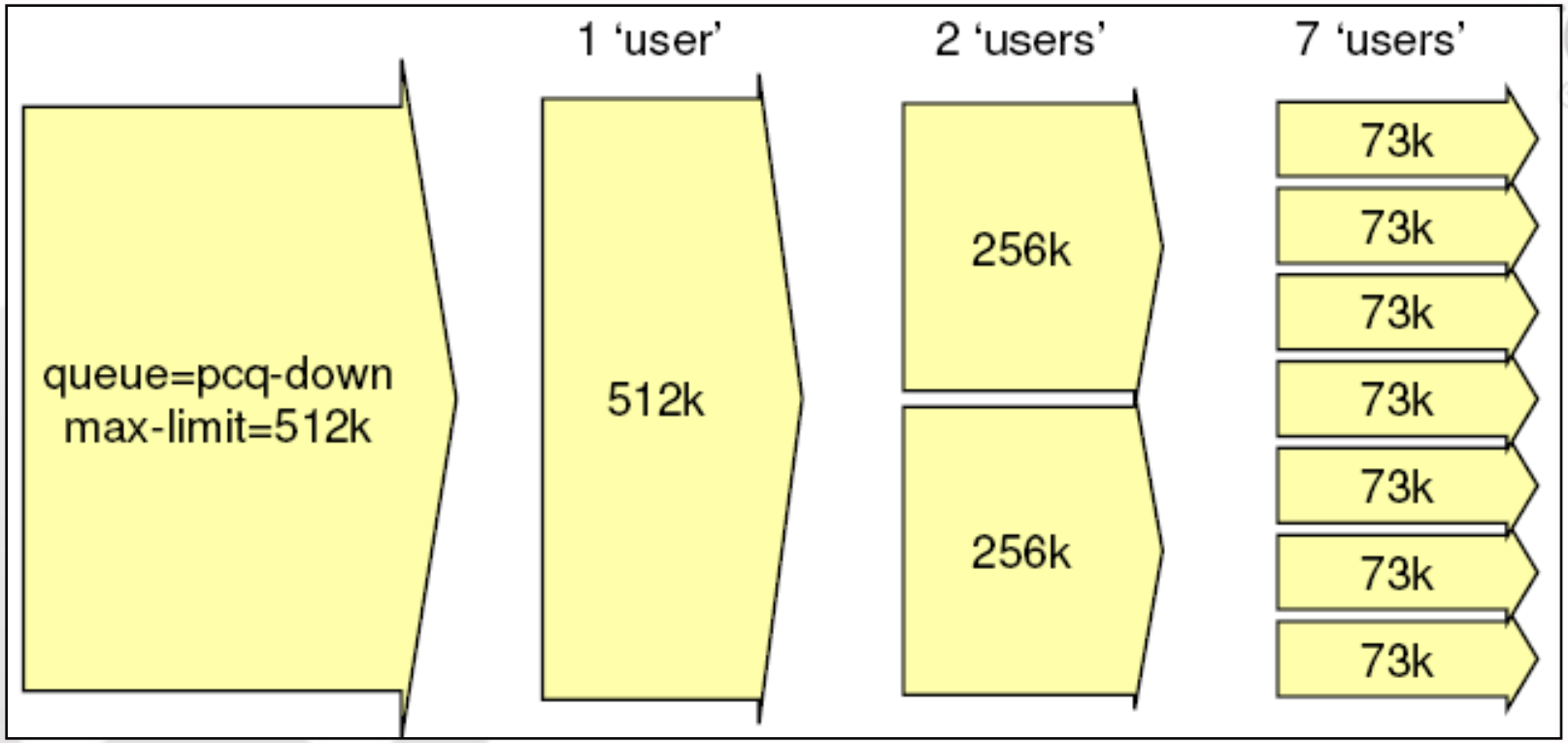
Contoh Penggunaan PCQ

- PCQ Rate = 128k

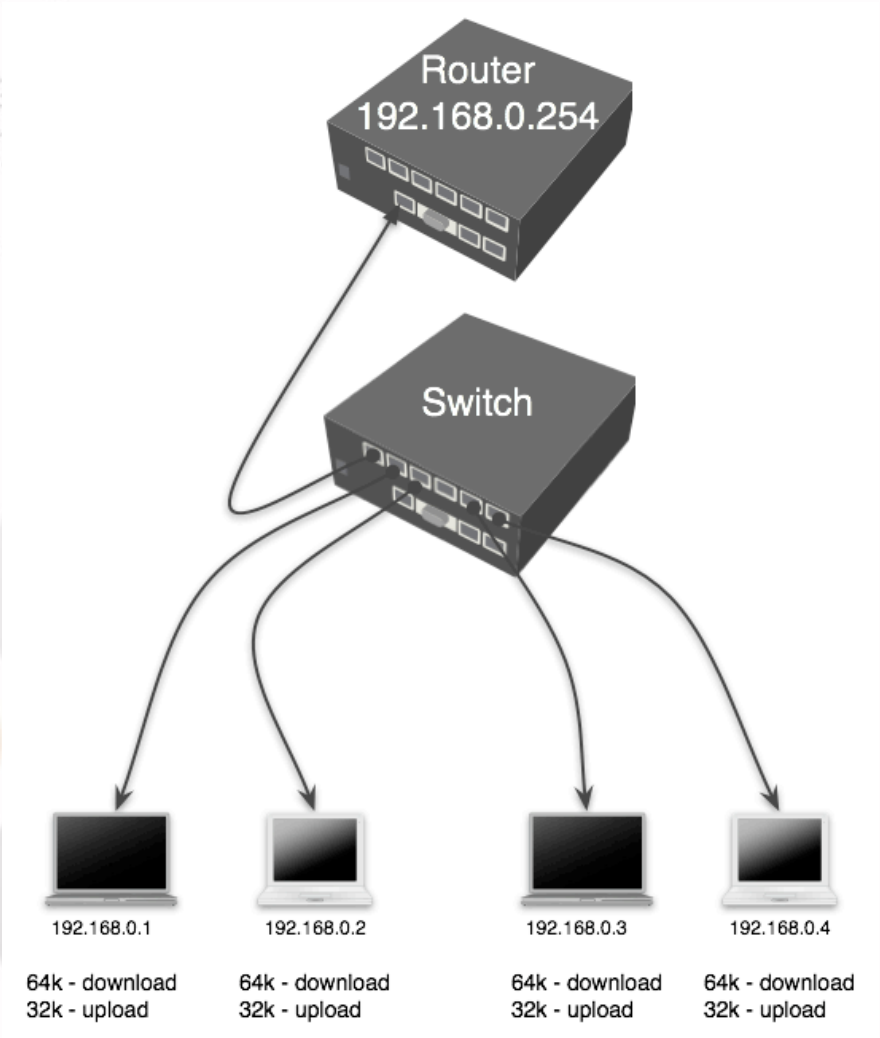


Contoh Penggunaan PCQ

- PCQ Rate = 0



LAB- PCQ



LAB - PCQ

- Buat Mark Packet upload & download

```
/ip firewall mangle add chain=prerouting action=mark-packet in-interface=etherLAN new-packet-mark=client_upload
/ip firewall mangle add chain=prerouting action=mark-packet in-interface=etherWAN new-packet-mark=client_download
```

- Buat 2 PCQ queue types – satu untuk download dan satu untuk upload. dst-address untuk traffik download user, src-address untuk traffik upload

```
/queue type add name="PCQ_download" kind=pcq pcq-rate=64000 pcq-classifier=dst-address
/queue type add name="PCQ_upload" kind=pcq pcq-rate=32000 pcq-classifier=src-address
```

- Buat 1 rule simple queue

```
/queue simple add target-addresses=192.168.0.0/24 queue=PCQ_upload/PCQ_download \ packet-marks=client_download,client_upload
```

Network Management

ARP

- Meskipun pengalamatan paket data menggunakan alamat IP, alamat hardware/hardware address harus digunakan untuk transport data host to host pada connected network.
- ARP digunakan untuk mapping layer OSI level 3 (IP) ke layer OS level 2 (MAC Address).
- Router memiliki tabel entri ARP saat ini digunakan, biasanya tabel ARP dibuat secara dinamis oleh router, tetapi untuk meningkatkan keamanan jaringan, dapat juga dibuat secara statis baik sebagian atau semuanya dengan menambahkan secara manual pada entri ARP tabel.

Interface ARP Mode

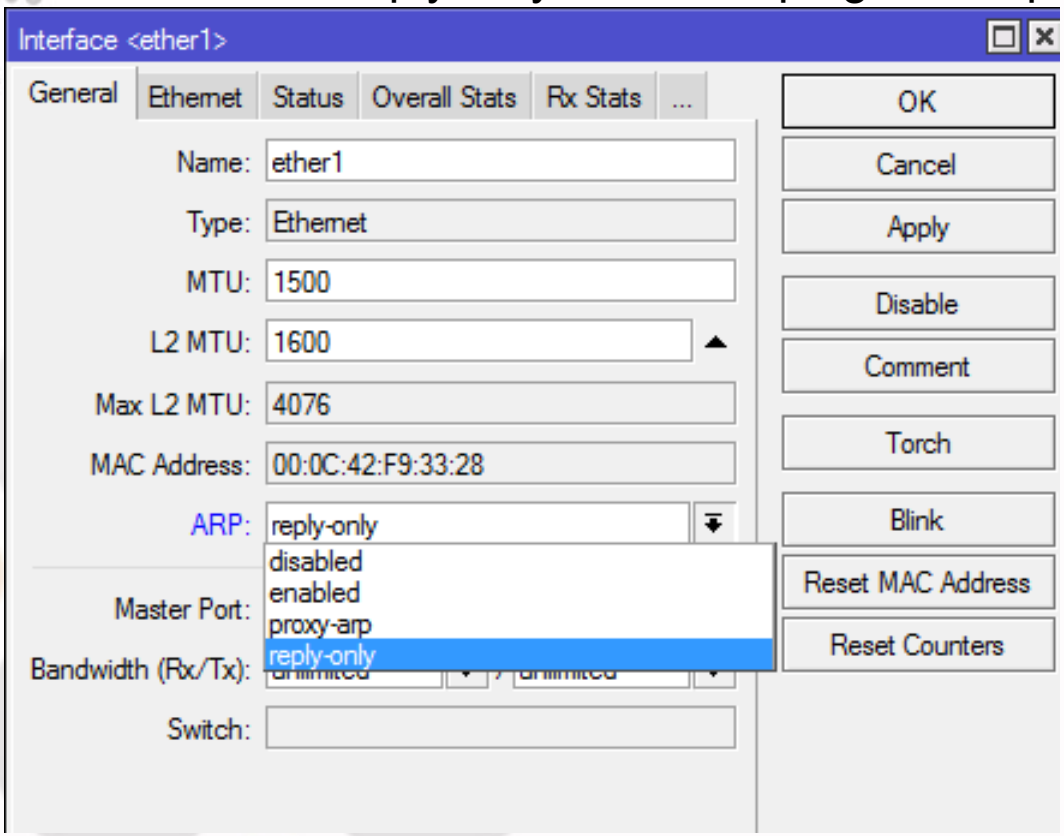
- Enable → Mode ini default enable pada semua interface di MikroTik. Semua ARP akan ditemukan dan secara dinamik ditambahkan dalam ARP tabel.
- Proxy ARP → Router dengan mode ARP proxy akan bertindak sebagai transparan proxy ARP antara dia atau lebih jaringan yang terhubung langsung.
- Reply Only →ARP reply-only memungkinkan router hanya kan mereply ARP statis ditemukan di tabel ARP, akses ke router dan ke jaringan di belakang router hanya dapat diakses oleh kombinasi Ip dan mac address yang ditemukan di tabel ARP.
- Disable → permintaan ARP dari klien tidak dijawab oleh router. Oleh karena itu, statis arp entri harus ditambahkan disamping disisi router juga disisi client. misal pada Windows menggunakan perintah arp:

  C: \> arp-s 192.168.2.1 00-aa-00-62-c6-09

LAB- ARP Mode

ARP Reply-Only

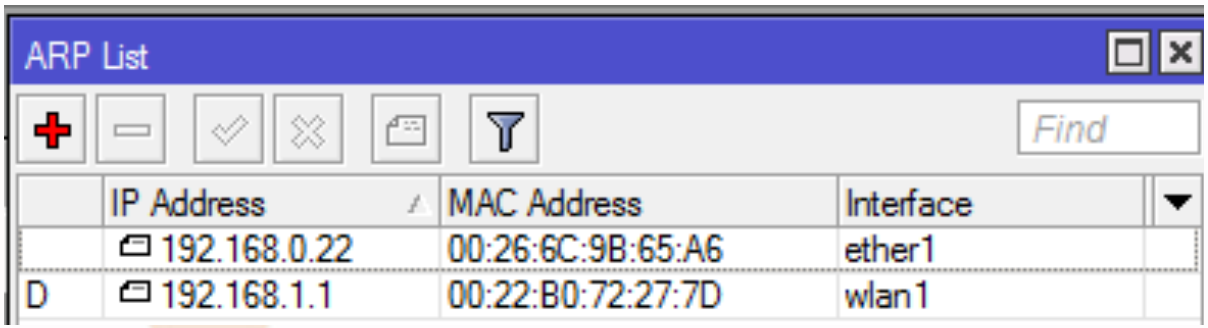
- Koneksikan Laptop dengan salah satu interface.
- Set interface reply-only dan coba ping, dari laptop ke router.



LAB- ARP Mode

ARP Reply-Only

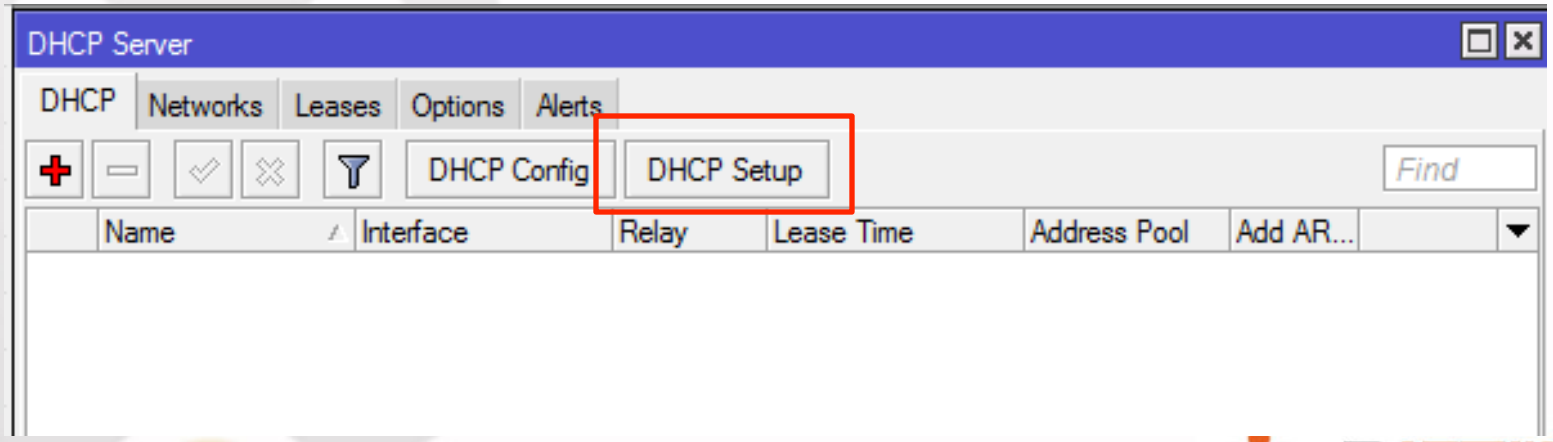
- Tambahkan kombinasi IP dan ARP dari laptop pada menu IP>ARP



- Coba ping kembali ip router dari laptop.
- Gunakan laptop peserta lain, isikan IP yang sama dengan IP laptop anda sebelumnya.
- Coba ping kembali

LAB - DHCP Server

- DHCP server dapat dijalankan pada masing-masing interface di router.
- Untuk memudahkan seting DHCP server, sebelumnya add IP address untuk interface yang akan menjalankan DHCP server.
- Setting DHCP server pada menu IP>DHCP Server>DHCP Setup



CONTACT

rofiq.fauzi@gmail.com

Skype : rofiq.fauzi

+6281-565-83-545

www.id-networkers.com

www.training-mikrotik.com

ID NETWORKERS
Expert Trainer & Consultant