Mikrotik Training Basic

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

Jadwal Training

	Session 1	Session 2	Session 3	Session 4
Hari 1	Introduction Pre-Test	TCP/IP Instalation	Basic Configuration	
Hari 2	Bridge	Wireless		Routing
Hari 3	Firewall		QOS	
Hari 4	Hotspot		VPN	Test

Jadwal Harian

Sessi 1	08.30 – 10.00
Coffee Break	10.00 – 10.30
Sessi 2	10.30 - 12.00
Lunch	12.00 – 13.00
Sessi 3	13.00 – 14.30
Coffee Break	14.30 – 15.00
Sessi 4	15.00 - 17.00

New Training Scheme 2010

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

Certification Test

- Diadakan oleh **Mikrotik.com** secara online
- Dilakukan pada sessi terakhir
- Jumlah soal : **25** Waktu: **60 menit**
- Nilai minimal kelulusan : **60%**, Trainer : **75%**
- Yang mendapatkan nilai **50%** hingga **59%** berkesempatan mengambil "***second chance***"
- Yang lulus akan mendapatkan sertifikat yang diakui secara internasional

Introduction to Mikrotik

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

Citraweb Nusa Infomedia

- Using Mikrotik since 2001, as Wireless ISP (Citra-Net)
- Mikrotik OEM Authorized Reseller (2002)
  http://www.mikrotik.com/1howtobuy.html
- One engineer:
  Mikrotik Certified Consultant (2005)
  http://www.mikrotik.com/consultants.html
- Mikrotik Certified Training Partner (2005)
  http://www.mikrotik.com/training.php

Citraweb Nusa Infomedia

- Head Office
  - Jalan Petung 31 Papringan
    Yogyakarta 55281
    Telp: 0274-554444
    Fax: 0274-553055
- Rep. Office
  - Gd Cyber Lt 11
    Jl Kuningan Barat 8 Jakarta 12710
    Telp: 021-5209612
    Fax: 021-5209614

What Is Mikrotik?

- Software Router untuk PC (x86, AMD, dll) → **RouterOS**
  - Menjadikan PC biasa memiliki fungsi router yang lengkap
  - Diinstall sebagai Operating System, tidak membutuhkan operating system lainnya
- Hardware untuk jaringan (terutama wireless)→ **RouterBoard**
  - Wireless board
    contoh: RB400, RB600, RB750, RB1000
  - Wireless interface (R52, R52H, R5H, R52N, R2N)
  - menggunakan RouterOS sebagai software

What Is Mikrotik?

- Mikrotik adalah kependekan dari “**mikrotikls**”
- Artinya: “network kecil” dalam bahasa Latvia

Routerboard for Wireless

Jenis	Processor	RAM	Ether	MiniPCI	USB	Radio	Lisensi
RB800	MPC8544 800MHz	256MB	3 (gig)	4	-	-	6
RB435G	AR71xx 680MHz	256MB	3 (gig)	5	2	-	5
RB433UAH	AR71xx 680MHz	128MB	3	3	2	-	5
RB433/ **AH**	AR71xx 300/**680MHz**	64MB/**128MB**	3	3	-	-	4 / **5**
RB411UAHR	AR71xx 680 MHz	64MB	1	1	1	1	4
RB411AH	AR71xx 680 MHz	64MB	1	1	-	-	4
RB411U/ **AR**	AR71xx 300 MHz	32MB/**64MB**	1	1	1 / **-**	- / **1**	4
GrooveA-5Hn	AR72xx 400MHz	64MB	1	-	-	1	4
RB711A-5nH	AR72xx 400MHz	64MB	1	-	-	1	4
Groove-5Hn	AR72xx 400MHz	32MB	1	-	-	1	3
RB711-5nH	AR72xx 400MHz	32M	1	-	-	1	3

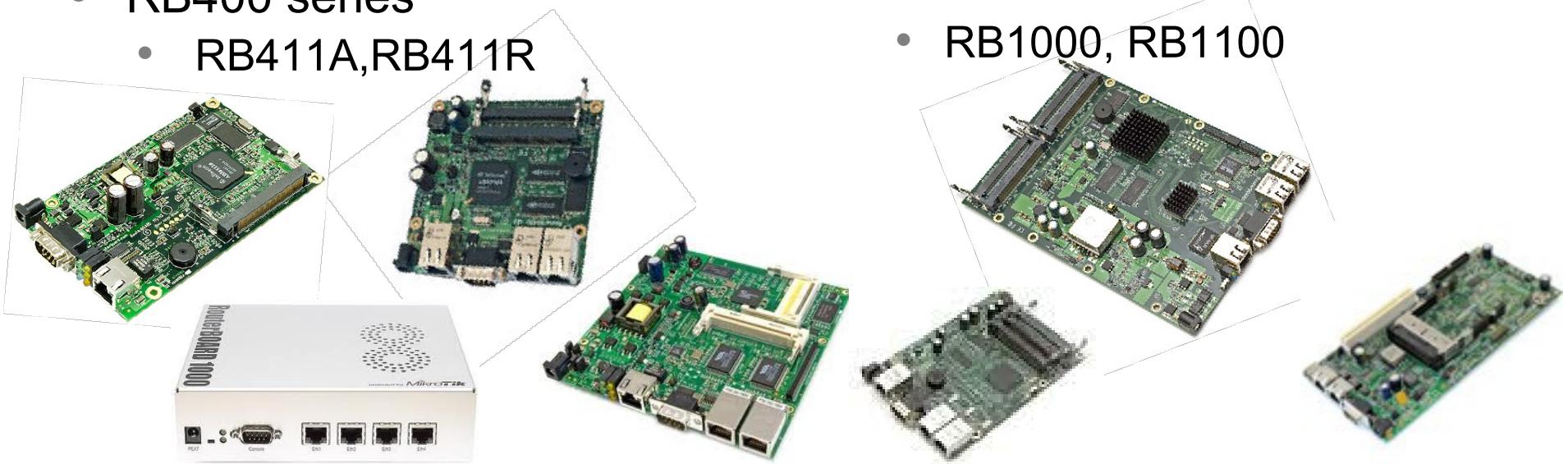
- For Client or Point to Point Connection

Routerboard for Indoor Router

Jenis	Processor	RAM	Ethernet	MiniPCI	Lisensi
RB1100**AH X2**	PPC **1Ghz dual Core**	**2GB**	13 (gigabit)	0	6
RB1100**AH**	PPC **1Ghz**	**2GB**	13 (gigabit)	0	6
RB1200	PPC 1Ghz	512MB	10 (gigabit)	0	6
RB493G	AR71xx 680 MHz	256MB	9 (gigabit)	3	5
RB493 / **AH**	AR71xx 300 / **680 MHz**	64MB / **128MB**	9	3	4 / **5**
RB450G	AR71xx 680 MHz	256MB	5 (gigabit)	0	5
RB450	AR71xx 300 MHz	32MB	5	0	5
RB750	AR72xx 400MHz	32MB	5	0	4
RB750GL	AR72xx 400MHz	64MB	5 (gigabit)	0	4

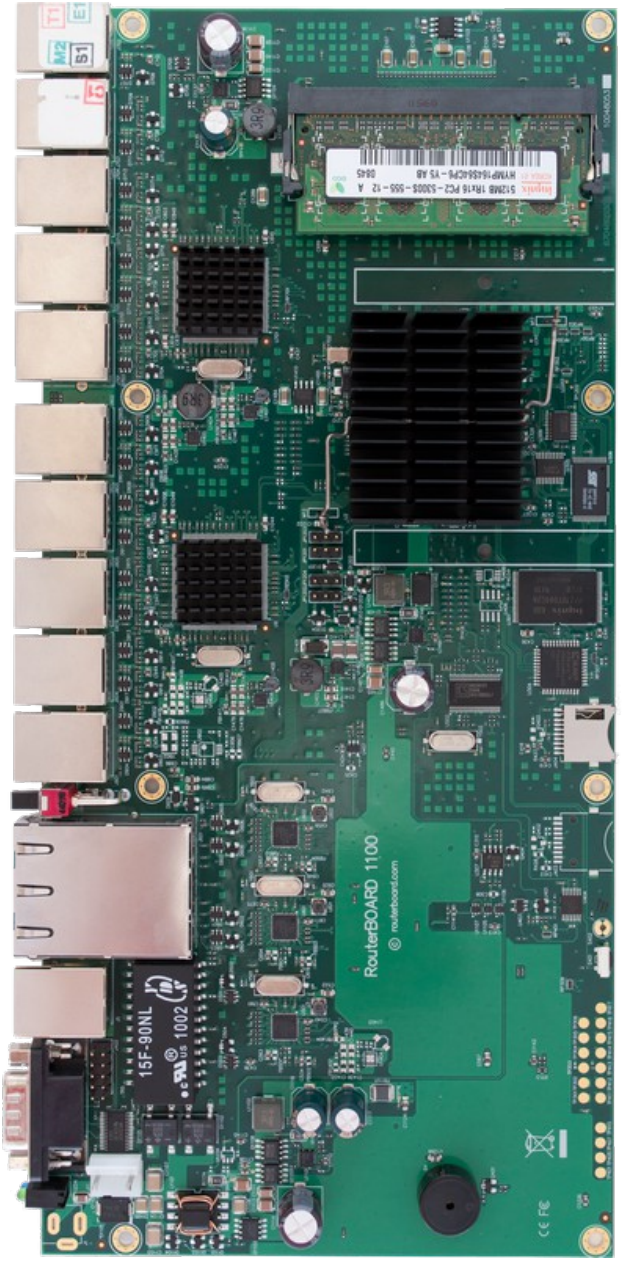
Discontinued Hardware

- RB100 series
  - RB112,RB133,RB133C
  - RB153,RB150,RB192
- RB200 series
  - RB230
- RB300series
  - RB333
- RB400 series
  - RB411A,RB411R
- RB500 series
  - RB532,RB511
- RB600 series
  - RB600
- RB700 series
  - RB750G
- RB1000 series
  - RB1000, RB1100

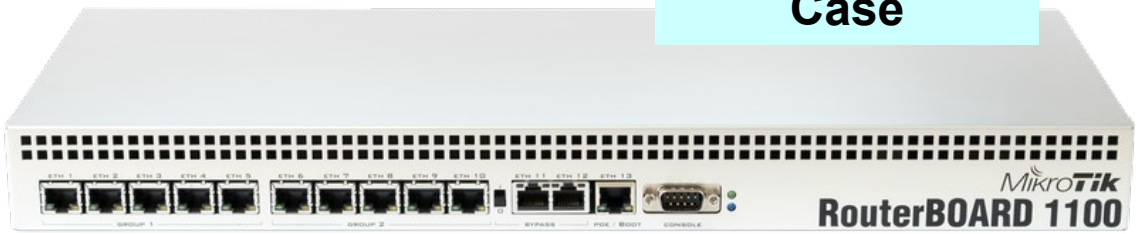


RB1100**AH / X2**

- **13 Port** Gigabit ethernet
- **1GHz** Network Processor / Dual Core
- RAM: **2GB**
- up to:
  - 2 Gbps
  - 250.000 pps / 1M pps
- **1U** rackmount
- Bypass Function



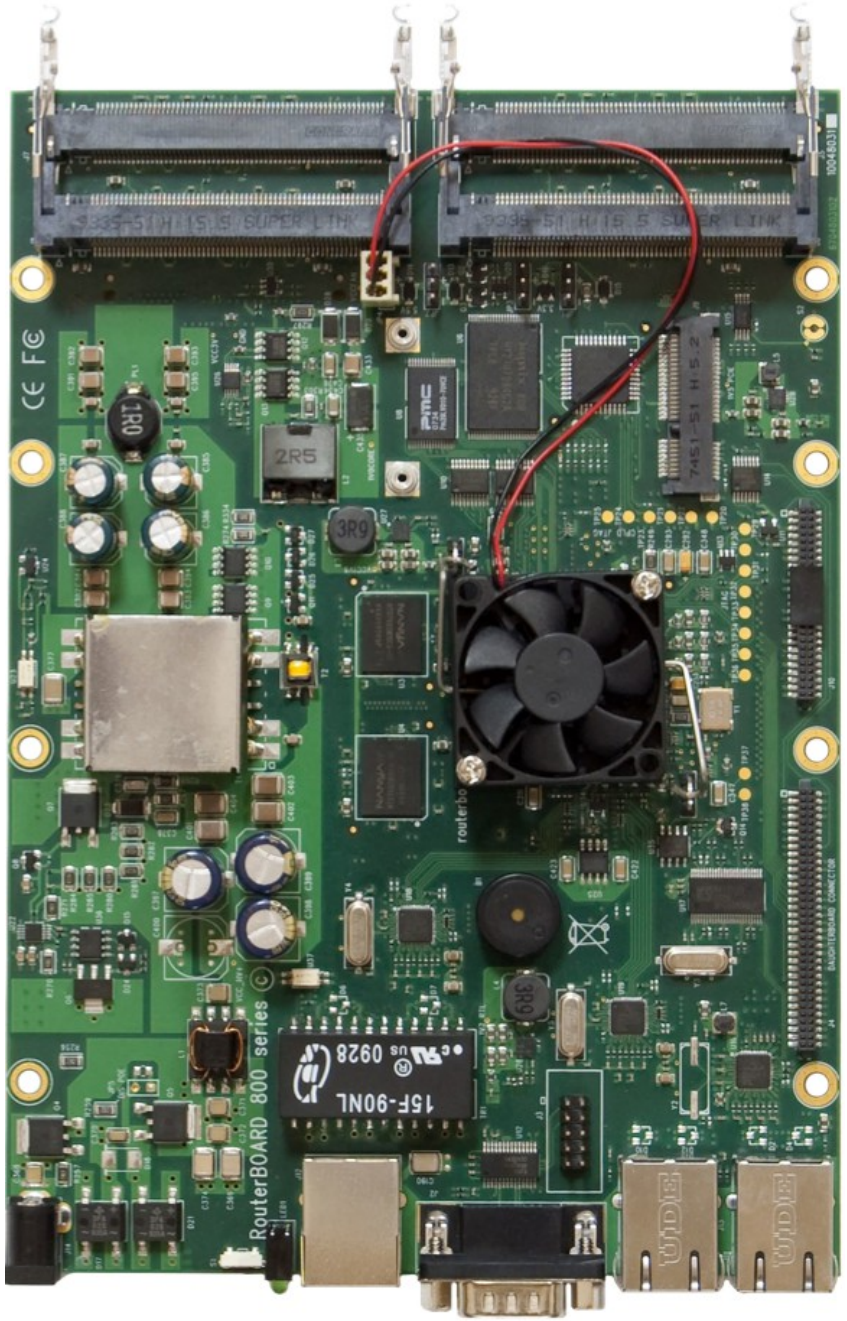
RackMount Case



RB800

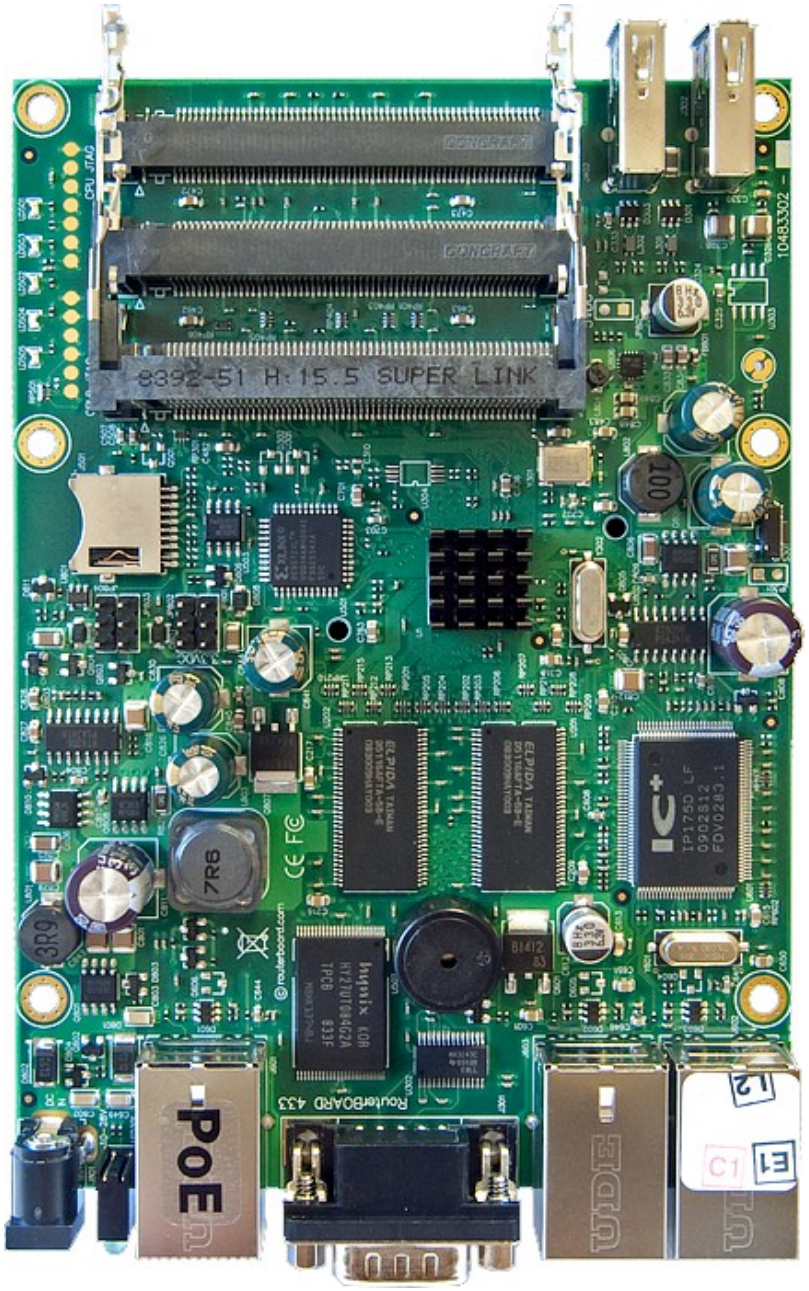
- 3 Gigabit Ethernet
- 4 Minipci Slot
- DoughterBoard Expandable
- CF slot
- MPC8544 800MHz CPU
- 256 DDR SDRAM

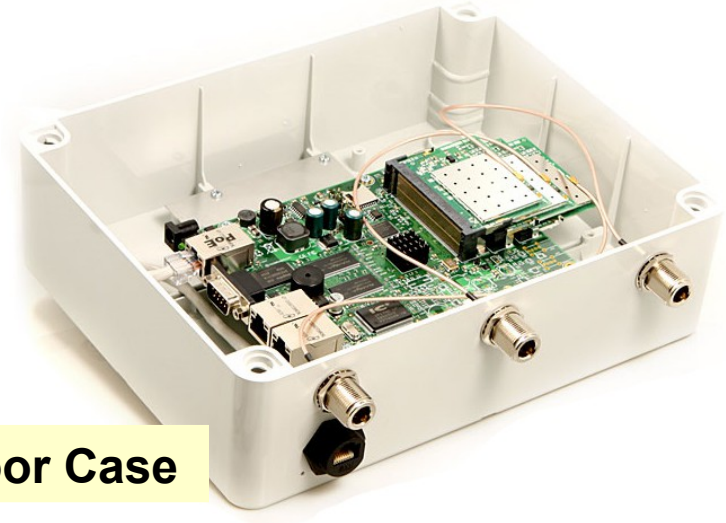
Doughter Board



RB433UAH

- 3 Ethernet, 3 Minipci
- Atheros AR7161 680MHz
- RAM: 128MB
- With micro-SD slot
- RouterOS Level 5
- 2 port USB

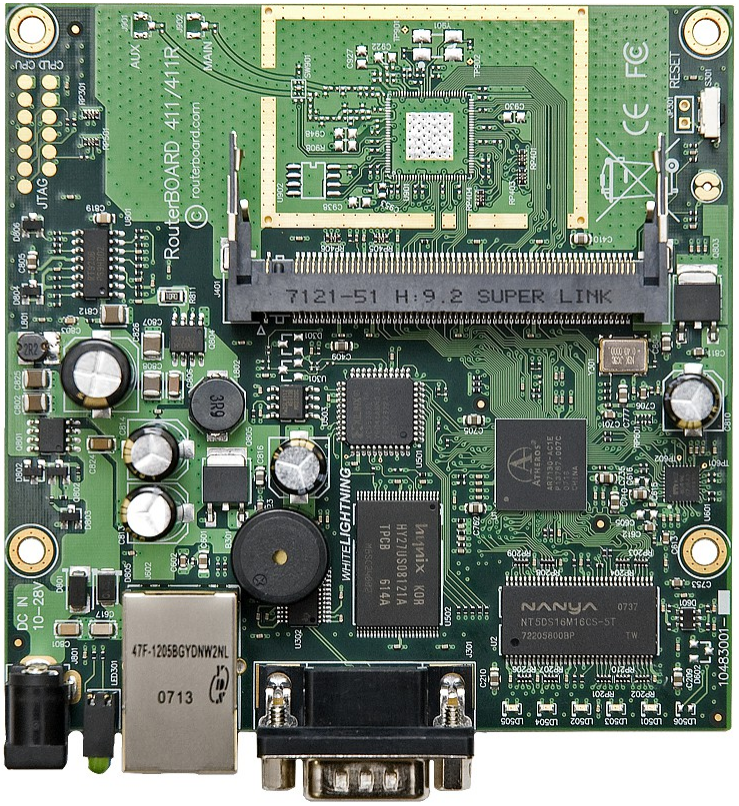




OutDoor Case

RB411 / U / AR / AH / UAHR

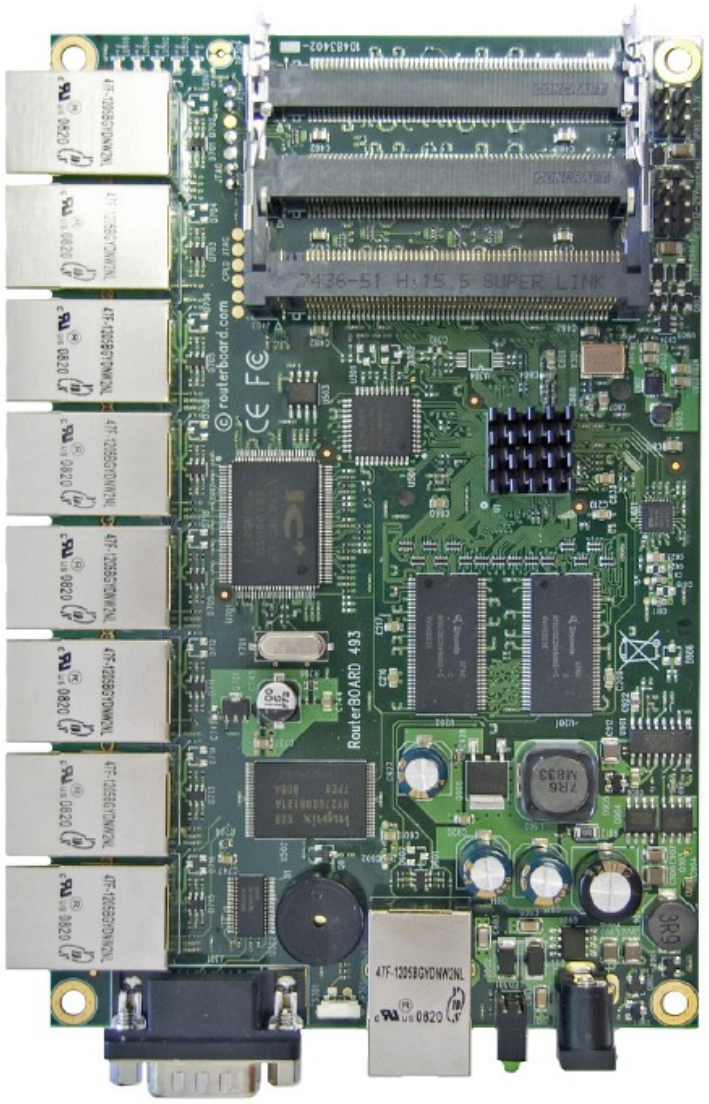
- CPU: Atheros
  - AR7130 300MHz (411/U/AR)
  - AR7161 680 MHz (411AH/UAHR)
- Memory:
  - 32 MB (411/U)
  - 64MB (411AR/UAHR/AH)
- Wireless Embedded (411AR/UAHR)
- 1 ethernet
- 1 MiniPCI (411/U/AR/AH/UAHR)
- Lisensi RouterOS:
  - Level 3 (411)
  - Level 4 (411U/AR/AH/UAHR)



RB493/AH/G

- 9 ethernet (gigabit di 493G)
- 3 Minipci Slot
- Processor :
  - Atheros AR7161 680MHz (493AH & G)
  - Atheros AR7130 300MHz (493)
- RAM: 64MB
- RouterOS:
  - Level 4 (RB493)
  - Level 5 (RB493AH & G)

Switch Mode



Embeded Solution

- Embedded Antenna 2,4GHz & 5GHz
- With Routerboard 411 series / 711 Series

RB450 / G

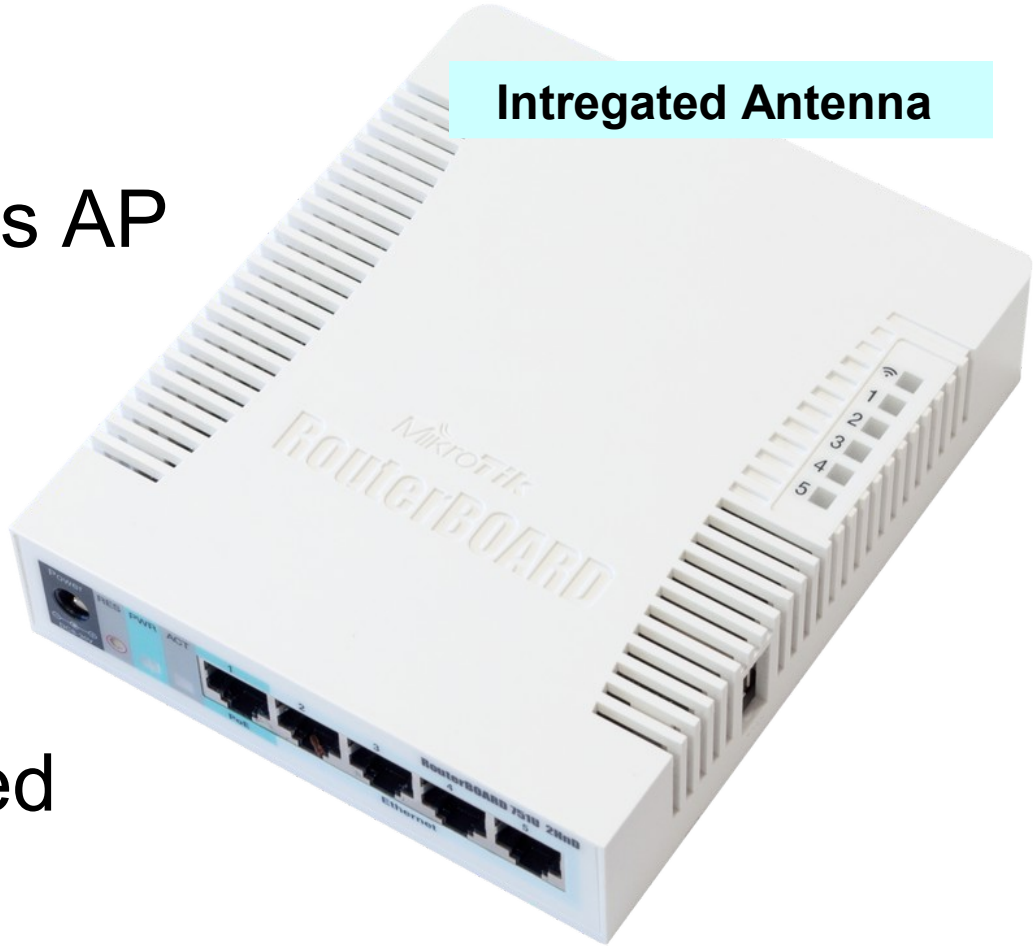
- 5 port Ethernet / gigabit
- Tanpa minipci port
- Processor : Atheros 300MHz / 680 MHz
- RAM: 64 / 256 MB
- RouterOS Level 5

RB750 / GL

- Produk routerboard terhemat dan terkecil
- Processor : AR7240 400Mhz
- 5 ethernet port (750)
  5 gigabit port (750GL)
- Lisensi Level 4

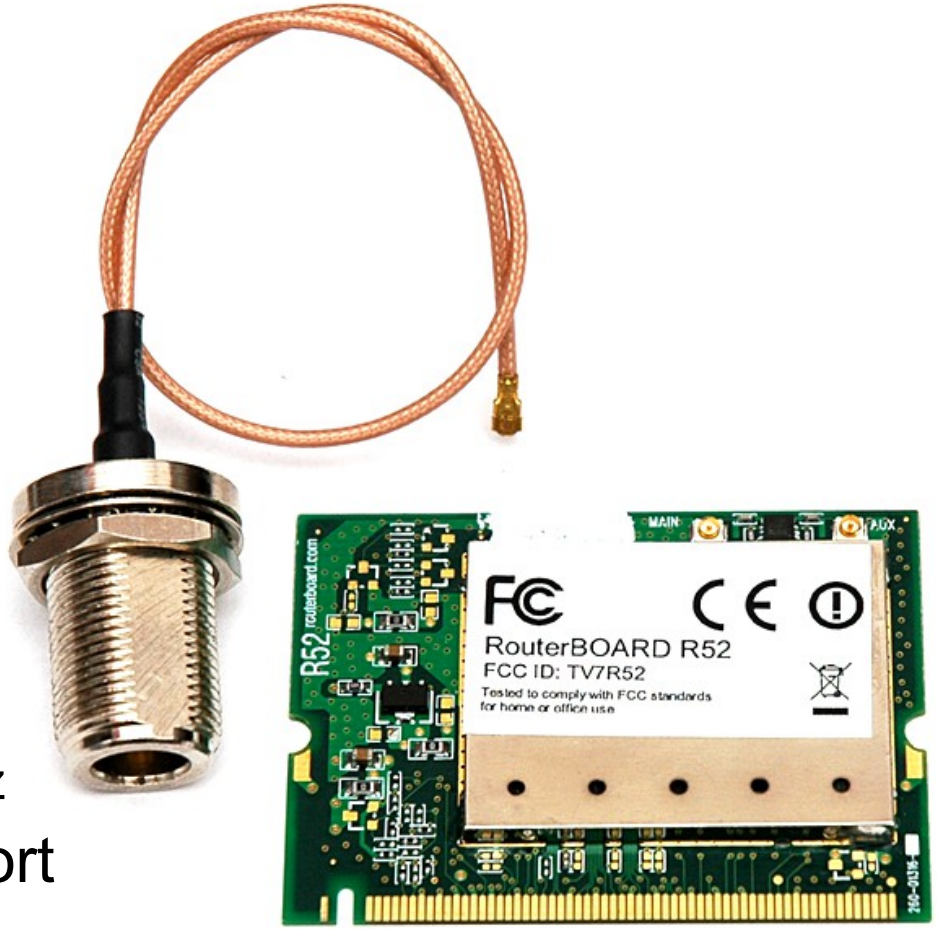
RB751U-2HND

- High power 1W 802.11b/g/n wireless AP
- 5 Port Ethernet
- 1 Port USB
  - For Modem
  - For Flashdisk
- 2x2 MIMO Integrated Antenna



Wireless Interface

- R52/**H (a/b/g)**
  - Atheros chipset
  - MiniPCI type interface
  - 65 mWatt / **350 mWatt**
  - 3 band wireless
    - 2.4 GHz, 5.2 GHz, 5.8 GHz
  - Custom Frequency Support
    - 2.1 – 2.5 GHz
    - 4.9 – 6.0 GHz



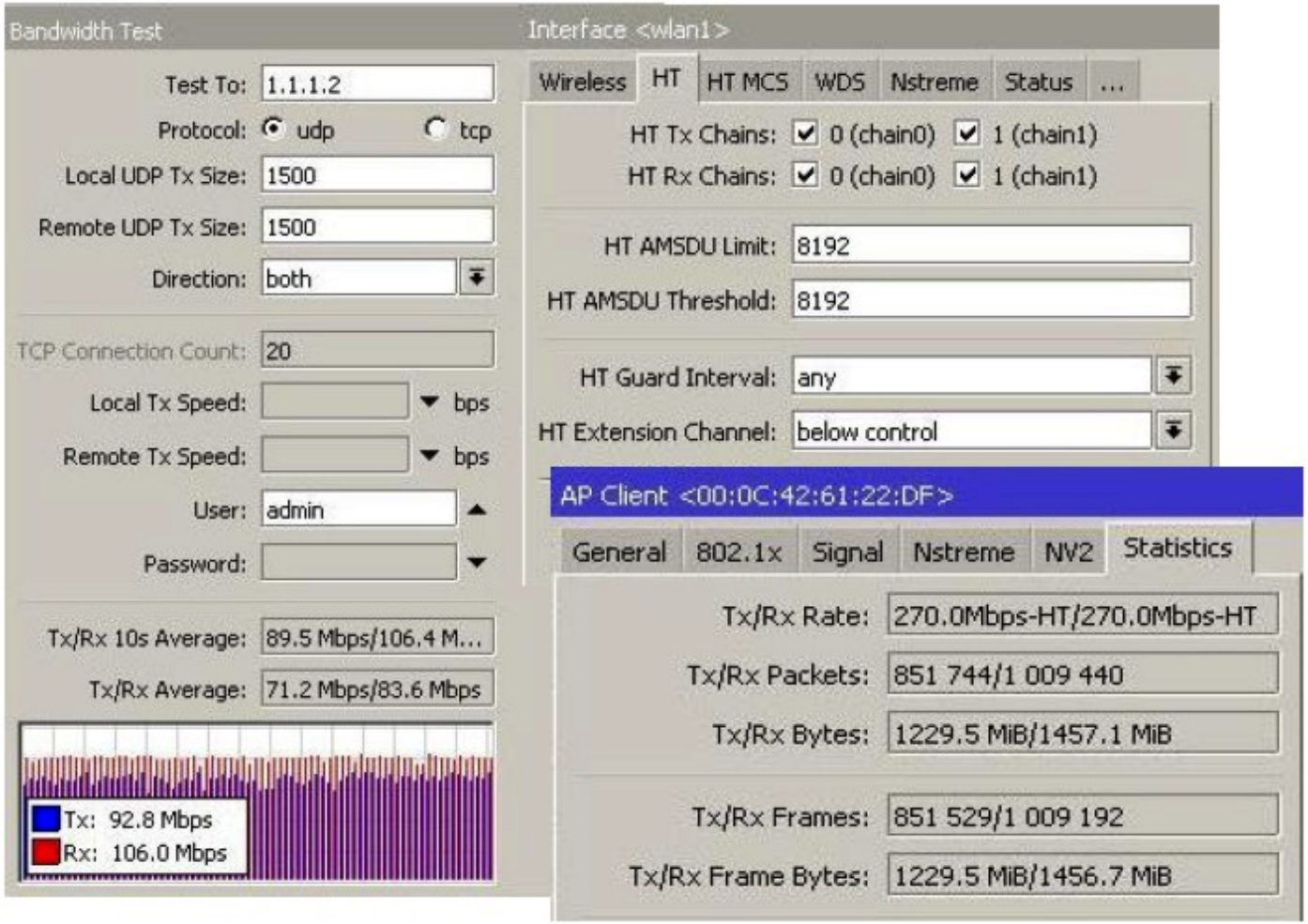
R52N (a/b/g/n)

NEW PRODUCT

- Dual band IEEE 802.11a/b/g/n standard
- Output Power of up to 25dBm @ b/g/n Band
- Support for up to 2x2 MIMO with spatial multiplexing
- Four times the throughput of 802.11a/g
- Atheros AR9220, chipset
- 2 X U.FL Antenna Connector
- Operating temperatures: 0ºC to 60ºC
- Power consumption MAX 2.4W
- Modulations: OFMD: BPSK, QPSK, 16 QAM, 64QAM DSSS: DBPSK, DQPSK, CCK

- High Performance (up to 300Mbps physical data rates and 200Mbps of actual user throughput) with Low Power Consumption
- ESD protection agaist +/-10kV ESD discharge on Antenna port

Wireless N - Performance



- Throughput: 195 ~ 200 Mbps

Mikrobits – Enterprise Router

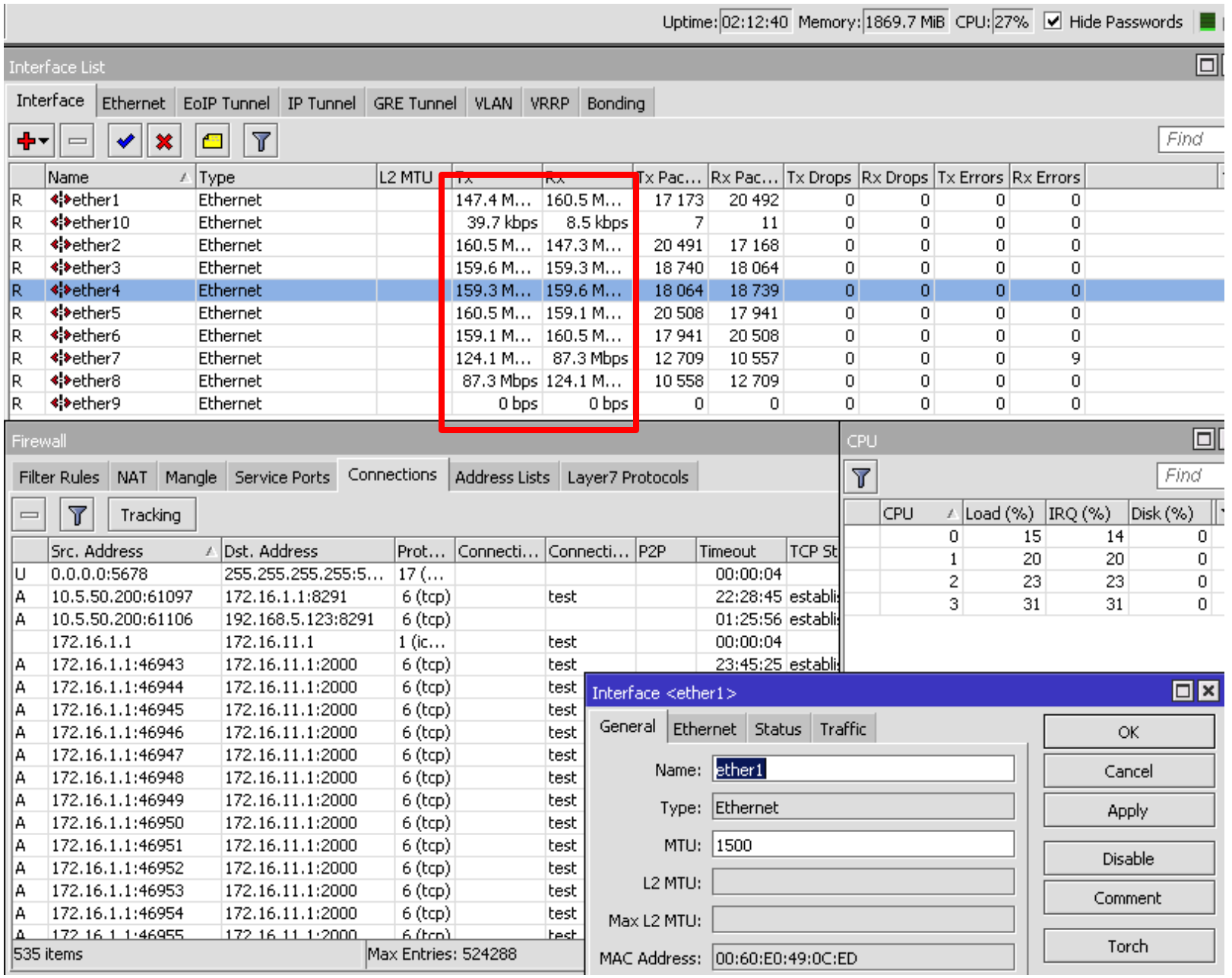
- **7** / **11** Intel gigabit ethernet
- **Multi Core Processor**
- 1U rackmount
- 2 GB RAM
  - Industrial grade

- Performance :
  - **2-4 Gbps** full duplex (**Ainos**)
  - **3-5 Gbps** full duplex (**Celoica**)
- 9000 jumbo frame supported

Mikrobits – Fiber Optic Router

- **16** Intel gigabit ethernet
- **Xeon Multi Core Processor**
- 1U rackmount
- 2 GB RAM
  - Industrial grade

- Performance :
  - **6-8 Gbps** full duplex
- 9000 jumbo frame supported
- **4** SFP or **8** SFP


Uptime: 02:12:40 Memory: 1869.7 MiB CPU: 27% Hide Passwords
Interface List
Interface Ethernet EoIP Tunnel IP Tunnel GRE Tunnel VLAN VRRP Bonding
Find
Name Type L2 MTU Tx Rx Tx Pac... Rx Pac... Tx Drops Rx Drops Tx Errors Rx Errors
R ether1 Ethernet 147.4 M... 160.5 M... 17 173 20 492 0 0 0 0
R ether10 Ethernet 39.7 kbps 8.5 kbps 7 11 0 0 0 0
R ether2 Ethernet 160.5 M... 147.3 M... 20 491 17 168 0 0 0 0
R ether3 Ethernet 159.6 M... 159.3 M... 18 740 18 064 0 0 0 0
R ether4 Ethernet 159.3 M... 159.6 M... 18 064 18 739 0 0 0 0
R ether5 Ethernet 160.5 M... 159.1 M... 20 508 17 941 0 0 0 0
R ether6 Ethernet 159.1 M... 160.5 M... 17 941 20 508 0 0 0 0
R ether7 Ethernet 124.1 M... 87.3 Mbps 12 709 10 557 0 0 0 9
R ether8 Ethernet 87.3 Mbps 124.1 M... 10 558 12 709 0 0 0 0
R ether9 Ethernet 0 bps 0 bps 0 0 0 0 0 0
Firewall
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols
Tracking
Src. Address Dst. Address Prot... Connecti... Connecti... P2P Timeout TCP St
U 0.0.0.0:5678 255.255.255.255:5... 17 (... 00:00:04
A 10.5.50.200:61097 172.16.1.1:8291 6 (tcp) test 22:28:45 establi
A 10.5.50.200:61106 192.168.5.123:8291 6 (tcp) 01:25:56 establi
172.16.1.1 172.16.11.1 1 (ic... test 00:00:04
A 172.16.1.1:46943 172.16.11.1:2000 6 (tcp) test 23:45:25 establi
A 172.16.1.1:46944 172.16.11.1:2000 6 (tcp) test
A 172.16.1.1:46945 172.16.11.1:2000 6 (tcp) test
A 172.16.1.1:46946 172.16.11.1:2000 6 (tcp) test
A 172.16.1.1:46947 172.16.11.1:2000 6 (tcp) test
A 172.16.1.1:46948 172.16.11.1:2000 6 (tcp) test
A 172.16.1.1:46949 172.16.11.1:2000 6 (tcp) test
A 172.16.1.1:46950 172.16.11.1:2000 6 (tcp) test
A 172.16.1.1:46951 172.16.11.1:2000 6 (tcp) test
A 172.16.1.1:46952 172.16.11.1:2000 6 (tcp) test
A 172.16.1.1:46953 172.16.11.1:2000 6 (tcp) test
A 172.16.1.1:46954 172.16.11.1:2000 6 (tcp) test
A 172.16.1.1:46955 172.16.11.1:2000 6 (tcp) test
535 items
Max Entries: 524288
CPU
Find
CPU Load (%) IRQ (%) Disk (%)
0 15 14 0
1 20 20 0
2 23 23 0
3 31 31 0
Interface <ether1>
General Ethernet Status Traffic
Name: ether1
Type: Ethernet
MTU: 1500
L2 MTU:
Max L2 MTU:
MAC Address: 00:60:E0:49:0C:ED
OK
Cancel
Apply
Disable
Comment
Torch

Mikrotik RouterOS

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

Fitur Mikrotik RouterOS (1)

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

Fitur Mikrotik RouterOS (2)

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

Licence Level

Level	3	4	5	6
Upgrade time	dalam 1 versi mayor dan versi berikutnya			
Wireless CPE/PTP	yes			
Wireless AP	no	yes		
Sync Interface	no	yes		
EoIP	1	unlimited		
PPPoE	1	200	500	unlimited
PPTP & L2TP	1	200	unlimited	
VLAN, Firewall, Queue	unlimited			
Proxy, Radius Client	yes			
Dynamic Routing	RB = yes	yes		
Hotspot Active User	1	200	500	unlimited
User Manager Active User	10	20	50	unlimited

- **Level 0** = **Trial 24 Jam** , **Level 1** = Hanya bisa **1 rule di semua fitur**

Produk Mana Yang Dipilih

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

Buyer's Guide

- 300 / 400 Mhz Processor (< **5Mbps** Traffic)
  - *RB450, RB750, RB433, RB493*
- 680 Mhz Processor (**5 ~ 20 Mbps** Traffic)
  - *RB450G, RB433AH, RB493G*
- 1Ghz Processor (**20 ~ 100 Mbps** Traffic)
  - *RB1200, RB1100AH*
- 1Ghz Dual Core Processor (**> 100 Mbps** Traffic)
  - *RB1100AHx2*
- Multi Core x86 Processor (**> 1 Gbps** Traffic)
  - *Mikrobits : Aneto, Ainos, Dinara*
- Xeon Processor (**> 10 Gbps** Traffic)
  - *Mikrobits : Dinara*

Quiz !

- Pada sebuah router mikrotik terdapat dua service yang aktif yaitu HOTSPOT server (150 user) dan PPTP server (120 user), maka Ruter Mikrotik tersbut membutuhkan license Level ?

- Pada Routerboard RB411UAHR **tidak** memerlukan wireless card miniPCI tambahan untuk menjadikan routerboard tersebut Access Point 5Ghz (Benar / Salah), Kenapa ?

- Kita bisa menambahkan storage pada Routerboard RB450G ? (Benar / Salah)

Mikrotik Installation

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

Installasi Mikrotik

- Media Installasi (Penyimpan) Mikrotik RouterOS
  - Harddisk
  - CF Disk
  - DOM (Disk On Module)
    - SATA DOM (coming soon on mikrotik.co.id)
  - USB Flash Disk
    - komputer harus bisa booting dari USB (setting BIOS)
  - Routerboard

Installation Method

- **CD**
  - Create CD from CD image (iso file)
  - For PC Router Fresh-Install
    - CD-Rom Required
- **Netinstall**
  - Via network using NetInstall program.
  - For PC Router (Fresh-Install / Re-Install)
    - PXE,EtherBoot Required
  - For Reinstall Routerboard

Download Area

Software Instalasi

CD Instalation

Jika Anda bermaksud menginstall Mikrotik di PC Anda, mungkin file inilah yang Anda butuhkan untuk membuat CD Boot instalasi. [panduan]

mikrotik-4.17.iso (19.16 MByte, didownload 8655 kali)

Mikrotik NetInstall

Software yang dibutuhkan untuk melakukan netinstall. Masih dibutuhkan juga modul all_packages di bawah. [panduan].

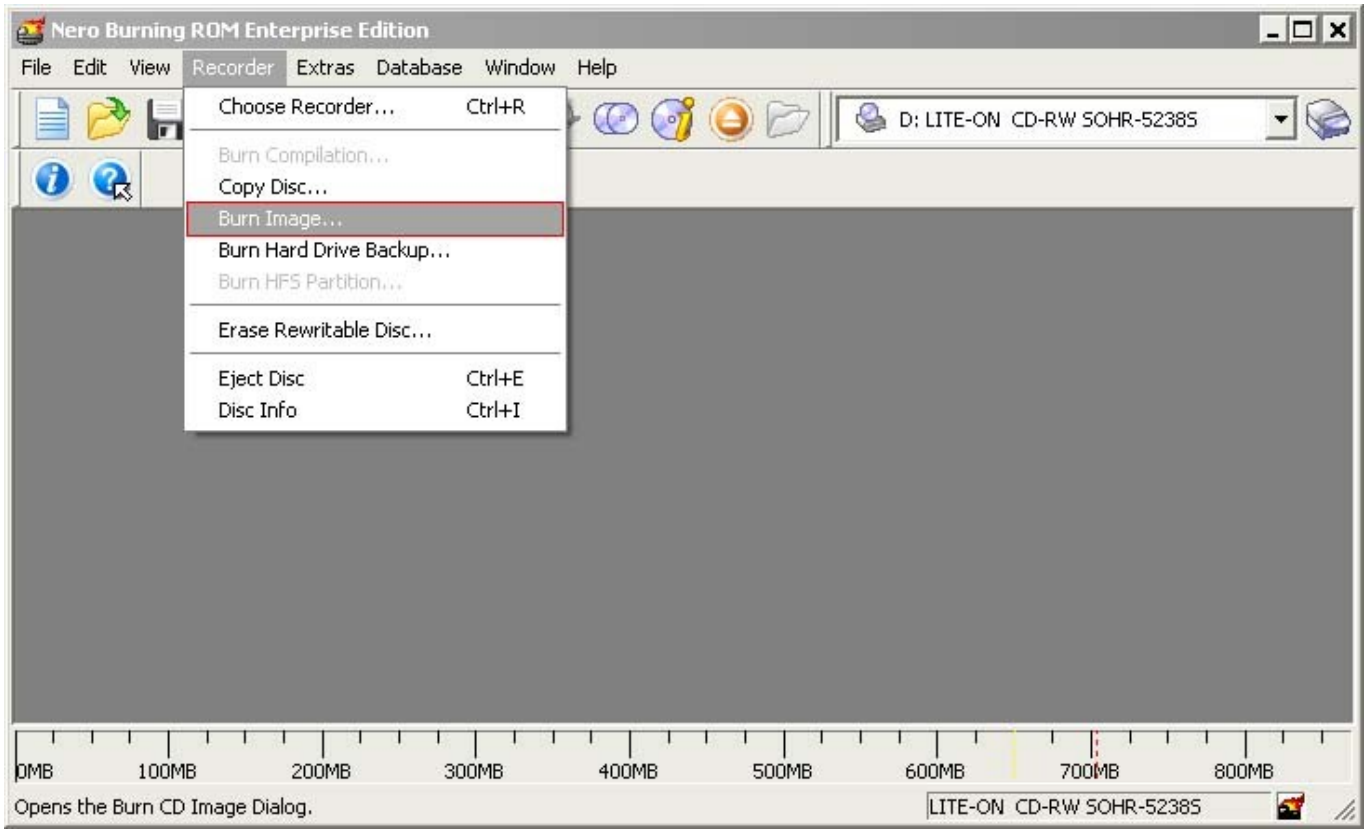
netinstall.zip (6.05 MByte, didownload 37519 kali)

netinstall-4.17.zip (11.11 MByte, didownload 3283 kali)

- **Mikrotik.co.id – Download Area**
  - Connected 1Gbps to OpenIXP.
- **Mikrotik.com – Download Area**

CD Installation (1)

- Download ISO file (mikrotik-***.iso) dan buatlah CD bootable dengan file tersebut.



CD Installation (2)

- Gunakanlah CD yang telah dibuat untuk melakukan booting pada komputer
- Pilihlah module yang ingin diinstall

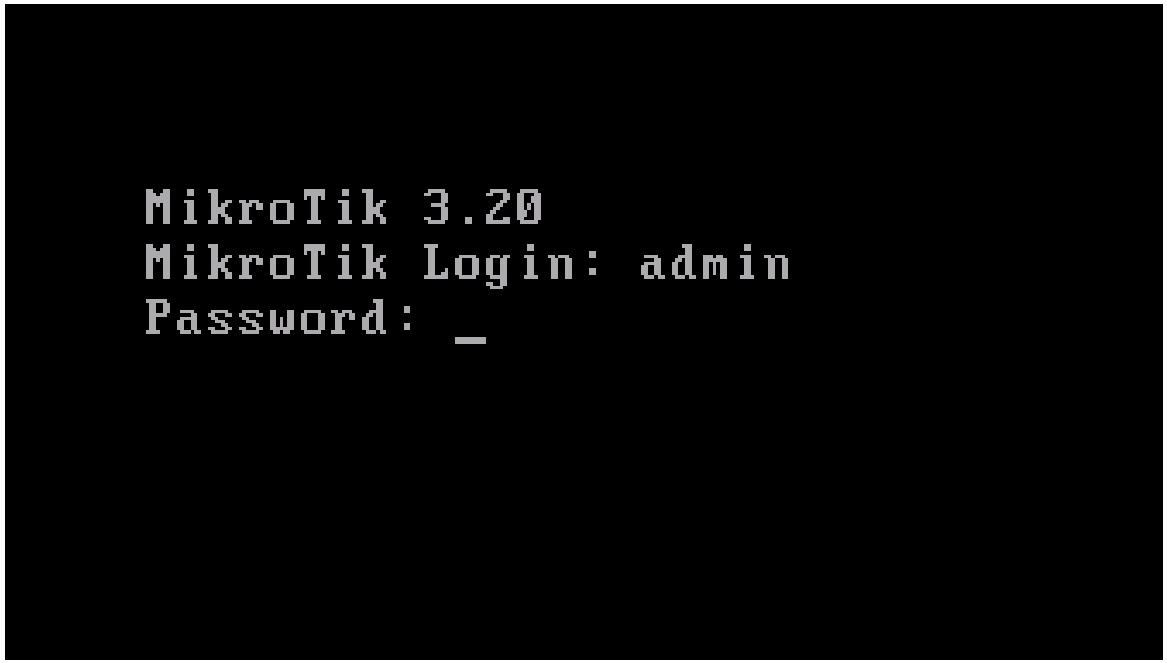
```
                Welcome to MikroTik Router Software installation

Move around menu using 'p' and 'n' or arrow keys, select with 'spacebar'.
Select all with 'a', minimum with 'm'. Press 'i' to install locally or 'r' to
install remote router or 'q' to cancel and reboot.

  [X] system              [ ] isdn              [ ] synchronous
  [X] ppp                 [ ] lcd               [ ] telephony
  [X] dhcp                [ ] ntp               [ ] ups
  [X] advanced-tools      [ ] radiolan          [ ] web-proxy
  [ ] arlan               [ ] routerboard       [ ] wireless
  [ ] gps                 [X] routing
  [ ] hotspot             [X] security
```

CD Installation (3)

- **Warning: all data on the disk will be erased! Continue? [y/n]**
  Choose Yes
- **Do you want to keep old configuration? [y/n]:**
  Yes/No
- **Creating partition...**
- **Formatting disk...**
- **Software installed.**
- **Press ENTER to reboot**

Installation Check

- Default Login User dan password
  - user = admin dan password = [kosong]
- Welcome menu



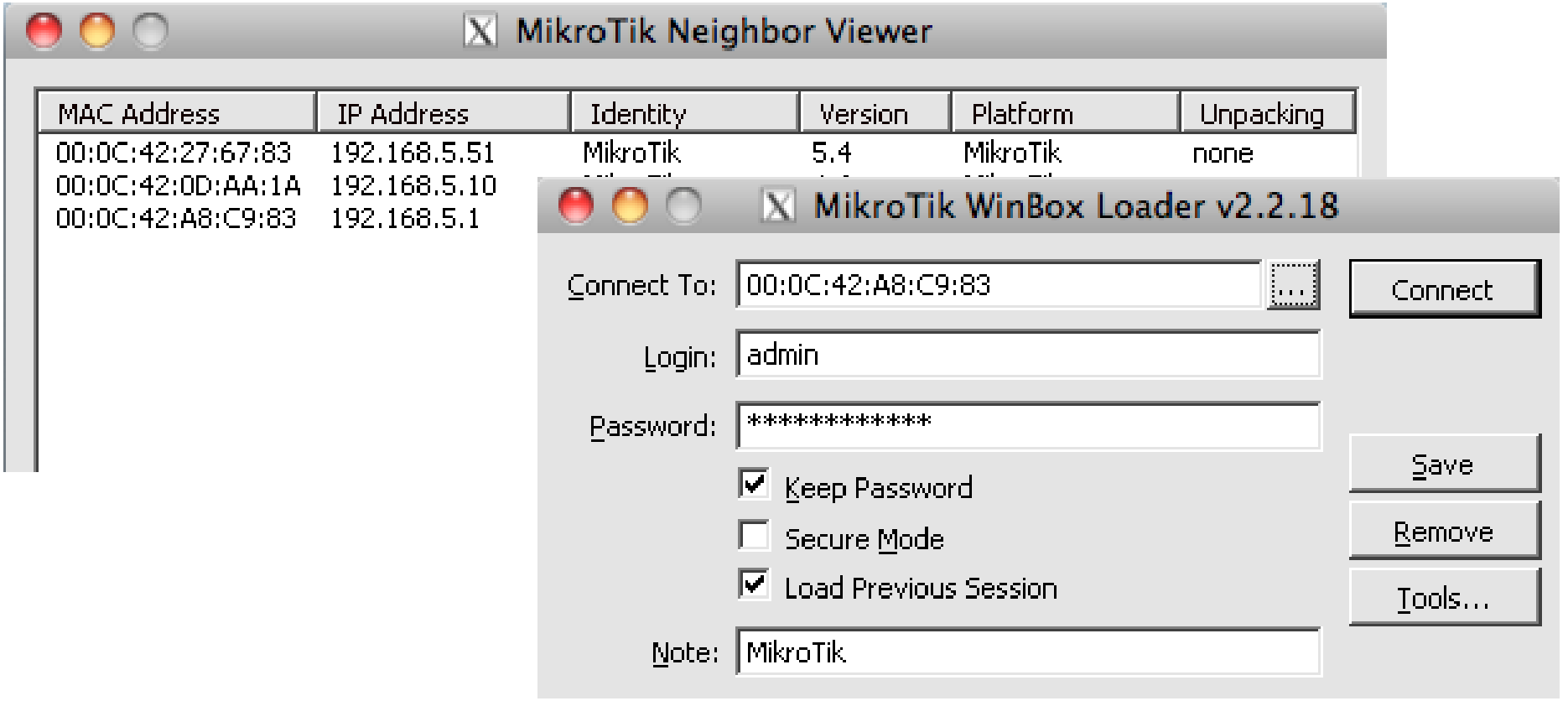
License Trial

- License level 0 = Trial time 24 jam

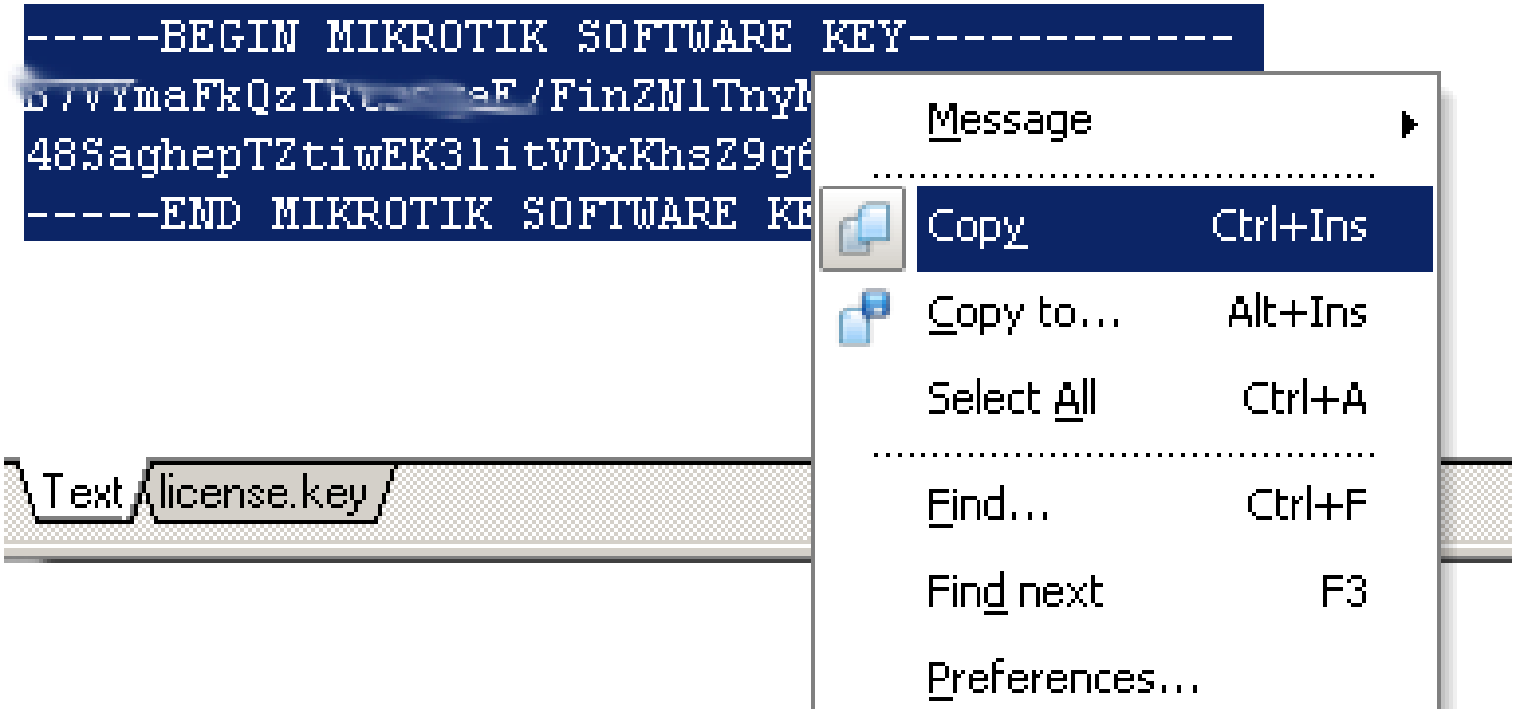
```
  MMM       MMM        KKK                          TTTTTTTTTTT      KKK
  MMMM     MMMM        KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM   III   KKK  KKK   RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM   III   KKKKK      RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM   III   KKK KKK    RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM   III   KKK  KKK   RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 3.20 (c) 1999-2009       http://www.mikrotik.com/


ROUTER HAS NO SOFTWARE KEY
--------------------------
You have 23h49m to configure the router to be remotely accessible,
and to enter the key by pasting it in a Telnet window or in Winbox.
See www.mikrotik.com/key for more details.

Current installation "software ID": FTGX-E1N
Please press "Enter" to continue!

[admin@MikroTik] > _
```

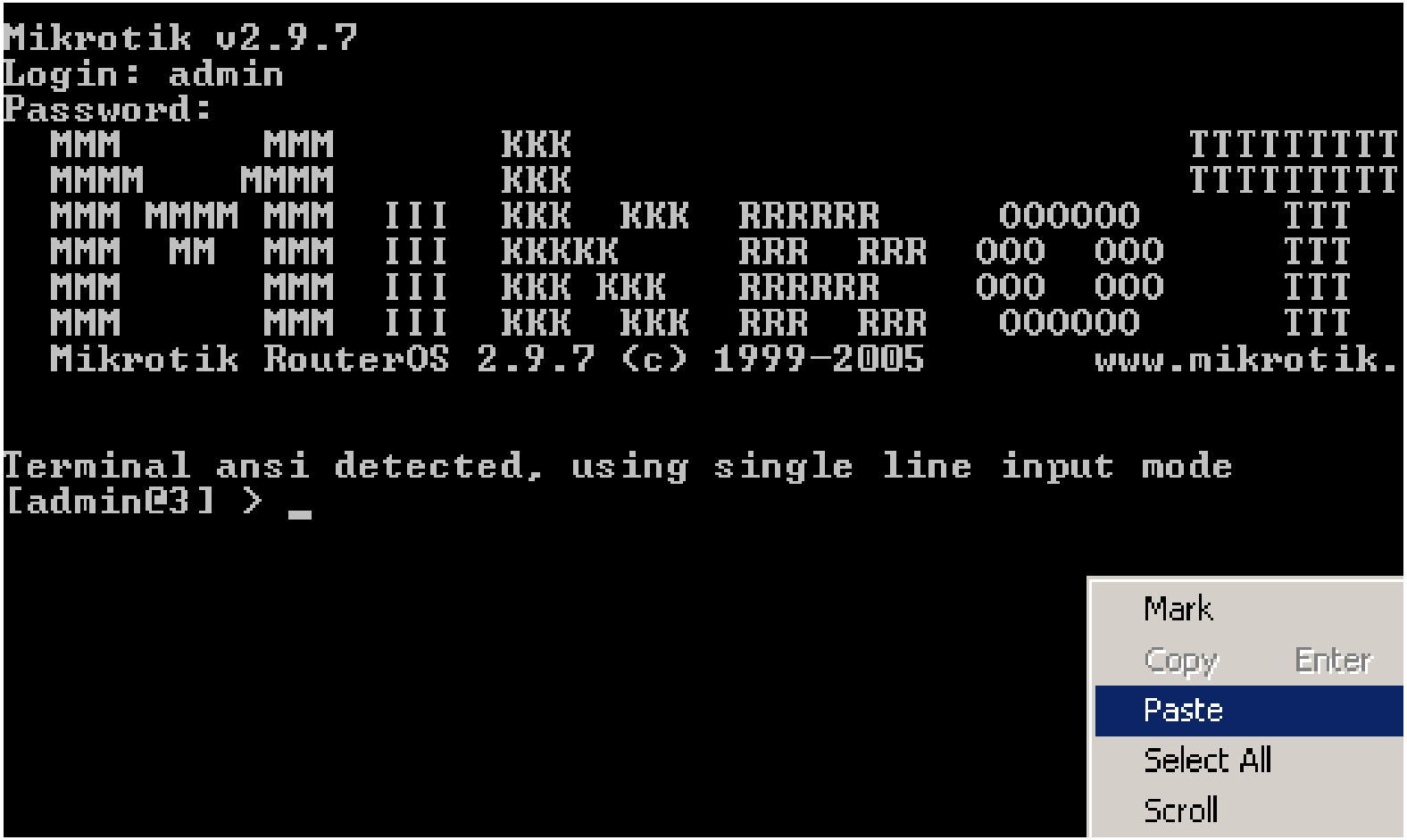
Access the Router (First Time)

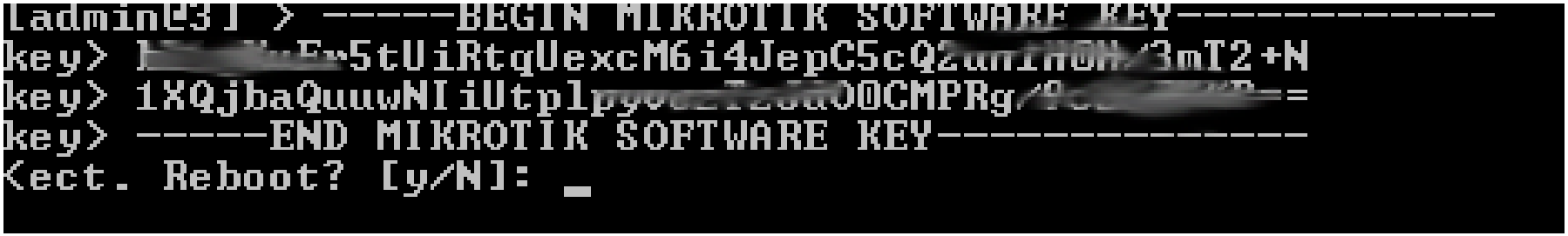
- **Direct Console** (Keyboard & Monitor)
- **MAC-Telnet** – NeighbourViewer.exe
- **MAC-Winbox** – winbox.exe



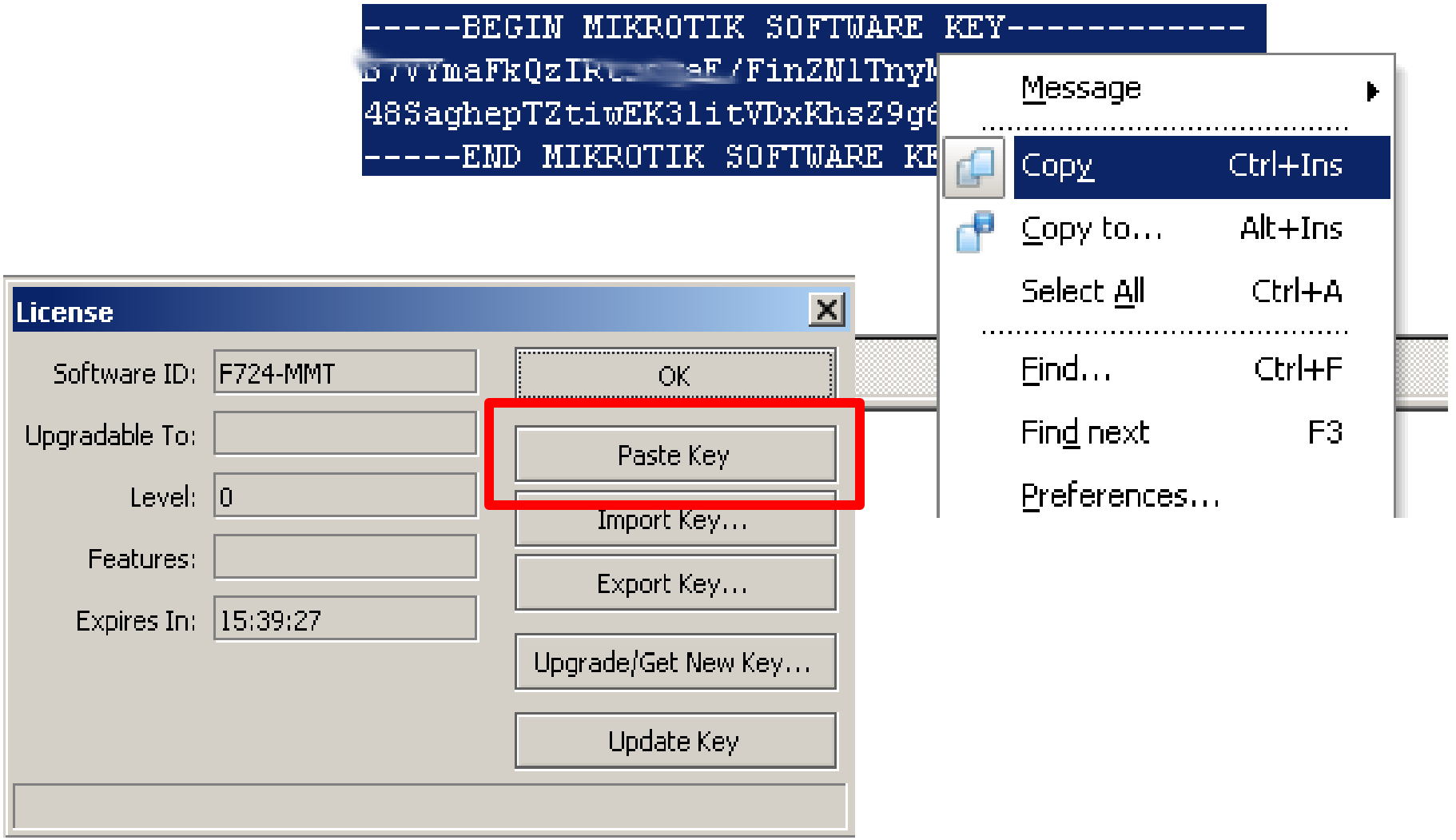
Input License (Telnet)



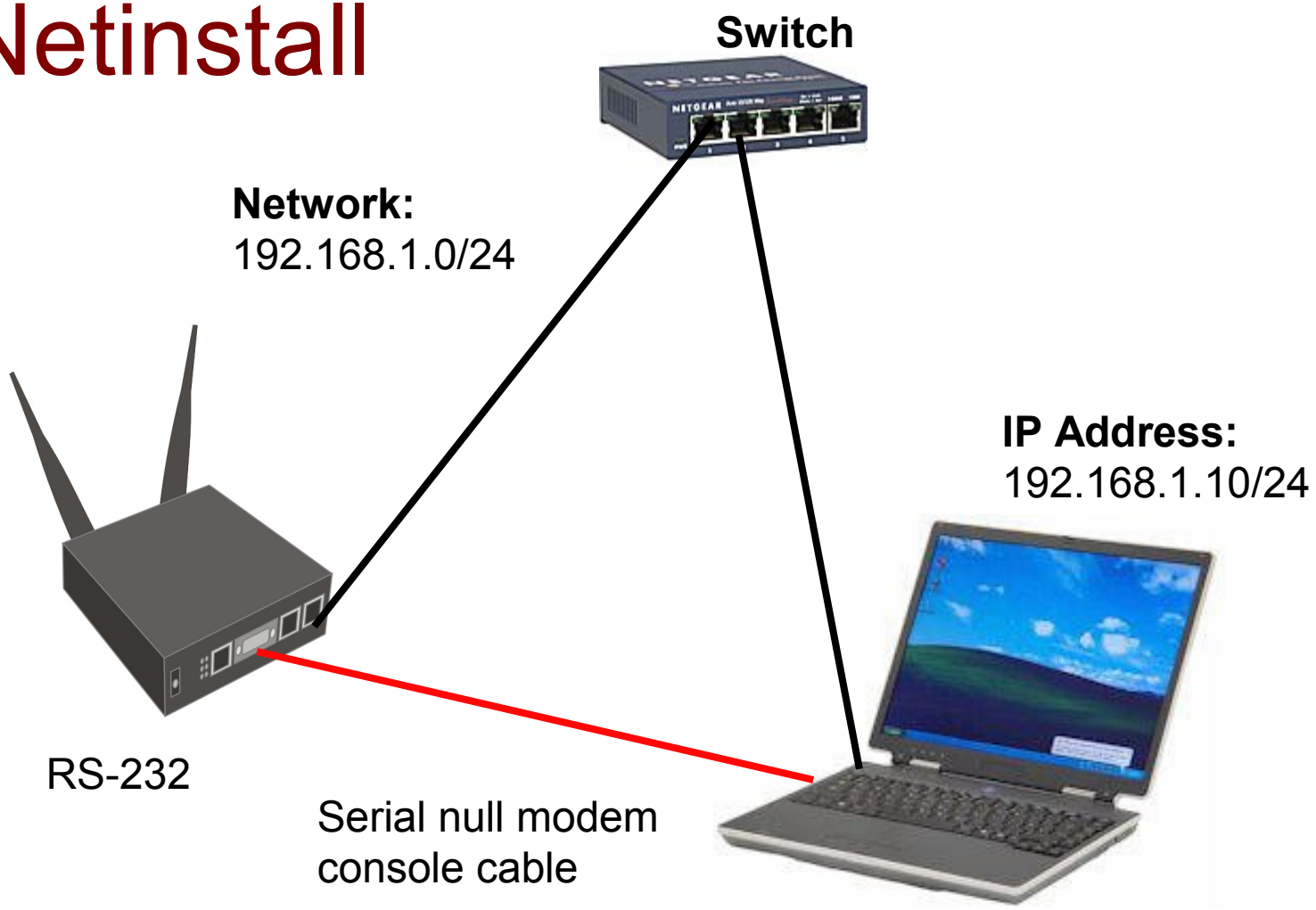

Mikrotik v2.9.7
Login: admin
Password:
MMM MMM KKK TTTTTTTTT
MMMM MMMM KKK TTTTTTTTT
MMM MMMM MMM III KKK KKK RRRRRR 000000 TTT
MMM MM MMM III KKKKK RRR RRR 000 000 TTT
MMM MMM III KKK KKK RRRRRR 000 000 TTT
MMM MMM III KKK KKK RRR RRR 000000 TTT
Mikrotik RouterOS 2.9.7 (c) 1999-2005 www.mikrotik.
Terminal ansi detected, using single line input mode
[admin@3] > _
Mark
Copy Enter
Paste
Select All
Scroll


[admin@3] > -----BEGIN MIKROTIK SOFTWARE KEY----------
key> [redacted]5tUiRtqUexcM6i4JepC5cQ2[redacted]3mT2+N
key> 1XQjbaQuuwNIiUtp1[redacted]OOCMPRg[redacted]=
key> -----END MIKROTIK SOFTWARE KEY----------
<ect. Reboot? [y/N]: _

Input License (Winbox)



Netinstall



- **Metode Netinstall biasa digunakan untuk melakukan install ulang RouterBoard / PC Router yang sudah support net-boot.**

Netinstall

- **Download program netinstall dan module yang dibutuhkan**

Mikrotik NetInstall

Software yang dibutuhkan untuk melakukan netinstall. Masih dibutuhkan juga modul all_packages di bawah. [panduan].

netinstall.zip (6.05 MByte, didownload 37519 kali)

netinstall-4.17.zip (11.11 MByte, didownload 3283 kali)

Software Upgrade

Semua modul dalam satu paket

Satu buah paket yang berisikan semua modul Mikrotik. Untuk penggunaan versi 2.9 atau yang lebih baru, gunakanlah paket ini. [panduan]

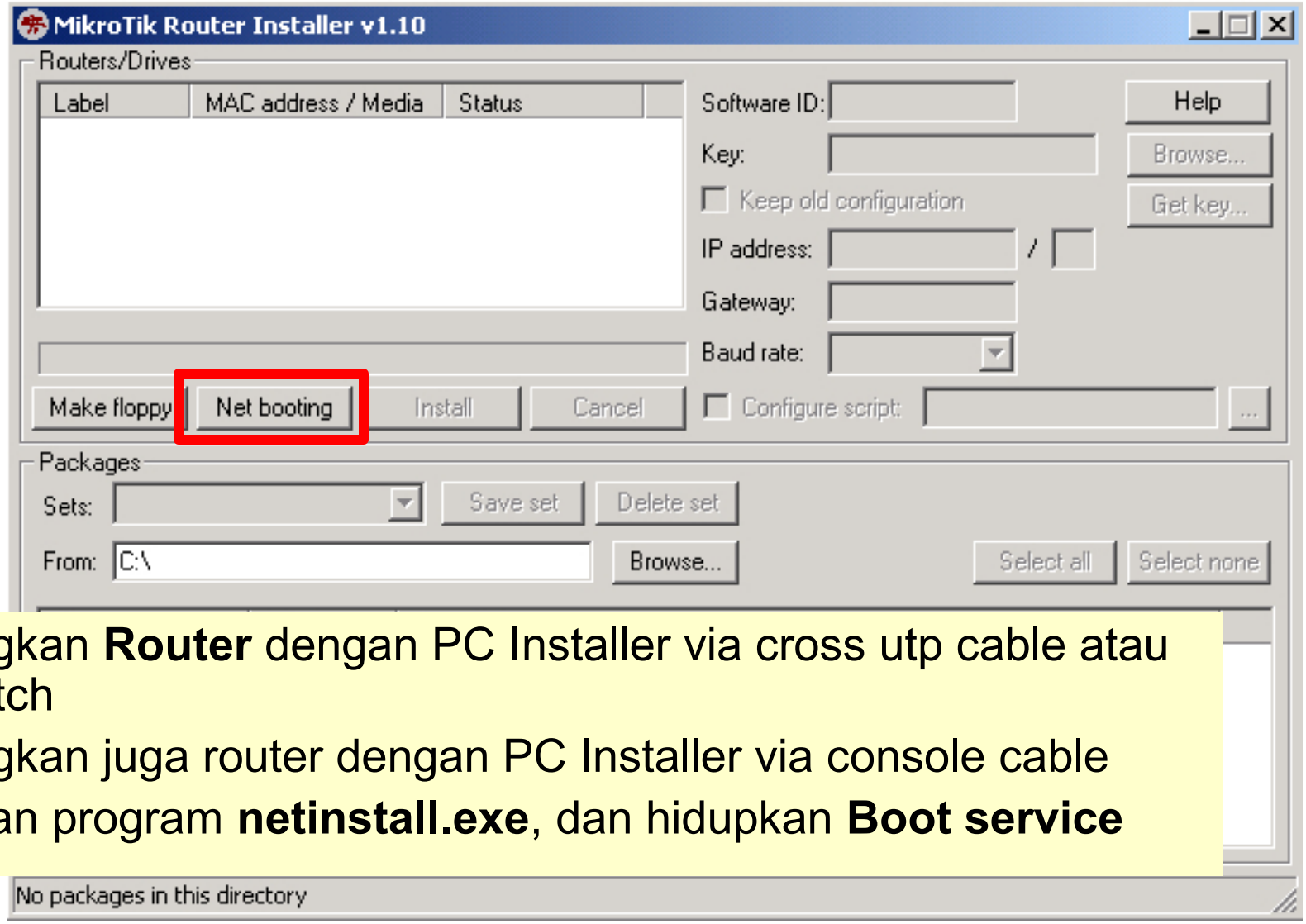
routeros-mipsbe-4.17.npk (12.21 MByte, didownload 4262 kali)

routeros-mipsle-4.17.npk (11.79 MByte, didownload 901 kali)

routeros-powerpc-4.17.npk (11.92 MByte, didownload 1040 kali)

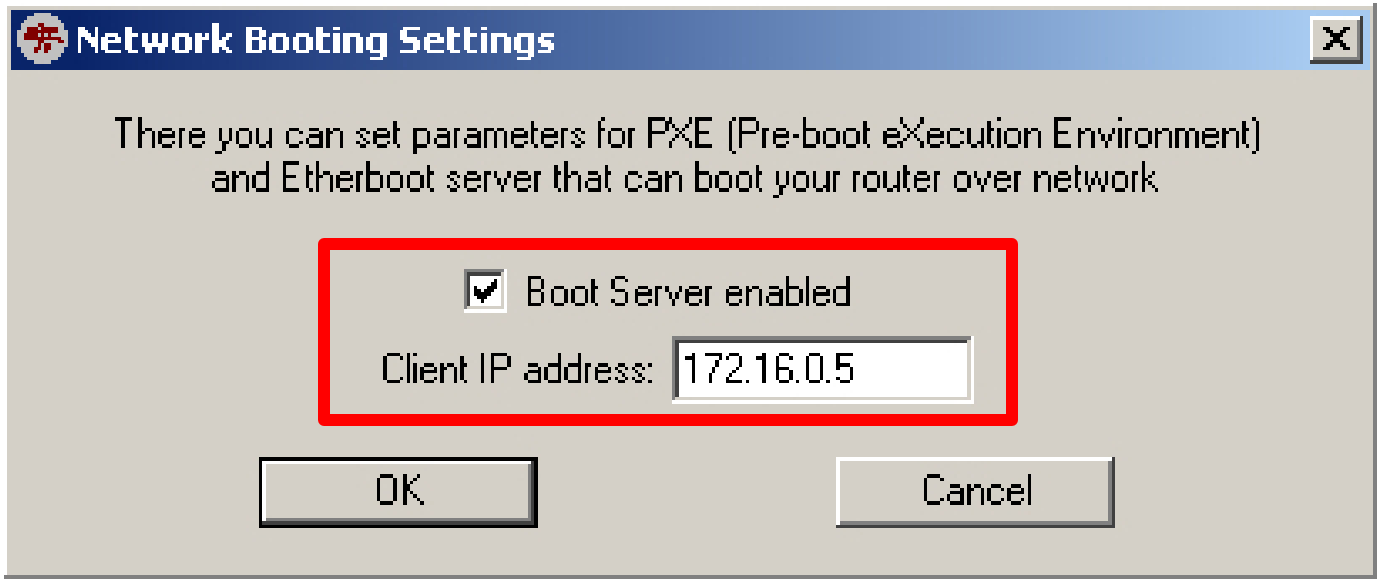
routeros-x86-4.17.npk (14.57 MByte, didownload 1576 kali)

Netinstall



- Hubungkan **Router** dengan PC Installer via cross utp cable atau via switch
- Hubungkan juga router dengan PC Installer via console cable
- Jalankan program **netinstall.exe**, dan hidupkan **Boot service**

Netinstall - Config



Masukkanlah **IP Address** yang berbeda dengan IP Address laptop / komputer Anda, namun berada dalam **subnet yang sama**

Netinstall – BIOS Setting

- **Hidupkan router, masuk ke setting BIOS**

```
RouterBOOT booter 2.12

RouterBoard 333

CPU frequency: 333 MHz
  Memory size:  64 MB

Press any key within 2 seconds to enter setup
```

Netinstall – BIOS Setting

```
RouterBOOT-2.12
What do you want to configure?
   d - boot delay
   k - boot key
   s - serial console
   o - boot device
   f - cpu frequency
   r - reset booter configuration
   g - upgrade firmware
   i - board info
   p - boot protocol
   t - do memory testing
   x - exit setup
your choice: o - boot device
```

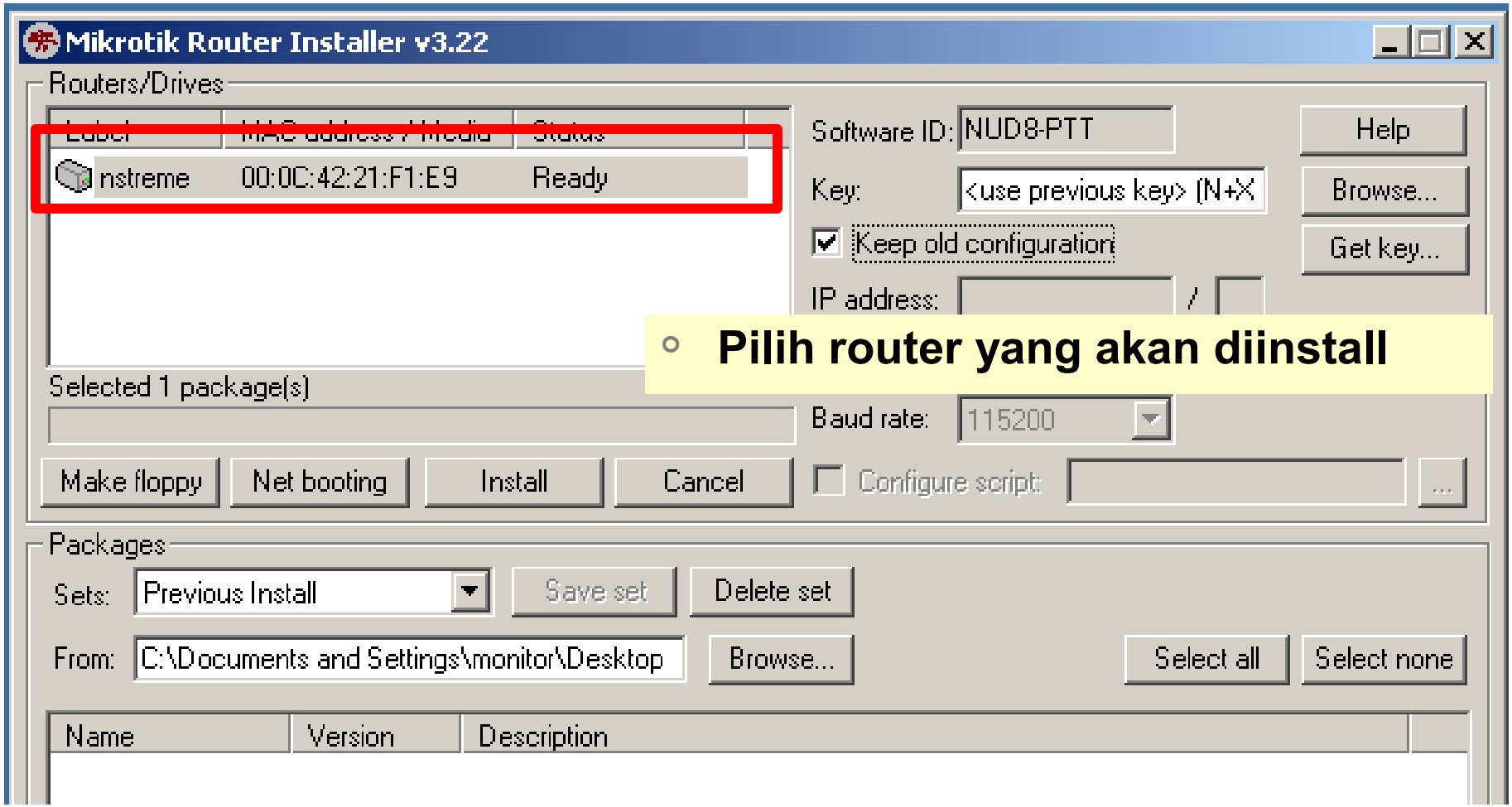
- **Konfigurasi booting pada BIOS (RouterBoot)**

Netinstall – BIOS Setting

```
Select boot device:
 * e - boot over Ethernet
   n - boot from NAND, if fail then Ethernet
   1 - boot Ethernet once, then NAND
   o - boot from NAND only
   b - boot chosen device
your choice:
```

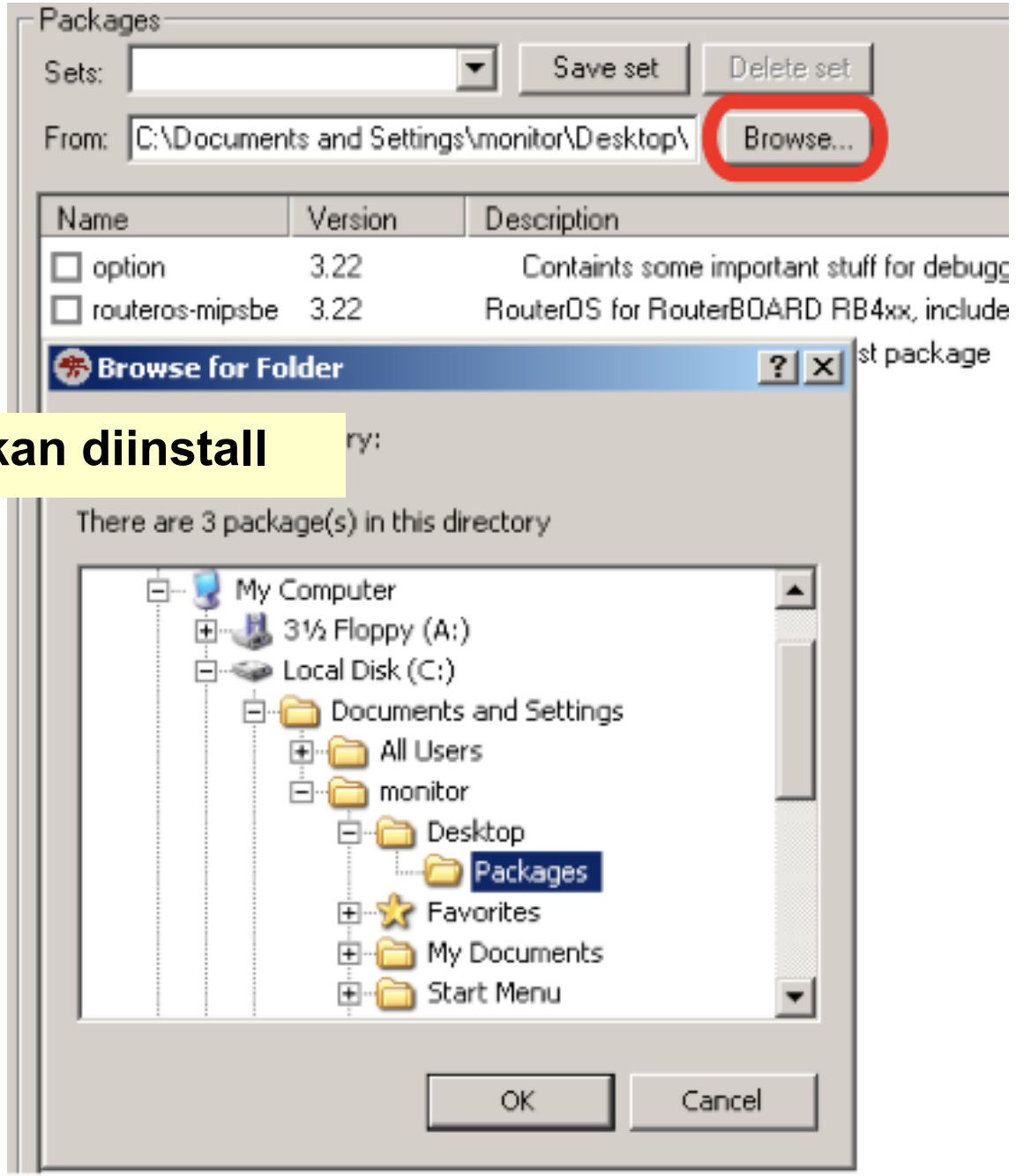
- **Pilih boot-device : 1 – boot ethernet once, then NAND**

Netinstall - Install

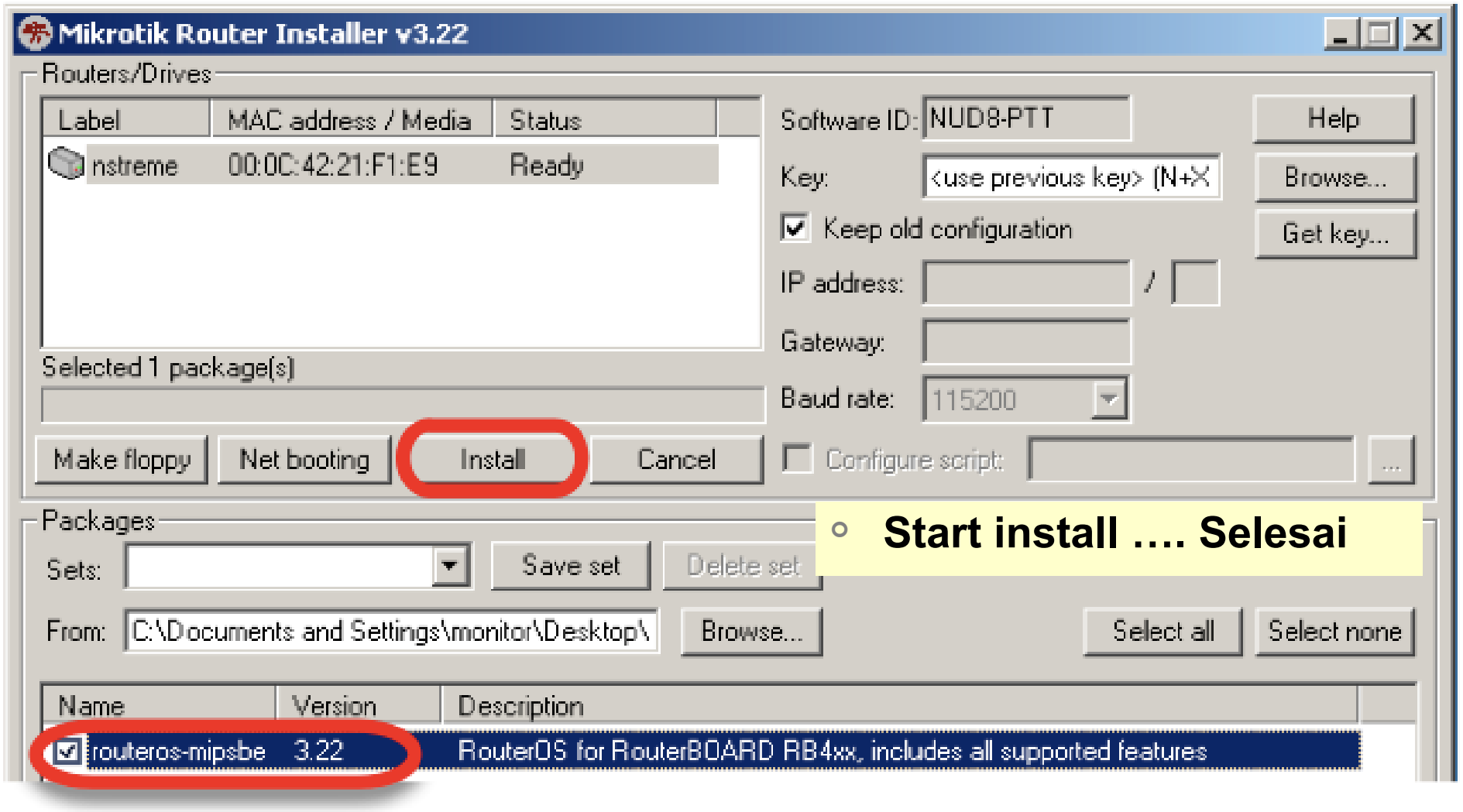


- **Pilih router yang akan diinstall**

- **Pilih module yang akan diinstall**

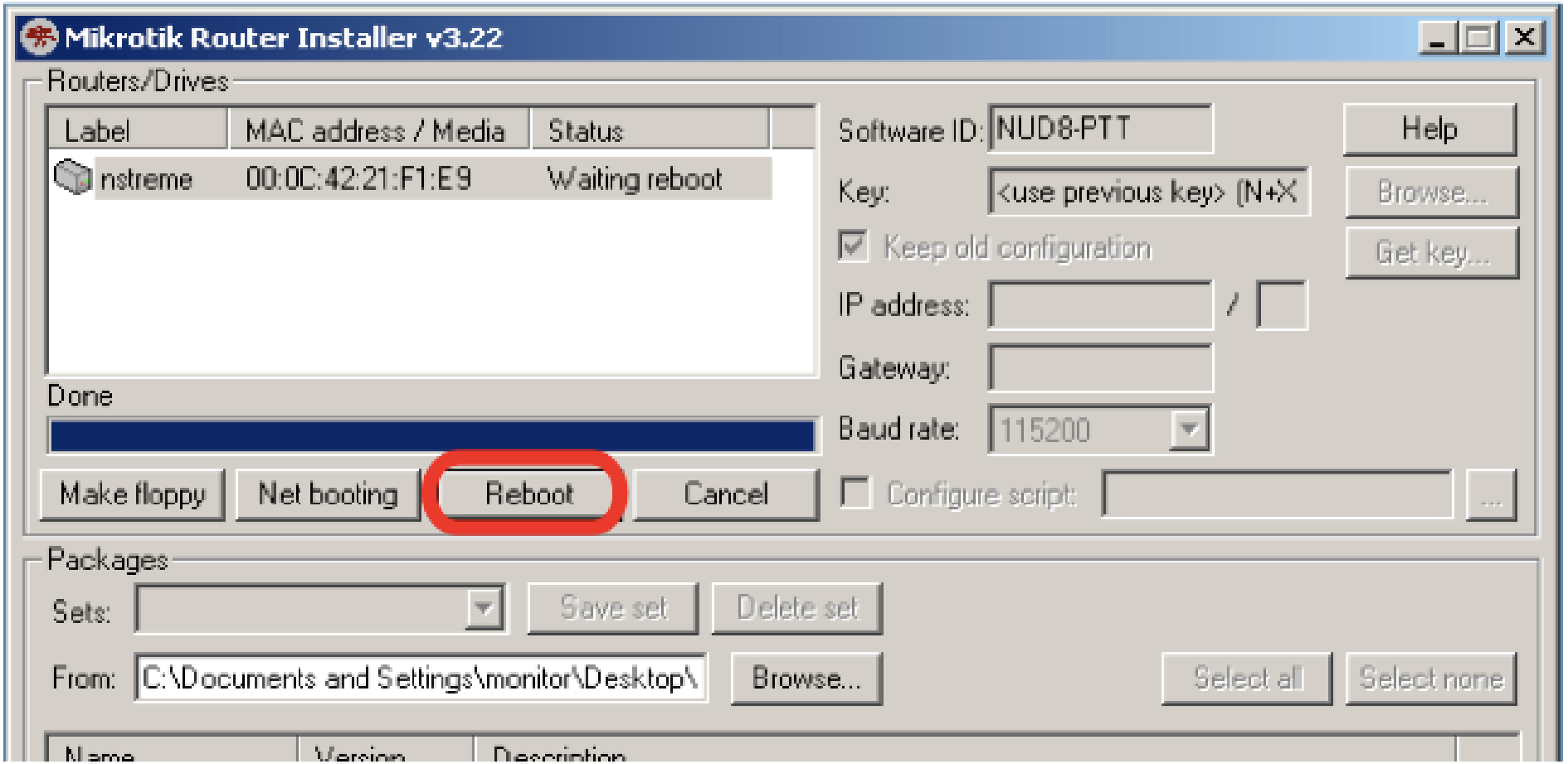


Netinstall - Install



- **Start install …. Selesai**

Netinstall – Reboot



Netinstall - Cleanup

```
Select boot device:
 * e - boot over Ethernet
   n - boot from NAND, if fail then Ethernet
   1 - boot Ethernet once, then NAND
   o - boot from NAND only
   b - boot chosen device
your choice:
```

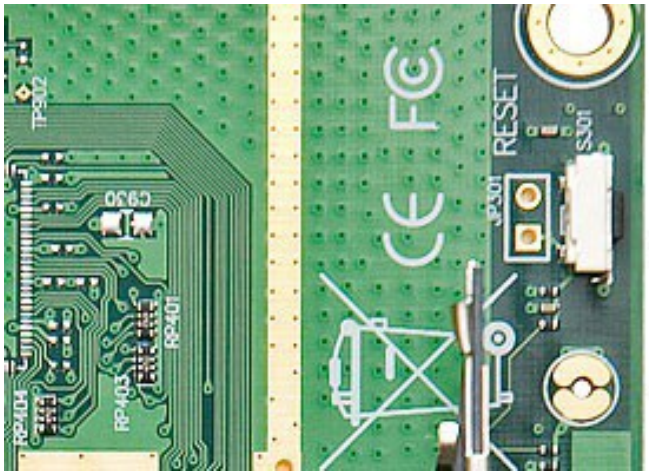
- **Kembalikan boot ke IDE / NAND drive**

- **Video Tutorial :**
  - **http://www.mikrotik.co.id/artikel_lihat.php?id=25**

Reset Password

- Reset password bisa dilakukan di beberapa routerboard menggunakan tombol “**Reset**”

- Hard Reset :



To reset RouterOS config
Hold metal object in here
while the board boots.

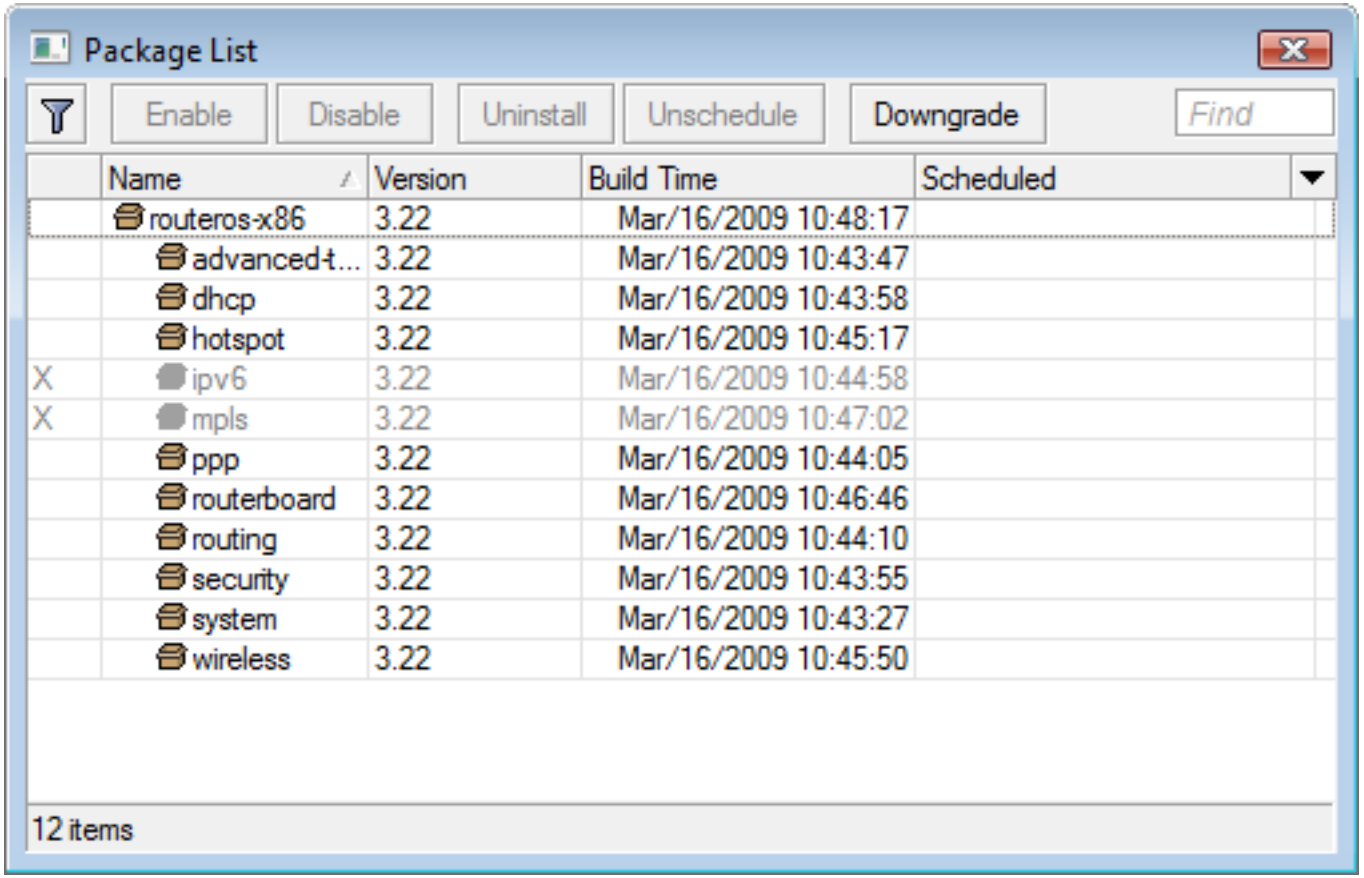
Quiz !

- Routerboard RB433UAH bisa menggunakan USB flashdisk sebagai penyimpanan RouterOS Mikrotik ?

- Netinstall menggunakan kabel serial untuk transfer data OS mikrotik pada saat installasi berlangsung. (Benar / Salah), Kenapa ?

System Package Check

- Pada terminal: /system package print



RouterOS Package

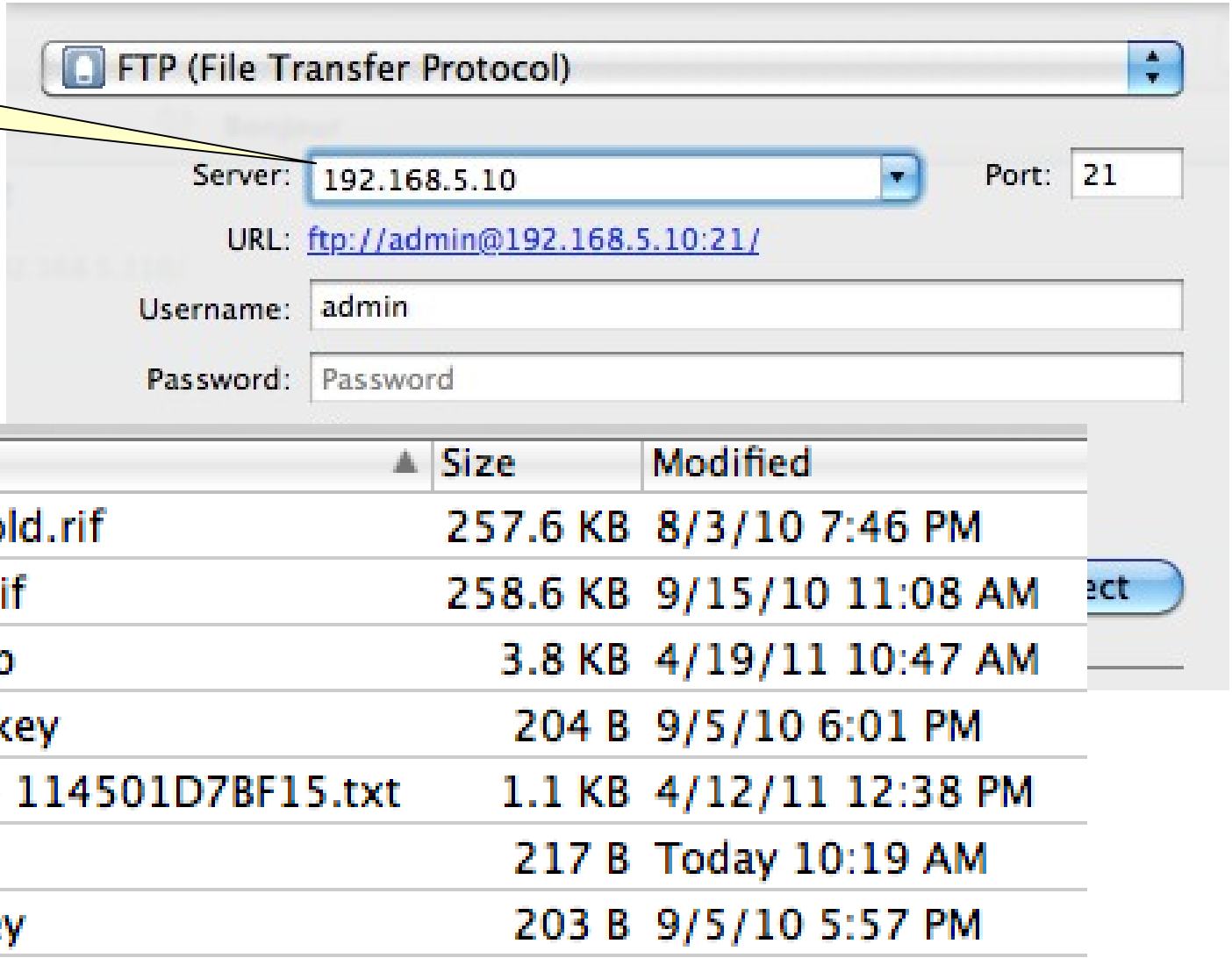
Nama Paket	Fungsi
advanced-tools	email client, ping, netwatch
dhcp	DHCP server dan client
hotspot	hotspot gateway
ntp	NTP server
ppp	PPP,PPTP,L2TP,PPPoE
routerboard	Fungsi khusus Routerboard
routing	RIP, OSPF, BGP
security	secure winbox, SSH, IPSec
wireless	Wireless 802.11a/b/g
user-manager	User-Manager management system
ipv6	IPv6

Version Upgrade

- Download modul terlebih dahulu
  - routeros-**mipsbe**-3.xx.npk (RB400 & RB700)
  - routeros-**mipsle**-3.xx.npk (RB100 & RB500)
  - routeros-**powerpc**-3.xx.npk (RB300 & RB600)
  - routeros-**x86**-3.xx.npk (PC & RB200)
- FTP modul tersebut ke router
  - Harus menggunakan userid yang full access
  - FTP://xxx.xxx.xxx.xxx ← **IP Router**
- Soft Reboot, jangan hard reboot
  - Command - "**/system reboot**"

FTP ke Router

IP Router



Version Downgrade

- Download modul yang lama
- FTP dan copykan modul OS versi yang lama tersebut ke FTP router.
- Cek modul : */file print*
- "***/system package downgrade***"

  admin@MikroTik] system package> downgrade

  Router will be rebooted. Continue? [y/N]: y

  system will reboot shortly

Command Line Interface

- Struktur *Command* dalam mikrotik mirip dengan shell dalam unix
- Dibagi ke dalam beberapa kelompok sesuai hirarki menu levelnya
- Misalnya menambahkan ip address
  - *Ip address add address=192.168.0.1/24 interface=ether1*
  - Menu Ip (level0) memiliki sub menu address (level1)

General Command CLI

add	menambahkan entri tertentu
comment	membubuhkan komentar pada suatu entri
disable	menonaktifkan entri tertentu
enable	mengaktifkan entri tertentu
monitor	memonitor parameter secara live
print	menampilkan semua entri secara singkat
print detail	menampilkan semua entri secara lengkap
remove	menghapus entri tertentu
set	mengubah parameter tertentu pada sebuah entri

Navigasi pada CLI

?	Menampilkan pilihan perintah yang tersedia beserta keterangannya
[TAB]	Melengkapi perintah yang baru terketik sebagian
[TAB][TAB]	Menampilkan pilihan perintah yang tersedia beserta keterangannya
..	Berpindah 1 level ke atas pada hirarki menu
/	Berpindah ke level teratas pada hirarki menu

Command Line Interface

- Quick Typing
  - [TAB] untuk melengkapi perintah tertentu
    - */system shut [TAB] = /system shutdown*
  - Juga bisa menggunakan singkatan
    - /sys shut = /system shutdown
- Untuk Detail penggunaan Script di RouterOS Mikrotik bisa didapatkan manualnya di :
  - **http://wiki.mikrotik.com/wiki/Scripting**

Quiz !

- Paket apa saja yang dibutuhkan untuk menginstall mikrotik (Minimal):
  - System
  - Routing
  - Advance-tools
  - DHCP

- Apakah bisa menambahkan driver secara manual di RouterOS ?

Basic TCP/IP

Certified Mikrotik Training Basic Class

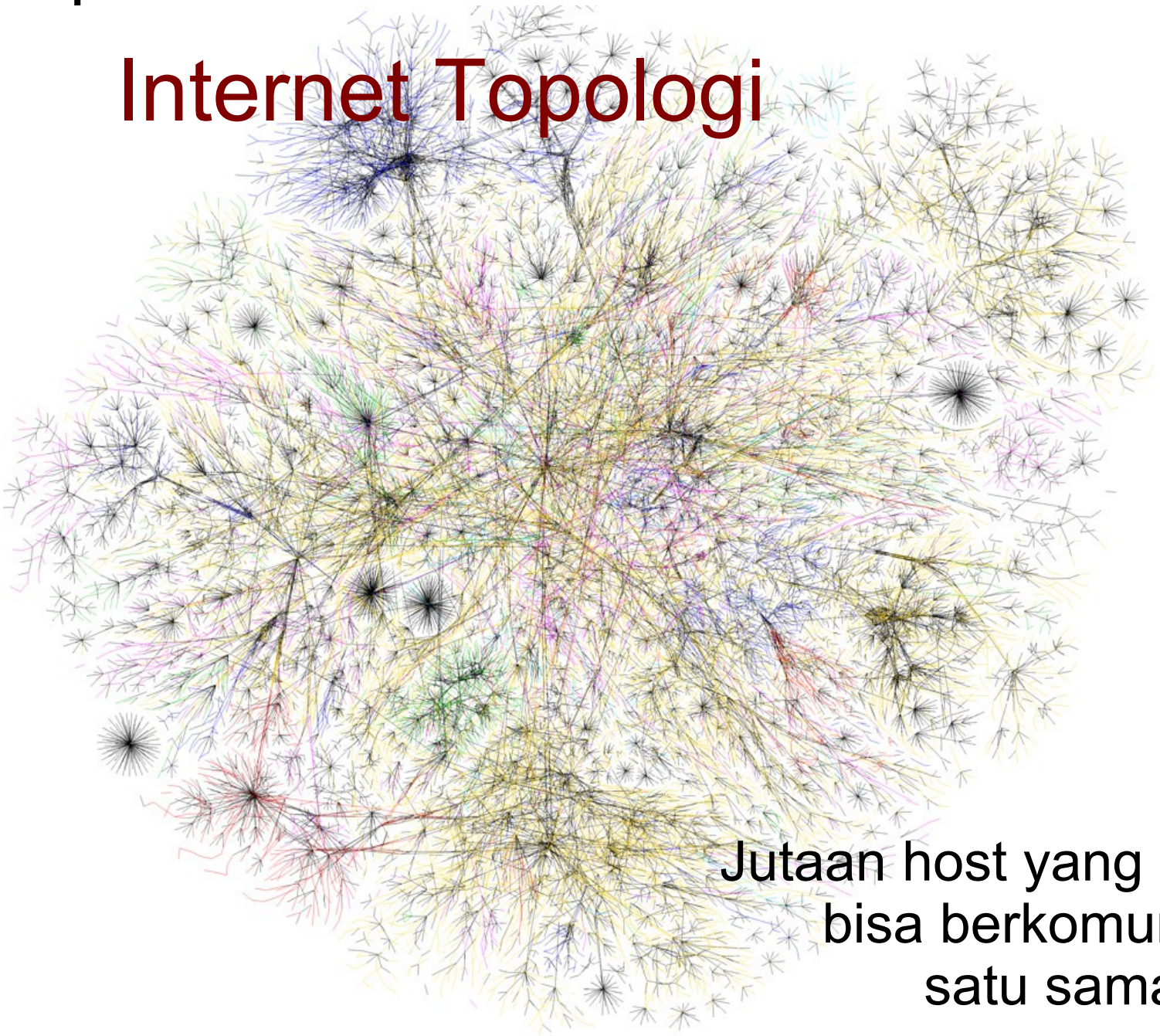
Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

Training Outline

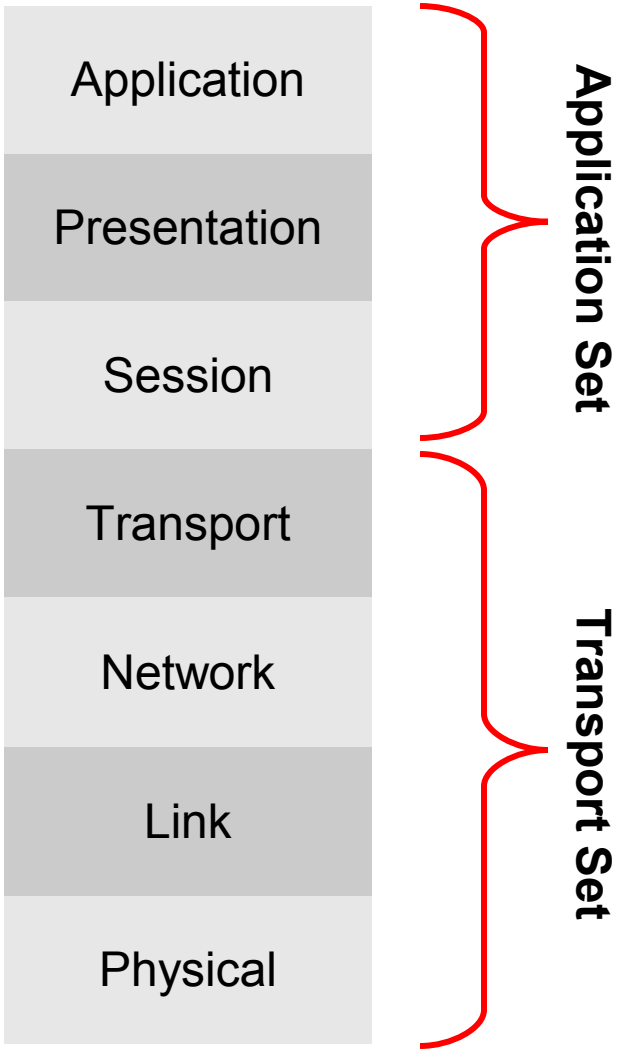
- OSI Layer
- Packet Header
- Mac Address
- IP Address and subnetting
- IP Protocol
- Basic networking, DNS, gateway

Internet Topologi



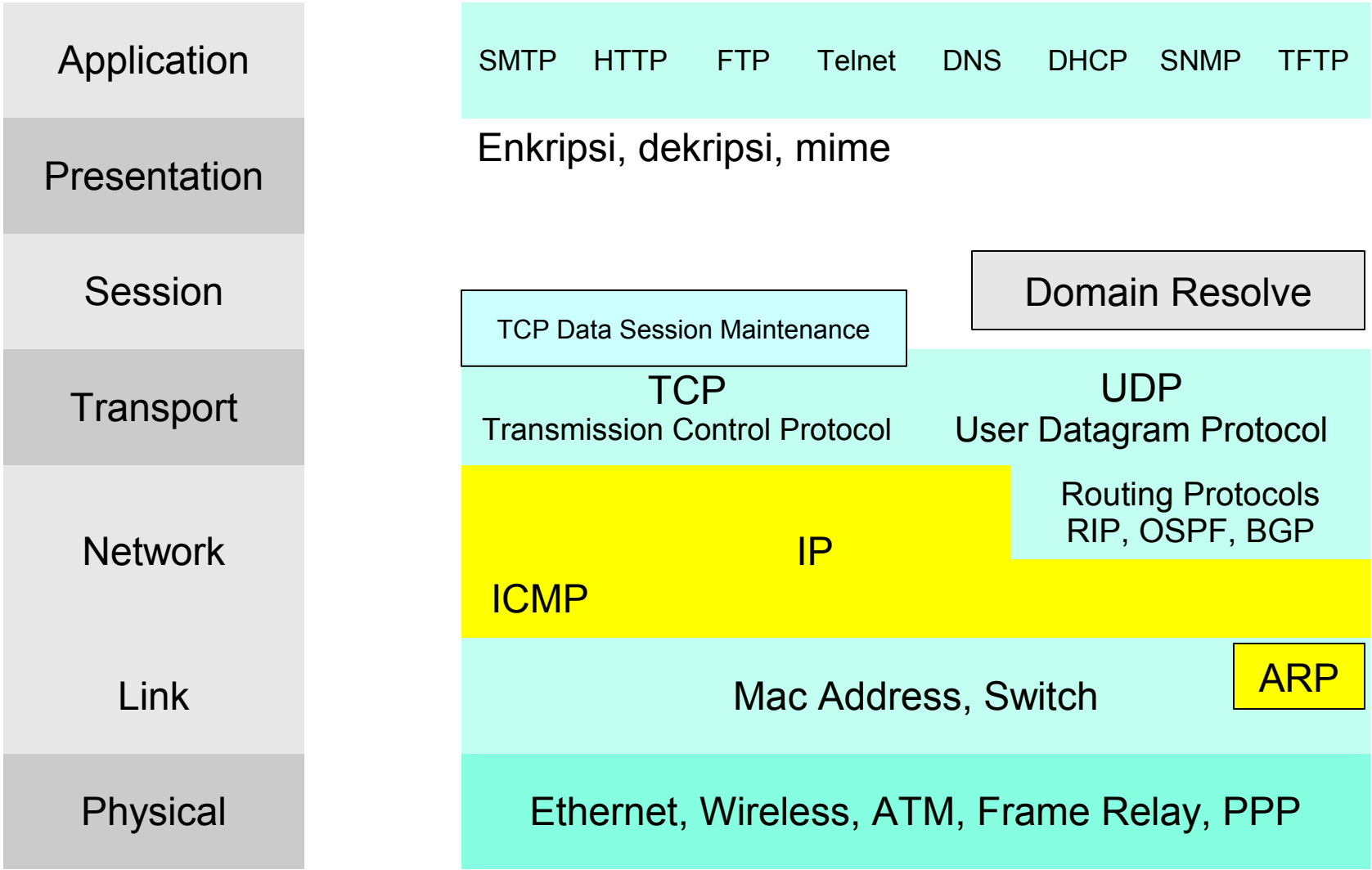
Jutaan host yang harus
bisa berkomunikasi
satu sama lain.

OSI Layer dan Protokol

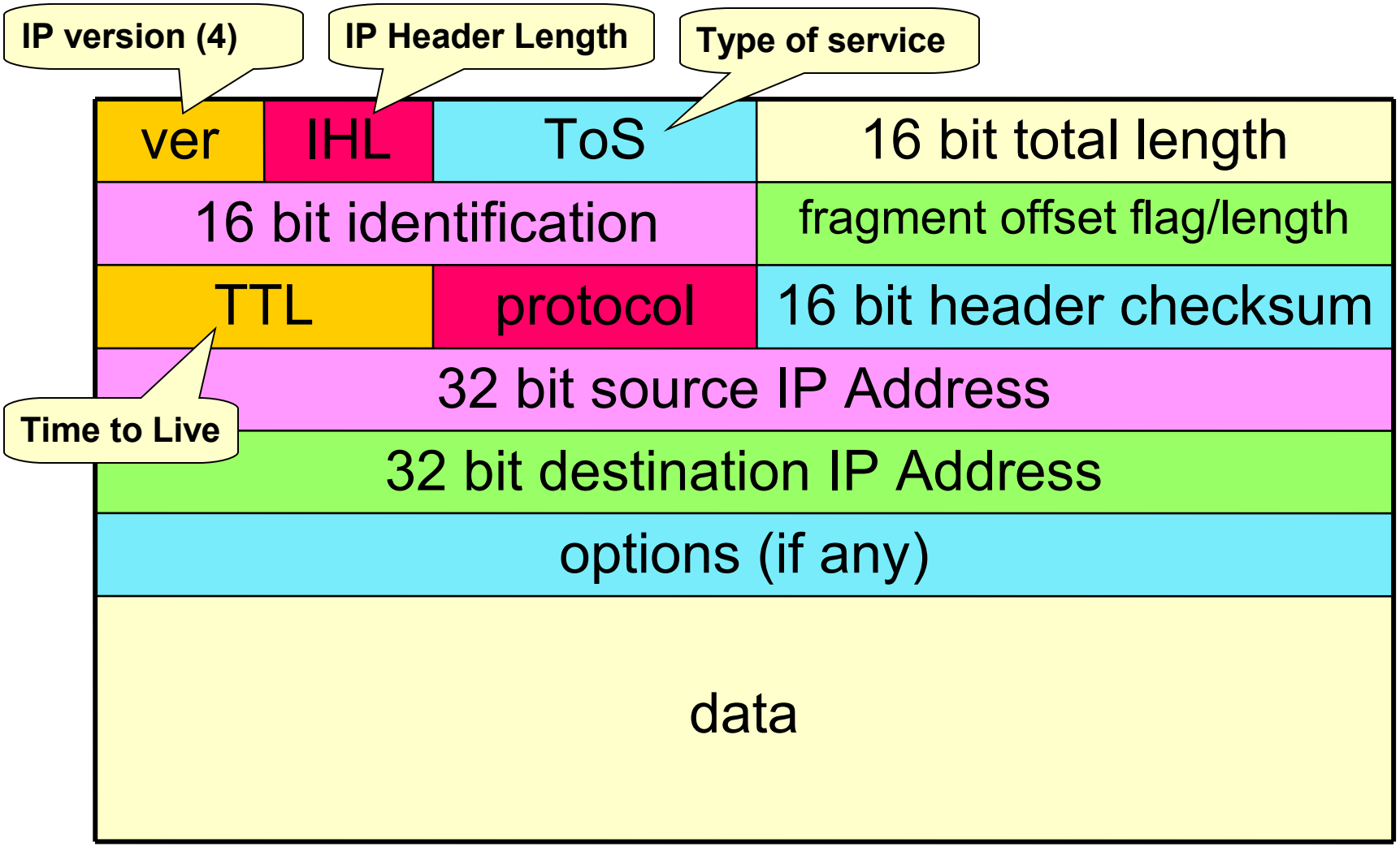


Open Systems Interconnection (OSI) adalah sebuah model referensi arsitektur antarmuka jaringan yang dikembangkan oleh ISO yang kemudian menjadi konsep standard komunikasi jaringan di hampir semua perangkat jaringan.

OSI Layer dan Protokol



Packet Header

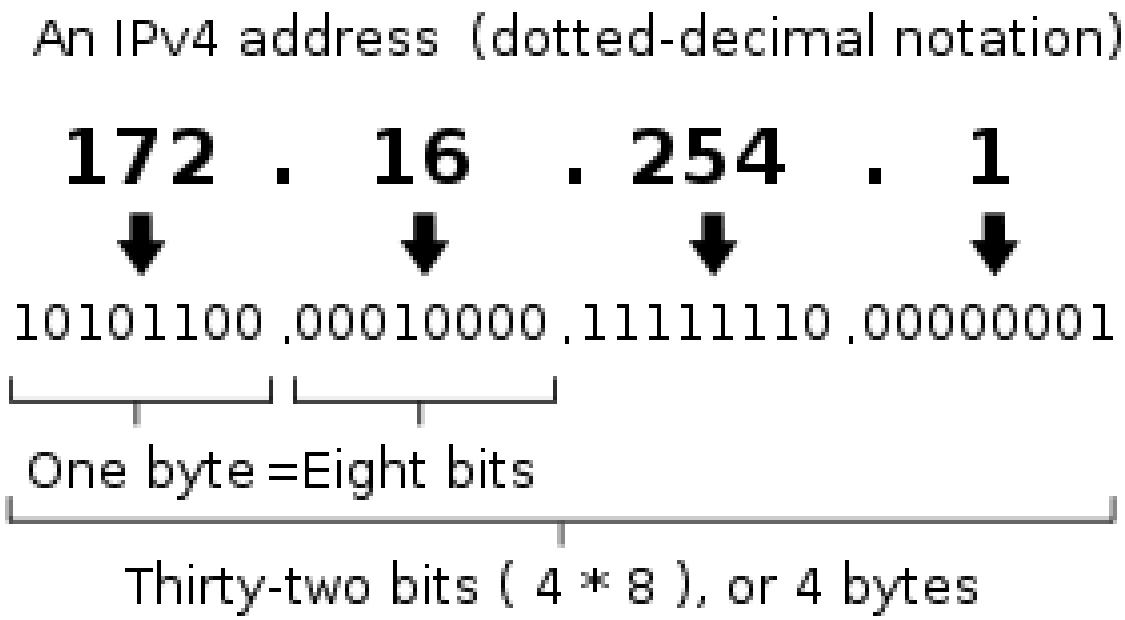


MAC Address

- MAC = Media Access Control
- Digunakan sebagai identitas yang unik dari setiap interface hardware, yang merupakan identitas untuk berkomunikasi di OSI layer 2.
- Sebagian bit merupakan identitas pabrik pembuat hardware
- 48 bit hex. Contoh: "**AA:BB:CC:DD:EE:FF**"
- Jika sebuah router memiliki 3 interface fisik, maka akan memiliki 3 buah mac address
- Untuk virtual interface (VLAN, EoIP) maka ditambahkan mac address virtual.

IP Address

- Adalah sistem pengalamatan setiap host yang terhubung ke jaringan
- Saat ini IP Address yang banyak digunakan adalah IP versi 4. (32 bits / 4 bytes) - 4,294,967,296 hosts



Pengelompokan IP Address

- Pengelompokan IP Address dilakukan dengan subnet-ing.
- Subnet ….. 0 – 32
  - Melambangkan jumlah IP dalam subnet tersebut dengan rumus $2^{(32-x)}$
  - Subnet 0 berarti semua IP Address
  - Subnet 32 berarti 1 IP Address

IP Subneting (contoh 1)

- Contoh: 192.168.0.0/24
  - Netmask : 255.255.255.0
  - Prefix : /24
  - IP Network : 192.168.0.0
  - First HostIP: 192.168.0.1
  - Last HostIP : 192.168.0.254
  - Broadcast : 192.168.0.255
  - HostIP : total IP di dalam Subnet (–) minus 2

IP Subneting (contoh 2)

- Contoh: 192.168.0.0/25
  - Netmask : 255.255.255.128
  - Prefix : /25
  - IP Network : 192.168.0.0
  - First HostIP: 192.168.0.1
  - Last HostIP : 192.168.0.126
  - Broadcast : 192.168.0.127
  - HostIP : total IP di dalam Subnet (–) minus 2

Tabel Subnet

Subnet Mask	Prefix	No of IP	Usable IP
255.255.255.0	/24	256	254
255.255.255.128	/25	128	126
255.255.255.192	/26	64	62
255.255.255.224	/27	32	30
255.255.255.240	/28	16	14
255.255.255.248	/29	8	6
255.255.255.252	/30	4	2
255.255.255.254	/31	2	-
255.255.255.255	/32	1	-

Quiz !

- Berikut ini adalah IP Address yang tidak boleh digunakan oleh host atau server yang berada pada internet network (public internet) :
  a. 192.186.0.1
  b. 172.31.76.76
  c. 110.10.12.10
  d. 10.100.123.45

- Seiring perjalanan data dari layer 1 ke layer 7 dalam 7 layer OSI, header dari paket data :
  a. di-susun-ulang
  b. di-modifikasi
  c. di-tambah
  d. di-hilangkan

Public and Private IP Address

- **Public IP Address**
  IP Address yang dapat diakses di jaringan internet.
  Kita bisa mendapatkan Public IP Address dari:
  - Dipinjami dari ISP
  - Alokasi dari APNIC/IDNIC (www.idnic.net)
- **Private IP Address**
  IP Address yang diperuntukkan untuk jaringan lokal (tidak dapat diakses di jaringan internet)
  - 10.0.0.0 – 10.255.255.255 (10./8)
  - 172.16.0.0 – 172.31.255.255 (172.16./12)
  - 192.168.0.0 – 192.168.255.255 (192.168./16)

IP Address Khusus Lainnya

Penggunaan	IP / subnet
Self Identification	0.0.0.0/8
Localhost	127.0.0.1
Not Used	Other 127.0.0.0/8
Multicast	224.0.0.0/4
Local link/DHCP error	169.245.0.0/16
TEST-NET-1	192.0.2.0/24
TEST-NET-2	198.51.100.0/24
TEST-NET-3	203.0.113.0/24
6to4 Relay Anycast	192.88.99.0/24
Benchmark Test	198.18.0.0/15
Future Used	240.0.0.0/4
Limited Broadcast	255.255.255.255/32

RFC5735 Jan 2010: http://tools.ietf.org/html/rfc5735

IP Protocol

- Adalah protokol standart yang digunakan untuk mengkomunikasikan data melalui berbagai jenis perangkat dan layer.
- Pengiriman data dilakukan dengan sistem “per paket” dan/atau “per connection”.
- Sistem ini menjamin keutuhan data, dan mencegah terjadinya kekurangan ataupun duplikasi data.
- Ada beragam protokol yang biasa digunakan, yang umum adalah TCP, UDP, dan ICMP.

ICMP (Internet Control Message Protocol)

- Disalurkan berbasis “best effort” sehingga bisa terjadi error (datagram lost)
- Banyak digunakan untuk pengecekan jaringan
- Prinsip kerja:
  - Host (router ataupun tujuan) akan mendeteksi apabila terjadi permasalahan tranmisi, dan membuat “ICMP message” yang akan dikirimkan ke host asal.
- Aplikasi ICMP yang paling banyak digunakan: Ping dan Traceroute

Type	Name
0	Echo Reply
1	Unassigned
2	Unassigned
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address
7	Unassigned
8	Echo
9	Router Advertisement
10	Router Solicitation
11	Time Exceeded

UDP (User Datagram Protocol)

- Komputer yang satu bisa mengirimkan pesan/datagram ke komputer lainnya di jaringan, tanpa terlebih dahulu melakukan “hand-shake” (connectionless communication)
- Biasanya digunakan untuk servis yang mengirimkan data kecil ke banyak host
- Tidak ada flow control ataupun mekanisme lain untuk menjaga keutuhan datagram
- Aplikasi yang paling umum menggunakan UDP adalah DNS dan berbagai game online

TCP (Transmission Control Protocol)

- Merupakan protokol yang paling banyak digunakan di internet.
- Bekerja dengan pengalamatan port
  - Port 1 – 1024 : low port (standard service port)
  - Port 1025…: high port (untuk transmisi lanjutan)
- Contoh aplikasi: http, email, ftp, dll
- Prinsip Kerja: Connection Oriented, Reliable Transmission, Error Detection, Flow Control, Segment Size Control, Congestion Control

Prinsip Kerja TCP

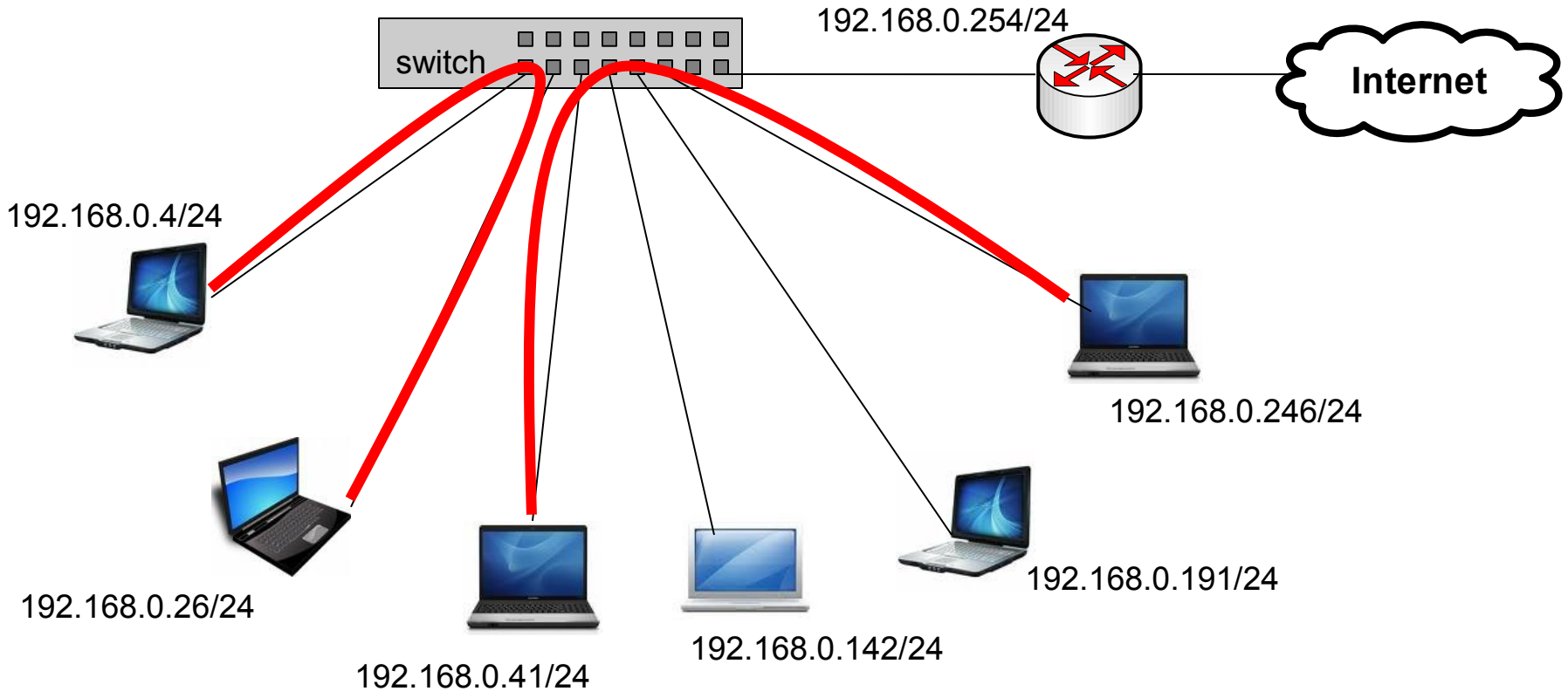
- Connection Oriented
  - Koneksi diawali dengan proses “handshake”
    - Client → SYN → Server
    - Server → SYN-ACK → Client
    - Client → ACK → Server
- Reliable Transmission
  - Mampu melakukan pengurutan paket data, setiap byte data ditandai dengan nomor yang unik
- Error Detection
  - Jika terjadi error, bisa dilakukan pengiriman ulang data

Prinsip Kerja TCP

- Flow Control
  - Mendeteksi supaya satu host tidak mengirimkan data ke host lainnya terlalu cepat
- Segment Size Control
  - Mendeteksi besaran MSS (maximum segment size) yang bisa dikirimkan supaya tidak terjadi IP fragmentation
- Congestion Control
  - TCP menggunakan beberapa mekanisme untuk mencegah terjadinya congestion pada network

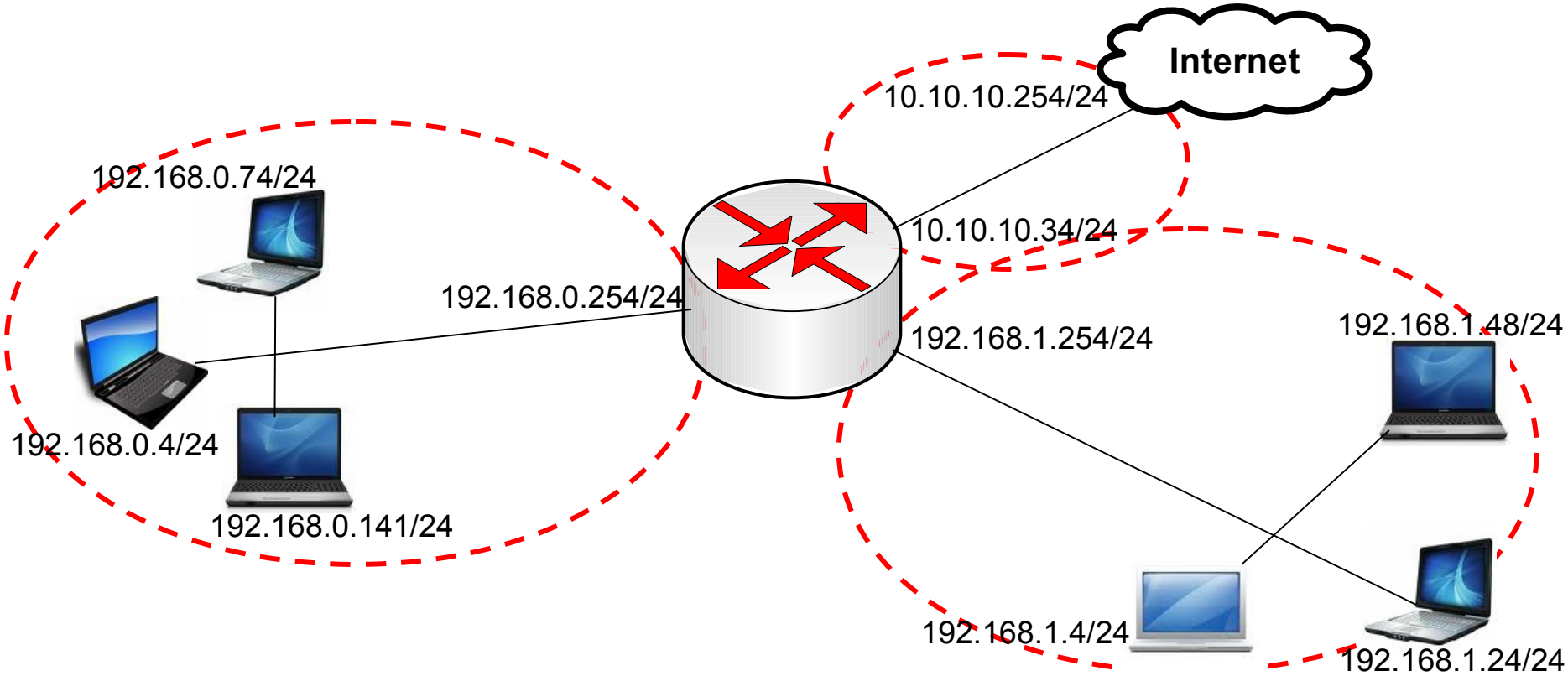
Konsep Dasar Jaringan

- Host yang memiliki IP Address dari subnet yang sama bisa terkoneksi langsung, tanpa melalui router
  - From : **192.168.0.4** To : **192.168.0.26**



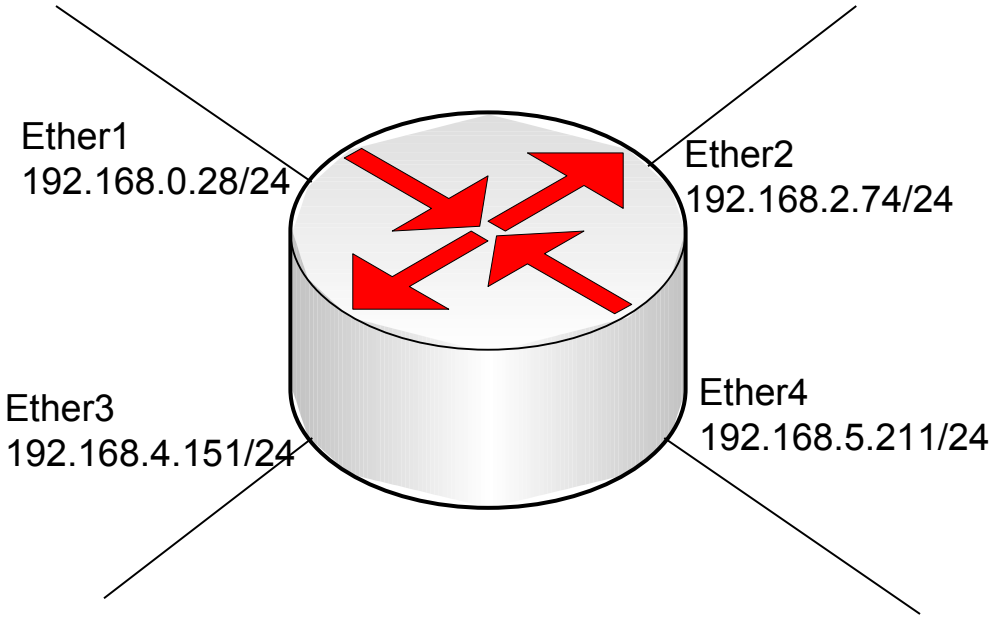
Konsep Dasar Jaringan

- Router bertugas untuk menghubungkan dua atau lebih jaringan yang memiliki subnet yang berbeda



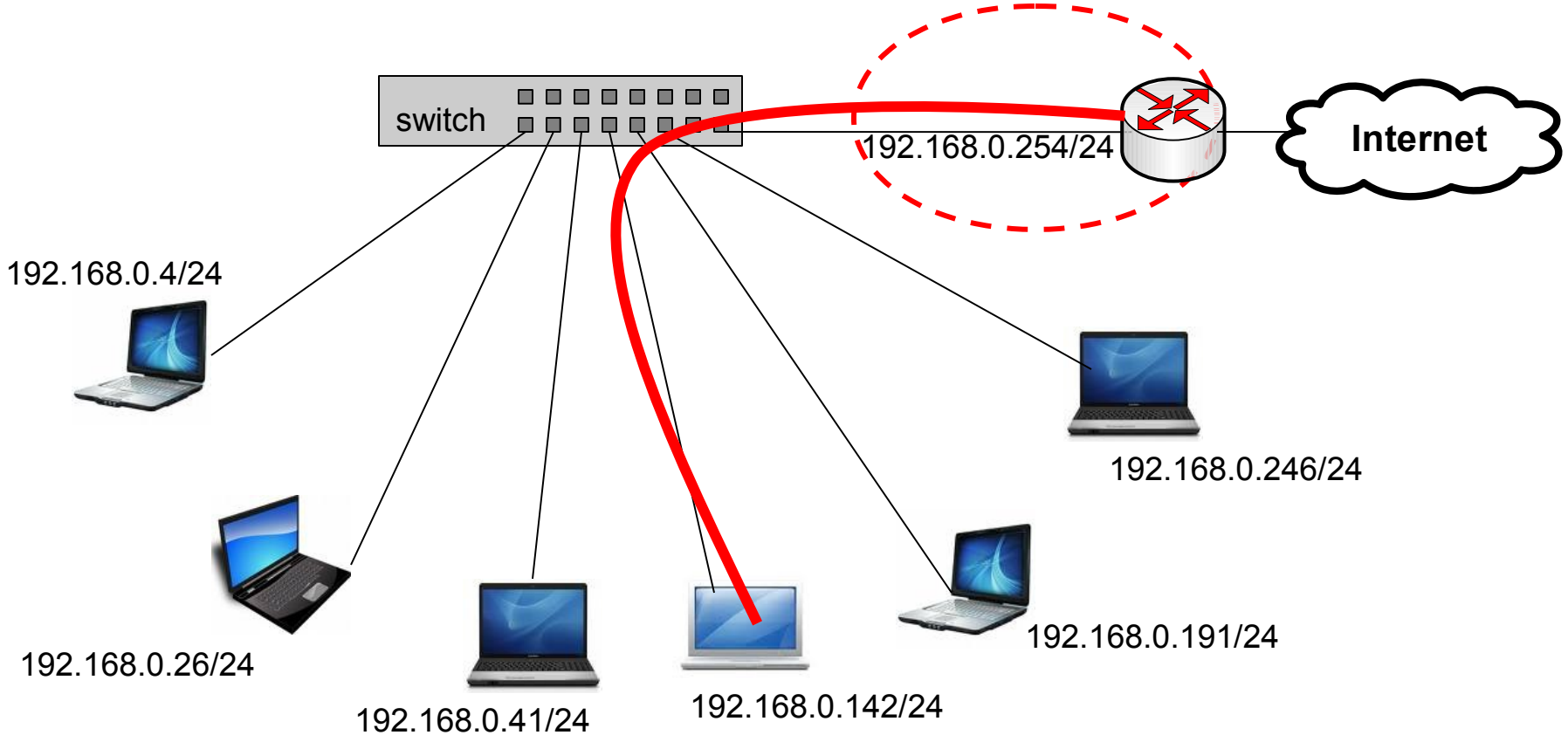
Konsep Dasar Jaringan

- Dua buah IP Address yang berasal dari subnet yang sama tidak boleh dipasang pada dua buah interface yang berbeda pada sebuah router



Konsep Dasar Jaringan

- Default gateway menentukan ke arah mana trafik harus disalurkan untuk menuju ke internet
  - From : **192.168.0.142** To : **222.24.112.34**



Konsep Dasar Jaringan

- DNS diperlukan untuk melakukan pengubahan nama domain menjadi ip address, karena seluruh proses pengaturan trafik dilakukan berdasarkan layer 3 OSI, yaitu ip address
- Contoh:
  - www.yahoo.com → 203.0.113.5

Quiz !

- DNS diperlukan untuk terkoneksi ke internet ? (Benar / Salah) Kenapa ?
- Protocol email SMTP menggunakan protocol & port ?
- Protocol TCP memiliki beberapa fungsi berikut, kecuali!
  - Proper Sequencing of Packet
  - Flow Control Packet
  - Retransmission Packet
  - Addressing Packet

RouterOS Basic Configuration

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

Winbox - Download

- Download terlebih dahulu program **winbox.exe** untuk mengkonfigurasi RouterOS Mikrotik.

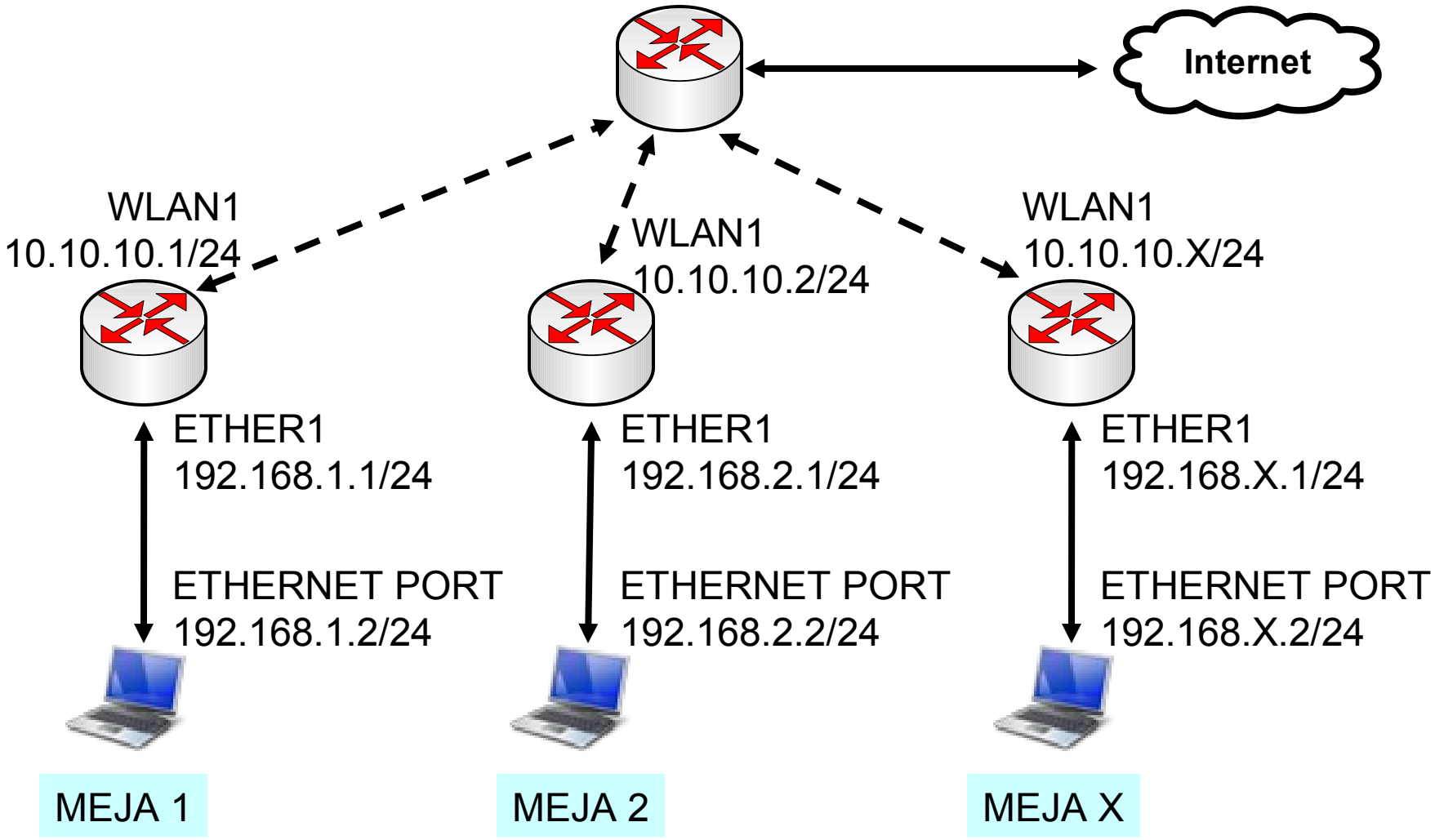
Mikrotik Utility

Winbox

Utility untuk melakukan remote GUI ke Router Mikrotik. For windows.

winbox-2.2.13.exe (34.5 KByte, didownload 376887 kali)
winbox-2.2.11.exe (34.5 KByte, didownload 76782 kali)
winbox-2.2.10.exe (34.5 KByte, didownload 60046 kali)
winbox-2.2.15.exe (36.5 KByte, didownload 239230 kali)
winbox-2.2.18.exe (111.5 KByte, didownload 36747 kali)

Basic Config - Topology



IP Configuration

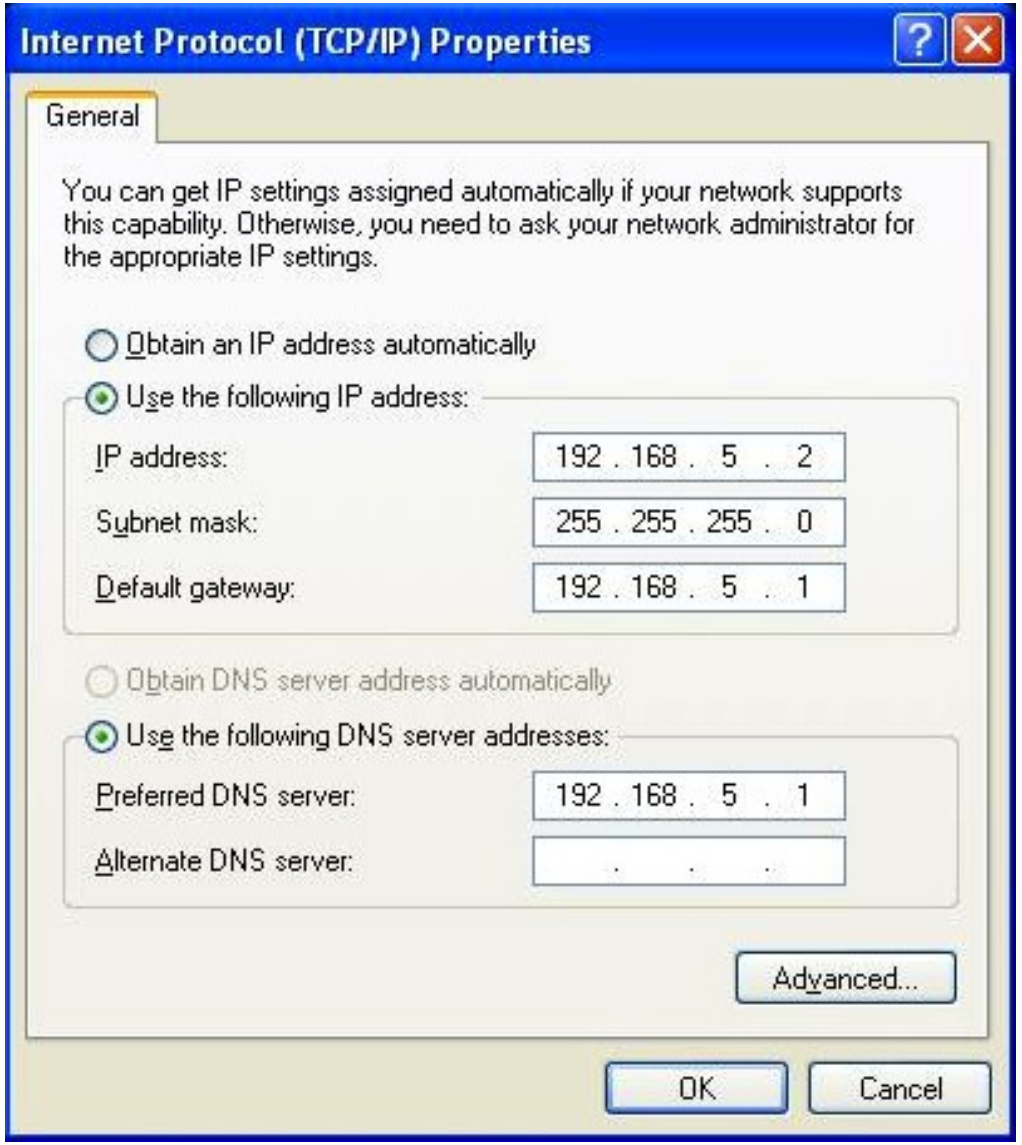
Lab-1 adalah sebuah simulasi konfigurasi dasar sebuah Router Mikrotik yang akan digunakan di jaringan local seperti **Warnet**, **Office**, **Kampus** atau bahkan di **RT/RW-NET**

X = nomor peserta

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

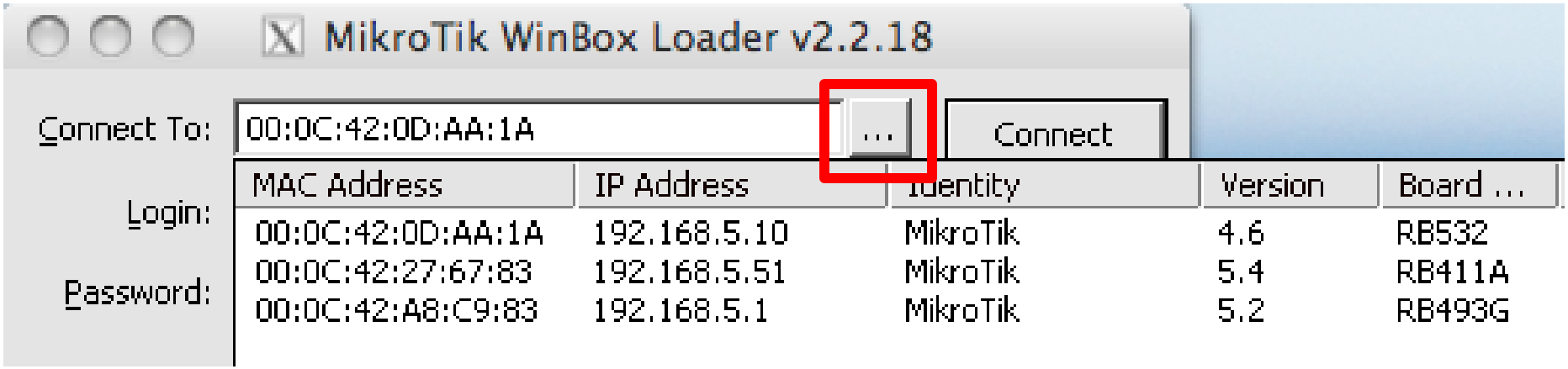
Laptop Config

- Konfigurasi ip-address statik pada laptop.



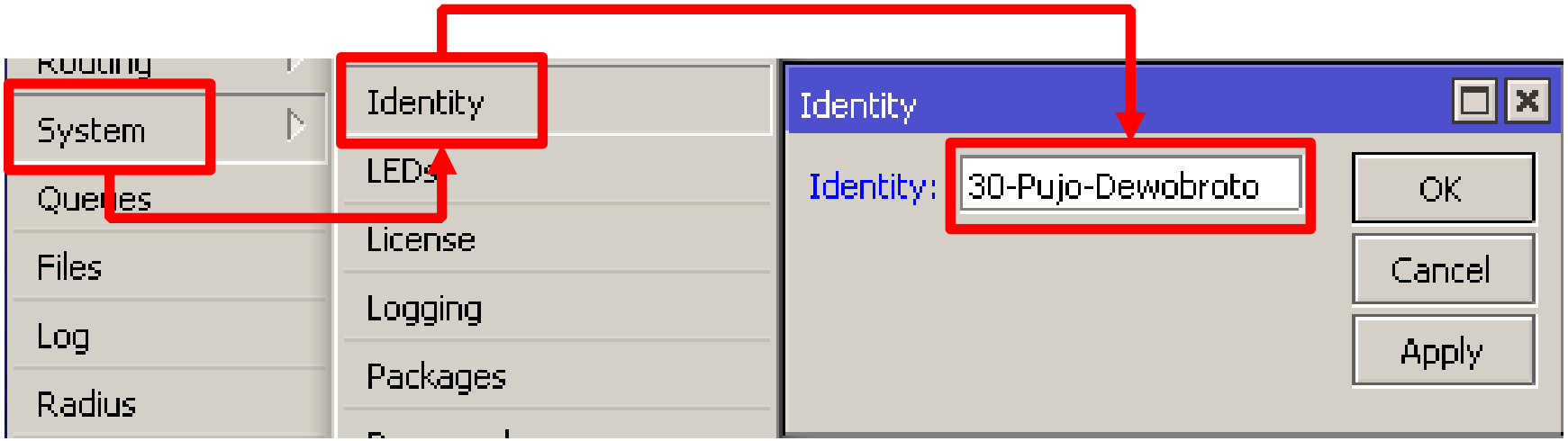
First Setup

- Hubungkan port ethernet Laptop Anda dengan **ether1** pada Routerboard.
- Pastikan ethernet port di laptop Anda memiliki IP statik
- Jalankan program winbox.exe, klik pada tombol **[...]** untuk melihat router Anda.

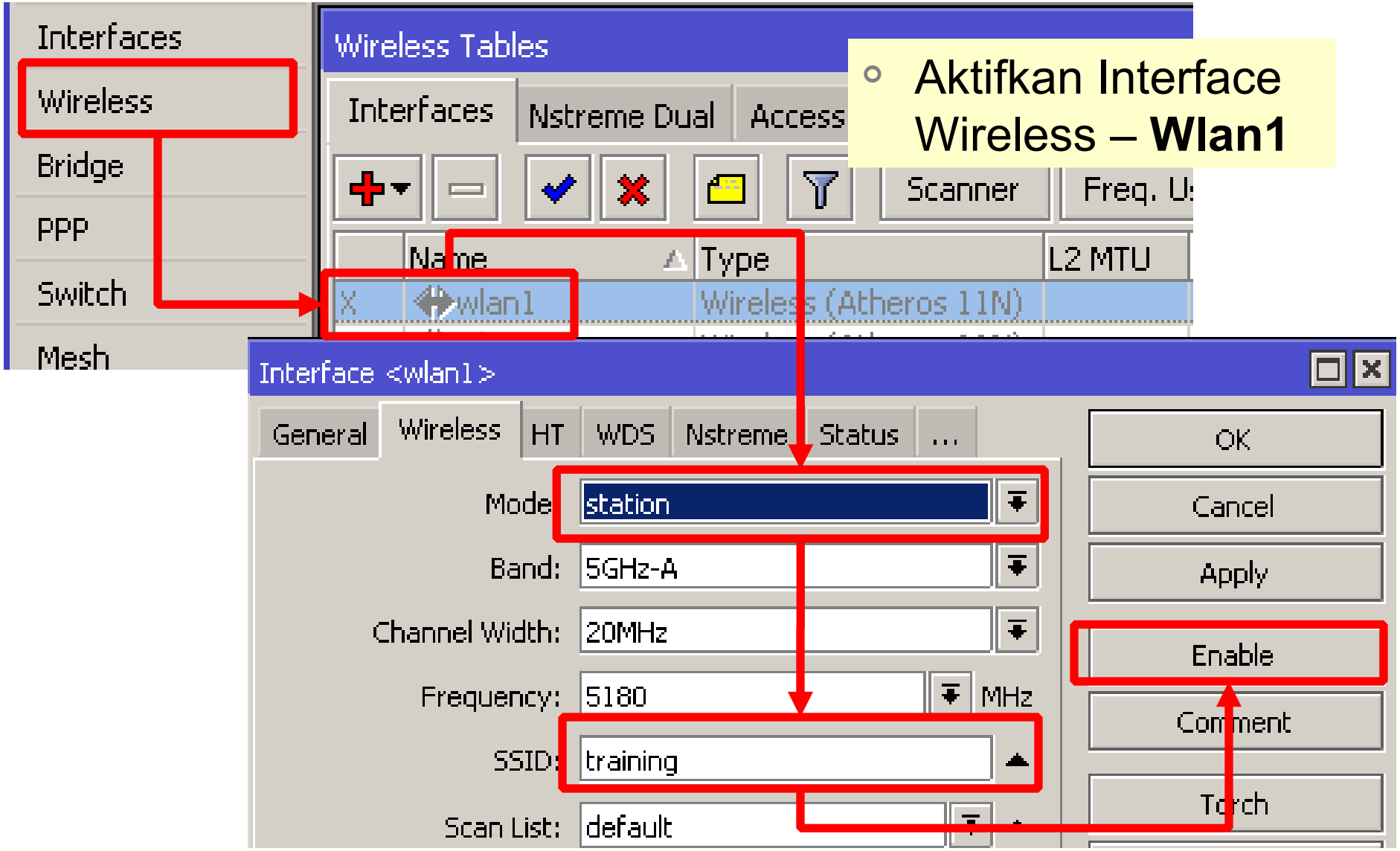


[LAB-1] System Identity

- Supaya tidak membingungkan, ubahlah nama router Anda.
- Format: **xx-NamaAnda**
- Contoh: 30-Pujo-Dewobroto

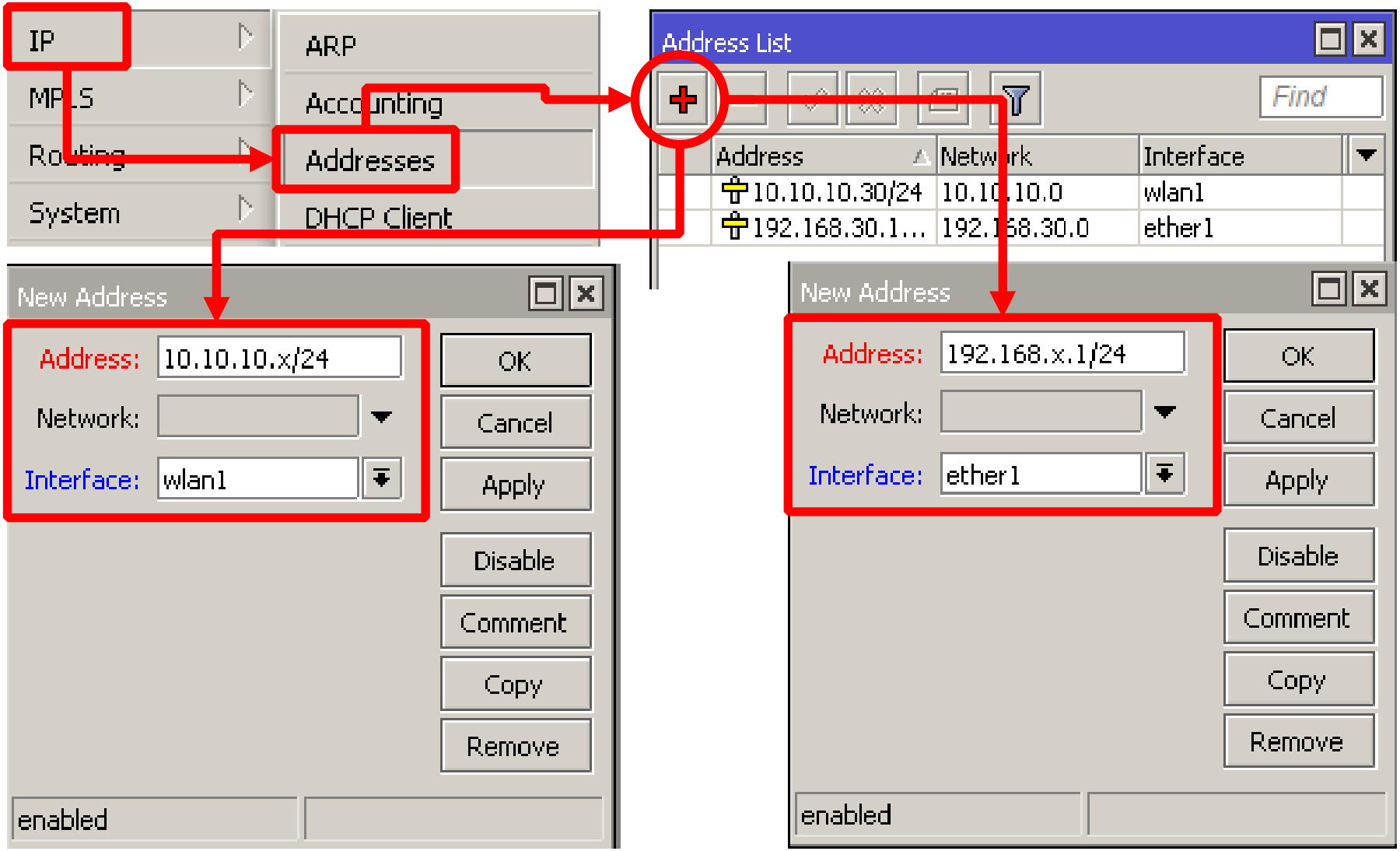


[LAB-2] Wireless Config

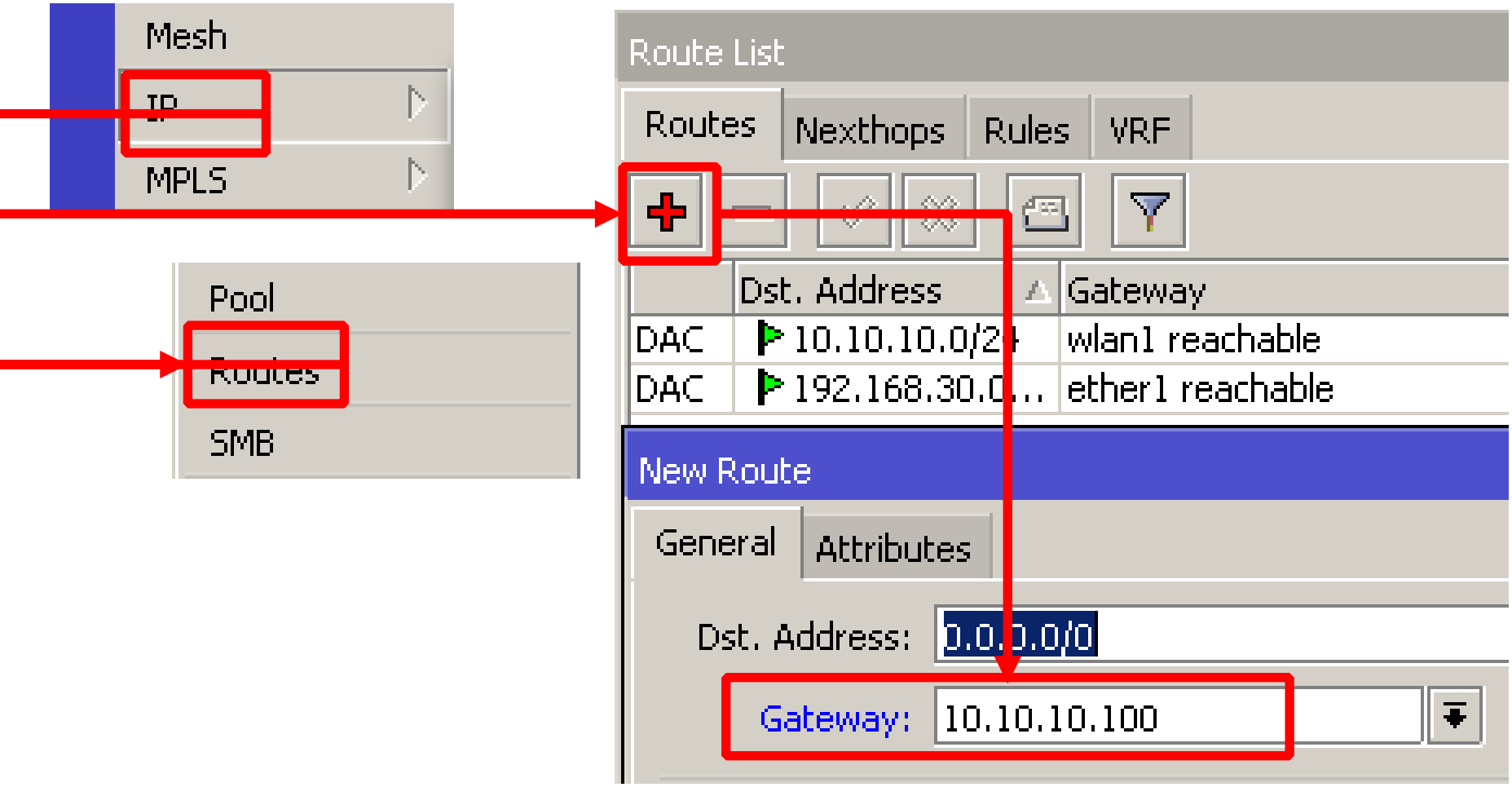


- Aktifkan Interface Wireless – **Wlan1**

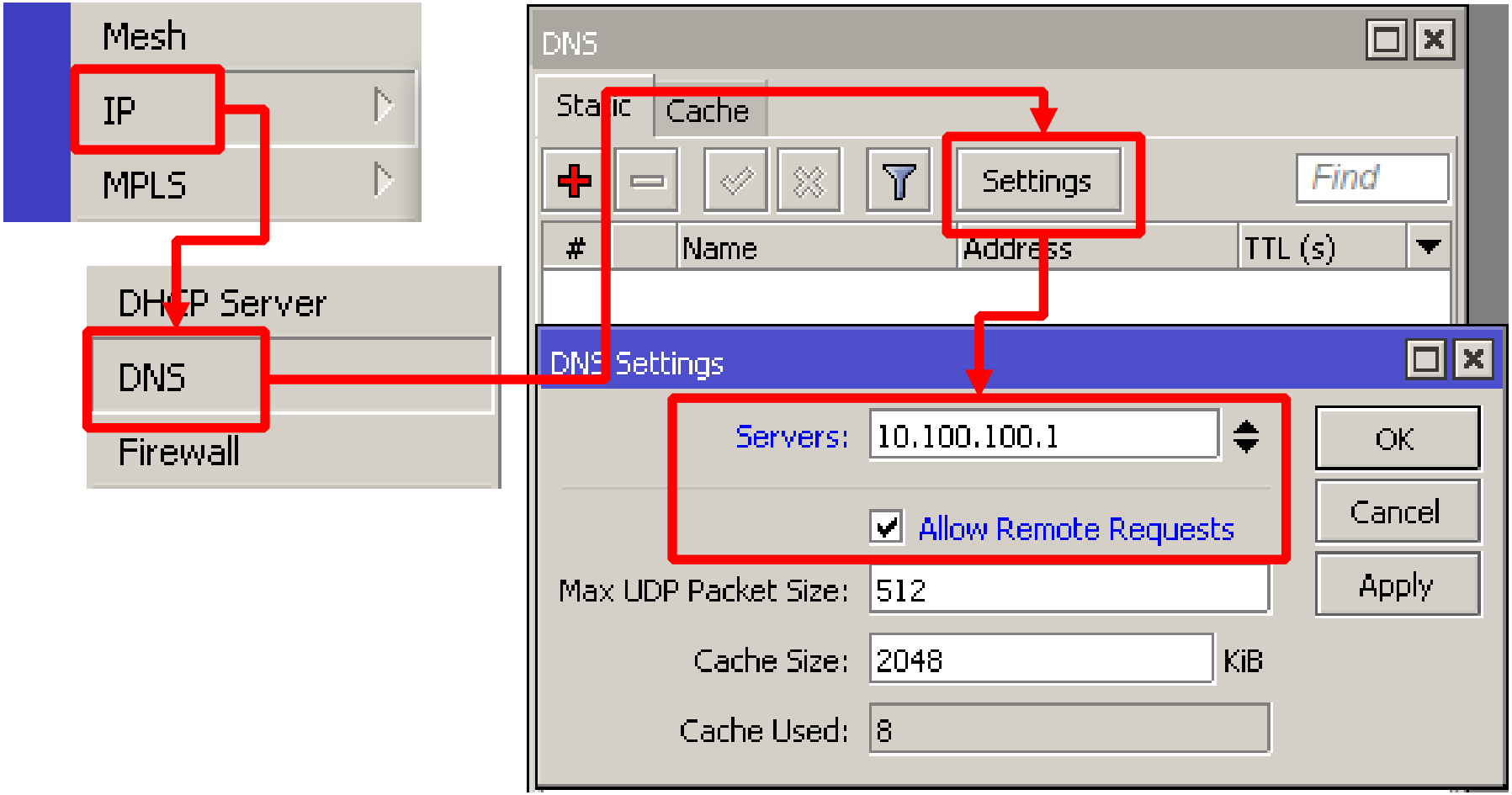
[LAB-3] IP Address Config



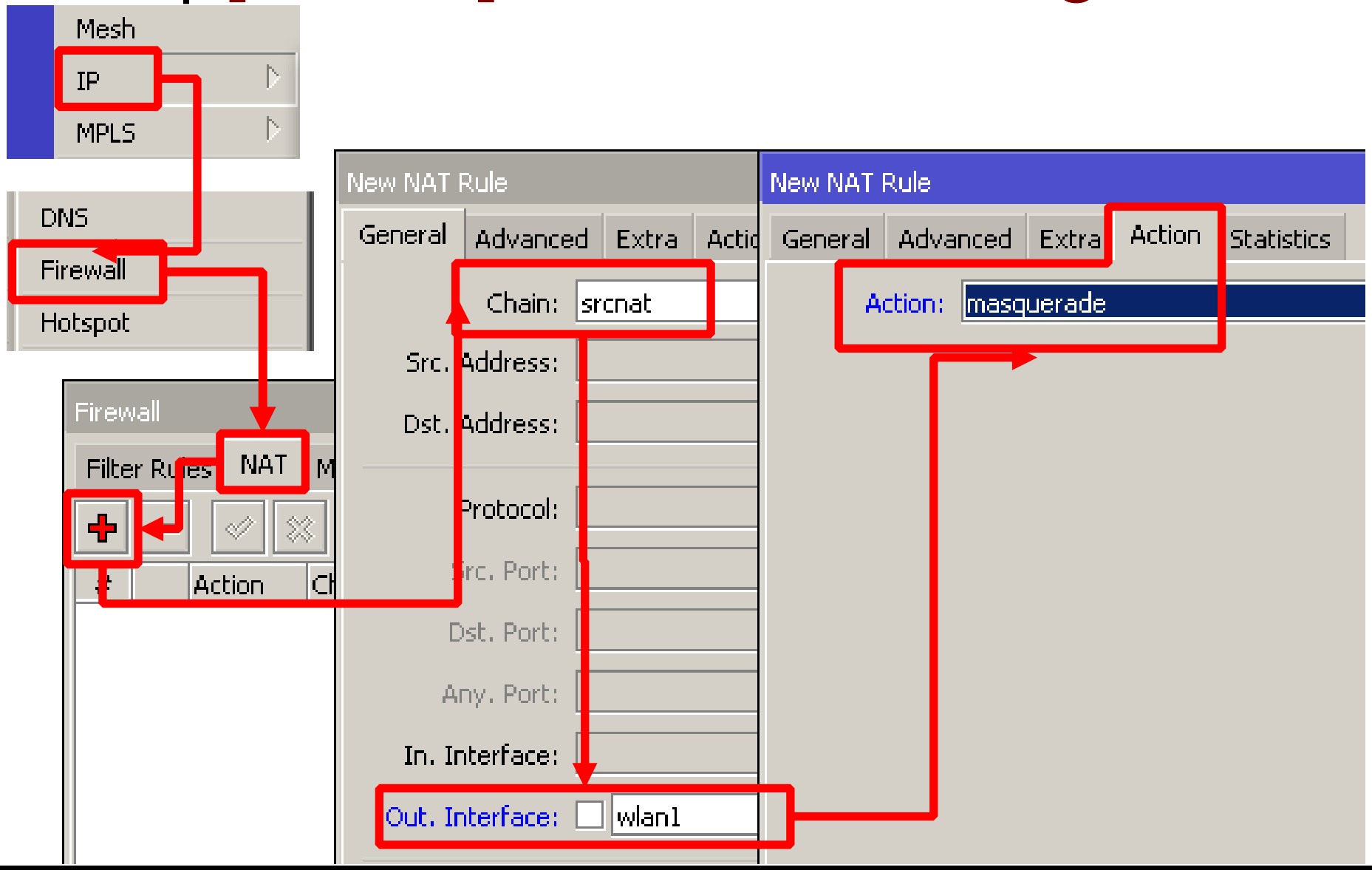
[LAB-4] Gateway Config



[LAB-5] DNS Config



[LAB-6] Src-NAT Config



Terminal / Console Config

- Konfigurasi identity router
  - */system identity set name="xx-nama-anda"*
- Konfigurasi wireless sebagai media untuk backbone
  - */interface wireless set wlan1 mode=station ssid=training band=5ghz-a disabled=no*
- Konfigurasi IP Address
  - */ip address add address=10.10.10.x/24 interface=wlan1*
  - */ip address add address=192.168.x.1/24 interface=ether1*
- Konfigurasi Routing – Default Gateway
  - */ip route add gateway=10.10.10.100*
- Konfigurasi DNS
  - */ip dns set servers=10.100.100.1 allow-remote-request=yes*
- Konfigurasi NAT
  - */ip firewall nat add chain=srcnat out-interface=wlan1 action=masquerade*

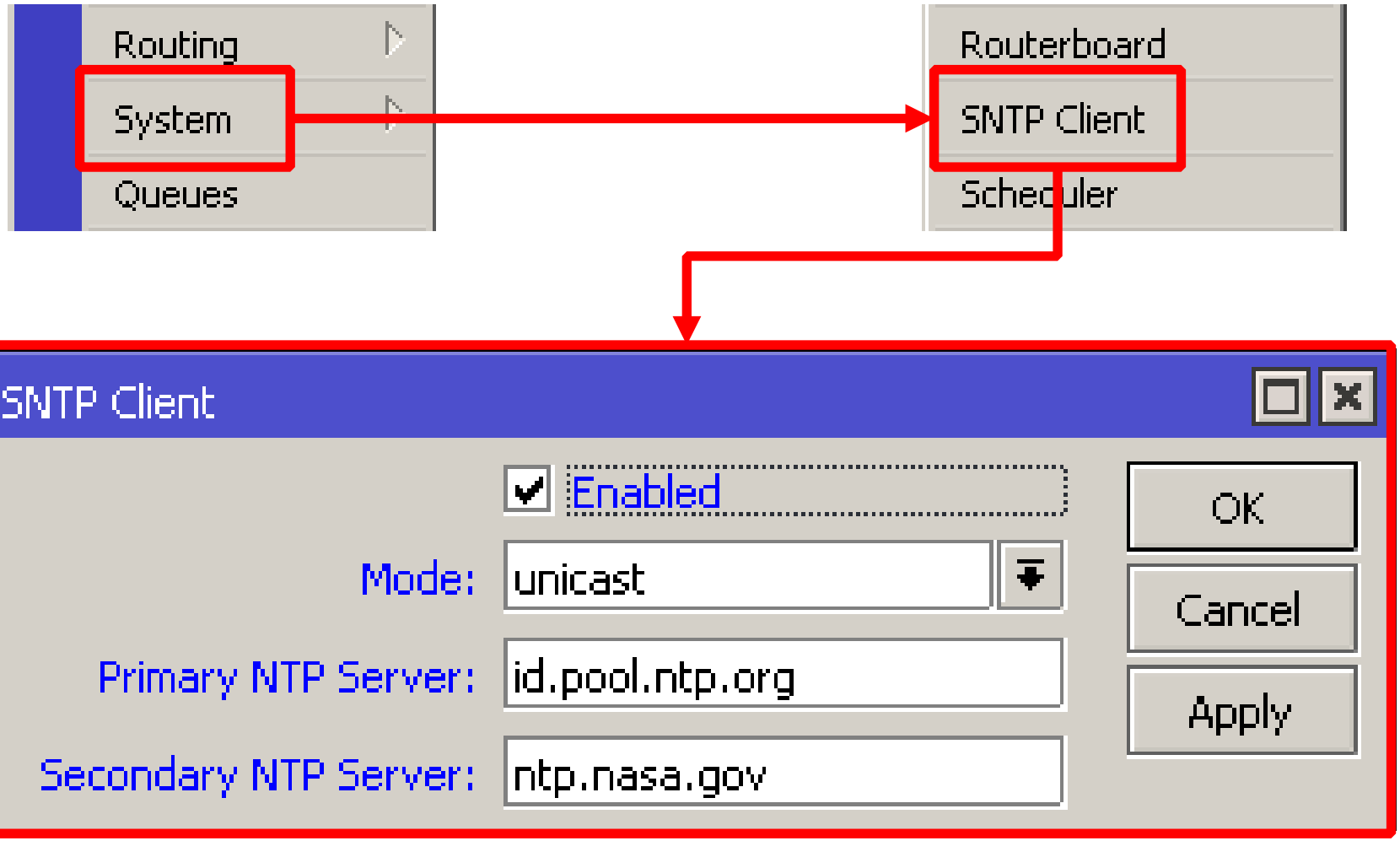
Installation Debug

- Test ping dari **Router** ke **Gateway** (10.10.10.100)
  - Jika error : Cek Wireless connection, Cek IP Address pada wlan1
- Test ping dari **Router** ke **Internet** (contoh: yahoo.com)
  - Jika error : Cek DNS Server Setting
- Test ping dari **Laptop** ke **Router** Anda (10.10.10.x)
  - Jika error : Cek konfigurasi laptop, Cek IP Address pada Ether1
- Test ping dari **Laptop** ke **Gateway** (10.10.10.100)
  - Jika error : Cek Firewall - NAT
- Test ping dari **Laptop** ke **Internet** (contoh: yahoo.com)
  - Jika error : Cek setting DNS pada laptop dan router

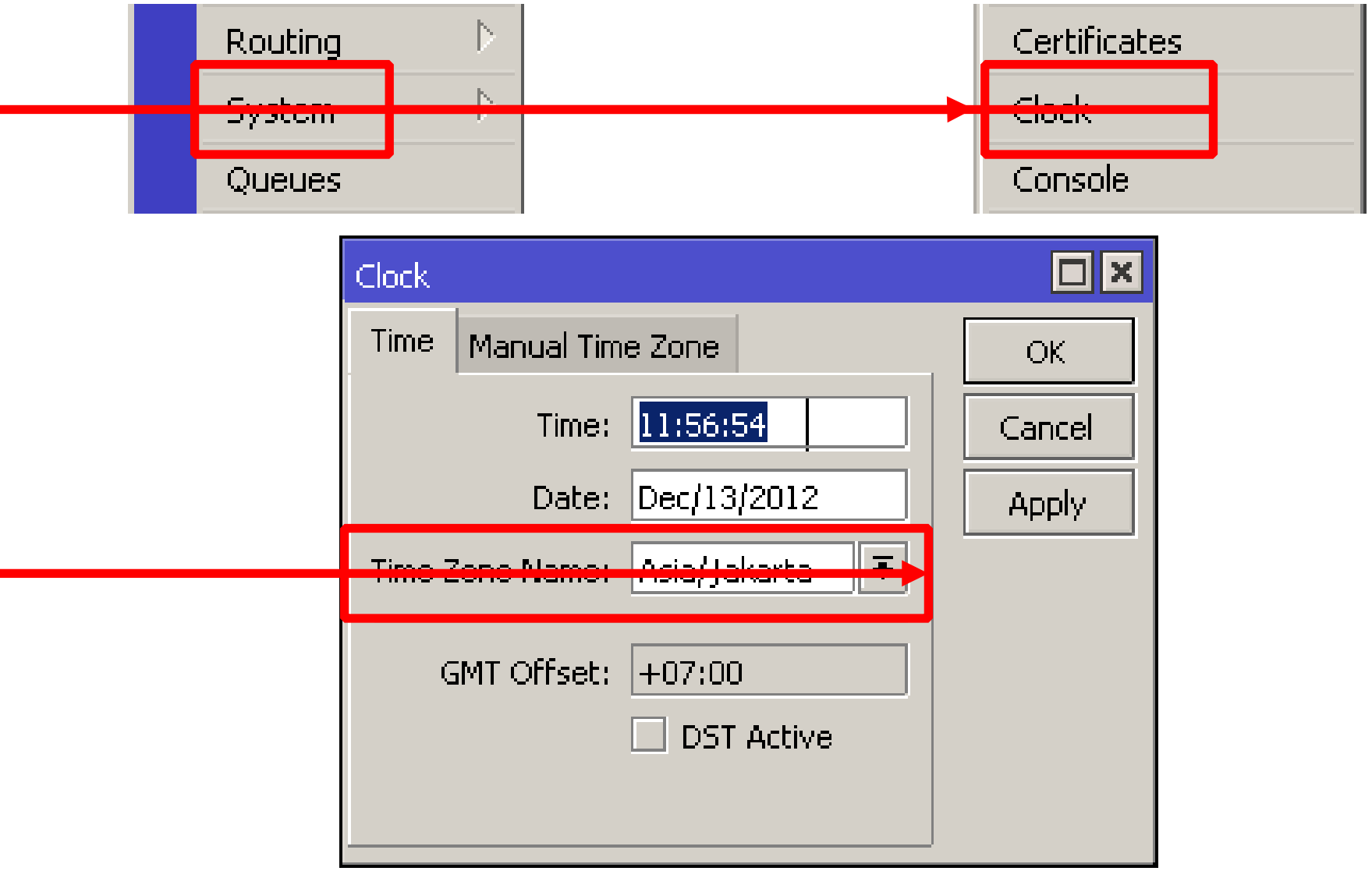
Network Time Protocol (NTP)

- NTP protocol memungkinkan sinkronisasi waktu dalam sebuah jaringan
- Mikrotik support sebagai NTP server dan sebagai NTP Client
- NTP Server
  - Install paket **ntp-xxxx-(versi).npk**, karena paket 'system' hanya menyertakan servis ntp client
  - Mode:**broadcast**,**manycast**,**multicast**
- NTP Client sudah builtin dalam package system

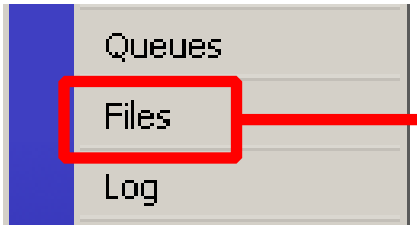
[LAB-7] NTP

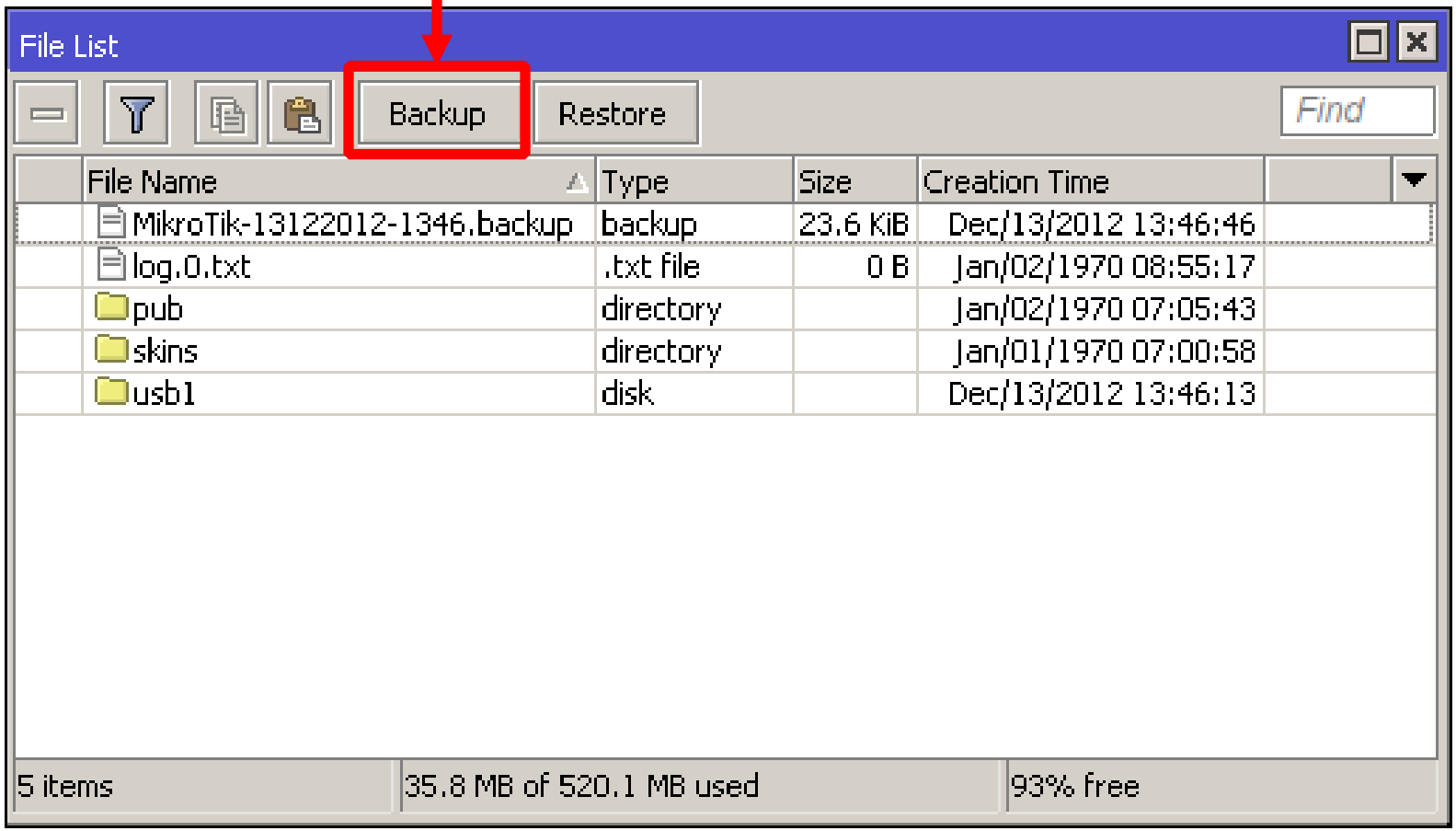

Routing
System
Queues
Routerboard
SNTP Client
Scheduler
SNTP Client
Enabled
Mode:
unicast
Primary NTP Server:
id.pool.ntp.org
Secondary NTP Server:
ntp.nasa.gov
OK
Cancel
Apply

System - Clock



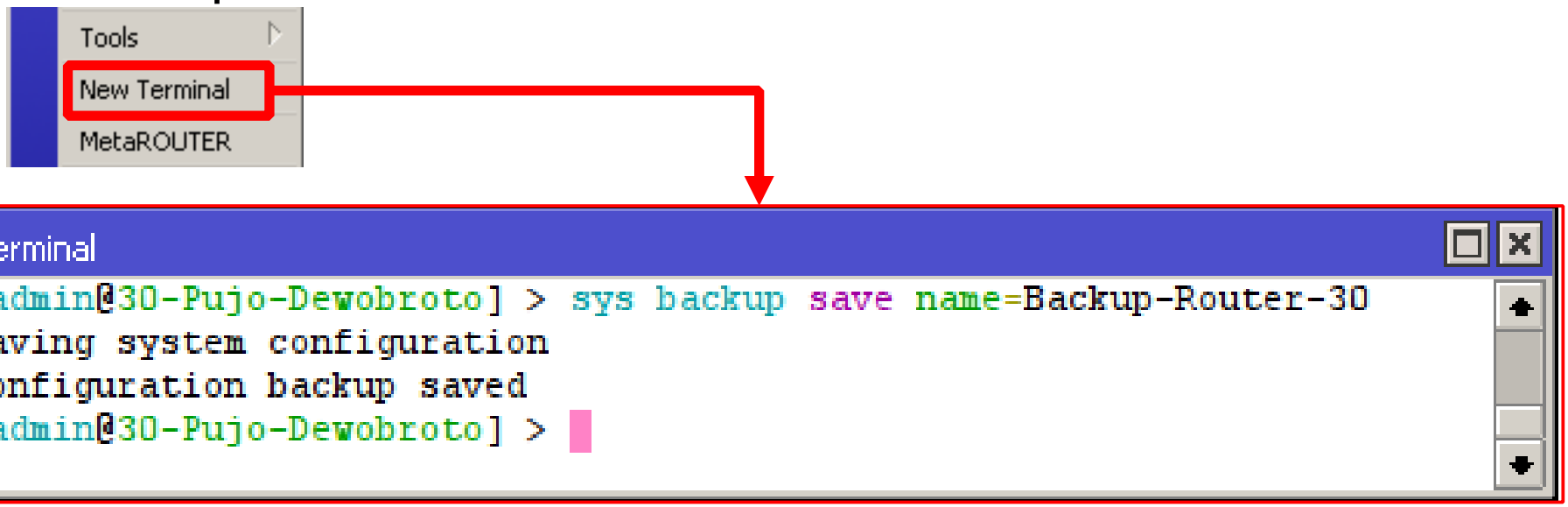
[LAB-8] Backup Config





Backup from CLI

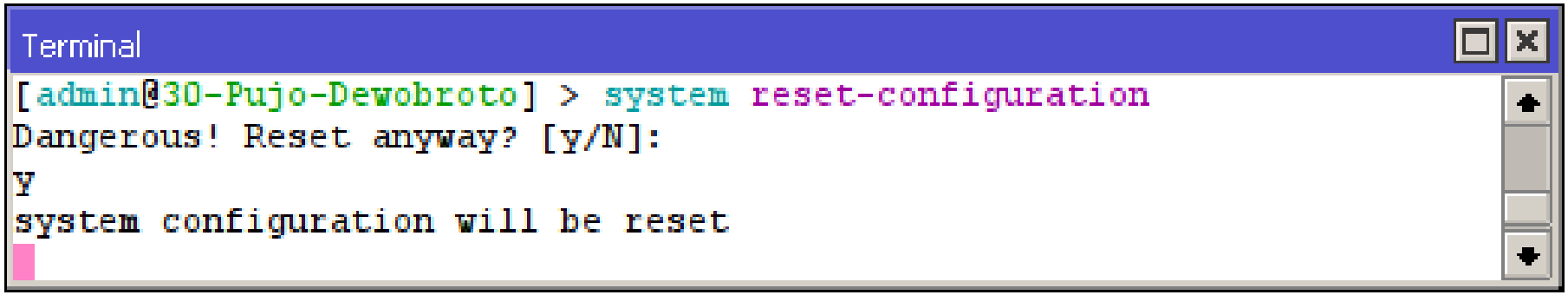
- Jika ingin menentukan nama file backup, bisa melakukan backup melalui new terminal



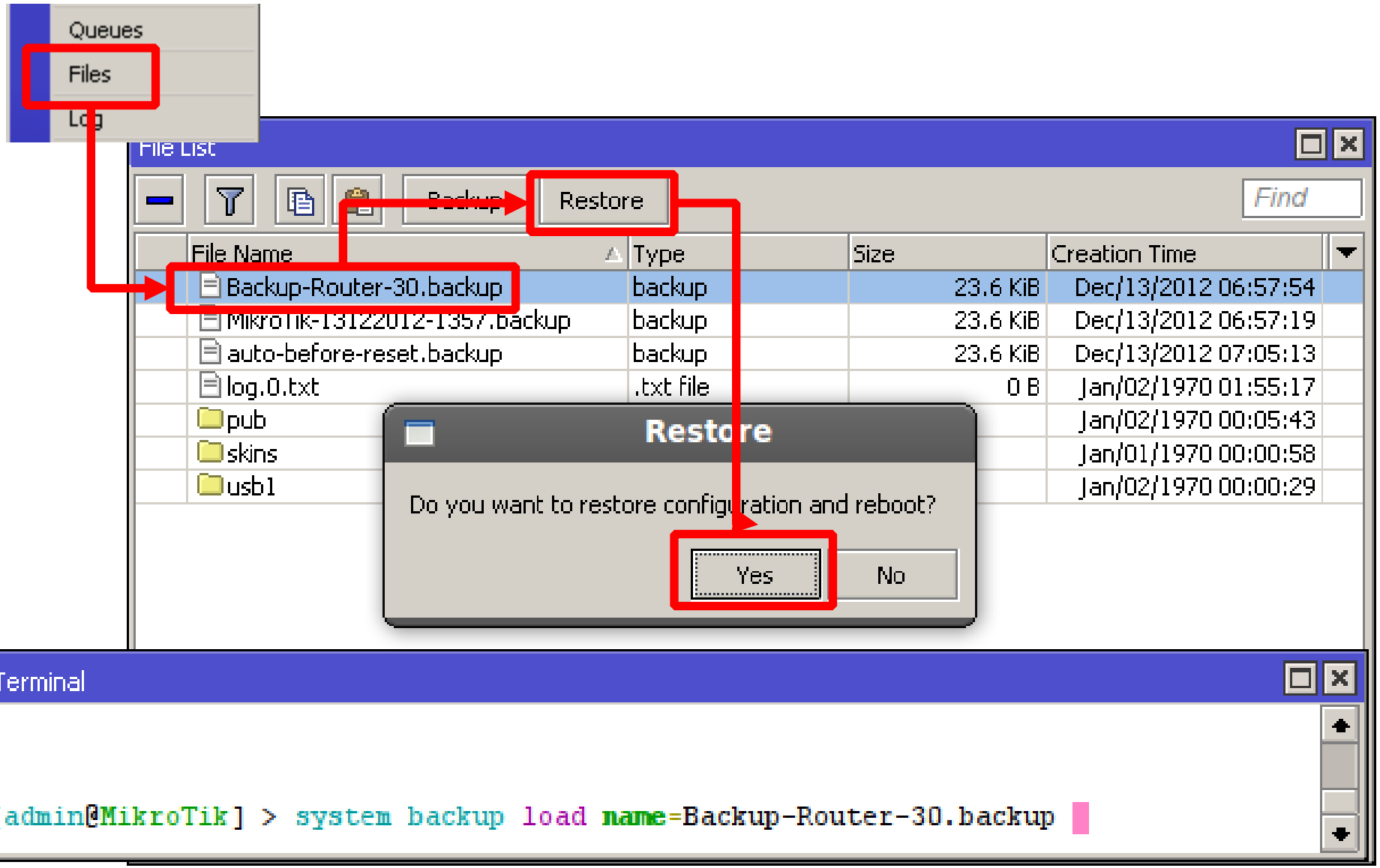
- File hasil backup dapat dilihat di menu file dan didownload via FTP
- File backup tidak dapat di-edit !

System Reset

- Untuk mengembalikan ke konfigurasi awal (default).
- Perintah ini menghapus semua konfigurasi yang telah dibuat, termasuk user dan password.
- Hanya bisa dilakukan oleh user dengan hak penuh (grup: full)



[LAB-9] Restore Configuration



Backup – Export Configuration

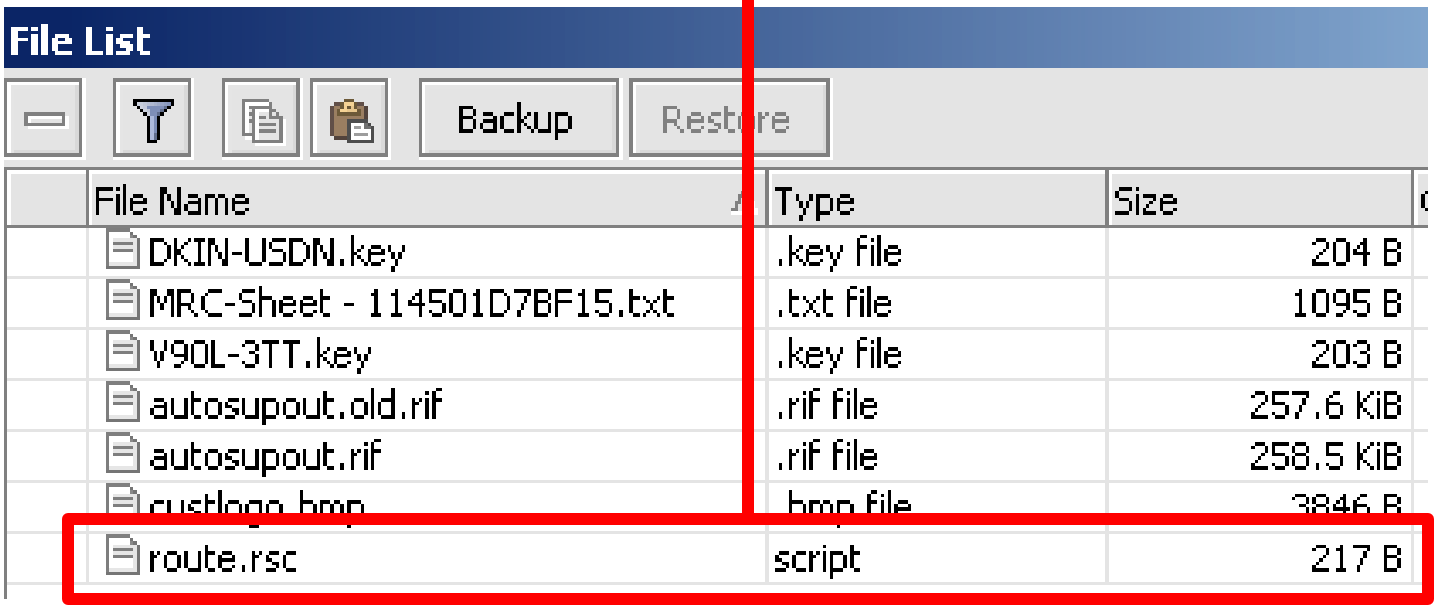
- Backup bisa dilakukan juga menggunakan perintah export.

```
[admin@MikroTik] > /ip route export
# jun/30/2011 10:16:16 by RouterOS 4.6
# software id = DKIN-USDN
#
/ip route
add comment="rrr" disabled=no distance=1 dst-address=0.0.0.0/0 \
    gateway=192.168.5.1 pref-src=192.168.5.201 scope=30 \
    target-scope=10
[admin@MikroTik] >
```

Backup – Export to File

- Hasil export ini berupa script (text base configuration) yang bisa dilihat dan diedit menggunakan text editor.

```
[admin@MikroTik] > /ip route export file=route.rsc
[admin@MikroTik] >
```



Restore – Import Script

- File script bisa langsung di restore ke router

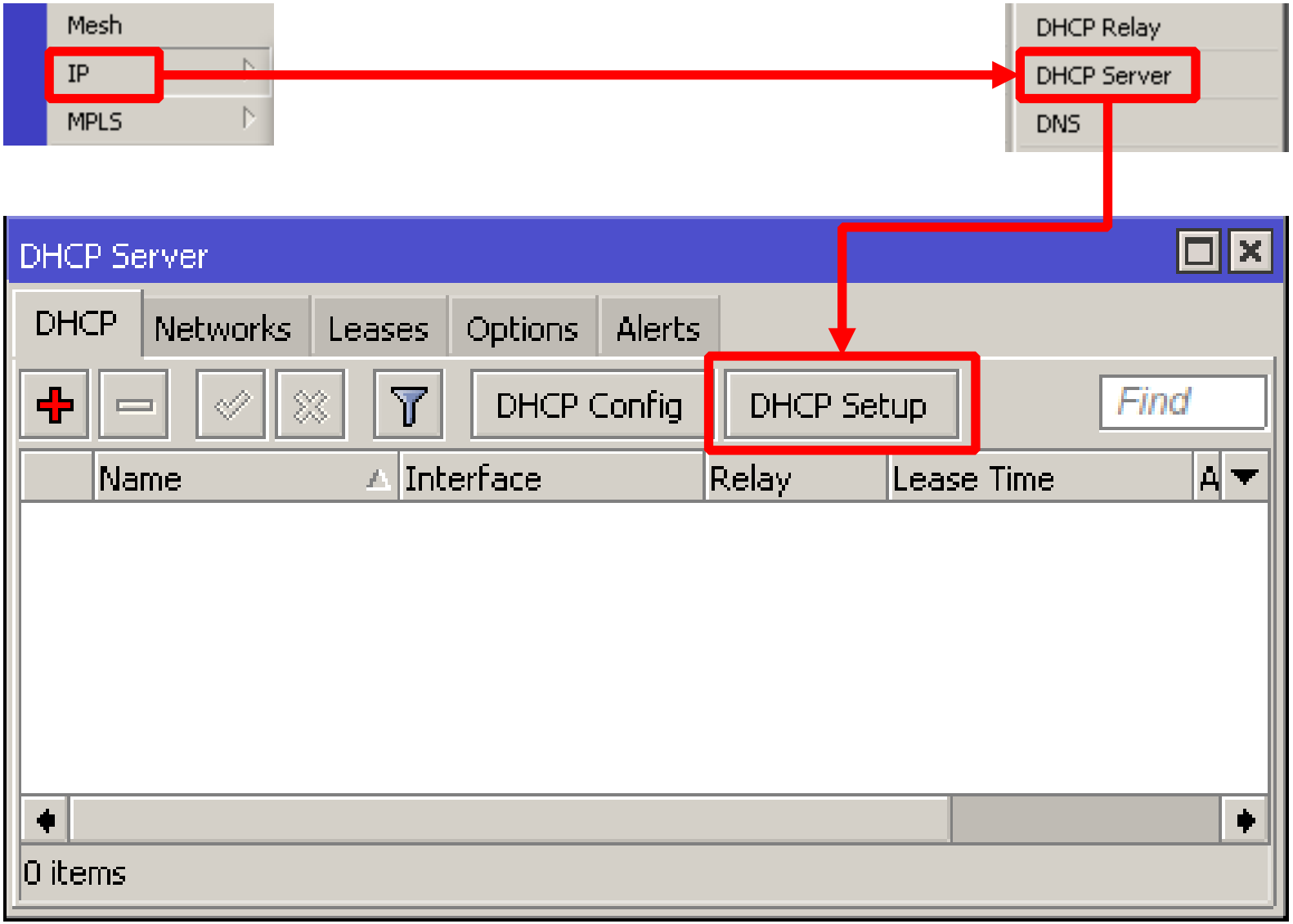
```
MMM       MMM        KKK                                TTTTTTTTTTT      KKK
MMMM     MMMM        KKK                                TTTTTTTTTTT      KKK
MMM MMMM MMM   III   KKK  KKK   RRRRRR     000000        TTT      III   KKK  KKK
MMM  MM  MMM   III   KKKKK      RRR  RRR   000  000      TTT      III   KKKKK
MMM      MMM   III   KKK KKK    RRRRRR     000  000      TTT      III   KKK KKK
MMM      MMM   III   KKK  KKK   RRR  RRR    000000      TTT      III   KKK  KKK

MikroTik RouterOS 4.6 (c) 1999-2010       http://www.mikrotik.com/
```

```
[admin@MikroTik] > import route.rsc
Opening script file route.rsc

Script file loaded and executed successfully
[admin@MikroTik] >
```

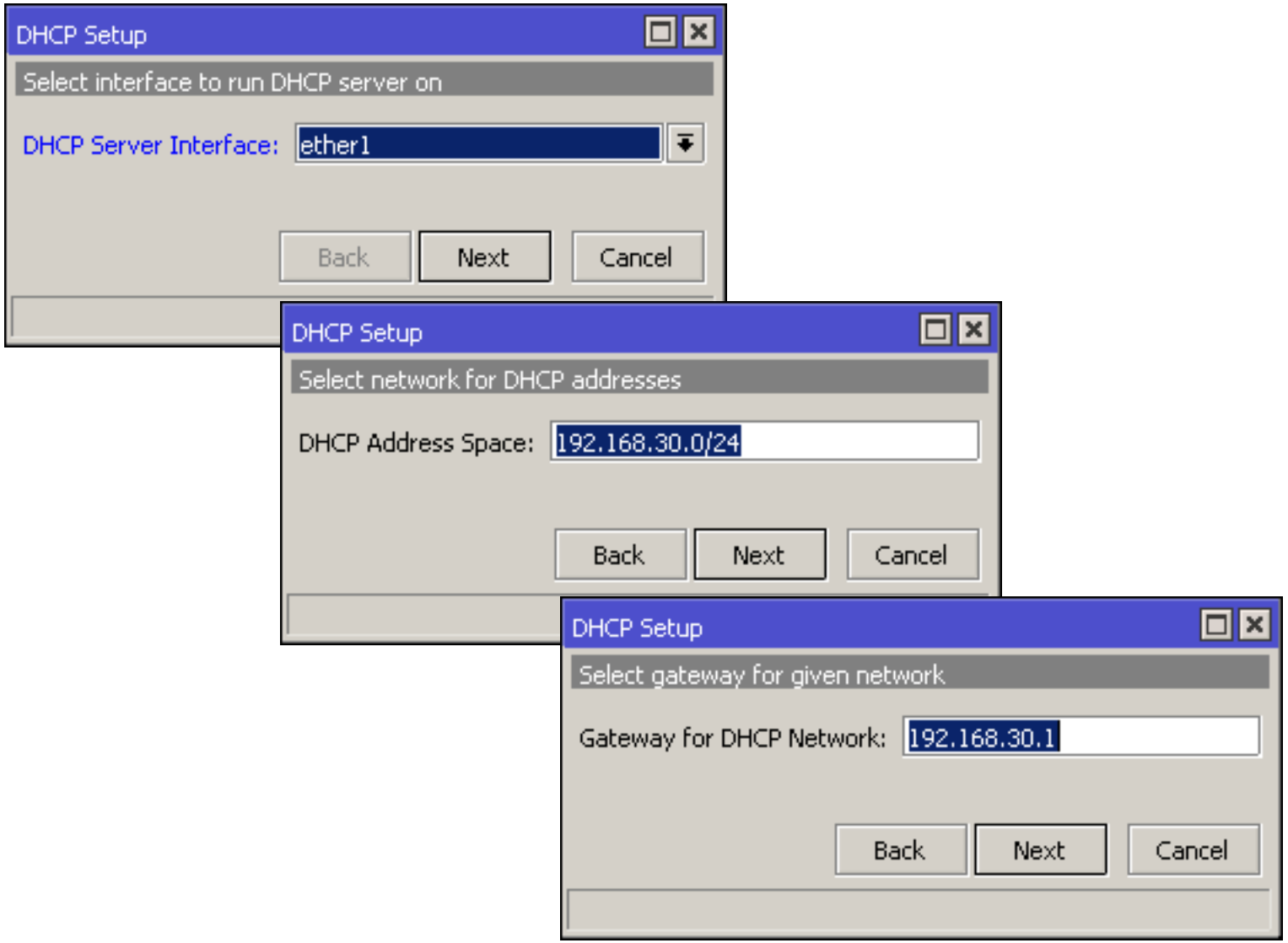
DHCP Server

- Dynamic Host Configuration Protocol digunakan untuk secara dinamik mendistribusikan konfigurasi jaringan, seperti:
  - IP Address dan netmask
  - IP Address default gateway
  - Konfigurasi DNS dan NTP Server
  - Dan masih banyak lagi custom option (tergantung apakah DHCP client bisa support)

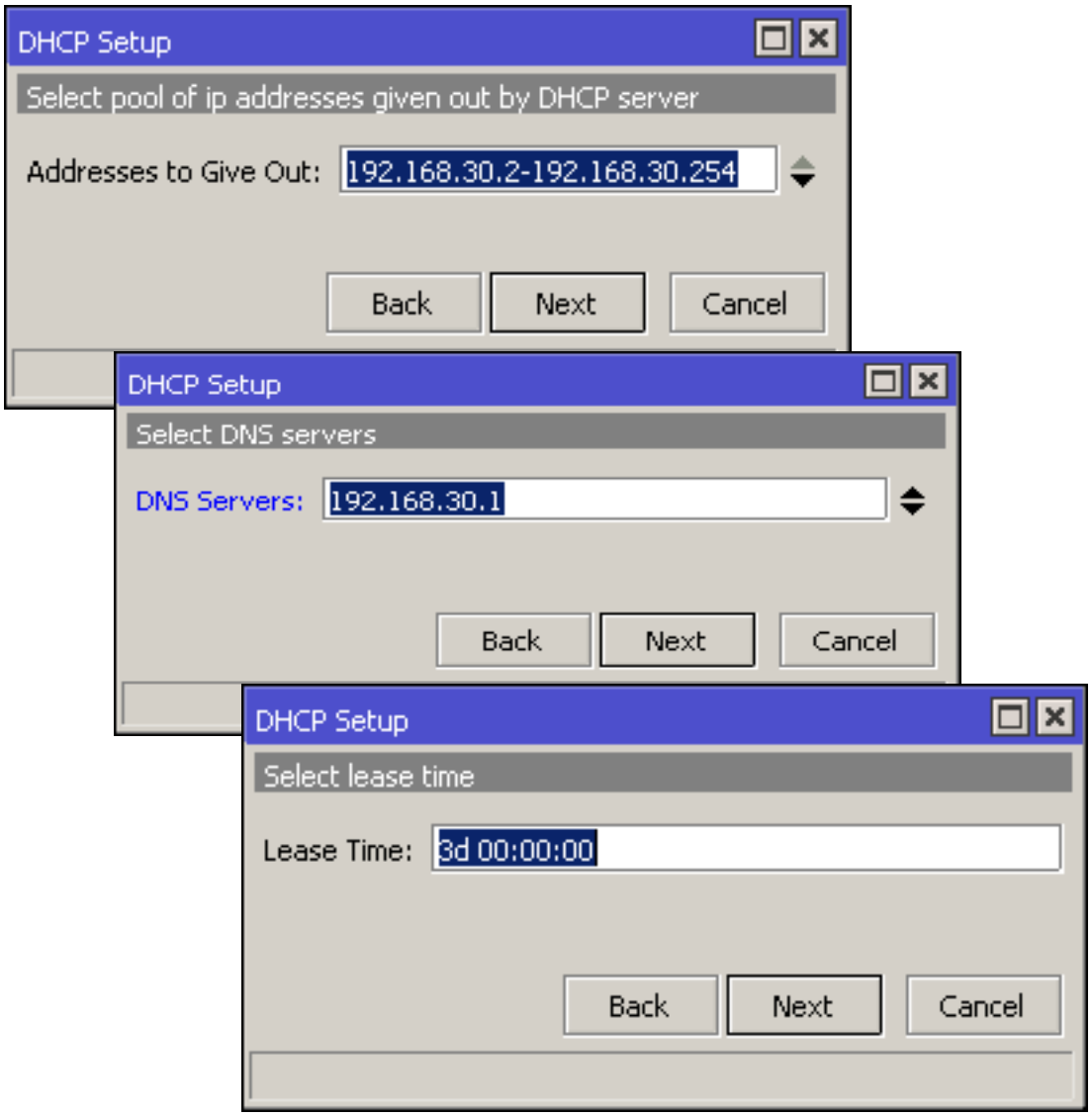
[LAB-10] DHCP Server (1)

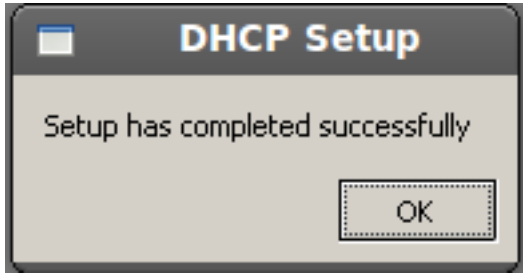


[LAB-10] DHCP Server (2)



[LAB-10] DHCP Server (3)





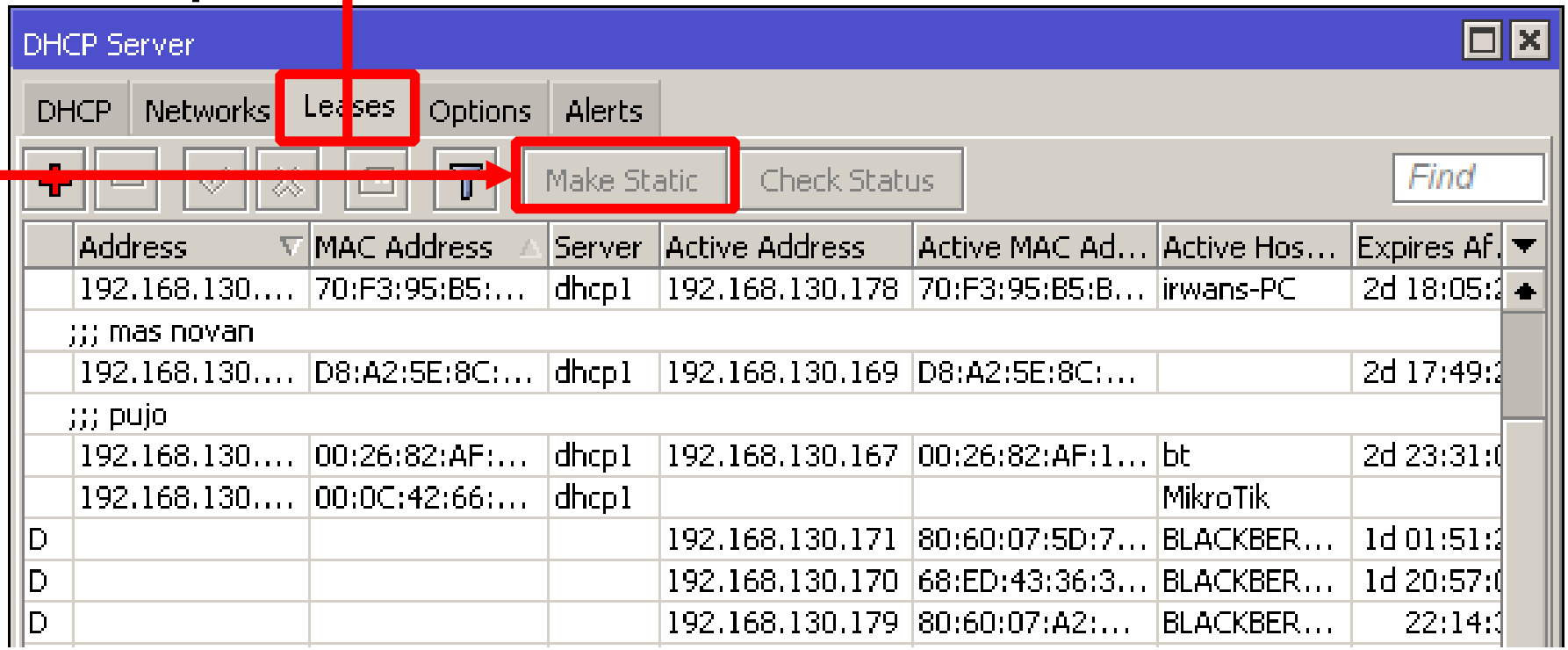
Terminal – DHCP Server Wizard

- Konfigurasi DHCP-Server setup
  - /ip dhcp-server setup
  - dhcp server interface: ether1
  - dhcp address space: 192.168.x.0/24
  - gateway for dhcp network: 192.168.x.1
  - dhcp relay: none
  - addresses to give out: 192.168.x.10-192.168.x.20
  - dns servers: 192.168.x.1
  - lease time: 3d

DHCP Test

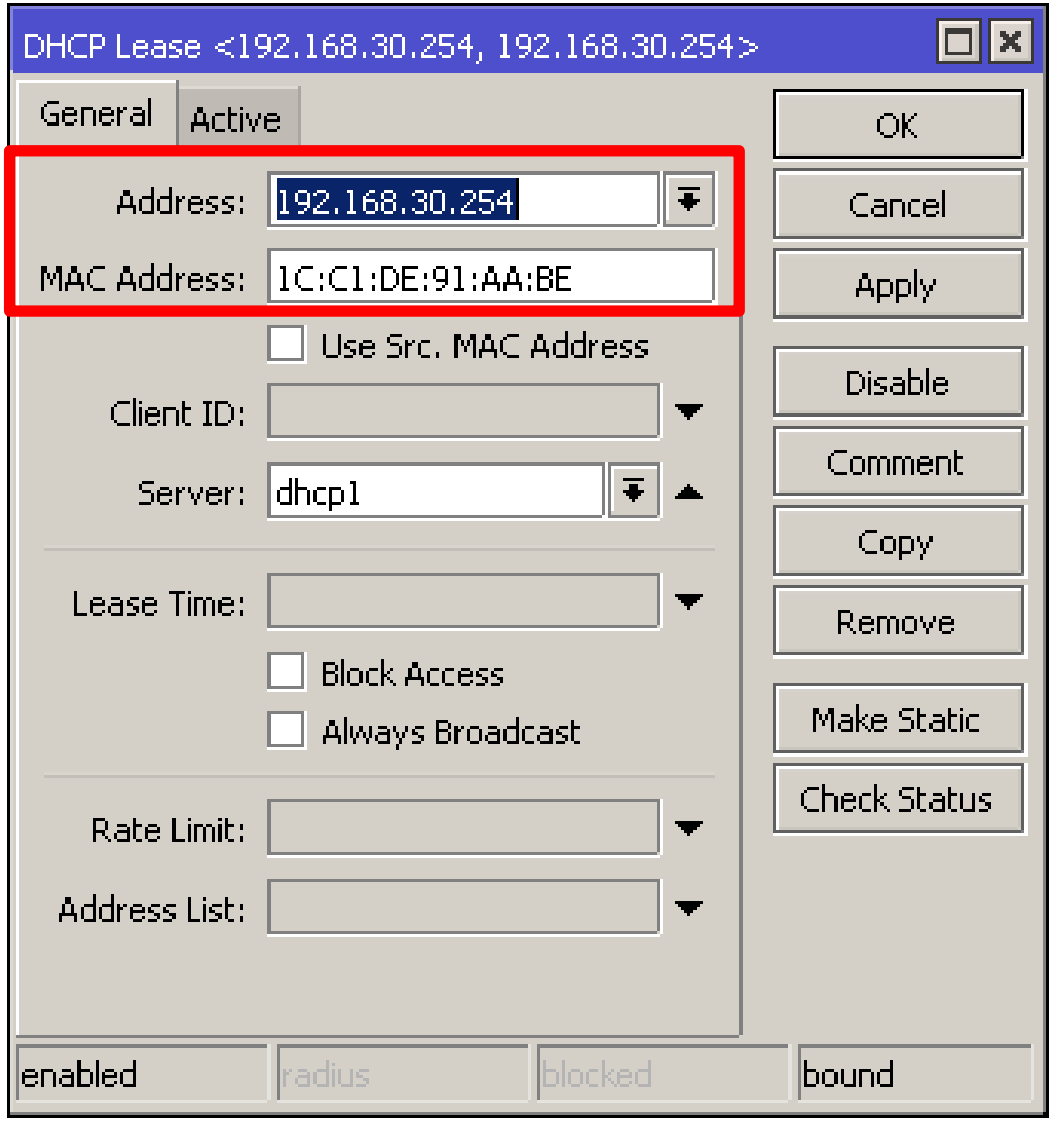
- Ubahlah konfigurasi IP Address dan DNS pada laptop menjadi otomatis
- Cek pada laptop apakah sudah mendapatkan alokasi IP Address dari DHCP
  - **C:\ ipconfig [enter]**
- Cobalah melakukan koneksi internet

DHCP Management



- Daftar DHCP client yang aktif terlihat pada menu **DHCP-Server – Leasses**
- Untuk membuat IP Address tertentu hanya digunakan oleh Mac Address tertentu, bisa menggunakan **DHCP-Statik**

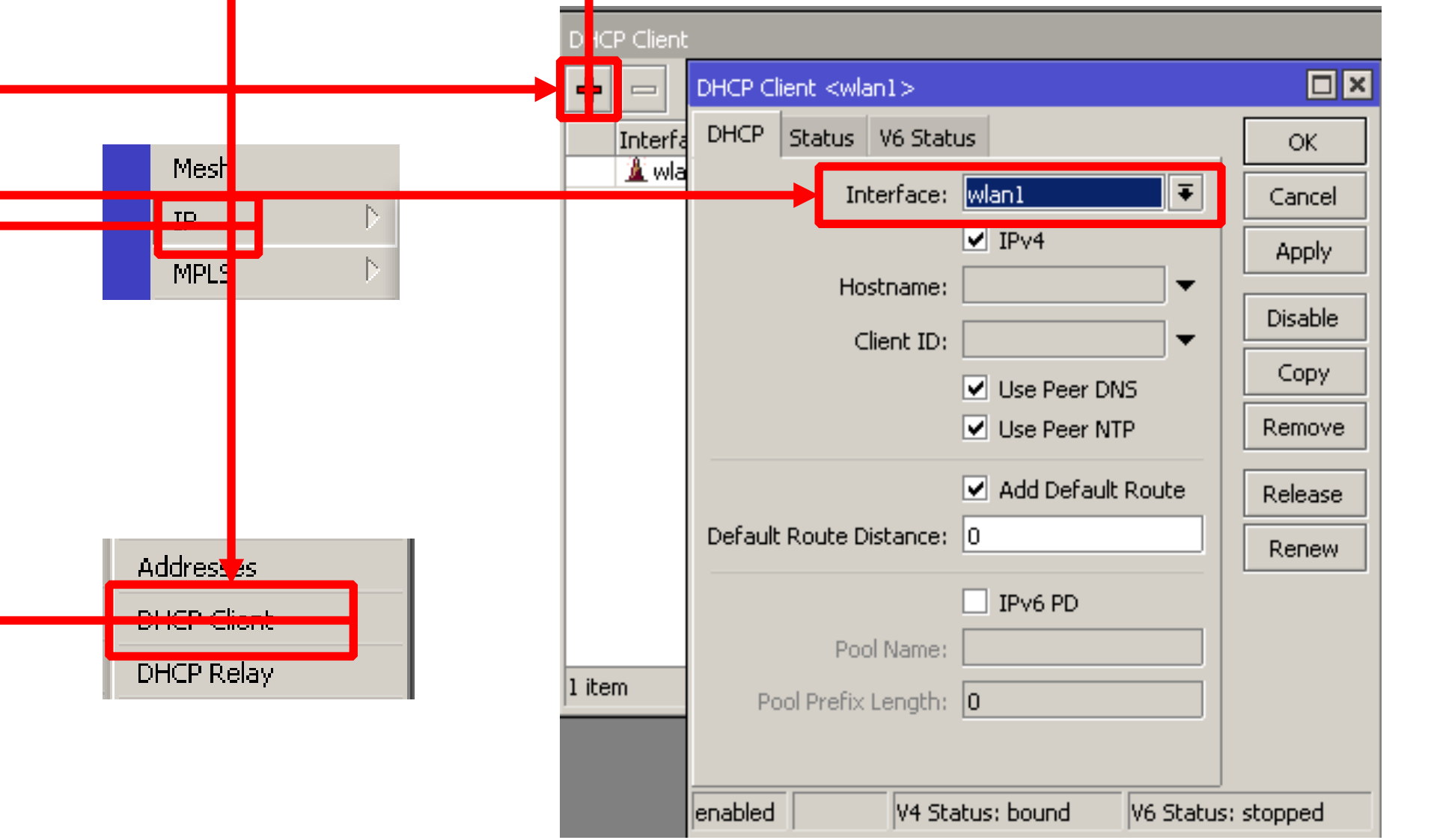
DHCP Static


DHCP Lease <192.168.30.254, 192.168.30.254>
General
Active
Address: 192.168.30.254
MAC Address: 1C:C1:DE:91:AA:BE
Use Src. MAC Address
Client ID:
Server: dhcp1
Lease Time:
Block Access
Always Broadcast
Rate Limit:
Address List:
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Make Static
Check Status
enabled
radius
blocked
bound

DHCP Client

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

[LAB-11] DHCP Client



DHCP Client (1)

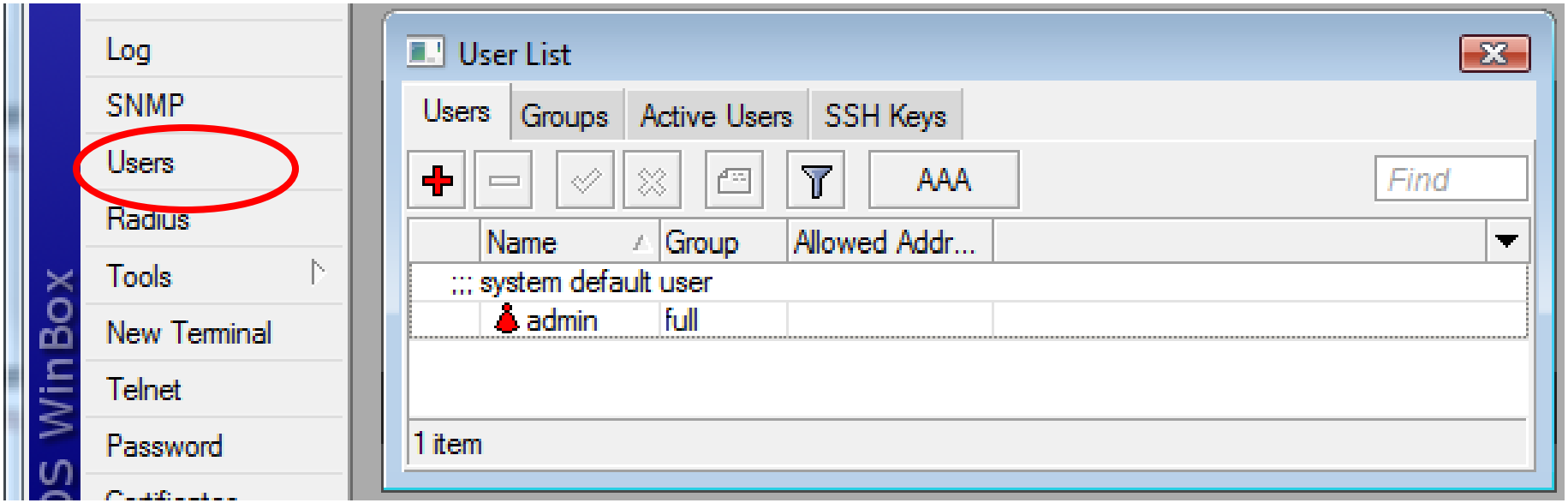
- **Interface**
  - Pilihlah interface yang sesuai yang terkoneksi ke DHCP Server
- **Host name** *(tidak harus diisi)*
  - Nama DHCP client yang akan dikenali oleh DHCP Server
- **Client ID** *(tidak harus diisi)*
  - Biasanya merupakan mac-address interface yang kita gunakan, apabila proses DHCP di server menggunakan sistem radius

DHCP Client (2)

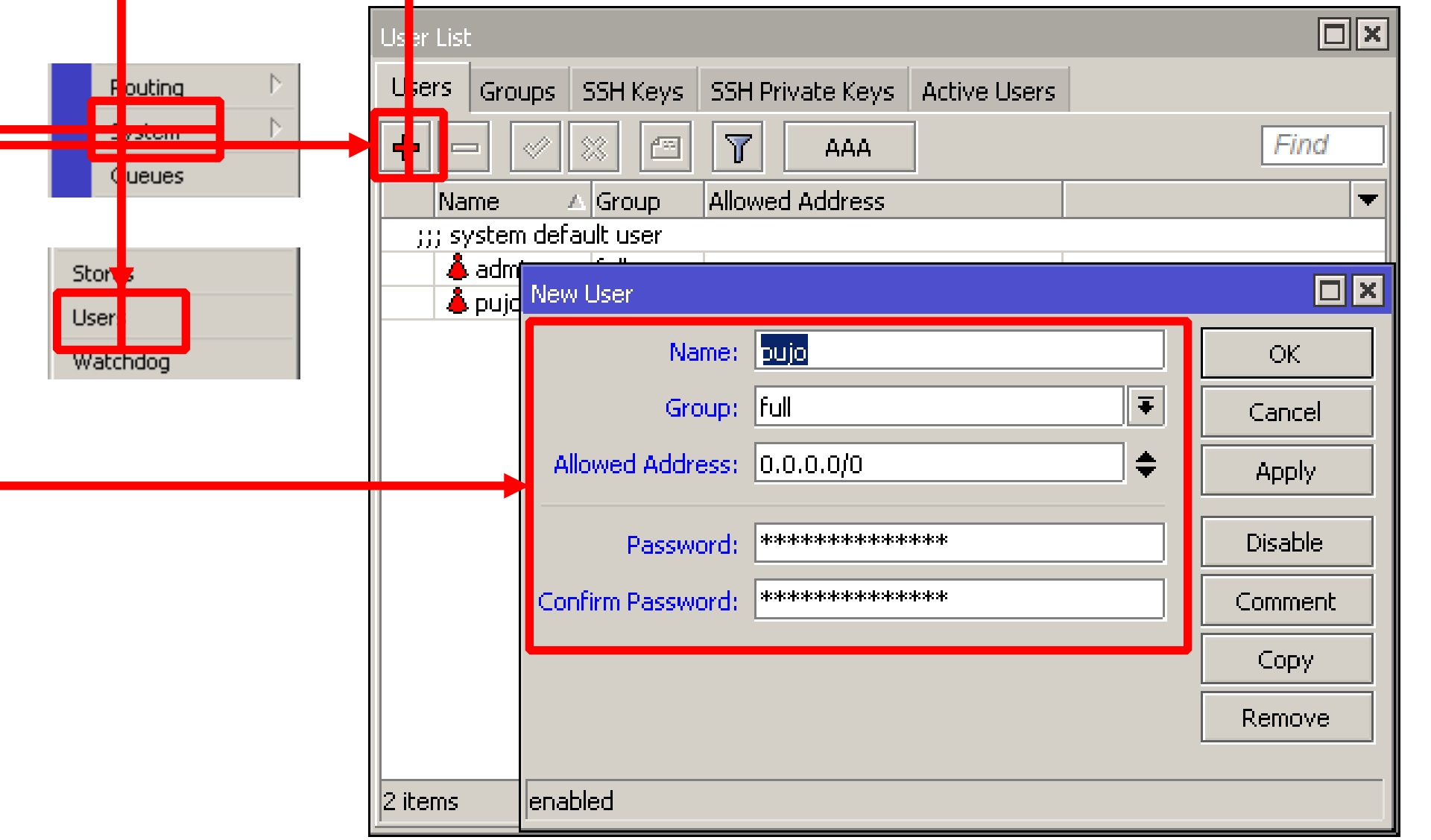
- **Add default route**
  - Bila kita menginginkan default route kita mengarah sesuai dengan informasi DHCP
- **Use Peer DNS**
  - Bila kita hendak menggunakan DNS server sesuai dengan informasi DHCP
- **Use Peer NTP**
  - Bila kita hendak menggunakan informasi pengaturan waktu di router (NTP) sesuai dengan informasi dari DHCP
- **Default route distance**
  - Menentukan prioritas routing jika terdapat lebih dari satu DHCP Server yang digunakan. Routing akan melalui distance yang lebih kecil

Internal User RouterOS

- Secara default, akan ada user admin dengan password [kosong]

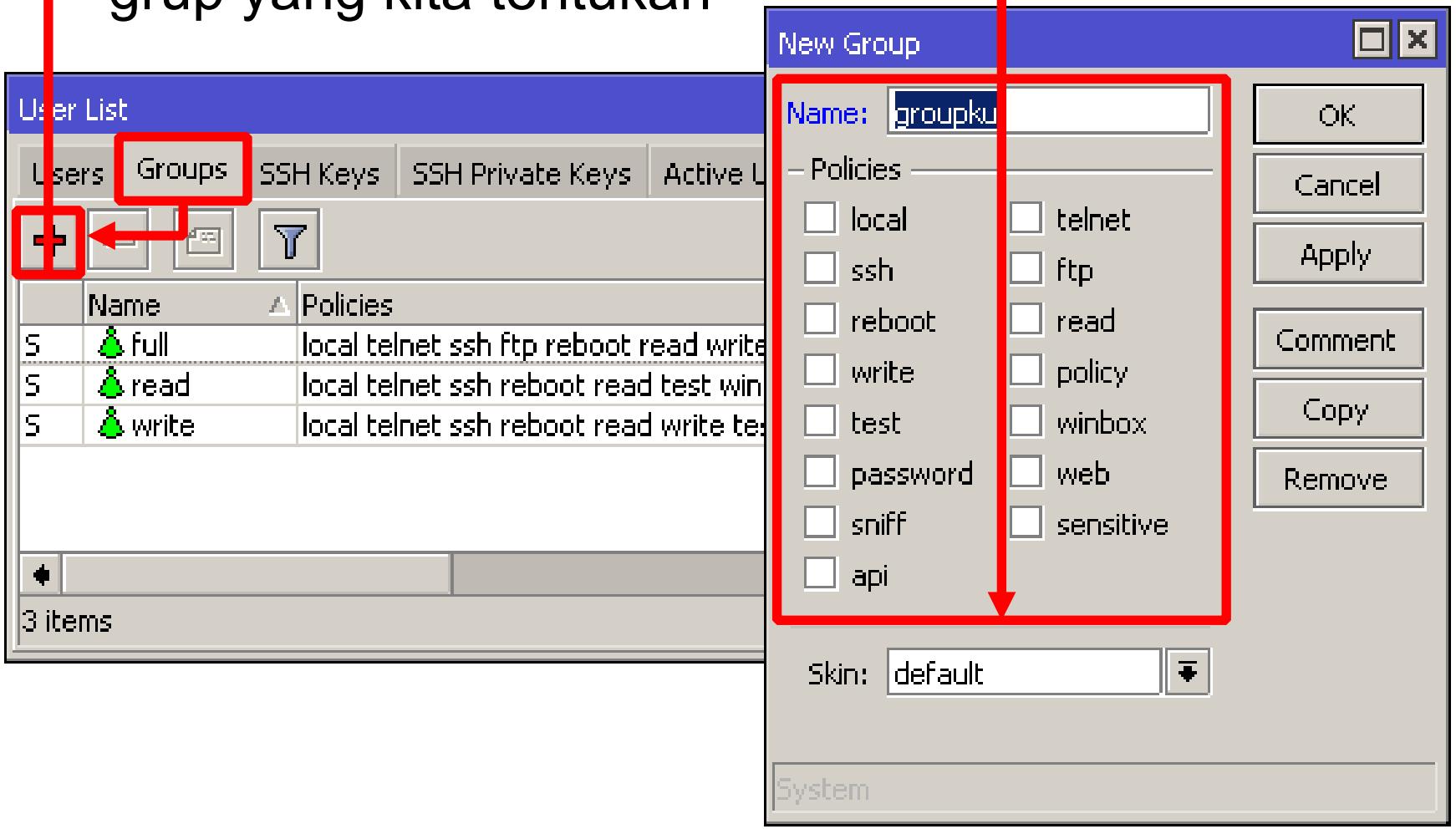


RouterOS User Add



Internal User Groups

- User dapat dikategorikan hak nya berdasarkan grup yang kita tentukan



About User

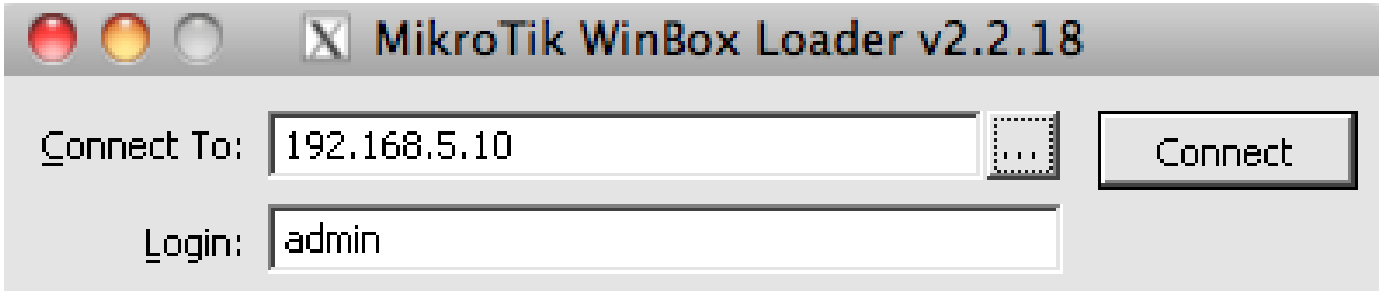
- Buatlah user baru yang memiliki hak penuh dan non aktifkan user “**admin**”
- Untuk teknisi bisa diberikan grup **write** (bukan **full**) sehingga kita masih memiliki hak penuh terhadap router kita
- Untuk pemantauan, bisa menggunakan user dengan grup **read**

[LAB-12] Internal User

- Buat user tambahan untuk rekan semeja anda
- Buat grup beserta hak yang dimiliki
- Tentukan juga address yang diijinkan untuk mengakses router

Access to Router (IP Base)

- **IP-Winbox**
- **Telnet**
- **SSH**
- **WebFig**

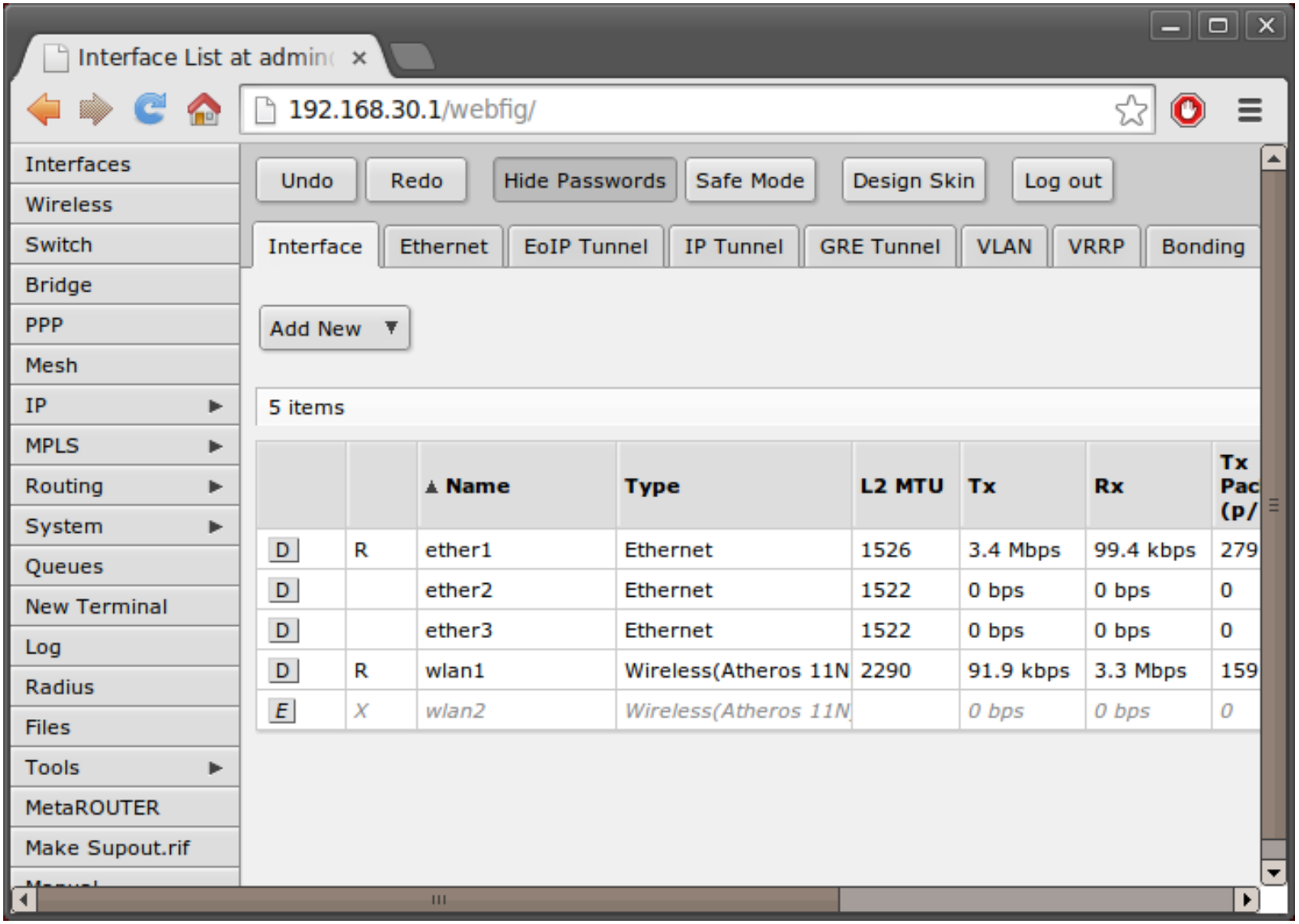



```
Novan-Chriss-MacBook-Pro:~ novan$ telnet 192.168.5.10
Trying 192.168.5.10...
Connected to 192.168.5.10.
Escape character is '^]'.
Password:
```

Access to Router - WebFig

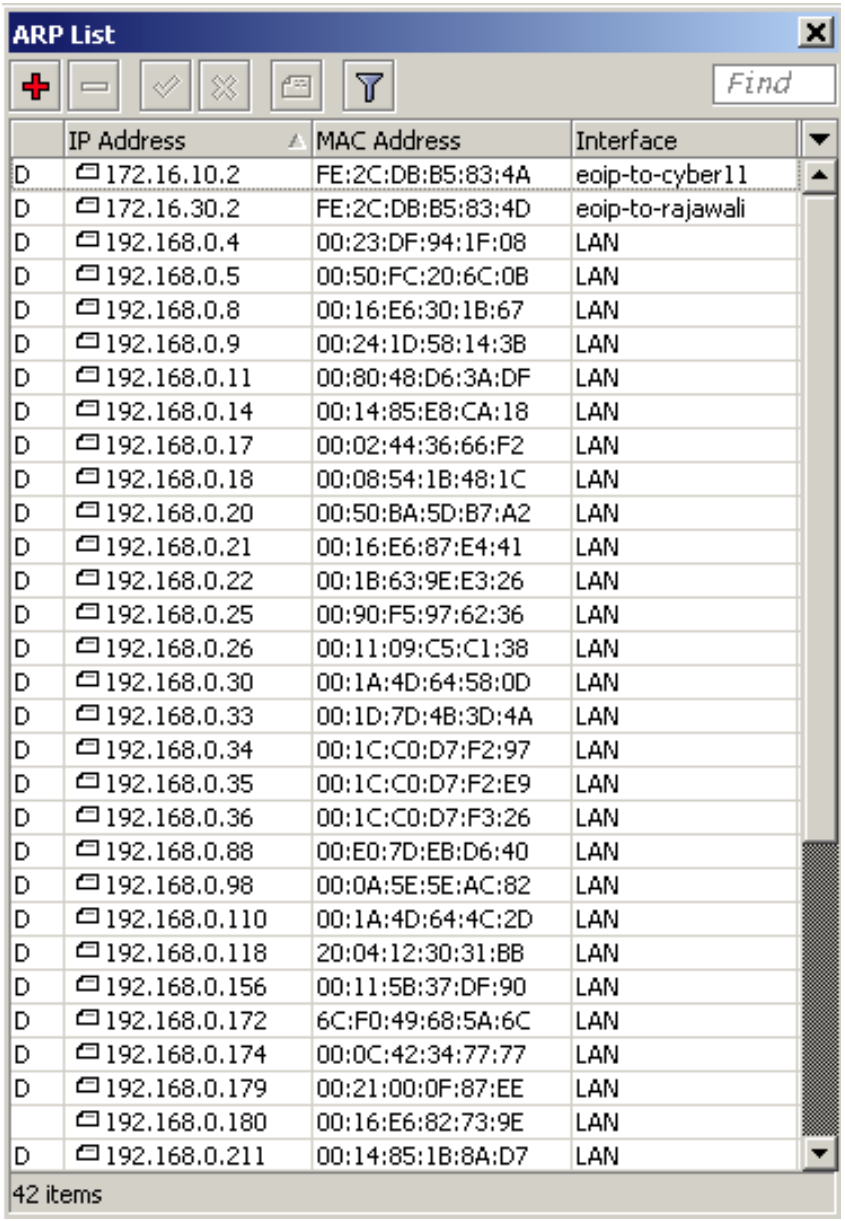
- Konfigurasi realtime berbasis Web memungkinkan konfigurasi mikrotik menggunakan perangkat mobile
- Webfig bisa diakses dengan memasukkan IP router didalam address bar browser

Access to Router - WebFig



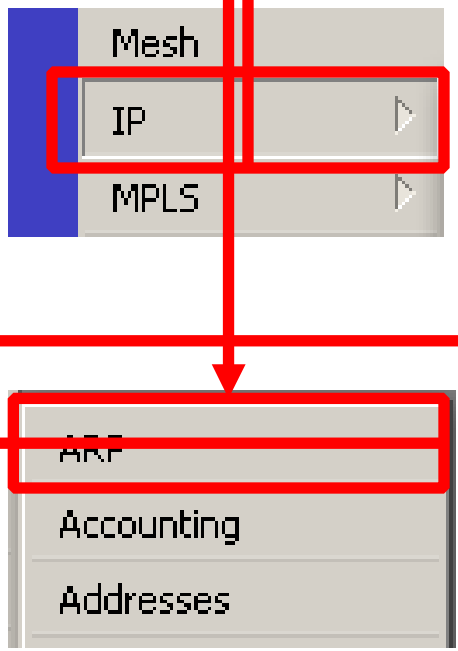
ARP Table

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



Address Resolution Protocol

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



ARP List

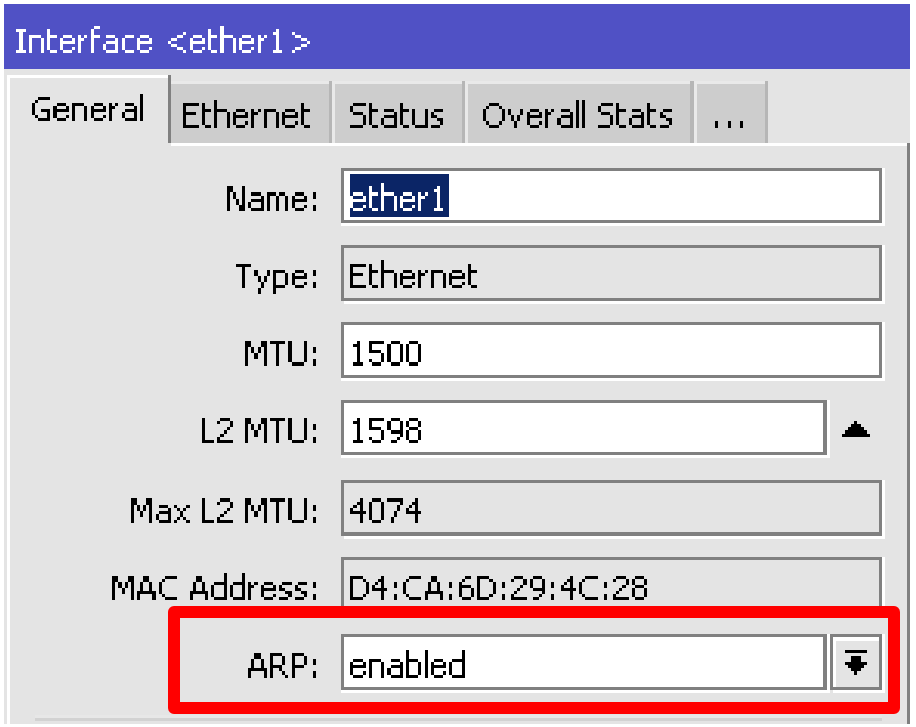
Find

	IP Address	MAC Address	Interface
D	192.168.0.6	00:08:9B:8C:8F:0C	ether1
D	192.168.130.3	00:0C:42:33:89:37	vlan1
D	192.168.130.4	00:0C:42:34:77:7E	vlan1
D	192.168.130.2	00:0C:42:91:D3:D3	vlan1
D	10.31.31.1	00:0C:42:9E:D0:71	ether1
D	192.168.130.35	00:0C:42:A5:94:DD	vlan2
D	192.168.130.36	00:15:65:26:14:88	vlan2
D	192.168.130.37	00:15:65:26:16:46	vlan2
D	192.168.130.55	00:1C:C0:E9:F9:5C	vlan2
D	192.168.0.5	00:60:E0:4E:7C:63	ether1
D	192.168.130.39	00:80:91:45:98:A9	vlan2
D	192.168.0.100	02:5E:71:2F:18:63	ether1
D	192.168.130.52	3C:D9:2B:21:C4:A8	vlan2
D	192.168.130.61	9C:8E:99:48:F6:14	vlan2
D	192.168.130.62	9C:8E:99:48:F6:1C	vlan2

16 items

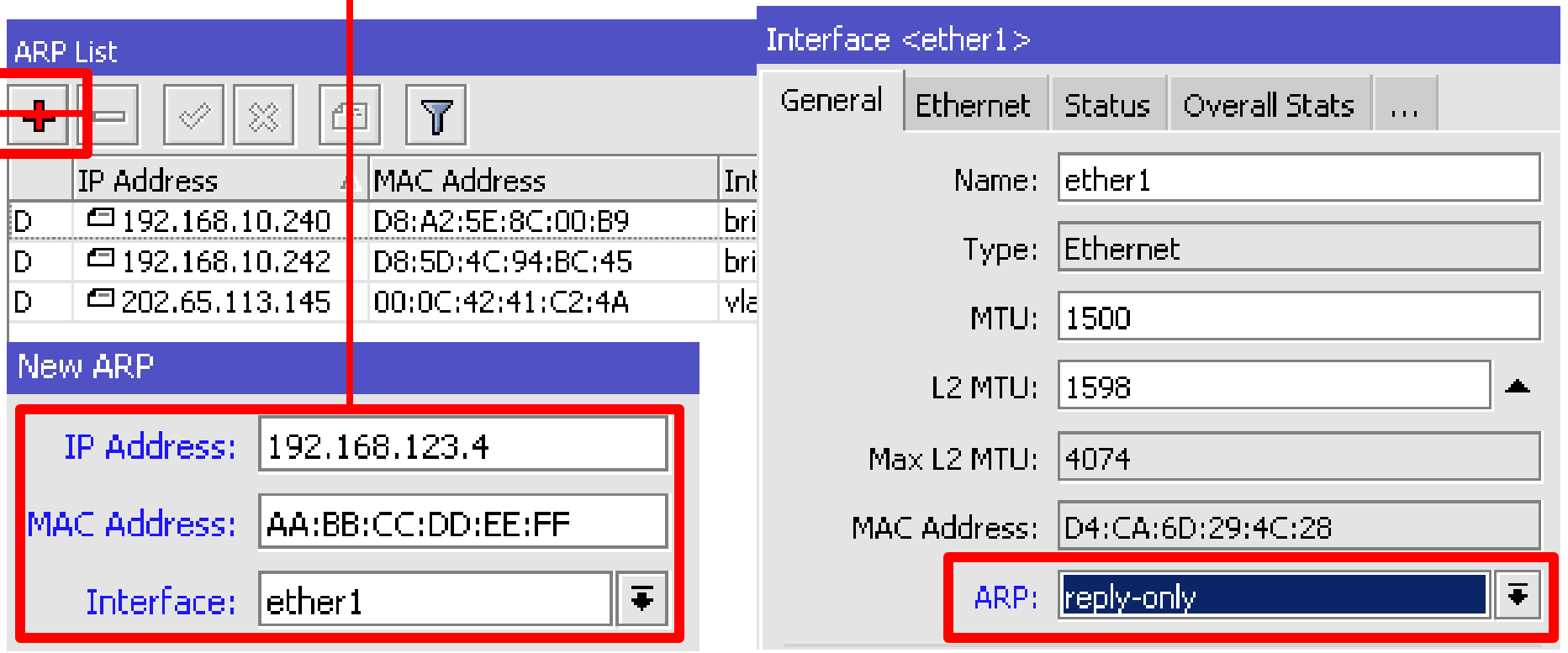
ARP Protocol

- ARP protocol secara “default” aktif di setiap interface.
- ARP = Enabled – menandakan Interface akan mengupdate tabel ARP secara otomatis



ARP – Security !

- ARP = Reply-only – menandakan ARP protocol pada interface tidak mengupdate data di ARP table secara otomatis.



Monitoring - Ping

- Tool monitoring
  - Ping
    - Ping uses Internet Control Message Protocol (ICMP) Echo messages to determine if a remote host is active or inactive and to determine the round-trip delay when communicating with it.

      [user1@MKI] > ping 192.168.0.100

      192.168.0.100 64 byte ping: ttl=64 time=1 ms

      192.168.0.100 64 byte ping: ttl=64 time=1 ms

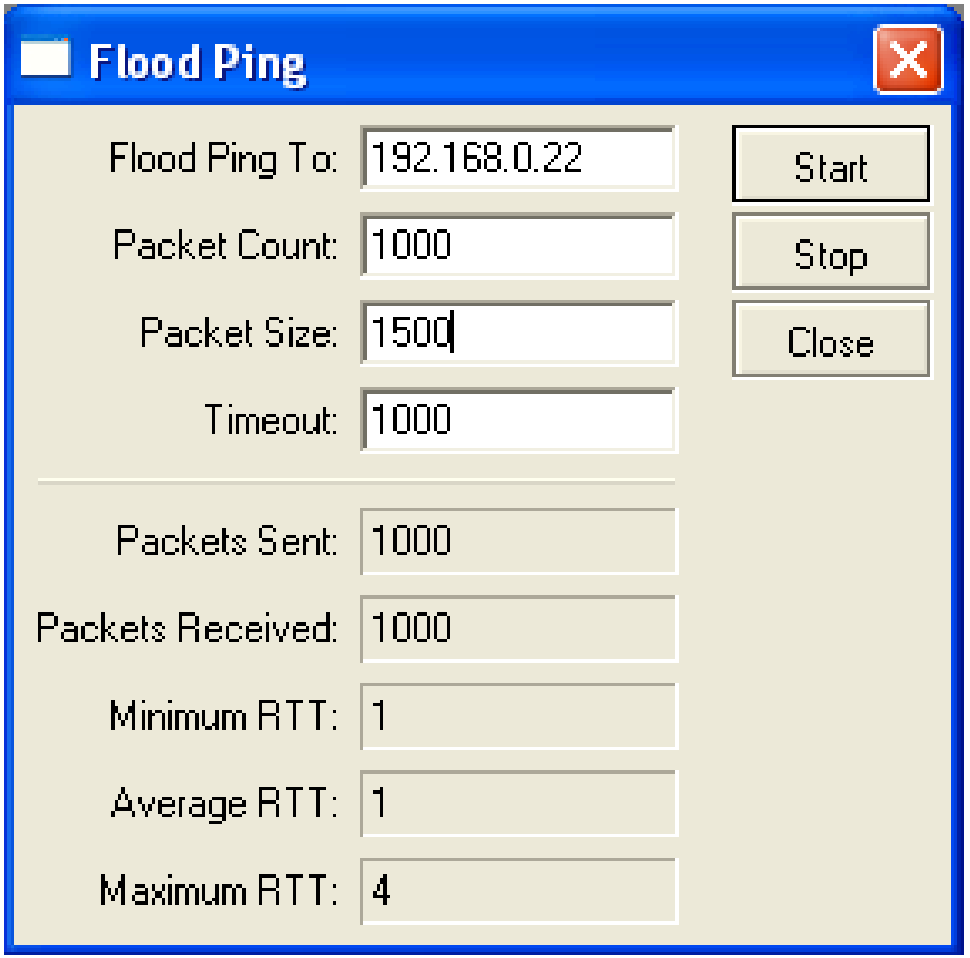
      192.168.0.100 64 byte ping: ttl=64 time=1 ms

      3 packets transmitted, 3 packets received, 0% packet loss

      round-trip min/avg/max = 1/1.0/1 ms

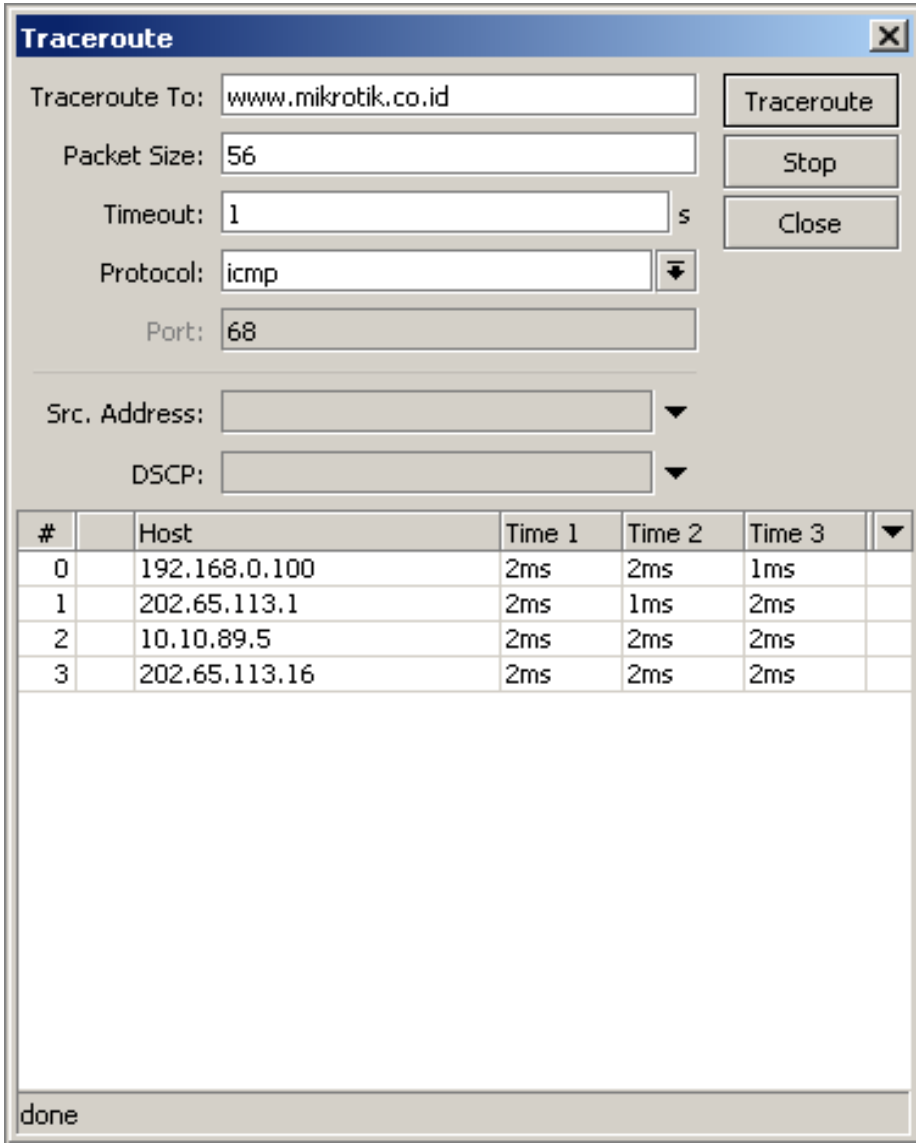
Monitoring – Ping Flood

- Flood Ping



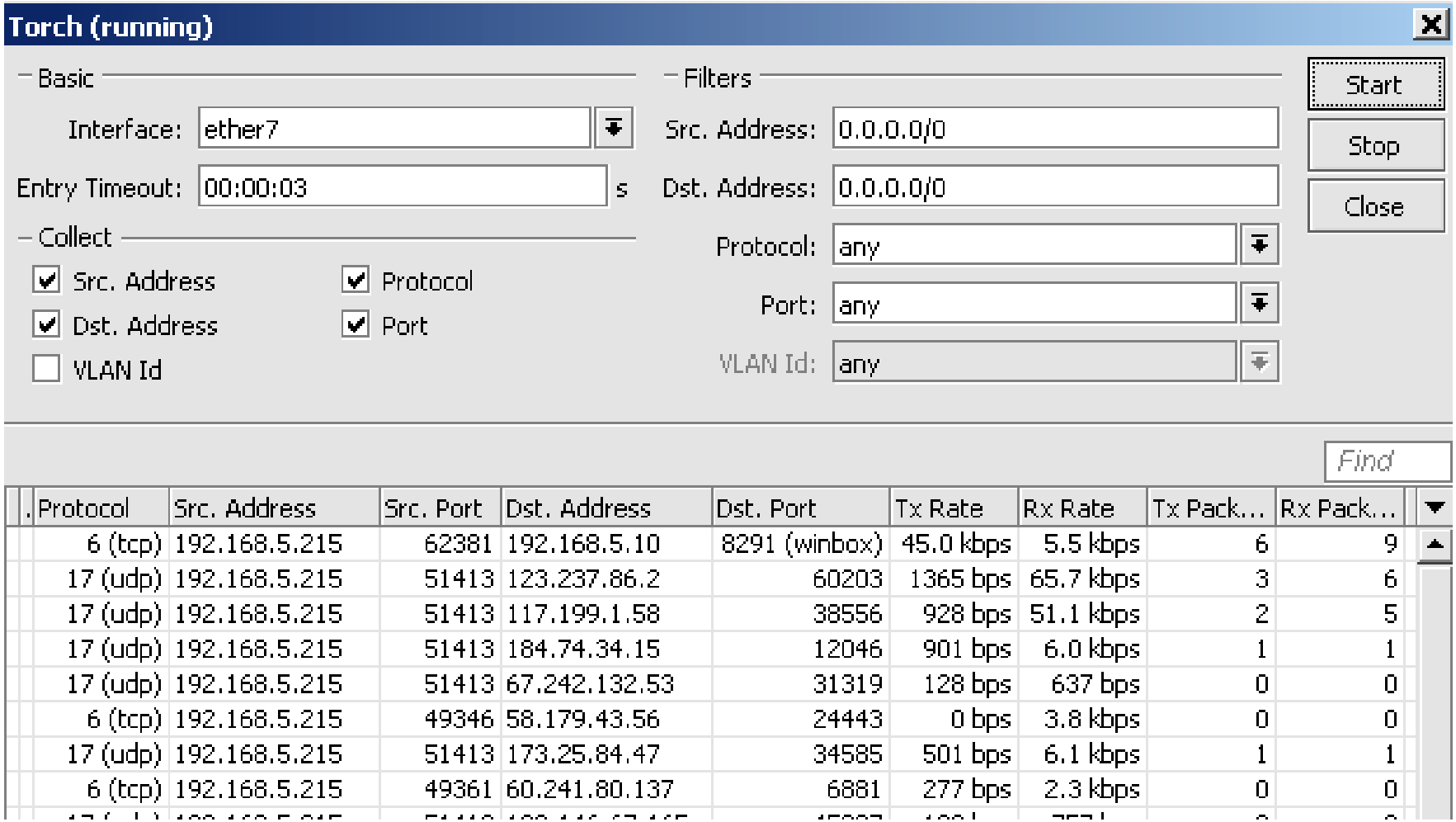
Monitoring - Traceroute

- Traceroute
  - Traceroute determines how packets are being routed to a particular host
  - We can choose the protocol : ICMP or UDP



Monitoring - Torch

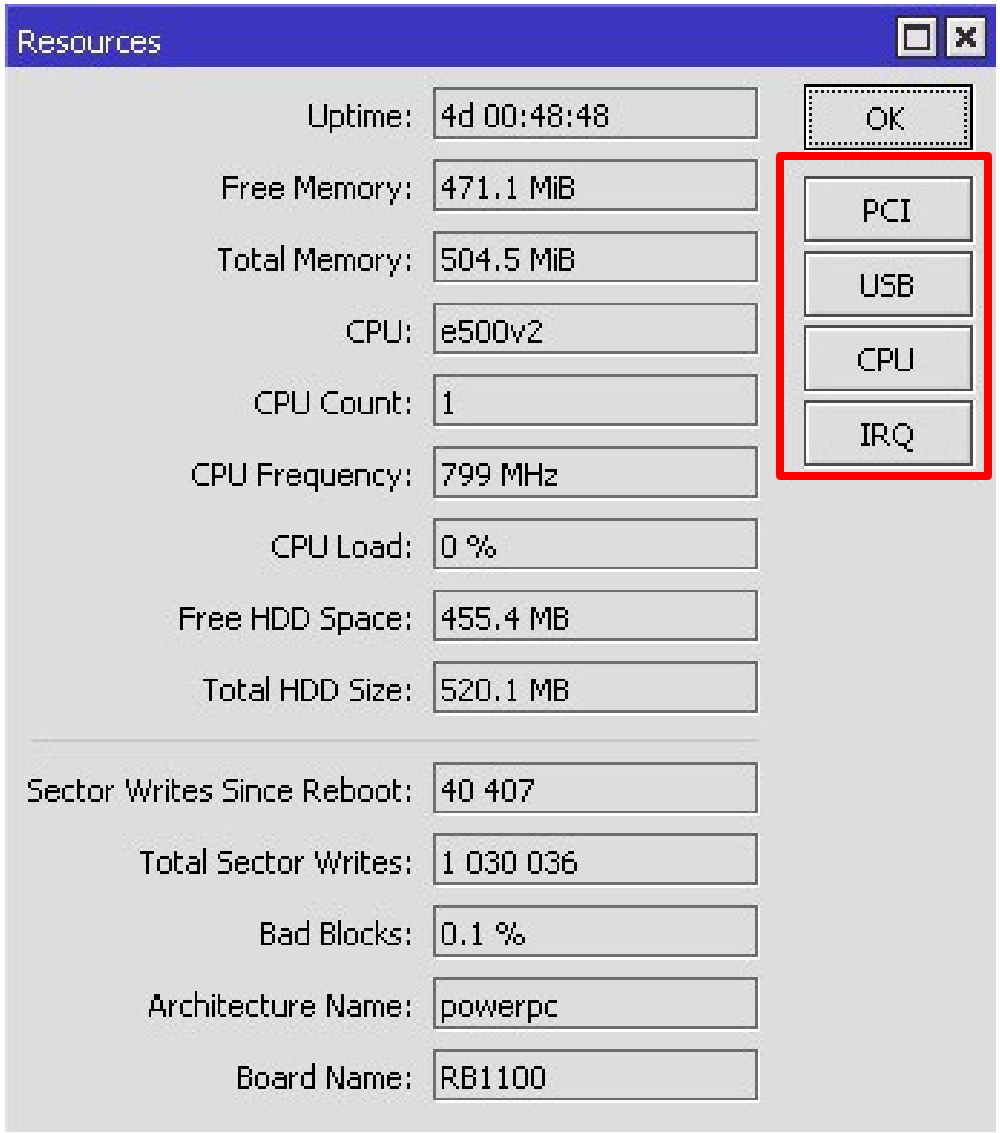
- Torch - Realtime traffic monitor



Protocol	Src. Address	Src. Port	Dst. Address	Dst. Port	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
6 (tcp)	192.168.5.215	62381	192.168.5.10	8291 (winbox)	45.0 kbps	5.5 kbps	6	9
17 (udp)	192.168.5.215	51413	123.237.86.2	60203	1365 bps	65.7 kbps	3	6
17 (udp)	192.168.5.215	51413	117.199.1.58	38556	928 bps	51.1 kbps	2	5
17 (udp)	192.168.5.215	51413	184.74.34.15	12046	901 bps	6.0 kbps	1	1
17 (udp)	192.168.5.215	51413	67.242.132.53	31319	128 bps	637 bps	0	0
6 (tcp)	192.168.5.215	49346	58.179.43.56	24443	0 bps	3.8 kbps	0	0
17 (udp)	192.168.5.215	51413	173.25.84.47	34585	501 bps	6.1 kbps	1	1
6 (tcp)	192.168.5.215	49361	60.241.80.137	6881	277 bps	2.3 kbps	0	0

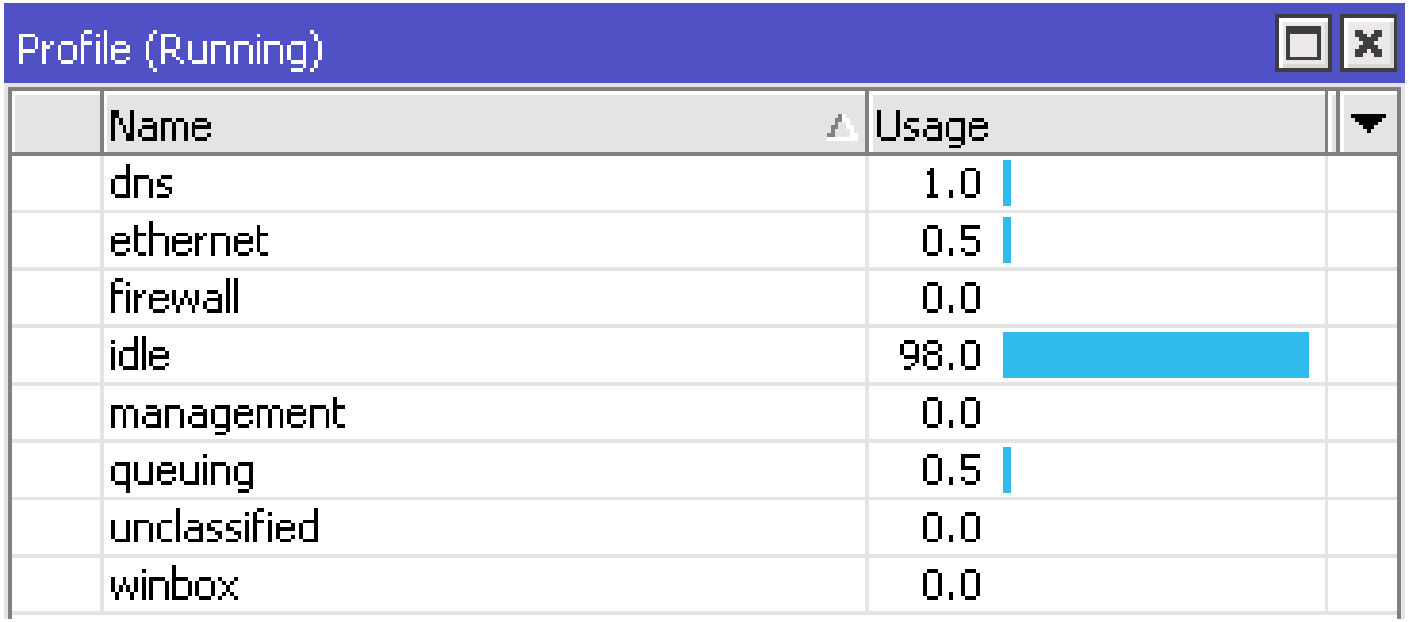
Monitoring - Resource

- Resource
  - To monitor the System.
  - Detail Resource monitor located on right side buttons



Monitoring – CPU Load

- Tool – Profile untuk monitoring CPU Load



Bridge, Switch & EoIP

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

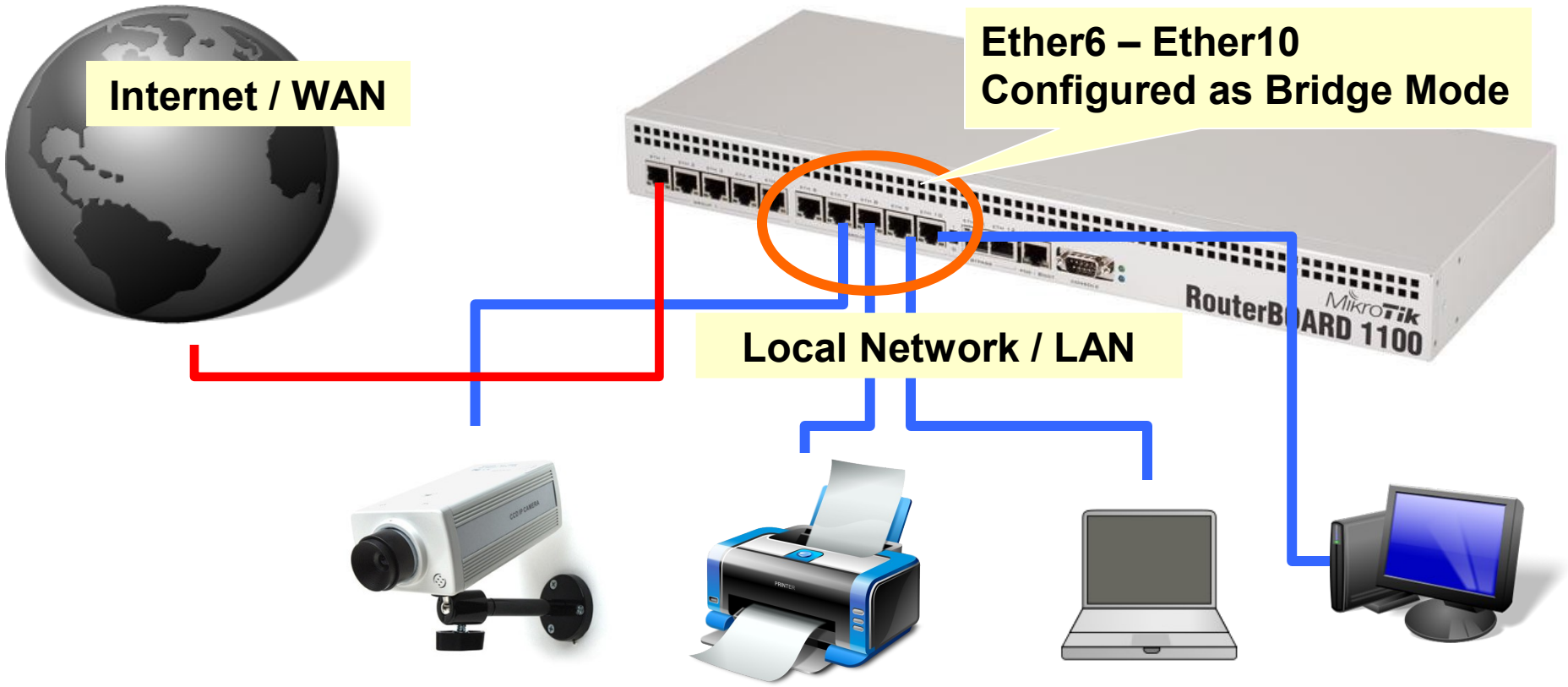
(Mikrotik Certified Training Partner)

Bridge - Concept

- Menggabungkan 2 atau lebih interface yang bertipe ethernet, atau sejenisnya, seolah-olah berada dalam 1 segmen network yang sama.
- Proses penggabungan ini terjadi pada layer data link.
- Mengaktifkan bridge pada 2 buah interface akan menonaktifkan fungsi routing di antara kedua interface tersebut.
- Mengemulasi mode **switch** secara software pada dua atau lebih interface.

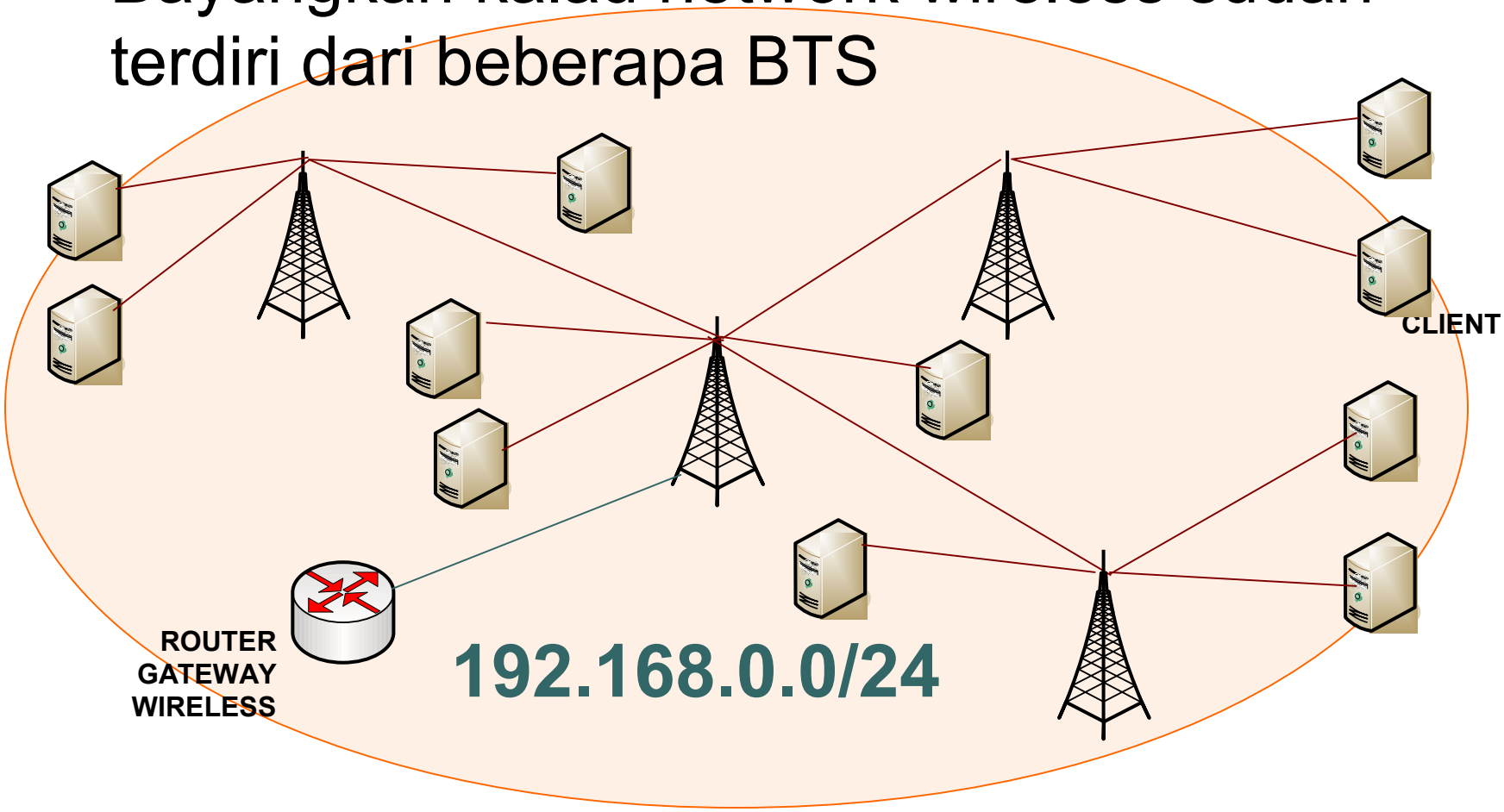
System Bridge - Example

- Memanfaatkan port-port pada Routerboard untuk menghubungkan Perangkat-perangkat jaringan **supaya berada dalam satu subnet / bridge network yang sama** layaknya seperti **Switch**.



Bridge – Topology for Wireless

- Bayangkan kalau network wireless sudah terdiri dari beberapa BTS



System Bridge

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

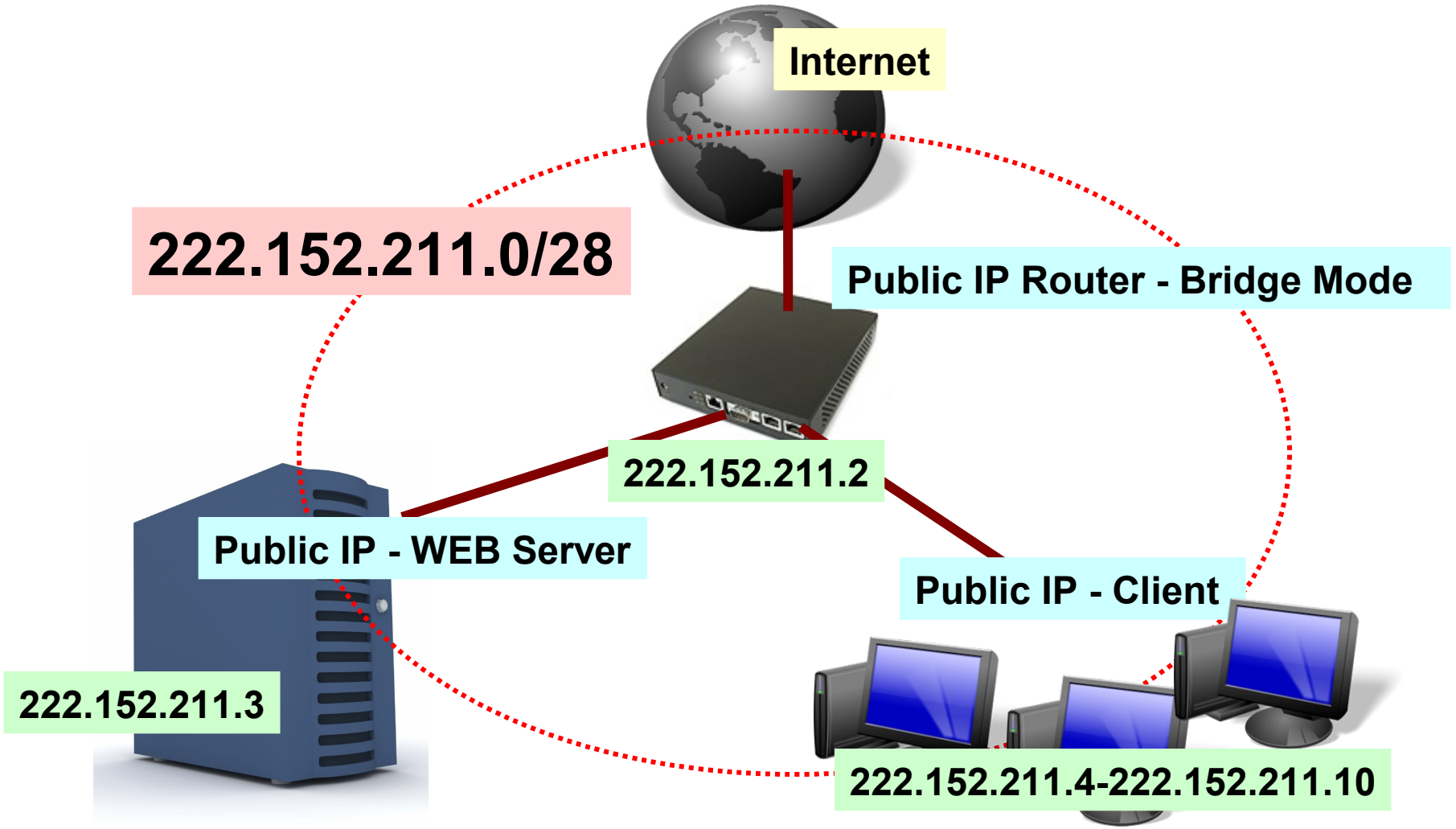
Interface for Bridge Port

- Berikut ini jenis-jenis interface yang dapat dijadikan Bridge Port :
  - **Ethernet**
  - **VLAN**
    - Merupakan bagian dari ethernet atau wireless interface
    - Jangan melakukan bridge sebuah VLAN dengan interface induknya
  - **Wireless AP, WDS,** dan **Station-pseudobridge**
    - Note: station-pseudobridge tidak bisa di-bonding
  - **EoIP (**Ethernet over IP)
    - Lebih detail pada slide lain
  - **PPTP**
    - Selama bridge dilakukan baik di sisi server maupun client

Bridge!

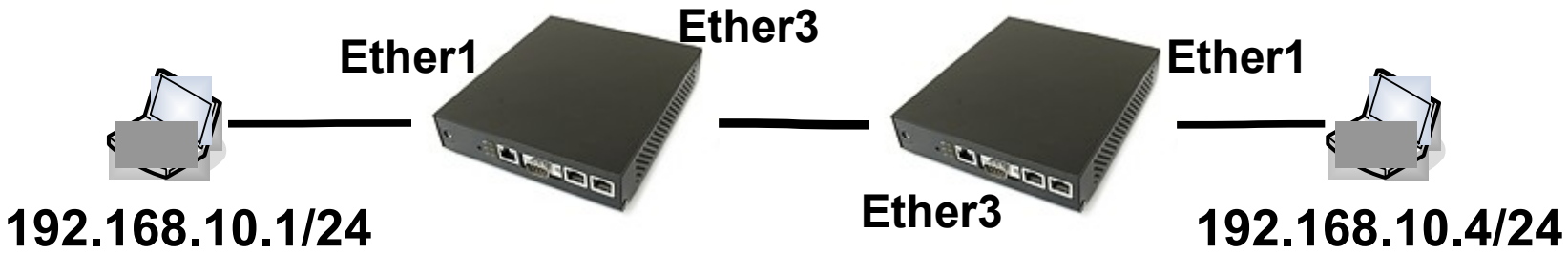
- Kita tidak harus memasang IP Address pada sebuah bridge interface
- Jika kita menonaktifkan bridge, pada IP Address yang terpasang pada bridge akan menjadi invalid
- Kita tidak bisa membuat bridge dengan interface yang bukan bertipe ethernet seperti synchronous (serial), IPIP, PPPoE, dll.
- Namun, bisa kita lakukan bridge pada interface tersebut dengan membuat EoIP Tunnel terlebih dahulu.
- EoIP Tunnel dijelaskan lebih detail di bagian yang lain.

Bridge – Implementation Example



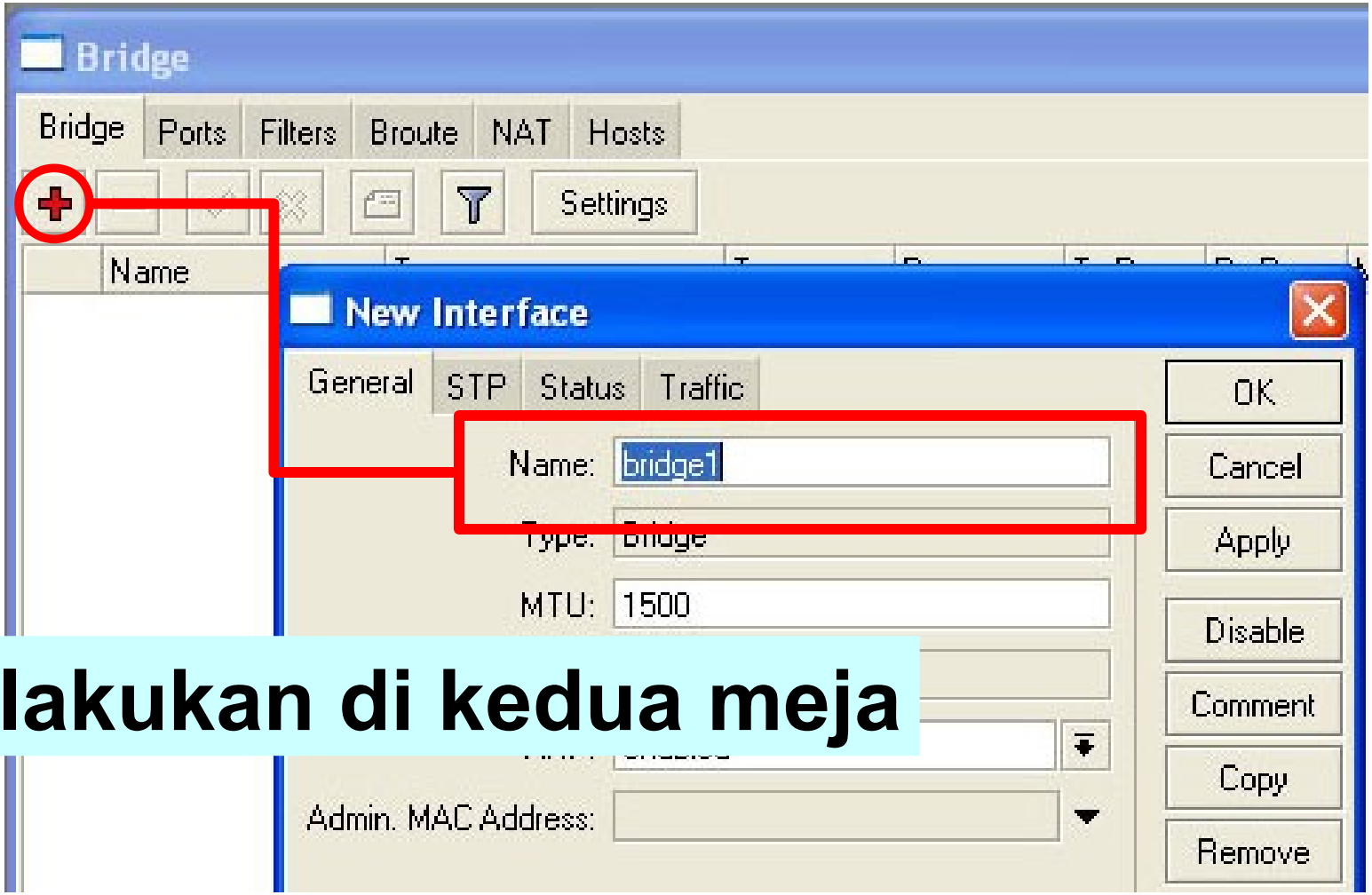
[LAB-1] Bridge Config

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



[LAB-1] Create Bridge

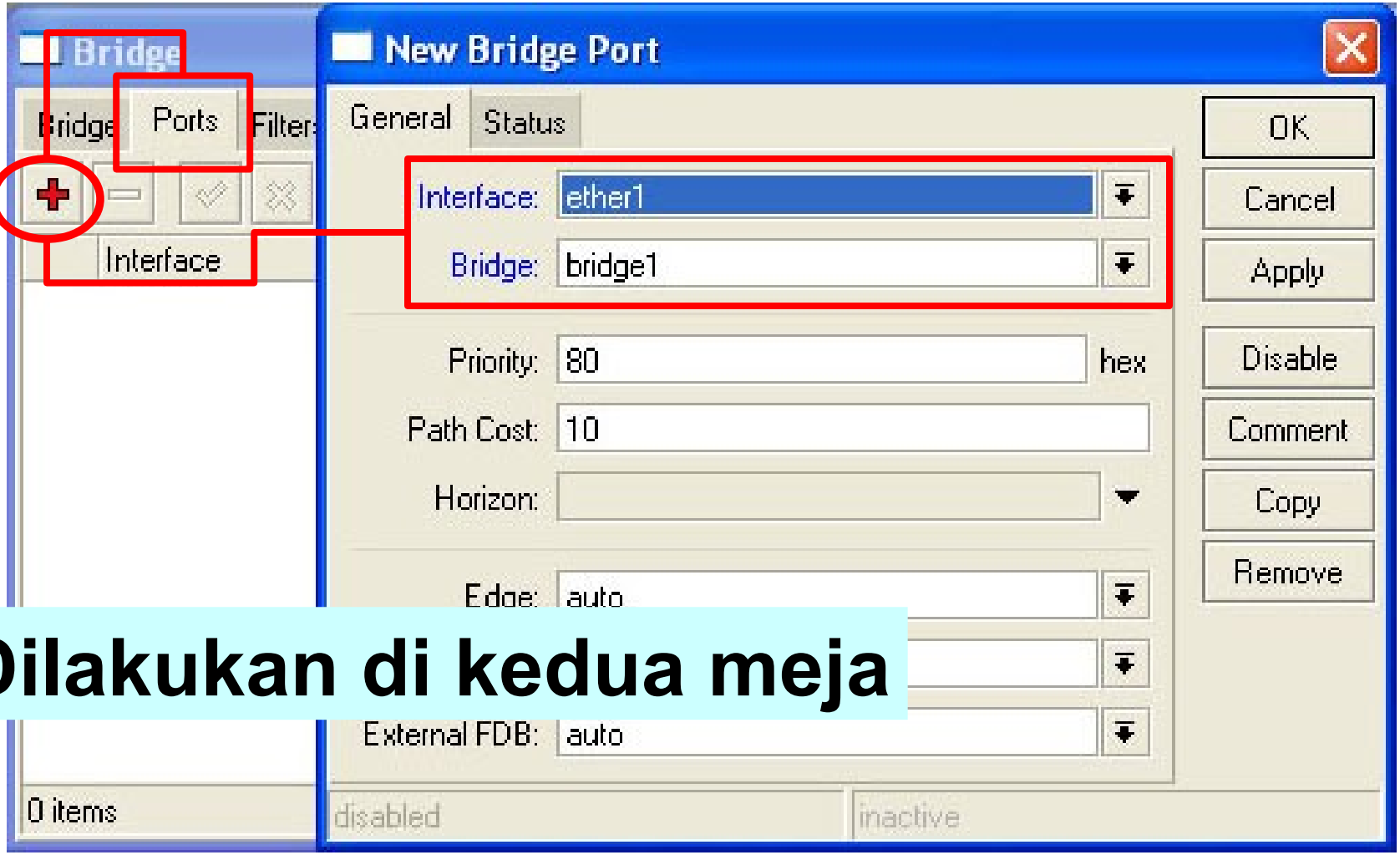
- Membuat interface bridge



Dilakukan di kedua meja

[LAB-1] Bridge Port

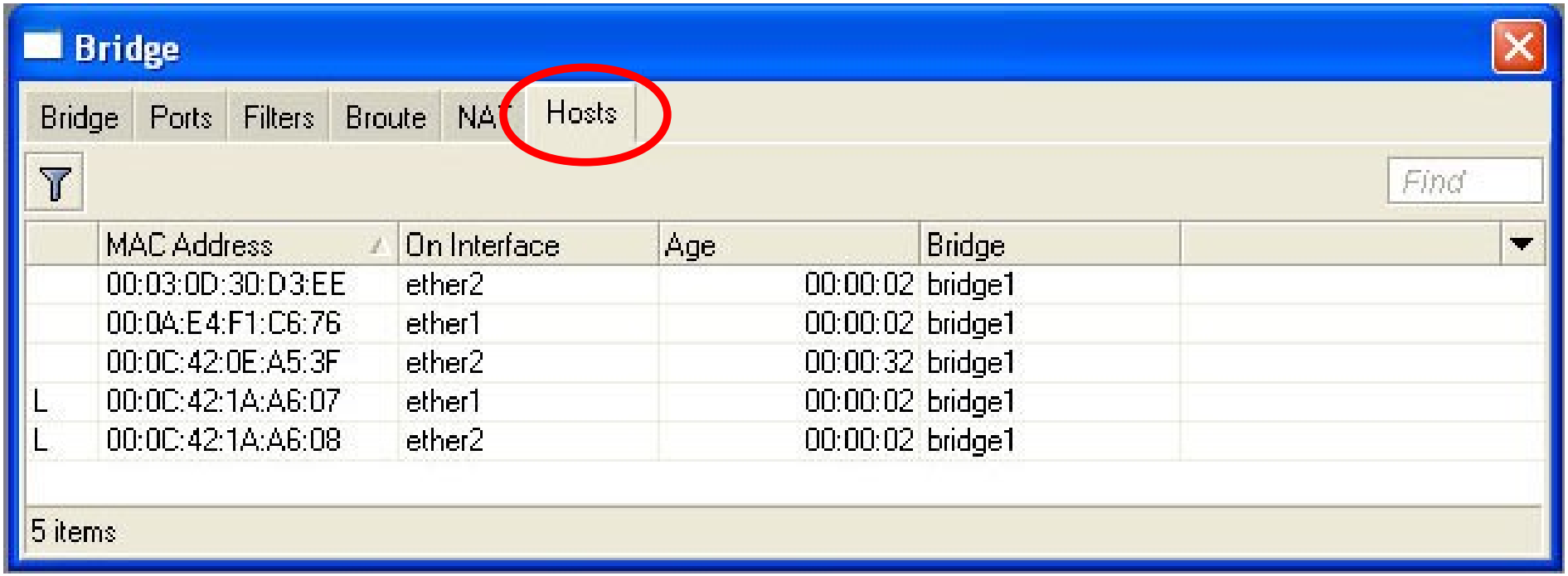
- Memasukkan interface ethernet ke interface bridge



Dilakukan di kedua meja

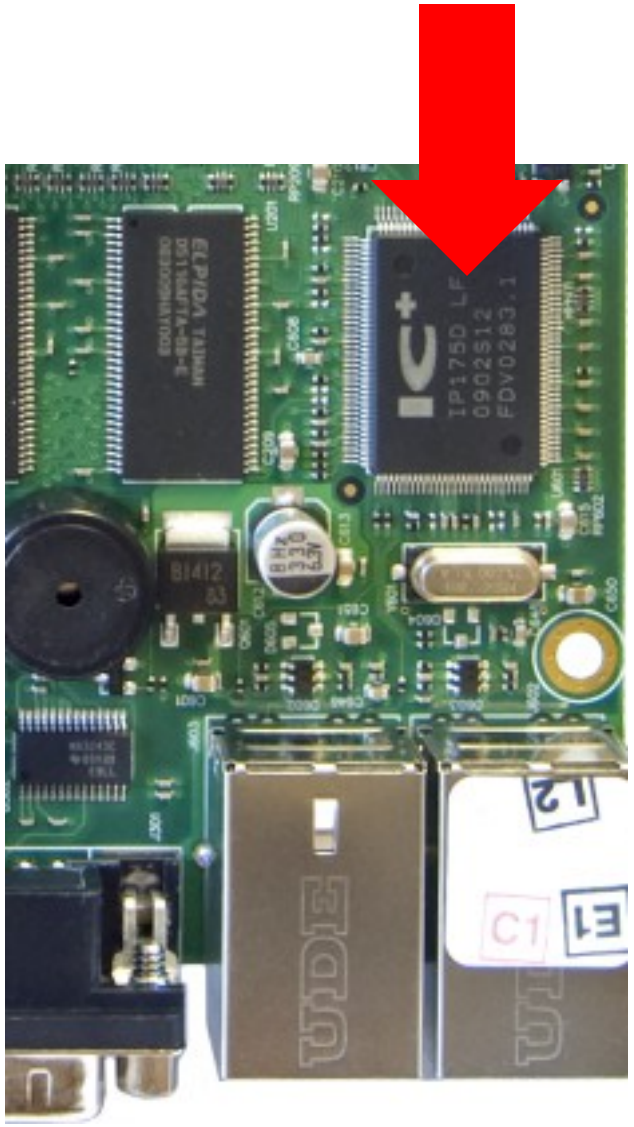
Bridge Monitoring

- Untuk melihat mac-address host yang terkoneksi dengan bridge tersebut



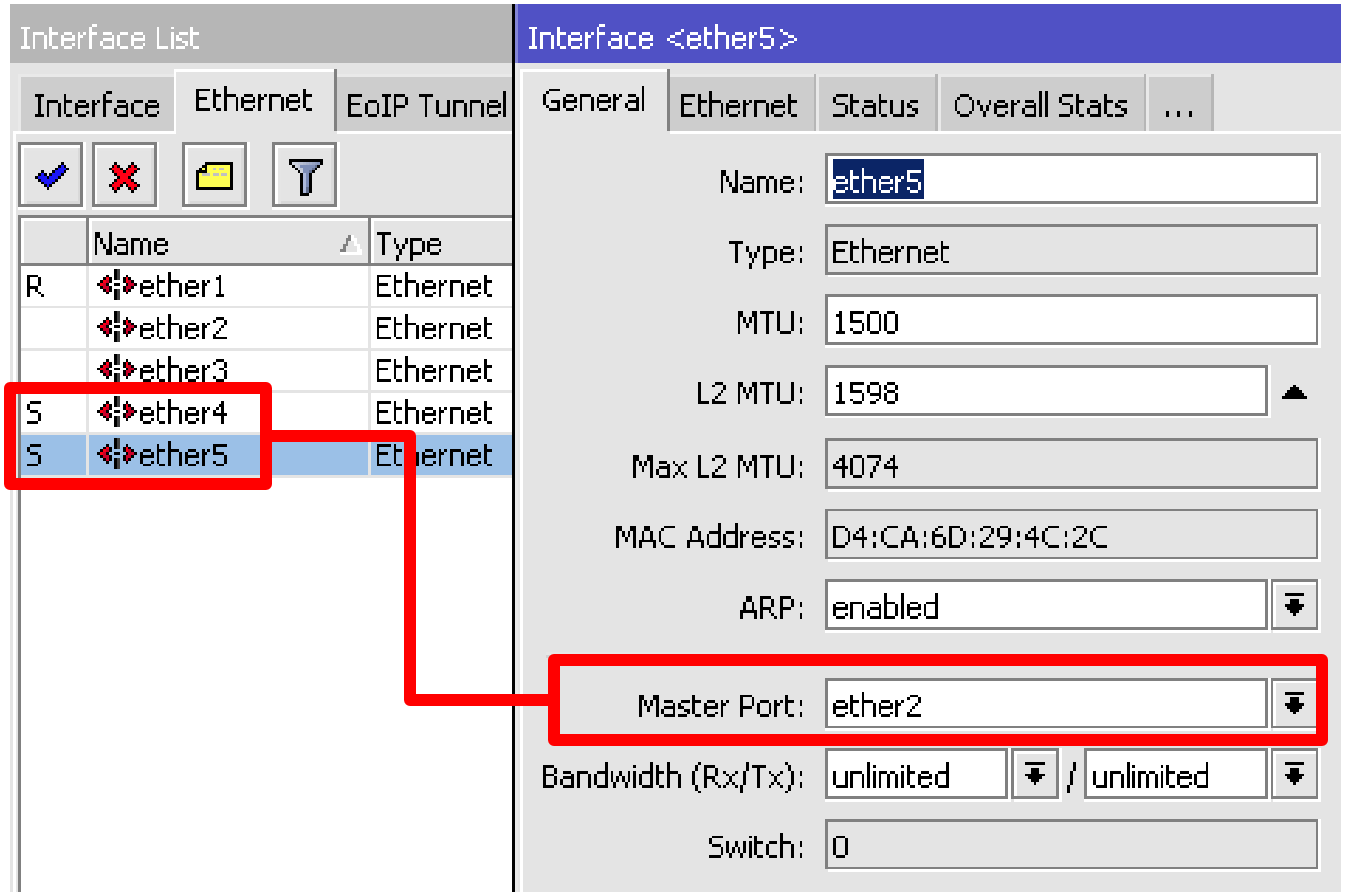
Switch Chipset

- Digunakan pertama di RB433 dan RB450, Mikrotik mulai menggunakan “Switch CHIP” di beberapa produk RouterBoard terbaru.
- Memungkinkan untuk memanfaatkan port ethernet di RouterBoard yang sebelumnya hanya bisa digunakan untuk Routed Network menjadi Switched Network.



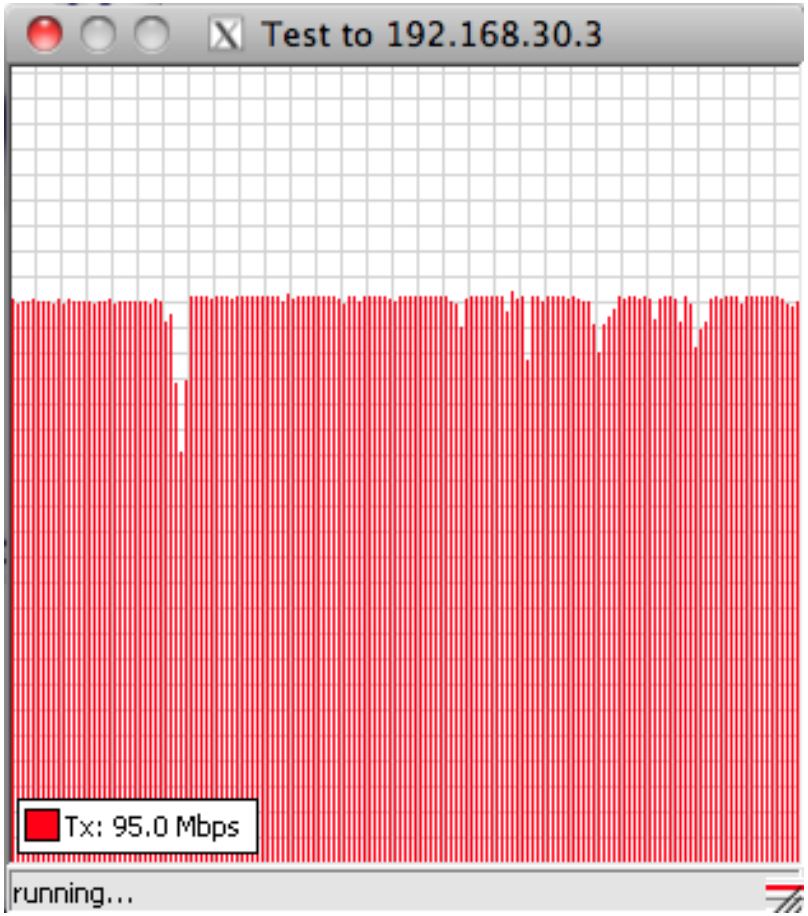
Switch Chipset – Master Port

- Di beberapa hardware Routerboard, Chipset ethernet yang terpasang sudah memiliki fungsi Switch Chip.



Switch Chip – Cable SPEED !

- Dengan Switch Chip, memungkinkan transfer data antar port bisa mencapai cable speed tanpa membebani processor.



Quiz !

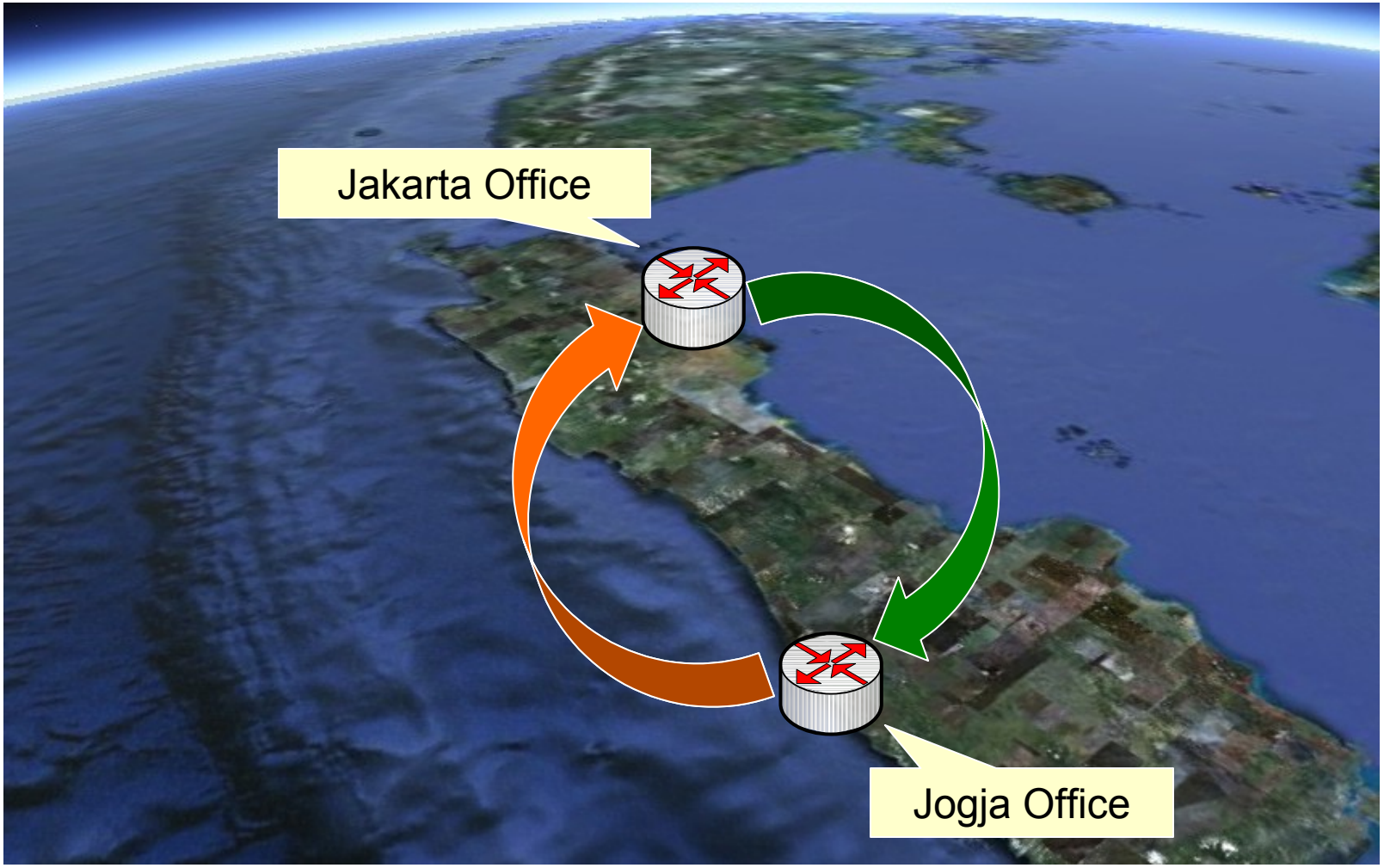
- Beda fungsi Bridge dan Switch ?
- Fungsi Switch bisa dijalankan antara interface ethernet dan wireless pada RouterBoard RB411AR ? Kenapa ?
- Hotspot server dan DHCP server tidak bisa dijalankan pada Bridge ? (Benar / Salah) Kenapa ?

Ethernet over IP (EoIP)

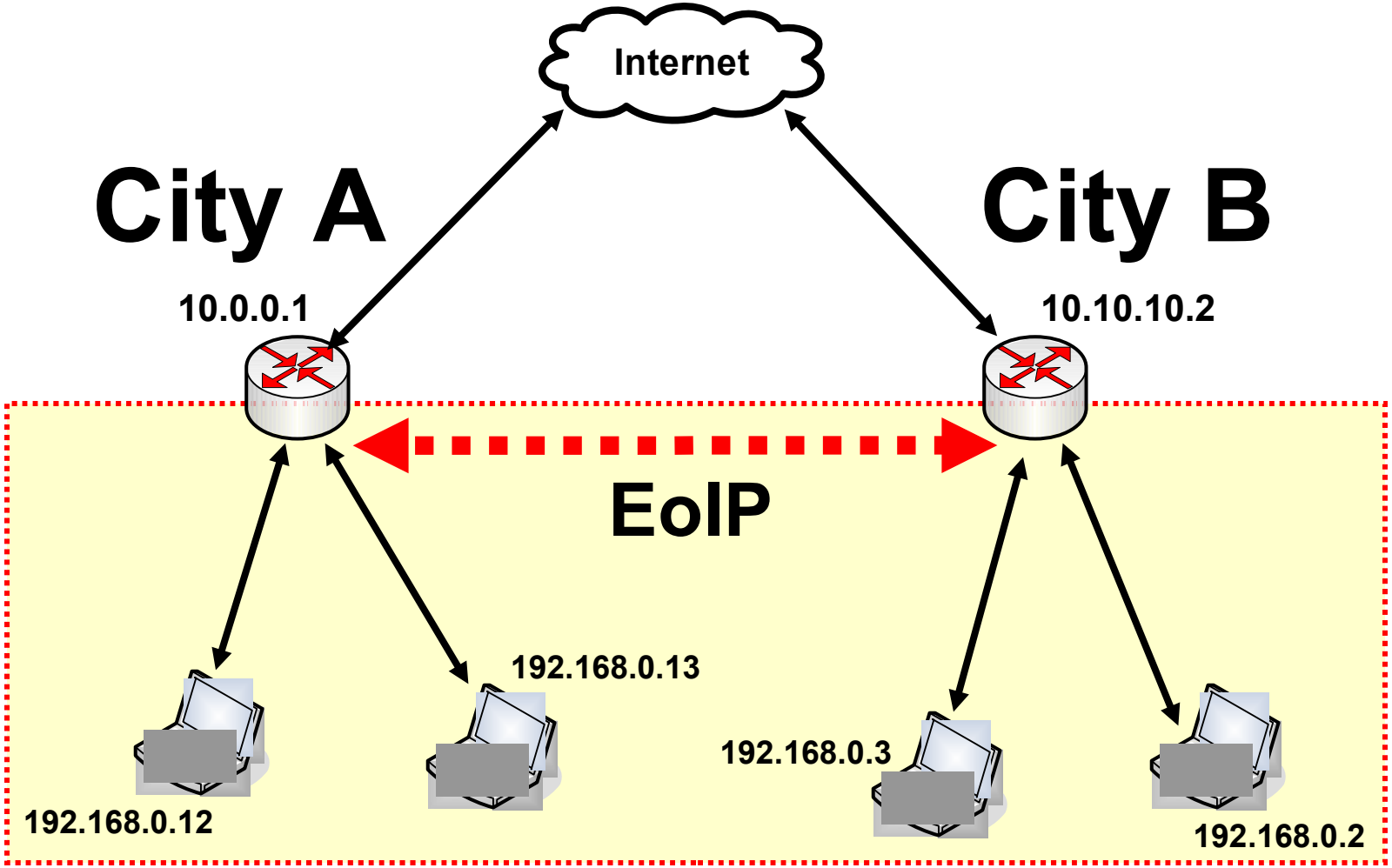
- Adalah protocol pada Mikrotik RouterOS yang membangun sebuah **Network Tunnel** antar mikrotik router di atas sebuah koneksi TCP/IP.
- Interface EoIP dianggap sebagai sebuah Interface Ethernet
- Jika Bridge mode diberlakukan pada EoIP tunnel maka semua protocol yang berbasis ethernet akan dapat berjalan di Bridge tersebut (Dianggap seperti hardware interface ethernet yang di bridge).
- Hanya dapat dibuat di Mikrotik RouterOS
- Menggunakan Protocol **GRE** (RFC1701)

Network Skenario

- Bridge over WAN / Internet

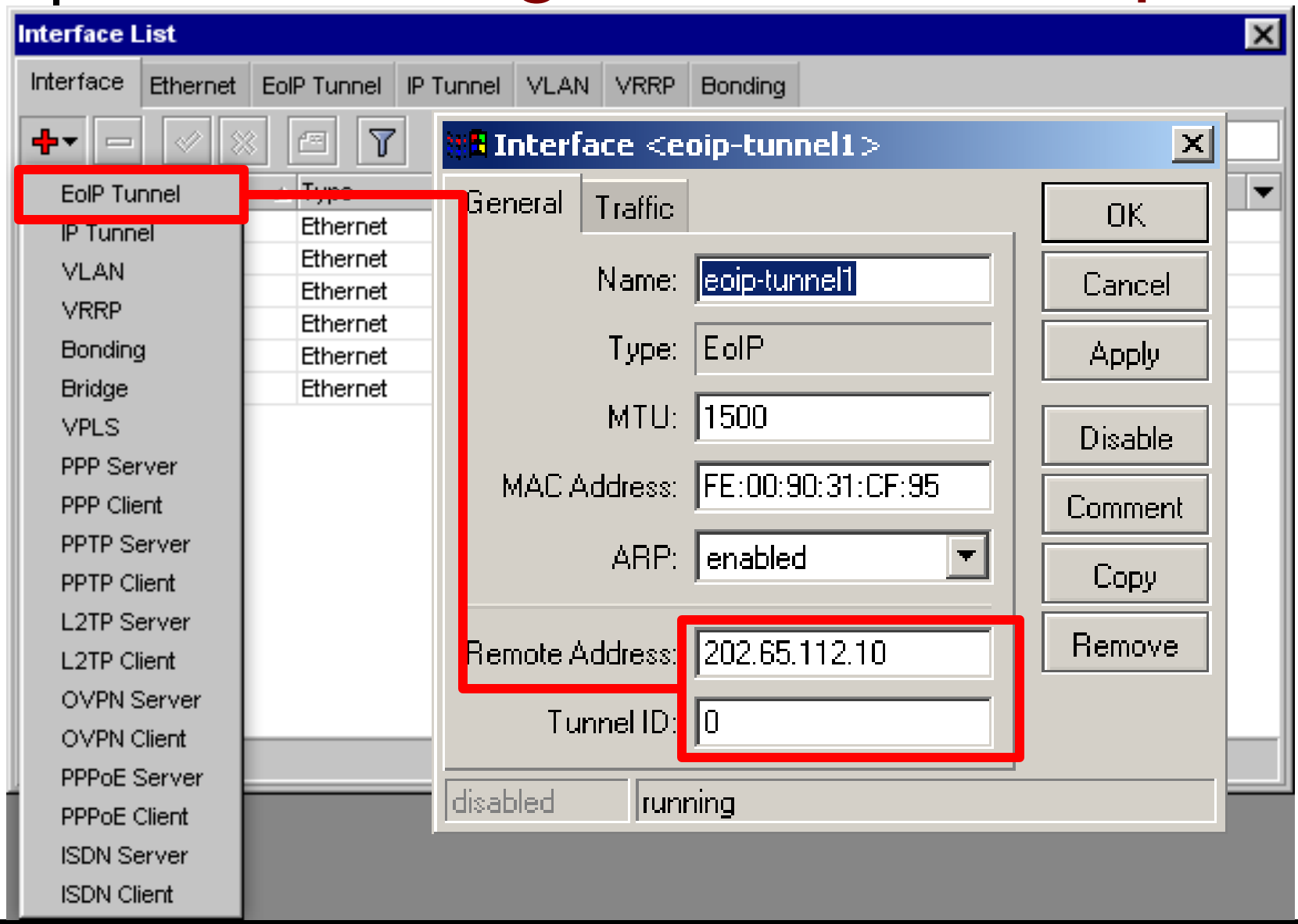


EoIP Example

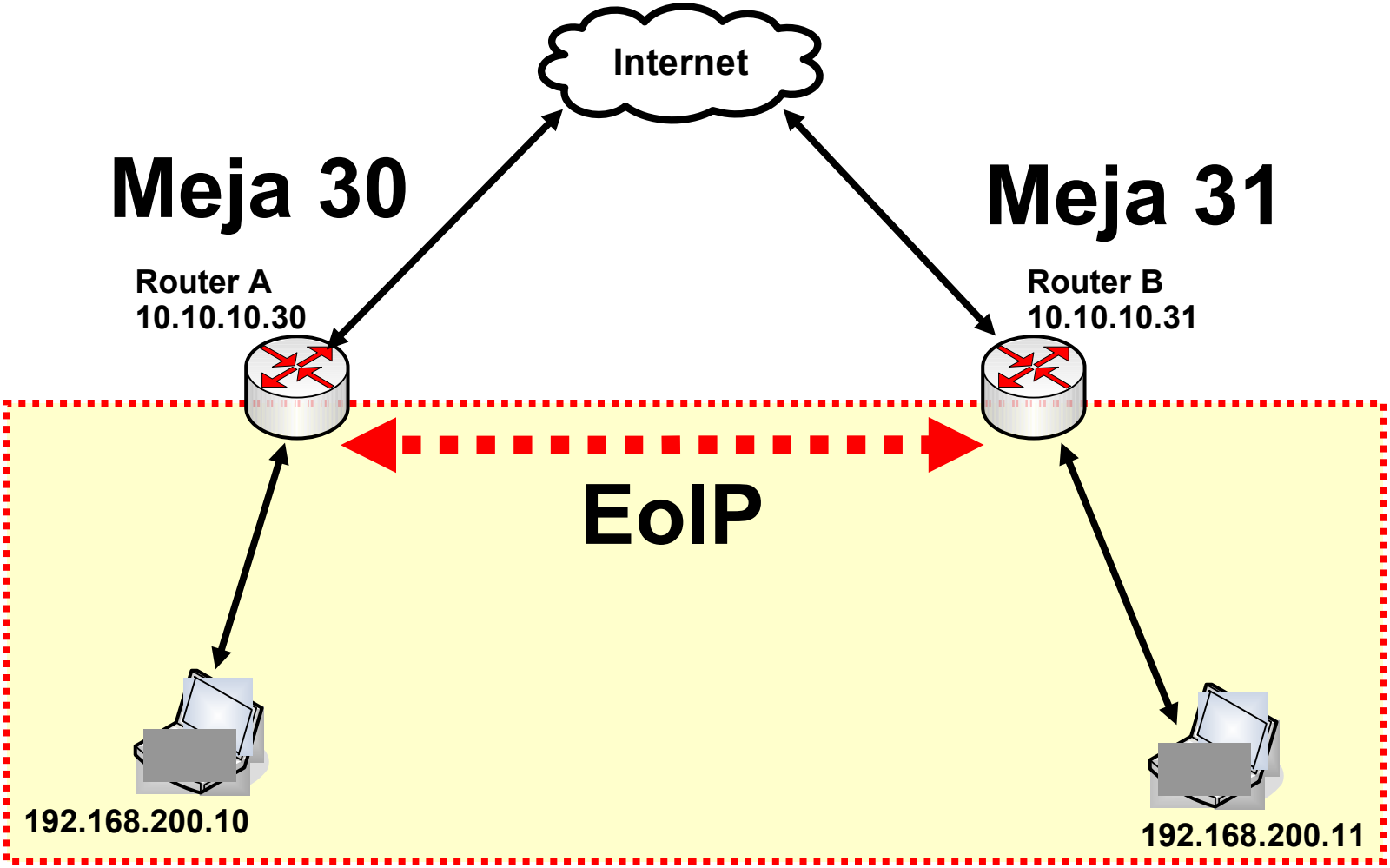


Secara Virtual setiap Laptop terletak di dalam satu segmen network yang sama.

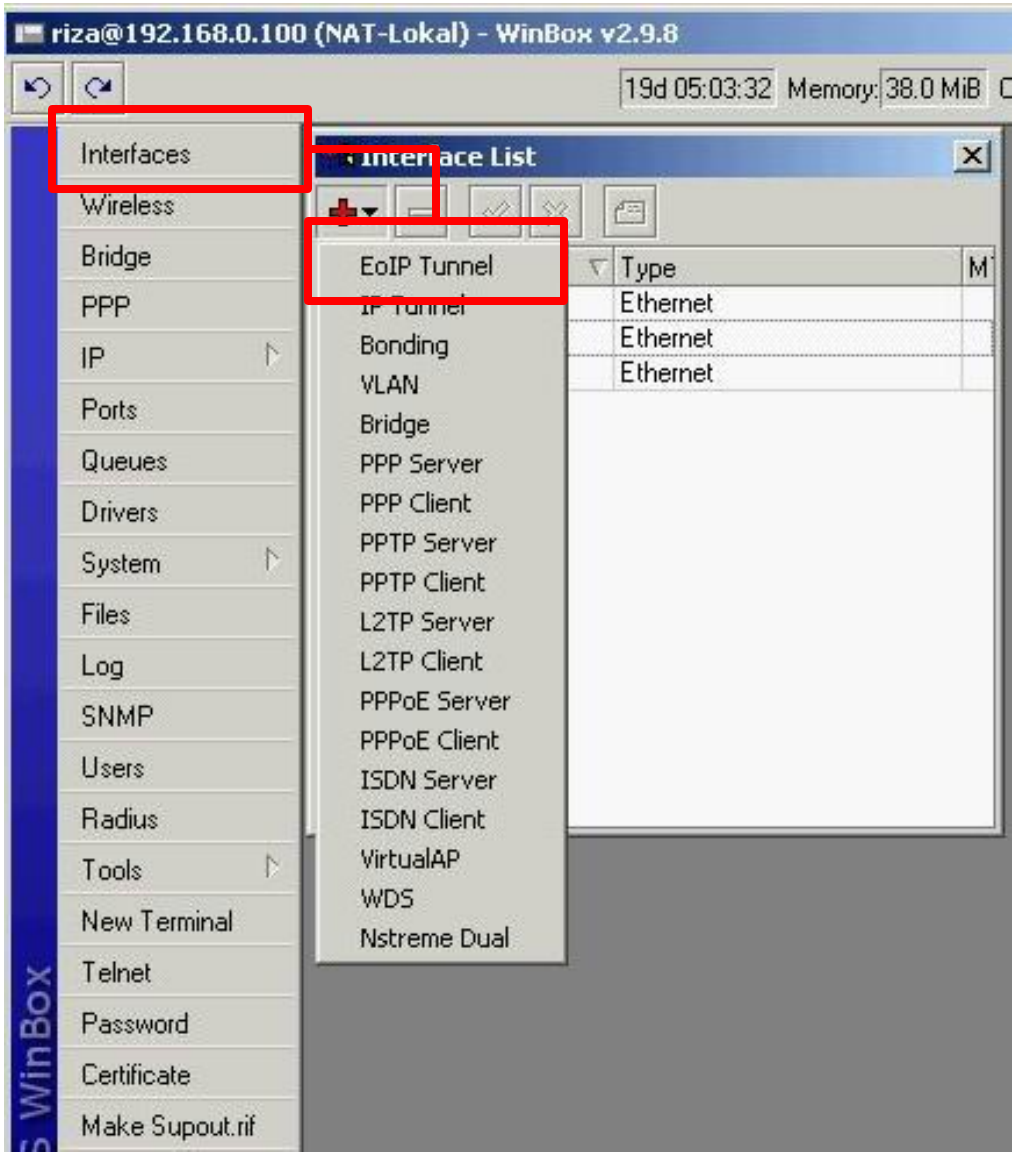
EoIP Configuration - Example



[LAB-2] EoIP Tunnels



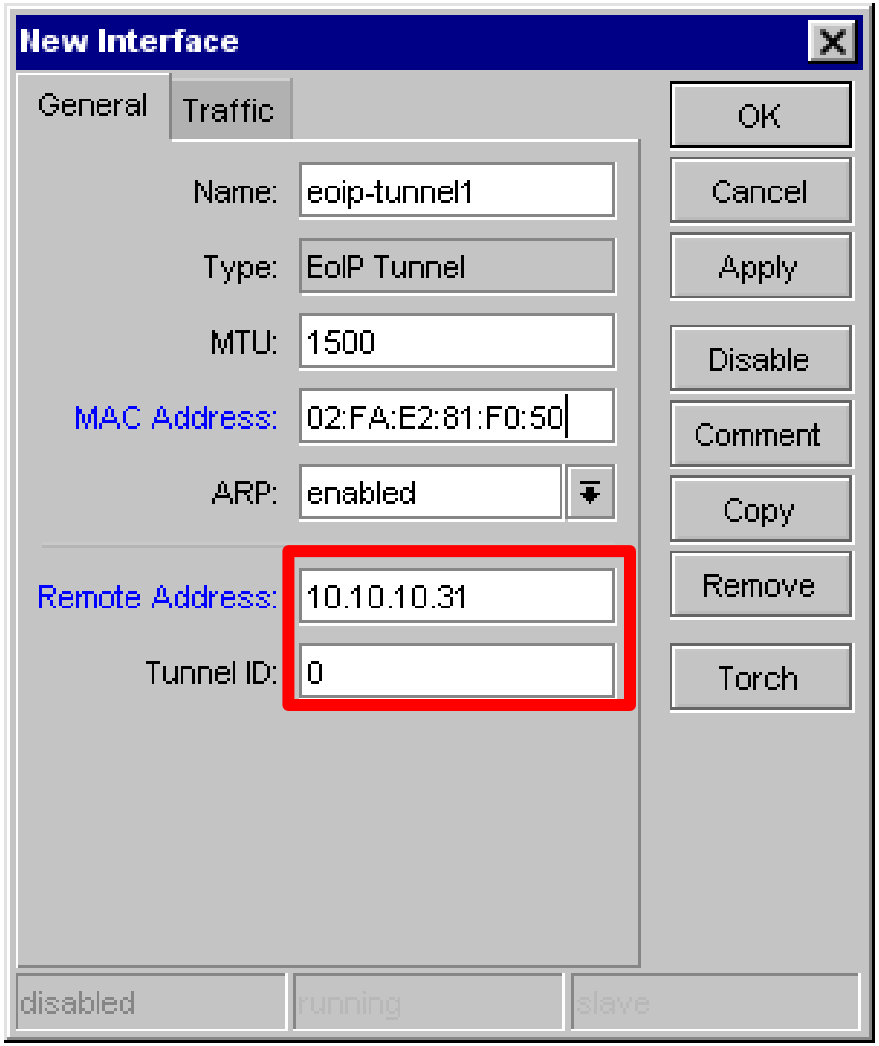
EoIP Tunnels - Config



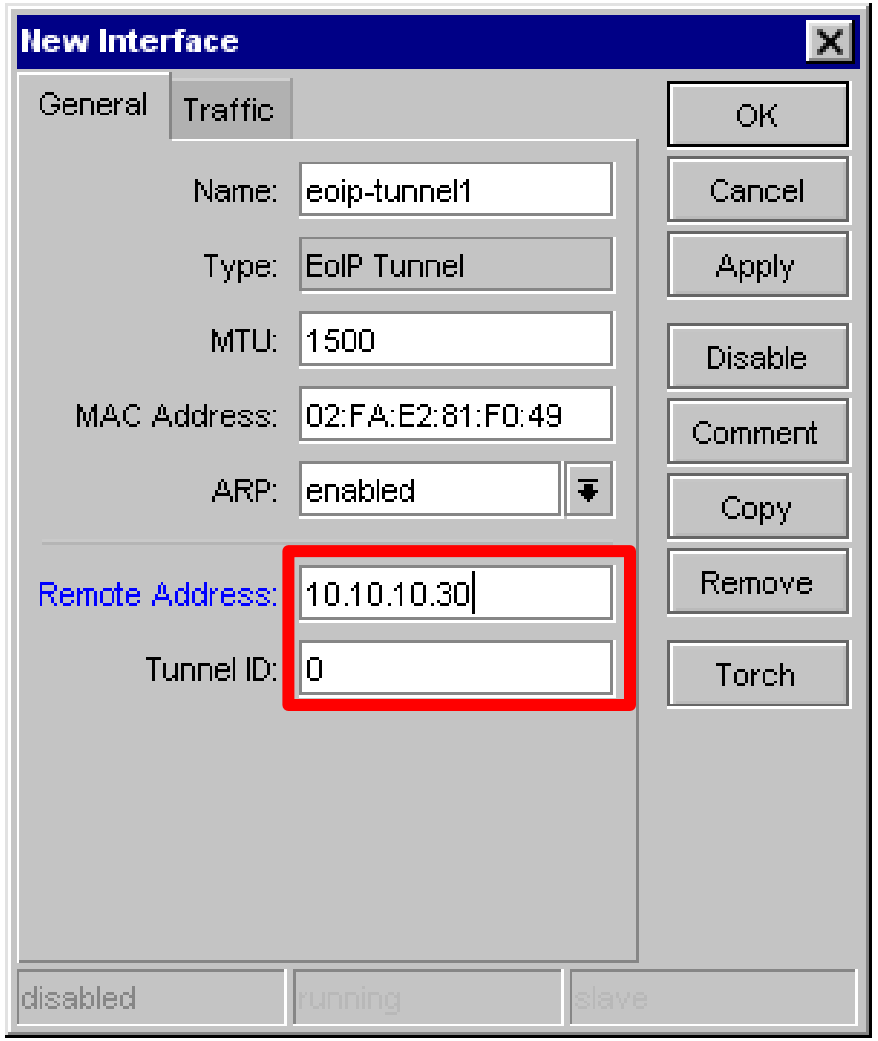
- Perlu diingat bahwa **TUNNEL ID** pada sebuah EoIP tunnel harus sama antar kedua EoIP Tunnel.
- **MAC Address** antar EoIP harus berbeda satu dengan yang lain.

EoIP Tunnels Config

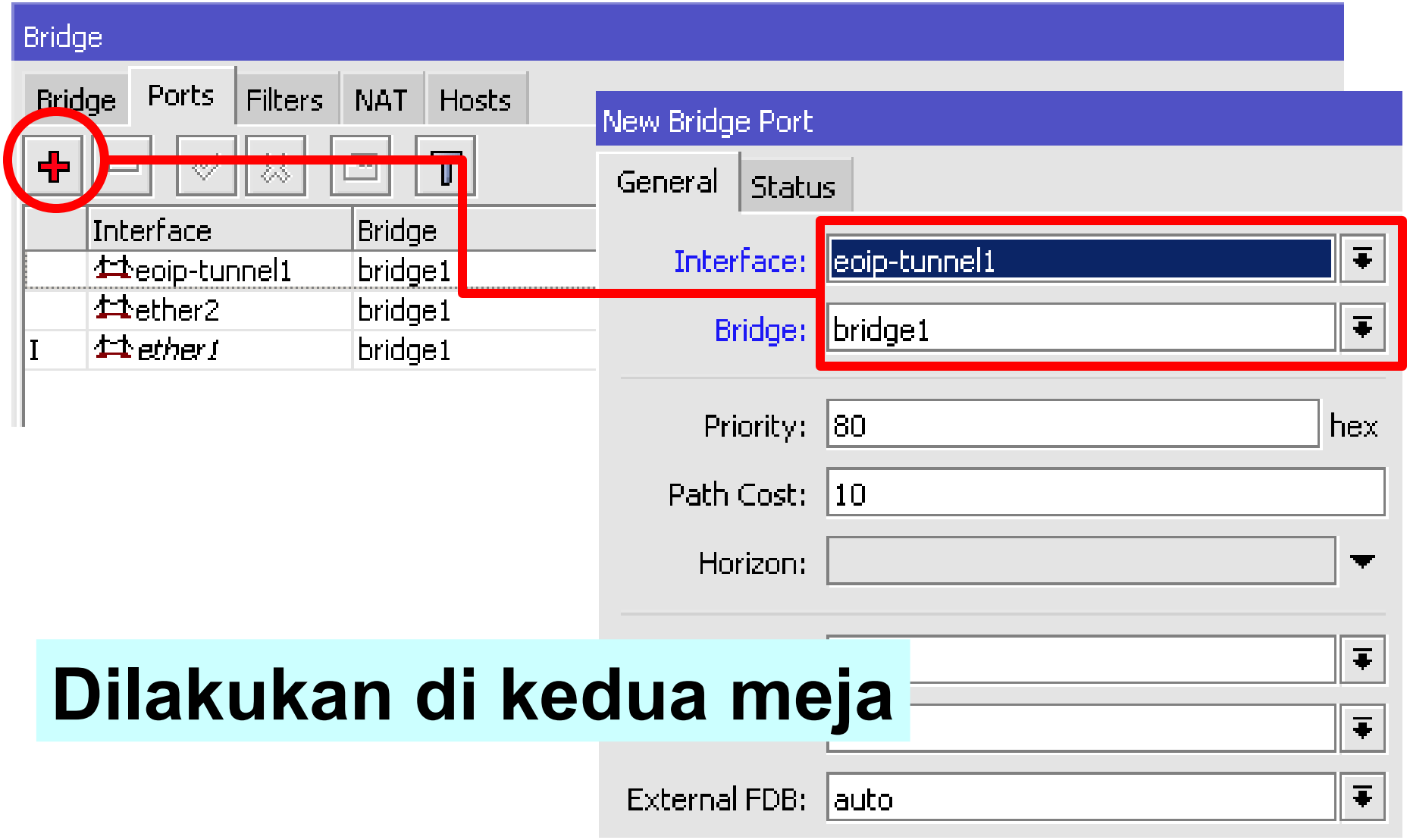
ROUTER A



ROUTER B



Bridge Port Config – Add EoIP



Dilakukan di kedua meja

Quiz !

- EoIP harus menggunakan ip Public supaya bisa berjalan dengan normal ? Kenapa ?

- Untuk mengaktifkan EoIP harus juga mengaktifkan bridge ? Kenapa ?

Wireless Concept

Certified Mikrotik Training Basic Class

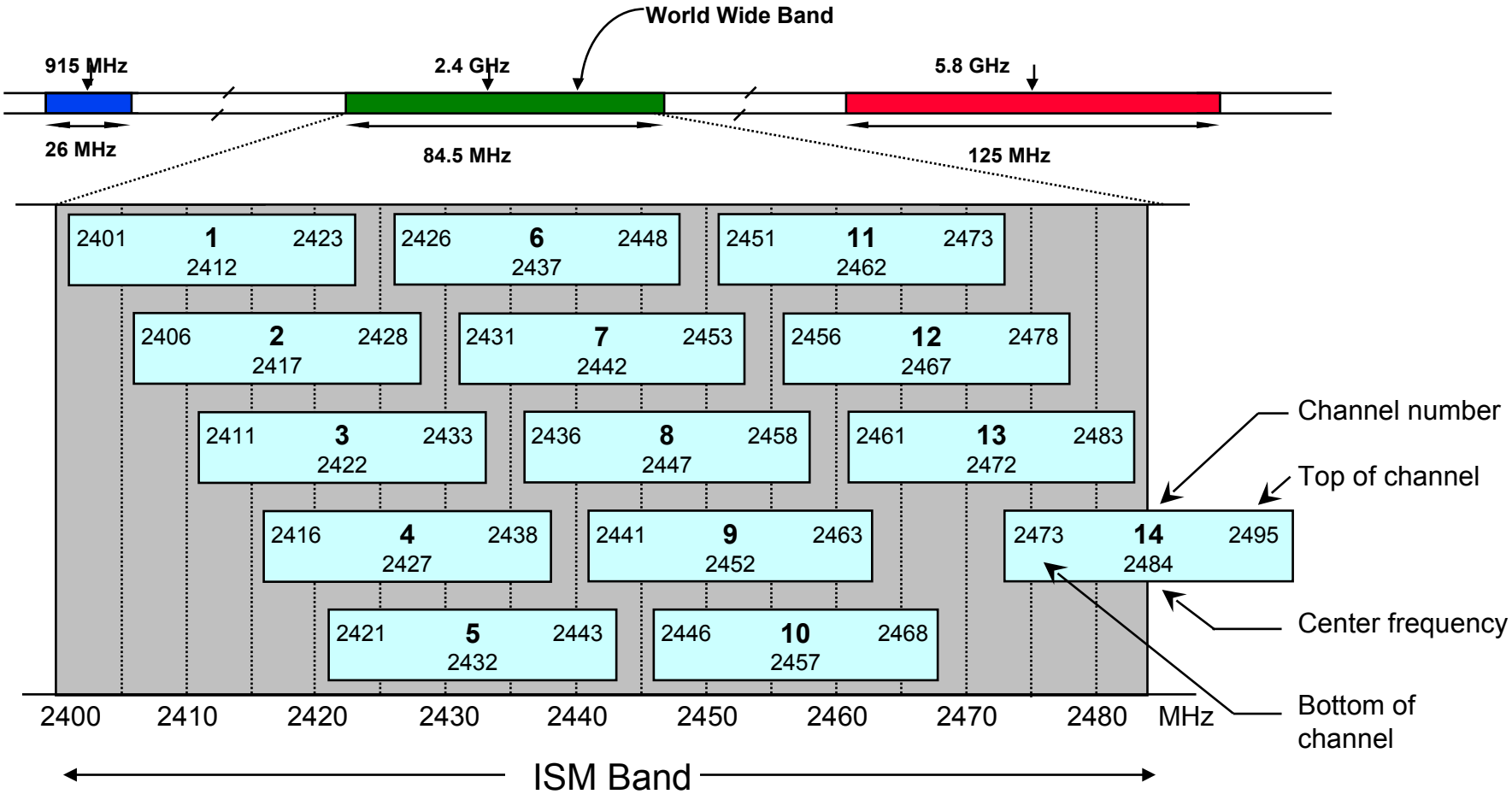
Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

Wireless LAN – 802.11

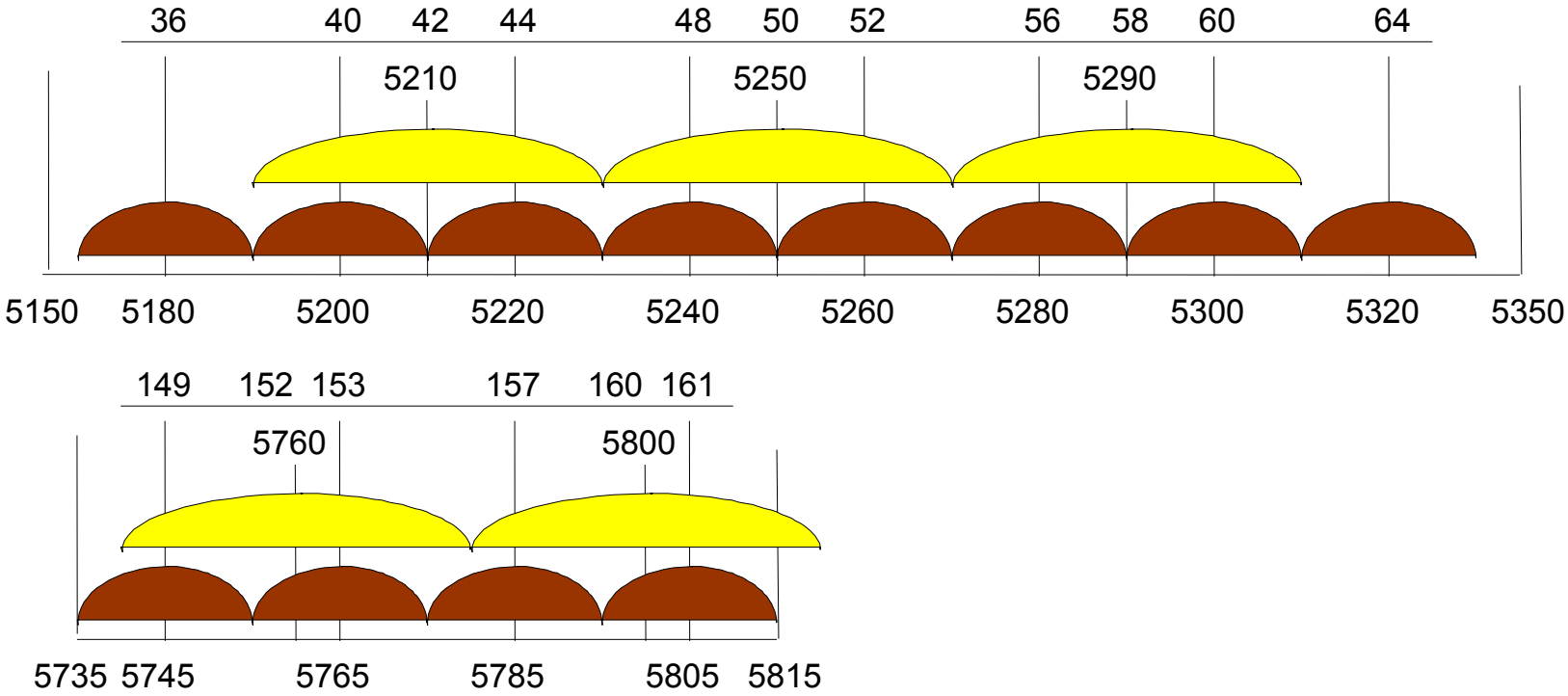
- **802.11 – 2.4Ghz**
  - ***802.11-b*** : Wireless Lan yang menggunakan Frequency 2.4Ghz berkecepatan transfer data **11Mbps**
  - ***802.11-b/g*** : Wireless Lan yang menggunakan Frequency 2.4Ghz berkecepatan transfer data **54Mbps**
  - ***802.11-b/g/n*** : Wireless Lan yang menggunakan Frequency 2.4Ghz berkecepatan transfer data **300Mbps**
- **802.11 – 5Ghz**
  - ***802.11-a/g*** : Wireless Lan yang menggunakan Frequency 5Ghz berkecepatan transfer data **54Mbps**
  - ***802.11-a/g/n*** : Wireless Lan yang menggunakan Frequency 5Ghz berkecepatan transfer data **300Mbps**

Channels 80211-b



- (14) 20 MHz wide channels

Channels 80211-a

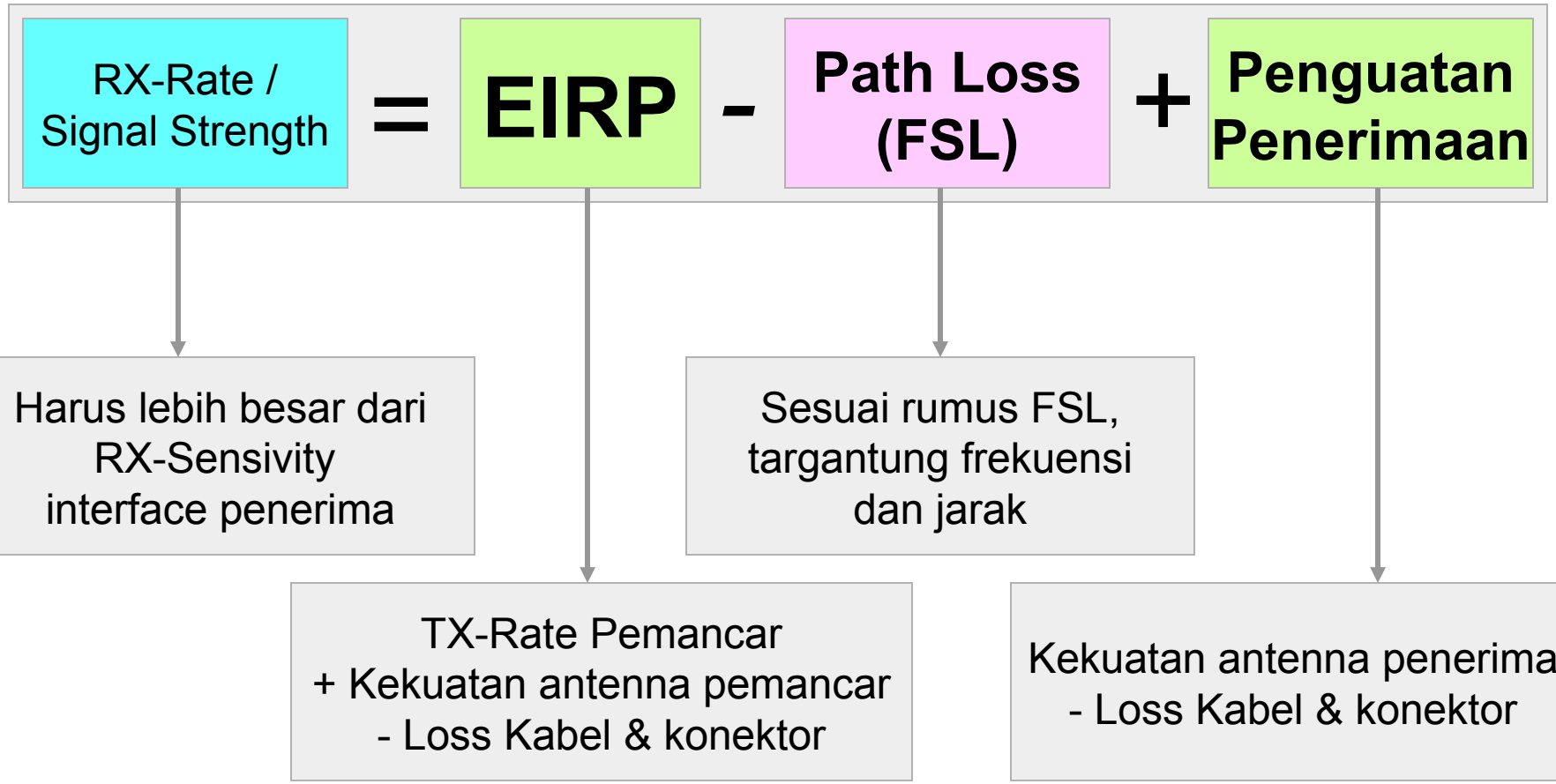


- (12) 20 MHz wide channels
- (5) 40MHz wide turbo channels

Kaidah dalam WirelessLAN

- Kaidah Wireless :
  - **Tx Power** – Daya Pancar signal wireless
  - **Rx Sensivity** – Sesitifitas Menerima signal
  - **Looses** – hambatan karena Kabel & Konektor
  - **EIRP** – Daya pancar total beserta Antenna
  - **Free Space Loss (FSL)** – Hambatan udara
- Kaidah Wireless Outdoor :
  - **Line of Sight** – Hambatan dan penghalang
  - **Freznel Zone** – Media rambat Frequency
  - **Lengkung Bumi** – Penghalang WLan jarak jauh

Signal Calculation Formula



RX-Rate Calculation

- Contoh Kasus :
  - Access Point 100 mWatt
  - tanpa booster
  - kabel LMR400 100 feet
  - antenna grid 24 db
  - frekuensi 2,4 GHz
  - jarak 10 km

Calculation Example

Perangkat			*db*
Pemancar (EIRP)			37.2 db **(EIRP)**
	Access Point 100 mWatt	20 dbm	
	Kabel 30 meter	-6.8 db	
	Antenna 24 db	24 dbi	
FSL / Path Loss 2,4 GHz 10 km			-120.026 db
Penerima (Penguatan Penerimaan)			17.2 db
	Kabel 30 meter	-6.8 db	
	Antenna 24 db	24 dbi	
RX-Rate / Signal Strength			**-65.626 db**

Online Calculator

- www.mikrotik.co.id/test_link.php

Link Possibility Calculator

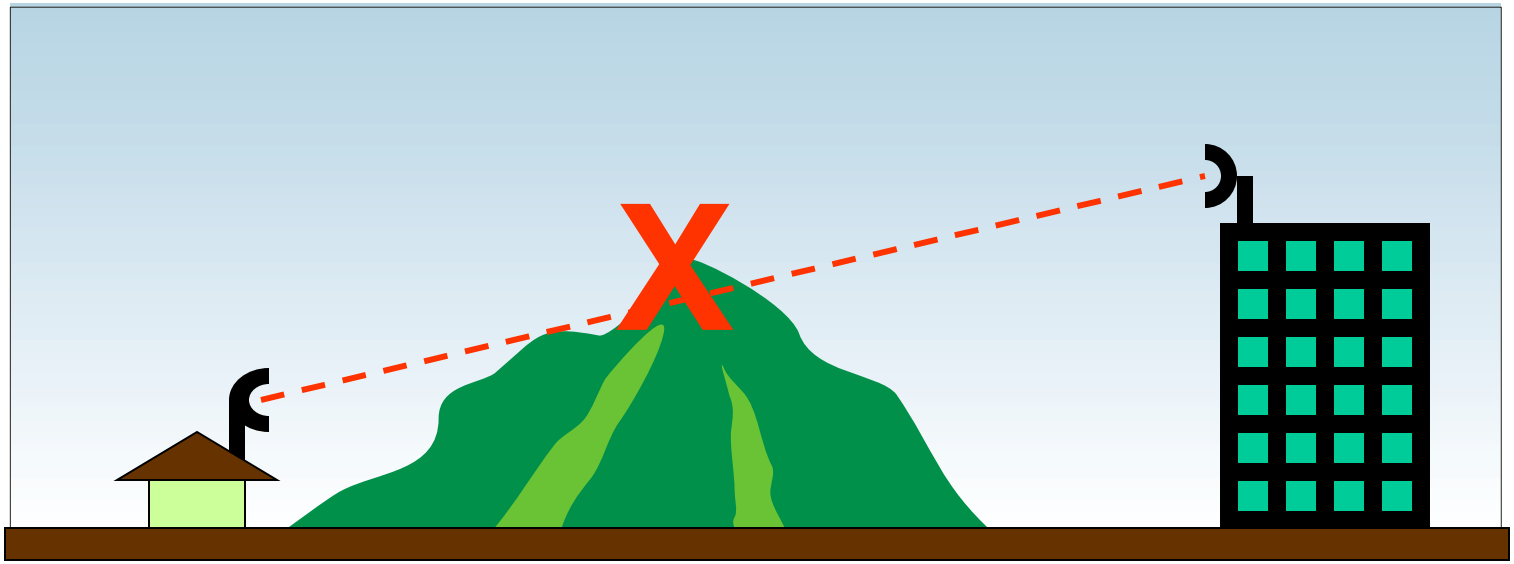
Parametrs	SITE 1	SITE 2
Wireless cards		
Power	65 mW	65 mW
RX Sensitivity	-90 dBm	-90 dBm
Antennas		
Gain	24 dBi	24 dBi
Cables		
Length	3 m	3 m
Type:	LMR400	LMR400
Link		
Distance	10 km	
Frequency	2400 MHz	

Calculate

Link theoretical status	reliable
Theoretical signal level at site 1	-56/required -90
Theoretical signal level at site 2	-56/required -90

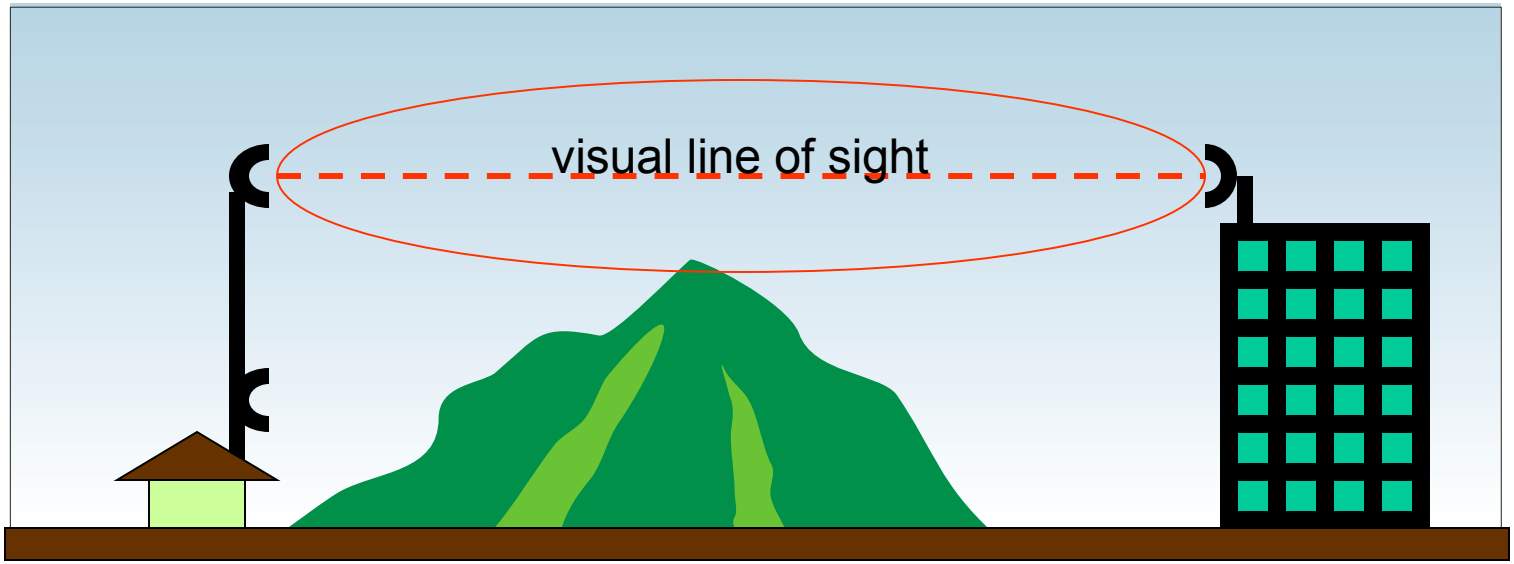
Line of Sight (LOS)

- Aplikasi Wireless LAN di luar ruangan harus memenuhi prinsip Line of Sight



Line of Sight (LOS)

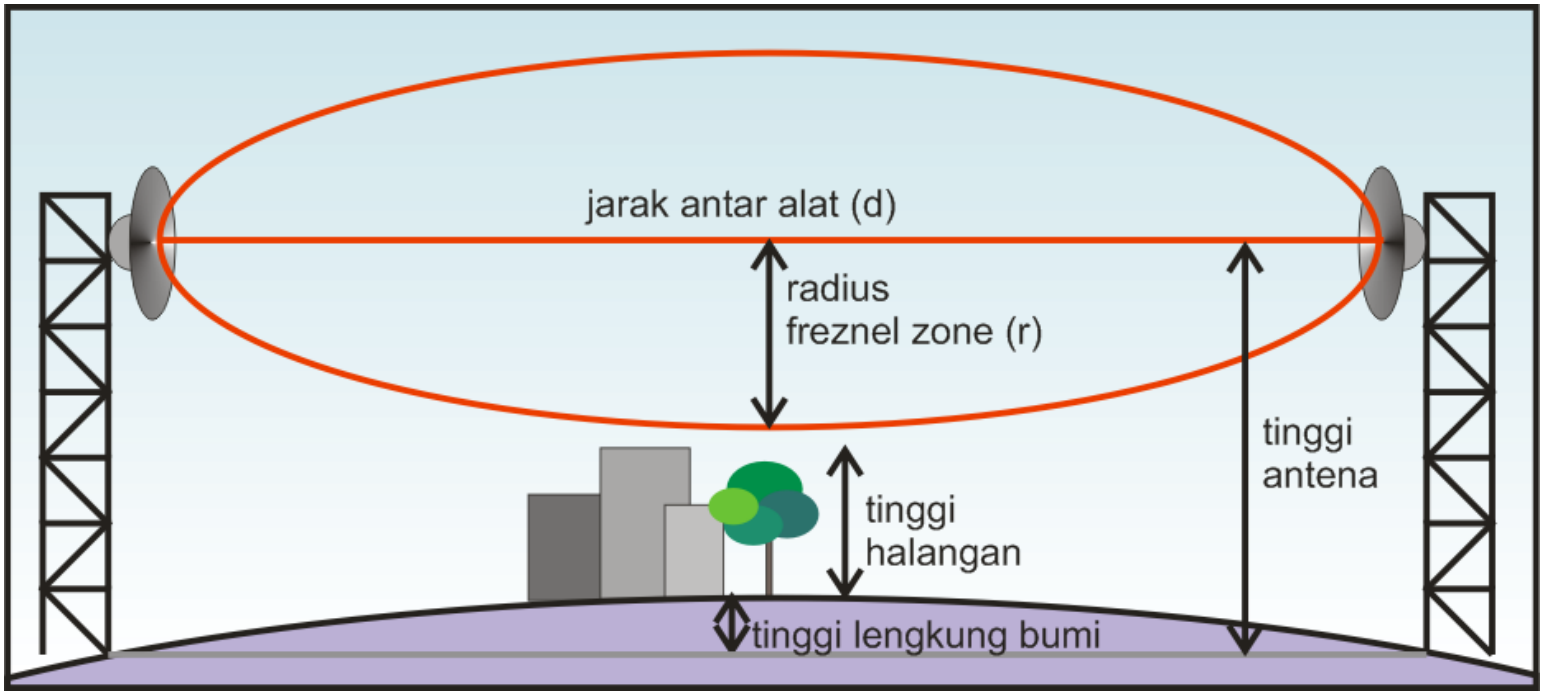
- Aplikasi Wireless LAN di luar ruangan harus memenuhi prinsip Line of Sight



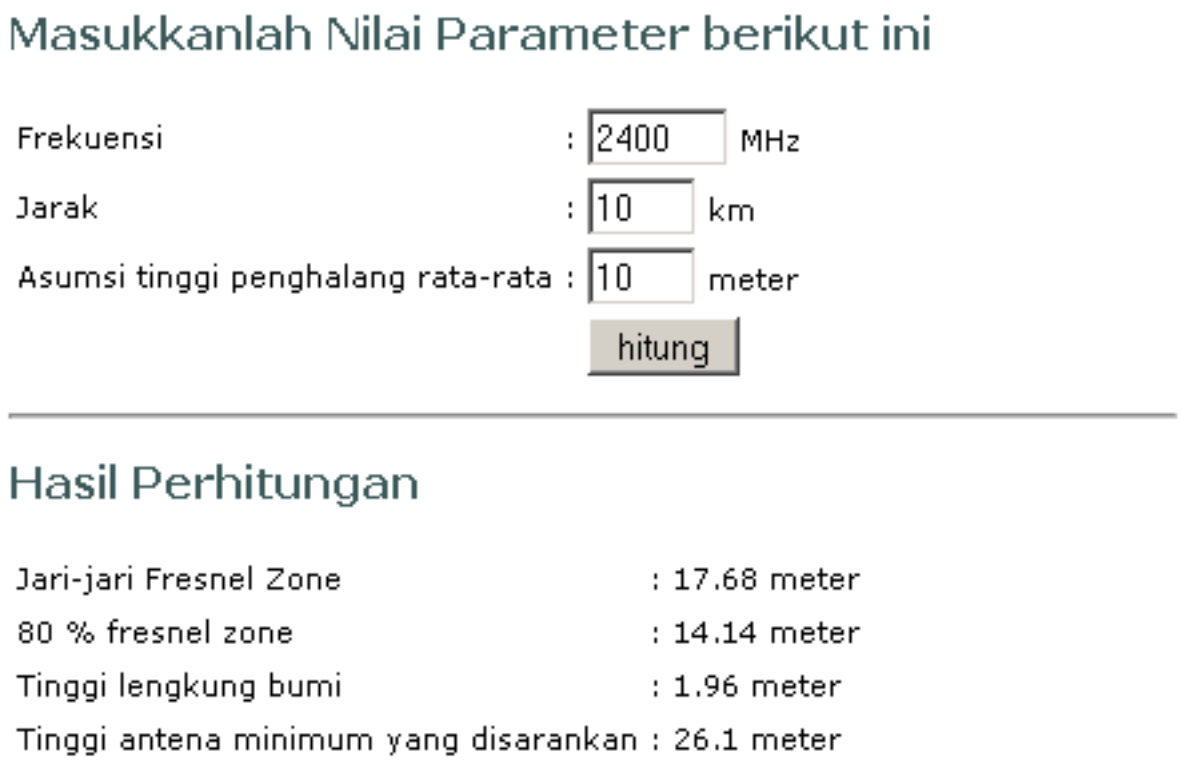
Ketinggian alat harus disesuaikan untuk mencapai line of sight

Earth Curve

- Untuk jarak yang cukup jauh, perencanaan ketinggian antena/tower harus memperhitungkan lengkung bumi.



Antena Height Calculator



- http://www.mikrotik.co.id/test_tower.php

Antenna Concept

- Directionality
  - Omnidirectional
  - Directional (limited range of coverage)
- Antenna Gain
  - In db
  - Higher db, longer distance coverage
- Polarization
  - Ussualy using vertical polarization

Omni Directional

Applications:

- 2.4 GHz ISM Band
- IEEE 802.11b, 802.11g Wireless LAN
- IEEE 802.11n (Pre-N, Draft-N, MIMO) Applications
- Bluetooth®
- WiFi
- Wireless Video Systems
- Multipoint and Mobile Applications

Features:

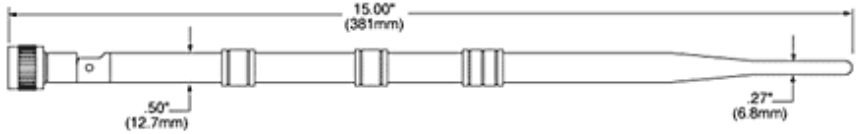
- Flexible "Rubber Duck" antenna
- Tilt and swivel design
- N-Male Connector
- RoHS Compliant

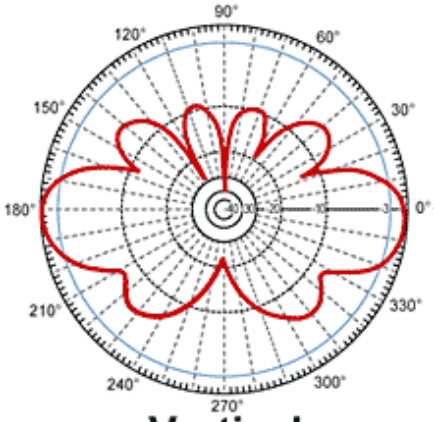
Electrical Specifications

- Frequency 2400-2500 MHz
- Gain 9 dBi
- Horizontal Beam Width 360°
- Vertical Beam Width 25°
- Impedance 50 Ohm
- Max. Power 50W
- VSWR < 2.0:1
- Lightning Protection DC Ground

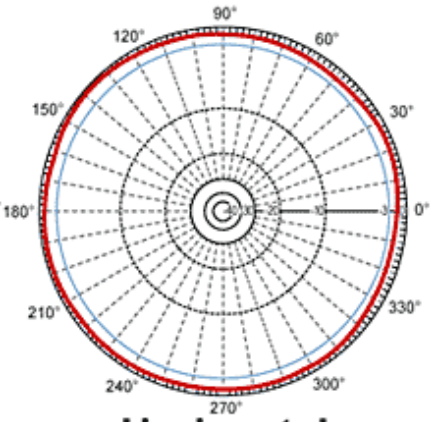
Mechanical Specifications

- Length 15" (381 mm)
- Max. Diameter 0.62" (15.7 mm)
- Finish Matte Black
- Connector N-Male
- Operating Temperature -40° C to to 60° C (-40° F to 140° F)
- Polarization Vertical
- Flame Rating: UL 94HB
- RoHS Compliant: Yes





Vertical



Horizontal

Flat Panel Antenna

Electrical

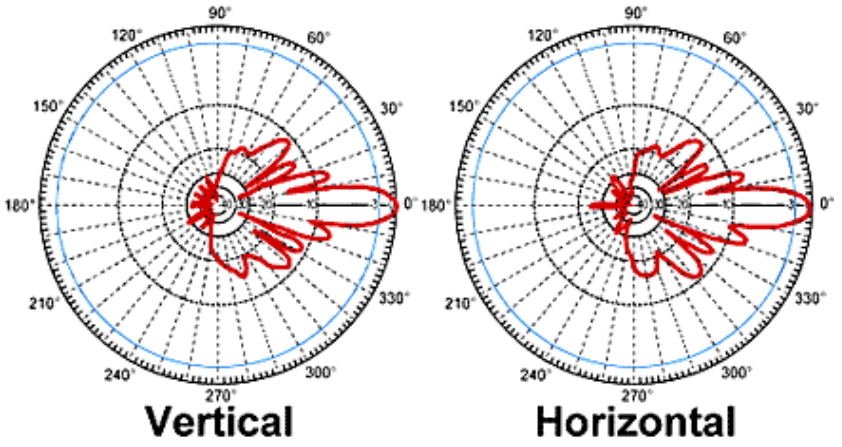
- **Frequency range:** 4.9 - 5.875 GHz
- **Gain,typ.:** 23 dBi @ 5.15-5.875 , 21 dBi @ 4.9-5.15
- **VSWR, max.:** 1.5 : 1@ 5.15-5.875 , 1.9: 1 @ 4.9-5.15
- **3 dB Beam-Width, H-Plane, typ.:** 10.5 °
- **3 dB Beam-Width, E-Plane, typ.:** 10.5 °
- **Side Lobes, min.:** -23 dB
- **Polarization:** Linear Vertical
- **Cross Polarization, min.:** -24 dB
- **Front to Back Ratio, min.:** -30 dB
- **Input power, max:** 30 Watt
- **Input Impedance:** 50 Ohm
- **Lightning Protection:** DC Grounded

Mechanical

- **Dimensions (HxWxD):** 305 x 305 x 15 mm (12"x12"x0.6")
- **Connector:** N-Type, Female
- **Back Plane:** Aluminum; protected through chemical passivation
- **Radome:** UV Protected Polycarbonate

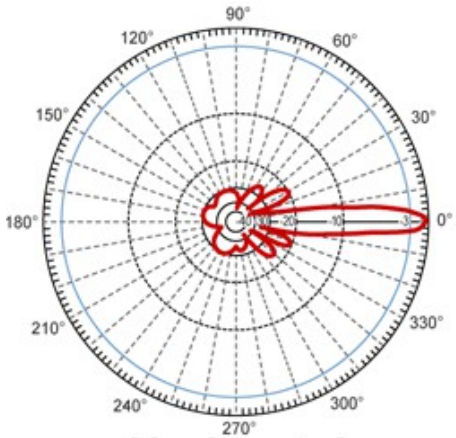
Environmemtal

- **Operating Temperature Range:** -40° C to +65° C
- **Vibration:** According to IEC 60721-3-4
- **Wind Load:** 200 km/h (survival)
- **Flammability:** UL94
- **Water Proofing:** IP-67
- **Humidity:** ETS 300 019-1-4, EN 302 085 (annex. A.1.1)
- **Ice and Snow:** 25 mm radial (survival)
- **Salt Fog:** According to IEC 68-2-11
- **Service Life:** > 10 years

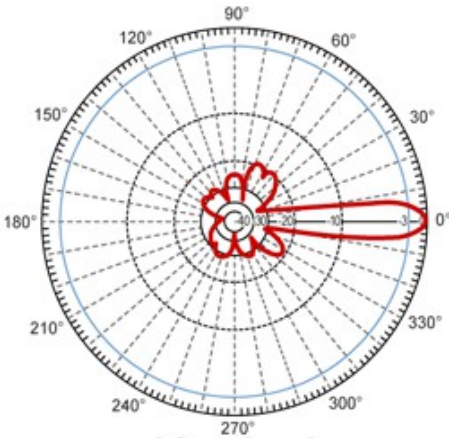


Grid Antenna

Model	HG5822G	HG5827G
Frequency	5725-5850 MHz	
Gain	22 dBi	27 dBi
Polarization	Horizontal or Vertical	
Horizontal Beam Width	10 °	6°
Vertical Beam Width	13 °	9°
Front to Back Ratio	25 dB	
Impedance	50 Ohm	
Max. Input Power	100 Watts	
VSWR	< 1.5:1 avg.	
Weight	3.0 lbs. (1.4 kg)	5.3 lbs. (2.4 kg)
Grid Dimensions	11.8 x 15.7 inches (300 x 400 mm)	15.7 x 23.6 inches (400 x 600 mm)
Mounting	2 in. (50.8 mm) diameter mast max.	
Operating Temperature	-40° C to to 85° C (-40° F to 185° F)	
Lighting Protection	DC Ground	
Connector	N-Female	



Horizontal



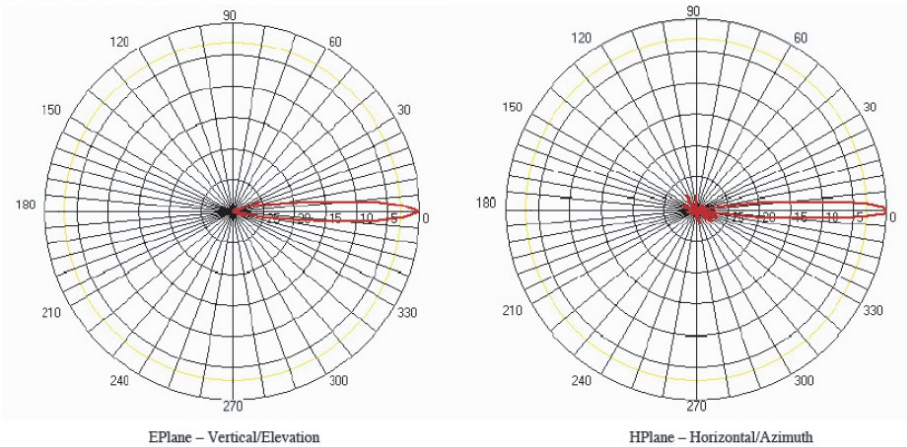
Vertical

Solid Disc Antenna

Spesifikasi Teknis

- **Frequency Band:** 5470 – 5725 MHz
- **Dimensions:** Diameter 500 mm
- **Gain:** 26,1 dBi
- **-3 dB Beamwidth:** 6°
- **Weight:** 1 500 g
- **Connector:** N – Female
- **Polarization:** Horizontal / Vertical
- **Impedance:** 50 ?
- **Material:** Aluminium + ABS

Antenna Patterns



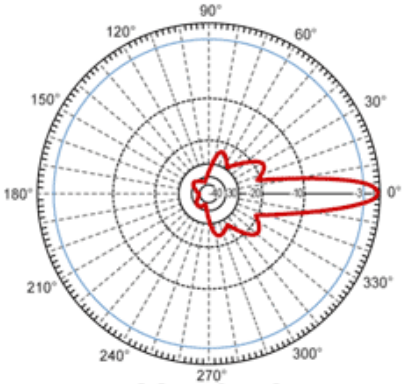
Biasanya digunakan untuk aplikasi point to point untuk jarak yang jauh.

Mounting pada tower harus baik, faktor angin cukup berpengaruh. Dibutuhkan ketelitian pointing.

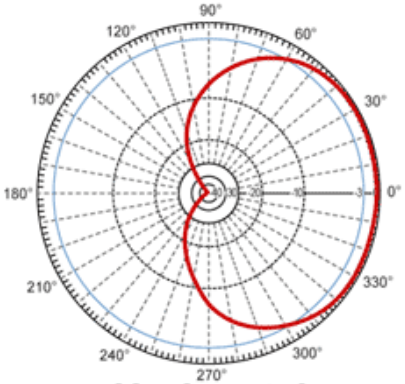
Sectoral Antenna

Frequency	2400-2500 MHz
Gain	20 dBi
Horizontal Beam Width	120 degrees
Vertical Beam Width	+/- 6.5°
Impedance	50 Ohm
Max. Input Power	250 Watts
VSWR	< 1.3:1 avg.
Connector	N Female
Lightning Protection	Direct Ground

Weight	12 lbs. (5.44 Kg)
Dimensions	39 x 9 x 2.5 inches (99 x 22.9 x 6.4 cm)
Radome Material	UV-Inhibited Polymer
Reflector Material	Aluminum
Operating Temperature	-40° C to to 85° C (-40° F to 185° F)
Mounting	2 inch (5 cm) O.D. pipe max.
Polarization	Vertical
Downtilt (mech)	0 to 20 degrees (adjustable)



Vertical

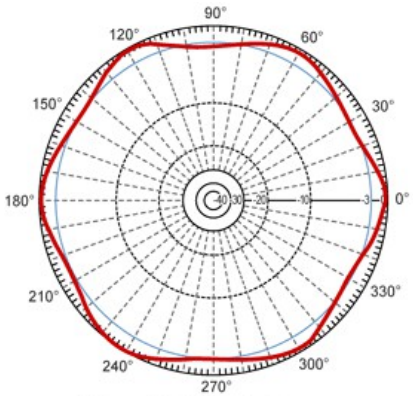


Horizontal

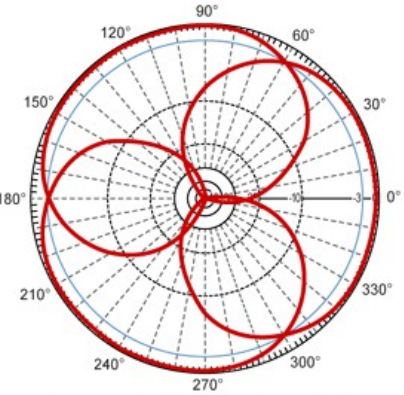
Sectoral Antenna (Array)

Models	HK2414-120	HK2417-120	HK2420-120
Frequency	2400 - 2500 MHz		
Antenna Gain	14 dBi*	17 dBi*	20 dBi*
Polarization	Vertical		
Horizontal Beam Width (Individual antenna)	120°	120°	120°
Vertical Beam Width (Individual antenna)	15°	6.5°	6.5°
Lightning Protection	DC Ground		
Power Rating (Single Fed)	25 Watts		
Antenna Radome Material	UV-inhibited Plastic		
Mounting System Material	Stainless Steel		
Mounting (Round Mast)	1¼" to 2" (31.7 to 50.8 mm) dia.		
Mounting (Square Mast/Beam)	3¼" (82.5 mm) square max.		
Dimensions **(O.D. Panels Fully Retracted)	20" (508 mm) x 17" (432 mm) O.D.**	39" (990 mm) x 17" (432 mm) O.D.**	39" (990 mm) x 17" (432 mm) O.D.**
Weight	14 lbs. (6.3 kg)	31 lbs. (14 kg)	44 lbs. (20 kg)

* Antenna gains specified when sectors are individually fed.



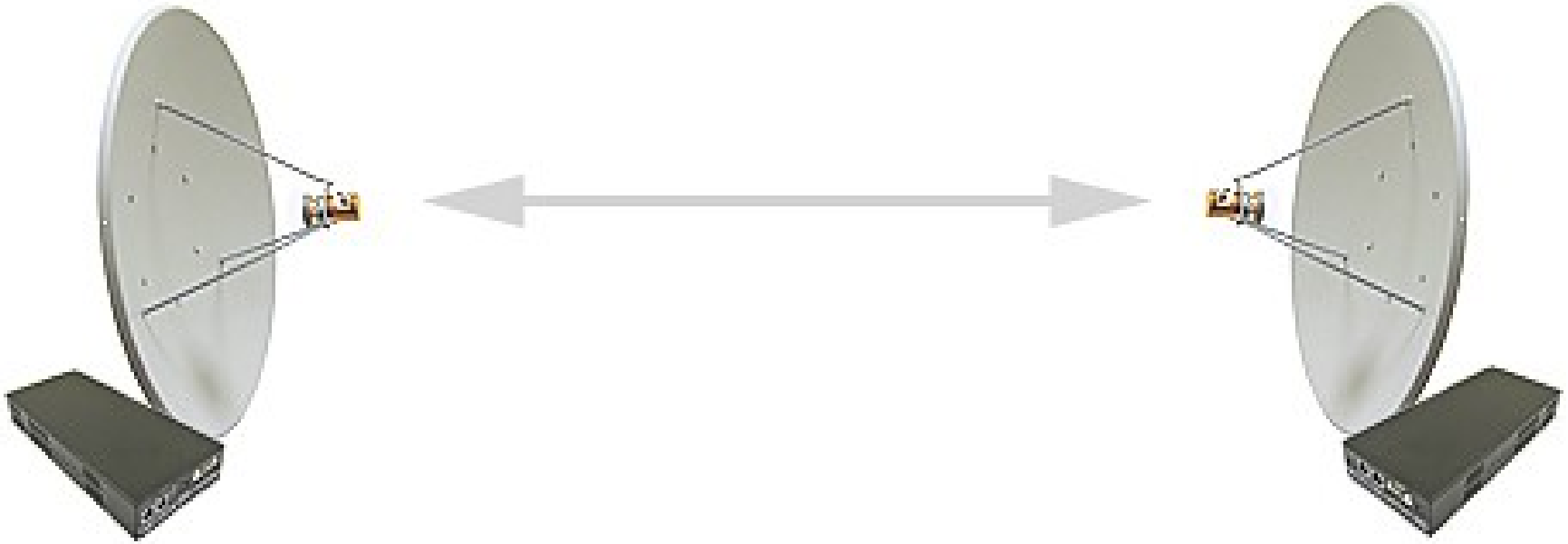
Single Fed Array



Individual Fed Array

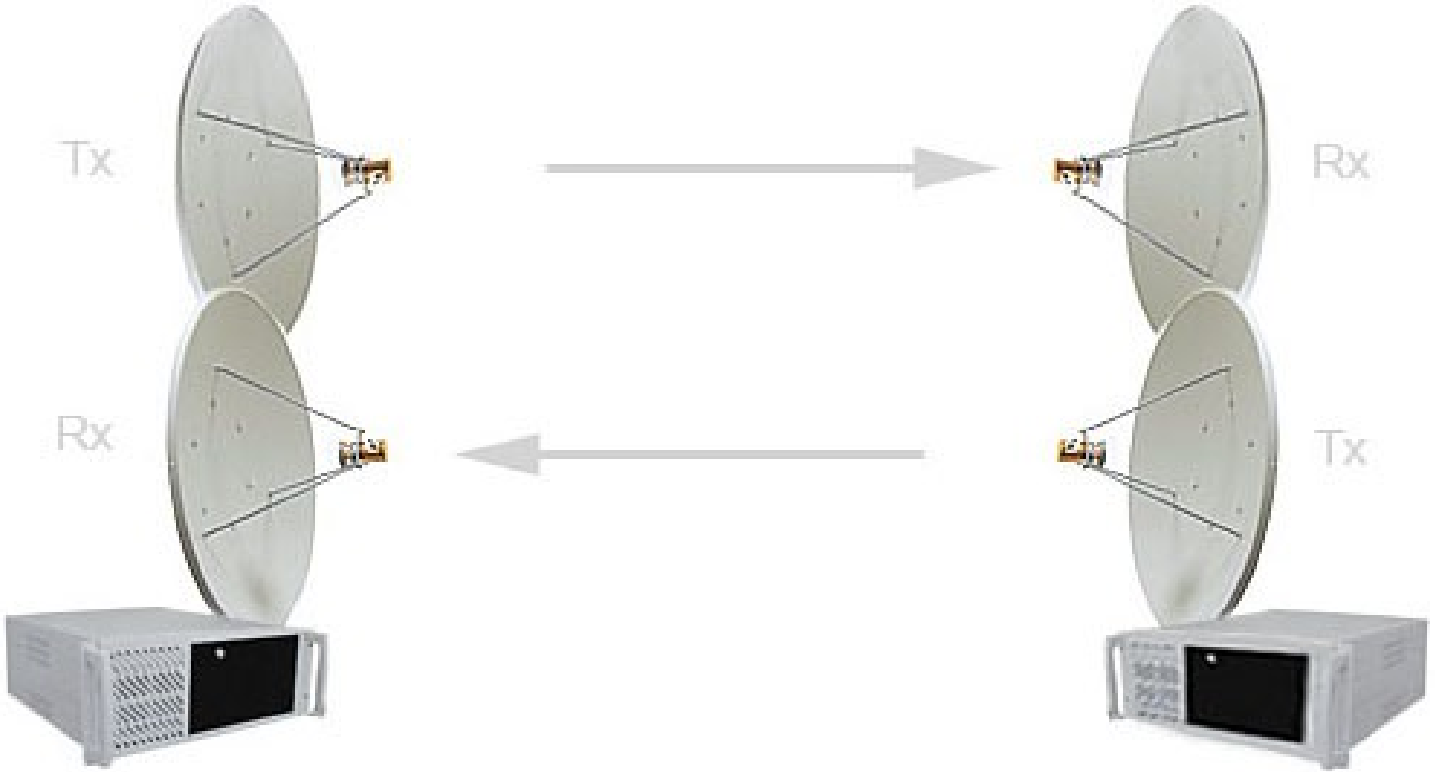
Point to Point

- Menghubungkan 2 buah alat, biasanya menggunakan antenna directional dan jarak yang cukup jauh
- Kedua alat cukup menggunakan lisensi level 4 : Bridge dan Station
- Bisa menggunakan proprietary setting (nstream, Custom Frequency)



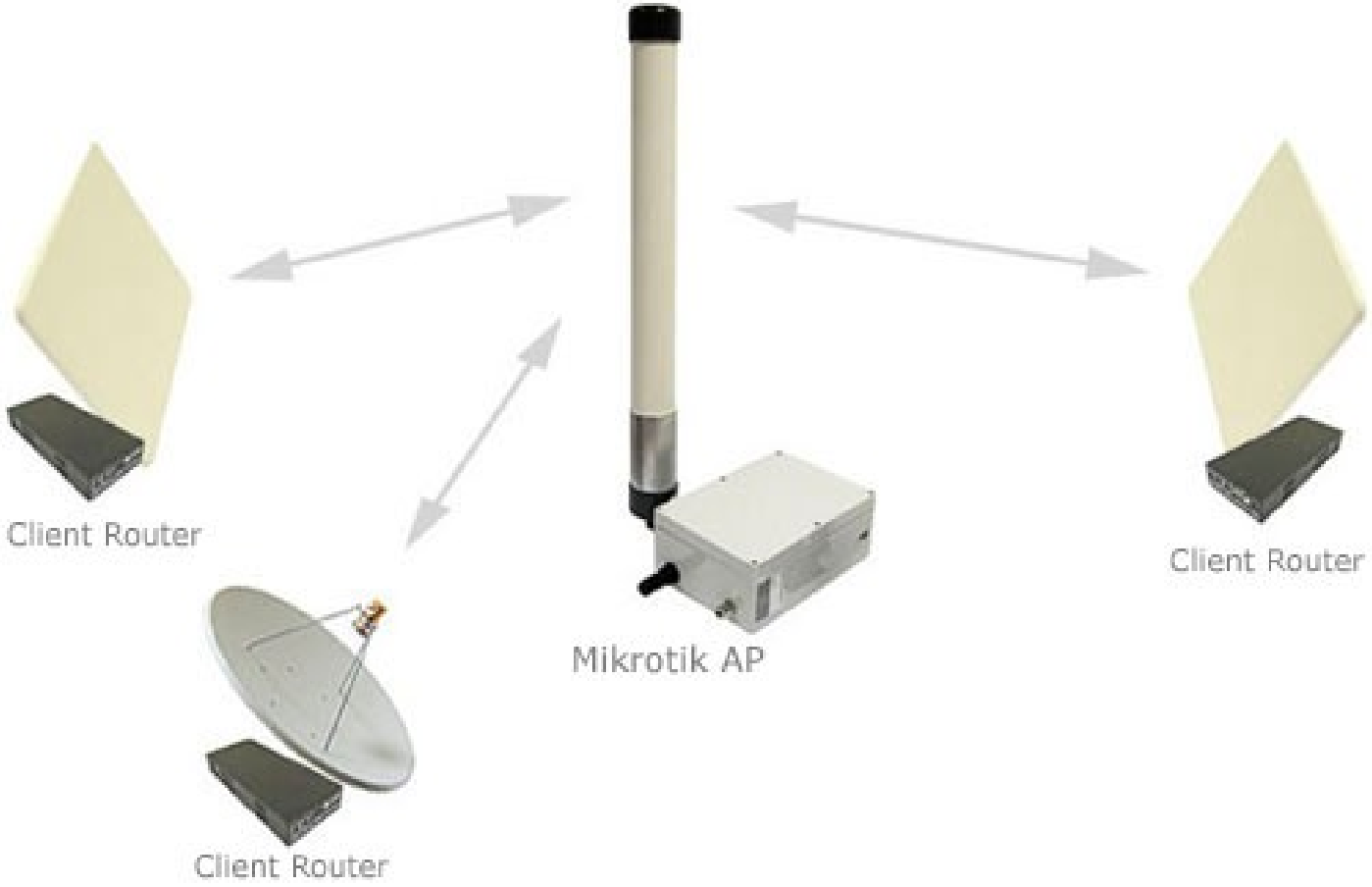
Point to Point (Dual Nstream)

- Masing-masing titik menggunakan 2 buah antena dan 2 buah wireless card
- Satu link untuk transmit dan satu link untuk receive.
- Mikrotik proprietary setting



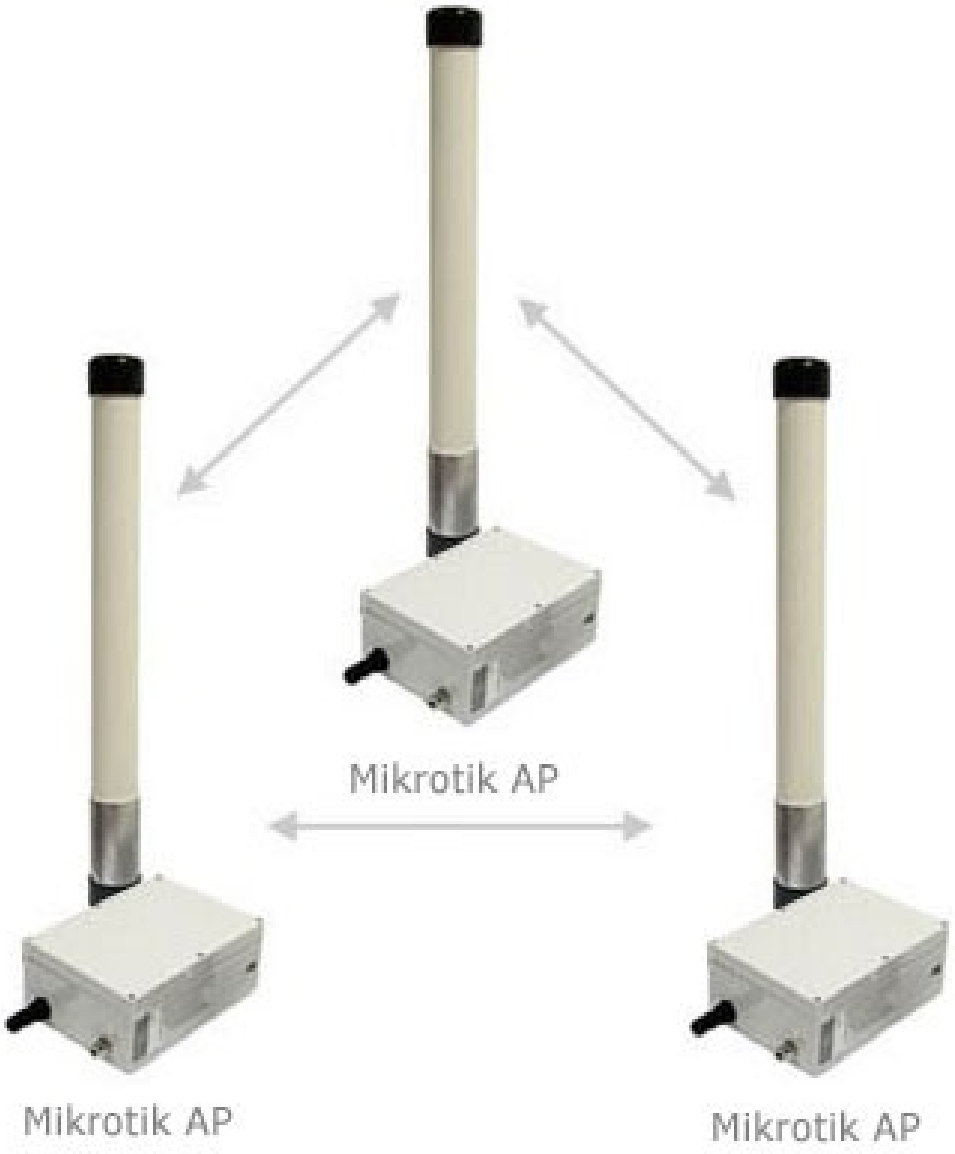
Point to Multipoint

- 1 buah AP Mikrotik sebagai base station untuk melayani CPE



Wireless Distribution System (WDS)

- WDS (Wireless Distribution System) is the best way how to interconnect many access points and allow users to move around without getting disconnected from network.



Wireless Configuration

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

Wireless Configuration

- Basic Configuration :
  - **Wireless Tools** – Scan, Snoop, Freq-Usage (site survey)
  - **Point to Point** – only "**one**" Client
  - **Registration Table** – Wireless Link Monitoring
  - **Wireless N (example)** – For "**N Wireless Card**"
  - **Wireless Bridge** – Inter-building Connection
  - **Point to Multi Point** – more than one Client
  - **Access List** – **mac-address** security
  - **Wireless Security** – **Encryption** wireless security
- Wireless Protocol
  - **VAP** – Virtual Access Point
  - **Nstreme** – Mikrotik Wireless Performance Protocol
  - **WDS** – Wireless Mesh Network

Scan Tool

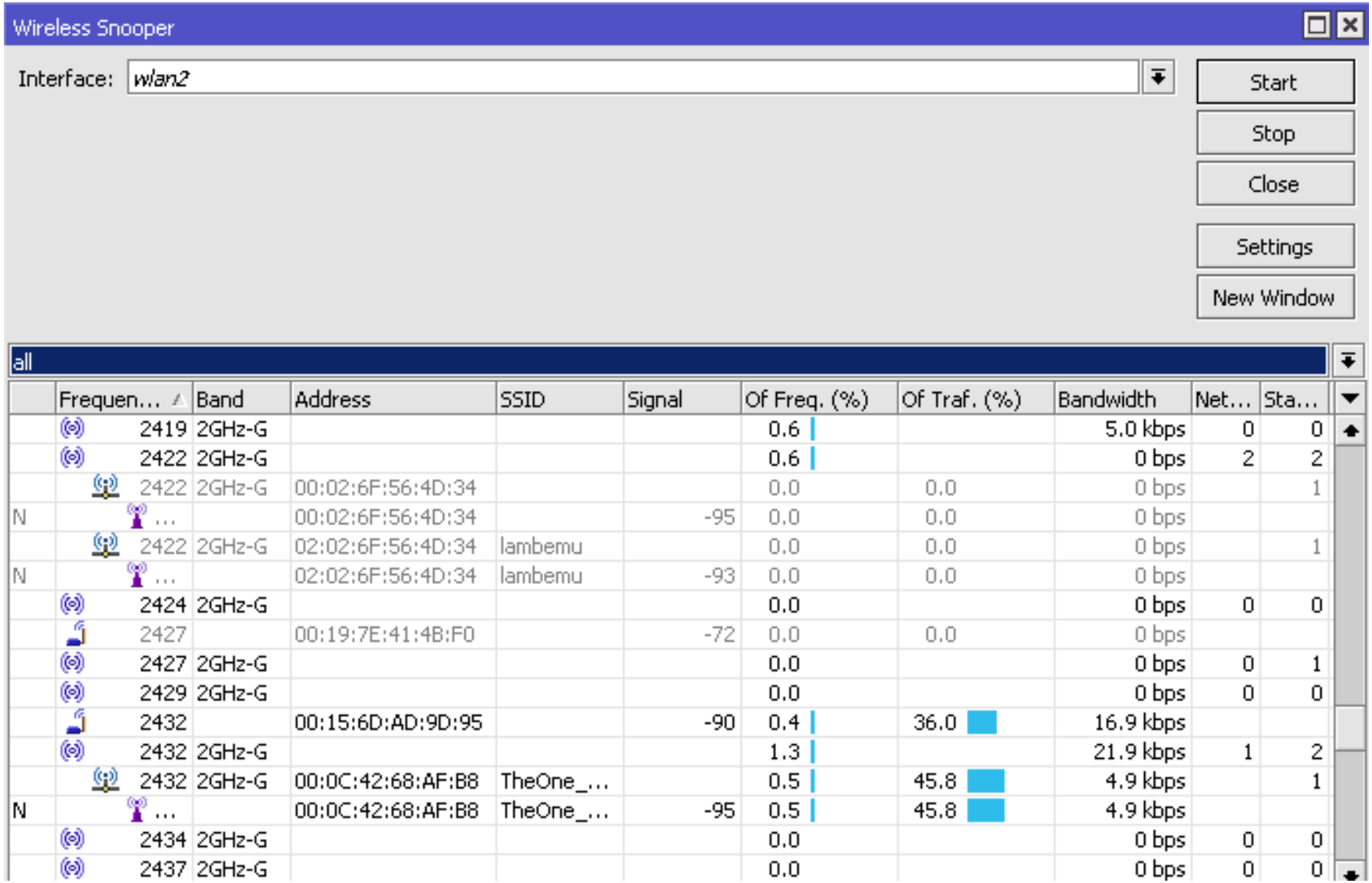
Scanner (Running)

Interface: wlan2

Start | Stop | Close | New Window | Connect | Use Network

	Address	SSID	Band	Cha...	Freq...	Sign...	Nois...	Sign...	Radio Name	Router...
BR	00:21:A4:35:00:37	Ndalem ...	2GHz-G	20Mhz	2412	-43	-100	57	0021A4350037	5.3
BR	00:02:6F:56:4D:34		2GHz-G	20Mhz	2422	-92	-101	9	Maspion Rukun...	3.4
BR	02:02:6F:56:4D:34	lambemu	2GHz-G	20Mhz	2422	-92	-101	9	Maspion Rukun...	3.4
BR	02:02:6F:56:4D:35	kijing	2GHz-G	20Mhz	2422	-91	-101	10	Maspion Rukun...	3.4
BR	00:15:6D:65:F7:E5	Giant4	2GHz-G	20Mhz	2447	-92	-103	11	00156D65F7E5	3.25
BP	00:4F:62:28:4D:75	airlive	2GHz-G	20Mhz	2462	-92	-103	11		

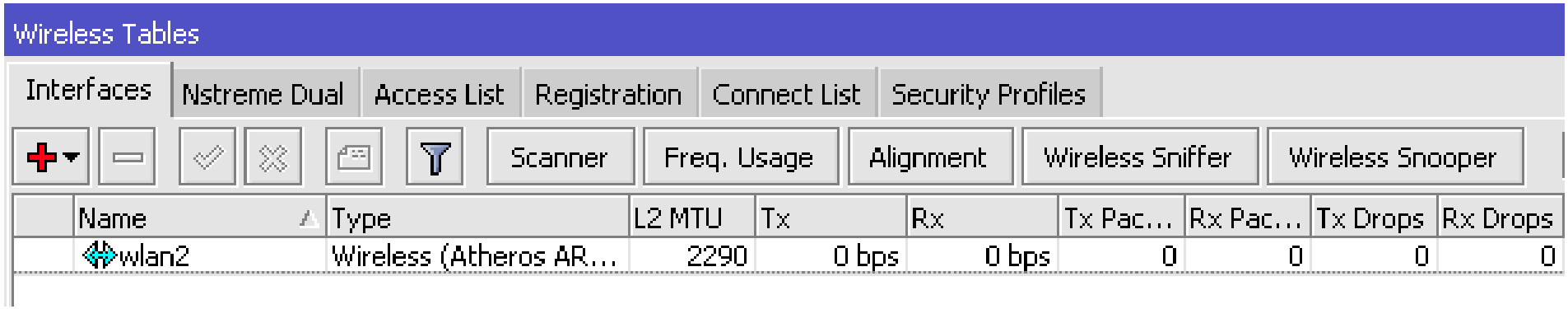
Snoop Tool



	Frequen...	Band	Address	SSID	Signal	Of Freq. (%)	Of Traf. (%)	Bandwidth	Net...	Sta...
	2419	2GHz-G				0.6		5.0 kbps	0	0
	2422	2GHz-G				0.6		0 bps	2	2
	2422	2GHz-G	00:02:6F:56:4D:34			0.0	0.0	0 bps		1
N	...		00:02:6F:56:4D:34		-95	0.0	0.0	0 bps		
	2422	2GHz-G	02:02:6F:56:4D:34	lambemu		0.0	0.0	0 bps		1
N	...		02:02:6F:56:4D:34	lambemu	-93	0.0	0.0	0 bps		
	2424	2GHz-G				0.0		0 bps	0	0
	2427		00:19:7E:41:4B:F0		-72	0.0	0.0	0 bps		
	2427	2GHz-G				0.0		0 bps	0	1
	2429	2GHz-G				0.0		0 bps	0	0
	2432		00:15:6D:AD:9D:95		-90	0.4	36.0	16.9 kbps		
	2432	2GHz-G				1.3		21.9 kbps	1	2
	2432	2GHz-G	00:0C:42:68:AF:B8	TheOne_...		0.5	45.8	4.9 kbps		1
N	...		00:0C:42:68:AF:B8	TheOne_...	-95	0.5	45.8	4.9 kbps		
	2434	2GHz-G				0.0		0 bps	0	0
	2437	2GHz-G				0.0		0 bps	0	0

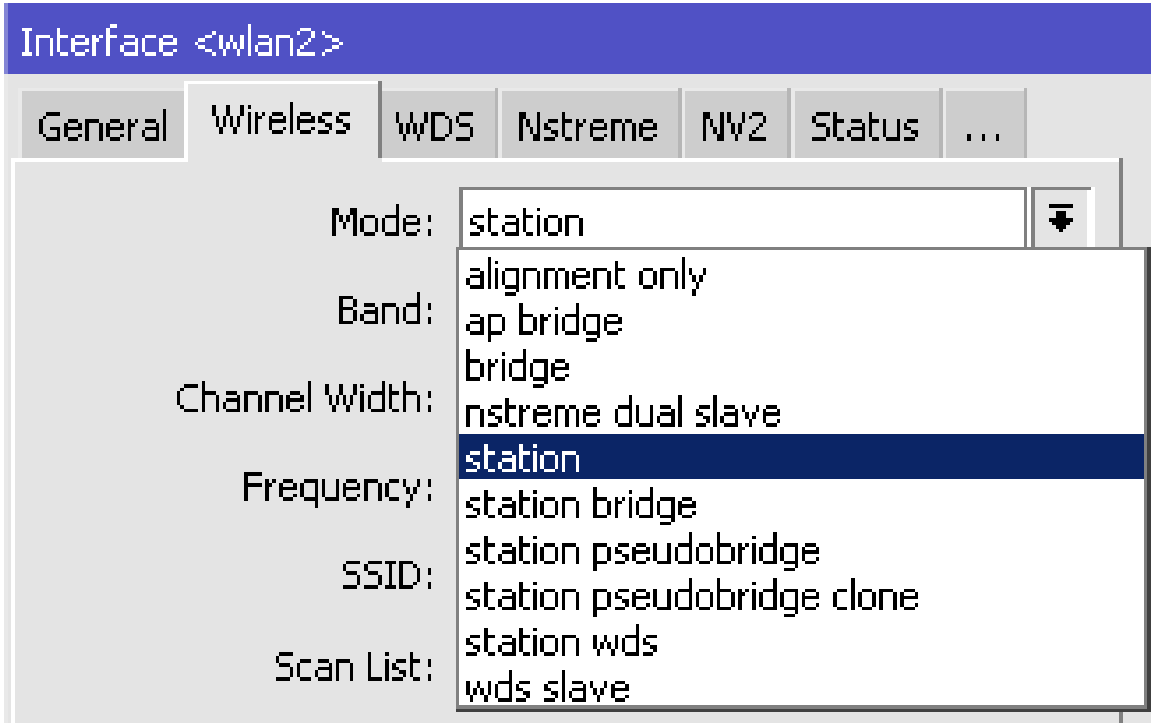
Wireless Menu

- Wireless Menu:
  - **Interface** – Daftar Interface wireless yang terpasang
  - **Access-List** – Security Mac-address Client (AP Mode)
  - **Registration** – Daftar Wireless yang terkoneksi
  - **Connect-List** – Security Mac-address AP (Station Mode)
  - **Security-Profile** – Konfigurasi Wireless Security (WPA/WEP)



Wireless Mode List

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



Wireless Mode - 1

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

Wireless Mode – 2

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

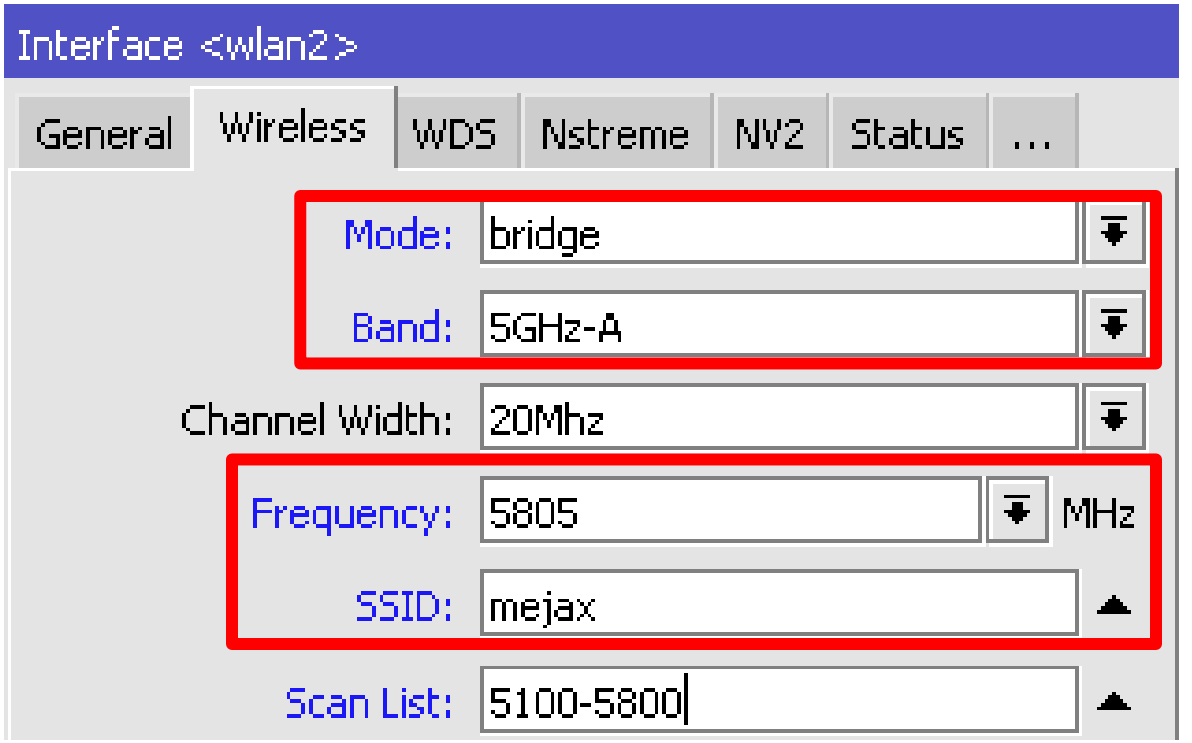
[LAB-1] Point to Point

- **AP Side**
  - Mikrotik Min Licence Level 3
  - Set mode, ssid, band, frequency
  - mode=bridge
    - Can serve only 1 station

- **Client Side**
  - Mikrotik Min Licence Level 3
  - Set mode, ssid, band, scan-list
  - mode=station
  - Make sure frequency is in scan-list

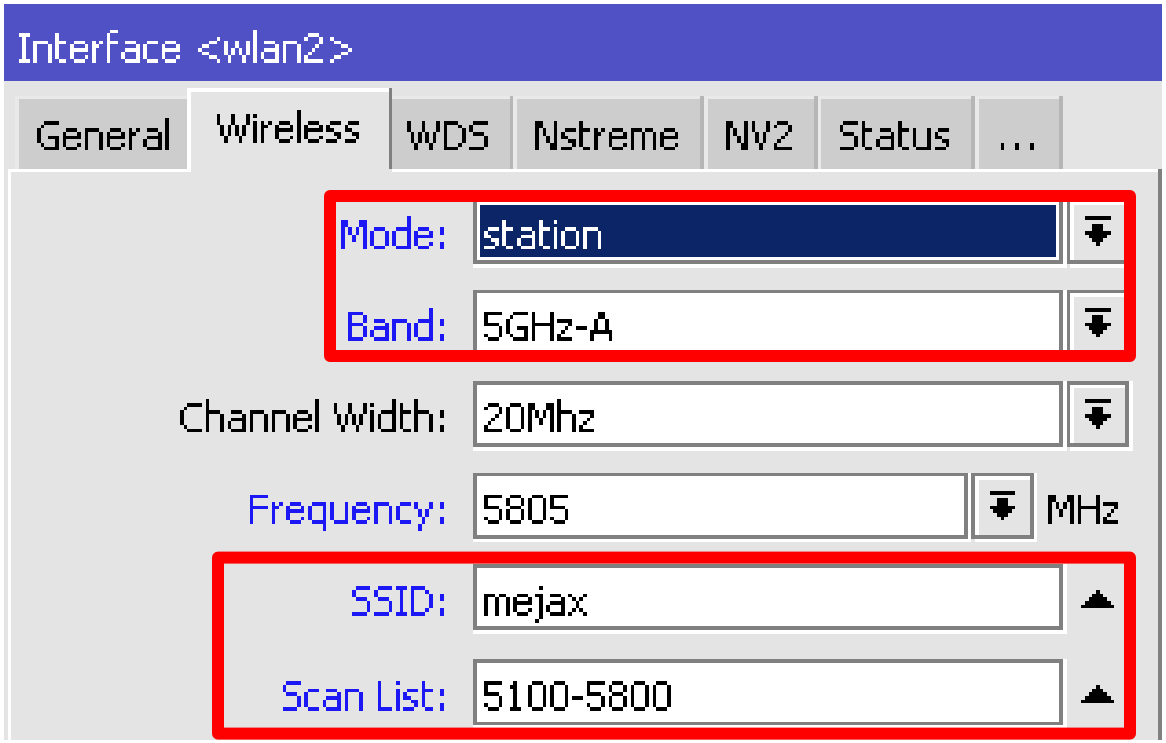
[LAB-1] P2P (AP Side)

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

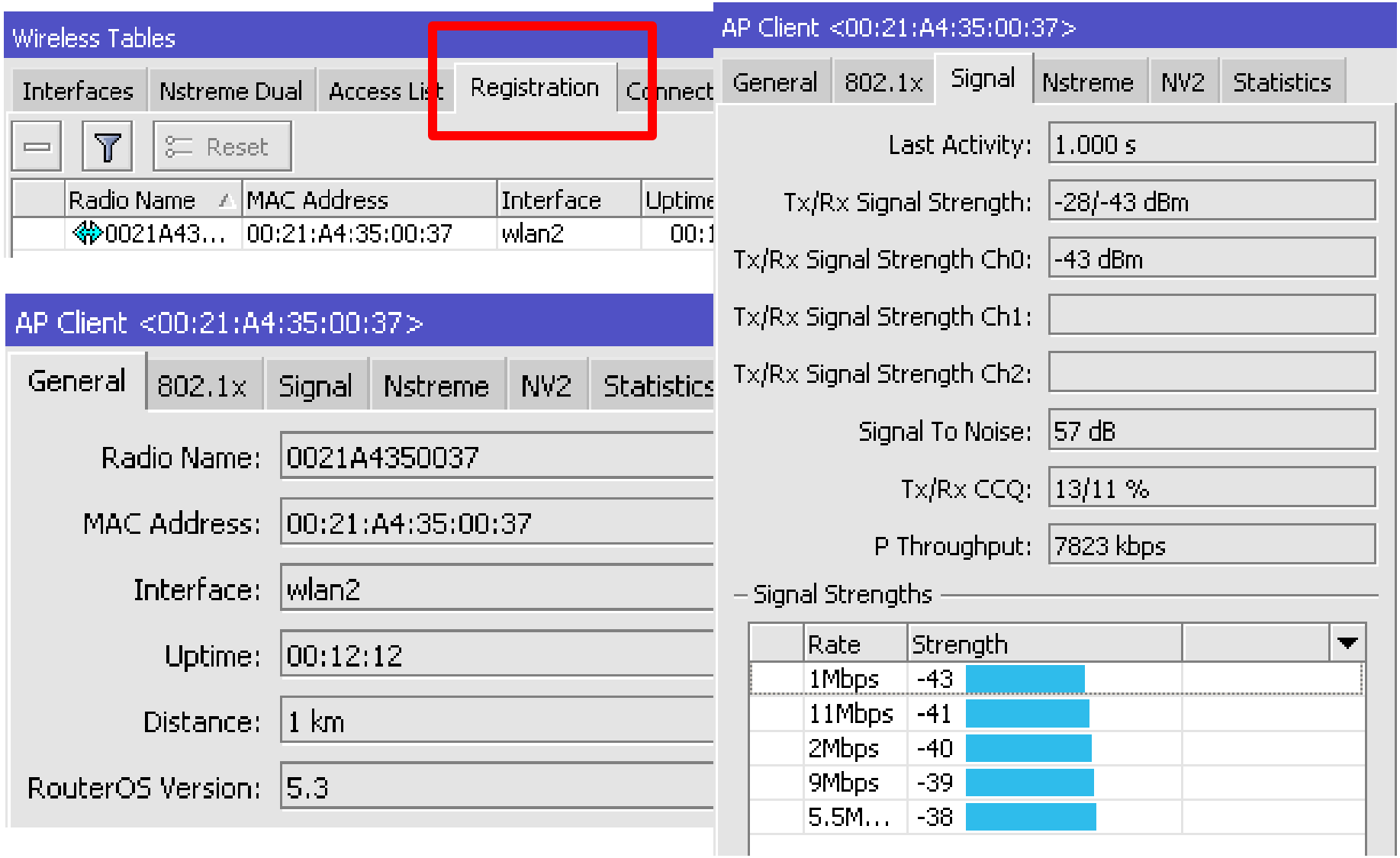


[LAB-1] P2P (Client Side)

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

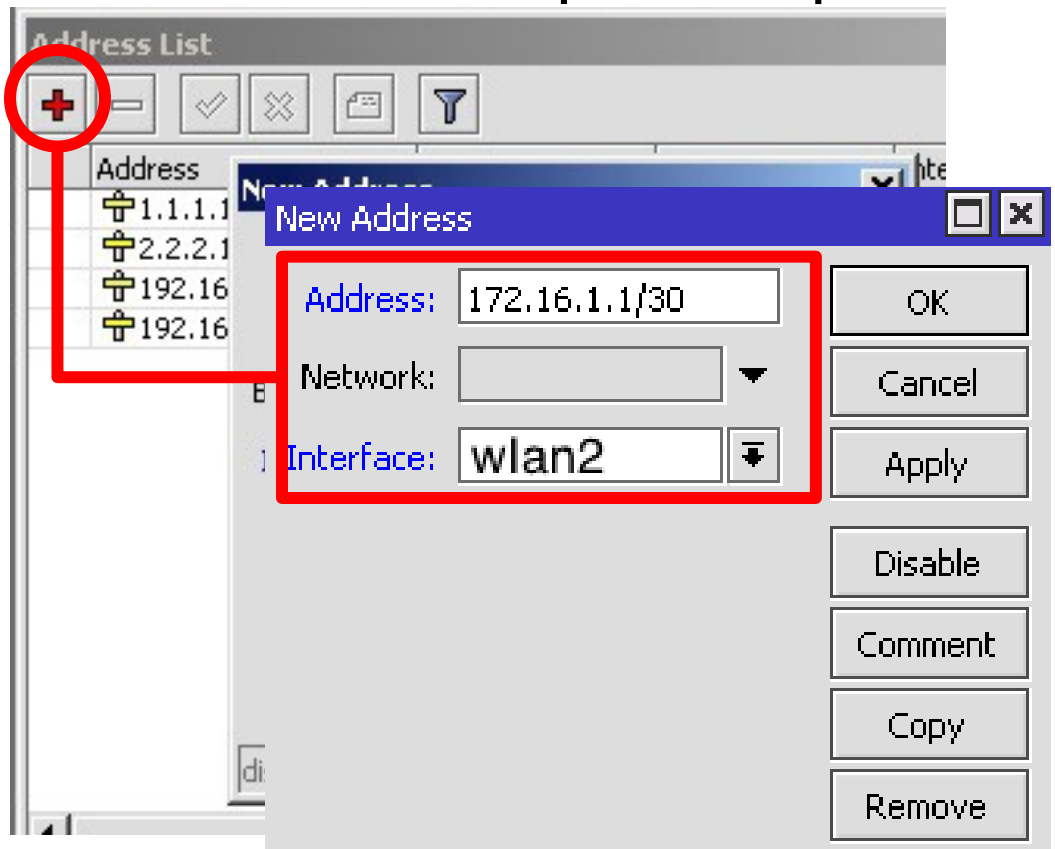


Monitoring Wireless Interface

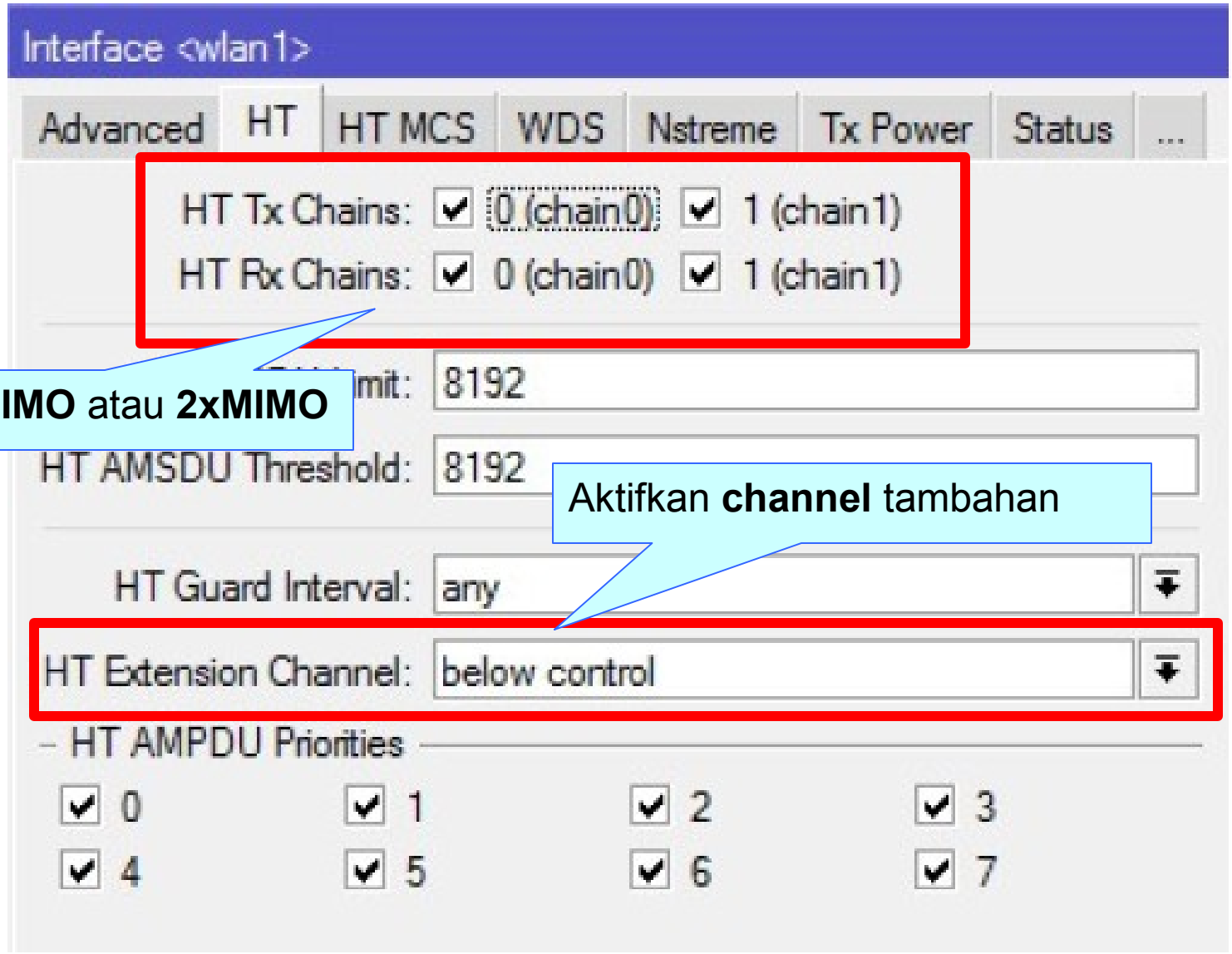


[LAB-2] Point to Point Test

- Tambahkan IP address di interface **Wlan2**.
- Test koneksi wireless kedua router dengan tool Ping.
- Setelah test ping berhasil maka wireless point-to-point sudah siap.



Wireless N Config - Example



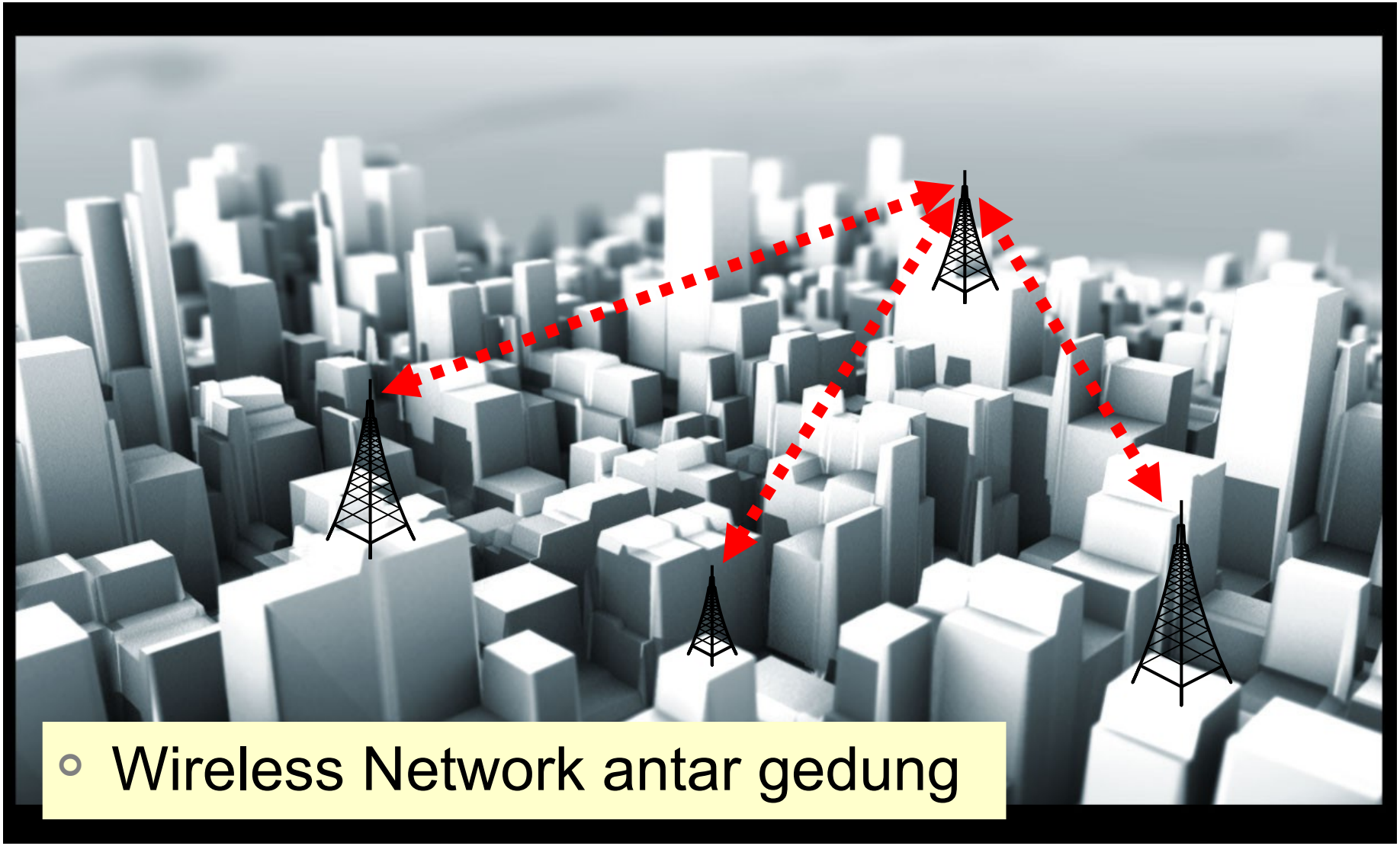
Aktifkan **1xMIMO** atau **2xMIMO**

Aktifkan **channel** tambahan

Wireless Bridge

- Mikrotik **Station** mode **“tidak bisa”** langsung dimasukkan ke bridge port (keterbatasan protocol)
- maka?
  - Bisa menggunakan **EoIP** antara **ap-bridge** and **station** – seperti pada lab di materi bridge
  - Pilihan kedua menggunakan mode **WDS-station!** (Troughput drop…).
  - Pilihan ke 3 menggunakan mode baru yaitu **station-pseudobridge**

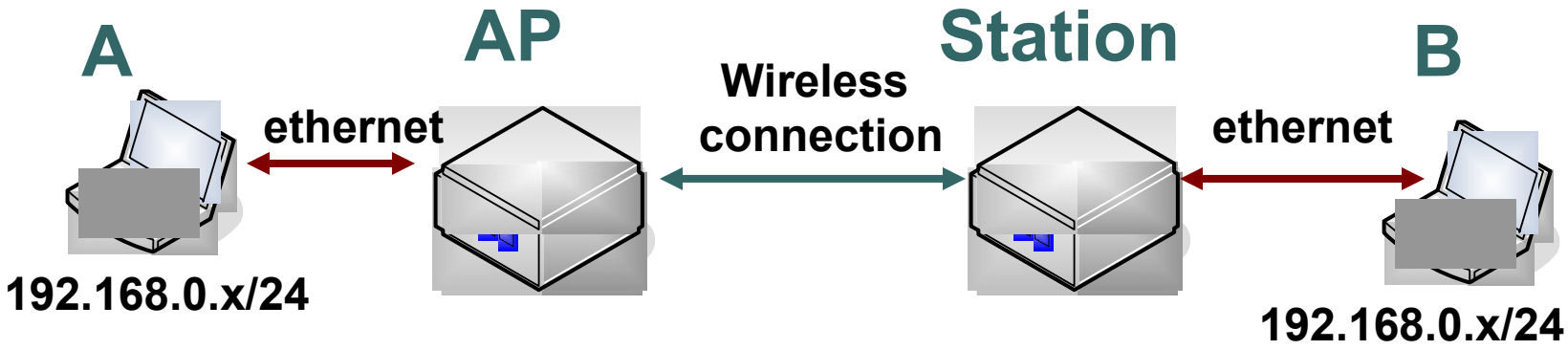
Wireless Bridge - Implementation



- Wireless Network antar gedung

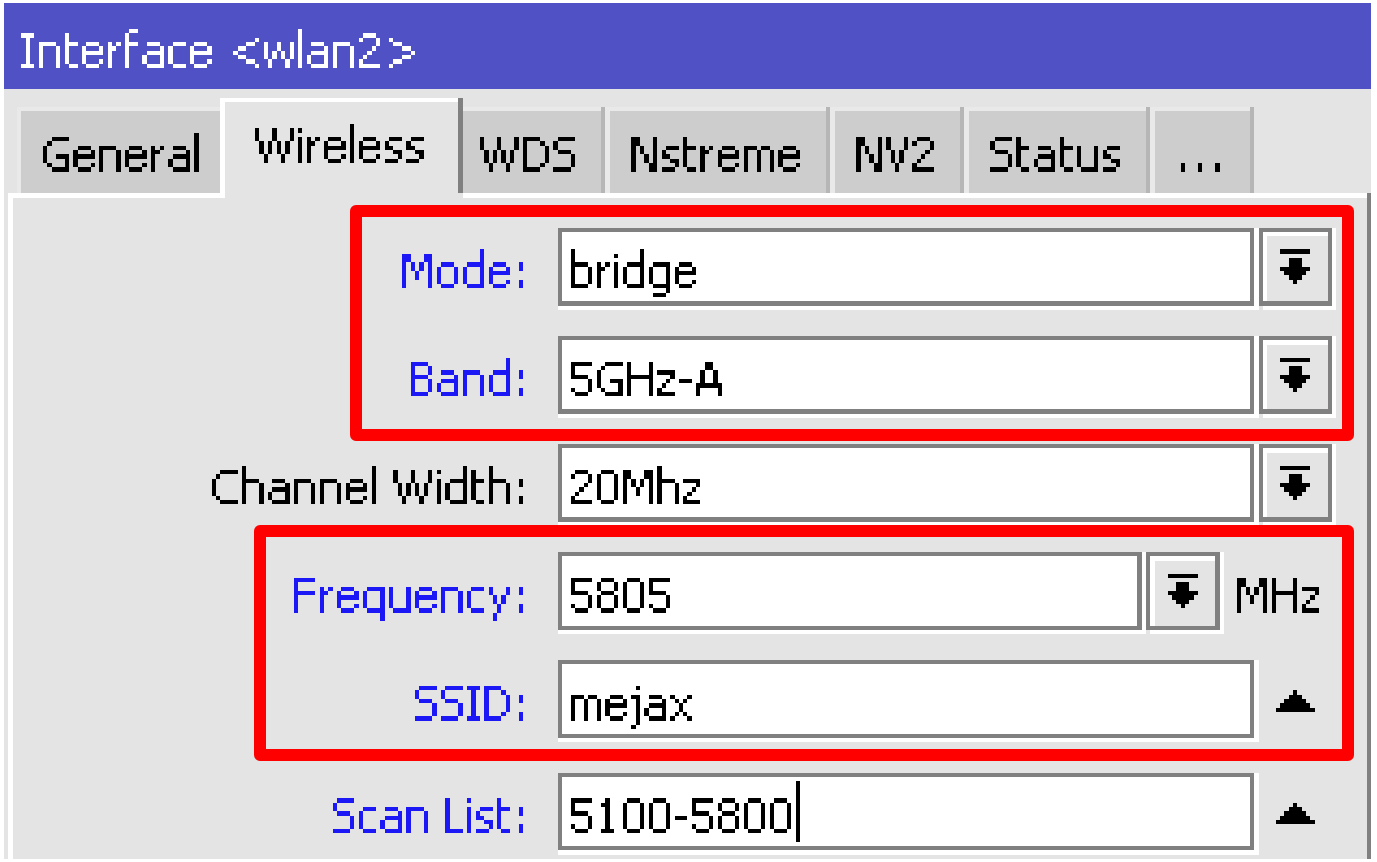
[LAB-3] Wireless Bridge

- Buatlah konfigurasi **AP** vs **client** yang digunakan untuk Bridge Network via wireless, sisi client menggunakan mode **station-pseudobridge**.
- Setelah wireless sudah terkoneksi masukkan interface wireless Wlan2 dan ether1 ke dalam **Bridge Port** (dilakukan di kedua router). Maka laptop kedua sisi bisa berkomunikasi dalam satu segmen.



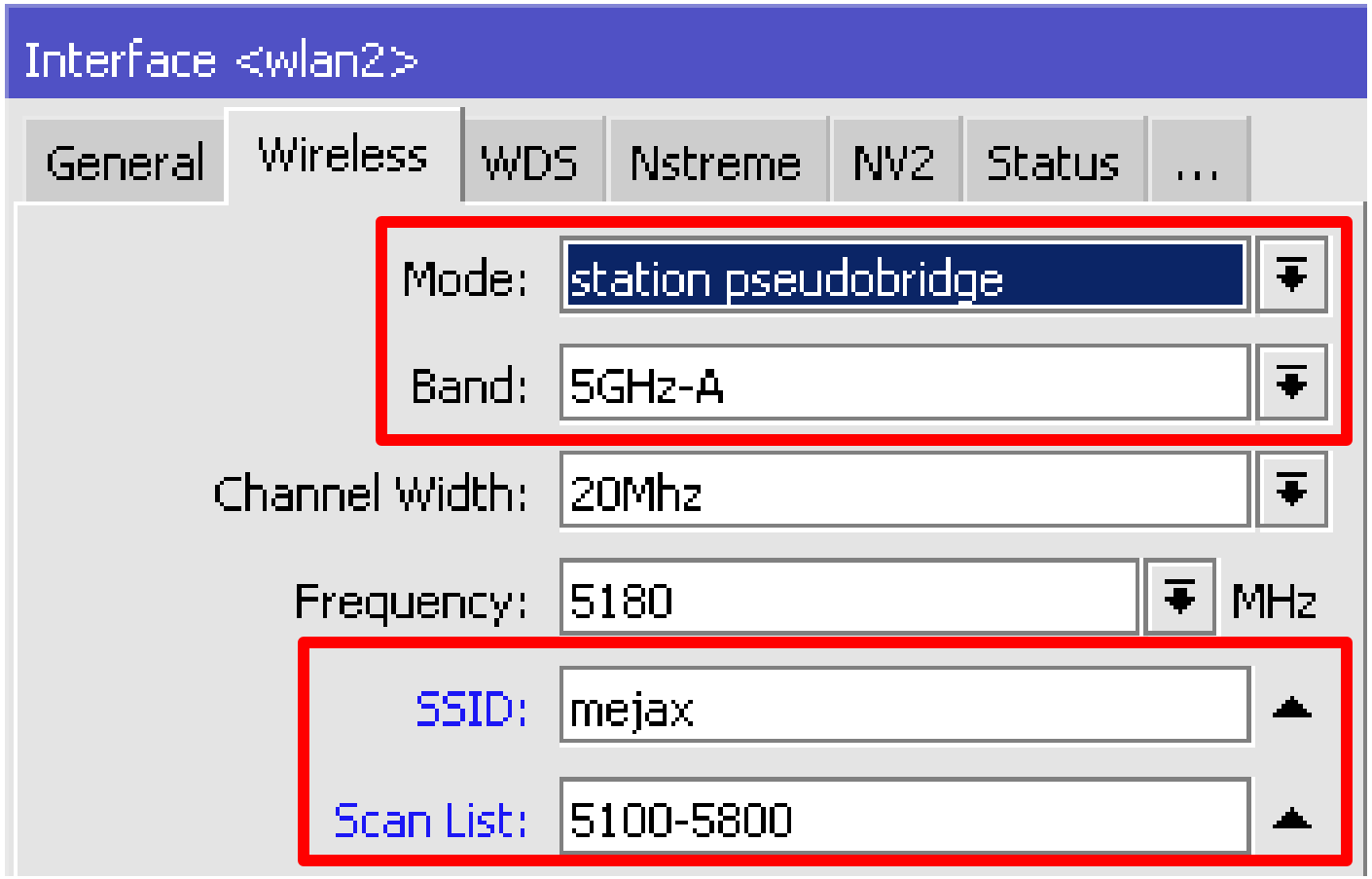
[LAB-3] Wireless Bridge – AP side

- AP Side using Bridge Mode

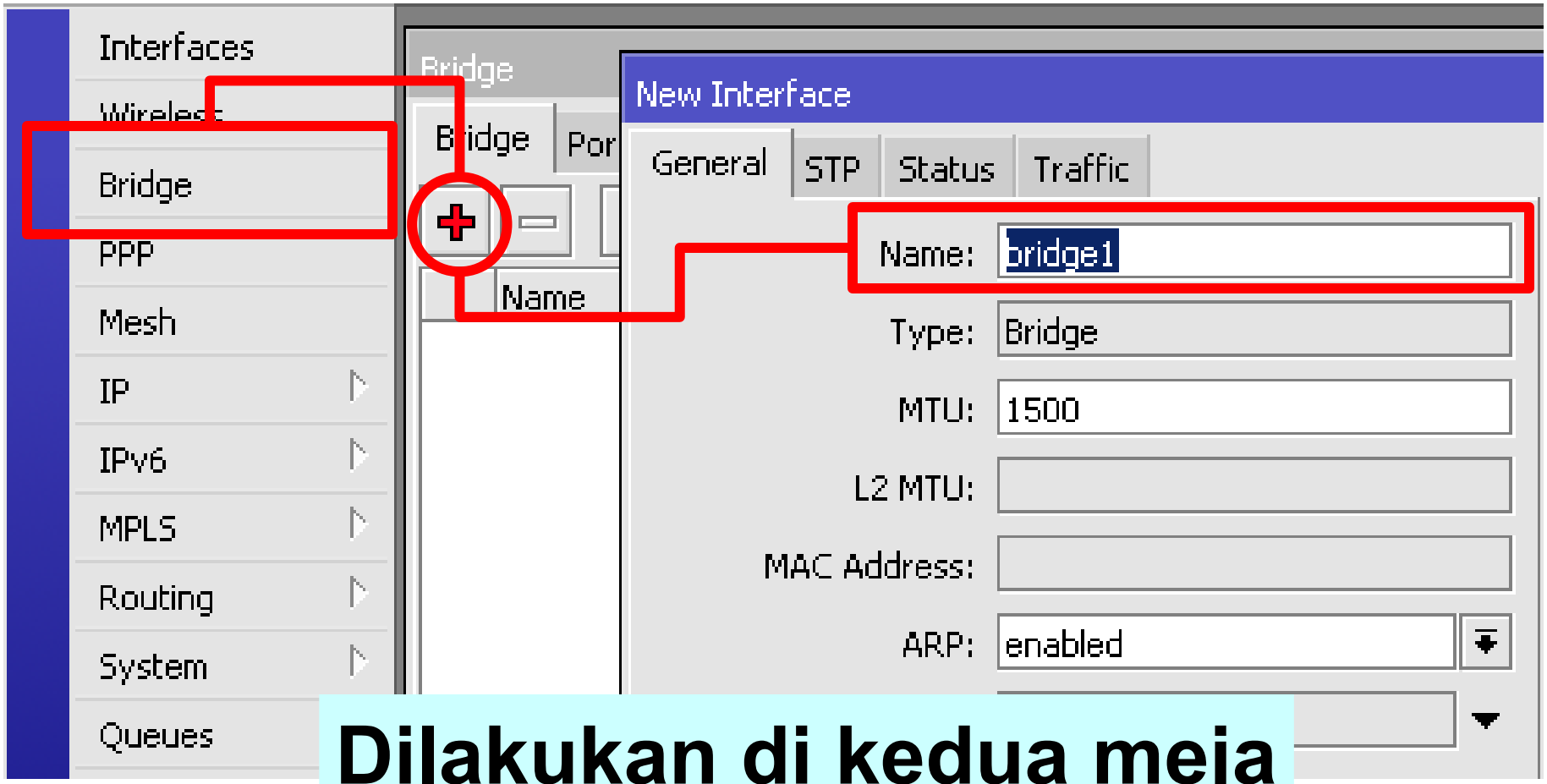


[LAB-3] Wireless Bridge – Client side

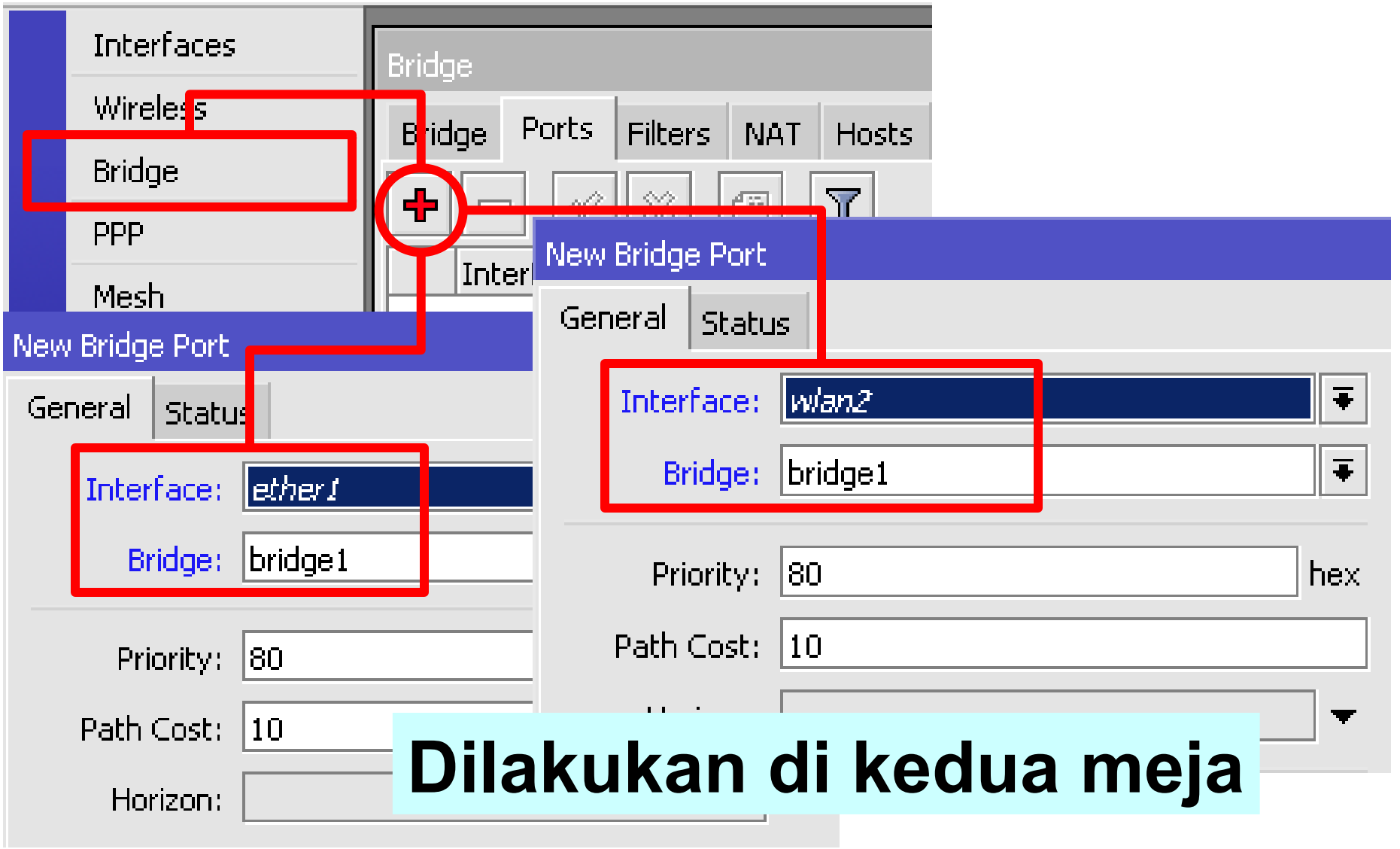
- Client Side:
  - Set mode= **station-pseudobridge**



[LAB-3] Wireless Bridge- Bridge Config



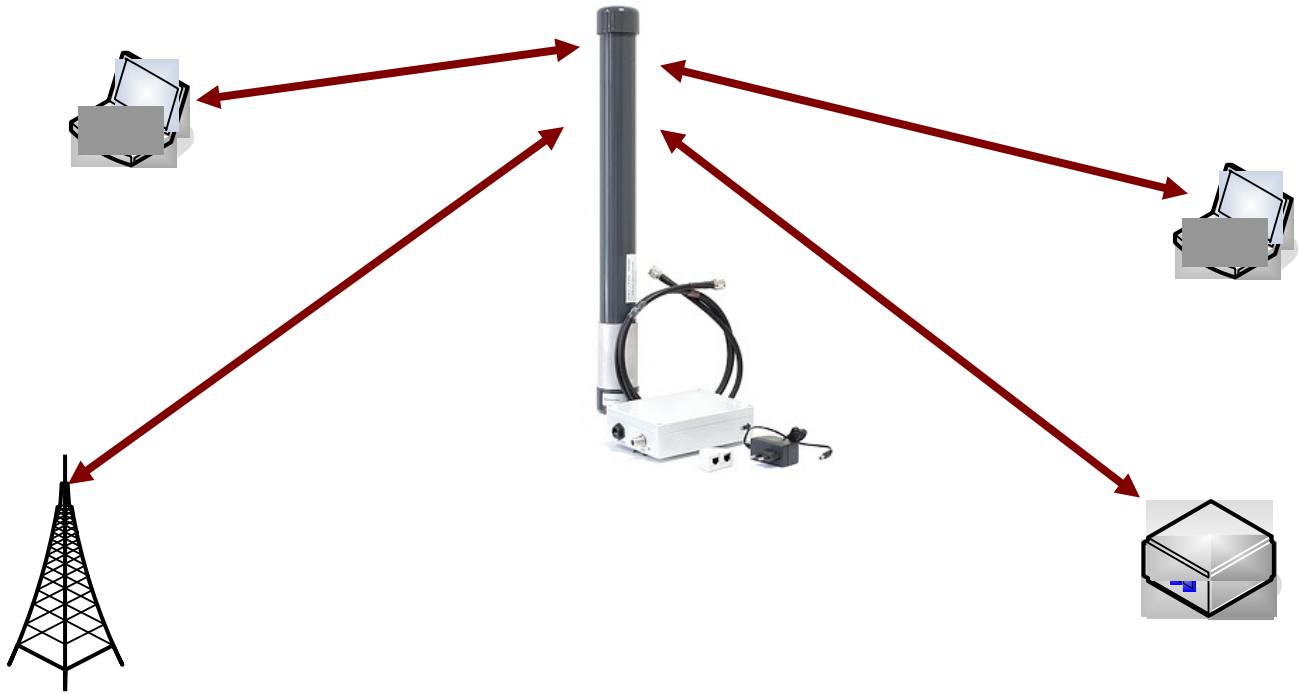
[LAB-3] Wireless Bridge – Bridge Ports Config



Dilakukan di kedua meja

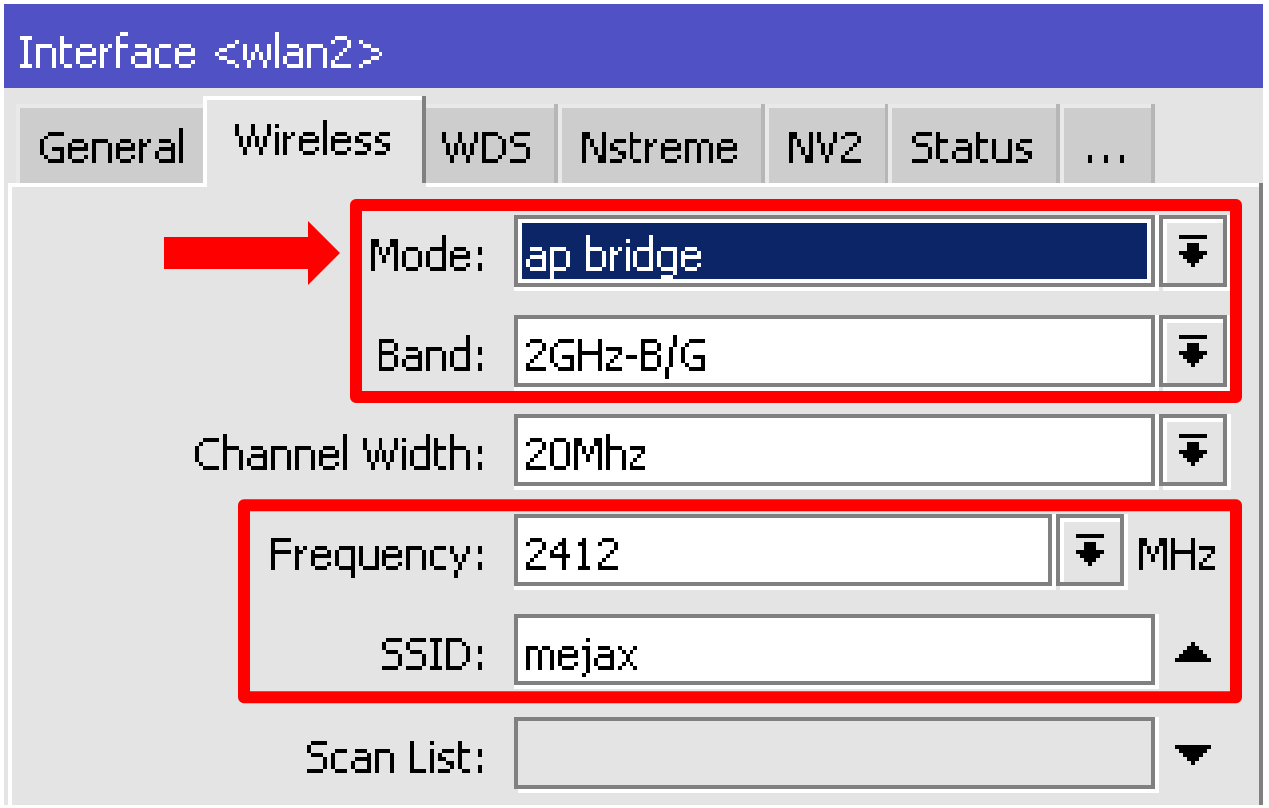
[LAB-4] Point to Multi Point

- Mikrotik difungsikan sebagai access point. Digunakan standart 80211b atau 80211b/g sehingga semua client (berbagai vendor dan berbagai type) dapat terkoneksi.



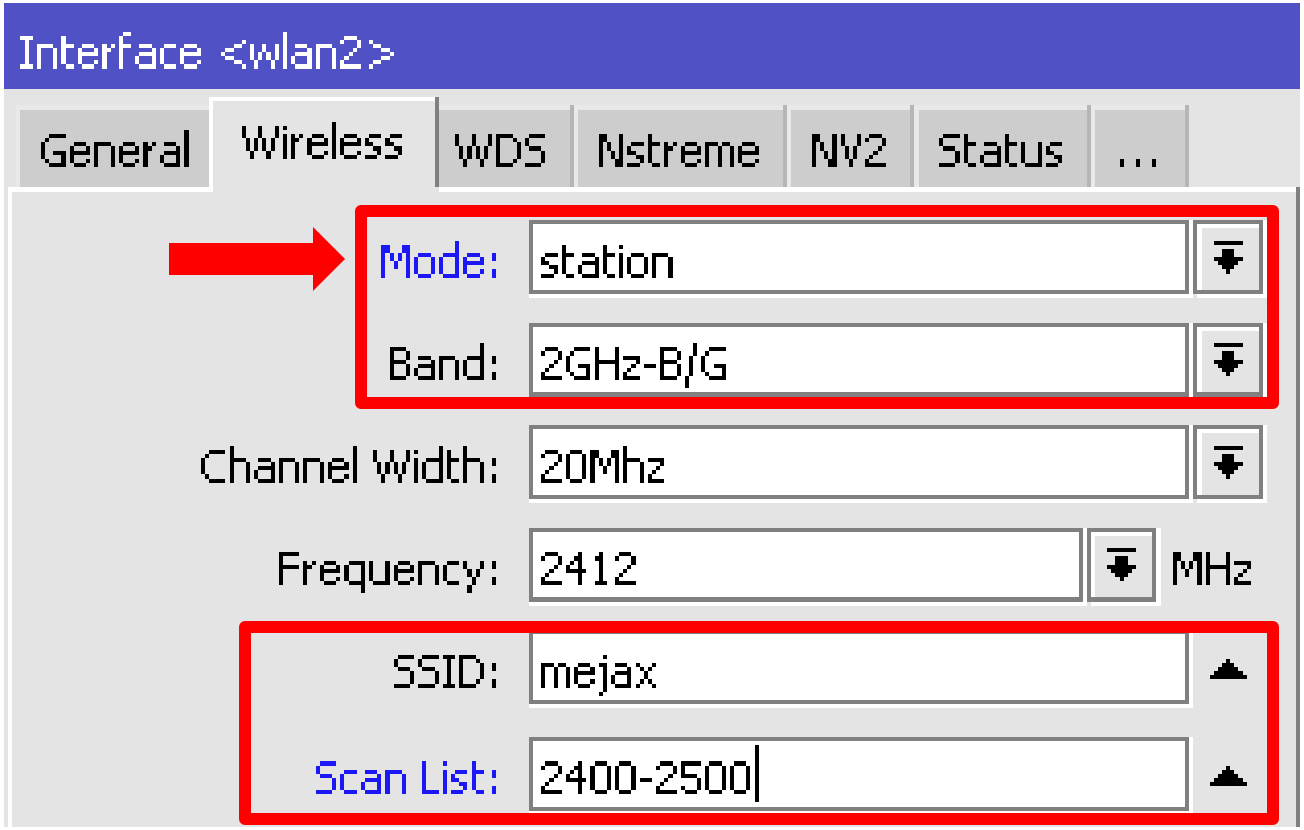
[LAB-4] P2MP – AP Side

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



[LAB-4] P2MP – Station Side

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

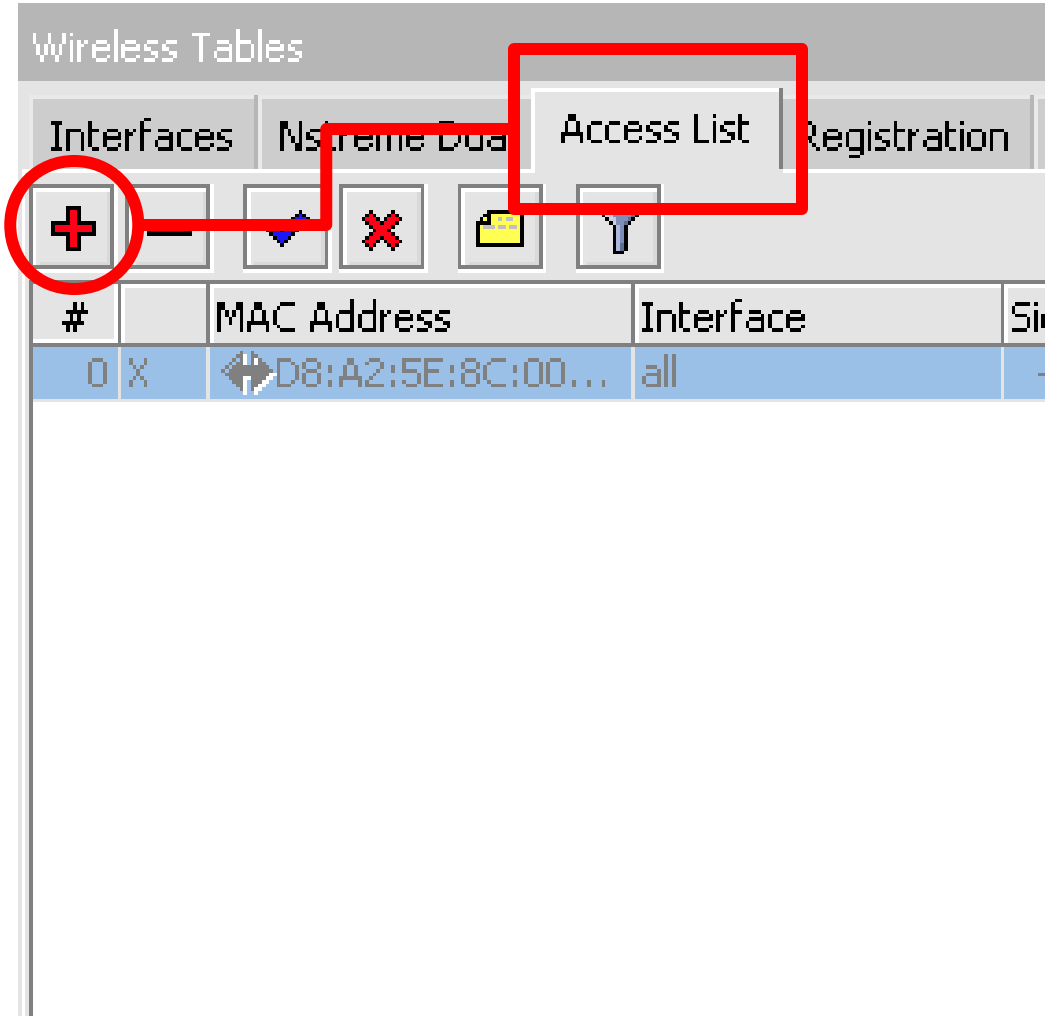


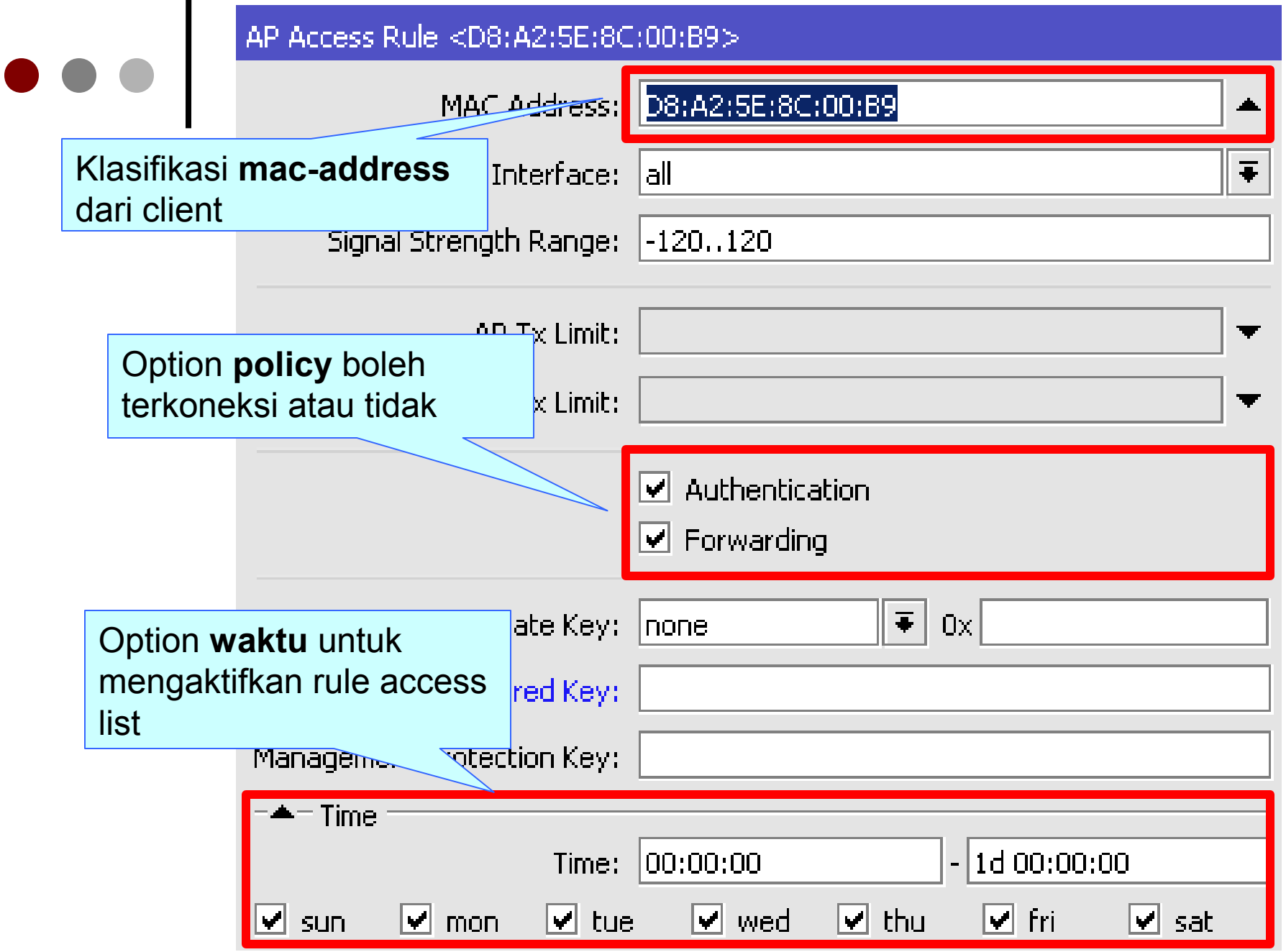
Wireless Access Management

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

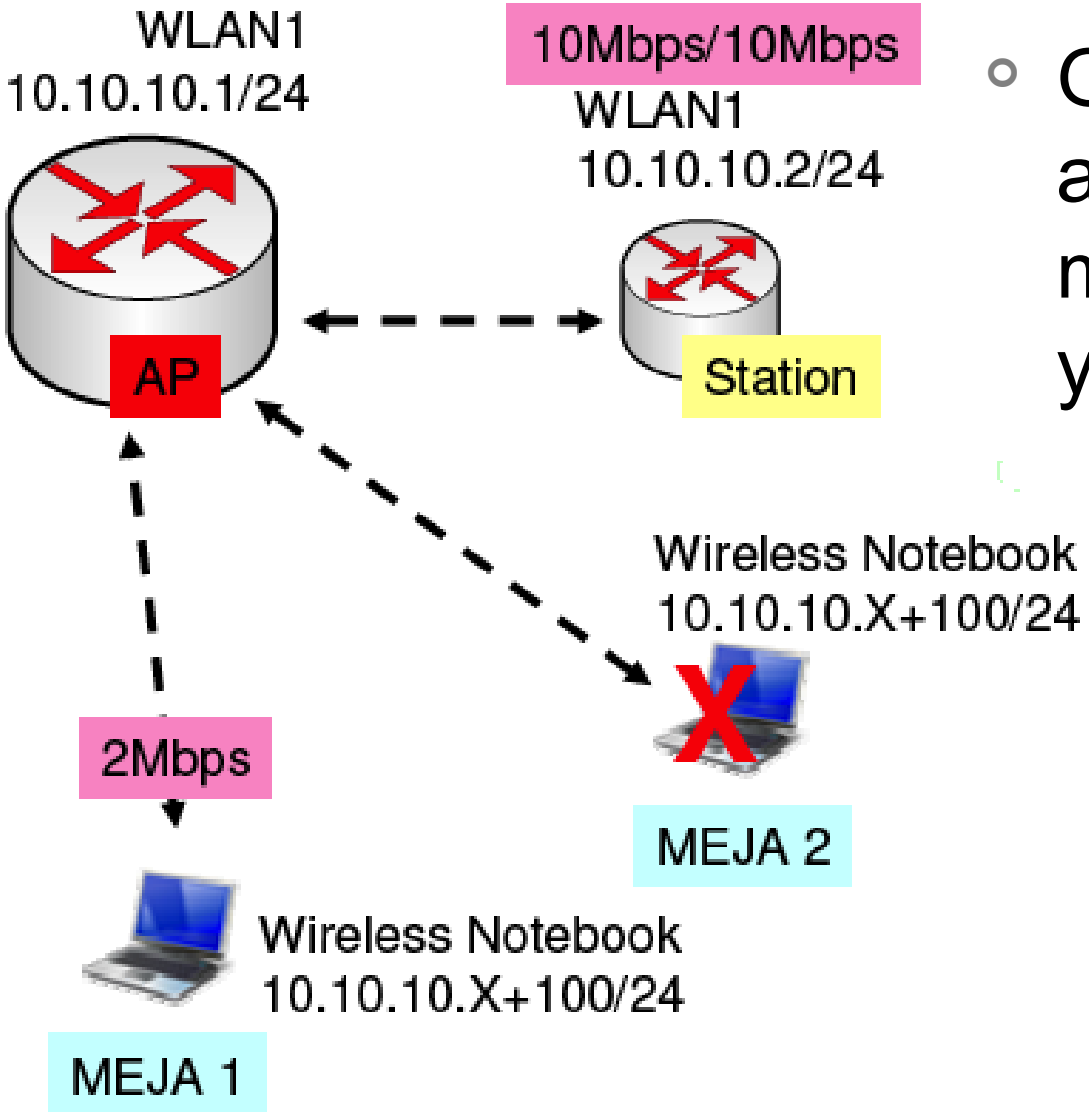
Client Management

- Kita dapat melakukan pengaturan untuk setiap klien menggunakan :
- Access List :
  - MAC Address
  - Signal Strength
  - Time




AP Access Rule <D8:A2:5E:8C:00:B9>
MAC Address:
D8:A2:5E:8C:00:B9
Interface:
all
Signal Strength Range:
-120..120
Authentication
Forwarding
none
0x
Time
Time:
00:00:00
1d 00:00:00
sun
mon
tue
wed
thu
fri
sat
Klasifikasi mac-address dari client
Option policy boleh terkoneksi atau tidak
Option waktu untuk mengaktifkan rule access list

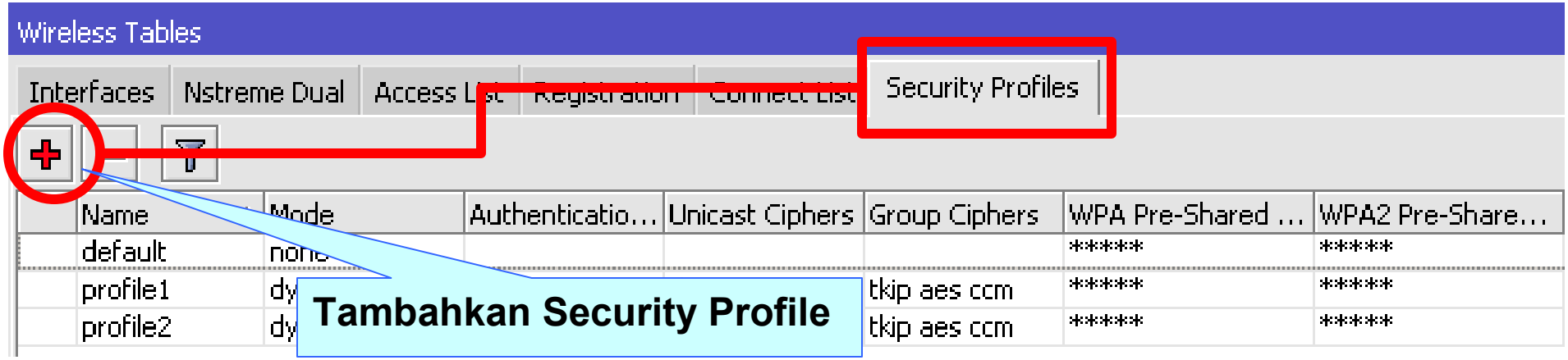
[LAB-5] Access List Mac filter

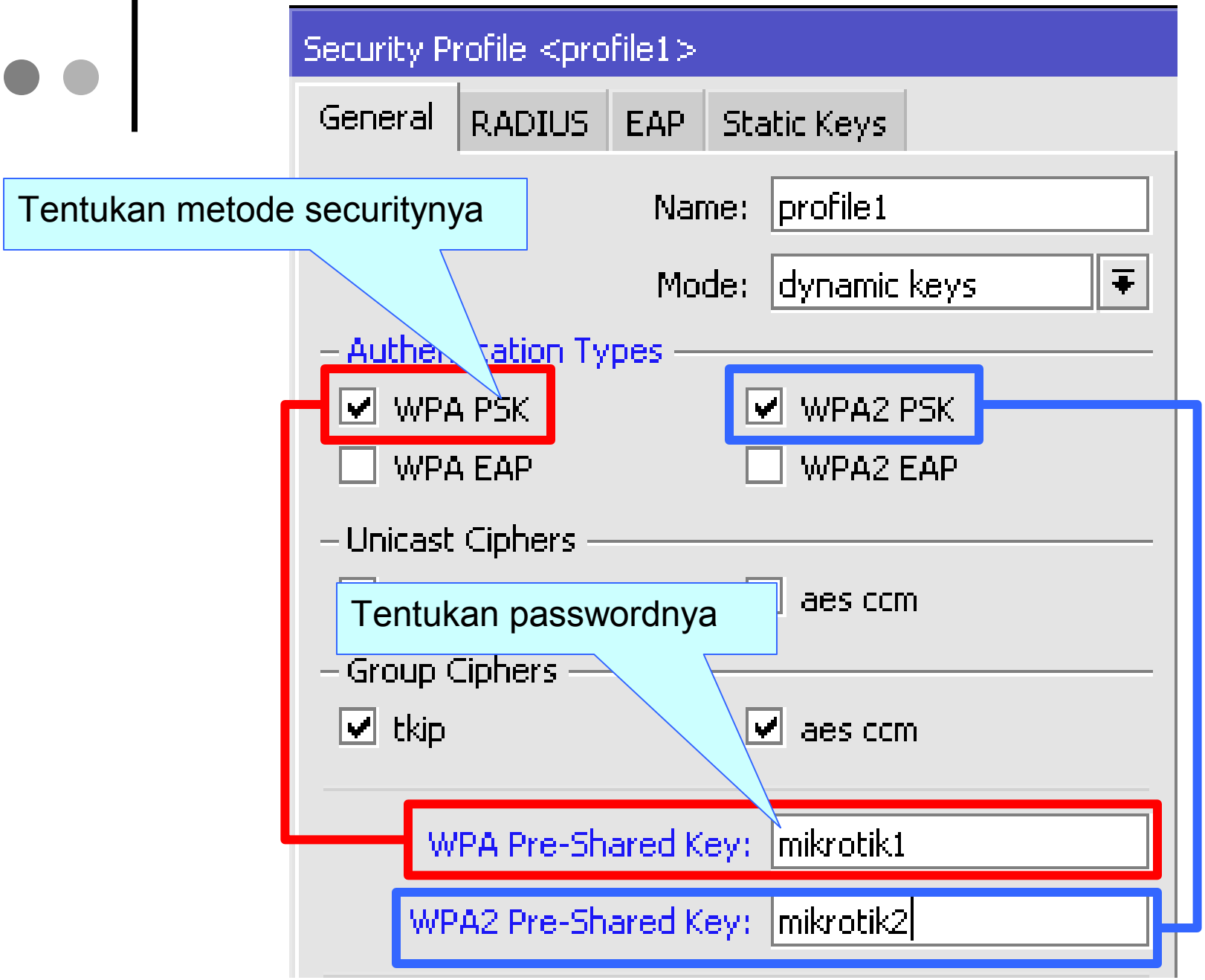


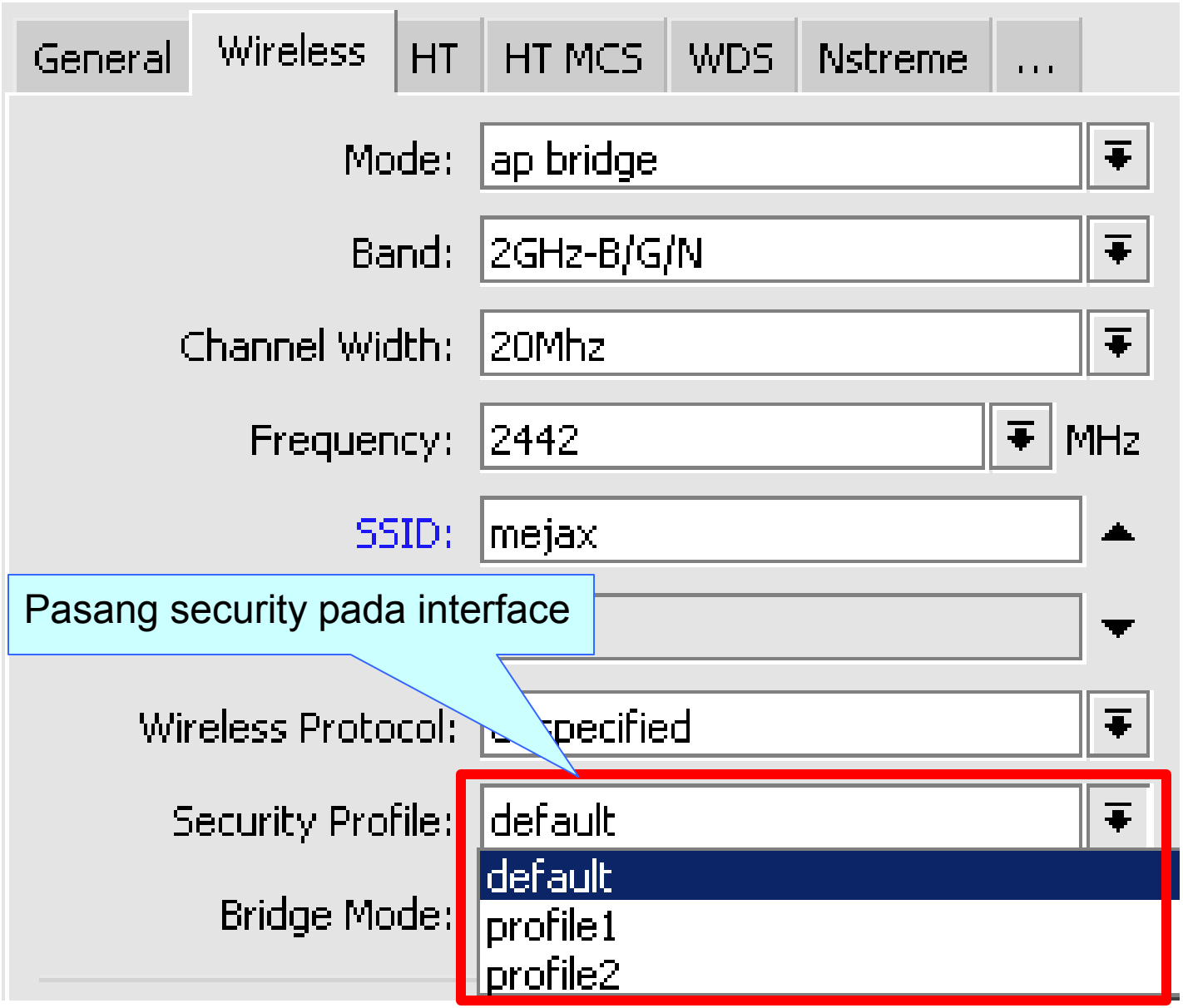
- Gunakan filter Mac-address untuk menetukan client yang terkoneksi.

Wireless Security

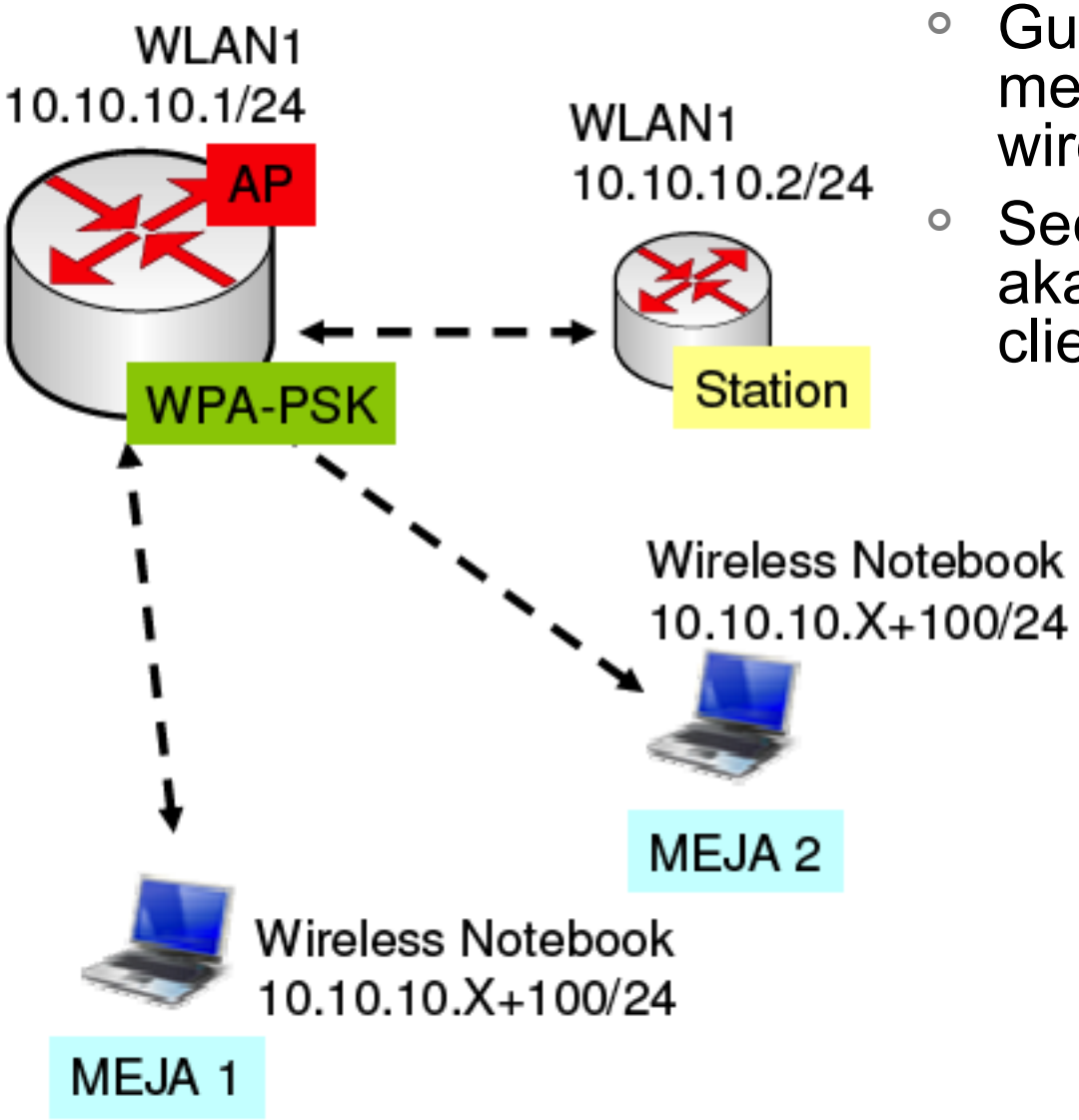
- Karena sifat dari wireless yang “open access” maka sebuah access point akan rentan terhadap serangan dari pihak yang tida bertanggung jawab.
- Sudah saatnya untuk mengimplementasikan Wireless Security untuk menjaga AP tersebut dari berbagai serangan.




Security Profile <profile1>
General
RADIUS
EAP
Static Keys
Tentukan metode securitynya
Name: profile1
Mode: dynamic keys
Authentication Types
WPA PSK
WPA2 PSK
WPA EAP
WPA2 EAP
Unicast Ciphers
aes ccm
Tentukan passwordnya
Group Ciphers
tkip
aes ccm
WPA Pre-Shared Key: mikrotik1
WPA2 Pre-Shared Key: mikrotik2


General
Wireless
HT
HT MCS
WDS
Nstreme
...
Mode:
ap bridge
Band:
2GHz-B/G/N
Channel Width:
20Mhz
Frequency:
2442
MHz
SSID:
mejax
Pasang security pada interface
Wireless Protocol:
Security Profile:
default
Bridge Mode:
default
profile1
profile2

[LAB-6] WPA Lab



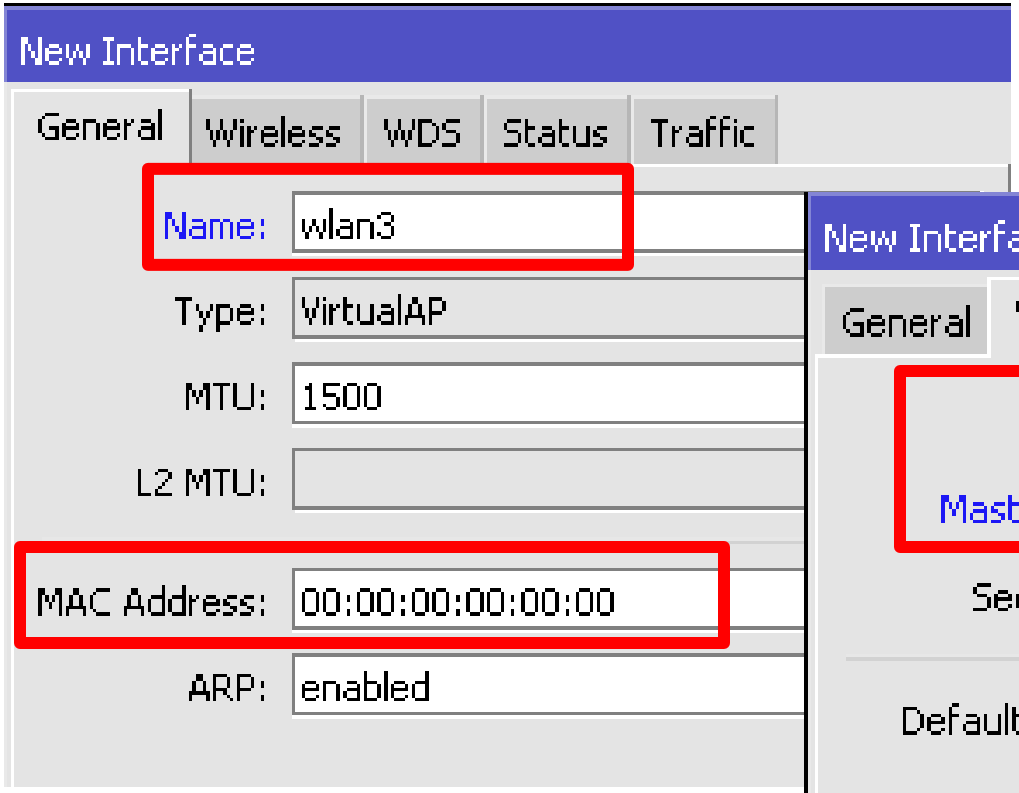
- Gunakan WPA-PSK untuk mengamankan jaringan wireless.
- Security profile pada interface akan mempengaruhi semua client.

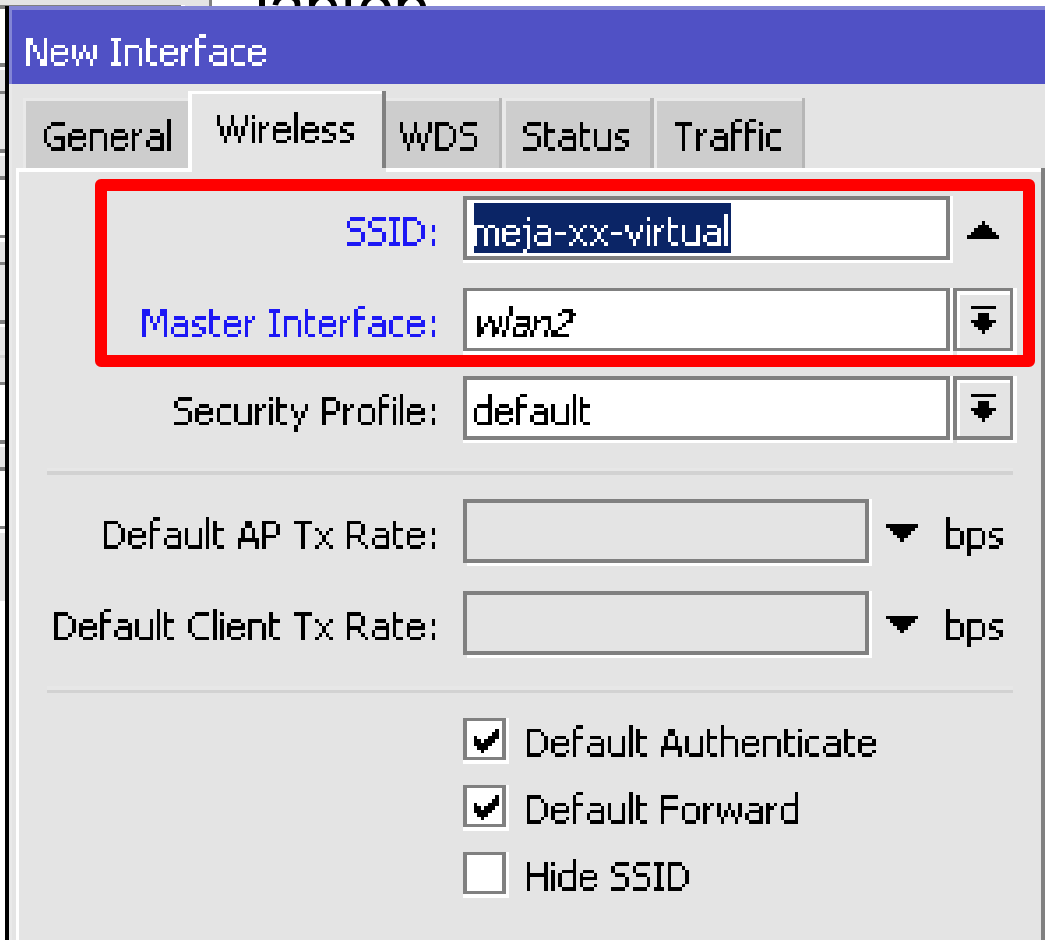
Wireless Protocol - VAP

- Virtual Access Point (VAP) interface digunakan untuk membuat AP tambahan dari satu interface wireless yang ada di mikrotik.
- Virtual AP dianggap sebagai interface wireless yang independen dan bisa memiliki konfigurasi berbeda :
  - **SSID**
  - **Mac-Address**
  - **IP Address**
  - **WDS**
  - **Security Profile**
- Sedangkan untuk konfigurasi wireless **Mode**, **Band**, **Frequency** serta **Nstreme** tetap mengambil dari interface wireless master.
- Bisa diibaratkan seperti VLAN di wireless.

[LAB-7] Virtual AP Lab

Buat Virtual AP, dan cermati hasil scan di laptop





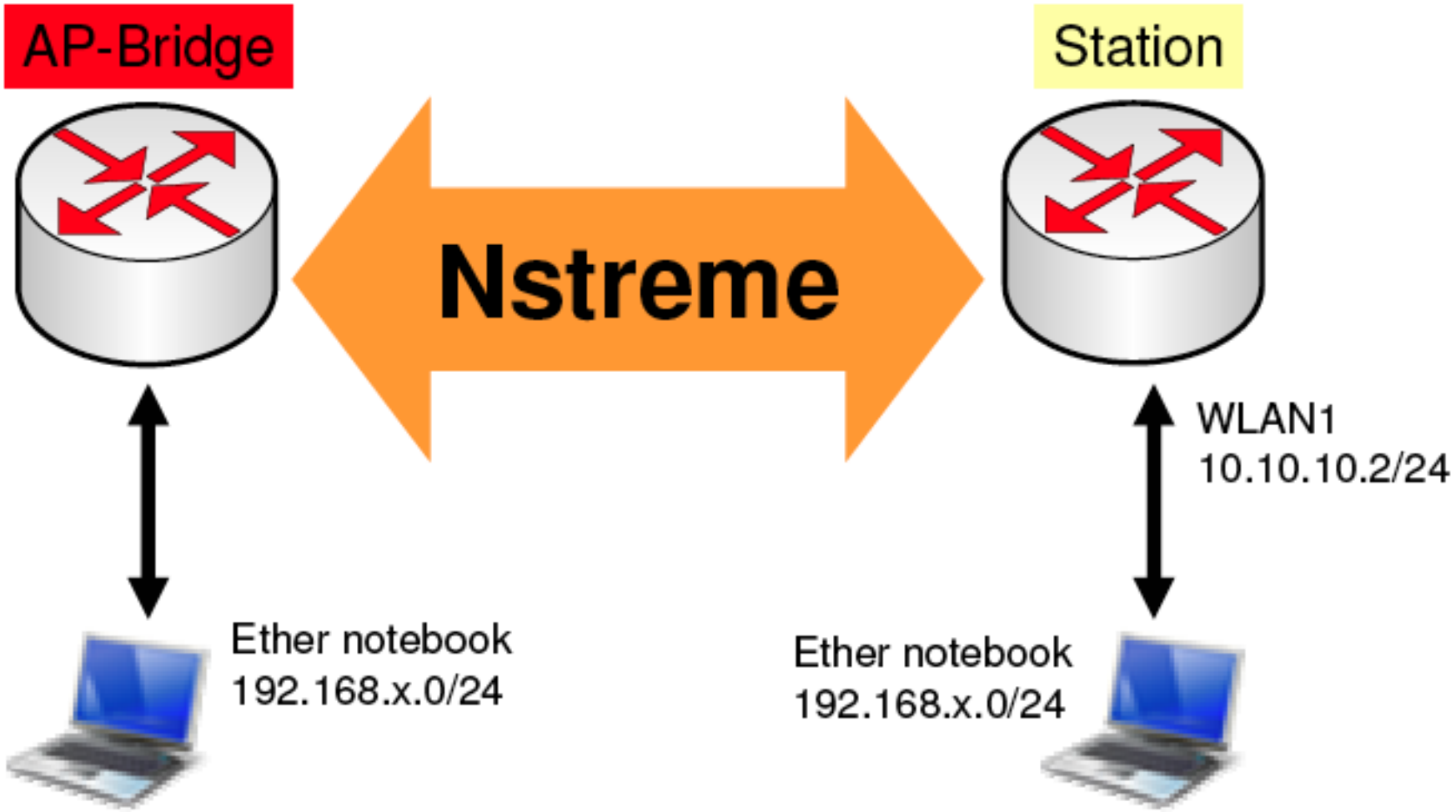
Wireless Protocol - Nstreme

- Nstreme adalah wireless protocol yang **MikroTik's proprietary** (protocol yang tidak kompatibel dengan vendor lain), yang digunakan untuk meningkatkan unjuk kerja jaringan wireless point-to-point maupun point-to-multipoint.
- Hanya bisa dilaktifkan di AP dan Client Mikrotik, tidak disupport oleh perangkat wireless brand lain.

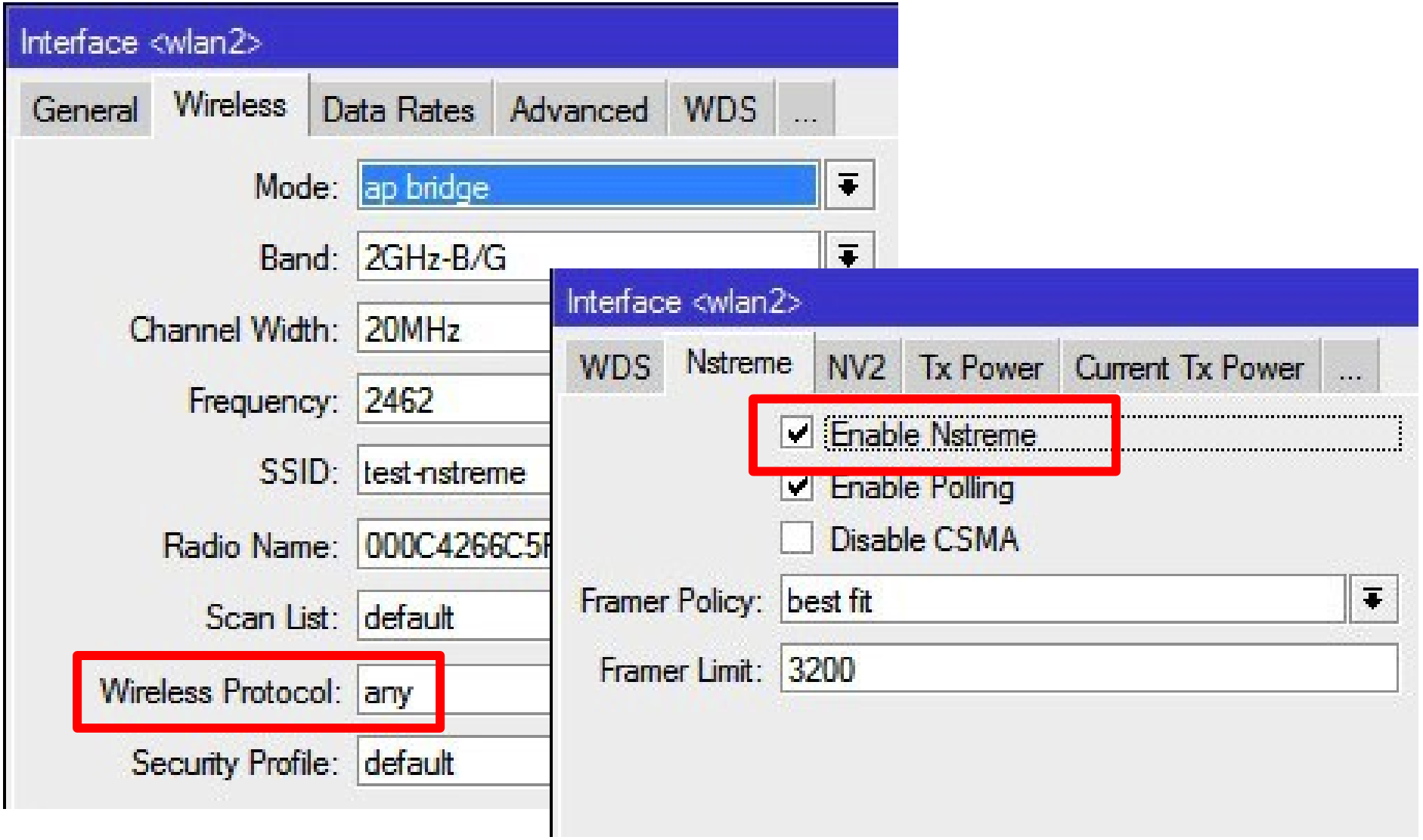
Mikrotik Nstreme

- Keuntungan dari penggunaan Nstreme protocol :
- **Client polling** – melakukan kontrol terhadap jaringan wireless point-to-multipoint dengan mengaktifkan client polling (menyerupai sebuah AP meggunakan kontrol TokenRing).
- **Disable CSMA**.
- Tidak ada limitasi protocol (ACK timeout) di link wireless jarak jauh.
- Beban protocol di tiap frame data akan menjadi lebih ringan sehingga akan mempermudah untuk mendapatkan data-rate yang tinggi.
- Tidak ada lagi protocol yang menyebabkan penurunan kecepatan data-rate untuk link jarak jauh.

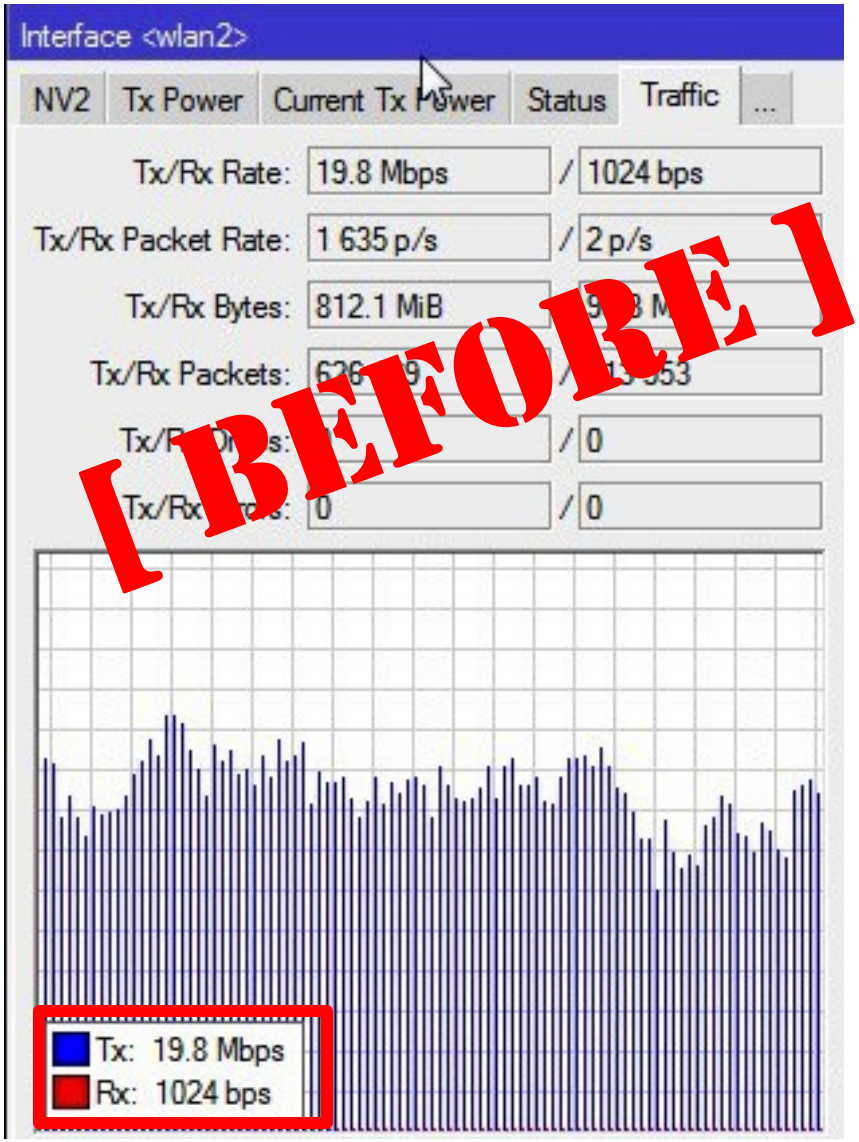
[LAB-9] Nstreme

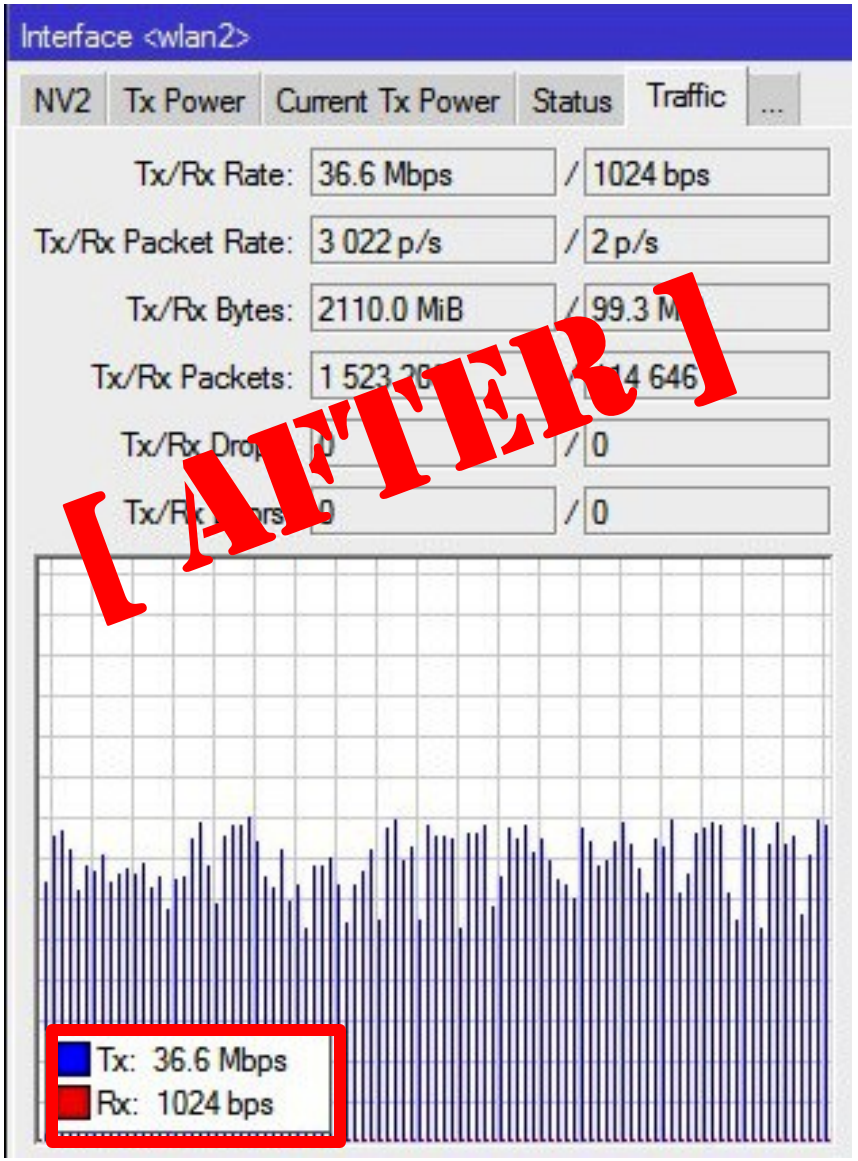


Activate Nstreme on AP & Client



Nstreme - Results



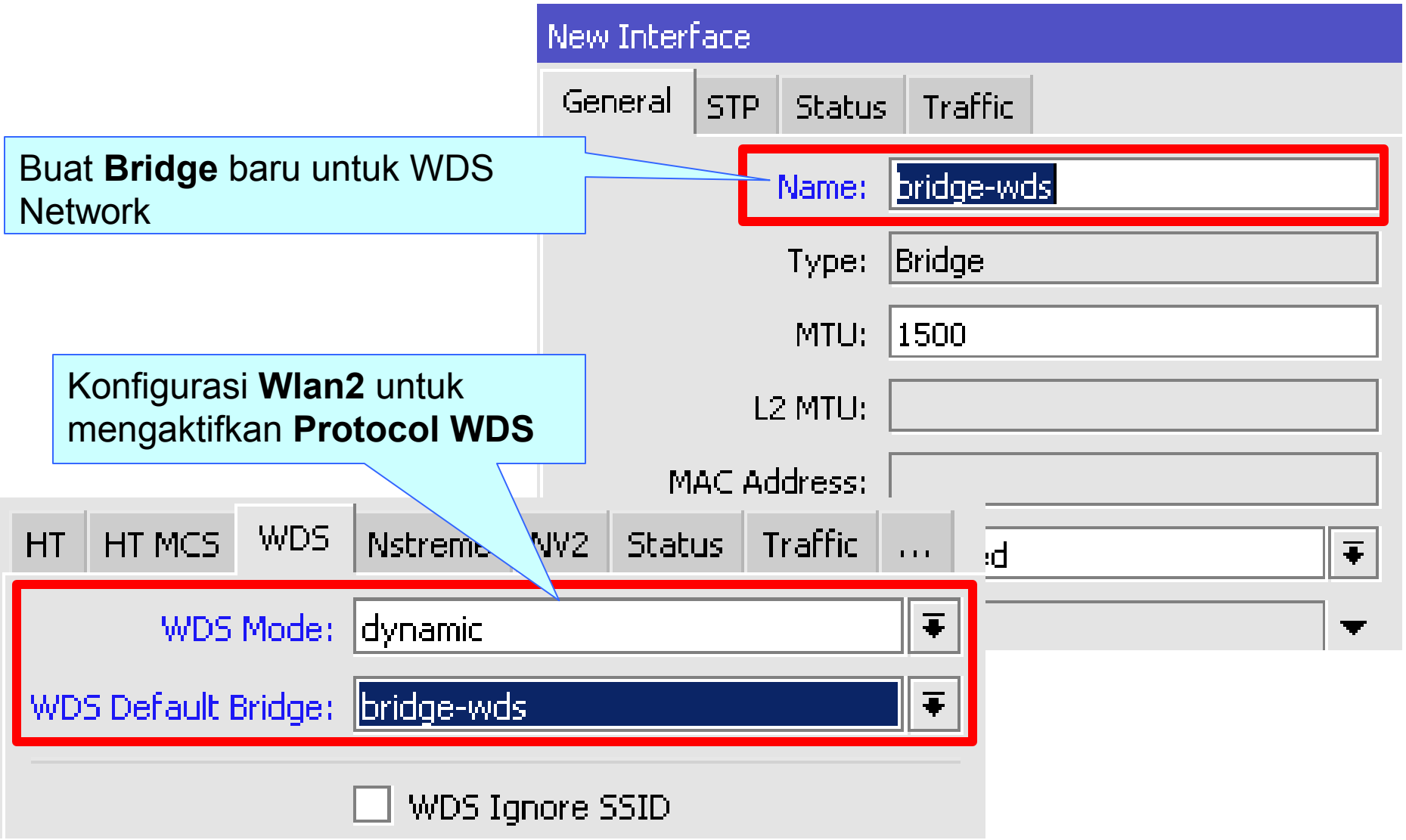


WDS – Wireless Distribution System

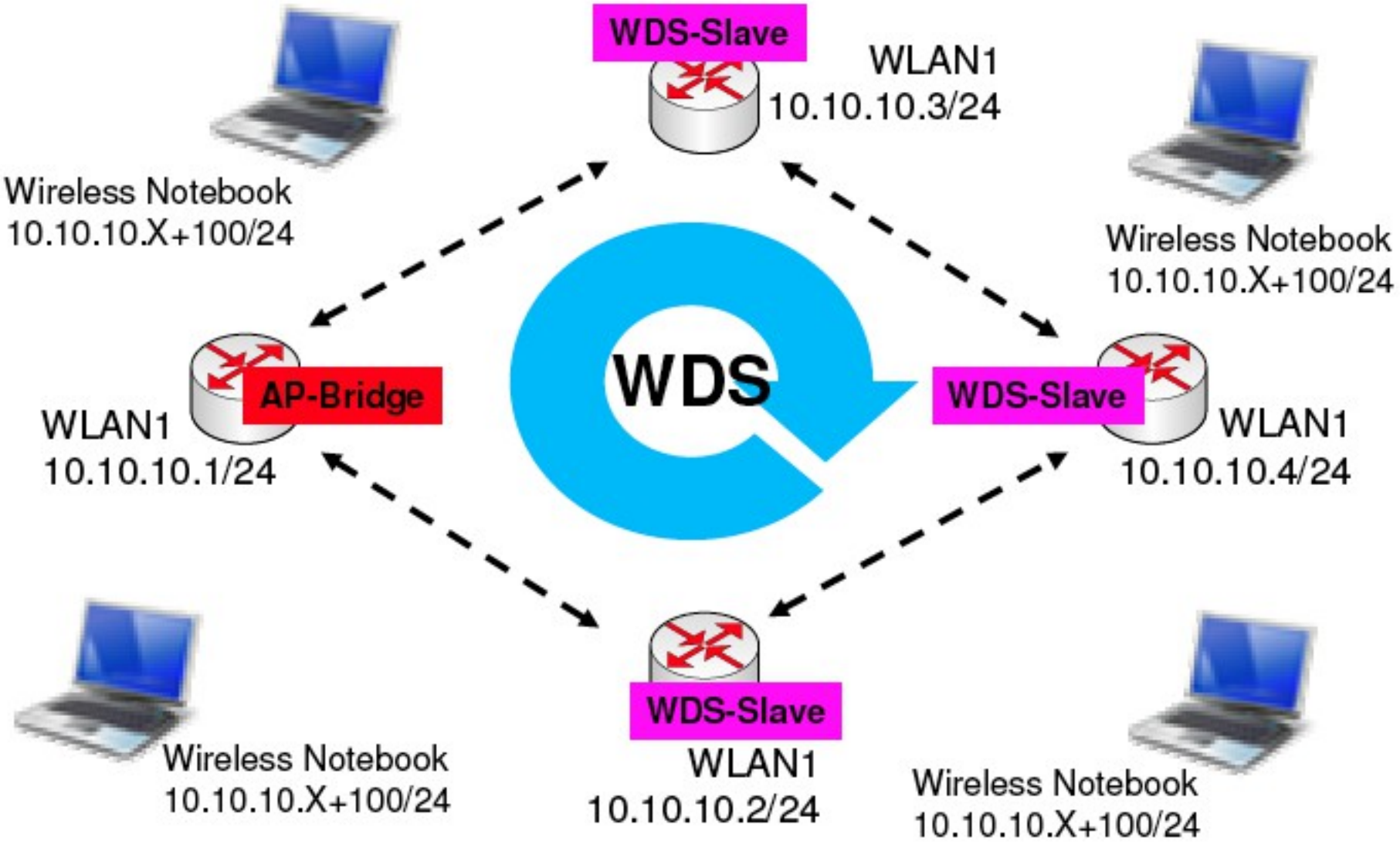
- Dengan menggunakan **WDS** system memungkinkan untuk melakukan konfigurasi wireless yang sedikit berbeda untuk **meningkatkan jangkauan area jaringan wireless**. Dengan **menggunakan beberapa perangkat AP menjadi sebuah satu kesatuan**.
- Dengan menggunakan WDS ini memungkinkan komunikasi data melewati beberapa AP seperti halnya sebuah jaringan ethernet, bisa diibaratkan perangkat AP tersebut sebagai sebuah switch.
- Beberapa AP yang tergabung di dalam Jaringan WDS harus menggunakan **band**, **frequency** dan **SSID** yang sama.

Wireless WDS

WDS - Config


New Interface
General
STP
Status
Traffic
Buat **Bridge** baru untuk WDS Network
Name:
bridge-wds
Type:
Bridge
MTU:
1500
L2 MTU:
MAC Address:
Konfigurasi **Wlan2** untuk mengaktifkan **Protocol WDS**
HT
HT MCS
WDS
Nstreme
NV2
Status
Traffic
...
WDS Mode:
dynamic
WDS Default Bridge:
bridge-wds
WDS Ignore SSID

[LAB-9] WDS – Multi AP



Routing

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

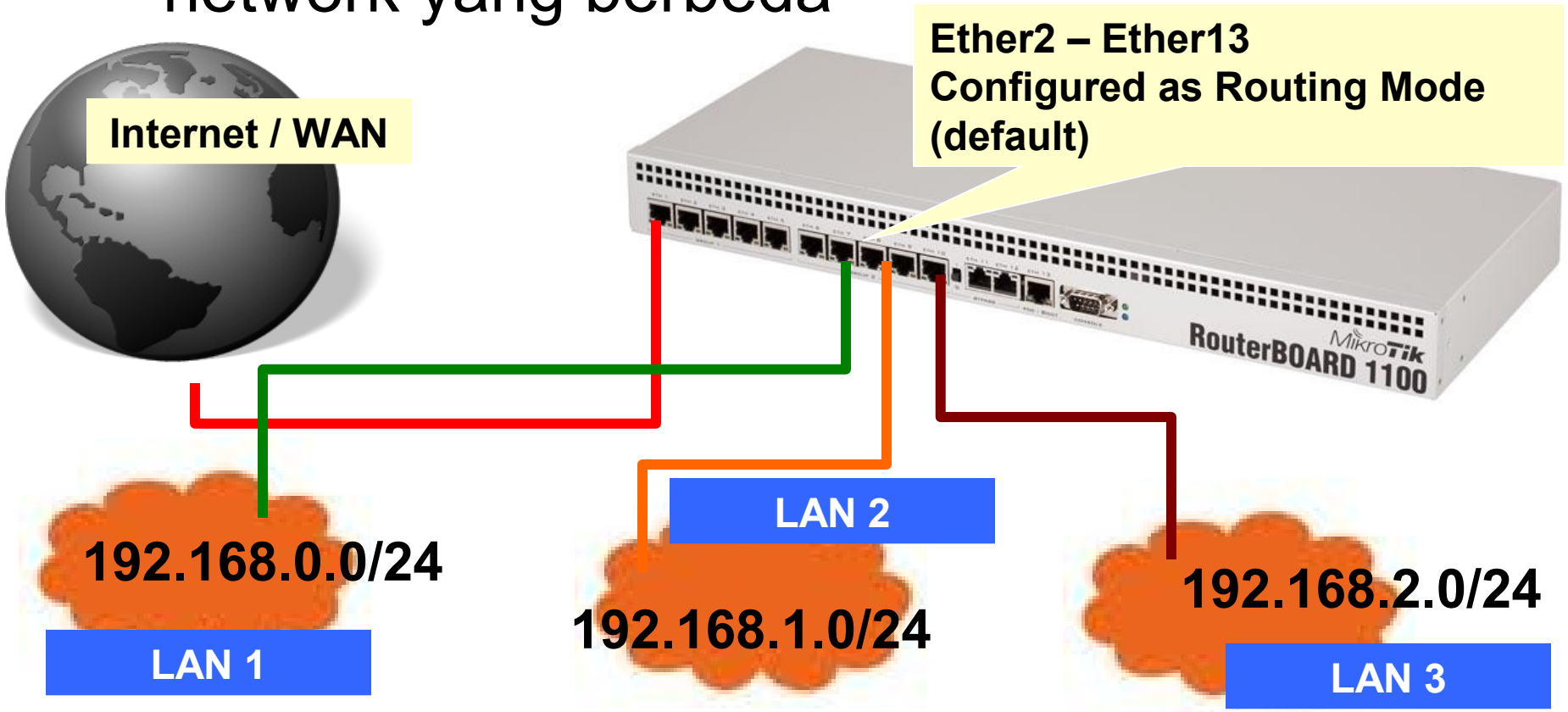
(Mikrotik Certified Training Partner)

Routed Network

- **Routing -** Pengaturan jalur antar Segment Network yang berbeda berdasarkan IP Address tujuan (atau bisa juga asal).
- Bekerja pada OSI layer 3 (Network).
- Untuk menghubungkan network yang berbeda segment (subnet) memerlukan sebuah perangkat yang mampu melakukan proses routing yang disebut dengan Router.

Routing Example

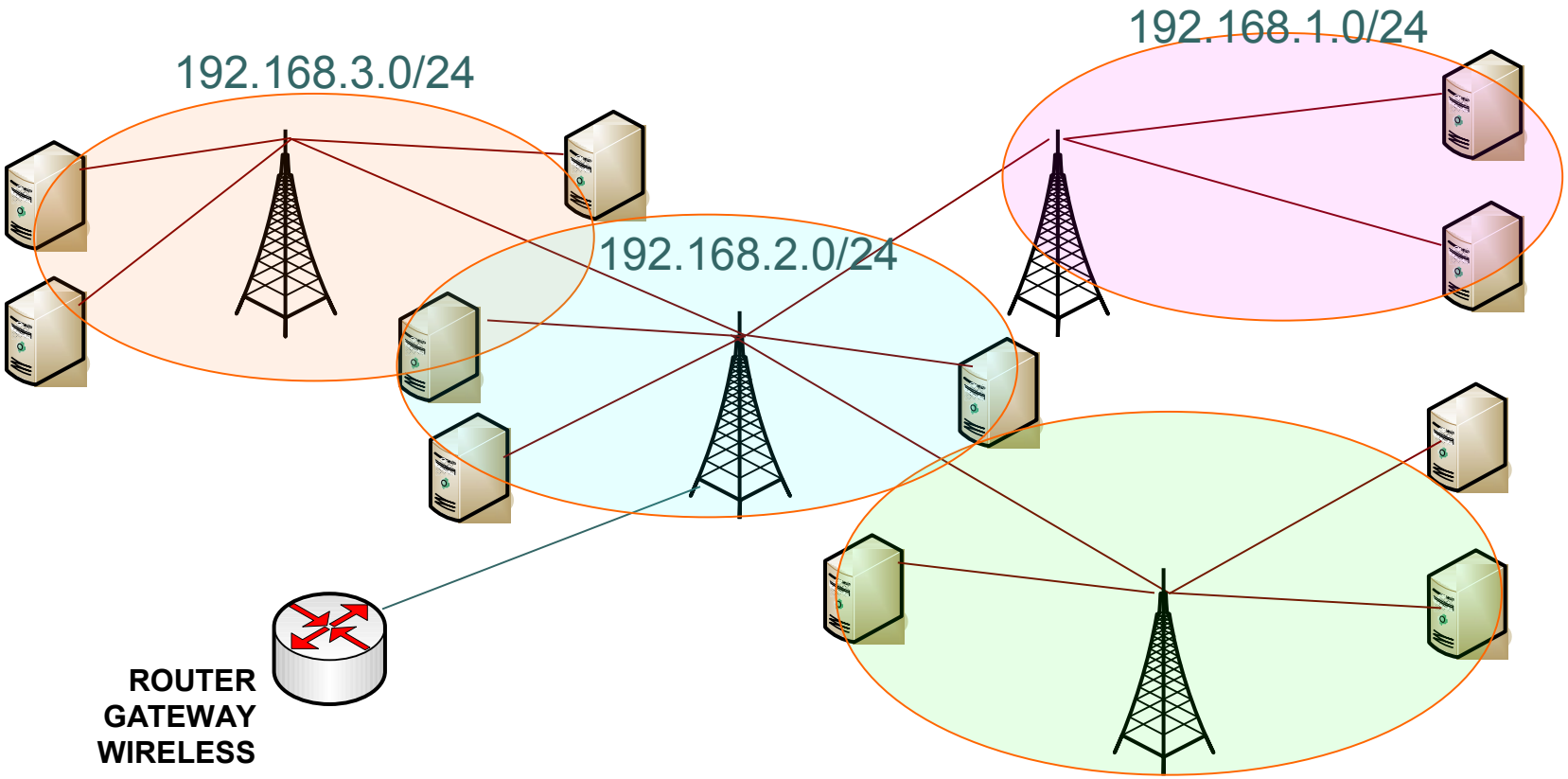
- Routerboard yang berfungsi sebagai router akan menjembatani komunikasi antar network yang berbeda



Routing Benefit

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

More Routing – for Wireless

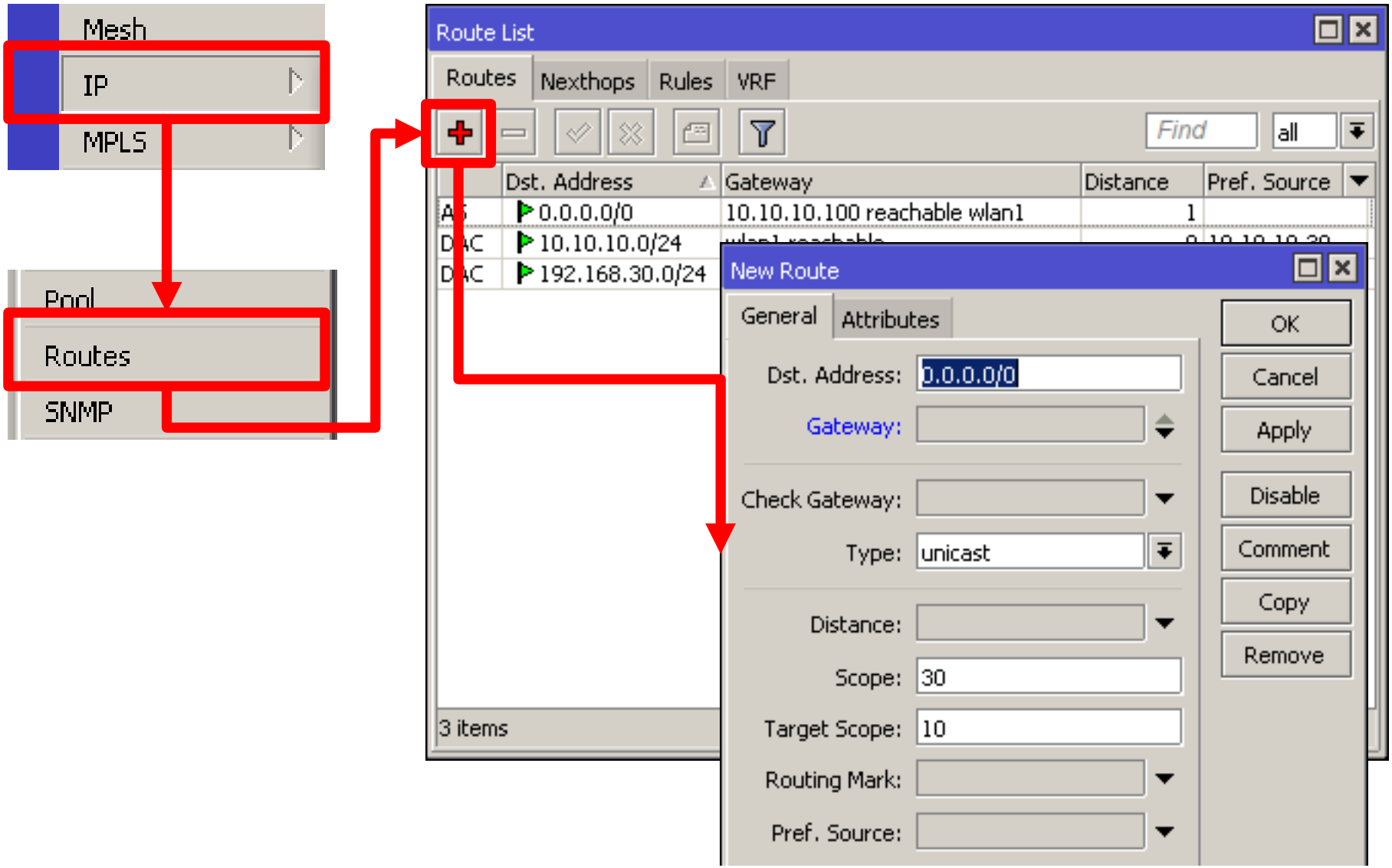


setiap segment jaringan memiliki subnet IP address yang berbeda.

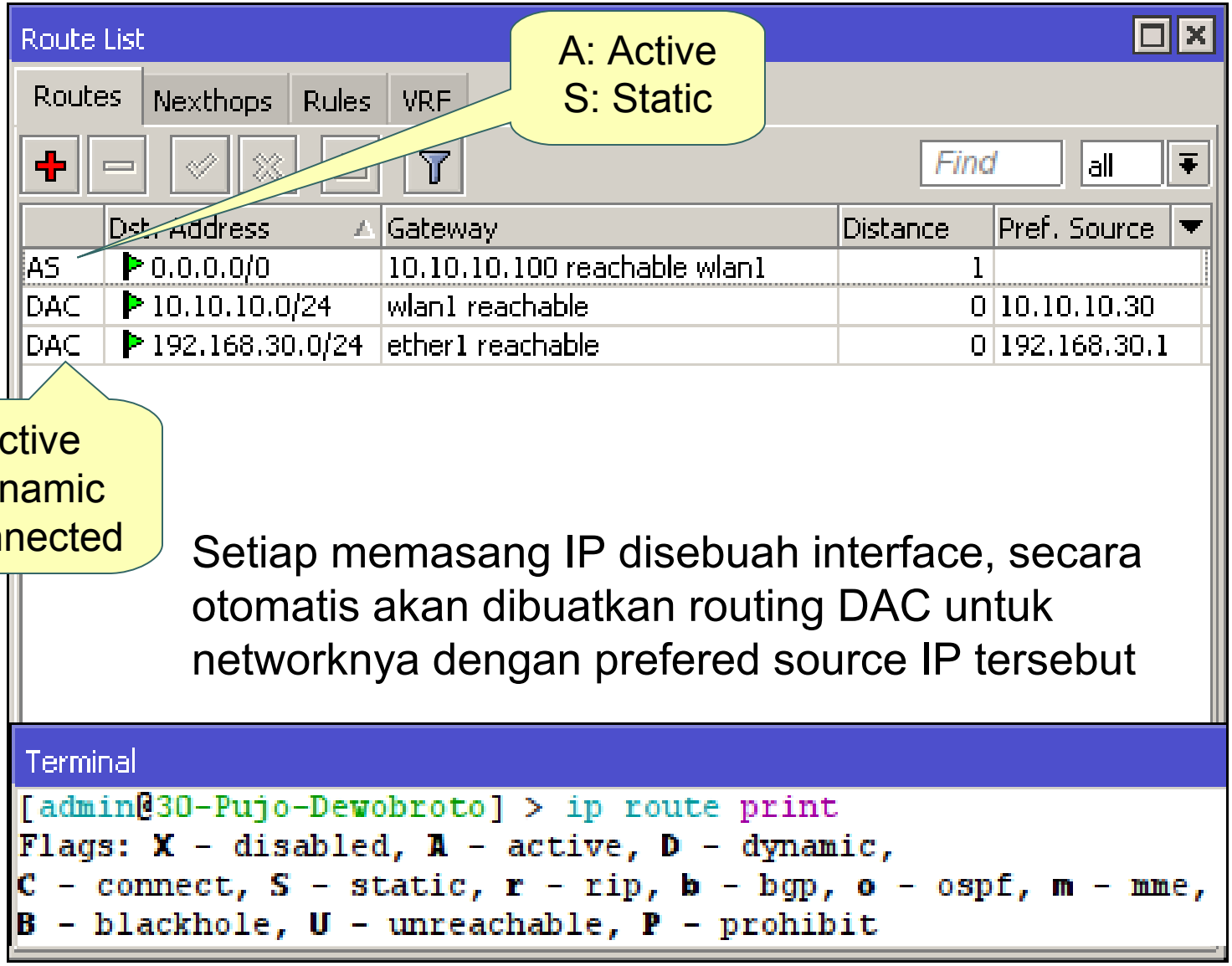
Tipe Informasi Routing

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

Menambahkan Routing



Tipe Routing



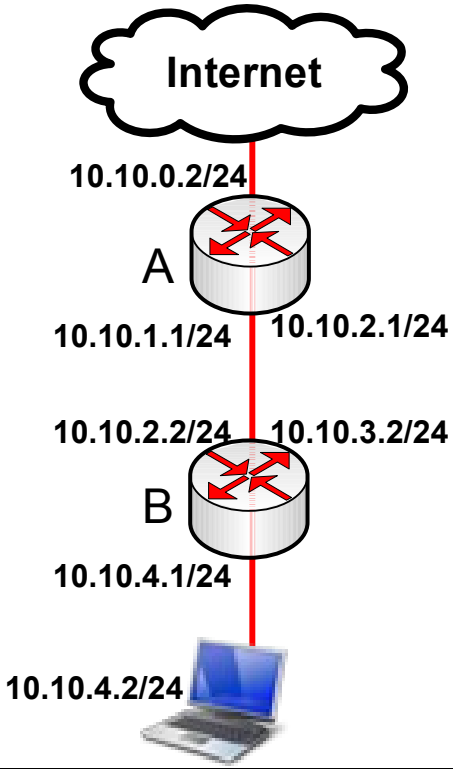
Setiap memasang IP disebuah interface, secara otomatis akan dibuatkan routing DAC untuk networknya dengan prefered source IP tersebut

Parameter Dasar Routing

- **Destination**
  - Destination address – 222.152.211.7
  - Network mask – 202.53.246.0/24
  - 0.0.0.0/0 -> ke semua network
- **Gateway**
  - IP Address gateway, harus merupakan IP Address yang satu subnet dengan IP yang terpasang pada salah satu interface
- **Gateway Interface**
  - Digunakan apabila IP gateway tidak diketahui dan bersifat dinamik (biasanya digunakan di **ppp** interface).
- **Pref Source**
  - source IP address dari paket yang akan meninggalkan router
- **Distance**
  - Beban untuk kalkulasi pemilihan routing

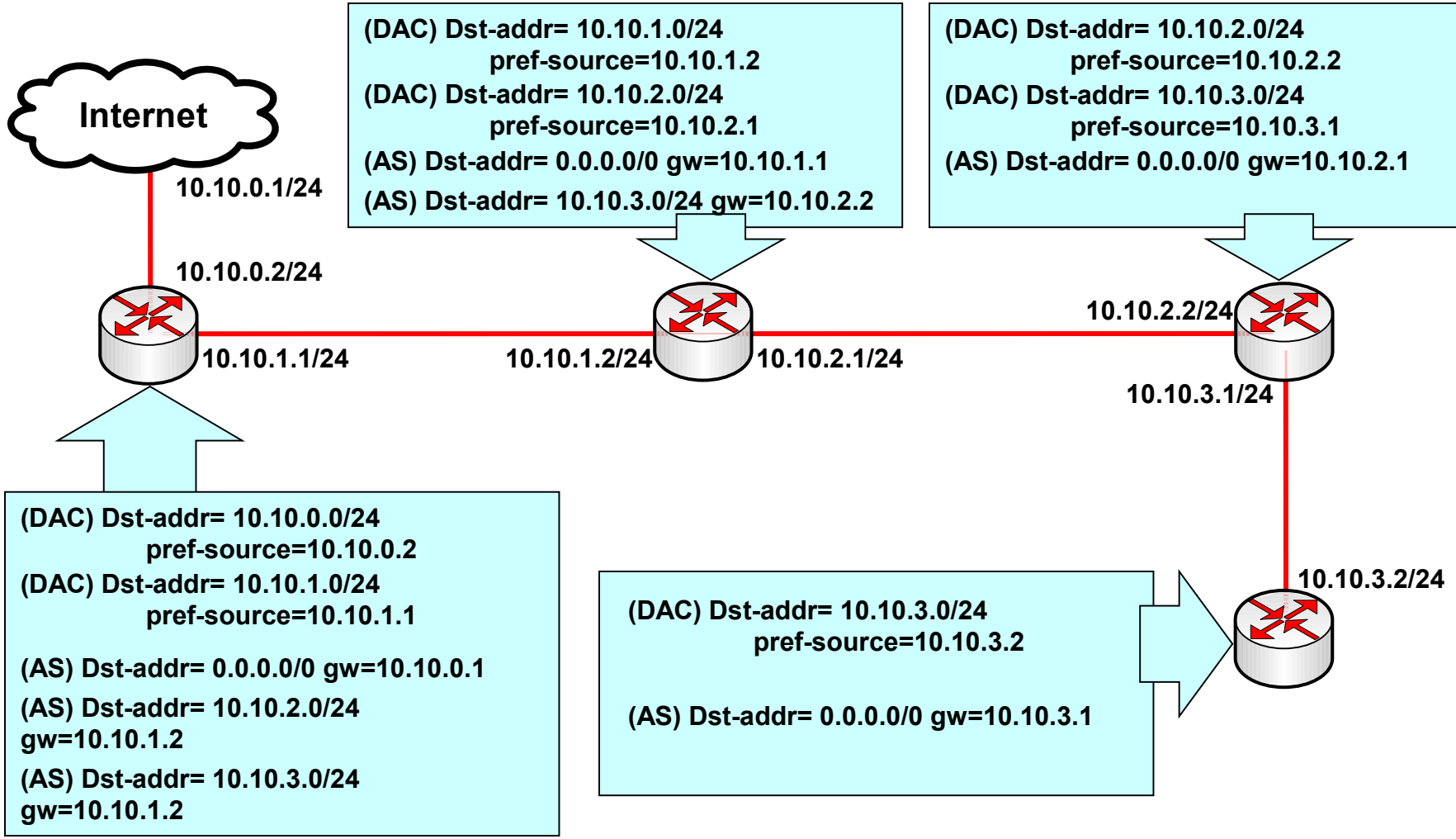
Konsep Dasar Routing

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



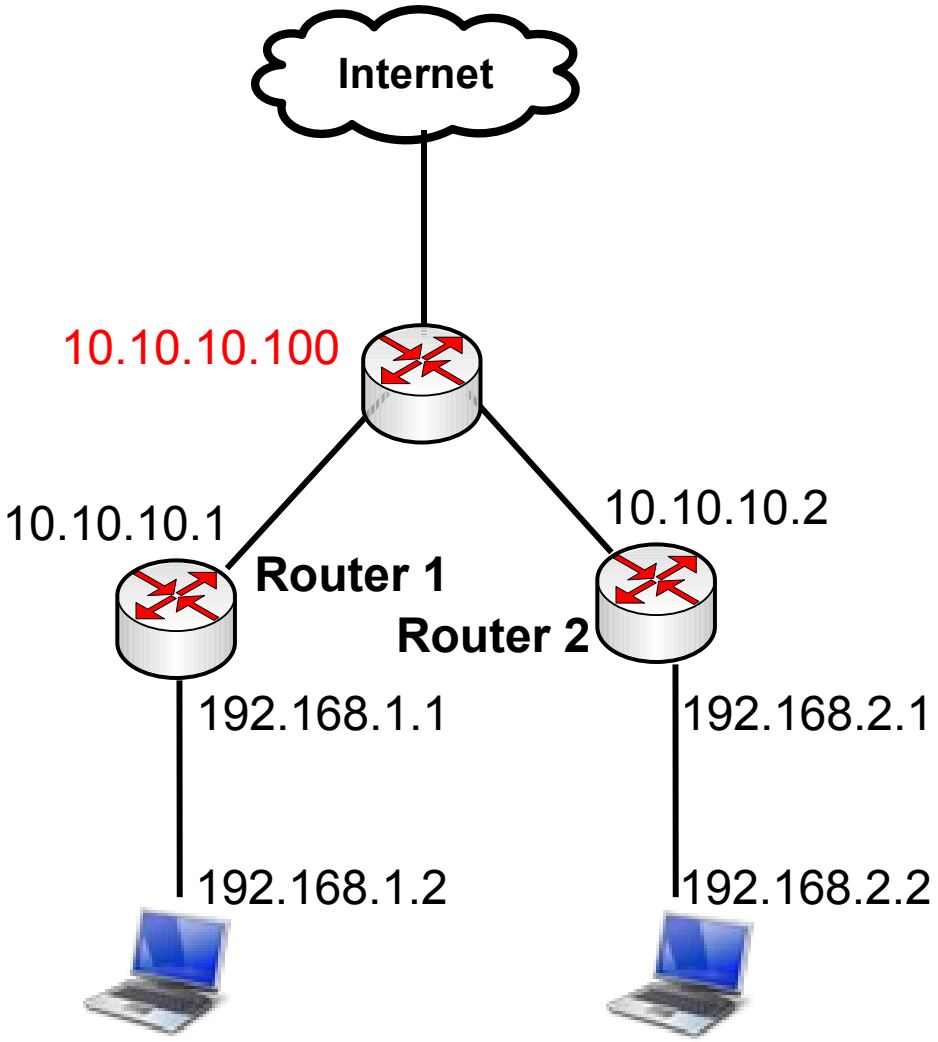
- Pada interface yang menghubungkan router A dan B, pada masing-masing router terdapat lebih dari 1 buah IP Address.
- Default gateway pada router B adalah router A
- IP Address yang menjadi default gateway router B adalah 10.10.2.1, karena IP Address tersebut berada dalam subnet yang sama dengan salah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

Implementasi Konsep Routing



[LAB-1] Static Route

- Dari konfigurasi lab hari 1, semua router hanya memiliki default gateway.
- Tambahkan rule static route supaya ping bisa dilakukan antar notebook yang berbeda network.



Langkah-langkah

- Matikanlah ! src-nat masquerade
- Buatlah static route pada kedua router
- Contoh di meja 1 untuk membuat static route ke meja 2:
  - /ip route add dst-address=192.168.2.0/24 gateway=10.10.10.2
- Contoh di meja 2 untuk membuat static route ke meja 1:
  - /ip route add dst-address=192.168.1.0/24 gateway=10.10.10.1

Dasar Pemilihan Routing

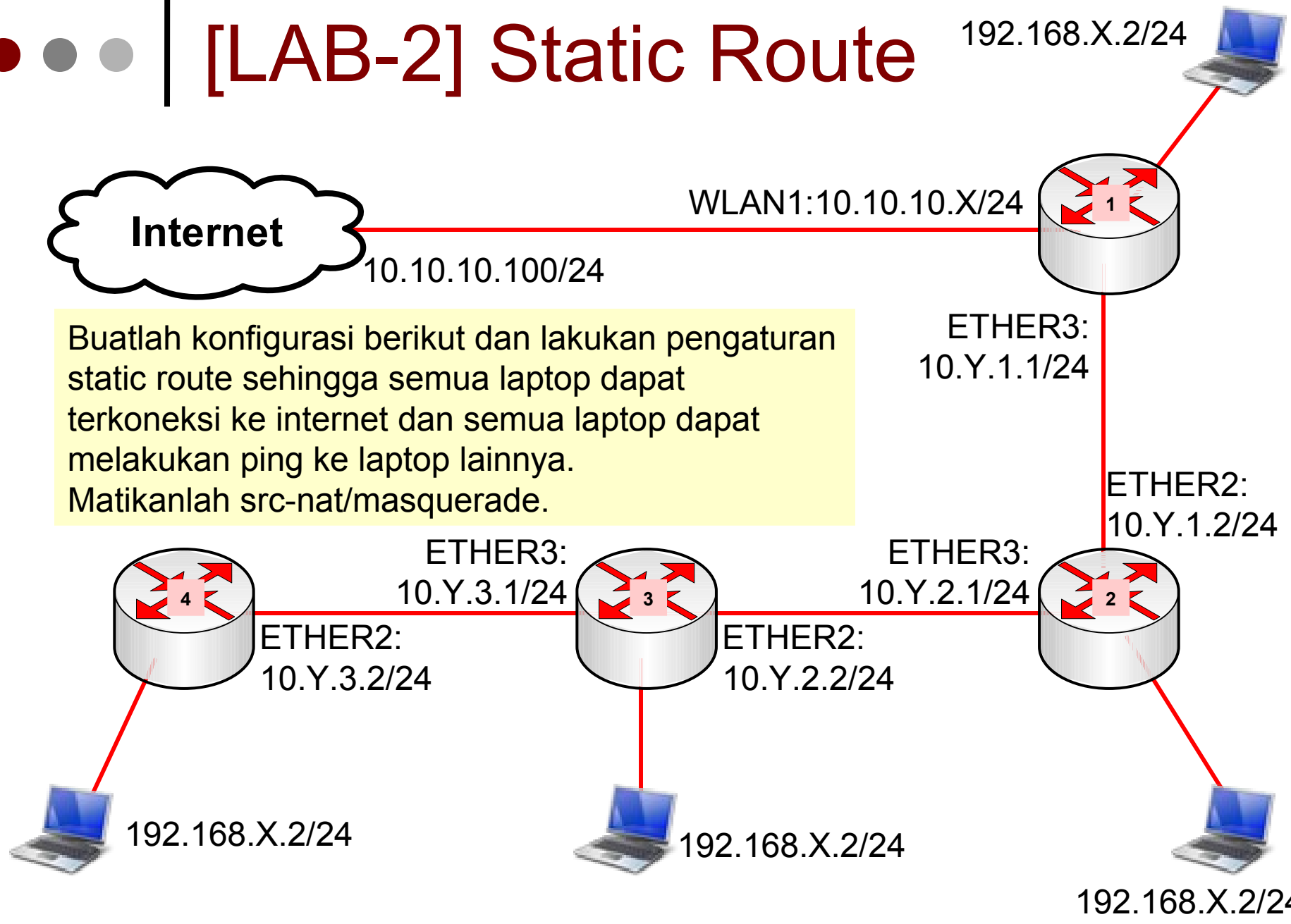
- Untuk pemilihan routing, router akan memilih berdasarkan:
  - Rule routing yang paling spesifik tujuannya
    - Contoh: destination 192.168.0.128/26 lebih spesific dari 192.168.0.0/24
  - Distance
    - Router akan memilih yang distance nya paling kecil
  - Round robin (random)

Contoh Pemilihan

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

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

[LAB-2] Static Route

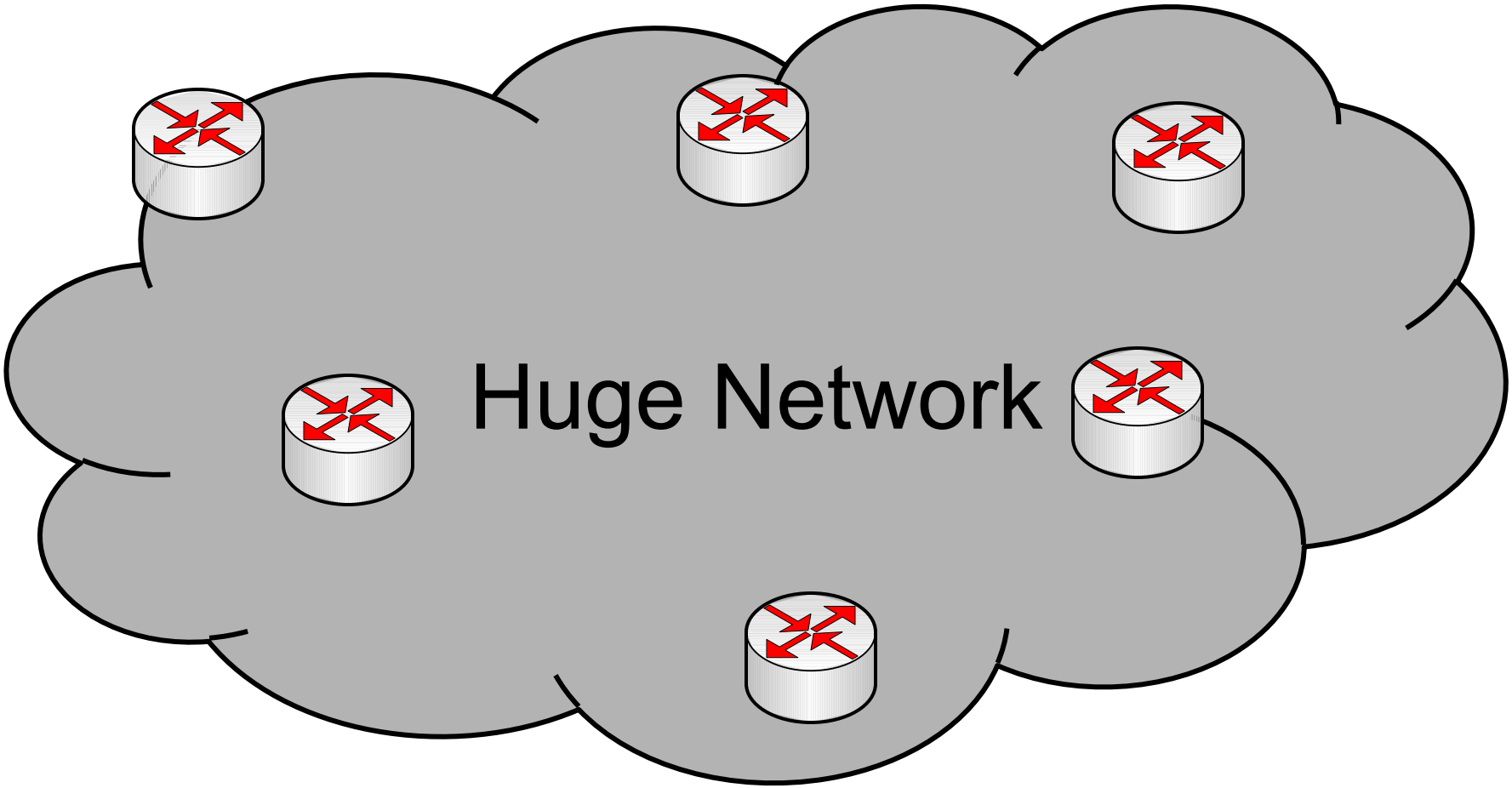


Buatlah konfigurasi berikut dan lakukan pengaturan static route sehingga semua laptop dapat terkoneksi ke internet dan semua laptop dapat melakukan ping ke laptop lainnya.
Matikanlah src-nat/masquerade.

Dynamic Routing

- Karena sebuah jaringan memiliki besar skala yang berbeda satu sama lain, maka sangat memungkinkan jika jaringan tersebut berkembang menjadi besar sekali. Maka penggunaan routing menjadi sangat penting dan kritis.
- **Informasi routing haruslah tepat** dan kesalahan melakukan distribusi informasi routing harus diminimalisasi sedikit mungkin.
- Sangatlah tidak nyaman jika harus menuliskan rule routing untuk puluhan bahkan ratusan router secara static.

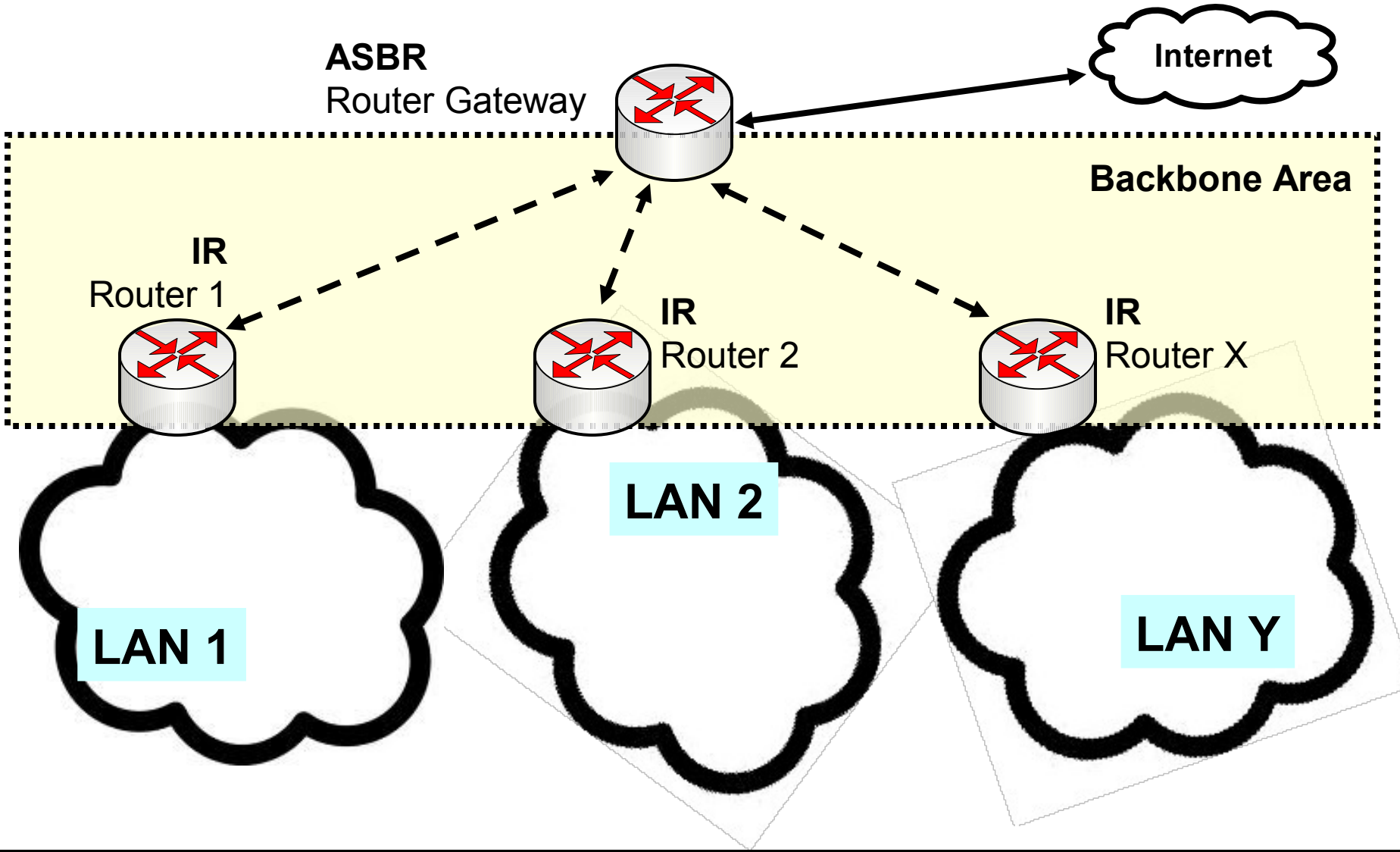
Very Big Network



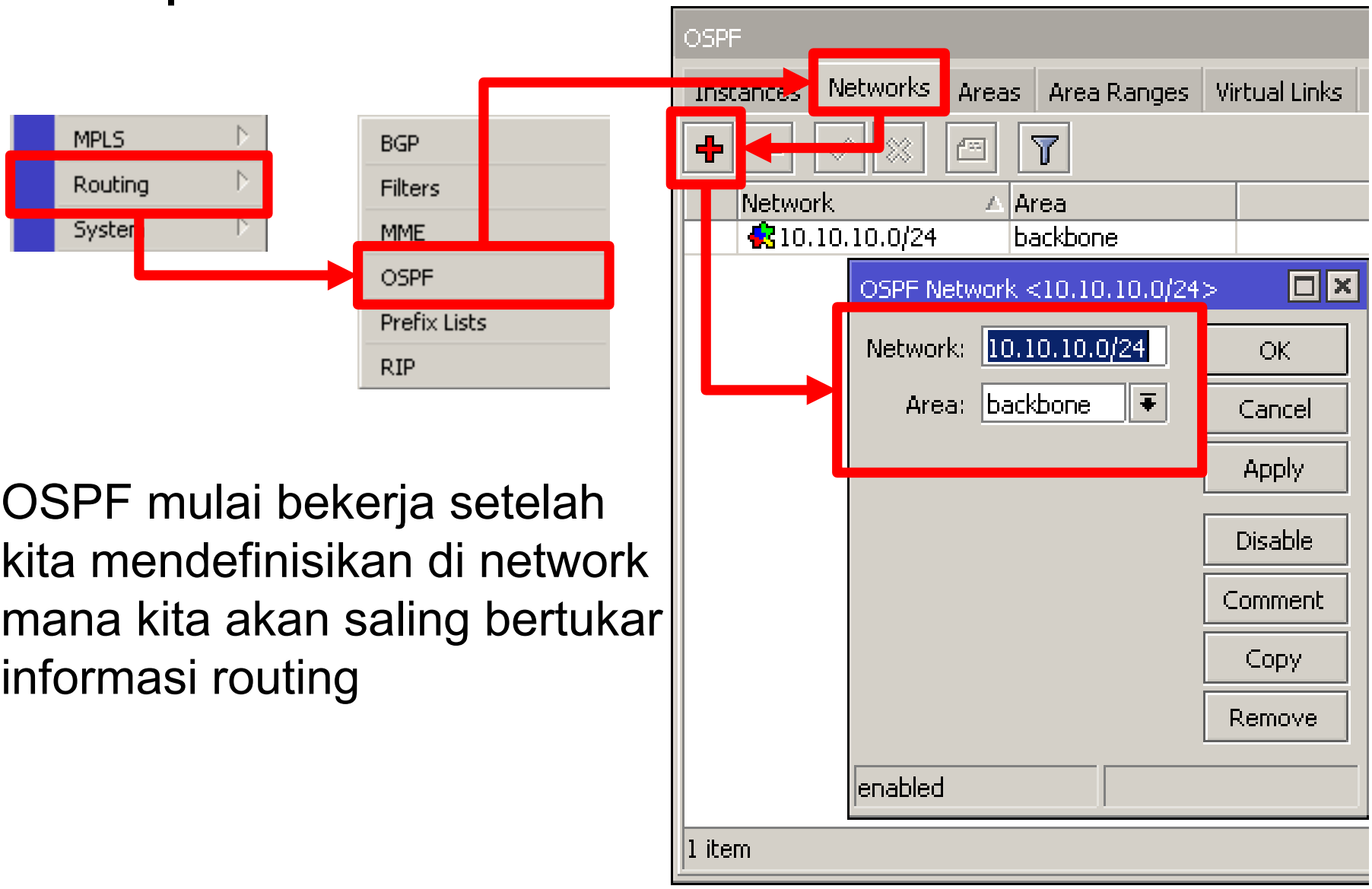
Dynamic Routing - OSPF

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

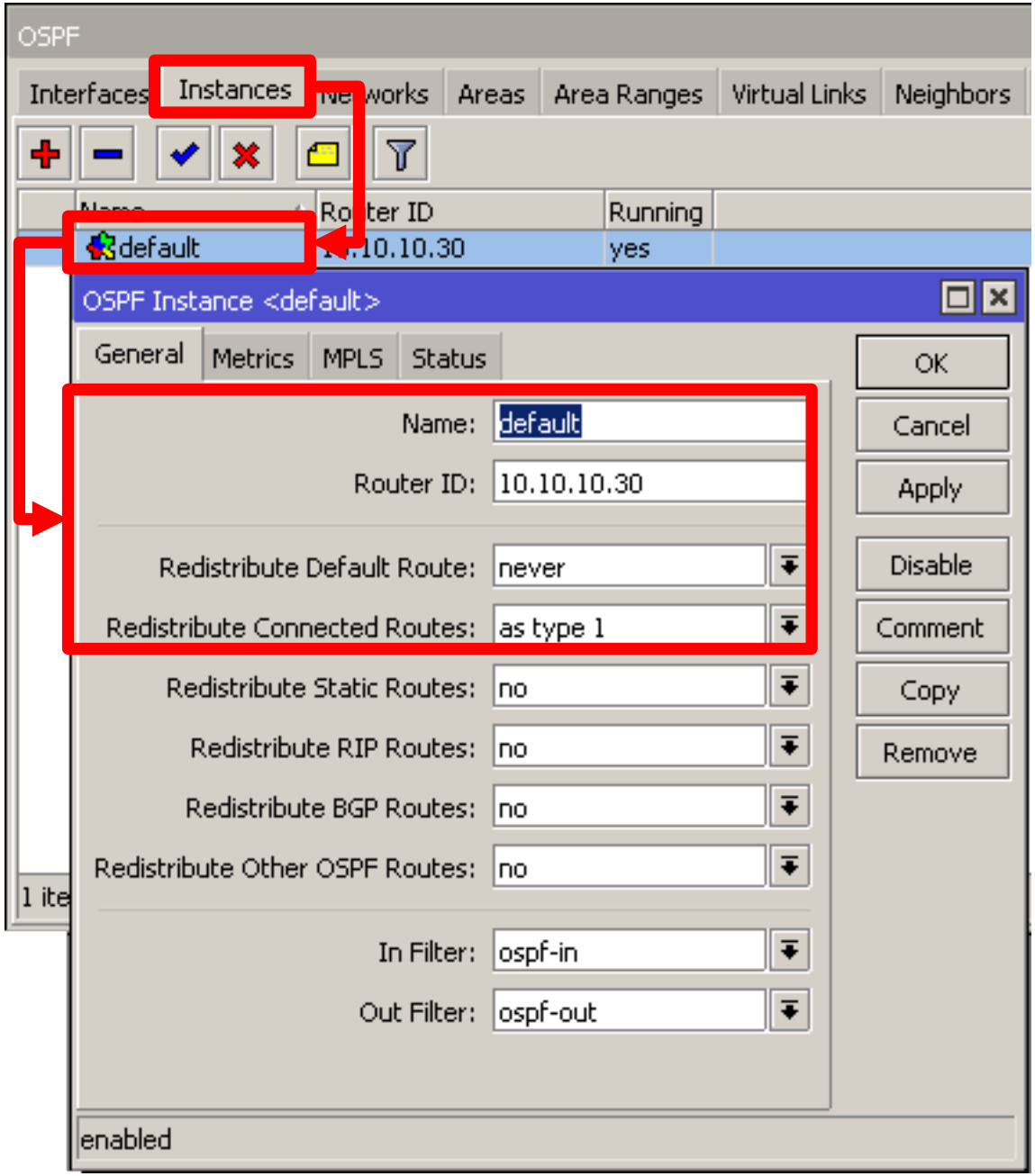
[LAB-3] Konfigurasi OSPF



OSPF - Configuration

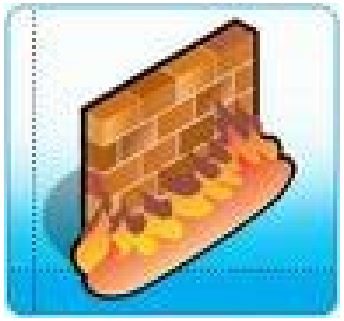


OSPF mulai bekerja setelah kita mendefinisikan di network mana kita akan saling bertukar informasi routing


OSPF
Interfaces
Instances
Networks
Areas
Area Ranges
Virtual Links
Neighbors
Router ID
Running
default
10.10.10.30
yes
OSPF Instance <default>
General
Metrics
MPLS
Status
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Name:
default
Router ID:
10.10.10.30
Redistribute Default Route:
never
Redistribute Connected Routes:
as type 1
Redistribute Static Routes:
no
Redistribute RIP Routes:
no
Redistribute BGP Routes:
no
Redistribute Other OSPF Routes:
no
In Filter:
ospf-in
Out Filter:
ospf-out
enabled

MikroTik

Firewall



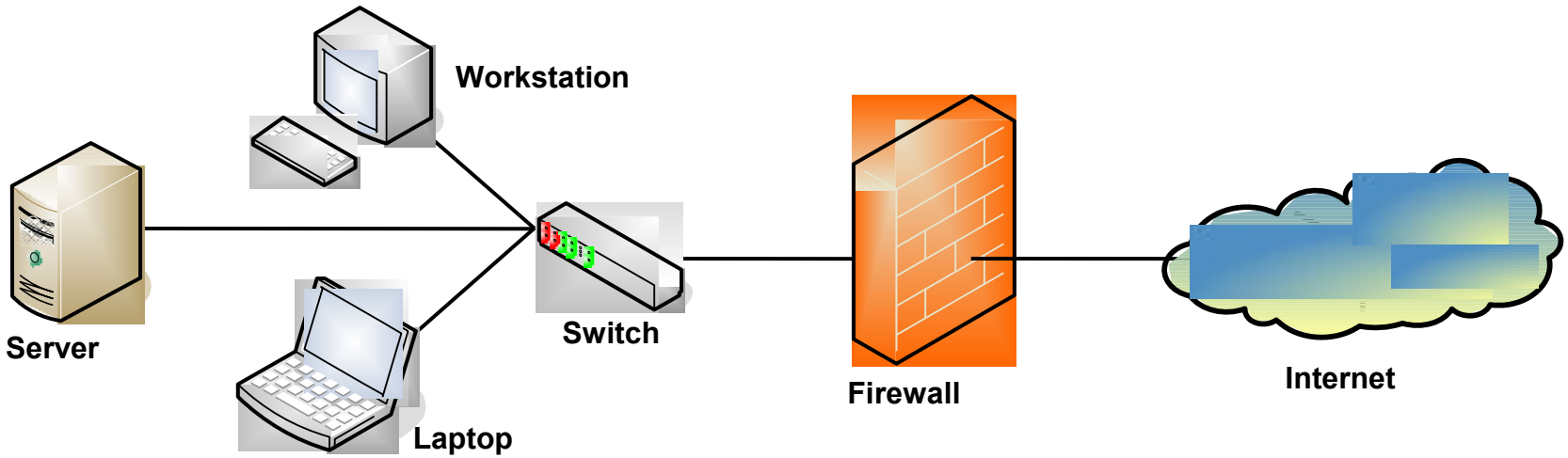
Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

Firewall ?

- Firewall diposisikan antara jaringan lokal dan jaringan publik, bertujuan melindungi komputer dari serangan, dan secara efektif mengontrol koneksi data menuju, dari, dan melalui router.



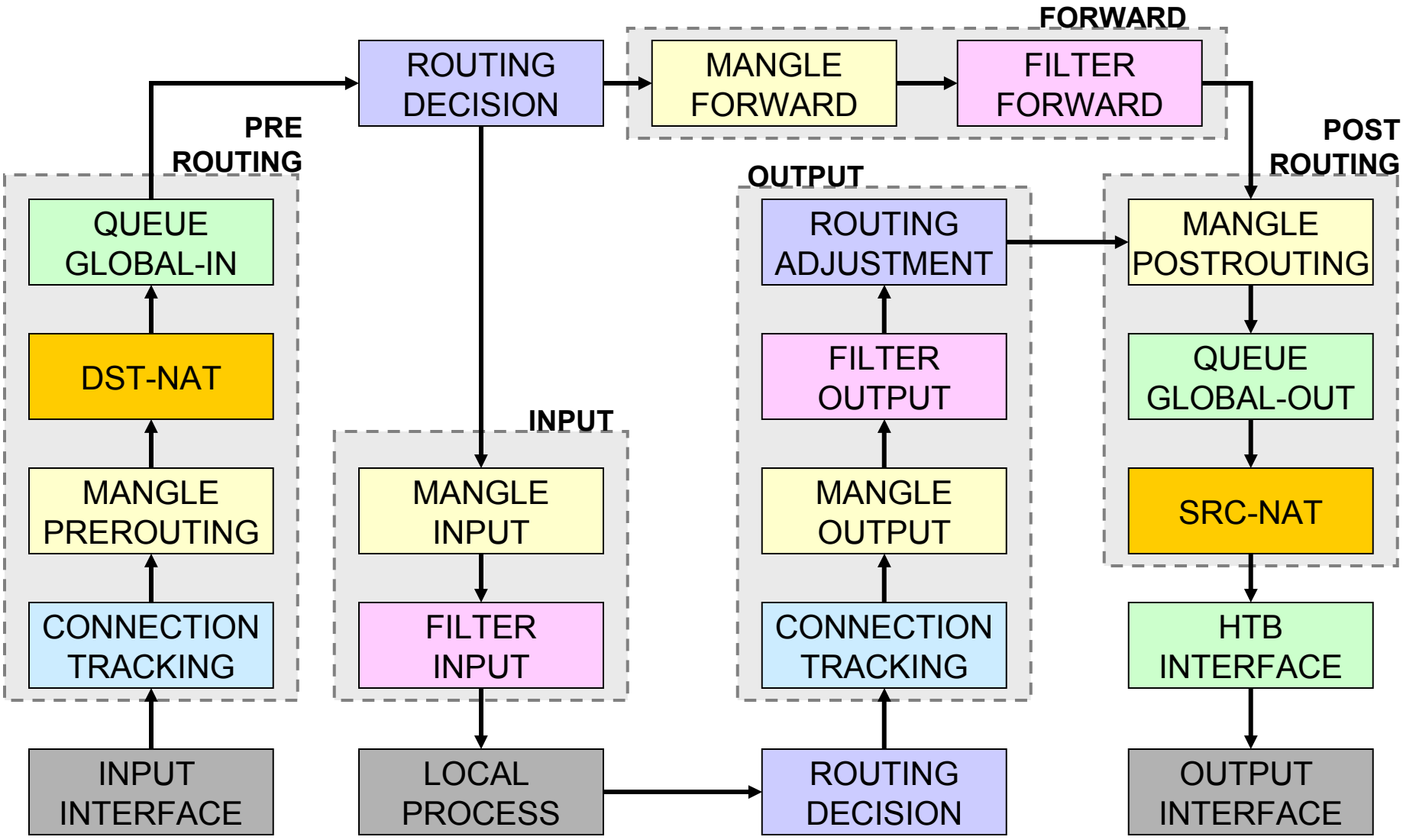
Mikrotik Firewall - Features

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

Traffic Flow (Aliran Data)

- Setiap paket data memiliki asal (source) dan tujuan (destination).
- Traffic flow bisa dibedakan menjadi 3 kategori, dilihat dari sudut pandang router.
  - **Dari Luar router menuju ke luar router lagi**
    - Contoh : traffic client browsing ke internet
  - **Dari luar router menuju ke dalam router itu sendiri (Local process)**.
    - Contoh : traffic winbox ke router
  - **Dari dalam router (local process) menuju ke luar router**.
    - Contoh : traffic ping dari new terminal winbox

Simple Packet Flow



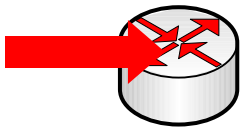
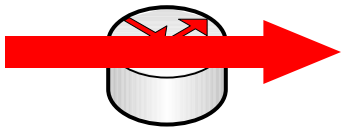
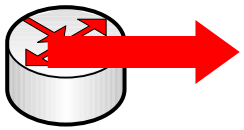
Posisi Chain / Parent

From	To	Mangle	Firewall	Queue
Outside	Router/ Local Process	Prerouting		Global-In
		Input	Input	Global-Total
Router/ Local Process	Outside	Output	Output	Global-Out
		Postrouting		Global-Total
				Interface
Outside	Outside	Prerouting		Global-In
		Forward	Forward	Global-Out
		Postrouting		Global-Total
				Interface

Firewall Filters – Blocking Rules

- Adalah cara untuk memfilter paket, dilakukan untuk meningkatkan keamanan jaringan, dan mengatur flow data dari, ke client, ataupun router
- Pembacaan rule filter dilakukan dari atas ke bawah secara berurutan. Jika melewati rule yang kriterianya sesuai akan dilakukan action yang ditentukan, jika tidak sesuai, akan dianalisa ke baris selanjutnya.

Chain pada Filter

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

RouterOS v5 Services

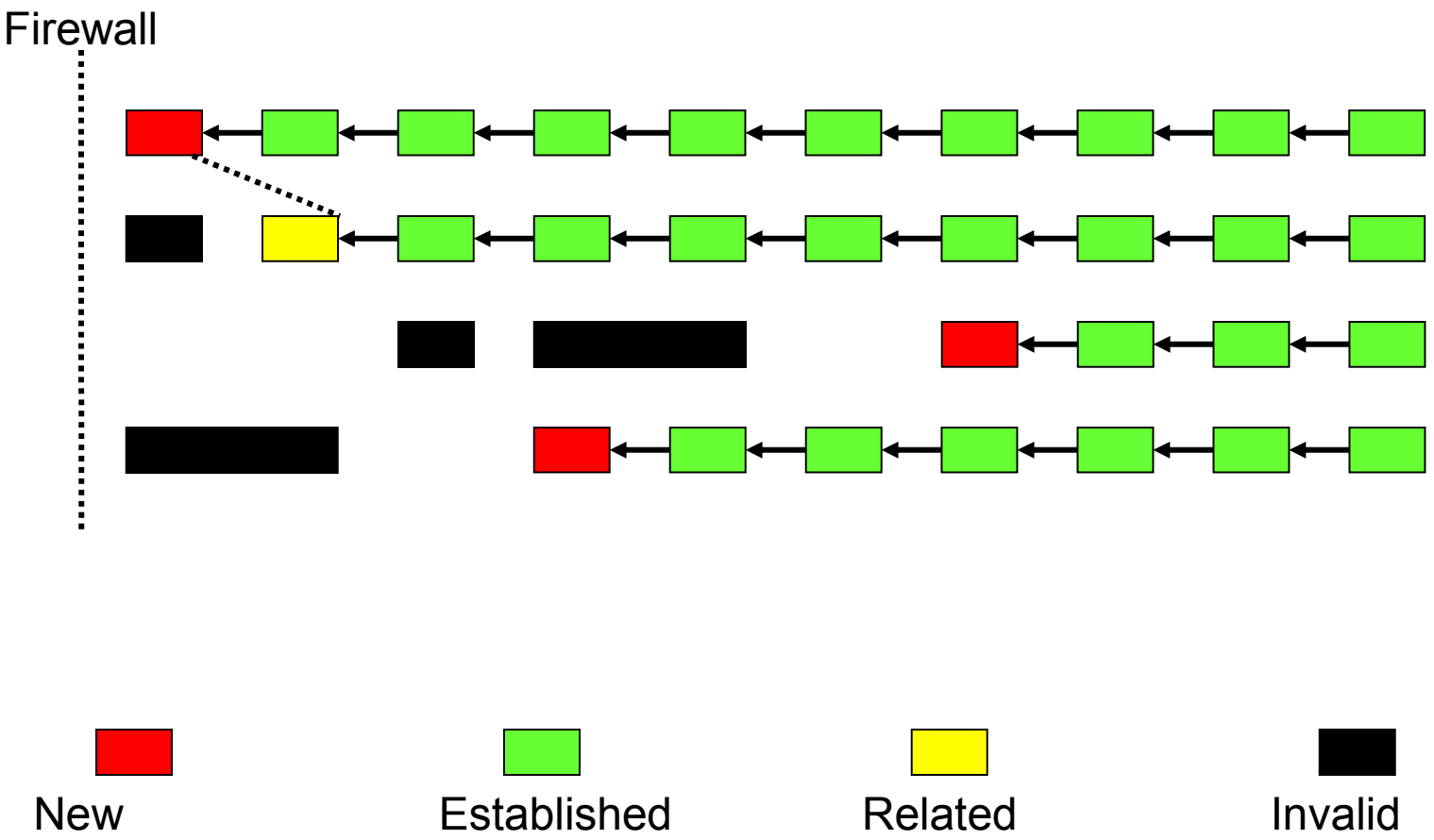
	PORT	PROTOCOL	DESCRIPTION
1	20	tcp	FTP
2	21	tcp	FTP
3	22	tcp	SSH, SFTP
4	23	tcp	Telnet
5	53	tcp	DNS
6	80	tcp	HTTP
7	179	tcp	BGP
8	443	tcp	SHTTP (Hotspot)
9	646	tcp	LDP (MPLS)
10	1080	tcp	SoCKS (Hotspot)
11	1723	tcp	PPTP
12	1968	tcp	MME
13	2000	tcp	Bandwidth Server
14	2210	tcp	Dude Server
15	2211	tcp	Dude Server
16	2828	tcp	uPnP
17	3128	tcp	Web Proxy
18	8291	tcp	Winbox
19	8728	tcp	API
20	---	/1	ICMP
21	---	/2	IGMP (Multicast)
22	---	/4	IPIP

	PORT	PROTOCOL	DESCRIPTION
23	53	udp	DNS
24	123	udp	NTP
25	161	udp	SNMP
26	500	udp	IPSec
27	520	udp	RIP
28	521	udp	RIP
29	646	udp	LDP (MPLS)
30	1698	udp	RSVP (MPLS)
31	1699	udp	RSVP (MPLS)
32	1701	udp	L2TP
33	1812	udp	User-Manager
34	1813	udp	User-Manager
35	1900	udp	uPnP
36	1966	udp	MME
37	5678	udp	Neighbor Discovery
38	---	/46	RSVP (MPLS)
39	---	/47	PPRP, EoIP
40	---	/50	IPSec
41	---	/51	IPSec
42	---	/89	OSPF
43	---	/103	PIM (Multicast)
44	---	/112	VRRP

Connection State

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

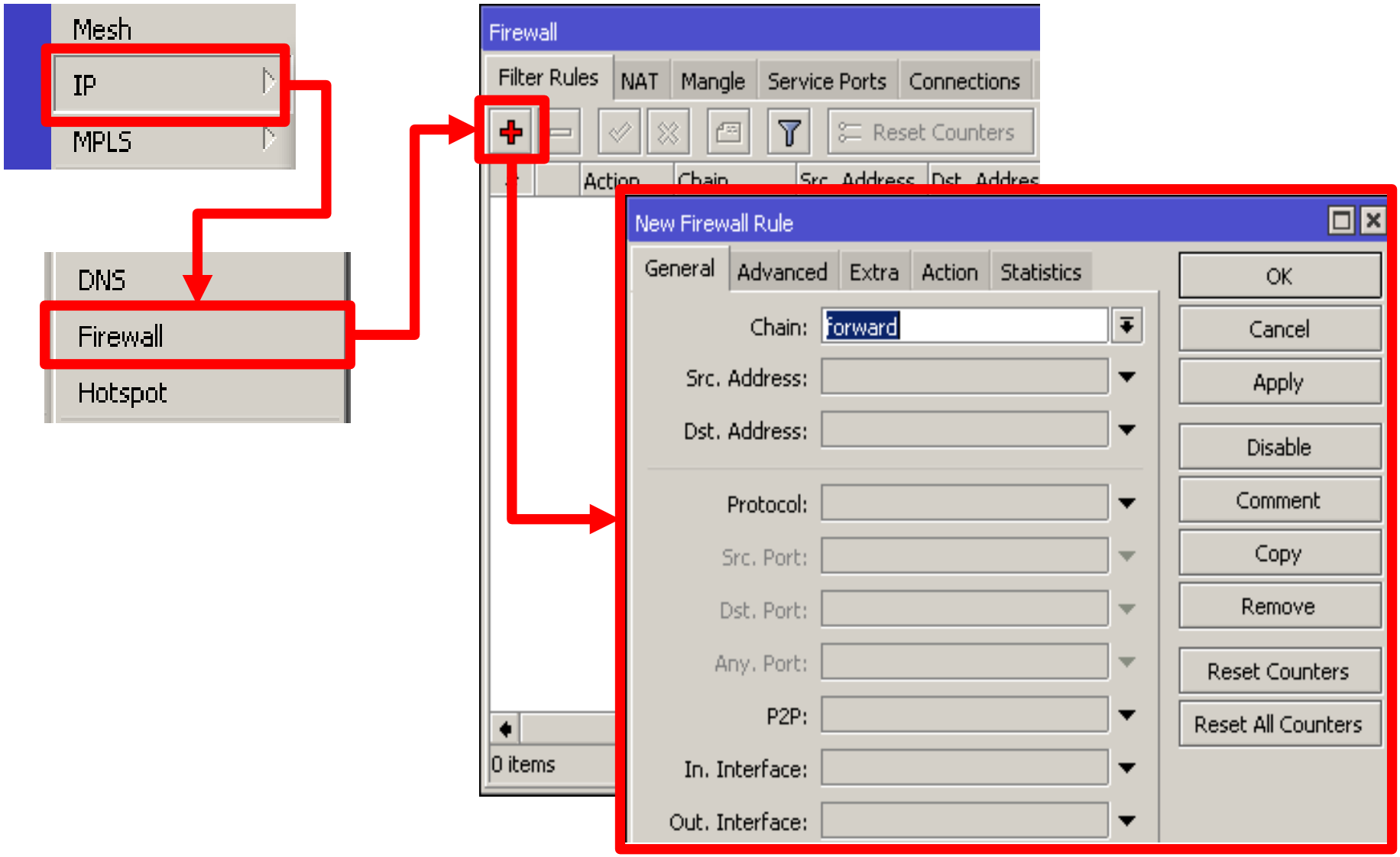
Connection State



Action Filter

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

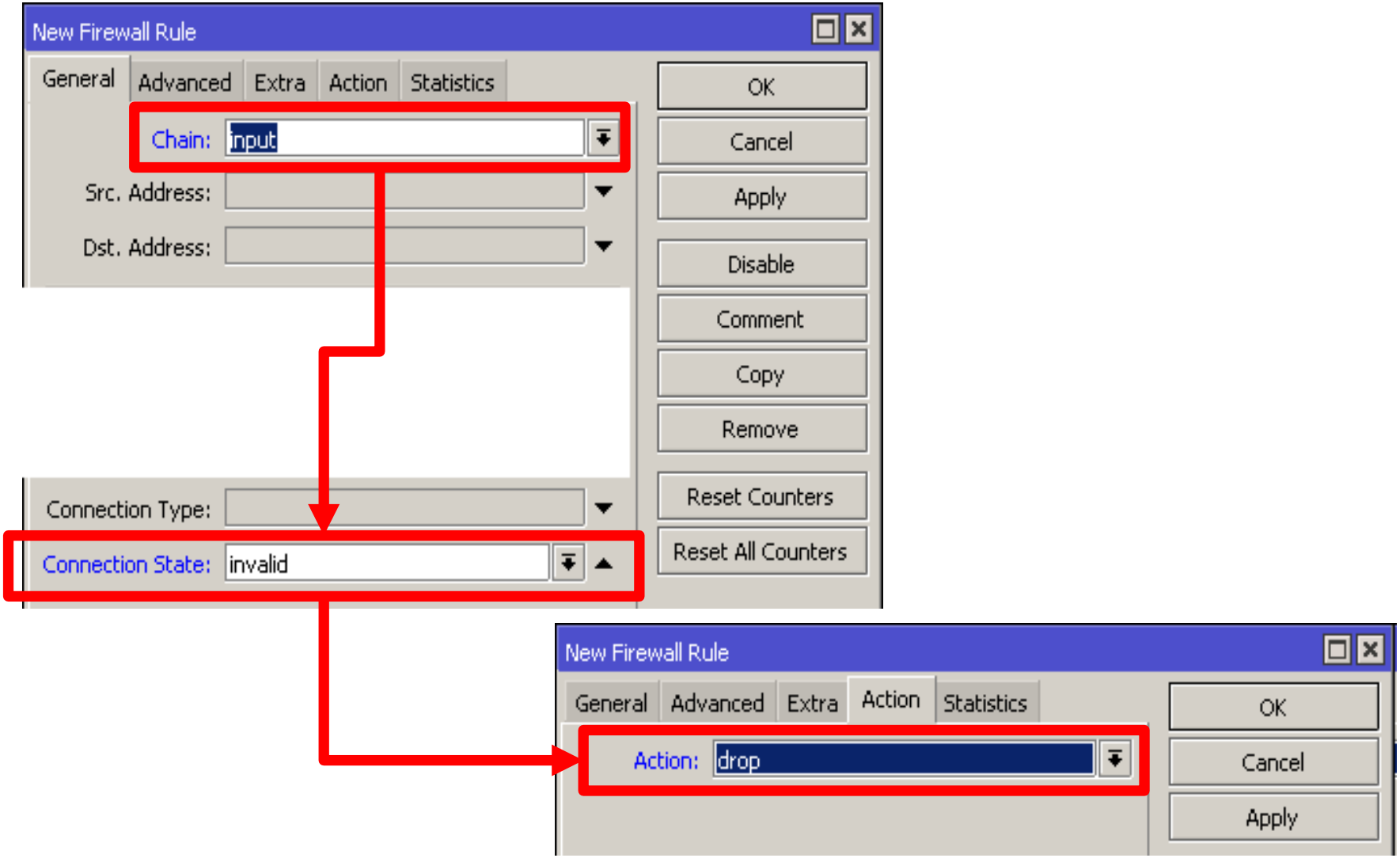
Filter Rules



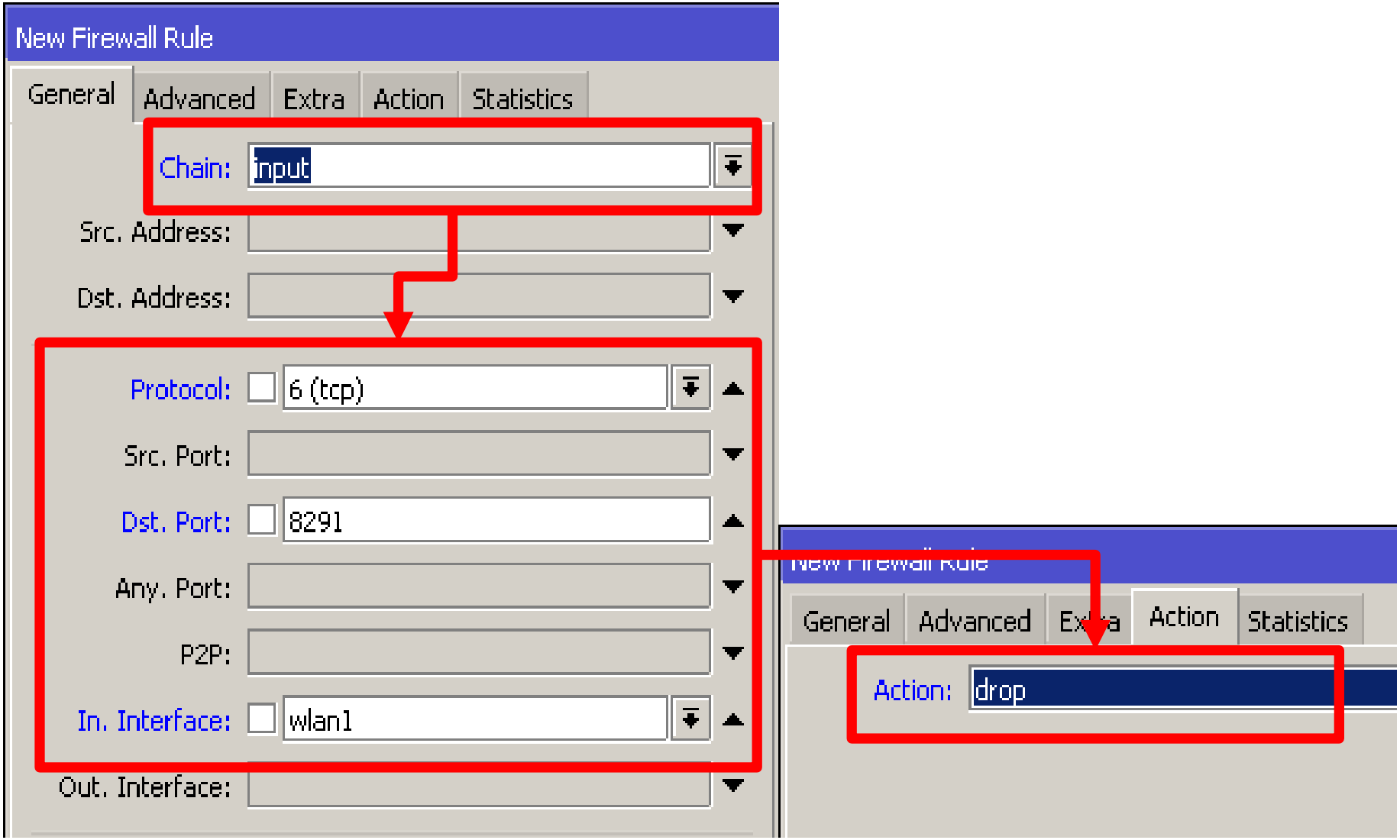
[LAB-2] Simple Blocking

- Blok semua invalid connection ke router
- Accept koneksi related dan established
- Blok koneksi winbox ke router yang masuk melalui interface public (wlan)
- Blok koneksi dari laptop ke ip tertentu, contoh: 10.10.10.100

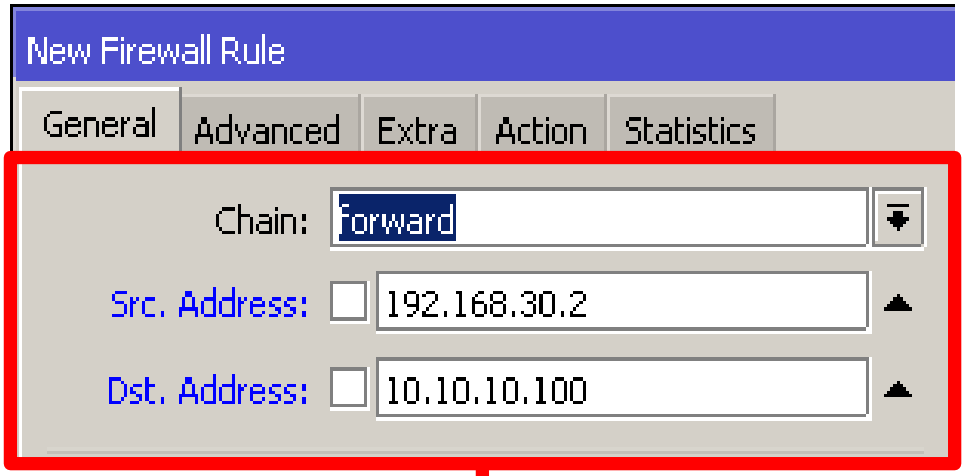
Blok Invalid Connection

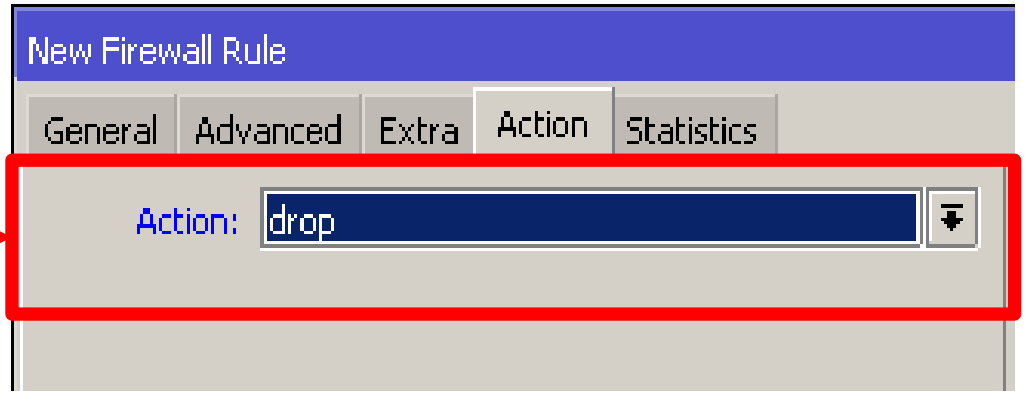


Blok Koneksi Winbox ke Router dari interface publik (wlan)



Blok Akses ke IP tujuan tertentu

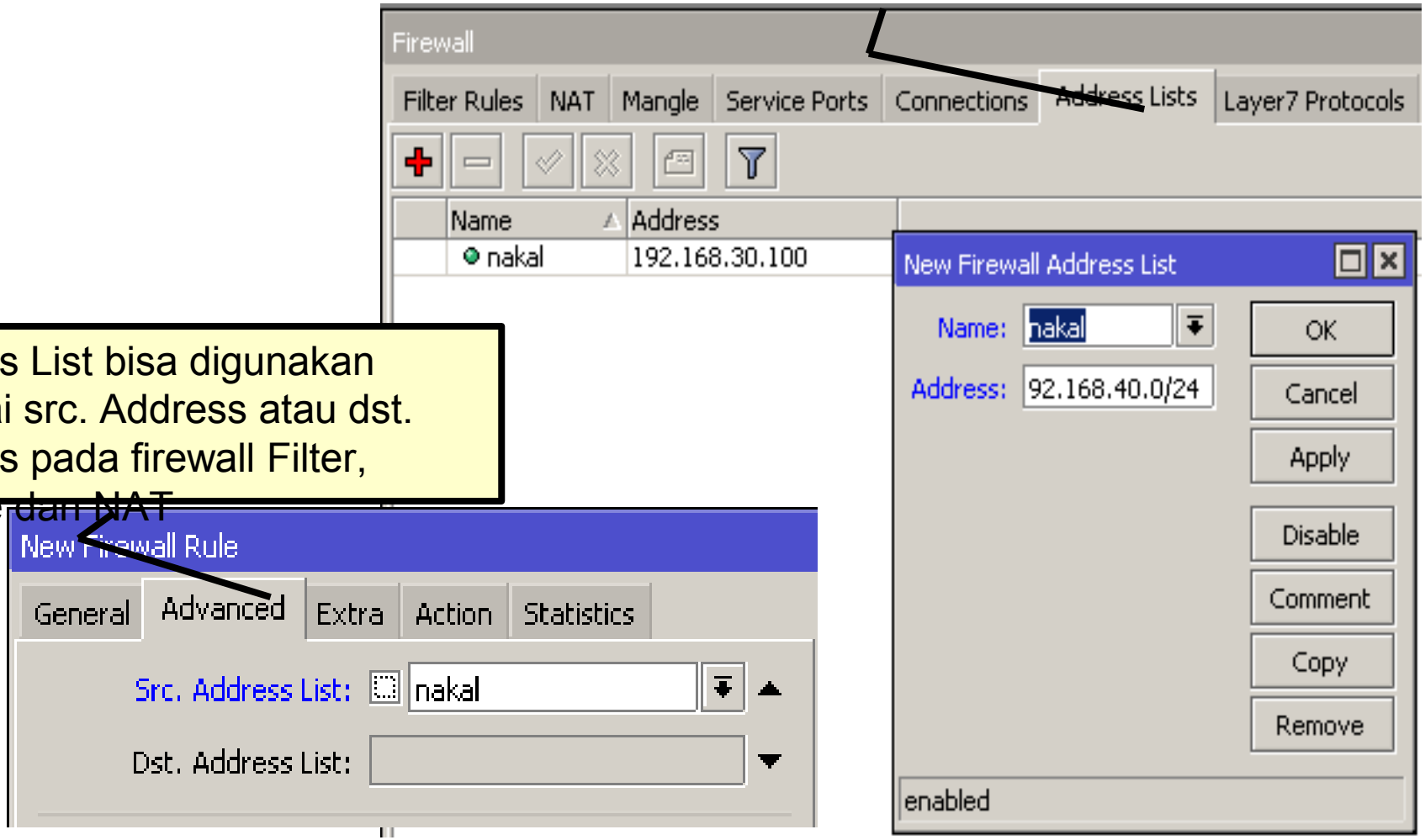




IP Address List

- Kita dapat melakukan pengelompokan IP Address dengan **Address List**

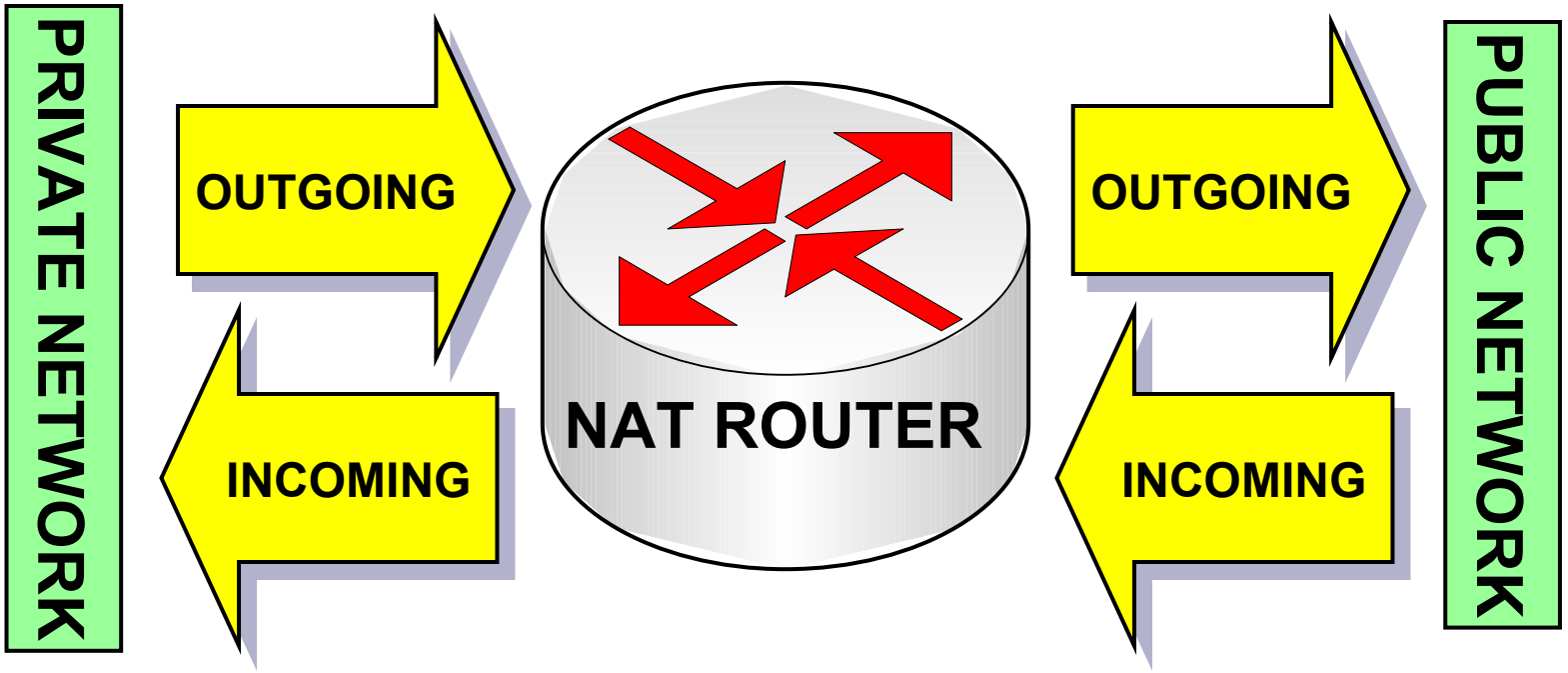
Address List bisa digunakan sebagai src. Address atau dst. Address pada firewall Filter, Mangle dan NAT



Network Address Translation (NAT)

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

Firewall NAT



The NAT router translates traffic coming into and leaving the private network

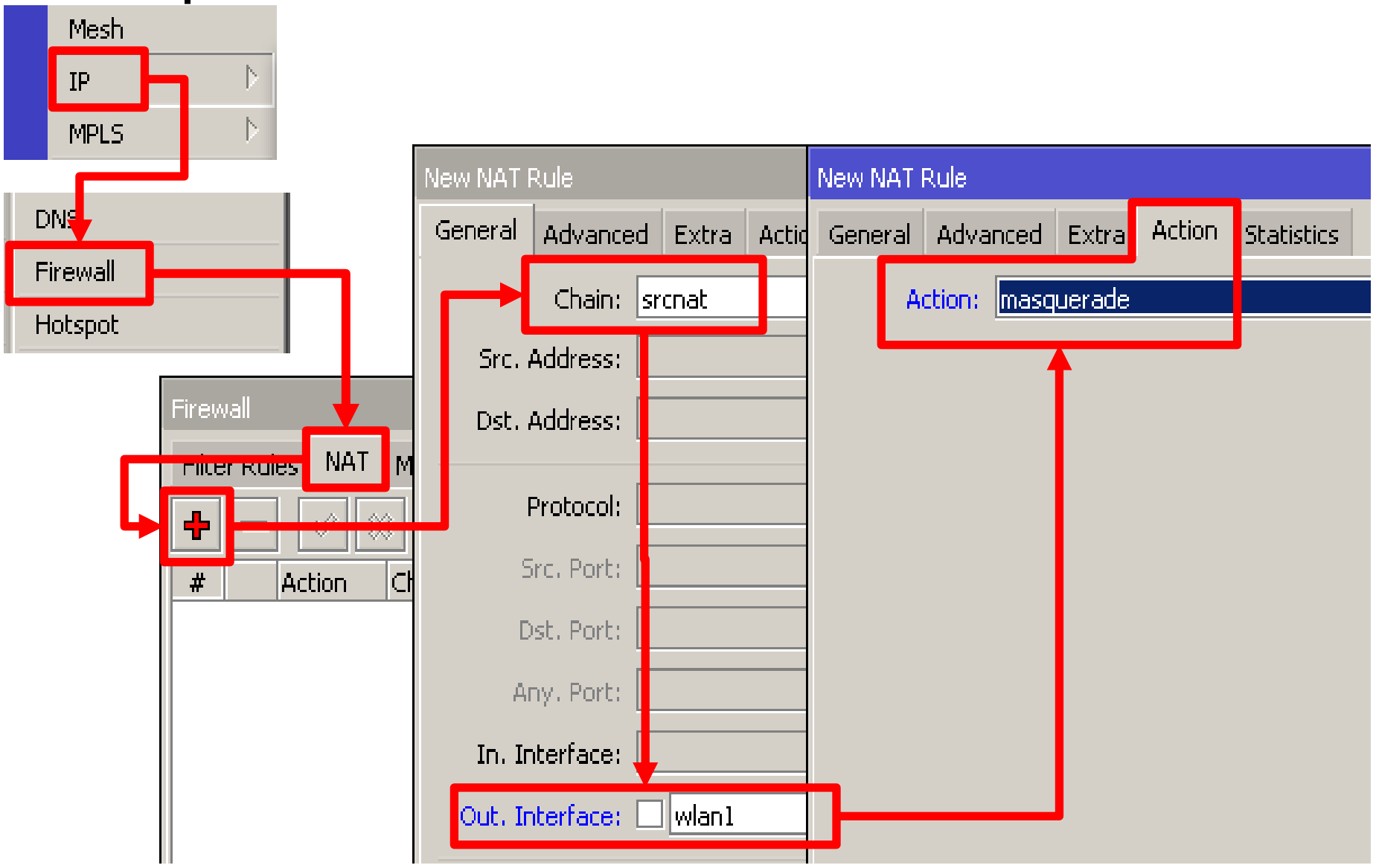
src-nat and masquerade

- Untuk menyembunyikan IP Address lokal dan menggantikannya dengan IP Address publik yang sudah terpasang pada router
- **src-nat**
  - Kita bisa memilih IP Address publik yang digunakan untuk menggantikan.
- **masquerade**
  - Secara otomatis akan menggunakan IP Address pada interface publik.
  - Digunakan untuk mempermudah instalasi dan bila IP Address publik pada interface publik menggunakan IP Address yang dinamik (misalnya DHCP, PPTP atau EoIP)

dst-nat and redirect

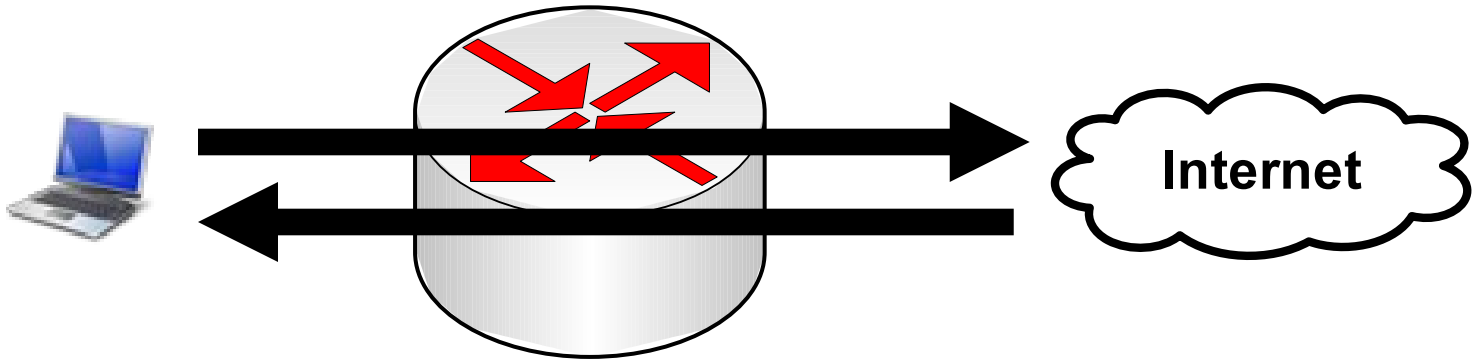
- Untuk melakukan penggantian IP Address tujuan, atau mengarahkan koneksi ke localhost.
- **dst-nat**
  - Kita bisa mengganti IP Address dan port tujuan dari seuatu koneksi.
- **redirect**
  - Untuk mengalihkan koneksi yang tadinya melwati router, dan dialihkan menuju ke loclhost

Firewall NAT

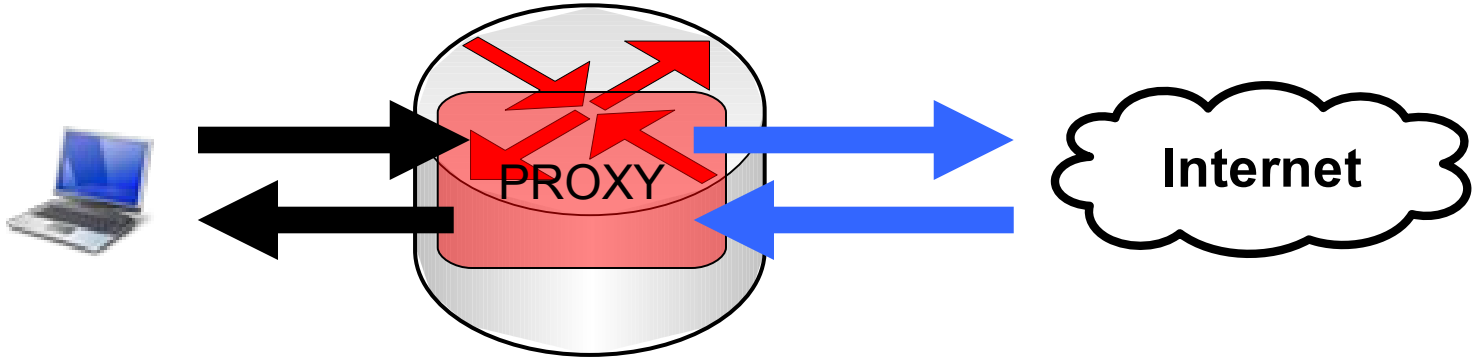


Konsep Proxy

- Pada semua level routeros, baik yang diinstall pada PC maupun yang diinstall pada routerboard, kita bisa mengaktifkan fitur proxy
- Koneksi tanpa proxy



- Koneksi dengan proxy



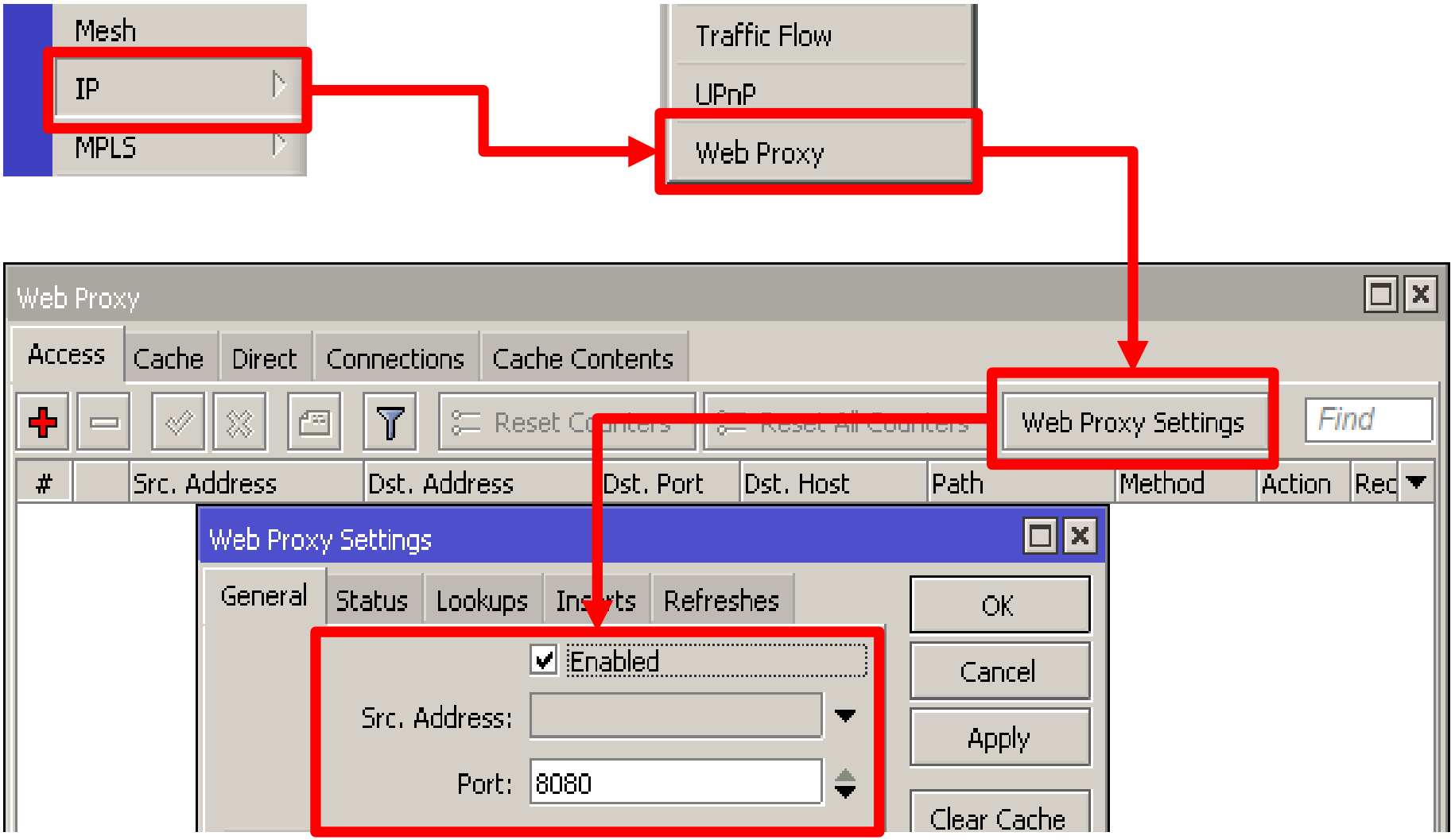
Fitur Proxy di RouterOS

- **Regular HTTP proxy**
- **Transparent proxy**
  - Dapat berfungsi juga sebagai transparan dan sekaligus normal pada saat yang bersamaan
- **Access list**
  - Berdasarkan source, destination, URL dan requested method
- **Cache Access list**
  - Menentukan objek mana yang disimpan pada cache
- **Direct Access List**
  - Mengatur koneksi mana yang diakses secara langsung dan yang melalui proxy server lainnya
- **Logging facility**

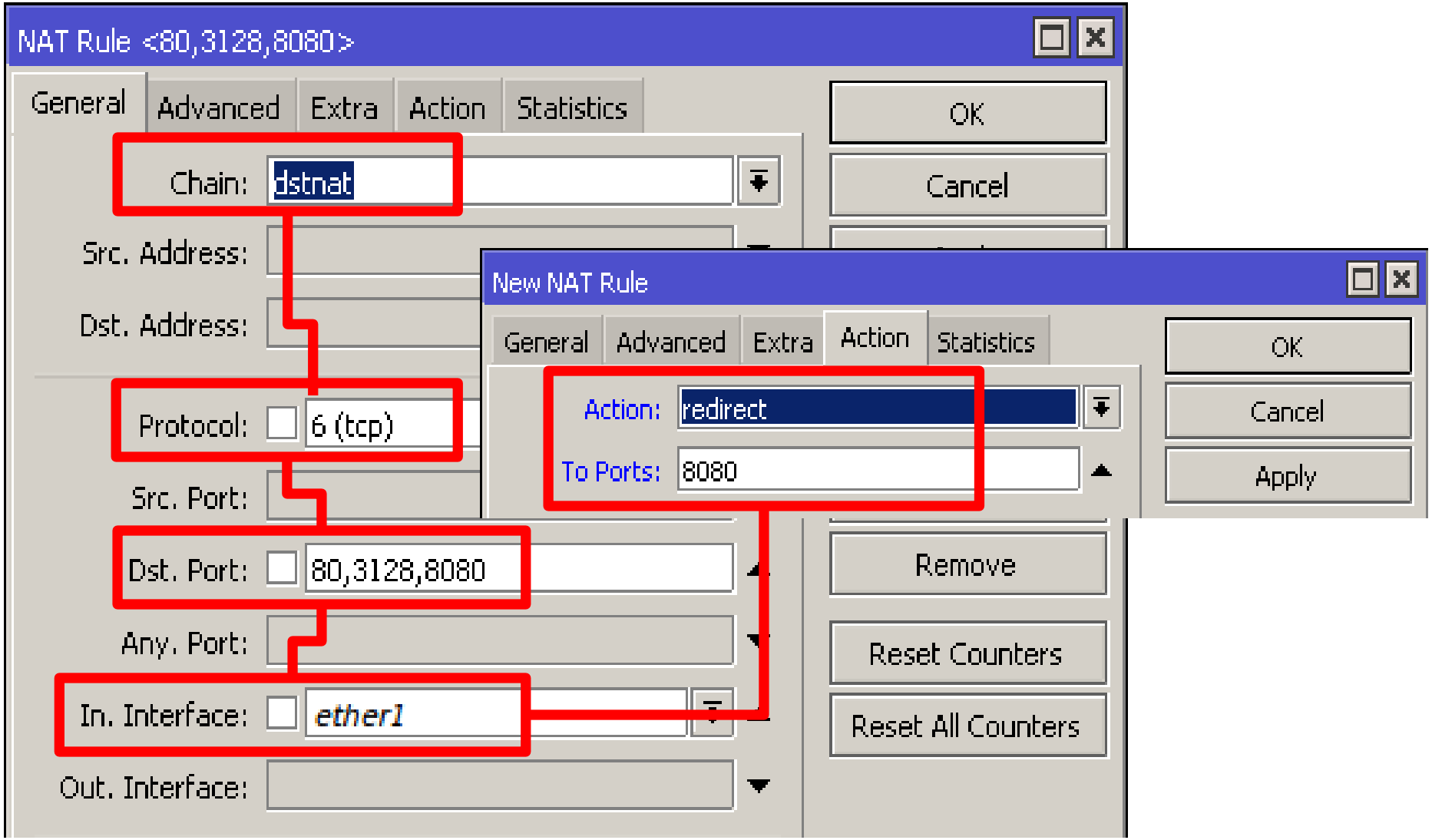
[LAB-5] dst-nat & local proxy

- Aktifkanlah service **web-proxy** pada router Anda.
- Lakukanlah pengalihan koneksi secara **transparan** sehingga semua koneksi HTTP akan **melalui web proxy** pada router.

Mengaktifkan Proxy

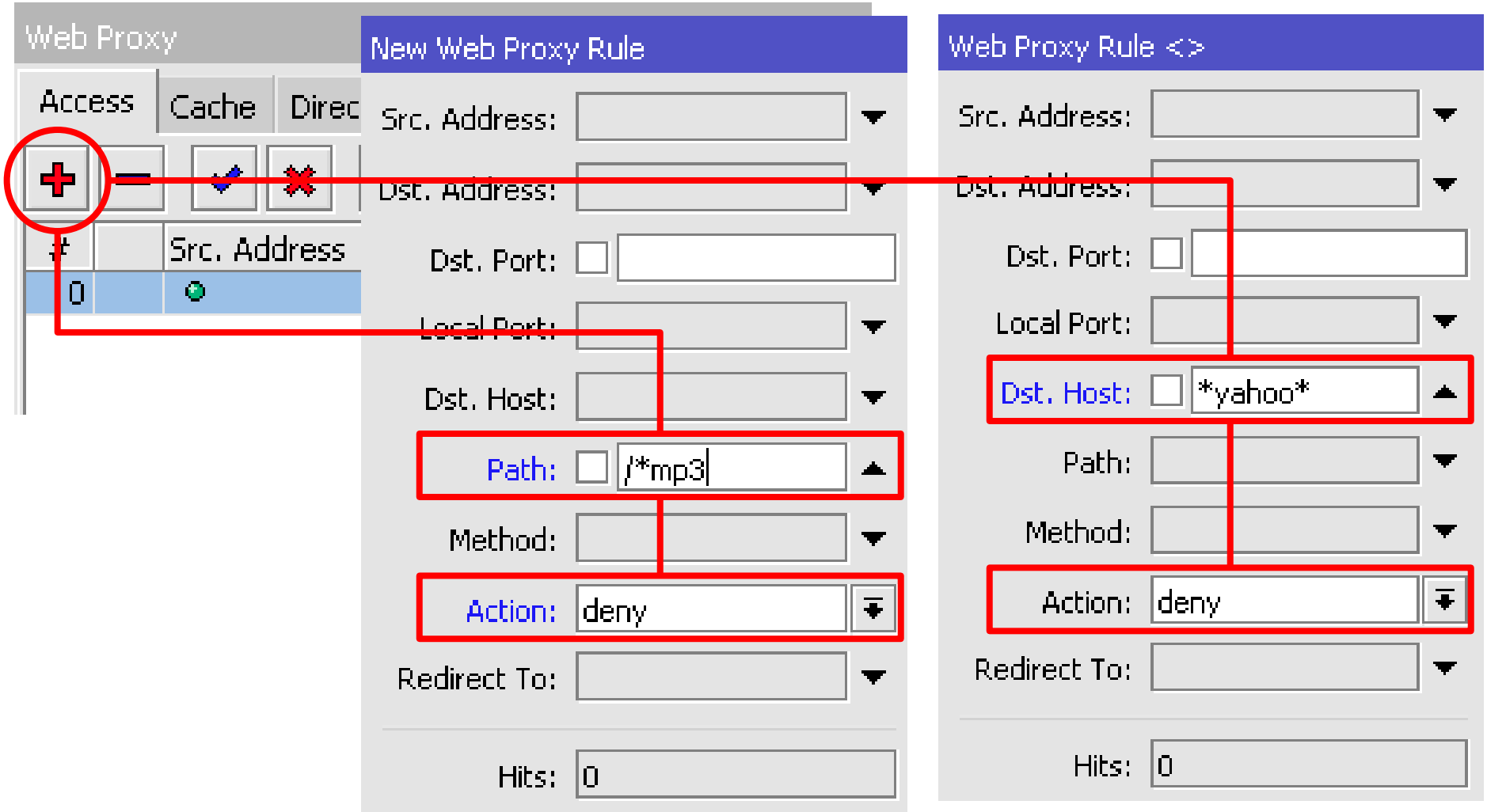


Redirect TCP-80



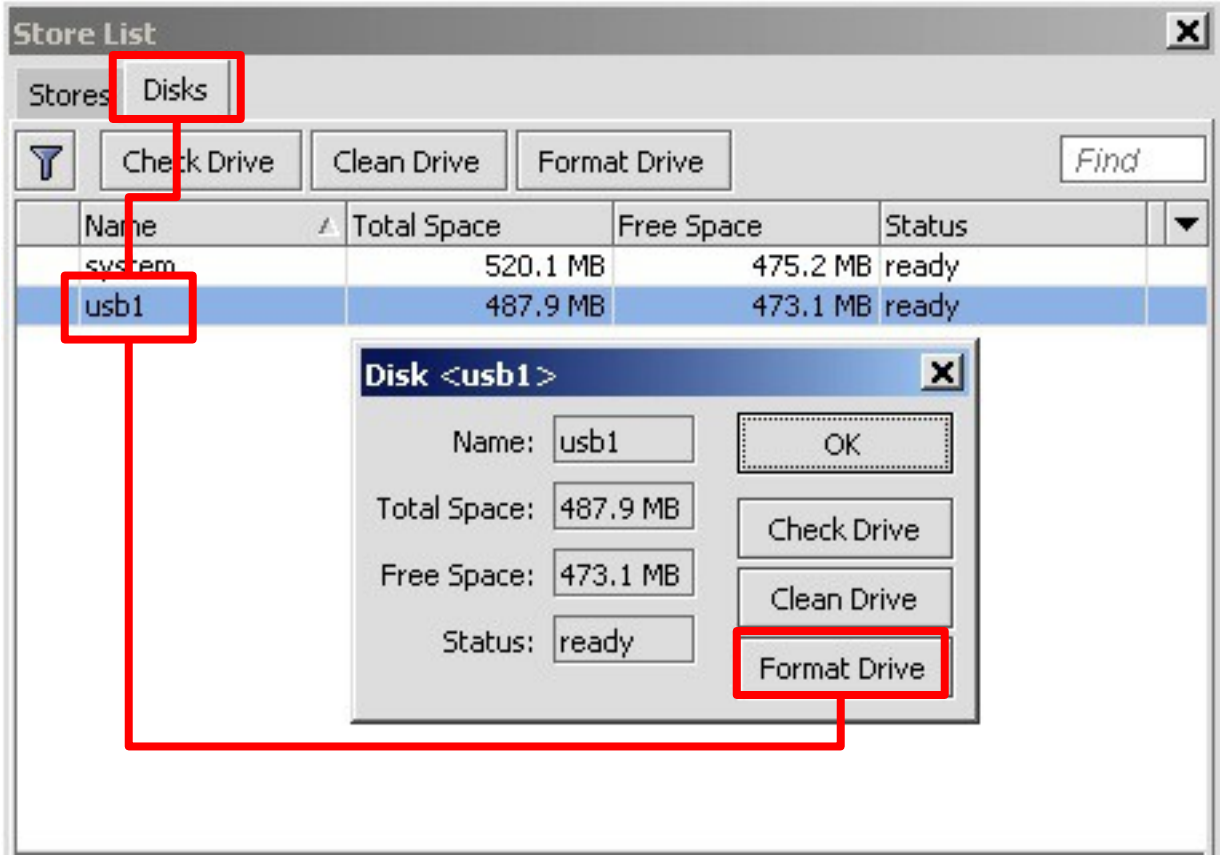
Akses

- Mengatur hak akses client (Access Filter)



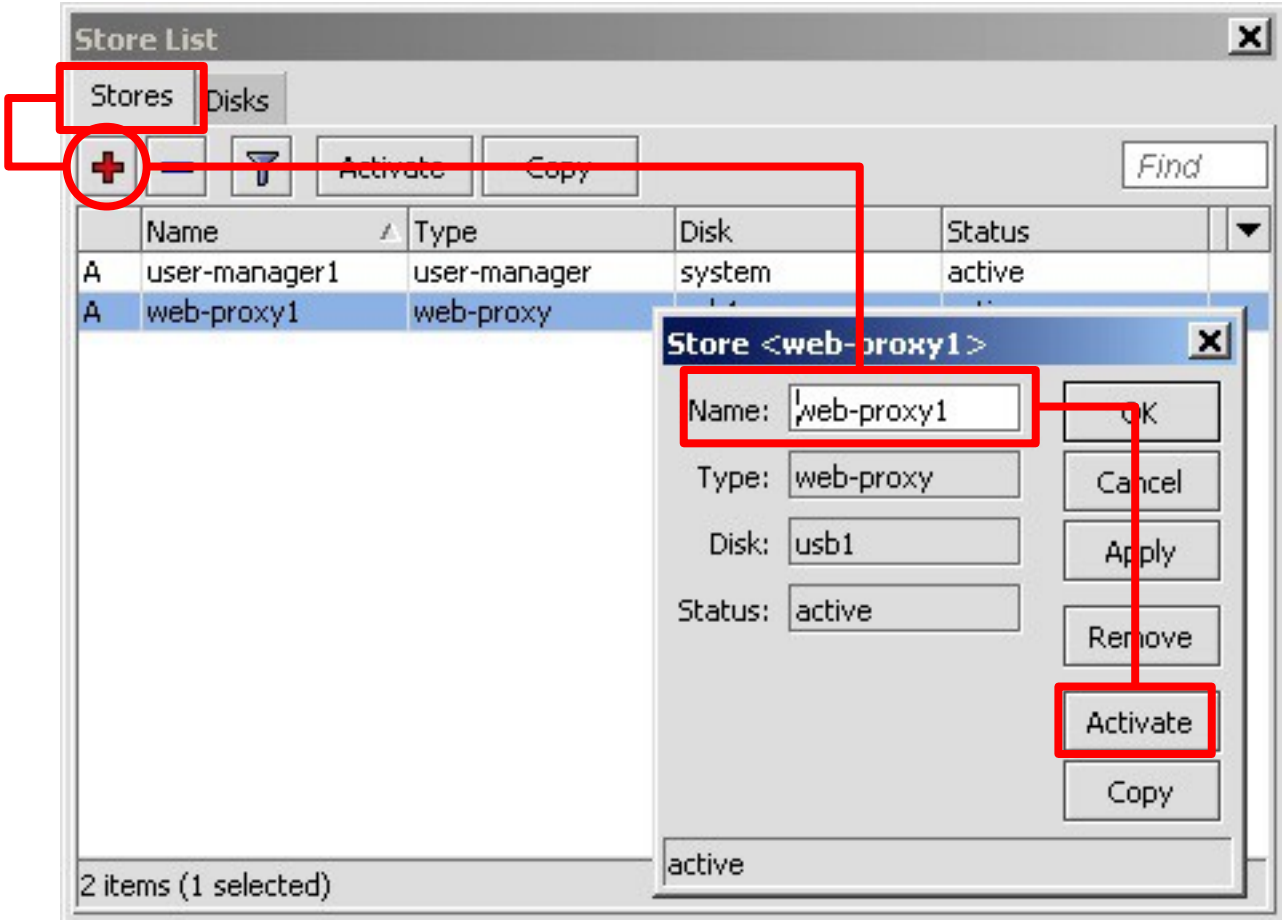
System Store - Disk

- Penyimpanan Cache
  - System Disk
  - Hardisk
  - Flash memory
- Format terlebih dahulu



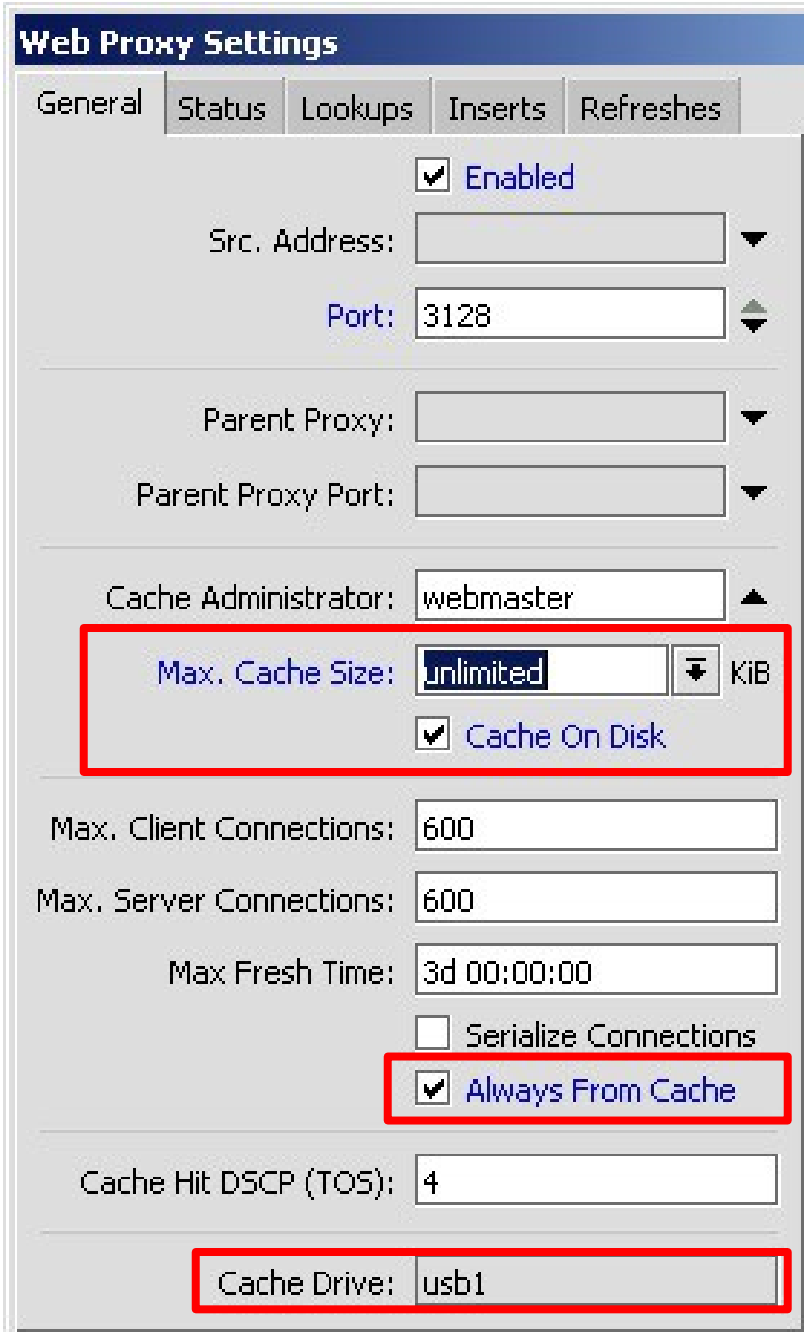
System Store – Store Mount

- Setelah diformat Disk di mount untuk service proxy.



Proxy - Cache

- Aktifkan “Cache On Disk” untuk mengaktifkan Mikrotik Proxy Cache.
- Perhatikan pada pada parameter “Cache Drive” sudah menggunakan USB disk.



MikroTik

Daftar Protokol dan Port yang Sebaiknya Ditutup

Karena Virus, Spyware, dll

Block Bogus IP Address

- add chain=forward src-address=0.0.0.0/8 action=drop
- add chain=forward dst-address=0.0.0.0/8 action=drop
- add chain=forward src-address=127.0.0.0/8 action=drop
- add chain=forward dst-address=127.0.0.0/8 action=drop
- add chain=forward src-address=224.0.0.0/3 action=drop
- add chain=forward dst-address=224.0.0.0/3 action=drop

Separate Protocol into Chains

- add chain=forward protocol=tcp action=jump jump-target=tcp
- add chain=forward protocol=udp action=jump jump-target=udp
- add chain=forward protocol=icmp action=jump jump-target=icmp

Blocking UDP Packet

- add chain=udp protocol=udp dst-port=69 action=drop comment="deny TFTP“
- add chain=udp protocol=udp dst-port=111 action=drop comment="deny PRC portmapper“
- add chain=udp protocol=udp dst-port=135 action=drop comment="deny PRC portmapper“
- add chain=udp protocol=udp dst-port=137-139 action=drop comment="deny NBT“
- add chain=udp protocol=udp dst-port=2049 action=drop comment="deny NFS"
- add chain=udp protocol=udp dst-port=3133 action=drop comment="deny BackOriffice"

Only needed icmp codes in icmp chain

- add chain=icmp protocol=icmp icmp-options=0:0 action=accept comment="drop invalid connections"
- add chain=icmp protocol=icmp icmp-options=3:0 action=accept comment="allow established connections"
- add chain=icmp protocol=icmp icmp-options=3:1 action=accept comment="allow already established connections"
- add chain=icmp protocol=icmp icmp-options=4:0 action=accept comment="allow source quench"
- add chain=icmp protocol=icmp icmp-options=8:0 action=accept comment="allow echo request"
- add chain=icmp protocol=icmp icmp-options=11:0 action=accept comment="allow time exceed"
- add chain=icmp protocol=icmp icmp-options=12:0 action=accept comment="allow parameter bad"
- add chain=icmp action=drop comment="deny all other types"

Deny Some TCP Ports

- add chain=tcp protocol=tcp dst-port=69 action=drop comment="deny TFTP"
- add chain=tcp protocol=tcp dst-port=111 action=drop comment="deny RPC portmapper"
- add chain=tcp protocol=tcp dst-port=135 action=drop comment="deny RPC portmapper"
- add chain=tcp protocol=tcp dst-port=137-139 action=drop comment="deny NBT"
- add chain=tcp protocol=tcp dst-port=445 action=drop comment="deny cifs"
- add chain=tcp protocol=tcp dst-port=2049 action=drop comment="deny NFS"
- add chain=tcp protocol=tcp dst-port=12345-12346 action=drop comment="deny NetBus"
- add chain=tcp protocol=tcp dst-port=20034 action=drop comment="deny NetBus"
- add chain=tcp protocol=tcp dst-port=3133 action=drop comment="deny BackOriffice"
- add chain=tcp protocol=tcp dst-port=67-68 action=drop comment="deny DHCP"

Virus and Worms (1)

- Worm tcp dst-port=135-139
- Messenger Worm udp dst-port=135-139
- Blaster Worm tcp dst-port=445
- Blaster Worm udp dst-port=445
- Virus tcp dst-port=593
- Virus tcp dst-port=1024-1030
- MyDoom tcp dst-port=1080
- Virus tcp dst-port=1214
- ndm requester tcp dst-port=1363
- ndm server tcp dst-port=1364
- screen cast tcp dst-port=1368
- hromgrafx tcp dst-port=1373
- cichlid tcp dst-port=1377
- Worm tcp dst-port=1433-1434
- Bagle Virus tcp dst-port=2745

Virus and Worms (2)

- Dumaru.Y tcp dst-port=2283
- Beagle tcp dst-port=2535
- Beagle.C-K tcp dst-port=2745
- MyDoom tcp dst-port=3127-3128
- Backdoor OptixPro tcp dst-port=3410
- Worm tcp dst-port=4444
- Worm udp dst-port=4444
- Sasser tcp dst-port=5554
- Beagle.B tcp dst-port=8866
- Dabber.A-B tcp dst-port=9898
- Dumaru.Y tcp dst-port=10000
- MyDoom.B tcp dst-port=10080
- NetBus tcp dst-port=12345
- Kuang2 tcp dst-port=17300
- SubSeven tcp dst-port=27374
- PhatBot, Gaobot tcp dst-port=65506

Quality of Service

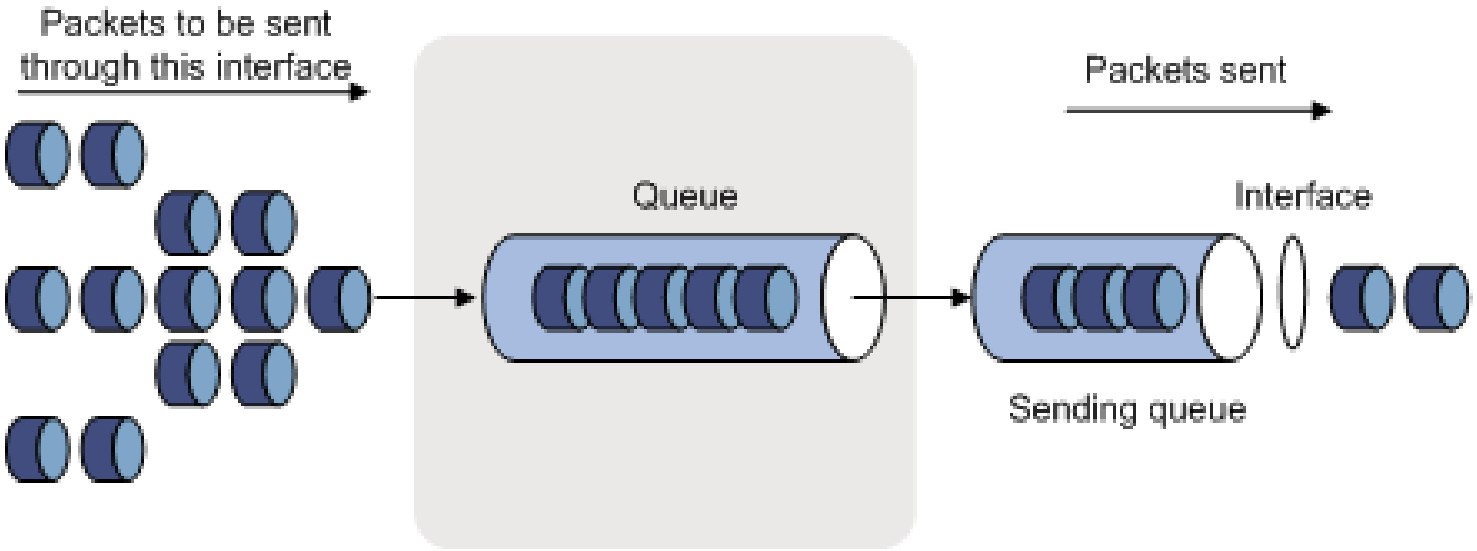
Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

Quality of Service

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



Quality of Service

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

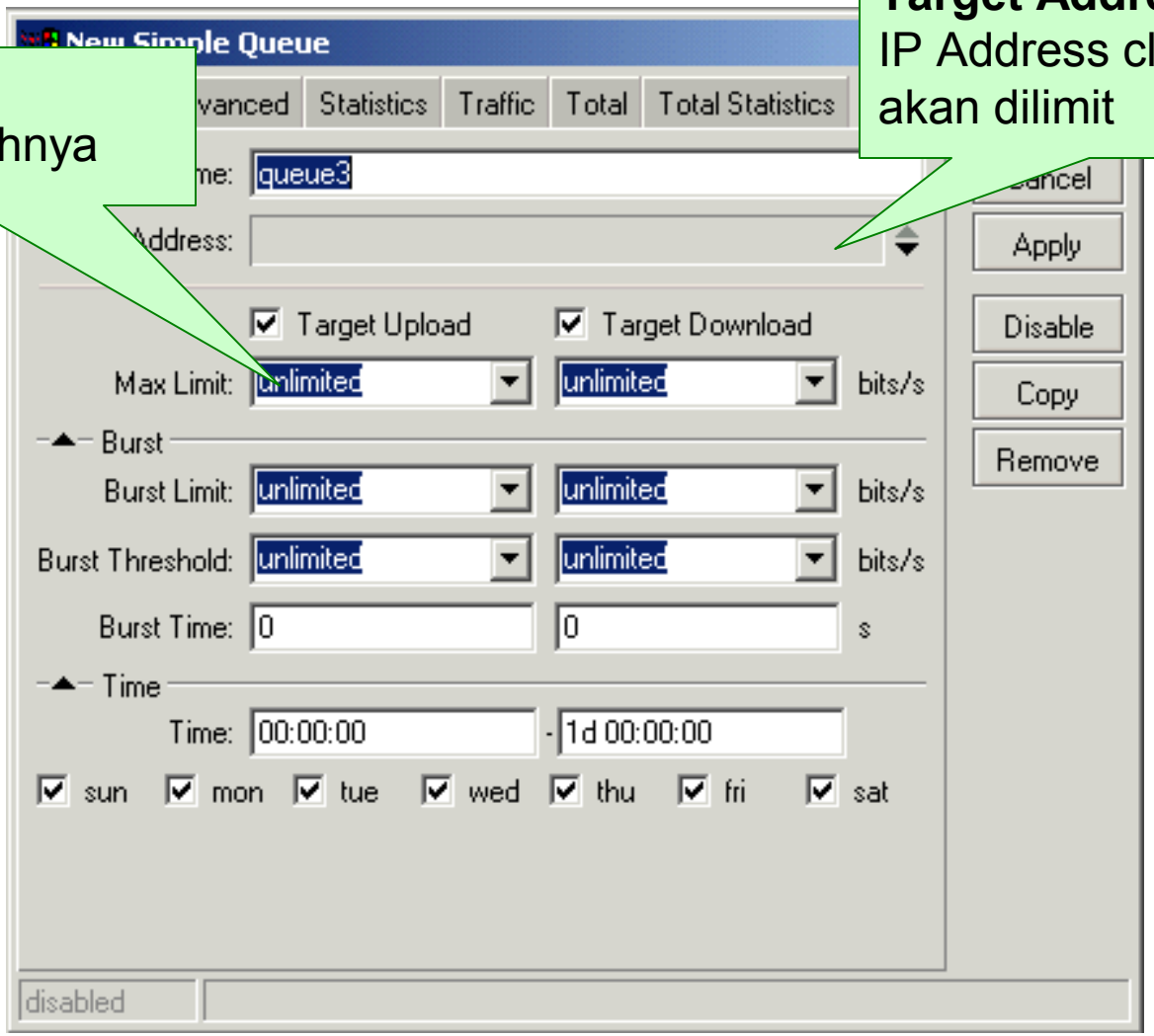
Simple Queue

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

Simple Queue Menu

MAX Limit :
Limitasi bandwithnya

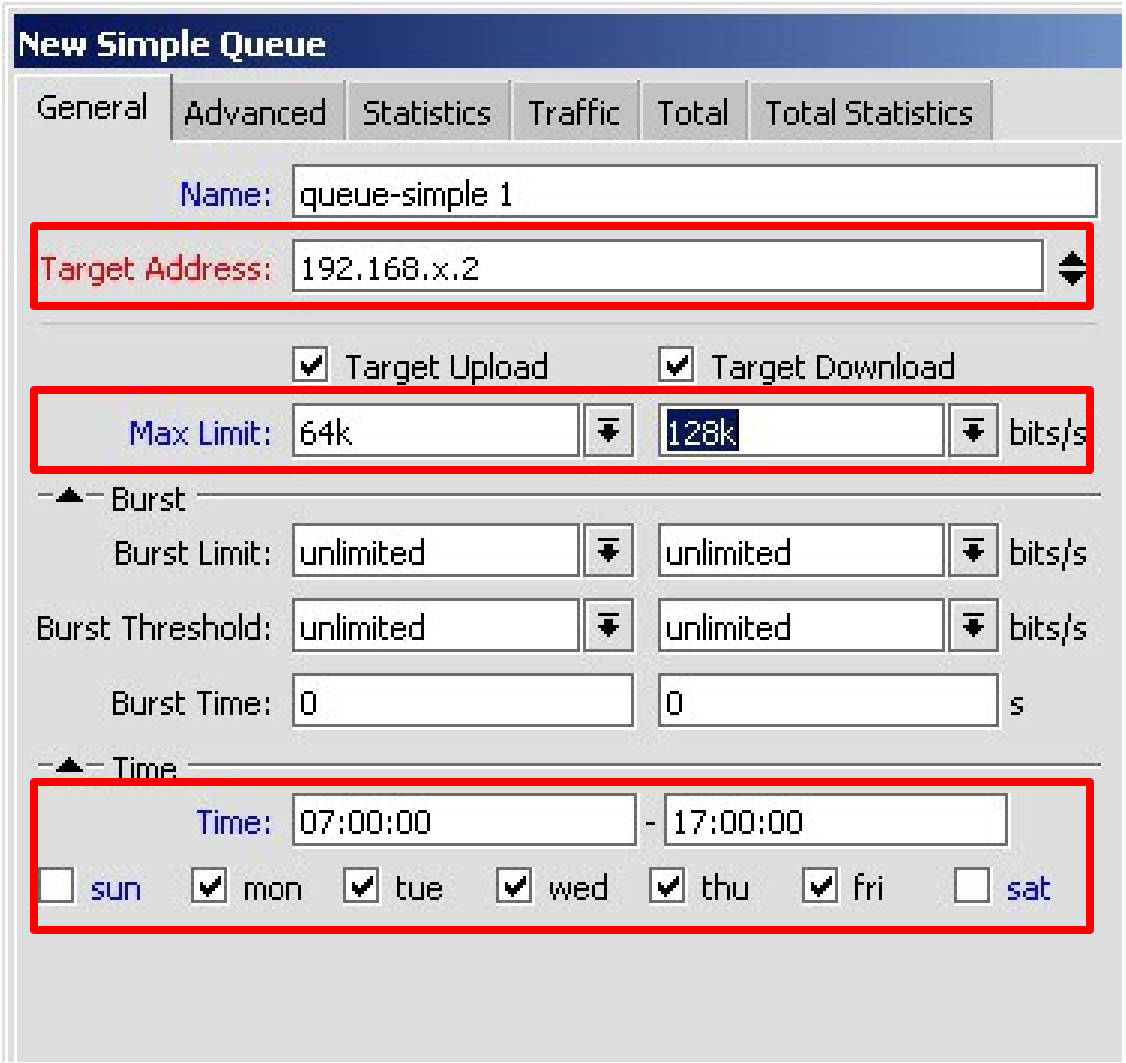
Target Address :
IP Address client yang akan dilimit



[LAB-1] Simple Queue 1

- Make a simple queue for your laptop
  - Downstream : 128 kbps
  - Upstream : 64 kbps
- Try Using **Time** (based from system clock)

[LAB-1] Simple Queue

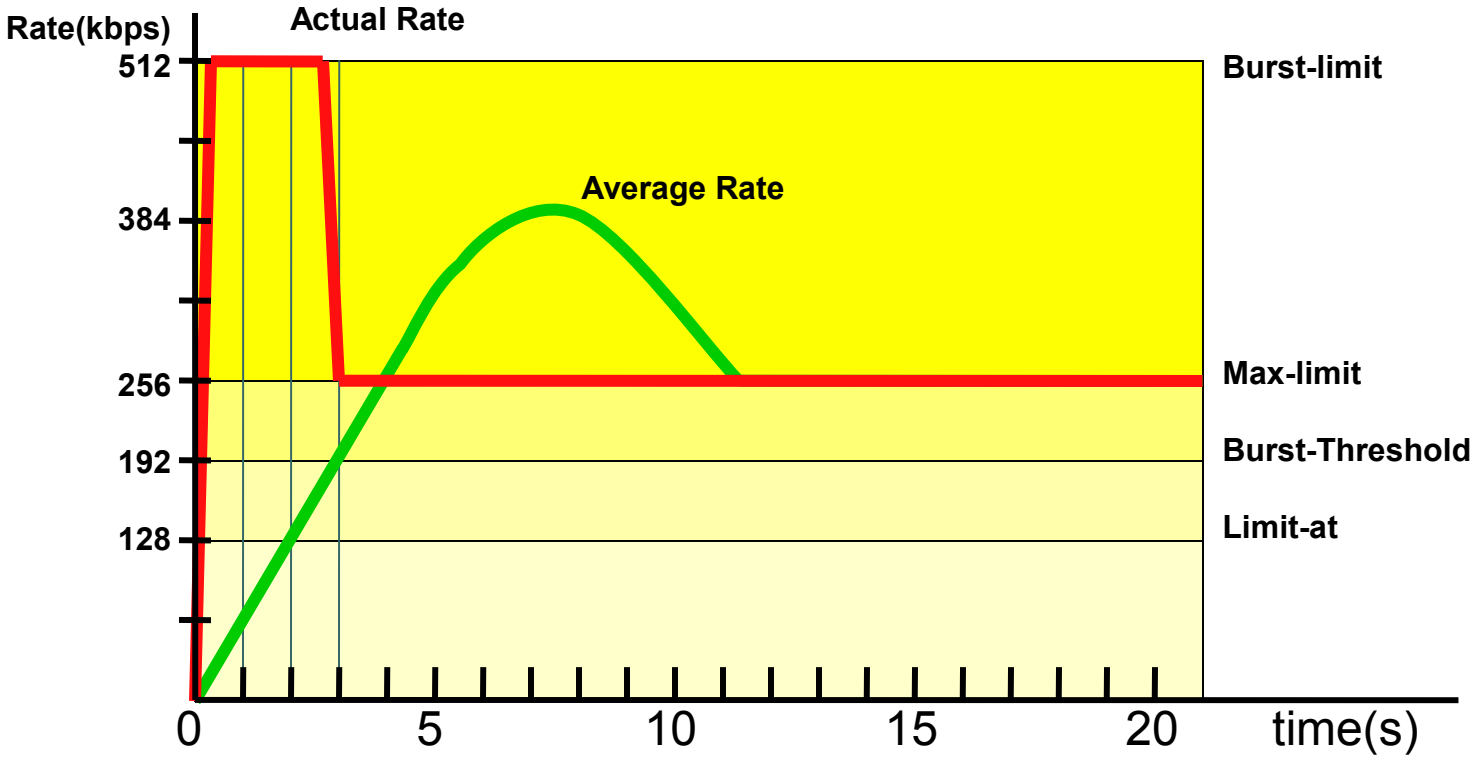


Burst

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

Contoh Burst (1)

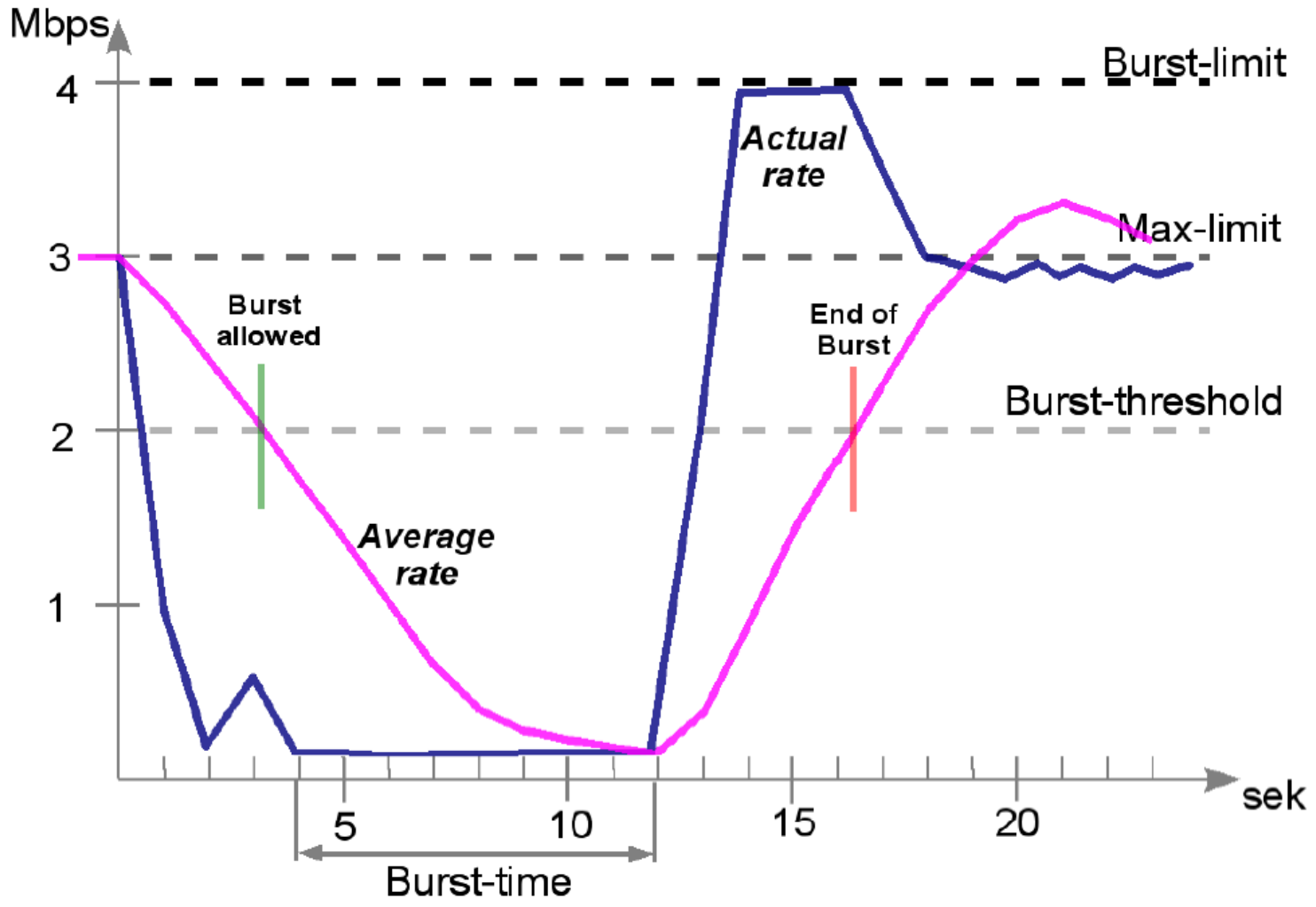
- **Max-limit**=256kbps, **burst-time**=8, **burst-threshold**=192kbps, **burst-limit**=512kbps.



Contoh Burst (1)

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

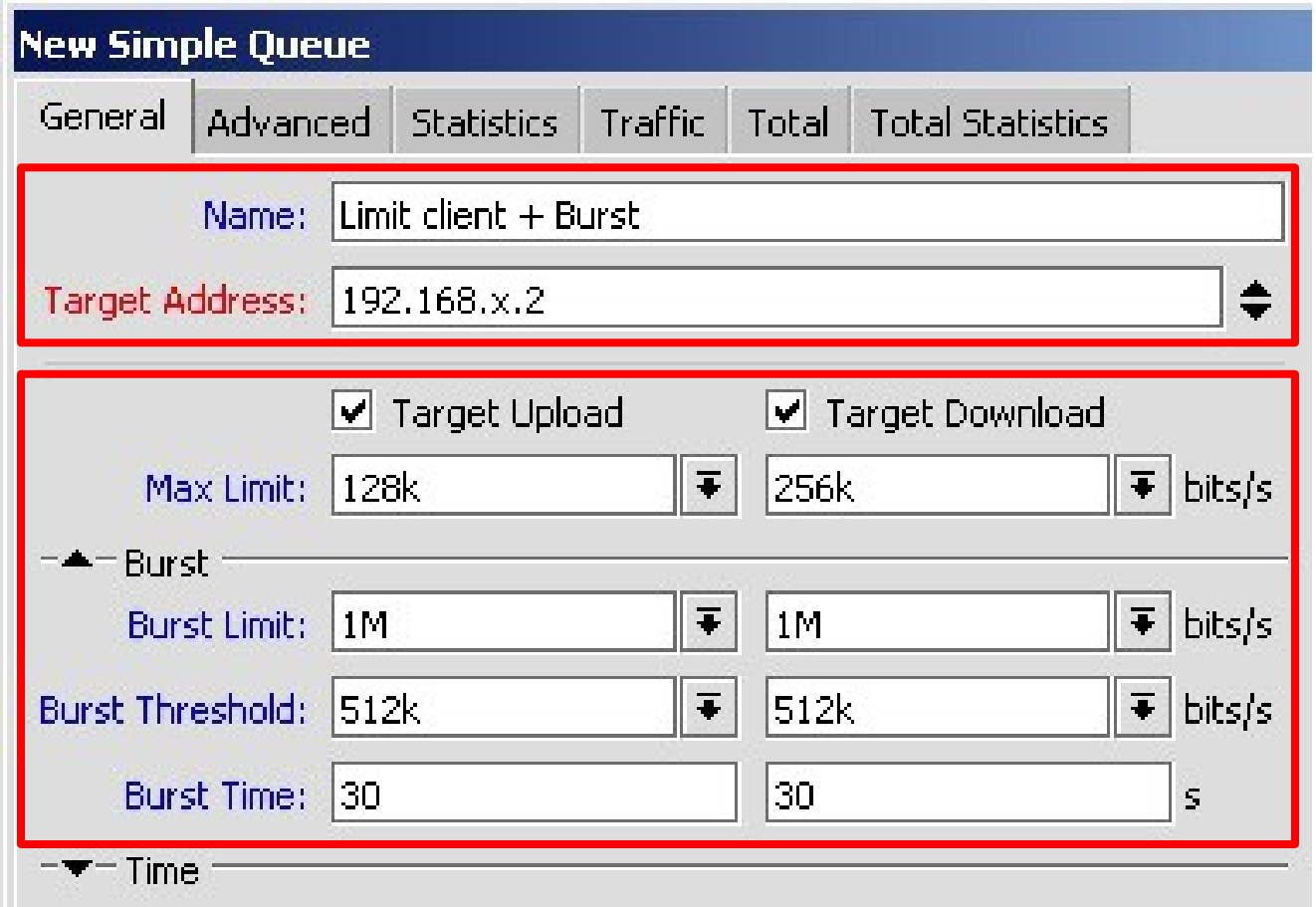
Contoh Burst (2)



[LAB-2] Simple Queue 2

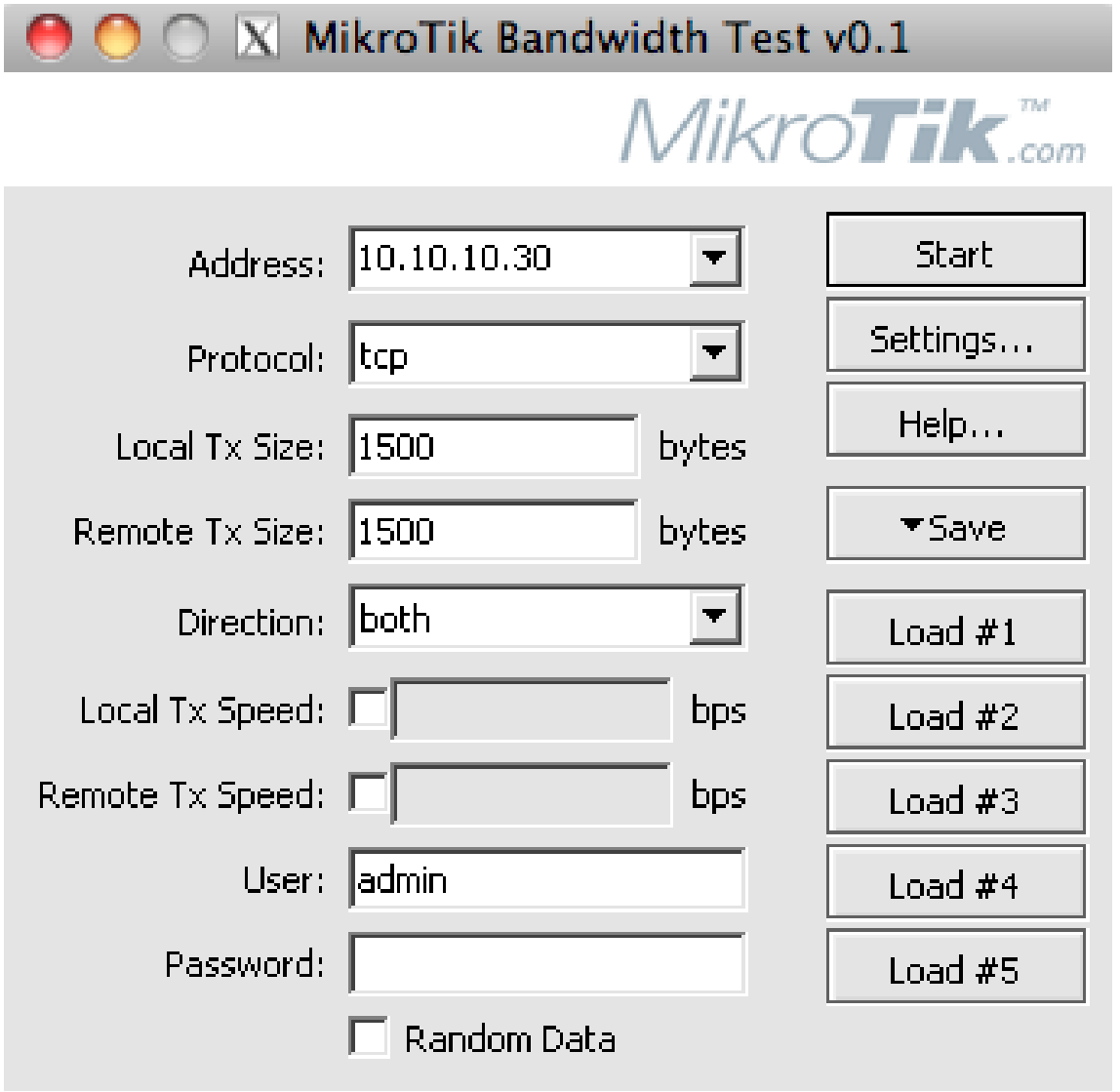
- Make a simple queue for your laptop
  - Downstream max-limit=256k
  - Upstream max-limit=128k
- Try Using Burst
  - Burst-limit=1M
  - Burst-threshold=512K
  - Burst-time=30s

[LAB-2] Simple Queue 2



Simple Queue – Bandwith Test

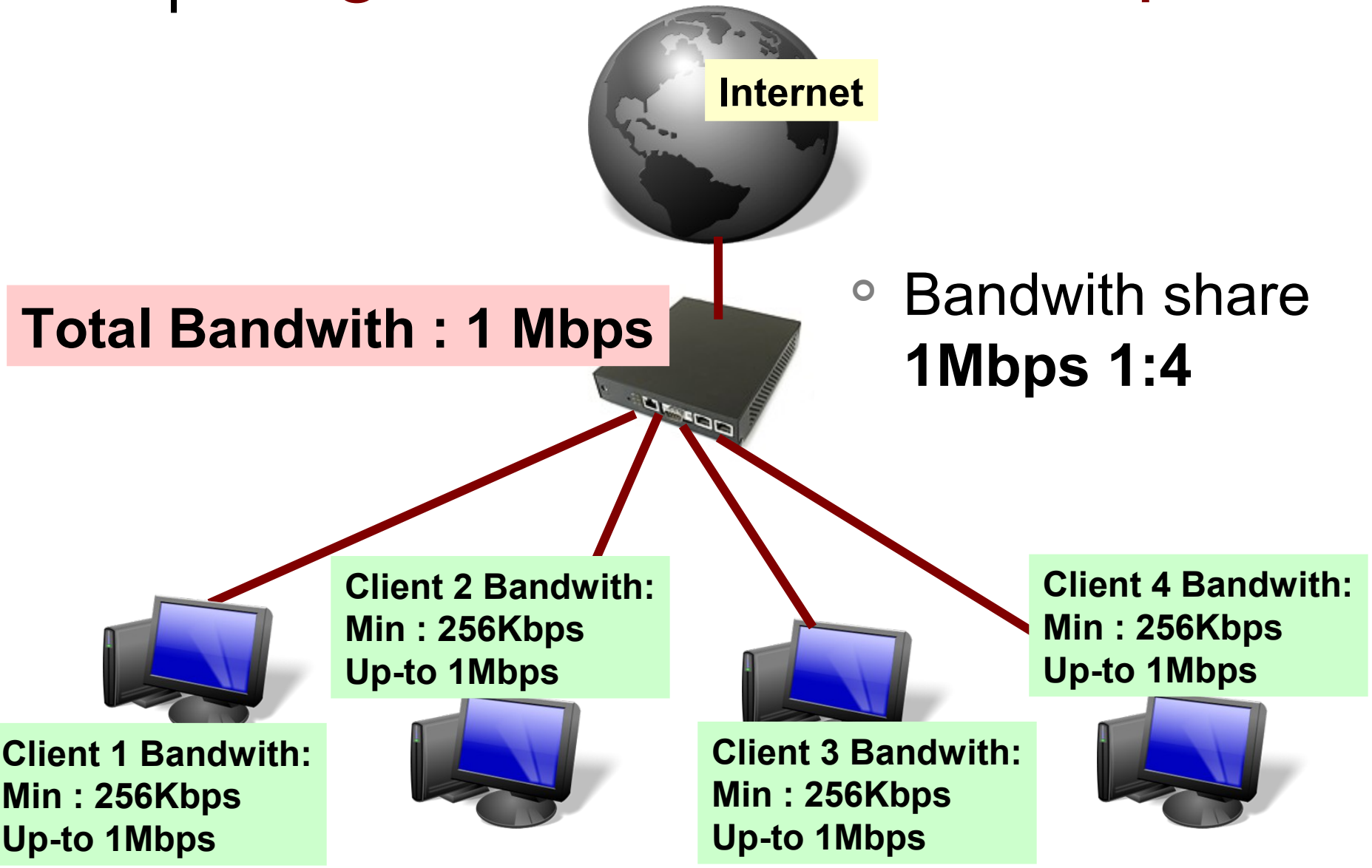
- **Address** :
  - Ip address test server
- **Direction** :
  - Upload
  - Download
  - Upload & Download
- **Protocol** :
  - TCP / UDP
- **User & Password** :
  - Autentikasi



Staged Limitation

- Pada RouterOS, dikenal 2 buah limitasi:
  - **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**"

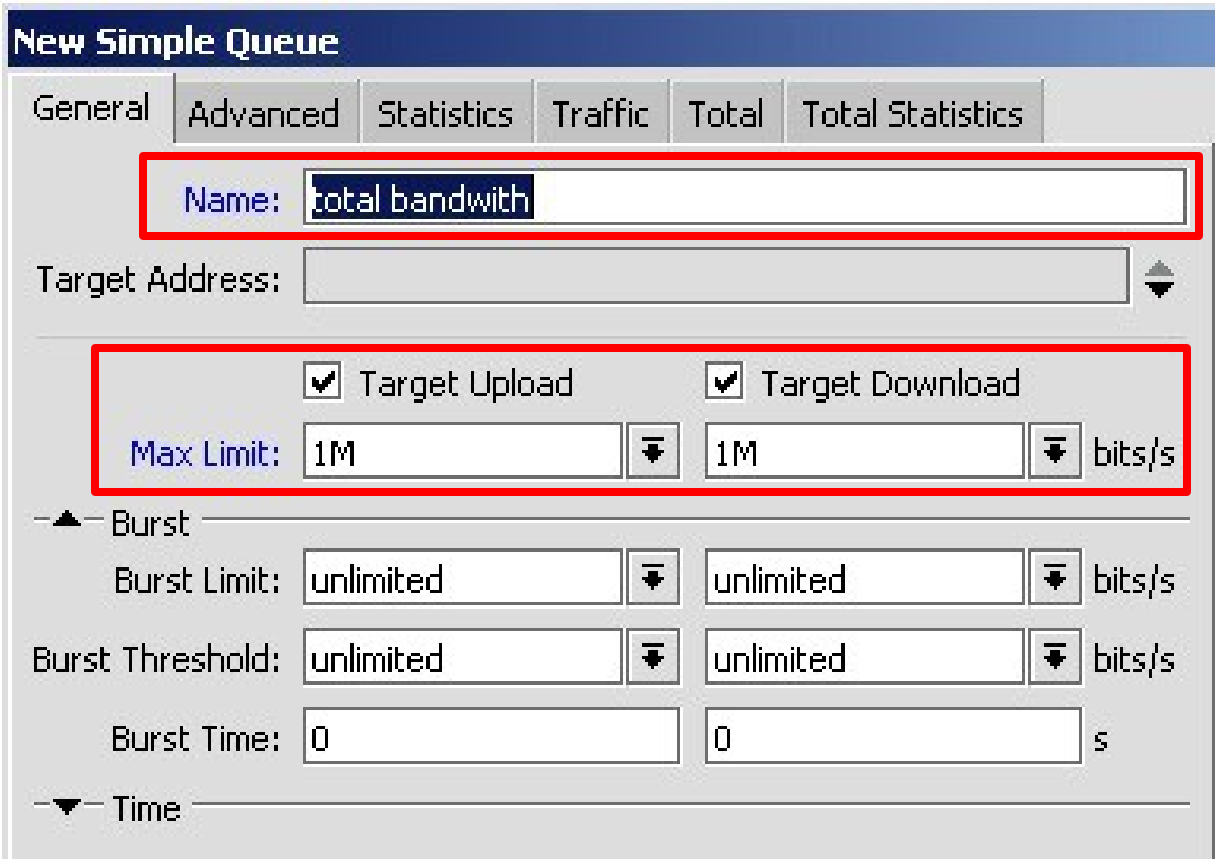
Staged Limitation - Example



- Bandwith share **1Mbps 1:4**

[LAB-3] Staged Queue - Parent

- Parent queue harus dibuat terlebih dahulu untuk membantu router menentukan Total bandwith yang dimiliki.



[LAB-3] Staged Queue - Child

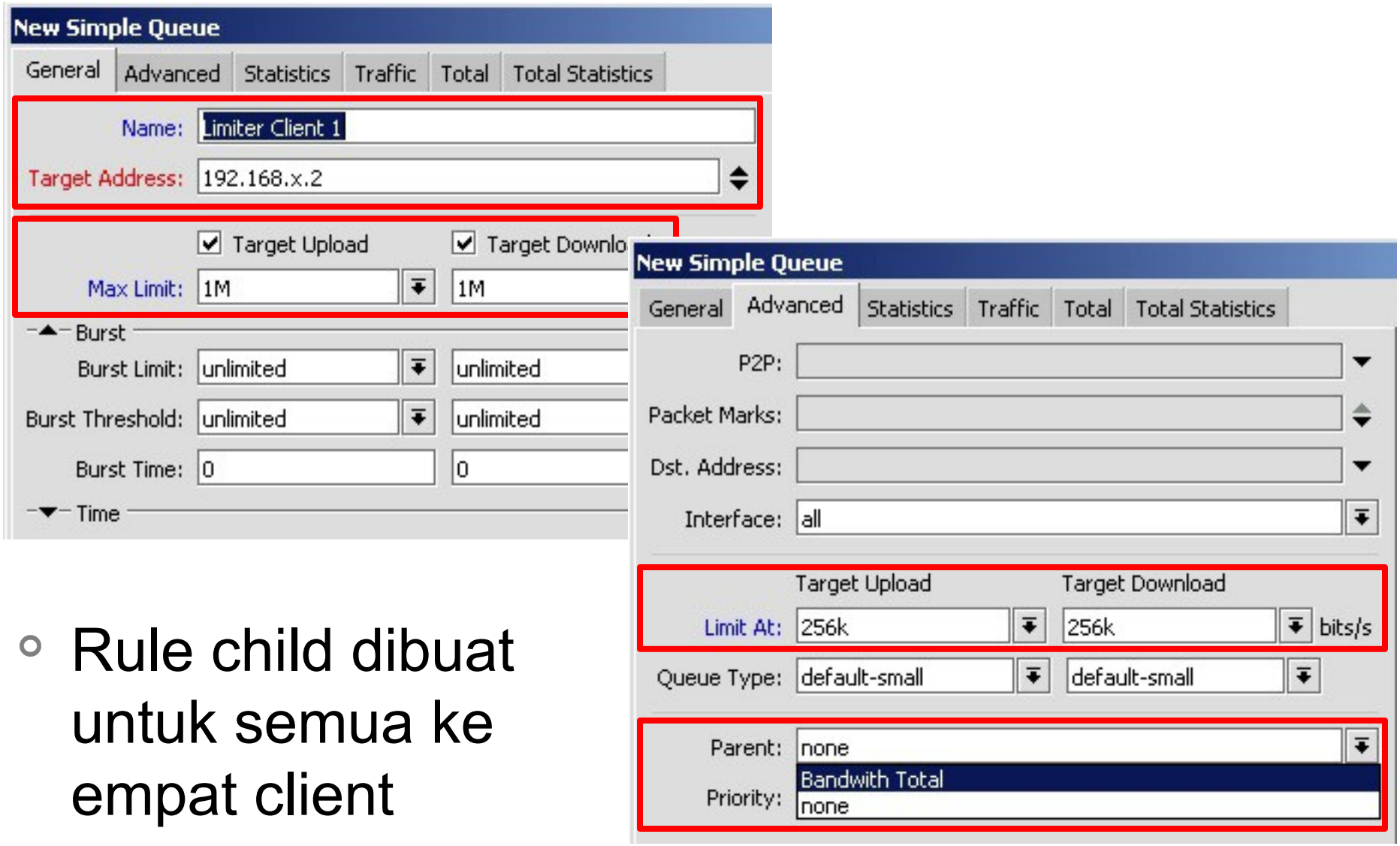
- Child queue baru dibuat untuk melimit tiap clientnya.
- Untuk pembagian bandwithnya adalah :
  - **Limit-At = Total Bandwith / Jumlah Client**
  - **Max-Limit = < Total Bandwith**

  - Jika jumlah client terlalu banyak maka bisa digunakan perhitungan :

  - **Limit-At = Total Bandwith / jumlah rata-rata maksimal client yang aktif**
  - **Max-Limit = TotalBandwith / jumlah rata-rata minimal client yang aktif**

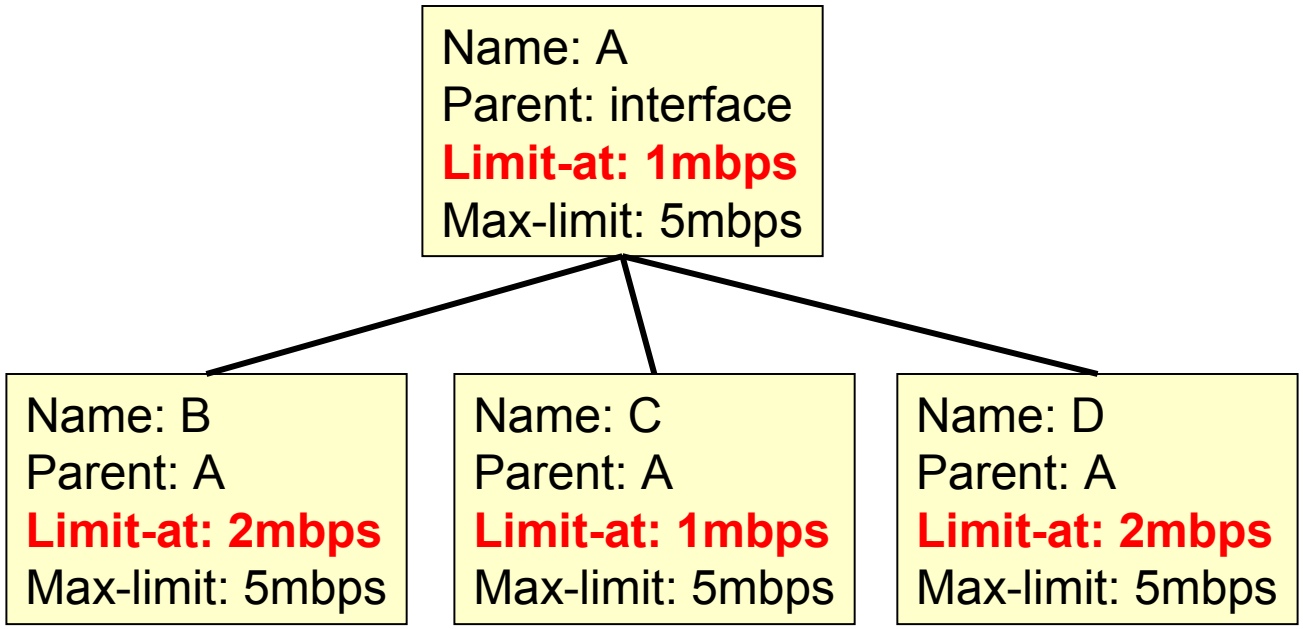
Name	Parent	Packet Mark	Priority	Limit At ...	Max Limit...	Avg. Rate
parent	ether3		8		400k	400.6 kbps
q1	parent	p1	3	75k	200k	133.5 kbps
q2	parent	p2	3	75k	200k	130.6 kbps
q3	parent	p3	3	75k	200k	136.4 kbps

[LAB-3] Staged Queue - Child

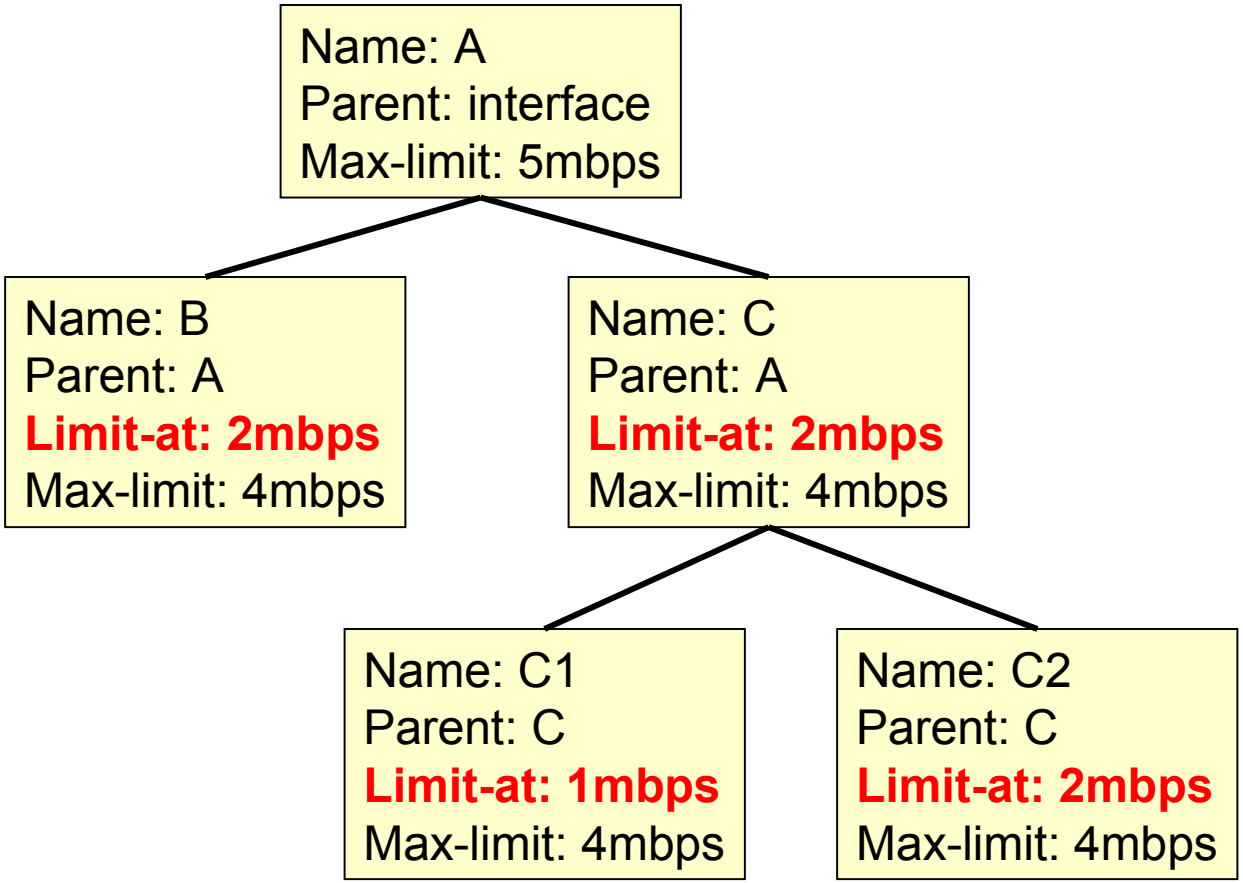


- Rule child dibuat untuk semua ke empat client

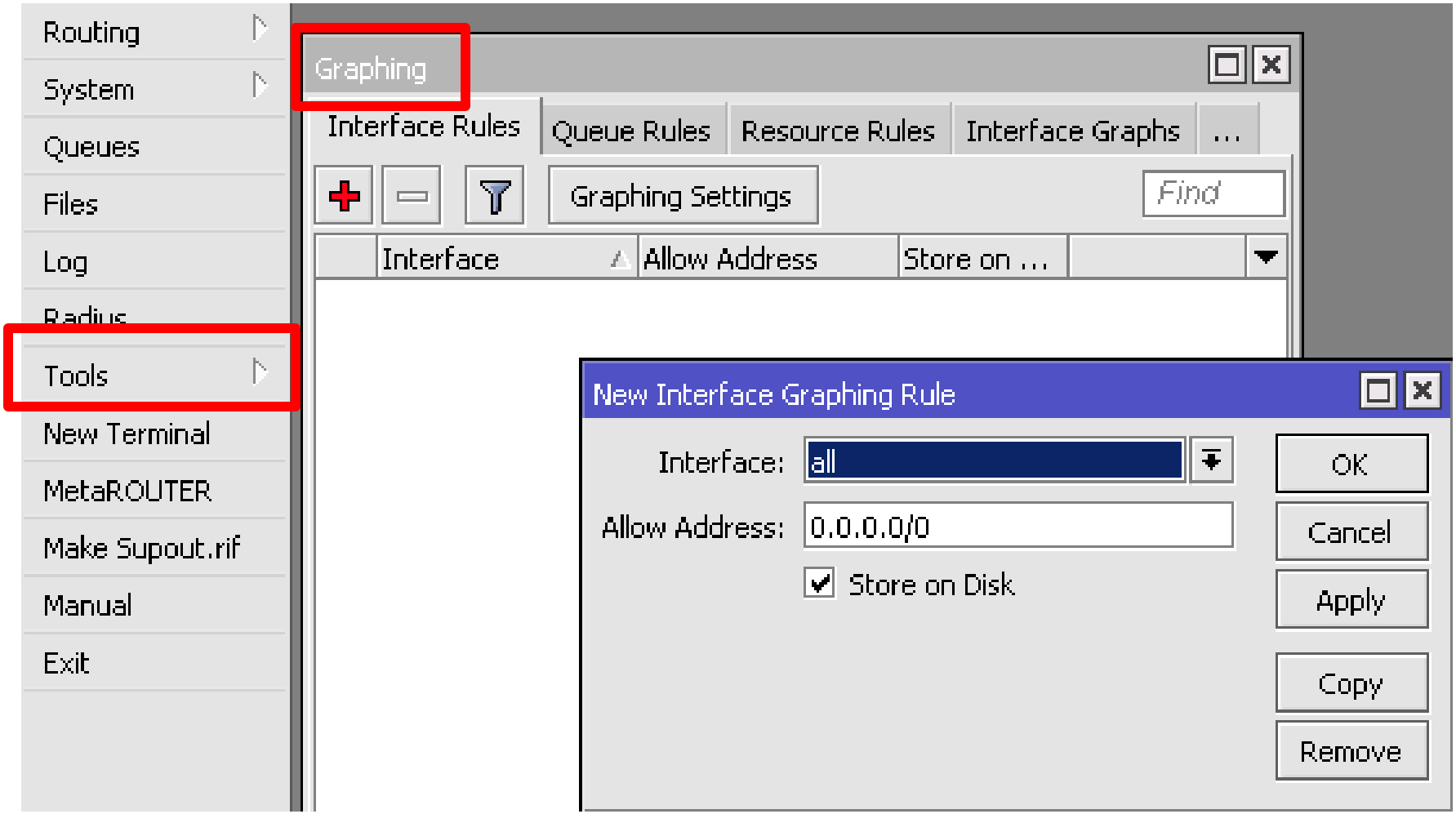
Contoh soal : 1



Contoh soal : 2



Using Mikrotik Graph



Graph

Mikrotik Router -> NAT-Lokal -> Graphing - Mozilla Firef

File Edit View Go Bookmarks Tools Help

http://192.16

Toko FN Donasi Mikrotik-IND Mikrotik Fotog

Traffic and system resou

You have access to 1 queue:

valens-test

You have access to 4 interfaces:

LAN
WAN
ether1
bridge1

Mikrotik Router -> NAT-Lokal -> Queue Traffic Graphing - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://19 Go

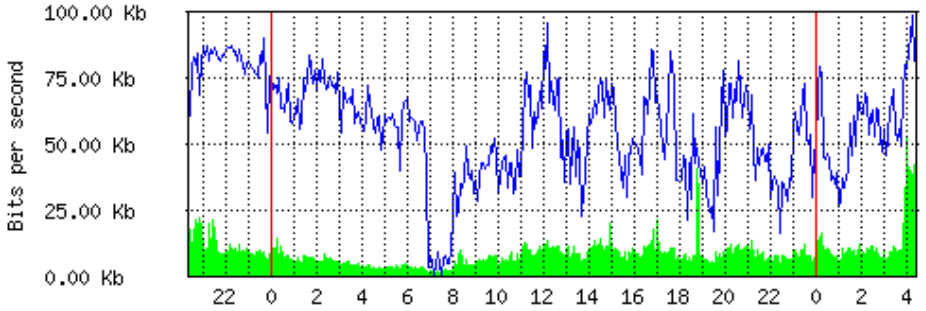
Toko FN Donasi Mikrotik-IND Mikrotik Fotografer.Net KlikBCA

Queue Statistics

valens-test

Source-address: 192.168.0.4/32
Destination-address: 0.0.0.0/0
Max-limit: 96.00 Kb/64.00 Kb (Total: *unlimited*)
Limit-at: 64.00 Kb/32.00 Kb (Total: *unlimited*)
Last update: Tue Dec 13 04:21:11 2005

"Daily" Graph (5 Minute Average)

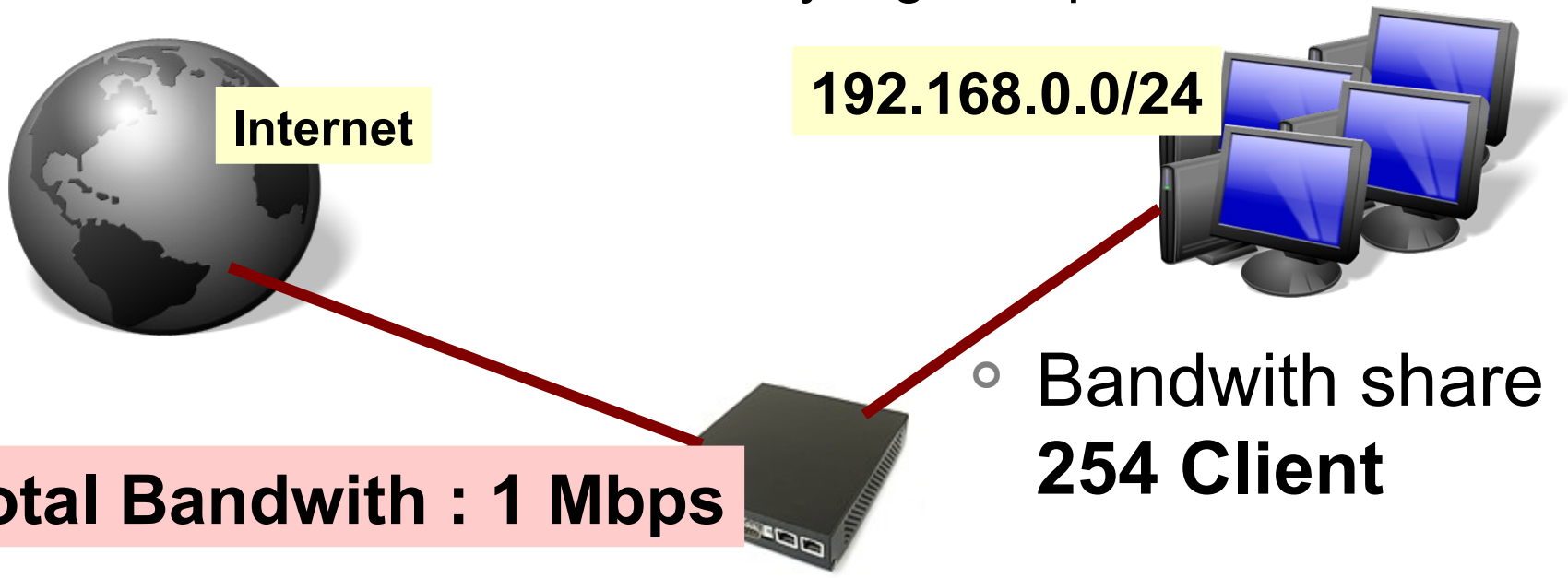


Max In: 67.01 Kb (104.7%) Average In: 66.39 Kb (103.7%) Current In: 66.73 Kb (104.3%)
Max Out: 94.32 Kb (98.2%) Average Out: 90.59 Kb (94.4%) Current Out: 91.06 Kb (94.9%)

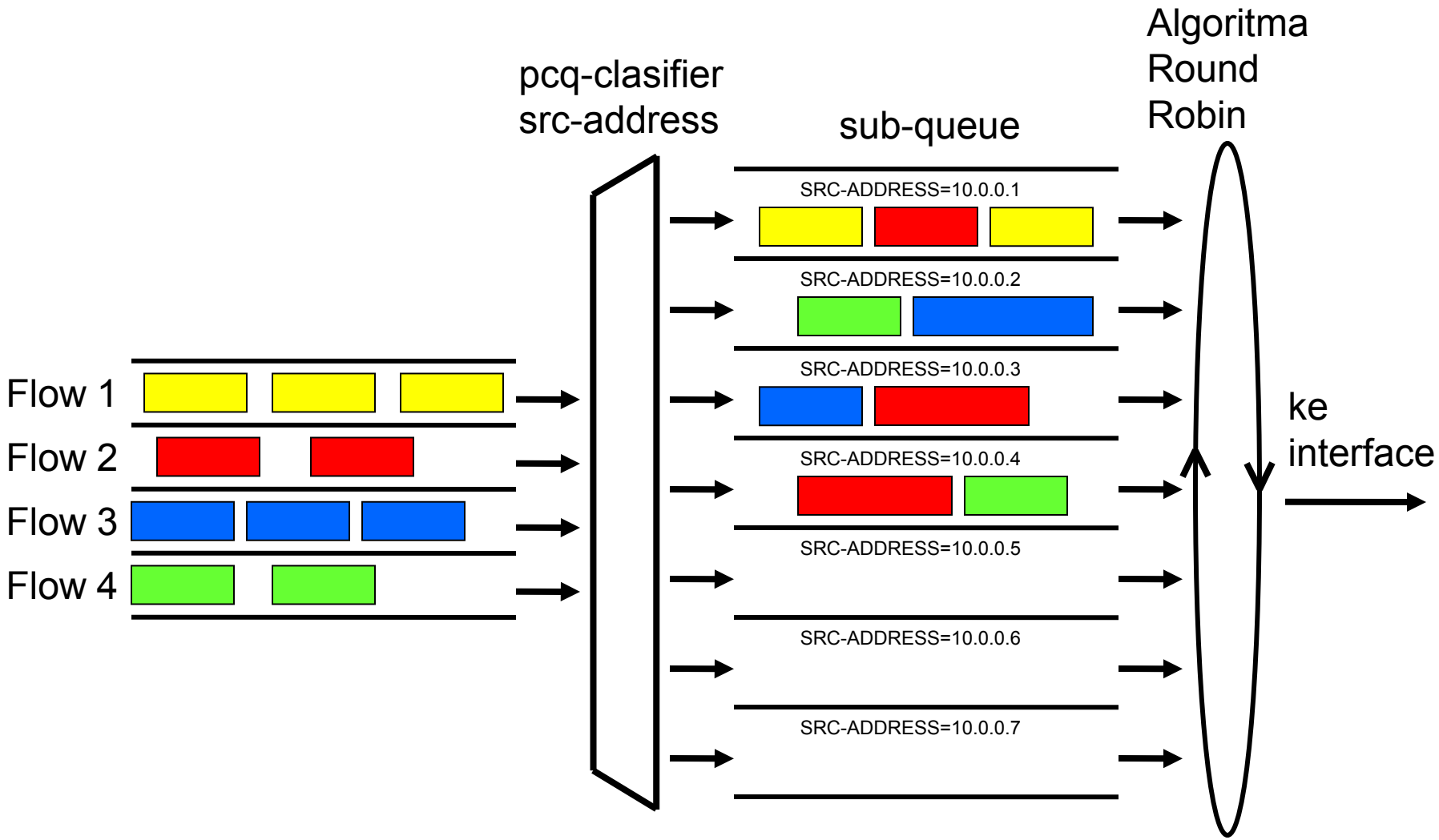
"Weekly" Graph (30 Minute Average)

PCQ (Per Connection Queue)

- Untuk kondisi client yang sangat banyak dan sangat merepotkan jika harus membuat banyak rule maka bisa menggunakan metode PCQ :
  - PCQ dibuat sebagai penyempurnaan SFQ.
  - PCQ bisa **membatasi bandwith client secara merata**
  - PCQ membutuhkan memori yang cukup besar

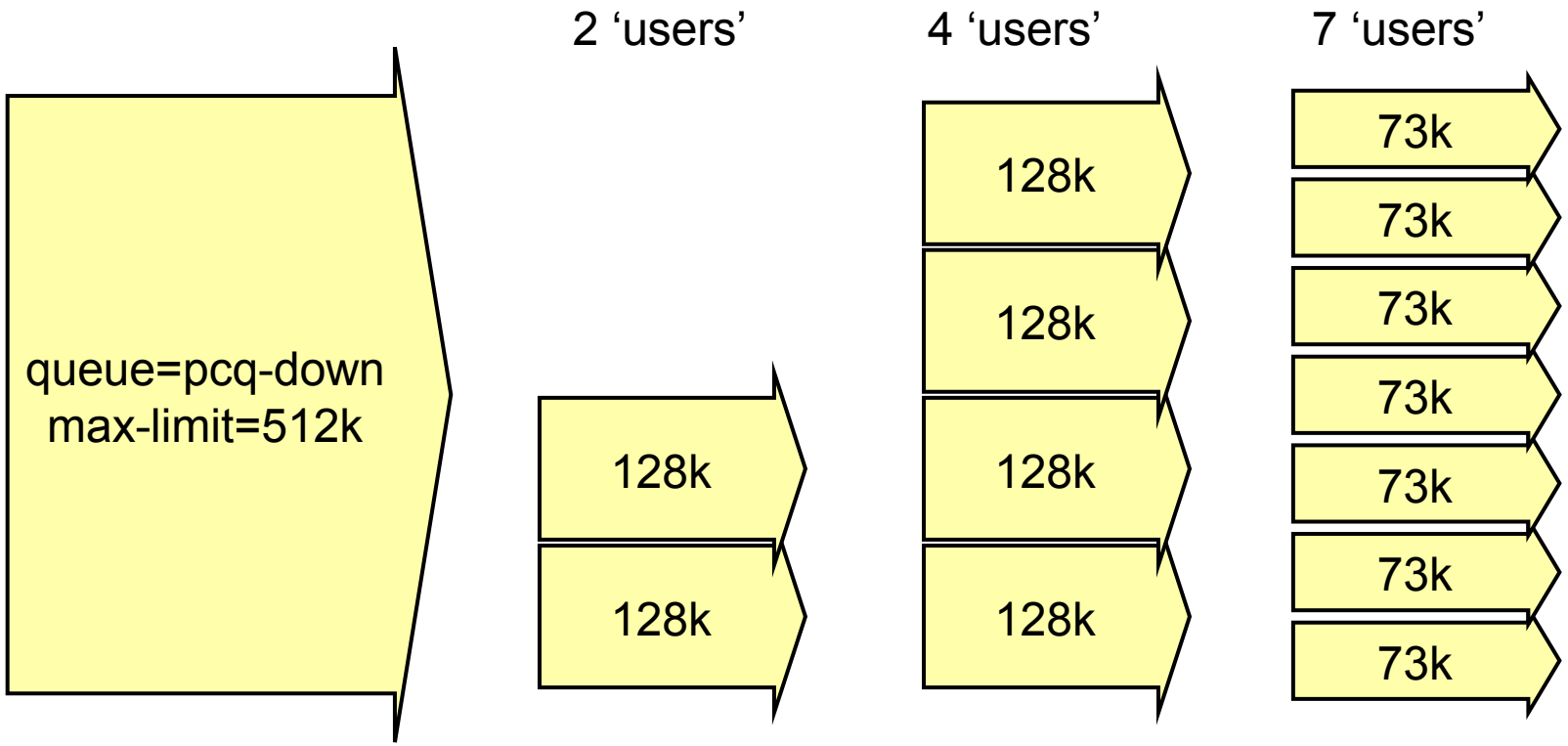


Skema PCQ


Algoritma
Round
Robin
pcq-clasifier
src-address
sub-queue
SRC-ADDRESS=10.0.0.1
SRC-ADDRESS=10.0.0.2
SRC-ADDRESS=10.0.0.3
SRC-ADDRESS=10.0.0.4
SRC-ADDRESS=10.0.0.5
SRC-ADDRESS=10.0.0.6
SRC-ADDRESS=10.0.0.7
Flow 1
Flow 2
Flow 3
Flow 4
ke
interface

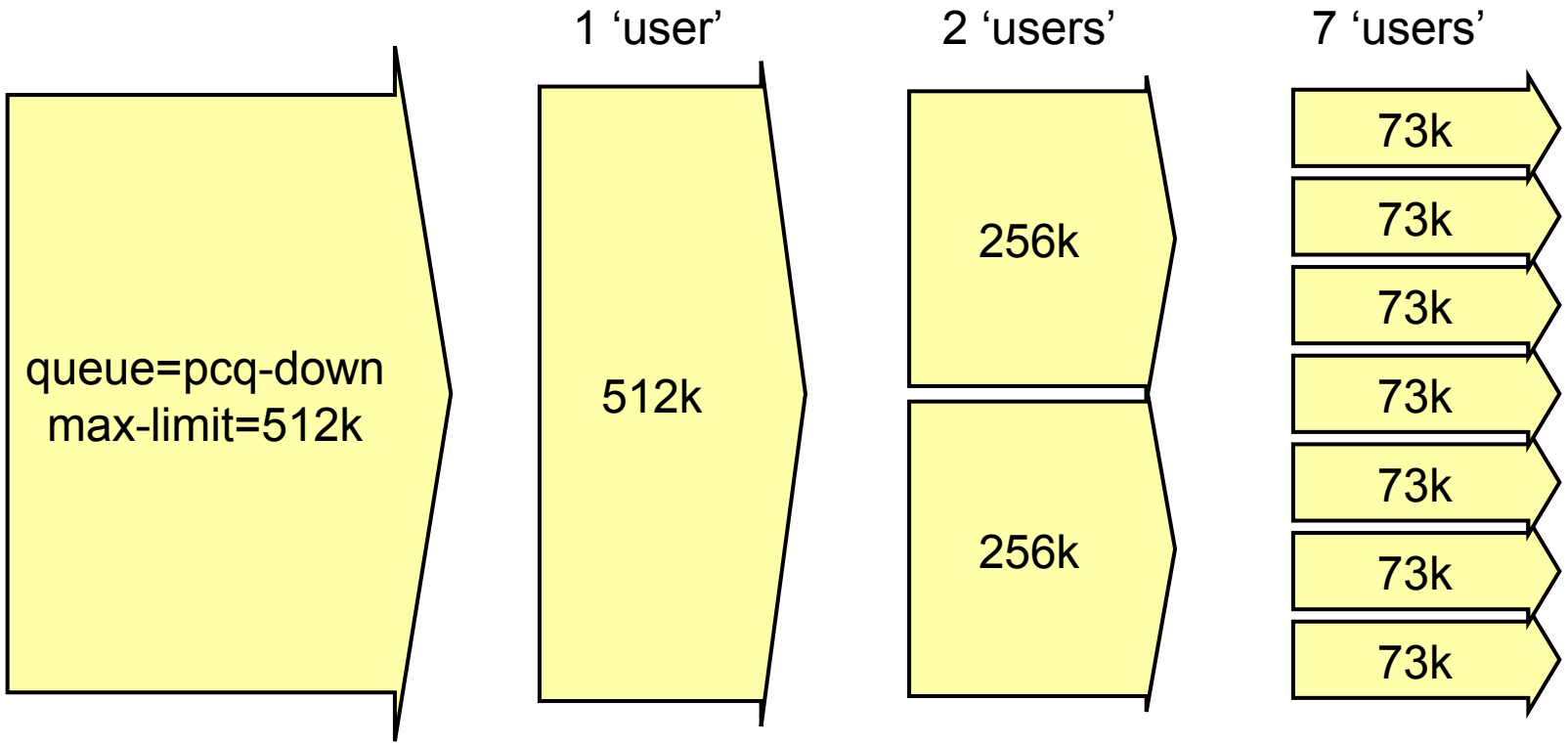
PCQ in Action (1)

- Pcq-rate=128000

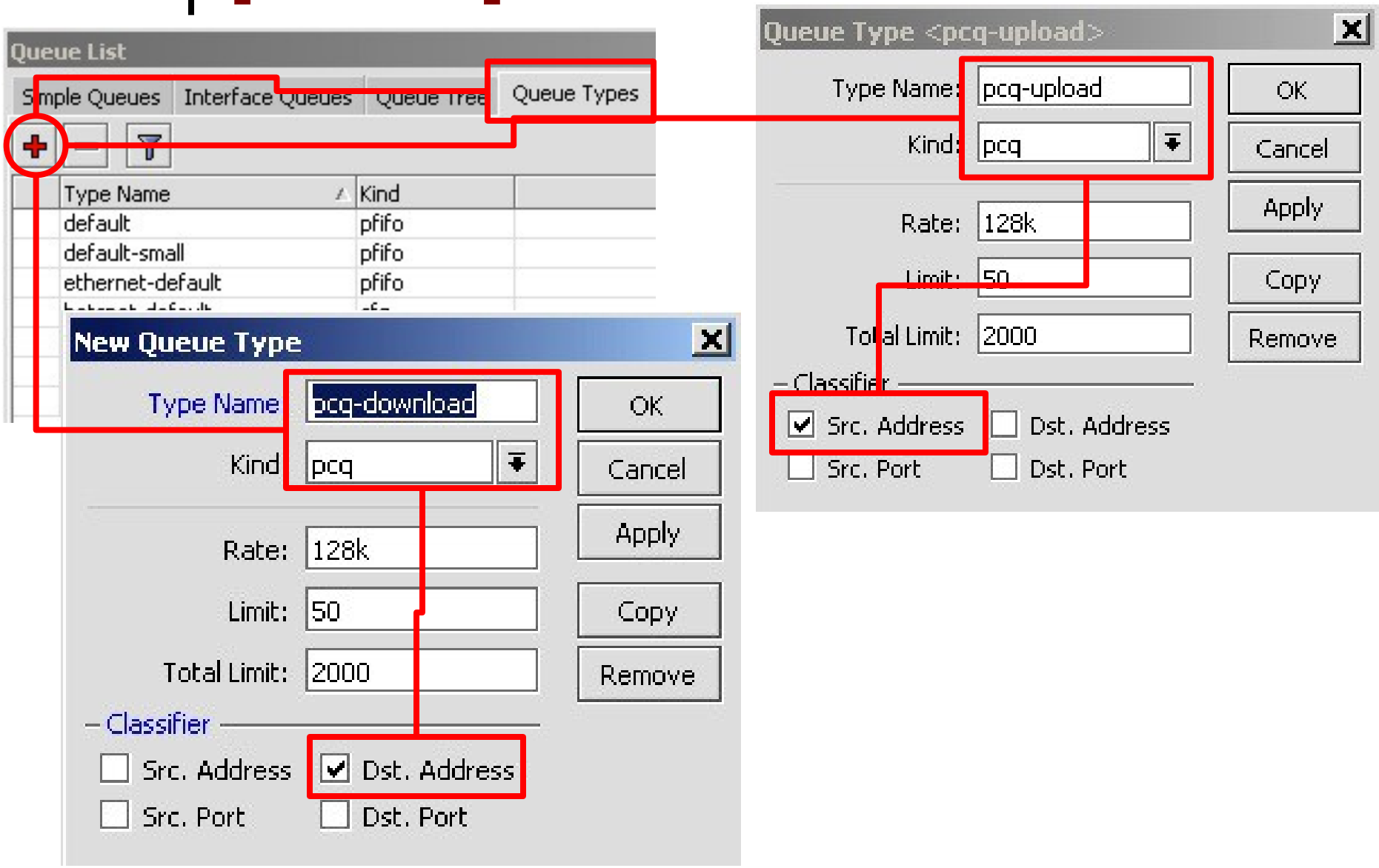


PCQ in Action (2)

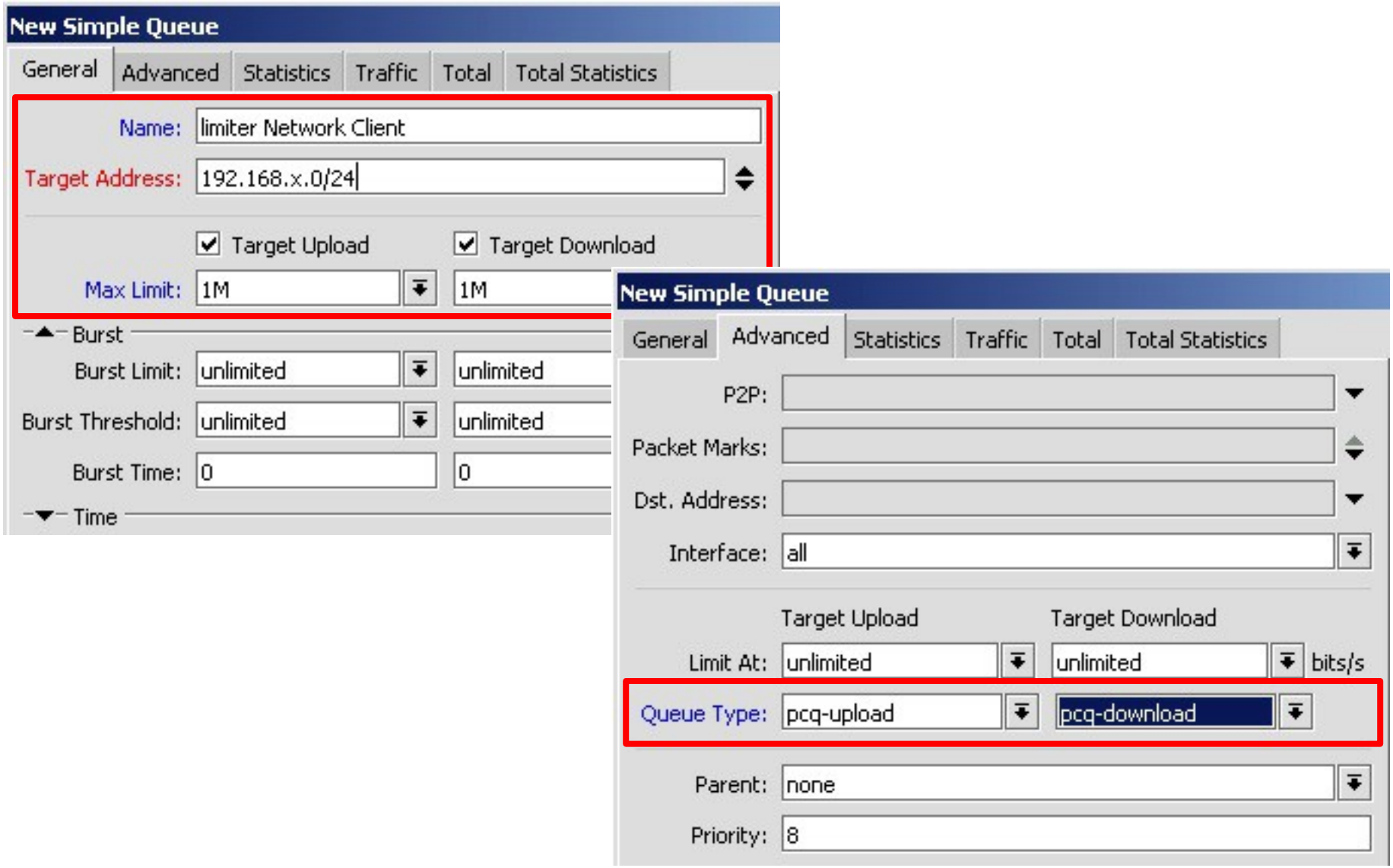
- Pcq-rate=0



[LAB-4] Queue Kind - PCQ



[LAB-4] Queue Kind - PCQ



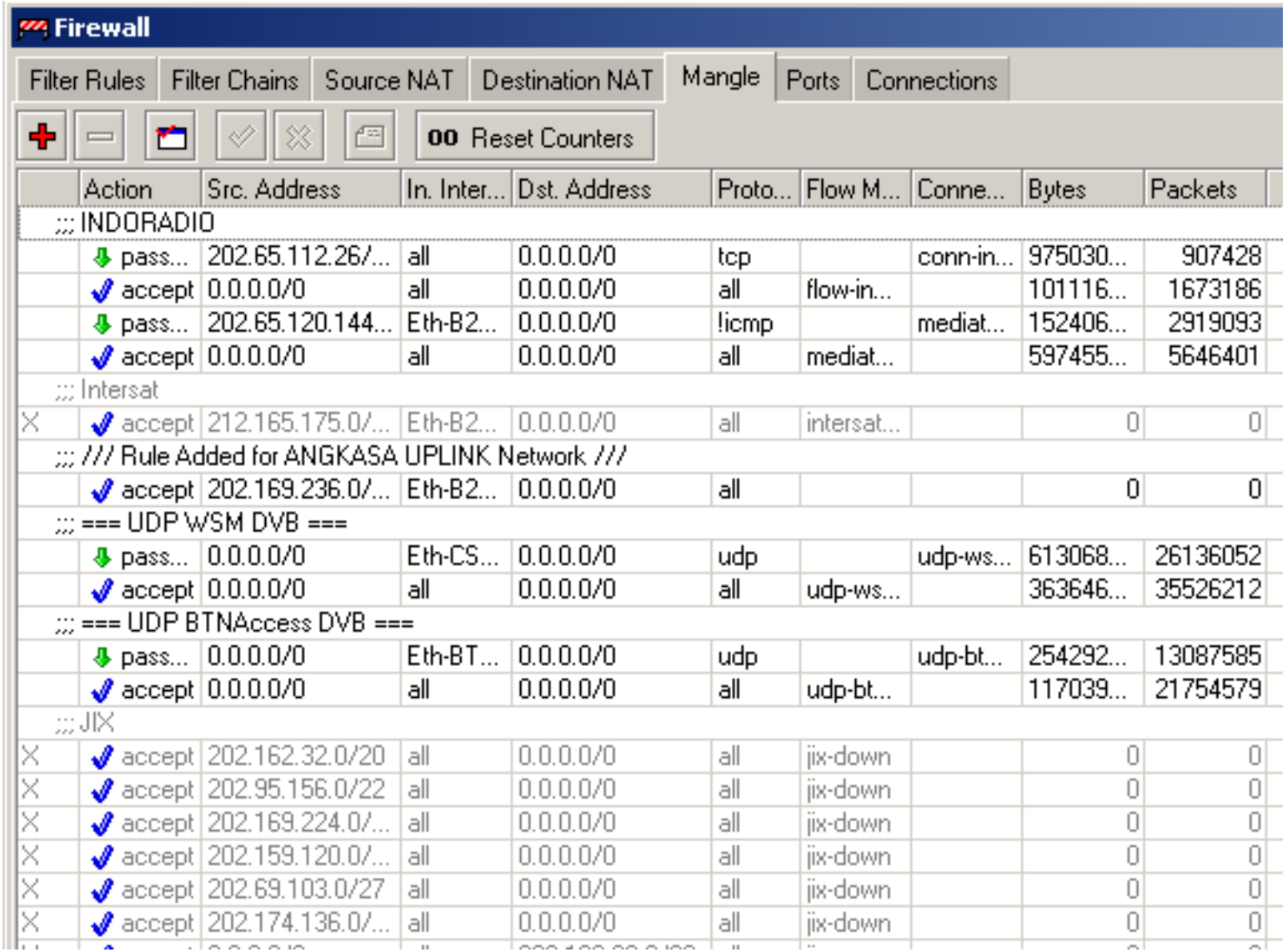
Queue Tree & Mangle

- QueueTree adalah tool mikrotik yang memiliki kemampuan melimitasi bandwith yang lebih lengkap dibandingkan dengan simple-queue.
- Dengan QueueTree memungkinkan untuk melakukan limitasi yang lebih fleksible karena supaya QueueTree bisa berfungsi maka harus menggunakan Mangle terlebih dahulu.

Mangle

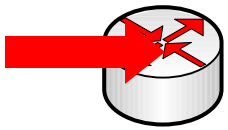
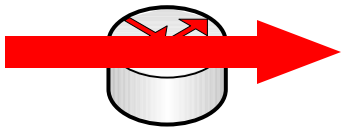
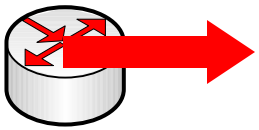
- Mangle adalah cara untuk menandai paket-paket data tertentu, dan kita akan menggunakan tanda tersebut pada fitur lainnya, misalnya pada filter, routing, NAT, ataupun queue.
- Pada mangle kita juga bisa melakukan pengubahan beberapa parameter pada IP Header, misalnya TOS (DSCP) dan TTL fields.
- Tanda mangle ini hanya bisa digunakan pada router yang sama, dan tidak terbaca pada router lainnya.
- Pembacaan rule mangle akan dilakukan dari atas ke bawah secara berurutan.

Mangle on Winbox - Example



	Action	Src. Address	In. Inter...	Dst. Address	Proto...	Flow M...	Conne...	Bytes	Packets
;;; INDORADIO									
	pass...	202.65.112.26/...	all	0.0.0.0/0	tcp		conn-in...	975030...	907428
	accept	0.0.0.0/0	all	0.0.0.0/0	all	flow-in...		101116...	1673186
	pass...	202.65.120.144...	Eth-B2...	0.0.0.0/0	!icmp		mediat...	152406...	2919093
	accept	0.0.0.0/0	all	0.0.0.0/0	all	mediat...		597455...	5646401
;;; Intersat									
X	accept	212.165.175.0/...	Eth-B2...	0.0.0.0/0	all	intersat...		0	0
;;; /// Rule Added for ANGKASA UPLINK Network ///									
	accept	202.169.236.0/...	Eth-B2...	0.0.0.0/0	all			0	0
;;; === UDP WSM DVB ===									
	pass...	0.0.0.0/0	Eth-CS...	0.0.0.0/0	udp		udp-ws...	613068...	26136052
	accept	0.0.0.0/0	all	0.0.0.0/0	all	udp-ws...		363646...	35526212
;;; === UDP BTNAccess DVB ===									
	pass...	0.0.0.0/0	Eth-BT...	0.0.0.0/0	udp		udp-bt...	254292...	13087585
	accept	0.0.0.0/0	all	0.0.0.0/0	all	udp-bt...		117039...	21754579
;;; JIX									
X	accept	202.162.32.0/20	all	0.0.0.0/0	all	jix-down		0	0
X	accept	202.95.156.0/22	all	0.0.0.0/0	all	jix-down		0	0
X	accept	202.169.224.0/...	all	0.0.0.0/0	all	jix-down		0	0
X	accept	202.159.120.0/...	all	0.0.0.0/0	all	jix-down		0	0
X	accept	202.69.103.0/27	all	0.0.0.0/0	all	jix-down		0	0
X	accept	202.174.136.0/...	all	0.0.0.0/0	all	jix-down		0	0

Chain pada mangle

			
Prerouting	yes	yes	no
Input	yes	no	no
Forward	no	yes	no
Output	no	no	yes
Postrouting	no	yes	yes

Type of Mark

- Packet Mark
  - Penandaan untuk setiap paket data
- Connection Mark
  - Penandaan untuk koneksi
- Route Mark
  - Penandaan paket khusus untuk routing

Pada saat yang bersamaan, setiap paket data hanya bisa memiliki 1 conn-mark, 1 packet-mark, dan 1 route-mark

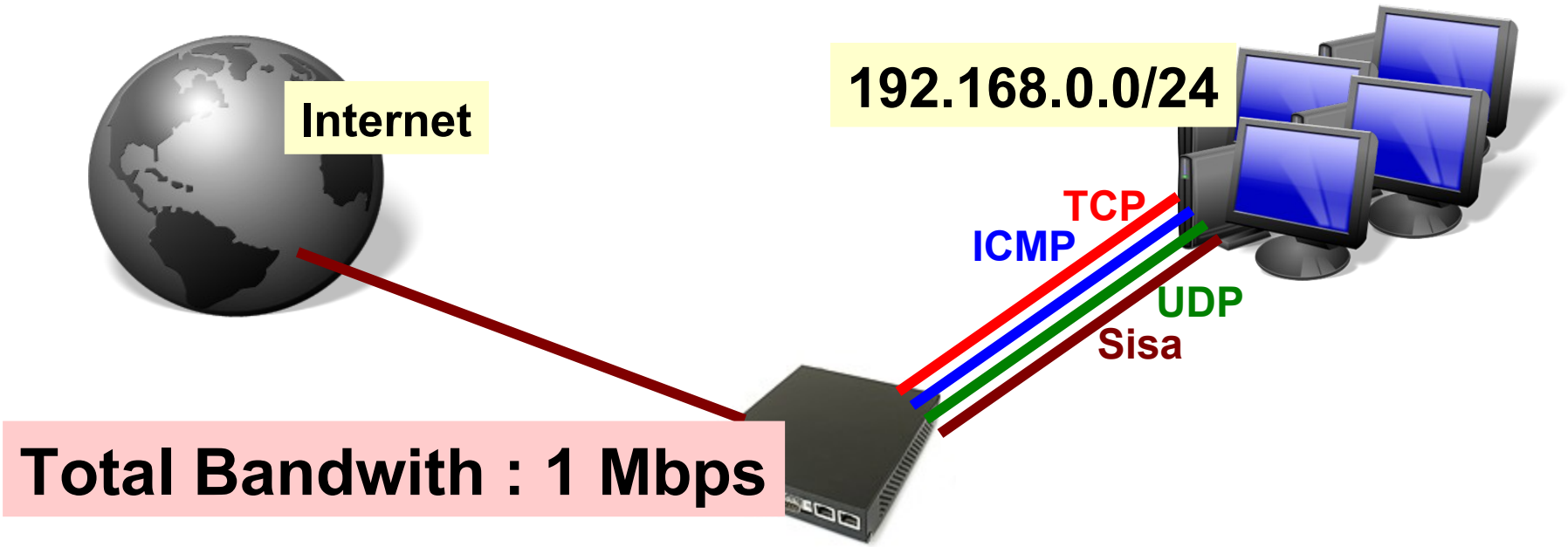
Connection Mark

- Adalah fitur mangle untuk menandai suatu koneksi (berlaku baik untuk request, maupun untuk response) sebagai satu kesatuan
- Untuk jaringan dengan src-nat atau kalau kita mau melakukan marking berdasarkan protokol tcp, disarankan untuk melakukan mark-connection terlebih dahulu, baru membuat mark-packet atau mark-routing berdasarkan conn-mark nya
- Mark-connection cukup dibuat pada saat proses request saja.

Passthrough

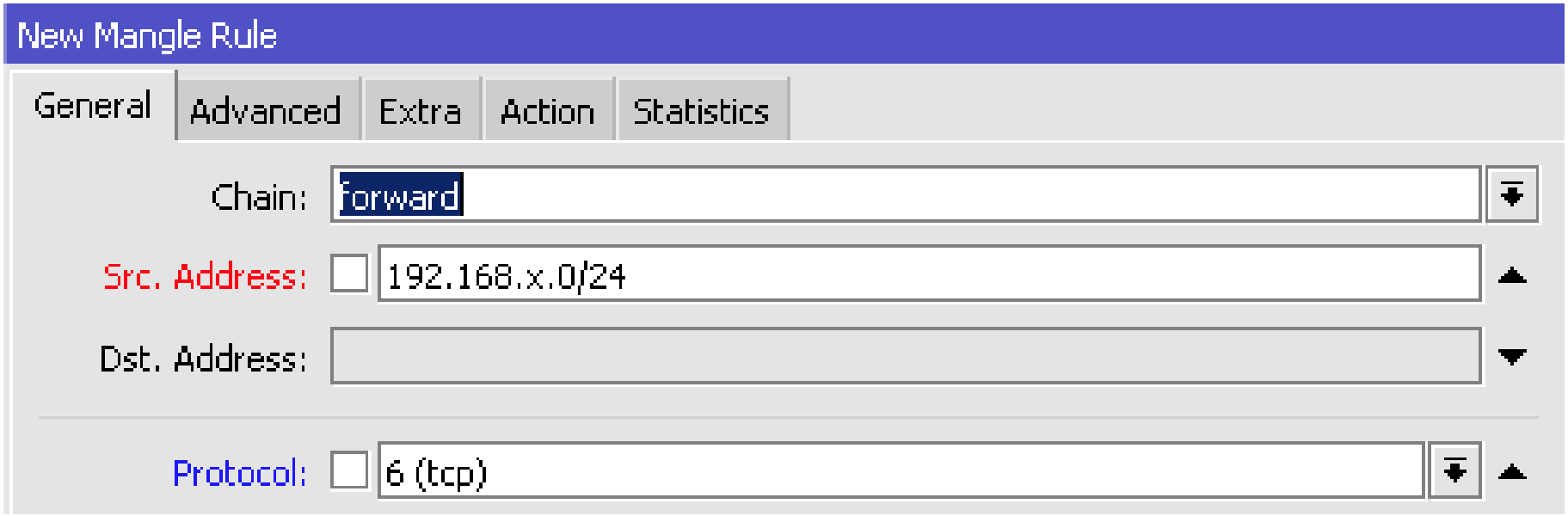
- Passthrough=no
  - berarti jika parameter sesuai, maka baris mangle berikutnya tidak lagi dibaca
  - value mangle sudah final, tidak diubah lagi
- Passthrough=yes
  - akan tetap membaca baris mangle berikutnya
  - value mangle bisa diubah lagi di baris berikutnya
- Biasanya pada :
  - mark-connection, passthrough = yes
  - mark-packet, passthrough=no

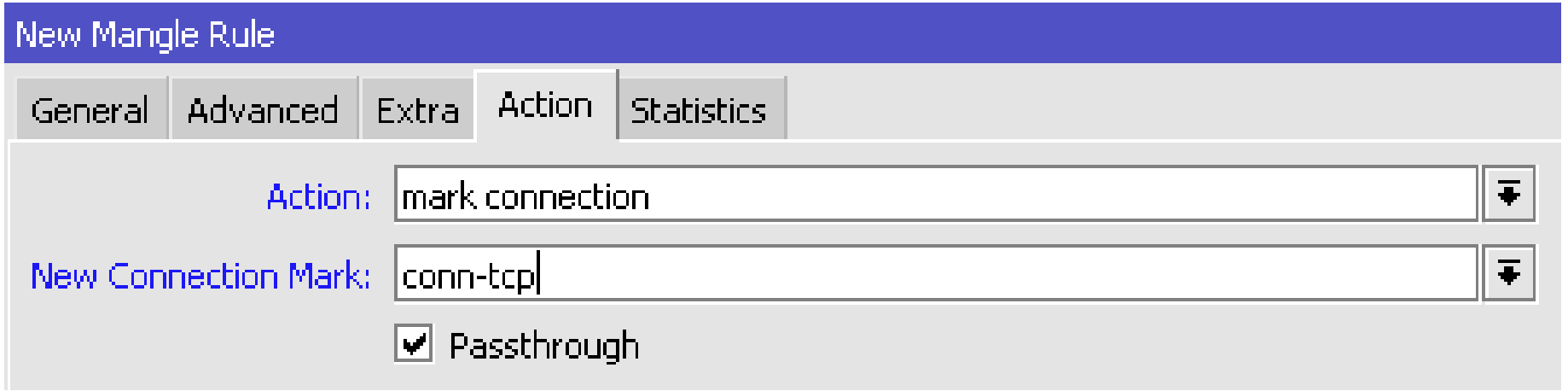
[LAB-5] QueueTree & Mangle



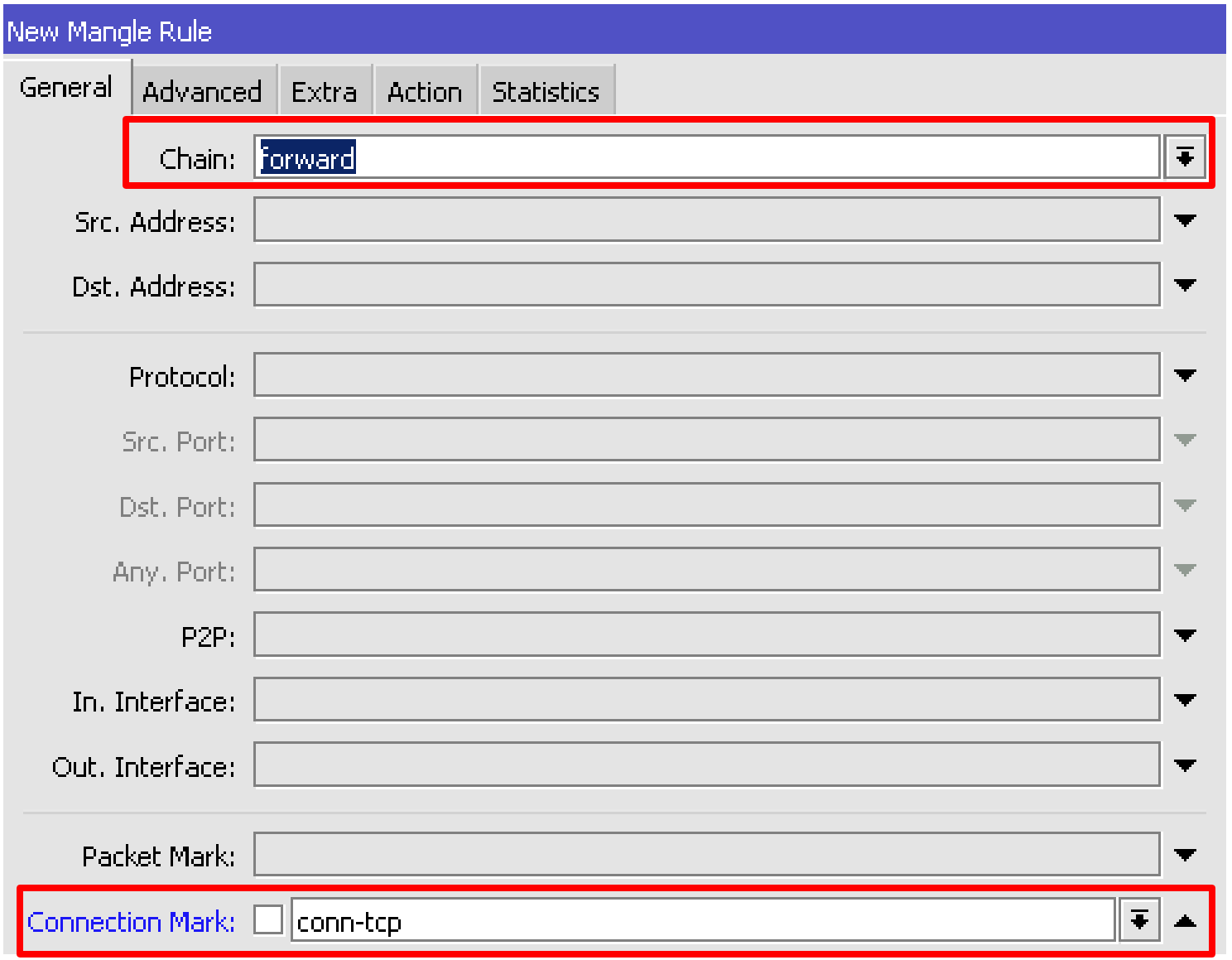
- Lakukan limitasi traffic dari client sekaligus dengan memisahkan type trafficnya.

Mark Connection - TCP

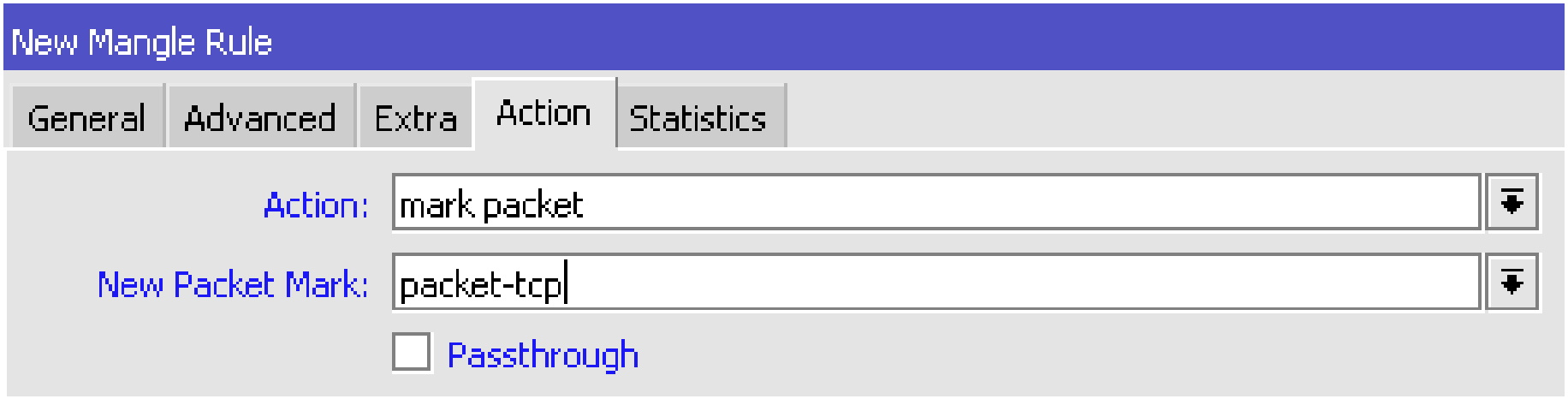




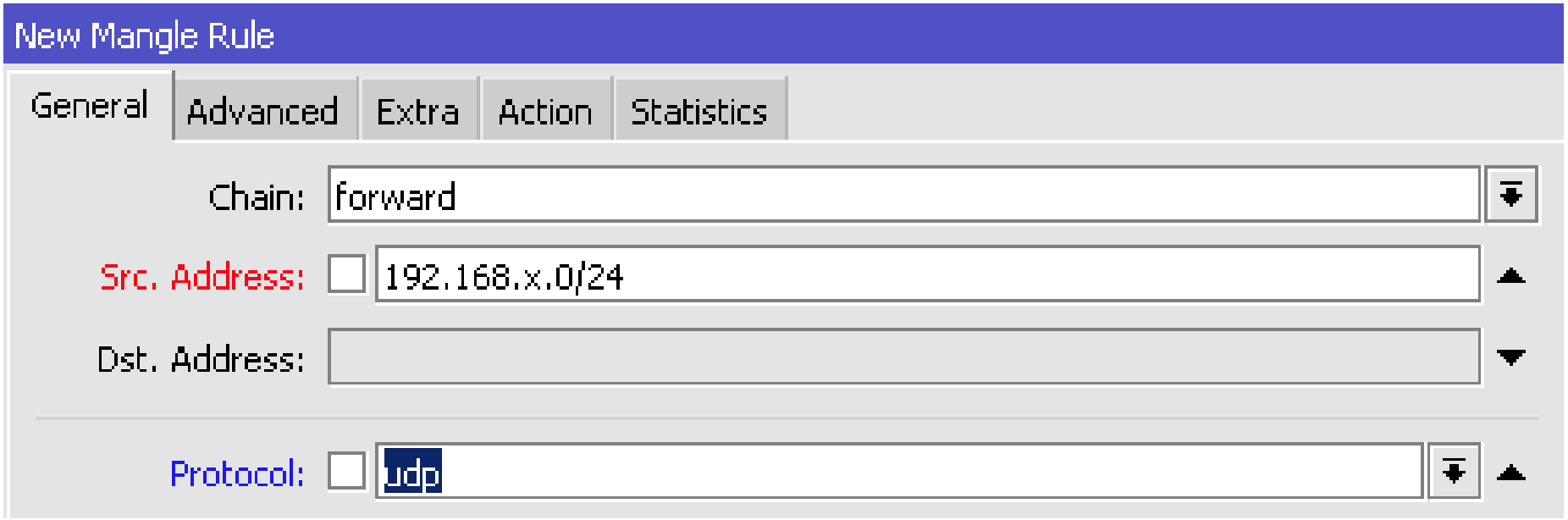
Mark Packet – TCP

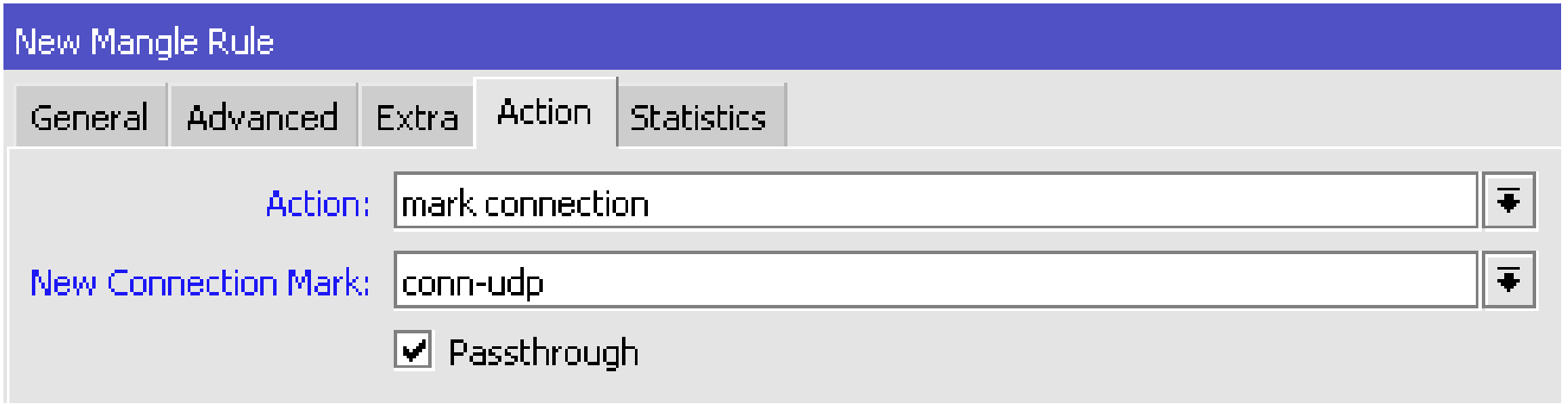


Mark Packet - TCP

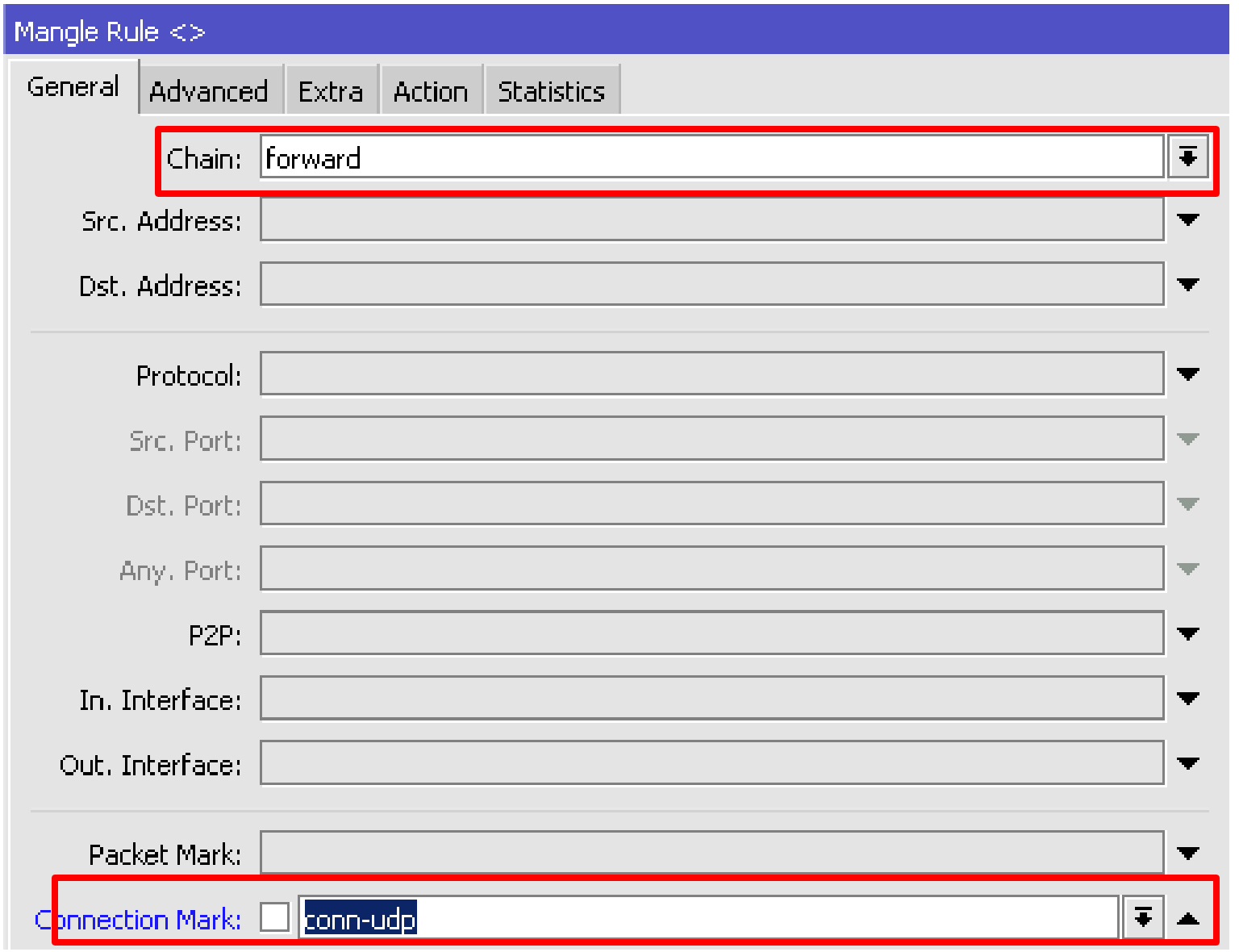


Mark Connection - UDP

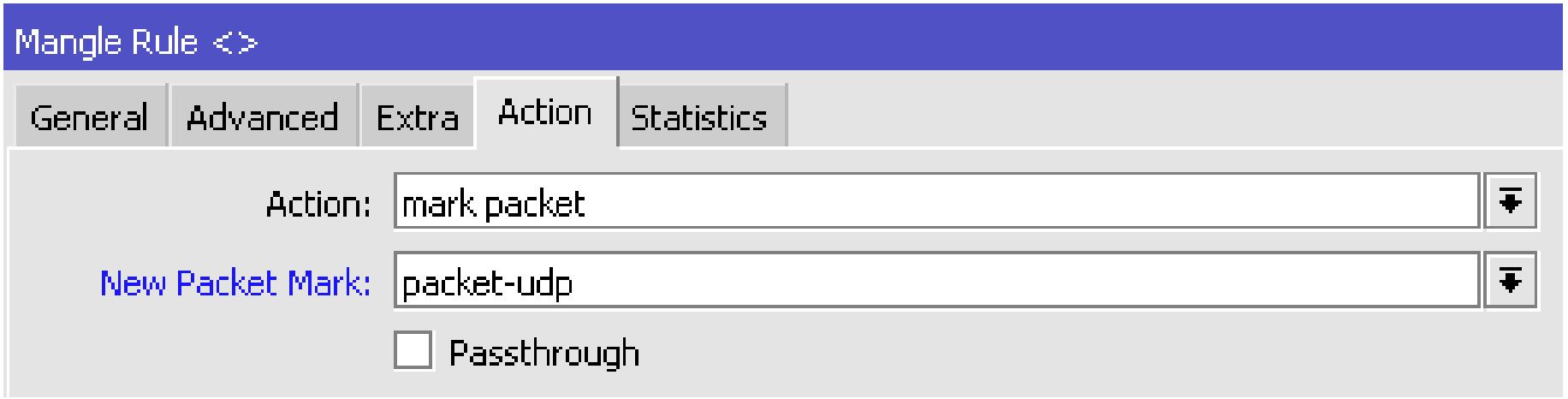




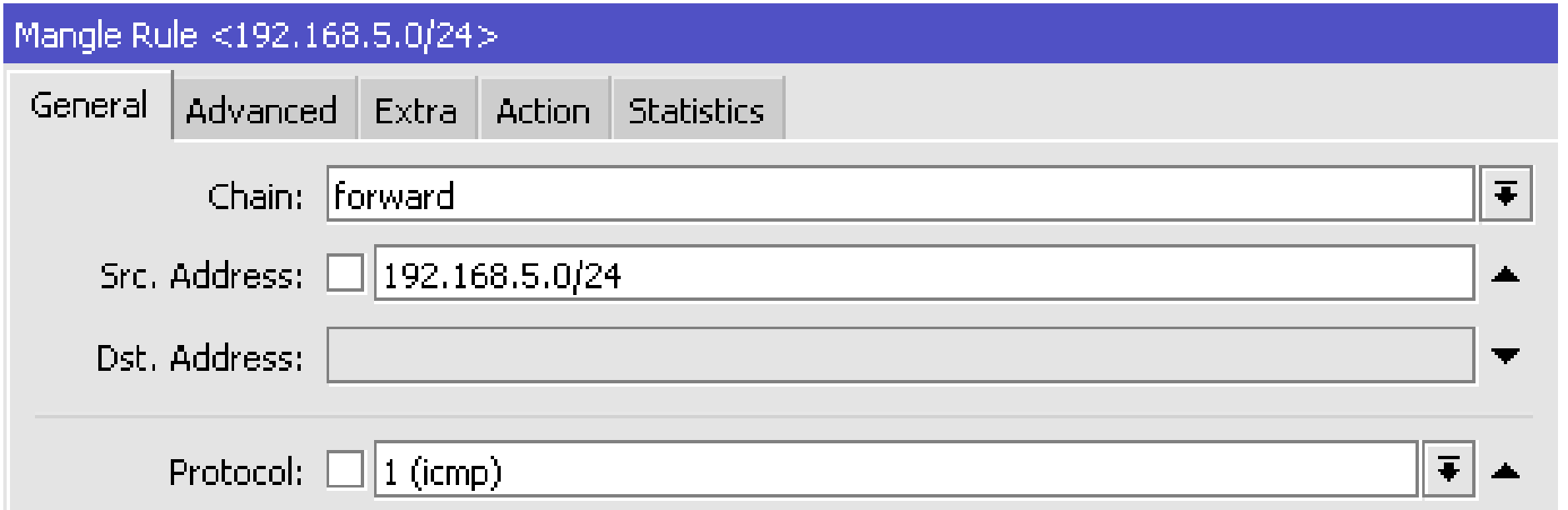
Mark Packet - UDP

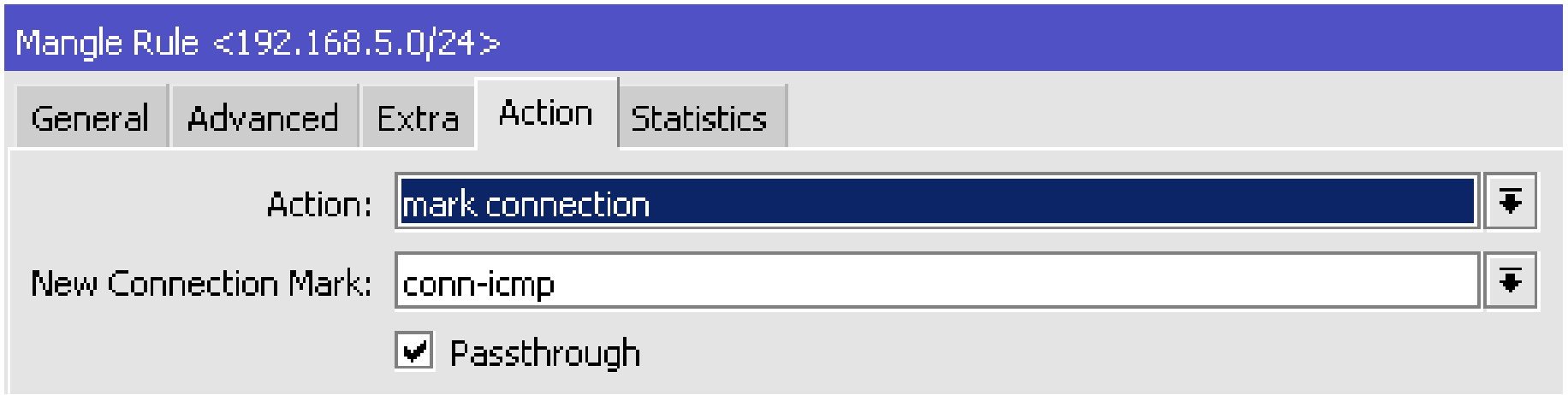


Mark Packet - UDP

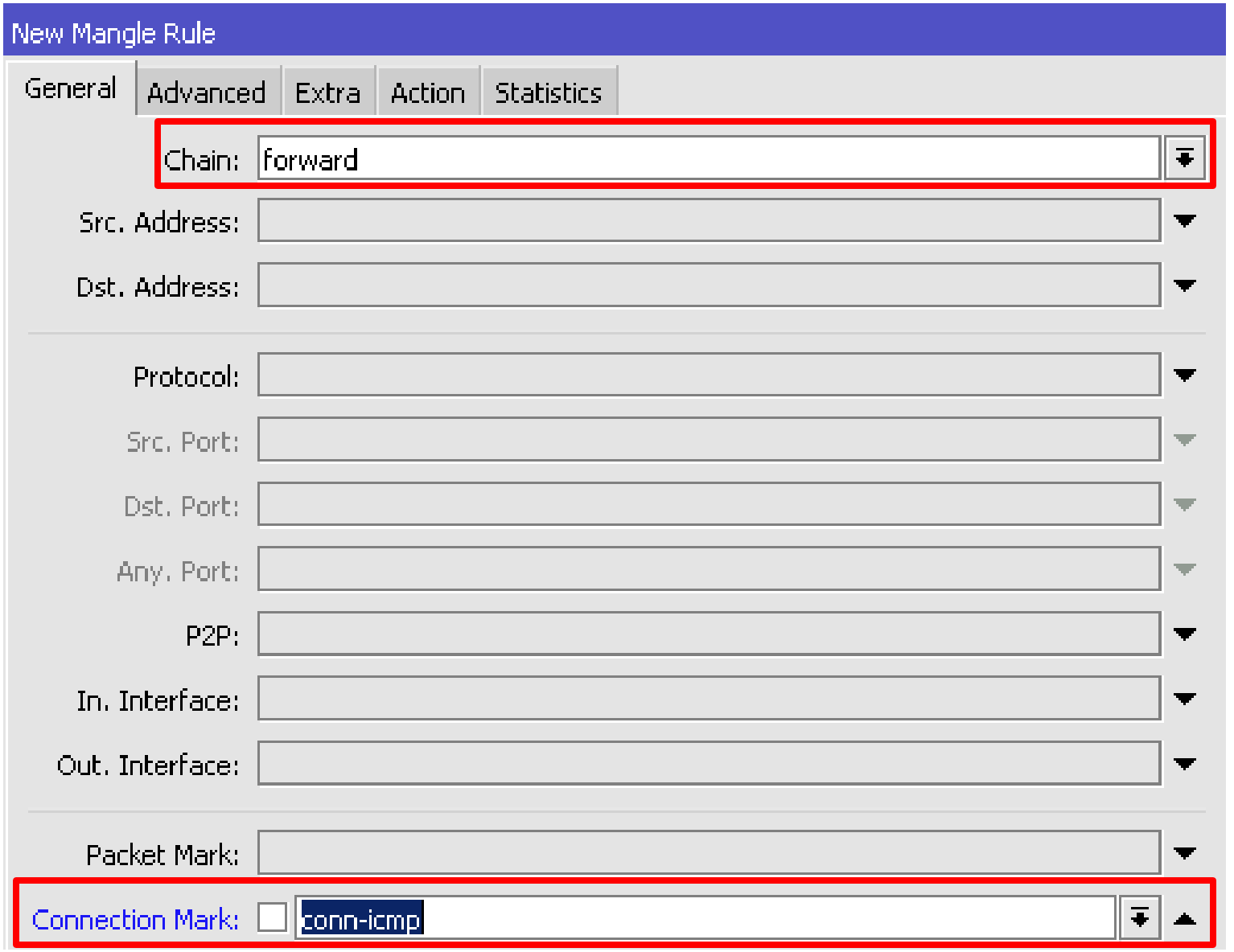


Mark Connection - ICMP

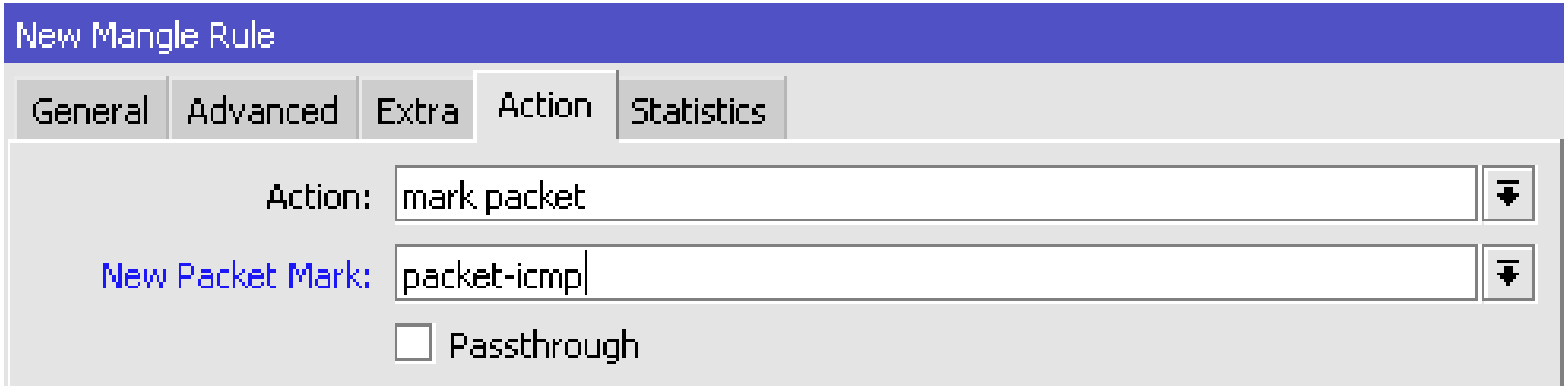




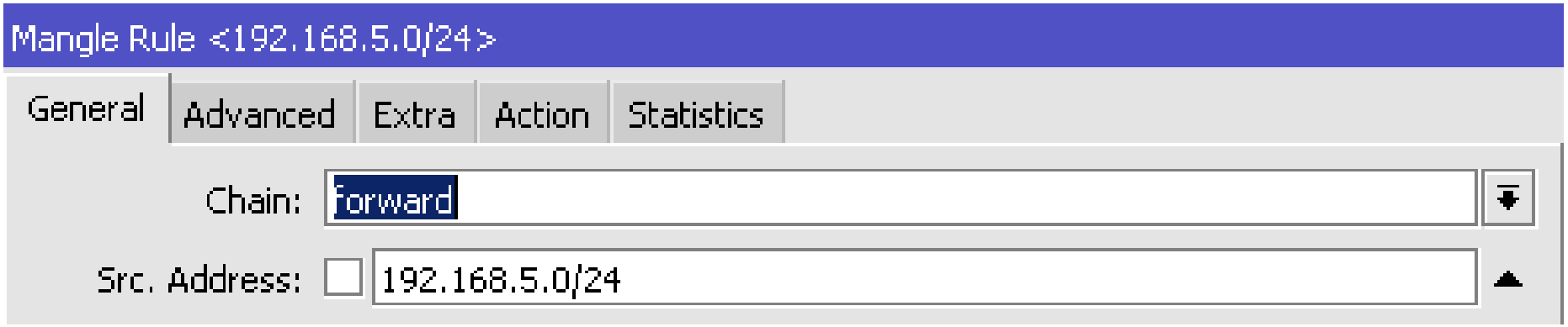
Mark Packet - ICMP

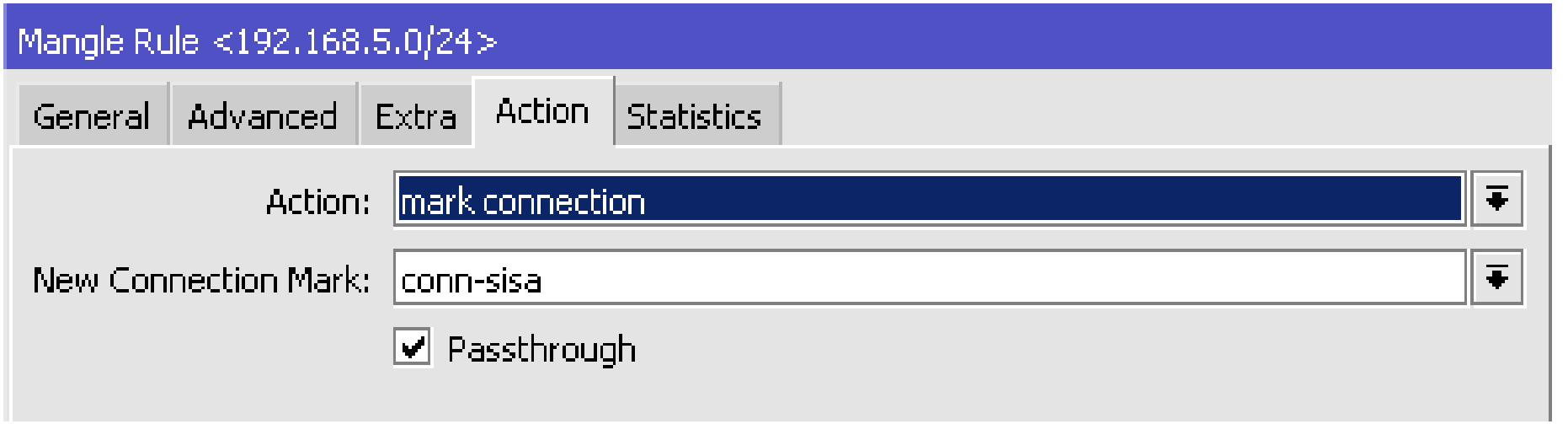


Mark Packet - ICMP

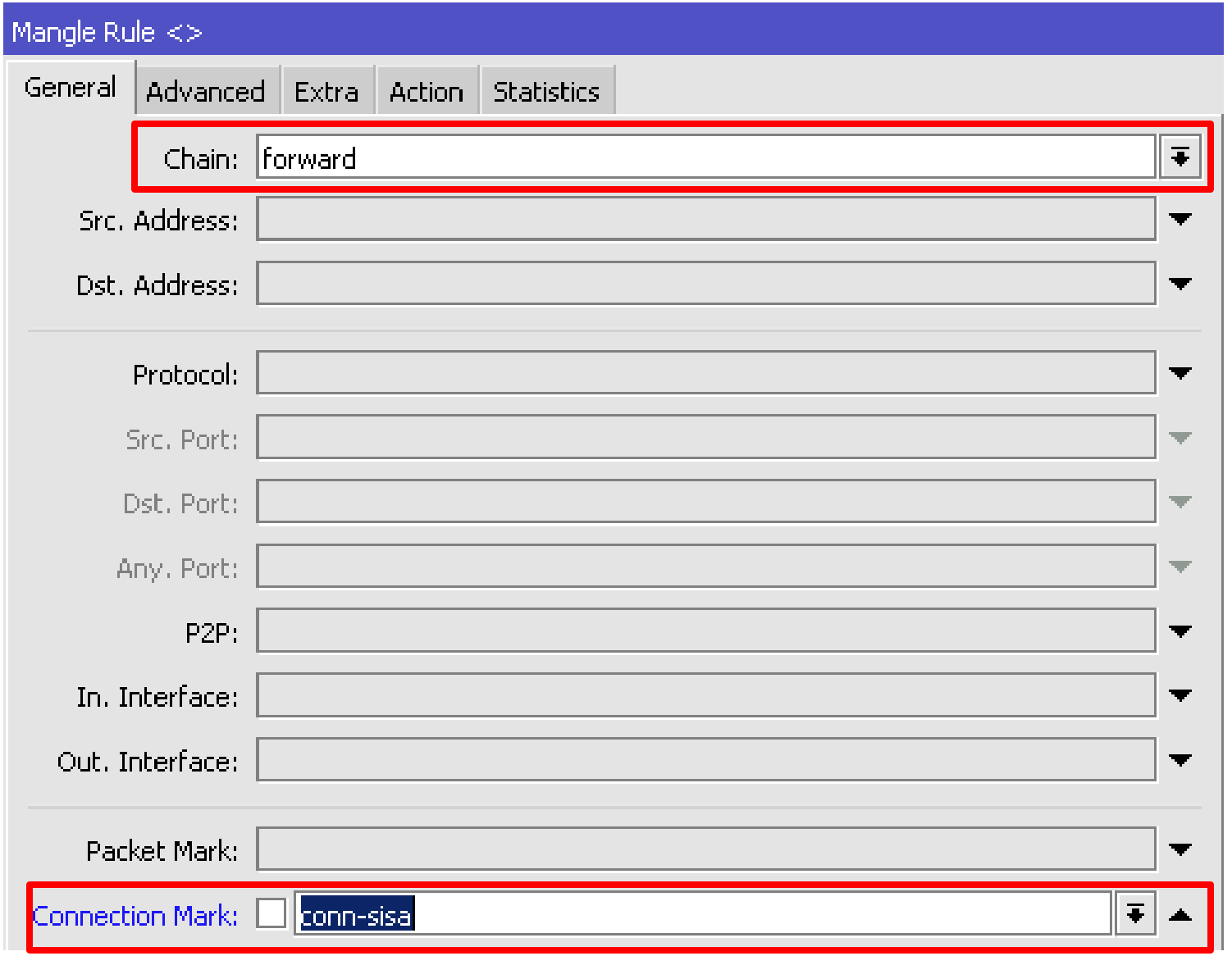


Mark Connection - Sisa

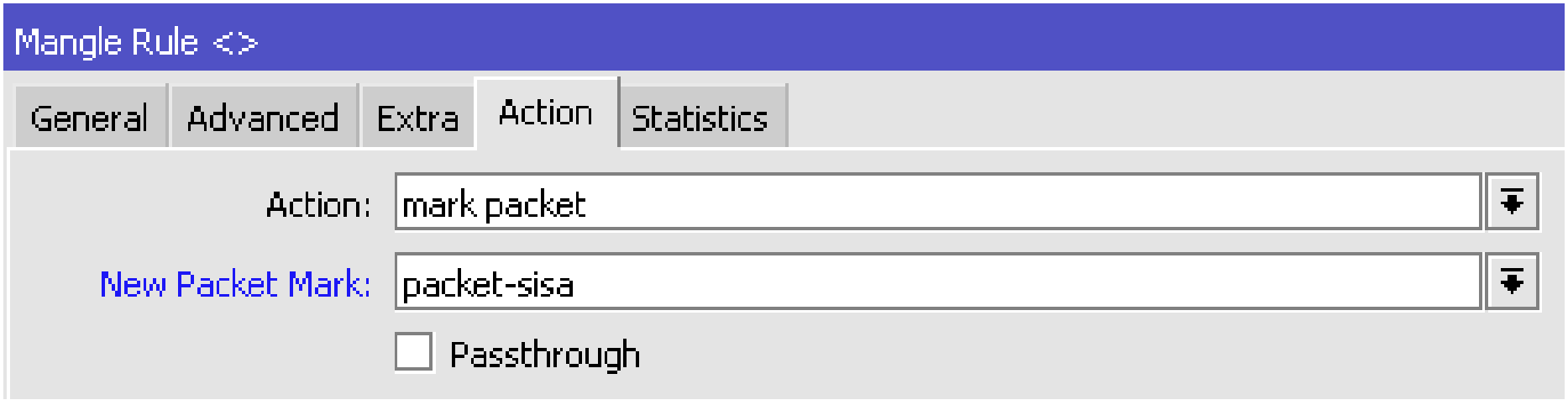




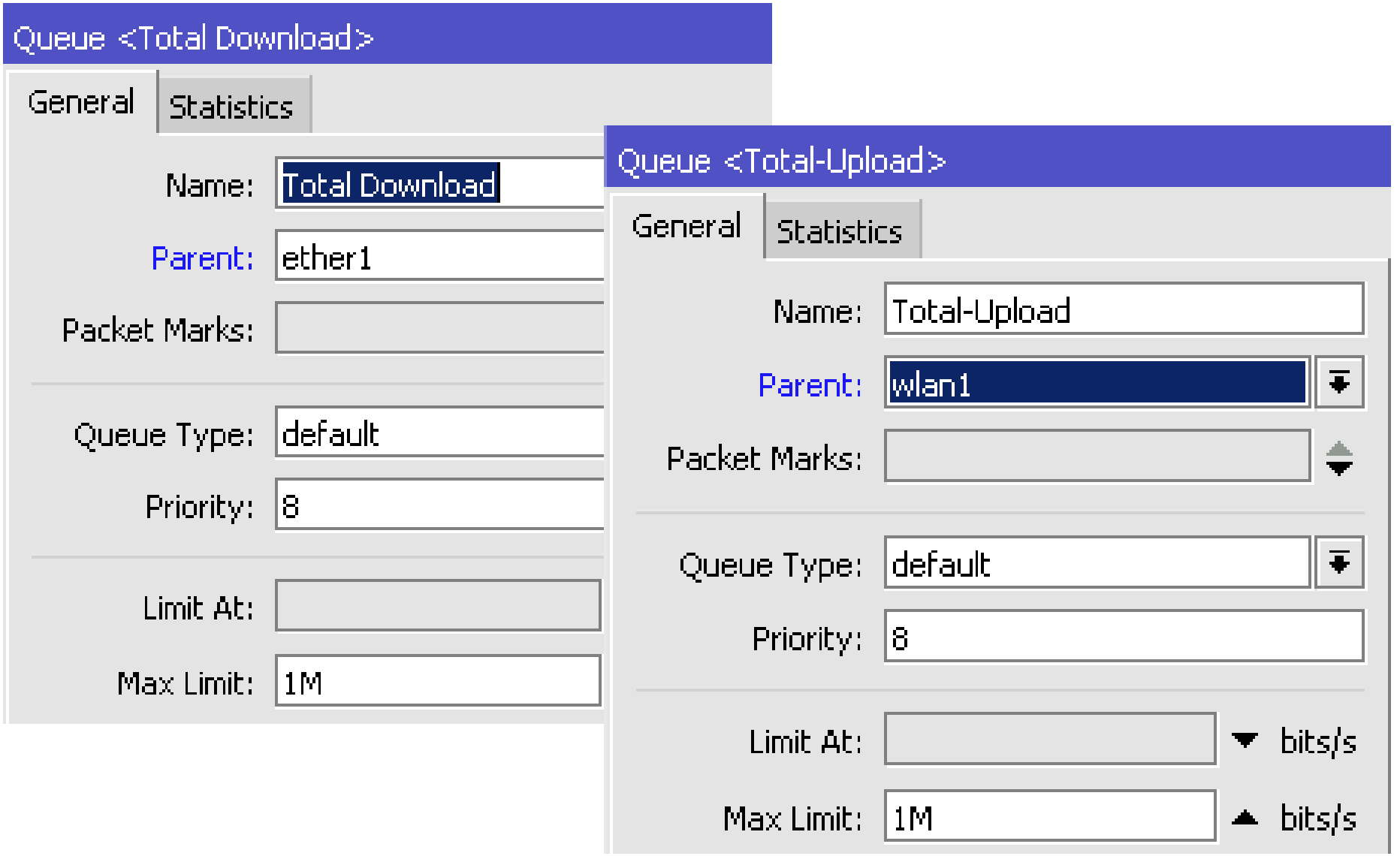
Mark Packet - Sisa



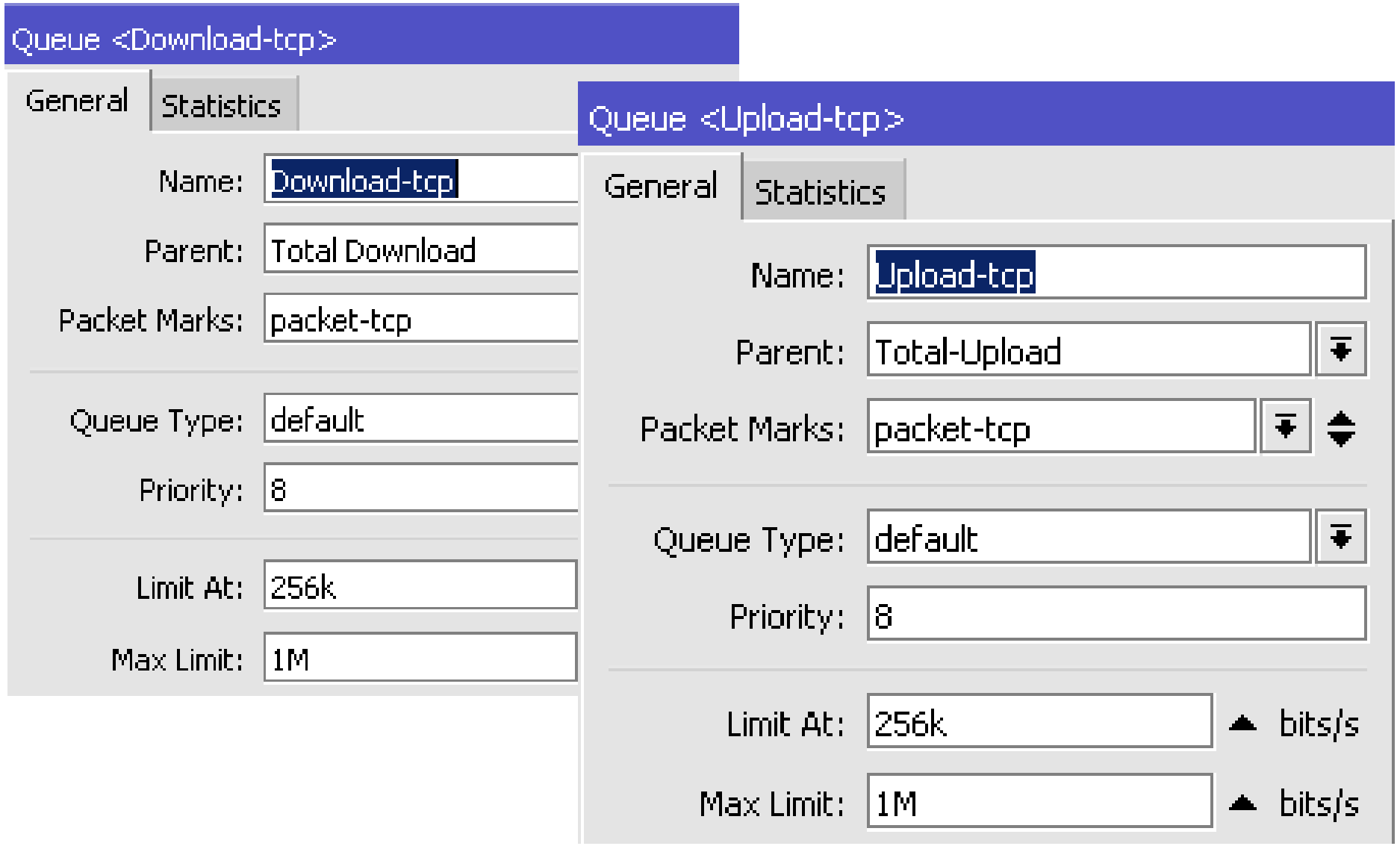
Mark Packet - Sisa



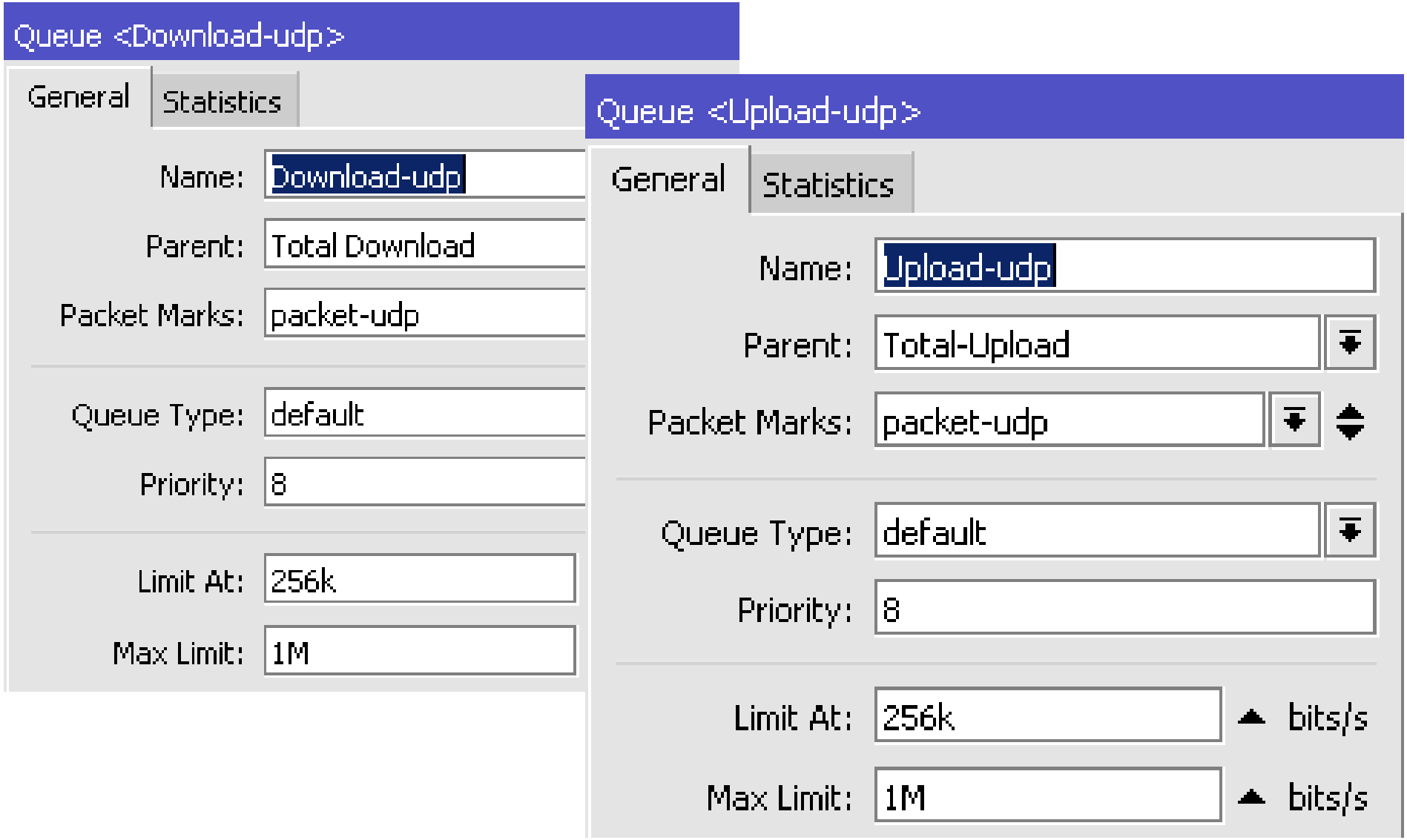
QueueTree – Parent



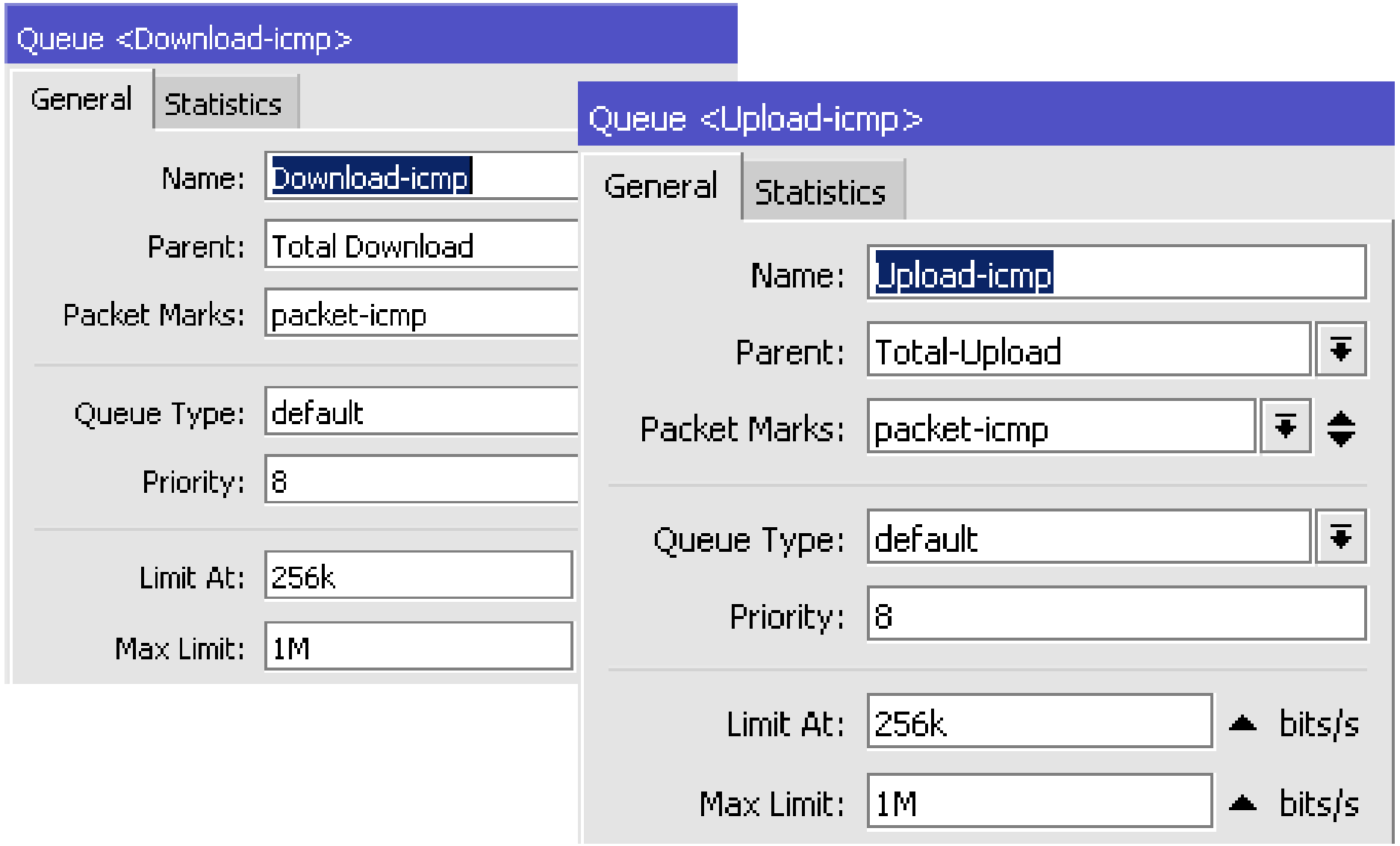
QueueTree – Child TCP



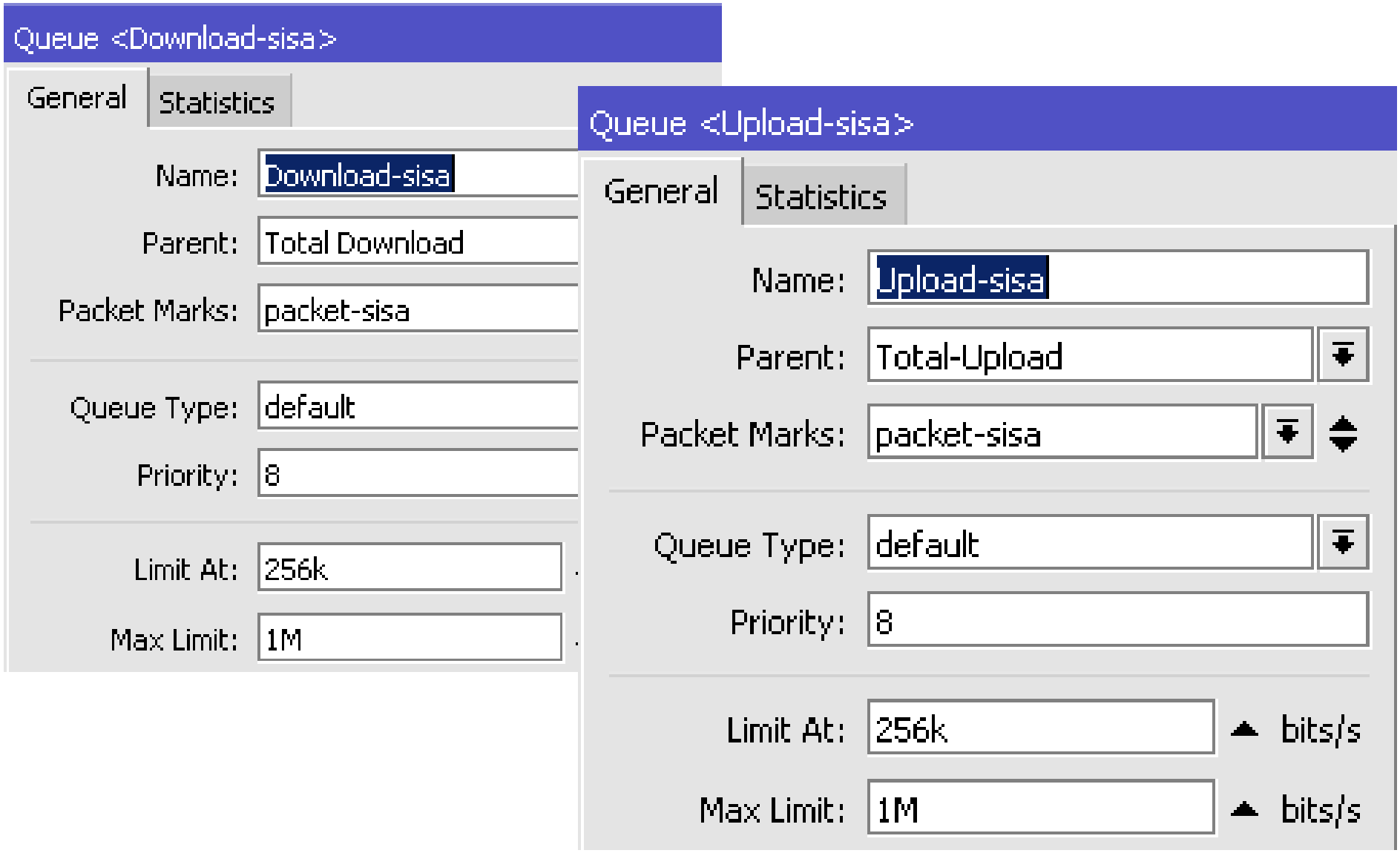
QueueTree – Child UDP



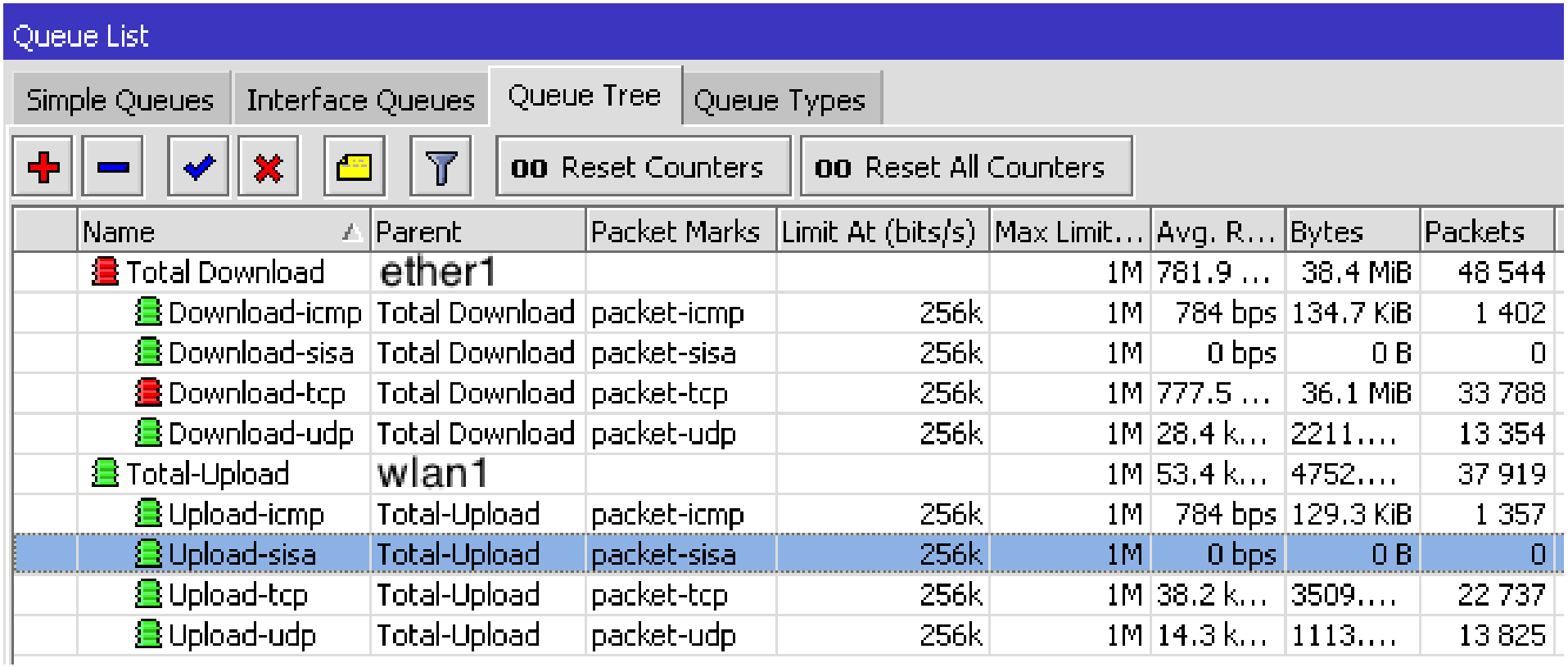
QueueTree – Child ICMP



QueueTree – Child Sisa



QueueTree - Action



Name	Parent	Packet Marks	Limit At (bits/s)	Max Limit...	Avg. R...	Bytes	Packets
Total Download	ether1			1M	781.9 ...	38.4 MiB	48 544
Download-icmp	Total Download	packet-icmp	256k	1M	784 bps	134.7 KiB	1 402
Download-sisa	Total Download	packet-sisa	256k	1M	0 bps	0 B	0
Download-tcp	Total Download	packet-tcp	256k	1M	777.5 ...	36.1 MiB	33 788
Download-udp	Total Download	packet-udp	256k	1M	28.4 k...	2211....	13 354
Total-Upload	wlan1			1M	53.4 k...	4752....	37 919
Upload-icmp	Total-Upload	packet-icmp	256k	1M	784 bps	129.3 KiB	1 357
Upload-sisa	Total-Upload	packet-sisa	256k	1M	0 bps	0 B	0
Upload-tcp	Total-Upload	packet-tcp	256k	1M	38.2 k...	3509....	22 737
Upload-udp	Total-Upload	packet-udp	256k	1M	14.3 k...	1113....	13 825

Hotspot

Certified Mikrotik Training Basic Class

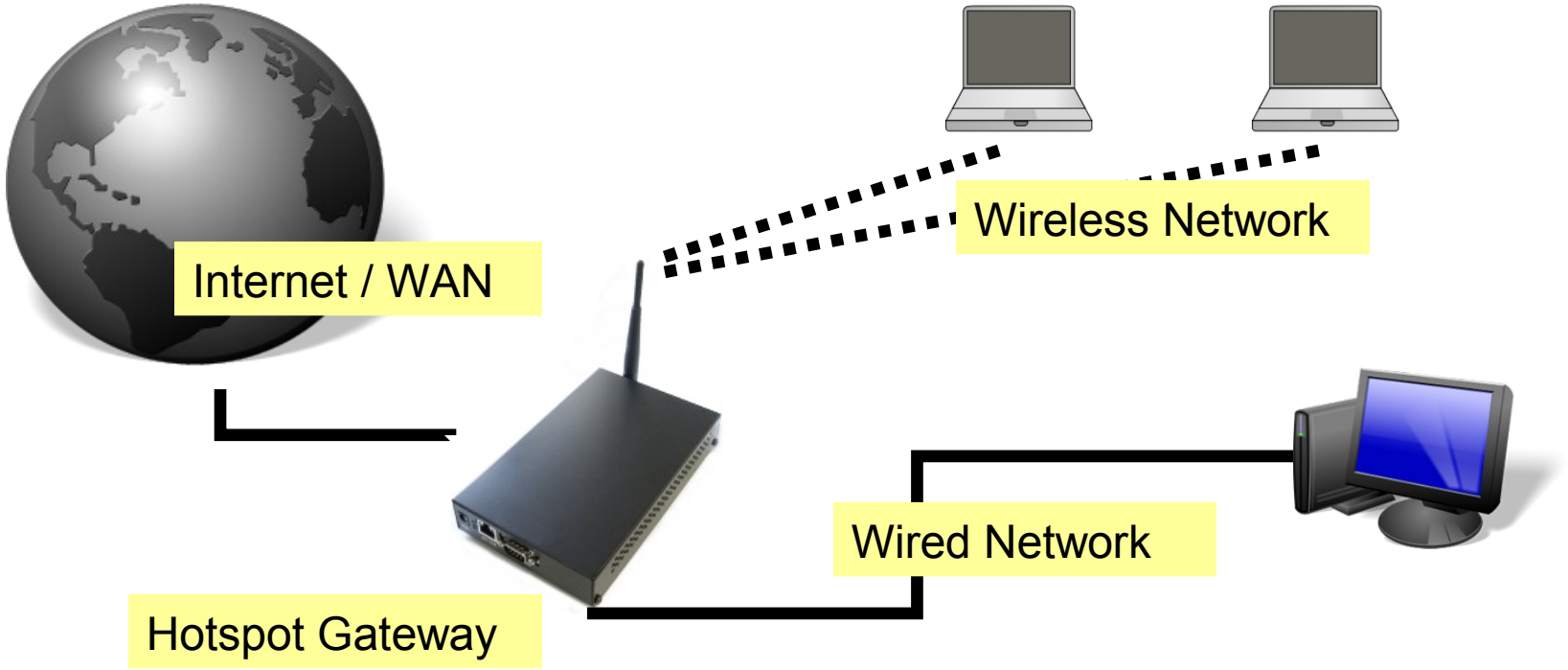
Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

HotSpot

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

HotSpot Network - Example



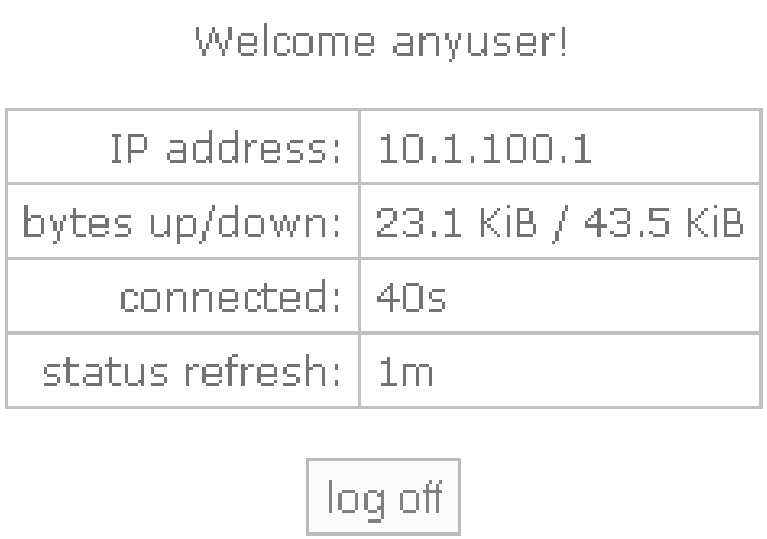
- Hotspot System bisa digunakan pada jaringan Wireless maupun jaringan Kabel bahkan kombinasi dari keduanya.
- Jaringan Hotspot bersifat **Bridge Network**

How does it work ?

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

How does it work ?

- Jika informasi login sudah tepat, router akan :
  - Mengautentikasi client di hotspot system.
  - Membuka halaman web yang diminta sebelumnya.
  - Membuka popup halaman status.
- User dapat menggunakan akses jaringan.



HotSpot features

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

HotSpot setup wizard

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

HotSpot Setup Wizard

- Pada Langkah awal Tentukan interface mana yang akan digunakan untuk menjalankan Hotspot System:
  hotspot interface: (ex: ether1,wlan1,bridge1,vlan1)
- Tentukan Alamat IP untuk Interface Hotspot :
  Local address of hotspot network: (ex: 10.5.50.1/24)
- Opsi Hotspot Network akan NAT atau Routing :
  masquerade hotspot network: yes
- Tentukan IP-Pool untuk jaringan Hotspot :
  address pool of hotspot network: 10.5.50.2-10.5.50.254
- Menggunaan SSL-certificate jika ingin menggunakan Login-By HTTPS :
  select certificate: none

HotSpot Setup Wizard

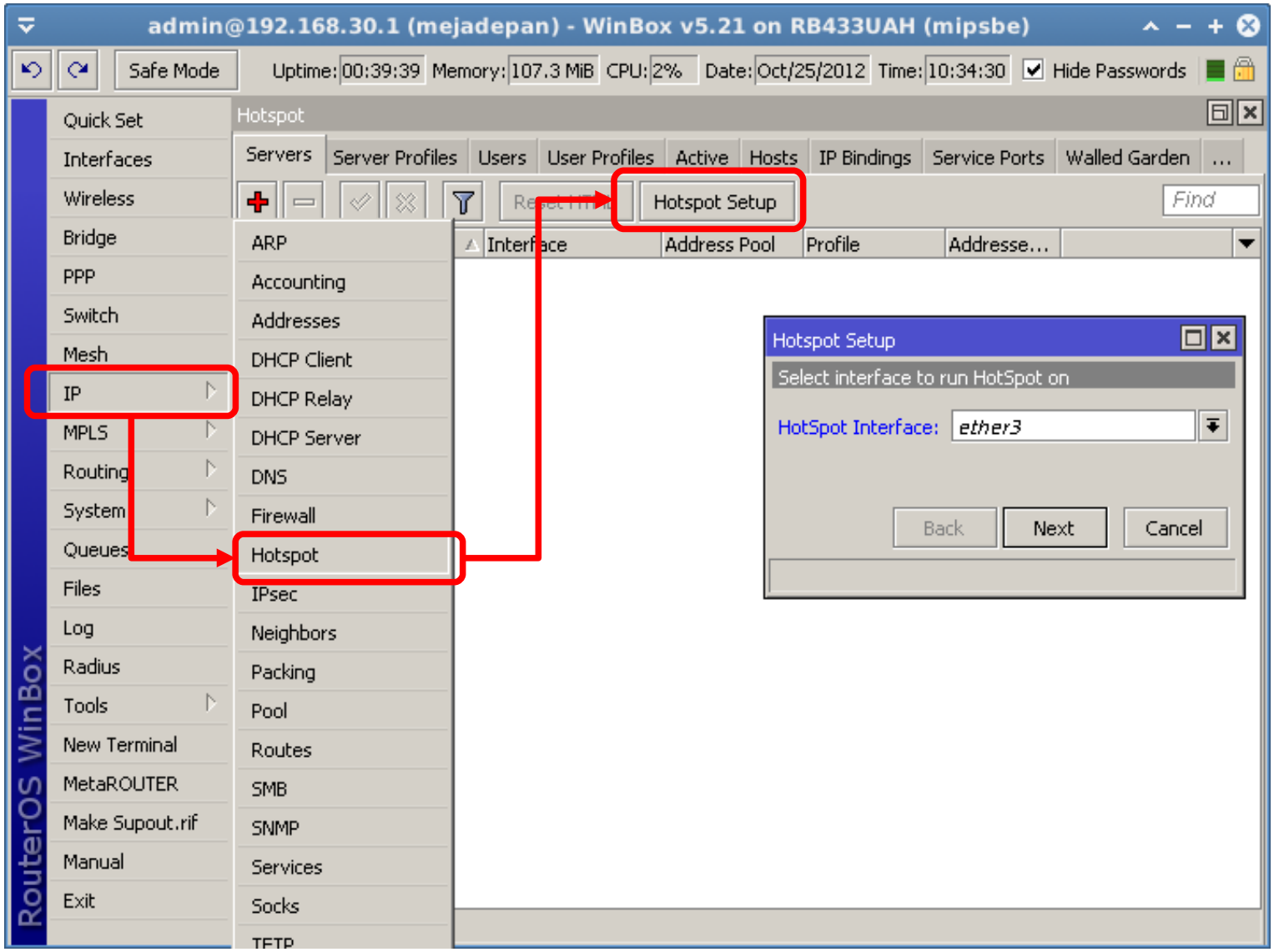
- Jika diperlukan SMTP server khusus untuk Server hotspot bisa ditentukan, sehingga Server bisa mengirimkan email (misal email notifikasi). Konfigurasi SMTP server :

  Ip address of smtp server: 0.0.0.0 (ex: 159.148.147.194)
- Konfigurasi DNS server yang akan digunakan oleh user Hotspot :

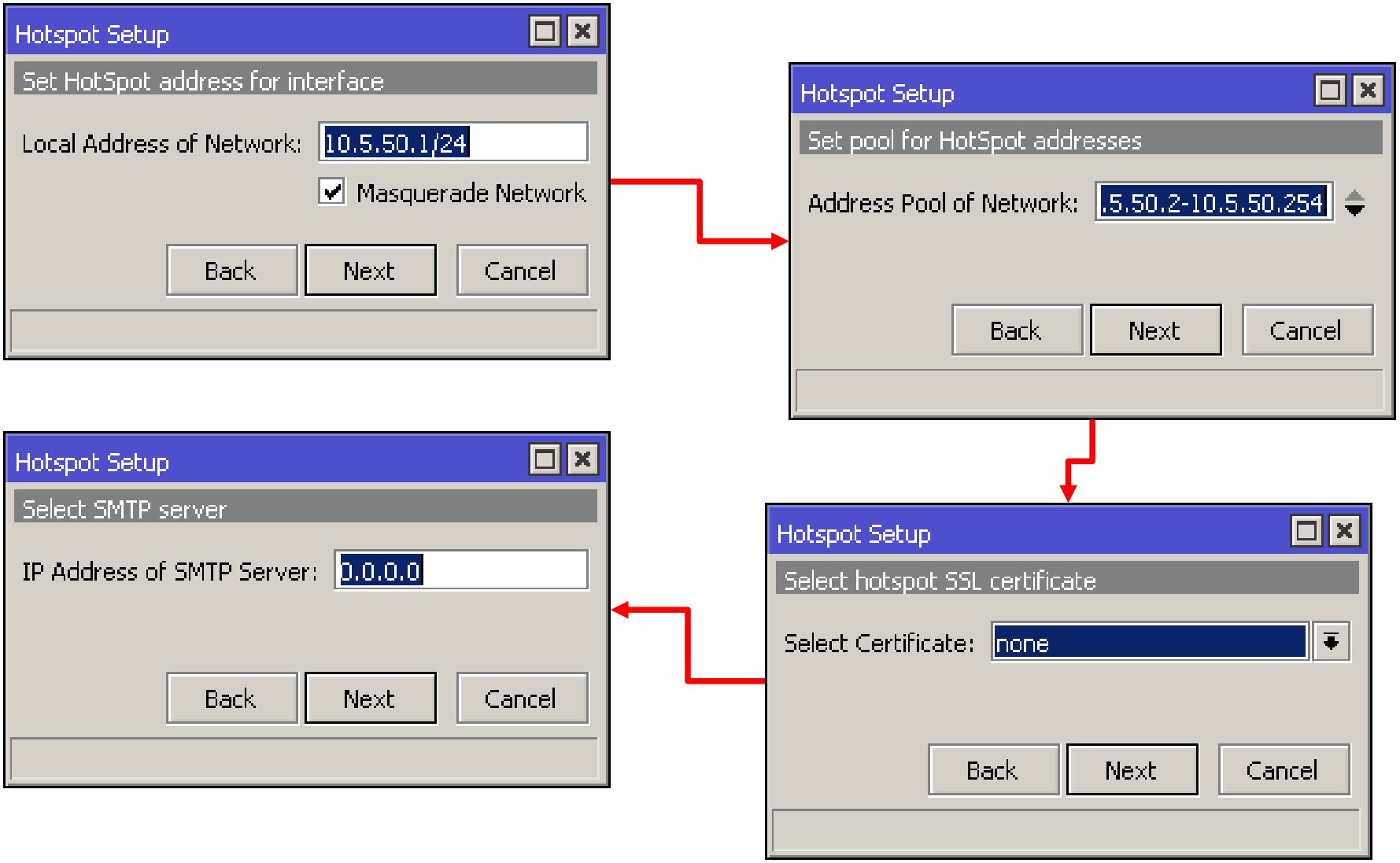
  dns servers: 159.148.147.194,159.148.60.20
- Konfigurasi DNS-name dari router Hotspot, Hal ini digunakan jika Router memiliki DNS-Name yang valid (FQDN), Jika tidak ada biarkan kosong.
- Langkah terakhir dari wizard adalah pembuatan sebuah user hotspot :

  name of local hotspot user: usrox
  password for the user: 12345

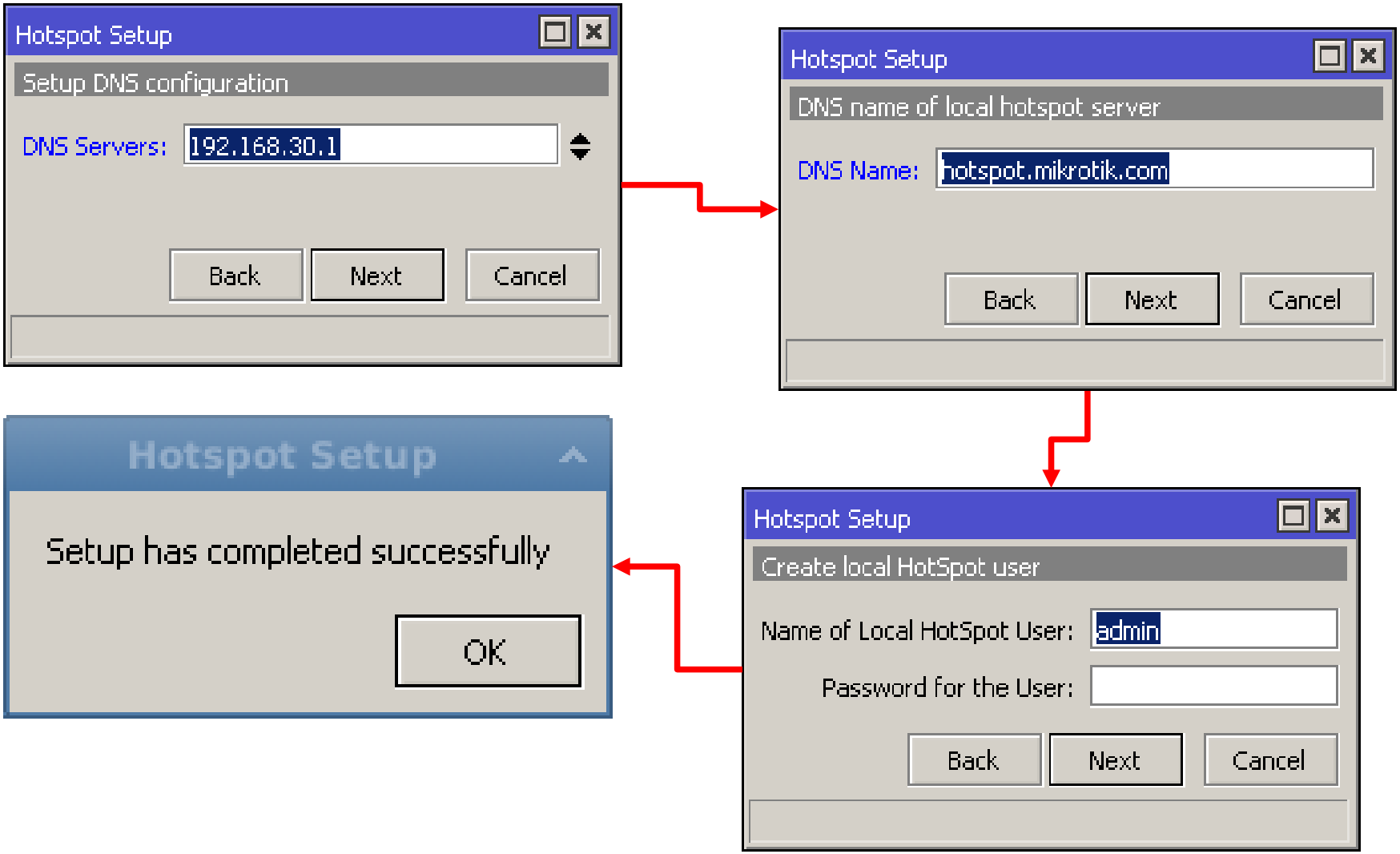
HotSpot Setup Wizard (Step 1)



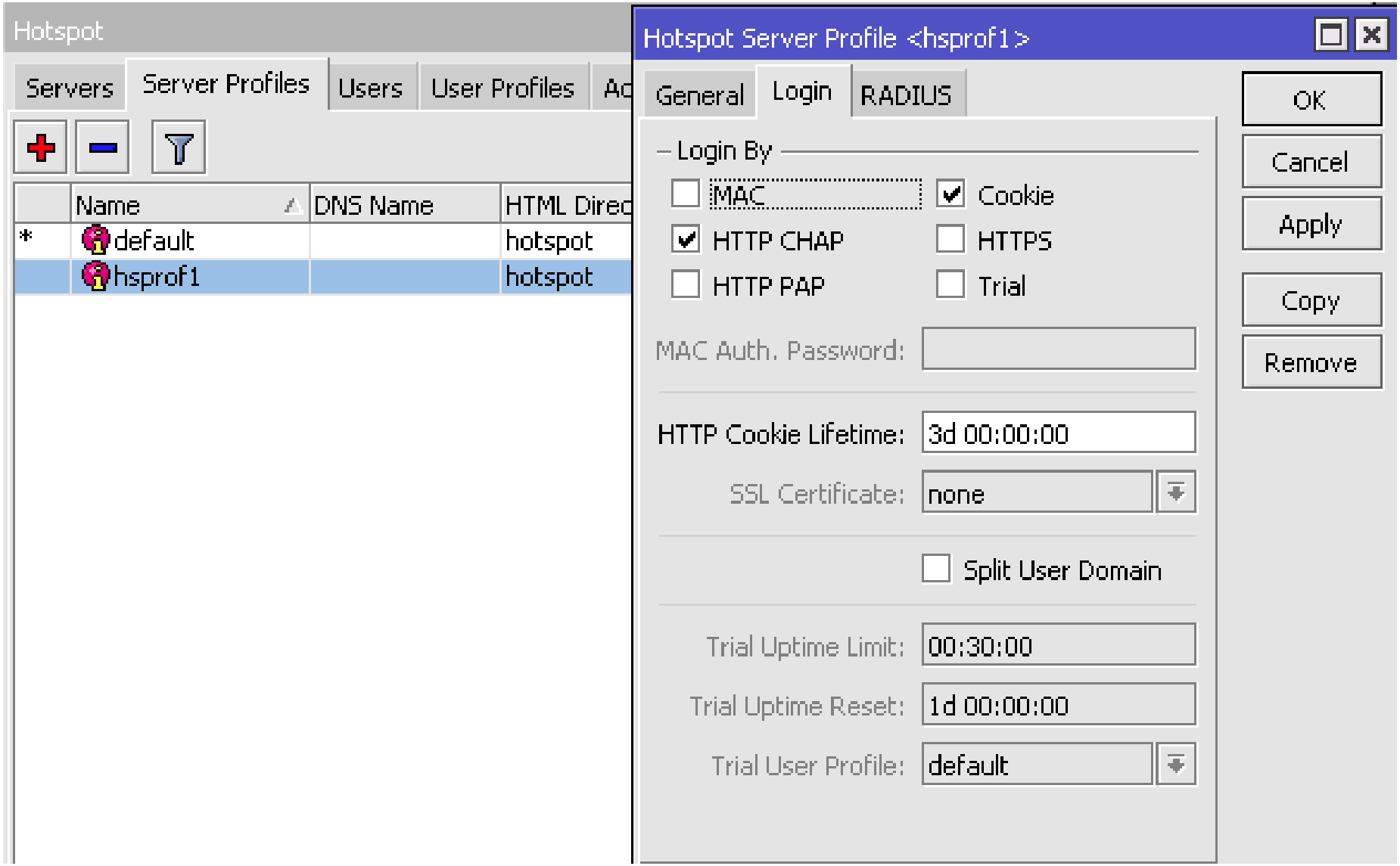
HotSpot Setup Wizard (Step 2-5)



HotSpot setup wizard (step 5-8)



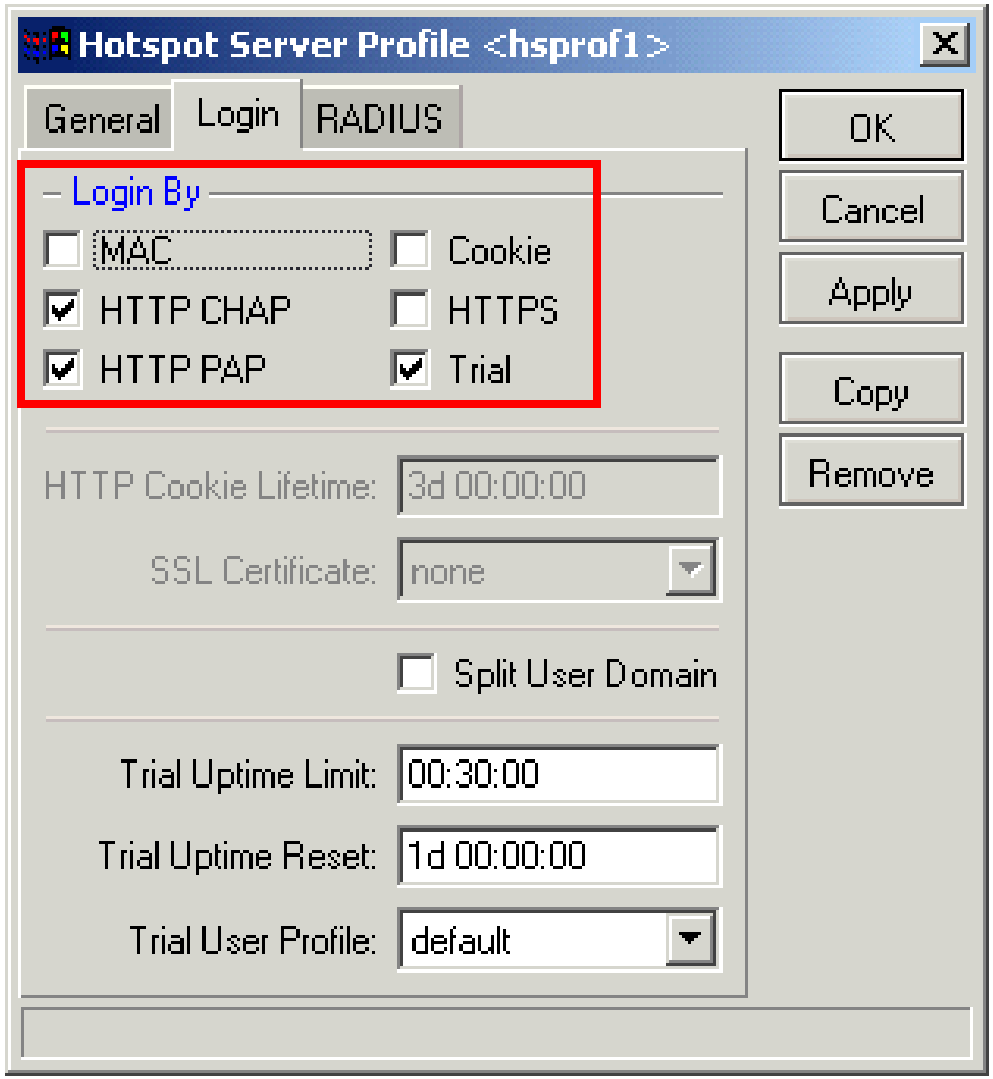
HotSpot Server Profiles



HotSpot Server profiles

- Hotspot Server Profile digunakan untuk menyimpan konfigurasi-konfigurasi umum dari beberapa hotspot server.
- Profile ini digunakan untuk grouping beberapa hotspot server dalam satu router.
- Pada server profile terdapat konfigurasi yang berpengaruh pada user hotspot seperti :
  - **Metode Autentikasi**
- Ada 6 Metode autentikasi yang bisa digunakan di Server-Profile.

Authentication Method



- 6 Metode autentikasi yang bebeda pada server profile.

Hotspot Authentication Methods

- **HTTP-PAP** - metode autentikasi yang paling sederhana, yaitu menampilkan halaman login dan mengirimkan info login berupa plain text.
- **HTTP-CHAP** - metode standard yang mengintegrasikan proses CHAP pada proses login.
- **HTTPS** – menggunakan Enkripsi Protocol SSL untuk Autentikasi.
- **HTTP Cookie** - setelah user berhasil login data cookie akan dikirimkan ke web-browser dan juga disimpan oleh router di 'Active HTTP cookie list' yang akan digunakan untuk autentikasi login selanjutnya.
- **MAC Address** - metode ini akan mengautentikasi user mulai dari user tersebut muncul di 'host-list', dan menggunakan MAC address dari client sebagai username dan password.
- **Trial** - User tidak memerlukan autentikasi pada periode waktu yang sudah ditentukan.

HotSpot User Profiles

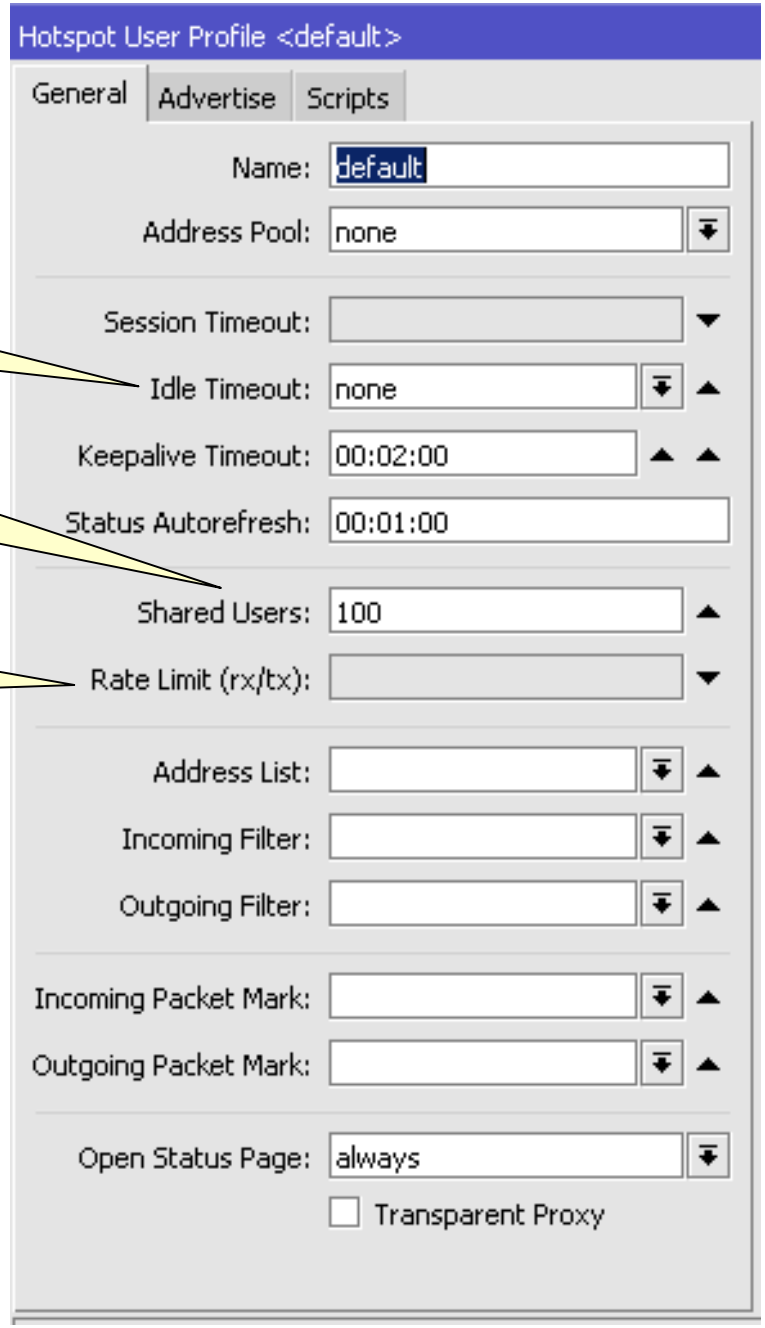
- Hotspot User Profile digunakan untuk menyimpan konfigurasi-konfigurasi umum dari User-user hotspot. Profile ini digunakan untuk grouping beberapa User.
- Pada User Profile, mampu melakukan assign pool-ip tertentu ke group user.
- Parameter Time-out juga bisa diaktifkan untuk mencegah monopoli oleh salah satu user.
- Limitasi juga bisa ditentukan di UserProfile
  - Data Rate (Kecepatan Akses)
  - Session Time (Sesi Akses)

User Profiles

Untuk melakukan log-off otomatis bagi user yang tidak ada traffic atau lupa menekan tombol log-off.

Untuk menentukan jumlah user maksimal jika menggunakan “username” yang sama.

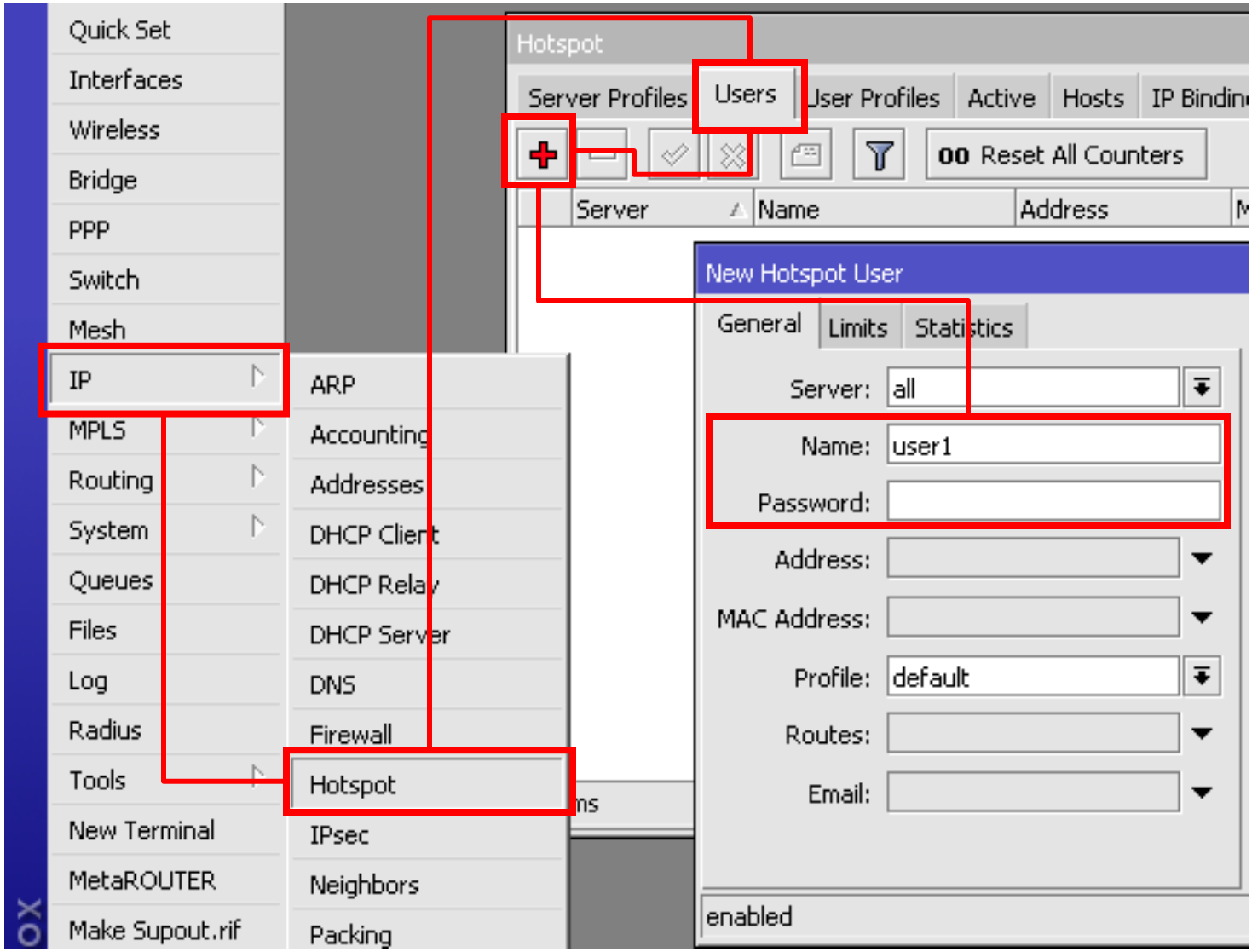
Untuk menentukan bandwith “per-user” yang menggunakan profile yang sama.
Format : **Upload** / **Download**



HotSpot User

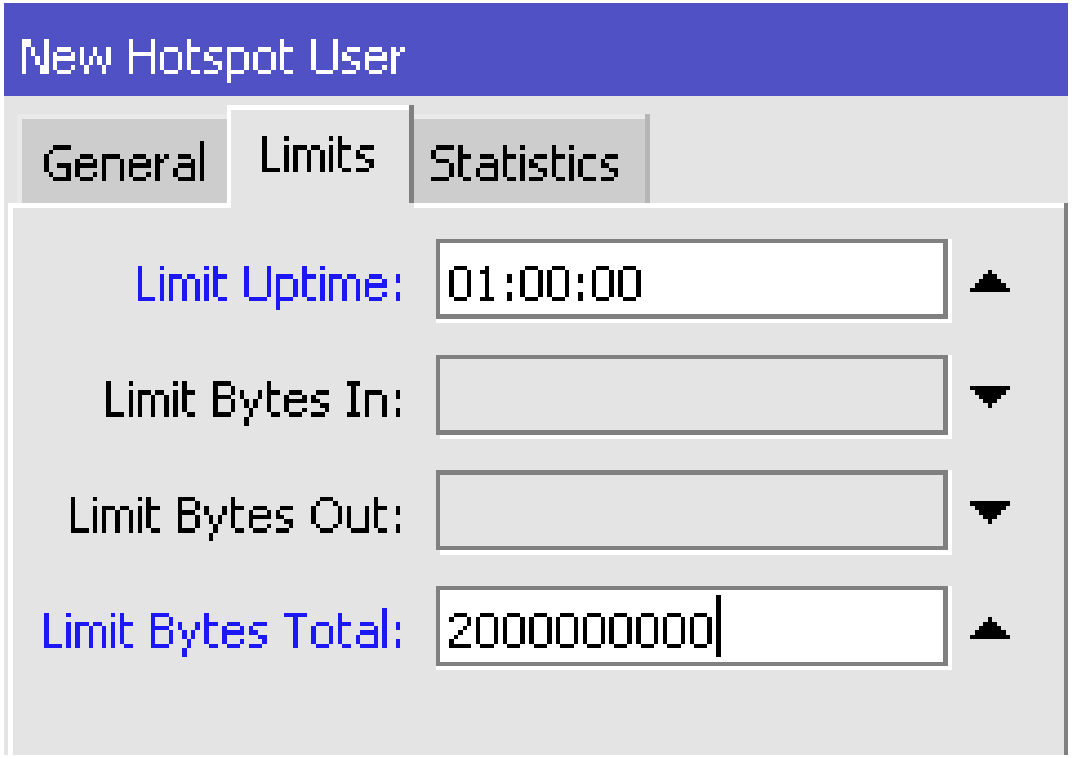
- Halaman dimana parameter username, password dan profile dari user disimpan.
- Beberapa limitasi juga bisa ditentukan di halaman user seperti uptime-limit dan bytes-in/bytes-out. Jika limitasi sudah tercapai maka user tersebut akan expired dan tidak dapat digunakan lagi.
- IP yang spesifik juga bisa ditentukan di halaman ini sehingga user akan mendapat ip yang sama.
- User bisa dibatasi pada MAC-address tertentu.

HotSpot users



User Limitation

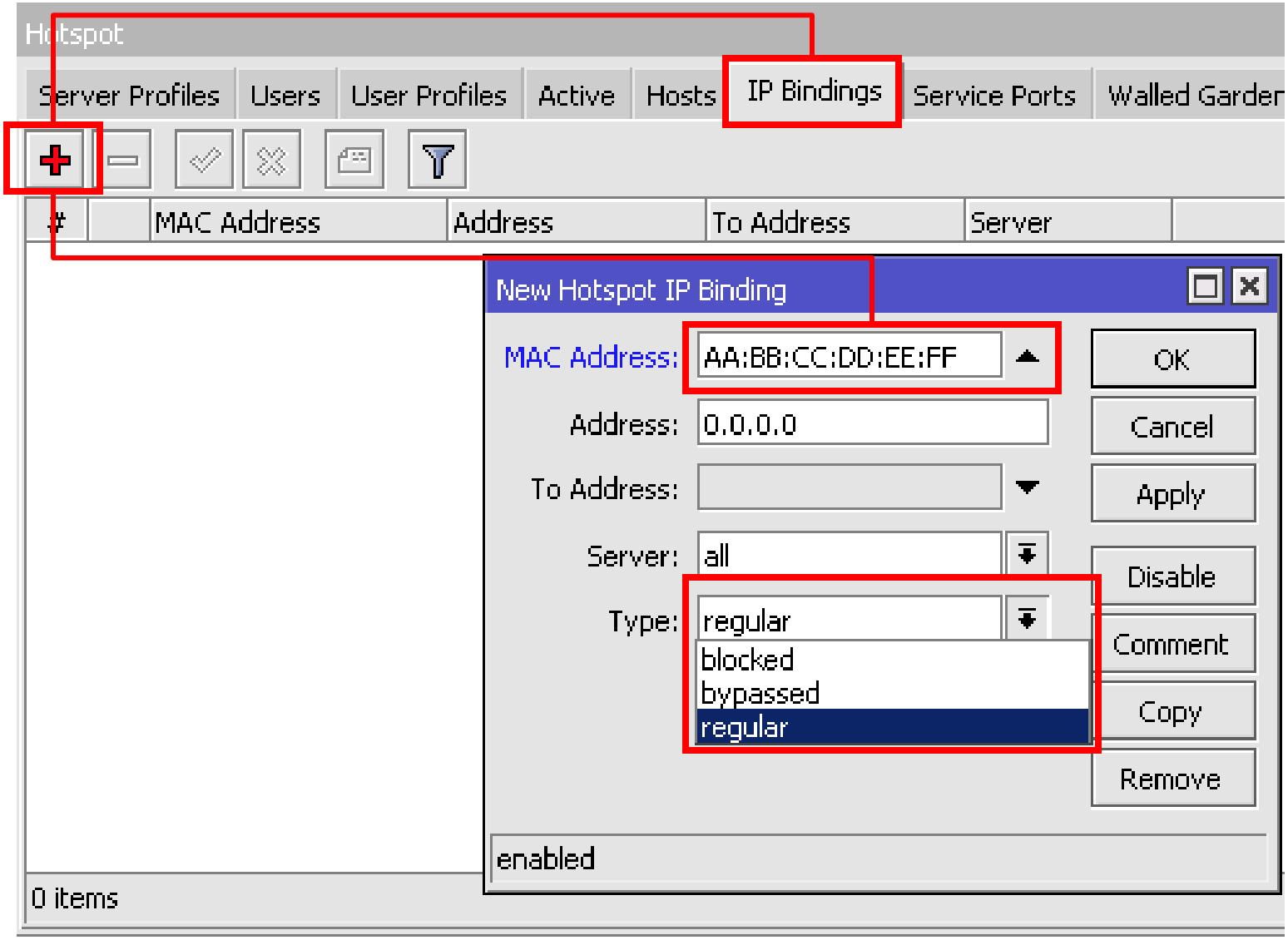
- **Limit Uptime** batas waktu user dapat menggunakan akses ke Hotspot Network.
- **Limit-bytes-in**, **Limit-bytes-out** dan **Limit-bytes-total** batas quota trasfer data yang bisa dilakukan oleh user.



Bypass! - IP bindings

- One-to-one NAT bisa dikonfigurasi secara static berdasarkan :
  - Original IP Host
  - Original MAC Address
- Bypass host terhadap Hotspot Authentication bisa dilakukan menggunakan IP-Bindings.
- Block Akses dari host tertentu (Berdasarkan Original MAC-address atau Original IP-Address) juga bisa dilakukan menggunakan IP-Bindings.

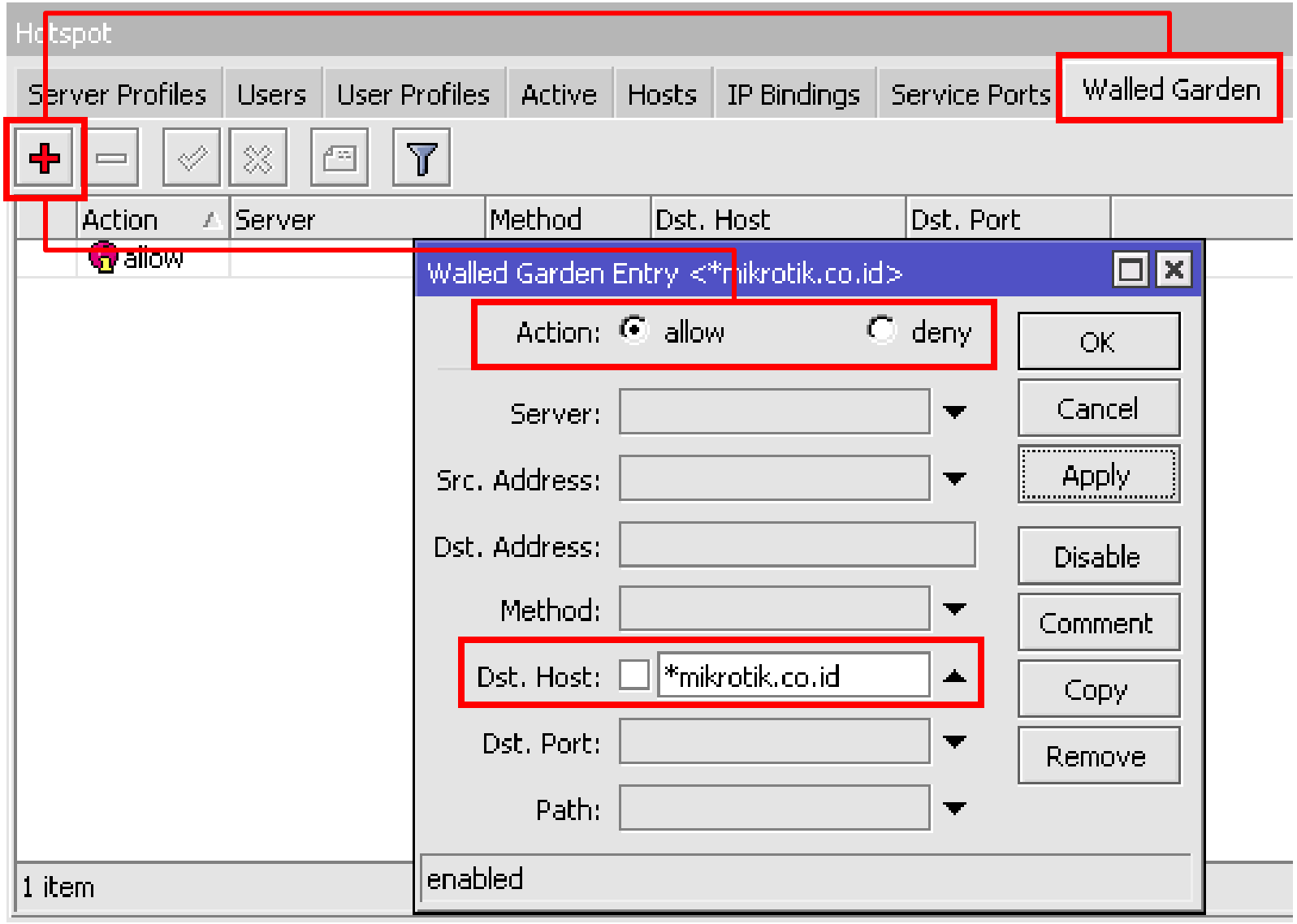
HotSpot IP bindings



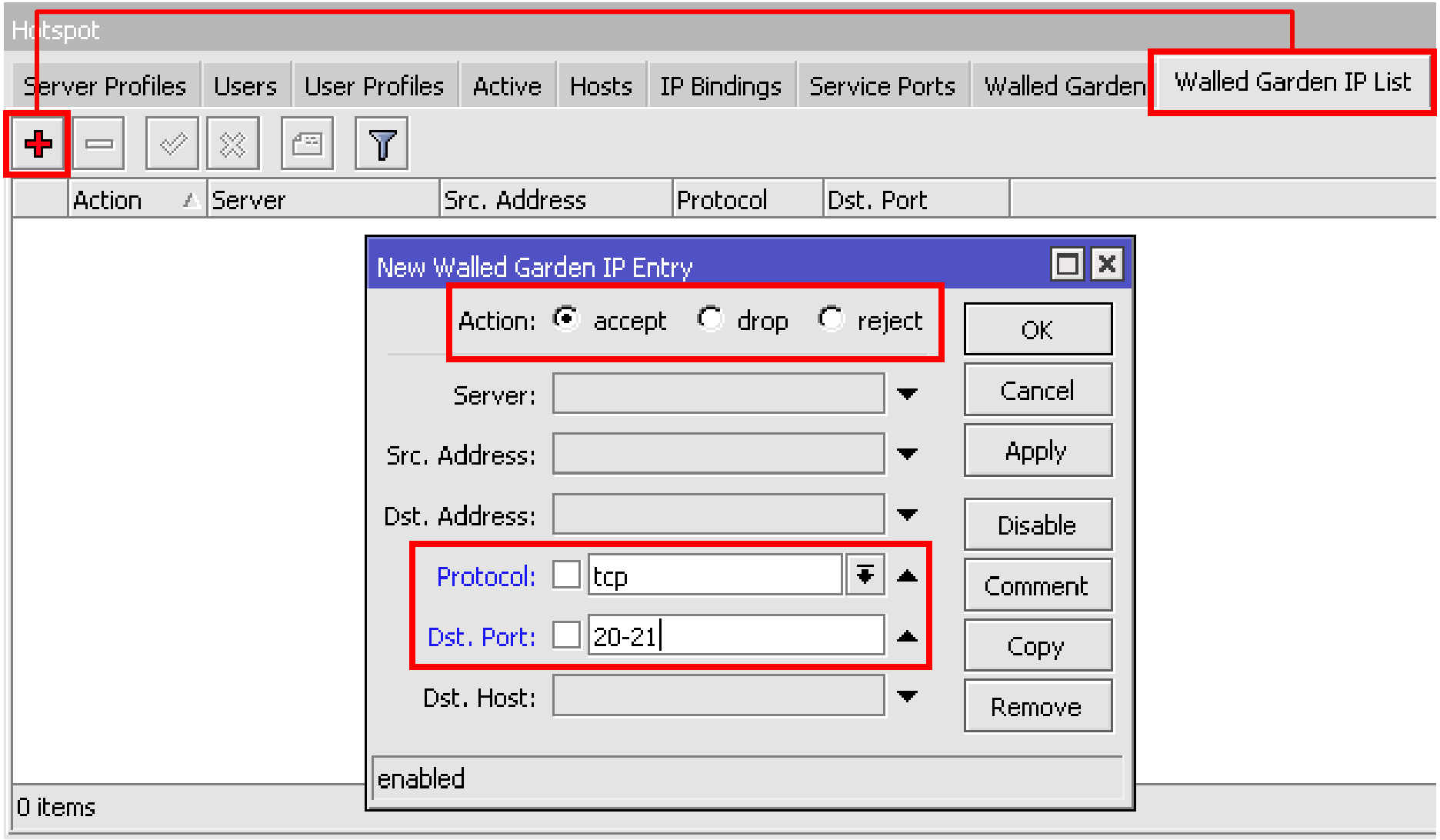
Bypass - WalledGarden

- **WalledGarden** adalah sebuah system yang memungkinkan untuk user yang belum terautentikasi menggunakan (Bypass!) beberapa resource jaringan tertentu tetapi tetap memerlukan autentikasi jika ingin menggunakan resource yang lain.
- **IP-WalledGarden** hampir sama seperti WalledGarden tetapi mampu melakukan bypass terhadap resource yang lebih spesifik pada protocol dan port tertentu.
- Biasanya digunakan untuk melakukan bypass terhadap server local yang tidak memerlukan autentikasi.

HTTP-level WalledGarden



IP-WalledGarden

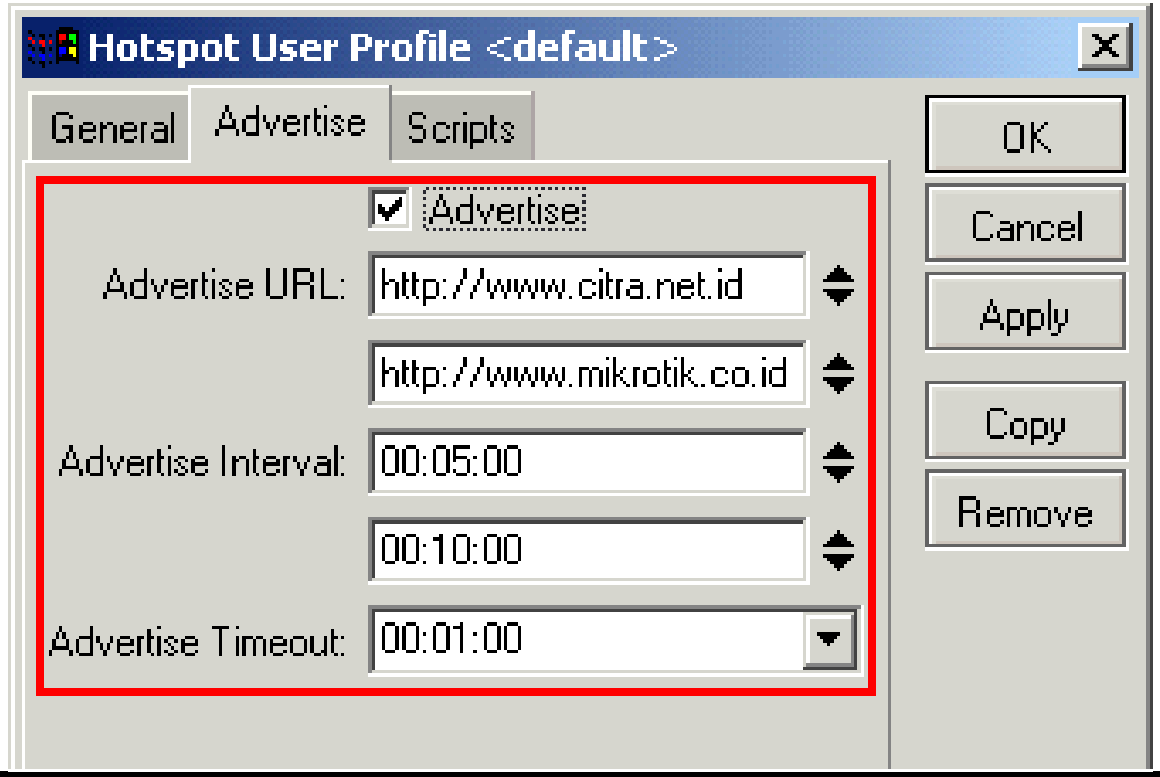


Advertisement

- Sama seperti yang digunakan pada fasilitas WalledGarden, Advertisement juga menggunakan ProxyEngine di Hotspot System untuk menampilkan popup halaman web (iklan) di web-browser para user yang sudah terautentikasi.
- Halaman Advertisement dimunculkan berdasarkan periode waktu yang sudah ditentukan, dan akses akan dihentikan jika pop-up halaman advertisement diblock (pop-up blocker aktif), dan akan disambungkan kembali jika halaman Advertisement sudah dimunculkan.

Advertisement

- Jika sudah waktunya untuk memunculkan advertisement, server akan memanggil halaman status dan merideredirect halaman status tersebut ke halaman web iklan yang sudah ditentukan.



VPN Basic

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

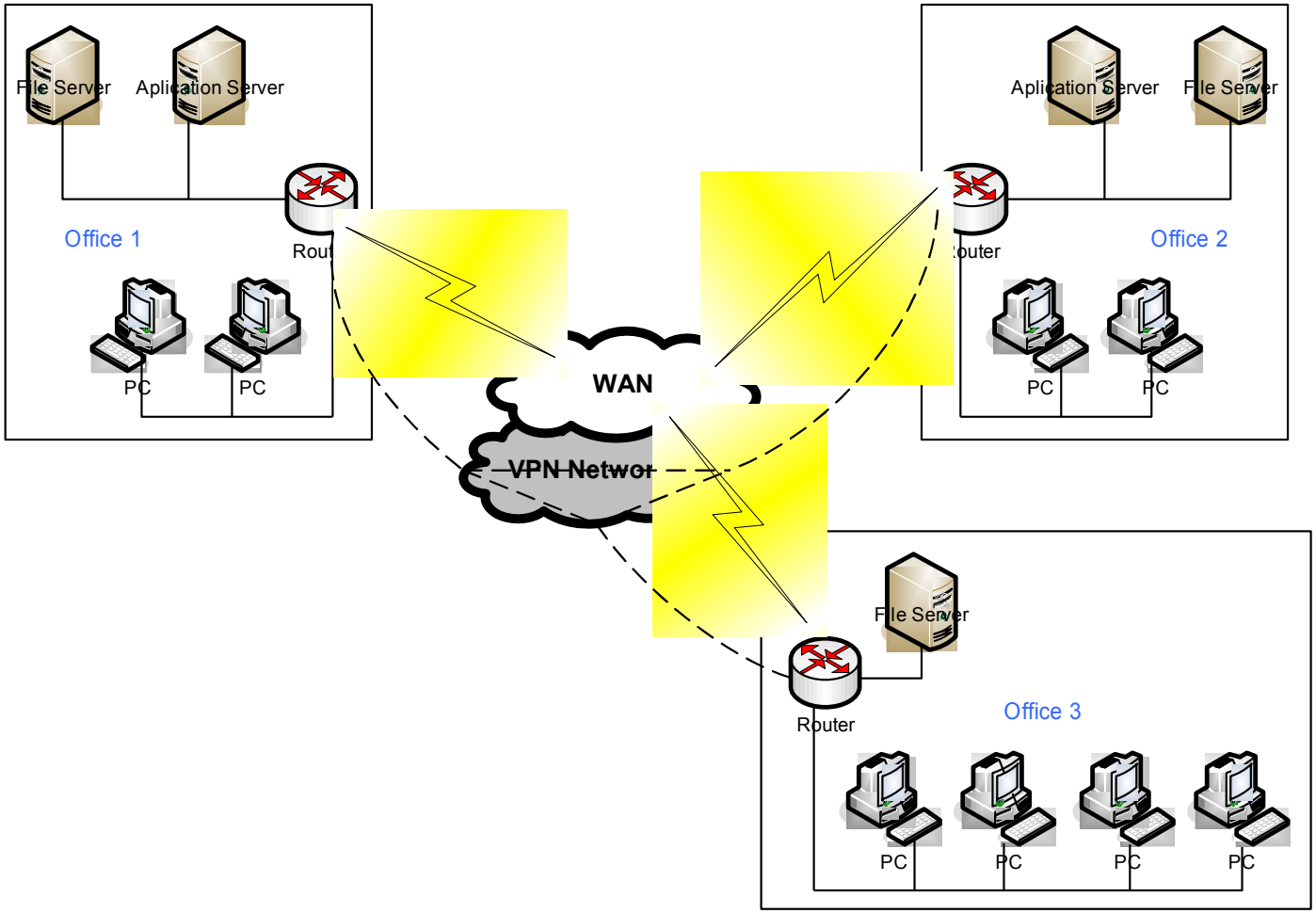
(Mikrotik Certified Training Partner)

VPN (Virtual Private Networks)

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

VPN Networks

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



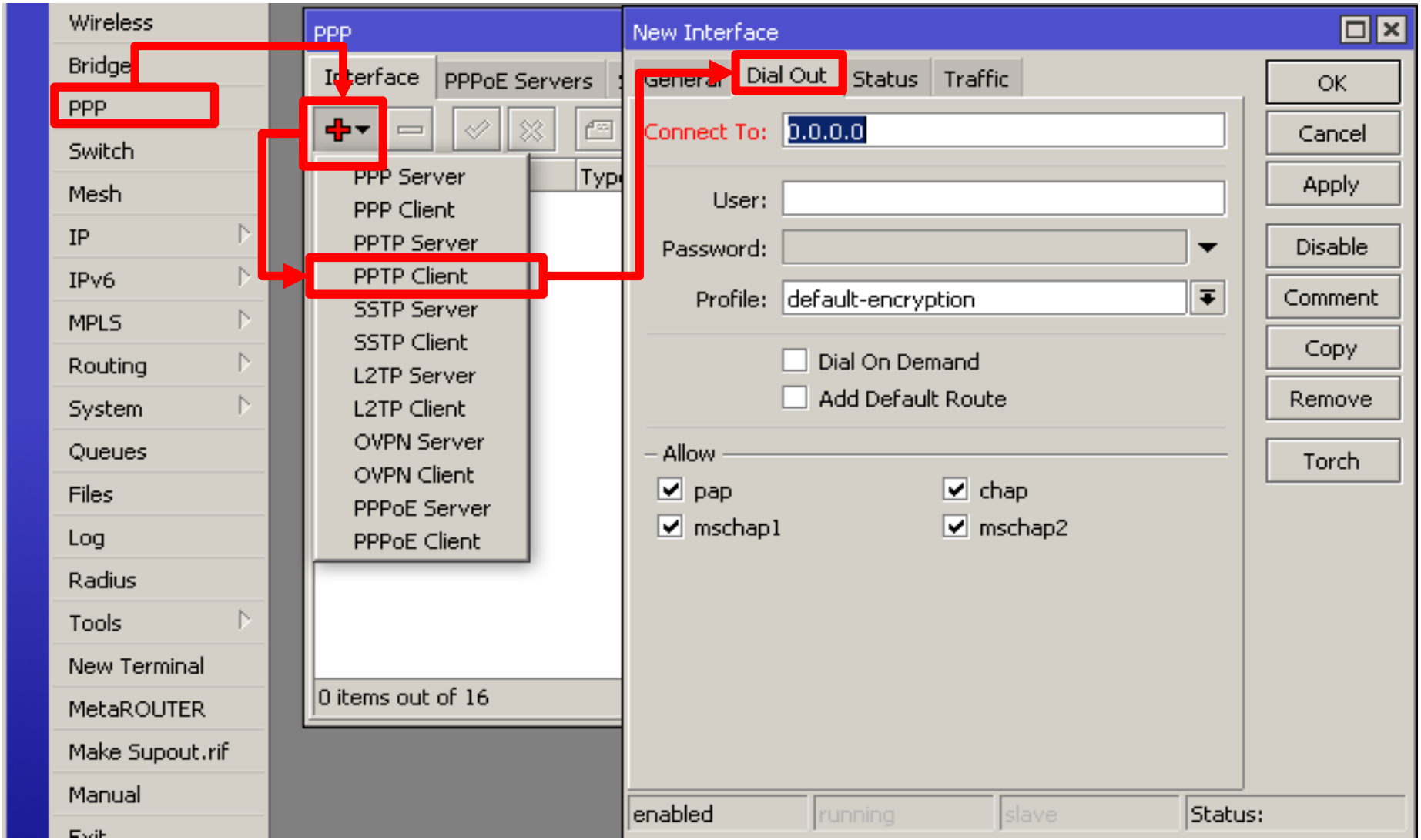
VPN Type

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

Point to Point Tunnel Protocol (PPTP)

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

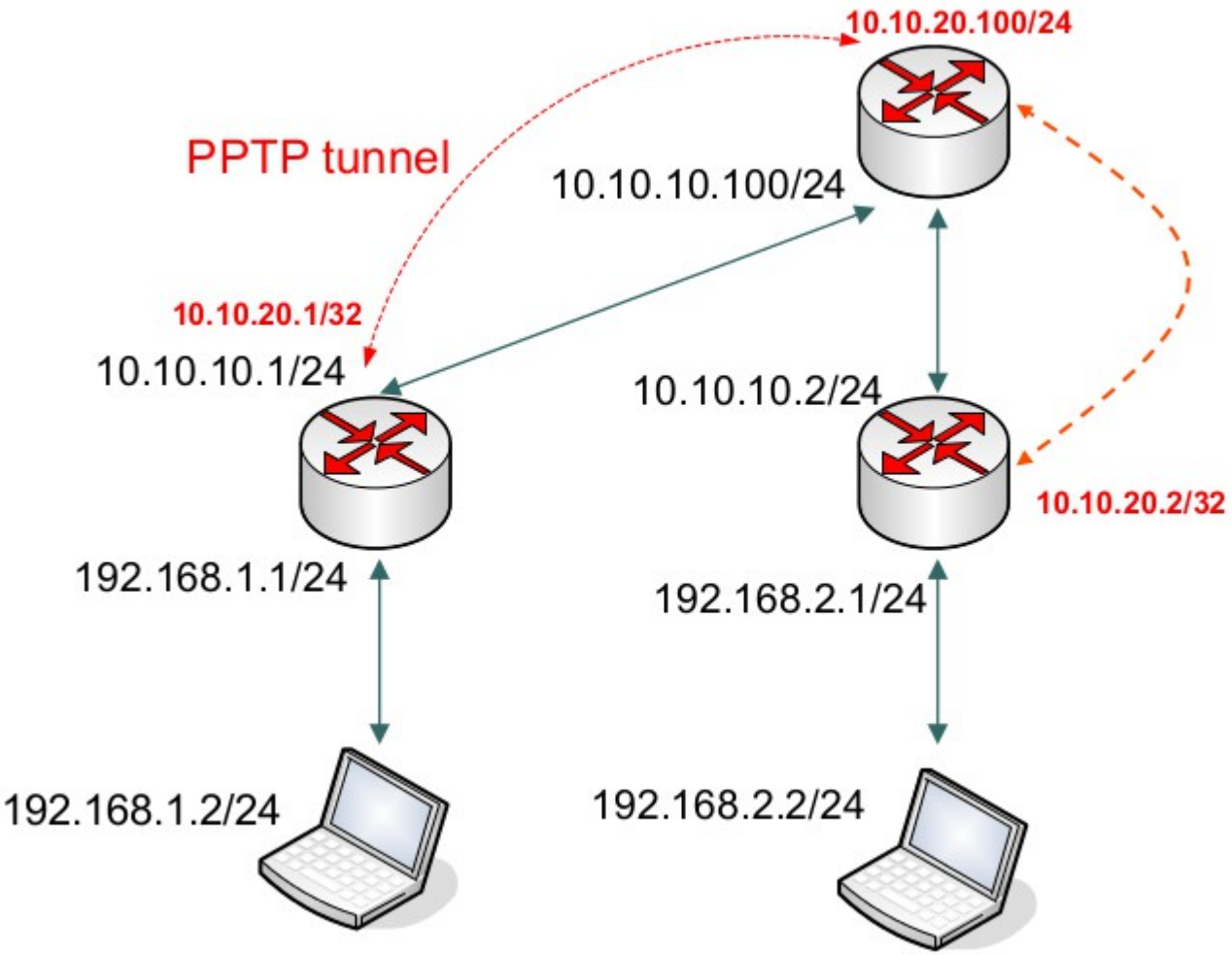
PPTP Client Configuration



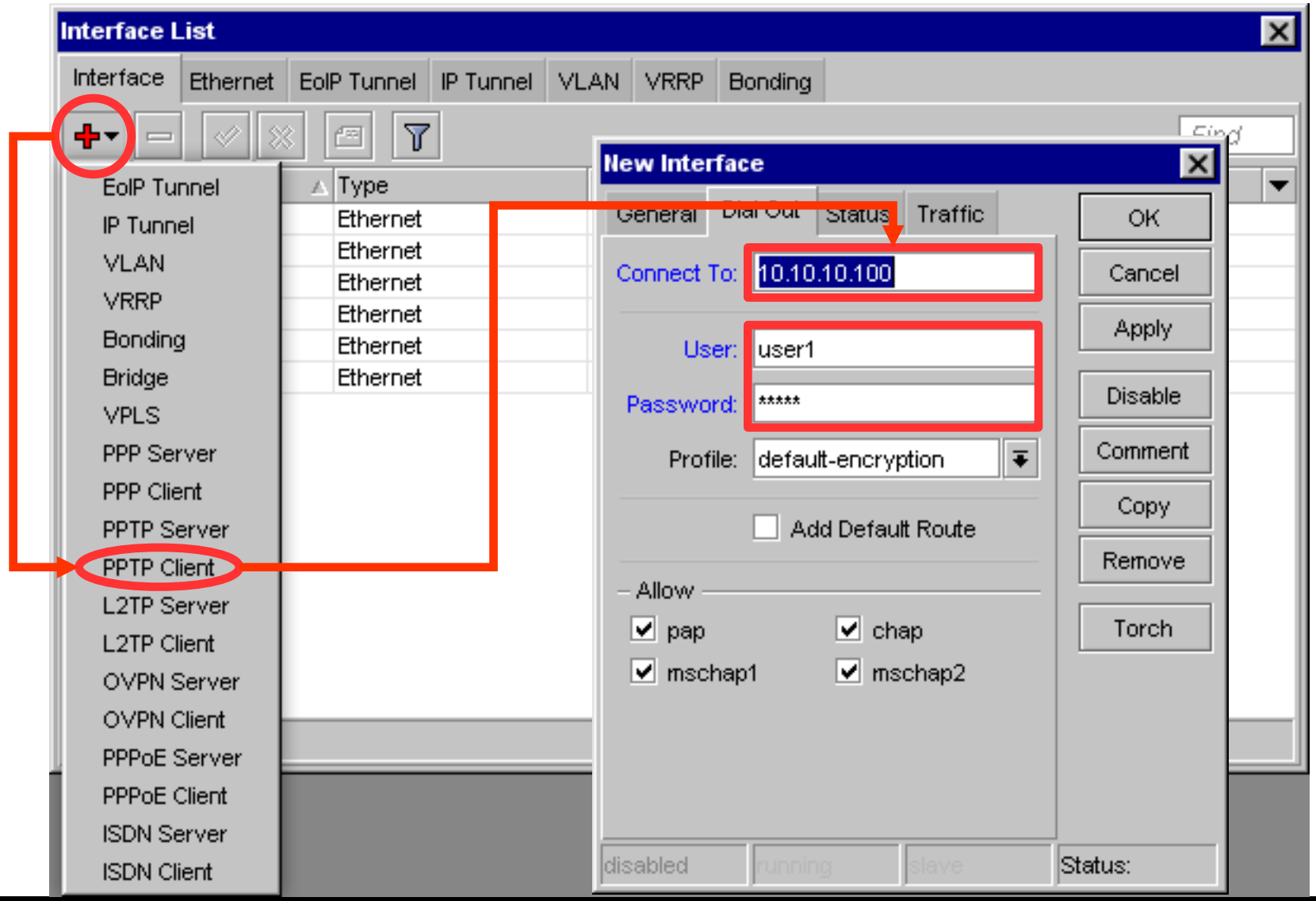
PPTP Client Configuration

- **Server Address** – Parameter server PPTP yang akan di dial
- **User** – Parameter username
- **Password** – Parameter password
- **Profile** – Parameter optional untuk mengaktifkan enkripsi pada link pptp atau tidak.

[LAB-1] PPTP Tunnels - Client



[LAB-1] PPTP Tunnels - Client

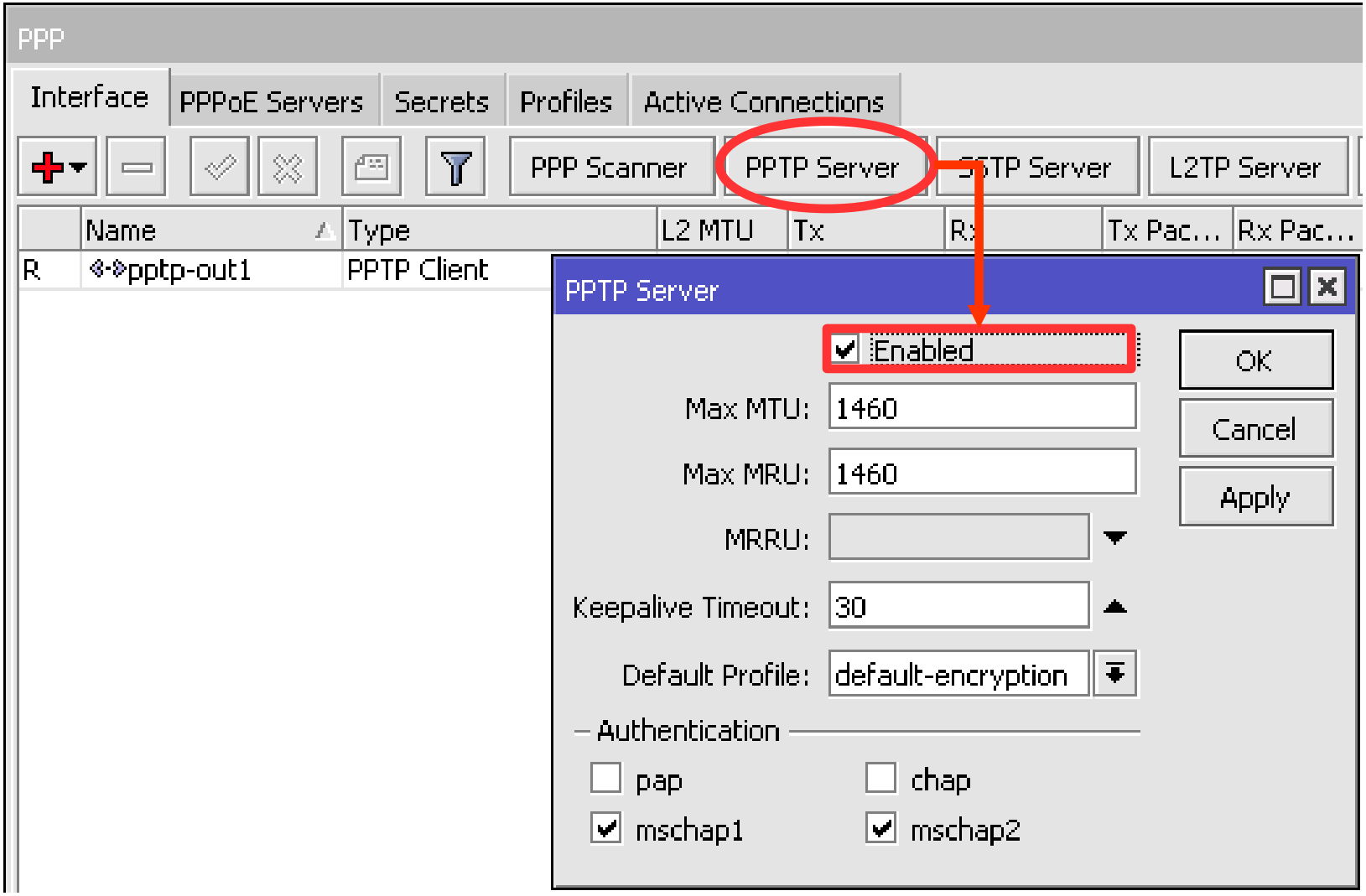


[LAB-1] PPTP Tunnels - Client

- Membuat PPTP-Client :
  - “Username” dan “Password” disesuaikan dari konfigurasi server.
  - “Connect-to” adalah parameter Alamat IP dari PPTP-Server.
  - “Add-Default-Route” adalah parameter jika akan menggunakan koneksi PPTP sebagai gateway utama.

- Membuat PPTP-Client Interface :
  - /interface pptp-client add name=pptp-out1 connect-to=10.10.10.100 user=user1 password=user1

PPTP Server Configuration

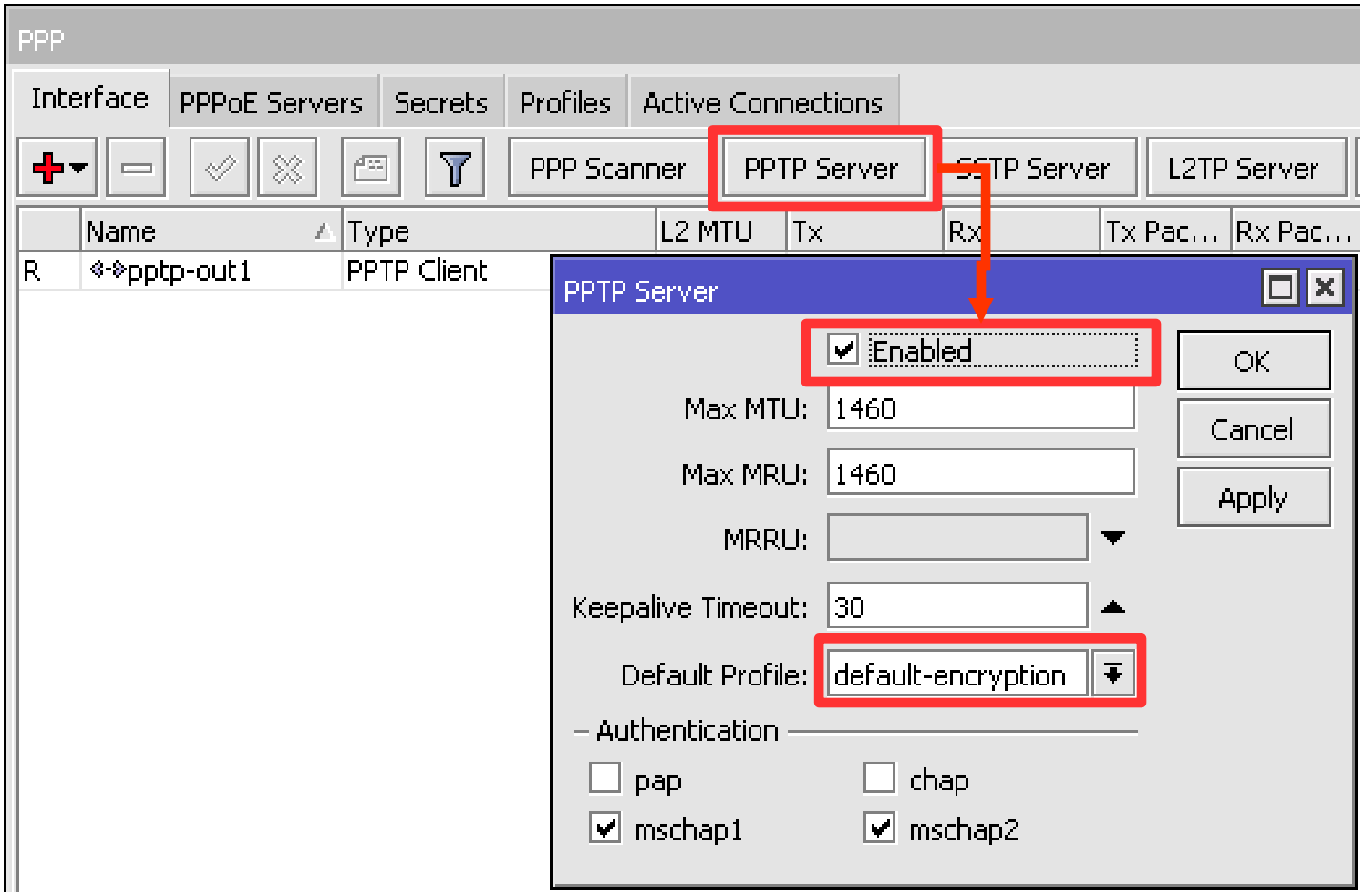


PPTP Server Configuration

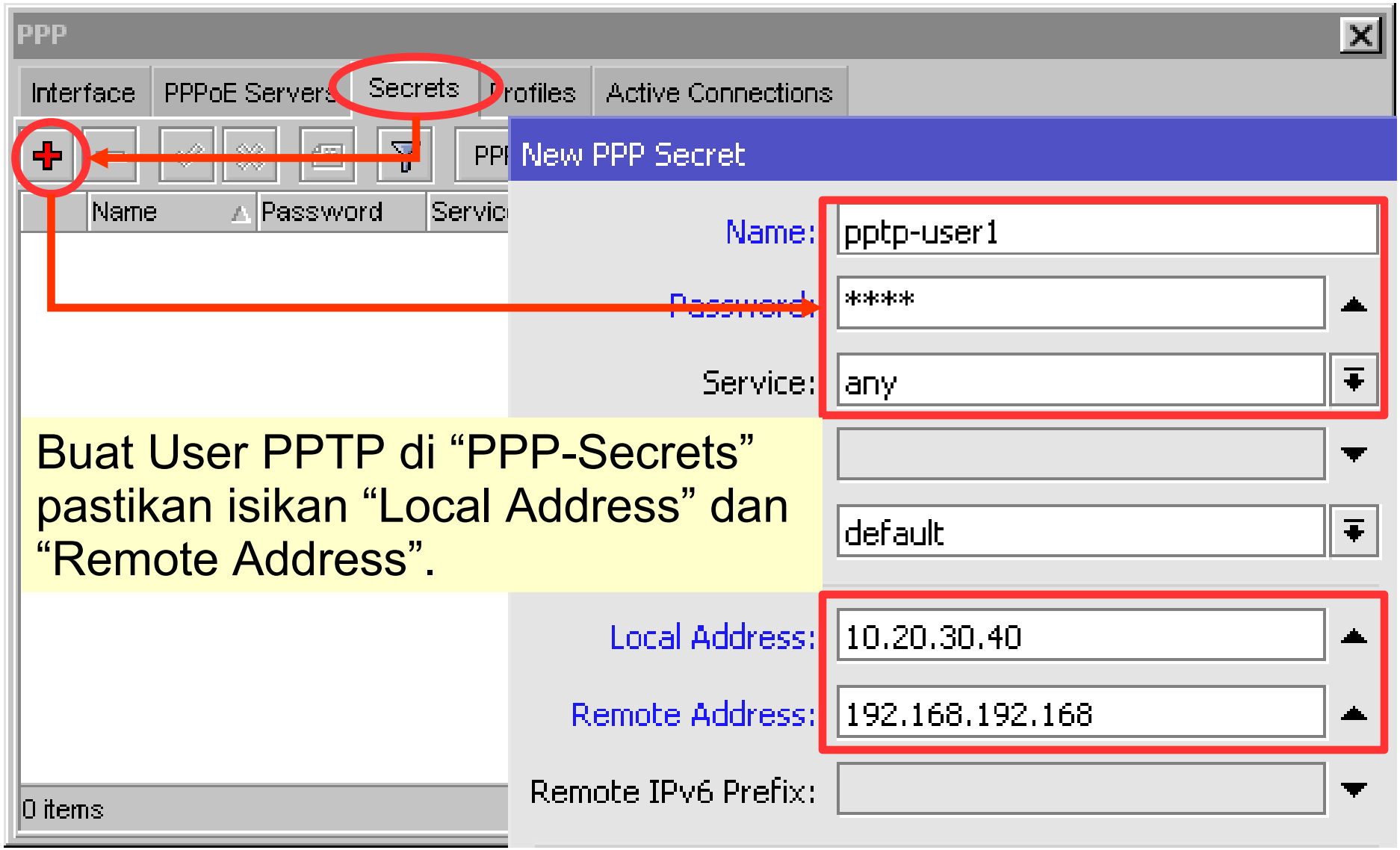
- **Service** PPTP server bisa diaktifkan pada PPP configuration
- **Default Profile** digunakan untuk menetukan group dan memberikan konfigurasi dasar seperti ip address, penggunaan enkripsi dan juga limitasi user
- Default Profile digunakan untuk user-user yang tidak terdapat di database local router contohnya jika autentikasi user menggunakan RADIUS.

[LAB-2] PPTP Tunnels - Server

Aktifkan PPTP server, pastikan menggunakan profile “default-encryption” supaya link VPN terenkripsi.



[LAB-2] PPTP Tunnels - Server



Buat User PPTP di “PPP-Secrets” pastikan isikan “Local Address” dan “Remote Address”.

PPP - Secret

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

PPPoE - Point to Point Protocol over Ethernet

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

PPPoE Server