

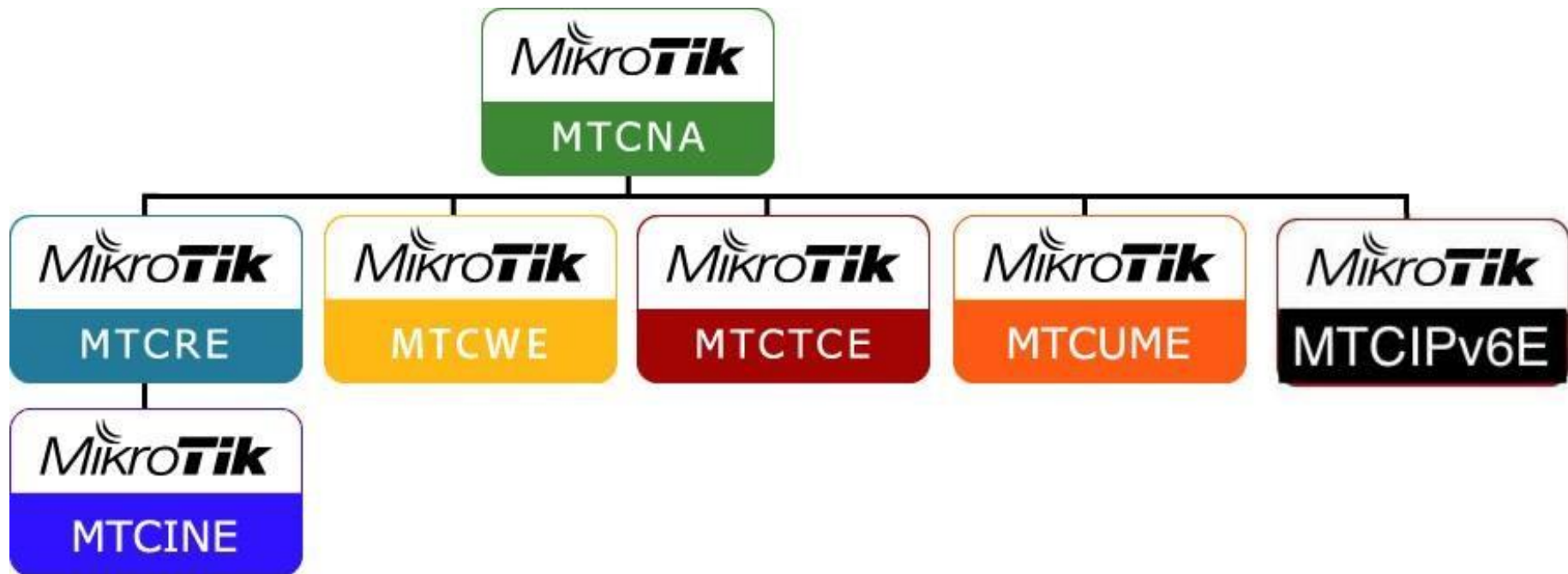


**Certified Network Associate
(MTCNA)**

Tujuan Training

- Memperkenalkan dan memberikan gambaran tentang RouterOS dan Produk-produk RouterBOARD
- Mempelajari dan memahami MikroTik router Konfigurasi, maintenance dan dasar troubleshooting
- Mendapatkan kualifikasi sebagai MikroTik Certified Network Associate

Sertifikat Mikrotik



- Sertifikat berjenjang wajib telah lulus ujian MTCNA jika ingin mengikuti training advance (level engineer)
- Masa Berlaku Sertifikat 3 tahun, dan dapat diperpanjang

Tentang Ujian MikroTik

- Online test terdiri dari 25 soal dalam waktu 1 jam
- Dinyatakan lulus jika hasil nilai ujian diatas 60%
- Jika mendapatkan nilai 50%-59% mendapatkan kesempatan mengulang ujian langsung
- Bagi yang mendapatkan nilai dibawah 50% maka akan diberikan kesempatan mengulang dalam waktu 3 bulan berikutnya

MTCNA Outline

- Module 1 : Introduction
- Module 2 : Wireless
- Module 3 : Bridging
- Module 4 : DHCP
- Module 5 : Routing
- Module 6 : Firewall

MTCNA Outline

- Module 7 : Quality of Service
- Module 8 : Tunnels
- Module 9 : Misc
- More detail outline available on mikrotik.com



**Certified Network Associate
(MTCNA)**

Module 1

Introduction

Tentang Mikrotik

- 1996: Established
- 1997: RouterOS software for x86 (PC)
- 2002: First RouterBOARD device
- 2006: MUM Pertama diadakan di Prague, Czech Republic
- 2015: MUM Indonesia, 2500+

Tentang Mikrotik

- Lokasi: Riga, Latvia (Eropa Utara)
- Produsen router software dan hardware
- Moto: Routing the world
- Produk banyak digunakan oleh ISP, perusahaan dan personal



MikroTik RouterOS

- Operating system yang digunakan sebagai pendukung RouterBOARD hardware
- Berbasis Linux
- Bisa Install di PC maupun pada virtual mesin (VM)

Fitur RouterOS

- Full 802.11 a/b/g/n/ac support
- Routing (BGP, OSPF, RIP, ...)
- Firewall/Bandwidth shaping
- Tunneling (PPTP, PPPoE, SSTP, OpenVPN, ...)
- DHCP/Proxy/Hotspot
- dan masih banyak lagi... see: wiki.mikrotik.com

Mikrotik RouterBOARD

- Built-in hardware yang menggunakan RouterOS sebagai system operasi nya
- Tersedia dari low-end hingga high-end Router
- Ready to use and custom RouterBOARD



RouterBOARD type

- RouterBOARD memiliki sistem kode tertentu
 - U - dilengkapi dengan USB
 - A - Advance, biasa nya digunakan level4 keatas
 - H - High Performance, Processor lebih tinggi
 - G - dilengkapi dengan Gigabit ethernet
 - n - 802.11n support
 - D - Dual Chain
 - More detail ... See: wiki.mikrotik.com

RB751

→ Seri / Kelas Router

→ Jumlah Slot MiniPCI / Wireless

→ Jumlah Port Ethernet

Arsitektur RouterBOARD

- Arsitektur RouterBOARD dibedakan berdasarkan jenis Processor pada instalasi RouterOS

RouterOS

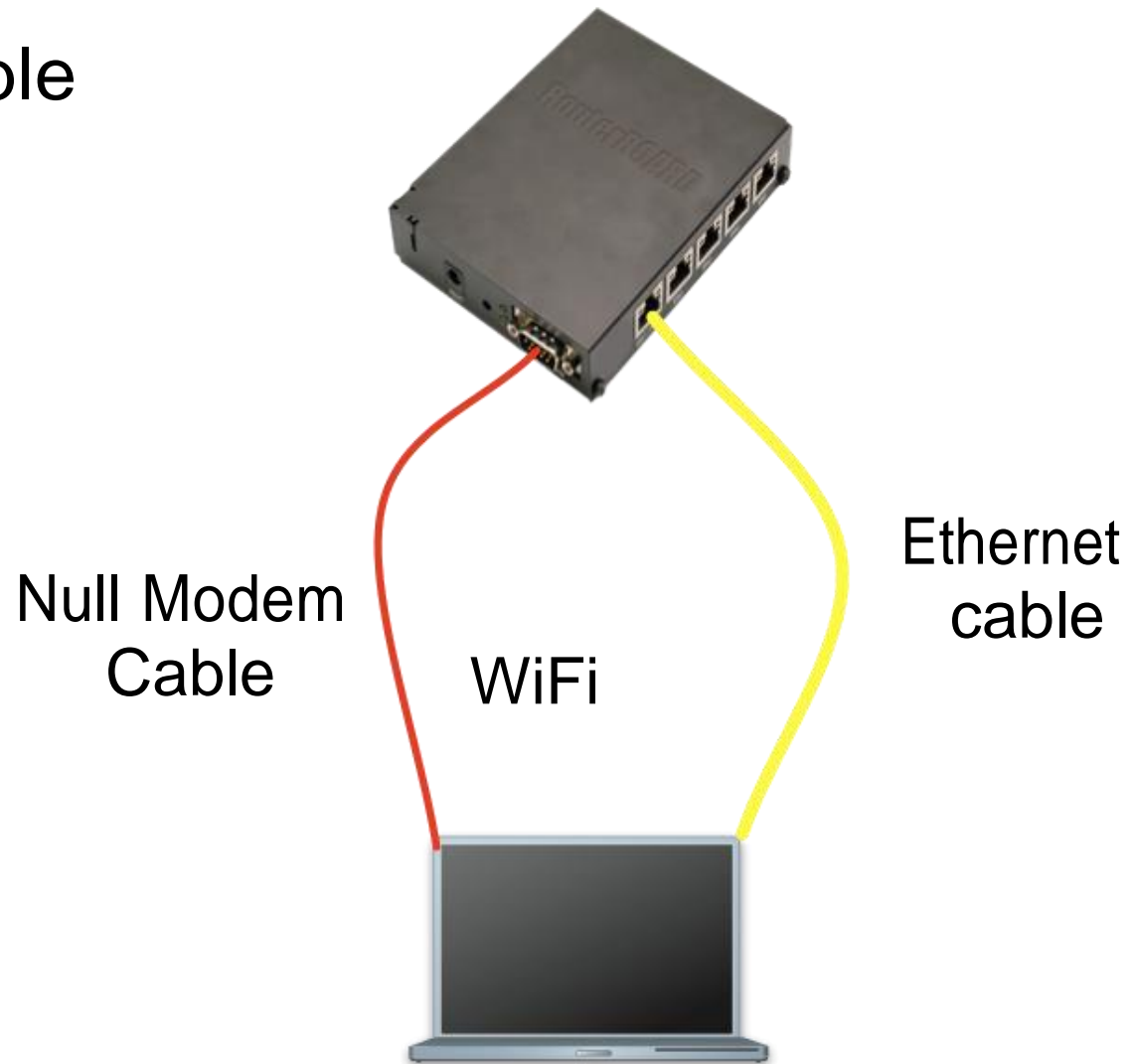


	6.36.4 (Bugfix only)	6.37.3 (Current)	5.26 (Legacy)	6.38rc45 (Release candidate)
MIPSBE	CRS, NetBox, NetMetal, PowerBox, QRT, RB9xx, hAP, hAP ac, hAP ac lite, mAP, RB4xx, cAP, hEX, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx			
Main package				
Extra packages				
SMIPS	hAP lite			
Main package			-	
Extra packages			-	
TILE	CCR			
Main package			-	
Extra packages			-	
The Dude server			-	
PPC	RB3xx, RB600, RB8xx, RB1xxx			
Main package				
Extra packages				

- More detail ... See: mikrotik.com/download

Akses ke RouterOS

- Null modem cable
- Ethernet cable
- Wifi

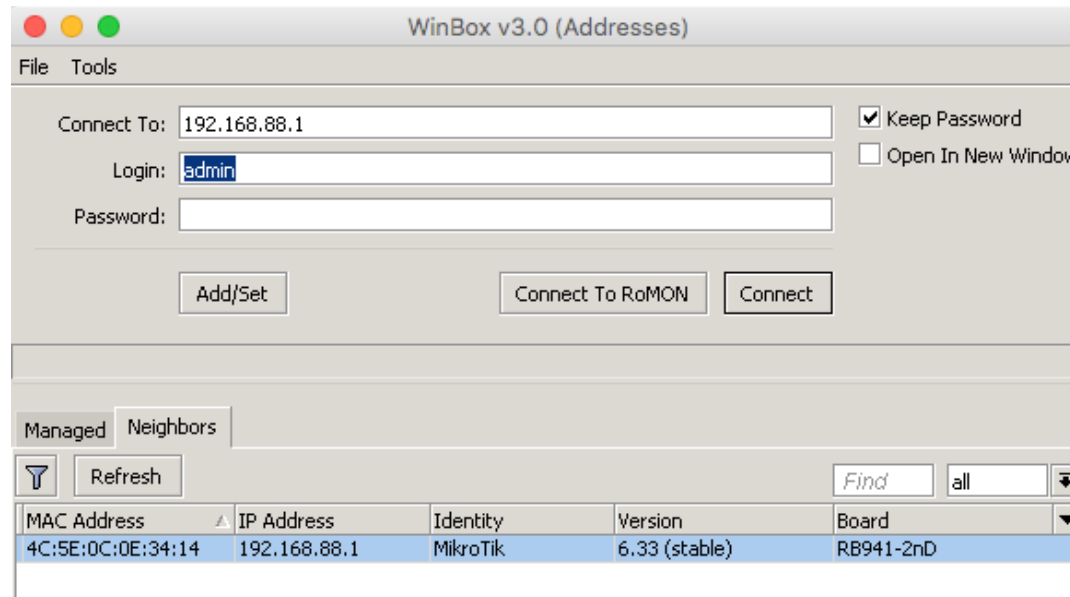


Akses ke RouterOS

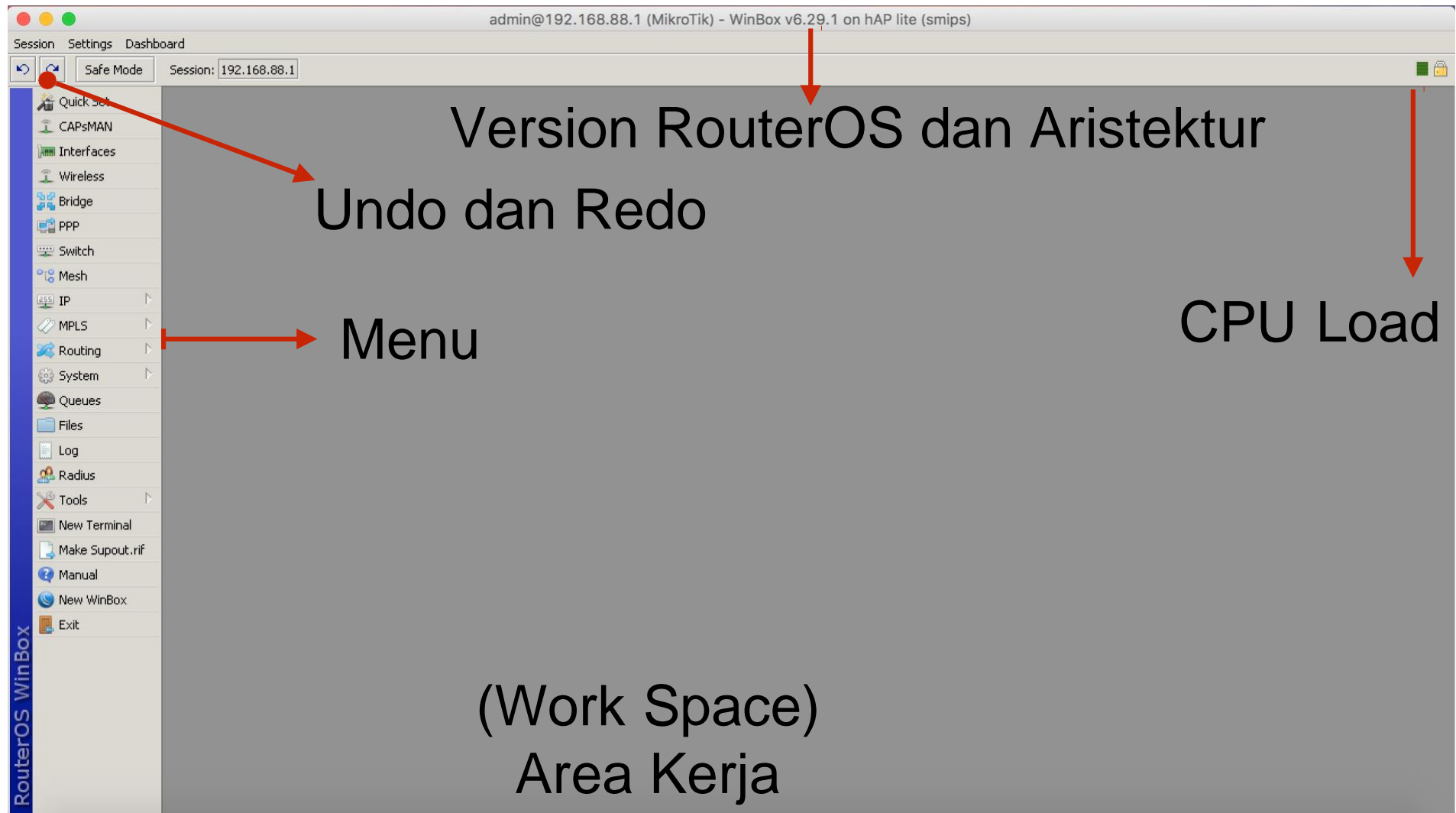
Akses via	Koneksi	CLI	GUI	Need IP
Keyboard	Monitor PC langsung	yes		
Serial Console	Kabel Serial	yes		
Telnet & SSH	Layer 3	yes		yes
Winbox	Menggunakan OS Windows, MAC OSX atau Linux (emulator wine)	yes	yes	yes
FTP	FTP Client (FileZilla, etc)		yes	yes
API	Socket Programing			yes
WEB	Layer 3	yes	yes	yes
MAC-Winbox	Layer 2	yes	yes	
MAC-Telnet	Layer 2	yes		

WinBox

- Default IP address (LAN side): 192.168.88.1
- User: admin
- Password: (blank)

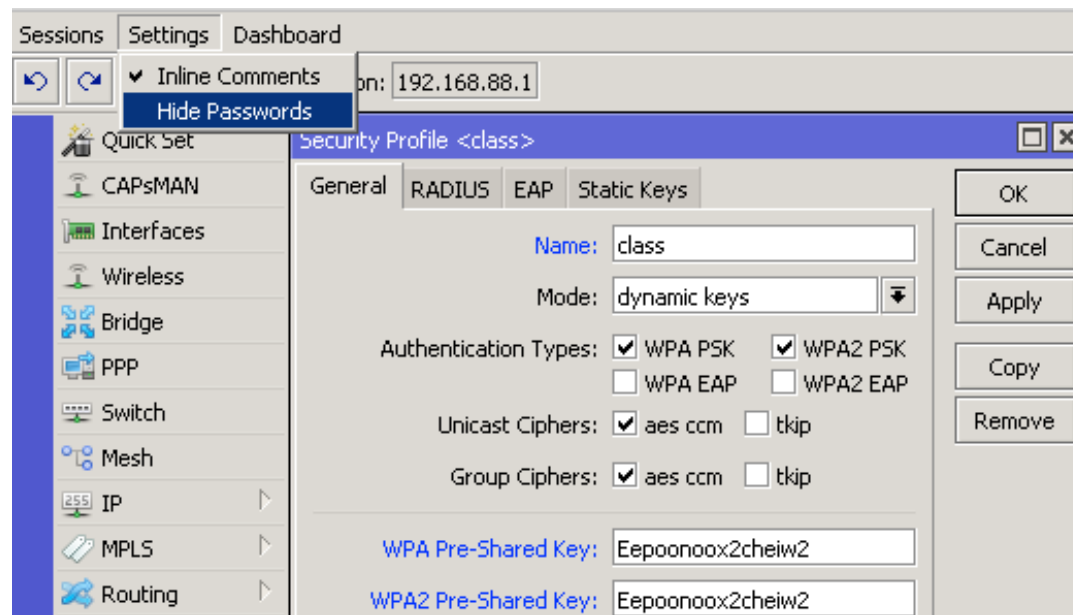


WinBox



WinBox Tip

- Untuk Membuka atau melihat password yang tersembunyi dapat dilakukan pada menu settings>Hide Passwords



Wireless → Security Profiles

WinBox

- Download winbox, bisa dilakukan pada router atau pada web mikrotik.com/download
- Cobalah akses menggunakan MAC address pada winbox
- Cobalah Akses menggunakan IP address pada winbox

WebFig

- Browser - <http://192.168.88.1>



The image shows the WebFig login interface for MikroTik RouterOS v6.33. The interface is light gray with a white central panel. At the top right is the MikroTik logo. Below it, the text "RouterOS v6.33" is displayed. A warning message states: "You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator." The "WebFig Login:" section contains a "Login:" label, a text input field with "admin", a "Login" button, a "Password:" label, and a password input field with a key icon and a checkmark. Below the login fields is a row of five icons: Winbox (blue sphere), Telnet (terminal), Graphs (green square), License (document), and Help (red lifebuoy). The copyright notice "© mikrotik" is at the bottom right.

MikroTik


RouterOS v6.33

You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.

WebFig Login:

Login:

Password: 

 Winbox  Telnet  Graphs  License  Help

© mikrotik

Quick Set

- Dasar konfigurasi router secara cepat dan mudah
- Dapat dilakukan pada winbox dan webfig

Quick Set

CPE Quick Set

CPE
Home AP
PTP Bridge
WISP AP

ess: 4C:5E:0C:0E:34:17

LAN MAC Address: 4C:5E:0C:0E:34:13

Wireless

Status: connected to ess

AP MAC: 4C:5E:0C:0A:0F:A3

Network Name: 3rd_fl

Tx/Rx Signal Strength: -42/-43 dBm

Tx/Rx CCQ: 47/46 %

Signal To Noise: 66 dB

Wireless Protocol: 802.11

Rx Signal: -43 dB
Tx Signal: -42 dB

Disconnect

Configuration

Mode: ☒ Router ☐ Bridge

Wireless Network

Address Acquisition: ☐ Static ☒ Automatic ☐ PPPoE

IP Address: 10.5.120.244 Renew Release

Netmask: 255.255.255.0 (/24)

Gateway: 10.5.120.1

Upload: unlimited bits/s

Download: unlimited bits/s

Local Network

IP Address: 192.168.88.1

Netmask: 255.255.255.0 (/24)

☒ DHCP Server

DHCP Server Range: 192.168.88.10-192.168.88.254

☒ NAT

System

Router Identity: MikroTik

Check For Updates Reset Configuration

Password:

Confirm Password:

OK
Cancel
Apply

Default Configuration

- Default Konfigurasi RouterOS ether2-5 mode switch dan bridge-local dengan wlan
- IP default 192.168.88.1
- Default Konfigurasi akan muncul pada winbox pada saat pertama kali dibuka

Command Line Interface

- Dapat dilakukan dengan SSH, Telnet atau New Terminal pada WinBox dan WebFig

```
MMM   MMM   KKK                               TTTTTTTTTT   KKK
MMM MMM 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 6.33 (c) 1999-2015      http://www.mikrotik.com/

[?]           Gives the list of available commands
command [?]   Gives help on the command and list of arguments

[Tab]         Completes the command/word. If the input is ambiguous,
               a second [Tab] gives possible options

/             Move up to base level
..           Move up one level
/command      Use command at the base level

[admin@MikroTik] > █
```

Command Line Interface

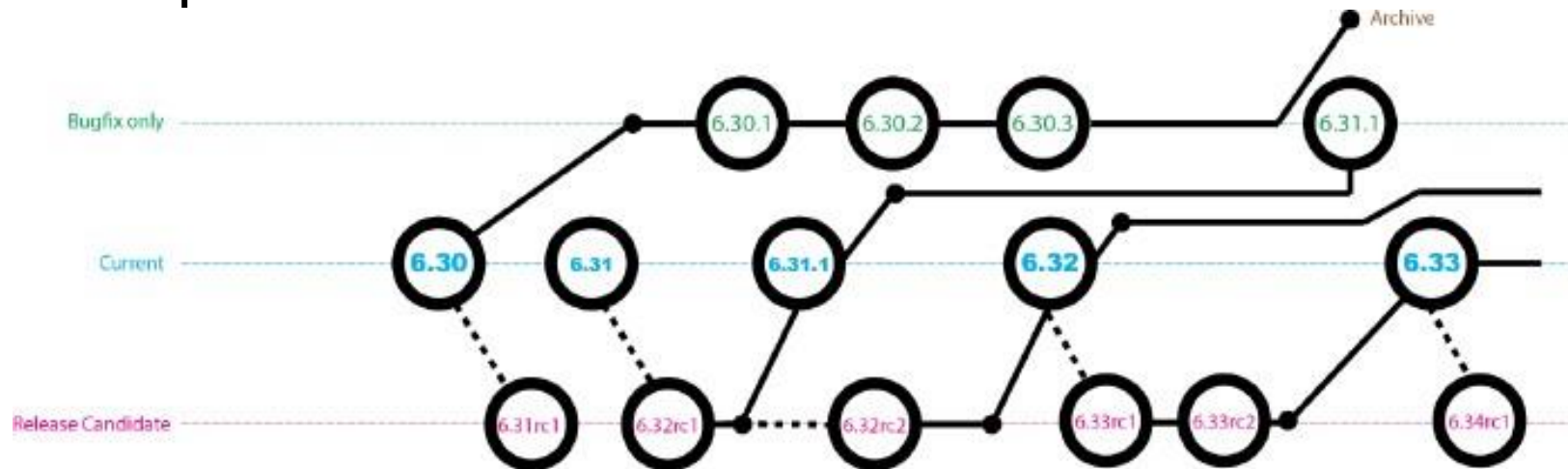
- **<tab>** completes command
- **Double <tab>** shows available commands
- **'?'** Shows help
- Navigate previous commands with **<↑>**, **<↓>** buttons

Command Line Interface

- Gunakan Command telnet, atau program putty ssh/telnet client untuk windows OS
- Lakukan perintah dasar CLI MikroTik superit **<tab>** dan lainnya

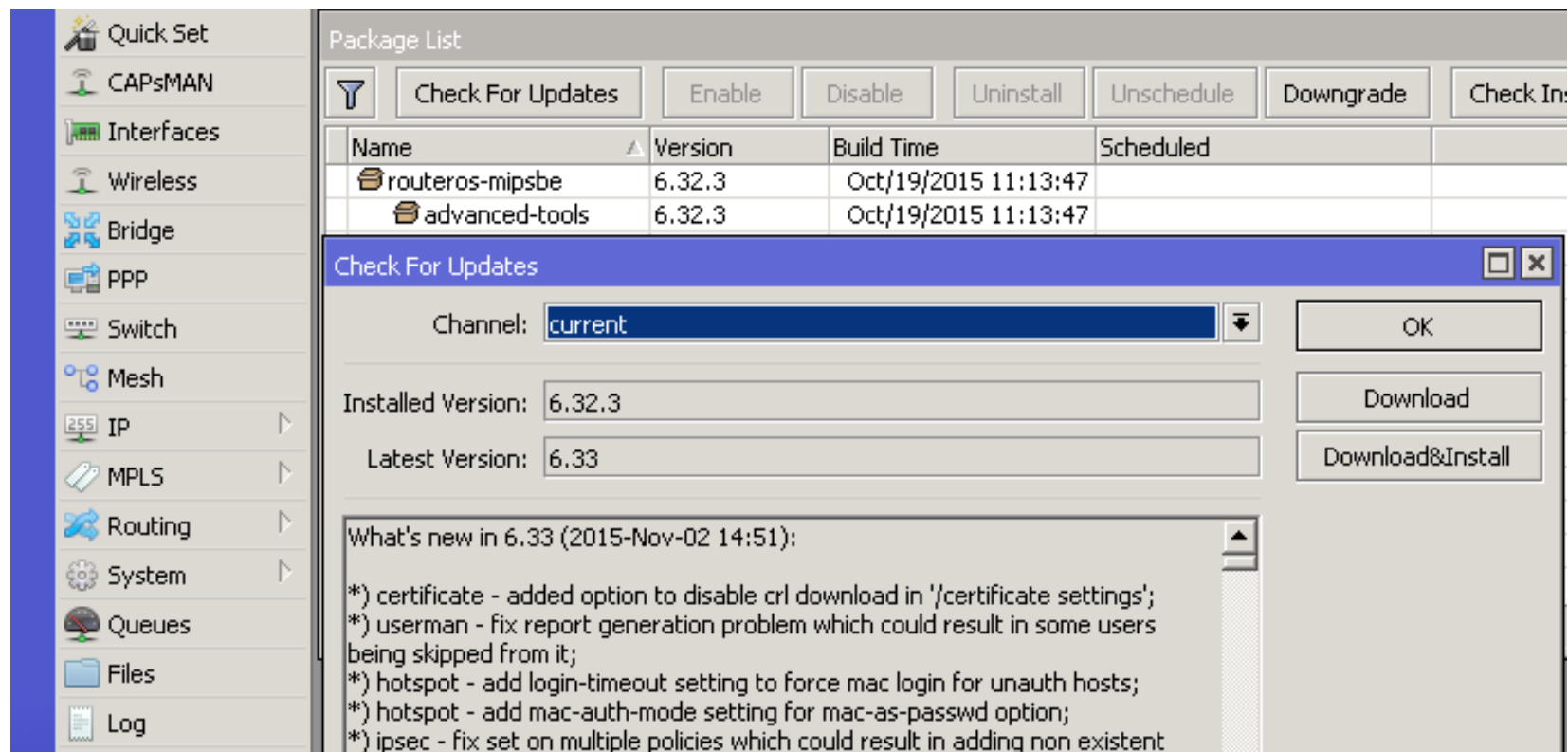
RouterOS Releases

- Bugfix only (long-term) - perbaikan, tidak ada fitur baru
- Current (stable) - perbaikan yang sama + fitur baru
- Release Candidate (testing) - Proses perancangan untuk perbaikan dan fitur



Upgrading the RouterOS

- Cara termudah untuk upgrade RouterOS



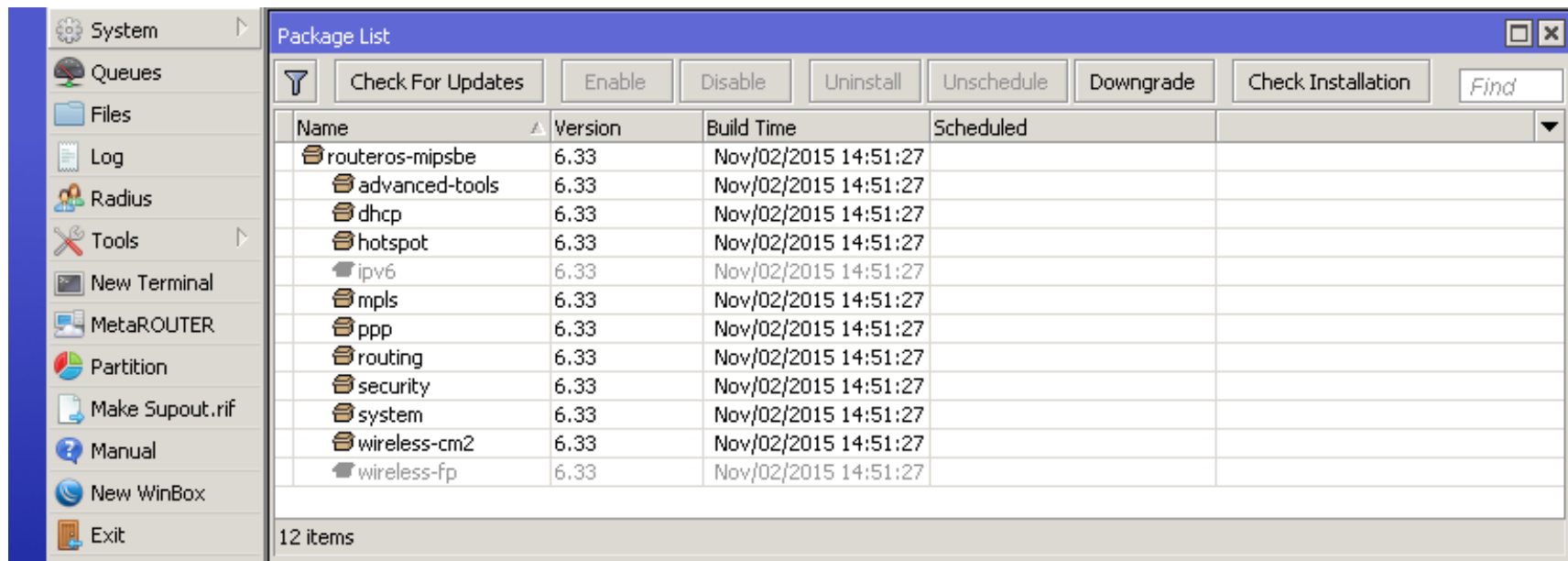
System → Packages → Check For Updates

Upgrading the RouterOS

- Update dapat dilakukan dengan cara drag&drop file .npk yang telah kita download ke dalam WinBox
 - Atau dapat dilakukan upload file .npk melalui WebFig Files menu, FTP, sFTP
- Download file di mikrotik.com/download page
 - cek arsitektur yang disupport pada router
- Reboot the Router

Package Management

- RouterOS package dapat kita aktifkan atau non aktif dengan cara enable/disable



System → Packages

RouterOS Packages

Package	Functionality
advanced-	Netwatch, wake-on-LAN
dhcp	DHCP client and server
hotspot	HotSpot captive portal server
ipv6	IPv6 support
ppp	PPP, PPTP, L2TP, PPPoE clients and servers
routing	Dynamic routing: RIP, BGP, OSPF
security	Secure WinBox, SSH, IPsec
system	Basic features: static routing, firewall, bridging,
wireless-cm2	802.11 a/b/g/n/ac support, CAPsMAN v2

- For more info see [packages wiki page](#)

RouterOS Packages

- RouterOS Package dapat ditambahkan dan dihilangkan install/uninstall
- Extra Package dapat di download di mikrotik.com/download pilih extra package
- Package yang terinstall tanpa extra package (bundling) secara default tidak dapat di uninstall

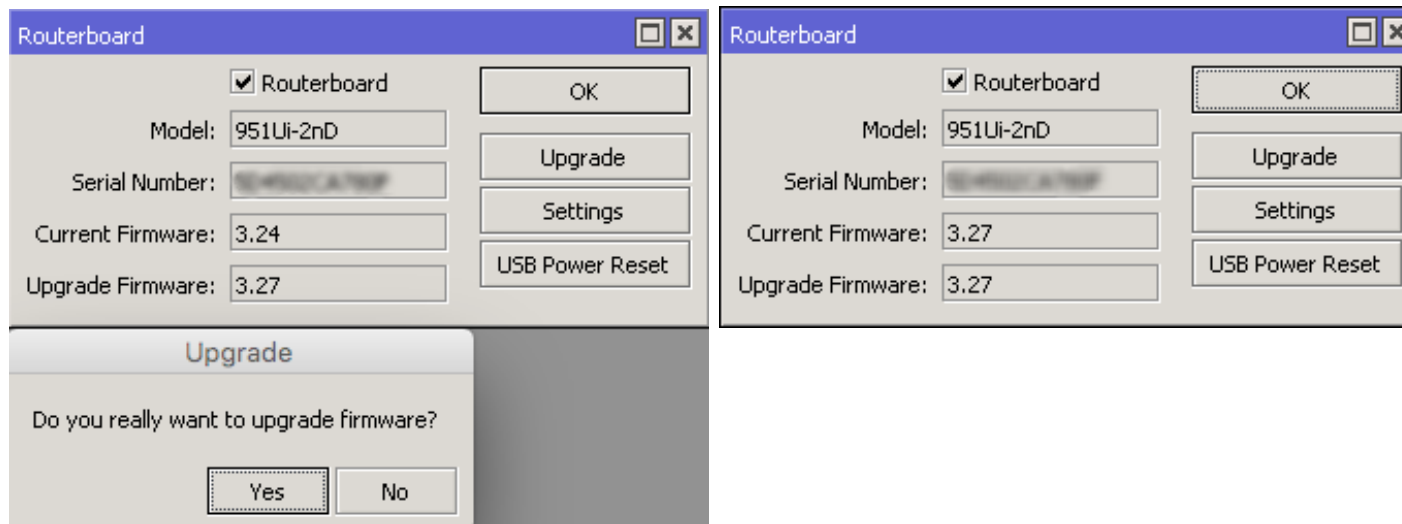
Package Management

- Disable wireless package
- Reboot router anda
- Apa yang terjadi pada router tersebut
- Enable kembali wireless package
- Reboot kembali router anda

Package Management

- download extra package file yang arsitektur CPU sesuai dengan router anda
 - Pastikan versi package pada router anda sama dengan versi package yang akan ditambahkan pada router
- Tambahkan/Install package baru pada router anda
- Upload file yang telah di download dengan metode drag&drop maupun FTP

RouterBOOT

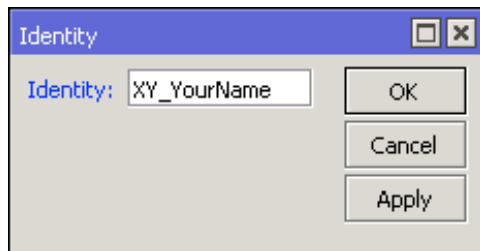


System → Routerboard

- For more info see [RouterBOOT wiki page](#)

Router Identity

- Merupakan Optional untuk memberikan identitas pada router kita



System → Identity

```
/                Move up to base level
..              Move up one level
/command        Use command at the base level
[admin@XY_YourName] >
```

Managed Neighbors				
Refresh				
MAC Address	IP Address	Identity	Version	Board
D4:CA:6D:E2:65:90	192.168.88.1	XY_YourName	6.33 (stable)	RB951Ui-2nD

Router Identity

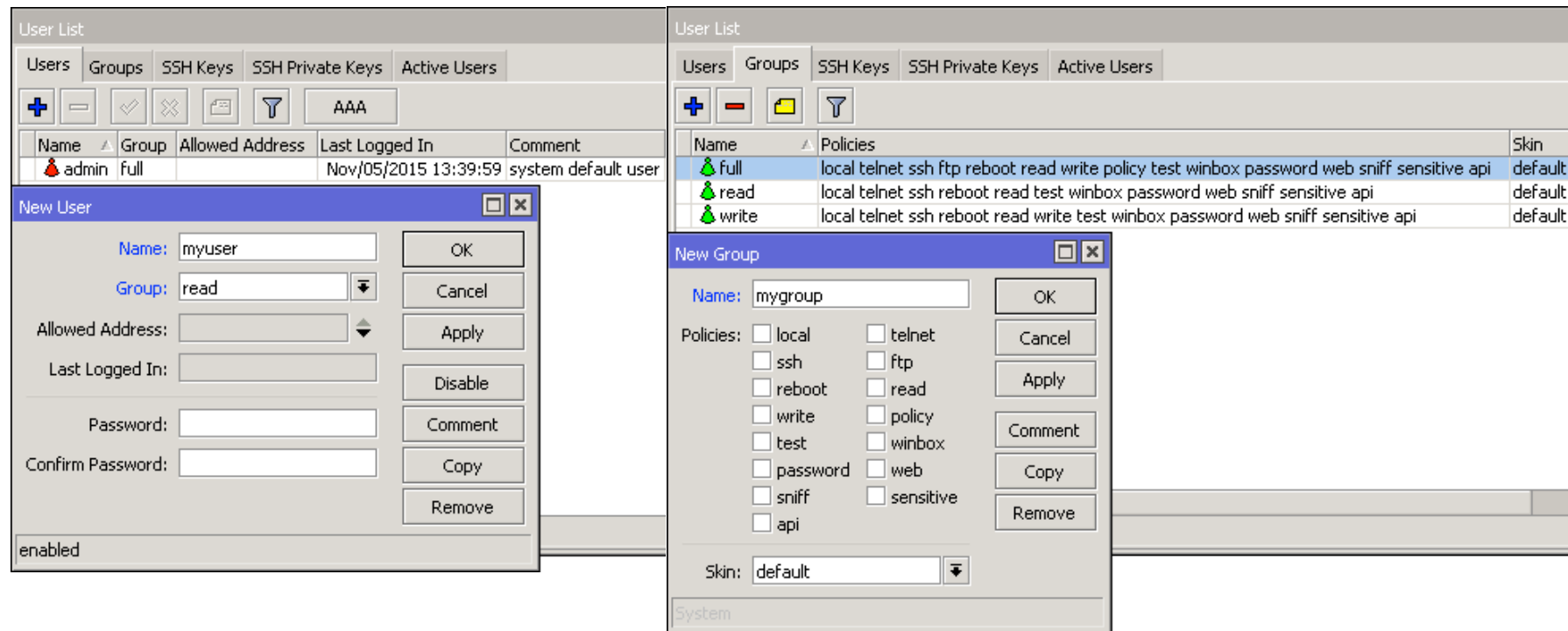
LAB

- Berilah identitas nama pada router anda
 - . NoAnda_NamaAnda
- Contoh : 01_Rivan

RouterOS Users

- Default user **admin**, group **full**
- Additional groups - **read** and **write**
- Group dapat kita custom sesuai dengan kebutuhan

RouterOS Users



The image displays the RouterOS User Management interface, showing the 'User List' and 'New User' dialog boxes. The 'User List' table shows the 'admin' user with the 'full' group. The 'New User' dialog is open, showing fields for Name, Group, Allowed Address, Last Logged In, Password, and Confirm Password. The 'New Group' dialog is also open, showing fields for Name, Policies, and Skin.

User List

Name	Group	Allowed Address	Last Logged In	Comment
admin	full		Nov/05/2015 13:39:59	system default user

New User

Name: myuser
Group: read
Allowed Address:
Last Logged In:
Password:
Confirm Password:
Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

New Group

Name: mygroup
Policies:
Skin: default
Buttons: OK, Cancel, Apply, Comment, Copy, Remove

System → Users

RouterOS Users

- Buatlah User baru pada router anda dengan group **full access**
- Rubahlah group user **admin** dengan group **read**
- Logout user admin yang sebelumnya
- Login kembali dengan user admin
- Lakukan perubahan atau tambah konfigurasi (apakah bisa dilakukan)

RouterOS Services

- Merupakan additional Firewall
- Dapat merubah port default atau men-disable service yang tidak kita gunakan
- Allow IP “Available from”

	Name	Port	Available From	Certificate	
X	• api	8728			
X	• api-ssl	8729		none	
	• ftp	21	192.168.88.5		
	• ssh	22			
	• telnet	23			
	• winbox	8291			
	• www	80			
X	• www-ssl	443		none	

8 items

IP → Services

RouterOS Services

LAB

- Lakukan disable pada service www
- Lakukan akses router menggunakan browser http
- Apakah kita dapat mengakses router kita?

Configurasi Backup

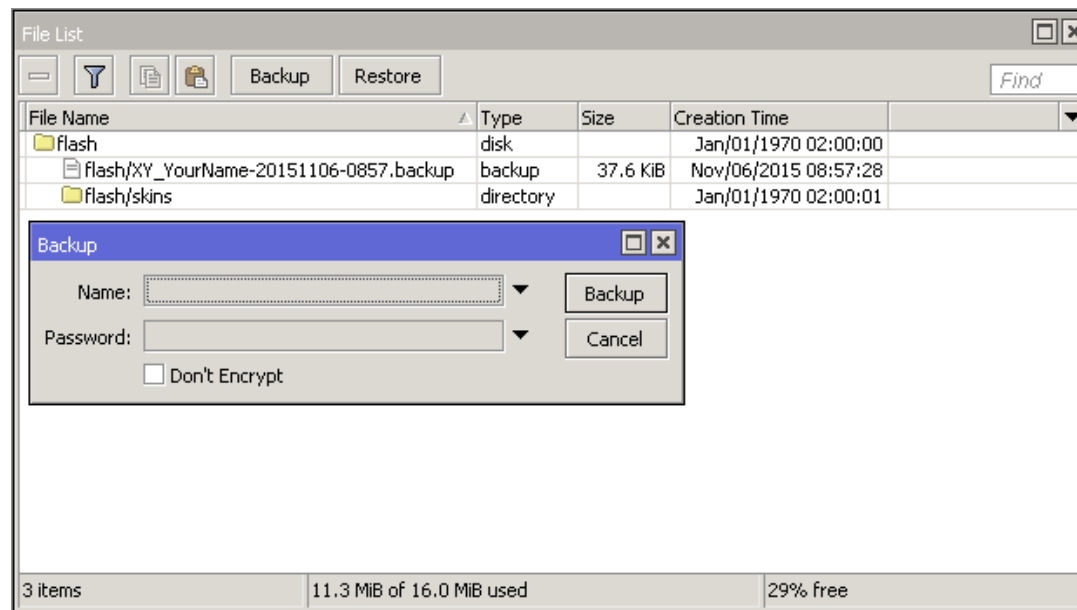
- Terdapat dua type cara backup
- Backup (.backup) file - digunakan untuk restoring konfigurasi di router yang sama
- Export (.rsc) file - digunakan untuk memindahkan konfigurasi ke router lain

Configurasi Backup

- Backup file bisa kita created and restored pada menu file di dalam WinBox
- Backup File merupakan binary, secara default terenkripsi dengan user password.
- backup File akan mengembalikan semua konfigurasi

Configurasi Backup

- Dapat memasukkan nama dan password
- Router identity dan tanggal pada saat backup akan menjadi file name backup



Configurasi Backup

- Export (.rsc) file merupakan script dengan router konfigurasi yang dapat dibackup dan direstore
- Plain-text-file (editable)
- Hanya ada konfigurasi backup yang sesuai dengan yang kita export
- Export file hanya dapat dilakukan pada command in CLI
- RouterOS user password tidak dapat dibackup
- Restore menggunakan import

Configurasi Backup

```
[admin@XY_YourName] > /export file=flash/router_conf_20151106
[admin@XY_YourName] > /file print
```

#	NAME	TYPE	SIZE	CREATION-TIME
0	flash	disk		jan/01/1970 02:00:00
1	flash/skins	directory		jan/01/1970 02:00:01
2	flash/XY_YourName-20151106-0939.backup	backup	37.6KiB	nov/06/2015 09:39:10
3	flash/router_conf_20151106.rsc	script	3595	nov/06/2015 09:40:35

```
[admin@XY_YourName] > █
```

```
[admin@XY_YourName] > /import flash/router_conf_20151106.rsc
```

Script file loaded and executed successfully

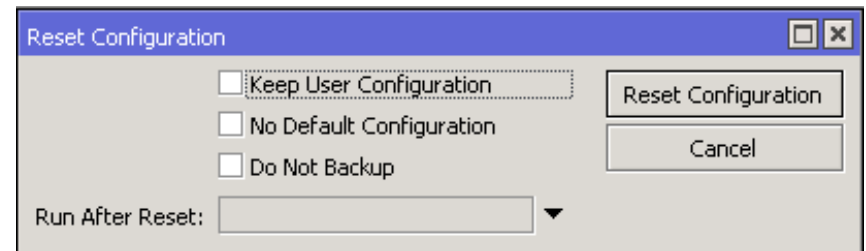
```
[admin@XY_YourName] > █
```

Configuration Backup

- Backup router pada menu file
- lalu download ke dalam pc/laptop menggunakan winbox(drag&drop), FTP atau WebFig
- Lakukan juga backup menggunakan CLI “Export”

Reset Configuration

- Reset ke default configuration
 - Soft Reset (CLI, WinBox, dll)
 - Hard Reset (Pada tombol reset RouterBOARD)



System → Reset Configuration

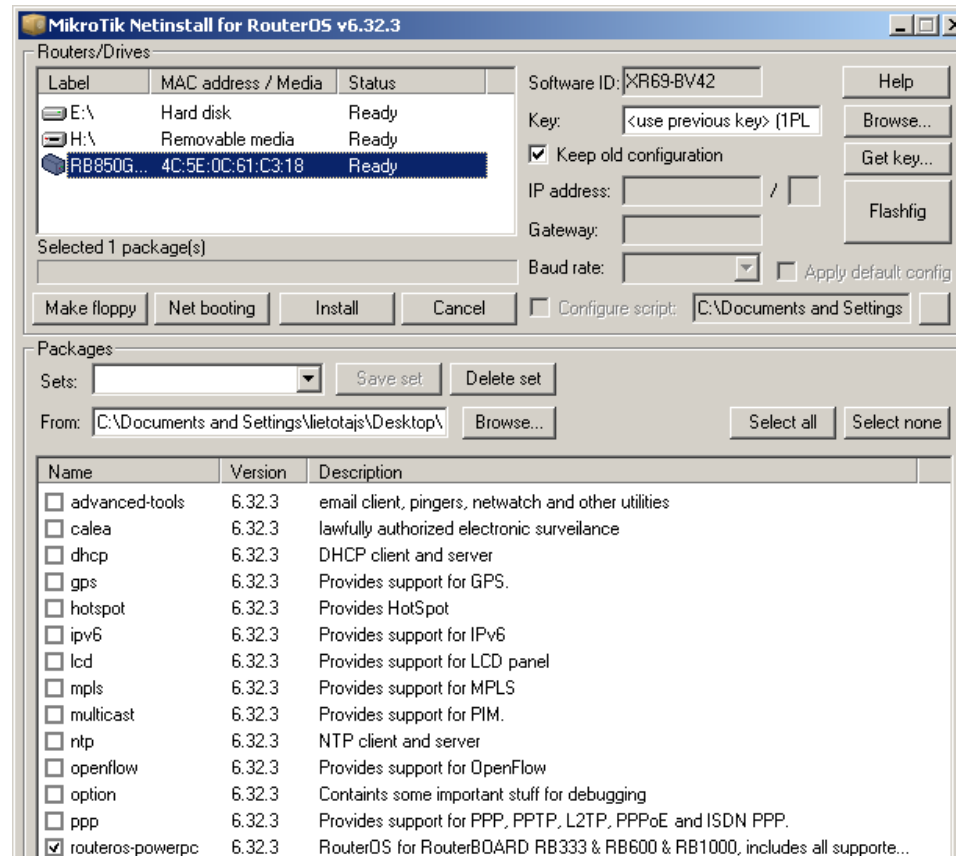
Reset Configuration

- Yang akan dilakukan jika tombol Hard Reset di router kita tekan
 - Load backup RouterBOOT loader
 - Reset router to default configuration
 - Enable CAPs mode (Controlled AP)
 - Start in Netinstall mode
- For more info see [reset button wiki page](#)

Netinstall

- Digunakan untuk install dan reinstall RouterOS
- Kabel harus langsung terhubung antara router dengan PC/Laptop
- Kabel harus connect ke ether1 (kecuali CCR dan RB1xxx - last port/ethernet)
- hanya berjalan pada OS Windows
- For more info see [Netinstall wiki page](#)

Netinstall



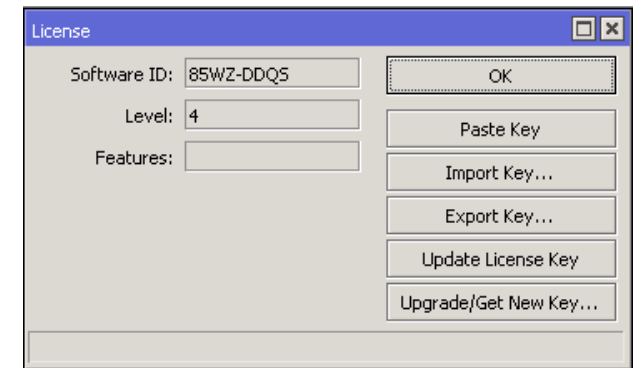
- Netinstall data di download ada mikrotik.com/download

Netinstall

- Download Netinstall
- Boot router anda menggunakan netinstall mode
- Pastikan net boot satu segment ip dengan pc/laptop
- Install RouterOS
- Restore configuration yang telah kita simpan sebelumnya

RouterOS License

- Semua perangkat RouterBOARD sudah ada lisensi nya
- Setiap License level itu berbeda (fitur)
- RouterOS license tidak akan hangus
- X86 license bisa dibeli di mikrotik.com untuk distributor dan lain - lain



System → License

RouterOS License

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

Additional Information

- wiki.mikrotik.com - RouterOS documentation and examples
- forum.mikrotik.com - communicate with other RouterOS users
- mum.mikrotik.com - MikroTik User Meeting page
- Distributor and consultant support
- support@mikrotik.com

Module 1

Summary



**Certified Network Associate
(MTCNA)**

Module 2

Wireless

Wireless

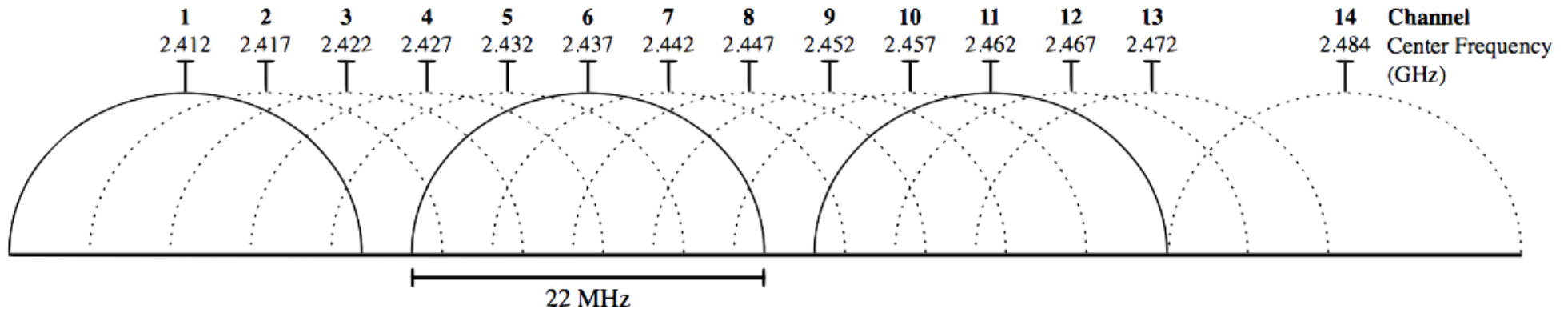
- MikroTik RouterOS mendukung kelengkapan pendukung untuk IEEE 802.11 a/n/ac (5Ghz) dan 802.11 b/g/n (2.4Ghz) wireless networking standard

Wireless Standards

IEEE Standard	Frequency	Speed
802.11a	5GHz	54Mbps
802.11b	2.4GHz	11Mbps
802.11g	2.4GHz	54Mbps
802.11n	2.4 and 5GHz	Up to 450 Mbps*
802.11ac	5GHz	Up to 1300 Mbps*

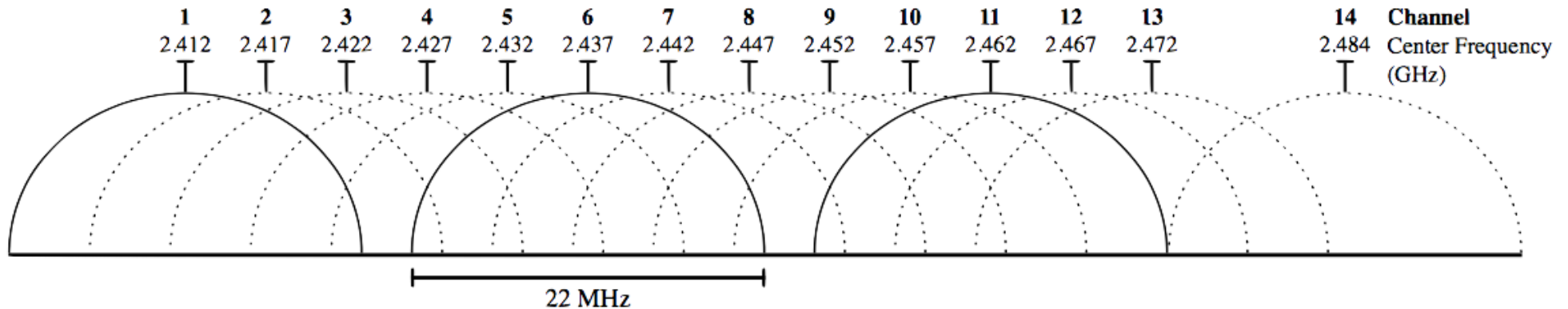
* Depending on RouterBOARD model

2.4Ghz Channels



- 13x 22Mhz channels (sebagian besar dunia)
- 3 channel yang tidal saling tumpang tindih
- 3 AP dapat menempati area yang sama tanpa mengganggu

2.4Ghz Channels



- ID: 13 channels
- Channel width:
 - 802.11b 22Mhz, 802.11g 20Mhz, 802.11n 20/40Mhz

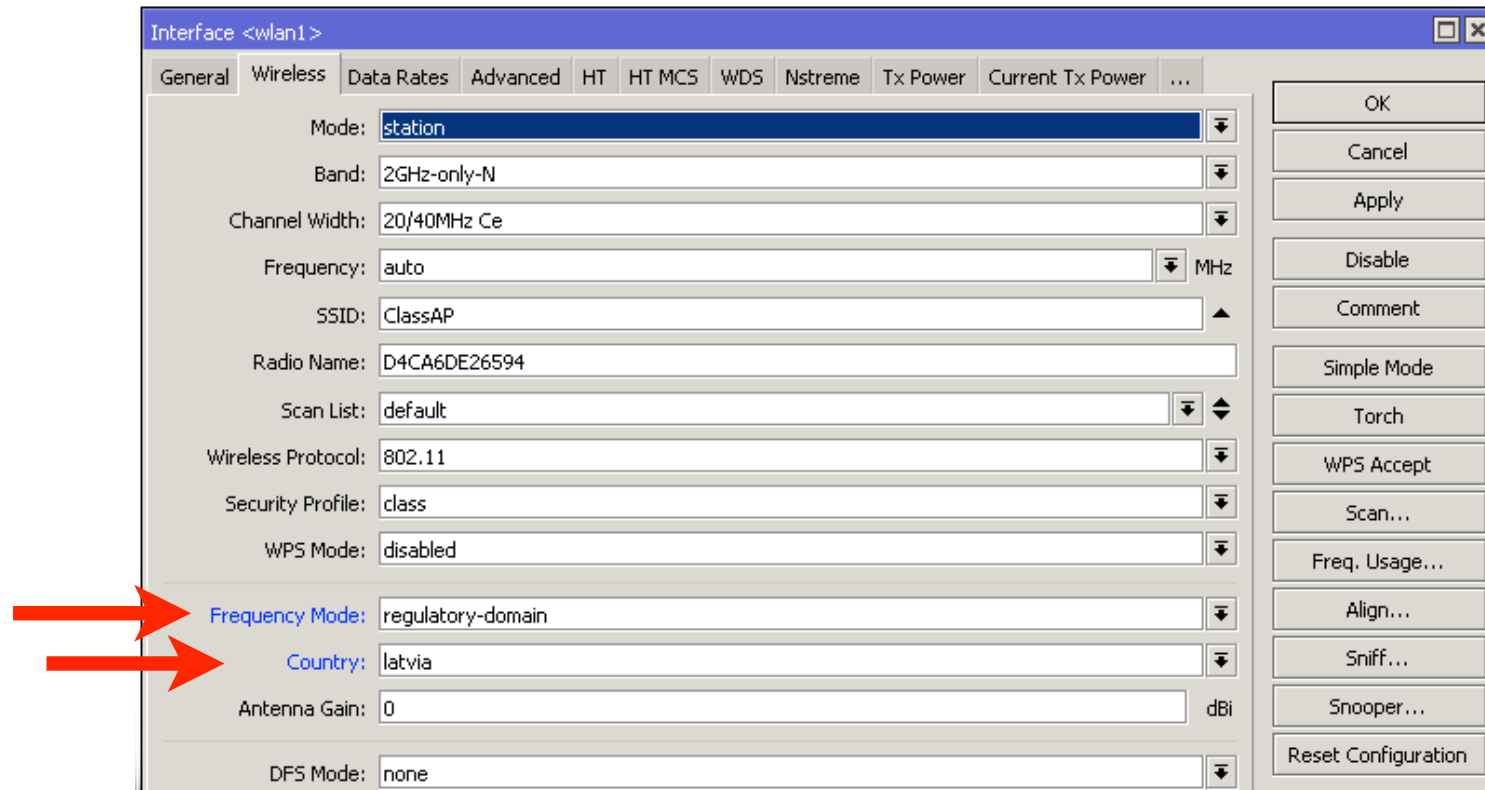
5Ghz Channels

- RouterOS mendukung full rentan frekuensi 5Ghz
- 4920-6100Mhz (tergantung pada wireless card)
- Setiap negara memiliki regulasi frekuensi masing-masing yang telah ditetapkan

5Ghz Channels

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

Country Regulation



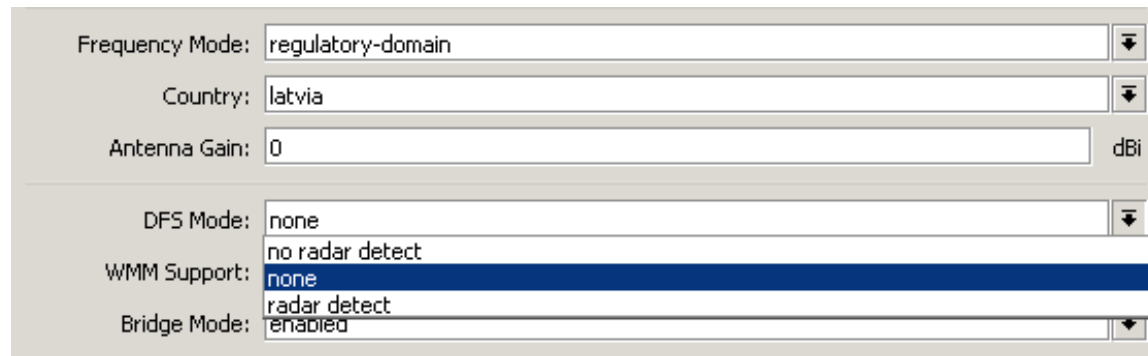
- Switch to 'Advanced Mode' and select your country to apply regulations

Country Regulations

- Dynamic Frequency Selection (DFS) adalah fitur yang merupakan sebagai identify radar ketika menggunakan band 5Ghz dan memilih channel berbeda jika radar ditemukan
- Beberapa channels hanya bisa digunakan ketika DFS enable (EU: 52-140, US: 50-144)

Country Regulations

- DFS Mode **radar detect** akan memilih channel dengan nomor yang terendah pada network yang terdeteksi dan akan digunakan jika tidak terdapat radar terdeteksi selama 60s
- Switch ke 'Advance Mode' untuk enable DFS



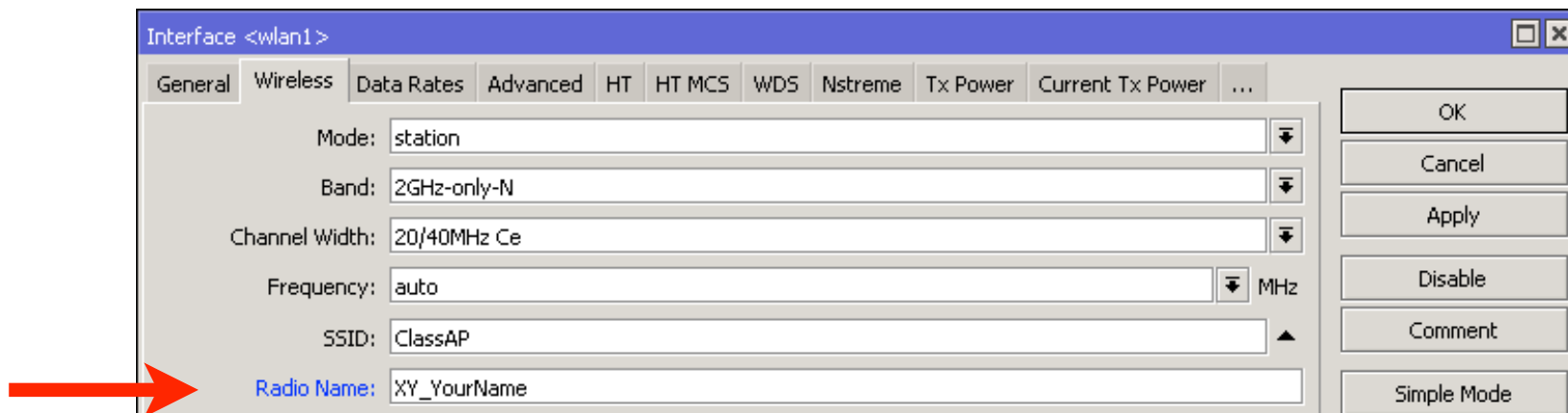
The image shows a configuration window for wireless settings. It contains several dropdown menus and text fields. The 'Frequency Mode' is set to 'regulatory-domain'. The 'Country' is set to 'latvia'. The 'Antenna Gain' is set to '0' dBi. The 'DFS Mode' dropdown is open, showing options: 'none', 'no radar detect', 'radar detect' (which is highlighted in blue), and 'enabled'. The 'WMM Support' is set to 'none'. The 'Bridge Mode' is set to 'enabled'.

Frequency Mode:	regulatory-domain
Country:	latvia
Antenna Gain:	0 dBi
DFS Mode:	none no radar detect radar detect enabled
WMM Support:	none
Bridge Mode:	enabled

Wireless

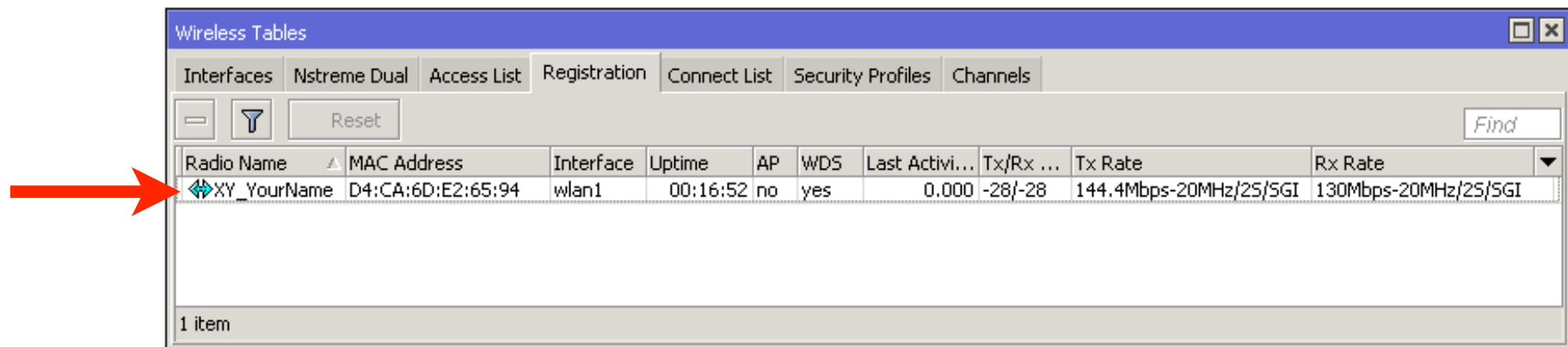
Radio Name

- Wireless interface “name”
- RouterOS - RouterOS only
- Bisa dilihat pada wireless tables



Radio Name

- Wireless interface “name”
- RouterOS - RouterOS only
- Bisa dilihat pada wireless tables



Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles Channels

[-] [Filter] [Reset] Find

Radio Name	MAC Address	Interface	Uptime	AP	WDS	Last Activi...	Tx/Rx ...	Tx Rate	Rx Rate
XY_YourName	D4:CA:6D:E2:65:94	wlan1	00:16:52	no	yes	0.000	-28/-28	144.4Mbps-20MHz/25/SGI	130Mbps-20MHz/25/SGI

1 item

Radio Name

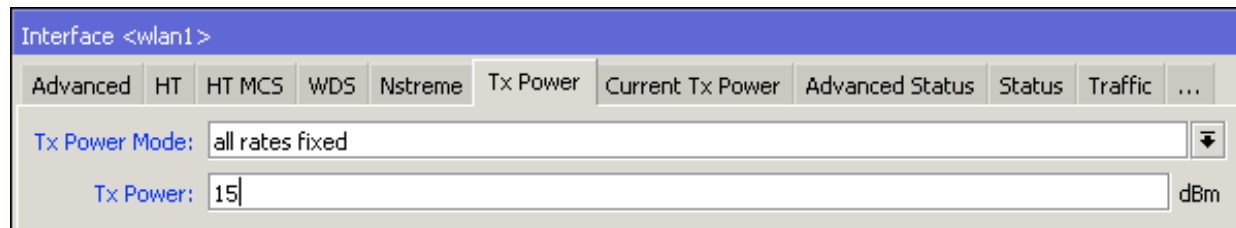
- Berilah nama identitas pada wireless masing-masing
- Contoh: 01_Rivan

Wireless Chains

- 802.11n memperkenalkan konsep MIMO (Multiple In and Multiple Out)
- Send dan Receive data menggunakan multiple radio di parallel
- 802.11n yang menggunakan satu chain (SISO) hanya bisa mencapai 72.2Mbps (pada card lawas 65Mbps)

Tx Power

- Digunakan untuk menyesuaikan power transmits pada wireless card
- Rubah ke **all rates fixed** dan sesuaikan power

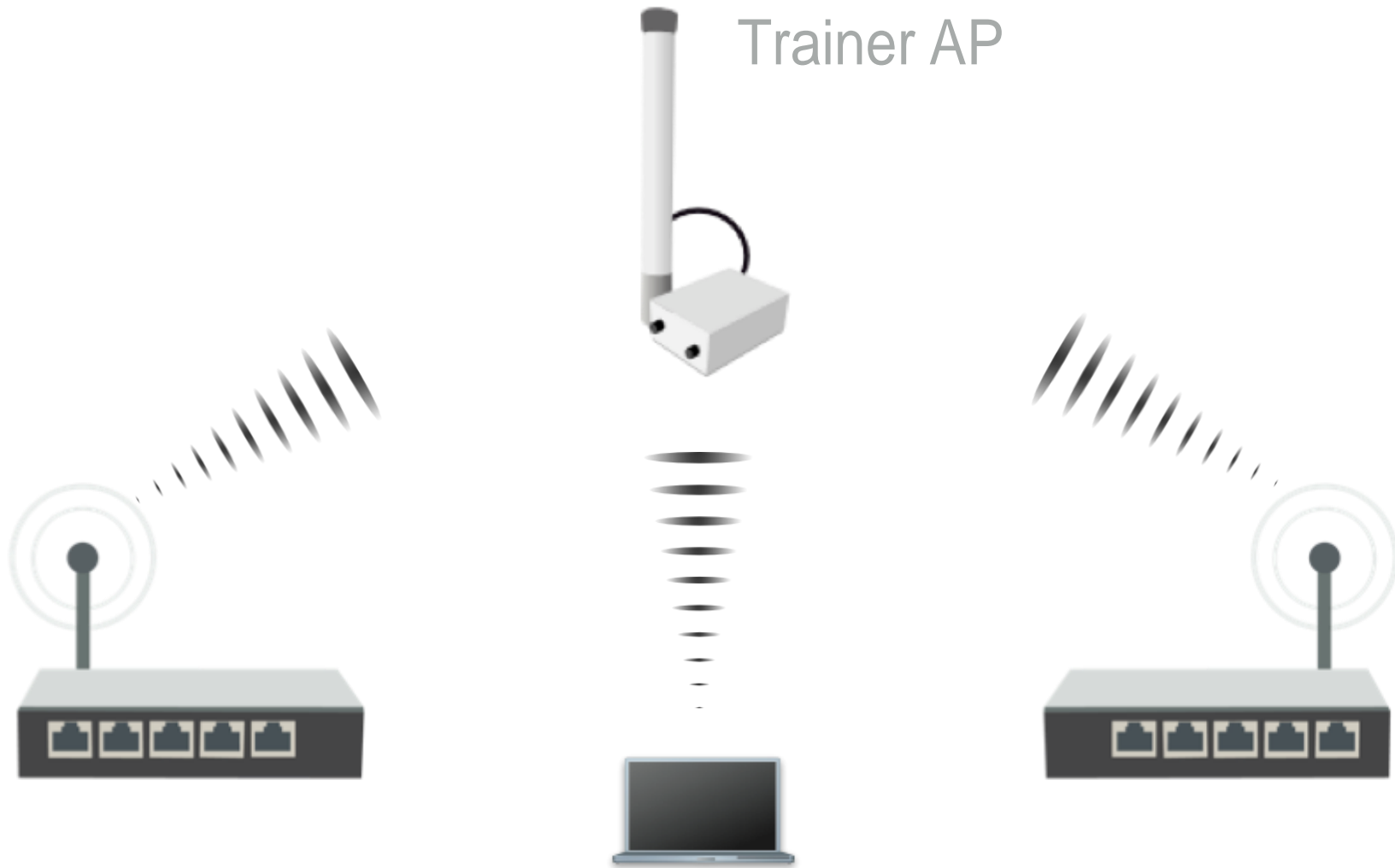


Wireless → Tx Power

Tx Power

Wireless card	Enabled Chains	Power per Chain	Total Power
802.11n	1	Equal to the selected Tx Power	Equal to the selected Tx Power
	2		+3dBm
	3		+5dBm
802.11ac	1	Equal to the selected Tx Power	Equal to the selected Tx Power
	2	-3dBm	
	3	-5dBm	

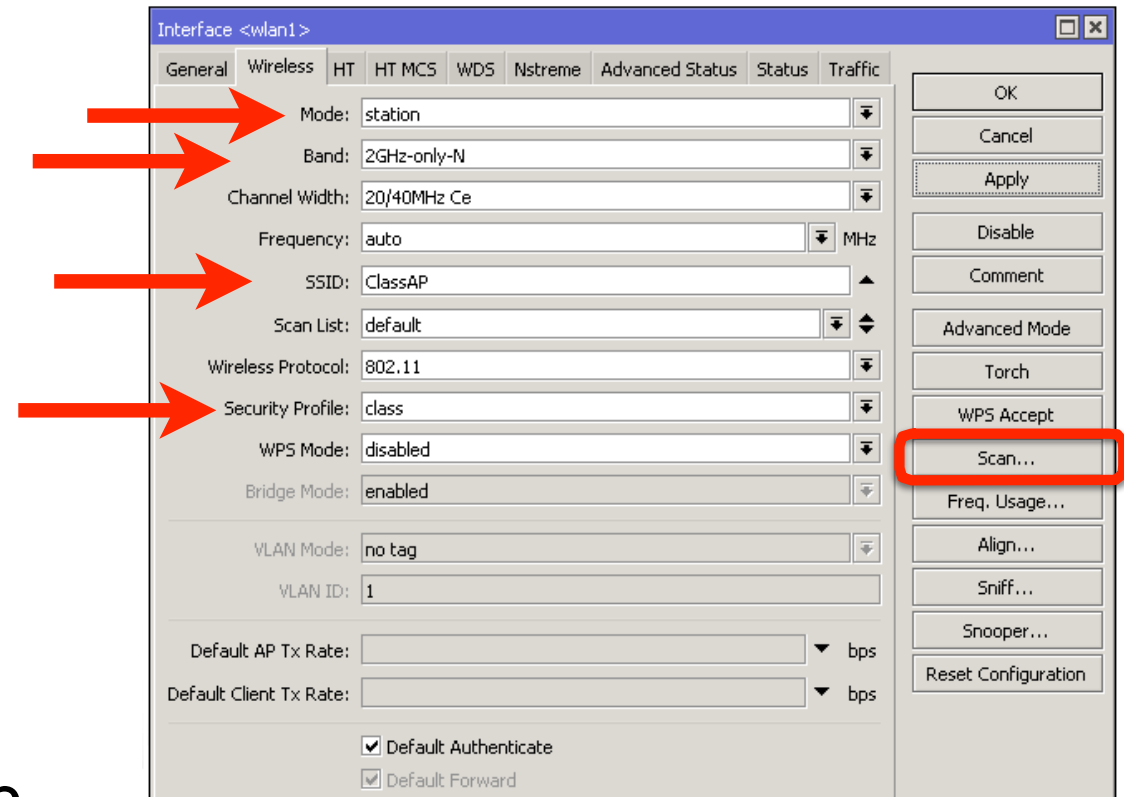
Wireless Network



Wireless stations

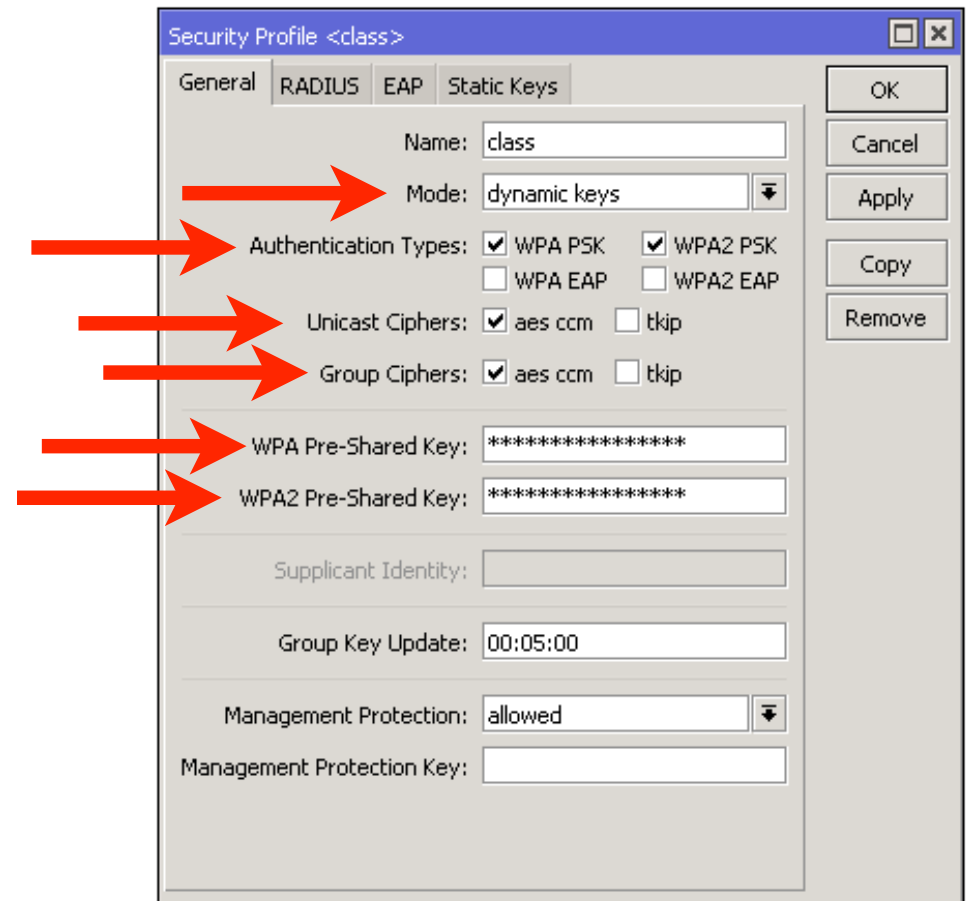
Wireless Station

- Set interface **mode=station**
- Select **band**
- Set **SSID** (wireless network ID)
- Frekuensi yang tidak penting, bisa gunakan **scan-list**



Security

- WPA dan WPA2 key secara bersamaan dapat dilakukan untuk mengizinkan spesifik koneksi dari device yang tidak didukung WPA2 juga sebaliknya
- Gunakan password yang aman (strong key)



Connect List

- Aturan penggunaan station untuk memilih (atau tidak memilih) AP

Station Connect Rule <4C:5E:0C:0A:0F:A3>

Interface: wlan1

MAC Address: 4C:5E:0C:0A:0F:A3

☒ Connect

SSID: ClassAP

Area Prefix:

Signal Strength Range: -120..120

Wireless Protocol: 802.11

Security Profile: class

enabled

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

Wireless → Connect List

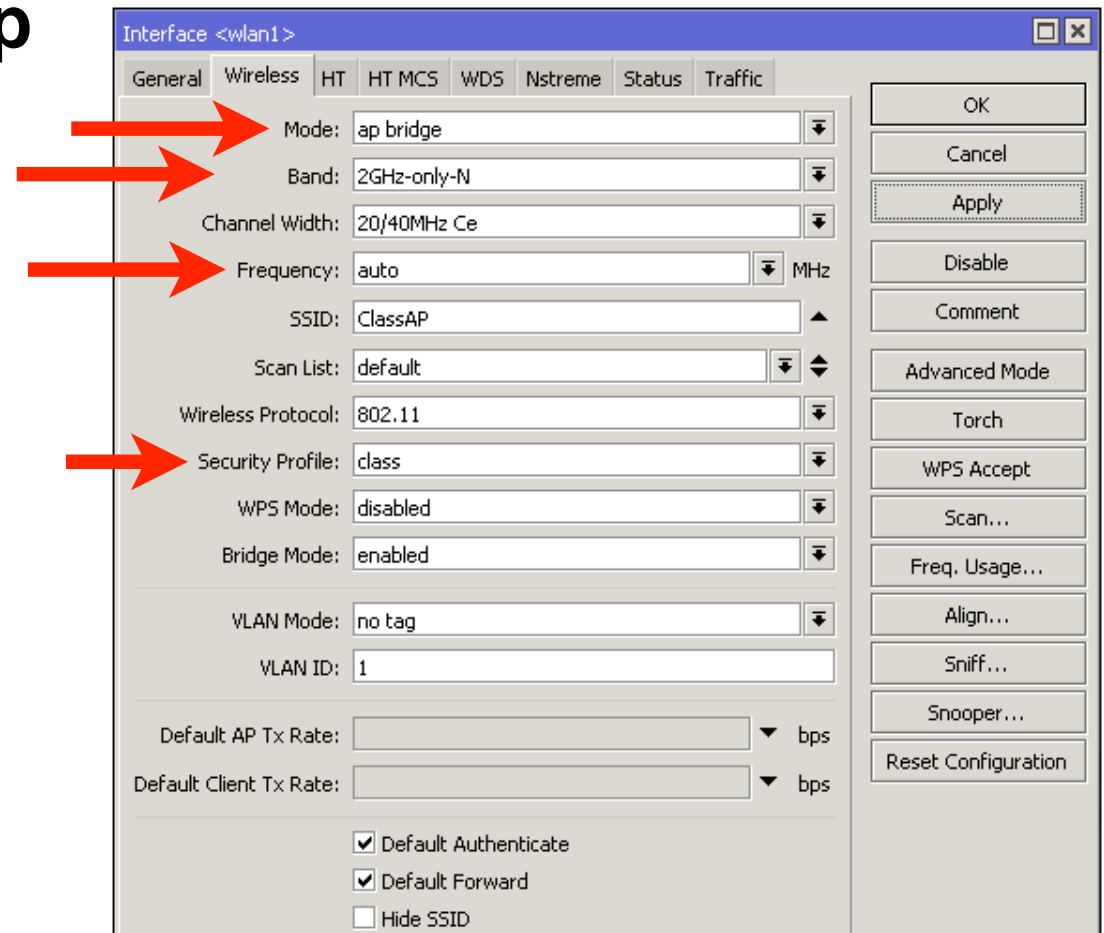
Wireless Lab

LAB

- Reset router anda, dan
- Hubungkan Wireless Router kalian ke AP.
- Terdapat di Wireless Registration jika sudah terhubung.

Access Point

- Set interface **mode=ap bridge**
- Select **band**
- set **frequency**
- Set **SSID** (wireless network ID)
- Set **Security Profile**



WPS

- Wifi Protected Setup (WPS) adalah fitur untuk akses mudah ke wifi tanpa membutuhkan input password
- RouterOS mendukung penggunaan secara bersamaan antara mode WPS accept (untuk AP) dan WPS client (untuk station)

WPS Accept

- Untuk mempermudah mengizinkan akses guest menuju AP bisa menggunakan tombol WPS accept
- Ketika ditekan, maka akan memberikan akses untuk terhubung ke AP selama 2menit atau sampai device (station) masih terhubung.
- Tombol WPS accept harus ditekan setiap kali ada device baru yang ingin dihubungkan

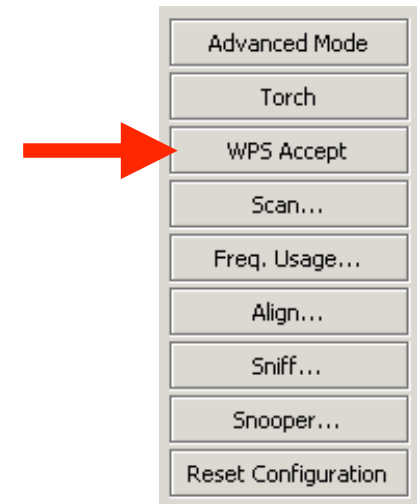
WPS Accept

- Untuk setiap device dilakukan hanya satu kali
- Semua RouterOS device dengan wifi interface memiliki virtual WPS button
- Beberapa memiliki fisik tombol wps pada router



WPS Accept

- Virtual tombol wps berada pada menu wireless interface
- Dapat di non aktifkan jika di inginkan
- WPS client didukung hampir seluruh operating systems termasuk RouterOS
- RouterOS tidak mendukung mode PIN tidak aman



Access Point

- Buatlah security baru pada profile wireless anda
- Jadikan router anda sebagai AP dan masukan security yang telah dibuat sebelumnya
- Disconnect kabel PC/Laptop dari router
- Lalu hubungkan PC/Laptop anda ke AP yang telah dibuat

WPS

LAB

- Jika perangkat PC/Laptop anda support WPS client, hubungkan ke AP anda menggunakan WPS accept button
- Check router logs selama proses berlangsung

Registration Table

- Digunakan untuk melihat semua perangkat yang terhubung ke AP kita

Radio Name	MAC Address	Interface	Uptime	AP	WDS	Last Activi...	Tx/Rx ...	Tx Rate	Rx Rate
	40:B0:FA:81:21:4A	wlan1	00:47:14	no	no	11.130	-79	48Mbps	1Mbps
XY_YourName	D4:CA:6D:E2:65:94	wlan1	00:42:39	no	no	0.000	-28/-32	144.4Mbps-20MHz/25/5GI	130Mbps-20MHz/25/5GI

2 items

Wireless → Registration

Access List

- Digunakan AP untuk mengontrol client yang terhubung
- Memberikan identitas MAC address dengan comment
- Konfigurasi station apakah boleh terhubung atau tidak (authentication)
- Menentukan limit waktu pada saat terhubung

Access List

Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles Channels

+ - ✓ ✗ 📁 🔍 Find

#	MAC Address	Interface	Signal St...	Authentication	Forwarding
0	AA:6C:B4:8A:C0:C9	wlan1	-120..120	yes	yes

AP Access Rule <AA:6C:B4:8A:C0:C9>

MAC Address: AA:6C:B4:8A:C0:C9

Interface: wlan1

Signal Strength Range: -120..120

AP Tx Limit:

Client Tx Limit:

☒ Authentication

☒ Forwarding

VLAN Mode: no tag

VLAN ID: 1

Private Key: none 0x

Private Pre Shared Key:

Management Protection Key:

Time

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

Days: ☒ sun ☒ mon ☒ tue ☒ wed ☒ thu ☒ fri ☒ sat

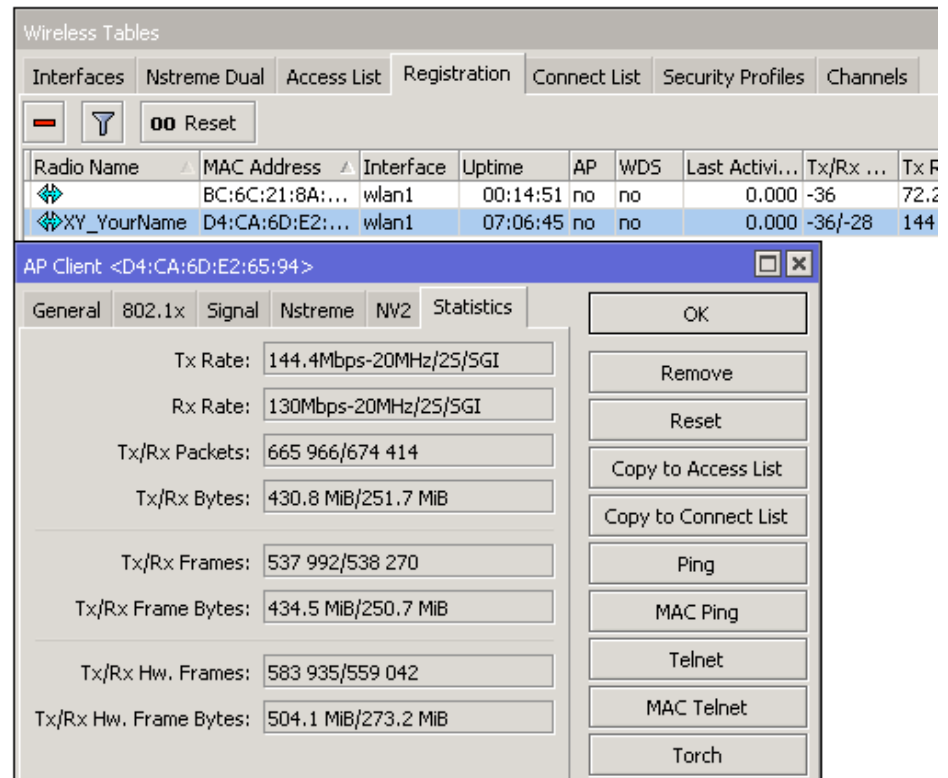
enabled

OK Cancel Apply Disable Comment Copy Remove

Wireless → Access List

Registration Table

- Kita dapat menggunakan copy to access list atau copy to connect list yang terdapat pada menu registration table setelah perangkat terhubung jika kita ingin kan



Wireless → Registration

Default Authenticate

Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme Status Traffic

Mode: ap bridge

Band: 2GHz-only-N

Channel Width: 20/40MHz Ce

Frequency: auto MHz

SSID: ClassAP

Scan List: default

Wireless Protocol: 802.11

Security Profile: class

WPS Mode: disabled

Bridge Mode: enabled

VLAN Mode: no tag

VLAN ID: 1

Default AP Tx Rate: bps

Default Client Tx Rate: bps

☒ Default Authenticate

☒ Default Forward

☐ Hide SSID

OK

Cancel

Apply

Disable

Comment

Advanced Mode

Torch

WPS Accept

Scan...

Freq. Usage...

Align...

Sniff...

Snooper...

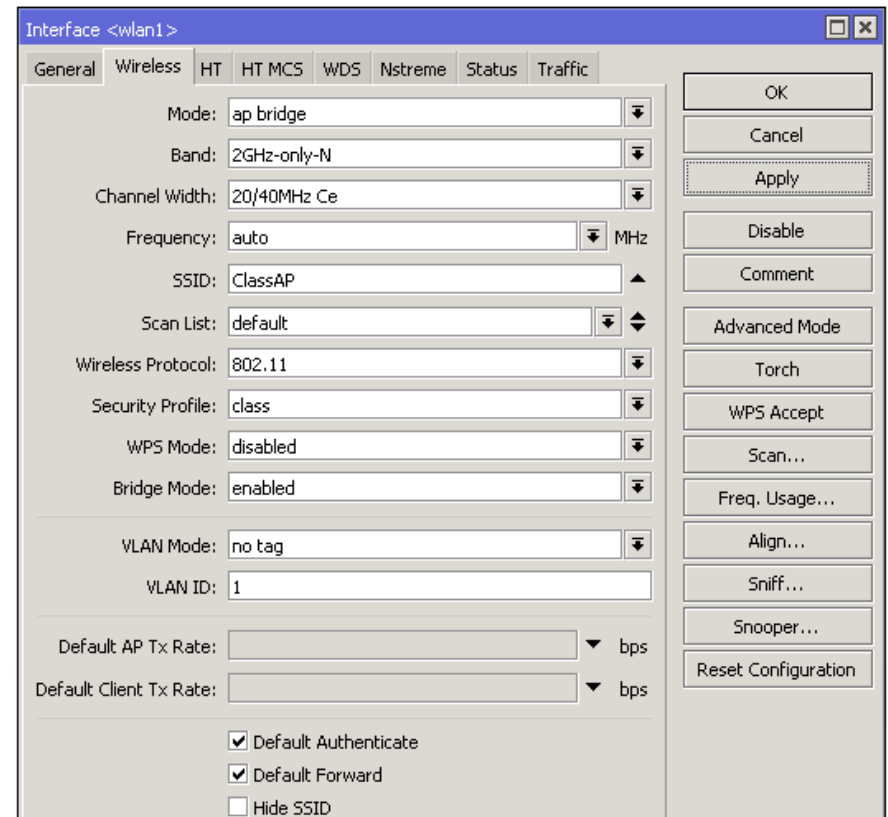
Reset Configuration

Default Authenticate

Default Authentication	Access/Connect List Entry	Behavior
✓	+	Based on access/connect list settings
	-	Authenticate
✗	+	Based on access/connect list settings
	-	Don't authenticate

Default Forward

- Digunakan untuk mengizinkan client dapat saling komunikasi
- Secara default sudah aktif
- Forwarding bisa kita tentukan pada beberapa client saja menggunakan access list



Snooper

- Dapatkan gambaran penuh dari wireless network pada band yang dipilih
- Wireless interface akan **disconnect** selama proses scanning
- Gunakan untuk menentukan keputusan channel untuk dipilih

Snooper

Wireless Snooper (Running)

Interface: wlan1

Start
Stop
Close
Settings
New Window

all

Channel	Address	SSID	Signal	Of Freq. (%)	Of Traf. (%)	Bandwidth	Net...	Sta...
2412/20/gn(20dBm)	64:66:B3:40:E6:5E	Maximums	-71	0.0	0.0	0 bps		
2412/20/gn(20dBm)	50:56:A8:01:69:71		-81	0.0	0.0	0 bps		
2412/20/gn(20dBm)	4C:5E:0C:61:B4:36	Hotspot		1.3	8.4	12.4 kbps		1
2412/20/gn(20dBm)	4C:5E:0C:61:B4:36	Hotspot	-91	1.3	8.4	12.4 kbps		
2412/20/gn(20dBm)	00:0C:42:18:5C:49		-86	0.0	0.0	0 bps		
2412/20/gn(20dBm)	00:0C:42:0C:1B:4E			0.1	1.2	9.1 kbps		1
2412/20/gn(20dBm)	00:0C:42:0C:1B:4E		-86	0.1	1.2	9.1 kbps		
2412/20/gn(20dBm)	00:0B:6B:30:7F:A6	raivis		0.0	0.0	0 bps		0
2412/20/gn(20dBm)	00:0B:6B:30:7F:A6		-73	0.0	0.0	0 bps		
2412/20/gn(20dBm)				16.0		108.8 kbps	7	12
2417/20/gn(20dBm)	84:A6:C8:06:F3:83		-83	0.0	0.0	0 bps		
2417/20/gn(20dBm)				11.4		81.4 kbps	0	1
2422/20/gn(20dBm)	58:48:22:3F:56:B5	Mob	-80	0.0	0.0	0 bps		
2422/20/gn(20dBm)	4C:5E:0C:D6:CB:81	Mob		1.2	14.7	11.0 kbps		2
2422/20/gn(20dBm)	4C:5E:0C:D6:CB:81	Mob	-51	1.2	14.7	11.0 kbps		
2422/20/gn(20dBm)	4C:5E:0C:6C:5C:F2	anrijs-map		1.3	16.2	12.3 kbps		1
2422/20/gn(20dBm)	4C:5E:0C:6C:5C:F2	anrijs-map	-61	1.3	16.2	12.3 kbps		
2422/20/gn(20dBm)	4C:5E:0C:13:E6:65	MikroTik-mAPlite		0.0	0.0	0 bps		1
2422/20/gn(20dBm)	4C:5E:0C:13:E6:65	MikroTik-mAPlite	-88	0.0	0.0	0 bps		

Wireless → Snooper

Module 2

Summary



**Certified Network Associate
(MTCNA)**

Module 3

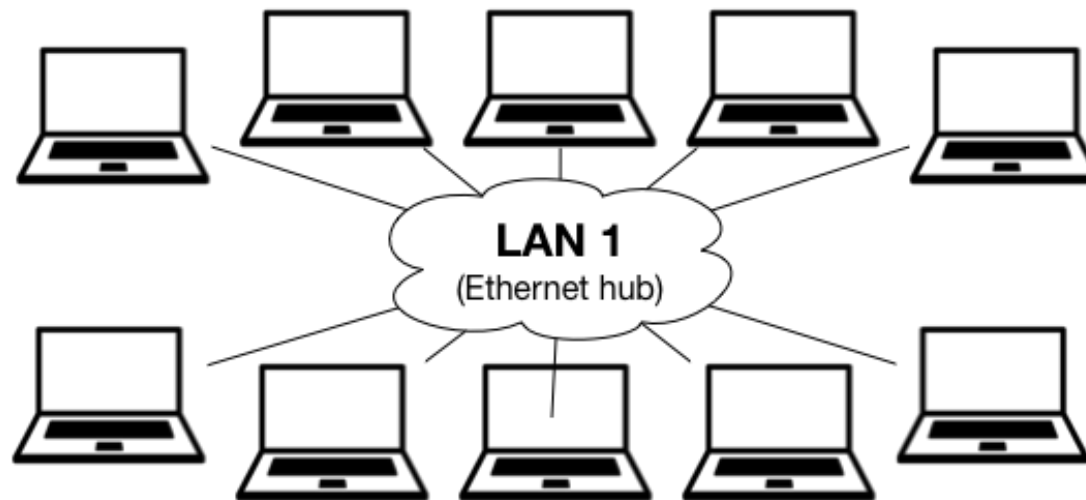
Bridging

Bridge

- Bridge berjalan pada OSI layer 2
- Bridge adalah transparent device
- Menggabungkan dua atau lebih interface seolah-olah berada dalam satu segmen network yang sama
- Interface bridge adalah Interface virtual, dimana kita dapat membuat sebanyak yang kita inginkan
- Tahap pembuatan bridge adalah, membuat bridge baru dan menambahkan interface kedalam port

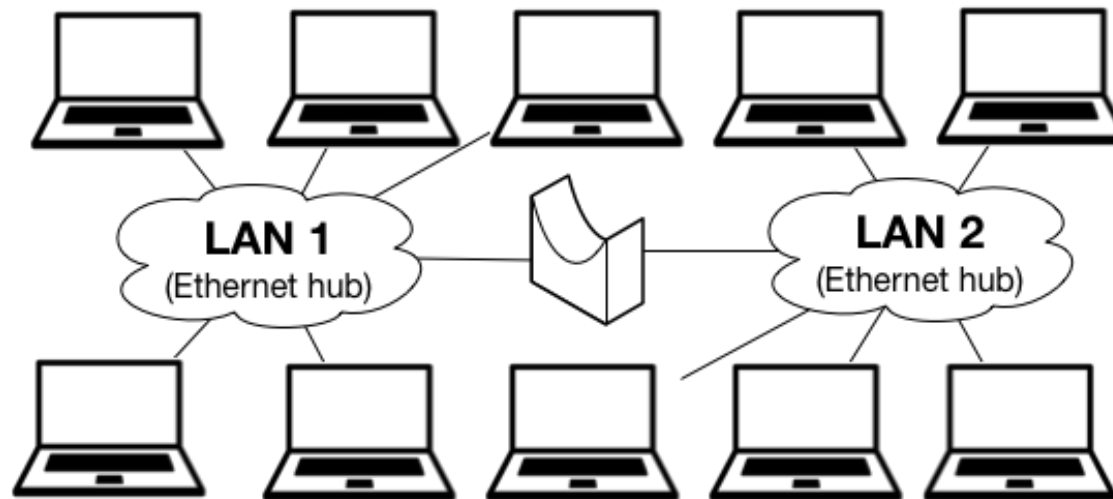
Bridge

- Semua hosts bisa saling komunikasi antar sesama
- Berbagi Collision domain yang sama pada sebuah jaringan



Bridge

- Semua hosts tetap bisa saling komunikasi antar sesama
- Terdapat 2 collision domains



Bridge

- RouterOS implementasi bridge secara default pada;
 - Port bridge wireless dengan ether2
 - Ether2-5 digabungkan bersama pada mode switch (before Router v6.41).
- Ethernet, Wireless, SFP dan tunnel interface bisa dimasukkan kedalam port bridge

Bridge

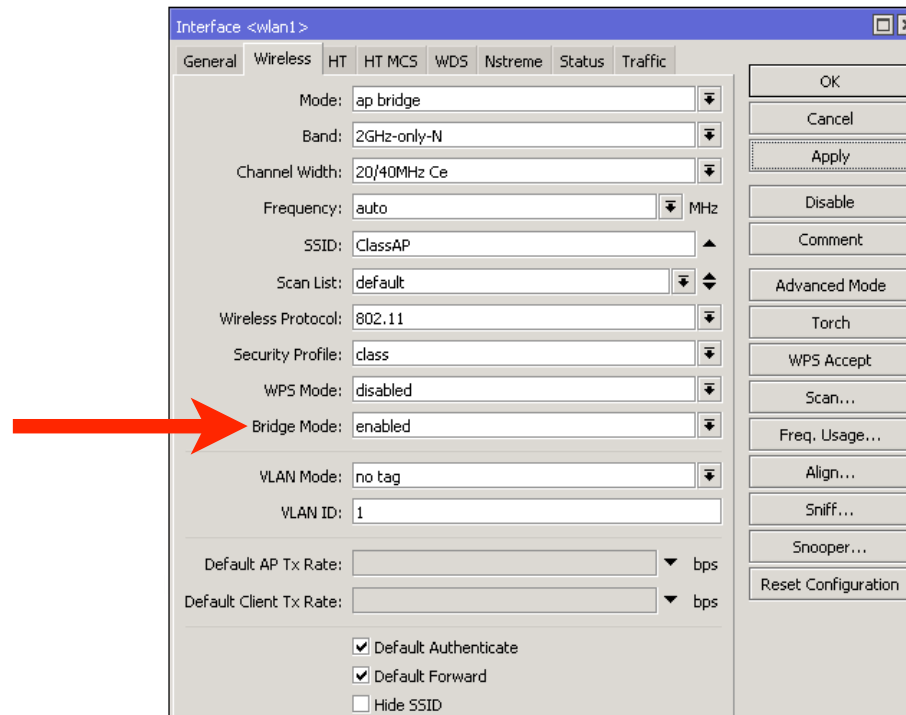
- Mode Bridge dapat menggunakan IP Firewall
- Ethernet dalam kondisi mode switch tidak dapat dimasukkan kedalam port bridge begitupun sebaliknya
- Wireless mode “station” tidak dapat di bridge
- RouterOS memberikan solusi atas keterbatasan tersebut

Wireless Bridge

- **Station-bridge** - RouterOS to RouterOS
- **Station-pseudobridge** - RouterOS to other
- **Station-wds** (Wireless Distribution System) - RouterOS to RouterOS

Wireless Bridge

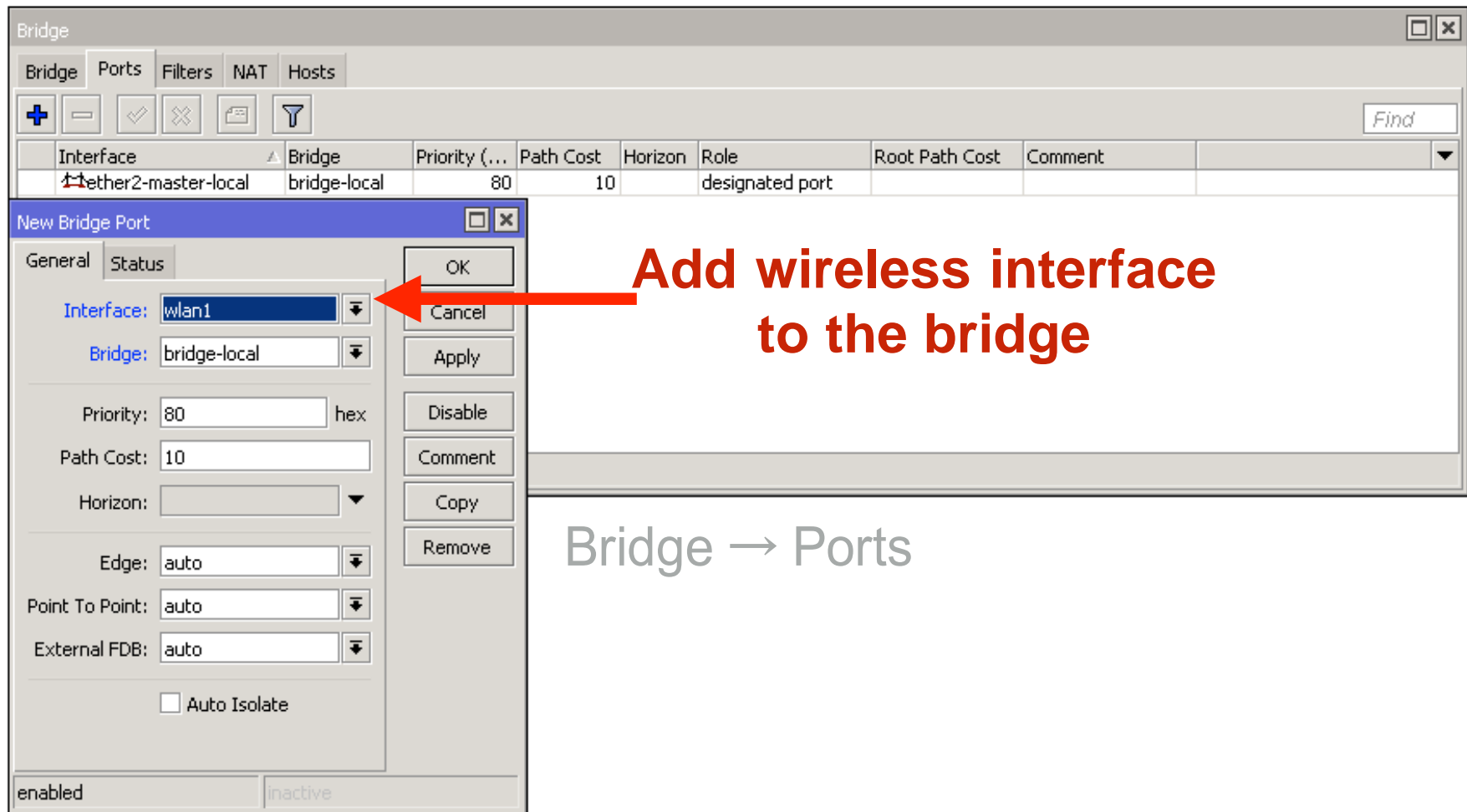
- Untuk dapat menggunakan **station-bridge**, “Bridge Mode” harus sudah dalam kondisi enable pada AP



Bridge

- Kita akan membuat bridge network antara lokal ethernet dengan wireless interface
- Semua PC/Laptop akan mendapatkan IP dari Router AP
- Lakukan Backup Sebelum melakukan LAB ini!

Bridge



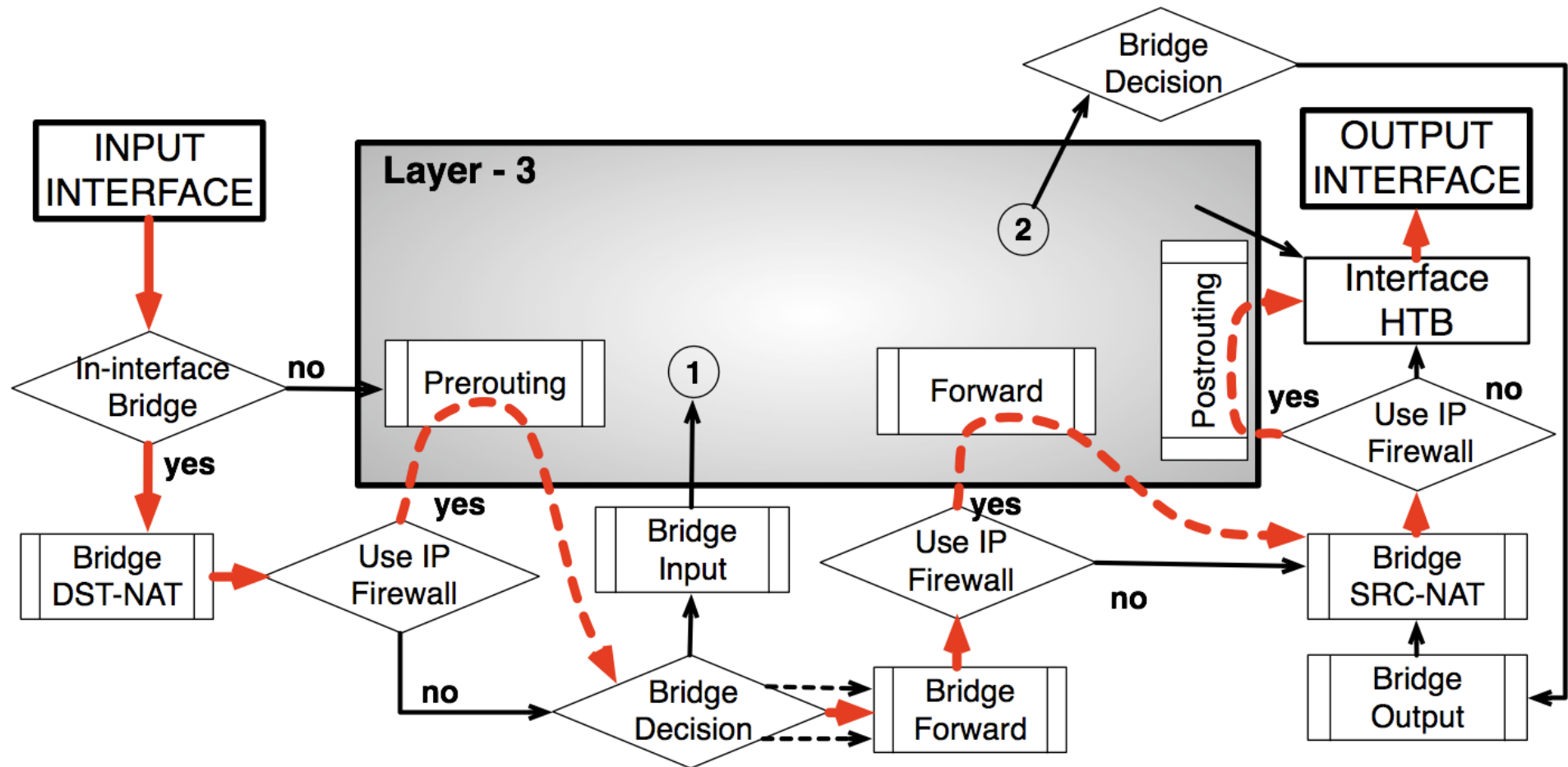
Bridge

- Perbarui IP address pada PC/Laptop anda
- Anda akan mendapatkan semua routerOS yang terhubung dengan neighbor discovery
- Router anda bekerja sebagai **transparent bridge**

Bridge Firewall

- RouterOS bridge interface support firewall
- Trafik yang melalui bridge dapat diproses dengan mode firewall aktif
- Untuk dapat mengaktifkan: Bridge → Settings → Use IP Firewall

Bridge Firewall



Module 3

Summary



**Certified Network Associate
(MTCNA)**

Module 4

DHCP

DHCP

- Dynamic Host Configuration Protocol
- Digunakan pada jaringan yang akan mendistribusikan IP address nya secara auto
- Menggunakan DHCP hanya di network yang kita percaya
- Bekerja dengan broadcast domain
- RouterOS support DHCP client and Server running secara bersamaan

DHCP Client

- Digunakan untuk mendapatkan IP address, subnet, gateway, DNS Server dan additional setting lainnya
- MikroTik Routers secara default memiliki DHCP client konfigurasi pada ether1 (WAN) interface

DHCP Client

The screenshot displays the DHCP Client management interface. At the top, a table lists active clients. Below this, two windows provide detailed configuration for the 'wlan1' interface.

Interface	Use Peer DNS	Add Default Route	IP Address	Expires After	Status
wlan1	yes	yes	10.5.120.243/24	00:20:57	bound

DHCP Client <wlan1> Configuration (Left Window):

- Interface: wlan1
- ☒ Use Peer DNS
- ☒ Use Peer NTP
- DHCP Options: hostname, clientid
- Add Default Route: yes
- Default Route Distance: 1

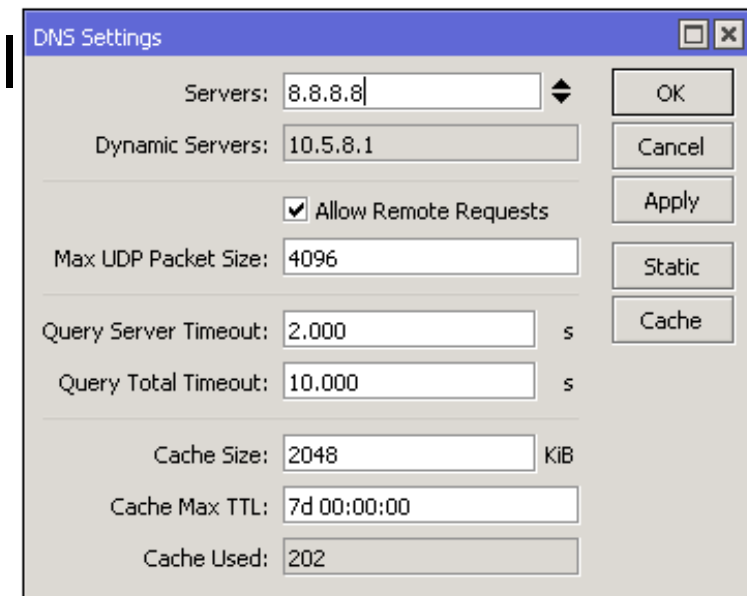
DHCP Client <wlan1> Configuration (Right Window):

- IP Address: 10.5.120.243/24
- Gateway: 10.5.120.1
- DHCP Server: 10.5.120.2
- Expires After: 00:21:25
- Primary DNS: 10.5.120.1
- Secondary DNS:
- Primary NTP: 10.5.8.1
- Secondary NTP:
- CAPS Managers:

IP → DHCP Client

DNS

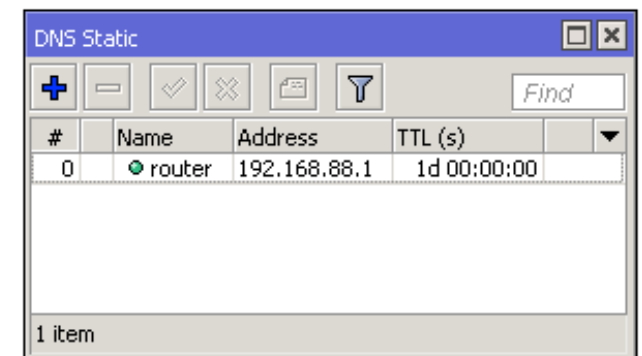
- Secara default DHCP client akan mengcreate secara auto jika dibutuhkan
- dapat dikonfig secara manual



IP → DNS

DNS

- RouterOS support static DNS entries
- By default static DNS A record named **router** akan diarahkan ke ip 192.168.88.1
- <http://router>

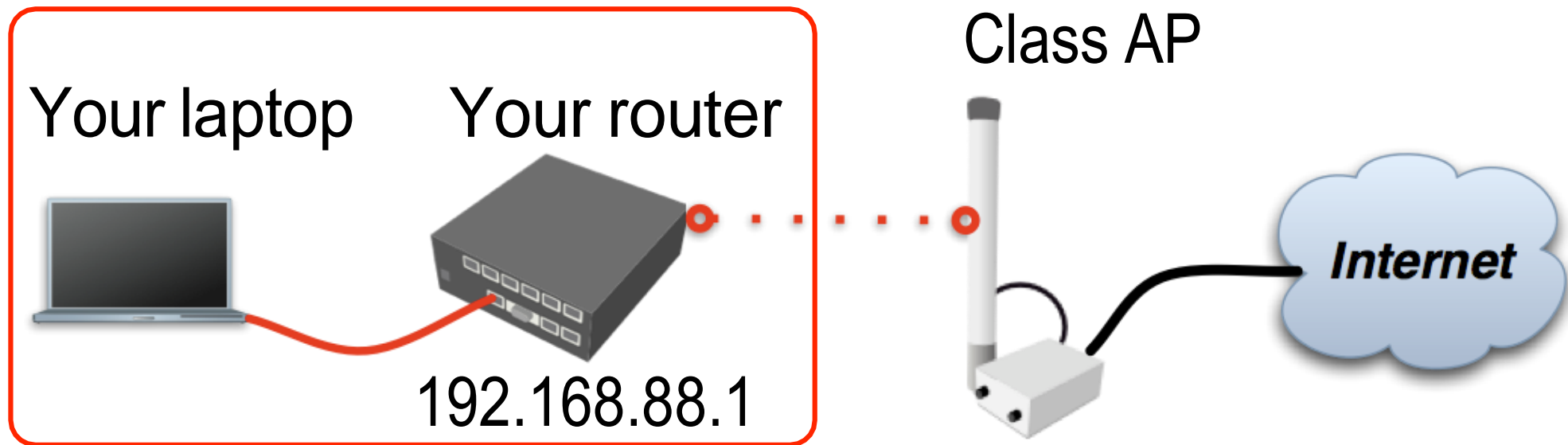


IP → DNS → Static

DHCP Server

- Secara Auto akan memberikan IP kepada DHCP client yang me-request
- IP address harus di instal pada interface yang akan dituju
- Simple setup DHCP Server cukup dengan command “DHCP Setup”

Internet Setup



Router - Internet

**Remove
the WiFi
interface
from the
bridge**

Bridge

Bridge Ports Filters NAT Hosts

+ - ✓ ✗ 📄 🔍

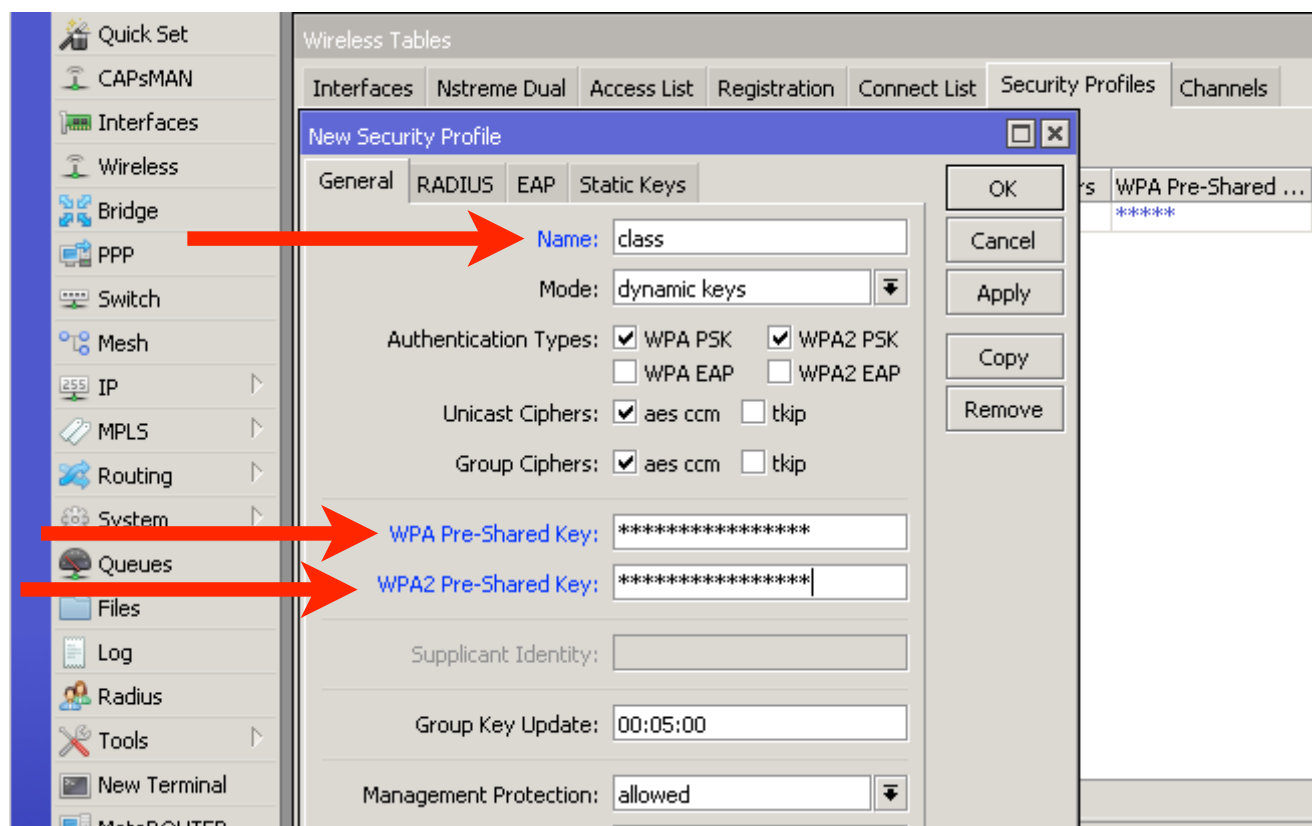
	Interface	Bridge	Priority (...)	Path Cost	Horizon	Role
	ether2-master-local	bridge-local	80	10		designated port
I	wlan1	bridge-local	80	10		disabled port

2 items (1 selected)

Bridge → Ports

Router - Internet

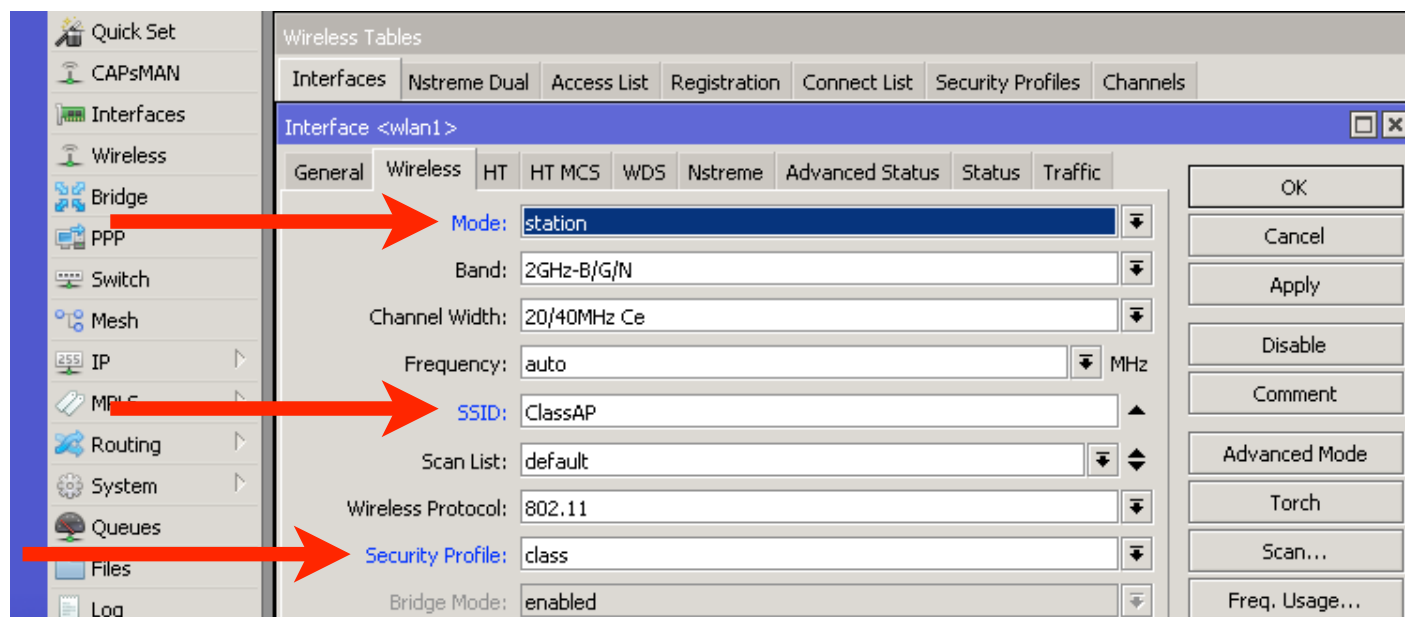
**Set Name
and
Pre-Shared
Keys**



Wireless → Security Profiles

Router - Internet

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

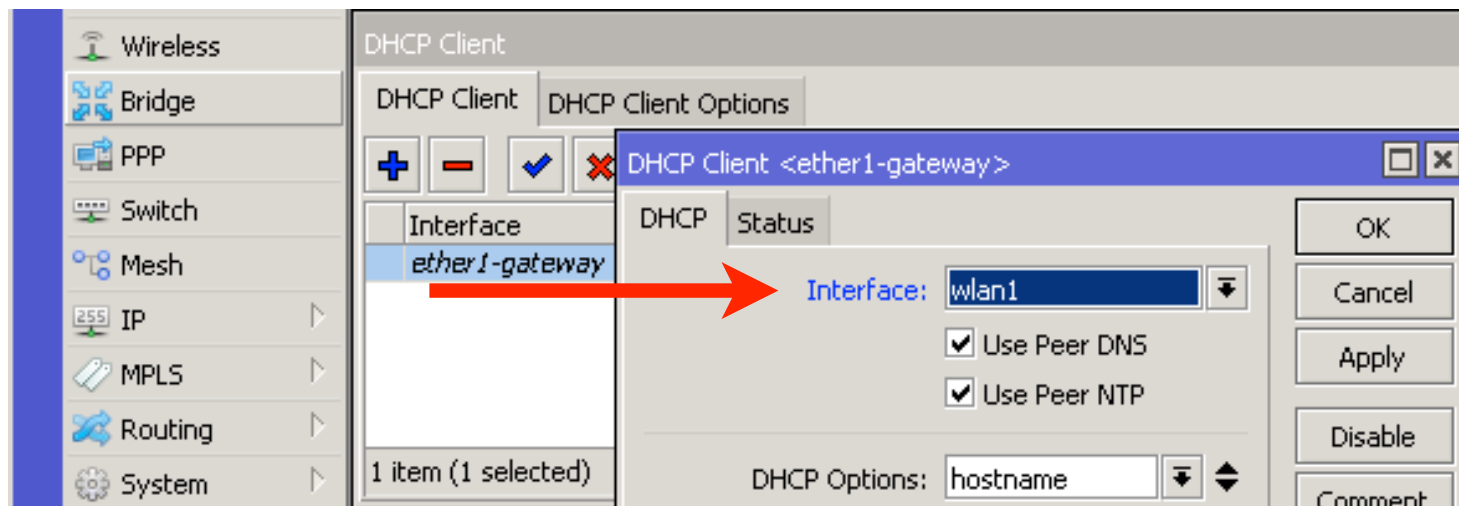


Wireless → Interfaces

- “Scan...” tool digunakan untuk melihat SSID yang tersedia

Router - Internet

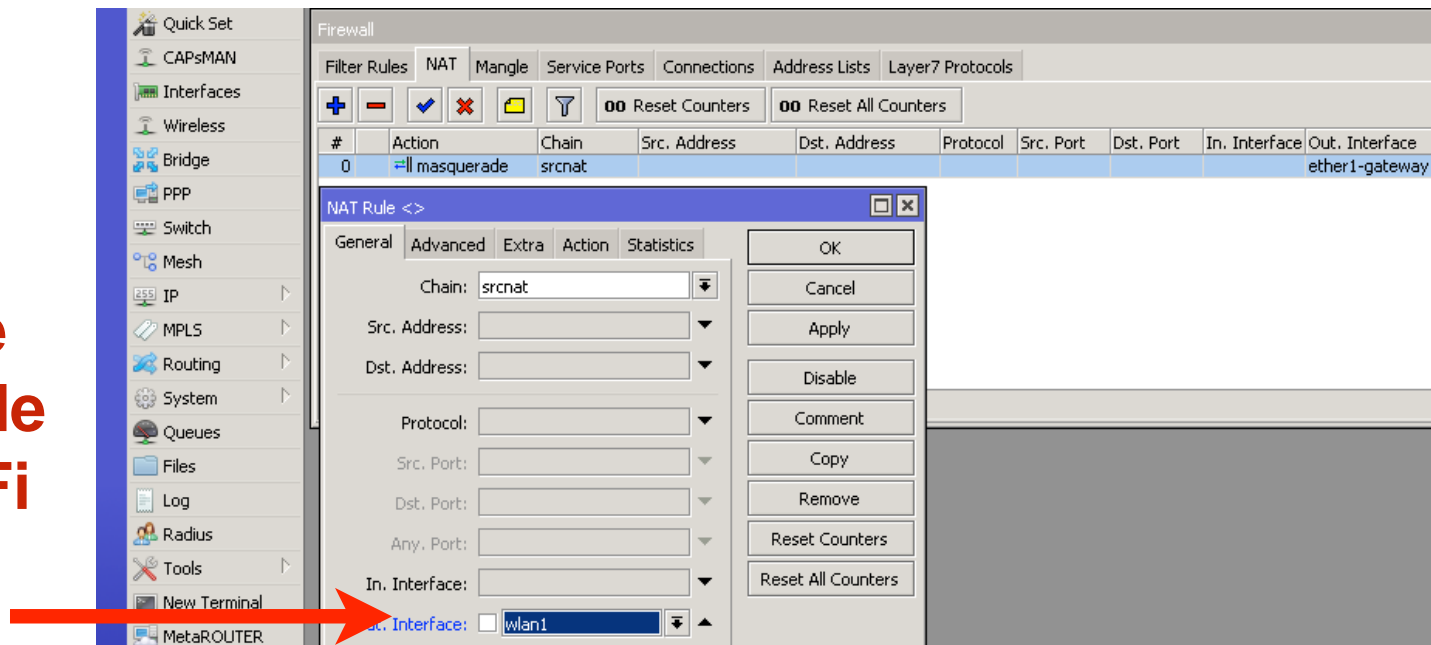
Set DHCP client to the WiFi interface



IP → DHCP Client

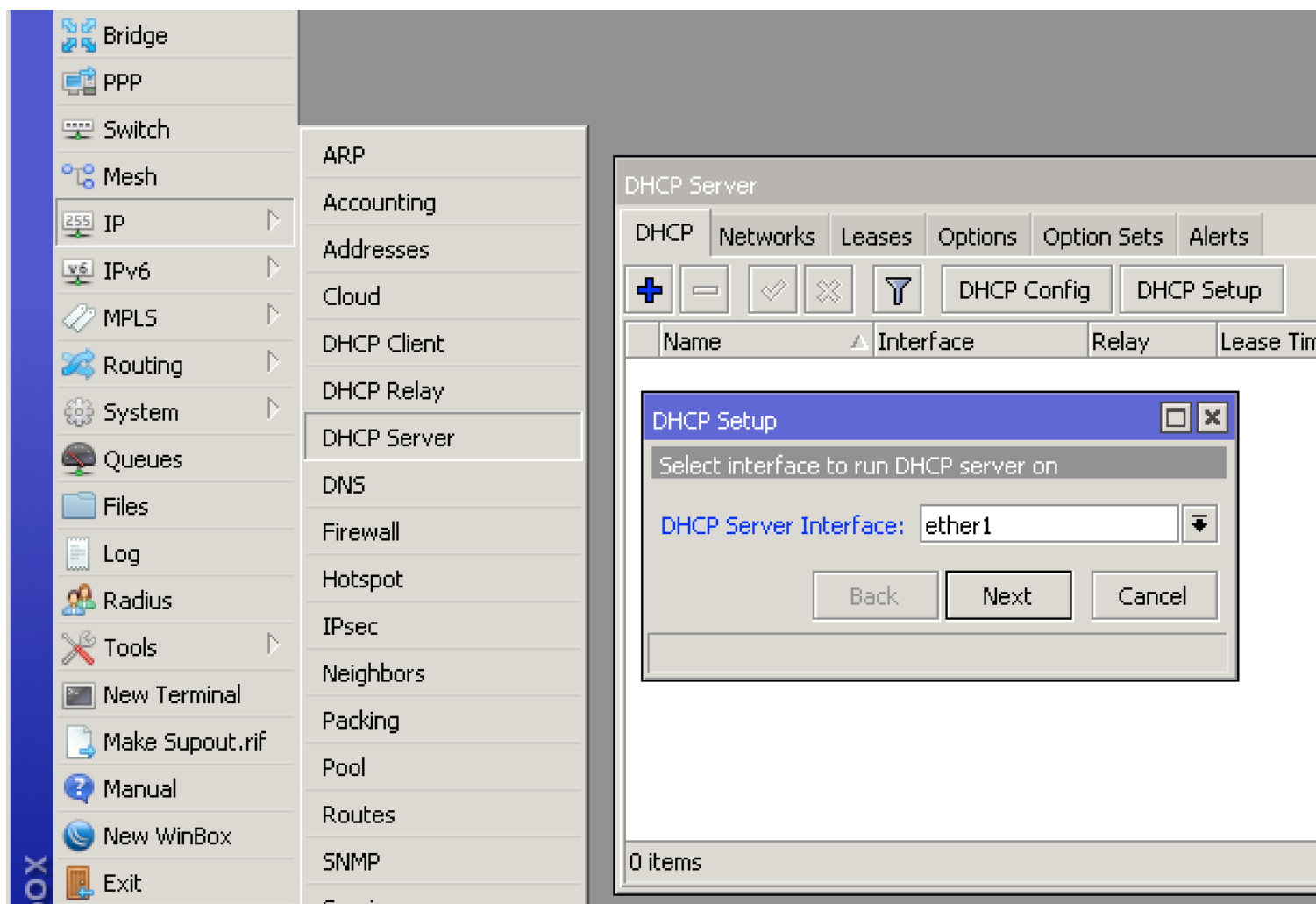
Router - Internet

**Configure
masquerade
on the WiFi
interface**



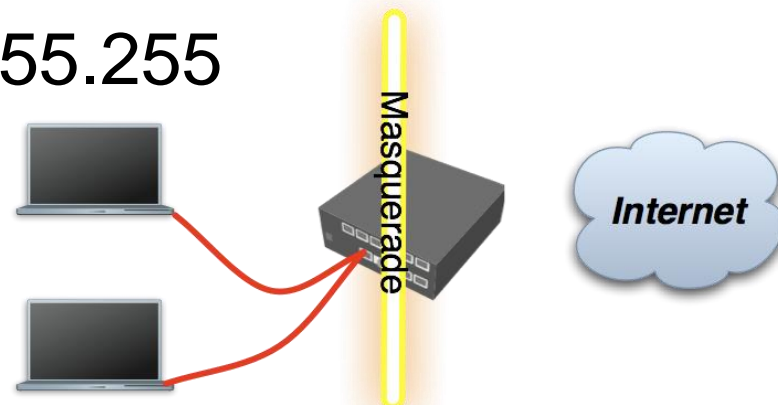
IP → Firewall → NAT

DHCP Server



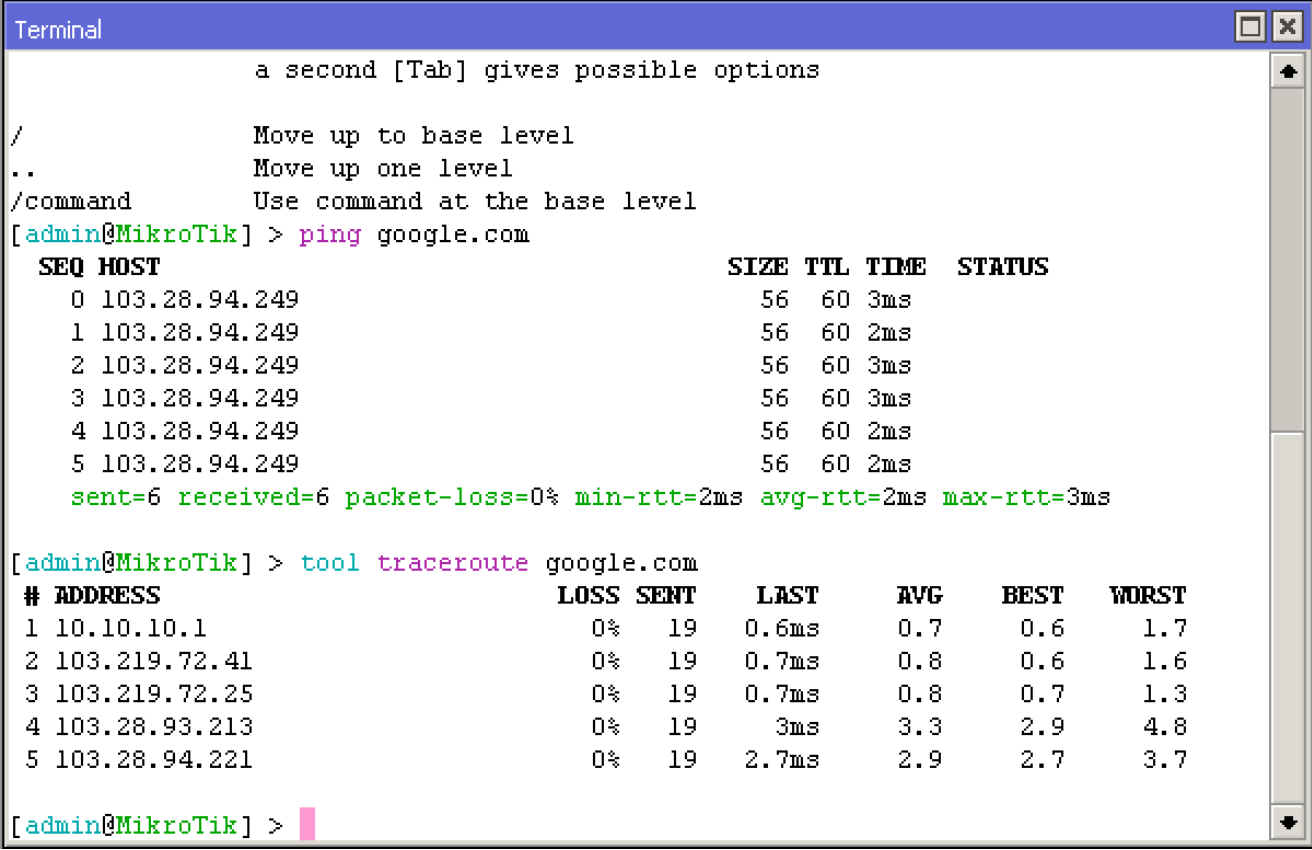
Private and Public Space

- **Masquerade** digunakan untuk jaringan private agar dapat dikenali pada jaringan publik (internet)
- Private networks
 - 10.0.0.0 - 10.255.255.255
 - 172.16.0.0 - 172.31.255.255
 - 192.168.0.0 - 192.168.255.255



Check Connectivity

- Ping atau traceroute ke mikrotik.com (atau kemana saja) pada new terminal router



```
Terminal
a second [Tab] gives possible options

/      Move up to base level
..     Move up one level
/command Use command at the base level
[admin@MikroTik] > ping google.com
  SEQ HOST                                SIZE TTL TIME  STATUS
    0 103.28.94.249                        56  60 3ms
    1 103.28.94.249                        56  60 2ms
    2 103.28.94.249                        56  60 3ms
    3 103.28.94.249                        56  60 3ms
    4 103.28.94.249                        56  60 2ms
    5 103.28.94.249                        56  60 2ms
  sent=6 received=6 packet-loss=0% min-rtt=2ms avg-rtt=2ms max-rtt=3ms

[admin@MikroTik] > tool traceroute google.com
# ADDRESS                                LOSS SENT    LAST    AVG    BEST    WORST
1 10.10.10.1                             0%   19    0.6ms   0.7    0.6    1.7
2 103.219.72.41                           0%   19    0.7ms   0.8    0.6    1.6
3 103.219.72.25                           0%   19    0.7ms   0.8    0.7    1.3
4 103.28.93.213                           0%   19     3ms    3.3    2.9    4.8
5 103.28.94.221                           0%   19    2.7ms   2.9    2.7    3.7

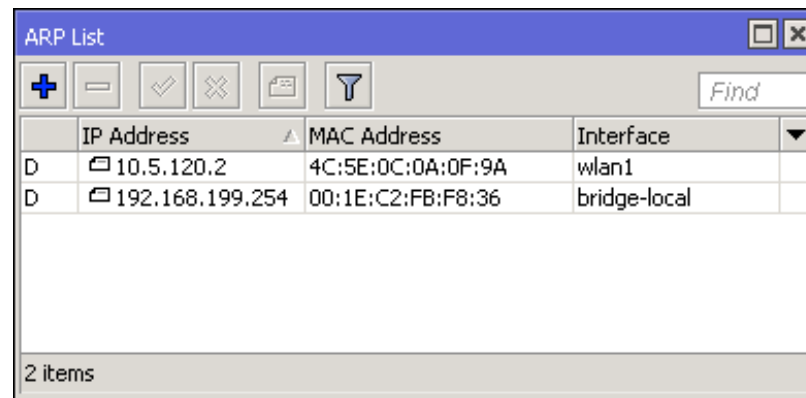
[admin@MikroTik] > 
```


ARP

- Address Resolution Protocol
- ARP menggabungkan bersama IP address (layer3) dengan MAC address (layer2)
- ARP bekerja secara dynamic
- bisa juga dikonfig secara manual (static)

ARP Table

- ARP akan memberikan informasi tentang IP address dan MAC address yang terhubung



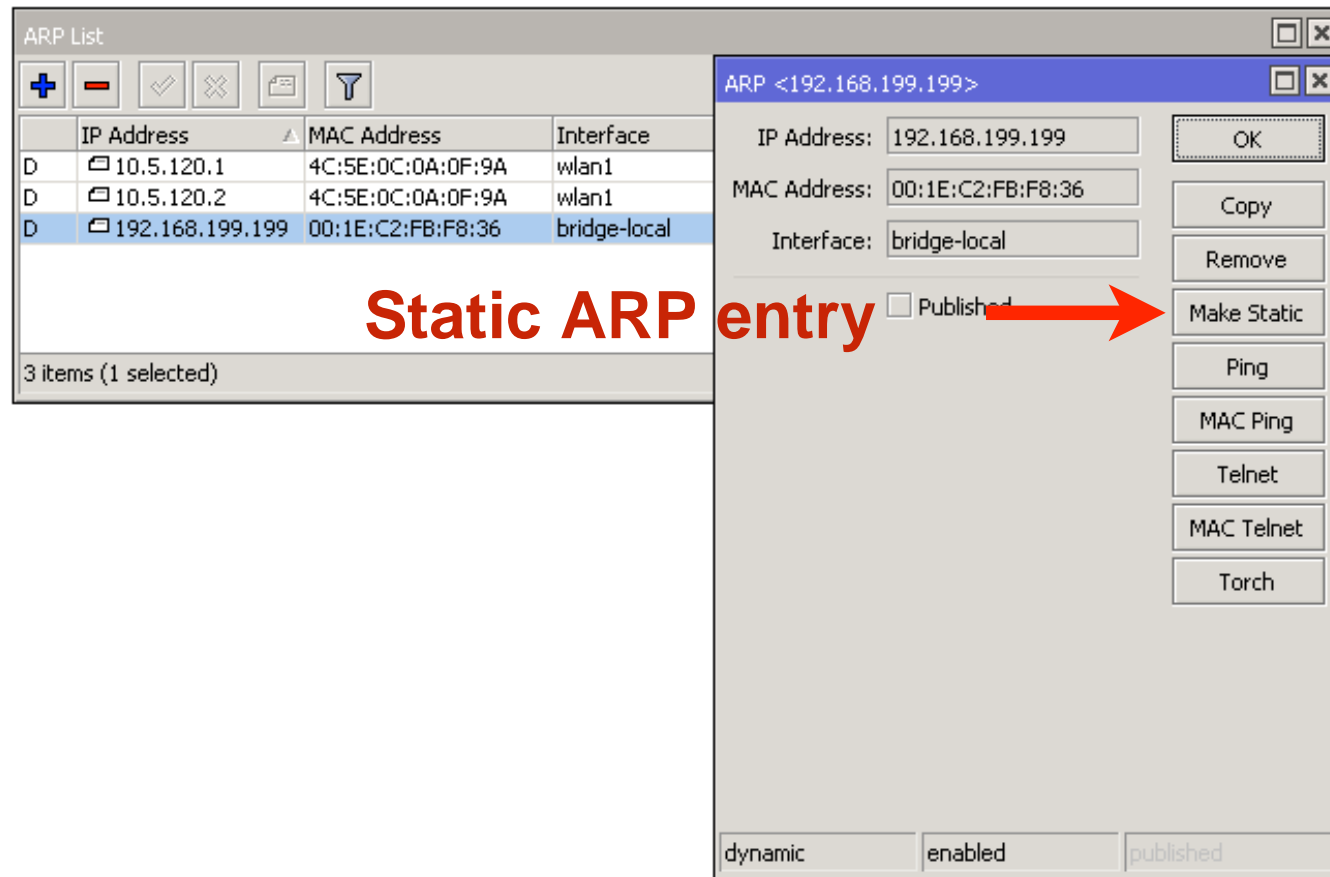
The screenshot shows a window titled "ARP List" with a toolbar containing icons for adding, removing, checking, unchecking, refreshing, and filtering, along with a "Find" search box. The table below lists two entries:

	IP Address	MAC Address	Interface
D	10.5.120.2	4C:5E:0C:0A:0F:9A	wlan1
D	192.168.199.254	00:1E:C2:FB:F8:36	bridge-local

2 items

IP → ARP

Static ARP



IP → ARP

Static ARP

**Interface will
reply only to
known ARP
entries**

Interface <bridge-local>

General STP Status Traffic

Name: bridge-local

Type: Bridge

MTU:

Actual MTU: 1500

L2 MTU: 1598

MAC Address: D4:CA:6D:E2:65:90

ARP: reply-only

Admin. MAC Address: D4:CA:6D:E2:65:90

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave

Interfaces → bridge-local

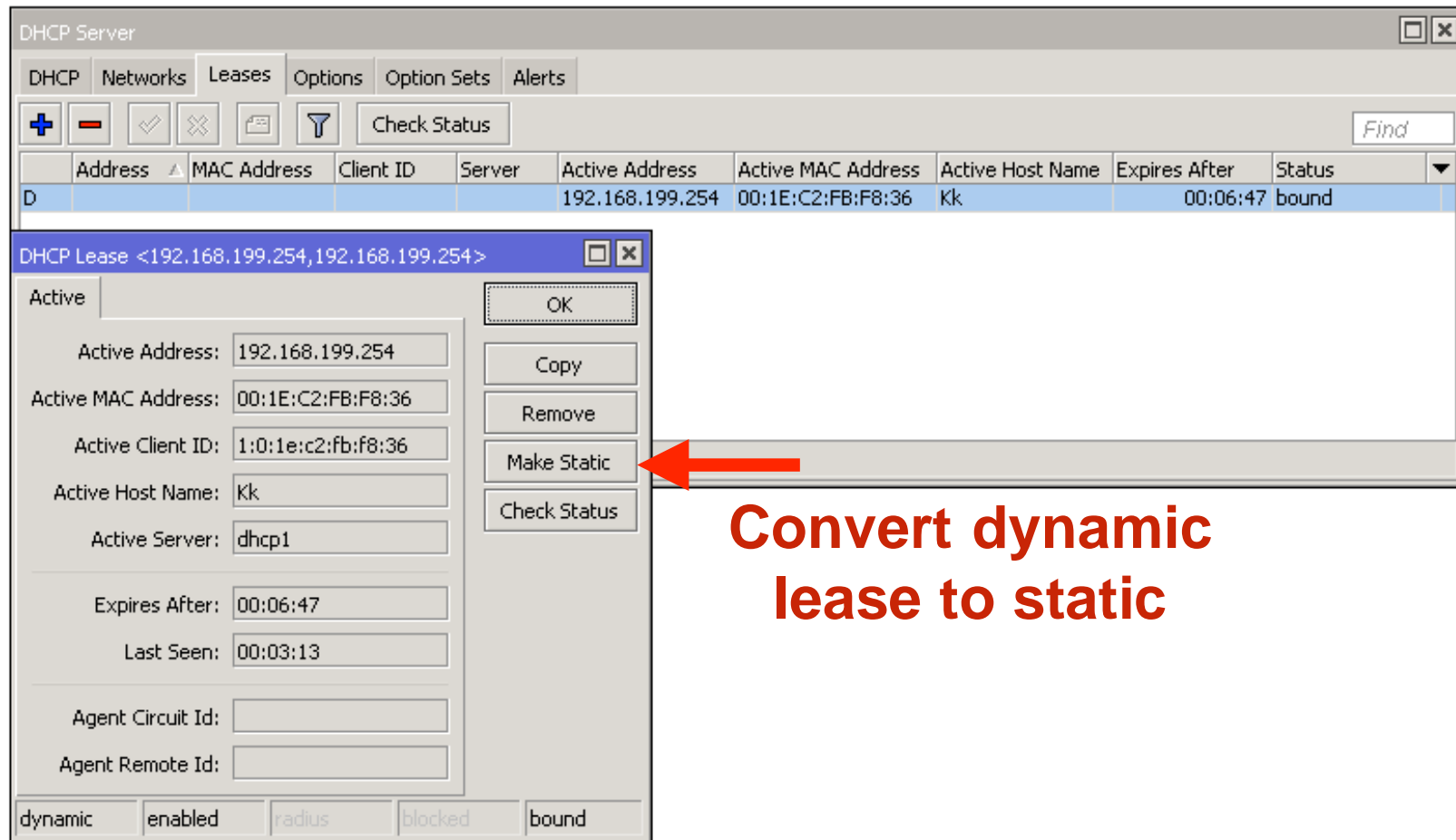
DHCP dan ARP

- DHCP Server bisa menambahkan ARP entries secara auto
- Menggabungkan static leases and replay-only ARP dapat meningkatkan keamanan sementara tetap memberikan kemudahan

DHCP Static Leases

- Memungkinkan untuk memberikan IP address yang selalu sama pada device (identifikasi menggunakan MAC address)
- DHCP Server bahkan bisa digunakan tanpa dynamic IP pool dan memberikan alamat berdasarkan yang dikonfigurasi

DHCP Static Leases



DHCP dan ARP

DHCP Server <dhcp1>

Name: dhcp1

Interface: bridge-local

Relay:

Lease Time: 00:10:00

Bootp Lease Time: forever

Address Pool: dhcp_pool1

Src. Address:

Delay Threshold:

Authoritative: after 2s delay

Bootp Support: static

Lease Script:

☒ Add ARP For Leases

☐ Always Broadcast

☐ Use RADIUS

enabled

Address Pool	Add ARP For Leases
pool1	no

IP → DHCP Server

**Add ARP entries
for DHCP leases**

DHCP Static Leases

- Buatlah static lease pada pc/laptop anda
- Set ke reply-only pada Interface
- Enable “add ARP for leases” pada DHCP Server

Static ARP

1

**Interface will
reply only to
known ARP
entries**

Interface <bridge-local>

General STP Status Traffic

Name: bridge-local

Type: Bridge

MTU:

Actual MTU: 1500

L2 MTU: 1598

MAC Address: D4:CA:6D:E2:65:90

ARP: reply-only

Admin. MAC Address: D4:CA:6D:E2:65:90

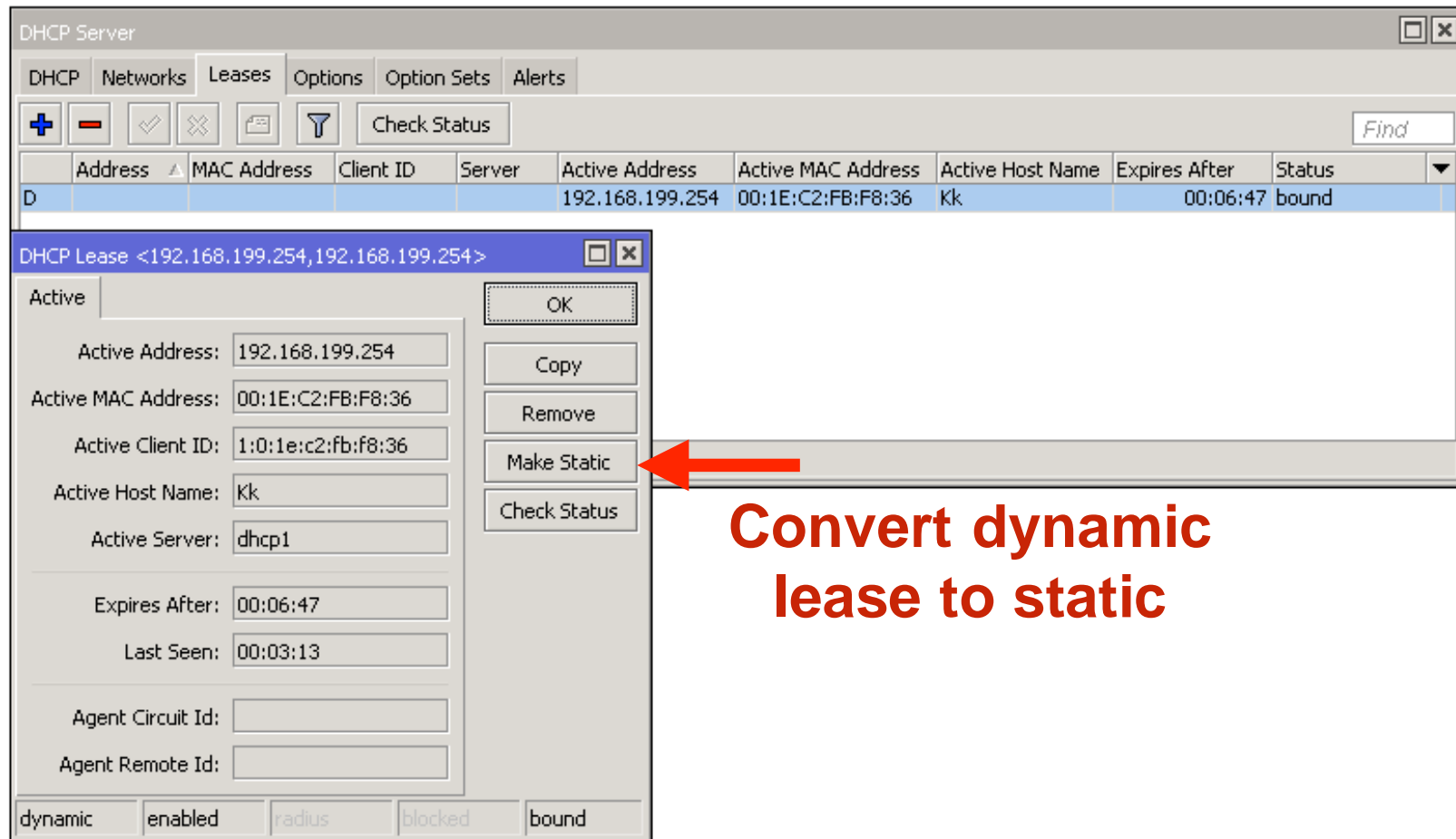
OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave

Interfaces → bridge-local

DHCP Static Leases

2



IP → DHCP Server → Leases

DHCP dan ARP

3

DHCP Server <dhcp1>

Name: dhcp1

Interface: bridge-local

Relay:

Lease Time: 00:10:00

Bootp Lease Time: forever

Address Pool: dhcp_pool1

Src. Address:

Delay Threshold:

Authoritative: after 2s delay

Bootp Support: static

Lease Script:

☒ Add ARP For Leases

☐ Always Broadcast

☐ Use RADIUS

enabled

Address Pool	Add ARP For Leases
pool1	no

IP → DHCP Server

**Add ARP entries
for DHCP leases**

DHCP Static Leases

- Lakukan perubahan IP address pada laptop anda (berbeda dengan yang ada di static lease yang telah dibuat)
- Cek apakah PC/Laptop anda mendapatkan IP address

Module 4

Summary



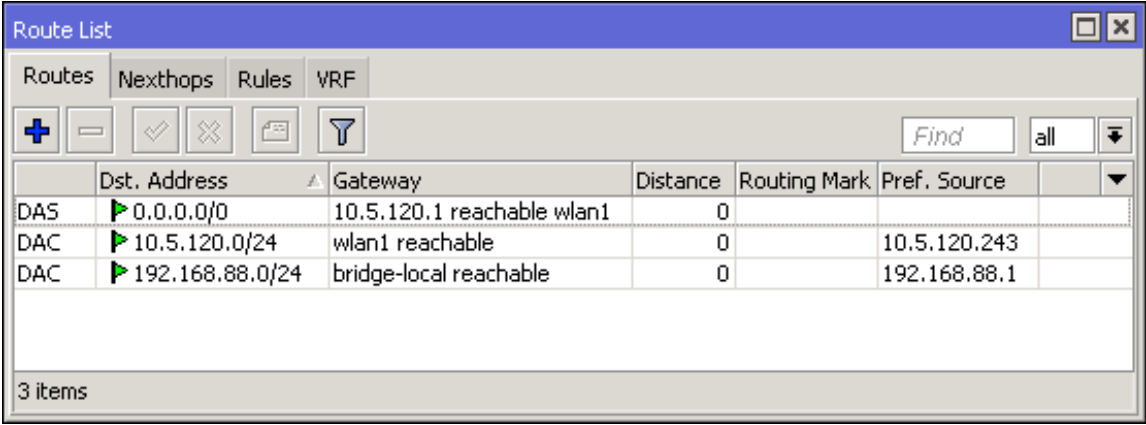
**Certified Network Associate
(MTCNA)**

Module 5

Routing

Routing

- Bekerja pada OSI network layer 3
- RouterOS routing rules mendefinisikan kemana packet akan dikirim



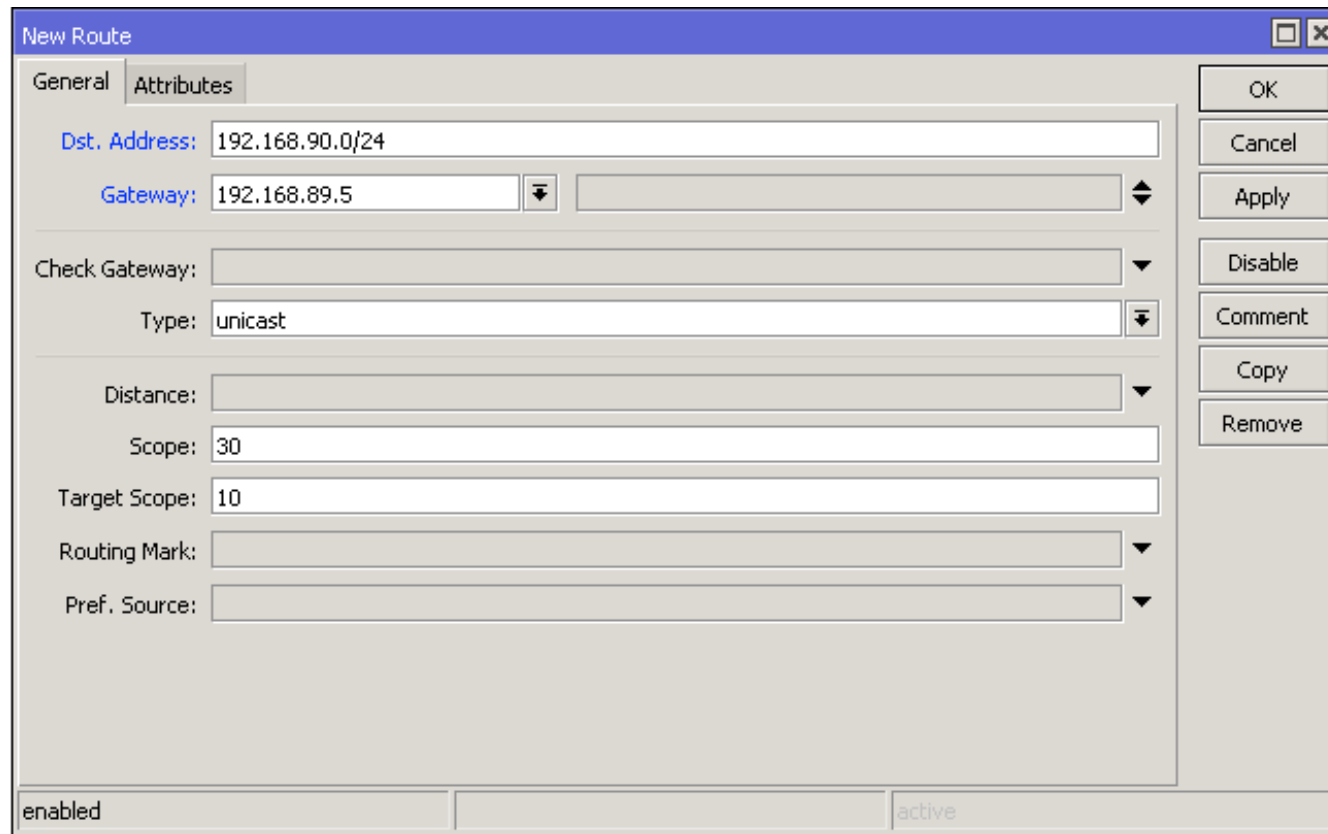
The screenshot shows the 'Route List' window in RouterOS. It has tabs for 'Routes', 'Nexthops', 'Rules', and 'VRF'. The 'Routes' tab is active. Below the tabs are several icons: a plus sign, a minus sign, a checkmark, a cross, a folder, and a funnel. To the right of these icons is a 'Find' search bar with a dropdown menu set to 'all'. The main area contains a table with the following data:

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source	
DAS	0.0.0.0/0	10.5.120.1 reachable wlan1	0			
DAC	10.5.120.0/24	wlan1 reachable	0		10.5.120.243	
DAC	192.168.88.0/24	bridge-local reachable	0		192.168.88.1	

At the bottom of the window, it says '3 items'.

IP → Routes

New Static Route



The image shows a 'New Route' dialog box with a blue title bar and standard window controls. It has two tabs: 'General' (selected) and 'Attributes'. The 'General' tab contains several input fields: 'Dst. Address' with the value '192.168.90.0/24', 'Gateway' with the value '192.168.89.5' and a dropdown arrow, 'Check Gateway' with a dropdown arrow, 'Type' with the value 'unicast' and a dropdown arrow, 'Distance' with a dropdown arrow, 'Scope' with the value '30', 'Target Scope' with the value '10', 'Routing Mark' with a dropdown arrow, and 'Pref. Source' with a dropdown arrow. On the right side of the dialog, there is a vertical stack of buttons: 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'. At the bottom of the dialog, there are two checkboxes: 'enabled' (checked) and 'active' (unchecked).

New Route

General Attributes

Dst. Address: 192.168.90.0/24

Gateway: 192.168.89.5

Check Gateway:

Type: unicast

Distance:

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

enabled active

IP → Routes

Routing

- Check gateway - setiap 10 detik mengirim balik permintaan echo ping ICMP atau ARP
- Jika beberapa route menggunakan gateway yang sama dan ada salah satu yang enable **check-gateway**, semua route akan dikenakan perilaku check-gateway

Routing

- Jika ada dua atau lebih route yang diarahkan ke address yang sama, yang lebih tepat yang akan digunakan
 - Dst: 192.168.90.0/24, gateway 1.2.3.4
 - Dst: 192.168.90.128/25, gateway 5.6.7.8
 - Jika paket ingin dikirim ke 192.168.90.135, gateway yang akan digunakan 5.6.7.8

Routing

Destination	Gateway	Distance	Prioritas
192.168.0.0/24	10.10.0.1	1	1
192.168.0.0/24	172.16.0.1	4	2
192.168.0.0/29	192.168.1.1	1	3
192.168.0.0/27	192.168.88.1	1	4

IP → 192.168.0.254

Routing

Destination	Gateway	Distance
192.168.10.32/27	10.10.0.1	1
192.168.10.0/27	172.16.0.1	4
192.168.10.0/27	192.168.1.1	1
0.0.0.0/0	192.168.88.1	1

IP → 192.168.10.25

Routing

- Default gateway: router (next hop) dimana semua trafik untuk yang tidak memiliki spesifik tujuan (destination) jelas yang akan di kirim
- Hal ini di bedakan dengan tujuan network menjadi 0.0.0.0/0

Dynamic Route

- Route yang secara dynamic akan memiliki tanda **DAC**
- **D = dynamic**
- **A = Aktif**
- **C = Connected**

IP → Addresses

The top screenshot shows the 'Address List' window with the following data:

	Address	Network	Interface	Comment
D	10.5.120.243/24	10.5.120.0	wlan1	
	192.168.88.1/24	192.168.88.0	bridge-local	default configuration

The bottom screenshot shows the 'Route List' window with the following data:

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	10.5.120.1 reachable wlan1	1		
DAC	10.5.120.0/24	wlan1 reachable	0		10.5.120.243
DAC	192.168.88.0/24	bridge-local reachable	0		192.168.88.1

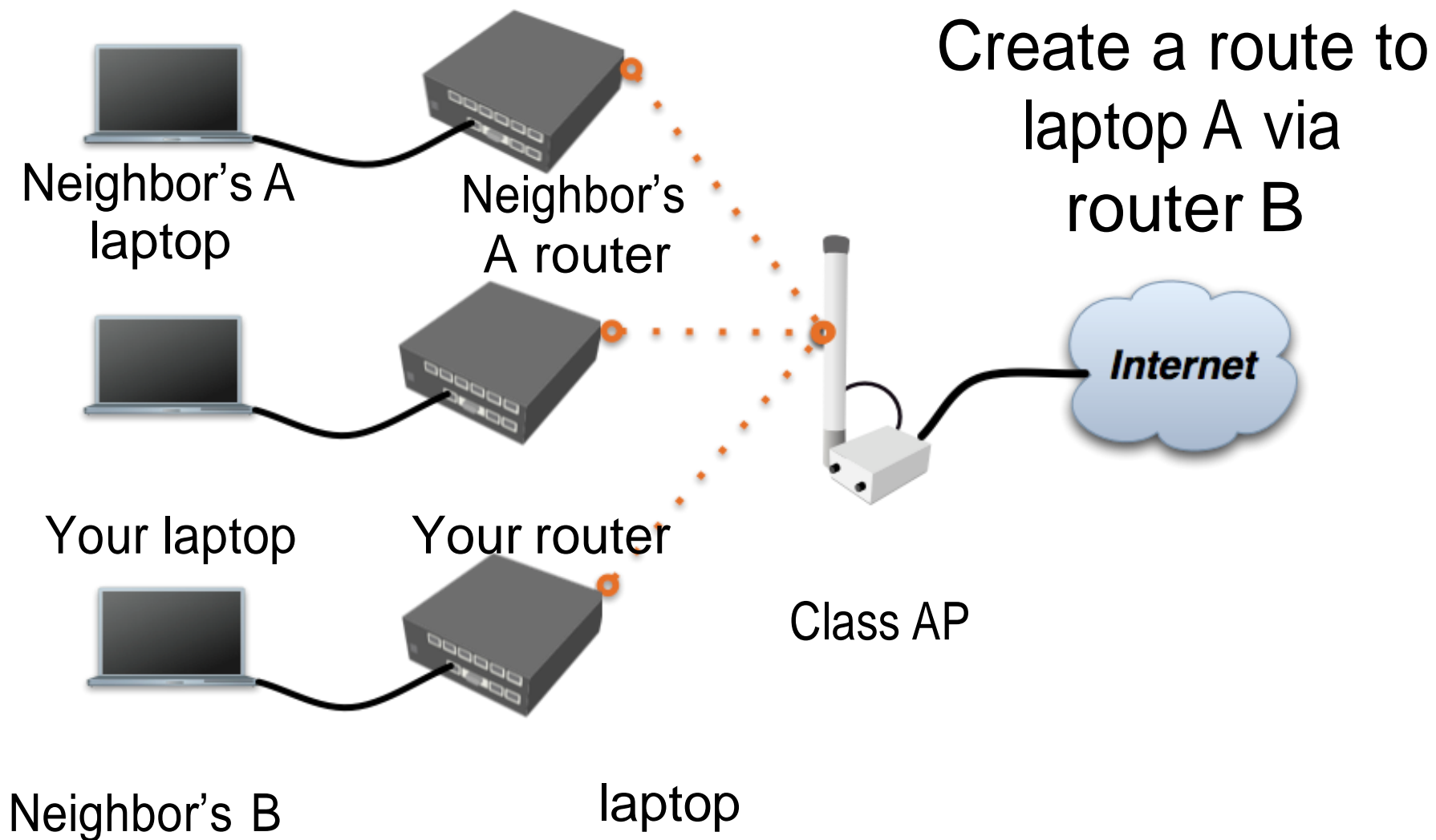
Static Routing

- Static route mendefinisikan bagaimana untuk mencapai network tujuan (destination)
- **Default gateway** juga merupakan static route. Ini menjadikan semua trafik langsung menuju ke gateway

Static Routing

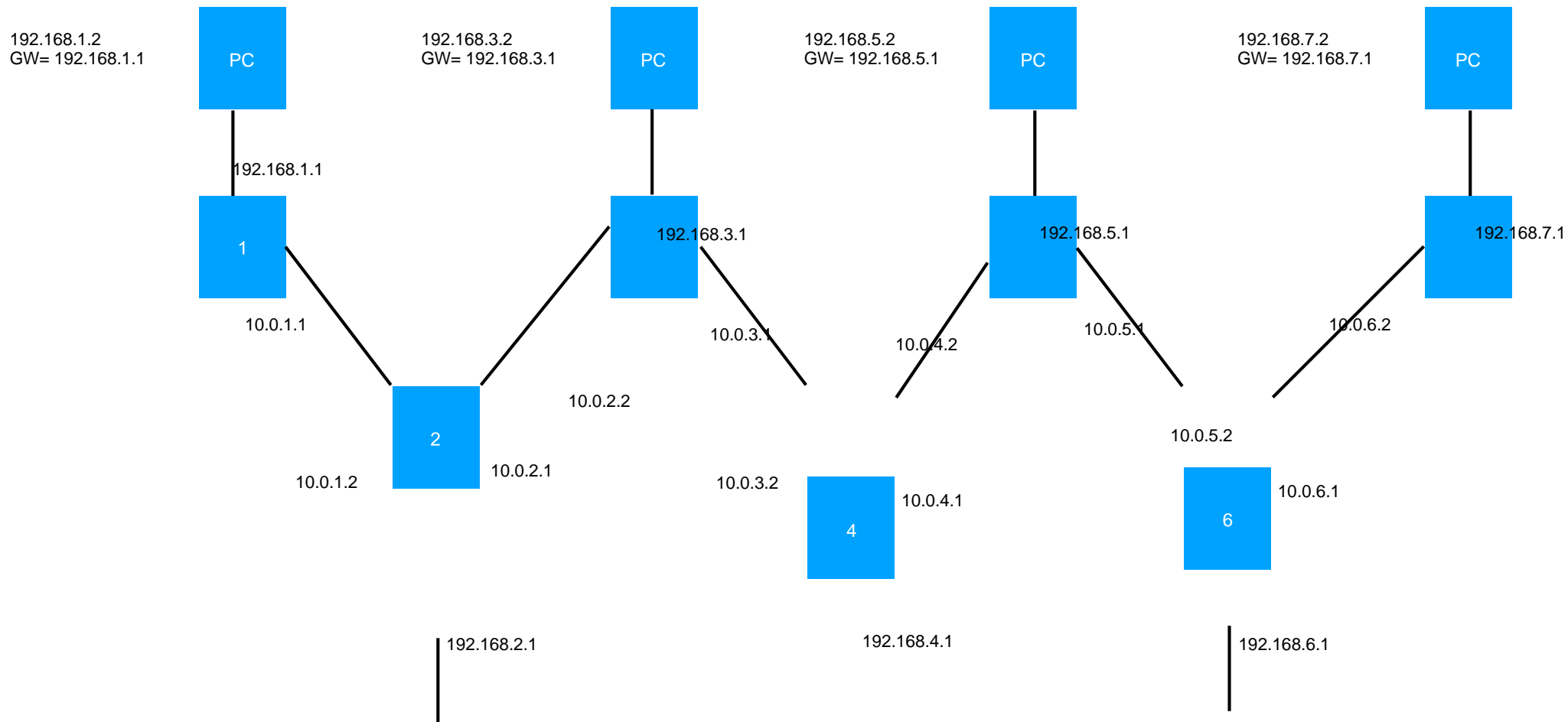
- Mudah untuk di konfig pada network yang kecil
- Sedikit menggunakan resource pada router
- Bukan menjadi pertimbangan yang baik
- Konfigurasi manual perlu dilakukan setiap saat jika terdapat subnet baru yang ingin dicapai

Static Routing

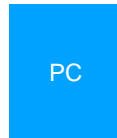


N
e
i
g
h
b
o
r
,
s
B
r
o
u
t
e
r

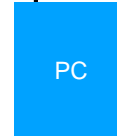
Static Routing



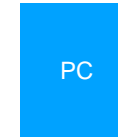
192.168.2.2
GW= 192.168.2.1



192.168.4.2
GW= 192.168.4.1



192.168.6.2
GW= 192.168.6.1



Module 5

Summary



**Certified Network Associate
(MTCNA)**

Module 6

Firewall

Firewall

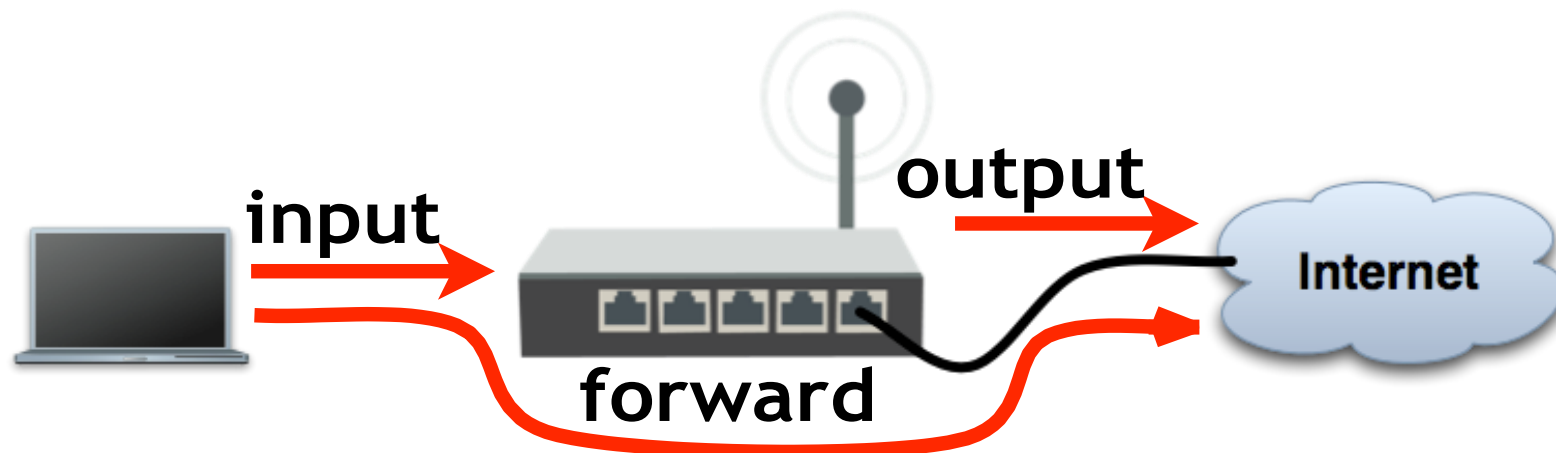
- Merupakan security network system dimana internal network akan di amankan dari luar (internet)
- Berdasarkan aturan yang dianalisa secara berurutan hingga ditemukan kecocokan
- Aturan firewall RouterOS di kelola pada menu Firewall Filter dan Firewall NAT

Firewall Rules

- Bekerja menggunakan **If-Then (Jika - Maka)**
- Berdasaraskan chain yang ber-urutan
- Terdapat chain default yang sudah ditetapkan
- Namun chain baru dapat dibuat

Firewall Filter

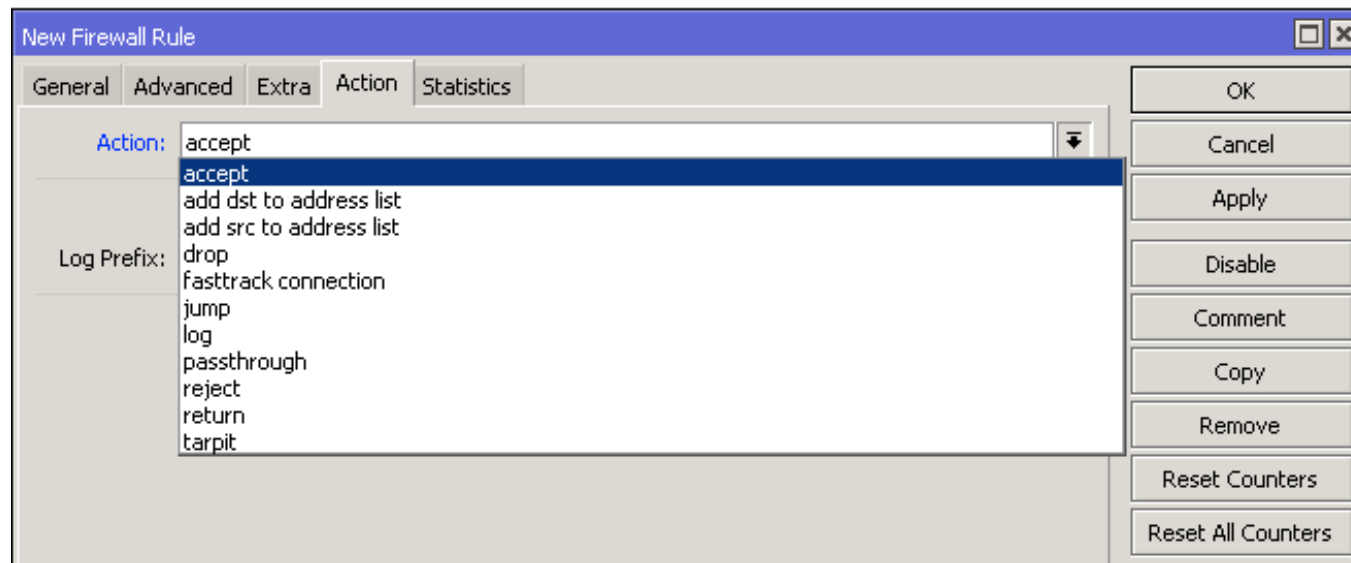
- Default chains yang telah ditetapkan
 - **Input** (menuju router)
 - **Output** (dari router)
 - **Forward** (melalui router)



Filter Actions

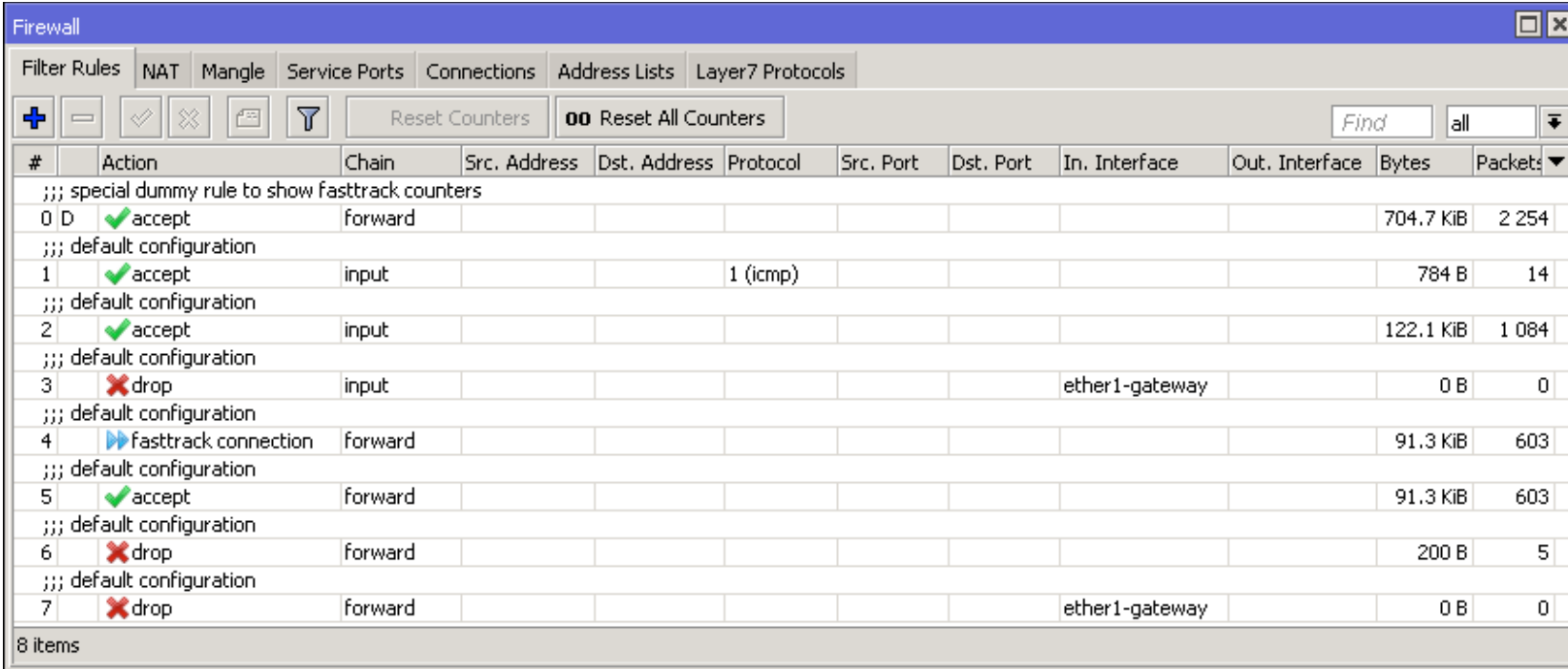
- Setiap aturan memiliki action - apa yang akan dilakukan ketika paket ada yang cocok
- Accept
- Drop (diam-diam) atau reject (drop dan send ICMP status)
- Jump/return menuju atau dari chain yang telah didefinisikan user
- And other - see [firewall wiki page](#)

Filter Actions



IP → Firewall → New Firewall Rule (+) → Action

Filter Chains



#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Interface	Bytes	Packets
;;; special dummy rule to show fasttrack counters											
0	✓ accept	forward								704.7 KiB	2 254
;;; default configuration											
1	✓ accept	input			1 (icmp)					784 B	14
;;; default configuration											
2	✓ accept	input								122.1 KiB	1 084
;;; default configuration											
3	✗ drop	input						ether1-gateway		0 B	0
;;; default configuration											
4	▶ fasttrack connection	forward								91.3 KiB	603
;;; default configuration											
5	✓ accept	forward								91.3 KiB	603
;;; default configuration											
6	✗ drop	forward								200 B	5
;;; default configuration											
7	✗ drop	forward						ether1-gateway		0 B	0

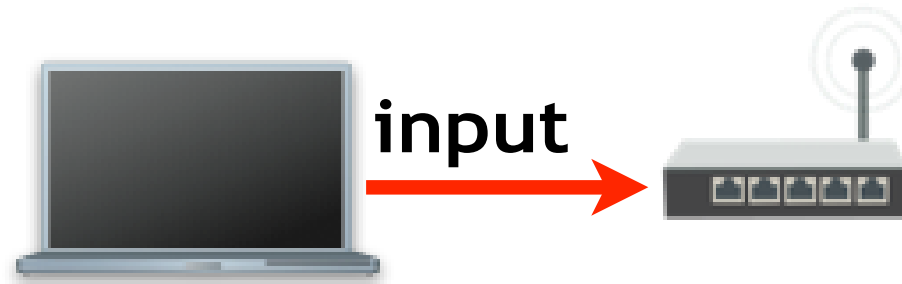
8 items

IP → Firewall

- TIP: alangkah lebih baik jika firewall yang kita buat diberi comments agar mudah dikenali

Chains: input

- Melindungi router
- Salah satunya dari Internet atau dari internal network



Chains: input

- Buatlah action = **accept** chain = **input** aturan filter pada interface yang menuju PC/Laptop anda (src.address = 192.168.X.X)
- Buatlah action = **drop** chain = **input** aturan filter pada interface yang menuju PC/Laptop tanpa src.address (untuk siapa pun)

Chains: input

New Firewall Rule

General Advanced Extra Action Statistics

Chain: input

Src. Address: ☐ 192.168.199.200

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface: ☐ bridge-local

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

IP → Firewall → New Firewall Rule (+)

Chains: input

- Gantilah IP address PC/Laptop anda dengan memasukkan IP yang berbeda yang telah dibuat pada firewall input src.address sebelumnya
- Lakukan percobaan

Chains: forward

- Berisi aturan dimana paket yang melalui router akan dikontrol
- Forward mengontrol lalulintas traffic antara client dan internet maupun antara client diri sendiri

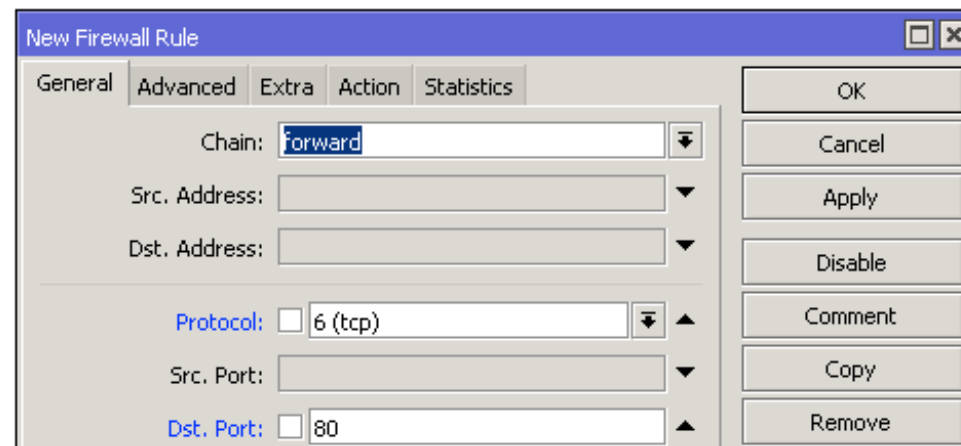


Chains: forward

- Secara default trafik internal antara client yang terhubung ke router akan di izinkan (allowed)
- Trafik antara client dan internet tidak dibatasi

Chains: forward

- Buatlah action = **drop** chain = **forward** aturan filter untuk http port (80/tcp)
- Ketika port lebih specific, IP protocol harus di pilih



IP → Firewall → New Firewall Rule (+)

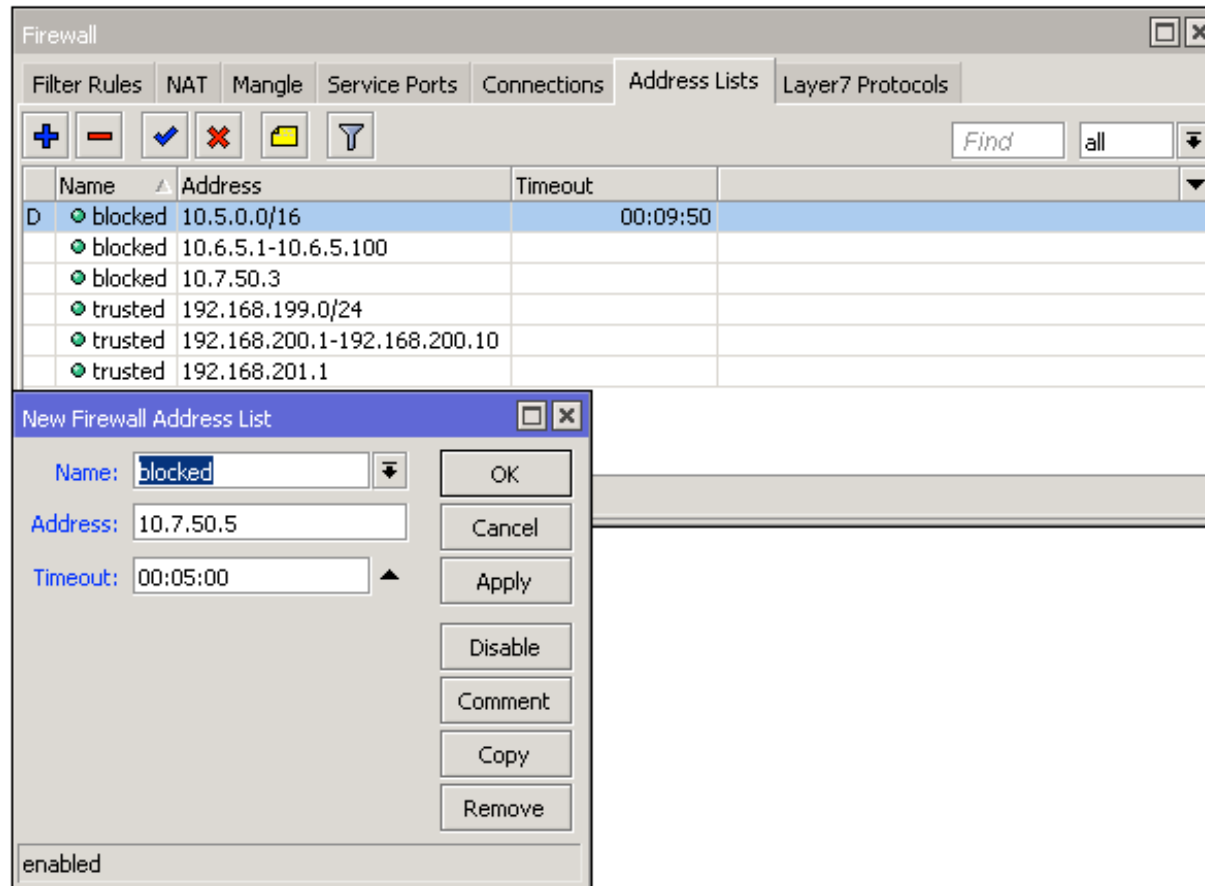
Frequently Used Ports

Port	Service
80/tcp	HTTP
443/tcp	HTTPS
22/tcp	SSH
23/tcp	Telnet
20,21/tcp	FTP
8291/tcp	WinBox
5678/udp	MikroTik Neighbor Discovery
20561/udp	MAC WinBox

Address List

- Address list memungkinkan untuk membuat multiple IP sekaligus
- Hal ini dimungkinkan untuk secara otomatis menambahkan IP address ke address list
- IP bisa di tambahkan ke list secara permanen atau sementara berdasarkan waktu
- Address list dapat berisi single IP address atau satu subnet

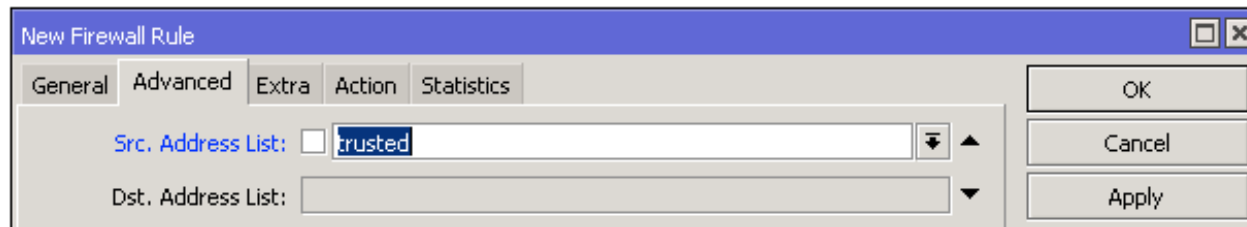
Address List



IP → Firewall → Address Lists → New Firewall Address List (+)

Address List

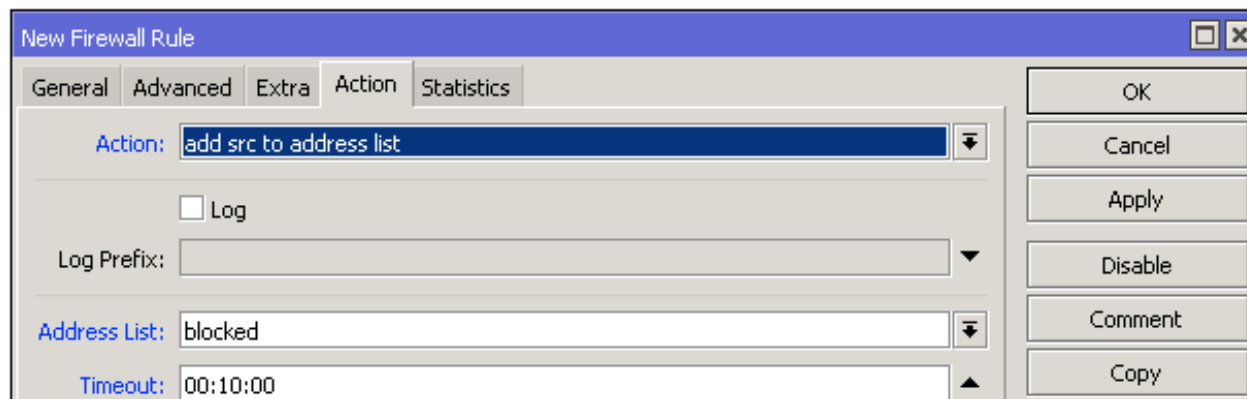
- Address list yang sudah dibuat dimasukan ke dalam src.address list atau dst.address list pada general tab pindahkan ke advanced



IP → Firewall → New Firewall Rule (+) → Advanced

Address List

- Firewall action dapat otomatis membuat address kedalam address list
- Dapat debut permanen atau sementara



IP → Firewall → New Firewall Rule (+) → Action

Address List

- Buatlah address list dengan domain address yang akan kita blok (seperti web porno atau lain-lain)
- Buatlah filter firewall **drop forward** dengan tujuan in-interface lokal stau menuju PC/Laptop anda agar semua traffic dengan tujuan address list yang kita buat dapat diblok

Firewall Log

- Setiap aturan Firewall dapat di masukan ke log
- Dapat ditentukan prefix specific (nama) untuk memudahkan mencari record dikemudian

Firewall Log

The screenshot displays the Mikrotik WinBox interface. The main window is the 'Firewall' configuration page, showing a list of rules. Rule 1 is selected, and its configuration is shown in the 'Firewall Rule <>' dialog box. The 'Action' tab is active, showing 'Action: accept', 'Log' checked, and 'Log Prefix: FWPING'. The 'Log' window is also open, showing a list of log entries for rule 1.

Firewall Rule List:

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Interface	Bytes	Packets
;;; special dummy rule to show fasttrack counters											
0	D	accept	forward							998.6 MIB	1 354 681
;;; default configuration											
1	accept	input			1 (icmp)					336 B	4

Firewall Rule <> Configuration:

- General: Action: accept
- Advanced: Log (checked), Log Prefix: FWPING
- Buttons: OK, Cancel, Apply, Disable

Log Window:

Time	Memory	Firewall, info	FWPING input: in:bridge-local out:(none), src-mac 00:1e:c2:fb:f8:36, proto ICMP (type 8, code 0), 192.168.199.200->192.168.199.254, len 84
Nov/26/2015 14:25:12	memory	firewall, info	FWPING input: in:bridge-local out:(none), src-mac 00:1e:c2:fb:f8:36, proto ICMP (type 8, code 0), 192.168.199.200->192.168.199.254, len 84
Nov/26/2015 14:25:13	memory	firewall, info	FWPING input: in:bridge-local out:(none), src-mac 00:1e:c2:fb:f8:36, proto ICMP (type 8, code 0), 192.168.199.200->192.168.199.254, len 84
Nov/26/2015 14:25:14	memory	firewall, info	FWPING input: in:bridge-local out:(none), src-mac 00:1e:c2:fb:f8:36, proto ICMP (type 8, code 0), 192.168.199.200->192.168.199.254, len 84

IP → Firewall → Edit Firewall Rule → Action

Firewall Log

- Buatlah Log ICMP menggunakan **forward** protocol ICMP dengan prefix pada record yang dapat dicek di log kemudian

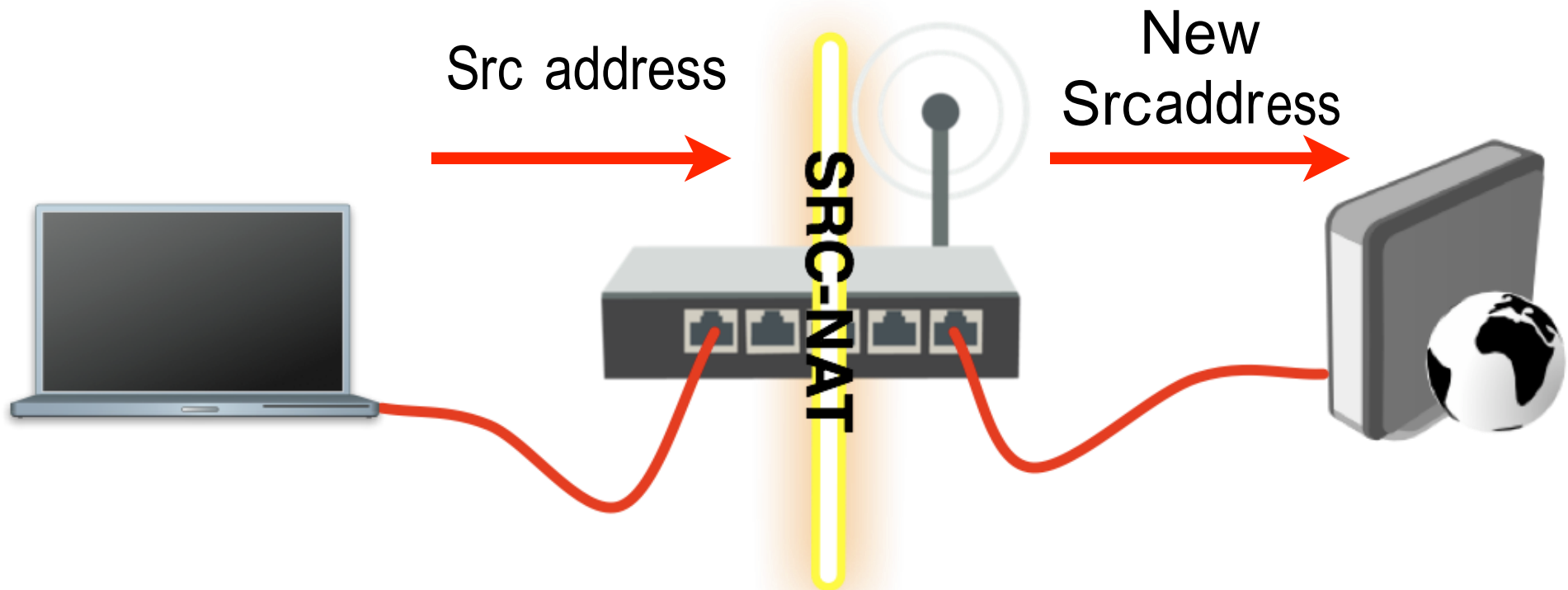
NAT

- Network Address Translation (NAT) adalah metode untuk menentukan atau memodifikasi source dan destination IP address
- NAT memiliki dua type - src-nat (source) dan dst-nat (destination)

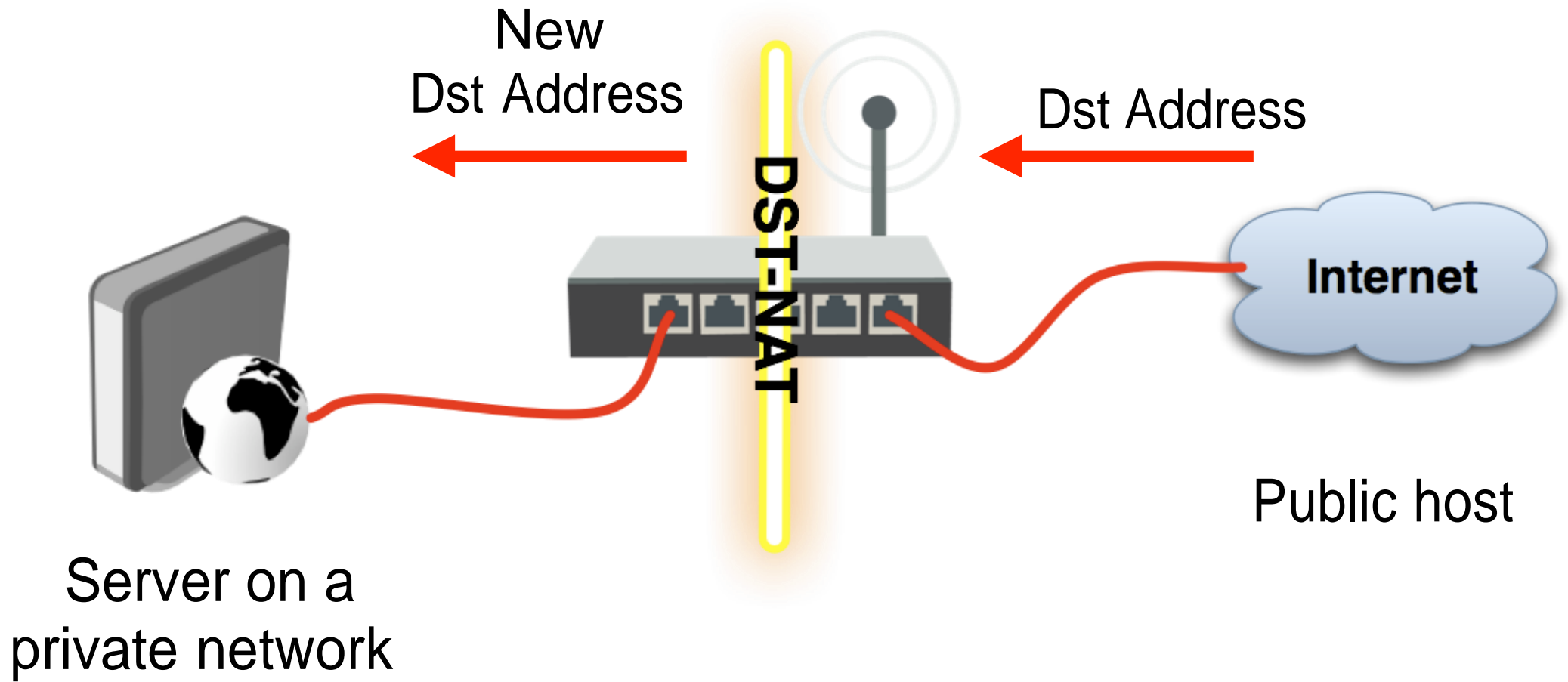
NAT

- NAT yang biasa digunakan untuk menyediakan akses jaringan eksternal agar dapat dikenali IP private (**src-nat**)
- atau dapat digunakan untuk akses jaringan eksternal dengan tujuan IP tertentu dengan port yang lebih spesifik pada network internal (**dst-nat**)

NAT



NAT



Dst NAT

The image displays two screenshots of the Mikrotik WinBox interface, specifically the Firewall NAT configuration section.

Top Screenshot: NAT Rule <80>

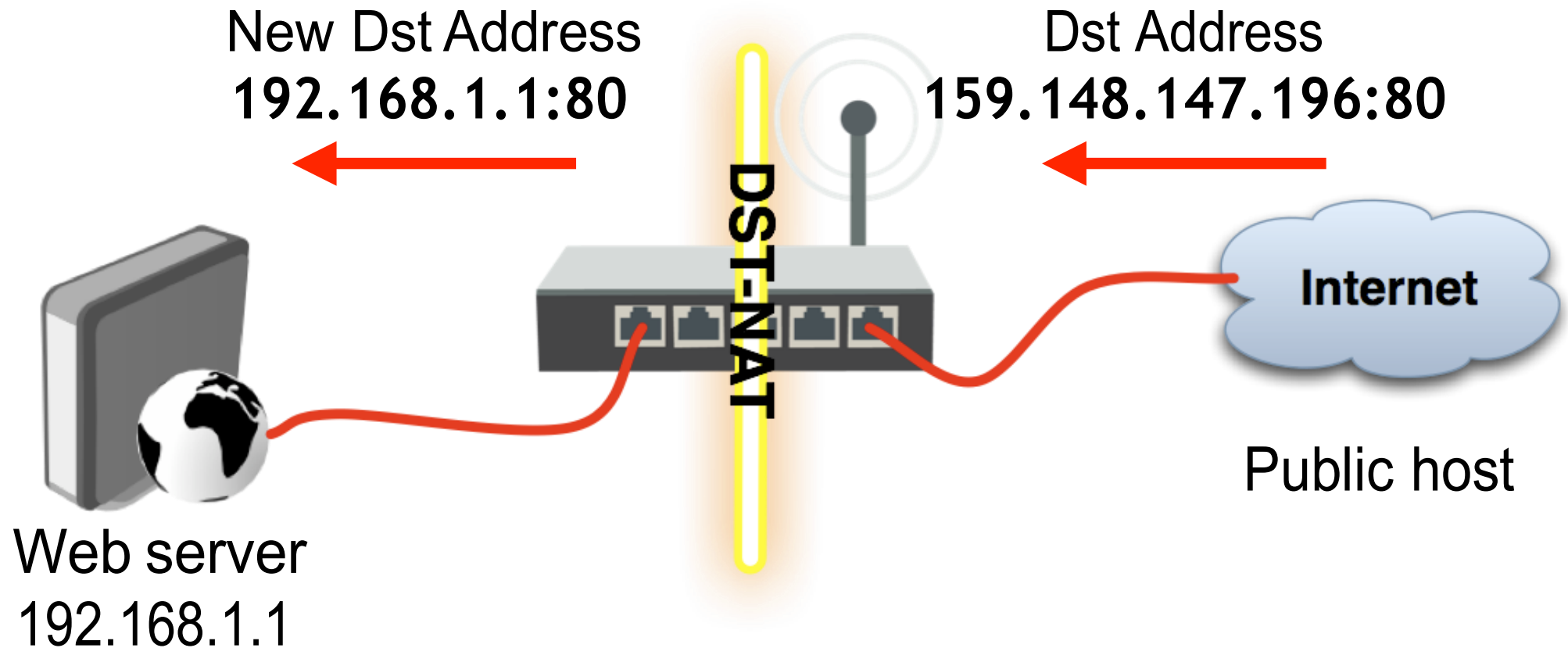
- Chain:** dstnat
- Src. Address:** (empty)
- Dst. Address:** (empty)
- Protocol:** ☐ 6 (tcp)
- Src. Port:** (empty)
- Dst. Port:** ☐ 80
- Any. Port:** (empty)
- In. Interface:** ☐ ether1-gateway
- Out. Interface:** (empty)

Bottom Screenshot: New NAT Rule

- Action:** dst-nat
- ☐ Log
- Log Prefix:** (empty)
- To Addresses:** 192.168.199.200
- To Ports:** 80

IP → Firewall → NAT → New NAT Rule (+)

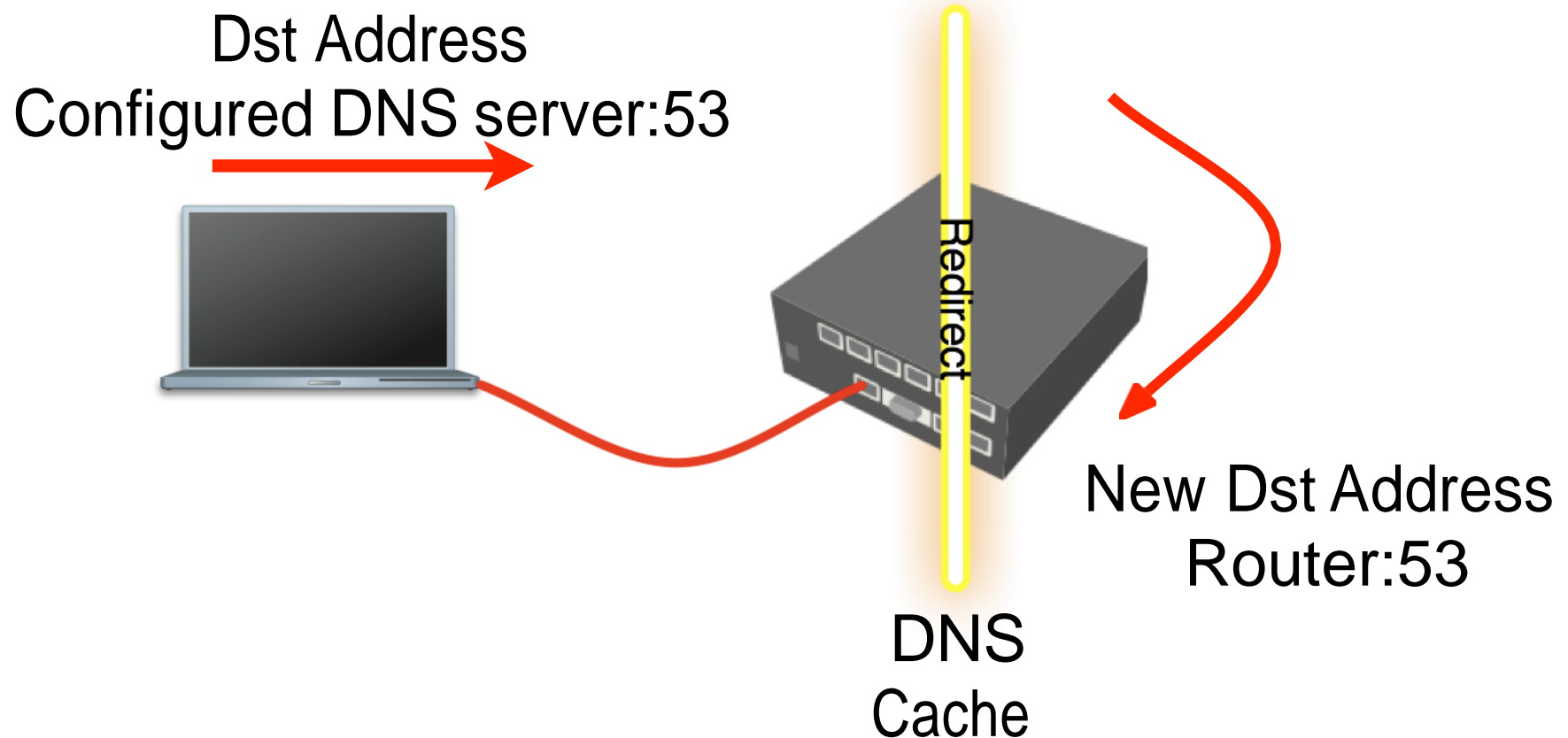
Dst NAT



Redirect

- Spesial type dari pada **dst-nat**
- paket ini akan men redirect sendiri kedalam router
- Biasa digunakan pada transparant proxy service

Redirect

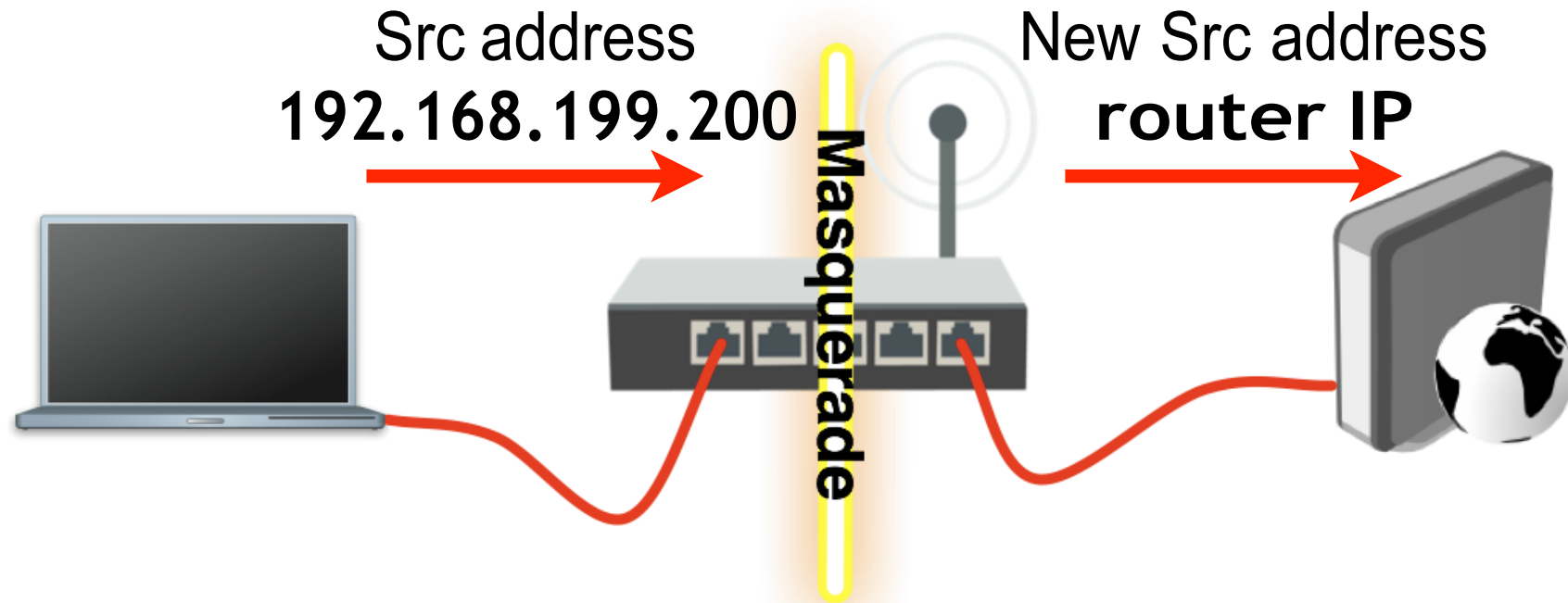


Redirect atau Dst-NAT

LAB

- Buatlah dst-nat dimana semua paket yang request port http (tcp/80) ke dalam router akan di arahkan ketujuan lain

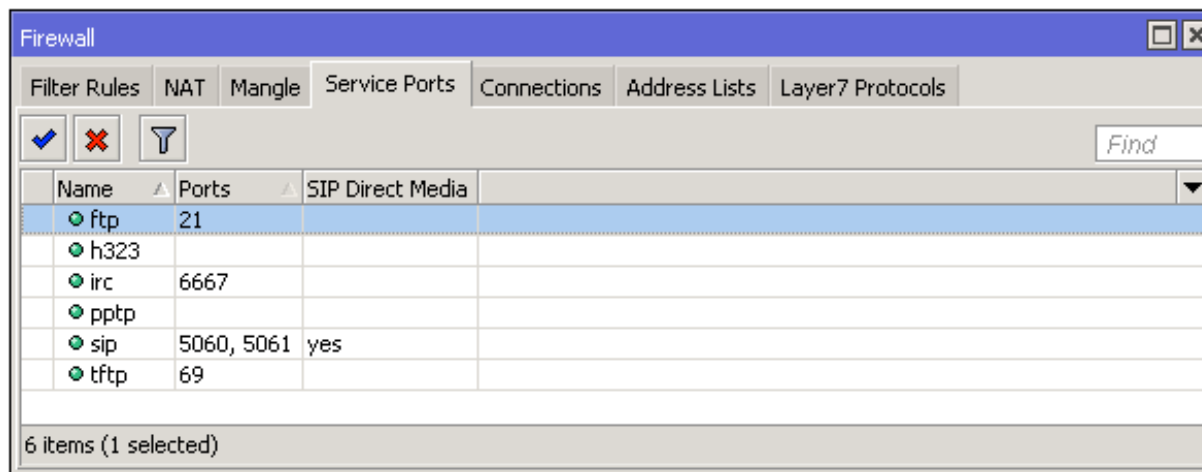
Src-NAT



- **Masquerade** merupakan special type dari srcnat

NAT Helpers

- Beberapa protocol sangat dibutuhkan NAT helper bekerja untuk membantu menentukan secara langsung



IP → Firewall → Service Ports

Connection Tracking

The screenshot shows the Mikrotik WinBox interface. The main window displays the 'Firewall' configuration, specifically the 'Connections' tab. A table lists active connections with columns for Src. Address, Dst. Address, Protocol, Connection Mark, Timeout, and TCP State. One connection is selected (highlighted in blue):

	Src. Address	Dst. Address	Protocol	Connection Mark	Timeout	TCP State
C	192.168.199.200:17500	255.255.255.255:17500	17 (udp)		00:00:09	
SACFs	192.168.199.200:11785	213.199.179.172:40035	17 (udp)		00:00:30	
SACFs	192.168.199.200:11785	213.199.179.157:40023	17 (udp)		00:02:35	
SACFs	192.168.199.200:11785	213.199.179.153:40025	17 (udp)		00:00:30	
C	192.168.199.200:17500	192.168.199.255:17500	17 (udp)		00:00:09	
SAC	192.168.199.200:59898	192.168.199.254:8291	6 (tcp)		23:59:59	established
SACFs	192.168.199.200:62355	191.235.128.131:443	6 (tcp)		00:00:09	close
SACFs	192.168.199.200:11785	157.56.52.44:40026	17 (udp)		00:00:30	
SACFs	192.168.199.200:11785	157.56.52.29:40021	17 (udp)		00:02:32	
SACFs	192.168.199.200:11785	157.55.235.172:40018	17 (udp)		00:02:30	
SACFs	192.168.199.200:11785	157.55.235.172:40002	17 (udp)		00:02:35	
SACFs	192.168.199.200:11785	157.55.235.157:40021	17 (udp)		00:02:32	
SACFs	192.168.199.200:11785	157.55.235.146:40005	17 (udp)		00:00:27	
SACFs	192.168.199.200:11785	157.55.130.176:40035	17 (udp)		00:02:32	
SACFs	192.168.199.200:11785	157.55.56.148:40032	17 (udp)		00:02:32	
SACFs	192.168.199.200:11785	152.236.66.231:48760	17 (udp)		00:02:32	
SACFs	192.168.199.200:11785	111.221.77.174:40003	17 (udp)		00:02:32	
SACFs	192.168.199.200:11785	111.221.77.170:40013	17 (udp)		00:00:31	

At the bottom of the table, it says '41 items (1 selected)' and 'Max Entries: 88080'.

Overlaid on the right is the 'Connection Tracking' settings dialog. It has a title bar with a close button. The 'Enabled' dropdown is set to 'auto'. There are 'OK', 'Cancel', and 'Apply' buttons on the right. The settings are as follows:

- TCP Syn Sent Timeout: 00:00:05
- TCP Syn Received Timeout: 00:00:05
- TCP Established Timeout: 1d 00:00:00
- TCP Fin Wait Timeout: 00:00:10
- TCP Close Wait Timeout: 00:00:10
- TCP Last Ack Timeout: 00:00:10
- TCP Time Wait: 00:00:10
- TCP Close: 00:00:10
- TCP Max Retransmit Timeout: 00:05:00
- TCP Unacked Timeout: 00:05:00
- UDP Timeout: 00:00:10
- UDP Stream Timeout: 00:03:00
- ICMP Timeout: 00:00:10
- Generic Timeout: 00:10:00

IP → Firewall → Connections

FastTrack

Without	With
360Mbps	890Mbps
Total CPU usage 100%	Total CPU usage 86%
44% CPU usage on firewall	6% CPU usage on firewall

* Tested on RB2011 with a single TCP stream

- For more info see [FastTrack wiki page](#)

Module 6

Summary



**Certified Network Associate
(MTCNA)**

Module 7

Quality of Service

Quality of Service

- QoS secara keseluruhan merupakan kinerja dari pada network, khususnya kinerja yang biasa dilihat pada user network
- RouterOS mengimplementasikan QoS untuk digunakan membatasi speed (shaping), traffic prioritas dan lainnya

Simple Queue

Specify client →

Specify Max Limit for the client →

The image shows two overlapping windows from a network configuration tool. The top window, titled 'Queue List', has tabs for 'Simple Queues', 'Interface Queues', 'Queue Tree', and 'Queue Types'. It contains a table with columns: '#', 'Name', 'Target', 'Upload Max Limit', 'Download Max Limit', 'Packet Marks', and 'Total Max Limit (bits/s)'. The bottom window, titled 'New Simple Queue', has tabs for 'General', 'Advanced', 'Statistics', 'Traffic', 'Total', and 'Total Statistics'. The 'General' tab is active, showing fields for 'Name' (set to 'queue1'), 'Target' (set to '192.168.199.200'), and 'Dst.'. Below these are 'Target Upload' and 'Target Download' sections, each with a 'Max Limit' field (set to '256k' and '512k' respectively) and a 'Burst' section with 'Burst Limit', 'Burst Threshold', and 'Burst Time' fields. The 'Max Limit' fields are highlighted with red arrows from the text 'Specify Max Limit for the client'. The 'Name' field is highlighted with a red arrow from the text 'Specify client'. The 'enabled' checkbox at the bottom is checked.

Queues → New Simple Queue(+)

- Disable Firewall FastTrack rule for Simple Queue to work

Simple Queue

- Queue simple dapat membatasi trafik suatu tujuan yang ditentukan

Set Target to any
Set Dst. to server
address

The screenshot shows the 'Simple Queue <queue1>' configuration window. The 'General' tab is selected. The 'Name' field is 'queue1'. The 'Target' field is '0.0.0.0/0' and the 'Dst.' field is '1.2.3.4'. The 'Max Limit' for Target Upload is '128k' and for Target Download is '256k'. The 'Burst Limit' for both is 'unlimited'. The 'Burst Threshold' for both is 'unlimited'. The 'Burst Time' for both is '0'. The 'enabled' checkbox is checked. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', 'Reset All Counters', and 'Torch'.

Queues

Torch

- Real-time traffic monitoring tool

Set interface →

Set laptop address ←

Observe the traffic →

The screenshot shows the Torch (Running) window with the following settings:

- Basic:** Interface: ether2-master-local, Entry Timeout: 00:00:03 s
- Collect:** ☒ Src. Address, ☒ Src. Address6, ☒ Dst. Address, ☒ Dst. Address6, ☐ MAC Protocol, ☒ Port, ☐ VLAN Id, ☐ DSCP
- Filters:** Src. Address: 192.168.199.200, Dst. Address: 0.0.0.0/0, Src. Address6: ::/0, Dst. Address6: ::/0, MAC Protocol: all, Protocol: any, Port: any, VLAN Id: any, DSCP: any

Buttons: Start, Stop, Close, New Window

Eth.	Protocol	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800	(ip)	6 (tcp)	192.168.199.200:55369	205.251.219.190:80 (http)			242.2 kbps	8.8 kbps	20	16
800	(ip)	6 (tcp)	192.168.199.200:54832	192.168.199.254:8291 (winbox)			17.0 kbps	1584 bps	3	3

2 items (1 selected) | Total Tx: 259.3 kbps | Total Rx: 10.4 kbps | Total Tx Packet: 23 | Total Rx Packet: 19

Tools → Torch
Torch

Guaranteed Bandwidth

- Digunakan untuk memastikan client mendapatkan batas minimum bandwidth
- Trafik yang akan dibagi berdasarkan yang diterima pertama maka dia akan mendapatkan lebih dahulu
- Konfigurasi guaranteed bandwidth terdapat pada **limit-at** parameter

Guaranteed Bandwidth

Set limit at



Simple Queue <129>

General Advanced Statistics Traffic Total Total Statistics

Packet Marks:

	Target Upload	Target Download
Limit At:	<input type="text" value="1M"/>	<input type="text" value="1M"/>
Priority:	<input type="text" value="8"/>	<input type="text" value="8"/>
Queue Type:	<input type="text" value="default-small"/>	<input type="text" value="default-small"/>
Parent:	<input type="text" value="parent"/>	

enabled

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

Queues → Simple Queue → Edit → Advanced

Burst

- Digunakan untuk memberikan batas lebih dari yang ditentukan max limit dengan priode
- Berguna untuk HTTP traffic - membuat web pages berjalan lebih cepat
- Untuk downloads file max limit yang akan bekerja

Burst

**Set burst limit,
threshold and
time**

Simple Queue <queue1>

General Advanced Statistics Traffic Total Total Statistics

Name: queue1

Target: 192.168.199.200

Dst.:

Target Upload Target Download

Max Limit: 256k 512k bits/s

Burst

Burst Limit: 4M 4M bits/s

Burst Threshold: 2M 2M bits/s

Burst Time: 16 16 s

Time

enabled

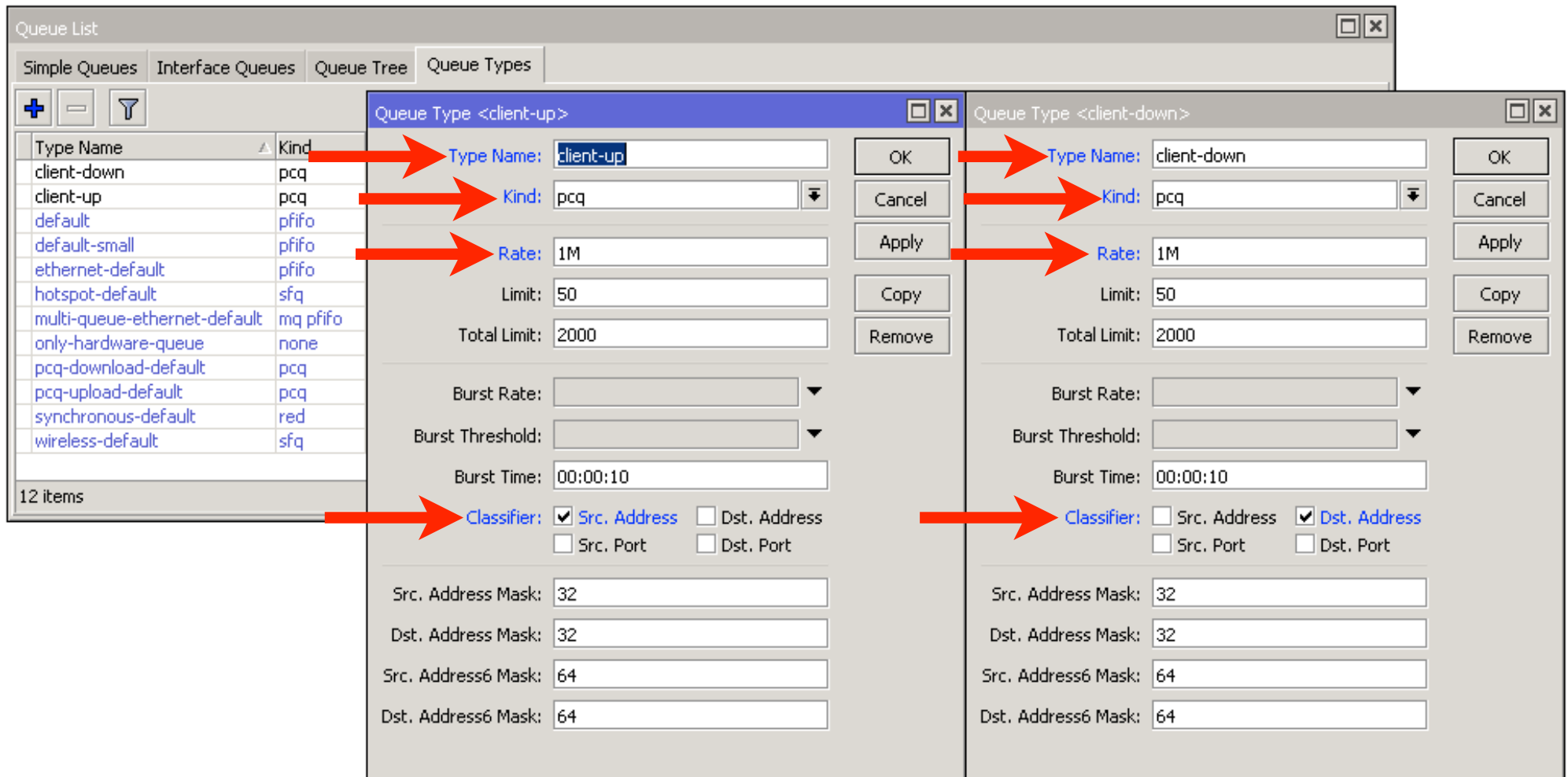
OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters Torch

Queues → Simple Queue → Edit

Per Connection Queueing

- Queue memiliki type salah satunya adalah PCQ
- PCQ mengoptimalkan bandwidth berdasarkan penggunaan
- Beberapa golongan digunakan seperti
 - source/destination IP address
 - source/destination port

PCQ



Queues → Queue Type → New Queue Type(+)

PCQ

**WAN
interface**

**LAN
interface**

The image shows two overlapping Mikrotik WinBox windows. The top window is titled 'Queue List' and has tabs for 'Simple Queues', 'Interface Queues', 'Queue Tree', and 'Queue Types'. The 'Interface Queues' tab is active, showing a table with 6 items. The second item, 'ether2-master-local', is selected. Below the table, it says '6 items (1 selected)'. The bottom window is titled 'Interface Queue <wlan1>' and shows configuration for the 'wlan1' interface. The 'Queue Type' is set to 'client-up'. Below this, there is another window titled 'Interface Queue <ether2-master-local>' showing configuration for the 'ether2-master-local' interface. The 'Queue Type' is set to 'client-down'.

Interface	Queue Type	Default Queue Type
ether1-gateway	only-hardware-queue	only-hardware-queue
ether2-master-local	only-hardware-queue	only-hardware-queue
ether3-slave-local	only-hardware-queue	only-hardware-queue
ether4-slave-local	only-hardware-queue	only-hardware-queue
ether5-slave-local	only-hardware-queue	only-hardware-queue
wlan1	only-hardware-queue	wireless-default

6 items (1 selected)

Interface Queue <wlan1>

Interface: wlan1

Queue Type: client-up

Default Queue Type: wireless-default

Interface Queue <ether2-master-local>

Interface: ether2-master-local

Queue Type: client-down

Default Queue Type: only-hardware-queue

Queues → Interface Queues

Module 7

Summary



**Certified Network Associate
(MTCNA)**

Module 8

Tunnels

Point-to-Point Protocol

- Point-to-Point Protocol (PPP) digunakan untuk membuat tunneling (direct connection)
- PPP bisa menggunakan authentication, enkripsi dan kompresi
- RouterOS support PPP tunnel seperti PPPoE, SSTP, PPTP dan tunnel lainnya

PPPoE

- Point-to-Point Protocol over Ethernet berjalan pada protocol layer 2 yang digunakan untuk akses/terhubung ke networknya
- PPPoE bisa digunakan tanpa IP address yang terinstall pada perangkat
- Menggunakan authentication untuk terhubung

PPPoE Client

**Set
interface,
service,
username,
password**



PPP

Interface | PPPoE Servers | Secrets | Profiles | Active Connections | L2TP Secrets

+ - ✓ ✗ [Filter] PPP Scanner PPTP Server SSTP Server L2TP Server OVPN Server PPPoE Scan Find

Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
------	------	--------	----	----	-----------------	-----------------

New Interface

General | Dial Out | Status | Traffic

Name: pppoe-out1

Type: PPPoE Client

L2 MTU:

Max MTU: 1480

Max MRU: 1480

MRRU: 1600

Interfaces: ether1-gateway

OK Cancel Apply Disable Comment Copy Remove Torch PPPoE Scan

enabled running slave Status:

New Interface

General | Dial Out | Status | Traffic

Service: MikroTik

AC Name:

User: mtcnaclass

Password: *****

Profile: default-encryption

Keepalive Timeout: 60

☐ Dial On Demand

☐ Use Peer DNS

☒ Add Default Route

Default Route Distance: 0

Allow: ☒ mschap2 ☒ mschap1 ☒ chap ☒ pap

OK Cancel Apply Disable Comment Copy Remove Torch PPPoE Scan

enabled running slave Status:

PPP → New PPPoE Client(+)

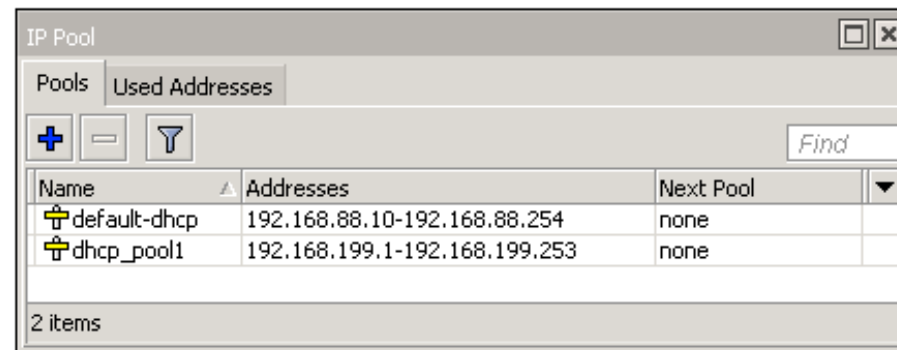
PPPoE Client

- Jika terdapat banyak atau lebih dari satu PPPoE server maka **service name** harus lebih spesifik
- Jika tidak ditentukan maka client akan mencoba terhubung ke yang merespon lebih dulu

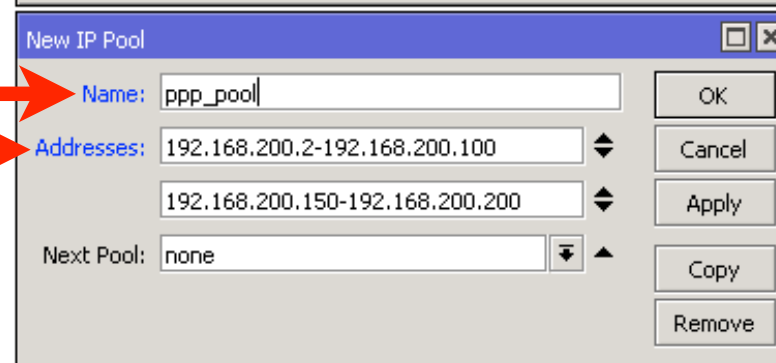
IP Pool

- Mendefinisikan range IP address untuk menghandel RouterOS service
- Seperti DHCP, PPP, dan Hotspot
- Akan mendapatkan address secara otomatis dari pool

IP Pool



**Set the pool
name and
address range(s)**



IP → Pool → New IP Pool(+)

PPP Profile

- Profile digunakan PPP server untuk PPP client
- Dengan menggunakan PPP Profile maka multiple client akan bisa kita seting sesuai yang di inginkan
- Misalkan digunakan untuk memberikan IP address dalam jumlah yang telah ditentukan

PPP Profile

**Set the local
and remote
address of
the tunnel**

The screenshot shows the 'PPP' configuration window with the 'Profiles' tab selected. Below the main table, the 'New PPP Profile' dialog box is open. The 'General' tab is active, showing the following settings:

- Name: profile1
- Local Address: 192.168.200.1
- Remote Address: ppp_pool
- Bridge: ppp_pool
- Bridge Port Priority: (empty)
- Bridge Path Cost: (empty)
- Incoming Filter: (empty)
- Outgoing Filter: (empty)
- Address List: (empty)
- DNS Server: (empty)
- WINS Server: (empty)
- Change TCP MSS: ☒ no ☐ yes ☒ default
- Use UPnP: ☒ no ☐ yes ☒ default

On the right side of the dialog, the 'Protocols' tab is active, showing the following settings:

- Use MPLS: ☐ no ☐ yes ☐ required ☒ default
- Use Compression: ☐ no ☐ yes ☒ default
- Use Encryption: ☐ no ☒ yes ☐ required ☐ default

Red arrows point from the text 'Set the local and remote address of the tunnel' to the 'Local Address' and 'Remote Address' fields. Another red arrow points from the text 'It is suggested to use encryption' to the 'Use Encryption' radio button.

**It is suggested to
use encryption**

PPP → Profiles → New PPP Profile(+)

PPP Secret

- Local database user PPP
- Username, password dan lain yang lebih specific dapat dikonfig
- Seperti kita menentukan PPP profile yang telah kita buat
- PPP secret akan menyesuaikan PPP profile setting

PPP Secret

**Set the username,
password and
profile. Specify
service if necessary**

PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

PPP Authentication&Accounting

Name	Password	Service	Caller ID	Profile	Local Address	Remote Address	Last Logged Out
------	----------	---------	-----------	---------	---------------	----------------	-----------------

New PPP Secret

Name: client1

Password: *****

Service: any

Caller ID:

Profile: profile1

Local Address:

Remote Address:

Routes:

Limit Bytes In:

Limit Bytes Out:

Last Logged Out:

enabled

OK Cancel Apply Disable Comment Copy Remove

PPP → Secrets → New PPP Secret(+)

PPPoE Server

- PPPoE server berjalan di dalam interface yang akan dituju
- Tidak dapat dikonfigurasi pada interface yang terdapat bridge
- Untuk alasan keamanan IP address tidak harus digunakan atau dipasang pada interface yang akan dijalankan PPPoE Server

PPPoE Server

Set the service name, interface, profile and authentication protocols

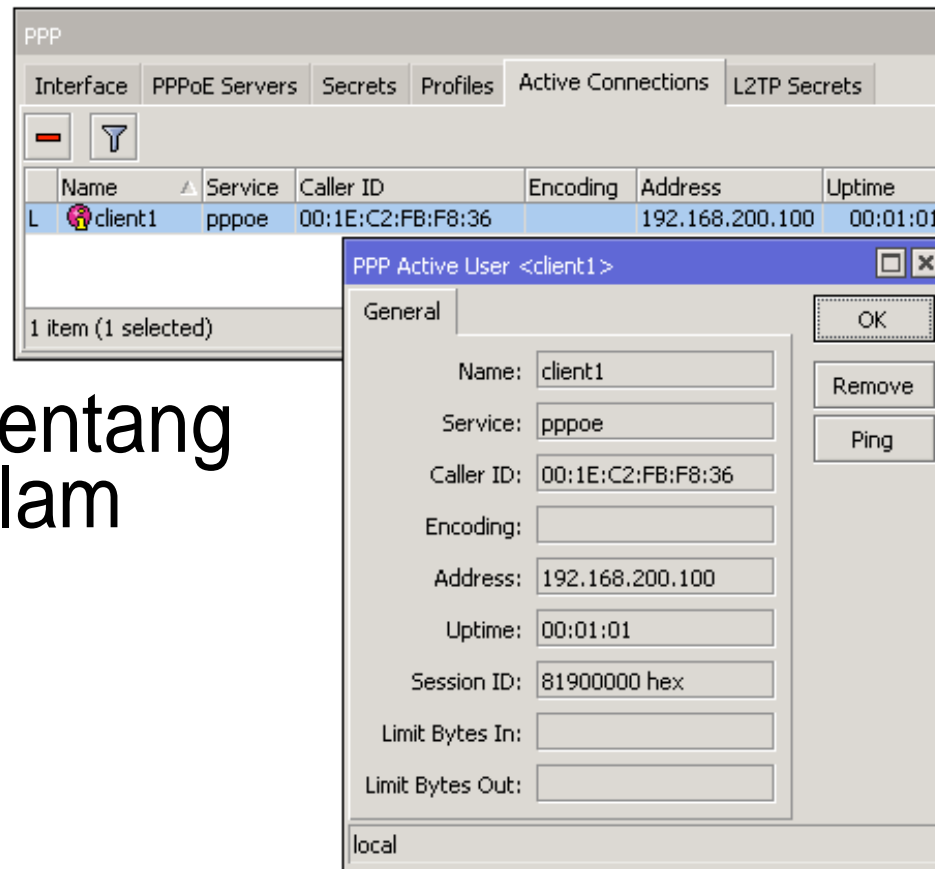
The screenshot shows the 'New PPPoE Service' configuration window. Red arrows point to the following fields:

- Service Name:** ppoe_server
- Interface:** ether5
- Default Profile:** profile1
- Authentication:** ☒ mschap2, ☐ mschap1, ☐ chap, ☐ pap

Other visible fields include Max MTU (1480), Max MRU (1480), MRRU (1600), and Keepalive Timeout (10). The 'enabled' checkbox at the bottom is checked.

PPP Status

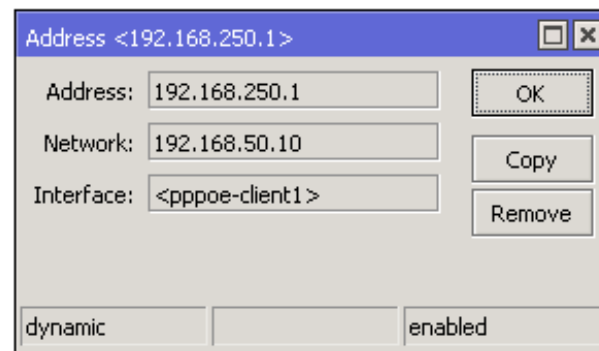
- Information tentang PPP user dalam kondisi aktif



PPP → Active Connections

Point-to-Point Addressing

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



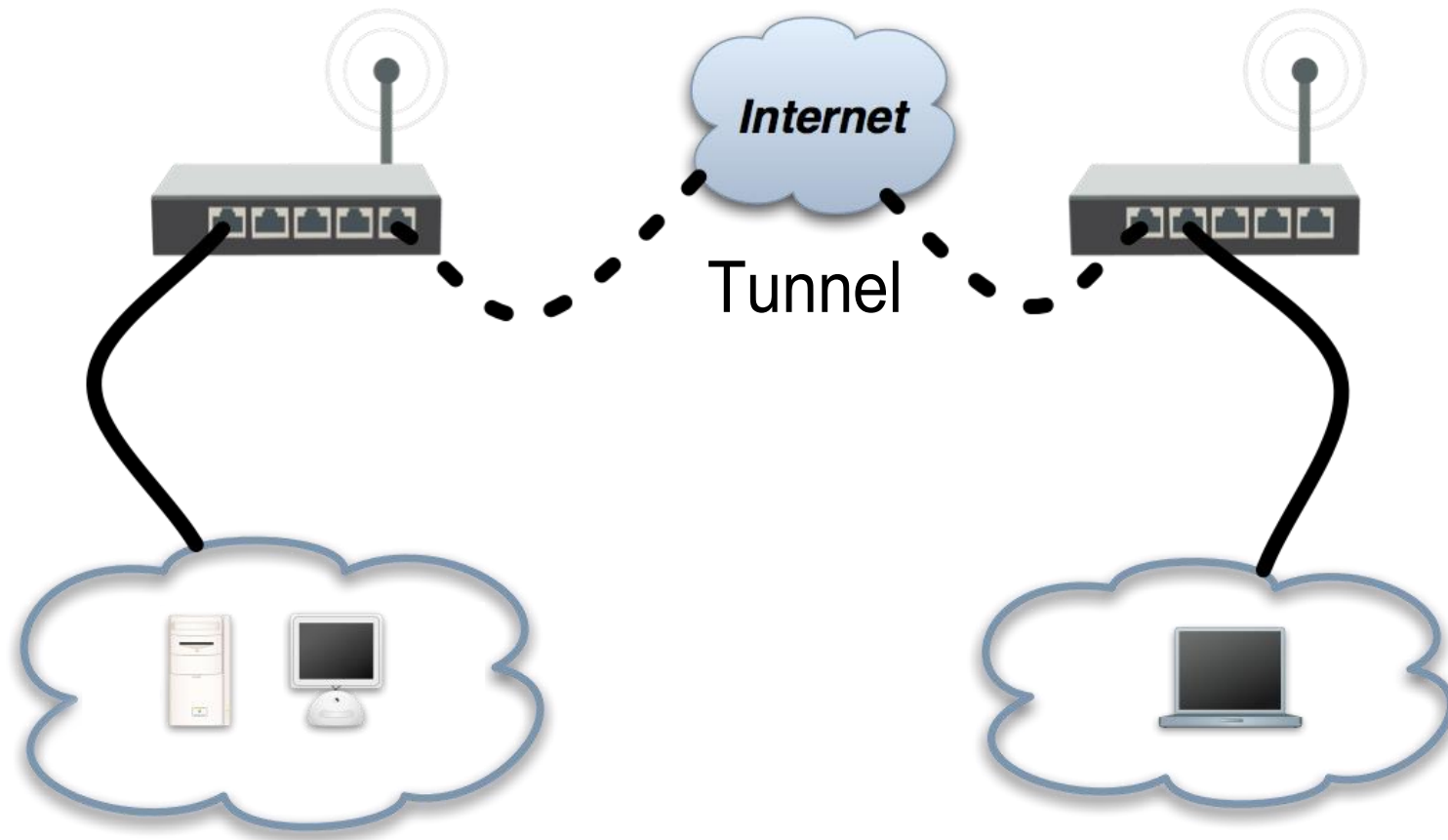
Point-to-Point Addressing

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

PPTP

- Point-to-Point Tunneling Protocol (PPTP) melayani enkripsi tunnel melalui IP
- Dapat digunakan sebagai koneksi yang aman antara lokal network melalui Internet
- RouterOS support menjalankan PPTP client dan server secara bersamaan
- NAT helper digunakan untuk mendukung PPTP didalam NAT
- Port tcp/1723 dan IP protocol nomor 47 - GRE

PPTP Tunnel



PPTP Client

Set name,
PPTP server
IP address,
username,
password

The image shows two overlapping 'New Interface' dialog boxes from a PPP configuration utility. The left dialog is for a PPTP Client, and the right dialog is for a PPTP Server. A red arrow points from the text 'Set name, PPTP server IP address, username, password' to the 'Name' field in the left dialog.

Left Dialog (New Interface):

- General tab selected.
- Name: pptp-out1
- Type: PPTP Client
- L2 MTU: (empty)
- Max MTU: 1450
- Max MRU: 1450
- MRRU: 1600
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch.
- Status: enabled, running, slave.

Right Dialog (New Interface):

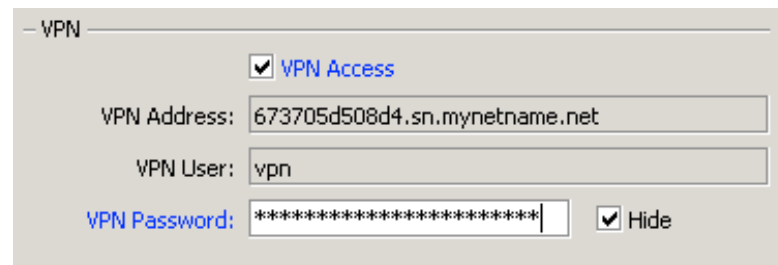
- General tab selected.
- Connect To: 1.2.3.4
- User: pptpclient1
- Password: (masked with asterisks)
- Profile: default-encryption
- Keepalive Timeout: 60
- Options: ☐ Dial On Demand, ☐ Add Default Route.
- Default Route Distance: 0
- Allowed Protocols: ☒ mschap2, ☒ mschap1, ☒ chap, ☒ pap.
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch.
- Status: enabled, running, slave.

PPP → New PPTP Client(+)

PPTP Server

- RouterOS melayani simple PPTP Server untuk mempermudah setup
- Gunakan QuickSet untuk enable VPN Access

**Enable VPN
access and
set VPN
password**



The screenshot shows the 'VPN' configuration window in RouterOS QuickSet. It includes a checkbox for 'VPN Access' which is checked. Below this, there are three input fields: 'VPN Address' with the value '673705d508d4.sn.mynetname.net', 'VPN User' with the value 'vpn', and 'VPN Password' with a masked password '*****'. A 'Hide' checkbox is also present next to the password field.

- VPN	
<input checked="" type="checkbox"/>	VPN Access
VPN Address:	673705d508d4.sn.mynetname.net
VPN User:	vpn
VPN Password:	***** <input checked="" type="checkbox"/> Hide

SSTP

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

SSTP Client

Set name,
SSTP server
IP address,
username,
password

The screenshot shows the PPP configuration window with two 'New Interface' dialog boxes open. The left dialog is for 'SSTP Client' and the right is for 'SSTP Server'. Red arrows point to the 'Name', 'Connect To', 'User', and 'Password' fields.

Left Dialog (SSTP Client):

- Name: sstp-out1
- Type: SSTP Client
- L2 MTU: (empty)
- Max MTU: 1500
- MRRU: 1600

Right Dialog (SSTP Server):

- Connect To: 1.2.3.4
- Port: 443
- Proxy: (empty)
- Proxy Port: 443
- Certificate: none
- ☐ Verify Server Certificate
- ☒ Verify Server Address From Certificate
- ☐ PFS
- User: sstpclient1
- Password: (masked)
- Profile: default-encryption
- Keepalive Timeout: 60
- ☐ Dial On Demand
- ☐ Add Default Route
- Default Route Distance: 0
- Allow: ☒ mschap2 ☒ mschap1 ☒ chap ☒ pap

SSTP Client

- Untuk terhubung ke windows, harus memiliki sertifikat yang valid
- namun pada perangkat RouterOS ke RouterOS tidak memerlukan sertifikat (SSL)
- Sertifikat dapat dibuat pada system - certificate (certificate authority - CA)

Module 8

Summary



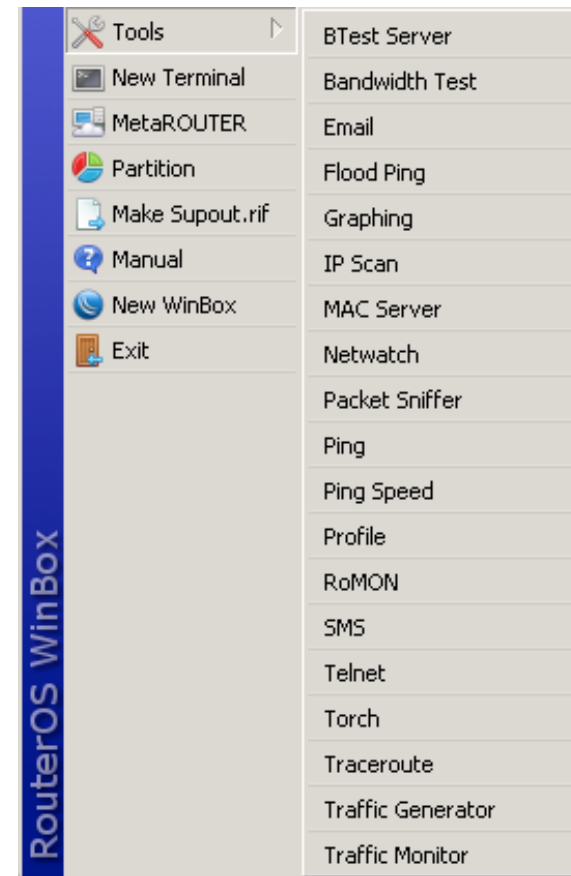
**Certified Network Associate
(MTCNA)**

Module 9

Misc

RouterOS Tools

- RouterOS memiliki variasi utilities yang dapat membantu network administrator me monitor router lebih sepesifik



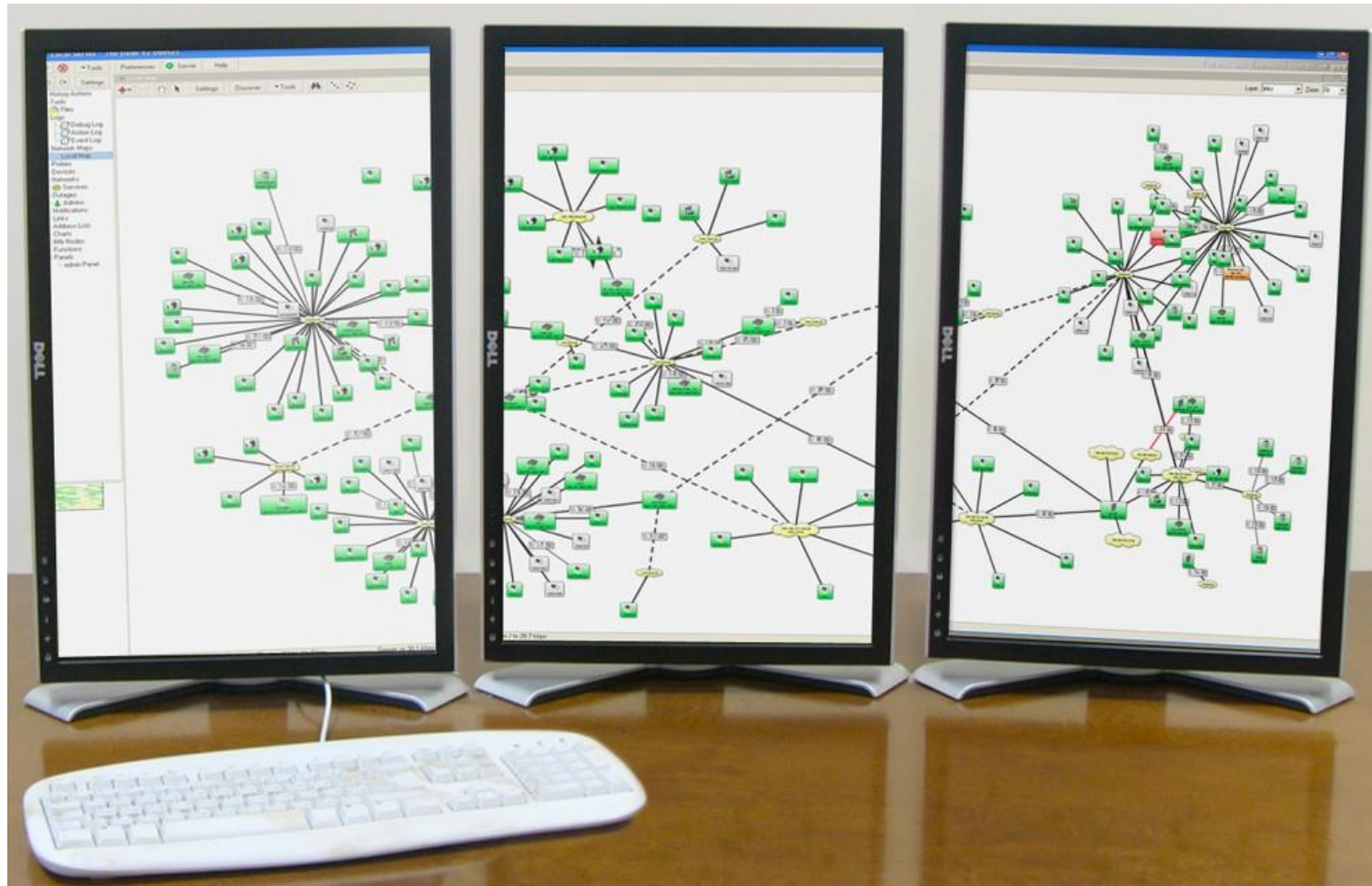
The Dude

- Aplikasi yang disediakan oleh MikroTik untuk memberikan kemudahan monitoring bagi networks admin
- Otomatis discovery dan layout map
- Monitoring service dan alarm
- Gratis

The Dude

- Support SNMP, ICMP, DNS, dan TCP monitoring
- Server running pada RouterOS (CCR, CHR or X86)
- Client pada Windows (Linux dan OS X menggunakan wine emulator)
- For more info see [The Dude wiki page](#)

The Dude



The Dude

- Download the Dude client
- Install dan hubungkan ke MikroTik Dude demo server : **dude.mt.lv**
- Lakukan observasi tentang The Dude

The Dude

