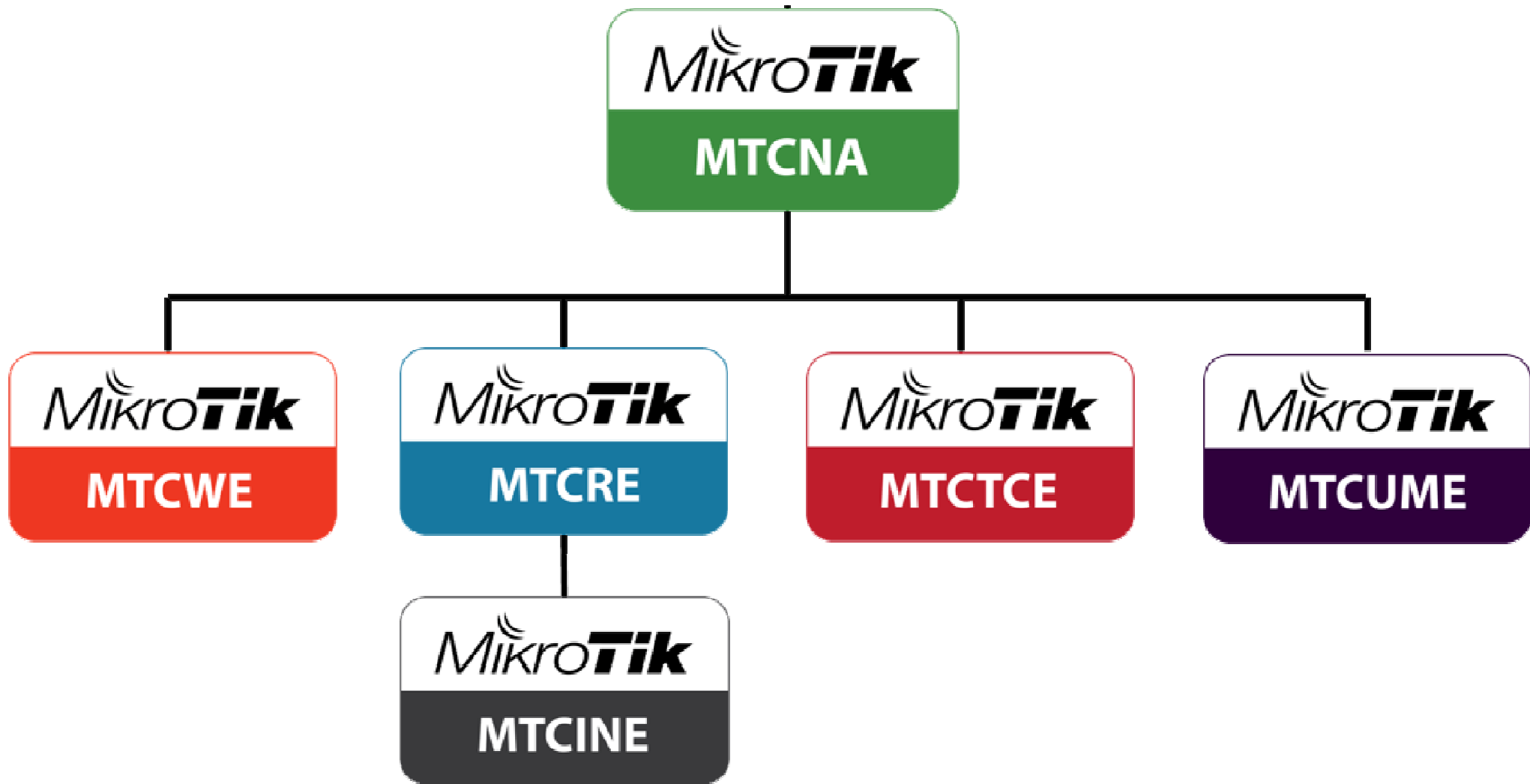


Academy Preparation

MTCNA

MikroTik Training



RouterOS ?

- RouterOS adalah sebuah sistem operasi yang dapat diinstall di PC Atau juga di routerboard berfungsi sebagai:
 - Router
 - Bandwidth Manager
 - Packet Filter
 - Wireless (AP/Station)
 - Hotspot
 - VPN dll

ROUTERBOARD

- Router hardware yang dibuat oleh MikroTik untuk digunakan dengan RouterOS sebagai sistem operasinya.

RB:Routerboard

H:High Powered

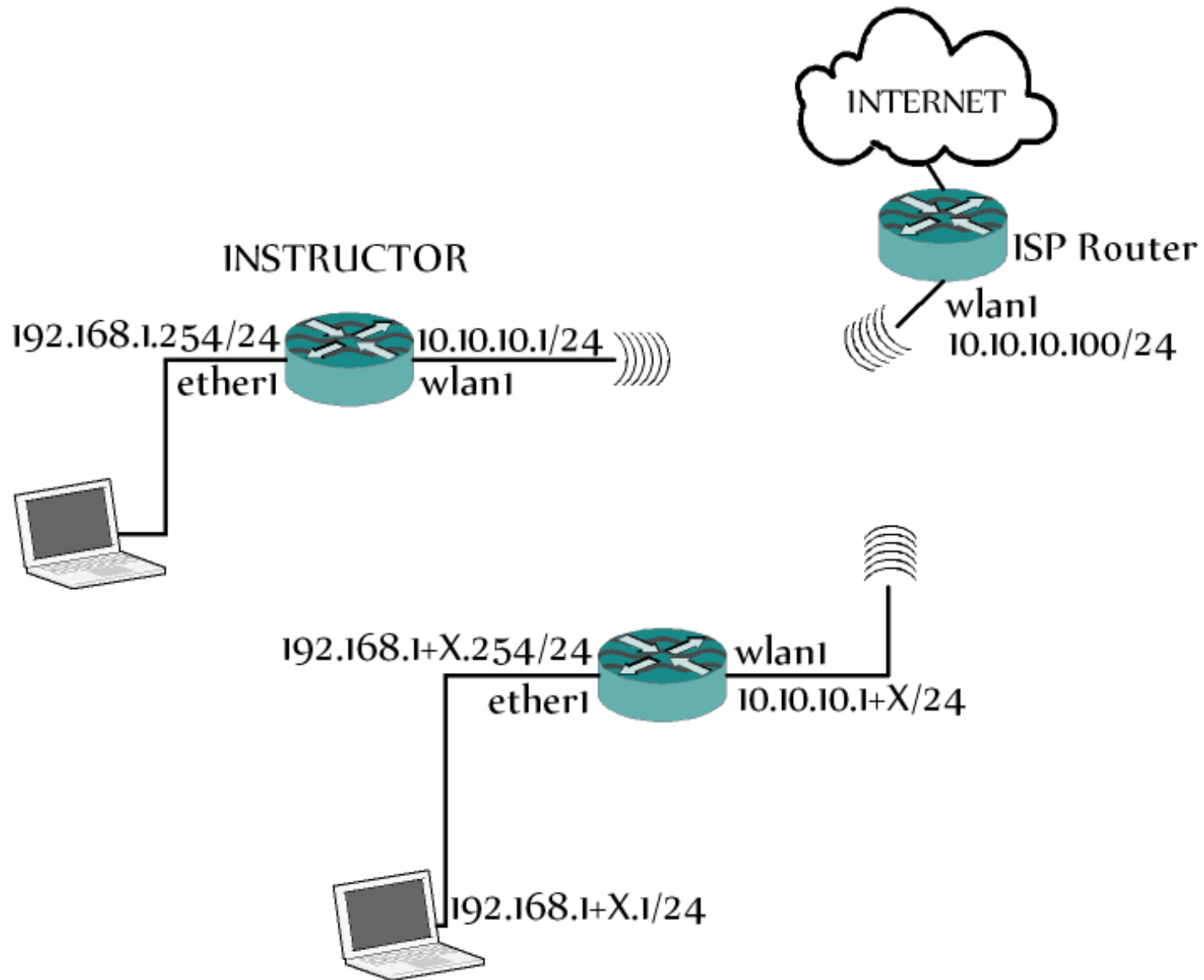
S:SFP

U:USB

G:Gigabit

i:Injector

LAB TOPOLOGI



Koneksi ke Router

Serial RS-232,
default rate **115200**
bps, 8 data bits,
no parity

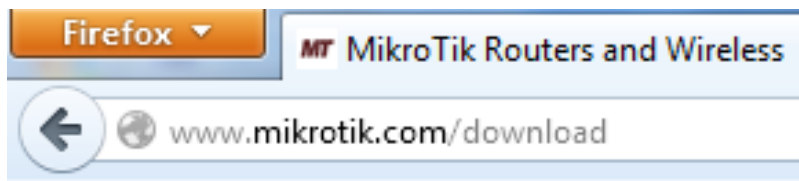


Ethernet Cable/
MAC Winbox



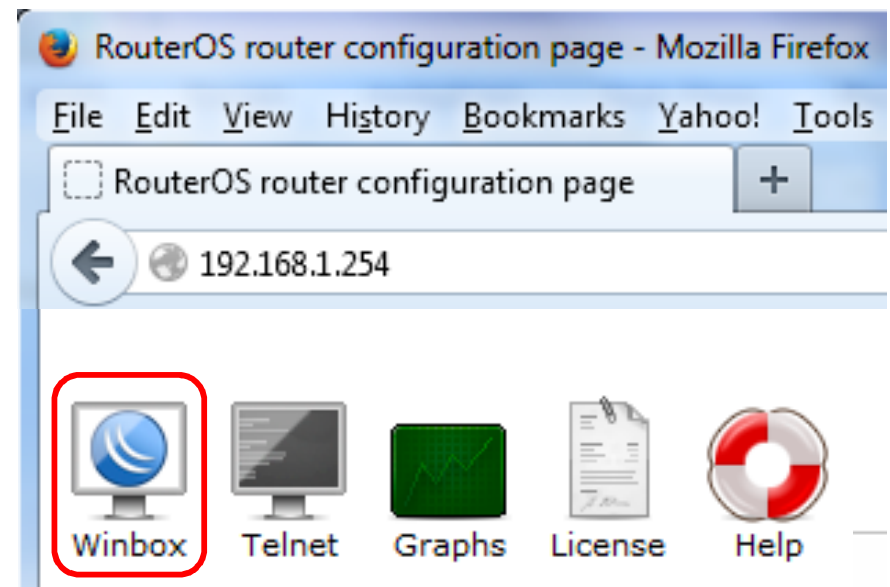
Winbox

- Aplikasi untuk konfigurasi RouterOS, dapat menggunakan IP (layer 3) atau MAC (layer 2)
- Download di mikrotik.com atau di web router



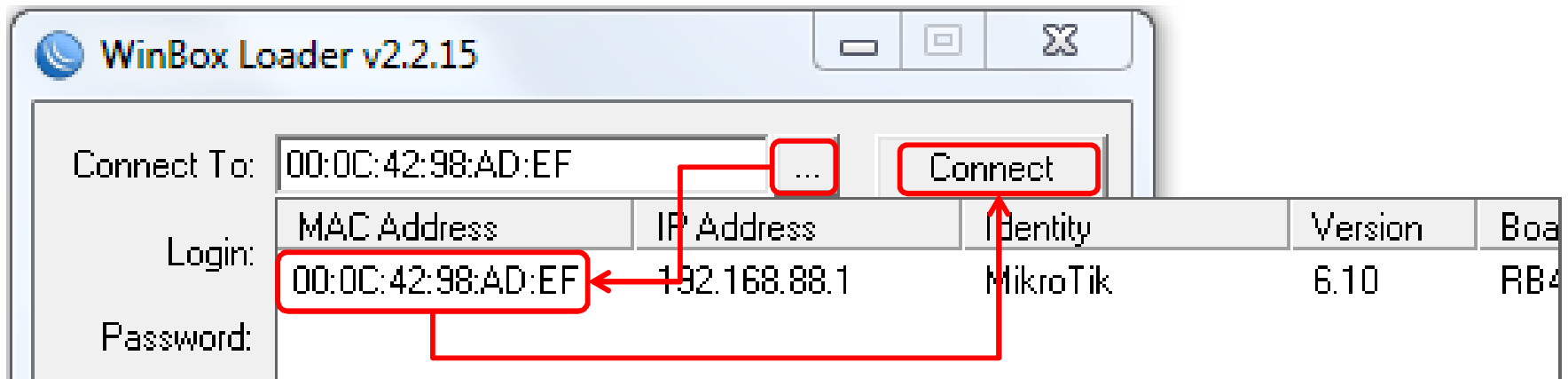
Useful tools and utilities

Winbox	Configuration
Netinstall	RouterOS Inst
The Dude	Network monit



Winbox

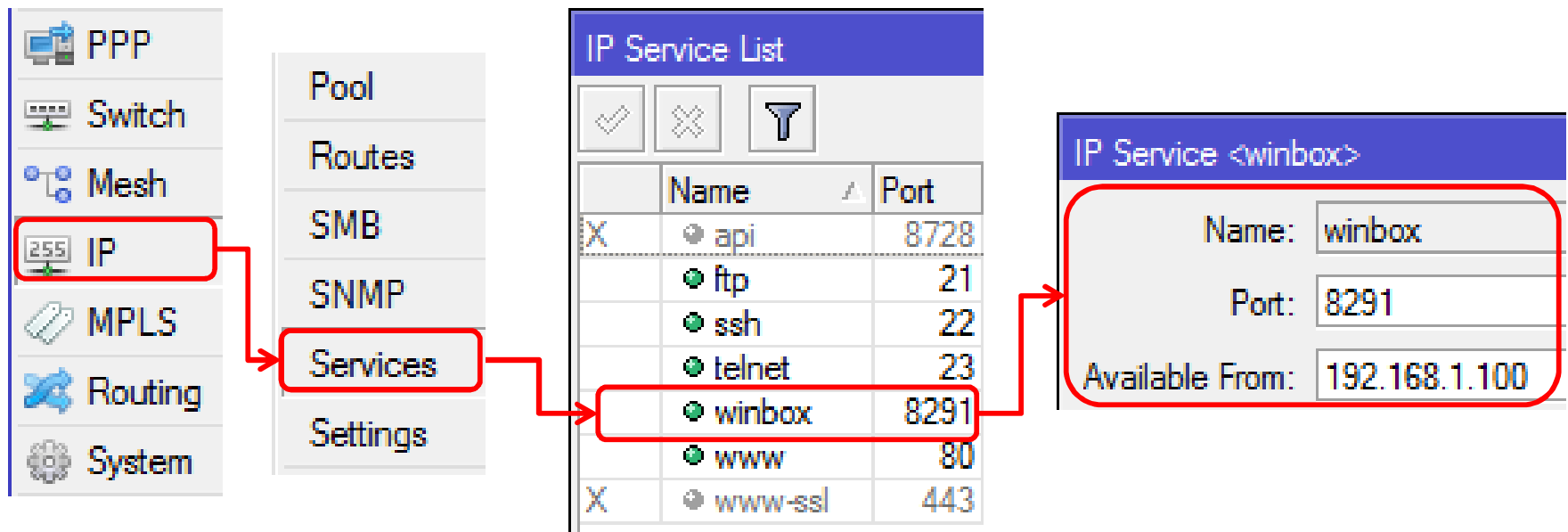
- Login: **admin**, passw:, klik tombol [...], MikroTik Neighbor Discovery Protocol MNDP akan mencari informasi router, klik **Connect**



- MNDP menggunakan UDP port 5678

Winbox

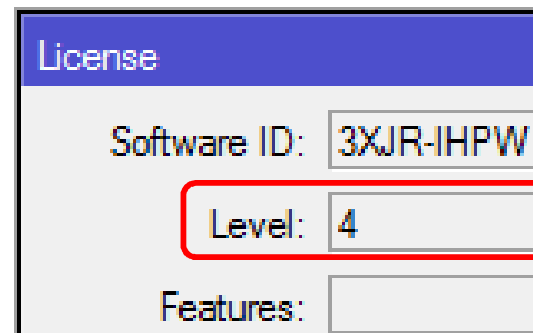
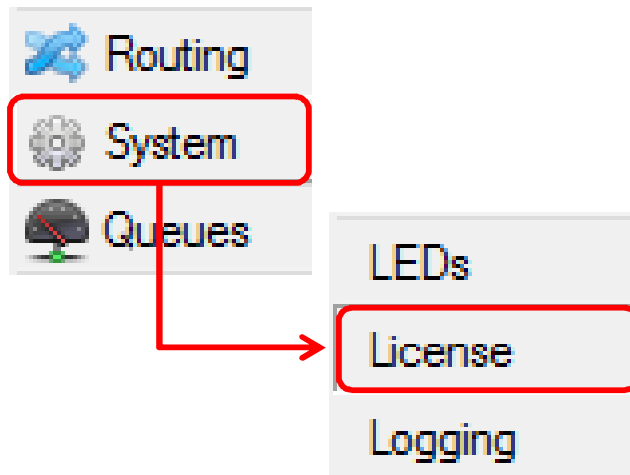
- Winbox menggunakan port 8291/TCP (default) untuk login ke router



- IP Service digunakan untuk mengatur akses menuju router

LISENSI ROUTEROS

- Lisensi RouterOS dapat diupgrade sampai dua versi mayor berikutnya, dengan level:
 - Level 0 (demo), fitur lengkap, berlaku 24 jam,
 - Level 1 (free) s.d 5, fitur terbatas dan bertingkat sesuai levelnya, masa berlaku tak terbatas
 - Level 6, fitur lengkap masa berlaku tak terbatas



LISENSI ROUTEROS

License	0 (FREE)	1 (DEMO)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Wireless AP	24h limit	-	-	yes	yes	yes
Wireless Client and Bridge	24h limit	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h limit	-	yes(*)	yes	yes	yes
EoIP tunnels	24h limit	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h limit	1	200	200	500	unlimited
PPTP tunnels	24h limit	1	200	200	500	unlimited
L2TP tunnels	24h limit	1	200	200	500	unlimited
OVPN tunnels	24h limit	1	200	200	unlimited	unlimited
VLAN interfaces	24h limit	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h limit	1	1	200	500	unlimited
RADIUS client	24h limit	-	yes	yes	yes	yes
Queues	24h limit	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h limit	-	yes	yes	yes	yes
Synchronous interfaces	24h limit	-	-	yes	yes	yes
User manager active sessions	24h limit	1	10	20	50	Unlimited

ROUTEROS VERSION

- Tipe RouterOS dan Routernya:
 - routeros-mipsle (RB100, RB500)
 - routeros-mipsbe (RB400)
 - routeros-powerpc (RB300, RB600, RB1000)
 - routeros-x86 (Intel/AMD PC, RB230)
- File upgrade
 - NPK, paket standar ROS
 - ZIP, dapat diinstal sesuai kebutuhan

UPGRADE VERSION

- Upgrade versi RouterOS dilakukan dengan:
 - Upload file RouterOS melalui upload ke **Files**, atau dengan proses FTP root directory
 - Check for updates (System → Packages)
 - Auto Upgrade (System → Auto Upgrade)
- Selalu membaca **changelog** sebelum upgrade

Changelog

What's new in 6.24 (2014-Dec-23 13:38):

- *) ntp - fixed vulnerabilities;
- *) web proxy - fix problem when dscp was not set when ipv6 was enabled;
- *) fixed problem where some of ethernet cards do not work on x86;
- *) improved CCR ethernet driver (less dropped packets);

UPGRADE VERSION

The image shows a composite screenshot of the Mikrotik WinBox interface during a system upgrade. On the left, a 'File List' window displays a directory of files, including 'system-6.23-mipsbe.npk'. An 'Uploading Files' dialog box is overlaid on top, showing progress for 'system-6.23-mips...' (8.5 MiB of 11.2 MiB at 879.59 kb). In the center, the 'System' menu is open, with 'System' and 'Reboot' options highlighted with red boxes. A red arrow points from the 'Reboot' option to a 'Do you want to reboot the router?' dialog box on the right, which has 'Yes' and 'No' buttons. Another red arrow points from the 'Yes' button back to the 'System' menu. A third red arrow points from the 'Reboot' option to the 'File List' window.

DOWNGRADE VERSION

The screenshot illustrates the steps to downgrade a package version in Mikrotik WinBox. The left sidebar shows the 'System' menu selected, leading to the 'Packages' option. The main window displays the 'Package List' table, which contains the following data:

Name	Version	Build Time	Scheduled
advanced-tools	6.24	Dec/23/2014 13:38:45	
calea	6.24	Dec/23/2014 13:38:45	
dhcp	6.24	Dec/23/2014 13:38:45	
gps	6.24	Dec/23/2014 13:38:45	
hotspot	6.24	Dec/23/2014 13:38:45	
ipv6	6.24	Dec/23/2014 13:38:45	
lcd	6.24	Dec/23/2014 13:38:45	
mpls	6.24	Dec/23/2014 13:38:45	
multicast	6.24	Dec/23/2014 13:38:45	

The 'Downgrade' button is highlighted in the top right of the 'Package List' window. A confirmation dialog titled 'Confirm Reboot' is shown, with the text: 'To downgrade, router needs to be rebooted, reboot?'. The 'Yes' button is highlighted, indicating the user's response.

PACKAGE MANAGEMENT

- Router dapat berfungsi berdasarkan paket-paket yang diaktifkan (*lampiran*)

ppp	PPP, PPTP, L2TP, PPPoE
routerboard	RouterBOARD specific functions
routing	RIP, OSPF, BGP
security	Secure Winbox, SSH, IPSec
wireless	Wireless 802.11 a/b/g
user-manager	User-Manager management system
ipv6	IPv6

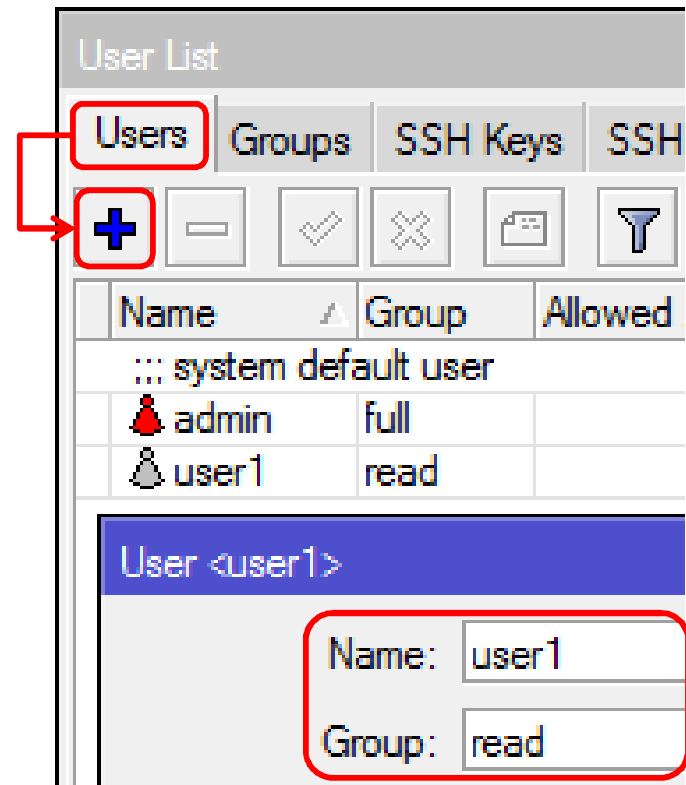
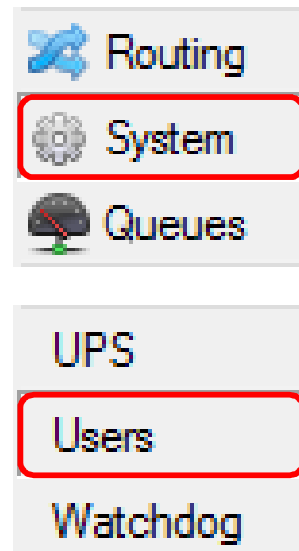
PACKAGE MANAGEMENT

The screenshot displays the Mikrotik WinBox interface. On the left, a sidebar menu includes 'IP', 'MPLS', 'Routing', 'System', and 'Queues'. The 'System' menu is expanded, showing options like 'NTP Client', 'NTP Server', 'Packages', 'Password', 'Ports', 'Reboot', 'Reset Configuration', 'Resources', and 'Routerboard'. The 'Packages' option is highlighted with a red box. A red arrow points from this box to the 'Disable' button in the 'Package List' window. Another red arrow points from the 'Reboot' option to the 'Disable' button. A third red arrow points from the 'Reboot' option to the 'wireless' package row in the table. The 'Package List' window has buttons for 'Enable', 'Disable', 'Uninstall', 'Unschedule', and 'Downgrade'. The 'Disable' button is highlighted with a red box. Below the buttons is a table with columns: Name, Ver..., Build Time, and Scheduled. The 'wireless' package is highlighted in blue and has the status 'scheduled for disable' in the Scheduled column.

Name	Ver...	Build Time	Scheduled
routeros-mipsbe	5.20	Aug/15/2012 10:06:50	
advanced-t...	5.20	Aug/15/2012 10:05:02	
dhcp	5.20	Aug/15/2012 10:05:10	
hotspot	5.20	Aug/15/2012 10:05:38	
X ipv6	5.20	Aug/15/2012 10:05:33	
mpls	5.20	Aug/15/2012 10:05:26	
ppp	5.20	Aug/15/2012 10:05:19	
routerboard	5.20	Aug/15/2012 10:05:59	
routing	5.20	Aug/15/2012 10:05:21	
security	5.20	Aug/15/2012 10:05:09	
system	5.20	Aug/15/2012 10:04:54	
wireless	5.20	Aug/15/2012 10:05:48	scheduled for disable

USER MANAJEMEN

- Koneksi ke router dapat diatur termasuk membuat tipe user yang berbeda.
- Tipe User:
 - Full
 - Read
 - Write
 - Custom



USER MANAJEMEN - Groups

User List

Users **Groups** SSH Keys SSH Private Keys

+ - [Folder Icon] [Filter Icon]

	Name	Policies
S	full	local telnet ssh ftp reboot read wr
S	read	local telnet ssh reboot read test w
S	write	local telnet ssh reboot read write t

Group <read>

Name:

- Policies -

<input checked="" type="checkbox"/> local	<input checked="" type="checkbox"/> telnet
<input checked="" type="checkbox"/> ssh	<input type="checkbox"/> ftp
<input checked="" type="checkbox"/> reboot	<input checked="" type="checkbox"/> read
<input type="checkbox"/> write	<input type="checkbox"/> policy
<input checked="" type="checkbox"/> test	<input checked="" type="checkbox"/> winbox
<input checked="" type="checkbox"/> password	<input checked="" type="checkbox"/> web
<input checked="" type="checkbox"/> sniff	<input checked="" type="checkbox"/> sensitive
<input checked="" type="checkbox"/> api	

User List

Users **Groups** SSH Keys SS

+ - [Folder Icon] [Filter Icon]

	Name	Policies
	full	local telnet ssh
	group5	read winbox
	read	local telnet ssh
	write	local telnet ssh

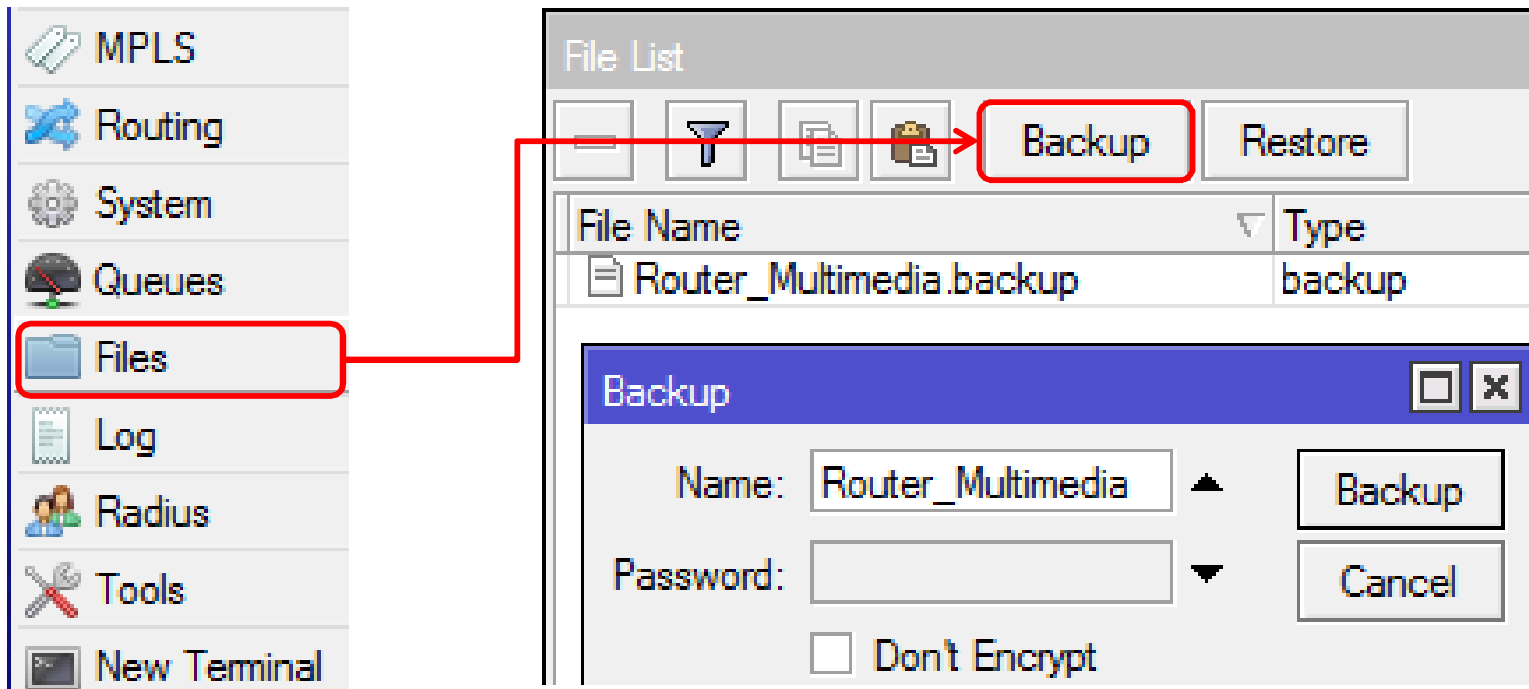
Group <group5>

Name:

- Policies -

<input type="checkbox"/> local	<input type="checkbox"/> telnet
<input type="checkbox"/> ssh	<input type="checkbox"/> ftp
<input type="checkbox"/> reboot	<input checked="" type="checkbox"/> read
<input type="checkbox"/> write	<input type="checkbox"/> policy
<input type="checkbox"/> test	<input checked="" type="checkbox"/> winbox
<input type="checkbox"/> password	<input type="checkbox"/> web

BACKUP



Hasil backup dapat di simpan di USB, Hardisk, CD. File backup ini tidak dapat diedit, berisi seluruh konfigurasi router, password dan username, tidak termasuk file yang ada di **/Files**

RESET

Reset router akan menghapus semua konfigurasi yang telah dibuat termasuk user dan password. Reset ini hanya bisa dilakukan oleh user dengan hak penuh (full)

The image shows a screenshot of the MikroTik WinBox interface. On the left, there is a 'Tools' menu with 'New Terminal' highlighted by a red box and an arrow pointing to a terminal window. The terminal window shows the following text:

```
[admin@MikroTik] > system reset  
Dangerous! Reset anyway? [y/N]:  
y  
system configuration will be reset
```

Below the terminal window, a dialog box is displayed with three buttons: 'Remove Configuration' (highlighted with a red box), 'Show Script...', and 'OK' (dashed border).

RESTORE

Merestore hasil backup sebelumnya

The screenshot shows the Mikrotik WinBox interface. On the left, a sidebar menu has the 'Files' option highlighted with a red box. A red arrow points from this menu to the 'Restore' button in the 'File List' toolbar, which is also highlighted with a red box. Below the toolbar, a table lists files for backup. The 'Restore' dialog box is open, showing the selected backup file and a password field.

File Name	Type	Size
Router_Multimedia.backup	backup	

Restore dialog box fields:

- Backup File: Router_Multimedia.backup
- Password: [Empty field]
- Buttons: Restore, Cancel

A confirmation dialog box titled 'Restore' with the text 'Do you want to restore configuration and reboot?'. The 'Yes' button is highlighted with a red box.

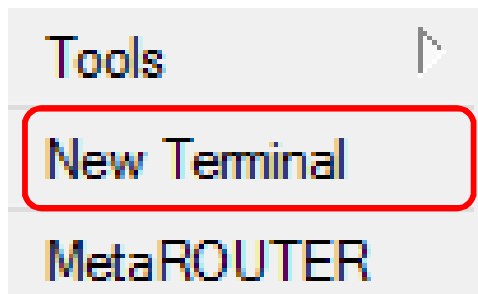
Restore

Do you want to restore configuration and reboot?

Yes No

COMMAND LINE INTERFACE

- CLI merupakan proses konfigurasi berbasis text yang memiliki hirarkinya yang sama pada menu di sistem winbox.



```
[admin@MikroTik] > ip address add  
address=172.16.1.1/24  
interface=ether3
```

EXPORT

- Konfigurasi router juga dapat dibackup dengan export, file export berupa text sehingga mudah diedit dan tersimpan di menu Files.
- Backup konfigurasi IP Address saja,

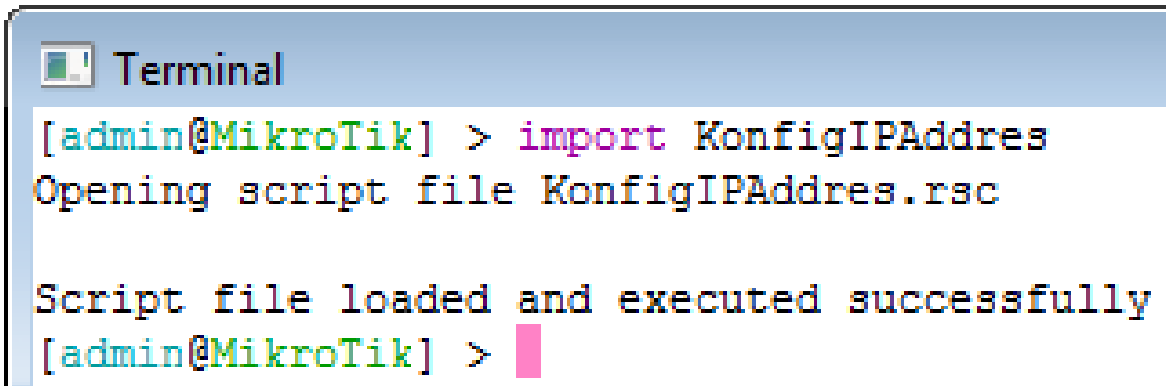
```
[admin@MikroTik] > ip address  
[admin@MikroTik] /ip address> export file=KonfigIPAdres  
[admin@MikroTik] /ip address> █
```

- Backup keseluruhan (kecuali router password), harus dilakukan dari hirarki menu paling atas

```
[admin@MikroTik] >  
[admin@MikroTik] > export file=Konfigurasi_Router_A  
[admin@MikroTik] >
```

IMPORT

- Import dilakukan dari hirarki menu teratas



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

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

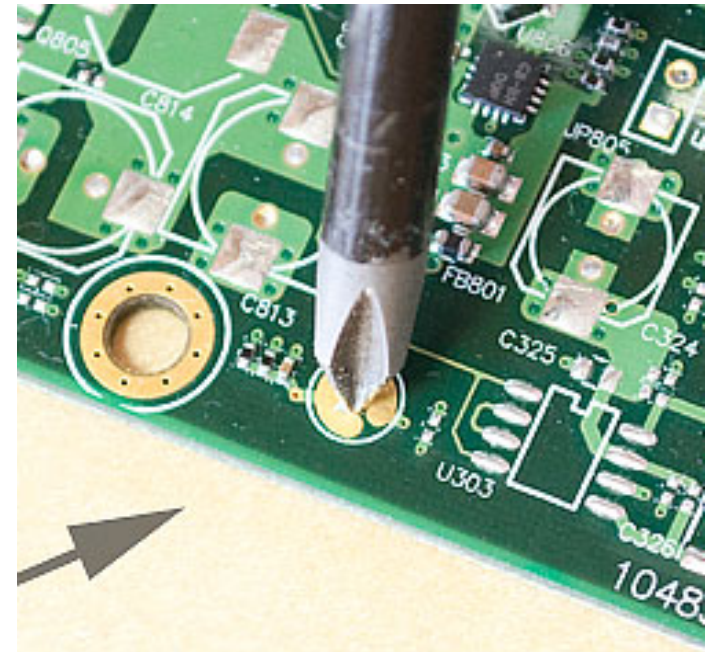
- Setelah proses import file **rsc**, konfigurasi akan langsung aktif dan tidak perlu proses reboot

RESET PASSWORD

Reset password dapat dilakukan melalui:

- Reset Jumper,
Menghapus konfigurasi termasuk password,
file backup tidak terhapus

- Netinstall



NETINSTALL ROUTERBOARD

- Netinstall digunakan untuk melakukan instalasi baru/reinstall apabila terjadi kerusakan software, tidak menghilangkan lisensi namun akan menghapus password, file backup dan konfigurasi (jika option *keep old configuration disable*).
- Netinstall dapat dilakukan baik di routerboard /PC melalui ethernet atau kabel serial

IP ADDRESSING

- Sebelum router digunakan sebagai peralatan jaringan, interface harus diberi IP Address.

The screenshot illustrates the configuration process in Mikrotik WinBox. On the left, the 'IP' menu item is highlighted with a red box. An arrow points from this menu to the 'Addresses' option in the central sidebar, which is also highlighted with a red box. Another arrow points from 'Addresses' to the 'Address List' window. In this window, the '+' icon is highlighted with a red box. Below the window, a smaller dialog box titled 'Address <192.168.1.254/24>' is shown, with its input fields highlighted by a red box. The fields contain: Address: 192.168.1.254/24, Network: 192.168.1.0, and Interface: ether1. The 'Address List' window contains a table with the following data:

Address	Network	Interface
192.168.1.254/24	192.168.1.0	ether1

IP ADDRESSING

- Setiap IP Address yang terpasang di interface router, secara otomatis akan menambahkan DAC routing di route list

The screenshot illustrates the navigation path in Mikrotik WinBox. On the left, the 'IP' menu item is highlighted with a red box. A red arrow points from 'IP' to the 'Routes' menu item in the central sidebar, which is also highlighted with a red box. A second red arrow points from 'Routes' to the 'Route List' window on the right. The 'Route List' window has the 'Routes' tab selected and highlighted with a red box. Below the tab, there are several icons: a red plus sign, a minus sign, a checkmark, a cross, a document, and a funnel. A table displays the route list with the following data:

	Dst. Address	Gateway	Distance
DAC	▶ 192.168.1.0/24	ether1 reachable	0

Below the table, a legend box contains the text: "D - dynamic, A - active, C - connected".

TELNET/SSH

Akses dan konfigurasi router juga dapat dilakukan melalui **Telnet** (tidak secure)/ atau **SSH** (secure), konfigurasi dilakukan dengan CLI

Akses Telnet/SSH dapat ditutup dengan mendisable port 23 di **IP Service**

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address)	Port
192.168.1.254	23

Connection type:

Raw Telnet Rlogin SSH Serial

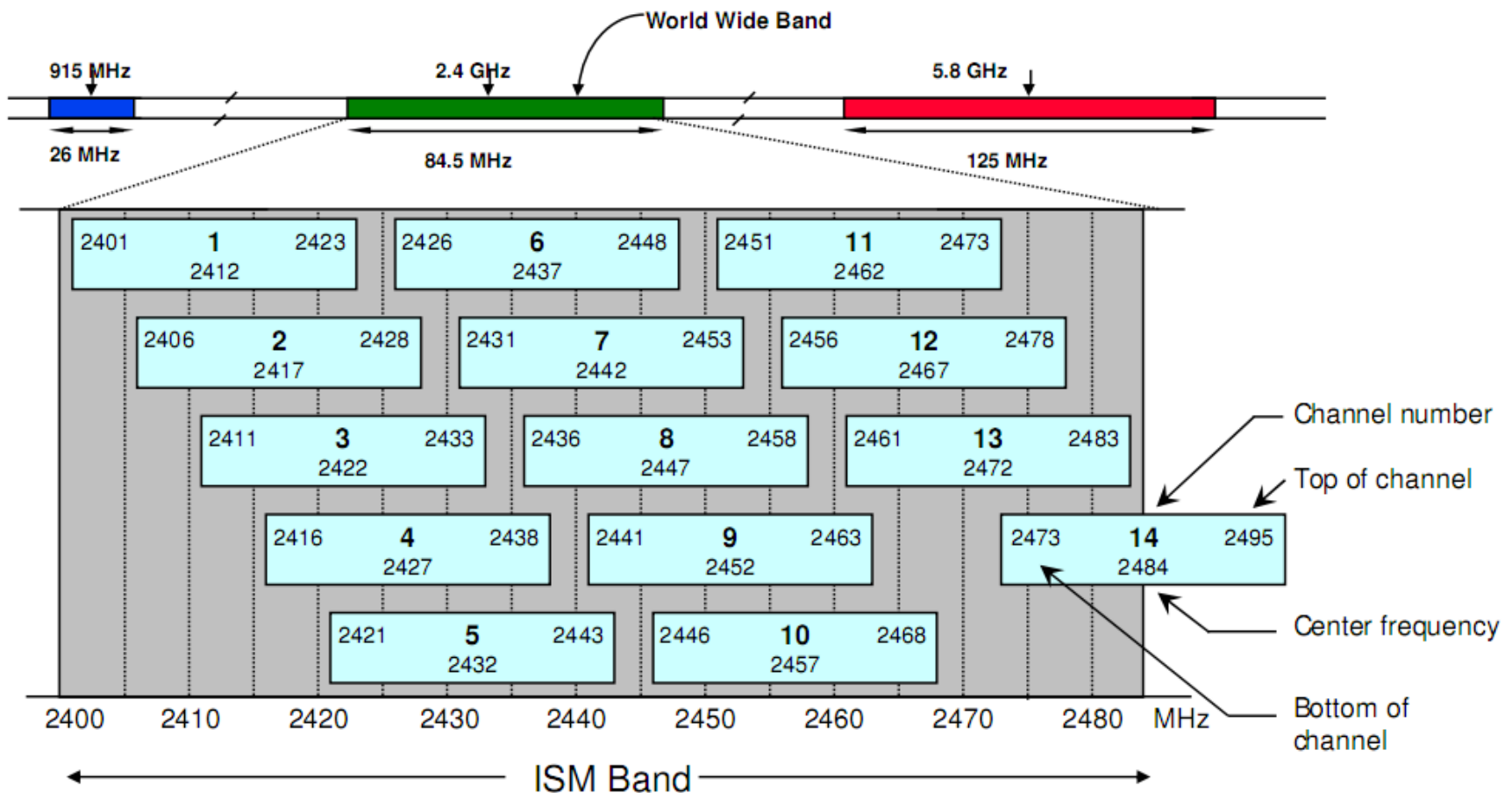
Load, save or delete a stored session

IP Service List		
	Name	Port
X	api	8728
	api-ssl	8729
	ftp	21
X	ssh	22
X	telnet	23
	winbox	8291
	www	80
X	www-ssl	443

WIRELESS

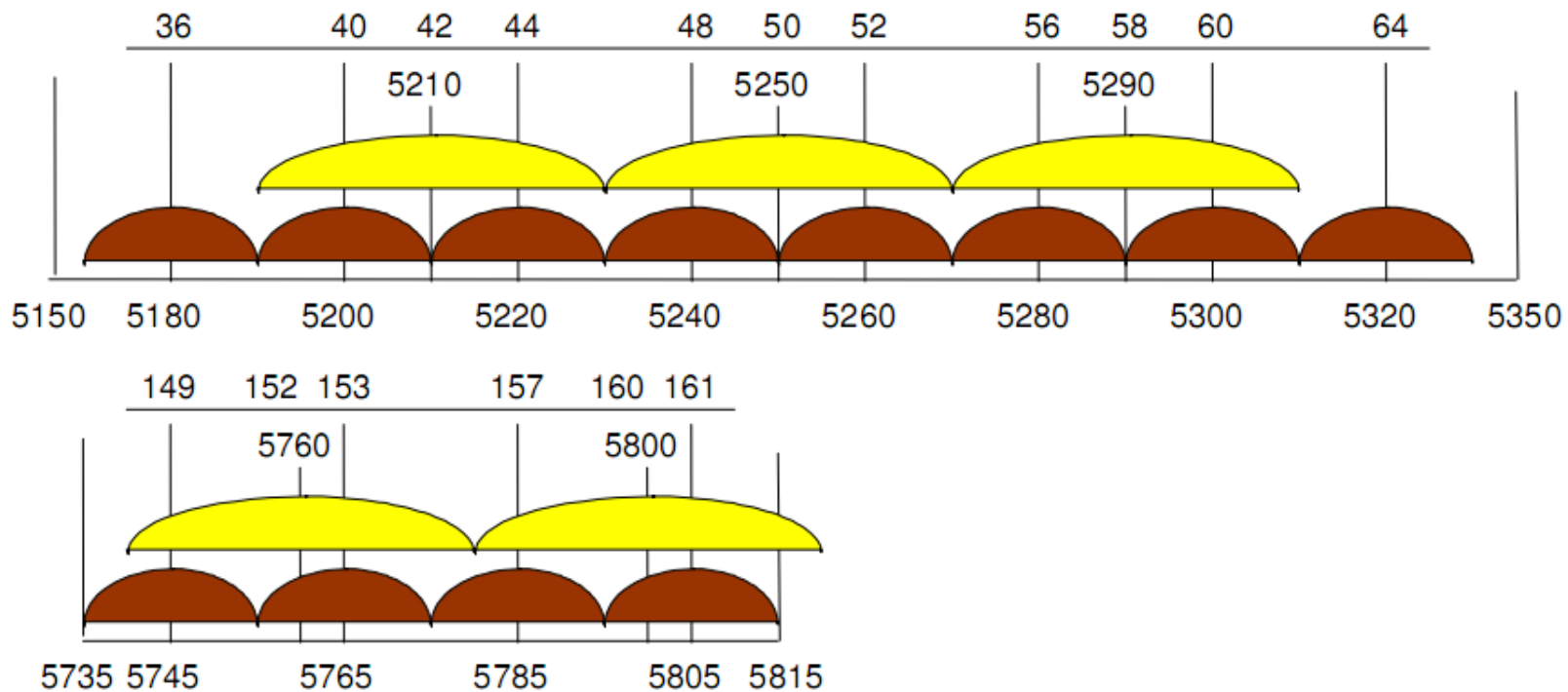
WIRELESS STANDAR

- IEEE 802.11b - 2.4GHz frequencies, 11Mbps
- IEEE 802.11g - 2.4GHz frequencies, 54Mbps



WIRELESS STANDAR

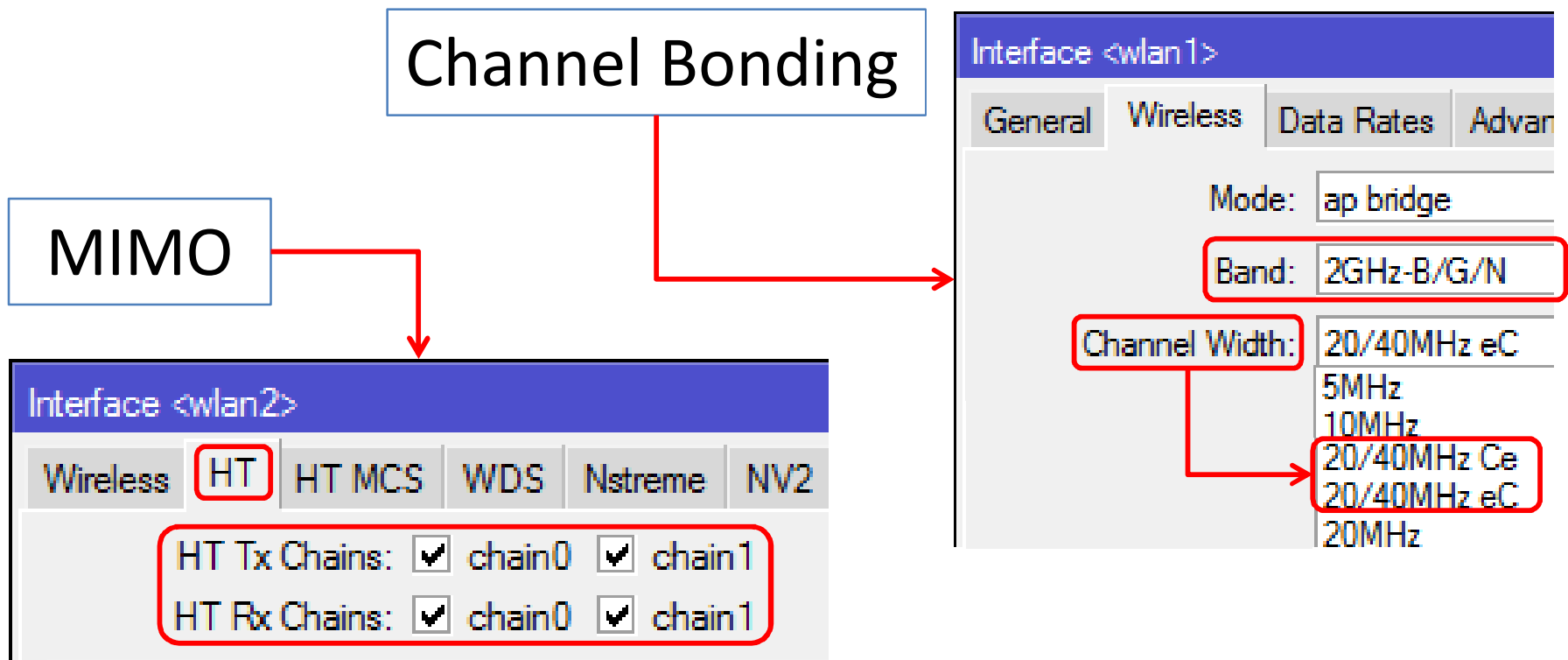
- IEEE 802.11a - 5GHz frequencies, 54Mbps



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

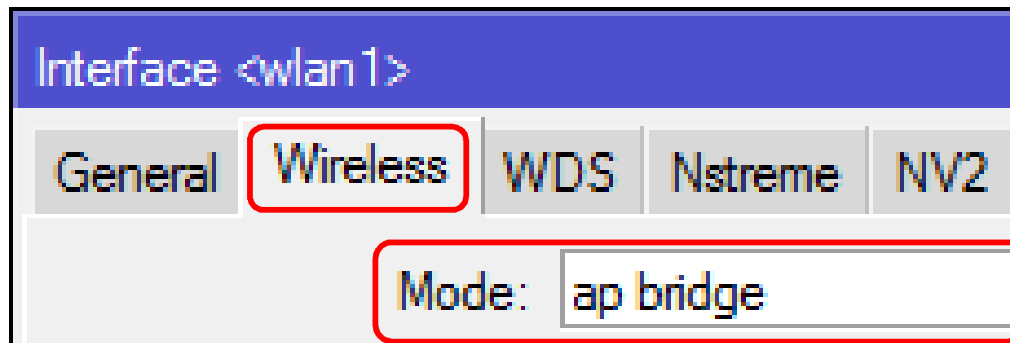
WIRELESS STANDAR

- IEEE 802.11n - 300Mbps serta dapat bekerja pada frekuensi 2,4GHz dan 5GHz.



MODE

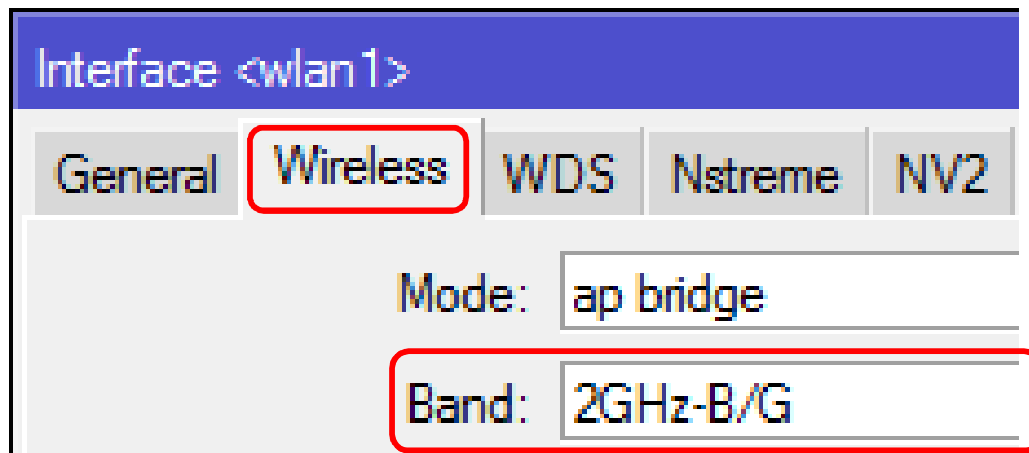
- **ap bridge**, sebagai akses poin multi klien
- **bridge**, sebagai akses poin dengan satu klien
- **station**, digunakan untuk melakukan koneksi ke ap bridge/bridge
- **station-bridge**, proprietary digunakan untuk membuat koneksi bridge jika AP MikroTik



BAND

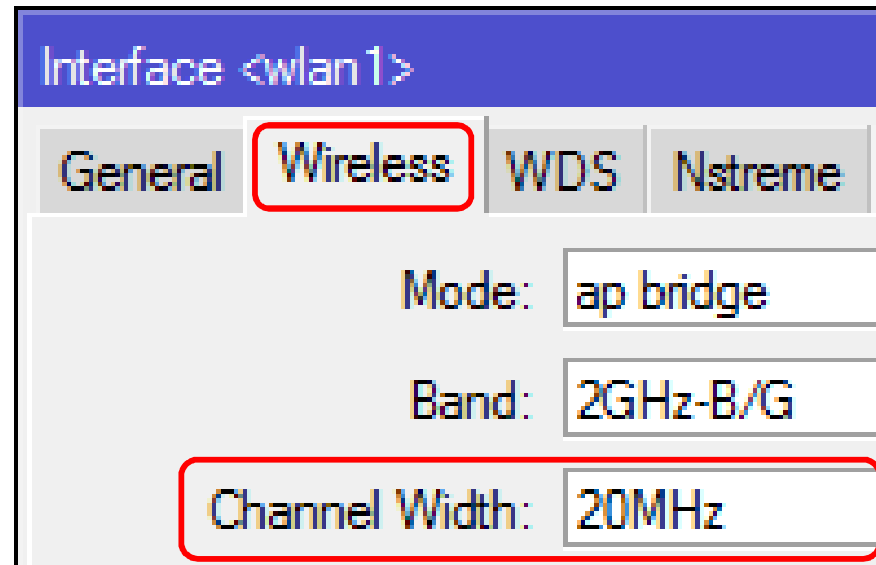
Standar band yang digunakan,

- 2,4 Ghz, standard IEEE 802.11b/g/n
- 5 GHz, standard 802.11a/n



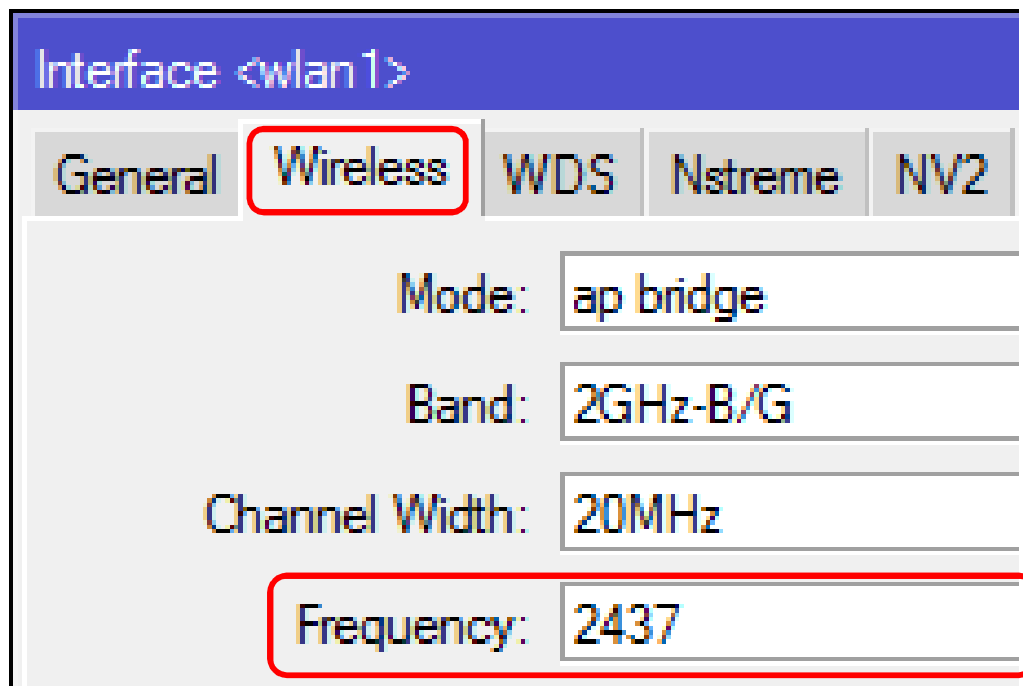
CHANNEL WIDTH

- Lebar pita channel, semakin lebar channel semakin rentan terhadap interferensi tapi semakin tinggi throughputnya.
- MikroTik mendukung channel width:
 - 5MHz, throughput $\frac{1}{4}$
 - 10MHz, throughput $\frac{1}{2}$
 - 20MHz, standard
 - 40MHz, throughput 2x



FREQUENCY

- Nilai frekuensi yang ditentukan tergantung pada band, konfigurasi country serta fitur wireless cardnya, penentuan tidak berfungsi di mode station.



Interface <wlan1>

General **Wireless** WDS Nstreme NV2

Mode: ap bridge

Band: 2GHz-B/G

Channel Width: 20MHz

Frequency: 2437

RADIO NAME

- Identitas wireless interface yang sudah terkoneksi untuk memudahkan mengenal perangkat pasangan

The image shows two screenshots from Mikrotik WinBox. The top screenshot shows the configuration for the wireless interface 'wlan1'. The SSID is 'MikroLine' and the Radio Name is 'radio 1-isp'. A red box highlights the Radio Name field, and a blue box labeled 'ISP Router' has an arrow pointing to it. The bottom screenshot shows the 'Wireless Tables' section with the 'Registration' tab selected. A table lists the registered wireless interfaces. The first entry is 'radio 1-isp' with MAC address '00:0C:42:89:49:D5' and interface 'wlan1'. A red box highlights the 'radio 1-isp' entry, and a blue box labeled 'Klien Router' has an arrow pointing to it.

ISP Router

SSID: MikroLine

Radio Name: radio 1-isp

Wireless Tables

Interfaces Nstreme Dual Access List Registration

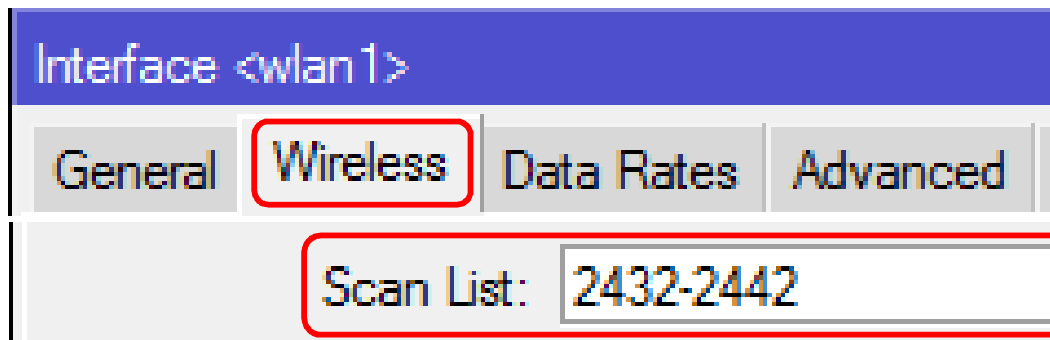
Reset

Radio Name	MAC Address	Interface	Uptime
radio 1-isp	00:0C:42:89:49:D5	wlan1	

Klien Router

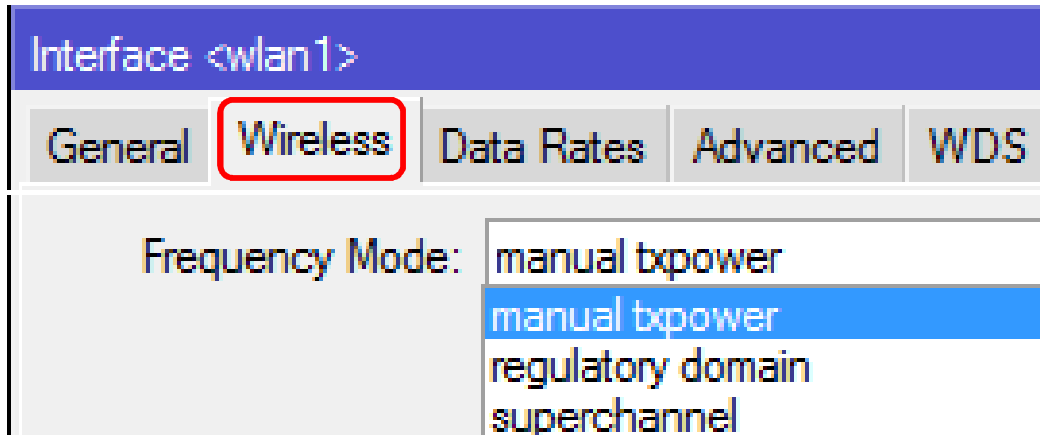
SCAN LIST

- Digunakan oleh station untuk menentukan batas frekuensi yang akan di scan dalam proses pencarian AP. Format scan-list selain default, bisa dibuat secara manual yaitu:
 - Rentang frekuensi, 2432-2442
 - Frekuensi statis: 2437



FREQUENCY MODE

- **manual tx power**, pengaturan tx power manual



- **regulatory domain**, disesuaikan dengan frekuensi yang diijinkan di suatu negara.
- **superchannel**, membuka semua frekuensi yang bisa didukung oleh wireless card.

COUNTRY

- Pilihan negara yang akan diaplikasikan regulasi pembatasan channel dan TX Power

Frequency Mode:

Country:

Frequency:

Current Tx Powers

Rate	Δ	Tx Power
1Mbps		14dBm
2Mbps		14dBm

2412
2417
2422
2427
2432
2437
2442
2447
2452
2457
2462
2467
2472

Frequency Mode:

Country:

Frequency:

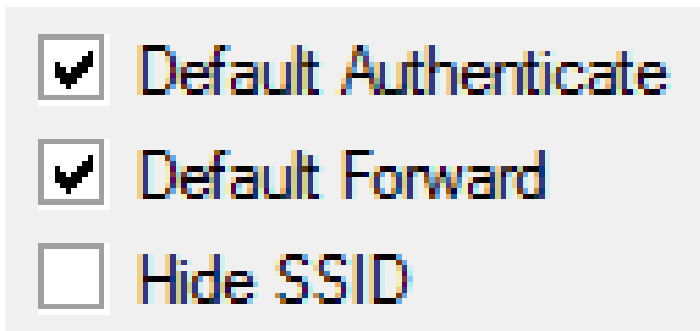
Current Tx Powers

Rate	Δ	Tx Power
1Mbps		15dBm
2Mbps		15dBm

2412
2417
2422
2427
2432
2437
2442
2447
2452
2457
2462
2467
2472
2484

DEFAULT AUTHENTICATE/FORWARD

- **Default Authenticate**, jika enable, interface akan menggunakan aturan di security profile, jika disable interface akan menggunakan aturan di acces-list/connect-list



- **Default Forward**, parameter yang digunakan untuk mencegah koneksi antar klien.
- **Hide SSID**, untuk menyembunyikan SSID

DEFAULT AP Tx RATE

Default AP Tx Rate:

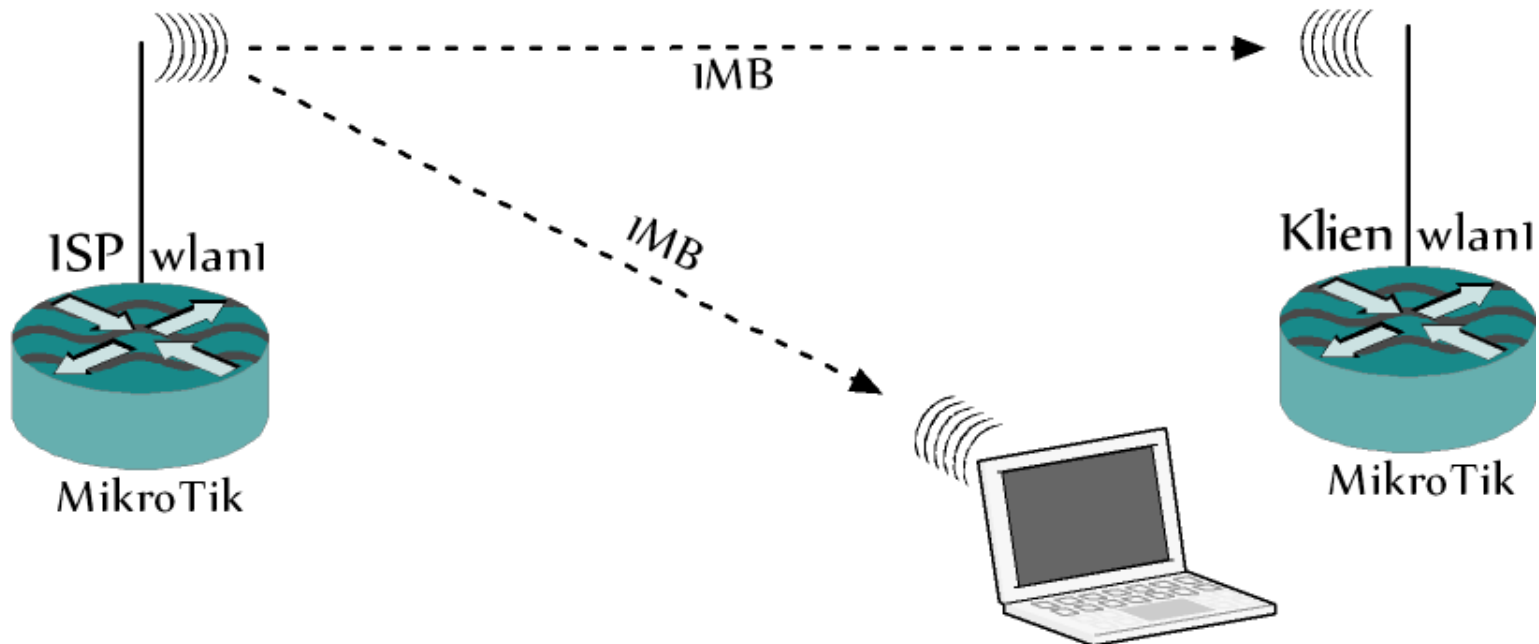
Default Client Tx Rate:

Default Authenticate

Default Forward

Hide SSID

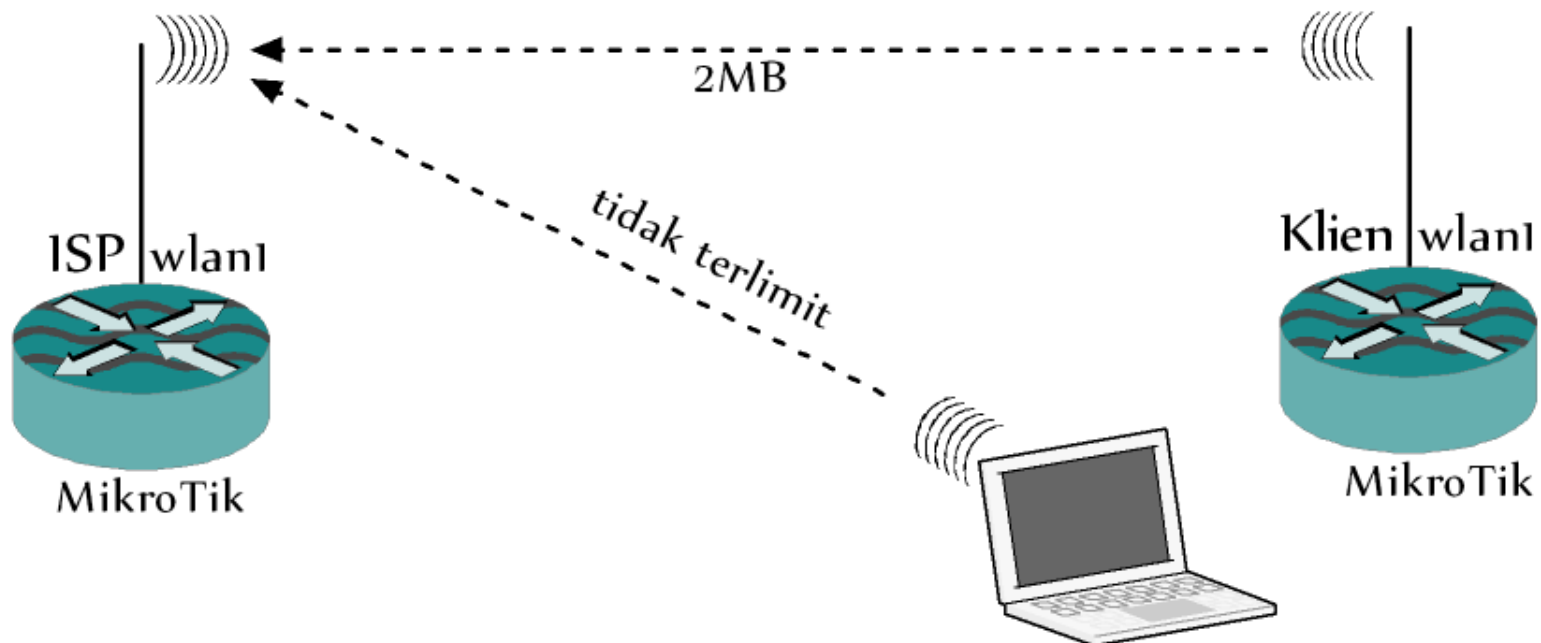
Limitasi trafik dari AP ke klien (MikroTik maupun non MikroTik).



DEFAULT CLIENT Tx RATE

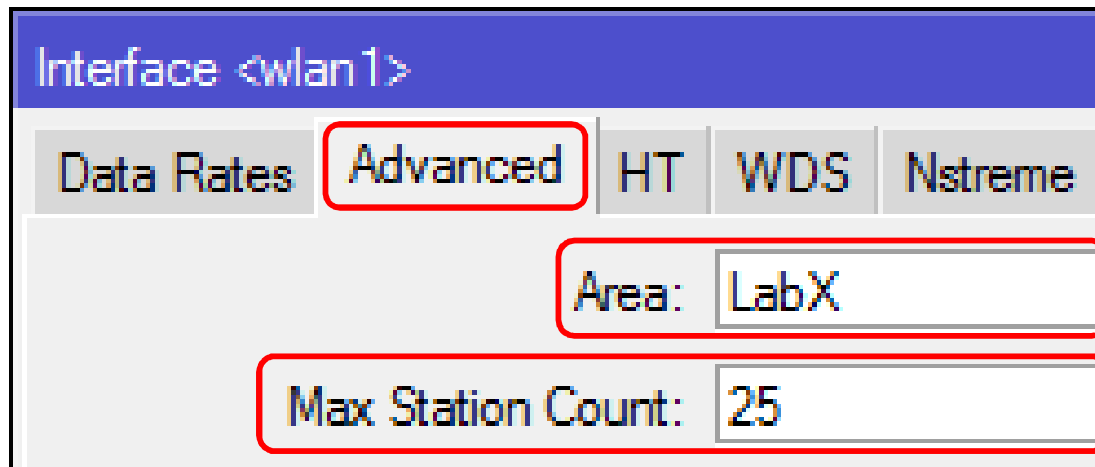
Default AP Tx Rate:	1M
Default Client Tx Rate:	2M
<input checked="" type="checkbox"/> Default Authenticate	
<input checked="" type="checkbox"/> Default Forward	
<input type="checkbox"/> Hide SSID	

Limitasi trafik dari klien MikroTik ke AP MikroTik.



AREA & MAX STATION COUNT

- **Area**, digunakan di AP, sebagai penanda/pembeda dengan AP lain, klien memasukkan area prefix pada konfigurasi connect list



Interface <wlan1>

Data Rates **Advanced** HT WDS Nstreme

Area: LabX

Max Station Count: 25

- **Max Station Count**, membatasi jumlah klien

SCAN

A vertical menu of network management options. The 'Scan...' option is highlighted with a red box. A red line connects this box to the 'Scanner (Running)' window.

- OK
- Cancel
- Apply
- Disable
- Comment
- Torch
- Scan...**
- Freq. Usage...
- Align...
- Sniff...
- Snooper...

The 'Scanner (Running)' window shows the interface 'wlan1' selected. It has buttons for Start, Stop, Close, New Window, and Connect. A table below displays scan results for the selected interface. Red boxes highlight the 'Start' button, the 'Connect' button, and the scan results table. Red arrows point from the 'Start' button to the table and from the 'Connect' button to the table.

	Address	SSID	Band	Chan...	Frequ...	Signa...	Noise...	Signa...	Radio Name	Rout
ARB	00:0C:42:63:E8:8C	MikroTik ISP	2GHz-B/G	20MHz	2412	-16	-101	85	000C4263E88C	5.18

The 'Wireless Tables' window shows the status of wireless interfaces. The 'Scanner' tab is selected. A table below shows the status of 'wlan1' and 'wlan2'. A tooltip 'R - running' is shown over the 'wlan1' entry.

	Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...
R	wlan1	Wireless (Atheros AR5413)	2290	0 bps	0 bps	0	0
X	wlan2	Wireless (Atheros 11N)		0 bps	0 bps	0	0

REGISTRATION TABLE

- Informasi interface wireless yang sudah terkoneksi bisa dilihat di registration table.

Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Pr

[-] [Filter] [Reset]

Radio Name	MAC Address	Interface	Uptime	AP
🔗 Klien_Mikrotik	00:0C:42:65:81:9E	wlan1	00:02:48	no

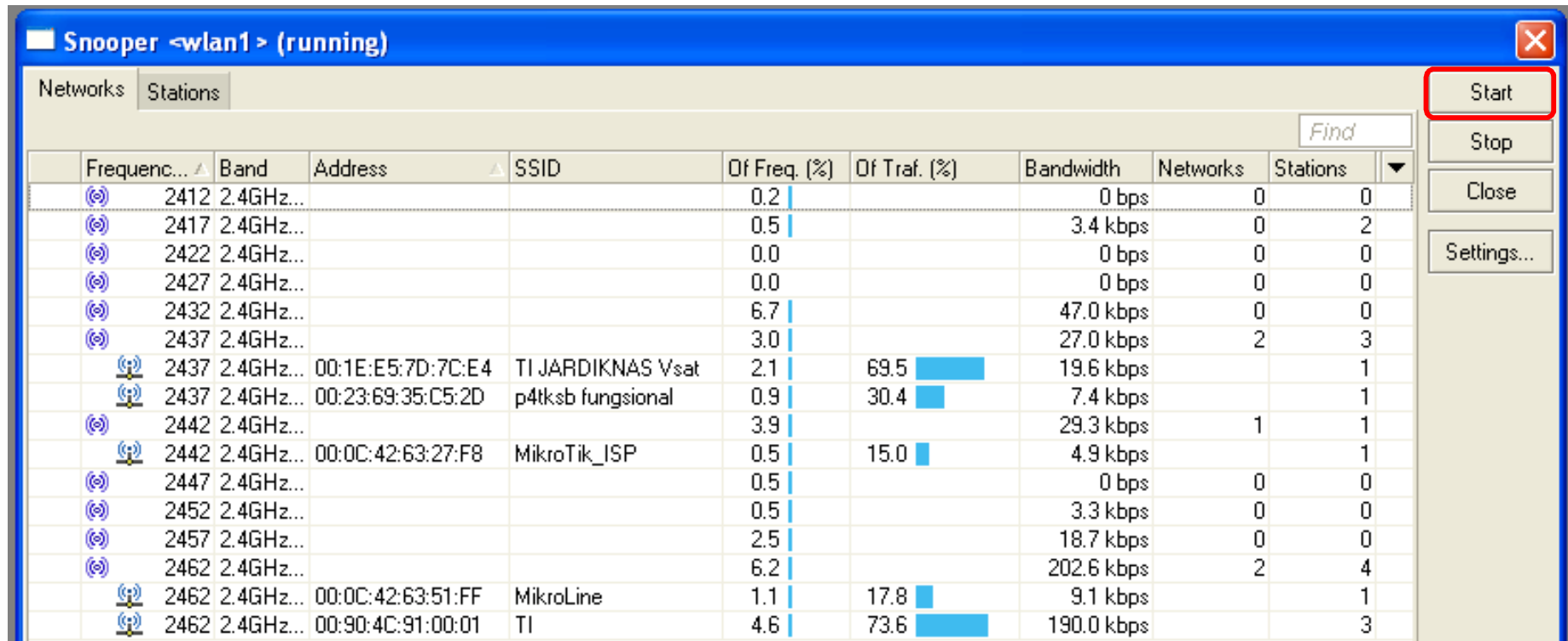
Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Pr

[-] [Filter] [Reset]

Radio Name	MAC Address	Interface	Uptime	AP
🔗 AP_Mikrotik	00:0C:42:65:81:6C	wlan1	00:00:29	yes

SNOOPER

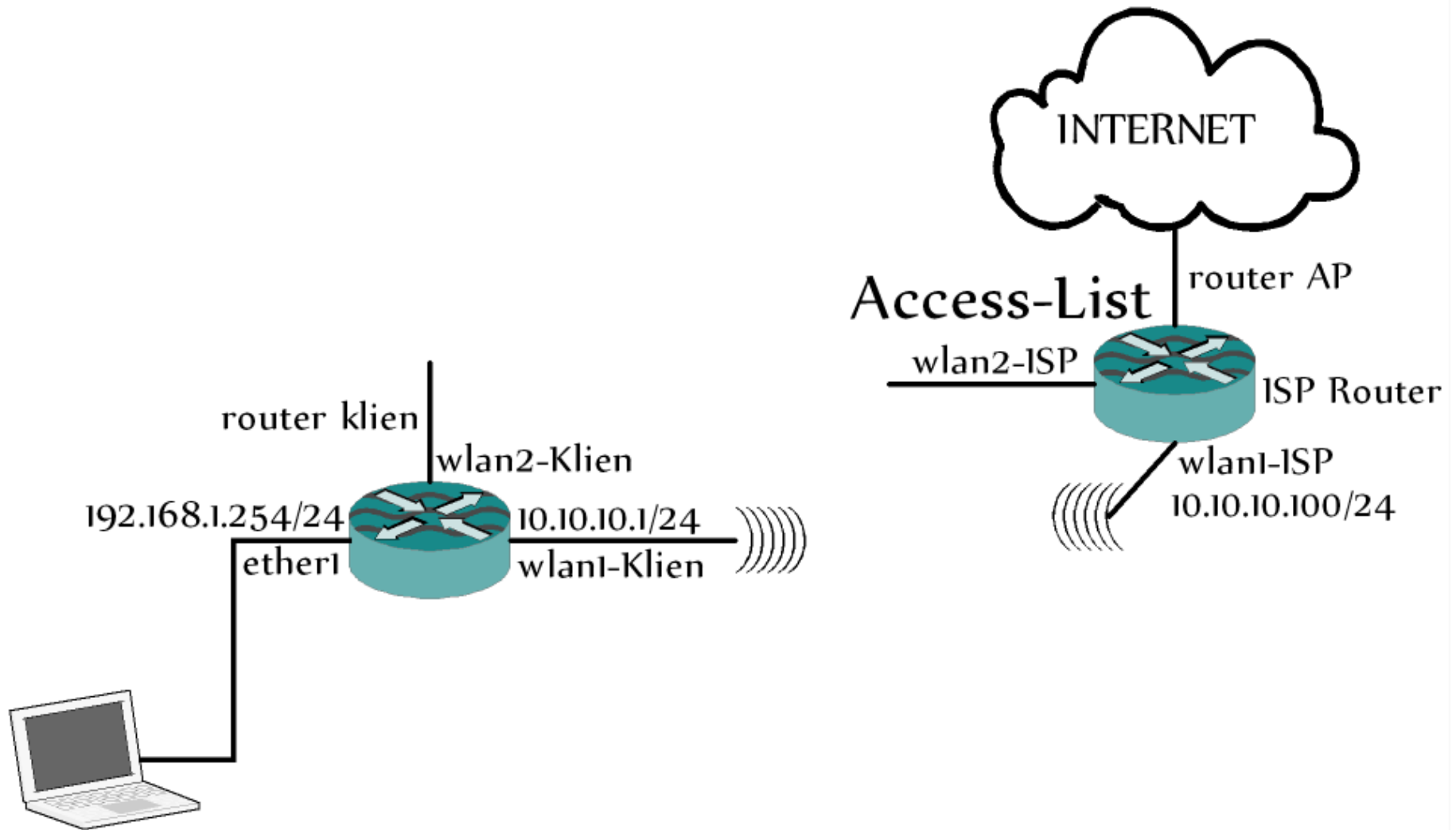


The screenshot shows the Mikrotik Snooper interface for interface wlan1, which is running. The interface has tabs for 'Networks' and 'Stations'. A 'Find' search box is located at the top right. On the right side, there are buttons for 'Start', 'Stop', 'Close', and 'Settings...'. The 'Start' button is highlighted with a red box. The main table displays the following data:

	Frequenc...	Band	Address	SSID	Of Freq. (%)	Of Traf. (%)	Bandwidth	Networks	Stations
	2412	2.4GHz...			0.2		0 bps	0	0
	2417	2.4GHz...			0.5		3.4 kbps	0	2
	2422	2.4GHz...			0.0		0 bps	0	0
	2427	2.4GHz...			0.0		0 bps	0	0
	2432	2.4GHz...			6.7		47.0 kbps	0	0
	2437	2.4GHz...			3.0		27.0 kbps	2	3
	2437	2.4GHz...	00:1E:E5:7D:7C:E4	TI JARDIKNAS Vsat	2.1	69.5	19.6 kbps		1
	2437	2.4GHz...	00:23:69:35:C5:2D	p4tksb fungsional	0.9	30.4	7.4 kbps		1
	2442	2.4GHz...			3.9		29.3 kbps	1	1
	2442	2.4GHz...	00:0C:42:63:27:F8	MikroTik_ISP	0.5	15.0	4.9 kbps		1
	2447	2.4GHz...			0.5		0 bps	0	0
	2452	2.4GHz...			0.5		3.3 kbps	0	0
	2457	2.4GHz...			2.5		18.7 kbps	0	0
	2462	2.4GHz...			6.2		202.6 kbps	2	4
	2462	2.4GHz...	00:0C:42:63:51:FF	MikroLine	1.1	17.8	9.1 kbps		1
	2462	2.4GHz...	00:90:4C:91:00:01	TI	4.6	73.6	190.0 kbps		3

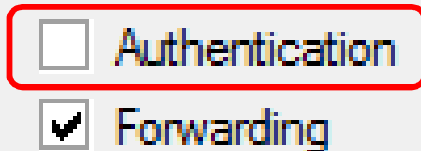
Snooper digunakan untuk melihat data AP lain

ACCESS LIST



ACCESS LIST

- **Access-list**, digunakan AP Router untuk **menolak/menerima** koneksi Router Klien/PC.
- Jika MAC Address klien tidak terdaftar di Access-List, koneksi dari klien akan ditolak .
- Jika MAC Address klien terdaftar di Access-list, koneksi dari router klien akan diterima, tetapi jika terdaftar sedangkan “**authentication**” disable akan ditolak.



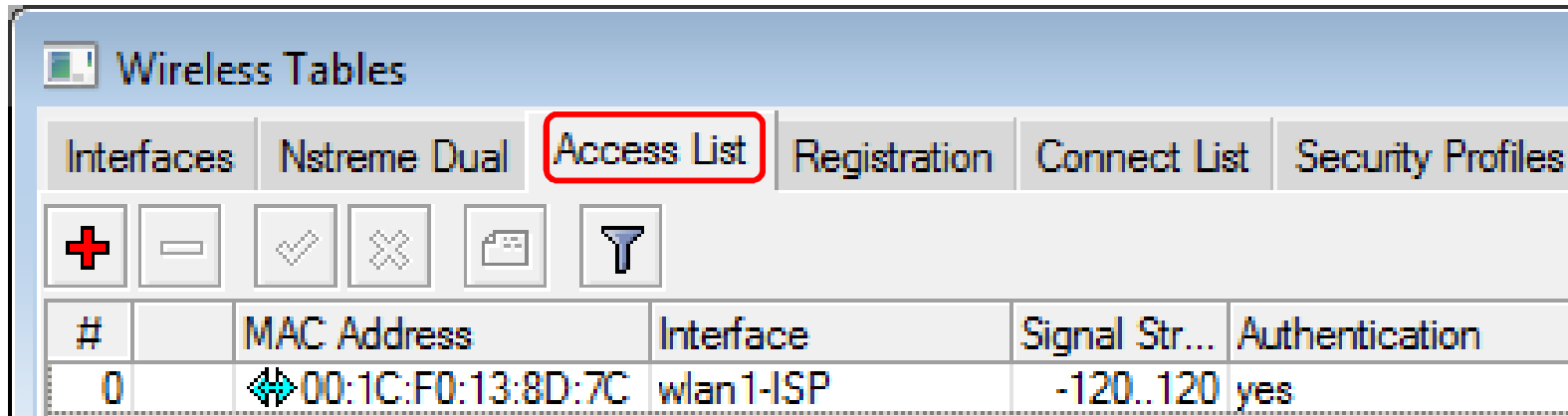
ACCESS LIST

The screenshot shows the Mikrotik Wireless Tables interface. The 'Registration' tab is selected and highlighted with a red box. A table of radio entries is displayed, with the first row selected. A context menu is open over the selected row, and the 'Copy to Access List' option is highlighted with a red box. A red arrow points from the 'Copy to Access List' option back to the selected row in the table.

Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activit...
001CF013...	00:1C:F0:13:8D:7C	1-100	00:00:00			0.000

- Show Categories
- Detail Mode
- Inline Comments
- Show Columns
- Find (Ctrl+F)
- Find Next (Ctrl+G)
- Copy to Access List

ACCESS LIST

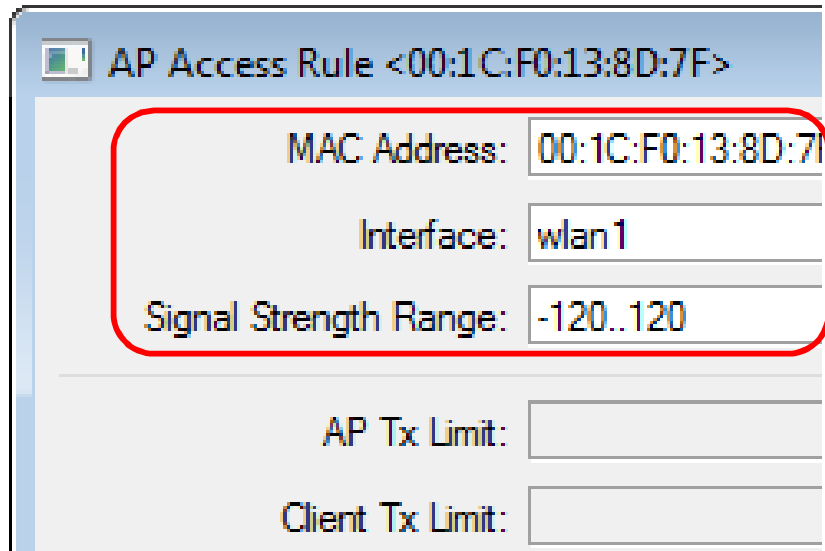


#	MAC Address	Interface	Signal Str...	Authentication
0	↔ 00:1C:F0:13:8D:7C	wlan1-ISP	-120..120	yes

- Disable Default Authenticate di Interface wireless Router AP.

 Default Authenticate
 Default Forward
 Hide SSID

ACCESS LIST



AP Access Rule <00:1C:F0:13:8D:7F>

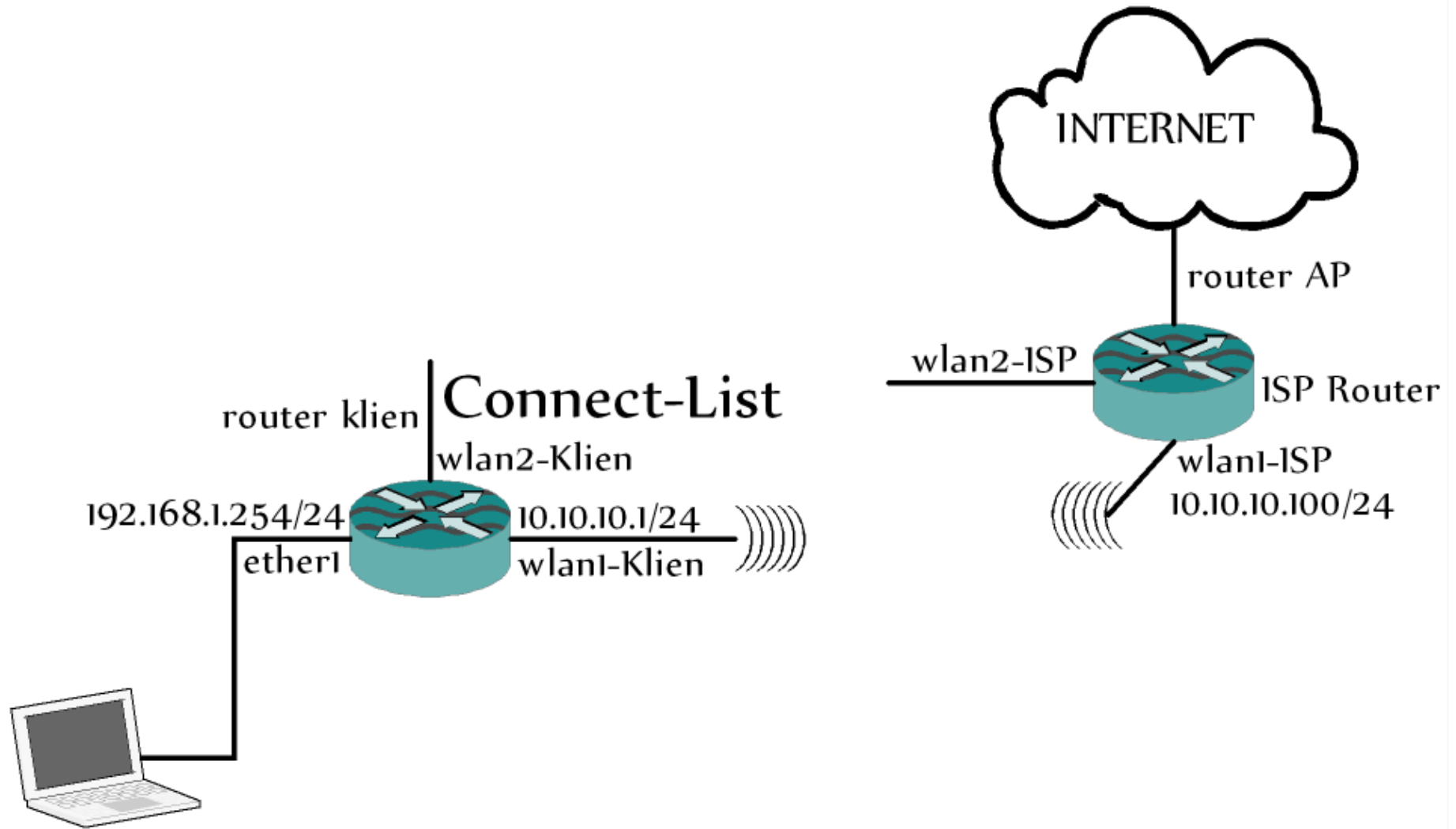
MAC Address:	00:1C:F0:13:8D:7F
Interface:	wlan1
Signal Strength Range:	-120..120
AP Tx Limit:	
Client Tx Limit:	

MAC Address, MAC Address klien yang terdaftar.

Interface, interface Access-list.

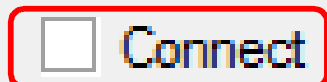
Signal Strength Range, batas sinyal yang boleh terkoneksi, jika diluar rentang sinyal maka koneksi tidak akan terjadi.

CONNECT LIST



CONNECT LIST

- **Connect-List**, digunakan oleh Router Klien untuk **mengijinkan/melarang** koneksi ke Router AP berdasarkan MAC Address dan diproses secara berurutan (sequence).
- Jika MAC Address Router AP tidak terdaftar di Connect-List, koneksi ke Router AP tidak diijinkan, atau meskipun terdaftar namun disable **Connect**, koneksi ke AP Router juga tidak diijinkan.



CONNECT LIST

The screenshot shows the Mikrotik WinBox interface. At the top, the 'Wireless Tables' section is active, with the 'Registration' tab selected. Below the tabs, there are icons for a minus sign, a funnel, and a 'Reset' button. The main area displays a table with the following columns: Radio Name, MAC Address, Interface, Uptime, AP, W..., and Last. One row is selected, showing a radio name starting with '001CF013...', a MAC address of '00:1C:FD:13:8D:7F', and an interface of 'wlan1-KLIEN'. A context menu is open over this row, listing options such as 'Show Categories', 'Detail Mode', 'Inline Comments', 'Show Columns', 'Find', 'Find Next', 'Copy to Access List', and 'Copy to Connect List'. The 'Copy to Connect List' option is highlighted with a red box. A red arrow points from the 'Registration' tab to the table, and another red arrow points from the 'Copy to Connect List' option to the bottom of the page.

Radio Name	MAC Address	Interface	Uptime	AP	W...	Last
001CF013...	00:1C:FD:13:8D:7F	wlan1-KLIEN	00:04:29

CONNECT LIST

#	Interface	MAC Address	Connect	Area Prefix	Signal Str...	Security ...
0	wlan1-KLIEN	00:1C:F0:13:8D:7F	yes		-120..120	default

Station Connect Rule <00:0C:42:E2:34:34>

Interface: wlan1-KLIEN

MAC Address: 00:0C:42:E2:34:34

Connect

- Default Authenticate
- Default Forward
- Hide SSID

Disable Default Authenticate di Interface wireless klien.

Connect, mengizinkan/melarang koneksi ke AP.

SECURITY PROFILE

- Selain menggunakan connect-list dan access-list, koneksi wireless juga bisa diamankan dengan menggunakan metode keamanan WPA/WPA2, keamanan metode pengamanan ini harus diterapkan pada dua sisi, baik sisi AP maupun sisi klien, melalui konfigurasi di security profile.

Name	Mode	Authentication	Unicast Ciphers	Group Ciphers	WPA Pre-Shared
* default	none				*****

SECURITY PROFILE

- **Authentication Types**, metode autentikasi yang digunakan. Klien akan terkoneksi ke AP menggunakan metode autentikasi yang sesuai.

- Authentication Types

<input checked="" type="checkbox"/> WPA PSK	<input checked="" type="checkbox"/> WPA2 PSK
<input type="checkbox"/> WPA EAP	<input type="checkbox"/> WPA2 EAP

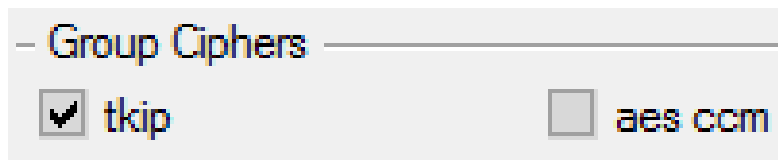
- **Unicast Ciphers**, Klien dapat terkoneksi jika menggunakan salah satu ciphers yang juga digunakan di AP.

- Unicast Ciphers

<input checked="" type="checkbox"/> tkip	<input type="checkbox"/> aes ccm
--	----------------------------------

SECURITY PROFILE


- Untuk Group Cipher, jika AP memilih keduanya maka **AES sebagai yang terkuatlah yang akan digunakan**, disarankan untuk memilih salah satu group cipher dalam mode sebagai AP.
- Jika sebagai station memilih keduanya maka koneksi ke AP dengan salah satu metode dapat terjadi.



WPA AP/STATION

Wireless Tables

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

+ 

Name	Mode	Authentication Types	Unicast Ciphers	Group Ciphers	WPA Pre-Shared Key	WPA2 Pre-Shared Key
default	none					
psk_mikrotik	dynamic keys	WPA PSK WPA2 PSK	tkip	tkip	01234567890	12345678901

Security Profile <psk_mikrotik>

General | **RADIUS** | EAP | Static Keys

Name: psk_mikrotik

Mode: dynamic keys

- Authentication Types -

WPA PSK WPA2 PSK

WPA EAP WPA2 EAP

- Unicast Ciphers -

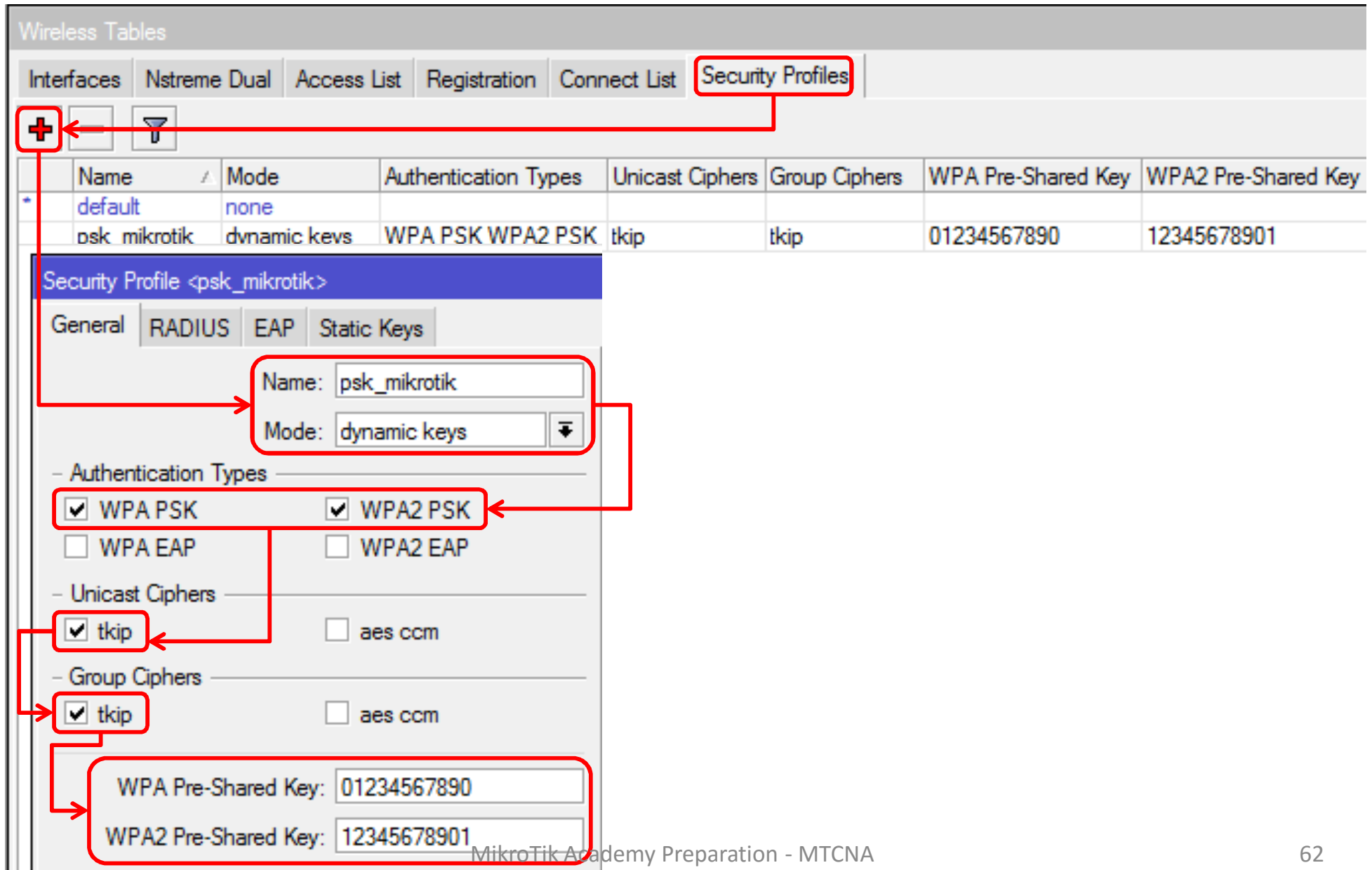
tkip aes ccm

- Group Ciphers -

tkip aes ccm

WPA Pre-Shared Key: 01234567890

WPA2 Pre-Shared Key: 12345678901



WPA AP/STATION

Interface <wlan1>

General Wireless HT WDS Nstreme

Mode: ap bridge

SSID: MikroTik ISP

Scan List: default

Wireless Protocol: unspecified

Security Profile: psk_mikrotik

Bridge Mode: enabled

Interface <wlan1>

General Wireless HT WDS Nstreme

Mode: station

SSID: MikroTik ISP

Scan List: default

Wireless Protocol: unspecified

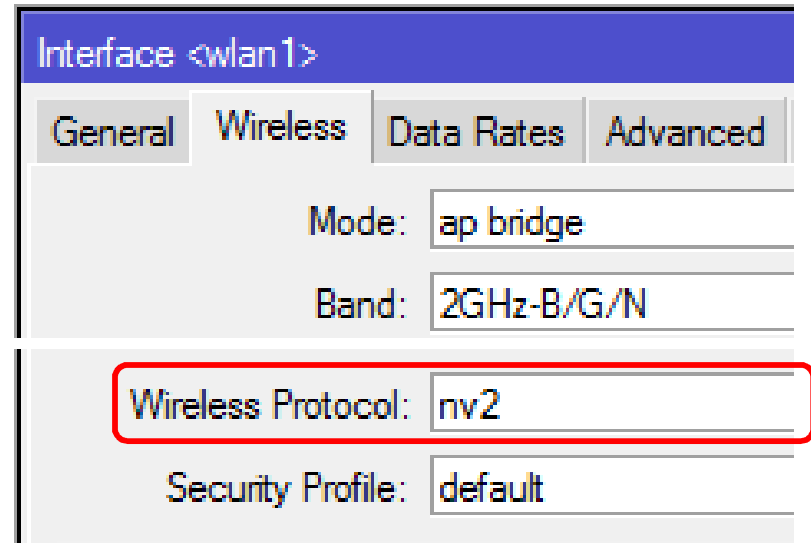
Security Profile: psk_mikrotik

Bridge Mode: enabled

- Default Authenticate
- Default Forward
- Hide SSID

NV2

- NV2 adalah protocol proprietary MikroTik (nstreme versi 2) digunakan berdasarkan protocol TDMA (Time Division Multiple Access).
- Peningkatan kecepatan.
- Pengurangan latency.
- Station yang lebih banyak (511).



Interface <wlan1>

General Wireless Data Rates Advanced

Mode: ap bridge

Band: 2GHz-B/G/N

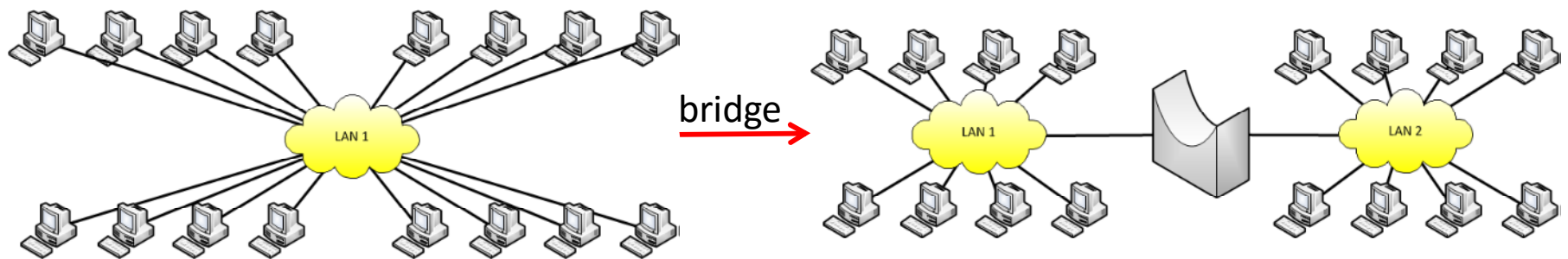
Wireless Protocol: nv2

Security Profile: default

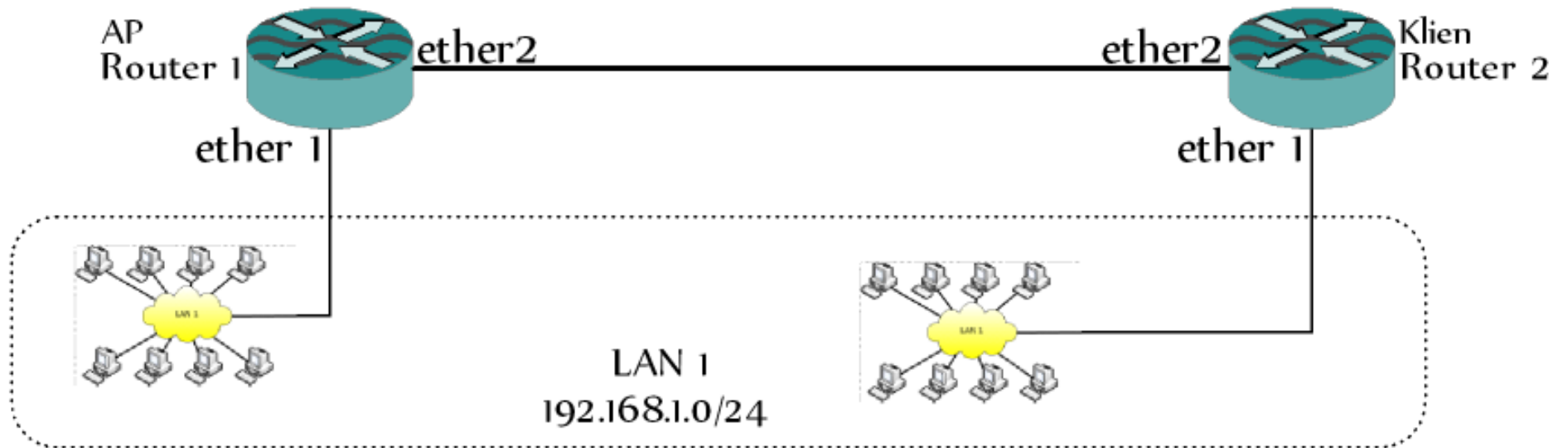
BRIDGE

BRIDGE

- Menggabungkan 2 atau lebih interface bertipe ethernet yang berada dalam 1 segmen network yang sama, dapat digunakan untuk memperkecil collision domain



BRIDGE



WIRELESS BRIDGE

Quick Set
Interfaces
Wireless
Bridge
PPP

Bridge

Bridge	Ports	Filters	NAT	Host
+	-	✓	✗	📄

Name	Type	L2 MTU	T
bridge1	Bridge	65535	0

Interface <bridge1>

General STP Status Traffic

Name: bridge1

Type: Bridge

Bridge

Bridge	Ports	Filters	NAT
+	-	✓	✗

Interface	Bridge
ether1	bridge1
ether2	bridge1

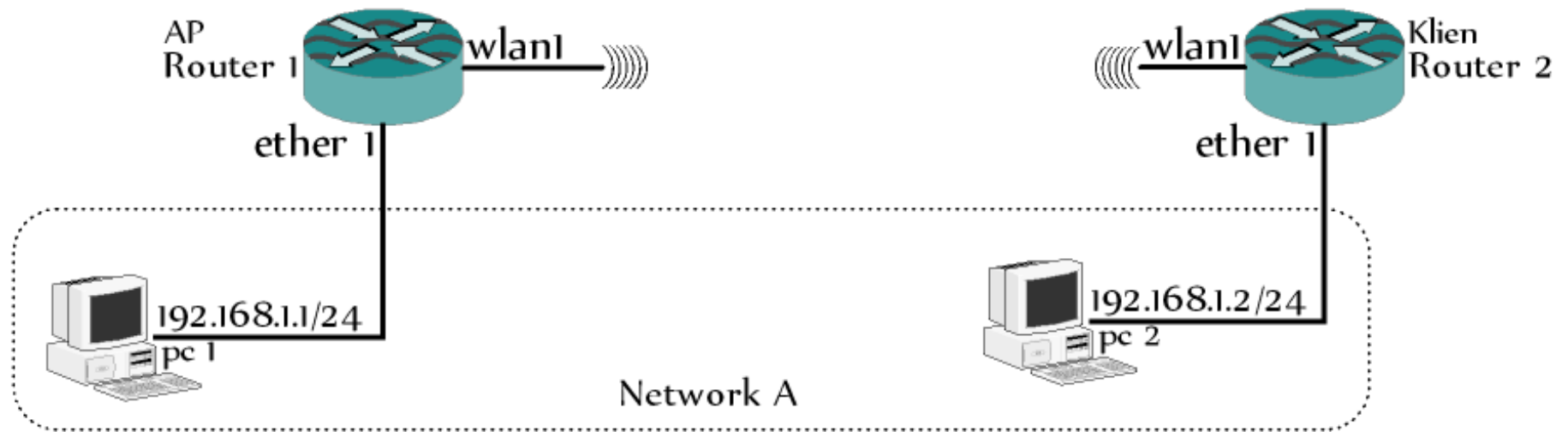
Bridge Port <ether2>

General Status

Interface: ether2

Bridge: bridge1

WIRELESS BRIDGE



WIRELESS BRIDGE

Bridge configuration window showing the 'Ports' tab. A red box highlights the '+' icon in the top left. A table below shows the interface configuration:

Interface	Bridge
ether1	bridge1

The 'Bridge Port <ether1>' configuration is shown with the 'General' tab selected. A red box highlights the 'General' tab. The configuration fields are:

Interface: ether1
Bridge: bridge1

Bridge configuration window showing the 'Ports' tab. A red box highlights the '+' icon in the top left. A table below shows the interface configuration:

Interface	Bridge
ether1	bridge1
wlan1	bridge1

The 'Bridge Port <wlan1>' configuration is shown with the 'General' tab selected. A red box highlights the 'General' tab. The configuration fields are:

Interface: wlan1
Bridge: bridge1

Interface configuration window for 'wlan1'. The 'Wireless' tab is selected. A red box highlights the 'Wireless' tab. The configuration field is:

Mode: ap bridge

Interface configuration window for 'wlan1'. The 'Wireless' tab is selected. A red box highlights the 'Wireless' tab. The configuration field is:

Mode: station bridge

ROUTING

ROUTING

- Pengaturan jalur antar network berdasarkan IP Address asal dan tujuan
- Static Routing adalah jalur spesifik yang ditentukan oleh admin untuk meneruskan paket dari jaringan sumber ke jaringan tujuan, dimana jaringan tujuan sudah diketahui.
- Default routing juga merupakan static routing yang alamat jaringan tujuan tidak diketahui.

PARAMETER ROUTING

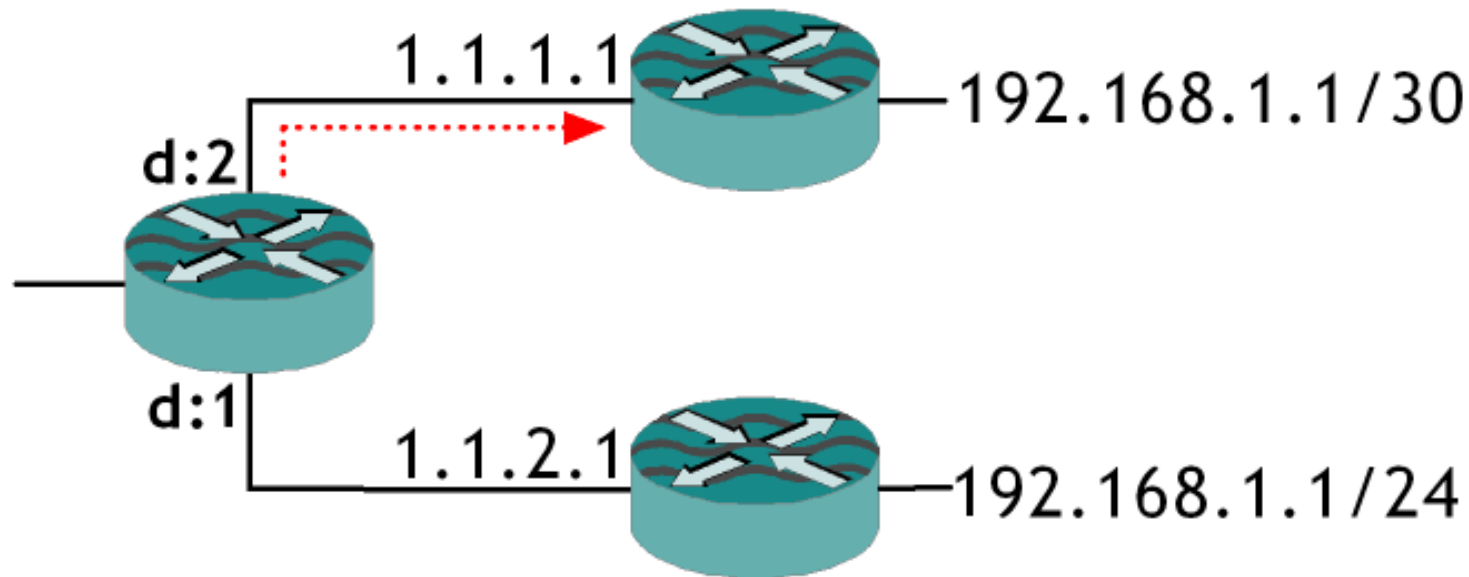
- Jaringan tujuan (Destination)
 - Destination address & network mask (contoh: 192.168.1.0/24, static routing)
 - 0.0.0.0/0 -> ke semua network atau ke network yang belum diketahui. (default routing)
- Gateway
 - IP Address gateway, harus merupakan IP Address yang satu subnet dengan IP yang terpasang pada salah satu interface, seringkali disebut sebagai *next hop address*. (IP Address yang dikonfigurasi di router yang berdampingan)
 - Gateway dapat berupa IP Address atau interface (PPP)

PARAMETER ROUTING

- Distance adalah nilai digunakan untuk memilih jalur routing, nilainya (0-255) secara default tergantung protocol routing yang digunakan:
 - Connected routes : 0; Static Routes : 1; eBGP : 20
 - OSPF : 110
 - RIP : 120, MME : 130
 - iBGP : 200

PARAMETER ROUTING

- Untuk pemilihan routing, router akan memilih berdasarkan:
 - Network tujuan dengan subnet yang lebih kecil

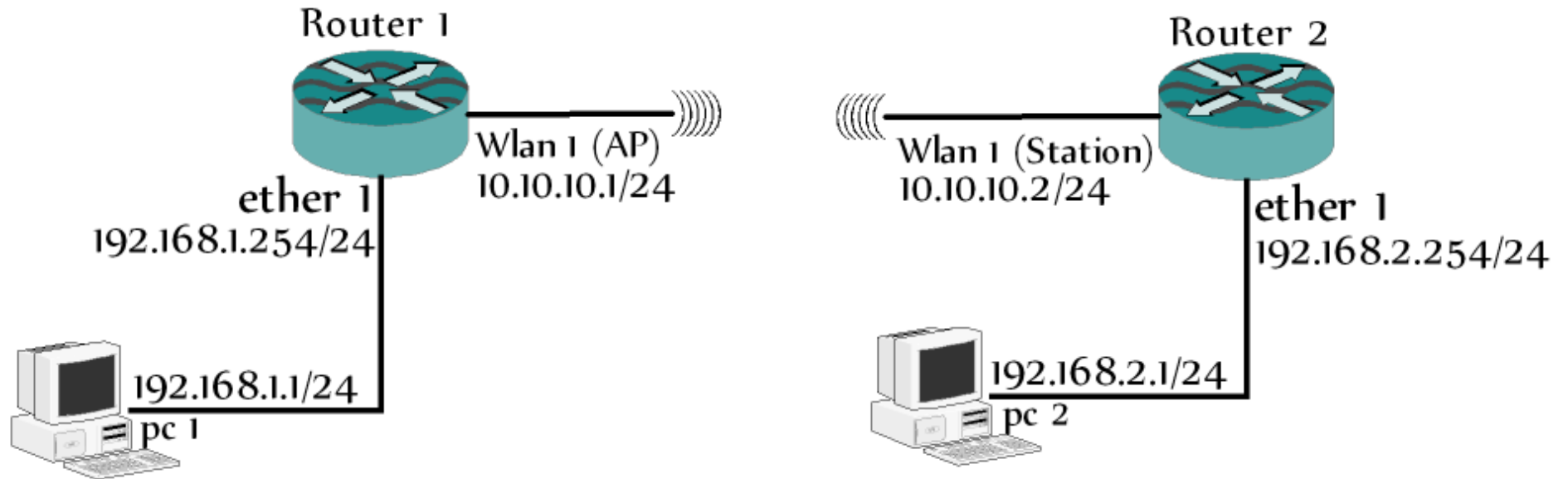


- Distance yang lebih kecil jika subnetnya sama

ROUTE FLAGS

- X: Disabled, tidak mempengaruhi proses routing
- A: Active, aktif, digunakan dalam proses routing
- D: Dynamic, aktif, dihasilkan dari routing dynamic
- C: Connected, aktif dan terkoneksi langsung
- S: Static, aktif, konfigurasi manual.
- Dynamic Routing Flags:
 - r=RIP; b=BGP; o=OSPF; m=MME

STATIC ROUTING

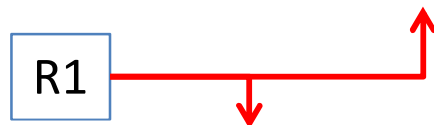


STATIC ROUTING

Route List

Routes	Nexthops	Rules	VRF
	Dst. Address	Gateway	
DAC	▶ 10.10.10.0/24	wlan1 reachable	
DAC	▶ 192.168.1.0/24	ether1 reachable	
AS	▶ 192.168.2.0/24	10.10.10.2 reachable wlan1	

A - active, S - static



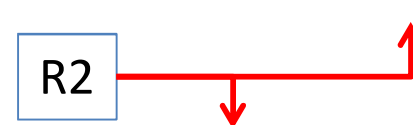
Route <192.168.2.0/24>

General	Attributes
Dst. Address:	192.168.2.0/24
Gateway:	10.10.10.2 reachable wlan1

Route List

Routes	Nexthops	Rules	VRF
	Dst. Address	Gateway	
DAC	▶ 10.10.10.0/24	wlan1 reachable	
AS	▶ 192.168.1.0/24	10.10.10.1 reachable wlan1	
DAC	▶ 192.168.2.0/24	ether1 reachable	

A - active, S - static



Route <192.168.1.0/24>

General	Attributes
Dst. Address:	192.168.1.0/24
Gateway:	10.10.10.1 reachable wlan1

FIREWALL NAT

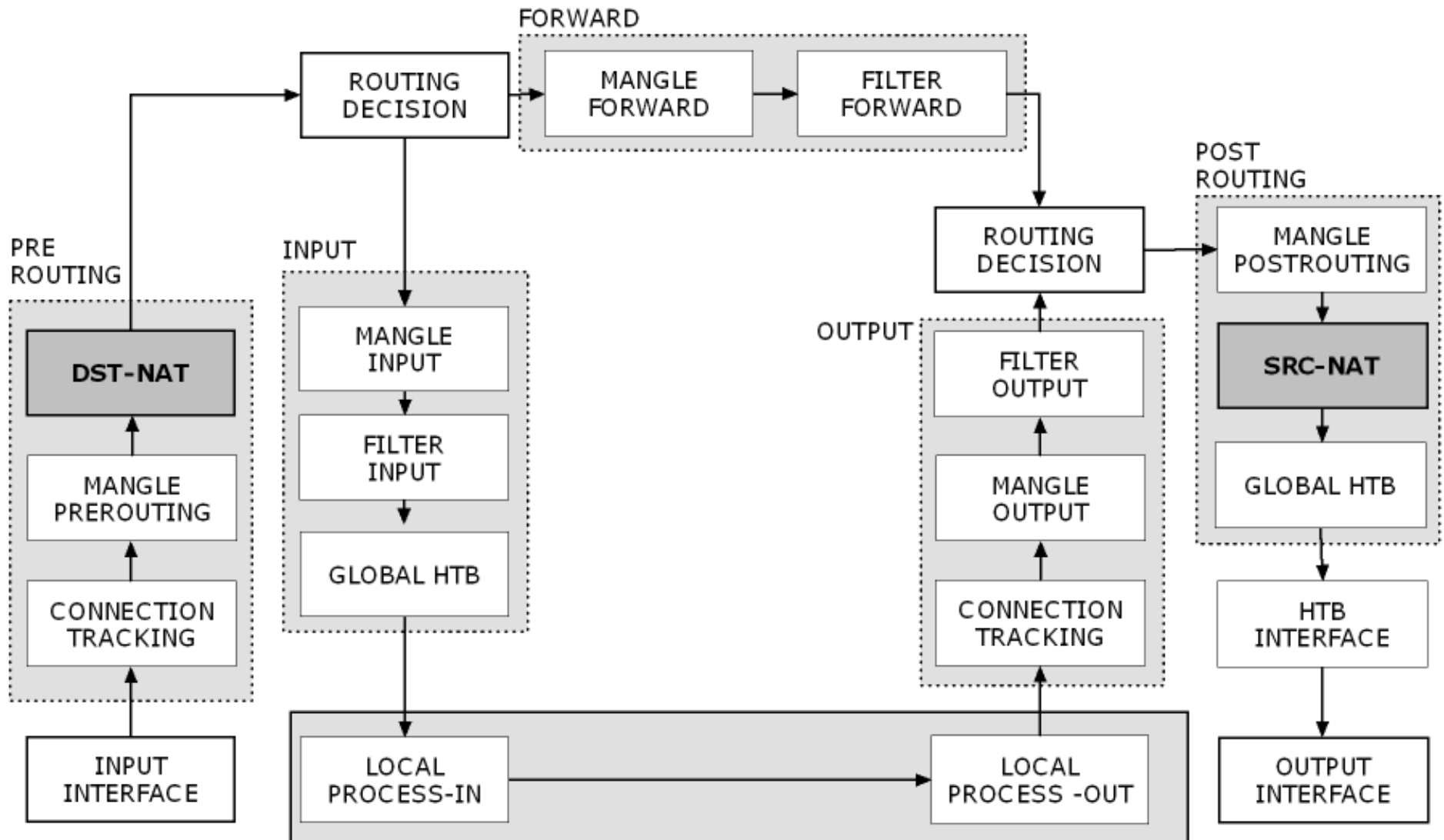
NAT

- NAT melakukan perubahan alamat dan port, ada dua tipe NAT yaitu merubah alamat sumber dan atau port disebut sebagai **srcnat**, dan merubah alamat tujuan dan atau port disebut sebagai **dstnat**
- Proses NAT hanya dilakukan pada paket data pertama dari sebuah koneksi, kemudian paket berikutnya pada koneksi tersebut otomatis terkena NAT

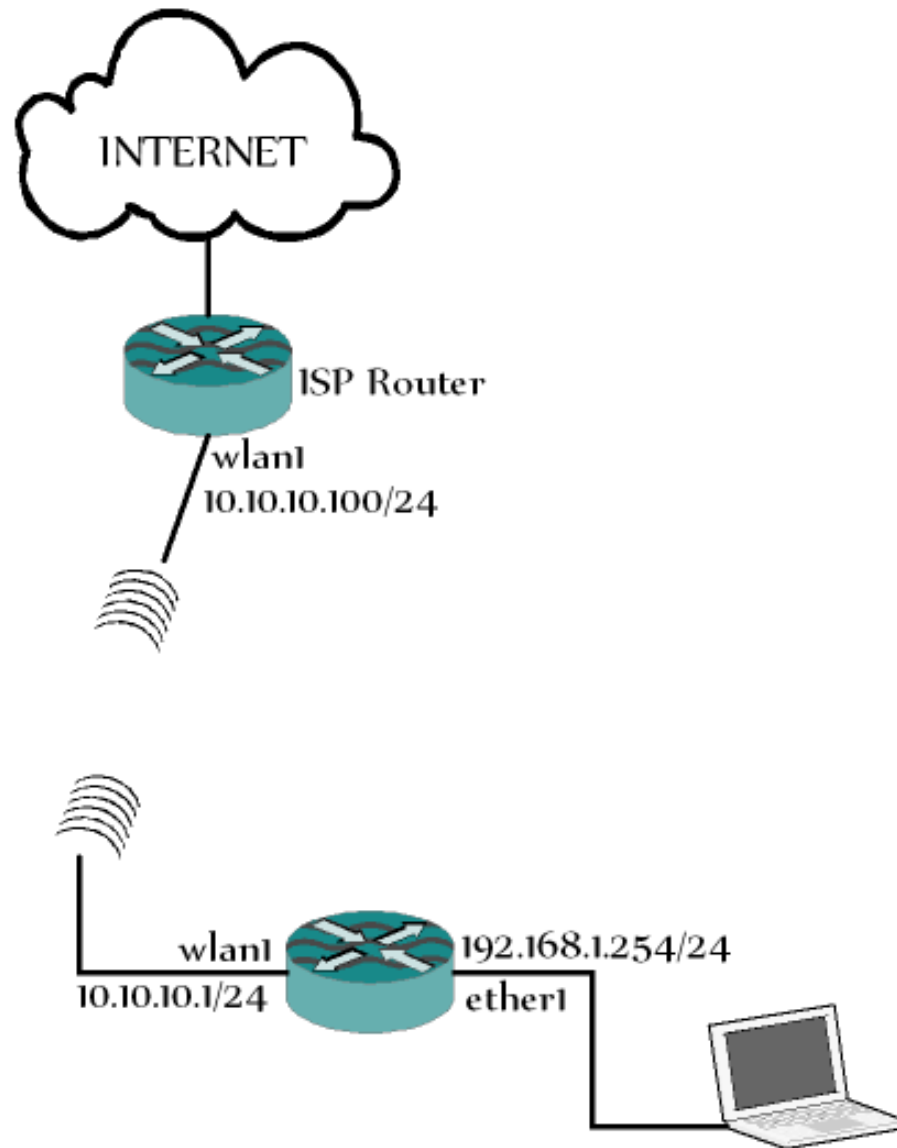
NAT

- Ada dua default chain dalam NAT
 - **srcnat**, memproses traffic yang keluar dari router sesudah chain output dan yang melalui router sesudah chain forward.
 - **dstnat**, memproses traffic yang menuju/melalui router sebelum chain input dan forward.
- Selain default chain, dapat dibuat user-define chain

DIAGRAM NAT



SRC-NAT



SRC-NAT

Firewall

Filter Rules **NAT** Mangle Service Ports Connec

+ - ✓ ✗ ☰ Reset Count

#	Action	Chain	Src. Address
---	--------	-------	--------------

New NAT Rule

General Advanced Extra Action Statistics

Chain: srcnat

Any. Port:

In. Interface:

Out. Interface: wlan1

Firewall

Filter Rules **NAT** Mangle Service Por

+ - ✓ ✗ ☰

#	Action	Chain
0	masquerade	srcnat

NAT Rule

General Advanced Extra **Action**

Action: masquerade

Log

Log Prefix:

DEFAULT ROUTING & DNS

Route <0.0.0.0/0>

General Attributes

Dst. Address: 0.0.0.0/0

Gateway: 10.10.10.100 reachable wlan 1

DNS Settings

Servers: 10.10.10.100

Dynamic Servers:

Allow Remote Requests

Max UDP Packet Size: 512

Cache Size: 2048 KB

Cache Used: 27

Obtain an IP address automatically

Use the following IP address:

IP address: 192 . 168 . 1 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 254

Obtain DNS server address automatically

Use the following DNS server addresses

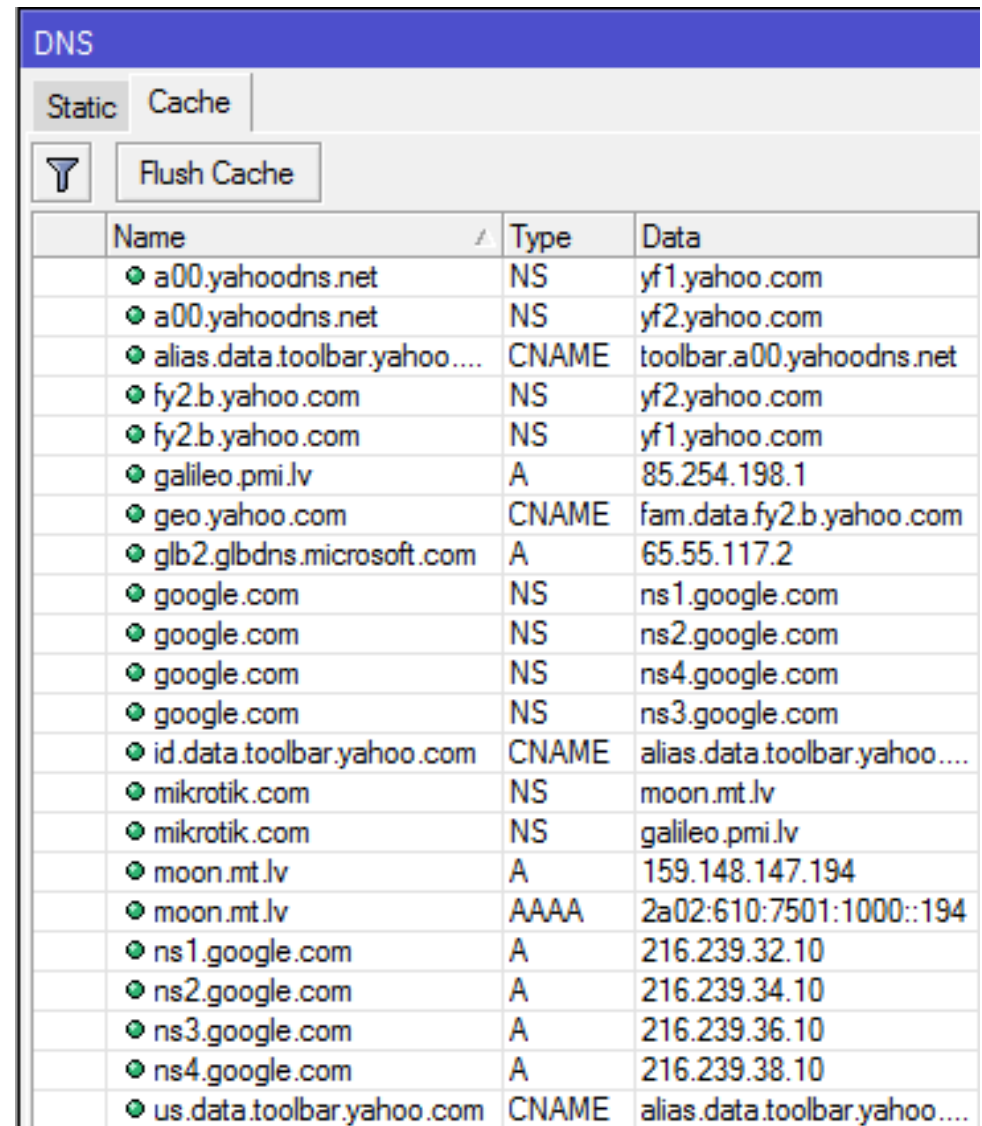
Preferred DNS server: 192 . 168 . 1 . 254

Alternate DNS server: . . .

“Allow Remote Request” mengubah DNS Client menjadi DNS Cache

DNS

- DNS Client digunakan oleh router dalam konfigurasi web-proxy atau hotspot
- Aktivasi DNS Cache meminimalkan waktu request dan berfungsi sebagai DNS Server lokal



The screenshot shows the DNS Cache configuration window in Mikrotik WinBox. It features a 'Static' tab and a 'Cache' tab. Below the tabs is a 'Flush Cache' button. The main area contains a table with the following columns: Name, Type, and Data. The table lists various DNS records, including NS, CNAME, and A records for domains like yahoo.com, google.com, and mikrotik.com.

Name	Type	Data
a00.yahoodns.net	NS	yf1.yahoo.com
a00.yahoodns.net	NS	yf2.yahoo.com
alias.data.toolbar.yahoo....	CNAME	toolbar.a00.yahoodns.net
fy2.b.yahoo.com	NS	yf2.yahoo.com
fy2.b.yahoo.com	NS	yf1.yahoo.com
galileo.pmi.lv	A	85.254.198.1
geo.yahoo.com	CNAME	fam.data.fy2.b.yahoo.com
glb2.glb dns.microsoft.com	A	65.55.117.2
google.com	NS	ns1.google.com
google.com	NS	ns2.google.com
google.com	NS	ns4.google.com
google.com	NS	ns3.google.com
id.data.toolbar.yahoo.com	CNAME	alias.data.toolbar.yahoo....
mikrotik.com	NS	moon.mt.lv
mikrotik.com	NS	galileo.pmi.lv
moon.mt.lv	A	159.148.147.194
moon.mt.lv	AAAA	2a02:610:7501:1000::194
ns1.google.com	A	216.239.32.10
ns2.google.com	A	216.239.34.10
ns3.google.com	A	216.239.36.10
ns4.google.com	A	216.239.38.10
us.data.toolbar.yahoo.com	CNAME	alias.data.toolbar.yahoo....

STATIC DNS ENTRY

- Static DNS digunakan untuk mempercepat proses trace route, Static DNS akan menimpa dynamic entry yang ada di DNS cache

DNS Static

+ - ✓ ✗ ⏏

#	Name	Address
0	www.mikrotik.com	1.1.1.1

DNS Static Entry <www.mikrotik.com>

Name:

Address:

TTL: s

DNS Cache

⏏ Flush Cache

	Name	Type	Data
S	1.1.1.1.in-addr.arpa	PTR	www.mikrotik.com
	ed.microsoft.com	CNAME	crf.www.ms.akadns.net
S - static	s.msftncsi.com	AAAA	fd3e:4f5a:5b81::1
	ds-sg-fp3-fb.wg1.b.yaho...	CNAME	ds-sg-fp3.wg1.b.yahoo.c...
	fd-fp3.wg1.b.yahoo.com	CNAME	ds-fp3.wg1.b.yahoo.com
	geo.kaspersky.com	SOA	dnsmaster.kasperskylab...
	kaspersky-labs.com	SOA	dnsmaster.kasperskylab...
	ksn-file-geo.kaspersky-la...	CNAME	ksn-file.geo.kaspersky.c...

ACTION: SRC NAT

- Melakukan NAT, dari beberapa IP lokal ke satu IP Publik

NAT Rule <192.168.1.1-192.168.1.3>

General Advanced Extra Action Statistics

Chain: srcnat

Src. Address: 192.168.1.1-192.168.1.3

NAT Rule <192.168.1.1-192.168.1.3>

General Advanced Extra Action

Action: src-nat

Log

Log Prefix:

To Addresses: 10.10.10.1

To Ports:

ACTION: SAME

- **Same**, Melakukan NAT, dari sekelompok IP lokal ke sekelompok IP Publik dengan rentang IP Address diantara kedua network boleh berbeda.

NAT Rule <192.168.1.1-192.168.1.3>

General Advanced Extra Action Statistics

Chain: srcnat

Src. Address: 192.168.1.1-192.168.1.3

NAT Rule <192.168.1.1-192.168.1.3>

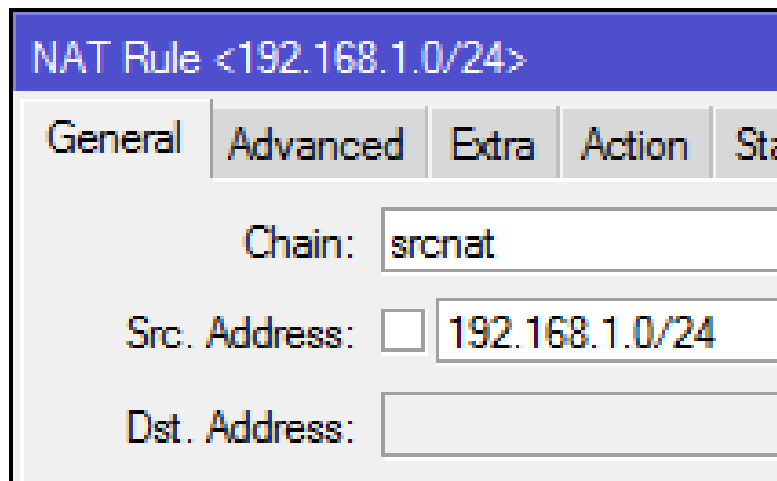
General Advanced Extra Action Statistics

Action: same

To Addresses: 10.10.10.1-10.10.10.2

ACTION: NETMAP

- **Netmap**, sama dengan SAME, namun dengan rentang IP lokal dan IP publik berbanding 1:1



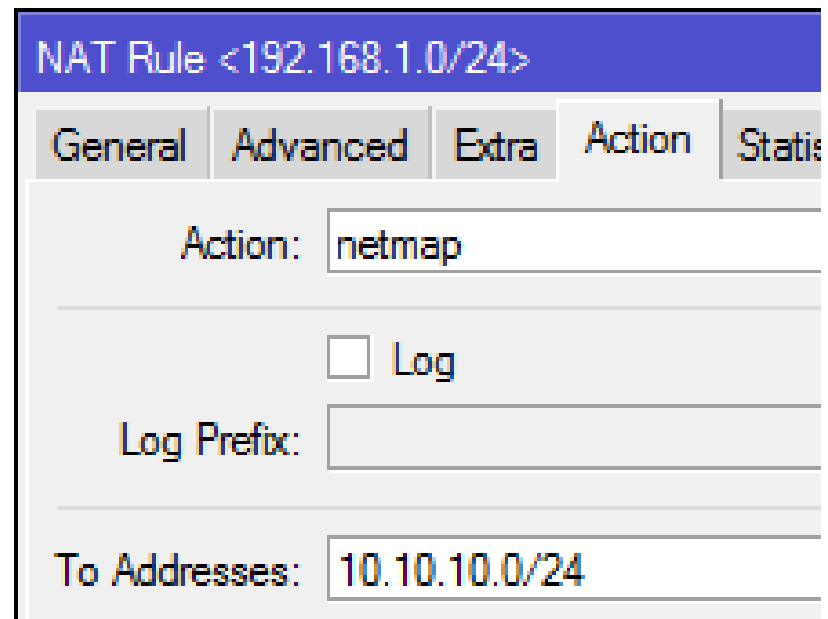
NAT Rule <192.168.1.0/24>

General | Advanced | Extra | Action | Statistics

Chain: srcnat

Src. Address: 192.168.1.0/24

Dst. Address:



NAT Rule <192.168.1.0/24>

General | Advanced | Extra | Action | Statistics

Action: netmap

Log

Log Prefix:

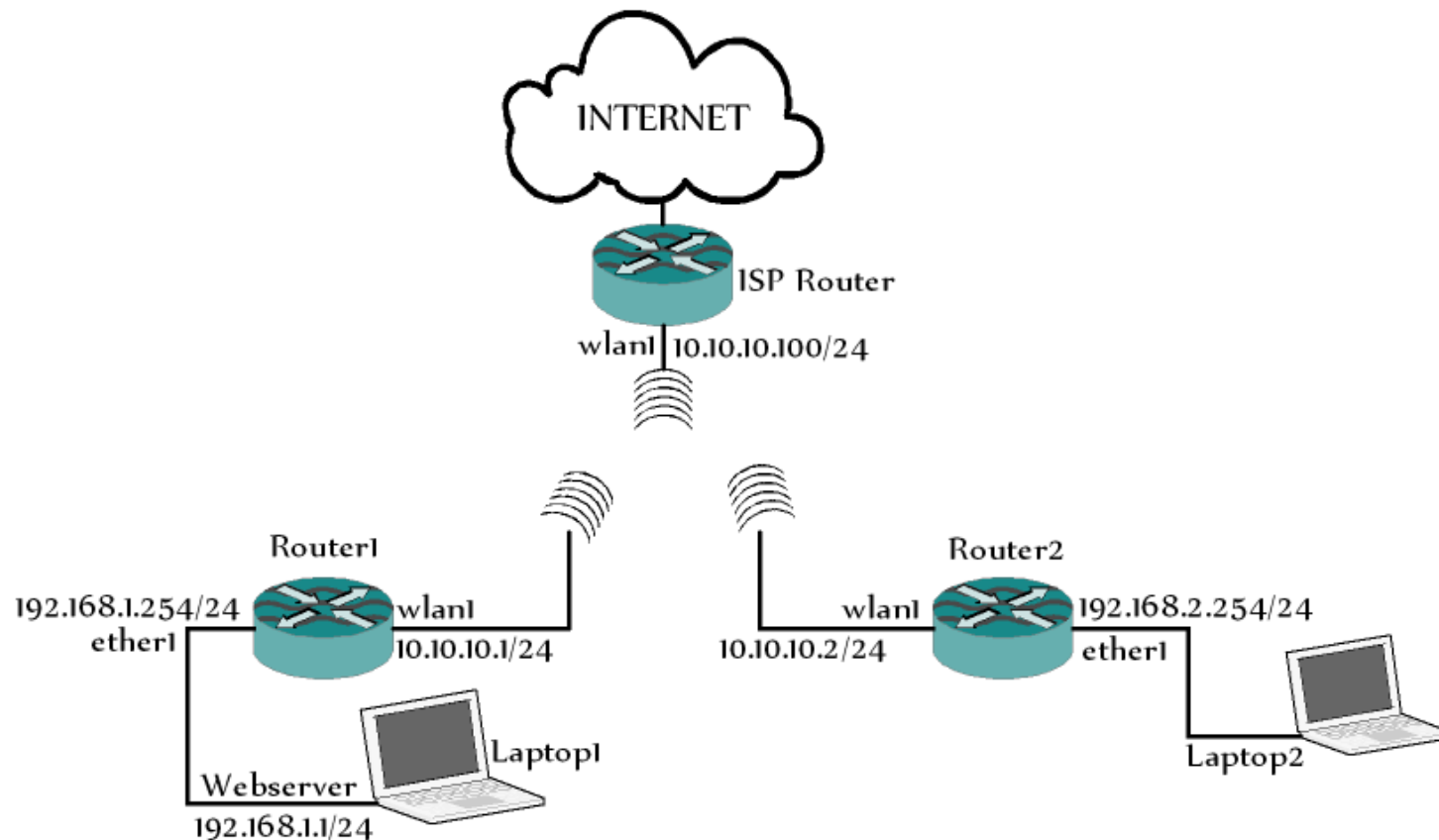
To Addresses: 10.10.10.0/24

DST-NAT

- DST-NAT dapat digunakan untuk pengalihan:
 - Alamat tujuan & portnya
 - Akses web kembali router
 - Port tujuan
 - DNS klien ke DNS router

ACTION: DST-NAT

- DST-NAT dapat digunakan untuk mengubah alamat tujuan & port, agar pengguna internet dapat melakukan akses server di jaringan lokal



ACTION: DST-NAT

Firewall

Filter Rules **NAT** Mangle Service Ports

+ - ✓ ✗ 📄 🗑️

#	Action	Chain	Src. Address
0	→ mas...	srcnat	

New NAT Rule

General Advanced Extra Action

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Firewall

Filter Rules **NAT** Mangle Service Ports Connections Address

+ - ✓ ✗ 📄 🗑️ Reset Counters 00 Re

#	Action	Chain	Src. Address	Dst. Address	Protocol
0	→ masquerade	srcnat			
1	→ ^ dst-nat	dstnat		10.10.10.1	6 (tcp)

NAT Rule <10.10.10.1>

General Advanced Extra **Action** Statistics

Action:

Log

Log Prefix:

To Addresses:

To Ports:

ACTION: REDIRECT

- Pengalihan akses web kembali router (port 80)

NAT Rule <192.168.1.1->80>

General Advanced Extra Action

Chain: dstnat

Src. Address: 192.168.1.1

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port: 80

Firewall

Filter Rules NAT Mangle Service Ports Connections Address List

+ - ✓ ✕ 📄 📏 ⚙️ Reset Counters 00 Reset

#	Action	Chain	Src. Address	Dst. Address	Protocol	State
0	masquerade	srcnat				
1	dst-nat	dstnat		10.10.10.1	6 (tcp)	
2	redirect	dstnat	192.168.1.1		6 (tcp)	

NAT Rule <192.168.1.1->80>

General Advanced Extra Action Statistics

Action: redirect

Log

Log Prefix:

To Ports: 80

ACTION: REDIRECT

- Pengalihan port tujuan

NAT Rule <192.168.1.1->8291>

General Advanced Extra Action

Chain: dstnat

Src. Address: 192.168.1.1

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port: 8291

NAT Rule <192.168.1.1->8291>

General Advanced Extra Action Statistics

Action: redirect

Log

Log Prefix:

To Ports: 8111

IP Service <winbox>

Name: winbox

Port: 8111

Available From:

ACTION: REDIRECT

- Pengalihan DNS klien ke DNS router, apapun DNS klien tetap menggunakan DNS di router

NAT Rule <53>

General Advanced Extra Action

Chain: dstnat

Src. Address:

Dst. Address:

Protocol: 17 (udp)

Src. Port:

Dst. Port: 53

NAT Rule <53>

General Advanced Extra Action

Action: redirect

Log

Log Prefix:

To Ports: 53

FIREWALL FILTER

FIREWALL FILTER

- Mengatur perlindungan router dari akses yang tidak diinginkan dengan membuat aturan
- Aturan berisi predifine rule yang bekerja berdasarkan prinsip **IF-Then**, yang diurutkan dalam chain
- Ada tiga chain utama yaitu: input, output, forward, serta ada juga user define chain

FIREWALL FILTER

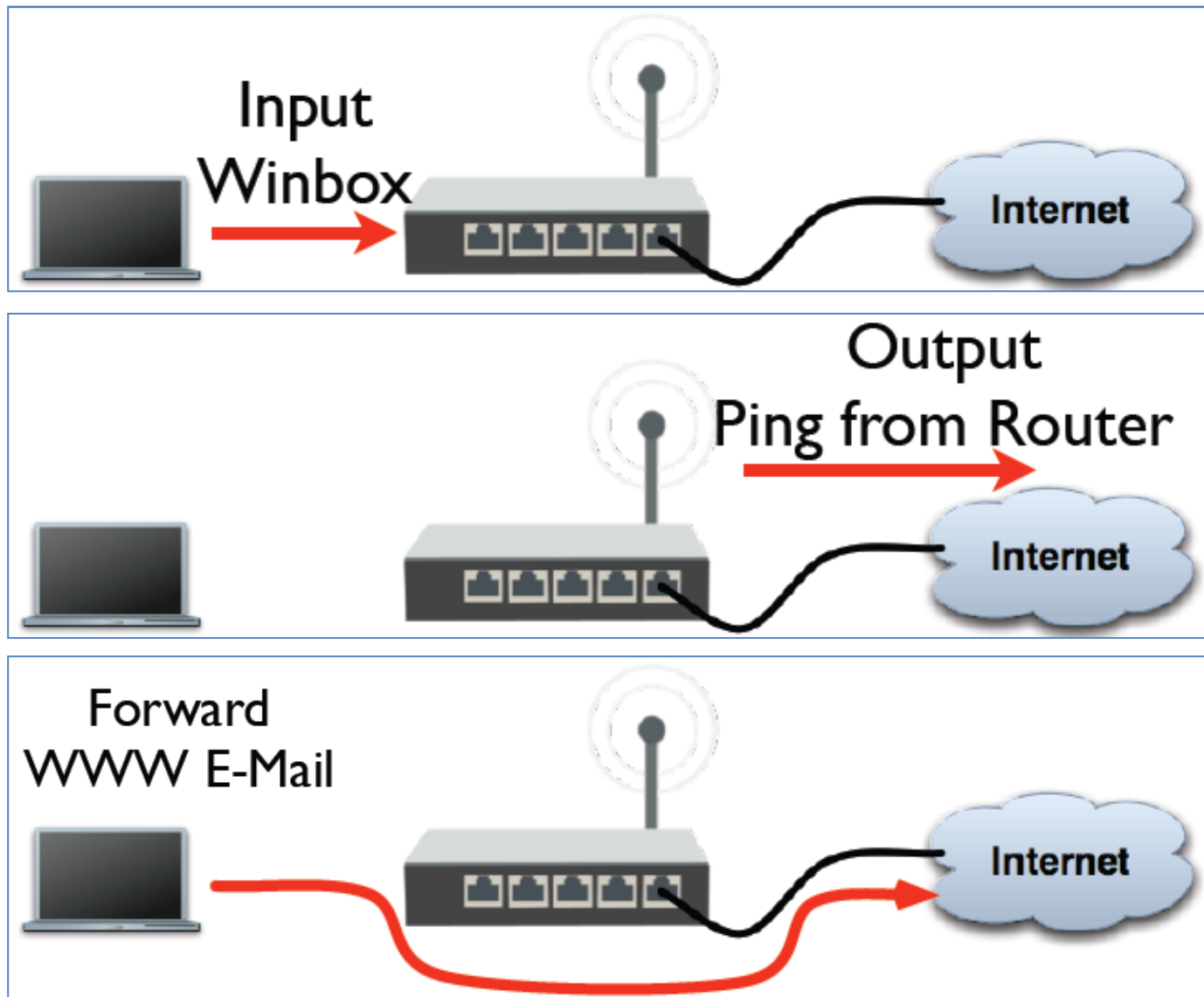
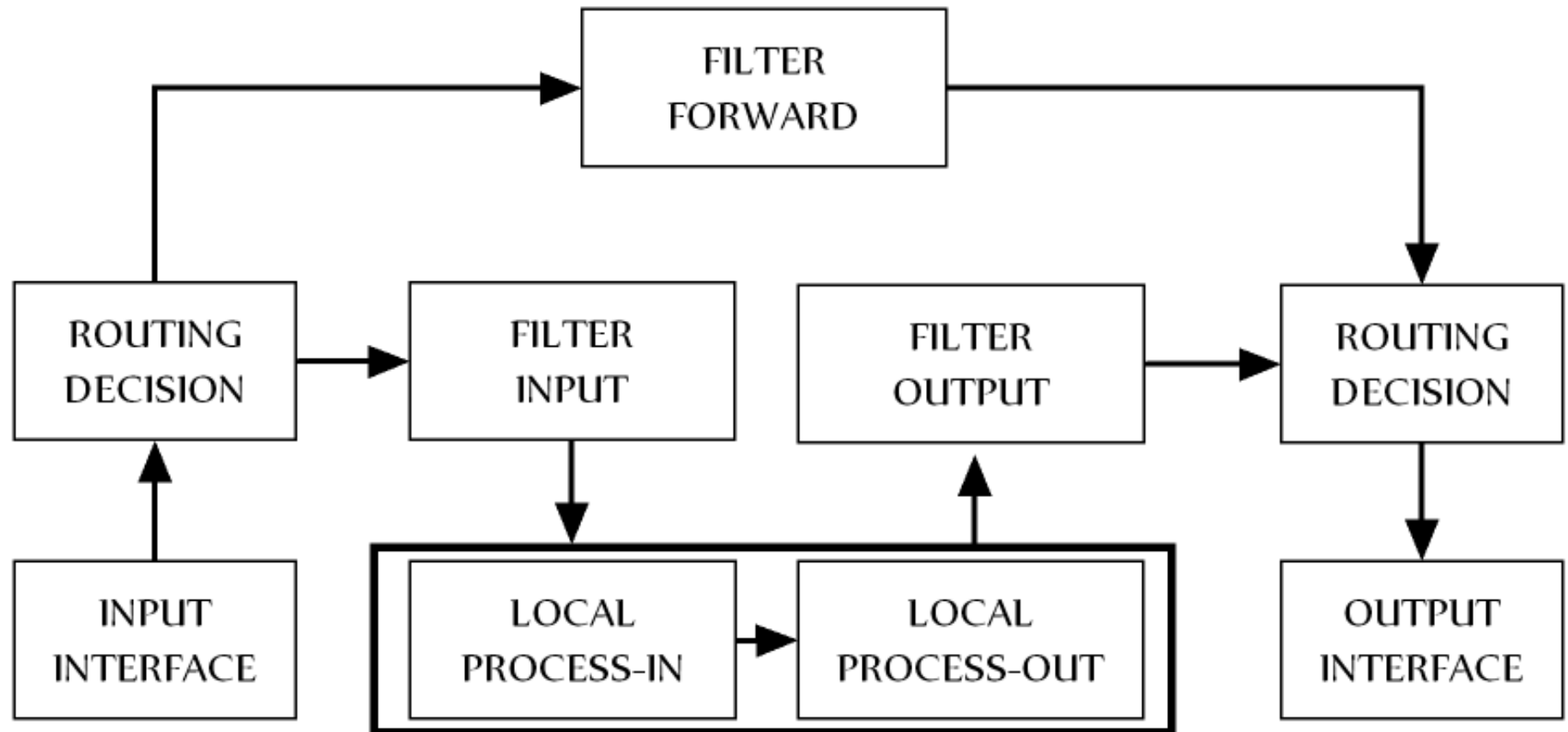
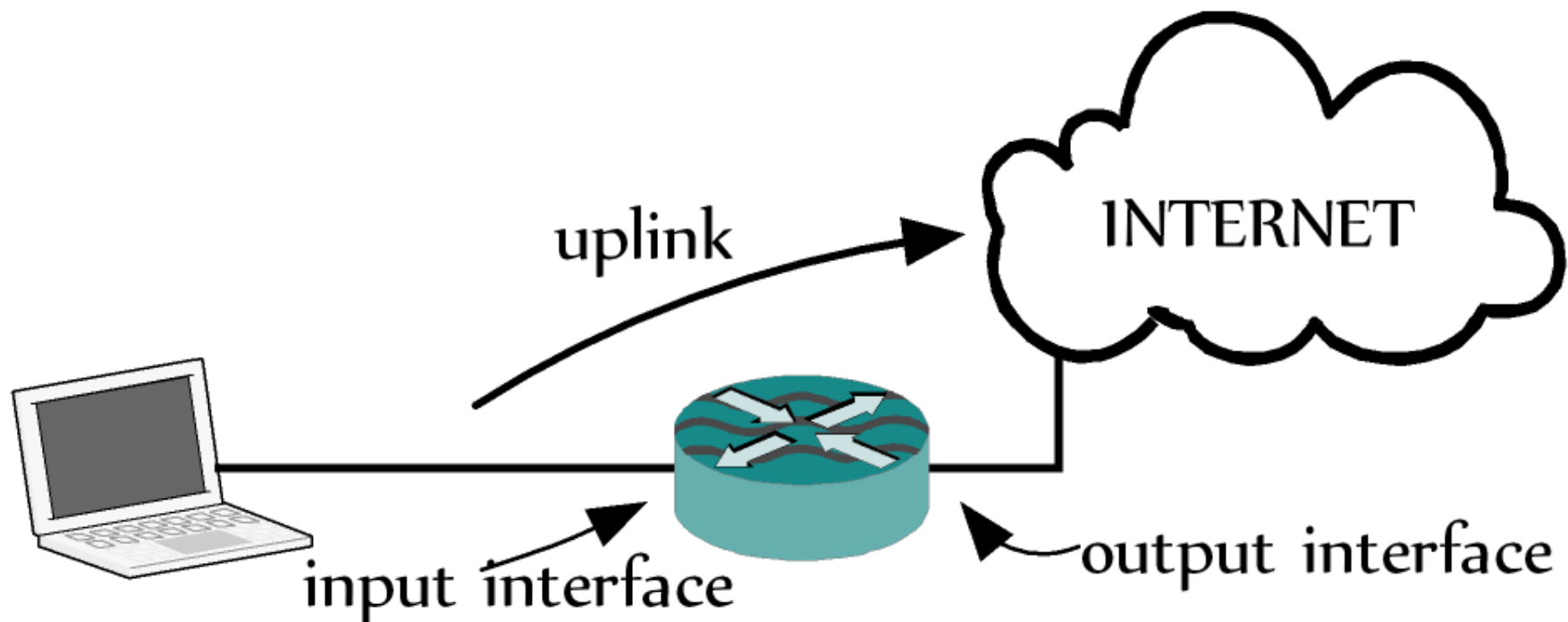


DIAGRAM FIREWALL FILTER



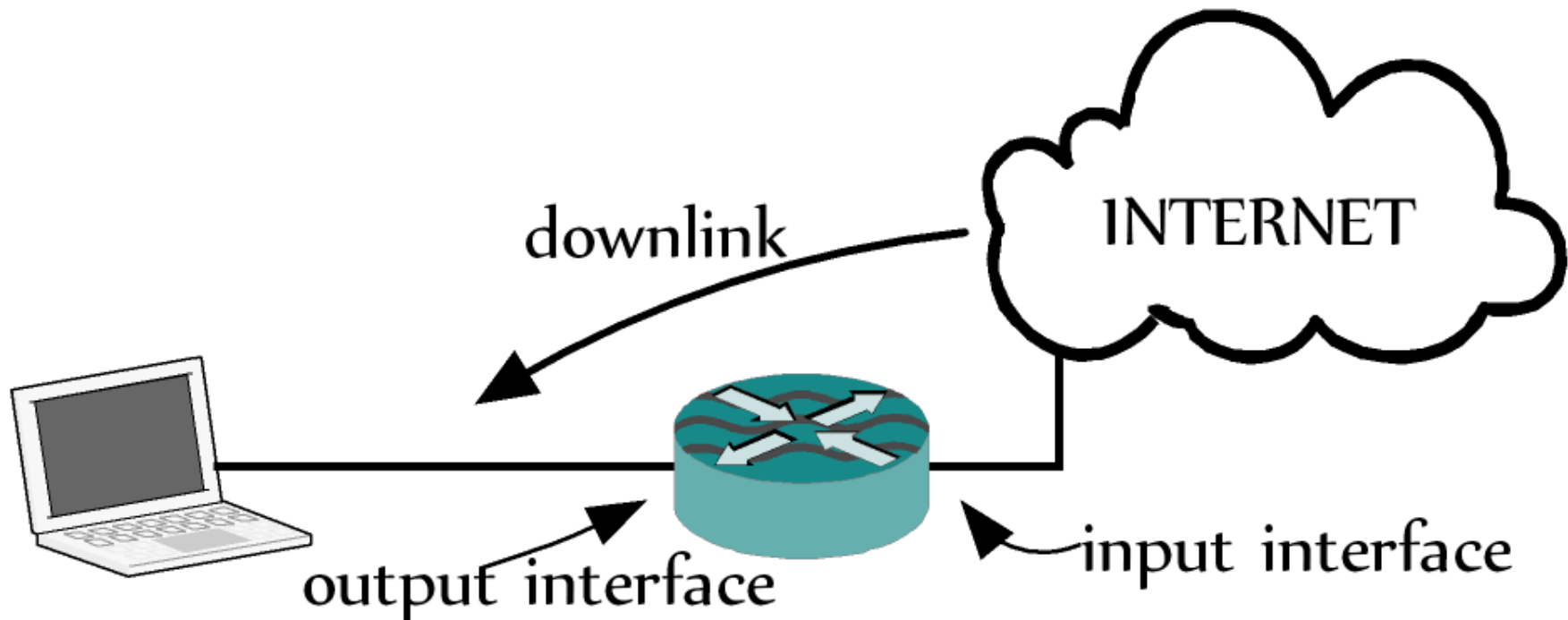
INPUT INTERFACE

- Adalah interface yang dilalui oleh paket data ketika masuk di router



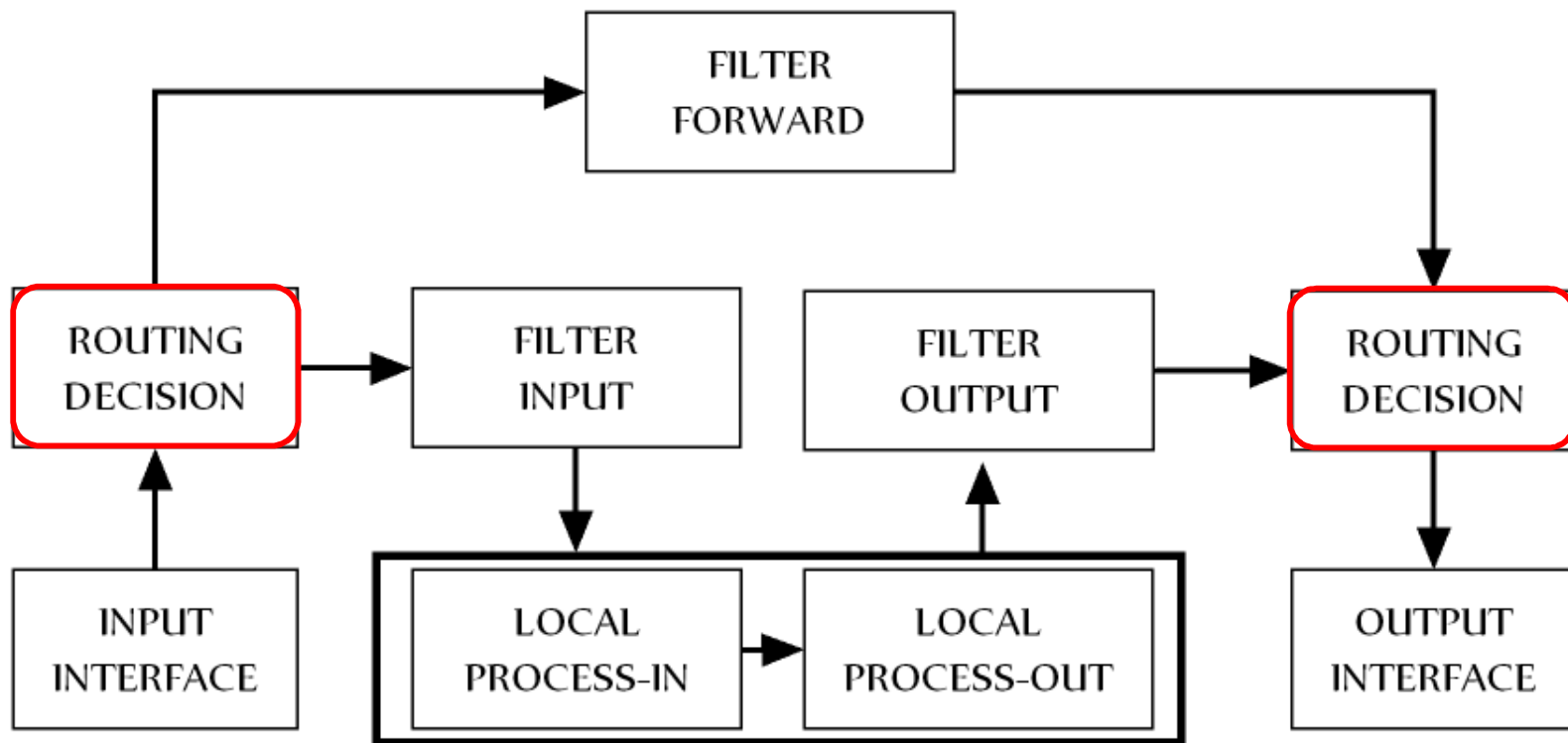
OUTPUT INTERFACE

- Adalah interface yang dilalui oleh paket data ketika keluar dari router



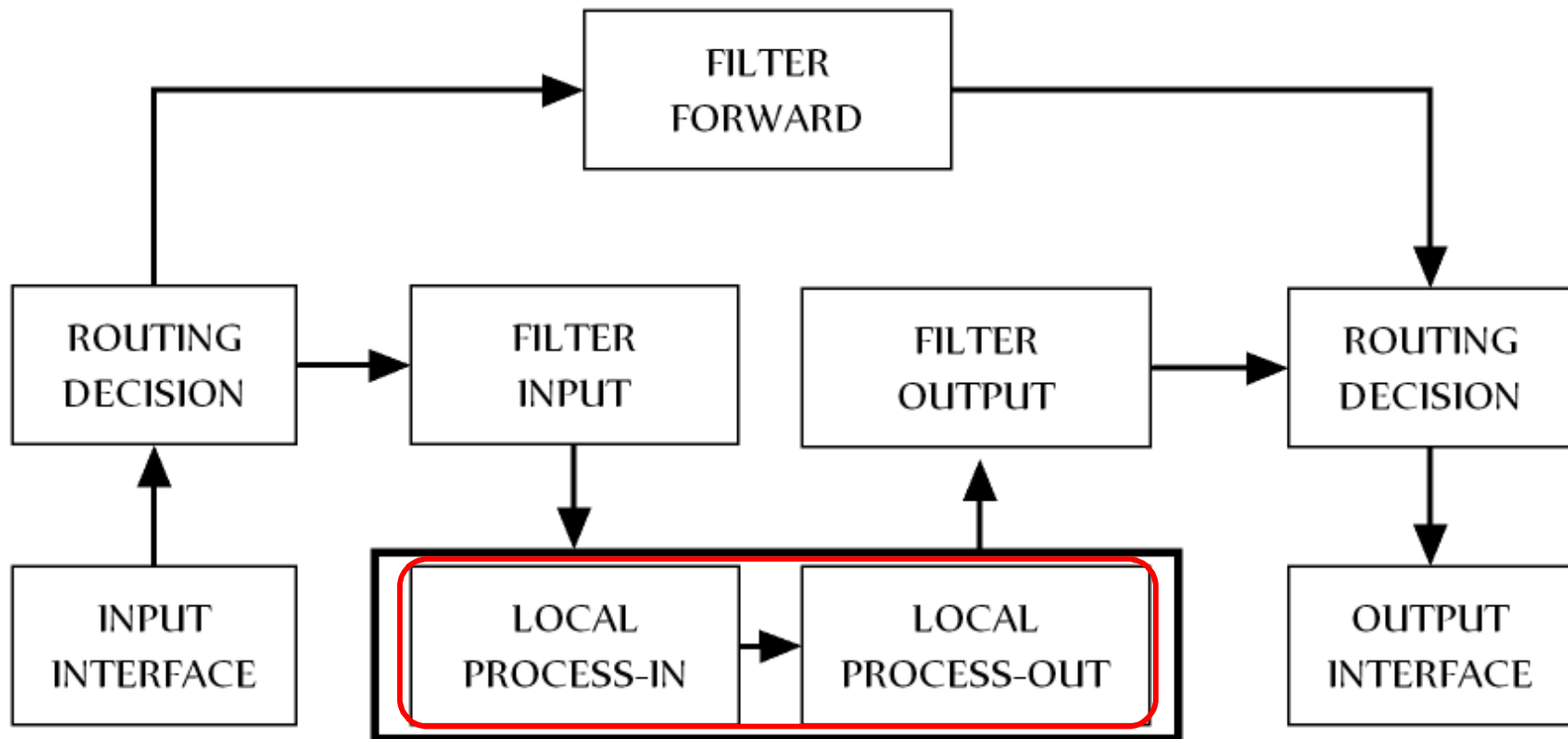
ROUTING DECISION

- Adalah proses yang menentukan apakah paket data yang masuk akan disalurkan ke luar router, atau menuju ke router itu sendiri



LOCAL PROCES

- Router itu sendiri, jika ada paket data yang menuju ke router atau berasal dari router



PARAMETER FIREWALL (ACTION)

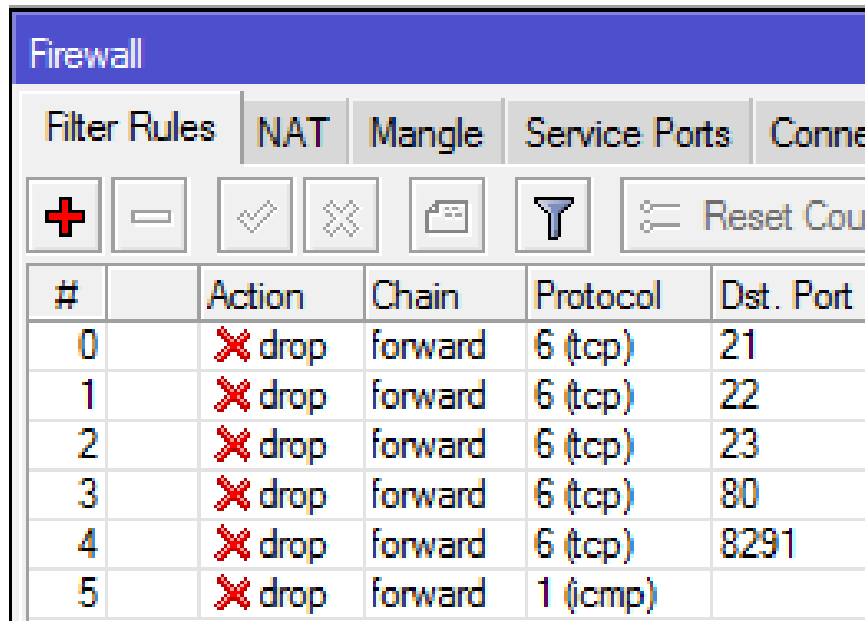
- **accept** , paket diterima
- **add-dst-to-address-list** , menambahkan IP Address tujuan ke dalam daftar **address-list**
- **add-src-to-address-list**, menambahkan IP Address asal ke dalam daftar **address-list**
- **drop**, menolak paket secara diam-diam (tidak mengirimkan pesan penolakan ICMP, timeout)

PARAMETER FIREWALL (ACTION)

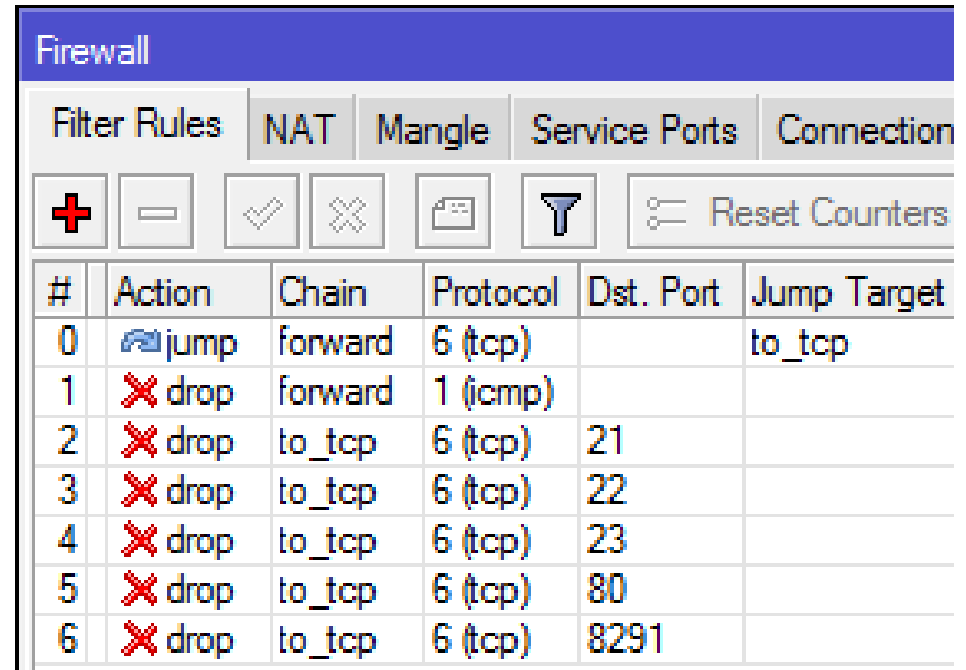
- **reject**, menolak paket dan mengirimkan pesan penolakan ICMP
- **log**, mencatat informasi di log
- **passthrough**, tidak melakukan action apapun, melanjutkan ke baris berikutnya
- **tarpit**, menahan koneksi TCP, tetap menjaga TCP connections yang masuk (membalas dengan SYN/ACK untuk paket TCP SYN yang masuk)

PARAMETER FIREWALL (ACTION)

- **jump**, berpindah ke chain lainnya sesuai **jump-target**, tanpa jump, paket input ICMP akan melewati 5 baris sebelum di drop



#	Action	Chain	Protocol	Dst. Port
0	✗ drop	forward	6 (tcp)	21
1	✗ drop	forward	6 (tcp)	22
2	✗ drop	forward	6 (tcp)	23
3	✗ drop	forward	6 (tcp)	80
4	✗ drop	forward	6 (tcp)	8291
5	✗ drop	forward	1 (icmp)	



#	Action	Chain	Protocol	Dst. Port	Jump Target
0	🔗 jump	forward	6 (tcp)		to_tcp
1	✗ drop	forward	1 (icmp)		
2	✗ drop	to_tcp	6 (tcp)	21	
3	✗ drop	to_tcp	6 (tcp)	22	
4	✗ drop	to_tcp	6 (tcp)	23	
5	✗ drop	to_tcp	6 (tcp)	80	
6	✗ drop	to_tcp	6 (tcp)	8291	

PARAMETER FIREWALL (ACTION)

- **return**, kembali ke chain sebelumnya sesudah melalui **jump**

chain=forward	chain=to_tcp
protocol=tcp, action=jump, target=to_tcp	protocol=tcp, dst-port=21, action=drop
protocol=icmp, action=drop	protocol=tcp, dst-port=22, action=drop
protocol=tcp, action=log	protocol=tcp, dst-port=23, action=drop
	protocol=tcp, dst-port=80, action=drop
	protocol=tcp, dst-port=8291, action=drop
	protocol=tcp, action=return

#	Action	Chain	Protocol	Dst. Port	Jump Target
0	jump	forward	6 (tcp)		to_tcp
1	drop	forward	1 (icmp)		
2	log	forward	6 (tcp)		
3	drop	to_tcp	6 (tcp)	21	
4	drop	to_tcp	6 (tcp)	22	
5	drop	to_tcp	6 (tcp)	23	
6	drop	to_tcp	6 (tcp)	80	
7	drop	to_tcp	6 (tcp)	8291	
8	return	to_tcp			

Jika tidak ada paket tcp yang sesuai dengan chain to_tcp, akan dikembalikan ke chain forward dan dicatat di log

FIREWALL FILTER INPUT

- Drop semua IP yang menuju router, kecuali 192.168.1.1,

Firewall

Filter Rules NAT Mangle Service Ports

#	Action	Chain	Src. Address	Dst. Address
0	drop	input	!192.168.1.1	

Firewall Rule <!192.168.2.1>

General Advanced Extra Action Status

Chain: input

Src. Address: ! 192.168.1.1

Dst. Address:

Firewall

Filter Rules NAT Mangle Service Ports

#	Action	Chain	Src. Address	Dst. Address
0	drop	input	!192.168.1.1	

Firewall Rule <!192.168.2.1>

General Advanced Extra Action Status

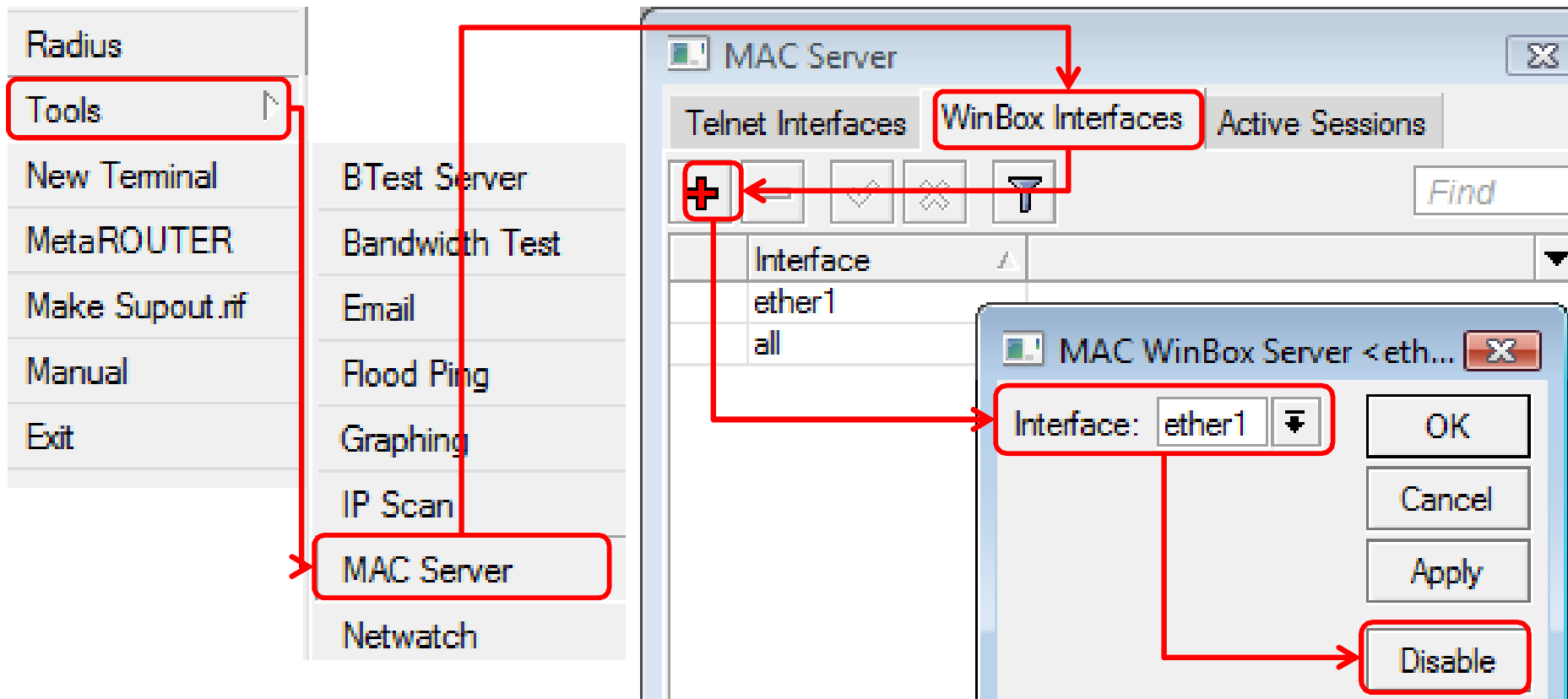
Action: drop

Log

Log Prefix:

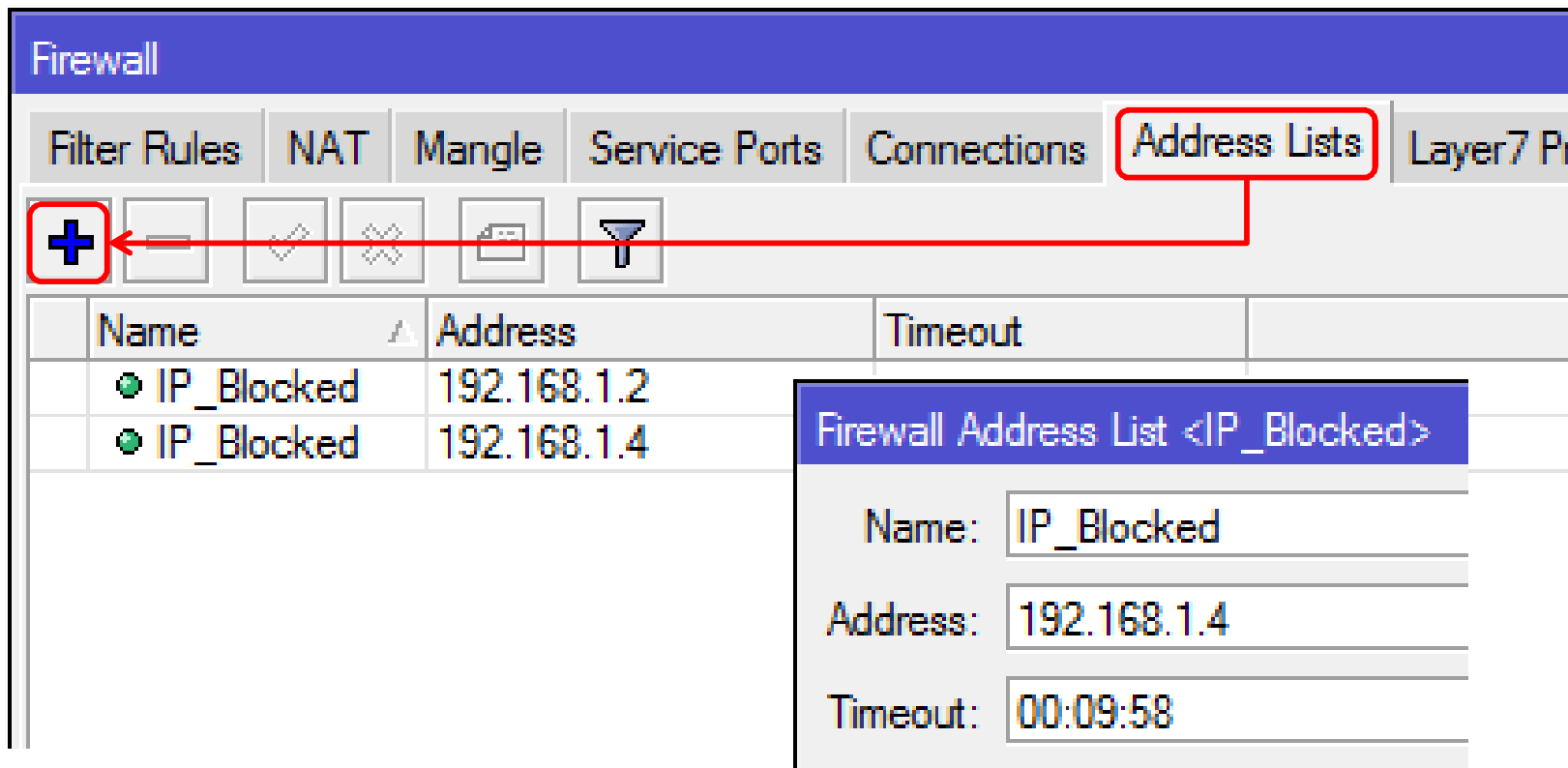
DISABLE MAC ADDRESS

- Firewall berlaku di Layer 3, login ke router masih dapat dilakukan melalui MAC Address, kecuali MAC Address di disable



ADDRESS LIST

- Address-list melakukan firewall action untuk sekelompok IP Address dengan dengan cara ditambahkan satu demi satu.



Firewall

Filter Rules NAT Mangle Service Ports Connections **Address Lists** Layer7 Pr

+ ←

Name	Address	Timeout
● IP_Blocked	192.168.1.2	
● IP_Blocked	192.168.1.4	

Firewall Address List <IP_Blocked>

Name: IP_Blocked

Address: 192.168.1.4

Timeout: 00:09:58

IMPLEMENTASI ADDRESS LIST

New Firewall Rule

General Advanced Extra Action Statistics

Chain: input

Src. Address:

New Firewall Rule

General Advanced Extra Action Statistics

Src. Address List: IP_Blocked

Firewall Rule <>

General Advanced Extra Action Statistics

Action: drop

FIREWALL FILTER FORWARD

Mengatur trafik yang melalui router.

The screenshot shows the Mikrotik WinBox Firewall Filter configuration interface. The 'Filter Rules' tab is active. Below the main menu, there are several icons for adding, deleting, and editing rules. A table below shows the current filter rules. A 'New Firewall Rule' dialog box is open, showing the 'General' tab. The 'Chain' is set to 'forward' and the 'Src. Address' is set to '192.168.1.1'. The 'Dst. Address' field is empty.

#	Action	Chain	Src. Address	Dst. Address
0	drop	forward	192.168.1.1	

New Firewall Rule

General Advanced Extra Action

Chain: forward

Src. Address: 192.168.1.1

Dst. Address:

The screenshot shows the Mikrotik WinBox Firewall Filter configuration interface. The 'Filter Rules' tab is active. Below the main menu, there are several icons for adding, deleting, and editing rules. A table below shows the current filter rules. A 'Firewall Rule <192.168.1.1>' dialog box is open, showing the 'Action' tab. The 'Action' is set to 'drop'.

#	Action	Chain	Src. Address	Dst. Address
0	drop	forward	192.168.1.1	

Firewall Rule <192.168.1.1>

General Advanced Extra Action Statistics

Action: drop

FIREWALL FILTER OUTPUT

Mengatur trafik yang keluar dari router.

Firewall

Filter Rules NAT Mangle Service Ports

+ - ✓ ✗ [icon] [icon] Res

#	Action	Chain	Src. Address
---	--------	-------	--------------

New Firewall Rule

General Advanced Extra Action Stat

Chain:

Src. Address:

Firewall

Filter Rules NAT Mangle Service Ports Conn

+ - ✓ ✗ [icon] [icon] Reset Cou

#	Action	Chain	Src. Address
0	✗ drop	output	10.10.10.1

Firewall Rule <10.10.10.1>

General Advanced Extra Action Statistics

Action:

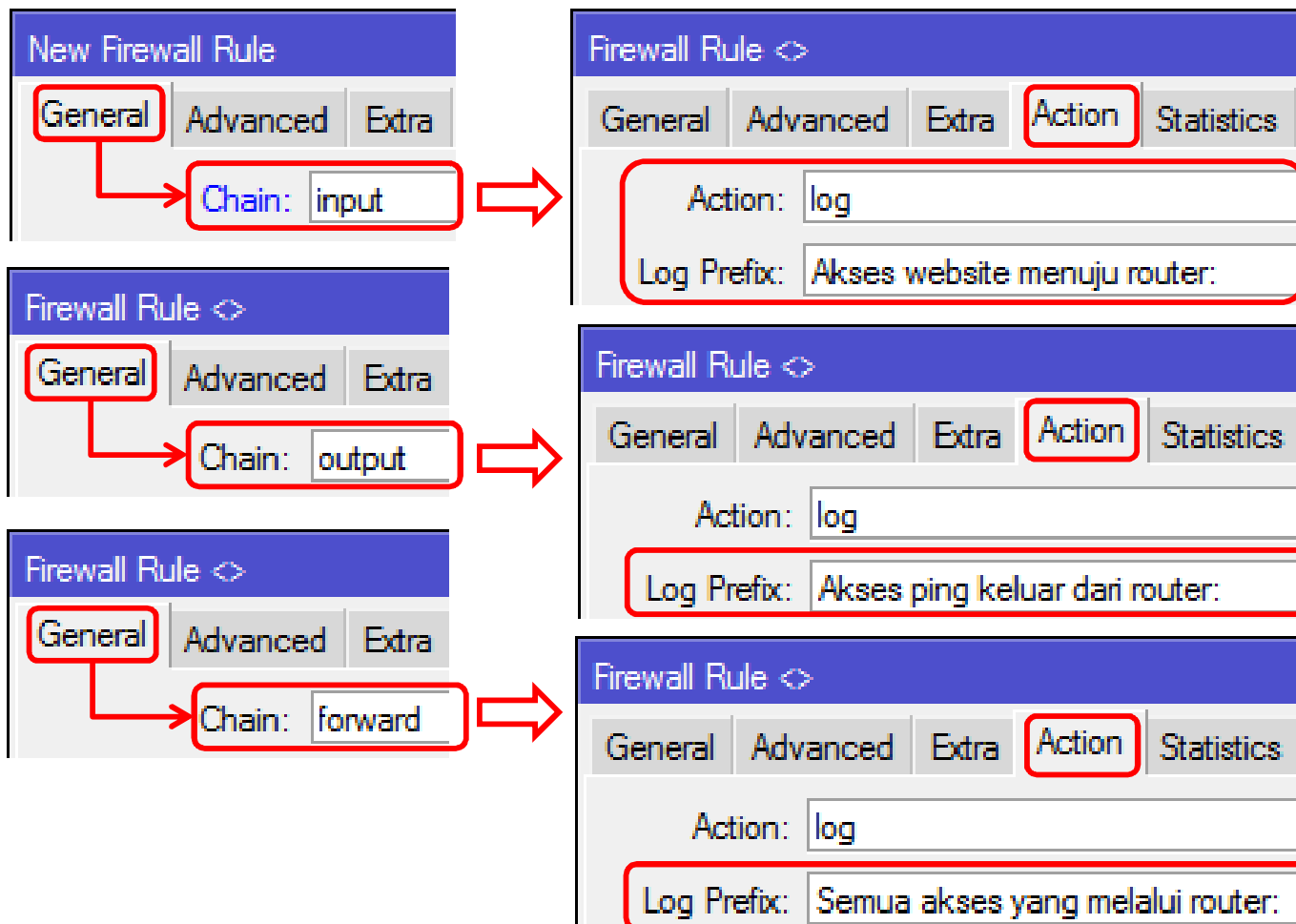
FIREWALL FILTER OUTPUT

The screenshot shows the Mikrotik WinBox Ping tool interface. The 'General' tab is active, and the 'Ping To' field is set to '10.10.10.100'. The 'Interface' is set to 'any', and the 'Timeout' is set to '1000 ms'. The 'Packet Count' is set to '1'. The 'ARP Ping' checkbox is unchecked. The 'Ping' button is highlighted with a red box, and a red arrow points from the 'Ping To' field to it. The 'Stop', 'Close', and 'New Window' buttons are also visible.

#	Host	Time	Reply Size	TTL	Status
2	10.10.10.100	timeout			packet rejected
3	10.10.10.100	timeout			packet rejected
4	10.10.10.100	timeout			packet rejected

FIREWALL LOG

- Mencatat aktifitas yang menuju router, melalui router dan keluar dari router



SYSLOG

Logging

Rules **Actions**

+ - Filter

Name	Type
* disk	disk
* echo	echo
* memory	memory
* remote	remote

Log Action <remote>

Name: remote

Type: remote

Remote Address: 192.168.1.1

Remote Port: 514

Src. Address: 192.168.1.254

BSD Syslog

Logging

Rules Actions

+ - ✓ ✗ Filter

	Topics	Prefix	Action
* critical			echo
* error			memory
* info	LogInfo		remote
* warning			memory

Log Rule <info>

Topics: info

Prefix: LogInfo

Action: remote

MikroTik Syslog Daemon

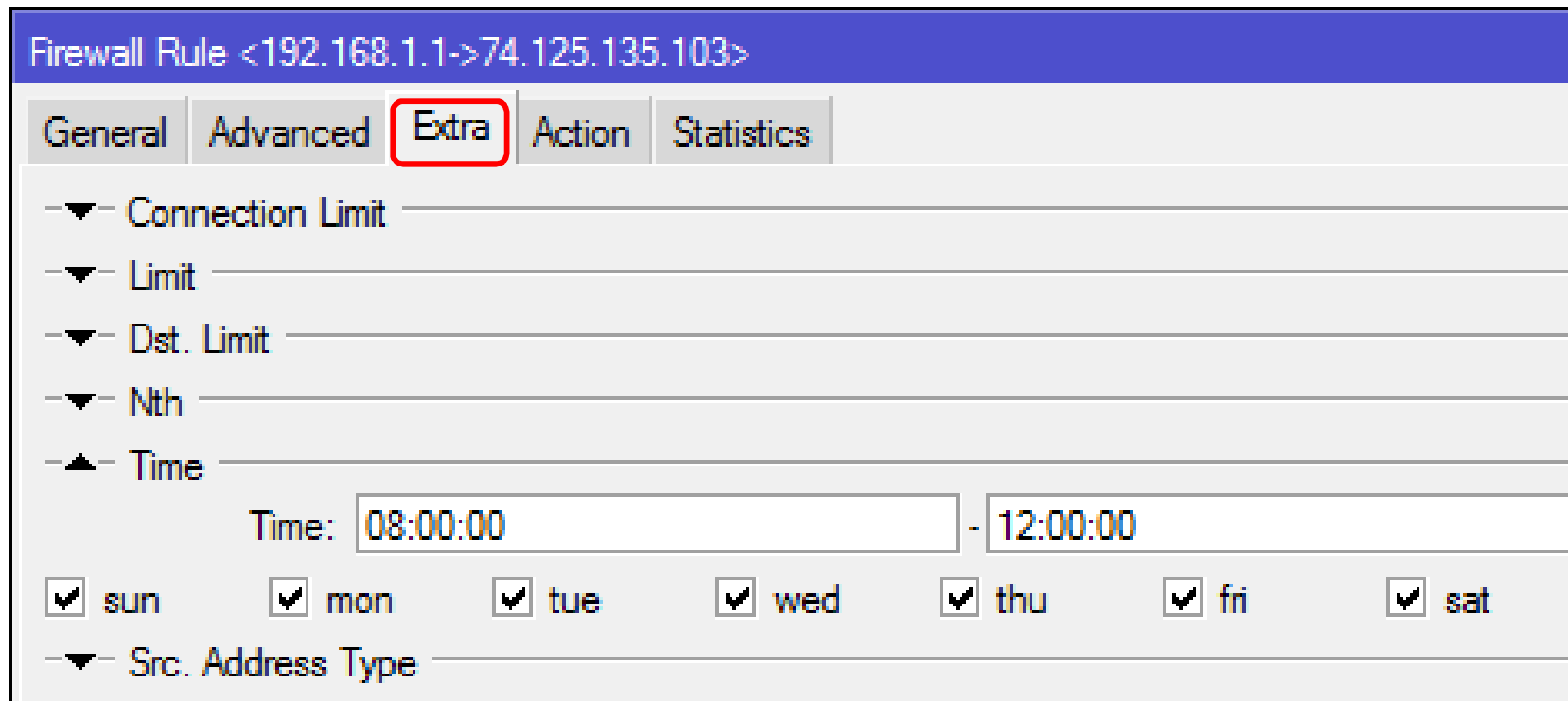
File Options Help

Time	Message	IP
8-Jul 14:29:39.74	system,info LogInfo: log rule changed by admin	192.168.1.254
8-Jul 14:29:50.38	system,info LogInfo: device changed by admin	192.168.1.254
8-Jul 14:29:52.39	system,info LogInfo: device changed by admin	192.168.1.254
8-Jul 14:30:6.18	system,info LogInfo: address added by admin	192.168.1.254
8-Jul 14:30:12.76	system,info LogInfo: device changed by admin	192.168.1.254

..... Main queue

FIREWALL FILTER (Extra)

- Aturan di firewal filter hanya berlaku di waktu yang ditentukan



Firewall Rule <192.168.1.1->74.125.135.103>

General Advanced **Extra** Action Statistics

-▼ Connection Limit _____

-▼ Limit _____

-▼ Dst. Limit _____

-▼ Nth _____

-▲ Time _____

Time: -

sun mon tue wed thu fri sat

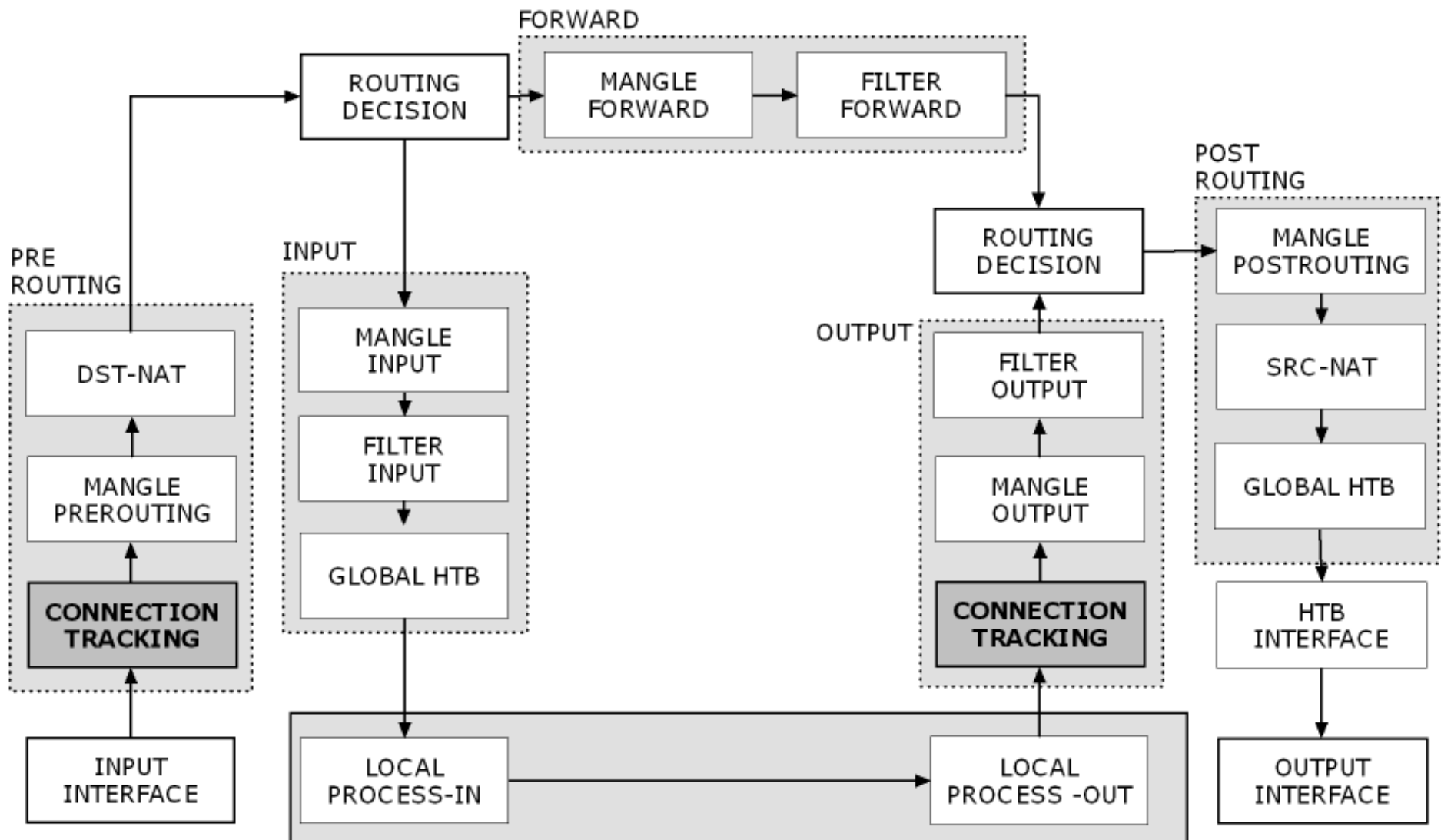
-▼ Src. Address Type _____

Firewall akan aktif setiap hari mulai pukul 08.00 - 12.00

CONNECTION TRACKING

- Connection Tracking, mengelola semua aktivitas koneksi di dalam router
- Mendisable connection tracking, router akan kehilangan fungsi Firewall Filter, NAT & Mangle
- Connection tracking menggunakan banyak sumber daya CPU, kita bisa mendisable jika tidak menggunakan firewall

CONNECTION TRACKING



CONNECTION TRACKING

Firewall

Filter Rules NAT Mangle Service Ports **Connections** Address Lists Layer7 Protocol

Tracking

	Src. Address	^	Dst. Address	Protocol	Timeout	TCP State
	10.10.10.1:44496		10.8.17.4:53	17 (udp)	00:00:10	
	10.10.10.1:44918		10.8.17.4:53	17 (udp)	00:00:13	
	10.10.10.1:45283		10.8.17.4:53	17 (udp)	00:00:12	
	10.10.10.1:51811		10.8.17.4:53	17 (udp)	00:00:12	
	10.10.10.1:58672		10.8.17.4:53	17 (udp)	00:00:12	
	192.168.1.1		174.120.70.144	1 (icmp)	00:00:06	
	192.168.1.1:49655		192.168.1.254:53	17 (udp)	00:00:12	
A	192.168.1.1:49976		63.245.217.112:443	6 (tcp)	00:00:08	close
A	192.168.1.1:49980		199.7.48.72:80	6 (tcp)	23:59:40	established
A	192.168.1.1:49982		199.7.48.72:80	6 (tcp)	23:59:41	established
A	192.168.1.1:49988		199.7.54.72:80	6 (tcp)	23:59:41	established
A	192.168.1.1:49990		199.7.54.72:80	6 (tcp)	23:59:41	established
A	192.168.1.1:50004		67.227.176.121:80	6 (tcp)	1d 00:00:00	established
A	192.168.1.1:50006		67.227.176.121:80	6 (tcp)	1d 00:00:00	established
A	192.168.1.1:50008		82.98.86.163:80	6 (tcp)	00:00:12	time wait
A	192.168.1.1:50010		82.98.86.163:80	6 (tcp)	1d 00:00:02	established
A	192.168.1.1:50012		74.125.135.156:80	6 (tcp)	1d 00:00:03	established
A	192.168.1.1:50014		74.125.135.156:80	6 (tcp)	1d 00:00:03	established

Connection Tracking

Enabled

TCP Syn Sent Timeout: 00:00:05

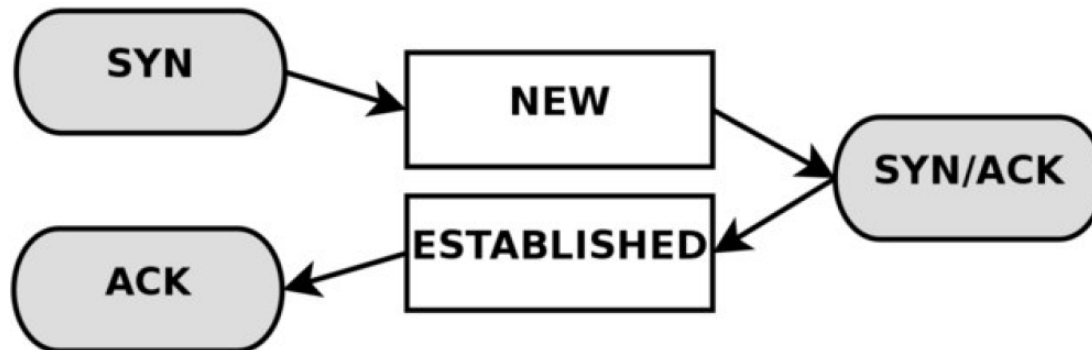
TCP Syn Received Timeout: 00:00:05

state of TCP connection :

- "established"
- "time-wait"
- "close"
- "syn-sent"
- "syn-received"

CONNECTION STATE

- Connection State, status yang diberikan setiap paket oleh connection tracking
 - **New**, paket yang merupakan pembuka sebuah koneksi/paket pertama dari sebuah koneksi (paket SYN dalam koneksi TCP)
 - **Established**, paket kelanjutan dari paket new (paket SYN/ACK dalam koneksi TCP)

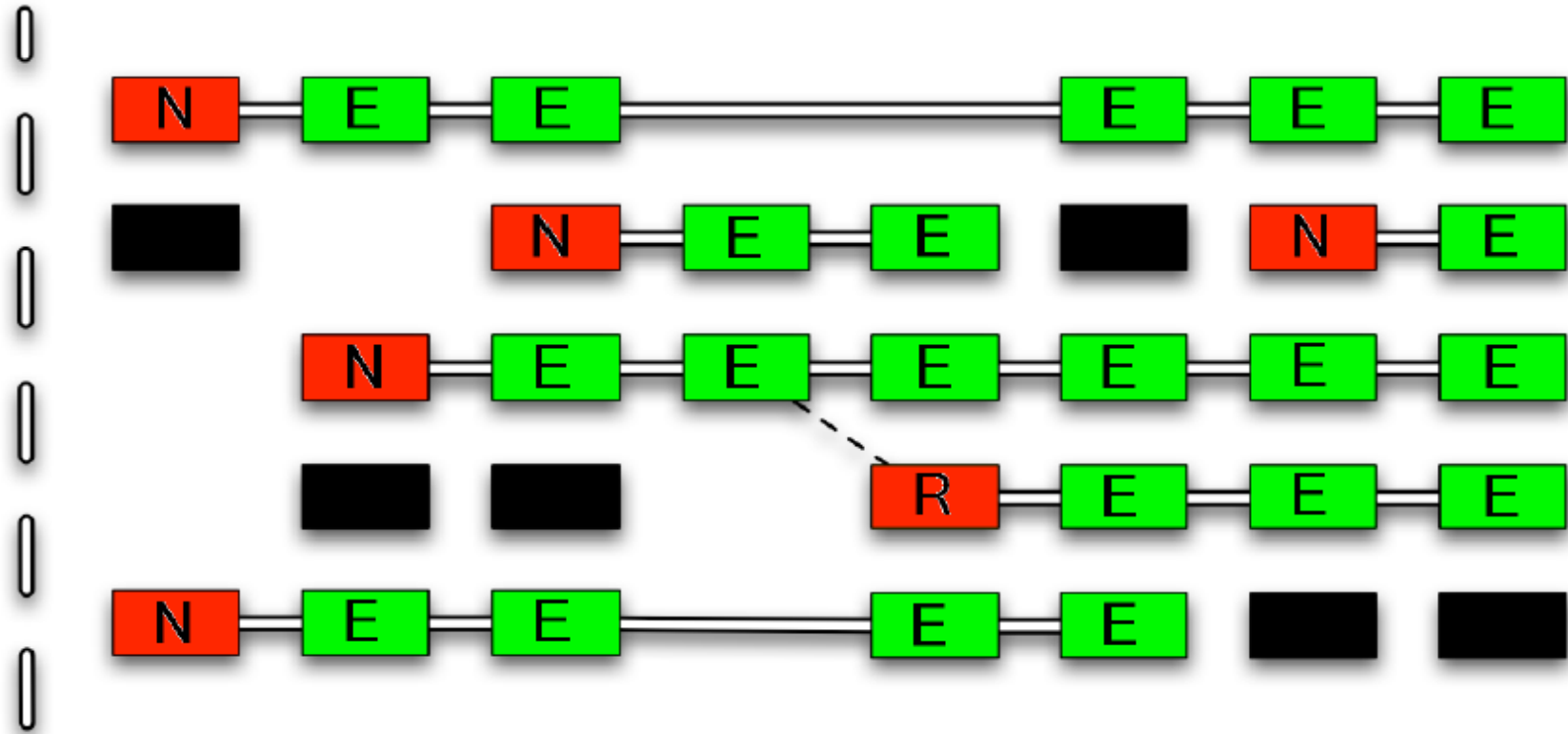


CONNECTION STATE

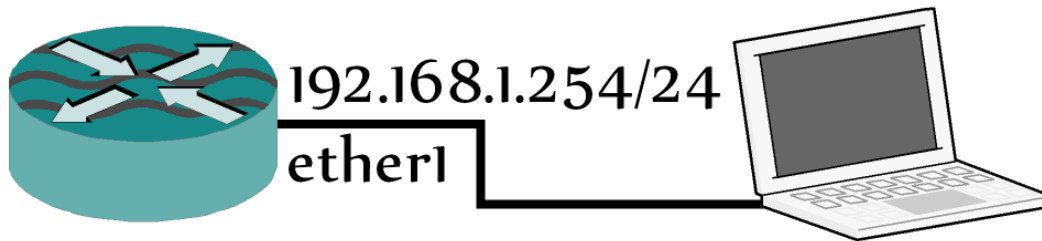
- **Related**, paket yang masih berhubungan dengan koneksi sebelumnya (FTP), connection state dianggap related apa bila sudah terjadi established terlebih dahulu
- **Invalid**, paket tidak dapat diidentifikasi dan tidak dimiliki oleh koneksi apapun, tidak berguna
- Connection State \neq TCP State

CONNECTION STATE

Firewall



CONNECTION STATE



Firewall				
Filter Rules				
NAT				
Mangle				
Service Ports				
Connections				
+	-	✓	✗	📄
🔍	🔧	Reset Count		
#	Action	Chain	Protocol	Connection State
0	✗ drop	input	1 (icmp)	

Firewall akan **drop** akses ICMP, PC ke router dan router ke PC

Firewall				
Filter Rules				
NAT				
Mangle				
Service Ports				
Connections				
+	-	✓	✗	📄
🔍	🔧	Reset Count		
#	Action	Chain	Protocol	Connection State
0	✓ accept	input	1 (icmp)	established
1	✗ drop	input	1 (icmp)	

Firewall akan **drop** akses ICMP, PC ke router, tetapi **accept** router ke PC

CONNECTION STATE

- Firewall filter, sebaiknya selalu diawali aturan:
 - connection-state= invalid → drop
 - connection-state=related → accept
 - connection-state=established → accept
 - connection state=new, proses rule selanjutnya
- Rule seperti ini akan sangat menghemat resources router, karena proses filtering hanya dilakukan pada saat connection dimulai (connection-state=new)

QoS

QOS

- QOS mengatur penggunaan bandwidth dan prioritas, dilakukan melalui **Simple Queue** atau **Queue Tree**

SIMPLE QUEUE

Queue List

Simple Queues | Interface Queues | Queue Tree | Queue Types

+ - ✓ ✗ [Filter Icon] [Reset Counters] [Reset All Counters]

#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks
0	queue1	192.168.1.1	256k	512k	

Simple Queue <queue1>

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

Name: queue1

Target: 192.168.1.1

Dst.: [Dropdown]

Target Upload: Max Limit: 256k

Target Download: Max Limit: 512k bits/s

Limitasi bandwidth Upload 256k, download 512k

SIMPLE QUEUE

Queue List

Simple Queues | Interface Queues | Queue Tree | Queue Types

+ - ✓ ✕ 🗑️ 🏠 ⚙️ Reset Counters 00 Reset All Counters

#	Name	Target	Upload Max Limit	Download Max Limit	Total Max Limit (bits/s)
0	queue1	192.168.1.1	256k	512k	
1	queue2	192.168.1.2	unlimited	unlimited	1M

Simple Queue <queue2>

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

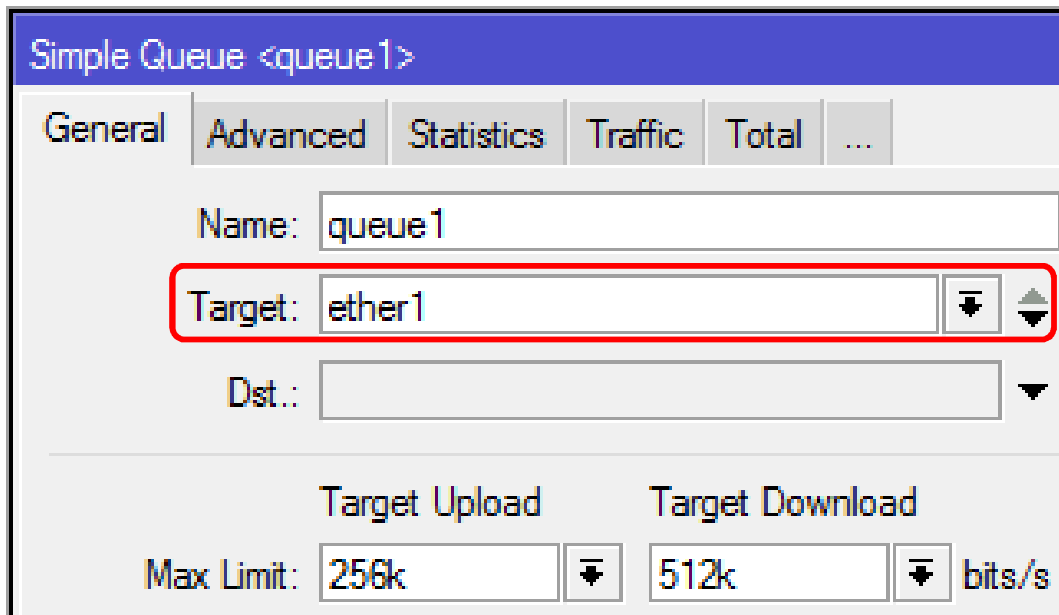
Total Limit At: ▼ bits/s

Total Max Limit: ▲ bits/s

Limitasi bandwidth Total: upload + download = 1M

SIMPLE QUEUE

- Pembatasan bisa diterapkan di interface router, yang berarti semua klien yang melewati interface tersebut, akan terkena pengaturan bandwidth yang sama.

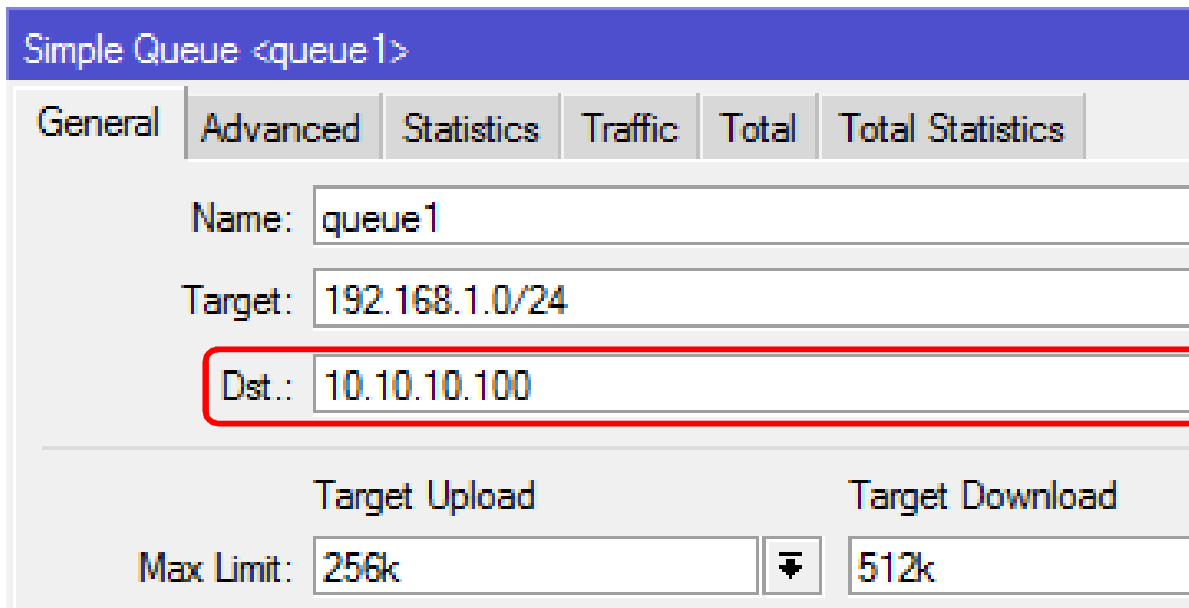


The screenshot shows the Mikrotik Simple Queue configuration window for a queue named 'queue1'. The 'General' tab is selected. The 'Name' field is 'queue1'. The 'Target' field is 'ether1', which is highlighted with a red rectangle. Below it is the 'Dst.' field. At the bottom, there are two sections: 'Target Upload' with a 'Max Limit' of '256k' and 'Target Download' with a 'Max Limit' of '512k', both in 'bits/s'.

Field	Value
Name	queue1
Target	ether1
Dst.	
Target Upload Max Limit	256k bits/s
Target Download Max Limit	512k bits/s

SPEKIFIK SIMPLE QUEUE

- Pembatasan yang lebih spesifik bisa dilakukan, berdasarkan IP Address tujuan



Simple Queue <queue1>

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

Name: queue1

Target: 192.168.1.0/24

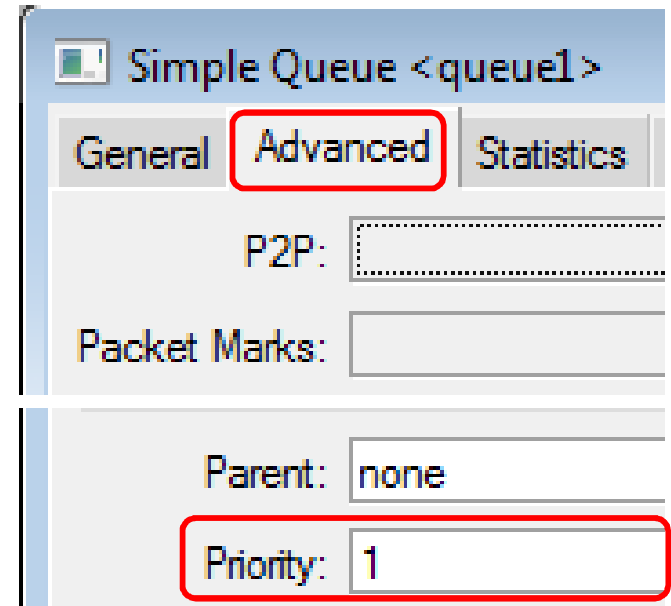
Dst.: 10.10.10.100

Target Upload: 256k

Target Download: 512k

PRIORITY

- Pengaturan proritas (1 sd 8), jika terdapat beberapa klien yang dibatasi bandwidthnya, nilai 1 lebih diprioritaskan daripada nilai 8



GRAPH

- Graph menampilkan rata-rata penggunaan traffic untuk jangka waktu tertentu, diakses melalui browser (port 80)
http://IP_Router/graphs/
- Hasil Queue bisa ditampilkan melalui graph

GRAPH

The image shows the Mikrotik WinBox interface. On the left is a menu with 'Tools' and 'Graphing' highlighted. The main window is titled 'Graphing' and has tabs for 'Queue Graphs', 'Interface Graphs', 'Resource Graphs', 'Queue Rules', and 'Interface Rules'. The 'Queue Rules' tab is active, showing a table with columns for 'Simple Queue', 'Allow Address', 'Store on D...', and 'Allow Target'. A table entry is shown with 'SimpleQueue', '0.0.0.0/0', 'yes', and 'yes'. A 'Queue Graphing Rule <Simple' dialog box is open, showing configuration for 'Simple Queue: SimpleQueue', 'Allow Address: 0.0.0.0/0', and checked options for 'Store on Disk' and 'Allow Target'. Red arrows indicate the flow from the menu to the 'Queue Rules' tab and then to the configuration dialog.

Simple Queue	Allow Address	Store on D...	Allow Target
SimpleQueue	0.0.0.0/0	yes	yes

Queue Graphing Rule <Simple

Simple Queue: SimpleQueue

Allow Address: 0.0.0.0/0

Store on Disk

Allow Target

STAGED LIMITATION

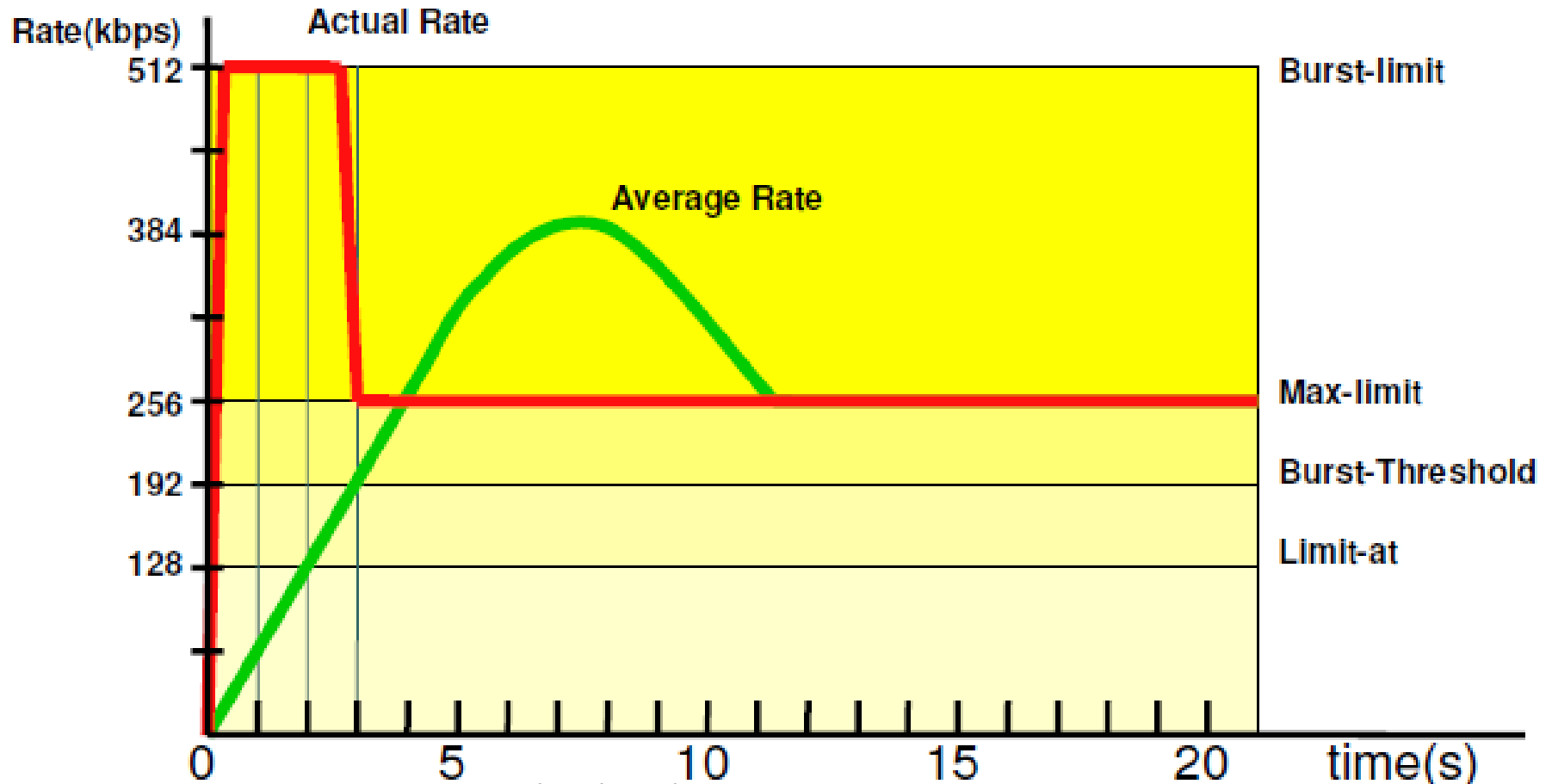
- Pada RouterOS, dikenal 2 buah limit:
 - CIR (Committed Information Rate)
Klien dijamin mendapatkan bandwidth sesuai dengan “**limit-at**”
 - MIR (Maximal Information Rate)
Klien bisa mendapatkan bandwidth tambahan hingga “**max-limit**”

BURST

- 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**
- **Burst time** digunakan untuk menghitung rata-rata data rate.

BURST

Limit-at=128kbps, max-limit=256kbps, burst-time=8, burst-threshold=192kbps, burst-limit=512kbps.



BURST

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

BURST - SIMPLE QUEUE

Simple Queue <QueueBurst>

General Advanced Statistics Traffic Total ...

Name: QueueBurst

Target: 192.168.1.1

Dst.:

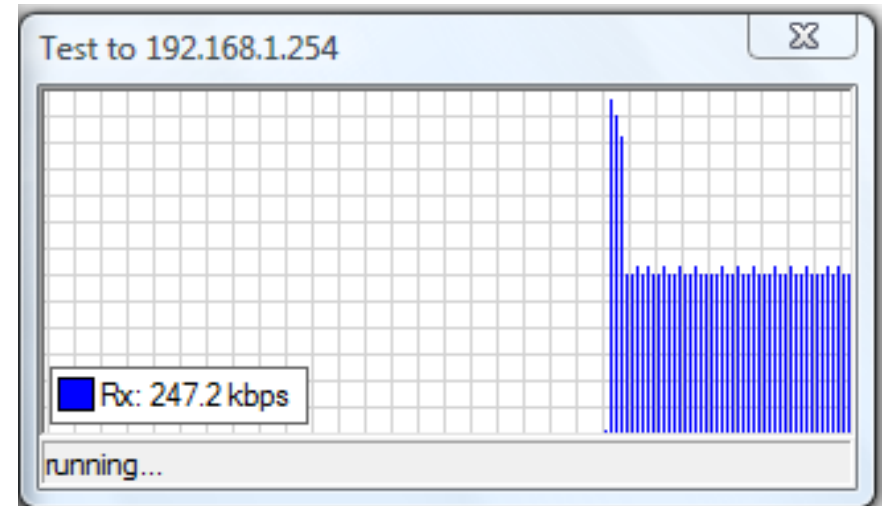
	Target Upload	Target Downlo
Max Limit:	unlimited	256k
Burst Limit:	unlimited	512k
Burst Threshold:	unlimited	192k
Burst Time:	0	8

Simple Queue <QueueBurst>

General Advanced Statistics Traffic Total ...

Packet Marks:

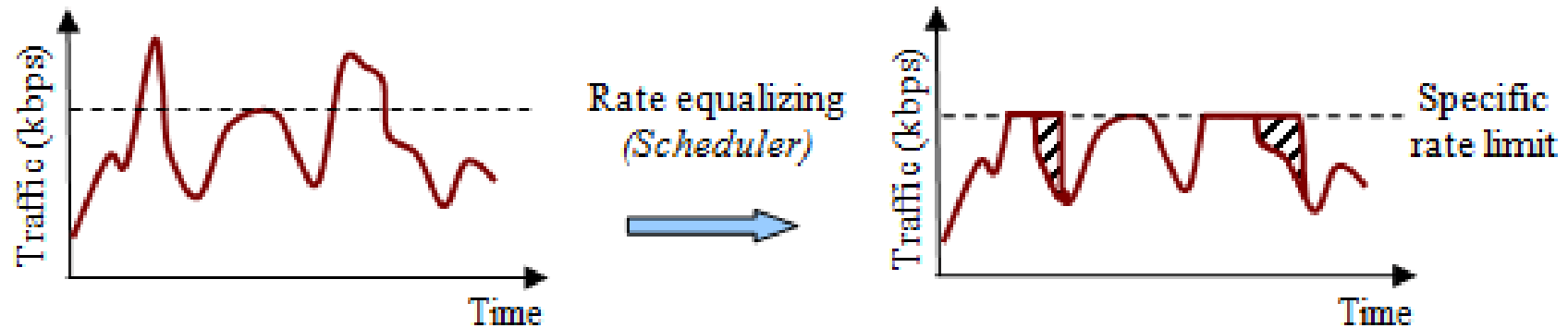
	Target Upload	Target Downlo
Limit At:	unlimited	128k
Priority:	8	8



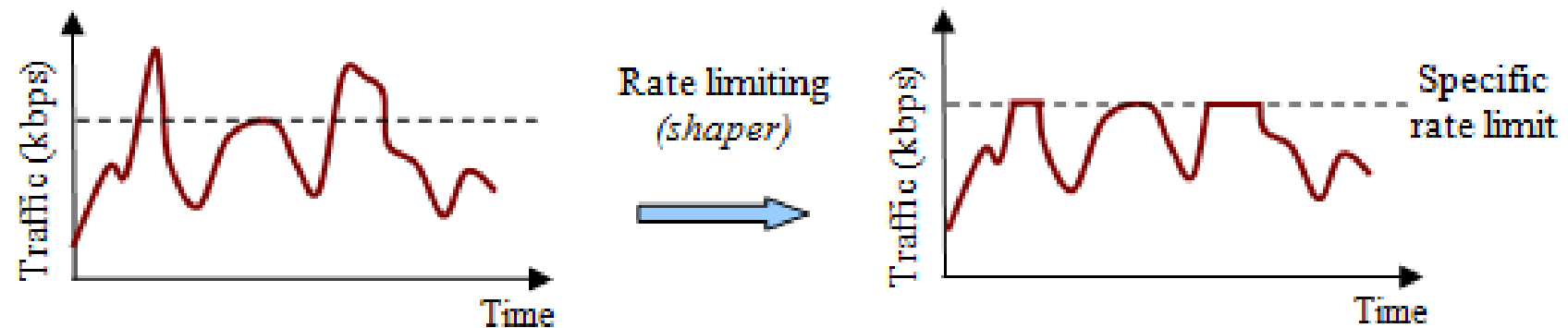
QUEUE TYPE

Queue Type dapat dibedakan menjadi 2:

(1) Scheduler queues (BFIFO, PFIFO, RED, SFQ)

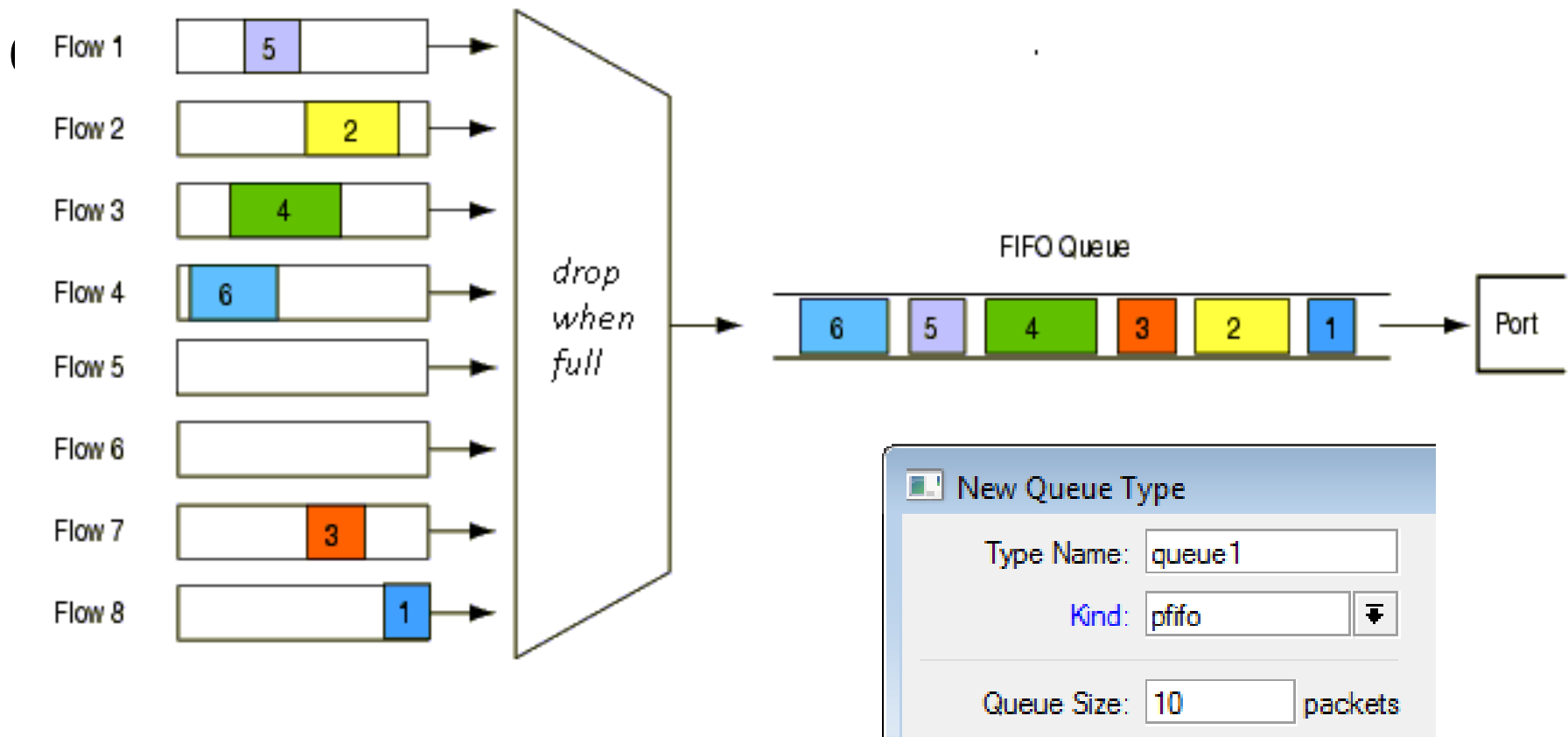


(2) Shaper queues (PCQ & HTB)



PFIFO & BFIFO

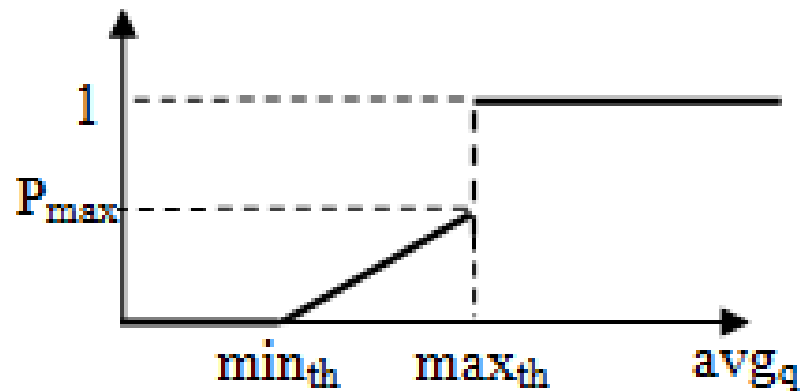
- FIFO mengirimkan paket berdasarkan waktu kedatangannya, parameter queue size menentukan jumlah data yang bisa diantri



RED

- RED melihat trafik rata-rata

Probability (P_d)



$avg_q \leq min_{th}$ – no dropped packets

$avg_q \geq max_{th}$ – dropped all packets

$min_{th} \leq avg_q \leq max_{th}$ – packets are dropped with probability P_d

New Queue Type

Type Name:

Kind:

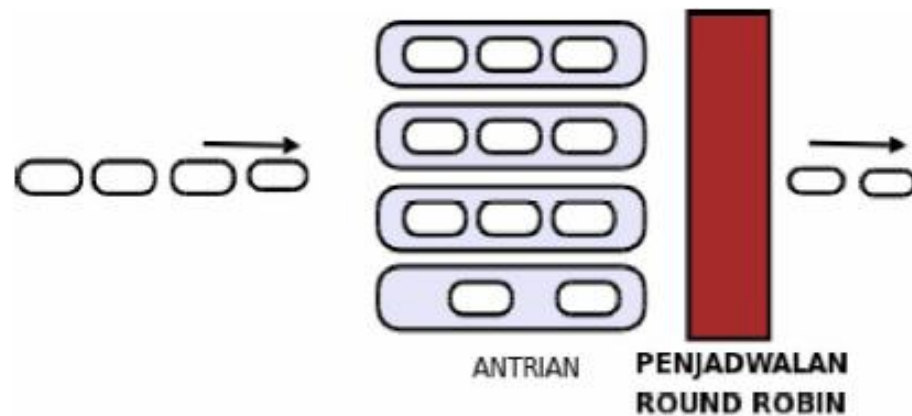
Queue Size: packets

Min Threshold: packets

Max Threshold: packets

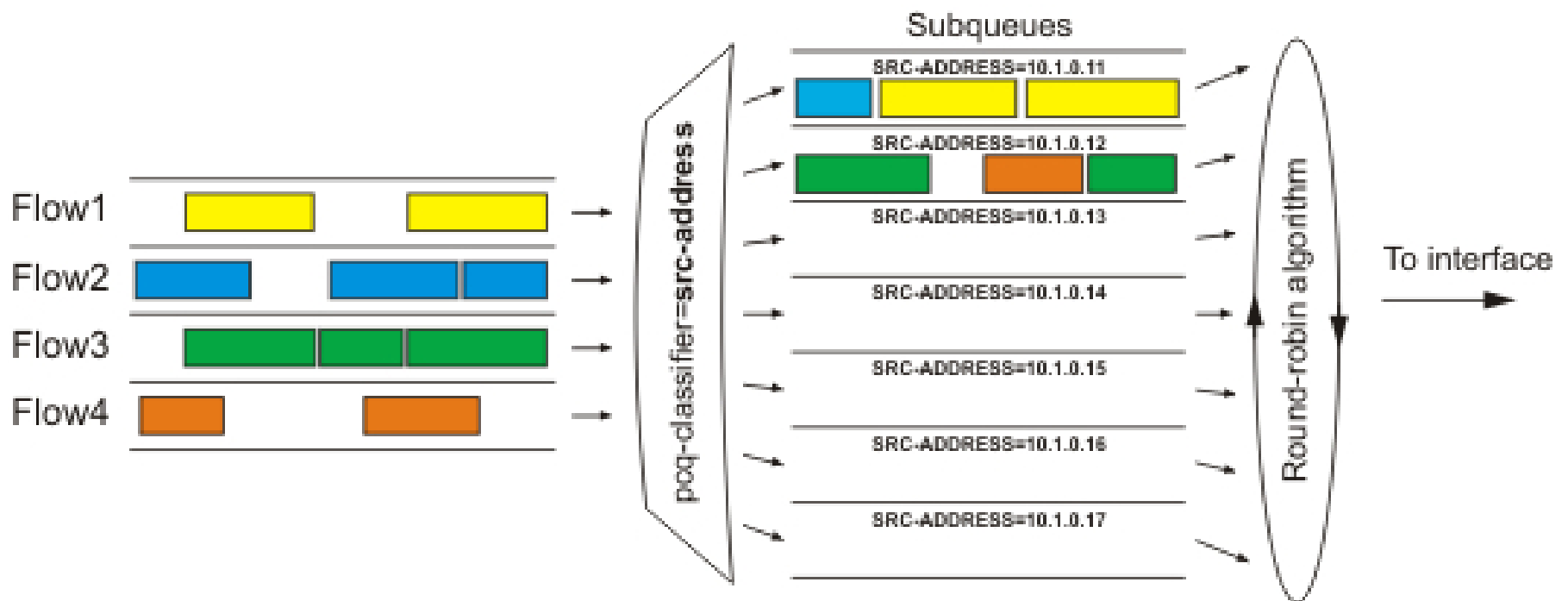
SFQ

- *Stochastic Fairness Queuing* membagi paket dalam ukuran yang sama besar kemudian memasukkan ke dalam beberapa antrian. Kemudian di keluarkan dengan algoritma round robin. SFQ dapat berisi 128 packets dan dapat menyediakan 1024 sub queue



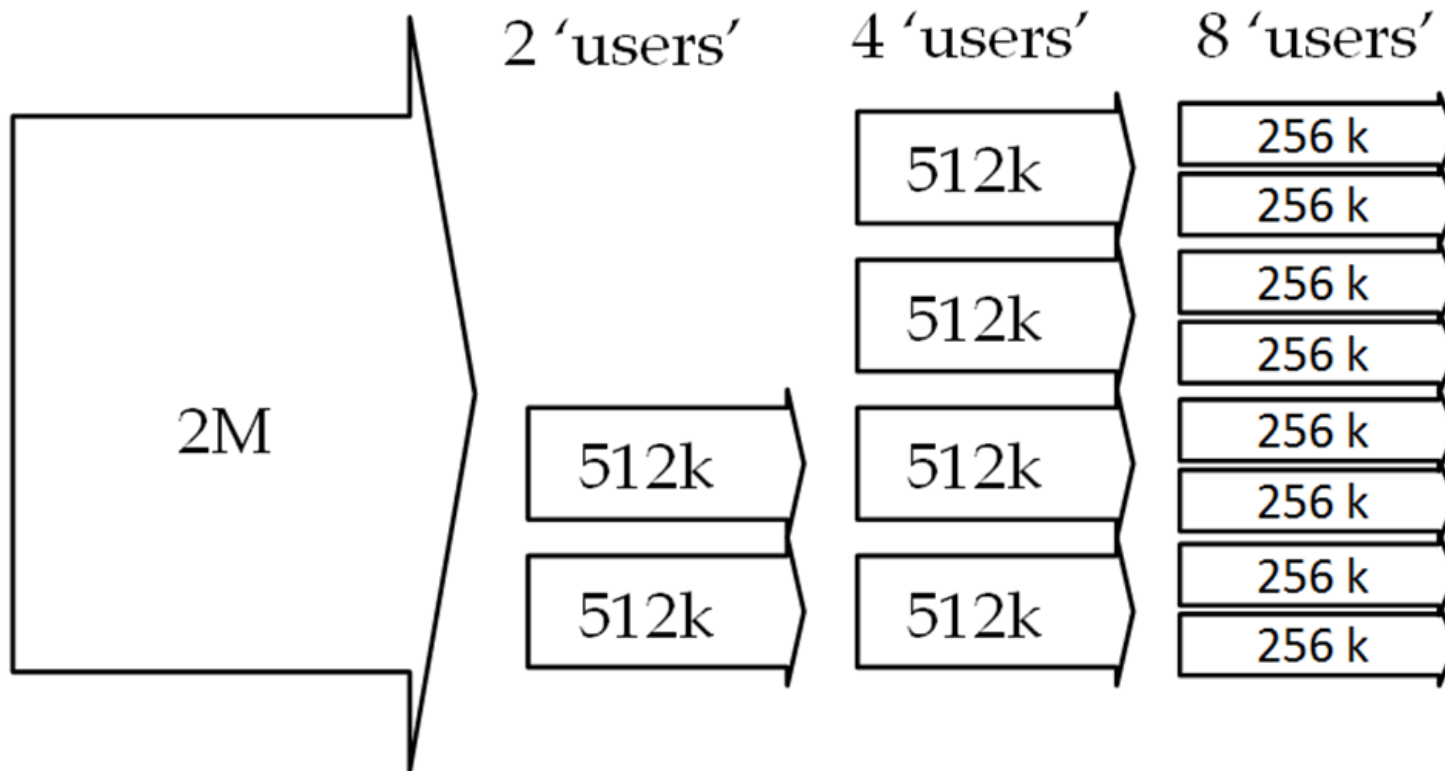
PCQ

- PCQ tidak membatasi jumlah sub-queue
- PCQ akan membuat sub-queue, berdasarkan parameter **pcq-classifier**, yaitu: *src-address*, *dst-address*, *src-port*, *dst-port*



PCQ

- PCQ dapat digunakan untuk menyamakan penggunaan bandwidth bagi setiap user



PCQ

Queue List

Simple Queues Interface Queues Queue Tree **Queue Types**

+ **-** **Y**

Type Name	Kind
PCQ_Download	pcq



Queue Type <PCQ_Download>

Type Name: PCQ_Download

Kind: pcq

Rate: 512k

Limit: 50

Total Limit: 2000

Burst Rate:

Burst Threshold:

Burst Time: 00:00:10

- Classifier -

Src. Address **Dst. Address**

Src. Port Dst. Port

Classifier Dst. Address
digunakan untuk trafik
download, sedangkan untuk
trafik upload menggunakan
classifier **Src. Address**

PCQ

Simple Queue <queue1>

General Advanced Statistics Traffic Total Total Statistics

Name:

Target Upload Target Download

Max Limit:
 bits/s

Simple Queue <queue1>

General Advanced Statistics Traffic Total Total Statistics

Target Upload Target Download

Limit At: bits/s


Queue Type:

PCQ

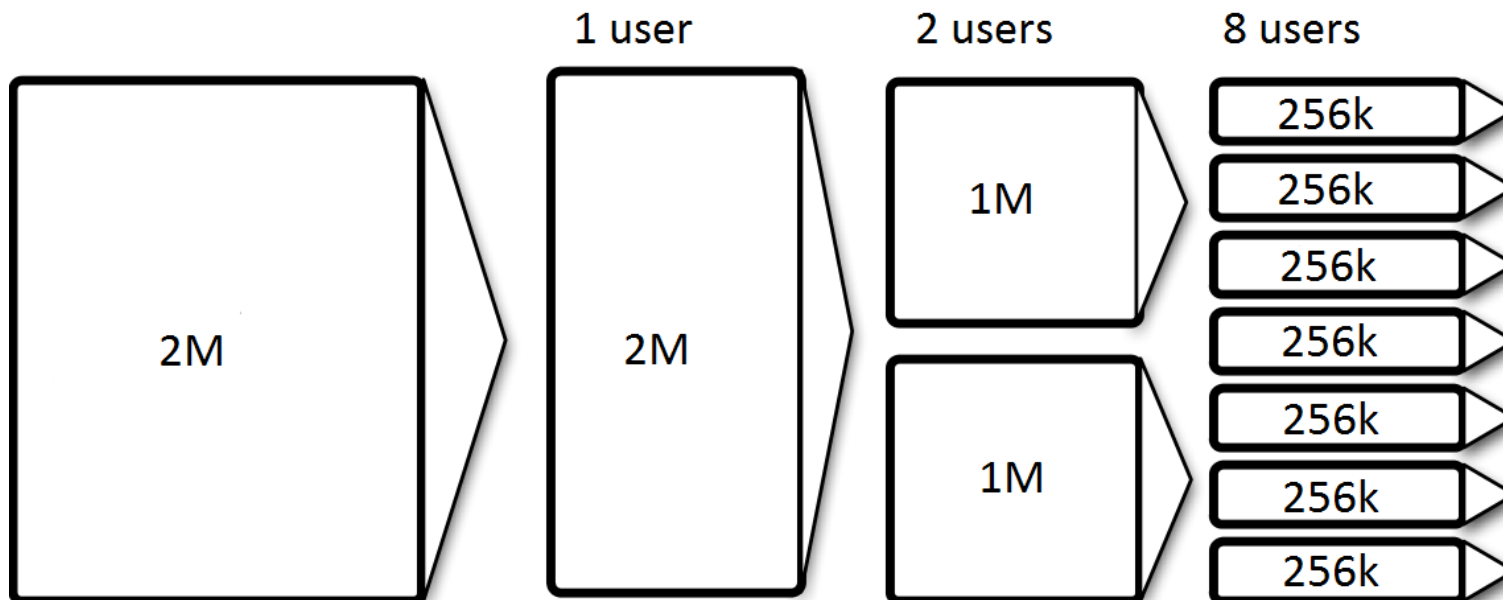
- PCQ membagi bandwidth merata bagi user aktif

Queue Type <PCQ_Download>

Type Name:

Kind: 

Rate:



TRAFFIC MONITOR

Radius

Tools

New Terminal

Traffic Generator

Traffic Monitor

Traffic Monitor List

Name	Interface	Traffic	Trigger	Threshold
tmon1	ether1	received	above	1500000

Traffic Monitor <tmon1>

Name: tmon1

Interface: ether1

Traffic: received

Trigger: above

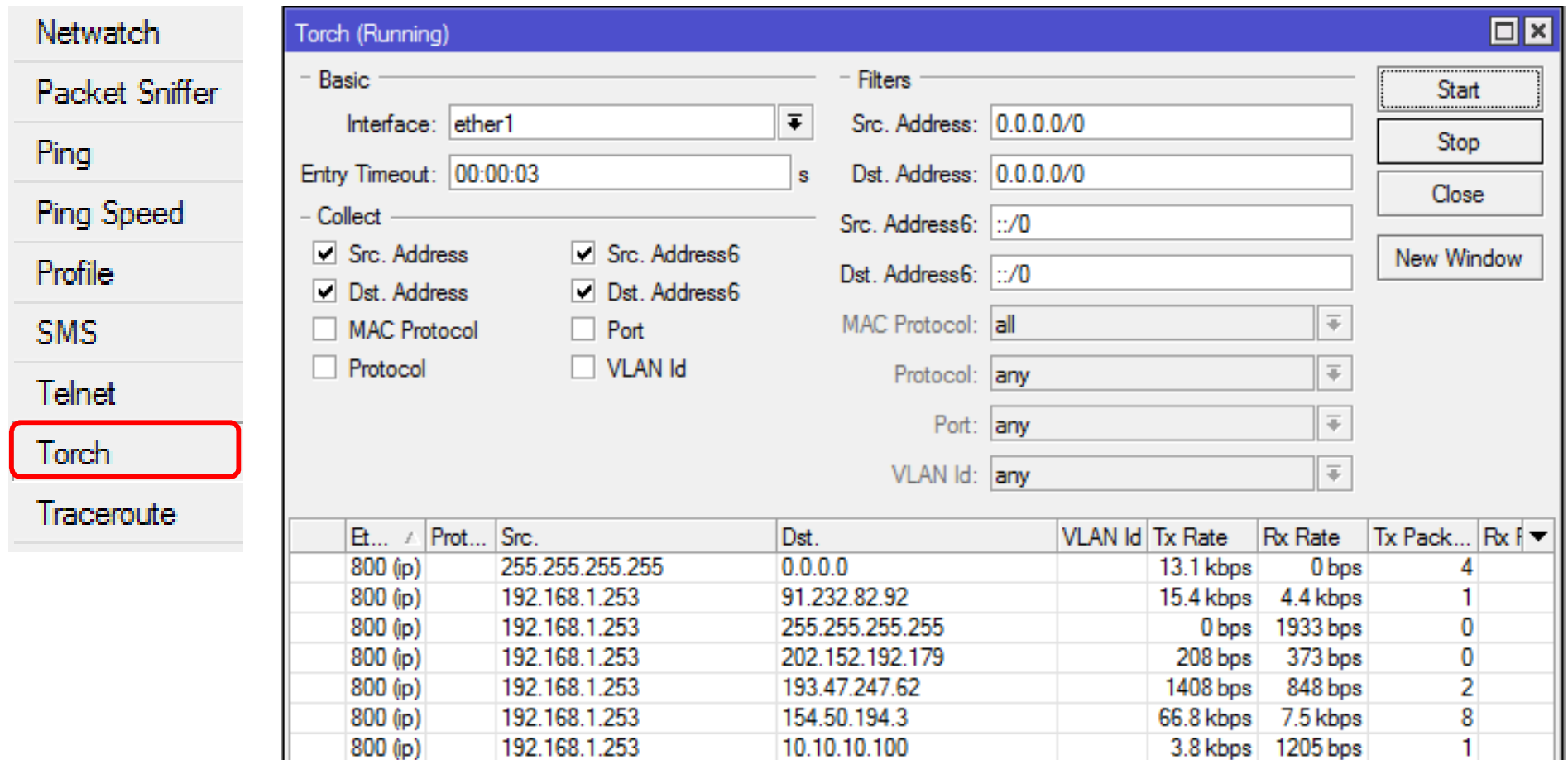
Threshold: 1500000

On Event:

```
:log info message="Awat trafik melampaui batas !!!"
```

TORCH

- Memeriksa trafik yang melalui interface



The screenshot displays the Mikrotik WinBox interface with the Torch (Running) window open. The left sidebar shows navigation options: Netwatch, Packet Sniffer, Ping, Ping Speed, Profile, SMS, Telnet, Torch (highlighted with a red box), and Traceroute.

The Torch (Running) window is divided into several sections:

- Basic:** Interface: ether1, Entry Timeout: 00:00:03 s.
- Collect:** Src. Address, Dst. Address, MAC Protocol, Protocol, Src. Address6, Dst. Address6, Port, VLAN Id.
- Filters:** Src. Address: 0.0.0.0/0, Dst. Address: 0.0.0.0/0, Src. Address6: ::/0, Dst. Address6: ::/0, MAC Protocol: all, Protocol: any, Port: any, VLAN Id: any.

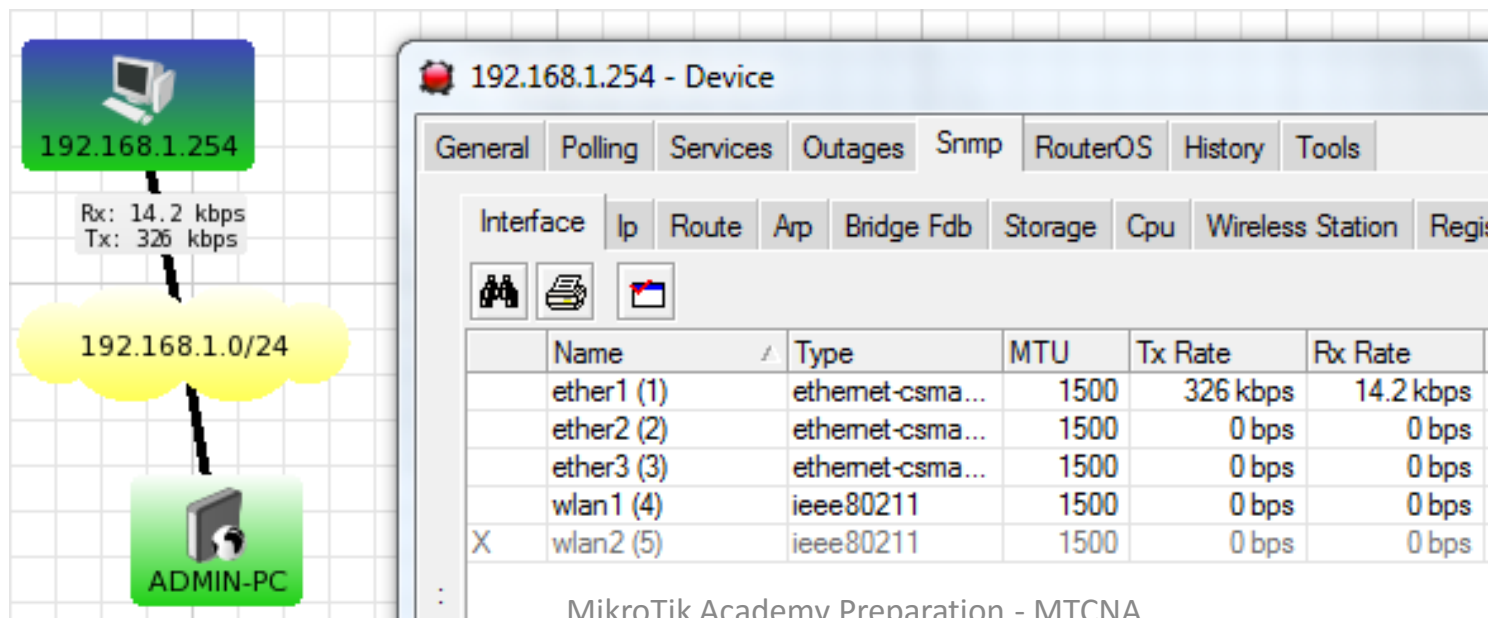
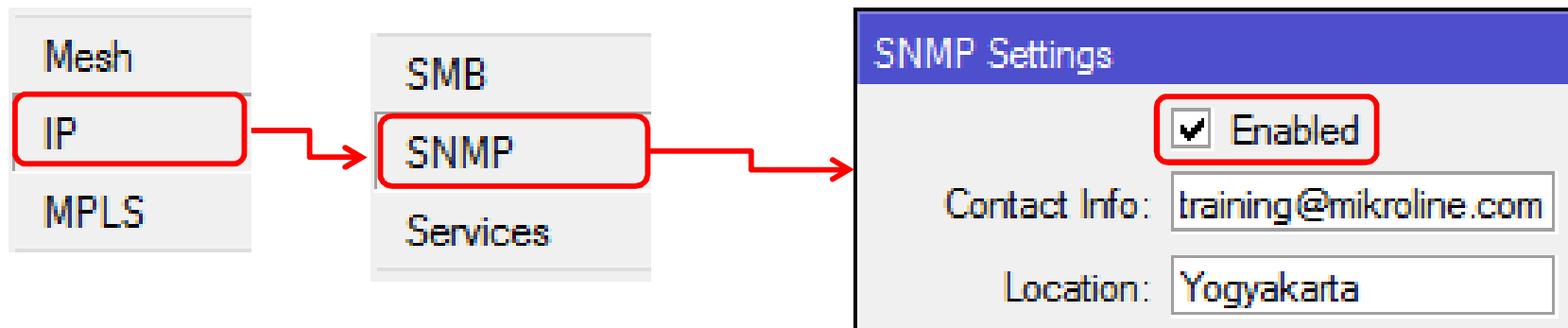
On the right side of the window, there are buttons for Start, Stop, Close, and New Window.

At the bottom of the window, a table displays traffic statistics:

Et...	Prot...	Src.	Dst.	VLAN Id	Tx Rate	Rx Rate	Tx Pack...	Rx f	▼
800 (ip)		255.255.255.255	0.0.0.0		13.1 kbps	0 bps	4		
800 (ip)		192.168.1.253	91.232.82.92		15.4 kbps	4.4 kbps	1		
800 (ip)		192.168.1.253	255.255.255.255		0 bps	1933 bps	0		
800 (ip)		192.168.1.253	202.152.192.179		208 bps	373 bps	0		
800 (ip)		192.168.1.253	193.47.247.62		1408 bps	848 bps	2		
800 (ip)		192.168.1.253	154.50.194.3		66.8 kbps	7.5 kbps	8		
800 (ip)		192.168.1.253	10.10.10.100		3.8 kbps	1205 bps	1		

SNMP

- Simple Network Management Protocol (SNMP) digunakan untuk memonitor jaringan,



LOCAL MANAGEMENT

ARP

- **ARP** melakukan pemetaan IP Address dan MAC Address yang bersifat dinamik

The screenshot shows the Mikrotik WinBox interface. On the left, a navigation menu has 'IP' and 'ARP' highlighted with red boxes. The main window displays the 'ARP List' table. The table has columns for 'IP Address' and 'MAC Address'. The entries are as follows:

	IP Address	MAC Address
D	172.16.10.100	D0:DF:9A:22:36:67
D	172.16.10.101	50:B7:C3:5D:DE:B5
D	172.16.10.102	20:68:9D:77:B0:AA
D	172.16.10.106	20:7C:8F:68:D7:0C
D	D - dynamic 10.108	D0:DF:9A:97:23:C2
D	172.16.10.112	20:68:9D:8A:C0:3B
	172.16.10.121	00:26:C7:77:6E:32
D	172.16.10.128	9C:4E:36:40:19:94
D	172.16.10.133	00:15:AF:4C:08:A2
D	172.16.10.150	00:22:5F:39:CD:E4
D	192.168.1.1	00:0C:42:55:5B:C4
D	192.168.1.73	00:E0:4C:36:01:99

A red bracket on the right side of the table is labeled 'Max 8192', indicating the maximum number of entries in the ARP table.

ARP

- ARP dapat digunakan untuk memasangkan sebuah IP Address, MAC Address dan port router, dengan demikian port yang ada di router hanya bisa digunakan oleh pengguna yang memiliki pasangan IP Address dan MAC Address tertentu. Namun demikian pengguna lain masih dapat login ke winbox melalui MAC Address

ARP

- Pemasangan IP Address dengan MAC Address

The diagram illustrates the steps to configure a static ARP entry in MikroTik WinBox:

- Menu Path:** A red box highlights the **IP** menu, with an arrow pointing to the **ARP** sub-menu. Another arrow points from **ARP** to the **Accounting** option.
- ARP List Table:** Two screenshots of the ARP List table are shown. The left screenshot shows a table with one entry: IP Address: 192.168.1.253, MAC Address: 60:EB:69:74:FC:13, Interface: ether1. A red box highlights this entry, with an arrow pointing to the **Make Static** button in the dialog box below. The right screenshot shows the same table with a red box highlighting the empty space at the beginning of the first row, indicating where a new entry is added.
- Dialog Box:** A dialog box titled **ARP <192.168.1.253>** is shown. It contains fields for IP Address (192.168.1.253), MAC Address (60:EB:69:74:FC:13), and Interface (ether1). The **Make Static** button is highlighted with a red box, and an arrow points from it to the empty space in the ARP List table on the right.

ARP

- Pemasangan dengan port router

The screenshot shows the Mikrotik WinBox interface configuration for the 'ether1' interface. The 'Interface List' table is visible, with the 'ether1' entry highlighted. Below the table, the 'Interface <ether1>' configuration page is shown, with the 'General' tab selected. The 'Name' is 'ether1', 'Type' is 'Ethernet', and 'MTU' is '1500'. The 'MAC Address' is '00:0C:42:5E:2B:53'. The 'ARP' field is set to 'reply-only'.

Interface	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel
R	ether1			

Interface <ether1>

General | Ethernet | Status | Overall Stats | Rx Stats | ...

Name: ether1

Type: Ethernet

MTU: 1500

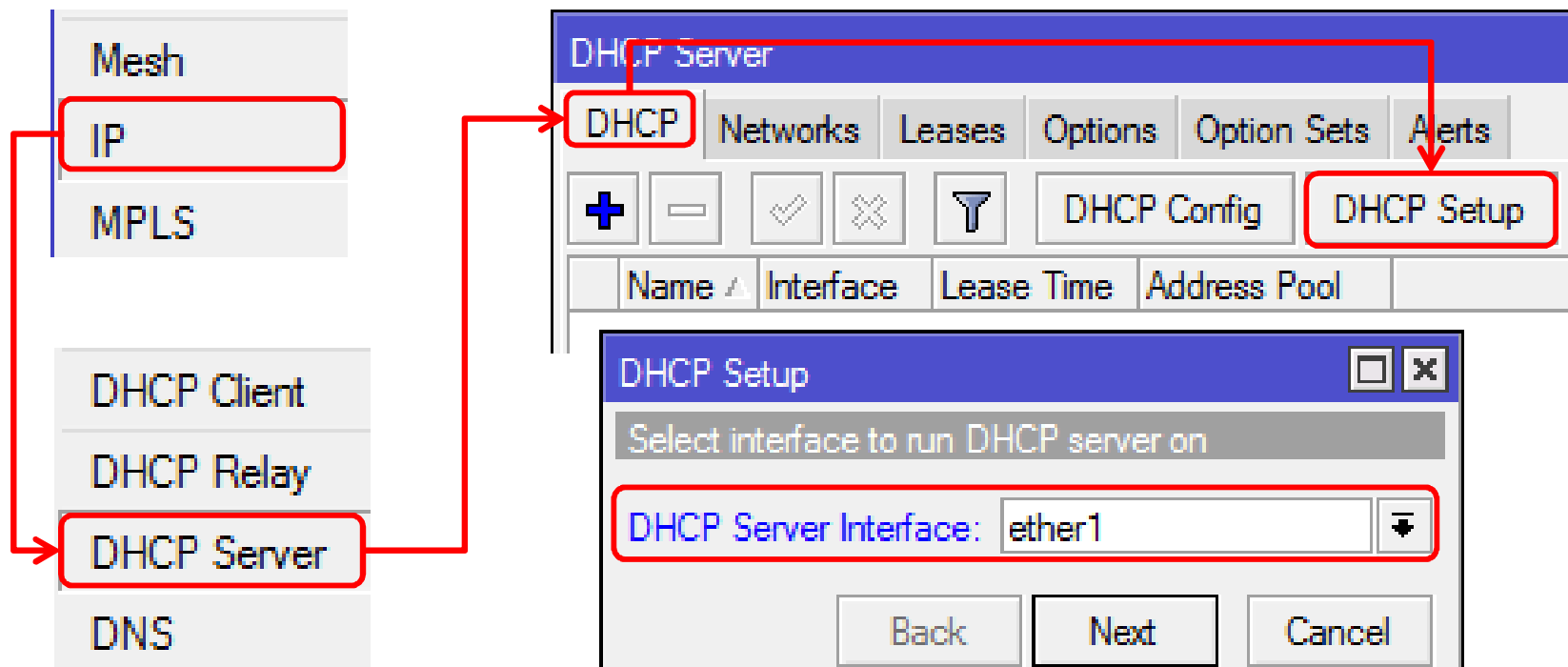
MAC Address: 00:0C:42:5E:2B:53

ARP: reply-only

Jika ARP
dikonfigurasi
dengan reply-only
di interface, router
hanya akan
membalas ARP
request saja.

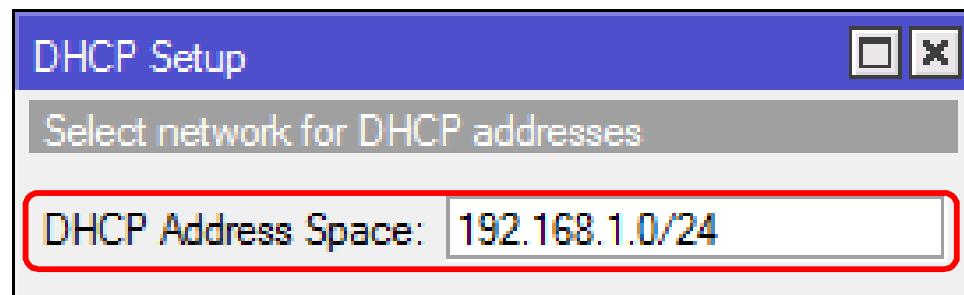
DHCP SERVER

- DHCP Server merupakan protocol yang memungkinkan setiap peralatan komputer dalam jaringan mendapatkan IP Address otomatis
- Hanya ada satu DHCP Server di setiap interface

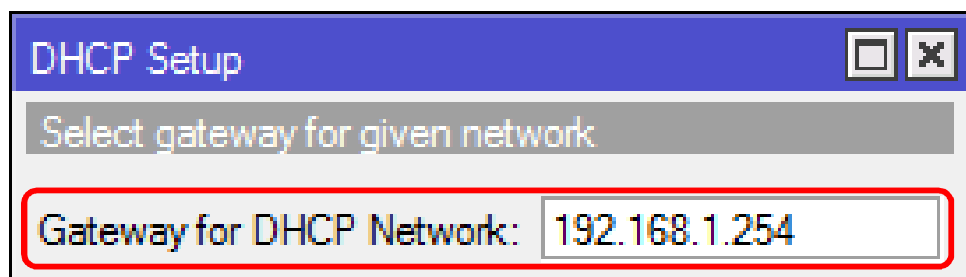


DHCP SERVER

- *DHCP Server Address Space* merupakan IP Address untuk DHCP



- *Gateway for DHCP Network*, IP Address yang dijadikan gateway bagi DHCP Client



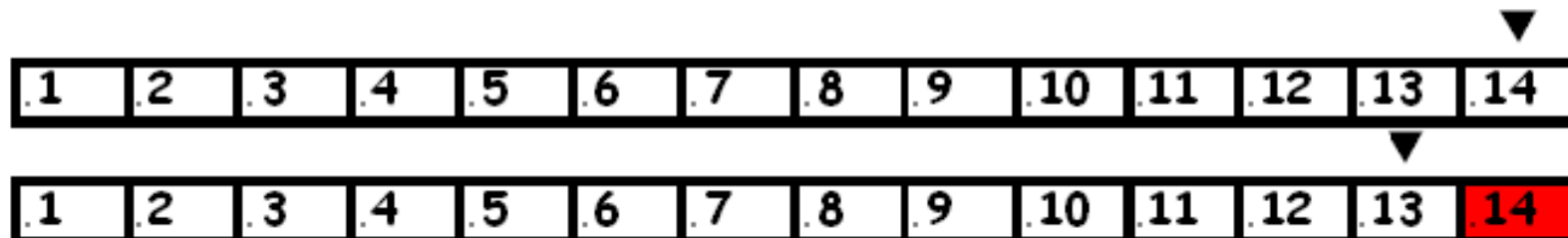
DHCP SERVER

- *Addresses to Give Out*, merupakan rentang IP yang disediakan untuk klien melalui DHCP, secara otomatis akan terbentuk di IP Pool

The image shows two windows from Mikrotik WinBox. The 'DHCP Setup' window on the left has a red box around the 'Addresses to Give Out' field, which contains the IP range '.168.1.1-192.168.1.253'. The 'IP Pool' window on the right shows a table with one entry: 'dhcp_pool1' with the address range '192.168.1.1-192.168.1.253'. A red arrow points from the DHCP Setup window to the IP Pool window.

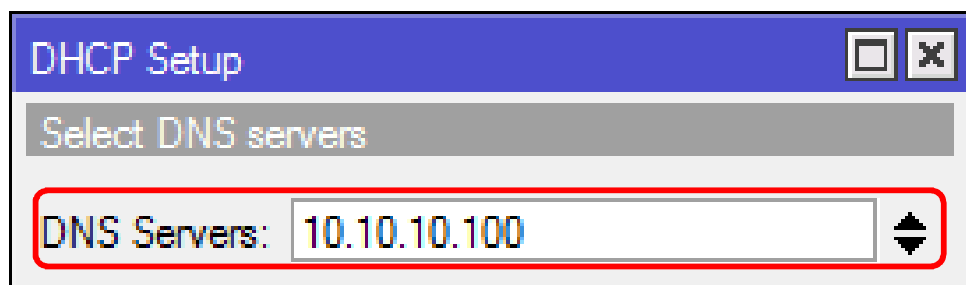
Name	Addresses
dhcp_pool1	192.168.1.1-192.168.1.253

Pembagian IP address oleh DHCP Server dimulai dari IP terbesar dari pool (default)

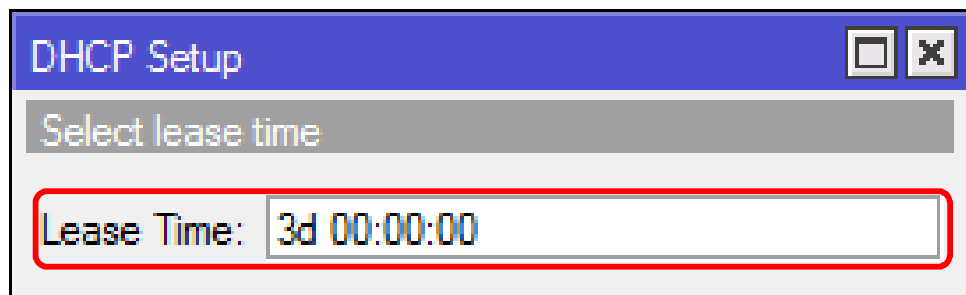


DHCP SERVER

- *DNS Servers*, IP DNS yang diberikan kepada DHCP Client, mengacu pada konfigurasi DNS



- *Lease Time*, jangka waktu penggunaan IP Address oleh DHCP Client



DHCP SERVER

DHCP Server

DHCP Networks Leases Options Option Sets Alerts

+ - ✓ ✗ ⏏ DHCP Config DHCP Setup

Name	Interface	Lease Time	Address Pool
dhcp1	ether1	3d 00:00:00	dhcp_pool2

DHCP Setup

Setup has completed successfully

OK

DHCP Server

DHCP **Networks** Leases Options Option Se

+ - ⏏ ⏏

Address	Gateway	DNS Servers
192.168.1.0/24	192.168.1.254	10.10.10.100

DHCP Network <192.168.1.0/24>

Address: 192.168.1.0/24

Gateway: 192.168.1.254

Netmask:

DNS Servers: 10.10.10.100

Domain:

WINS Servers:

NTP Servers:

IP Pool

- IP Pool digunakan untuk mendefinisikan rentang IP Address di DHCP Server

The screenshot displays the Mikrotik WinBox IP Pool configuration interface. The main window has two tabs: "Pools" and "Used Addresses". The "Pools" tab is active, showing a table of existing IP pools. A red box highlights the "+" button in the toolbar, indicating the action to add a new pool. An inset window titled "IP Pool <Multimedia_Pool>" shows the configuration for a specific pool. The "Name" field is set to "Multimedia_Pool". The "Addresses" field contains two ranges: "192.168.1.10-192.168.1.25" and "192.168.9.10-192.168.9.25". The "Next Pool" field is set to "none". Buttons for "OK", "Cancel", "Apply", and "Copy" are visible on the right side of the inset window.

Name	Addresses	Next
Multimedia_Pool	192.168.1.10-192.168.1.25, 192.168.9.10-192.168.9.25	none
dhcp_pool1	192.168.1.1-192.168.1.253	none

IP Pool <Multimedia_Pool>

Name: Multimedia_Pool

Addresses: 192.168.1.10-192.168.1.25
192.168.9.10-192.168.9.25

Next Pool: none

Buttons: OK, Cancel, Apply, Copy

IP Pool

DHCP Server

DHCP Networks Leases Options Option Sets Alerts

+ - ✓ ✗ ⌵ DHCP Config DHCP Setup

Na...	Interface	Relay	Lease Time	Address Pool	Add AF
dhcp1	ether1		3d 00:00:00	Multimedia_Pool	no

DHCP Server <dhcp1>

Name: dhcp1

Interface: ether1

Relay:

Lease Time: 3d 00:00:00

Bootp Lease Time: forever

Address Pool: Multimedia_Pool

OK
Cancel
Apply
Disable
Copy
Remove

STATIC LEASE

IP Address hanya digunakan oleh komputer tertentu berdasarkan MAC Addressnya

DHCP Server

DHCP Networks **Leases** Options Option Sets Alerts

+ - ✓ ✗ ⓘ ⏏ Make Static Check Status

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Expires After	Status
D					192.168.1.253	60:EB:69:74:FC:13	2d 23:58:22	bound

D - dynamic

+ - - ✓ ✗ ⓘ ⏏ **Make Static** Check Status

	Address	MAC Address	Client ID	Server
D				

DHCP Server

DHCP Networks **Leases** Options Option Sets Alerts

+ - ✓ ✗ ⓘ ⏏ Make Static Check Status

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Expires After	Status
	192.168.1.253	60:EB:69:74:FC:13	1:60:eb:69:74:fc:13	dhcp1	192.168.1.253	60:EB:69:74:FC:13	2d 23:56:22	bound

STATIC LEASE

DHCP Server

DHCP Networks Leases Options Option Sets Alerts

+ - ✓ ✗ ⏏ DHCP Config DHCP Setup

Name	Interface	Lease Time	Address Pool
dhcp1	ether1	3d 00:00:00	static-only

DHCP Server <dhcp1>

Name: dhcp1

Interface: ether1

Relay:

Lease Time: 3d 00:00:00

Bootp Lease Time: forever

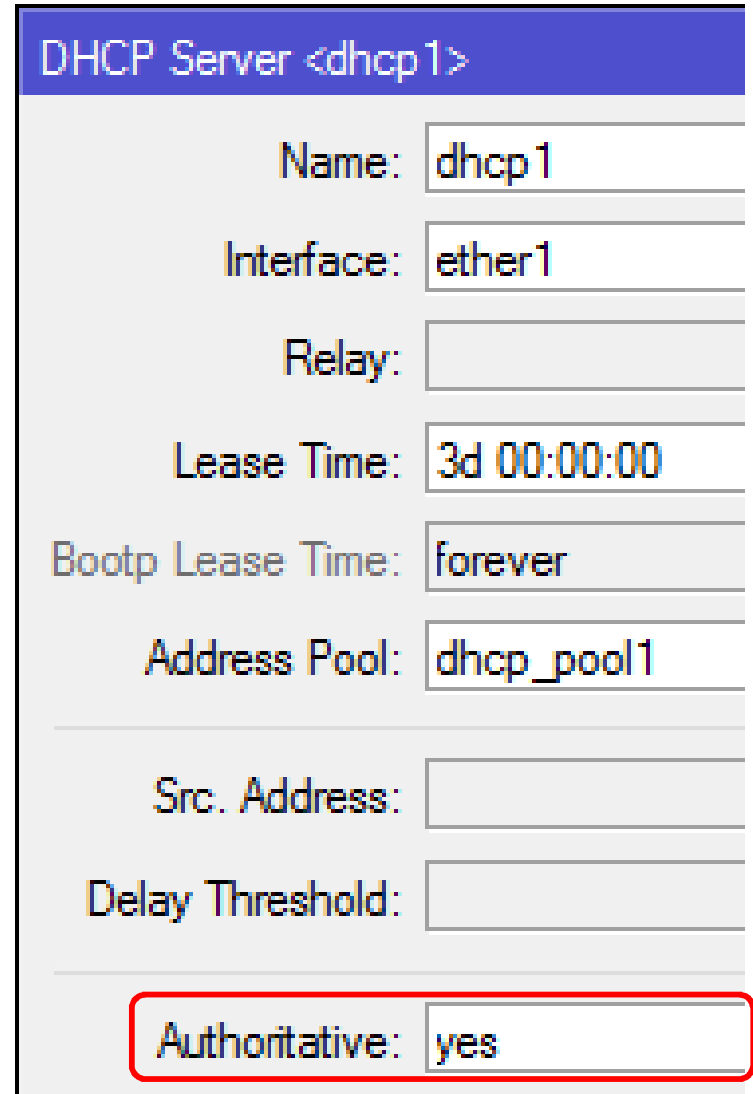
Address Pool: static-only

OK Cancel Apply Disable Copy Remove

Jika static-only,
DHCP tidak
memerlukan
Address Pool

AUTHORITATIVE

- **“Authoritative = yes”**
Untuk mengganggu adanya DHCP Server tandingan (rouge/ilegal) dalam satu network
- Adaptasi jaringan lebih cepat jika ada perubahan konfigurasi DHCP



The image shows a screenshot of the Mikrotik WinBox configuration interface for a DHCP Server named 'dhcp1'. The configuration is as follows:

DHCP Server <dhcp1>	
Name:	dhcp1
Interface:	ether1
Relay:	
Lease Time:	3d 00:00:00
Bootp Lease Time:	forever
Address Pool:	dhcp_pool1
Src. Address:	
Delay Threshold:	
Authoritative:	yes

DHCP ALERTS

The screenshot shows the Mikrotik WinBox interface for configuring DHCP Alerts. The 'Alerts' tab is selected and highlighted with a red box. Below the tabs is a toolbar with icons for adding, removing, checking, unchecking, and filtering. A table lists the interface 'ether1' with an alert timeout of '00:00:05'. Below the table, the configuration for the selected alert is shown, including the interface name, valid servers (MAC address), alert timeout, unknown servers, and the on-alert script.

Interface	Alert Timeout
ether1	00:00:05

DHCP Alert <ether1>

Interface: ether1

Valid Servers: 00:0C:42:43:A0:66

Alert Timeout: 00:00:05

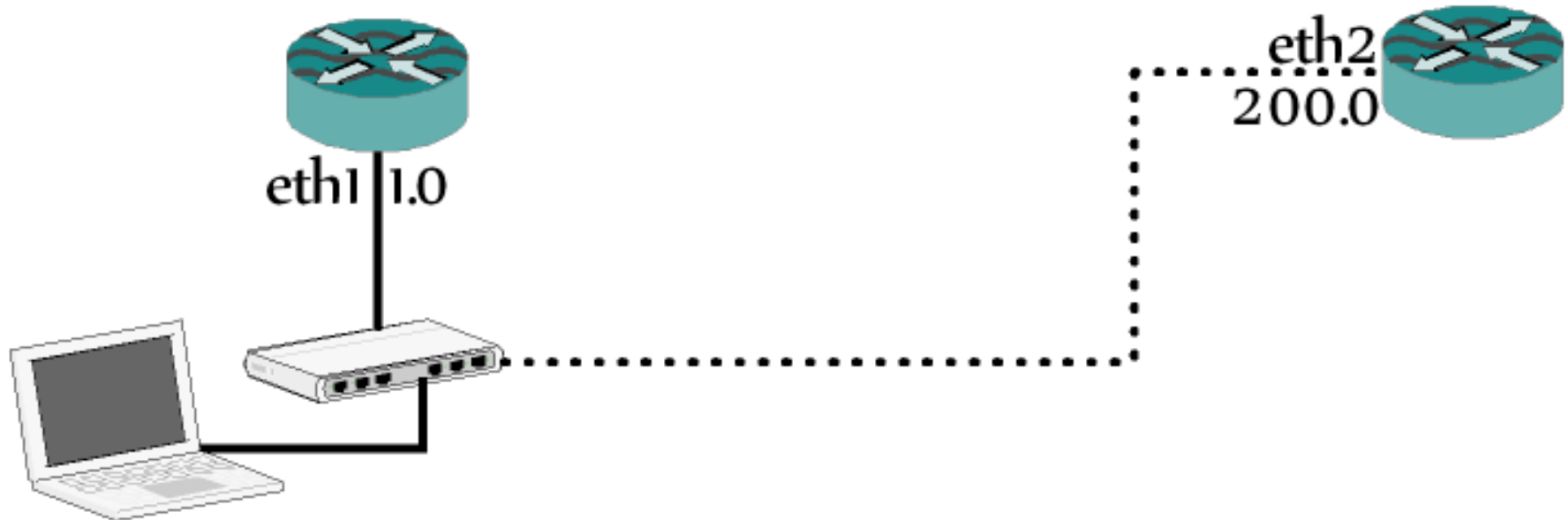
Unknown Servers:

On Alert:
:log info message="Awat DHCP Palsu"

Valid-Server, MAC
Address interface DHCP
Server yg sah

On-Alert, menjalankan
script tertentu jika ada
DHCP-Server lain

DHCP ALERTS



Log			
Freeze			
Jan/01/2002 01:00:04	memory	system, info	router rebooted
Jan/01/2002 01:00:11	memory	interface, info	ether1 link up (speed 100M, full duplex)
Jan/01/2002 01:00:12	memory	wireless, info	00:0C:42:B7:B0:EF@wlan1 established connection on 2462000, SSID Quitrex
Mar/11/2014 05:49:16	memory	system, info, account	user admin logged in via winbox
Mar/11/2014 05:50:00	memory	dhcp, critical, error	dhcp alert on ether1: discovered unknown dhcp server, mac 00:0C:42:95:14:67, ip 192.168.100.254
Mar/11/2014 05:50:01	memory	script, info	Awas DHCP Palsu
Mar/11/2014 05:51:09	memory	dhcp, critical, error	dhcp alert on ether1: discovered unknown dhcp server, mac 00:0C:42:95:14:67, ip 192.168.100.254
Mar/11/2014 05:51:09	memory	script, info	Awas DHCP Palsu
Mar/11/2014 05:51:51	memory	dhcp, critical, error	dhcp alert on ether1: discovered unknown dhcp server, mac 00:0C:42:95:14:67, ip 192.168.100.254
Mar/11/2014 05:51:51	memory	script, info	Awas DHCP Palsu

DHCP Options

- DHCP Options memungkinkan pemberian informasi tambahan bagi DHCP Client sesuai option list di :
 - <http://www.iana.org/assignments/bootp-dhcp-parameters>

DHCP Options

- Options yang bisa dilakukan tanpa DHCP options:
 - Subnet-mask/netmask (option 1)
 - Router/gateway (option 3)
 - Domain-Server/DNS Server (option 6)
 - NTP-Servers (option 42)
 - NETBIOS-Name-Server/WINS server (option 44)

DHCP Network <192.168.1.0/24>	
Address:	<input type="text" value="192.168.1.0/24"/>
Gateway:	<input type="text" value="192.168.1.254"/>
Netmask:	<input type="text"/>
DNS Servers:	<input type="text"/>
Domain:	<input type="text"/>
WINS Servers:	<input type="text"/>
NTP Servers:	<input type="text"/>
Next Server:	<input type="text"/>
Boot File Name:	<input type="text"/>

DHCP Options

- Custom DHCP options:
 - Classless Static Route (option 121) –
 - “0x18AC10010A0A1464” = “network=172.16.1.0/24 gateway=10.10.20.100”

0x | 18 | AC1001 | 0A0A1464 |

0x – **Hex Number**

18 – **Subnet/Prefix = 24**

AC 10 01 – **Network = 172.16.1.0**

0A0A1464 – **Gateway = 10.10.20.100**

DHCP Options

DHCP Server

DHCP Networks Leases **Options** Option Sets Alerts

+ - Filter

Name	Code	Value
opsi_dhcp	121	0x18AC10010A0A1464

DHCP Option <opsi_dhcp>

Name: opsi_dhcp OK

Code: 121 Cancel

Value: 0x18AC10010A0A1464 Apply

Raw Value: 18ac10010a0a1464 Copy

DHCP Server

DHCP **Networks** Leases Options Optio

+ - Filter

Address	Gateway
192.168.1.0/24	192.168.1.254

DHCP Network <192.168.1.0/24>

Address: 192.168.1.0/24

Gateway: 192.168.1.254

Netmask:

Boot File Name:

DHCP Options: opsi_dhcp

DHCP Option Set:

DHCP CLIENT

Interface	Use Peer DNS	Add Default Route	IP Address	Expires After
ether1	yes	yes	192.168.1.253/24	2d 23:59:42

DHCP Client <ether1>

DHCP | Status

Interface: ether1

Use Peer DNS

Use Peer NTP

DHCP Options: hostname

clientid

Add Default Route: yes

Default Route Distance: 0

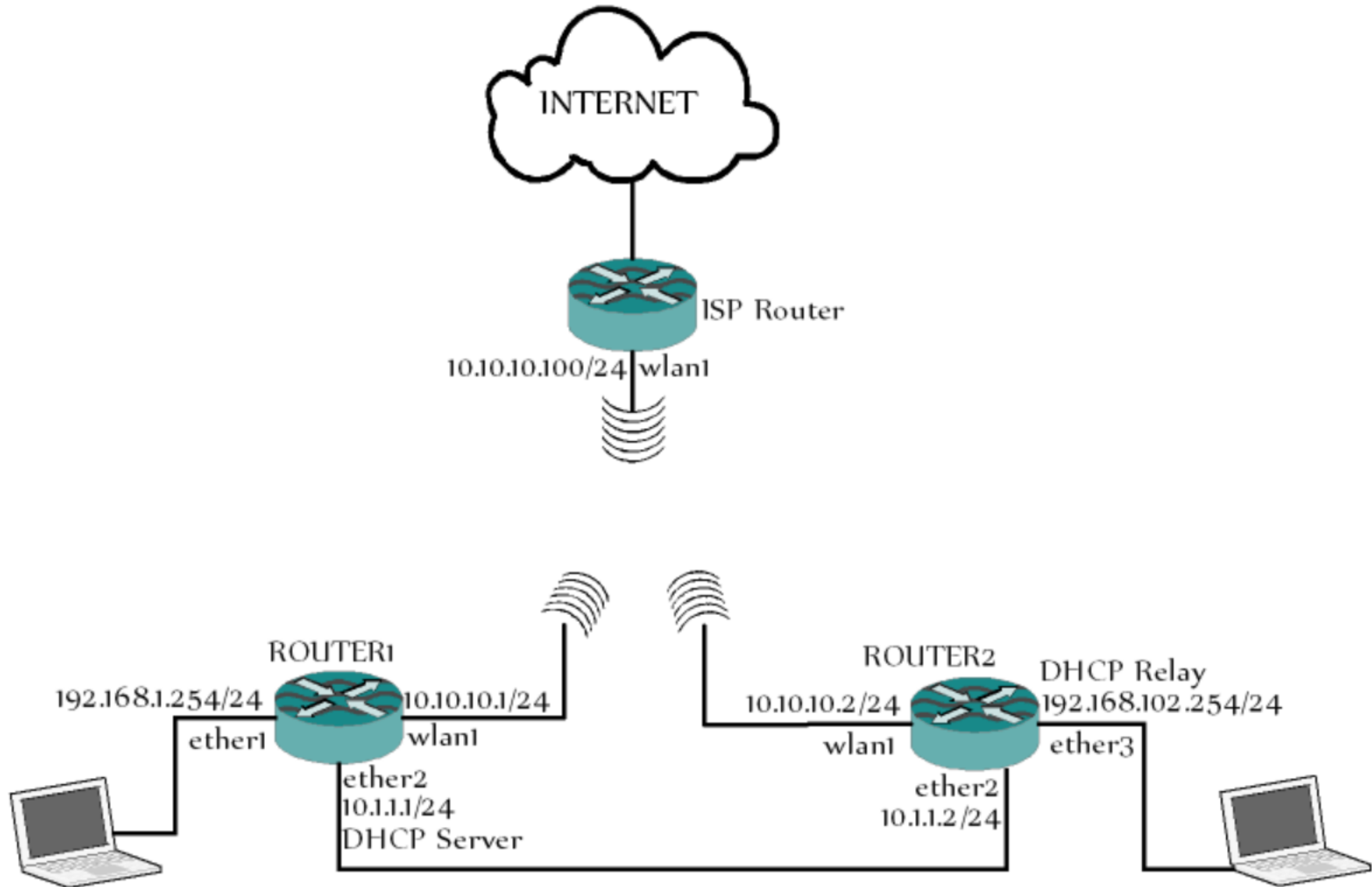
DHCP Client dapat menerima IP Address/ Subnet mask, Gateway, DNS

Informasi Hostname dan Client ID akan dikirim ke DHCP Server, jika tidak diisi Hostname akan berisi System Identity dan Client ID berisi MAC Address

DHCP RELAY

- DHCP Relay menerima DHCP discovery dan request kemudian meneruskannya ke DHCP server
- Hanya ada 1 DHCP relay antara DHCP Server dan DHCP Client
- Konfigurasi “local address” pada DHCP Relay harus sama dengan “relay address” pada DHCP Server.

DHCP RELAY



DHCP SERVER - R1

Address <10.1.1.1/24>

Address: 10.1.1.1/24

Network: 10.1.1.0

Interface: ether2

IP Pool <dhcp_pool_relay_r2>

Name: dhcp_pool_relay_r2

Addresses: 192.168.102.1-192.168.102.253

DHCP Server

DHCP Networks Leases Options Option Sets Alerts

+ - ✓ ✗ ⏏ DHCP Config DHCP Setup

	Name ^	Interface	Relay	Address Pool
	dhcp1	ether1		dhcp_pool1
⇒	dhcp2	ether2	192.168.102.254	dhcp_pool_relay_r2 ⇒

DHCP Server <dhcp2>

Name: dhcp2

Interface: ether2

Relay: 192.168.102.254

Address Pool: dhcp_pool_relay_r2

DHCP Server

DHCP **Networks** Leases Options

+ - ⏏ ⏏

Address ^	Gateway
192.168.1.0/24	192.168.1.254
192.168.102.0/24	192.168.102.254

DHCP Network <192.168.102.0/24>

Address: 192.168.102.0/24

Gateway: 192.168.102.254

Netmask:

DNS Servers: 10.10.10.100

DHCP RELAY - R2

Address <10.1.1.2/24>

Address: 10.1.1.2/24

Network: 10.1.1.0

Interface: ether2

Address <192.168.102.254/24>

Address: 192.168.102.254/24

Network: 192.168.102.0

Interface: ether3

DHCP Relay

+ - ✓ ✕ ⏏ Reset Counters

Name	Interface	DHCP Server	Local Address
relay1	ether3	10.1.1.1	192.168.102.254

DHCP Relay <relay1>

General Status

Name: relay1

Interface: ether3

DHCP Server: 10.1.1.1

Delay Threshold:

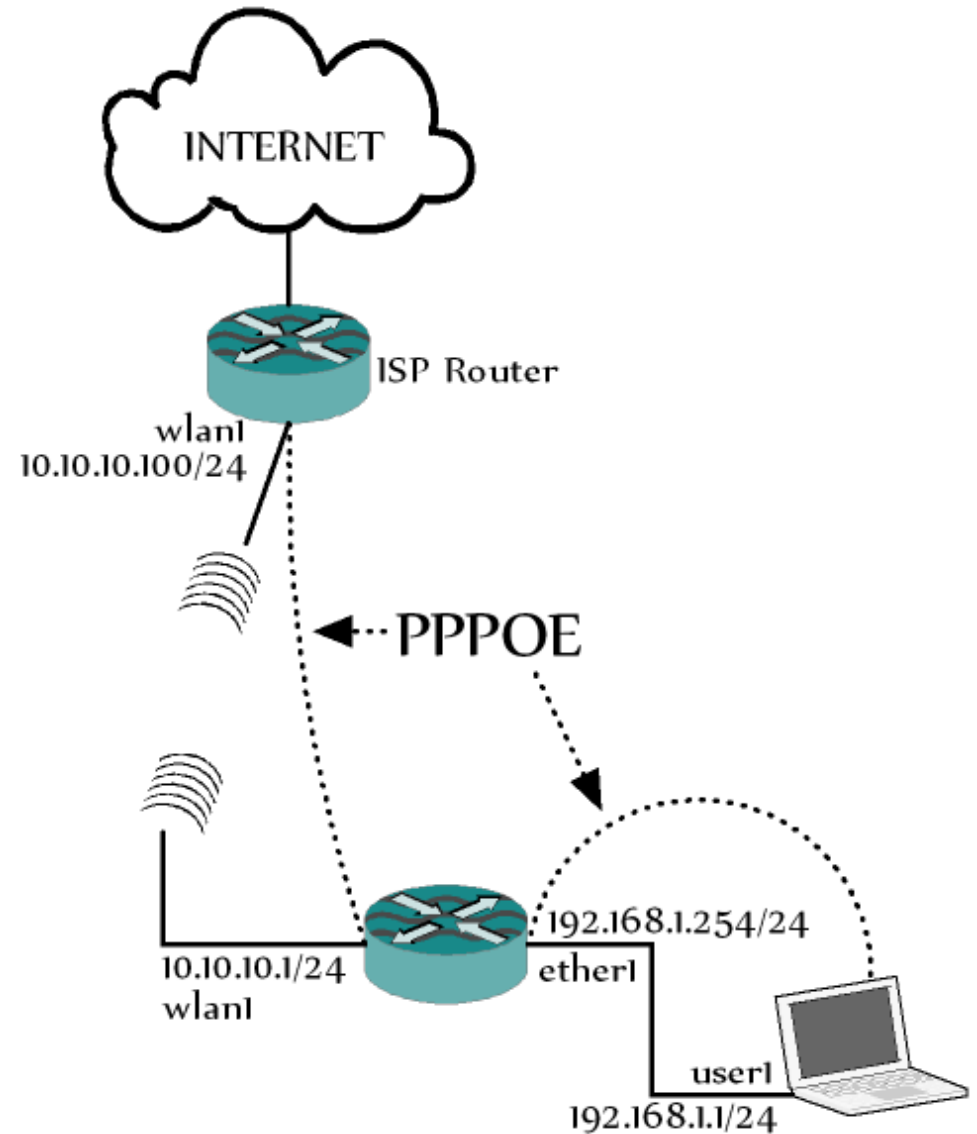
Local Address: 192.168.102.254

Disable ethernet laptop di router2, enable lagi IP Address yang diperoleh?

TUNNEL

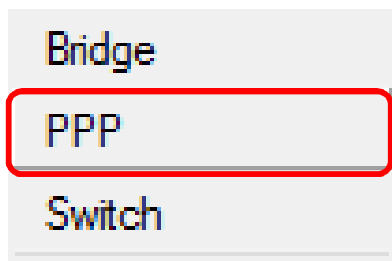
PPPOE

PPPOE merupakan tunneling L2 oleh karena itu PPPOE Server dan PPPOE Client harus berada dalam jaringan fisik yang sama.

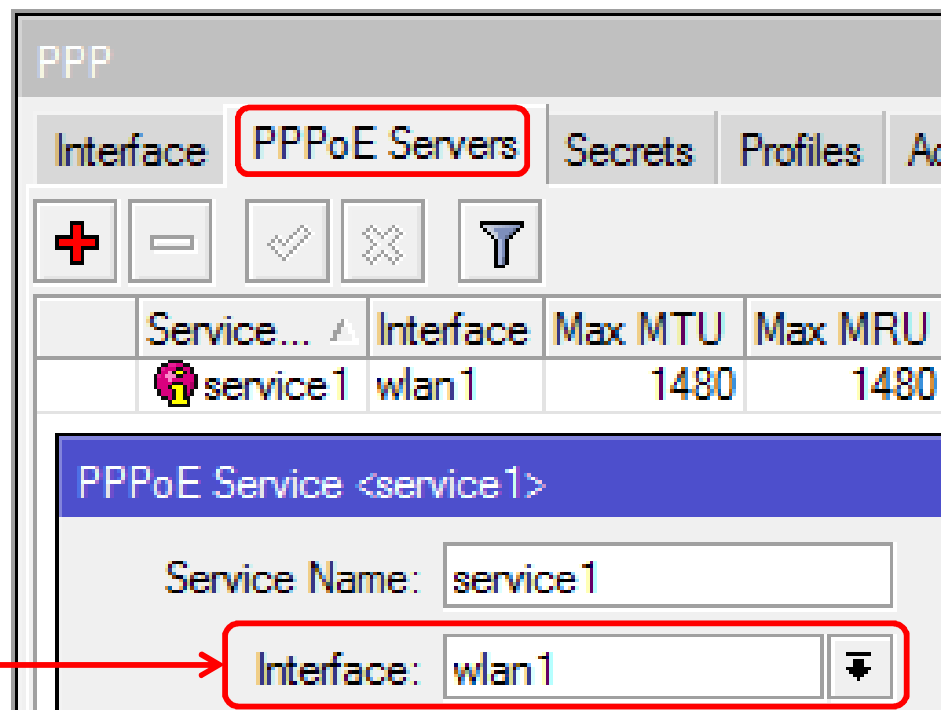


PPPOE Server

- PPPOE Server menerima koneksi klien pada interface tertentu melalui proses autentikasi
- Klien dapat diautentikasi melalui: Lokal user PPP (Secret), MikroTik Radius, Free Radius Linux



interface koneksi ke PPPOE Client



PPP Secret

- PPP Secret menyimpan **username** dan **password** untuk diberikan ke user maupun pengaturan lainnya
- **Service**, sebuah username dapat dikonfigurasi untuk service tertentu atau semua service (any)

PPP Secret <user1>

Name: user1

Password: user1

Service: any

any
async
l2tp
ovpn
pppoe
pptp
sstp

PPP Secret

- **Local Address**, IP Address yang diberikan ke server ketika ada user yang login dan sudah terautentikasi.
- **Remote Address**, IP Address bagi user yang diautentikasi.

PPP Secret <user1>

Name:	user1
Password:	user1
Service:	any
Caller ID:	
Profile:	default
Local Address:	12.1.1.1
Remote Address:	12.1.1.2

PPP Profile

- PPP Profile mendefinisikan parameter bagi sekelompok user di database lokal (Secret)

The image shows two screenshots from the Mikrotik WinBox interface. The top screenshot displays the 'PPP' menu with sub-tabs: 'Interface', 'PPPoE Servers', 'Secrets', 'Profiles', and 'Active Connections'. The 'Profiles' tab is selected and highlighted with a red box. Below the tabs is a toolbar with four icons: a plus sign (+), a minus sign (-), a refresh icon, and a filter icon. The plus sign icon is also highlighted with a red box. A red arrow points from the plus sign icon to the 'General' tab of the second screenshot. The second screenshot shows the configuration for a 'PPP Profile <Profile_PPPOE>'. The 'General' tab is selected and highlighted with a red box. The configuration fields are: 'Name: Profile_PPPOE', 'Local Address: 11.1.1.1', and 'Remote Address: 11.1.1.2'. Each address field has a dropdown arrow and a directional arrow (down for local, up for remote).

PPPOE Client

PPPOE Client adalah host yang akan melakukan koneksi ke PPPOE Server dan akan diberikan IP Address jika autentikasinya berhasil

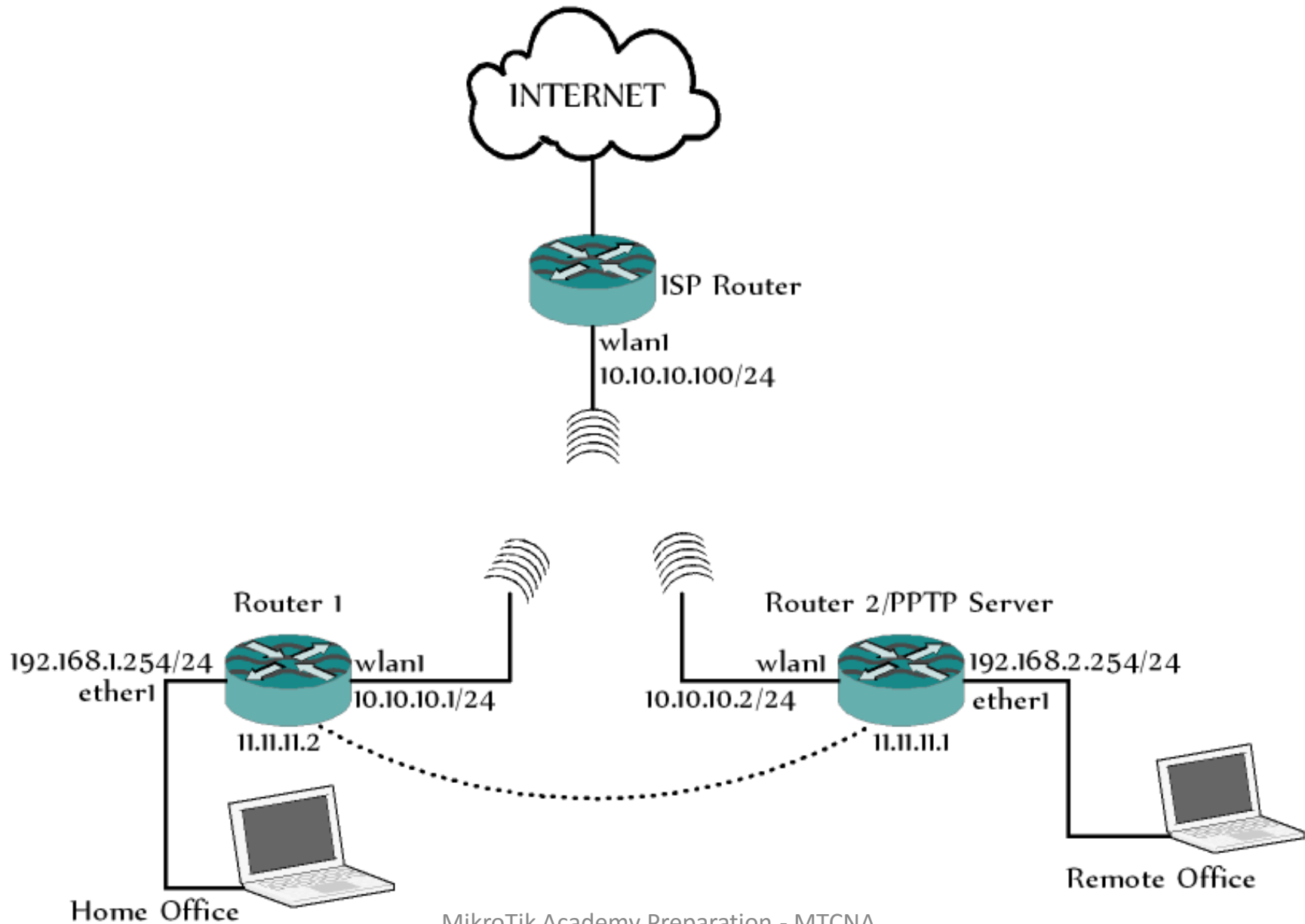
The image displays three sequential screenshots from the MikroTik WinBox interface, illustrating the configuration of a PPPOE Client. Red boxes and arrows highlight the key steps:

- First Screenshot:** The 'PPP' menu is open, and 'PPPoE Client' is selected. A red box highlights the 'Interface' tab and the '+' icon, with an arrow pointing to the 'PPPoE Client' option.
- Second Screenshot:** The 'Interface <pppoe-out1>' configuration page is shown. The 'General' tab is selected. The 'Name' field is set to 'pppoe-out1' and the 'Type' is set to 'PPPoE Client'. A red box highlights the 'Interfaces' field, which is set to 'wlan1'.
- Third Screenshot:** The 'Dial Out' configuration page is shown. The 'User' field is set to 'user1' and the 'Password' field is set to 'user1'. A red box highlights these two fields.

PPTP

- Koneksi antar router melalui Internet yang bersifat secure, digunakan untuk koneksi jaringan lokal melalui WAN.
- Mikrotik RouterOS bisa berfungsi sebagai PPTP Server maupun PPTP Client atau gabungan dari keduanya.
- Fungsi PPTP Client sudah tersedia dalam sebagian besar Sistem Operasi.

PPTP



PPTP SERVER

PPP

Interface | PPPoE Servers | Secrets | Profiles | Active Connections

PPP Scanner | PPTP Server

Name	Type	L2 MTU	Tx
PPTP Server			

Enabled

Max MTU: 1460

PPP

Interface | PPPoE Servers | Secrets | Profiles

+

Name	Password	Service	Caller ID
user1	user1	pptp	

PPP Secret <user1>

Name: user1

Password: user1

Service: pptp

Caller ID:

Profile: default

Local Address: 11.11.11.1

Remote Address: 11.11.11.2

PPP

Interface | PPPoE Servers | Secrets | Profiles | Active Connections

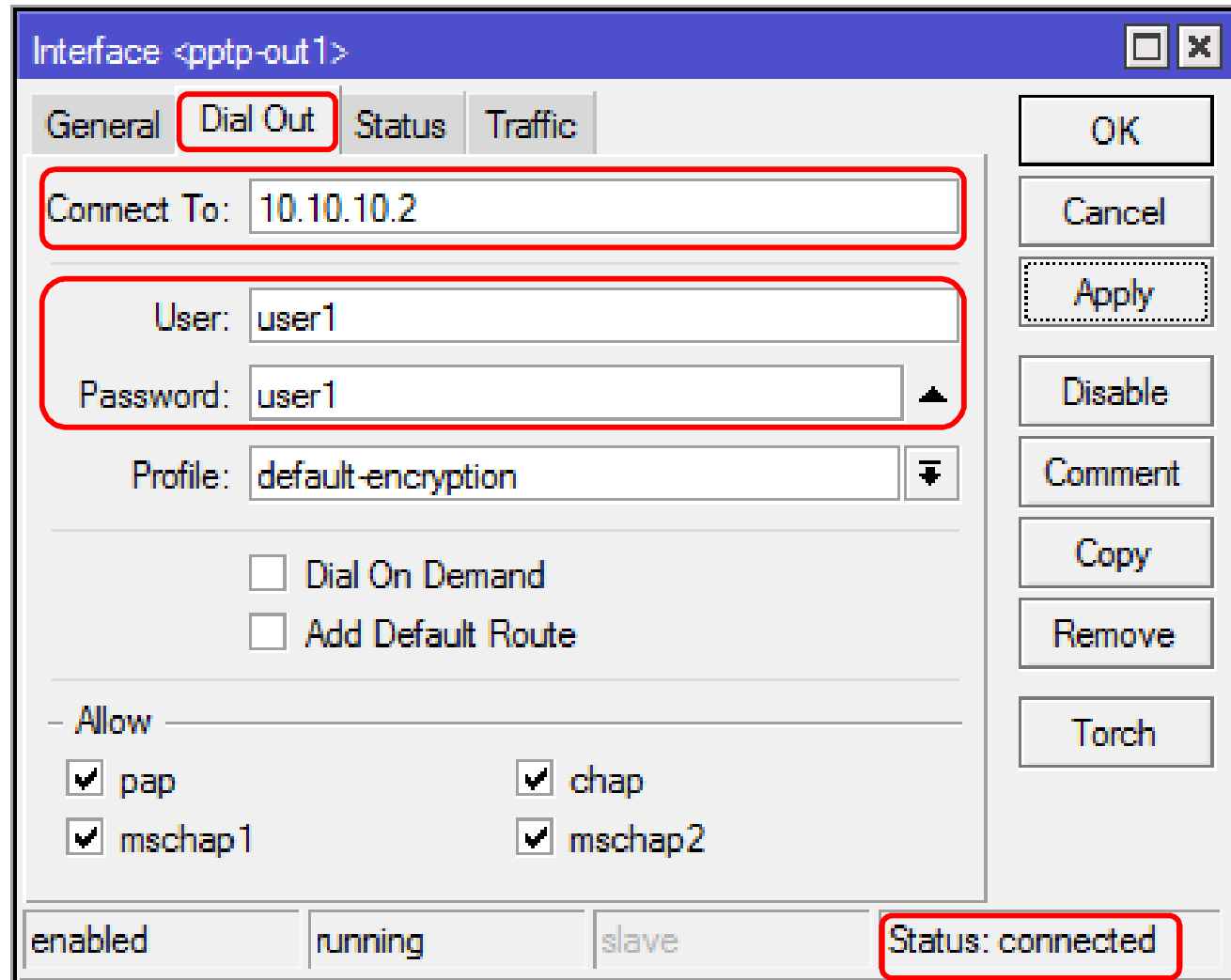
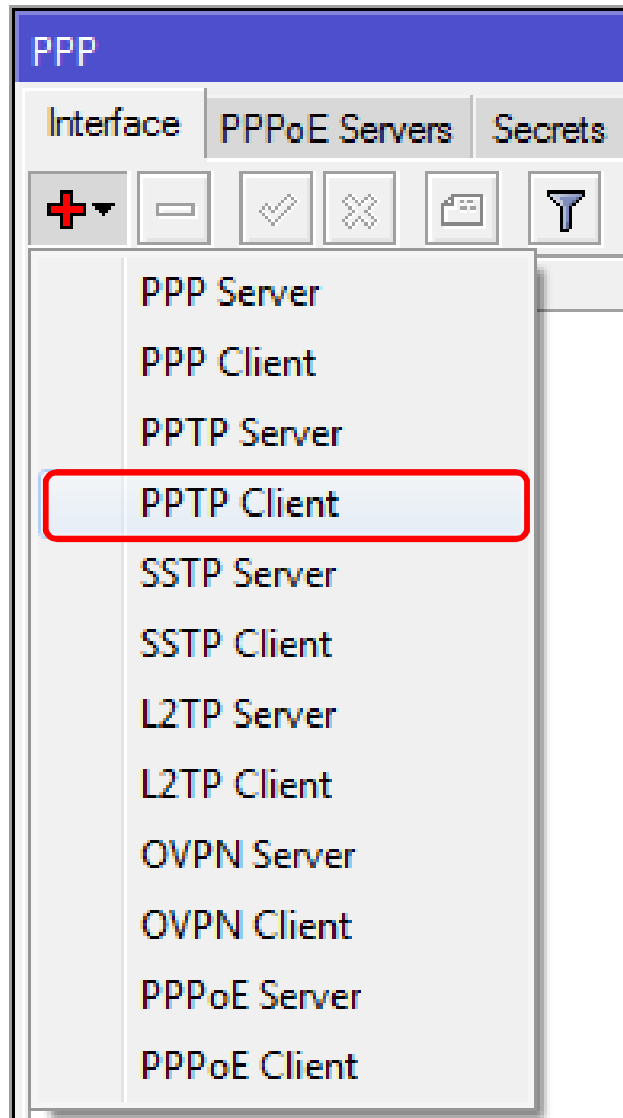
Name	Service	Caller ID	Encoding	Address
L user1	pptp	10.10.10.1	MPPE128 stateless	11.11.11.2

L - local

R - RADIUS

Active Connections, user yang terhubung ke PPTP Server

PPTP CLIENT



STATIC ROUTE - PPTP

- Koneksikan antar klien dengan static route?

Route List

Routes Nexthops Rules VRF

+ - ✓ ✗ 📄 🏠

	Dst. Address	Gateway
AS	0.0.0.0/0	10.10.10.100 reachable wlan1
DAC	10.10.10.0/24	wlan1 reachable
DAC	11.11.11.1	pptp-out1 reachable
DAC	192.168.1.0/24	ether1 reachable
AS	192.168.2.0	11.11.11.1 reachable pptp-out1

Route <192.168.2.0>

General Attributes

Dst. Address: 192.168.2.0

Gateway: 11.11.11.1 reachable pptp-out1

PPTP Klien

Route List

Routes Nexthops Rules VRF

+ - ✓ ✗ 📄 🏠

	Dst. Address	Gateway
AS	0.0.0.0/0	10.10.10.100 reachable wlan1
DAC	10.10.10.0/24	wlan1 reachable
DAC	11.11.11.2	pptp-in reachable
AS	192.168.1.0/24	11.11.11.2 reachable pptp-in
DAC	192.168.2.0/24	ether1 reachable

Route <192.168.1.0/24>

General Attributes

Dst. Address: 192.168.1.0/24

Gateway: 11.11.11.2 reachable pptp-in

PPTP Server

SSTP

- SSTP adalah protocol tunnel (TCP Port 443) yang memanfaatkan SSL 3.0 digunakan untuk meningkatkan keamanan tunel dengan enkripsi dan autentikasi berbasis SSL (Secure Socket Layer)
- SSTP Protocol tidak disupport oleh banyak OS salah satu OS yang memiliki SSTP Clients adalah Windows 7 dan Windows Vista
- Untuk koneksi SSTP antar MikroTik, koneksi dapat dilakukan tanpa sertifikat SSL

KONFIGURASI SSTP

SSTP Server

SSTP Server

Enabled

Port: 443

Max MTU: 1500

Max MRU: 1500

MRRU: ▼

Keepalive Timeout: 60 ▲

Default Profile: default ▼

– Authentication –

pap chap

mschap1 mschap2

Certificate: none ▼

Verify Client Certificate

SSTP Client

Interface <sstp-out1>

General Dial Out Status Traffic

Connect To: 10.10.10.1

Port: 443

Proxy:

Proxy Port: 443

Certificate: none

Verify Server Certificate

Verify Server Address Fro

User: user1

Password: *****

Academy Preparation

MTCTCE

NETWORK INTRUSION

NETWORK INTRUSION

- Network intrusion adalah gangguan yang dapat menurunkan kinerja jaringan, diantaranya adalah sebagai berikut:
 - Port scan
 - Dos Attack/SYN Flood
 - Ddos Attack

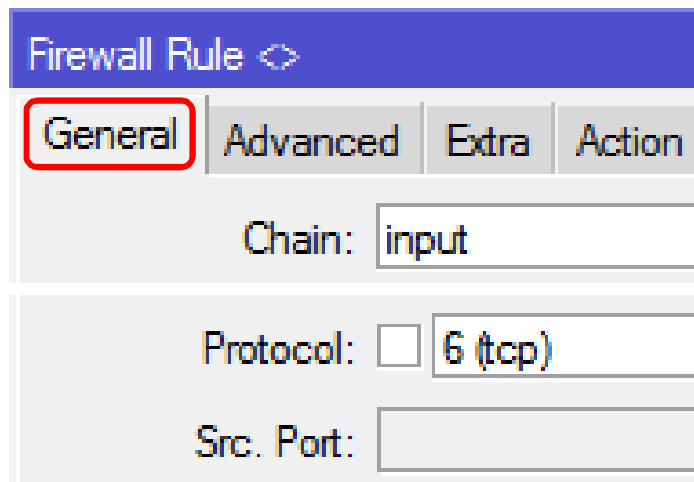
PORT SCAN DETECTION

- Port scan digunakan untuk mencari adanya port yang terbuka
- Port yang tidak digunakan sebaiknya ditutup (disable) dengan *IP Service*
- MikroTik menyediakan opsi Port Scan Detection (PSD) untuk mencegah port scan TCP

	Name	Port
X	api	8728
X	ftp	21
	ssh	22
	telnet	23
	winbox	8291
	www	80

PORT SCAN DETECTION

- PSD akan mendeteksi jika skor **Weight Threshold** tercapai dalam durasi **Delay Threshold**
- Kalkulasi Weight Threshold:
 - port ≤ 1024 : 3, (Low)
 - port > 1024 : 1, (High)
 - scan port 11, 12, 13, 2000: **10**



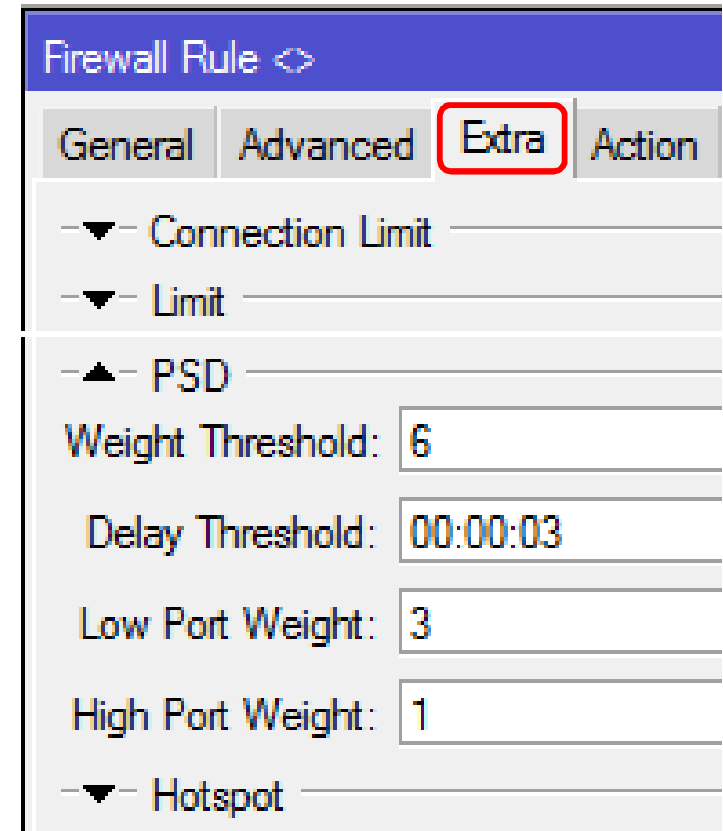
Firewall Rule <>

General Advanced Extra Action

Chain: input

Protocol: 6 (tcp)

Src. Port:



Firewall Rule <>

General Advanced Extra Action

Connection Limit

Limit

PSD

Weight Threshold: 6

Delay Threshold: 00:00:03

Low Port Weight: 3

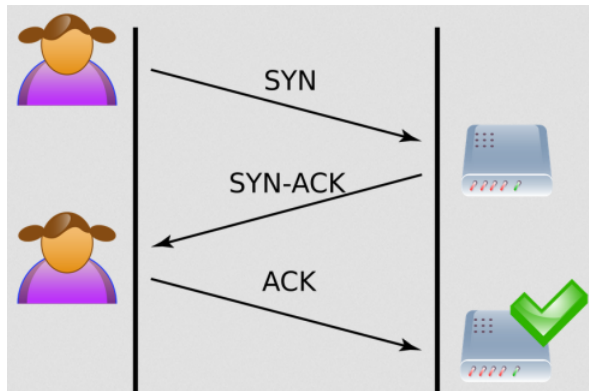
High Port Weight: 1

Hotspot

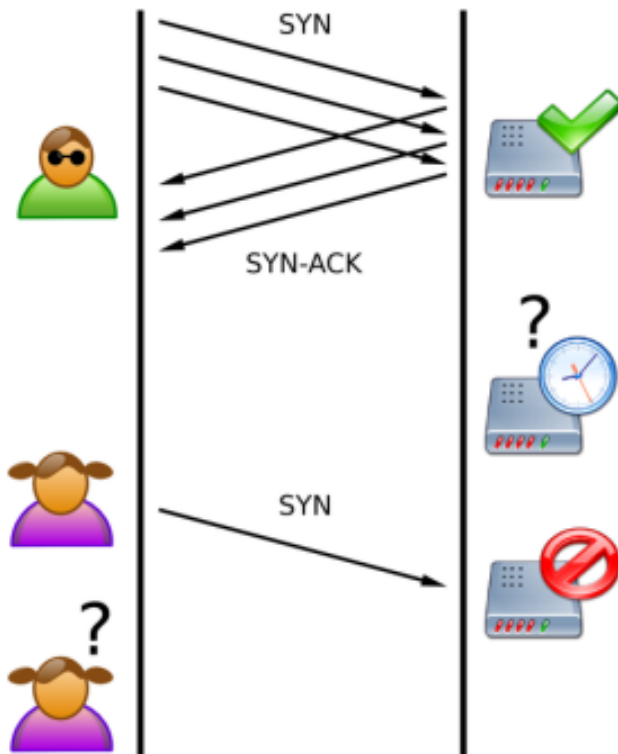
DOS ATTACK/SYN FLOOD

- Target dari Dos Attack adalah menghabiskan sumber daya router, misalnya overload CPU (100%) dan bandwidth
- Router akan dibanjiri dengan paket TCP/SYN, yang menyebabkan router akan merespon dengan paket TCP/SYN-ACK dan menunggu paket TCP/ACK

DOS ATTACK/SYN FLOOD



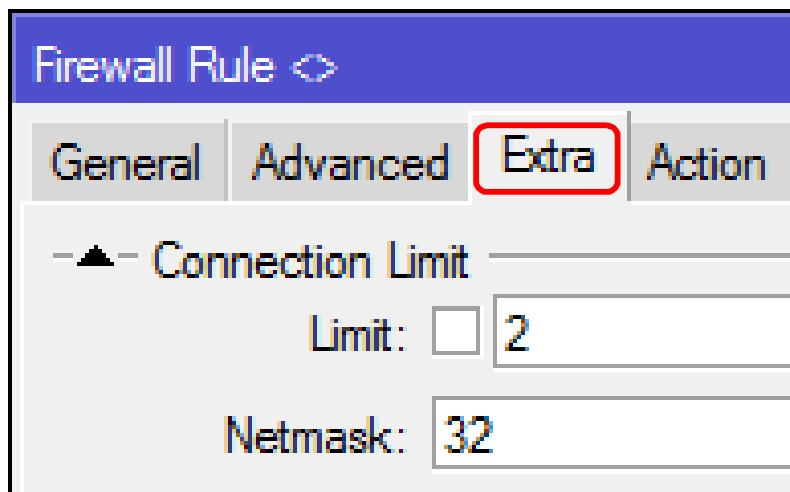
Pada kondisi normal koneksi TCP user dan server melalui three-way handshake




Attacker mengirim paket SYN terus menerus tapi tidak mengirim "ACK", ini akan menghabiskan sumber daya router, sehingga user yang sah justru akan ditolak

DOS ATTACK/SYN FLOOD

- Solusi: IP yang menggunakan koneksi sejumlah tertentu akan diasumsikan sebagai penyerang
- Tahap awal tahap menerapkan DOS protection dengan membuat daftar penyerang berdasarkan pada connection-limit



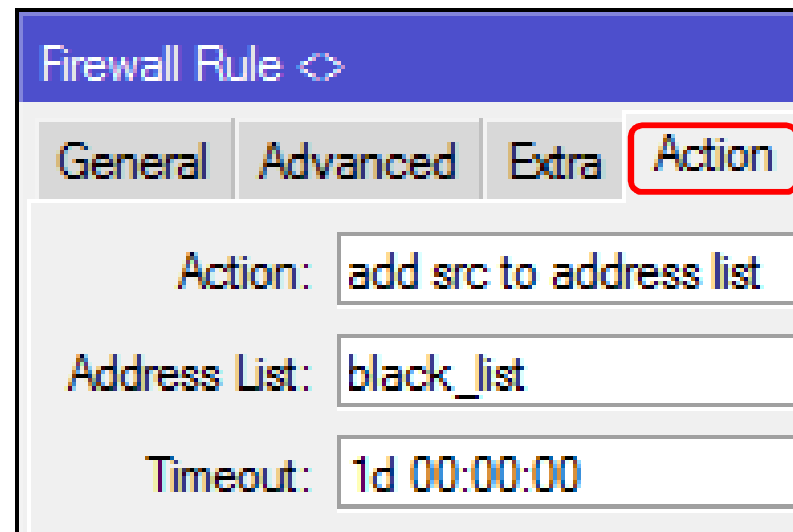
Firewall Rule 


General Advanced **Extra** Action

Connection Limit

Limit: 2

Netmask: 32



Firewall Rule 

General Advanced Extra **Action**

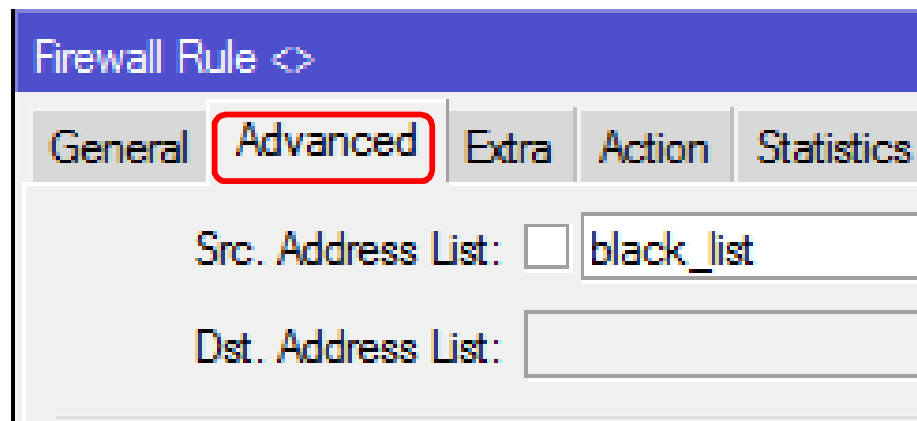
Action: add src to address list

Address List: black_list

Timeout: 1d 00:00:00

DOS ATTACK/SYN FLOOD

- Menerapkan “drop” ke daftar yang terdeteksi, untuk menghindari setiap koneksi TCP yang di drop membuat new connection, gunakan action tarpit

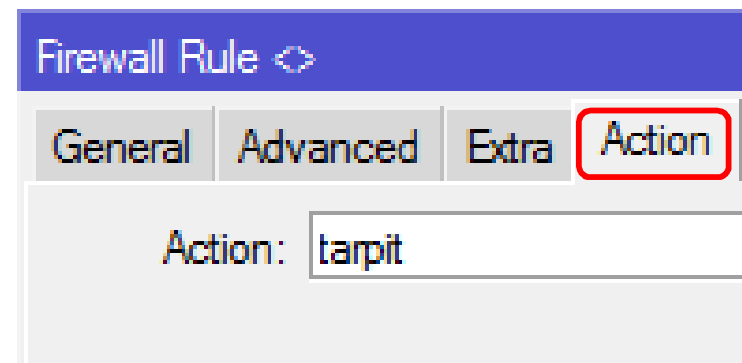


Firewall Rule <>

General **Advanced** Extra Action Statistics

Src. Address List: black_list

Dst. Address List:

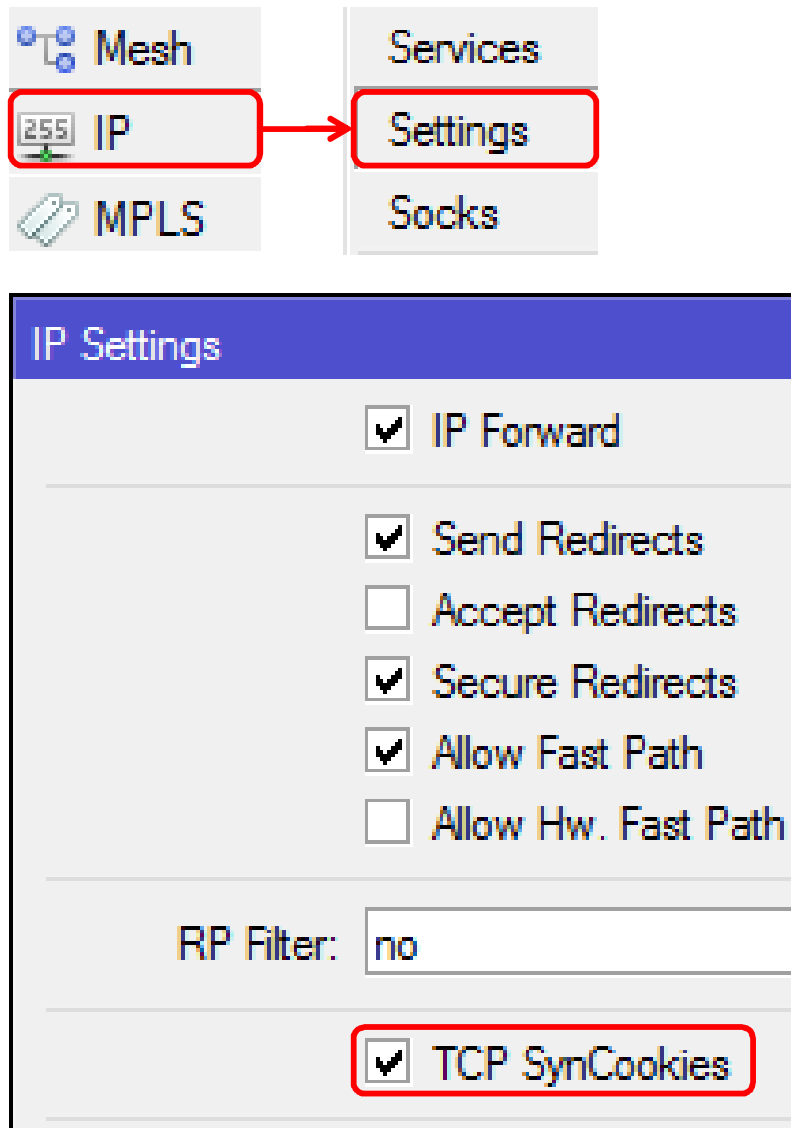


Firewall Rule <>

General Advanced Extra **Action**

Action: tarpit

DDOS ATTACKS



- A Distributed Denial of Service attack is very similar to DoS attack only it occurs from **multiple** Compromised systems
- Only thing that could help is “TCPSyn Cookie” option

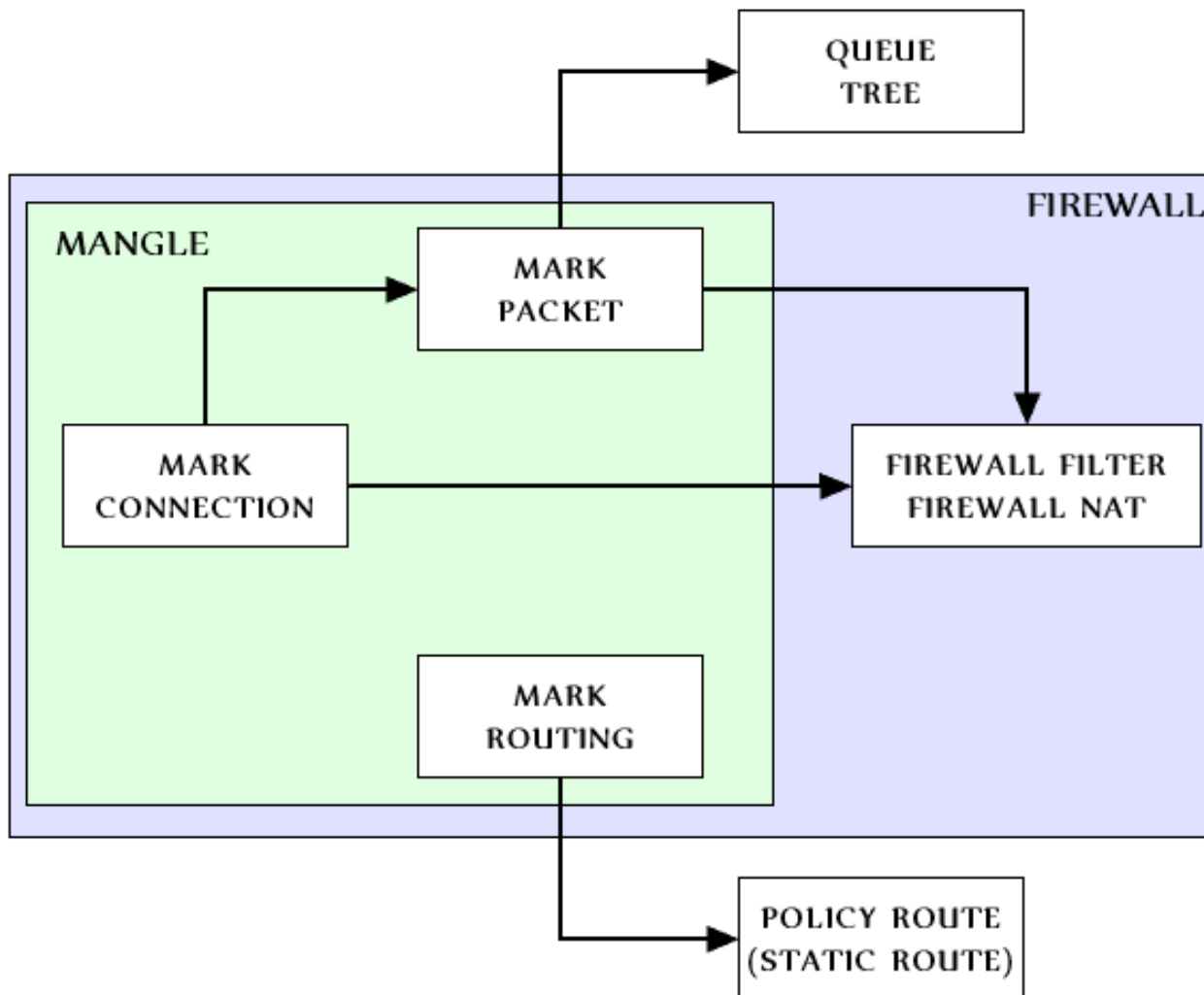
FIREWALL MANGLE

MANGLE

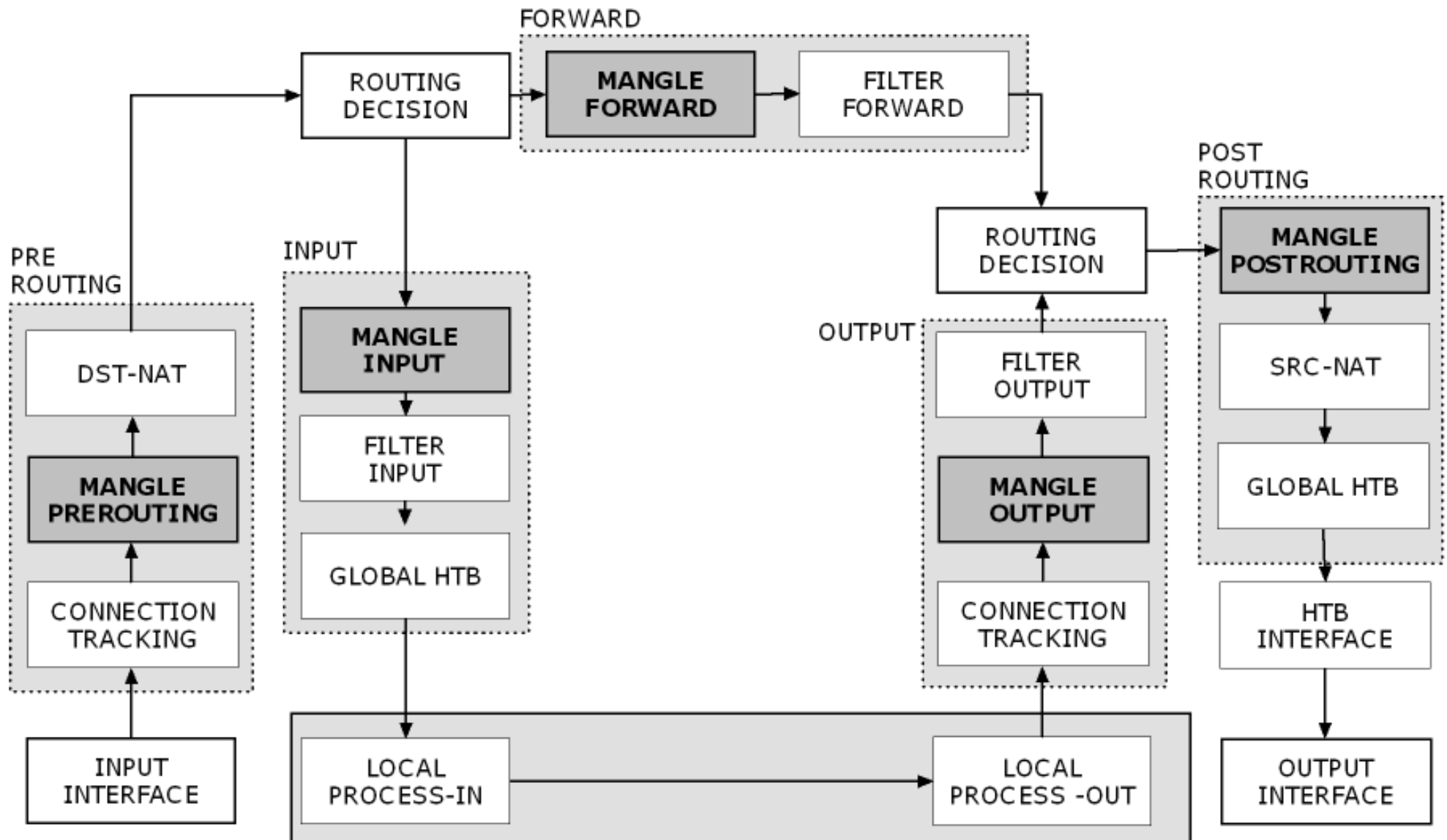
- Mangle hanya bisa digunakan di router yang sama, dan tidak terbaca oleh router lainnya.
- Pembacaan rule mangle akan dilakukan dari atas ke bawah secara berurutan.
- Setiap paket data hanya memiliki maksimal 1 conn-mark, 1 packet-mark, dan 1 route-mark
- Ada lima chain utama yaitu: prerouting, input, forward, output, postrouting, serta ada juga user define chain

MANGLE

- Mangle adalah cara untuk menandai (*mark*)



MANGLE

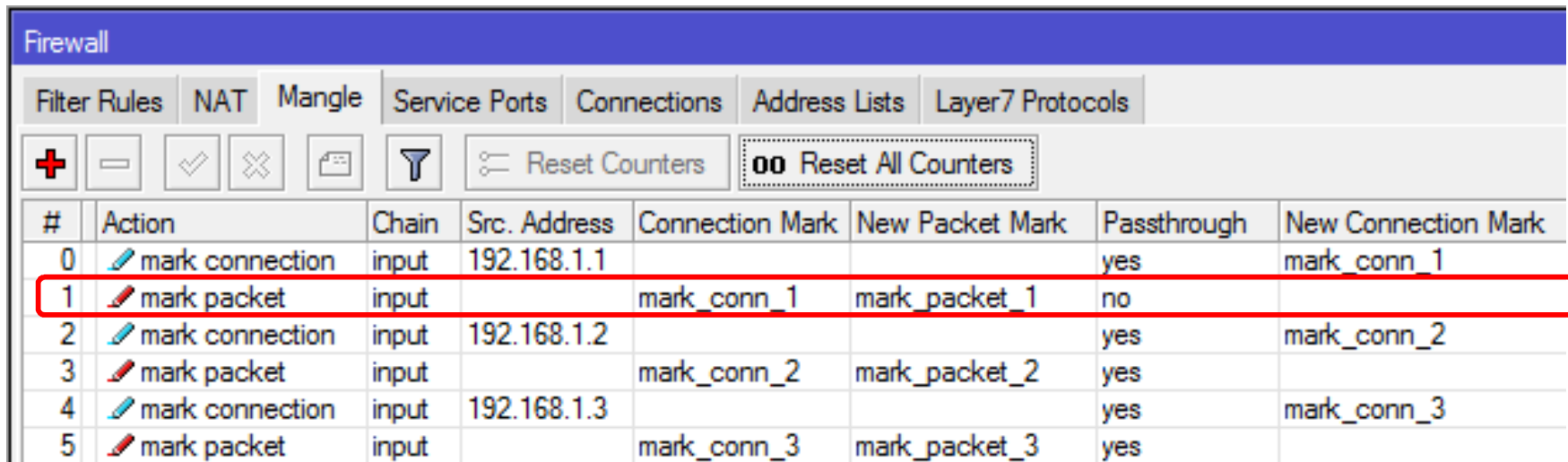


MANGLE (Action)

- **accept**, paket data diterima
- **jump**, paket data akan diforward ke chain lain sesuai parameter **jump-target**
- **return**, paket data akan dikembalikan ke chain asal sesuai urutan rule firewall jump sebelumnya.
- **passthrough**, mengabaikan rule dan akan diteruskan ke rule dibawahnya.

MANGLE (Action)

- Jika passthrough =no, paket data 192.168.1.1 akan melewati 2 rule saja.



The screenshot shows the Mikrotik Firewall configuration interface, specifically the Mangle tab. The interface includes a header bar with the title 'Firewall' and a navigation menu with tabs for 'Filter Rules', 'NAT', 'Mangle', 'Service Ports', 'Connections', 'Address Lists', and 'Layer7 Protocols'. Below the menu is a toolbar with icons for adding, deleting, enabling, disabling, and refreshing rules, along with buttons for 'Reset Counters' and 'Reset All Counters'. The main area contains a table of Mangle rules. Rule 1 is highlighted with a red border. The table has the following columns: '#', 'Action', 'Chain', 'Src. Address', 'Connection Mark', 'New Packet Mark', 'Passthrough', and 'New Connection Mark'.

#	Action	Chain	Src. Address	Connection Mark	New Packet Mark	Passthrough	New Connection Mark
0	mark connection	input	192.168.1.1			yes	mark_conn_1
1	mark packet	input		mark_conn_1	mark_packet_1	no	
2	mark connection	input	192.168.1.2			yes	mark_conn_2
3	mark packet	input		mark_conn_2	mark_packet_2	yes	
4	mark connection	input	192.168.1.3			yes	mark_conn_3
5	mark packet	input		mark_conn_3	mark_packet_3	yes	

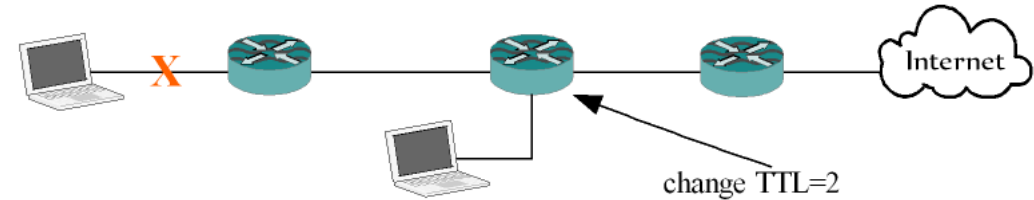
MANGLE (Action)

- **mark-connection**, menandai paket “new” dari sebuah connection.
- **mark-packet**, menandai semua paket data.
- **mark-routing**, menandai jalur routing
- **change MSS**, mengubah besar MSS dari paket di paket header, agar tidak terfragmentasi ketika menggunakan koneksi VPN

MANGLE (Action)

Change TTL, default 64,
berkurang satu setiap kali
forwarding.

Router tidak melewatkan
trafik ke route selanjutnya
jika TTL yang diterima 1



Mangle Rule <>

General Advanced Extra Action Statistics

Chain: forward

Out. Interface: ether1

Mangle Rule <>

General Advanced Extra Action Statistics

Action: change TTL

Log

Log Prefix: _____

- TTL Action _____

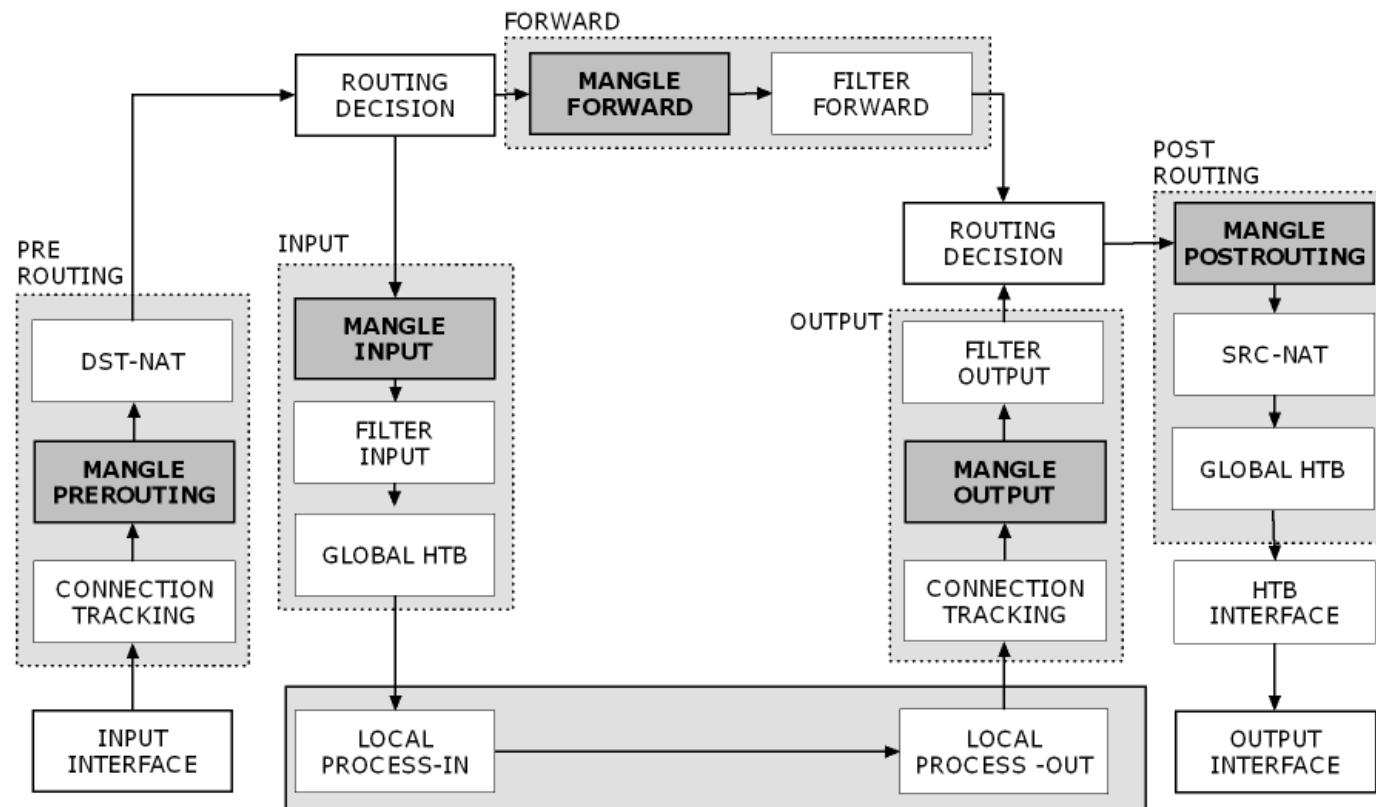
change increment decrement

New TTL: 2

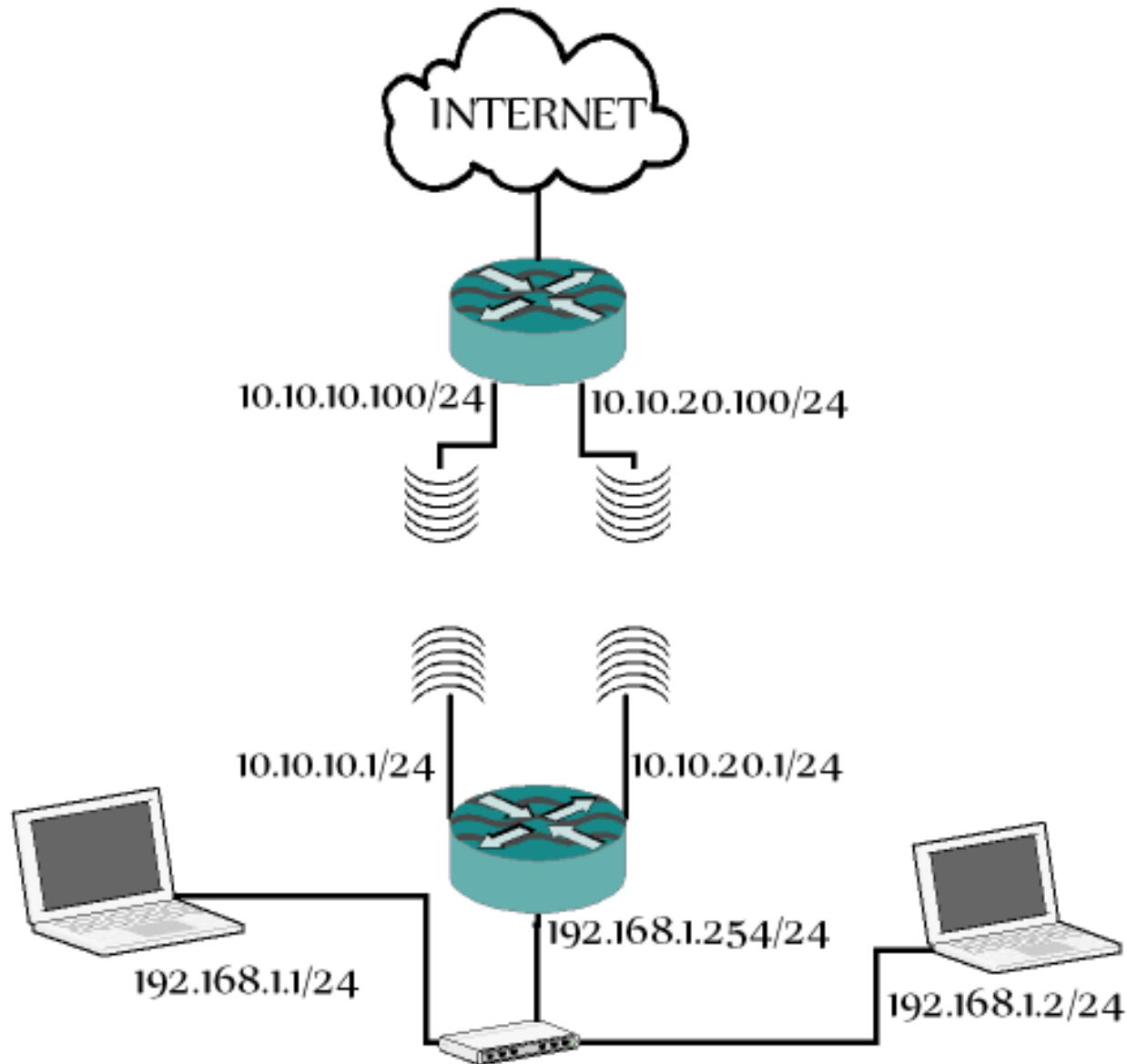
Passthrough

MARK ROUTING

- Dilakukan sebelum proses routing decision, gunakan **prerouting** untuk trafik yang menuju/ melalui router. Untuk trafik dari router **output**.



MARK ROUTING



MARK ROUTING

- Mark Routing

Mangle Rule <192.168.1.2>

General Advanced Extra Action

Chain: prerouting

Src. Address: 192.168.1.2

Dst. Address:

Mangle Rule <192.168.1.2>

General Advanced Extra Action Statistics

Action: mark routing

New Routing Mark: route_isp2

Passthrough

- NAT

NAT Rule <>

General Advanced Extra Action

Chain: srcnat

Src. Address:

NAT Rule <>

General Advanced Extra Action

Action: masquerade

MARK ROUTING

Route <0.0.0.0/0>

General | Attributes

Dst. Address: 0.0.0.0/0

Gateway: 10.10.20.100 reachable wlan2

Target Scope: 10

Routing Mark: route_jsp2

Route List

Routes | Nexthops | Rules | VRF

+ - ✓ ✗ 📄 🔍

	Dst. Address	Gateway	Distance	Routing Mark
AS	▶ 0.0.0.0/0	10.10.10.100 reachable wlan 1	1	
AS	▶ 0.0.0.0/0	10.10.20.100 reachable wlan2	1	route_jsp2
DAC	▶ 10.10.10.0/24	wlan1 reachable	0	
DAC	▶ 10.10.20.0/24	wlan2 reachable	0	
DAC	▶ 192.168.1.0/24	bridge1 reachable	0	

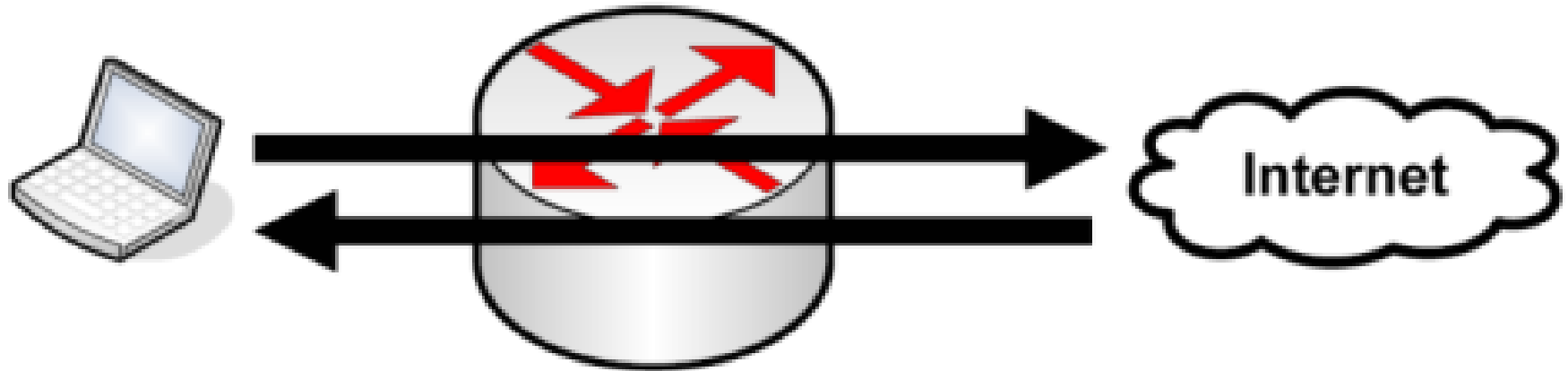
PROXY

PROXY

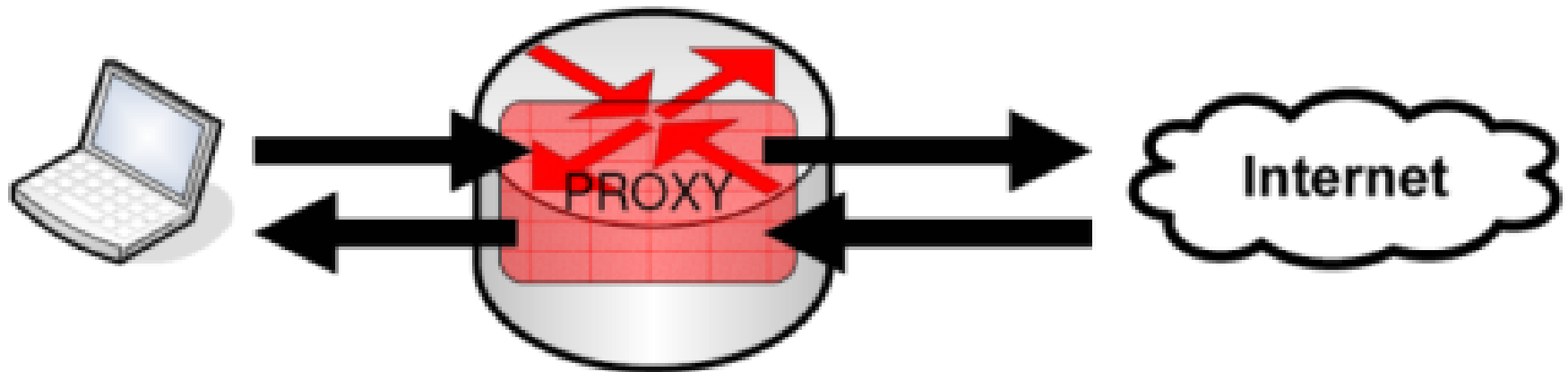
- Mempercepat proses browsing dengan cara menyimpan data-data yang sudah pernah diakses dari internet di cache, kemudian jika data-data tersebut diakses lagi, Proxy akan mengambil data tersebut dari cache, sehingga tidak perlu lagi mengambil dari internet, hal ini akan lebih menghemat bandwidth dan juga mempercepat akses.

PROXY

- o Koneksi tanpa proxy



- o Koneksi dengan proxy



PROXY

MEDIA PENYIMPANAN

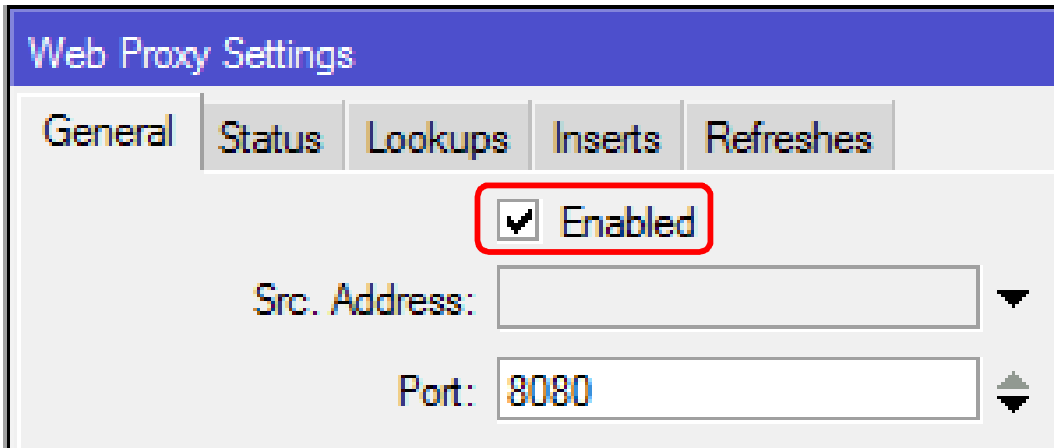
- PC Router :
 - 1 harddisk (system + cache)
 - 1 DOM (system) + 1 harddisk (cache)
- Routerboard (RB450G, RB433UAH, RB1000)
 - Internal storage/NAND (system) + kartu memori tambahan (CF/Micro-SD) untuk cache

PROXY

FITUR PROXY:

- Regular HTTP Proxy, konfigurasi di browser
- Transparent Proxy, konfigurasi hanya di router
- HTTP caching
- FTP caching
- Access list
- Cache access List
- Direct access list
- Logging

PROXY



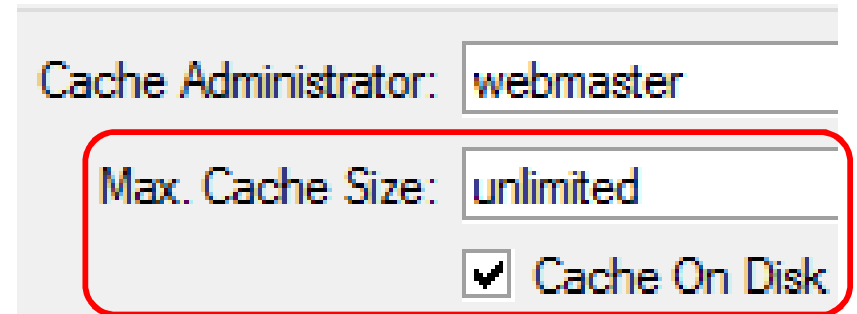
Web Proxy Settings

General Status Lookups Inserts Refreshes

Enabled

Src. Address:

Port:



Cache Administrator:

Max. Cache Size:

Cache On Disk

- **Tanpa cache**
Max Cache Size=none,
- **Cache to RAM,**
Cache On Disk=no
- **Cache to Disk,**
Cache On Disk=yes

PROXY

New NAT Rule

General | Advanced | Extra | Action

Chain: dstnat

Src. Address:

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port: 80

Any. Port:

In. Interface: ether1

Firewall

Filter Rules | **NAT** | Mangle | Service Ports | Connections | Address L

+ - ✓ ✗ [icon] [icon] [icon] Reset Counters [icon] Reset

#	Action	Chain	Protocol	Dst. Port	In. Interface
0	masquerade	srcnat			
1	redirect	dstnat	6 (tcp)	80	ether1

NAT Rule <80>

General | Advanced | Extra | **Action** | Statistics

Action: redirect

Log

Log Prefix:

To Ports: 8080

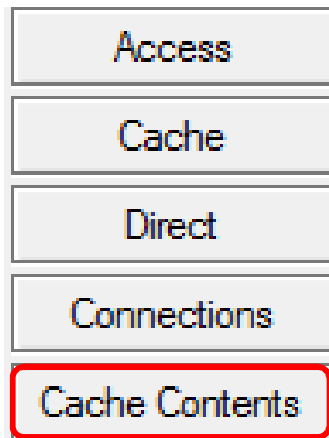
PROXY

Web Proxy Settings				
General	Status	Lookups	Inserts	Refreshes
Uptime:	00:07:56			
Requests:	539			
Hits:	83			
Cache Used:	1 074 KiB			
Total RAM Used:	1 099 KiB			
Received From Servers:	2 425 KiB			
Sent To Clients:	3 072 KiB			
Hits Sent To Clients:	232 KiB			

Ulangi browsing dan download yang telah dilakukan, amati kecepatan serta amati pula, perubahan *cache* yang tersedia.

Hits, menunjukkan keberhasilan penggunaan proxy

PROXY










Alamat yang sudah masuk bisa dilihat di menu *Cache Contents*

Web Proxy Cache Contents			
	URI	File Size	Last Modified
	http://i.mt.lv/banner_mum_generic.png	12 kB	Jan/01/2002 03:17:50
	http://i.mt.lv/flags/australia.png	3 kB	Jan/01/2002 03:17:57
	http://i.mt.lv/flags/brazil.png	3 kB	Jan/01/2002 03:17:59
	http://i.mt.lv/flags/china.png	3 kB	Jan/01/2002 03:17:55
	http://i.mt.lv/flags/indonesia.png	2 kB	Jan/01/2002 03:17:56
	http://i.mt.lv/flags/peru.png	2 kB	Jan/01/2002 03:18:02
	http://i.mt.lv/made_mfm.png	16 kB	Jan/01/2002 03:18:05
	http://l.yimg.com/a/i/tb/yso/16x16_m...	0 kB	Jan/01/2002 03:17:57
	http://l.yimg.com/a/i/tb/yso/16x16_vit...	0 kB	Jan/01/2002 03:17:59
	http://l.yimg.com/a/i/tb/yso/22x22_ca...	0 kB	Jan/01/2002 03:18:01
	http://l.yimg.com/a/i/tb/yso/22x22_ca...	0 kB	Jan/01/2002 03:17:53
	http://l.yimg.com/a/i/tb/yso/22x22_inf...	0 kB	Jan/01/2002 03:18:01
	http://l.yimg.com/a/i/tb/yso/22x22_inf...	0 kB	Jan/01/2002 03:17:53
	http://l.yimg.com/a/i/tb/yso/active-20...	0 kB	Jan/01/2002 03:17:54
	http://l.yimg.com/a/i/tb/yso/app_icon-...	8 kB	Jan/01/2002 03:17:55
	http://l.yimg.com/a/i/tb/yso/btn_close...	0 kB	Jan/01/2002 03:17:46
	http://l.yimg.com/a/i/tb/yso/gripper2-2...	3 kB	Jan/01/2002 03:17:56
	http://l.yimg.com/a/i/tb/yso/intro_heas...	12 kB	Jan/01/2002 03:18:04
	http://l.yimg.com/a/i/tb/yso/introbk-20...	3 kB	Jan/01/2002 03:17:54
	http://l.yimg.com/a/i/tb/yso/option_bt...	0 kB	Jan/01/2002 03:17:59

PROXY:Access

Web Proxy Access

      Reset Counters  Reset All Counters

#	Src. Address	Dst. Address	Dst. Port	Dst. Host	Path	Action	Redirect To	Hits
0	192.168.1.1			www.google.com		deny		1
1				www.mikrotik.com	/support.html	deny		3

Web Proxy Rule

Src. Address:

Dst. Address:

Dst. Port:

Local Port:

Dst. Host:

Path:

Method:

Action:

Redirect To:









Hits:

Tambahkan satu aturan lagi, **semua** tidak diperbolehkan mengakses `www.mikrotik.com/support.html`, namun diperbolehkan melakukan akses ke `www.mikrotik.com/download`


Hits, menunjukkan keberhasilan penggunaan proxy

PROXY:Access - Redirect

Web Proxy Access

       Reset Counters  Reset All Counters

#	Dst. Address	Dst. Port	Path	Action	Redirect To	Hits
0				deny		1
1			/support.html	deny	www.mikroline.com	5

Web Proxy Rule 

Src. Address:

Dst. Address:

Dst. Port:

Local Port:

Dst. Host:

Path:

Method:

Action:

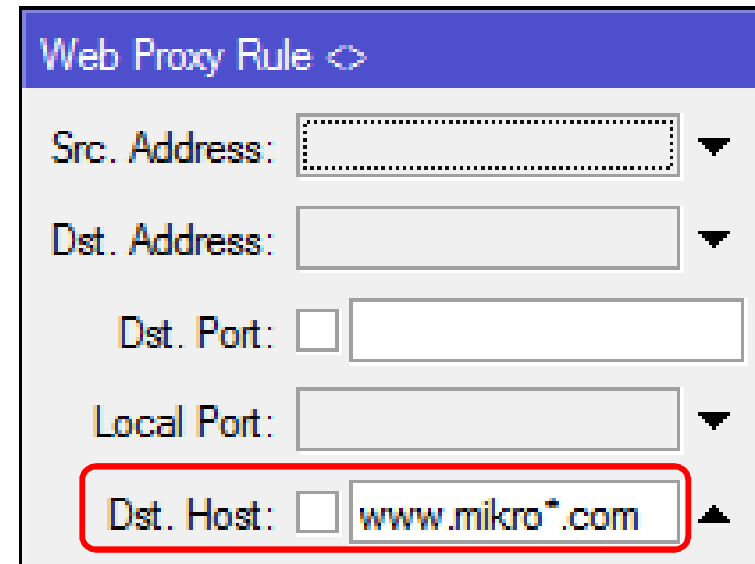
Redirect To:

URL Filtering

Memfilter alamat host
*= karakter apapun

- www.mikro*.com,
untuk filter host:
- www.mikroline.com,
www.mikrotik.com

? = satu karakter
www.mi?????????.com,
untuk filter host:
www.mikroline.com,
www.microsoft.com



Web Proxy Rule <>

Src. Address:

Dst. Address:

Dst. Port:

Local Port:

Dst. Host: www.mikro*.com



Local Port:

Dst. Host: www.mi?????????.com

Path:

PROXY:Cache

- Menentukan objek mana yang disimpan pada cache, sebagai contoh akses dari laptop dengan IP Address 192.168.1.1 ke website MikroTik, akan disimpan di proxy.

PROXY:Cache

Web Proxy Cache

+ - ✓ ✗ 📄 🏠 ⚙️ Reset Counters ⚙️ Reset

#	Src. Address	Dst. Host	Action	Hits
0	192.168.1.1	www.mikrotik.com	allow	2

Web Proxy Rule <192.168.1.1>

Src. Address: 192.168.1.1

Dst. Address:

Dst. Port:

Local Port:

Dst. Host: www.mikrotik.com

Path:

Method:

Action:

Hits: 2

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

allow,
masukkan dalam
cache

deny,
tidak dimasukkan
ke dalam cache

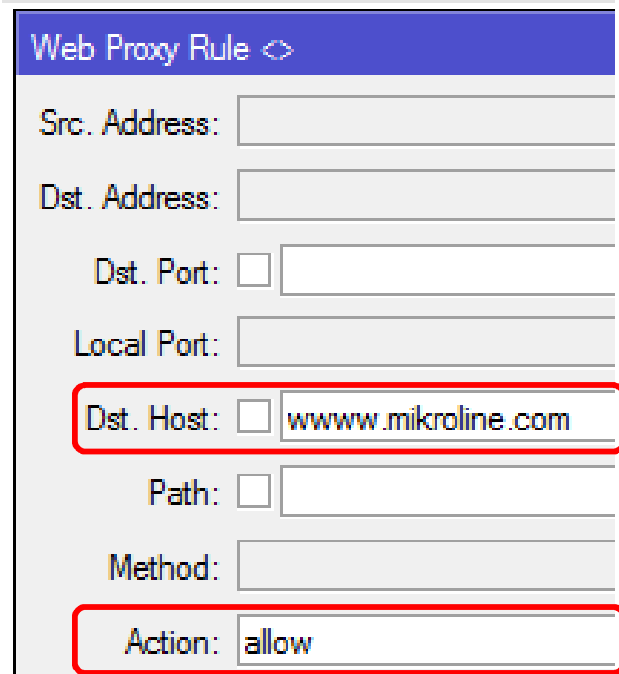
PROXY:Direct

- Mengatur koneksi mana yang diakses secara langsung dan yang melalui proxy server



Web Proxy Direct

#	Src. Address	Dst. Host	Action
0	<input checked="" type="checkbox"/>	www.mikroline.com	allow



Web Proxy Rule

Src. Address:

Dst. Address:

Dst. Port:

Local Port:

Dst. Host:

Path:

Method:

Action:

allow, akan langsung mengakses data ke internet

deny, akan mencari dulu di cache proxy jika tidak ditemukan akan melakukan proses yang sama dengan allow

HTTP LOGGING

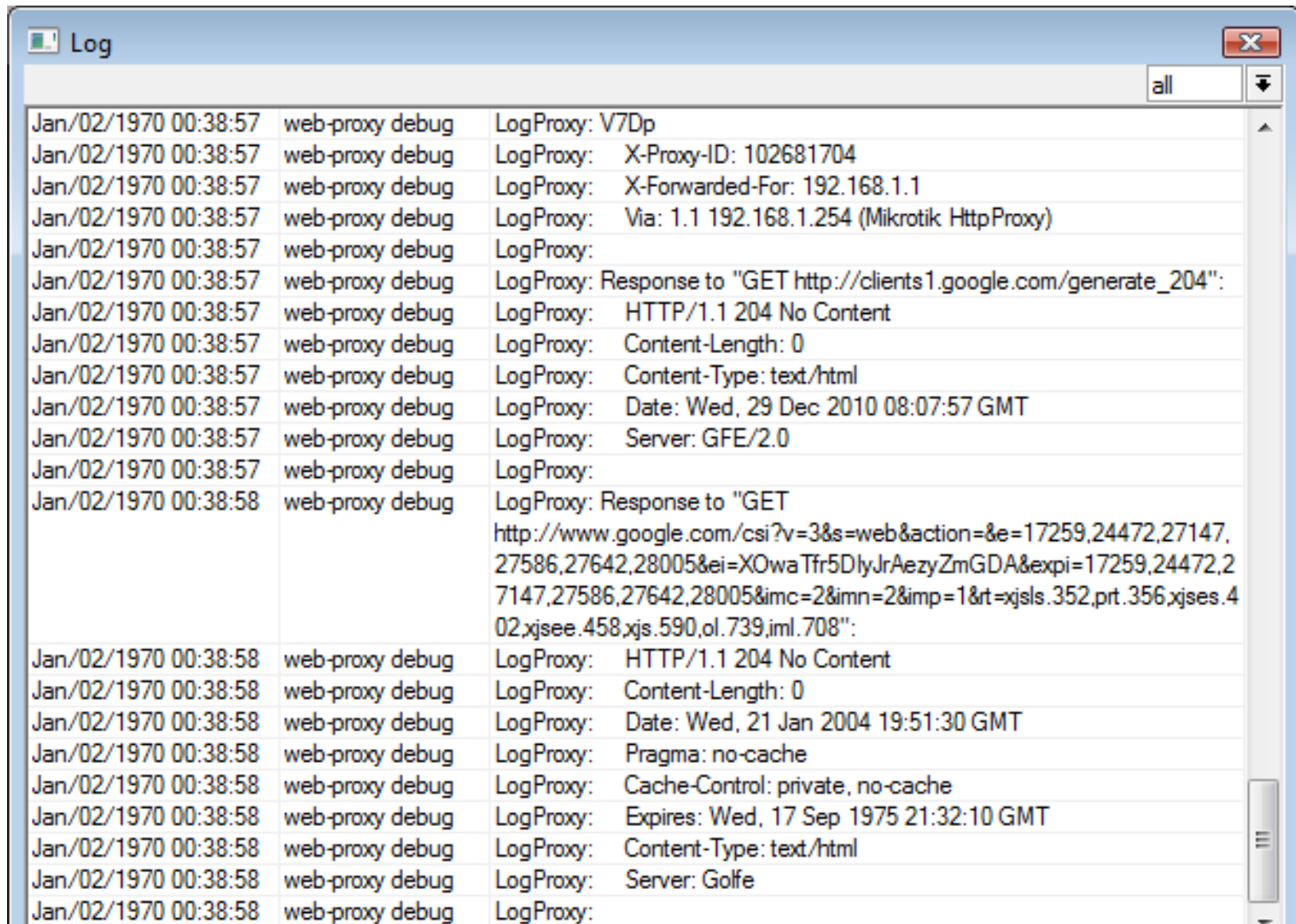
- HTTP Logging mencatat proses proxy yang terjadi selama proxy digunakan

The screenshot displays the Mikrotik WinBox interface. On the left, the 'System' menu is expanded to 'Logging'. The 'Rules' tab is selected, showing a table of logging rules. A red box highlights the '+' icon for adding a new rule. Below the table, a detailed view of the 'web-proxy' rule is shown, with red boxes highlighting the 'Topics', 'Prefix', and 'Action' fields.

	Topics	Prefix	Action
*	critical		echo
*	error		memory
*	info		memory
*	warning		memory
	web-proxy	LogProxy	memory

Log Rule <web-proxy>	
Topics:	<input type="checkbox"/> web-proxy
Prefix:	LogProxy
Action:	memory

HTTP LOGGING

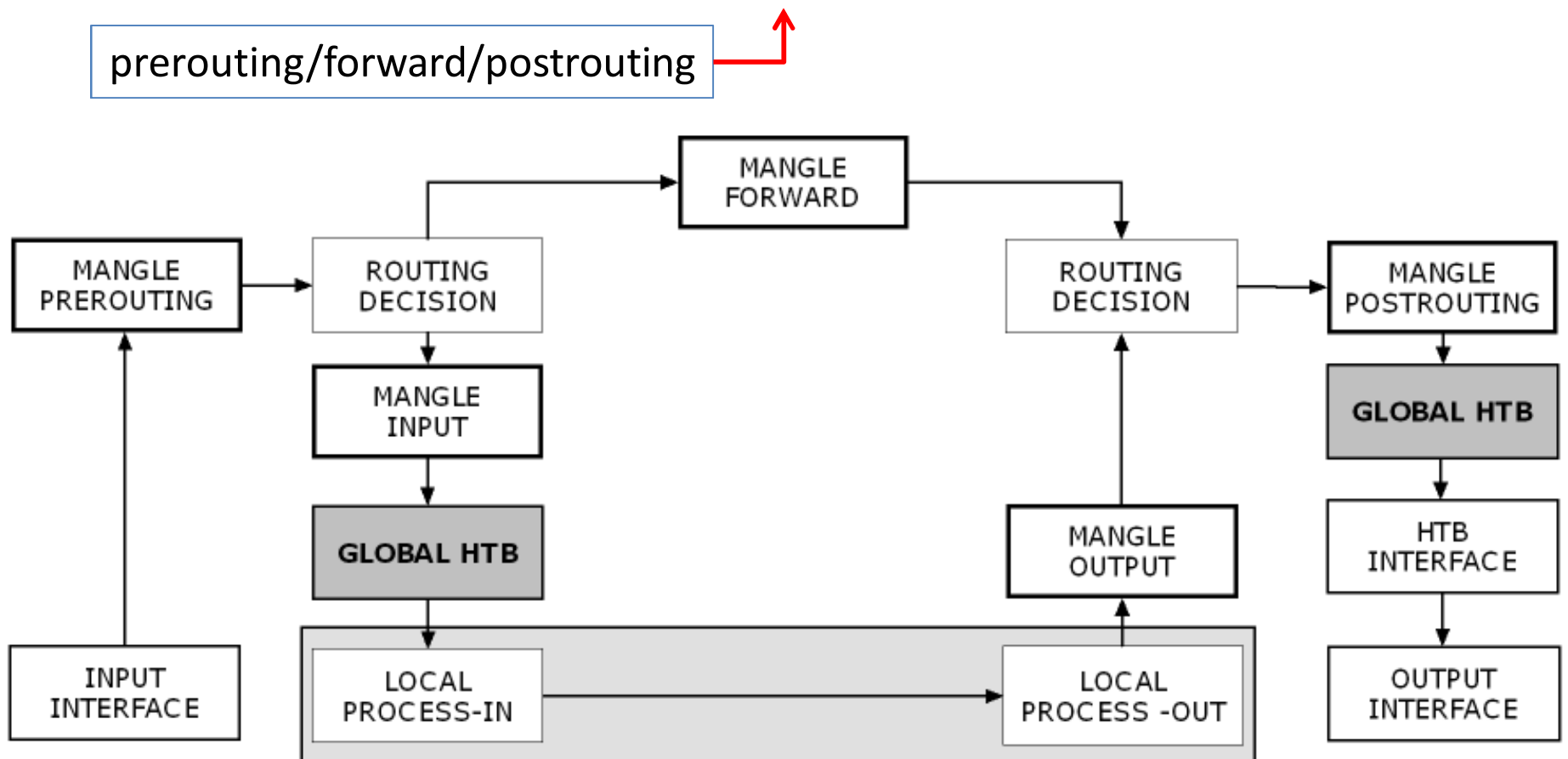
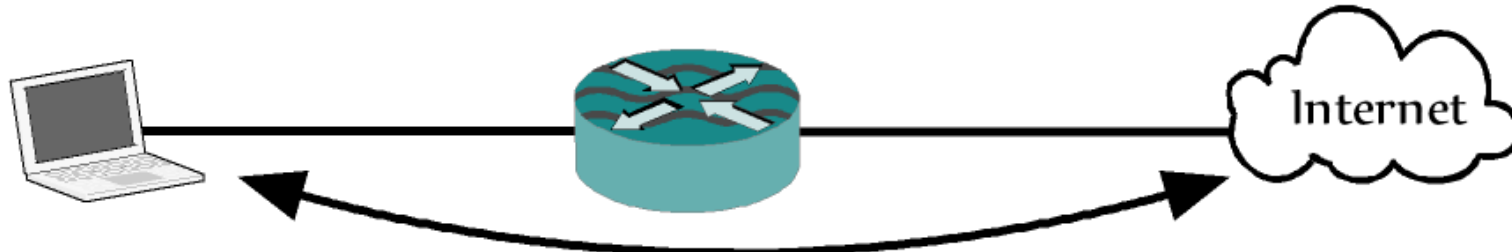


Timestamp	Level	Message
Jan/02/1970 00:38:57	web-proxy debug	LogProxy: V7Dp
Jan/02/1970 00:38:57	web-proxy debug	LogProxy: X-Proxy-ID: 102681704
Jan/02/1970 00:38:57	web-proxy debug	LogProxy: X-Forwarded-For: 192.168.1.1
Jan/02/1970 00:38:57	web-proxy debug	LogProxy: Via: 1.1 192.168.1.254 (Mikrotik HttpProxy)
Jan/02/1970 00:38:57	web-proxy debug	LogProxy:
Jan/02/1970 00:38:57	web-proxy debug	LogProxy: Response to "GET http://clients1.google.com/generate_204":
Jan/02/1970 00:38:57	web-proxy debug	LogProxy: HTTP/1.1 204 No Content
Jan/02/1970 00:38:57	web-proxy debug	LogProxy: Content-Length: 0
Jan/02/1970 00:38:57	web-proxy debug	LogProxy: Content-Type: text/html
Jan/02/1970 00:38:57	web-proxy debug	LogProxy: Date: Wed, 29 Dec 2010 08:07:57 GMT
Jan/02/1970 00:38:57	web-proxy debug	LogProxy: Server: GFE/2.0
Jan/02/1970 00:38:57	web-proxy debug	LogProxy:
Jan/02/1970 00:38:58	web-proxy debug	LogProxy: Response to "GET http://www.google.com/csi?v=3&s=web&action=&e=17259,24472,27147, 27586,27642,28005&ei=XOwaTfr5DlyJrAezyZmGDA&expi=17259,24472,2 7147,27586,27642,28005&imc=2&imn=2&imp=1&rt=xjsls.352,prt.356,xjses.4 02,xjsee.458,xjs.590,ol.739,iml.708":
Jan/02/1970 00:38:58	web-proxy debug	LogProxy: HTTP/1.1 204 No Content
Jan/02/1970 00:38:58	web-proxy debug	LogProxy: Content-Length: 0
Jan/02/1970 00:38:58	web-proxy debug	LogProxy: Date: Wed, 21 Jan 2004 19:51:30 GMT
Jan/02/1970 00:38:58	web-proxy debug	LogProxy: Pragma: no-cache
Jan/02/1970 00:38:58	web-proxy debug	LogProxy: Cache-Control: private, no-cache
Jan/02/1970 00:38:58	web-proxy debug	LogProxy: Expires: Wed, 17 Sep 1975 21:32:10 GMT
Jan/02/1970 00:38:58	web-proxy debug	LogProxy: Content-Type: text/html
Jan/02/1970 00:38:58	web-proxy debug	LogProxy: Server: Golfe
Jan/02/1970 00:38:58	web-proxy debug	LogProxy:

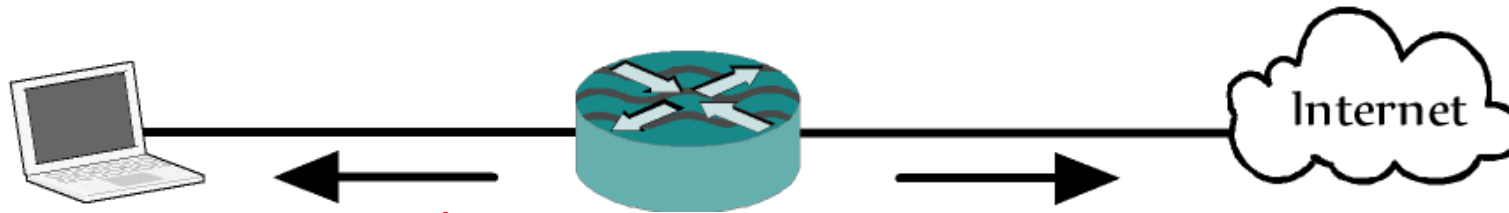
QUEUE TREE

- Pengaturan bandwidth dapat dilakukan di Queue Tree dan dilakukan di parent, yaitu parent,
 - a) Virtual Interface (Global HTB)
 - b) HTB Interface
- Queue Tree harus menggunakan Mangle

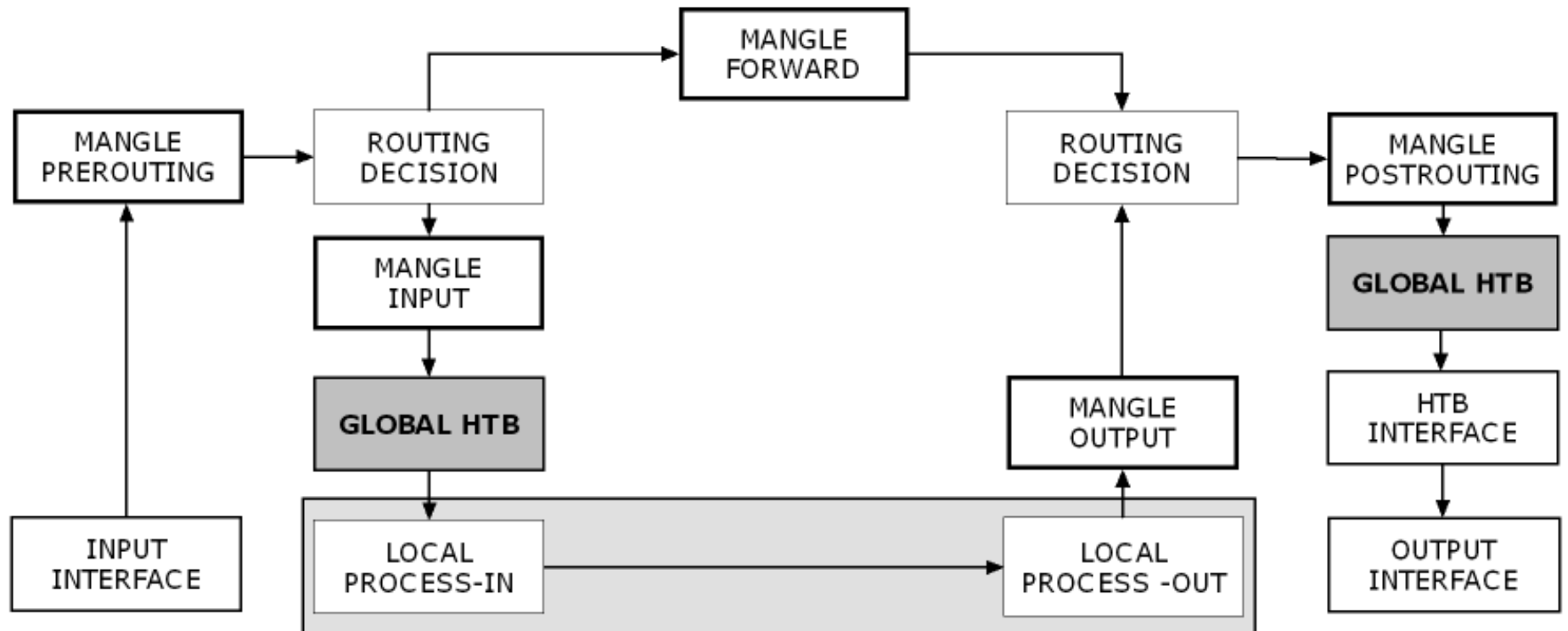
VIRTUAL INTERFACE (GLOBAL HTB)



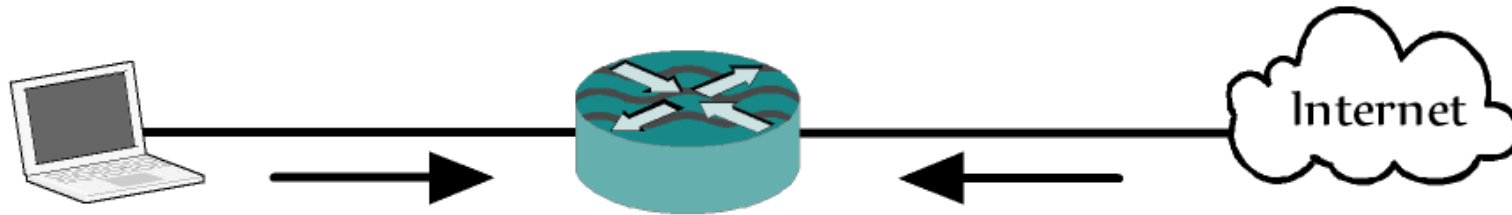
VIRTUAL INTERFACE (GLOBAL HTB)



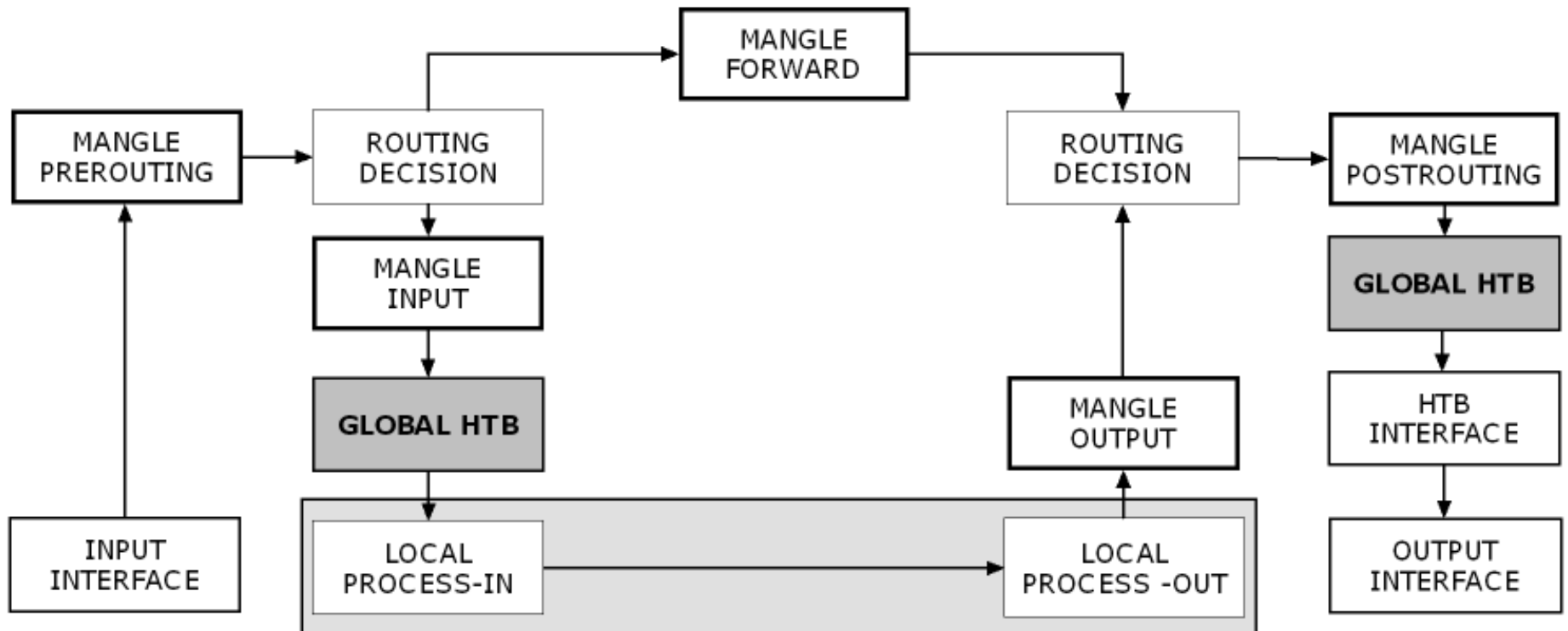
output/postrouting



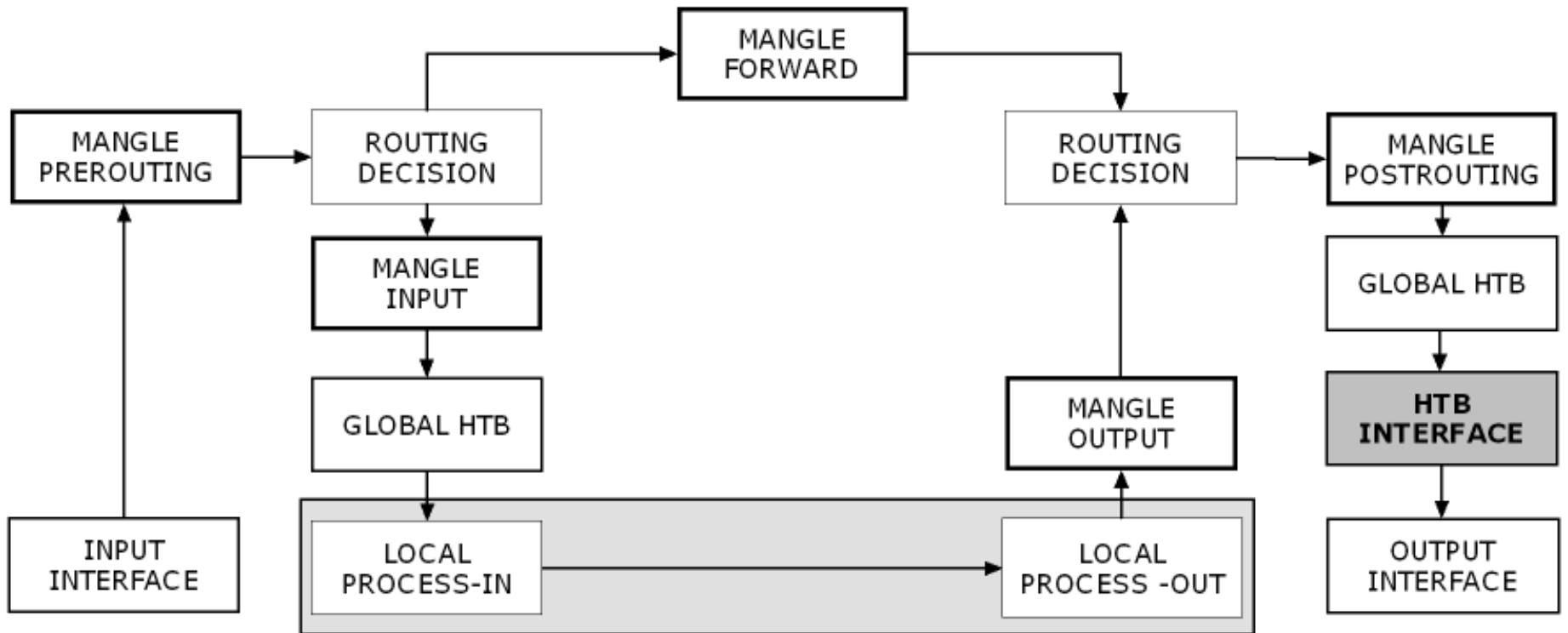
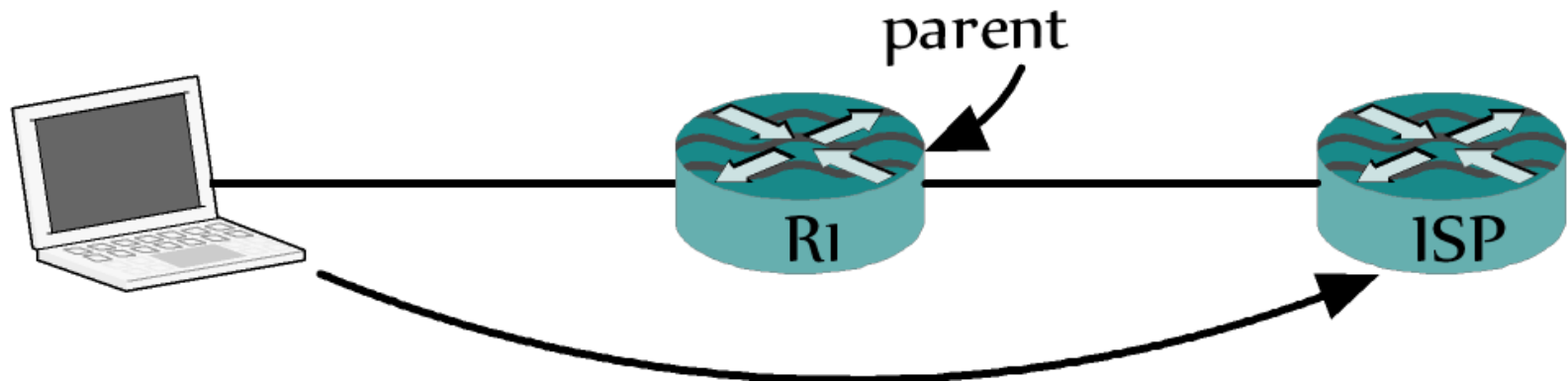
VIRTUAL INTERFACE (GLOBAL HTB)



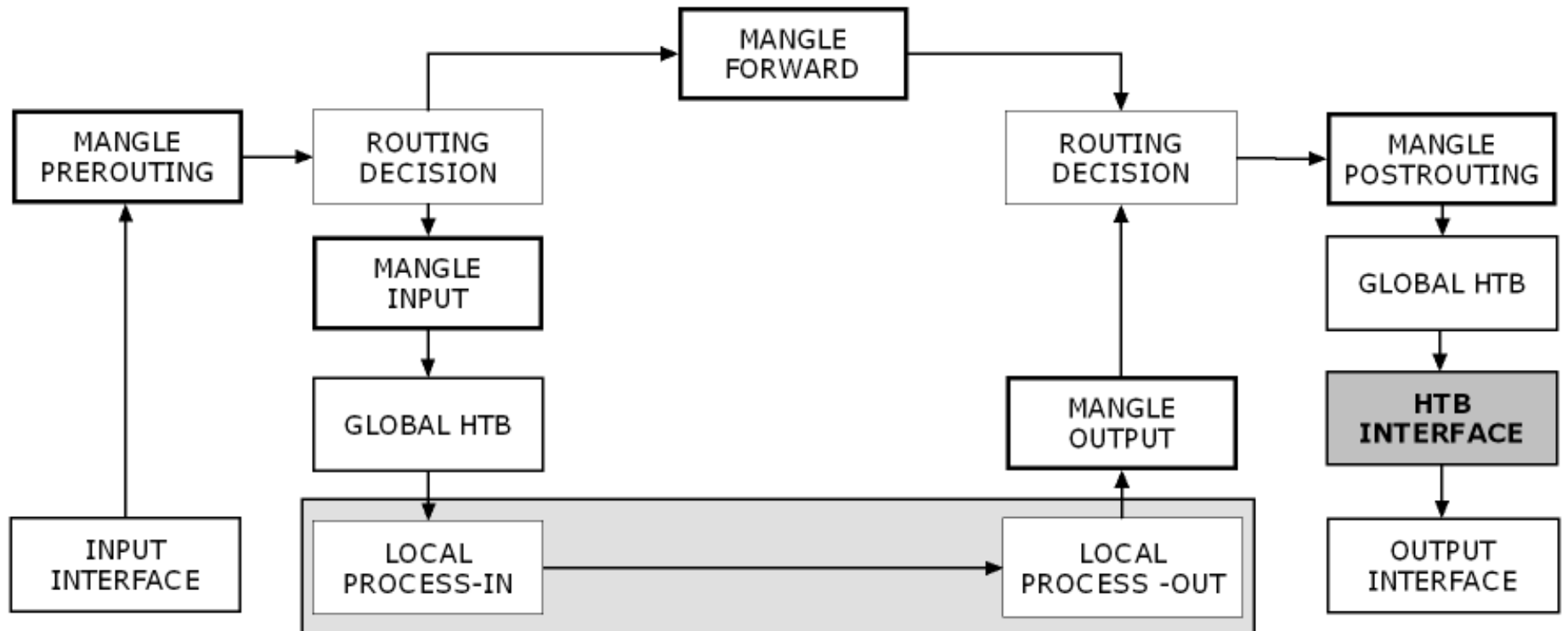
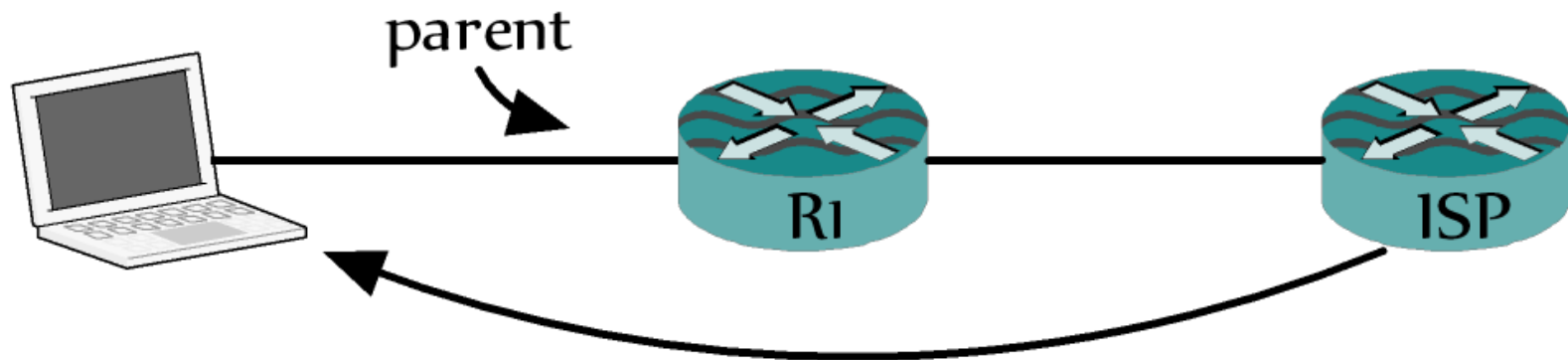
input/prerouting



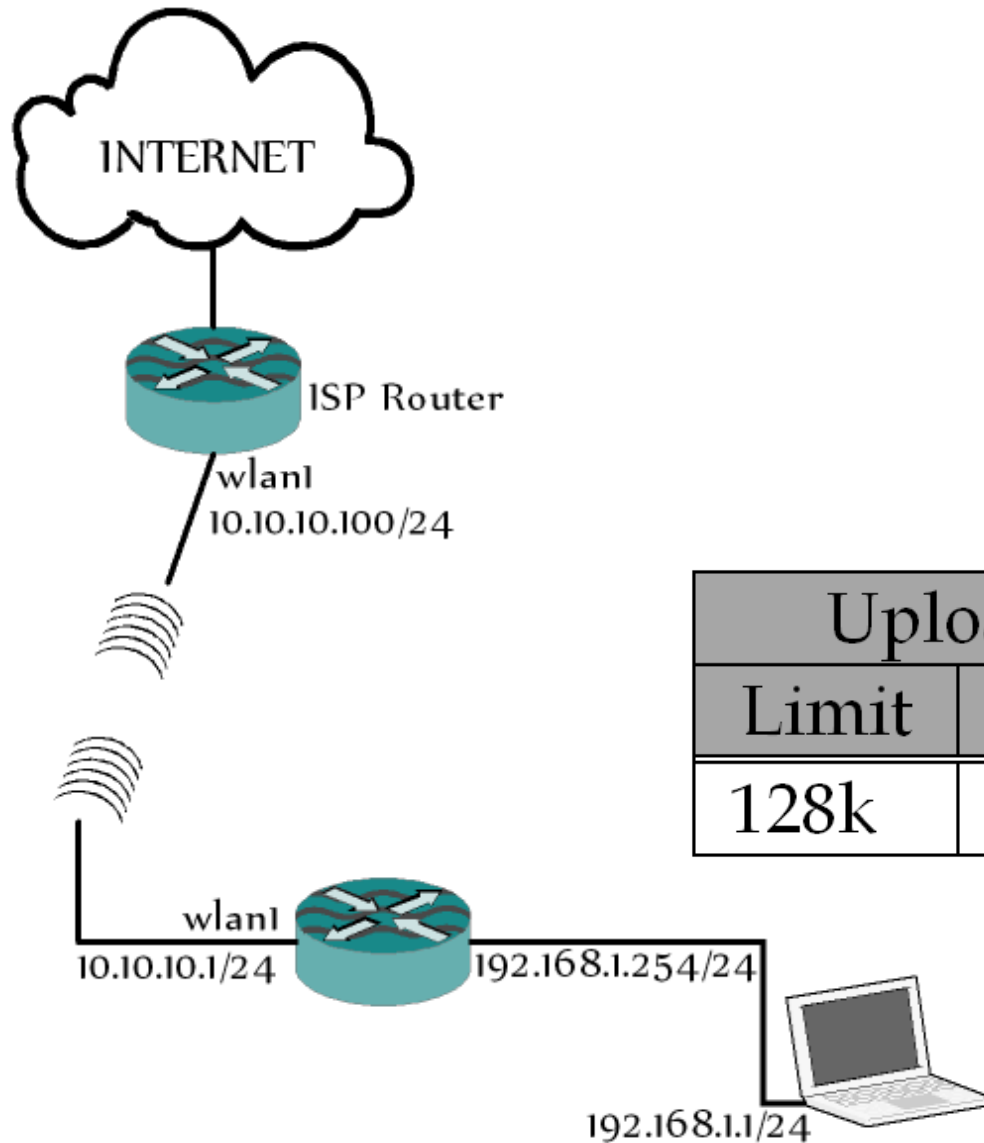
HTB INTERFACE



HTB INTERFACE



MANGLE - QUEUE TREE



Upload		Download	
Limit	Max	Limit	Max
128k	256k	512k	1M

MARK CONNECTION - USER1

New Mangle Rule

General | Advanced | Extra | Action | Statistics

Chain: forward

Src. Address: 192.168.1.1

Firewall

Filter Rules | NAT | Mangle | Service Ports | Connection

+ - ✓ ✗ [icon] [icon] Reset Counter

#	Action	Chain	Src. Address
0	mark connection	forward	192.168.1.1

Mangle Rule <192.168.1.1>

General | Advanced | Extra | Action | Statistics

Action: mark connection

New Connection Mark: Mark_Conn_User01

Passthrough

MARK PACKET - USER1

Mangle Rule

General | Advanced | Extra | Action | Statistics

Chain: forward

Src. Address:

Packet Mark:

Connection Mark: Mark_Conn_User01

Firewall

Filter Rules | NAT | Mangle | Service Ports | Connection

Reset Counters

#	Action	Chain	Src. Address
0	mark connection	forward	192.168.1.1
1	mark packet	forward	

Mangle Rule

General | Advanced | Extra | Action | Statistics

Action: mark packet









New Packet Mark: Mark_Packet_User01



Passthrough

QUEUE TREE

Queue List

Simple Queues | Interface Queues | **Queue Tree** | Queue Types

       Reset Counters  Reset All Counters

	Name	Parent	Packet Marks	Limit At (bits/s)	Max Limit (bits/s)	Avg. Rate
	Queue_Download	ether1	Mark_Packet_User01	512k	1M	0 bps
	Queue_Upload	wlan1	Mark_Packet_User01	128k	256k	0 bps

Queue <Queue_Download>

General | **Statistics**

Name:

Parent: ▼

Packet Marks: ▼ ▲

Queue Type: ▼

Priority:

Limit At: ▲ bits/s

Max Limit: ▲ bits/s

Queue <Queue_Upload>

General | **Statistics**

Name:

Parent: ▼

Packet Marks: ▼ ▲

Queue Type: ▼

Priority:

Limit At: ▲ bits/s

Max Limit: ▲ bits/s

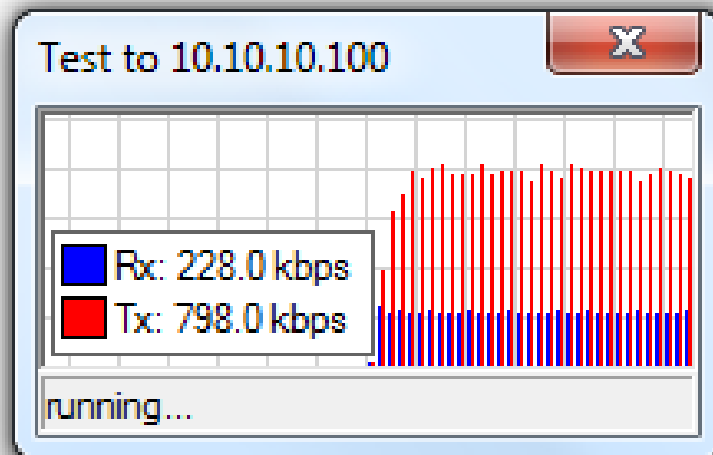
BANDWIDTH TEST

Queue List

Simple Queues | Interface Queues | Queue Tree | Queue Types

00 Reset All Counters

Name	Parent	Packet Marks	Limit At (bits/s)	Max Limit (bits/s)	Avg. Rate
Queue_Download	ether1	Mark_Packet_User01	512k	1M	944.8 kbps
Queue_Upload	wlan1	Mark_Packet_User01	128k	256k	258.3 kbps



MikroTik Bandwidth Test v0.1

Mikr

Address:

Protocol:

Local Tx Size: bytes

Remote Tx Size: bytes

Direction:

HTB

HTB & QUEUE TREE

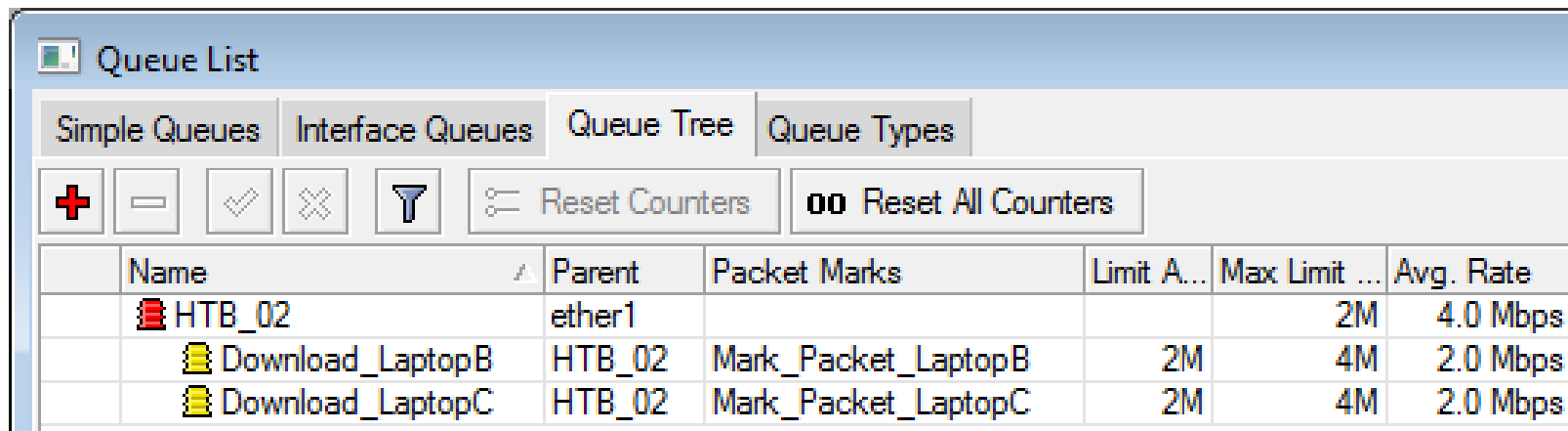
- HTB memungkinkan membuat struktur Queue yang hirarkis, dimana suatu queue bisa menjadi parent untuk queue lainnya
- Implementasi HTB di Queue Tree harus menggunakan packet mark
- Setiap queue hanya menerapkan satu HTB

HTB & QUEUE TREE

- Max-limit parent harus lebih besar atau sama dengan jumlah limit-at clientnya
 - $\text{max-limit}(\text{parent}) \geq \text{limit-at}(\text{child1}) + \dots + \text{limit-at}(\text{childN})$
- Max-limit child harus kurang atau sama dengan max-limit parentnya
 - $\text{max-limit}(\text{parent}) \geq \text{max-limit}(\text{child1})$
 - $\text{max-limit}(\text{parent}) \geq \text{max-limit}(\text{child2})$
 - $\text{max-limit}(\text{parent}) \geq \text{max-limit}(\text{childN})$

HTB & QUEUE TREE

- Parent paling atas, hanya membutuhkan max-limit, tidak membutuhkan limit-at dan priority



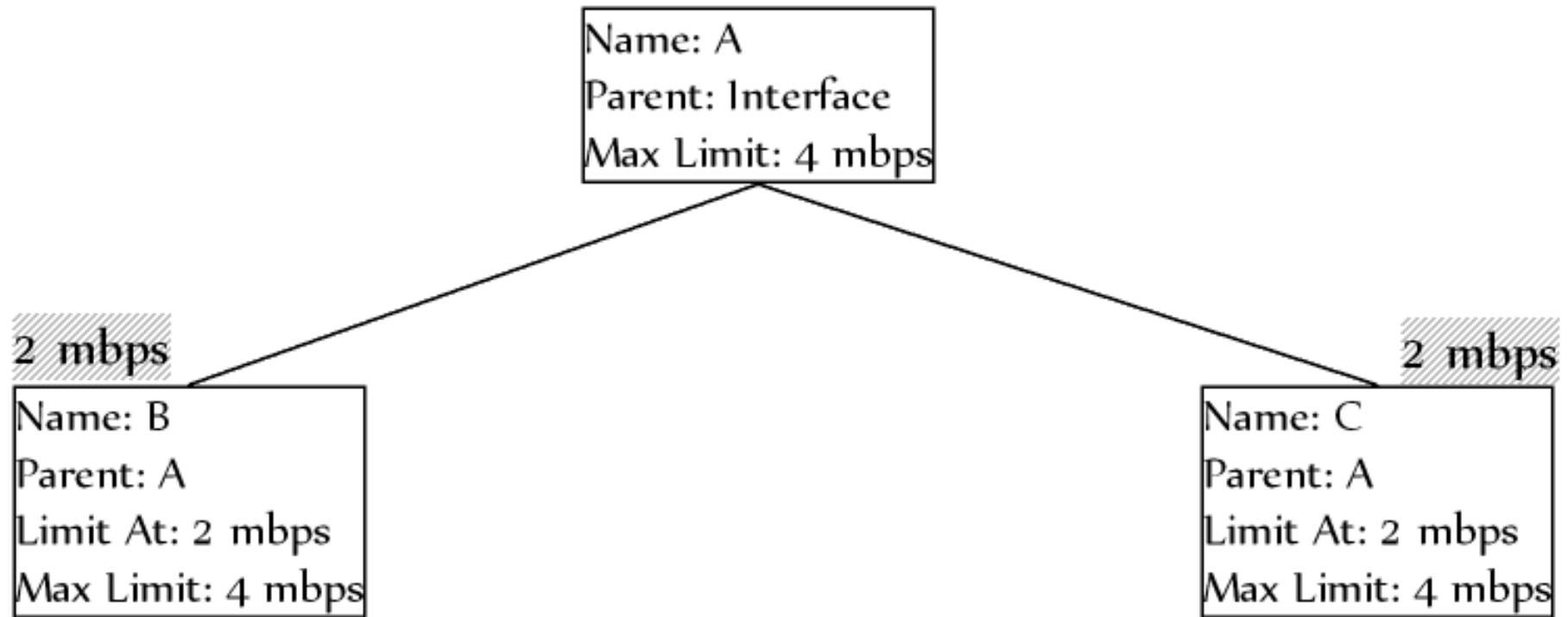
The screenshot shows the Mikrotik Queue List interface. The 'Queue Tree' tab is selected. The table below displays the configuration for a Queue Tree structure.

Name	Parent	Packet Marks	Limit A...	Max Limit ...	Avg. Rate
HTB_02	ether1			2M	4.0 Mbps
Download_LaptopB	HTB_02	Mark_Packet_LaptopB	2M	4M	2.0 Mbps
Download_LaptopC	HTB_02	Mark_Packet_LaptopC	2M	4M	2.0 Mbps

HTB & QUEUE TREE

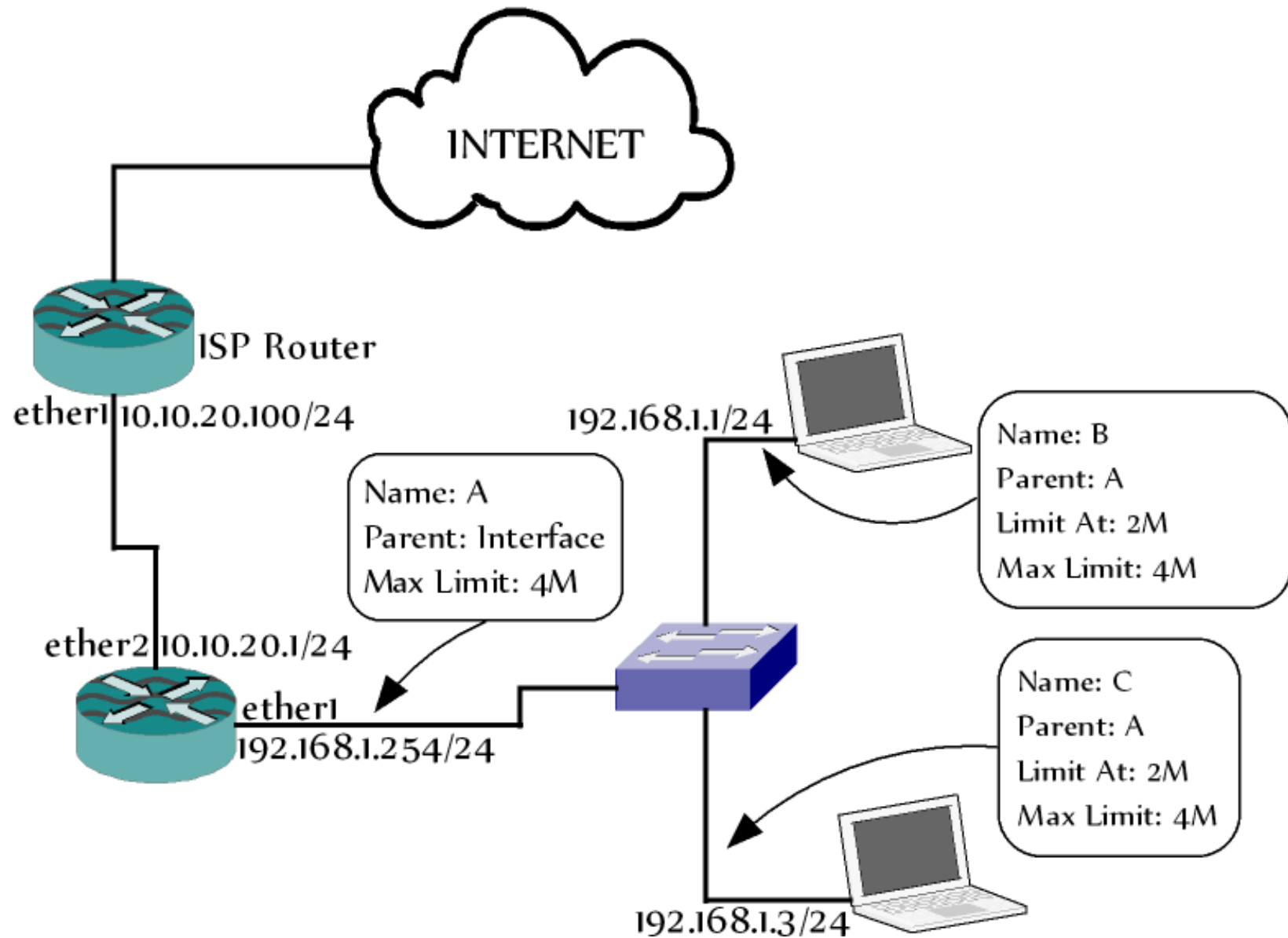
- Priority hanya bekerja pada child paling bawah
- Priority akan berfungsi (diperhitungkan) jika semua queue sudah mendapatkan limit-at nya

DISTRIBUSI HTB (1)

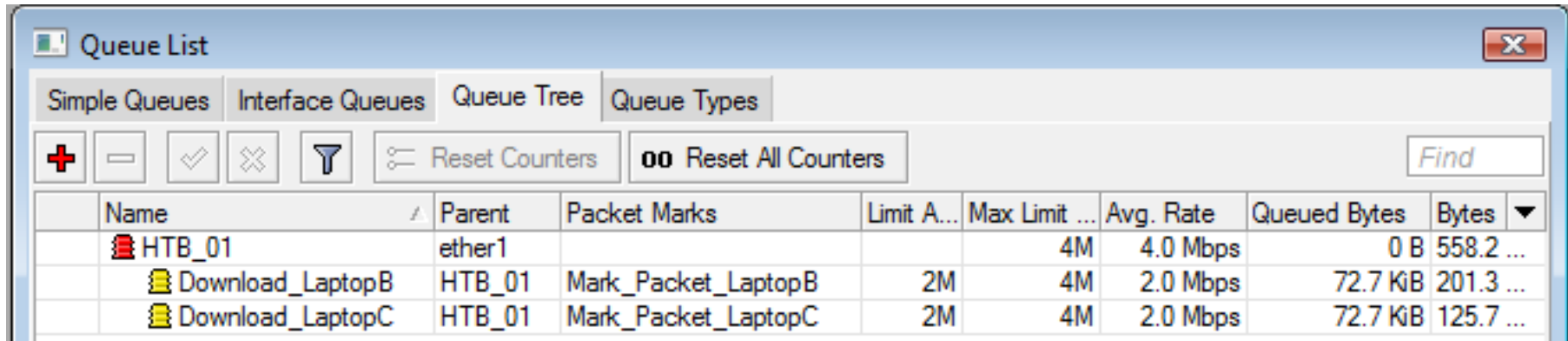


Jika semua menggunakan internet dengan maksimal,
maka B dan C masing masing akan mendapatkan 2 mbps,
Jika B tidak menggunakan internet, C akan mendapat 4 mbps

DISTRIBUSI HTB (1)

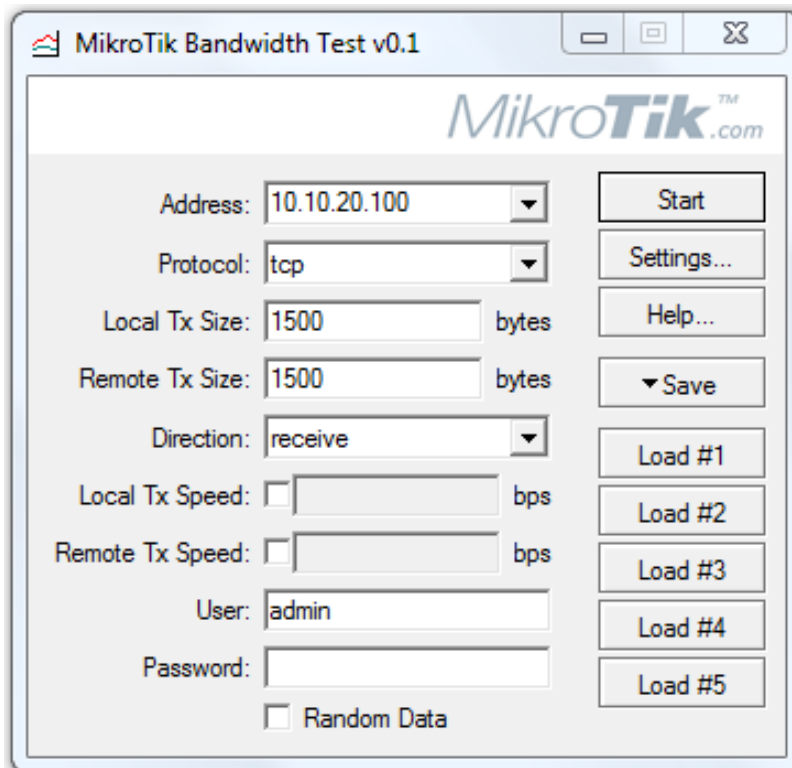


KONFIGURASI HTB (1)



The screenshot shows the Mikrotik Queue List window with the following configuration:

Name	Parent	Packet Marks	Limit A...	Max Limit ...	Avg. Rate	Queued Bytes	Bytes
HTB_01	ether1			4M	4.0 Mbps	0 B	558.2 ...
Download_LaptopB	HTB_01	Mark_Packet_LaptopB	2M	4M	2.0 Mbps	72.7 KiB	201.3 ...
Download_LaptopC	HTB_01	Mark_Packet_LaptopC	2M	4M	2.0 Mbps	72.7 KiB	125.7 ...

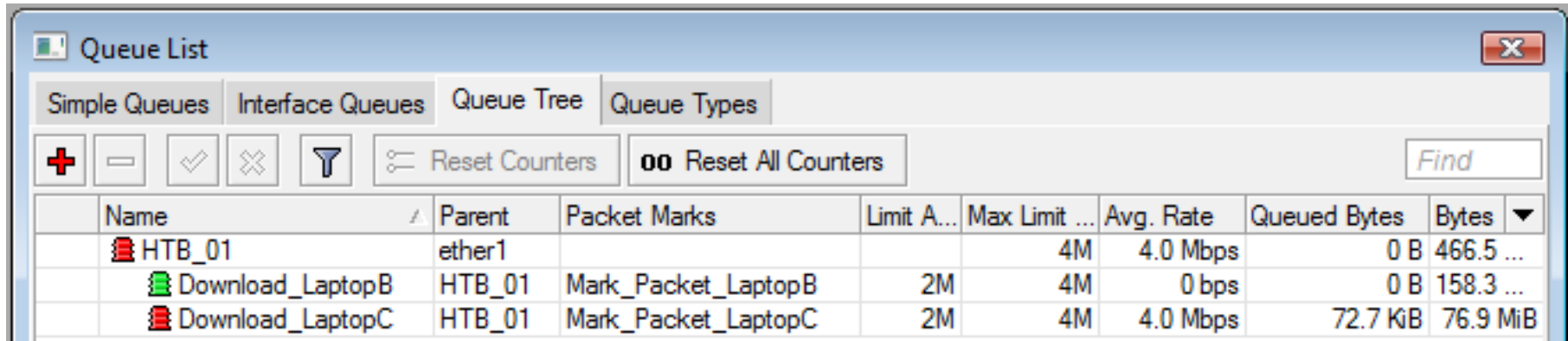


The screenshot shows the Mikrotik Bandwidth Test v0.1 window with the following configuration:

Address: 10.10.20.100
Protocol: tcp
Local Tx Size: 1500 bytes
Remote Tx Size: 1500 bytes
Direction: receive
Local Tx Speed: bps
Remote Tx Speed: bps
User: admin
Password:
 Random Data

Buttons: Start, Settings..., Help..., Save, Load #1, Load #2, Load #3, Load #4, Load #5

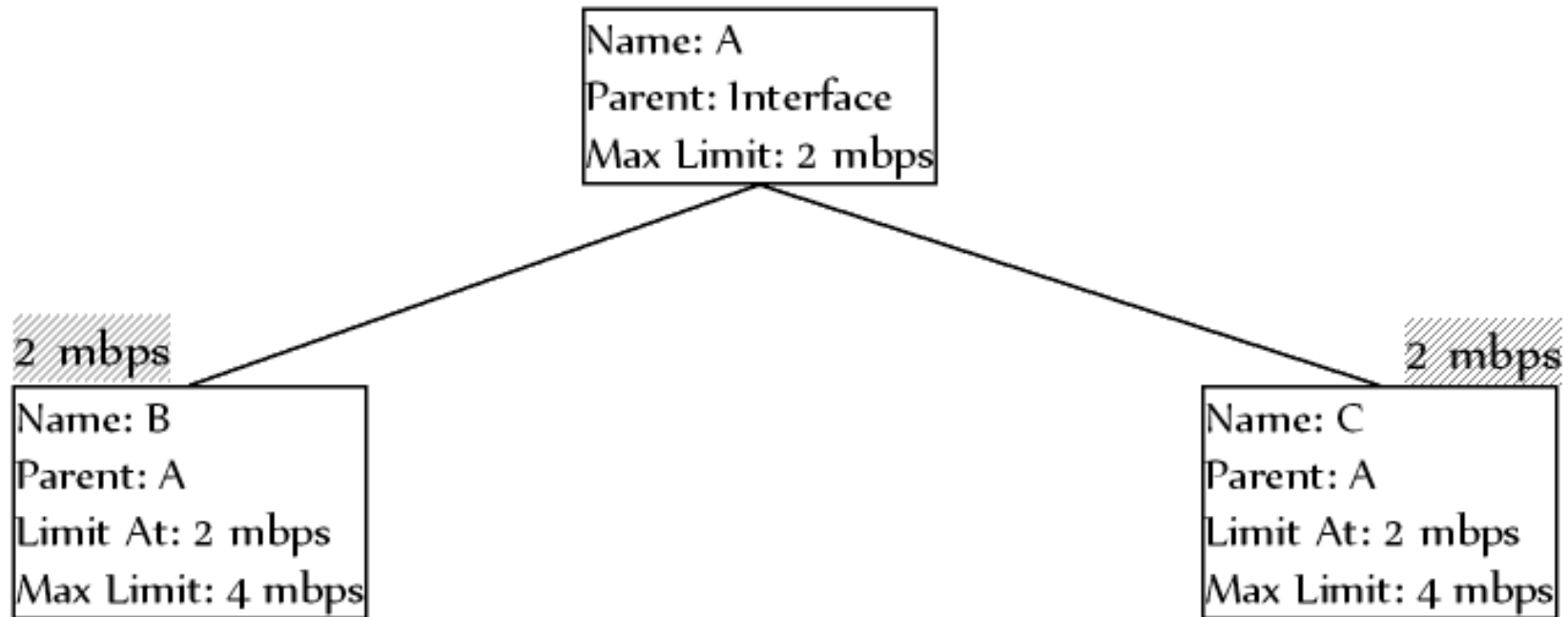
KONFIGURASI HTB (1)



The screenshot shows the Mikrotik WinBox 'Queue List' window. It has tabs for 'Simple Queues', 'Interface Queues', 'Queue Tree', and 'Queue Types'. Below the tabs are control buttons: '+', '-', a checkmark, a cross, a funnel, 'Reset Counters', and 'Reset All Counters'. A 'Find' search box is on the right. The main area contains a table with the following data:

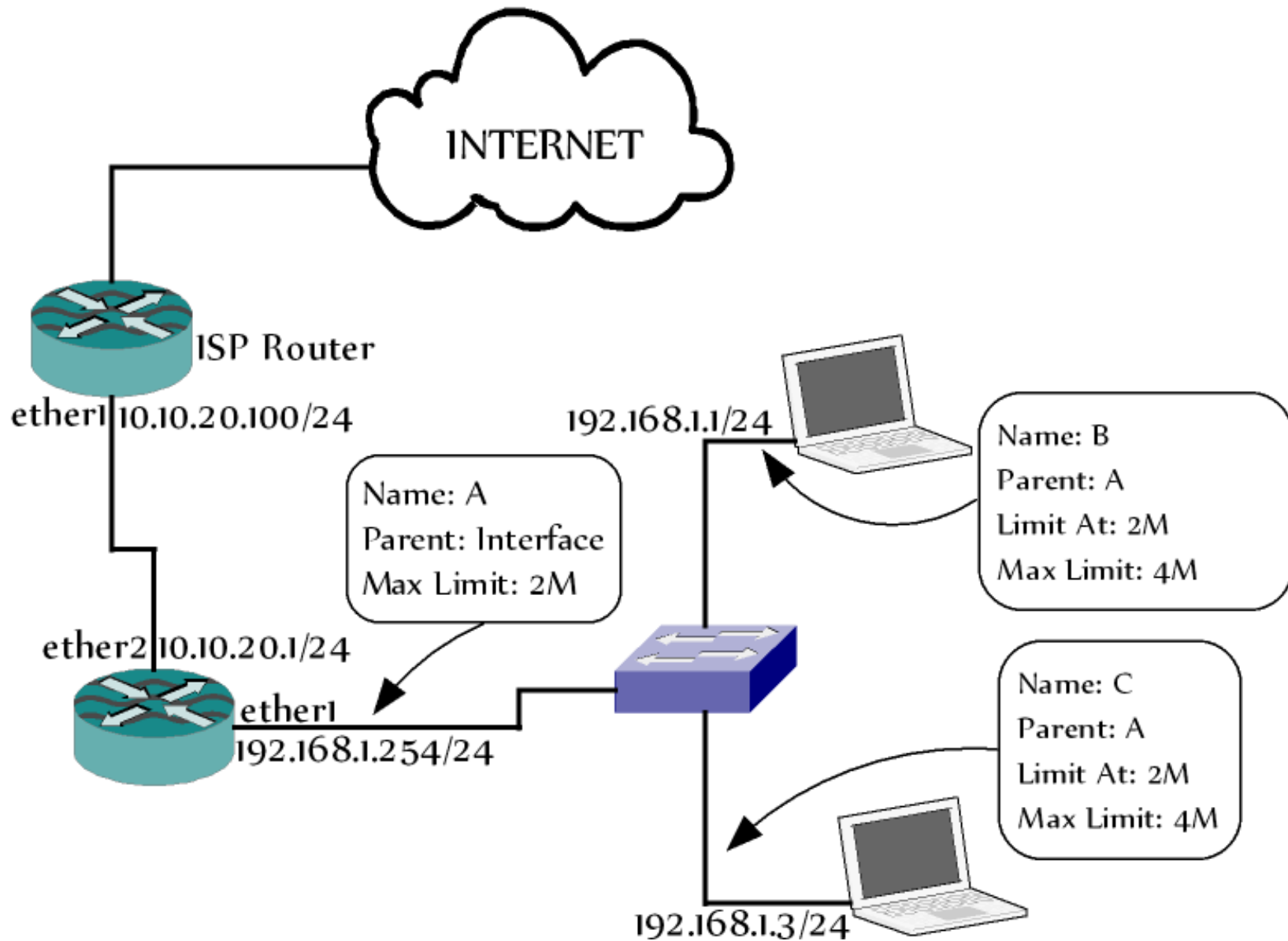
Name	Parent	Packet Marks	Limit A...	Max Limit ...	Avg. Rate	Queued Bytes	Bytes
HTB_01	ether1			4M	4.0 Mbps	0 B	466.5 ...
Download_LaptopB	HTB_01	Mark_Packet_LaptopB	2M	4M	0 bps	0 B	158.3 ...
Download_LaptopC	HTB_01	Mark_Packet_LaptopC	2M	4M	4.0 Mbps	72.7 KiB	76.9 MiB

DISTRIBUSI HTB (2)



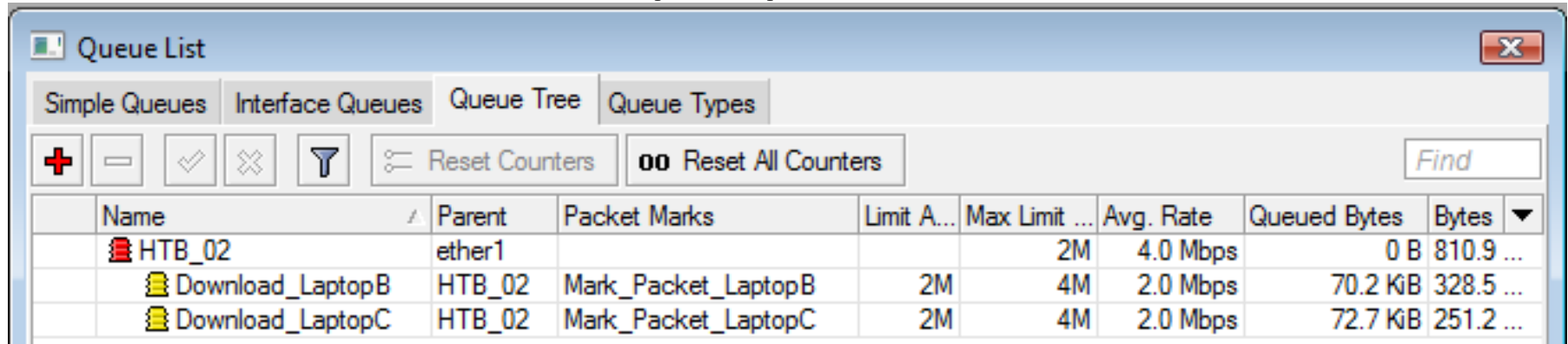
Meskipun Max Limit A hanya 2 mbps,
tetapi B dan C masing masing akan tetap mendapat 2 mbps
karena Max Limit Parent \geq Total Limit At Client.
Jika B tidak menggunakan internet,
C tetap hanya akan mendapatkan 2 mpbs

DISTRIBUSI HTB (2)



KONFIGURASI HTB (2)

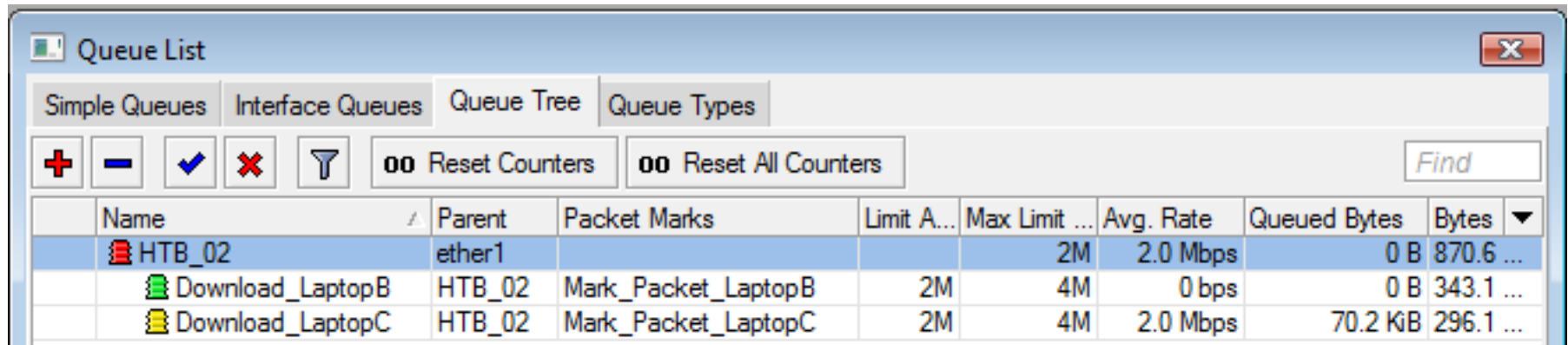
- Test bandwidth 2 laptop aktif



The screenshot shows the Mikrotik Queue List window with the 'Queue Tree' tab selected. The table below represents the data shown in the window:

Name	Parent	Packet Marks	Limit A...	Max Limit ...	Avg. Rate	Queued Bytes	Bytes
HTB_02	ether1			2M	4.0 Mbps	0 B	810.9 ...
Download_LaptopB	HTB_02	Mark_Packet_LaptopB	2M	4M	2.0 Mbps	70.2 KiB	328.5 ...
Download_LaptopC	HTB_02	Mark_Packet_LaptopC	2M	4M	2.0 Mbps	72.7 KiB	251.2 ...

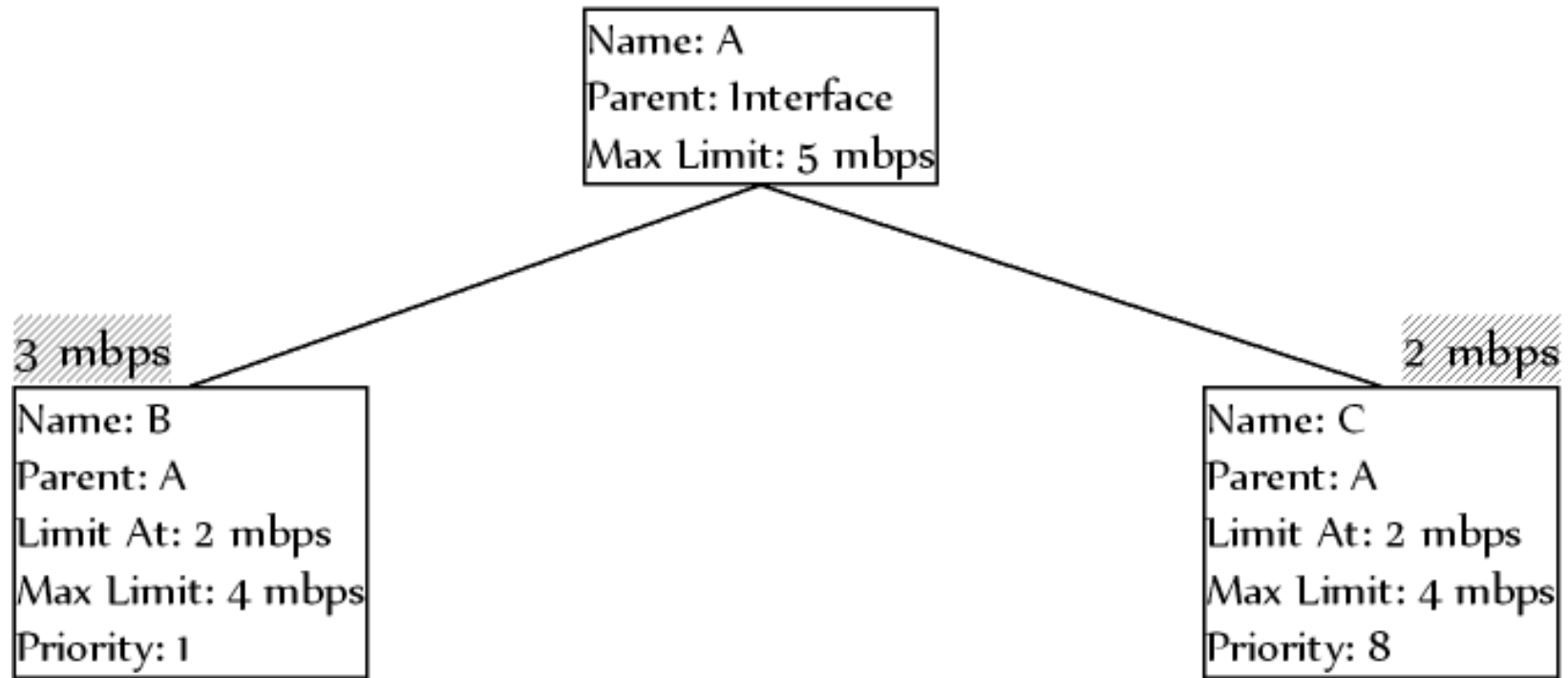
- Test bandwidth 1 laptop aktif



The screenshot shows the Mikrotik Queue List window with the 'Queue Tree' tab selected. The table below represents the data shown in the window:

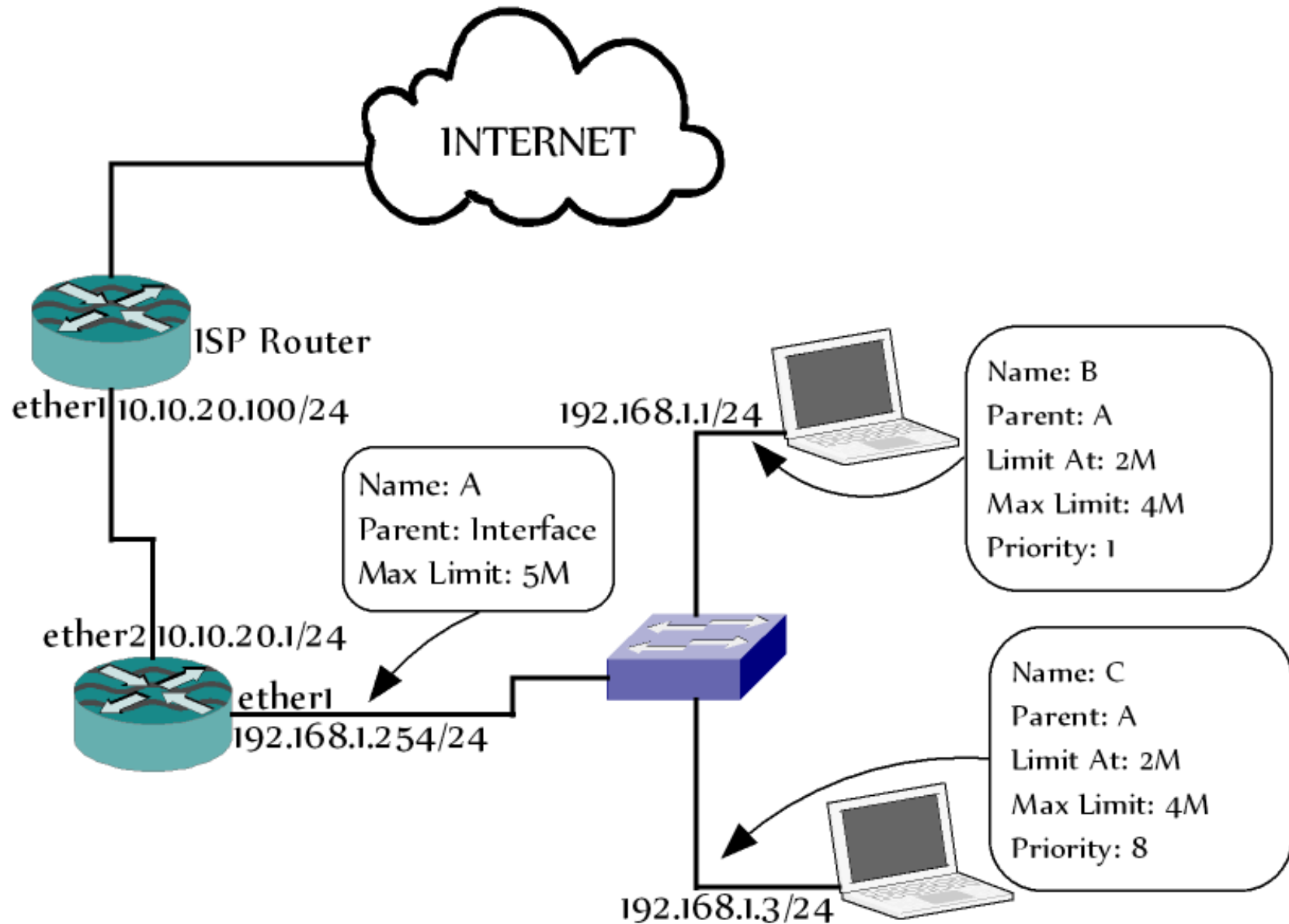
Name	Parent	Packet Marks	Limit A...	Max Limit ...	Avg. Rate	Queued Bytes	Bytes
HTB_02	ether1			2M	2.0 Mbps	0 B	870.6 ...
Download_LaptopB	HTB_02	Mark_Packet_LaptopB	2M	4M	0 bps	0 B	343.1 ...
Download_LaptopC	HTB_02	Mark_Packet_LaptopC	2M	4M	2.0 Mbps	70.2 KiB	296.1 ...

DISTRIBUSI HTB (3)



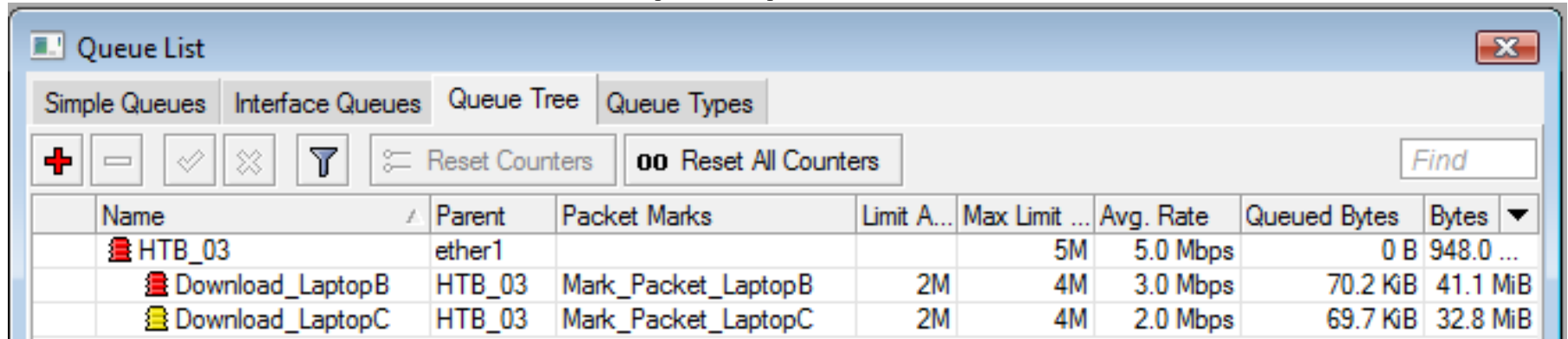
B memiliki prioritas lebih tinggi daripada C

DISTRIBUSI HTB (3)



KONFIGURASI HTB (3)

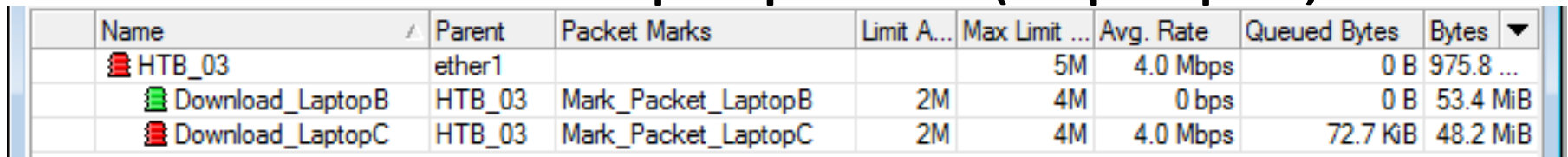
- Test bandwidth 2 laptop aktif



The screenshot shows the Mikrotik WinBox Queue List window. The 'Queue Tree' tab is selected. The table below shows the configuration for HTB_03 and its child queues. The 'Avg. Rate' column shows that both child queues are active.

Name	Parent	Packet Marks	Limit A...	Max Limit ...	Avg. Rate	Queued Bytes	Bytes
HTB_03	ether1			5M	5.0 Mbps	0 B	948.0 ...
Download_LaptopB	HTB_03	Mark_Packet_LaptopB	2M	4M	3.0 Mbps	70.2 KiB	41.1 MiB
Download_LaptopC	HTB_03	Mark_Packet_LaptopC	2M	4M	2.0 Mbps	69.7 KiB	32.8 MiB

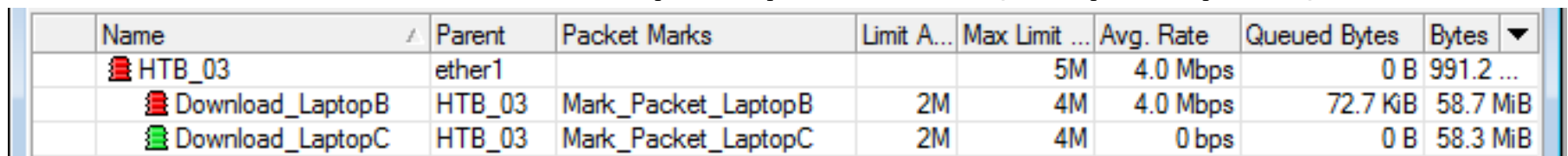
- Test bandwidth 1 laptop aktif (Laptop C)



The screenshot shows the Mikrotik WinBox Queue List window. The 'Queue Tree' tab is selected. The table below shows the configuration for HTB_03 and its child queues. The 'Avg. Rate' column shows that only the Laptop C queue is active.

Name	Parent	Packet Marks	Limit A...	Max Limit ...	Avg. Rate	Queued Bytes	Bytes
HTB_03	ether1			5M	4.0 Mbps	0 B	975.8 ...
Download_LaptopB	HTB_03	Mark_Packet_LaptopB	2M	4M	0 bps	0 B	53.4 MiB
Download_LaptopC	HTB_03	Mark_Packet_LaptopC	2M	4M	4.0 Mbps	72.7 KiB	48.2 MiB

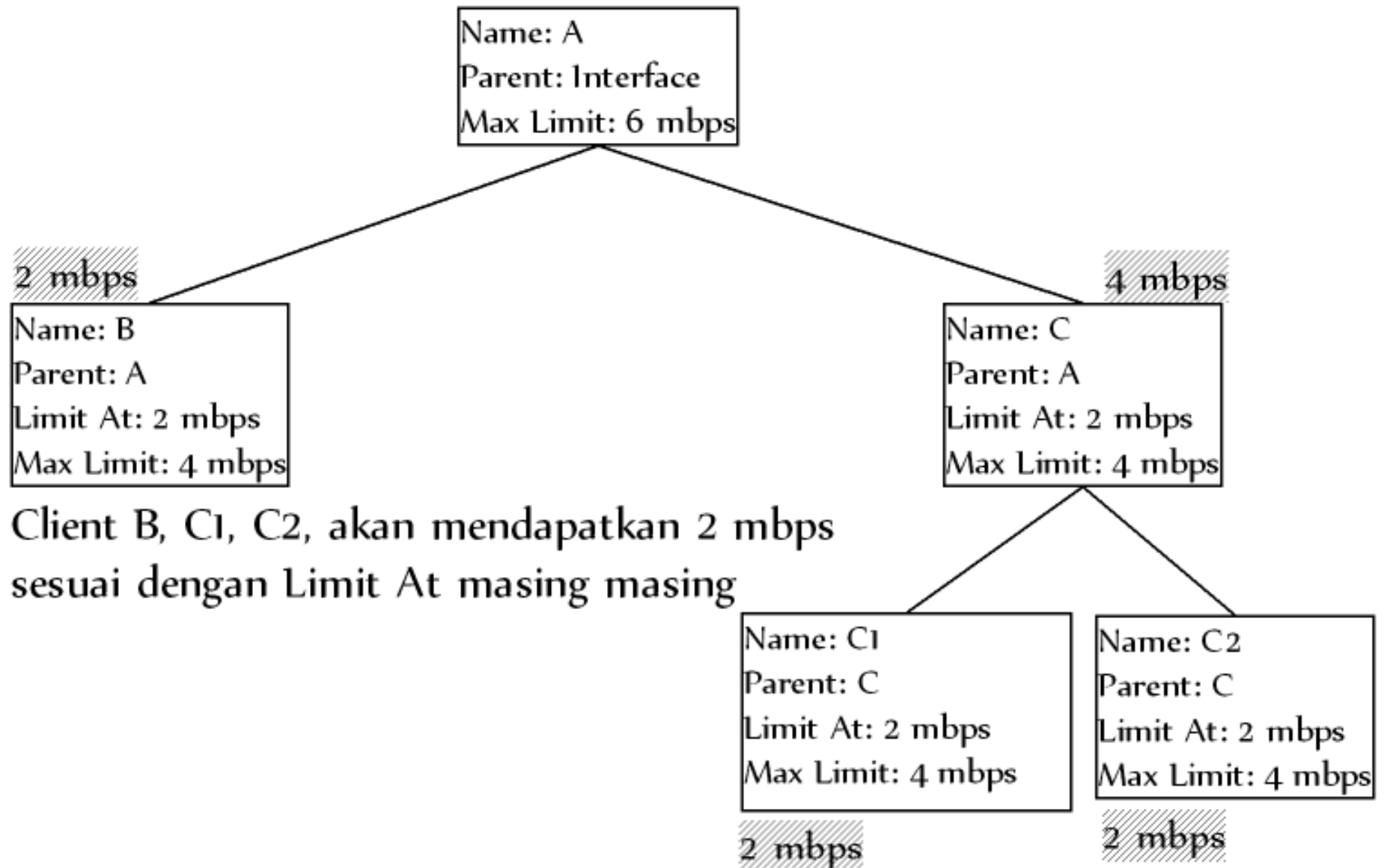
- Test bandwidth 1 laptop aktif (Laptop B)



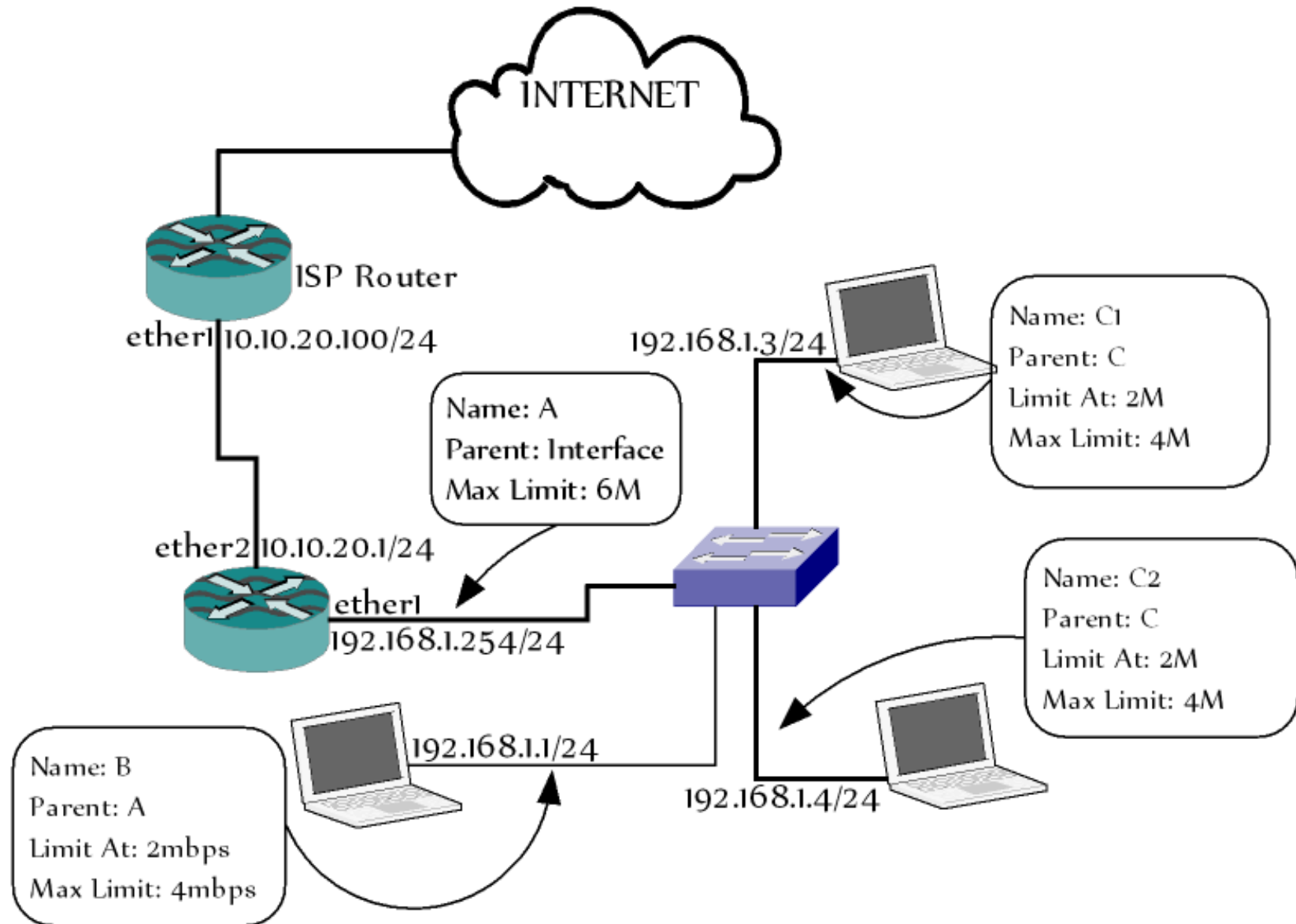
The screenshot shows the Mikrotik WinBox Queue List window. The 'Queue Tree' tab is selected. The table below shows the configuration for HTB_03 and its child queues. The 'Avg. Rate' column shows that only the Laptop B queue is active.

Name	Parent	Packet Marks	Limit A...	Max Limit ...	Avg. Rate	Queued Bytes	Bytes
HTB_03	ether1			5M	4.0 Mbps	0 B	991.2 ...
Download_LaptopB	HTB_03	Mark_Packet_LaptopB	2M	4M	4.0 Mbps	72.7 KiB	58.7 MiB
Download_LaptopC	HTB_03	Mark_Packet_LaptopC	2M	4M	0 bps	0 B	58.3 MiB

DISTRIBUSI HTB (4)

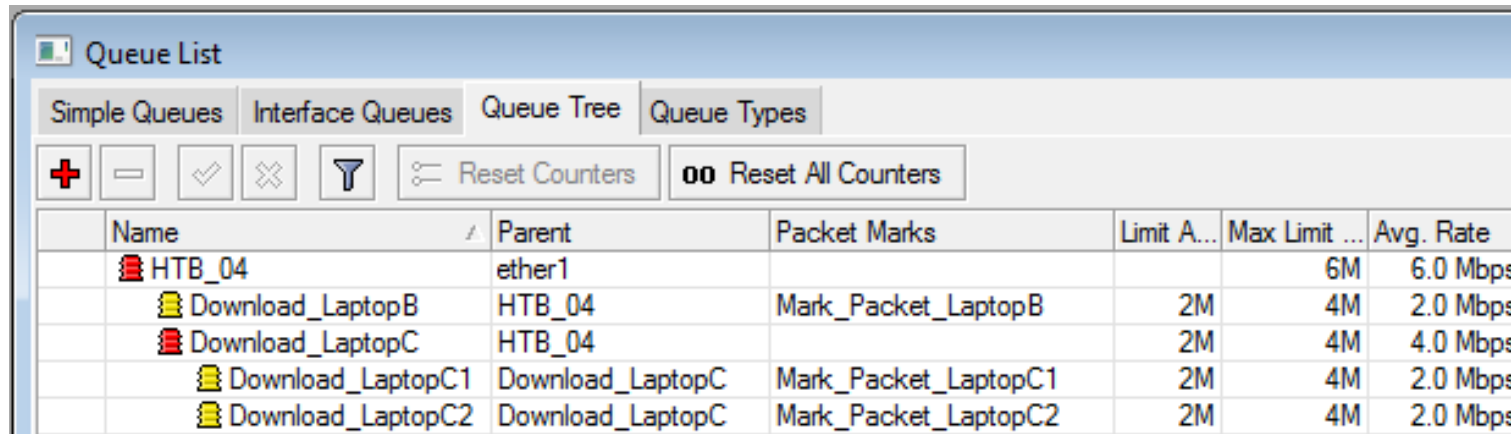


DISTRIBUSI HTB (4)



KONFIGURASI HTB (4)

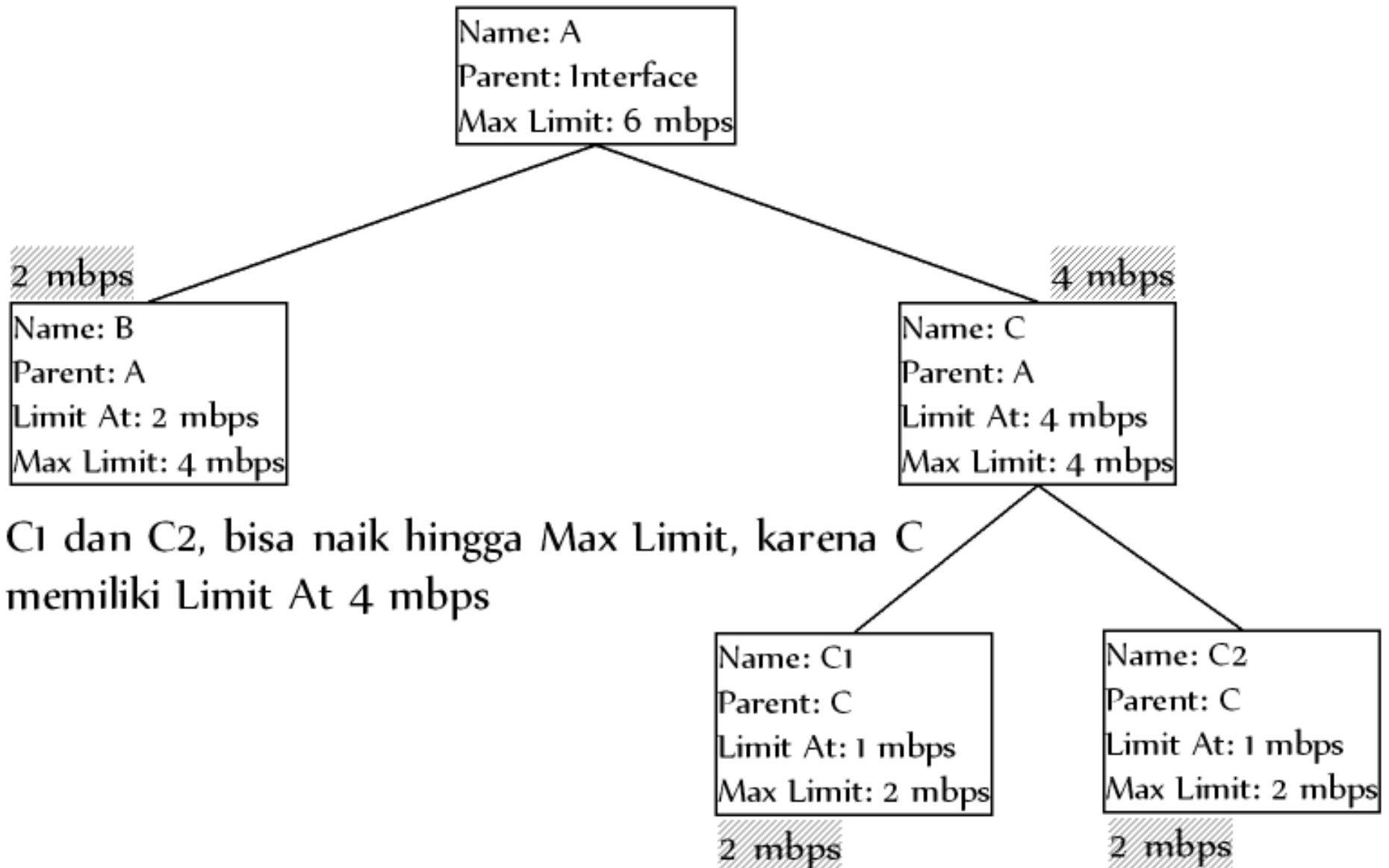
- Test bandwidth semua laptop aktif



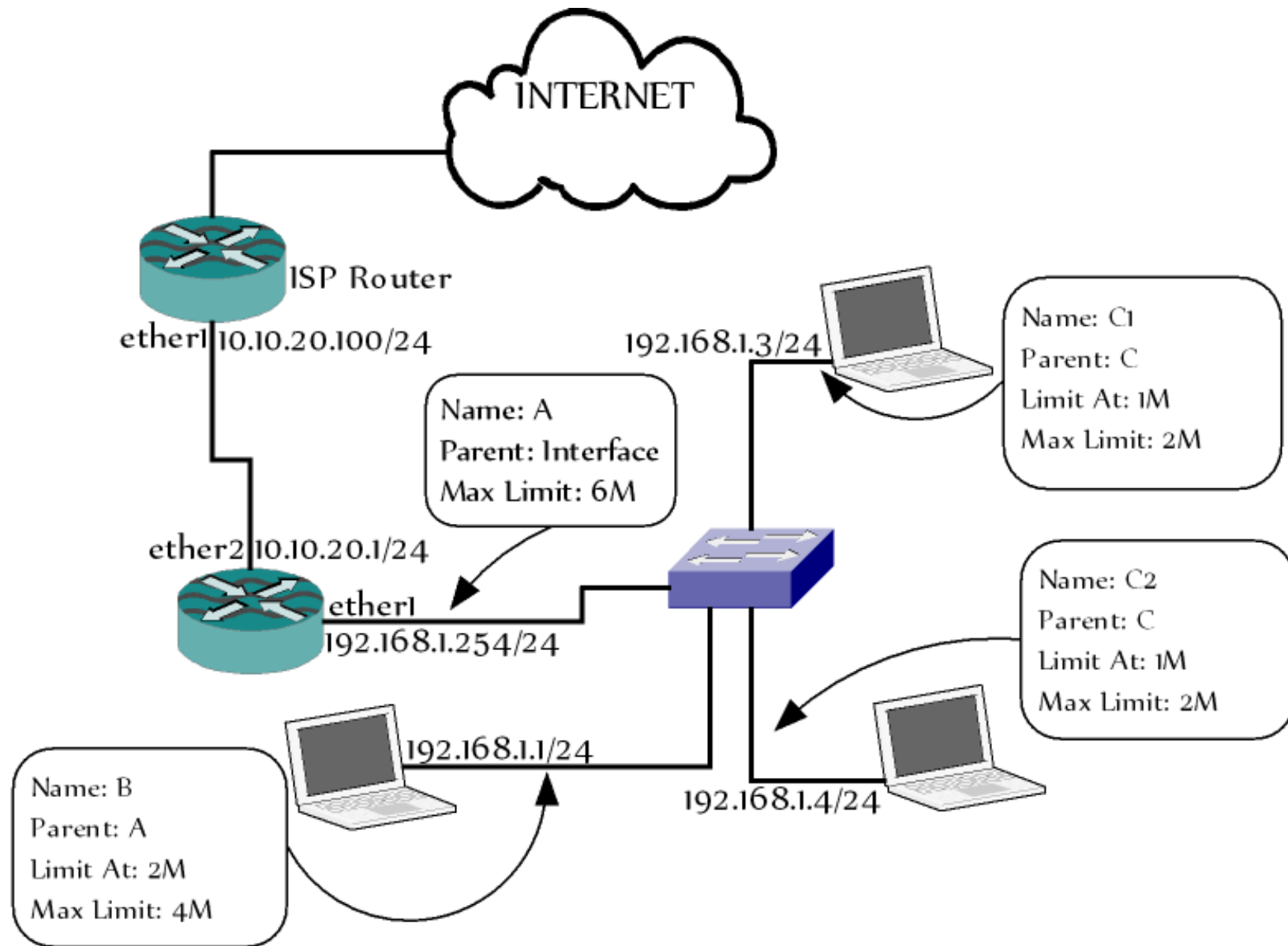
The screenshot shows the Mikrotik WinBox 'Queue List' window. It displays a table of queues configured for the 'ether1' interface. The table has columns for Name, Parent, Packet Marks, Limit A..., Max Limit ..., and Avg. Rate. The configuration includes a root queue 'HTB_04' with a 6M limit and 6.0 Mbps average rate, and several child queues for different laptops with 2M limits and 2.0 Mbps average rates.

Name	Parent	Packet Marks	Limit A...	Max Limit ...	Avg. Rate
HTB_04	ether1			6M	6.0 Mbps
Download_LaptopB	HTB_04	Mark_Packet_LaptopB	2M	4M	2.0 Mbps
Download_LaptopC	HTB_04		2M	4M	4.0 Mbps
Download_LaptopC1	Download_LaptopC	Mark_Packet_LaptopC1	2M	4M	2.0 Mbps
Download_LaptopC2	Download_LaptopC	Mark_Packet_LaptopC2	2M	4M	2.0 Mbps

DISTRIBUSI HTB (5)

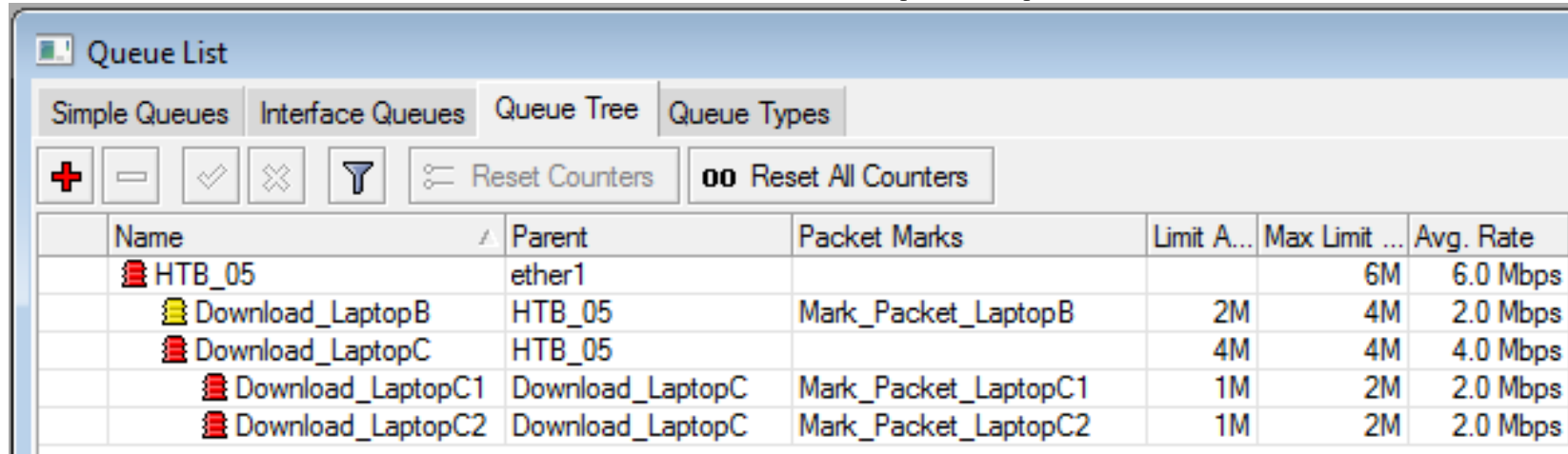


DISTRIBUSI HTB (5)



KONFIGURASI HTB (5)

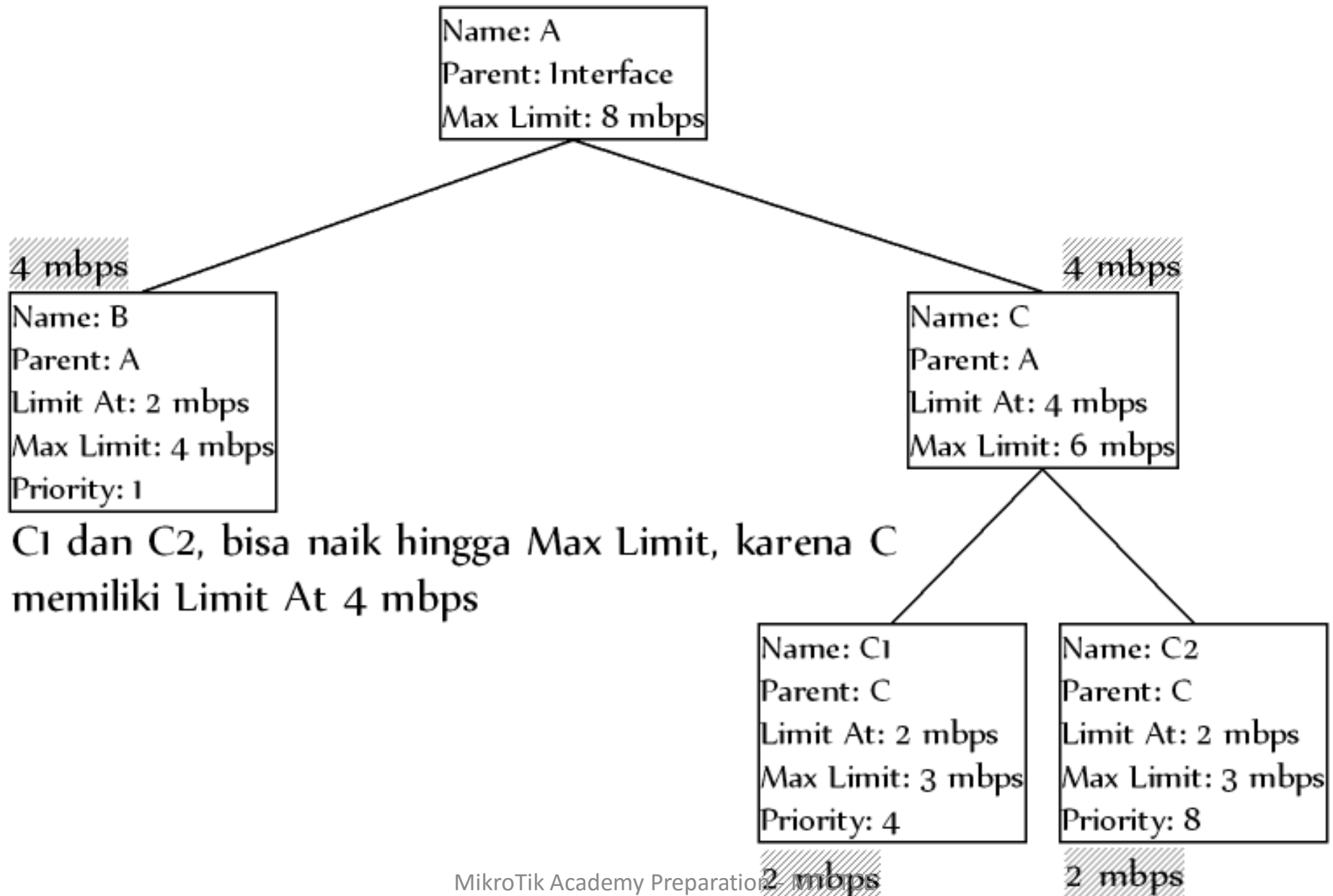
- Test bandwidth semua laptop aktif



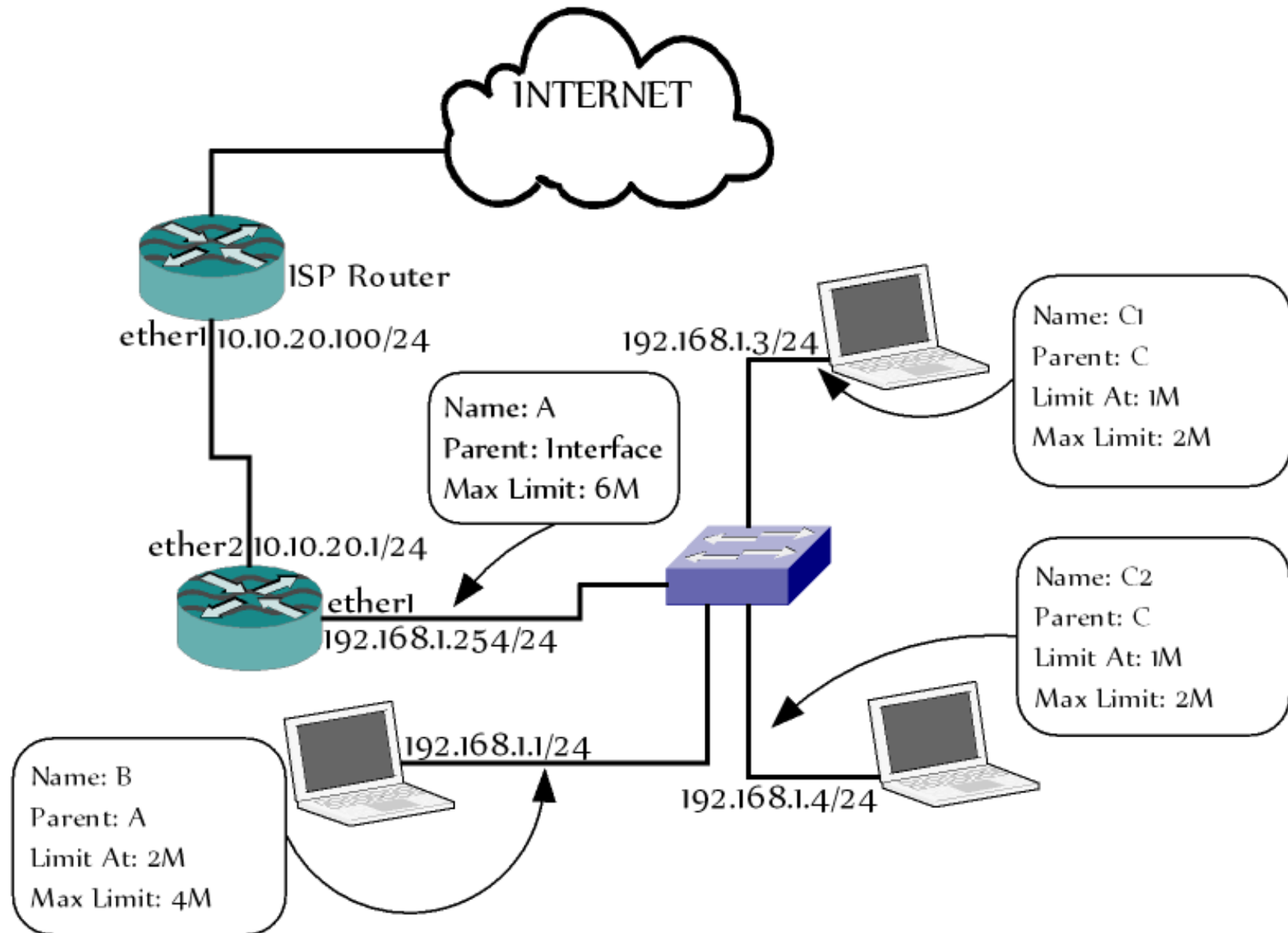
The screenshot shows the Mikrotik WinBox 'Queue List' window. The 'Queue Tree' tab is selected. The table below displays the configuration for the HTB_05 queue tree on interface ether1.

Name	Parent	Packet Marks	Limit A...	Max Limit ...	Avg. Rate
HTB_05	ether1			6M	6.0 Mbps
Download_LaptopB	HTB_05	Mark_Packet_LaptopB	2M	4M	2.0 Mbps
Download_LaptopC	HTB_05		4M	4M	4.0 Mbps
Download_LaptopC1	Download_LaptopC	Mark_Packet_LaptopC1	1M	2M	2.0 Mbps
Download_LaptopC2	Download_LaptopC	Mark_Packet_LaptopC2	1M	2M	2.0 Mbps

DISTRIBUSI HTB (6)

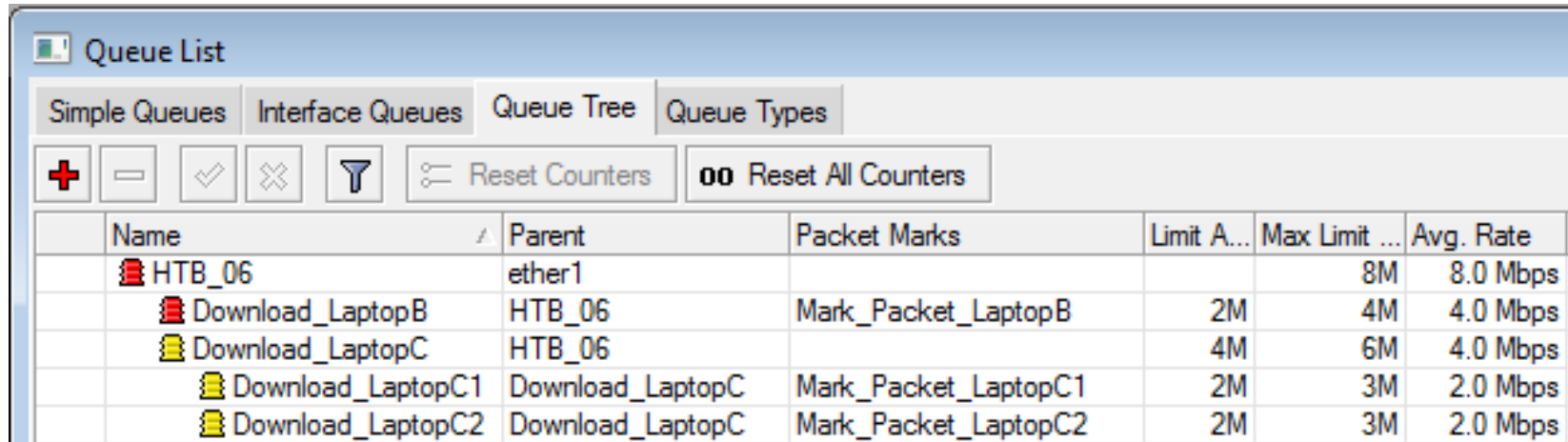


DISTRIBUSI HTB (6)



KONFIGURASI HTB (6)

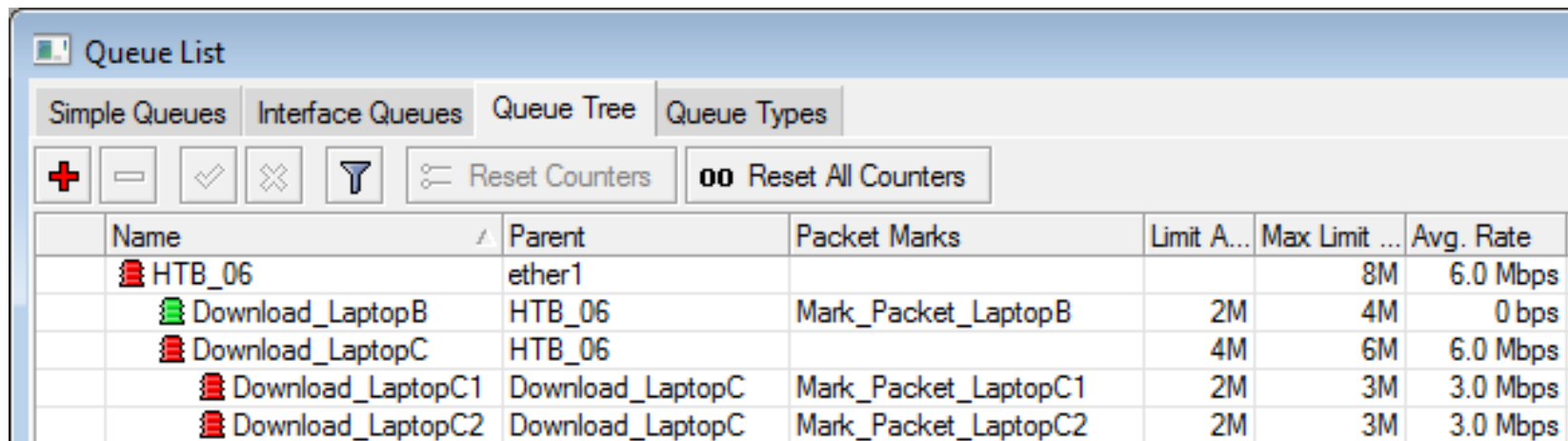
- Test bandwidth semua laptop aktif



The screenshot shows the Mikrotik Queue List interface with the 'Queue Tree' tab selected. The table displays the following data:

Name	Parent	Packet Marks	Limit A...	Max Limit ...	Avg. Rate
HTB_06	ether1			8M	8.0 Mbps
Download_LaptopB	HTB_06	Mark_Packet_LaptopB	2M	4M	4.0 Mbps
Download_LaptopC	HTB_06		4M	6M	4.0 Mbps
Download_LaptopC1	Download_LaptopC	Mark_Packet_LaptopC1	2M	3M	2.0 Mbps
Download_LaptopC2	Download_LaptopC	Mark_Packet_LaptopC2	2M	3M	2.0 Mbps

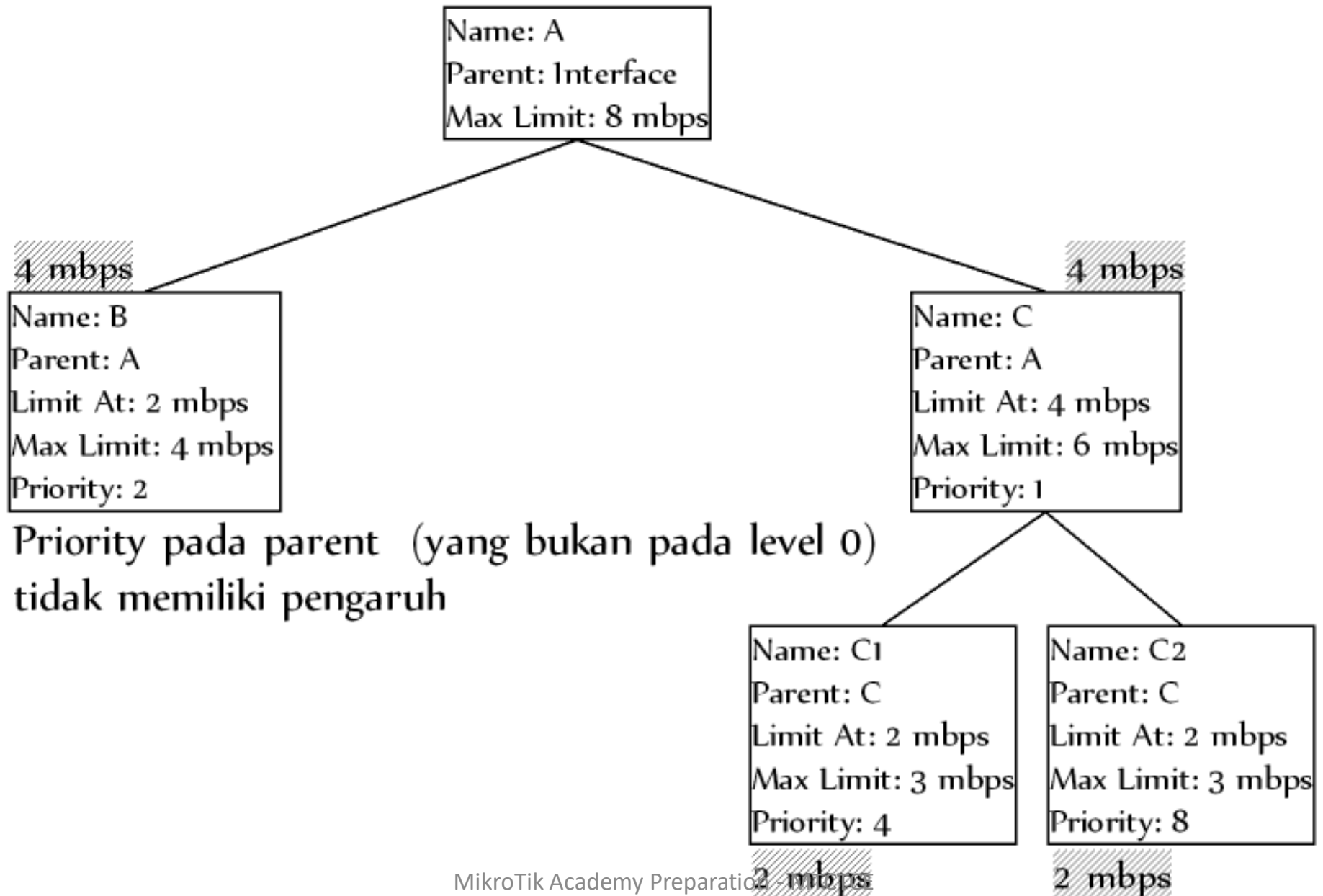
- Jika laptop B dimatikan



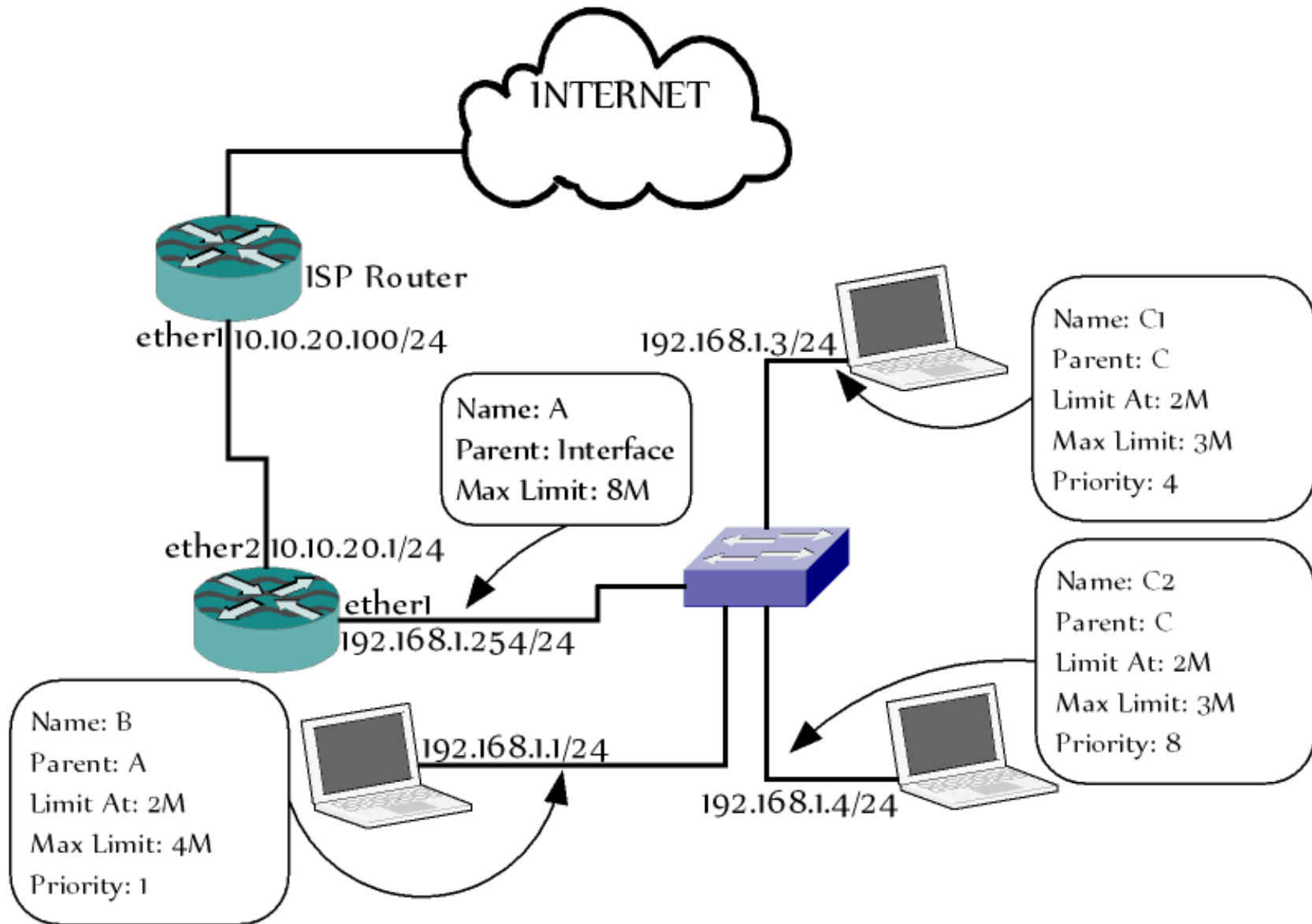
The screenshot shows the Mikrotik Queue List interface with the 'Queue Tree' tab selected. The table displays the following data:

Name	Parent	Packet Marks	Limit A...	Max Limit ...	Avg. Rate
HTB_06	ether1			8M	6.0 Mbps
Download_LaptopB	HTB_06	Mark_Packet_LaptopB	2M	4M	0 bps
Download_LaptopC	HTB_06		4M	6M	6.0 Mbps
Download_LaptopC1	Download_LaptopC	Mark_Packet_LaptopC1	2M	3M	3.0 Mbps
Download_LaptopC2	Download_LaptopC	Mark_Packet_LaptopC2	2M	3M	3.0 Mbps

DISTRIBUSI HTB (7)

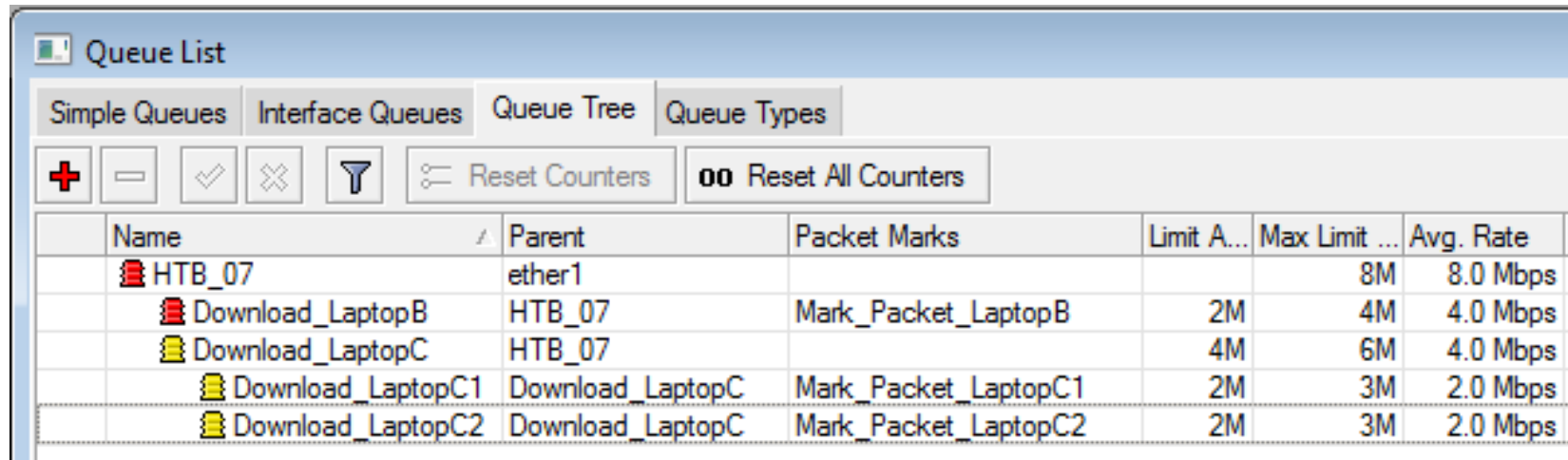


DISTRIBUSI HTB (7)



KONFIGURASI HTB (7)

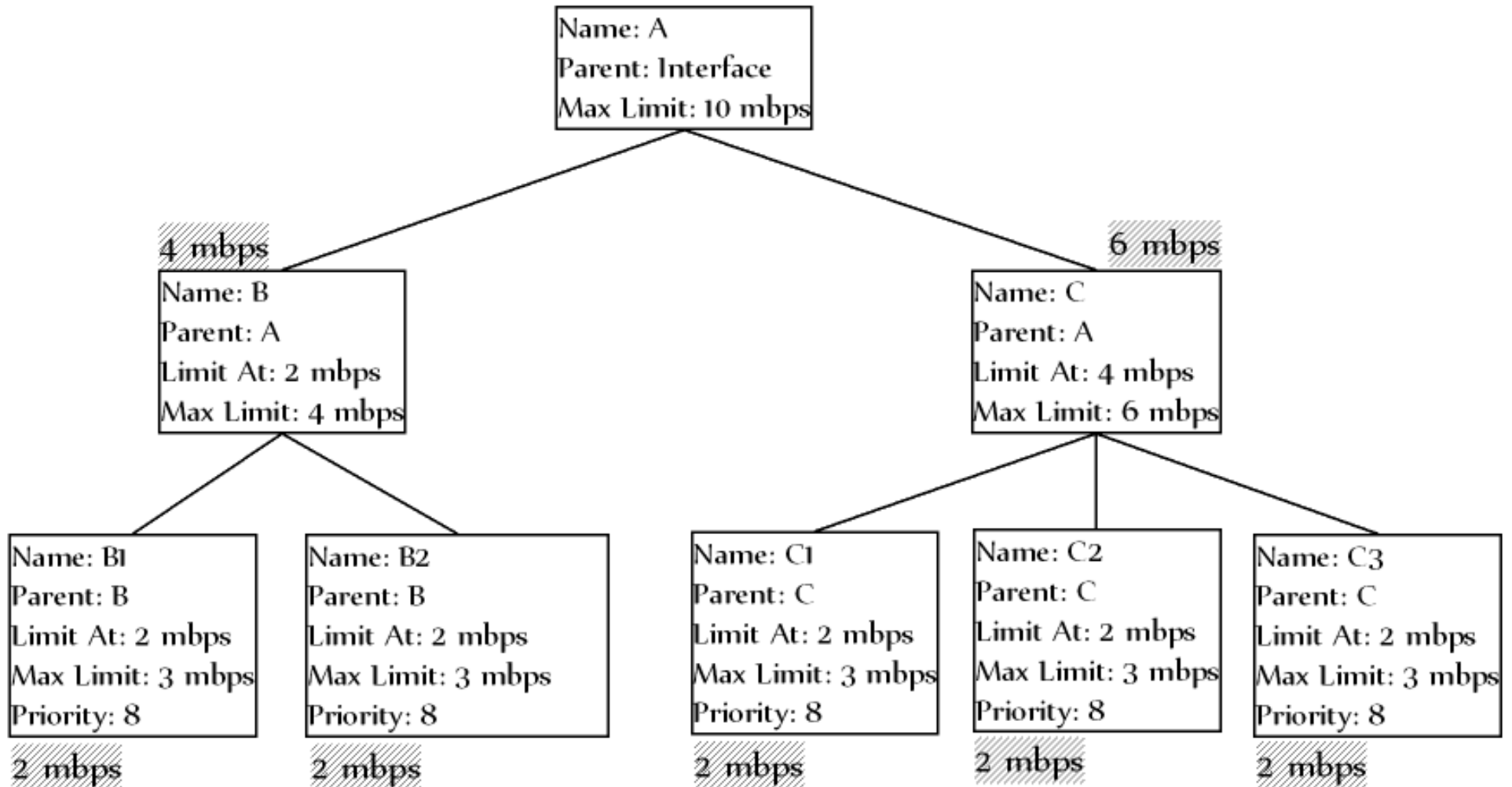
- Test Bandwidth Semua laptop aktif



The screenshot shows the Mikrotik WinBox Queue List window. The 'Queue Tree' tab is selected, displaying a hierarchical list of queues. The root queue is 'HTB_07' on interface 'ether1' with a limit of 8M and an average rate of 8.0 Mbps. It has two children: 'Download_LaptopB' (2M limit, 4.0 Mbps rate) and 'Download_LaptopC' (4M limit, 4.0 Mbps rate). 'Download_LaptopC' has two children: 'Download_LaptopC1' (2M limit, 2.0 Mbps rate) and 'Download_LaptopC2' (2M limit, 2.0 Mbps rate). The table also shows packet marks for each queue.

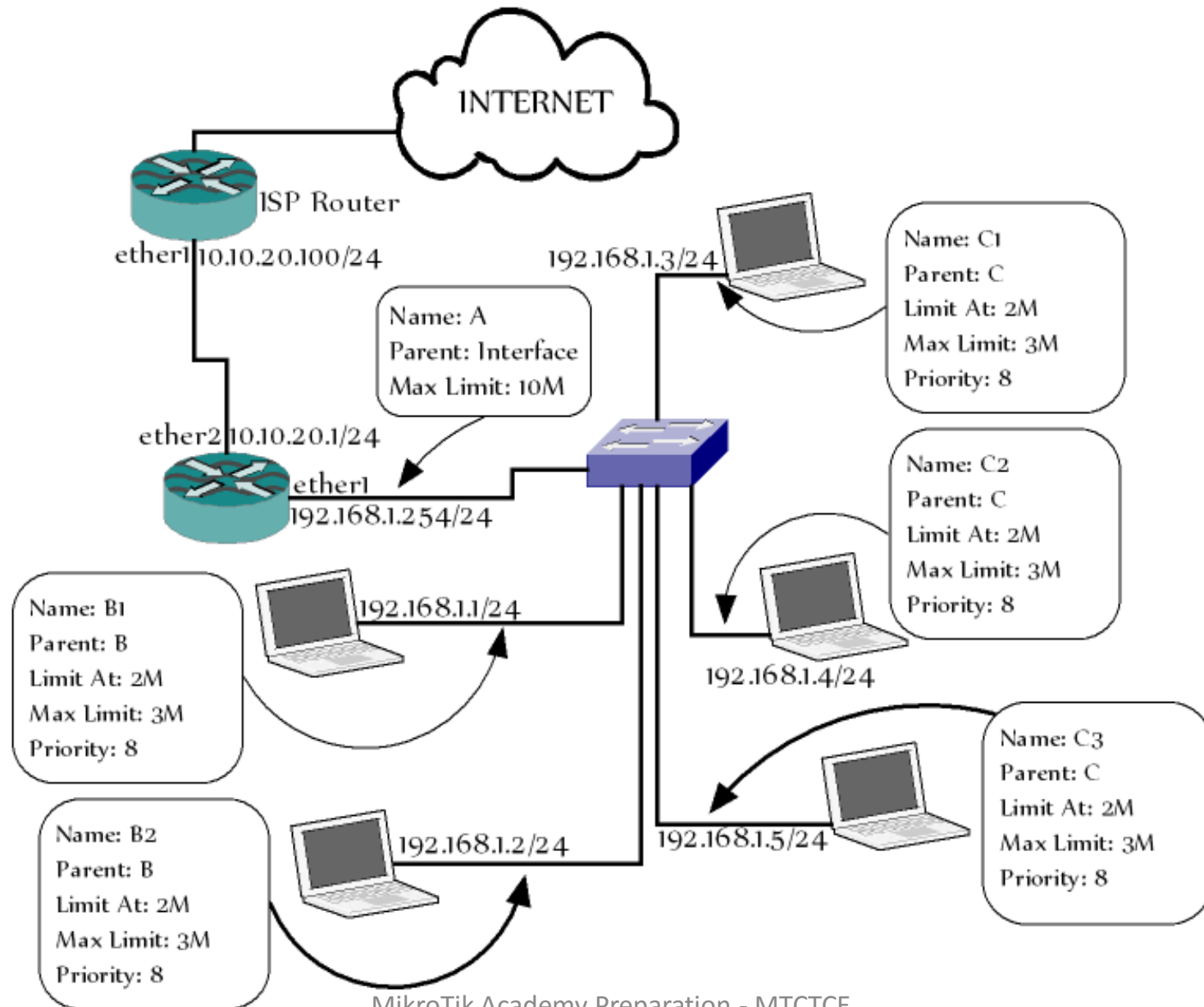
Name	Parent	Packet Marks	Limit A...	Max Limit ...	Avg. Rate
HTB_07	ether1			8M	8.0 Mbps
Download_LaptopB	HTB_07	Mark_Packet_LaptopB	2M	4M	4.0 Mbps
Download_LaptopC	HTB_07		4M	6M	4.0 Mbps
Download_LaptopC1	Download_LaptopC	Mark_Packet_LaptopC1	2M	3M	2.0 Mbps
Download_LaptopC2	Download_LaptopC	Mark_Packet_LaptopC2	2M	3M	2.0 Mbps

DISTRIBUSI HTB (8)



Semua Child akan mendapatkan trafik 2 mbps

DISTRIBUSI HTB (8)



DISTRIBUSI HTB (8)

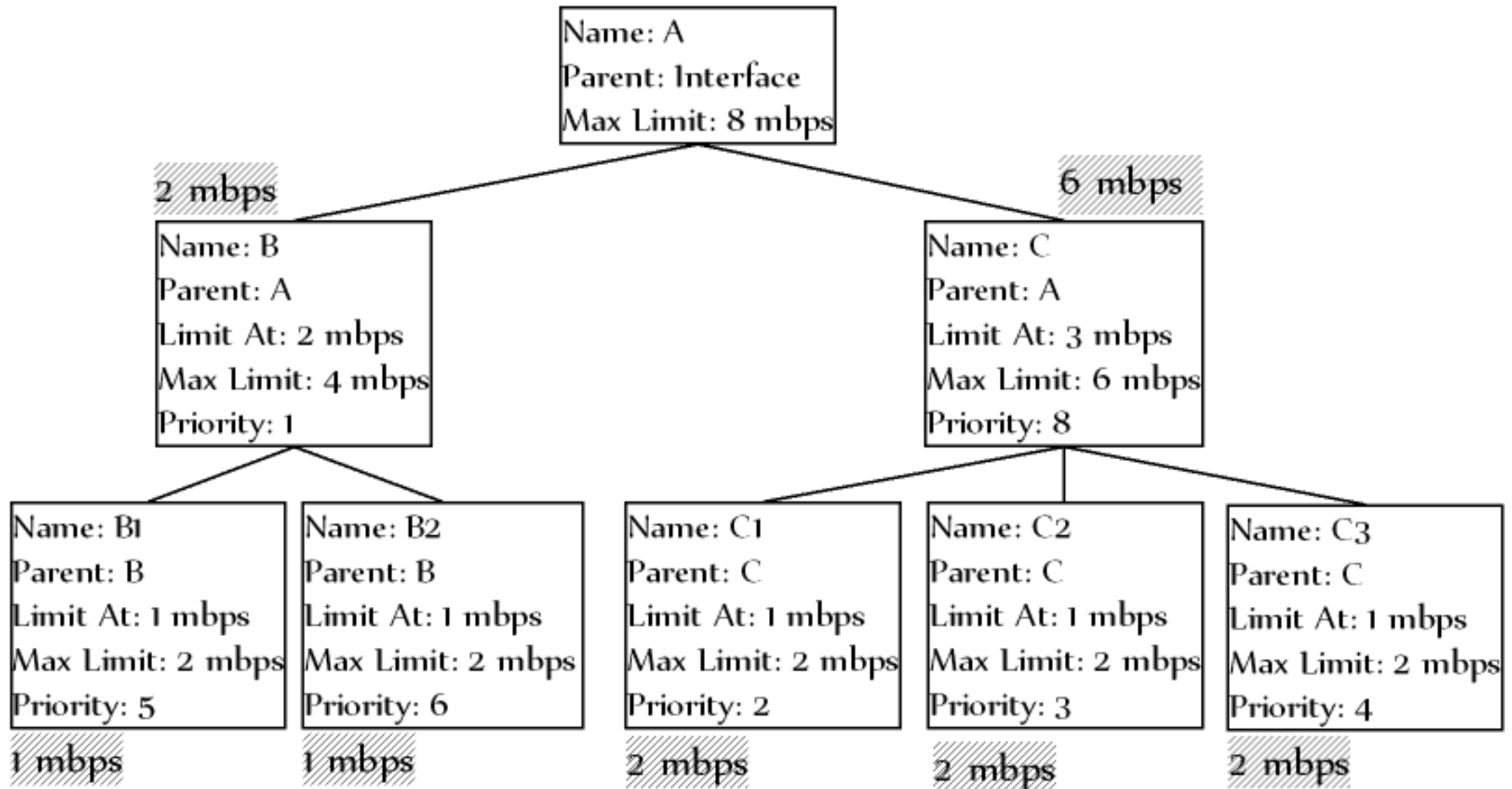
Queue List

Simple Queues Interface Queues Queue Tree Queue Types

+ - ✓ ✗ ⌵ 00 Reset Counters 00 Reset All Counters

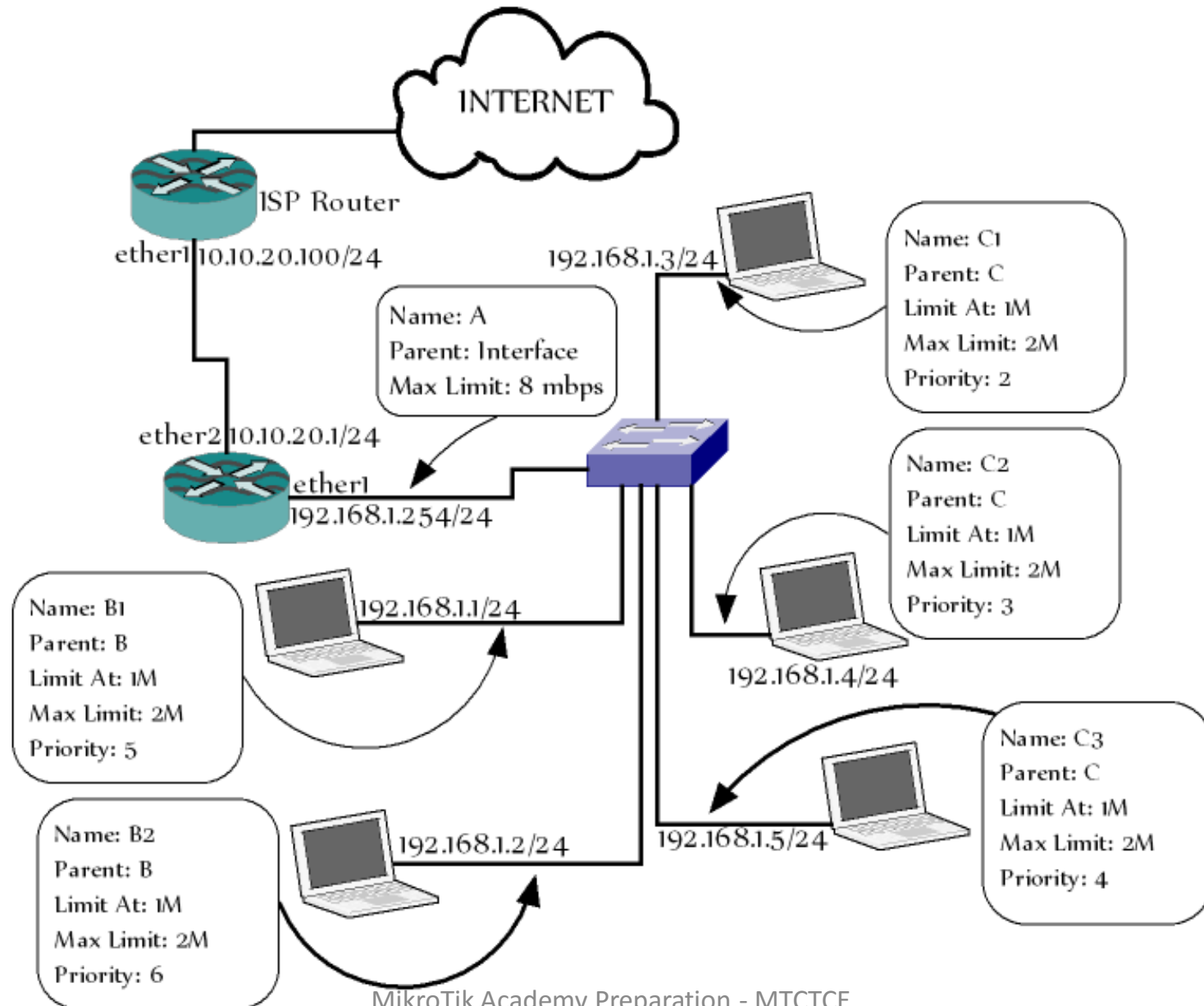
Name	Parent	Packet Marks	Limit A...	Max Limit ...	Avg. Rate
HTB_08	ether1			10M	10.0 Mbps
Download_LaptopB	HTB_08		2M	4M	4.0 Mbps
Download_LaptopB1	Download_LaptopB	Mark_Packet_LaptopB1	2M	3M	2.0 Mbps
Download_LaptopB2	Download_LaptopB	Mark_Packet_LaptopB2	2M	3M	2.0 Mbps
Download_LaptopC	HTB_08		4M	6M	6.0 Mbps
Download_LaptopC1	Download_LaptopC	Mark_Packet_LaptopC1	2M	3M	2.0 Mbps
Download_LaptopC2	Download_LaptopC	Mark_Packet_LaptopC2	2M	3M	2.0 Mbps
Download_LaptopC3	Download_LaptopC	Mark_Packet_LaptopC3	2M	3M	2.0 Mbps

DISTRIBUSI HTB (9)



C1, C2, C3 mendapatkan 2 mbps karena prioritynya lebih tinggi dari B1 dan B2

DISTRIBUSI HTB (9)



DISTRIBUSI HTB (9)

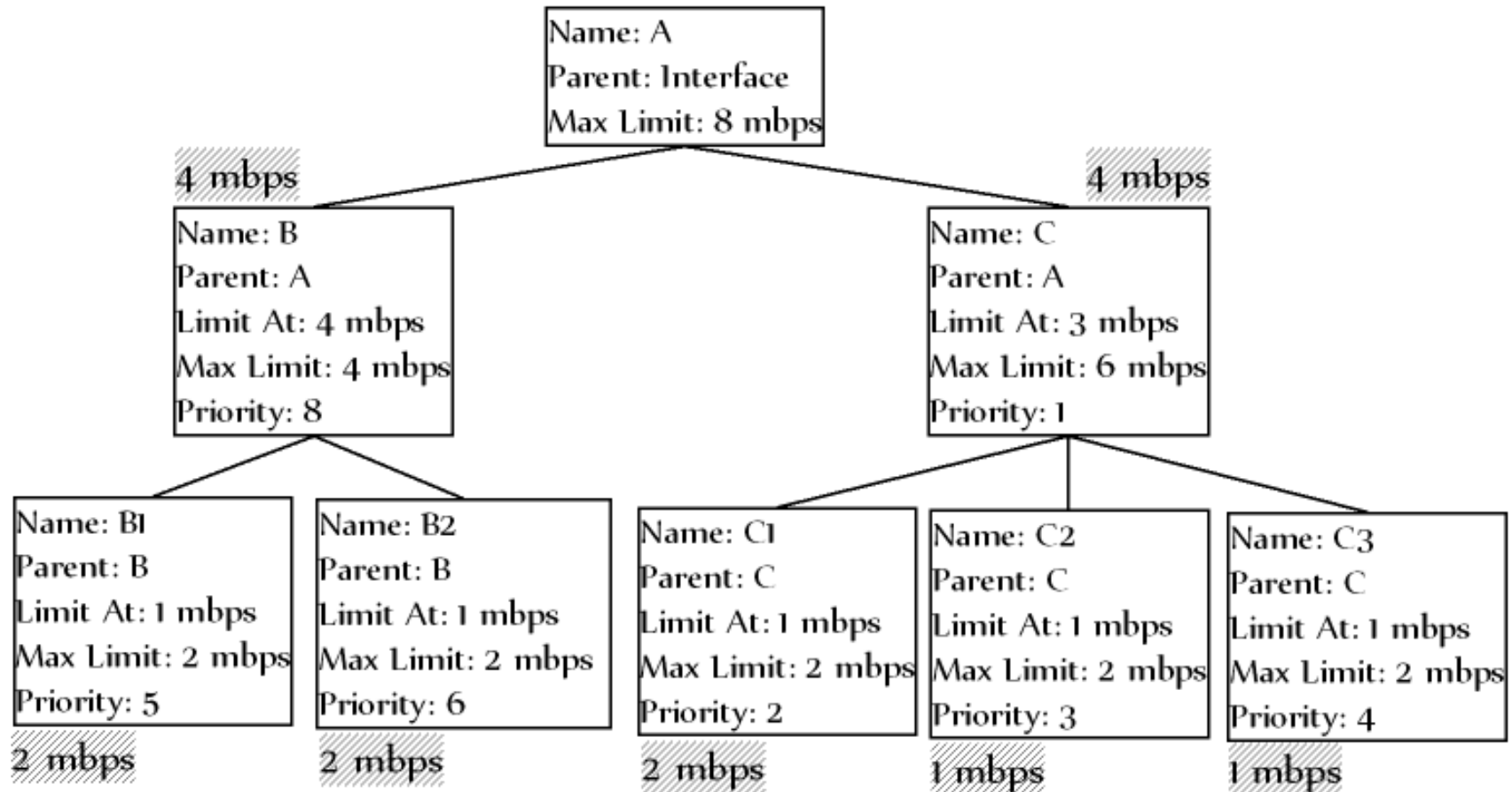
Queue List

Simple Queues Interface Queues Queue Tree Queue Types

+ - ✓ ✗ ⌵ 00 Reset Counters 00 Reset All Counters

Name	Parent	Packet Marks	Limit A...	Max Limit ...	Avg. Rate
HTB_09	ether1			8M	8.0 Mbps
Download_LaptopB	HTB_09		2M	4M	2.0 Mbps
Download_LaptopB1	Download_LaptopB	Mark_Packet_LaptopB1	1M	2M	1000.0 kbps
Download_LaptopB2	Download_LaptopB	Mark_Packet_LaptopB2	1M	2M	996.2 kbps
Download_LaptopC	HTB_09		3M	6M	6.0 Mbps
Download_LaptopC1	Download_LaptopC	Mark_Packet_LaptopC1	2M	3M	2.0 Mbps
Download_LaptopC2	Download_LaptopC	Mark_Packet_LaptopC2	2M	3M	2.0 Mbps
Download_LaptopC3	Download_LaptopC	Mark_Packet_LaptopC3	2M	3M	2.0 Mbps

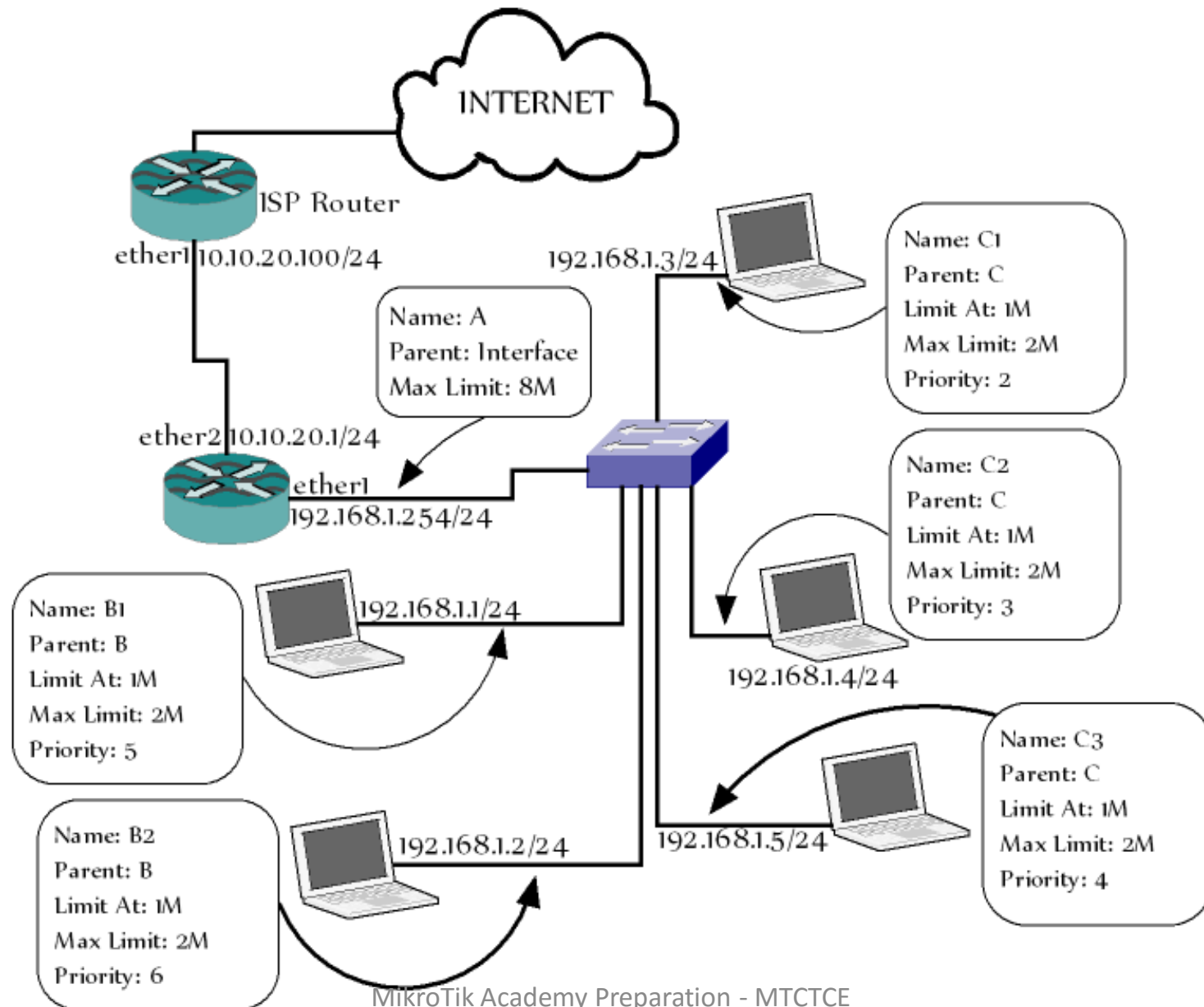
DISTRIBUSI HTB (10)



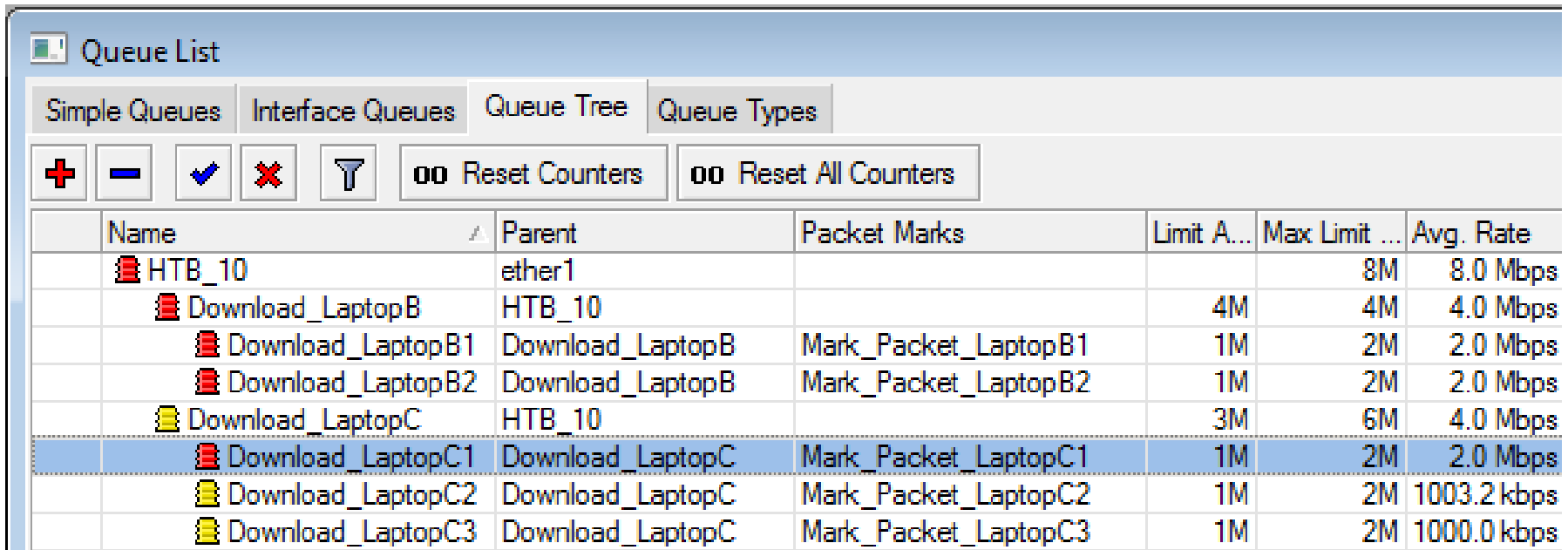
B akan mendapatkan 4 mbps karena Limit At

C1 mendapatkan lebih besar dari C2 dan C3 karena priority

DISTRIBUSI HTB (10)



DISTRIBUSI HTB (10)



Queue List

Simple Queues Interface Queues Queue Tree Queue Types

+ - ✓ ✗ ⏏ Reset Counters ⏏ Reset All Counters

Name	Parent	Packet Marks	Limit A...	Max Limit ...	Avg. Rate
HTB_10	ether1			8M	8.0 Mbps
Download_LaptopB	HTB_10		4M	4M	4.0 Mbps
Download_LaptopB1	Download_LaptopB	Mark_Packet_LaptopB1	1M	2M	2.0 Mbps
Download_LaptopB2	Download_LaptopB	Mark_Packet_LaptopB2	1M	2M	2.0 Mbps
Download_LaptopC	HTB_10		3M	6M	4.0 Mbps
Download_LaptopC1	Download_LaptopC	Mark_Packet_LaptopC1	1M	2M	2.0 Mbps
Download_LaptopC2	Download_LaptopC	Mark_Packet_LaptopC2	1M	2M	1003.2 kbps
Download_LaptopC3	Download_LaptopC	Mark_Packet_LaptopC3	1M	2M	1000.0 kbps

- Jika parent interface diubah menjadi 10 MB berapakah masing masing akan mendapatkan bandwidth ?

SCRIPT & SCHEDULER

SCRIPT

- Script digunakan untuk membuat command yang nantinya akan dijalankan secara otomatis oleh router sesuai dengan jadwal

Script <Internet>

Name:

Source:

```
/ip firewall nat enable 0
```

Script <No_Intemet>

Name:

Owner:

- Policy -

<input checked="" type="checkbox"/> ftp	<input checked="" type="checkbox"/> reboot
<input checked="" type="checkbox"/> read	<input checked="" type="checkbox"/> write
<input checked="" type="checkbox"/> policy	<input checked="" type="checkbox"/> test
<input checked="" type="checkbox"/> password	<input checked="" type="checkbox"/> sniff
<input checked="" type="checkbox"/> sensitive	

Last Time Started:

Run Count:

Source:

```
/ip firewall nat disable 0
```

SCHEDULER

- Menjalankan script yang telah dibuat
- **Interval**, interval eksekusi antara dua script, jika 0, script dieksekusi saat start saja, jika tidak 0 akan diulang sesuai interval waktu

Schedule <Jadwal_Intemet>

Name:

Start Date:

Start Time:

Interval:

On Event:
 ←

Schedule <JadwalTanpaInternet>

Name:

Start Date:

Start Time:

Interval:

On Event:
 ←