



Introduction to Mikrotik



Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia
(Mikrotik Certified Training Partner)



Citraweb Nusa Infomedia

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



Citraweb Nusa Infomedia

- Head Office

- Jalan Petung 31 Papringan
Yogyakarta 55281
Telp: 0274-554444
Fax: 0274-553055

- Rep. Office

- Gd Cyber Lt 11
Jl Kuningan Barat 8 Jakarta 12710
Telp: 021-5209612
Fax: 021-5209614



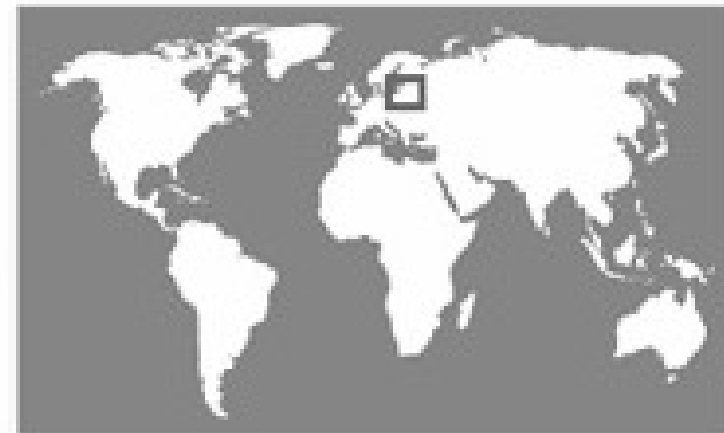
Apa itu Mikrotik?

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



Arti Kata Mikrotik ?

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



● ● ● | Pemilihan Routerboard

- Kinerja Processor
- Memori (RAM)
- Jumlah interface
 - Ethernet
 - MiniPCI
- Level Lisensi
 - Level 3 → wireless client / PTP
 - Level 4 → wireless access point
 - Custom Frequency ?



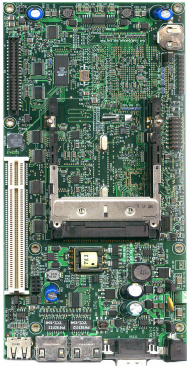
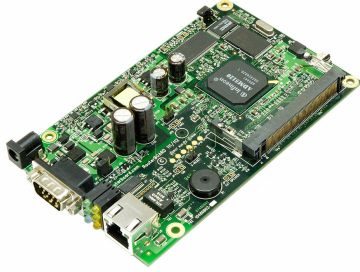
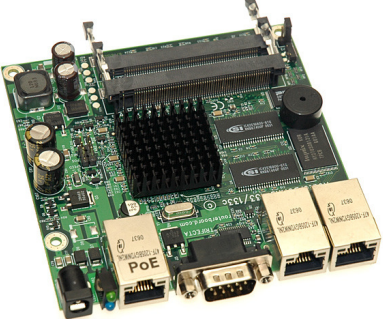
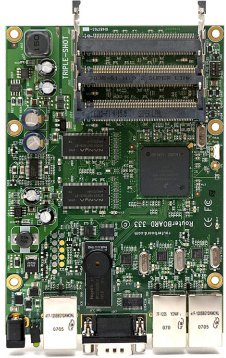
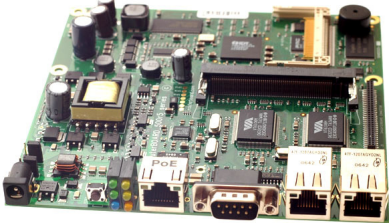
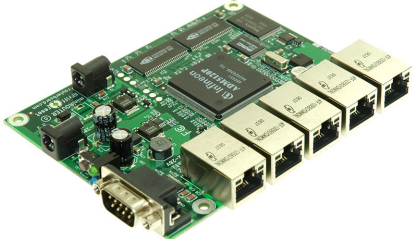
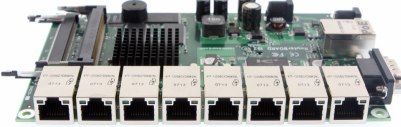

Routerboard untuk AP & CPE

Jenis	Processor	RAM	Ether	MiniPCI	USB	Radio	Lisensi
RB800	MPC8544 800MHz	256MB	3 (gig)	4	-	-	6
RB600	PPC266/400	128MB	3 (gig)	4	-	-	4
RB433UAH	AR7161 800MHz	128MB	3	3	2	-	5
RB433AH	AR7161 800MHz	128MB	3	3	-	-	5
RB433	AR7130 300 MHz	64MB	3	3	-	-	4
RB411AH	AR7161 800MHz	64MB	1	1	-	-	4
RB411AR	AR7130 300 MHz	64MB	1	1	-	1	4
RB411U	AR7130 300 MHz	32MB	1	1	1	-	4
RB411R	AR7130 300 MHz	32MB	1	-	-	1	3
RB411	AR7130 300 MHz	32MB	1	1	-	-	3

Routerboard untuk Indoor

Jenis	Processor	RAM	Ethernet	MiniPCI	Lisensi
RB1000	PPC 1333MHz	512MB	4 (gigabit)	0	6
RB493AH	Atheros AR7161 680 MHz/800MHz	64MB	9	3	5
RB493	Atheros AR7130 300 MHz	64MB	9	3	4
RB450G	Atheros AR7161 680 MHz/800MHz	256MB	5 (gigabit)	0	5
RB450	Atheros AR7130 300 MHz	32MB	5	0	5
RB750	Atheros AR7240 400MHz	32MB	5	0	4
RB750G	Atheros AR7161 680 MHz/800MHz	32MB	5 (gigabit)	0	4

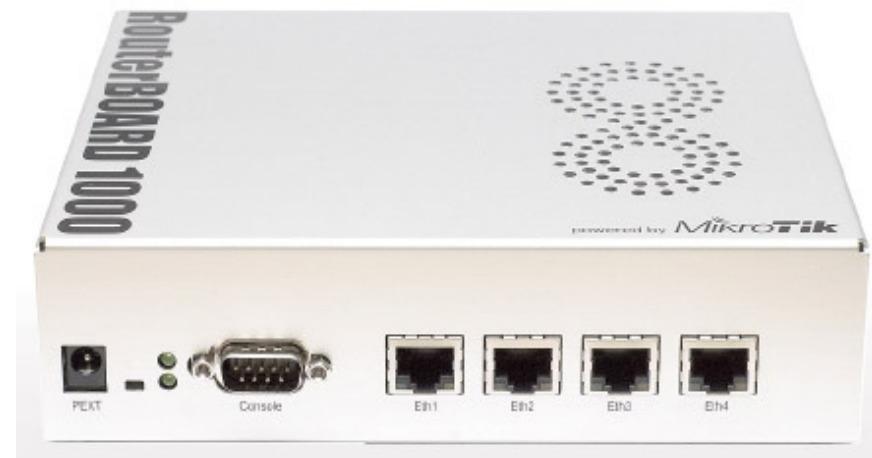
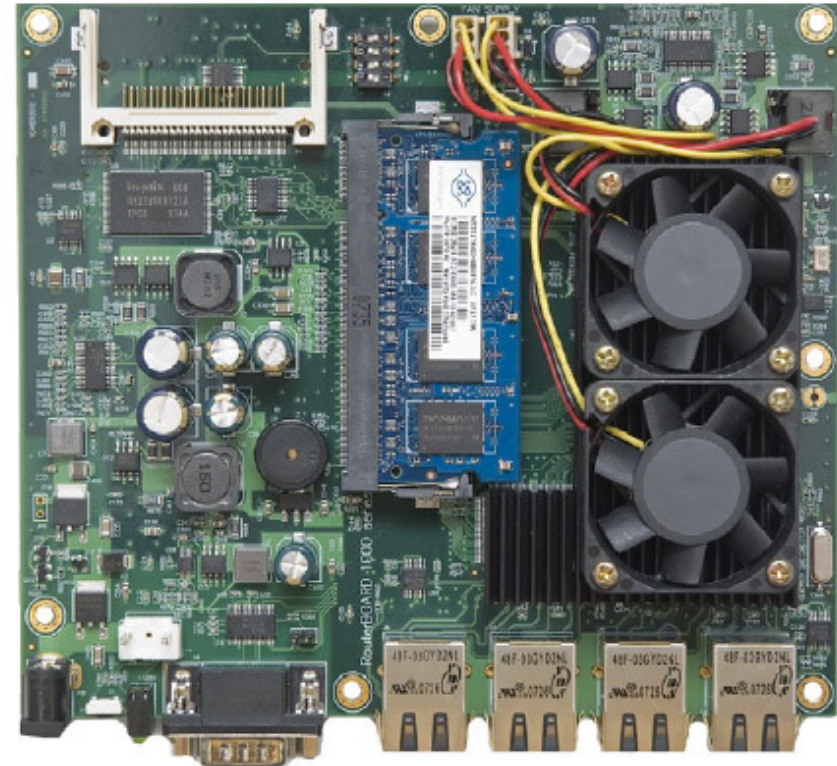
Discontinued Hardware

			
RB230	RB112	RB133	RB333
			
RB532	RB150	RB192	RB153



RB1000

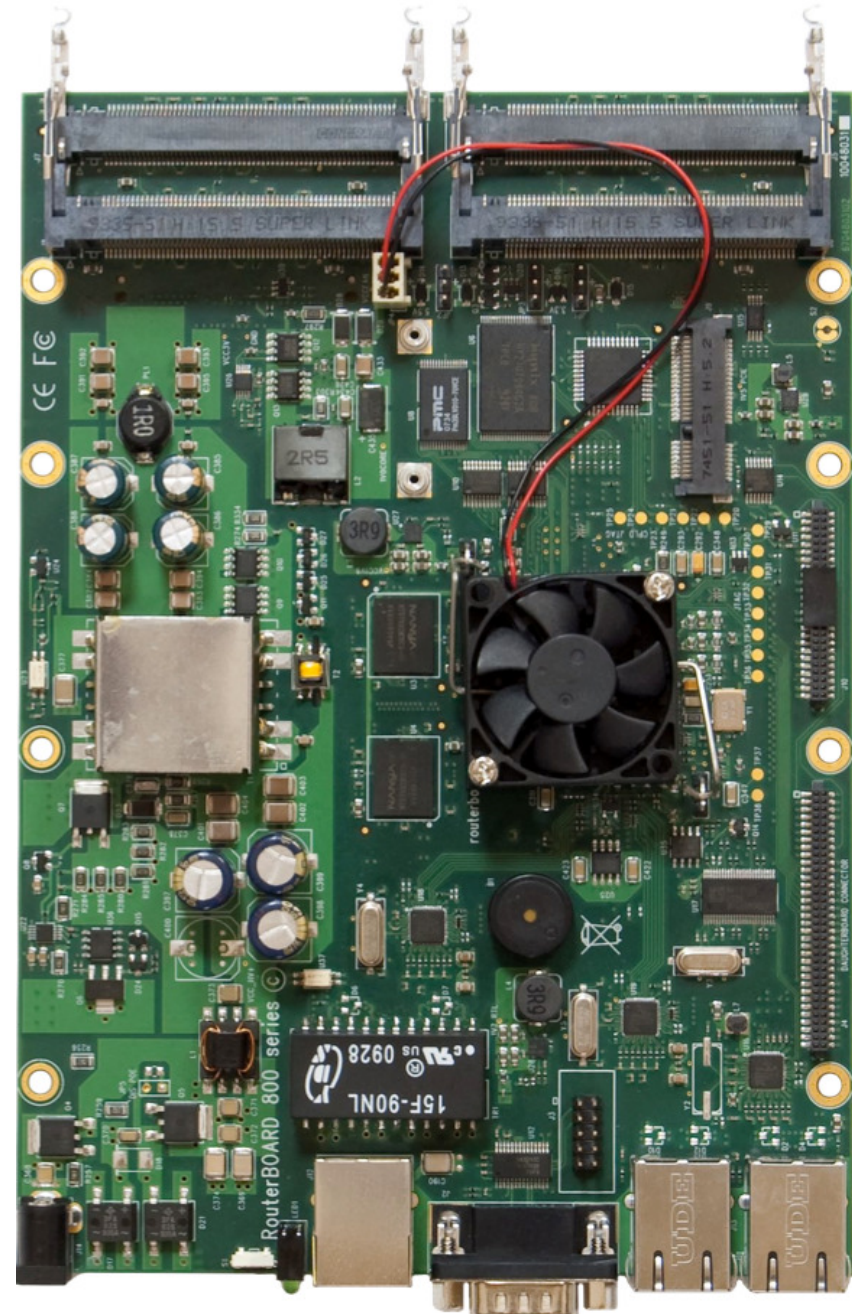
- 4 gigabit ethernet
- 0 minipci
- 1333 MHz processor
- RAM: 512MB
- up to:
 - 3 Gbps
 - 340.000 pps
- Tersedia juga dalam versi 1U rackmount





RB800

- 3 gigabit ethernet
- 4 minipci slot
- 1 minipci-e slot
- CF slot
- MPC8544 800MHz network CPU
- 256 DDR SDRAM
- RouterOS Level 5





RB600

- 3 gigabit ethernet
- 4 minipci slot
- MPC8343E 266/400MHz network CPU
- RouterOS Level 4



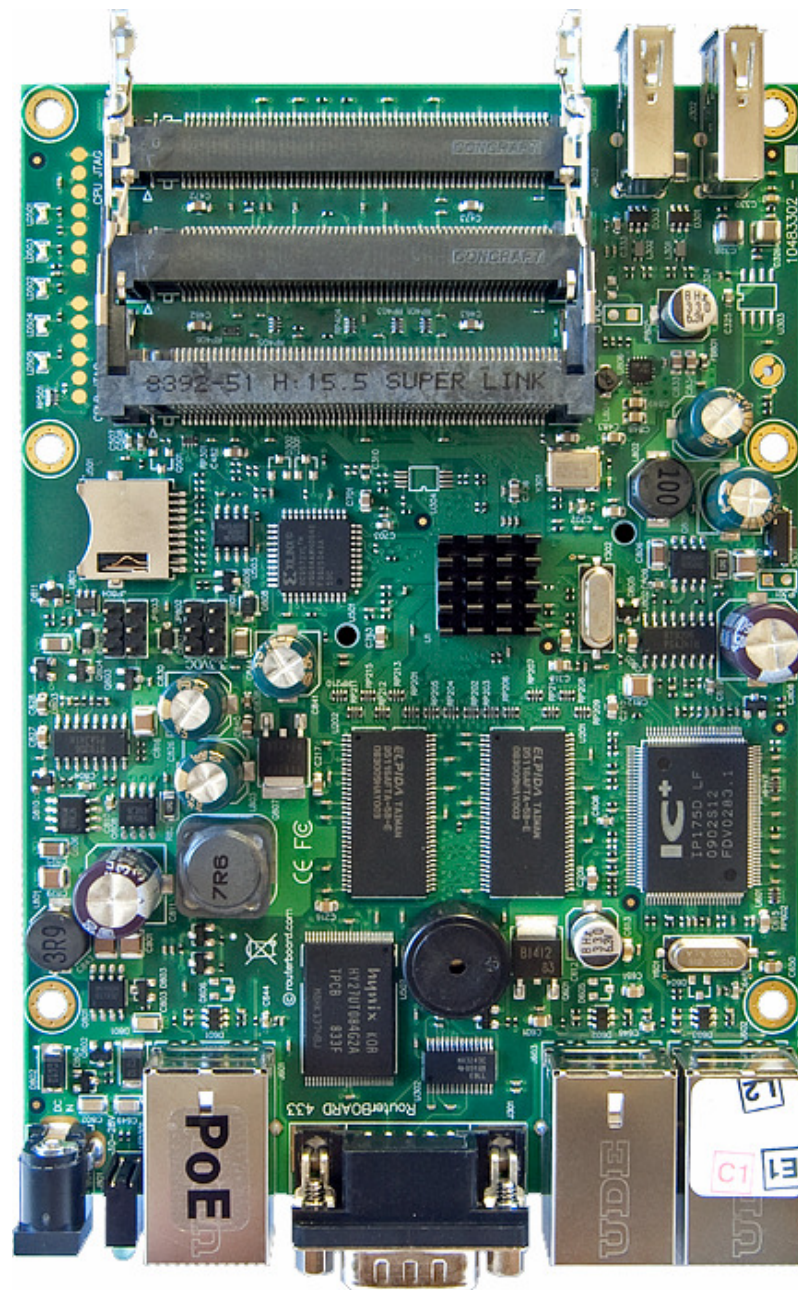
Tersedia daughterboard RB604

- Menambah jumlah minipci port 4 buah



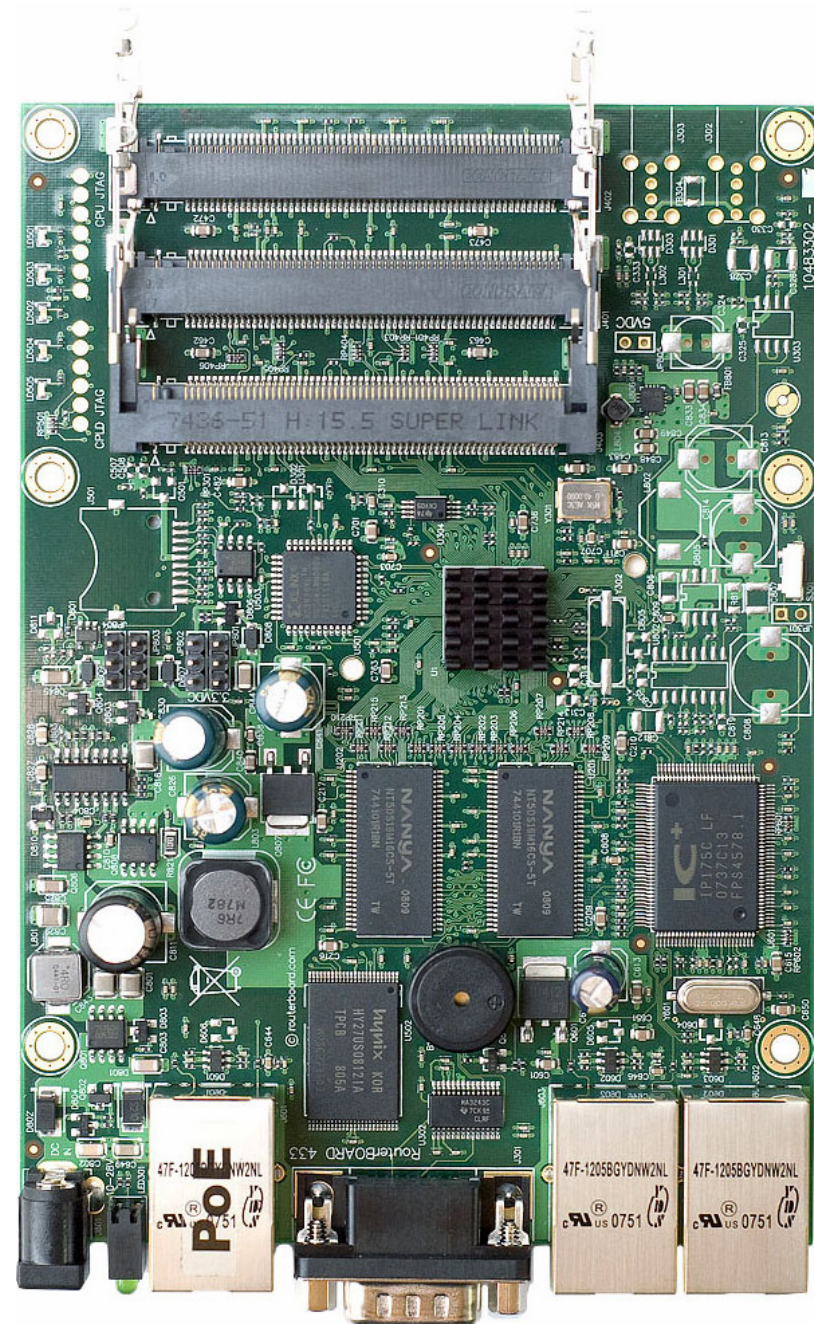
RB433UAH

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



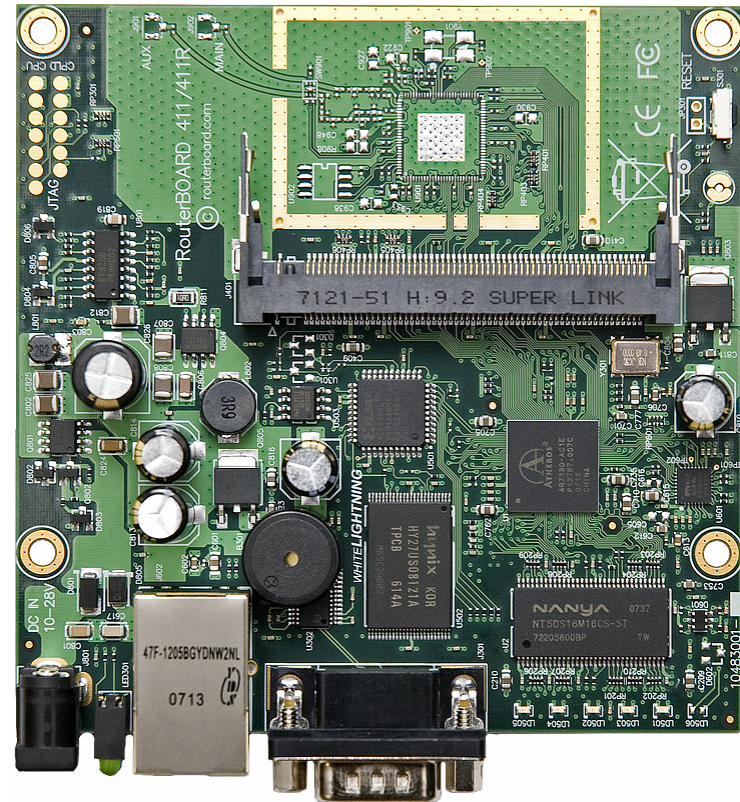
RB433

- 3 ethernet, 3 minipci
- Atheros AR7130 300 MHz
- RAM: 64MB
- RouterOS Level 4



RB411 / 411U / 411R / 411AR / 411AH

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





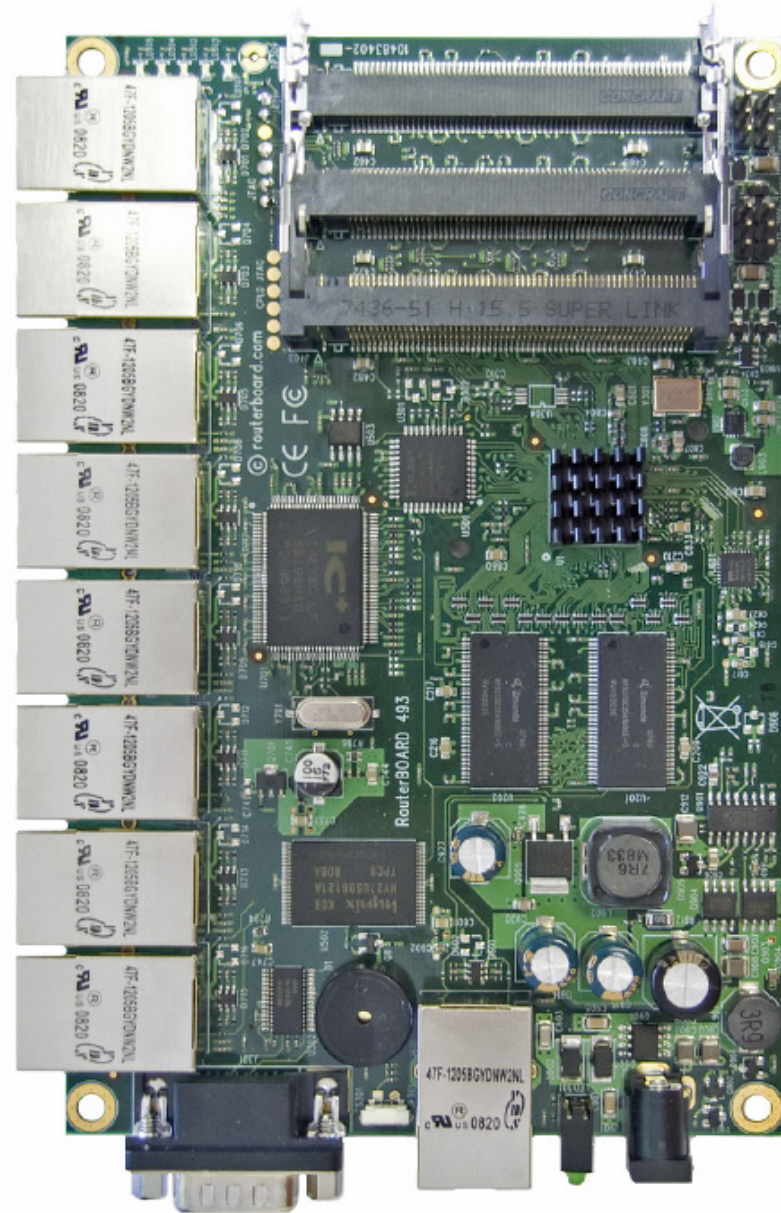
MikroPoynt

- Embedded Antenna 2,4GHz 11dbi
- With Routerboard 411 series



RB493(AH)

- 9 ethernet, 3 minipci
- Processor :
 - Atheros AR7161 680-800MHz (493AH)
 - Atheros AR7130 300MHz (493)
- RAM: 64MB
- RouterOS:
 - Level 4 (RB493)
 - Level 5 (RB493AH)





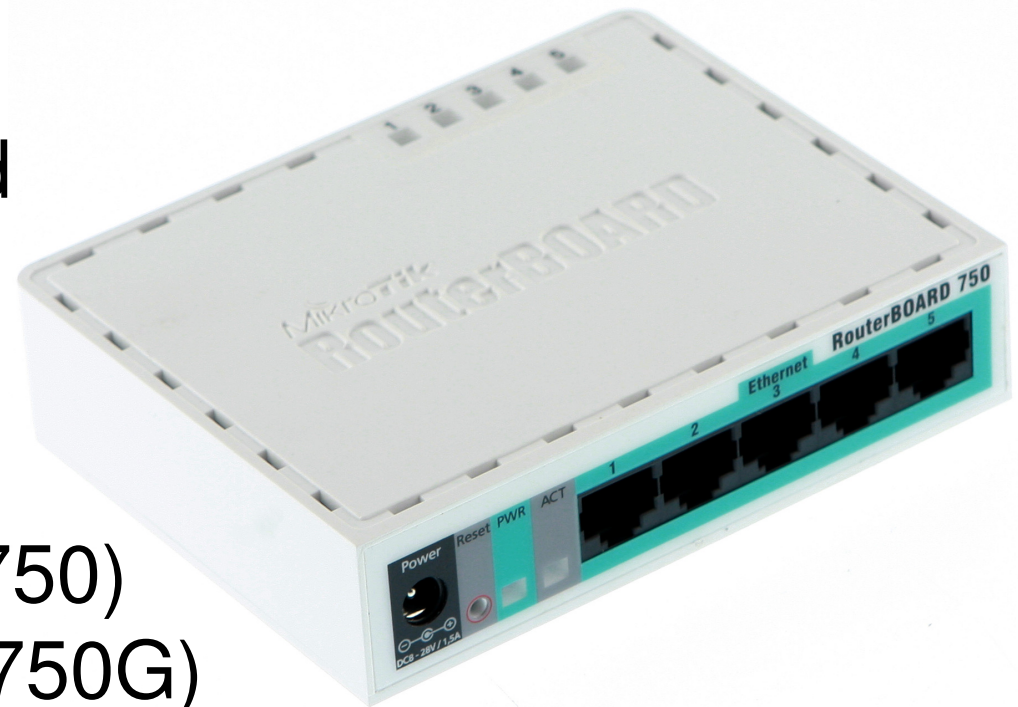
RB450G

- 5 gigabit port
- Tanpa minipci port
- Processor : Atheros AR7161 680 MHz
- RAM: 256 MB
- RouterOS Level 5



● ● ● | RB750 (G)

- Produk routerboard terbaru dan terkecil
- Processor :
AR7240 400Mhz (750)
AR7161 680MHz (750G)
- 5 ethernet port (750)
5 gigabit port (750G)
- Lisensi Level 4



● ● ● | Hardware (Interface)

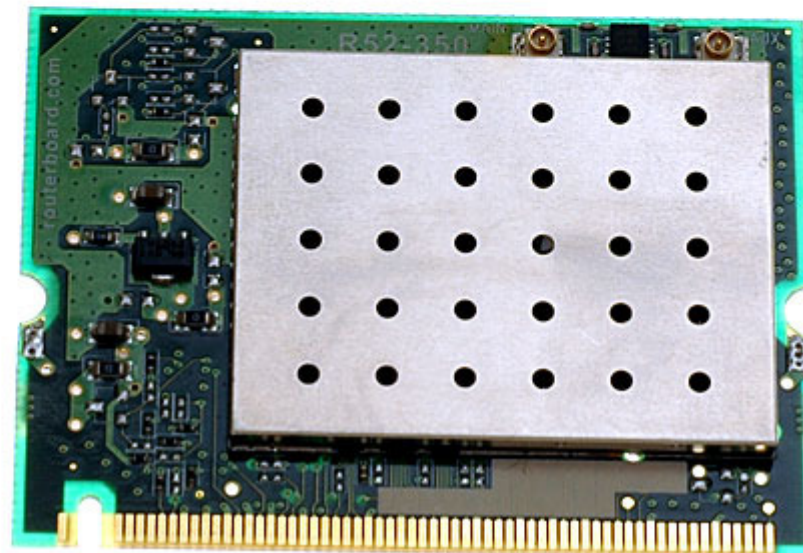
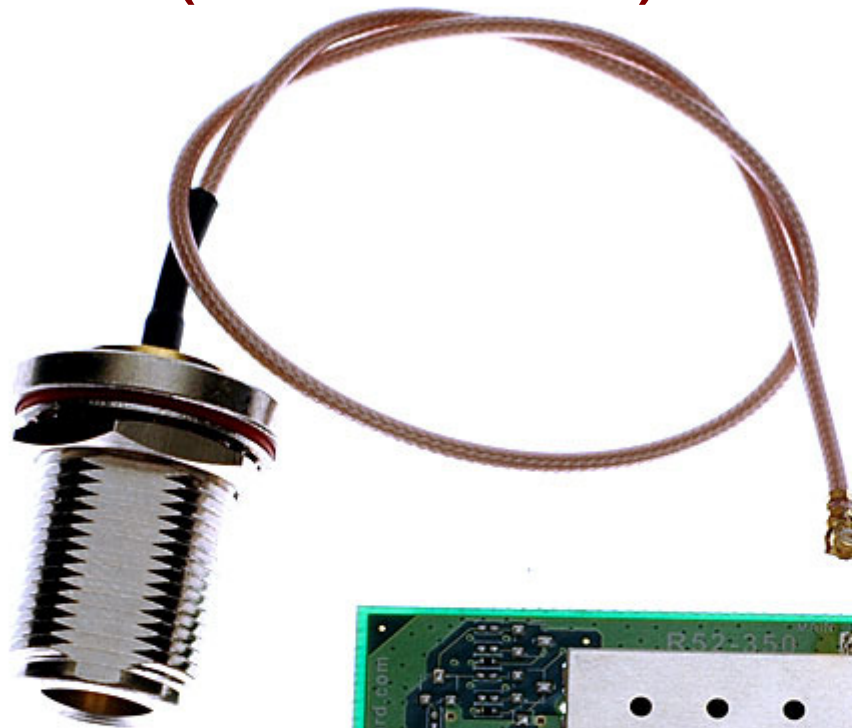
- R52
 - Atheros chipset
 - MiniPCI type interface
 - 65 mWatt
 - 3 band wireless
 - 2.4 GHz, 5.2 GHz, 5.8 GHz
 - Custom Frequency Support
 - 2.1 – 2.5 GHz
 - 4.9 – 6.0 GHz





Hardware (Interface)

- R52H
 - Atheros chipset
 - MiniPCI type interface
 - 350 mWatt
 - 3 band wireless
 - 2.4 GHz,
 - 5.2 GHz,
 - 5.8 GHz
 - Custom Frequency Support
 - 2.1 – 2.5 GHz
 - 4.9 – 6.0 GHz



R52N

NEW
PRODUCT

- Dual band IEEE 802.11 a/b/g/n standard
- Output Power of up to 25dBm @ b/g/n Band
- Support for up to 2x2 MIMO with spatial multiplexing
- Four times the throughput of 802.11 a/g
- Atheros AR9220, chipset
- 2 X U.FL Antenna Connector
- Operating temperatures: 0°C to 60°C
- Power consumption MAX 2.4W
- Modulations: OFDM: BPSK, QPSK, 16 QAM, 64QAM DSSS: DBPSK, DQPSK, CCK
- High Performance (up to 300Mbps physical data rates and 200Mbps of actual user throughput) with Low Power Consumption
- ESD protection against +/-10kV ESD discharge on Antenna port



R2N

NEW
PRODUCT

- 4.4GHz IEEE 802.11b/g/n standard
- Output Power of up to 25dBm @ b/g/n Band
- Support for up to 2x2 MIMO with spatial multiplexing
- Four times the throughput of 802.11a/g
- Atheros AR9223, chipset
- 2 X U.FL Antenna Connector
- Operating temperatures: 0°C to 60°C
- Power consumption MAX 2.4W
- Modulations:
OFDM: BPSK, QPSK, 16 QAM, 64QAM
DSSS: DBPSK, DQPSK, CCK
- High Performance (up to 300Mbps physical data rates and 200Mbps of actual user throughput) with Low Power Consumption
- ESD protection against +/-10kV ESD discharge on Antenna port



RB600 + R52N



- Throughput: 195 Mbps



Mikrotik RouterOS

- RouterOS adalah sistem operasi dan perangkat lunak yang mampu membuat PC berbasis Intel/AMD mampu melakukan fungsi router, bridge, firewall, pengaturan bandwidth, wireless AP ataupun client, dan masih banyak fungsi lainnya
- RouterOS dapat melakukan hampir semua fungsi networking dan juga beberapa fungsi server.



Keunggulan

- Membuat PC yang murah menjadi router yang handal
- Pembaharuan versi secara berkala
- Memiliki banyak fitur
- Memiliki user interface yang mudah dan konsisten
- Ada banyak cara untuk mengakses dan mengontrol
- Instalasi yang cepat dan mudah
- Memungkinkan upgrade hardware
- Banyak alternatif interface yang dapat digunakan

● ● ● | Penggunaan Kernel

- RouterOS version 2.9.xx
 - Linux Kernel version 2.4.31
- RouterOS version 3.X
 - Linux Kernel version 2.6.19
- RouterOS version 4.X
 - Linux Kernel version 2.6.27.39

For more detailed information see:

<http://www.kernel.org>

Hardware Compability (versi 3.x)

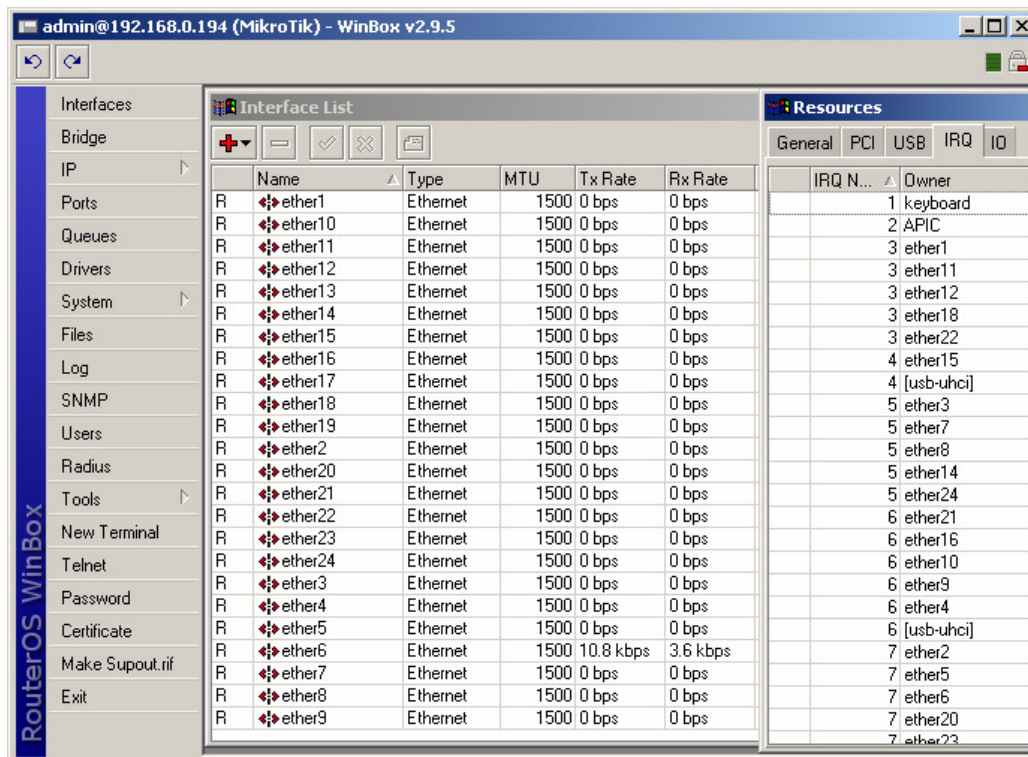
- SMP (Symetric Multiprocessing) support



- SATA disk support
- Maximum RAM support increased from 1GB to 2 GB
- Latest interface driver support
- Dropped Legacy interface support

RB44 Test

- 6 pcs RB44
- Total of 24 ethernet ports



The screenshot shows the MikroTik WinBox v2.9.5 interface. The 'Interface List' table is displayed, showing 24 Ethernet interfaces (ether1 through ether24) with their respective MTU, Tx Rate, and Rx Rate. The 'Resources' tab is also visible, showing IRQ assignments for each interface.

Name	Type	MTU	Tx Rate	Rx Rate
ether1	Ethernet	1500	0 bps	0 bps
ether10	Ethernet	1500	0 bps	0 bps
ether11	Ethernet	1500	0 bps	0 bps
ether12	Ethernet	1500	0 bps	0 bps
ether13	Ethernet	1500	0 bps	0 bps
ether14	Ethernet	1500	0 bps	0 bps
ether15	Ethernet	1500	0 bps	0 bps
ether16	Ethernet	1500	0 bps	0 bps
ether17	Ethernet	1500	0 bps	0 bps
ether18	Ethernet	1500	0 bps	0 bps
ether19	Ethernet	1500	0 bps	0 bps
ether2	Ethernet	1500	0 bps	0 bps
ether20	Ethernet	1500	0 bps	0 bps
ether21	Ethernet	1500	0 bps	0 bps
ether22	Ethernet	1500	0 bps	0 bps
ether23	Ethernet	1500	0 bps	0 bps
ether24	Ethernet	1500	0 bps	0 bps
ether3	Ethernet	1500	0 bps	0 bps
ether4	Ethernet	1500	0 bps	0 bps
ether5	Ethernet	1500	0 bps	0 bps
ether6	Ethernet	1500	10.8 kbps	3.6 kbps
ether7	Ethernet	1500	0 bps	0 bps
ether8	Ethernet	1500	0 bps	0 bps
ether9	Ethernet	1500	0 bps	0 bps





Fitur Mikrotik RouterOS (1)

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



Fitur Mikrotik RouterOS (2)

- Services
 - Web Proxy, Hotspot, DHCP, IP Pool, DNS Server
- AAA
 - PPP, Radius Client, User-Manager
 - IP Accounting, Traffic Flow
- Monitoring
 - Graphs, Watchdog, Torch, Custom Log, SNMP
- Diagnostic Tools & Scripting
 - Ping, TCP Ping, Tracert, Network Monitoring, Traffic Monitoring, Scheduler, Scripting
- VRRP



Licence Level

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



Pembelian Lisensi

- Online, real time, pembayaran dengan kartu kredit, di www.mikrotik.com
- Online di www.mikrotik.co.id
 - Waktu proses 1 hari kerja
 - Transfer ke rekening bank lokal
 - Lebih murah!
 - Real time license processing! Setelah pembayaran diterima.
 - Real time payment processing, via IndoMOG

Checking Licence

The screenshot shows the Mikrotik WinBox interface. The left sidebar contains a menu with 'System' and 'License' highlighted with red circles. The main window displays two sub-windows: 'License' and 'Package List'.

License Window:

- Software ID: H2Z6-3TT
- Upgradable To: v3.x
- Level: 4
- Features: extra-channels
- Expires In: [empty]
- Buttons: OK, Paste Key, Import Key..., Export Key..., Upgrade/Get New Key...

Package List Window:

Name	Version	Build Time	Scheduled
routeros-mipsle	3.2	Jan/31/2008 18:18:50	
advanced-t...	3.2	Jan/31/2008 17:04:52	
dhcp	3.2	Jan/31/2008 17:07:45	
hotspot	3.2	Jan/31/2008 17:16:23	
X ipv6	3.2	Jan/31/2008 17:14:42	
X mpls	3.2	Jan/31/2008 18:00:24	
ppp	3.2	Jan/31/2008 17:10:30	
routerboard	3.2	Jan/31/2008 17:52:18	
routing	3.2	Jan/31/2008 17:14:02	
security	3.2	Jan/31/2008 17:06:44	
system	3.2	Jan/31/2008 17:03:53	
wireless	3.2	Jan/31/2008 17:21:29	

● ● ● | Produk Mana Yang Dipilih

- Kenalilah kebutuhan Anda:
 - Fungsi perangkat
 - Jumlah trafik
 - Fitur yang dibutuhkan
 - Interface yang dibutuhkan
- Baik menggunakan PC ataupun menggunakan Routerboard, fitur Mikrotik RouterOS selalu sama (tergantung pada level yang digunakan)

● ● ● | Berdasarkan Processor

- PC
 - SMP (Symmetric Multiprocessing) support
 - Single Core
- Routerboard System
 - RB411,411U,411R,411AR,433,450,493 – 300mhz
 - RB411AH,433AH,493AH,450G,433UAH – 680mhz
 - RB600 – PPC 400mhz with co-processor
 - RB1000 – PPC 1333Mhz with co-processor

● ● ● | Kebutuhan Router

- Berapa jumlah interface yang dibutuhkan?
 - untuk WAN
 - untuk LAN
 - untuk kebutuhan khusus (proxy, server)
- Kita dapat memanfaatkan VLAN dengan switch untuk mengurangi jumlah interface fisik

● ● ● | Fungsi Web-Proxy

- Untuk fungsi web-proxy, kita membutuhkan router yang bisa memiliki storage yang cukup besar:
 - PC + DoM sebagai system + HD sebagai cache
 - RB1000 + compact flash
 - RB600 + compact flash
 - RB433AH + micro drive
 - RB433UAH + micro drive / external HD
 - RB493AH + micro drive



GSM Router

- RB433UAH + modem GSM/3G (USB)
- RB411U + modem GSM/3G (USB)

● ● ● | Wireless Device

- Berapa interface wireless yang dibutuhkan?
- Beberapa perangkat yang tidak memiliki minipci :
 - RB1000, RB450, RB450G, RB750
- Untuk access point, tidak bisa menggunakan level 3, harus minimal level 4 (RB411 & 411R memiliki level 3, sehingga tidak bisa dijadikan access point)



Wireless Repeater

- Wireless repeater bisa dilakukan Menggunakan lebih dari satu MiniPCI Wireless Card
 - RB433, RB433AH - 3 MiniPCI slot Available
 - RB600 - 4 MiniPCI slot Available
 - RB800 - 4 MiniPCI slot Available

● ● ● | Wireless Full Duplex

- Komunikasi wireless sebenarnya menggunakan transmisi half-duplex.
- Mikrotik mampu mengimplementasikan Wireless FullDuplex menggunakan Nstreme-Dual.
- RB433 & RB433AH – 2 Wireless card
- RB600 – 2 wireless card

● ● ● | Kebutuhan Gigabit

- Beberapa perangkat yang memiliki interface gigabit :
 - PC + DOM + RB44GV
 - RB1000
 - RB600
 - RB800
 - RB450G
 - RB750G

● ● ● | Radius Server (UserManager)

- Radius Server dapat digunakan secara lengkap menggunakan :
 - PC + License Level 6
 - RB1000
 - RB800
 - RB433AH (maksimal 50 active users)
 - RB433UAH (maksimal 50 active users)



Mikrotik Installation

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

● ● ● | Instalasi Mikrotik

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



Installation

- CD
 - Create CD from CD image (iso file)
- Netinstall
 - Via network using NetInstall program. The prospective router should be booted from a network by using special floppy or network cards features (PXE, EtherBoot)



Download Area mikrotik.co.id

- Faster from Indonesia internet
- Connected 100mbps to OpenIXP

Download Area

Halaman ini merupakan mirror download area, supaya pengguna yang ada di Indonesia dan terhubung ke jaringan OpenIXP bisa mendownload installer ataupun paket upgrade dengan lebih mudah.

Lihat juga: [change-log terbaru](#).

Keterangan:

- File dengan nama "*mipsle*" : RB100, RB500
- File dengan nama "*x86*" : PC Intel/AMD/RB200
- File dengan nama "*ppc/powerpc*" : RB300, RB600
- File dengan nama "*mipsbe*" : RB400

Software Instalasi

CD Instalation

Jika Anda bermaksud menginstall Mikrotik di PC Anda, mungkin file inilah yang Anda butuhkan untuk membuat CD Boot instalasi. [\[panduan\]](#)
[mikrotik-3.2.iso](#) (20.35 MByte, didownload 234 kali)

Mikrotik NetInstall

Software yang dibutuhkan untuk melakukan netinstall. Masih dibutuhkan juga modul all_packages di bawah. [\[panduan\]](#).
[netinstall.zip](#) (6.05 MByte, didownload 2773 kali)

Software Upgrade

Semua modul dalam satu paket

Satu buah paket yang berisikan semua modul Mikrotik. Untuk penggunaan versi 2.9 atau yang lebih baru, gunakanlah paket ini. [\[panduan\]](#)
[routeros-mipsbe-3.2.npk](#) (9.38 MByte, didownload 69 kali)
[routeros-mipsle-3.2.npk](#) (9.31 MByte, didownload 52 kali)
[routeros-powerpc-3.2.npk](#) (9.65 MByte, didownload 54 kali)
[routeros-x86-3.2.npk](#) (11.14 MByte, didownload 73 kali)

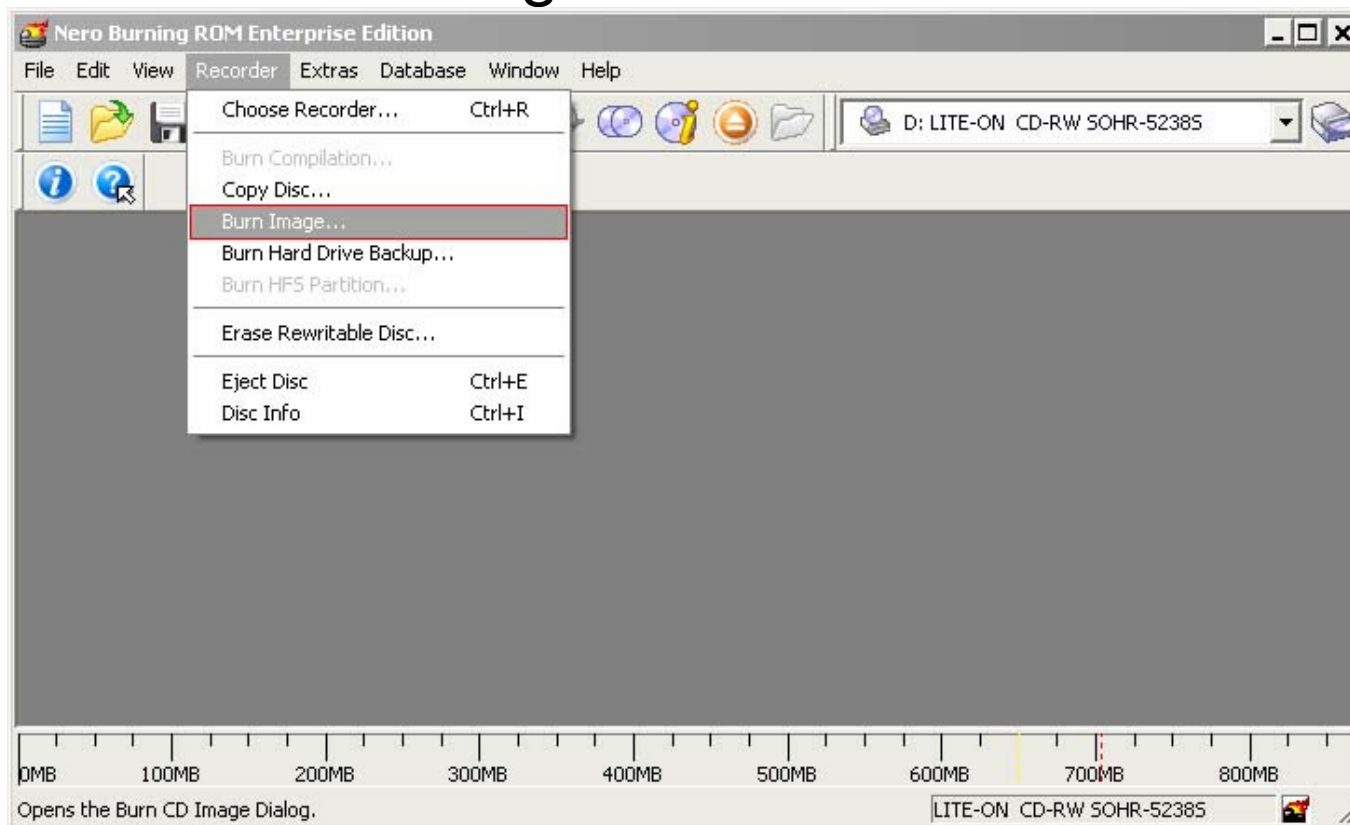
All Packages

Berisikan paket-paket yang bisa digunakan untuk upgrade versi. Cukup dipilih paket-paket yang dibutuhkan saja saat melakukan FTP ke router. [\[panduan\]](#).
[all_packages-mipsbe-3.2.zip](#) (14.99 MByte, didownload 29 kali)
[all_packages-mipsle-3.2.zip](#) (14.87 MByte, didownload 38 kali)
[all_packages-ppc-3.2.zip](#) (14.89 MByte, didownload 20 kali)
[all_packages-x86-3.2.zip](#) (17.5 MByte, didownload 41 kali)



CD Installation (1)

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





CD Installation (2)

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

```
Welcome to MikroTik Router Software installation
```

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

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



CD Installation (2)

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

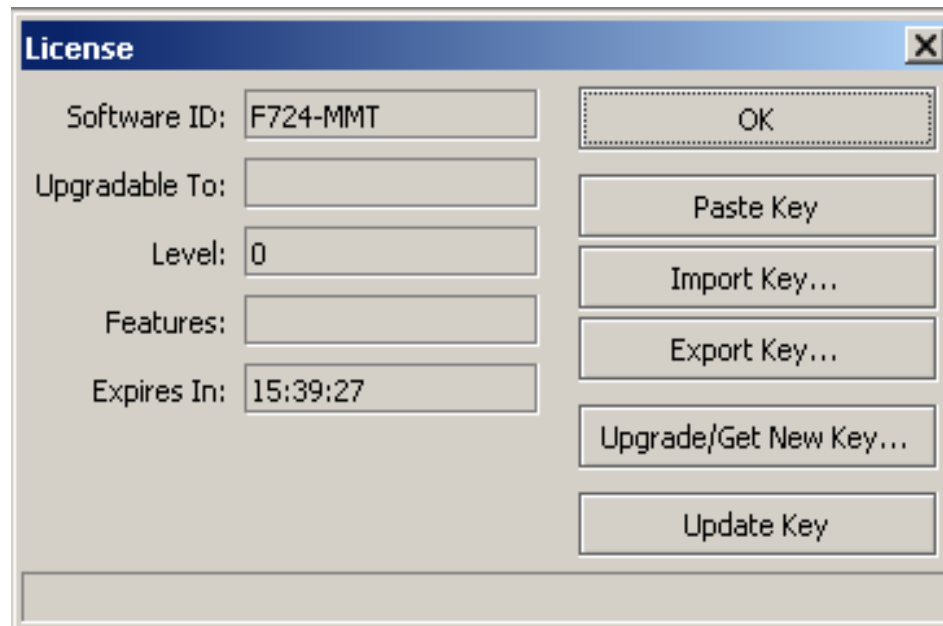
● ● ● | Installation

- Login User dan password
 - user = admin dan password = [kosong]
- Welcome menu
- Level 0
- Software id =
F724-MMT



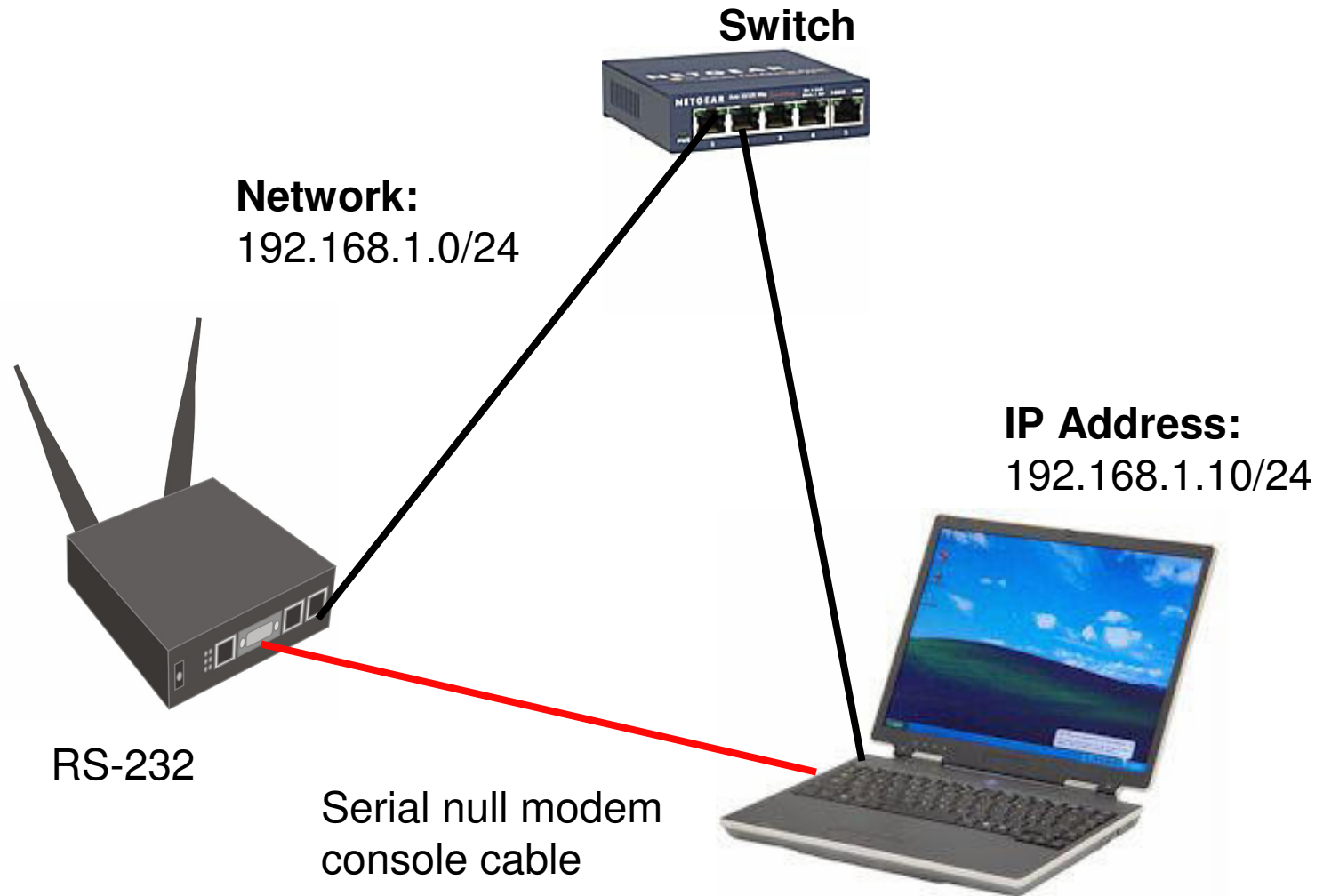
● ● ● | Installation

- License level 0
- Demo time
15:39:27 jam
- Copy license key
tekan tombol
Paste Key





Netinstall





Netinstall

- Download program netinstall dan module yang dibutuhkan
- Hubungkan router dengan komputer via cross utp cable atau via switch
- Hubungkan juga router dengan komputer via console cable
- Jalankan program netinstall, dan hidupkan service
- Hidupkan router, masuk ke setting BIOS
- Pilih boot via ethernet restart
- Pilih router
- Pilih module yang akan diinstall
- Start install Selesai
- Kembalikan boot ke IDE drive



Netinstall – BIOS Setting

```
RouterBOOT booter 2.12
```

```
RouterBoard 333
```

```
CPU frequency: 333 MHz
```

```
Memory size: 64 MB
```

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




Netinstall – BIOS Setting

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



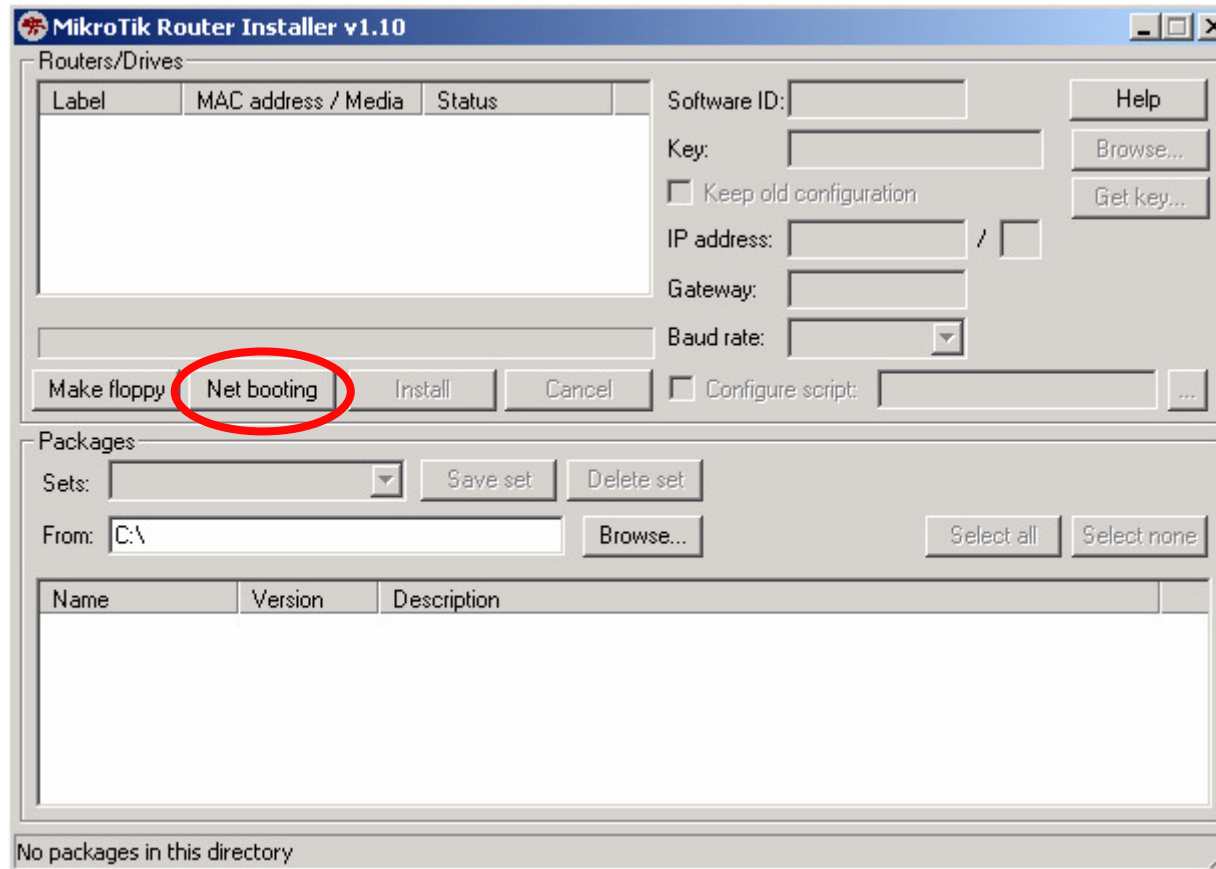
Netinstall – BIOS Setting

Select boot device:

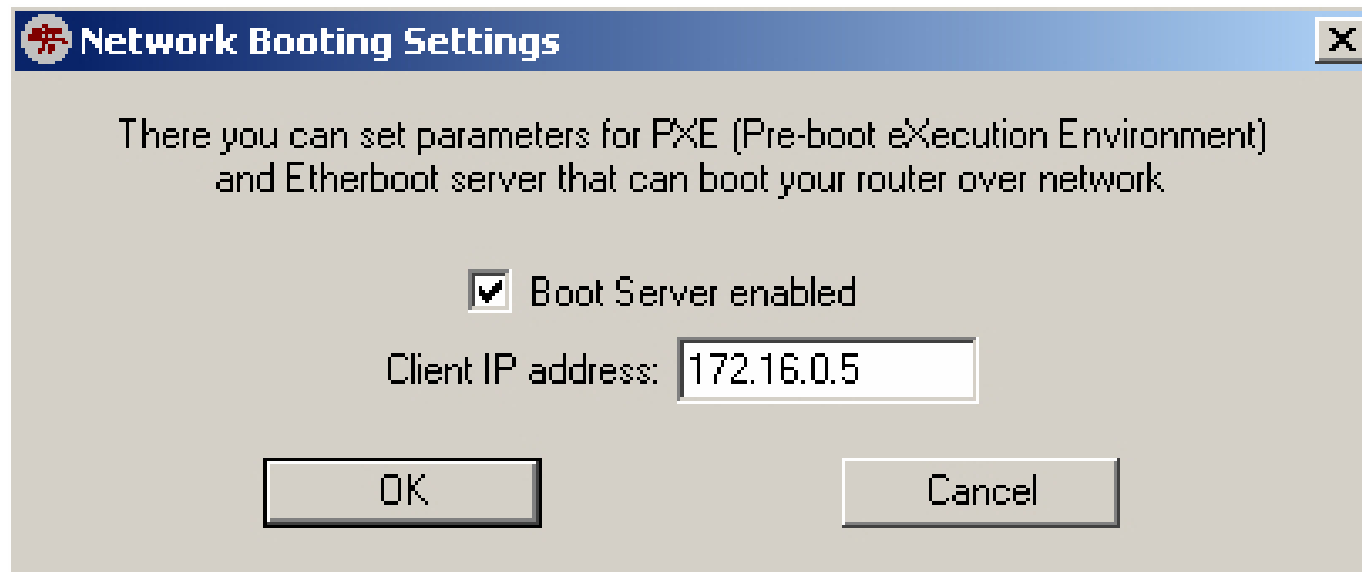
- * e - boot over Ethernet
- n - boot from NAND, if fail then Ethernet
- l - boot Ethernet once, then NAND
- o - boot from NAND only
- b - boot chosen device

your choice: █

Netinstall Software

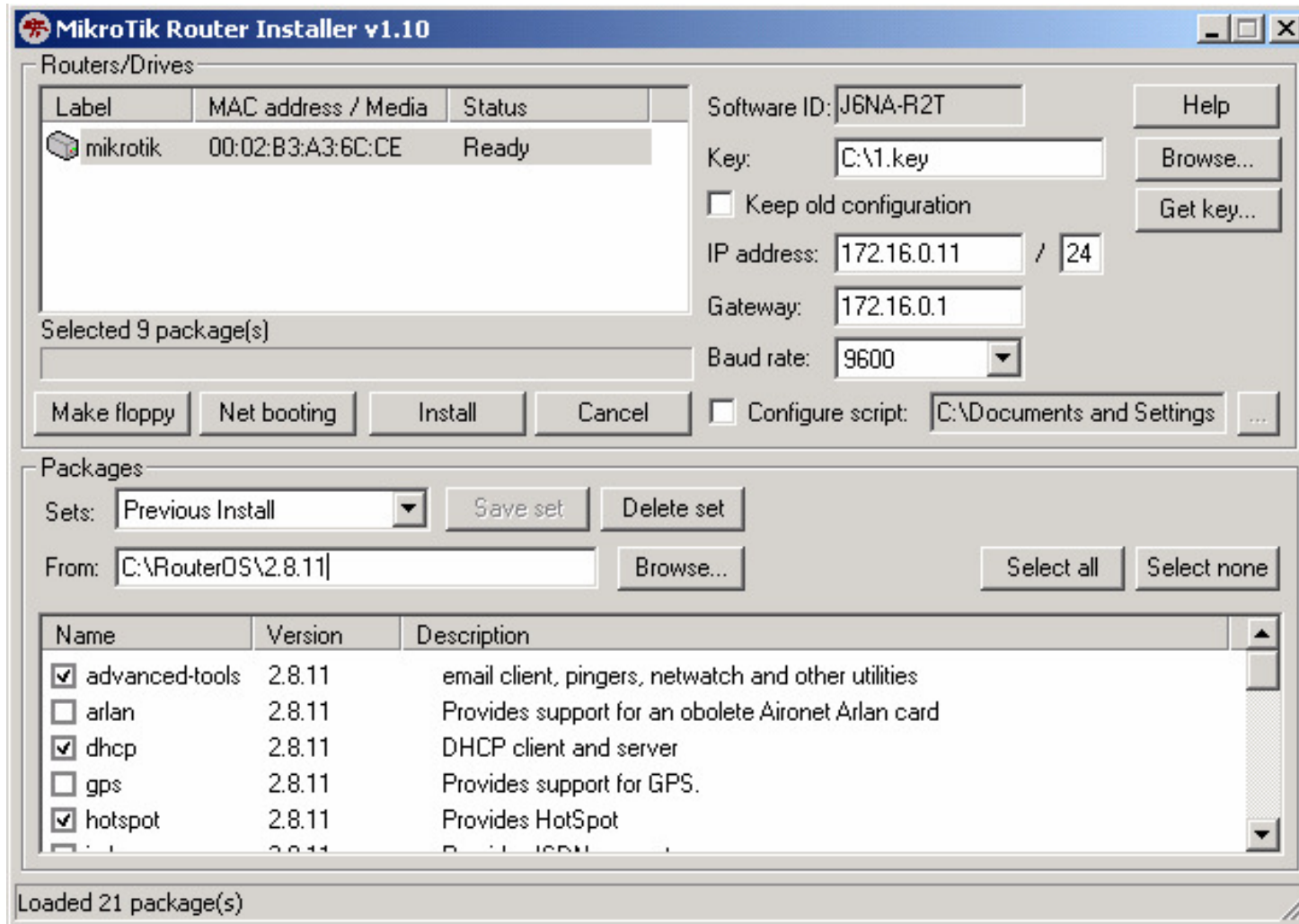


Netinstall Software



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

Netinstall Software



System Package

- Pada terminal: `/system package print`

Name	Version	Build Time	Scheduled
routeros-x86	3.22	Mar/16/2009 10:48:17	
advancedt...	3.22	Mar/16/2009 10:43:47	
dhcp	3.22	Mar/16/2009 10:43:58	
hotspot	3.22	Mar/16/2009 10:45:17	
X ipv6	3.22	Mar/16/2009 10:44:58	
X mpls	3.22	Mar/16/2009 10:47:02	
ppp	3.22	Mar/16/2009 10:44:05	
routerboard	3.22	Mar/16/2009 10:46:46	
routing	3.22	Mar/16/2009 10:44:10	
security	3.22	Mar/16/2009 10:43:55	
system	3.22	Mar/16/2009 10:43:27	
wireless	3.22	Mar/16/2009 10:45:50	

12 items

Paket di RouterOS

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



Version Upgrade

- Download modul
 - routers-mipsbe-3.xx.npk (RB400 & RB700)
 - routers-mipsle-3.xx.npk (RB100 & RB500)
 - routers-powerpc-3.xx.npk (RB300 & RB600)
 - routers-x86-3.xx.npk (PC & RB200)
- FTP modul tersebut ke router
 - Harus menggunakan userid yang full access
- Soft Reboot, jangan hard reboot

● ● ● | Version Downgrade

- Download modul
- FTP modul tersebut ke router
- Cek modul : */file print*
- */system package downgrade*

```
admin@MikroTik] system package> downgrade  
Router will be rebooted. Continue? [y/N]: y  
system will reboot shortly
```

● ● ● | Command Line Interface

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



General Command CLI

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



Navigasi pada CLI

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

● ● ● | Command Line Interface

- Quick Typing
 - [TAB] untuk melengkapi perintah tertentu
 - */system shut [TAB] = /system shutdown*
 - Juga bisa menggunakan singkatan
 - */sys shut = /system shutdown*



RouterOS Basic Configuration

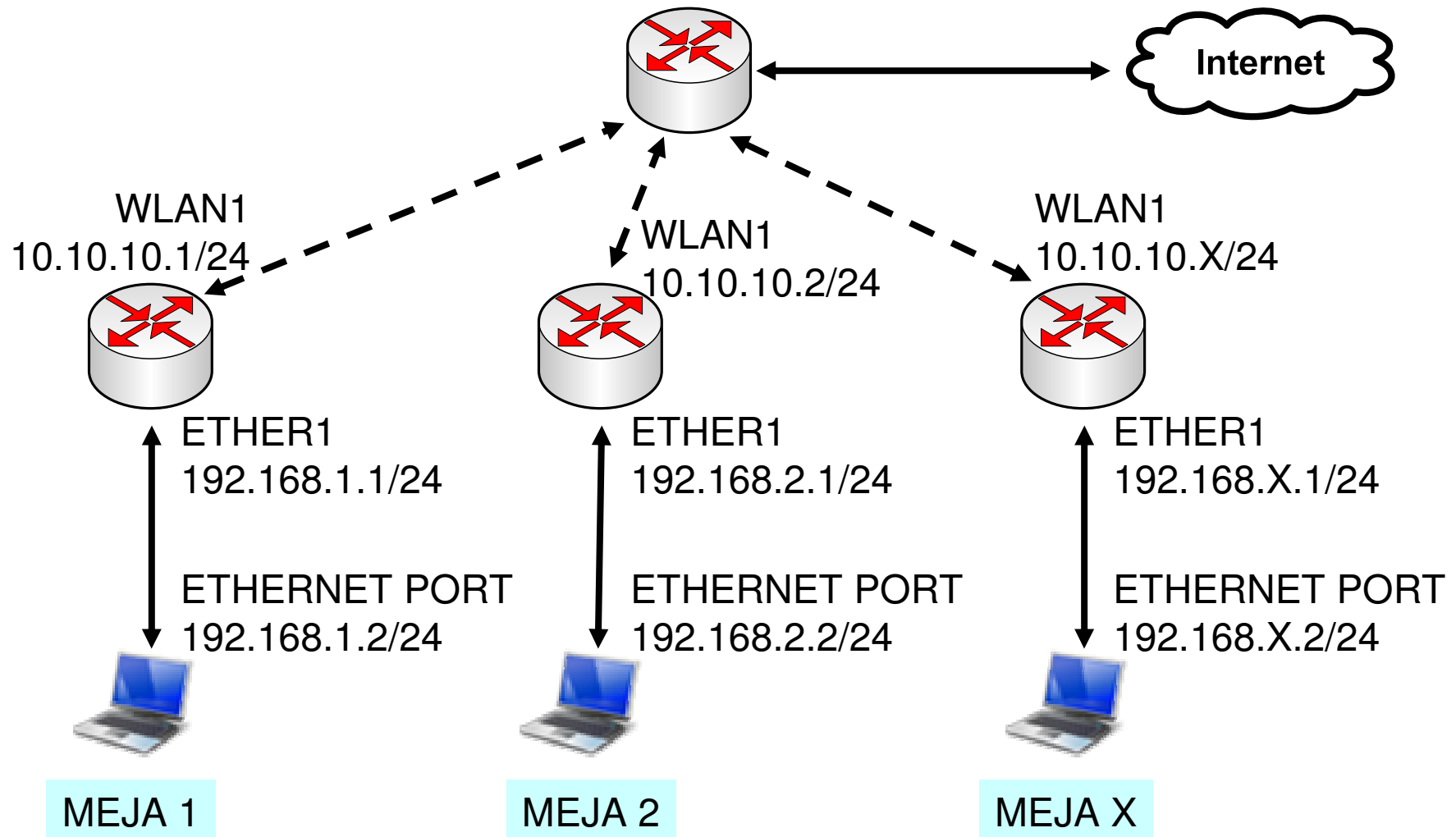
Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)



● ● ● | [LAB-1] Konfigurasi Dasar





IP Configuration

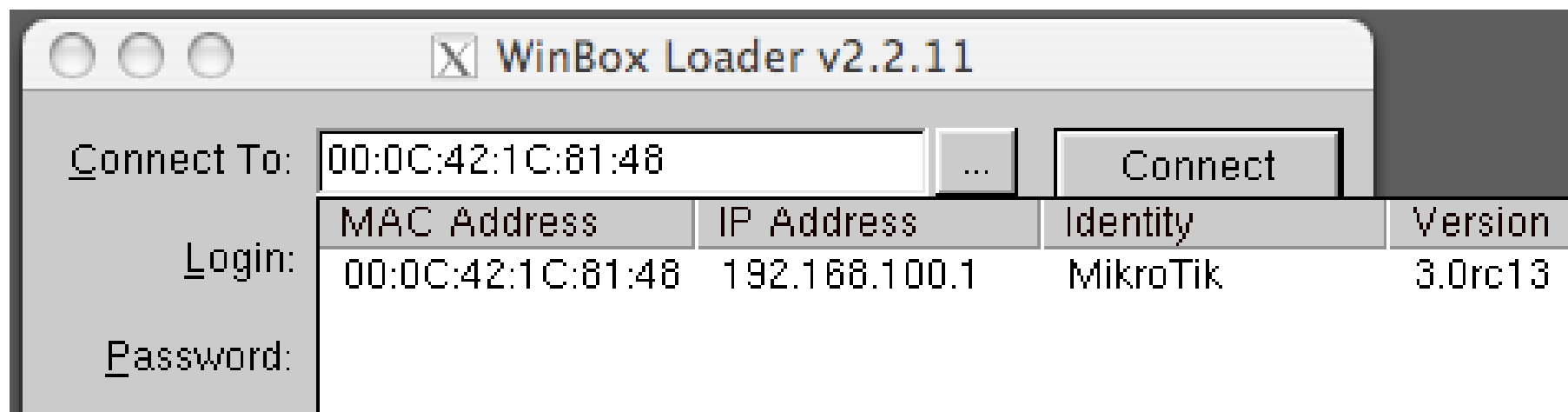
Lab-1 adalah sebuah simulasi konfigurasi dasar sebuah Router Mikrotik yang akan digunakan di jaringan local seperti warnet, office, kampus atau bahkan di RT/RW-NET

X = nomor peserta

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

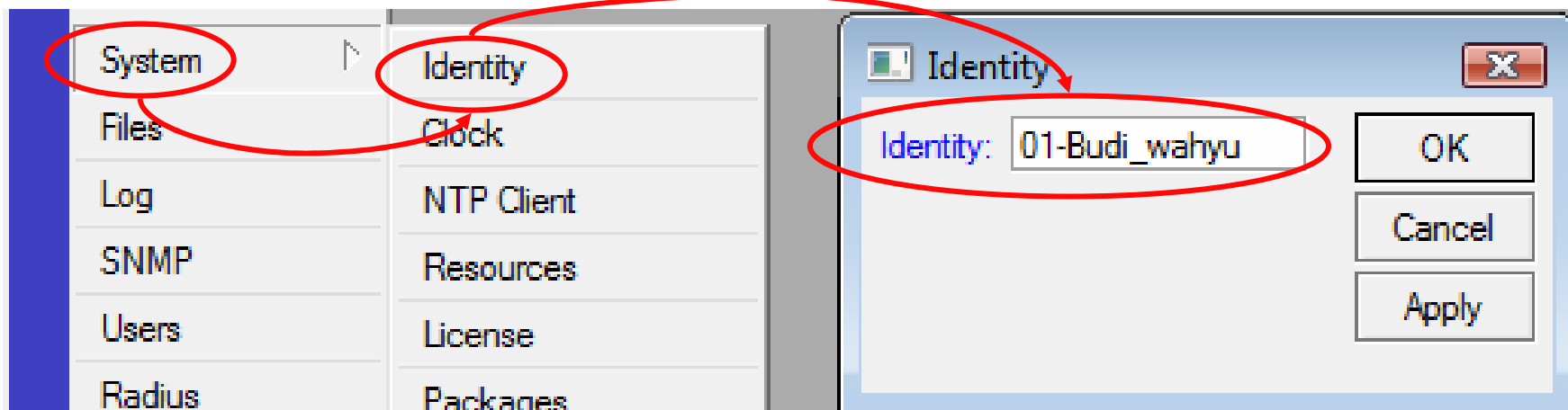
● ● ● | Koneksi pertama ke router

- Hubungkan port ethernet Anda dengan ether1 pada routerboard.
- Pastikan ethernet port Anda memiliki IP statik
- Jalankan program winbox, klik pada [..] untuk melihat router Anda.



● ● ● | Set System Identity

- Supaya tidak membingungkan, ubahlah nama router Anda.
- Format: xx>NamaAnda
- Contoh: 01-Budi-Wahyu
- Aktifkan semua interface



Konfigurasi Wireless

The image shows two screenshots from the Mikrotik WinBox interface. The left screenshot shows the 'Wireless Tables' window with the 'wlan1' interface selected and its status set to 'running'. The right screenshot shows the 'Interface <wlan1>' configuration window with several settings highlighted in red circles: 'Mode: station', 'Band: 2.4GHz-B/G', 'SSID: training', and the 'Default Authenticate' checkbox.

- Aktifkan Interface Wireless pada Ether1

Konfigurasi IP dan Routing

The screenshot displays the Mikrotik WinBox v3.2 interface. On the left, a navigation tree shows 'IP' and 'Routing' selected, with 'Addresses' and 'Routes' sub-items also highlighted. The main area contains two windows: 'Address List' and 'Route List'. The 'Address List' window shows a table with two entries: 10.10.10.1/24 on wlan1 and 192.168.1.1/24 on ether1. The 'Route List' window shows a table with three entries: AS (0.0.0.0/0) on wlan1 with distance 1, and two DAC entries (10.10.10.0/24 and 192.168.1.0/24) on wlan1 and ether1 respectively, both with distance 0.

Address	Network	Broadcast	Interface
10.10.10.1/24	10.10.10.0	10.10.10.255	wlan1
192.168.1.1/24	192.168.1.0	192.168.1.255	ether1

Destination	Gateway	Gateway ...	Interface	Distance	Route
AS 0.0.0.0/0	10.10.10.100		wlan1	1	
DAC 10.10.10.0/24			wlan1	0	
DAC 192.168.1.0/24			ether1	0	

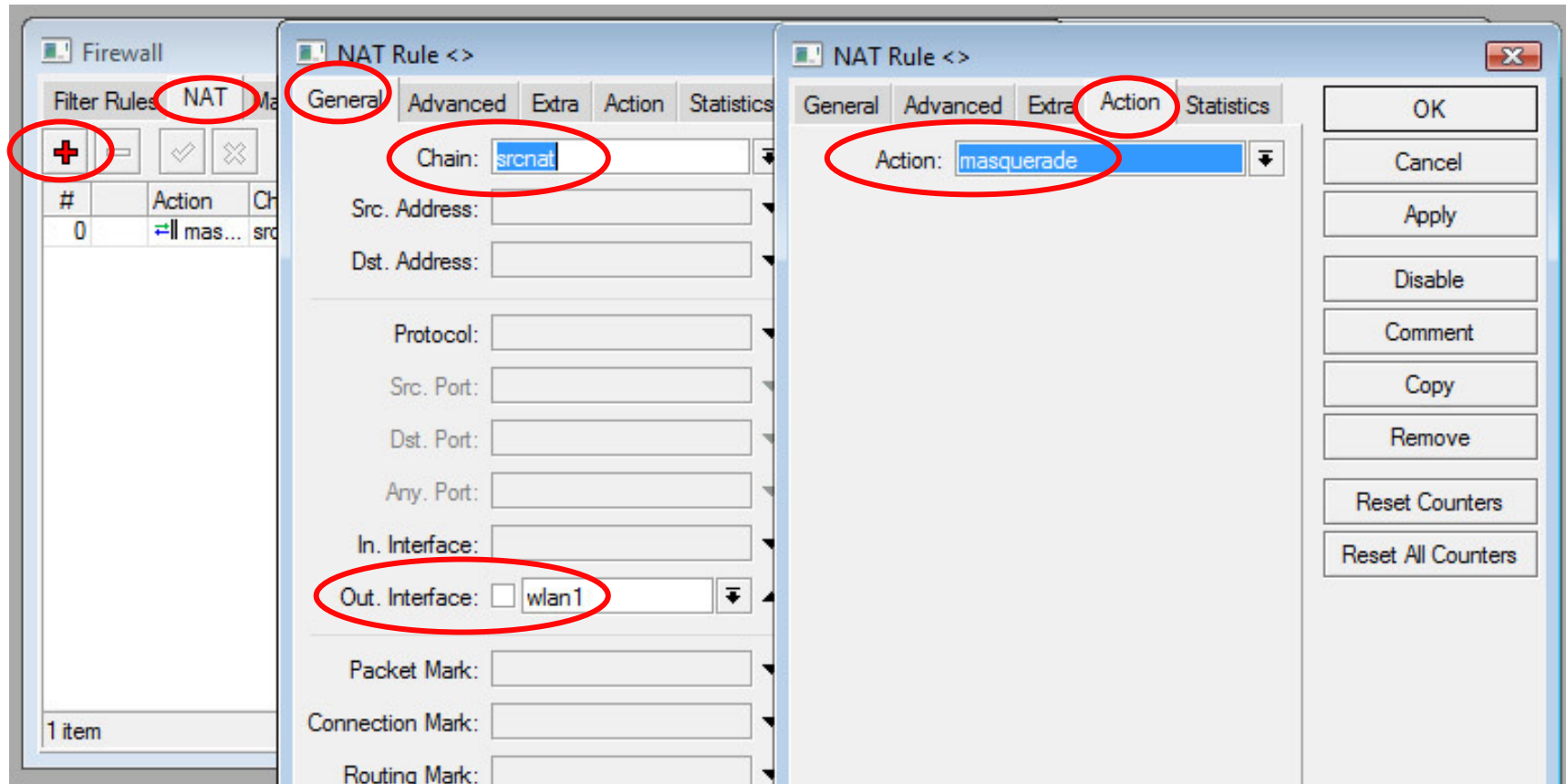
Konfigurasi DNS Server

The screenshot shows the Mikrotik WinBox interface. The left sidebar menu has 'IP' and 'DNS' highlighted with red circles. The main window displays the 'DNS' configuration window, with the 'Settings' tab selected and also highlighted with a red circle. Below it, the 'DNS Settings' dialog box is open, showing the following configuration:

- Primary DNS: 10.100.100.1
- Secondary DNS: 0.0.0.0
- Allow Remote Requests
- Max UDP Packet Size: 512
- Cache Size: 2048 KB
- Cache Used: 5

The 'OK' and 'Apply' buttons are visible in the 'DNS Settings' dialog.

Firewall-Src-NAT



Konfigurasi Console-Terminal LAB-1

- Konfigurasi wireless sebagai media untuk backbone
 - /interface wireless set wlan1 mode=station ssid=training band=2.4.ghz-b/g scan-list=2400-2500 disabled=no
- Konfigurasi IP Address
 - /ip address add address=10.10.10.x/24 interface=wlan1
 - /ip address add address=192.168.x.1/24 interface=ether1
- Konfigurasi Routing – Default Gateway
 - /ip route add gateway=10.10.10.100
- Konfigurasi DNS
 - /ip dns set primary-dns=10.100.100.1 allow-remote-request=yes
- Konfigurasi NAT
 - /ip firewall nat add chain=srcnat out-interface=wlan1 action=masquerade



Cek Hasil Instalasi

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

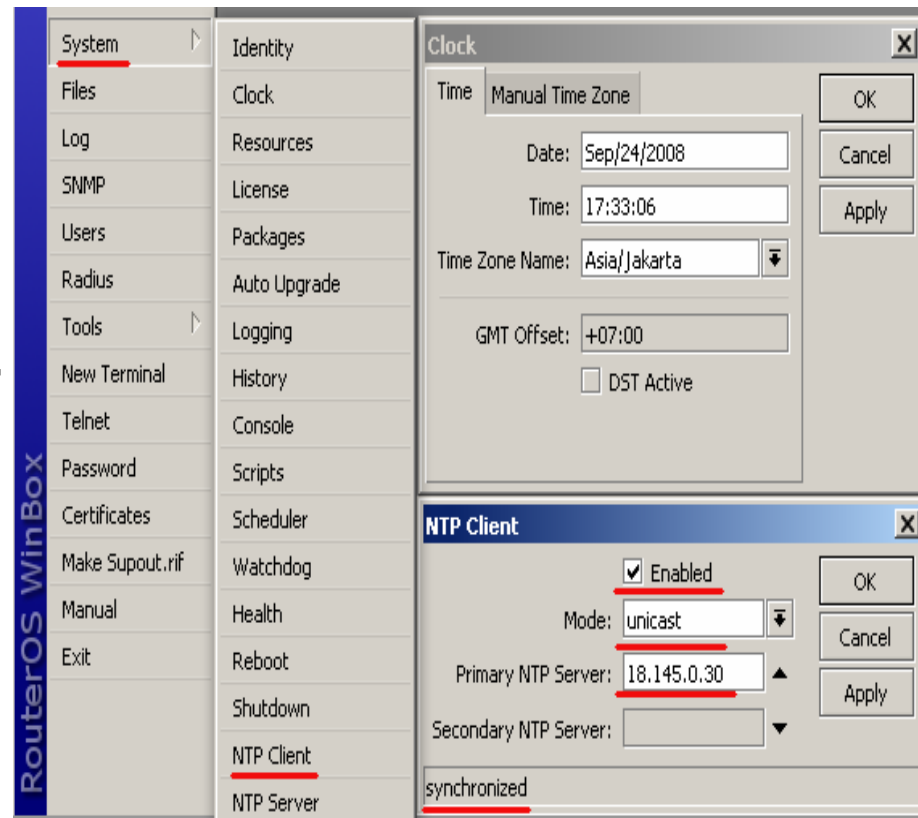


Network Time Protocol (NTP)

- NTP protocol memungkinkan sinkronisasi waktu dalam sebuah jaringan
- Mikrotik support NTP server dan NTP Client
- NTP Server
 - Install paket ntp, karena paket 'system' hanya menyertakan servis ntp client
 - Mode:**broadcast,manycast,multicast**
 - Konfigurasi NTP Server
 - Setting clock → /system clock
 - Set enable → /system ntp server set enabled=yes

Network Time Protocol (NTP)

- NTP Client
- Konfigurasi
 - Set enable
 - Set mode unicast
 - Set IP NTP server
 - Set time zone pada menu /system clock



● ● ● | Network Time Protocol (NTP)

- 4 fase sinkronisasi
 - Started : start service NTP
 - Reached : terkoneksi dengan NTP server
 - Timeset : mengganti waktu/tanggal lokal sesuai waktu NTP server
 - Synchronized : mengganti jam lokal sama dengan jam NTP server
- Latihan: setting NTP server maupun NTP Client bersama rekan semeja

[LAB-2] Membuat File Backup

The screenshot shows the Mikrotik WinBox v3.2 interface. On the left sidebar, the 'Files' menu item is circled in red. The main window displays a 'File List' dialog box. In this dialog, the 'Backup' button is circled in red, and the file 'MikroTik-01012000-0138.backup' is also circled in red. The file list contains the following items:

File Name	Type	Size	Creation Time
MikroTik-01012000-0138.backup	Backup	12.3 KiB	Jan/01/2
hotspot	Directory	0 B	Jan/01/2
hotspot/alogin.html	File	1293 B	Jan/01/2
hotspot/error.html	File	898 B	Jan/01/2
hotspot/errors.txt	File	3615 B	Jan/01/2
hotspot/img	Directory	0 B	Jan/01/2
hotspot/img/logobottom.p...	File	4317 B	Jan/01/2
hotspot/img/user-manage...	File	0 B	Jan/01/2
hotspot/login.html	File	3384 B	Jan/01/2
hotspot/logout.html	File	1813 B	Jan/01/2
hotspot/lv	Directory	0 B	Jan/01/2
hotspot/lv/alogin.html	File	1303 B	Jan/01/2
hotspot/lv/errors.txt	File	3810 B	Jan/01/2
hotspot/lv/login.html	File	3408 B	Jan/01/2
hotspot/lv/logout.html	File	1843 B	Jan/01/2
hotspot/lv/radvert.html	File	1475 B	Jan/01/2
hotspot/lv/status.html	File	2760 B	Jan/01/2
hotspot/md5.js	File	7.0 KiB	Jan/01/2
hotspot/radvert.html	File	1481 B	Jan/01/2
hotspot/redirect.html	File	213 B	Jan/01/2
hotspot/rlogin.html	File	739 B	Jan/01/2
hotspot/status.html	File	3082 B	Jan/01/2

At the bottom of the File List window, it shows '32 items', '33.7 MB of 126.9 M...', and '73% free'.



Backup melalui Console

- Jika ingin menentukan nama file backup, bisa melakukan backup melalui console
- Membuat file backup:

```
[admin@MikroTik] > /system backup save name=backup-1  
Saving system configuration  
Configuration backup saved  
[admin@MikroTik] >
```

- File backup dapat dilihat di submenu /file
- Dapat didownload via FTP

● ● ● | System Reset

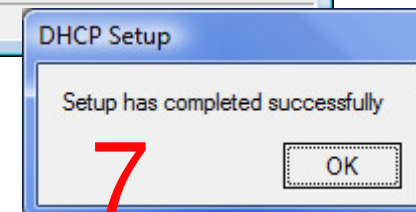
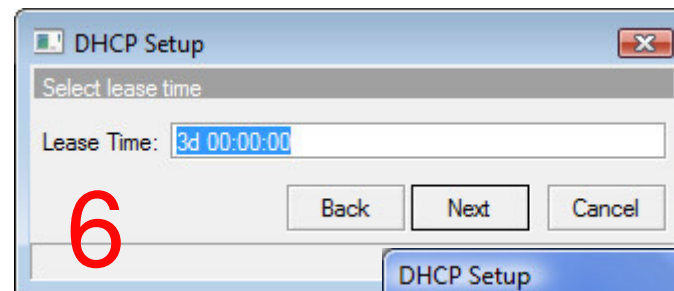
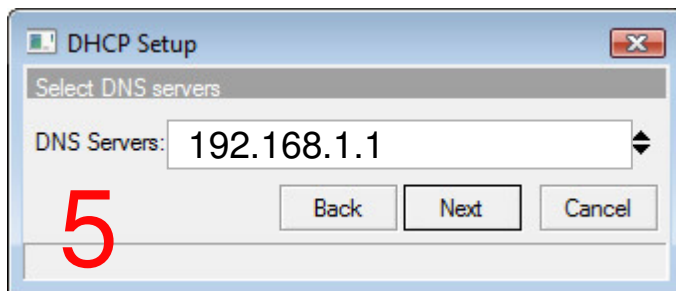
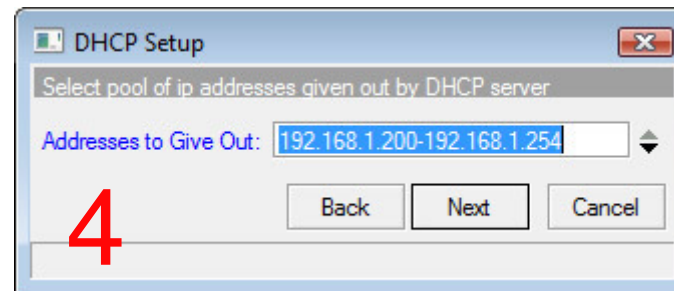
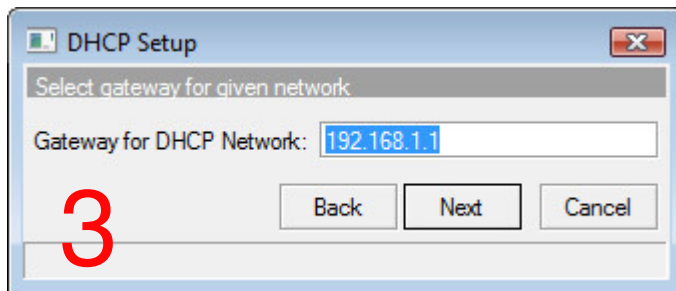
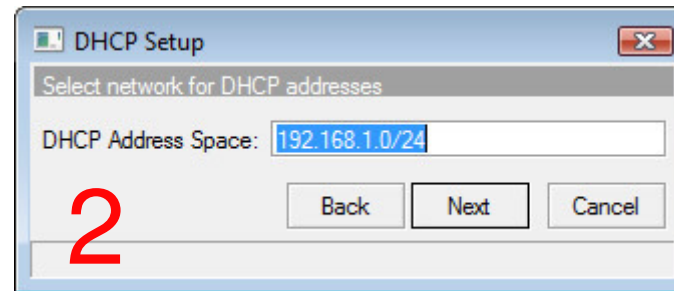
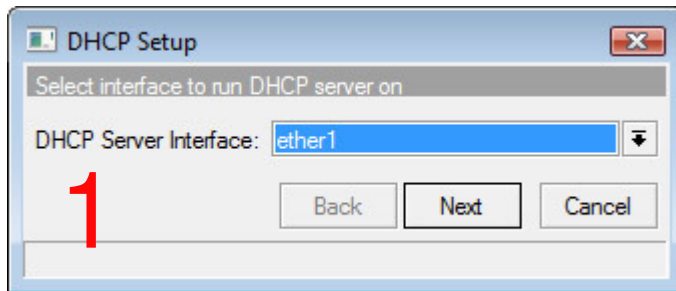
- Untuk mengembalikan ke konfigurasi awal (default).
- Perintah ini menghapus semua konfigurasi yang telah dibuat, termasuk user dan password.
- Hanya bisa dilakukan oleh user dengan hak penuh (grup: full)

```
[admin@Router-MikroTik] > system reset  
Dangerous! Reset anyway? [y/N]: y
```

[LAB-4] DHCP Server (1)

The screenshot displays the Mikrotik WinBox v3.2 interface. On the left sidebar, the 'IP' menu item is circled in red. In the main menu area, 'DHCP Server' is also circled in red. A 'DHCP Server' configuration window is open, with the 'DHCP' tab selected and circled in red. Within this window, the 'DHCP Setup' button is circled in red. A smaller 'DHCP Setup' dialog box is overlaid on top, showing a dropdown menu for 'DHCP Server Interface' with 'ether1' selected. The dialog box includes 'Back', 'Next', and 'Cancel' buttons. The main window shows a table with columns for Name, I. Relay, Lease Time, and Address Pool, currently displaying 0 items.

[LAB-4] DHCP Server (2)





Konfigurasi Console-Terminal LAB-4

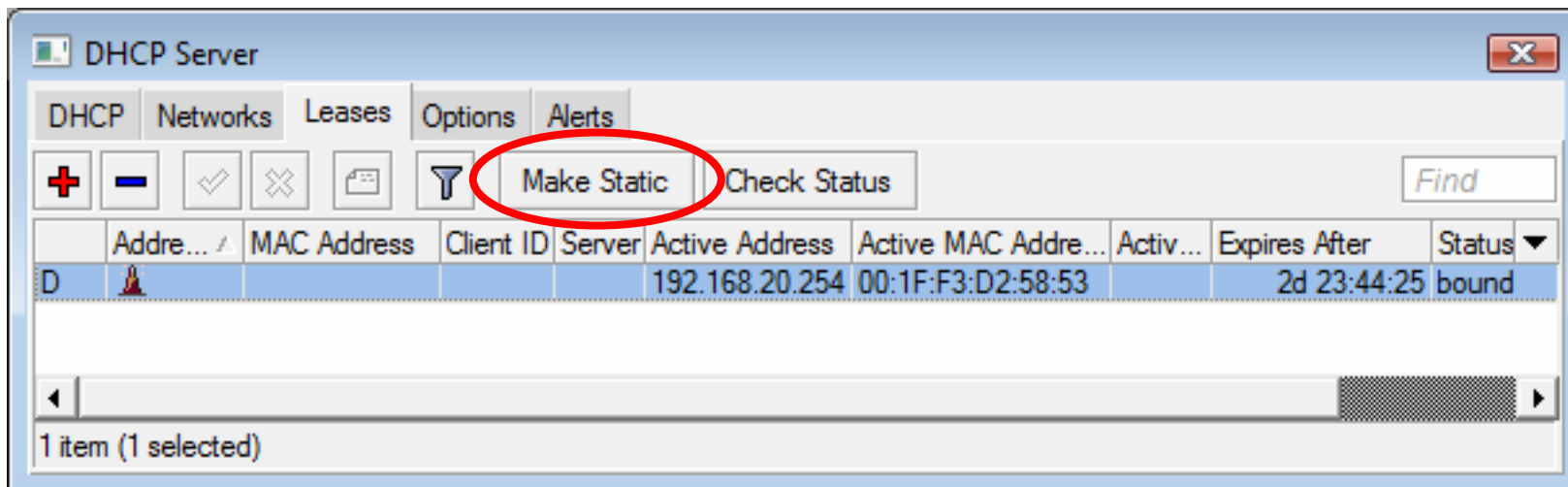
- Konfigurasi DHCP-Server setup
 - /ip dhcp-server setup
 - dhcp server interface: ether1
 - dhcp address space: 192.168.x.0/24
 - gateway for dhcp network: 192.168.x.1
 - dhcp relay: 192.168.x.1
 - addresses to give out: 192.168.x.10-192.168.x.20
 - dns servers: 192.168.x.1
 - lease time: 3d

● ● ● | Cek Setting DHCP

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

● ● ● | Pengelolaan DHCP Client

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



Konfigurasi DHCP Statik

The screenshot shows the Mikrotik DHCP Lease configuration window for a static lease. The window title is "DHCP Lease <192.168.20.254, 192.168.20.254>". The "General" tab is selected, and the lease is currently "Active".

Configuration fields include:

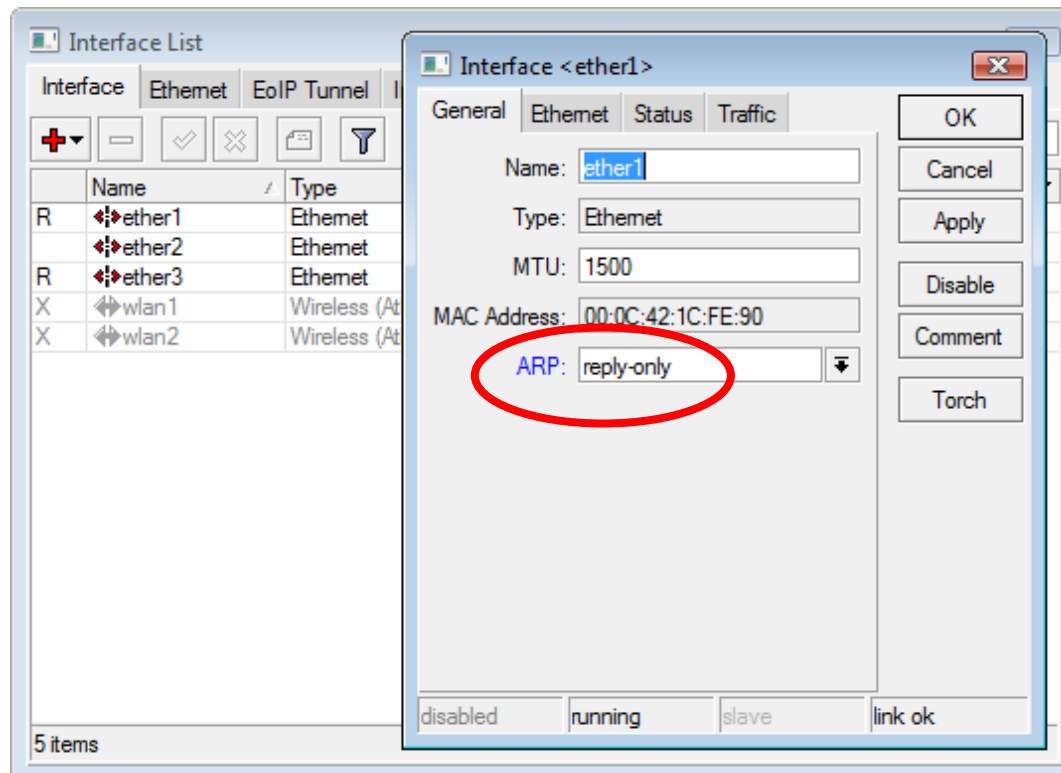
- Address: 192.168.20.254
- MAC Address: 00:1F:F3:D2:58:53
- Use Src. MAC Address
- Client ID: 1:0:1ff3:d2:58:53
- Server: dhcp1
- Lease Time: (empty)
- Block Access
- Always Broadcast
- Rate Limit: (empty)

Buttons on the right side of the window include: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Make Static, and Check Status.

At the bottom of the window, there are four status indicators: disabled, radius, blocked, and bound.

Keamanan DHCP

- ARP=reply-only
Client yang bisa terkoneksi hanyalah yang mendapatkan IP Address melalui proses DHCP, bukan pengisian manual



● ● ● | LAB – Konfigurasi DHCP Client

- Dalam beberapa kondisi tertentu, IP Address pada router bukanlah IP Address statik, melainkan IP Address dinamis yang di dapat melalui DHCP.
- Dalam hal ini, kita menggunakan fitur DHCP-Client

Konfigurasi DHCP Client

The image shows the Mikrotik WinBox interface with several elements highlighted by red circles and arrows:

- The **IP** menu item in the left sidebar is circled in red.
- The **DHCP Client** menu item in the left sidebar is circled in red.
- The **+** (Add) button in the DHCP Client window is circled in red, with an arrow pointing to it from the IP menu.
- The **Interface: wlan1** dropdown menu in the New DHCP Client dialog is circled in red.
- The checkboxes for **Add Default Route**, **Use Peer DNS**, and **Use Peer NTP** in the New DHCP Client dialog are circled in red.

● ● ● | Parameter DHCP Client (1)

- **Interface**

- Pilihlah interface yang sesuai yang terkoneksi ke DHCP Server

- **Host name** (*tidak harus diisi*)

- Nama DHCP client yang akan dikenali oleh DHCP Server

- **Client ID** (*tidak harus diisi*)

- Biasanya merupakan mac-address interface yang kita gunakan, apabila proses DHCP di server menggunakan sistem radius



Parameter DHCP Client (2)

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

Konfigurasi DHCP Client

admin@00:0C:42:1C:FE:96 (MikroTik) - WinBox v3.14 on RB333 (powerpc)

Hide Passwords

Address List

Address	Network	Broadcast	Interface
20.20.20.254/24	20.20.20.0	20.20.20.255	ether2
30.30.30.22/24	30.30.30.0	30.30.30.255	ether3

Route List

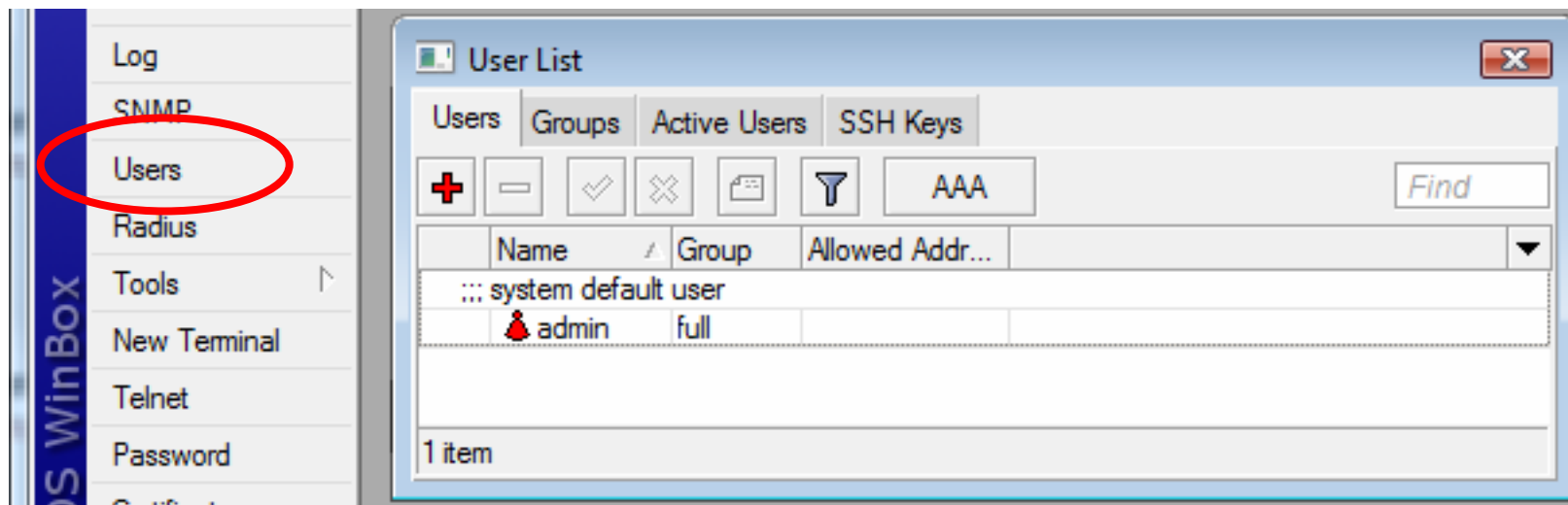
Routes Rules

Destination	Gateway	Gateway ...	Interface	Distance	Routing Mark	Pref. Source
DAS 0.0.0.0/0	20.20.20.1		ether2	5		
DS 8.8.8.8/8	30.30.30.1			10		
DAC 20.20.20.0/24			ether2	0		20.20.20.254
DAC 30.30.30.0/24			ether3	0		30.30.30.22

4 items

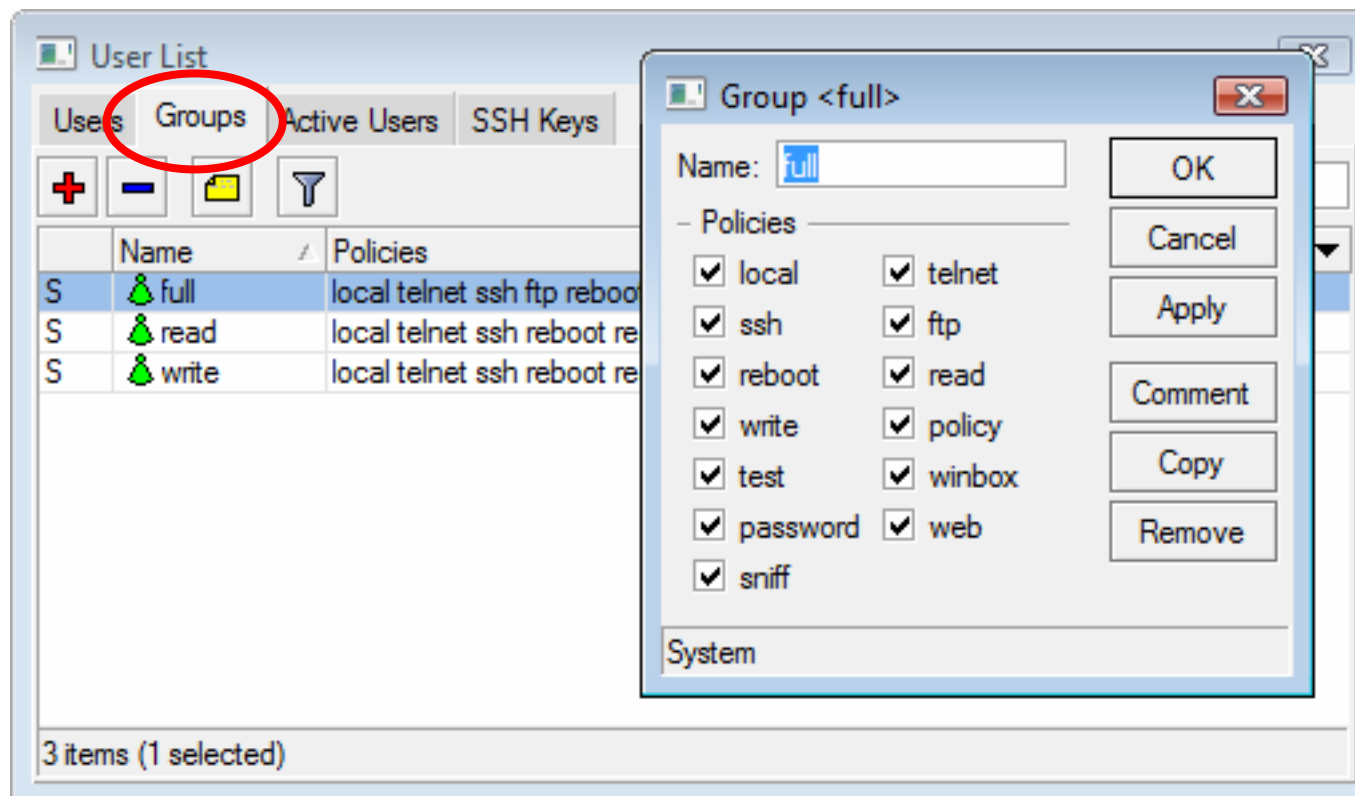
● ● ● | Internal User RouterOS

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



Internal User Groups

- User dapat dikategorikan hak nya berdasarkan grupnya.
- Kita bisa menambahkan user baru dengan hak tertentu.



● ● ● | Tips mengenai User

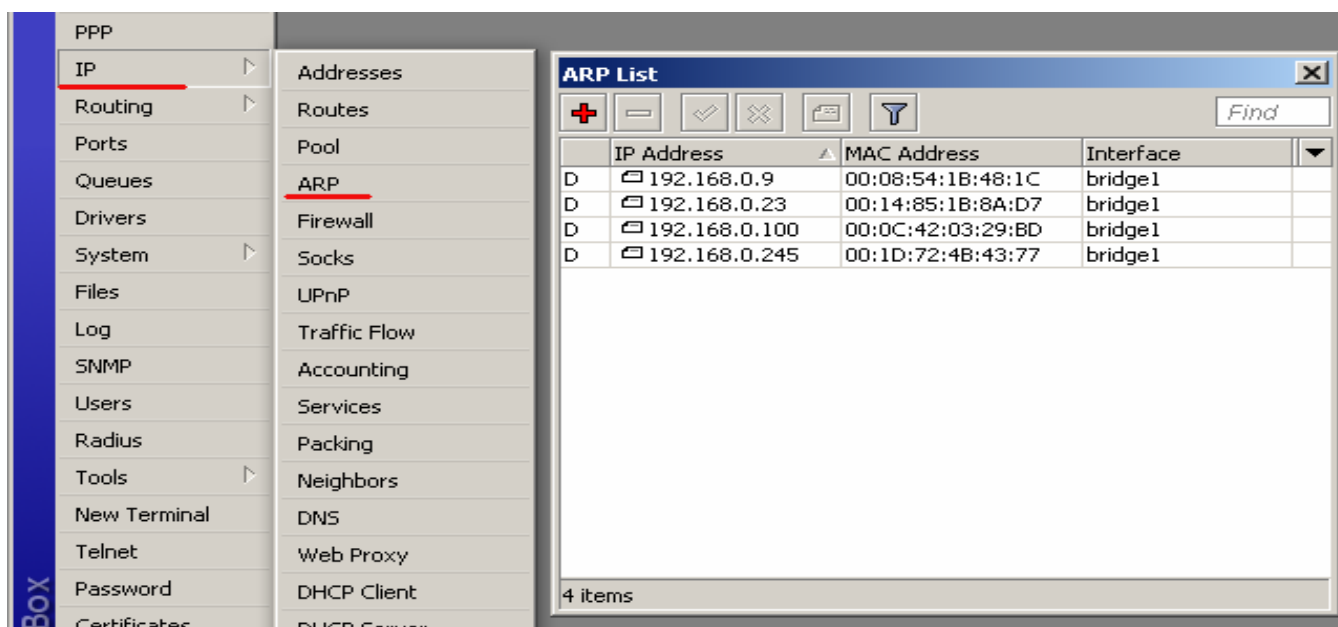
- Buatlah user baru yang memiliki hak penuh dan non aktifkan user “**admin**”
- Untuk teknisi bisa diberikan grup **write** (bukan **full**) sehingga kita masih memiliki hak penuh terhadap router kita
- Untuk pemantauan, bisa menggunakan user dengan grup **read**

● ● ● | LAB Internal User

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

● ● ● | Address Resolution Protocol

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



The screenshot shows the Mikrotik WinBox interface. On the left, the 'IP' menu is expanded, and 'ARP' is selected. The main window displays the 'ARP List' window, which contains a table with the following data:

	IP Address	MAC Address	Interface
D	192.168.0.9	00:08:54:1B:48:1C	bridge1
D	192.168.0.23	00:14:85:1B:8A:D7	bridge1
D	192.168.0.100	00:0C:42:03:29:BD	bridge1
D	192.168.0.245	00:1D:72:4B:43:77	bridge1

4 items

● ● ● | Monitoring

○ Tool monitoring

● Ping

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

```
[user1@MKI] > ping 192.168.0.100
```

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

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

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

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

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

Monitoring

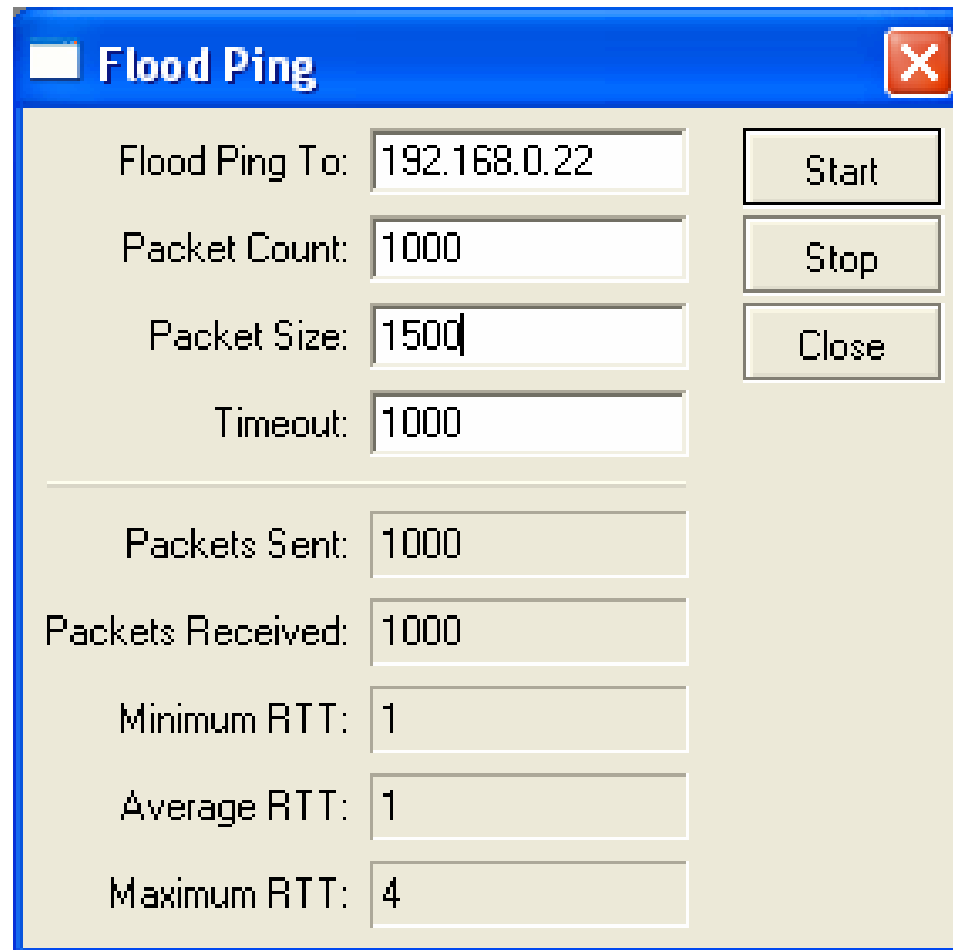
- Mac Ping

The screenshot shows the 'MAC Ping' utility window. It has a blue title bar with the text 'MAC Ping' and a close button. The main area is light gray and contains several input fields and buttons. The 'Ping To:' field is a dropdown menu with '00:0C:42:02:1D:CF' selected. Below it is a list of MAC addresses: '00:0C:76:E3:E5:FD', '00:0C:42:02:1D:CF' (highlighted), '00:0C:42:02:34:77', and '00:0C:42:02:29:40'. The 'Packet Count:' field is empty. The 'Timeout:' field is empty. The 'Packet Size:' field contains '50'. To the right of these fields are three buttons: 'Ping', 'Stop', and 'Close'. Below the input fields is a table with the following data:

MAC Address	Time	Reply Size	Sta
00:0C:42:02:1D:CF	0 ms	50	
00:0C:42:02:1D:CF	0 ms	50	
00:0C:42:02:1D:CF	0 ms	50	
00:0C:42:02:1D:CF	1 ms	50	

Monitoring

- Flood Ping



The screenshot shows a window titled "Flood Ping" with a close button (X) in the top right corner. The window contains several input fields and buttons. The configuration fields are: "Flood Ping To:" with the value "192.168.0.22", "Packet Count:" with "1000", "Packet Size:" with "1500", and "Timeout:" with "1000". To the right of these fields are three buttons: "Start", "Stop", and "Close". Below a horizontal line, the results fields are: "Packets Sent:" with "1000", "Packets Received:" with "1000", "Minimum RTT:" with "1", "Average RTT:" with "1", and "Maximum RTT:" with "4".

Field	Value
Flood Ping To:	192.168.0.22
Packet Count:	1000
Packet Size:	1500
Timeout:	1000
Packets Sent:	1000
Packets Received:	1000
Minimum RTT:	1
Average RTT:	1
Maximum RTT:	4



Monitoring

- Torch

Realtime Traffic Monitor called also torch is used for monitoring traffic that is going through an interface.

Torch (running)

Basic: Interface: ether1, Entry Timeout: 00:00:03 s

Filters: Src. Address: 0.0.0.0/0, Dst. Address: 0.0.0.0/0, Protocol: any, Port: any, VLAN Id: any

Collect: Src. Address, Dst. Address, VLAN Id, Protocol, Port

Src. Address	Dst. Address	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
255.255.255.255	192.168.0.23	4.8 kbps	0 bps	7	0
202.65.113.146	192.168.0.173	13.7 kbps	1472 bps	12	4
152.118.24.30	192.168.0.22	672 bps	0 bps	1	0
209.85.171.93	192.168.0.22	3.1 kbps	193.9 k...	9	16
192.168.0.100	192.168.0.22	1344 bps	2.1 kbps	2	1
192.168.0.98	192.168.0.23	0 bps	0 bps	0	0

6 items | Total Tx: 23.7 ... | Total Rx: 197... | Total Tx Packet: 31 | Total Rx Packet: 21

Monitoring

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

The screenshot shows the Traceroute utility window with the following configuration and results:

Traceroute To: Traceroute

Packet Size: Stop

Timeout: s Close

Protocol: ▾

Port:

Src. Address: ▾

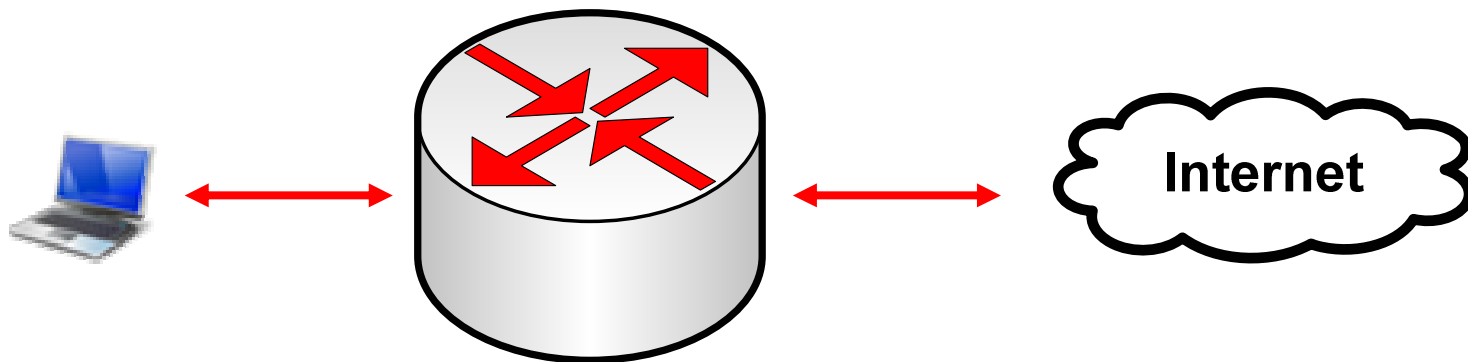
DSCP: ▾

#	Host	Time 1	Time 2	Time 3	▾
0	192.168.0.100	2ms	2ms	1ms	
1	202.65.113.1	2ms	1ms	2ms	
2	10.10.89.5	2ms	2ms	2ms	
3	202.65.113.16	2ms	2ms	2ms	

done

● ● ● | Proxy

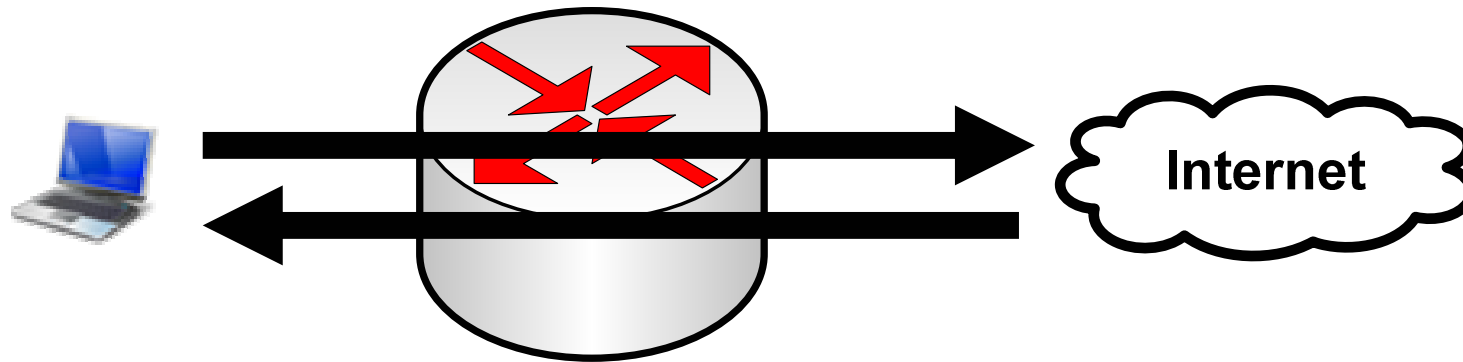
- Pada semua level routers, baik yang diinstall pada PC maupun yang diinstall pada routerboard, kita bisa mengaktifkan fitur proxy



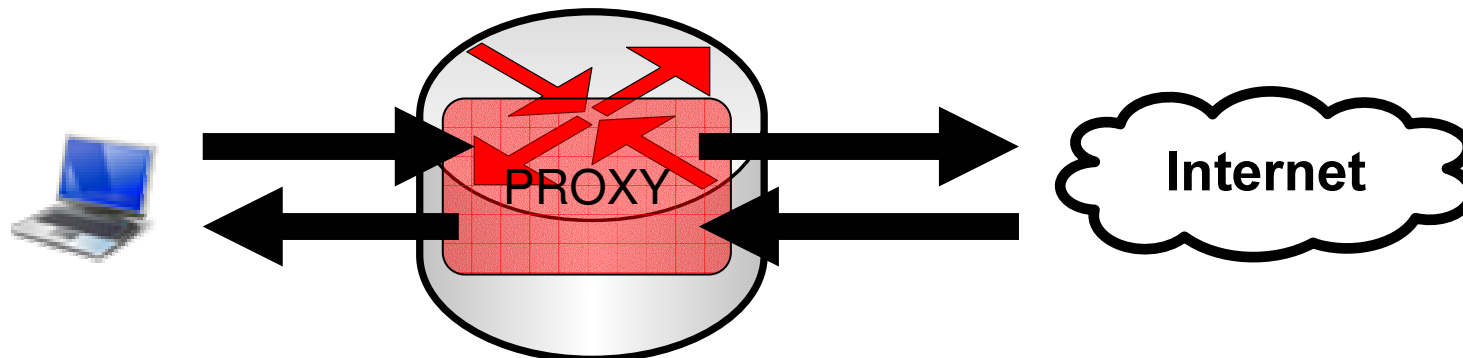


Konsep Proxy

- o Koneksi tanpa proxy



- o Koneksi dengan proxy



● ● ● | Konsep Proxy

- Untuk mempercepat proses browsing, kita menggunakan proxy untuk menyimpan sebagian data website.
- Data yang sudah ada, akan langsung diberikan ke user (HIT).
- Jika belum ada, akan dimintakan dari internet, baru kemudian diberikan ke user (MISS).

● ● ● | Kebutuhan Proxy

- Jika ingin menjalankan cache (penyimpanan data proxy), dibutuhkan storage untuk penyimpanan.
 - PC Router :
 - 1 harddisk (system + cache)
 - 1 DOM (system) + 1 harddisk (cache)
 - Routerboard (RB500, RB600, RB433AH, RB1000)
 - Internal storage/NAND (system) + kartu memori tambahan (CF/Micro-SD) untuk cache

● ● ● | Fitur Proxy di RouterOS

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

● ● ● | Setup Proxy

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

Mengaktifkan Proxy

The screenshot displays the Mikrotik WinBox interface for configuring the Web Proxy. The main window is titled "Web Proxy" and has tabs for "Access", "Cache", "Direct", and "Connections". The "Cache" tab is selected. Below the tabs are several icons and buttons, including "Reset Counters" and "Reset All Counters". A "Web Proxy Settings" button is also visible. The "Web Proxy Settings" dialog box is open, showing the "General" tab. The "Enabled" checkbox is checked. The "Src. Address" field is empty, and the "Port" is set to 3128. The "Parent Proxy" and "Parent Proxy Port" fields are also empty. The "Cache Drive" is set to "system", and the "Cache Administrator" is "webmaster". The "Max. Cache Size" is set to "none" KB, and the "Cache On Disk" checkbox is unchecked. The "Max. Client Connections" and "Max. Server Connections" are both set to 600. The "Max Fresh Time" is set to 3d 00:00:00. The "Serialize Connections" and "Always From Cache" checkboxes are unchecked. The "Cache Hit DSCP (TOS)" is set to 4. The status bar at the bottom of the dialog shows "running".



Redirect TCP-80

The image shows two overlapping windows from Mikrotik WinBox. The background window is titled "NAT Rule <80>" and has tabs for "General", "Advanced", "Extra", "Action", and "Statistics". The "General" tab is active, showing the following configuration:

- Chain: dstnat
- Src. Address: (empty)
- Dst. Address: (empty)
- Protocol: 6 (tcp)
- Src. Port: (empty)
- Dst. Port: 80
- Any. Port: (empty)
- In. Interface: ether1
- Out. Interface: (empty)
- Packet Mark: (empty)
- Connection Mark: (empty)
- Routing Mark: (empty)
- Connection Type: (empty)

The status bar at the bottom of this window says "disabled".

The foreground window is titled "New NAT Rule" and also has tabs for "General", "Advanced", "Extra", "Action", and "Statistics". The "General" tab is active, showing:

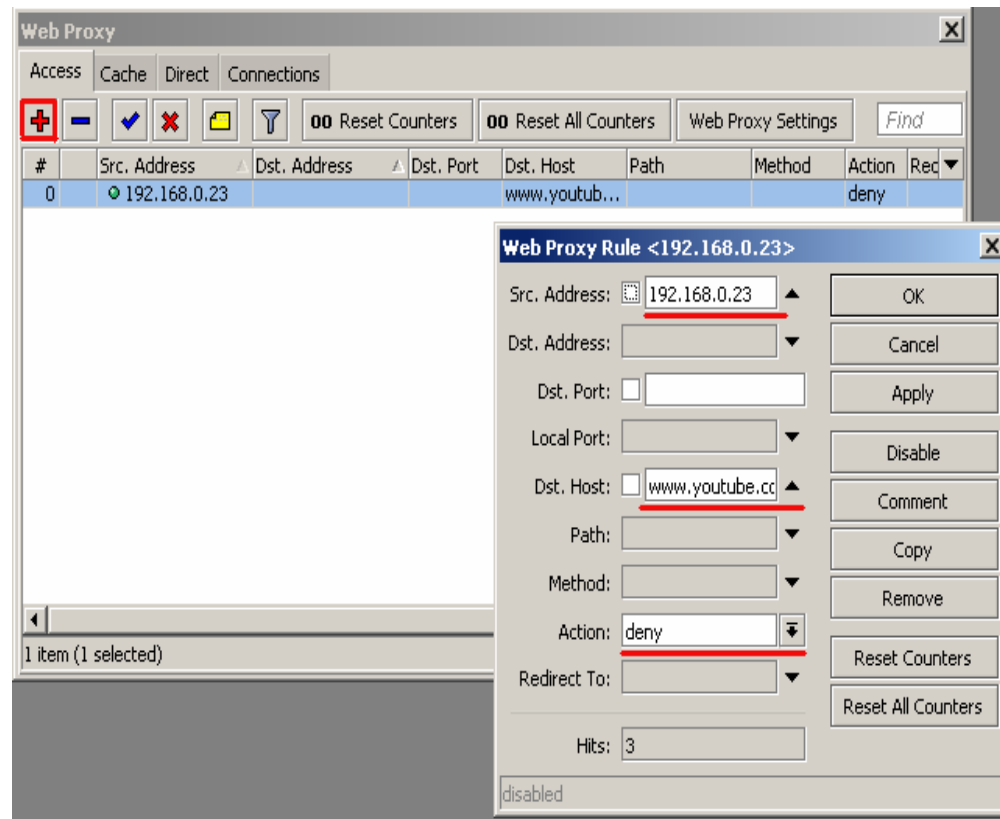
- Action: redirect
- To Ports: 3128

The status bar at the bottom of this window also says "disabled".

On the right side of the "New NAT Rule" window, there is a vertical stack of buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

Akses

- o Mengatur hak akses client



Cache

- Pengaturan penyimpanan objek ke dalam cache

The screenshot displays the Mikrotik WinBox interface for configuring the Web Proxy. The main window shows a table with the following data:

#	Src. Address	Dst. Address	Dst. Port	Dst. Host	Path	Method	Action	Hits
0	192.168.0.23			www.google...			allow	1

The 'Web Proxy Rule <192.168.0.23>' dialog box is open, showing the following configuration:

- Src. Address: 192.168.0.23
- Dst. Address: (empty)
- Dst. Port: (empty)
- Local Port: (empty)
- Dst. Host: www.google.co.i
- Path: (empty)
- Method: (empty)
- Action: allow
- Hits: 1

The terminal window at the bottom shows the following command and output:

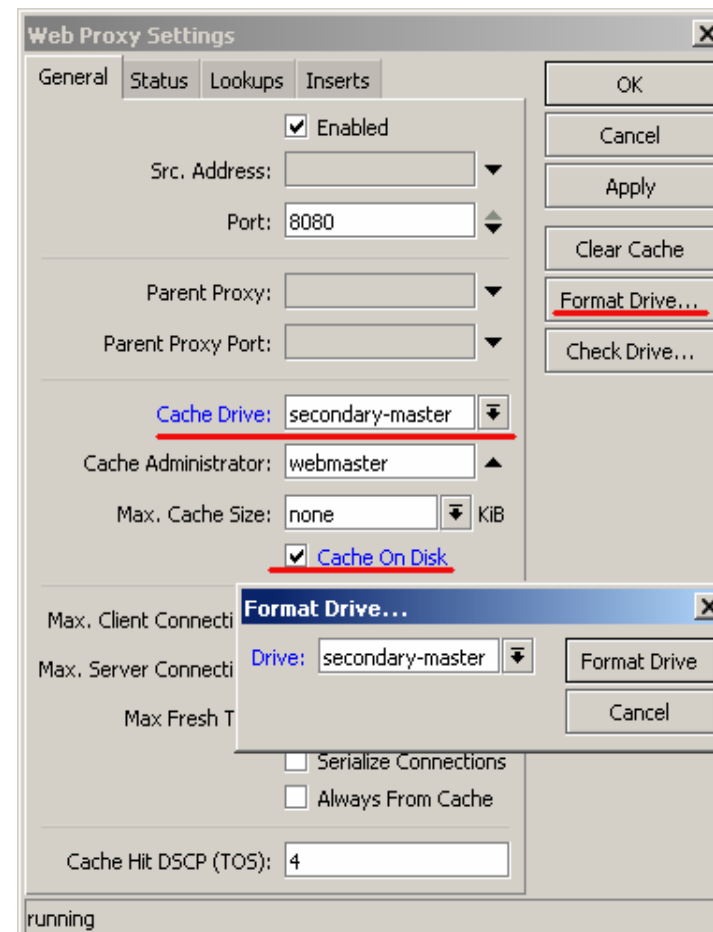
```
[admin@MKI] > ip proxy cache pr
Flags: X - disabled
#  DST-PORT  DST PAT METHOD  ACT.. HITS
0   www       allow 1
[admin@MKI] >
```

● ● ● | Direct Access list

- Mengatur request dari client untuk diproses langsung oleh parent proxy server
- Berfungsi jika Transparent proxy telah didefinisikan

Storage

- Penyimpanan Cache
 - System
 - Harddisk
- Format Drive terlebih dahulu
- Aktifkan Cache on Disk





Basic TCP/IP

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

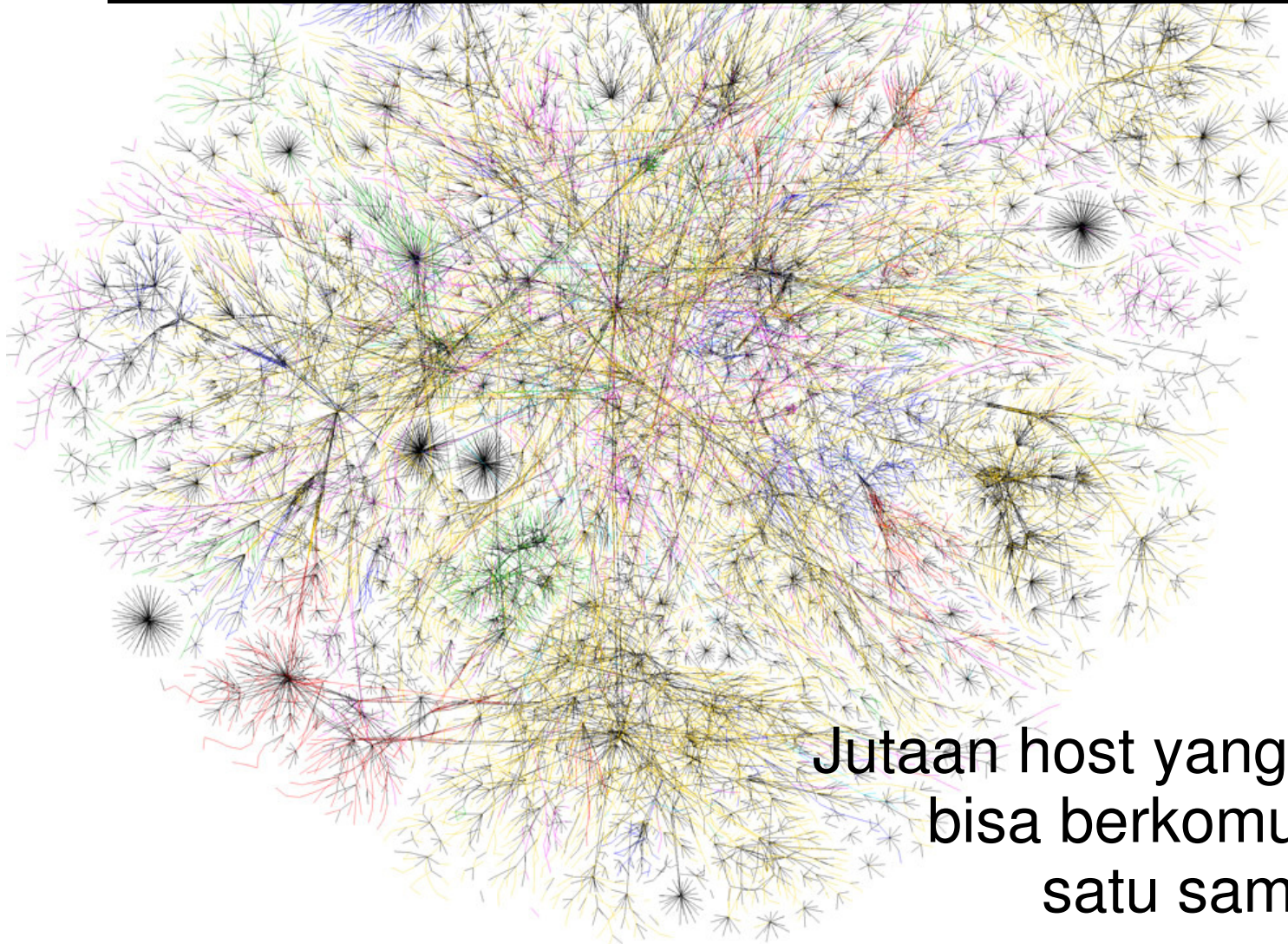
(Mikrotik Certified Training Partner)



Training Outline

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

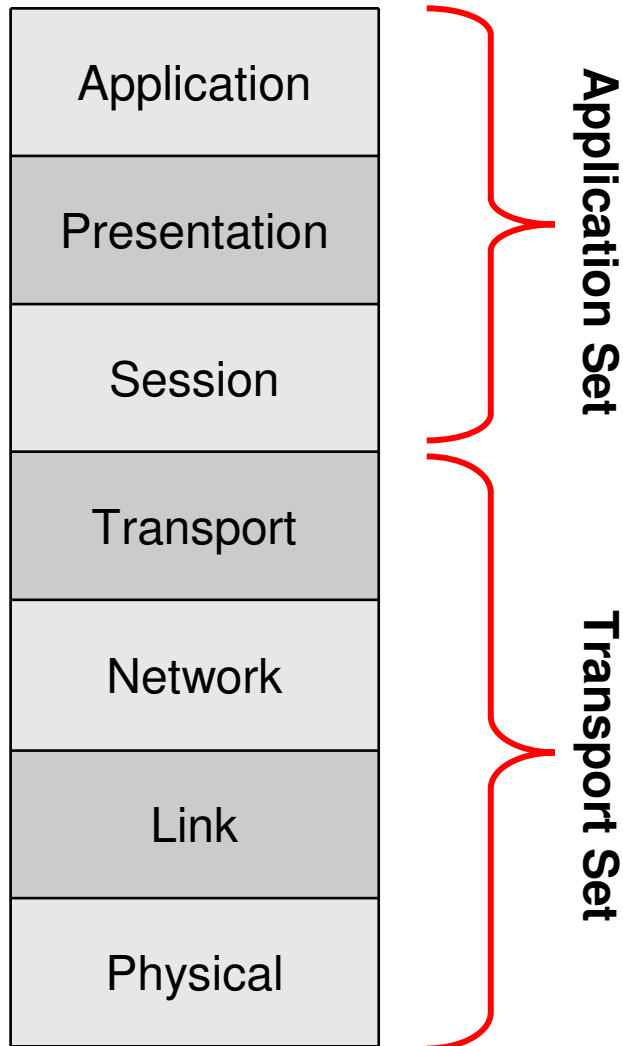
Internet Topology



Jutaan host yang harus
bisa berkomunikasi
satu sama lain.



OSI Layer dan Protokol

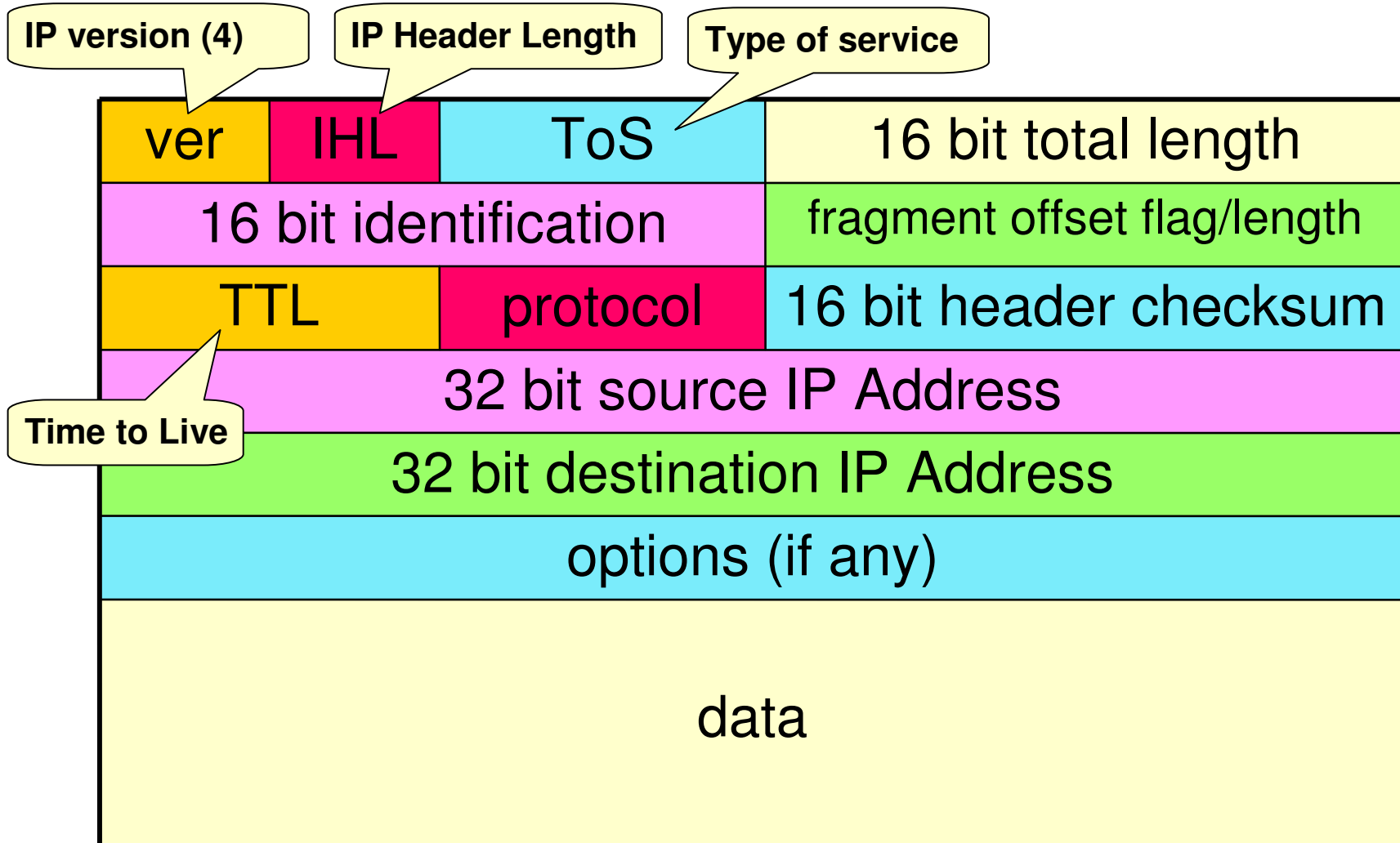


Open Systems Interconnection (OSI) adalah sebuah model referensi arsitektur antarmuka jaringan yang dikembangkan oleh ISO yang kemudian menjadi konsep standard komunikasi jaringan di hampir semua perangkat jaringan.

OSI Layer dan Protokol

Application	SMTP	HTTP	FTP	Telnet	DNS	DHCP	SNMP	TFTP
Presentation	Enkripsi, dekripsi, mime							
Session								
Transport	TCP Transmission Control Protocol				UDP User Datagram Protocol			
Network	IP						Routing Protocols RIP, OSPF, BGP	
	ICMP							
Link	Mac Address, Switch							ARP
Physical	Ethernet, Wireless, ATM, Frame Relay, PPP							

Packet Header

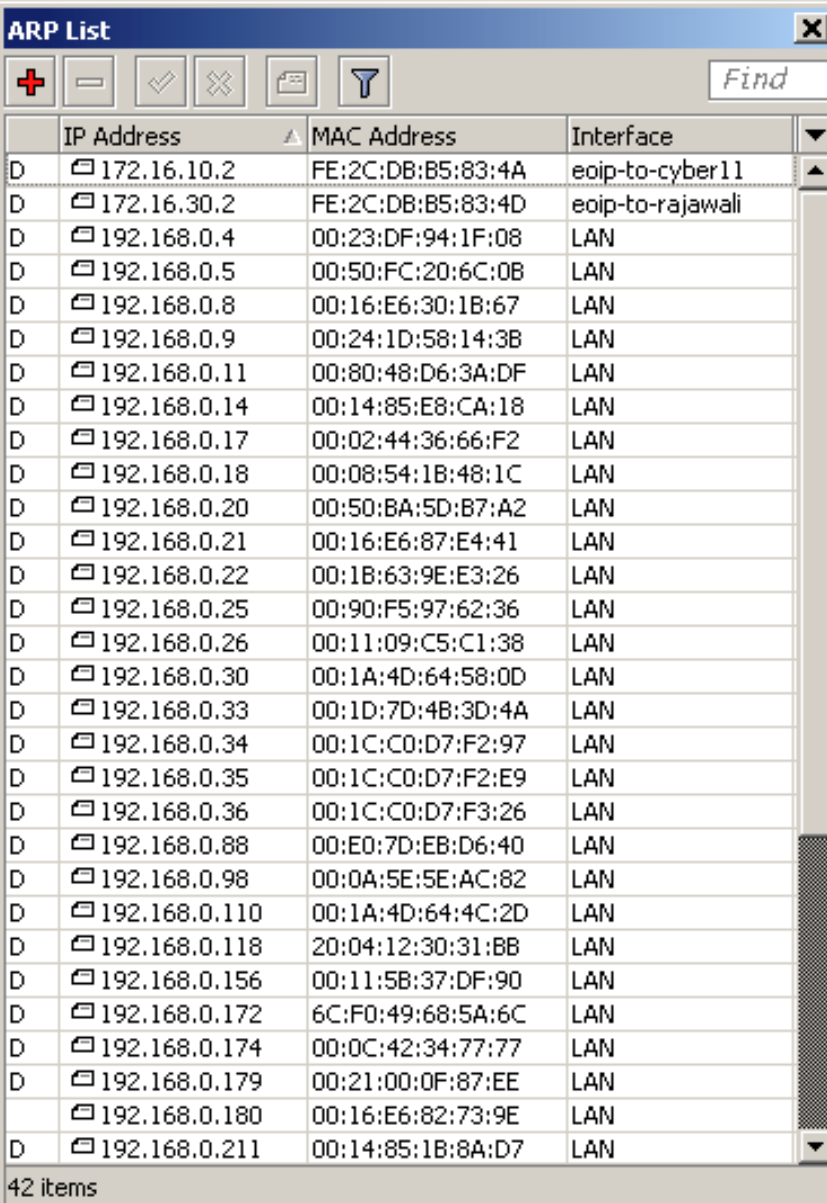


● ● ● | MAC Address

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

ARP Table

- Address Resolution Protocol
- Merupakan protokol penghubung antara layer **data-link** dan **network**.
- ARP Table di router merupakan daftar **host yang terhubung langsung** berisi informasi pasangan **mac address** dan **ip address**



The screenshot shows the 'ARP List' window in Mikrotik WinBox. It displays a table with the following columns: IP Address, MAC Address, and Interface. The table contains 42 entries, each with a status 'D' in the first column. The IP addresses range from 172.16.10.2 to 192.168.0.211. The MAC addresses are in hexadecimal format, and the interfaces are either 'eoip-to-cyber11' or 'LAN'. A search bar labeled 'Find' is located at the top right of the window.

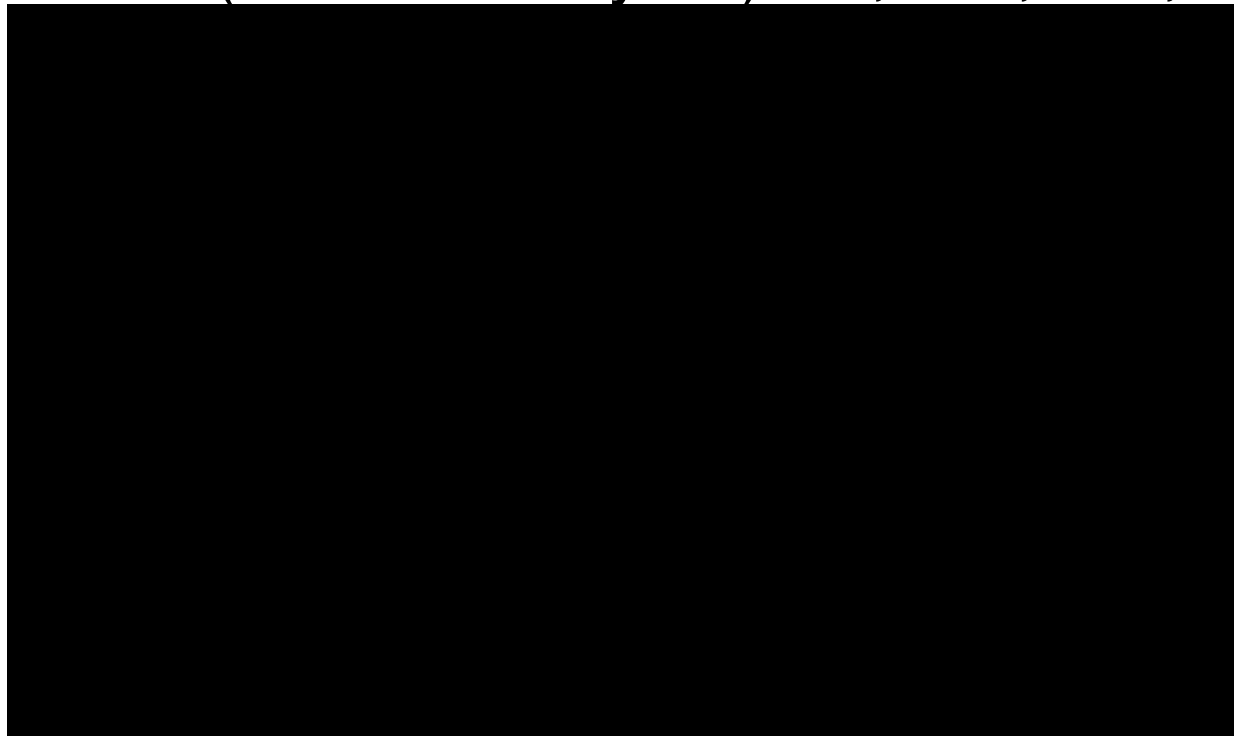
	IP Address	MAC Address	Interface
D	172.16.10.2	FE:2C:DB:B5:83:4A	eoip-to-cyber11
D	172.16.30.2	FE:2C:DB:B5:83:4D	eoip-to-rajawali
D	192.168.0.4	00:23:DF:94:1F:08	LAN
D	192.168.0.5	00:50:FC:20:6C:0B	LAN
D	192.168.0.8	00:16:E6:30:1B:67	LAN
D	192.168.0.9	00:24:1D:58:14:3B	LAN
D	192.168.0.11	00:80:48:D6:3A:DF	LAN
D	192.168.0.14	00:14:85:E8:CA:18	LAN
D	192.168.0.17	00:02:44:36:66:F2	LAN
D	192.168.0.18	00:08:54:1B:48:1C	LAN
D	192.168.0.20	00:50:BA:5D:B7:A2	LAN
D	192.168.0.21	00:16:E6:87:E4:41	LAN
D	192.168.0.22	00:1B:63:9E:E3:26	LAN
D	192.168.0.25	00:90:F5:97:62:36	LAN
D	192.168.0.26	00:11:09:C5:C1:38	LAN
D	192.168.0.30	00:1A:4D:64:58:0D	LAN
D	192.168.0.33	00:1D:7D:4B:3D:4A	LAN
D	192.168.0.34	00:1C:C0:D7:F2:97	LAN
D	192.168.0.35	00:1C:C0:D7:F2:E9	LAN
D	192.168.0.36	00:1C:C0:D7:F3:26	LAN
D	192.168.0.88	00:E0:7D:EB:D6:40	LAN
D	192.168.0.98	00:0A:5E:5E:AC:82	LAN
D	192.168.0.110	00:1A:4D:64:4C:2D	LAN
D	192.168.0.118	20:04:12:30:31:BB	LAN
D	192.168.0.156	00:11:5B:37:DF:90	LAN
D	192.168.0.172	6C:F0:49:68:5A:6C	LAN
D	192.168.0.174	00:0C:42:34:77:77	LAN
D	192.168.0.179	00:21:00:0F:87:EE	LAN
D	192.168.0.180	00:16:E6:82:73:9E	LAN
D	192.168.0.211	00:14:85:1B:8A:D7	LAN

42 items



IP Address

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



● ● ● | Pengelompokan IP Address

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

● ● ● | IP Subneting (contoh 1)

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

● ● ● | IP Subneting (contoh 2)

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



Tabel Subnet

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



Public and Private IP Address

○ **Public IP Address**

IP Address yang dapat diakses di jaringan internet.
Kita bisa mendapatkan Public IP Address dari:

- Dipinjami dari ISP
- Alokasi dari APNIC/IDNIC (www.idnic.net)

○ **Private IP Address**

IP Address yang diperuntukkan untuk jaringan lokal (tidak dapat diakses di jaringan internet)

- 10.0.0.0 – 10.255.255.255 (10./8)
- 172.16.0.0 – 172.31.255.255 (172.16./12)
- 192.168.0.0 – 192.168.255.255 (192.168./16)



IP Address Khusus Lainnya

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

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

- ● ● | IP Address v6

- Sistem IP Address yang baru, penyempurnaan dari IPv4 yang akan habis (diperkirakan tahun 2012)
- Menggunakan 128bit, ada $3,4 \times 10^{38}$ hosts

● ● ● | IP Protocol

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



ICMP (Internet Control Message Protocol)

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

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

● ● ● | UDP (User Datagram Protocol)

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

● ● ● | TCP (Transmission Control Protocol)

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



Prinsip Kerja TCP

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

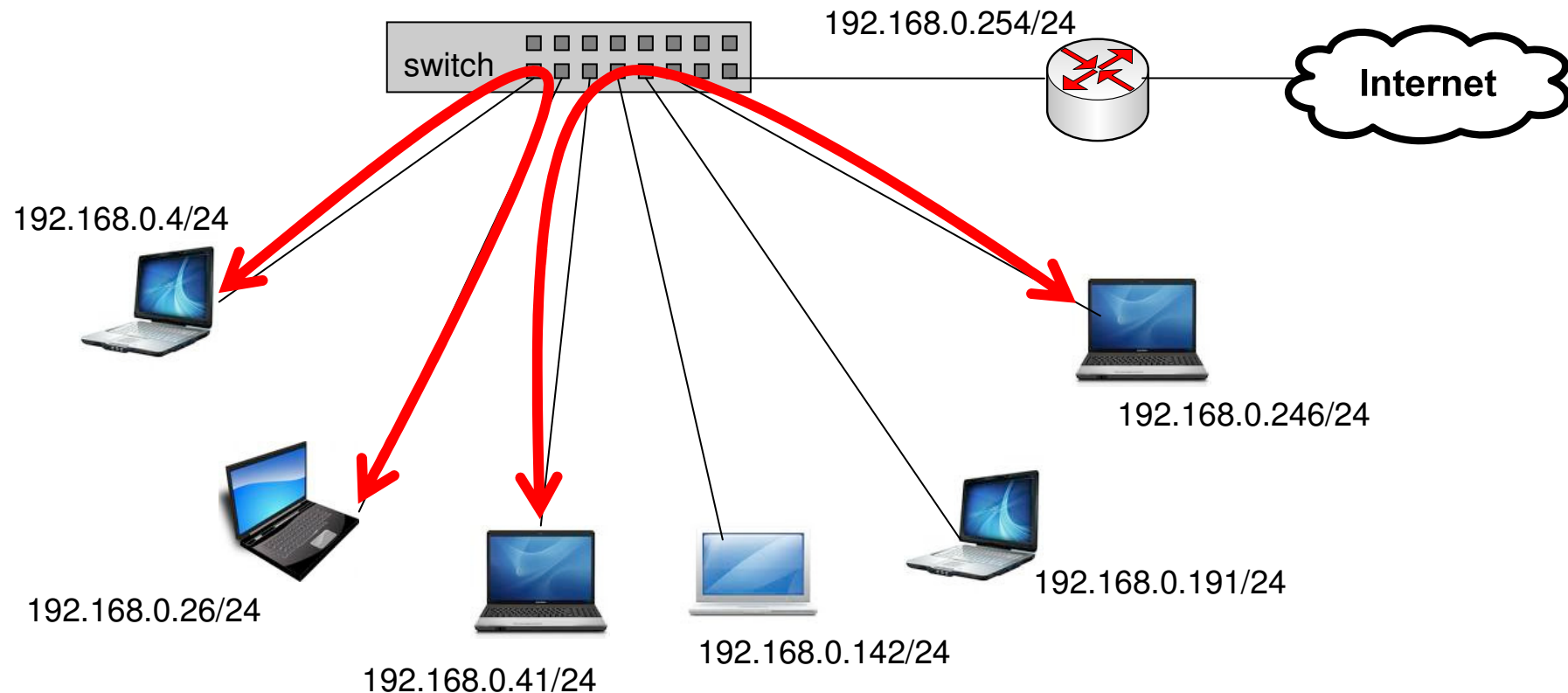
● ● ● | Prinsip Kerja TCP

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



Konsep Dasar Jaringan

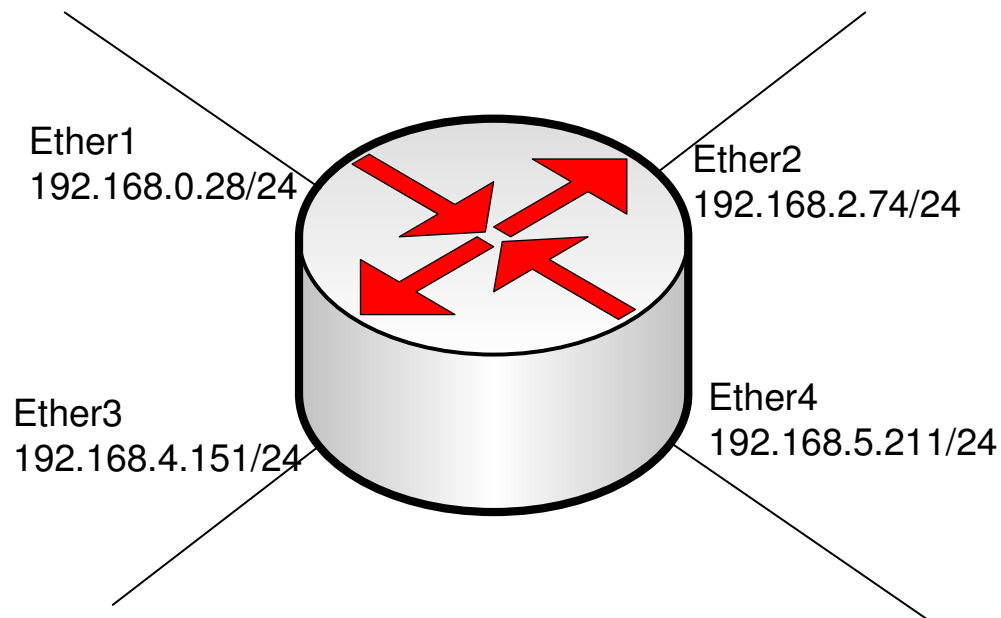
- Host yang memiliki IP Address dari subnet yang sama bisa terkoneksi langsung, tanpa melalui router





Konsep Dasar Jaringan

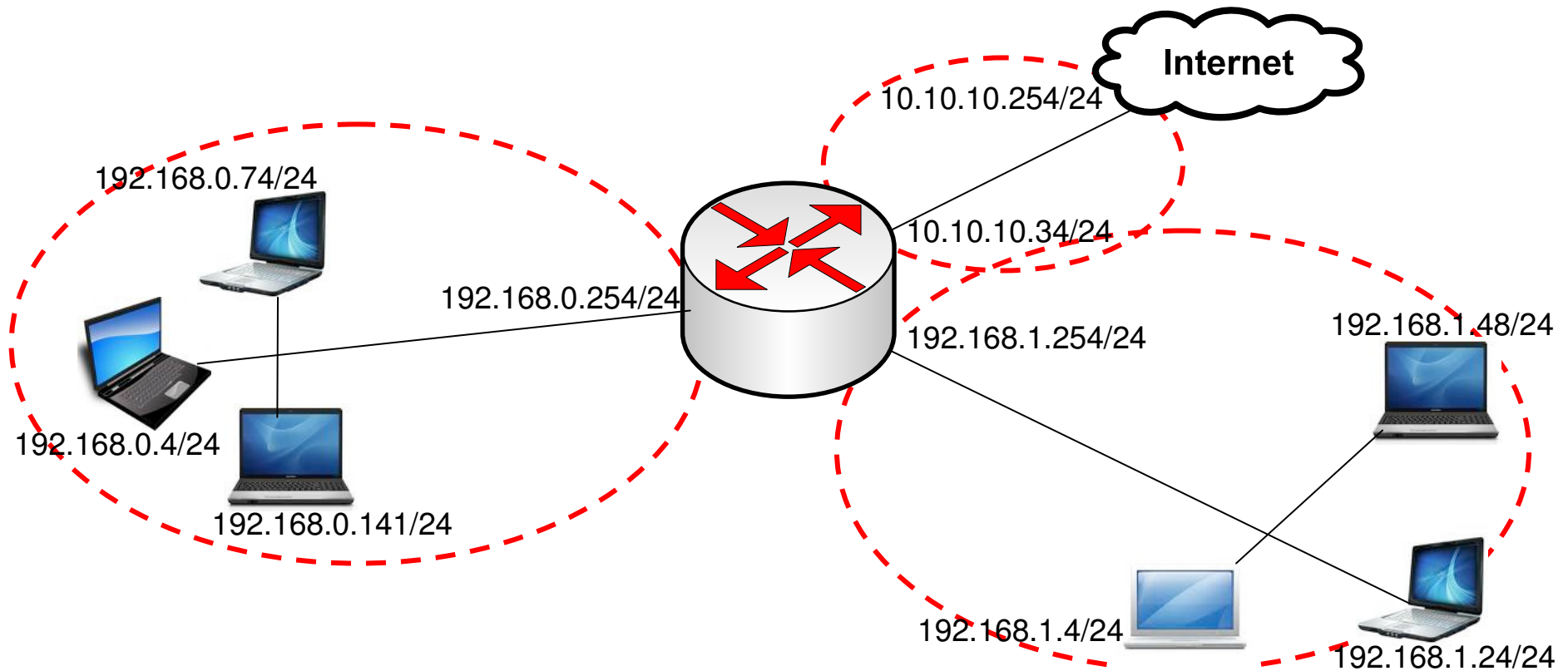
- Dua buah IP Address yang berasal dari subnet yang sama tidak boleh dipasang pada dua buah interface yang berbeda pada sebuah router





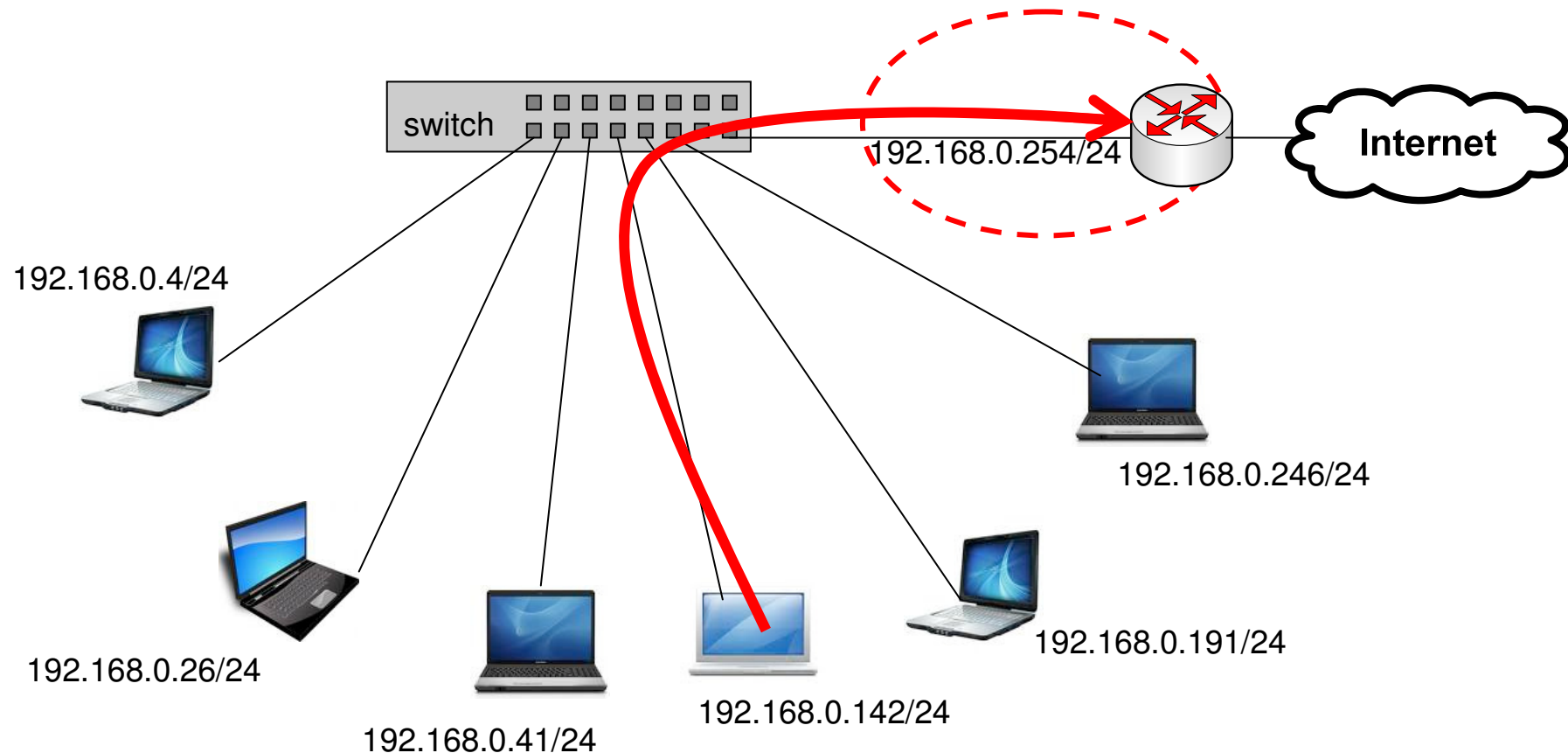
Konsep Dasar Jaringan

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



● ● ● | Konsep Dasar Jaringan

- **Default gateway** menentukan ke arah mana trafik harus disalurkan untuk menuju ke internet



● ● ● | Konsep Dasar Jaringan

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



Static Route

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

● ● ● | Routed Network

- Pengaturan jalur antar network segment berdasarkan IP Address tujuan (atau juga asal), pada OSI layer Network.
- Tiap network segment biasanya memiliki subnet network (IP Address) yang berbeda-beda.

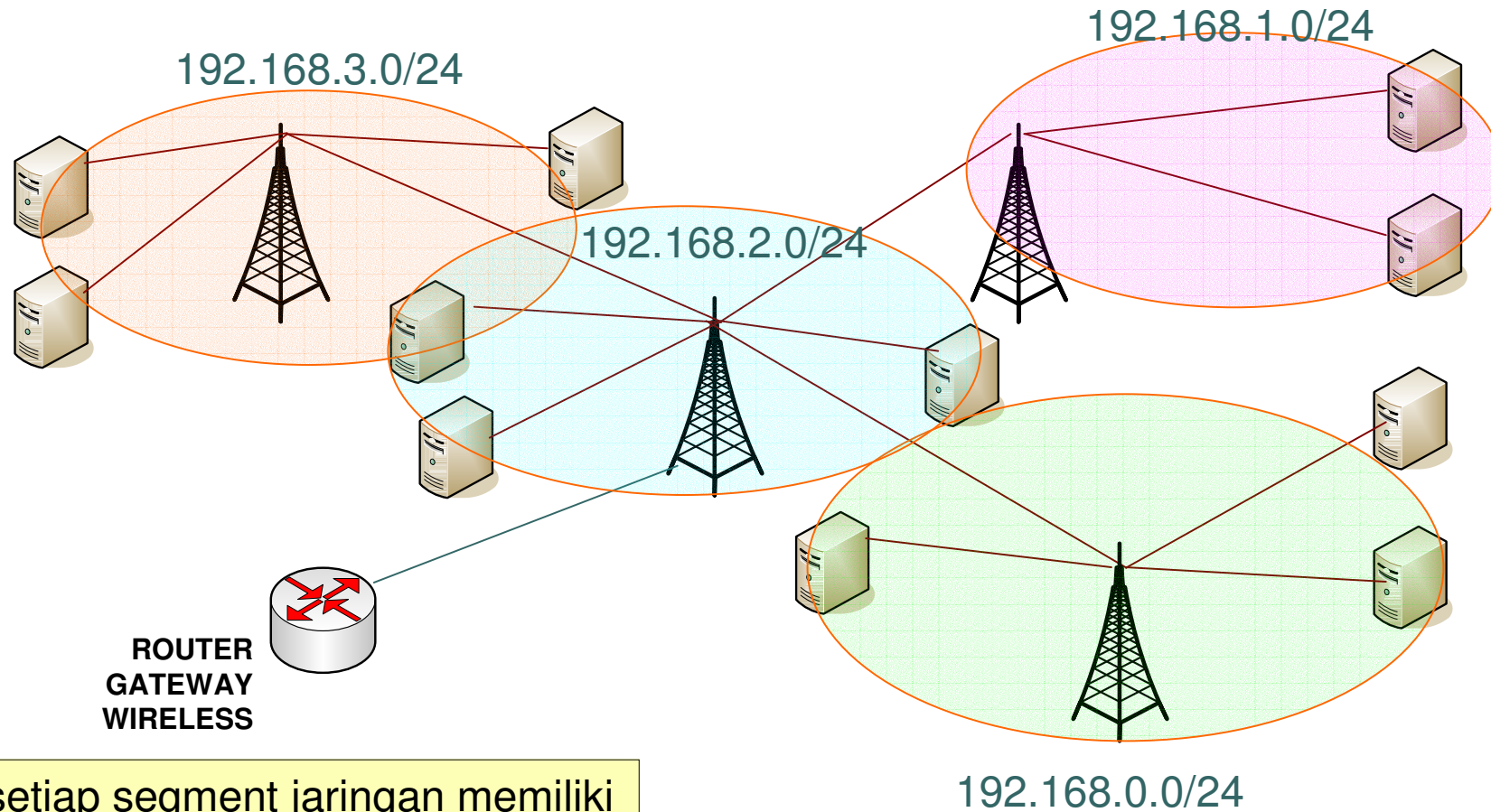


Routing!

- Memungkinkan kita melakukan pemantauan dan pengelolaan jaringan yang lebih baik
- Lebih aman (firewall filtering lebih mudah dan lengkap)
- Trafik broadcast hanya terkonsentrasi di setiap subnet
- Dibutuhkan perangkat wireless yang mampu melakukan full routing, atau menambahkan router di BTS.
- Untuk skala besar, bisa digunakan Dynamic Routing (RIP/OSPF/BGP)



Routing



setiap segment jaringan memiliki subnet IP address yang berbeda.

● ● ● | Tipe Informasi Routing

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

Menambahkan Routing

The screenshot shows the Mikrotik WinBox interface. In the left sidebar, the 'IP' menu item is circled in red, and its sub-menu 'Routes' is also circled in red. A red arrow points to the '+' icon in the 'Route List' window. The 'Route List' window displays a table of routes:

	Destination	Gateway	Gateway ...	Interface	Distance	Route
AS	0.0.0.0/0	10.10.10.100		wlan1	1	
DAC	10.10.10.0/24			wlan1	0	
DAC	192.168.1.0/24			ether1	0	

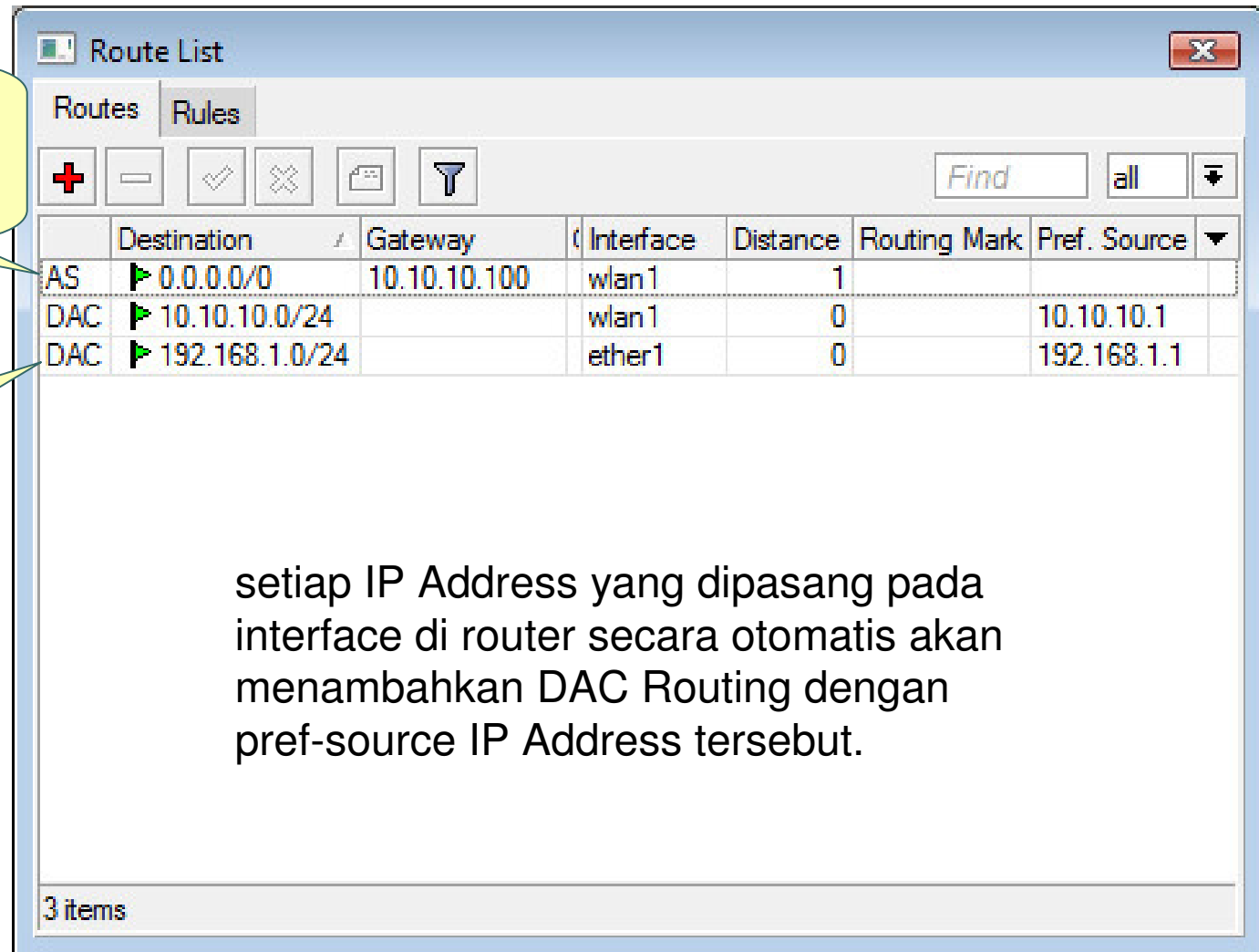
The 'Route <0.0.0.0/0>' configuration window is open, showing the following fields:

- Destination: 0.0.0.0/0
- Gateway: 10.10.10.100
- Gateway Interface: (empty)
- Interface: wlan1
- Check Gateway: (empty)
- Type: unicast
- Distance: 1
- Scope: 255
- Target Scope: 10
- Routing Mark: (empty)
- Pref. Source: (empty)

Tipe Routing

A: Active
S: Static

A: Active
D: Dynamic
C: Connected



The screenshot shows the 'Route List' window in Mikrotik WinBox. It displays a table of routes with columns for Destination, Gateway, Interface, Distance, Routing Mark, and Pref. Source. The first row is highlighted in blue, indicating it is the active route. The second and third rows are marked as 'DAC' (Dynamic Active Connected).

	Destination	Gateway	Interface	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	10.10.10.100	wlan1	1		
DAC	10.10.10.0/24		wlan1	0		10.10.10.1
DAC	192.168.1.0/24		ether1	0		192.168.1.1

3 items

setiap IP Address yang dipasang pada interface di router secara otomatis akan menambahkan DAC Routing dengan pref-source IP Address tersebut.

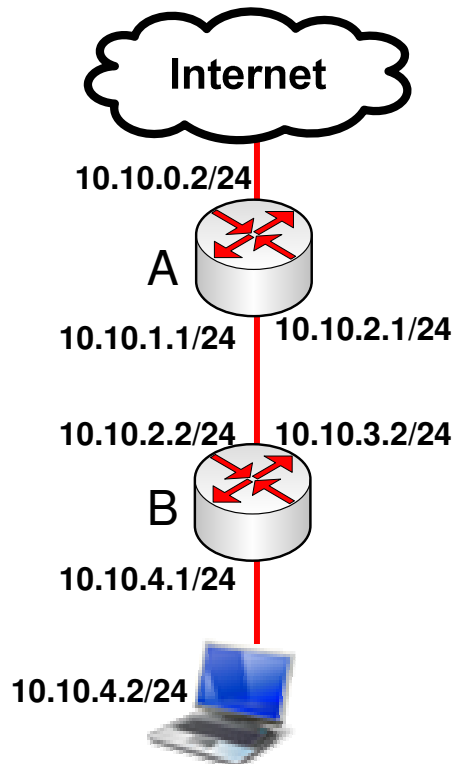


Parameter Dasar Routing

- Destination
 - Destination address & network mask
 - 0.0.0.0/0 -> ke semua network
- Gateway
 - IP Address gateway, harus merupakan IP Address yang satu subnet dengan IP yang terpasang pada salah satu interface
- Gateway Interface
 - Digunakan apabila IP gateway tidak diketahui dan bersifat dinamik.
- Pref Source
 - source IP address dari paket yang akan meninggalkan router
- Distance
 - Beban untuk kalkulasi pemilihan routing

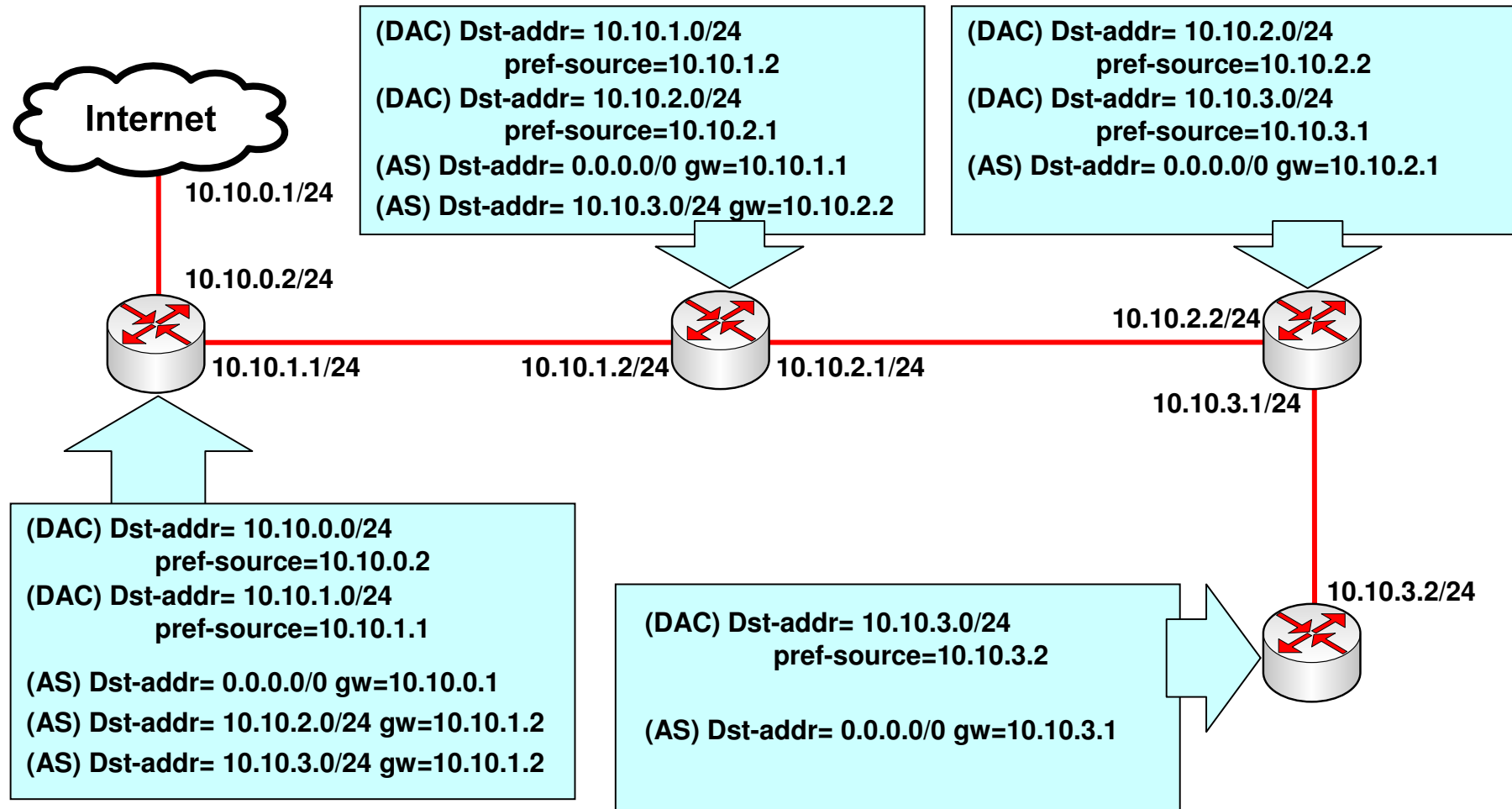
Konsep Dasar Routing

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



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

Implementasi Konsep Routing



● ● ● | Konsep Dasar Routing

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

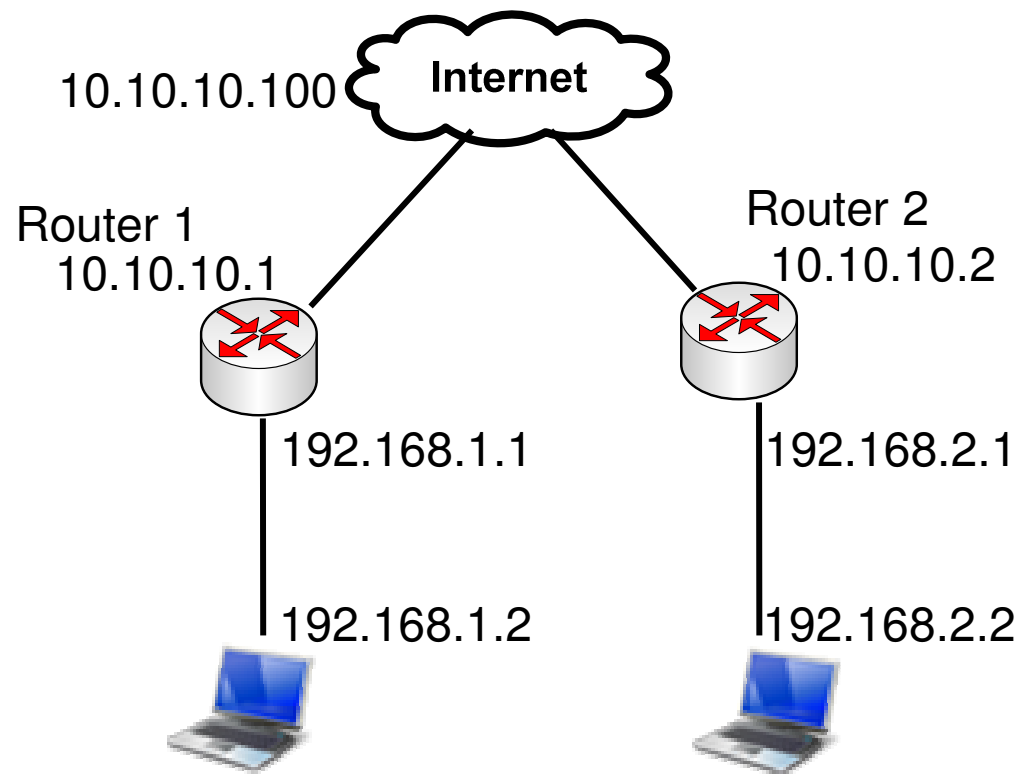
● ● ● | Contoh Pemilihan

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

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

● ● ● | [LAB-1] Static Route

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

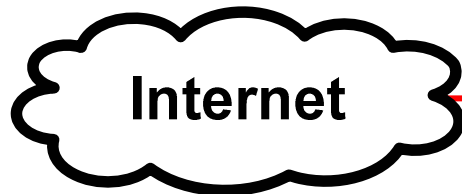


Langkah-langkah

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

[LAB-2] Static Route

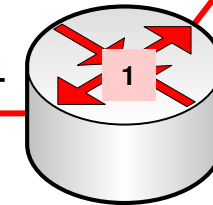
192.168.X.2/24



Internet

10.10.10.100/24

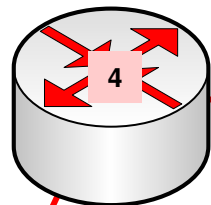
WLAN1:10.10.10.X/24



ETHER3:
10.Y.1.1/24

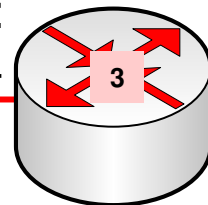
ETHER2:
10.Y.1.2/24

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



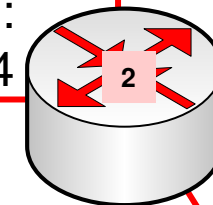
ETHER2:
10.Y.3.2/24

ETHER3:
10.Y.3.1/24



ETHER2:
10.Y.2.2/24

ETHER3:
10.Y.2.1/24



192.168.X.2/24

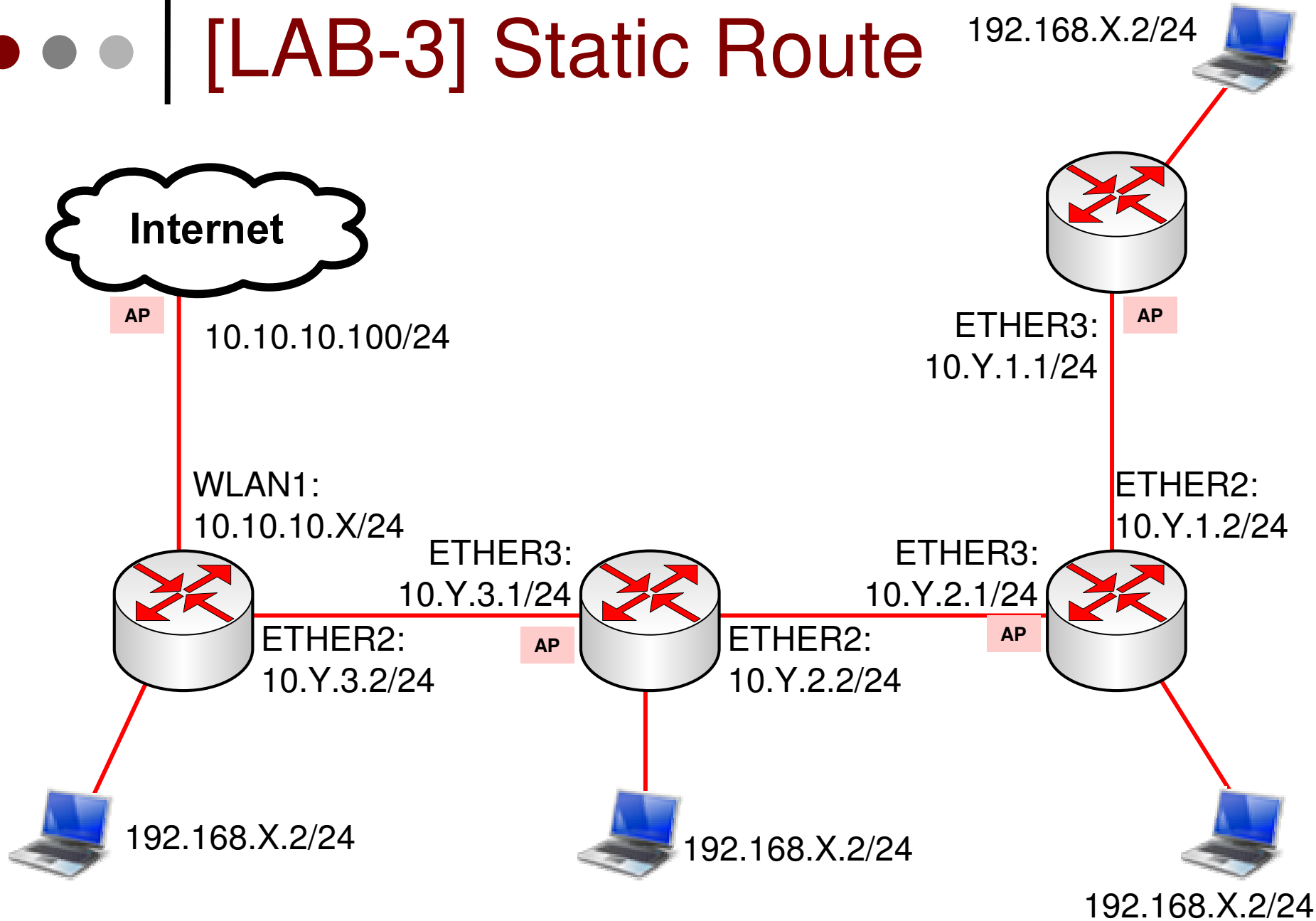


192.168.X.2/24



192.168.X.2/24

[LAB-3] Static Route





Bridge & EoIP

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

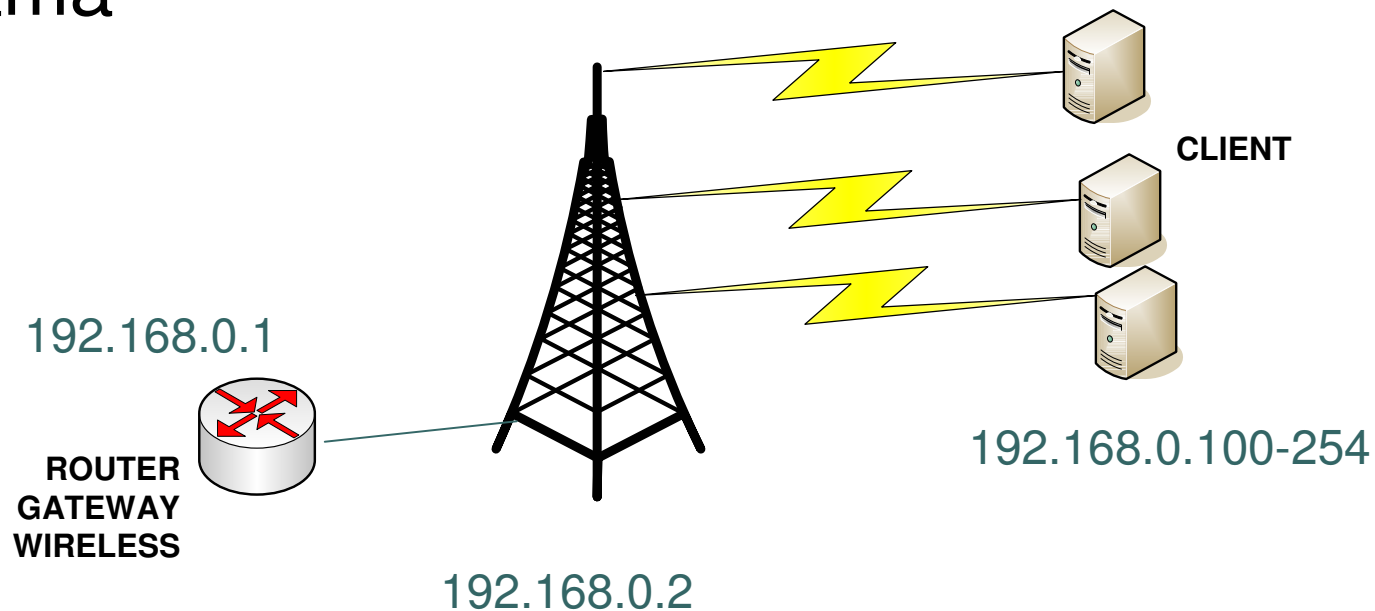


Bridge

- Menggabungkan 2 atau lebih interface yang bertipe ethernet, atau sejenisnya, seolah-olah berada dalam 1 segmen network yang sama.
- Proses pada layer data link.
- Mengaktifkan bridge pada 2 buah interface akan menonaktifkan fungsi routing di antara kedua interface tersebut.
- Sebagian orang suka menggunakan sistem bridge pada wireless network mereka, karena:
 - Lebih mudah dibuat
 - Perangkat wireless umumnya tidak mendukung routing

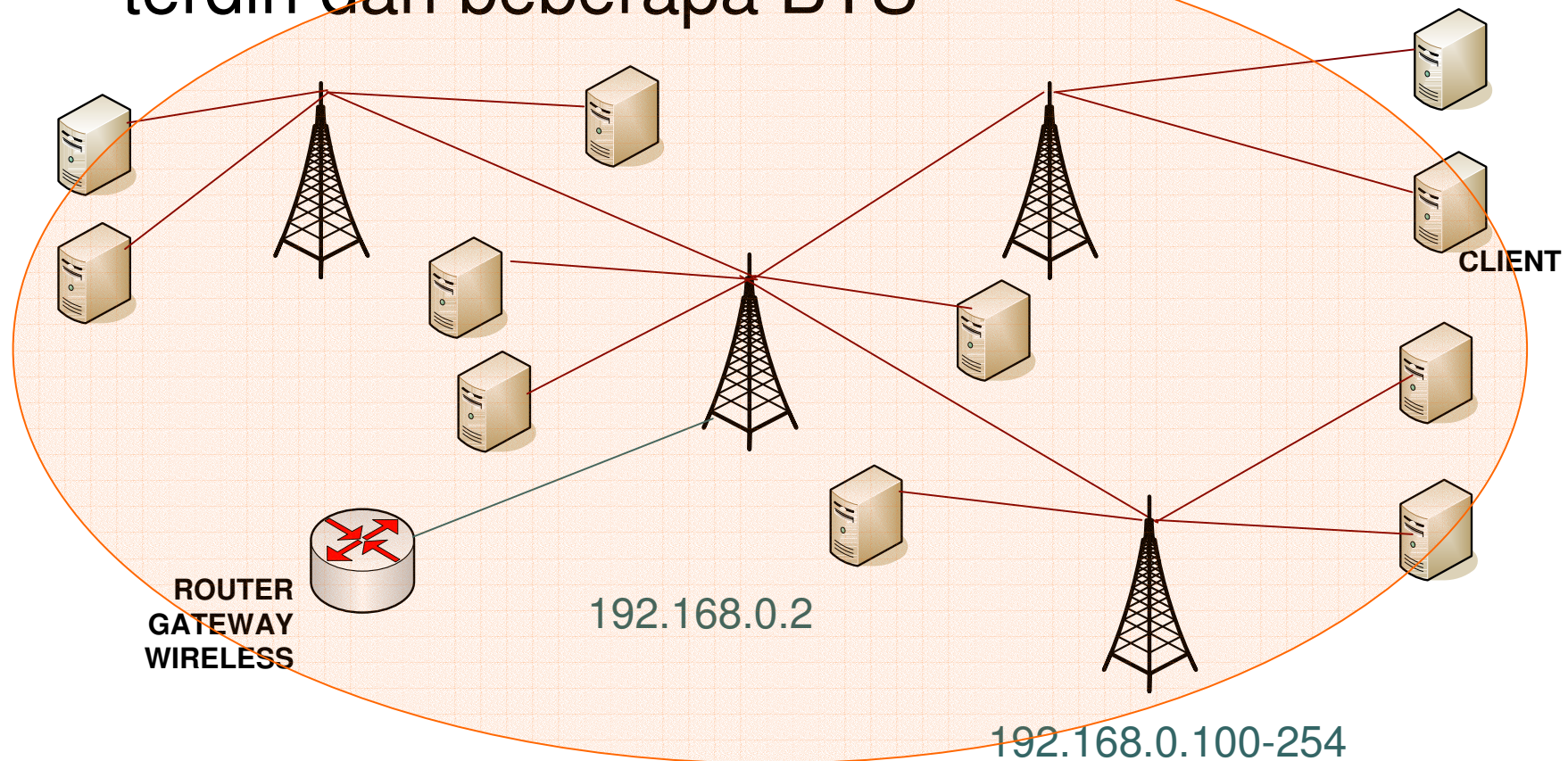
Sistem Bridge

- Perangkat-perangkat wireless berada dalam satu subnet / bridge network yang sama



● ● ● | Sistem Bridge

- Bayangkan kalau network wireless sudah terdiri dari beberapa BTS





Sistem Bridge

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

● ● ● | Bridge Interface

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



Perhatikan!

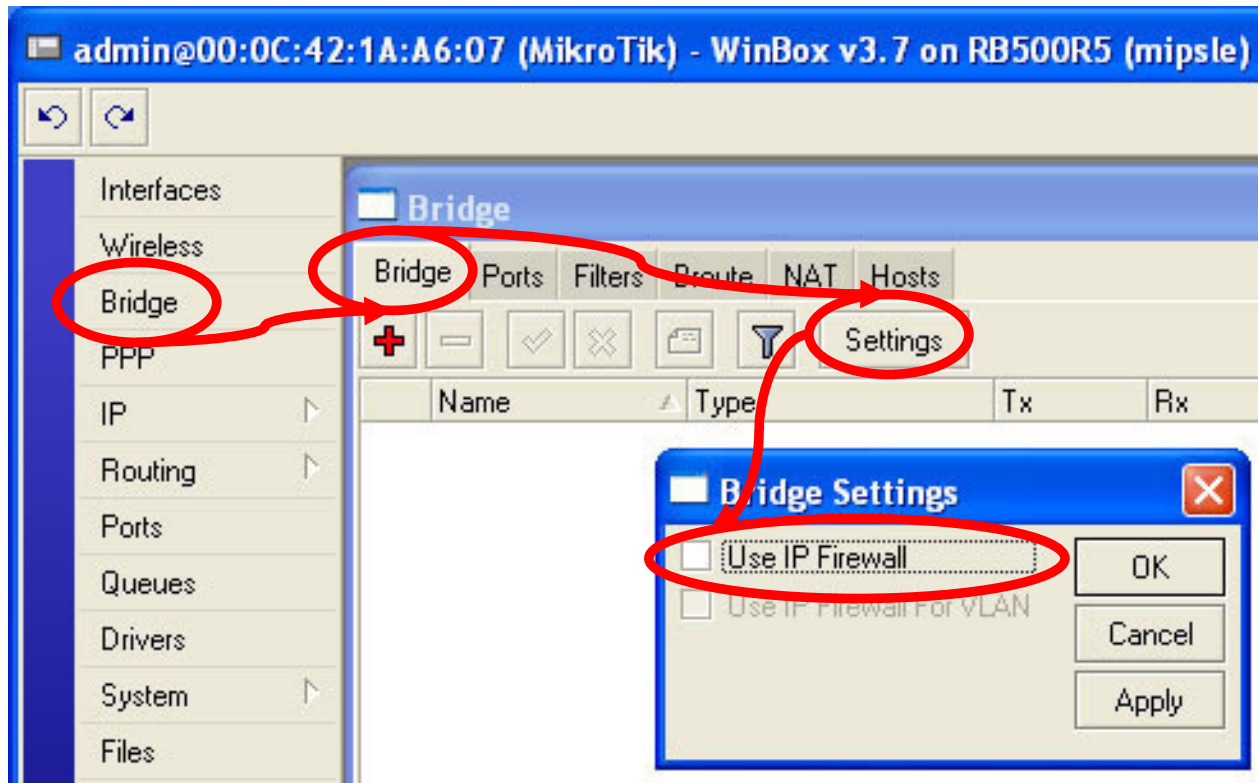
- Kita tidak harus memasang IP Address pada sebuah bridge interface
- Jika kita menonaktifkan bridge, pada IP Address yang terpasang pada bridge akan menjadi invalid
- Kita tidak bisa membuat bridge dengan interface lainnya, seperti synchronous, IPIP, PPPoE, dll.
- Namun, kita bisa melakukan bridge pada interface lainnya dengan membuat EoIP terlebih dahulu pada interface tersebut
- EoIP hanya bekerja antar perangkat Mikrotik, dan tidak bisa dihubungkan dengan perangkat merk lain.

- ● ● |

Membuat Bridge

- Membuat interface bridge
 - Memasukkan interface ethernet ke interface bridge
 - Pastikan bahwa IP Address berada dalam satu segmen network
-

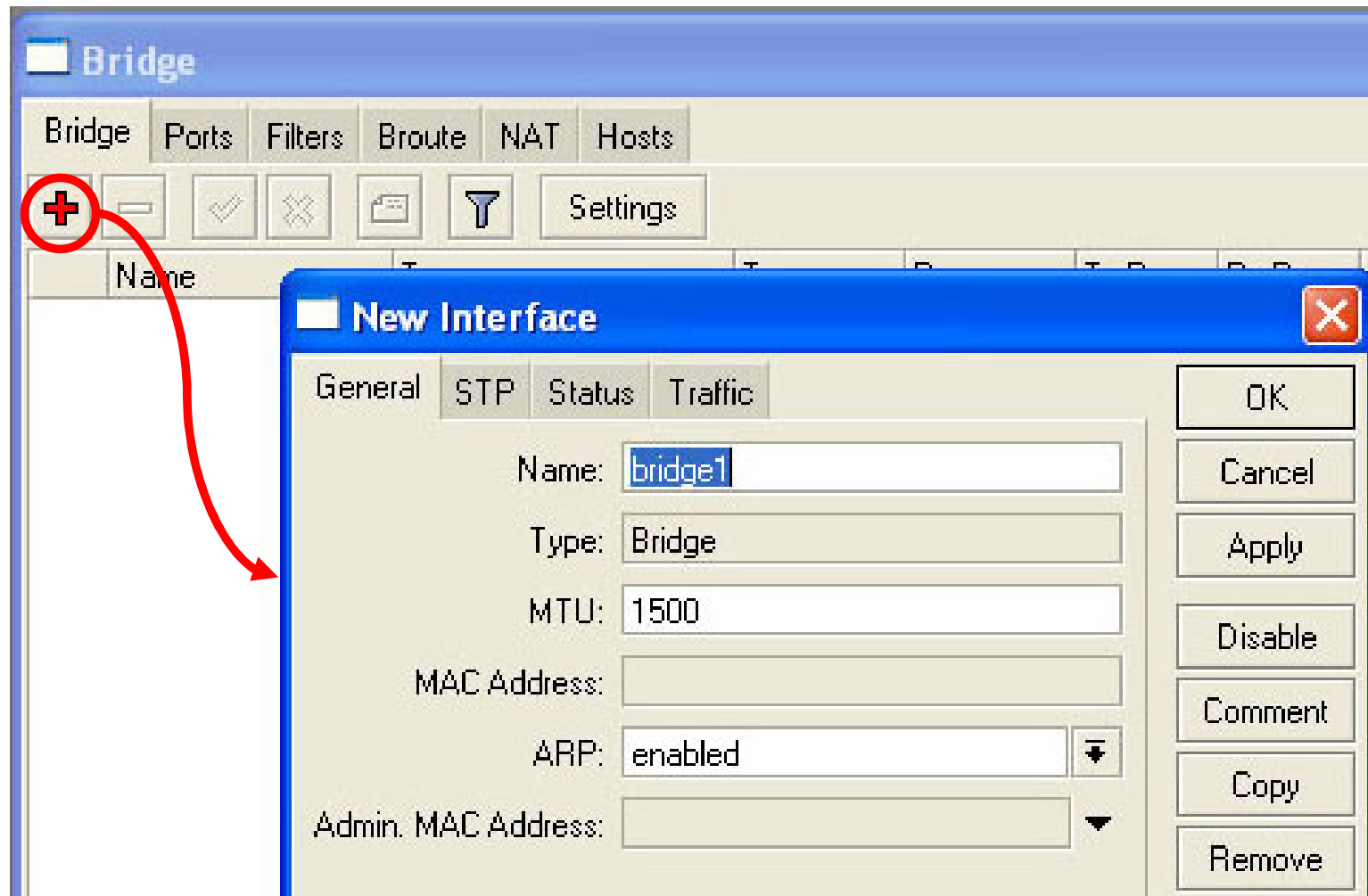
Konfigurasi Bridge



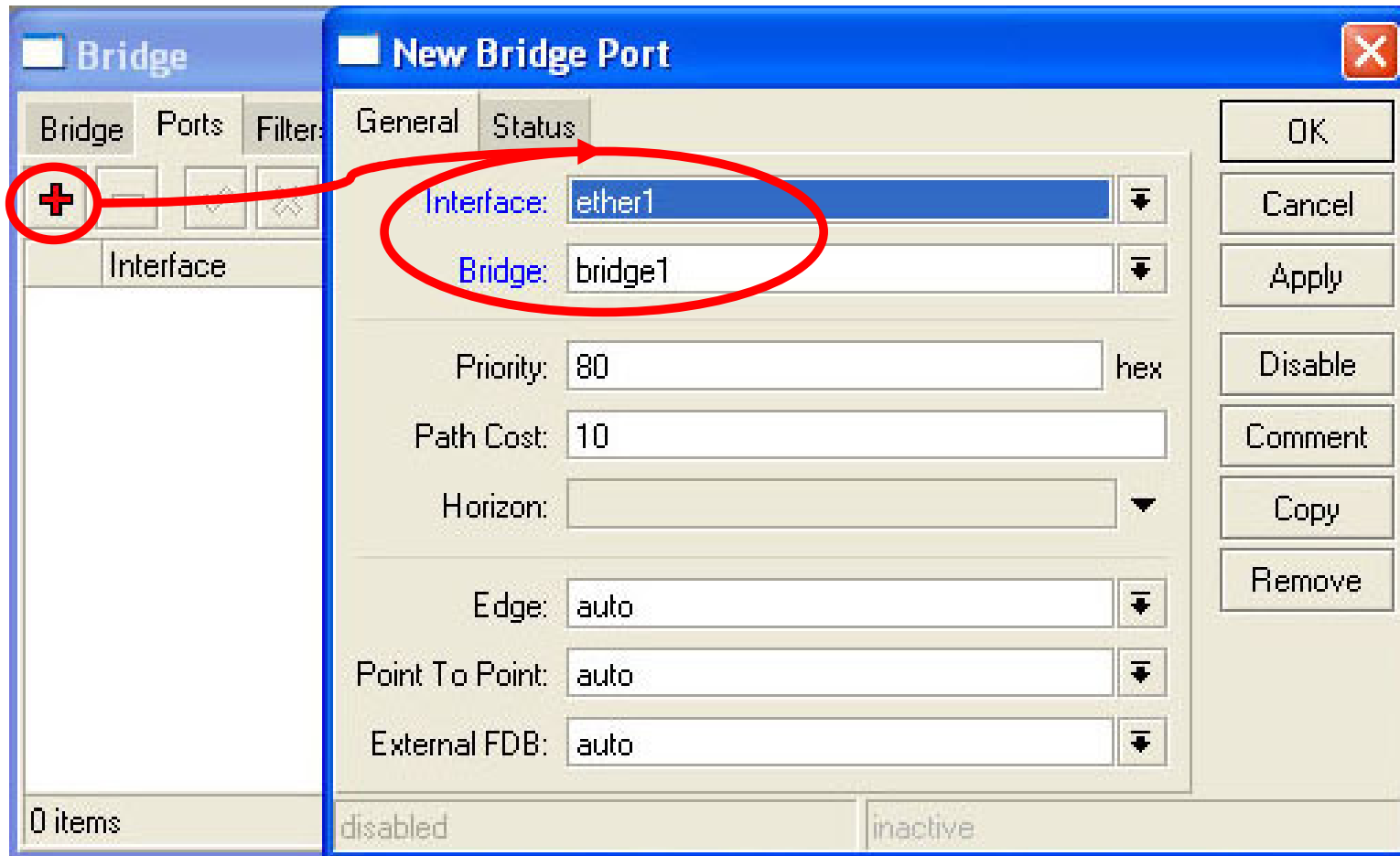
Secara default, jika kita menggunakan bridge, maka rule yang ada di firewall tidak akan berpengaruh. Aktifkanlah setting ini jika dibutuhkan.



Membuat Interface Bridge

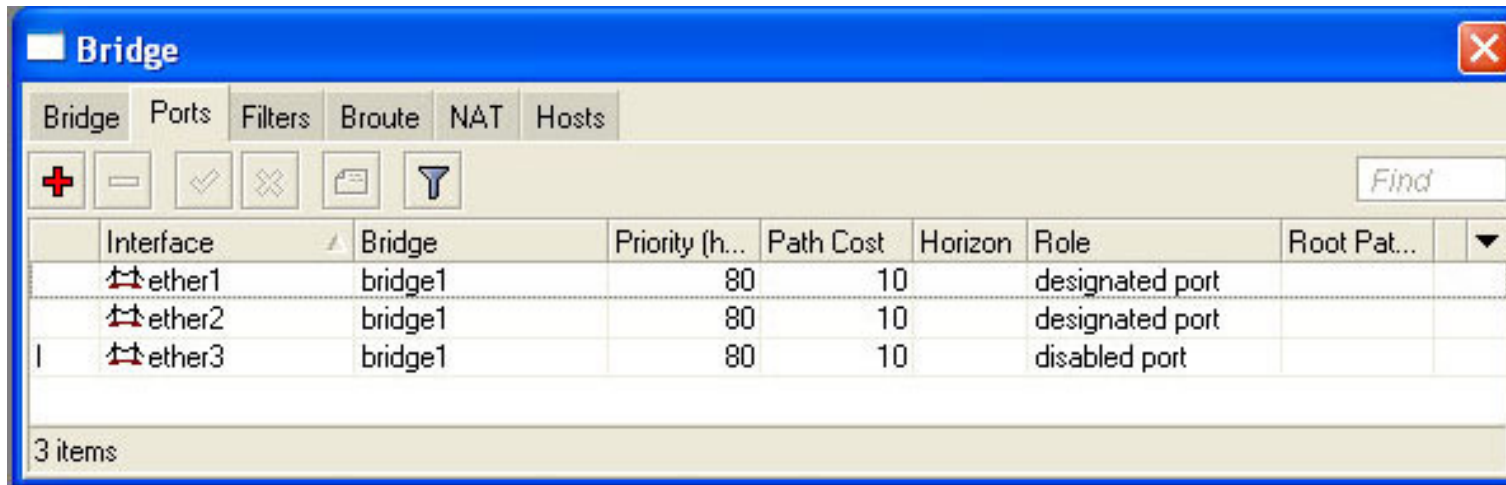


Setting Bridge Ports



Bridge Ports

Setelah ketiga interface dimasukkan ke dalam bridge

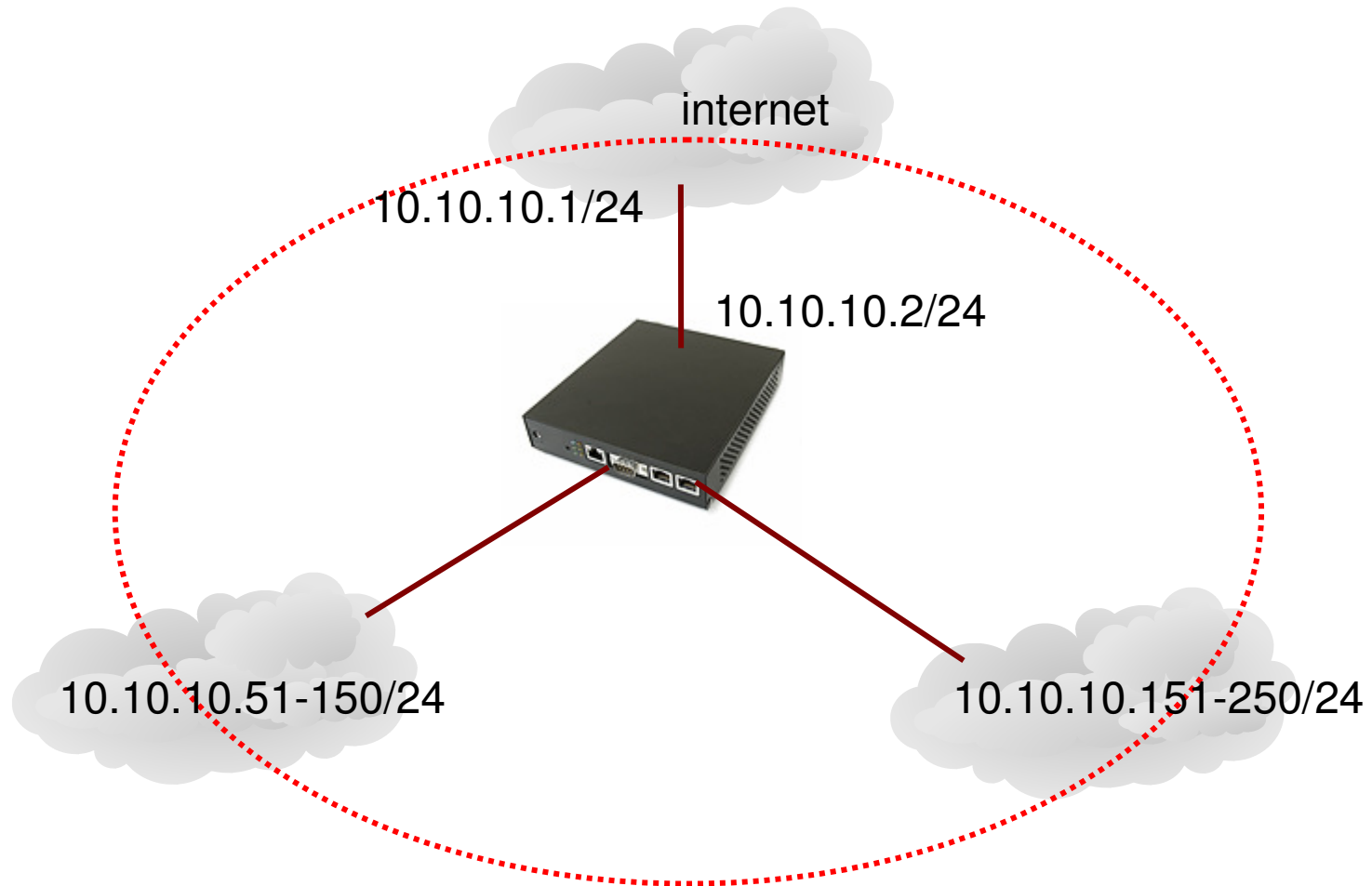


Interface	Bridge	Priority (h...	Path Cost	Horizon	Role	Root Pat...
ether1	bridge1	80	10		designated port	
ether2	bridge1	80	10		designated port	
ether3	bridge1	80	10		disabled port	

```
/interface bridge add name=bridge1 disabled=no  
/interface bridge port add interface=ether1 bridge=bridge1  
/interface bridge port add interface=ether2 bridge=bridge1  
/interface bridge port add interface=ether2 bridge=bridge1
```

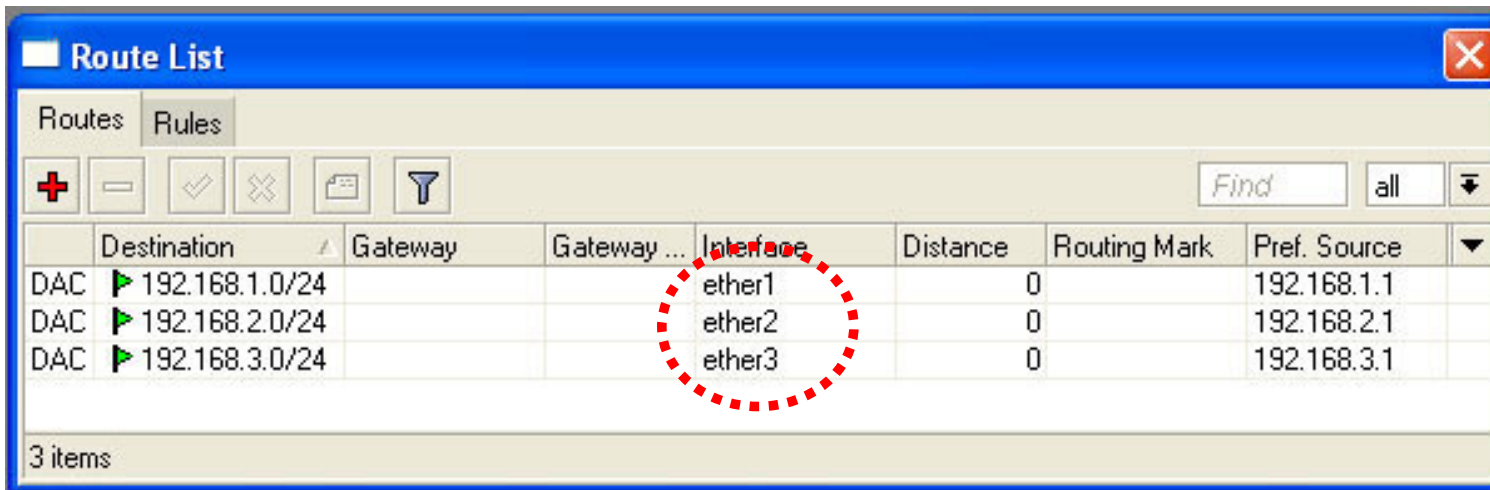



Contoh (bridge network)



● ● ● | Perhatikanlah IP Route

Sebelum bridge dibuat IP Address terletak pada interface masing-masing



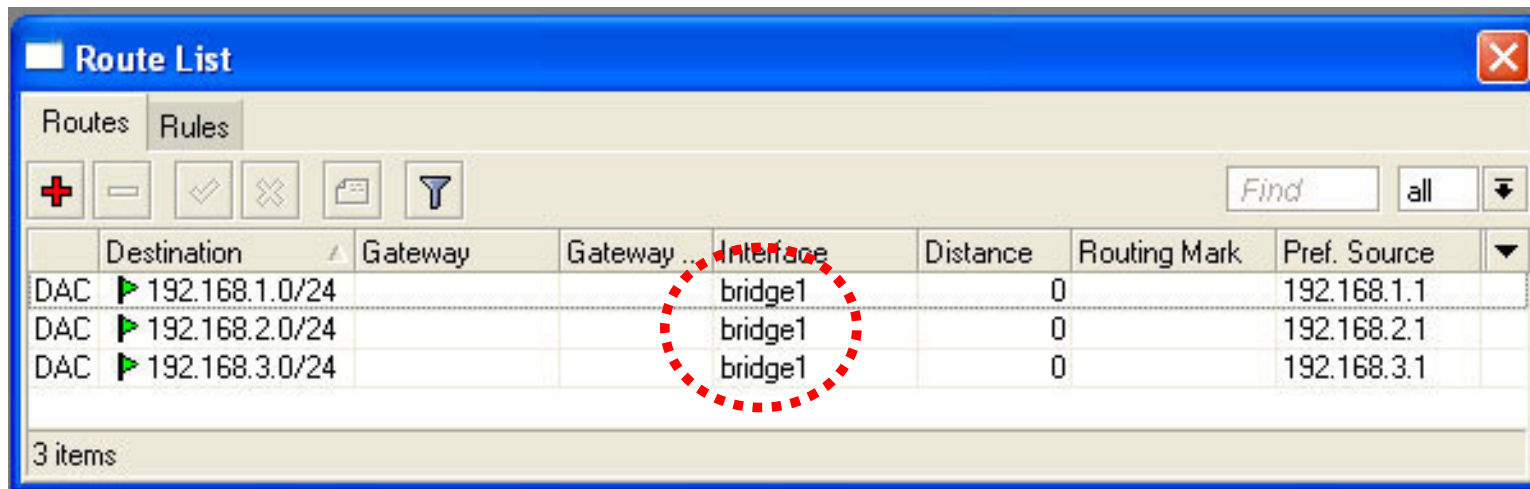
The screenshot shows the 'Route List' window in Mikrotik WinBox. It displays three routes, each with a destination of 192.168.x.0/24 and a distance of 0. The interfaces are ether1, ether2, and ether3. The 'Interface' column is circled in red.

	Destination	Gateway	Gateway ...	Interface	Distance	Routing Mark	Pref. Source	
DAC	▶ 192.168.1.0/24			ether1	0		192.168.1.1	
DAC	▶ 192.168.2.0/24			ether2	0		192.168.2.1	
DAC	▶ 192.168.3.0/24			ether3	0		192.168.3.1	

3 items

IP Route

- Setelah interface dimasukkan ke dalam bridge, maka dynamic routing juga akan berpindah ke interface bridge:



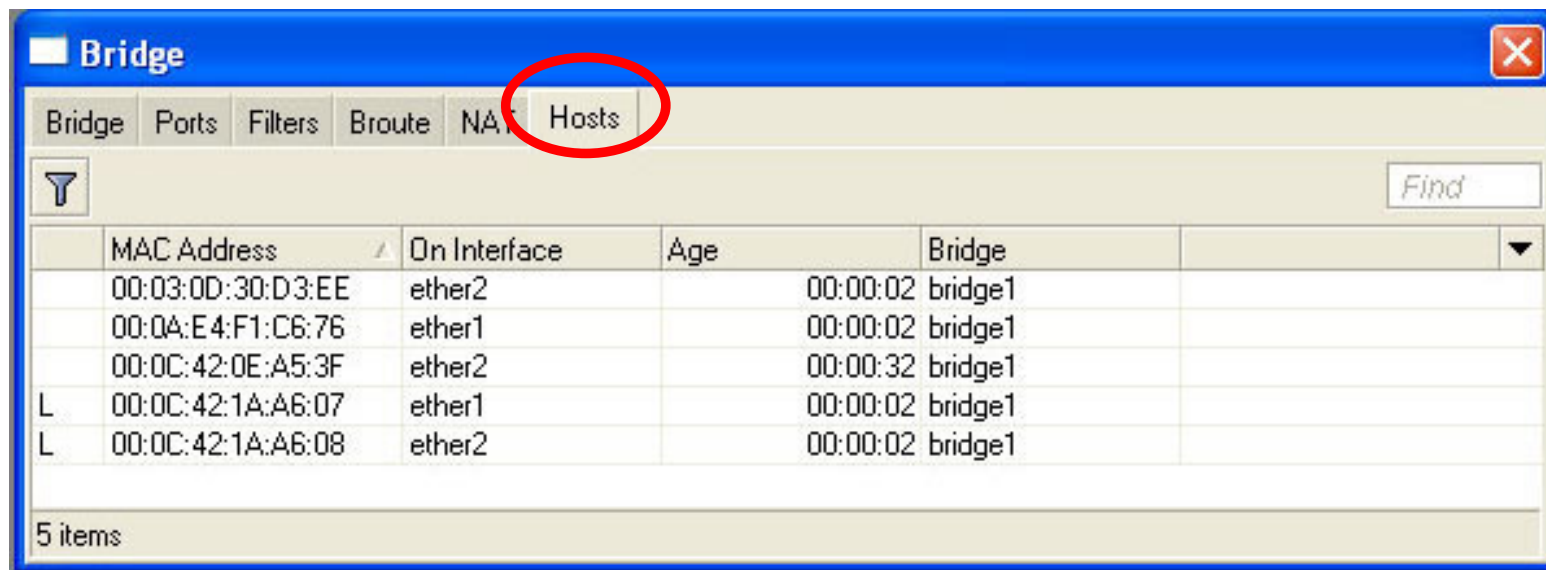
The screenshot shows a window titled "Route List" with a table of routes. The table has columns for Destination, Gateway, Gateway..., Interface, Distance, Routing Mark, and Pref. Source. Three routes are listed, all with a distance of 0 and a preferred source of 192.168.x.x. The interface for all three routes is "bridge1".

	Destination	Gateway	Gateway ...	Interface	Distance	Routing Mark	Pref. Source
DAC	▶ 192.168.1.0/24			bridge1	0		192.168.1.1
DAC	▶ 192.168.2.0/24			bridge1	0		192.168.2.1
DAC	▶ 192.168.3.0/24			bridge1	0		192.168.3.1

3 items

Bridge Monitoring

- o Untuk melihat mac-address host yang terkoneksi



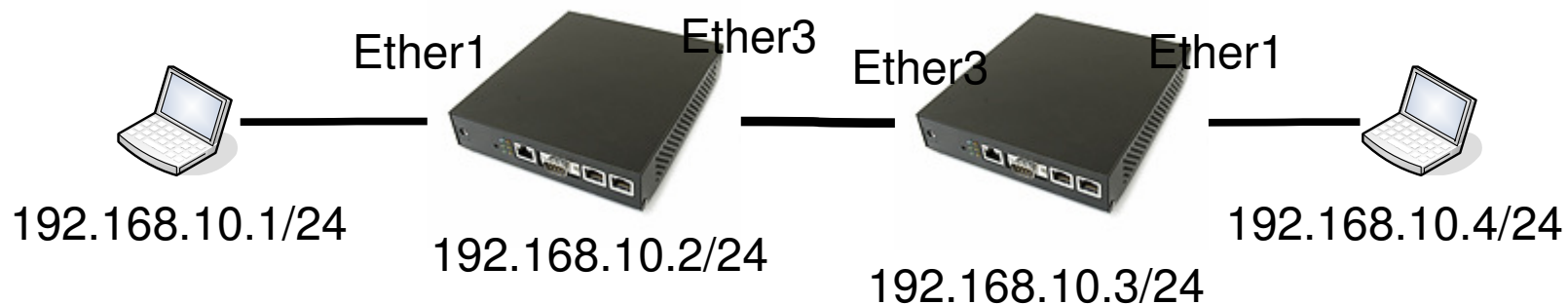
The screenshot shows the Mikrotik WinBox interface for Bridge Monitoring. The 'Hosts' tab is selected and circled in red. The table below displays the MAC addresses of hosts connected to the bridge.

	MAC Address	On Interface	Age	Bridge
	00:03:0D:30:D3:EE	ether2		00:00:02 bridge1
	00:0A:E4:F1:C6:76	ether1		00:00:02 bridge1
	00:0C:42:0E:A5:3F	ether2		00:00:32 bridge1
L	00:0C:42:1A:A6:07	ether1		00:00:02 bridge1
L	00:0C:42:1A:A6:08	ether2		00:00:02 bridge1

5 items

● ● ● | LAB – Bridge (1)

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



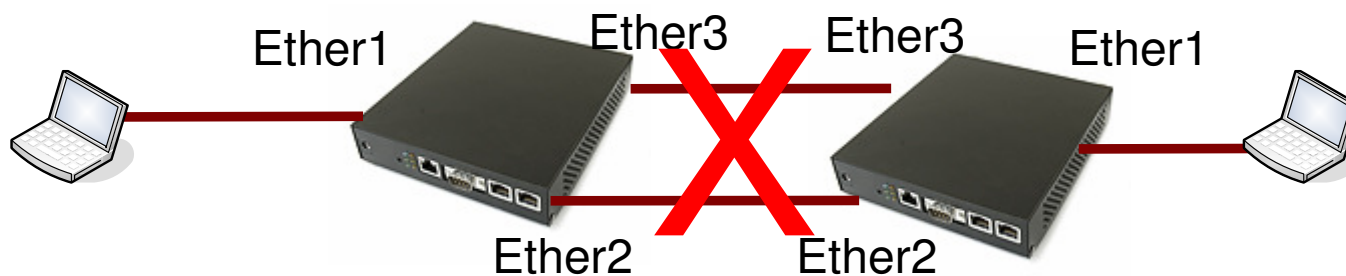
- ● ● |

Bridge Loop

- Jika terdapat dua atau lebih jalur yang berada dalam sebuah network bridge, hati-hati terjadinya bridge loop.
 - Untuk menghindari terjadinya bridge loop, kita menggunakan STP (*Spanning Tree Protocol*)
 - Meskipun tidak terlalu bagus (kurang responsif), STP dapat juga digunakan sebagai fail over system
-

● ● ● | Contoh Bridge Loop

- Jika Ether1 dan Ether2 pada kedua router dimasukkan ke dalam bridge, maka akan terjadi bridge loop



- Untuk menghindari terjadinya bridge-loop, kita menggunakan fitur STP / RSTP

RSTP (Rapid Spanning Tree Protocol)

- **Rapid Spanning Tree Protocol (RSTP)**
- In 1998, the IEEE introduced an evolution of the Spanning Tree Protocol: Rapid Spanning Tree Protocol (RSTP) or 802.1w. In the 2004 edition of 802.1D, STP is superseded by the RSTP.
- RSTP is an evolution of the Spanning Tree Protocol, and was introduced in the extension IEEE 802.1w, and provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP.
- **RSTP switch port roles:**
 - **Root** - A forwarding port that has been elected for the spanning-tree topology
 - **Designated** - A forwarding port for every LAN segment
 - **Alternate** - An alternate path to the root bridge. This path is different than using the root port.
 - **Backup** - A backup/redundant path to a segment where another switch port already connects.
 - **Disabled** - Not strictly part of STP, a network administrator can manually disable a port

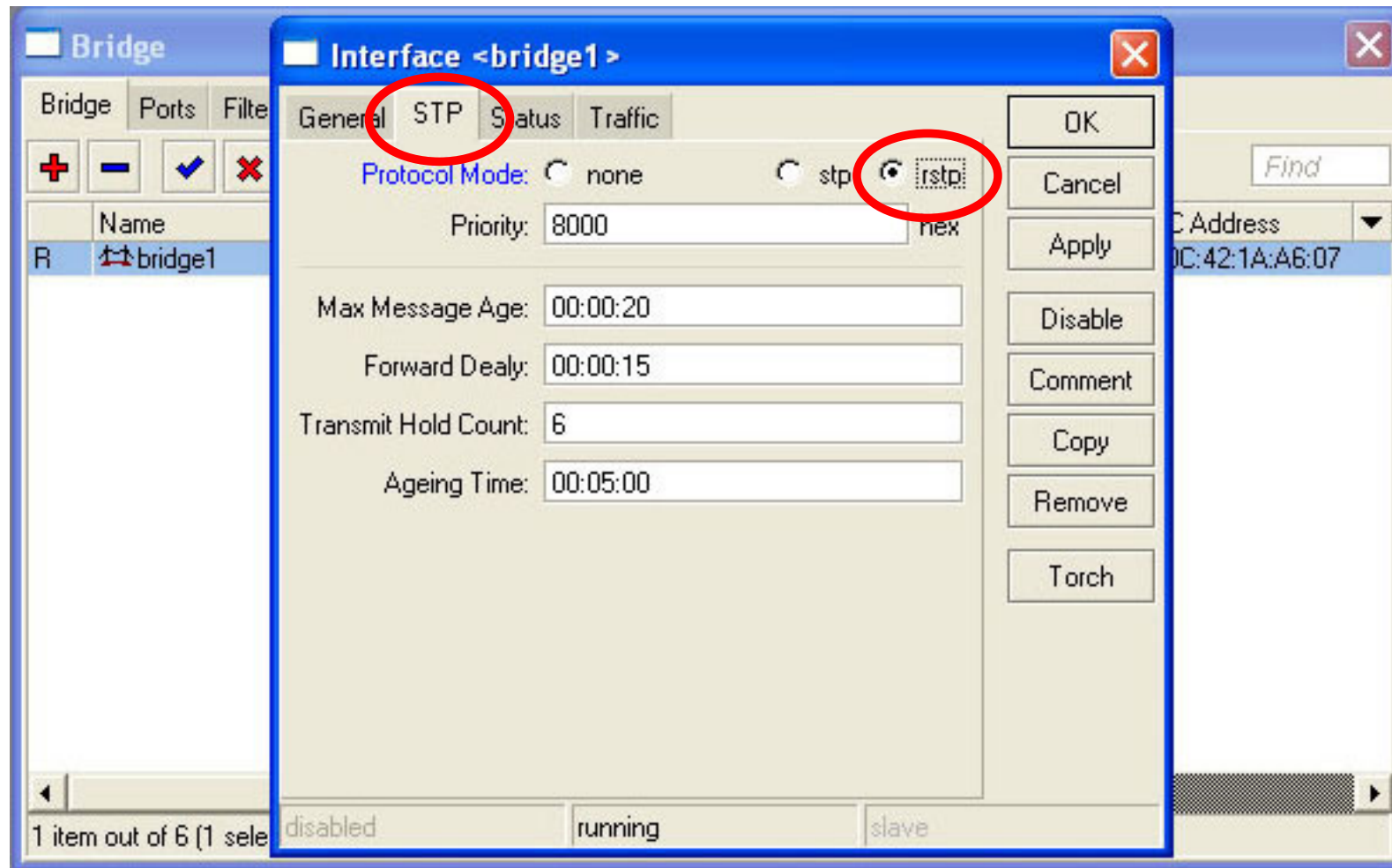
RSTP

- RSTP is a refinement of STP and therefore share most of its basic operation characteristics. However there are some notable differences as summarized below
- Detection of root switch failure is done in 3 hello times or 6 seconds if default hello time have not been changed
- All ports that have been configured as access ports are placed in forwarding state without ever checking for loops. However the switch will disable them if it detects a loop.
- Unlike in STP where the algorithm is passive - ie wait for time to pass for information collection, RSTP will actively send inquiry packet seeking information from neighboring switches. This leads to a faster convergence.

	STP	RSTP
Recovery Time	30~60 sec	3~6 sec
Protocol	IEEE802.1D	IEEE802.1w
Configuration	complex	complex

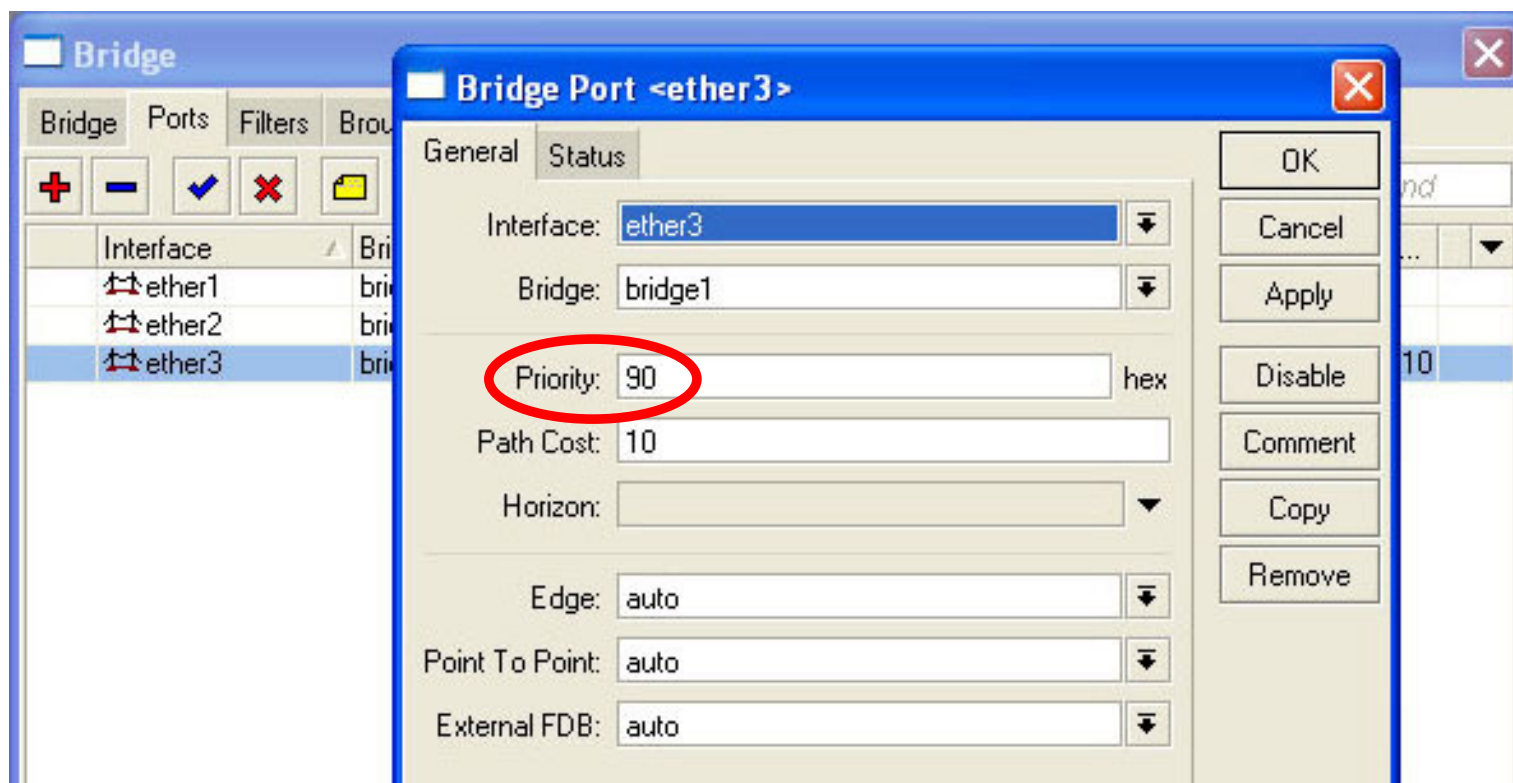


Menset RSTP pada bridge



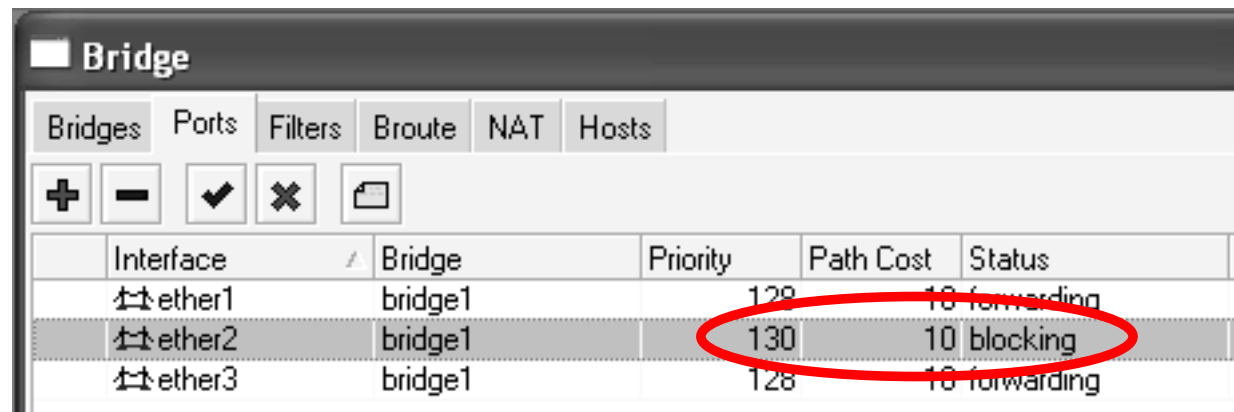
● ● ● | Prioritas Bridge

- Kita bisa menentukan prioritas jalur yang digunakan pada bridge, jalur lainnya akan menjadi backup (fail over system)



● ● ● | Status Bridge

- Pada salah satu router, link back up akan berstatus blocking



Bridge

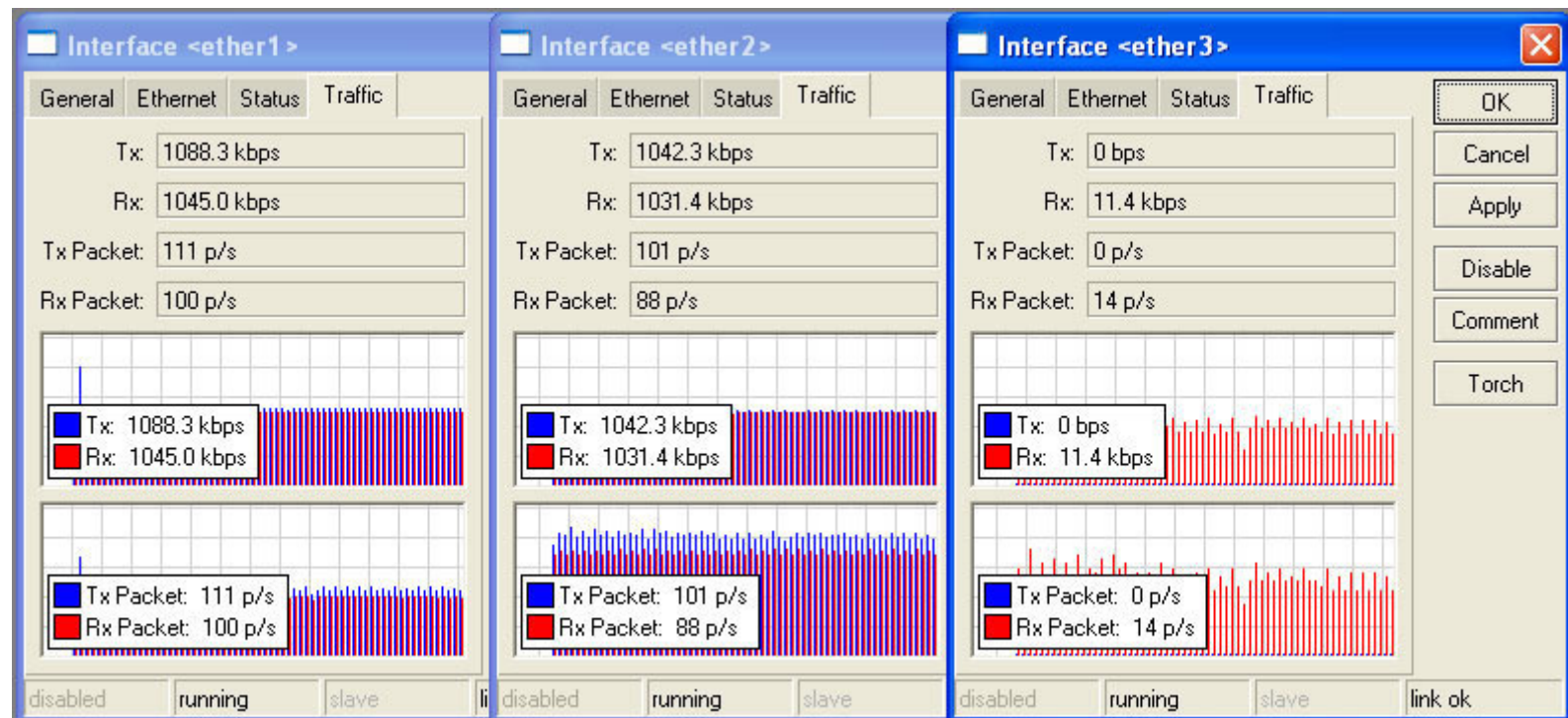
Bridges Ports Filters Broute NAT Hosts

+ - ✓ ✗ 📄

Interface	Bridge	Priority	Path Cost	Status
ether1	bridge1	128	10	forwarding
ether2	bridge1	130	10	blocking
ether3	bridge1	128	10	forwarding

Monitoring Link

- Cobalah lakukan bandwidth test dari laptop ke laptop. Amati besarnya trafik yang melalui setiap interface



- ● ● |

Fail Over Test

- Cobalah mencabut kabel pada ether2 dan amati perubahannya.



Interface List

Interface Ethernet EoIP Tunnel IP Tunnel VLAN VRRP Bonding

+ - ✓ ✗ 📄 🔍 Find

	Name	Type	Tx	Rx	Tx Pac...	Rx Pac...
R	↔ bridge1	Bridge	0 bps	10.7 kbps	0	15
R	↔ ether1	Ethernet	1094.4 k...	1046.0 k...	113	101
	↔ ether2	Ethernet	0 bps	0 bps	0	0
R	↔ ether3	Ethernet	1042.8 k...	1031.4 k...	101	88

Bridge

Bridge Ports Filters Broute NAT Hosts

+ - ✓ ✗ 📄 🔍 Find

	Interface	Bridge	Priority (h...	Path Cost	Horizon	Role	Root Pat...
	↔ ether1	bridge1	80	10		designated port	
I	↔ ether2	bridge1	80	10		disabled port	
	↔ ether3	bridge1	90	10		designated port	

Interface <ether1>

General Ethernet Status Traffic

Tx: 1094.4 kbps
Rx: 1046.0 kbps
Tx Packet: 113 p/s
Rx Packet: 101 p/s

Tx: 1094.4 kbps
Rx: 1046.0 kbps

Tx Packet: 113 p/s
Rx Packet: 101 p/s

disabled running slave

Interface <ether2>

General Ethernet Status Traffic

Tx: 0 bps
Rx: 0 bps
Tx Packet: 0 p/s
Rx Packet: 0 p/s

Tx: 0 bps
Rx: 0 bps

Tx Packet: 0 p/s
Rx Packet: 0 p/s

disabled running slave

Interface <ether3>

General Ethernet Status Traffic

Tx: 1042.8 kbps
Rx: 1031.4 kbps
Tx Packet: 101 p/s
Rx Packet: 88 p/s

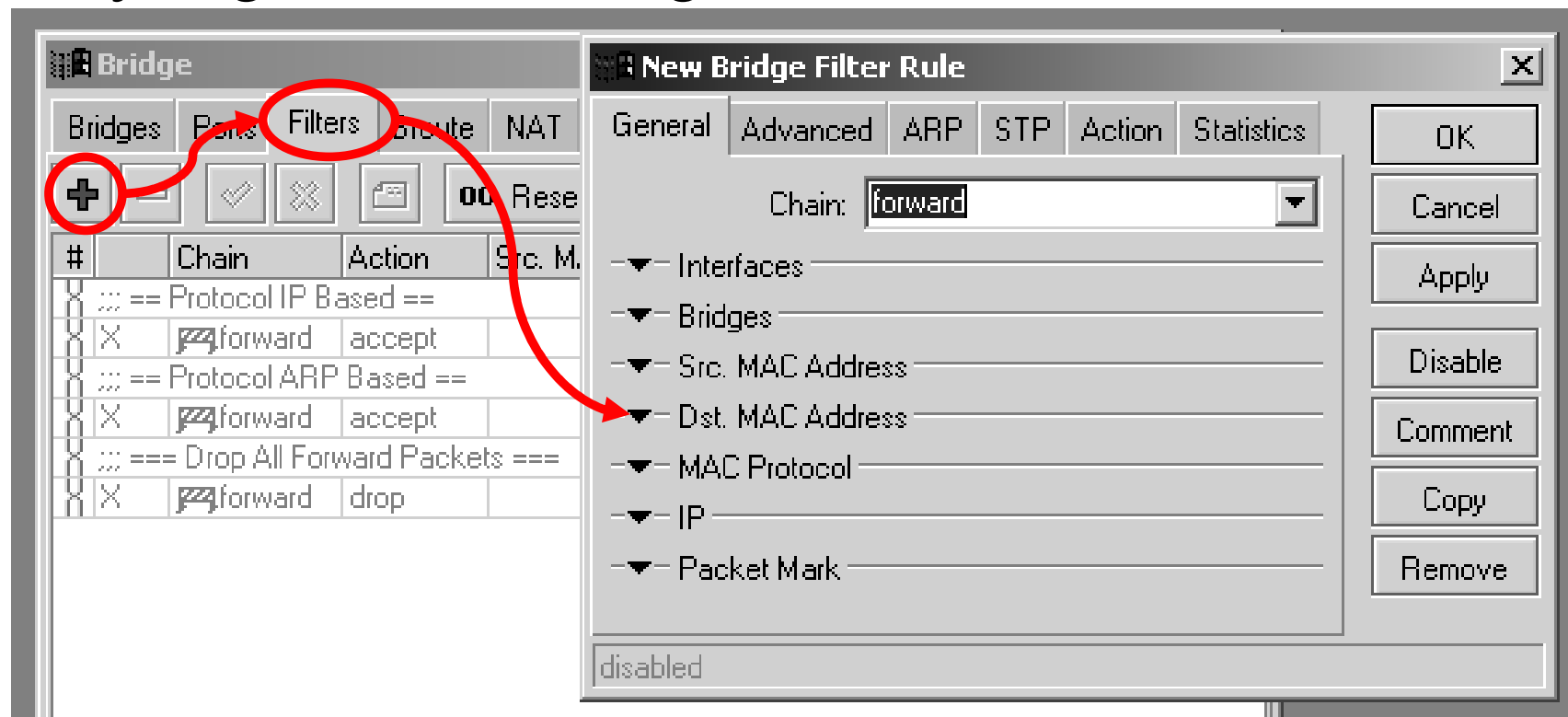
Tx: 1042.8 kbps
Rx: 1031.4 kbps

Tx Packet: 101 p/s
Rx Packet: 88 p/s

disabled running slave

Bridge Filtering

- Kita dapat melakukan filtering pada trafik yang melalui bridge





Memblok ICMP pada Bridge

New Bridge Filter Rule

General | Advanced | ARP | STP | Action | Statistics

Chain: **forward**

Interfaces

In. Interface: ether3

Out. Interface: ether1

Bridges

Src. MAC Address

Dst. MAC Address

MAC Protocol

MAC Protocol: **800 (ip)** hex

IP

Src. Address:

Src. Port:

Dst. Address: 0.0.0.0/0

Dst. Port:

Protocol: **1 (icmp)**

Packet Mark

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

New Bridge Filter Rule

General | Advanced | ARP | STP | Action | Statistics

Action: **drop**

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove



Konfigurasi Console-Terminal

○ Mengaktifkan Protocol RSTP

- `/interface bridge set bridge1 protocol=rstp`

○ Membuat rule filtering ICMP apda bridge

- `/interface bridge filter add chain=forward
in-interface=ether3 out-interface=ether3
mac-protocol=ip dst-address=0.0.0.0/0
ip-protocol=tcp action=drop`

- ● ● | LAB Bridge (3)

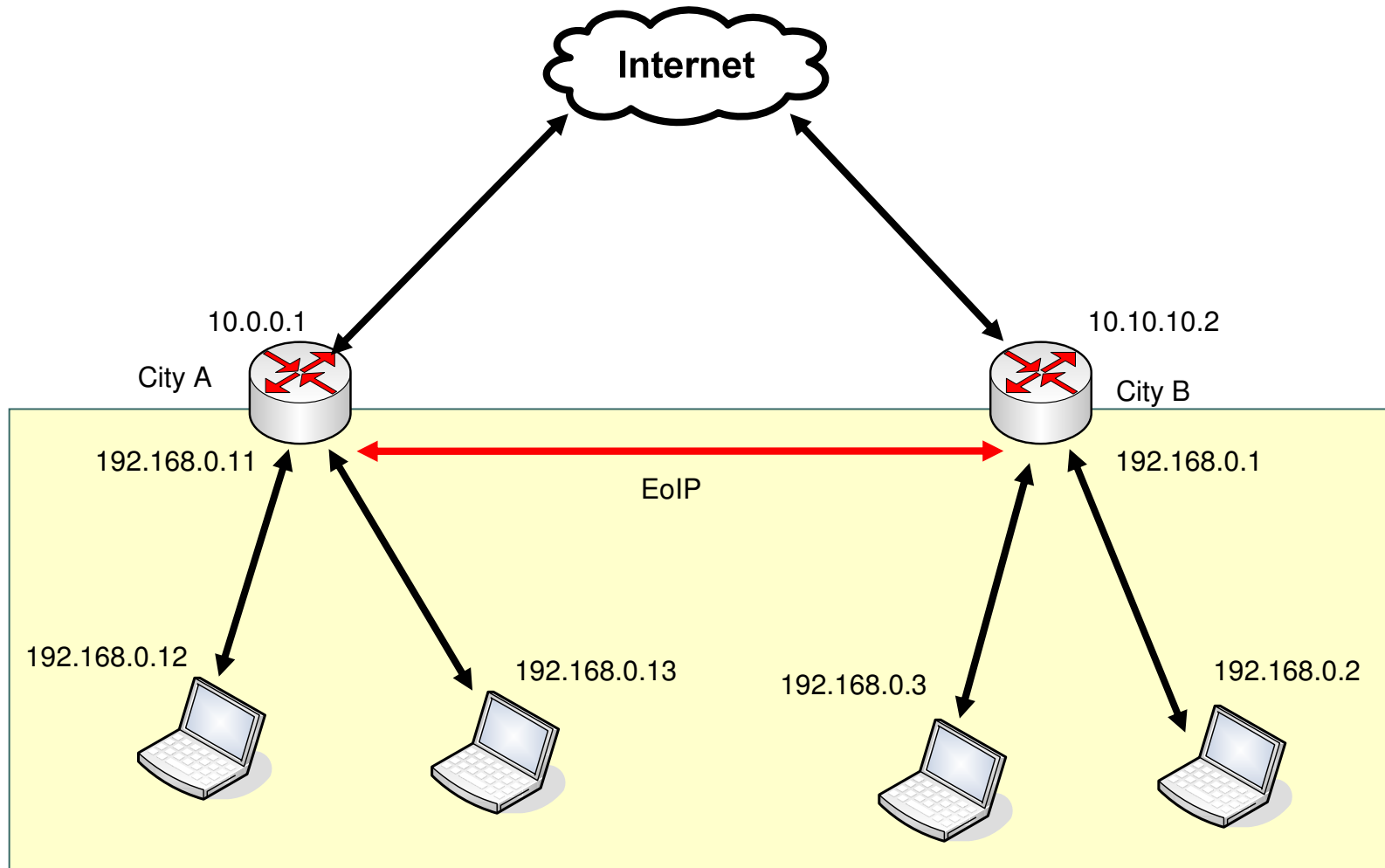
- Lakukanlah filtering ICMP / UDP pada bridge antar kedua belah laptop



Ethernet over IP (EoIP)

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

EoIP Example



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

EoIP Configuration

The screenshot displays a network configuration window titled "Interface List". The "EoIP Tunnel" tab is selected. A red circle highlights the "+" icon in the toolbar, and a red arrow points from it to the "EoIP Tunnel" entry in the list. A second red circle highlights the "EoIP Tunnel" entry in the list, with a red arrow pointing to the "Interface <eoip-tunnel1>" configuration dialog box.

The "Interface List" window shows a table of interfaces:

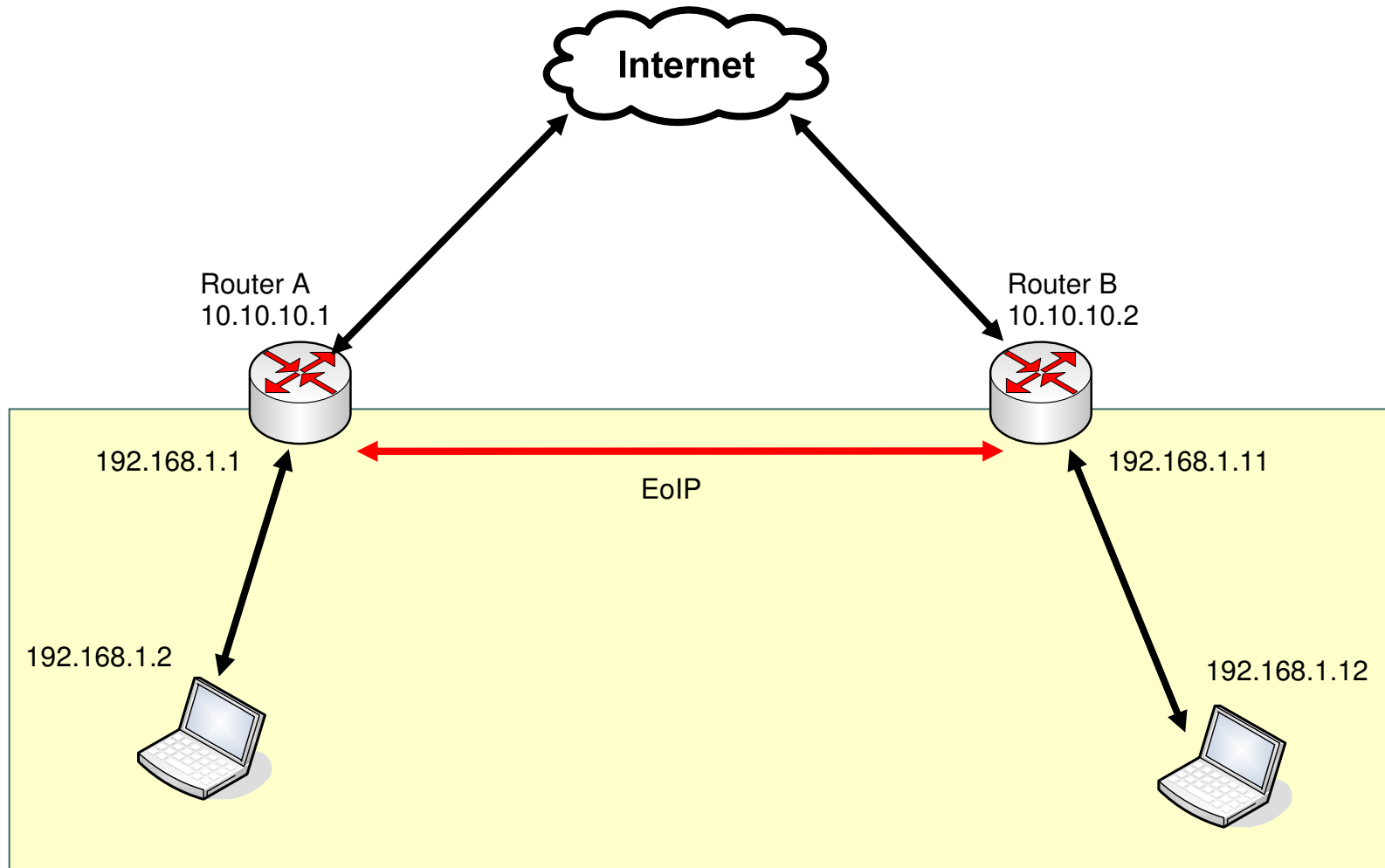
Interface	Type	Tx	Rx	Tx Pac...	Rx Pac...
EoIP Tunnel	Ethernet	0 bps	0 bps	0	0
IP Tunnel	Ethernet				
VLAN	Ethernet				
VRRP	Ethernet				
Bonding	Ethernet				
Bridge	Ethernet				
VPLS					
PPP Server					
PPP Client					
PPTP Server					
PPTP Client					
L2TP Server					
L2TP Client					
OVPN Server					
OVPN Client					
PPPoE Server					
PPPoE Client					
ISDN Server					
ISDN Client					

The "Interface <eoip-tunnel1>" dialog box shows the following configuration:

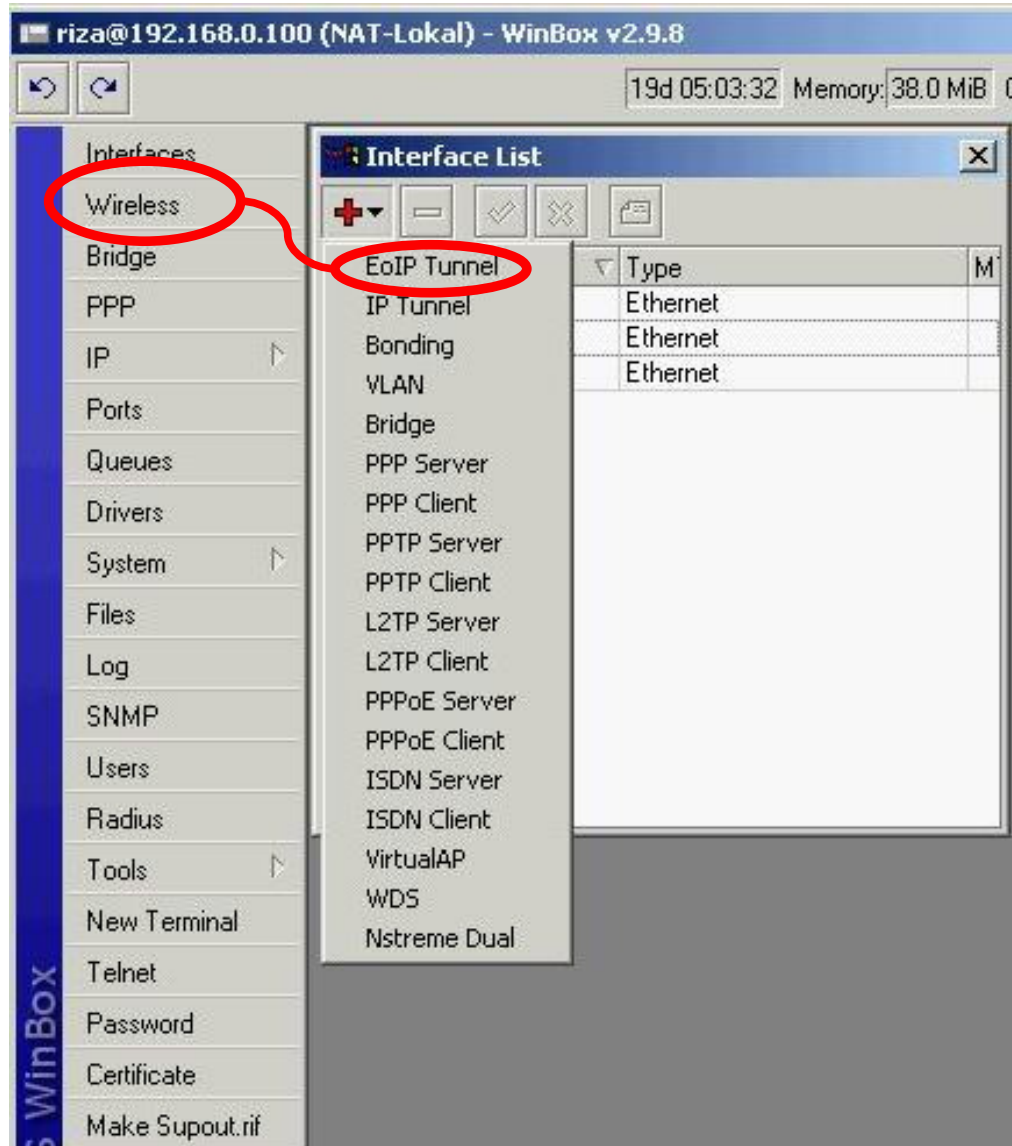
- Name: eoip-tunnel1
- Type: EoIP
- MTU: 1500
- MAC Address: FE:00:90:31:CF:95
- ARP: enabled
- Remote Address: 202.65.112.10
- Tunnel ID: 0

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove. Status: disabled, running.

[LAB] EoIP Tunnels



[LAB] EoIP Tunnels



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



[LAB] EoIP Tunnels

ROUTER A

ROUTER B

New Interface [X]

General Traffic [OK] [Cancel] [Apply] [Disable] [Comment] [Copy] [Remove] [Torch]

Name: eoip-tunnel1

Type: EoIP Tunnel

MTU: 1500

MAC Address: 02:FA:E2:81:F0:49

ARP: enabled [v]

Remote Address: 10.10.10.30

Tunnel ID: 0

disabled running slave

New Interface [X]

General Traffic [OK] [Cancel] [Apply] [Disable] [Comment] [Copy] [Remove] [Torch]

Name: eoip-tunnel1

Type: EoIP Tunnel

MTU: 1500

MAC Address: 02:FA:E2:81:F0:50

ARP: enabled [v]

Remote Address: 10.10.10.31

Tunnel ID: 0

disabled running slave



Wireless Concept

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

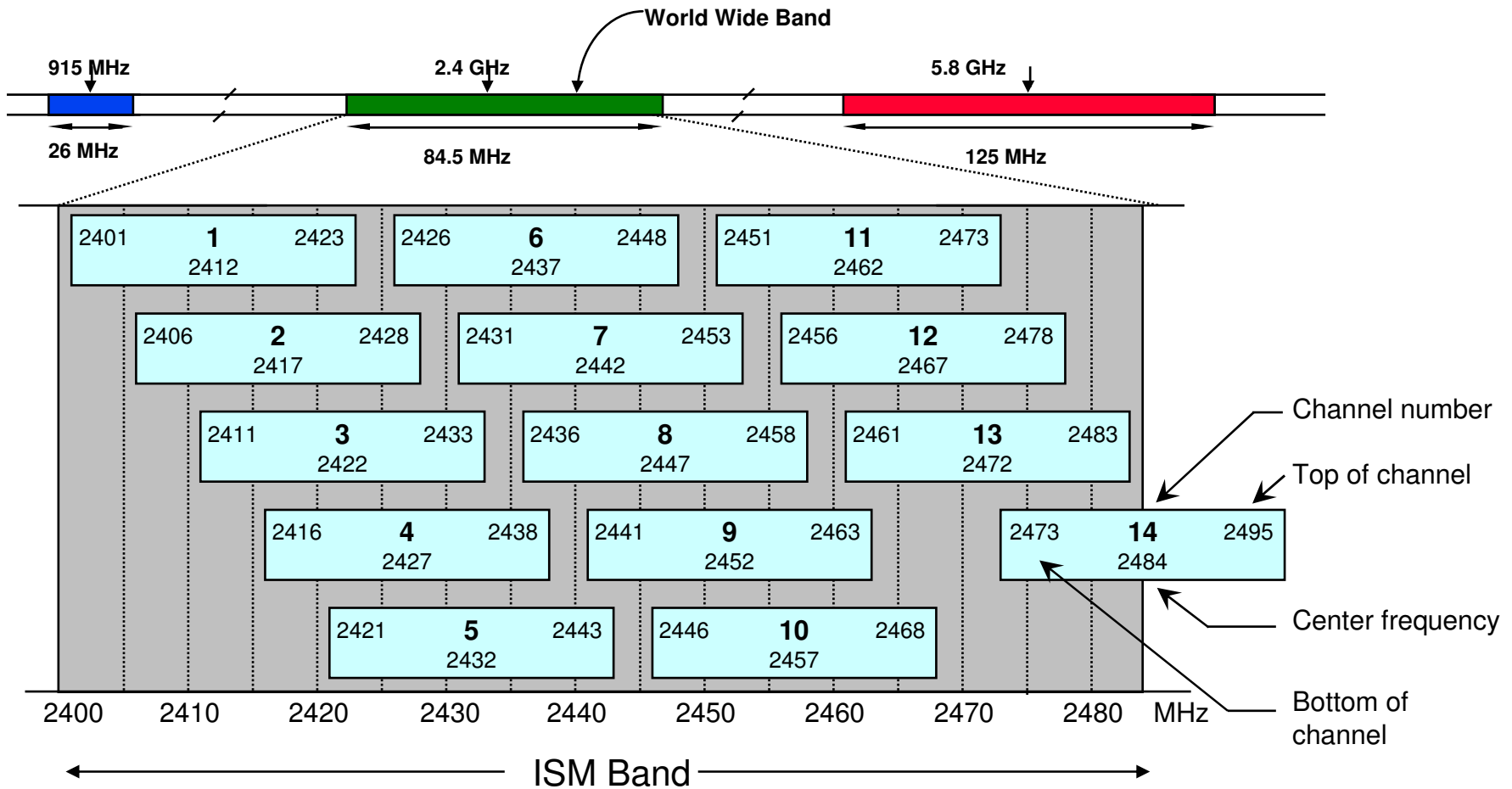


Kemudahan WirelessLAN

- Wireless LAN cukup mencengangkan dunia perkomputeran, karena berbagai kemudahan bisa kita dapatkan untuk menyambung dua atau lebih titik komputer :
 - Tidak perlu menarik kabel
 - Perangkatnya bisa di geser-geser semauanya
 - Pemeliharaan jaringan relatif lebih mudah
 - Rancangan tempat bisnis bisa sangat fleksibel
 - Mengikuti tren

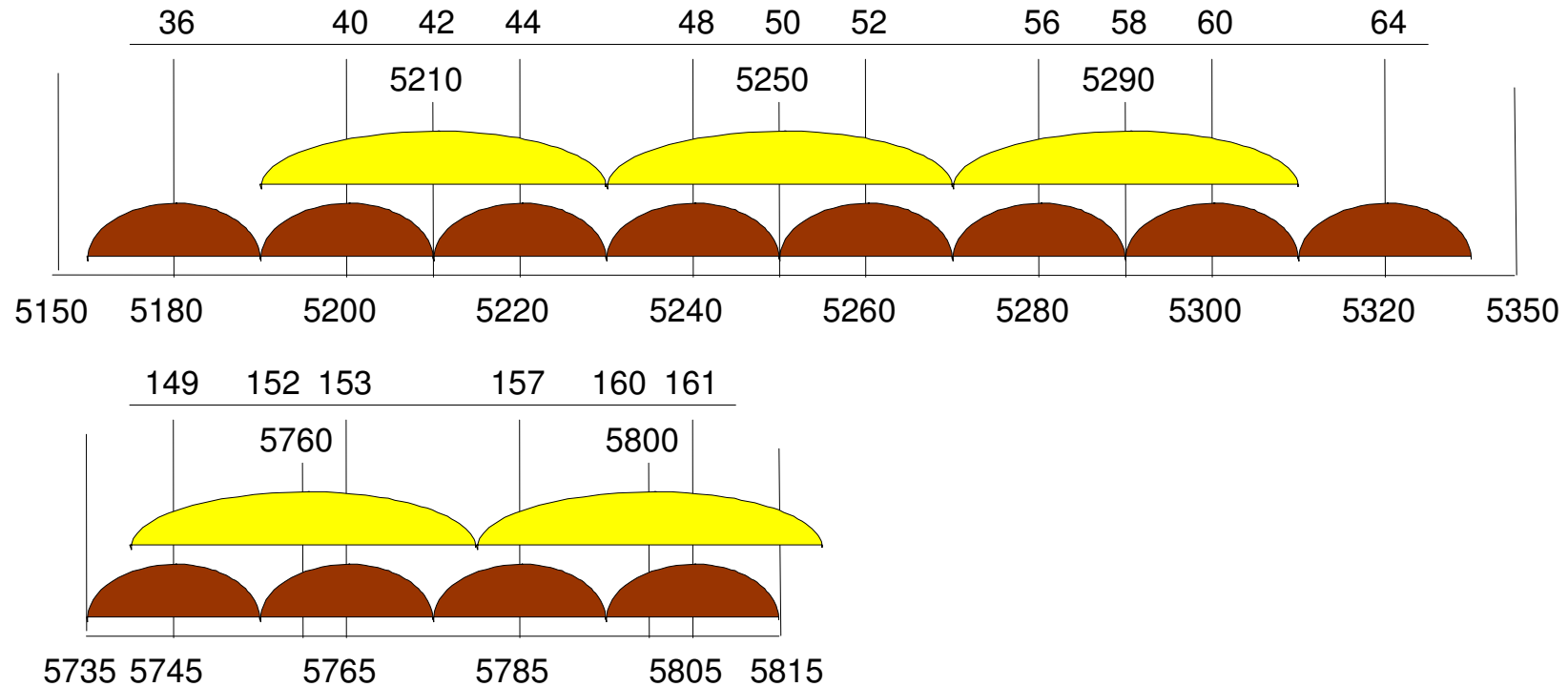


Channels 80211b





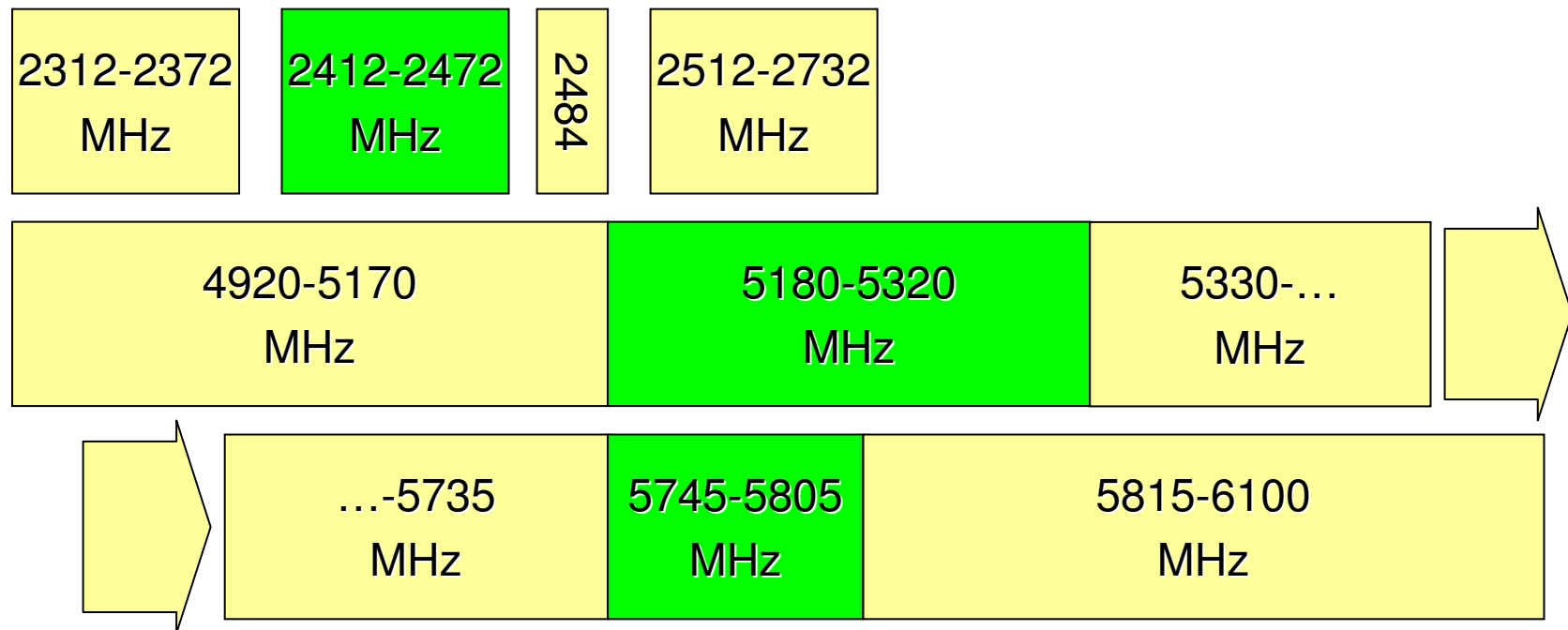
Channels 80211a



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

● ● ● | Custom Frequencies

- MikroTik RouterOS supports ISM Band and 'custom' frequencies for Atheros cards:



Spectrum Analyzer

- Perangkat Spectrum Analyzer untuk melihat bentuk dan posisi sinyal frekwensi tinggi



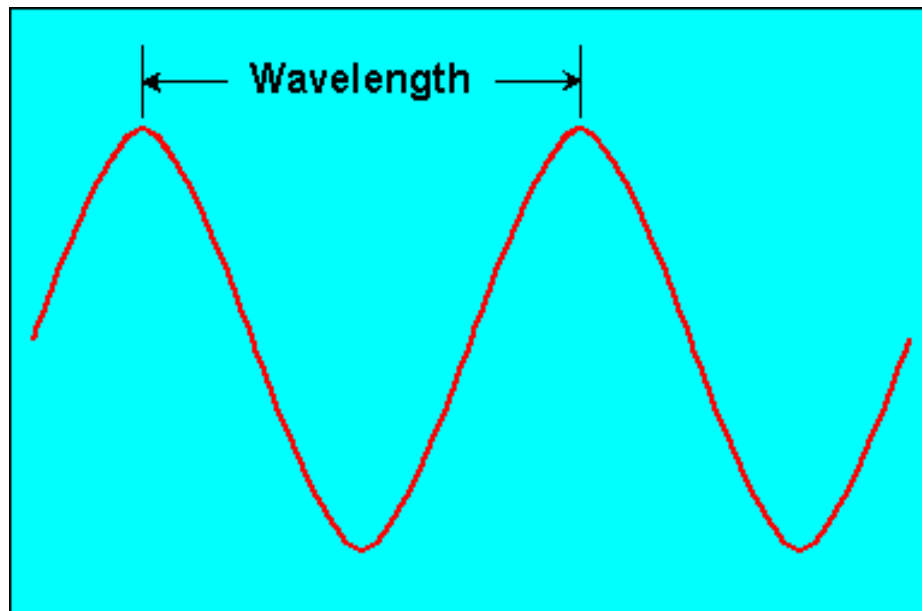
- ● ● | **Kaidah dalam WirelessLAN**

- Frequency dan Wavelength
 - Tx Power
 - Rx Sensivity
 - Looses
 - EIRP
 - Free Space Loss (FSL)
 - Line of Sight
 - Fresnel Zone
-



Wavelength

- Panjang Gelombang atau Wavelength adalah jarak diantara kedua titik yang sama pada satu getaran. Dalam sistem wireless, biasanya diukur dalam satuan meter, sentimeter atau milli meter



● ● ● | Frequency dan Wavelength

Frequency dan Wavelength digambarkan dalam persamaan :

$$\lambda = \frac{c}{f}$$

dimana :

λ = wavelength dalam meters

f = frequency dalam Hertz (getaran/detik)

c = kecepatan cahaya (3×10^8 meter/detik)



Panjang Gelombang 2,4 GHz

- o Contoh perhitungan panjang gelombang (wavelength) untuk frekwensi 2,4GHz :

$$\lambda = \frac{3 \times 10^8 \text{ m/s}}{2,4 \times 10^9 \text{ Hz}}$$

$$\lambda = 0,125 \text{ meter}$$

- o Jadi panjang gelombang-nya hanya 12,5 cm



Tx Power

- Radio mempunyai daya untuk menyalurkan sinyal pada frekwensi tertentu, daya tersebut disebut Transmit (Tx) Power dan dihitung dari besar energi yang disalurkan melalui satu lebar frekwensi (bandwidth)
 - Misalnya, satu radio memiliki Tx Power +18dBm, maka jika di konversi ke Watt akan didapat 0,064 W atau 64 mW.
-

● ● ● | Perhitungan db - mWatt

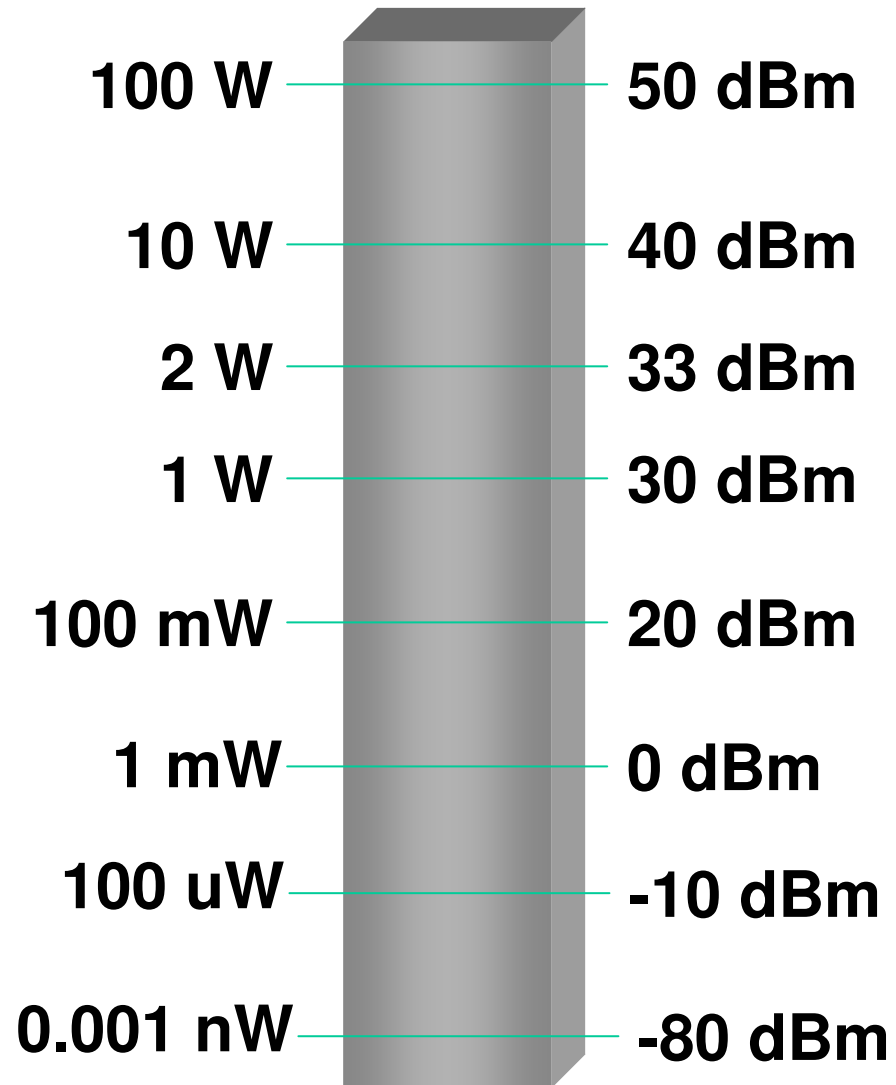
- dBm adalah nilai $10 \log$ dari sinyal untuk 1 milli Watt
- dBW adalah nilai $10 \log$ dari sinyal untuk 1 Watt
- Sinyal 100 milli Watt jika dijadikan dBm akan menjadi :

$$10 \log \frac{100 \text{ mW}}{1 \text{ mW}} = 20 \text{ dBm}$$



Watts vs dbm

Setiap kenaikan atau kehilangan 3 dB, kita akan mendapatkan dua kali lipat daya atau kehilangan setengahnya .





Rx Sensivity

- Semua radio memiliki point of no return, yaitu keadaan dimana radio menerima sinyal kurang dari Rx Sensitivity yang ditentukan, dan radio tidak mampu melihat data-nya
 - Misalnya, 802.11b mempunyai Received Sensitivity of -76 dBm, maka pada level ini, Bit Error Rate (BER) dari 10^{-5} (99.999%) akan terlihat.
 - Rx Sensitivity yang sebetulnya dari radio akan bervariasi tergantung dari banyak faktor.
-

Effective Isotropic Radiated Power (EIRP)

- Adalah daya pancar total perangkat setelah diperhitungkan dengan antenna dan gangguan lainnya.
- $EIRP = \text{dbm Alat} + \text{dbi Antenna} - \text{Losses}$
- Losses dapat diakibatkan konektor, kabel pigtail, dll

- ● ● |

Losses Kabel

- Kehilangan daya pada setiap 100 feet (30 meter) kabel untuk frekuensi 2,4 GHz
 - RG8 : 10
 - LMR400 : 6,8
 - LMR600 : 5,4
 - Heliax 3/8" : 5,36
 - Heliax 1/2" : 3,74
 - Heliax 5/8 : 2,15

● ● ● | Free Space Loss

- Rambatan frekuensi di udara akan mengalami loss, yang dapat dihitung dengan rumus:

$$\text{FSL(dB)} = 32.45 + 20 \text{ Log}_{10} F(\text{MHz}) + 20 \text{ Log}_{10} D(\text{km})$$

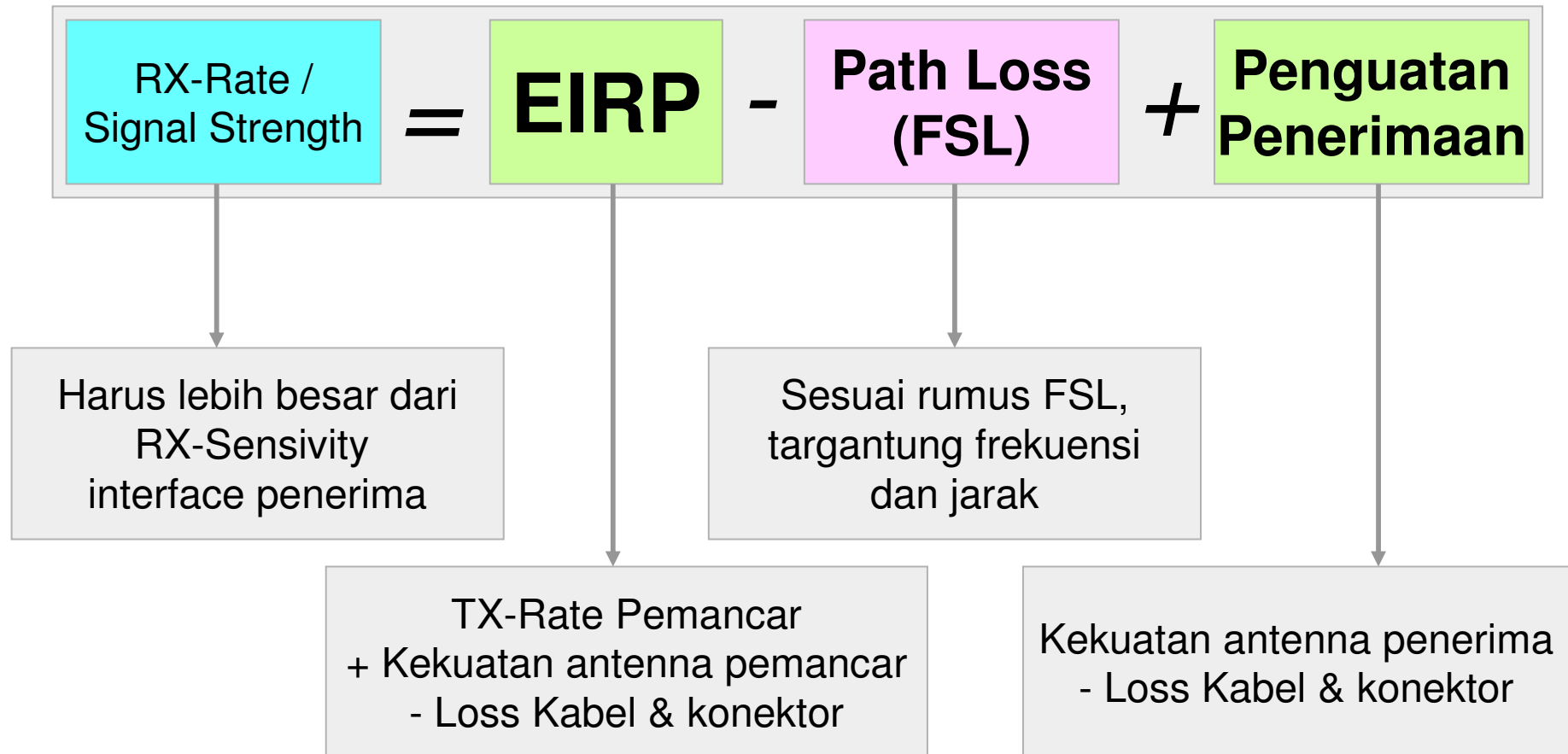
- Jadi Free Space Loss pada jarak 1 km yang menggunakan frekwensi 2.4 GHz :

$$\begin{aligned} \text{FSL(dB)} &= 32.45 + 20 \text{ Log}_{10} (2400) + 20 \\ &\quad \text{Log}_{10} (1) \\ &= 32.45 + 67.6 + 0 \\ &= 100.05 \text{ dB} \end{aligned}$$

● ● ● | **Tabel FSL (db)**

Jarak	2.4 GHz	5.2 GHz	5.8 GHz
1 km	100.026	106.742	107.69
3 km	109.568	116.284	117.233
5 km	114.005	120.721	121.670
10 km	120.026	126.742	127.690
15 km	123.548	130.264	131.212
20 km	126.047	132.762	133.711
30 km	129.568	136.284	137.233
40 km	132.067	138.783	139.732

Perhitungan RX-Rate





Perhitungan RX-Rate

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



Perhitungan

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

Online Calculator

Link Possibility Calculator

Parameters	SITE 1	SITE 2
Wireless cards		
Power	<input type="text" value="65"/> mW	<input type="text" value="65"/> mW
RX Sensitivity	<input type="text" value="-90"/> dBm	<input type="text" value="-90"/> dBm
Antennas		
Gain	<input type="text" value="24"/> dBi	<input type="text" value="24"/> dBi
Cables		
Length	<input type="text" value="3"/> m	<input type="text" value="3"/> m
Type:	<input type="text" value="LMR400"/>	<input type="text" value="LMR400"/>
Link		
Distance	<input type="text" value="10"/> km	
Frequency	<input type="text" value="2400"/> MHz	

Calculate

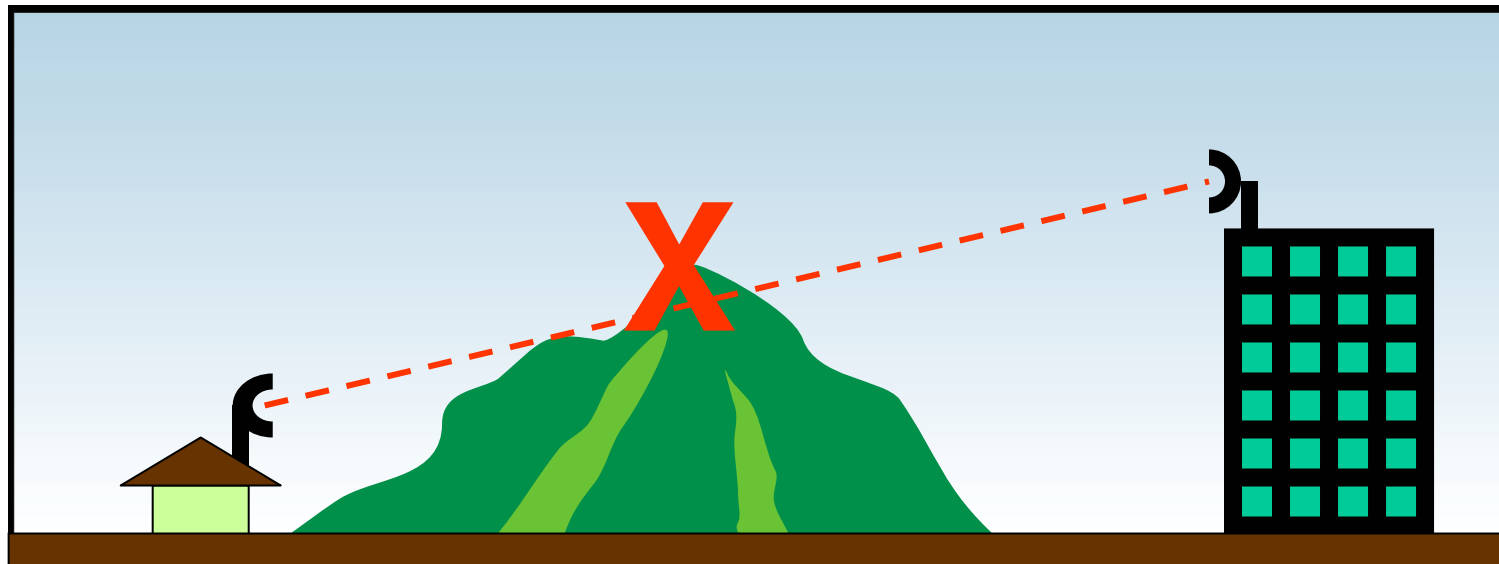
Link theoretical status	reliable
Theoretical signal level at site 1	-56/required -90
Theoretical signal level at site 2	-56/required -90

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

- ● ● |

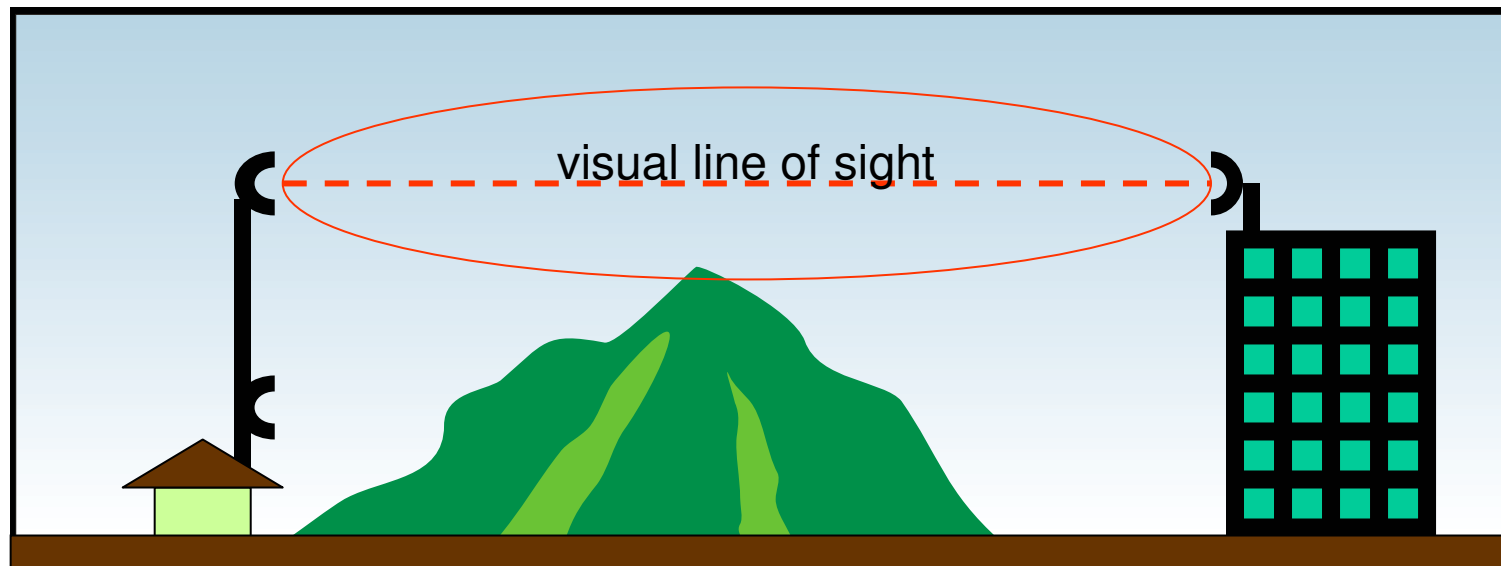
Line of Sight (LOS)

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



Line of Sight (LOS)

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



Ketinggian alat harus disesuaikan untuk mencapai line of sight



Fresnel Zone

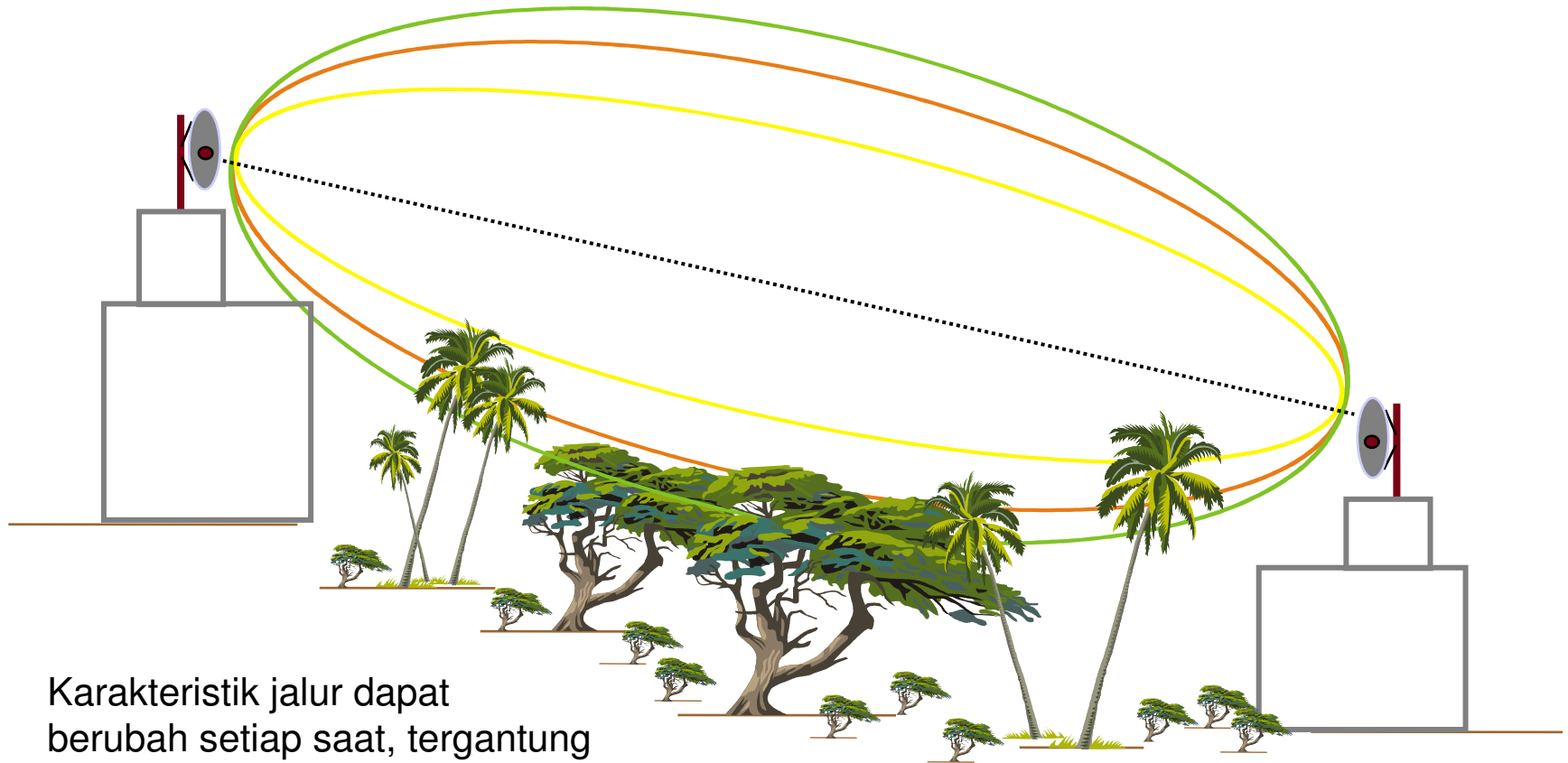
- Adalah area di sekitar garis lurus antar antenna yang digunakan sebagai media rambat frekuensi
 - Secara ideal, fresnel zone harus terpenuhi
 - 20% gangguan fresnel zone akan sedikit mempengaruhi kualitas link, namun lebih dari itu, akan sangat mempengaruhi
 - Halangan fresnel zone dapat berupa bangunan, dan juga pepohonan (karena air pada daun akan menyerap signal)
-

• • • Untuk mendapatkan Fresnel Zone yang baik

- Meningkatkan letak posisi antena pada infrastruktur yang ada
 - Membangun infrastruktur yang baru sebagai contoh membangun sebuah tower, maka antena harus diletakkan setinggi mungkin pada tower tersebut
 - Menaikan ketinggian tower
 - Meletakkan posisi antena yang berbeda
 - Memotong rintangan yang dapat mengganggu RF seperti pohon, dll
-



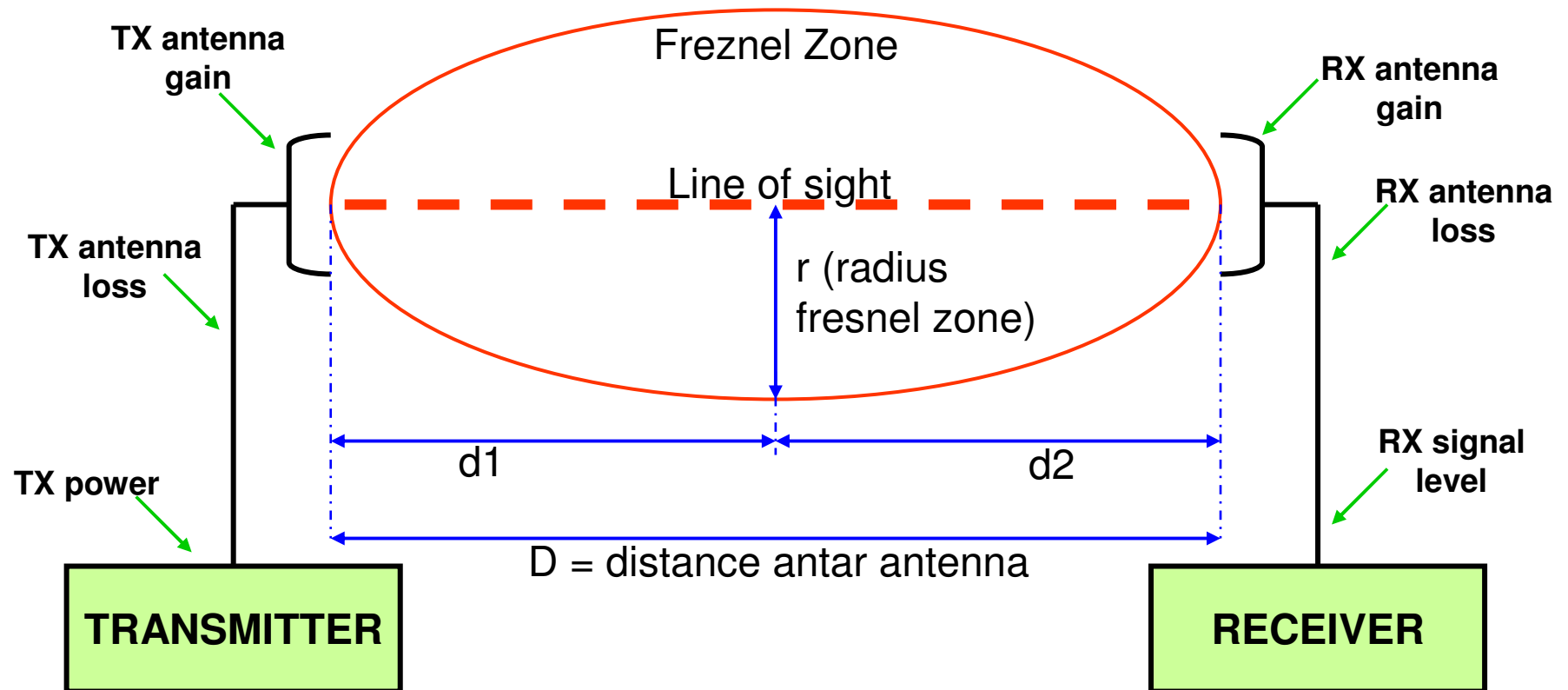
Fresnel Zone



Karakteristik jalur dapat berubah setiap saat, tergantung keadaan.

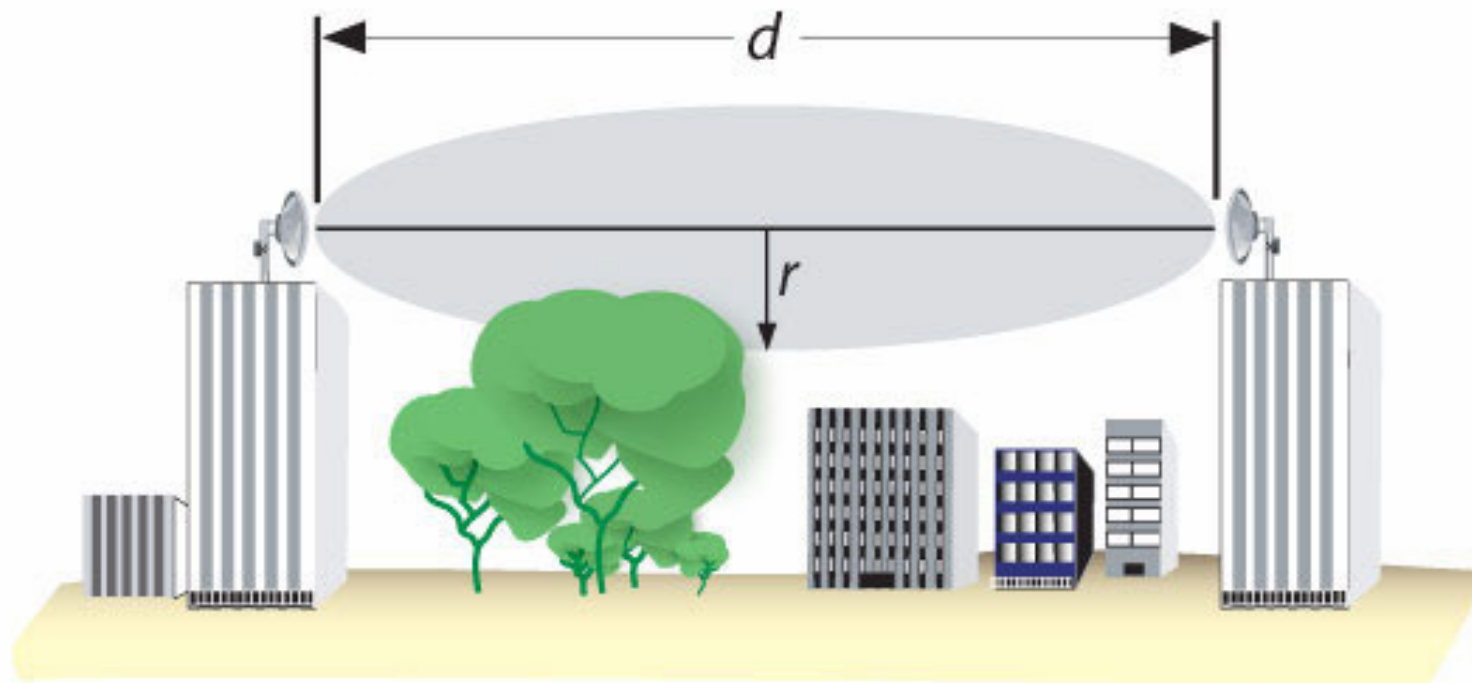
Freznel Zone

Selain Line of Sight juga memenuhi ketentuan Freznel Zone



Fresnel Zone Formula

- Perhitungan fresnel zone berdasarkan asumsi bumi yang datar



$$r_{(\text{in mts})} = 17.32 \times \sqrt{\frac{d_{(\text{in Km})}}{4f_{(\text{in GHz})}}}$$

$$r_{(\text{in ft})} = 72.05 \times \sqrt{\frac{d_{(\text{in miles})}}{4f_{(\text{in GHz})}}}$$

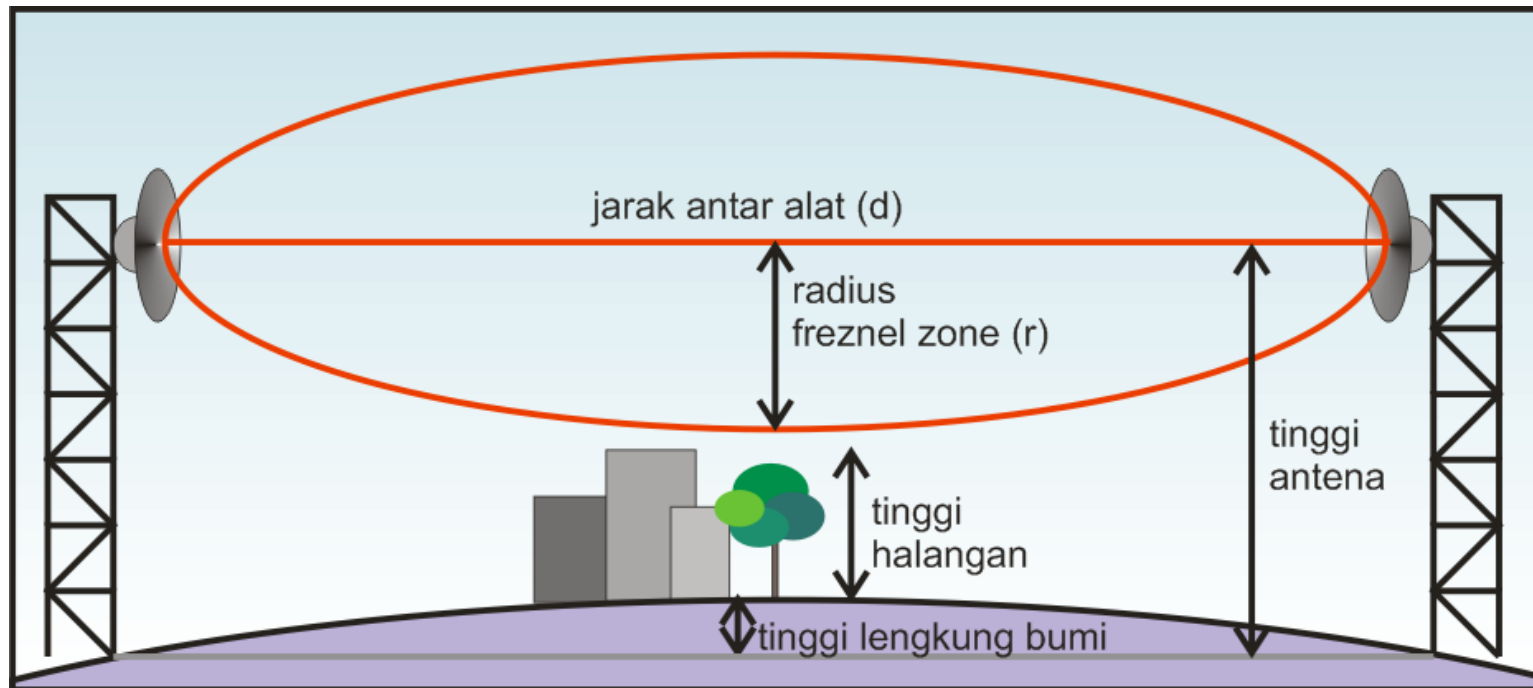
● ● ● | Fresnel Zone Calculation

- Frequency : 2.4 GHz ; Distance : 10 km

$$\begin{aligned} r \text{ (meter)} &= 17.32 * \sqrt{\frac{d \text{ (km)}}{4 f \text{ (GHz)}}} \\ &= 17.32 * \sqrt{\frac{10 \text{ (km)}}{4 * 2.4 \text{ (GHz)}}} \\ &= 17.32 * \sqrt{1.042} = 17.68 \text{ meter} \end{aligned}$$

● ● ● | Lengkung Bumi

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





Perhitungan Tinggi Antena

Masukkanlah Nilai Parameter berikut ini

Frekuensi : MHz
Jarak : km
Asumsi tinggi penghalang rata-rata : meter

Hasil Perhitungan

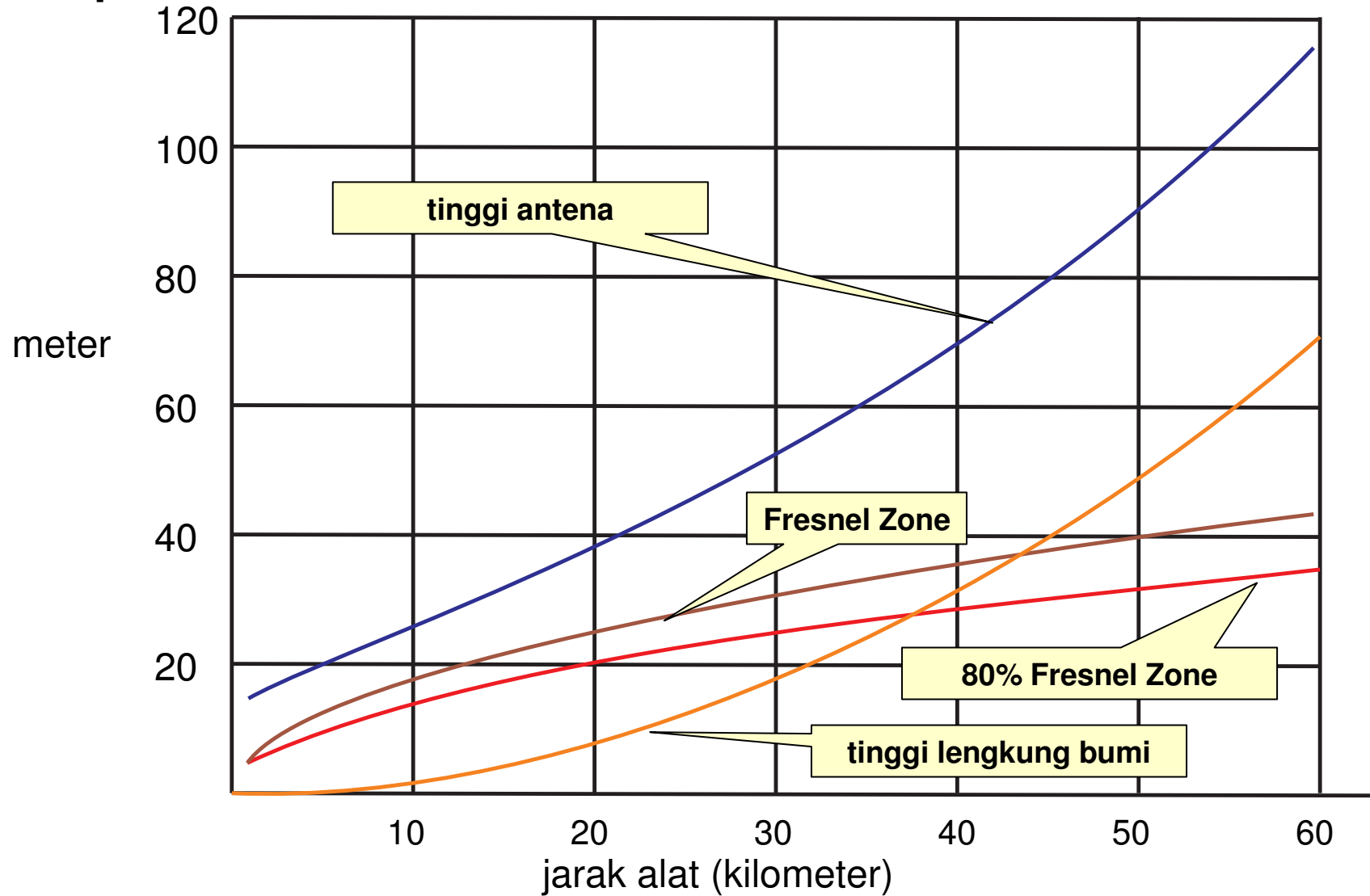
Jari-jari Fresnel Zone : 17.68 meter
80 % fresnel zone : 14.14 meter
Tinggi lengkung bumi : 1.96 meter
Tinggi antena minimum yang disarankan : 26.1 meter

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



Tinggi Antena

asumsi tinggi halangan 10 meter
frekuensi 2,4 GHz



GPS

- o Untuk mengukur ketinggian dan posisi pemasangan di dua titik, digunakan alat GPS (Global Positioning System)



- ● ● |

Antenna Concept

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



Antenna Type

- Omni Directional (3 – 15 db)
- Directional
 - Flat Panel (15 – 23 db)
 - Yagi
 - Grid (15 – 28 db)
 - Solid Disc (24 – 32 db)

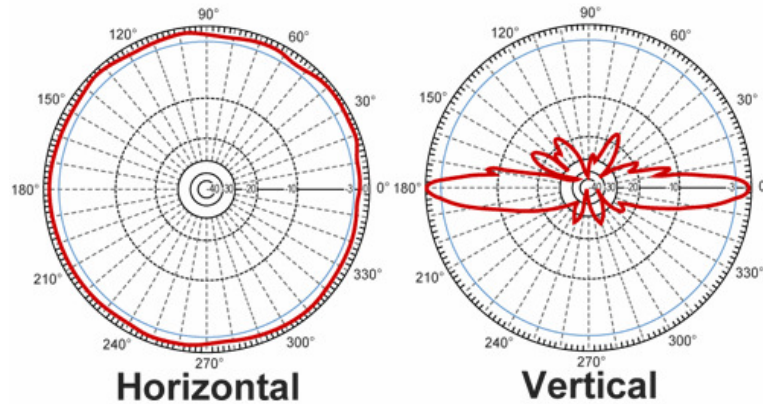
Pastikan antenna yang digunakan sesuai dengan frekuensi yang dipakai



Omni Directional

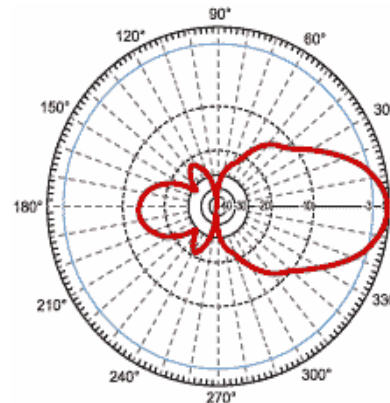
Frequency	2400-2500 MHz
Gain	15 dBi
Polarization	Vertical
Vertical Beam Width	8°
Horizontal Beam Width	360°
Impedance	50 Ohm
Max. Input Power	100 Watts
VSWR	< 1.5:1 avg.
Lightning Protection	DC Ground

Weight	3.3 lbs (1.5kg)
Length	40.5 in. (1.03m)
Base Diameter	1.69 in. (42.9mm)
Radome Diameter	1.52 in. (38.6mm)
Radome Material	Gray Fiberglass
Mounting	2.0" diameter mast max.
Wind Survival	up to 150 MPH
Operating Temperature	-40° C to to 85° C (-40° F to 185° F)
Connector	Integral N-Female

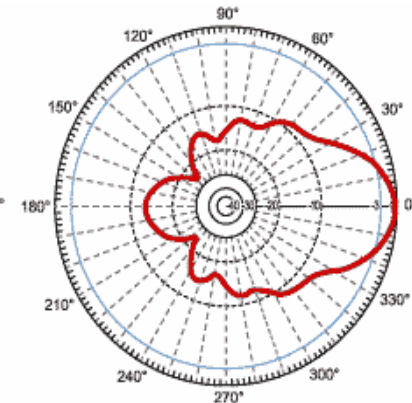




Yagi Antenna



Vertical



Horizontal

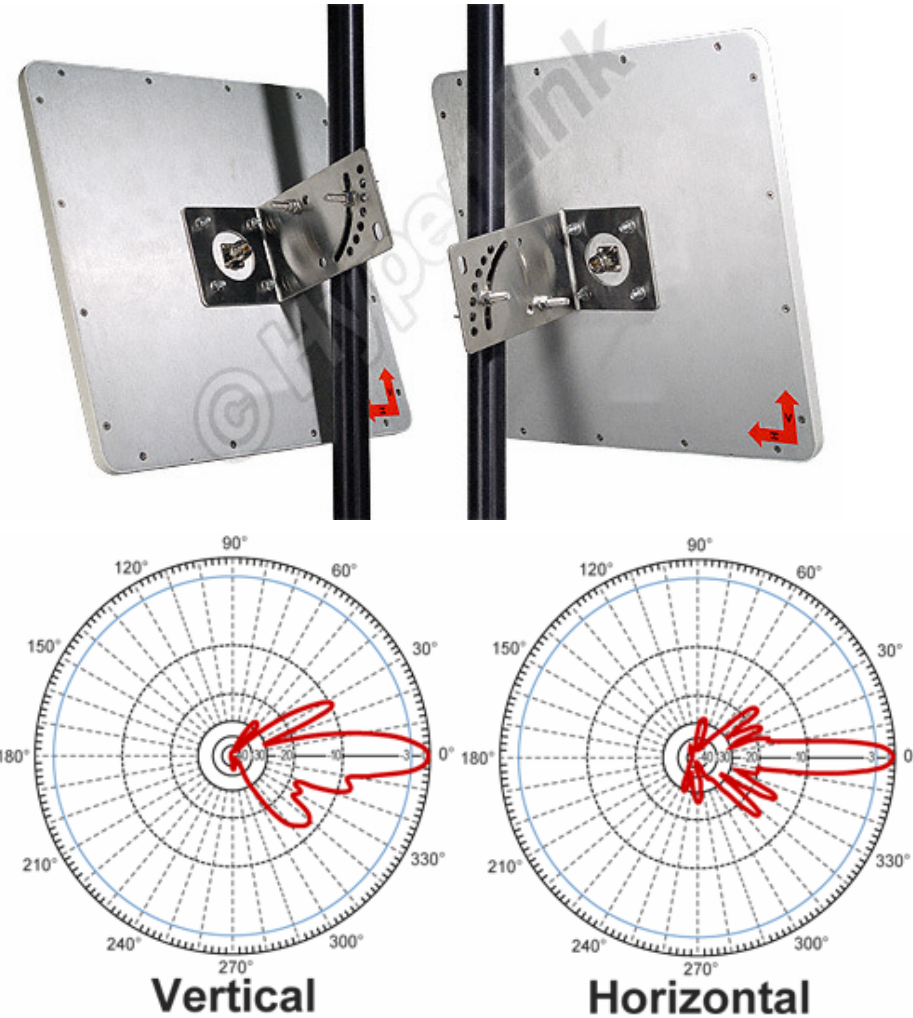
Frequency	2400-2500 MHz
Gain	14.5 dBi
-3 dB Beam Width	30 degrees
Impedance	50 Ohm
Max. Input Power	50 Watts
VSWR	< 1.5:1 avg.
Lightning Protection	DC Short

Weight	1.8 lbs. (.81 kg)
Dimensions Length x Diameter	18.2 x 3 (inches) 462 x 76 (mm)
Radome Material	UV-inhibited Polymer
Flame Rating	UL 94HB
Operating Temperature	-40° C to 85° C (-40° F to 185° F)
Mounting	1-1/4" (32 mm) to 2" (51 mm) dia. masts
Polarization	Vertical and Horizontal
Wind Survival	>150 MPH

Flat Panel Antenna

Frequency	5725-5850 MHz
Gain	22 dBi
Horizontal Beam Width	8°
Vertical Beam Width	8°
Polarization	Vertical or Horizontal
Front to Back Ratio	>25 dB
Impedance	50 Ohm
Max. Input Power	50 Watts
VSWR	< 1.5:1 avg.
Lightning Protection	DC Short
Connector	Integral N-Female

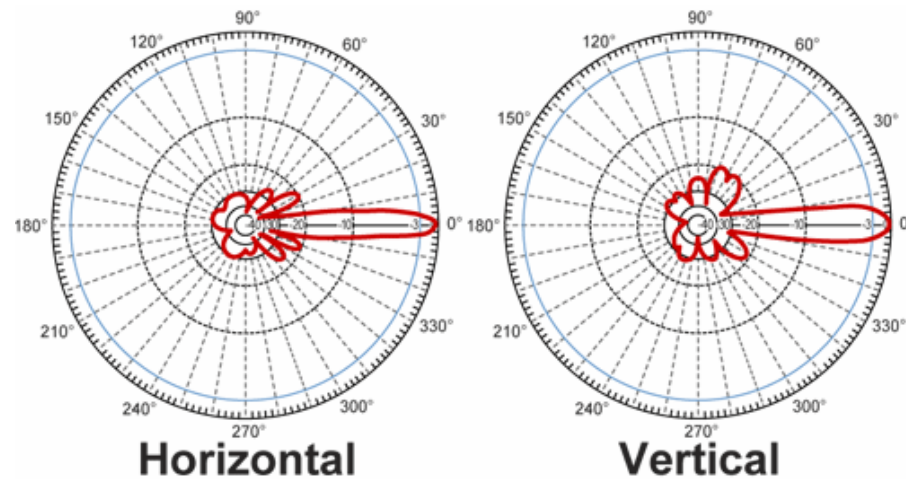
Weight	3.27 lbs. (1.5 Kg)
Dimensions	12 x 12 x .75 inches (305 x 305 x 19 mm)
Radome Material	UV-Stable Fiberglass
Operating Temperature	-40° C to to 85° C (-40° F to 185° F)
Mounting	1.25 inch (32 mm) to 3 inch (75 mm) O.D. pipe max.
Rated Wind Velocity	130mph (210km/h)



Grid Antenna



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



Solid Disc Antenna



Technical Specifications

Frequency Range:	5.725 - 5.850 GHz
Gain:	32.5 dBi (typical)
3 dB Beam Angle:	4°
Impedence:	50 OHM
VSWR:	1.5:1 (typical)
Side Lobe:	-28 dB (typical)
Cross Polarization:	-34 dB
Input Power:	100 W max
Input Return Loss:	-14 dBi
Connector:	N-type Female
Operating Temperature:	-40 °C to 70 °C

Antenna Diameter:	35.4 inches (900mm)
Pole Diameter:	1.5 - 3.0 inches
Antenna Weight:	22 lbs.
Wind Load	100MPH: 256 125MPH: 400 100MPH w/ 1/2" Radical Ice: 258
Front to Back:	38dB (minimum)

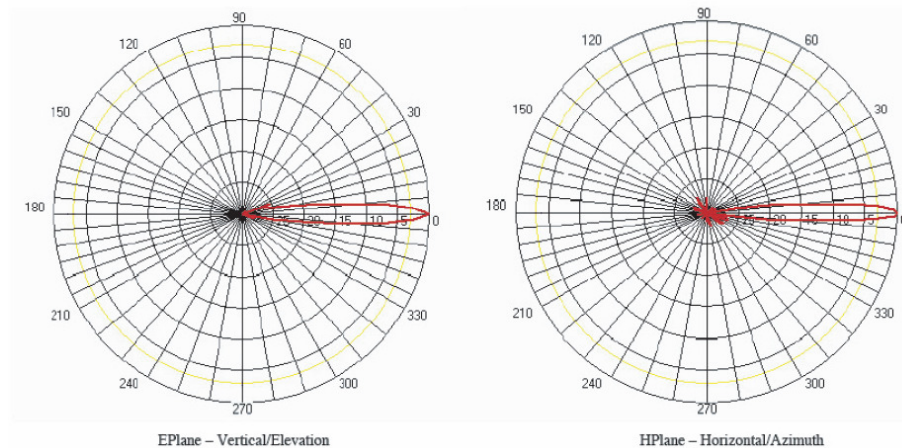
Features:

1. High Gain 32 dBi Antenna
2. Adjustable tilt pole mount
3. Vertical or Horizontal Polarization
4. Type N Female Connector

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

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

Antenna Patterns

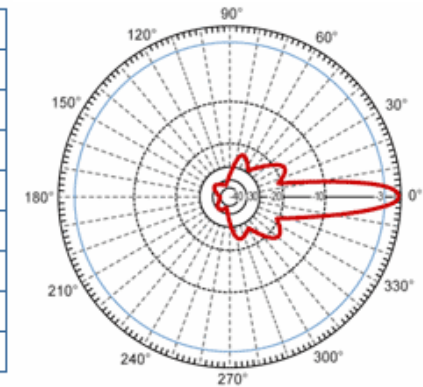


Sectoral Antenna

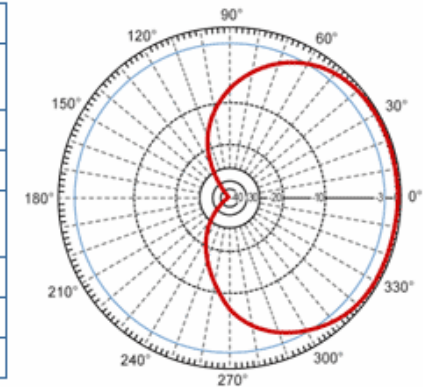


Frequency	2400-2500 MHz
Gain	20 dBi
Horizontal Beam Width	120 degrees
Vertical Beam Width	+/- 6.5°
Impedance	50 Ohm
Max. Input Power	250 Watts
VSWR	< 1.3:1 avg.
Connector	N Female
Lightning Protection	Direct Ground

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



Vertical



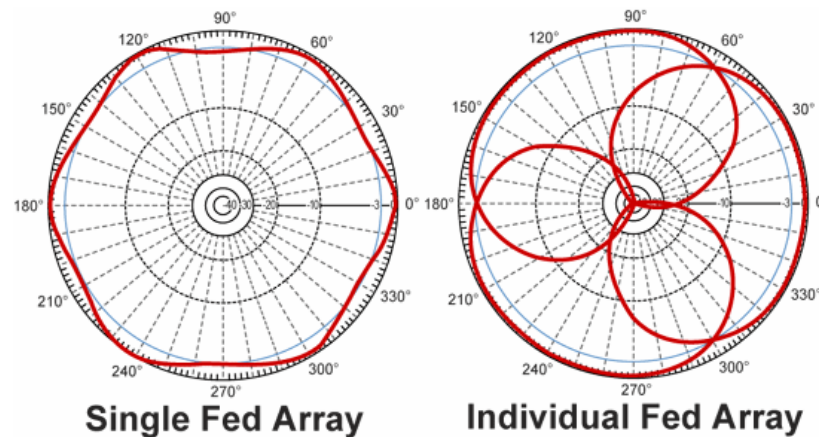
Horizontal

Sectoral Antenna (Array)



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

* Antenna gains specified when sectors are individually fed.



● ● ● | Instalasi Sectoral Antenna





PROTEKSI CUACA

- Cuaca akan sangat berpengaruh dalam sistem jaringan wireless maka perlu diperhatikan antara lain:
 - Konektor harus ditutupi untuk melindunginya dari kelembaban udara
 - Gunakanlah isolasi karet listrik atau bahan lain yang kekuatannya sama dengan selotip karet sebagai contoh 3M
 - Bahan Vinyl tidak bagus untuk perlindungan
-



Pastikan perangkat anda aman





Network Topology

- Point to Point
 - Dual Nstream
- Point to Multi Point
- WDS



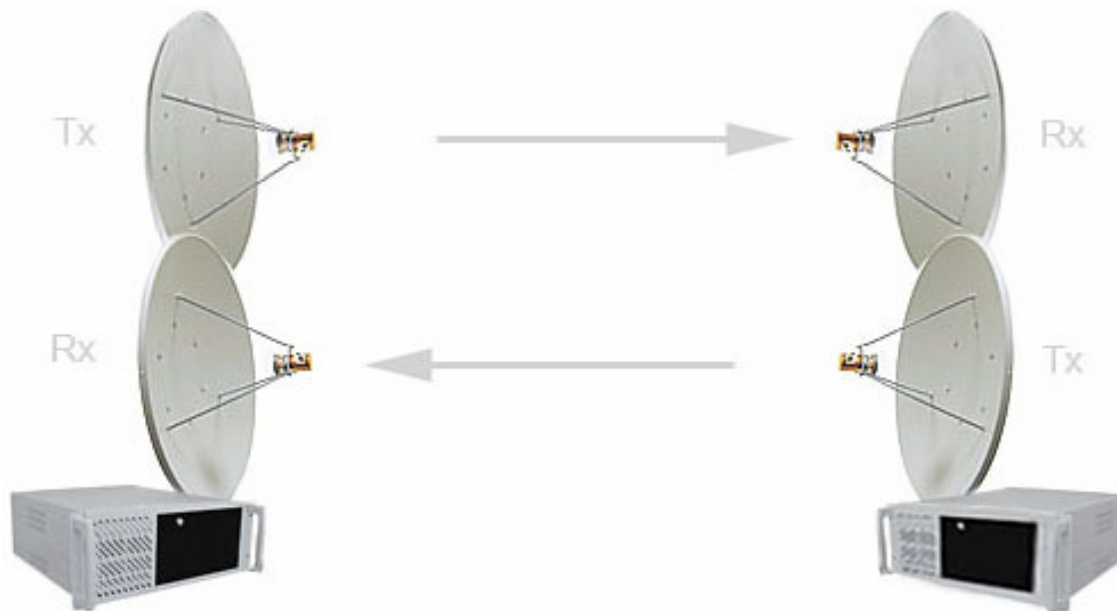
Point to Point

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



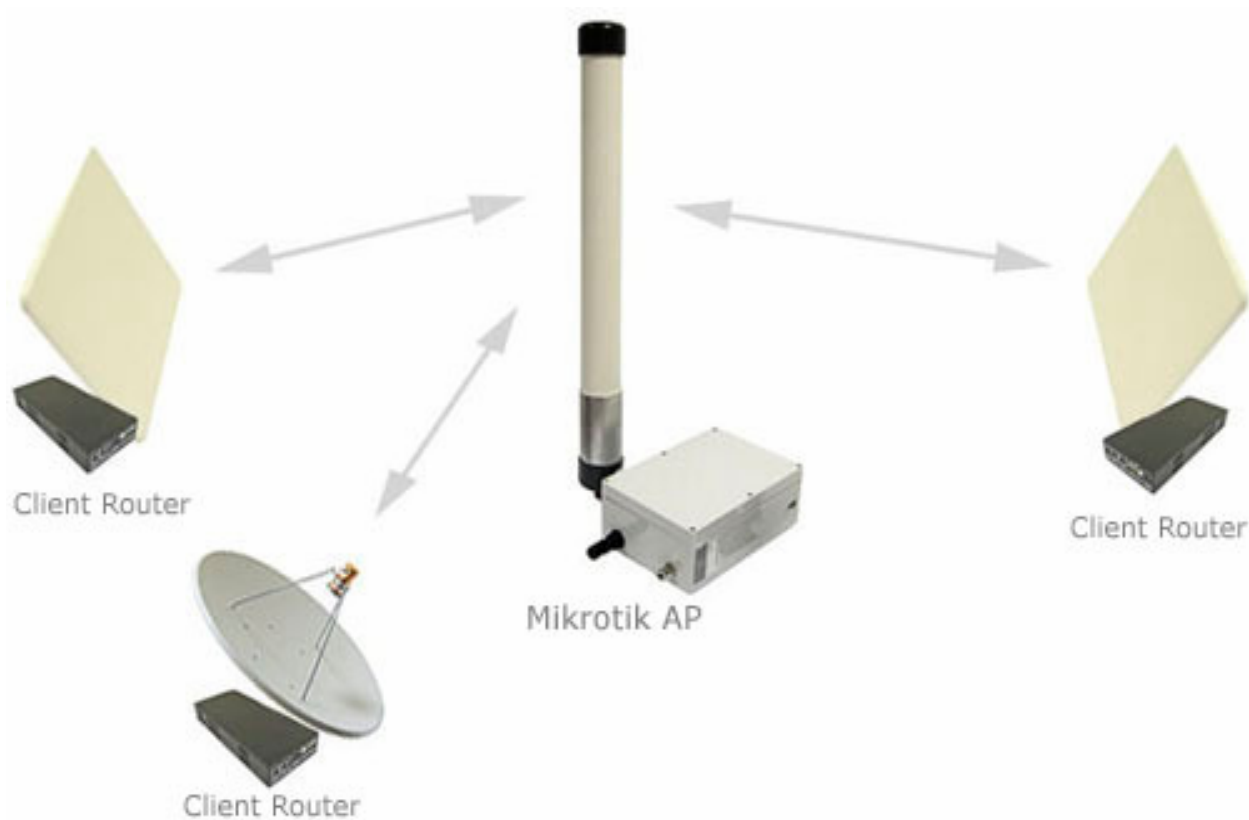
● ● ● | Point to Point (Dual Nstream)

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



● ● ● | Point to Multipoint

- 1 buah AP Mikrotik sebagai base station untuk melayani CPE



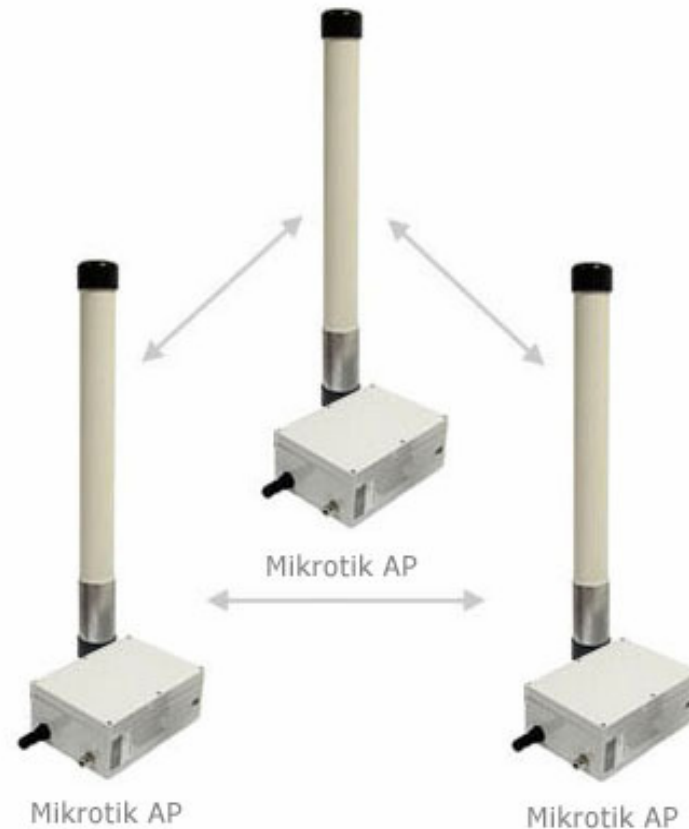


Point to Multipoint

- Antena bisa menggunakan Omnidirectional atau sectoral. Jika client berada di satu area, bisa menggunakan flat panel atau bahkan directional antenna. Perhatikan besaran bukaan antena.
- Gunakan standart 80211.b, supaya semua tipe CPE bisa terkoneksi.

Wireless Distribution System (WDS)

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



Wireless Distribution System (WDS)

- Cover large areas and allow users to move for large distances while still being on-line. This system allows packets to pass from one wireless AP (Access Point) to another, just as if the APs were ports on a wired Ethernet switch.
- APs must use the same standard (802.11a, 802.11b or 802.11g) and work on the same frequencies in order to connect to each other.

- ● ● |

Keamanan Wireless

- Hidden SSID
 - Disable Default Authenticate
 - MAC Address List
 - WEP
-



Wireless Configuration

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

Wireless Menu

- Wireless Sub-Menu:
 - **Nstreme-Dual** - list of Dual-Nstreme Interface
 - **Access-List** - list of associations of clients
 - **Registration** - list of connected clients
 - **Connect-List** - list of rules, that determine to which AP the station should connect to
 - **Security-Profile** – list of security functions to wireless interfaces WEP and WPA/WPA2



admin@00:0C:42:0E:A5:36 (router2) - WinBox v3.1 on RB500R5 (mipsle)

CPU: 5%

Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles

Find

Name	Type	Tx	Rx	MAC Address	ARP	Mode	Band	Fre...	SSID
X wlan1	Wireless (Atheros AR5413)			00:0C:42:1B:5C:81	enabled	station	5GHz	5180	MikroTik
R wlan2	Wireless (Atheros AR5413)	22.2 kbps	0 bps	00:0C:42:1B:5C:85	enabled	station pseudobridge	2.4GHz-B/G	2192	MikroTik

Wireless Interface Menu

Interface <wlan2>

General | **Wireless** | WDS | Nstreme | Status | ...

Mode: station pseudobridge
Band: 2.4GHz-B/G
Frequency: 2412 MHz
SSID: MikroTik
Scan List: 2400-2500
Security Profile: default
Antenna Mode: antenna a

Default AP Tx Rate: bps
Default Client Tx Rate: bps

Default Authenticate
 Default Forward
 Hide SSID
 Compression

Buttons: OK, Cancel, Apply, Disable, Comment, Torch, Scan..., Freq. Usage..., Align..., Sniff..., Snooper..., Reset Configuration, **Advanced Mode**

disabled | running | idle | connected to ess

Advance &
Simple Menu

Interface <wlan2>

General | **Wireless** | Data Rates | Advanced | WDS | ...

Mode: station pseudobridge
Band: 2.4GHz-B/G
Frequency: 2412 MHz
SSID: MikroTik
Radio Name: 000C421B5C6A
Scan List: 2400-2500
Security Profile: default

Frequency Mode: manual txpower
Country: no_country_set
Antenna Mode: antenna a
Antenna Gain: 0 dBi

DFS Mode: none
Proprietary Extensions: post-2.9.25
WMM Support: disabled

Default AP Tx Rate: bps
Default Client Tx Rate: bps

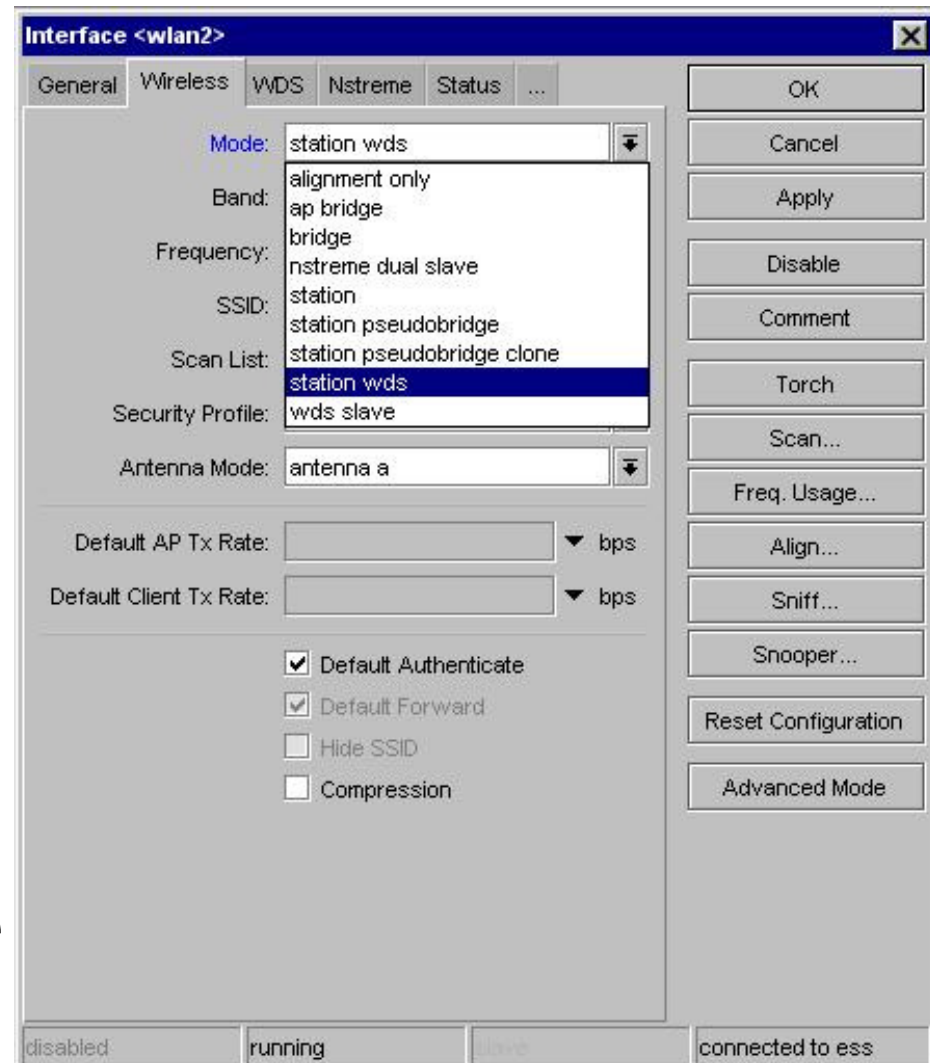
Default Authenticate
 Default Forward
 Hide SSID
 Compression

Buttons: OK, Cancel, Apply, Disable, Comment, Torch, Scan..., Freq. Usage..., Align..., Sniff..., Snooper..., Reset Configuration, **Simple Mode**

disabled | running | idle | connected to ess

● ● ● | Wireless Mode List

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



● ● ● | Wireless Mode - 1

- **alignment-only** - this mode is used for positioning antennas (to get the best direction)
- **ap-bridge** - the interface is operating as an Access Point
- **bridge** - the interface is operating as a bridge. This mode acts like ap-bridge with the only difference being it allows only one client
- **nstreme-dual-slave** - the interface is used for nstreme-dual mode
- **station** - the interface is operating as a client

● ● ● | Wireless Mode – 2

- **station-wds** - the interface is working as a station, but can communicate with a WDS peer
- **wds-slave** - the interface is working as it would work in ap-bridge mode, but it adapts to its WDS peer's frequency if it is changed
- **station-pseudobridge** - wireless station that can be put in bridge
- **station-pseudobridge-clone** - similar to the station-pseudobridge, but the station will clone MAC address of a particular device (set in the station-bridge-clone-mac property), i.e. it will change its own address to the one of a different device

● ● ● | Wireless Configuration

- Basic Configuration :
 - Point to Point
 - Point to Multi Point
 - Wireless Bridge
 - Virtual AP
- Advance Configuration :
 - Nstreme
 - Dual Nstreme
 - WDS



Point to Point

- AP Side

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

- Client Side

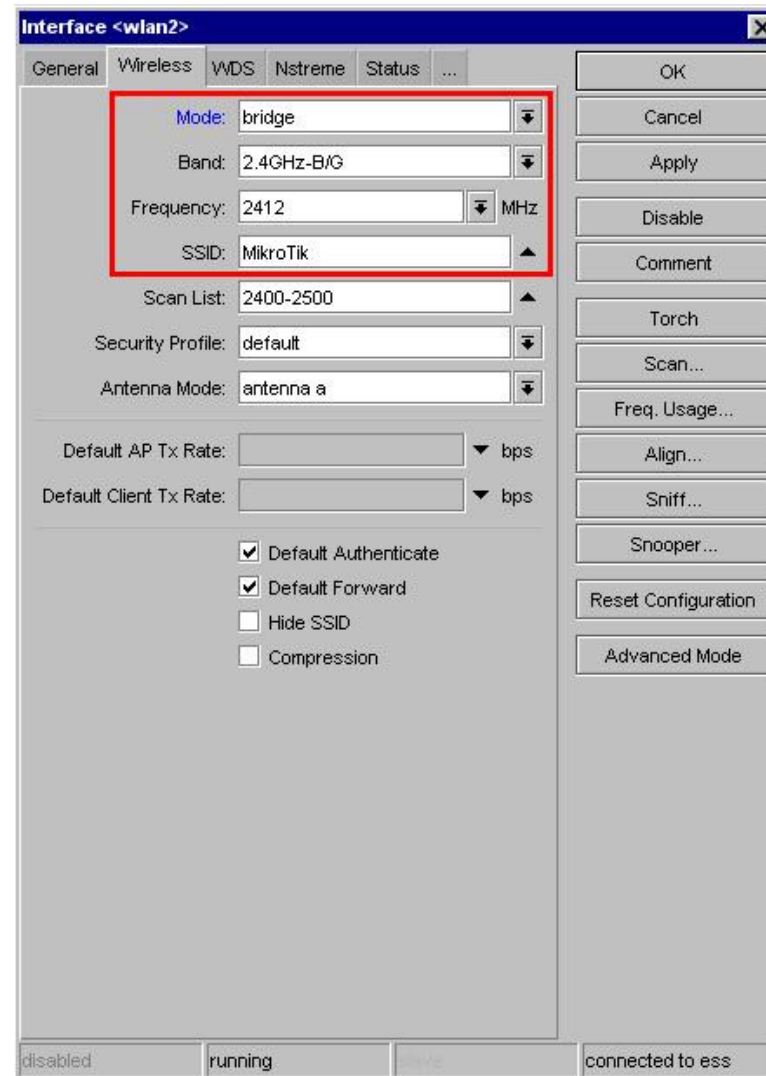
- Min Licence Level 3
- Set mode, ssid, band, scan-list
- mode=station
- Make sure frequency is in scan-list





Point to Point (AP Side)

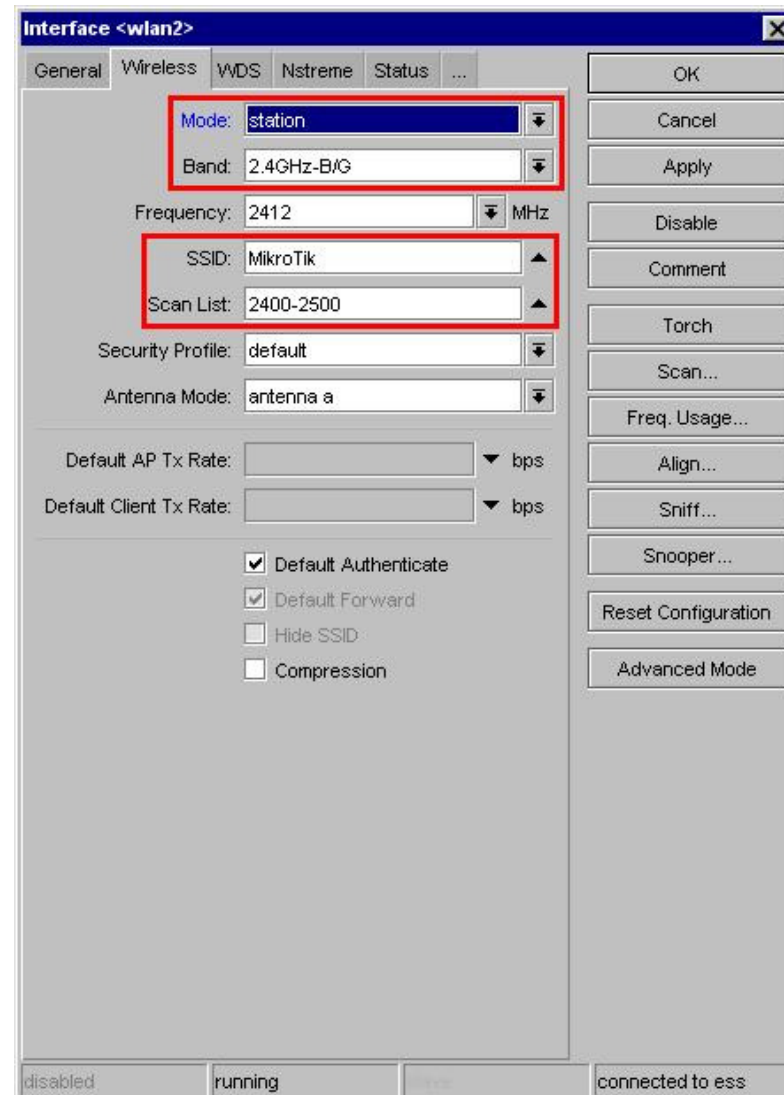
- Min Licence Level 3
- Set mode, ssid, band, frequency
- mode=bridge
 - Can serve only 1 station





Point to Point (Client Side)

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



● ● ● | [LAB] Point to Point

- Add IP Address to both router on wlan interface
- Try to ping from winbox to another router
- The router is ready for routed traffic, but not bridged. Wireless Station mode can't be bridge! it can be bridged using another mode in another chapter!

Configuration Console-Terminal - point-to-point

- Configuration AP Side
 - /interface wireless set wlan1 mode=bridge frequency=2412 band=2.4ghz-b/g ssid=meja1
- Configuration Client Side
 - /interface wireless set wlan1 mode=station band=2.4ghz-b/g scan-list=2400-2500 ssid=meja1

Monitoring Wireless Interface

- To Monitor the interface

The top screenshot shows the 'Wireless Tables' window in WinBox v3.1 on RB500R5 (mipsle). The 'Wireless' menu item is circled in red. The table below shows the following data:

Name	Type	Tx	Rx	MAC Address	ARP	Mode	Band	Fre...	SSID
wlan1	Wireless (Atheros AR5413)			00:0C:42:1B:5C:81	enabled	station	5GHz	5180	MikroTik
wlan2	Wireless (Atheros AR5413)	22.2 kbps	0 bps	00:0C:42:1B:5C:85	enabled	station pseudobridge	2.4GHz-B/G	2192	MikroTik

The bottom screenshot shows the 'Registration' tab in WinBox v3.2 on RB500R5 (mipsle). The 'Wireless' menu item and the 'Registration' tab are circled in red. A red box highlights the following registration entry:

Radio Name	MAC Address	Interface	Uptime	AP	W	Last Active	Signal Strength
000C421B...	00:0C:42:1B:5C:85	wlan2	02:10:42	yes	no	0.810	-13



Monitoring Wireless Interface

- To check connected client

Wireless Tables

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

[-] [Filter] [Reset] Find

Radio Name	MAC Address	Interface	Uptime	AP	iW...	Last Activi...	Signal Streng
000C421B...	00:0C:42:1B:5C:85	wlan2	02:11:47	yes	no	0.020	-10

Context Menu:

- Show Categories
- Detail Mode
- Inline Comments
- Show Columns
- Find (Ctrl+F)
- Find Next (Ctrl+G)
- Copy to Access List**
- Copy to Connect List
- Ping
- MAC Ping
- Telnet
- MAC Telnet
- Torch

Pilih client dan klik di sini untuk mendaftarkan mac-address

Monitoring Wireless Interface

- To check registered client

The screenshot shows the Mikrotik WinBox v3.2 interface. The left sidebar has a menu with 'Wireless' circled in red. The main window displays the 'Wireless Tables' window with the 'Access List' tab selected and circled in red. Below the tabs is a table with the following data:

#	MAC Address	Interface	Signal Str...	Authentication	Forwarding
0	00:0C:42:1B:5C:85	wlan2	-120..120	yes	yes

“Used only when Default Authenticated disabled”

Client Management

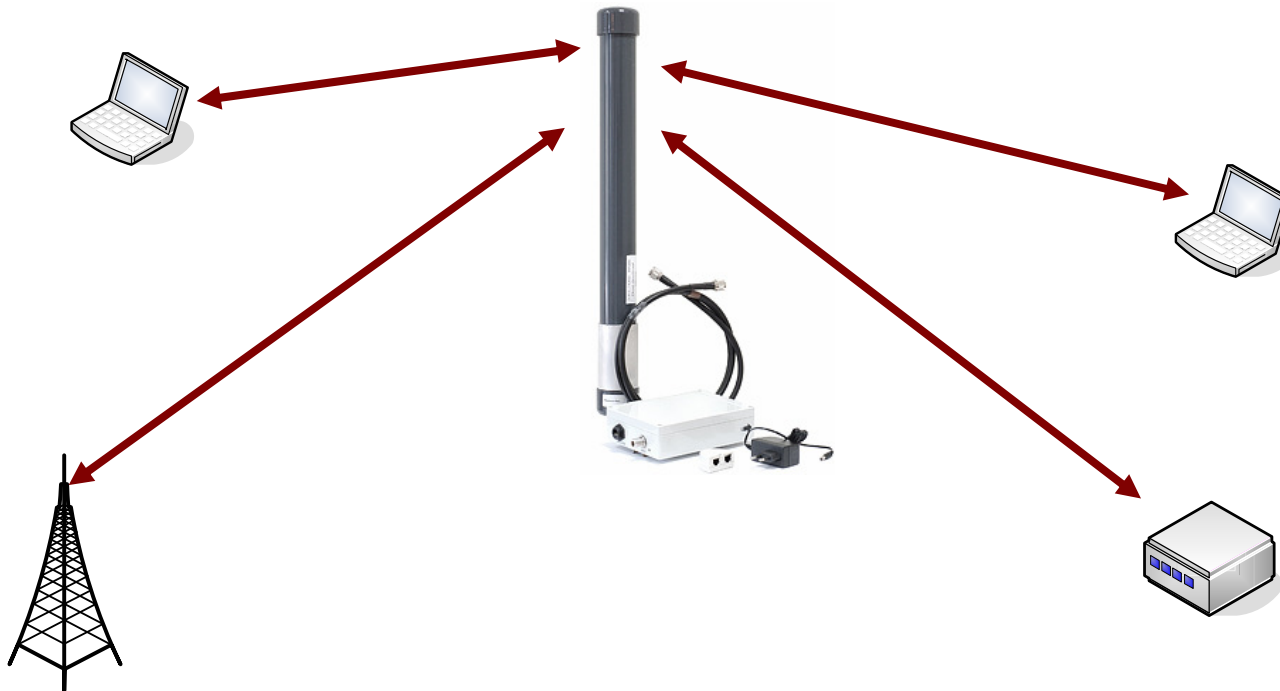
- Kita dapat melakukan pengaturan untuk setiap klien dan hal ini akan mengabaikan konfigurasi global

The screenshot shows the Mikrotik WinBox v3.2 interface. The left sidebar contains a menu with options: Interfaces, Wireless, Bridge, PPP, IP, Routing, Ports, Queues, Drivers, System, Files, Log, SNMP, Users, Radius, Tools, New Terminal, Telnet, Password, and Certificates. The main window displays the 'Wireless Tables' configuration page, which includes tabs for Interfaces, Nstreme Dual, Access List, Registration, Connect List, and Security Profiles. A table lists wireless clients with columns for #, MAC Address, Interface, Signal Str..., and Authentication. One entry is visible: # 0, MAC Address 00:0C:42:1B:5C:85, Interface wlan2, Signal Str... -120..120, and Authentication yes. Below the table, the 'AP Access Rule <00:0C:42:1B:5C:85>' configuration window is open, showing fields for MAC Address (00:0C:42:1B:5C:85), Interface (wlan2), and Signal Strength Range (-120..120). It also includes checkboxes for Authentication and Forwarding, and a Private Key field set to none. The status at the bottom is 'disabled'.



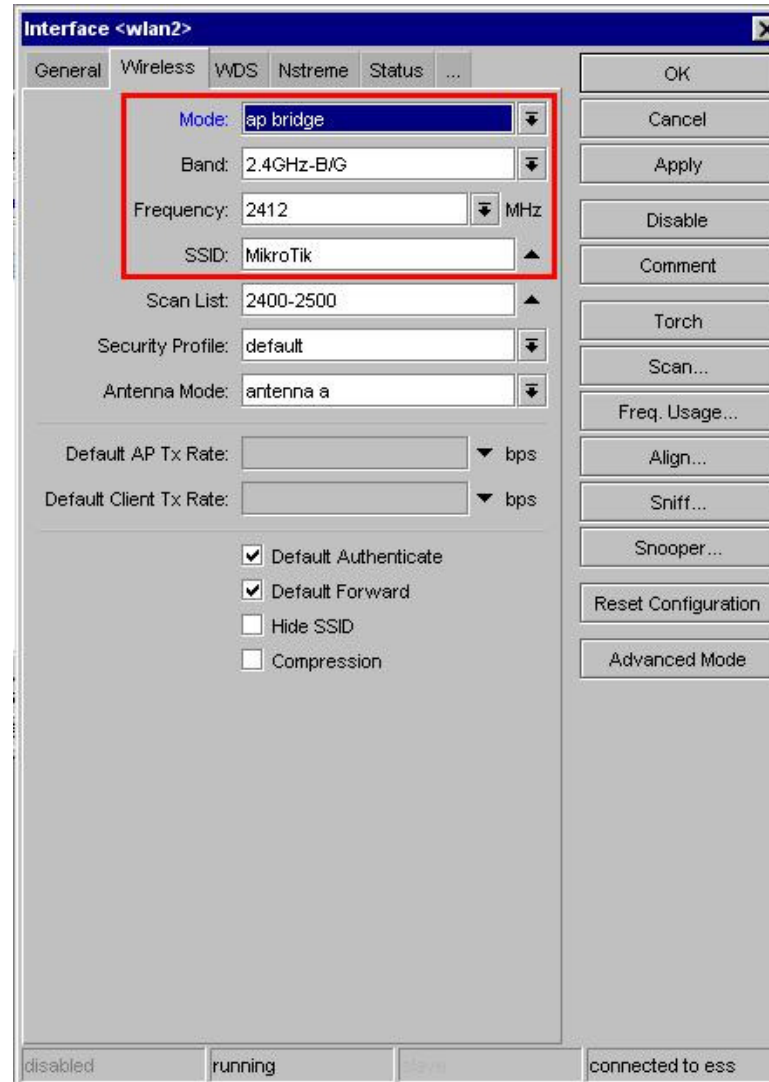
Point to Multi Point

- Mikrotik difungsikan sebagai access point. Digunakan standart 802.11b atau 802.11b/g sehingga semua client dapat terkoneksi.



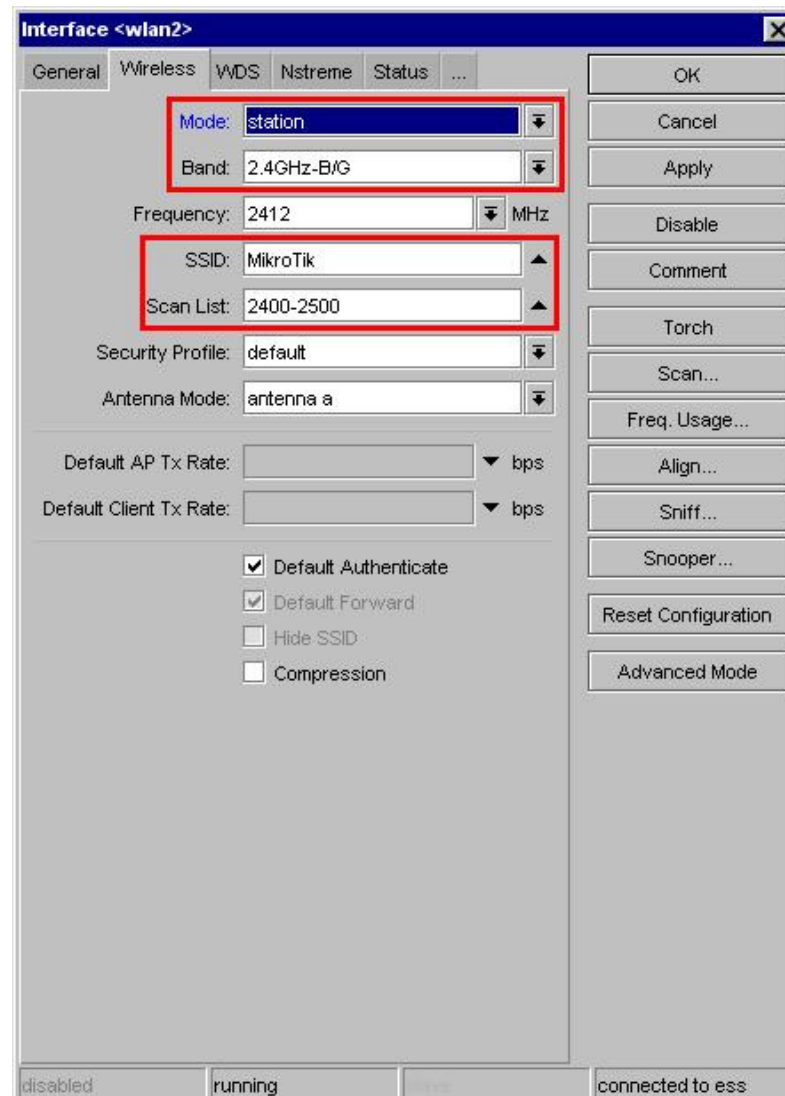
Point to Multi Point - AP

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



● ● ● | Point to Multi Point – Station

- Dapat menggunakan lisensi level 3
- Set mode, ssid, band, scan-list
- Set mode=station
- Pastikan frekuensi yang digunakan berada dalam rentang scan-list



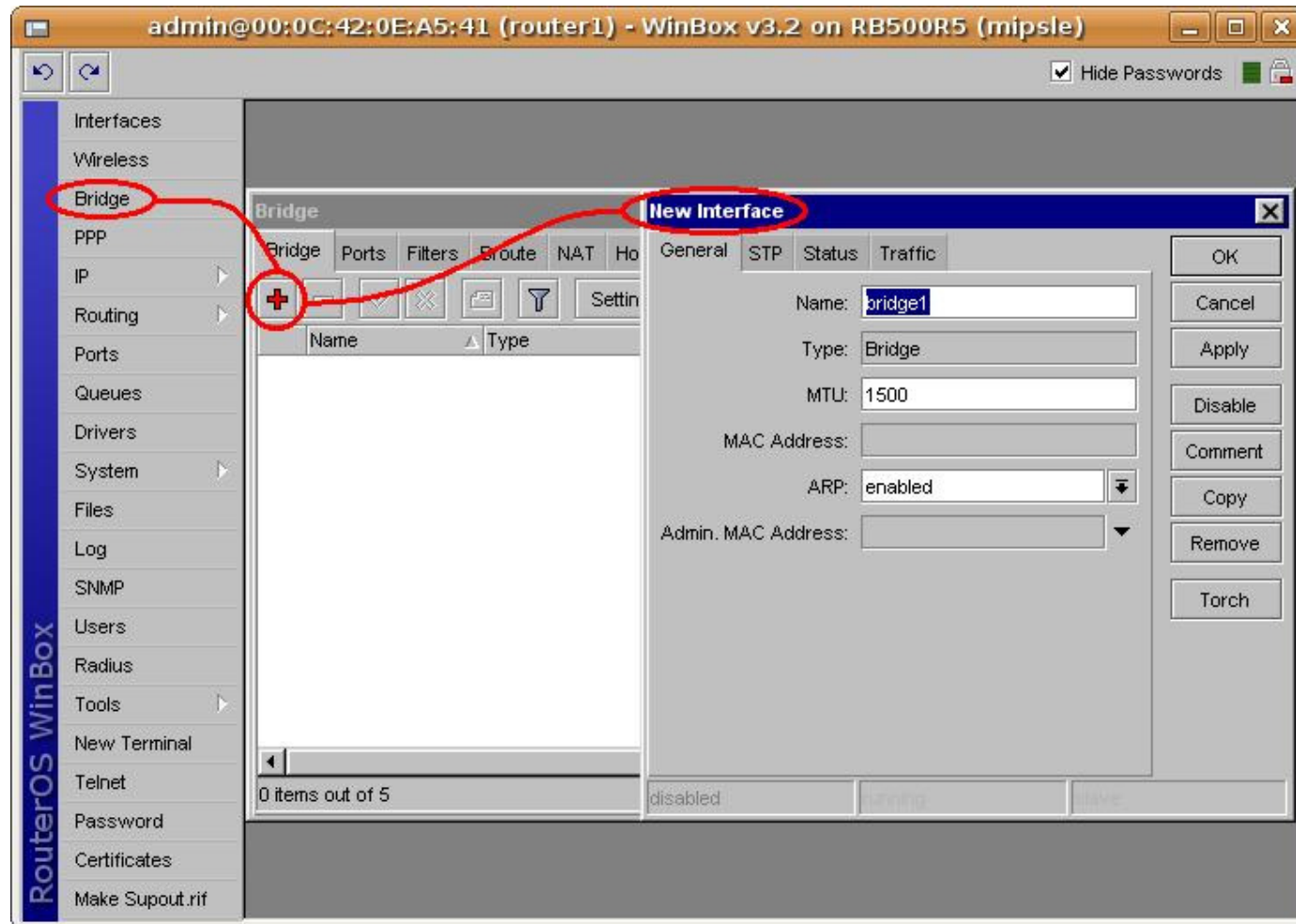
Configuration Console-Terminal - point-to-multipoint

- Configuration AP Side
 - /interface wireless set wlan1 mode=ap-bridge frequency=2412 band=2.4ghz-b/g ssid=meja1
- Configuration Client Side
 - /interface wireless set wlan1 mode=station band=2.4ghz-b/g scan-list=2400-2500 ssid=meja1



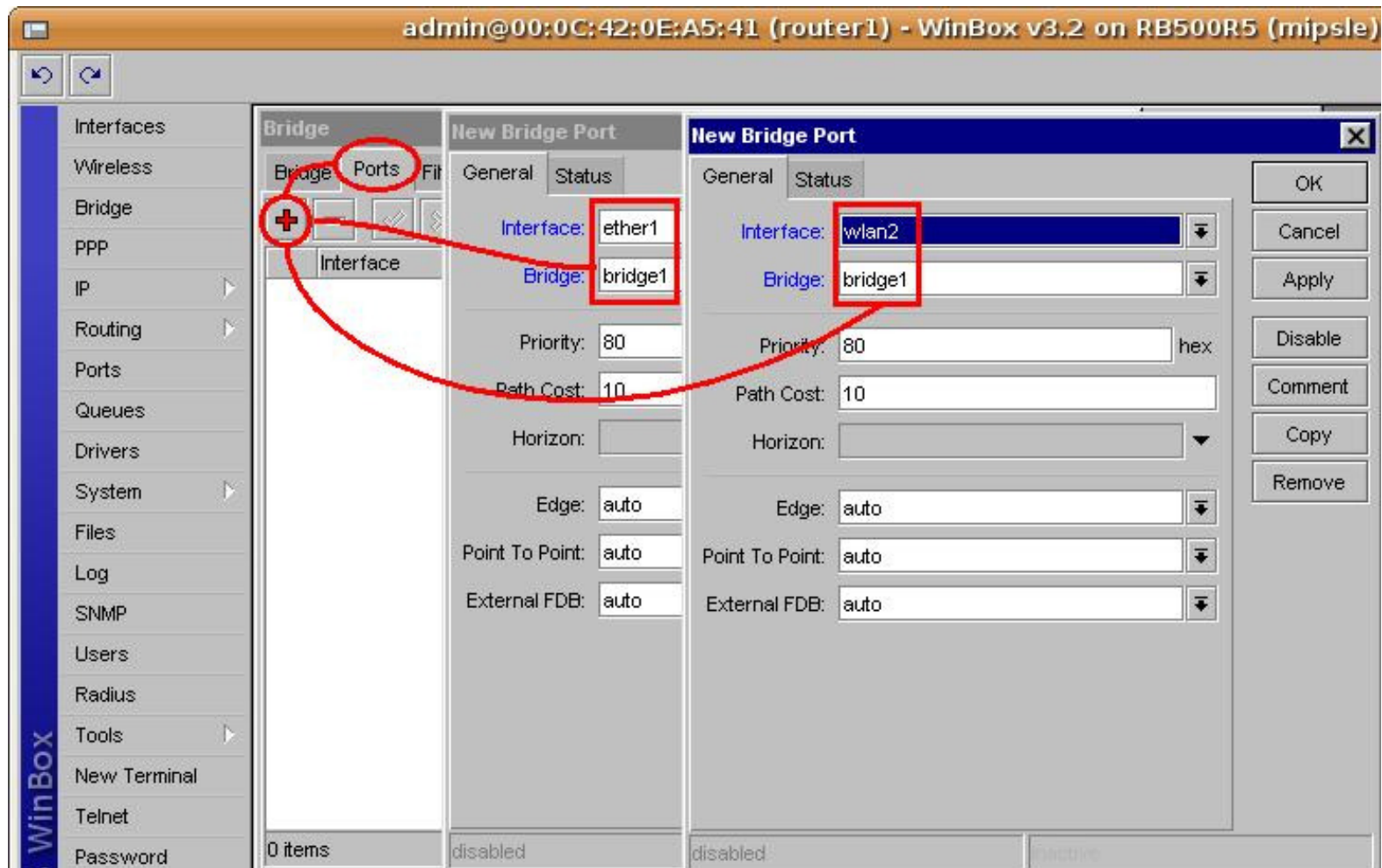
Need Bridge AP? - Step 1

- Add a bridge Interface



Need Bridge AP? - Step 2

- Set bridge for each interface



Configuration Console-Terminal – Bridge-AP

- Make Bridge Interface
 - /interface bridge add name=bridge1
disabled=no
- Configuration bridged - AP
 - /interface bridge ports add interface=wlan1
bridge=bridge1
 - /interface bridge ports add interface=ether1
bridge=bridge1

● ● ● | Virtual AP

- Virtual Access Point (VAP) interface is used to have an additional AP.
- You can create a new AP with different ssid and mac-address.
- It can be compared with a VLAN where the ssid from VAP is the VLAN tag and the hardware interface is the VLAN switch.



Virtual AP Configuration

- Add Virtual Ap Interface

The screenshot displays the Mikrotik WinBox v3.1 interface for configuring a Virtual AP. The 'Wireless Tables' window is open, showing a table with the following data:

Type	MTU	MAC Address
Wireless (Ather...	1500	00:02:6F:43:FB:47
Wireless (Ather...	1500	00:0B:6B:37:69:B6

The 'Interface <wlan3>' configuration window is also open, showing the following settings:

- SSID: MikroTik
- Master Interface: wlan2
- Security Profile: default
- Default AP Tx Rate: [] bps
- Default Client Tx Rate: [] bps
- Default Authenticate
- Default Forward
- Hide SSID

The 'Interfaces' table in the background shows the following entries:

Name	Type
wlan1	Wireless (Athe...
wlan2	Wireless (Athe...
wlan3	VirtualAP

Configuration Console-Terminal – VAP

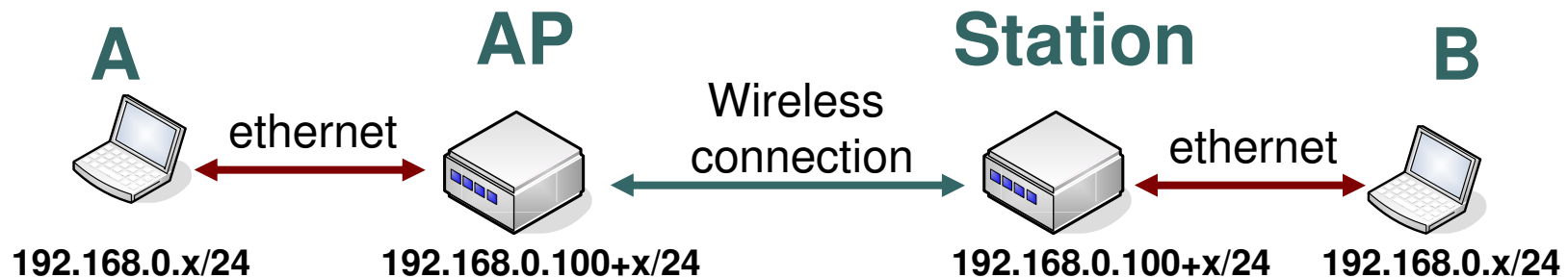
- Configure interface wlan2
 - /interface wireless set wlan2 mode=ap-bridge frequency=2462 band=2.4ghz-b/g disabled=no
- Make VAP Interface
 - /interface wireless add disabled=no name=wlan3 master-interface=wlan2
- Configuration - VAP
 - /interface wireless set wlan3 ssid=MikroTik

● ● ● | Wireless Bridge

- Mikrotik Station **can not** be bridged
- So?
 - We use EoIP for AP and station
<http://www.mikrotik.com/docs/ros/2.9/interface/eoip>
 - We Use WDS-station mode! (faster 10-20 % than E0IP).
 - We use station-pseudobridge

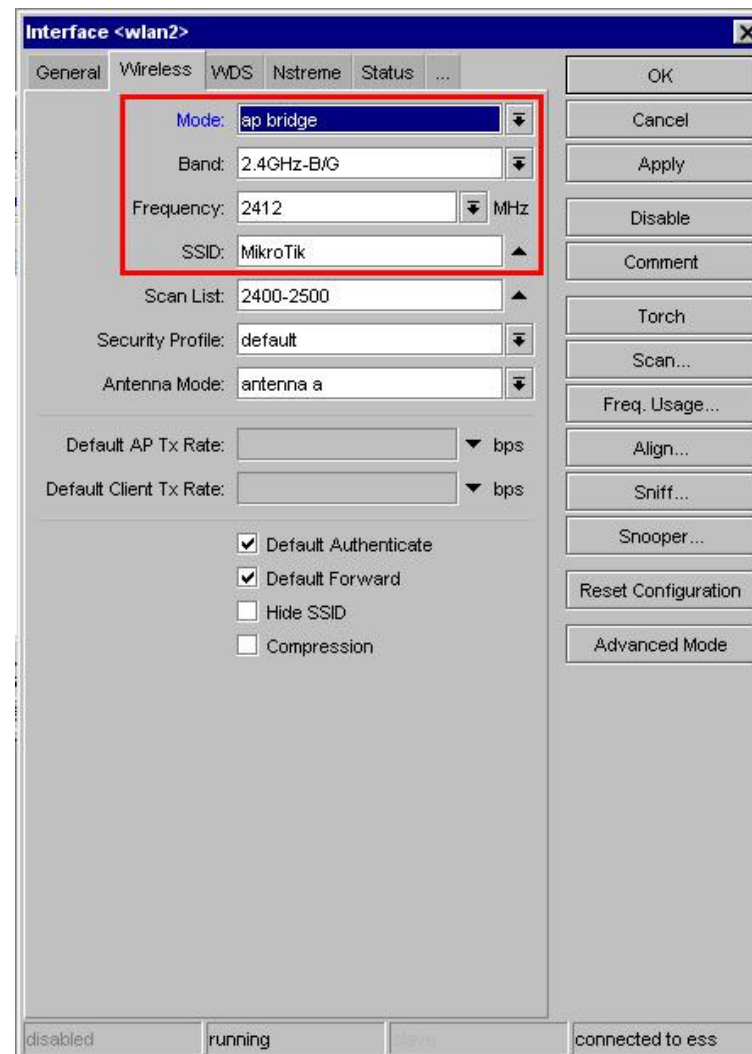
● ● ● | [LAB] Wireless Bridge

- Make AP-Client Bridge Network using station-pseudobridge mode
- After successful making a bridge wireless connection, laptop A can ping laptop B



● ● ● | [LAB] Wireless Bridge – AP side

- AP Side using AP-Bridge Mode





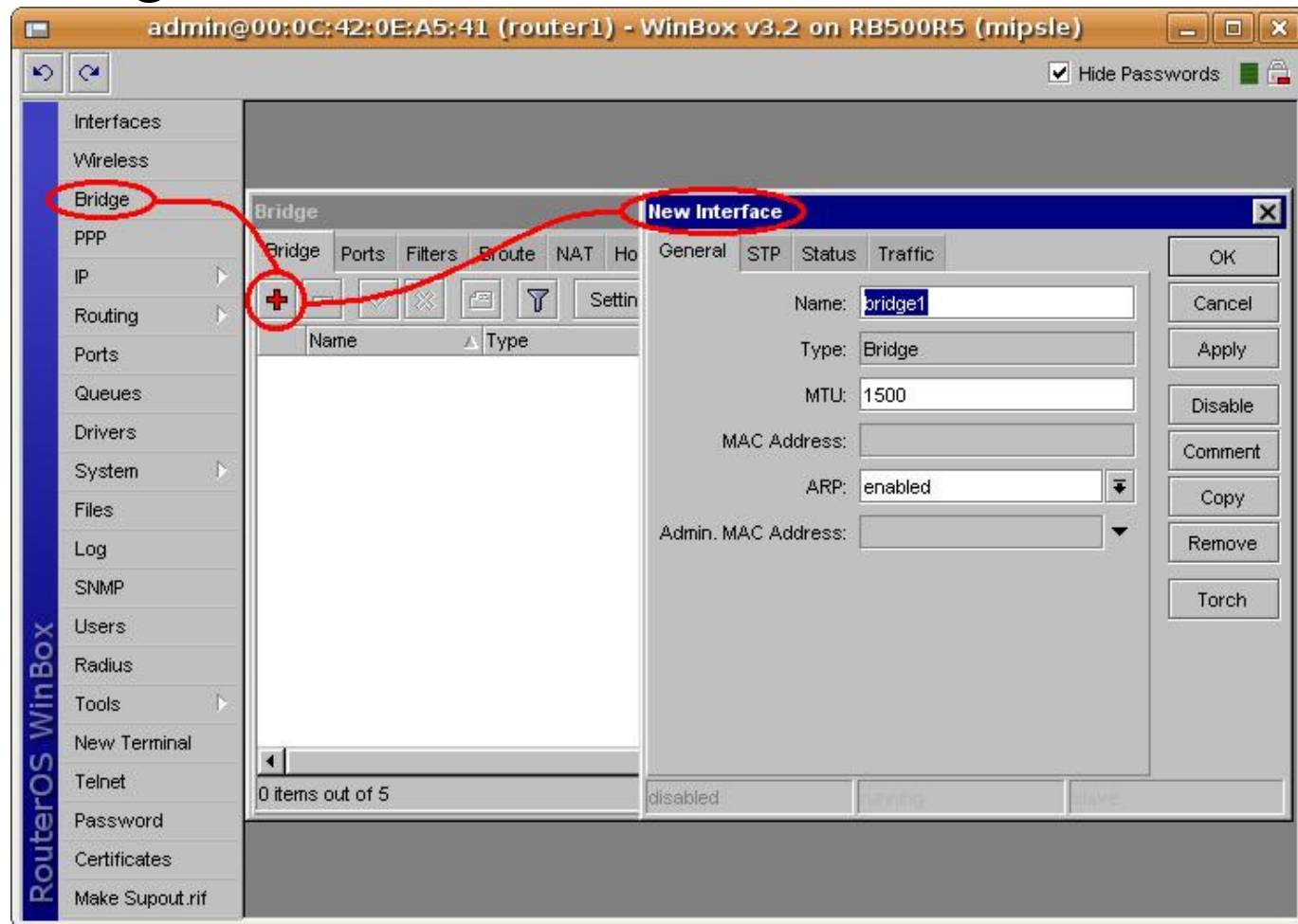
[LAB] Wireless Bridge – Client side

- Client Side: Set mode= station-pseudobridge

The screenshot shows the Mikrotik WinBox configuration window for the 'wlan2' interface. The 'Wireless' tab is active. The 'Mode' is set to 'station pseudobridge', 'Band' is '2.4GHz-B/G', 'Frequency' is '2412 MHz', 'SSID' is 'MikroTik', and 'Scan List' is '2400-2500'. Other settings include 'Security Profile: default', 'Antenna Mode: antenna a', 'Default AP Tx Rate' and 'Default Client Tx Rate' (both empty), and checkboxes for 'Default Authenticate', 'Default Forward', 'Hide SSID', and 'Compression'. The status bar at the bottom shows 'disabled', 'running', 'save', and 'connected to ess'.

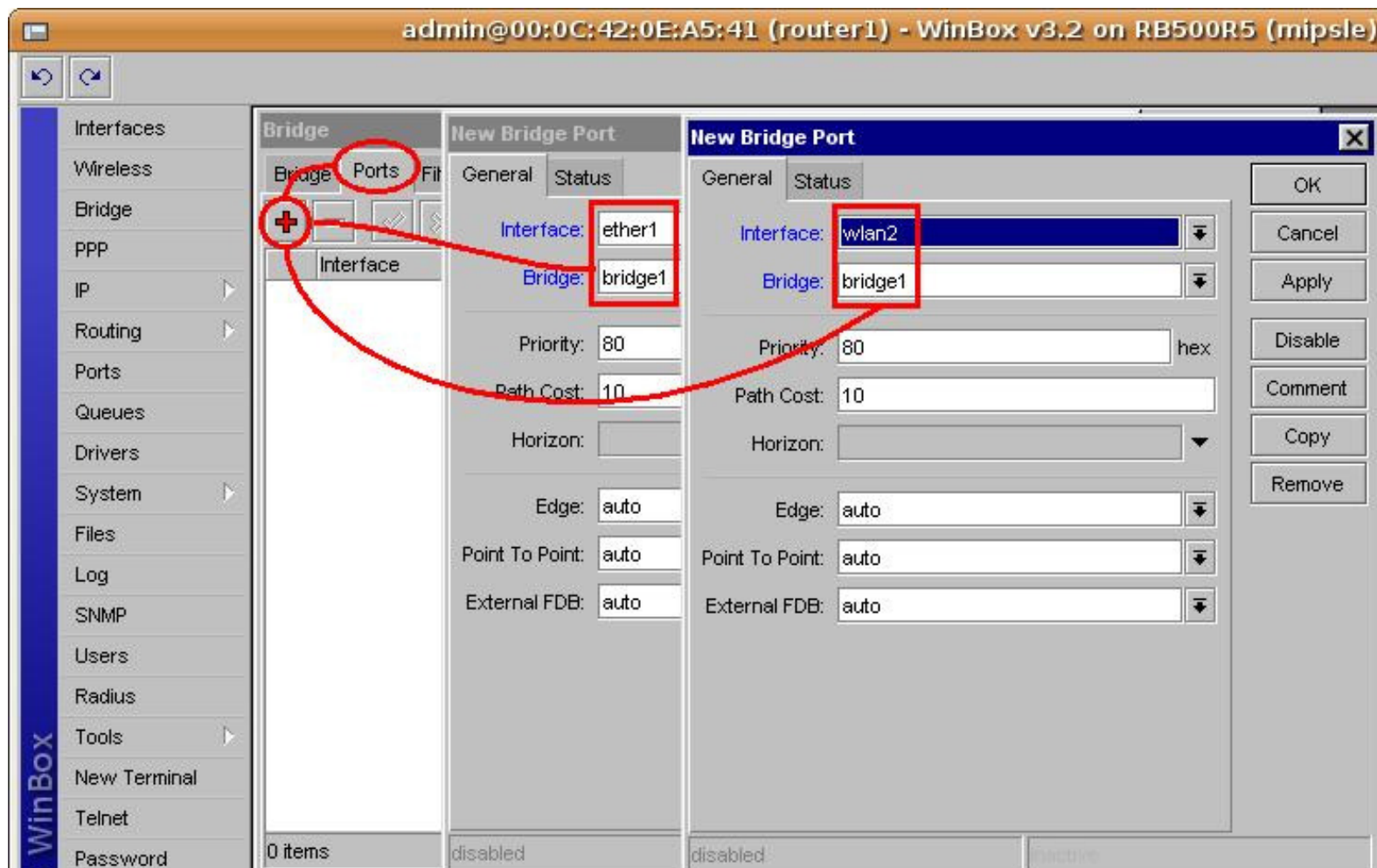
● ● ● [LAB] Wireless Bridge- Bridge Config

- Make Bridge Interface



[LAB] Wireless Bridge – Bridge Ports Config

- Define and set the ports



● ● ● | Other Setting

- **Periodic Calibration** → Set to default to ensure performance of chipset over temperature and environmental changes, the software performs periodic calibration
- **Default Forward**
To allow clients to communicate each other
- **Ack-Timeout**
acknowledgement code timeout (transmission acceptance timeout) in microseconds for acknowledgement messages

See table at: <http://www.mikrotik.com/docs/ros/2.9/interface/wireless>



Scan Tool

Scan <wlan2> (running) Find

	Address	SSID	Band	Freq...	Signa...	Noise...	Signa...	Radio Name	RouterO...
ABR	00:0B:6B:37:69:B6	week2	2.4GHz-G	2412	-47	-99	52	000B6B3769B6	2.9.50
ABR	00:0C:42:1B:5C:69	MikroTik	2.4GHz-G	2437	-46	-99	53	000C421B5C69	3.2
ABR	00:0C:42:1B:5C:81	MikroTik	2.4GHz-G	2427	-47	-100	53	000C421B5C81	3.1
ABR	00:0C:42:1B:5C:85	MikroTik	2.4GHz-G	2422	-5	-99	94	000C421B5C85	3.1

Start
Stop
Close
Connect
Use Network

4 items



Snoop Tool

Snooper <wlan2> (running)

Networks Stations

Find

Frequen...	Band	Address	SSID	Of Freq. (%)	Of Traf. (%)	Bandwidth	Net...	Stati...
2412	2.4GHz...	00:02:6F:48:37:C4	IAP1	0.0	0.0	0 bps		1
2412	2.4GHz...	00:0B:6B:37:69:B6	week2	1.1	35.2	9.3 kbps		1
2412	2.4GHz...			3.2		22.3 kbps	2	2
2417	2.4GHz...			2.9		18.4 kbps	0	0
2422	2.4GHz...			6.3		46.8 kbps	1	1
2427	2.4GHz...							
2432	2.4GHz...							
2437	2.4GHz...							
2442	2.4GHz...							
2447	2.4GHz...							
2452	2.4GHz...							
2457	2.4GHz...							
2462	2.4GHz...							

16 items

Snooper <wlan2> (running)

Networks Stations

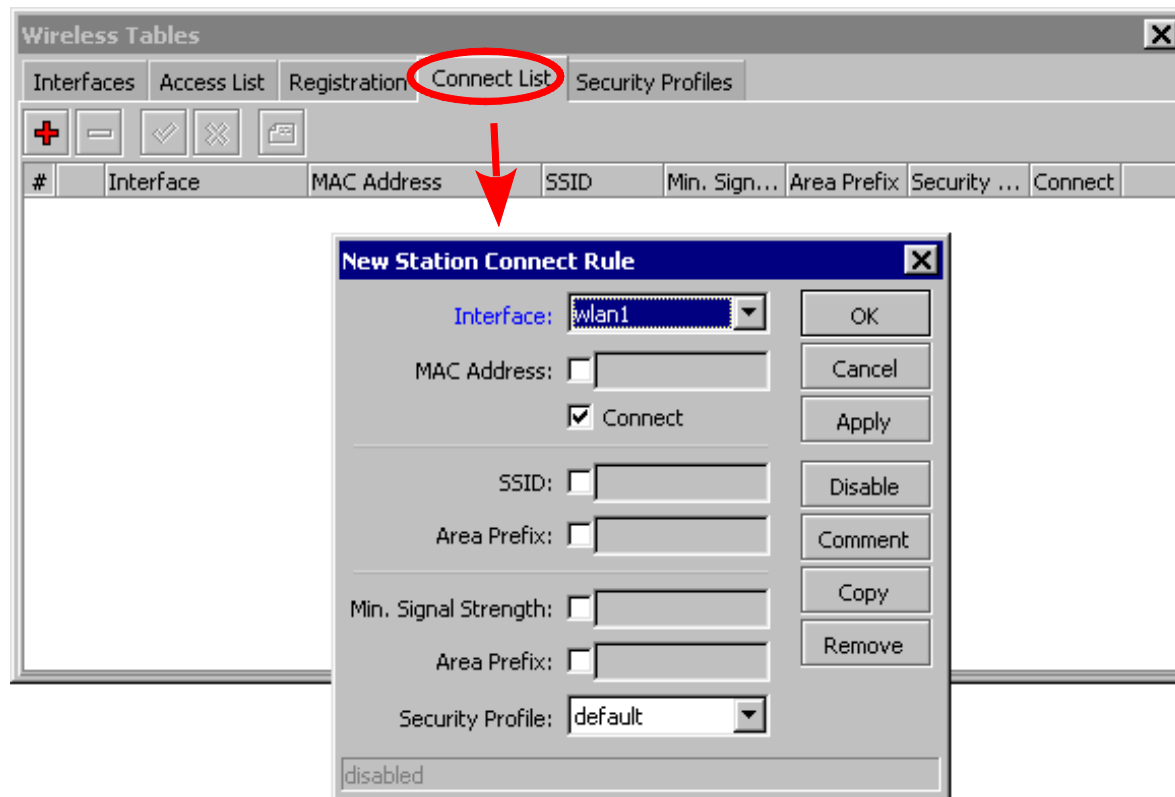
Find

Frequen...	Address	SSID	Signal	Of Freq. (%)	Of Traf. (%)	Bandwidth	Stati...
2412	00:0B:6B:37:69:B6	week2		1.1	58.8	9.5 kbps	1
N	2412 00:0B:6B:37:69:B6	week2	-49	1.1	58.8	9.5 kbps	
2412	00:02:6F:48:37:C4	IAP1		0.0	0.0	0 bps	1
N	2412 00:02:6F:48:37:C4	IAP1	-91	0.0	0.0	0 bps	
2422	00:0C:42:1B:5C:85	MikroTik		1.0	65.2	8.8 kbps	1
N	2422 00:0C:42:1B:5C:85	MikroTik	-6	1.0	65.2	8.8 kbps	
2427	00:0C:42:1B:5C:81	MikroTik		0.5	34.0	4.7 kbps	1
N	2427 00:0C:42:1B:5C:81	MikroTik	-47	0.5	34.0	4.7 kbps	
2437	00:0C:42:1B:5C:69	MikroTik		1.1	100.0	9.4 kbps	1
N	2437 00:0C:42:1B:5C:69	MikroTik	-45	1.1	100.0	9.4 kbps	
2462	00:16:CB:B7:34:09			0.0	0.0	0 bps	

11 items

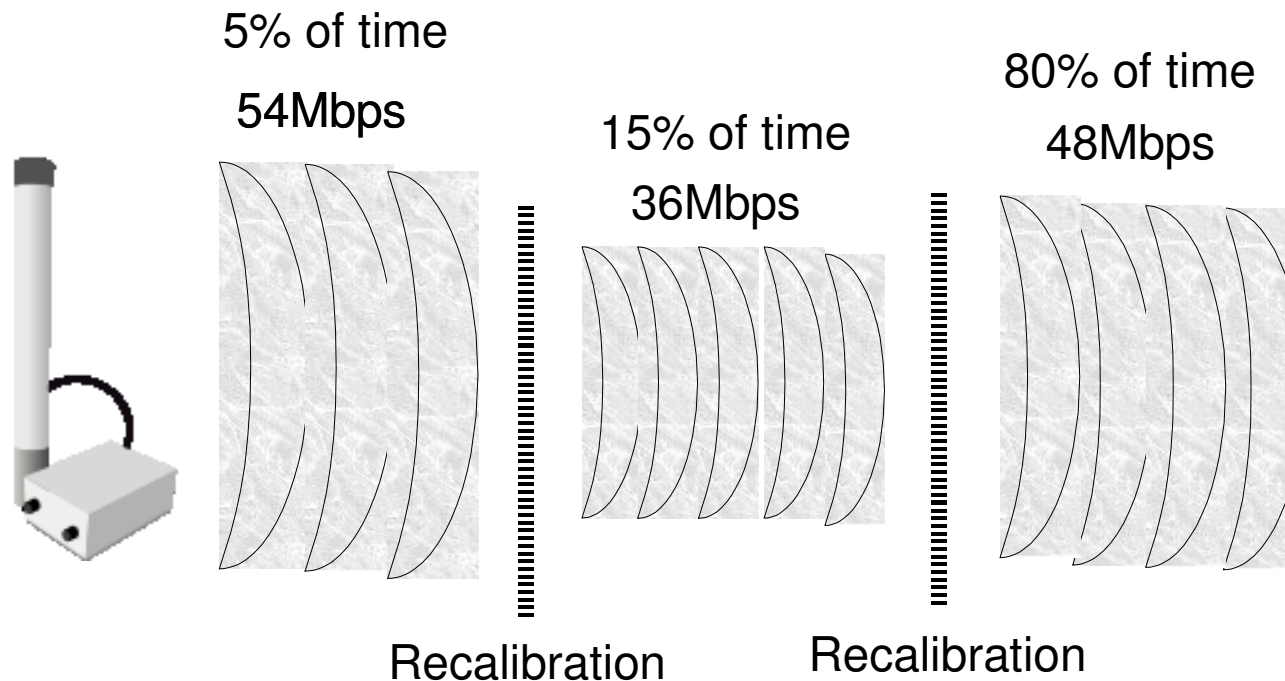
Connect List

- You can allow or deny clients from connecting to specific AP by using Connect list (popular for wds)





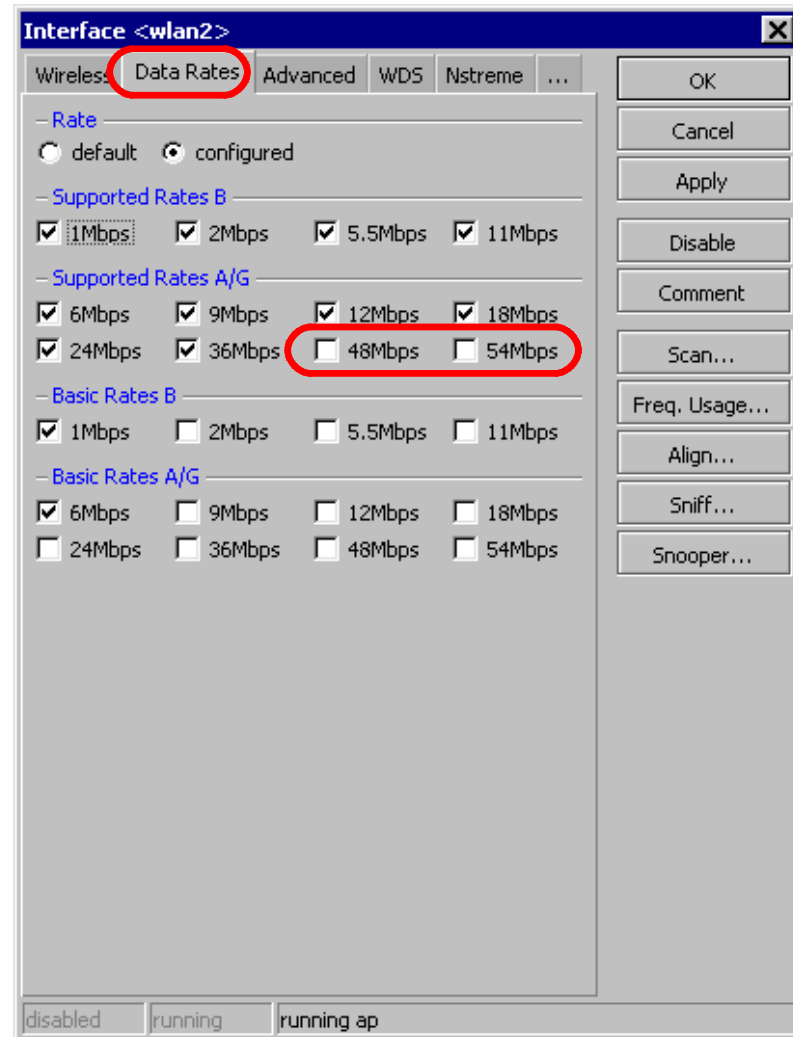
Rate Jumping



- You can optimize link performance, by avoiding rate jumps, in this case link will work more stable at 36Mbps rate

Basic and Supported Rates

- Supported rates – client data rates
- Basic rates – link management data rates
- If router can't send or receive data at basic rate – link goes down





Hotspot

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

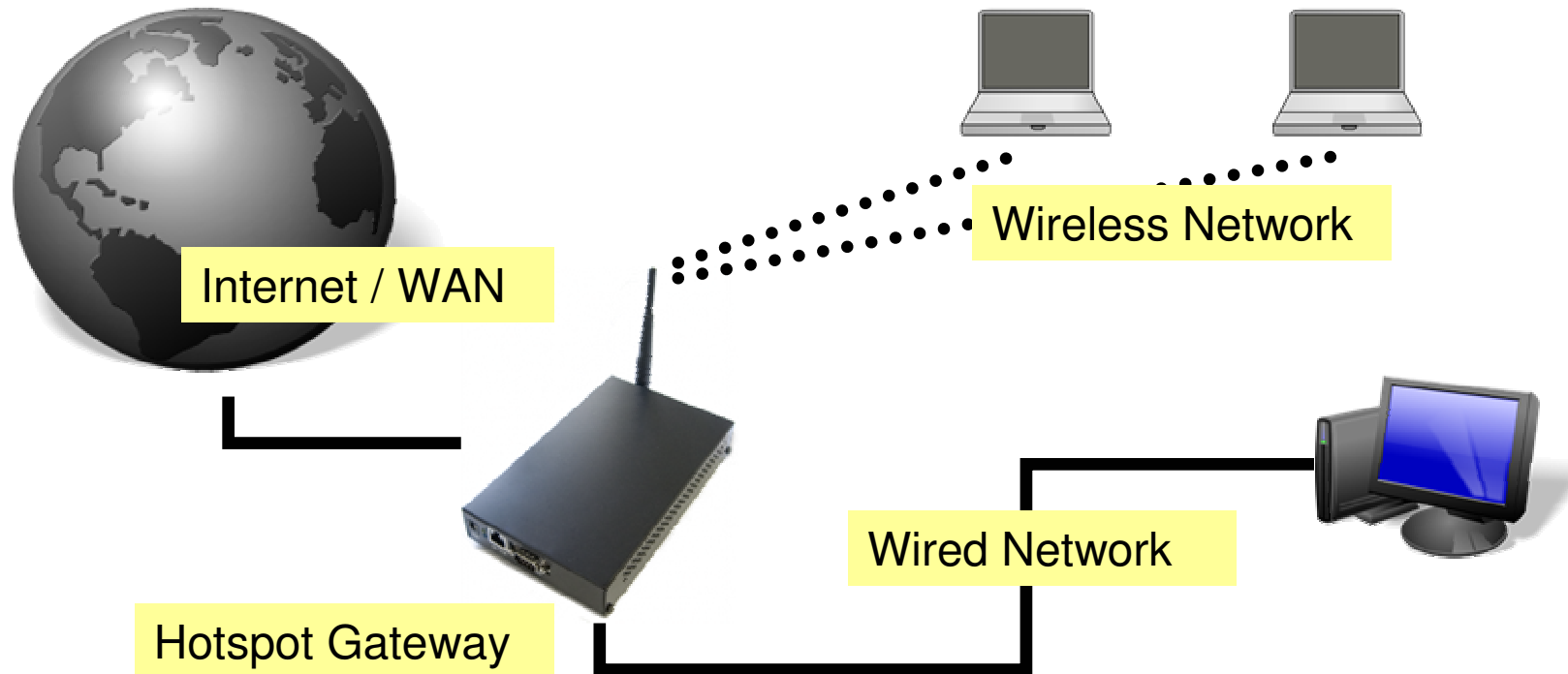
(Mikrotik Certified Training Partner)



HotSpot

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

HotSpot Network - Example

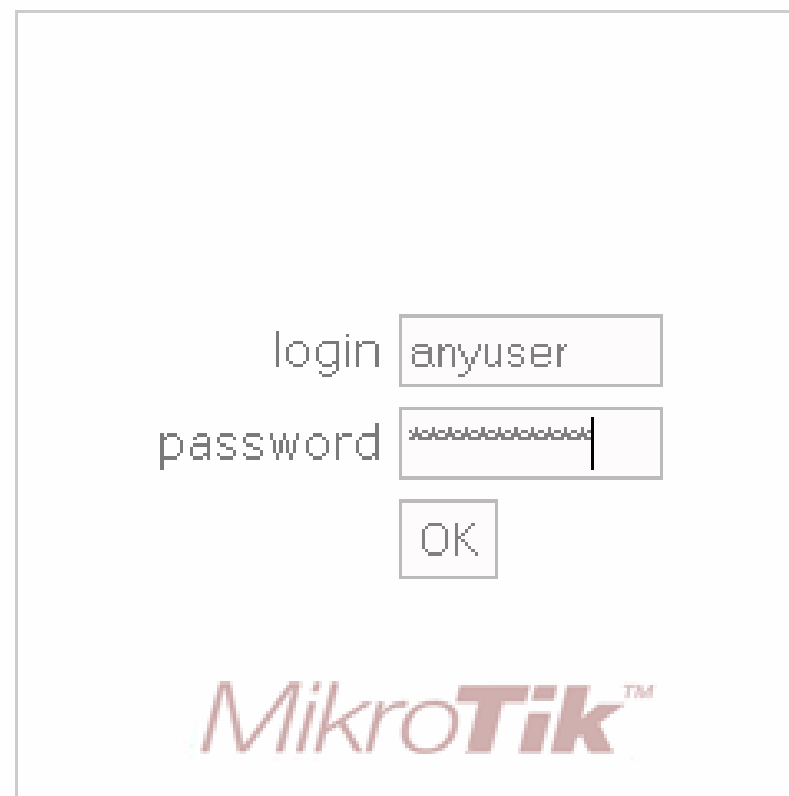


- Hotspot System bisa digunakan pada jaringan Wireless maupun jaringan Kabel bahkan kombinasi dari keduanya.
- Jaringan Hotspot bersifat **Bridge Network**

● ● ● | How does it work ?

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

Please log on to use the mikrotik hotspot service



A screenshot of a Mikrotik Hotspot login interface. It features a white background with a light gray border. At the top, the text "Please log on to use the mikrotik hotspot service" is displayed in a small, gray font. Below this, there are three input fields: a "login" field containing the text "anyuser", a "password" field containing a series of asterisks, and an "OK" button. At the bottom of the form, the "MikroTik" logo is displayed in a stylized, reddish-brown font.

Powered by mikrotik routers © 2005 mikrotik

● ● ● | How does it work ?

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

Welcome anyuser!

IP address:	10.1.100.1
bytes up/down:	23.1 KiB / 43.5 KiB
connected:	40s
status refresh:	1m

log off



HotSpot features

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



HotSpot setup wizard

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

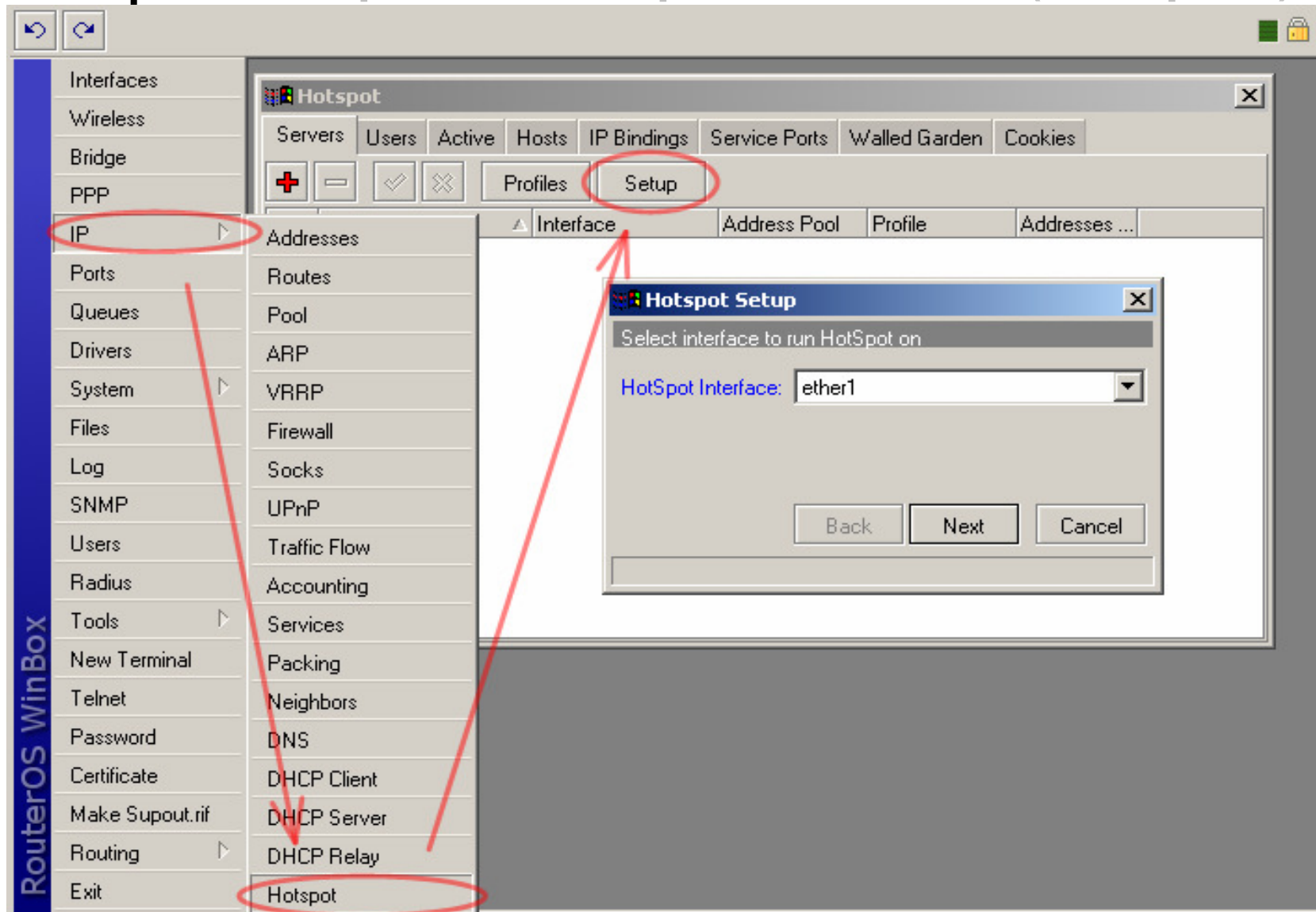
HotSpot Setup Wizard

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

HotSpot Setup Wizard

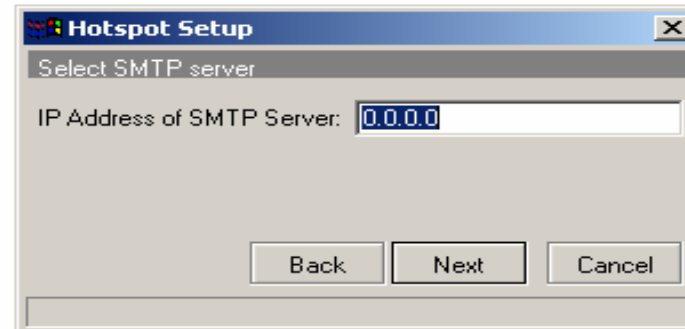
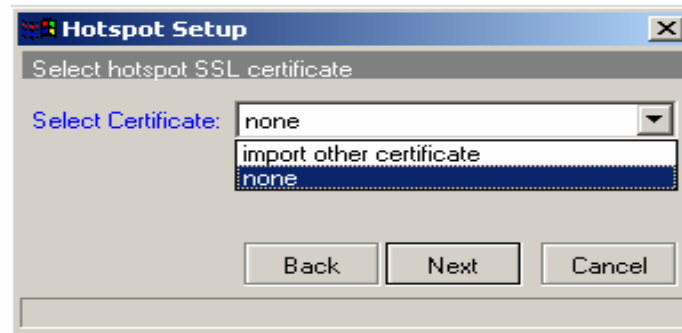
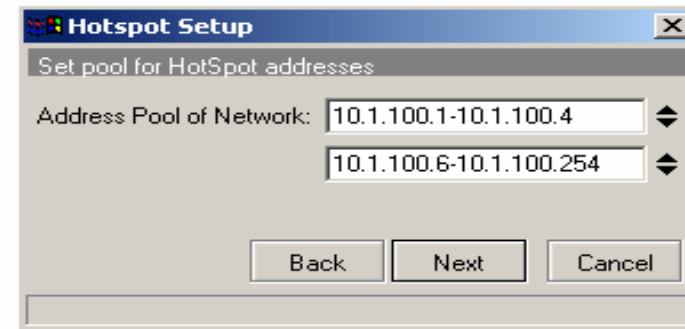
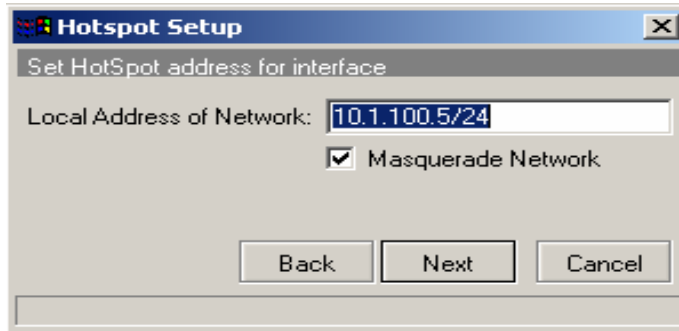
- Jika diperlukan SMTP server khusus untuk jaringan hotspot bisa ditentukan, sehingga client tidak perlu merubah konfigurasi SMTP server :
Ip address of smtp server: 0.0.0.0 (ex: 159.148.147.194)
- Konfigurasi DNS server yang akan digunakan oleh user Hotspot :
dns servers: 159.148.147.194,159.148.60.20
- Konfigurasi DNS-name dari router Hotspot, Hal ini digunakan jika Router memiliki DNS-Name yang valid (FQDN), Jika tidak ada biarkan kosong.
- Langkah terakhir dari wizard adalah pembuatan sebuah user hotspot :
name of local hotspot user: usrox
password for the user: 12345

HotSpot Setup Wizard (Step 1)



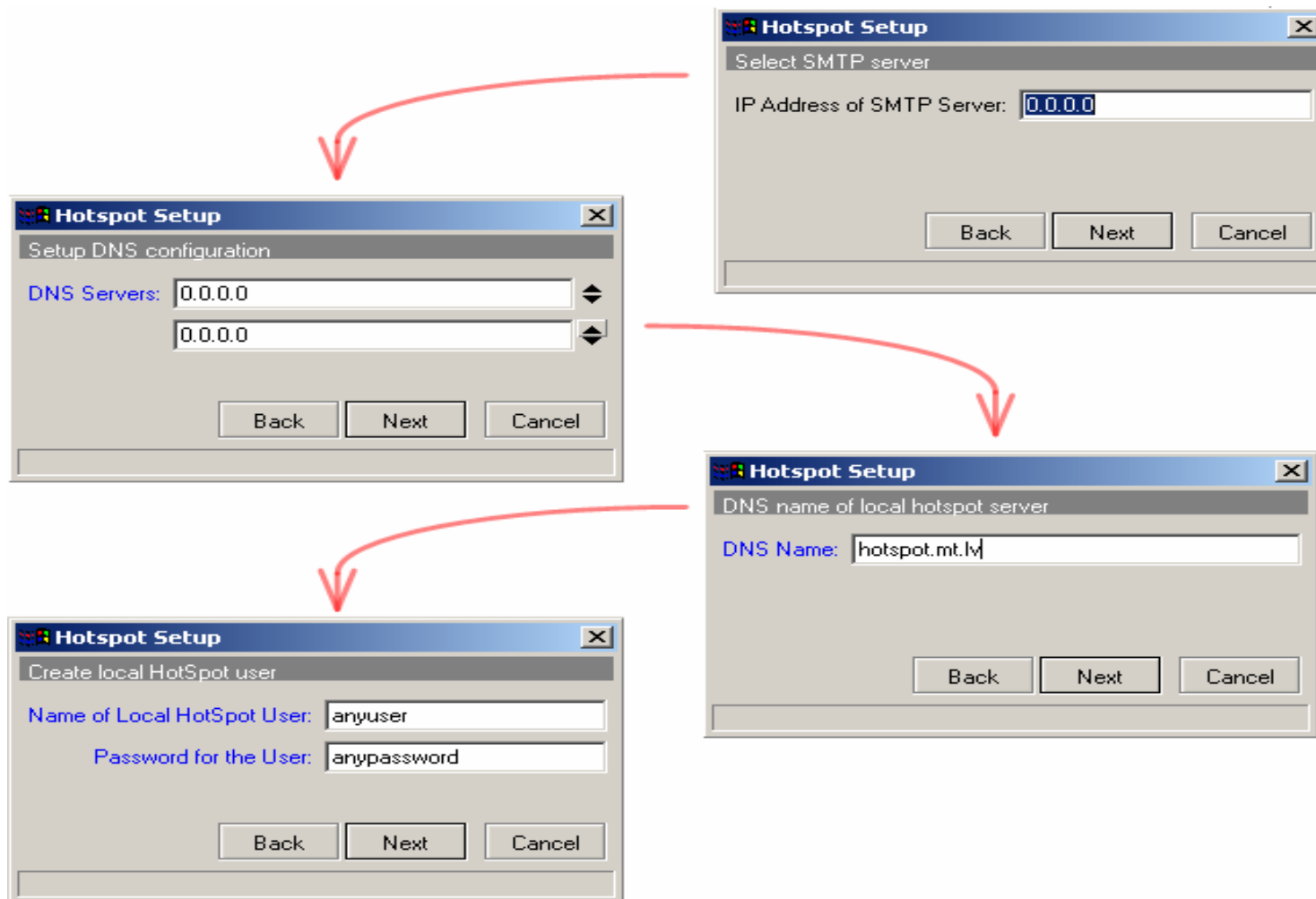


HotSpot Setup Wizard (Step 2-5)





HotSpot setup wizard (step 5-8)



HotSpot Server Profiles

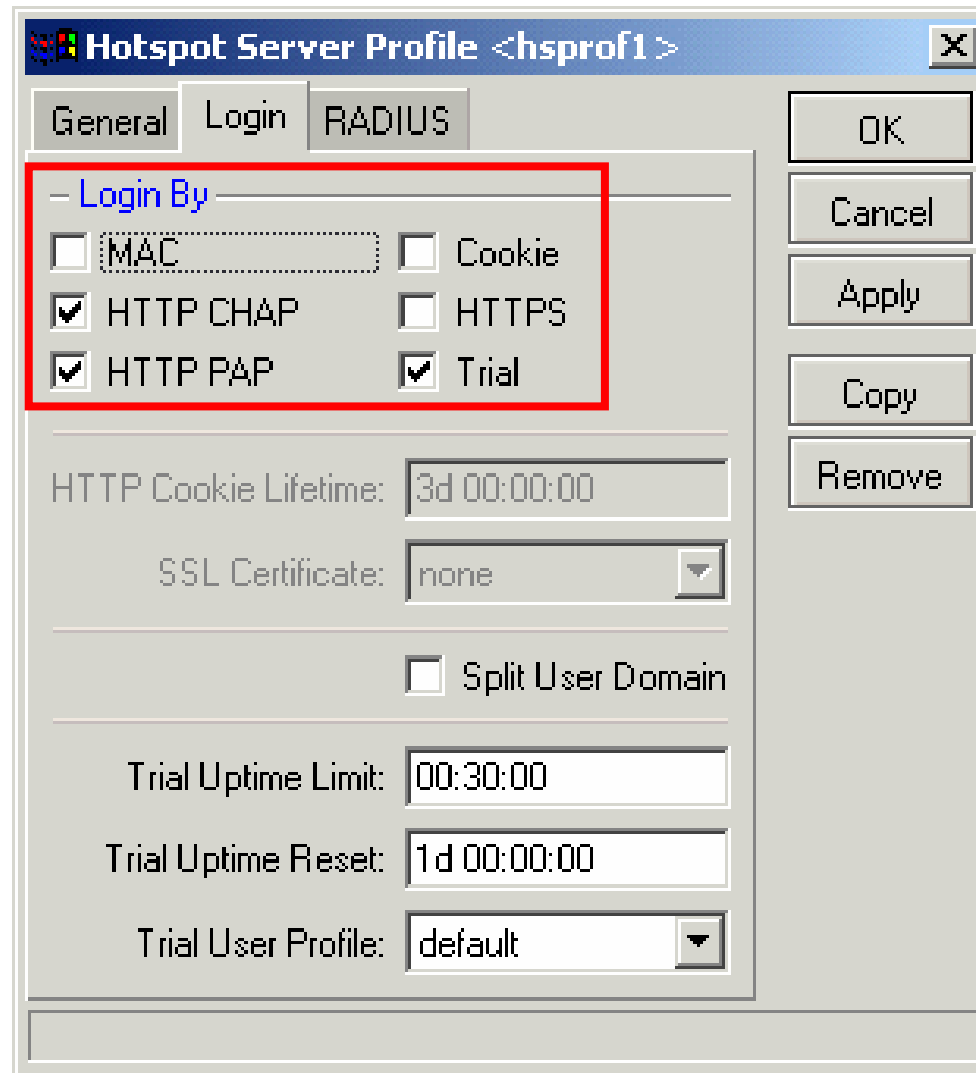
The screenshot illustrates the configuration process for Hotspot Server Profiles in RouterOS WinBox. The interface is divided into several sections:

- Left Panel (WinBox Menu):** A vertical sidebar with various configuration categories. The **Hotspot** category is circled in red, and a red arrow points from it to the main configuration area.
- Main Configuration Area:** The **Hotspot** configuration page is shown. The **Servers** and **Profiles** tabs are circled in red. A red arrow points from the **Profiles** tab to a sub-window.
- Hotspot Server Profiles Sub-window:** A smaller window titled "Hotspot Server Profiles" is open, showing a table of profiles. The **Profiles** tab is circled in red, and a red arrow points from it to the table. The table contains two entries: "default" and "hspof1".
- Hotspot Server Profile <hspof1> Dialogs:** Two dialog boxes are shown for the "hspof1" profile. The top dialog is the **General** tab, and the bottom dialog is the **Login** tab. Both tabs are circled in red. The **General** tab shows fields for Name (hspof1), Hotspot Address (10.1.100.5), DNS Name, HTML Directory, Rate Limit, HTTP Proxy, HTTP Proxy Port, and SMTP Server. The **Login** tab shows options for Login By (MAC, Cookie, HTTP CHAP, HTTP PAP, HTTPS) and HTTP Cookie Lifetime (3d 00:00:00).

● ● ● | HotSpot Server profiles

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

Authentication Method



- 6 Metode autentikasi yang berbeda pada server profile.

Hotspot Authentication Methods

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



HotSpot User Profiles

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

HotSpot User Profiles

The image shows the RouterOS WinBox interface with the 'Hotspot' menu open. The 'Hotspot' menu is circled in red, and the 'Users' sub-menu is also circled. A red arrow points from the 'Users' sub-menu to the 'New Hotspot User Profile' dialog box. The 'New Hotspot User Profile' dialog box is open, showing the 'General' tab. The 'Name' field is set to 'uprof1', the 'Address Pool' is set to 'hs-pool-1', the 'Idle Timeout' is set to 'none', the 'Keepalive Timeout' is checked and set to '00:02:00', the 'Status Autorefresh' is set to '00:01:00', the 'Shared Users' is checked and set to '1', and the 'Rate Limit' is unchecked. The 'Incoming Filter' and 'Outgoing Filter' are both set to empty. The 'Incoming Packet Mark' and 'Outgoing Packet Mark' are both set to empty. The 'Open Status Page' is set to 'always' and the 'Transparent Proxy' checkbox is unchecked. The 'OK', 'Cancel', 'Apply', 'Copy', and 'Remove' buttons are visible on the right side of the dialog box.

RouterOS WinBox

Hotspot

Users

New Hotspot User Profile

General

Name: uprof1

Address Pool: hs-pool-1

Session Timeout:

Idle Timeout: none

Keepalive Timeout: 00:02:00

Status Autorefresh: 00:01:00

Shared Users: 1

Rate Limit:

Incoming Filter:

Outgoing Filter:

Incoming Packet Mark:

Outgoing Packet Mark:

Open Status Page: always

Transparent Proxy

OK

Cancel

Apply

Copy

Remove



HotSpot User

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

HotSpot users

The image shows the RouterOS WinBox interface with the Hotspot configuration window open. The 'Hotspot' window has tabs for 'Servers', 'Users', 'Active', 'Hosts', and 'IP Bindings'. The 'Users' tab is selected, showing a table with one user named 'admin'. A 'New Hotspot User' dialog is open, showing the 'Limits' tab with fields for 'Limit Uptime', 'Limit Bytes In', and 'Limit Bytes Out'. A second 'New Hotspot User' dialog is also open, showing the 'General' tab with fields for 'Server', 'Name', 'Password', 'Address', 'MAC Address', 'Profile', and 'Routes'. The 'Name' field is set to 'anyuser' and the 'Password' field is set to 'anypassword'. The 'Profile' dropdown is set to 'default'. The 'Server' dropdown is set to 'all'. The 'Routes' checkbox is unchecked. The 'disabled' status is shown at the bottom of the dialog.

RouterOS WinBox

Hotspot

Servers Users Active Hosts IP Bindings

Profiles 00

Limit Uptime:

Limit Bytes In:

Limit Bytes Out:

00:00

OK Cancel Apply Disable

New Hotspot User

General Limits Statistics

OK Cancel Apply Disable Comment Copy Remove

Server: all

Name: anyuser

Password: anypassword

Address:

MAC Address:

Profile: default

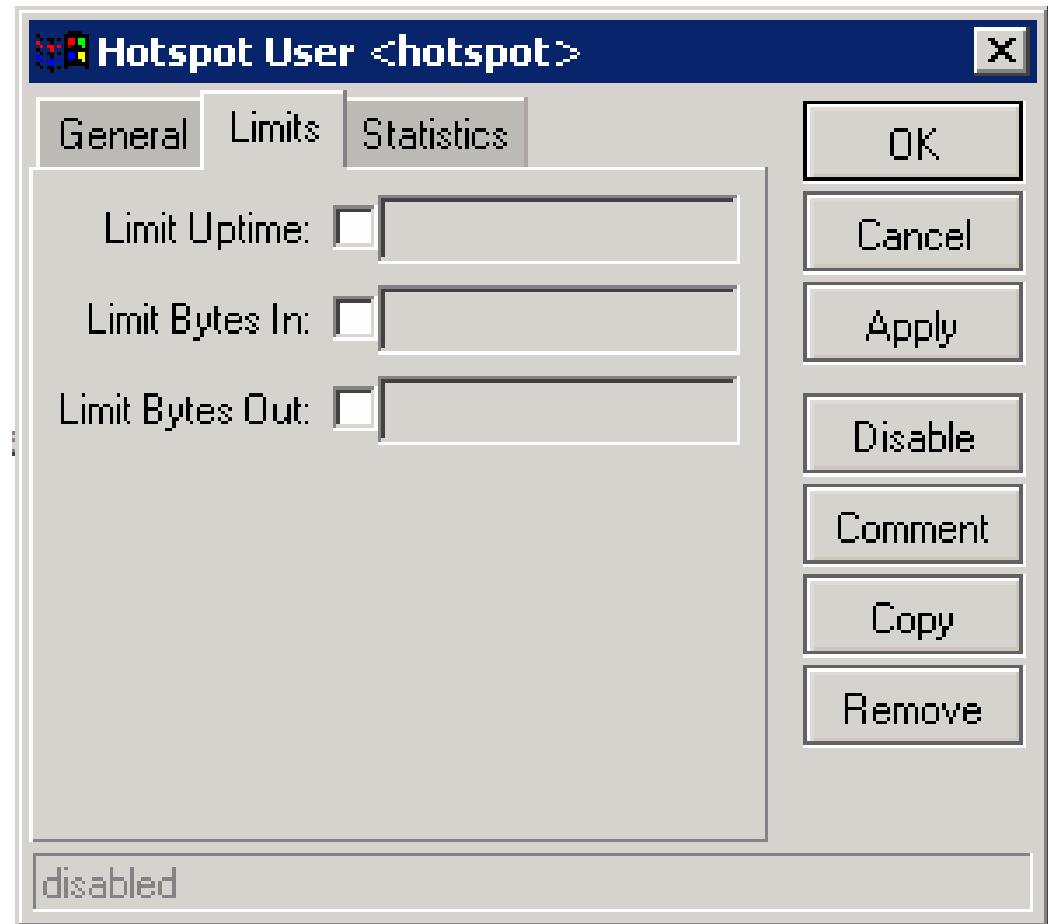
Routes:

disabled



User Limitation

- **Limit Uptime** batas waktu user dapat menggunakan akses ke Hotspot Network.
- **Limit-bytes-in** dan **Limit-bytes-out** batas Jumlah transfer data yang bisa dilakukan oleh user.





Bypass! - IP bindings

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

HotSpot IP bindings

The screenshot displays the RouterOS WinBox interface. On the left, the 'RouterOS WinBox' sidebar is visible, with the 'Hotspot' menu item circled in red. A red arrow points from this menu item to the 'Hotspot' tab in the main window. The 'Hotspot' window has several tabs: 'Servers', 'Users', 'Active', 'Hosts', 'IP Bindings', 'Service Ports', 'Walled Garden', and 'Cookies'. The 'IP Bindings' tab is selected and circled in red. Below the tabs, there is a table with columns for '#', 'MAC Address', 'Address', 'To Address', and 'Server'. A red arrow points from the '+' icon in the toolbar to the 'New Hotspot IP Binding' dialog box. The dialog box contains the following fields and options:

- MAC Address: [text box]
- Address: [text box]
- To Address: [text box]
- Server: all (dropdown menu)
- Type: regular (dropdown menu)
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove
- Status: disabled



Bypass - WalledGarden

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

HTTP-level WalledGarden

The screenshot displays the RouterOS WinBox interface. On the left, the 'RouterOS WinBox' menu is visible, with 'Hotspot' circled in red. The main window shows the 'Hotspot' configuration page, with the 'Walled Garden' tab selected and circled in red. A red arrow points from the 'Hotspot' menu item to the 'Walled Garden' tab. Below the 'Walled Garden' tab, a table with columns for '#', 'Action', 'Server', 'Method', 'Dst. Host', and 'Dst. Port' is shown. A red circle highlights the '+' icon for adding a new entry. A 'Walled Garden Entry' dialog box is open, showing configuration options: 'Action' (radio buttons for 'allow' and 'deny'), 'Server', 'Src. Address', 'Method', 'Dst. Host', 'Dst. Port', and 'Path'. The dialog also includes buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'. The status at the bottom of the dialog is 'disabled'.

IP-WalledGarden

The screenshot displays the RouterOS WinBox interface. The left sidebar shows the 'RouterOS WinBox' menu with 'Hotspot' selected. The main window shows the 'Hotspot' configuration page with the 'Walled Garden' tab active. The 'IP List' button is highlighted, and a dialog box for adding a new IP entry is open. The dialog shows fields for Action (accept, drop, reject), Server, Src. Address, Dst. Address, Protocol, Dst. Port, and Dst. Host.

Hotspot

Servers Users Active Hosts IP Bindings Service Ports **Walled Garden** Cookies

+ - ✓ ✗ **IP List**

#	Action	Server	Method	Dst. Host	Dst. Port
---	--------	--------	--------	-----------	-----------

Walled Garden IP List

+ - ✓ ✗

#	Action	Server	Protocol	Dst. Host	Dst. Address
---	--------	--------	----------	-----------	--------------

Walled Garden IP Entry

Action: accept drop reject

Server:

Src. Address:

Dst. Address:

Protocol:

Dst. Port:

Dst. Host:

disabled

OK Cancel Apply Disable Comment Copy Remove

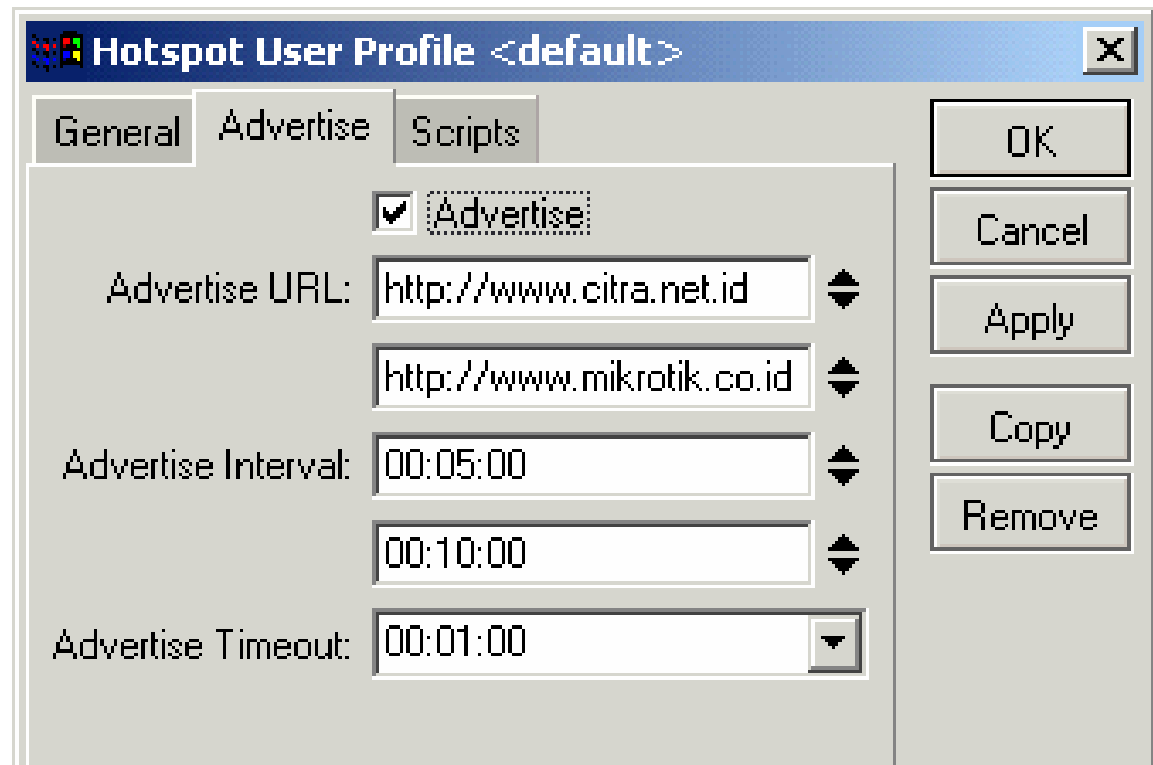


Advertisement

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

Advertisement

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





VPN Basic

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

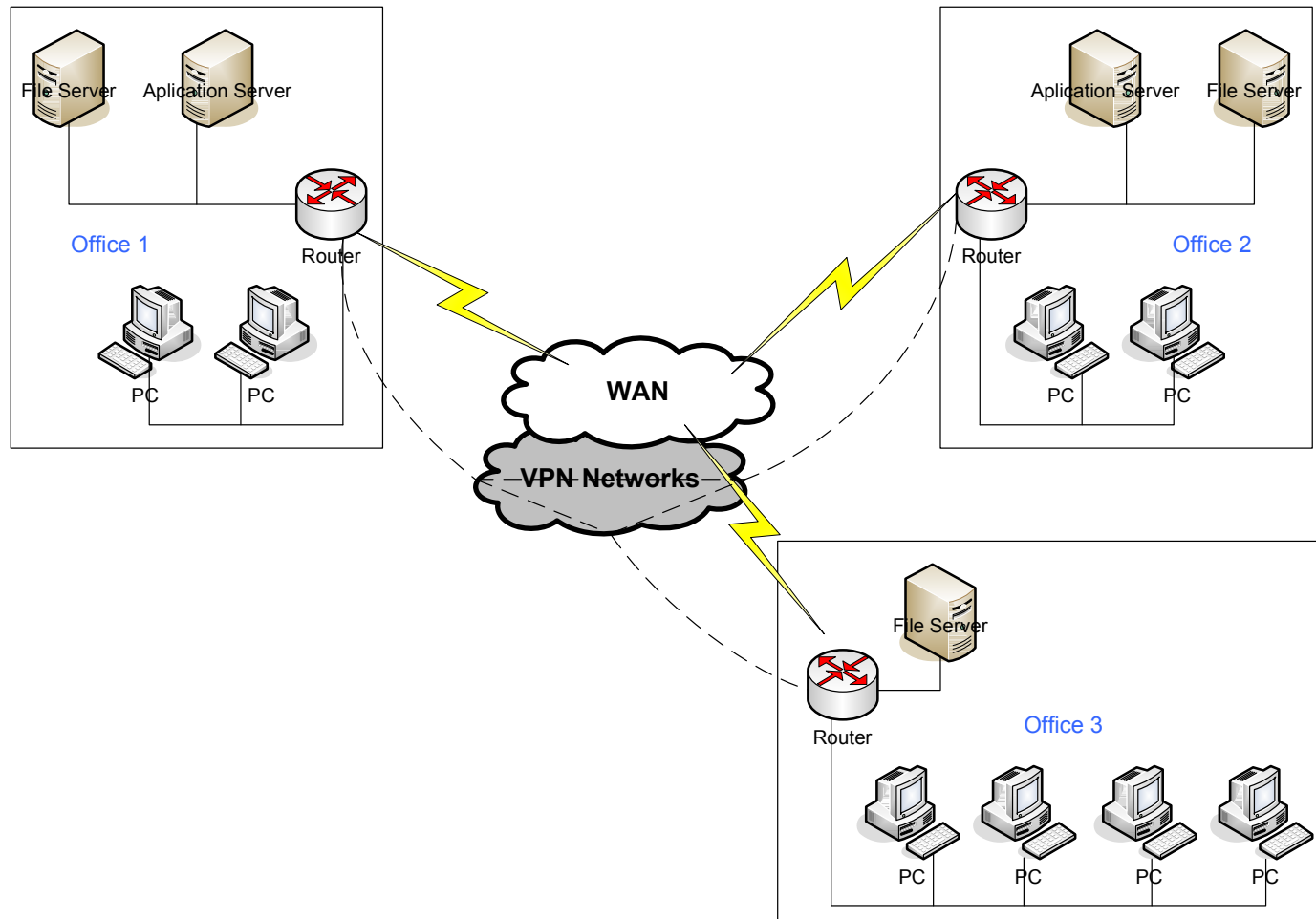
(Mikrotik Certified Training Partner)

VPN (Virtual Private Networks)

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

VPN Networks

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



Point to Point Tunnel Protocol (PPTP)

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

PPTP Client Configuration

The screenshot displays the 'Interface List' window with a tree view on the left and a 'New Interface' dialog box open. The tree view shows various interface types, with 'PPTP Client' selected and circled in red. A red arrow points from this selection to the 'New Interface' dialog. The dialog has two tabs: 'General' and 'Dial Out', both of which are circled in red. The 'General' tab shows the name 'pptp-out1' and type 'PPTP out'. The 'Dial Out' tab shows the 'Server Address' field set to '0.0.0.0' and the 'Profile' dropdown set to 'default-encryption', both circled in red. At the bottom of the dialog, there are checkboxes for authentication protocols: 'pap', 'mschap1', 'chap', and 'mschap2', all of which are checked.

Interface List

Interface Ethernet EoIP Tunnel IP Tunnel VLAN VRRP Bonding

+ - ✓ ✗

EoIP Tunnel
IP Tunnel
VLAN
VRRP
Bonding
Bridge
VPLS
PPP Server
PPP Client
PPTP Server
PPTP Client
L2TP Server
L2TP Client
OVPN Server
OVPN Client
PPPoE Server
PPPoE Client
ISDN Server
ISDN Client

Type Tx Rx Tx Pac... Rx Pac...

Ethernet
Ethernet
Ethernet
Ethernet
Ethernet
Ethernet

New Interface

General Dial Out Status Traffic

Name: pptp-out1
Type: PPTP out
Max MTU: 1460
Max MRU: 1460

Server Address: 0.0.0.0

User:
Password:

Profile: default-encryption

Add Default Route

- Allow -

pap chap
 mschap1 mschap2

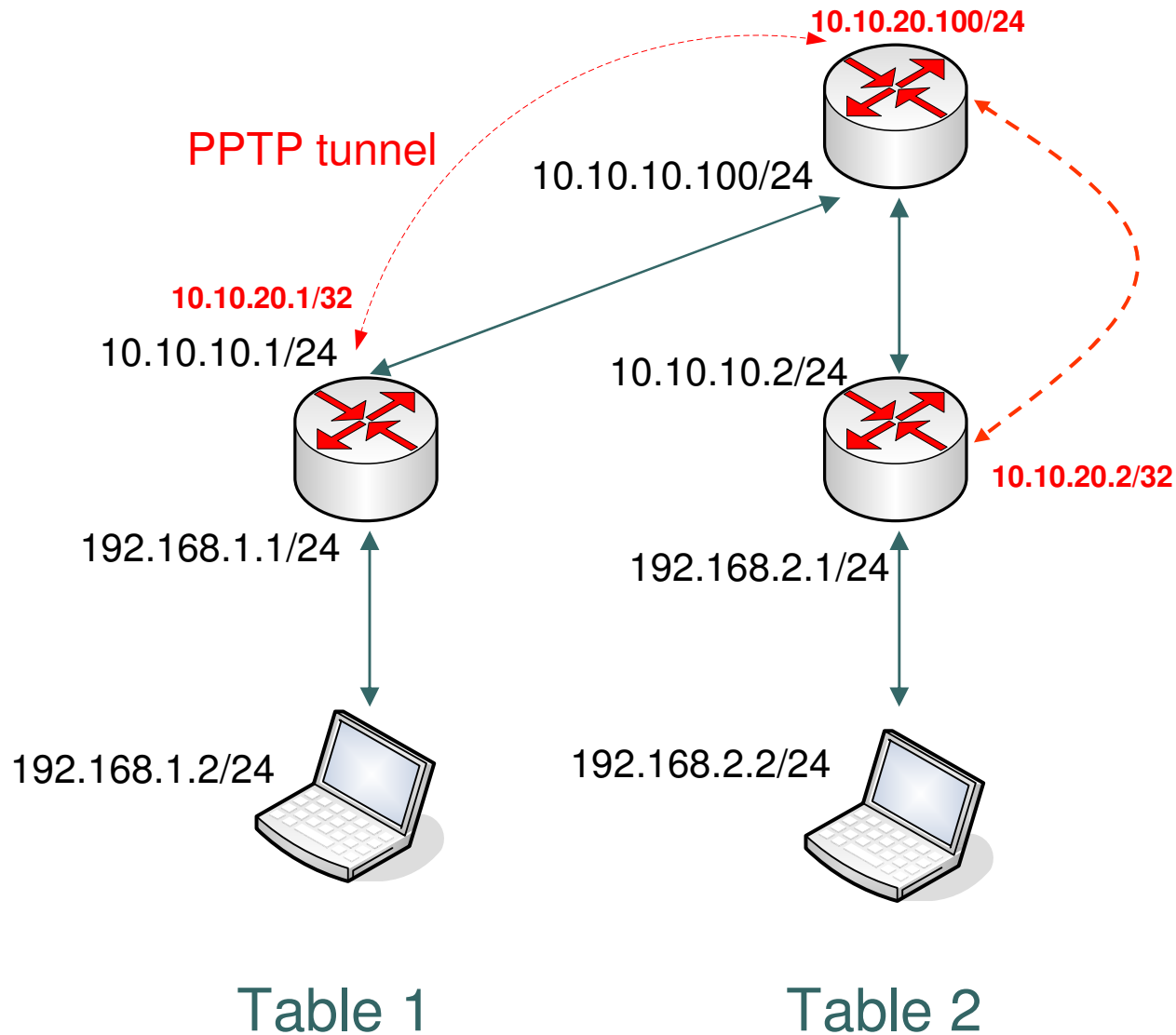
disabled running disabled running



PPTP Client Configuration

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

[LAB] PPTP Tunnels - Client



[LAB] PPTP Tunnels - Client

The screenshot displays a network configuration tool with two windows. The 'Interface List' window shows a tree view of interface types, with 'PPTP Client' selected. The 'New Interface' dialog box is open, showing the configuration for a PPTP Client. The 'Connect To' field is set to '10.10.10.100', the 'User' is 'user1', and the 'Password' is masked with '*****'. The 'Profile' is set to 'default-encryption'. The 'Allow' section has checkboxes for 'pap', 'mschap1', 'chap', and 'mschap2', all of which are checked. The 'Status' field at the bottom is set to 'disabled'.

Interface	Type
EoIP Tunnel	Ethernet
IP Tunnel	Ethernet
VLAN	Ethernet
VRRP	Ethernet
Bonding	Ethernet
Bridge	Ethernet
VPLS	
PPP Server	
PPP Client	
PPTP Server	
PPTP Client	
L2TP Server	
L2TP Client	
OVPN Server	
OVPN Client	
PPPoE Server	
PPPoE Client	
ISDN Server	
ISDN Client	

New Interface

General | Dial Out | Status | Traffic

Connect To: 10.10.10.100

User: user1

Password: *****

Profile: default-encryption

Add Default Route

Allow

pap chap

mschap1 mschap2

disabled | running | slave | Status:

● ● ● | [LAB] PPTP Tunnels - Client

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

- Membuat PPTP-Client Interface :

```
•/interface pptp-client add name=pptp-out1  
connect-to=10.10.10.100 user=user1 password=user1
```

PPTP Server Configuration

The screenshot displays the PPP configuration interface. The main window has tabs for Interface, PPPoE Servers, Secrets, Profiles, and Active Connections. Below the tabs is a toolbar with icons for adding, deleting, and filtering items. A table lists server types: PPTP Server, L2TP Server, and VPN Server. The PPTP Server tab is selected, and its configuration dialog is open. The dialog shows the following settings:

- Enabled
- Max MTU: 1460
- Max MRU: 1460
- MRRU: [empty]
- Keepalive Timeout: 30
- Default Profile: profile-pptp
- Authentication options:
 - pap
 - chap
 - mschap1
 - mschap2

Buttons for OK, Cancel, and Apply are visible on the right side of the dialog. The status bar at the bottom of the main window indicates "0 items out of 6".

● ● ● | PPTP Server Configuration

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

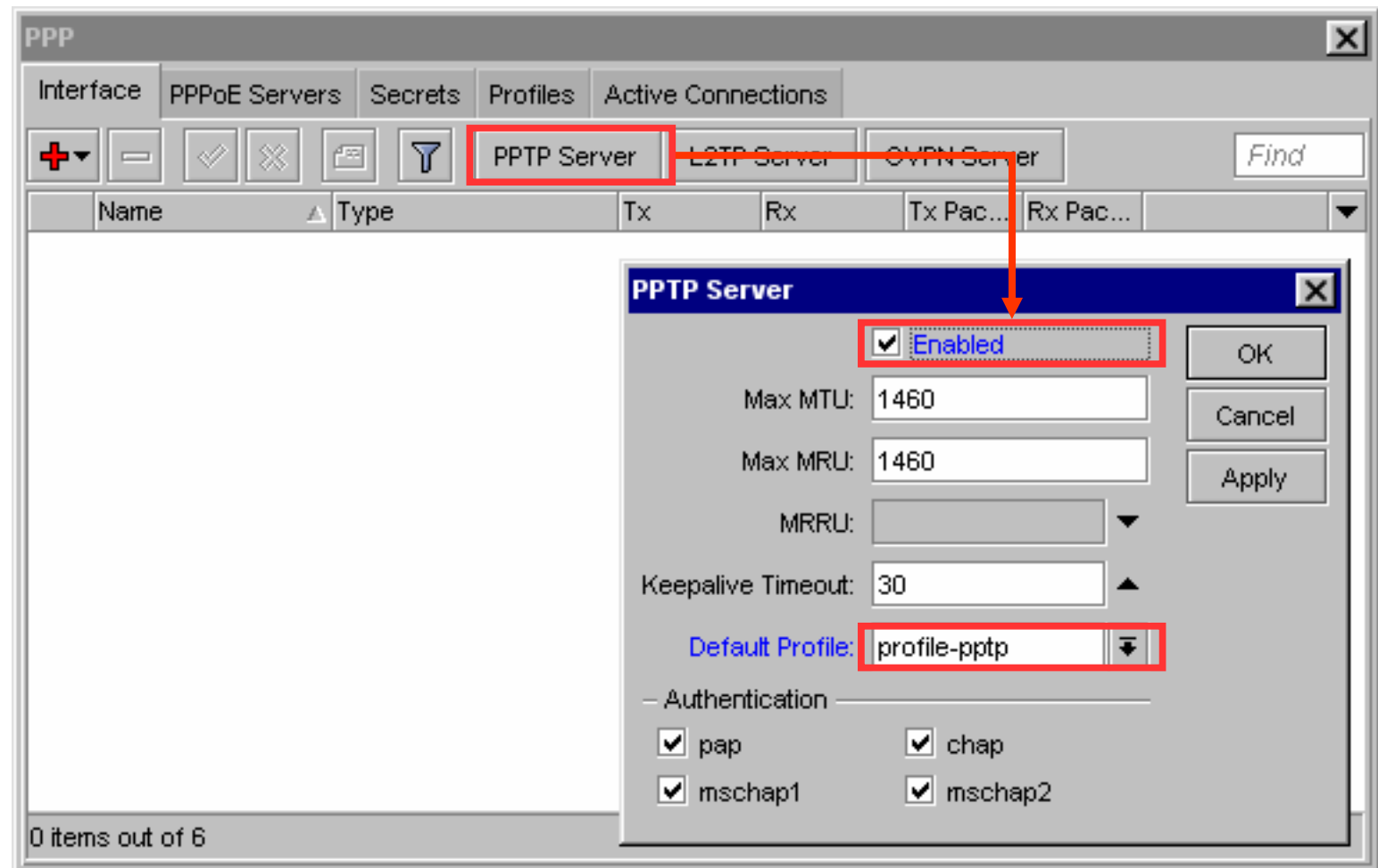
[LAB] PPTP Tunnels - Server

- ● ●
- Buat Pool ip untuk network PPTP terlebih dahulu menggunakan perintah :
 - *"/ip pool add name=pool-pptp ranges=10.200.200.2-10.200.200.254"*
- Buat PPP-Profile untuk network PPTP.
- Tentukan "Local-Address" sebagai IP yang akan dipasang di server.
- Tentukan "Remote-Address" menggunakan "pool-pptp" sebagai ip yang akan dibagikan ke client.

The screenshot shows the 'PPP Profile <profile-pptp>' configuration window. The 'Limits' tab is active. The 'Name' field is 'profile-pptp'. The 'Local Address' is '10.200.200.1'. The 'Remote Address' is 'Pool-pptp'. The 'Bridge' field is empty. The 'Incoming Filter' and 'Outgoing Filter' fields are empty. The 'DNS Server' and 'WINS Server' fields are empty. The 'Use Compression' section has 'default' selected. The 'Use VJ Compression' section has 'default' selected. The 'Use Encryption' section has 'default' selected. The 'Change TCP MSS' section has 'default' selected. The 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove' buttons are visible on the right side.

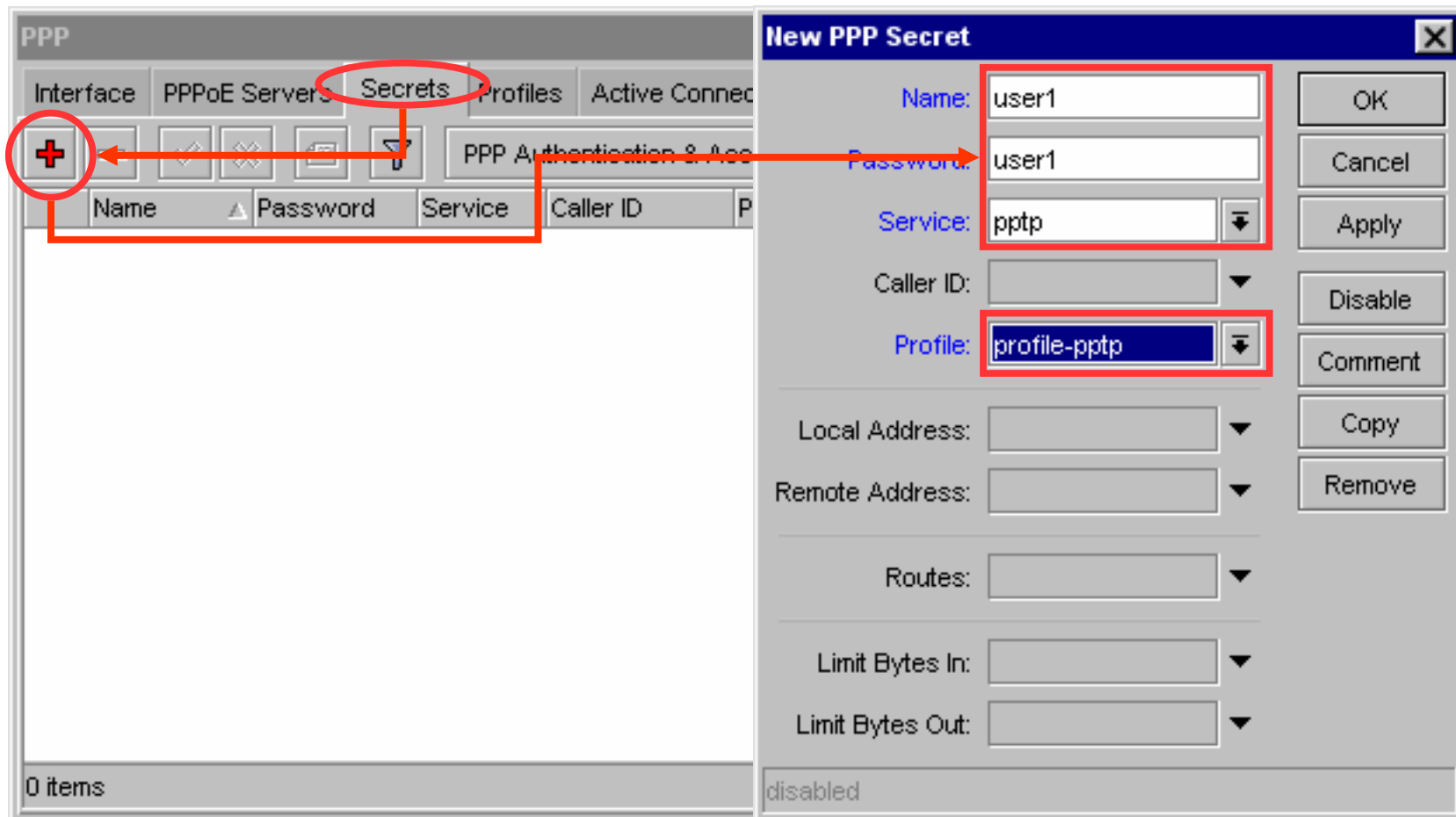
● ● ● | [LAB] PPTP Tunnels - Server

Aktifkan PPTP server, pastikan menggunakan profile “profile-pptp” yang sudah dibuat sebelumnya.



[LAB] PPTP Tunnels - Server

Buat User PPTP di “PPP-Secrets” pastikan menggunakan profile “profile-pptp” supaya user mendapatkan ip sesuai pool yang ada.

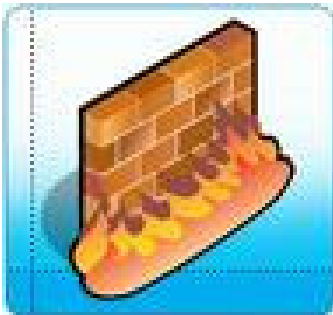


● ● ● | PPP - Secret

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



Firewall



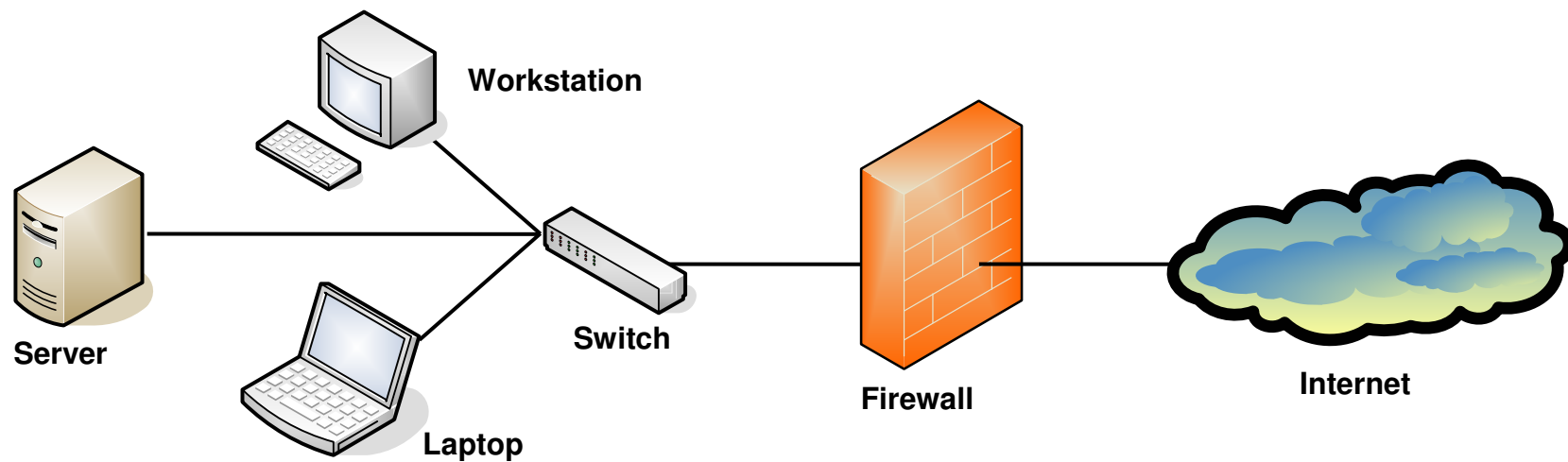
Certified Mikrotik Training Basic Class

Organized by: **Citraweb Nusa Infomedia**

(Mikrotik Certified Training Partner)

Firewall

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





Firewall

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

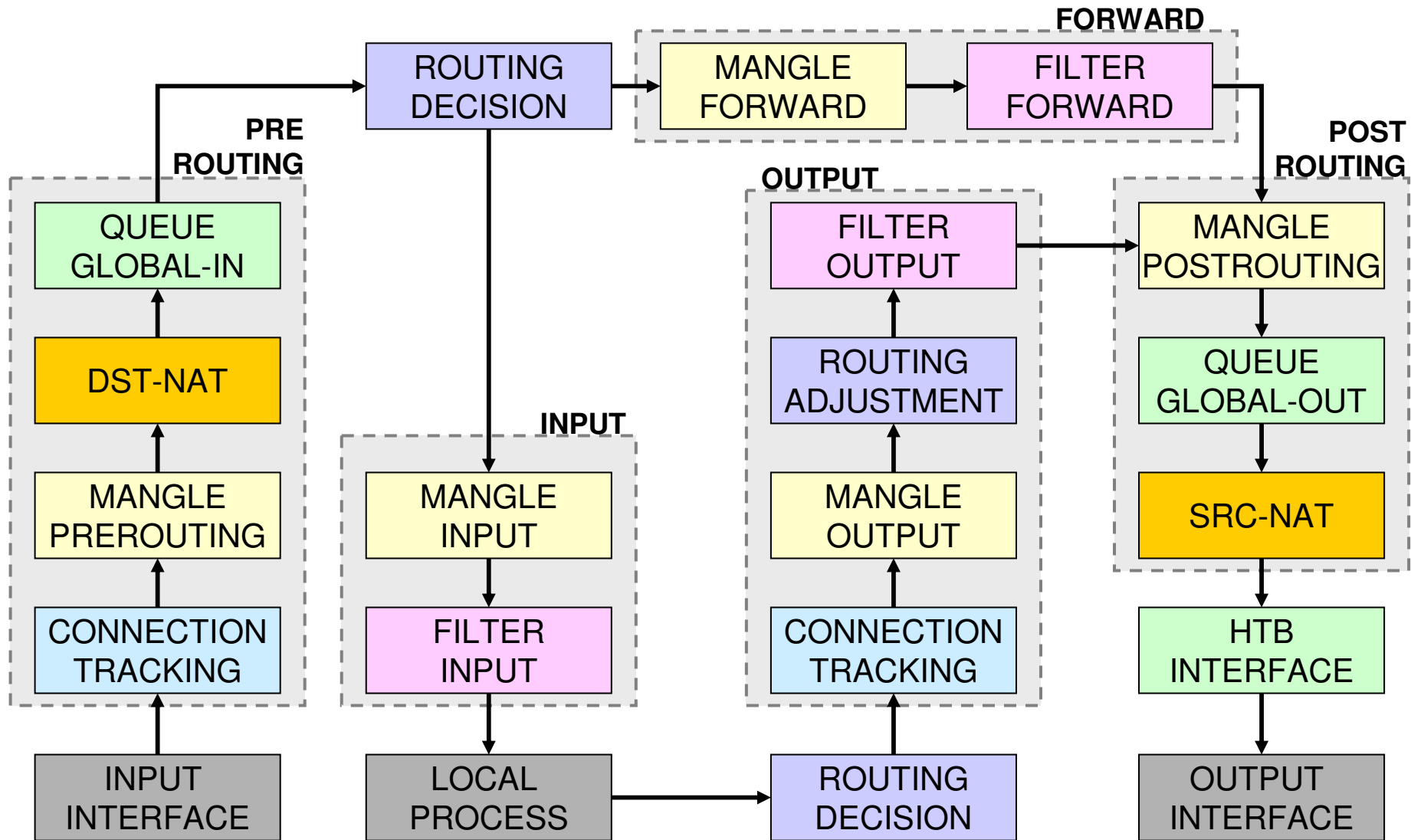


Paket Data

- Setiap paket data memiliki asal (source) dan tujuan (destination)
 - Dari/ke host di luar router
 - Local process (router itu sendiri)



Simple Packet Flow



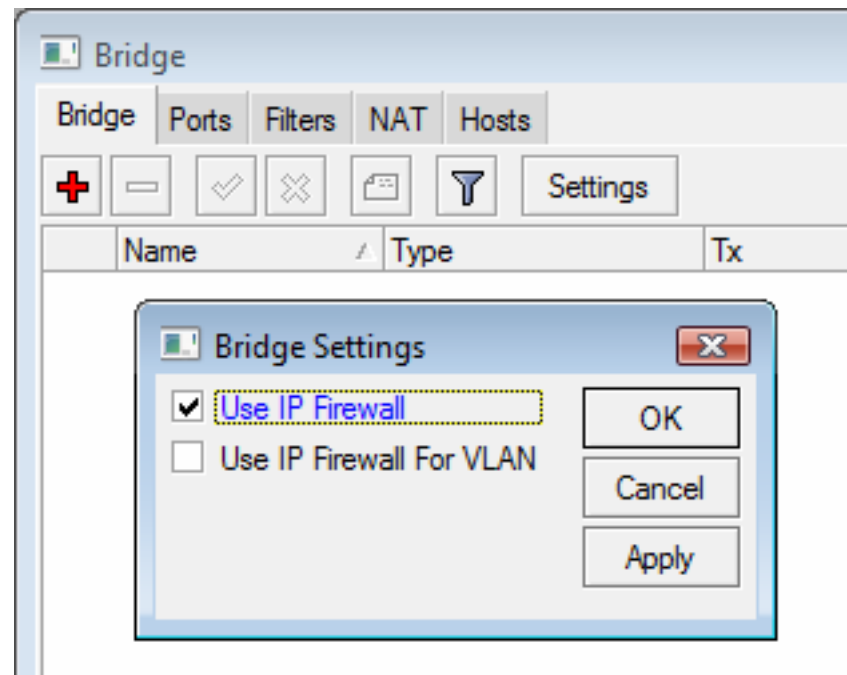


Posisi Chain / Parent

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

● ● ● | Use IP Firewall

- Jika kita mengaktifkan bridge, dan ingin menggunakan firewall filter ataupun mangle, kita harus mengaktifkan setting use ip firewall





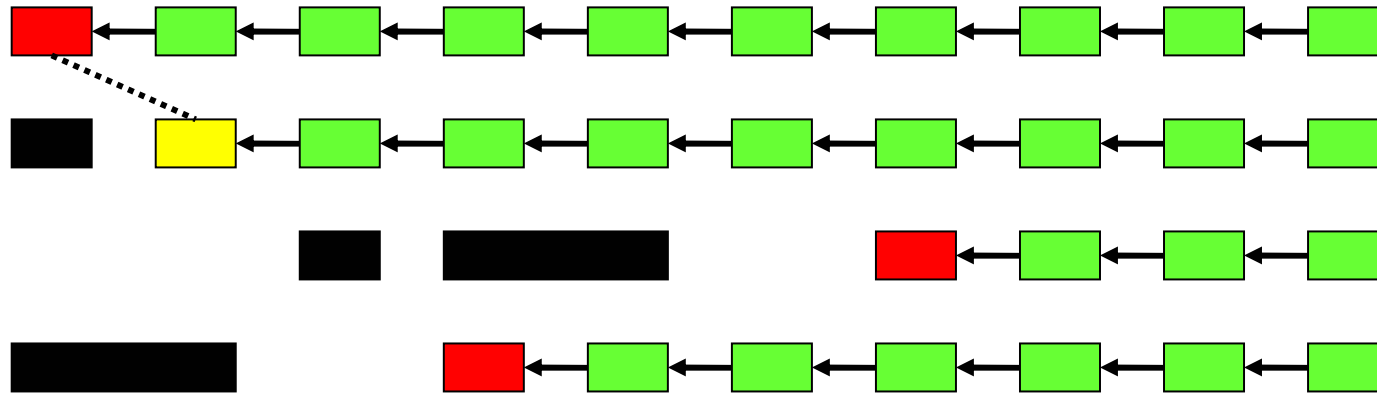
Connection State

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



Connection State

Firewall



New



Established



Related



Invalid

● ● ● | Implikasi Connection State

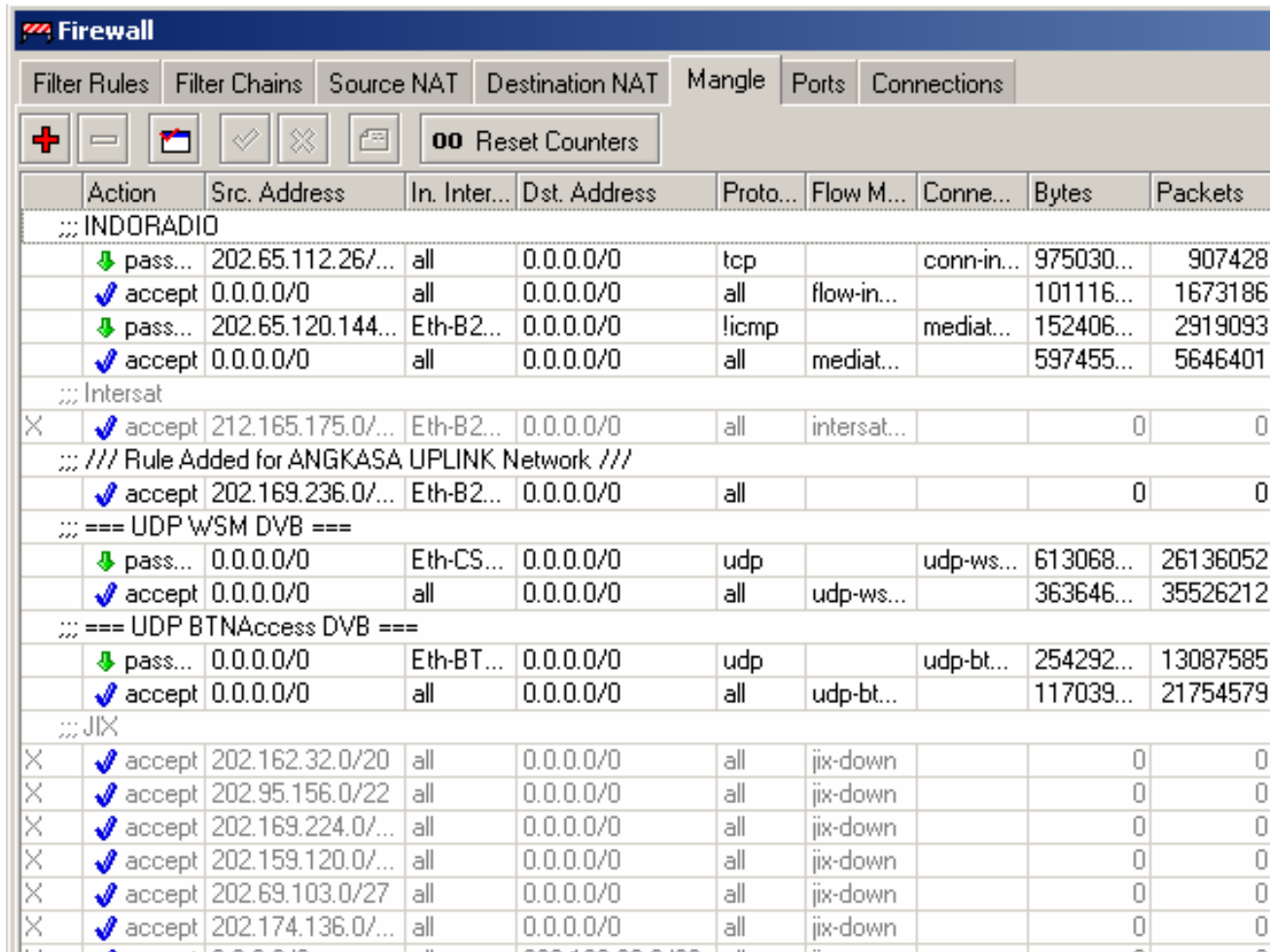
- Pada rule Firewall filter, pada baris paling atas biasanya kita membuat rule :
 - Connection state=invalid → drop
 - Connection state=related → accept
 - Connection state=established → accept
 - Connection state=new → diproses ke rule berikutnya
- Sistem rule seperti ini akan sangat menghemat resources router, karena proses filtering hanya dilakukan pada saat connection dimulai (connection-state=new)



Mangle

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

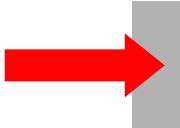


Mangle on Winbox



The screenshot displays the Mikrotik WinBox Firewall configuration interface, specifically the Mangle tab. The interface includes a toolbar with icons for adding, deleting, and applying rules, along with a 'Reset Counters' button. The main area contains a table of firewall rules, each with a status icon (green arrow for pass, blue checkmark for accept, red X for deny) and various configuration parameters.

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

Chain pada mangle

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

- ● ● |

Type of Mark

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

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



Connection Mark

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



Passthrough

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

- ● ● | [LAB-1] Mangle dgn SRC-NAT

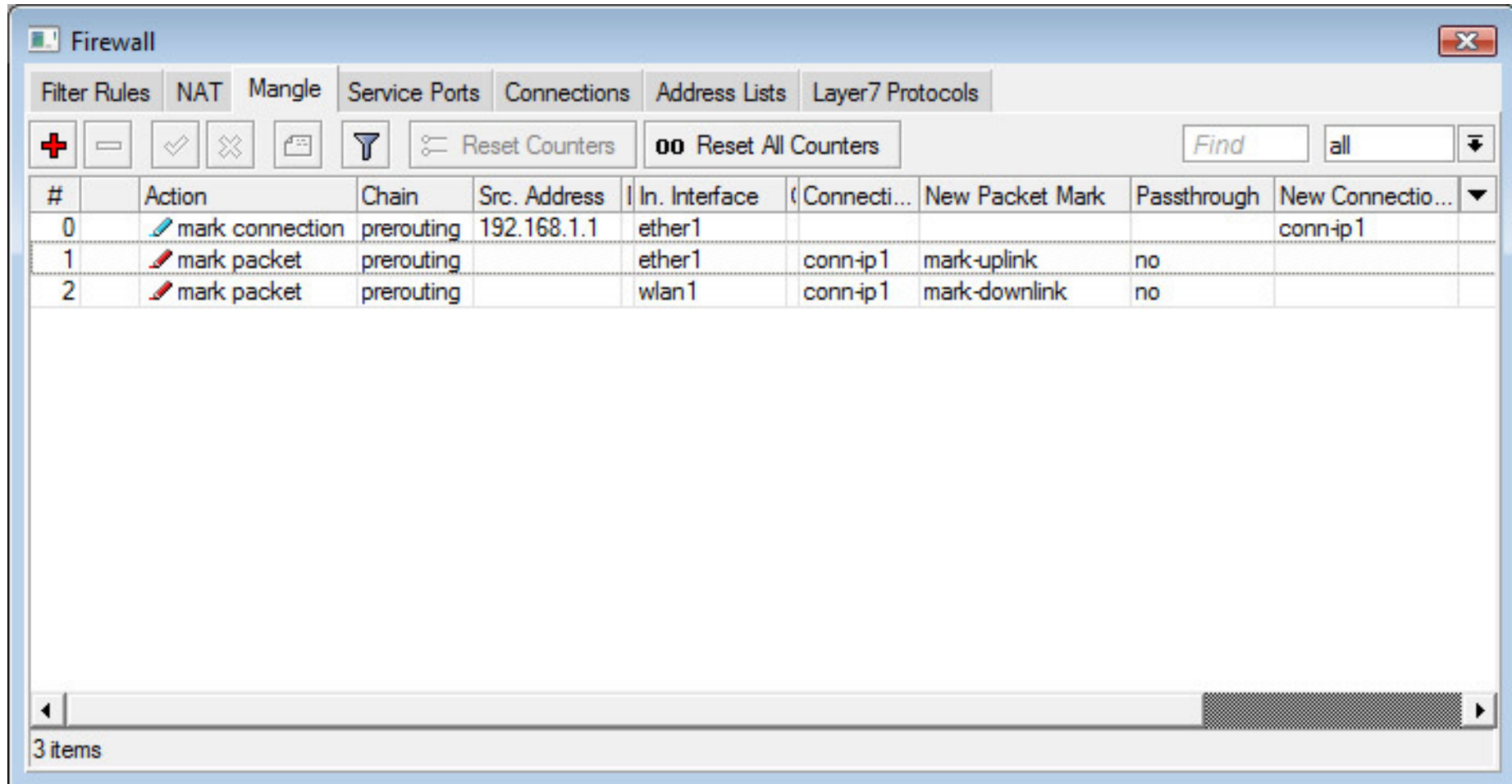
- Uplink traffic
 - add src-address=192.168.0.2/32
action=mark-packet chain=prerouting
new-packet-mark=mark-uplink
- Downlink traffic
 - add dst-address=192.168.0.2/32
action=mark-packet chain=prerouting
new-packet-mark=mark-downlink
- **NOT WORK for downlink traffic!**

- ● ● |




Mangle dengan SRC NAT

- Karena urutan proses NAT dan mangle, maka kita harus menggunakan conn-mark jika kita ingin membuat mangle untuk menandai proses uplink dan downlink IP tertentu.

Mark-Conn & Mark-Packet



The screenshot shows the Mikrotik WinBox Firewall configuration window, specifically the Connections tab. The window title is "Firewall". The tabs at the top are Filter Rules, NAT, Mangle, Service Ports, Connections, Address Lists, and Layer7 Protocols. The Connections tab is active, showing a table of connection rules. The table has columns for #, Action, Chain, Src. Address, In. Interface, (Connecti..., New Packet Mark, Passthrough, and New Connectio... (with a dropdown arrow). There are three rows of data. Below the table is a scrollbar and a status bar indicating "3 items".

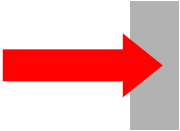

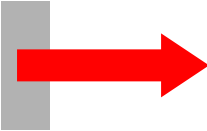
#	Action	Chain	Src. Address	In. Interface	(Connecti...	New Packet Mark	Passthrough	New Connectio...
0	 mark connection	prerouting	192.168.1.1	ether1				conn-ip1
1	 mark packet	prerouting		ether1	conn-ip1	mark-uplink	no	
2	 mark packet	prerouting		wlan1	conn-ip1	mark-downlink	no	



Firewall Filters

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

Chain pada Filter

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



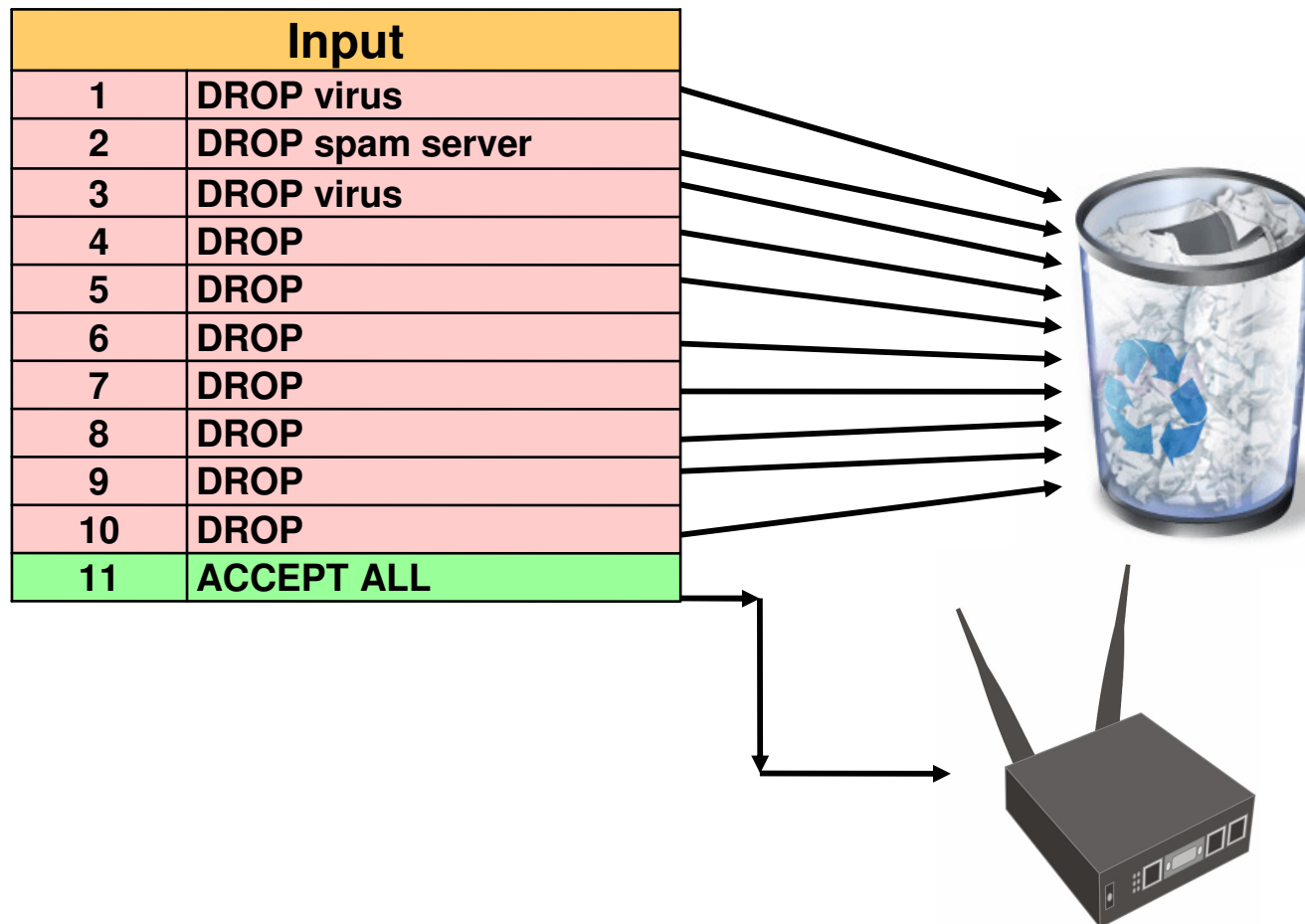
Action Filter (1)

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



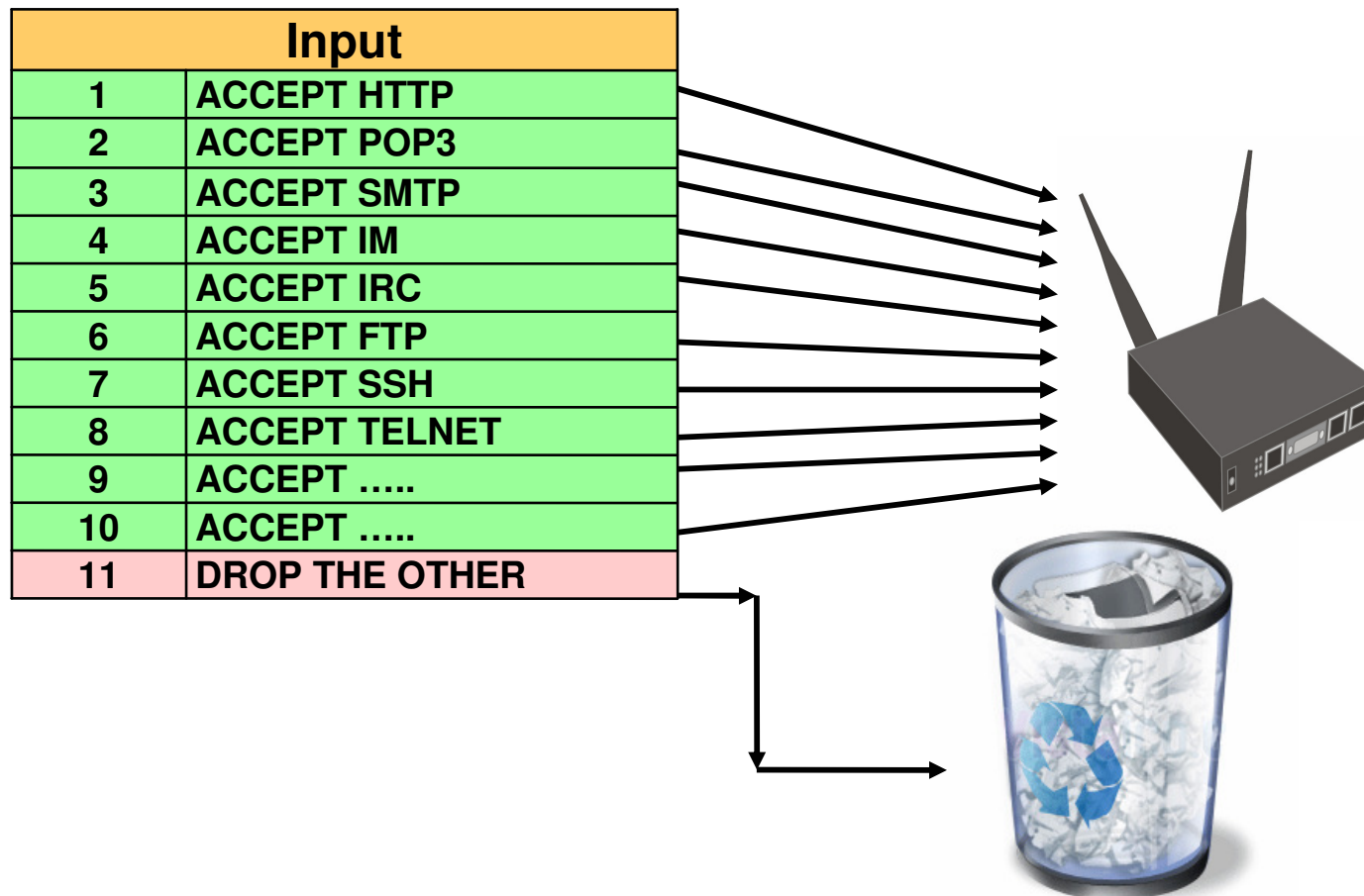
Firewall Tactics (1)

Drop all unneeded, accept everything else



Firewall Tactics (2)

Accept only needed, drop everything else



Filter Rules

The screenshot shows the Mikrotik WinBox v3.2 interface. The title bar reads "admin@00:0C:42:1B:5C:C1 (MikroTik) - WinBox v3.2 on RB500R5 (mipsle)". The left sidebar contains a tree view with categories: Interfaces, Wireless, Bridge, PPP, IP, Routing, Ports, Queues, Drivers, System, Files, Log, SNMP, and Users. The "IP" category is expanded, showing sub-items: Addresses, Routes, Pool, ARP, Firewall, Socks, UPnP, Traffic Flow, Accounting, and Services. The "Firewall" sub-item is circled in red. A red arrow points from the "IP" category to the "Firewall" sub-item. In the main window, the "Firewall" tab is selected, and the "Filter Rules" sub-tab is active. A red circle highlights the "Filter Rules" sub-tab. Another red circle highlights the "+" icon in the toolbar. The "New Firewall Rule" dialog is open, showing the "General" tab. The dialog has fields for Chain (set to "forward"), Src. Address, Dst. Address, Protocol, Src. Port, Dst. Port, Any. Port, P2P, and In. Interface. On the right side of the dialog, there are buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

RouterOS v3 Services

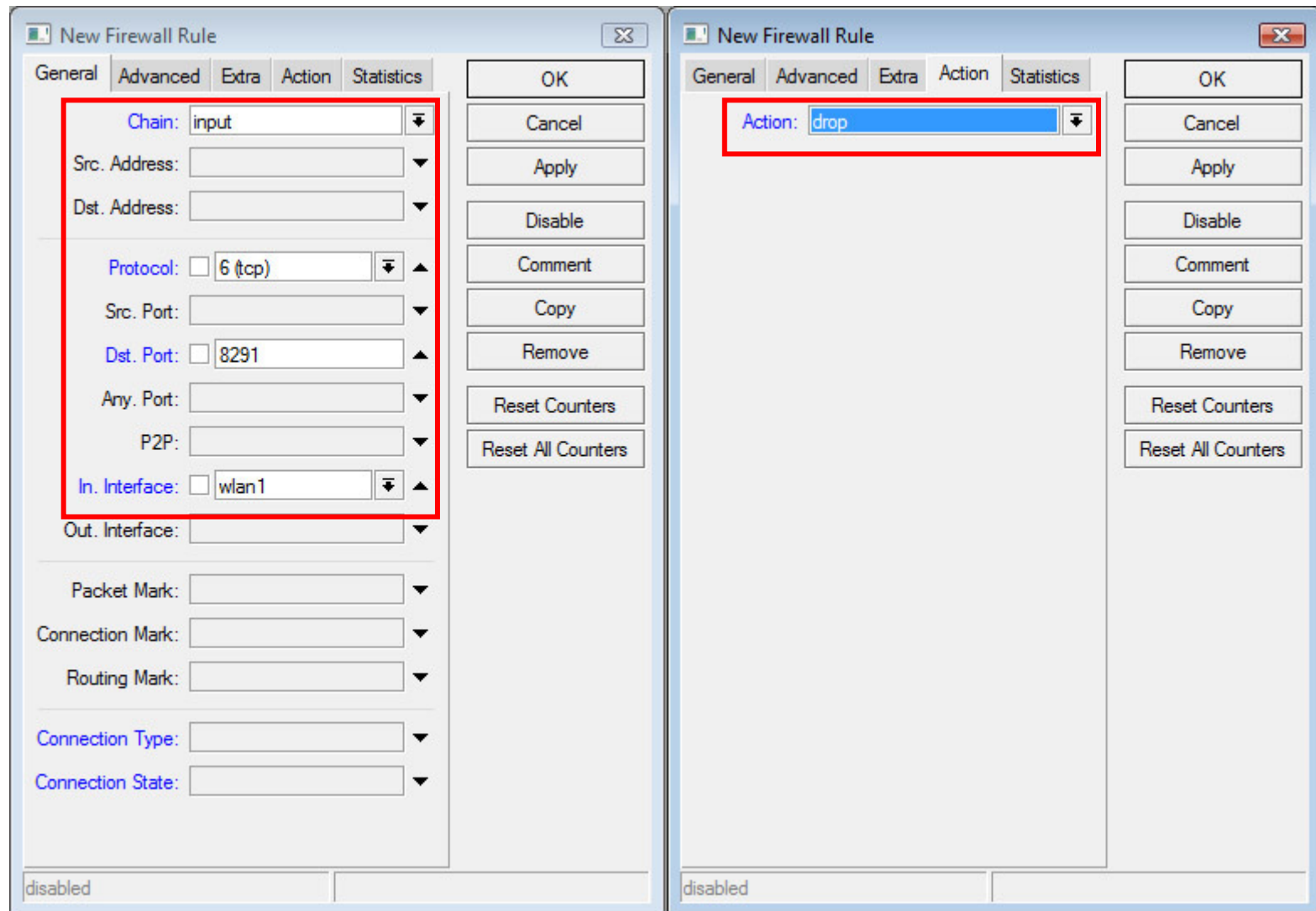
	PORT	PROTOCOL	DESCRIPTION
1	20	tcp	FTP
2	21	tcp	FTP
3	22	tcp	SSH, SFTP
4	23	tcp	Telnet
5	53	tcp	DNS
6	80	tcp	HTTP
7	179	tcp	BGP
8	443	tcp	SHTTP (Hotspot)
9	646	tcp	LDP (MPLS)
10	1080	tcp	SoCKS (Hotspot)
11	1723	tcp	PPTP
12	1968	tcp	MME
13	2000	tcp	Bandwidth Server
14	2210	tcp	Dude Server
15	2211	tcp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

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

- ● ● | [LAB-2] Simple Blocking

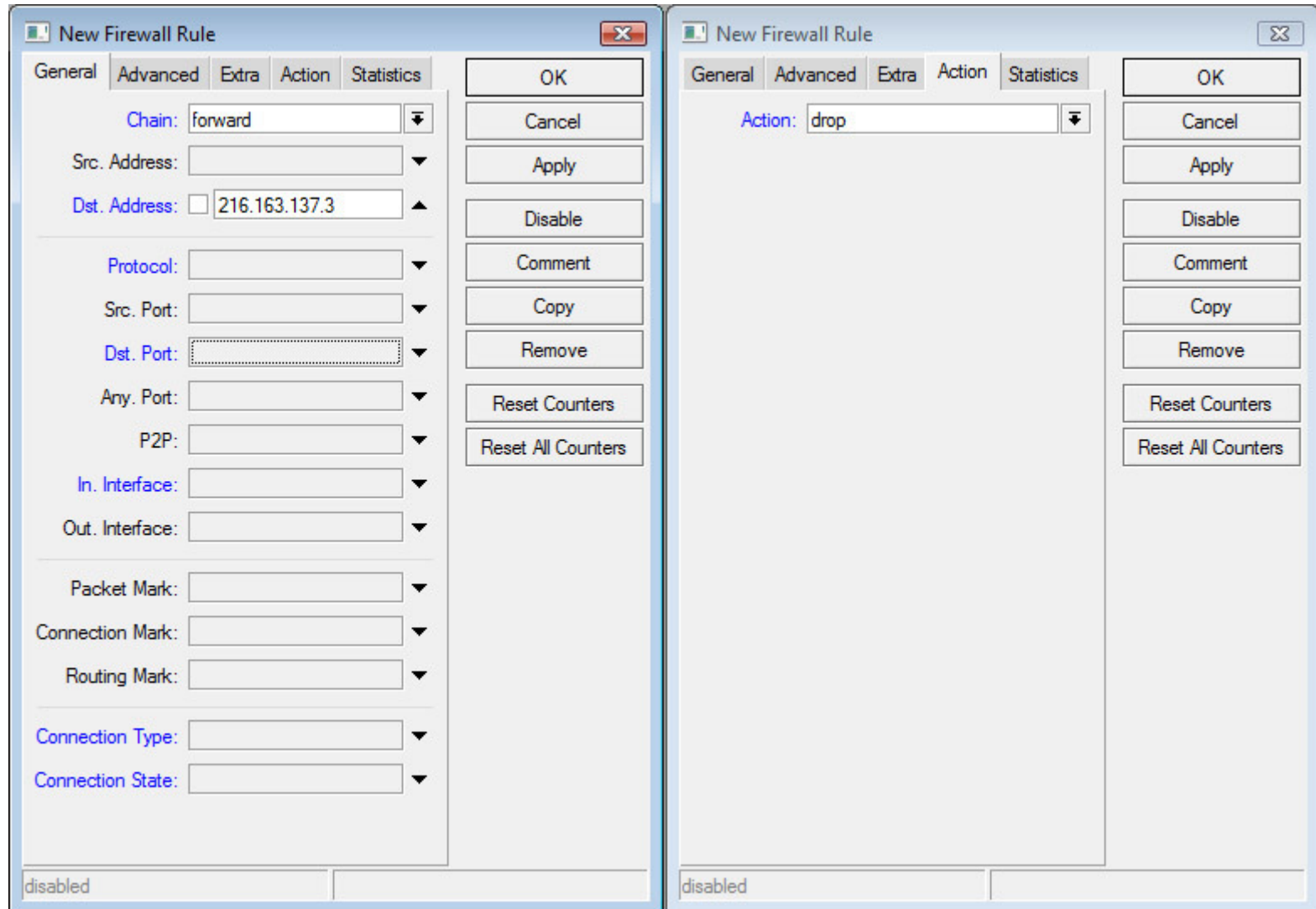
- Blok semua invalid connection ke router
 - Blok koneksi winbox ke router yang masuk melalui interface public (wlan)
 - Blok koneksi ke website:
 - Playboy - 216.163.137.3
 - Penthouse - 64.124.57.235
-

Blok Koneksi Winbox ke Router dari interface publik (wlan)



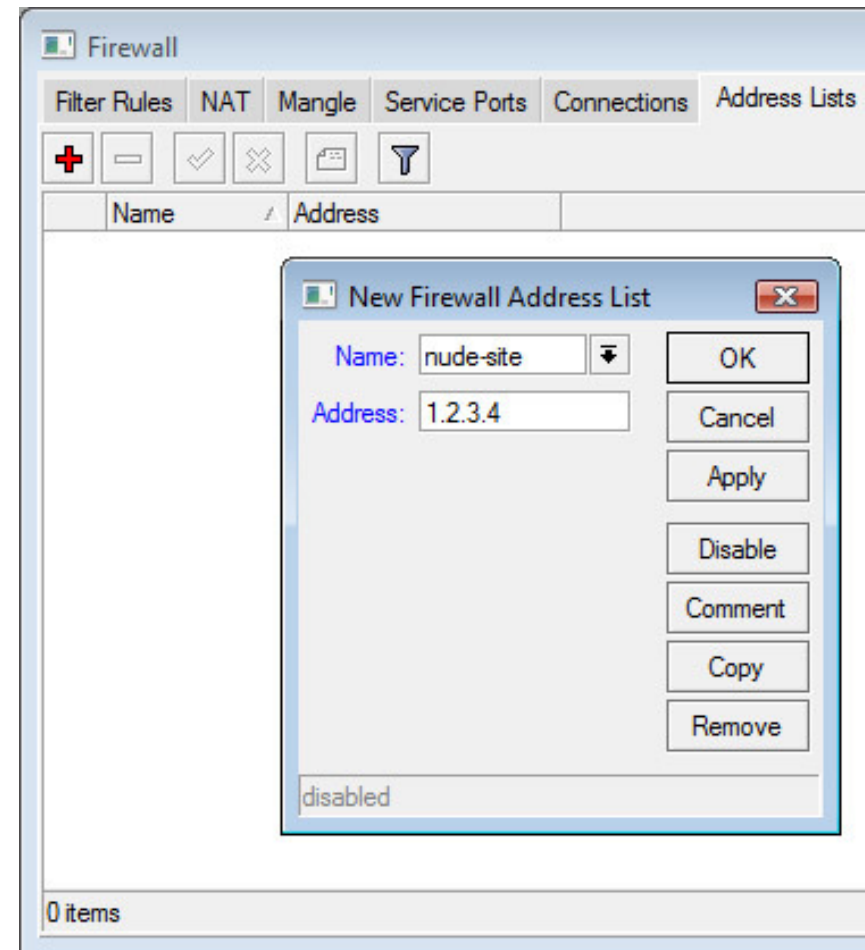


Blok Nude Site



● ● ● | IP Address List

- Kita dapat melakukan pengelompokan IP Address dengan **Address List**
- Address List (seperti halnya mangle) bisa dijadikan parameter dalam pembuatan filter, queue, mangle, NAT, dll.
- Dengan Filter dan Mangle, kita bisa secara otomatis memasukkan IP Address tertentu ke dalam **address list** dan juga menentukan jangka waktu expire nya.





[LAB-3] IP Address List

- Buatlah Mangle yang secara otomatis akan memasukkan src-address mesin yang melakukan ping ke router dan secara otomatis dan setelah 15 detik secara otomatis menghapus IP tersebut dari address-list.
 - Pada Filter, buatlah sebuah filter yang melakukan blok terhadap koneksi dari IP Address yang berada dalam address-list.
-



Memasukkan ke Address-List

The image displays two screenshots of the Mikrotik WinBox Firewall Rule configuration interface.

Left Window: New Firewall Rule

- Chain: input
- Src. Address: [Empty]
- Dst. Address: [Empty]
- Protocol: 1 (icmp)
- Src. Port: [Empty]
- Dst. Port: [Empty]
- Any. Port: [Empty]
- P2P: [Empty]
- In. Interface: [Empty]
- Out. Interface: [Empty]
- Packet Mark: [Empty]
- Connection Mark: [Empty]
- Routing Mark: [Empty]
- Connection Type: [Empty]
- Connection State: [Empty]

Right Window: Firewall Rule <>

- Action: add src to address list
- Address List: doing-ping
- Timeout: 00:00:15

Both windows have a 'General' tab selected and show a 'disabled' status at the bottom left. The right window also shows a '<>' icon in the title bar.



The screenshot shows the Mikrotik WinBox Firewall configuration window. The 'Address Lists' tab is active, displaying a table of address lists:

	Name	Address
	● auto-blok	0.0.0.0
D	● doing-ping	192.168.0.4
D	● doing-ping	202.65.112.18

Below the table is a command prompt window titled 'C:\WINNT\system32\cmd.exe - ping 192.168.0.100'. The prompt shows the following output:

```
C:\Documents and Settings\valens>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time<10ms TTL=64
Reply from 192.168.0.100: bytes=32 time<10ms TTL=64
Reply from 192.168.0.100: bytes=32 time<10ms TTL=64
Reply from 192.168.0.100: bytes=32 time<10ms TTL=64

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\valens>
C:\Documents and Settings\valens>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time<10ms TTL=64
Reply from 192.168.0.100: bytes=32 time<10ms TTL=64
```

Blok IP di Address-List

The image displays the Mikrotik WinBox Firewall Rule configuration interface. On the left, a 'Firewall Rule <>' window is shown with the 'General' tab selected. The 'Chain' is set to 'input'. Below this, there are fields for 'Src. Address', 'Dst. Address', 'Protocol', 'Src. Port', 'Dst. Port', 'Any. Port', 'P2P', 'In. Interface', 'Out. Interface', 'Packet Mark', 'Connection Mark', 'Routing Mark', 'Connection Type', and 'Connection State'. The status at the bottom is 'disabled'.

Two 'New Firewall Rule' dialog boxes are overlaid on the right. The top dialog has the 'General' tab selected, with 'Src. Address List' set to 'doing-ping'. The bottom dialog has the 'Action' tab selected, with 'Action' set to 'drop'. Both dialog boxes feature a vertical stack of buttons on the right: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.



[LAB-4] Proteksi Mac Address

- Buatlah Firewall Filter untuk memproteksi sehingga mac-address tertentu hanya bisa menggunakan IP Address tertentu, dan juga sebaliknya.
 - Lakukan Accept pada Filter untuk setiap pasangan IP Address dan Mac Address pada in/out-interface tertentu.
 - Pada baris paling akhir, blok koneksi lainnya.
-

Filter untuk Setiap IP dan Mac

The image displays three screenshots of the Mikrotik WinBox Firewall Rule configuration interface, illustrating the setup for a rule that filters traffic based on IP and MAC address.

Firewall Rule <192.168.1.2> (General Tab):

- Chain: forward
- Src. Address: 192.168.1.2
- Protocol: (empty)
- Src. Port: (empty)
- Dst. Port: (empty)
- Any. Port: (empty)
- P2P: (empty)
- In. Interface: ether1
- Out. Interface: wlan1

Firewall Rule <192.168.1.2> (Advanced Tab):

- Src. Address List: (empty)
- Dst. Address List: (empty)
- Layer7 Protocol: (empty)
- Content: (empty)
- Connection Bytes: (empty)
- Src. MAC Address: AA:BB:CC:DD:EE:FF
- Out. Bridge Port: (empty)
- In. Bridge Port: (empty)
- Ingress Priority: (empty)
- DSCP (TOS): (empty)
- TCP MSS: (empty)
- Packet Size: (empty)
- Random: (empty)
- TCP Flags: (expanded)
- IPv4 Options: (empty)
- ICMP Options: (expanded)

New Firewall Rule (General Tab):

- Action: accept

Red boxes highlight the Chain, Src. Address, In. Interface, Src. MAC Address, and Action fields. Red arrows indicate the flow of configuration from the General tab to the Advanced tab and then to the New Firewall Rule window.

Blok Trafik Lainnya

Firewall Rule <192.168.1.2>

General Advanced Extra Action Statistics

Chain: forward

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface: ether1

Out. Interface: wlan1

Packet Mark:

Connection Mark:

Routing Mark:

Connection Type:

Connection State:

disabled

New Firewall Rule

General Advanced Extra Action Statistics

Action: drop

disabled

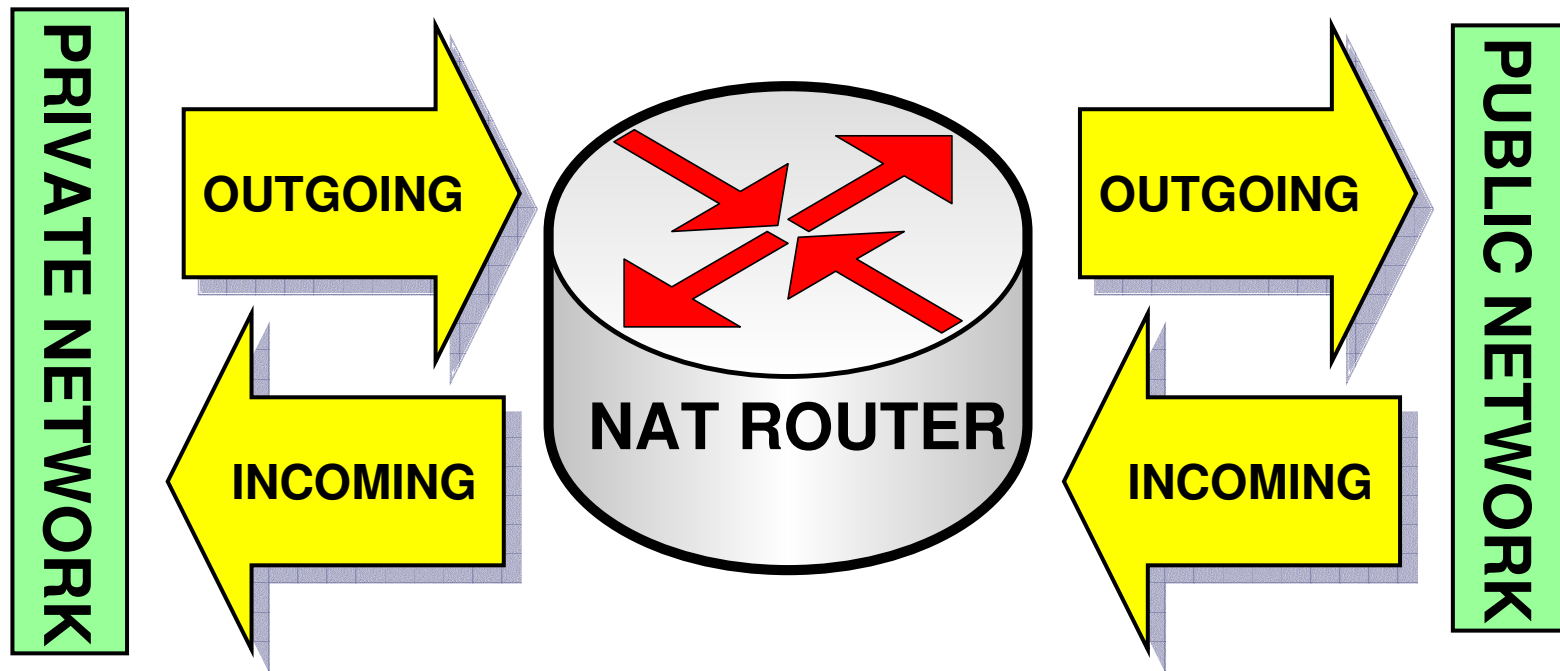
- o Buatlah rule berikut ini pada akhir rule untuk memblokir koneksi lainnya

- ● ● |

Network Address Translation (NAT)

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

Firewall NAT



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

Firewall NAT

The screenshot displays the Mikrotik WinBox v3.2 interface on an RB500R5 device. The main window is titled "admin@00:0C:42:1B:5C:C1 (MikroTik) - WinBox v3.2 on RB500R5 (mipsle)".

The left sidebar contains a tree view of system settings. The "IP" menu item is circled in red. A sub-menu is open under "IP", and the "Firewall" option is also circled in red. Other options in the sub-menu include Addresses, Routes, Pool, ARP, Socks, UPnP, Traffic Flow, Accounting, Services, Packing, Neighbors, DNS, Web Proxy, DHCP Client, and DHCP Server.

The main window shows the "Firewall" configuration page. The "NAT" tab is selected and circled in red. A red circle highlights the "+" button used to add a new rule. Below the tabs, a table lists existing NAT rules, with one rule named "mas..." visible.

The "NAT Rule <>" dialog box is open, showing the configuration for a new rule. The "Chain" is set to "srcnat" and the "Out. Interface" is set to "wlan1". The "General" tab is active, and the "Action" tab is also visible. The dialog includes fields for Src. Address, Dst. Address, Protocol, Src. Port, Dst. Port, Any. Port, In. Interface, Out. Interface, Packet Mark, Connection Mark, Routing Mark, and Connection Type. Buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters are located on the right side of the dialog.



src-nat and masquerade

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

- ● ● | **dst-nat and redirect**

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

- ● ● | [LAB-5] dst-nat & local proxy

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

Mengaktifkan Web-Proxy

The screenshot displays the Mikrotik WinBox v3.2 interface for configuring the Web Proxy. The left sidebar shows the navigation menu with 'IP' and 'Web Proxy' highlighted. The main window shows the 'Web Proxy' configuration page with the 'Web Proxy Settings' dialog open. The 'Enabled' checkbox is checked, and the 'Port' is set to 3128. The 'Src. Address' field is also visible.

admin@00:0C:42:1B:5C:C1 (MikroTik) - WinBox v3.2 on RB500R5 (mipsle)

Web Proxy

Access Cache Direct Connections

Reset Counters Reset All Counters Web Proxy Settings

IP

Addresses

Routes

Pool

ARP

Firewall

Socks

UPnP

Traffic Flow

Accounting

Services

Packing

Neighbors

DNS

Web Proxy

DHCP Client

DHCP Server

DHCP Relay

Hotspot

IPsec

Web Proxy Settings

General Status Lookups Inserts

Enabled

Src. Address: []

Port: 3128

Parent Proxy: []

Parent Proxy Port: []

Cache Drive: system

Cache Administrator: webmaster

Max. Cache Size: none KB

Cache On Disk

Max. Client Connections: 600

Max. Server Connections: 600

Max Fresh Time: 3d 00:00:00

Serialize Connections

Always From Cache

Cache Hit DSCP (TOS): 4

running

Redirect TCP-80

The image displays two screenshots of Mikrotik WinBox NAT rule configuration windows. The left window, titled "NAT Rule <80>", shows the configuration for an existing rule. The right window, titled "New NAT Rule", shows the configuration for a new rule.

NAT Rule <80> Configuration:

- Chain: dstnat
- Src. Address: (empty)
- Dst. Address: (empty)
- Protocol: 6 (tcp)
- Src. Port: (empty)
- Dst. Port: 80
- Any. Port: (empty)
- In. Interface: ether1
- Out. Interface: (empty)
- Packet Mark: (empty)
- Connection Mark: (empty)
- Routing Mark: (empty)
- Connection Type: (empty)

New NAT Rule Configuration:

- Action: redirect
- To Ports: 3128

Both windows have a "disabled" status at the bottom. The right window includes a vertical stack of buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.



Last Issue

- Firewall Filter hanya melakukan filter pada komunikasi layer 3, dan tidak memfilter layer 2, seperti komunikasi mac-winbox dan mac-telnet.
 - Untuk interface yang berhadapan dengan public, seperti pada internet exchange, atau public DHCP, matikanlah fitur mac-server pada interface tersebut.
-

Mematikan Fitur Mac-Server

The image shows a screenshot of the RouterOS WinBox interface. On the left, a vertical menu lists various tools and features. The 'Tools' menu is expanded, showing a list of options including 'MAC Server'. The 'MAC Server' window is open, displaying a configuration interface with tabs for 'Telnet Interfaces', 'WinBox Interfaces', and 'Active Sessions'. The 'WinBox Interfaces' tab is active, showing a table with one row labeled 'all' under the 'Interface' column. The status bar at the bottom of the window indicates '1 item (1 selected)'. The RouterOS WinBox logo is visible on the left side of the interface.

RouterOS WinBox

Radius

Tools

New Terminal

Telnet

Password

Certificates

Make Supout.rif

Manual

Exit

Ping

Traceroute

Bandwidth Test

BTest Server

Traffic Monitor

Packet Sniffer

Torch

MAC Server

Graphing

Email

IP Scan

Ping Speed

Flood Ping

Netwatch

MAC Server

Telnet Interfaces WinBox Interfaces Active Sessions

+ - ✓ ✗

MAC Ping Server Find

Interface

all

1 item (1 selected)



Daftar Protokol dan Port yang Sebaiknya Ditutup

Karena Virus, Spyware, dll

● ● ● | Block Bogus IP Address

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



Separate Protocol into Chains

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

Blocking UDP Packet

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

Only needed icmp codes in icmp chain

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




Deny Some TCP Ports

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



Virus and Worms (1)

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

Virus and Worms (2)

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



Quality of Service

Certified Mikrotik Training Basic Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)



Quality of Service

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



Quality of Service

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



Simple Queue

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

Simple Queue Menu

New Simple Queue

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

Name:

Target Address:

Target Upload Target Download

Max Limit: bits/s

Burst

Burst Limit: bits/s

Burst Threshold: bits/s

Burst Time: s

Time

Time: -

sun mon tue wed thu fri sat

disabled

OK
Cancel
Apply
Disable
Copy
Remove

Simple Queue Advance Menu

New Simple Queue

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

P2P:

Packet Mark:

Dst. Address:

Interface:

Target Upload: Limit At: bits/s

Target Download: Limit At: bits/s

Queue Type:

Parent:

Priority:

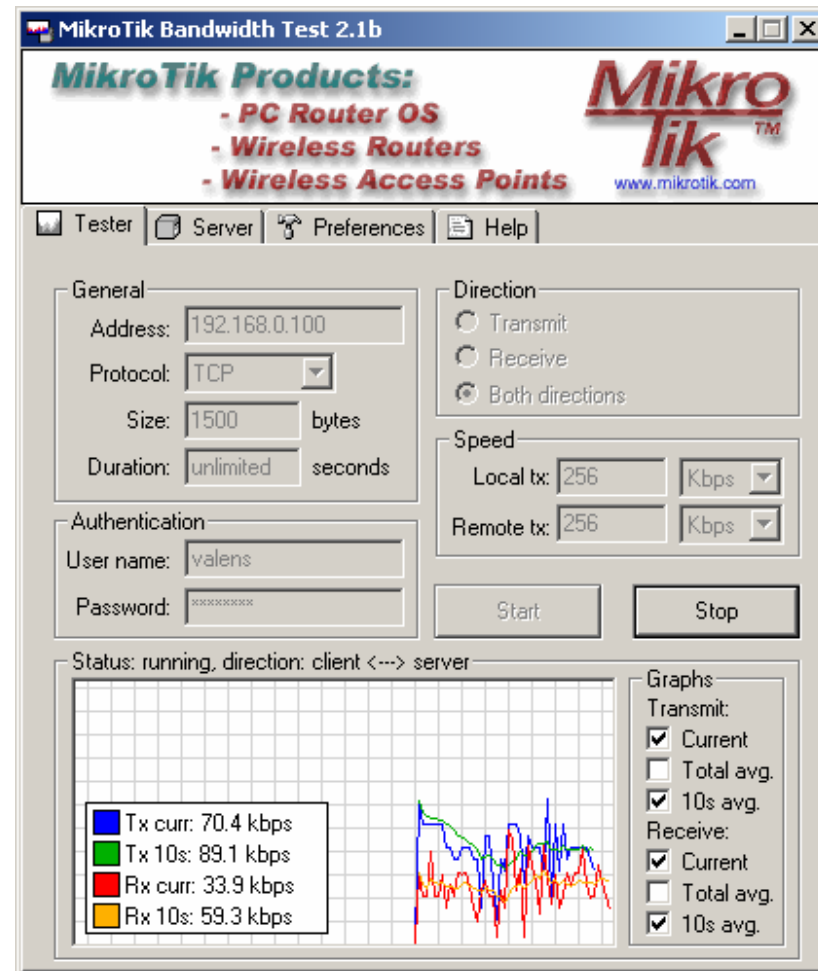
disabled

OK
Cancel
Apply
Disable
Copy
Remove

Interface adalah port di mana client terkoneksi ke router

Simple Queue - Test

- Monitor the result using bandwidth application



- ● ● | [LAB] Simple Queue 1

- Make a simple queue for your laptop
 - Downstream : 128 kbps
 - Upstream : 64 kbps
- Try Using Time
- Try Using Interface and P2P





Staged Limitation

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

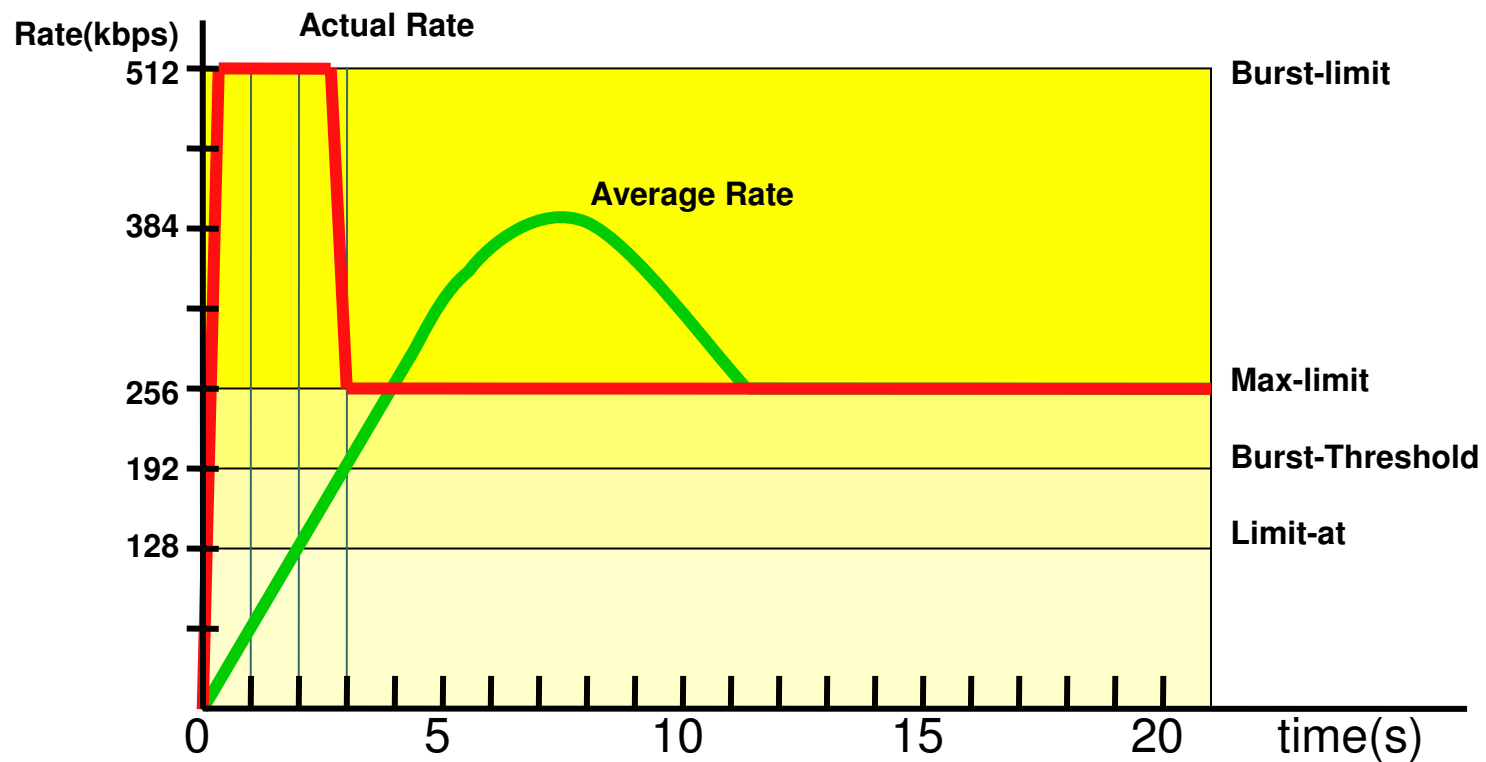


Burst

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

● ● ● | Contoh Burst (1)

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

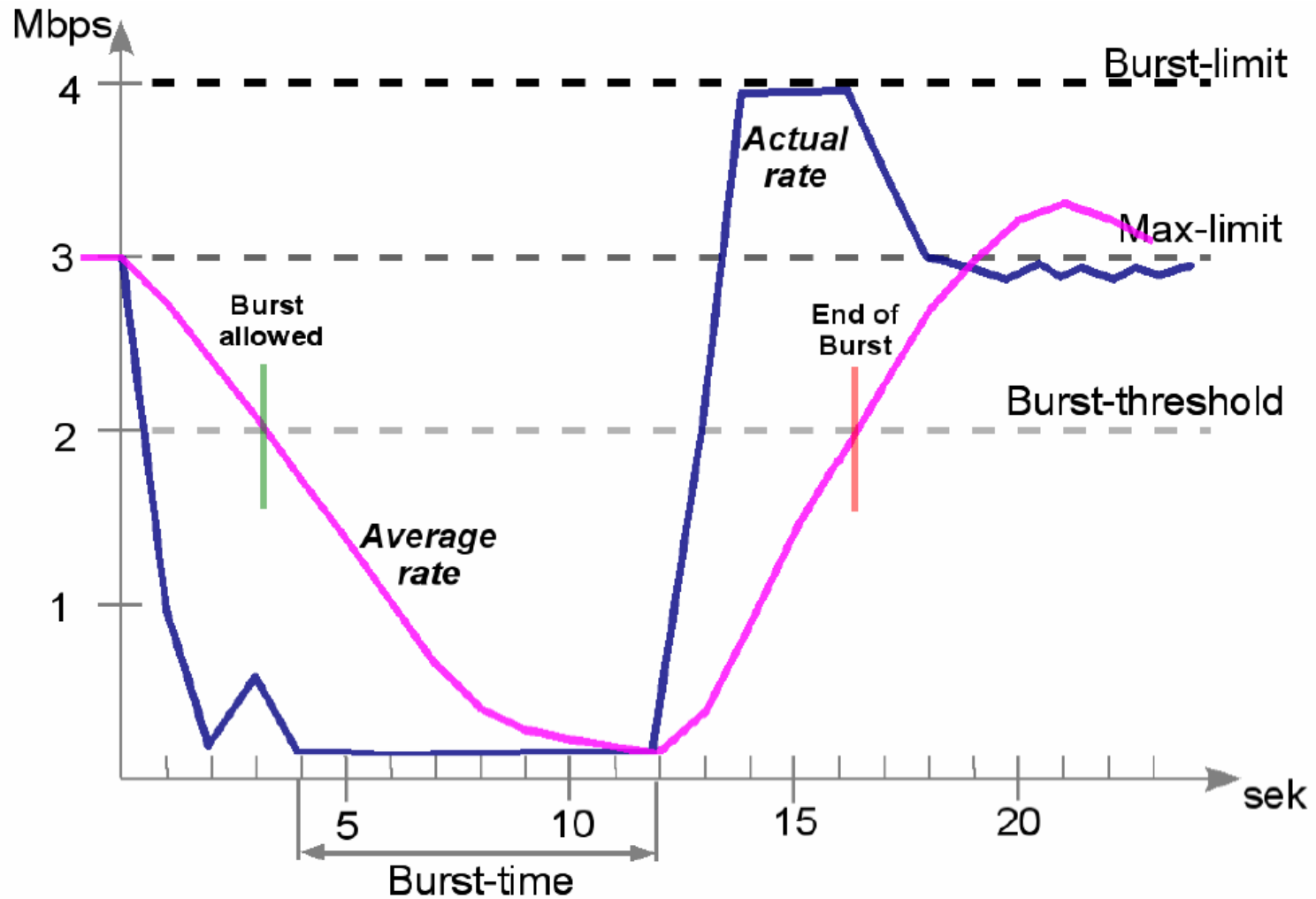


● ● ● | Contoh Burst (1)

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



Contoh Burst (2)

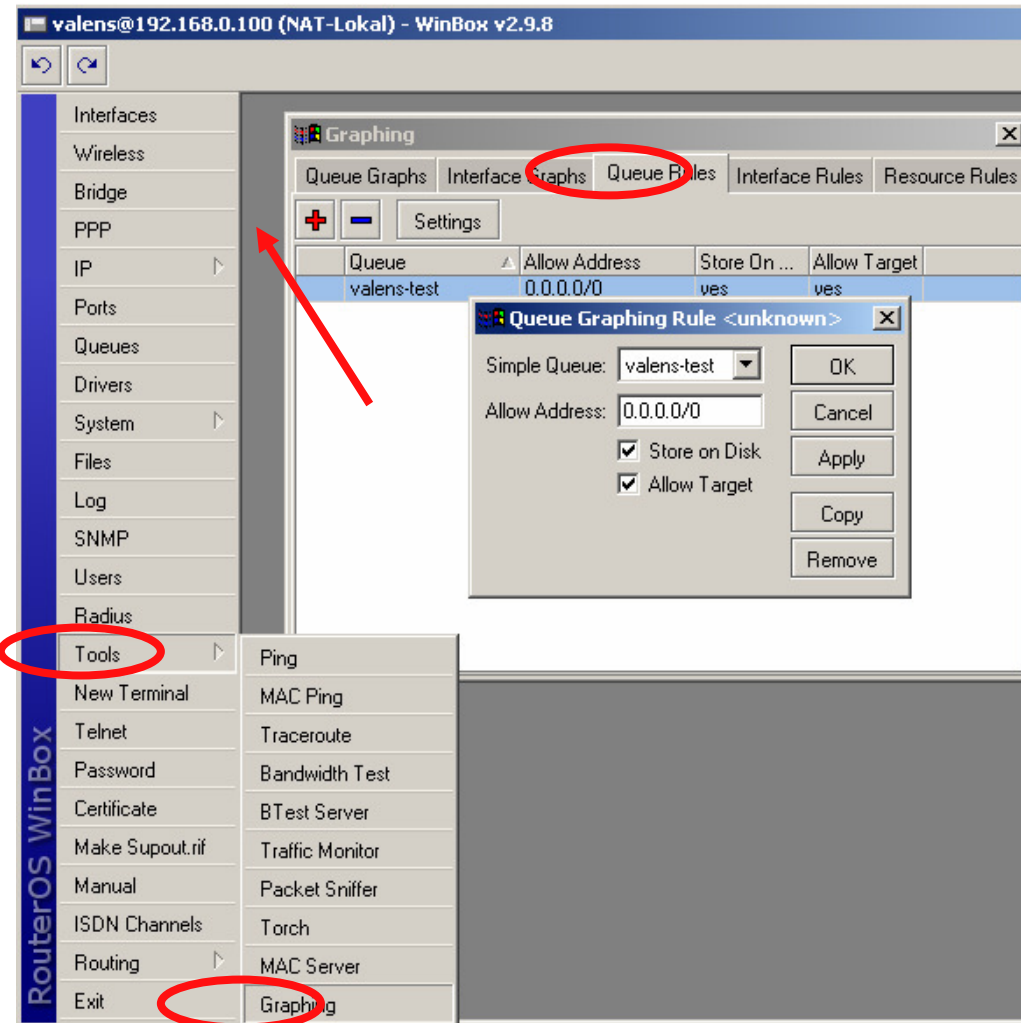


- ● ● | [LAB] Simple Queue 2

- Make a simple queue for your laptop
 - Downstream limit-at=128k, max-limit=256k
 - Upstream limit-at=64k, max-limit=128k
 - Try Using Limit-At and Burst
 - Burst-limit=1M
 - Burst-threshold=512K
 - Burst-time=30s
-

Graphic from Simple Queue

- Dengan simple queue, kita bisa membuat grafik penggunaan per client.
 - **allow-address**
IP address yang dapat melihat grafik tersebut
 - **allow-target**
memperbolehkan IP Address yang tercantum pada target untuk melihat grafik.



Graphic from Simple Queue

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

File Edit View Go Bookmarks Tools Help

http://192.168.0.100/graphs/

Toko FN Donasi Mikrotik-IND Mikrotik Fotografer.Net KlikBCA

Traffic and system resource graphing

You have access to 1 queue:
[valens-test](#)

You have access to 4 interfaces:
[LAN](#)
[WAN](#)
[ether1](#)
[bridge1](#)

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

File Edit View Go Bookmarks Tools Help

http://192.168.0.100/graphs/

Toko FN Donasi Mikrotik-IND Mikrotik Fotografer.Net KlikBCA

Queue Statistics

valens-test

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

"Daily" Graph (5 Minute Average)

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

"Weekly" Graph (30 Minute Average)



Prinsip Dasar Queue

- Queuing disciplines mengatur bagaimana paket data menunggu giliran untuk disalurkan ke interface, atau jika melebihi akan di drop.
 - Interface Queue bekerja pada interface yang meninggalkan router
 - Hanya boleh ada satu macam queuing discipline yang digunakan pada suatu interface.
-

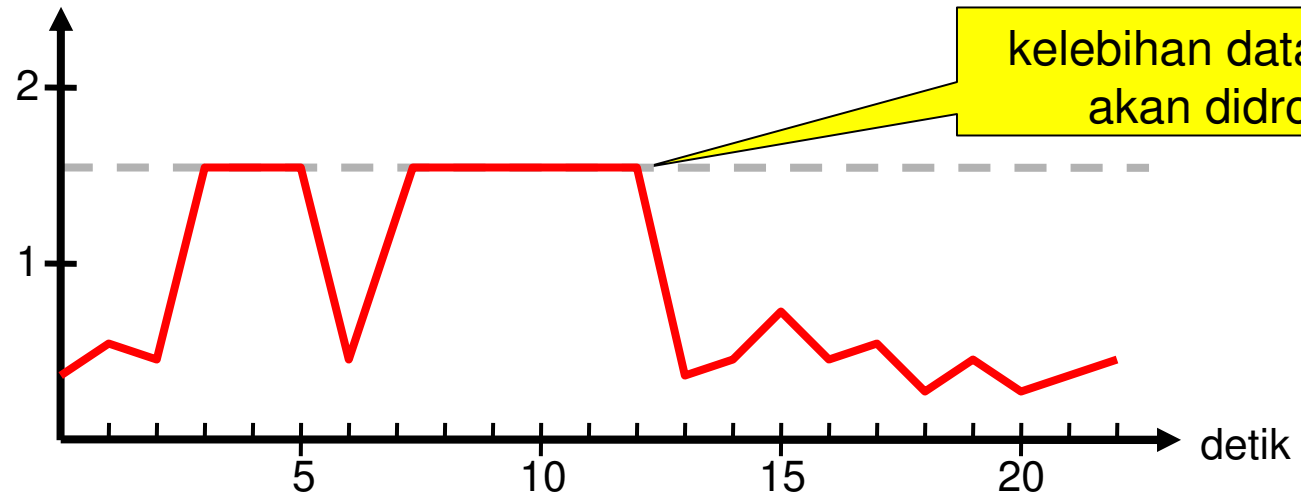
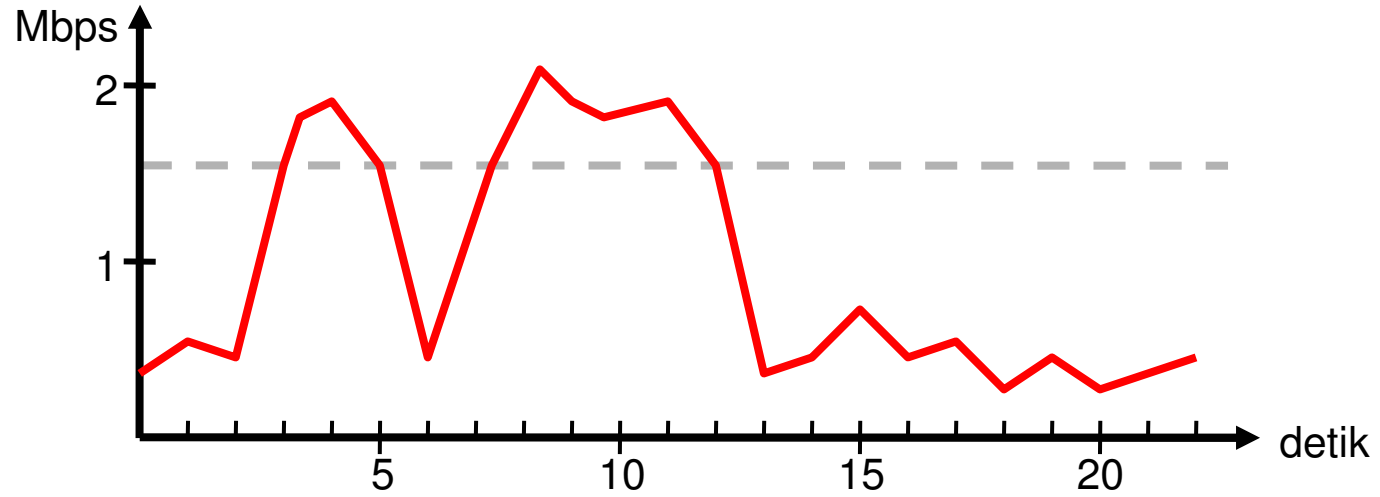


Queue Disciplines

- Queuing disciplines dapat dibedakan menjadi 2:
 - Scheduler queues
 - Mengatur packet flow, sesuai dengan jumlah paket data yang “menunggu di antrian”, dan bukan melimit kecepatan data rate.
 - Shaper queues
 - Mengontrol kecepatan data rate.

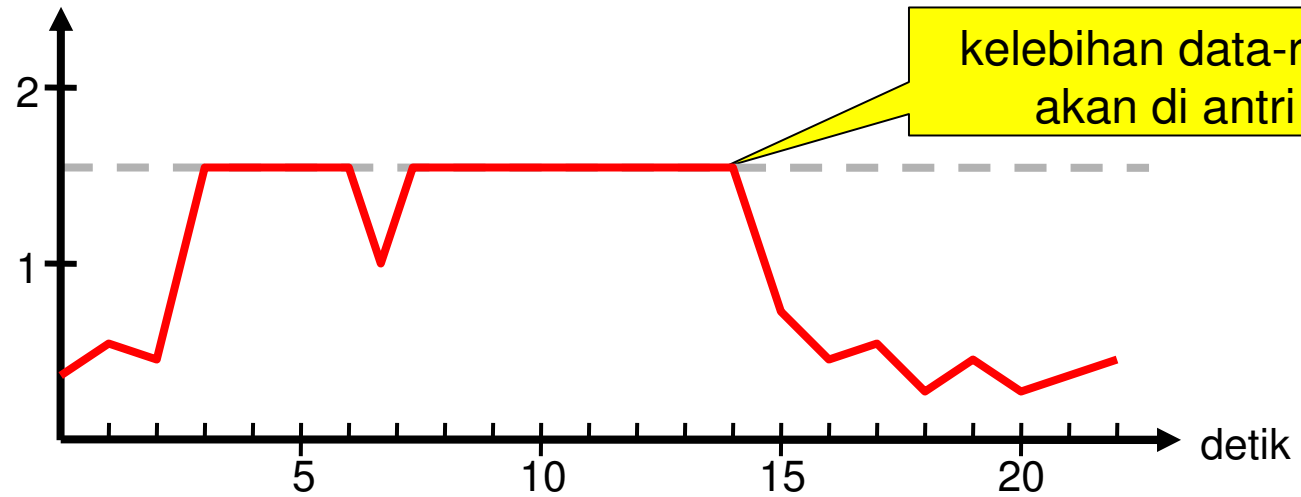
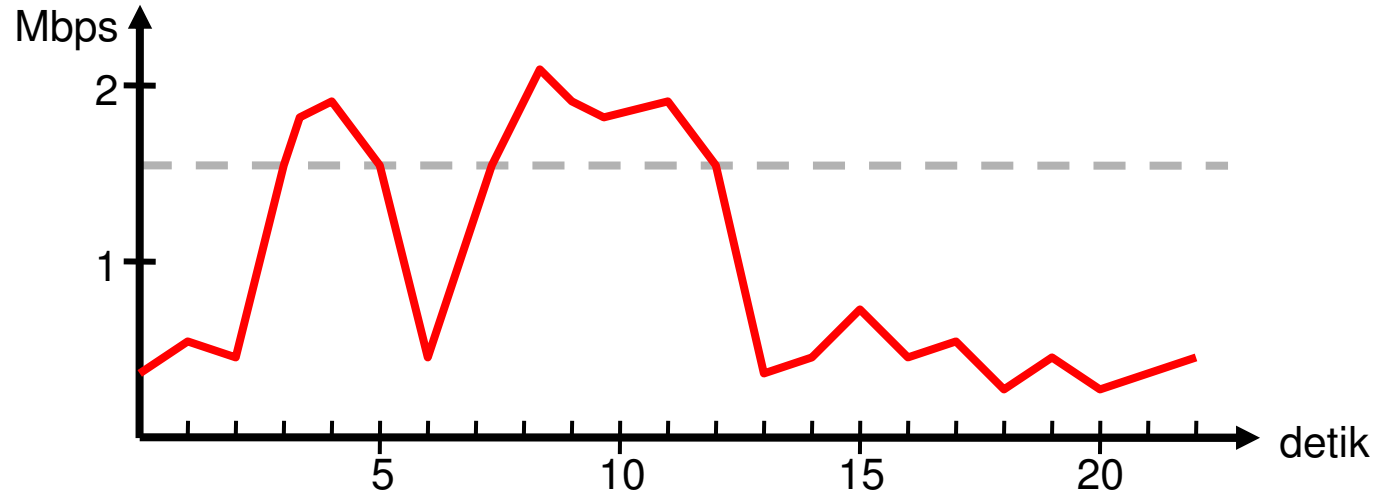


Shaper





Scheduler



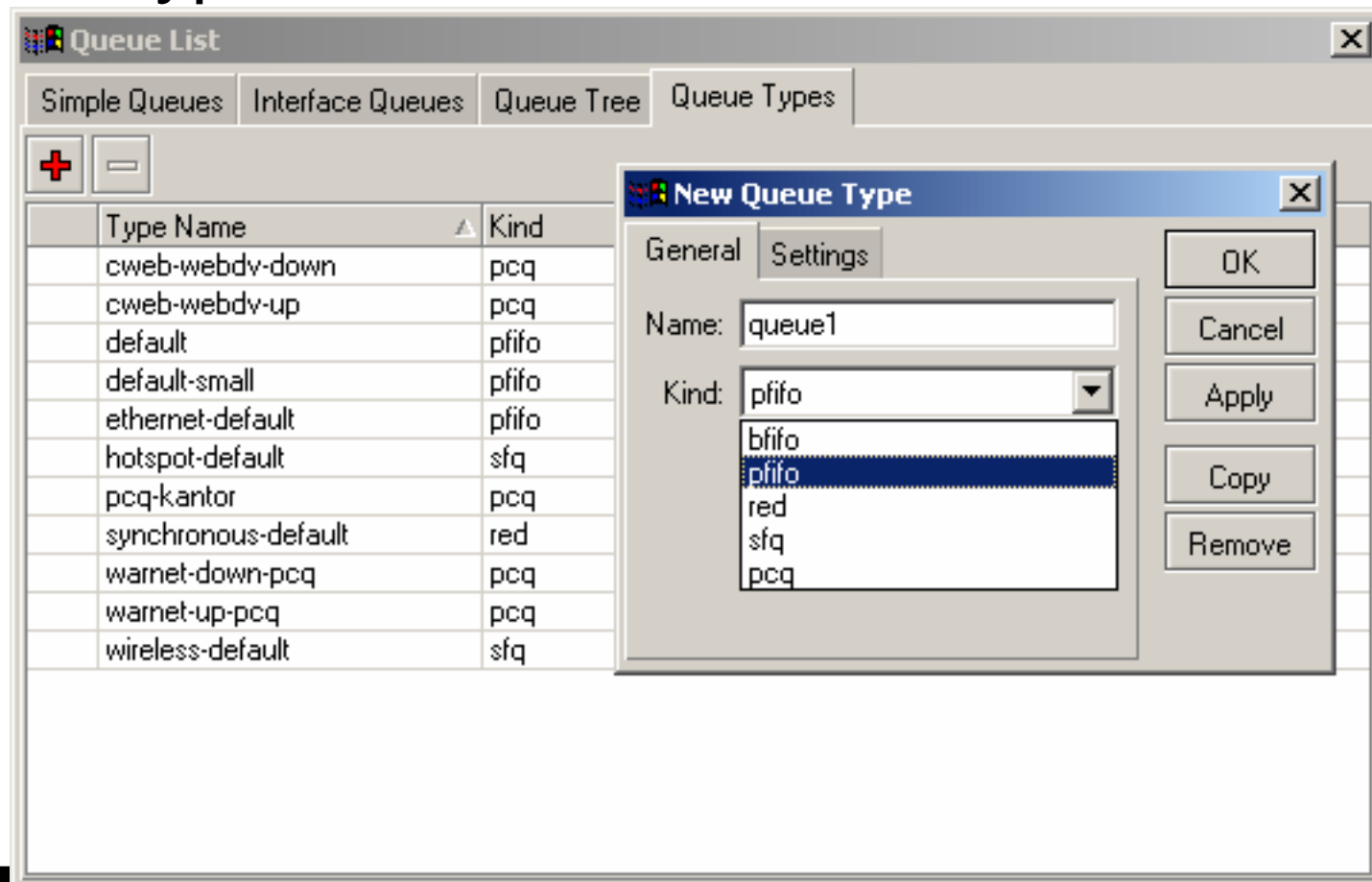


Queue Kinds

- Scheduler queues:
 - BFIFO (Bytes First-In First-Out)
 - PFIFO (Packets First-In First-Out)
 - RED (Random Early Detect)
 - SFQ (Stochastic Fairness Queuing)
 - Shaper queues:
 - PCQ (Per Connection Queue)
 - HTB (Hierarchical Token Bucket)
 - You can configure queue properties in “/queue type”
-

Queue Kinds

- Kita dapat mengatur tipe queue pada “/queue type”

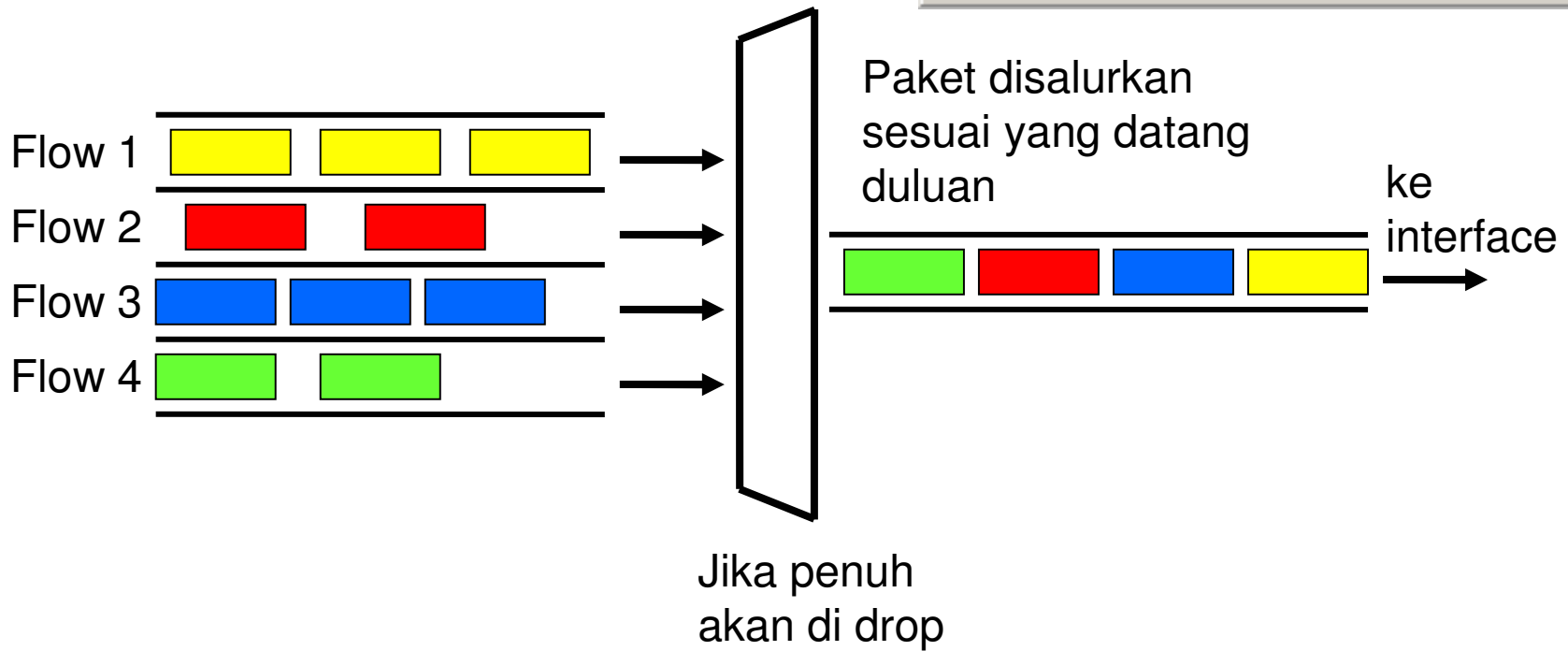
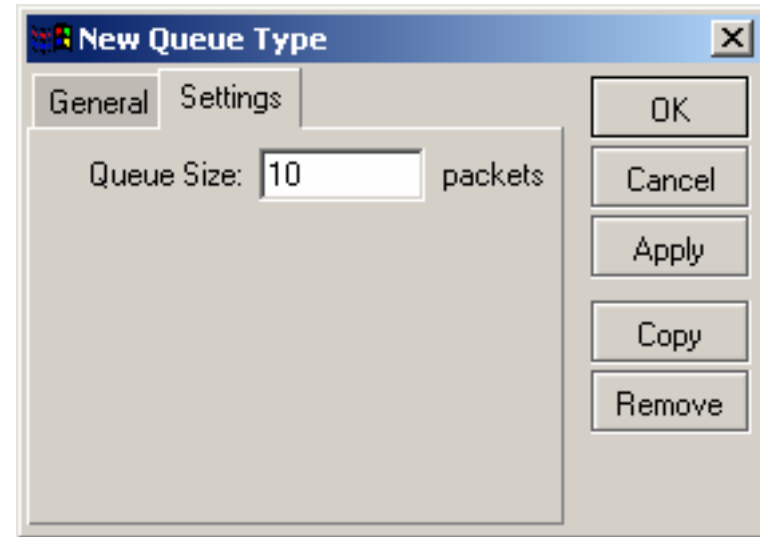




FIFO (First In First Out)

- PFIFO dan BFIFO keduanya menggunakan algoritma FIFO, dengan buffer yang kecil.
 - FIFO tidak mengubah urutan paket data, hanya menahan dan menyalurkan bila sudah memungkinkan.
 - Jika buffer penuh maka paket data akan di drop
 - FIFO baik digunakan bila jalur data tidak congested
 - Parameter pfifo-limit dan bfifo-limit menentukan jumlah data yang bisa diantri di buffer
-

Skema FIFO

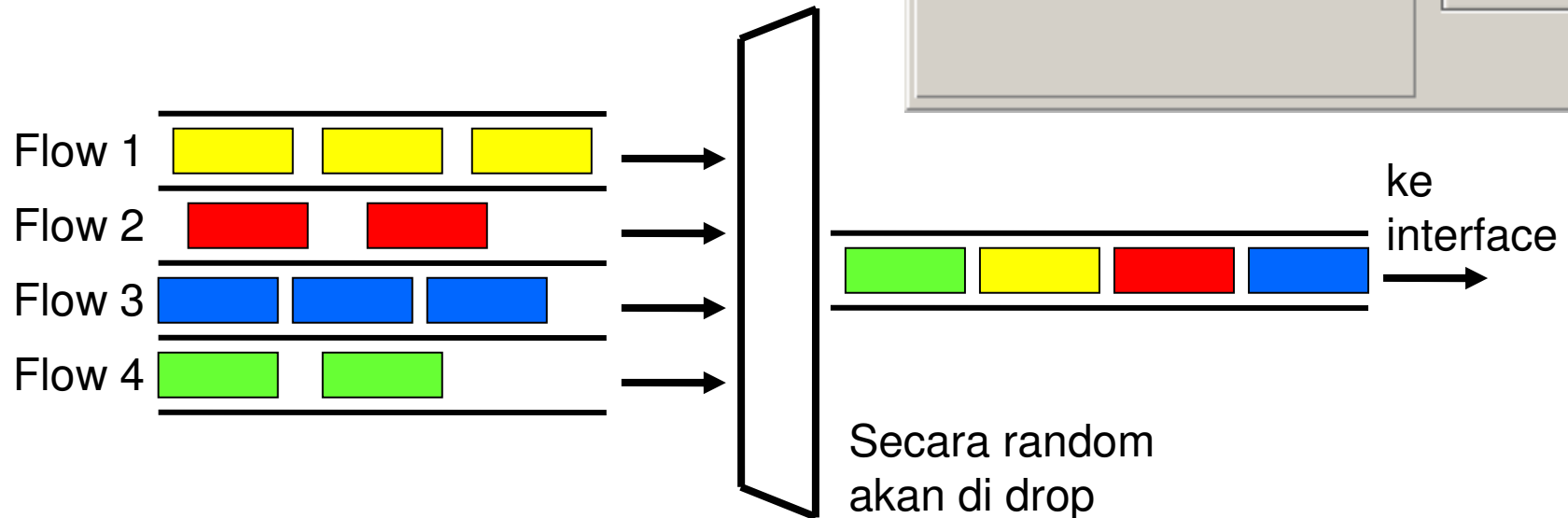
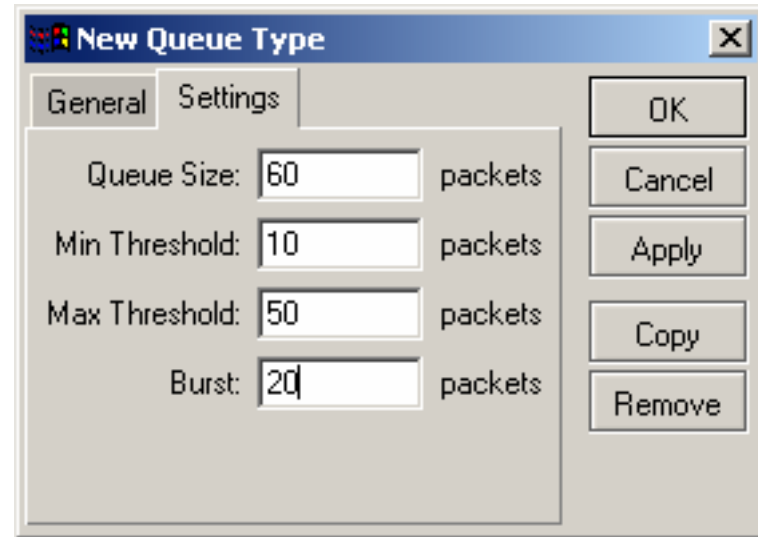




RED (Random Early Detect)

- RED tidak melimit kecepatan, tetapi bila buffer sudah penuh, maka secara tidak langsung akan menyeimbangkan data rate setiap user.
- Saat ukuran queue rata-rata mencapai min-threshold, RED secara random akan memilih paket data untuk di drop
- Saat ukuran queue rata-rata mencapai max-threshold, paket data akan di drop
- Jika ukuran queue sebenarnya (bukan rata-ratanya) jauh lebih besar dari **red-max-threshold**, maka semua paket yang melebihi **red-limit** akan didrop.
- RED digunakan jika kita memiliki trafik yang congested. Sangat sesuai untuk trafik TCP, tetapi kurang baik digunakan untuk trafik UDP.

Skema RED

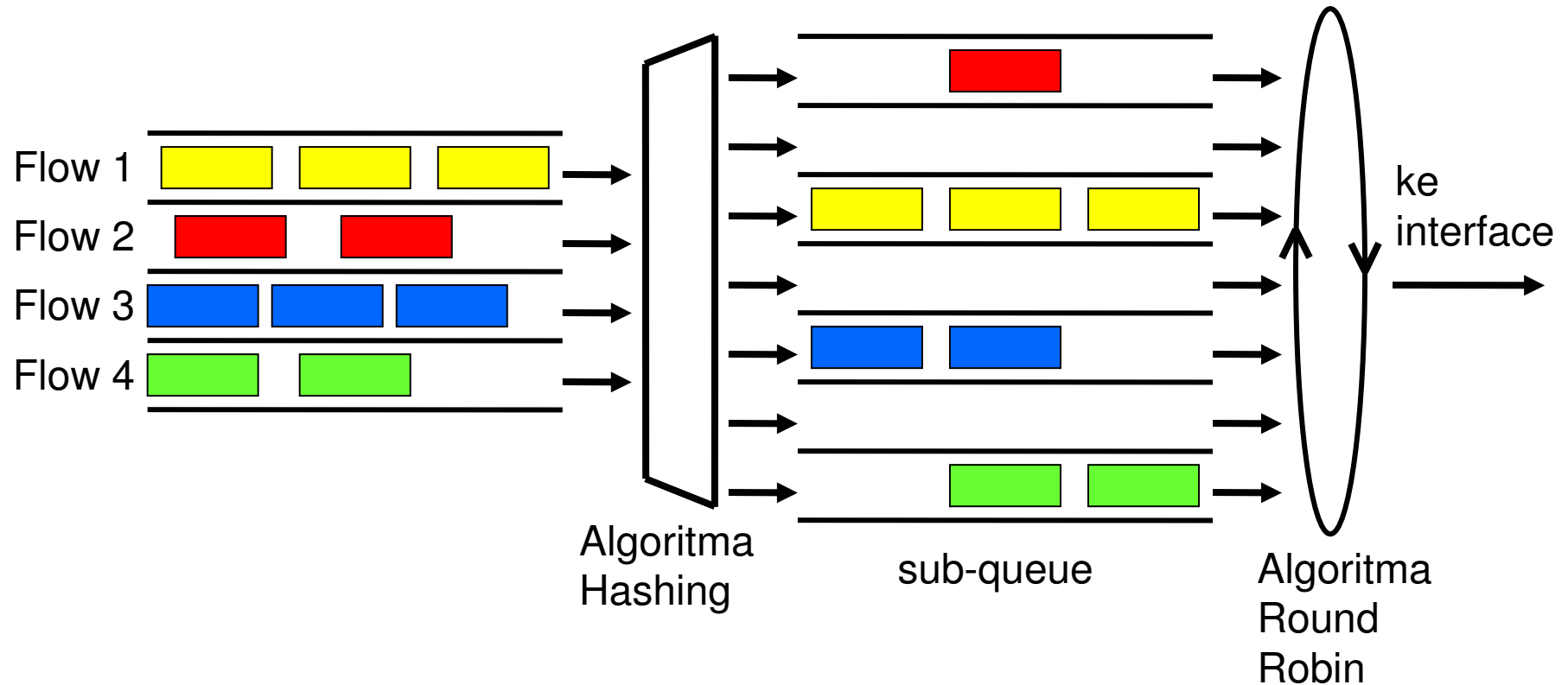
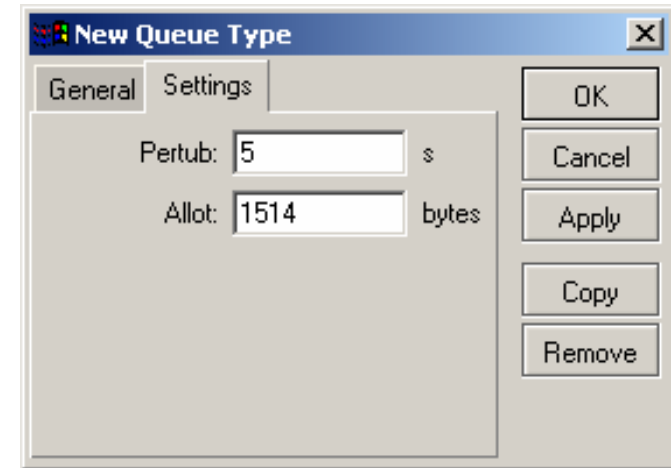


SFQ (Stochastic Fairness Queuing)

- SFQ sama sekali tidak dapat melimit trafik. Fungsi utamanya adalah menyeimbangkan flow trafik jika link telah benar-benar penuh.
- Dapat digunakan untuk TCP maupun UDP.
- SFQ menggunakan metoda hasing dan round robin.
- Total SFQ queue terdiri dari 128 paket.
- Algoritma hasing dapat membagi trafik menjadi 1024 sub queue, dan jika terdapat lebih maka akan dilewati.
- Algoritma round robin akan melakukan queue ulang sejumlah bandwidth (allot) dari setiap queue.

Skema SFQ

- Setelah **perturb** detik algoritma hasing akan berganti dan membagi session trafik ke sub-queue lainnya

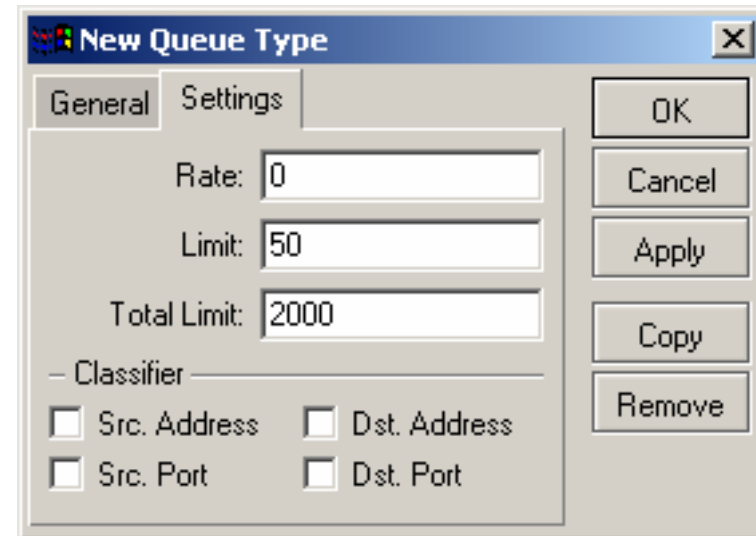




PCQ (Per Connection Queue)

- PCQ dibuat sebagai penyempurnaan SFQ.
 - PCQ tidak membatasi jumlah sub-queue
 - PCQ membutuhkan memori yang cukup besar
-

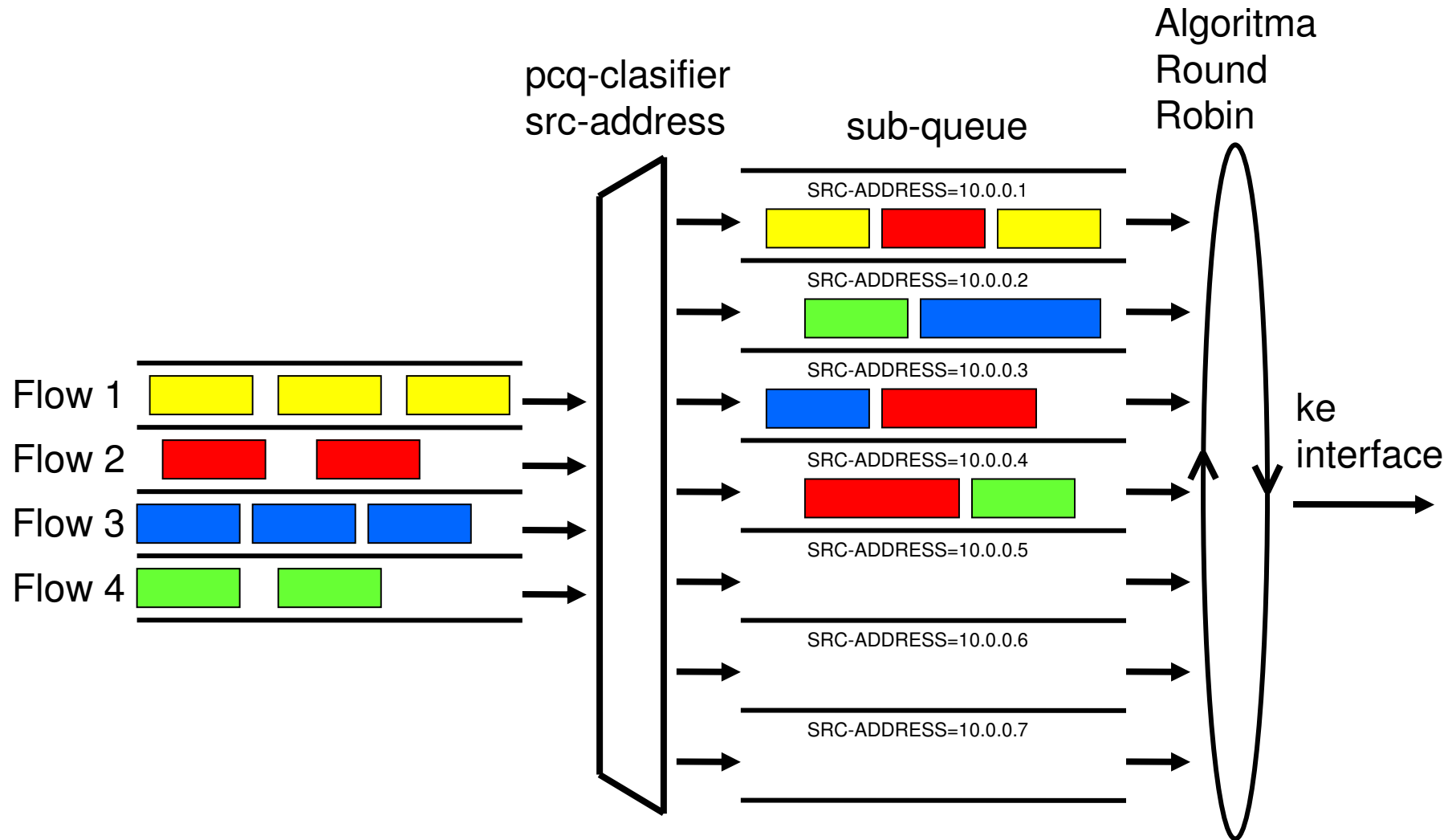
Setting PCQ



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

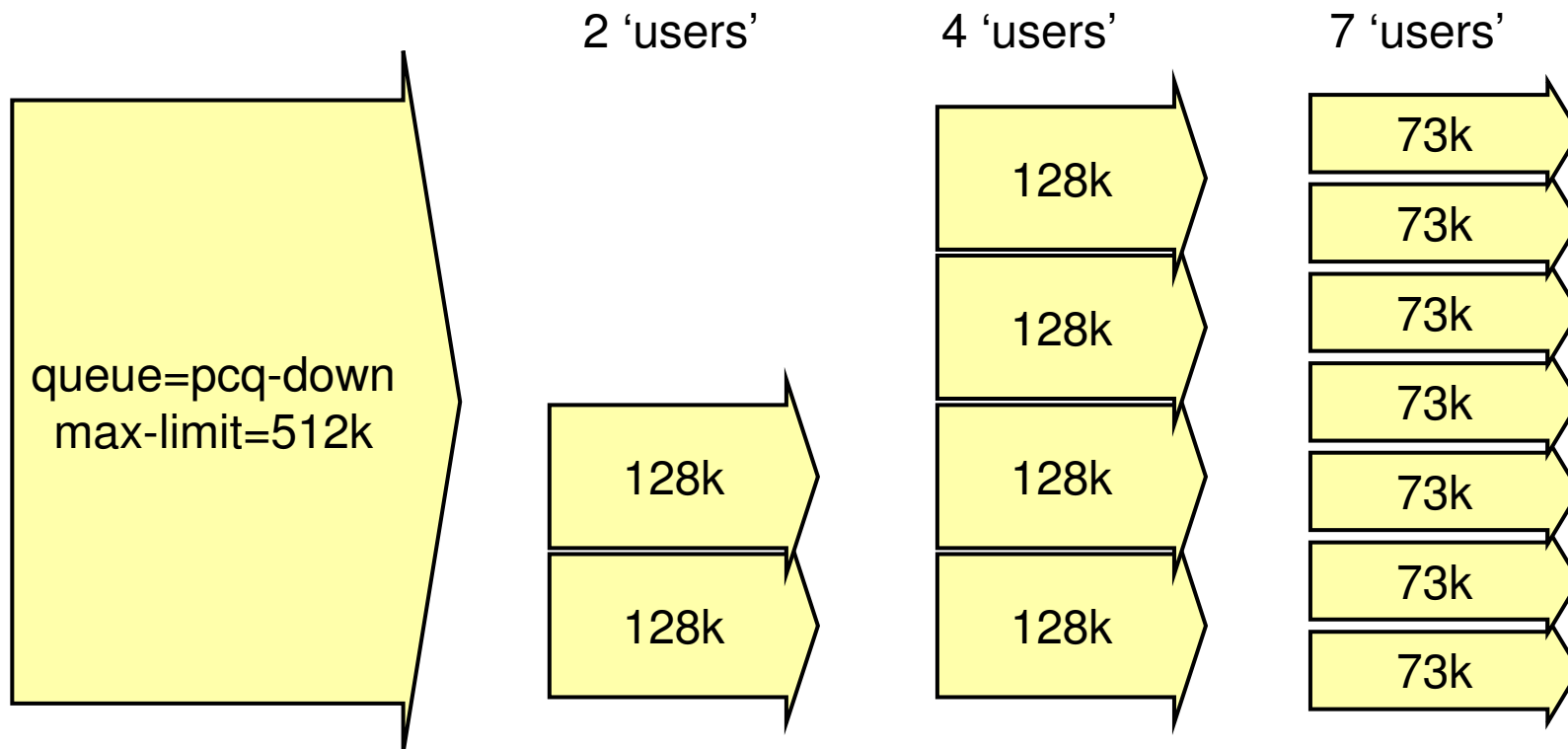


Skema PCQ



● ● ● | PCQ in Action (1)

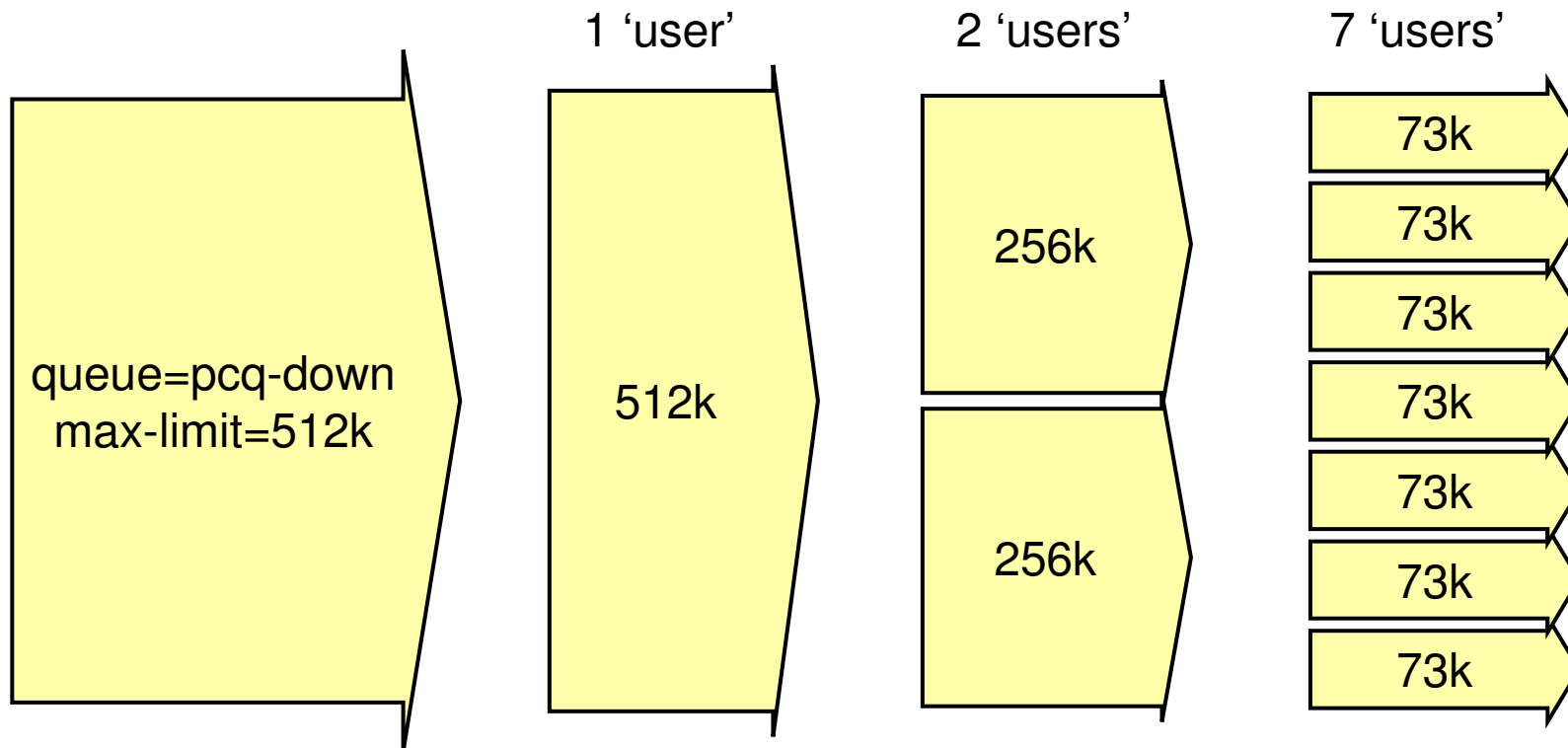
- Pcq-rate=128000





PCQ in Action (2)

- o Pcq-rate=0



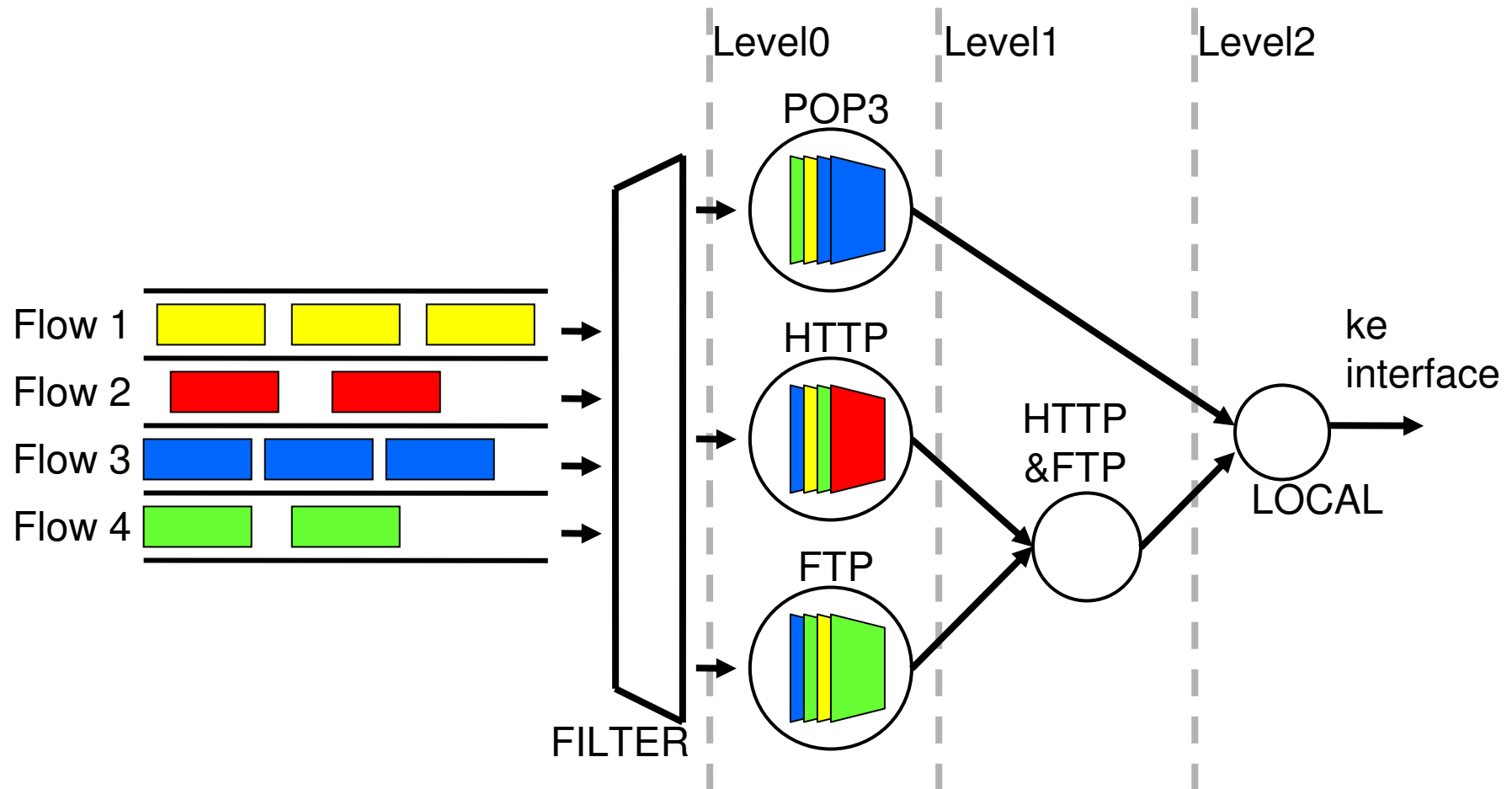


HTB (Hierarchical Token Bucket)

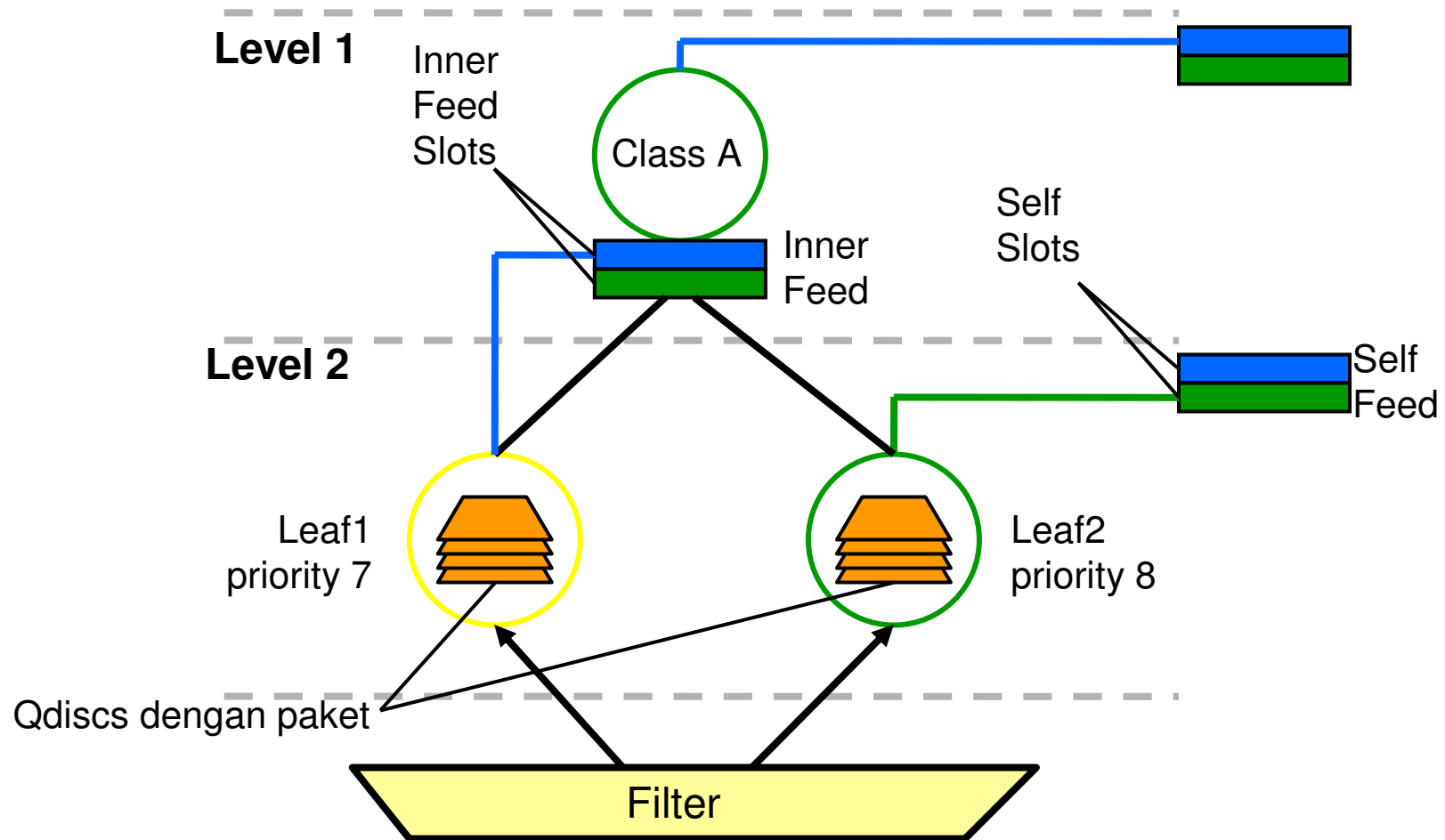
- HTB adalah classful queuing discipline yang dapat digunakan untuk mengaplikasikan handling yang berbeda untuk beberapa jenis trafik.
 - Secara umum, kita hanya dapat membuat 1 tipe queue untuk setiap interface. Namun dengan HTB di RouterOS, kita dapat mengaplikasikan properti yang berbeda-beda.
 - HTB dapat melakukan prioritas untuk grup yang berbeda.
-



Skema Hirarki pada HTB



Skema HTB

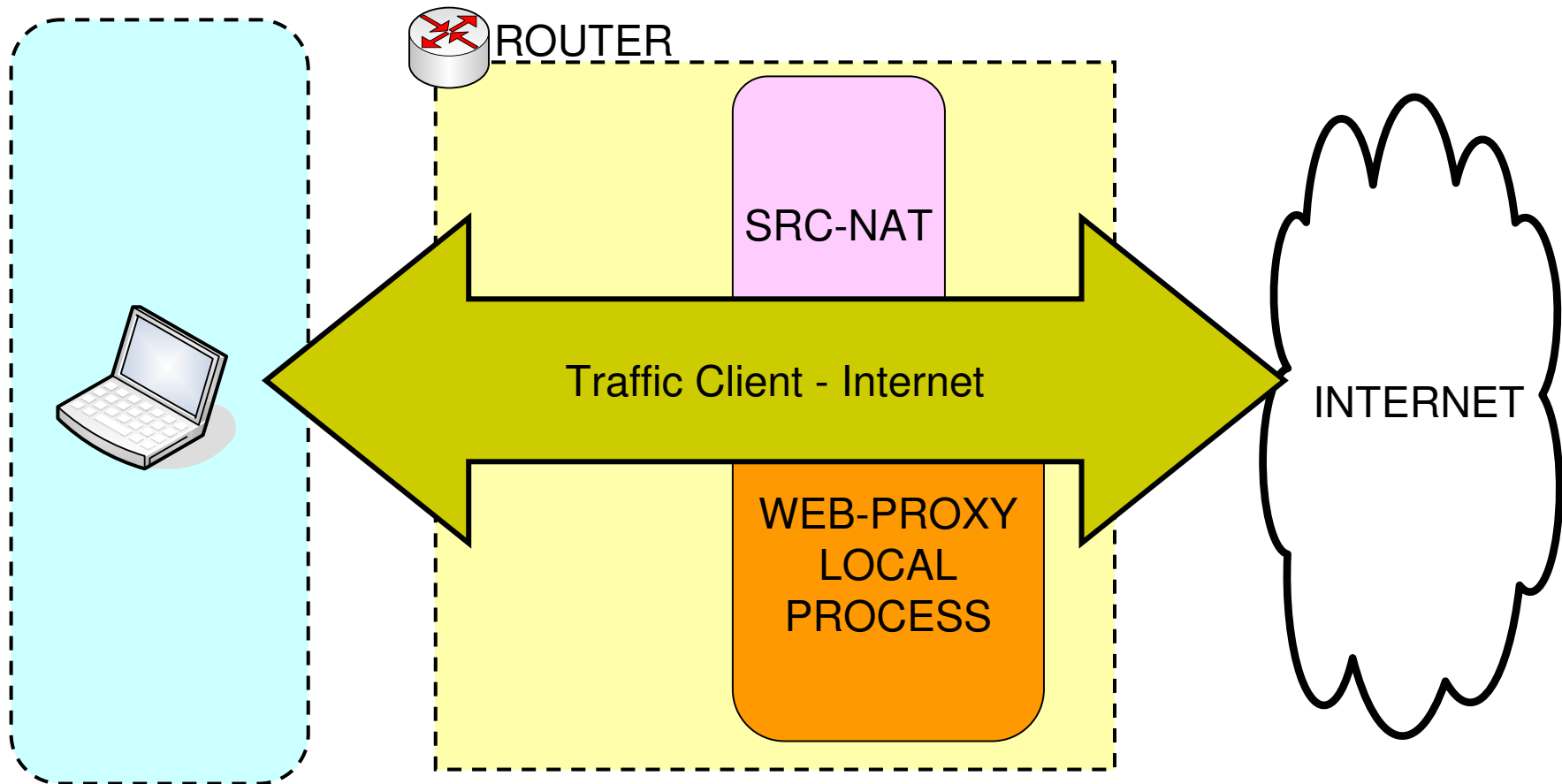




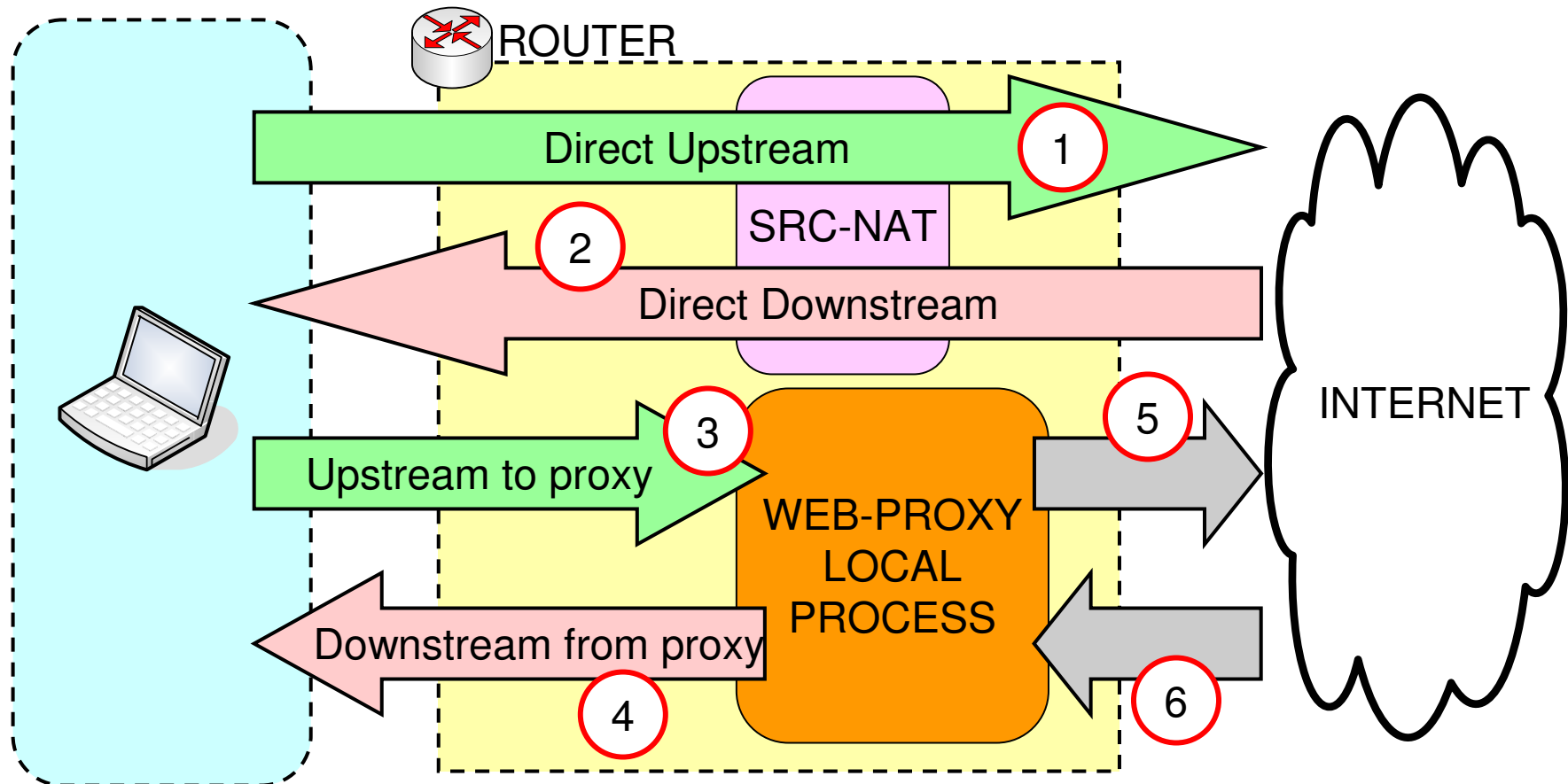
HTB States

- **hijau**
 - Posisi di mana data-rate lebih kecil dari limit-at.
 - Nilai limit-at pada kelas tersebut akan dilihat terlebih dahulu daripada parent classnya.
 - Contoh, sebuah class memiliki limit-at 512k, dan parent-nya memiliki limit-at 128k. Maka class tersebut akan selalu mendapatkan data-rate 512k.
- **kuning**
 - Posisi di mana data-rate lebih besar dari limit-at, namun lebih kecil dari max-limit.
 - Diiijinkan atau tidaknya penambahan trafik bergantung pada :
 - posisi parent, jika prioritas class sama dengan parentnya dan parentnya dalam posisi kuning
 - posisi class itu sendiri, jika parent sudah berstatus kuning.
- **merah**
 - Posisi di mana data-rate sudah melebihi max-limit.
 - Tidak dapat lagi meminjam dari parentnya.

Queue with SRC-NAT & Internal Proxy



[LAB] Simple Queue with SRC-NAT & Internal Proxy





Web-Proxy Setup

```
> ip web-proxy pr enabled: yes  
src-address: 0.0.0.0  
port: 3128  
hostname: "proxy"  
transparent-proxy: yes  
parent-proxy: 0.0.0.0:0  
cache-administrator: "webmaster"  
max-object-size: 4096KiB  
cache-drive: system  
max-cache-size: none  
max-ram-cache-size: unlimited  
status: running  
reserved-for-cache: 0KiB  
reserved-for-ram-cache: 154624KiB
```

- ● ● |

Firewall Setup

- [admin@instaler] ip firewall nat> pr
Flags: X - disabled, I - invalid, D - dynamic
- 0 chain=srcnat out-interface=public
src-address=192.168.x.0/24
action=masquerade
- 1 chain=dstnat in-interface=lan src-
address=192.168.1.0/24 protocol=tcp
dst-port=80 action=redirect to-ports=3128



Queue Setup

Simple-Queue Setup :

name="queue-notebook"

target-addresses=192.168.x.2/32

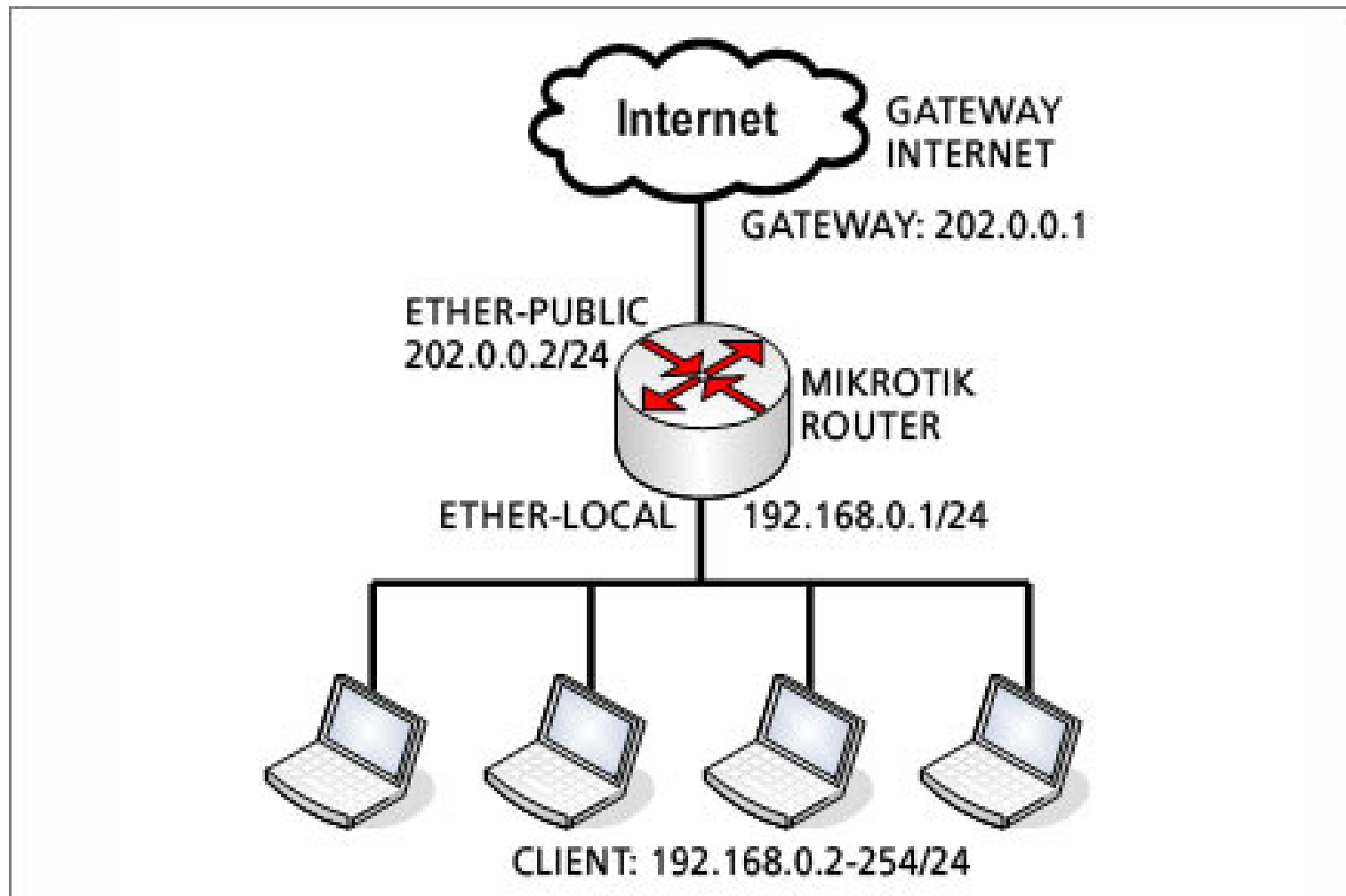
interface=all

parent=none

direction=both

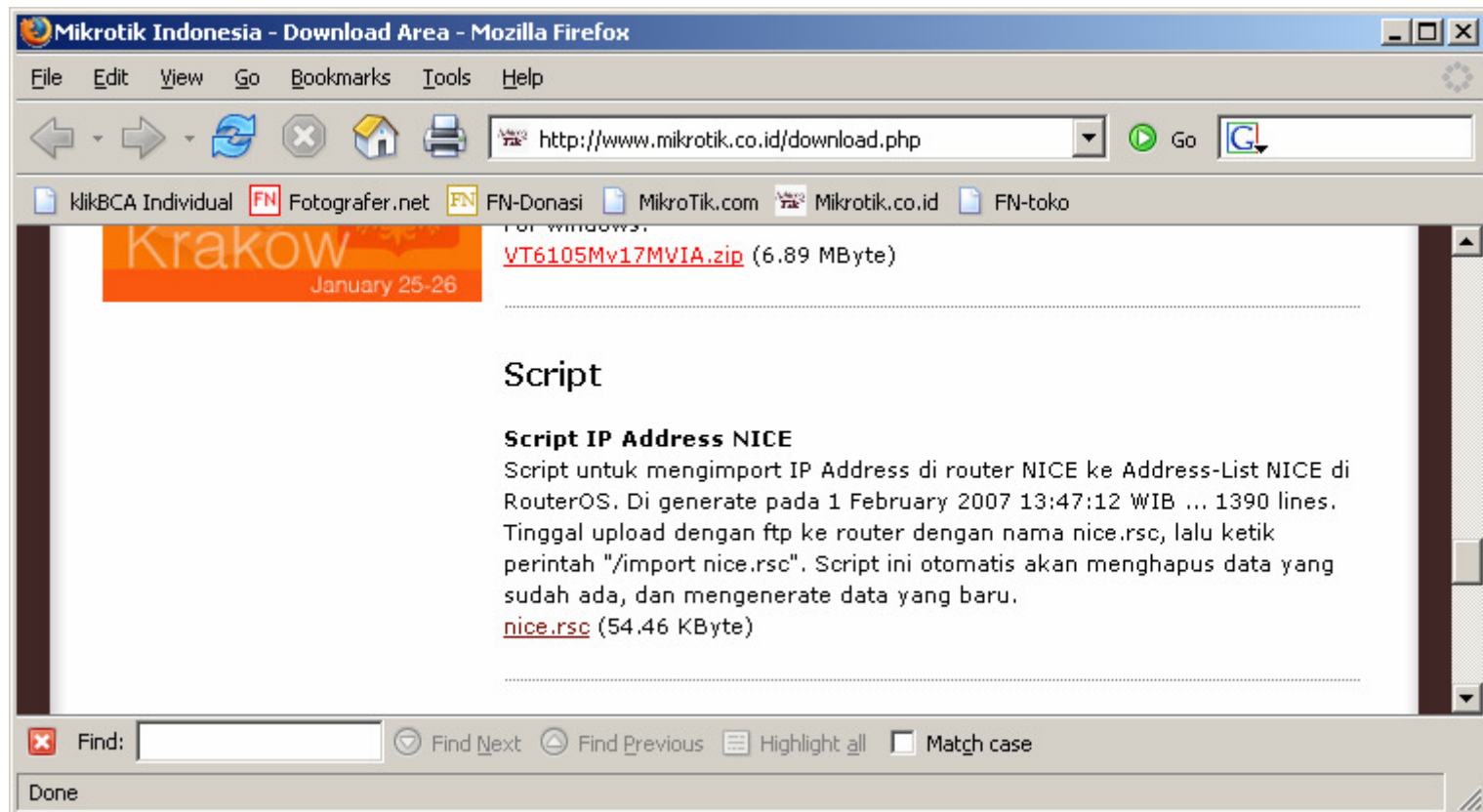
queue=default-small/default-small

[LAB] Simple-Queue Traffic Internasional dan IIX



IP Address lokal - IIX

- Bisa didownload dari :
<http://www.mikrotik.co.id/download.php>
- Upload file nice.rsc dan lakukan import





Nice.rsc

```
# Script untuk mengenerate IP Address di Router NICE  
# Script by www.mikrotik.co.id  
# Generated at 1 February 2007 13:47:12 WIB ... 1390 lines
```

```
/ip firewall address-list  
rem [find list=nice]  
add list=nice address="61.94.0.0/16"  
add list=nice address="125.160.0.0/16"  
add list=nice address="125.161.0.0/16"  
add list=nice address="125.162.0.0/16"  
add list=nice address="125.163.0.0/16"  
add list=nice address="125.164.0.0/16"  
add list=nice address="222.124.0.0/16"  
add list=nice address="61.5.0.0/17"  
add list=nice address="202.158.0.0/17"  
add list=nice address="61.14.0.0/18"  
.....
```



Address-List on Winbox

Name	Address
nice	61.94.0.0/16
nice	125.160.0.0/16
nice	125.161.0.0/16
nice	125.162.0.0/16
nice	125.163.0.0/16
nice	125.164.0.0/16
nice	222.124.0.0/16
nice	61.5.0.0/17
nice	202.158.0.0/17
nice	61.14.0.0/18
nice	125.208.128.0/18
nice	152.118.0.0/18
nice	152.118.64.0/18
nice	152.118.128.0/18
nice	152.118.192.0/18
nice	202.152.0.0/18
nice	203.130.192.0/18
nice	206.182.192.0/18
nice	207.209.192.0/18
nice	210.210.128.0/18
nice	221.132.192.0/18
nice	124.195.0.0/19
nice	141.103.224.0/19
nice	202.47.192.0/19
nice	202.51.192.0/19
nice	202.136.64.0/19
nice	202.146.224.0/19
nice	202.147.224.0/19
nice	202.149.128.0/19
nice	202.159.64.0/19
nice	202.169.32.0/19
nice	202.171.0.0/19
nice	203.99.96.0/19
nice	209.93.224.0/19
nice	61.8.64.0/20
nice	122.200.0.0/20
nice	124.81.0.0/20
nice	124.81.16.0/20
nice	124.81.48.0/20
nice	124.81.64.0/20
nice	124.81.80.0/20



Pengaturan Mangle

```
[admin@MikroTik] > /ip firewall mangle pr
Flags: X - disabled, I - invalid, D - dynamic
0 chain=prerouting in-interface=[interface menuju network local]
  dst-address-list=nice
  action=mark-connection new-connection-mark=conn-iix
  passthrough=yes

1 chain=prerouting connection-mark=conn-iix
  action=mark-packet new-packet-mark=packet-iix
  passthrough=no

2 chain=prerouting action=mark-packet
  new-packet-mark=packet-intl passthrough=no
```

● ● ● | Pengaturan Simple-Queue

```
[admin@MikroTik]> /queue simple pr  
Flags: X - disabled, I - invalid, D - dynamic
```

```
0 name="client-iix" target-addresses=192.168.x.2/32  
dst-address=0.0.0.0/0 interface=all parent=none  
packet-marks=packet-iix direction=both priority=8  
queue=default-small/default-small limit-at=0/0  
max-limit=64000/256000 total-queue=default-small
```

```
1 name="client-intl" target-addresses=192.168.x.2/32  
dst-address=0.0.0.0/0 interface=all parent=none  
packet-marks=packet-intl direction=both priority=8  
queue=default-small/default-small limit-at=0/0  
max-limit=32000/128000 total-queue=default-small
```