Mikrotik Training Basic

Certified Mikrotik Training Basic Class

STMIK KHARISMA Makassar-Mikrotik Certified Academy

Mikrotik Academy

- Educational institutions such as universities, technical schools, colleges, vocational schools, and other educational institutions offering semester time based Internet networking courses for their academic students using MikroTik RouterOS as a learning tool.
- **Credit Training Material :**

  www.mikrotik.co.id (Citraweb Nusa Infomedia - *Mikrotik Certified Training Partner*)

Trainer & Staff

- **Saiful Rahman (Koordinator)**
  - *MTCNA (Mikrotik Certified Network Associate)*
  - *MTCTCE (Mikrotik Certified Traffic Control Expert)*
- **Abd. Munir S.**
  - *MTCNA (Mikrotik Certified Network Associate)*
  - *MTCTCE (Mikrotik Certified Traffic Control Expert)*
  - *MTCIPv6E (Mikrotik Certified IPv6 Enginer)*
- **Agus Halid**
  - *MTCNA (Mikrotik Certified Network Associate)*
  - *MTCTCE (Mikrotik Certified Traffic Control Expert)*

New Training Scheme 2010

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

Certification Test

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

Module 1

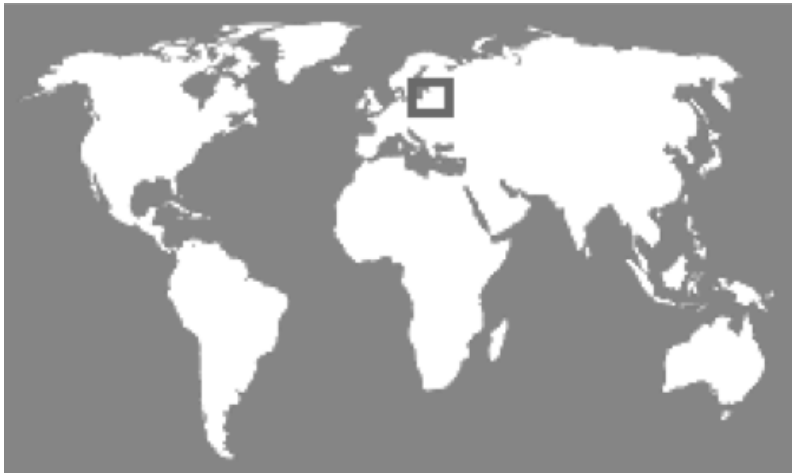
Mikrotik RouterOS

Introduction

STMIK KHARISMA Makassar

- Menjadi bagian dari Mikrotik Academy pada tahun 2013.
- Resmi menyelenggarakan Mikrotik Training Basic yang bersertifikasi Internasional

Where is MikroTik ?



Arti Kata Mikrotik

- Mikrotik adalah kependekan dari ***mikrotikls*** yang dalam bahasa Latvia berarti "***network kecil***"

What Is Mikrotik?

- Software Router untuk PC (x86, AMD, dll) #RouterOS#
  - Menjadikan PC biasa memiliki fungsi router yang lengkap
  - Diinstall sebagai Operating System, tidak membutuhkan operating system lainnya
- Hardware untuk jaringan (terutama wireless) #Routerboard#
  - Wireless board

    contoh: RB400, RB600, RB750, RB1000
  - Wireless interface (R52, R52H, R5H, R52N, R2N) menggunakan RouterOS sebagai software

Routerboard

- RouterBOARD is the hardware platform made by MikroTik. Our routers are powered by the powerful RouterOS Software. RouterBOARD routers are used by ISPs, integrators, system builders and large corporations around the world.
- Routerboard seperti sebuah pc mini yang terintegrasi karena dalam satu board tertanam prosesor, ram, rom, dan memori flash

Keunggulan

- Harga lebih murah dibanding berbagai macam product sekelas
- Compability hardware banyak
- Feature cukup banyak
- Untuk product Router Board yang udah dibundle dengan mikrotik performancenya sangat memenuhi kebutuhan dan sangat bisa bersaing dengan product yang lebih mahal

Routerboard for Wireless

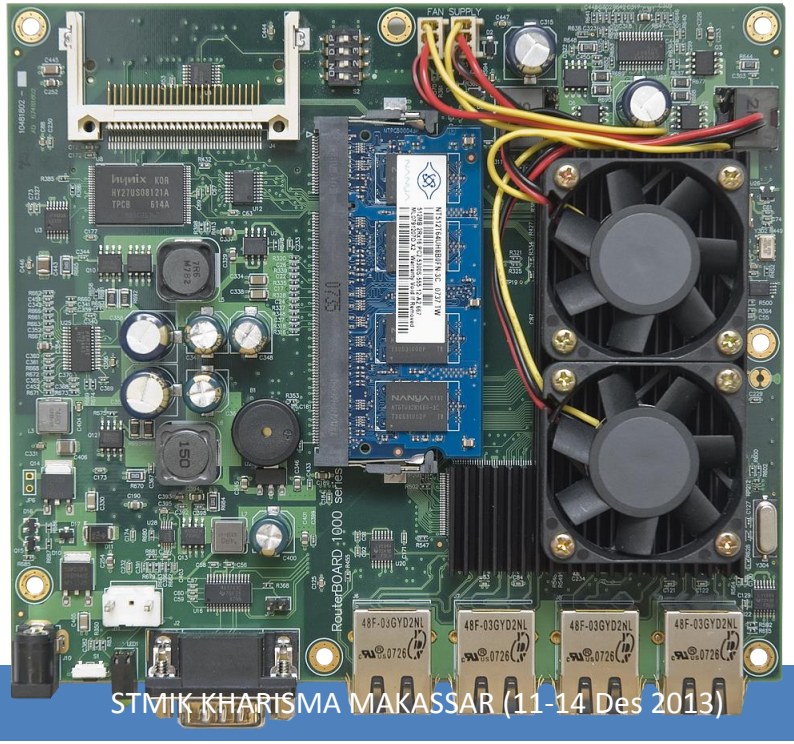
Jenis	Processor	RAM	Ether	MiniPCI	USB	Radio	Lisensi
RB800	MPC8544 800MHz	256MB	3 (gig)	4	-	-	6
RB435G	AR71xx 680MHz	256MB	3 (gig)	5	2	-	5
RB433UAH	AR71xx 680MHz	128MB	3	3	2	-	5
RB433/ **AH**	AR71xx 300/**680MHz**	64MB/**128MB**	3	3	-	-	4/5
RB411UAHR	AR71xx 680 MHz	64MB	1	1	1	1	4
RB411AH	AR71xx 680 MHz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

Routerboard for Indoor Router

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

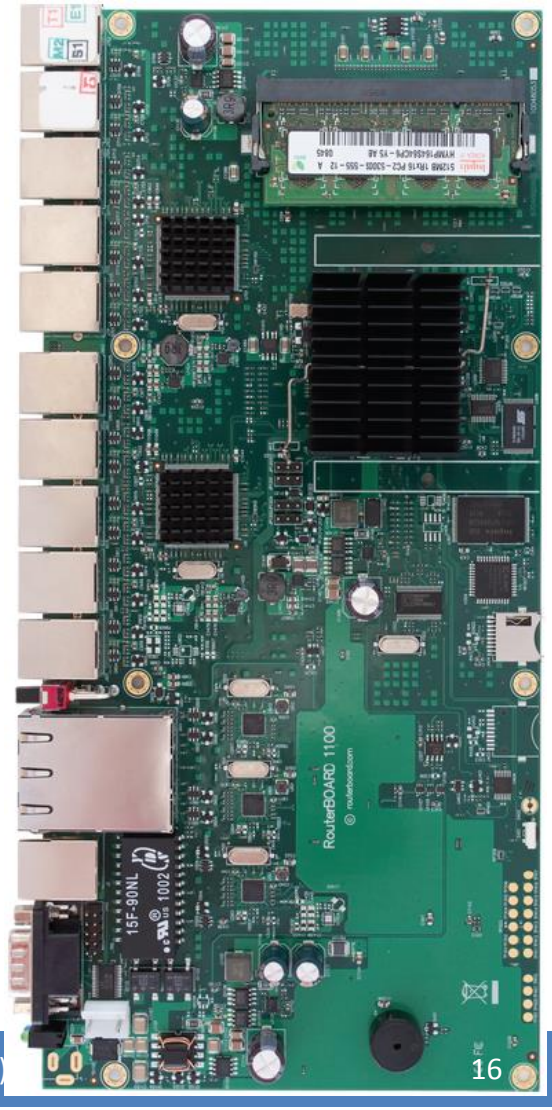
Discontinued Hardware

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



RB1100**AH / X2**

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

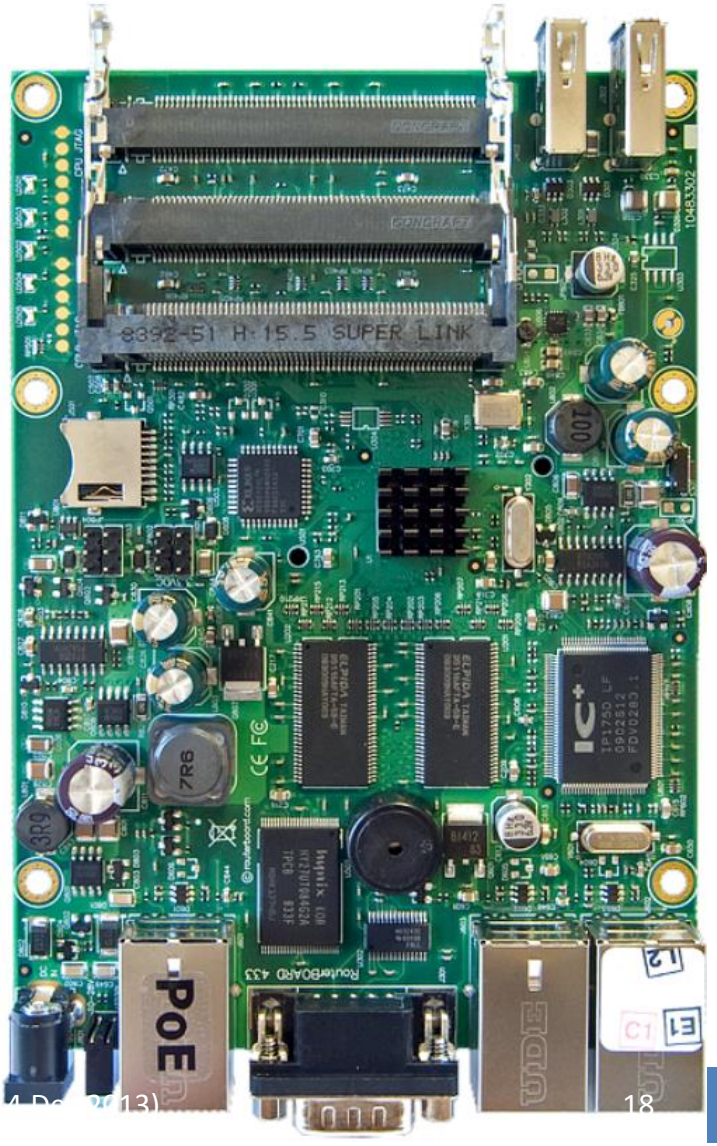


RB800

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

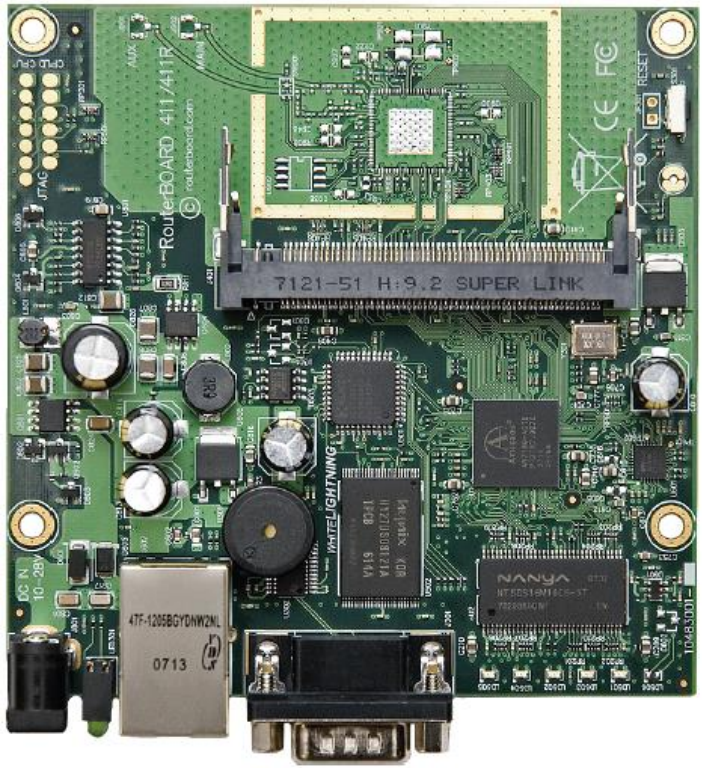
RB433UAH

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



RB411 / U / AR / AH / UAHR

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



RB493/AH/G

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

Embeded Solution

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

RB450 / G

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

RB750 / GL

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

RB751U-2HND

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

Wireless Interface

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

Mikrotik RouterOS

- MikroTik RouterOS™ adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer manjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless, cocok digunakan oleh ISP dan provider hotspot. (*www.mikrotik.co.id*)
- MikroTik routerOS merupakan sistem operasi Linux base yang diperuntukkan sebagai network router. Didesain untuk memberikan kemudahan bagi penggunanya.

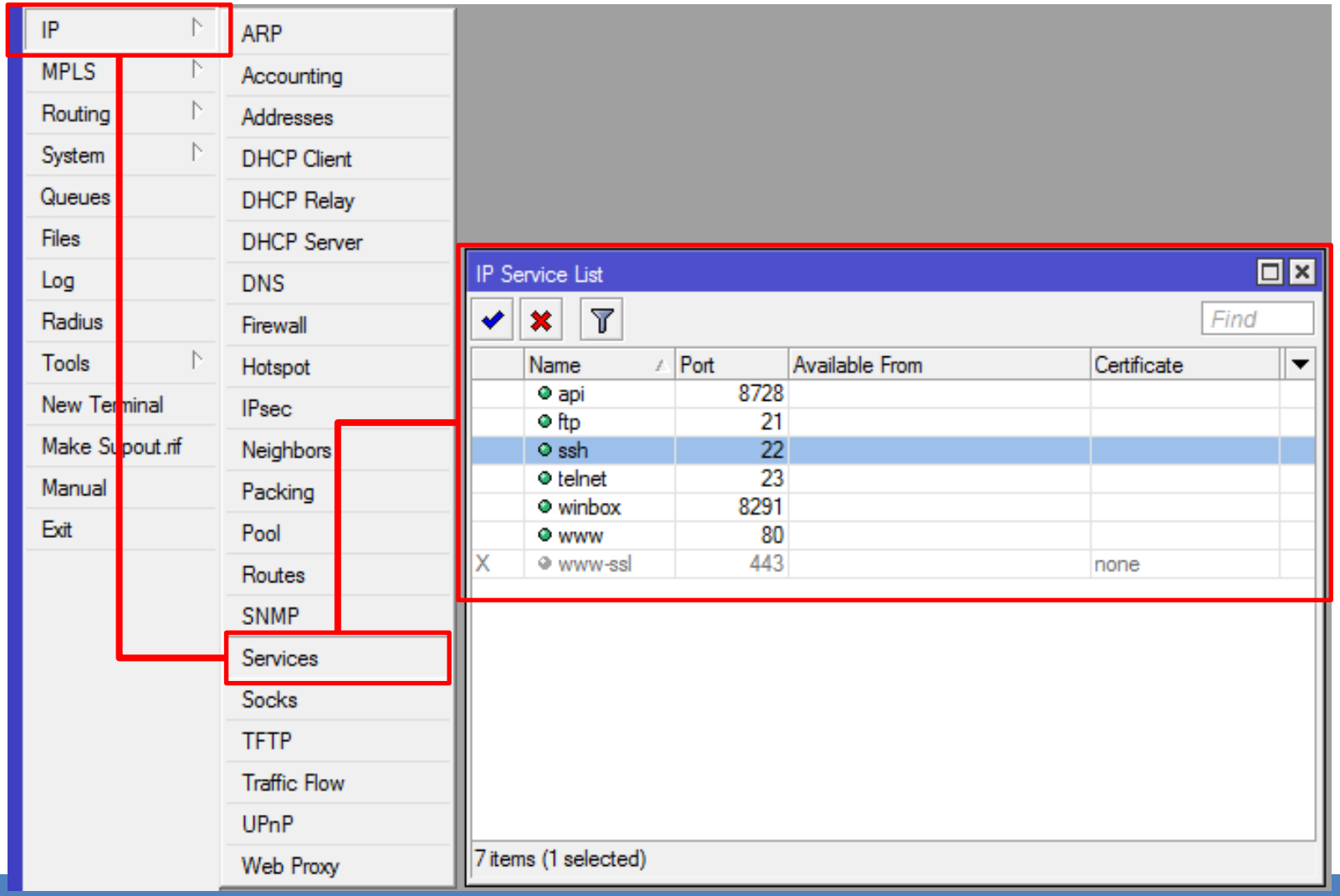
Fitur

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

Fitur

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

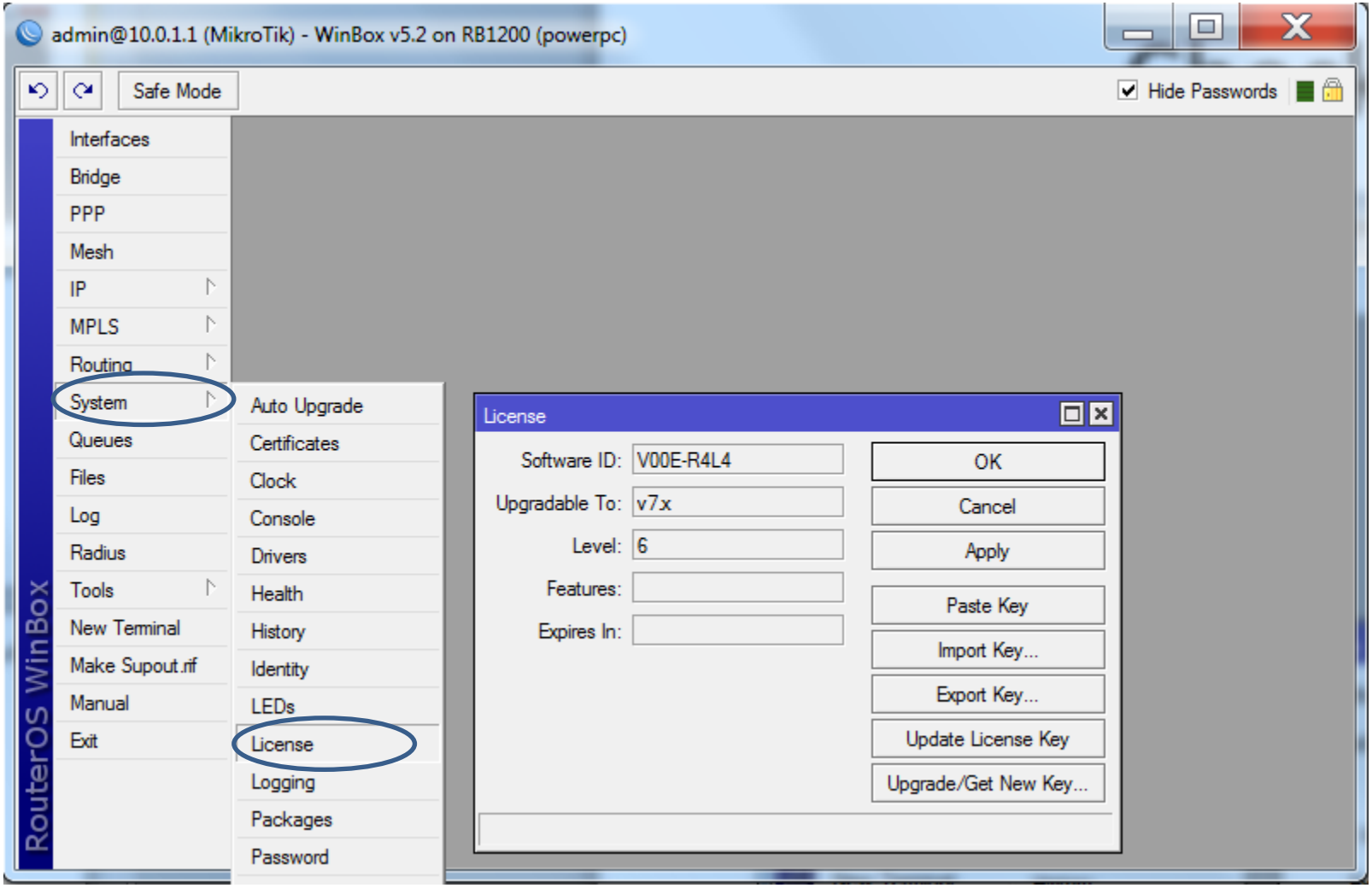
Manage RouterOS services



RouterOS license

Level number	0 (Demo mode)	1 (Free)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key	registration required	volume only	$45	$95	$250
Upgradable To	-	no upgrades	ROS v7.x	ROS v7.x	ROS v8.x	ROS v8.x
Wireless AP	24h trial	-	-	yes		
Wireless Client and Bridge	24h trial	-	yes			
RIP, OSPF, BGP protocols	24h trial	-	yes(*)	yes		
EoIP tunnels, VLAN interfaces, Queues	24h trial	1	unlimited			
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited
L2TP tunnels	24h trial	1	200	200	500	unlimited
OVPN tunnels	24h trial	1	200	200	unlimited	unlimited
HotSpot active users	24h trial	1	1	200	500	unlimited
RADIUS client	24h trial	-	yes			
Web proxy	24h trial	-	yes			
User manager active sessions	24h trial	1	10	20	50	Unlimited

Checking Licence



Buy Licence

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

Produk Mana Yang Dipilih

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

Buyer's Guide

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

Useful Links

- www.mikrotik.com - manage licenses, documentation
- forum.mikrotik.com - share experience with other users
- wiki.mikrotik.com - tons of examples

Mikrotik Installation

Installasi Mikrotik

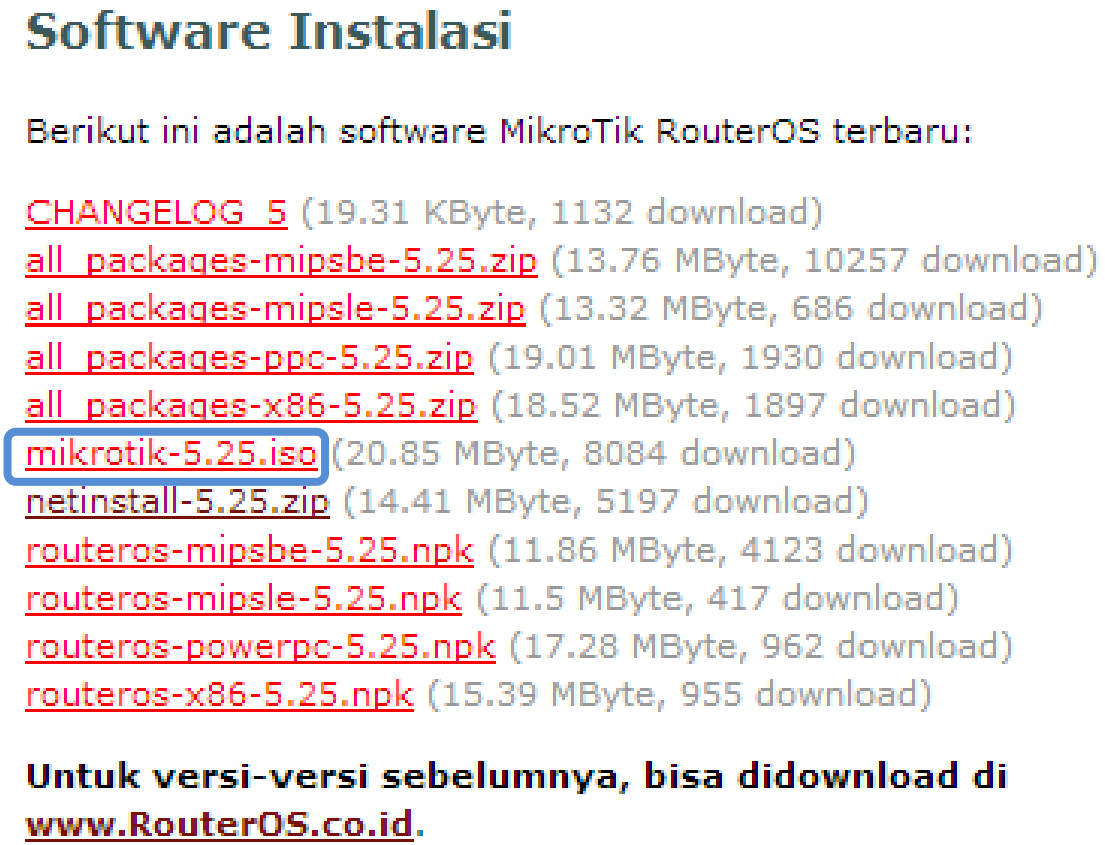
- Media Installasi (Penyimpan) Mikrotik RouterOS
  - Harddisk
  - CF Disk
  - DOM (Disk On Module)
    - SATA DOM (coming soon on mikrotik.co.id)
  - USB Flash Disk
    - Komputer harus bisa booting dari USB (setting BIOS)
  - Routerboard

Installation Method

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

Download Area

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



Software Instalasi

Berikut ini adalah software MikroTik RouterOS terbaru:

CHANGELOG_5 (19.31 KByte, 1132 download)
all_packages-mipsbe-5.25.zip (13.76 MByte, 10257 download)
all_packages-mipsle-5.25.zip (13.32 MByte, 686 download)
all_packages-ppc-5.25.zip (19.01 MByte, 1930 download)
all_packages-x86-5.25.zip (18.52 MByte, 1897 download)
mikrotik-5.25.iso (20.85 MByte, 8084 download)
netinstall-5.25.zip (14.41 MByte, 5197 download)
routeros-mipsbe-5.25.npk (11.86 MByte, 4123 download)
routeros-mipsle-5.25.npk (11.5 MByte, 417 download)
routeros-powerpc-5.25.npk (17.28 MByte, 962 download)
routeros-x86-5.25.npk (15.39 MByte, 955 download)

Untuk versi-versi sebelumnya, bisa didownload di www.RouterOS.co.id.

CD Installation (1)

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

```
                Welcome to MikroTik Router Software installation

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

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

CD Installation (3)

- **Warning: all data on the disk will be erased! Continue? [y/n]**

  Choose Yes

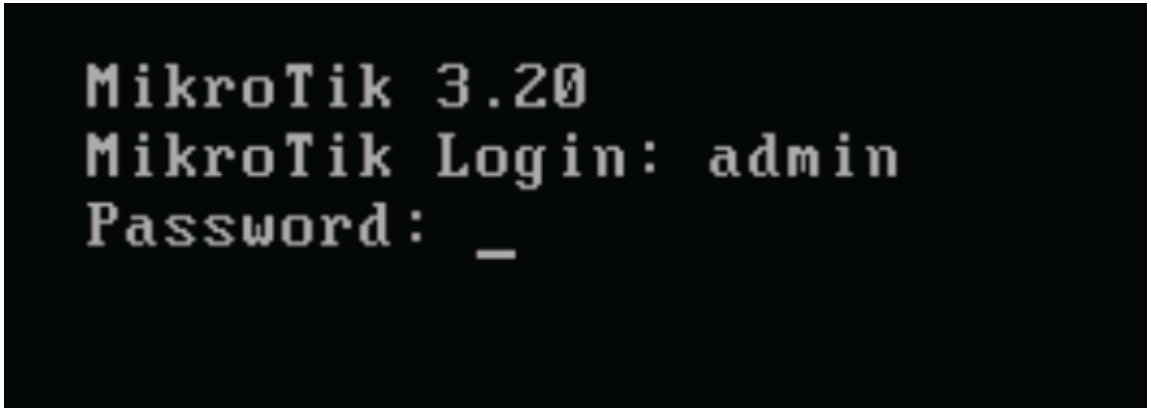
- **Do you want to keep old configuration? [y/n]:**

  Yes/No

- **Creating partition...**
- **Formatting disk...**
- **Software installed.**
- **Press ENTER to reboot**

Installation Check

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

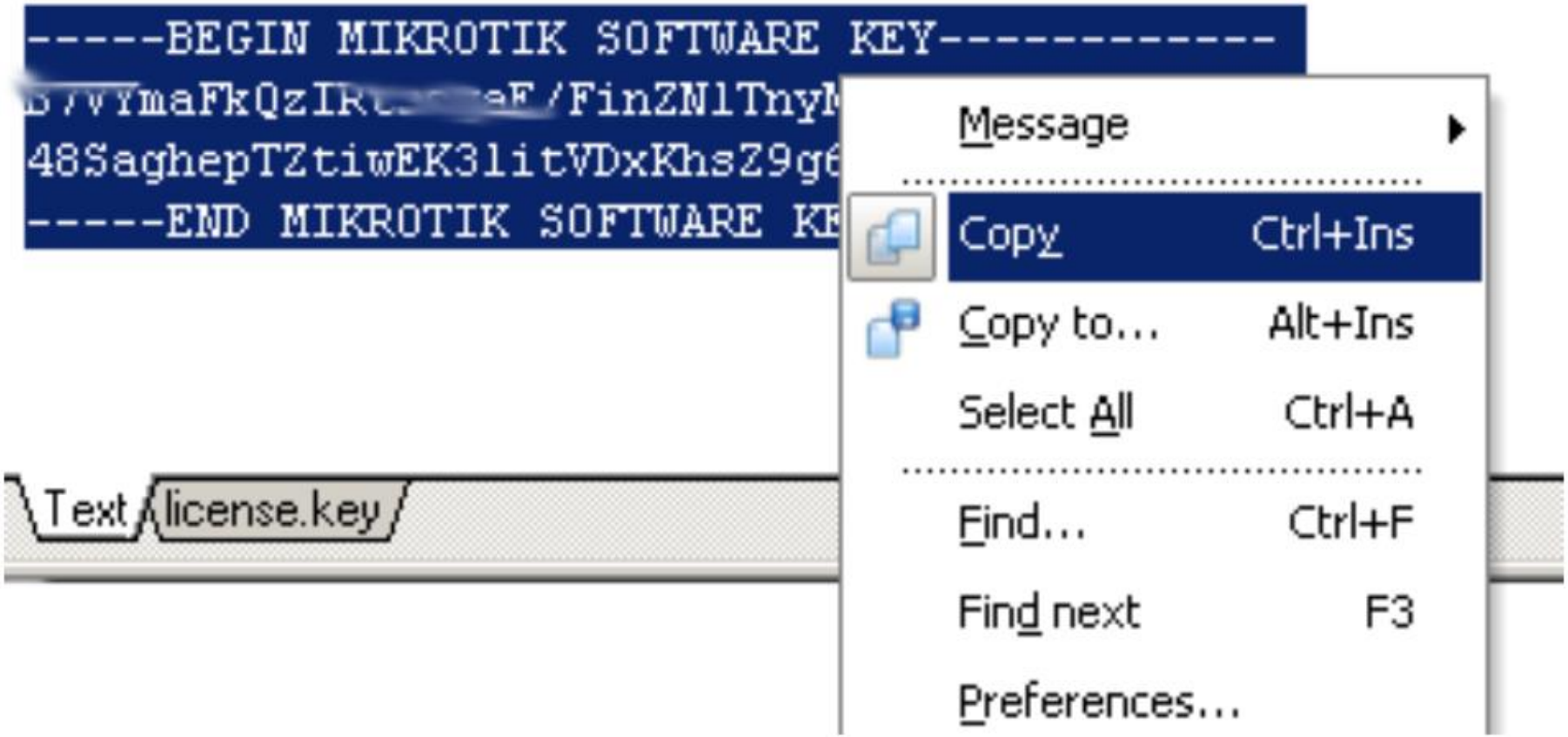


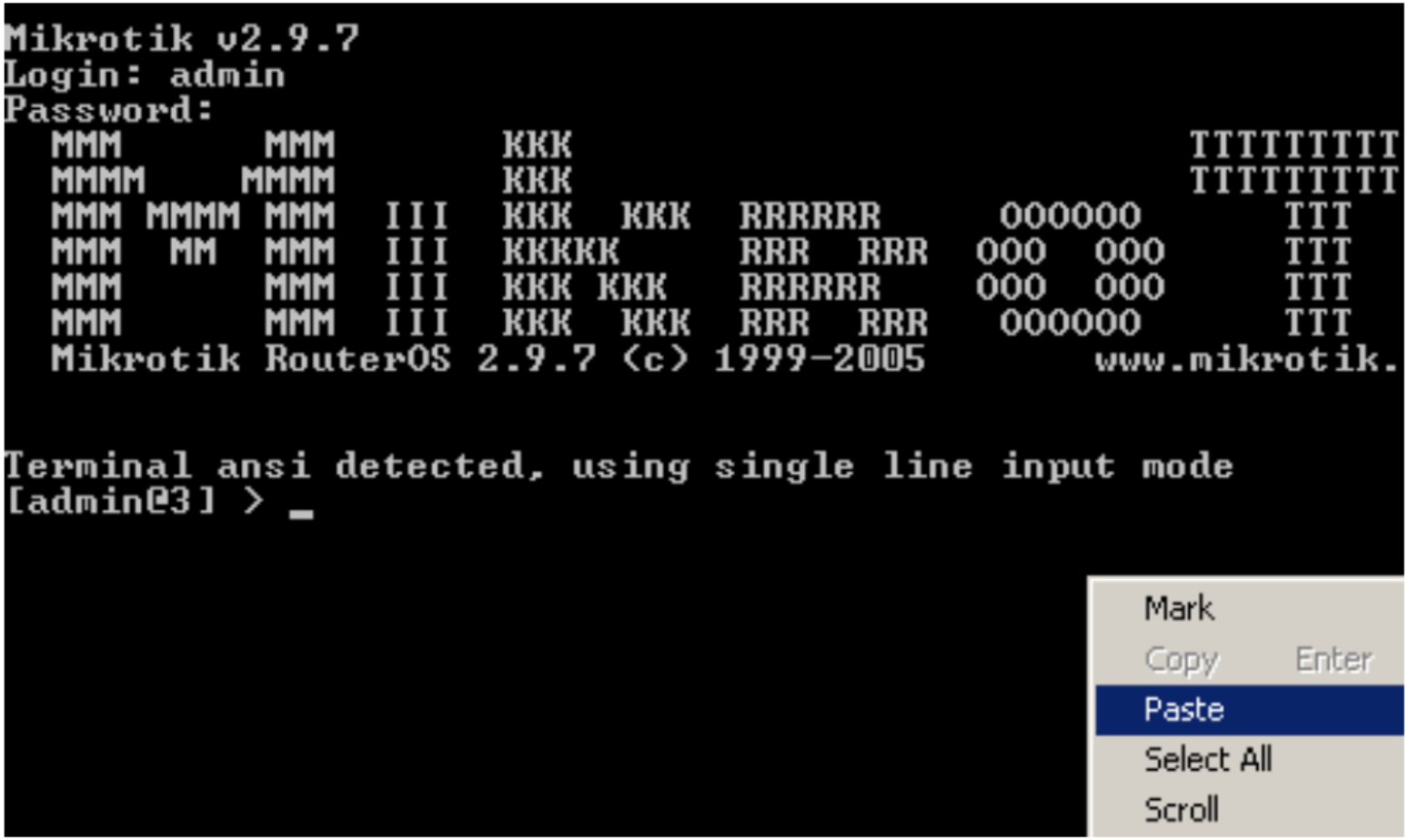
Demo

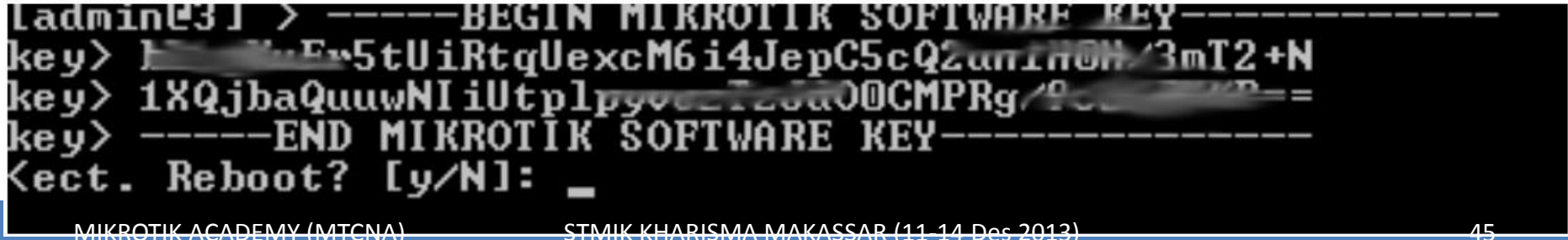
- License level 0 = Demo time 24 jam

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

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


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

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

[admin@MikroTik] > _
```

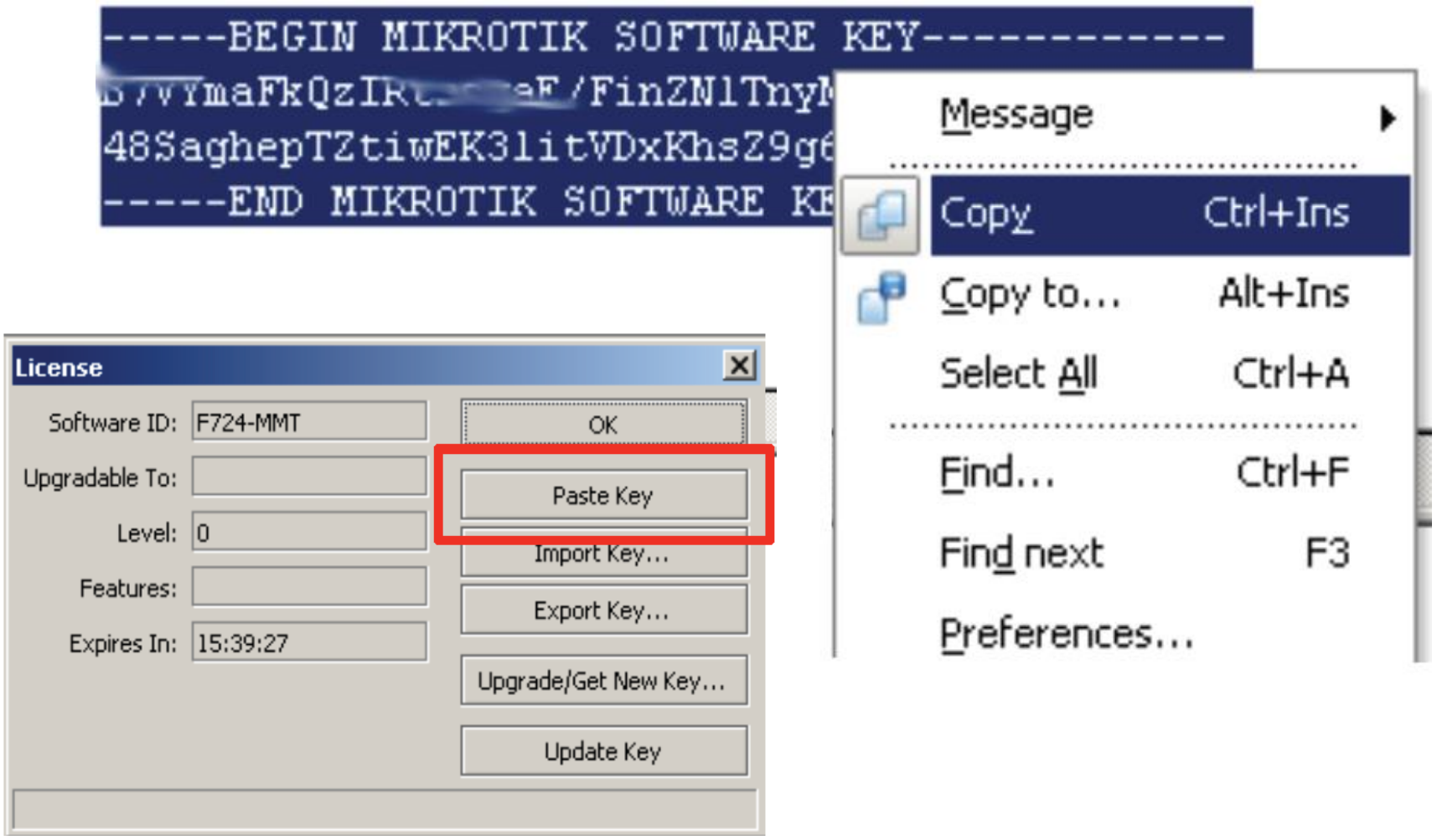
Input License (Telnet)




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

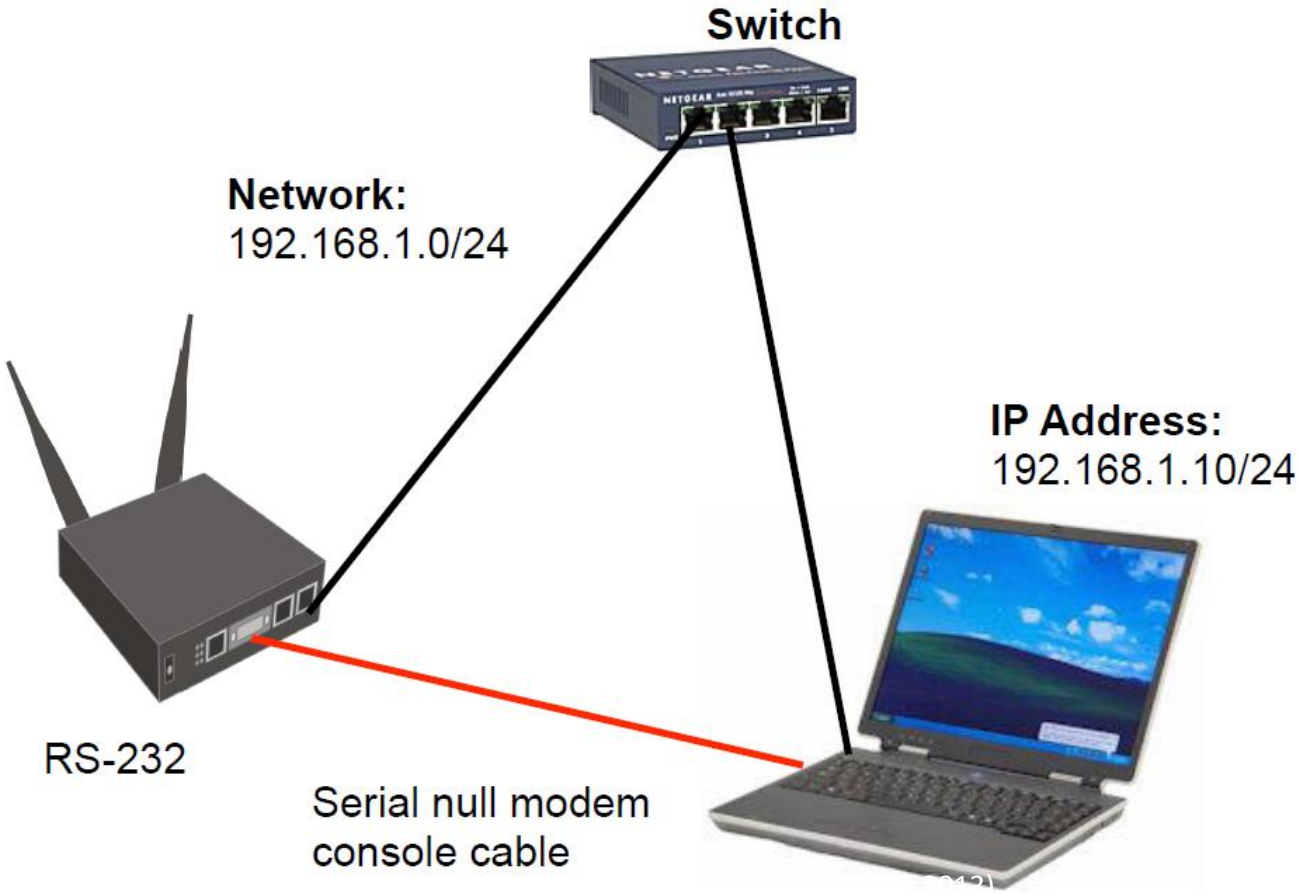

[admin@3] > -----BEGIN MIKROTIK SOFTWARE KEY----------
key> 5tUiRtqUexcM6i4JepC5cQ
key> 1XQjbaQuuwNIiUtpl
key> -----END MIKROTIK SOFTWARE KEY----------
Reboot? [y/N]: _

Input License (Winbox)



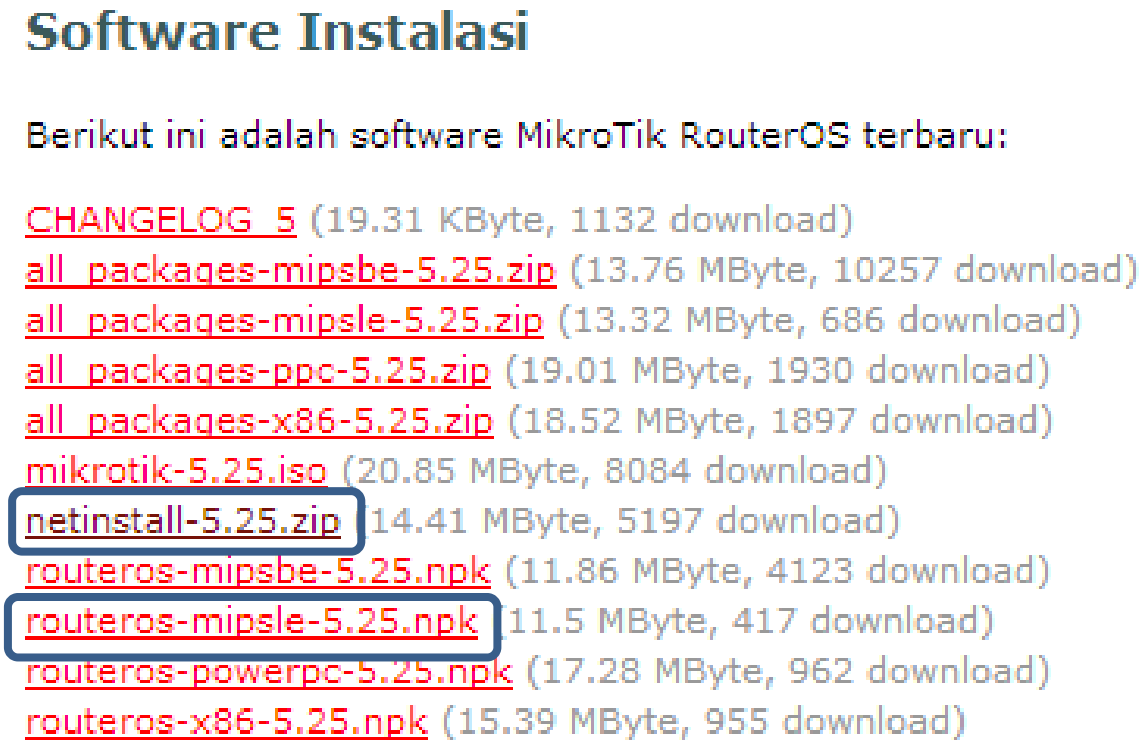
Netinstall

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



Netinstall

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



Software Instalasi

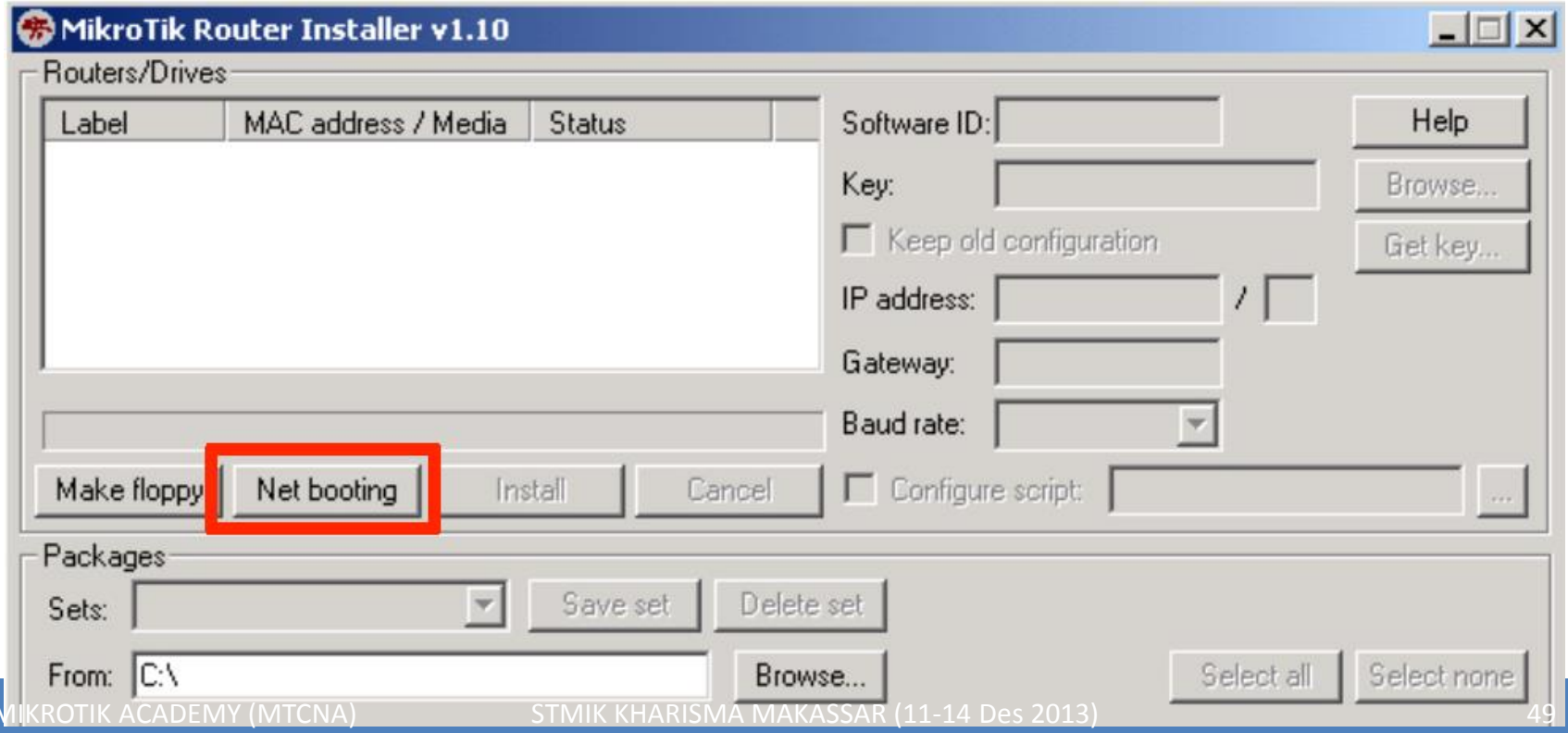
Berikut ini adalah software MikroTik RouterOS terbaru:

CHANGELOG 5 (19.31 KByte, 1132 download)
all_packages-mipsbe-5.25.zip (13.76 MByte, 10257 download)
all_packages-mipsle-5.25.zip (13.32 MByte, 686 download)
all_packages-ppc-5.25.zip (19.01 MByte, 1930 download)
all_packages-x86-5.25.zip (18.52 MByte, 1897 download)
mikrotik-5.25.iso (20.85 MByte, 8084 download)
netinstall-5.25.zip (14.41 MByte, 5197 download)
routeros-mipsbe-5.25.npk (11.86 MByte, 4123 download)
routeros-mipsle-5.25.npk (11.5 MByte, 417 download)
routeros-powerpc-5.25.npk (17.28 MByte, 962 download)
routeros-x86-5.25.npk (15.39 MByte, 955 download)

Untuk versi-versi sebelumnya, bisa didownload di www.RouterOS.co.id.

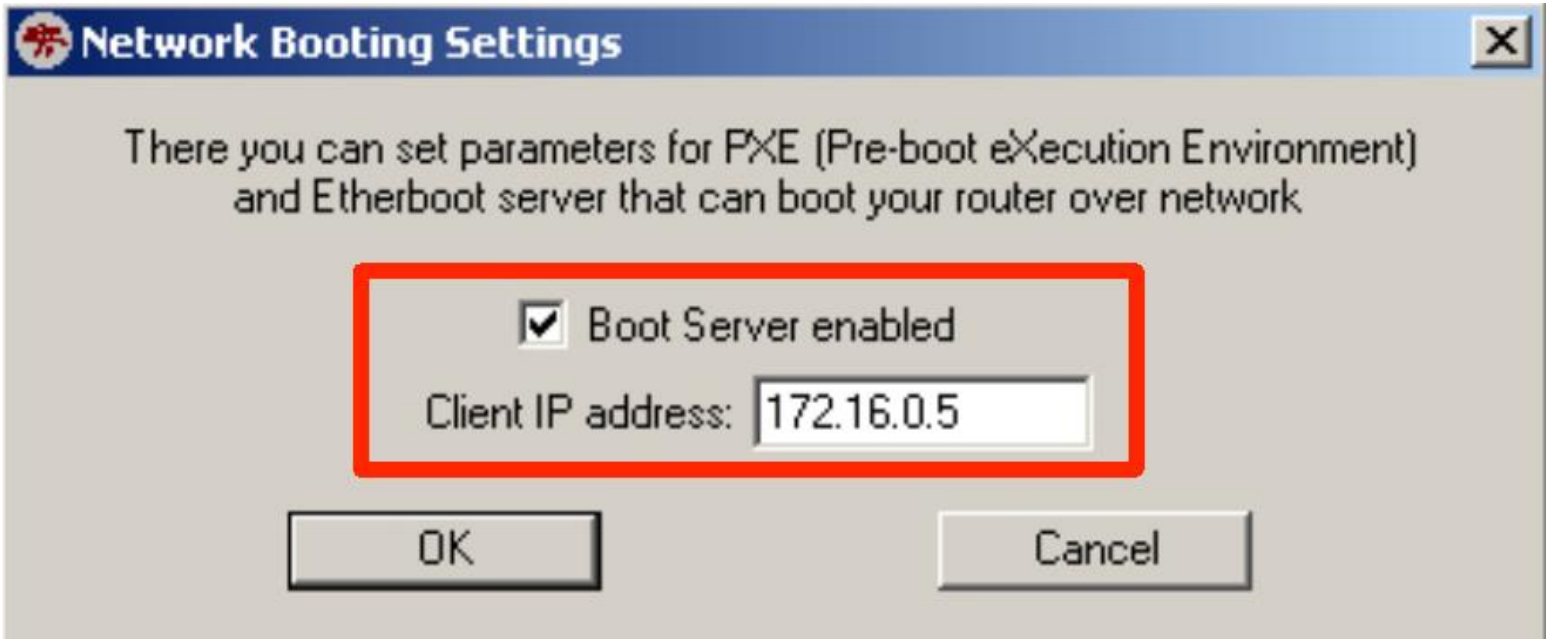
Netinstall

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



Netinstall - Config

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



Netinstall – BIOS Setting

Hidupkan router, masuk ke setting BIOS

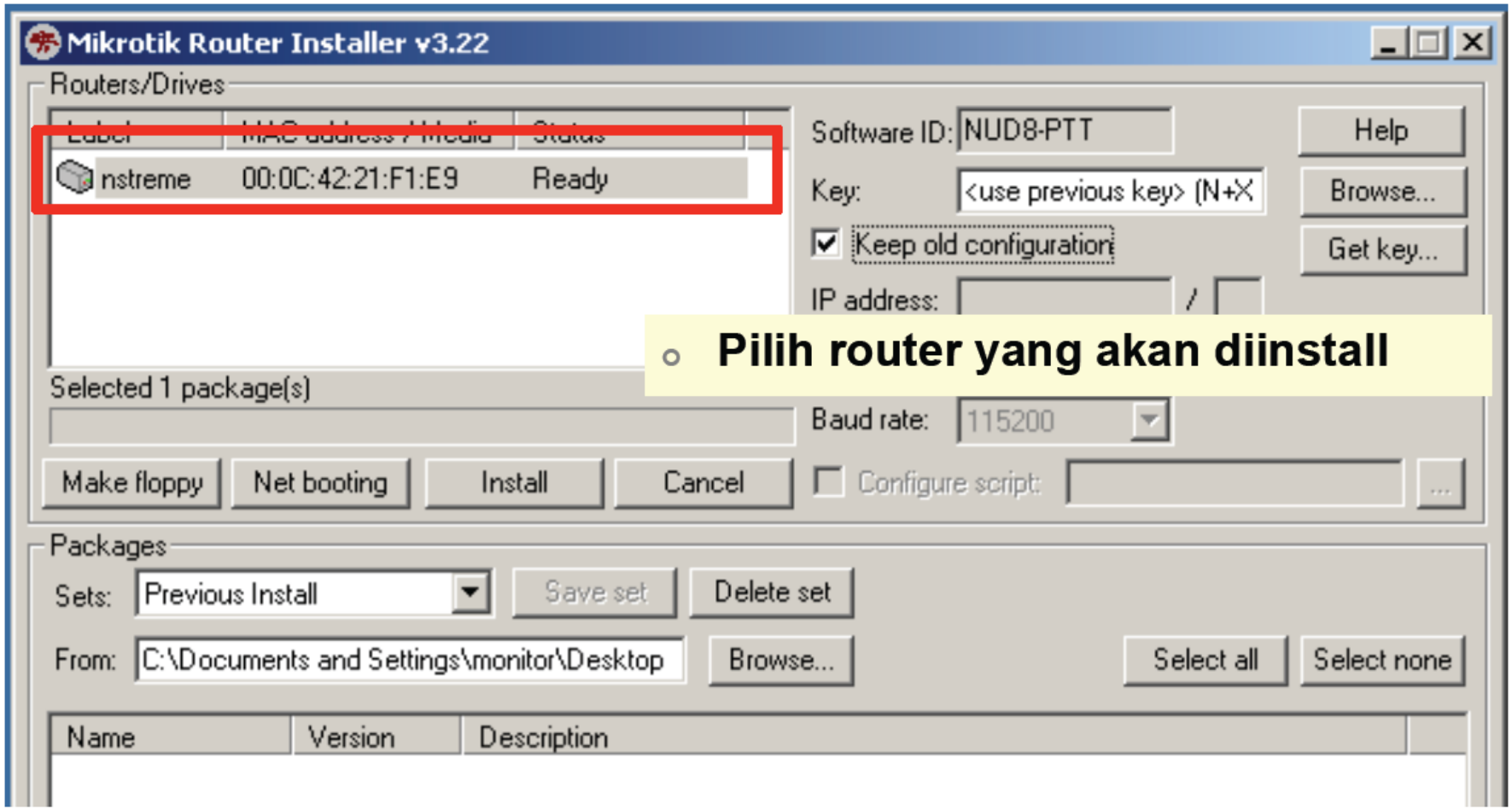
```
RouterBOOT booter 2.12

RouterBoard 333

CPU frequency: 333 MHz
  Memory size:  64 MB

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

Netinstall – BIOS Setting

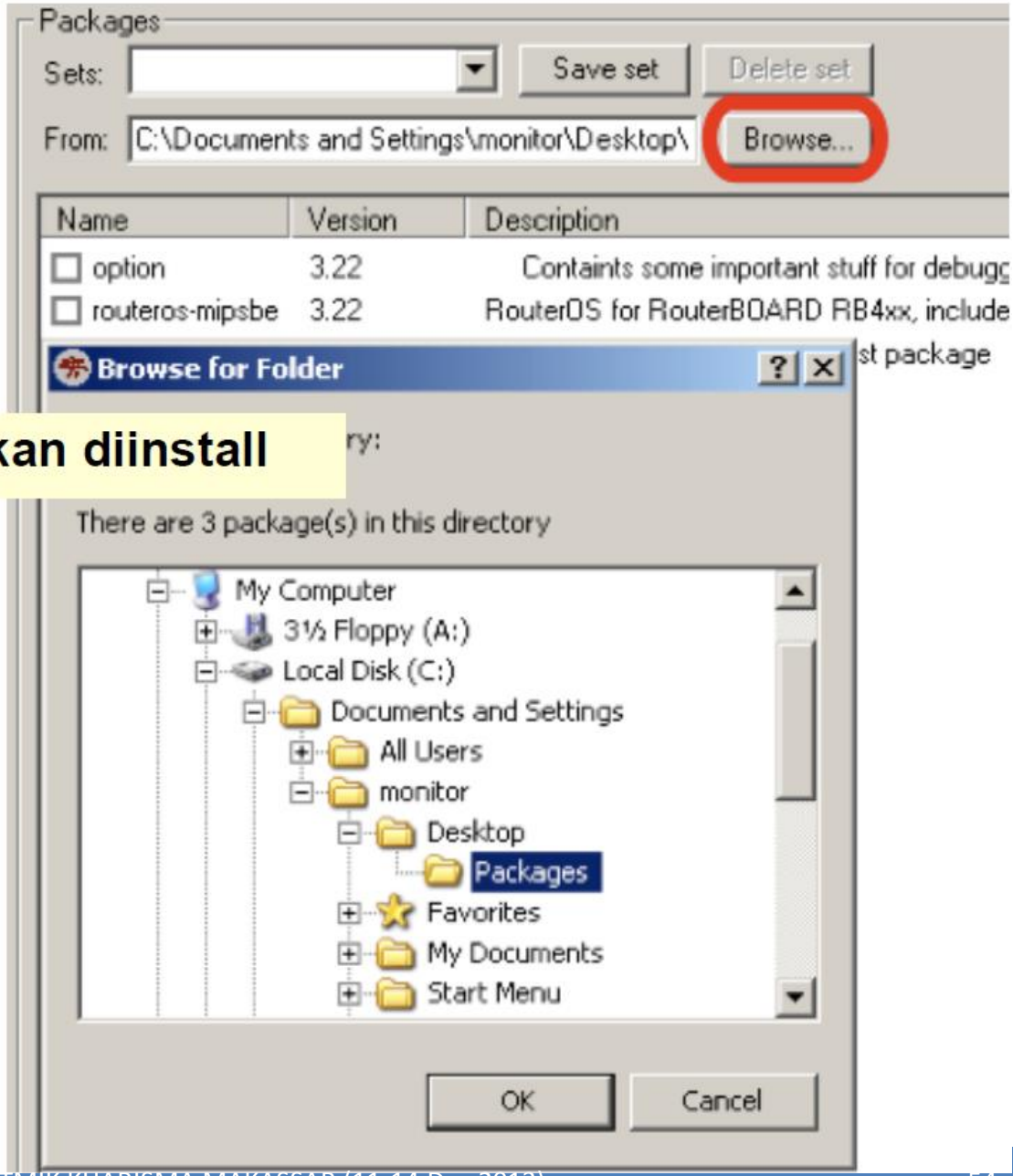
- ***RouterBOOT-2.41***
  What do you want to configure?
  d – boot delay
  k – boot key
  s – serial console
  n – silent boot
  o – boot device
  u – cpu mode
  f – cpu frequency
  r – reset booter configuration
  e – format nand
  g – upgrade firmware
  i – board info
  p – boot protocol
  b – booter options
  t – do memory testing
  x – exit setup
  your choice: o – boot device

- ***Select boot device:***
  e – boot over Ethernet
  **** n – boot from NAND, if fail then Ethernet***
  1 – boot Ethernet once, then NAND
  o – boot from NAND only
  b – boot chosen device
  f – boot Flash Configure Mode
  3 – boot Flash Configure Mode once, then NAND
  your choice: 1 – boot Ethernet once, then NAND

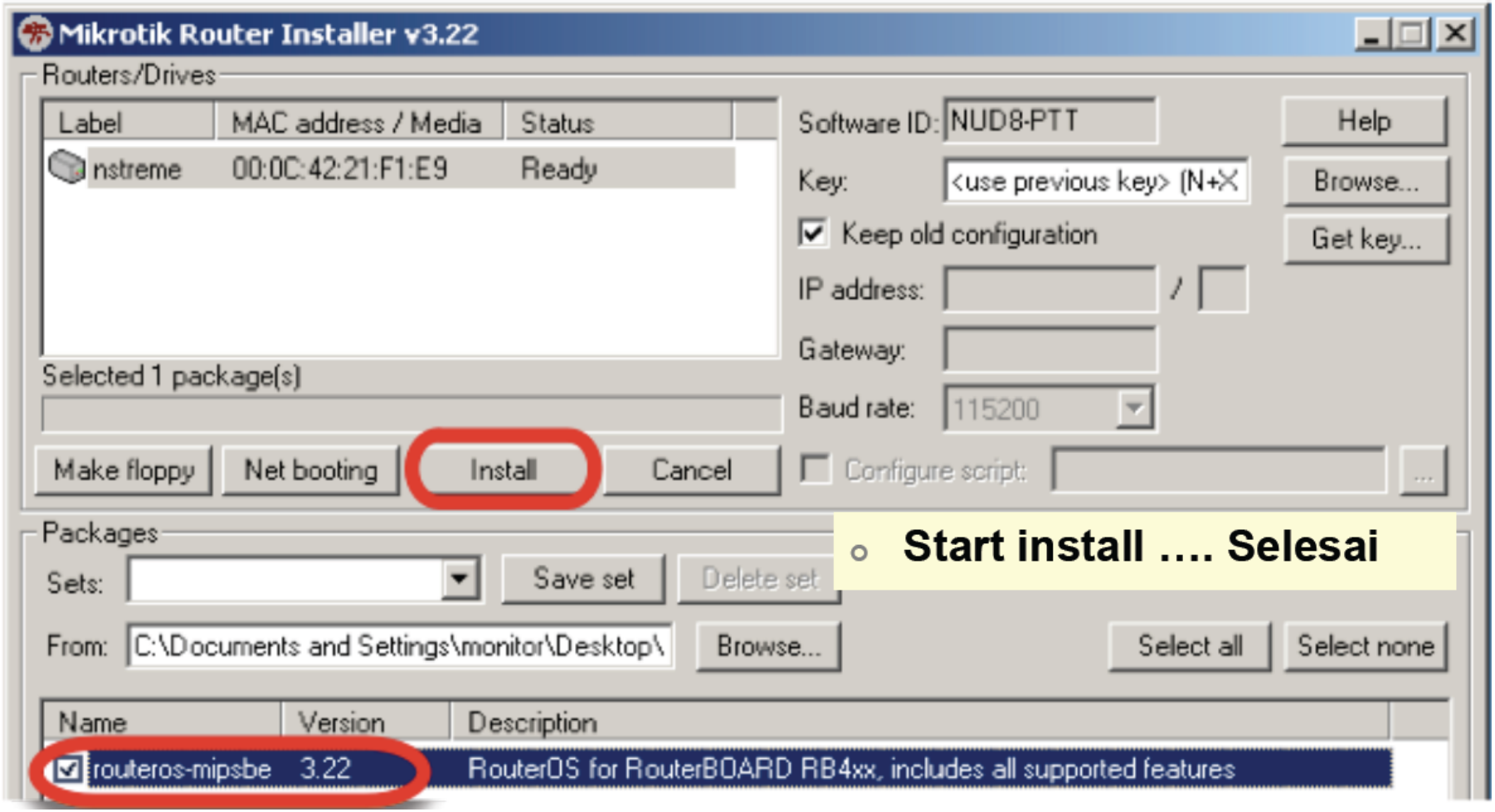
Netinstall - Install



- **Pilih module yang akan diinstall**

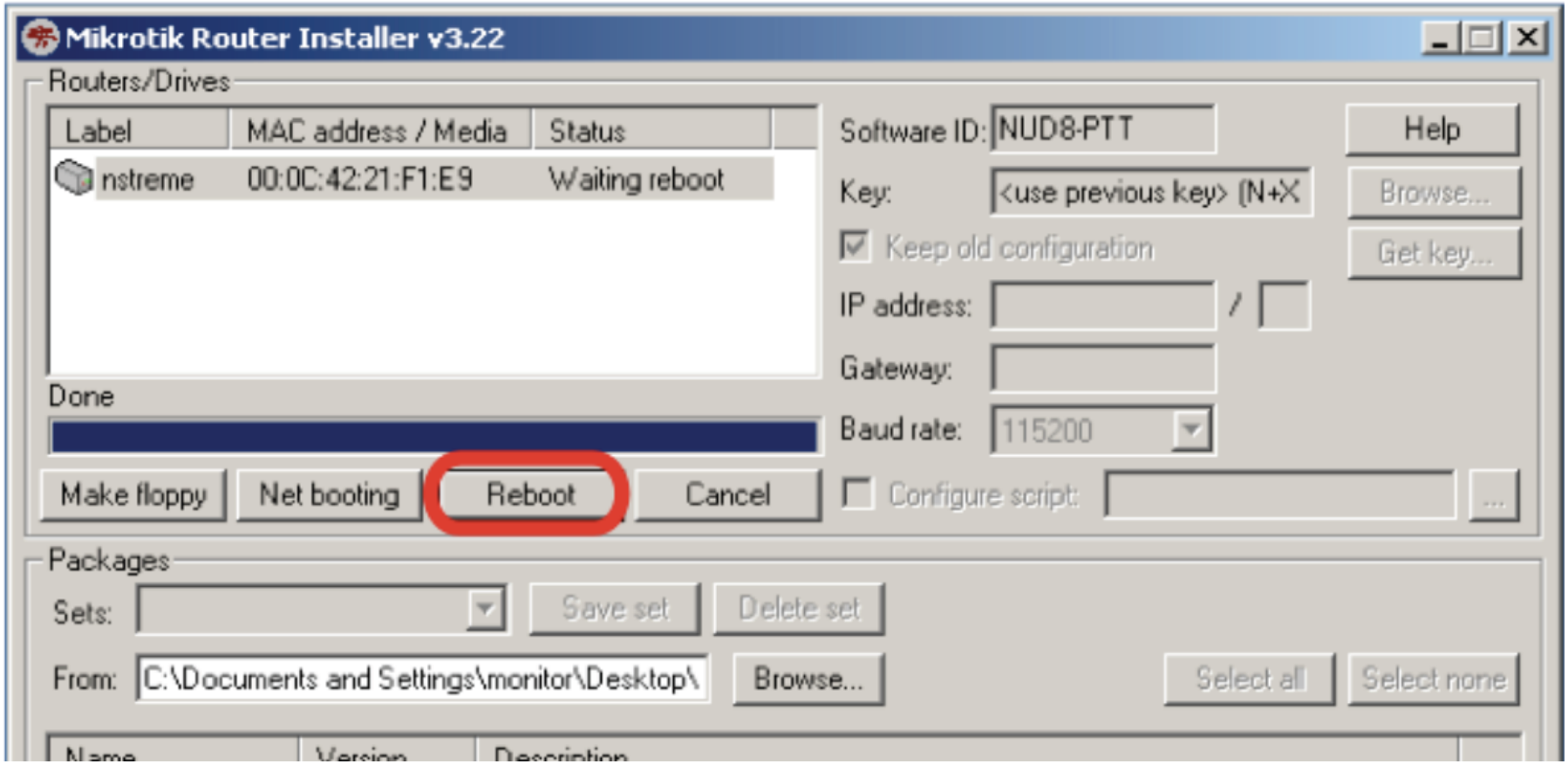


Netinstall - Install



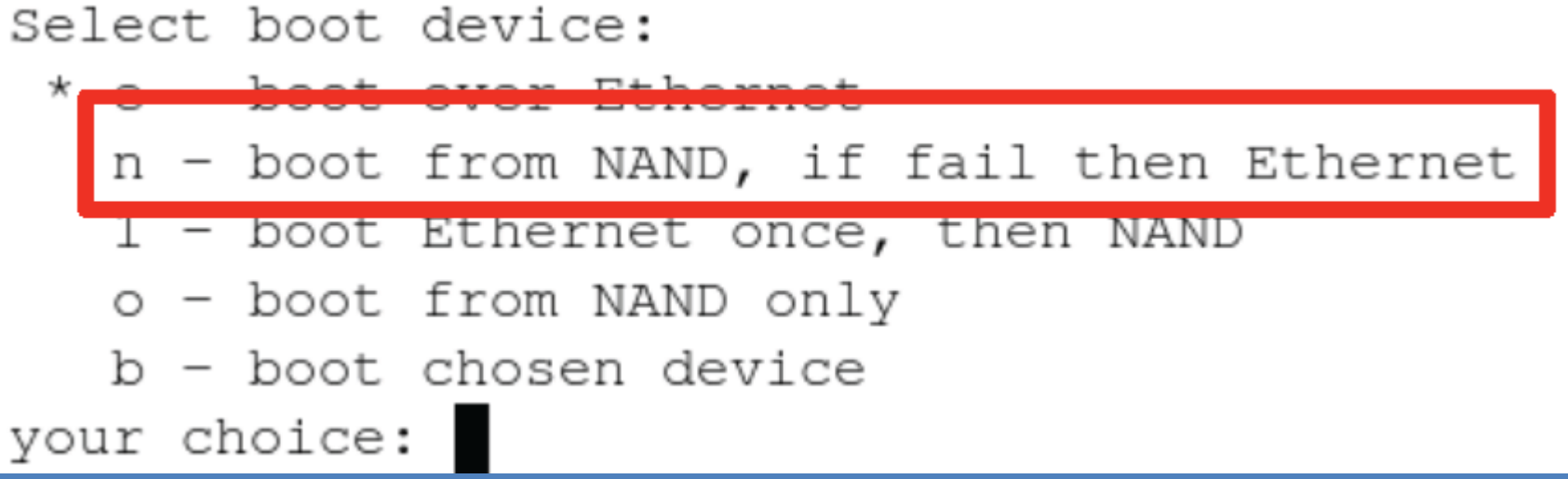
- **Start install …. Selesai**

Netinstall – Reboot



Netinstall - Cleanup

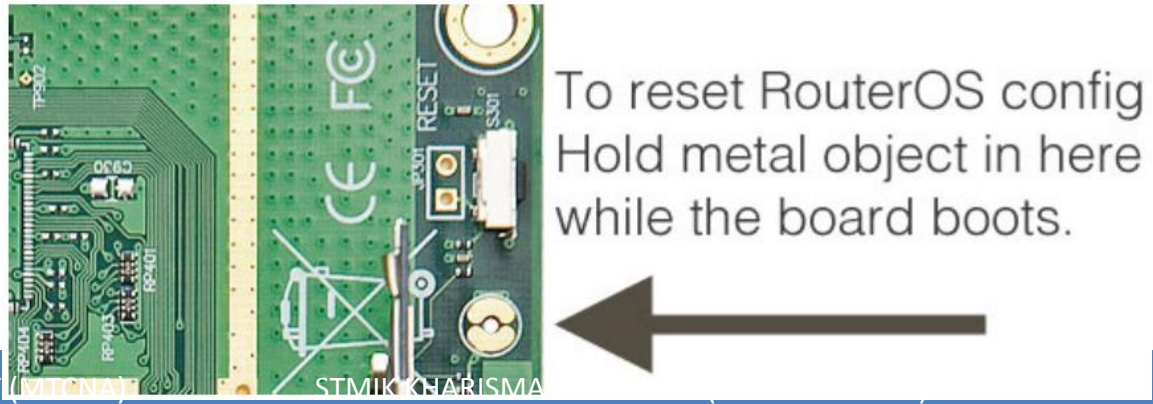
- **Kembalikan boot ke IDE / NAND drive**
- **Video Tutorial :**
  - **http://www.mikrotik.co.id/artikel_lihat.php?id=25**



Reset Password

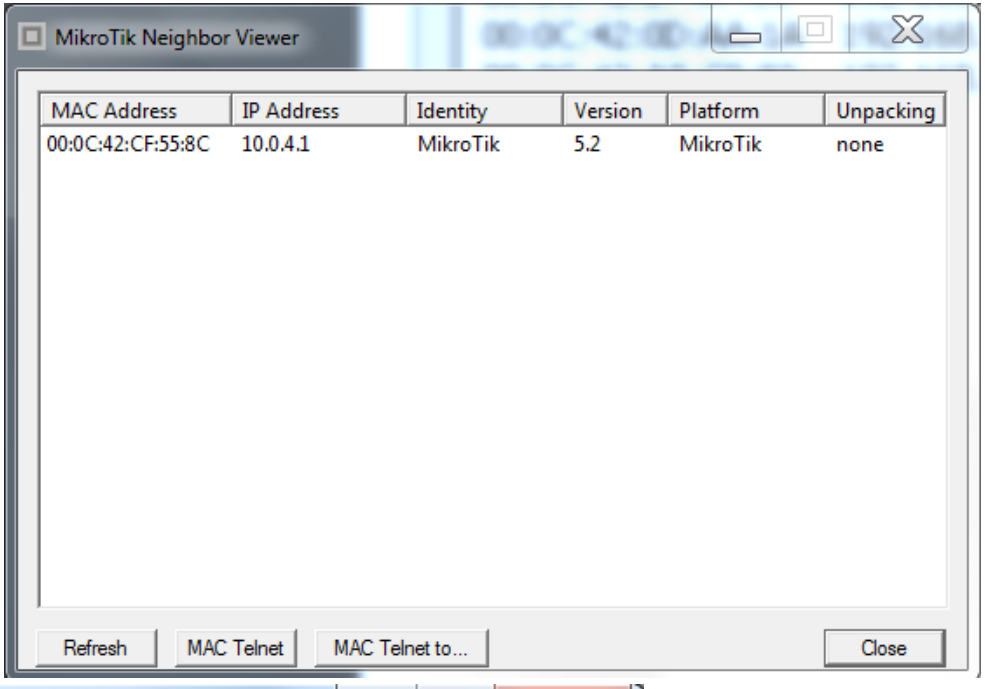
- Reset password bisa dilakukan di beberapa routerboard menggunakan tombol "**Reset**"

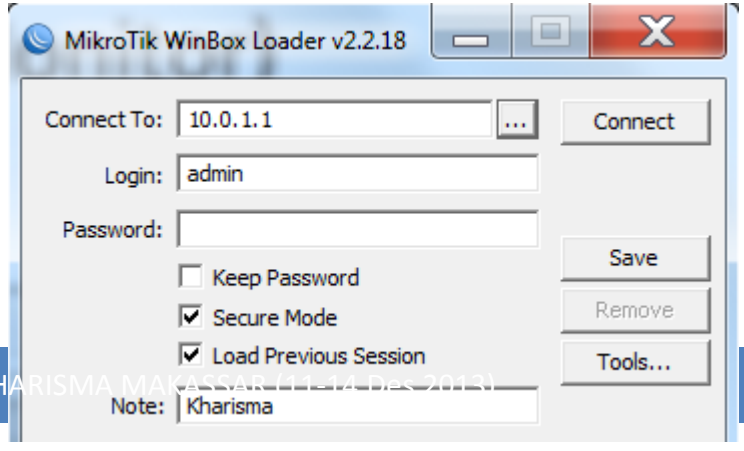
- Hard reset



First Time Accessing The Router

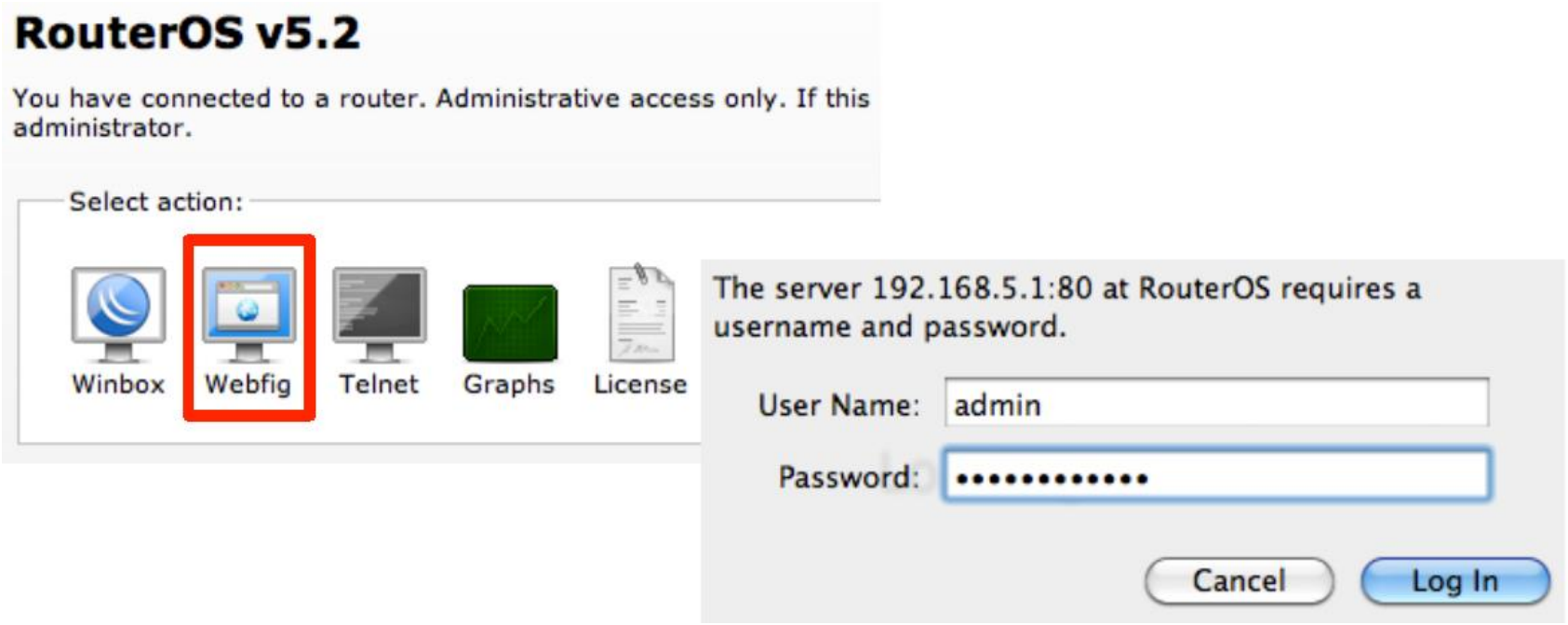
- Direct Console (Keyboard & Monitor)
- MAC-Winbox – Winbox.exe
- MAC-Telnet – NeighbourViewer.exe
- Null Modem cable
- SSH and Telnet



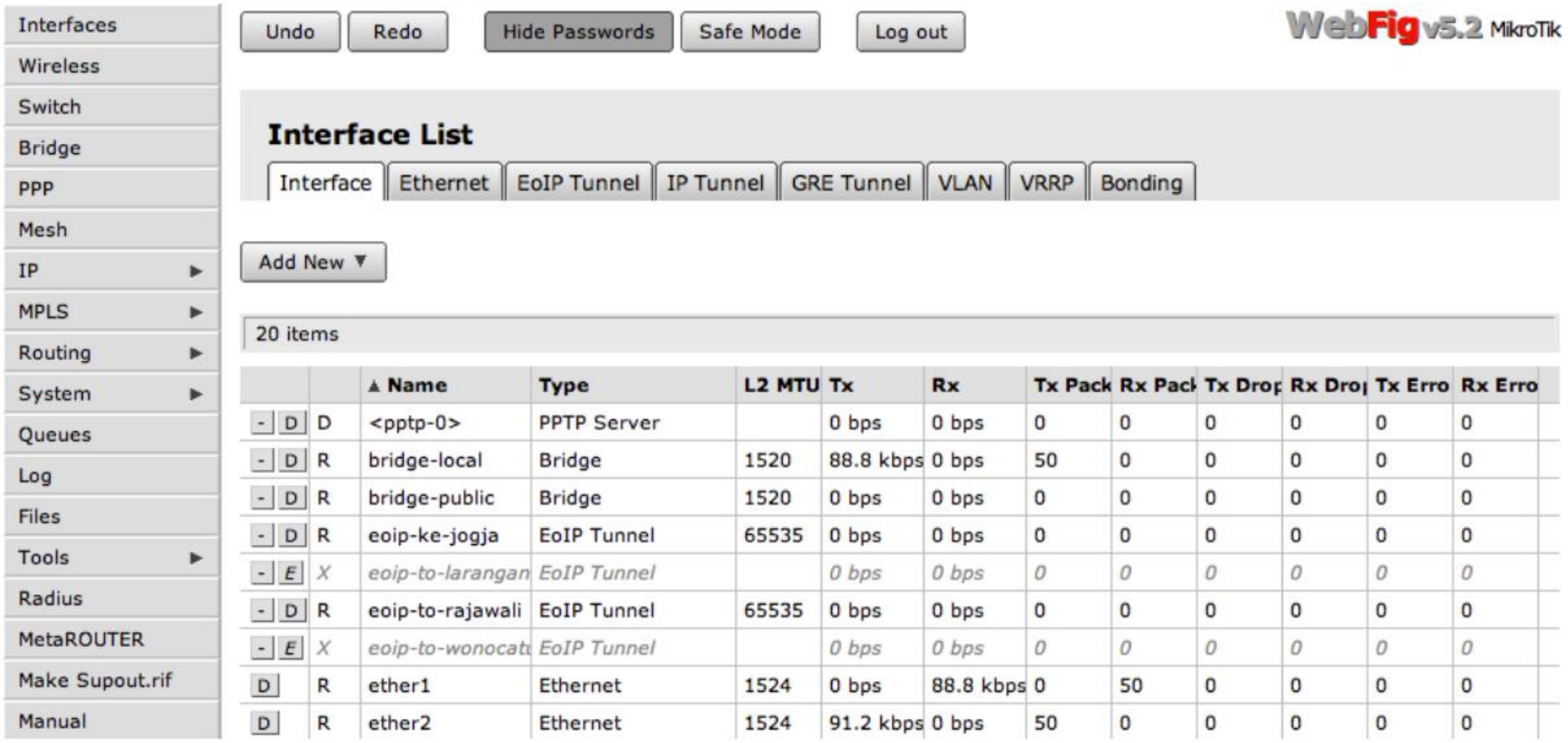


Access to Router - WebFig

Konfigurasi realtime berbasis Web memungkinkan konfigurasi mikrotik menggunakan perangkat mobile

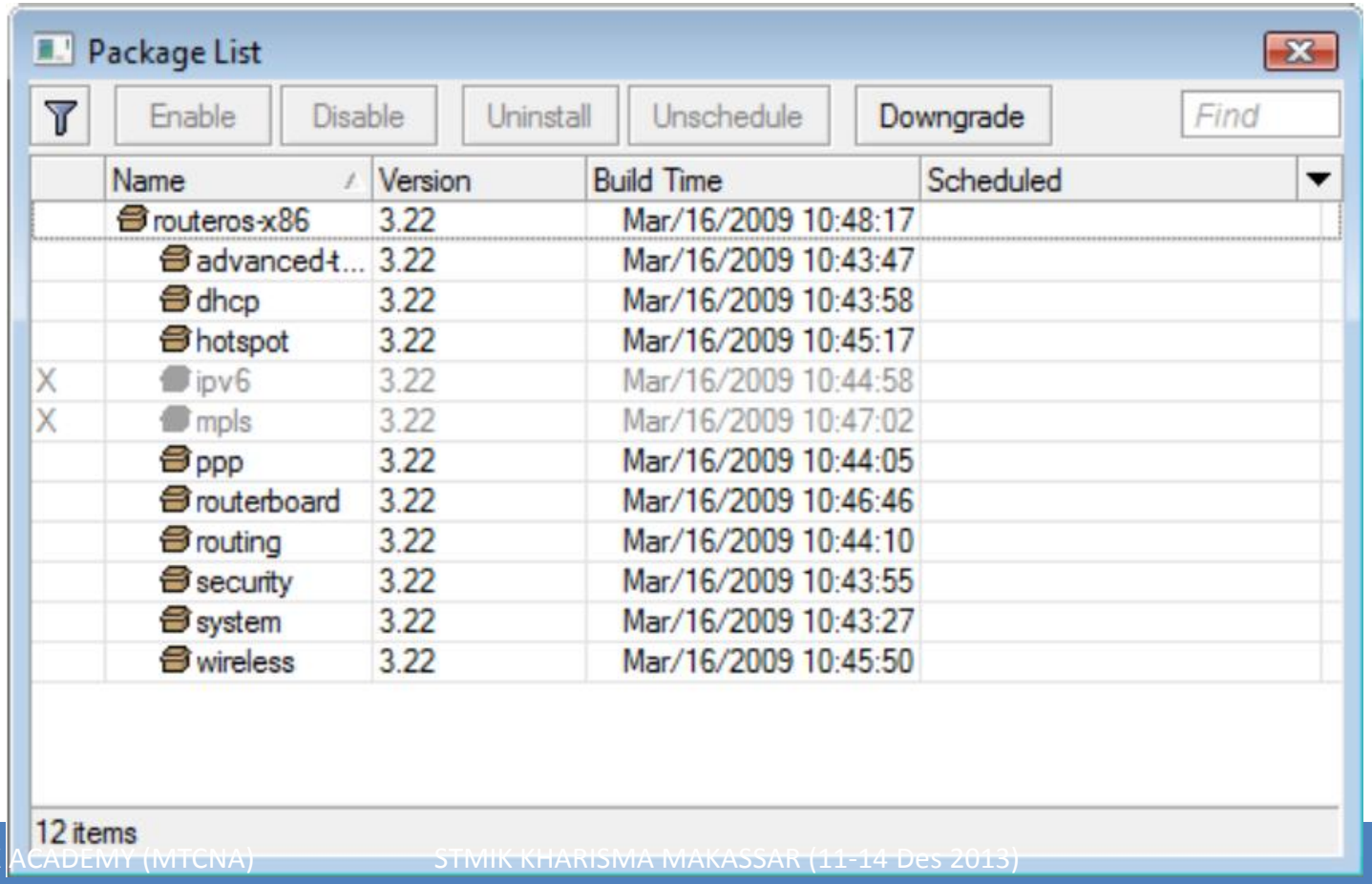


Access to Router - WebFig



System Package Check

- Pada terminal: /system package print



RouterOS Package

Nama Paket	Fungsi
advanced-tools	email client, ping, netwatch
dhcp	DHCP server dan client
Hotspot	hotspot gateway
Ntp	NTP server
Ppp	PPP,PPTP,L2TP,PPPoE
Routerboard	Fungsi khusus Routerboard
Routing	RIP, OSPF, BGP
Security	secure winbox, SSH, IPSec
Wireless	Wireless 802.11a/b/g
user-manager	User-Manager management system
Ipv6	IPv6

Version Upgrade

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

Version Downgrade

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

  admin@MikroTik] system package> downgrade

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

  system will reboot shortly

Command Line Interface

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

General Command CLI

Perintah	Fungsi
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

Perintah	Fungsi
?	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

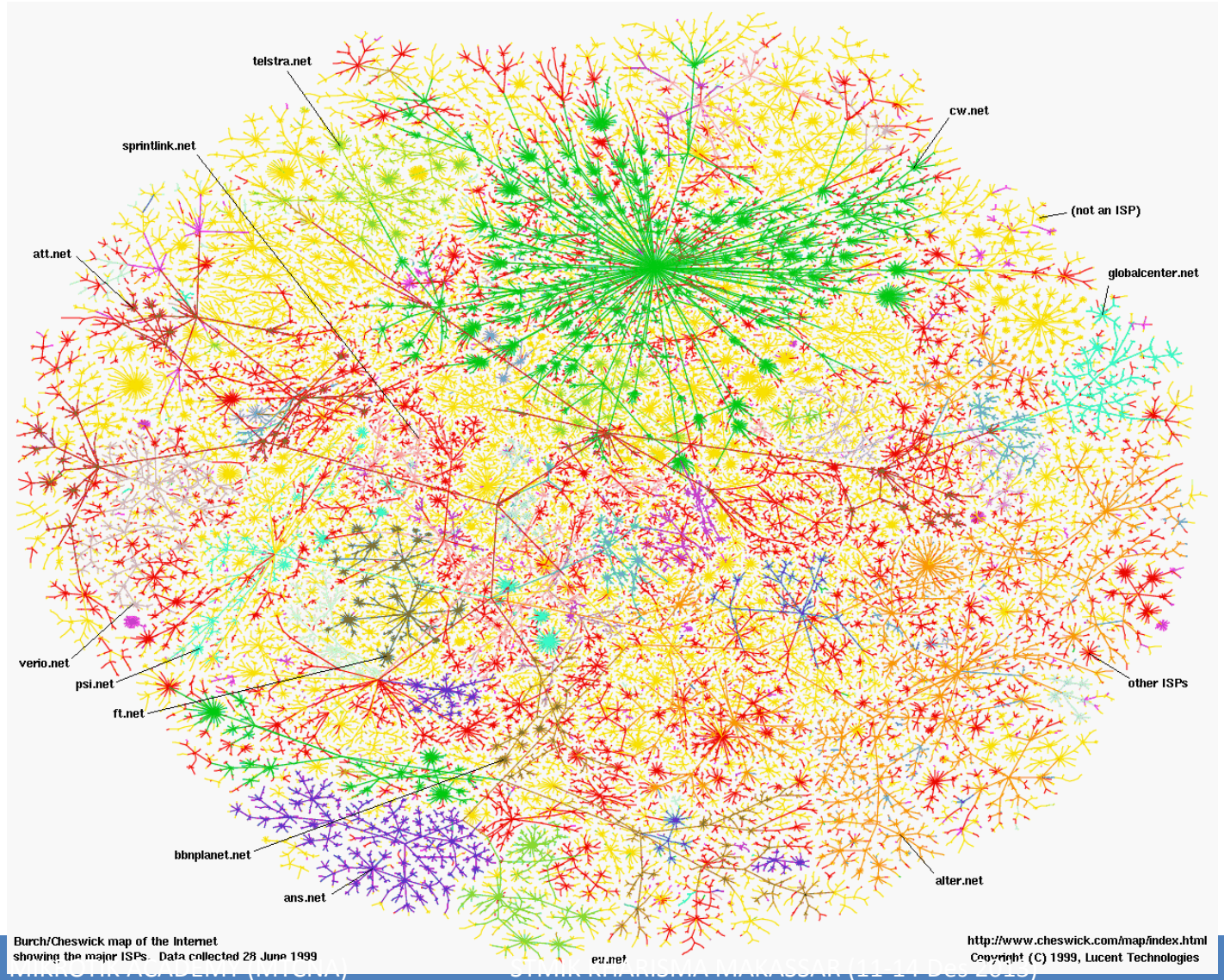
- Quick Typing
  - [TAB] untuk melengkapi perintah tertentu
    - */system shut [TAB] = /system shutdown*
  - Juga bisa menggunakan singkatan
    - /sys shut = /system shutdown

TCP/IP Basics

TCP/IP Outline

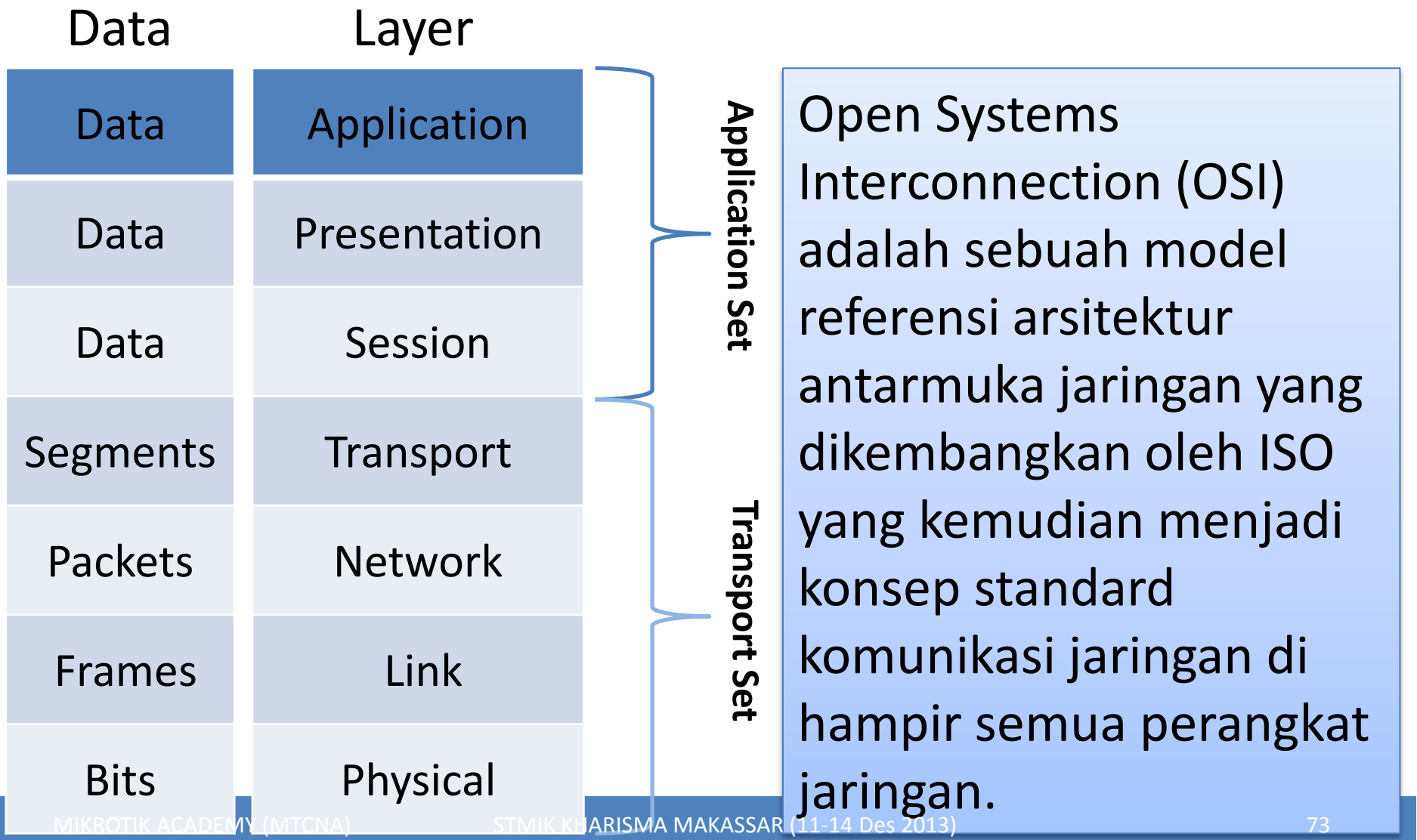
- OSI Layer
- Packet Header
- Mac Address
- IP Address and subnetting
- IP Protocol
- Basic networking, DNS, gateway

Internet Topologi



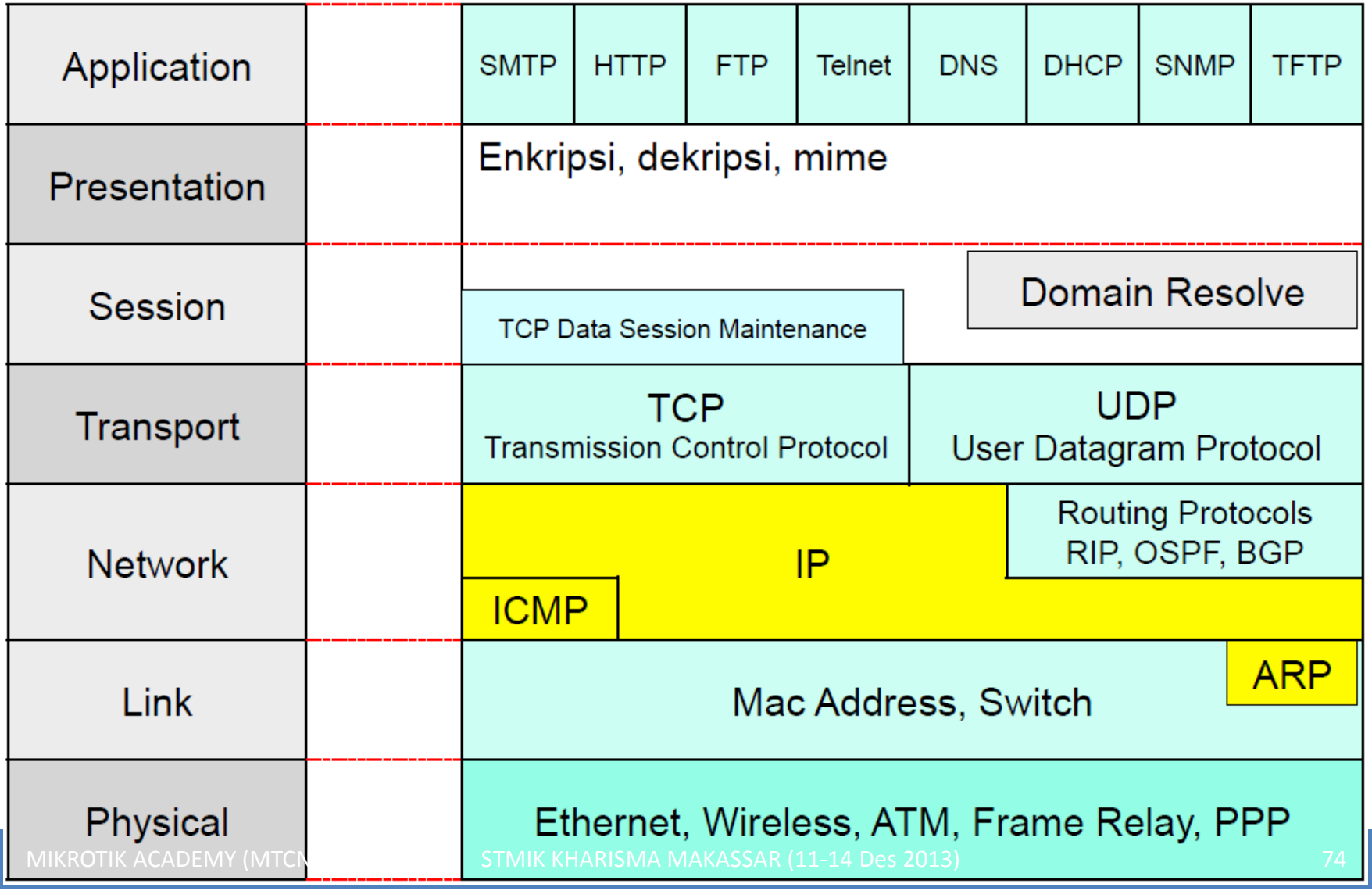
Jutaan host yang harus bisa berkomunikasi satu sama lain.

OSI Layer dan Protokol

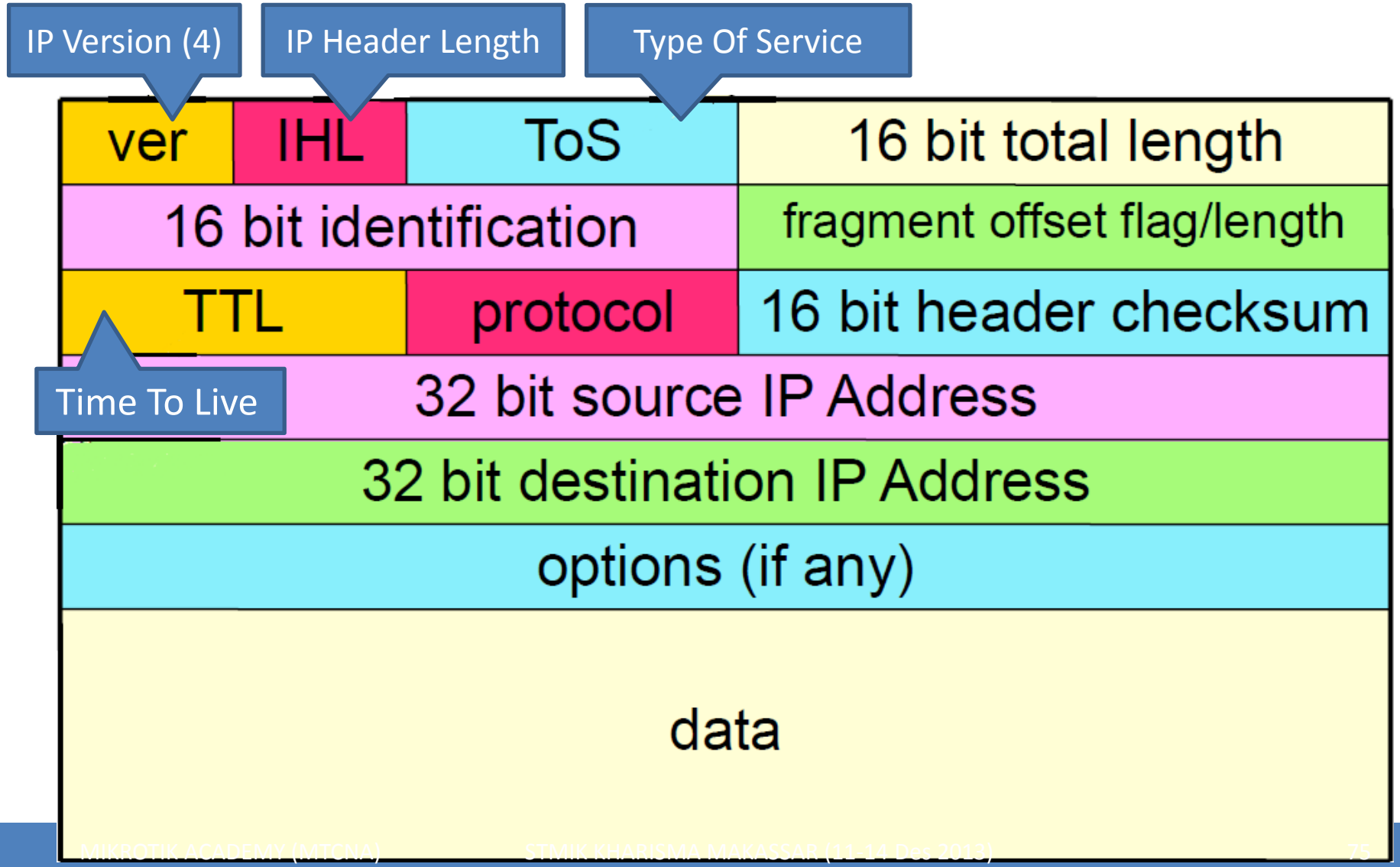


Open Systems Interconnection (OSI) adalah sebuah model referensi arsitektur antarmuka jaringan yang dikembangkan oleh ISO yang kemudian menjadi konsep standard komunikasi jaringan di hampir semua perangkat jaringan.

OSI Layer dan Protokol



Packet Header

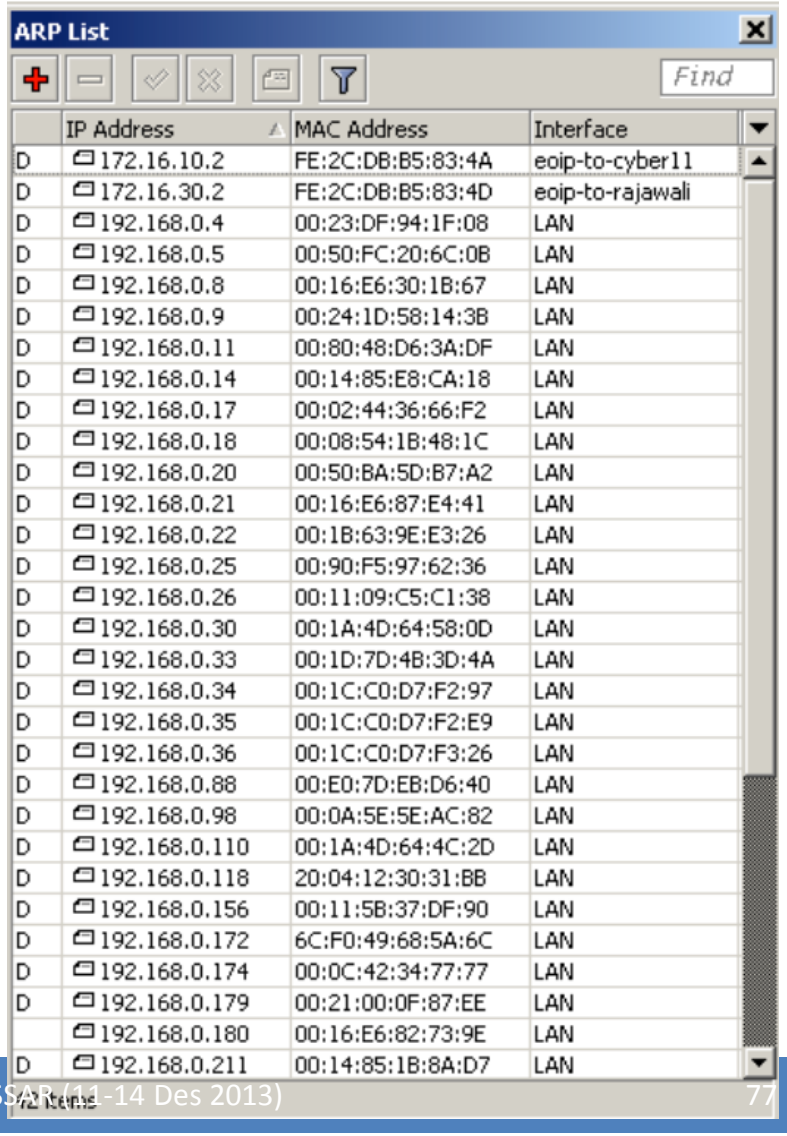


MAC Address

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

ARP Table

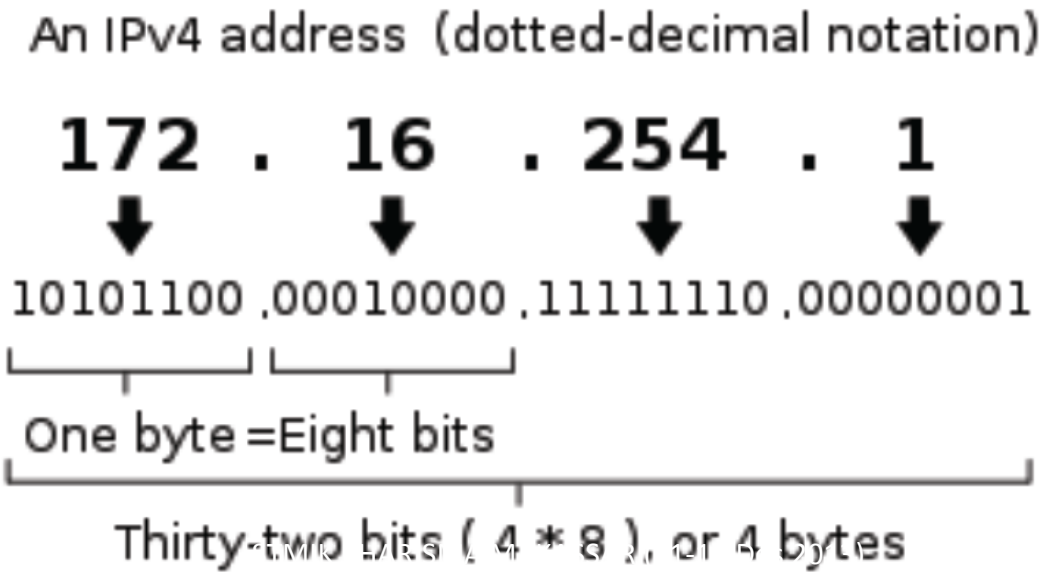
- Merupakan protokol penghubung antara layer **2** data-link dan **3** network.
- ARP Table di router merupakan daftar host yang terhubung langsung berisi informasi pasangan macaddress dan ip address.
- Di **IPv6** arp digntikan dengan **NDP** (Network Discovery Protocol).



	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
	192.168.0.180	00:16:E6:82:73:9E	LAN
D	192.168.0.211	00:14:85:1B:8A:D7	LAN

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 Protocol

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

ICMP (Internet Control Message Protocol)

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

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

UDP (User Datagram Protocol)

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

TCP (Transmission Control Protocol)

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

Prinsip Kerja TCP

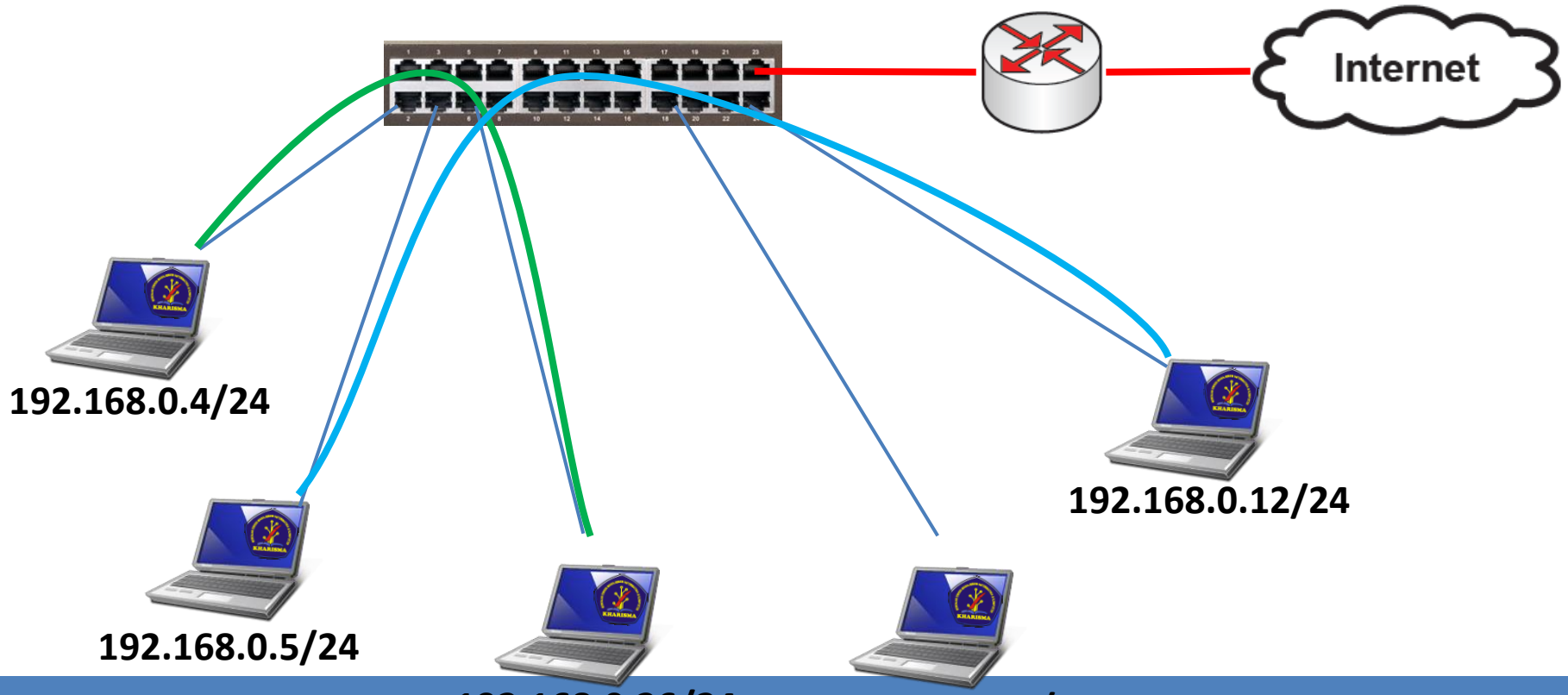
- Connection Oriented
  - Koneksi diawali dengan proses “handshake”
    - Client → SYN → Server
    - Server → SYN-ACK → Client
    - Client → ACK → Server
- Reliable Transmission
  - Mampu melakukan pengurutan paket data, setiap byte data ditandai dengan nomor yang unik
- Error Detection
  - Jika terjadi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

Prinsip Kerja TCP

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

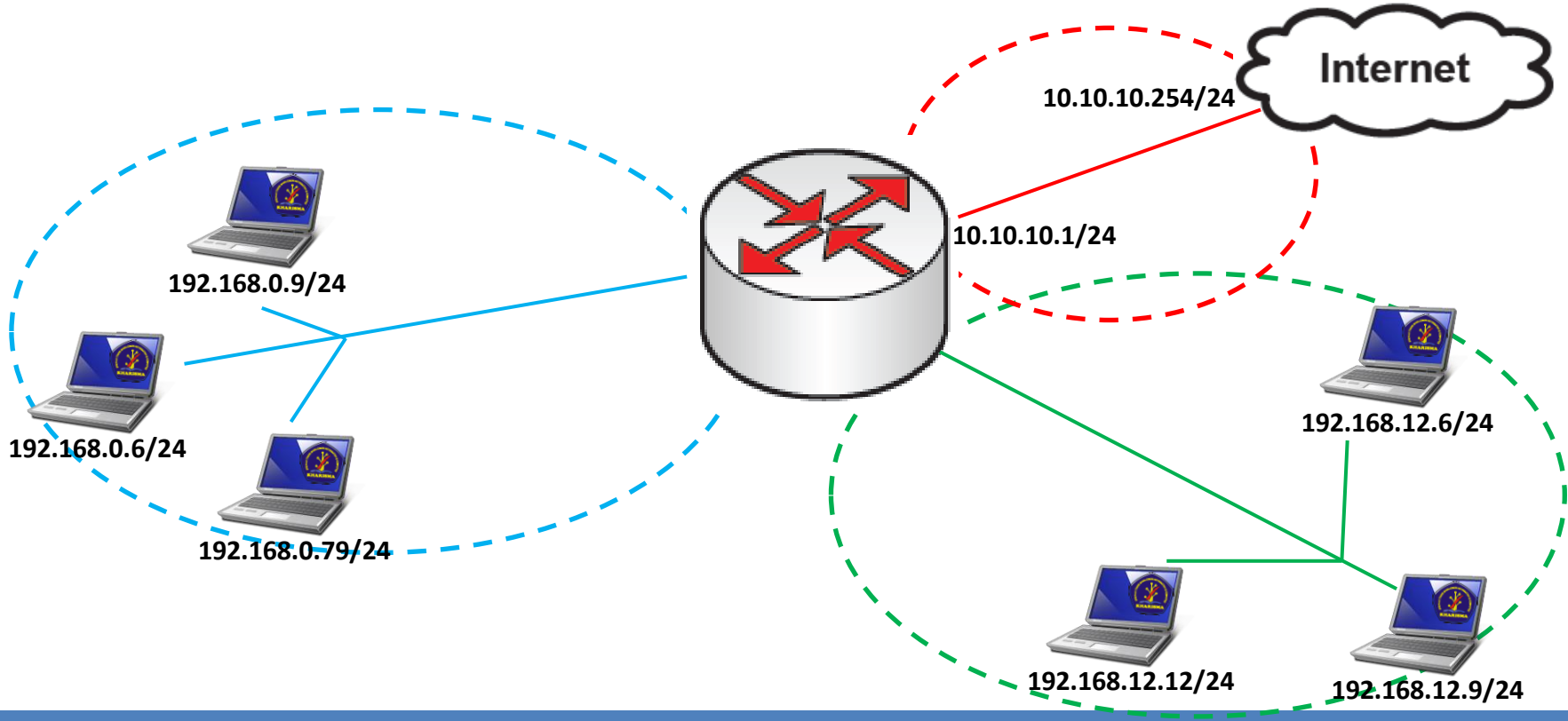
Konsep Dasar Jaringan

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



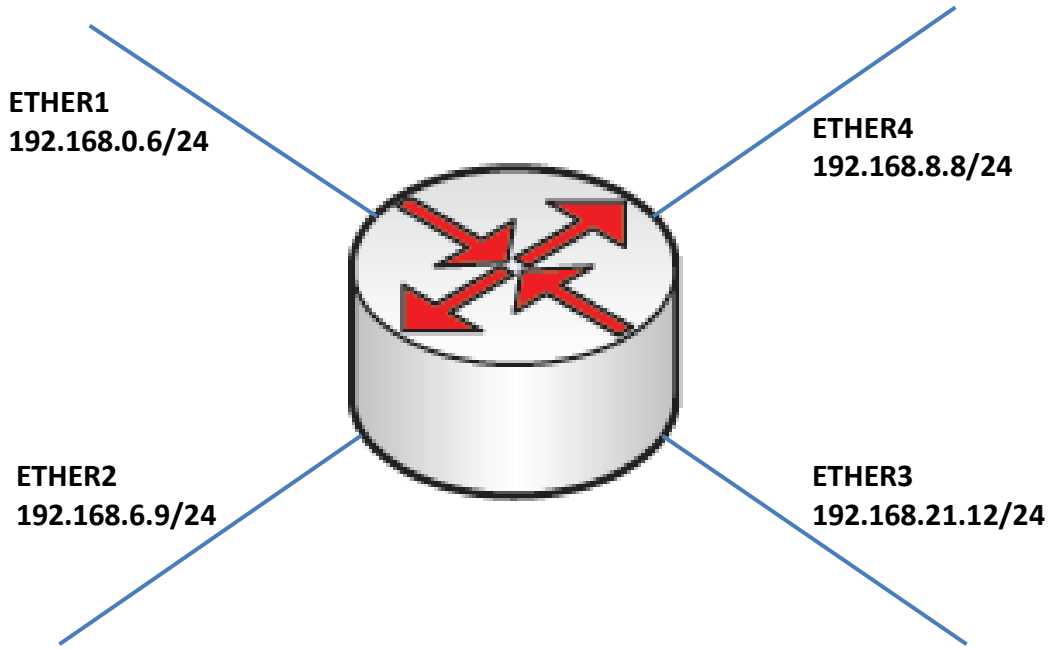
Konsep Dasar Jaringan

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



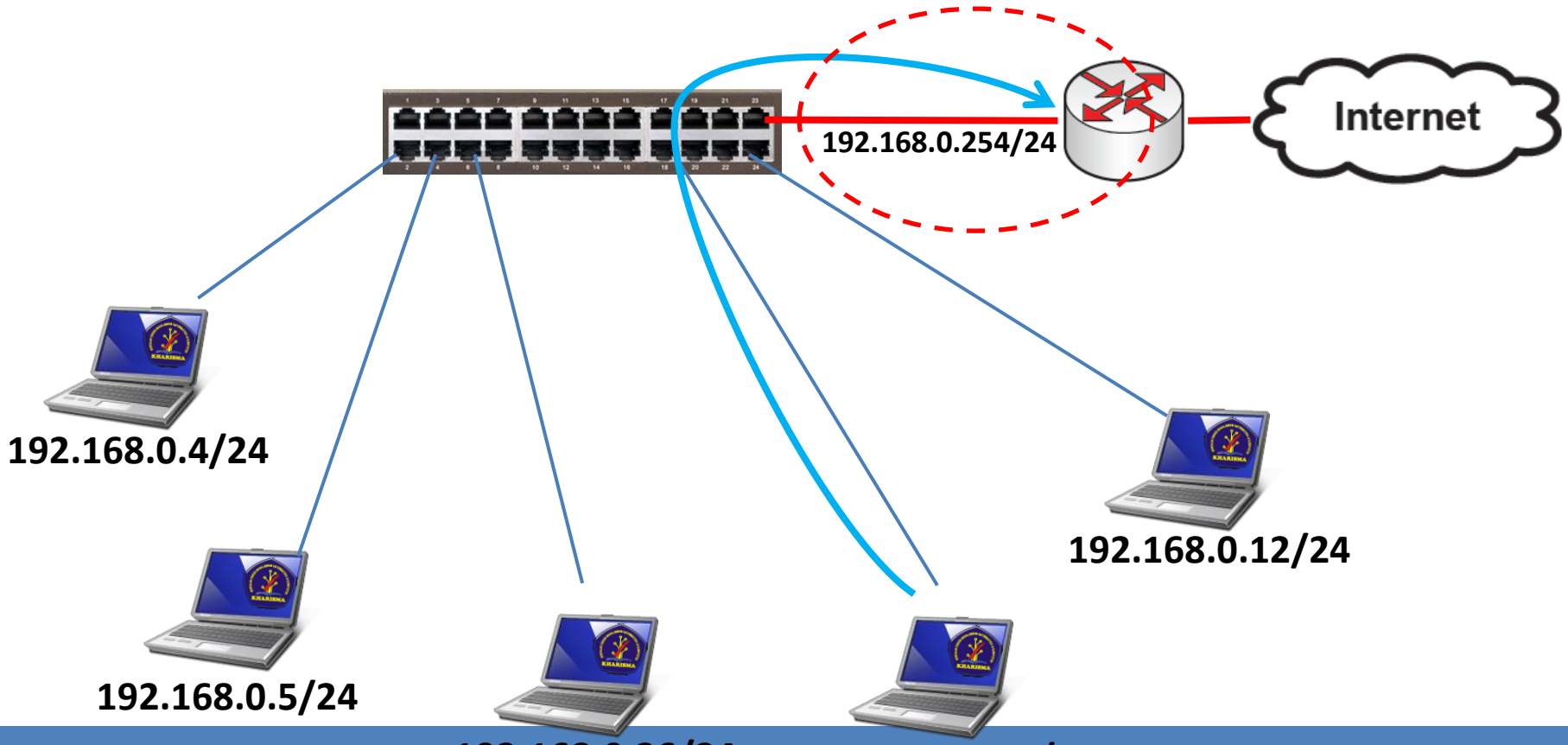
Konsep Dasar Jaringan

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



Konsep Dasar Jaringan

- Default gateway menentukan ke arah mana trafik harus disalurkan untuk menuju ke internet
  - From : **192.168.0.8** To : **222.24.112.34**



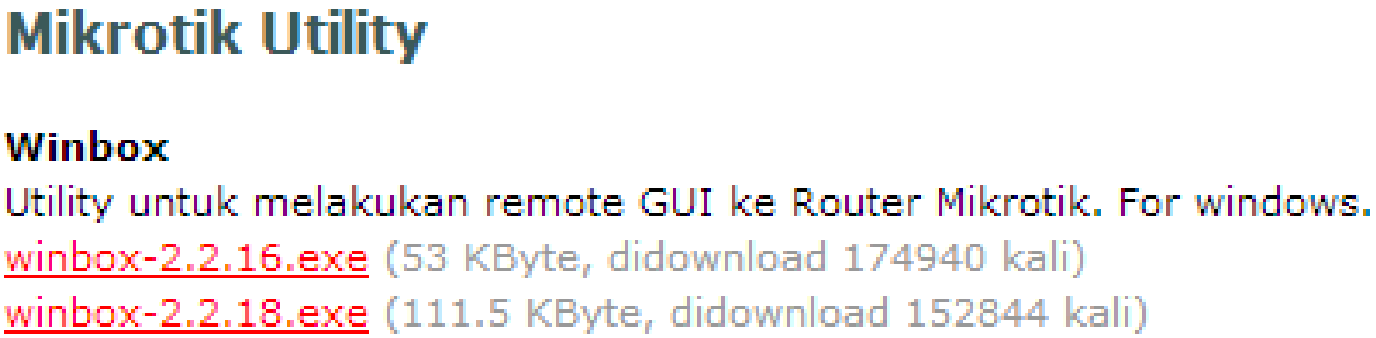
Konsep Dasar Jaringan

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

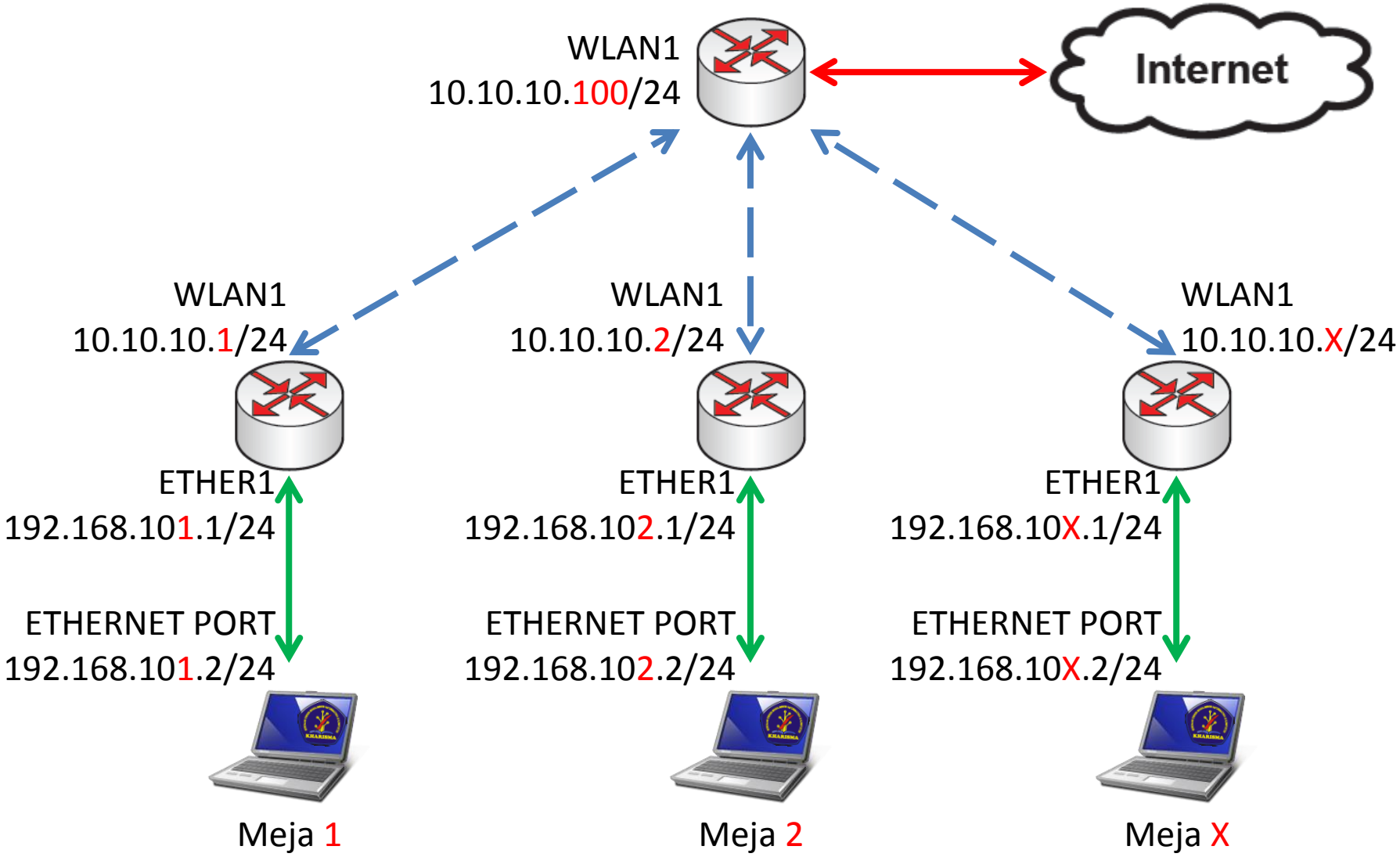
RouterOS
Basic Configuration

Winbox - Download

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



Basic Config - Topology



IP Configuration

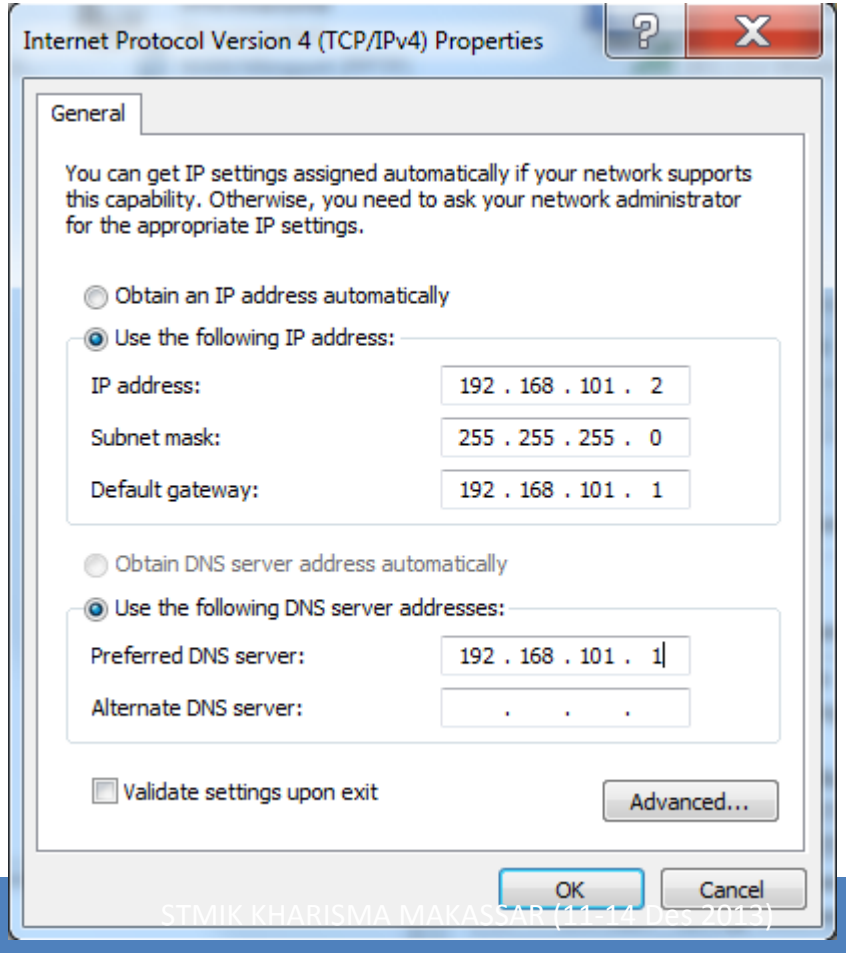
- Routerboard Setting
  - WAN IP : 10.10.10.**X**/24
  - Gateway : 10.10.10.100
  - LAN IP : 192.168.10**X**.1/24
  - DNS : 10.10.10.100
  - Src-NAT and DNS Server
- Laptop Setting
  - IP Address : 192.168.10**X**.2/24
  - Gateway : 192.168.10**X**.1
  - DNS : 192.168.10**X**.1

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

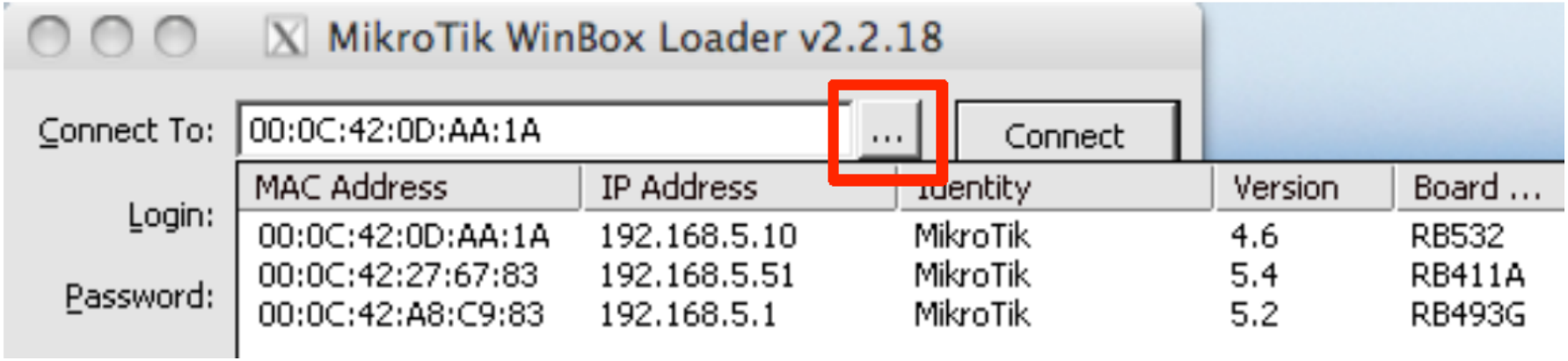
Laptop Config

- Konfigurasi IP Address statik pada laptop.



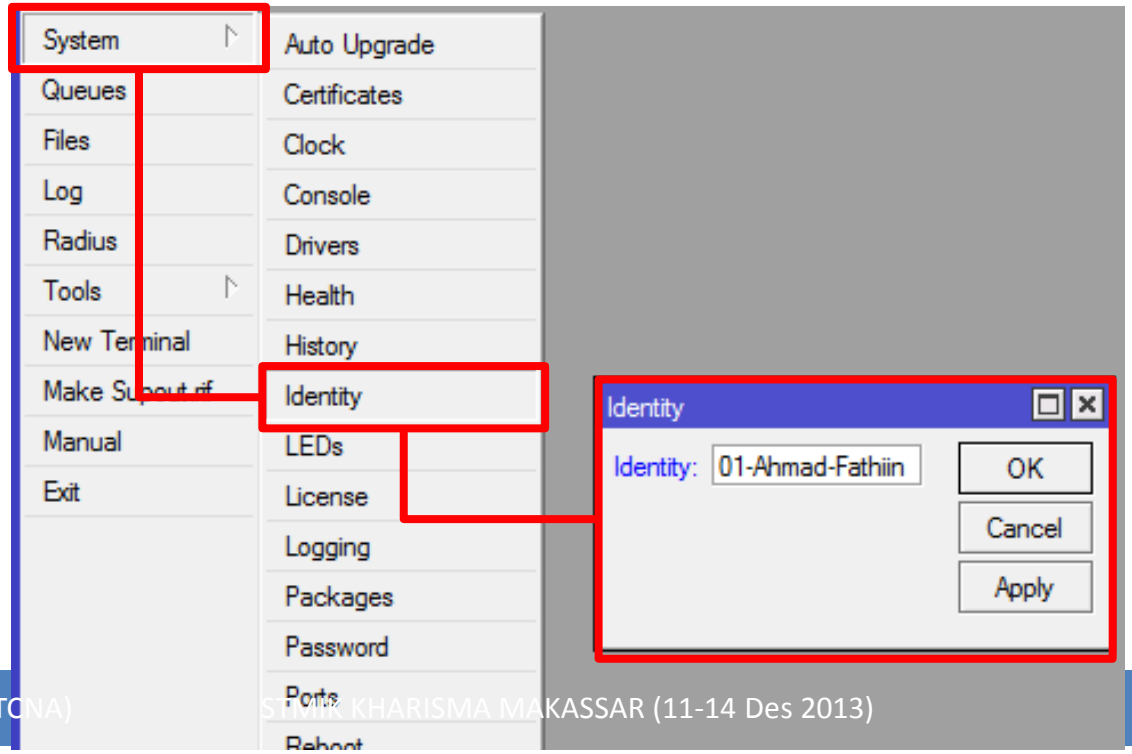
First Setup

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

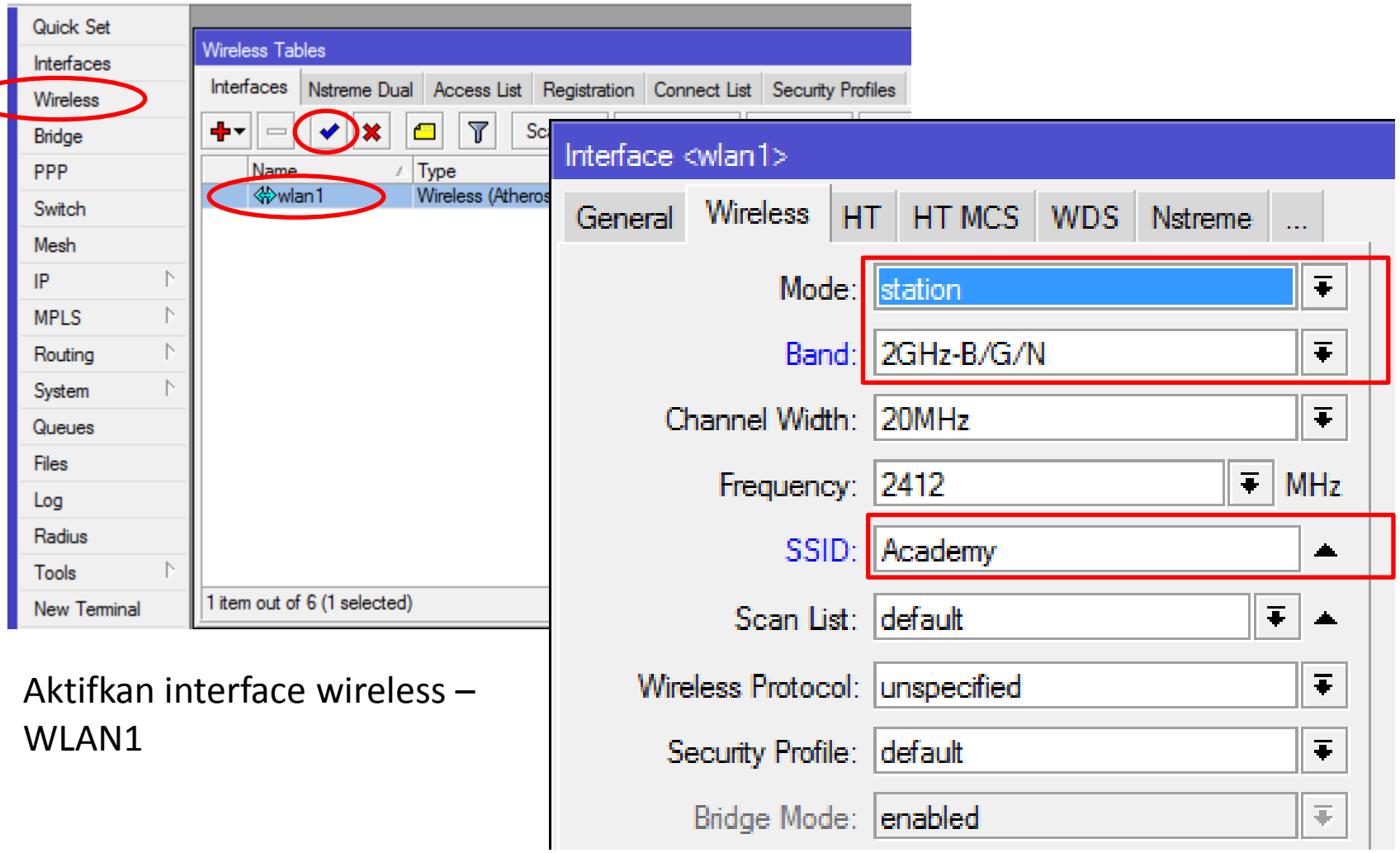


[LAB-1] System Identity

- Supaya tidak membingungkan, ubahlah nama router Anda.
- Format: **xx-NamaAnda**
- Contoh: 01-Ahmad-Fathiin
- Aktifkan semua interface

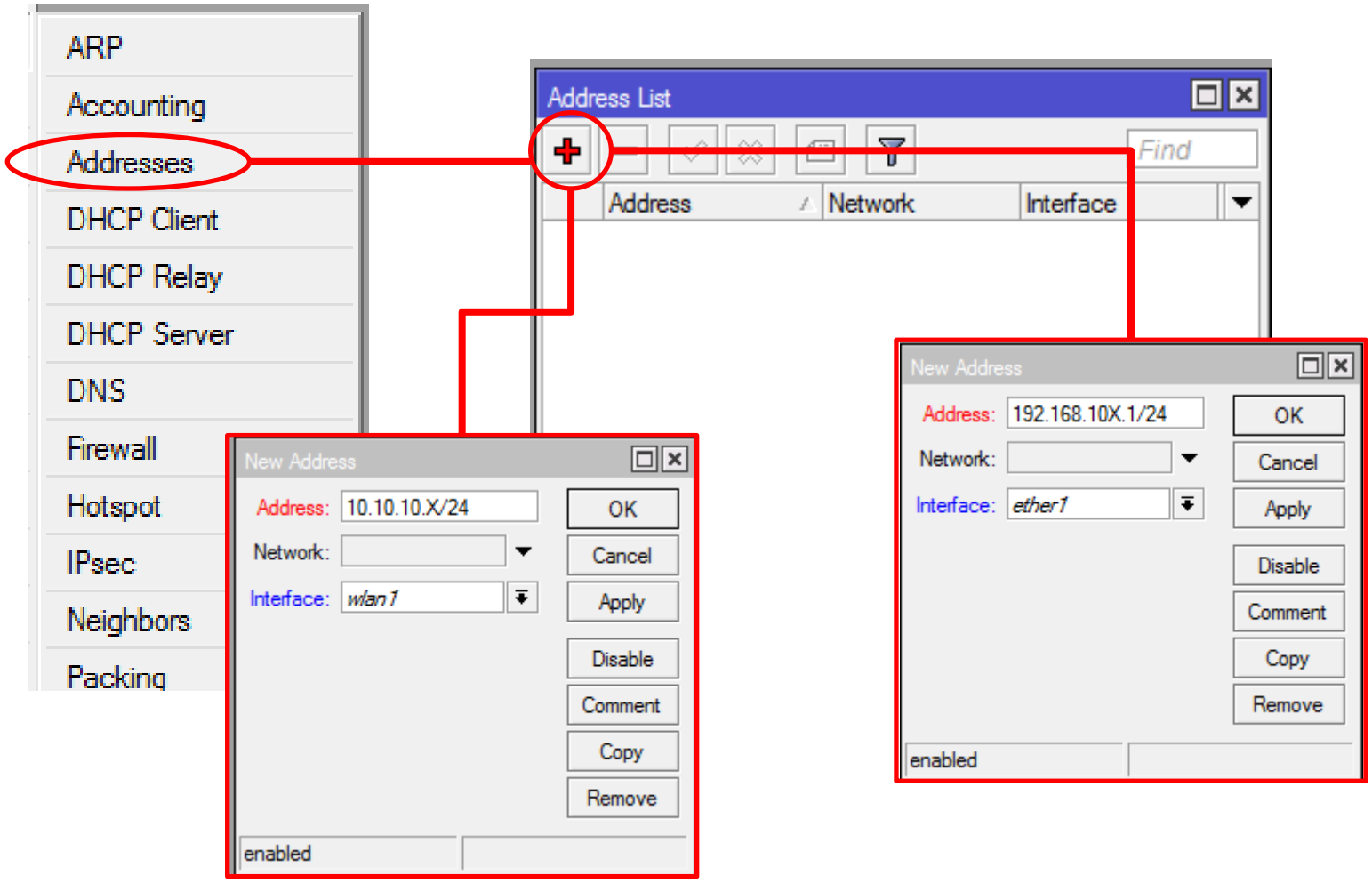


[LAB-2] Wireless Config

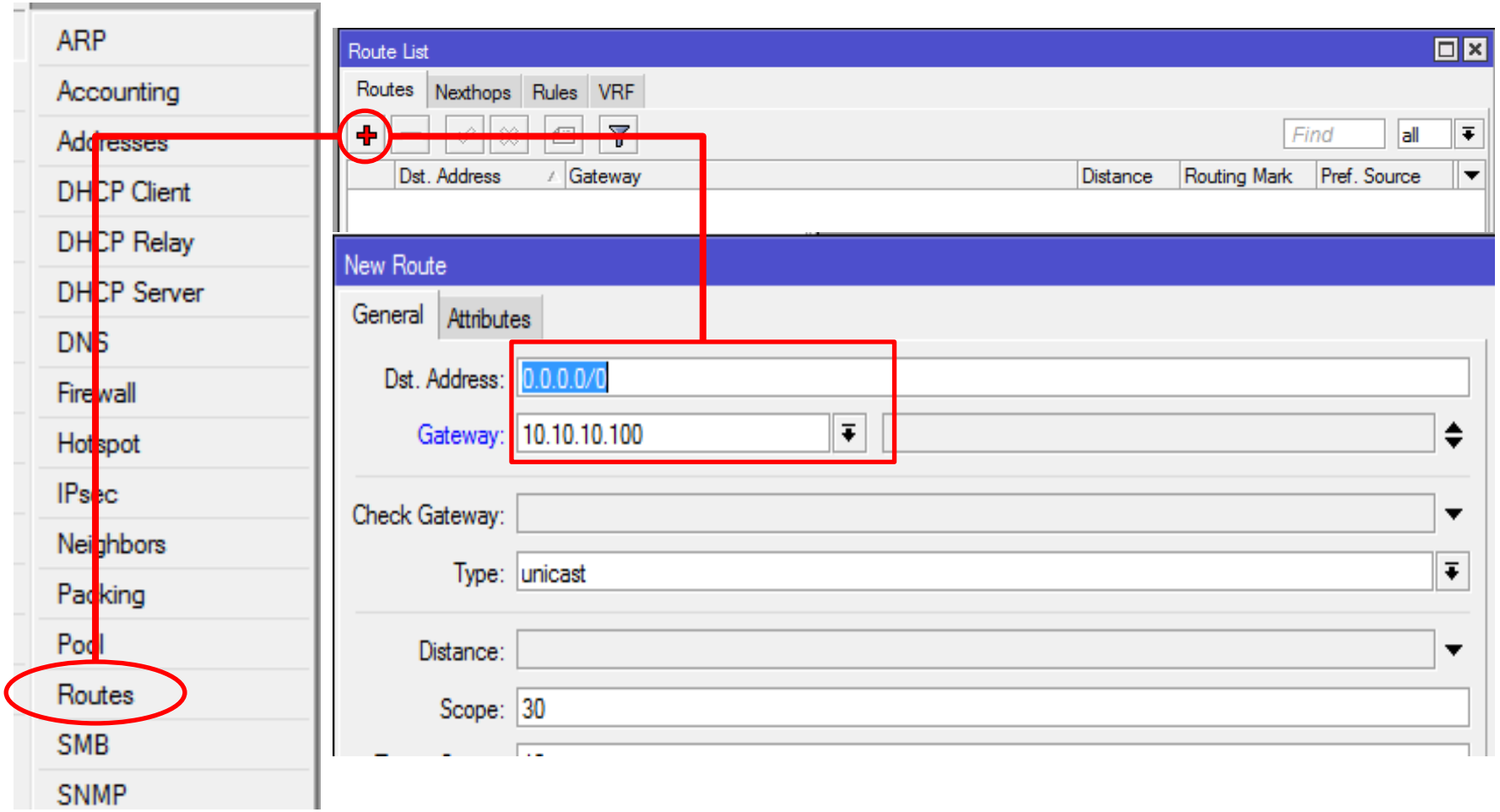


Aktifkan interface wireless – WLAN1

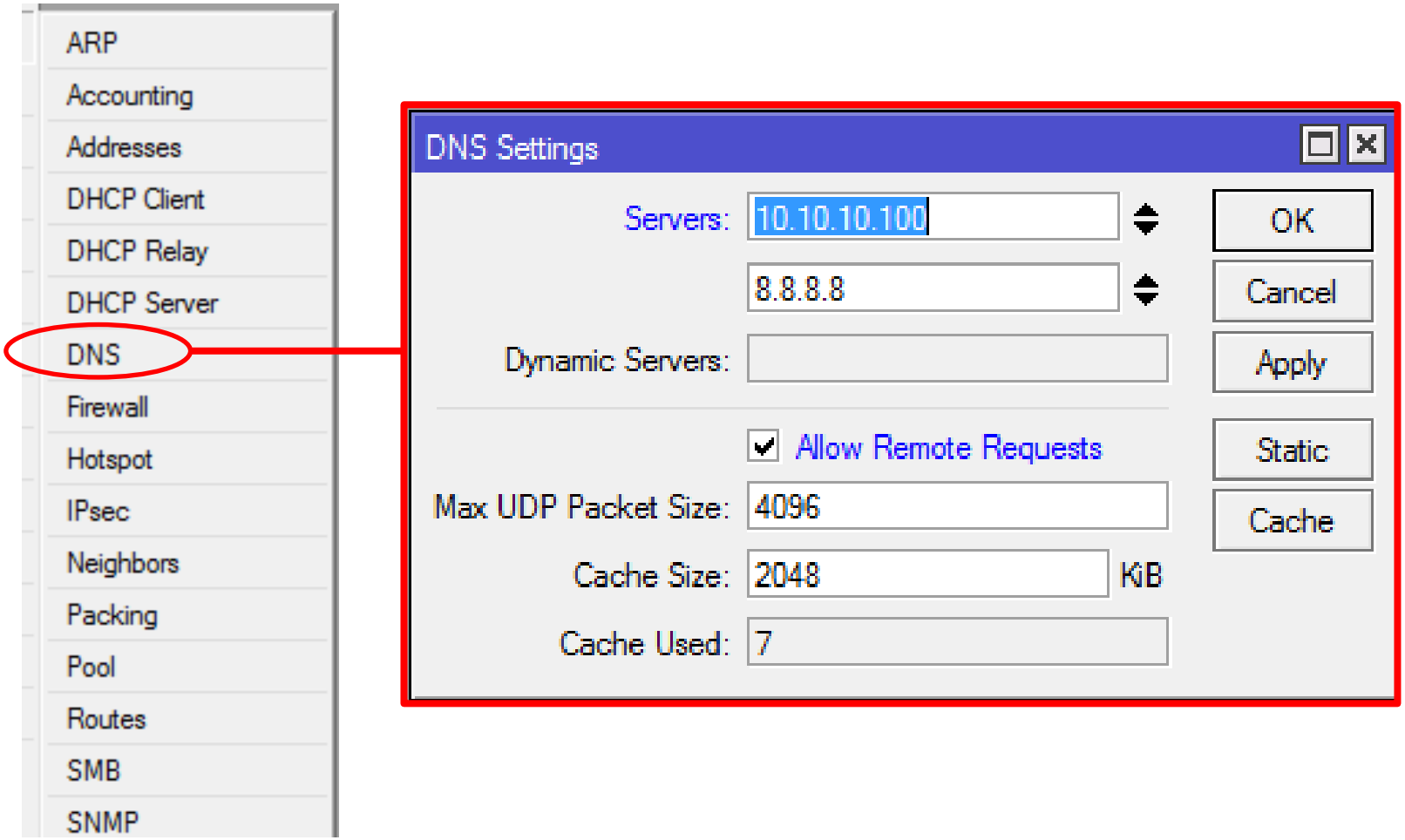
[LAB-3] IP Address Config



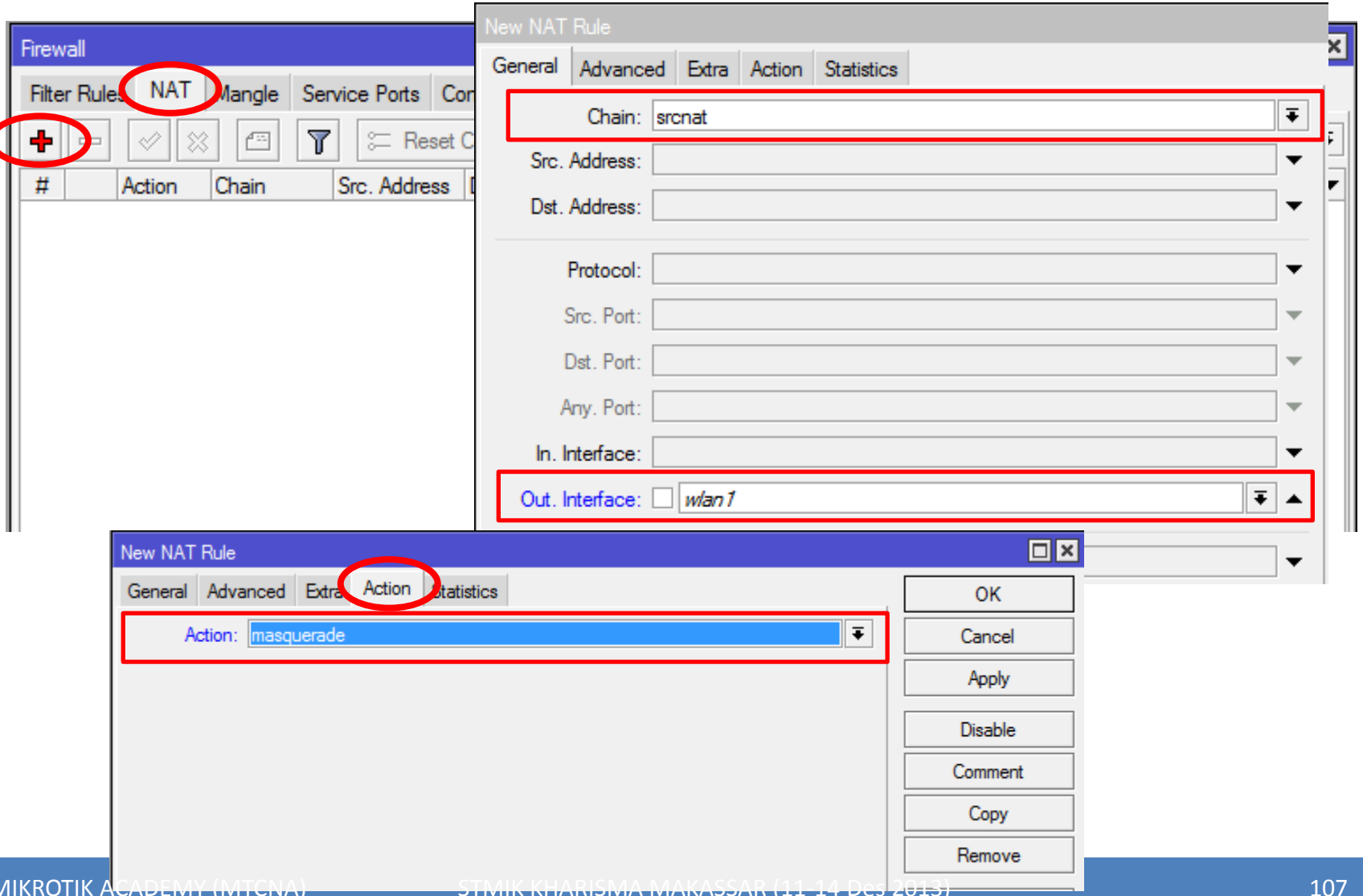
[LAB-4] Gateway Config



[LAB-5] DNS Config



[LAB-6] Src-NAT Config



Terminal / Console Config

- Konfigurasi wireless sebagai media untuk backbone
  - interface wireless set wlan1 mode=station ssid=training band=2.4.ghz-b/g/n 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 servers=10.10.10.100 allow-remote-request=yes
- Konfigurasi NAT
  - /ip firewall nat add chain=srcnat out-interface=wlan1 action=masquerade

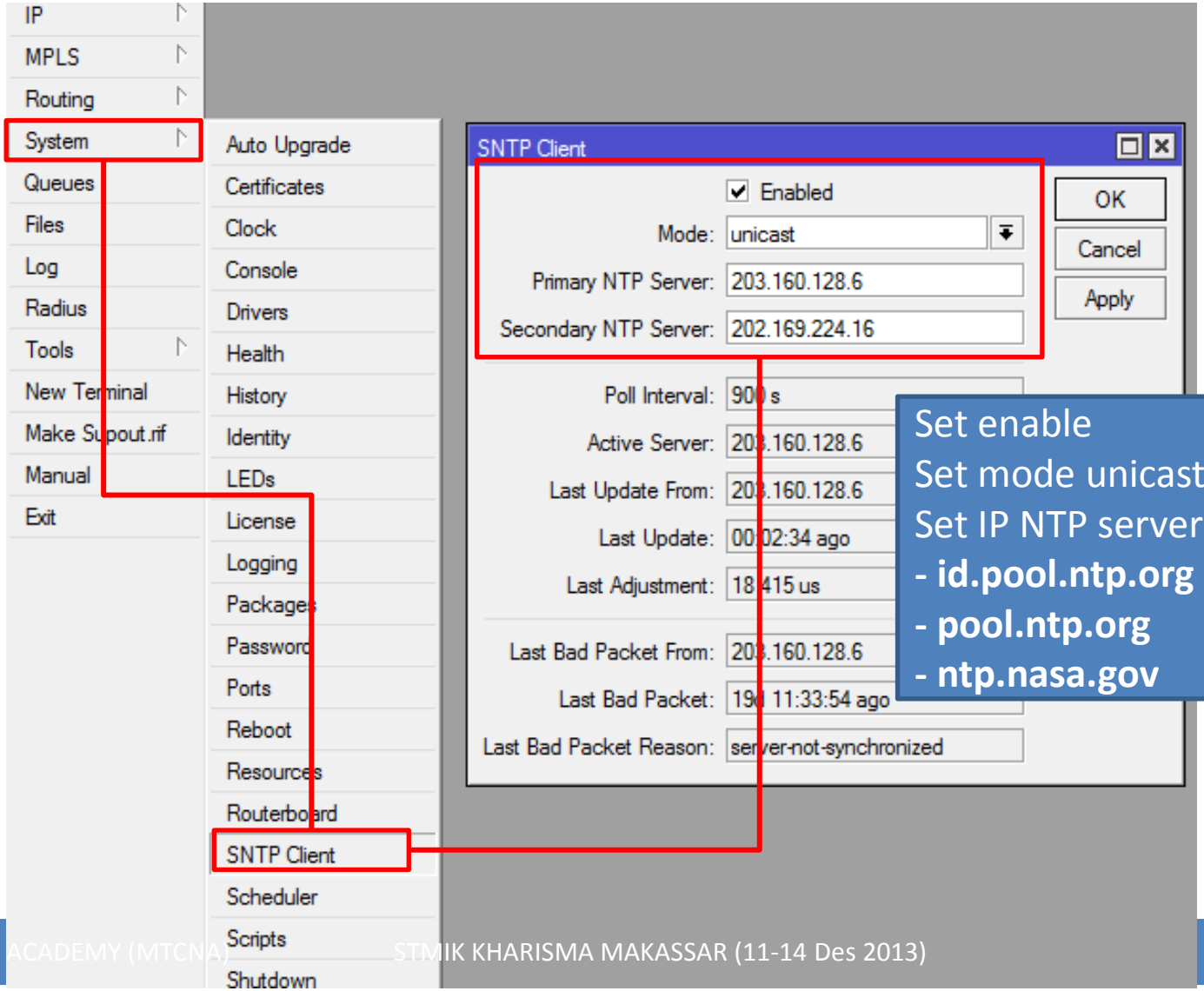
Installation Debug

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

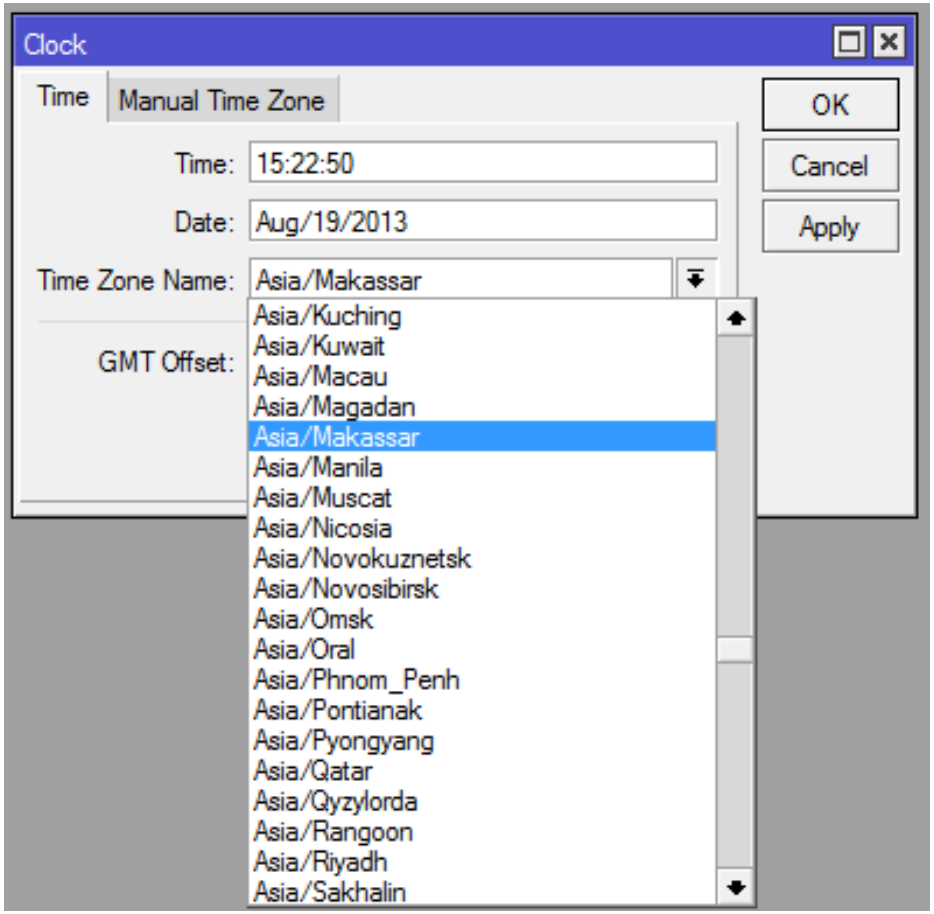
Network Time Protocol (NTP)

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

[LAB-7] NTP


IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
Make Supout.rif
Manual
Exit
Auto Upgrade
Certificates
Clock
Console
Drivers
Health
History
Identity
LEDs
License
Logging
Packages
Password
Ports
Reboot
Resources
Routerboard
SNTP Client
Scheduler
Scripts
Shutdown
SNTP Client
Enabled
Mode: unicast
Primary NTP Server: 203.160.128.6
Secondary NTP Server: 202.169.224.16
OK
Cancel
Apply
Poll Interval: 900 s
Active Server: 203.160.128.6
Last Update From: 203.160.128.6
Last Update: 00:02:34 ago
Last Adjustment: 18.415 us
Last Bad Packet From: 203.160.128.6
Last Bad Packet: 19d 11:33:54 ago
Last Bad Packet Reason: server-not-synchronized
Set enable
Set mode unicast
Set IP NTP server
- id.pool.ntp.org
- pool.ntp.org
- ntp.nasa.gov

System - Clock



Sesuikan time zone lokasi

Backup from CLI

- 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
- File backup tidak dapat di-edit !

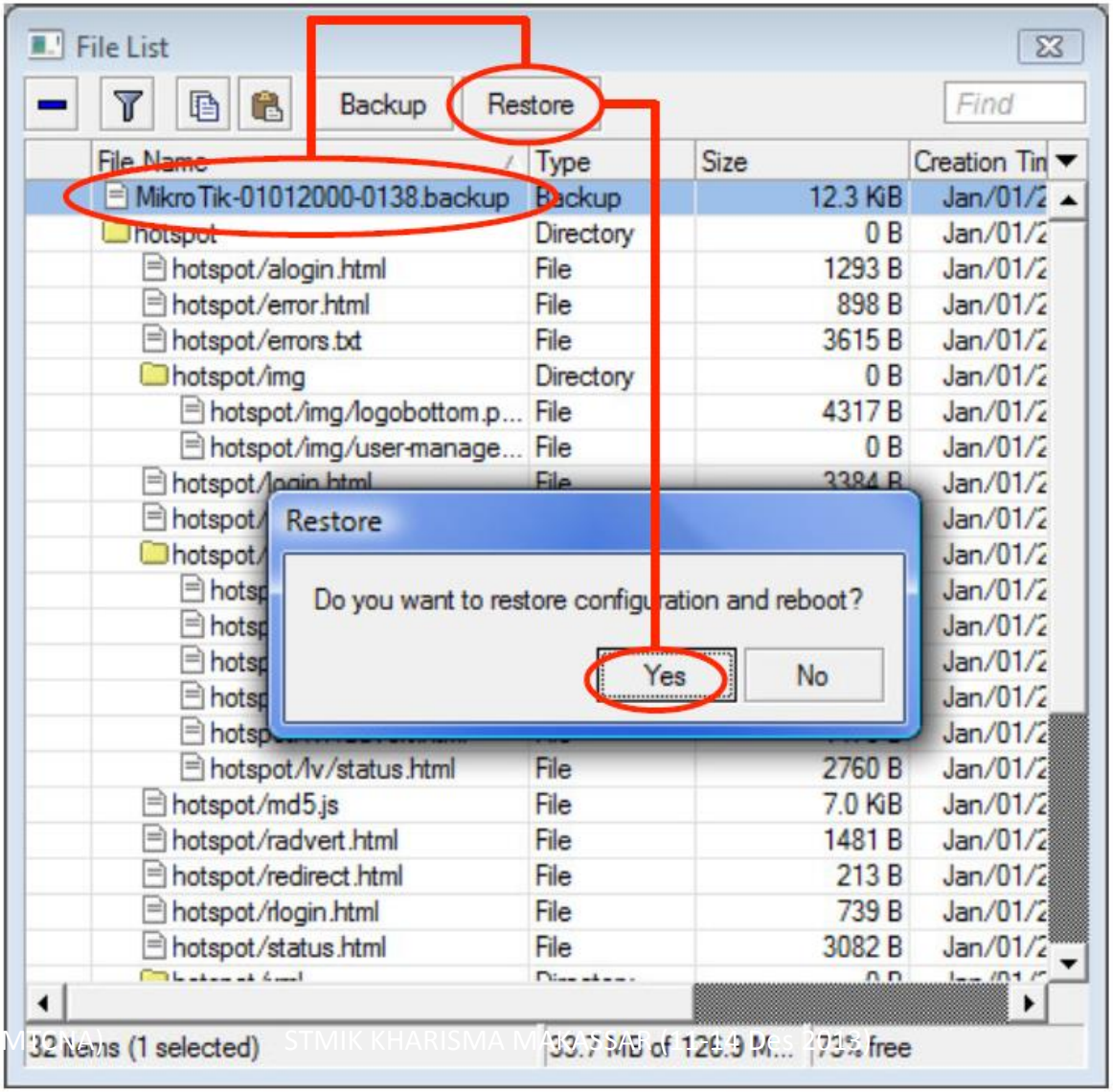
System Reset

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

[admin@Router-MikroTik] > system reset

Dangerous! Reset anyway? [y/N]: y

[LAB-9] Restore Configuration



Backup – Export Configuration

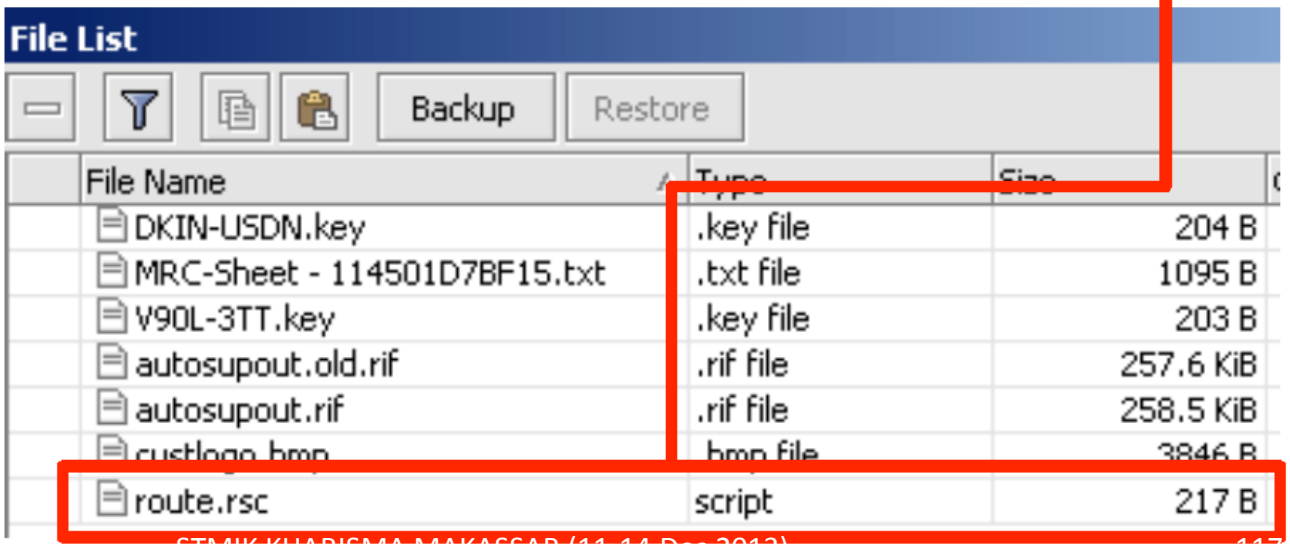
- Backup bisa dilakukan juga menggunakan perintah export.

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

Backup – Export to File

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

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



Restore – Import Script

- File script bisa langsung di restore ke router

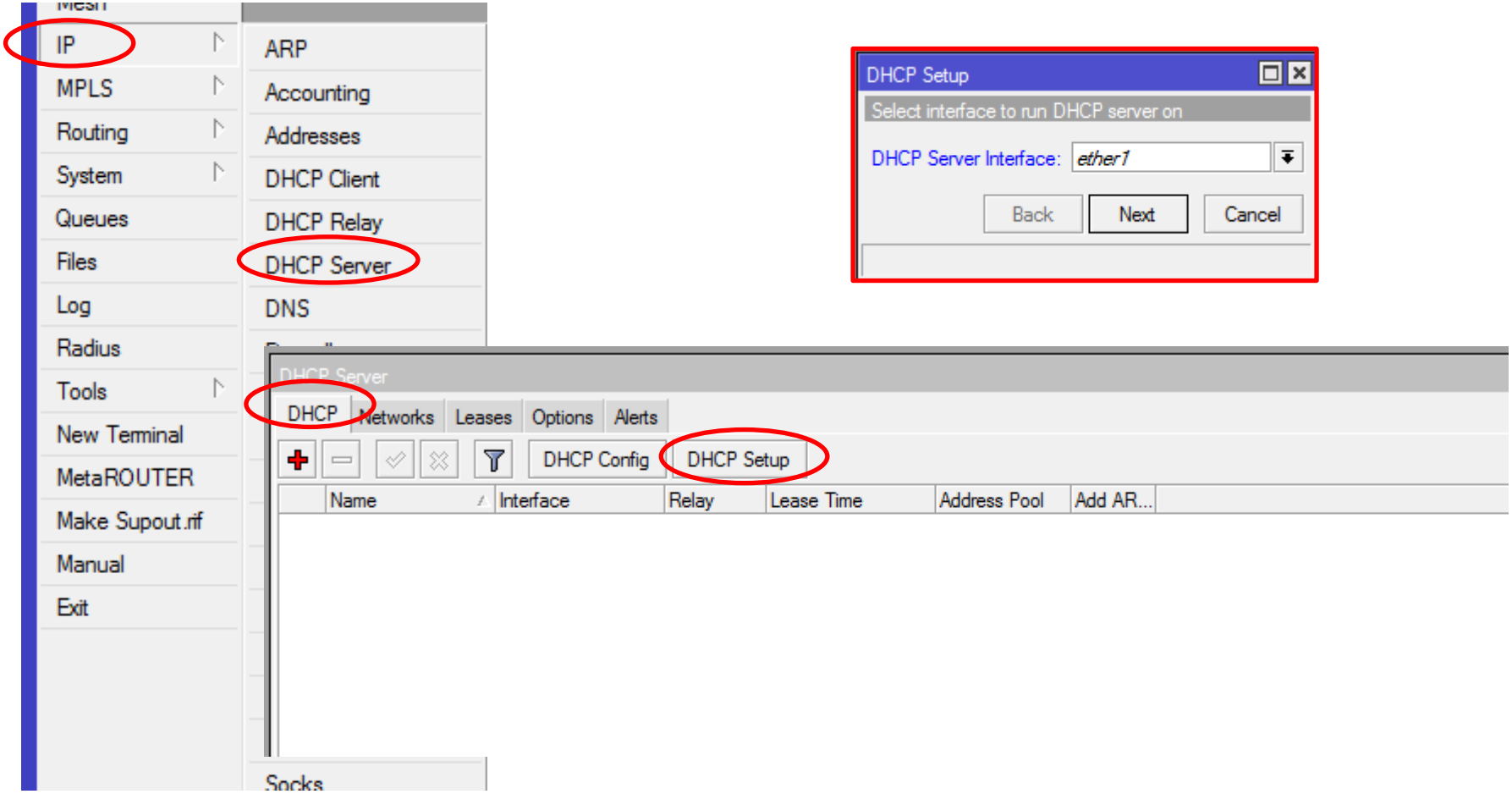
```
MMM       MMM        KKK                                TTTTTTTTTTT      KKK
MMMM     MMMM        KKK                                TTTTTTTTTTT      KKK
MMM MMMM MMM   III   KKK  KKK  RRRRRR     000000      TTT     III  KKK  KKK
MMM  MM  MMM   III   KKKKK     RRR  RRR  000  000     TTT     III 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

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

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

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

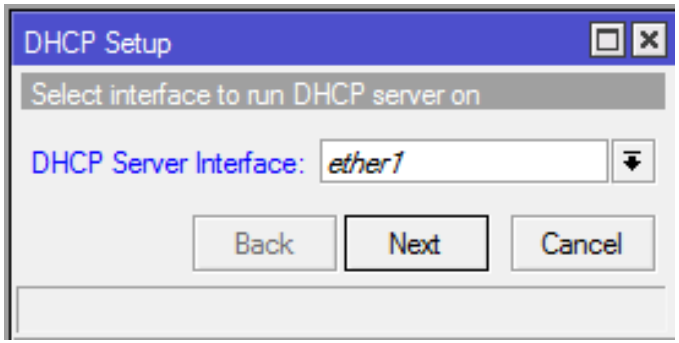
DHCP Server

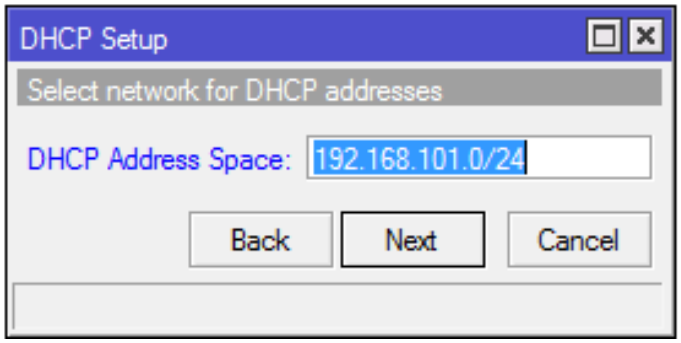
- Dynamic Host Configuration Protocol digunakan untuk secara dinamik mendistribusikan konfigurasi jaringan, seperti:
  - IP Address dan netmask
  - IP Address default gateway
  - Konfigurasi DNS dan NTP Server
  - Dan masih banyak lagi custom option (tergantungapakah DHCP client bisa support)

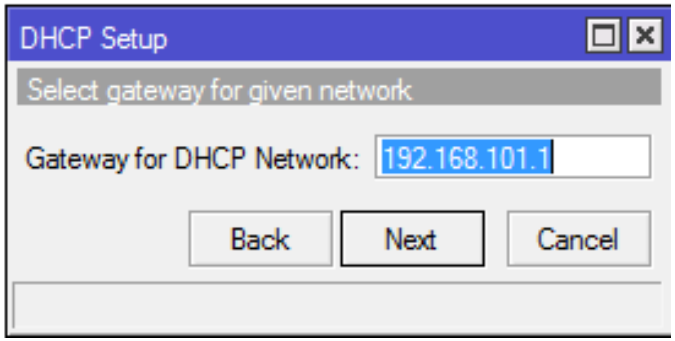
[LAB-10] DHCP Server (1)

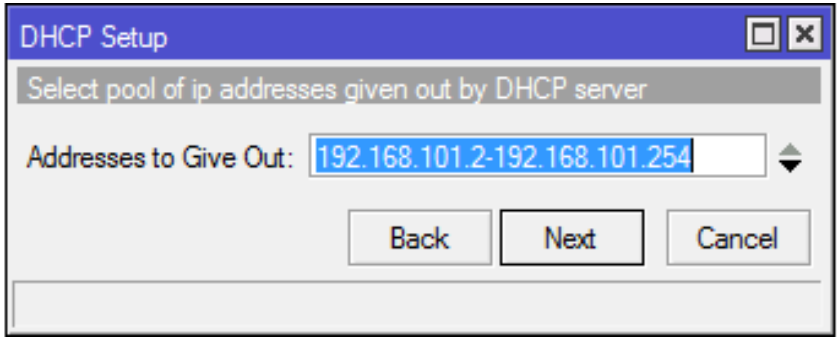


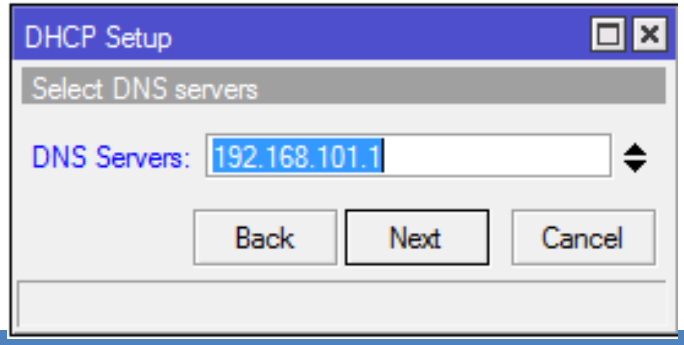
[LAB-10] DHCP Server (2)

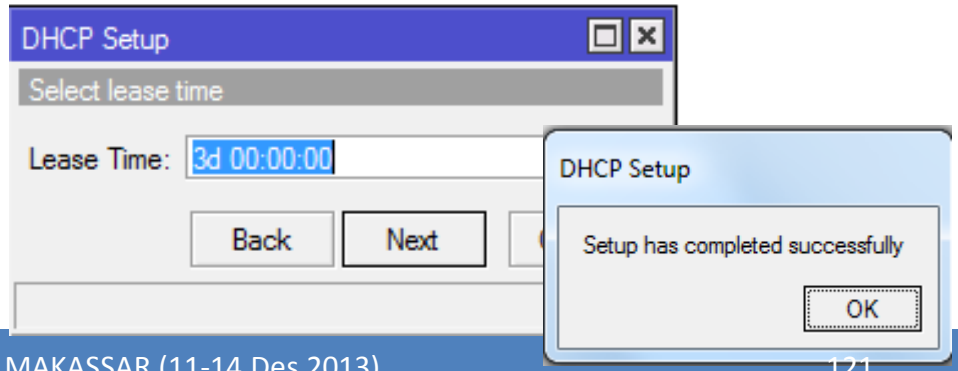












Terminal – DHCP Server Wizard

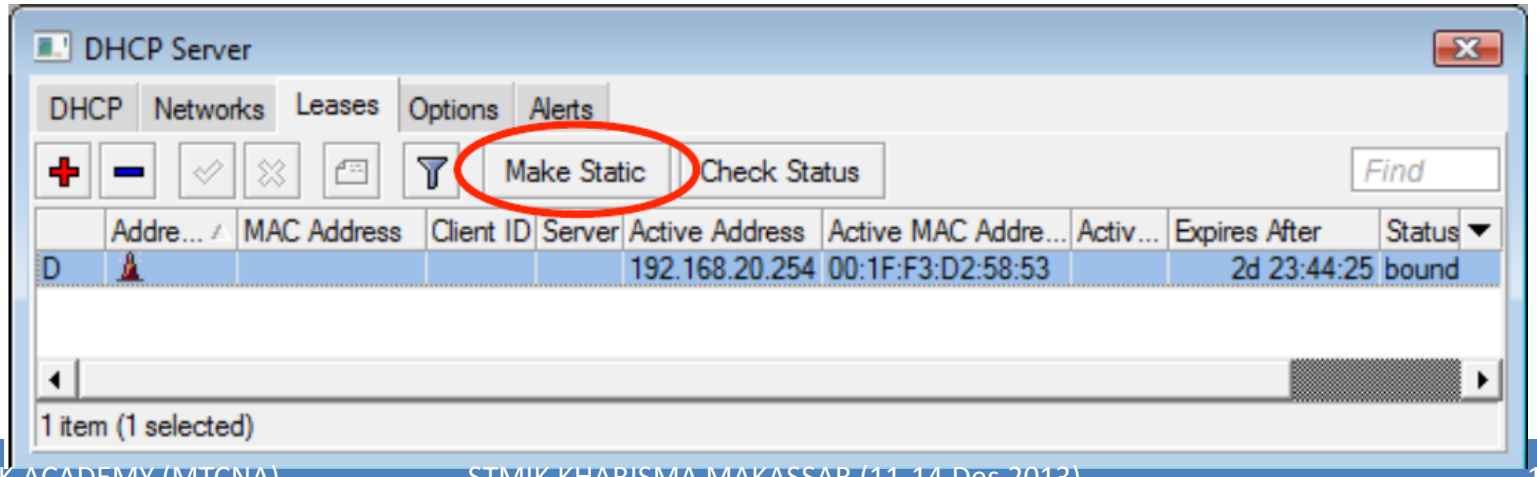
- Konfigurasi DHCP-Server setup
  - /ip dhcp-server setup
  - dhcp server interface: ether1
  - dhcp address space: 192.168.10**X**.0/24
  - gateway for dhcp network: 192.168.10**X**.1
  - dhcp relay: 192.168.10**X**.1
  - addresses to give out: 192.168.10**X**.10-192.168.10**X**.20
  - dns servers: 192.168.10**X**.1
  - lease time: 3d

DHCP Test

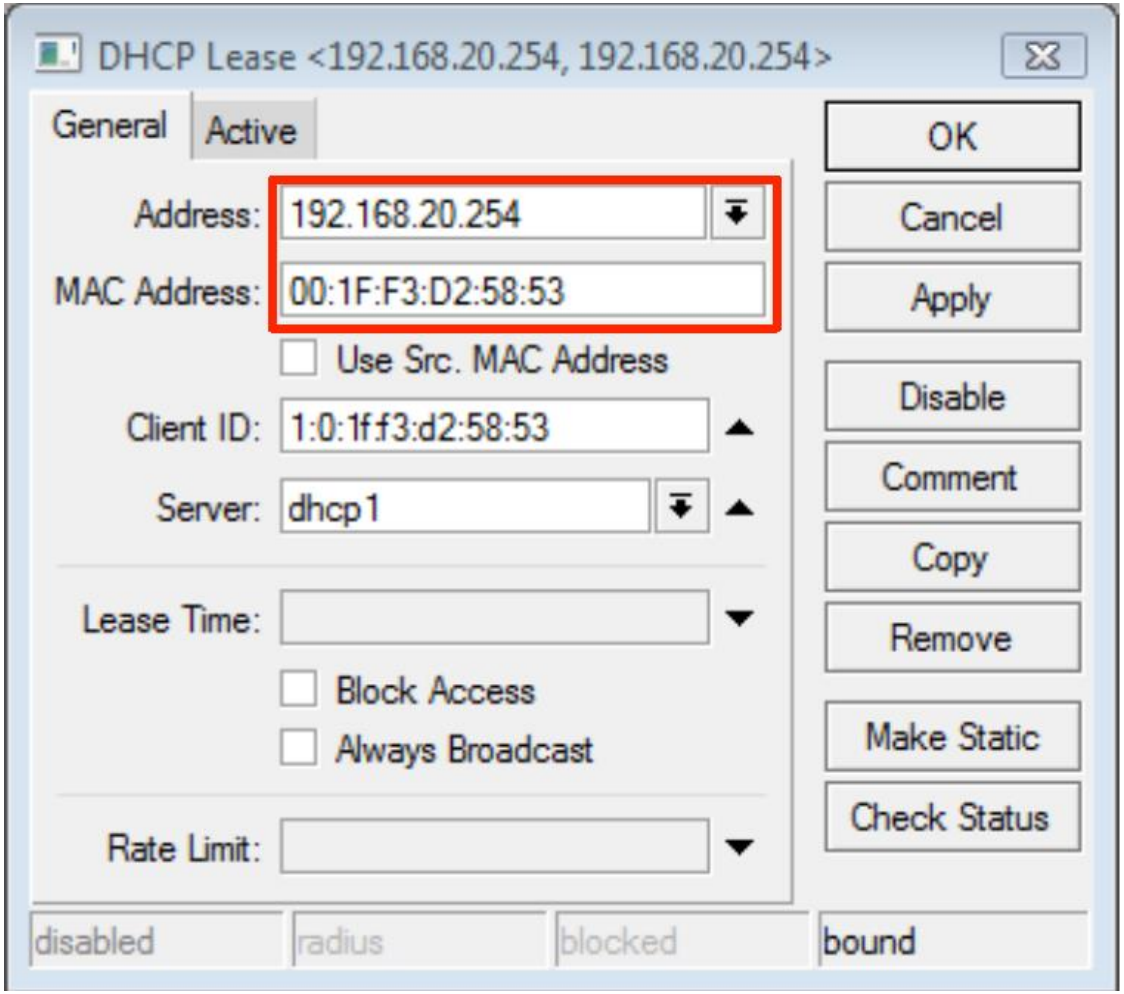
- Ubahlah konfigurasi IP Address dan DNS pada laptop menjadi otomatis
- Cek pada laptop apakah sudah mendapatkan alokasi IP Address dari DHCP
  - **C:\ ipconfig [enter]**
- Cobalah melakukan koneksi internet

DHCP Management

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



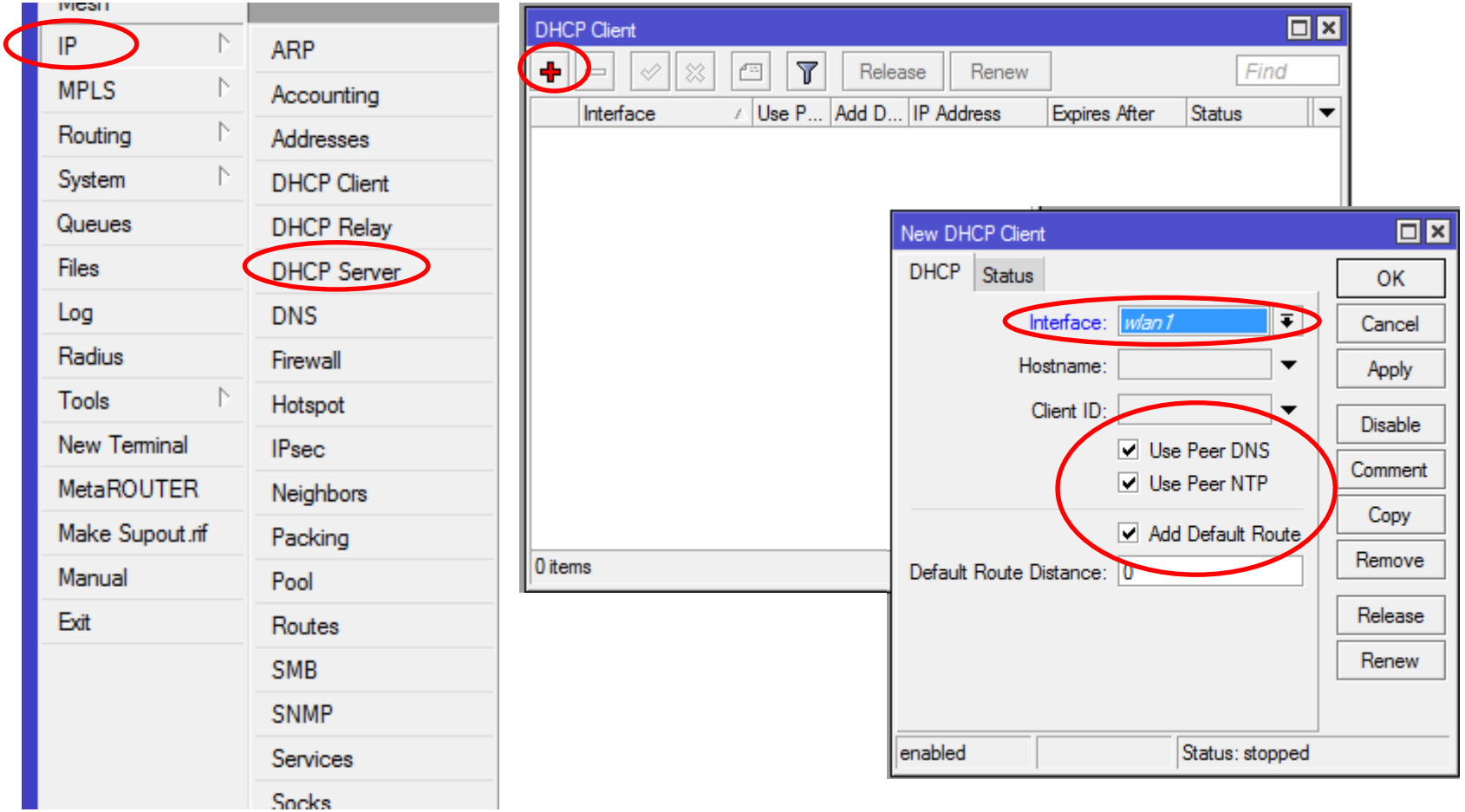
DHCP Static


DHCP Lease <192.168.20.254, 192.168.20.254>
General
Active
Address: 192.168.20.254
MAC Address: 00:1F:F3:D2:58:53
Use Src. MAC Address
Client ID: 1:0:1f:f3:d2:58:53
Server: dhcp1
Lease Time:
Block Access
Always Broadcast
Rate Limit:
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Make Static
Check Status
disabled
radius
blocked
bound

DHCP Client

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

[LAB-11] DHCP Client



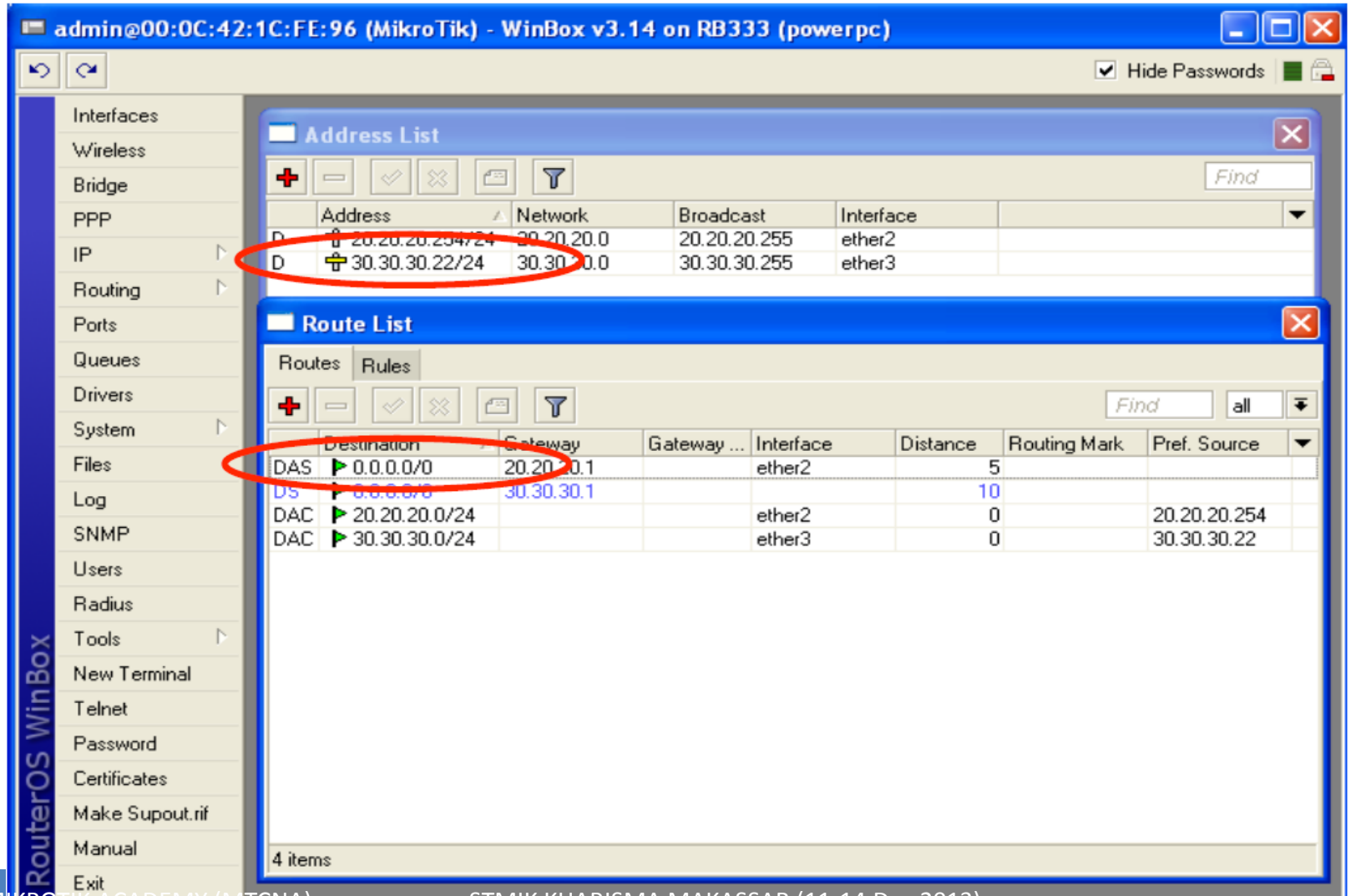
DHCP Client (1)

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

DHCP Client (2)

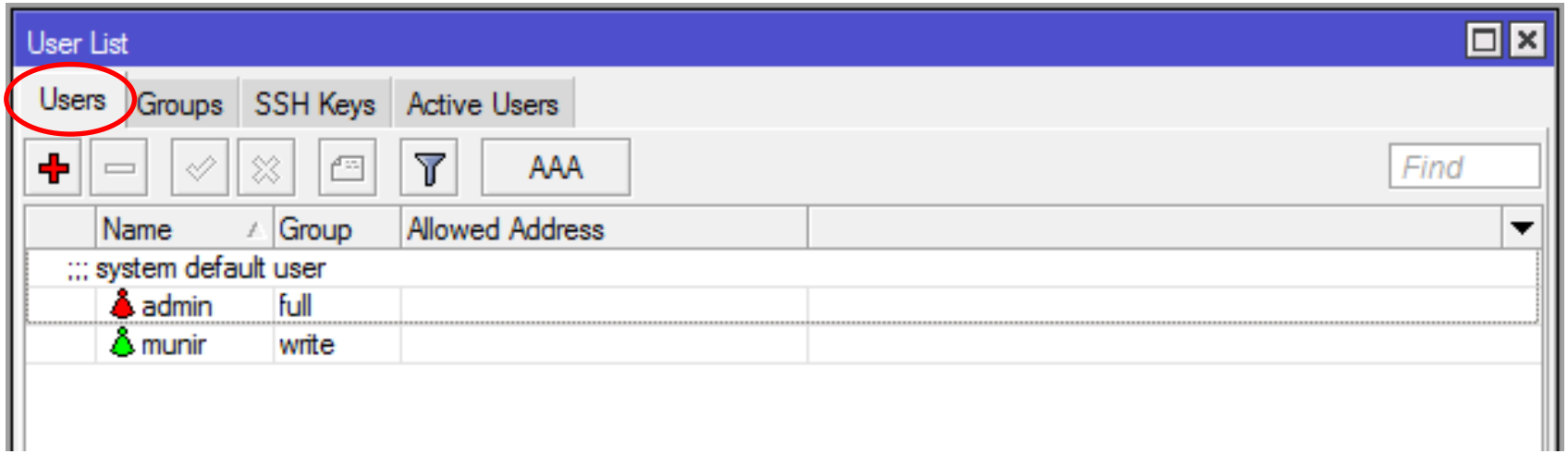
- **Add default route**
  - Bila kita menginginkan default route kita mengarah sesuai dengan informasi DHCP
- **Use Peer DNS**
  - Bila kita hendak menggunakan DNS server sesuai dengan informasi DHCP
- **Use Peer NTP**
  - Bila kita hendak menggunakan informasi pengaturan waktu di router (NTP) sesuai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

DHCP Client – Automatic Gateway



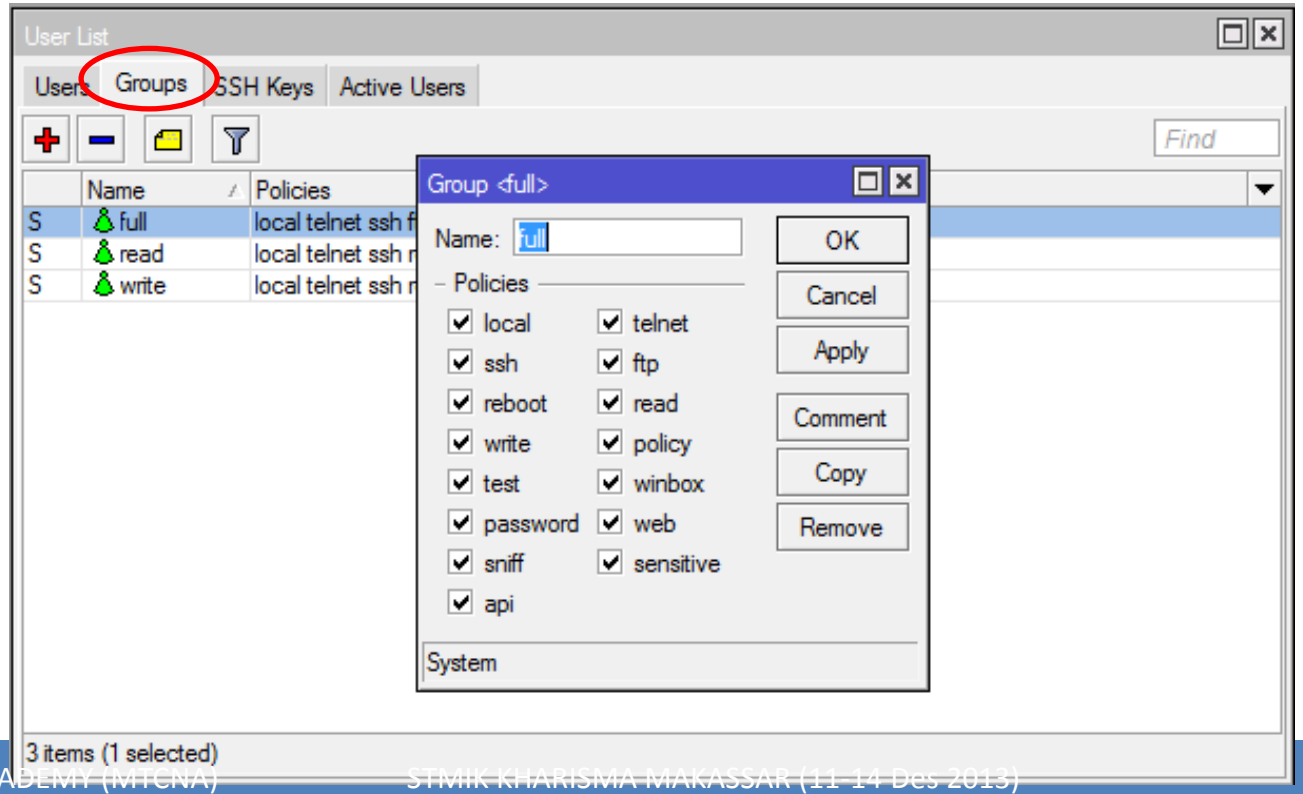
Manage RouterOS logins

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



Internal User Groups

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



About User

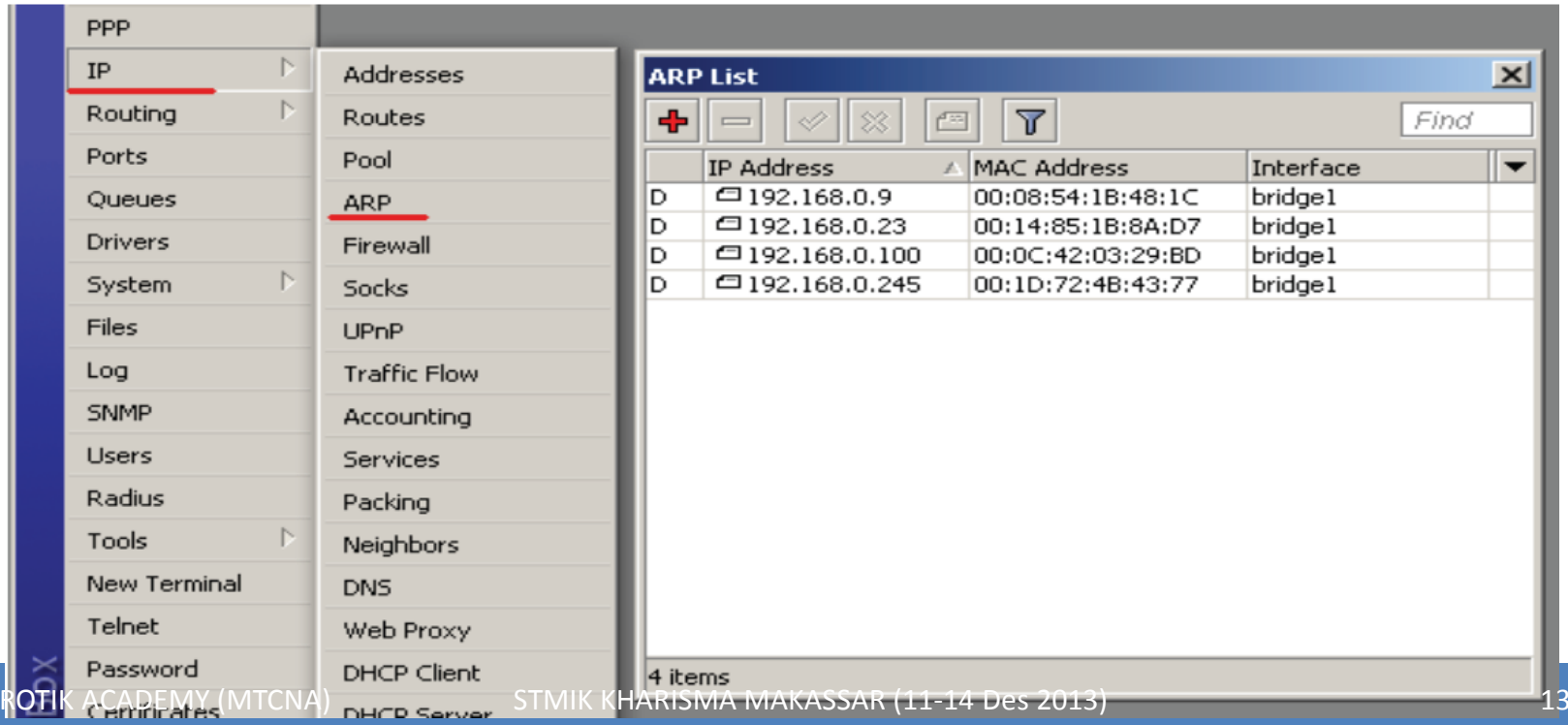
- Buatlah user baru yang memiliki hak penuh dan non aktifkan user "**admin**"
- Untuk teknisi bisa diberikan grup **write** (bukan **full**) sehingga kita masih memiliki hak penuh terhadap router kita
- Untuk pemantauan, bisa menggunakan user dengan grup **read**

[LAB-12] Internal User

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

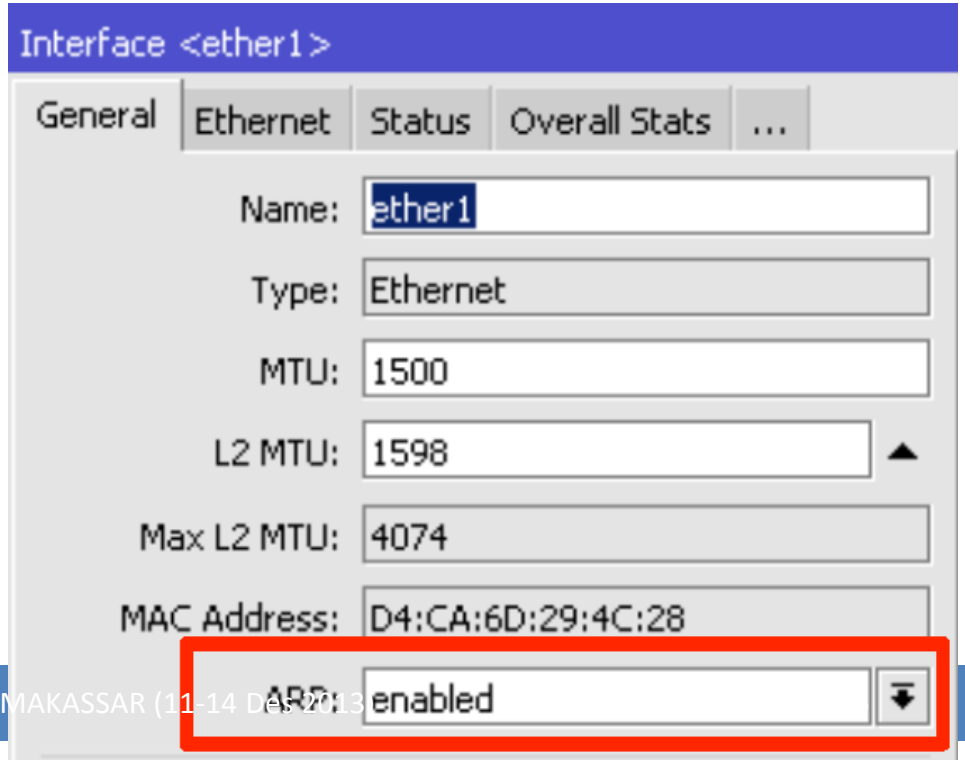
Address Resolution Protocol

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



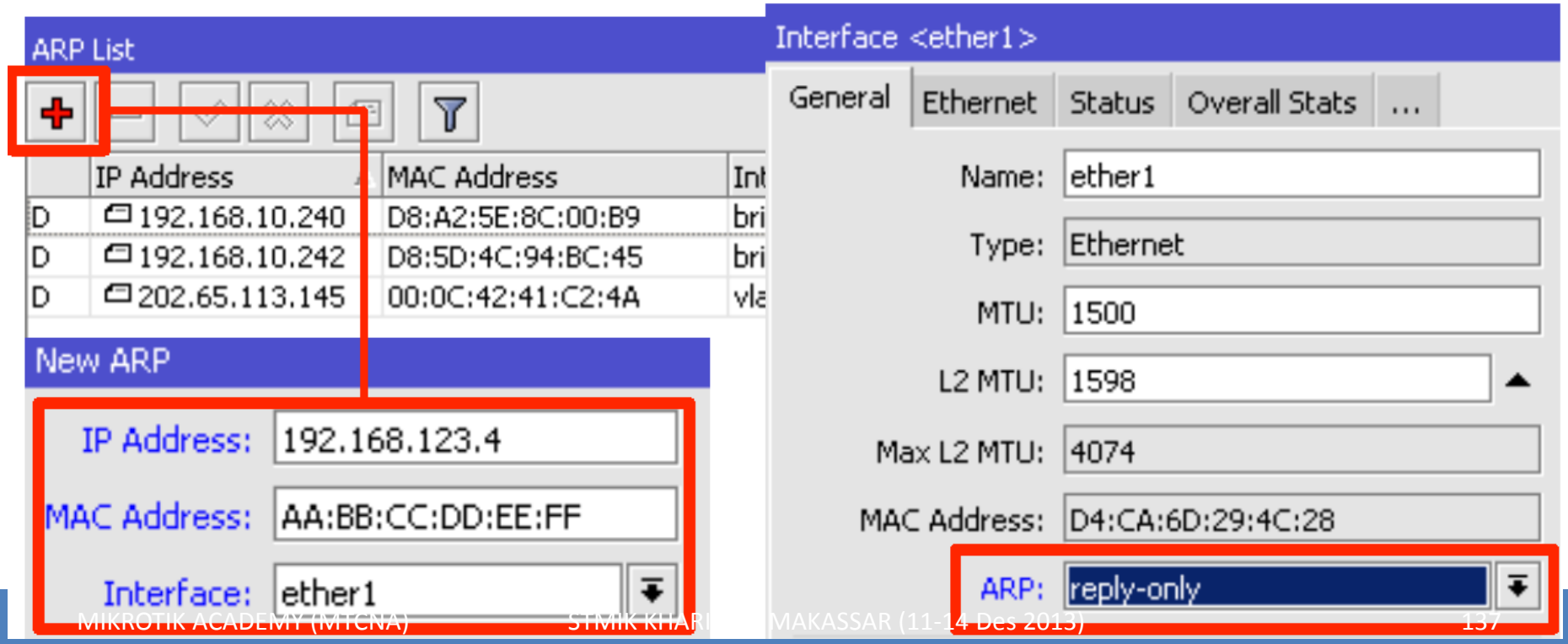
ARP Protocol

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



ARP – Security !

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

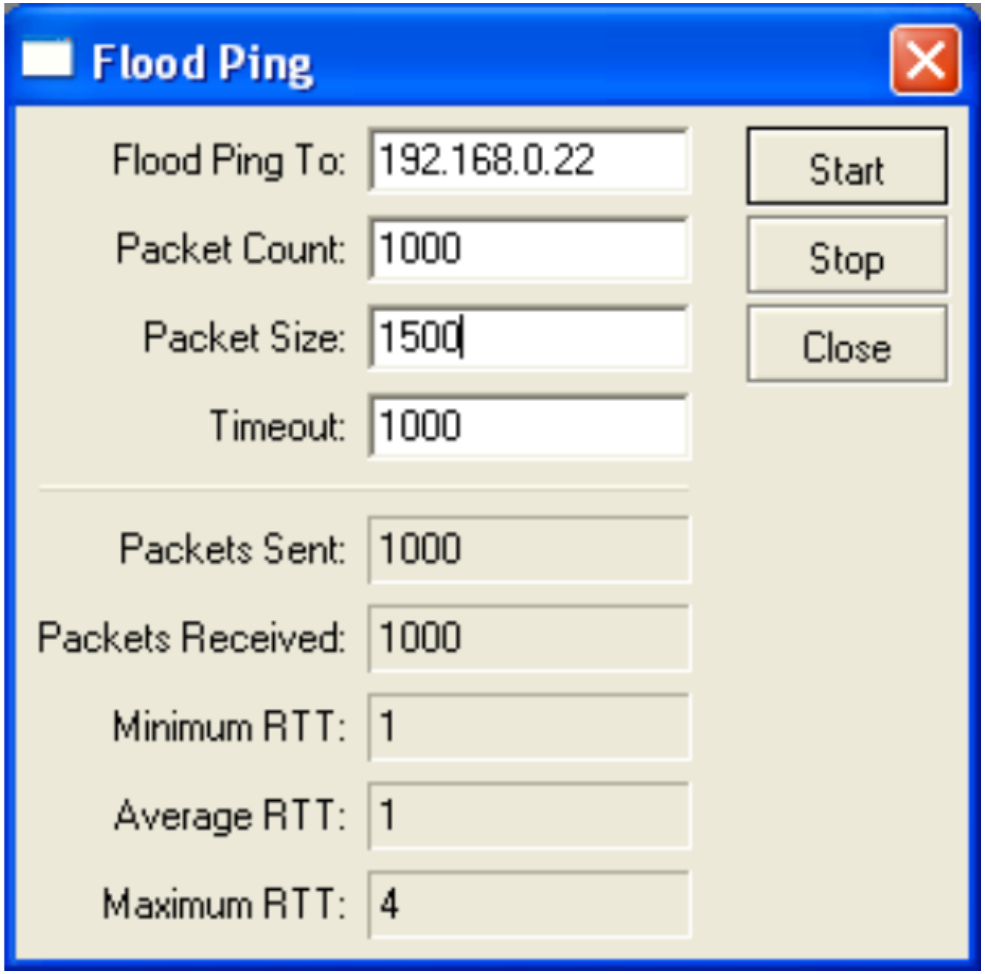


Monitoring - Ping

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

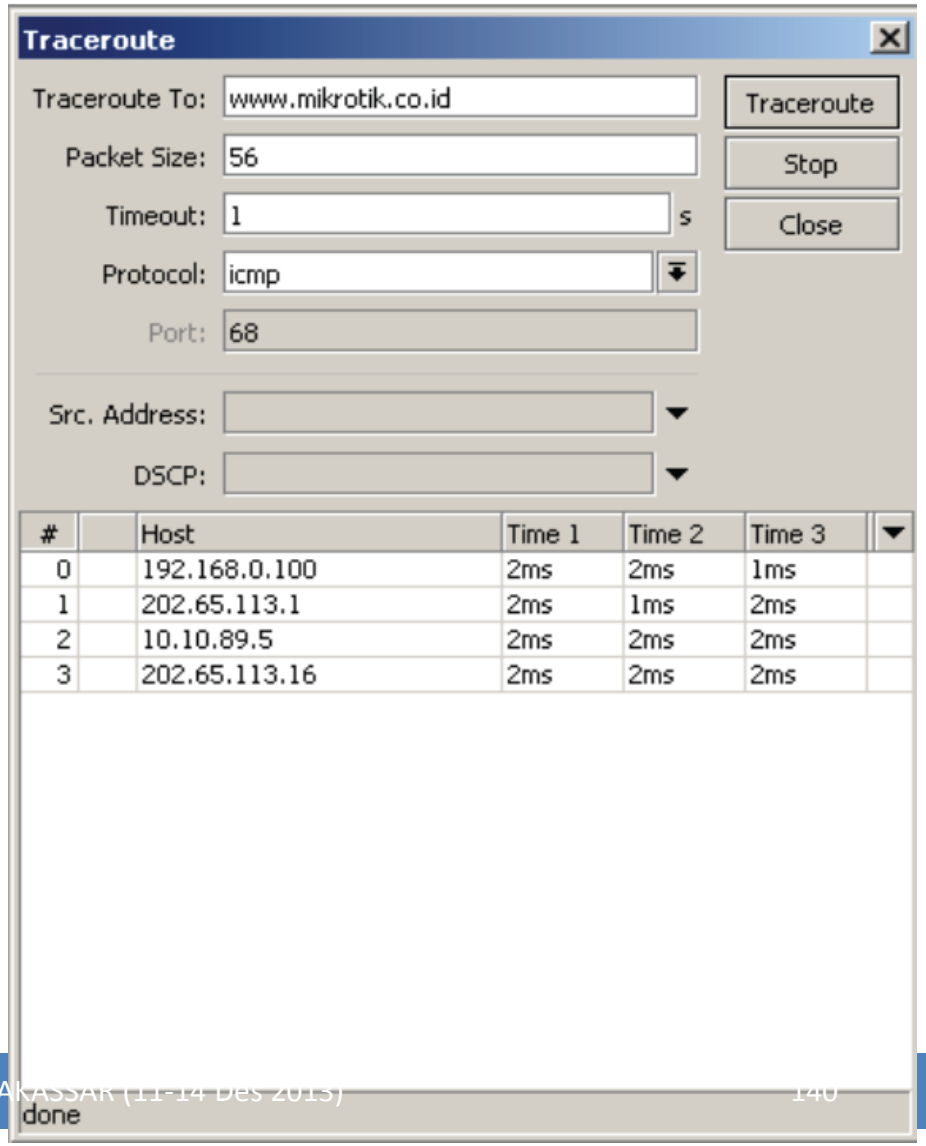
```
[user1@MKI] > ping 192.168.0.100
192.168.0.100 64 byte ping: ttl=64 time=1 ms
192.168.0.100 64 byte ping: ttl=64 time=1 ms
192.168.0.100 64 byte ping: ttl=64 time=1 ms
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1/1.0/1 ms
```

Monitoring – Ping Flood

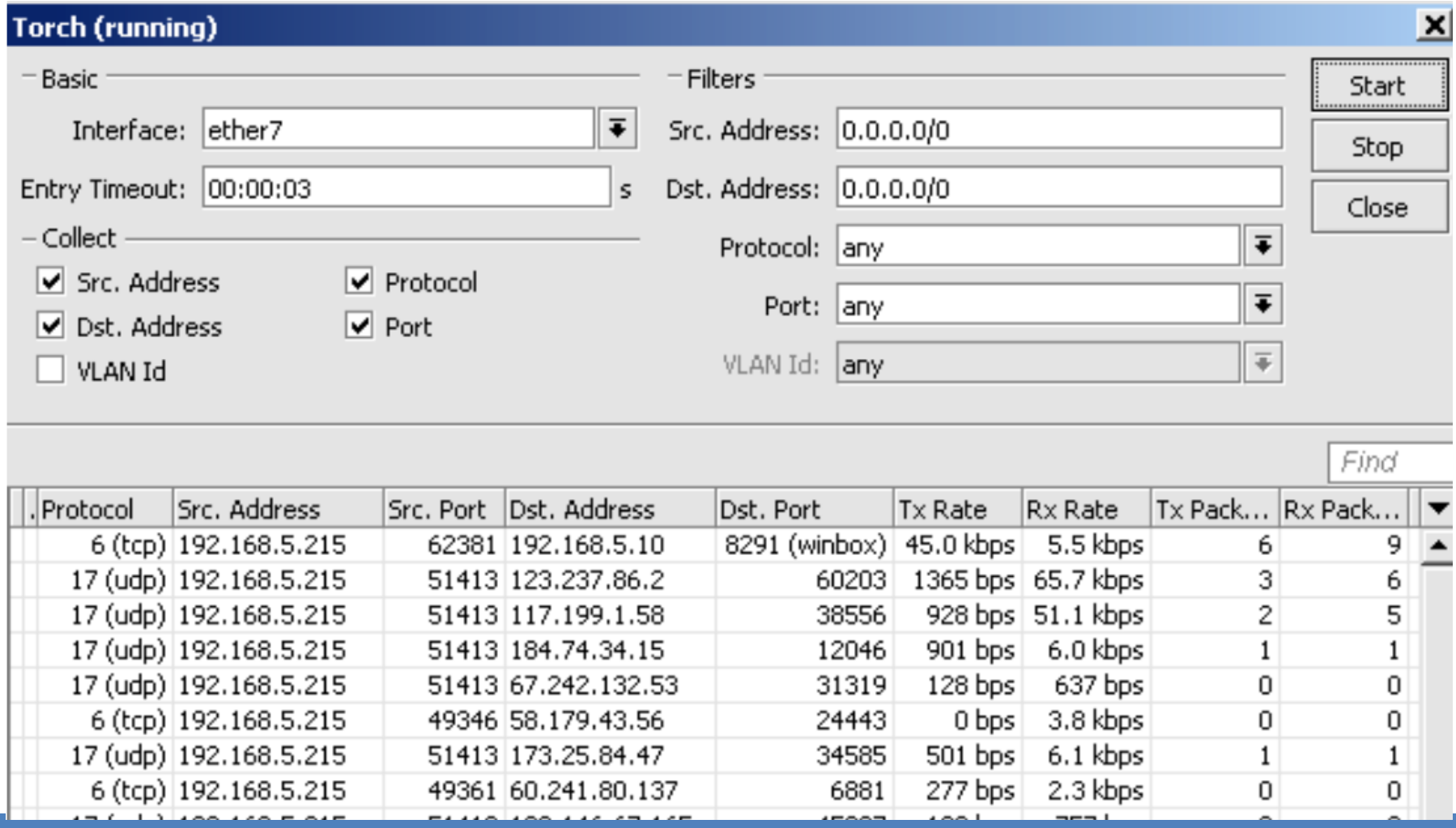


Monitoring - Traceroute

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

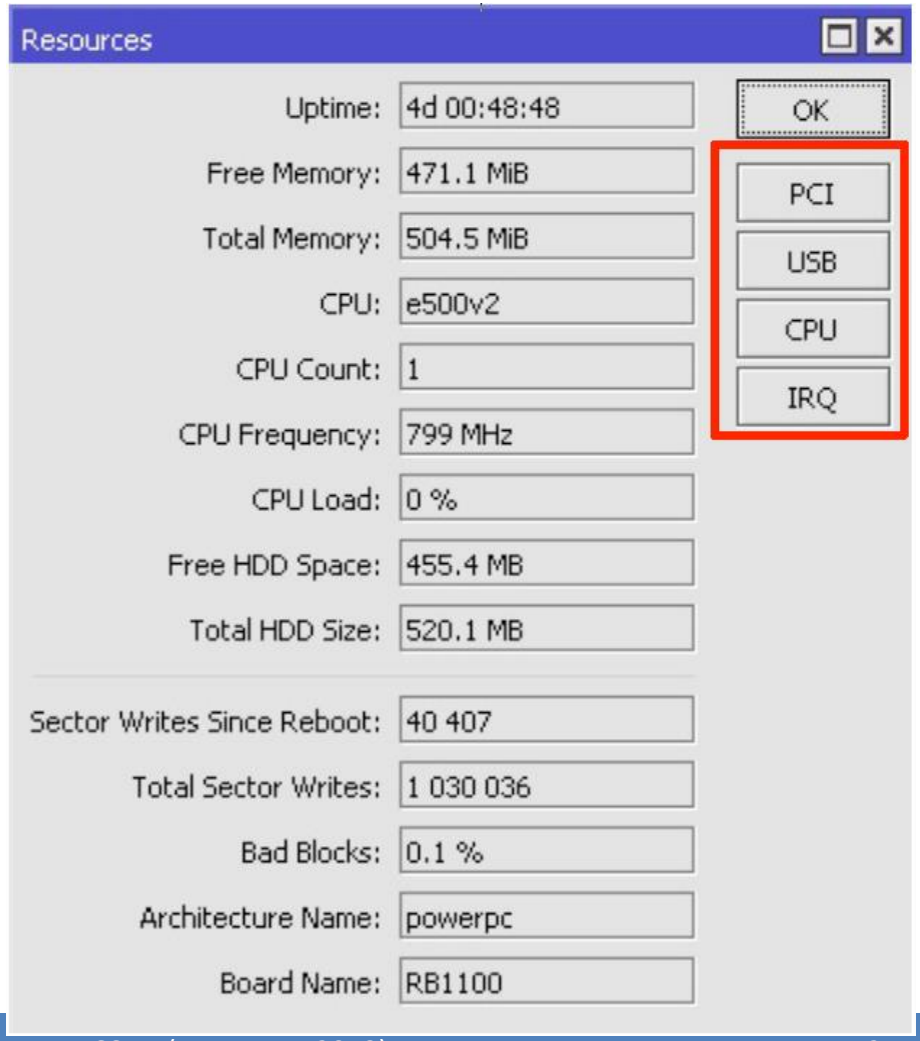


Monitoring - Torch



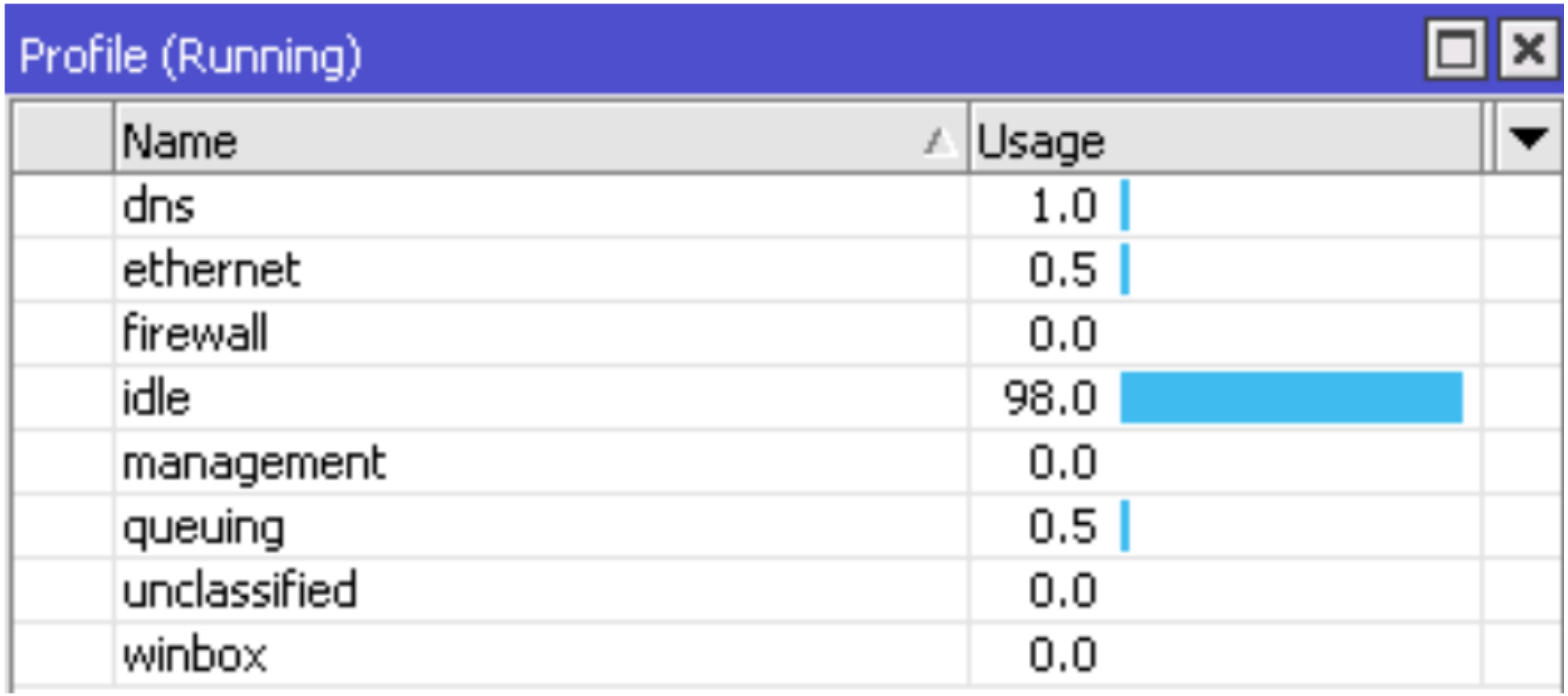
Monitoring - Resource

- Resource
  - To monitor the System.
  - Detail Resource monitor located onright side buttons



Monitoring – CPU Load

Tool – Profile untuk monitoring CPU Load



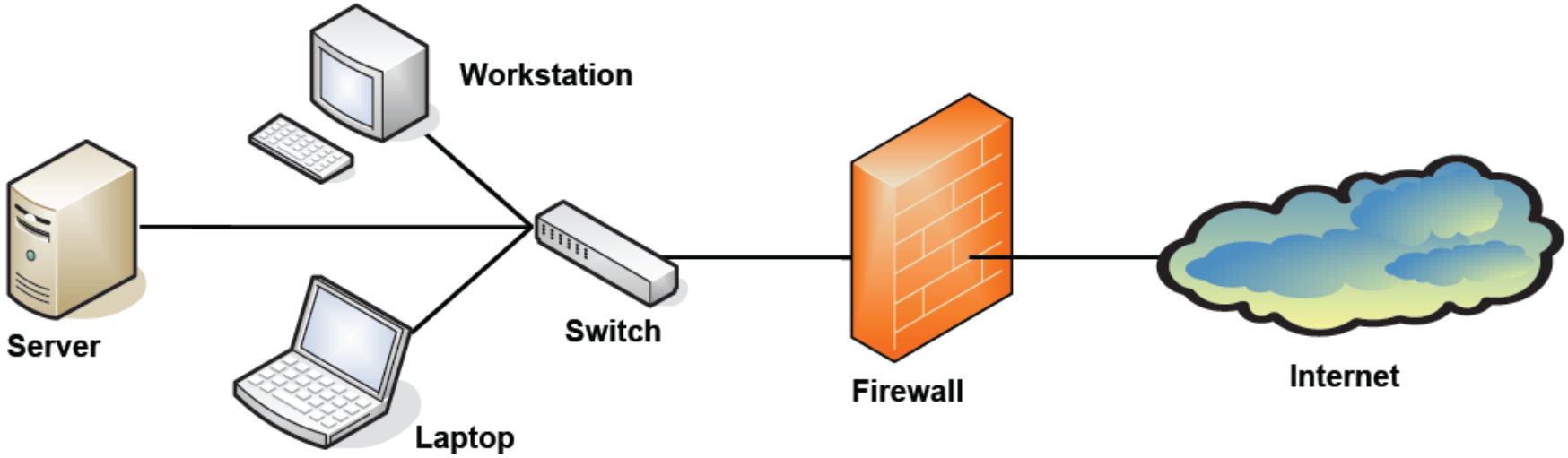
Module 2

MikroTik RouterOS

Firewall

Firewall

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



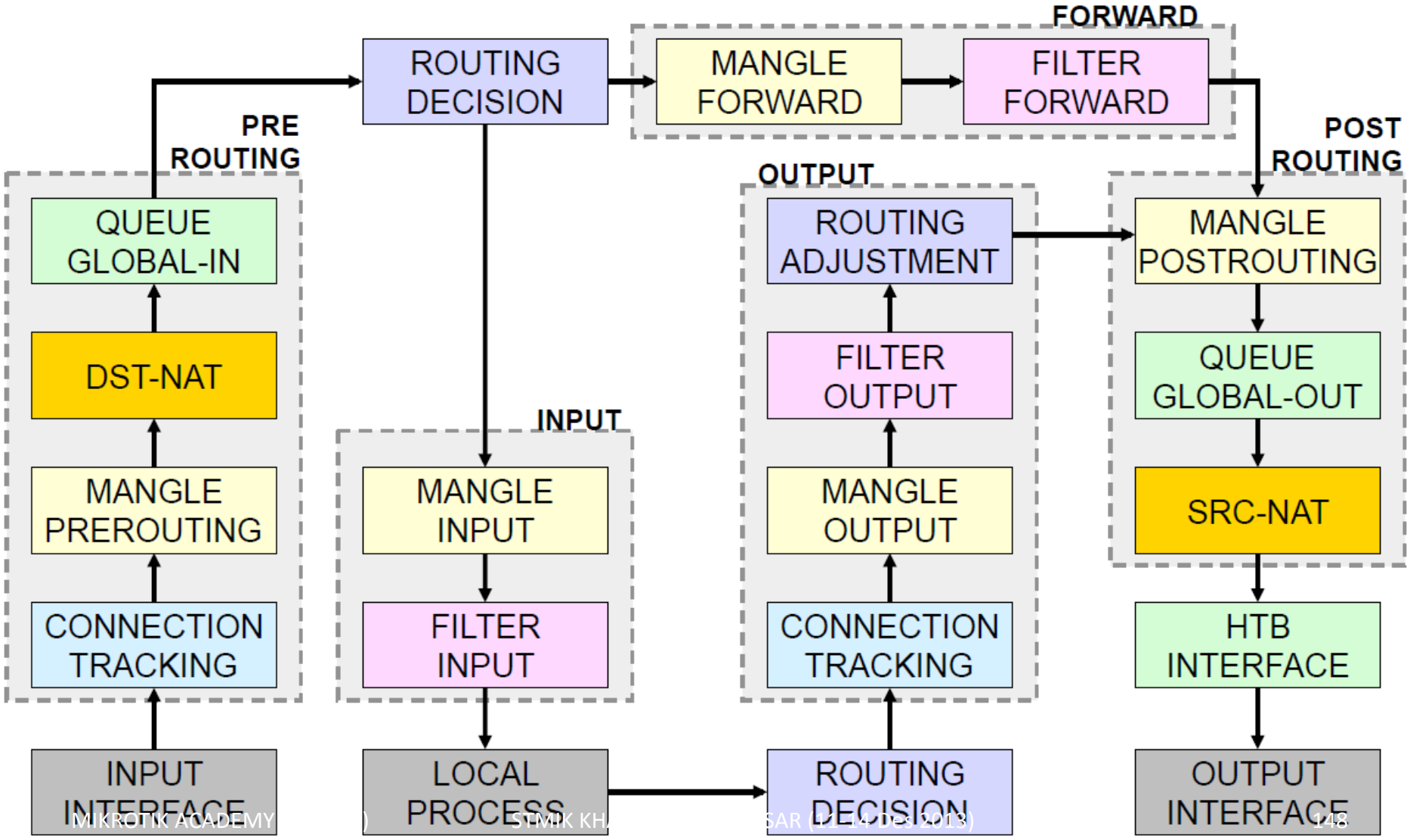
Mikrotik Firewall - Features

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

Traffic Flow (Aliran Data)

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

Simple Packet Flow



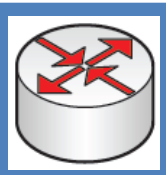
Posisi Chain / Parent

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

Firewall Filters – Blocking Rules

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

Chain pada Filter

			
Prerouting	Not Implemented	Not Implemented	Not Implemented
Input	Yes	No	No
Forward	No	Yes	No
Output	No	No	Yes
Postrouting	Not Implemented	Not Implemented	Not Implemented

Action Filter

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

RouterOS v5 Services

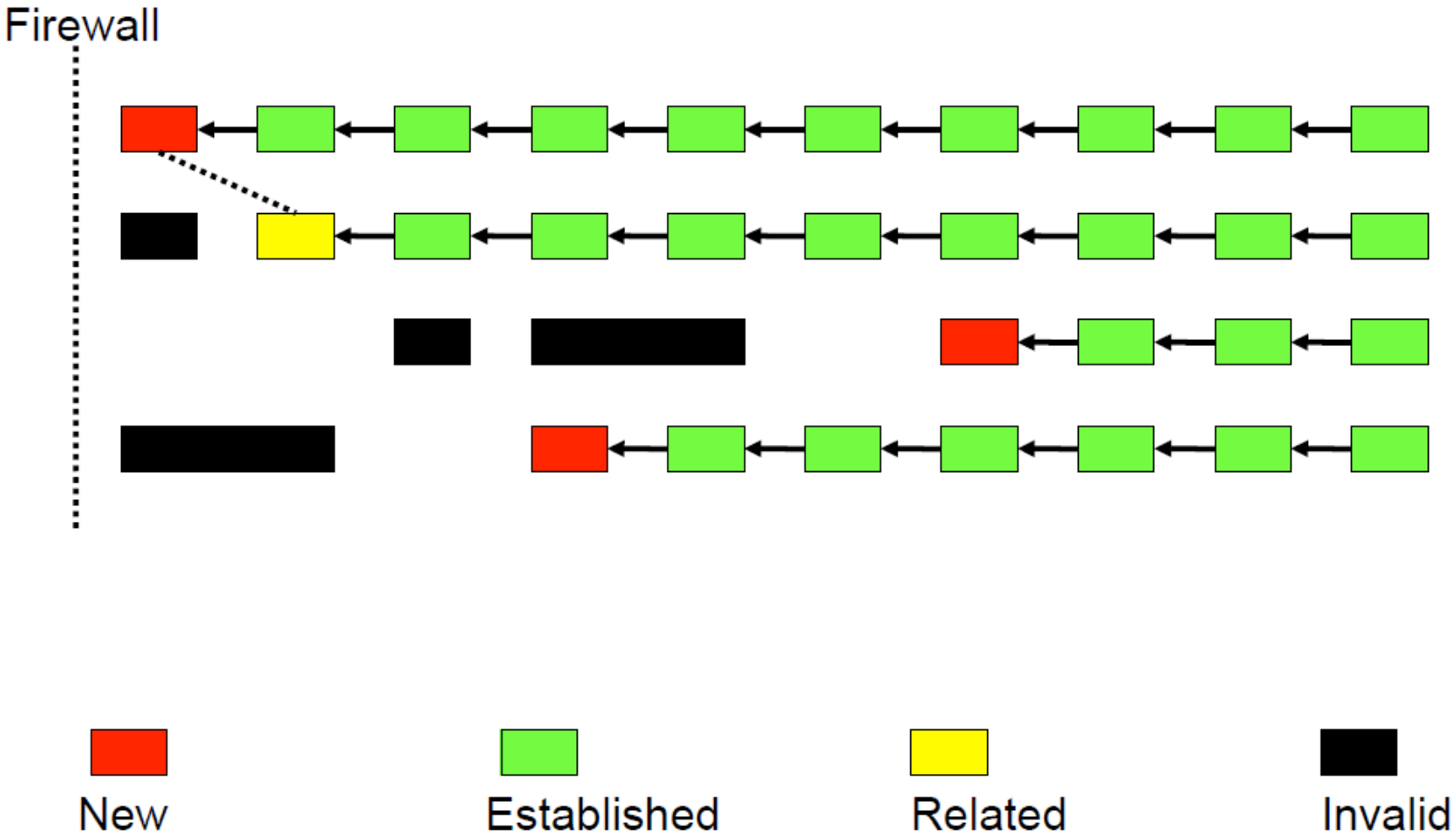
	PORT	PROTOCOL	DESCRIPTION
1	20	tcp	FTP
2	21	tcp	FTP
3	22	tcp	SSH, SFTP
4	23	tcp	Telnet
5	53	tcp	DNS
6	80	tcp	HTTP
7	179	tcp	BGP
8	443	tcp	SHTTP (Hotspot)
9	646	tcp	LDP (MPLS)
10	1080	tcp	SoCKS (Hotspot)
11	1723	tcp	PPTP
12	1968	tcp	MME
13	2000	tcp	Bandwidth Server
14	2210	tcp	Dude Server
15	2211	tcp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

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

Connection State

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

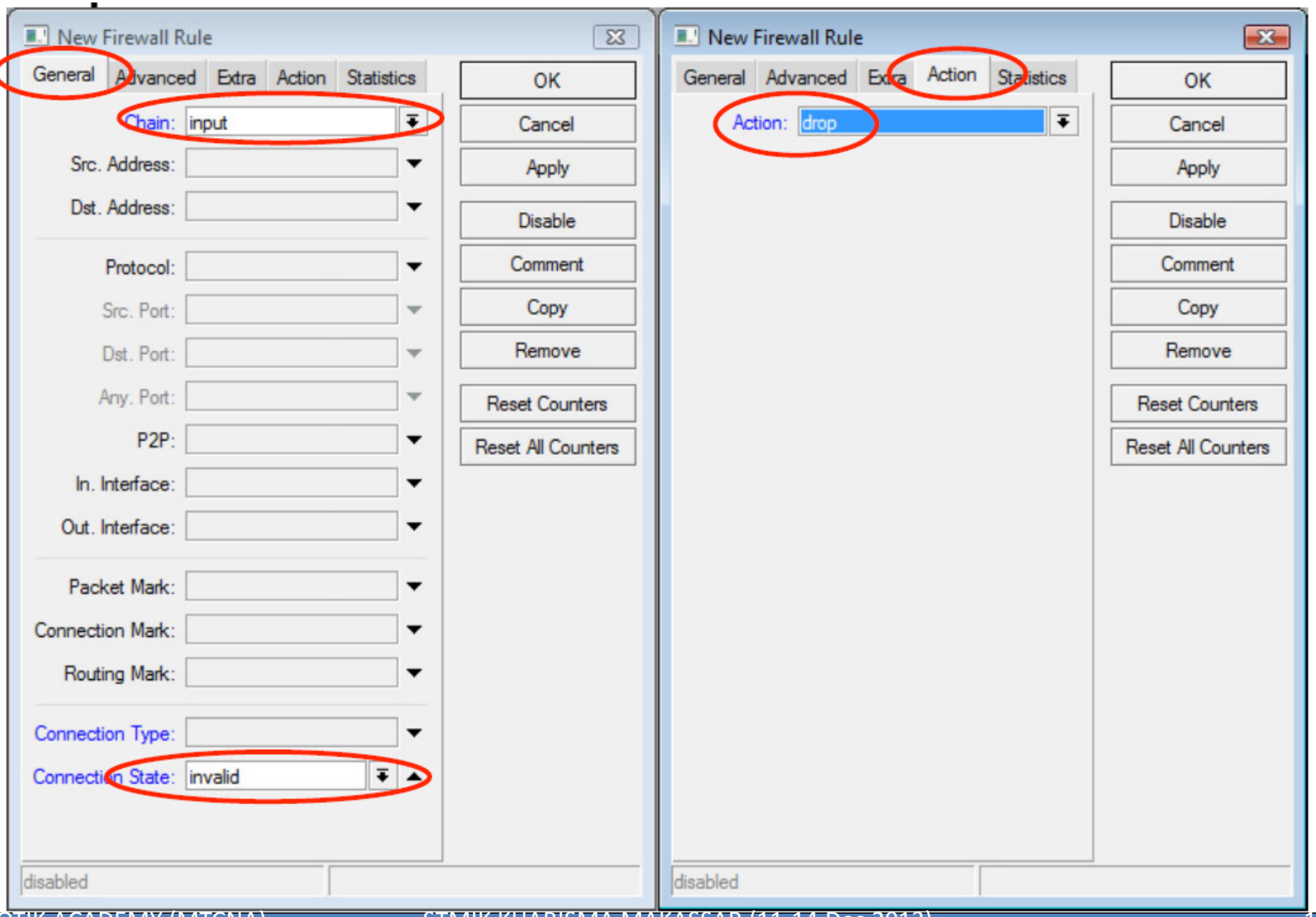
Connection State



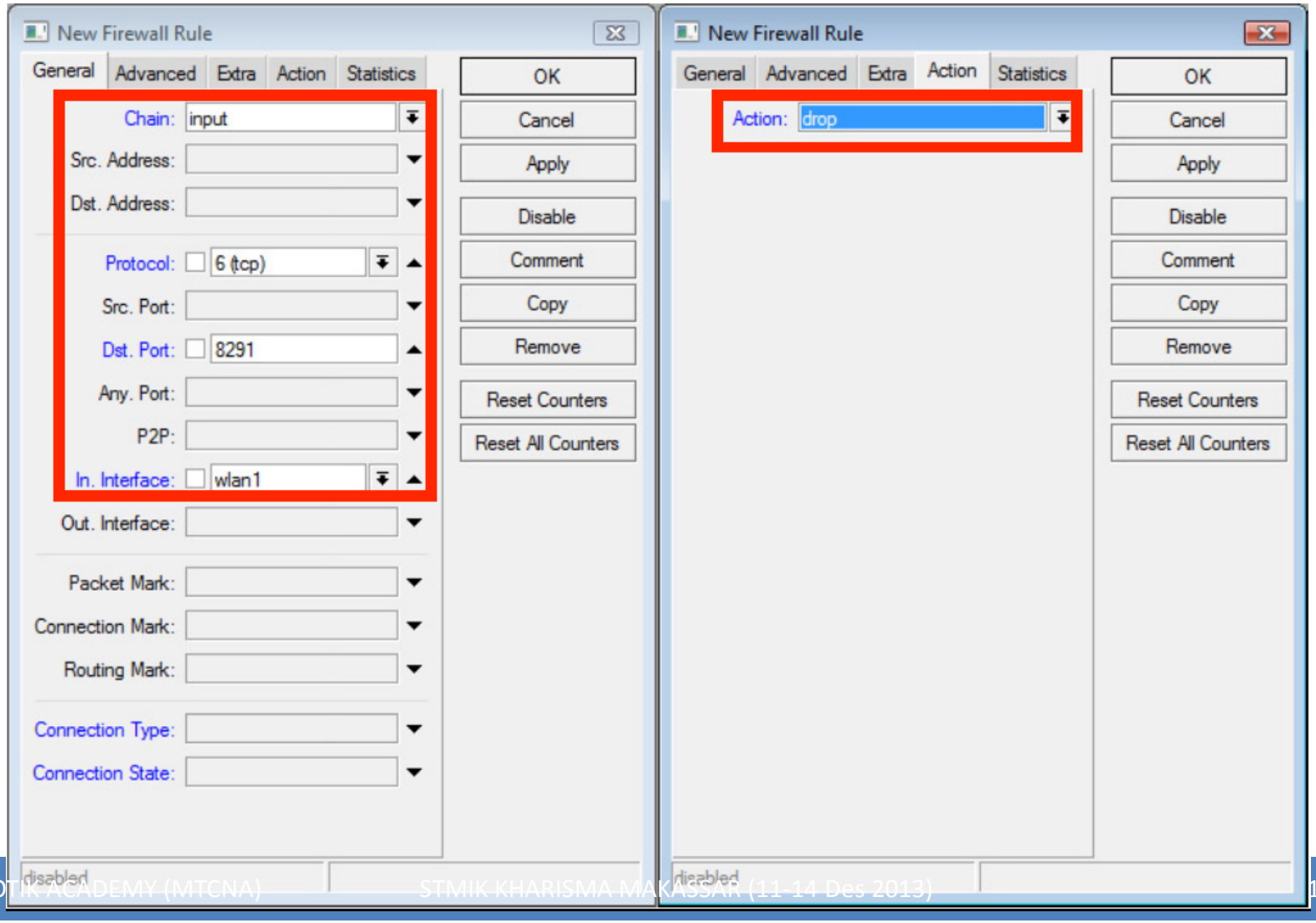
[LAB-2] Simple Blocking

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

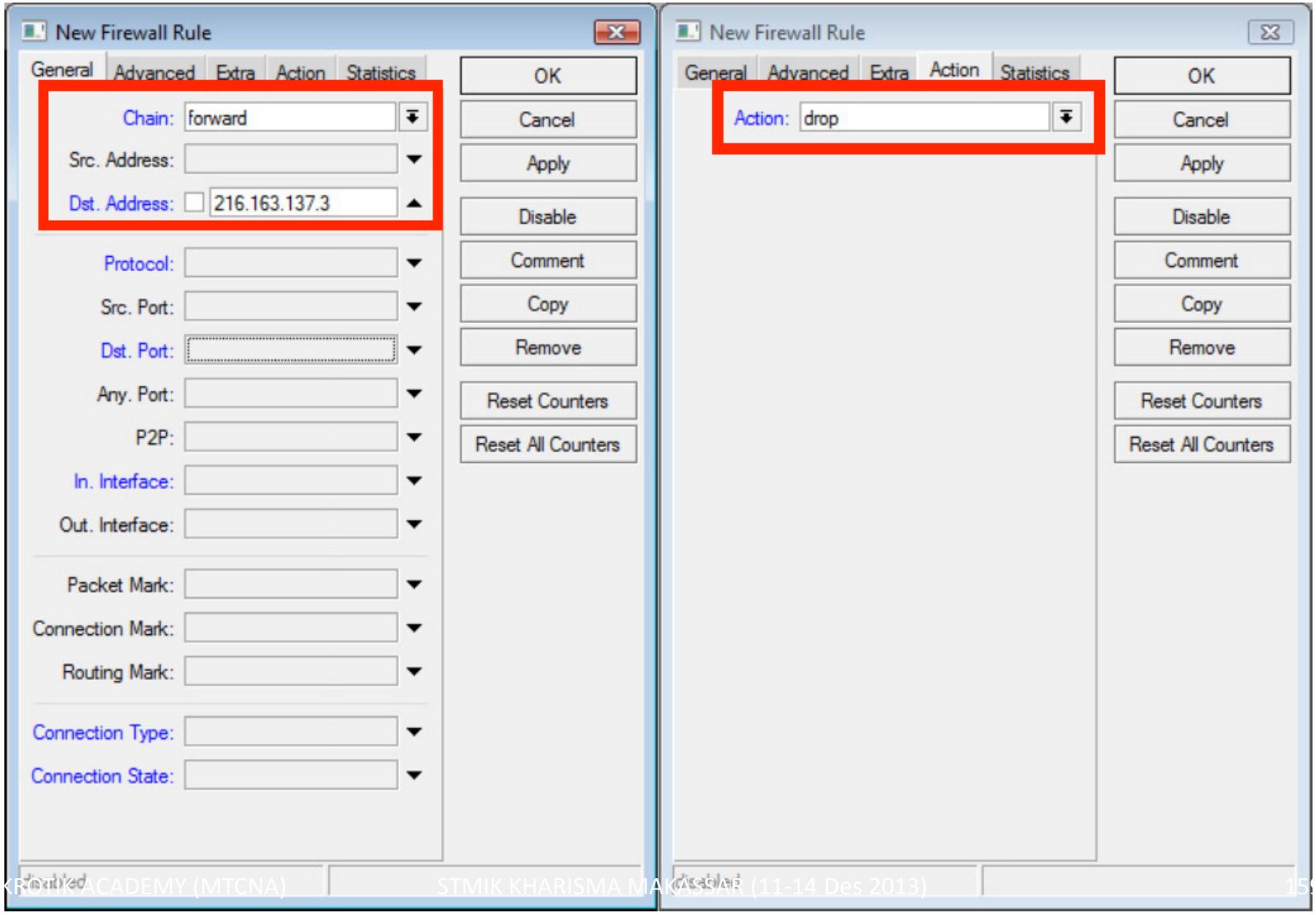
Blok Invalid Connection



Blok Koneksi Winbox ke Router dari interface publik (wlan)



Blok Nude Site



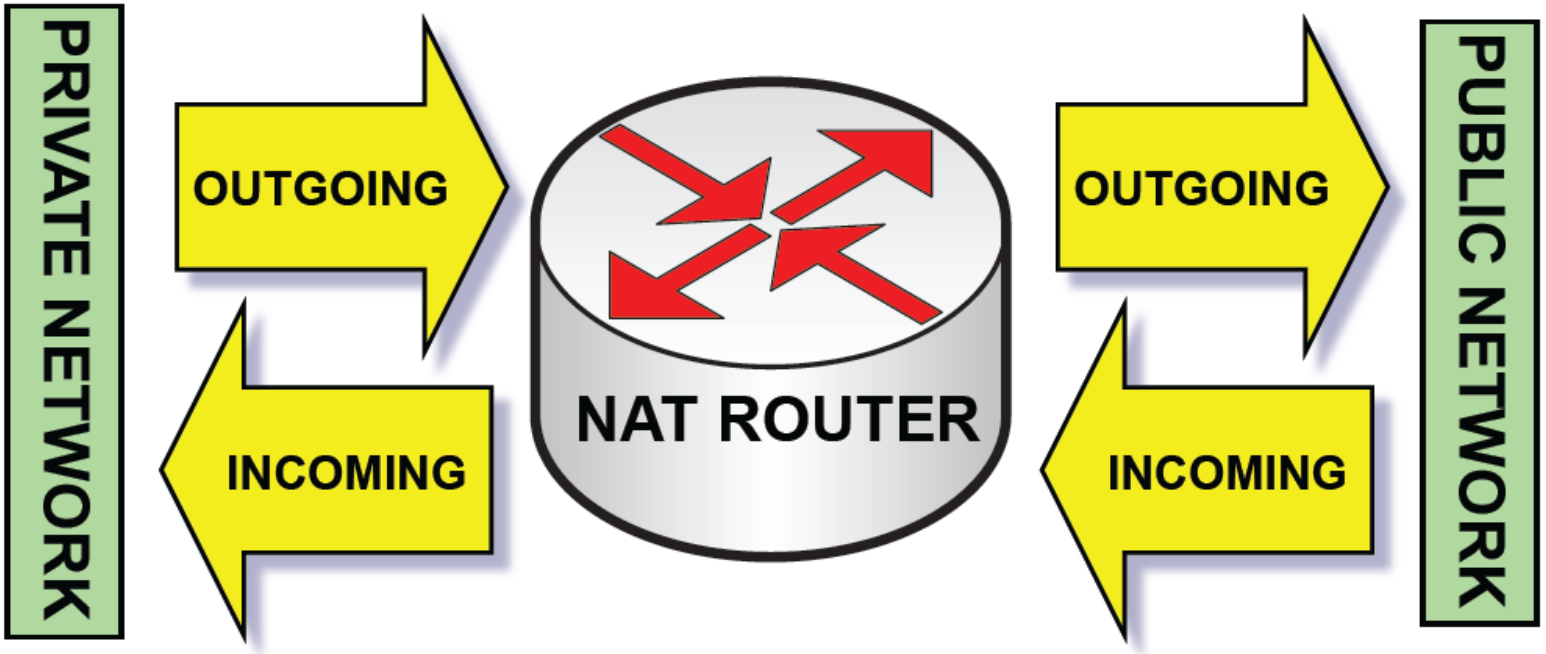
IP Address List

- 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.

Network Address Translation (NAT)

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

Firewall NAT



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

src-nat and masquerade

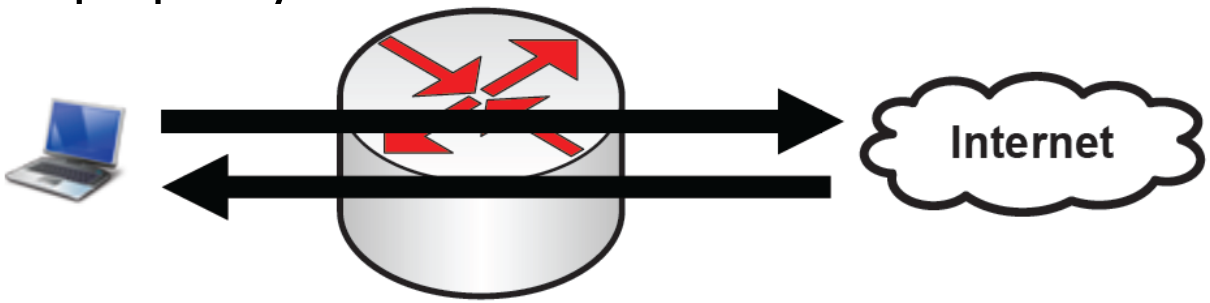
- Untuk menyembunyikan IP Address lokal dan menggantikannya dengan IP Address publik yang sudah terpasang pada router
- **src-nat**
  - Kita bisa memilih IP Address publik yang digunakan untuk menggantikan.
- **masquerade**
  - Secara otomatis akan menggunakan IP Address pada interface publik.
  - Digunakan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

dst-nat and redirect

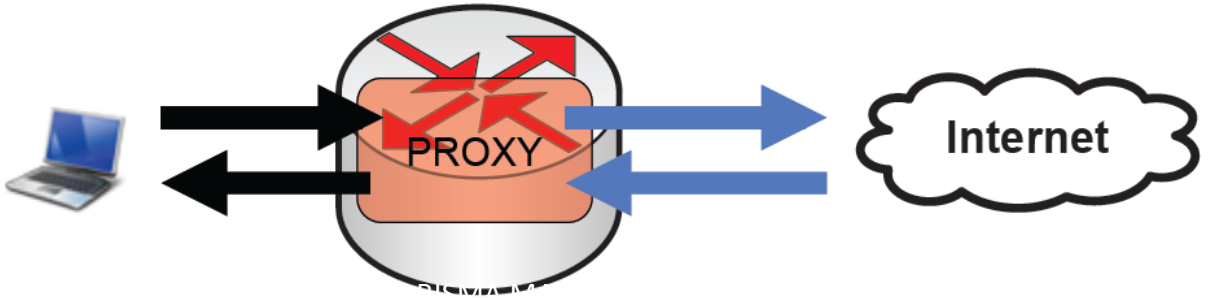
- Untuk melakukan penggantian IP Address tujuan, atau mengarahkan koneksi ke localhost.
- **dst-nat**
  - Kita bisa mengganti IP Address dan port tujuan dari seuatu koneksi.
- **redirect**
  - Untuk mengalihkan koneksi yang tadinya melwati router, dan dialihkan menuju ke loclhost

Konsep Proxy

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



- Koneksi dengan proxy



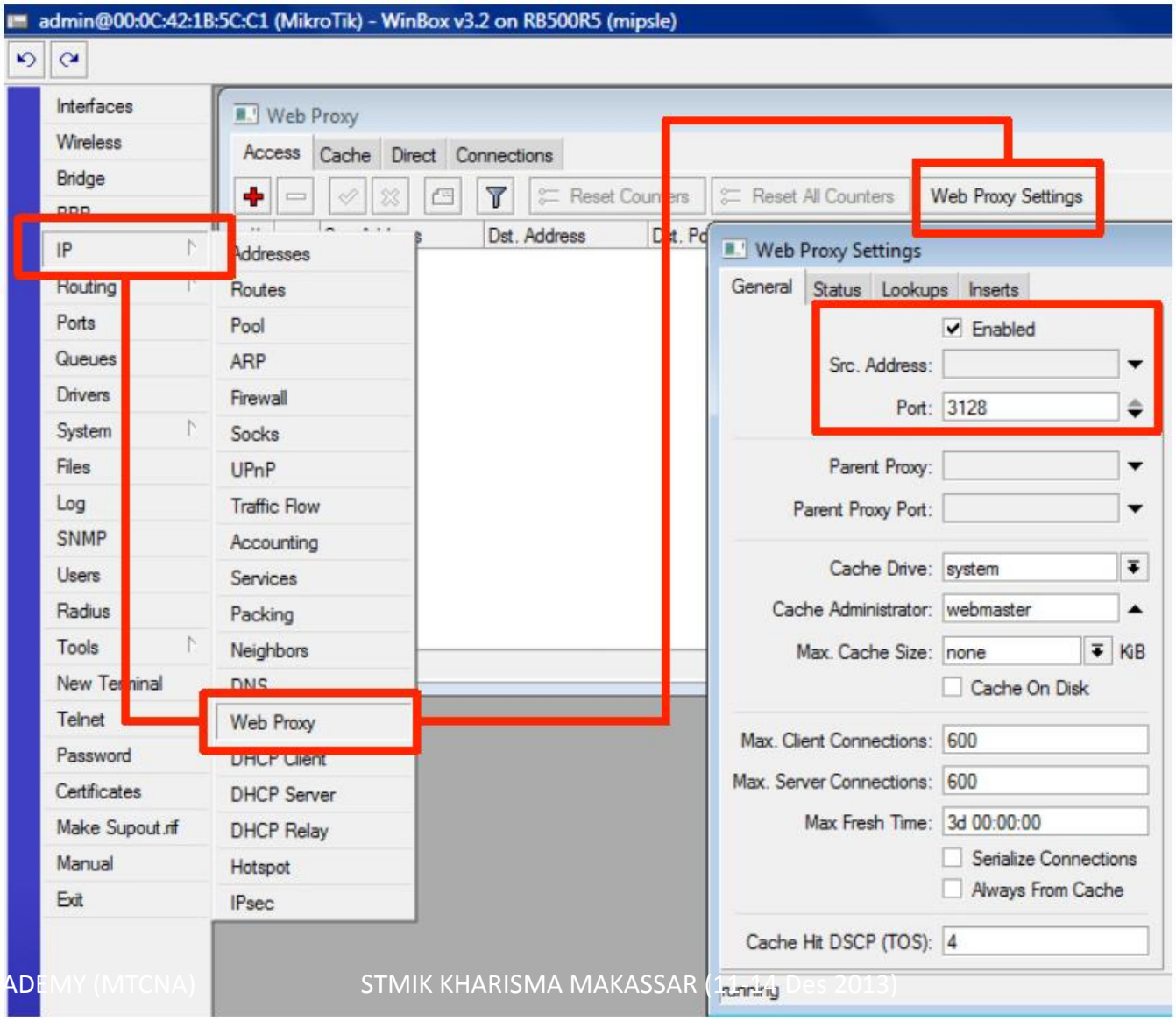
Fitur Proxy di RouterOS

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

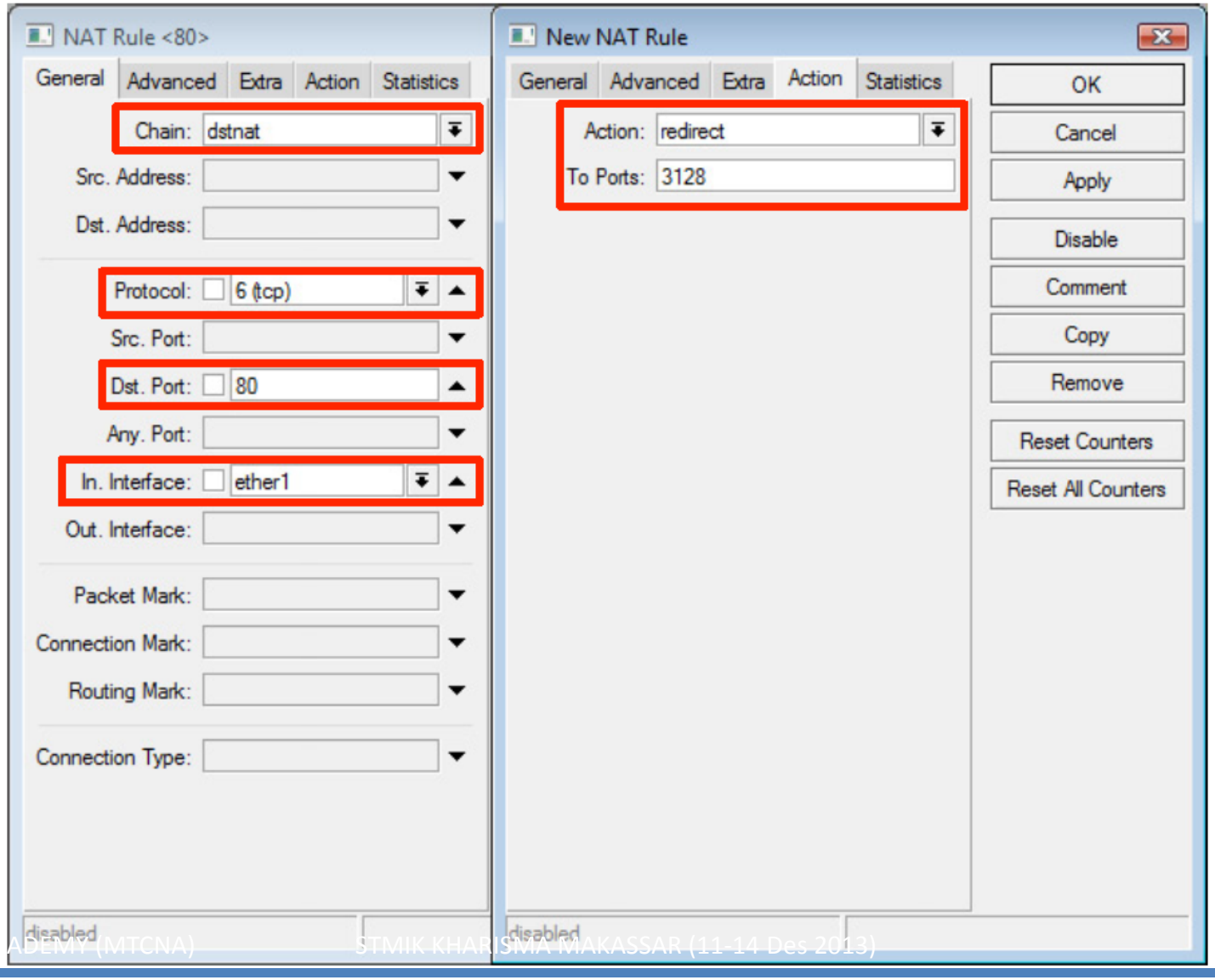
[LAB-5] dst-nat & local proxy

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

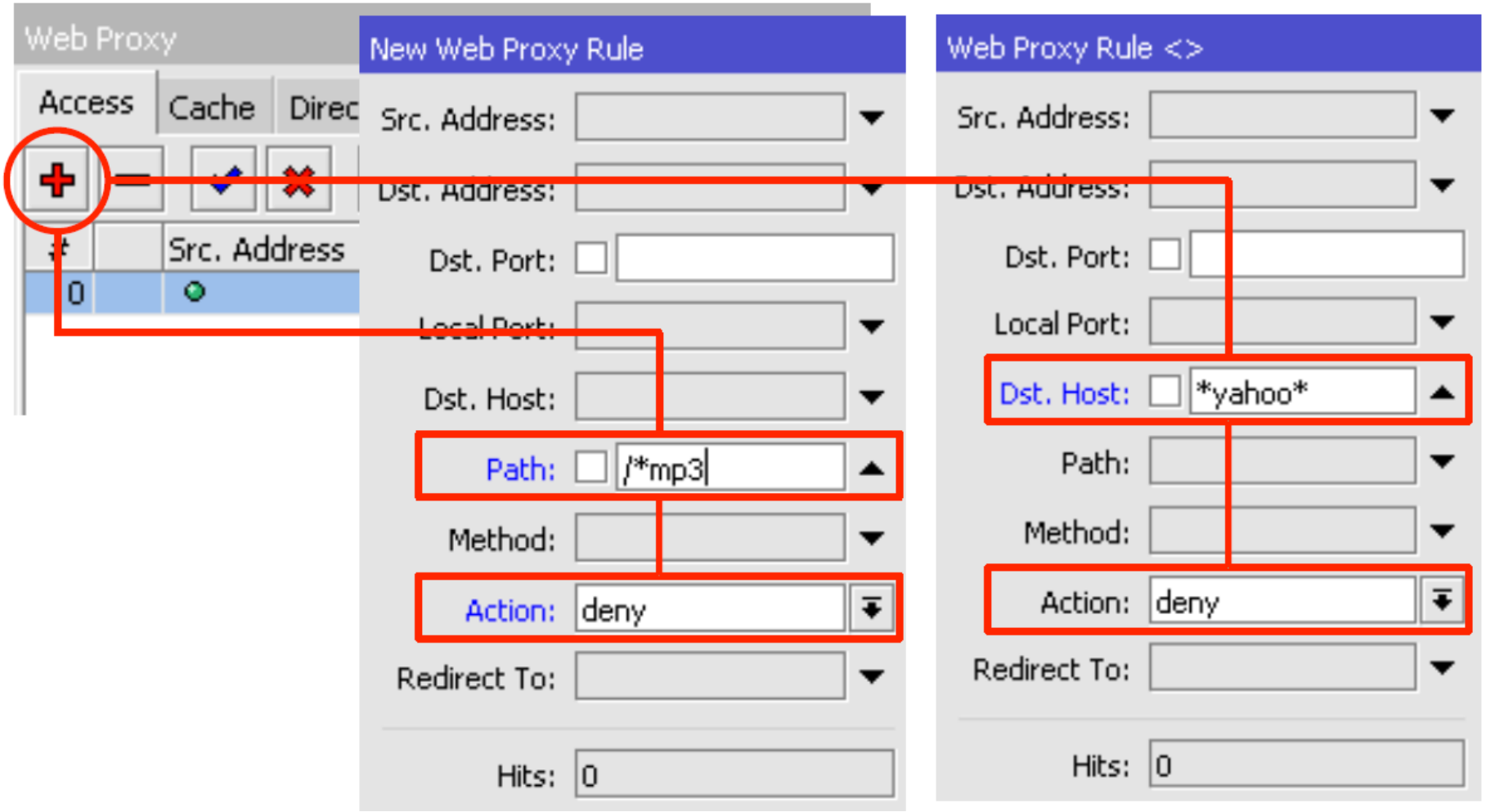
Mengaktifkan Proxy



Redirect TCP-80

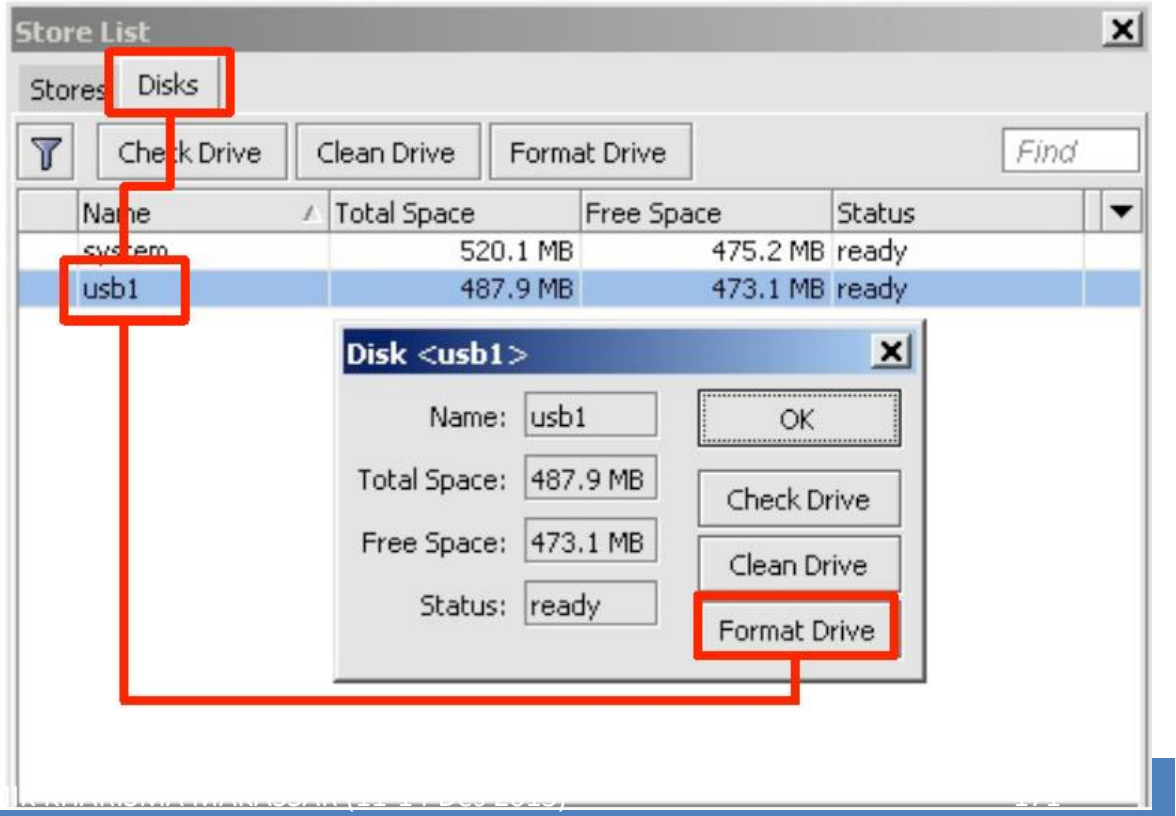


Akses


Web Proxy
Access
Cache
Direc
Src. Address
0
New Web Proxy Rule
Src. Address:
Dst. Address:
Dst. Port:
Local Port:
Dst. Host:
Path:
/*mp3
Method:
Action:
deny
Redirect To:
Hits:
0
Web Proxy Rule <>
Src. Address:
Dst. Address:
Dst. Port:
Local Port:
Dst. Host:
yahoo
Path:
Method:
Action:
deny
Redirect To:
Hits:
0

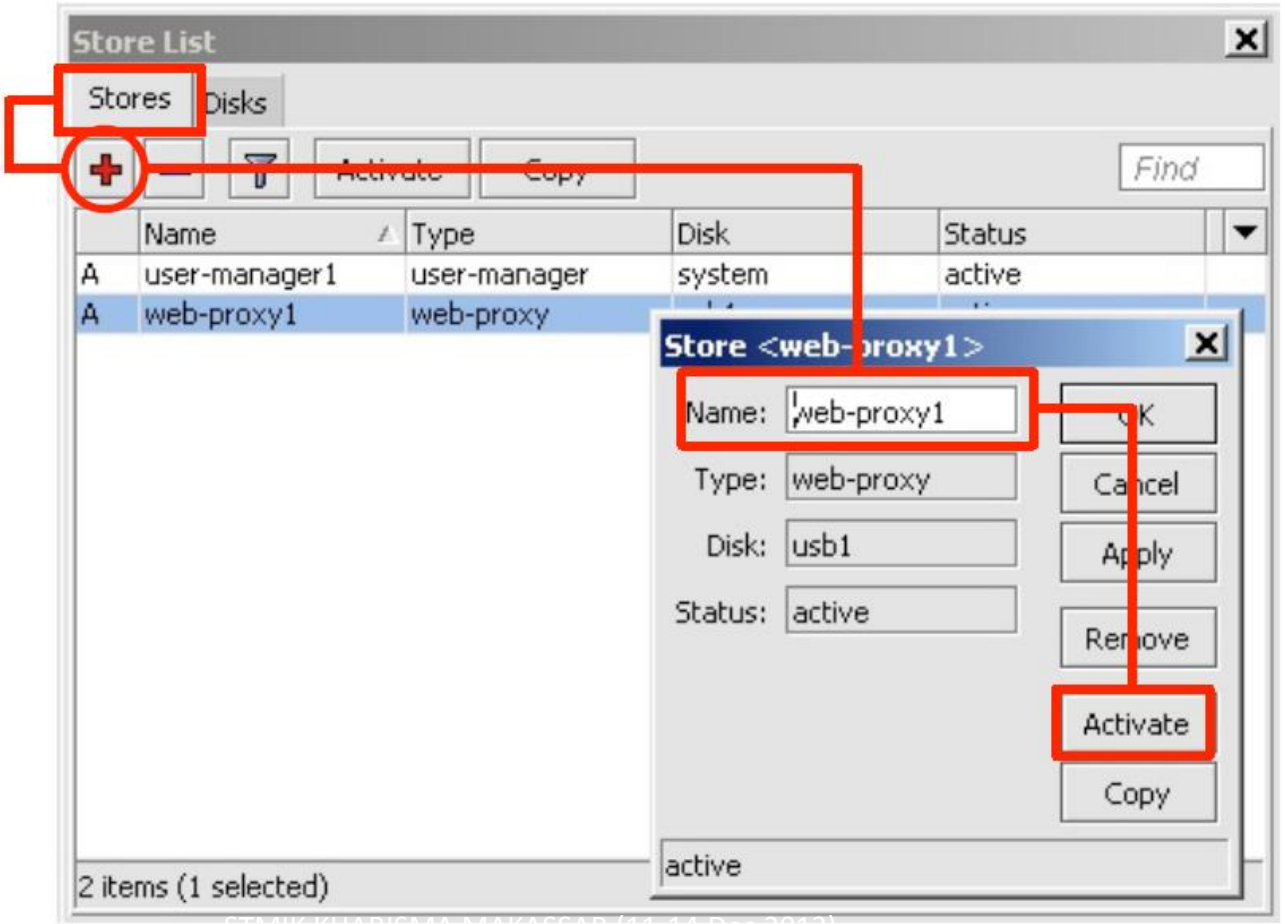
System Store - Disk

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



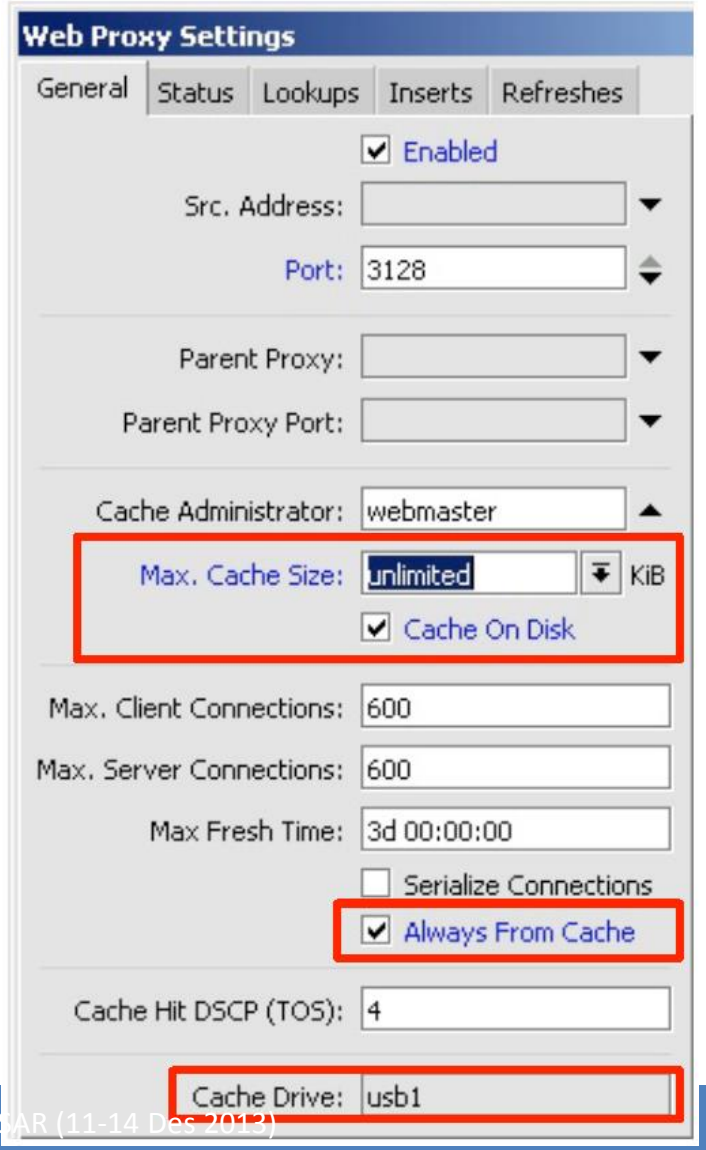
System Store – Store Mount

- Setelah diformat Disk di mount untuk service proxy.



Proxy - Cache

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



Daftar Protokol dan Port yang Sebaiknya Ditutup

Karena Virus, Spyware, dll

Block Bogus IP Address

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

Separate Protocol into Chains

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

Blocking UDP Packet

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

Only needed icmp codes in icmp chain

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

Deny Some TCP Ports

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

Virus and Worms (1)

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

Virus and Worms (2)

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

Terima Kasih