

MTCNA

MikroTik Certified Network Associate Training

Rofiq Fauzi, MTCNA, MTCRE, MTCWE, TR0165
ID-Networkers | www.Training-MikroTik.com

ID-NETWORKERS

Cisco, Juniper, **MikroTik**

Trainer	CCNA	CCNP	CCIP	CCIE	JNCIA	JNCIS	JNCIP	JNCIE	MTCNA	MTCRE	MTCTCE	MTCWE	Mikrotik Certified trainer
Dedi Gunawan	V	V	V	V					V	V	V		
Rofiq Fauzi									V	V		V	V
M. Amin					V	V	V	V					
Hadi Subowo	V		V										
Albertus Danar W	V				V	V							

Why us?

- ID-Networkers adalah kawah candradimuka bagi network engineer !!
- Siapapun boleh keluar masuk, belajar, tanya-tanya, konsultasi, nge-Lab dengan semua buku-buku dan perangkat yang ada disini, dll

Our Clients

- | | | |
|-----------------------------------|--|--|
| 1.PT. ERICSSON INDONESIA | 33.SENTRANET | 65.CORE MEDIATECH |
| 2.PT. INDOSAT | 34.BSI | 66.PT. COMPNET INTEGRATOR |
| 3.PT. MULTIMEDIA NUSANTARA | 35.PT. TEKUN DUTA MULTIMEDIA | 67.PT. PRIMA INTERAKTIF |
| 4.PT. XL AXIATA | 36.PT. SISTECH | 68.INDOSAT M2 |
| 5.PT. IBM INDONESIA | 37.PT. INOVASI LINTAS MEDIA | 69.PT. PRIMA INTERAKTIF |
| 6.PT. PASIFIK SATELIT NUSANTARA | 38.DIAN GRAHA ELEKTRIKA | 70.UKM (Universitas Kebangsaan Malaysia) |
| 7.PT. ASAHIMAS CHEMICAL | 39.PT. CIPTAMA PANCATUNGGAL | 71.BINA NUSANTARA |
| 8.PT. ASIAKOMNET MULTIMEDIA | 40.DTEX INDONESIA | 72.UNIVERSITAS INDONESIA |
| 9.PT. PRIMA MASTER BANK | 41.PT. ADICIPTA INOVASI TEKNOLOGI | 73.UNIVERSITAS BUDI LUHUR |
| 10.CV.MITRA USAHA CEMERLANG | 42.CV. COMMTECH | 74.PRESIDENT UNIVERSITY DORMITORY |
| 11.GENERAL LAJU | 43.MANULIFE | 75.KEMENTRIAN PAN DAN RB |
| 12.PT. APLIKANUSA LINTASARTA | 44.BERCA CAKRA TEKNOLOGI | 76. LINTAS ARTHA |
| 13.PT. DATACOMM | 45.DTP | 77.TELE GLOBAL GLOBAL |
| 14.PT. BERLIAN SISTEM INFORMASI | 46.PT. NOKIA SIEMENS NETWORK | 79. UNIVERSITAS SEBELAS MARET |
| 15.PT. PRAWEDANET | 47.INIXINDO | 80. UMARA SAT (IRAQ COMPANY) |
| 16.KARYAMEGAH ADIJAYA | 48.CISCO SYSTEM | |
| 17.TECHMAHINDRA INDONESIA | 49.HUAWEI | |
| 18.PERTAMINA EP | 50.PT. BUANA LINTAS MEDIA | and many more |
| 19.FUJITSU LTD | 51.LEMBAGA PEMBIAYAAN EKSPOR INDONESIA | |
| 20.ACCTURE | 53.PT. LG ELECTRONIC | |
| 21.PT. TELESAT | 54.INDOVISION | |
| 22.PT. MULTIPOLAR TECHNOLOGY | 55.BPR OLYMPINDO | |
| 23.PT. NCI | 56.PT. UNITED FLOW CONTROL | |
| 24.MITRA INTEGRASI INFORMATIKA | 57.ALLIANZ | |
| 25.PT. REKADAYA ELEKTRIKA | 58.PT. KALTIM PASIFIK AMONIAK | |
| 26.HARAPAN RAINFOREST | 59.PT. AGUNG WAHANA INDONESIA | |
| 27.METRODATA | 60.PT. FORTIUS INFORMATIKA | |
| 28.PT. PROSYS BANGUN PERSADA | 61.PT. LGEIN | |
| 29.PT. KAYREACH SYSTEM | 62.PT. VISIONET INTERNASIONAL | |
| 30.IT PARTNERSHIP PRIVATE | 63.PT. SCIENTIA PELITA | |
| 31.PT. ADICIPTA INOVASI TEKNOLOGI | 64.CV. PUTRI INDAH | |
| 32.TAEJIN PERKASA | | |



Rofiq Fauzi

- Using MikroTik (v.2.97) since 2005, as Network Engineer at WISP company.
- 2007, Network & Wireless Engineer at INDOSAT (Internet Network Provider Division).
- 2008, IT & Telco Procurement (Procurement Group) at INDOSAT
- 2012, MikroTik Certified Trainer (MTCNA, MTCRE, MTCWE, TR0156) at ID-Networkers.

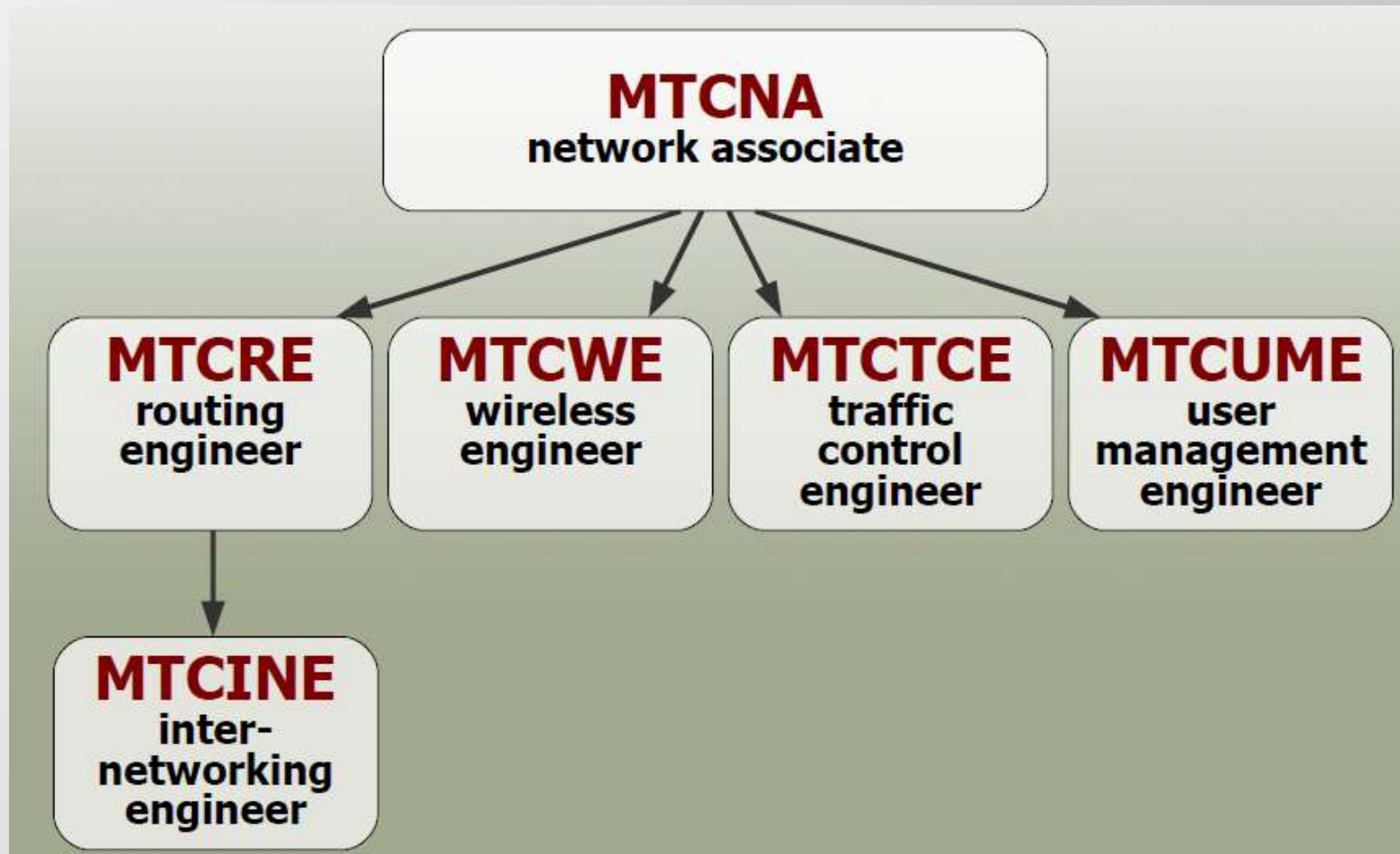
Perkenalkan Diri Anda

- Silahkan perkenalkan diri anda:
 - Nama?
 - Perusahaan / Universitas?
 - Pengalaman menggunakan MikroTik?
 - Pengalaman tentang jaringan?
 - Apa yang diharapkan dari training ini?

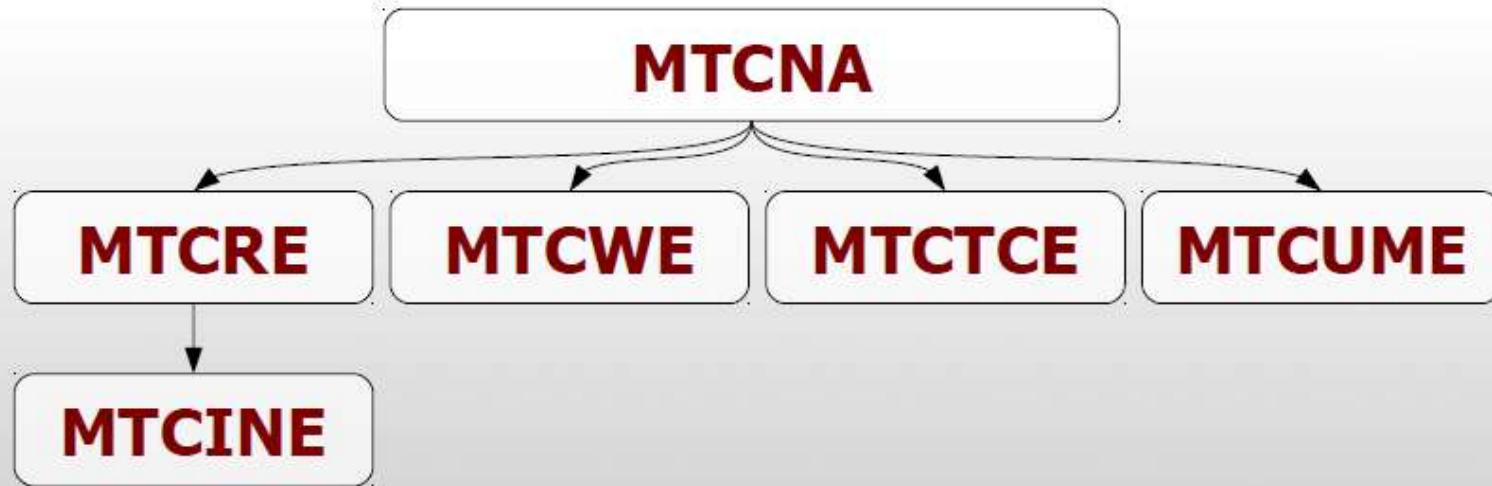
Tujuan Training MTCNA

1. Mempelajari karakteristik, fitur-fitur dan kemampuan MikroTik RouterOS.
2. Mempelajari cara instalasi, konfigurasi, fungsi, maintenance dan troubleshoot dasar MikroTik RouterOS.
3. Mendapatkan kualifikasi sebagai MikroTik Certified Network Associate.

Sertifikasi MikroTik



Certificate Prerequisite



... if certificates are expired



Connect Internet

- Wifi = IDN Mantab
- Password = 12345lupa



Registrasi Account di Mikrotik.com

- Register account di www.mikrotik.com.
- Pastikan nama anda ditulis lengkap dalam profil, karena otomatis akan tercetak dalam sertifikat.

User Information

Company Name (or person name):	Rofiq Fauzi, ID-Networkers *
Authorised Person (<i>Firstname Lastname</i>) or Purchaser (for ordering):	Rofiq Fauzi *
E-mail (License key will be sent here):	rofiq.fauzi@gmail.com *

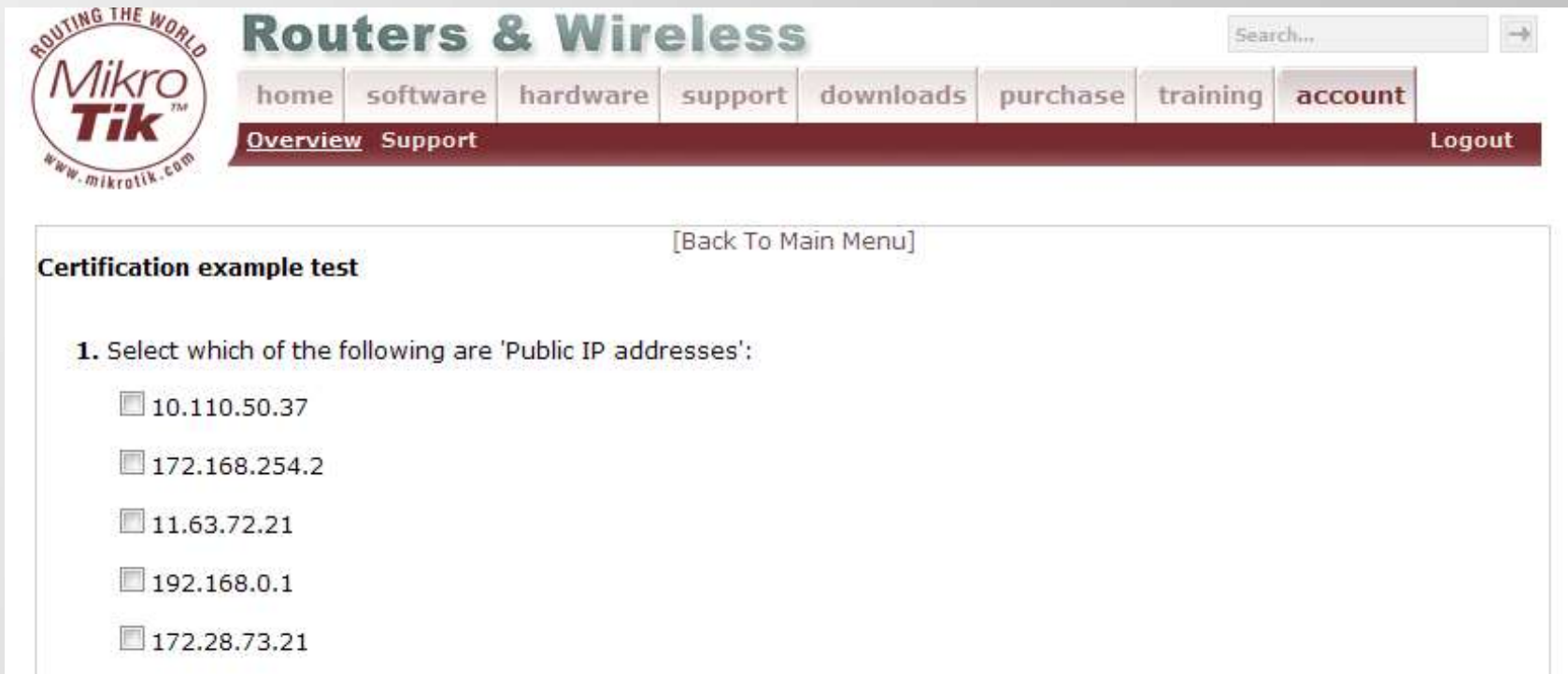
- Informasikan email anda ke instruktur, peserta harus mendapat invitation dari instruktur.

Tentang Ujian MTCNA

- Online test terdiri atas 25 soal dalam waktu 1 jam.
- Soal setiap test random, dengan beberapa soal mungkin ada yang sama dengan soal sebelumnya.
- Passing grade **60%**, nilai 50%-59% bisa test ulang.
- Hati-hati membaca soal, disamping bahasa inggris dari soal yang kadang-kadang kurang mudah dipahami, juga banyak jebakan batman 😊.
- **Silahkan melakukan latihan test training di web mikrotik, dan lihat scorenya.**

Latihan Test

- Setelah mendapatkan invitation dari trainer, peserta dapat melakukan latihan ujian MTCNA di website mikrotik.com
- Latihan ujian MTCNA ada di menu Account , My training session, Try example test



ROUTING THE WORLD
MikroTik
 www.mikrotik.com

Routers & Wireless

Search... →

home software hardware support downloads purchase training **account**

Overview Support Logout

[Back To Main Menu]

Certification example test

1. Select which of the following are 'Public IP addresses':

- 10.110.50.37
- 172.168.254.2
- 11.63.72.21
- 192.168.0.1
- 172.28.73.21

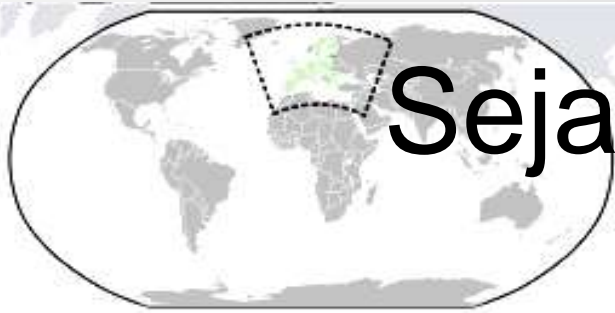
MTCNA – Outline

- Module 1 – Introduction of MikroTik RouterOS
 - TCP/IP Review
- Module 2 - Firewall
- Module 3 - Wireless
- Module 4 - QoS
- Module 5 - Bridging
- Module 6 - Network Management
- Module 7 – Routing
- Module 8 – Tunnels


BAB I

Introduction MikroTik RouterOS & RouterBOARD





Sejarah MikroTik

- Lokasi : Riga, Latvia (Eropa Utara) 
- Produsen software dan hardware router.
- Menjadikan teknologi internet lebih murah, cepat, handal dan terjangkau luas.
- Motto Mikrotik : Routing the World.
- Founder (1996): John Trully & Arnis Reikstins.

Jenis MikroTik

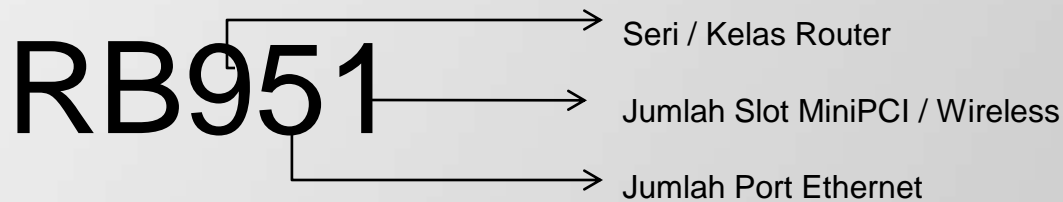
- MikroTik RouterOS™
 - ✓ Software untuk mengubah PC bisa menjadi sebuah Router yang handal.
 - ✓ Berbasis Linux
 - ✓ Diinstall sebagai Sistem Operasi
 - ✓ Biasanya diinstall pada power PC
- MikroTik RouterBOARD
 - ✓ Built in hardware (board) yang menggunakan RouterOS sebagai Operating Sistemnya.
 - ✓ Tersedia mulai low-end s/d high-end Router.

Fitur-Fitur Mikrotik

- Router OS support berbagai driver perangkat
 - ✓ Ethernet, Wireless Card, V35, ISDN, USB Mass Storage, USB 3G Modem, E1/T1.
- Memiliki fitur yang melebihi sebuah “router”
 - ✓ User Management (DHCP, Hotspot, Radius, dll).
 - ✓ Routing (RIP, OSPF, BGP, RIPng, OSPF V3).
 - ✓ Firewall & NAT (fully-customized, linux based).
 - ✓ QoS/Bandwidth limiter (fully customized, linux based).
 - ✓ Tunnel (EoIP, PPTP, L2TP, PPPoE, SSTP, OpenVPN).
 - ✓ Real-time Tools (Torch, watchdog, mac-ping, MRTG, sniffer).

RouterBOARD - Type

- RouterBoard memiliki sistem kode tertentu



- Kode Lain ada di belakang tipe
 - ✓ U - dilengkapi port USB
 - ✓ A - Advanced, biasanya diatas lisensi level 4
 - ✓ H - Hight Performance, processor lebih tinggi
 - ✓ R - dilengkapi wireless card embedded.
 - ✓ G - dilengkapi port ethernet Gigabit
 - ✓ 2nD – dual channel

Arsitektur RouterBoard

- Arsitektur RouterBoard dibedakan berdasarkan jenis dan kinerja processor,
- software/OS untuk setiap arsitektur berbeda

routeros-mipsle (<i>mipsle</i>)	combined package for mipsle (RB100, RB500) (includes <i>system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing</i>)
routeros-mipsbe (<i>mipsbe</i>)	combined package for mipsbe (RB400) (includes <i>system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing</i>)
routeros-powerpc (<i>ppc</i>)	combined package for powerpc (RB300, RB600, RB1000) (includes <i>system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing</i>)
routeros-x86 (<i>x86</i>)	combined package for x86 (Intel/AMD PC, RB230) (includes <i>system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing</i>)
mpls-test (<i>mipsle, mipsbe, ppc, x86</i>)	Multi Protocol Labels Switching support improvements
routing-test (<i>mipsle, mipsbe, ppc, x86</i>)	routing protocols (RIP, OSPF, BGP) improvements

MikroTik VS Cisco

source: http://wiki.MikroTik.com/wiki/Manual:RouterOS_FAQ

How does this software compare to using a Cisco router?

*You can **do almost everything** that a proprietary router does at a fraction of the **cost** of such a router and have flexibility in upgrading, **ease of management and maintenance**.*

Anda dapat melakukan **hampir semua** yang dilakukan proprietary router tersebut (Cisco) dengan hanya sebagian kecil dari biaya router tersebut dan memiliki **fleksibilitas dalam mengupgrade, kemudahan manajemen dan pemeliharaan**.

Prerequisites MTCNA Training

TCP / IP Basic

Internet Protocol

Internet Protocol adalah sebuah aturan atau standar yang mengatur atau mengizinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer.

Tugas Internet Protocol



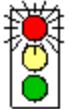




- Melakukan deteksi koneksi fisik.
- Melakukan metode “jabat-tangan” (handshaking).
- Negosiasi berbagai macam karakteristik hubungan.
- Mengawali dan mengakhiri suatu pesan/session.
- Bagaimana format pesan yang digunakan.
- Apa yang dilakukan apabila terjadi error pengiriman?.
- Mengkalkulasi dan menentukan jalur pengiriman.
- Mengakhiri suatu koneksi.

OSI Layer Model

- Tidak adanya suatu protokol yang sama, membuat banyak perangkat tidak bisa saling berkomunikasi.
- ***Open System Interconnection*** atau OSI layer 7 adalah model arsitektural jaringan yang dikembangkan oleh International Organization for Standardization (ISO) di Eropa tahun 1977.
- Sebelum ada OSI, sistem jaringan **sangat tergantung kepada vendor** pemasok perangkat jaringan yang berbeda-beda.
- Model OSI layer 7 merupakan koneksi logis yang harus terjadi agar terjadi komunikasi data dalam jaringan.

OSI Layer

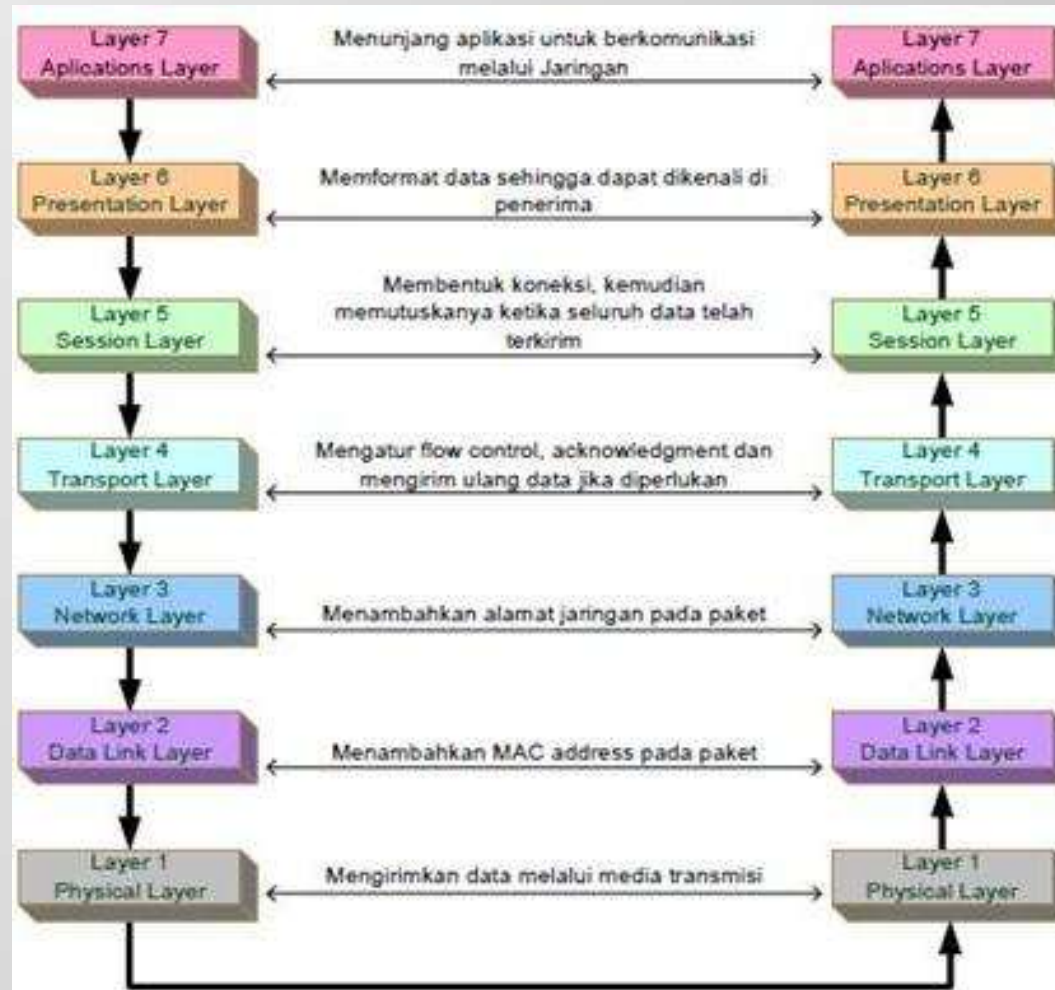
- Apabila 7 OSI Layer susah untuk dihafal, maka Layer 1, Layer 2 dan Layer 3 adalah suatu keharusan, karena dapat menunjukkan bedanya antara Hub/bridge, Switch dan Router
- Ketiganya berada di layer yang berbeda sehingga memiliki cara kerja yang berbeda tentunya

OSI MODEL	
7	 Application Layer Type of communication: E-mail, file transfer, client/server.
6	 Presentation Layer Encryption, data conversion: ASCII to EBCDIC, BCD to binary, etc.
5	 Session Layer Starts, stops session. Maintains order.
4	 Transport Layer Ensures delivery of entire file or message.
3	 Network Layer Routes data to different LANs and WANs based on network address.
2	 Data Link (MAC) Layer Transmits packets from node to node based on station address.
1	 Physical Layer Electrical signals and cabling.

Layer	Name	Device	Data Unit	Addressing
Layer 3	Network	Router	Paket	IP Address
Layer 2	Data Link	Switch	Frame	MAC Address
Layer 1	Physical	Hub	Bit	0111001110

Device	Connectivity	Data Transfer	Memory
Router	Antar network yang berbeda	Destination IP Address	Routing Table
Switch	Antar network yang sama	Berdasar MAC Address Tujuan	MAC Address Table
Hub	Antar network yang sama	Broadcast ke semua port	none

OSI 7 Leyer - Koneksi Antar Host



MAC Address

- MAC Address (Media Access Control Address) adalah alamat jaringan pada lapisan data-link (layer 2) dalam OSI 7 Layer Model.
- Dalam sebuah komputer, MAC address ditetapkan ke sebuah kartu jaringan (network interface card/NIC).
- MAC address merupakan alamat yang unik yang memiliki panjang 48-bit.
- MAC terdiri atas 12 digit bilangan heksadesimal (0 s/d F), **6 digit pertama** merepresentasikan **vendor pembuat kartu jaringan**.
- Contoh MAC Address : **02-00-4C-4F-4F-50**.


IP Address

- IP (Internet Protocol) terdapat dalam Network Layer (layer 3) OSI.
- IP address digunakan untuk pengalamatan suatu PC / host secara logic
- Terdapat 2 jenis IP Address
 - ✓ IPv4
 - ✓ Pengalamatan 32 bit
 - ✓ Jumlah max host 4,294,967,296
 - ✓ IPv6
 - ✓ Pengalamatan 128 bit
 - ✓ Jumlah max host
340,282,366,920,938,463,374,607,431,768,211,456

IPv4

- IPv4 diekspresikan dalam notasi desimal bertitik, yang dibagi ke dalam 4 buah oktet berukuran 8-bit.
- Karena setiap oktet berukuran 8-bit, maka nilainya berkisar antara 0 hingga 255 (2^0 s/d 2^7)
- Aturan pengalamatan IPv4, misal IP 192.148.41.1

11000000.10010100.00101111.00000001



$$\begin{aligned}
 &1x2^7 + 0x2^6 + 0x2^5 + 1x2^4 + 0x2^3 + 1x2^2 + 0x2^1 + 0x2^0 \\
 &1x128 + 0x64 + 0x32 + 1x16 + 0x8 + 1x4 + 0x2 + 0x1 \\
 &128 + 0 + 0 + 16 + 0 + 4 + 0 + 0 = \boxed{148}
 \end{aligned}$$

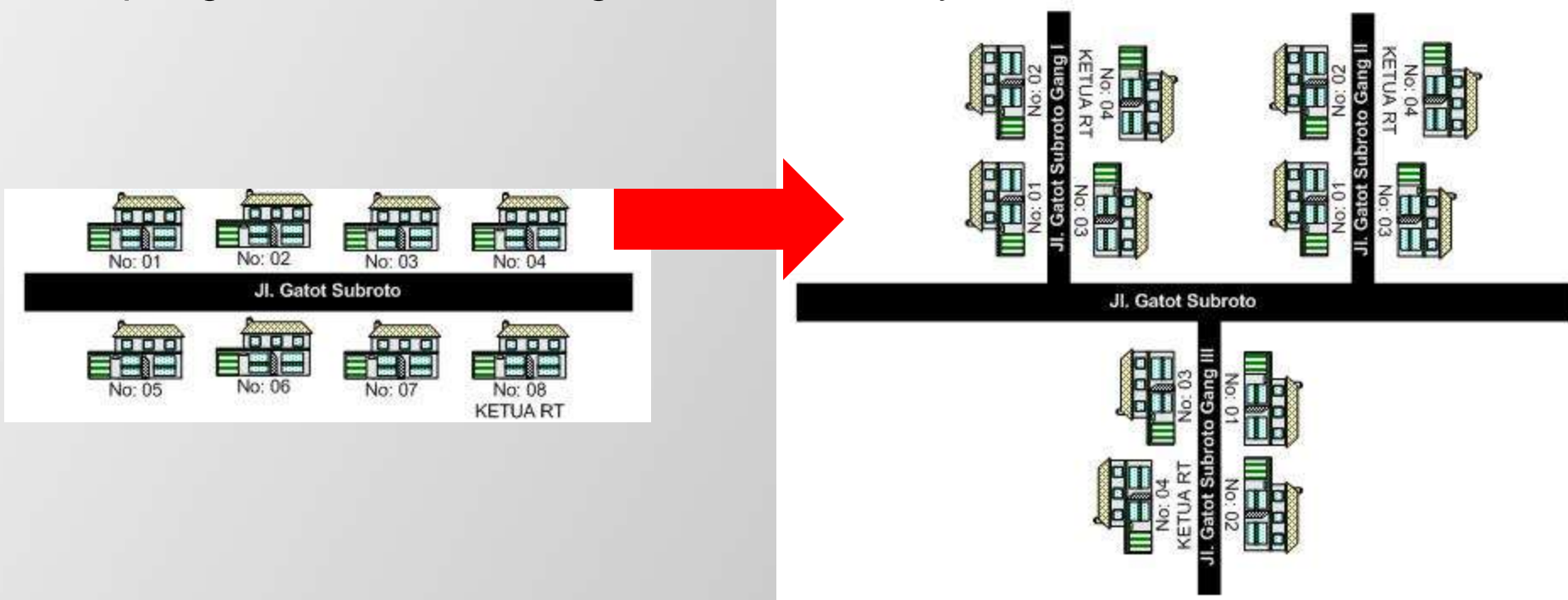
192 . 148 . 41 . 1

Subneting

- Alamat IP didesain untuk digunakan secara berkelompok (sub-jaringan/subnet).
- Subneting adalah cara untuk memisahkan dan mendistribusikan beberapa alamat IP.
- Host/perangkat yang terletak pada subnet yang sama dapat berkomunikasi satu sama lain secara langsung (tanpa melibatkan router/routing).

Subneting

- Apabila jaringan dianalogikan sebuah jalan, apabila disepanjang jalan cuma ada 8 rumah, ketua RT mengumumkan sesuatu dari rumah ke rumah lewat jalan itu.
- Apabila sepanjang jalan sudah penuh rumah butuh ada gang-gang . Butuh ada ketua RT tiap gang untuk meminimalis transportasi saat pengumuman dan mengatur urusan RTnya sendiri



Notasi Subnet

- Subnet ditulis dalam format 32 bit (seperti IP), atau dalam bentuk desimal (prefix Length)

Subnet mask (biner)	Subnet mask (desimal)	Prefix Length
11111111.00000000.00000000.00000000	255.0.0.0	/8
11111111.11111111.00000000.00000000	255.255.0.0	/16
11111111.11111111.11111111.00000000	255.255.255.0	/24

- Sebagai contoh, network 192.168.1.0 yang memiliki subnet mask 255.255.255.0 dapat direpresentasikan di dalam notasi prefix length sebagai **192.168.1.0/24**.

Network ID dan Broadcast

- Dalam kelompok IP address ada 2 IP yang sifatnya khusus
 - Network ID : identitas suatu kelompok IP / Subnet.
 - Broadcast : alamat IP yang digunakan untuk memanggil semua IP dalam satu kelompok.
- Untuk menentukan network id dan broadcast dari sebuah alamat IP dengan subnet mask tertentu, dapat dilakukan dengan operasi logika AND

Alamat IP	10000011	01101011	10100100	00011010	(131.107.164.026)
Subnet Mask	11111111	11111111	1111 0000	00000000	(255.255.240.000)
----- AND					
Network ID	10000011	01101011	1010 0000	00000000	(131.107.160.000)
Broadcast	10000011	01101011	1010 1111	11111111	(131.107.175.255)

↓

Perhitungan IP Subnet

Prefix	Subnet Mask	Jumlah IP	Jumlah Host (Jml IP - 2)
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2
/31	255.255.255.252	2	-
/32	255.255.255.252	1	-

Perhitungan Subnet

Rumus menghitung Jumlah IP address dalam subnetmask:

$$2^{(32-n)}, \text{ dimana } n=\text{prefix subnet}$$

Contoh, IP kelas C: 20.20.20.20/30,

Tentukan Range IP, IP Host , Network ID, Broadcast dan Subnet Masknya:

- Jumlah IP dalam subnet:

Gunakan Rumus $2^{(32-30)} = 2^2 = 4$

- Range IP

Range IP dicari berdasarkan kelipatan Jumlah IPnya (kelipatan 4):

20.20.20.0 s/d 20.20.20.3

20.20.20.4 s/d 20.20.20.7, (8-11),(12-15)...terus sampai (252-255)

IP address pada soal (20.20.20.20) ada pada range:

20.20.20.20 s/d 20.20.20.23

Perhitungan Subnet

IP kelas C: 20.20.20.20/30,

Tentukan Range IP, IP Host , Network ID, Broadcast dan Subnet Masknya :

- Network ID dan Broadcast:

Dari range IP yang telah ditemukan (20.20.20.20 s/d 20.20.20.23)

IP terkecil digunakan untuk network ID, terbesar untuk Broadcast

Network ID → 20.20.20.20, Broadcast → 20.20.20.23

- IP Host → Range IP dikurangi Network ID dan broadcast

IP host → 20.20.20.21 s/d 20.20.20.22

Jumlah IP host → jumlah IP dalam subnet dikurangi dua

- Subnet mask → 255.255.255.(256 – jumlah IP)

Subnet mask → 255.255.255.252

Kerjakan Soal Berikut

Tentukan jumlah IP, network id & broadcast, IP Host, dan subnet mask dari IP address berikut:

1. 11.11.11.11/26
2. 22.22.22.22/28
3. 33.33.33.33/25
4. 44.44.44.44/29
5. 55.55.55.55/27
6. 66.66.66.66/28
7. 77.77.77.77/30
8. 88.88.88.88/31
9. 99.99.99.99/25
10. 100.100.100.100/27
11. 111.111.111.111/30
12. 122.122.122.122/25
13. 133.133.133.133/28
14. 144.144.144.144/24
15. 155.155.155.155/26
16. 166.166.166.166/29

IP Address Kelas B

IP address 12.12.12.12/**22**, Tentukan Range IP, IP Host , Network ID, Broadcast dan Subnet Masknya :

- Translate prefix netmask menjadi kelas C dengan ditambah 8, menjadi (**22**+8)=30
- Jumlah IP prefix /30 dalam kelas C adalah $2^{(32-30)} = 4$
- Jumlah IP dalam kelas B = $4 \times 256 = 1024$

Range IP Address

- Jumlah IP kelas C nya, yaitu 4, Range IP diimplementasikan pada oktet ke 3
 12.12.**0**.0 – 12.12.**3**.255, **4 – 7**, **8 – 11**, **12 -15**, dan seterusnya
- Range IP → 12.12.**12**.0 s/d 12.12.**15**.255
- Network ID → 12.12.**12**.0, broadcast 12.12.**15**.255
- Jumlah host yg dapat digunakan → 12.12.**12**.1 – 12.12.**15**.254
- Netmask = $255.255.(256-4).0 = 255.255.**252**.0$

Kerjakan Soal Berikut

1. 11.11.11.11/23
2. 22.22.22.22/21
3. 33.33.33.33/20
4. 44.44.44.44/22
5. 55.55.55.55/18

Contoh Soal

1. IP Host A 192.168.1.34/25 dan IP Host B 192.168.1.129/24, bisakah antara Host A dan Host B berkomunikasi?

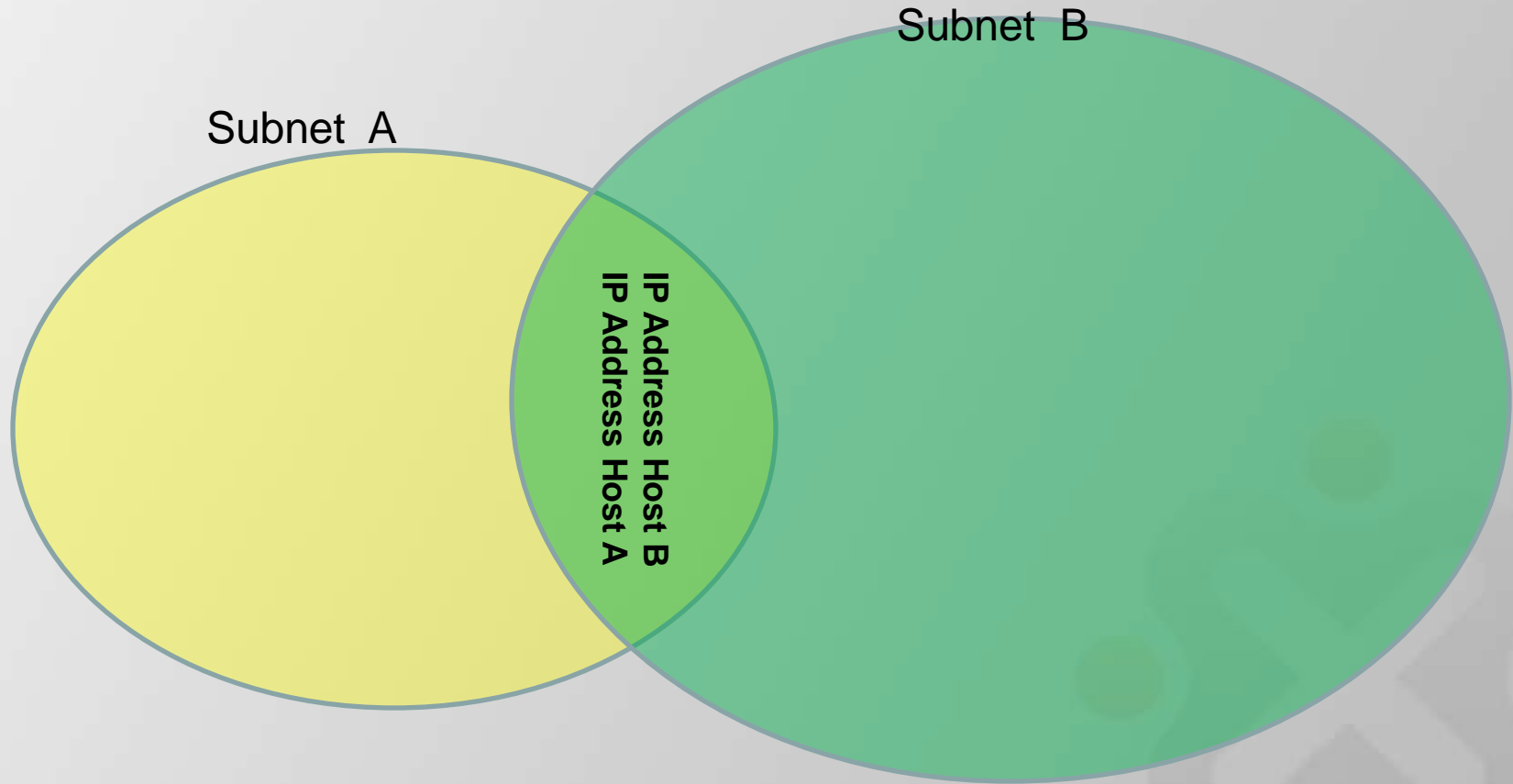
Jawab:

Range subnet A = 192.168.1.0 – 192.168.1.127 | Host B 192.168.1.129

Range subnet B = 192.168.1.0 – 192.168.1.255 | Host A 192.168.1.34

IP host B **tidak termasuk** pada range subnet A, Host A dan Host B tidak dapat berkomunikasi

Koneksi Beda Subnet



IP Privat

- Berdasarkan jenisnya IP address dibedakan menjadi **IP Public** dan **IP Private**.
- IP Public adalah IP address yang digunakan untuk koneksi jaringan **global (internet)** secara langsung dan bersifat unik.
- IP Private digunakan untuk **jaringan lokal (LAN)**
- Alokasi IP Privat adalah sbb:

RFC1918 name	IP address range	number of addresses
24-bit block	10.0.0.0 – 10.255.255.255	16,777,216
20-bit block	172.16.0.0 – 172.31.255.255	1,048,576
16-bit block	192.168.0.0 – 192.168.255.255	65,536

IP Bogon

- IP Bogon adalah IP yang tidak dapat dipakai karena tidak diatur dalam aturan organisasi internet.
- IP bogon biasanya muncul karena kesalahan konfigurasi yang tidak disengaja atau sengaja untuk tujuan tertentu
- Contoh IP bogon : 0.0.0.0/8, 10.0.0.0/8, 127.0.0.0/8, 169.254.0.0/16, 172.16.0.0/12, 192.0.0.0/24, 192.0.2.0/24, 192.168.0.0/16, 198.18.0.0/15, 198.51.100.0/24, 203.0.113.0/24, 224.0.0.0/4, dsb
- Bogons dapat difilter menggunakan ACLs atau BGP blackholing.
- IP bisa digolongkan IP bogon untuk saat ini, namun bisa jadi kedepanya bukan merupakan IP bogon lagi jika ditetapkan oleh organisasi internet internasional (IANA).

Protocol

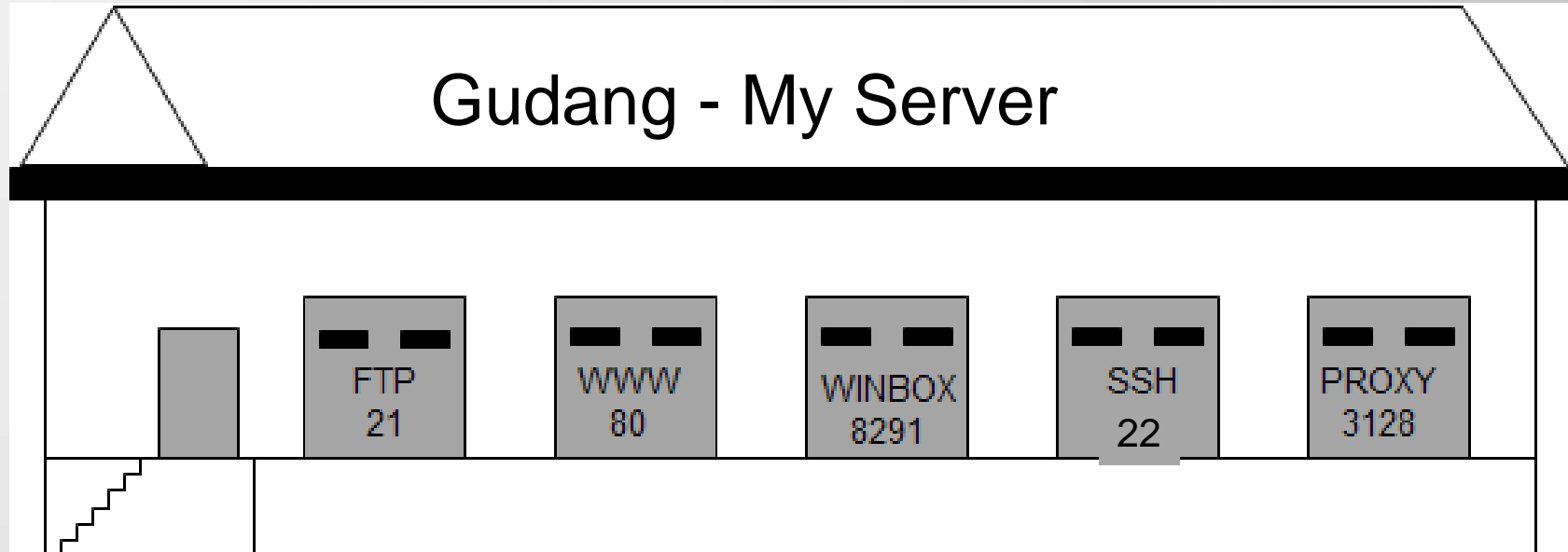
- Protocol menentukan prosedur pengiriman data.
- Protocol yang sering digunakan:
 - Transmission Control Protocol (TCP)
 - User Datagram Protocol (UDP) → DNS
 - Internet Control Message Protocol (ICMP) → ping traceroute
 - Hypertext Transfer Protocol (HTTP) → web
 - Post Office Protocol (POP3) → email
 - File Transfer Protocol (FTP)
 - Internet Message Access Protocol (IMAP) → email
 - dll

Port

- Port adalah sebuah aplikasi-spesifik atau proses software spesifik pada Komputer/host yang **menjalankan servise** untuk komunikasi jaringan.
- Sebuah port dikaitkan dengan alamat IP dari host, serta jenis protokol yang digunakan untuk komunikasi.
- Port diberi penomoran sebagai berikut:
 1. Dari 0 s/d 1023 (*well-known ports*),
 2. Dari 1024 s/d 49151 (*registered port*),
 3. Dari 49152 s/d 65535 (*unregistered / dynamic, private or ephemeral ports*)

-End of TCP/IP Modul-

Port



Port yang Biasa Digunakan

Port No	Protocol	Service	Remark
21	TCP	FTP	File Transfer Protocol
23	TCP	Telnet	Remote access
25	TCP	SMTP	Simple Mail Transfer Protocol
53	UDP	DNS	Domain Name Server
80	TCP	HTTP	Hypertext Transfer Protocol
110	TCP	POP3	Post Office Protocol v3
123	UDP	NTP	Network Time Protocol
137	TCP	NetBIOS-ns	NetBIOS – Name Service
161	TCP	SNMP	Simple Network Monitoring Protocol
3128	TCP	HTTP - Proxy	Web-Cache (default by Squid)
8080	TCP	HTTP - Proxy	Web-Cache (customized)

Modul 1

Mengkases MikroTik RouterOS



Akses ke MikroTik RouterOS

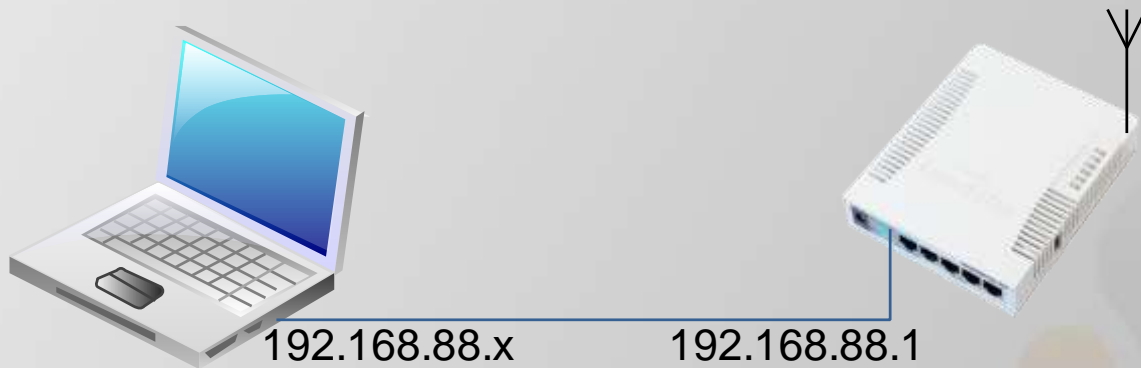
Akses Via	Koneksi	Text Base	GUI	Need IP
Keyboard	Langsung di PC	yes		
Serial Console	Konektor Kabel Serial	yes		
Telnet & SSH	Layer 3	yes		yes
Winbox	Menggunakan OS Windows	yes	yes	
FTP	Layer 3	yes		yes
API	Socket Programing			yes
Web (HTTP)	Layer 3		yes	yes
MAC-Telnet	Layer 2	yes		

Winbox

- Cara paling mudah dalam mengakses dan mengkonfigurasi MikroTik adalah menggunakan winbox.
- Winbox dapat didapatkan dari:
 - Web www.mikrotik.com
 - Via http/web IP atau domain Router MikroTik
 - Copy dari media penyimpanan

Default Setting RouterBoard

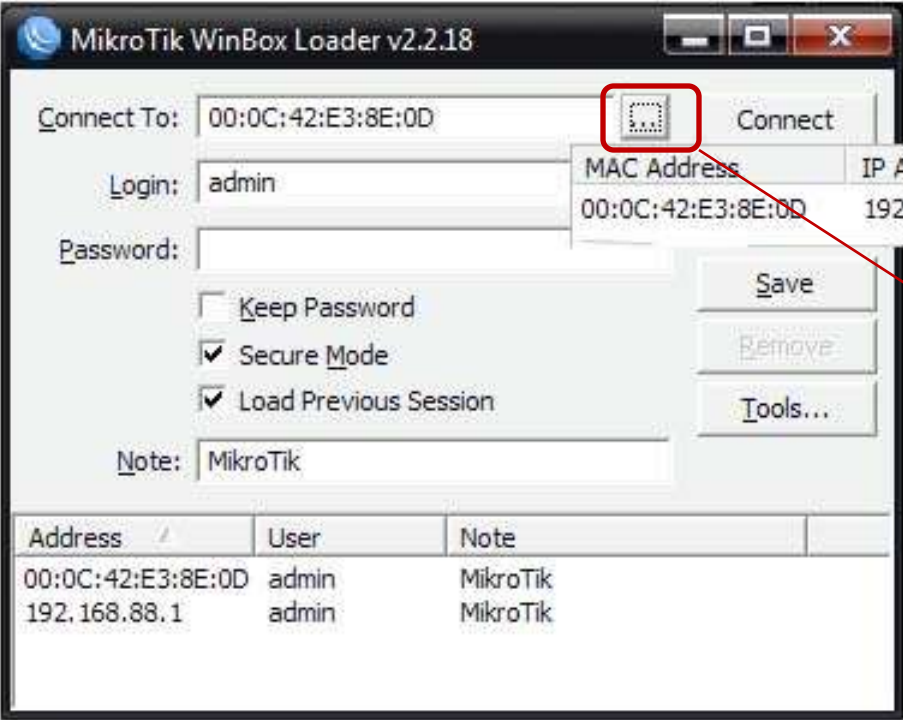
- RouterBoard (RB) baru, atau setelah di reset default , memiliki default konfigurasi:
 - IP Address Ether 1 : 192.168.88.1/24
 - Username “admin” password blank.
- Untuk meremote, Laptop/PC dihubungkan dengan ether1 dan diset dengan IP 192.168.88.xxx/24.



LAB – Konek Router

- Ubah IP Komputer anda menjadi:
 - IP Address 192.168.88.x
 - Netmask 255.255.255.0
- Ping ke RouterBOARD (192.168.88.1)
- Buka URL RouterBOARD (<http://192.168.88.1>)
- Download winbox dari halaman tersebut.

Winbox Login



MAC Address

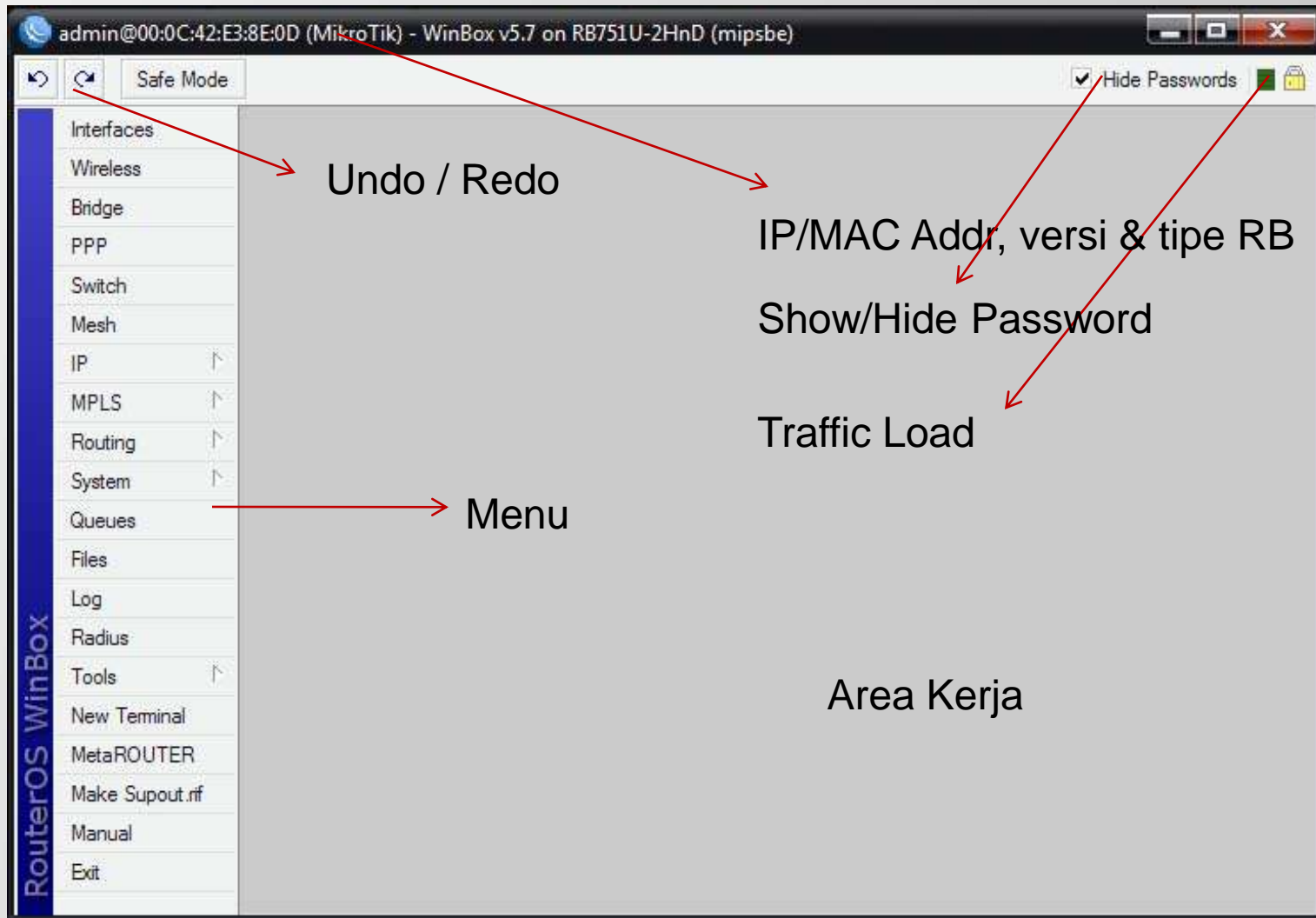
MAC Address	IP Address	Identity	Version	Board ...
00:0C:42:E3:8E:0D	192.168.88.1	MikroTik	5.7	RB751...

Network Discovery

Address	User	Note
00:0C:42:E3:8E:0D	admin	MikroTik
192.168.88.1	admin	MikroTik

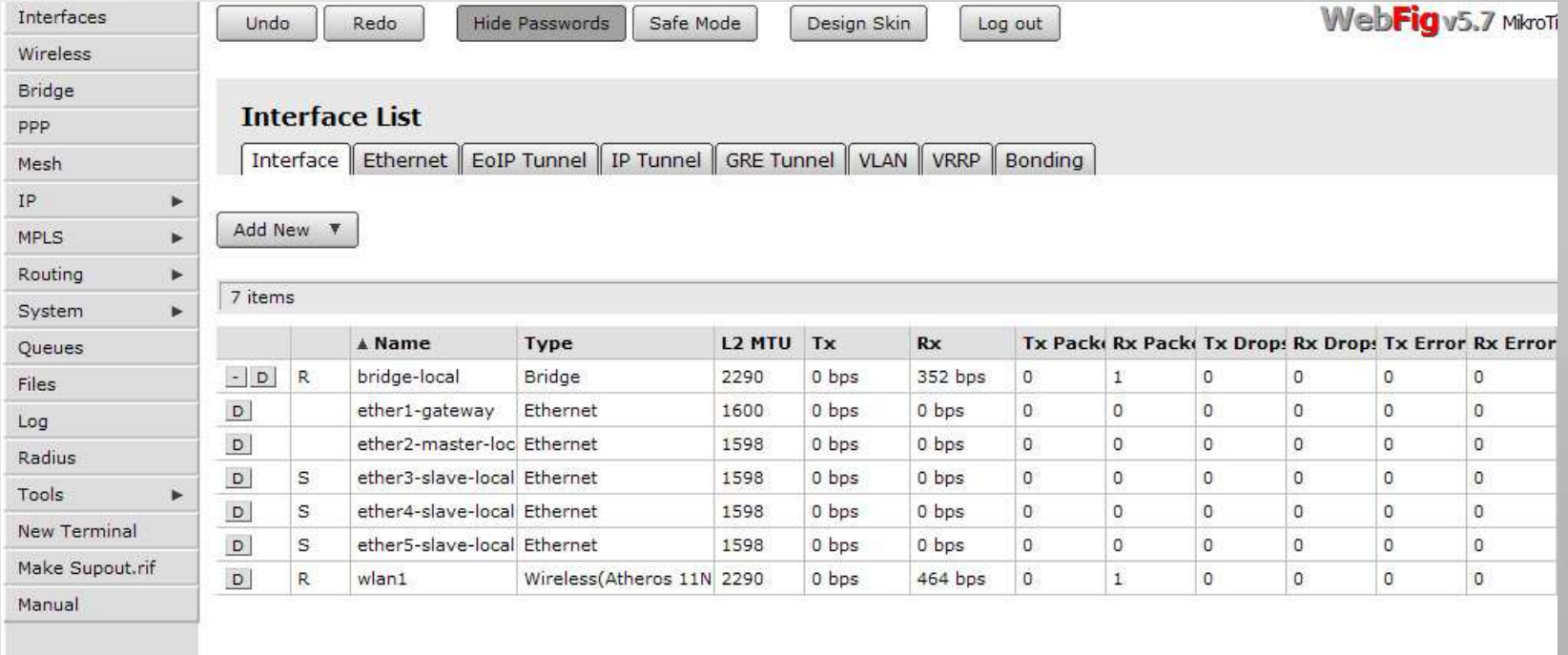
Winbox digunakan untuk mengkonfigurasi MikroTik Router secara mudah

Tampilan MikroTik – pada Winbox



WebFig

- Sejak versi 5.0, interface via web diperkenalkan, dengan fungsi-fungsi yang sama dengan Winbox.
- Coba akses webfig mikrotik router anda dengan browser.



WebFig v5.7 Mikrotik

Interface List

Interface Ethernet EoIP Tunnel IP Tunnel GRE Tunnel VLAN VRRP Bonding

Add New ▼

7 items

		▲ Name	Type	L2 MTU	Tx	Rx	Tx Pack	Rx Pack	Tx Drop	Rx Drop	Tx Error	Rx Error
-	D	R	bridge-local	Bridge	2290	0 bps	352 bps	0	1	0	0	0
D			ether1-gateway	Ethernet	1600	0 bps	0 bps	0	0	0	0	0
D			ether2-master-local	Ethernet	1598	0 bps	0 bps	0	0	0	0	0
D	S		ether3-slave-local	Ethernet	1598	0 bps	0 bps	0	0	0	0	0
D	S		ether4-slave-local	Ethernet	1598	0 bps	0 bps	0	0	0	0	0
D	S		ether5-slave-local	Ethernet	1598	0 bps	0 bps	0	0	0	0	0
D	R		wlan1	Wireless(Atheros 11N	2290	0 bps	464 bps	0	1	0	0	0

Konfigurasi Via Terminal

- Dalam kondisi tertentu remote dan konfigurasi via GUI tidak memungkinkan dikarenakan hal-hal seperti; keterbatasan bandwidth, kebutuhan untuk running script, remote via ..x console, dll.
- Remote & konfigurasi terminal bisa dilakukan dengan cara:
 - Telnet (via IP port 23, non secure connection)
 - SSH (via IP Port 22, lebih secure dari telnet)
 - Serial console (kabel serial)

LAB-Telnet & SSH

- Gunakan MsDOS prompt (telnet), atau program SSH/Telnet client lainnya, seperti putty, winSCP untuk remote mikrotik.



IP MikroTik dan Port

Serial Console

- Serial Console digunakan apabila kita lupa/salah telah mendisable semua interface pada MikroTik.
- Serial Console dibutuhkan juga saat kita menggunakan Netinstall.
- Remote via serial console membutuhkan kabel DB-9 (atau converter USB ke DB-9).
- Menggunakan program HyperTerminal.
- Baud rate 115200, Data bits 8, Parity None, Stop bits 1, dan Flow Control None.

Versi dan Lisensi Mikrotik



Lisensi MikroTik

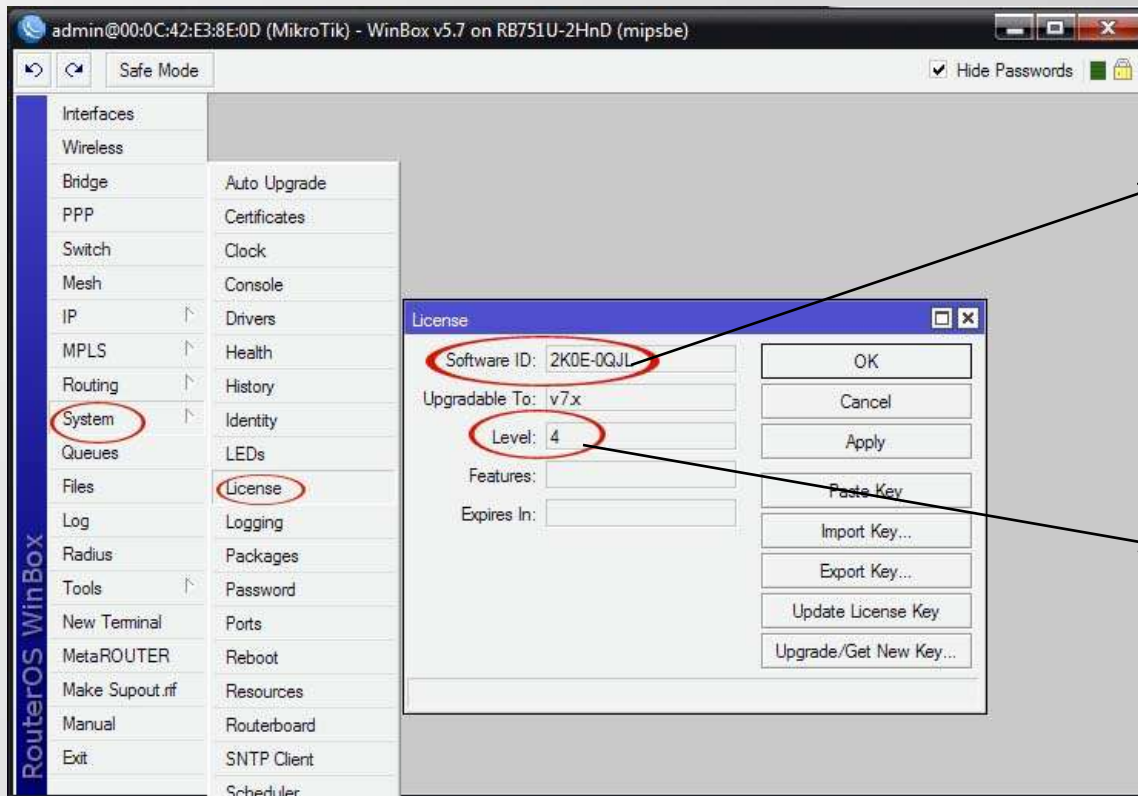
- Fitur-fitur RouterOS ditentukan oleh level lisensi yang melekat pada perangkat.
- Level dari lisensi juga menentukan batasan upgrade packet.
- Lisensi melekat pada storage/media penyimpanan (ex. Hardisk, NAND, USB, Compact Flash).
- Bila media penyimpanan diformat dengan non MikroTik, maka lisensi akan hilang.

Level Lisensi MikroTik

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 v6.x	ROS v6.x	ROS v7.x	ROS v7.x
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h trial	-	yes(*)	yes	yes	yes
EoIP tunnels	24h trial	1	unlimited	unlimited	unlimited	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
VLAN interfaces	24h trial	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h trial	1	1	200	500	unlimited
RADIUS client	24h trial	-	yes	yes	yes	yes
Queues	24h trial	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h trial	-	yes	yes	yes	yes
User manager active sessions	24h trial	1	10	20	50	Unlimited
Number of KVM guests	none	1	Unlimited	Unlimited	Unlimited	Unlimited

Lisensi dan Batasan Upgrade Versi

- Lisensi menentukan versi berapa dari MikroTikOS yang dapat diinstall/diupgrade di suatu hardware.
- L1 dan 2 mengizinkan upgrade 1 versi, L5 dan L6 mengizinkan upgrade sampai 2 versi.



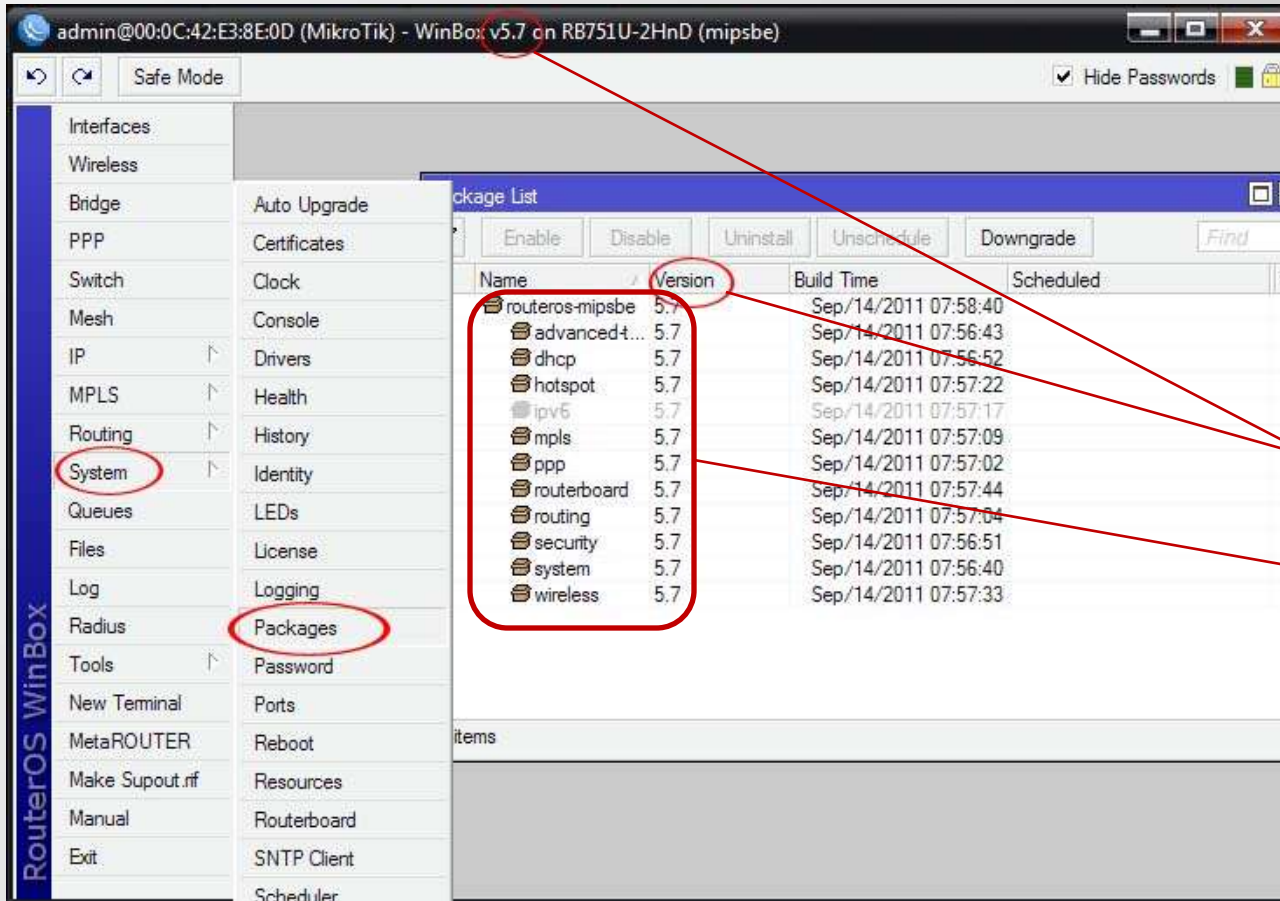
Software ID => unik hardware ID untuk saat membeli lisensi

RouterOS ini diinstall pada Level 4, versi 5,7, sehingga dapat diupgrade sampai dengan versi 7.x

Versi MikroTik

- Fitur-fitur MikroTik selain ditentukan oleh lisensi yang digunakan, juga ditentukan oleh versi dari MikroTik yang terinstall.
- Pada RouterOS, versi MikroTik dapat dilihat dari paket yang terinstall.
- Paket yang terinstall menunjukkan fitur apa saja yang didukung oleh RouterOS.

Melihat Versi MikroTik



admin@00:0C:42:E3:8E:0D (MikroTik) - WinBox v5.7 on RB751U-2HnD (mipsbe)

Safe Mode

Hide Passwords

RouterOS WinBox

System

Packages

Package List

Name	Version	Build Time	Scheduled
routeros-mipsbe	5.7	Sep/14/2011 07:58:40	
advancedt...	5.7	Sep/14/2011 07:56:43	
dhcp	5.7	Sep/14/2011 07:56:52	
hotspot	5.7	Sep/14/2011 07:57:22	
ipv6	5.7	Sep/14/2011 07:57:17	
mpls	5.7	Sep/14/2011 07:57:09	
ppp	5.7	Sep/14/2011 07:57:02	
routerboard	5.7	Sep/14/2011 07:57:44	
routing	5.7	Sep/14/2011 07:57:04	
security	5.7	Sep/14/2011 07:56:51	
system	5.7	Sep/14/2011 07:56:40	
wireless	5.7	Sep/14/2011 07:57:33	

Versi MikroTik

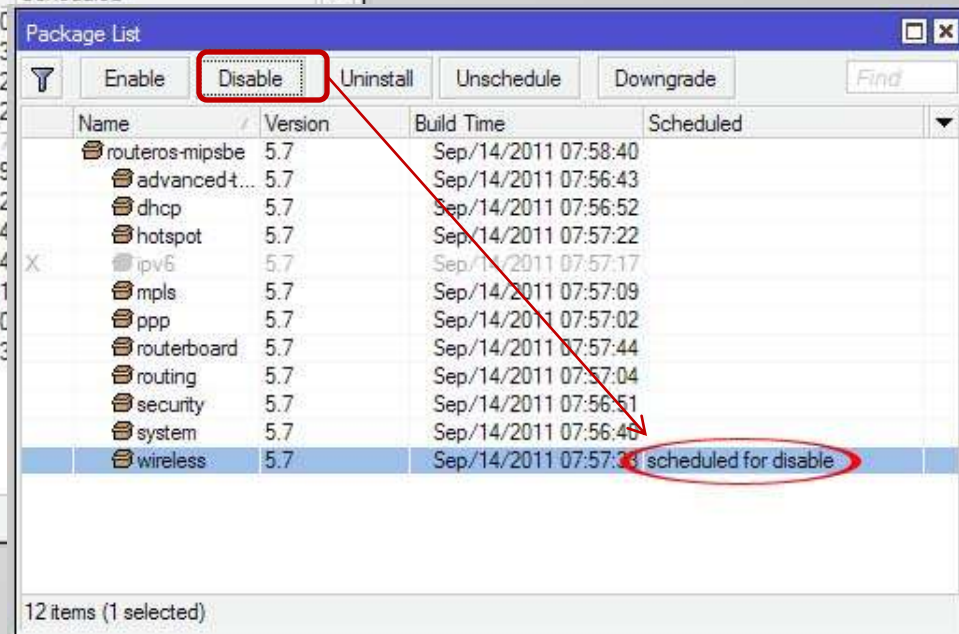
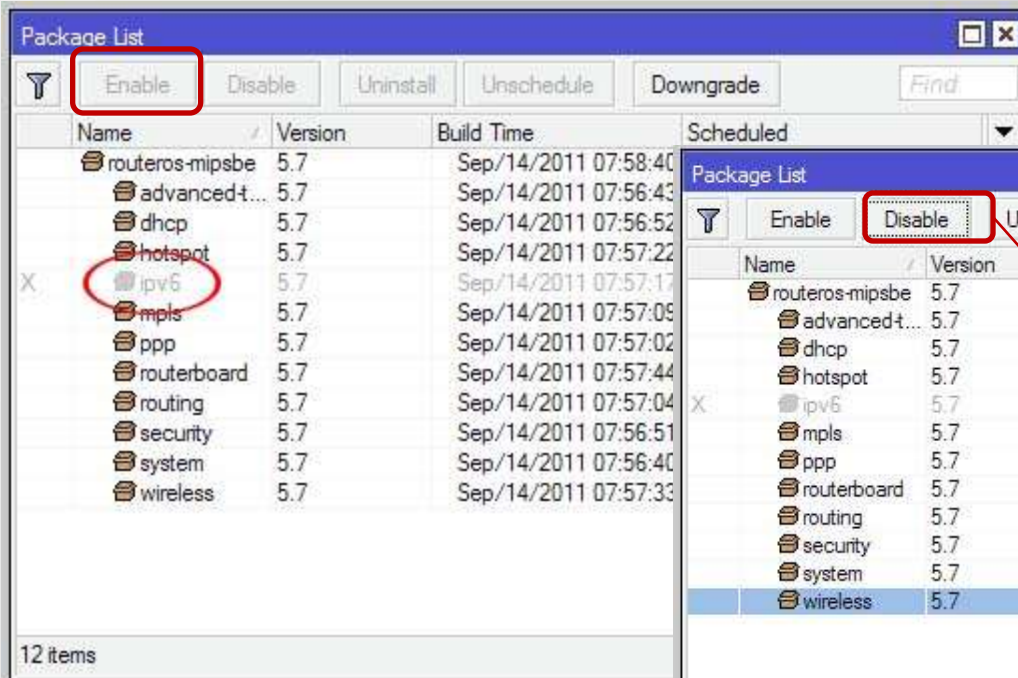
Paket

Paket – Fitur Paket

Package	Features
advanced-tools (<i>mipsle, mipsbe, ppc, x86</i>)	advanced ping tools. netwatch, ip-scan, sms tool, wake-on-LAN
calea (<i>mipsle, mipsbe, ppc, x86</i>)	data gathering tool for specific use due to "Communications Assistance for Law Enforcement Act" in USA
dhcp (<i>mipsle, mipsbe, ppc, x86</i>)	Dynamic Host Control Protocol client and server
gps (<i>mipsle, mipsbe, ppc, x86</i>)	Global Positioning System devices support
hotspot (<i>mipsle, mipsbe, ppc, x86</i>)	HotSpot user management
ipv6 (<i>mipsle, mipsbe, ppc, x86</i>)	IPv6 addressing support
mpls (<i>mipsle, mipsbe, ppc, x86</i>)	Multi Protocol Labels Switching support
multicast (<i>mipsle, mipsbe, ppc, x86</i>)	Protocol Independent Multicast - Sparse Mode ; Internet Group Managing Protocol - Proxy
ntp (<i>mipsle, mipsbe, ppc, x86</i>)	Network protocol client and service
ppp (<i>mipsle, mipsbe, ppc, x86</i>)	MIPPP client, PPP, PPTP, L2TP, PPPoE, ISDN PPP clients and servers
routerboard (<i>mipsle, mipsbe, ppc, x86</i>)	accessing and managing RouterBOOT. RouterBOARD specific information.
routing (<i>mipsle, mipsbe, ppc, x86</i>)	dynamic routing protocols like RIP , BGP , OSPF and routing utilities like BFD , filters for routes .
security (<i>mipsle, mipsbe, ppc, x86</i>)	IPSEC, SSH, Secure WinBox
system (<i>mipsle, mipsbe, ppc, x86</i>)	basic router features like <i>static routing, ip addresses, sNTP, telnet, API, queues, firewall, web proxy, DNS cache, TFTP, IP pool, SNMP, packet sniffer, e-mail send tool, graphing, bandwidth-test, torch, EoIP, IPIP, bridging, VLAN, VRRP</i> etc.). Also, for RouterBOARD platform - MetaROUTER Virtualization
ups (<i>mipsle, mipsbe, ppc, x86</i>)	APC ups
user-manager (<i>mipsle, mipsbe, ppc, x86</i>)	MikroTik User Manager
wireless (<i>mipsle, mipsbe, ppc, x86</i>)	wireless interface support

Paket – Enable/Disable

- Mengaktifkan / Menonaktifkan sebuah paket



Paket – Uninstall

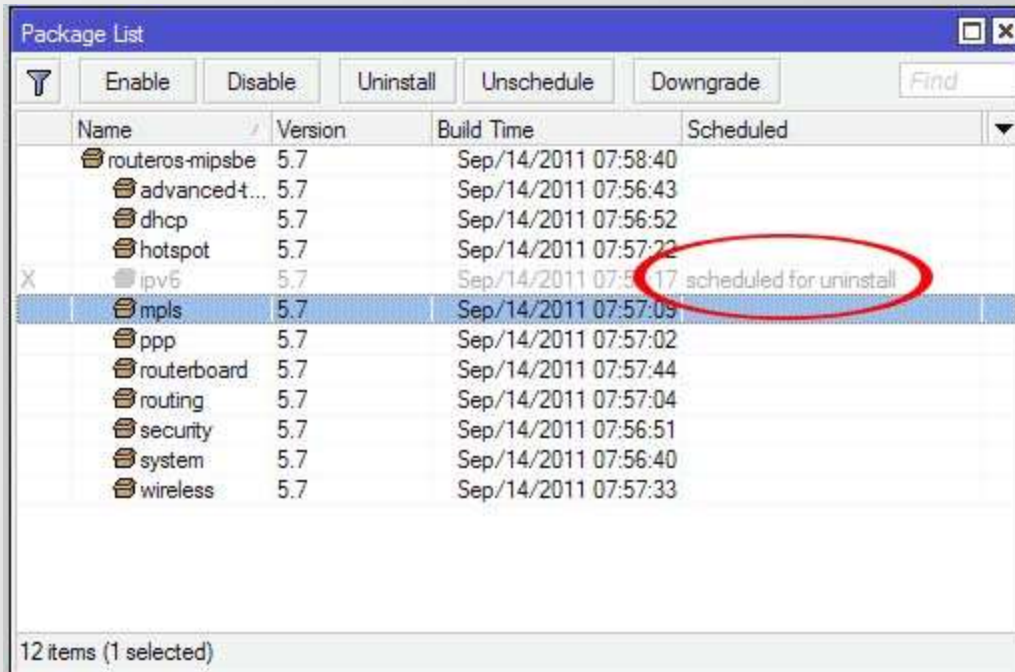
Package List

Name	Version	Build Time	Scheduled
routeros-mipsbe	5.7	Sep/14/2011 07:58:40	
advanced-t...	5.7	Sep/14/2011 07:56:43	
dhcp	5.7	Sep/14/2011 07:56:52	
hotspot	5.7	Sep/14/2011 07:57:22	
X ipv6	5.7	Sep/14/2011 07:57:17	scheduled for uninstall
mpls	5.7	Sep/14/2011 07:57:09	
ppp	5.7	Sep/14/2011 07:57:02	
routerboard	5.7	Sep/14/2011 07:57:44	
routing	5.7	Sep/14/2011 07:57:04	
security	5.7	Sep/14/2011 07:56:51	
system	5.7	Sep/14/2011 07:56:40	
wireless	5.7	Sep/14/2011 07:57:33	

12 items (1 selected)

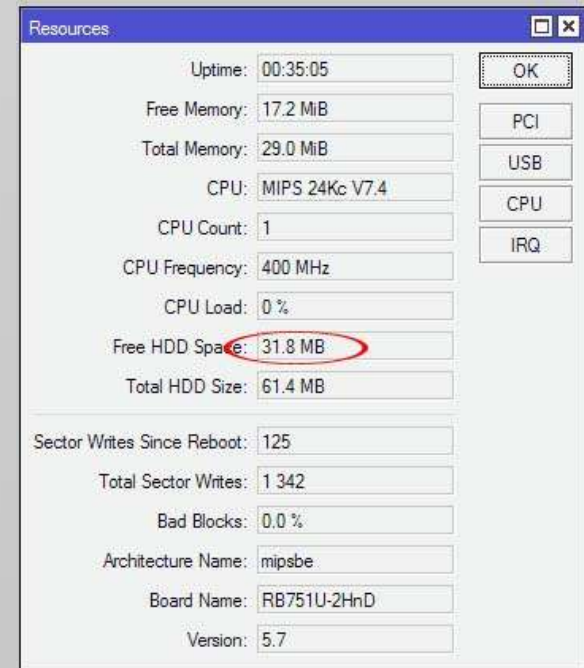
LAB- Paket

- Disable, Enable, Uninstall paket IPv6.
- Perhatikan juga kapasitas NAND sebelum dan setelah uninstall.
- Perintah-perintah tersebut tidak akan dieksekusi sebelum router direboot.



Name	Version	Build Time	Scheduled
routeros-mipsbe	5.7	Sep/14/2011 07:58:40	
advanced-t...	5.7	Sep/14/2011 07:56:43	
dhcp	5.7	Sep/14/2011 07:56:52	
hotspot	5.7	Sep/14/2011 07:57:22	
ipv6	5.7	Sep/14/2011 07:57:17	scheduled for uninstall
mpls	5.7	Sep/14/2011 07:57:05	
ppp	5.7	Sep/14/2011 07:57:02	
routerboard	5.7	Sep/14/2011 07:57:44	
routing	5.7	Sep/14/2011 07:57:04	
security	5.7	Sep/14/2011 07:56:51	
system	5.7	Sep/14/2011 07:56:40	
wireless	5.7	Sep/14/2011 07:57:33	

12 items (1 selected)



Uptime:	00:35:05	OK
Free Memory:	17.2 MiB	PCI
Total Memory:	29.0 MiB	USB
CPU:	MIPS 24Kc V7.4	CPU
CPU Count:	1	IRQ
CPU Frequency:	400 MHz	
CPU Load:	0 %	
Free HDD Space:	31.8 MB	
Total HDD Size:	61.4 MB	
Sector Writes Since Reboot:	125	
Total Sector Writes:	1 342	
Bad Blocks:	0.0 %	
Architecture Name:	mipsbe	
Board Name:	RB751U-2HnD	
Version:	5.7	

Paket – Upgrade / Downgrade










- Usahakan selalu upgrade versi terbaru, untuk fix bugs, new feature dll.
- Downgrade dilakukan apabila hardware kurang mendukung terhadap versi baru atau terdapat bug pada versi aktifnya.
- Upgrade paket harus memperhatikan aturan level dan lisensi yang berlaku.
- Upgrade dan downgrade juga harus memperhatikan kompatibilitas terhadap jenis arsitektur hardware.

LAB – Upgrade / Downgrade

- Pemilihan paket sangat penting dalam melakukan upgrade / downgrade, **jenis & arsitektur hardware** memiliki software yang berbeda.
- Bila ragu, dapat di crosscek dan didownload di www.mikrotik.com/download.html

Product	Devices	Mirror
RouterOS ▾	RB700 series ▾	USA (MikroTik USA) ▾

Please select appropriate device type before downloading your version.

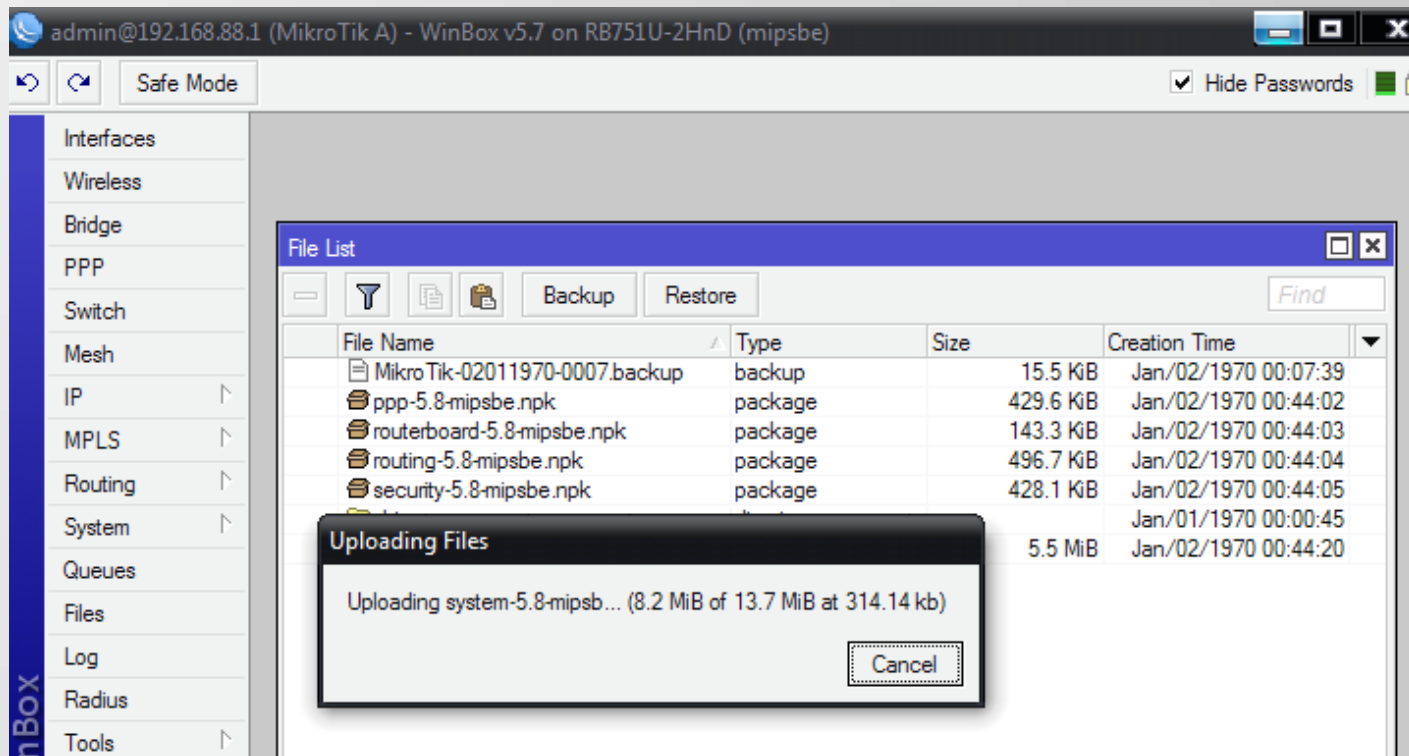
	Version 5.8 (Stable)	 Torrent	 NPK file	 ZIP file	 Netinstall	Changelog MD5
	Version 4.17 (Legacy)	 Torrent	 NPK file	 ZIP file	 Netinstall	Changelog MD5

LAB – Mengupload Paket

- Paket yang akan diinstall (versi lama/baru) harus diupload terlebih dahulu ke router pada bagian file.
- Upload dapat dilakukan dengan **drag-and drop** (via winbox), ataupun via FTP client.
- Upload paket tidak dapat digunakan via drag-and-drop winbox apabila koneksi menggunakan **MAC address**, karena menggunakan koneksi FTP.
- Untuk mengeksekusi upgrade, router harus direboot.

LAB – Mengupload Paket Baru

- Upgrade router anda ke versi terbaru.
- Pastikan winbox menggunakan koneksi via IP.



- Reboot setelah selesai upload, dan lihat hasilnya.

LAB – Mengupload Paket Baru

Cek log untuk melihat apabila ada error

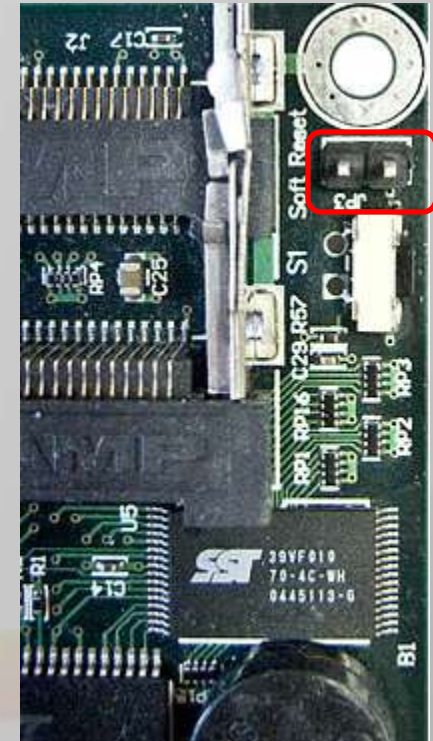
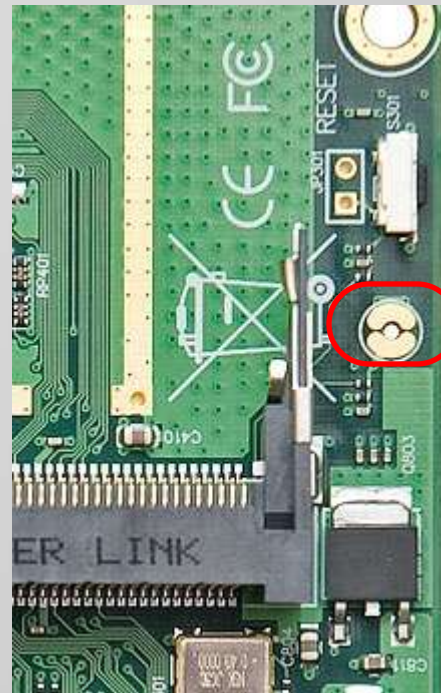
Log		
		all
Jan/02/1970 00:00:12	system info	verified ntp-5.9-mipsbe.npk
Jan/02/1970 00:00:13	system error	can not install ntp-5.9: system-5.9 is not installed, but is required
Jan/02/1970 00:00:14	system info	router rebooted
Jan/02/1970 00:00:19	wireless info	00:0C:42:E3:8E:11@wlan1 established connection on 2422, SSID Mikrotik A
Jan/02/1970 00:00:19	dhcp info	dhcp-client on wlan1 got IP address 192.168.1.254
Jan/02/1970 00:00:19	system info	SNTP client configuration changed

Reset Konfigurasi

- Reset konfigurasi MikroTik diperlukan jika:
 - Saat lupa username dan atau password
 - Saat konfigurasi terlalu komplek dan perlu ditata dari nol.
- Reset konfigurasi dapat dilakukan dengan cara:
 - Hard Reset, reset secara fisik.
 - Soft reset, reset secara software.
 - Install ulang.

Hard Reset

- Khusus RouterBoard memiliki rangkaian untuk reset pada board dengan cara menjumper sambil menyalakan RB, RB akan kembali ke konfigurasi awal/default.



Soft Reset

- Apabila anda masih bisa masuk kedalam system MikroTik, soft reset dapat dilakukan dengan perintah:

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

Install Ulang

- Install ulang router dapat mengembalikan ke posisi awal/default.
- Install dapat dilakukan menggunakan media CD dan software Netinstall.
- RouterBOARD hanya dapat diinstall ulang menggunakan software Netinstall.

Install Ulang via Netinstall

- Untuk melakukan instalasi menggunakan Netinstall, RB harus disetting agar booting dari jaringan (ether), dengan cara:
 - Setting via serial console
 - Setting via terminal console
 - Winbox
 - Tombol reset

Setting BIOS via Serial Console

- Untuk mengakses konfigurasi BIOS, akan ada tampilan untuk masuk dalam setup yaitu *“Press any key within 2 seconds to enter setup”*

```
What do you want to configure?
```

```
d - boot delay
k - boot key
s - serial console
l - debug level
o - boot device
b - beep on boot
v - vga to serial
t - ata translation
p - memory settings
m - memory test
u - cpu mode
f - pci back-off
r - reset configuration
g - bios upgrade through serial port
c - bios license information
x - exit setup
```

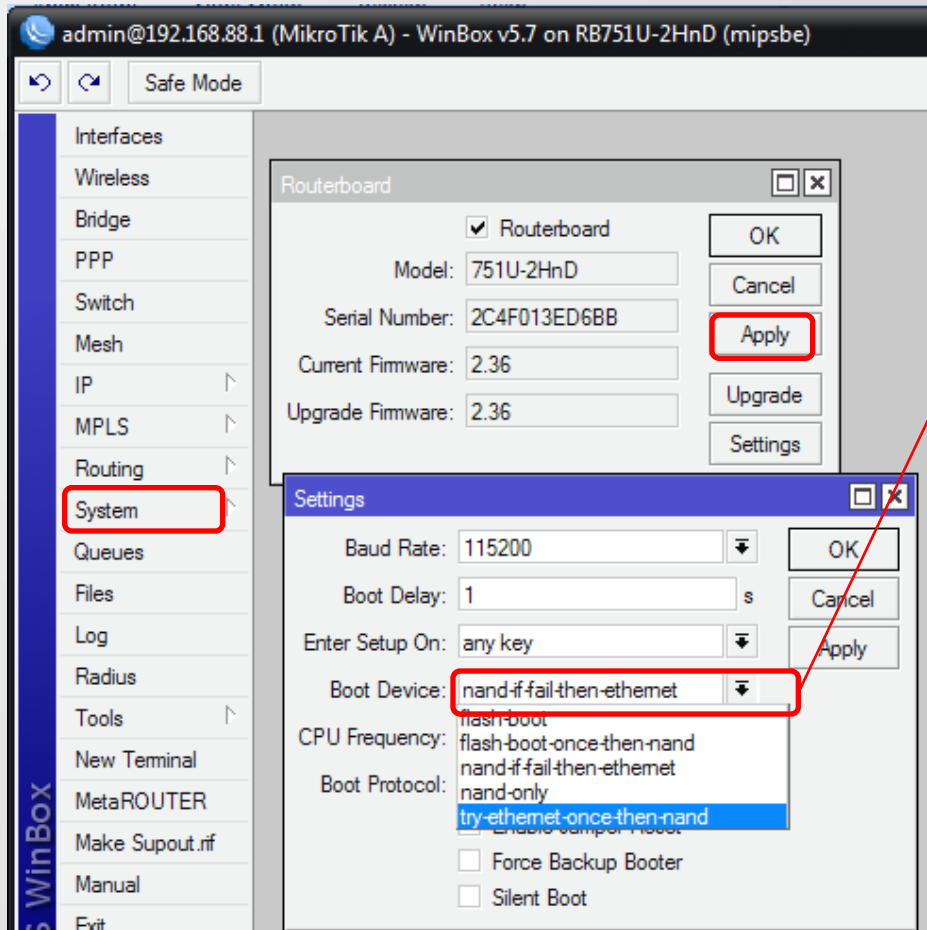
```
Select boot device:
```

```
* i - IDE
e - Etherboot
1 - Etherboot (timeout 15s), IDE
2 - Etherboot (timeout 1m), IDE
3 - Etherboot (timeout 5m), IDE
4 - Etherboot (timeout 30m), IDE
5 - IDE, try Etherboot first on next boot (15s)
6 - IDE, try Etherboot first on next boot (1m)
7 - IDE, try Etherboot first on next boot (5m)
8 - IDE, try Etherboot first on next boot (30m)
```

Router akan boot via Ethernet

Setting BIOS via winbox

Setting boot device MikroTik ada di menu System>Routerboard>Setting>Boot Device



Try-ethemet-once-then-nand

NetInstall

- Merupakan software yang running under windows.
- Digunakan untuk install awal dan install ulang RouterOS
- Digunakan untuk reset password apabila kita lupa.
- PC/Laptop yang menjalankan netinstall harus terhubung langsung dengan router melalui kabel UTP atau LAN.
- Software netinstall dapat didownload di web resmi MikroTik.

LAB – Reinstall RB 751 (optional)

- Download RouterOS dan Software Netinstall terbaru di <http://www.mikrotik.com/download.html>
- Pilih device untuk RB700 series

Product

RouterOS ▾

Devices

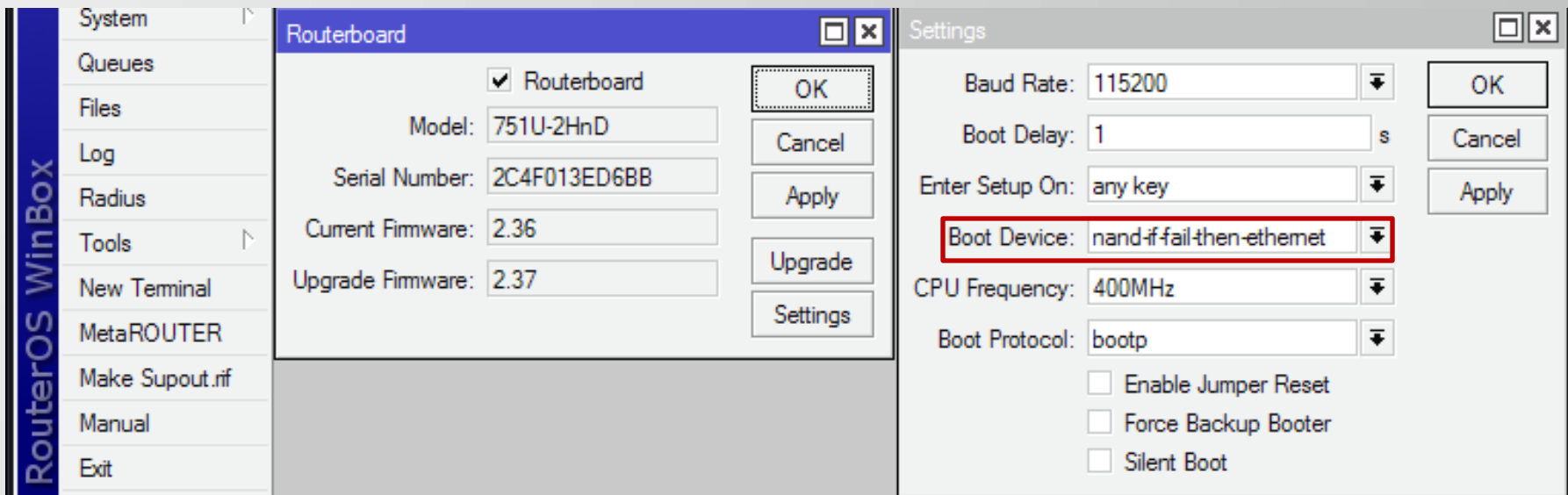
RB700 series ▾

Please select appropriate device type before downloading your version.

	Version 5.14 (Stable)	 Torrent	 NPK file	 ZIP file	 Netinstall	Changelog MD5
	Version 4.17 (Legacy)	 Torrent	 NPK file	 ZIP file	 Netinstall	Changelog MD5

LAB – Reinstall RB 751

- Pastikan Laptop sudah terkoneksi ke RB 751 melalui port ether1 dan dapat saling ping.
- Ubah boot device RB751 ke try-ethernet-once-then-nand

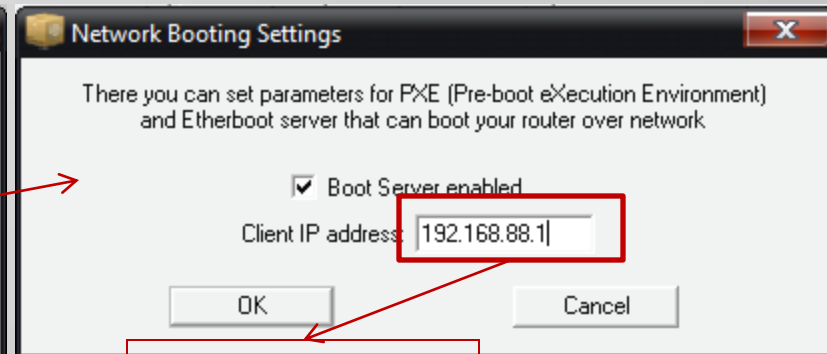
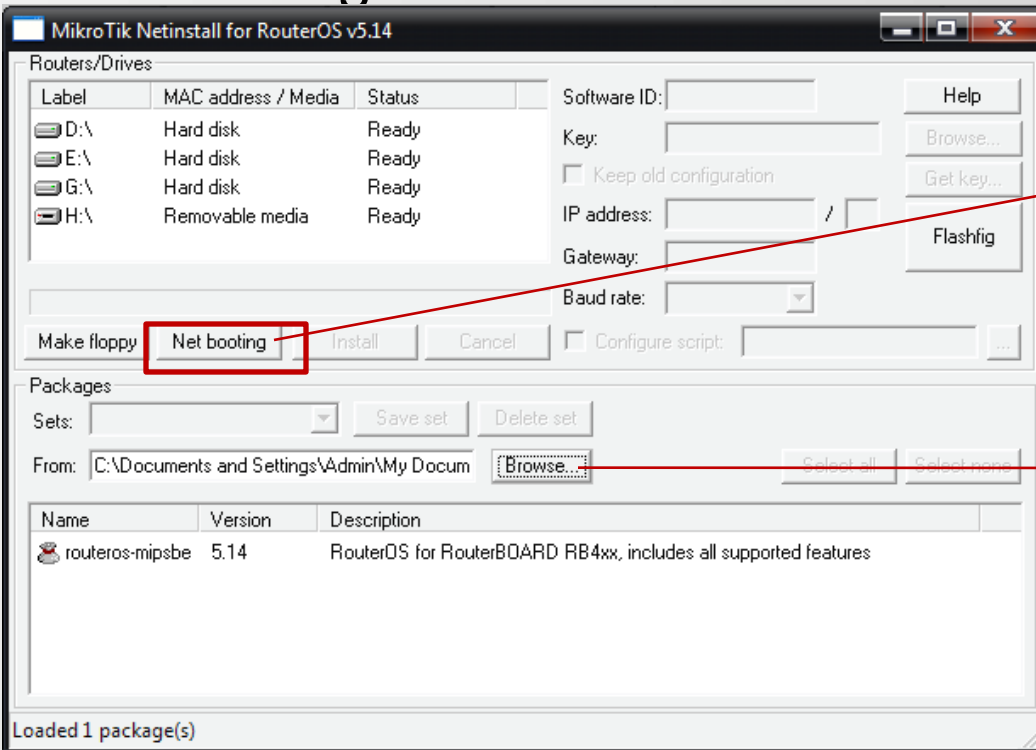


The screenshot shows the RouterOS WinBox interface. On the left is a vertical menu with options: System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, Make Supout.rif, Manual, and Exit. The main area contains two windows:

- Routerboard** window:
 - Routerboard
 - Model: 751U-2HnD
 - Serial Number: 2C4F013ED6BB
 - Current Firmware: 2.36
 - Upgrade Firmware: 2.37
 - Buttons: OK, Cancel, Apply, Upgrade, Settings
- Settings** window:
 - Baud Rate: 115200
 - Boot Delay: 1 s
 - Enter Setup On: any key
 - Boot Device: nand-if-fail-then-ethernet** (highlighted with a red box)
 - CPU Frequency: 400MHz
 - Boot Protocol: bootp
 - Options:
 - Enable Jumper Reset
 - Force Backup Booter
 - Silent Boot
 - Buttons: OK, Cancel, Apply

LAB – Reinstall RB 751

- Setting Netinstall

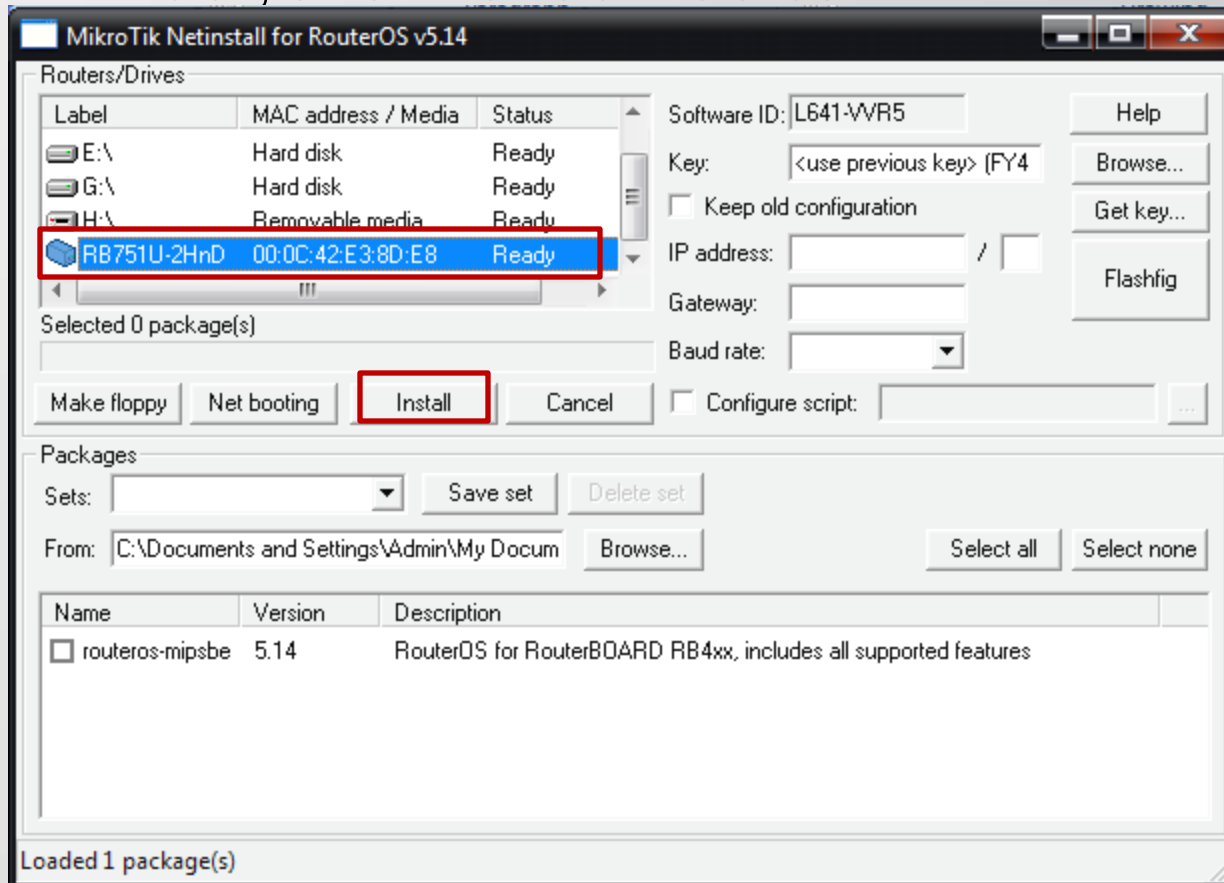


IP RouterOS

Arahkan ke folder dimana file npk routeros disimpan di laptop kita

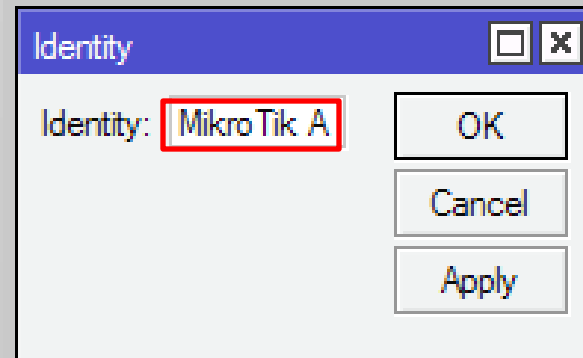
LAB – Reinstall RB 751

- Hard reset Mikrotik, dengan menekan tombol reset sambil router dinyalakan, sampai router terdeteksi oleh netinstall
- Klik install, untuk memulai instalasi



Router Identity

- Router Identity digunakan untuk membedakan router MikroTik satu dengan lainnya.
- Pada saat network menjadi komplek dan besar hal ini sangat diperlukan.
- Router Identity dapat disetting di menu System>Identity
- Router identity akan terlihat pada:
 - Winbox status bar.
 - Terminal console prompt
 - Neighbor Discovery
 - Halaman web/webfig

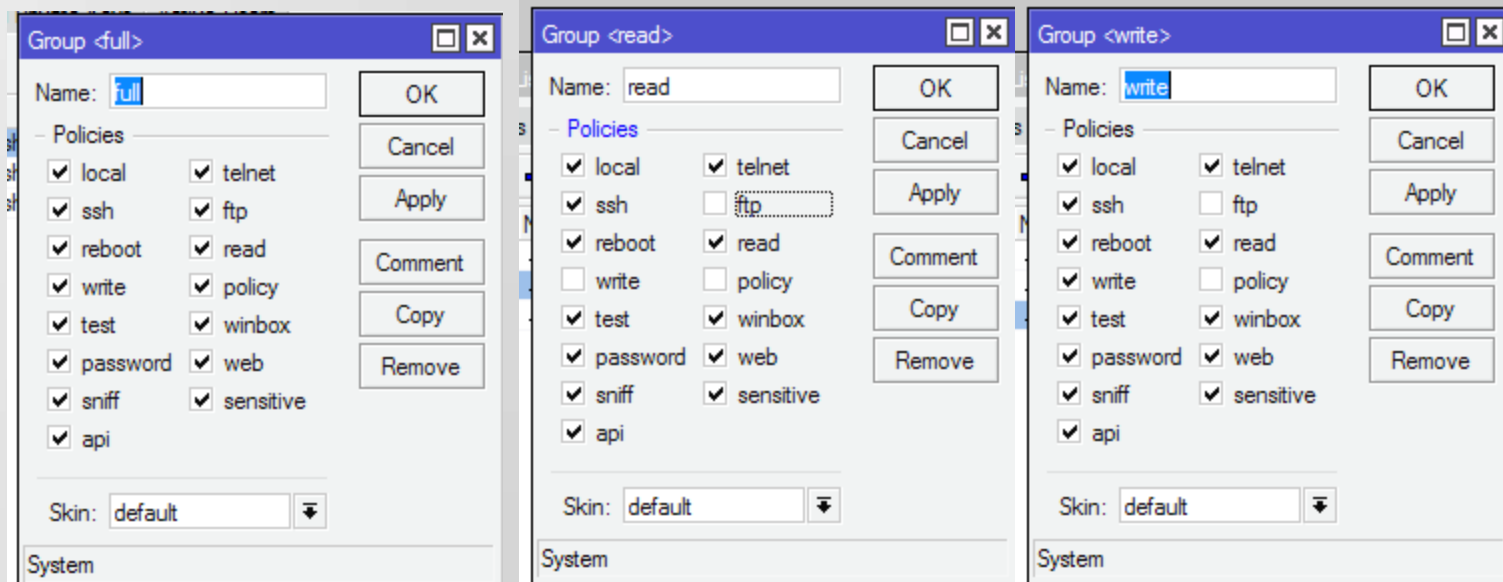


User Login Management

- Akses ke router ditentukan oleh menu user.
- Manajemen user dilakukan dengan
 - GROUP – profil pengelompokan user, menentukan privilege yang bisa diperoleh suatu user.
 - USER – merupakan login (username & password dari suatu user).
- Sesi user yang sedang melakukan koneksi ke router dapat dilihat pada menu System>Users>Active Users

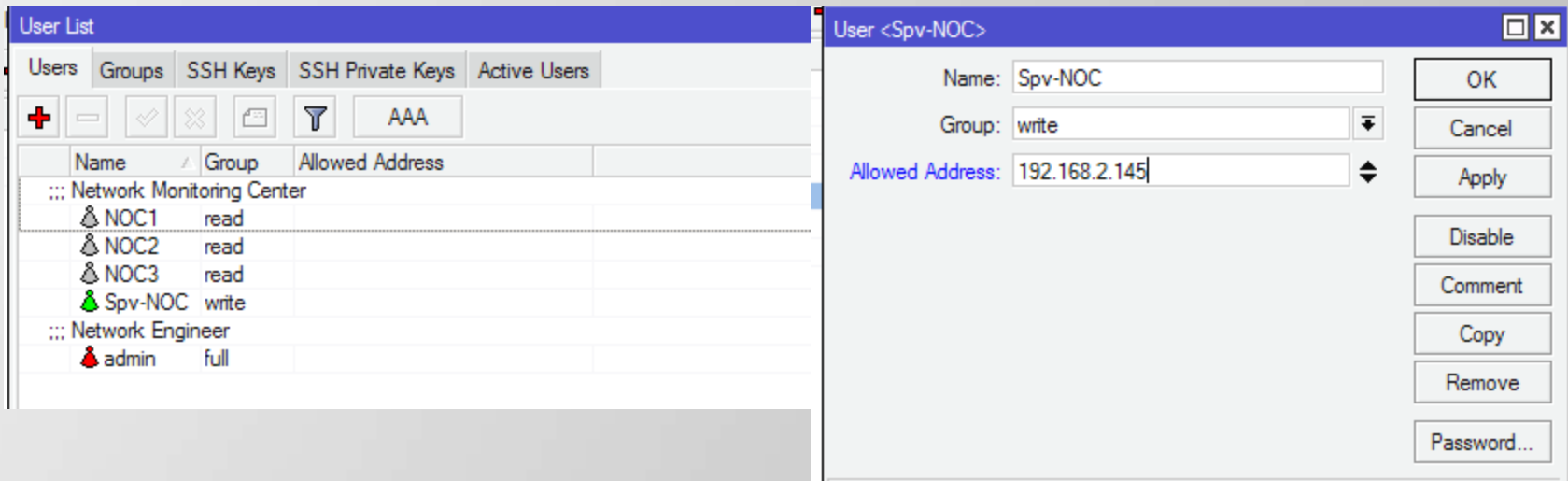
User Login Management - Group

- Group merupakan pengelompokan privilege/hak akses yang akan diberikan pada user.
- Ada 3 default privilege yang ada di MikroTik yaitu full, read dan write, namun diperbolehkan untuk customize sendiri.



User Login Management - Akses

- Masing-masing user dapat dibatasi hak aksesnya berdasarkan group.
- Masing-masing user juga dapat dibatasi berdasarkan IP address yang digunakannya.
- Misalkan si A hanya boleh login dengan IP A, atau hanya boleh dari network A.



The image shows two windows from a network management interface. The left window, titled 'User List', displays a table of users and their permissions. The right window, titled 'User <Spv-NOC>', shows the configuration for a specific user.

User List Table:

Name	Group	Allowed Address
::: Network Monitoring Center		
NOC1	read	
NOC2	read	
NOC3	read	
Spv-NOC	write	
::: Network Engineer		
admin	full	

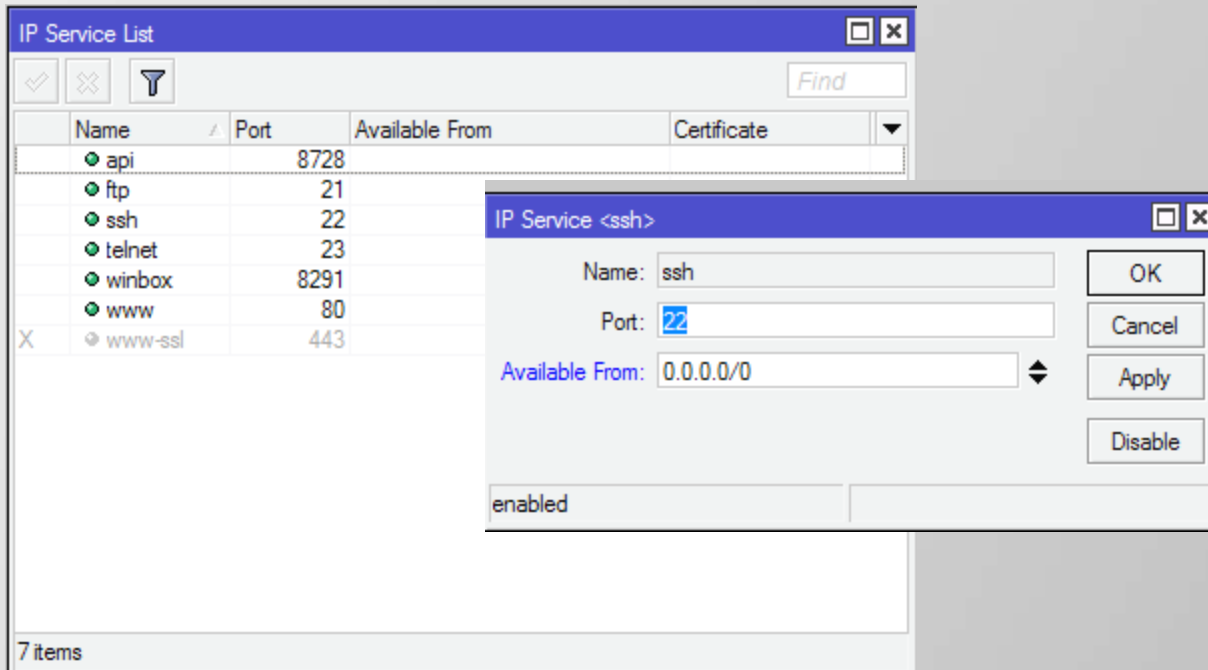
User <Spv-NOC> Configuration:

- Name: Spv-NOC
- Group: write
- Allowed Address: 192.168.2.145

Buttons on the right of the configuration window include: OK, Cancel, Apply, Disable, Comment, Copy, Remove, and Password...

User Login Management - Service

- Membatasi service (yang menjalankan remote login) yang bisa diakses oleh user dan dari IP tertentu.
- Setting konfigurasi ada di menu IP>Services
- Untuk keamanan kita juga dapat mengganti default port pada masing-masing services



The image shows two overlapping windows from a network management interface. The background window is titled "IP Service List" and contains a table with the following data:

Name	Port	Available From	Certificate
api	8728		
ftp	21		
ssh	22		
telnet	23		
winbox	8291		
www	80		
www-ssl	443		

The foreground window is titled "IP Service <ssh>" and shows configuration options for the SSH service:

- Name: ssh
- Port: 22
- Available From: 0.0.0.0/0
- Status: enabled

Buttons for "OK", "Cancel", "Apply", and "Disable" are visible on the right side of the foreground window.

LAB - User Login Management

- Gantilah identitas router menjadi NO_<nama anda>.
- Manajemen user
 - Buatlah username baru dalam kelompok group full.
 - Buatlah user “admin” hanya dapat akses dari IP selain IP laptop anda.
 - Coba login dengan user baru dan user “admin”
- Manajemen services
 - Gantilah port telnet menjadi port 8080
 - Buatlah agar winbox hanya dapat diakses dari IP laptop anda.

MikroTik Neighbor Discovery Protocol (MNDP)

- MNDP memudahkan konfigurasi dan manajemen jaringan dengan memungkinkan setiap router MikroTik untuk menemukan router MikroTik lainnya yang terhubung langsung
- MNDP juga memungkinkan kita menemukan router Mikrotik menggunakan winbox
- MNDP fitur:
 - bekerja pada koneksi IP
 - bekerja pada semua non-dinamic interface
 - mendistribusikan informasi dasar pada versi software
- MikroTik RouterOS mampu menemukan router yang menjalankan MNDP dan CDP (Cisco Discovery Protocol).

Lab – Block MNDP

Untuk menyembunyikan mikrotik anda agar tidak muncul pada Winbox MNDP scan, akses MNDP harus dibatasi dengan cara-cara sebagai berikut:

1. Block Port UDP protocol port 5678 (port untuk komunikasi MNDP) menggunakan **IP Firewall Filter Rule**
2. Disable MNDP pada menu **IP Neighbors Discovery**

Backup dan Restore

- Konfigurasi dalam router dapat dibackup dan disimpan untuk digunakan di kemudian hari. Ada 2 jenis backup yaitu
 1. **Binary file (.backup)**
 - ✓ **Tidak dapat dibaca** text editor.
 - ✓ Membackup **keseluruhan konfigurasi** router
 - ✓ Create return point (dapat kembali seperti semula)
 2. **Script file (.rsc)**
 - ✓ Berupa script, **dapat dibaca** dengan text editor.
 - ✓ Dapat membackup **sebagian atau keseluruhan konfigurasi** router.
 - ✓ Tidak mengembalikan ke konfigurasi seperti semula, melainkan menambahkan script tertentu pada konfigurasi utama.

Binary – Backup & Restore

- Backup ada pada menu File>backup

File List

Backup Restore Find

File Name	Type	Size	Creation Time
Mikro Tik-02011970-0007.backup	backup	15.5 KiB	Jan/02/1970 07:07:39
Mikro Tik-18112011-1358.backup	backup	24.7 KiB	Nov/18/2011 13:58:26
skins	directory		Jan/01/1970 07:00:45
um-before-migration.tar	.tar file	16.5 KiB	Jan/02/1970 07:00:18

Format backup file:
 MikroTik-[tanggal][bulan][tahun]-[jam][menit]
 File dapat disimpan di PC dengan cara drag-and-drop atau FTP

1. Tombol backup digunakan untuk backup konfigurasi router aktual.
2. Tombol restore digunakan untuk mengembalikan konfigurasi sesuai dengan file yang dipilih.

Binary – Backup & Restore

- Binary backup dan restore juga dapat dilakukan menggunakan terminal.
- Backup via terminal kelebihannya adalah dapat memberi nama file backup sesuai dengan keinginan kita

```
[admin@MikroTik A] > system backup save name=bakup_18_nov_11
Saving system configuration
Configuration backup saved
[admin@MikroTik A] > file print
```

#	NAME	TYPE	SIZE	CREATION-TIME
0	um-before-mi...	.tar file	16 896	jan/02/1970 07:00:18
1	skins	directory		jan/01/1970 07:00:45
2	MikroTik-181...	backup	25 338	nov/18/2011 13:58:26
3	MikroTik-020...	backup	15 865	jan/02/1970 07:07:39
4	bakup_18_nov...	backup	25 338	nov/18/2011 14:10:52

```
[admin@MikroTik A] > █
```

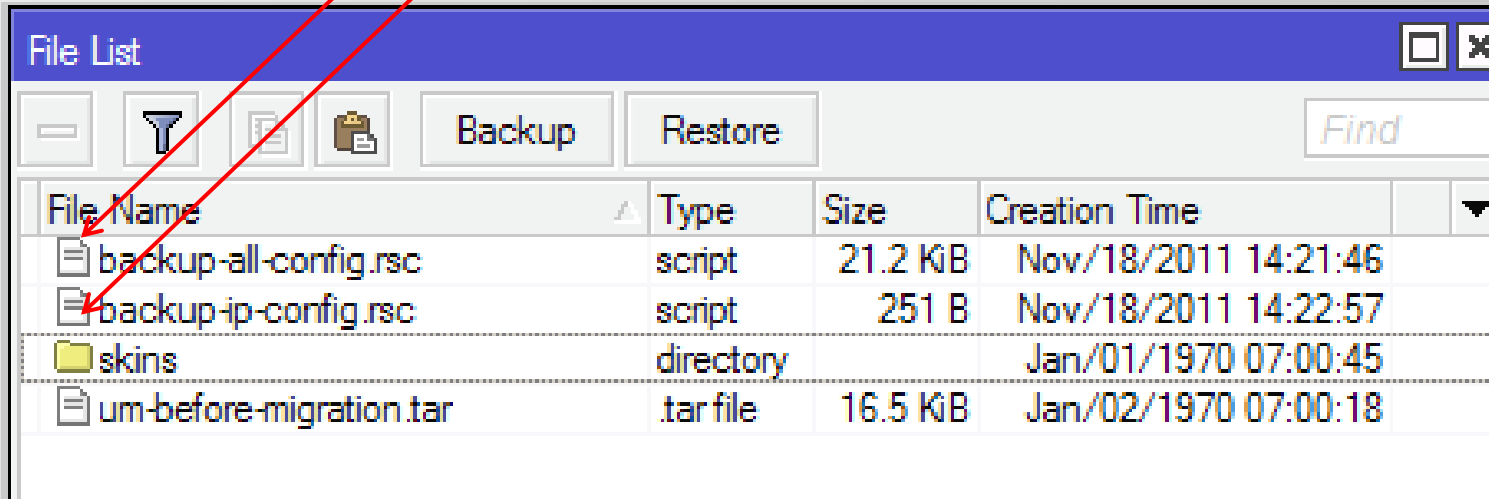
Script – Backup & Restore

- Backup dan restore dengan mode script dilakukan dengan perintah:
 - EXPORT akan menyimpan konfigurasi dengan bentuk script yang dapat dibaca dan diolah.
 - IMPORT akan menjalankan perintah yang terdapat dalam script.
- IMPORT/EXPORT dapat digunakan untuk membackup sebagian konfigurasi.
- IMPORT/EXPORT harus dilakukan melalui terminal.

Script – Backup & Restore

- Perintah EXPORT

```
[admin@MikroTik A] > export file=backup-all-config
[admin@MikroTik A] > /ip address export file=backup-ip-config
[admin@MikroTik A] >
```



File Name	Type	Size	Creation Time
backup-all-config.rsc	script	21.2 KB	Nov/18/2011 14:21:46
backup-ip-config.rsc	script	251 B	Nov/18/2011 14:22:57
skins	directory		Jan/01/1970 07:00:45
um-before-migration.tar	tar file	16.5 KB	Jan/02/1970 07:00:18

Script – Backup & Restore

- Perintah IMPORT

```
[admin@MikroTik A] > file print
# NAME                                TYPE                                SIZE CREATION-TIME
0 backup-all-config.rsc               script                             21 676 nov/18/2011 14:21:46
1 um-before-migratio...               .tar file                          16 896 jan/02/1970 07:00:18
2 skins                                directory                           jan/01/1970 07:00:45
3 backup-ip-config.rsc                script                             251 nov/18/2011 14:22:57
[admin@MikroTik A] > import backup-all-config.rsc
Opening script file backup-all-config.rsc

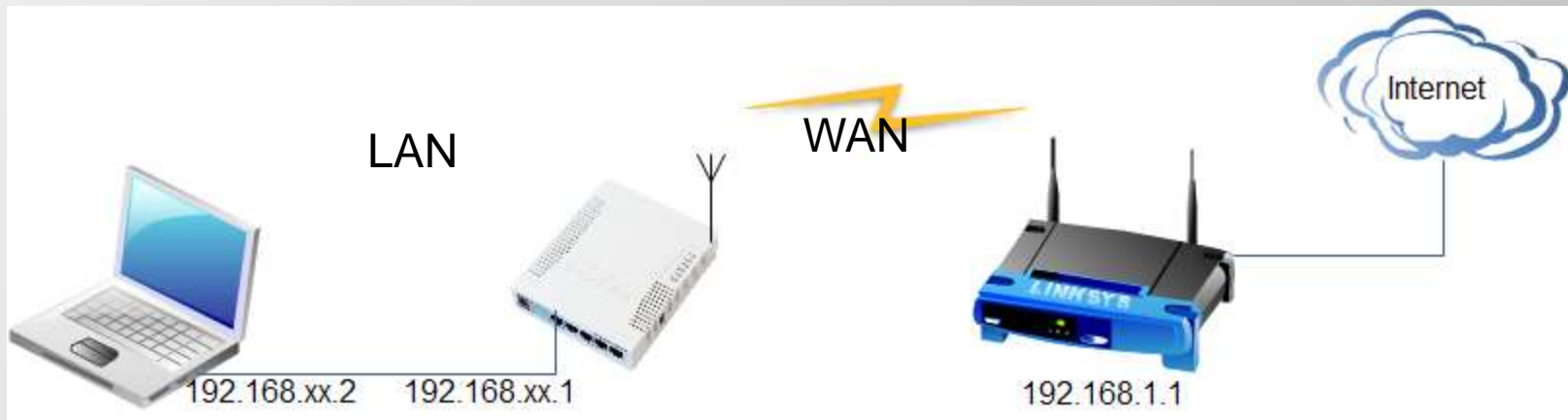
Script file loaded successfullyfailure: profile with the same name already exists
[admin@MikroTik A] > █
```

LAB - Backup & Restore

- Buatlah backup konfigurasi dengan perintah backup dan export.
- Pindahkan file backup dan rsc ke komputer/laptop.
- Coba buka dan edit file backup dan file rsc tersebut

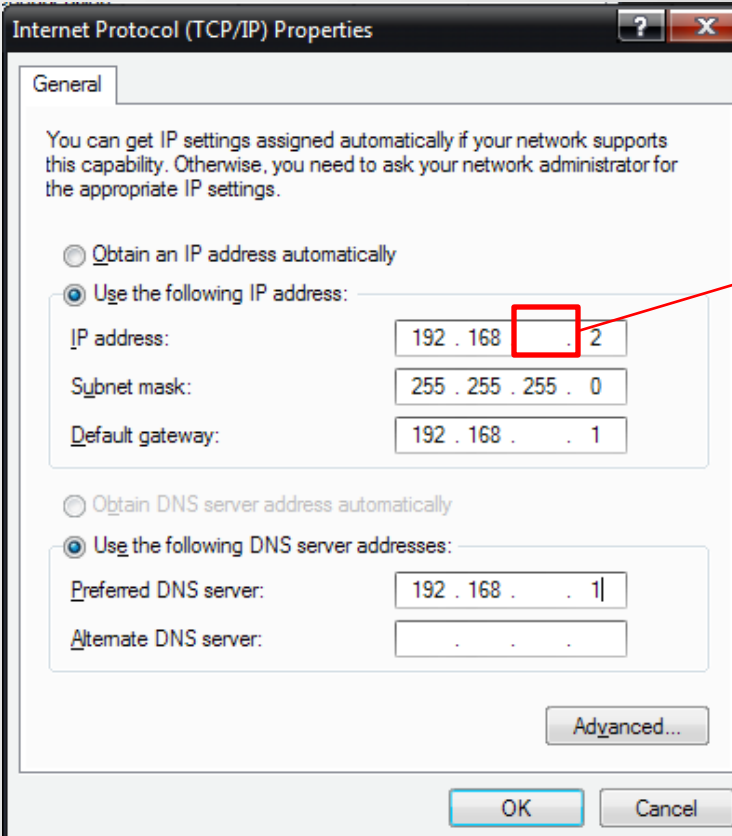
LAB – Koneksi Internet

- Ini adalah simulasi jaringan dasar untuk koneksi internet
- Setting koneksi internet menggunakan mikrotik sebagai Network Address Translation (NAT).



Konfigurasi LAN

- Setting IP pada Ethernet Laptop



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address: 192 . 168 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . . 1

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . . 1

Alternate DNS server: . . .

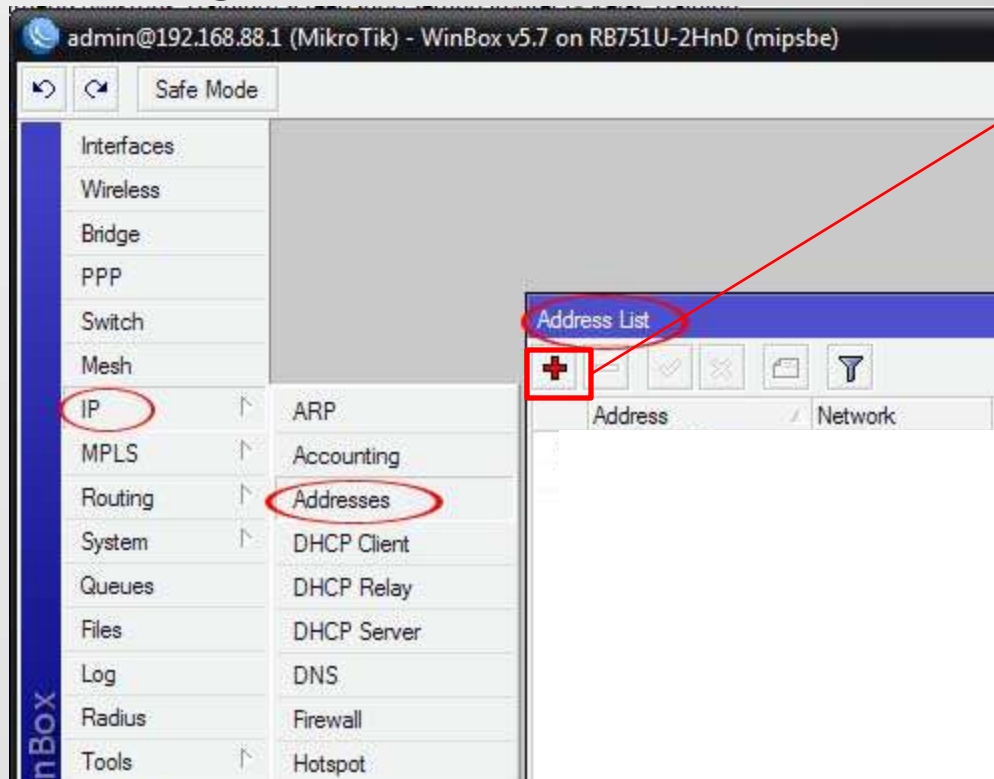
Advanced...

OK Cancel

Sesuaikan dengan nomor peserta

Konfigurasi LAN

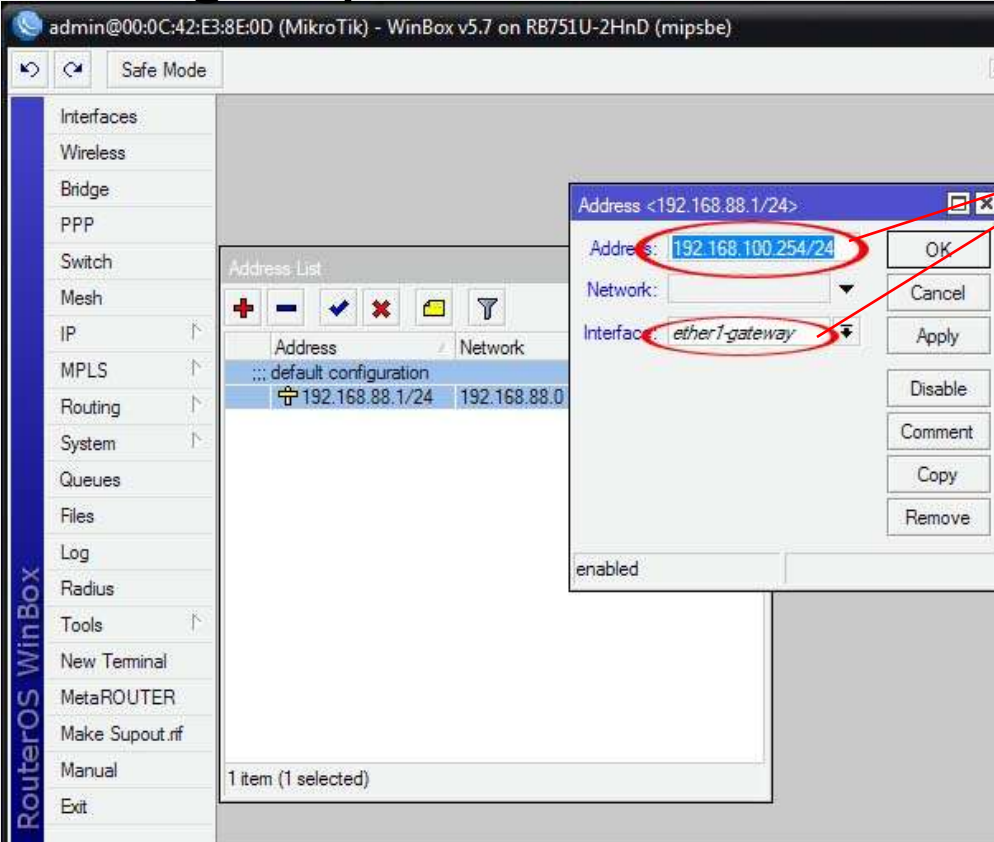
- Setting IP pada Ether1 MikroTik



Add IP address untuk ether 1

Konfigurasi LAN

- Setting IP pada Ether1 MikroTik



The screenshot shows the WinBox interface for a MikroTik router. The left sidebar contains a menu with options like Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, Make Supout.rf, Manual, and Exit. The main window displays the 'Address List' table with the following data:

Address	Network
... default configuration	
192.168.88.1/24	192.168.88.0

A dialog box titled 'Address <192.168.88.1/24>' is open, showing the configuration for a new address. The 'Address' field is set to '192.168.100.254/24' and the 'Interface' is set to 'ether1-gateway'. The 'enabled' checkbox is checked.

- Sesuaikan IP adress
- Set interface ether1

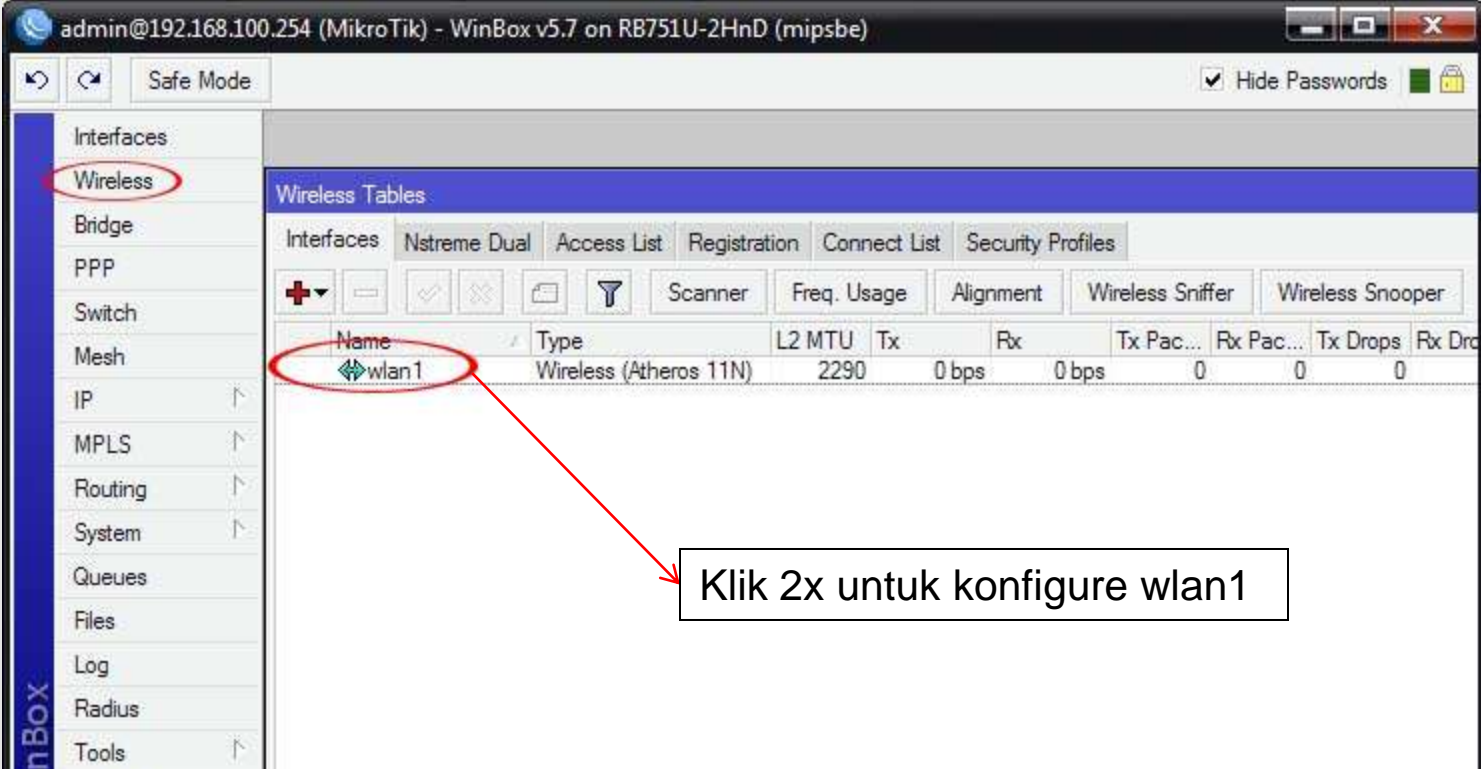
Konfigurasi LAN

- Konek winbox menggunakan IP address ether1




Konfigurasi WAN

- Setting wlan pada MikroTik sebagai station.



admin@192.168.100.254 (MikroTik) - WinBox v5.7 on RB751U-2HnD (mipsbe)

Safe Mode Hide Passwords 

Interfaces

Wireless

Bridge

PPP

Switch

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Radius

Tools

Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles

+ - ✓ ✕ 📄 🔍 Scanner Freq. Usage Alignment Wireless Sniffer Wireless Snooper

Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops	Rx Dro
wlan1	Wireless (Atheros 11N)	2290	0 bps	0 bps	0	0	0	0

Klik 2x untuk konfigure wlan1

Konfigurasi WAN

- Membuat Security Profile.

admin@192.168.2.2 (MikroTik) - WinBox v5.14 on RB751U-2HnD (mipsbe)

Safe Mode Hide Passwords

Wireless Tables

Name	Mode	Authenticatio...	Unicast Ciphers	Group Ciphers	WPA Pre-Shared ...	WPA2 Pr
default	none				*****	*****
profile1	dynamic keys	WPA PSK W...	tkip aes ccm	tkip aes ccm	*****	*****

Security Profile <profile 1>

General **RADIUS** EAP Static Keys

Name: profile1
Mode: dynamic keys

Authentication Types

- WPA PSK
- WPA2 PSK
- WPA EAP
- WPA2 EAP

Unicast Ciphers

- tkip
- aes ccm

Group Ciphers

- tkip
- aes ccm

WPA Pre-Shared Key: *****
WPA2 Pre-Shared Key: *****

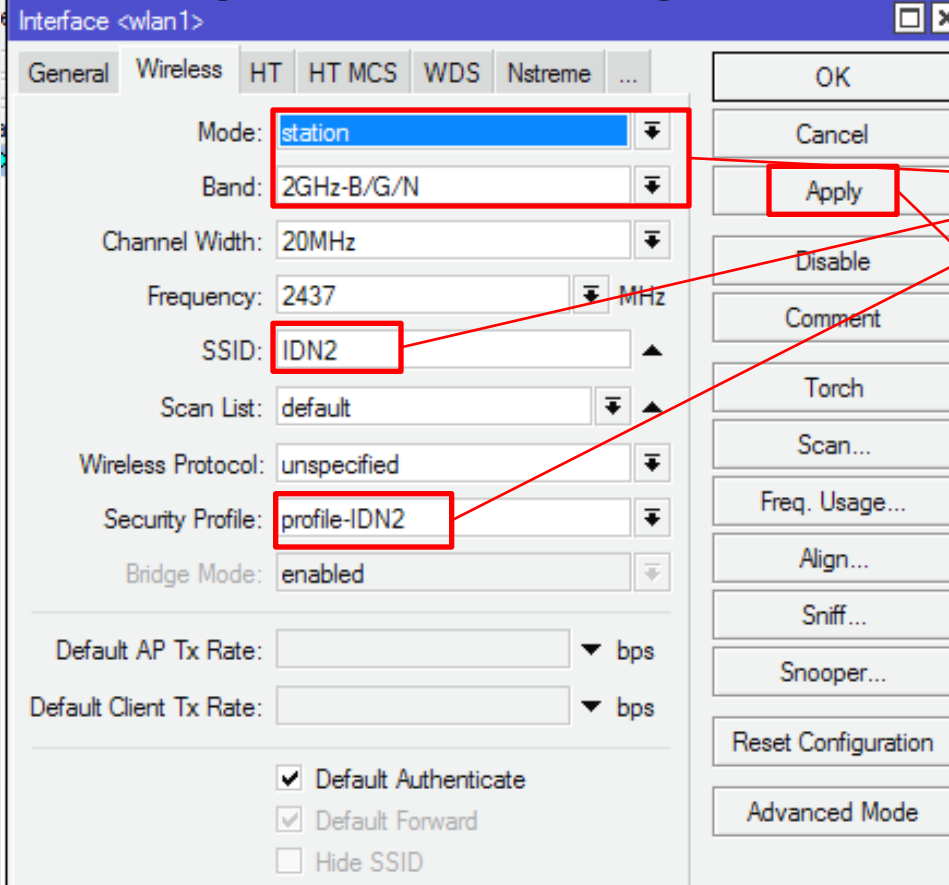
OK Cancel Apply Copy Remove

Check auth option tkip

Password wireless LAN

Konfigurasi WAN

- Setting wlan1 sebagai station



Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme ...

Mode: station

Band: 2GHz-B/G/N

Channel Width: 20MHz

Frequency: 2437 MHz

SSID: IDN2

Scan List: default

Wireless Protocol: unspecified

Security Profile: profile-IDN2

Bridge Mode: enabled

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

OK

Cancel

Apply

Disable

Comment

Torch

Scan...

Freq. Usage...

Align...

Sniff...

Snooper...

Reset Configuration

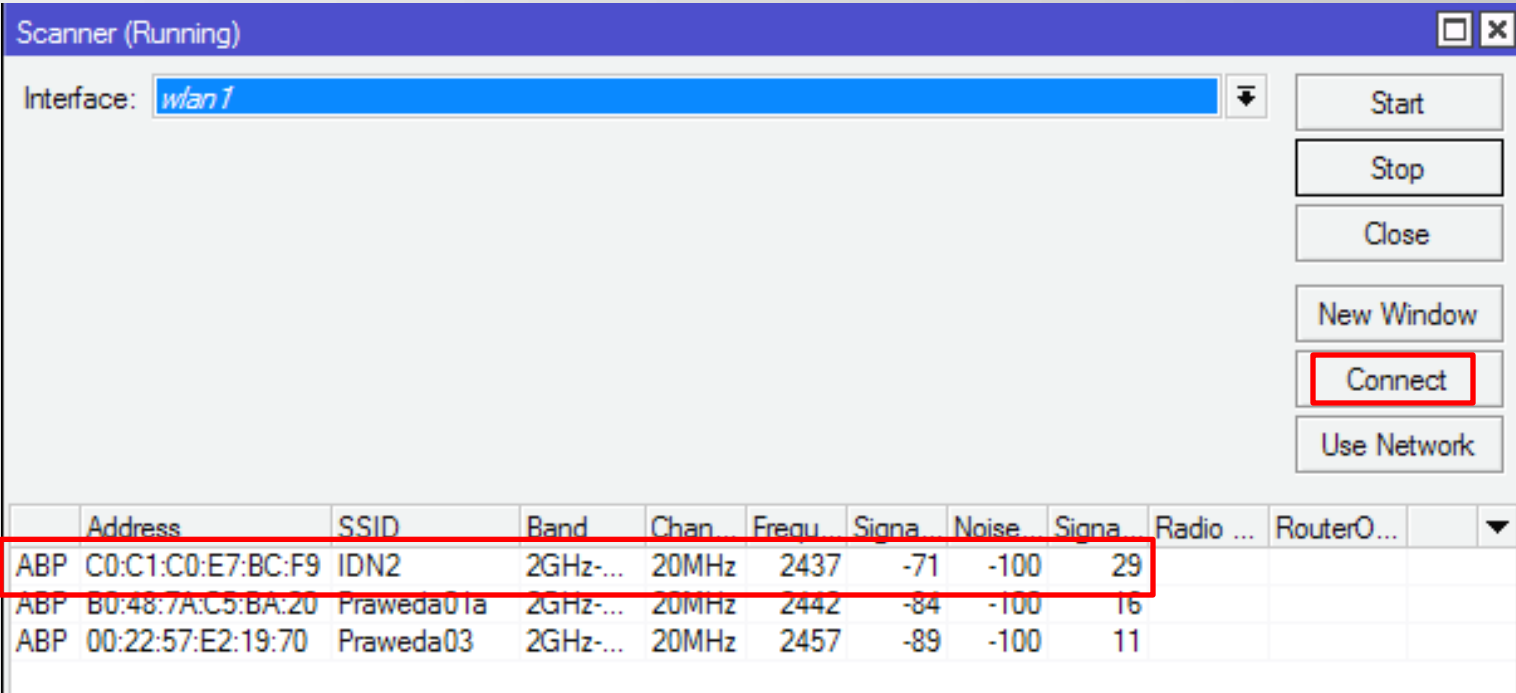
Advanced Mode

- Setting wireless mode
- Setting band
- Setting SSID
- Security Profile

Klik Apply untuk mengeksekusi hasil konfigurasi

Konfigurasi WAN

- Mode station juga dapat digunakan untuk scan network untuk mempermudah konek ke sebuah AP.



Scanner (Running)

Interface: *wlan 1*

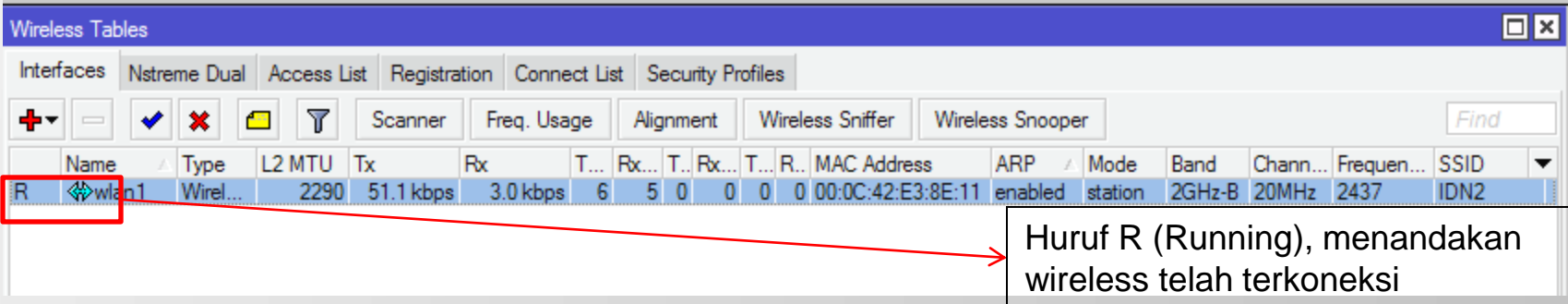
Start
Stop
Close
New Window
Connect
Use Network

	Address	SSID	Band	Chan	Frequ	Signa	Noise	Signa	Radio ...	RouterO...
ABP	C0:C1:C0:E7:BC:F9	IDN2	2GHz-...	20MHz	2437	-71	-100	29		
ABP	B0:48:7A:C5:BA:20	Praweda01a	2GHz-...	20MHz	2442	-84	-100	16		
ABP	00:22:57:E2:19:70	Praweda03	2GHz-...	20MHz	2457	-89	-100	11		

- Pilih AP yang ingin dikoneksikan dan klik tombol connect

Konfigurasi WAN

- Wireless telah terkoneksi



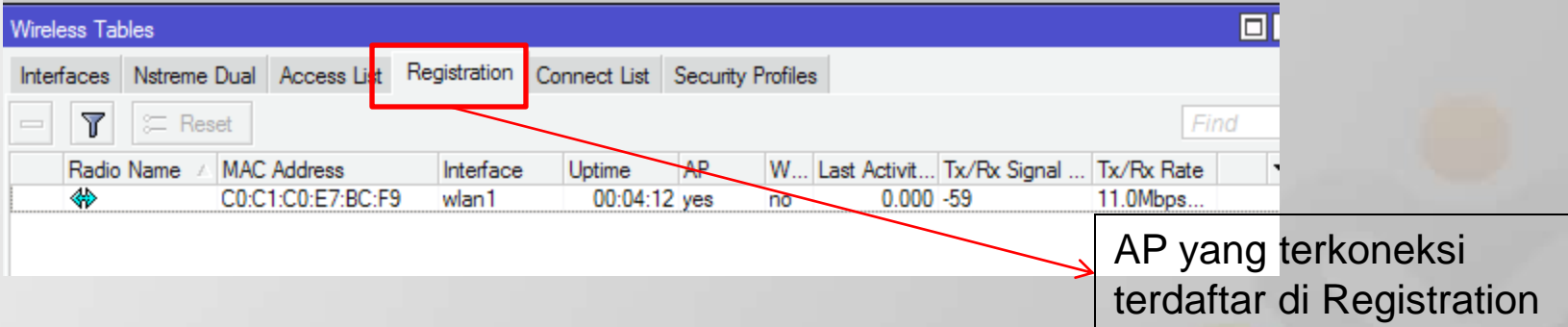
Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles

Scanner Freq. Usage Alignment Wireless Sniffer Wireless Snooper Find

Name	Type	L2 MTU	Tx	Rx	T...	Rx...	T...	Rx...	T...	R...	MAC Address	ARP	Mode	Band	Chann...	Frequen...	SSID
R wlan1	Wirel...	2290	51.1 kbps	3.0 kbps	6	5	0	0	0	0	00:0C:42:E3:8E:11	enabled	station	2GHz-B	20MHz	2437	IDN2

Huruf R (Running), menandakan wireless telah terkoneksi



Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles

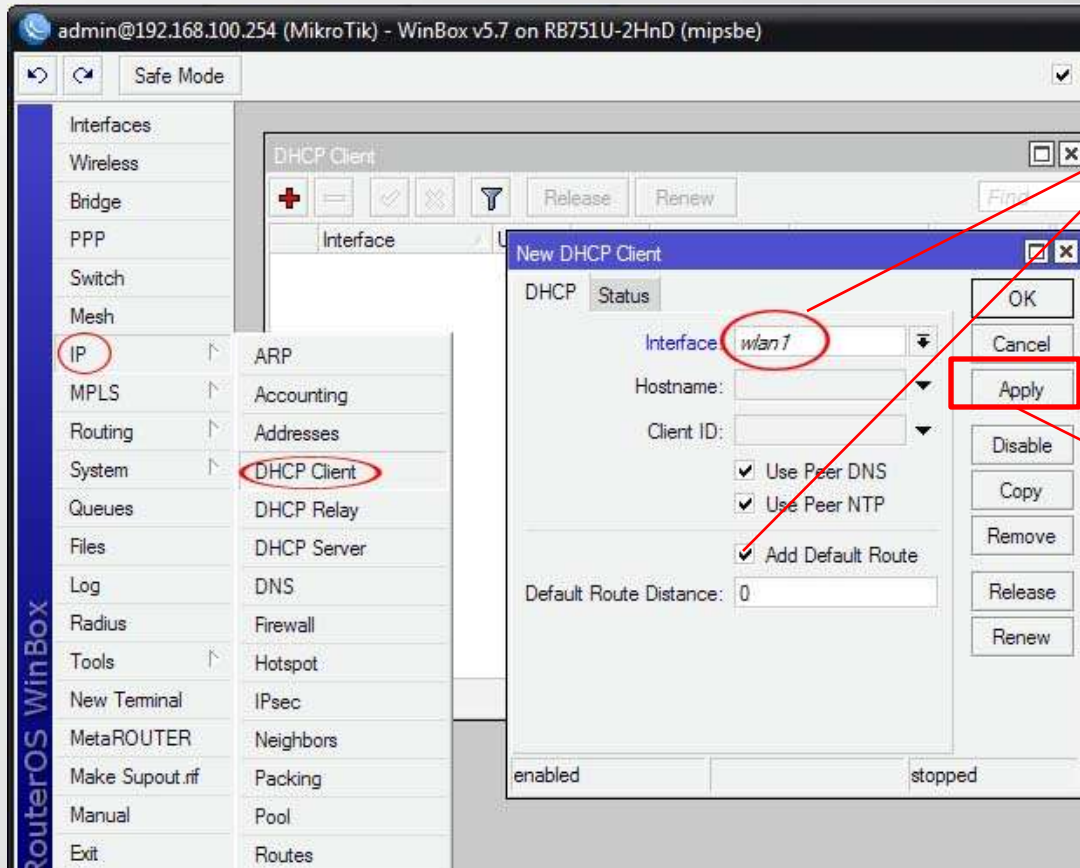
Reset Find

Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activit...	Tx/Rx Signal ...	Tx/Rx Rate
wlan1	C0:C1:C0:E7:BC:F9	wlan1	00:04:12	yes	no	0.000	-59	11.0Mbps...

AP yang terkoneksi terdaftar di Registration

Konfigurasi WAN

- Setting DHCP client



Setting DHCP client pada interface wlan1

Klik Apply untuk mengeksekusi hasil konfigurasi

Seting DHCP Client

- Pada menu IP DHCP Client

Pilih interface yang akan digunakan sebagai DHCP client

Set agar DNS, NTP dan default route otomatis didapatkan dari server

Seting DHCP Client

- Setting DHCP client

Interface	Use P...	Add D...	IP Address	Expires After	Status
wlan1	yes	yes	192.168.88.251/24	2d 23:27:32	bound

Status bound menandakan bahwa wlan1 sudah mendapatkan IP address dari AP

Address	Network	Interface
D 192.168.88.251/...	192.168.88.0	wlan1
D - dynamic 68.100.254...	192.168.100.0	ether1-gateway

2 items (1 selected)

Pada IP>address>interface terdapat dynamic IP address pada wlan1

DNS Server

- Pada IP DNS, setting DNS server, misal disini kita memakai DNS google

DNS Settings
☐ ✕

Servers: ⬆

Allow Remote Requests

Max UDP Packet Size:

Cache Size: KB

Cache Used:

Testing

- Coba lakukan ping dan traceroute dari MikroTik

Ping (Running)

General | Advanced

Ping To:

Interface:

ARP Ping

Packet Count:

Timeout: ms

Start
Stop
Close
New Window

Seq #	Host	Time	Reply Size	TTL	Status
44	98.137.149.56	343ms	50	52	
45	98.137.149.56	248ms	50	52	
46	98.137.149.56	228ms	50	52	
47	98.137.149.56	261ms	50	52	
48	98.137.149.56	235ms	50	52	
49	98.137.149.56	238ms	50	52	
50	98.137.149.56	356ms	50	52	
51	98.137.149.56	236ms	50	52	
52	98.137.149.56	240ms	50	52	
53	98.137.149.56	349ms	50	52	
54	98.137.149.56	235ms	50	52	
55	98.137.149.56	272ms	50	52	
56	98.137.149.56	234ms	50	52	
57	98.137.149.56	257ms	50	52	
58	98.137.149.56	231ms	50	52	
59	98.137.149.56	247ms	50	52	

60 of 60 packets received | 0% packet loss | Min: 225 ms | Avg: 276 ms | Max: 529 ms

Traceroute

Traceroute To:

Packet Size:

Timeout: ms

Protocol:

Port:

Start
Stop
Close
New Window

Src. Address:

Interface:

DSCP:

Routing Table:

#	Host	Time 1	Time 2	Time 3	Status
0	192.168.2.2	3ms	8ms	9ms	
1	192.168.1.1	7ms	8ms	8ms	
2	180.252.16.1	31ms	29ms	28ms	
3	125.160.15.41	24ms	39ms	32ms	
4	118.98.59.6	57ms	60ms	51ms	<MPLS:L=16973,E=0,T=255>
5	118.98.59.42	46ms	53ms	45ms	
6	180.240.190.13	66ms	82ms	48ms	
7	72.14.215.170	105ms	54ms	49ms	
8	209.85.243.158	227ms	50ms	54ms	
9	209.85.242.243	72ms	57ms	95ms	<MPLS:L=797265,E=4>
10	209.85.250.237	58ms	56ms	87ms	
11	66.249.94.126	61ms	161ms	70ms	
12	209.85.175.99	60ms	55ms	62ms	

Setting NAT

IP>firewall>NAT
Chain : srcnat
Out interface :wlan1
Action: masquerade

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	mas...	srcnat							wlan1	768 B	4

NAT Rule <>

General | Advanced | Extra | Action | Statistics

Chain: **srcnat**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface: wlan1

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

NAT Rule <>

General | Advanced | Extra | Action | Statistics

Action: **masquerade**

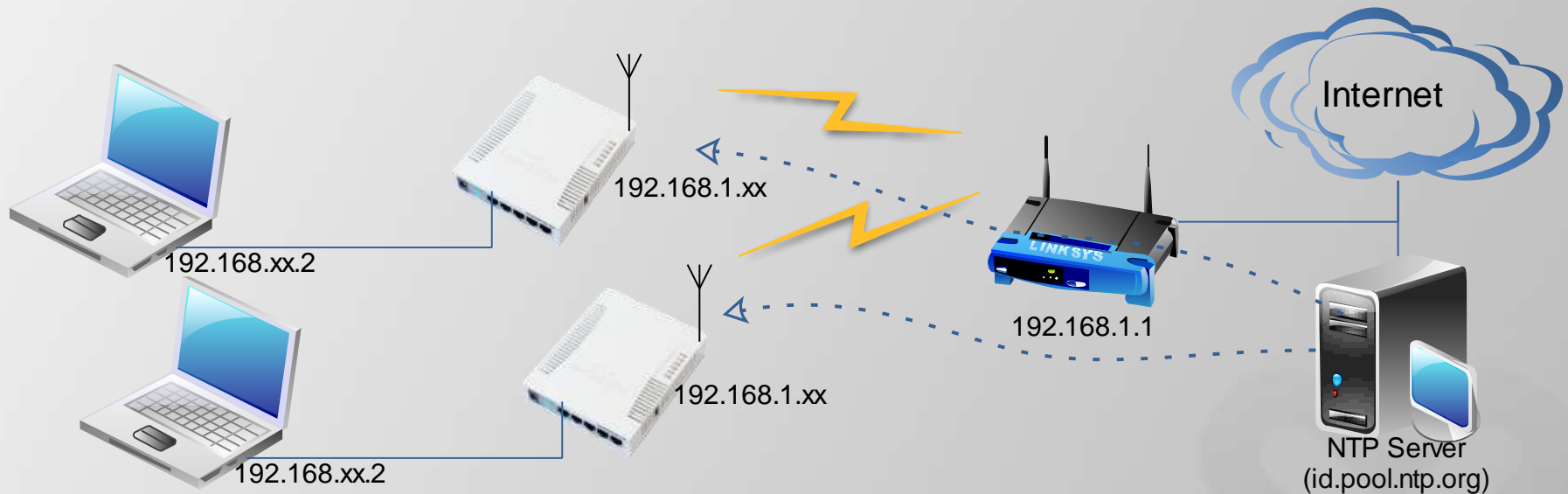
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Troubleshooting

- Router tidak bisa ping ke luar?
 - Cek apakah wireless sudah terkoneksi.
 - Cek DHCP client apakah sudah running dan mendapatkan IP (bound)
- Router bisa ping ke ip public tapi tidak bisa ping domain name.
 - Check IP DNS (allow remote request)
- Komputer tidak dapat ping ke router.
 - Cek ip address (pastikan sbnet /24)
- Komputer bisa ping ke IP luar tapi tidak bisa ping domain.
 - Check IP DNS di komputer.

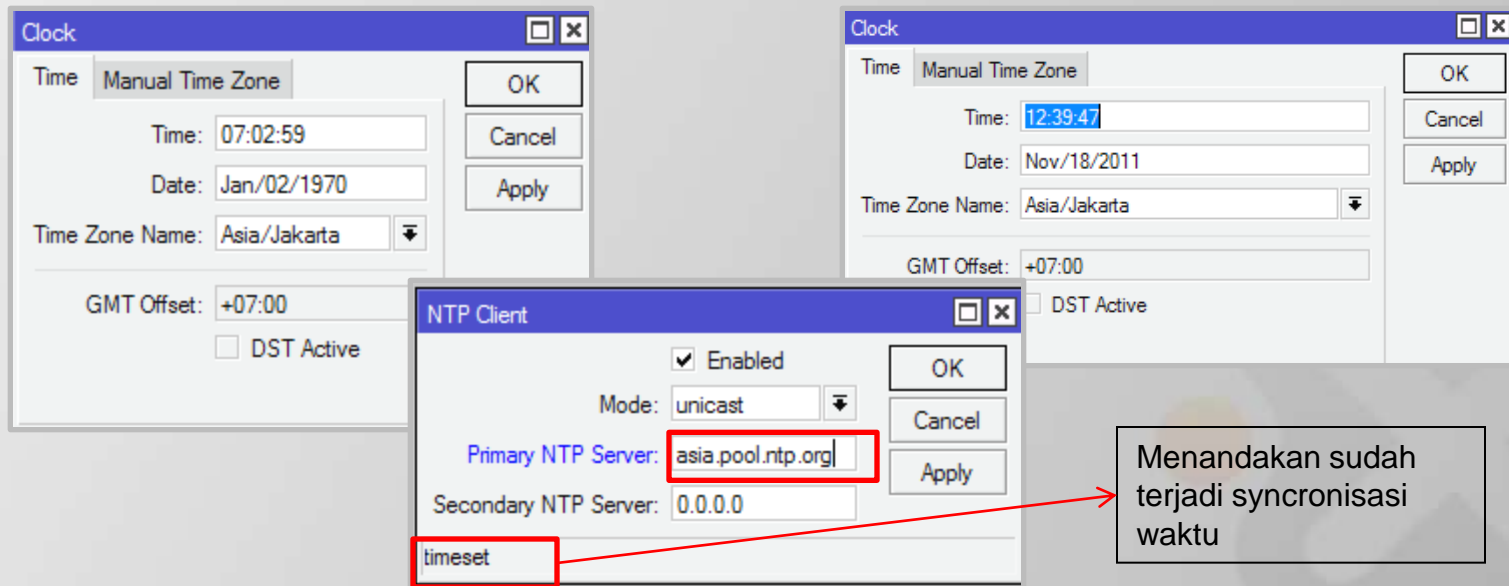
LAB- Network Time Protocol (NTP)

- Cobalah seting Mikrotik menggunakan NTP public service id.pool.ntp.org



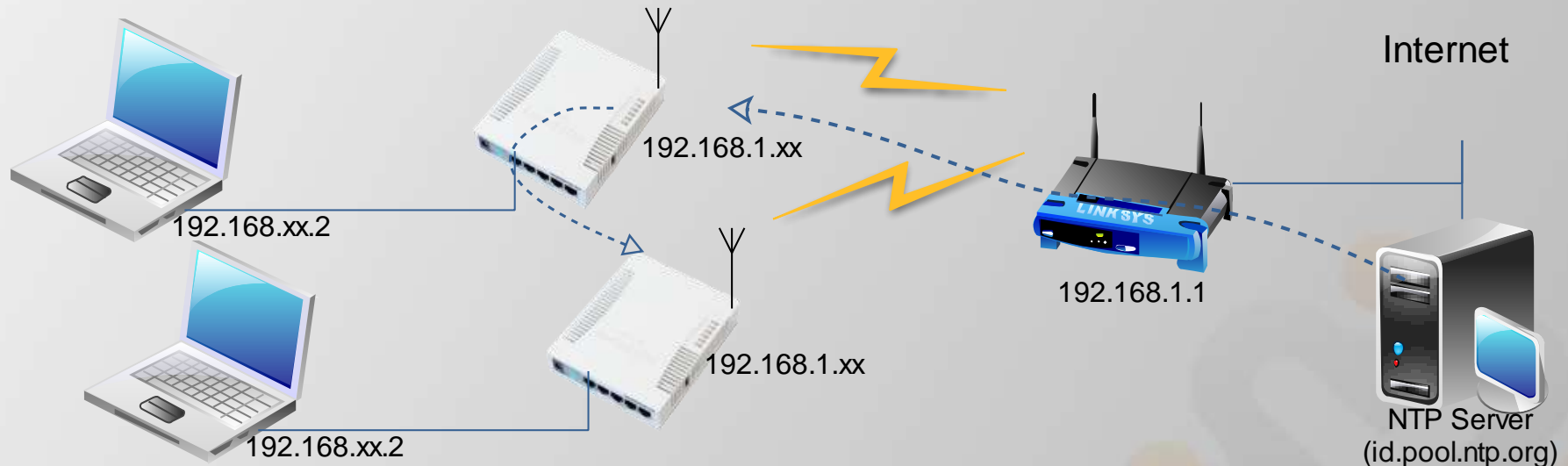
Network Time Protocol

- Kebanyakan RB mikrotik tidak memiliki battery untuk clock internal (kecuali RB230 dan powerpc)
- NTP untuk sinkronisasi waktu antar router/server lainnya.
- NTP juga bisa diarahkan ke public NTP server seperti **asia.pool.ntp.org**, atau **id.pool.ntp.org**



LAB- Network Time Protocol (NTP)

- Peserta 1 menggunakan NTP public service id.pool.ntp.org, peserta yang lain NTP server diarahkan ke peserta 1



NTP Client

Fase sinkronisasi NTP Client

- **Started** : start service NTP
- **Reached** : terkoneksi dengan NTP server
- **Synchronized** : sinkronisasi waktu dengan NTP server
- **Timeset** : mengganti waktu/tanggal lokal sesuai waktu NTP server

Module 2 - Firewall



Firewall – Overview

- Firewall digunakan untuk melindungi router dari akses yang tidak dikehendaki baik yang berasal dari luar (internet) maupun dari client (local).
- Firewall juga digunakan untuk memfilter akses antar network yang melewati router.
- Dalam MikroTik, firewall diimplementasikan dalam fitur Filter dan NAT.

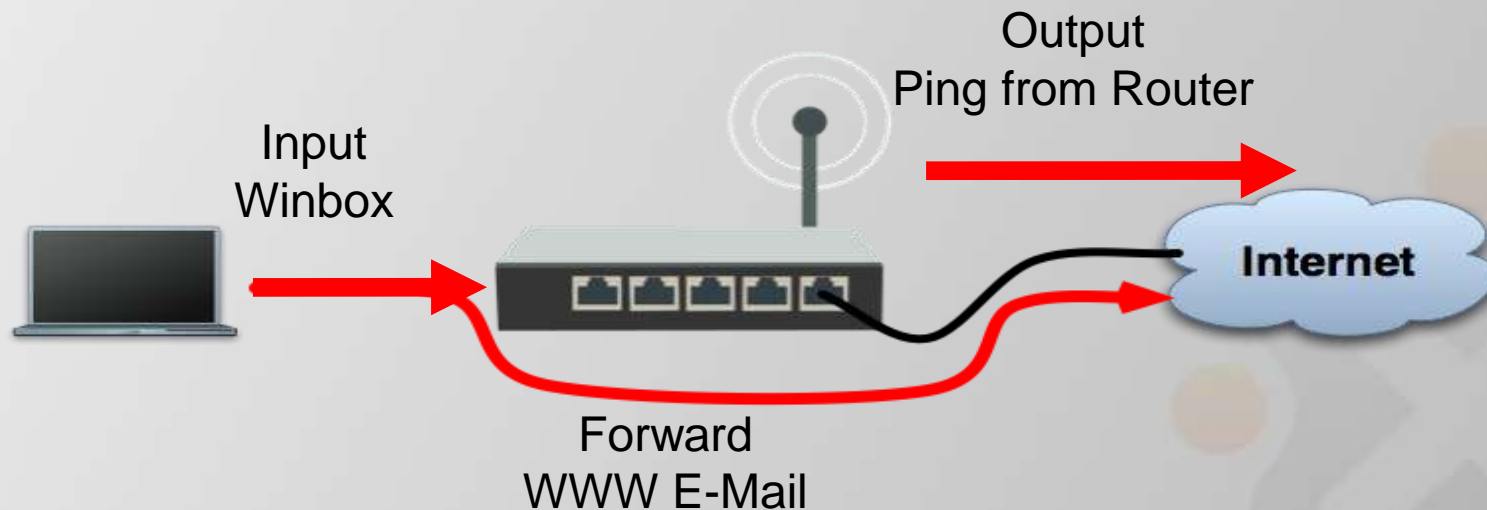
Firewall Filter Rule

- Setiap Firewall Filter rule diorganisir dalam chain (rantai)
- Dalam Firewall Filter, ada 3 default chain (input, forward, output).
- Setiap aturan chain yang dibuat akan dibaca oleh router dari atas ke bawah.
- Paket dicocokkan dengan kriteria/persyaratan dalam suatu chain, apabila cocok paket akan melalui kriteria/persyaratan chain berikutnya/ di bawahnya.

Packet Flow

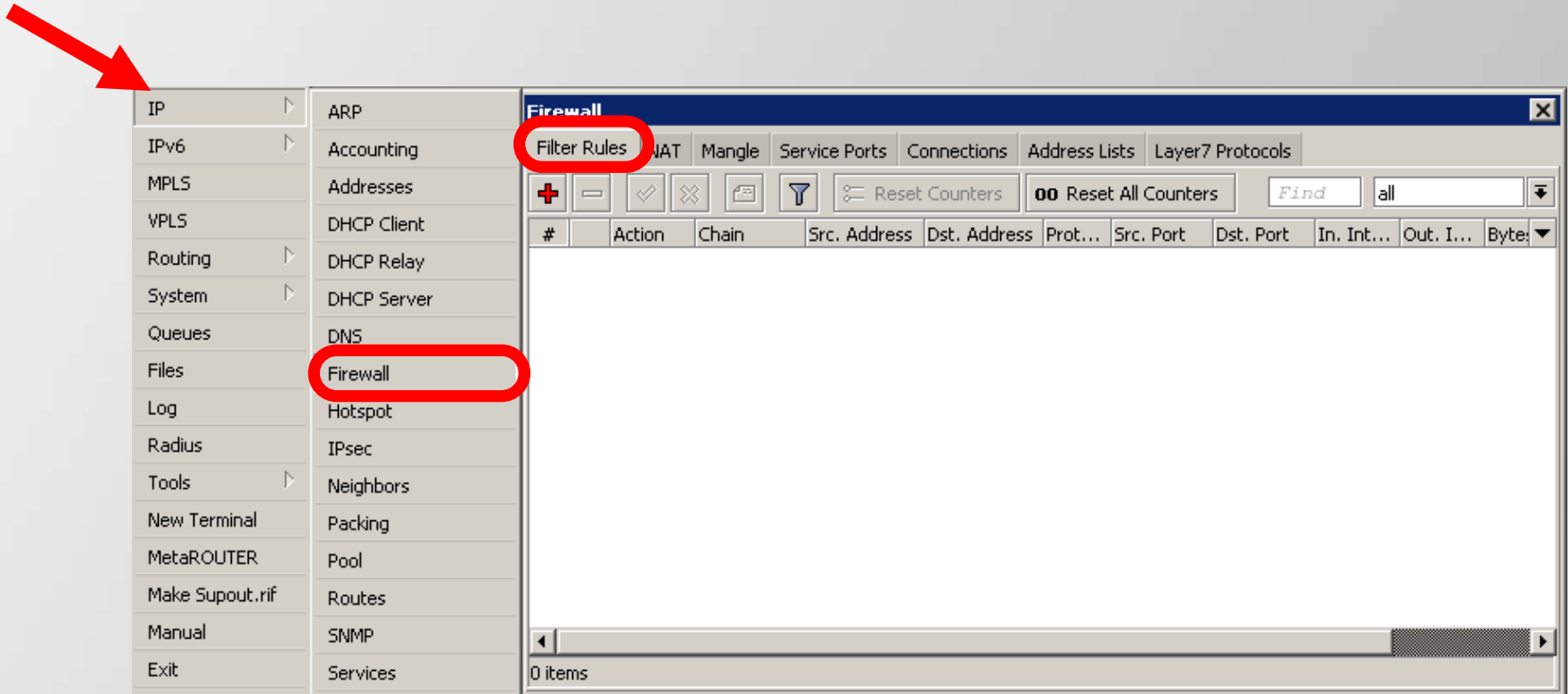
Tiga aturan dasar packet flow

- INPUT – **ke** router
- OUTPUT – **dari** router
- FORWARD – **melewati** router



Firewall Filter Rule

- IP Firewall Filter Rule



The screenshot shows the Mikrotik WinBox interface for configuring Firewall Filter Rules. The left sidebar contains a tree view of system settings, with 'Firewall' selected under the 'Files' category. The main window displays the 'Filter Rules' configuration page, which includes a toolbar with various icons and a table for listing rules. The table has the following columns: #, Action, Chain, Src. Address, Dst. Address, Prot..., Src. Port, Dst. Port, In. Int..., Out. I..., and Byte. The table is currently empty, and the status at the bottom indicates '0 items'.

Firewall Filter Rule

- Prinsip IF.....THEN.....
- IF (jika) packet memenuhi syarat pada rule yang kita buat.
- THEN (maka) action apa yang dilakukan pada packet tersebut

Firewall – IF (Condition)

IP>Firewall>Filter Rules>General

New Firewall Rule

General Advanced Extra Action Statistics

Chain: forward

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Source IP (IP client)
 Destination IP (IP internet)

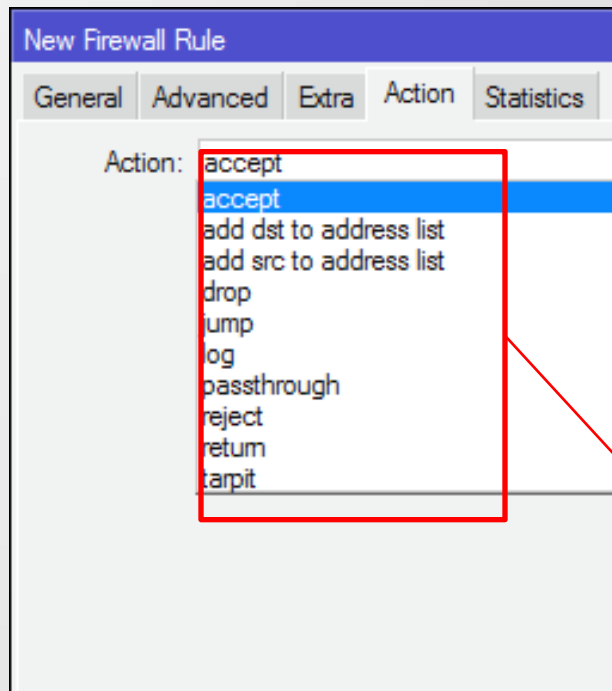
Protocol (TCP/UDP/ICMP, dll)
 Source port (biasanya port dari client)
 Destination port (service port tujuan)

Interface (traffik masuk atau keluar)

Paket yang sebelumnya telah ditandai

Firewall – THEN (Action)

IP>Firewall>Filter Rules>Action



accept - accept the packet. Packet is not passed to next firewall rule.

add-dst-to-address-list - add destination address to [address list](#) specified by address-list parameter

add-src-to-address-list - add source address to [address list](#) specified by address-list parameter

drop - silently drop the packet

jump - jump to the user defined chain specified by the value of jump-target parameter

log - add a message to the system log containing following data: in-interface, out-interface, src-mac, protocol, src-ip:port->dst-ip:port and length of the packet. After packet is matched it is passed to next rule in the list, similar as passthrough

passthrough - ignore this rule and go to next one (useful for statistics).

reject - drop the packet and send an ICMP reject message

return - passes control back to the chain from where the jump took place

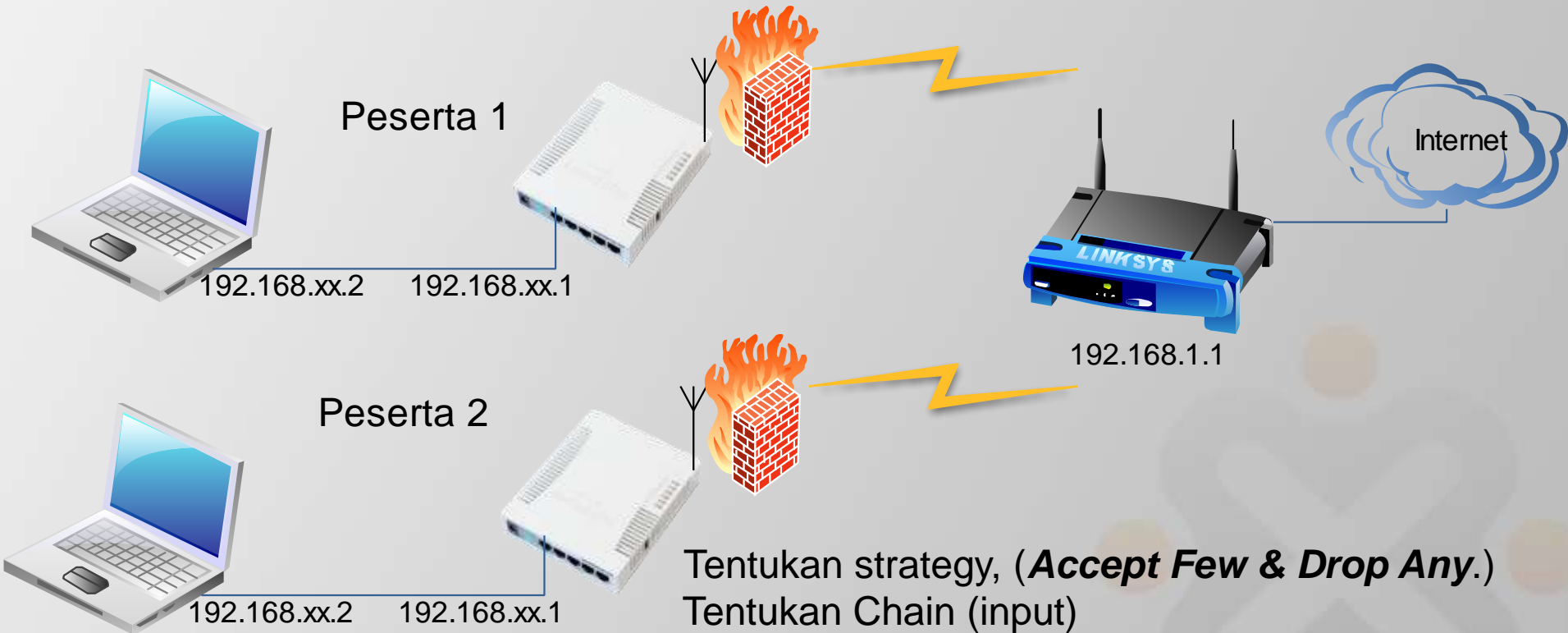
tarpit - captures and holds TCP connections (replies with SYN/ACK to the inbound TCP SYN packet)

Firewall Strategy

- Banyak trafik yang harus difilter dan dipilah mana yang harus di perbolehkan (accept) dan mana yang harus di buang (drop)
- Ada 2 metode untuk menyederhanakan rule firewall yang kita buat:
 - Drop beberapa, lainnya diterima (*drop few, accept any*)
 - Terima beberapa, lainnya dibuang (*accept few, drop any*)

LAB – Protecting Our Router

Cobalah buat firewall hanya memperbolehkan IP laptop sendiri yang hanya bisa akses router



LAB – Protecting Our Router

- IF ada traffic **input** yang berasal dari IP Laptop (**192.168.xx.2**)

New Firewall Rule

General

Advanced

Extra

Action

Statistics

Chain:

Src. Address:

Dst. Address:

- Then tentukan action → **accept**

New Firewall Rule

General

Advanced

Extra

Action

Statistics

Action:

LAB – Protecting Our Router

- IF ada traffic yang berasal dari all

New Firewall Rule

General

Advanced

Extra

Action

Statistics

Chain:

Src. Address:

Dst. Address:

- Then tentukan action (drop)

New Firewall Rule

General

Advanced

Extra

Action

Statistics

Action:

LAB – Protecting Our Router

- Akan ada 2 chain rules.

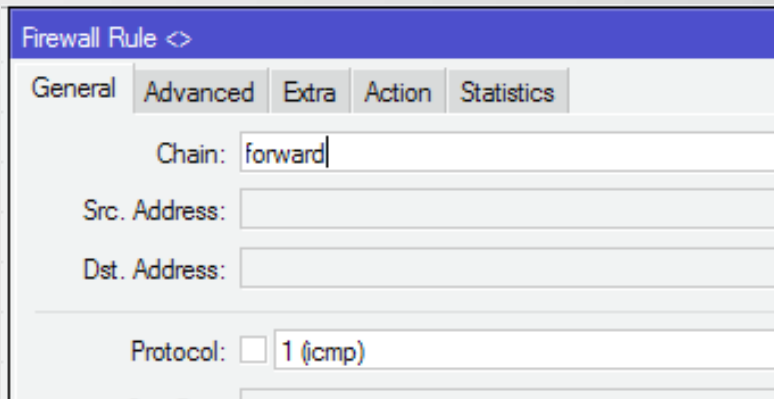
Firewall										
Filter Rules		NAT	Mangle	Service Ports	Connections	Address Lists	Layer7 Protocols			
+		-		✓	✗	📄	🔍	Reset Counters		00 Reset All Counters
#	Action	Chain	Src. Address		In. Inter...	Out. Int...	Bytes	Packets		
0	✓ accept	input	192.168.88.2				77 B	1		
1	✗ drop	input					5.5 KB	67		

- Perhatikan jumlah bytes pada setiap chain rule, tetap ataukah bertambah ketika kita melakukan akses ke router?
- Cobalah masing-masing peserta untuk melakukan ping, akses web, dan remote winbox ke router peserta lain.

LAB – Firewall Logging

Firewall Logging adalah fitur untuk mencatat (menampilkan pada log) aktifitas yang jaringan yang kita inginkan.

- Buat filter rule pada menu IP>Firewall>Filter Rules, untuk logging semua icmp yang mengarah ke interface wlan1,



Firewall Rule <>

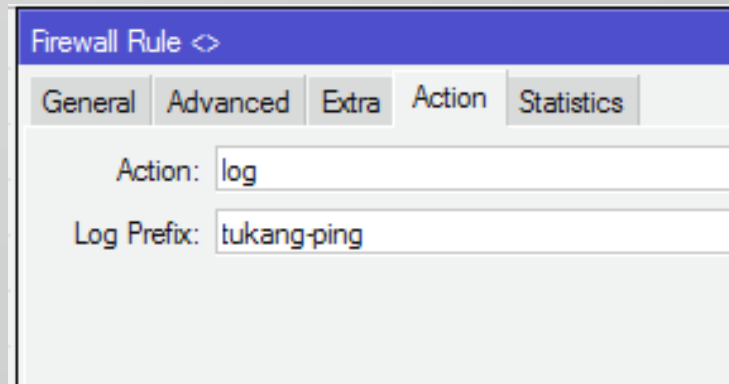
General | Advanced | Extra | Action | Statistics

Chain: forward

Src. Address:

Dst. Address:

Protocol: 1 (icmp)



Firewall Rule <>

General | Advanced | Extra | Action | Statistics

Action: log

Log Prefix: tukang-ping

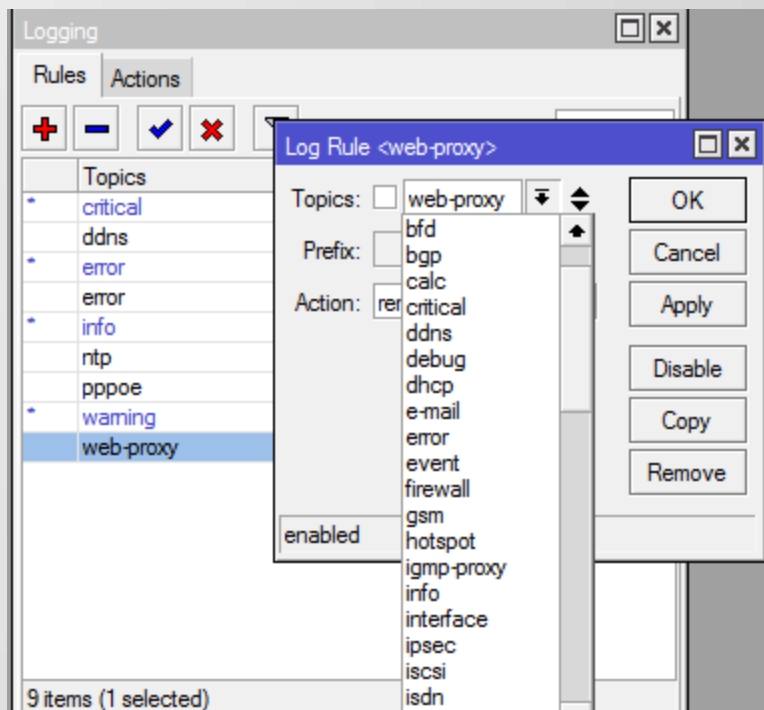
LAB – Firewall Logging

Ping dari laptop IP interface wlan1 dan amati log pada router:

Log		
Time	Level	Message
Jan/01/2002 08:49:53	firewall info	pinger input: in:wlan1 out:(none), src-mac 00:1c:26:13:73:2f, proto ICMP (type 8, code 0), 192.168.1.213->192.168.1.100, len 60
Jan/01/2002 08:49:54	firewall info	pinger input: in:wlan1 out:(none), src-mac 00:1c:26:13:73:2f, proto ICMP (type 8, code 0), 192.168.1.213->192.168.1.100, len 60
Jan/01/2002 08:49:55	firewall info	pinger input: in:wlan1 out:(none), src-mac 00:1c:26:13:73:2f, proto ICMP (type 8, code 0), 192.168.1.213->192.168.1.100, len 60
Jan/01/2002 08:49:56	firewall info	pinger input: in:wlan1 out:(none), src-mac 00:1c:26:13:73:2f, proto ICMP (type 8, code 0), 192.168.1.213->192.168.1.100, len 60
Jan/01/2002 08:49:57	firewall info	pinger input: in:wlan1 out:(none), src-mac 00:1c:26:13:73:2f, proto ICMP (type 8, code 0), 192.168.1.213->192.168.1.100, len 60
Jan/01/2002 08:49:58	firewall info	pinger input: in:wlan1 out:(none), src-mac 00:1c:26:13:73:2f, proto ICMP (type 8, code 0), 192.168.1.213->192.168.1.100, len 60
Jan/01/2002 08:49:59	firewall info	pinger input: in:wlan1 out:(none), src-mac 00:1c:26:13:73:2f, proto ICMP (type 8, code 0), 192.168.1.213->192.168.1.100, len 60
Jan/01/2002 08:50:00	firewall info	pinger input: in:wlan1 out:(none), src-mac 00:1c:26:13:73:2f, proto ICMP (type 8, code 0), 192.168.1.213->192.168.1.100, len 60
Jan/01/2002 08:50:01	firewall info	pinger input: in:wlan1 out:(none), src-mac 00:1c:26:13:73:2f, proto ICMP (type 8, code 0), 192.168.1.213->192.168.1.100, len 60
Jan/01/2002 08:50:02	firewall info	pinger input: in:wlan1 out:(none), src-mac 00:1c:26:13:73:2f, proto ICMP (type 8, code 0), 192.168.1.213->192.168.1.100, len 60

Logging

- Kita dapat mengatur aktivitas atau fitur apa yang akan ditampilkan dalam log.
- Kita juga dapat mengirimkan log ke syslog server tertentu menggunakan default protocol UDP port 514.
- Pengaturan logging ada dalam menu System Logging



Connection Tracking

Firewall

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

Tracking

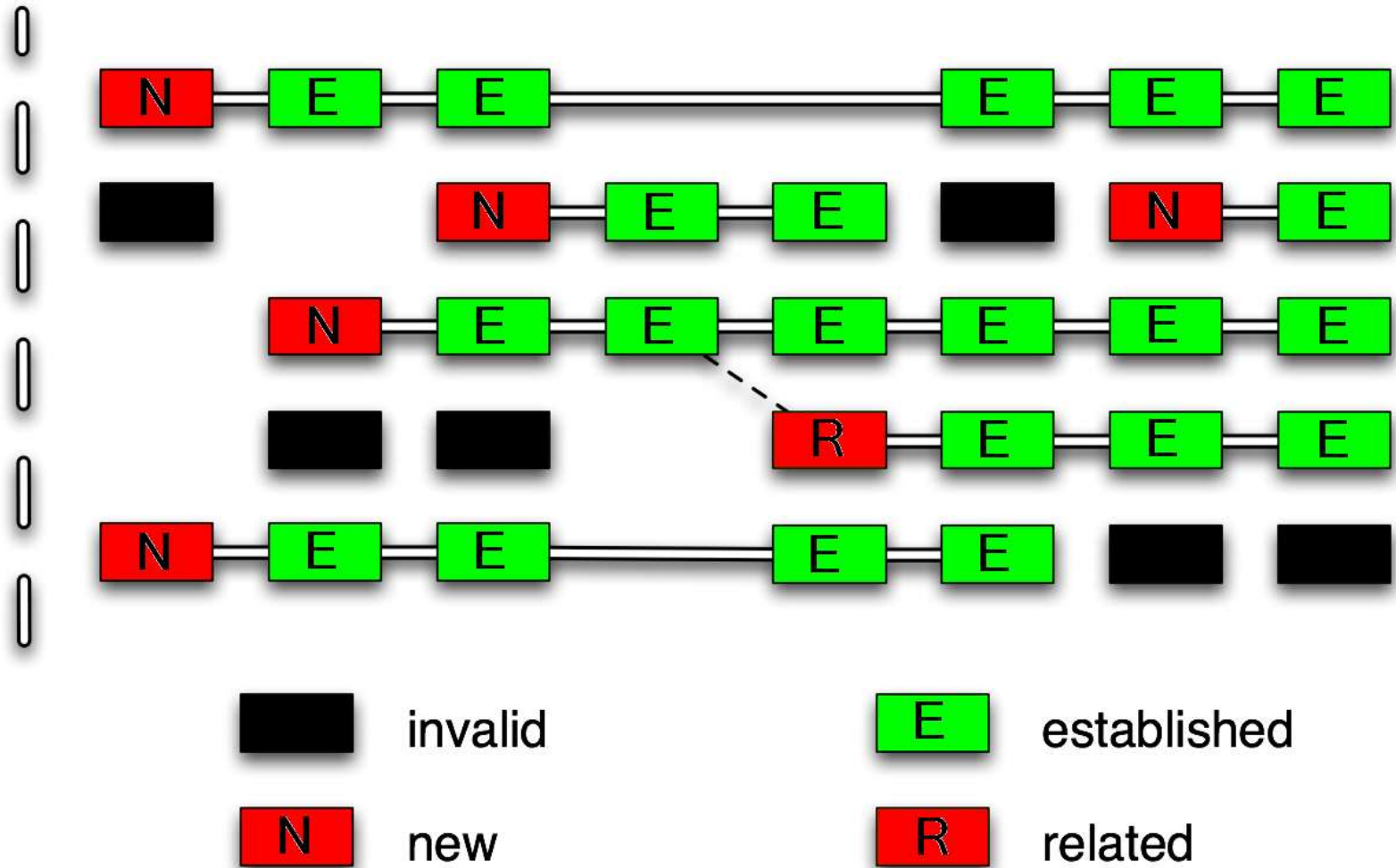
	Src. Address	Dst. Address	Protocol	Connection Type	Connecti...	P2P	Timeout	TCP St...
A	192.168.88.2:15511	203.106.85.232:443	6 (tcp)				00:00:08	time wait
A	192.168.88.2:15513	203.106.85.232:443	6 (tcp)				00:00:07	time wait
U	192.168.88.2:36667	180.235.148.74:56737	6 (tcp)				00:00:01	syn sent
U	192.168.88.2:36667	180.235.148.74:5222	6 (tcp)				00:00:01	syn sent
U	192.168.88.2:36667	180.235.148.74:1063	6 (tcp)				00:00:01	syn sent
U	192.168.88.2:36667	180.235.148.74:3268	6 (tcp)				00:00:01	syn sent
A	192.168.88.2:14505	192.168.88.1:8291	6 (tcp)				00:57:37	established
A	192.168.88.2:15262	69.171.227.53:443	6 (tcp)				23:13:27	established
A	192.168.88.2:15306	69.171.227.53:443	6 (tcp)				23:21:28	established
A	192.168.88.2:15350	69.171.227.53:443	6 (tcp)				23:26:04	established
A	192.168.88.2:15370	69.171.227.53:443	6 (tcp)				23:30:37	established
A	192.168.88.2:15503	69.171.234.96:443	6 (tcp)				23:57:41	established
A	192.168.88.2:15509	203.106.85.232:443	6 (tcp)				23:58:00	established
A	192.168.88.2:15516	180.235.148.74:21	6 (tcp) ftp				23:58:24	established
A	192.168.88.2:15528	69.171.228.76:443	6 (tcp)				23:59:34	established
A	192.168.88.2:15530	173.194.38.181:443	6 (tcp)				23:59:49	established
A	192.168.88.2:15532	199.59.148.20:443	6 (tcp)				23:59:52	established

Connection Tracking

- Connection Tracking dapat dilihat pada menu IP>firewall>connection.
- Connection tracking mempunyai kemampuan untuk melihat informasi koneksi seperti source dan destination IP dan port yang sedang digunakan, status koneksi, tipe protocol, dll.
- Status koneksi pada connection tracking:
 - **established** = *the packet is part of already known connection,*
 - **new** = *the packet starts a new connection or belongs to a connection that has not seen packets in both directions yet,*
 - **related** = *the packet starts a new connection, but is associated with an existing connection, such as FTP data transfer or ICMP error message.*
 - **invalid** = *the packet does not belong to any known connection and, at the same time, does not open a valid new connection.*

Connection Tracking

Firewall

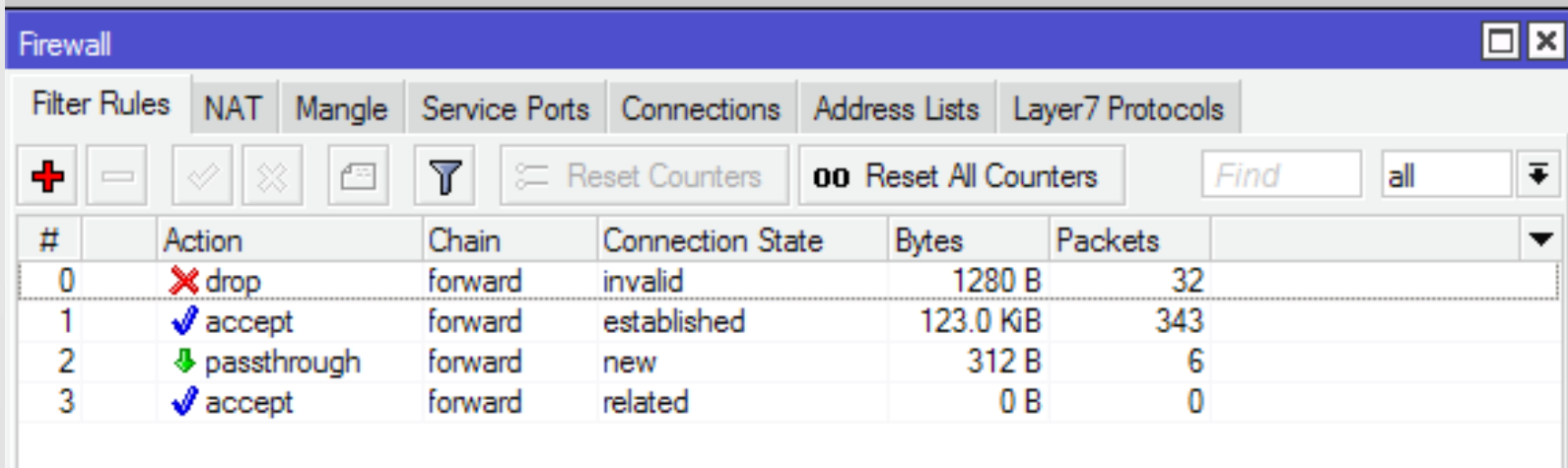


Implementasi Connection Tracking

- Pada saat membuat firewall, pada baris paling atas umumnya akan dibuat rule sebagai berikut:
 - Connection state invalid → Drop
 - Connection state established → Accept
 - Connection state related → Accept
 - Connection state new → Diproses ke rule berikutnya
- System rule ini akan sangat menghemat resource router, karena proses filtering selanjutnya akan dilakukan ketika koneksi dimulai (connection state = new)

LAB – Buatlah Firewall untuk Connection State

- Pada IP>Firewall>Filter Rule buat chain
- Chain Foward
 - Connection state invalid → action Drop
 - Connection state established → action Accept
 - Connection state related → action Accept
 - Connection state new → action pass-through



The screenshot shows the Mikrotik WinBox Firewall configuration interface. The 'Connections' tab is selected, displaying a table of active connections. The table has columns for #, Action, Chain, Connection State, Bytes, and Packets. There are four rows of data:

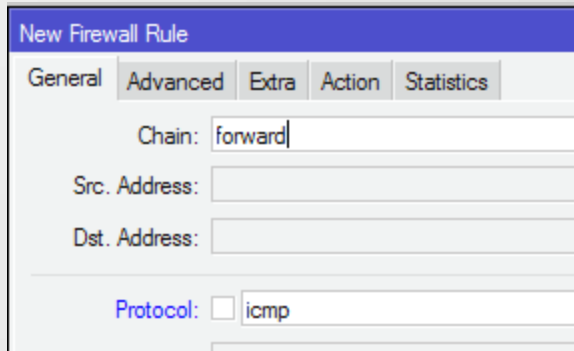
#	Action	Chain	Connection State	Bytes	Packets
0	drop	forward	invalid	1280 B	32
1	accept	forward	established	123.0 KiB	343
2	passthrough	forward	new	312 B	6
3	accept	forward	related	0 B	0

Firewall – Address List

- Address-list digunakan untuk memfilter group IP address dengan 1 rule firewall.
- Address-list juga bisa merupakan list IP hasil dari rule firewall yang memiliki action “add to address list”
- Satu line address-list dapat berupa subnet, range, atau 1 host IP address

LAB– Address List

- Buat rule firewall untuk memasukkan setiap IP yang melakukan ping ke dalam address-list dan beri nama address list “tukang-ping”.



New Firewall Rule

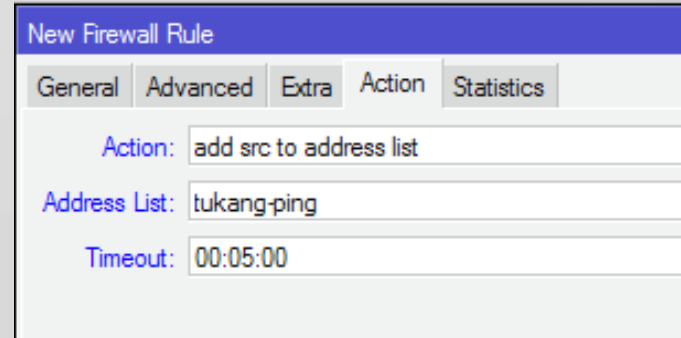
General | Advanced | Extra | Action | Statistics

Chain: forward

Src. Address:

Dst. Address:

Protocol: icmp



New Firewall Rule

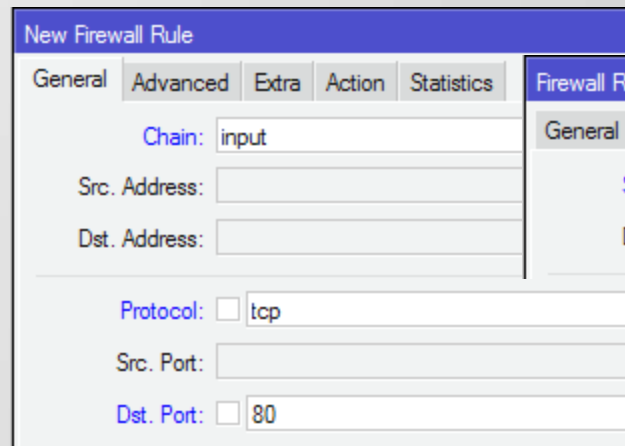
General | Advanced | Extra | Action | Statistics

Action: add src to address list

Address List: tukang-ping

Timeout: 00:05:00

- Kemudian buat rule untuk blok browsing (port 80) yang berasal dari address-list “tukang-ping”



New Firewall Rule

General | Advanced | Extra | Action | Statistics

Chain: input

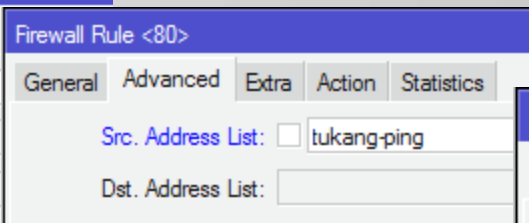
Src. Address:

Dst. Address:

Protocol: tcp

Src. Port:

Dst. Port: 80

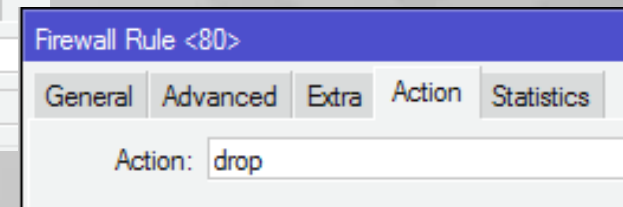


Firewall Rule <80>

General | Advanced | Extra | Action | Statistics

Src. Address List: tukang-ping

Dst. Address List:



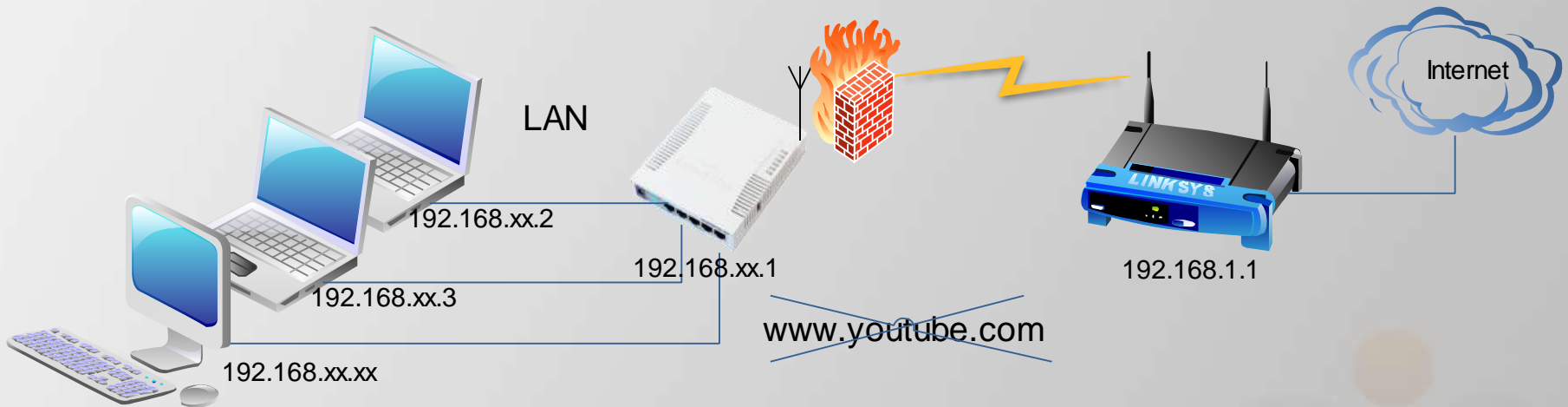
Firewall Rule <80>

General | Advanced | Extra | Action | Statistics

Action: drop

LAB – Block Situs Porno

Kita akan block akses dari LAN ke situs tertentu, misal youtube



LAB – Block Situs Porno

- Sebelumnya kita harus mengetahui IP server dari youtube, gunakan perintah nslookup pada MSDOS untuk mengetahui IP-IP yang dipake oleh domain youtube.com
- Atau bisa juga ping ke domain www.youtube.com

```

Command Prompt - nslookup
C:\Documents and Settings\Admin>nslookup
Default Server:  router
Address:  192.168.88.1

> youtube.com
Server:  router
Address:  192.168.88.1

Non-authoritative answer:
Name:    youtube.com
Addresses:  209.85.175.190, 209.85.175.91, 209.85.175.93, 209.85.175.136
  
```

```

Command Prompt
C:\Documents and Settings\Admin>ping youtube.com

Pinging youtube.com [209.85.175.91] with 32 bytes of data:

Reply from 209.85.175.91: bytes=32 time=50ms TTL=52
Reply from 209.85.175.91: bytes=32 time=50ms TTL=52
Reply from 209.85.175.91: bytes=32 time=52ms TTL=52
Reply from 209.85.175.91: bytes=32 time=50ms TTL=52
  
```

LAB – Block Situs Porno

- Buatlah Filter Rule, Chain=forward, Dst. Address = 209.85.175.91, Action = drop.
- Ulangi untuk semua IP youtube.

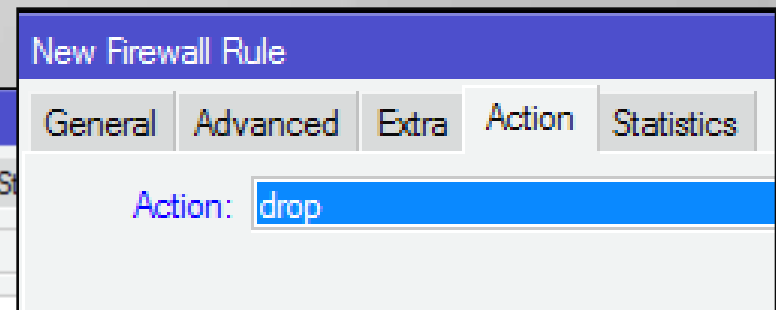
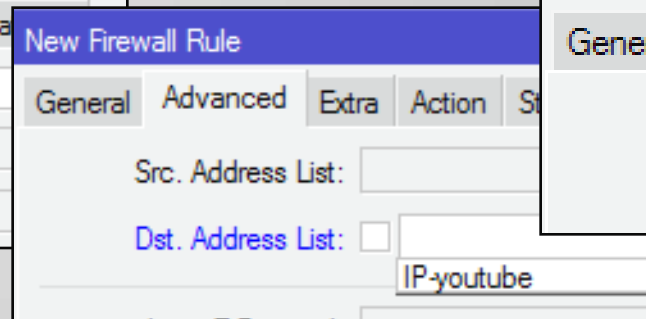
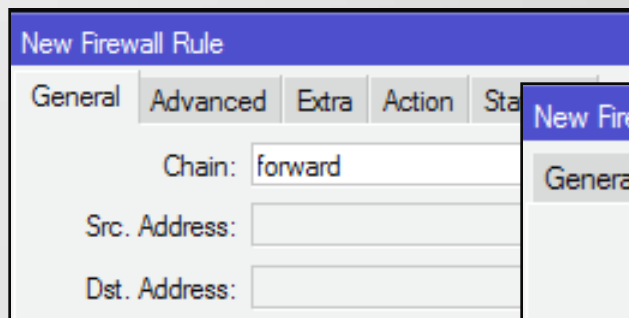
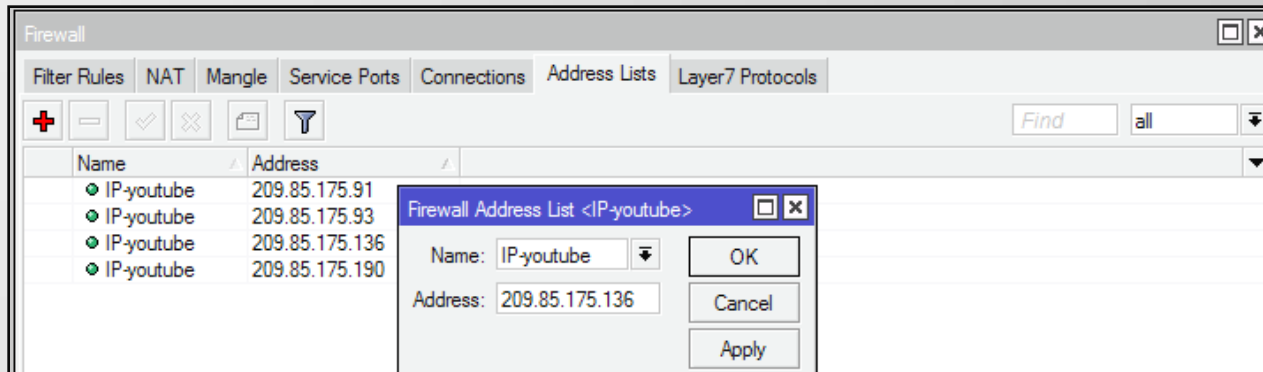
Firewall Rule <209.85.175.91>	
General	Advanced
Chain:	forward
Src. Address:	
Dst. Address:	<input type="checkbox"/> 209.85.175.91

New Firewall Rule	
General	Advanced
Action:	drop

- Coba browsing kembali ke youtube.com

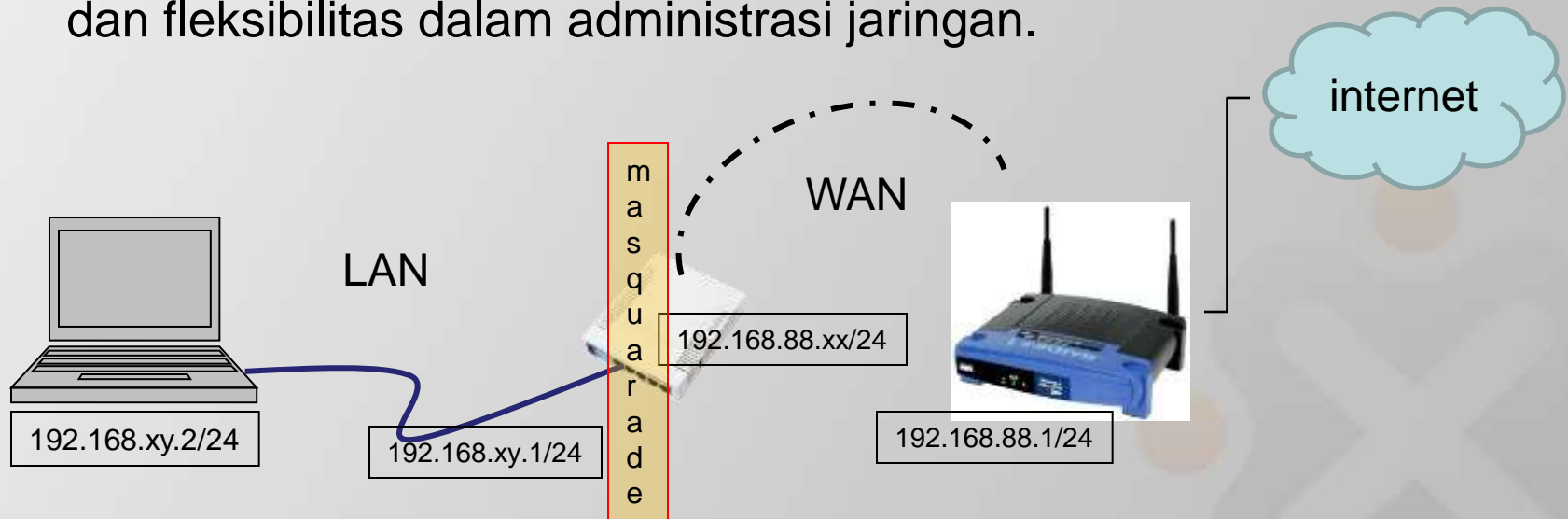
LAB – Block Situs Porno

- Kita juga dapat melakukan bloking situs menggunakan address-list
- Daftarkan semua IP youtube ke address-list dan beri nama misal “ip-youtube”
- Kemudian buat firewall rule untuk block address-list ip-youtube



NAT - Masquarade

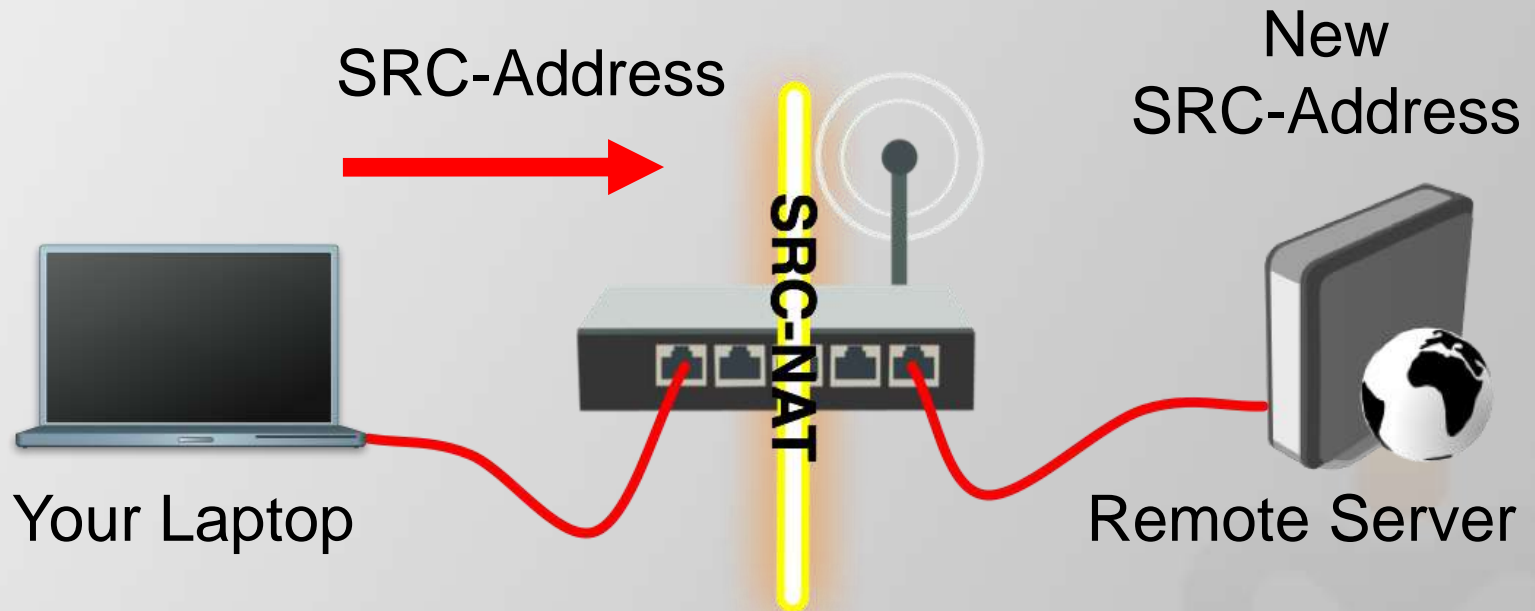
- NAT adalah suatu metode untuk menghubungkan banyak komputer ke jaringan internet dengan menggunakan satu atau lebih alamat IP.
- NAT digunakan karena ketersediaan alamat IP public.
- NAT juga digunakan untuk alasan keamanan (security), kemudahan dan fleksibilitas dalam administrasi jaringan.



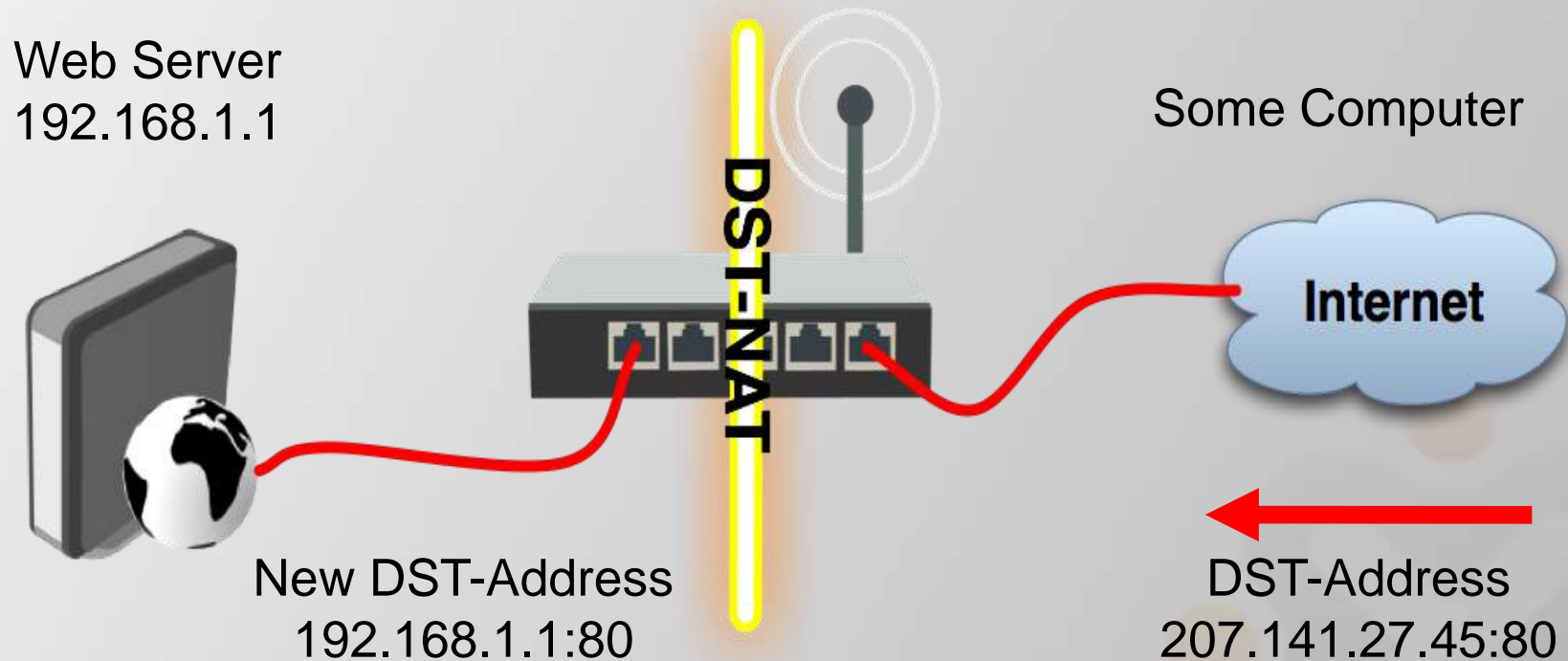
NAT

- Ada dua type NAT dalam Firewall MikroTik
- **source NAT or srcnat** → diberlakukan untuk paket yang berasal dari Network yang di NAT (privat/local network)
- **destination NAT or dstnat** → diberlakukan untuk paket yang menuju jaringan yang di NAT, biasanya digunakan untuk mengakses dari luar beberapa service pada jaringan.

srcNAT

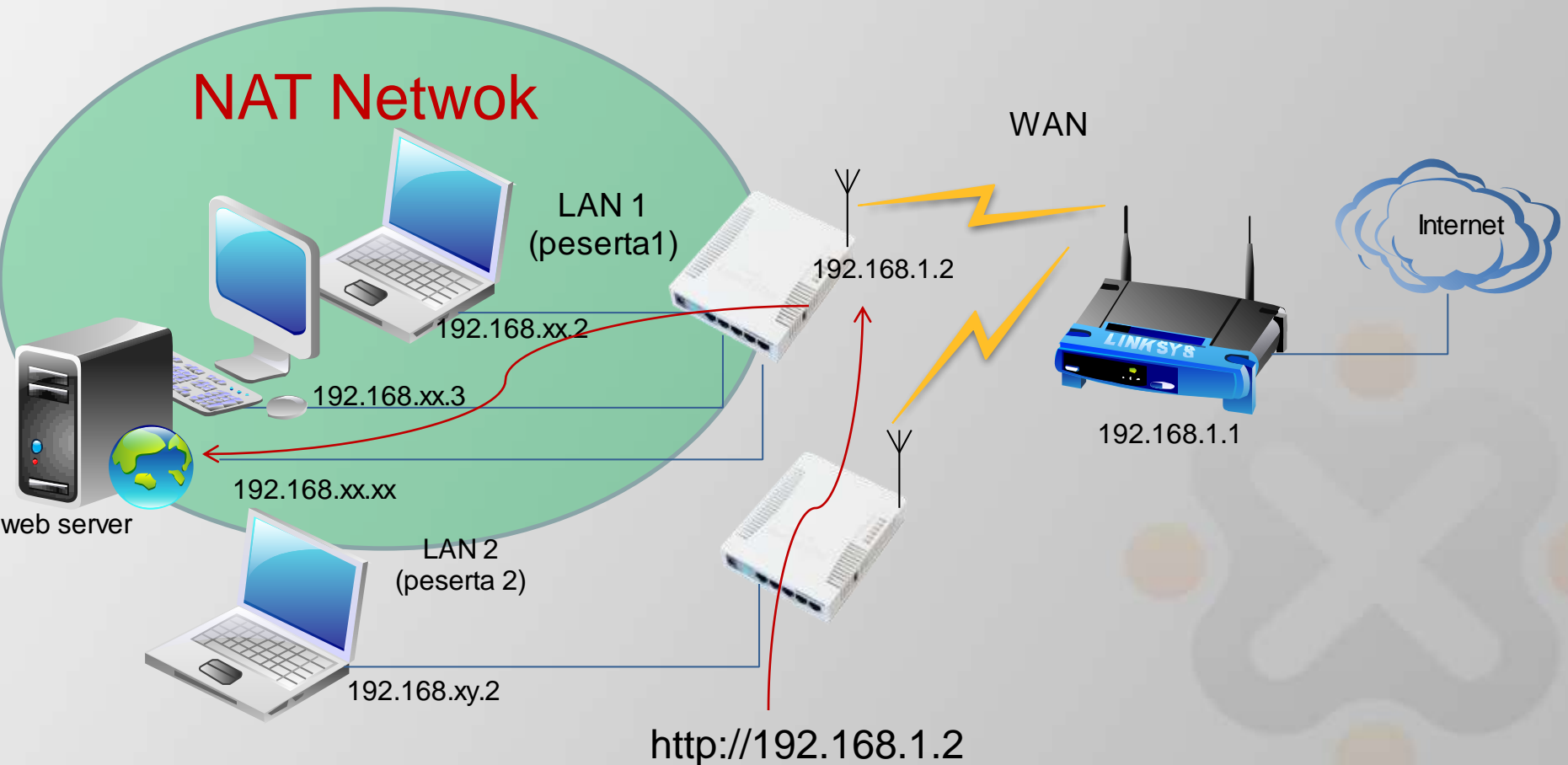


dstNAT



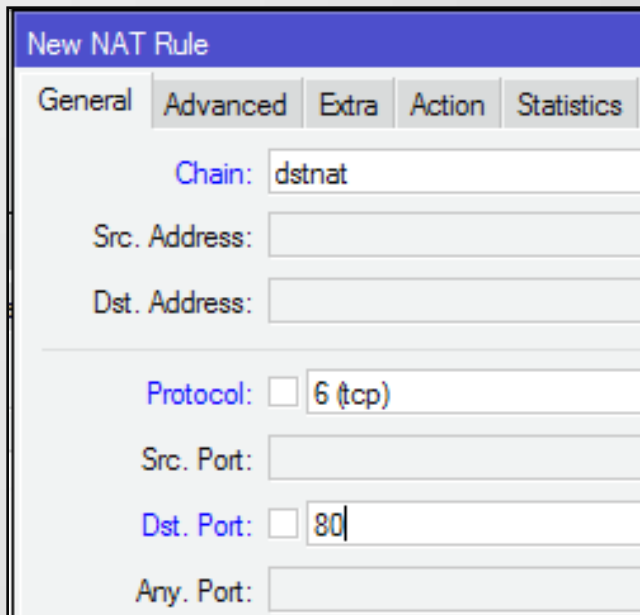
LAB- DstNAT

Redirect port http IP WAN router ke IP web server lokal (LAN)



LAB – DMZ Web Server

- Install dan Jalankan program web server di salah satu laptop peserta (LAN).
- Buat rule pada IP>Firewall>NAT untuk redirect port 80 router ke IP address dan port web server lokal.



New NAT Rule

General | Advanced | Extra | Action | Statistics

Chain: dstnat

Src. Address:

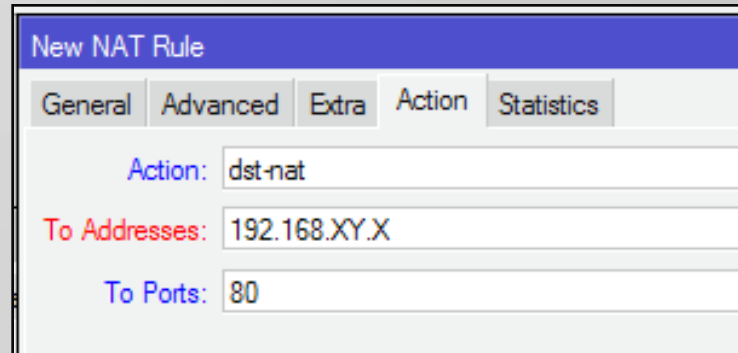
Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port: 80

Any. Port:



New NAT Rule

General | Advanced | Extra | Action | Statistics

Action: dst-nat

To Addresses: 192.168.XY.X

To Ports: 80

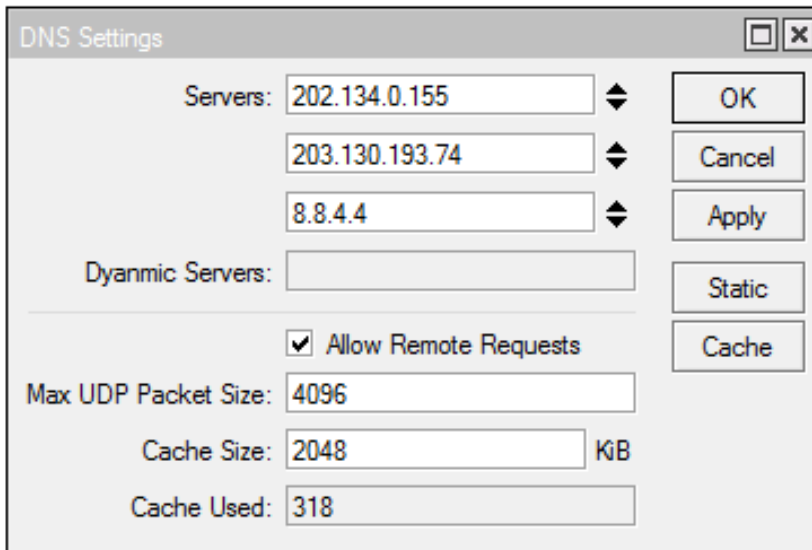
- Coba dengan mengakses router LAN 1 dari LAN2 melalui browser

DNS

- DNS (Domain Name System) berfungsi untuk menterjemahkan nama domain menjadi IP address.
- Kita lebih mudah mengingat nama domain (detik.com) dibanding dengan IP addressnya (203.190.241.43).
- DNS memiliki database/cache alamat domain dan IP address yang diperoleh dari primary DNS di atasnya.
- Client yang menggunakan DNS server akan menggunakan cache tersebut.
- Pada periode tertentu chache akan diperbaharui mengambil dari DNS server di atasnya.

LAB - Static DNS

- Kita dapat memanipulasi cache DNS yang ada dengan static entry pada tabel DNS.
- Misal apabila kita menambahkan domain detik.com, IP addressnya 192.168.88.1, maka apabila client yang menggunakan DNS tersebut mengakses detik.com akan dibelokkan ke alamat IP 192.168.88.1



DNS Settings

Servers: 202.134.0.155
 203.130.193.74
 8.8.4.4

Dyanmic Servers:

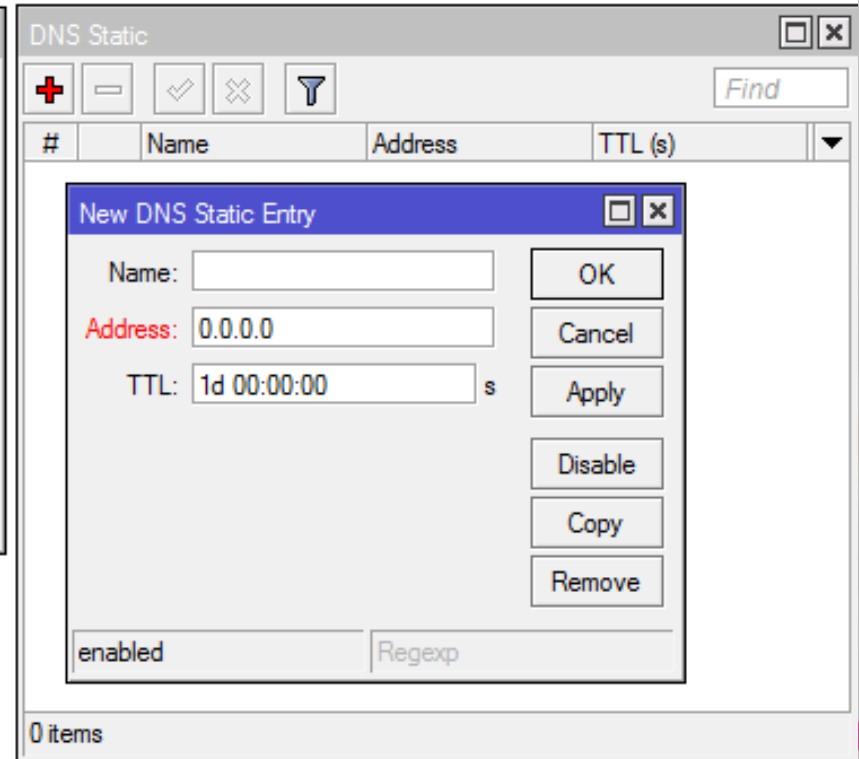
Allow Remote Requests

Max UDP Packet Size: 4096

Cache Size: 2048 KB

Cache Used: 318

OK
 Cancel
 Apply
 Static
 Cache



DNS Static

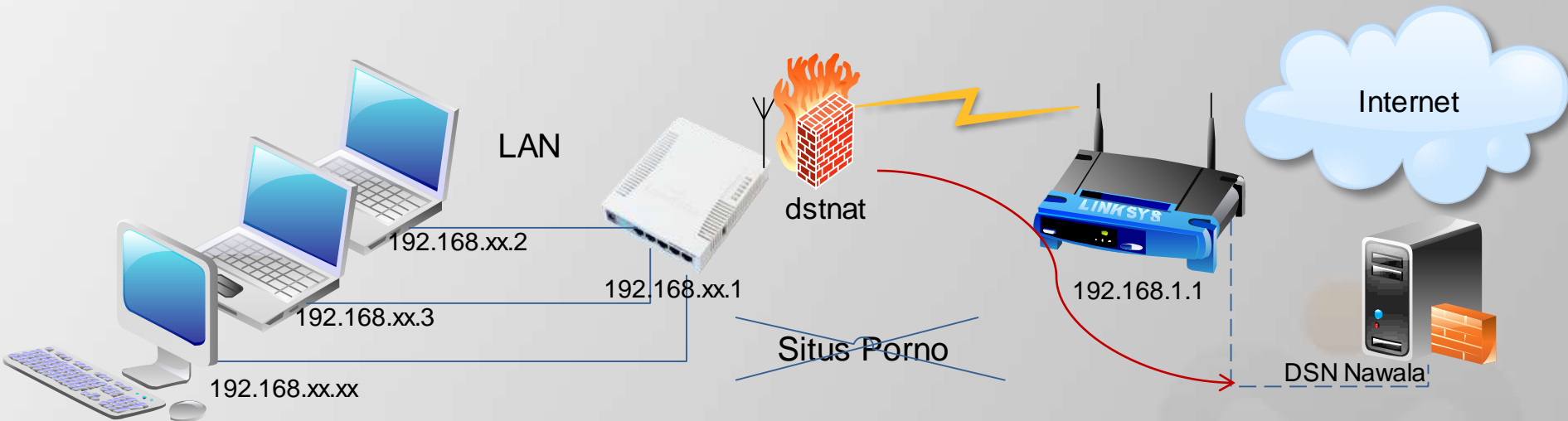
+ - ✓ ✕ 🔍 Find

#	Name	Address	TTL (s)
<div data-bbox="1052 835 1671 1335"> <p>New DNS Static Entry</p> <p>Name: <input type="text"/></p> <p>Address: 0.0.0.0</p> <p>TTL: 1d 00:00:00 s</p> <p>OK Cancel Apply Disable Copy Remove</p> <p>enabled Regexp</p> </div>			

0 items

LAB-Transparent DNS

- Kita akan melakukan block situs porno dengan transparent DNS Nawala



LAB – Transparent DNS

- Transparent DNS memaksa user untuk akses DNS server tertentu
- Buatlah rule baru pada menu IP>Firewall>NAT , redirect protocol TCP dan UDP port 53 ke IP port DNS Nawala 180.131.144.144

NAT Rule <53>

General Advanced Extra Action Statistics

Chain: dstnat

Src. Address:

Dst. Address:

Protocol: 17 (udp)

Src. Port:

Dst. Port: 53

NAT Rule <53>

General Advanced Extra Action Statistics

Action: dst-nat

To Addresses: 180.131.144.144

To Ports: 53

- Coba dengan mengakses router LAN 1 dari LAN2 melalui browser

Module 3 - Wireless

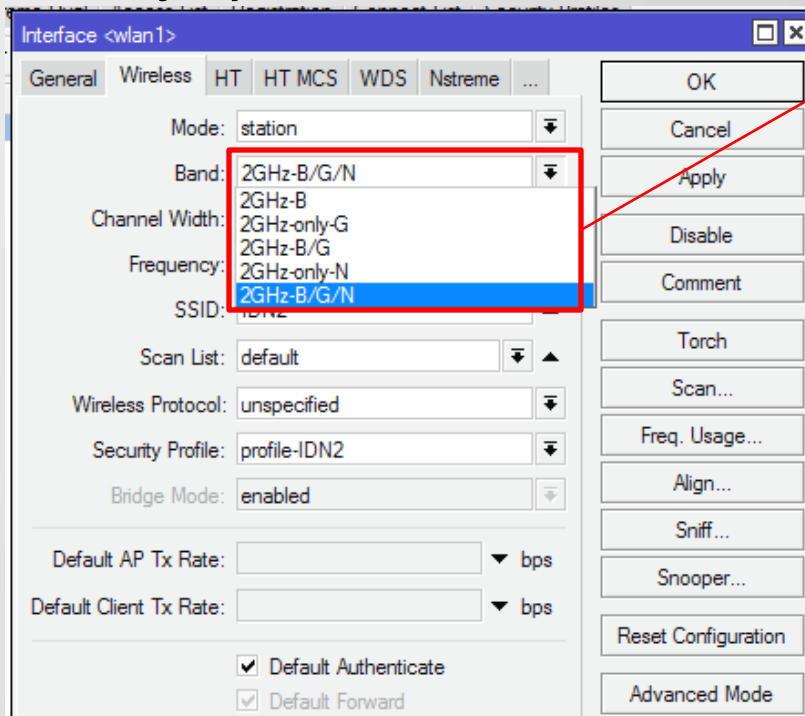


Wireless pada Mikrotik

- RouterOS mendukung beberapa modul radio (wireless card) untuk jaringan WLAN atau Wi-Fi (Wireless Fidelity).
- Wi-Fi memiliki standar & spesifikasi IEEE 802.11 dan menggunakan frekuensi 2,4GHz dan 5GHz.
- MikroTik mendukung standar IEEE 802.11a/b/g/n
 - 802.11a – frekuensi 5GHz, 54Mbps.
 - 802.11b – frekuensi 2,4GHz, 11 Mbps.
 - 802.11g – frekuensi 2,4GHz, 54Mbps.
 - 802.11n (Level 4 keatas) – frekuensi 2,4GHz atau 5GHz, 300Mbps

Wireless Band

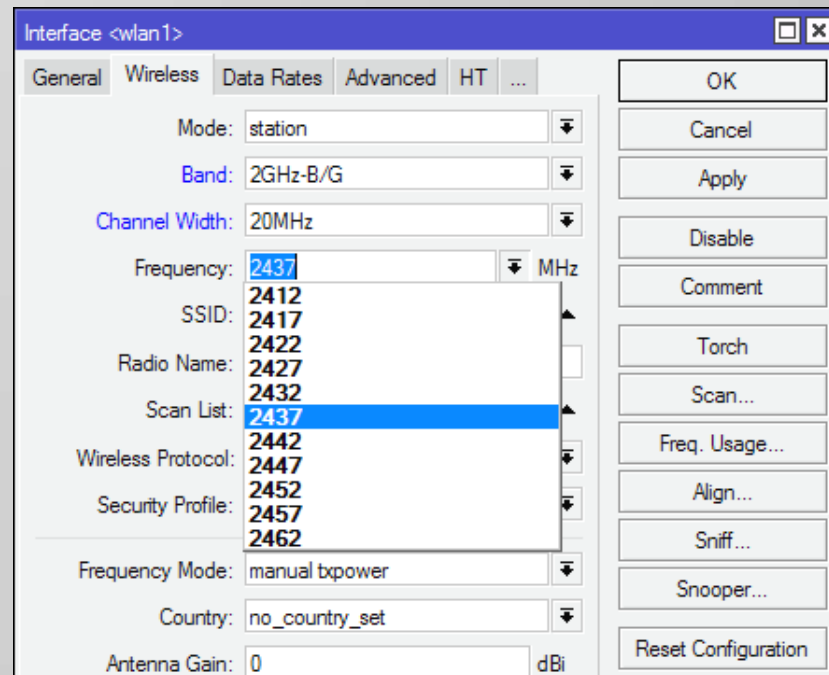
- Band merupakan mode kerja frekuensi dari suatu perangkat wireless.
- Untuk menghubungkan 2 perangkat, keduanya harus bekerja pada band frekuensi yang sama



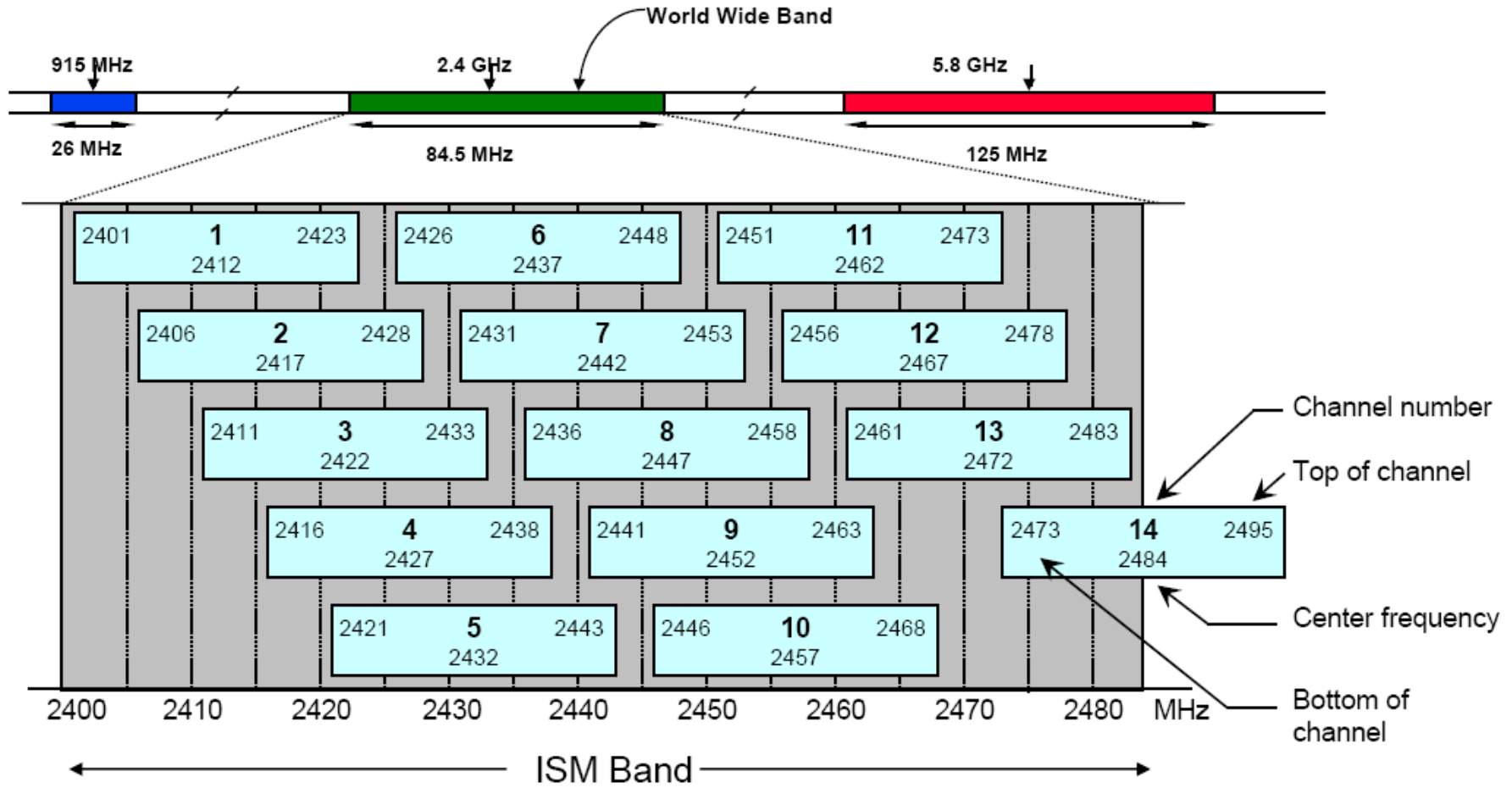
Band yang ada di list, bergantung pada jenis wireless card yang digunakan.

Wireless – Frequency Channel

- Frequency channel adalah pembagian frekuensi dalam suatu band dimana Access Point (AP) beroperasi.
- Nilai-nilai channel bergantung pada band yang dipilih, **kemampuan wireless card**, dan **aturan/regulasi frekuensi suatu negara**.
- Range frequency channel untuk masing-masing band adalah sbb:
 - 2,4Ghz = 2412 s/d 2499MHz
 - 5GHz = 4920 s/d 6100MHz

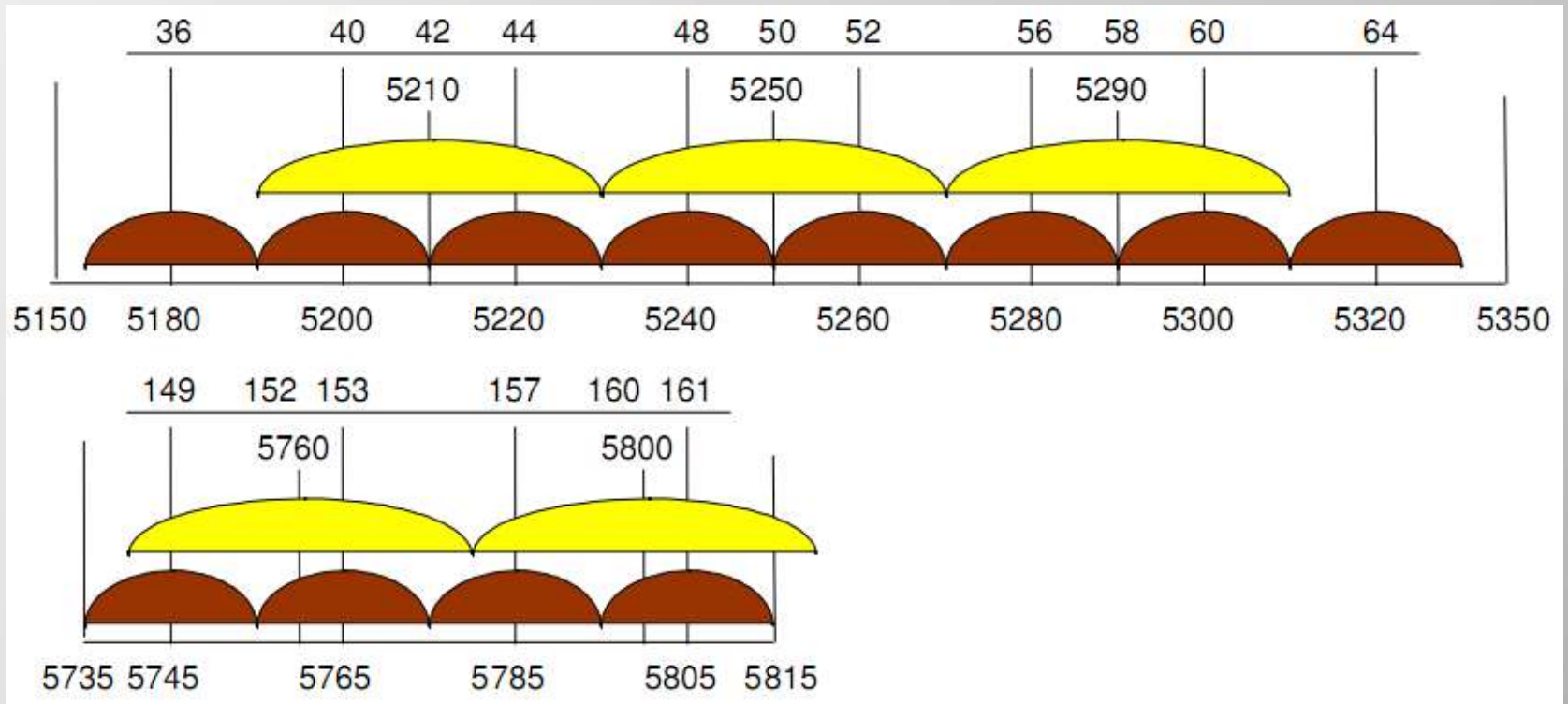


802.11 b/g Channels



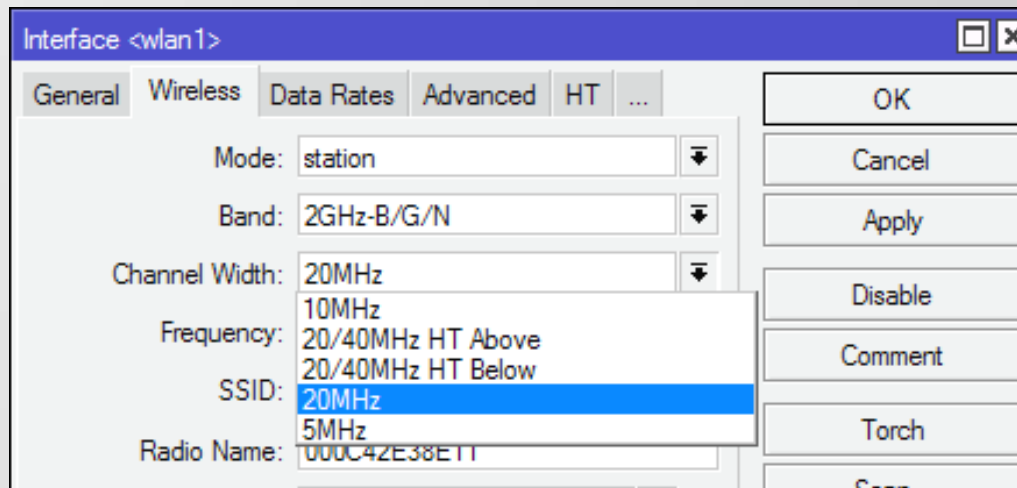
IEEE 802.11a - 5GHz

- IEEE 802.11a - 5GHz frequencies, 54Mbps



Wireless – Lebar Channel

- Lebar channel adalah rentang frekuensi batas bawah dan batas atas dalam 1 channel.
- MikroTik dapat mengatur berapa lebar channel yang akan digunakan.
- Default lebar channel yang digunakan adalah 20Mhz (ditulis 20MHz).
- Lebar channel dapat dikecilkan (5MHz) untuk meminimasil frekuensi, atau dibesarkan (40MHz) untuk mendapatkan trougthput yang lebih besar.

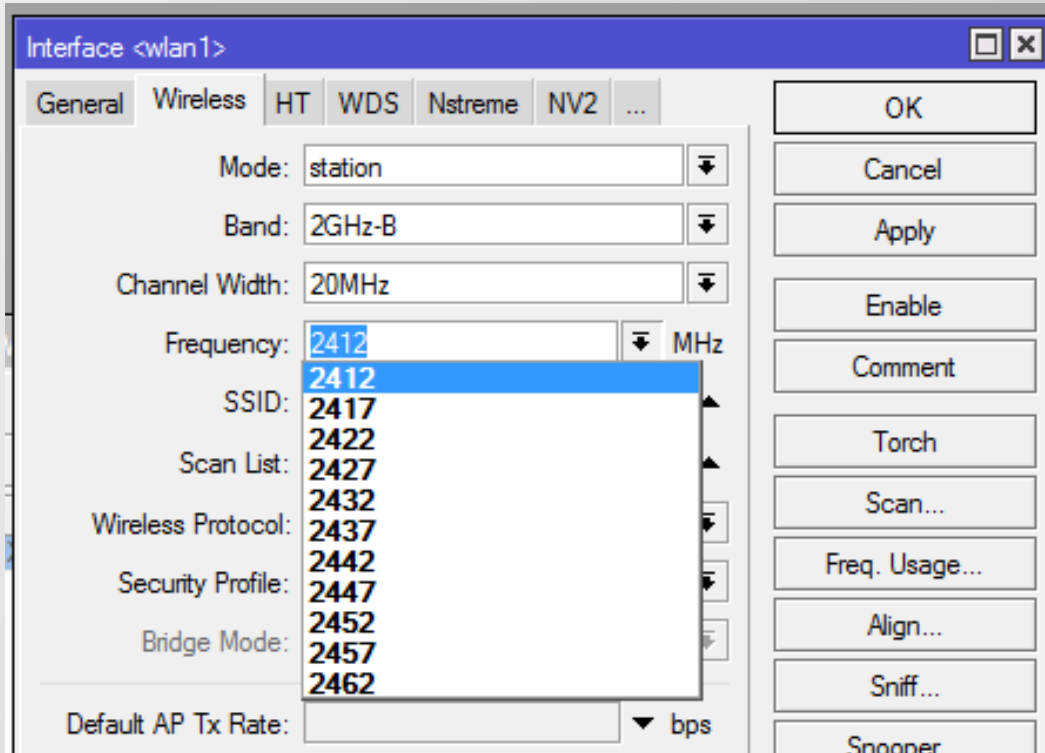


Wireless – Regulasi Frekuensi

- Setiap negara memiliki regulasi tertentu dalam hal frekuensi wireless untuk internet carrier.
- Indonesia telah merdeka untuk menggunakan frekuensi 2.4GHz berdasarkan KEPMENHUB No. 2/2005 berkat perjuangan para penggerak internet sejak tahun 2001
- Regulasi tersebut dalam mikrotik didefinisikan pada bagian Wireless “country-regulation”.
- Namun apabila diinginkan untuk membuka semua frekuensi yang dapat digunakan oleh wireless card, dapat menggunakan pilihan “**superchannel**”.

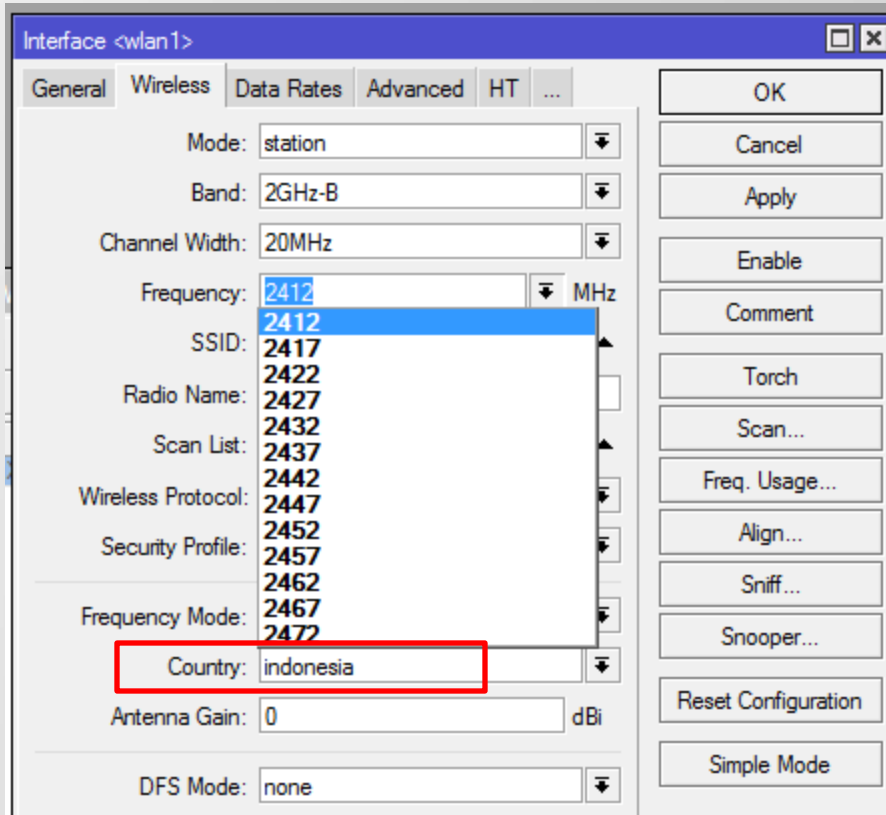
LAB-Regulasi Frekuensi

- Ada berapa channel frekuensi default MikroTik?
- Lihatnya di menu Wireless Wlan1 Wireless



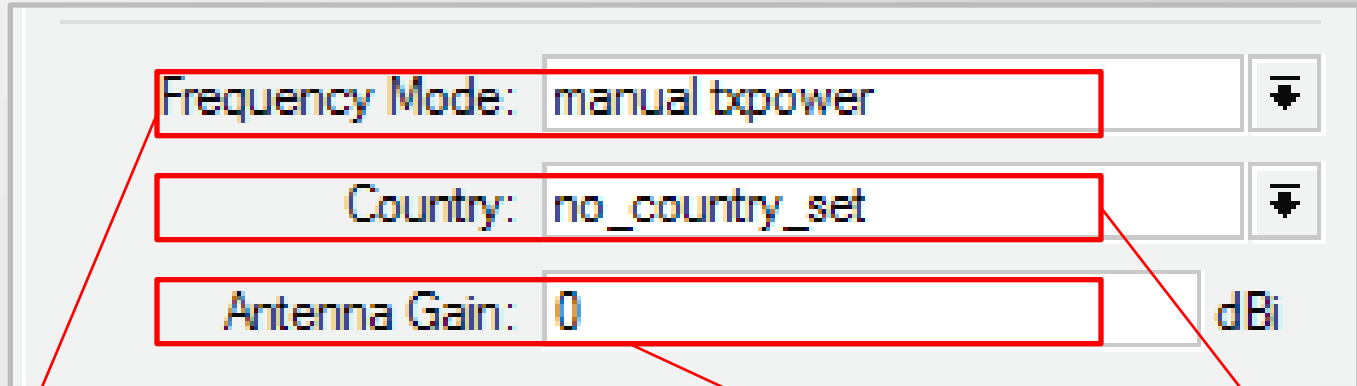
LAB-Regulasi Frekuensi

- Ada berapa channel frekuensi untuk country regulation Indonesia?
- Lihatnya di menu Wireless Wlan1 Wireless Advanced Mode



Coba ganti Frekuensi
 Mode = Superchannel

LAB-Regulasi Frekuensi



Frequency Mode: ▾

Country: ▾

Antenna Gain: dBm

Frequency Mode

1. manual-tx-power
Transmit power diatur manual (tidak menyesuaikan dengan negara tertentu).
2. regulation-domain
Frekuensi channel disesuaikan dengan frekuensi-frekuensi yang diijinkan di suatu negara.
3. Superchannel
Membuka semua frekuensi yang bisa disupport oleh wireless card

Pemilihan Country / Negara

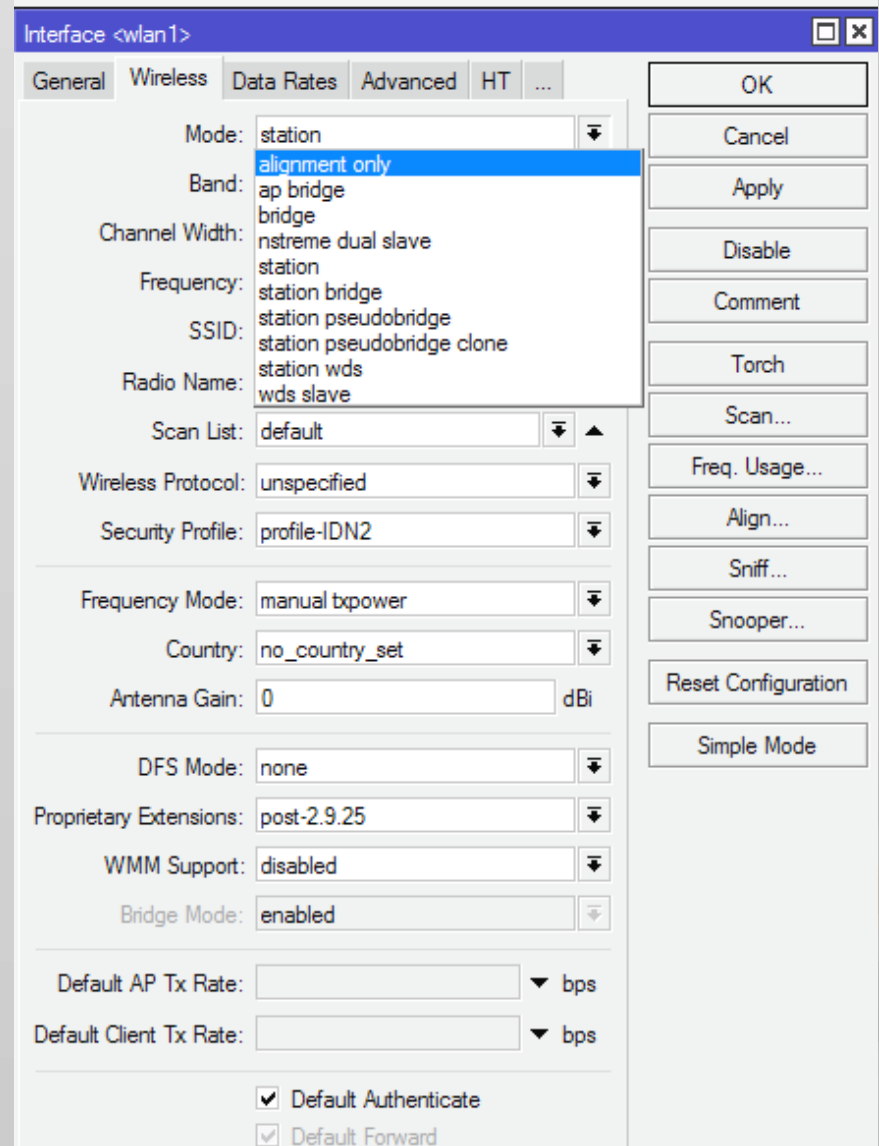
Default 0, akan otomatis menyesuaikan agar tidak melebihi EIRP country regulation

Konsep Koneksi Wireless

- Koneksi terjadi antara Akses Point (AP) dengan satu atau lebih station.
- Koneksi antar WDS-Slave dengan WDS-Slave
- Koneksi terjadi apabila ada kesamaan SSID dan kesamaan Band.
- Station secara otomatis akan mengikuti channel frekuensi pada AP.
- Station hanya dapat melakukan scan AP dengan list channel frekuensi yang diset pada station.

Mode Interface Wireless

- Aligement Only
- AP Bridge
- Bridge
- Nstream dual slave
- Station
- Station bridge
- Station pseudobridge
- Station pseudobridge clone
- Station wds
- Wds slave



Interface <wlan 1>

General Wireless Data Rates Advanced HT ...

Mode: station
 alignment only
 ap bridge
 bridge
 nstream dual slave
 station
 station bridge
 station pseudobridge
 station pseudobridge clone
 station wds
 wds slave

Band: ap bridge

Channel Width: nstream dual slave

Frequency: station

SSID: station bridge

Radio Name: station pseudobridge
 station pseudobridge clone
 station wds
 wds slave

Scan List: default

Wireless Protocol: unspecified

Security Profile: profile-IDN2

Frequency Mode: manual txpower

Country: no_country_set

Antenna Gain: 0 dBi

DFS Mode: none

Proprietary Extensions: post-2.9.25

WMM Support: disabled

Bridge Mode: enabled

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate
 Default Forward

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

Mode Interface Wireless

AP Mode

- **AP-bridge** – wireless difungsikan sebagai Akses Poin.
- **Bridge** - hampir sama dengan AP-bridge, namun hanya bisa dikoneksi oleh 1 station/client, mode ini biasanya digunakan untuk point-to-point.

Station Mode

- **Station** – scan dan content AP dengan frekuensi & SSID yang sama, mode ini TIDAK DAPAT di BRIDGE
- **Station-bridge** – sama seperti station, mode ini adalah MikroTik proprietary. Mode untuk L2 bridging, selain wds.
- **Station-wds** – sama seperti station, namun membentuk koneksi WDS dengan AP yang menjalankan WDS.
- **station-pseudobridge** – sama seperti *station*, dengan tambahan MAC address translation untuk bridge.
- **station-pseudobridge-clone** – Sama seperti *station-pseudobridge*, menggunakan **station-bridge-clone-mac** address untuk konek ke AP.

Interface Wireless Mode

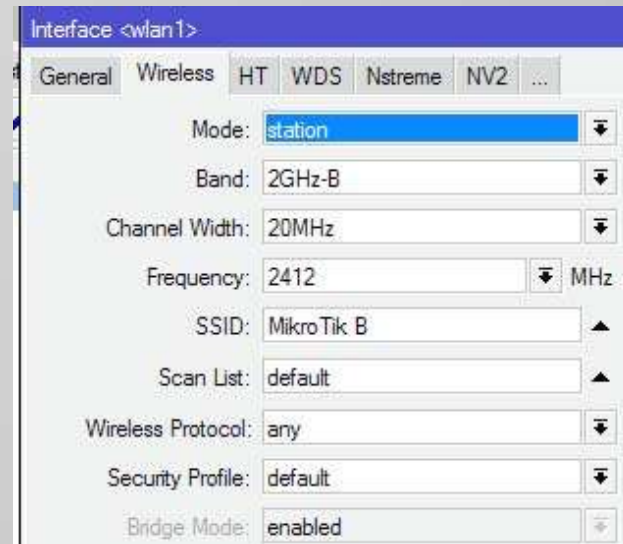
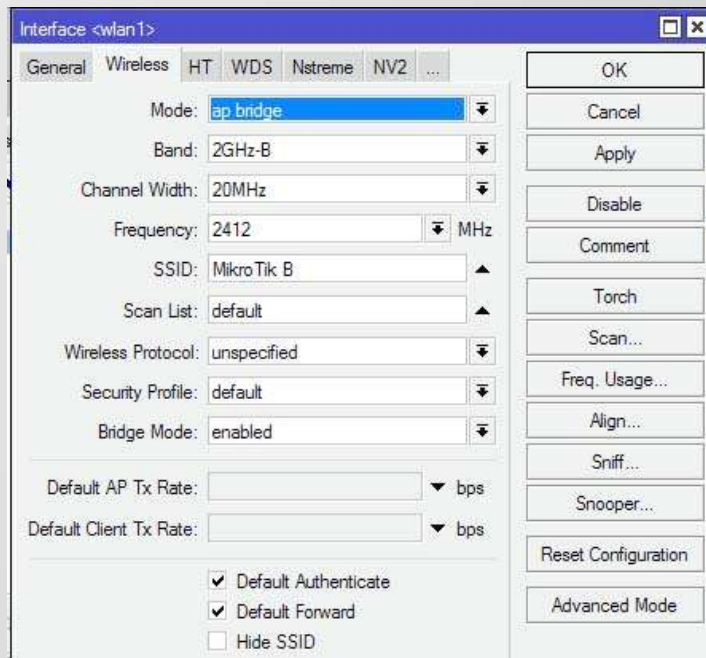
Special Mode

- **alignment-only** – mode transmit secara terus-menerus digunakan untuk positioning antenna jarak jauh.
- **nstreme-dual-slave** – digunakan untuk sistem nstreme-dual.
- **WDS-slave** - Sama seperti ap-bridge, namun melakukan scan ke AP dengan SSID yang sama dan melakukan koneksi dengan WDS. Apabila link terputus, akan melanjutkan scanning.

LAB – Wireless AP & Station



- Salah satu menjadi AP, salah satu station

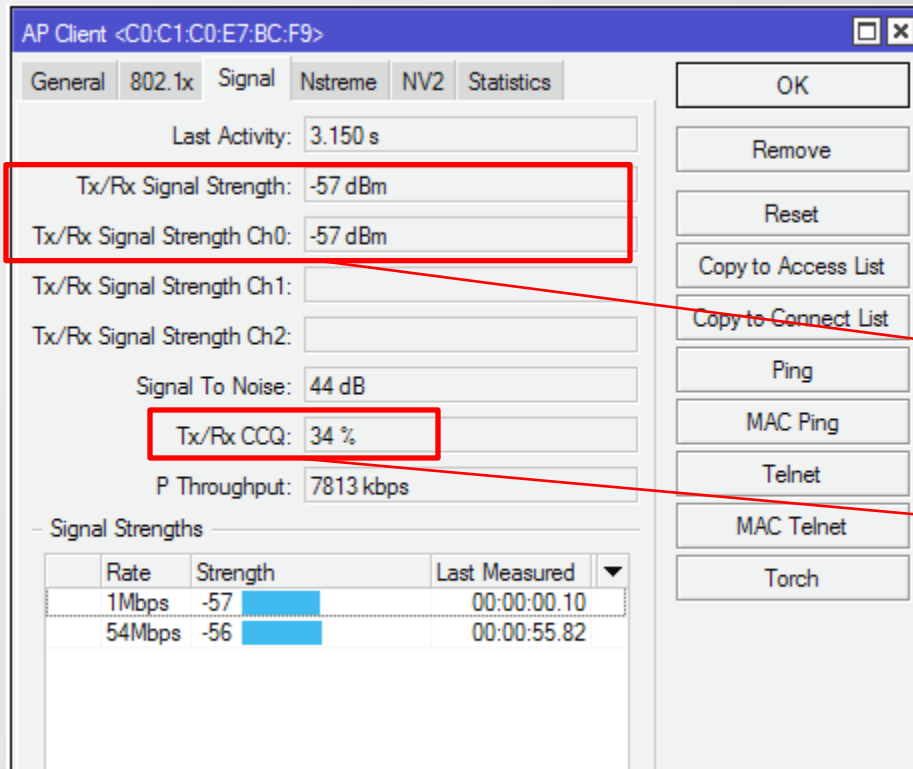


LAB – Wireless AP & Station

- Samakan SSID, band dan frekuensi.
- Setting IP Address interface wlan:
IP AP= 10.10.10.1/24
IP station = 10.10.10.2/24
- Pastikan koneksi layer 1 (wireless) terhubung, baru cek koneksi layer 3 (ping IP address)
- Lakukan ping dari masing-masing MikroTik.

LAB – Wireless AP & Station

- Coba gantilah frekuensi untuk mendapatkan signal terbaik.



AP Client <C0:C1:C0:E7:BC:F9>

General 802.1x Signal Nstreme NV2 Statistics

Last Activity: 3.150 s

Tx/Rx Signal Strength: -57 dBm

Tx/Rx Signal Strength Ch0: -57 dBm

Tx/Rx Signal Strength Ch1:

Tx/Rx Signal Strength Ch2:

Signal To Noise: 44 dB

Tx/Rx CCQ: 34 %

P Throughput: 7813 kbps

Signal Strengths

Rate	Strength	Last Measured
1Mbps	-57	00:00:00.10
54Mbps	-56	00:00:55.82

Signal yang dikirim dan diterima oleh antenna

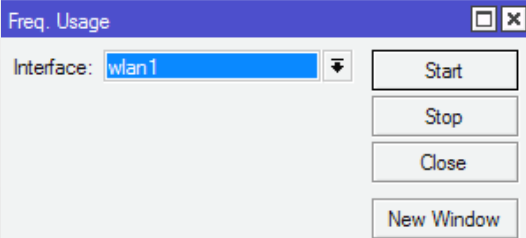
Client Connection Quality (CCQ) yaitu nilai yang menyatakan seberapa efektifkah kapasitas bandwidth yang dapat digunakan

Wireless Tools

- Ada beberapa tool dalam wireless MikroTik yang dapat digunakan untuk optimasi link.
 - **Scan** – untuk melihat informasi AP yang aktif, beserta SSID dan memudahkan untuk membuat koneksi ke AP aktif tersebut.
 - **Align** – untuk pointing antenna.
 - **Sniff** – untuk melihat lalu lintas paket data di jaringan.
 - **Snooper** – seperti tool scan, informasi AP yang aktif secara lengkap, SSID, channel yang digunakan, signal strength, utilisasi/traffic load dan jumlah station pada masing-masing AP.
 - **Bw Test** – digunakan untuk test bandwidth khusus untuk MikroTik, bw test dapat didownload di web resmi MikroTik.

LAB – Wireless Tools

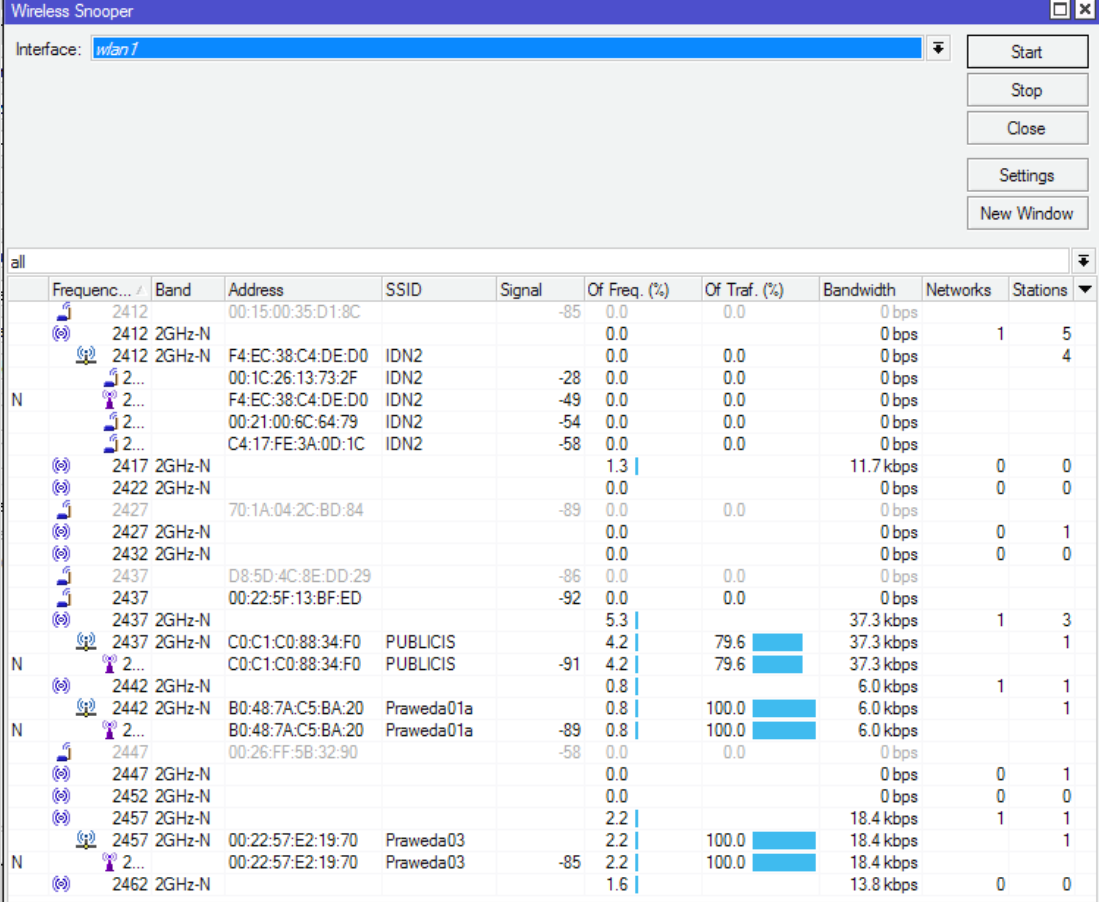
- Gunakan tool Frequency Use dan Snooper untuk pemilihan channel yang optimum, serta lakukan bandwidth test.



Interface: wlan1

Start
Stop
Close
New Window

Frequency (MHz)	Usage	Noise F...
2412	1.9	-101
2417	2.6	-102
2422	0.0	-102
2427	0.0	-102
2432	0.0	-101
2437	1.7	-100
2442	0.0	-101
2447	0.0	-99
2452	0.0	-103
2457	11.6	-103
2462	1.7	-103



Interface: wlan1

Start
Stop
Close
Settings
New Window

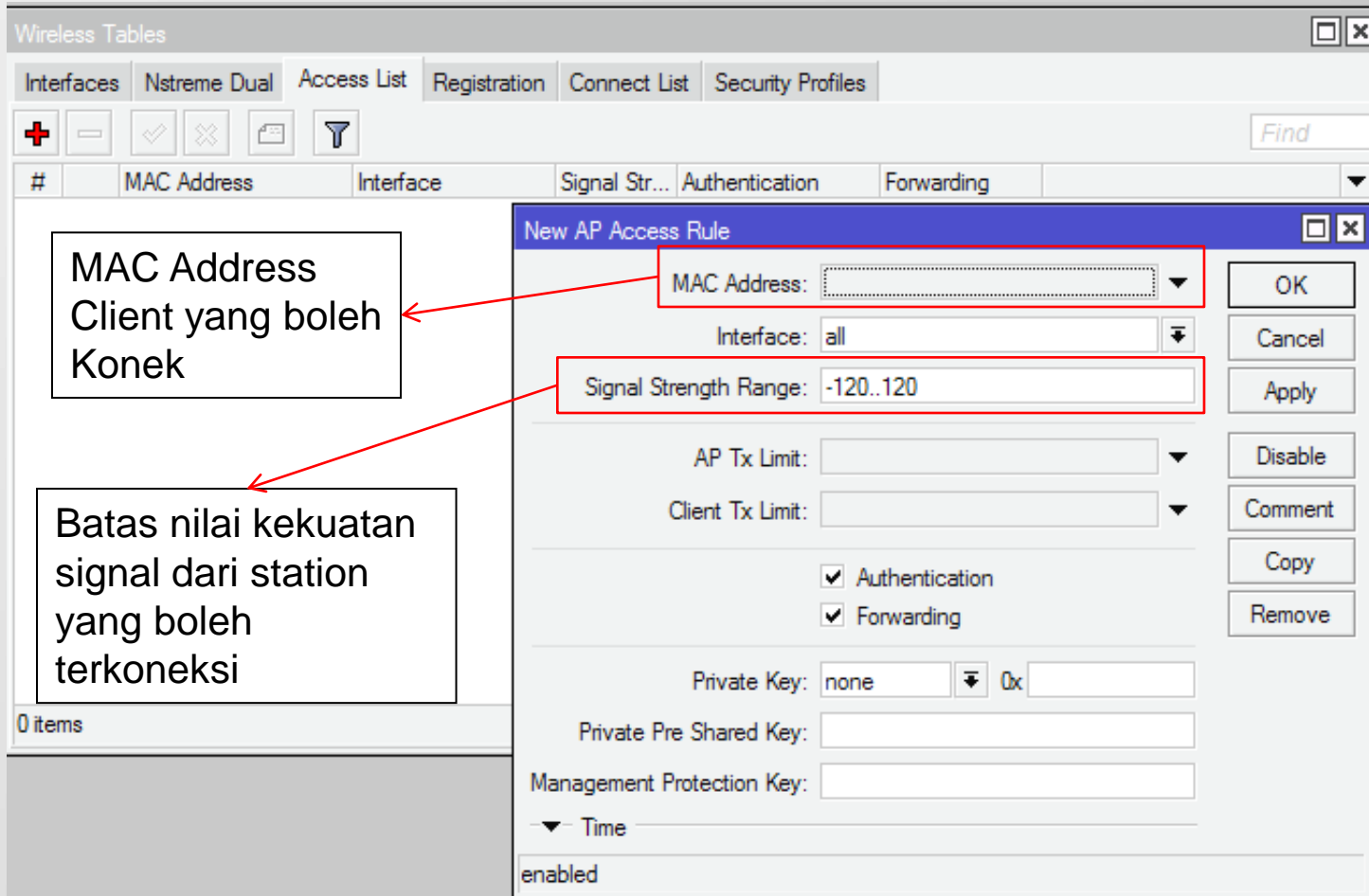
all	Frequenc...	Band	Address	SSID	Signal	Of Freq. (%)	Of Traf. (%)	Bandwidth	Networks	Stations
	2412		00:15:00:35:D1:8C		-85	0.0	0.0	0 bps		
	2412	2GHz-N				0.0	0.0	0 bps	1	5
	2412	2GHz-N	F4:EC:38:C4:DE:D0	IDN2		0.0	0.0	0 bps		4
N	2...		00:1C:26:13:73:2F	IDN2	-28	0.0	0.0	0 bps		
	2...		F4:EC:38:C4:DE:D0	IDN2	-49	0.0	0.0	0 bps		
	2...		00:21:00:6C:64:79	IDN2	-54	0.0	0.0	0 bps		
	2...		C4:17:FE:3A:0D:1C	IDN2	-58	0.0	0.0	0 bps		
	2417	2GHz-N				1.3		11.7 kbps	0	0
	2422	2GHz-N				0.0		0 bps	0	0
	2427		70:1A:04:2C:BD:84		-89	0.0	0.0	0 bps		
	2427	2GHz-N				0.0		0 bps	0	1
	2432	2GHz-N				0.0		0 bps	0	0
	2437		D8:5D:4C:8E:DD:29		-86	0.0	0.0	0 bps		
	2437		00:22:5F:13:BF:ED		-92	0.0	0.0	0 bps		
	2437	2GHz-N				5.3		37.3 kbps	1	3
	2437	2GHz-N	C0:C1:C0:88:34:F0	PUBLICIS		4.2	79.6	37.3 kbps		1
N	2...		C0:C1:C0:88:34:F0	PUBLICIS	-91	4.2	79.6	37.3 kbps		
	2442	2GHz-N				0.8		6.0 kbps	1	1
	2442	2GHz-N	B0:48:7A:C5:BA:20	Praweda01a		0.8	100.0	6.0 kbps		1
N	2...		B0:48:7A:C5:BA:20	Praweda01a	-89	0.8	100.0	6.0 kbps		
	2447		00:26:FF:5B:32:90		-58	0.0	0.0	0 bps		
	2447	2GHz-N				0.0		0 bps	0	1
	2452	2GHz-N				0.0		0 bps	0	0
	2457	2GHz-N				2.2		18.4 kbps	1	1
	2457	2GHz-N	00:22:57:E2:19:70	Praweda03		2.2	100.0	18.4 kbps		1
N	2...		00:22:57:E2:19:70	Praweda03	-85	2.2	100.0	18.4 kbps		
	2462	2GHz-N				1.6		13.8 kbps	0	0

Wireless MAC Filtering

- **Access Point**, dapat dilakukan pembatasan hak akses dimana AP hanya dapat dikonek oleh station yang sudah didaftarkan.
- **Station**, agar tidak tertipu dengan SSID AP yang sama, dapat dilock agar terkoneksi dengan AP yg sudah didaftarkan.
- **AP - Access List**
- **Station - Connect List.**

Access Point – Access List

- Access List pada Access Point, memfilter station mana saja yang boleh terkoneksi



The screenshot shows the Mikrotik WinBox interface for configuring an Access List. The main window is titled "Wireless Tables" and has tabs for "Interfaces", "Nstreme Dual", "Access List", "Registration", "Connect List", and "Security Profiles". The "Access List" tab is active, showing a table with columns for "#", "MAC Address", "Interface", "Signal Str...", "Authentication", and "Forwarding". The table currently contains 0 items.

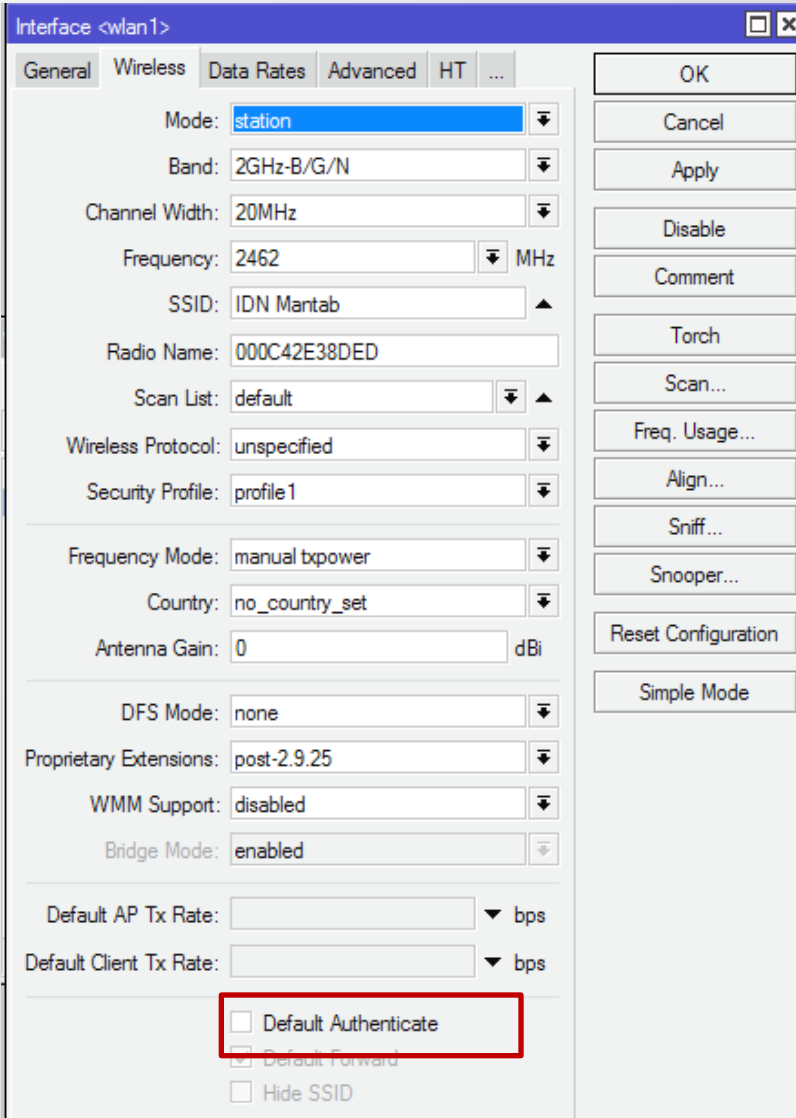
A "New AP Access Rule" dialog box is open, showing the following configuration options:

- MAC Address: [Empty field]
- Interface: all
- Signal Strength Range: -120..120
- AP Tx Limit: [Empty field]
- Client Tx Limit: [Empty field]
- Authentication:
- Forwarding:
- Private Key: none
- Private Pre Shared Key: [Empty field]
- Management Protection Key: [Empty field]
- Time: [Empty field]
- enabled

Two red boxes highlight the "MAC Address" and "Signal Strength Range" fields. Arrows point from these boxes to explanatory text on the left:

- The first box points to the text: "MAC Address Client yang boleh Konek".
- The second box points to the text: "Batas nilai kekuatan signal dari station yang boleh terkoneksi".

Access Point – Default Authenticate



Interface <wlan1>

General Wireless Data Rates Advanced HT ...

Mode: station

Band: 2GHz-B/G/N

Channel Width: 20MHz

Frequency: 2462 MHz

SSID: IDN Mantab

Radio Name: 000C42E38DED

Scan List: default

Wireless Protocol: unspecified

Security Profile: profile1

Frequency Mode: manual txpower

Country: no_country_set

Antenna Gain: 0 dBi

DFS Mode: none

Proprietary Extensions: post-2.9.25

WMM Support: disabled

Bridge Mode: enabled

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

OK

Cancel

Apply

Disable

Comment

Torch

Scan...

Freq. Usage...

Align...

Sniff...

Snooper...

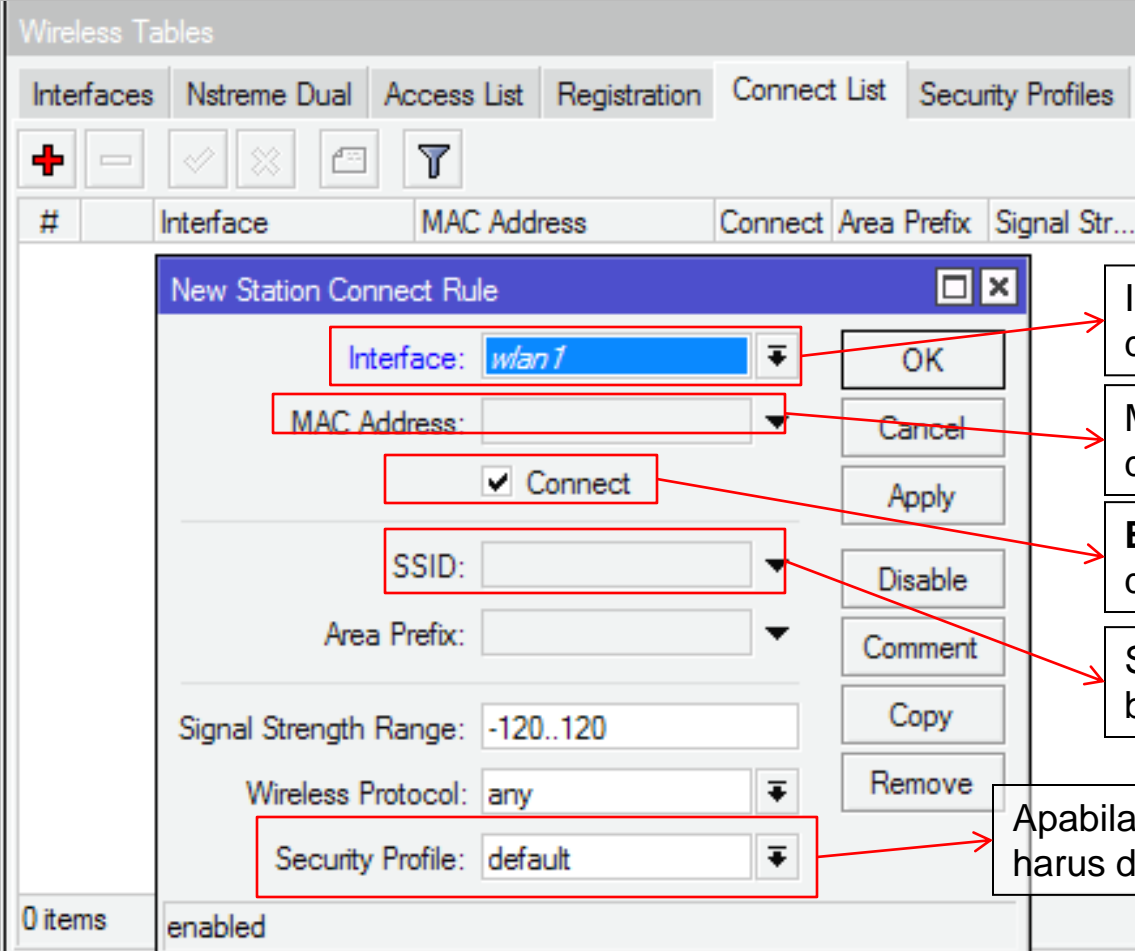
Reset Configuration

Simple Mode

Access List dapat berfungsi apabila wireless default authenticate di non aktifkan (uncheck).

Station – Connection List

- Pada wireless Station, Connect List membatasi AP mana saja yang boleh/tidak boleh terkoneksi



Interface radio yang difungsikan sebagai client

MAC address AP yang akan dikoneksikan.

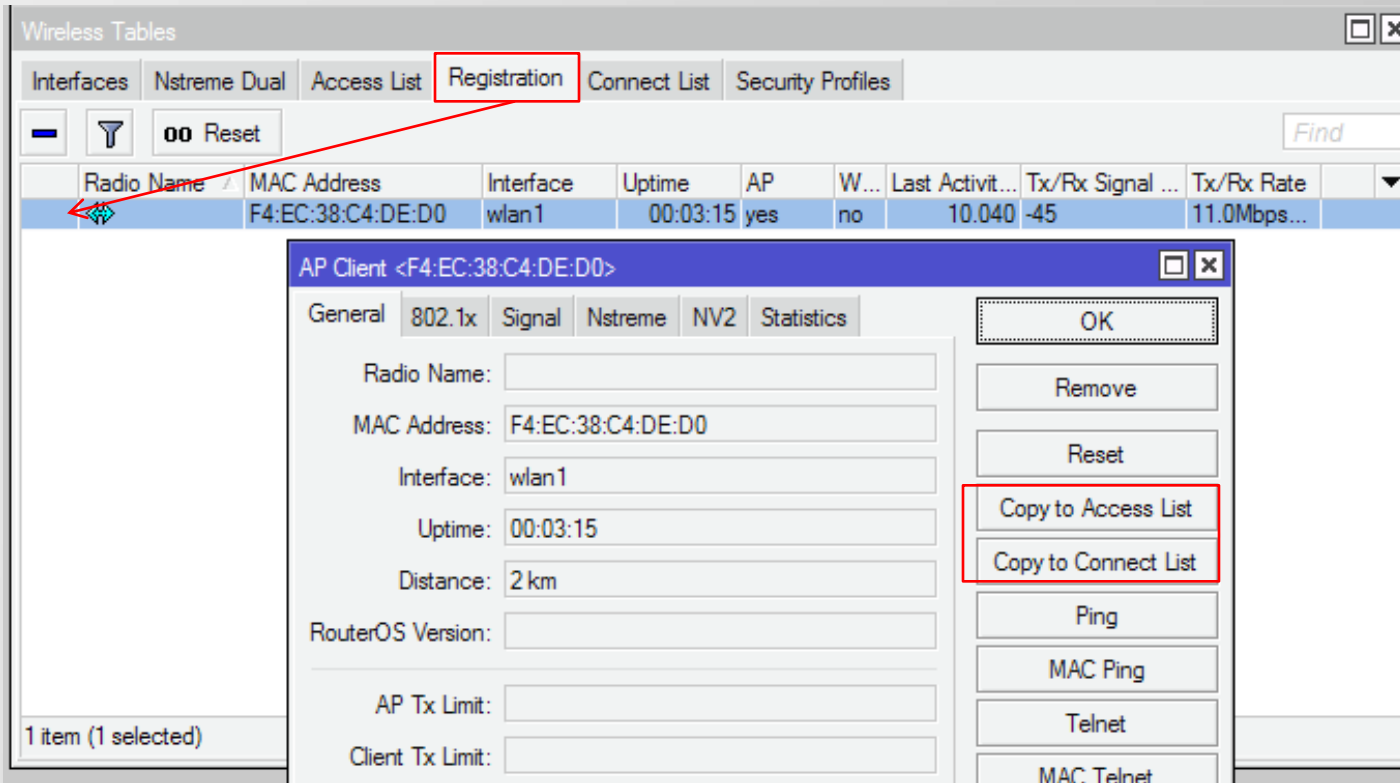
Boleh / tidak boleh konek dengan MAC diatas

SSID yang ingin dikoneksikan, bila kosong berarti any AP.

Apabila menggunakan security profile, harus diapply di ruleConnect List

Registration List

- Pada Access Point dan Station, Registered List berisi data AP/station yang sedang terkoneksi.
- Untuk memudahkan filtering pada Access List dan Connection List, menggunakan menu “Copy to Access/Connect List”



The screenshot shows the Mikrotik WinBox interface. The 'Registration' tab is selected in the 'Wireless Tables' window. A table lists registered clients, with one client selected. A red arrow points from the 'Registration' tab to the selected client. A dialog box titled 'AP Client <F4:EC:38:C4:DE:D0>' is open, showing details for the selected client. The 'Copy to Access List' and 'Copy to Connect List' buttons are highlighted with a red box.

Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activit...	Tx/Rx Signal ...	Tx/Rx Rate
	F4:EC:38:C4:DE:D0	wlan1	00:03:15	yes	no	10.040	-45	11.0Mbps...

AP Client <F4:EC:38:C4:DE:D0>

General | 802.1x | Signal | Nstreme | NV2 | Statistics

Radio Name:

MAC Address: F4:EC:38:C4:DE:D0

Interface: wlan1

Uptime: 00:03:15

Distance: 2 km

RouterOS Version:

AP Tx Limit:

Client Tx Limit:

Buttons: OK, Remove, Reset, Copy to Access List, Copy to Connect List, Ping, MAC Ping, Telnet, MAC Telnet

1 item (1 selected)

Default Authenticated

- Untuk menggunakan pilihan Connection List atau Access List baik pada AP atau Station Default Authenticated harus di uncheck.

Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme ...

Mode: station

Band: 2GHz-B/G/N

Channel Width: 20MHz

Frequency: 2412 MHz

SSID: IDN2

Scan List: default

Wireless Protocol: unspecified

Security Profile: profile-IDN2

Bridge Mode: enabled

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticated

Default Forward

Hide SSID

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

Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme ...

Mode: ap bridge

Band: 2GHz-B/G/N

Channel Width: 20MHz

Frequency: 2412 MHz

SSID: IDN3

Scan List: default

Wireless Protocol: unspecified

Security Profile: profile-IDN2

Bridge Mode: enabled

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticated

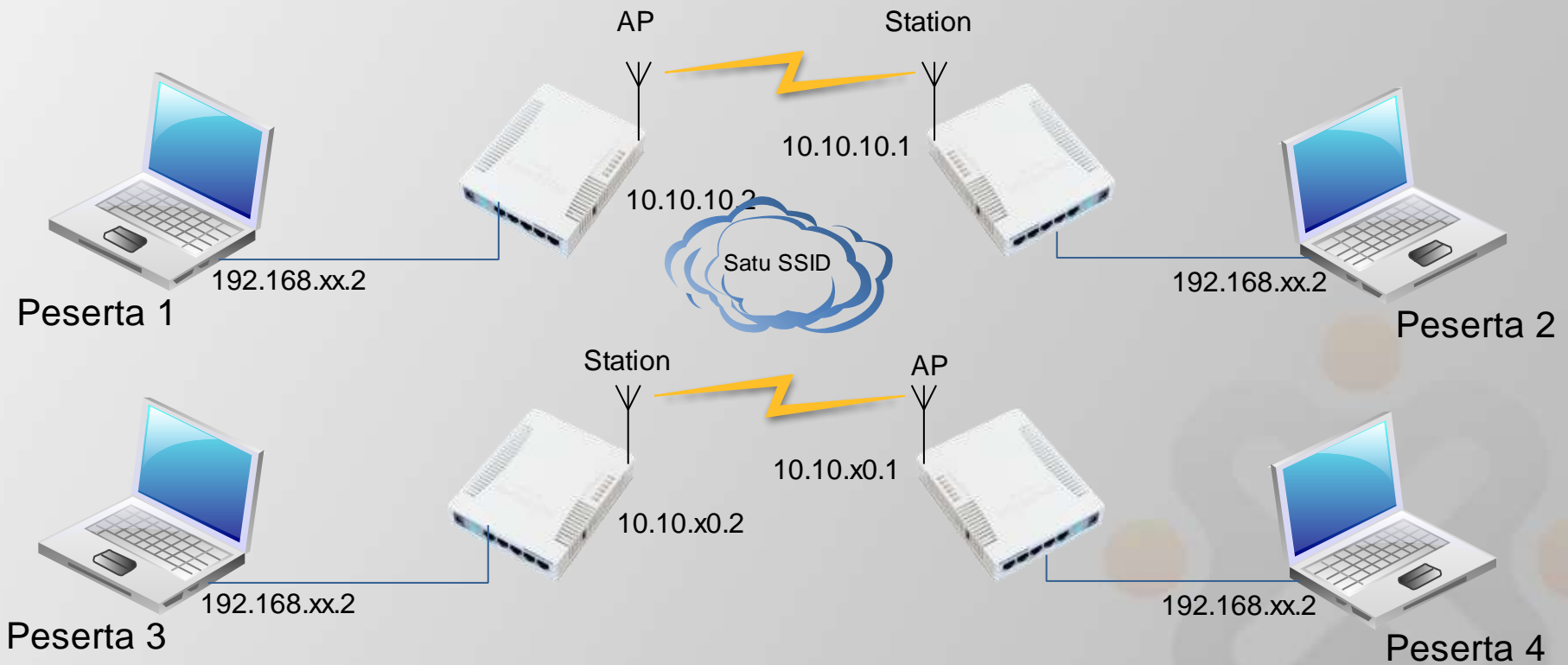
Default Forward

Hide SSID

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

LAB-Wireless Mac Filtering

Buatlah topologi AP-Station dengan SSID yang sama.

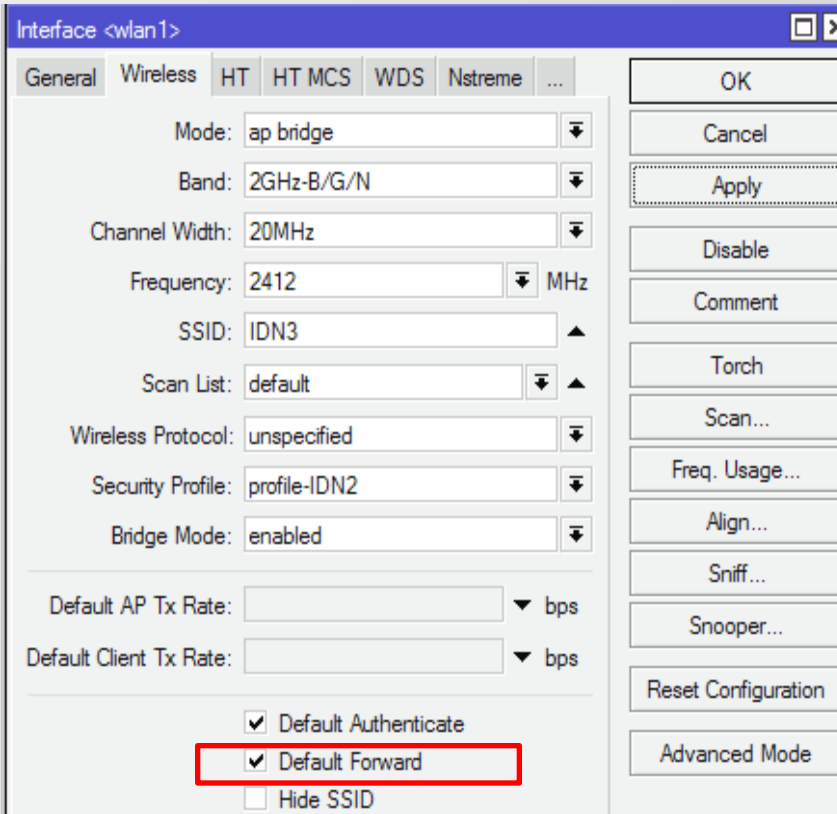


LAB – MAC Filtering

- Filter mac address agar koneksi point to point anda dengan partner tidak mudah dikacaukan oleh koneksi lain.
- Masukkan data mac address wireless partner ke list yang benar. Jika sebagai Station masukkan kedalam Connect-List, apabila sebagai AP masukkan dalam Access-List.
- Untuk setting wireless pada AP, default authenticate harus di-uncheck, agar tidak semua client bisa teraouthentikasi secara otomatis.
- Coba untuk konek ke AP yang bukan pasangan

Drop Koneksi Antar Client

- Default forward (hanya dapat diseting pada Access Point).
- Digunakan untuk mengizinkan/tidak komunikasi antar client/station yang terkoneksi dalam 1 Access Point.



Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme ...

Mode: ap bridge

Band: 2GHz-B/G/N

Channel Width: 20MHz

Frequency: 2412 MHz

SSID: IDN3

Scan List: default

Wireless Protocol: unspecified

Security Profile: profile-IDN2

Bridge Mode: enabled

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

OK

Cancel

Apply

Disable

Comment

Torch

Scan...

Freq. Usage...

Align...

Sniff...

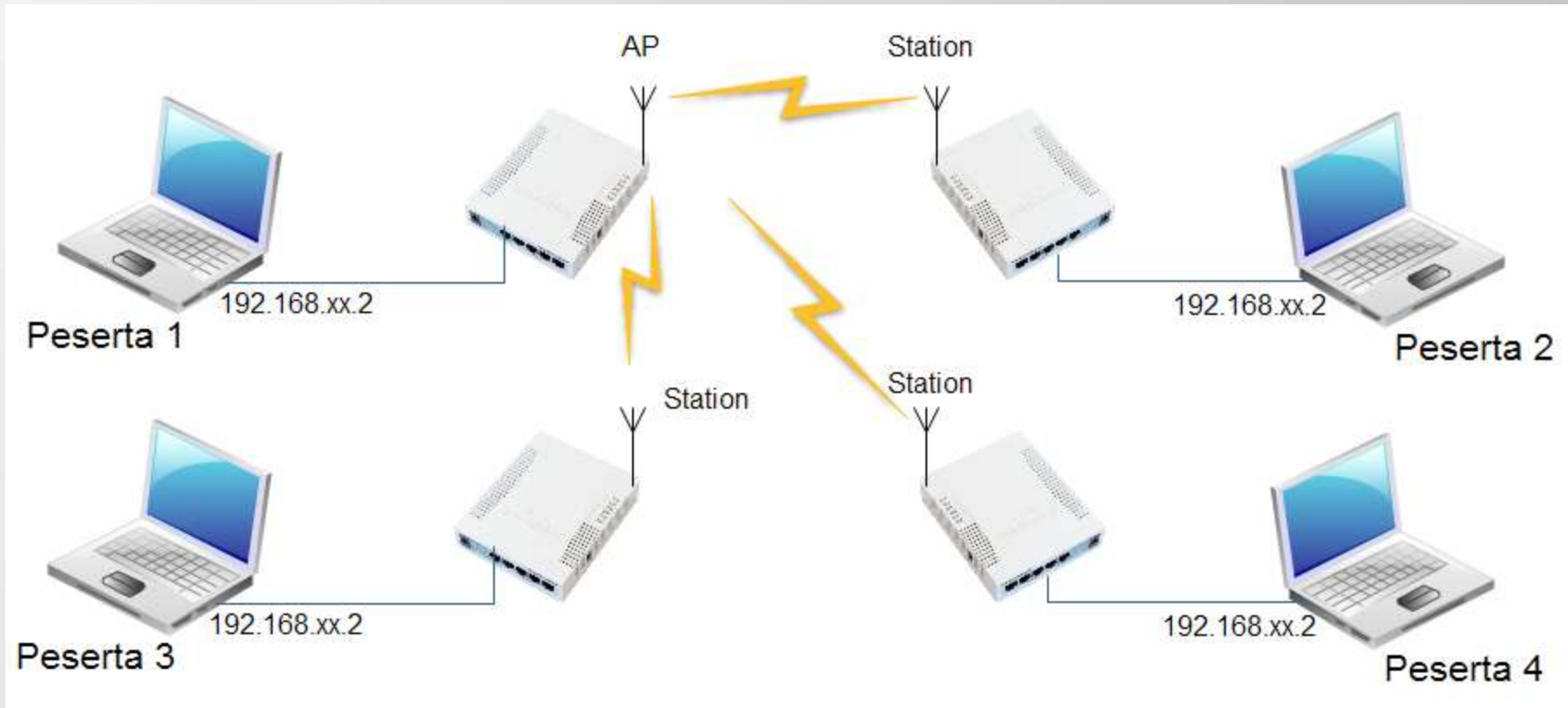
Snooper...

Reset Configuration

Advanced Mode

- Default forward biasanya didisable untuk keamanan hotspot client.

LAB – Default Forwarding



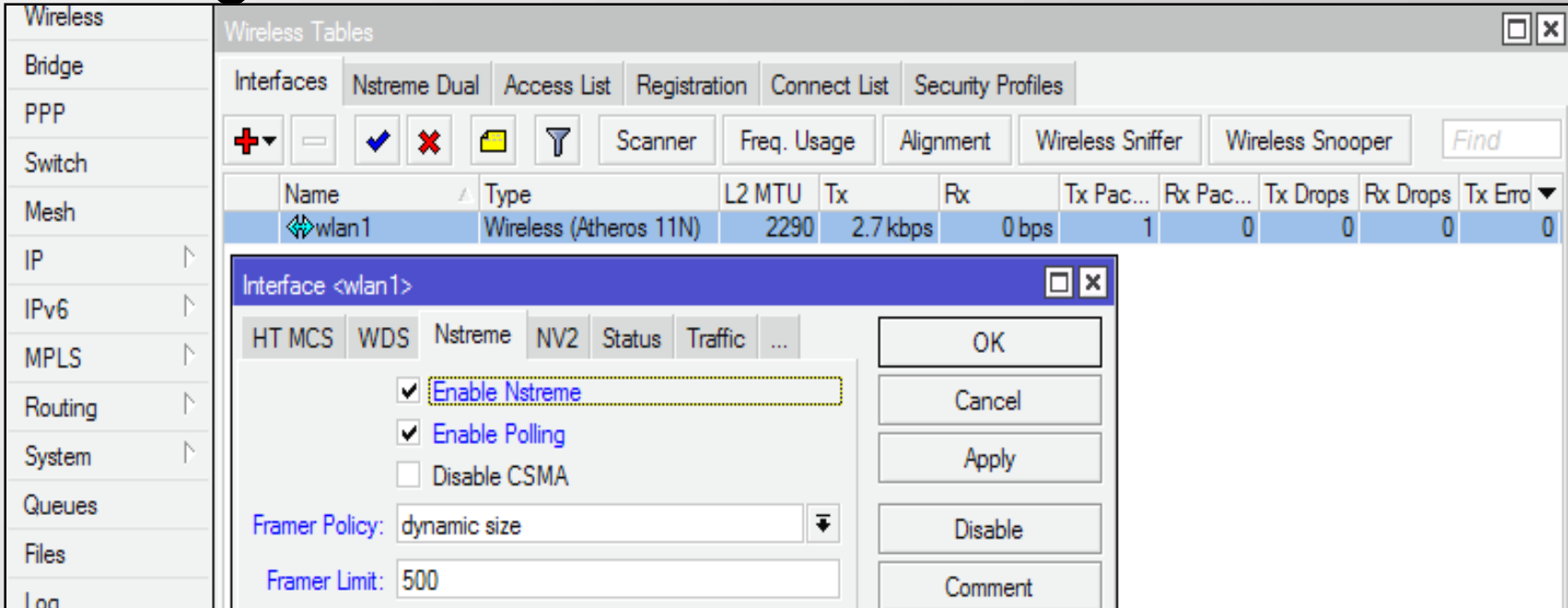
- Cobalah ping antar peserta ketika default forwarding check dan uncheck

Nstreme

- Nstreme adalah proprietary Mikrotik
- Meningkatkan performance link wireless, terutama pada jarak jauh.
- Nstreme harus diaktifkan di AP & klien
- Konfigurasi Nstreme hanya di AP, klien hanya mengikuti

LAB - Wireless Nstreme

Setting di AP

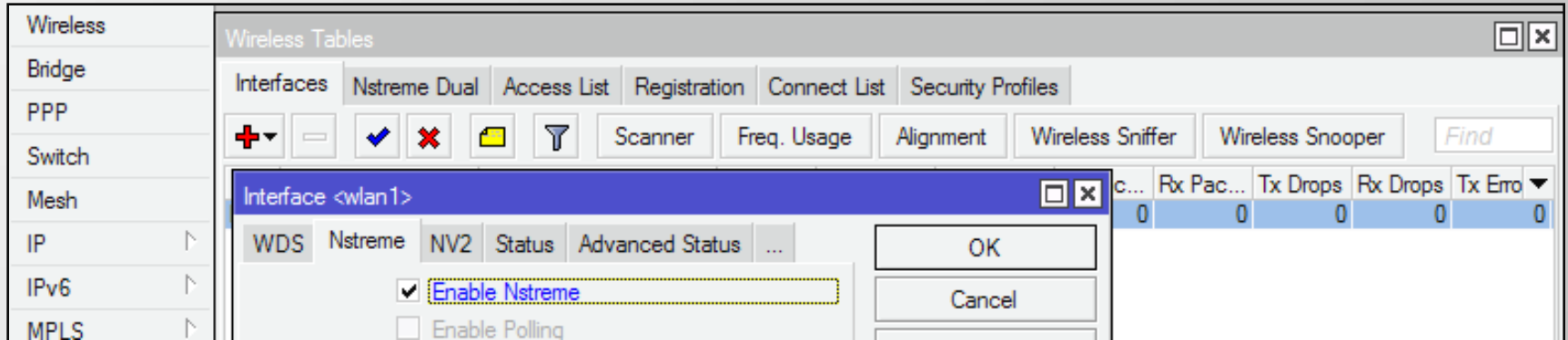


The screenshot shows the Mikrotik WinBox interface. On the left is a sidebar with a tree view containing: Wireless, Bridge, PPP, Switch, Mesh, IP, IPv6, MPLS, Routing, System, Queues, Files, and Log. The main window is titled "Wireless Tables" and has several tabs: Interfaces, Nstreme Dual, Access List, Registration, Connect List, and Security Profiles. Below the tabs are various utility buttons like Scanner, Freq. Usage, Alignment, Wireless Sniffer, and Wireless Snooper. A table lists wireless interfaces, with "wlan1" selected. Below the table, the "Interface <wlan1>" configuration dialog is open, showing the "Nstreme" tab. In this tab, the "Enable Nstreme" checkbox is checked and highlighted with a yellow dashed border. Other options include "Enable Polling" (checked), "Disable CSMA" (unchecked), "Framer Policy" (dynamic size), and "Framer Limit" (500). Buttons for OK, Cancel, Apply, Disable, and Comment are visible on the right side of the dialog.

Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops	Rx Drops	Tx Ero
wlan1	Wireless (Atheros 11N)	2290	2.7 kbps	0 bps	1	0	0	0	0

LAB - Wireless Nstream

Setting di Station



Wireless Tables

Interfaces: Nstream Dual | Access List | Registration | Connect List | Security Profiles

Scanner | Freq. Usage | Alignment | Wireless Sniffer | Wireless Snooper | Find

Interface <wlan1>

WDS | Nstream | NV2 | Status | Advanced Status | ...

Enable Nstream

Enable Polling

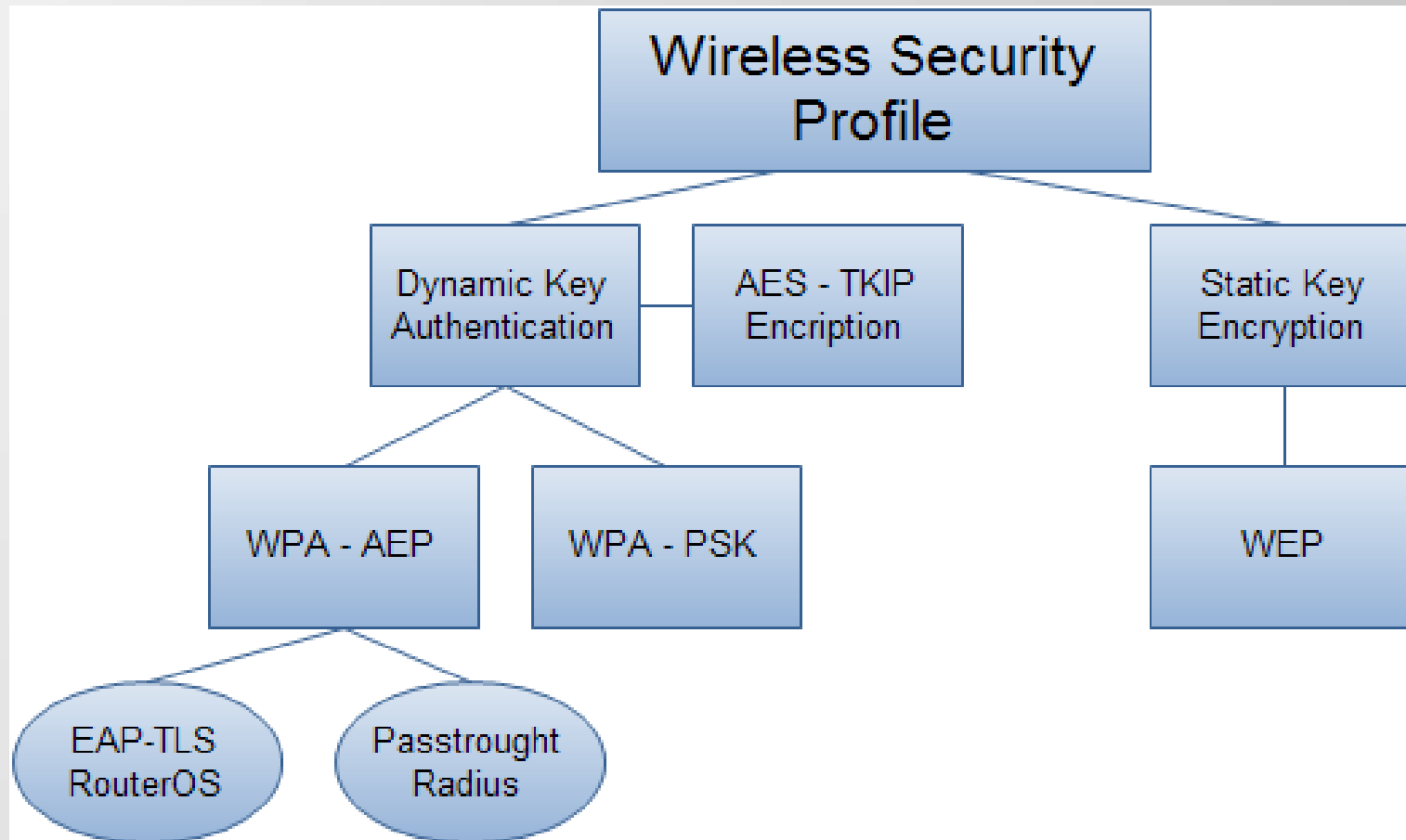
c...	Rx Pac...	Tx Drops	Rx Drops	Tx Erro
0	0	0	0	0

Cobalah konek dengan Laptop ke AP yang mengaktifkan feature nstream

Wireless Security

- Untuk pengamanan koneksi wireless, tidak hanya cukup dengan MAC-Filtering, karena data yang lewat ke jaringan bisa diambil dan dianalisa.
- Terdapat metode keamanan lain yang dapat digunakan yaitu:
 - Authentication (WPA-PSK, WPA-AEP)
 - Enkripsi (AES, TKIP, WEP)
 - Tunnel

Wireless Security



Wireless Encryption - WPA

- Pilihan wireless encryption terdapat pada menu Wireless>Security Profile.
- Security profile diberi nama tertentu untuk diimplementasikan dalam interface wireless.

Security Profile <profile-IDN2>

General | RADIUS | EAP | Static Keys

Name: profile-IDN2

Mode: dynamic keys

Authentication Types

- WPA PSK
- WPA2 PSK
- WPA EAP
- WPA2 EAP

Unicast Ciphers

- tkip
- aes ccm

Group Ciphers

- tkip
- aes ccm

WPA Pre-Shared Key:

WPA2 Pre-Shared Key:

Dynamic key = WPA
Static Key = WEP (lama)

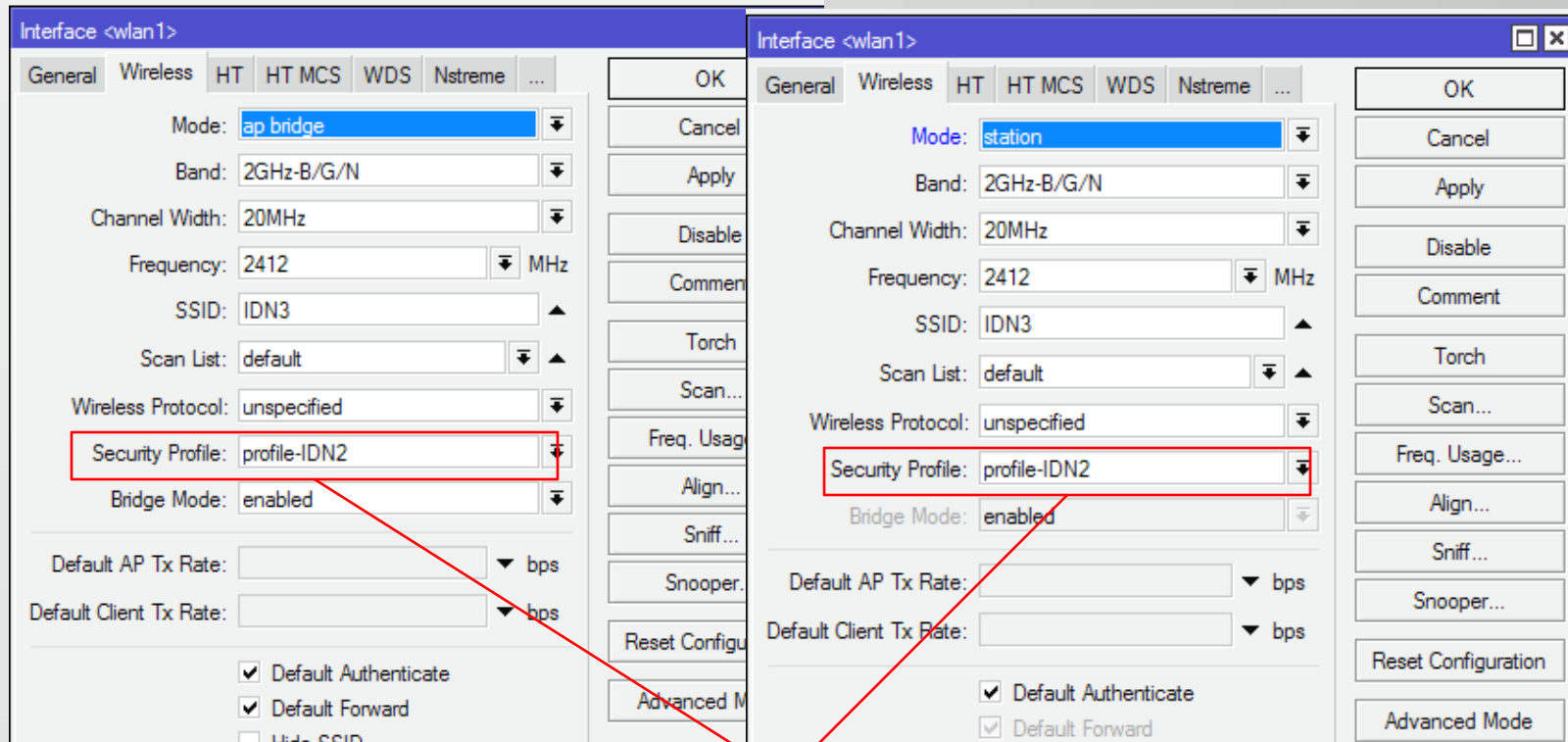
Jenis Authentifikasi

Model Enkripsi

Key Authentifikasi / password

Wireless Encryption

- Implementasi security profile



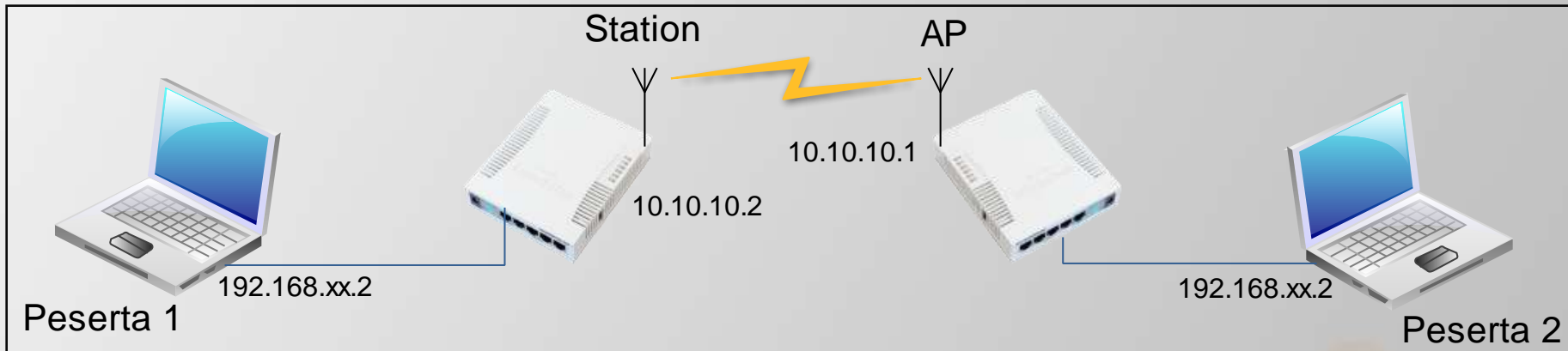
Pilih security profil yang telah kita buat sebelumnya baik di AP maupun Station

WEP Encryption

- WEP (Wired Equivalent Privacy) tipe wireless security yang pertama kali muncul dan masih sangat sederhana
- Tidak mempunyai authenticate method
- Not recommended as it is vulnerable to wireless hacking tools

LAB-WEP Encryption

- Buat koneksi AP-Station dengan pasangan anda.

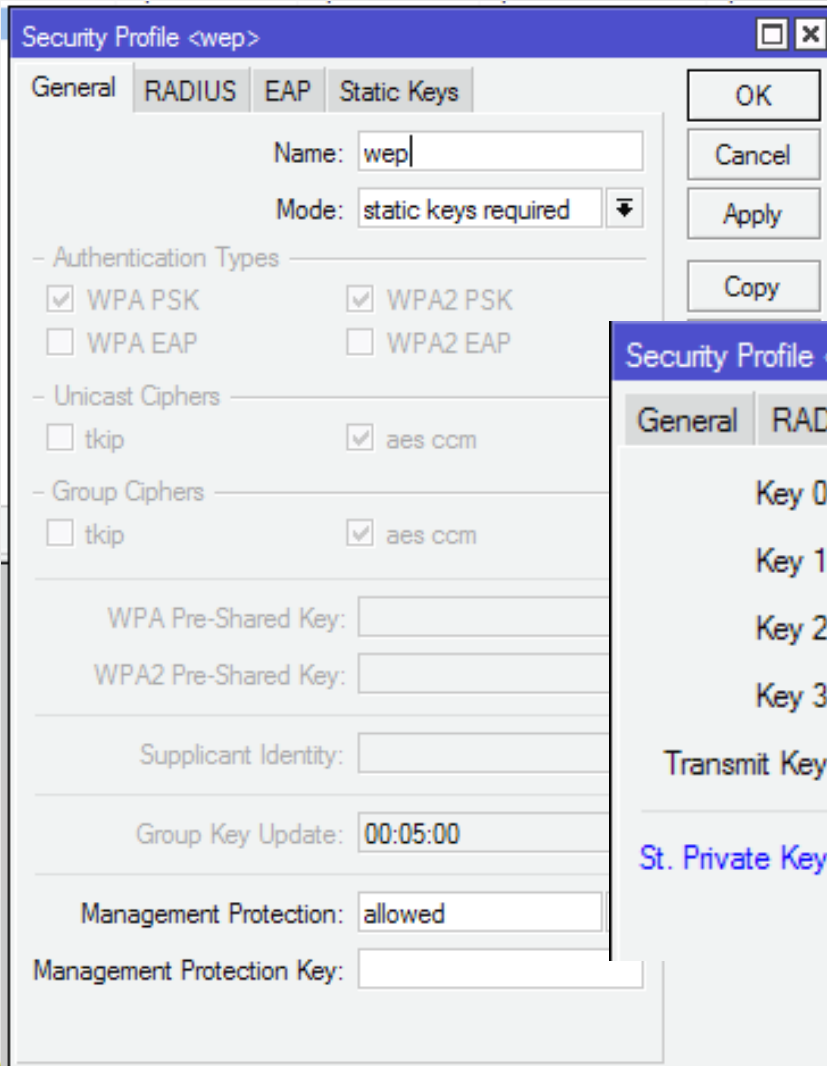


- Create WEP security profile pada kedua sisi wlan (AP & station), samakan static keynya.
- Apply security profile tersebut pada interface wireless wlan1

LAB-WEP Encryption

Wireless Security Profile:

- Mode: static keys required
- Key 0 : 40 bit
- 0x : 1234567890



Security Profile <wep>

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

Name:

Mode:

Authentication Types

WPA PSK WPA2 PSK

WPA EAP WPA2 EAP

Unicast Ciphers

tkip aes ccm

Group Ciphers

tkip aes ccm

WPA Pre-Shared Key:

WPA2 Pre-Shared Key:

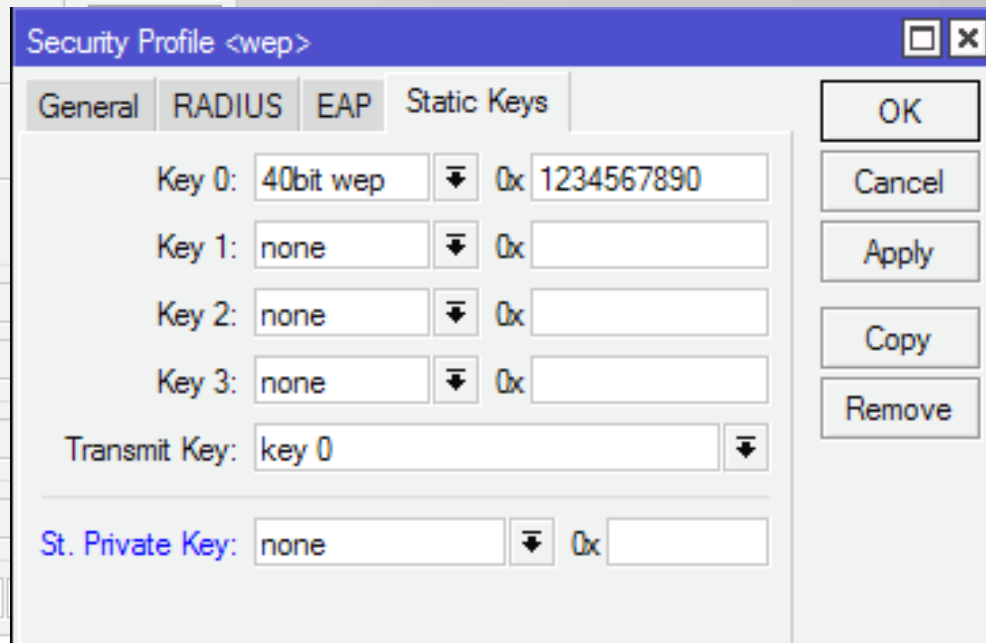
Supplicant Identity:

Group Key Update:

Management Protection:

Management Protection Key:

OK
Cancel
Apply
Copy



Security Profile <wep>

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

Key 0:

Key 1:

Key 2:

Key 3:

Transmit Key:

St. Private Key:

OK
Cancel
Apply
Copy
Remove

LAB - Virtual Access Point

- Virtual AP akan menjadi child dari wlan (interface real).
- Satu interface dapat memiliki banyak virtual AP (maksimum 128)
- Virtual AP dapat diset **dengan SSID, security profile dan access list** yang berbeda, namun menggunakan **frekuensi dan band yang sama** dengan wlan induk.
- Virtual AP bersifat sama seperti AP:
 - Dapat dikoneksikan dengan station / client.
 - Dapat difungsikan sebagai DHCP server.
 - Dapat difungsikan sebagai Hotspot server.

Wireless Tables

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

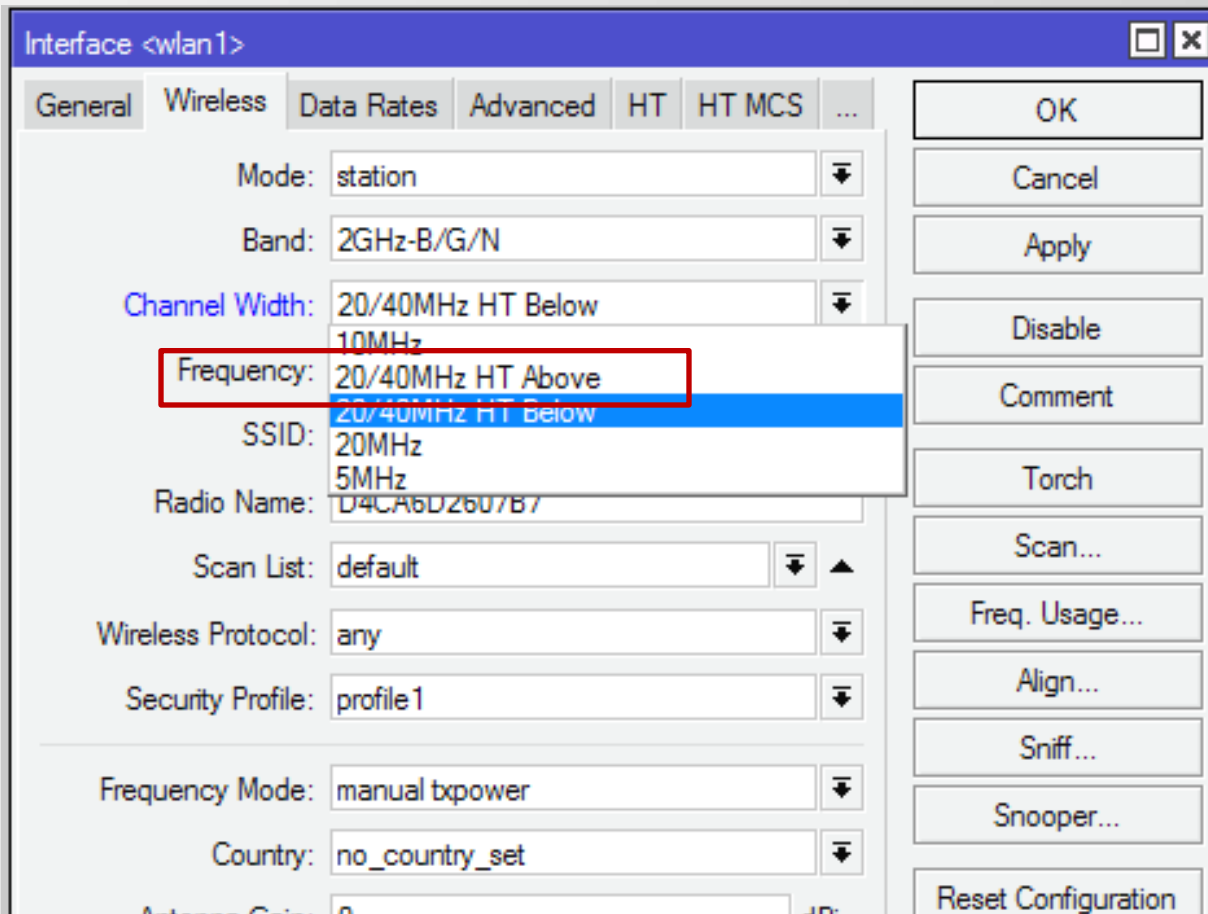
Scanner | Freq. Usage | Alignment | Wireless Sniffer | Wireless Snooper

Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops	Rx Drops	Tx Errors	Rx Errors	MAC Address	ARP	Mode	Band	Chann...	Frequen...	SSID
R wlan1	Wireless (Atheros 11N)	2290	0 bps	2.1 kbps	0	3	0	0	0	0	00:0C:42:E3:8E:11	enabled	ap bri...	2GHz-...	20MHz	2412	IDN2
↳ wlan2	VirtualAP	2290	0 bps	0 bps	0	0	0	0	0	0	02:0C:42:E3:8E:12	enabled					IDN5
↳ wlan3	VirtualAP	2290	0 bps	0 bps	0	0	0	0	0	0	02:0C:42:E3:8E:13	enabled					IDN6
↳ wlan4	VirtualAP	2290	0 bps	0 bps	0	0	0	0	0	0	02:0C:42:E3:8E:13	enabled					IDN7
↳ wlan5	VirtualAP	2290	0 bps	0 bps	0	0	0	0	0	0	02:0C:42:E3:8E:13	enabled					IDN8
↳ wlan6	VirtualAP	2290	0 bps	0 bps	0	0	0	0	0	0	02:0C:42:E3:8E:13	enabled					IDN9

802.11N

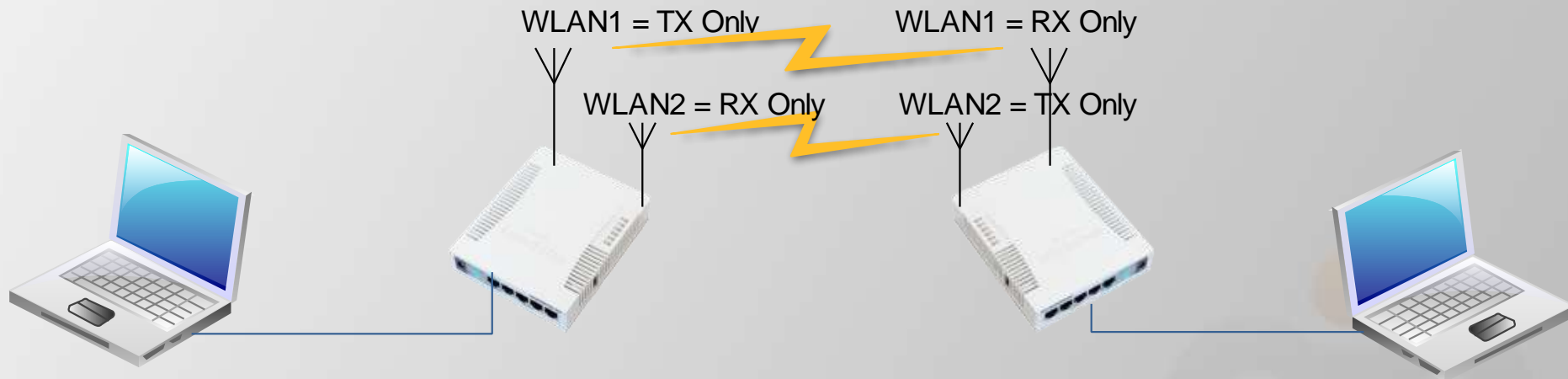
- Meningkatkan data rate sampai dengan 300Mbps
- Dapat menggunakan lebar pita 20 MHz atau 2x20MHz (channel bonding)
- Dapat bekerja pada frekuensi 2,4GHz dan 5GHz
- MIMO (Multiple Input Multiple Output)
 - SDM - Spatial Division Multiplexing
 - Stream/pancaran multi-spatial yang bekerja pada masing-masing antenna
 - Antenna yang digunakan dapat lebih dari 1 dan dikonfigurasi untuk transmit dan receive

Channel Bonding



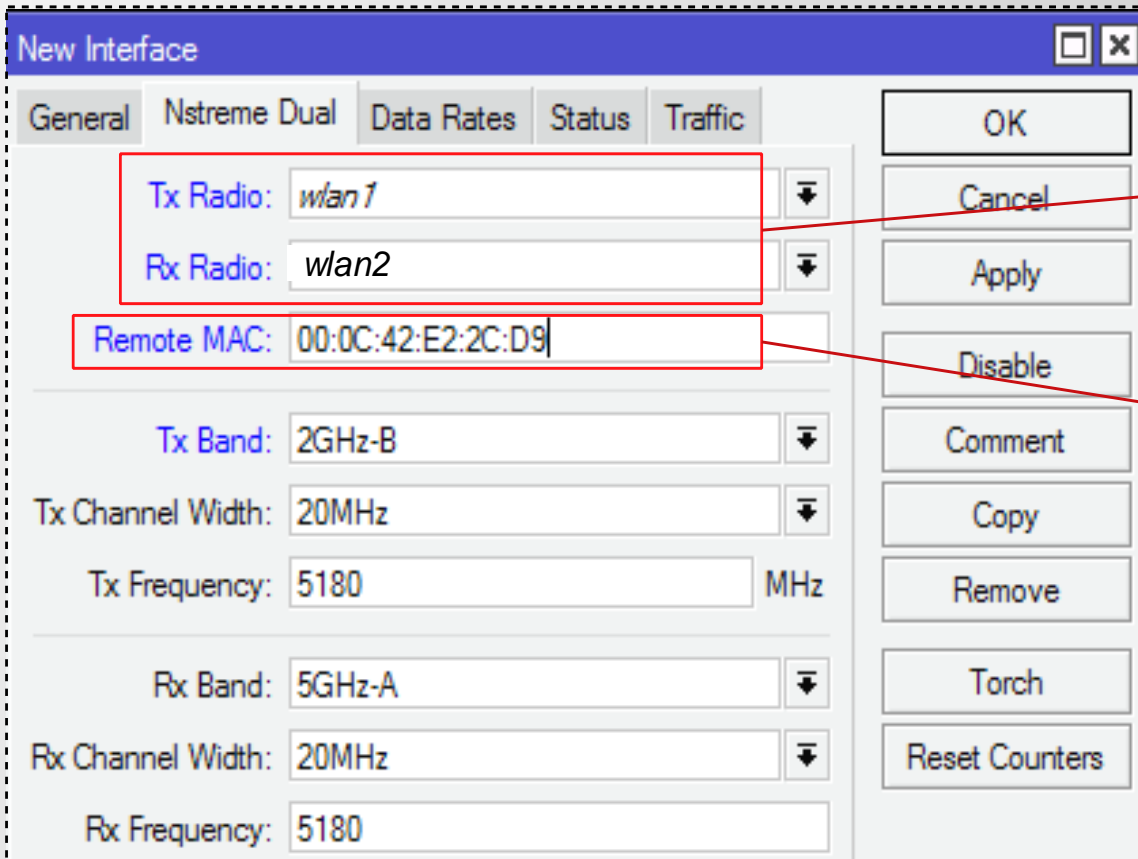
Nstreme Dual

Nstreme dual memanfaatkan keunggulan Nstreme (polling based) namun menggunakan 2 interface sekaligus yaitu 1 sebagai TX dan satu lagi sebagai RX.



Untuk menjalankan nstreme dual Mikrotik harus mempunyai 2 interface wireless.

Nstream Dual



New Interface

General | **Nstream Dual** | Data Rates | Status | Traffic

Tx Radio: ↓

Rx Radio: ↓

Remote MAC:

Tx Band: ↓

Tx Channel Width: ↓

Tx Frequency: MHz

Rx Band: ↓

Rx Channel Width: ↓

Rx Frequency:

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch, Reset Counters

Pemilihan interface wlan sebagai RX atau TX

Mac-address interface nstream-dual diisi remote

- Untuk konfigurasi Mikrotik lawannya frekuensi untuk TX dan Rxnya dibalik

Bridge (Layer 2 Connection)



Bridge

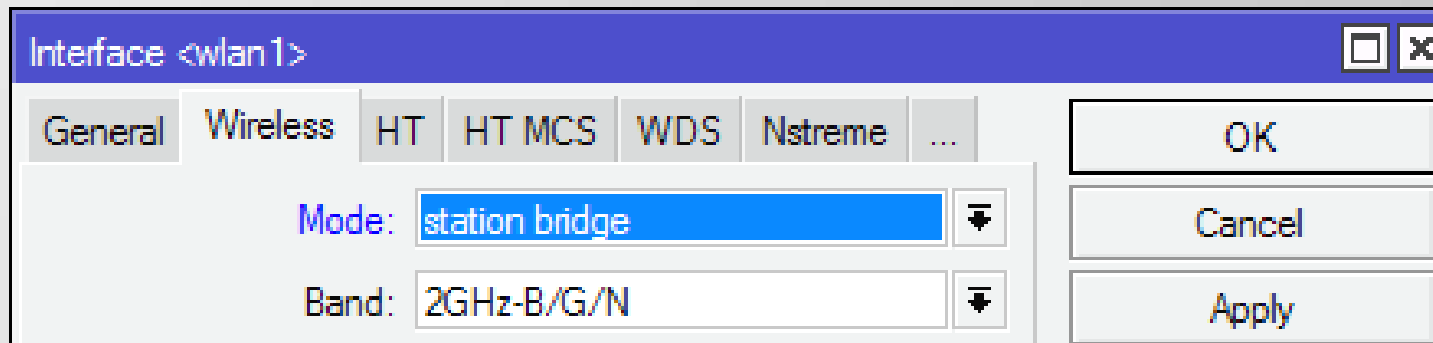
- Menggabungkan 2 atau lebih interface yang bertipe ethernet, atau sejenisnya, seolah-olah berada dalam 1 segmen network yang sama,
- Bridge juga dapat berjalan pada jaringan wireless
- Proses bridge berjalan pada layer data link (layer 2)
- Interface bridge adalah interface virtual, dimana kita dapat membuat sebanyak yang kita inginkan.
- Tahap pembuatan bridge adalah, membuat bridge baru dan menambahkan interface fisik kedalam port bridge.
- Jika kita membuat interface bride tanpa menambahkan interface fisik pada portnya, maka bridge tersebut dianggap sebagai interface loopback.

Bridge

- Kelemahan dari Bridge adalah:
 - Sulit untuk mengatur trafik broadcast (misalnya akibat virus, dll)
 - Permasalahan pada satu segmen akan membuat masalah di semua segmen pada bridge yang sama
 - Peningkatan beban trafik akibat terjadinya akumulasi traffic

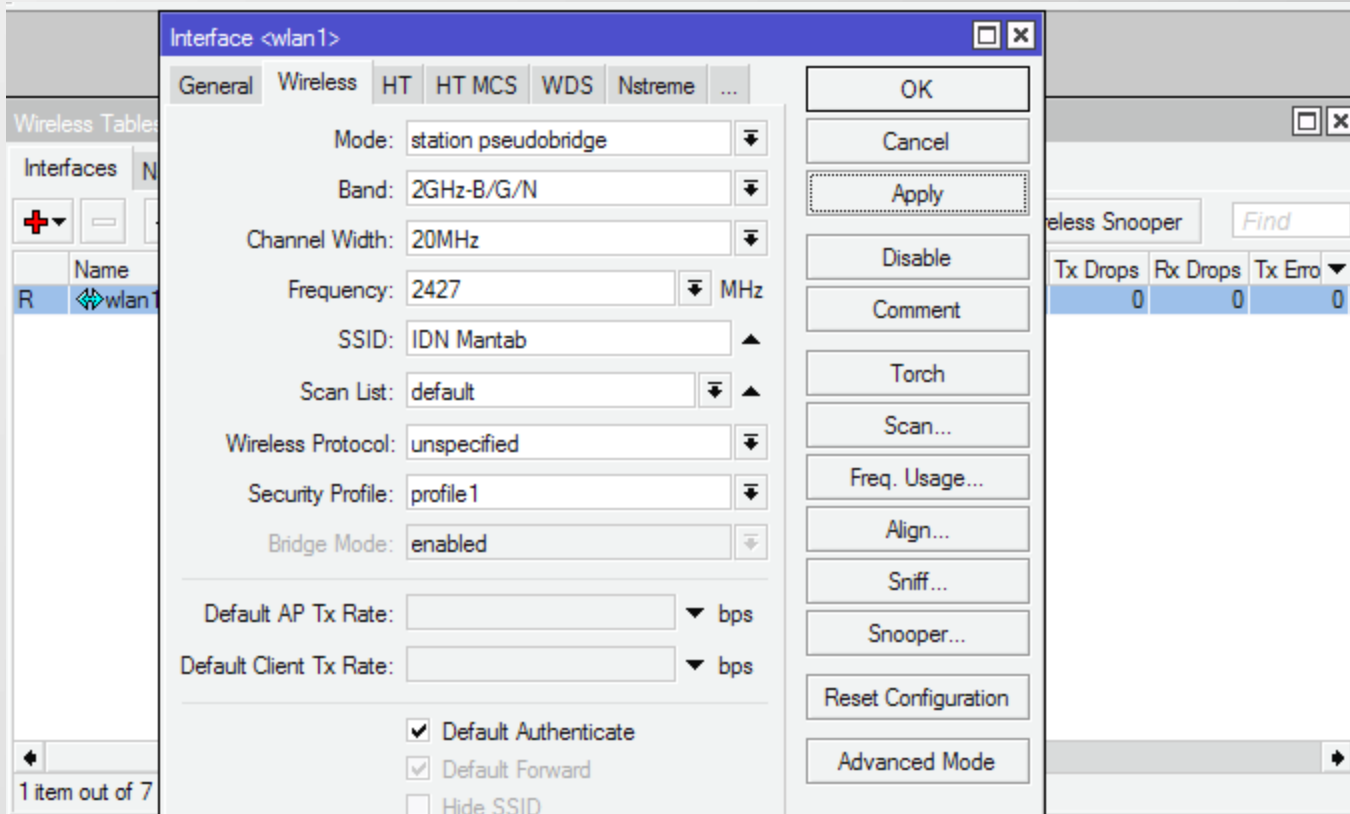
Station Bridge

- Station bridge adalah fitur MikroTik sejak v5 yang memungkinkan station untuk di-bridge.
- Station bridge hanya akan berjalan pada koneksi antar MikroTik (versi 5 keatas).



LAB-Simple Wireless Bridge

- Set wireless mode ke station pseudobridge



Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme ...

Mode: station pseudobridge

Band: 2GHz-B/G/N

Channel Width: 20MHz

Frequency: 2427 MHz

SSID: IDN Mantab

Scan List: default

Wireless Protocol: unspecified

Security Profile: profile1

Bridge Mode: enabled

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

OK

Cancel

Apply

Disable

Comment

Torch

Scan...

Freq. Usage...

Align...

Sniff...

Snooper...

Reset Configuration

Advanced Mode

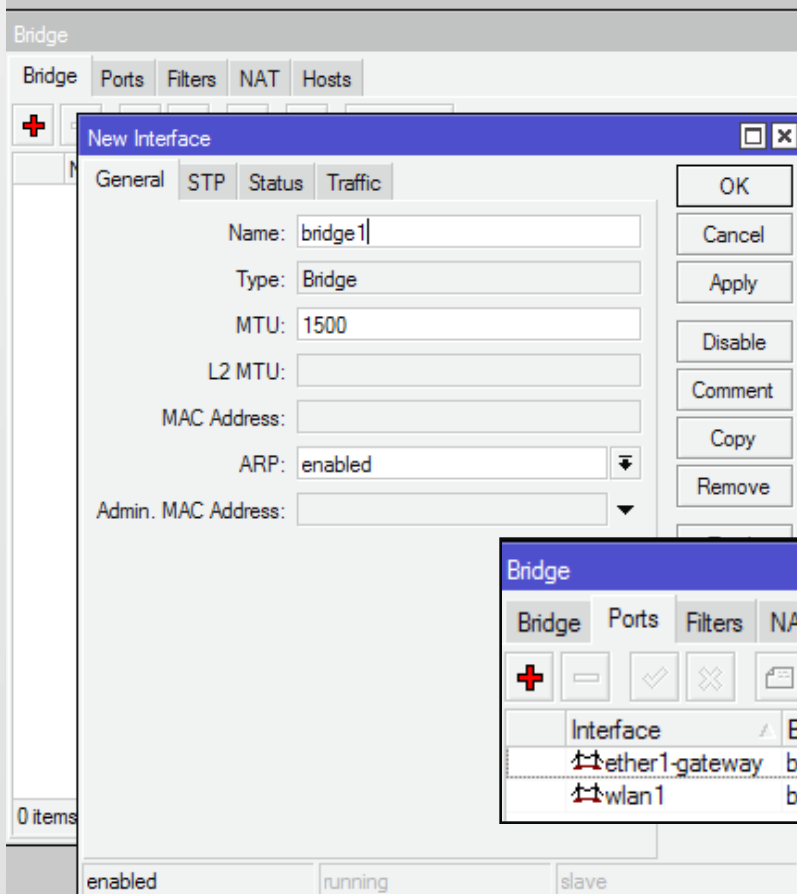
Wireless Snooper Find

Tx Drops	Rx Drops	Tx Err
0	0	0

1 item out of 7

LAB - Simple Wireless Bridge

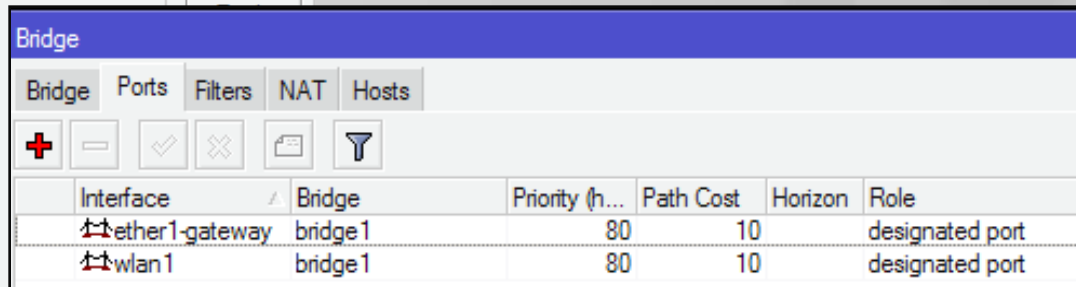
- Buatlah satu interface bride dan tambahkan interface ether1 dan wlan1 pada portsnya.



The screenshot shows the Mikrotik WinBox interface. A 'New Interface' dialog box is open, showing the configuration for a new bridge interface named 'bridge1'. The configuration includes:

- Name: bridge1
- Type: Bridge
- MTU: 1500
- L2 MTU: (empty)
- MAC Address: (empty)
- ARP: enabled
- Admin. MAC Address: (empty)

Buttons on the right side of the dialog include OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

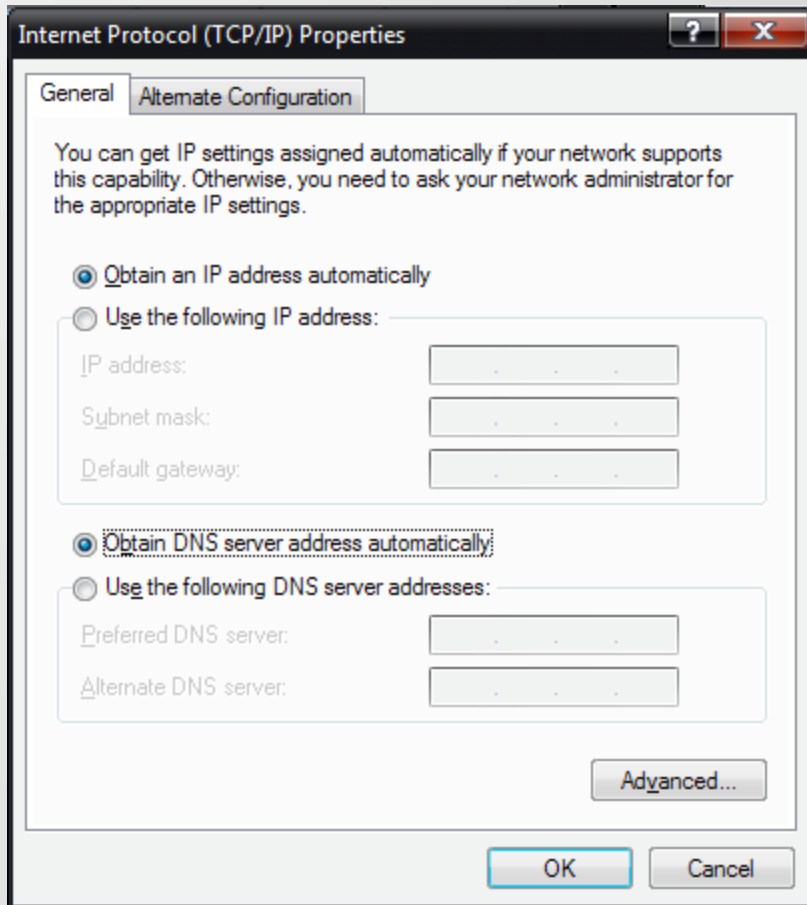


The screenshot shows the Mikrotik WinBox 'Bridge' configuration window. The 'Ports' tab is selected, displaying a table of ports added to the bridge.

Interface	Bridge	Priority (h...	Path Cost	Horizon	Role
ether1-gateway	bridge 1	80	10		designated port
wlan1	bridge 1	80	10		designated port

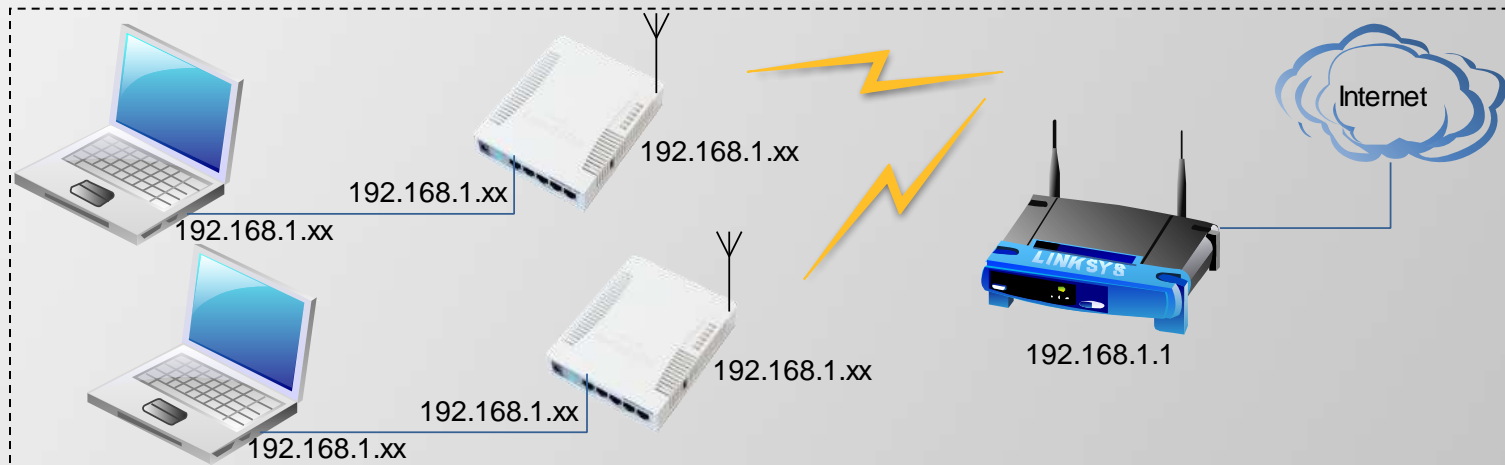
LAB - Simple Wireless Bridge

- Set IP DHCP client (dynamic IP address) di Laptop



Apakah Laptop mendapatkan IP DHCP dari Access Point IDN Mantab?

LAB – Jaringan Bridge



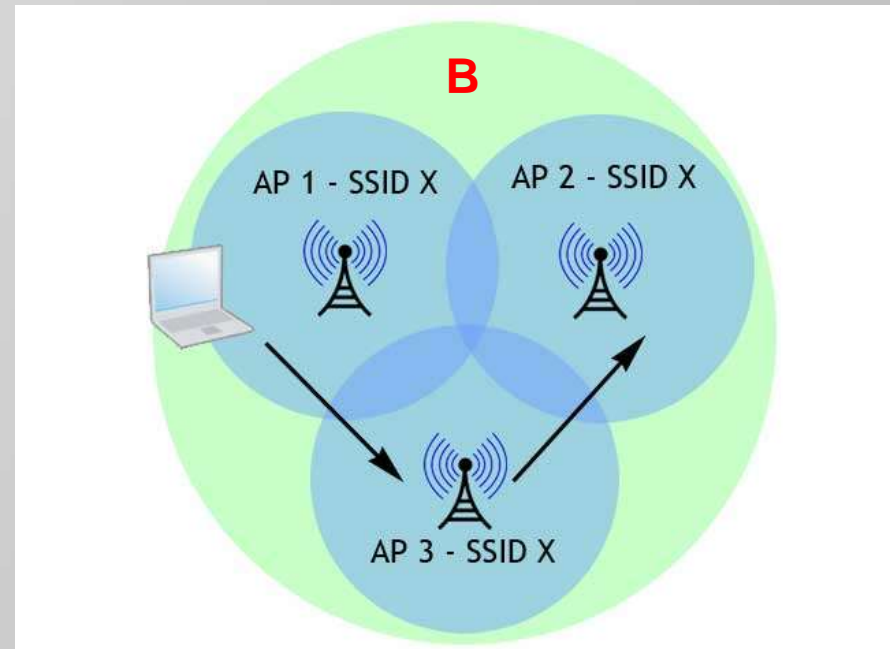
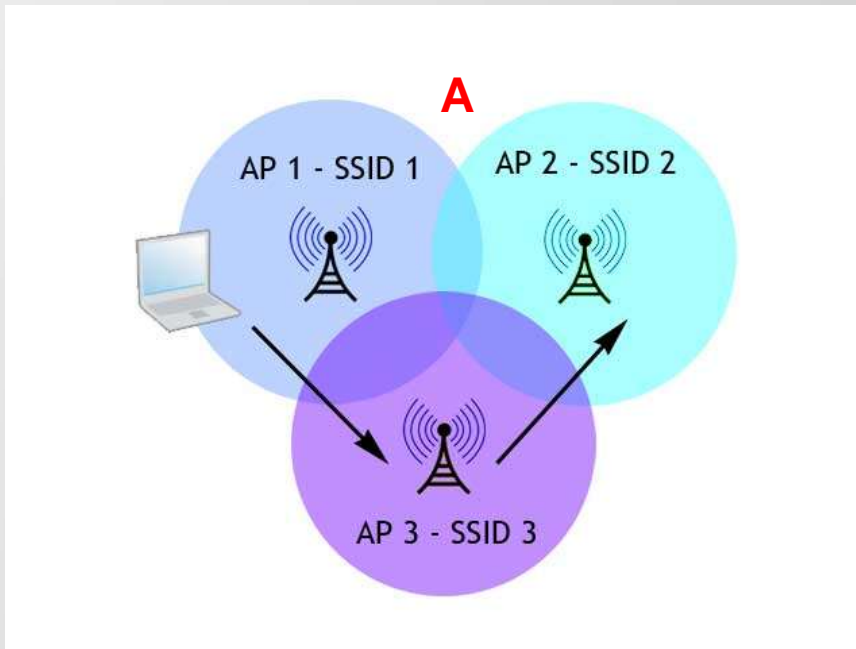
- Buatlah bridge untuk koneksi ke internet (AP LAB MTCNA), bridge interface wlan1 dan ether1.
- Setting IP Laptop satu network dengan IP DHCP client wlan1, gateway menggunakan IP 192.168.1.1.
- Jangan lupa, set mode wlan1 sebagai **station-pseudobridge**, karena mode station tidak bisa di bridge (limitasi protocol 802.11).
- Coba untuk koneksi ke internet, untuk troublesoot coba ping ke masing-masing interface (ether1, bridge, wlan1 & gateway)
- Coba untuk ping antar laptop peserta.
- Coba setting IP laptop menjadi DHCP client, apakah bisa?

Wireless Distribution System

- WDS menjadikan sebuah interface WLAN client dapat dibridge.
- WDS biasa digunakan sebagai repeater (koneksi AP dan AP, bukan lagi AP dan station)
- WDS juga memungkinkan kita membuat satu kesatuan jaringan wireless dengan beberapa akses point.
- Syarat koneksi dengan WDS
 - Mode AP (AP bridge atau bridge) yang mengaktifkan WDS, dan mode station WDS.
 - Mode AP yang mengaktifkan WDS dengan WDS slave
 - Mode WDS slave dengan WDS slave

Wireless Distribution System

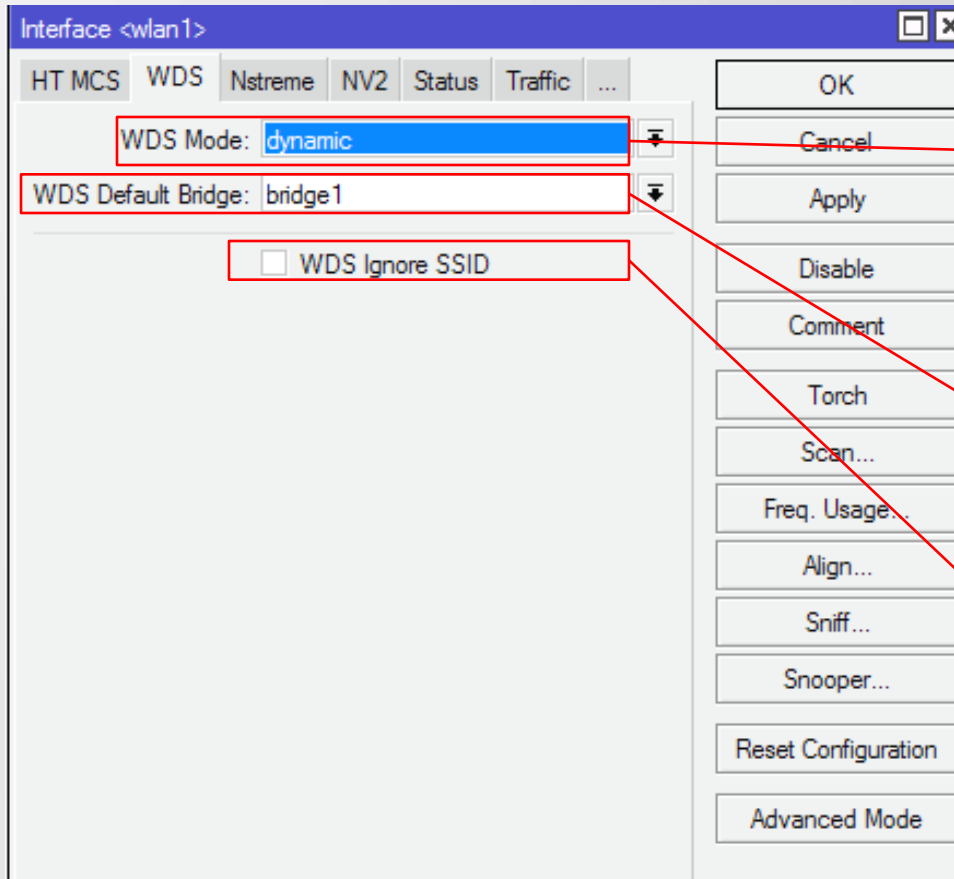
- Dengan topologi A, apabila user berpindah dari area AP1, ke area lain (AP2 / AP3), maka user akan kehilangan koneksi untuk beberapa saat sebelum bergabung dengan AP (atau SSID) yang baru. Meskipun semua AP di konfigurasi dengan SSID yang sama.
- Dengan mengkonfigurasi AP dengan WDS, maka apabila user berpindah dari satu area AP ke area AP lainnya, maka user seakan-akan tetap berada di area yang sama (SSID / IP & Subnet sama)



WDS

- Dengan WDS kita bisa membangun infrastruktur wireless tanpa harus membangun backbone kabel jaringan sebagai interkoneksi antar bridge.
- Fitur WDS memungkinkan kita membuat jaringan wireless yang besar dengan cara membuat link beberapa wireless access point dengan WDS.
- WDS biasanya digunakan untuk membangun jaringan yang besar dimana menarik kabel jaringan adalah tidak memungkinkan/mahal, terbatas, atau secara fisik tidak memungkinkan untuk ditarik.
- Type WDS pada MikroTik
 - WDS Static
 - WDS Dynamic
 - WDS Mesh

WDS-Dinamic



WDS Mode

Static = wds peering mac-address harus ditambahkan secara manual

Dynamic = wds peering mac-address ditambahkan secara otomatis

Dynamic mesh = digunakan dalam topologi jaringan mesh

WDS Default Bridge

WDS akan membentuk virtual interface yang secara otomatis akan ditambahkan ke dalam bridge.

WDS Ignore SSID, bila diaktifkan maka WDS akan membentuk koneksi ke SSID apapun, asal memiliki frekuensi yang sama

WDS - Dynamic

Wireless Tables

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

+ - ✓ ✗ 📄 🔍 Scanner Freq. Usage Alignment Wirele

	Name	Type	L2 MTU	Tx	Rx	Tx
R	wlan1	Wireless (Atheros 11N)	2290	0 bps	0 bps	
DRA	wds1	WDS	2290	0 bps	0 bps	
DRA	wds2	WDS	2290	0 bps	0 bps	
DRA	wds3	WDS	2290	0 bps	0 bps	

Link WDS aktif dan seolah-olah setiap client menjadi child dari AP wlan1

Bridge

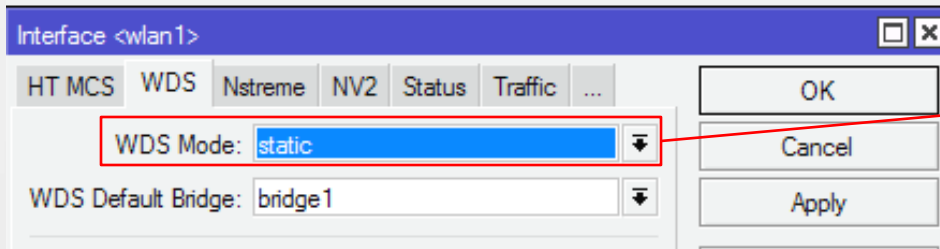
Bridge | Ports | Filters | NAT | Hosts

+ - ✓ ✗ 📄 🔍

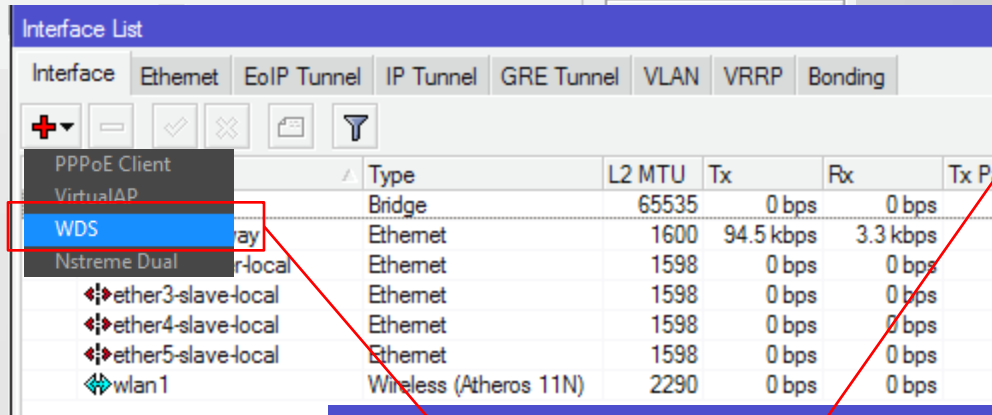
	Interface	Bridge	Priority (p...	Path Cost	Horizon	Role
	ether1-gateway	bridge1	80	10		designated port
D	wds1	bridge1	80	91		designated port
D	wds2	bridge1	80	100		designated port
D	wds3	bridge1	80	136		designated port
	wlan1	bridge1	80	10		designated port

Interface wds1 ditambahkan ke ports bridge1 secara otomatis/dinamic (D), karena setting pada WDS mode = dynamic

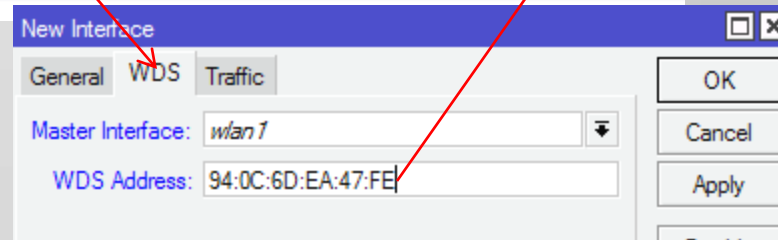
WDS - Static



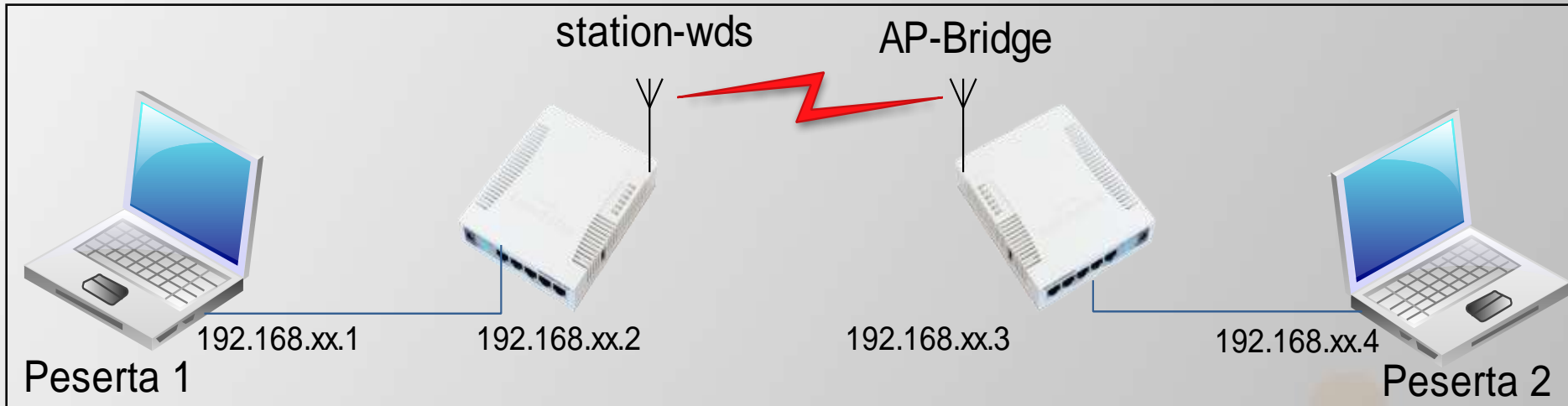
WDS Mode static, mac address dari client harus ditambahkan secara manual ke sebuah interface WDS baru (add interface WDS)



Add interface WDS, dan masukkan mac address client.



LAB – WDS Bridge

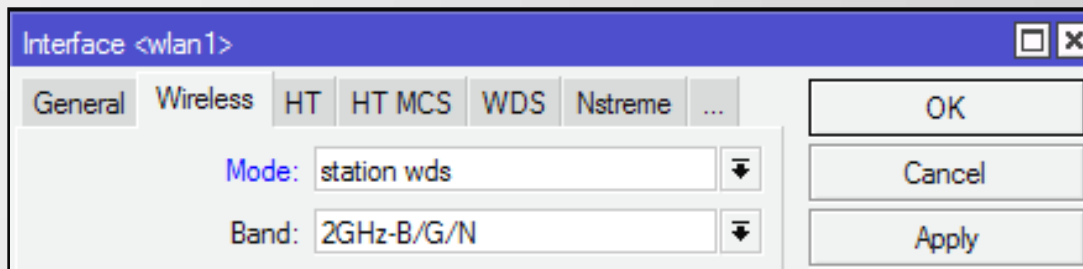


Peserta 1 → Wireless mode = AP Bridge

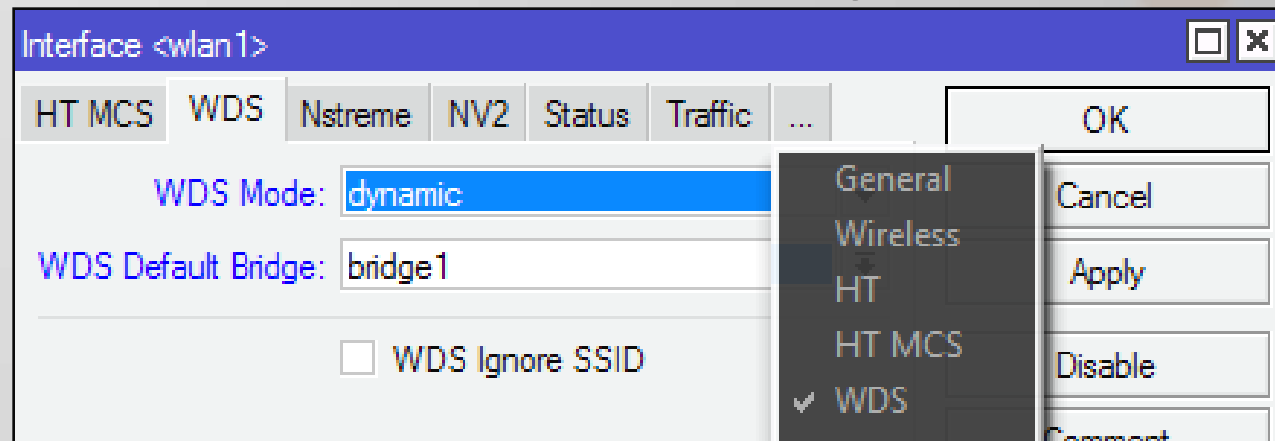
Peserta 2 → Wireless mode = Station WDS

LAB – WDS Bridge

Wireless WDS station setting



Access Point Wireless Setting









LAB – WDS Bridge

Interface wds1

Wireless Tables

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

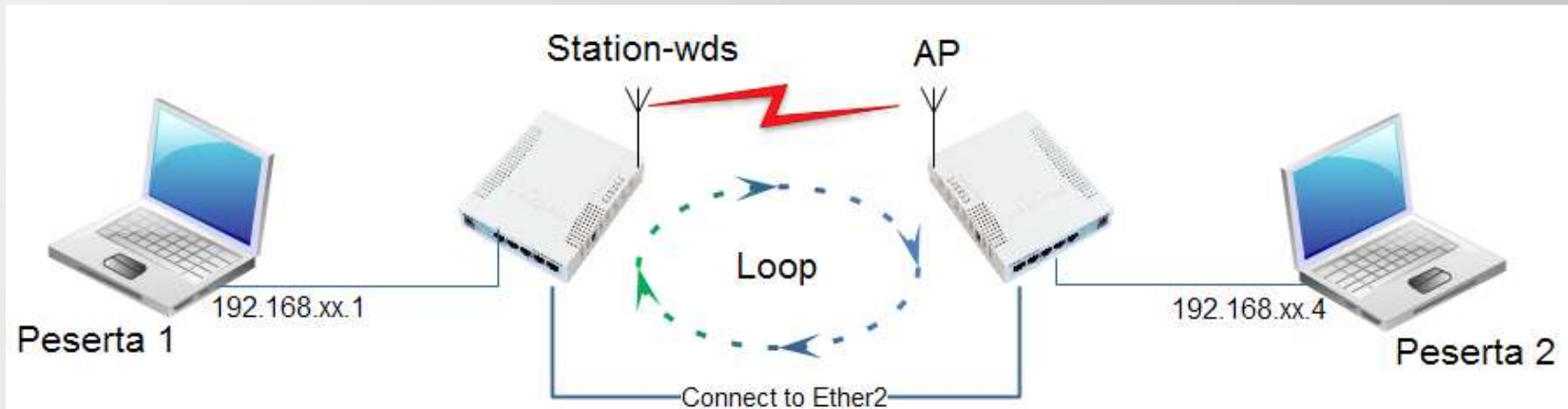






 Scanner | Freq. Usage | Alignment | Wireless Sniffer | Wireless Snoopers | Find

	Name	Type	L2 MTU	Tx	Rx	T...	R.	T..	R T.	R.	MAC Address	ARP
R	wlan1	Wireless (Atheros 11N)	2290	624 bps	624 bps	1	1	0	0	0	00:0C:42:E3:8E:11	enabled
DRA	wds1	WDS	2290	624 bps	624 bps	1	1	0	0	0	00:0C:42:E3:8E:11	enabled

Spanning Tree Protocol (STP)

- Bridge loop terjadi jika terdapat lebih dari 1 jalur dalam network bridge.
- Dampak dari bridge loop ini adalah broadcast storms.
- Broadcast storms adalah pengiriman paket (multicast atau unicast yang destination addressnya belum diketahui oleh bridge) terus berputar-putar (looping) dalam network tanpa henti.
- STP (Spanning Tree Protocol) Protocol digunakan untuk menghindari terjadinya bridge loop
- STP juga dapat dimanfaatkan sebagai fail over system
- RSTP Protocol adalah protocol STP yang memiliki kecepatan failover lebih tinggi.

Bridge Loop & RSTP



Bridge

Bridge Ports Filters NAT Hosts

+ - ✓ ✗ 📁 📏 Settings

	Name	Type
R	↑↕bridge1	Bridge

Interface <bridge1>

General STP Status Traffic

Protocol Mode: none stp rstp

Priority: 8000 hex

Max Message Age: 00:00:20

Forward Delay: 00:00:15

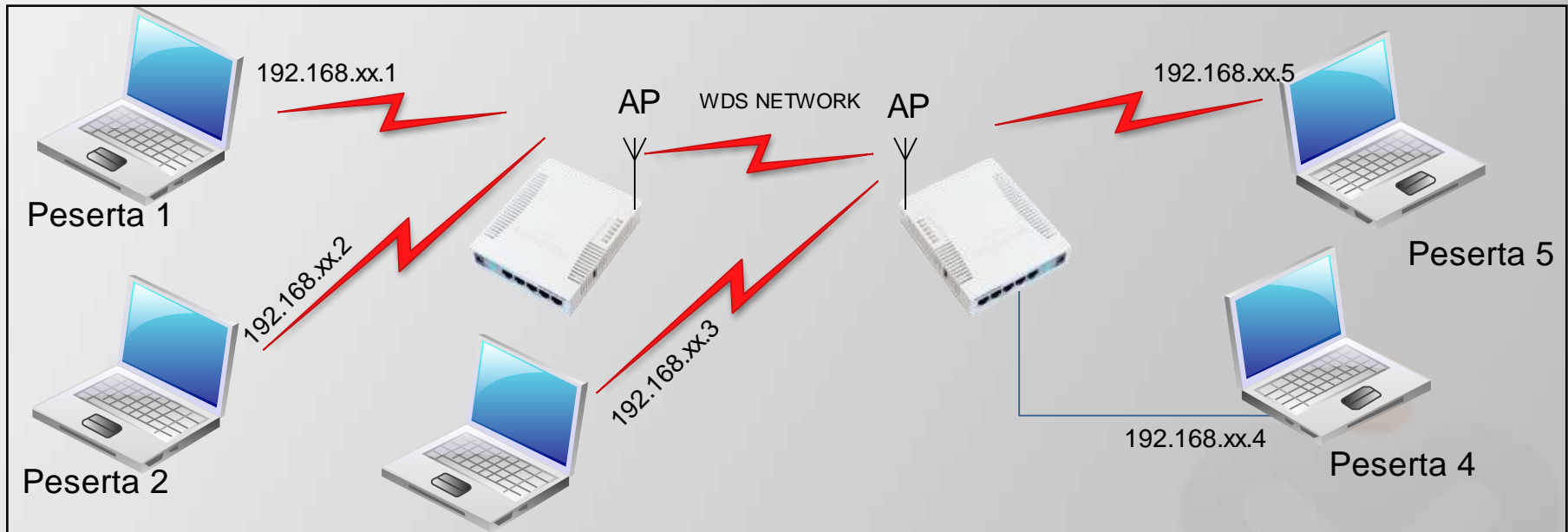
Transmit Hold Count: 6

Ageing Time: 00:05:00

OK Cancel Apply Disable Comment Copy Remove

Errors	Rx Errors	MAC Address
0	0	D4:CA:6D:26:07:B7

LAB – WDS Slave



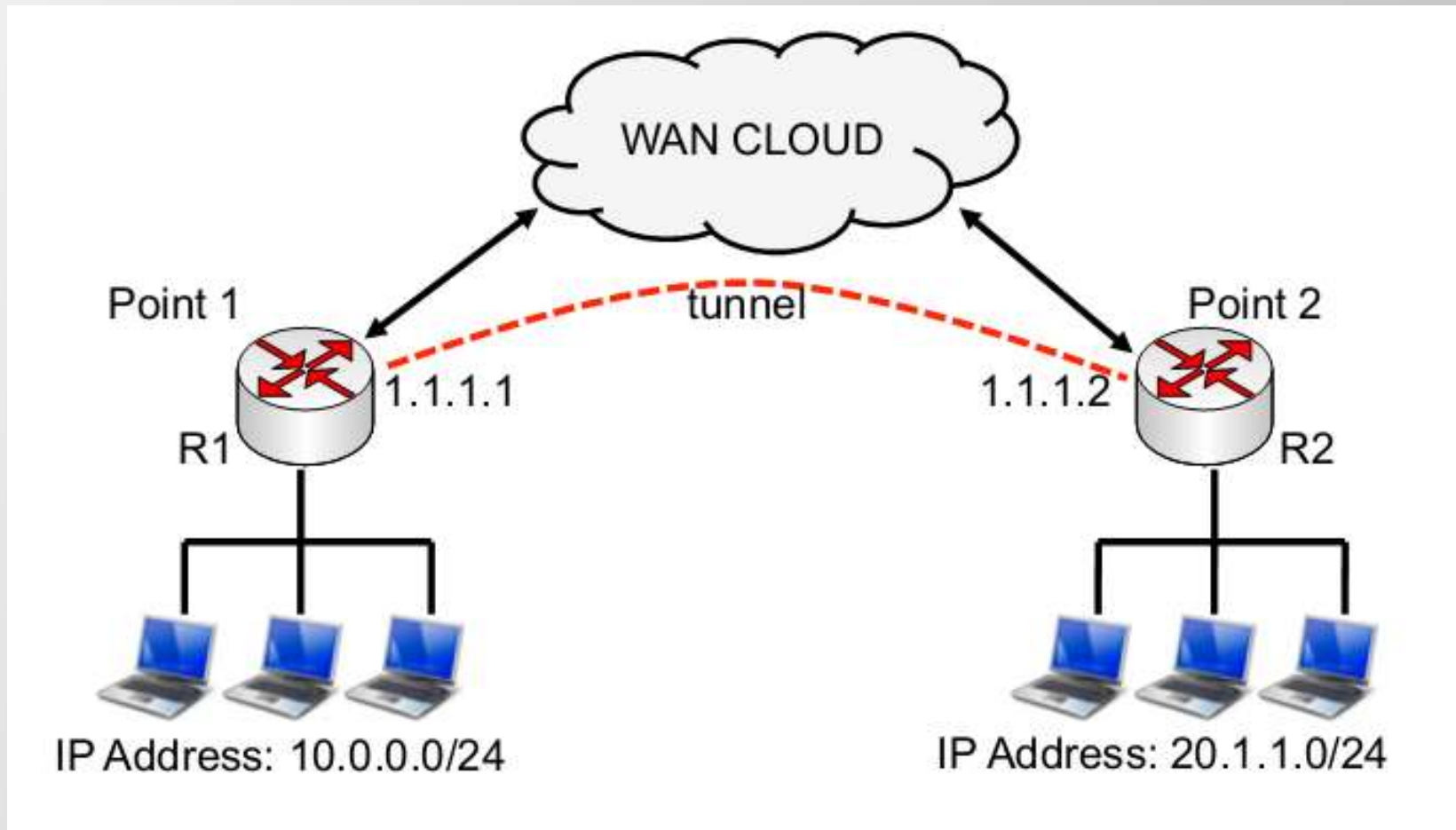
Tunnel



Tunnel

- Tunnel adalah sebuah metode penyelubungan (encapsulation) paket data di jaringan.
- Paket data mengalami sedikit pengubahan atau modifikasi, yaitu penambahan header dari tunnel
- Ketika data sudah melewati tunnel dan sampai di tujuan (ujung) tunnel, maka header dari paket data akan dikembalikan seperti semula (header tunnel dilepas).

Tunnel



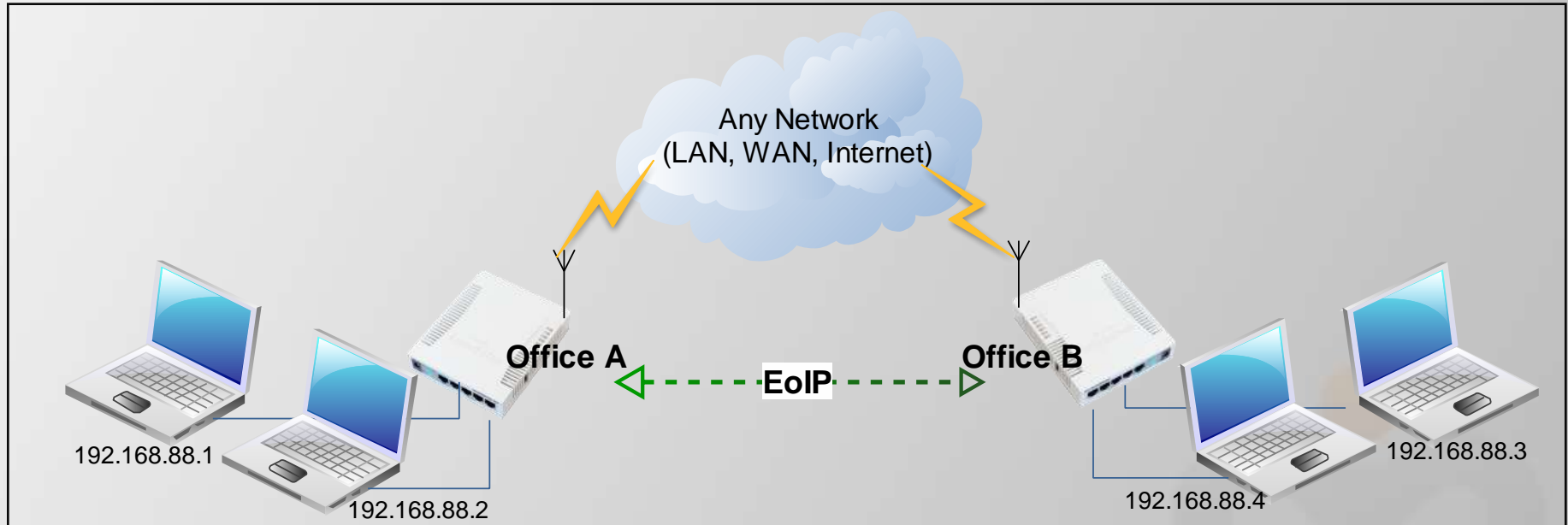
VPN

- VPN adalah sebuah cara aman untuk mengakses local area network dengan menggunakan internet atau jaringan publik.
- Tunnel atau terowongan merupakan kunci utama pada VPN, koneksi pribadi dalam VPN dapat terjadi dimana saja selama terdapat tunnel.

EOIP

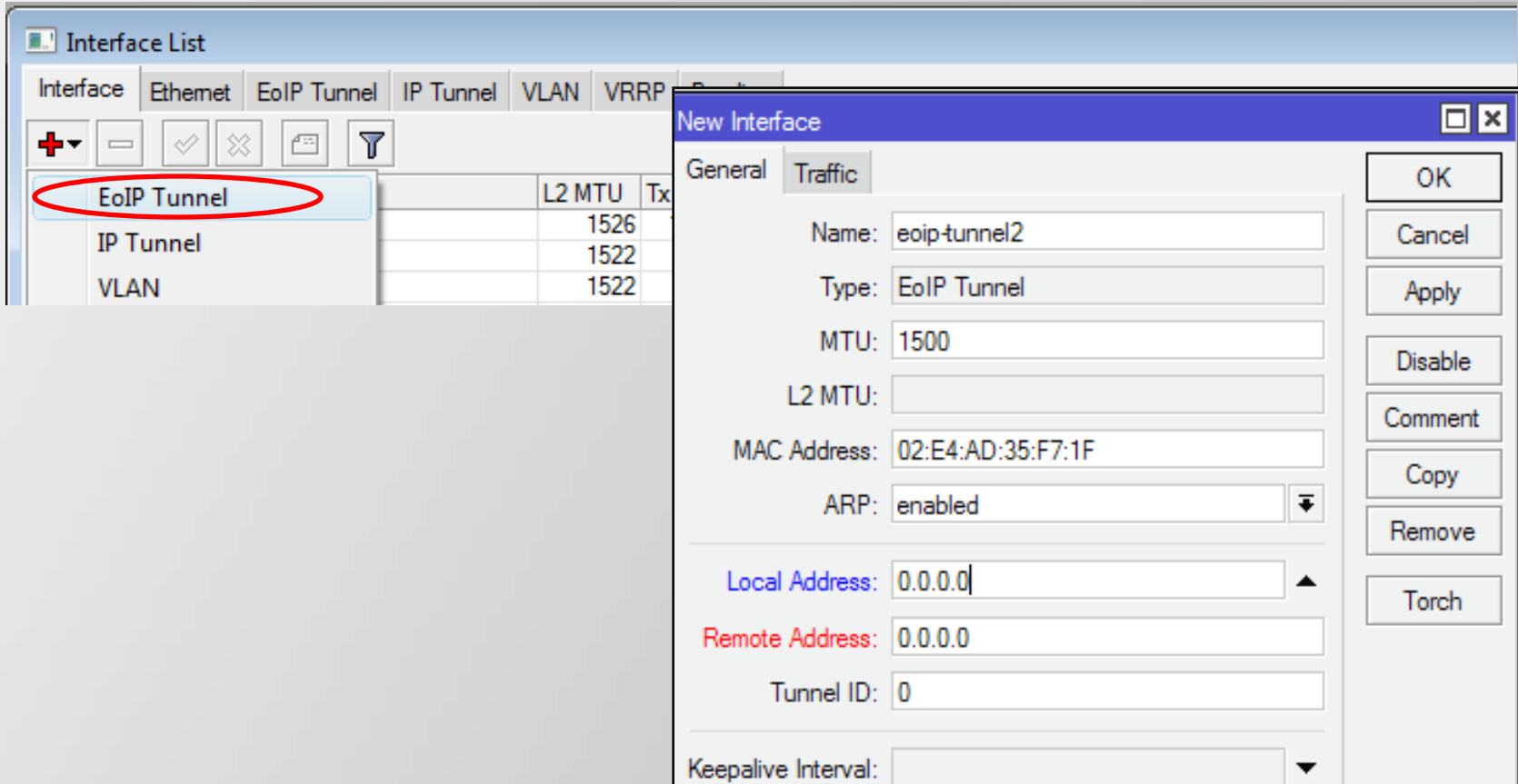
- EOIP merupakan protocol proprietary untuk membangun bridge dan tunnel antar router Mikrotik, dimana interface EOIP akan dianggap sebagai ethernet
- Tunnel ID di EOIP harus sama diantara kedua interface EOIP
- MAC Address diantara interface EOIP harus dibedakan

LAB -EOIP



EoIP Tunnel

- New Interface EoIP Tunnel



The screenshot shows the 'Interface List' window with the 'EoIP Tunnel' option selected. The 'New Interface' dialog box is open, showing the configuration for a new EoIP Tunnel interface named 'eoiptunnel2'.

Interface	Ethernet	EoIP Tunnel	IP Tunnel	VLAN	VRRP

Interface	L2 MTU	Tx
EoIP Tunnel	1526	
IP Tunnel	1522	
VLAN	1522	

New Interface (General tab)

Name: eoiptunnel2

Type: EoIP Tunnel

MTU: 1500

L2 MTU:

MAC Address: 02:E4:AD:35:F7:1F

ARP: enabled

Local Address: 0.0.0.0

Remote Address: 0.0.0.0

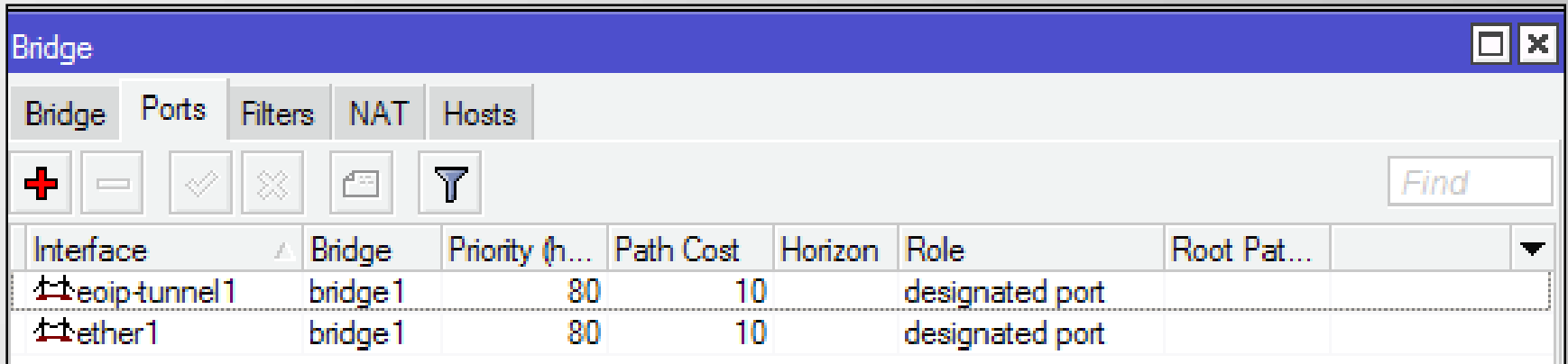
Tunnel ID: 0

Keepalive Interval:

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

EoIP Tunnel

- Masukkan dalam interface bride interface eoIP dan ether1



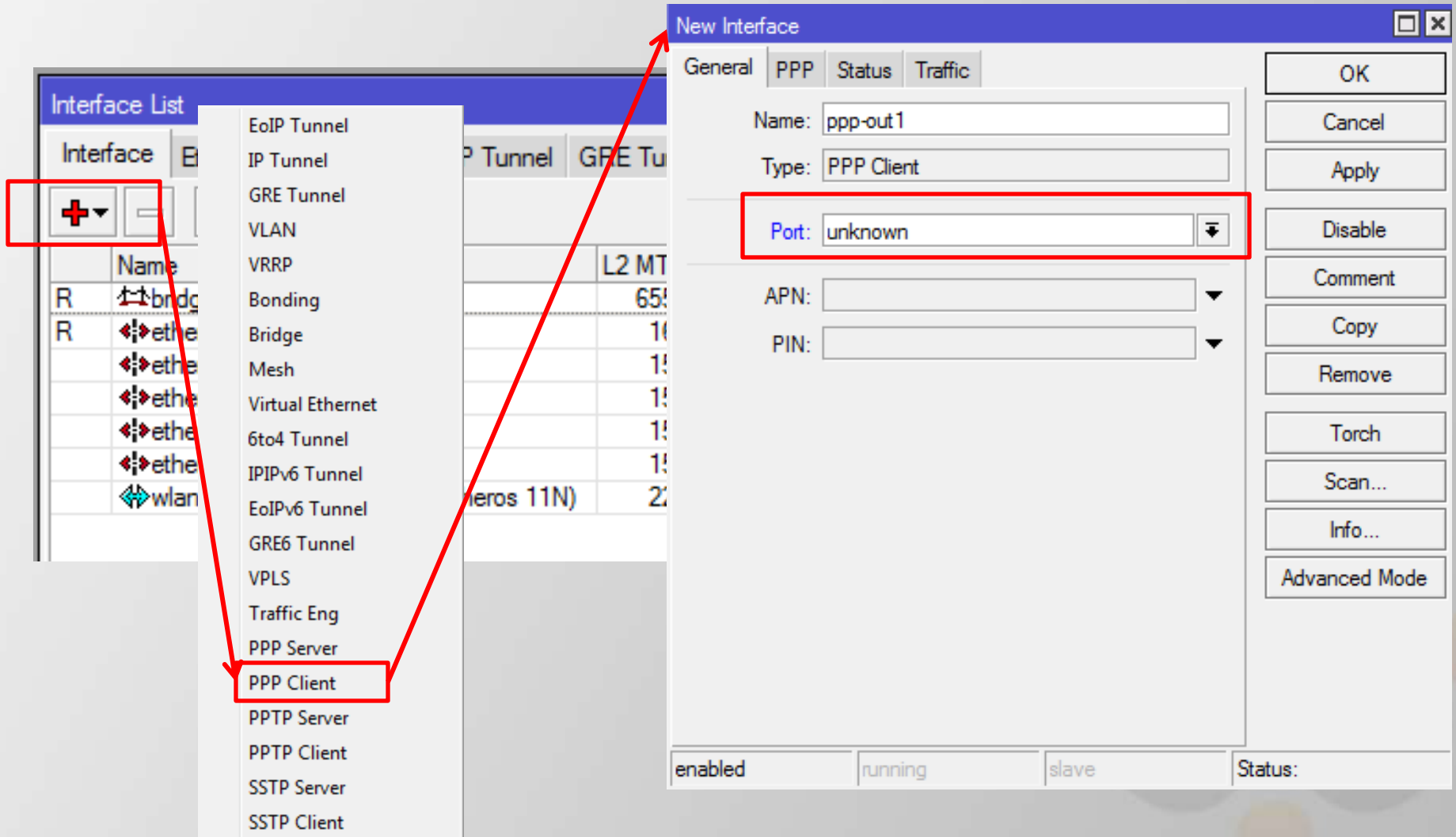
The screenshot shows a network configuration window titled "Bridge". It has tabs for "Bridge", "Ports", "Filters", "NAT", and "Hosts". Below the tabs are several icons: a red plus sign, a minus sign, a checkmark, a cross, a document, and a funnel. A "Find" search box is on the right. The main area contains a table with the following data:

Interface	Bridge	Priority (h...	Path Cost	Horizon	Role	Root Pat...
↕ eoip-tunnel1	bridge 1	80	10		designated port	
↕ ether1	bridge 1	80	10		designated port	

PPP

- PPP (Point to Point Protocol) adalah protocol layer 2 yang digunakan untuk komunikasi secara serial.
- Untuk menjalankan koneksi PPP, mikrotik RouterOS harus memiliki port/interface serial, line telephone port berupa RJ11 (PSTN), atau modem seluler (PCI atau PCMCIA)
- Untuk terbentuk koneksi PPP dilakukan melalui dial up nomer telepon tertentu ke ISP (misal nomor *99***1#).
- Kemudian ppp baru mendapatkan IP address untuk koneksi internet.
- MikroTik dapat digunakan sebagai PPP server dan atau PPP client.

Setting PPP Client



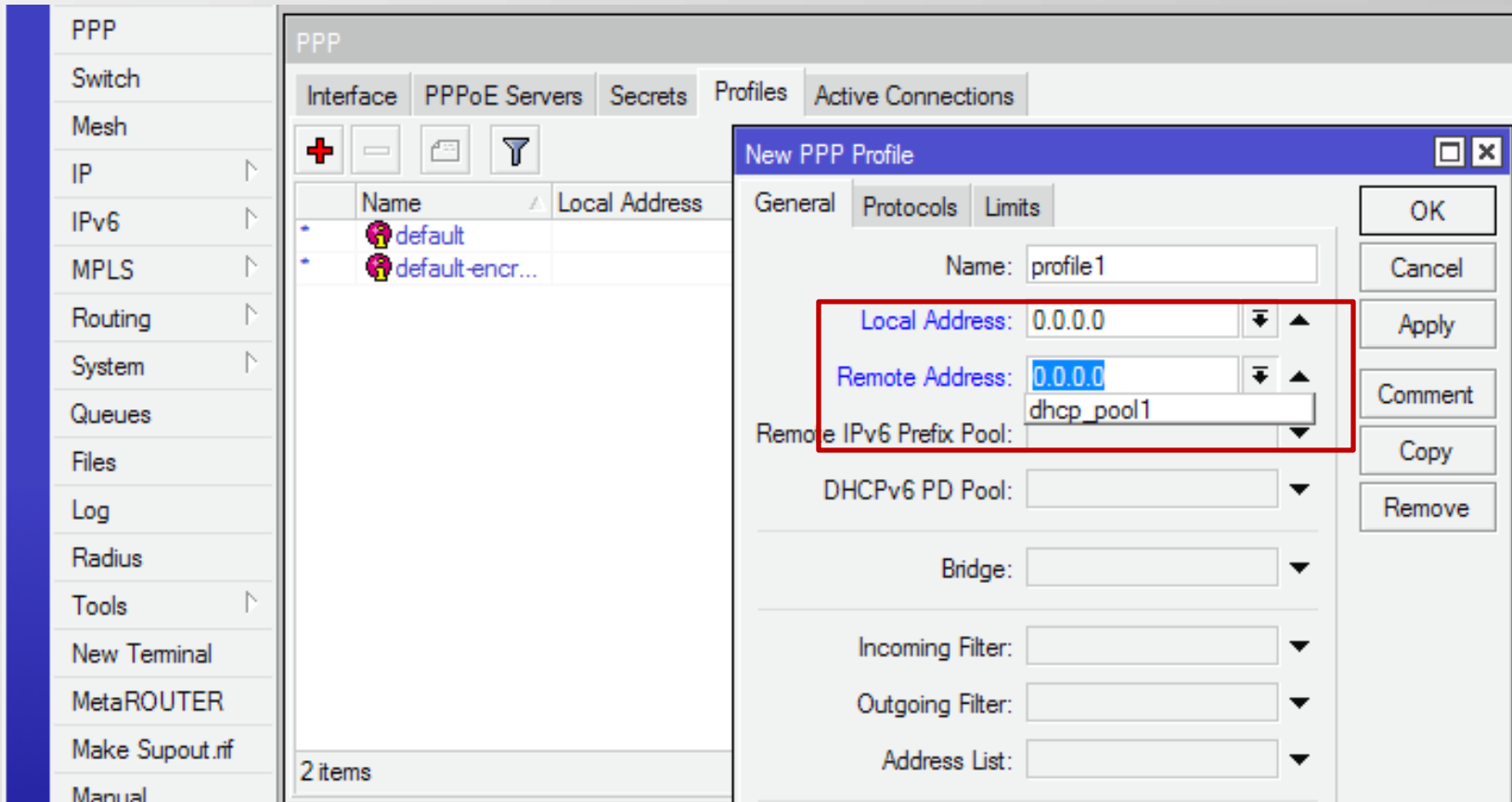
The image shows two windows from a network configuration application. On the left is the 'Interface List' window, which has a '+' button in the top-left corner highlighted with a red box. A red arrow points from this '+' button to the 'New Interface' dialog box on the right. In the 'New Interface' dialog, the 'General' tab is active. The 'Name' field contains 'ppp-out1' and the 'Type' is set to 'PPP Client'. The 'Port' dropdown menu is highlighted with a red box and currently shows 'unknown'. Below the dialog, there are status indicators for 'enabled', 'running', and 'slave', along with a 'Status:' label. On the right side of the dialog, there are several buttons: 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Torch', 'Scan...', 'Info...', and 'Advanced Mode'.

PPTP Tunneling

- PPTP melakukan tunneling IP packet kedalam PPP data link layer menggunakan protocol TCP dan GRE (Generic Routing Encapsulation).
- PPTP menggunakan enkripsi MPPE (Microsoft Point-to-Point Encryption) 40 – 128 bit
- PPTP menggunakan port TCP 1723
- PPTP banyak digunakan karena hampir semua OS dapat menjalankan PPTP client.
- Sebelum menjalankan PPTP server, hal yang perlu diperhatikan adalah setting **PPP Secret** dan **PPP Profiles**.

PPP Profile

- PPP Profile digunakan untuk setting ip local address dan remote address, remote address dapat menggunakan ip pool.



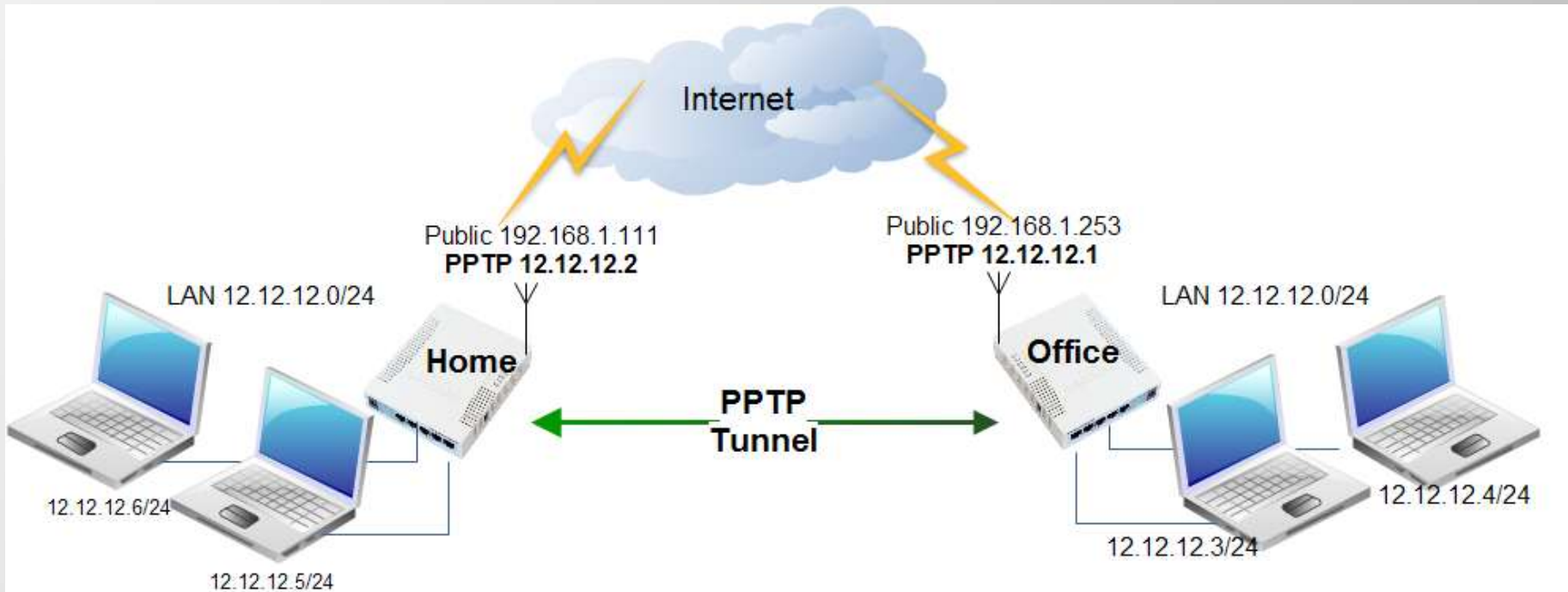
The screenshot shows the Mikrotik WinBox interface. On the left is a navigation tree with categories like PPP, Switch, Mesh, IP, IPv6, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, Make Supout.rif, and Manual. The main window is titled 'PPP' and has tabs for 'Interface', 'PPPoE Servers', 'Secrets', 'Profiles', and 'Active Connections'. The 'Profiles' tab is active, showing a table with columns 'Name' and 'Local Address'. Two profiles are listed: 'default' and 'default-encr...'. A 'New PPP Profile' dialog box is open over the main window. The dialog has tabs for 'General', 'Protocols', and 'Limits'. The 'General' tab is selected. The 'Name' field contains 'profile 1'. The 'Local Address' field is set to '0.0.0.0'. The 'Remote Address' field is set to '0.0.0.0'. The 'Remote IPv6 Prefix Pool' dropdown is set to 'dhcp_pool1'. A red rectangular box highlights the 'Local Address', 'Remote Address', and 'Remote IPv6 Prefix Pool' fields. On the right side of the dialog, there are buttons for 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove'.

PPP Secret

- Semua koneksi yang menggunakan protocol PPP selalu melibatkan autentikasi username dan password.
- Secara local, username dan password ini disimpan dan diatur dalam PPP secret.
- Username dan password ini juga dapat disimpan dalam RADIUS server terpisah.
- PPP Secret (database local PPP) menyimpan username dan password yang akan diberikan ke pelanggan/user. PPP secret dipakai untuk koneksi client ; **async**, **l2tp**, **openvpn**, **pppoe**, **pptp** dan **sstp**.

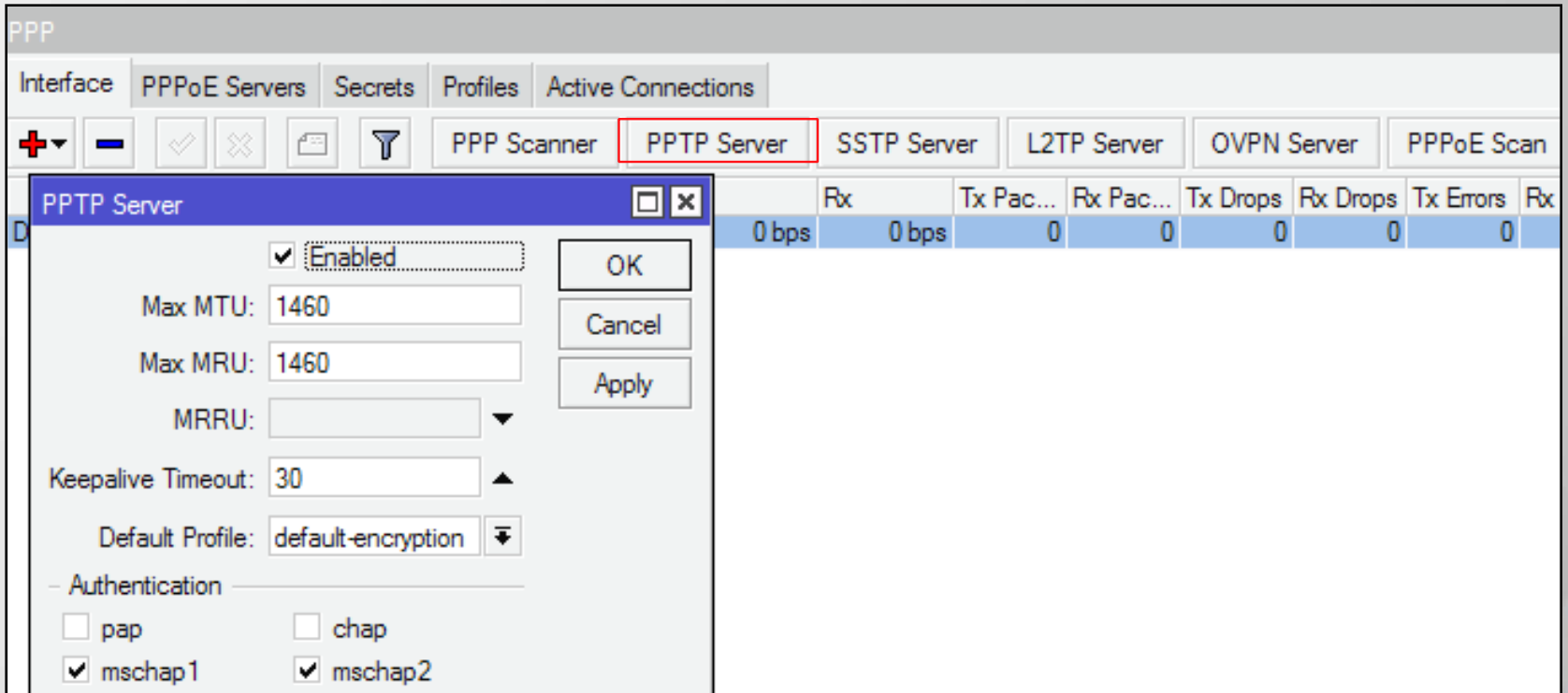
LAB Tunneling (MK-MK)

- PPTP antar router mikrotik (router home dan office)



Mengaktifkan PPTP Server

- Aktifkan PPTP server pada menu PPP>Interface>PPTP Server



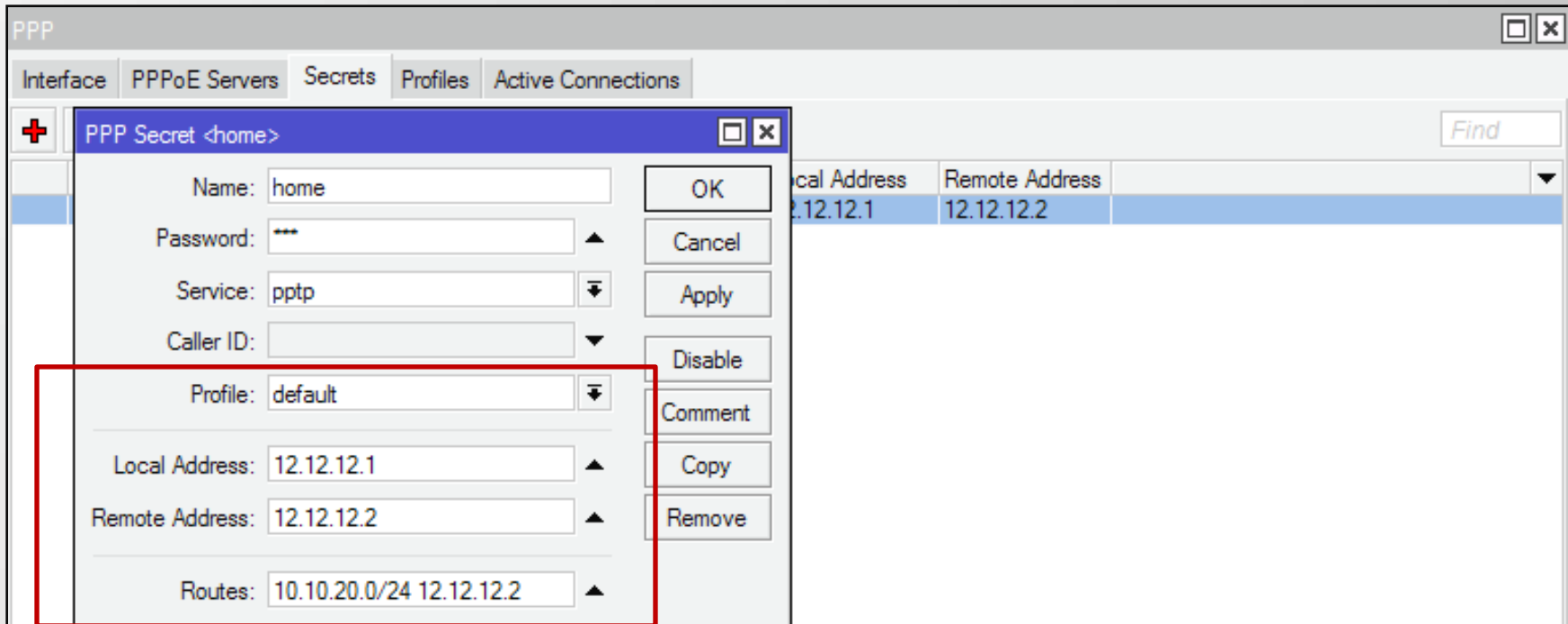
The screenshot shows the PPP configuration interface with the PPTP Server dialog box open. The dialog box is titled "PPTP Server" and has the following settings:

- Enabled
- Max MTU: 1460
- Max MRU: 1460
- MRRU: [dropdown menu]
- Keepalive Timeout: 30
- Default Profile: default-encryption
- Authentication:
 - pap
 - chap
 - mschap1
 - mschap2

The background interface shows the PPP configuration window with tabs for Interface, PPPoE Servers, Secrets, Profiles, and Active Connections. The PPTP Server tab is selected and highlighted with a red box. Below the tabs, there are buttons for PPP Scanner, PPTP Server, SSTP Server, L2TP Server, OVPN Server, and PPPoE Scan. A table at the bottom right shows statistics for Rx, Tx Pac..., Rx Pac..., Tx Drops, Rx Drops, Tx Errors, and Rx.

	Rx	Tx Pac...	Rx Pac...	Tx Drops	Rx Drops	Tx Errors	Rx
	0 bps	0 bps	0	0	0	0	0

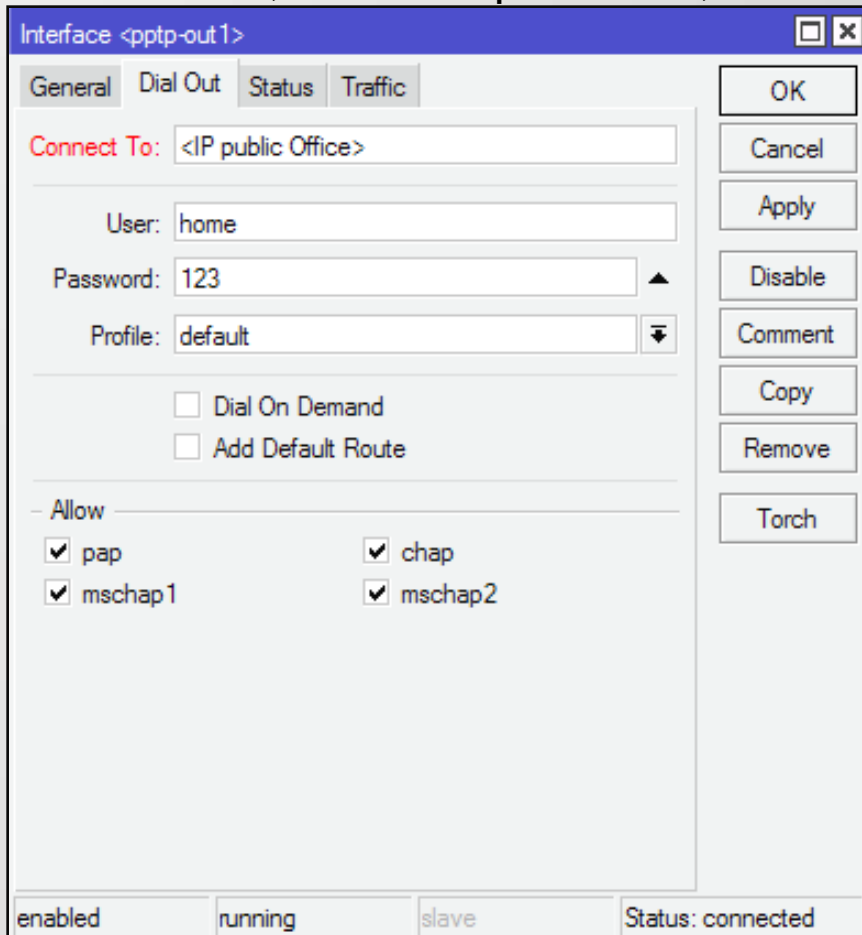
PPP Secret



- Profile = mengambil dari ppp profile
- Local & remote address = diisi IP untuk koneksi PPTP
- Routes = Disini kita menambahkan konfigurasi untuk routes 10.10.20.0/24 12.12.12.2 yang akan ditambahkan secara otomatis apabila terbentuk koneksi dari pptp client

MikroTik PPTP Client

- Add new interface pptp, pada tab Dial Out isikan dengan IP public dari router Office, user dan password, kemudian apply



Interface <pptp-out1>

General Dial Out Status Traffic

Connect To: <IP public Office>

User: home

Password: 123

Profile: default

Dial On Demand

Add Default Route

Allow

pap chap

mschap1 mschap2

OK

Cancel

Apply

Disable

Comment

Copy

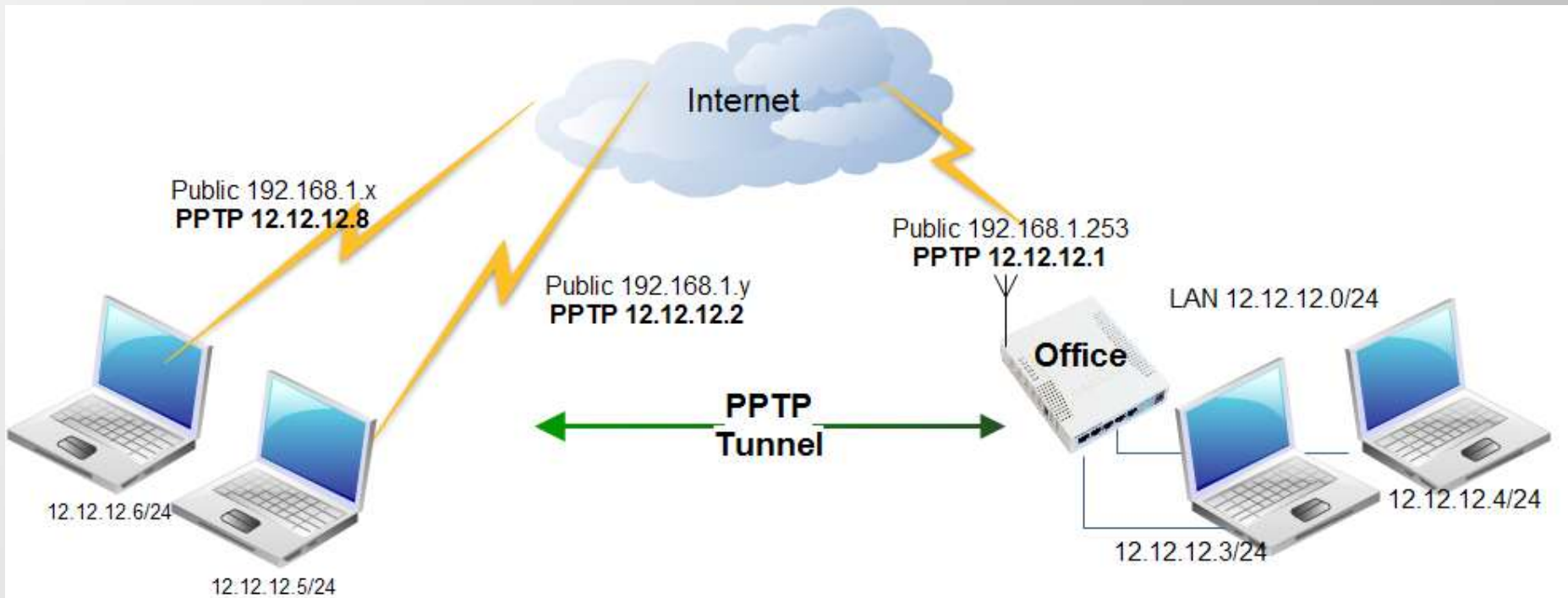
Remove

Torch

enabled running slave Status: connected

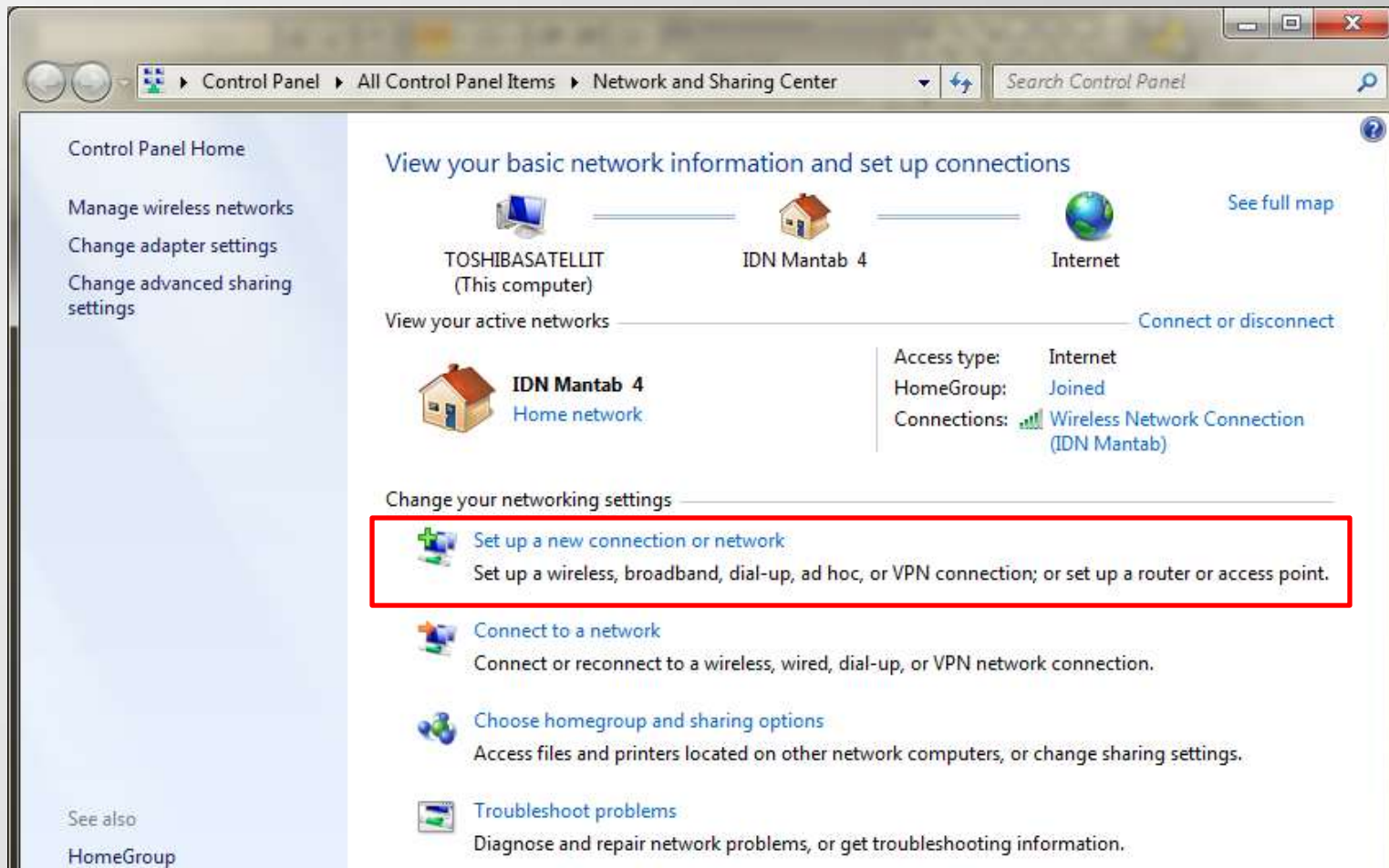
LAB Tunneling (MK-Laptop/PC)

- Koneksi PPTP client dengan Windows



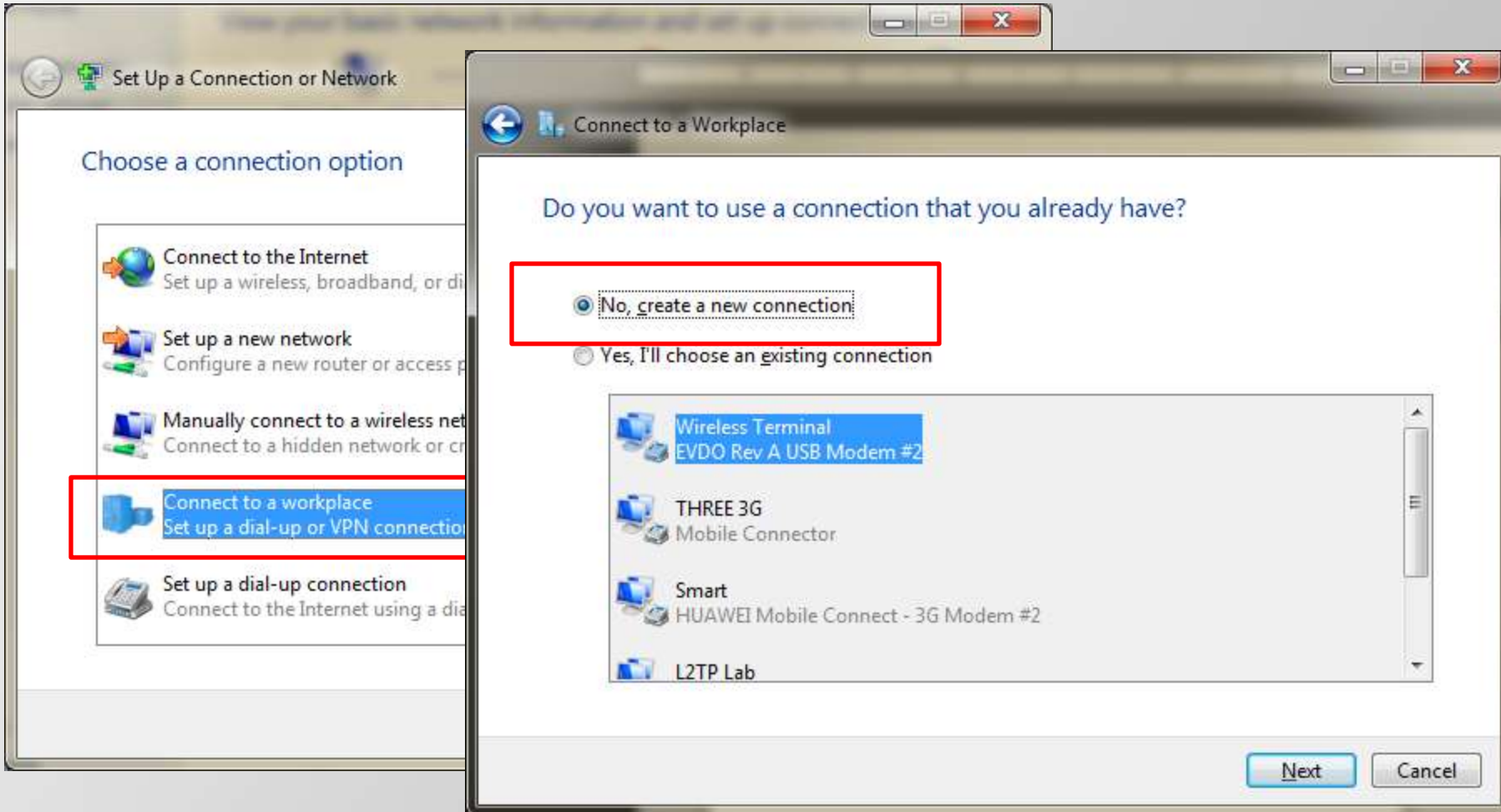
(Windows) PPTP Client

- Setup New Connection di Network Connection



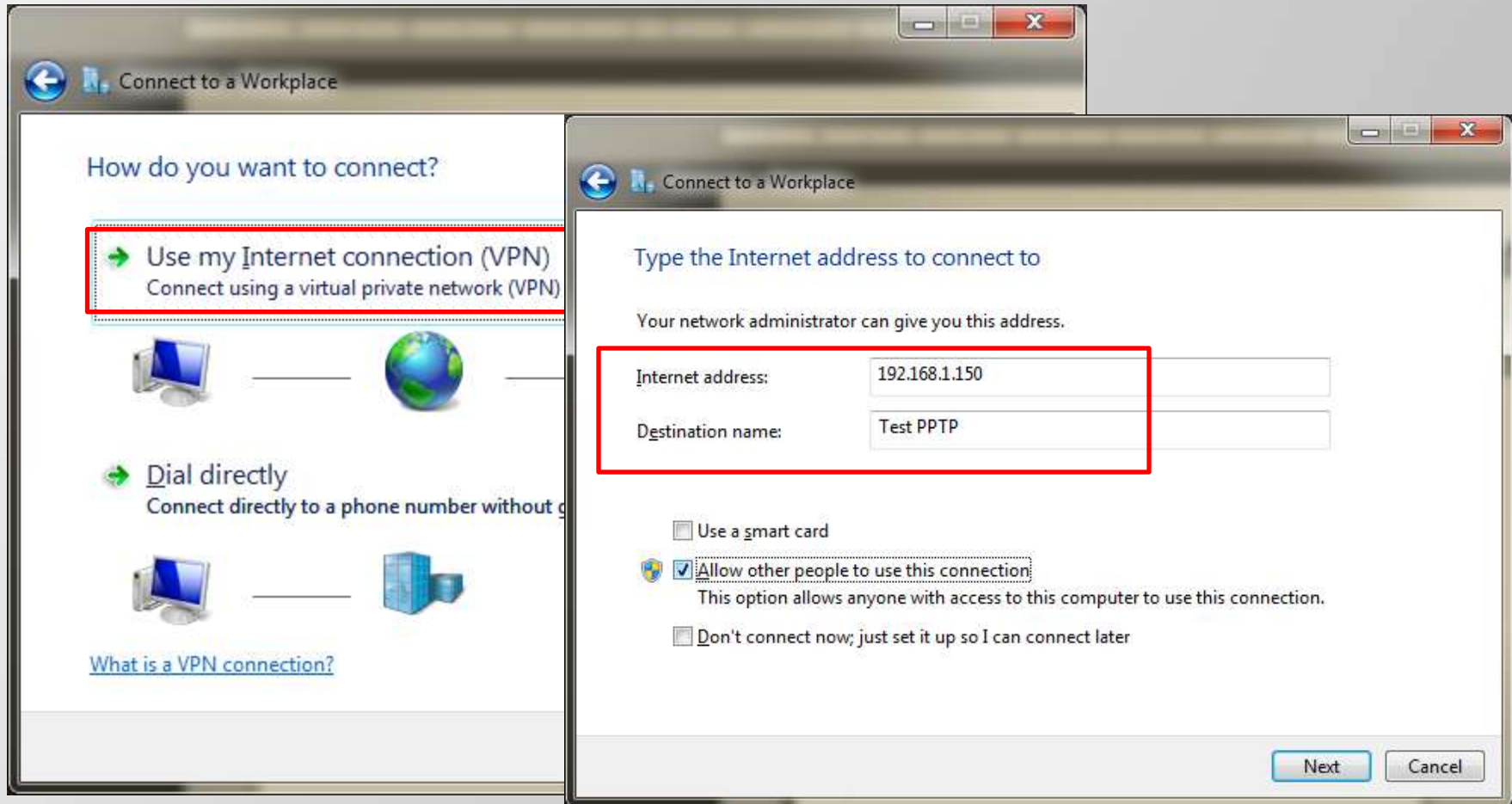
(Windows) PPTP Client

- Setup New Connection di Network Connection



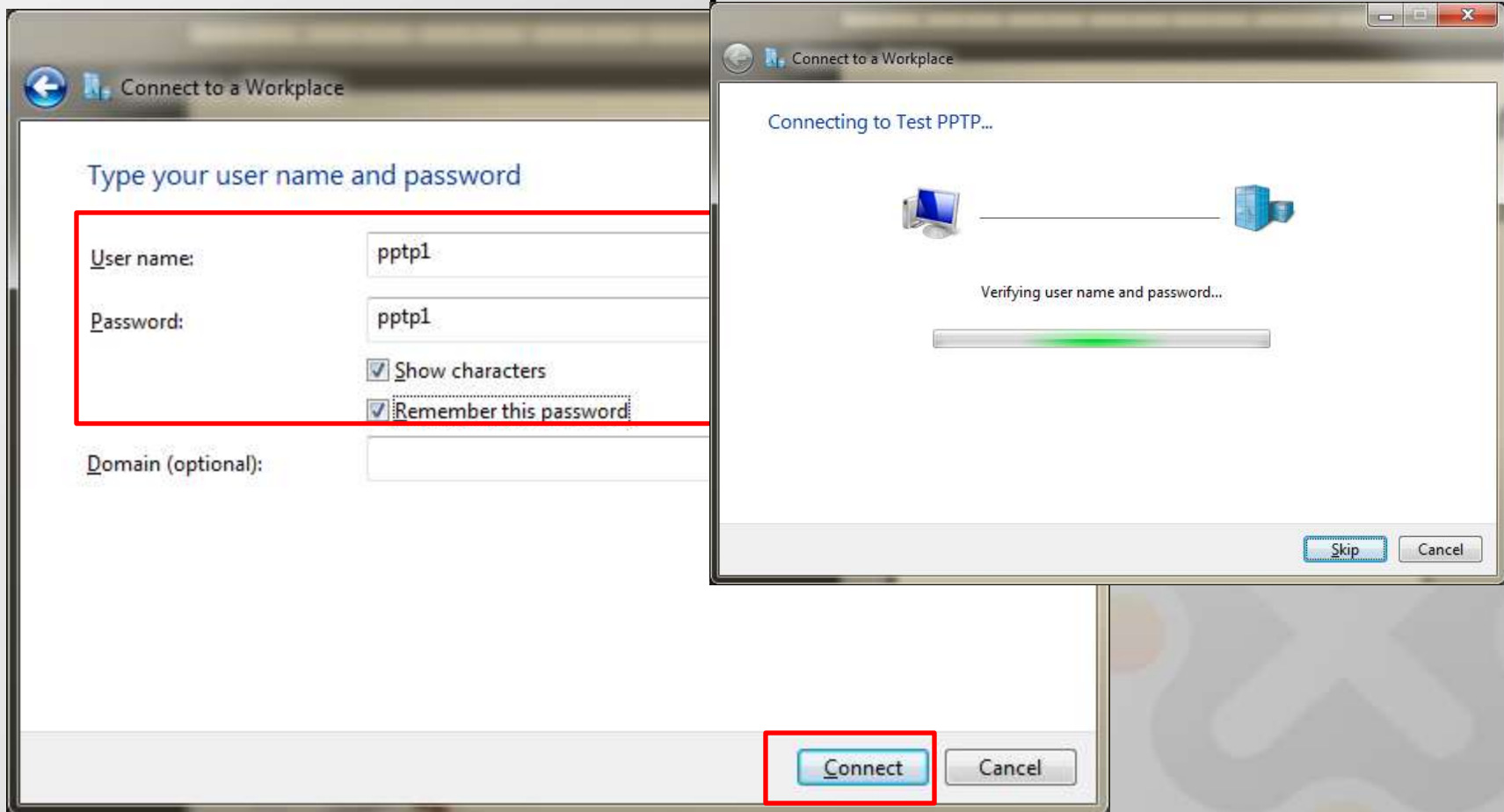
(Windows) PPTP Client

- Pilih Connect Using VPN & Isikan IP PPTP Server



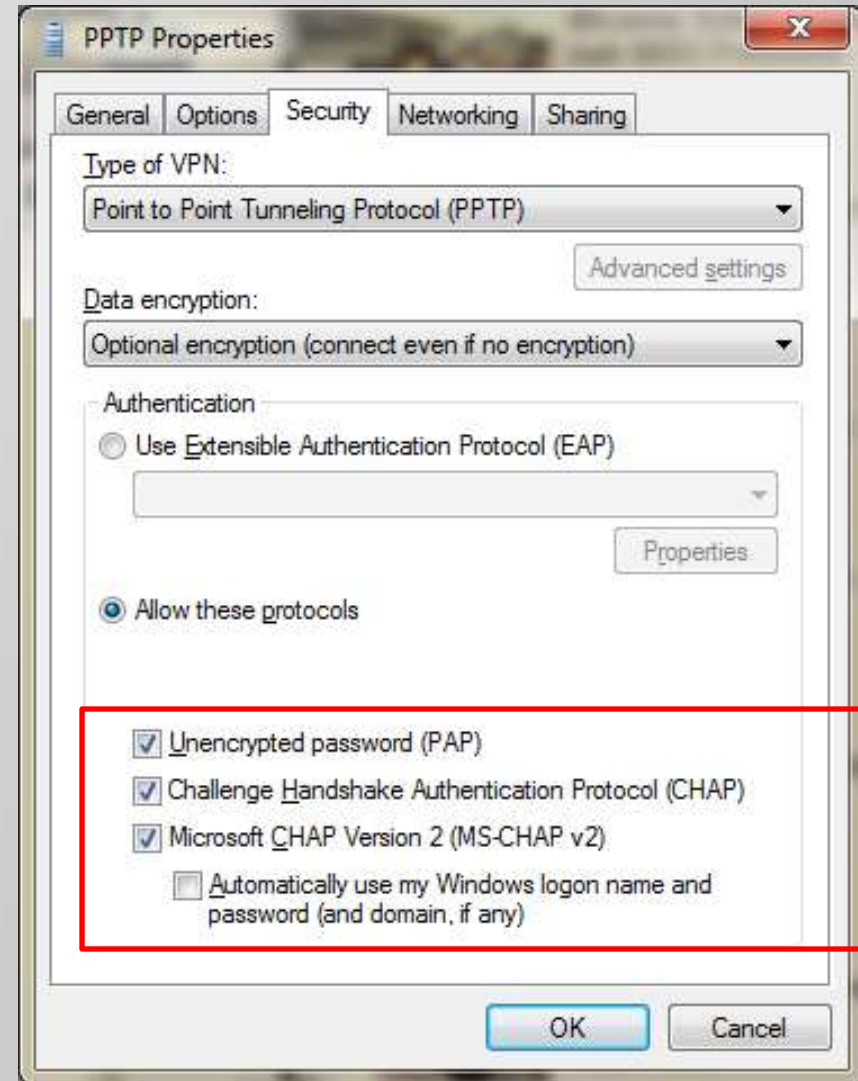
(Windows) PPTP Client

- Masukkan username & password PPTP-Client



(Windows) PPTP Client

- Set security type, samakan dengan setting pada PPTP servernya



PPTP Traffic Analyze

Torch (Running)

- Basic
 Interface: wlan1
 Entry Timeout: 00:00:03 s

- Collect
 Src. Address Src. Address6
 Dst. Address Dst. Address6
 MAC Protocol Port
 Protocol VLAN Id

- Filters
 Src. Address: 0.0.0.0/0
 Dst. Address: 0.0.0.0/0
 Src. Address6: ::/0
 Dst. Address6: ::/0
 MAC Protocol: all
 Protocol: any
 Port: any
 VLAN Id: any

Start
 Stop
 Close
 New Window

Et...	Protocol	Src.	Dst.	VLAN Id	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	6 (tcp)	192.168.10.6:50952	192.168.10.1:8291 (winbox)		5.9 kbps	3.3 kbps	2	4
800 (ip)	47	192.168.10.6	192.168.10.1		342.2 k...	36.2 kbps	47	34
800 (ip)	17 (udp)	192.168.10.5:28426	8.8.4.4:53 (dns)		0 bps	324 bps	0	0

- Apabila kita browsing di internet tidak, trafik aktual tidak terdeteksi.
- Koneksi yang terdeteksi adalah koneksi tunnel PPTP dengan Protocol 47 (GRE)

L2TP Server

- Layer 2 Tunneling Protocol (L2TP) adalah jenis tunneling & encapsulation lain untuk protocol PPP.
- L2TP mensupport non-TCP/IP protocols (Frame Relay, ATM and SONET).
- L2TP dikembangkan atas kerja sama antara Cisco dan Microsoft untuk menggabungkan fitur dari PPTP dengan protocol proprietary Cisco yaitu protokol Layer 2 Forwarding(L2F).
- L2TP tidak melakukan enkripsi paket, untuk enkripsi biasanya L2TP dikombinasikan dengan IPsec.
- L2TP menggunakan UDP port 1701.

L2TP Server

PPP

Interface | PPPoE Servers | Secrets | Profiles | Active Connections

Name	Type
DR <<-> <l2tp-l2tp>	L2TP
R <<-> <speedy>	PPPoE

L2TP Server

Enabled

Max MTU:

Max MRU:

MRRU:

Default Profile: ▾

- Authentication -

pap chap
 mschap1 mschap2

Pac...	Rx Pac...	Tx Drops	Rx Drops	Tx Errors	Rx Errors
1	1	0	0	1	0
1	1	0	0	0	0

PPP

Interface | PPPoE Servers | Secrets | Profiles | Active Connections

PPP Authentication & Accounting

Name	Password	Service	Caller ID	Profile
l2tp	*****	l2tp		default
pptp	*****	pptp		pptp-profile

PPP Secret <l2tp>

Name:

Password:

Service: ▾

Caller ID:

Profile: ▾

Local Address:

Remote Address:

MikroTik L2TP Client

Interface <l2tp-out1>

General Dial Out Status Traffic

Server Address: 192.168.2.118

User: heru

Password: *****

Profile: default-encryption

Dial On Demand

Add Default Route

- Allow -

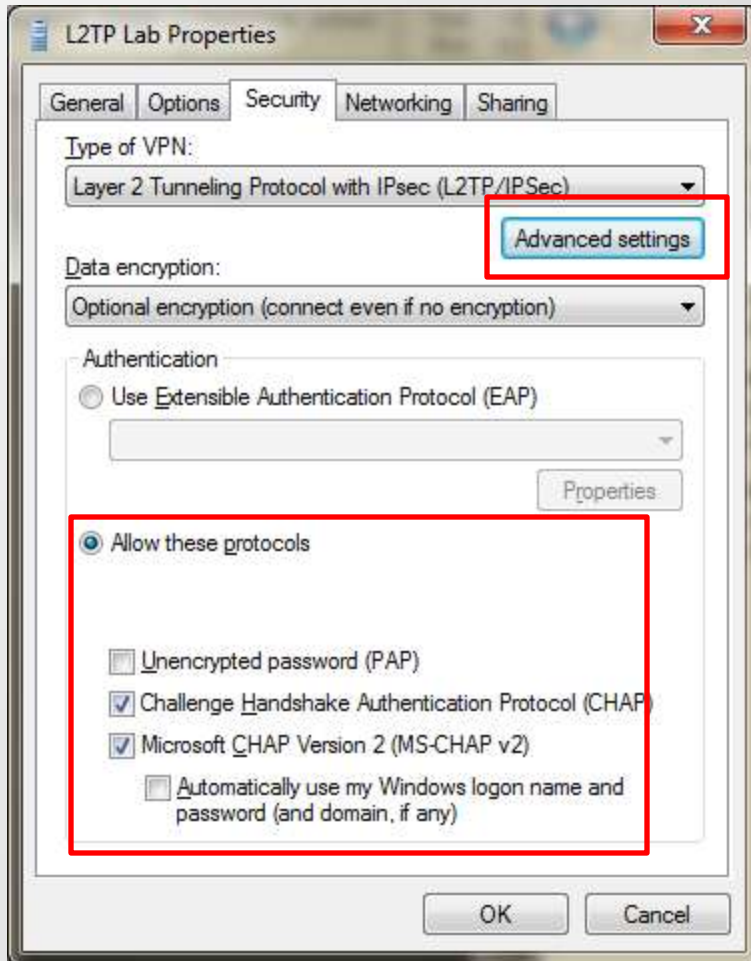
pap chap

mschap1 mschap2

enabled running slave Status: connected

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch

Windows L2TP Client



L2TP – Traffic Analyze

Torch (Running)

- Basic
 Interface: wlan1
 Entry Timeout: 00:00:03 s

- Collect
 Src. Address Src. Address6
 Dst. Address Dst. Address6
 MAC Protocol Port
 Protocol VLAN Id

- Filters
 Src. Address: 0.0.0.0/0
 Dst. Address: 0.0.0.0/0
 Src. Address6: ::/0
 Dst. Address6: ::/0
 MAC Protocol: all
 Protocol: any
 Port: any
 VLAN Id: any

Start
 Stop
 Close
 New Window

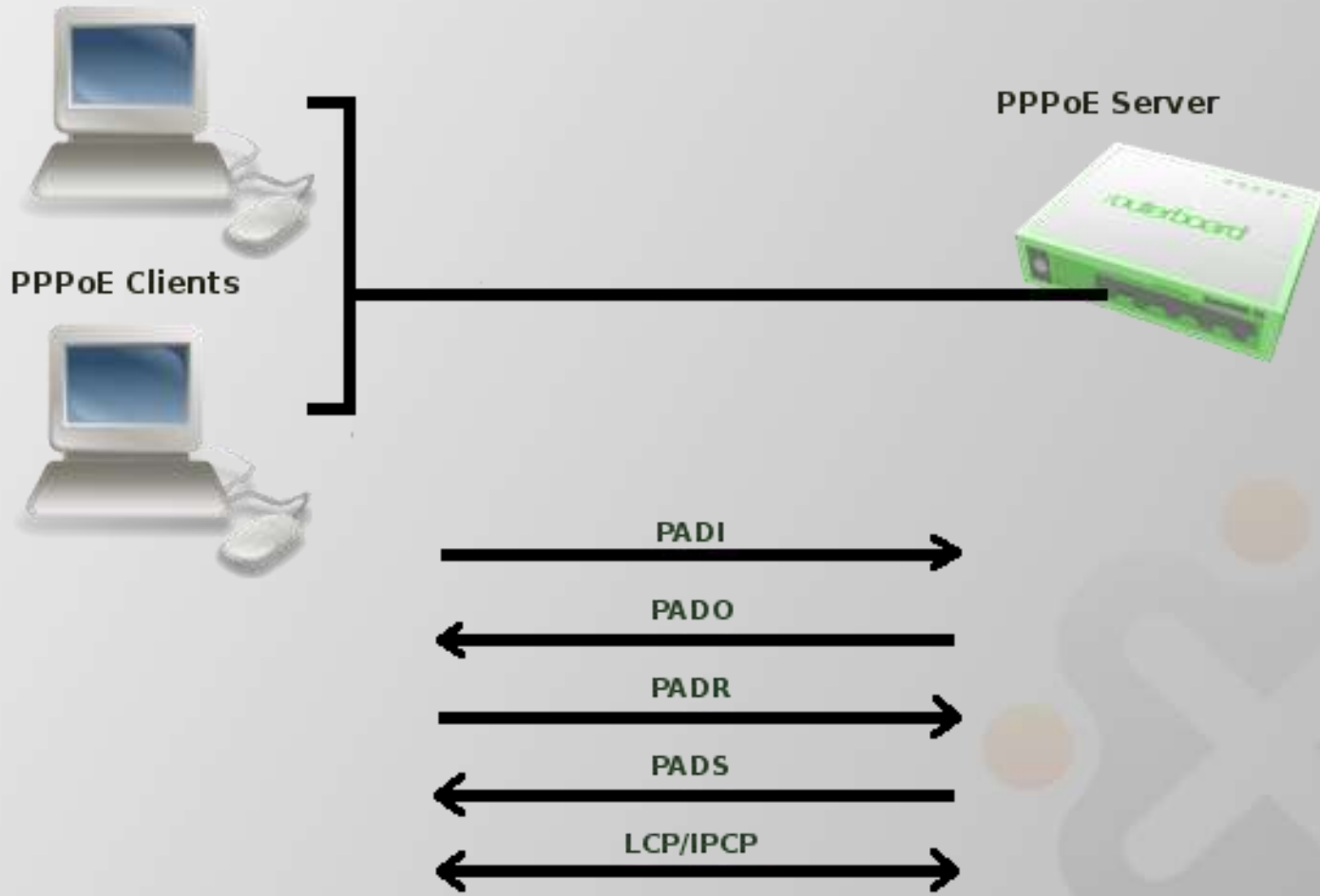
Et...	Protocol	Src.	Dst.	VLAN Id	Tx Rate	Rx Rate	Tx Pack...	Rx F
800 (ip)	6 (tcp)	192.168.10.6:50706	192.168.10.1:8291 (winbox)		5.3 kbps	2.5 kbps	2	
800 (ip)	17 (udp)	192.168.10.6:1701 (l2tp)	192.168.10.1:1701 (l2tp)		928 bps	944 bps	1	

- Setelah menggunakan L2TP tunnel, traffik pada wlan1 merupakan traffic L2TP
- Hanya menggunakan protocol UDP

PPPoE

- PPPoE adalah untuk enkapsulasi frame Point-to-Point Protocol (PPP) di dalam paket Ethernet,
- PPPoE biasanya dipakai untuk jasa layanan ADSL untuk menghubungkan modem ADSL (kabel modem) di dalam jaringan Ethernet (TCP/IP).
- PPPoE, adalah Point-to-Point, di mana harus ada satu point ke satu point lagi. Lalu, apabila point yang pertama adalah router ADSL kita, lalu di mana point satu nya lagi ?
- Tapi, bagaimana si modem ADSL bisa tahu point satunya lagi apabila kita (biasanya) hanya mendapatkan username dan password dari provider?
- Tahap awal dari PPPoE, adalah PADI (PPP Active Discovery Initiation), PADI mengirimkan paket broadcast ke jaringan untuk mencari di mana lokasi Access Concentrator di sisi ISP.

PPPoE



Tahapan Koneksi PPPoE

- PADI (PPP Active Discovery Initiation), Di sini PPOE client mengirimkan paket broadcast ke jaringan dengan alamat pengiriman mac address FF:FF:FF:FF:FF:FF. PPPoE client mencari di mana lokasi PPOE server dalam jaringan.
- PADO (PPPoE Active Discovery Offer). PADO ini merupakan jawaban dari PPOE server atas PADI yang didapatkan sebelumnya. PPPoE server memberikan identitas berupa MAC addressnya.
- PADR (PPP Active Discovery Request), merupakan konfirmasi dari PPOE client ke server. Disini PPOE client sudah dapat menghubungi PPOE server menggunakan mac addressnya, berbeda dengan paket PADI yang masih berupa broadcast.

Tahapan Koneksi PPPoE

- PADS (PPP Active Discovery Session-confirmation), dari PPOE server ke client. Session-confirmation di sini memang berarti ada session ID yang diberikan oleh server kepada client. Pada tahap ini juga terjadi negosiasi Username, password dan IP address.
- PADT (PPP Active Discovery Terminate), bisa dikirim dari server ataupun client, ketika salah satu ingin mengakhiri koneksinya

Tahapan Koneksi PPPoE

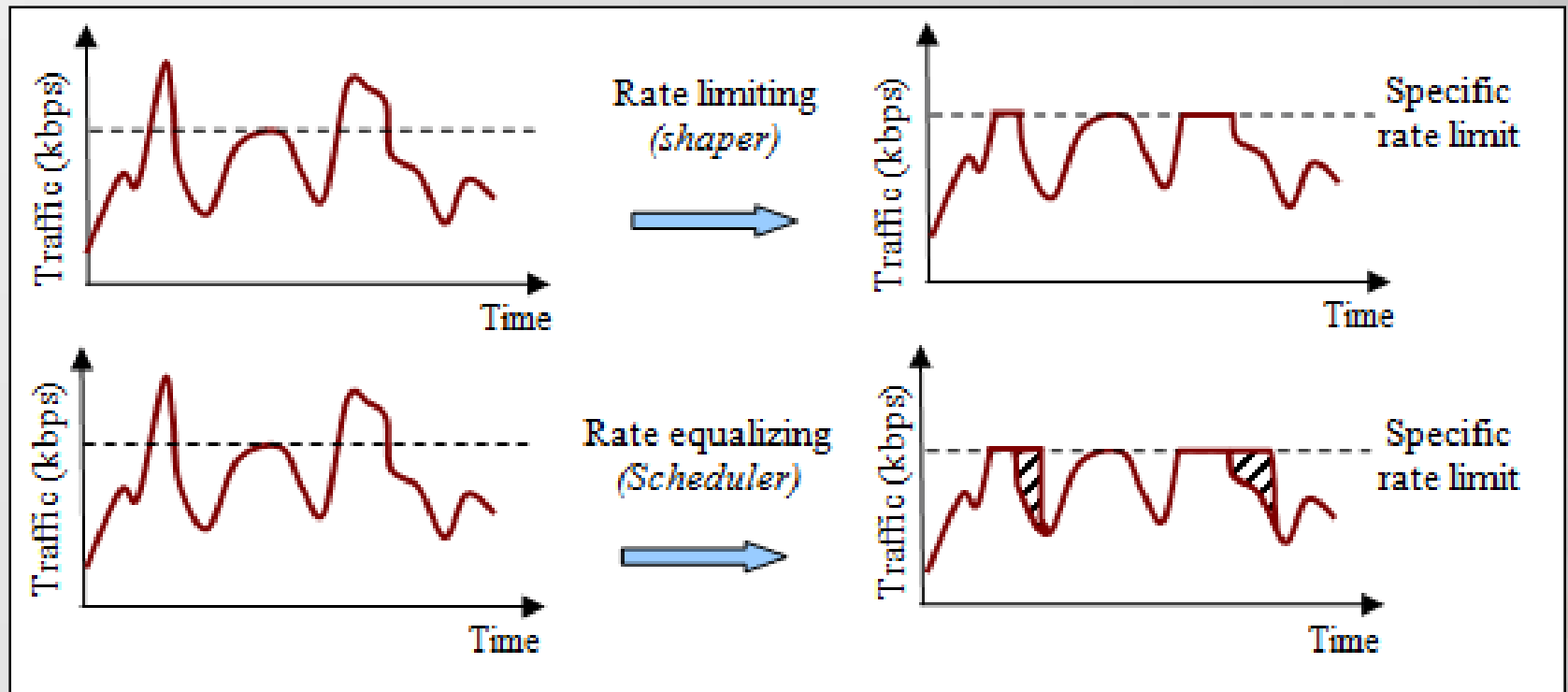
Log		
Time	Level	Message
May/29/2012 12:17:35	pppoe ppp info	speedy: dialing...
May/29/2012 12:17:35	pppoe debug pac...	ether1: sent PADI to FF:FF:FF:FF:FF:FF
May/29/2012 12:17:35	pppoe debug pac...	session-id=0x0000
May/29/2012 12:17:35	pppoe debug pac...	host-uniq=0x0
May/29/2012 12:17:35	pppoe debug pac...	service-name=
May/29/2012 12:17:35	pppoe debug pac...	ether1: rcvd PADO from 00:30:88:1A:23:A2
May/29/2012 12:17:35	pppoe debug pac...	session-id=0x0000
May/29/2012 12:17:35	pppoe debug pac...	host-uniq=0x0
May/29/2012 12:17:35	pppoe debug pac...	ac-name=BRAS-D4-GBL-D904L3610L0029
May/29/2012 12:17:35	pppoe debug pac...	service-name=
May/29/2012 12:17:35	pppoe debug pac...	ether1: sent PADR to 00:30:88:1A:23:A2
May/29/2012 12:17:35	pppoe debug pac...	session-id=0x0000
May/29/2012 12:17:35	pppoe debug pac...	host-uniq=0x1
May/29/2012 12:17:35	pppoe debug pac...	service-name=
May/29/2012 12:17:36	pppoe debug pac...	ether1: rcvd PADS from 00:30:88:1A:23:A2
May/29/2012 12:17:36	pppoe debug pac...	session-id=0x3a2c
May/29/2012 12:17:36	pppoe debug pac...	host-uniq=0x1
May/29/2012 12:17:36	pppoe debug pac...	service-name=
May/29/2012 12:17:36	pppoe debug pac...	ac-name=BRAS-D4-GBL-D904L3610L0029

QoS



QoS

- Bandwidth Limiter



Rate Limit

- Pada RouterOS, dikenal 2 jenis batasan rate 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**”.

Simple Queue

- Pada RouterOS, Bandwidth Limit dapat dilakukan dengan berbagai cara (wireless access list, ppp secret dan hotspot user)
- Simple queue mengatur pembatasan bandwidth dengan hanya mendefinisikan parameter IP address (target address) dari host/koneksi yang dilimit.
- Simple queue paling sederhana hanya melakukan pembatasan bandwidth max-limit (MIR)

LAB - Simple Queue

Batasi bandwidth Laptop anda 32k Upload, 64k Download

Simple Queue <queue1> □ ×

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

enabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Torch

LAB- Test Bandwidth

- Konek ke access point IDN Mantab
- Download file payload.bin via FTP ke IP 192.168.2.1
- User mtcna passwd 1



LAB-Cek Bandwidth Status

Simple Queue status

Queue List □ ✕

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

+ - ✓ ✗ 📁 🔍
00 Reset Counters 00 Reset All Counters

#	Name	Target Ad...	Rx Max Limit	Tx Max Limit	Packet ...
0	queue1	192.168.1.2	32k	64k	

Toot Torch status

Torch (Running) □ ✕

- Basic

Interface: ether1

Entry Timeout: 00:00:03 s

- Collect

Src. Address Src. Address6
 Dst. Address Dst. Address6
 MAC Protocol Port
 Protocol VLAN Id

- Filters

Src. Address: 192.168.1.2
 Dst. Address: 0.0.0.0/0
 Src. Address6: ::/0
 Dst. Address6: ::/0
 MAC Protocol: all
 Protocol: any
 Port: any
 VLAN Id: any

Et...	Prot...	Src.	Dst.	VLAN Id	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)		192.168.1.2	11.11.11.1		63.0 kbps	3.1 kbps	6	5
800 (ip)		192.168.1.2	192.168.1.1		1880 bps	613 bps	0	0
800 (ip)		192.168.1.2	8.8.4.4		0 bps	800 bps	0	1

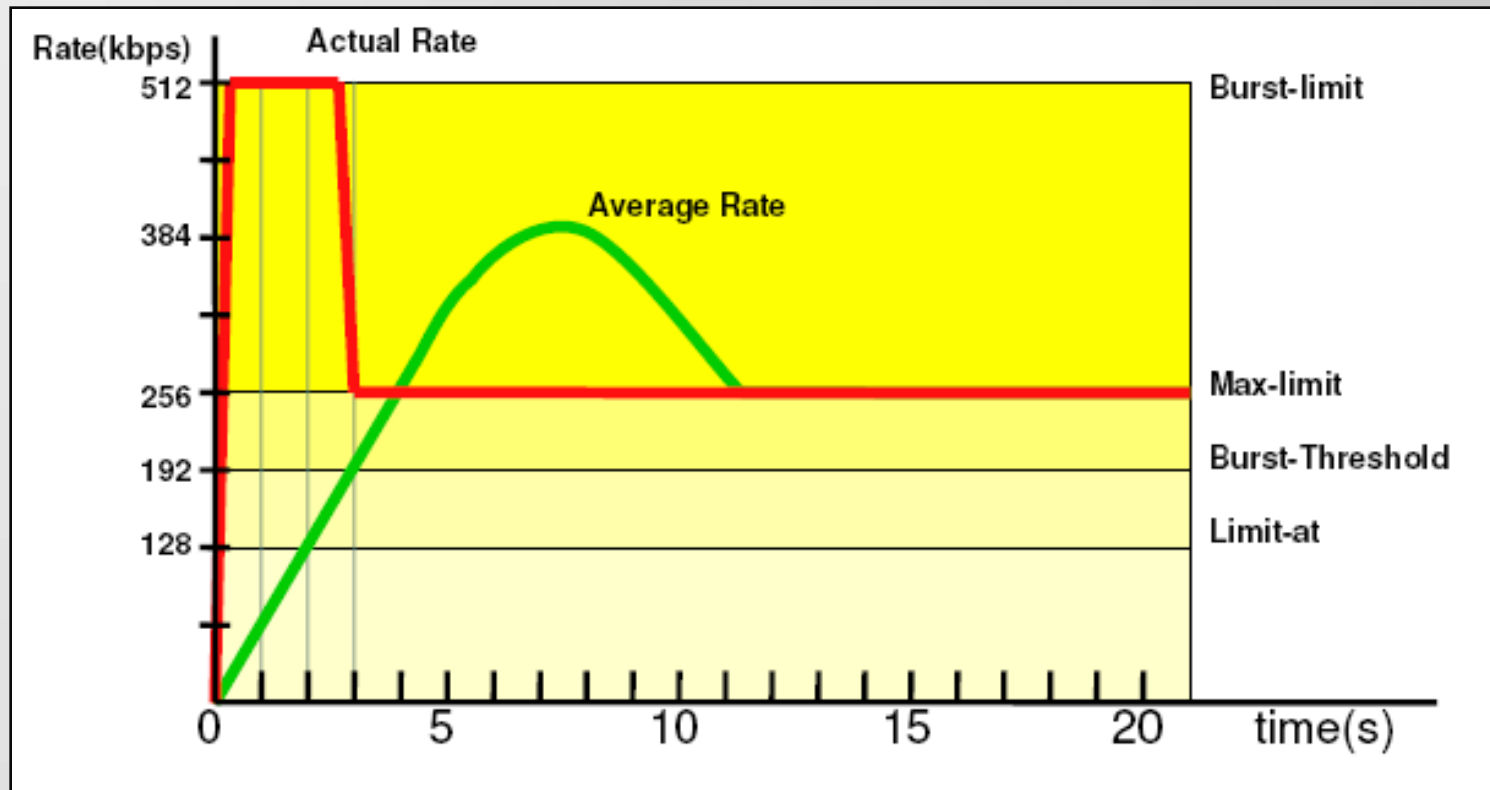
QoS Feature “Burst”

- Bursts adalah salah satu cara untuk meningkatkan performance koneksi HTTP
- Bursts digunakan untuk mengizinkan naiknya data rate dalam periode waktu yg singkat (bursts time)
- Jika Average data rate lebih kecil dari **burst-threshold**, burst dapat digunakan(actual data rate dapat mencapai **burst-limit**)
- Average data rate dihitung dari detik terakhir **burst-time**

Burst

Contoh

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



LAB – Burst Simple Queue

- Buat queue simple dengan contoh diatas
- Queue>Simple>add new

Simple Queue <queue1>

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

Name:

Target Address:

Target Upload Target Download

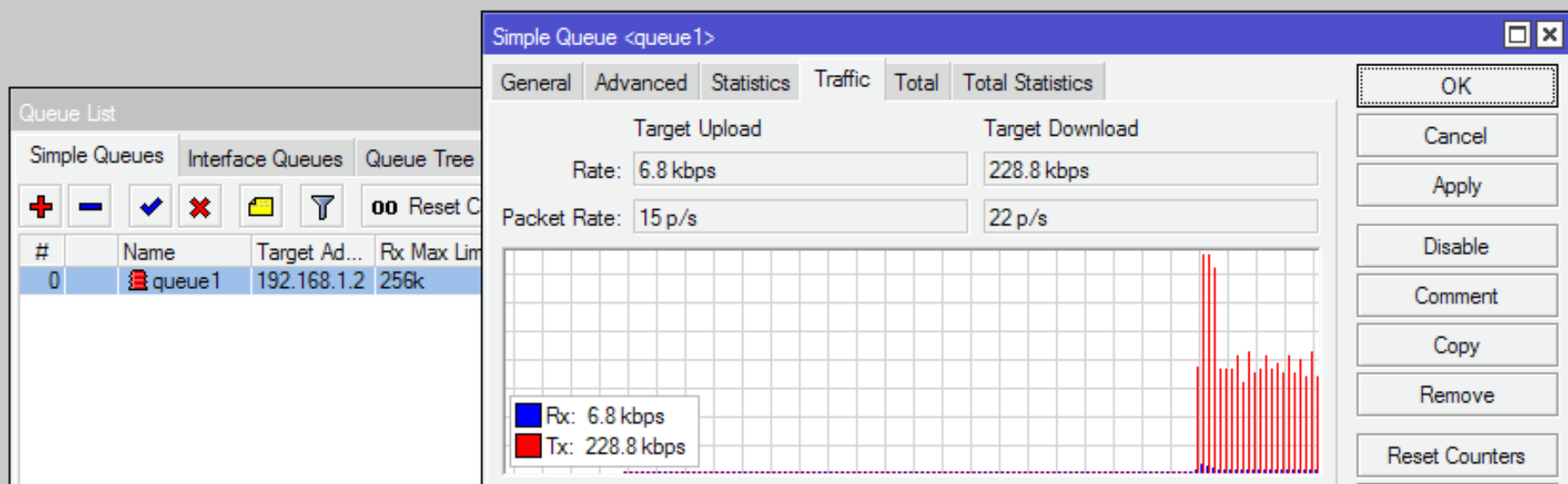
Max Limit:	<input type="text" value="256k"/>	<input type="text" value="256k"/>	<input type="text" value="bits/s"/>
Burst Limit:	<input type="text" value="512k"/>	<input type="text" value="512k"/>	<input type="text" value="bits/s"/>
Burst Threshold:	<input type="text" value="192k"/>	<input type="text" value="192k"/>	<input type="text" value="bits/s"/>
Burst Time:	<input type="text" value="8"/>	<input type="text" value="8"/>	<input type="text" value="s"/>

Time

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

LAB – Burst Simple Queue

- Queue>Queue Simple>Traffic



The screenshot shows the Mikrotik WinBox interface. On the left, the 'Queue List' window displays a table with the following data:

#	Name	Target Ad...	Rx Max Lim
0	queue1	192.168.1.2	256k

The main window shows the configuration for 'Simple Queue <queue1>'. The 'Traffic' tab is selected, showing the following settings:

- Target Upload Rate: 6.8 kbps
- Target Download Rate: 228.8 kbps
- Packet Rate: 15 p/s
- Packet Rate: 22 p/s

A traffic graph at the bottom shows a burst of red bars (Tx) reaching 228.8 kbps, while blue bars (Rx) remain at 6.8 kbps. A legend indicates: Rx: 6.8 kbps (blue), Tx: 228.8 kbps (red).

- Sambil download file payload.bin dari ftp 11.11.11.1



```

Command Prompt - ftp 11.11.11.1
C:\Documents and Settings\Admin>ftp 11.11.11.1
Connected to 11.11.11.1.
220 MikroTik FTP server (MikroTik 5.14) ready
User (11.11.11.1:(none)): admin
331 Password required for admin
Password:
230 User admin logged in
ftp> get payload.bin
  
```

LAB – Burst Simple Queue

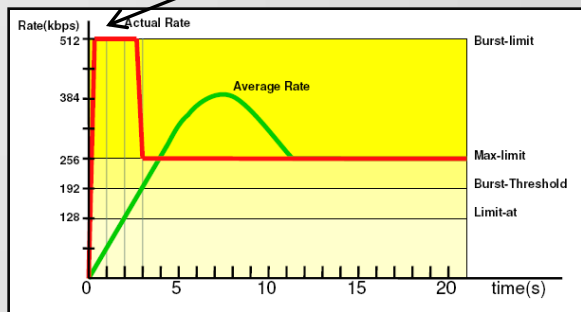
Simple Queue <queue1>

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

Target Upload: Rate: 6.8 kbps | Packet Rate: 15 p/s

Target Download: Rate: 228.8 kbps | Packet Rate: 22 p/s

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters



Queue Kind

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)

Queue Kind

Queue>Queue Type>Add New Queue Types

Queue List
□ ×

Simple Queues | Interface Queues | Queue Tree | Queue Types

+ - ⌵

	Type Name	Kind	
+	default	pfifo	
+	default-small	pfifo	
+	ethernet-default	pfifo	
+	hotspot-default	sfq	
+	multi-queue-ethernet-default	mq pfifo	
+	only-hardware-queue	none	
+	synchronous-default	red	
+	wireless-default	sfq	

New Queue Type
□ ×

Type Name:

Kind: ⌵

Queue Size:

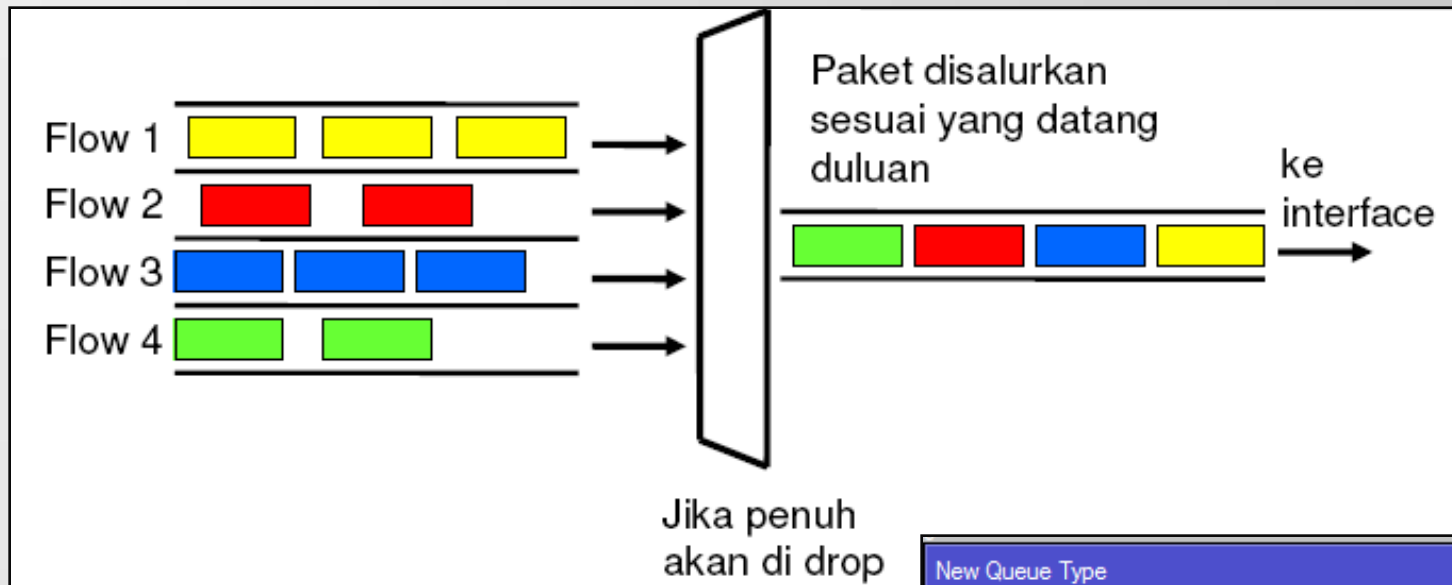
none
 pcq
 pfifo
 red
sfq

FIFO

- 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
- MQ-FIFO – adalah sebuah mekanisme fifo yang dikhususkan pada system hardware yang sudah SMP (multi core processor) dan harus pada interface yang support multiple transmit queues.

FIFO

- First In First Out



New Queue Type

Type Name:

Kind:

Queue Size: packets

OK

Cancel

Apply

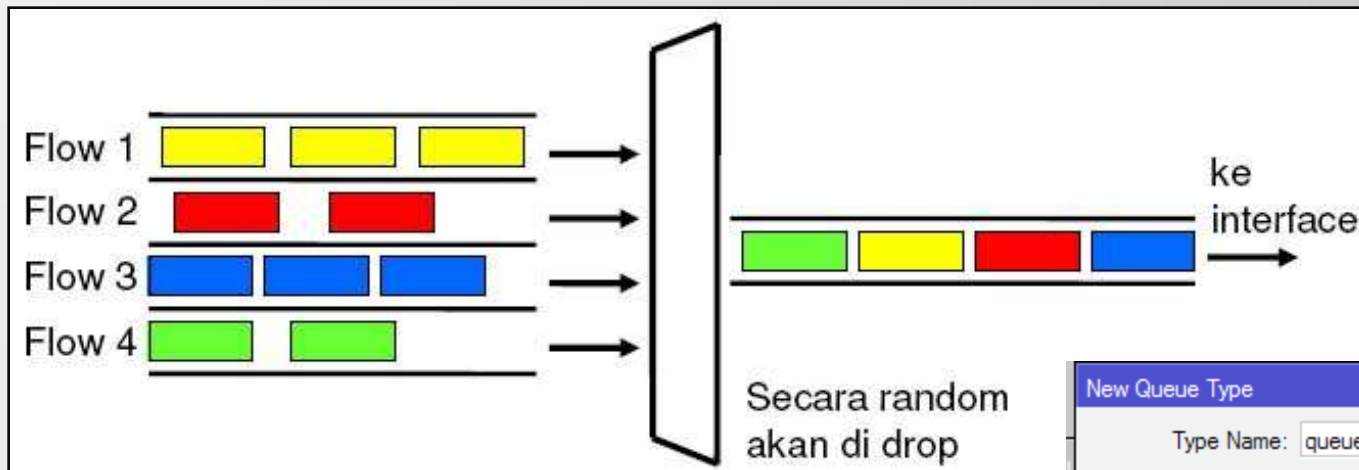
Copy

Remove

RED

- RED melimit packet dengan melihat rata-rata ukuran queue.
- Rata-rata ukuran queue dibandingkan dengan 2 parameter, min-treshold dan max-treshold
- Saat rata-rata ukuran queue sama dengan min-threshold, RED setidaknya ada paket yang di drop.
- Saat ukuran queue rata-rata lebih dari max-threshold, maka seluruh paket yang datang akan di drop
- Jika rata-rata ukuran queue diantara min dan max treshold, paket akan didrop berdasarkan probabilitas.
- RED digunakan jika kita memiliki trafik yang congested.
- Sangat sesuai untuk trafik TCP, tetapi kurang baik digunakan untuk trafik UDP.

RED (Random Early Detect)



New Queue Type

Type Name:

Kind:

Queue Size: packets

Min Threshold: packets

Max Threshold: packets

Burst: packets

Avg. Packet Size: bytes

OK

Cancel

Apply

Copy

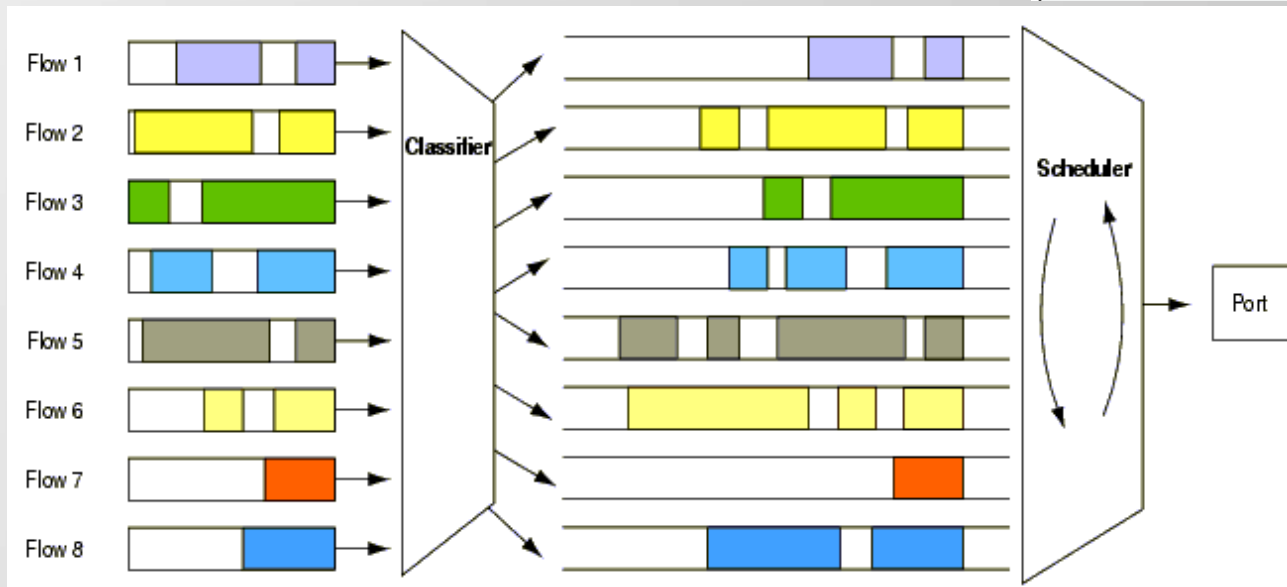
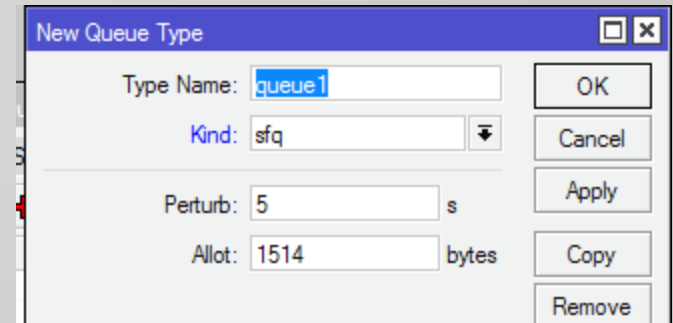
Remove

SFQ (Stochastic Fairness Queuing)

- SFQ sebenarnya tidak menyediakan queue (antrian).
- SFQ hanya menggunakan algoritma hasing dengan melihat 4 parameter (src & dst ip address dan src & dst port) untuk mengklasifikasikan packet menjadi 1024 sub queue.
- Kemudian Algoritma round robin akan melakukan queue ulang /mendistribusikan traffic dari masing-masing substream yang ada.

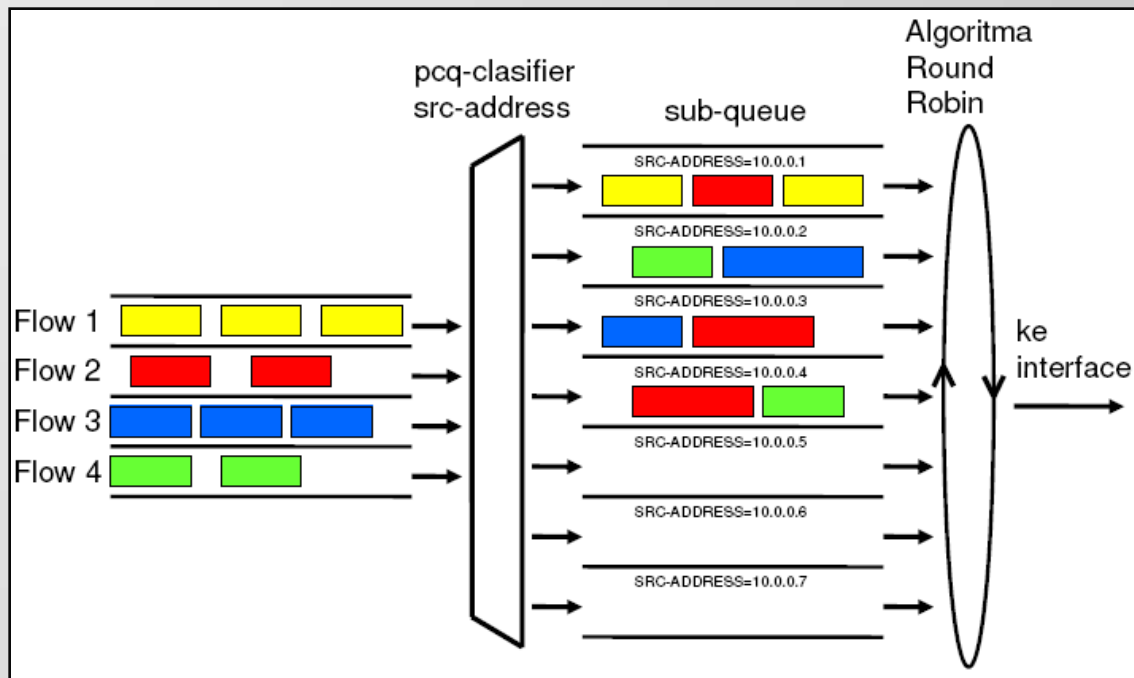
SFQ

- Setelah Perturb detik algoritma hasing akan berganti dan membagi session trafik ke sub-queue lainnya dengan Allot besar packet



PCQ (Per Connection Queue)

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



PCQ

New Queue Type [] [X]

Type Name:

Kind:

Rate:

Limit:

Total Limit:

Burst Rate: ▼

Burst Threshold: ▼

Burst Time:

- Classifier

Src. Address Dst. Address

Src. Port Dst. Port

Src. Address Mask:

Dst. Address Mask:

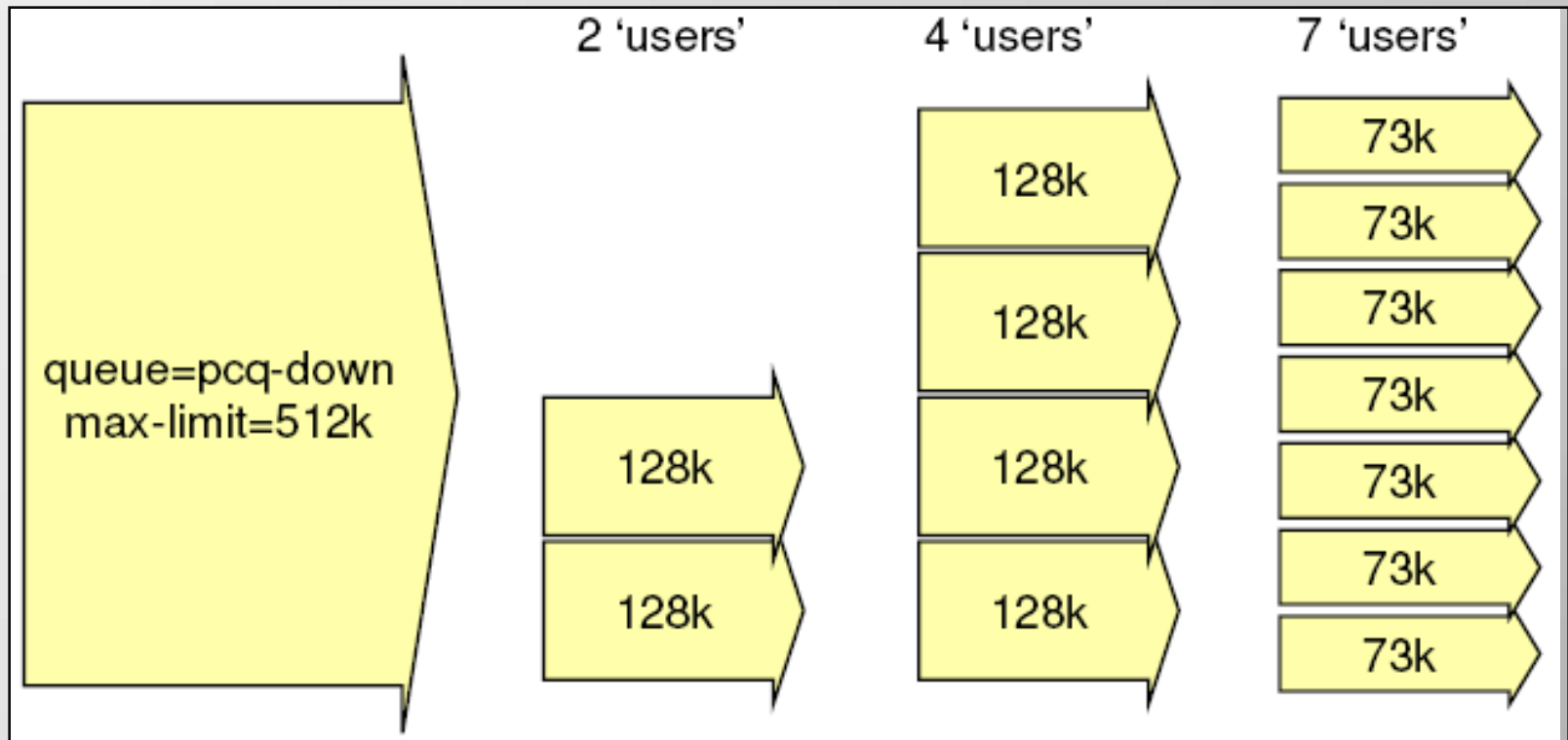
Src. Address6 Mask:

Dst. Address6 Mask:

- PCQ akan membuat sub-queue, berdasarkan parameter pcq-classifier (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-sub-queue tidak bisa melebihi jumlah paket sesuai pcq-total-limit

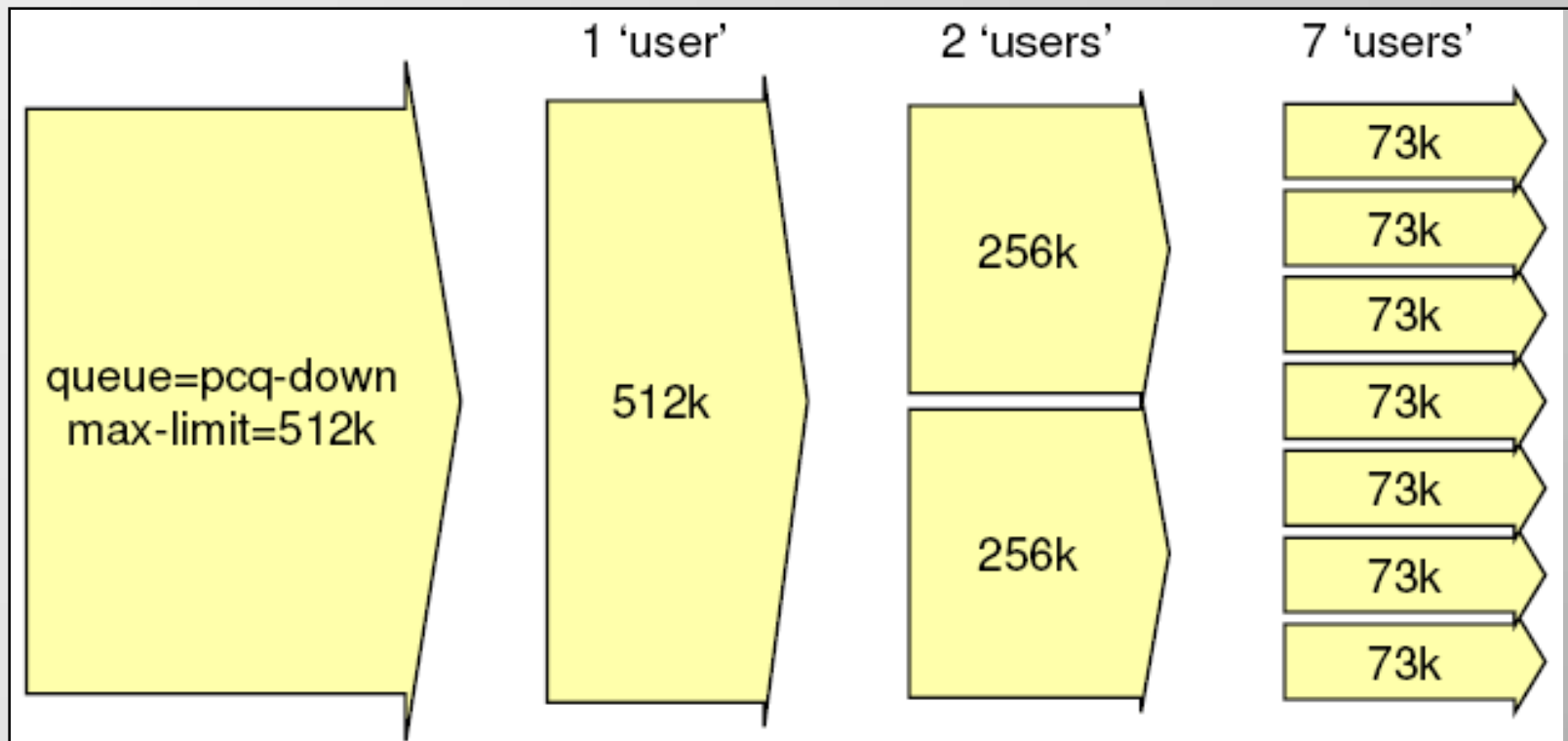
Contoh Penggunaan PCQ

- PCQ Rate = 128k



Contoh Penggunaan PCQ

- PCQ Rate = 0

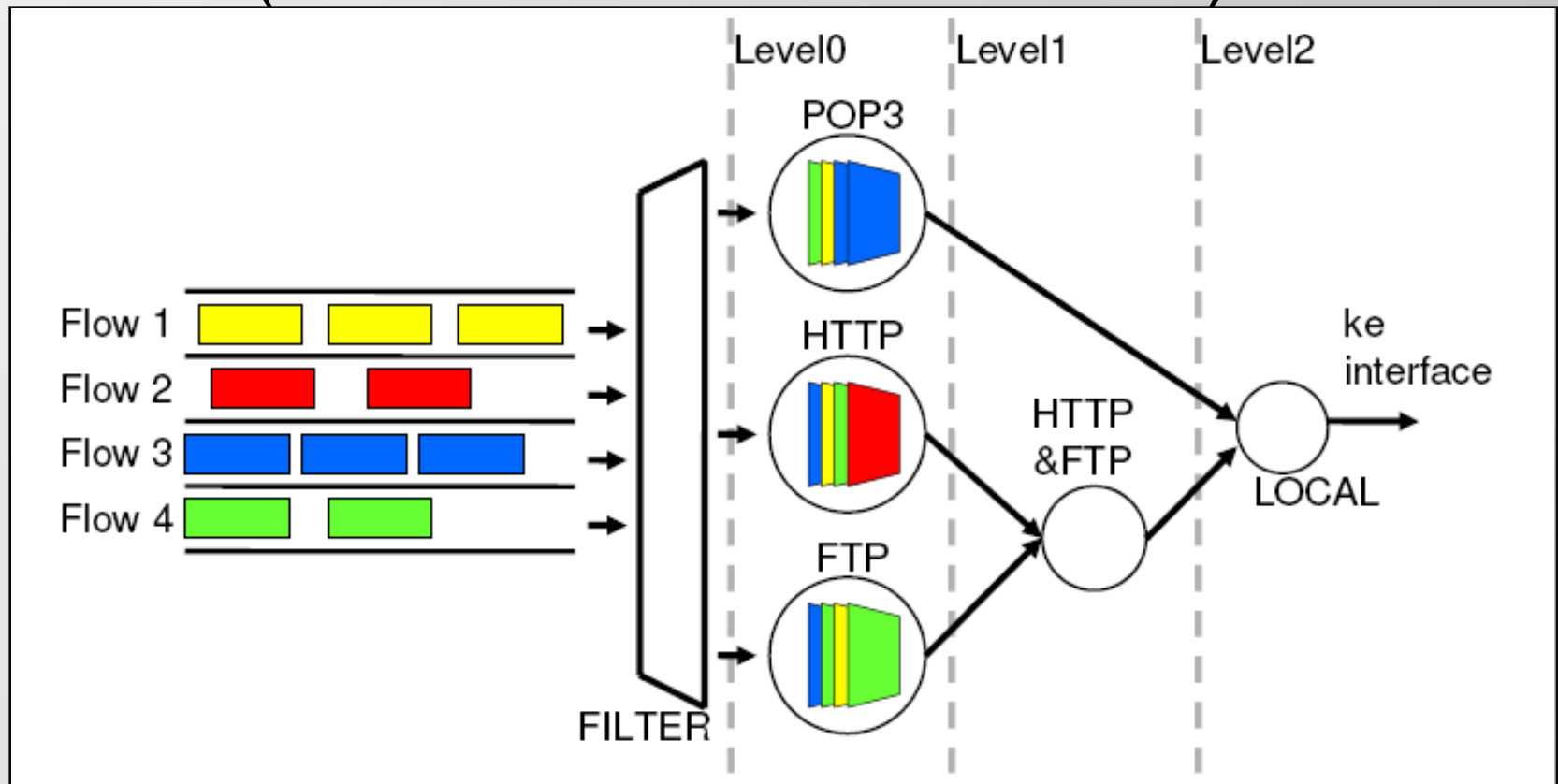


HTB

- 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, dengan HTB kita dapat mengaplikasikan properti yang berbeda-beda.
- HTB dapat melakukan prioritas untuk grup yang berbeda.

HTB

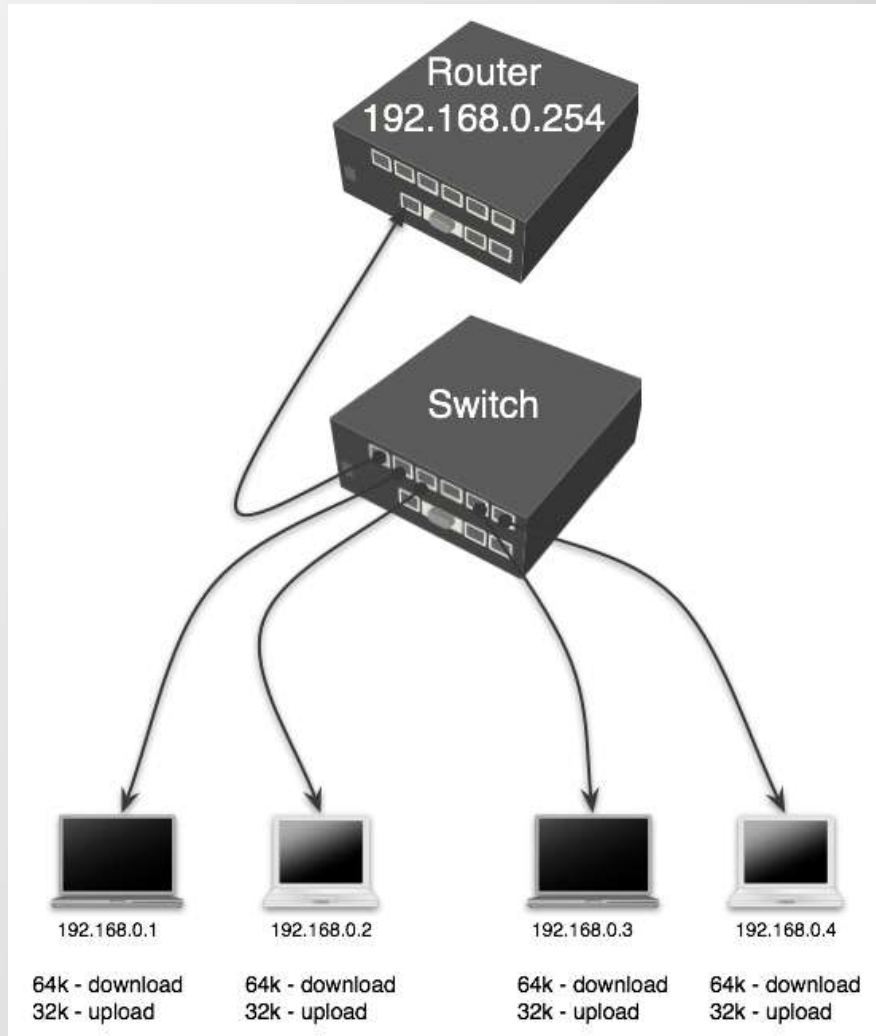
- HTB (Hierarchical Token Bucket)



Struktur HTB

- Setiap queue bisa menjadi parent untuk queue lainnya
- Semua child queue (tidak peduli berapa banyak level parentnya) akan berada pada level HTB yang sama (paling bawah)
- Semua Child queue akan mendapatkan trafik sekurang-kurangnya sebesar limit-at.

LAB- PCQ



LAB - PCQ

- Buat Mark Packet upload & download

```
/ip firewall mangle add chain=prerouting action=mark-packet in-interface=etherLAN new-packet-mark=client_upload
```

```
/ip firewall mangle add chain=prerouting action=mark-packet in-interface=etherWAN new-packet-mark=client_download
```

- Buat 2 PCQ queue types – satu untuk download dan satu untuk upload. dst-address untuk trafik download user, src-address untuk trafik upload

```
/queue type add name="PCQ_download" kind=pcq pcq-rate=64000 pcq-classifier=dst-address
```

```
/queue type add name="PCQ_upload" kind=pcq pcq-rate=32000 pcq-classifier=src-address
```

- Buat 1 rule simple queue

```
/queue simple add target-addresses=192.168.0.0/24
```

```
queue=PCQ_upload/PCQ_download \ packet-marks=client_download,client_upload
```

Posisi Queue

Queue pada RouterOS dilakukan pada parent interface:

- Interface fisik (ether1, ether2, wlan1...)
- Interface virtual:
 - Global In
 - Global Out
 - Global Total
- Simple-Queue tidak bisa melakukan queue pada parent interface sehingga secara otomatis menggunakan Virtual Interface.

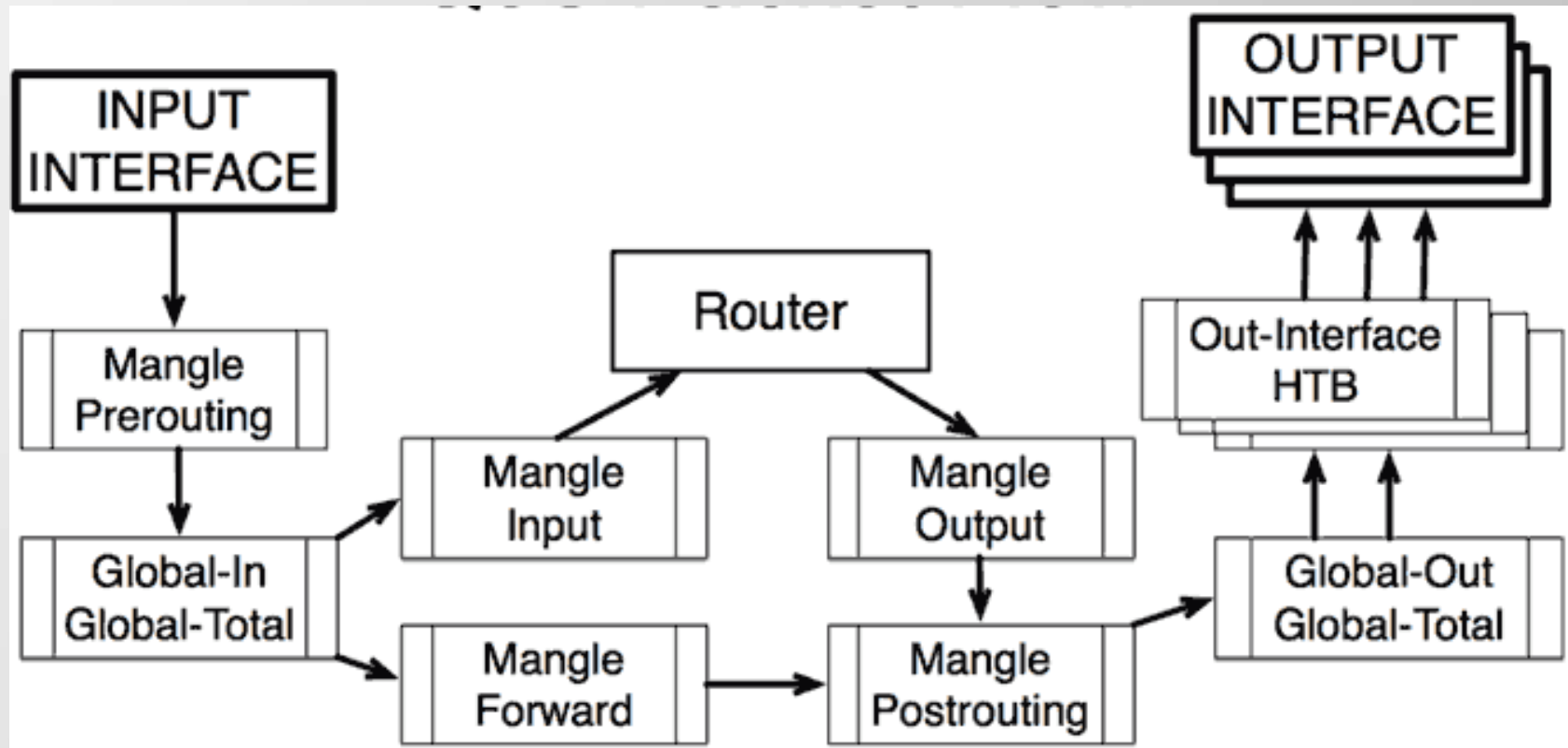
Posisi Queue

- **global-in:** mewakili semua interface input (ingress queue). Queue yang melekat ke global-in , berlaku untuk lalu lintas yang diterima oleh router sebelum paket filtering
- **global-out:** mewakili semua interface output pada umumnya (egress queue), traffic setelah filtering.
- **global-total:** mewakili semua input dan output interface bersama-sama (dengan kata lain itu adalah agregasi global-in dan global-out). Digunakan dalam kasus ketika pelanggan memiliki batlimit untuk total upload dan download.
- **<interface name>:** merupakan salah satu outgoing interface tertentu. Hanya lalu lintas yang ditujukan untuk pergi keluar melalui interface ini yang akan melewati HTB queue

Mangle Structure

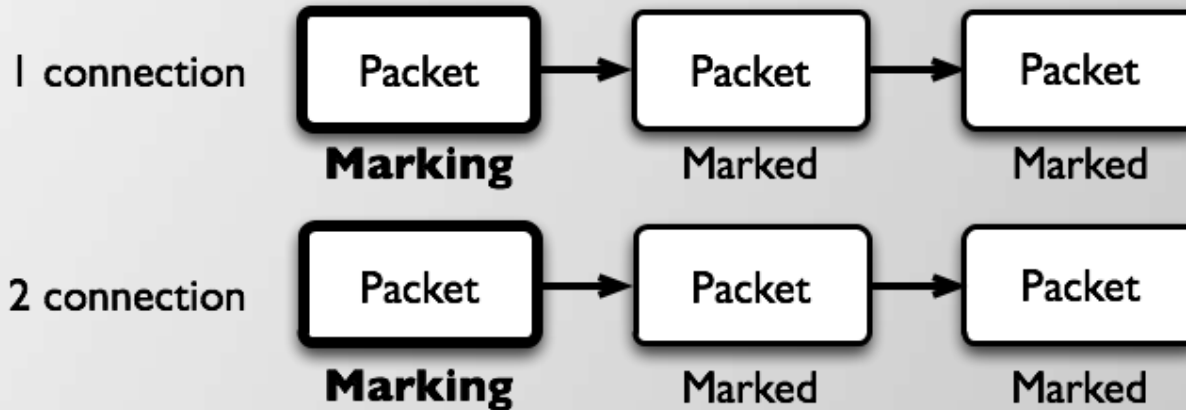
- Mangle diatur dan diorganisasikan chains
- Ada 5 built in chain mangle dalam mikrotik:
 - ◆ Prerouting- making a mark before Global-In queue
 - ◆ Postrouting - making a mark before Global-Out queue
 - ◆ Input - making a mark before Input filter
 - ◆ Output - making a mark before Output filter
 - ◆ Forward - making a mark before Forward filter
- Jika dibutuhkan user dapat membuat chain baru dengan nama tertentu

QoS Packet Flow

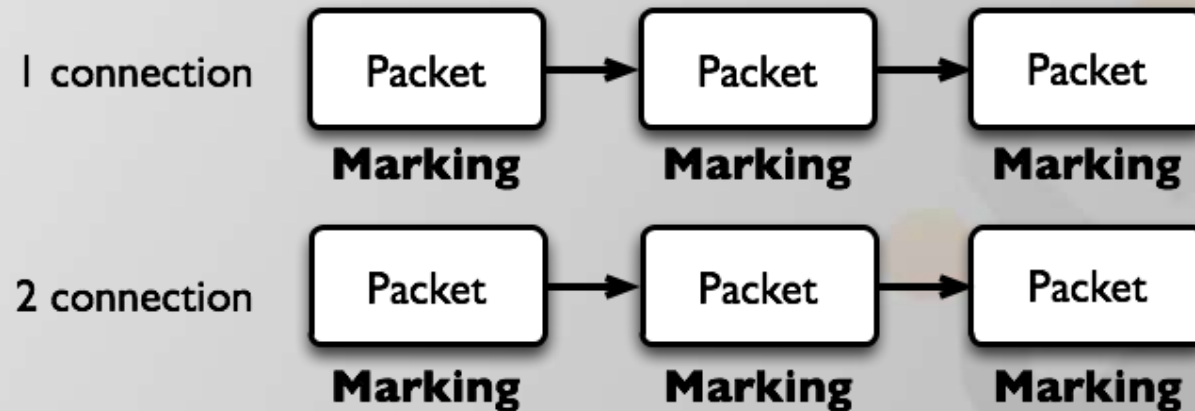


Mangle

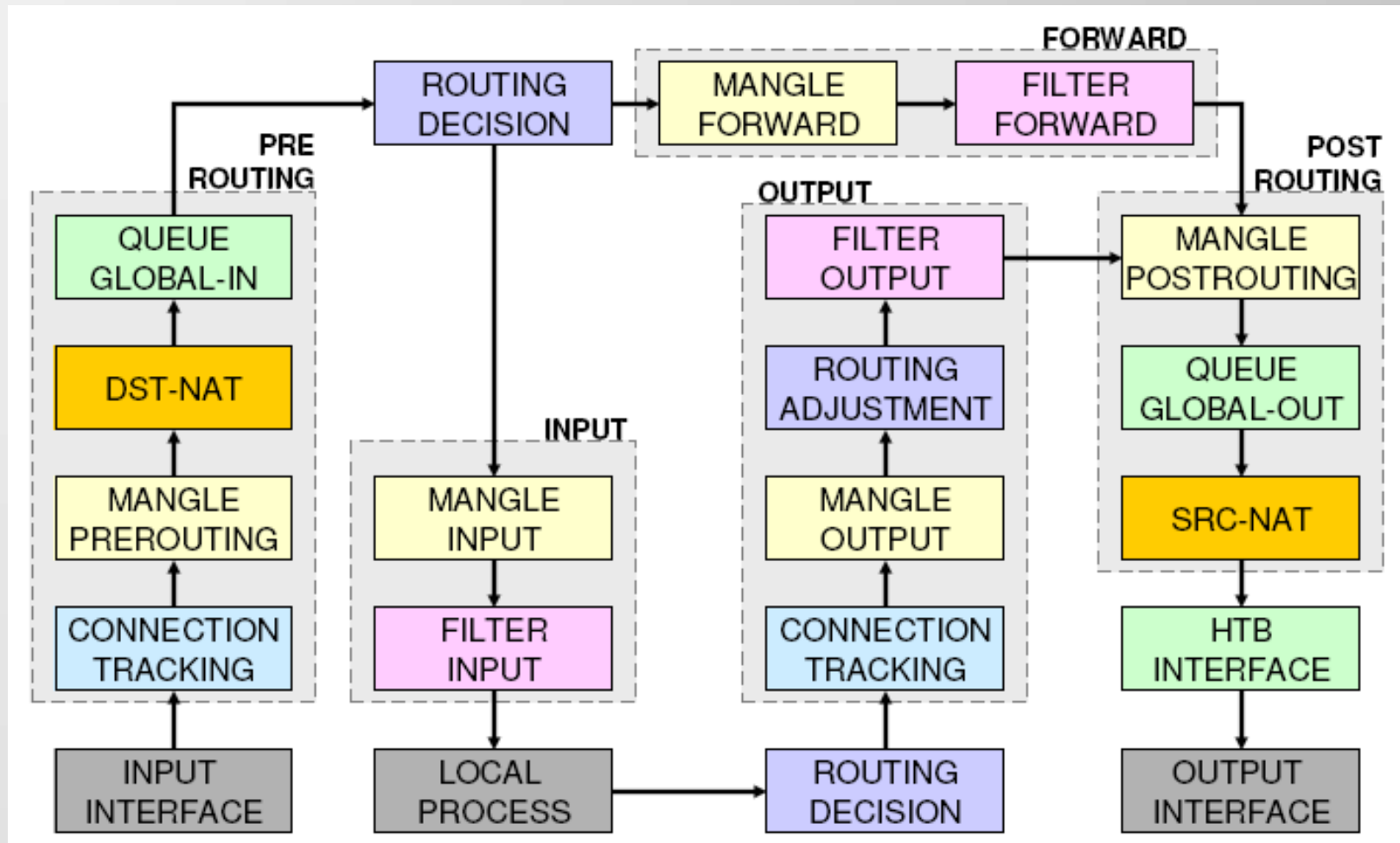
Mark-Connection



Mark-Packet



Packet Flow



Penggunaan Mangle untuk Queue

upstream :

PC --> in-interface(lan) --> prerouting(marking packet upstream) --> global-in(limitasi upstream) --> routing-decision --> forward --> postrouting --> global-out(walaupun disini ada global-out, gk perlu ada limitasi disini, karena dah di limit di global-in) --> out-interface(wan) --> Destination-Server

downstream :

Destination-Server --> in-interface=(wan) --> prerouting --> global-in --> routing-decision --> forward --> postrouting(mangle packet downstream disini, agar bisa di limit di global-out) --> global-out (limitasi downstream terjadi disini) --> out-interface(lan) --> PC

Network Management



Koneksi Host to Host



Ping dari PC 1 ke PC2, proses yang terjadi adalah sebagai berikut:

1. PC1 memeriksa tabel ARP cache internal
2. Bila tidak ada dia bertanya / broadcast ke network, siapa IP 182.168.43.2 dan berapa MAC addressnya.
3. PC2 mereplay "Saya pemilik IP 182.168.43.2, MAC address saya 00:6A:23:45:34:3D.
4. PC1 menerima informasi dari PC2 dan menambahkan entry pada tabel ARP cachanya.

ARP

- Meskipun pengalamatan paket data menggunakan alamat IP, alamat hardware/hardware address harus digunakan untuk transport data host to host pada connected network.
- ARP digunakan untuk mapping layer OSI level 3 (IP) ke layer OS level 2 (MAC Address).
- Router memiliki tabel entri ARP saat ini digunakan, biasanya tabel ARP dibuat secara dinamis oleh router, tetapi untuk meningkatkan keamanan jaringan, dapat juga dibuat secara statis baik sebagian atau semuanya dengan menambahkan secara manual pada entri ARP tabel.

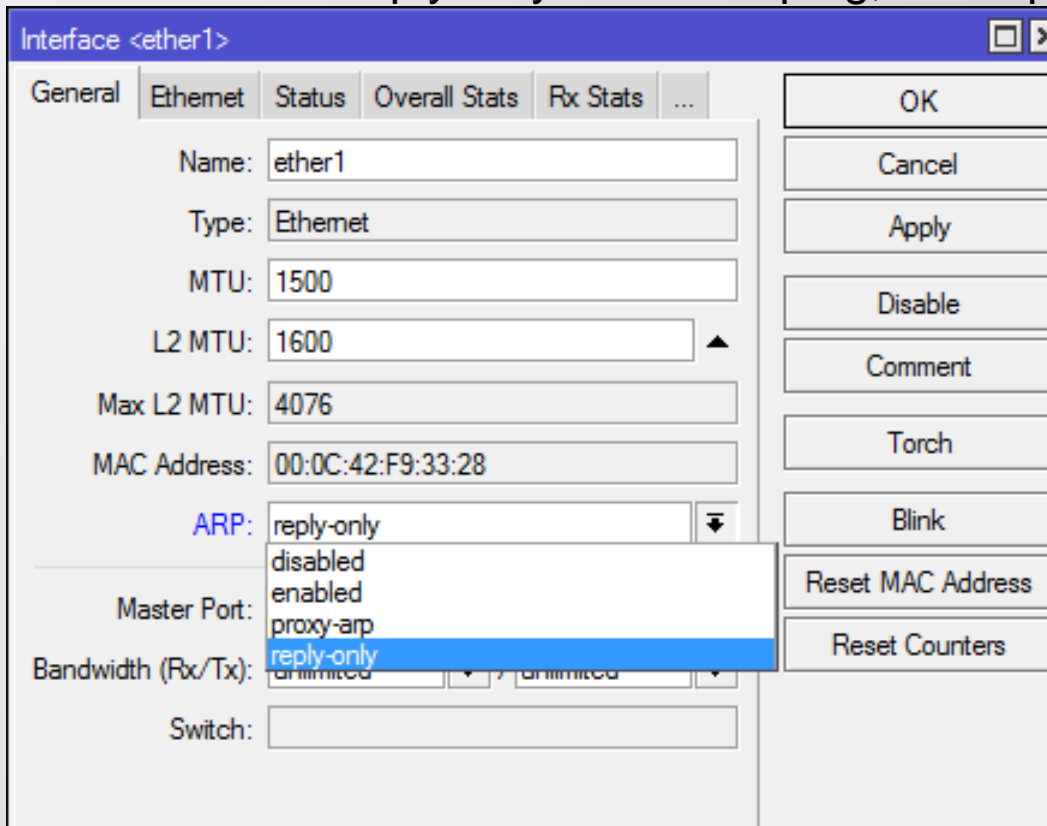
Interface ARP Mode

- Enable → Mode ini default enable pada semua interface di MikroTik. Semua ARP akan ditemukan dan secara dinamik ditambahkan dalam ARP tabel.
- Proxy ARP → Router dengan mode ARP proxy akan bertindak sebagai transparan proxy ARP antara dia atau lebih jaringan yang terhubung langsung.
- Reply Only → ARP reply-only memungkinkan router hanya kan mereply ARP statis ditemukan di tabel ARP, akses ke router dan ke jaringan di belakang router hanya dapat diakses oleh kombinasi Ip dan mac address yang ditemukan di tabel ARP.
- Disable → permintaan ARP dari klien tidak dijawab oleh router. Oleh karena itu, statis arp entri harus ditambahkan disamping disisi router juga disisi client. misal pada Windows menggunakan perintah arp:
C: \> arp-s 192.168.2.1 00-aa-00-62-c6-09

LAB- ARP Mode

ARP Reply-Only

- Koneksikan Laptop dengan salah satu interface.
- Set interface reply-only dan coba ping, dari laptop ke router.



Interface <ether1>

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

Name: ether1

Type: Ethernet

MTU: 1500

L2 MTU: 1600 ▲

Max L2 MTU: 4076

MAC Address: 00:0C:42:F9:33:28

ARP: reply-only

Master Port:

Bandwidth (Rx/Tx): unlimited / unlimited

Switch:

OK

Cancel

Apply

Disable

Comment

Torch

Blink

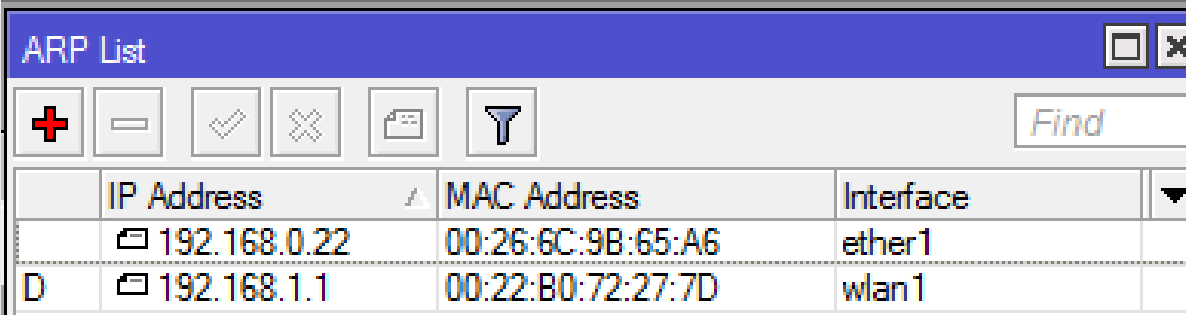
Reset MAC Address

Reset Counters

LAB- ARP Mode

ARP Reply-Only

- Tambahkan kombinasi IP dan ARP dari laptop pada menu IP>ARP

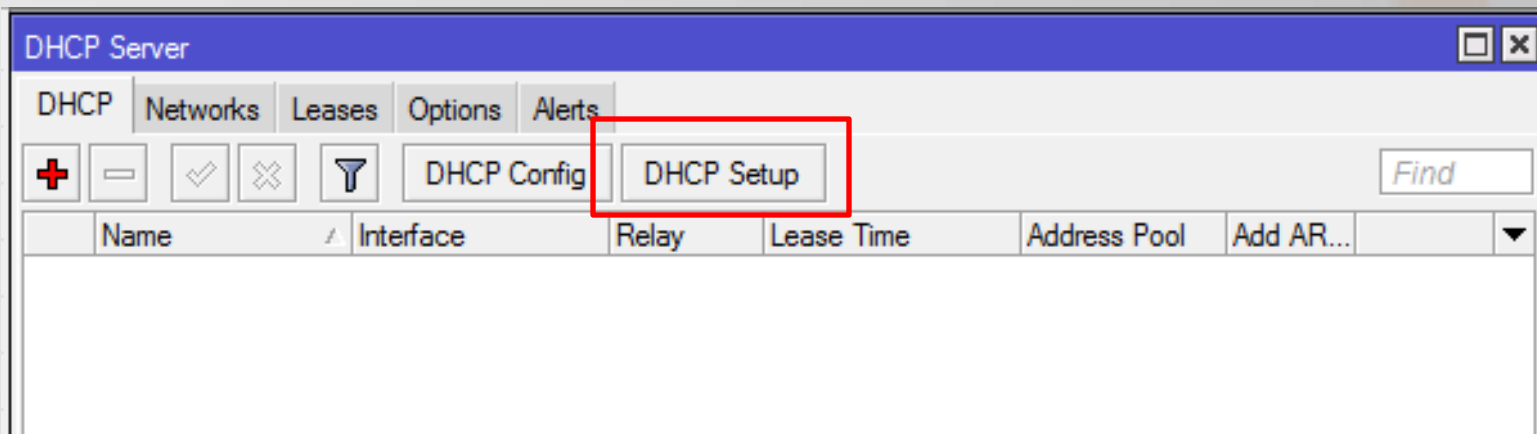


	IP Address	MAC Address	Interface
	192.168.0.22	00:26:6C:9B:65:A6	ether1
D	192.168.1.1	00:22:B0:72:27:7D	wlan1

- Coba ping kembali ip router dari laptop.
- Gunakan laptop peserta lain, isikan IP yang sama dengan IP laptop anda sebelumnya.
- Coba ping kembali

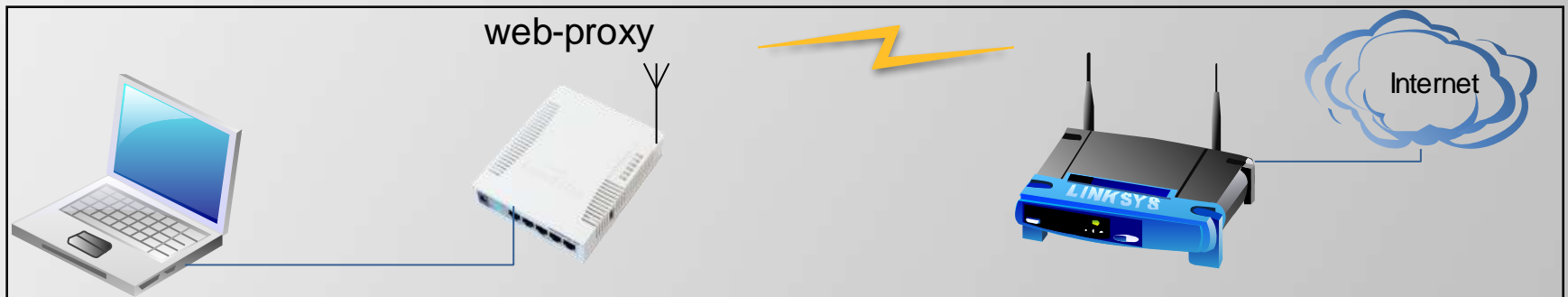
LAB - DHCP Server

- DHCP server dapat dijalankan pada masing-masing interface di router.
- Untuk memudahkan seting DHCP server, sebelumnya add IP address untuk interface yang akan menjalankan DHCP server.
- Setting DHCP server pada menu IP>DHCP Server>DHCP Setup



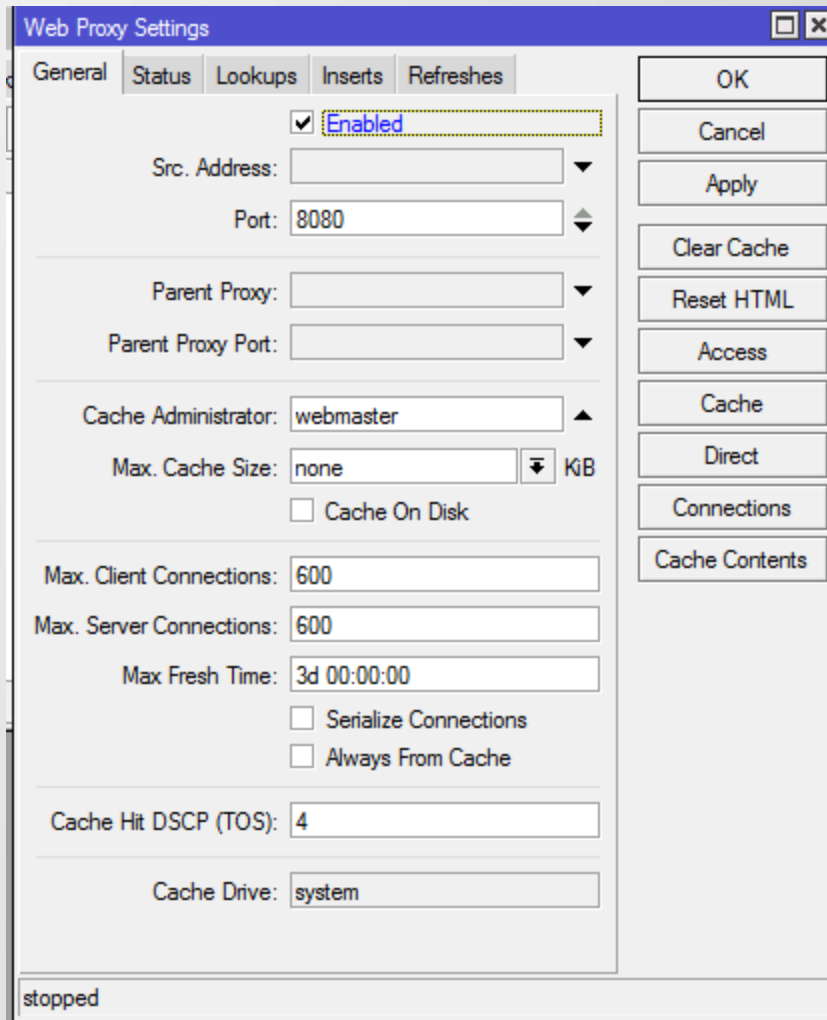
Lab – Web Proxy

- Topologi

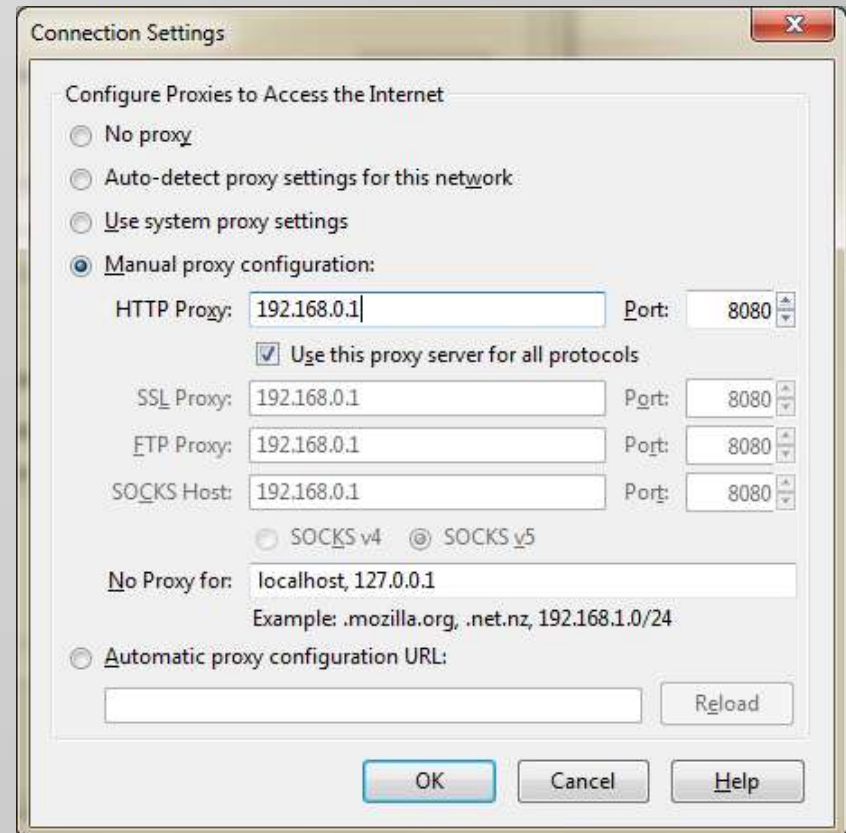


Lab – Web Proxy

- Enable Web Proxy pada menu IP>Web Proxy



Set manual proxy pada browser client, arahkan ke IP router



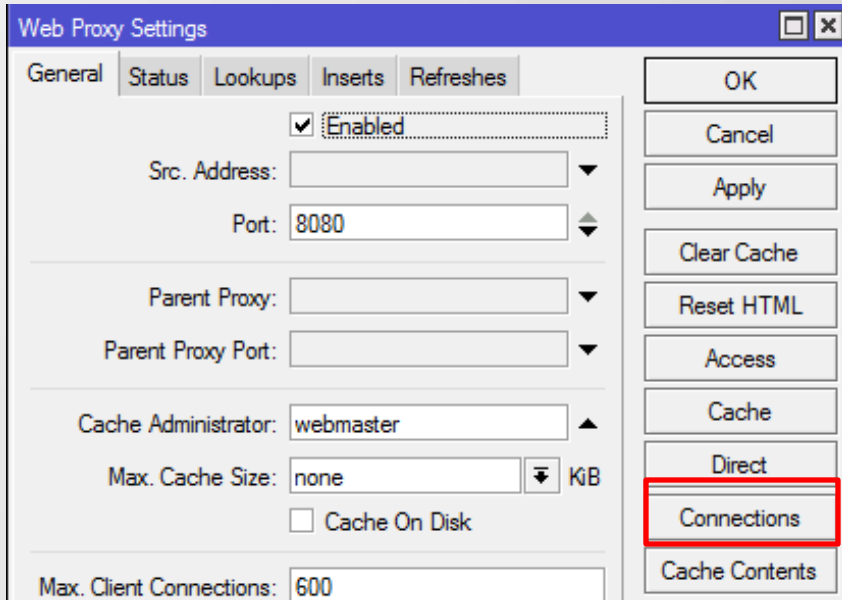
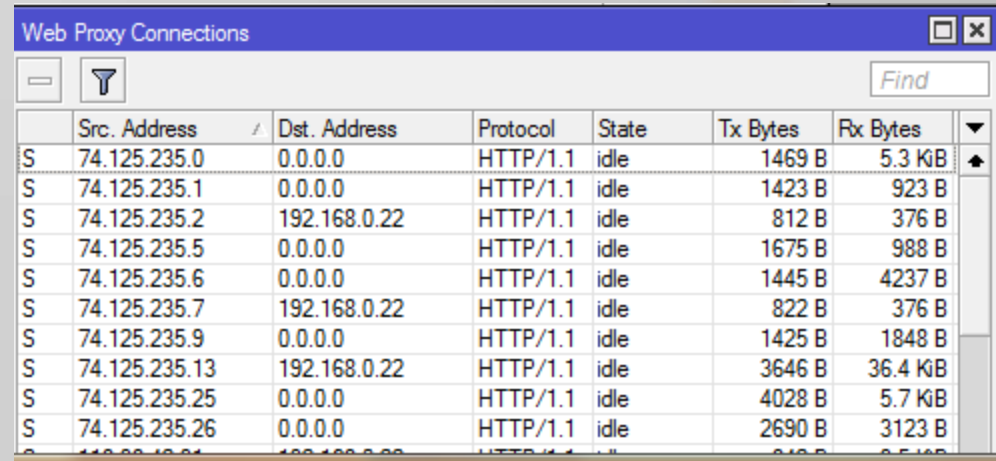
Lab – Web Proxy

- Cek konfigurasi proxy dengan akses web proxy detect, misal www.indonesiacyber.net

```

Anda terhubung lewat IP:
125.161.141.170
Host 192.168.0.22
Proxy: 1.1 192.168.0.1
(Mikrotik HttpProxy)
  
```

- Cek pada IP>Web Proxy> Connections

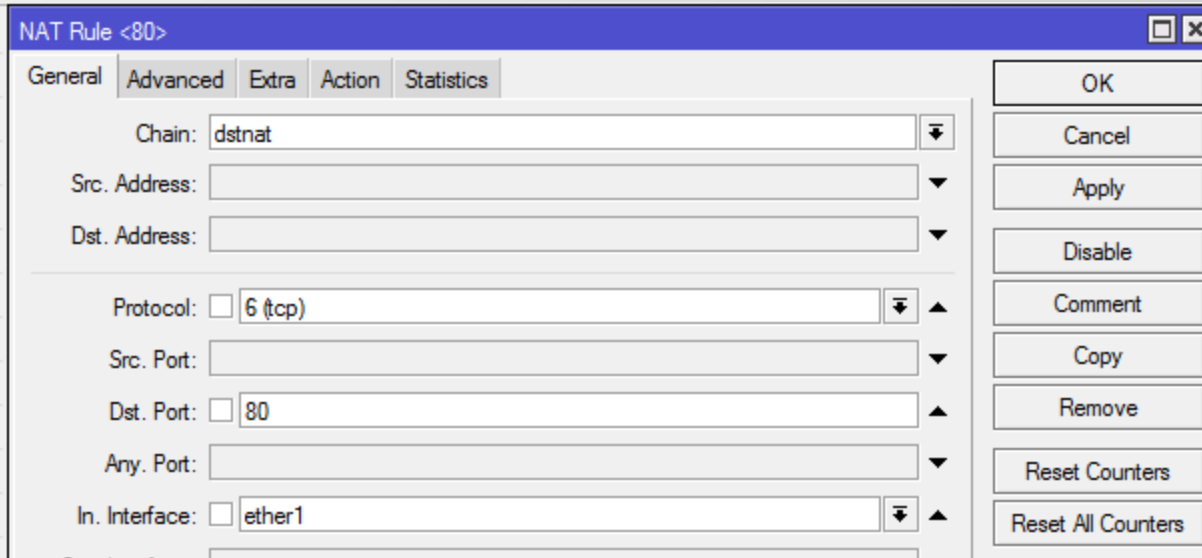



Web Proxy Connections

	Src. Address	Dst. Address	Protocol	State	Tx Bytes	Rx Bytes
S	74.125.235.0	0.0.0.0	HTTP/1.1	idle	1469 B	5.3 KB
S	74.125.235.1	0.0.0.0	HTTP/1.1	idle	1423 B	923 B
S	74.125.235.2	192.168.0.22	HTTP/1.1	idle	812 B	376 B
S	74.125.235.5	0.0.0.0	HTTP/1.1	idle	1675 B	988 B
S	74.125.235.6	0.0.0.0	HTTP/1.1	idle	1445 B	4237 B
S	74.125.235.7	192.168.0.22	HTTP/1.1	idle	822 B	376 B
S	74.125.235.9	0.0.0.0	HTTP/1.1	idle	1425 B	1848 B
S	74.125.235.13	192.168.0.22	HTTP/1.1	idle	3646 B	36.4 KB
S	74.125.235.25	0.0.0.0	HTTP/1.1	idle	4028 B	5.7 KB
S	74.125.235.26	0.0.0.0	HTTP/1.1	idle	2690 B	3123 B

Lab – Transparent Web Proxy

- Transparent proxy (proxy yang yang memaksa)
- Set pda IP>Firewall>NAT



NAT Rule <80>

General | Advanced | Extra | Action | Statistics

Chain: dstnat

Src. Address:

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

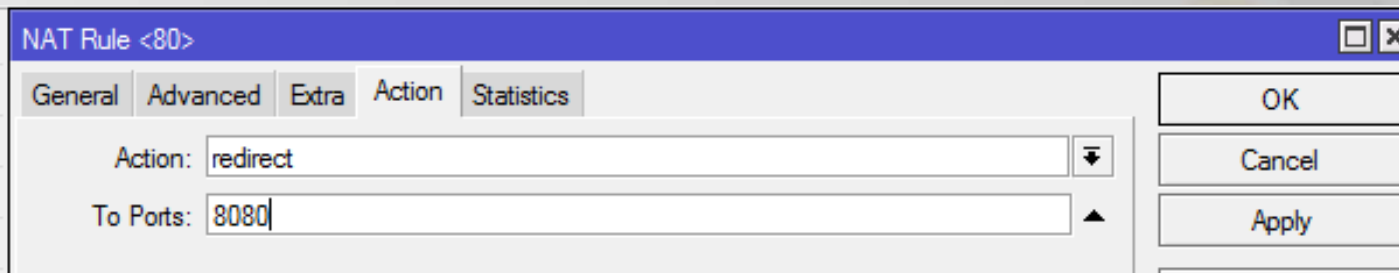
Dst. Port: 80

Any. Port:

In. Interface: ether1

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

- Action redirect to port 8080



NAT Rule <80>

General | Advanced | Extra | Action | Statistics

Action: redirect

To Ports: 8080

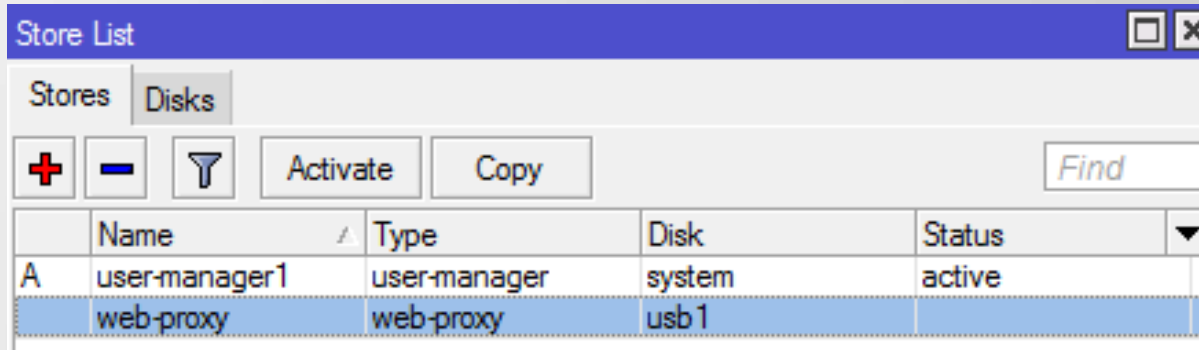
OK
Cancel
Apply

Store

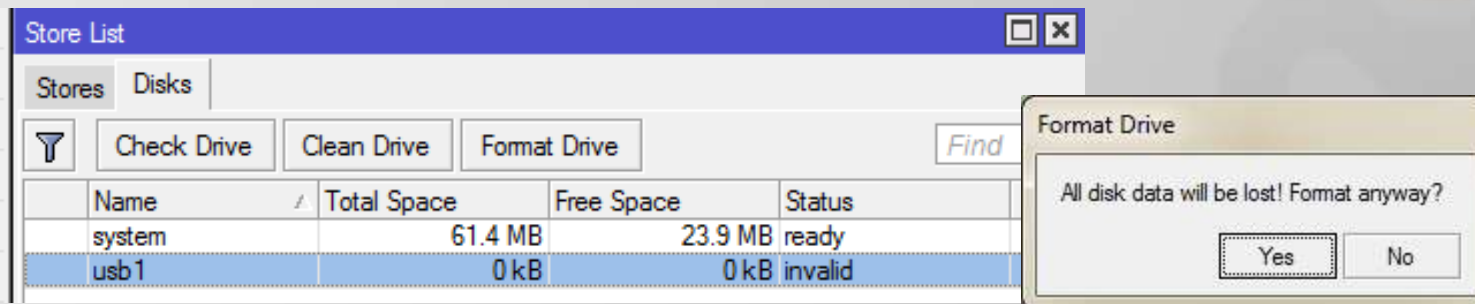
- Kita dapat mengatur media penyimpanan pada MikroTik
- Media penyimpanan dapat berupa internal disk (system storage) dan external disk (USB/Hardisk eksternal dll).
- Data yang dapat disimpan pada disk storage adalah data user manager dan web proxy.

Store

- Storage diseting pada menu System>Stores.



- Apabila menggunakan external disk (USB/hardisk external, disk harus diformat terlebih dahulu

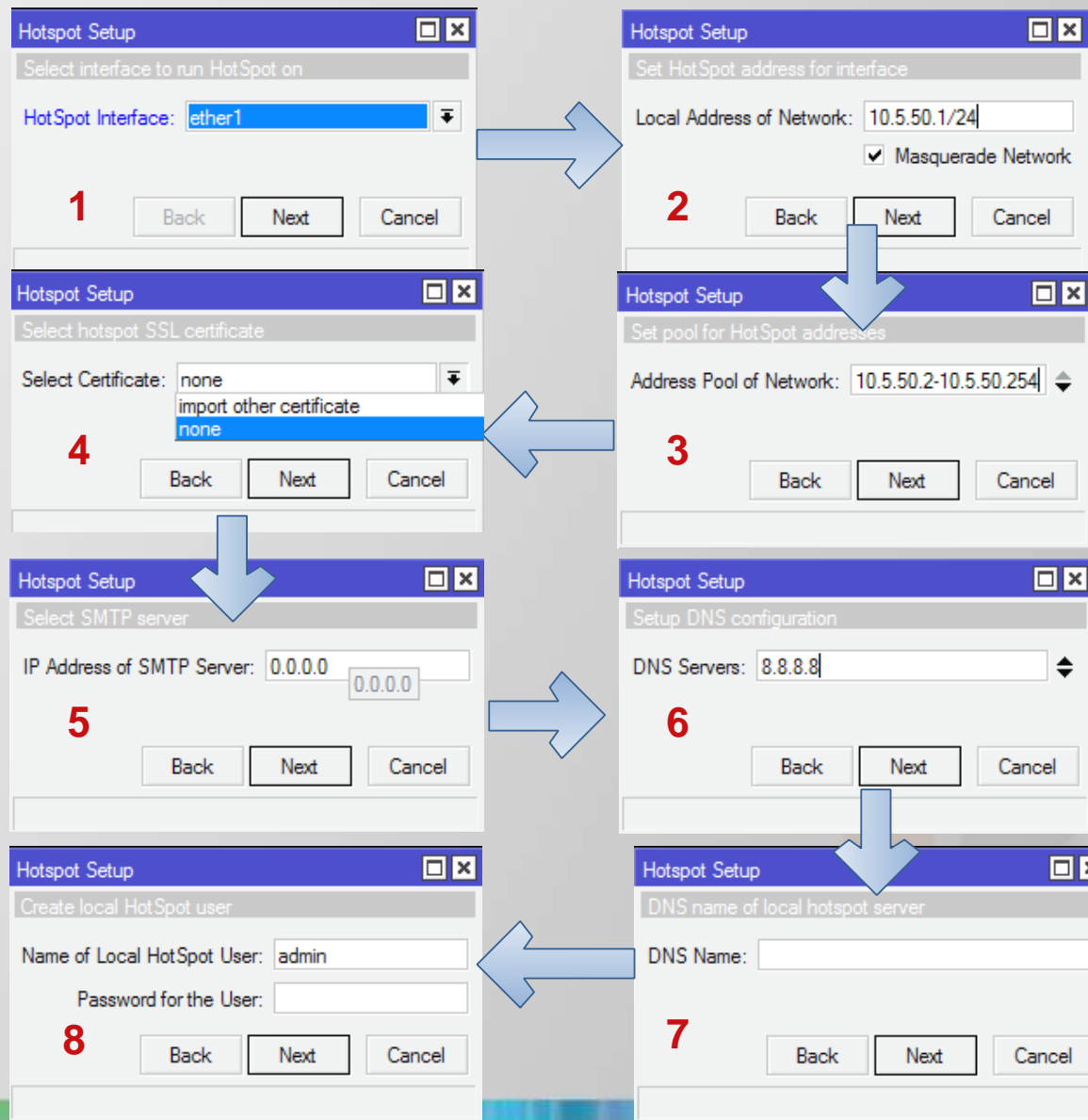


Hotspot

- Hotspot digunakan untuk memberikan layanan akses (Internet/Intranet) di area public, dengan media kabel maupun wireless.
- Ketika membuka halaman web maka router akan memeriksa apakah pengguna terautentifikasi atau tidak.
- Jika tidak melakukan otentikasi, pengguna akan dilempar ke halaman login hotspot yang memerlukan username dan password.
- Jika informasi login yang dimasukkan benar, maka router akan memasukkan user ke dalam sistem dan klien hotspot dapat mengakses halaman web.
- Penggunaan akses internet hotspot dapat dihitung berdasarkan waktu (time-based) dan data download / upload (volume-based). Selain itu, juga dapat dilakukan limit bandwidth berdasarkan time based dan volume based.

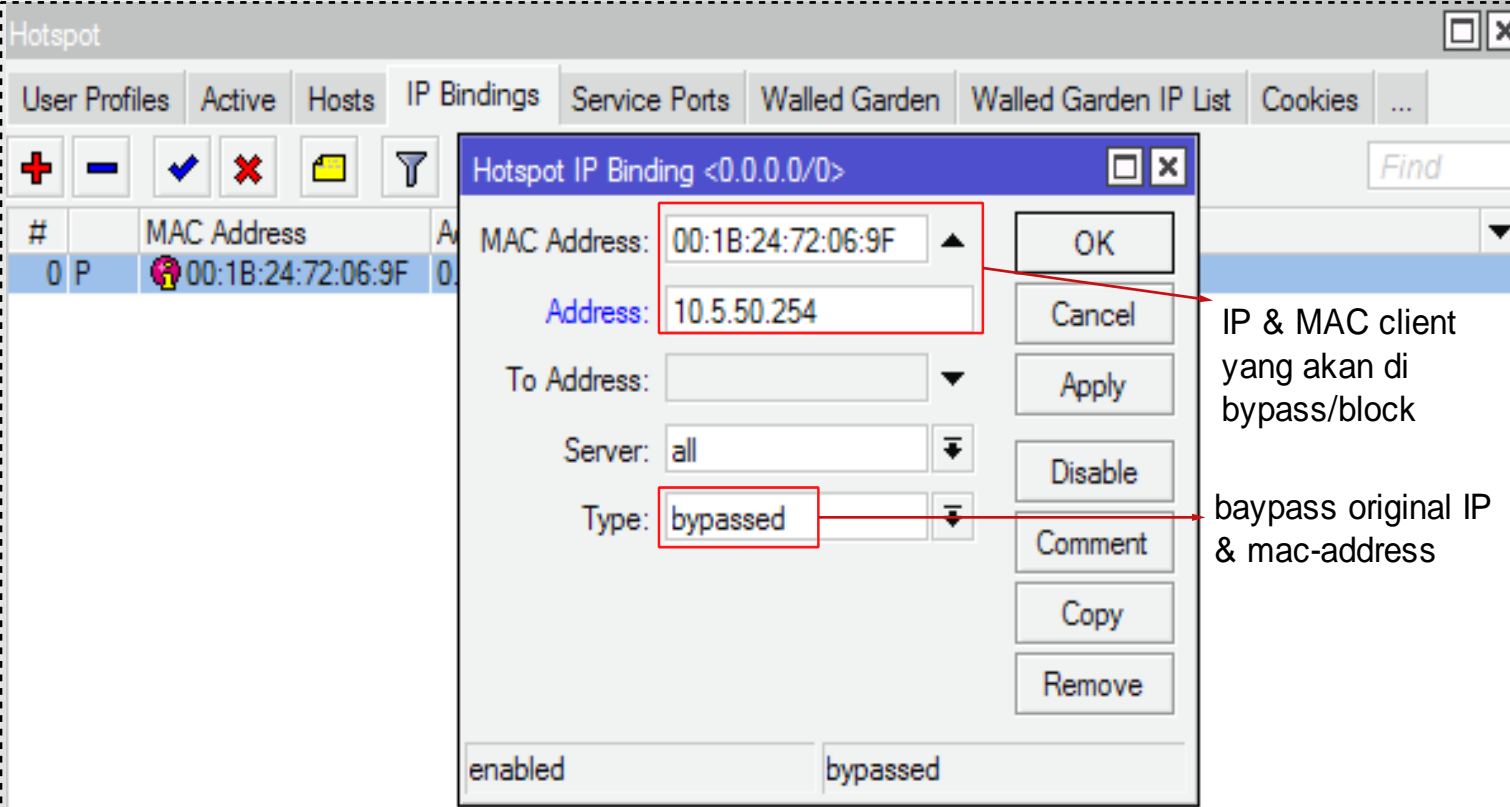
LAB-Hotspot

- Setting Hotspot



IP Binding

- Untuk bypass client tertentu dapat mengakses internet tanpa autentikasi (misal VIP client)



The screenshot shows the Mikrotik Hotspot configuration interface. The 'IP Bindings' tab is active, displaying a table with columns for '#', 'P', and 'MAC Address'. A single entry is visible with MAC address '00:1B:24:72:06:9F'. A dialog box titled 'Hotspot IP Binding <0.0.0.0/0>' is open, showing the configuration for this entry. The 'MAC Address' field is set to '00:1B:24:72:06:9F', the 'Address' field is set to '10.5.50.254', and the 'Type' dropdown is set to 'bypassed'. Red boxes highlight these fields, and red arrows point from text annotations to them.

#	P	MAC Address
0	P	00:1B:24:72:06:9F

Hotspot IP Binding <0.0.0.0/0>

MAC Address: 00:1B:24:72:06:9F

Address: 10.5.50.254

To Address: []

Server: all

Type: bypassed

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

Annotations:

- IP & MAC client yang akan di bypass/block (points to MAC and Address fields)
- bypass original IP & mac-address (points to Type dropdown)

enabled bypassed

Walled Garden

- Untuk bypass web tertentu bisa diakses all user tanpa autentikasi (misal web portal penyedia hotspot)

New Walled Garden Entry □ ×

Action: allow deny OK

Server: ▼ Cancel

Src. Address: ▼ Apply

Dst. Address: Disable

Method: ▼ -

Dst. Host:

Dst. Port:

Path:

enabled

Property	Description
action (<i>allow deny</i> ; Default: allow)	Action to perform, when packet matches the rule <ul style="list-style-type: none"> ▶ allow - allow access to the web-page without authorization ▶ deny - the authorization is required to access the web-page
server (<i>string</i> ; Default:)	Name of the HotSpot server, rule is applied to.
src-address (<i>IP</i> ; Default:)	Source address of the user, usually IP address of the HotSpot client
method (<i>string</i> ; Default:)	HTTP method of the request
dst-host (<i>string</i> ; Default:)	Domain name of the destination web-server
dst-port (<i>integer</i> ; Default:)	TCP port number, client sends request to
path (<i>string</i> ; Default:)	The path of the request, path comes after ""http://dst_host/""

Walled Garden IP

- Untuk bypass HOST/IP dengan ALL service bisa diakses all user tanpa autentikasi (misal web/email/ftp penyedia hotspot)

New Walled Garden IP Entry □ ×

Action: **accept** drop reject OK

Server: Cancel

Src. Address:

Dst. Address:

Protocol:

Dst. Port:

Dst. Host:

enabled

Property	Description
action (<i>allow deny reject</i> ; Default: allow)	Action to perform, when packet matches the rule <ul style="list-style-type: none"> ▶ allow - allow access to the web-page without authorization ▶ deny - the authorization is required to access the web-page ▶ reject - the authorization is required to access the resource, ICMP reject message will be sent to client, when packet will match the rule
server (<i>string</i> ; Default:)	Name of the HotSpot server, rule is applied to.
src-address (<i>IP</i> ; Default:)	Source address of the user, usually IP address of the HotSpot client
dst-address (<i>IP</i> ; Default:)	Destination IP address, IP address of the WEB-server. Ignored if dst-host is already specified.
dst-host (<i>string</i> ; Default:)	Domain name of the destination web-server. When this parameter is specified dynamic entry is added to Walled Garden
dst-port (<i>integer</i> ; Default:)	TCP port number, client sends request to
protocol (<i>integer string</i> ; Default:)	IP protocol

LAB Hotspot

- Koneksikan Router ke Internet sebagai NAT, laptop pada ether1 sebagai client.
- Jalankan Hotspot pada Ether1
- Apabila hotspot sudah running, buatlah agar:
- IP tertentu bisa dipakai laptop untuk browsing internet tanpa autentifikasi
- Hanya browsing www.training-mikrotik.com yang tanpa autentifikasi hotspot.
- FTP ke www.training-mikrotik.com tanpa autentifikasi hotspot