INTRA Training Center

PRE-MTCNA

21 - 23 April 2017

I.N.T.R.A Training Center
The Path of Development Skill

SMK-Net INDONESIA

Persembahan BLC TELKOM Untukmu INDONESIA

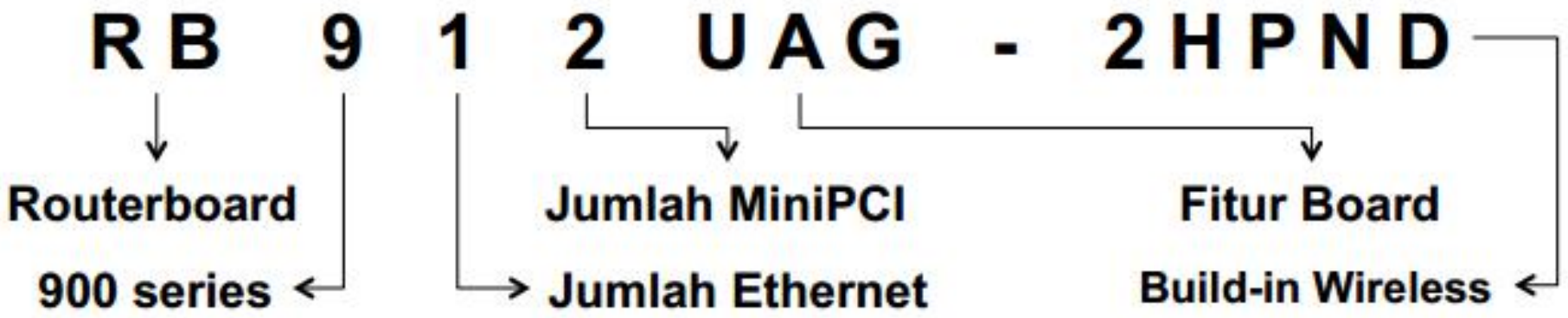
Introduction About MikroTik

- **RouterOS** > Software Router untuk PC (x86, AMD, DLL).
  - Menjadikan PC biasa memiliki fungsi router yang lengkap
  - Diinstall sebagai Operating System, Tidak membutuhkan operating system lainnya.
- **Routerboard >** Hardware untuk jaringan (terutama wireless)
  - Wireless board(Contoh : RB400, RB600, RB750, RB1000,dll)
  - Wireless Interface(R52, R52H, R5H, R52N, R2N,dll)
  - Menggunakan RouterOS sebagai software

Introduction About MikroTik

- MikroTik adalah kependekan dari "**mikrotikls**"
- Artinya : "network kecil" dalam bahasa Latvia

Product Code



Fitur Board Code :

U : USB
P : PoE out
i : single PoE out
A : RAM besar (bisa juga lisensi)
H : CPU besar

G : Gigabit
L : Light Edition
S : SFP Port
e : PCIe Extension Card
X : Jumlah CPU Core

MikroTik RouterOS

- RouterOS adalah sistem operasi dan perangkat lunak yang mampu membuat PC berbasis Intel/AMD mampu melakukan fungsi **Router, Bridge, Firewall, Bandwidth Management, Proxy, Hotspot,** dan masih banyak lagi.
- RouterOS dapat melakukan hampir semua fungsi networking dan juga beberapa fungsi server.

Fitur MikroTiK RouterOS

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

Fitur MikroTiK RouterOS

- Services (Server)
  - Proxy(cache), Hotspot, DHCP, IP Pool, DNS, NTP, Radius Server(User-Manager), Samba(v6.xx)
- AAA
  - PPP, Radius Client
  - IP Accounting, Traffic Flow
- Monitoring
  - Graphs, Watchdog, Tourch, Custom Log, SNMP, The Dude Monitoring Tools
- Diagnotic Tools & Scripting
  - Ping, TCP Ping, Tracert, Network Monitoring, Traffic Monitoring, Scheduller, Scripting
- VRRP

License Level

Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key	registration required	volume only	$45	$95	$250
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

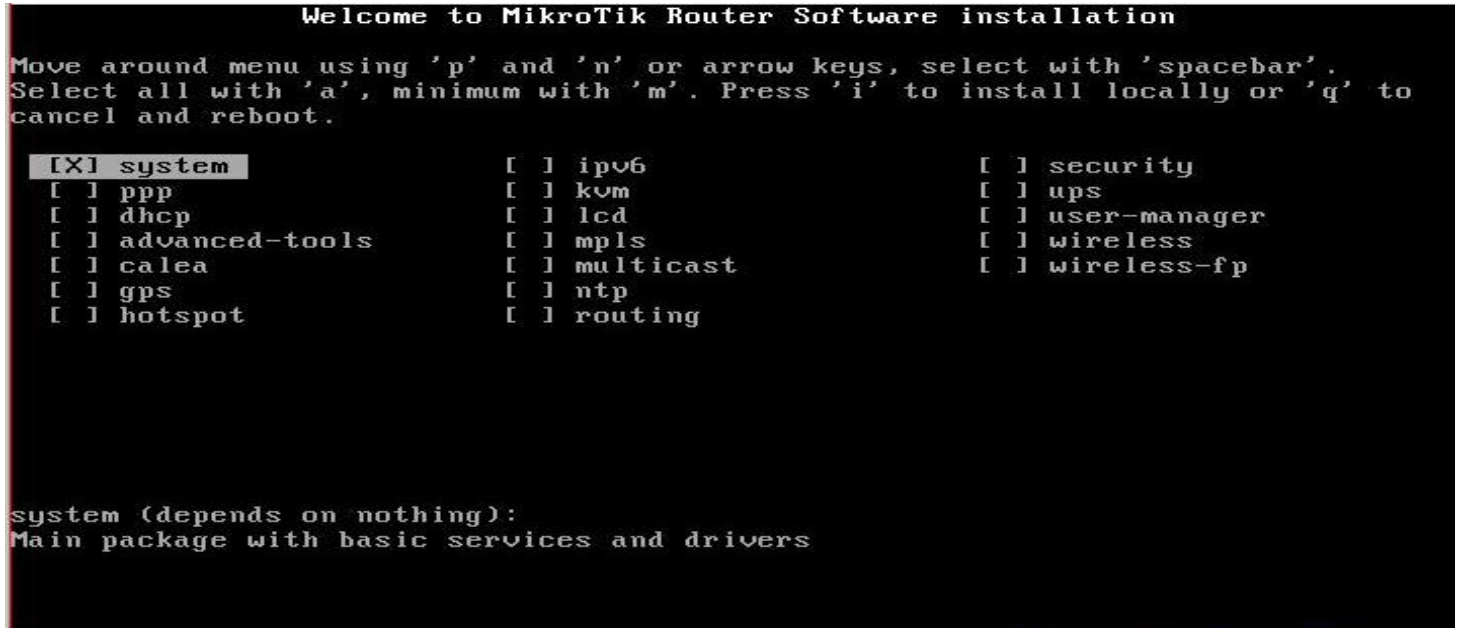
Buyer's Guide

- 300/400 Mhz Processor (< **5Mbps** Traffic)
  - RB450, RB750, RB433, RB493
- 680 Mhz Processor (**5 - 20 Mbps** Trafic)
  - RB450G, RB433AH, RB493G
- 1Ghz Processor (**20 - 100 Mbps** Traffic)
  - RBB1200, RB1100AH
- 1Ghz Dual Core Processor (> **100 Mbps** Traffic)
  - RB1100AHx2
- Multi Core x86 Processor (> **1 Gbps** Traffic)
  - Mikrobits : Aneto, Ainos, Dinara
- Xeon Processor (> **10 Gbps** Traffic)
  - Mikrobits : Dinara

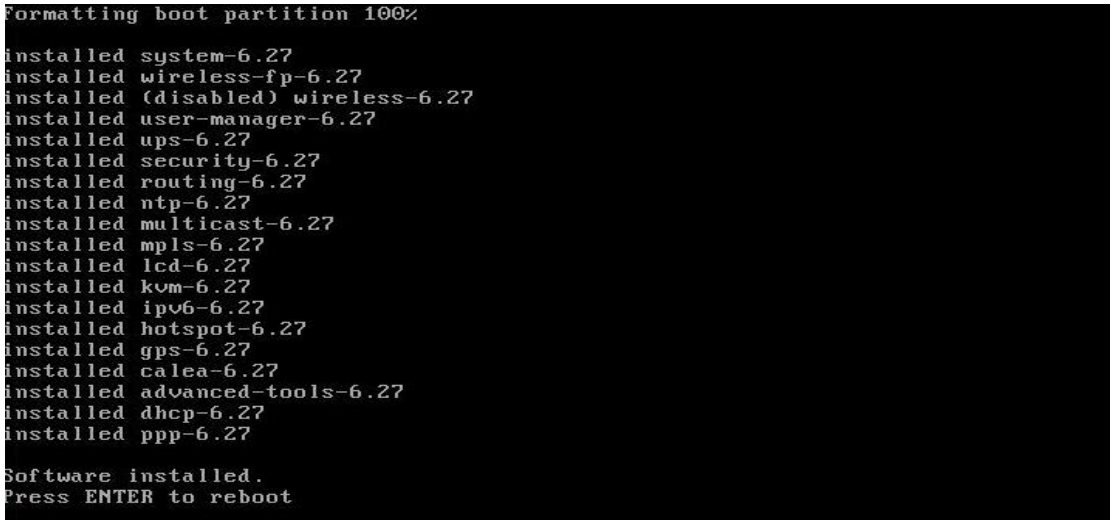
RouterOS

- Kita bisa menginstall system operasi MikroTik RouterOS di PC kita. Yang fungsinya sendiri untuk “merubah” fungsi computer kita menjadi layaknya suatu Router MikroTik. RouterOS sendiri mempunyai 6 Level Lisensi (berbayar). Kita bisa mendownload secara gratis versi Trial RouterOS yang tersedia di website MikroTik (www.MikroTik.com) dan hanya bisa digunakan selama 24 Jam. Atau kita juga bisa membeli Disk On Module yang telah ter install RouterOS MikroTik. Disini kita akan membahas cara menginstal RouterOS dengan menggunakan metode Harddisk. Sebelum itu, ada beberapa hal yang dibutuhkan :
- PC
- CD yang telah di Burning ISO RouterOS

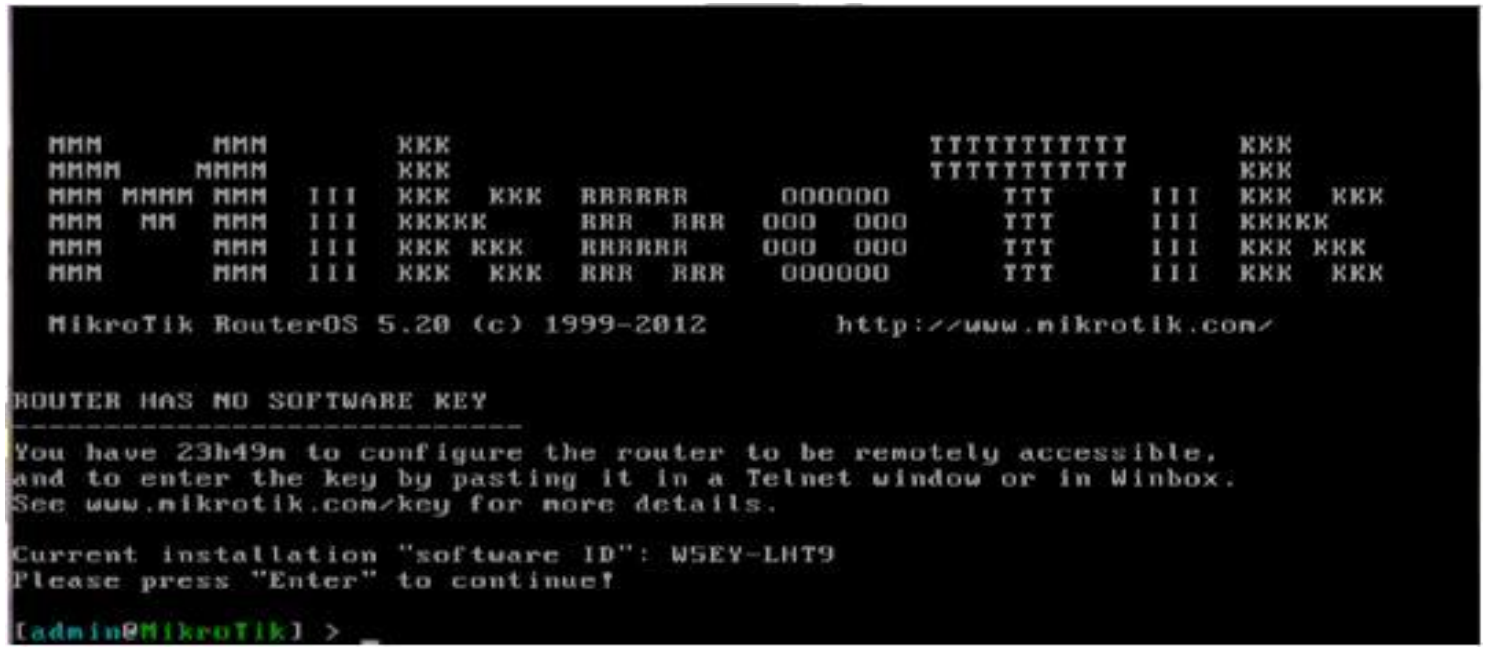
- Untuk melakukan penginstallan secara virtual, kita bisa menggunakan VM VirtualBox. Sekarang, kita langsung saja masuk menuju langkah cara menginstall RouterOS :
- 1.Kita masukkan CD yang telah terisi ISO RouterOS tadi ke dalam Komputer
- 2.Sebelum itu, pastikan setting First boot Devices pada BIOS menjadi CD/DVD ROM
- 3.Setelah mengatur First Boot Device pada BIOS, Save lalu Restart PC kita. Setelah itu, akan ada tampilan pertama instalasi RouterOS



- 4.Dibagian ini kita disuruh memilih Fitur RouterOS apa saja yang akan diinstall. Jika ingin menginstall semua Fitur, Tekan huruf “a” setelah itu tekan huruf “i” untuk memulai penginstalan RouterOS.
- 5.Setelah itu, kita akan ditanya apakah sudah yakin dengan paket yang akan diinstal. Kita tekan huruf “y” saja. Lalu akan ada peringatan bahwa harddisk akan diformat. Tekan huruf “y” lagi saja untuk memulai instalasi RouterOS
- 6.Proses instalasi dimulai. Jika sudah, maka kita tekan tombol enter untuk me reboot PC kita. Sebelum itu, Keluarkan CD instalasi RouterOS nya.

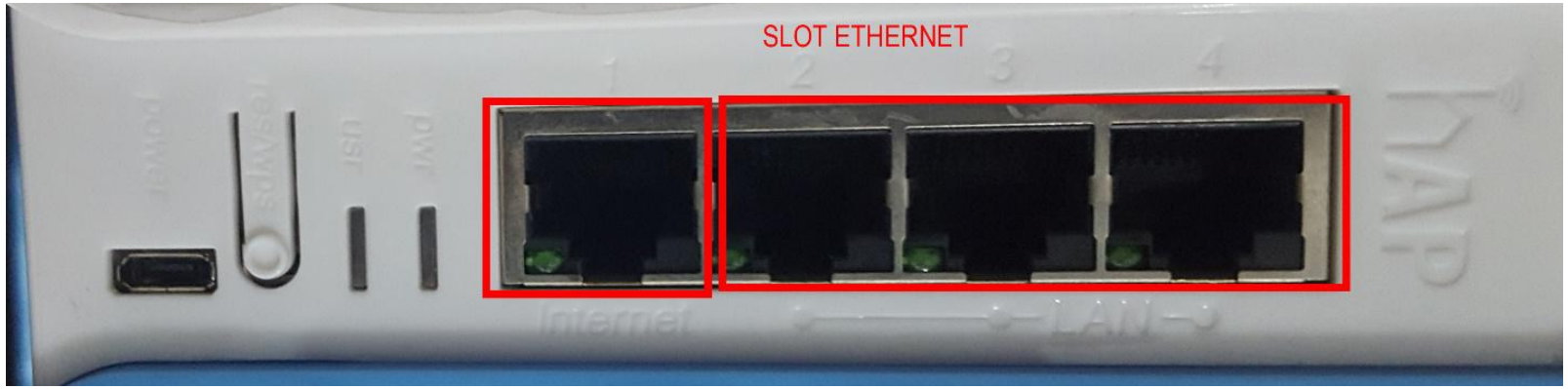


- 7.Setelah itu, akan ada tampilan Login. Untuk Login ke Router MikroTik, kita gunakan username : admin lalu passwordnya kosongkan saja (tidak menggunakan Password) setelah itu kita klik enter. Lalu akan ada tampilan pertama RouterOS

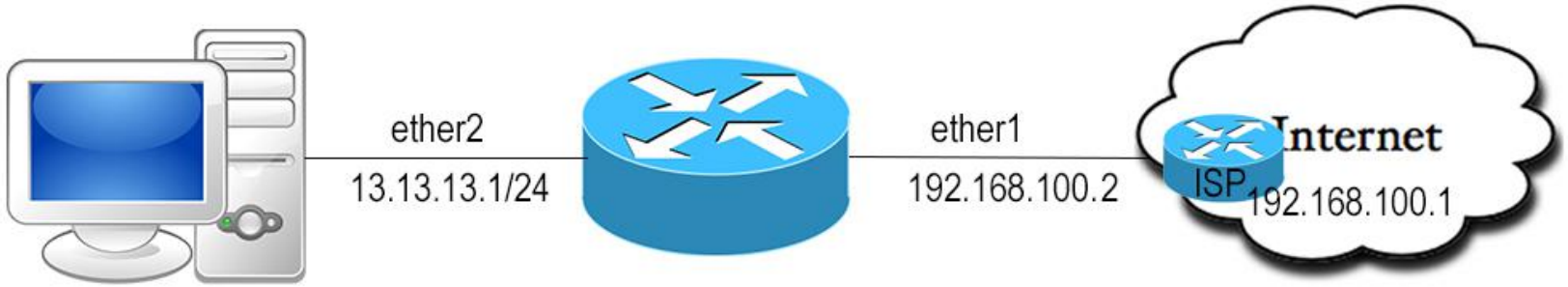


Fundamental RouterOS

- Kita akan mulai dengan cara meremote Routerboard menggunakan Winbox. Untuk melakukan konfigurasi pada Router, kita harus menghubungkan Router dengan PC Client dengan media Kabel (UTP) melalui interface ethernet. Pada setiap Routerboard sendiri mempunyai slot ethernet yang jumlahnya berbeda-beda. saya sendiri menggunakan salah satu Routerboard MikroTik yang mempunyai 4 interface ethernet dan 1 interface wireless.

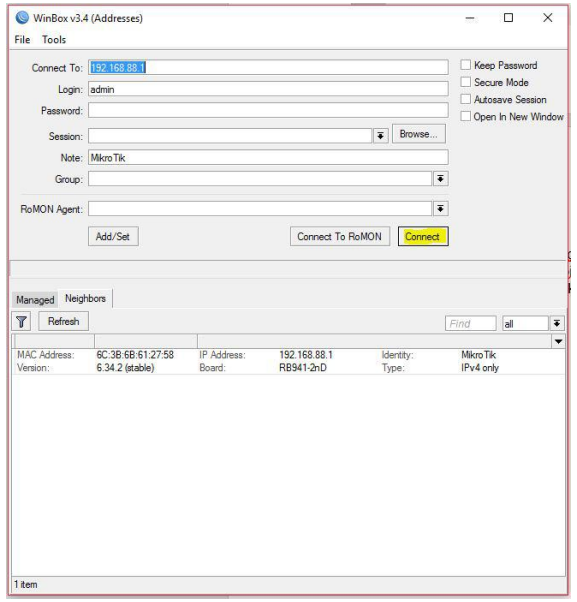


- Disini saya menggunakan Slot ethernet1 sebagai media penghubung antara router MikroTik dengan Internet (router ISP) dan slot ethernet2 saya gunakan untuk mengkoneksikan Routerboard dengan PC. Kita akan melakukan konfigurasi pada Router dengan Topologi dibawah ini :

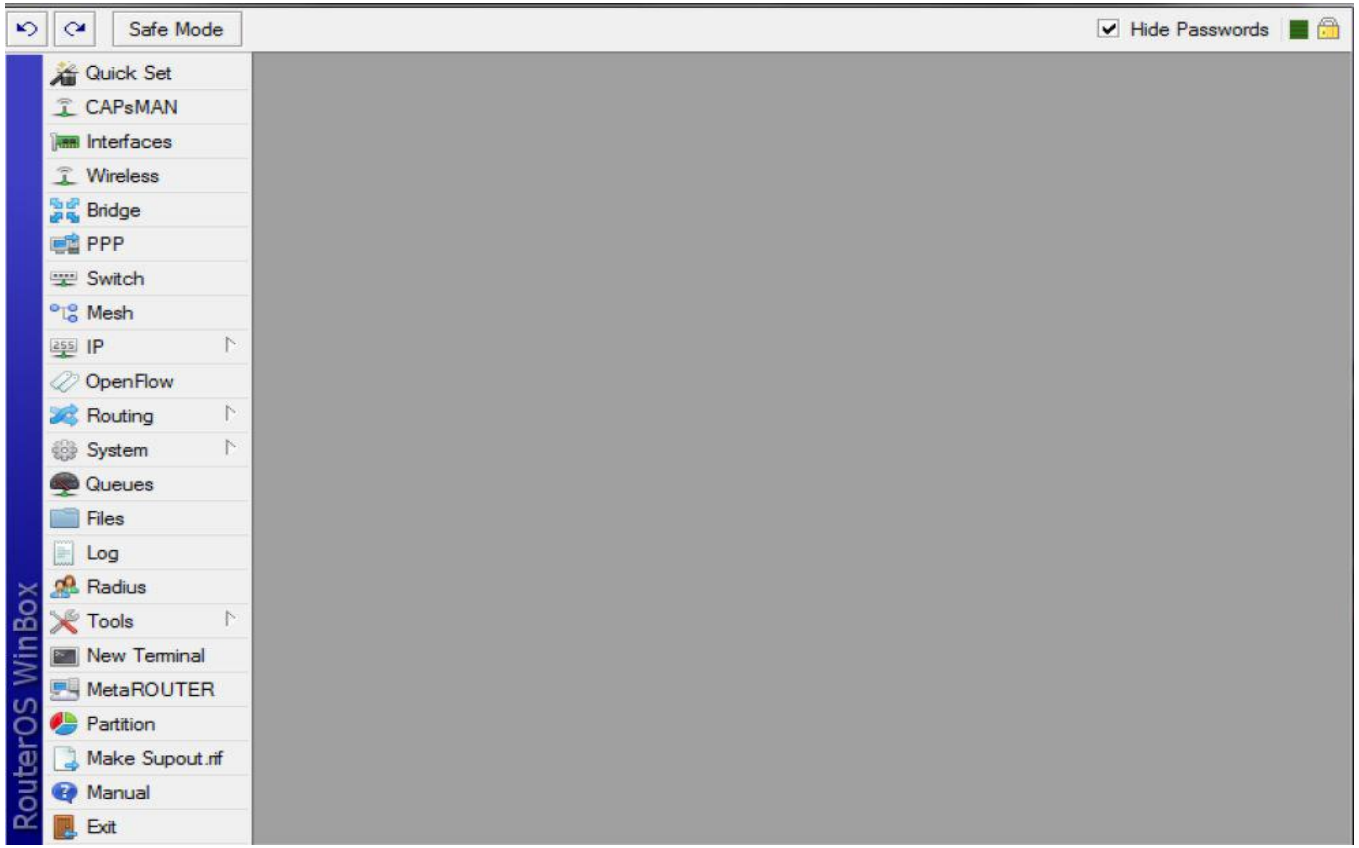


Meremote Routerboard (WinBox)

- Winbox adalah aplikasi untuk meremote Routerboard dengan melalui MAC Address atau melalui IP Address dari router tersebut. Menggunakan Winbox sendiri lebih mudah, karena aplikasi ini berbasi GUI, jadi hanya tinggal klak-klik saja untuk melakukan konfigurasi pada Routerboard kita, dan juga terdapat Terminal / Command Prompt pada aplikasi Winbox ini. Kita bisa meremote routerboard menggunakan winbox dengan cara berikut ini :
- 1.Pastikan PC dengan Router telah terhubung. Pertama, kita buka aplikasi WinBox yang telah di download. Maka, akan ada tampilan Winbox seperti berikut
- 2.Kita klik pada MAC Address router, setelah itu kita klik Connect
- 3.Kita bisa juga menggunakan IP Address router untuk meremote Routerboardnya, (IP Address default routerboard 192.168.88.1) tetapi, dianjurkan untuk menggunakan MAC Address. Agar jikalau kita melakukan konfigurasi IP, nanti tidak akan Logout sendiri.
- 4.Di samping adalah tampilan Winbox jika sudah terkoneksi

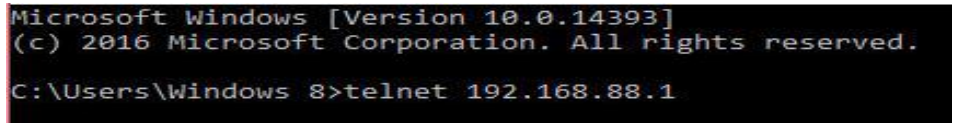


- 5.Setelah terkoneksi dengan winbox, kalian bisa melakukan Konfigurasi dengan cara meng-klik menu yang ada. Kita bisa juga mengkonfigurasi melalui CLI pada Winbox dengan cara klik menu New Terminal



Remote Routerboard (Telnet)

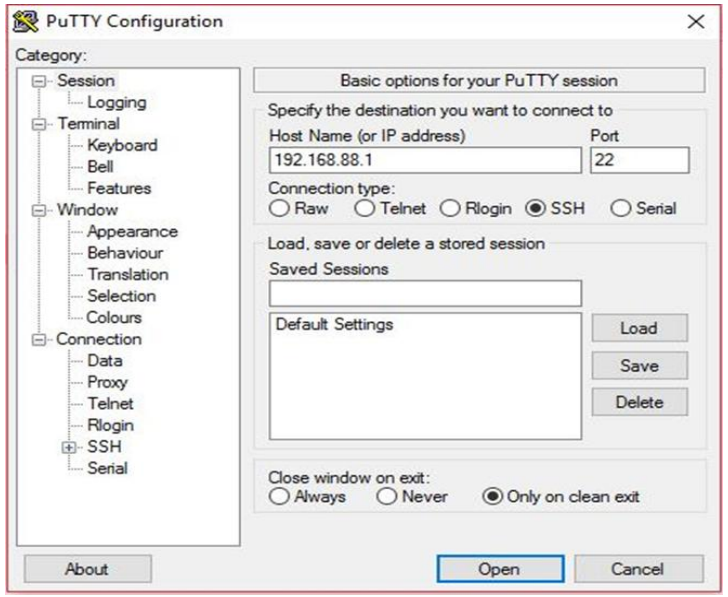
- Setelah tadi kita meremote menggunakan WinBox, kita juga bisa me remote routerboard melalui SSH dan Telnet. Jika melalui Telnet dan SSH, kita akan menggunakan Perintah Text (CLI) untuk melakukan konfigurasi. Untuk menggunakan Telnet, kita bisa melalui CMD atau bisa juga melalui aplikasi pihak ketiga yaitu PuTTy . Jika menggunakan Telnet melalui CMD, kita buka dulu CMD dengan cara menekan tombol Windows + R lalu ketik CMD. Setelah itu kita enter/run. Setelah CMD terbuka, kita ketik perintah seperti ini :
- telnet<spasi>[IP Address Routerboard] . contoh = telnet 192.168.88.1



- Setelah itu tekan enter, lalu akan muncul tampilan Login MikroTik. Isi dengan username admin lalu passwordnya kosongkan saja (tidak usah diisi)
- Setelah login, kalian bisa mengkonfigurasi Routerboard melalui CLI (text)

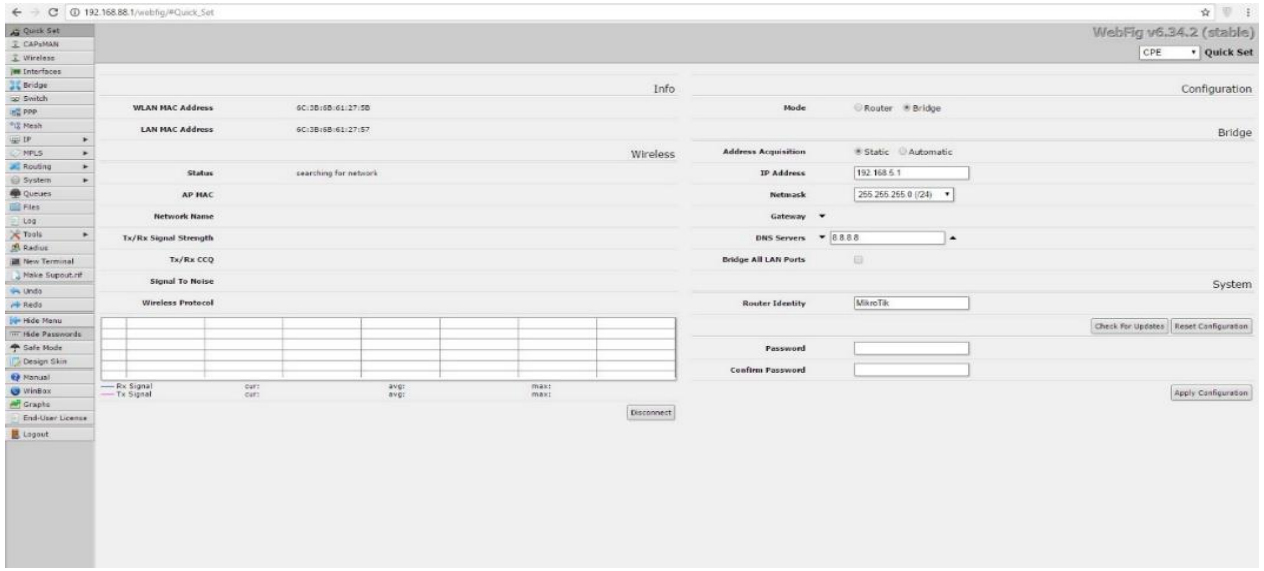
Remote Routerboard (SSH)

- Pertama, kalian download dulu aplikasi Putty. Jika sudah, buka aplikasinya. Akan ada tampilan seperti dibawah ini (Gambar 1.4)
- Kita isi IP Address routerboard kita, lalu di bagian connection type kita pilih Telnet (23) atau SSH (22) setelah itu klik open.
- Lalu kita login dengan Username Password yang tadi
- Dalam penggunaan SSH dan Telnet sendiri hampir sama, tetapi SSH lebih aman karena adanya proses enkripsi data.



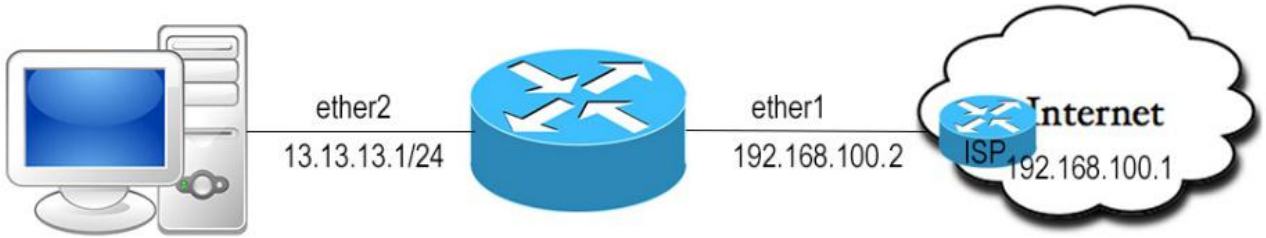
Remote Routerboard (Web Configuration)

- Sekarang, kita akan meremote routerboard melalui Web Configuration melalui aplikasi Web Browser, seperti Mozilla atau Google Chrome. Caranya sangat mudah, kita tinggal isi kan IP Address dari router di bagian Search Bar yang ada di browser. Lalu tekan enter.
- Setelah terbuka, akan ada tampilan Login, isi dengan username dan password yang sebelumnya. Setelah login, akan ada tampilan web konfig nya. Seperti gambar dibawah ini



Konfigurasi Interface

- Setelah tadi kita membahas cara meremote routerboard, sekarang kita akan membahas tentang konfigurasi Interface pada router. Routerboard sendiri mempunyai interface yang jumlahnya berbeda-beda dan biasanya dinamai dengan ether1, ether2, … kita bisa lihat gambar dibawah ini, saya menggunakan slot Ether2 untuk mengkoneksikan Router dengan Komputer dan slot Ether1 digunakan untuk menghubungkan Router dengan ISP (internet)



(LAB)Konfigurasi Interface

- Untuk melihat Jumlah interface, status interface di router, kita bisa menggunakan perintah (CLI) sebagai berikut : **interface print**

```
[admin@MikroTik] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                TYPE       ACTUAL-MTU L2MTU  MAX-L2MTU MAC-ADDRESS
 0  R  ether1                              ether            1500  1598       2028 6C:3B:6B:4F:CA:81
 1  R  ether2                              ether            1500  1598       2028 6C:3B:6B:4F:CA:82
 2     ether3                              ether            1500  1598       2028 6C:3B:6B:4F:CA:83
 3     ether4                              ether            1500  1598       2028 6C:3B:6B:4F:CA:84
 4  X  wlan1                               wlan             1500  1600       2290 6C:3B:6B:4F:CA:85
```

- Keterangan : # = Nomor Interface. (berguna untuk mengkonfigurasi Interface melalui CLI)
- R = Menandakan bahwa interface tersebut sedang berjalan (digunakan)
- Kita bisa mengganti nama interface router MikroTik. Misalkan, Ether1 kita ganti nama menjadi INTERNET dan ether2 menjadi CLIENT. Kita bisa menggantinya dengan perintah : **interface set (nomor interface) name=(nama yang akan diganti)**
- Contoh **: interface set 0 name=internet**
- Maka, nama interface akan terganti

(LAB)Konfigurasi Interface

```
[admin@Rangga] > interface set 0 name=internet
[admin@Rangga] > interface pr
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                    TYPE       ACTUAL-MTU L2MTU
 0  R  internet                                ether            1500
```

- Kita juga bisa mendisable interface yang tidak terpakai menggunakan perintah : **interface disable** (nomor interface)
- Contoh : **interface disable 2,3**
- Setelah itu, coba kita lihat interface nya tadi. Maka di sebelah nomor nya akan ada tanda X yang berarti interface tersebut tidak bisa di gunakan karena kita nonaktifkan.

```
[admin@Rangga] > interface disable 2,3
[admin@Rangga] > interface pr
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                    TYPE       ACTUAL-MTU L2MTU
 0  R  CLIENT                                  ether            1500
 1  R  INTERNET                                ether            1500
 2  X  ether3                                  ether            1500
 3  X  ether4                                  ether            1500
```

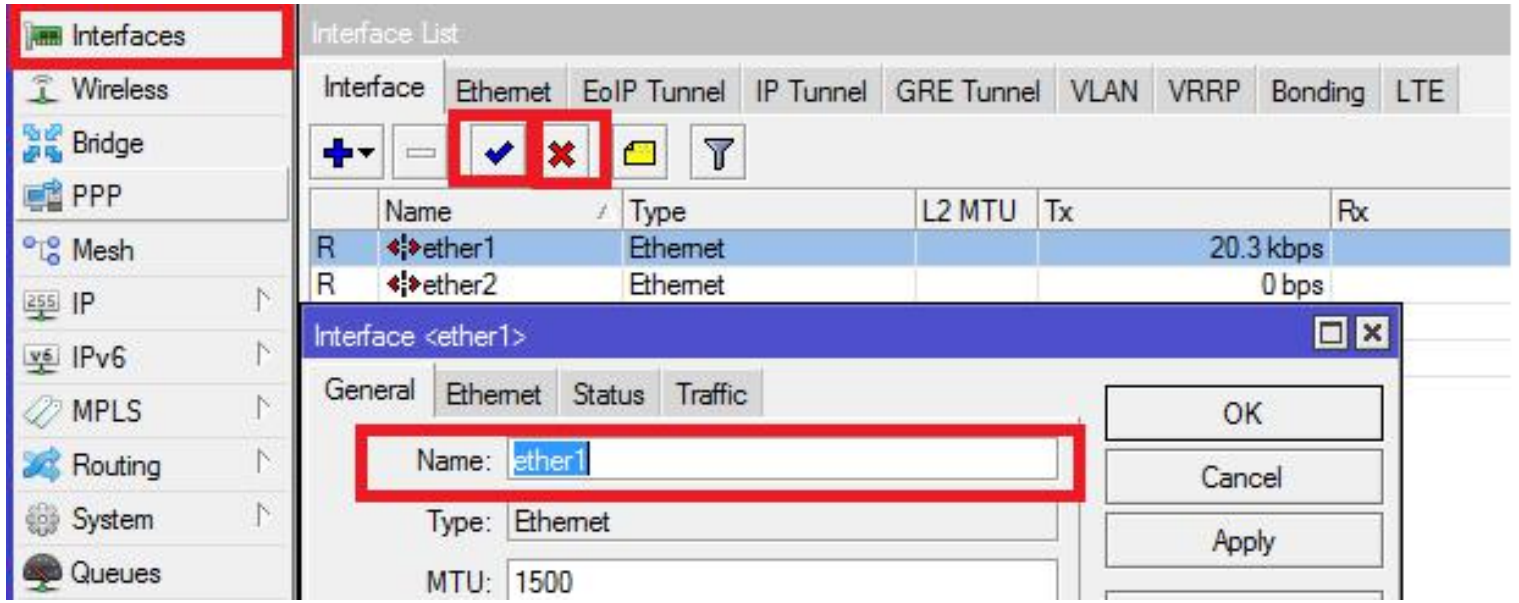
(LAB)Konfigurasi Interface

- Kita bisa lihat gambar diatas, interface yang sudah di nonaktifkan. Kita bisa mengaktifkan nya (enable) kembali, dengan perintah : interface enable (nomor interface)
- Contoh : **interface enable 2,3**
- Jika sudah, maka interface tersebut telah diaktifkan kembali dan bisa kita gunakan

```
[admin@Rangga] > interface enable 2,3
[admin@Rangga] > interface pr
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                TYPE       ACTUAL-MTU L2MTU
 0  R  CLIENT                              ether            1500
 1  R  INTERNET                            ether            1500
 2     ether3                              ether            1500
 3     ether4                              ether            1500
```

(LAB)Menambahkan IP Address

- Jika melalui WinBox (GUI) , kita bisa mengatur Interface dengan cara klik menu Interfaces
- Untuk mendisable Interfacenya, klik tombol X untuk men enable nya, klik tombol ceklis



(LAB)Menambahkan IP Address

- Setelah tadi kita membahas tentang interface, sekarang kita akan menambahkan IP Address untuk Interface tersebut. Sesuai dengan gambar Topologi, kita akan mengisi IP Address ether1 dengan IP Address yang satu network dengan IP Router ISP dan kita akan mengisi IP Address interface penghubung antara PC dan Router atau ether2 agar PC dan Router terhubung dengan baik. Untuk menambahkan IP Address menggunakan perintah text (CLI) dapat dilakukan dengan perintah sebagai berikut : **ip address add address=[no ip] interface=[nama interface]**
- Sebagai contoh, disini kita akan menambahkan IP ether1(internet), dan IP ether2 (client) maka perintahnya adalah sebagai berikut :
- Ether1 : **ip address add address=192.168.100.2/24 interface=ether1**
- Ether2 : **ip address add address=13.13.13.1/24 interface=ether2**

(LAB)Menambahkan IP Address

- Setelah itu, kita cek IP yang tadi kita buat menggunakan perintah : **ip address print**

```
[admin@MikroTik] > ip address add address=192.168.100.2/24 interface=ether1
[admin@MikroTik] > ip address add address=13.13.13.1/24 interface=ether2
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   192.168.100.2/24   192.168.100.0   ether1
 1   13.13.13.1/24      13.13.13.0      ether2
```

- Bisa kita lihat gambar diatas, kita sudah berhasil menambahkan IP Address. Jika ada kesalahan dan ingin menghapus IP Address tersebut, kita bisa menggunakan perintah :
- **Ip address remove [nomor index # IP]**
- Contoh : **ip address remove 1**
- Setelah itu, kita cek menggunakan perintah ip address print

(LAB)Menambahkan IP Address

```
[admin@MikroTik] > ip address remove 1
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   192.168.100.2/24   192.168.100.0   ether1
```

- IP sudah berhasil dihapus. Jika sudah dihapus, kita buat lagi dengan IP yang sesuai.
- Untuk menambahkan IP lewat WinBox,(GUI) bisa masuk ke menu IP Addresses +
- Lalu kita isi IP Addressnya, dan pilih Interface nya. Setelah itu, klik OK

(LAB)Menambahkan Gateway

- Kita lanjutkan Konfigurasi Router nya agar terhubung dengan koneksi internet, sekarang kita akan melakukan konfigurasi Gateway. Gateway berfungsi sebagai ”gerbang” antara router dengan koneksi internet, yang mana nantinya Gateway ini kita isi dengan IP Address ISP (biasanya, ISP menggunakan IP Host pertama, contoh 192.168.100.1) dan dst-address (destination address / alamat tujuan) nya menggunakan IP 0.0.0.0/0 karena kita akan menghubungkan router dengan koneksi internet. Kita langsung saja ke langkah konfigurasinya.
- Melalui perintah Text (CLI) : **ip route add dst-address=0.0.0.0/0 gateway=192.168.100.1**

(LAB)Menambahkan Gateway

- Setelah itu, kita cek gateway yang tadi kita buat dengan menggunakan perintah : ip route print Bisa kita lihat di sebelah kiri terdapat symbol A S yang berarti Active Static

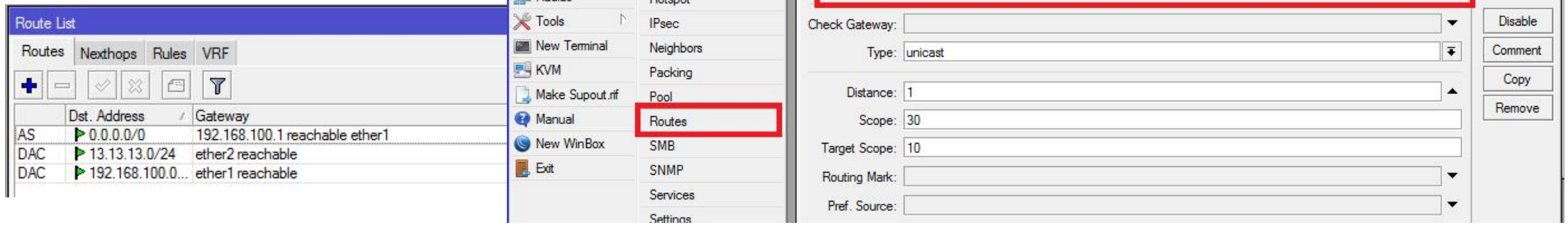
```
[admin@MikroTik] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 A S  0.0.0.0/0                          192.168.100.1             1
 1 ADC  13.13.13.0/24      13.13.13.1      ether2                    0
 2 ADC  192.168.100.0/24   192.168.100.2   ether1                    0
```

- Jika kalian melakukan kesalahan dalam melakukan konfigurasi gateway nya, kita bisa hapus dengan menggunakan perintah : **ip route remove 0**

```
[admin@MikroTik] > ip route remove 0
```

(LAB)Menambahkan Gateway

- Untuk cara mudahnya (melalui GUI Winbox) bisa dilakukan dengan cara klik menu IP Routes + (add) setelah itu kita isi dst-address nya dan gateway nya. Setelah itu klik OK.



- Jika sudah, bisa kita lihat akan ada **tulisan reachable ether1** yang artinya berhasil dan sudah tersambung.

Menambahkan DNS Server

- Setelah menambahkan default Gateway nya, sekarang kita akan menambahkan DNS (Domain Name System) Server. DNS sendiri fungsinya untuk pemetaan alamat IP yang tadinya angka menjadi nama. Karena kalau internetan, kita berkomunikasi dengan suatu web tersebut dengan IP Addressnya. Kan repot kalau kita harus memasukkan IP Address dari website tersebut kalau kita ingin melakukan browsing pada website tersebut. Jadi, disitulah fungsi DNS Server. Sekarang, kita langsung saja ke langkah konfigurasi nya :
- Kita disini akan menggunakan DNS dari ISP (sama seperti gateway tadi, yaitu 192.168.100.1). Untuk konfigurasi melalui perintah text (CLI) dapat dilakukan seperti berikut ini :

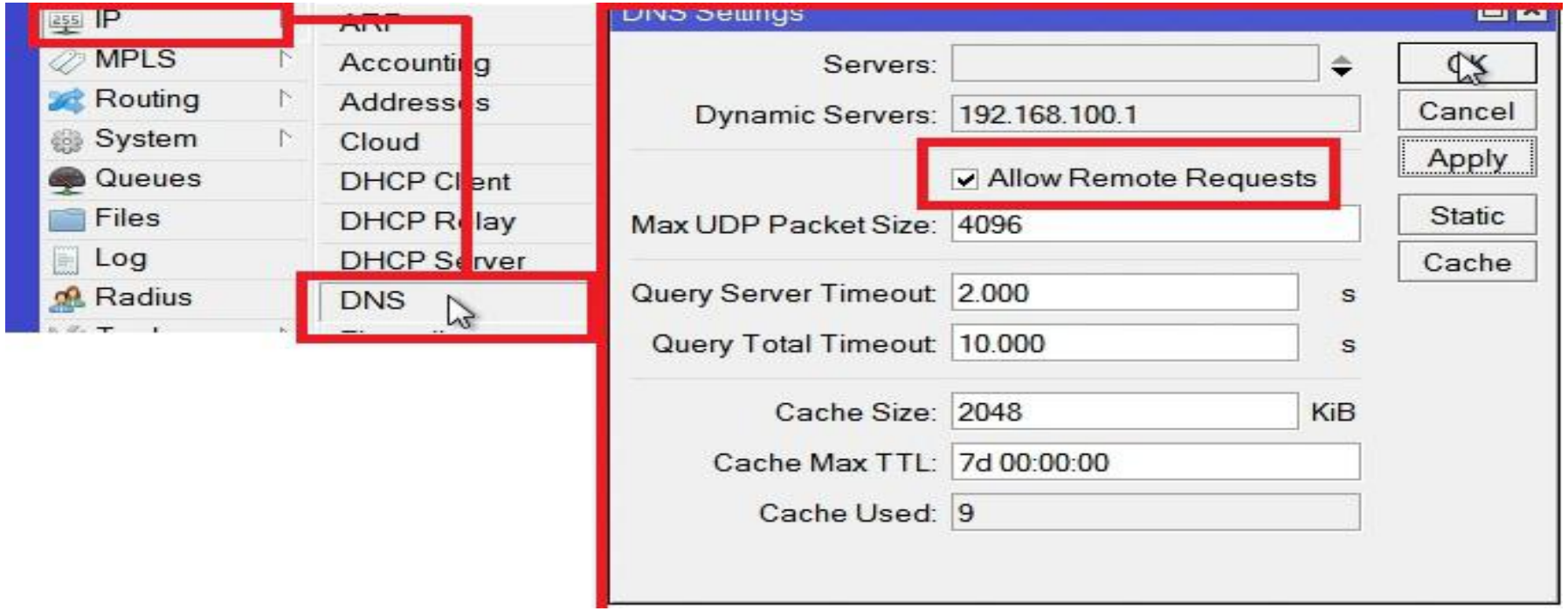
(LAB)Menambahkan Gateway

- **Ip dns set servers=[ip dns ips] allow-remote-requests=yes**
- (Allow Remote Requests disini berfungsi menjadikan Router sebagai DNS Server bagi client. Jadinya, Client tidak perlu menggunakan dns dari ISP lagi. Client Cukup menggunakan IP dari interface Router yang terhubung dengan Client (ether2). Karena nantinya Client akan diarahkan menuju DNS Server Router MikroTik)
- Contoh : **ip dns set servers=192.168.100.1 allow-remote-request=yes**
- Setelah kita buat, kita cek menggunakan perintah **ip dns print**

```
[admin@MikroTik] > ip dns set servers=192.168.100.1 allow-remote-requests=yes
[admin@MikroTik] > ip dns print
                  servers: 192.168.100.1
         dynamic-servers:
  allow-remote-requests: yes
    max-udp-packet-size: 4096
   query-server-timeout: 2s
    query-total-timeout: 10s
              cache-size: 2048KiB
          cache-max-ttl: 1w
             cache-used: 9KiB
```

(LAB)Menambahkan Gateway

- Jika melalui WinBox (GUI) klik menu IP DNS. Lalu setelah itu, isi Servers nya dengan IP host pertama dari ISP tadi (sama dengan gateway) dan beri tanda ceklis pada kotak Allow Remote Request. Setelah itu, klik OK.



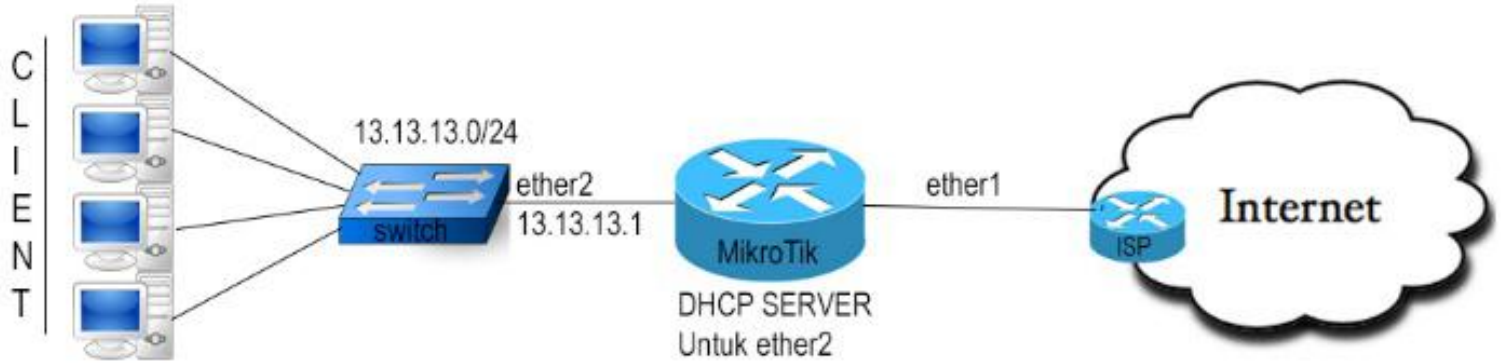
(LAB)Menambahkan Gateway

- Kita sudah selesai mengatur IP Address, Gateway, DNS Server nya. Berarti sekarang, router sudah bisa terkoneksi dengan Jaringan Internet. Untuk melakukan pengujian, Coba kita lakukan ping google.com pada router. Jika reply, artinya router telah terhubung dengan jaringan internet.

```
[admin@MikroTik] > ping google.com
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 74.125.68.101                              56  44 29ms
    1 74.125.68.101                              56  44 29ms
    2 74.125.68.101                              56  44 25ms
    3 74.125.68.101                              56  44 28ms
    4 74.125.68.101                              56  44 25ms
    sent=5 received=5 packet-loss=0% min-rtt=25ms avg-rtt=27ms max-rtt=29ms
```

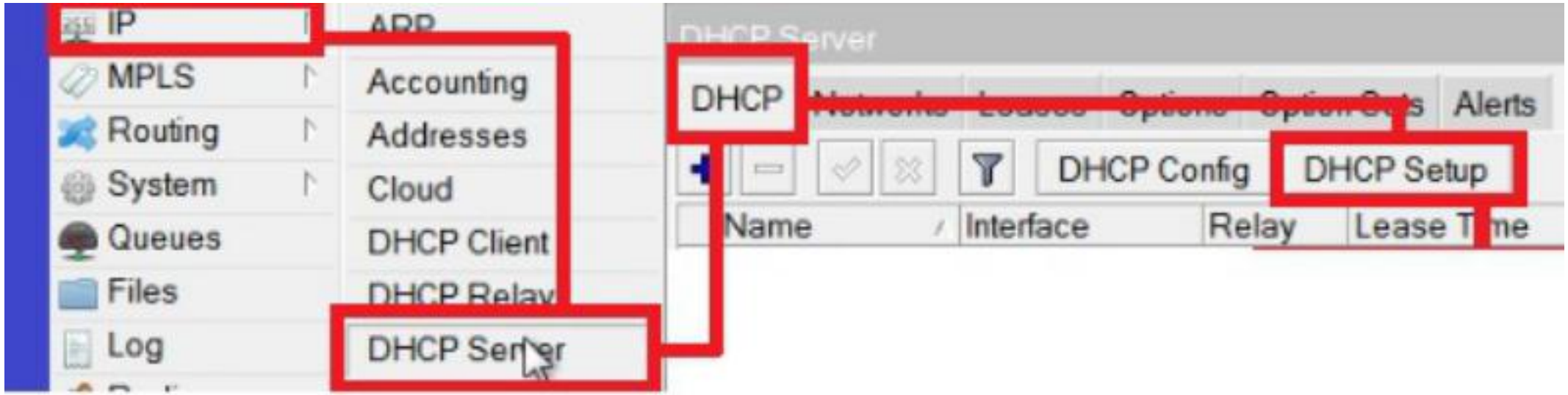
DHCP Server

- DHCP atau Dynamic Host Control Protocol berfungsi untuk memberikan IP Address, DNS , Gateway otomatis dari Server kepada Client.
- Pada MikroTik sendiri, kita dapat membuat router menjadi DHCP Server untuk para Client, dan bisa juga Router MikroTik menjadi DHCP Client dan meminta IP , DNS , Gateway dari ISP atau dari router lain yang terhubung melalui jaringan Ethernet atau pun Wireless.

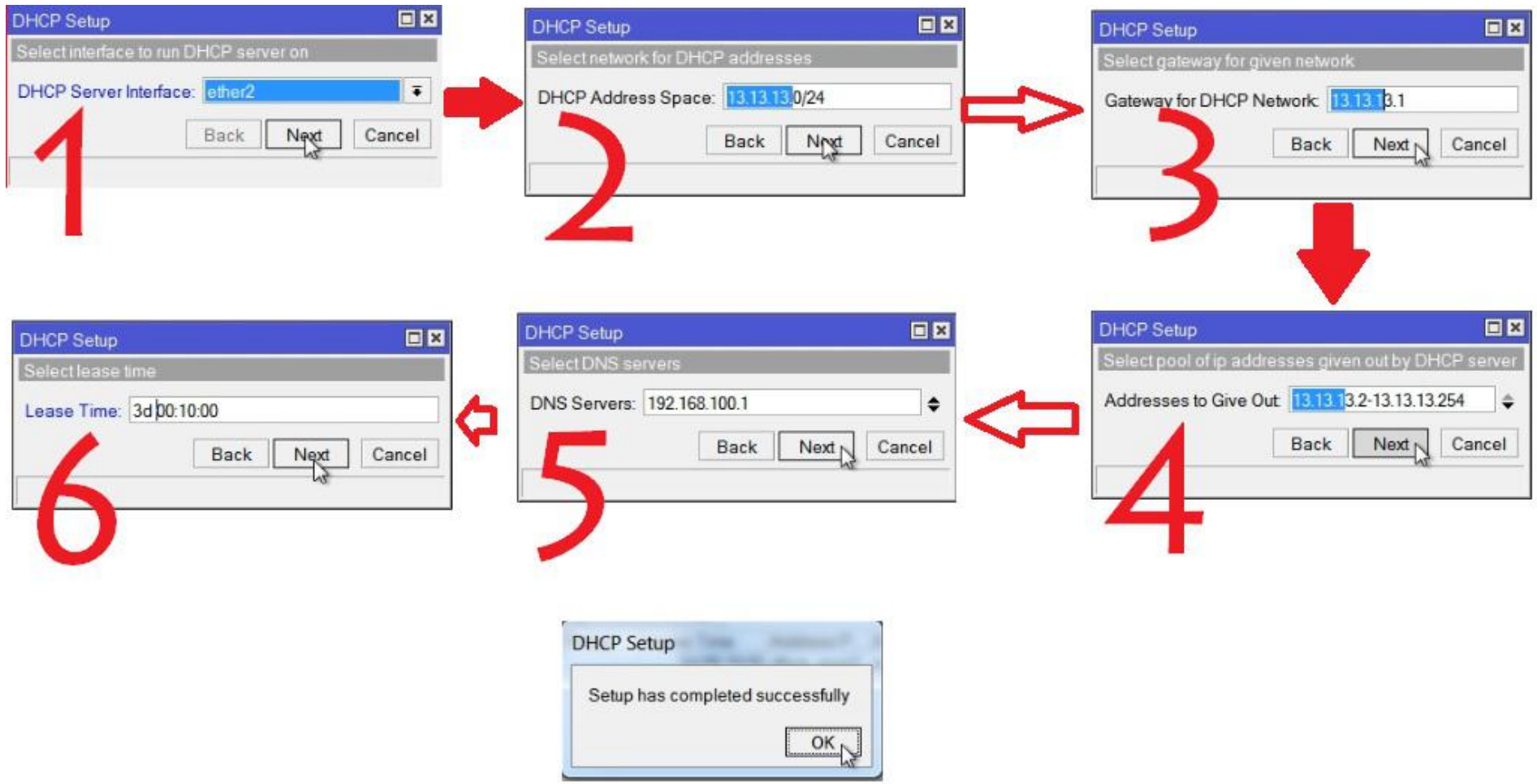


DHCP Server biasanya digunakan untuk ke client yang lebih dari 10 PC

(LAB)DHCP Server



(LAB)DHCP Server



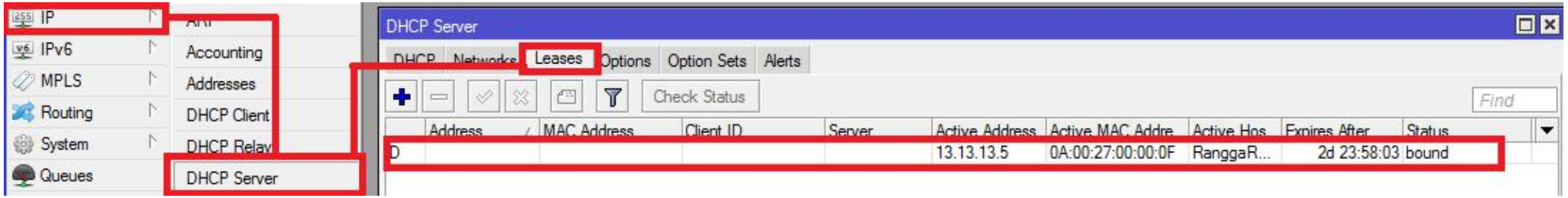
Terminal DHCP Server Wizard

```
[admin@Rangga] > ip dhcp-server setup
Select interface to run DHCP server on

dhcp server interface: ether2
Select network for DHCP addresses

dhcp address space: 13.13.13.0/24
Select gateway for given network

gateway for dhcp network: 13.13.13.1
Select pool of ip addresses given out by DHCP server

addresses to give out: 13.13.13.2-13.13.13.5
Select DNS servers

dns servers: 192.168.100.1
Select lease time
```

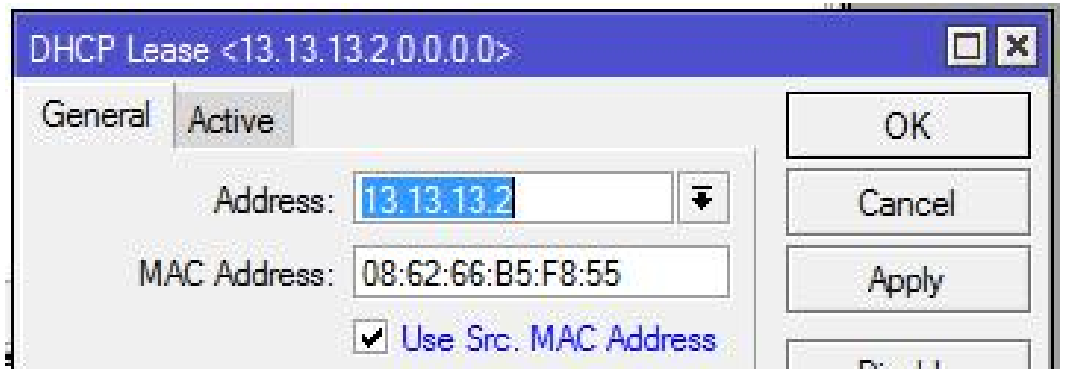
DHCP Server Test

- Ubahlah konfigurasi IP Address dan DNS pada laptop client menjadi otomatis
- Cek pada laptop apkah sudah mendapatkan alokasi IP Address dari DHCP
  - **C:\ipconfig** lalu tekan **enter**
- Cobalah melakukan koneksi ke Internet

DHCP Management

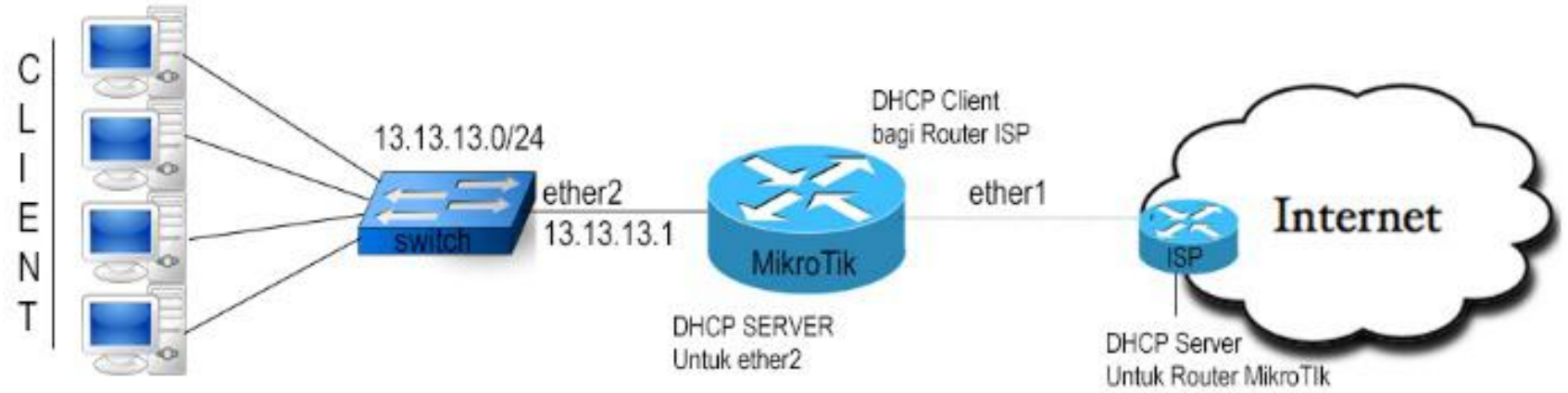


- Daftar DHCP yang aktif terlihat pada menu **DHCP Server > Leasses**
- Untuk membuat IP Address tertentu hanya digunakan oleh Mac Address tertentu, bisa menggunakan **DHCP-Static**

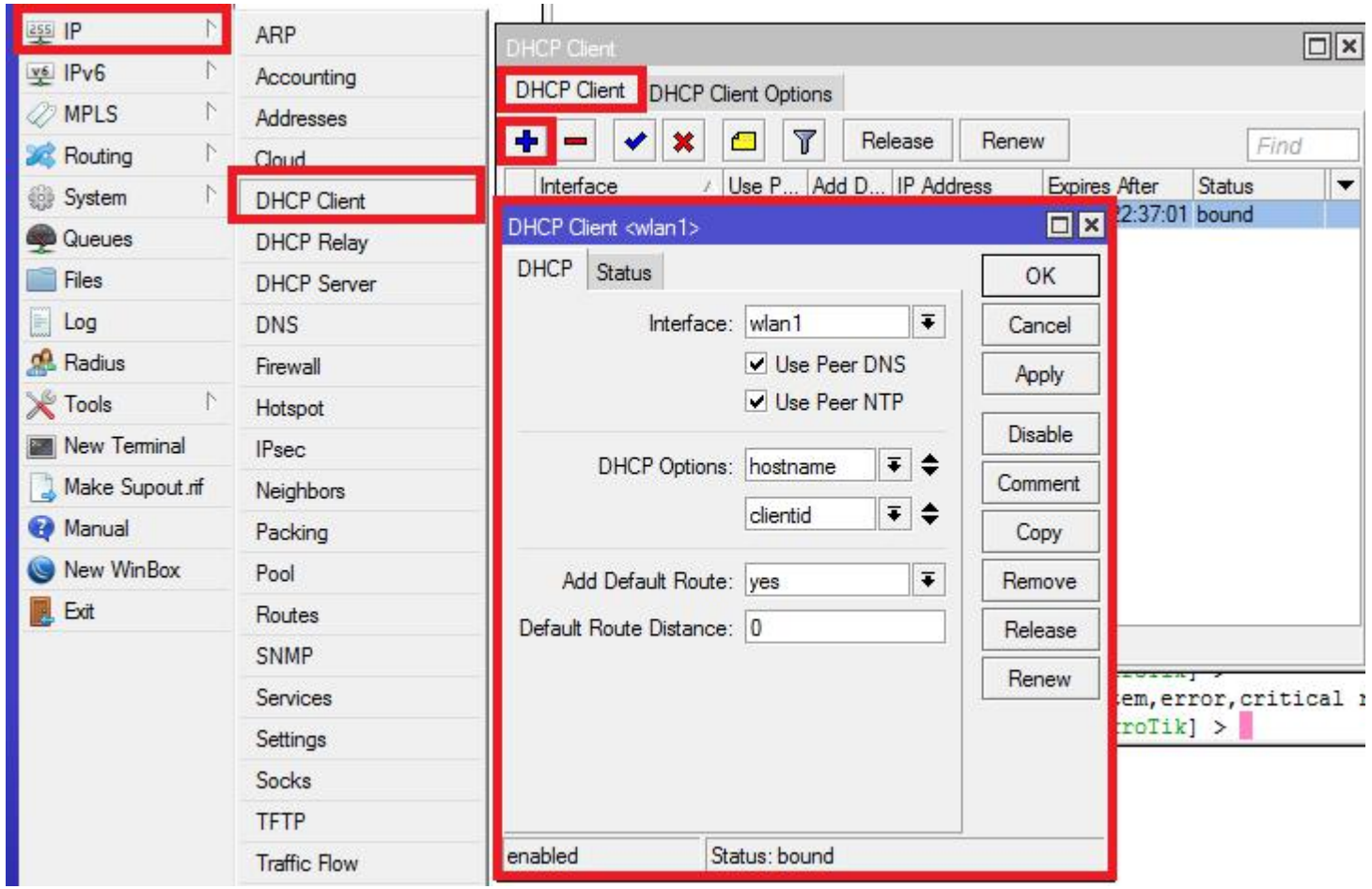


DHCP Client

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



(LAB)DHCP Client

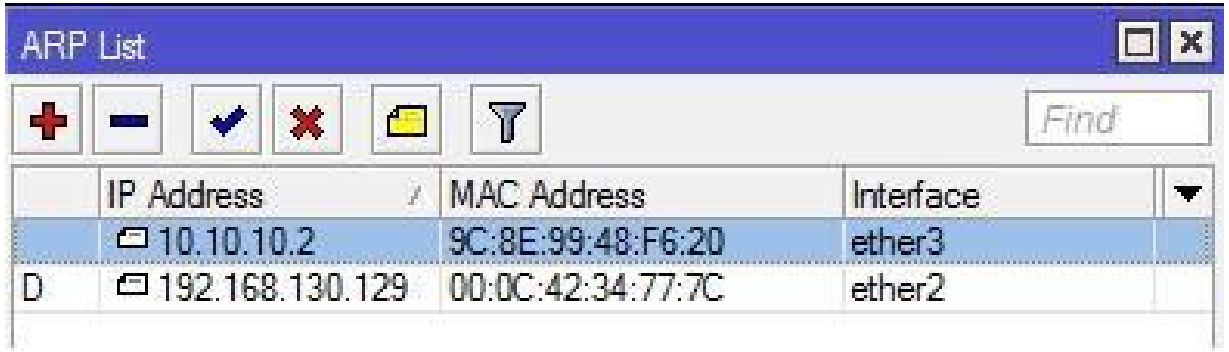


DHCP Client

- **Interface**
  - Pilihlah interface sesuai yang terkoneksi ke DHCP Server
- **Hostname (**tidak harus diisi**)**
  - Nama DHCP ciient yang akan dikenali oleh DHCP Server
- **Client ID (**tidak harus diisi**)**
  - Biasanya merupakan mac-address interface yang kita gunakan, apabila proses DHCP di server menggunakan sistem radius
- **Add default route**
  - Bila kita menginginkan default route kita mengarah sesuai dengan informasi DHCP
- **Use Peer DNS**
  - Bila kita hendak menggunakan DNS server sesuai dengan informasi DHCP
- **Use Peer NTP**
  - Bila kita hendak menggunakan informasi pengaturan waktu di router(NTP) sesuai dengan informasi dari DHCP
- **Default route distance**
  - Menentukan prioritas routing jika terdapat lebih dari satu DHCP Server yang digunakan. Routing akan melakukan distance yang lebih kecil

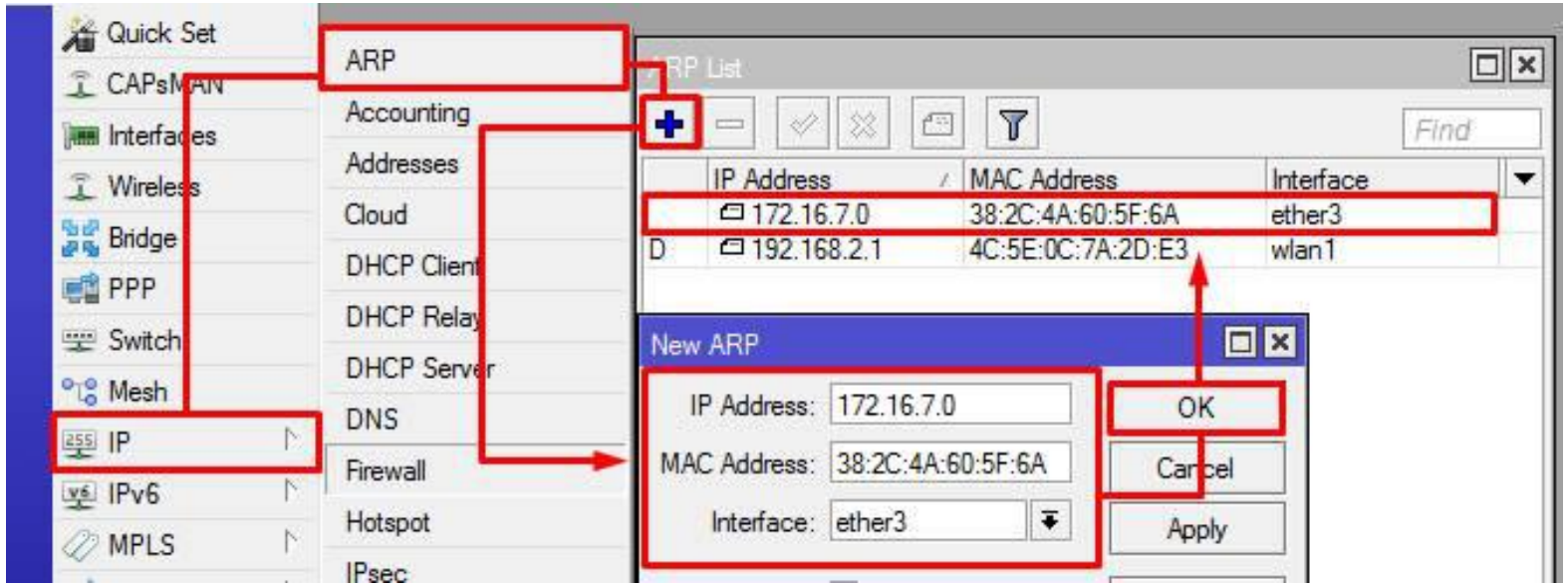
ARP Table

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



Address Resolution Protocol

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

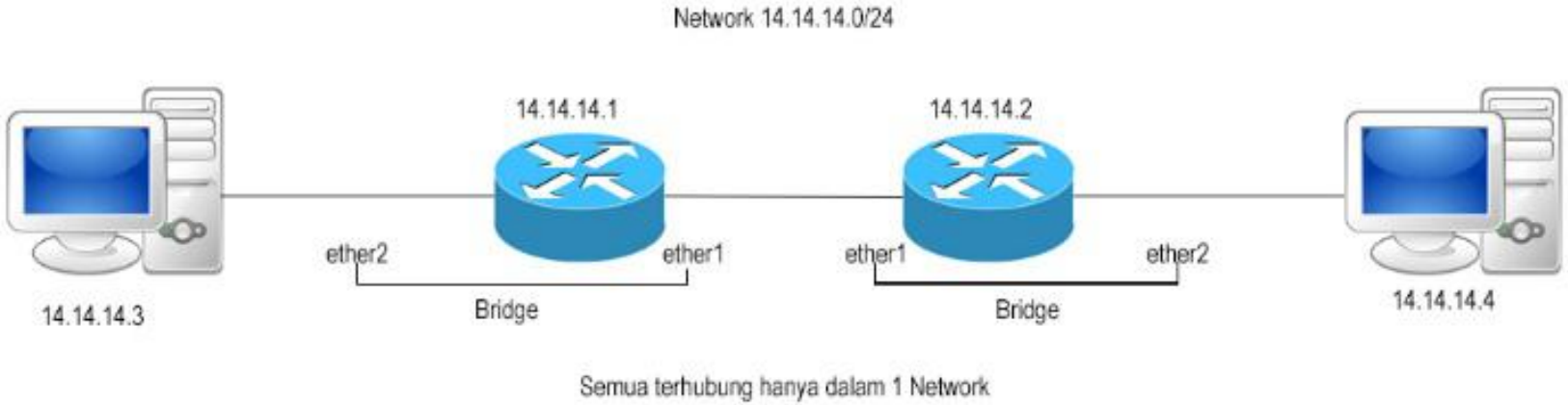


Bridge Concept

- Menggabungkan **dua atau lebih interface** yang bertipe ethernet, atau sejenisnya, seolah-olah berada dalam **satu segmen network yang sama**
- Proses penggabungan ini terjadi pada layer data-link
- Mengaktifkan bridge pada dua buah interface akan menonaktifkan fungsi routing di antara kedua interface tersebut
- Mengemulasi mode **switch** secara software pada dua atau lebih interface

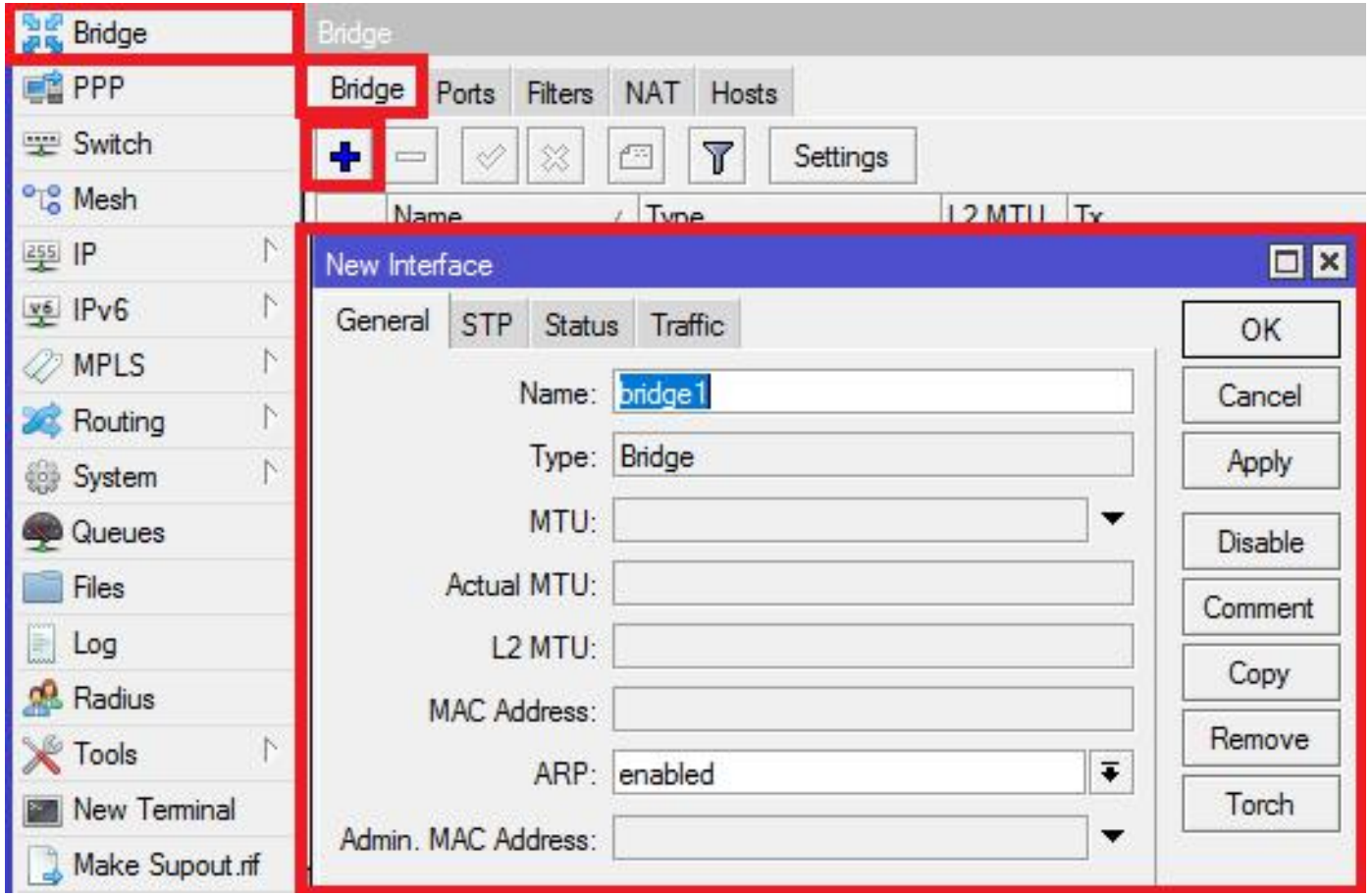
(LAB)Bridging

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



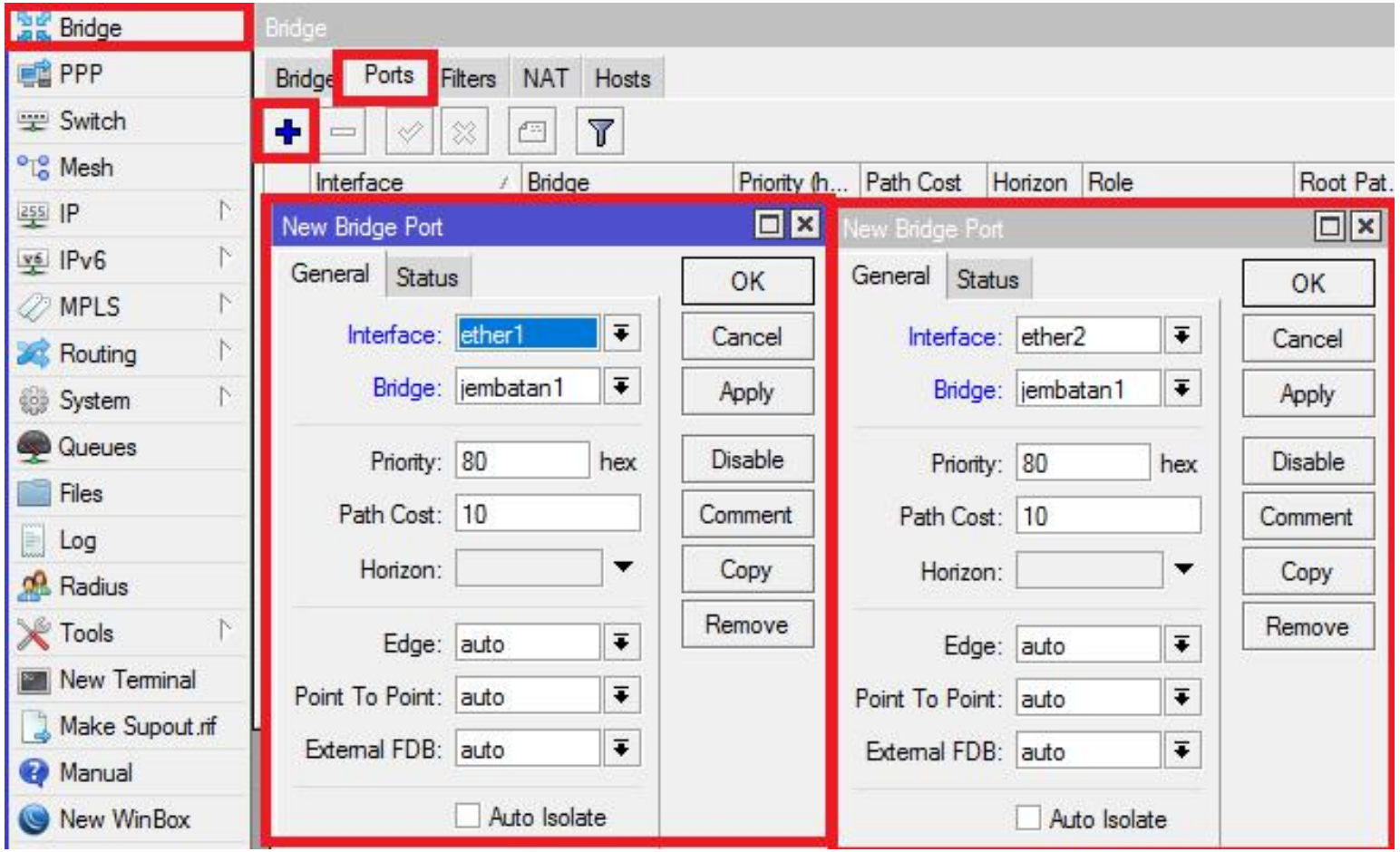
(LAB)Create Bridge

- Membuat Interface bridge



(LAB)Bridge Port

- Memasukkan interface ethernet ke interface bridge



(LAB)Bridge CLI

- Membuat Bridge

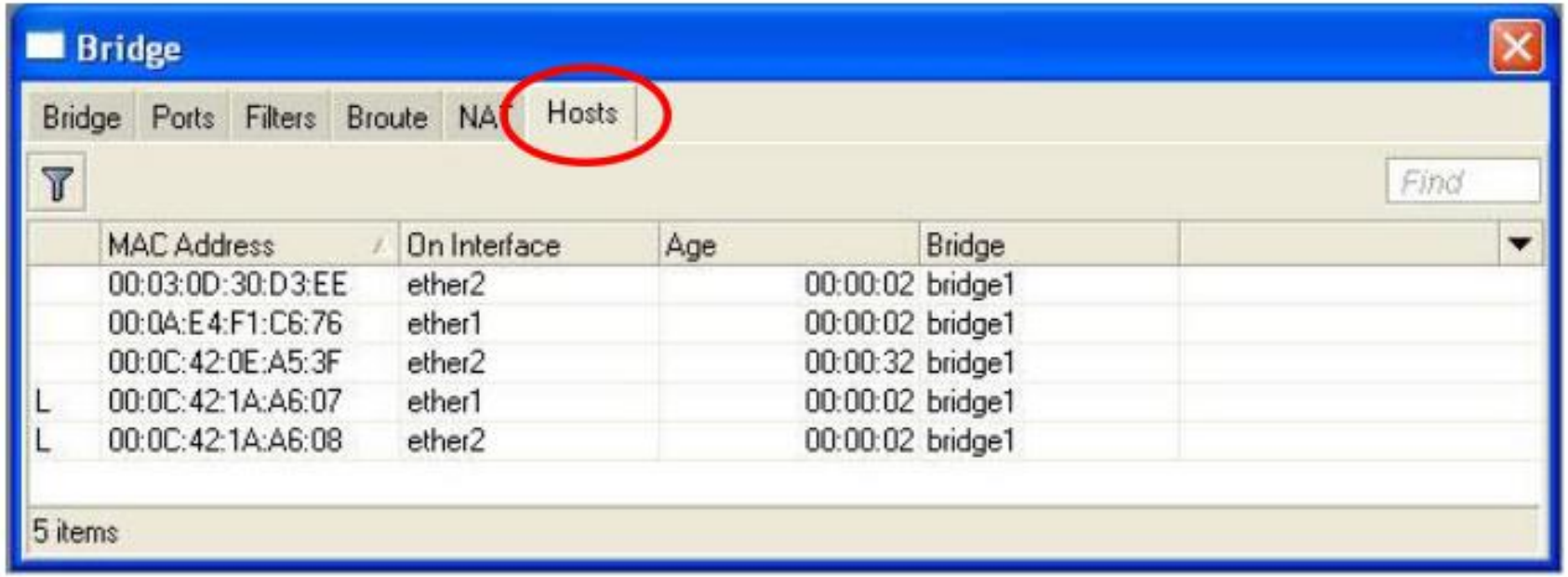
```
[admin@Mikrotik1] > interface bridge add name=jembatan1
[admin@Mikrotik1] > interface bridge print
Flags: X - disabled, R - running
 0  R name="jembatan1" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled mac-address=00:00:00:00:00:00
      protocol-mode=rstp priority=0x8000 auto-mac=yes admin-mac=00:00:00:00:00:00 max-message-age=20s
      forward-delay=15s transmit-hold-count=6 ageing-time=5m
```

- Menambahkan Bridge Port

```
[admin@Mikrotik1] > interface bridge port add interface=ether1 bridge=jembatan1
[admin@Mikrotik1] > interface bridge port add interface=ether2 bridge=jembatan1
[admin@Mikrotik1] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic
 #    INTERFACE                                BRIDGE                                   PRIORITY  PATH-COST    HORIZON
 0    ether1                                   jembatan1                                    0x80         10       none
 1    ether2                                   jembatan1                                    0x80         10       none
```

Bridge Monitoring

- Untuk melihat MAC Address host yang terkoneksi dengan bridge tersebut

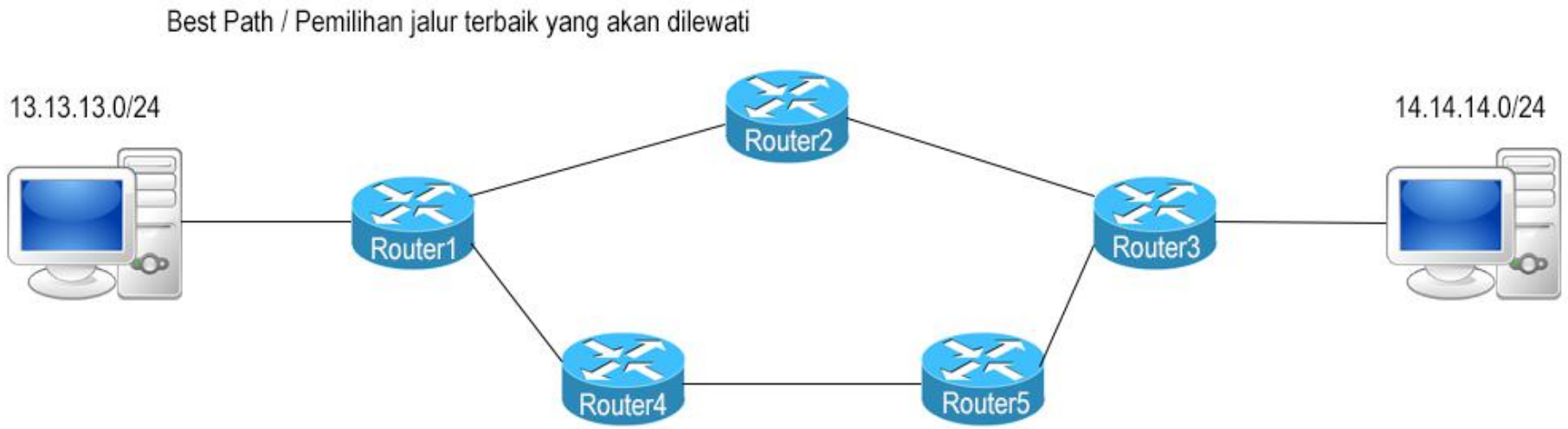


Routed Network

- **Routing** artinya menentukan jalur yang akan dilewati oleh sebuah traffic
- Bekerja pada OSI Layer 3 (Network)
- Untuk menghubungkan network yang berbeda segment (subnet) memerlukan sebuah perangkat yang mampu melakukan proses routing yang disebut dengan Rrouter

Routing Example

- Routerboard yang berfungsi sebagai router akan menjembatani komunikasi antar network yang berbeda, atau bisa juga berfungsi sebagai pemilihan jalur terbaik untuk mencapai suatu network tujuan



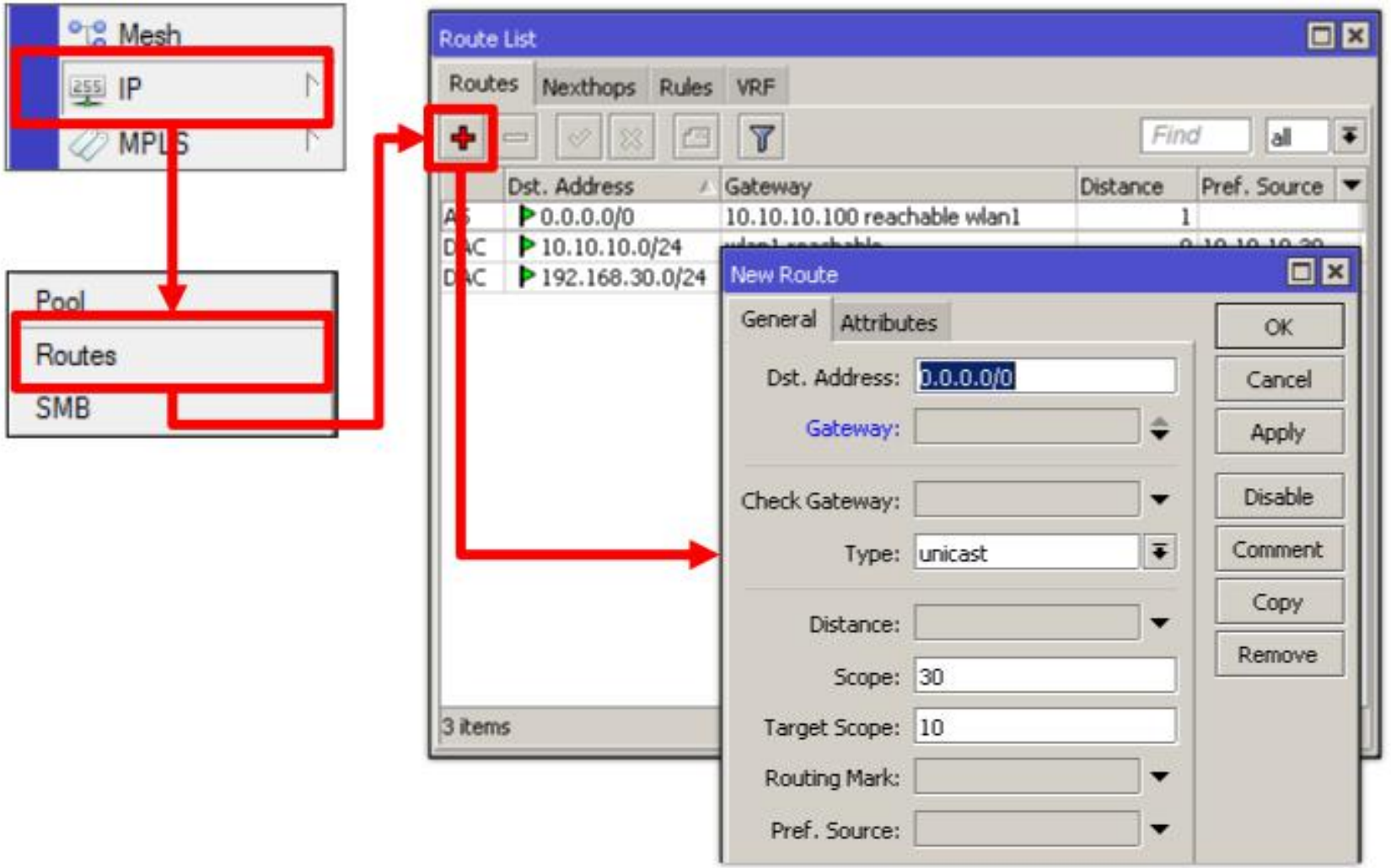
Keuntungan Routing

- Memungkinkan kita melakukan pemantauan dan pengelolaan jaringan yang lebih baik
- Lebih aman (firewall filtering lebih mudah)
- Traffik broadcast(virus) hanya terkonsentrasi di local network seggmen yang sama
- Untuk network skala besar, Routing bisa diimplementasikan menggunakan Dynamic Routing Protocol (RIP/OSPF/BGP)

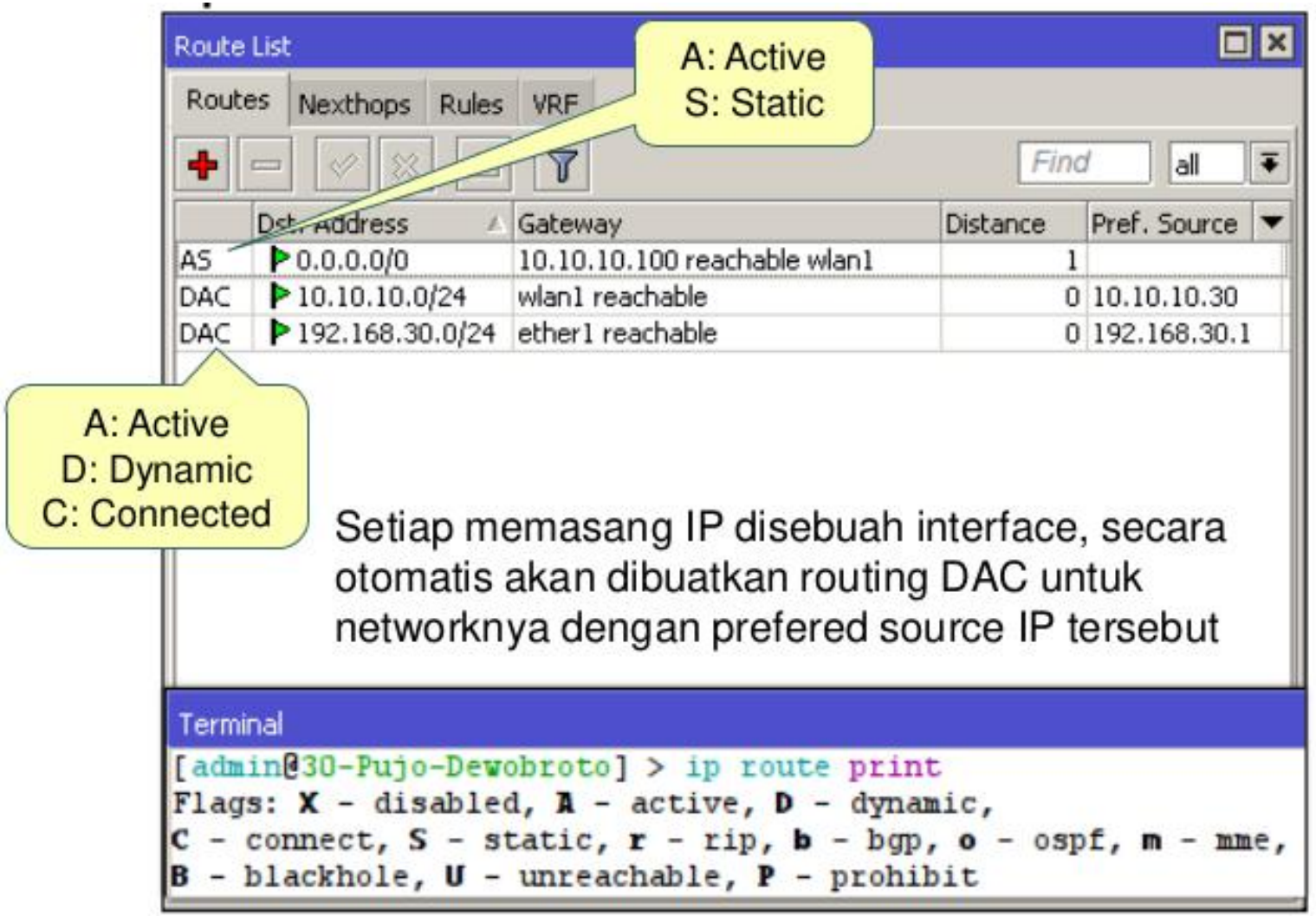
Tipe Informasi Routing

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

Menambahkan Routing



Status Routing

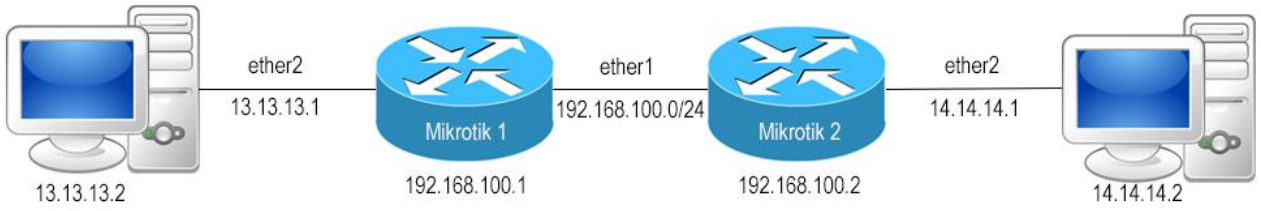


Parameter Dasar Routing

- Destination
  - Destination address : 222.162.115.10
  - Network mask : 202.134.1.0/24
  - 0.0.0.0/0 : ke semua network
- Gateway
  - IP Address gateway, harus merupakan IP Address yang satu subnet dengan IP yang terpasang pada salah satu interface
- Gateway Interface
  - Digunakan apabila IP gateway tidak diketahui dan bersifat dinamik (biasanya digunakan di **ppp** interface)
- Pref Source
  - source IP address dari paket yang akan meninggalkan router
- Distance
  - Beban untuk kalkulasi pemilihan routing

Konsep Dasar Routing

- IP Address Gateway harus merupakan IP Address dari router lawannya yang subnetnya sama dengan salah satu IP Address yang terpasang pada router kita (connect directly)
- Pada interface yang menghubungkan router 1 dan 2, pada masing-masing router terdapat lebih dari 1 buah IP Address
- Default gateway pada router 2 adalah router 1
- IP address yang menjadi default gateway router 2 adalah 192.168.100.1, karena IP Address tersebut berada dalam subnet yang sama dengan salah satu IP Address pada router B (192.168.100.2/24)
- Setting static route default :
  - Dst-address=0.0.0.0/0 gateway192.168.100.1



(LAB)Static Route

- Bisa kita lihat pada gambar topologi point to point diatas, Router 1 dan Router 2 terhubung melalui interface ether1, tetapi mempunyai IP Network yang berbeda. Topologi diatas disebut juga dengan topologi Point to Point Fisik, karena Router 1 dan Router 2 terhubung langsung secara fisik melalui interface ether1. Kenapa IP interface ether1 diatas memiliki IP Network yang berbeda? Apa masih bisa terhubung satu sama lain? Karena topologi diatas adalah point to point, maka pengalamatan IP Address pada interface ether1 tidak terlalu penting.oleh karena itu, Router 1 dan Router 2 pada topologi diatas dapat terhubung meskipun berbeda IP Networknya.

- Untuk melakukan konfigurasi pada topologi diatas, terdapat sedikit perbedaan dalam konfigurasi IP Address interface ether1. Kita akan menambahkan perintah text Network pada konfigurasi IP Address nya dan nantinya parameter network tersebut diisi dengan IP Address router lawan (Router 2). Maka perintah text nya adalah sebagai berikut
- Router 1

Ip address add address=13.13.13.1/32 network=11.11.11.1 interface=ether1

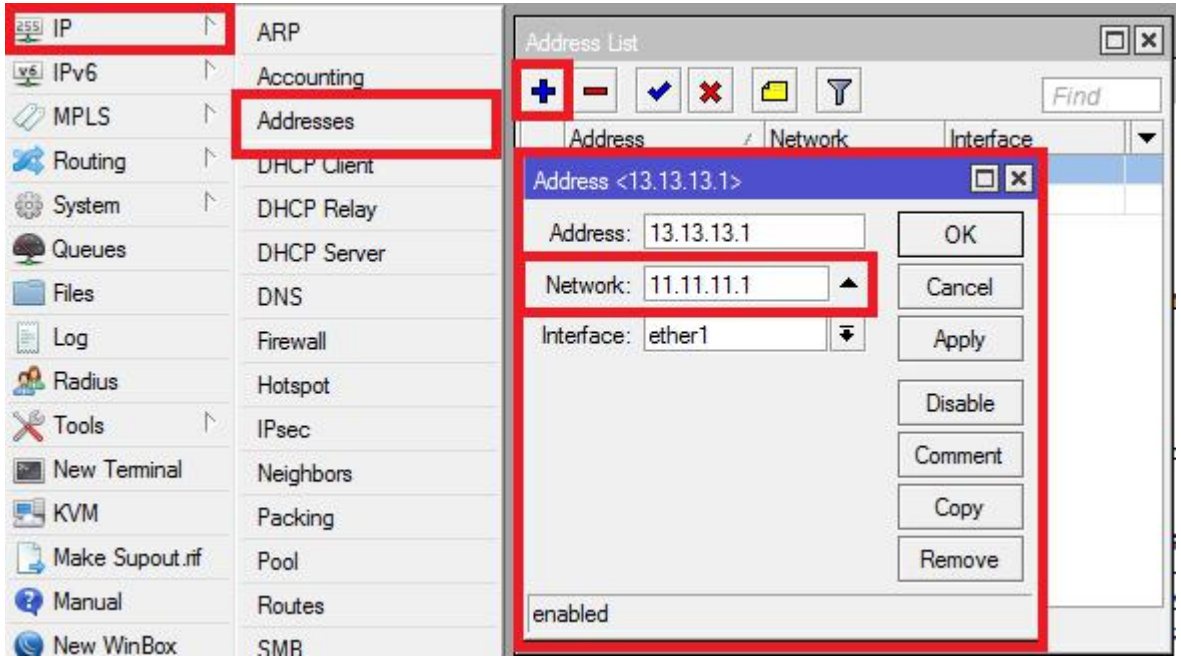
```
[admin@Router1] > ip address add address=13.13.13.1/32 network=11.11.11.1
interface=ether1
[admin@Router1] > ip address pr
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   14.14.14.1/24      14.14.14.0      ether2
 1   13.13.13.1/32      11.11.11.1      ether1
```

- Router 2

Ip address add address=11.11.11.1/32 network=13.13.13.1 interface=ether1

```
[admin@Router2] > ip address add address=11.11.11.1/32 network=13.13.13.1
interface=ether1
[admin@Router2] > ip address pr
Flags: X - disabled, I - invalid, D - dynamic
 #    ADDRESS            NETWORK         INTERFACE
 0    12.12.12.1/24      12.12.12.0      ether2
 1    11.11.11.1/32      13.13.13.1      ether1
```

Jika melalui Winbox (GUI) caranya hampir sama seperti sebelumnya, perbedaan nya kita aka nisi parameter Network nya. Lebih jelasnya bisa lihat gambar dibawah ini



- Setelah kita lakukan konfigurasi IP Address pada Router 1 dan 2, sekarang kita akan melakukan konfigurasi Routing Static nya pada Router 1 dan 2. Perintah text nya adalah sebagai berikut

- Router 1

ip route add dst-address=12.12.12.0/24 gateway=11.11.11.1

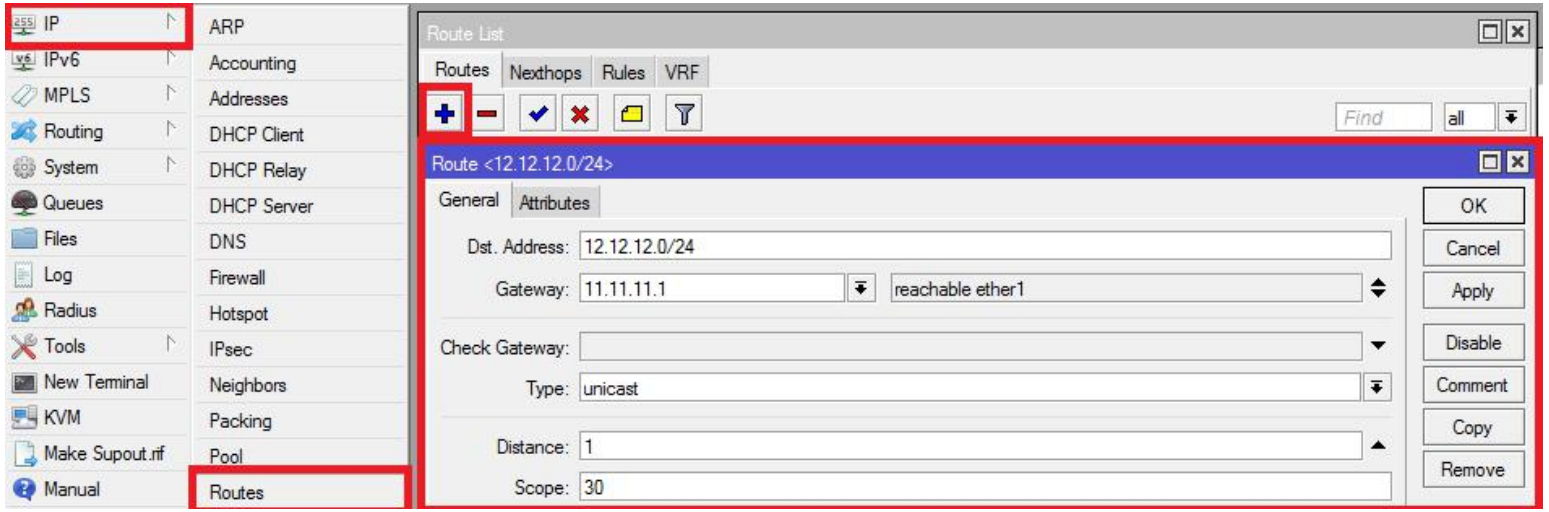
```
[admin@Router1] > ip route add dst-address=12.12.12.0/24 gateway=11.11.11.1
[admin@Router1] > ip route pr
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADC  11.11.11.1/32      13.13.13.1      ether1                    0
 1 A S  12.12.12.0/24                      11.11.11.1                1
 2 ADC  14.14.14.0/24      14.14.14.1      ether2                    0
```

Router 2

ip route add dst-address=14.14.14.0/24 gateway=13.13.13.1

```
[admin@Router2] > ip route add dst-address=14.14.14.0/24 gateway=13.13.13.1
[admin@Router2] > ip route pr
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADC  12.12.12.0/24      12.12.12.1      ether2                    0
 1 ADC  13.13.13.1/32      11.11.11.1      ether1                    0
 2 A S  14.14.14.0/24                      13.13.13.1                1
```

- Jika melalui Winbox (GUI), IP Routes + (add)



- Konfigurasi Routing Static topologi Point to Point diatas telah selesai. Sekarang, untuk melakukan pengujian, lakukan ping pada PC Client Router 1 menuju Client Router 2 dan sebaliknya

```
PC1> ping 12.12.12.2
84 bytes from 12.12.12.2 icmp_seq=1 ttl=62 time=2.001 ms
84 bytes from 12.12.12.2 icmp_seq=2 ttl=62 time=2.003 ms
84 bytes from 12.12.12.2 icmp_seq=3 ttl=62 time=1.498 ms
84 bytes from 12.12.12.2 icmp_seq=4 ttl=62 time=1.501 ms
```

```
PC2> ping 14.14.14.2
84 bytes from 14.14.14.2 icmp_seq=1 ttl=62 time=2.001 ms
84 bytes from 14.14.14.2 icmp_seq=2 ttl=62 time=1.498 ms
84 bytes from 14.14.14.2 icmp_seq=3 ttl=62 time=1.500 ms
84 bytes from 14.14.14.2 icmp_seq=4 ttl=62 time=1.499 ms
```

Dasar Pemilihan Routing

- Untuk pemilihan routing, router akan memilih berdasarkan :
  - Rule routing yang paling spesifik tujuannya
    - Contoh : destination 192.168.10.1/28 lebih spesifik dibanding 192.168.100.1/25
  - Distance
    - Router akan memilih distance routing protokol nya paling kecil
  - Round robin

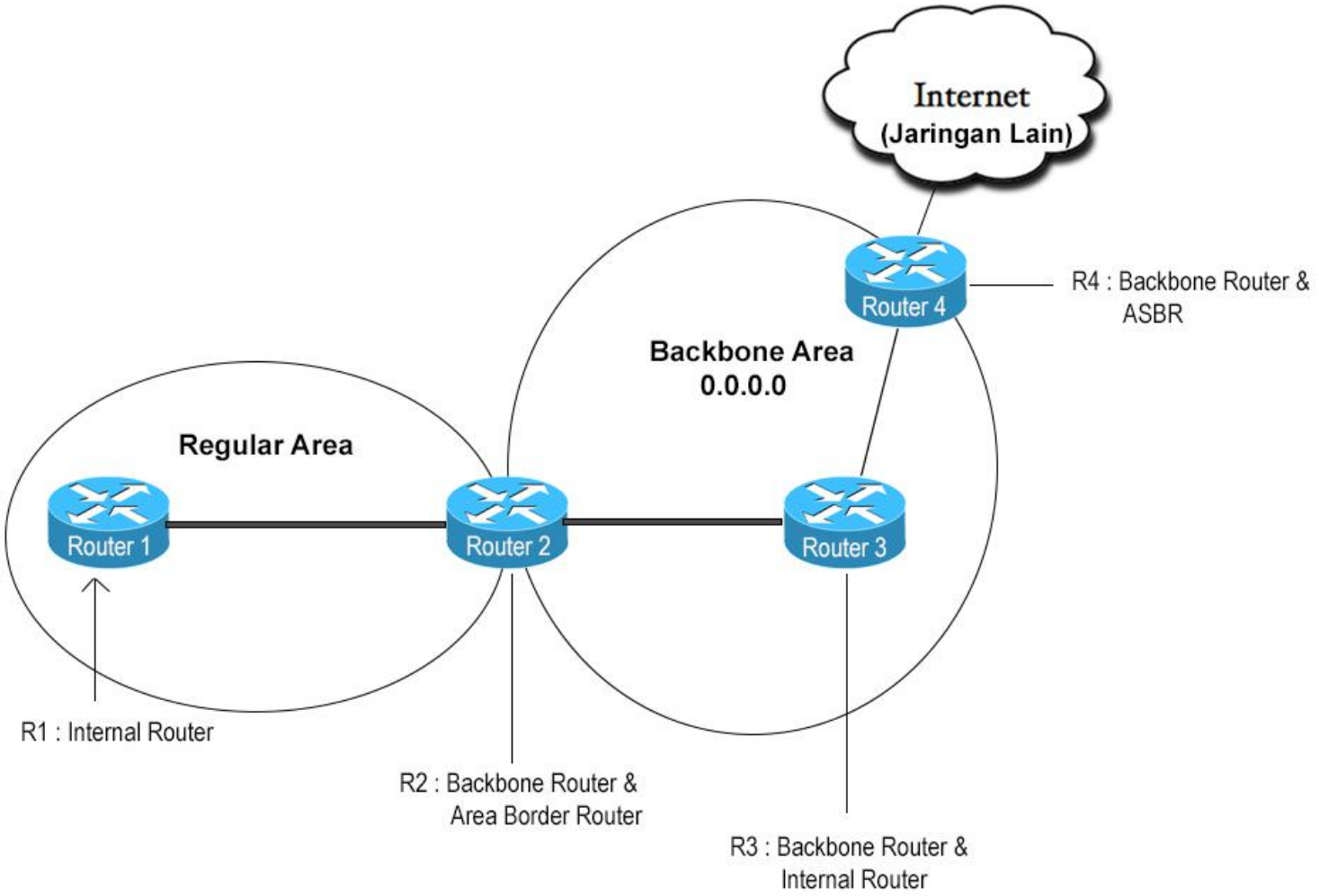
Dynamic Routing

- Karena sebuah jaringan memiliki skala yang berbeda satu sama lain, maka sangat memungkinkan jika jaringan tersebut berkembang menjadi sangat besar. Maka penggunaan routing menjadi sangat penting dan kritis.
- **Informasi routing haruslah tepat** dan kesalahan melakukan distribusi informasi routing harus diminimalisasi sedikit mungkin
- Sangatlah tidak nyaman jika harus menuliskan rule routing untuk puluhan bahkan ratusan router secara static

Dynamic Routing OSPF

- OSPF atau Open Shortest Path First adalah Protocol Routing jenis Link State yang digunakan untuk menghubungkan berbagai Router yang terdapat dalam satu Autonomous System. Autonomous System sendiri seperti yang telah dijelaskan pada sub menu sebelumnya adalah kumpulan beberapa router yang berada dibawah kendali admin dan strategi routing yang sama. Oleh karena itu OSPF masuk kedalam kategori IGP (Interior Gateway Protocol).
- Dalam mengimplementasikan OSPF sendiri, terdapat dua cara, yaitu Single Area OSPF dan Multi Area OSPF. Penggunaan Multi Area OSPF sendiri biasanya digunakan jika jumlah Router lebih dari 50.

Topologi OSPF



- Bisa kita lihat gambar diatas, terdapat 4 Router MikroTik dalam konfigurasi OSPF. Router 1 berperan atau berfungsi menjadi Internal Router pada Regular Area. Router 2 berperan menjadi Backbone Router dan juga berperan sebagai Area Border Router dikarenakan salah satu interface pada router 2 terhubung dengan Backbone Router dan salah satunya terhubung dengan Internal Router. Sedangkan pada Router 4, Router 4 berperan menjadi Backbone Router dan juga ASBR, dikarenakan salah satu interface terhubung dengan jaringan lain, yaitu Internet.

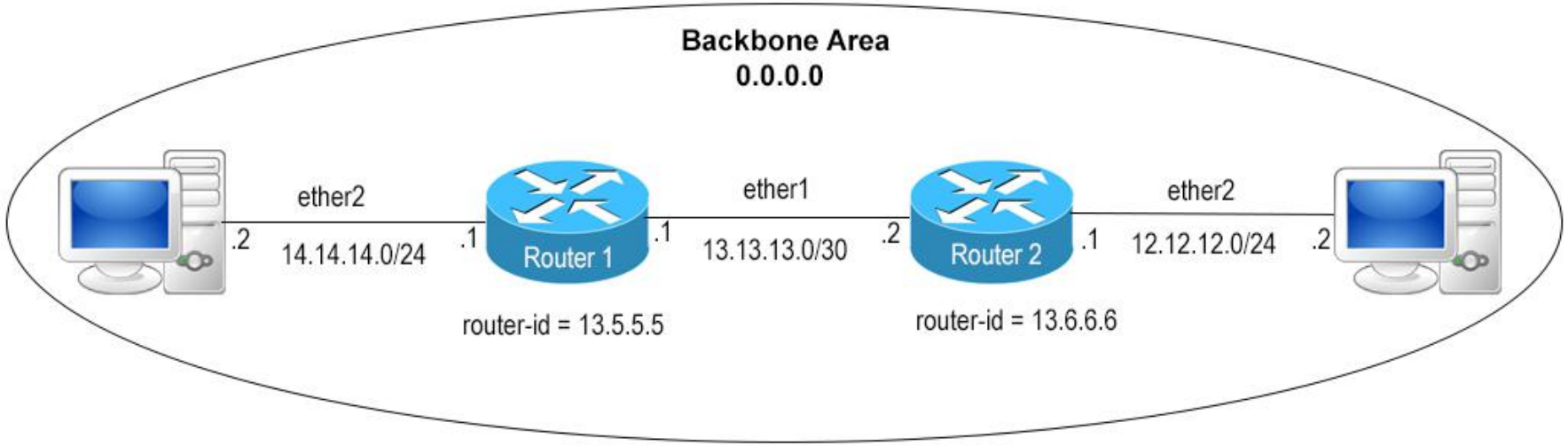
Konfigurasi OSPF

Ada beberapa tahapan untuk melakukan konfigurasi Protocol Routing OSPF pada MikroTik, yaitu

- 1.Mengaktifkan OSPF pada interface Router
- 2.Melakukan konfigurasi identitas Router atau router-id
- 3.Membuat Regular Area jika kita menerapkan konfigurasi Multi Area pada OSPF
- 4.Melakukan Advertise Network
- Oke, sekarang kita langsung saja melakukan konfigurasi OSPF dengan menerapkan Single Area

(LAB)OSPF Single Area

- Kita akan lakukan konfigurasi OSPF single area pada topologi dibawah ini



- Bisa kita lihat pada gambar diatas, Router 1 dan Router 2 terhubung melalui interface ether1 dan masing masing Router mempunyai Client dengan Network 14.14.14.0/24 (R1) dan 12.12.12.0/24 (R2). Karena kita akan melakukan konfigurasi OSPF Single Area, maka kita tidak perlu melakukan konfigurasi regular area, cukup menggunakan Backbone saja. Untuk Backbone Area sendiri telah tersedia secara default oleh MikroTik, jadi kita tidak perlu membuatnya terlebih dahulu. Untuk melihat area yang ada pada router mikrotik, bisa menggunakan perintah text seperti dibawah ini

(LAB)OSPF Single Area

- **routing ospf area print**

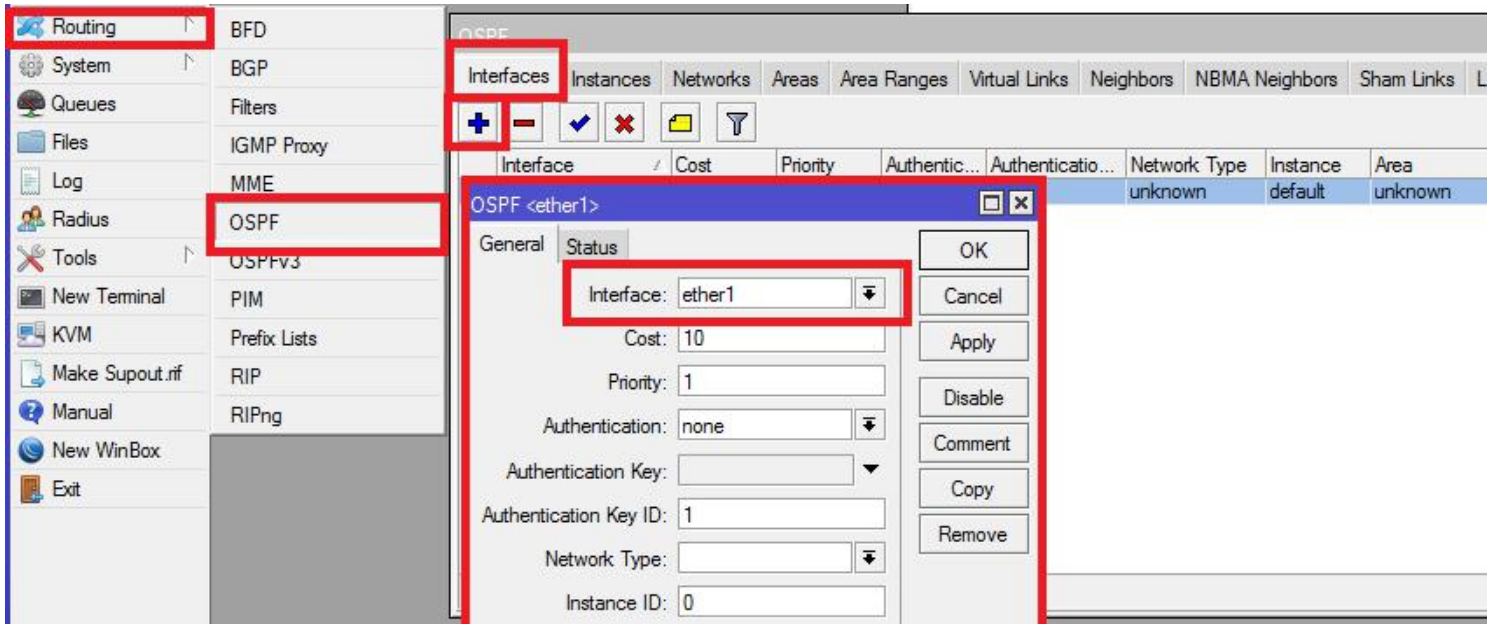
```
[admin@Router1] > routing ospf area print
Flags: X - disabled, I - invalid, * - default
 #    NAME                                AREA-ID         TYPE    DEFAULT-COST
 0  * backbone                            0.0.0.0         default
```

- Sekarang, menuju langkah yang pertama, yaitu mengaktifkan OSPF pada interface Router
- Untuk mengaktifkan Routing Protocol OSPF pada topologi diatas, kita hanya perlu mengaktifkan Routing Protocol OSPF pada interface ether1 terhadap kedua Router, tidak perlu diaktifkan pada ether2 karena PC Client tidak membutuhkan OSPF Packet. Untuk mengaktifkan OSPF, perintah text nya adalah sebagai berikut
- **routing ospf interface add interface=ether1**

```
[admin@Router1] > routing ospf interface add interface=ether1
[admin@Router2] > routing ospf interface add interface=ether1
```

(LAB)OSPF Single Area

- Jika menggunakan Winbox (GUI), klik pada menu Routing OSPF tab Interfaces + (add) lalu konfigurasikan seperti perintah text diatas atau bisa lihat gambar dibawah ini



OSPF Single Area

- Setelah kita mengaktifkan OSPF pada interface ether1, sekarang kita lakukan konfigurasi Router-ID pada kedua Router.
- Sebenarnya, kita bisa saja tidak melakukan konfigurasi Router ID secara manual. Nantinya, Router akan menggunakan IP Address dengan nilai paling besar yang ada pada Interface ether1 yang akan dijadikan Router ID, dalam hal ini jika pada Router 1 maka IP Address 14.14.14.1 akan menjadi Router ID karena nilainya lebih besar daripada 13.13.13.1. Tetapi, sebaiknya kita lakukan konfigurasi Router ID secara manual karena Router ID akan digunakan oleh Router sebagai identitas dari setiap LSA yang dibuat oleh router OSPF.
- Untuk melakukan konfigurasi Router ID melalui perintah text, perintahnya adalah sebagai berikut

(LAB)OSPF Single Area

Router 1

- **routing ospf instance set default router-id=13.5.5.5**

```
[admin@Router1] > routing ospf instance set default router-id=13.5.5.5
[admin@Router1] > routing ospf instance print
Flags: X - disabled, * - default
 0  * name="default" router-id=13.5.5.5 distribute-default=never
      redistribute-connected=no redistribute-static=no redistribute-rip=no
      redistribute-bgp=no redistribute-other-ospf=no metric-default=1
      metric-connected=20 metric-static=20 metric-rip=20 metric-bgp=auto
      metric-other-ospf=auto in-filter=ospf-in out-filter=ospf-out
```

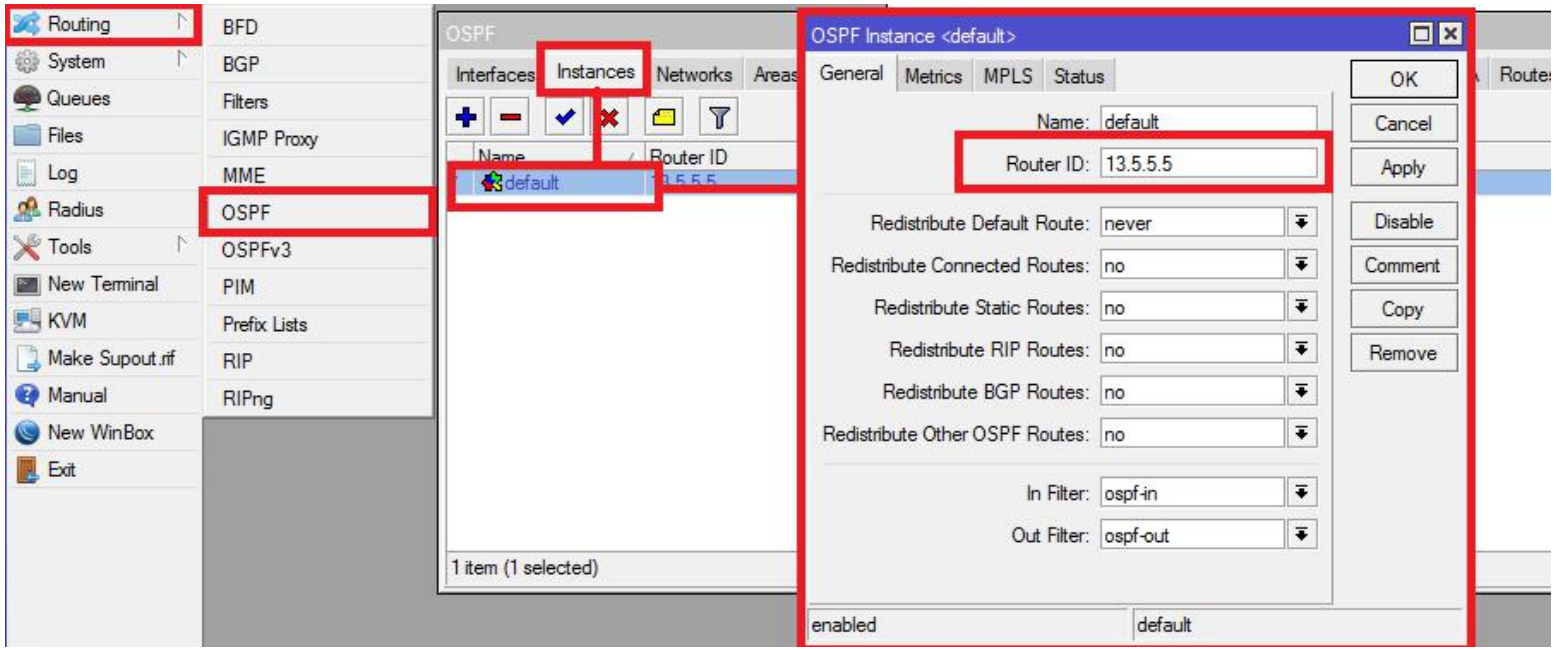
Router 2

- **routing ospf instance set default router-id=13.6.6.6**

```
[admin@Router2] > routing ospf instance set default router-id=13.6.6.6
[admin@Router2] > routing ospf instance print
Flags: X - disabled, * - default
 0  * name="default" router-id=13.6.6.6 distribute-default=never
      redistribute-connected=no redistribute-static=no redistribute-rip=no
      redistribute-bgp=no redistribute-other-ospf=no metric-default=1
      metric-connected=20 metric-static=20 metric-rip=20 metric-bgp=auto
      metric-other-ospf=auto in-filter=ospf-in out-filter=ospf-out
```

(LAB)OSPF Single Area

- Jika melalui Winbox (GUI), klik pada menu Routing OSPF tab Instances double klik pada Default. Lalu lakukan konfigurasi seperti perintah text diatas atau bisa lihat gambar dibawah ini :



Advertise Network OSPF

- Konfigurasi router-id diatas telah selesai. Sekarang, untuk langkah konfigurasi terakhir kita lakukan konfigurasi Advertise Network.
- Maksud dari Advertise Network ini adalah Network yang ingin “diperkenalkan” melalui OSPF. Jika kita lihat pada gambar topologi sebelumnya, setiap Router memiliki 2 Network. Sebagai contoh, Router 1 memiliki Network 13.13.13.0/30 dan Network 14.14.14.0/24 dan begitu juga Router 2 memiliki 2 Network. Oleh karena itu, kita akan melakukan 2 konfigurasi Advertise Network. Karena disini kita menggunakan Single Area, maka kita akan menggunakan Backbone Area pada Advertise Network. Backbone Area sendiri seperti yang sudah dijelaskan sebelumnya telah tersedia secara default pada router MikroTik.
- Untuk melakukan konfigurasi Advertise Network melalui Perintah text (CLI), perintah nya adalah sebagai berikut

(LAB)Advertise Network OSPF

Router 1

- **routing ospf network add network=13.13.13.0/30 area=backbone**
- **routing ospf network add network=14.14.14.0/24 area=backbone**

```
[admin@Router1] > routing ospf network add network=13.13.13.0/30 area=backbone
[admin@Router1] > routing ospf network add network=14.14.14.0/24 area=backbone
[admin@Router1] > routing ospf network pr
Flags: X - disabled, I - invalid
 #   NETWORK            AREA
 0   13.13.13.0/30      backbone
 1   14.14.14.0/24      backbone
```

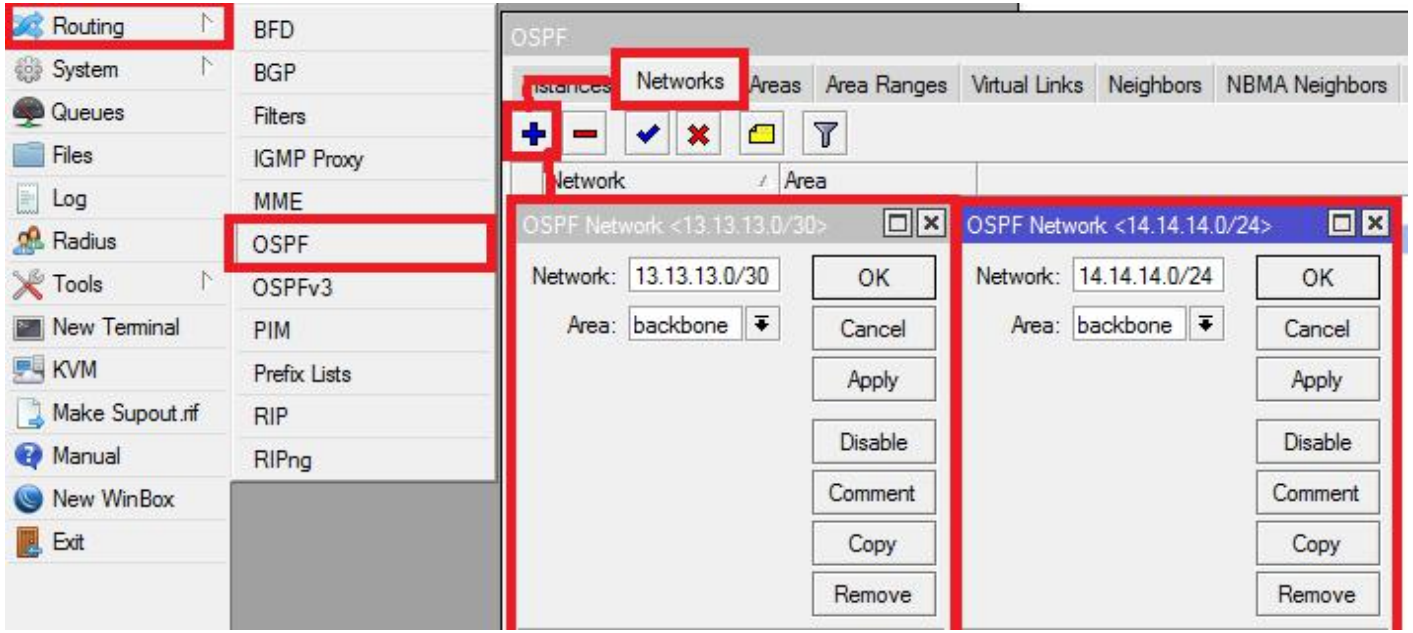
Router 2

- **routing ospf network add network=13.13.13.0/30 area=backbone**
- **routing ospf network add network=12.12.12.0/24 area=backbone**

```
[admin@Router2] > routing ospf network add network=13.13.13.0/30 area=backbone
[admin@Router2] > routing ospf network add network=12.12.12.0/24 area=backbone
[admin@Router2] > routing ospf network print
Flags: X - disabled, I - invalid
 #   NETWORK            AREA
 0   13.13.13.0/30      backbone
 1   12.12.12.0/24      backbone
```

(LAB)Advertise Network OSPF

- Jika melalui Winbox, klik pada menu Routing OSPF tab Networks + (add) lalu lakukan konfigurasi seperti perintah text diatas atau bisa lihat gambar dibawah ini



(LAB)Advertise Network OSPF

- Konfigurasi Advertise Network telah selesai. Maka, seharusnya jaringan-jaringan telah mencapai kondisi convergence dan dapat terhubung satu sama lainnya. Untuk melakukan pengujian, kita bisa lakukan ping antar PC Client Router 1 dan 2

```
PC1> ping 12.12.12.2
84 bytes from 12.12.12.2 icmp_seq=1 ttl=62 time=1.916 ms
84 bytes from 12.12.12.2 icmp_seq=2 ttl=62 time=1.927 ms
84 bytes from 12.12.12.2 icmp_seq=3 ttl=62 time=1.913 ms
84 bytes from 12.12.12.2 icmp_seq=4 ttl=62 time=0.978 ms
84 bytes from 12.12.12.2 icmp_seq=5 ttl=62 time=1.897 ms
```

```
PC2> ping 14.14.14.2
84 bytes from 14.14.14.2 icmp_seq=1 ttl=62 time=0.944 ms
84 bytes from 14.14.14.2 icmp_seq=2 ttl=62 time=0.940 ms
84 bytes from 14.14.14.2 icmp_seq=3 ttl=62 time=1.953 ms
84 bytes from 14.14.14.2 icmp_seq=4 ttl=62 time=1.914 ms
84 bytes from 14.14.14.2 icmp_seq=5 ttl=62 time=1.913 ms
```

- Bisa kita lihat diatas, hasilnya reply yang berarti kedua jaringan telah mencapai kondisi convergence dan saling terhubung satu sama lain
- Konfigurasi OSPF Single Area pada Topologi diatas telah selesai. Sekarang, coba kita lihat table routing pada Router 1, maka akan terlihat seperti dibawah ini

(LAB)OSPF Single Area Test

```
[admin@Router1] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADo  12.12.12.0/24                      13.13.13.2              110
 1 ADC  13.13.13.0/30      13.13.13.1      ether1                    0
 2 ADC  14.14.14.0/24      14.14.14.1      ether2                    0
```

- Bisa kita lihat diatas, pada no index 0 terdapat entry routing dengan symbol ADo, yang berarti Active, Dynamic, OSPF. Sekarang kita lihat table routing pada router 2

```
[admin@Router2] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADC  12.12.12.0/24      12.12.12.1      ether2                    0
 1 ADC  13.13.13.0/30      13.13.13.2      ether1                    0
 2 ADo  14.14.14.0/24                      13.13.13.1              110
```

- Bisa kita lihat juga pada gambar diatas, Router 2 mendapatkan entry routing dynamic dari OSPF untuk menuju network 14.14.14.0/24.
- Kita juga bisa melihat Network yang diketahui oleh Router melalui OSPF. Untuk melihatnya, kita bisa menggunakan perintah text
- **routing ospf route print**

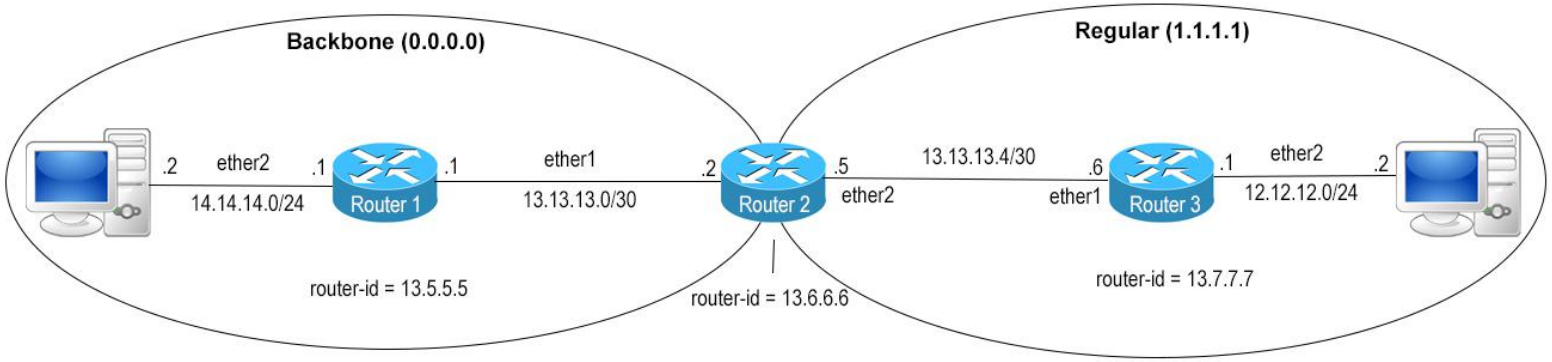
(LAB)OSPF Single Area Test

```
[admin@Router1] > routing ospf route print
 # DST-ADDRESS        STATE          COST        GATEWAY         INTERFACE
 0 12.12.12.0/24      intra-area     20          13.13.13.2      ether1
 1 13.13.13.0/30      intra-area     10          0.0.0.0         ether1
 2 14.14.14.0/24      intra-area     10          0.0.0.0         ether2
```

- Bisa kita lihat pada OSPF route diatas, terdapat network-network yang dikenal router melalui OSPF. Terdapat juga nilai cost dari masing masing entry tersebut, dimana nilai cost untuk menuju network 12.12.12.0/24 adalah 20 karena melewati 2 interface. Bisa kita lihat lagi, terdapat parameter STATE yang berisi intra-area. Maksud dari intra-area tersebut menunjukkan bahwa ketiga Network tersebut berada di area yang sama, yaitu Backbone Area.

OSPF Multi Area

- Setelah sebelumnya kita melakukan konfigurasi Dasar OSPF Single Area, sekarang kita akan lakukan konfigurasi dasar OSPF Multi Area. Konfigurasi nya sendiri hampir sama seperti sebelumnya, hanya saja pada Konfigurasi Multi Area, kita akan menggunakan Backbone Area dan Regular Area. Berbeda dengan Single Area hanya menggunakan Backbone. Kita akan melakukan konfigurasi OSPF Multi Area terhadap topologi dibawah ini



OSPF Multi Area

- Bisa kita lihat pada gambar topologi diatas, terdapat 3 Router MikroTik. Dimana Router 1 berperan menjadi Internal Router pada Backbone Area. Router 2 berperan sebagai ABR atau Area Border Router, dimana router 2 menjadi penghubung antara Backbone Area dan juga Regular Area. Sedangkan Router 3 berperan menjadi internal router pada Regular Area.
- Oke, kita langsung saja menuju langkah konfigurasi nya. Pertama, kita akan mengaktifkan routing protocol OSPF pada interface Router. Untuk langkahnya sendiri hampir sama seperti Single Area, perbedaan nya disini terletak pada Router 2 dimana kita akan mengaktifkan interface ether1 dan ether2 karena pada Router 2 kedua interface tersebut terhubung dengan Router OSPF lain nya.

(LAB)OSPF Multi Area

- Router 1

```
[admin@Router1] > routing ospf interface add interface=ether1
```

- Router 2

```
[admin@Router2] > routing ospf interface add interface=ether1
[admin@Router2] > routing ospf interface add interface=ether2
```

- Router 3

```
[admin@Router3] > routing ospf interface add interface=ether1
```

- Setelah mengaktifkan interface OSPF, sekarang kita akan menambahkan Router ID pada setiap Router. Untuk langkah konfigurasi nya sama seperti pada Single Area.
- Router 1

```
[admin@Router1] > routing ospf instance set default router-id=13.5.5.5
[admin@Router1] > routing ospf instance print
Flags: X - disabled, * - default
 0   * name="default" router-id=13.5.5.5 distribute-default=never
       redistribute-connected=no redistribute-static=no redistribute-rip=no
       redistribute-bgp=no redistribute-other-ospf=no metric-default=1
       metric-connected=20 metric-static=20 metric-rip=20 metric-bgp=auto
       metric-other-ospf=auto in-filter=ospf-in out-filter=ospf-out
```

(LAB)OSPF Multi Area

- Router 2

```
[admin@Router2] > routing ospf instance set default router-id=13.6.6.6
[admin@Router2] > routing ospf instance print
Flags: X - disabled, * - default
 0   * name="default" router-id=13.6.6.6 distribute-default=never
       redistribute-connected=no redistribute-static=no redistribute-rip=no
       redistribute-bgp=no redistribute-other-ospf=no metric-default=1
       metric-connected=20 metric-static=20 metric-rip=20 metric-bgp=auto
       metric-other-ospf=auto in-filter=ospf-in out-filter=ospf-out
```

- Router 3

```
[admin@Router3] > routing ospf instance set default router-id=13.7.7.7
[admin@Router3] > routing ospf instance print
Flags: X - disabled, * - default
 0   * name="default" router-id=13.7.7.7 distribute-default=never
       redistribute-connected=no redistribute-static=no redistribute-rip=no
       redistribute-bgp=no redistribute-other-ospf=no metric-default=1
       metric-connected=20 metric-static=20 metric-rip=20 metric-bgp=auto
       metric-other-ospf=auto in-filter=ospf-in out-filter=ospf-out
```

- Konfigurasi Router ID diatas telah selesai. Sekarang, kita akan melakukan konfigurasi Regular Area pada Router 2 dan Router 3. Pada Router 1 tidak perlu dilakukan konfigurasi Regular Area karena Router 1 berada pada Area Backbone.
- Kita akan lakukan konfigurasi Regular Area pada Router 2 dan 3 dengan area-id=1.1.1.1. Perintah text nya adalah sebagai berikut

(LAB)OSPF Multi Area

Router 2

- **routing ospf area add name=regular area-id=1.1.1.1**

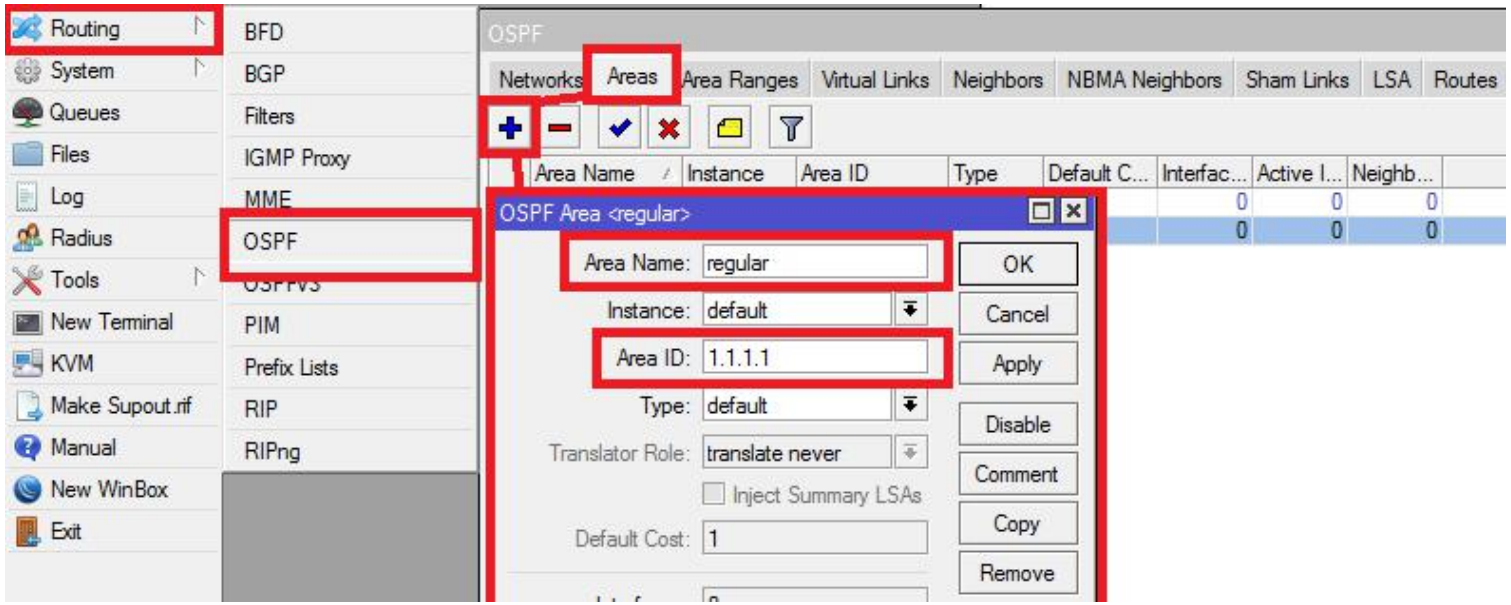
```
[admin@Router2] > routing ospf area add name=regular area-id=1.1.1.1
[admin@Router2] > routing ospf area print
Flags: X - disabled, I - invalid, * - default
 #    NAME                                AREA-ID         TYPE     DEFAULT-COST
 0  * backbone                            0.0.0.0         default
 1    regular                             1.1.1.1         default
```

- Router 3 (perintah text nya sama)

```
[admin@Router3] > routing ospf area add name=regular area-id=1.1.1.1
[admin@Router3] > routing ospf area print
Flags: X - disabled, I - invalid, * - default
 #    NAME                                AREA-ID         TYPE     DEFAULT-COST
 0  * backbone                            0.0.0.0         default
 1    regular                             1.1.1.1         default
```

- Jika melalui WInbox (GUI), klik pada menu Routing OSPF tab Areas + (add) lal lakukan konfigurasi seperti perintah text diatas, atau bisa lihat gambar dibawah ini

(LAB)OSPF Multi Area



- Konfigurasi Regular Area diatas telah selesai. Sekarang barulah kita lakukan konfigurasi Advertise Network

(LAB)OSPF Multi Area Advertise

- Konfigurasi Advertise Network pada Multi Area hampir sama pada Single Area. Dalam melakukan konfigurasi Advertise Network kita harus memperhatikan parameter area pada setiap Network nya. Kita langsung saja menuju langkah konfigurasi

Router 1

- Pada Router 1, kedua Network berada pada Area Backbone. Jadi, pada parameter area kedua Network kita isi dengan perintah text **area=backbone**

```
[admin@Router1] > routing ospf network add network=13.13.13.0/30 area=backbone
[admin@Router1] > routing ospf network add network=14.14.14.0/24 area=backbone
[admin@Router1] > routing ospf network print
Flags: X - disabled, I - invalid
 #    NETWORK            AREA
 0    13.13.13.0/30      backbone
 1    14.14.14.0/24      backbone
```

Router 2

- Pada Router 2 sedikit berbeda. Network ether1 (13.13.13.0/24) pada Router 2 masuk kedalam Area Backbone. Sedangkan Network ether2 (13.13.13.4/30) pada Router 2 masuk kedalam Area Regular. Maka perintah text nya adalah sebagai berikut

(LAB)OSPF Multi Area Advertise

```
[admin@Router2] > routing ospf network add network=13.13.13.0/30 area=backbone
[admin@Router2] > routing ospf network add network=13.13.13.4/30 area=regular
[admin@Router2] > routing ospf network print
Flags: X - disabled, I - invalid
 #    NETWORK            AREA
 0    13.13.13.0/30      backbone
 1    13.13.13.4/30      regular
```

Router 3

- Pada Router 3, kedua Network masuk kedalam Area Regular. Perintah text nya adalah sebagai berikut

```
[admin@Router3] > routing ospf network add network=13.13.13.4/30 area=regular
[admin@Router3] > routing ospf network add network=12.12.12.0/24 area=regular
[admin@Router3] > routing ospf network print
Flags: X - disabled, I - invalid
 #    NETWORK            AREA
 0    13.13.13.4/30      regular
 1    12.12.12.0/24      regular
```

- Konfigurasi Advertise Network telah selesai. Sekarang, seharusnya jaringan kita telah mencapai kondisi convergence.
- Konfigurasi OSPF Multi Area diatas telah selesai. Sekarang, kita lakukan pengecekan pada Routing Table dan juga OSPF Route.

(LAB)OSPF Multi Area Test

Router 1

```
[admin@Router1] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADo  12.12.12.0/24                      13.13.13.2              110
 1 ADC  13.13.13.0/30      13.13.13.1      ether1                    0
 2 ADo  13.13.13.4/30                      13.13.13.2              110
 3 ADC  14.14.14.0/24      14.14.14.1      ether2                    0
```

Router 2

```
[admin@Router2] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADo  12.12.12.0/24                      13.13.13.6              110
 1 ADC  13.13.13.0/30      13.13.13.2      ether1                    0
 2 ADC  13.13.13.4/30      13.13.13.5      ether2                    0
 3 ADo  14.14.14.0/24                      13.13.13.1              110
```

Router 3

```
[admin@Router3] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADC  12.12.12.0/24      12.12.12.1      ether2                    0
 1 ADo  13.13.13.0/30                      13.13.13.5              110
 2 ADC  13.13.13.4/30      13.13.13.6      ether1                    0
 3 ADo  14.14.14.0/24                      13.13.13.5              110
```

(LAB)OSPF Multi Area Test

- Bisa kita lihat pada gambar Routing Table diatas, ketiga router mendapatkan entry routing dynamic dari OSPF .

OSPF Route

Router 1

```
[admin@Router1] > routing ospf route print
 # DST-ADDRESS        STATE          COST        GATEWAY         INTERFACE
 0 12.12.12.0/24      inter-area     30          13.13.13.2      ether1
 1 13.13.13.0/30      intra-area     10          0.0.0.0         ether1
 2 13.13.13.4/30      inter-area     20          13.13.13.2      ether1
 3 14.14.14.0/24      intra-area     10          0.0.0.0         ether2
```

Router 2

```
[admin@Router2] > routing ospf route print
 # DST-ADDRESS        STATE          COST        GATEWAY         INTERFACE
 0 12.12.12.0/24      intra-area     20          13.13.13.6      ether2
 1 13.13.13.0/30      intra-area     10          0.0.0.0         ether1
 2 13.13.13.4/30      intra-area     10          0.0.0.0         ether2
 3 14.14.14.0/24      intra-area     20          13.13.13.1      ether1
```

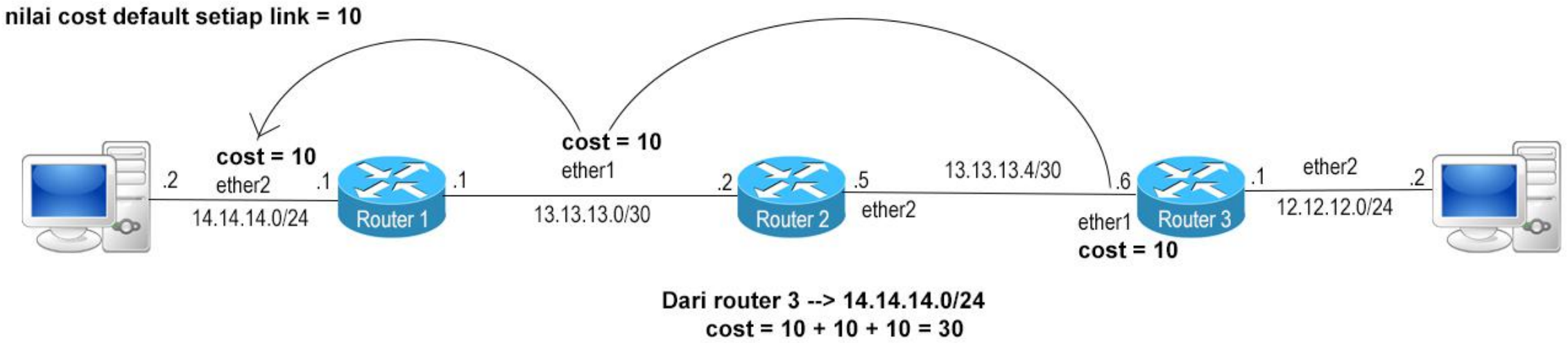
Router 3

```
[admin@Router3] > routing ospf route print
 # DST-ADDRESS        STATE          COST        GATEWAY         INTERFACE
 0 12.12.12.0/24      intra-area     10          0.0.0.0         ether2
 1 13.13.13.0/30      inter-area     20          13.13.13.5      ether1
 2 13.13.13.4/30      intra-area     10          0.0.0.0         ether1
 3 14.14.14.0/24      inter-area     30          13.13.13.5      ether1
```

(LAB)OSPF Multi Area

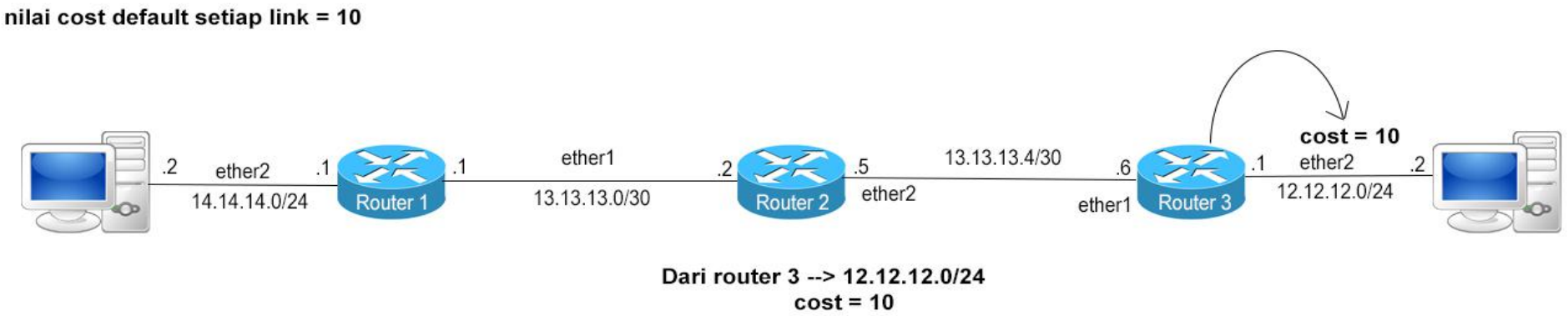
- Jika kita lihat pada table OSPF Route Router 1 pada entry routing nomor 0 dan 2, parameter STATE berisi inter-area sedangkan pada no index 1 dan 3 berisi intra-area. Maksud dari inter-area disini, berarti Network 12.12.12.0/24 dan 13.13.13.4/30 berada pada Area yang berbeda dengan Router 1. Network 12.12.12.0/24 dan 13.13.13.4/30 berada pada Area Regular, sedangkan Router 1 berada pada Area Backbone. Pada nomor 1 dan 3 berisi intra-area, yang berarti Network tersebut berada pada satu Area dengan Router 1.
- Pada Router 2, keempat entry route tersebut parameter STATE berisi intra-area. Kenapa? Karena Router 2 berada pada 2 area sekaligus, yaitu Regular dan Backbone. Oleh karena itu, Router 2 menganggap kedua Area itu adalah Area nya, jadi keempat entry route diatas dianggap berada dalam satu area oleh Router 2
- Pada Router 3, entry routing nomor 0 dan 2 parameter STATE berisi intra-area sedangkan pada nomor 1 dan 3 berisi inter-area. Sekarang kita lihat lagi parameter COST pada tabel OSPF Route pada Router 3. Cost untuk menuju Network 14.14.14.0/24 senilai 30, sedangkan menuju 12.12.12.0/24 hanya mempunyai nilai 10. Kok bisa beda? oke, agar lebih jelas, kita lihat dahulu gambar dibawah ini :

(LAB)OSPF Multi Area



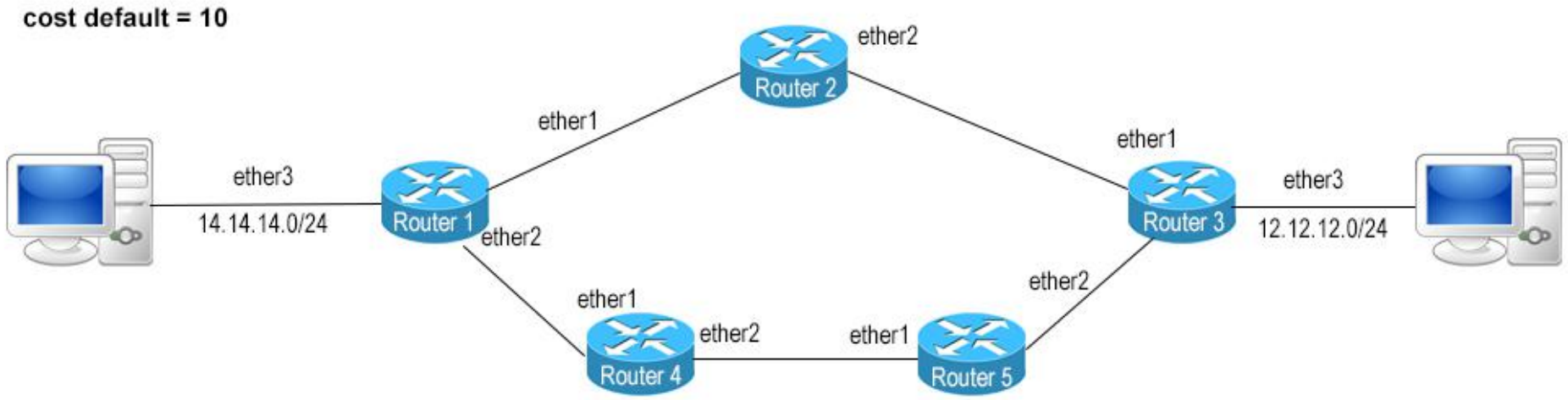
(LAB)OSPF Multi Area

- Bisa kita lihat pada gambar diatas, untuk menuju Network 14.14.14.0/24 dari Router 3, akan melewati beberapa Link, yaitu link ether1 Router 3 ether1 Router 2 ether2 Router 1. Berarti, untuk mencapai Network 14.14.14.0/24, Router 3 akan melewati 3 link, dimana pada setiap Link tersebut mempunyai nilai cost default dari MikroTik, yaitu 10. Karena Router 3 akan melewati 3 Link dan masing masing Link tersebut memiliki nilai cost=10 maka jumlah nilai cost dari Router 3 untuk menuju Network 14.14.14.0/24 adalah 10+10+10 = 30.
- Sedangkan jika Router 3 ingin menuju Network 12.12.12.0/24, maka nilai cost pada entry route akan mempunyai nilai 10 dikarenakan jika Router 3 ingin menuju Network 12.12.12.0/24 hanya melewati 1 link, yaitu ether 2 Router 3.



(LAB)OSPF Multi Area

- Seperti yang kita jelaskan sebelumnya, OSPF akan menggunakan Metric Cost untuk menentukan Best Path. Nilai Cost terkecil akan dianggap sebagai Best Path oleh OSPF. Sebagai contoh, kita lihat gambar dibawah ini :



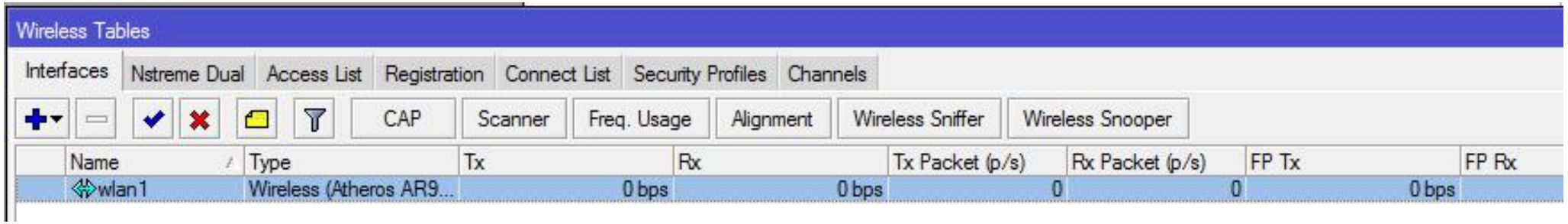
- Bagaimana jika Router 1 ingin menuju Network 12.12.12.0/24? Jalur mana yang akan dipilih?

Wireless LAN

- **Band 2.4Ghz**
  - 802.11 b : Wireless Lan yang menggunakan Frequency 2.4Ghz berkecepatan transfer data **11Mbps**
  - 802.11 b/g : Wireless Lan yang menggunakan Frequency 2.4Ghz berkecepatan transfer data **54Mbps**
  - 802.11 b/g/n : Wireless Lan yang menggunakan Frequency 2.4Ghz berkecepatan transfer data **300Mbps**
- **Band 5Ghz**
  - 802.11 a/g : Wireless Lan yang menggunakan Frequency 5Ghz berkecepatan transfer data **54Mbps**
  - 802.11 a/g/n : Wireless Lan yang menggunakan Frequency 5Ghz berkecepatan transfer data **300Mbps**

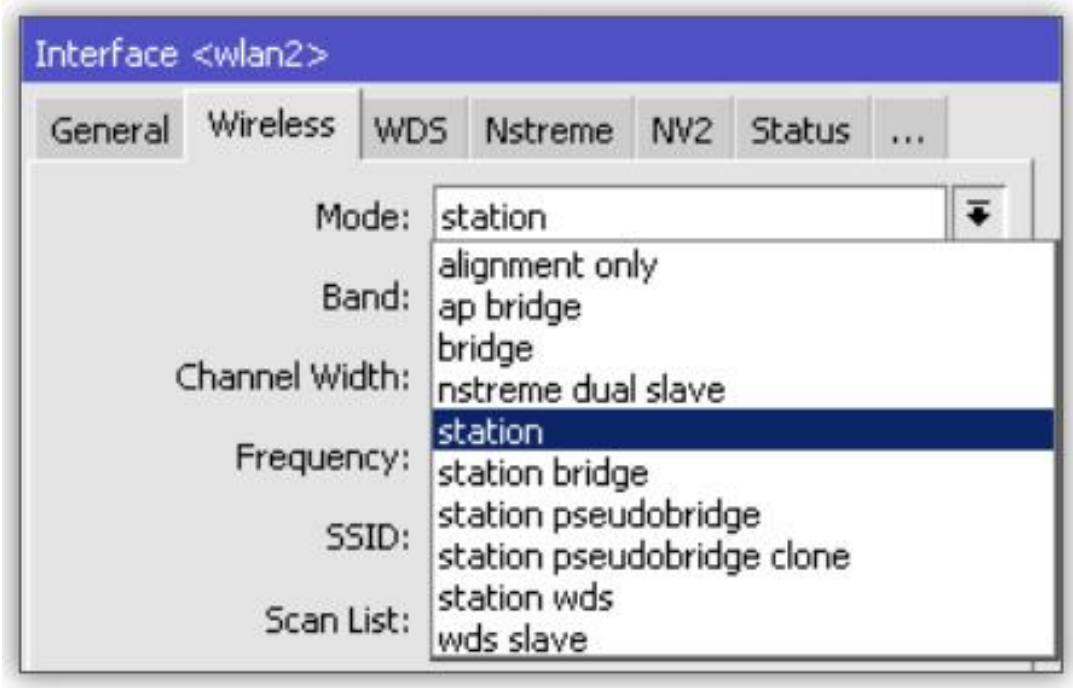
Wireless Menu

- Wireless Menu :
  - **Interface** > Daftar Interface wireless yang terpasang
  - **Access List** > Security MAC Address Client (AP Mode)
  - **Registration** > Daftar Wireless yang terkoneksi
  - **Connect List** > Security MAC Address AP (Station Mode)
  - **Security Profile** > Konfigurasi Wireless Security (WPA/WEP)



Wireless Mode List

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



Wireless Mode

- alignment-only : Digunakan untuk melakukan pointing dengan bantuan "**Beeper**" pada Routerboard.
- ap-bridge : Mode wireless sebagai Access Point untuk topologi **Point-to-Multipoint**
- bridge : Mode wireless sebagai Access Point untuk topologi **Point-to-Point** (hanya bisa menerima satu client)
- nstreme-dualslave : Mode wireless untuk mengaktifkan topologi Nstreme-dual (Wireless Full Duplex)
- station : Mode Wireless sebagai Client untuk topologi **Point-to-Point** dan juga **Point-to-Multipoint**

Wireless Mode

- station-wds : Mode wireless sebagai client tetapi mengaktifkan protocol WDS (Digunakan untuk wireless WDS client)
- wds-slave : Mode wireless sebagai Access Point dan juga mengaktifkan protocol WDS (Digunakan untuk wireless WDS repeater)
- station-pseudobridge : Mode wireless sebagai client yang bisa mengaktifkan bridge pada "**station**" tanpa harus menggunakan protocol WDS
- station-pseudobridge-clone : Mode wireless sama seperti **station-pseudobridge** yang dilengkapi dengan fungsi cloning mac-address dari interface ethernet
- station-bridge : Mode wireless client untuk bridge network sesama perangkat MikroTik

(LAB)Point to Point

AP Side

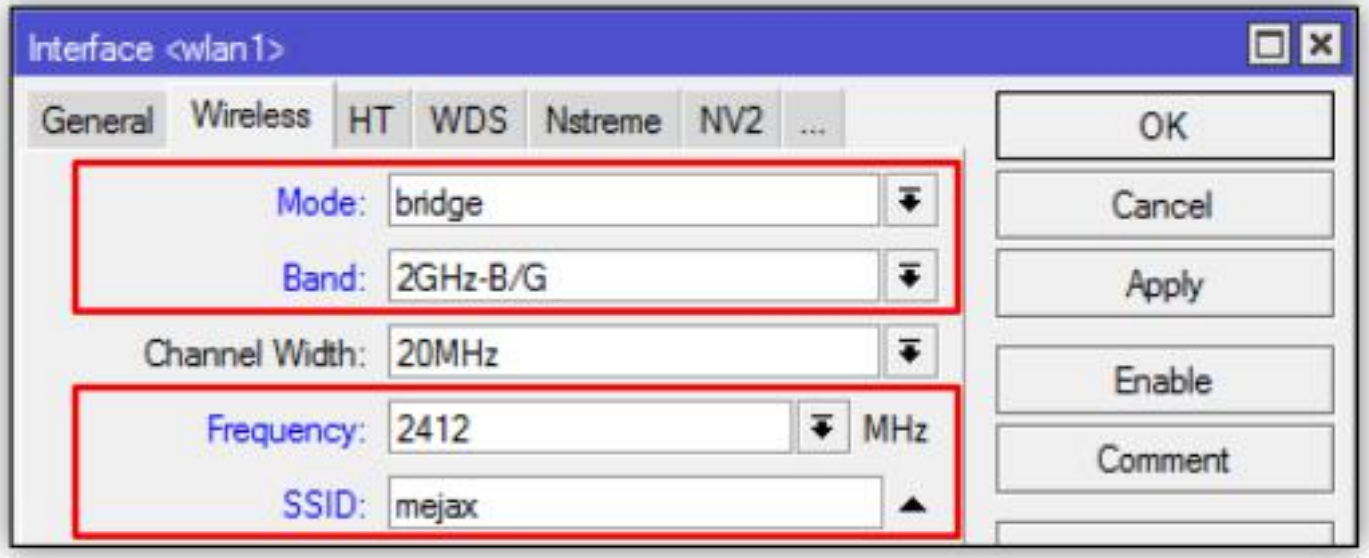
- Mikrotik Minimum Licence Level 3
- Set mode, ssid, band, frequency
- mode=bridge
  - **Hanya menerima 1 station**

Client Side

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

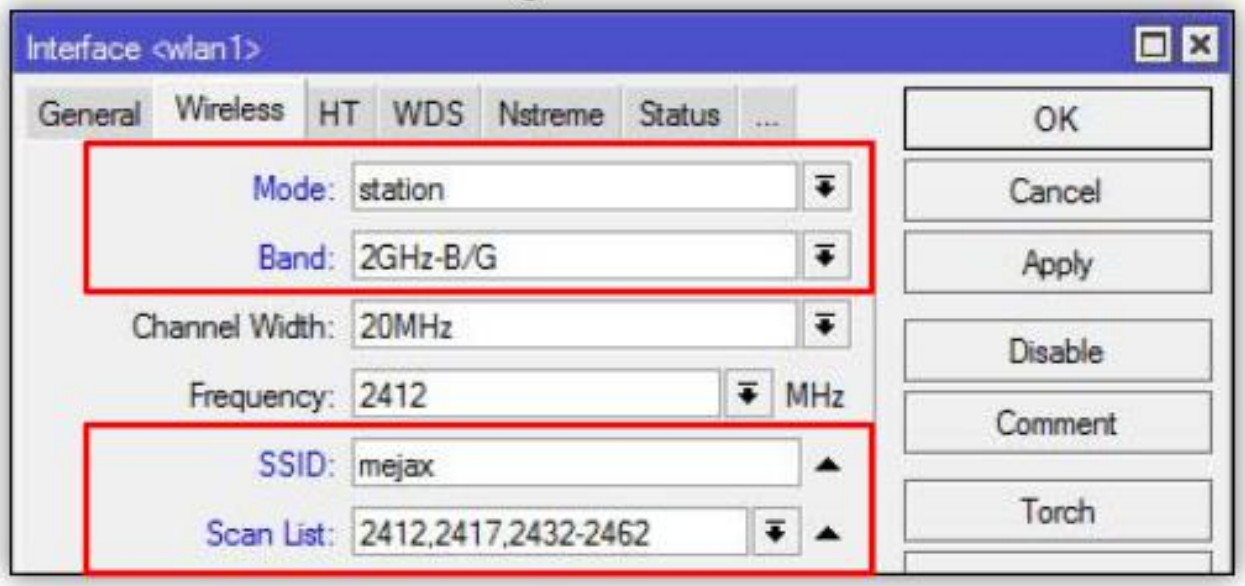
(LAB)Point to Point AP Side

- Konfigurasi :
  - Set **mode, ssid, band,** dan **frequency**
  - mode = **bridge**
    - Hanya bisa terkoneksi dengan satu station (1 client)

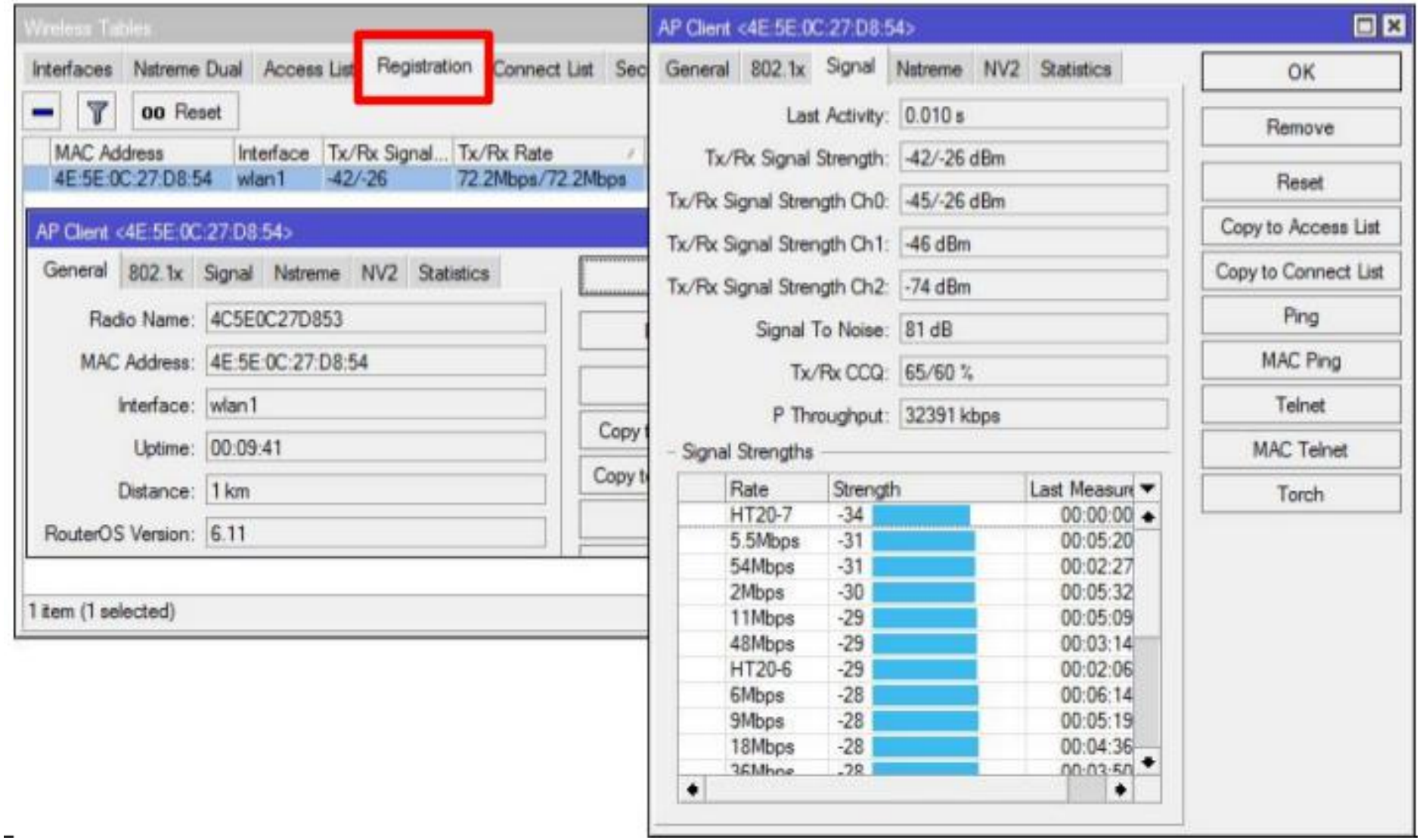


(LAB)Point to Point Client Side

- Konfigurasi :
  - Set **mode, ssid, band,** dan **scan-list**
  - mode **station**
  - Pastikan frequency yang dipilih oleh
  - AP masuk dalam range scan-list



Monitoring Wireless Interface



(LAB)Point to Point Test

- Tambahkan IP Address di interface **Wlan1**
- Test koneksi wireless kedua router dengan tool Ping
- Setelah test ping berhasil maka wireless Point-to-Point sudah selesai

Tips

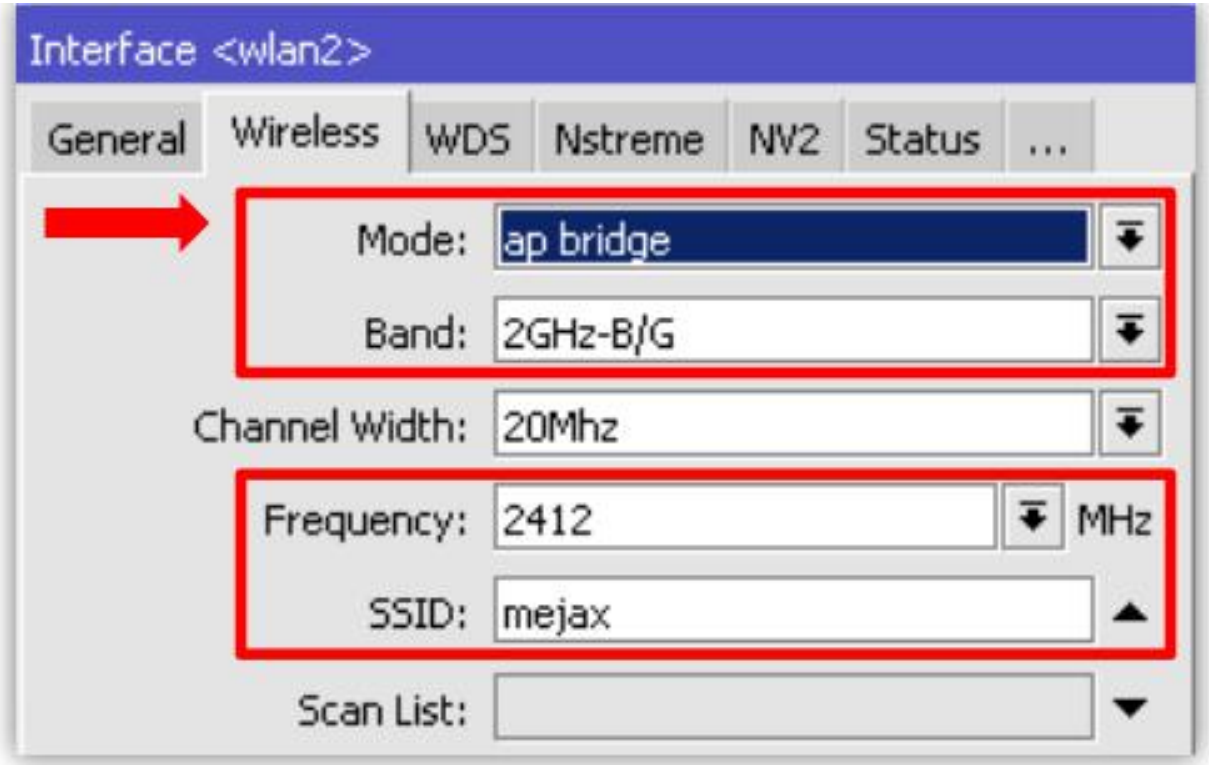
- Country : membatasi channel yang bisa digunakan sesuai dengan regulasi sebuah Negara
- Jika di set "*no_country_set*" maka akan menggunakan standard channel FCC compliant

(LAB)Point to Multipoint

- MikroTik difungsikan sebagai Access Point. Digunakan standard 802.11 b atau 802.11 b/g sehingga semua client (berbagai vendor dan berbagai tipe) dapat terkoneksi.

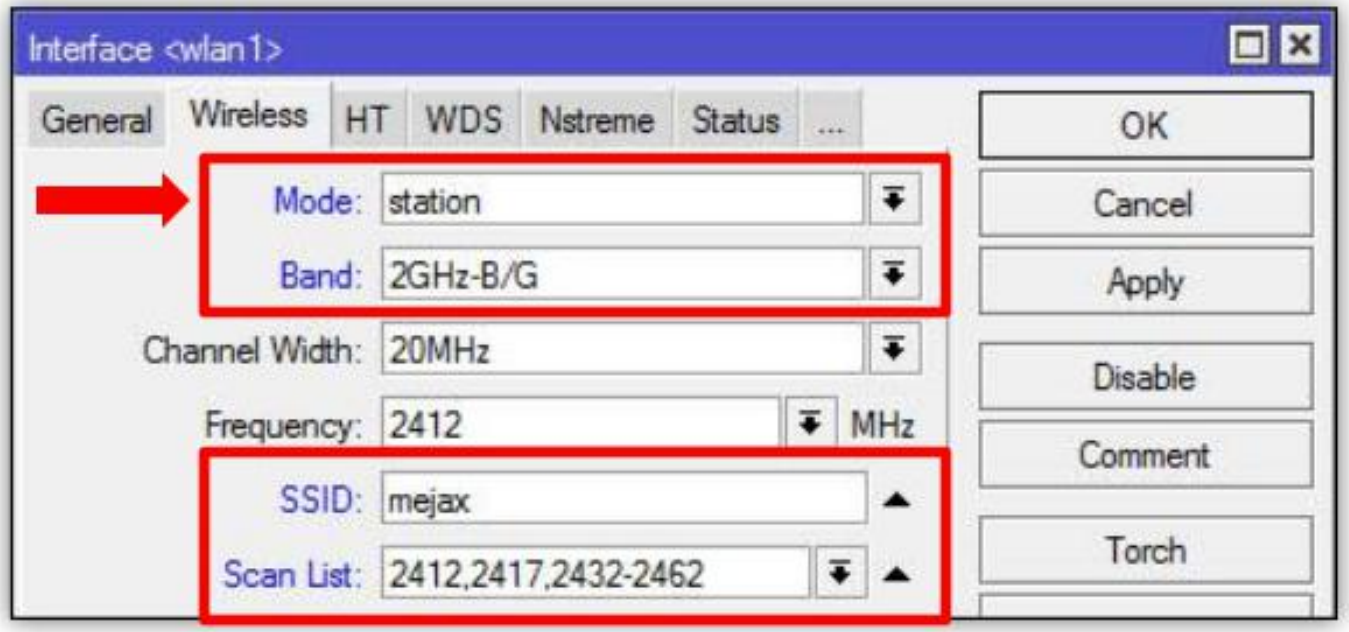
(LAB)Point to Multipoint AP Side

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



(LAB)Point to Multipoint Station Side

- Dapat menggunakan lisensi level 3
- Set mode, ssid, band, scan-list
- Set mode=station



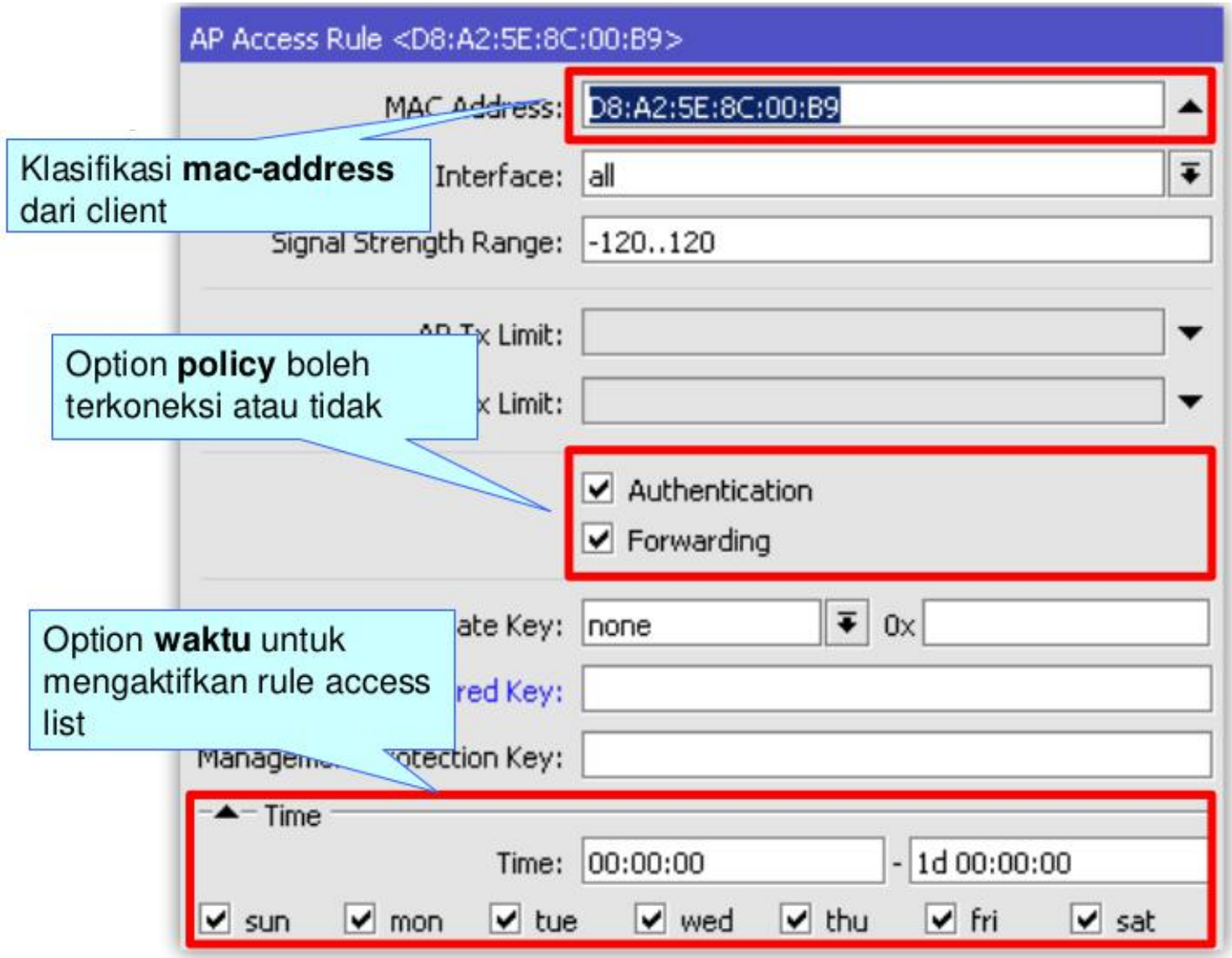
Wireless Access Management

- **Access list** : adalah filter autentikasi sebuah AP (AP Side) terhadap client yang terkoneksi
- **Connect List** : adalah filter autentikasi sebuah wireless station (Client Side) terhadap AP mana yang ingin terkoneksi
- Rule autentikasi atau filter autentikasi dibaca secara terurut dari atas ke bawah seperti halnya sebuah filter firewall sampai request autentikasi mencapai kecocokan
- Sangat dimungkiinkan untuk memasang beberapa filter untuk mac-address yang sama dan juga satu rule untuk semua mac-address
- sebuah rule filter mac-address bisa diterapkan pada sebuah interface wireless saja atau bisa juga untuk semua interface
- Jika tidak ada rule yang sesuai maka akan digunakan default policy (**default authentication** & **default forward**) dari wireless interface tersebut

Client Management

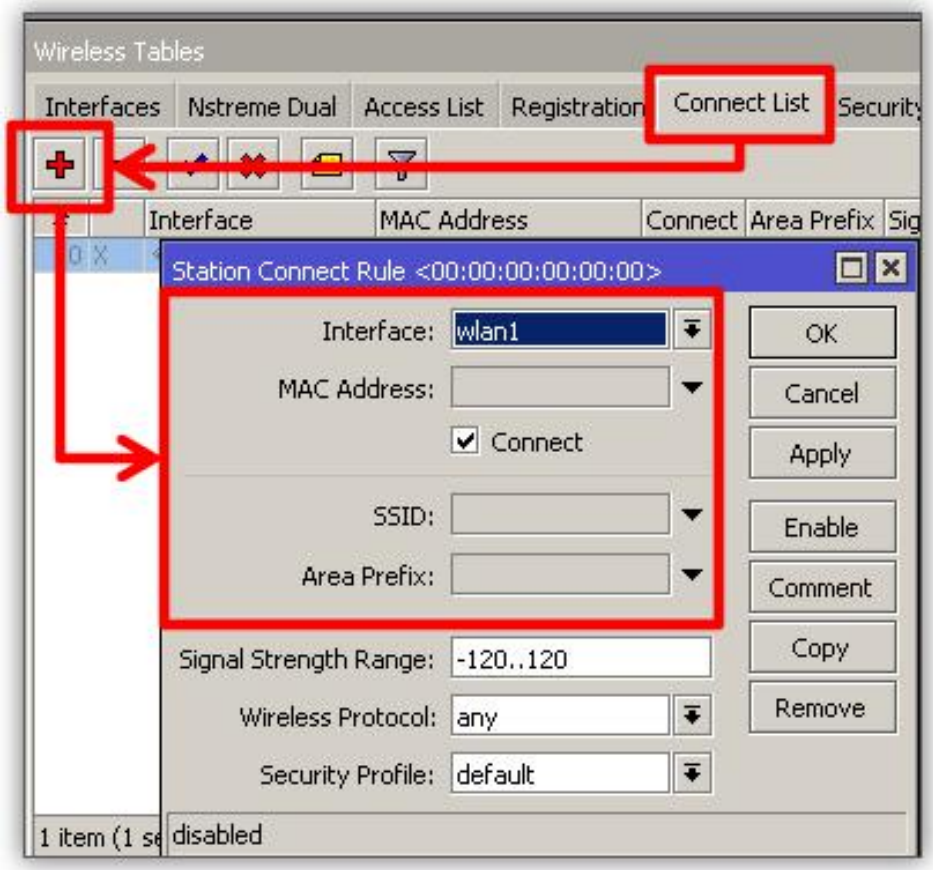
- Kita dapat melakukan pengaturan untuk setiap client menggunakan :
  - Access list :
    - MAC Address
    - Signal Strength
    - Time

Client Management



AP Management

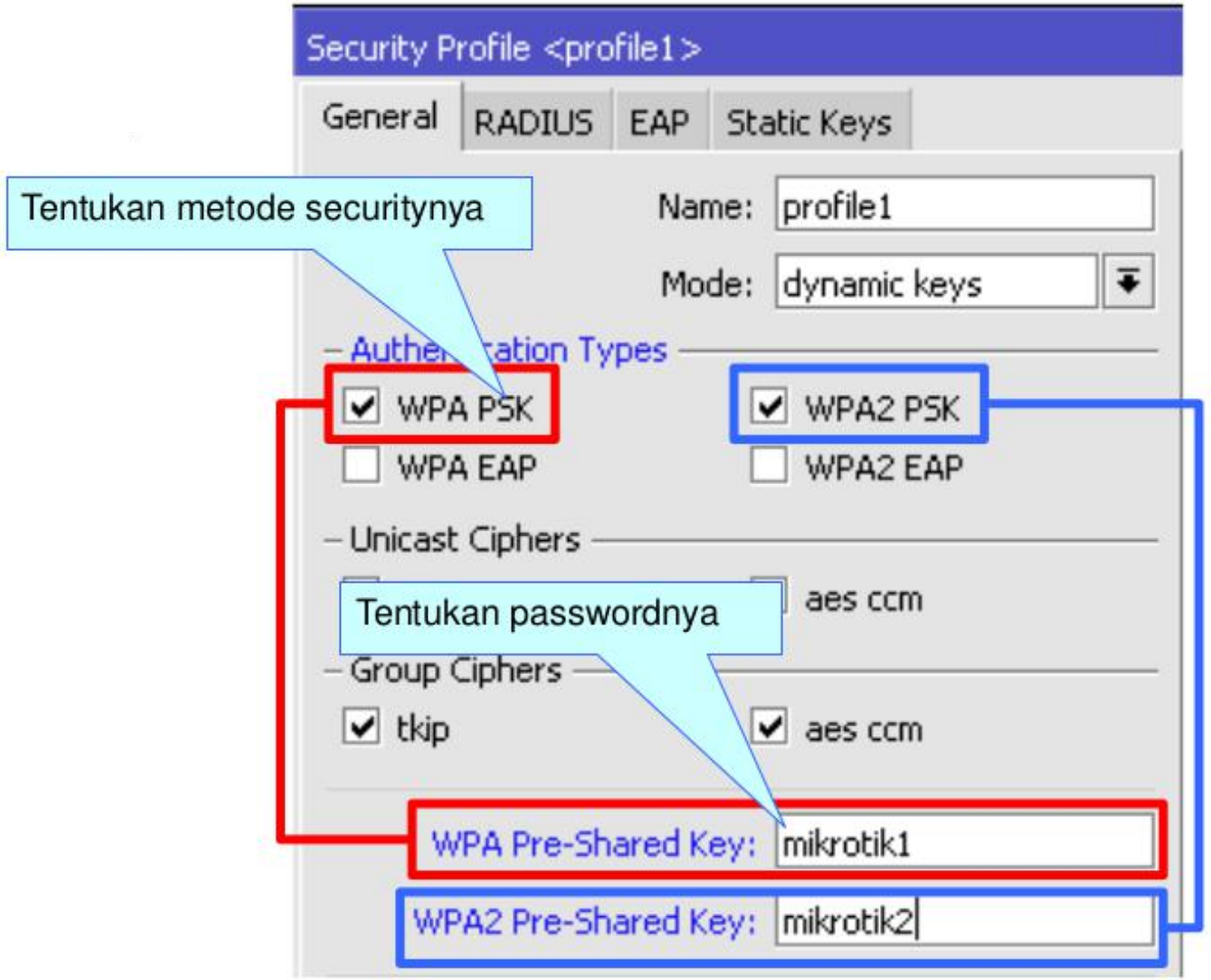
- Kita dapat melakukan pengaturan untuk AP yang akan kita hubungkan menggunakan
  - Connect List :
    - MAC Address
    - SSID
    - Area



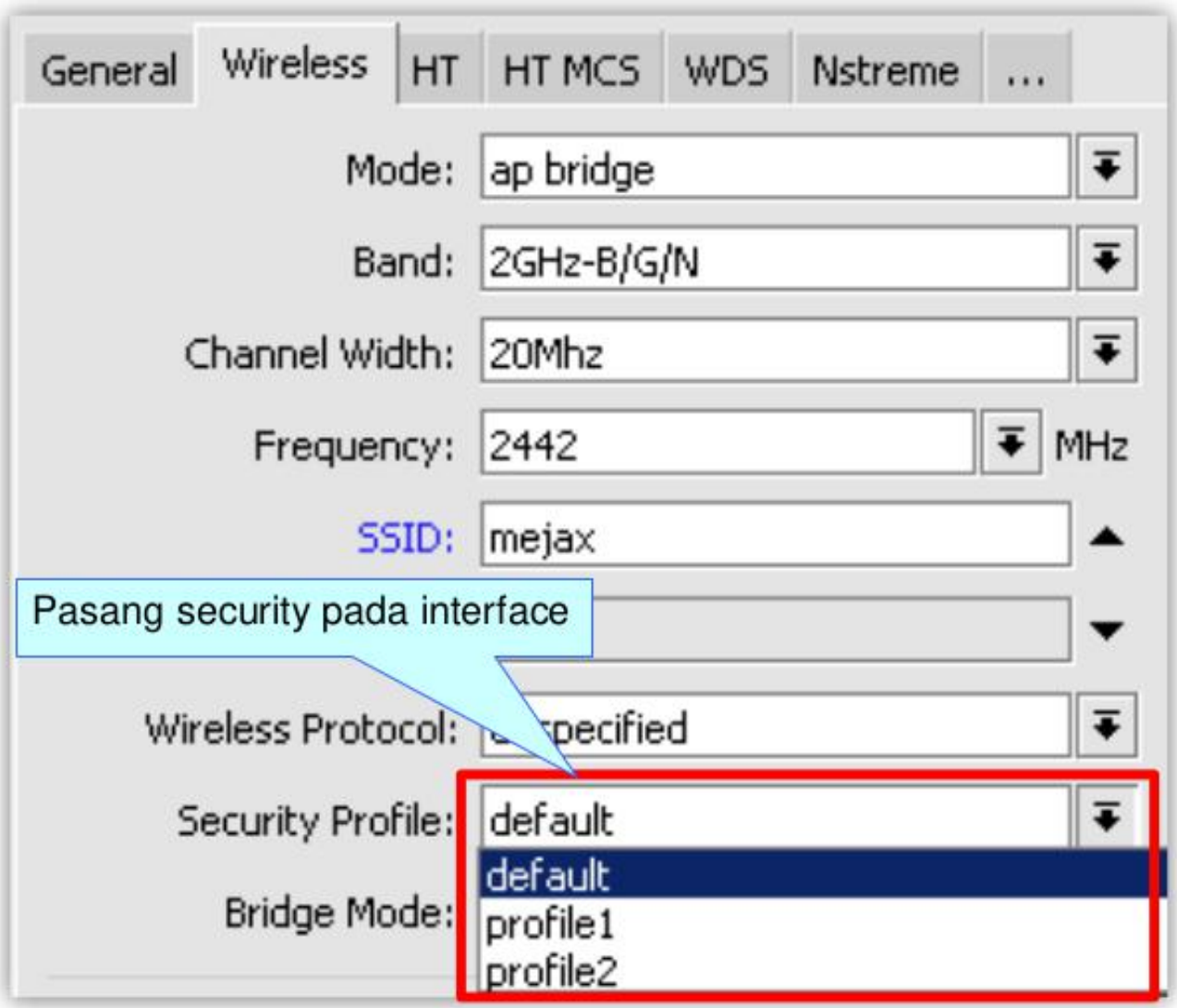
Wireless Security

- Karena sifat dari wireless yang "open access" maka sebuah Access Point akan rentan terhadap serangan dari pihak yang tidak bertanggung jawab
- Sudah saatnya untuk mengimplementasikan Wireless Security untuk menjaga AP tersebut dari berbagai serangan

(LAB)Create Wireless Security

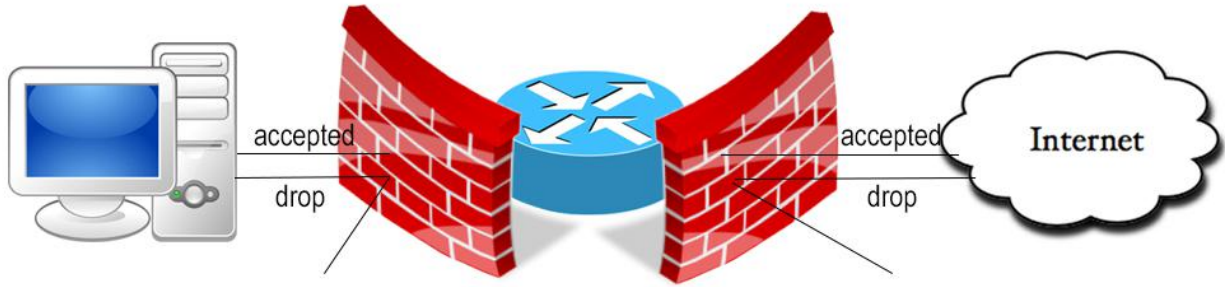


(LAB)Create Wireless Security



About Firewall

- Firewall adalah system pengaman (keamanan) yang memeriksa paket data yang keluar dan yang masuk. Dengan Firewall, kita bisa melindungi jaringan kita (local) dari serangan jaringan luar. Misalkan, melindungi jaringan LAN kita dari Internet.
- Firewall bisa digunakan untuk memblokir sebuah situs yang akan diakses oleh suatu Client. Misalkan situs Pornografi, atau situs-situs perjudian. Firewall ini sangat berguna jika kalian mempunyai warnet. Agar Client tidak sembarangan membuka situs-situs terlarang, apalagi yang buka masih anak kecil.
- Untuk mengetahui contoh cara kerja Firewall, kita bisa lihat Topologi sederhana dibawah ini



MikroTik Firewall Features

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

(LAB)NAT Masquerade IP Tertentu

- Maksud dari judul diatas adalah membatasi IP Address (Client) yang hanya boleh terkoneksi dengan jaringan Internet melalui Router MikroTik. Cara ini hampir sama seperti yang dibahas sebelumnya (Mengkonfigurasi NAT) hanya saja, disini Source Address nya kita isi dengan IP Client yang boleh menggunakan koneksi internet.
- Untuk langkah konfigurasi menggunakan perintah text (CLI), perintah nya adalah :

Ip firewall nat add chain=srcnat src-address=[ip yang boleh terkoneksi internet] out-interface=[interface yang mengarah ke internet] action=masquerade

- Sekarang, kita akan coba buat rule hanya IP yang mempunyai network 13.13.13.0/24 yang bisa terkoneksi dengan jaringan Internet. Perintah Text (CLI) nya

ip firewall nat add chain=srcnat src-address=13.13.13.0/24 out-interface=ether1 action=masquerade

- Setelah dibuat, kita cek dengan perintah **ip firewall nat print**

```
[admin@Rangga] > ip firewall nat add chain=srcnat src-address=13.13.13.0/24 out-
interface=ether1 action=masquerade
[admin@Rangga] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=srcnat action=masquerade src-address=13.13.13.0/24
      out-interface=ether1 log=no log-prefix=""
```

(LAB)NAT Masquerade IP Tertentu

- Setelah rule diatas dibuat, jadi hanya PC Client dengan IP Network 13.13.13.0/24 saja yang hanya bisa terkoneksi dengan Jaringan Internet melalui Router MikroTik
- Sekarang kita coba membuat rule, jadi hanya IP Client 13.13.13.1-13.13.13.10 saja yang bisa terkoneksi dengan Internet. Tetapi sebelum itu, **kita harus menghapus Rule firewall yang sebelumnya**. Karena MikroTik membaca Rule dari atas kebawah, jadi kalau rule yang sebelumnya (13.13.13.0/24) masih ada, maka PC Client yang mempunyai IP dengan network tersebut (13.13.13.1-13.13.13.254) masih bisa menggunakan internet, jadinya firewall yang kita buat akan sia-sia. Untuk menghapus rule firewall nya, bisa gunakan perintah text sebagai berikut

ip firewall nat remove [no index rule] berarti ip firewall nat remove 0

- setelah itu kita cek dengan perintah ip firewall nat print

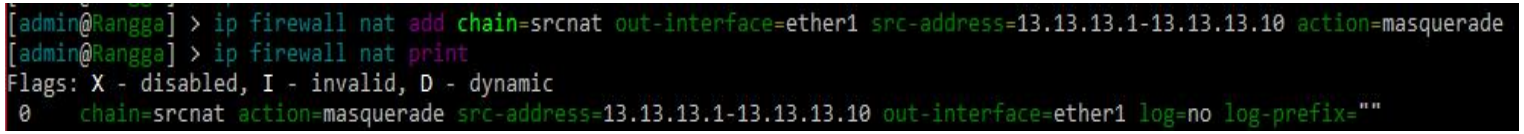
```
[admin@Rangga] > ip firewall nat remove 0
[admin@Rangga] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
```

- Bisa kita lihat diatas, Firewall Rules nya sudah kosong (tidak ada). Sekarang, kita lanjut buat firewall rules nya.

(LAB)NAT Masquerade IP Tertentu

ip firewall nat add chain=srcnat src-address=13.13.13.1-13.13.13.10 out-interface=ether1 action=masquerade

- setelah itu kita cek menggunakan **ip firewall nat print**

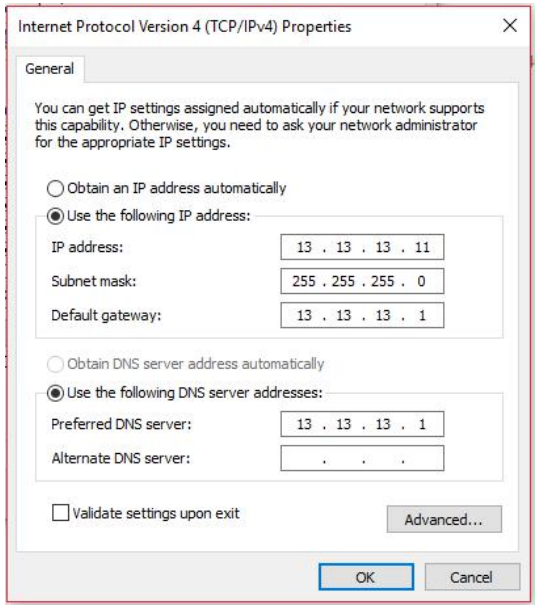


- Bisa kita lihat diatas, firewall rule sudah kita buat. Sekarang, untuk melakukan pengujian pada rule yang kita buat tadi, Kita ganti IP Address PC Client selain IP 13.13.13.1-13.13.13.10. Sebagai contoh disini saya akan menggunakan IP Address 13.13.13.11
- Untuk cara penggantian IP nya, buka **Network Sharing Center > Change adapter settings >** klik kanan **Local Area Connection lalu Properties**. Setelah itu, cari **IPv4** double klik, lalu ganti IP nya menjadi 13.13.13.11

NAT Masquerade IP Tertentu Test

- Setelah itu, kita coba ping google.com dengan PC tersebut. Maka hasilnya akan RTO karena tidak terhubung dengan jaringan internet

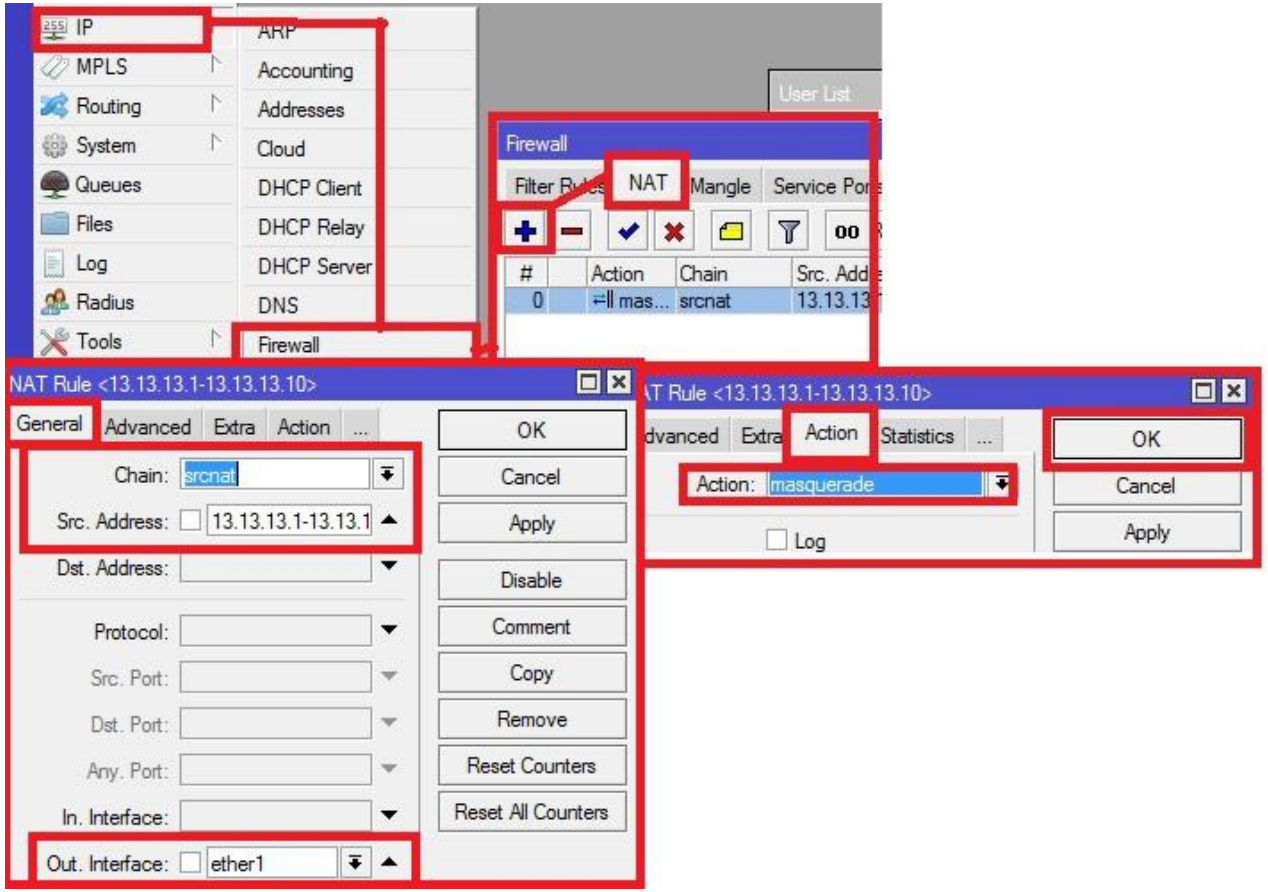
```
C:\Users\Windows 8>ping google.com

Pinging google.com [172.217.24.110] with 32 bytes of data:
Request timed out.
Request timed out.
```



- Jika RTO, berarti rule yang kita buat sudah selesai. Jadi, hanya client yang mempunyai IP 13.13.13.1-13.13.13.10 saja yang bisa terhubung dengan koneksi internet

(LAB)NAT Masquerade IP Tertentu

- Jika melalui Winbox (GUI) , kita masuk ke menu **IP > Firewall > tab NAT >+** (add) lalu isi dengan konfigurasi seperti tadi.



NAT Masquerade Port Tertentu

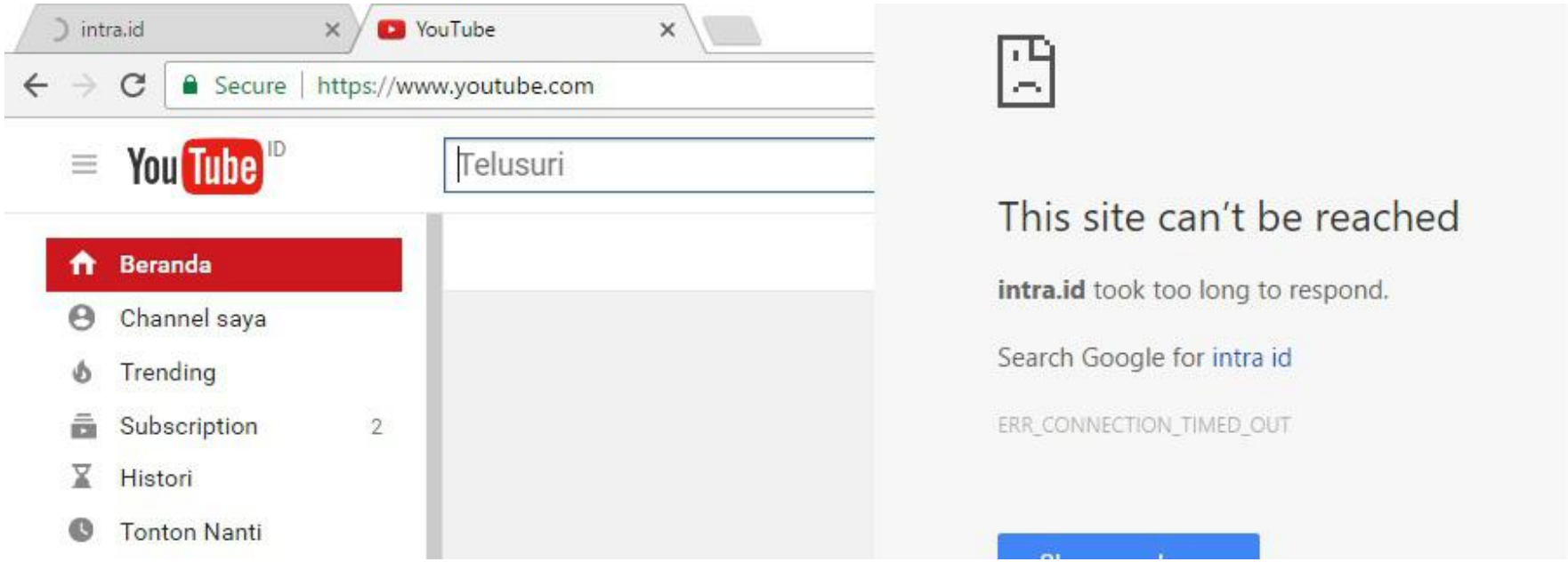
- sekarang kita akan melakukan masquerade pada port tertentu. Konfigurasinya hampir sama, hanya saja nanti kita akan mengisi bagian protocol dan dst-port. Misalnya, jika kalian ingin membatasi client hanya bisa melakukan browsing, berarti kalian isi HTTP (port 80) dan HTTPS (port 443) di dst-port dan pilih protocol nya tcp. Sekarang, langsung saja kita coba praktekan. Disini, saya akan membatasi client hanya bisa browsing website yang menerapkan HTTPS. Berarti client tersebut tidak bisa browsing website dengan HTTP. Sebelumnya, kita hapus dulu rules yang sebelumnya, atau bisa juga diedit (melalui Winbox). Perintah Text (CLI) nya adalah :

ip firewall nat add chain=srcnat src-address=13.13.13.1-13.13.13.10 out-interface=ether1 protocol=tcp dst-port=443 action=masquerade

```
[admin@Rangga] > ip firewall nat add chain=srcnat src-address=13.13.13.1-13.13.13.10 out-interface=ether1
protocol=tcp dst-port=443 action=masquerade
[admin@Rangga] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=srcnat action=masquerade protocol=tcp src-address=13.13.13.1-13.13.13.10 out-interface=ether1
      dst-port=443 log=no log-prefix=""
```

NAT Masquerade Port Tertentu Test

- Setelah itu, untuk melakukan pengujian kita coba melakukan browsing menuju web yang menggunakan protocol https, misalnya **youtube**. Dan test browsing menuju web yang menggunakan protocol http, misalnya **intra.id**
- Bisa kita lihat gambar yang dibawah ini. Youtube berhasil terbuka, sedangkan intra.id tidak terbuka sama sekali

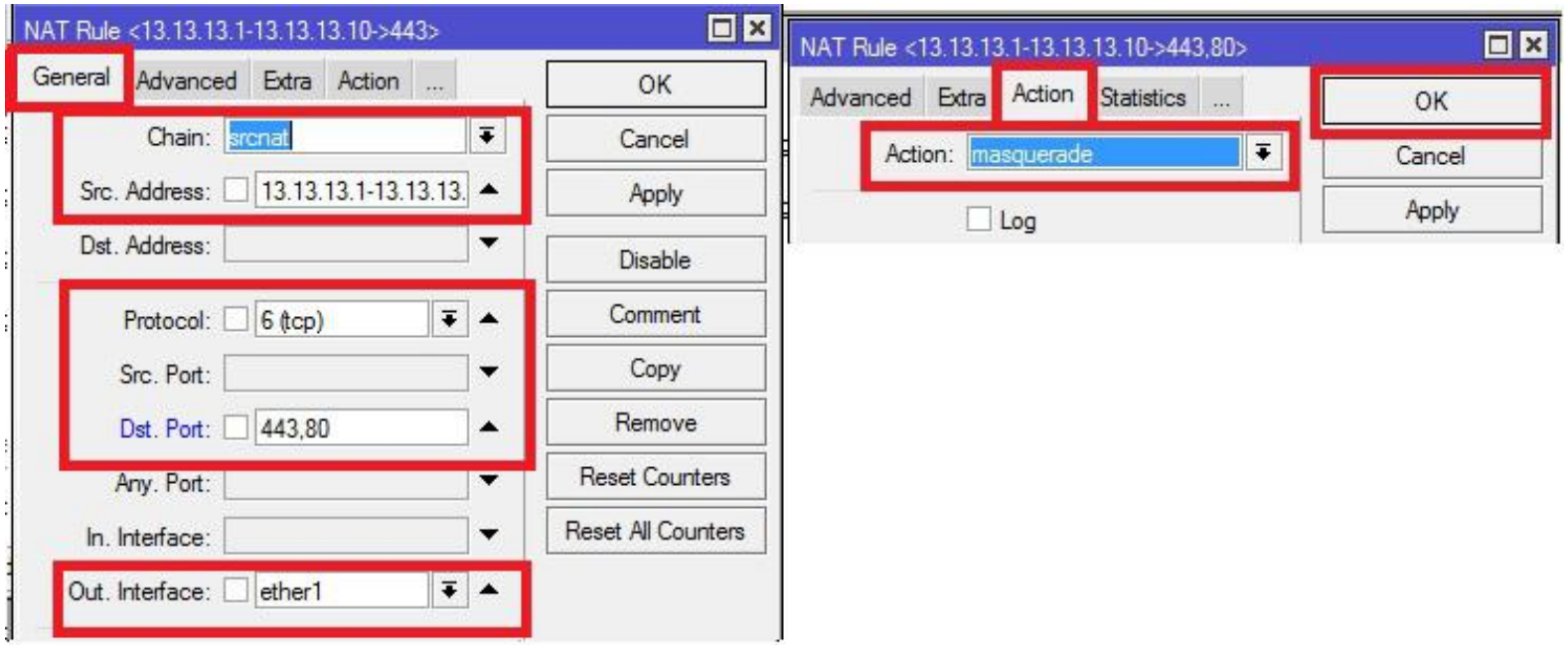


(LAB)NAT Masquerade Port Tertentu

- Agar client juga bisa browsing web yang menggunakan protocol http, dibagian dst-port kita tambahkan port http, yaitu 80. rule seperti dibawah ini.

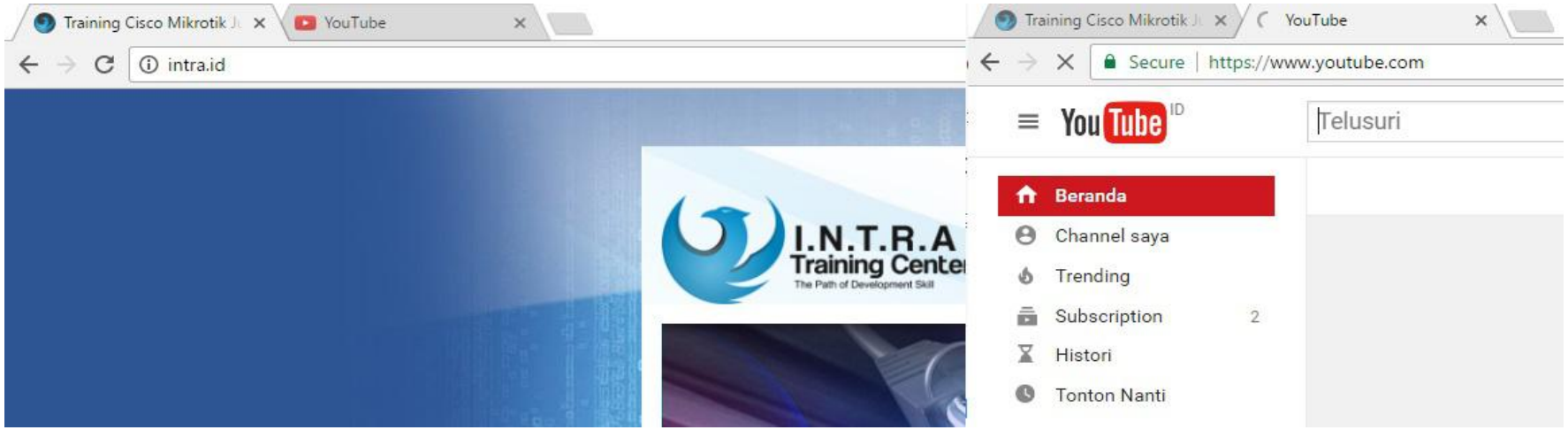
ip firewall nat set 0 dst-port=80,443

- Jika melalui Winbox (GUI) kita bisa masuk ke menu IP Firewall NAT + lalu konfigurasikan seperti tadi, atau bisa lihat gambar dibawah ini :



NAT Masquerade Port Tertentu Test

- Bisa kita lihat dibawah, sekarang web http (intra.id) nya bisa terbuka



- Jika konfigurasi nya sudah dilakukan, maka sekarang PC Client hanya bisa browsing dan download melalui web dengan protocol port HTTP dan HTTPS. Tidak bisa menggunakan Yahoo Mesenger dan sebagainya karena port nya berbeda. Untuk menambahkan portnya, langkahnya sama seperti langkah konfigurasi diatas.

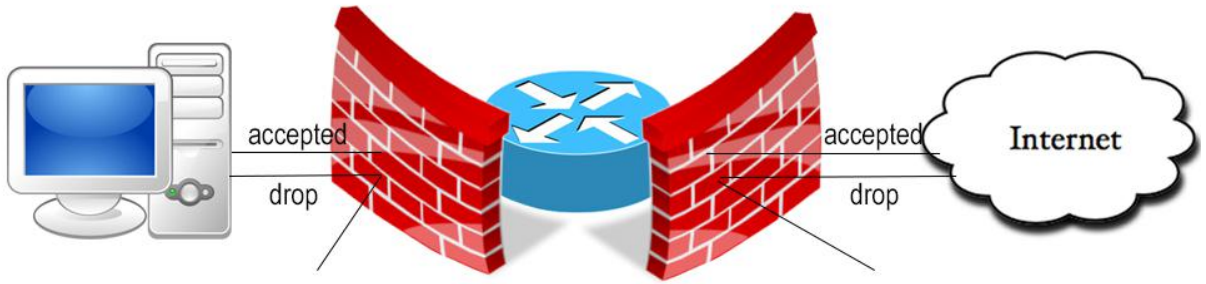
Firewall Filter

- Firewall Filter ini berfungsi menyaring (filter) paket data yang masuk dan keluar dari jaringan dalam (local) atau dari jaringan luar (internet). Jadi, nantinya router akan menyaring data apa saja yang boleh masuk / keluar. Firewall filter sendiri mempunyai 3 mode (chain) yaitu :
- **Forward** = Filter ini berfungsi untuk menangani paket data yang melewati router
- **Input** = Filter ini berfungsi untuk menangani paket data yang masuk ke router
- **Output** = Filter ini berfungsi untuk menangani paket data yang keluar dari router

Disini saya hanya akan membahas filter Input dan Forward.

Firewall Chain Input

- Seperti yang saya bahas diatas, firewall input ini berfungsi untuk menangani paket data yang masuk ke dalam router, seperti melakukan konfigurasi pada router (seperti menambah IP address, dsb) maupun ping dari jaringan luar (internet) dan jaringan local. Di MikroTik sendiri, port untuk konfigurasi seperti WinBox (8291), Telnet (23) itu terbuka. Maksudnya, bisa di akses oleh siapa saja yang terkoneksi dengan router MikroTik tersebut. Nah, bahaya kan kalau misalkan ada yang mengkonfigurasi router kita sembarangan? Disinilah contoh fungsi firewall input. Jadi nantinya kita bisa membatasi siapa saja yang bisa mengkonfigurasi routerboard.
- Agar lebih paham, Kita bisa lihat cara kerja dari Firewall Input pada gambar dibawah ini



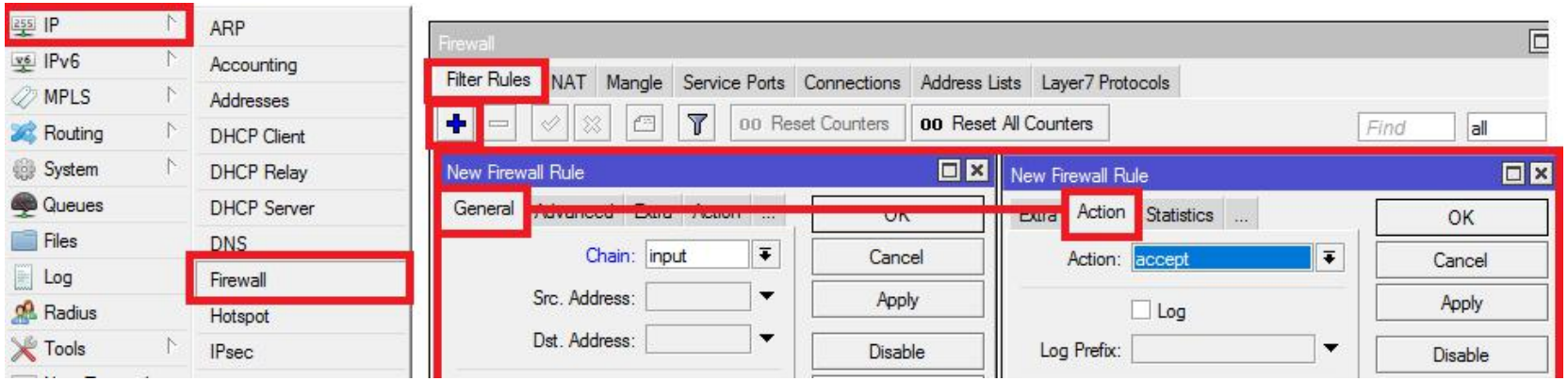
(LAB)Firewall Chain Input

- Sekarang kita akan melakukan percobaan drop semua paket data yang masuk ke router. Langsung ke langkah konfigurasi nya.
- Jika melalui Perintah text (CLI), perintahnya adalah sebagai berikut :

ip firewall filter add chain=input action=drop

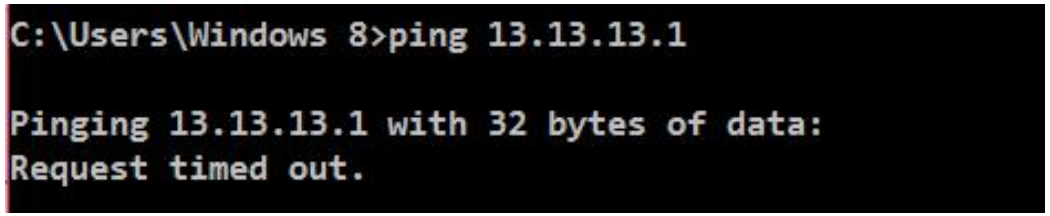
```
[admin@Rangga] > ip firewall filter add chain=input action=drop
```

Jika melalui Winbox (GUI), klik pada menu IP Firewall tab Filter + (add) lalu lakukan konfigurasi seperti perintah text diatas, atau kalian bisa lihat gambar dibawah ini



Firewall Chain Input Test

- Sekarang untuk melakukan percobaan, kita akan lakukan ping dari pc client menuju router.



- Bisa kita lihat gambar diatas, hasilnya akan RTO karena semua data yang masuk kedalam router akan di drop.
- Cara diatas hanya untuk percobaan saja dan bertujuan untuk mengerti cara kerja dari firewall input.

(LAB)Firewall Chain Input

- Sekarang, kita akan coba membatasi siapa saja yang dapat mengakses port konfigurasi pada router MikroTik dari jaringan local (ether2). Disini saya akan coba membuat rule, jadi hanya PC Admin (dengan IP 13.13.13.2) yang bisa melakukan konfigurasi pada router MikroTik. Selain dari PC admin (contoh 13.13.13.3) tidak akan bisa melakukan konfigurasi pada router. Port konfigurasi pada MikroTik:
- Winbox (8291) , Telnet (23) , SSH (22) , WebFig (80), ftp (20 & 21)

Jika melalui perintah text (CLI) , perintahnya adalah

ip firewall filter add chain=input src-address=13.13.13.2 in-interface=ether2 action=accept

```
[admin@Rangga] > ip firewall filter add chain=input src-address=13.13.13.2 in-interface=ether2  action=accept
[admin@Rangga] > ip firewall filter pr
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=input action=accept src-address=13.13.13.2 in-interface=ether2 log=no log-prefix=""
```

Jika diartikan, rule diatas berarti “jika ada input dari sumber 13.13.13.2 menuju interface ether2, maka diperbolehkan (accept)

Sekarang, kita akan membuat action drop nya. Perintah text (CLI) nya adalah

ip firewall filter add chain=input in-interface=ether2 protocol=tcp dst-port=8291,23,22,80,20,21 action=drop

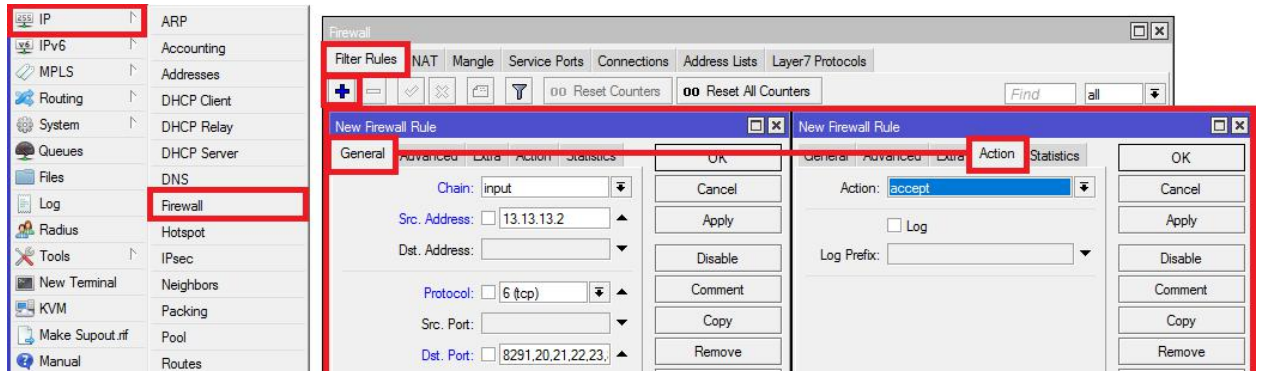
```
[admin@Rangga] > ip firewall filter add chain=input in-interface=ether2 protocol=tcp dst-port=8291,23,22,20,21,80 action=drop
```

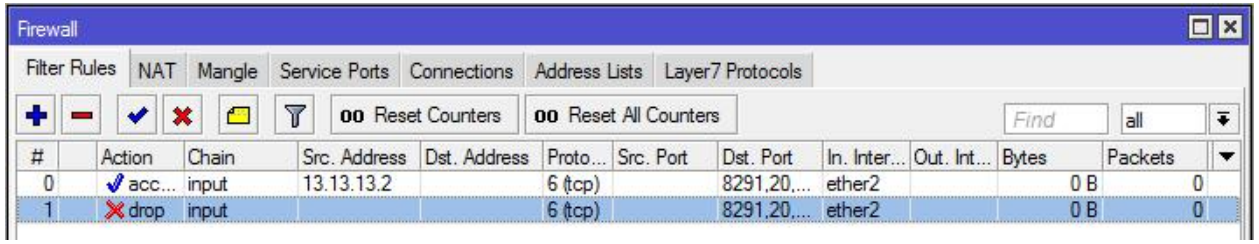
(LAB)Firewall Chain Input

- Setelah itu, kita cek menggunakan perintah **ip firewall filter print**

```
[admin@Rangga] > ip firewall filter pr
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=input action=accept src-address=13.13.13.2 in-interface=ether2 log=no log-prefix=""

 1    chain=input action=drop protocol=tcp in-interface=ether2 dst-port=8291,20,21,22,23,80 log=no log-prefix=""
```

- Jika diartikan, perintah diatas berarti “jika ada input (dari jaringan local) menuju interface ether2 untuk mengakses protocol tcp dengan port sekian, maka akan di drop”
- Jika melalui Winbox (GUI), klik pada menu IP Firewall tab Filter + (add) lalu lakukan konfigurasi seperti diatas, atau bisa lihat gambar dibawah ini





Firewall Chain Input Test

- Sekarang, untuk percobaan, coba kalian remote routerboard dengan telnet melalui IP 13.13.13.2, maka akan terbuka.

- Setelah itu, coba kalian buka melalui IP selain dari 13.13.13.2, maka akan di drop.

- Dengan rule diatas, kita telah mengamankan konfigurasi router dari PC Client yang lain. Sekarang, bagaimana cara mengamankan port yang terbuka dari jaringan luar (internet)? Caranya sama, tetapi pada bagian in-interface , kita isi dengan interface yang menuju ke Internet, yaitu ether1.

(LAB)Firewall Chain Input

- Karena MikroTik membaca Rule dari atas baru ke bawah, maka kita buat dulu rule dengan IP Address yang diperbolehkan mengakses router. Disini saya akan membuat IP Address 13.13.13.2 bisa mengakses port konfigurasi pada router. Maka perintah text (CLI) nya adalah sebagai berikut :

ip firewall filter add chain=input src-address=13.13.13.2 in-interface=ether1 action=accept

```
[admin@Rangga] > ip firewall filter add chain=input src-address=13.13.13.2 in-interface=ether1 action=accept
```

- Setelah itu, kita buat lagi rule yang kedua, yaitu rule drop perintahnya adalah :

ip firewall filter add chain=input in-interface=ether1 protocol=tcp dst-port=8291,23,22,80,20,21 action=drop

```
[admin@Rangga] > ip firewall filter add chain=input in-interface=ether1 protocol=tcp dst-port=8291,23,22,80,20,21 action=drop
```

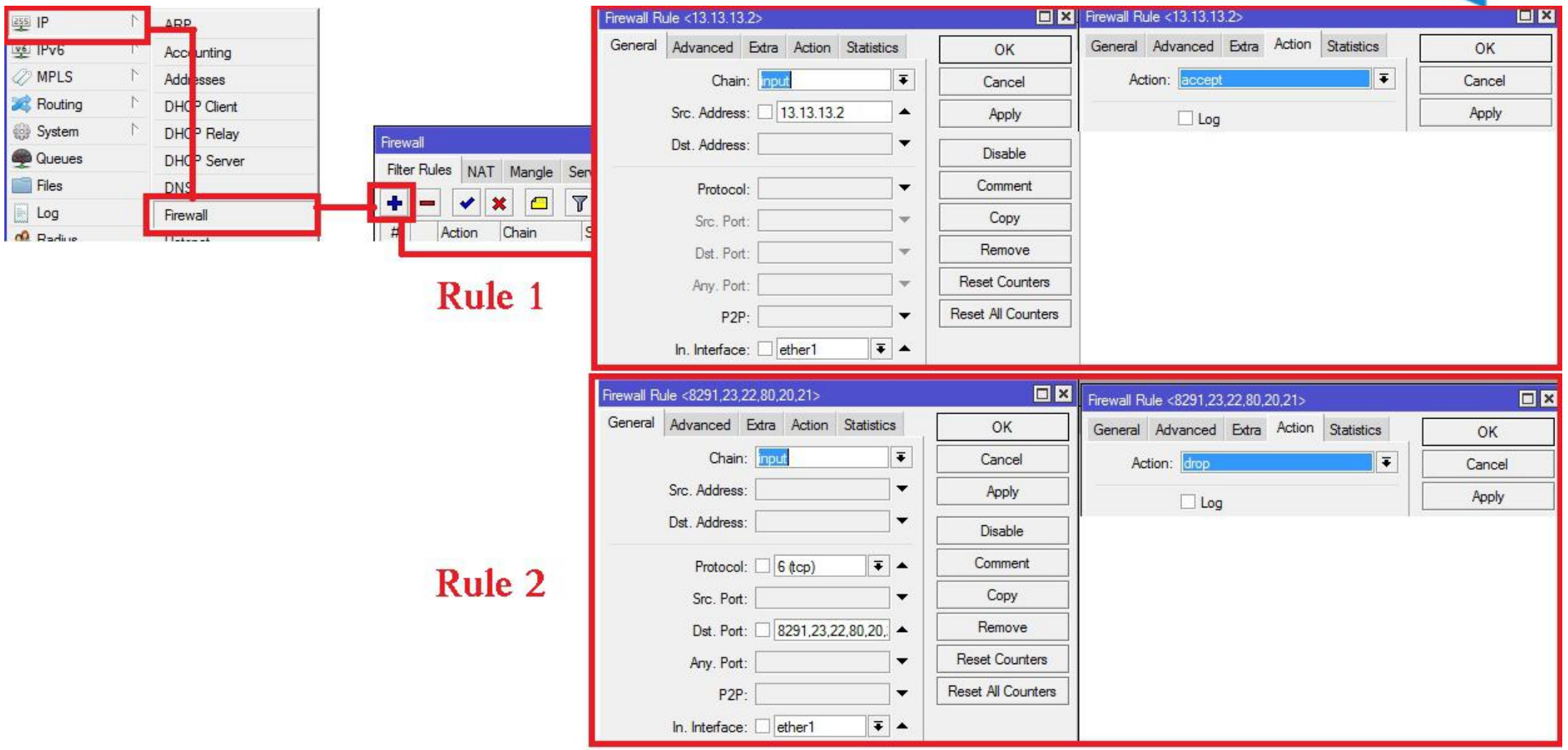
Firewall Chain Input Test

- Untuk mengecek rule yang tadi telah kita buat, perintah text nya adalah : **ip firewall filter print**

```
[admin@Rangga] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=input action=accept src-address=13.13.13.2 in-interface=ether1 log=no log-prefix=""

 1    chain=input action=drop protocol=tcp in-interface=ether1 dst-port=8291,23,22,80,20,21 log=no log-prefix=""
```

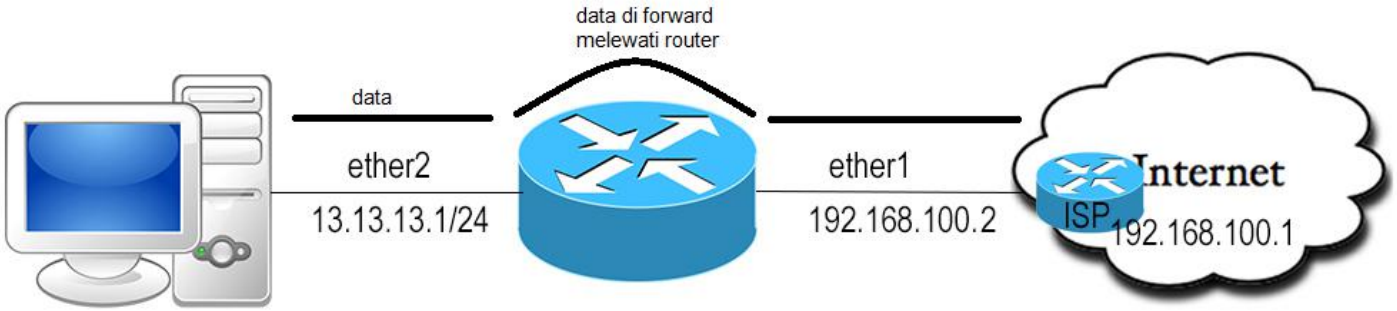
- Sekarang, berarti hanya PC dengan IP 13.13.13.2/24 saja yang bisa mengakses router melalui jaringan luar (internet)
- Jika melalui Winbox (GUI) , bisa masuk ke menu IP Firewall Filter Rules + (add) , lalu isi perintah rules nya seperti tadi.

(LAB)Firewall Chain Input



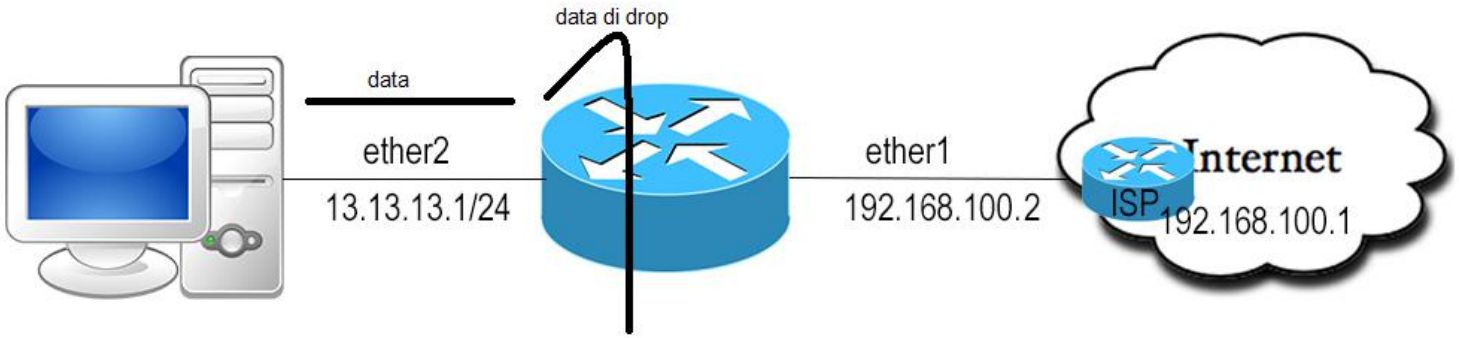
Firewall Forward

- Firewall Forward ini berfungsi untuk menangani paket data yang melewati (melintasi) router, baik dari jaringan local atau jaringan luar. Firewall Forward juga mengatur boleh / tidak nya suatu paket menuju jaringan internet atau jaringan local, jadi firewall forward ini bisa kita pakai untuk memblokir website yang akan di akses client. Menggunakan firewall forward hampir sama dengan menggunakan srcnat yang kita sudah bahas sebelumnya. Hanya saja, jika menggunakan srcnat, srcnat akan melakukan perubahan IP Address pada pengirim data. Tetapi, jika pada firewall forward, firewall forward hanya akan mengirim data dari si pengirim tanpa melakukan perubahan IP Address.



(LAB)Firewall Forward

- Untuk mengerti cara kerja firewall forward, kita akan melakukan percobaan blok akses internet pada client (Drop).



- Langsung ke langkah konfigurasi nya
- Jika melalui perintah text (CLI) , perintahnya adalah :

ip firewall filter add chain=forward action=drop

```
[admin@Rangga] > ip firewall filter add chain=forward action=drop
[admin@Rangga] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=forward action=drop log=no log-prefix=""
```

(LAB)Firewall Forward

- Setelah itu, kita test dengan cara ping dari pc client menuju internet, maka hasilnya akan RTO karena akses forward nya sudah kita drop.
- Jika melalui Winbox (GUI) , bisa dilakukan dengan cara klik menu IP Firewall Filter Rules + (add) . lalu di tab General pada bagian **chain** kita isi **forward**. Lalu klik tab **Action**, pilih **action=drop**

- Rule diatas hanya untuk percobaan saja, agar mengerti cara kerja dari firewall forward. Sebelum ke langkah selanjutnya, kita hapus dulu rule firewall forward drop ini

```
[admin@Rangga] > ip firewall filter remove 0
```

Firewall Forward Blokir IP Address

- Setelah kita melakukan percobaan Firewall Forward, sekarang kita coba memblokir situs dengan firewall forward. Disini kita akan memblokir website tersebut berdasarkan IP Address nya. Jadi, sebelum memblokir website tersebut, kita harus mengetahui IP Address dari website tersebut. Caranya, kita bisa menggunakan perintah **nslookup** menggunakan CMD. Sebelum menggunakan nslookup, pastikan dulu pc sudah terhubung akses internet. Disini saya akan mencoba memblokir situs web kompas.com, berarti perintahnya adalah sebagai berikut

nslookup kompas.com

Bisa kita lihat diatas, kompas.com mempunyai 2 IP yang berbeda. Berarti kita harus membuat 2 rule dengan 2 IP tujuan (dst-address) yang berbeda untuk memblokir situs kompas.com tersebut. Langsung saja ke langkah konfigurasi nya :

Jika melalui perintah text (CLI), maka perintahnya :

(LAB)Firewall Forward

ip firewall filter add chain=forward dst-address=202.146.4.100 action=drop

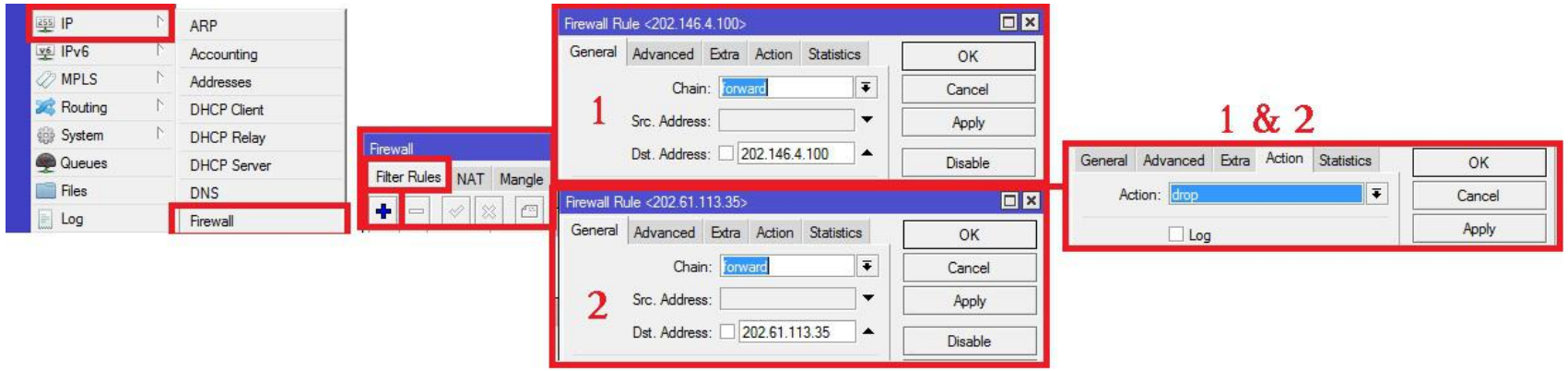
ip firewall filter add chain=forward dst-address=202.61.113.35 action=drop

untuk mengecek, **perintahnya ip firewall filter print**

```
[admin@Rangga] > ip firewall filter add chain=forward dst-address=202.146.4.100 action=drop
[admin@Rangga] > ip firewall filter add chain=forward dst-address=202.61.113.35 action=drop
[admin@Rangga] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=forward action=drop dst-address=202.146.4.100 log=no log-prefix=""

 1    chain=forward action=drop dst-address=202.61.113.35 log=no log-prefix=""
```

(LAB)Firewall Forward

- Jika melalui WInbox (GUI), bisa masuk ke menu IP Firewall Filter Rules + (add) lalu di tab **General** , kita isi **chain=forward** , lalu **dst-address** dengan IP tujuan yang tadi. Masuk ke tab **Action**, kita pilih **action** nya, yaitu **drop.** setelah itu, kita buat lagi rule, tetapi isi **dst-address** dengan IP kompas yang ke 2



Firewall Forward Test

- Rule sudah dibuat, sekarang kita coba buka kompas.com atau lakukan ping, maka website tersebut tidak akan terbuka dan akan loading terus menerus.

```
C:\Users\Windows 8>ping kompas.com

Pinging kompas.com [202.146.4.100] with 32 bytes of data:
Request timed out.
```

- Kita sudah berhasil memblokir website kompas. Tetapi dengan cara ini, mungkin sedikit repot karena harus mengetahui IP address dari website tersebut. Ada cara yang mungkin lebih efisien, yaitu memblokir situs berdasarkan content website.

(LAB)Firewall Blokir Kontent

- Sekarang kita akan mencoba memblokir situs berdasarkan content nya. Menggunakan fitur content ini juga bisa untuk memblokir download suatu ekstensi file (contoh .3gp) agar user tidak sembarangan download yang bukan-bukan. Sekarang langsung ke langkah konfigurasi :
- Disini, saya akan coba membuat 2 rule untuk memblokir content “porn” dan juga ekstensi “.3gp” Untuk perintah text (CLI), perintahnya adalah :

ip firewall filter add chain=forward content=porn action=drop

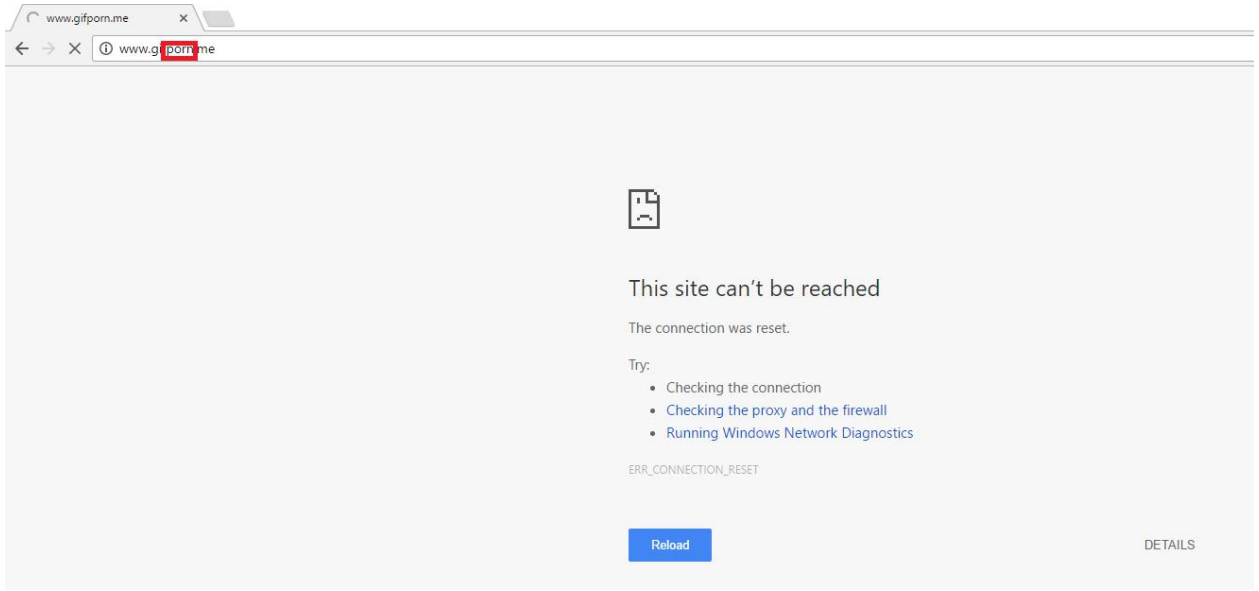
ip firewall filter add chain=forward content=.3gp action=drop

untuk mengecek nya**, gunakan perintah ip firewall print**

```
[admin@MikroTik] > ip firewall filter add chain=forward content=porn action=drop
[admin@MikroTik] > ip firewall filter add chain=forward content=.3gp action=drop
[admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=forward action=drop content=porn log=no log-prefix=""

 1    chain=forward action=drop content=.3gp log=no log-prefix=""
```

Firewall Blokir Kontent Test

- Rule diatas sudah dibuat. Berarti, siapa saja yang terkoneksi (termasuk admin) dengan router, maka tidak akan bisa mengakses website yang mengandung content “porn” dan “.3gp”.



(LAB)Firewall Blokir Kontent

- Disini juga kita bisa menambahkan src-address nya. Jadi, hanya IP tertentu saja yang tidak boleh mengakses website yang mempunyai content tersebut. Disini saya akan coba menambahkan src-address , jadi hanya IP Admin saja yang bisa mengakses web yang berisi content tersebut, huehue. Langkah konfigurasinya adalah sebagai berikut :
- Disini saya contohkan IP Address yang dimiliki admin adalah 13.13.13.2/24 . Jadi sisanya adalah IP Address client (13.13.13.3-13.13.13.254) yang akan kita masukkan ke src-address . untuk perintah text (CLI) nya adalah sebagai berikut :

ip firewall filter add chain=forward src-address=13.13.13.3.2 action=accept

- setelah itu, kita cek menggunakan **ip firewall filter print**

```
[admin@MikroTik] > ip firewall filter add chain=forward src-address=13.13.13.2 action=accept
[admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=forward action=drop content=porn log=no log-prefix=""

 1    chain=forward action=drop content=.3gp log=no log-prefix=""

 2    chain=forward action=accept src-address=13.13.13.2 log=no log-prefix=""
```

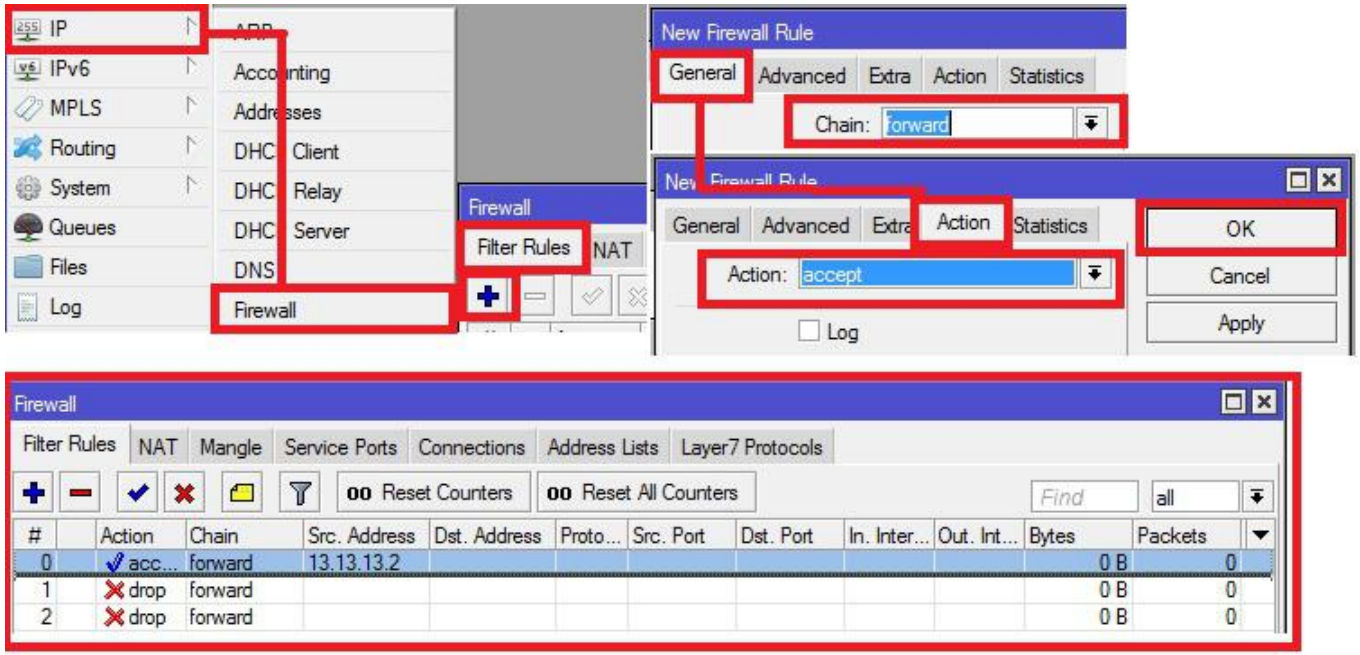
(LAB)Firewall Blokir Kontent

- Setelah itu, kita pindahkan rule yang tadi kita buat menjadi urutan paling atas dengan menggunakan perintah **ip firewall move 2 0**

```
[admin@MikroTik] > ip firewall filter move 2 0
[admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=forward action=accept src-address=13.13.13.2 log=no log-prefix=""

 1    chain=forward action=drop content=porn log=no log-prefix=""

 2    chain=forward action=drop content=.3gp log=no log-prefix=""
```

- Jika melalui Winbox (GUI) , kita klik menu IP Firewall Filter Rules + (add) . lalu pada tab General kita isi **chain=forward** , **src-address=13.13.13.2** , tab **action** kita isi **accept**. Setelah itu, kita drag & drop Rules yang kita buat menjadi paling atas

Firewall Blokir Kontent Test



- Sekarang, coba kita test mengakses website yang mempuyai content tersebut menggunakan PC dengan IP (13.13.13.2) maka akan berhasil. Sekarang, coba kita buka website dengan konten tersebut menggunakan PC selain dari IP 13.13.13.2 , maka akan gagal.

Address List

- Address List adalah suatu fitur di MikroTik yang berfungsi untuk menandakan IP Address tertentu menjadi sebuah Nama. Misalkan disini saya akan membuat 2 Address List dengan IP Address 13.13.13.2 dan akan saya namai “IP admin” dan untuk IP Address 13.13.13.0/24 saya namai “IP Client”. Langkah konfigurasinya adalah sebagai berikut :
- Jika melalui Perintah Text (CLI) , perintahnya adalah :

ip firewall address-list add address=13.13.13.2 list=”IP Admin”

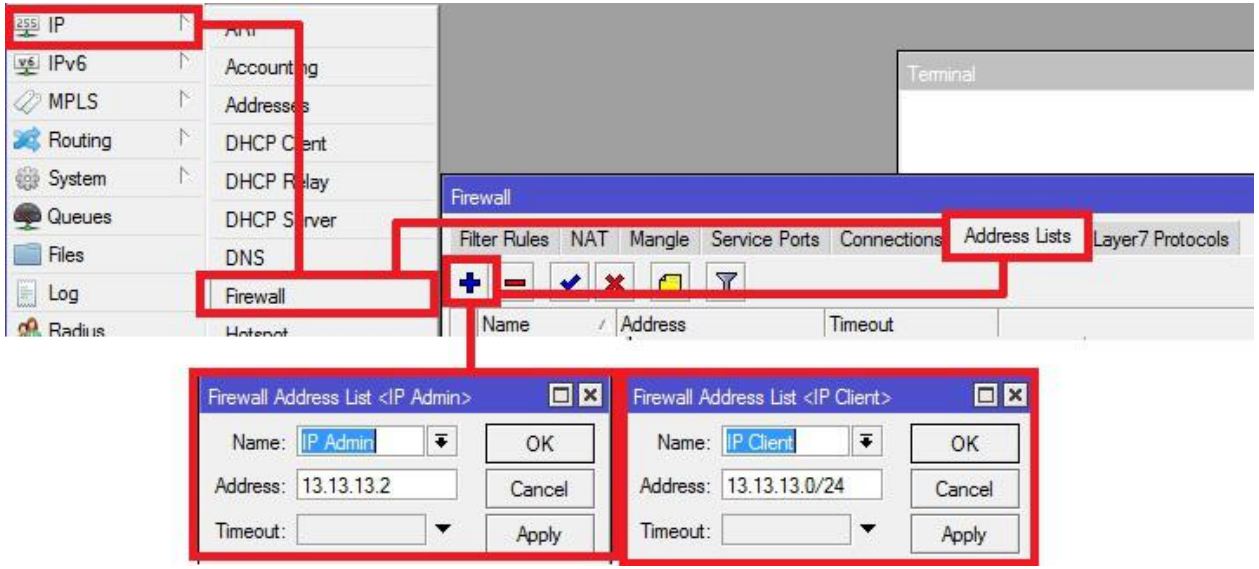
ip firewall address-list add address=13.13.13.0/24 list=”IP Client”

- untuk mengeceknya, kita bisa gunakan perintah **ip firewall address-list print**

```
[admin@Rangga] > ip firewall address-list add address=13.13.13.2 list="IP Admin"
[admin@Rangga] > ip firewall address-list add address=13.13.13.0/24 list="IP Client"
[admin@Rangga] > ip firewall address-list print
Flags: X - disabled, D - dynamic
 #   LIST                                                ADDRESS                                 TIMEOUT
 0   IP Admin                                            13.13.13.2
 1   IP Client                                           13.13.13.0/24
```

- Jika melalui Winbox (GUI) bisa klik menu IP Firewall Address List + setelah itu isi bagian **Name** dengan nama **address list** nya, lalu bagian address isi dengan IP Address.

(LAB)Address List



- Kita sudah buat Address List nya, sekarang kita akan coba menggunakan Address List nya. Misalkan disini kita akan buat pc admin mendapatkan semua akses internet, sedangkan PC client hanya bisa browsing dan tidak bisa mendownload file ber ekstensi .iso . Maka perintah textnya adalah sebagai berikut :

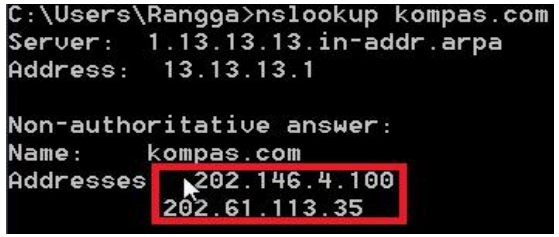
ip firewall filter add chain=forward src-address-list=”IP Admin” action=”accept”

ip firewall filter add chain=forward src-address-list=”IP Client” content=.iso action=”drop”

- setelah itu kita cek menggunakan **ip firewall filter print**

(LAB)Address List

- Kita bisa lihat diatas, di bagian src-address kita tidak perlu lagi masukkan IP Address dari pc admin, melainkan kita hanya perlu masukkan nama Address List nya saja. Address List juga bisa digunakan untuk memblokir website. Caranya sama seperti tadi, kita buat dulu Address List dari website yang ingin kita blok. Cara lengkapnya bisa lihat dibawah ini :
- Misalkan, kita akan blokir website kompas.com menggunakan Address List. Pertama kita cek dulu IP Address kompas.com menggunakan nslookup.



- Bisa kita lihat diatas, kalau kompas.com mempunyai 2 IP address. Jadi, kita harus membuat 2 Address List kompas dengan nama yang sama. untuk perintah text, perintah nya adalah

ip firewall address-list add address=202.146.4.100 list=”IP Kompas”

ip firewall address-list add address=202.61.113.35 list=”IP Kompas”

- setelah itu cek dengan perintah ip firewall address-list print

(LAB)Address List

```
[admin@Rangga] > ip firewall address-list add address=202.146.4.100 list="IP Kompas"
[admin@Rangga] > ip firewall address-list add address=202.61.113.35 list="IP Kompas"
[admin@Rangga] > ip firewall address-list print
Flags: X - disabled, D - dynamic
 #    LIST                                                              ADDRESS                                  TIMEOUT
 0    IP Admin                                                          13.13.13.2
 1    IP Client                                                         13.13.13.0/24
 2    IP Kompas                                                         202.146.4.100
 3    IP Kompas                                                         202.61.113.35
```

- Setelah kita buat address list nya, sekarang kita buat rule perintah drop nya. Perintah text nya adalah

ip firewall filter add chain=forward dst-address-list=”IP Kompas” action=drop

```
[admin@Rangga] > ip firewall filter add chain=forward dst-address-list="IP Kompas" action=drop
[admin@Rangga] > ip firewall filter pr
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=forward action=accept src-address-list=IP Admin log=no log-prefix=""

 1    chain=forward action=drop src-address-list=IP Client content=.iso log=no log-prefix=""

 2    chain=forward action=drop dst-address-list=IP Kompas log=no log-prefix=""
```

Address List Test

- Jika ada firewall rule yang sebelumnya, kita pindahkan dulu rule yang kita buat ke urutan atas

```
[admin@Rangga] > ip firewall filter move 2 0
[admin@Rangga] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=forward action=drop dst-address-list=IP Kompas log=no log-prefix=""

 1    chain=forward action=accept src-address-list=IP Admin log=no log-prefix=""

 2    chain=forward action=drop src-address-list=IP Client content=.iso log=no log-prefix=""
```

- sekarang, coba kalian buka kompas.com, maka website tersebut tidak akan terbuka dan hanya loading terus menerus karena sudah kita drop.

```
C:\Users\Windows 8>ping kompas.com

Pinging kompas.com [202.146.4.100] with 32 bytes of data:
Request timed out.
```

(LAB)Address List

- Untuk mengganti IP Address dari Address List tadi yang kita buat, bisa dilakukan dengan perintah text : **ip firewall address-list set [no index address list] address=[ip pengganti]** untuk contoh, disini saya akan mengganti IP Admin dengan nomor index (urutan) 0 dengan IP 13.13.13.3. berarti perintah text nya adalah

```
[admin@Rangga] > ip firewall address-list print
Flags: X - disabled, D - dynamic
 #   LIST                                              ADDRESS                                 TIMEOUT
 0   IP Admin                                          13.13.13.2
 1   IP Client                                         13.13.13.0/24
```

ip firewall address-list set 0 address=13.13.13.3

- untuk mengeceknya ketik **ip firewall address-list print**

```
[admin@Rangga] > ip firewall address-list set 0 address=13.13.13.3
[admin@Rangga] > ip firewall address-list print
Flags: X - disabled, D - dynamic
 #   LIST                                              ADDRESS                                 TIMEOUT
 0   IP Admin                                          13.13.13.3
 1   IP Client                                         13.13.13.0/24
```

(LAB)Address List

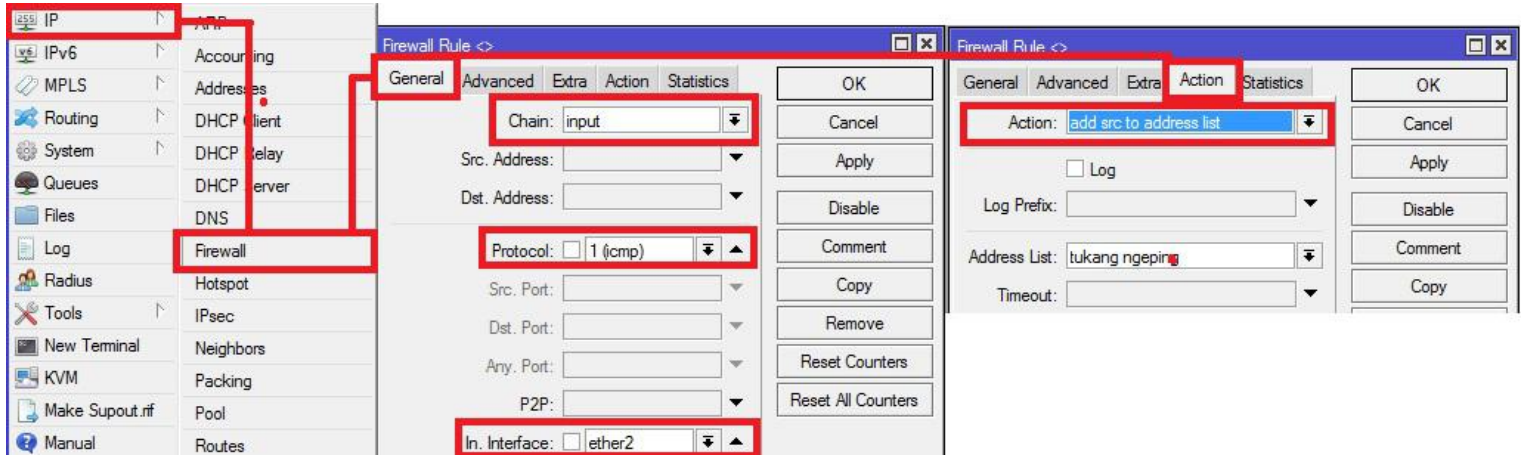
- IP address telah diganti. Jadi, misalkan sewaktu-waktu pc admin mengganti IP addressnya, kita hanya tinggal merubahnya di Address List, tidak perlu mengkonfigurasi ulang rule firewall nya.
- Address List juga bisa digunakan untuk menambahkan IP Address dari computer yang mencoba melakukan ping kepada router. Perintah text nya adalah :

ip firewall filter add chain=input in-interface=ether2 protocol=icmp action=add-src-to-address-list address-list=”tukang ngeping”

```
[admin@Rangga] > ip firewall filter add chain=input in-interface=ether2 protocol=icmp action=add-src-to-address-list
 address-list="tukang ngeping"
```

Jika melalui winbox (GUI) masuk ke menu IP Firewall Filter Rules + lalu konfigurasi kan sebagai berikut : (di tab **General, chain=input, in-interface=ether2, protocol=icmp** , sekarang masuk ke tab **Action , action=add-src-to-address-list, address list=tukang ngeping**

Address List Test



- Sekarang, coba kalian ping menggunakan user client, setelah itu kita cek Address List nya **(ip address-list print)** maka, IP Address yang ngeping ke router kalian akan di tambahkan dengan nama tukang ngeping.

```
C:\Users\Windows 8>ping 13.13.13.1

Pinging 13.13.13.1 with 32 bytes of data:
Reply from 13.13.13.1: bytes=32 time<1ms TTL=64
```

Address List Test

```
[admin@Rangga] > ip firewall address-list print
Flags: X - disabled, D - dynamic
 #   LIST                                            ADDRESS                                 TIMEOUT
 0   IP Admin                                        13.13.13.3
 1   IP Client                                       13.13.13.0/24
 2   IP Kompas                                       202.146.4.100
 3   IP Kompas                                       202.61.113.35
 4 D tukang ngeping                                  13.13.13.2
```

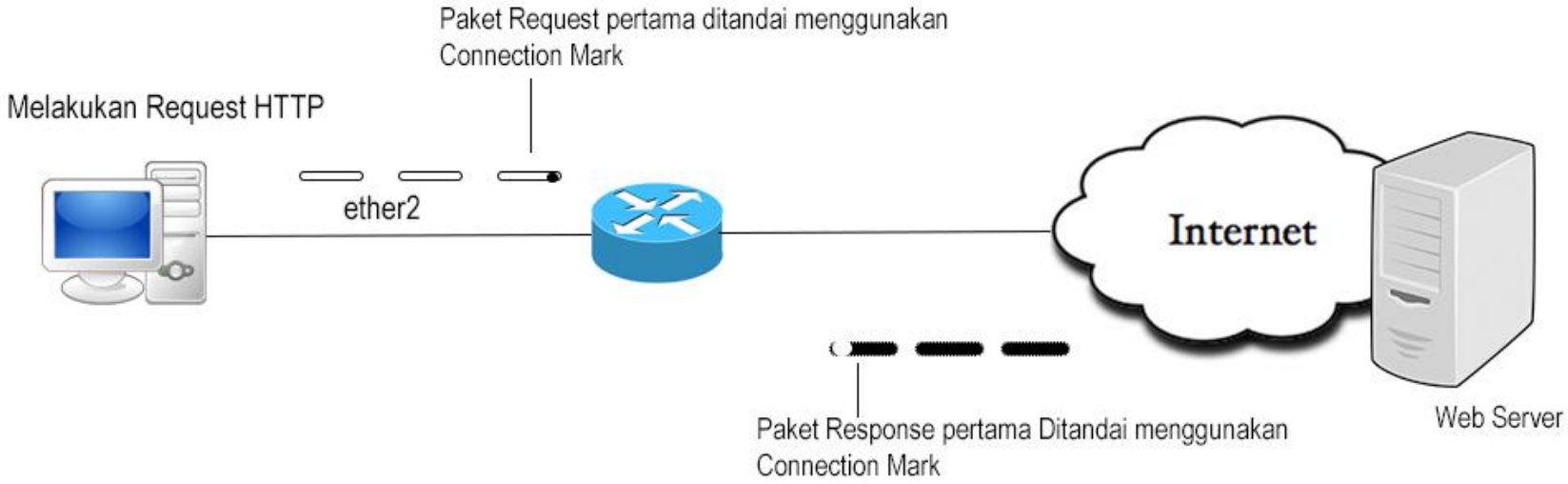
- Bisa kita lihat diatas, ada address list baru yang bernama tukang ngeping. Jika kita lihat sebelah kiri, ada huruf D yang berarti Dynamic atau Automatis

Firewall Mangle

- Firewall Mangle fungsinya untuk memberi tanda (mark) pada paket data dan koneksi tertentu. Tujuan nya sendiri adalah agar paket data lebih mudah dikenali. Dengan menggunakan Firewall Mangle (Marking) pada Router MikroTik ini, akan memudahkan dalam mengelola sebuah paket data. Misalnya, menerapkan marking pada firewall filter, NAT, Routing. Fitur Mangle ini hanya bisa digunakan pada router MikroTik itu sendiri dan tidak dapat digunakam oleh router lain. Karena marking tersebut akan dilepas pada saat paket data akan keluar / meninggalkan router.
- Di dalam Firewall Mangle ini, ada 3 jenis Marking yang bisa kita gunakan, yaitu
  - **Connection Mark** (Penandaan pada Koneksi)
  - **Packet Mark** (Penandaan pada paket data)
  - **Routing Mark** (Penandaan pada Routing)
- Kita langsung saja pada pembahasan marking yang pertama, yaitu Connection Mark

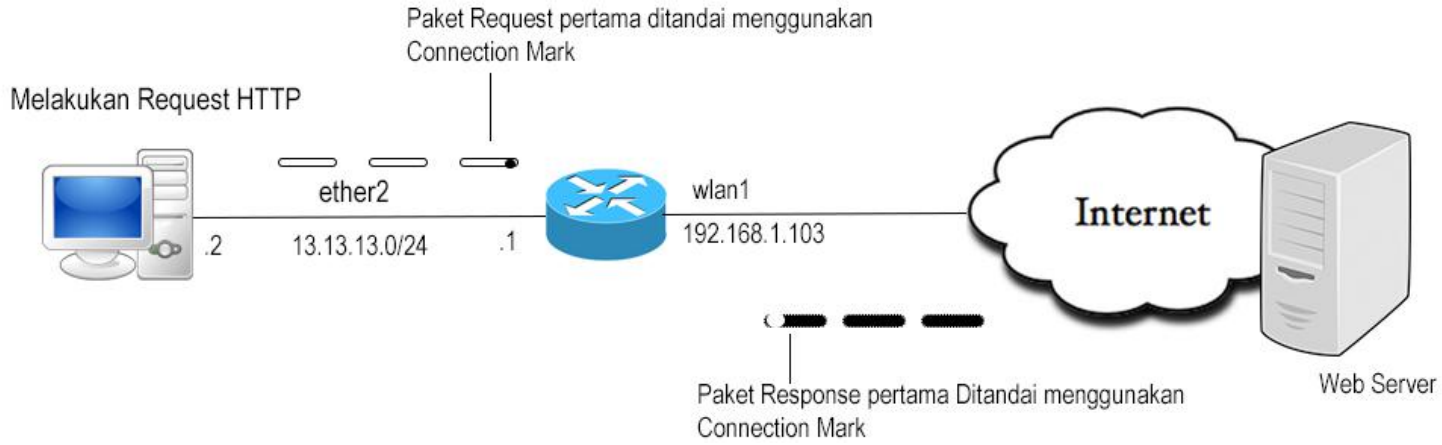
Connection Mark

- Seperti yang saya jelaskan sebelumnya, Connection Mark ini berfungsi untuk menandai sebuah Koneksi. Connection Mark bisa digunakan untuk memberikan tanda atau marking pada paket pertama yang dikeluarkan oleh Client ataupun Paket Response yang pertama dikeluarkan oleh Web Server



Connection Mark

- Bisa kita lihat gambar diatas, Client melakukan Request HTTP terhadap suatu Web Server. Terlihat pada gambar diatas, Request dari Client tersebut memiliki 3 paket, pada connection mark ini yang ditandai adalah paket yang pertama keluar dari Client, untuk paket ke dua dan ke tiga tidak ditandai. Begitu juga pada paket Response dari Web Server, paket yang pertama keluar dari Web Server tersebut yang akan ditandai.
- Sekarang, kita akan melakukan percobaan. Kita akan melakukan konfigurasi Connection Mark pada topologi dibawah ini :



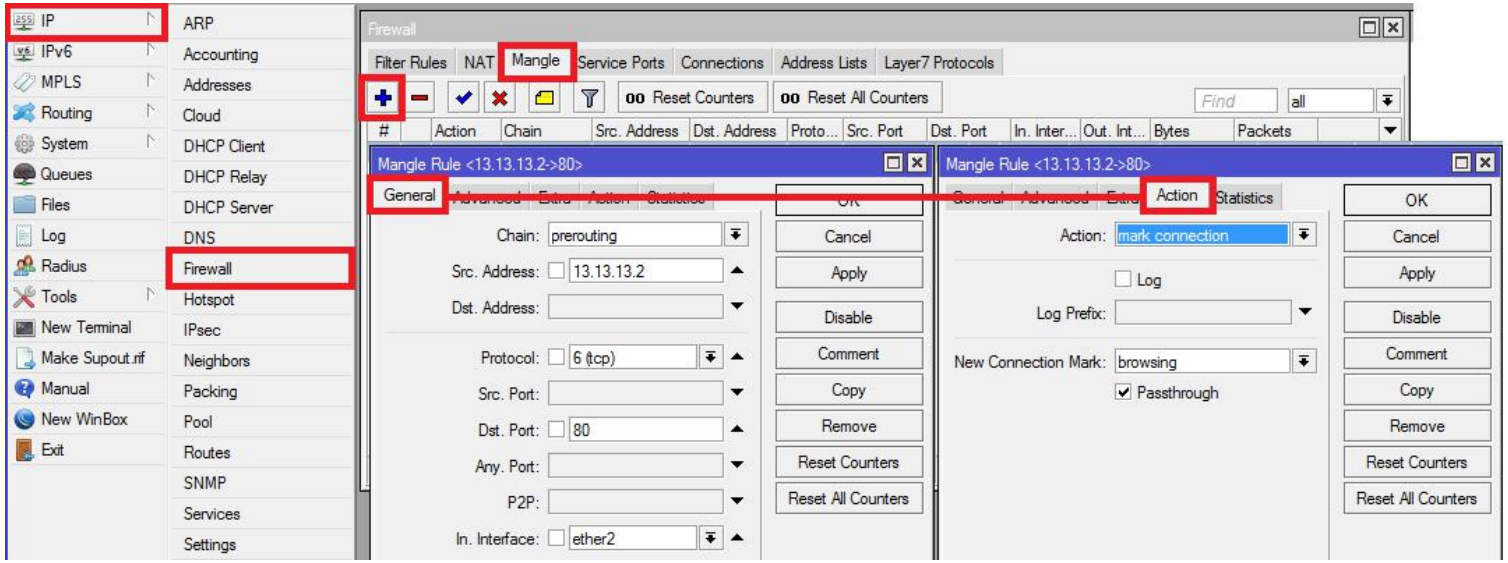
(LAB)Connection Mark

- Kita akan melakukan Connection Marking pada interface ether2 yang melakukan aktifitas browsing HTTP. Perintah text (CLI) nya adalah sebagai berikut
- **ip firewall mangle add chain=prerouting src-address=13.13.13.2 protocol=tcp dst-port=80 in-interface=ether2 action=mark-connection new-connection-mark=browsing**
- Keterangan :
  - **chain=prerouting =** chain yang digunakan untuk melakukan marking pada paket yang akan keluar / melintasi router
  - **src-address =** sumber yang mengeluarkan paket
  - **protocol=tcp port=80** = karena kita akan melakukan marking pada aktifitas HTTP, maka menggunakan protocol tcp dan port HTTP yaitu 80
  - **in-interface=ether2 =** masuk melalui interface ether2
  - **action=mark-connection=** untuk menandai koneksi
  - **new-connection-mark=browsing =** nama

```
[admin@Mikrotik2] > ip firewall mangle add chain=prerouting src-address=13.13.13.2 protocol=tcp dst-port=80
 in-interface=ether2 action=mark-connection new-connection-mark=browsing
[admin@Mikrotik2] > ip firewall mangle print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=prerouting action=mark-connection new-connection-mark=browsing passthrough=yes protocol=tcp
      src-address=13.13.13.2 in-interface=ether2 dst-port=80 log=no log-prefix=""
```

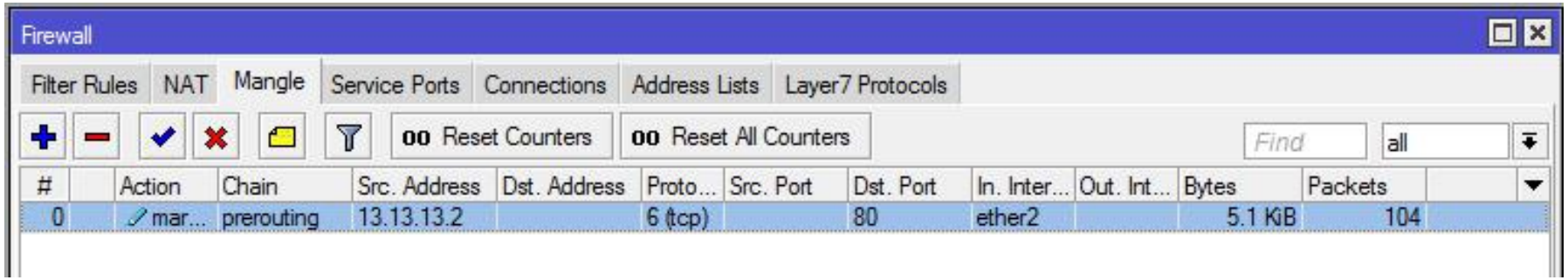
(LAB)Connection Mark

- Jika melalui Winbox (GUI), klik menu IP **Firewall** tab **Mangle** + (add) lalu lakukan konfigurasi seperti gambar dibawah ini



- Untuk melakukan pengecekan, bisa kita lihat pada menu IP Firewall Mangle< lalu lihat di bagian Packets. Setelah itu, kita test melakukan browsing, misalnya membuka website intra.id

(LAB)Connection Mark



- Bisa kita lihat dibagian Packets , PC Client membuat beberapa koneksi saat membuka website tersebut. Koneksi tersebut digunakan untuk membuka content misalnya gambar atau link pada website tersebut.
- Kita juga bisa melakukan marking sesuai dengan content yang diakses user. Misalnya, melakukan connection marking pada content file berekstensi .rar. Untuk melakukan konfigurasi nya hampir sama seperti sebelumnya. Hanya saja, disini kita akan menambahkan perintah content. Langsung saja ke langkah konfigurasi nya :

(LAB)Connection Mark

ip firewall mangle add chain=prerouting src-address=13.13.13.2 protocol=tcp port=80 content=.rar action=mark-connection new-connection-mark=download_rar

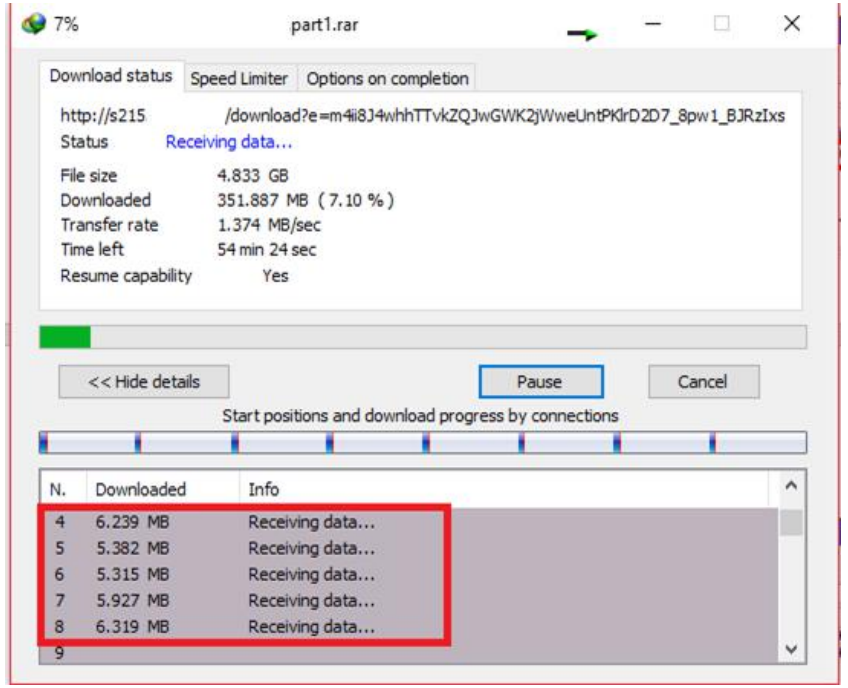
- Kita cek menggunakan perintah **ip firewall mangle print detail**

```
[admin@Mikrotik2] > ip firewall mangle add chain=prerouting src-address=13.13.13.2 protocol=tcp dst-port=80
 content=.rar action=mark-connection new-connection-mark=download_rar
[admin@Mikrotik2] > ip firewall mangle print detail
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=prerouting action=mark-connection new-connection-mark=browsing passthrough=yes protocol=tcp
      src-address=13.13.13.2 in-interface=ether2 dst-port=80 log=no log-prefix=""

 1    chain=prerouting action=mark-connection new-connection-mark=download_rar passthrough=yes
      protocol=tcp src-address=13.13.13.2 dst-port=80 content=.rar log=no log-prefix=""
```

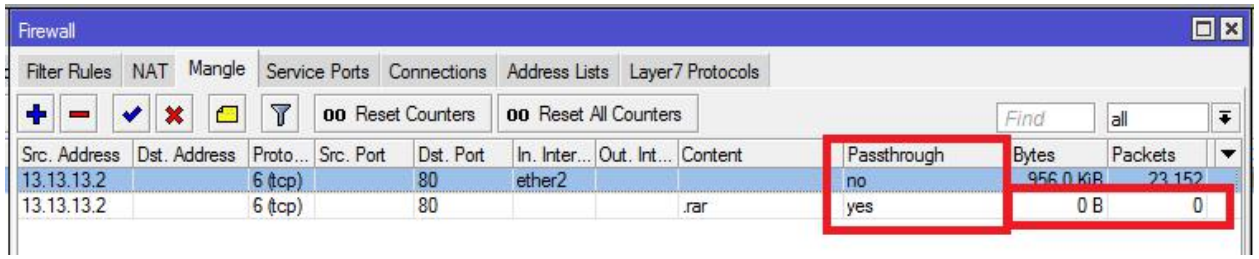
- Kita juga perlu memperhatikan perintah passtrough, jika passtrough pada rule pertama (0) adalah no , maka marking pada paket data tidak akan dilanjutkan pada rule selanjutnya. Jika passtrough=yes marking akan dilanjutkan pada rule selanjutnya. Agar lebih jelas, kita akan coba melakukan download file berekstensi rar.

Connection Mark Test

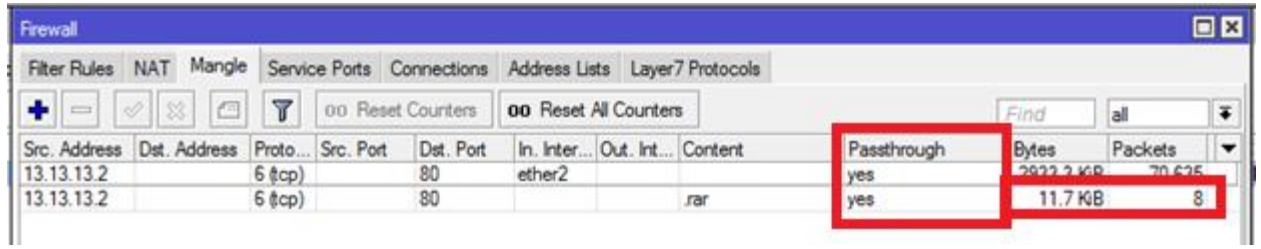
- IDM membuat 8 Koneksi pada saat mendownload file di samping



- Jika passtrough pada rule pertama (no index 0) adalah no

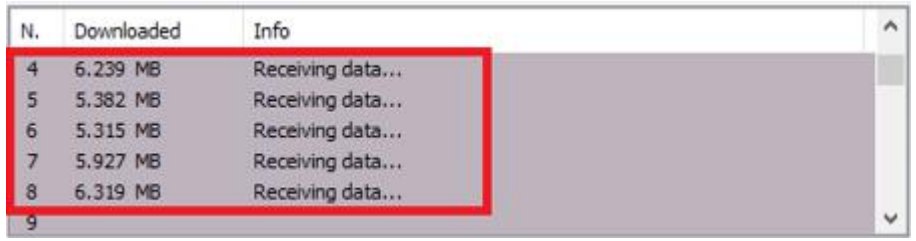


- Jika passtrough pada rule pertama (no index 0) adalah yes



Connection Mark Test

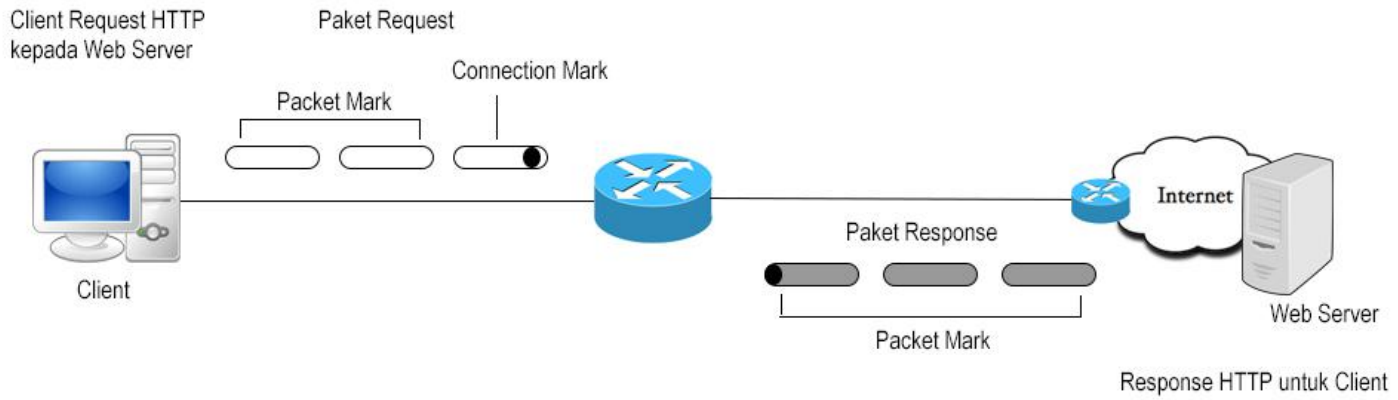
- Bisa kita lihat perbandingan diatas, rule ke 2 akan “menangkap” 8 paket (melakukan connection mark) pada saat client mendownload file rar jika parameter passtrough adalah yes. Berbeda jika pada rule pertama perintah passtrough nya adalah no.
- Jika kita lihat pada gambar diatas, kita melakukan test download menggunakan Internet Download Manager. Jika kita mendownload menggunakan IDM ini, nantinya download manager tersebut akan membuat beberapa koneksi seperti seperti gambar dibawah ini.



- Jika salah satu koneksi tersebut telah selesai mendownload, maka IDM akan membuat koneksi baru, dan pada Counter Packet connection mark juga akan bertambah sesuai dengan koneksi yang dibuat oleh download manager

Packet Mark

- Setelah kita membahas tentang Connection Mark, sekarang kita akan ke pembahasan selanjutnya, yaitu Packet Mark. Packet Mark sendiri berfungsi untuk melakukan marking pada paket data. Jika tadi Connection Mark hanya melakukan Marking pada paket yang pertama keluar dari Router, maka Packet Mark berfungsi untuk menandai paket paket selanjutnya. Agar lebih jelas, bisa lihat gambar dibawah ini :



Packet Mark

- Bisa kita lihat gambar diatas, Client melakukan Request HTTP kepada Web Server. Pada Request Client tersebut, Client mengirimkan 3 paket data (Traffic Upload). Paket pertama, ditandai atau di marking menggunakan Connection Mark, lalu paket selanjutnya ditandai / di marking menggunakan Packet Mark. Lalu Web Server meresponse dengan mengirim 3 paket data (Traffic Download) pada client. Pada gambar diatas, kita akan melakukan 3 konfigurasi Firewall Mangle, yaitu Connection Mark, Packet Mark untuk Traffic Upload dan Packet Mark untuk Traffic Download.
- Sekarang, kita akan mencoba melakukan konfigurasi Marking pada topologi dibawah ini

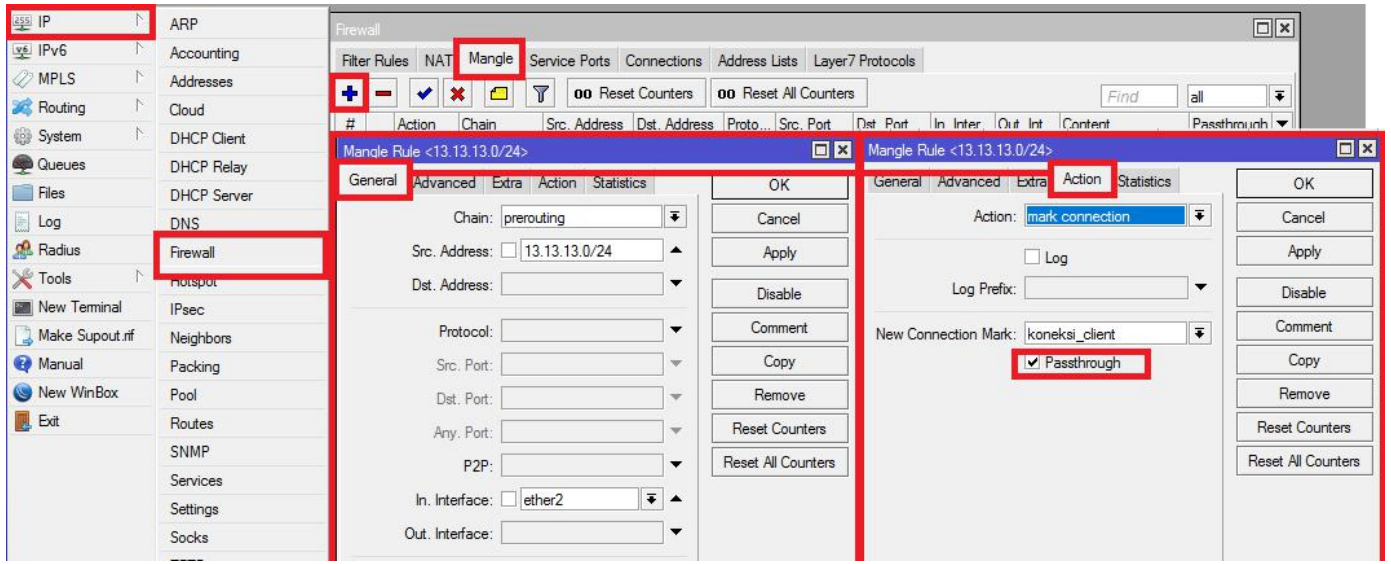
(LAB)Packet Mark

- Bisa lihat gambar diatas, Router mempunyai 1 Client melalui Interface ether2 lalu Router terhubung dengan internet melalui interface wlan1. Disini kita akan melakukan Marking pada Traffic Upload dan Download yang dilakukan oleh Client.
- Untuk langkah pertama, kita akan lakukan konfigurasi Connection Mark untuk komputer Client dengan IP Network 13.13.13.0/24 yang terhubung melalui interface ether2. Konfigurasinya adalah sebagai berikut
- Jika melalui perintah text (CLI), perintahnya adalah

ip firewall mangle add chain=prerouting src-address=13.13.13.0/24 in-interface=ether2 action=mark-connection new-connection-mark=koneksi_client passthrough=yes

- Jika melalui WInbox (GUI) klik pada meu IP Firewall Mangle + (add) lalu lakukan konfigurasi seperti perintah diatas, atau bisa lihat gambar dibawah ini

(LAB)Packet Mark



- Setelah melakukan konfigurasi Connection Mark, sekarang kita lakukan konfigurasi Packet Mark untuk Traffic Upload. Yang perlu diperhatikan pada konfigurasi ini adalah perintah text mark-connection kita isi dengan menggunakan connection mark yang tadi kita buat, yaitu koneksi_client. Lalu pada bagian in-interface kita isi dengan ether2 karena PC Client terhubung melalui interface ether2, jadi traffic upload akan masuk melalui interface tersebut. Dan perintah passthrough kita isi dengan no agar packet mark tidak dilanjutkan kepada rule selanjutnya

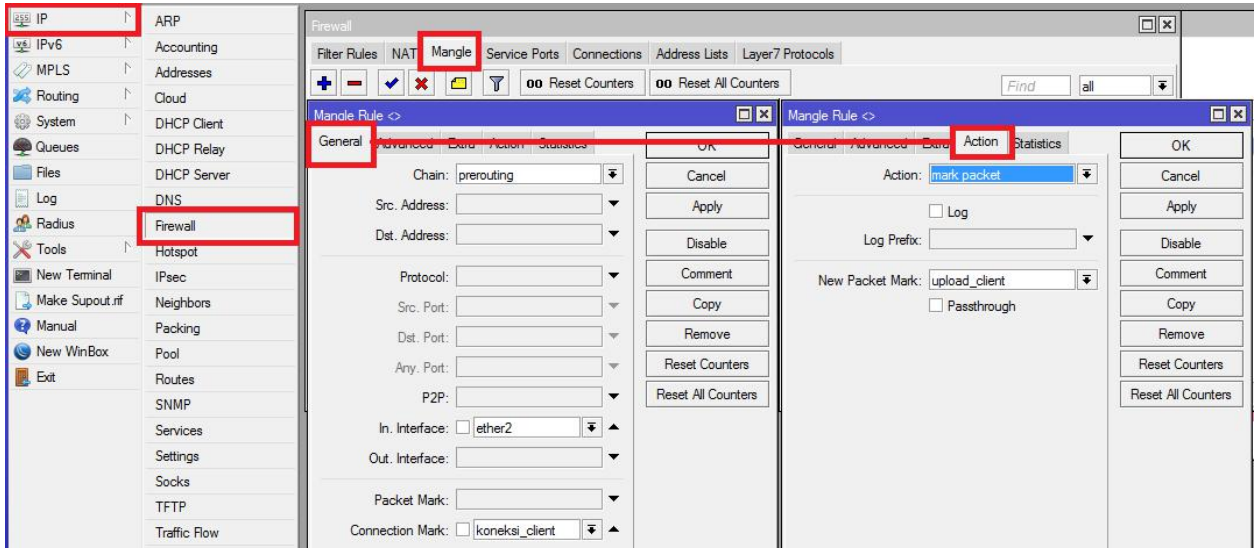
(LAB)Packet Mark

- Perintah text (CLI) nya adalah

ip firewall mangle add chain=prerouting in-interface=ether2 connection-mark=koneksi_client action=mark-packet new-packet-mark=upload_client passthrough=no

```
[admin@Mikrotik2] > ip firewall mangle add chain=prerouting in-interface=ether2 connection-mark=koneksi_client
 action=mark-packet new-packet-mark=upload_client passthrough=no
```

Jika melalui WInbox (GUI) klik pada menu IP Firewall Mangle + (add) lalu buat konfigurasi seperti perintah text diatas atau bisa lihat gambar dibawah ini

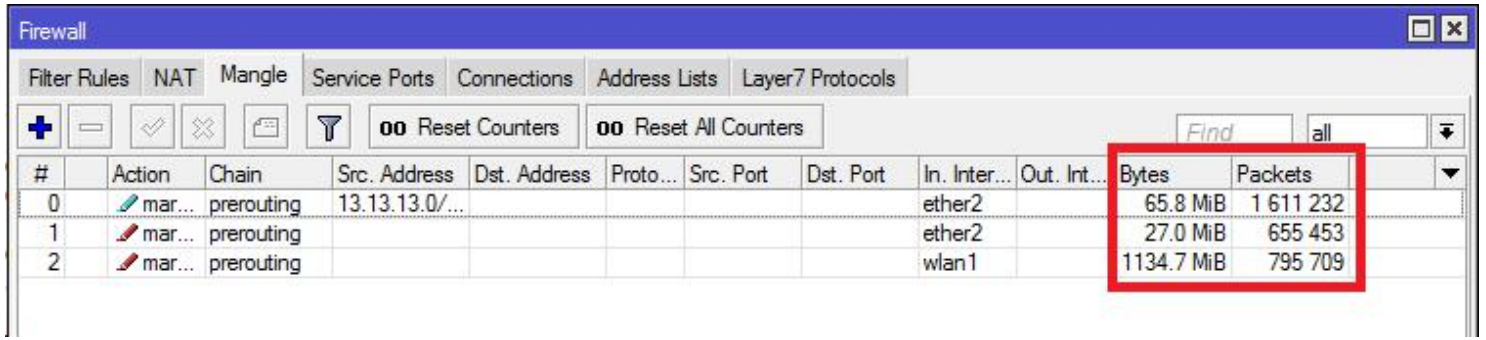


(LAB)Packet Mark

- Setelah ketiga rule tersebut dibuat, sekarang kita cek menggunakan perintah text (CLI) **ip firewall mangle print**

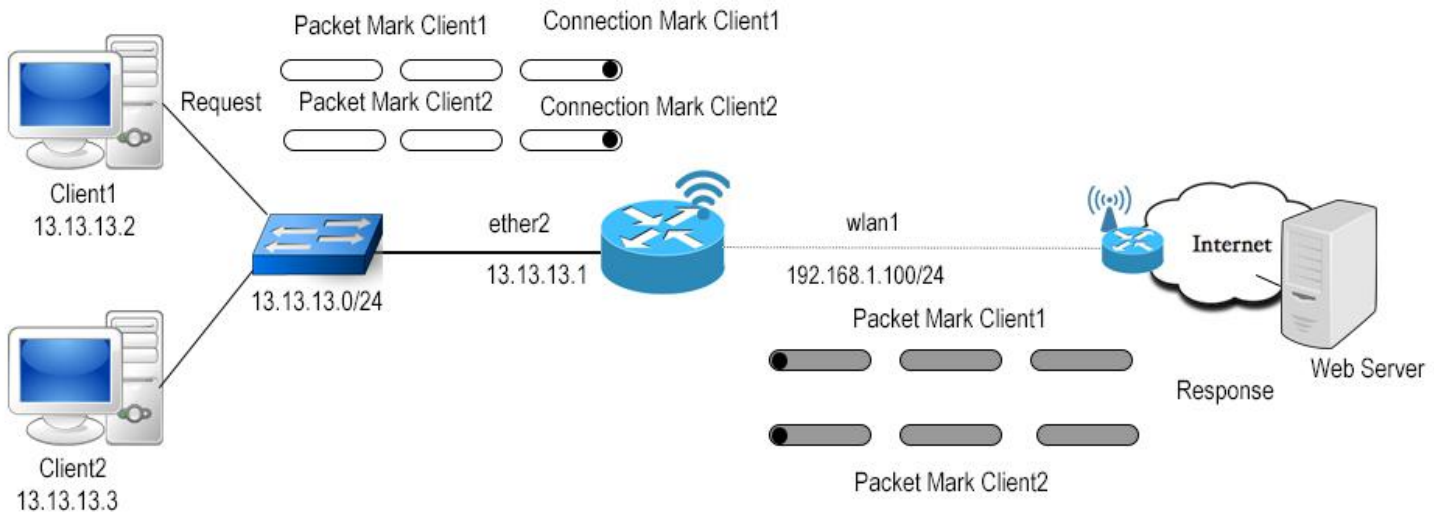
```
[admin@Mikrotik2] > ip firewall mangle print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=prerouting action=mark-connection new-connection-mark=koneksi_client passthrough=yes
      src-address=13.13.13.0/24 in-interface=ether2 log=no log-prefix=""

 1    chain=prerouting action=mark-packet new-packet-mark=upload_client passthrough=no in-interface=ether2
      connection-mark=koneksi_client log=no log-prefix=""

 2    chain=prerouting action=mark-packet new-packet-mark=download_client passthrough=no in-interface=wlan1
      connection-mark=koneksi_client log=no log-prefix=""
```

- Untuk melakukan Monitoring aktifitas download dan upload pada client, bisa dilihat melalui Winbox (GUI) pada menu **IP Firewall Mangle**



Packet Mark Test

- Bisa kita lihat diatas, dibagian Bytes terlihat jumlah/ukuran download dan upload yang dilakukan oleh Client pada network 13.13.13.0/24. Dan dibagian Packet terlihat packet traffic upload dan traffic download.
- Konfigurasi Marking diatas sudah selesai. Sekarang, bagaimana cara untuk melakukan marking pada PC Client 1 per 1? Agar lebih jelas, kita lihat gambar topologi dibawah ini



(LAB)Packet Mark + Mark Connection

- Untuk melakukan marking pada topologi diatas, kita hanya perlu melakukan konfigurasi marking 1 per 1 untuk client tersebut. Langsung saja kita mulai konfigurasi marking untuk client dengan IP 13.13.13.2
- Jika melalui perintah text (CLI), maka perintahnya adalah sebagai berikut
  - Konfigurasi Connection Mark Client 1

ip firewall mangle add chain=prerouting src-address=13.13.13.2 in-interface=ethernet2 action=mark-connection new-connection-mark=koneksi_client1 passthrough=yes

  - Konfigurasi Packet Mark traffic upload Client 1

ip firewall mangle add chain=prerouting in-interface=ether2 connection-mark=koneksi_client1 action=mark-packet new-packet-mark=upload_client1 passthrough=no

  - Konfigurasi Packet Mark Traffic Download Client 1

ip firewall mangle add chain=prerouting in-interface=wlan1 connection-mark=koneksi_client1 action=mark-packet new-packet-mark=download_client1 passthrough=no

(LAB)Packet Mark + Mark Connection

- Setelah itu, Kita cek menggunakan perintah **ip firewall mangle print detail**

```
[admin@Mikrotik2] > ip firewall mangle print detail
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=prerouting action=mark-connection new-connection-mark=koneksi_client1 passthrough=yes src-address=13.13.13.2 in-interface=ether2 log=no log-prefix=""

 1    chain=prerouting action=mark-packet new-packet-mark=upload_client1 passthrough=no in-interface=ether2 connection-mark=koneksi_client1 log=no log-prefix=""

 2    chain=prerouting action=mark-packet new-packet-mark=download_client1 passthrough=no in-interface=wlan1 connection-mark=koneksi_client1 log=no log-prefix=""
```

- Sekarang kita akan mengkonfigurasi marking untuk client 2 (13.13.13.3)
- Jika melalui perintah text (CLI)
  - Konfigurasi Connection Mark Client 2

ip firewall mangle add chain=prerouting src-address=13.13.13.3 in-interface=ether2 action=mark-connection new-connection-mark=koneksi_client2 passthrough=yes

  - Konfigurasi Packet Mark Traffic Upload Client 2

ip firewall mangle add chain=prerouting in-interface=ether2 connection-mark=koneksi_client2 action=mark-packet new-packet-mark=upload_client2 passthrough=no

  - Konfigurasi Packet Mark Traffic Download Client 2

ip firewall mangle add chain=prerouting in-interface=wlan1 connection=mark=koneksi_client2 action=mark-packet new-packet-mark=download_client2 passthrough=no

(LAB)Packet Mark

```
[admin@Mikrotik2] > ip firewall mangle add chain=prerouting src-address=13.13.13.3 in-interface=ether2 action=mark-connection new-connection-mark=koneksi_client2
passthrough=yes
[admin@Mikrotik2] > ip firewall mangle add chain=prerouting in-interface=ether2 connection-mark=koneksi_client2 action=mark-packet new-packet-mark=upload_client2
passthrough=no
[admin@Mikrotik2] > ip firewall mangle add chain=prerouting in-interface=wlan1 connection-mark=koneksi_client2 action=mark-packet new-packet-mark=download_client2
 passthrough=no
```

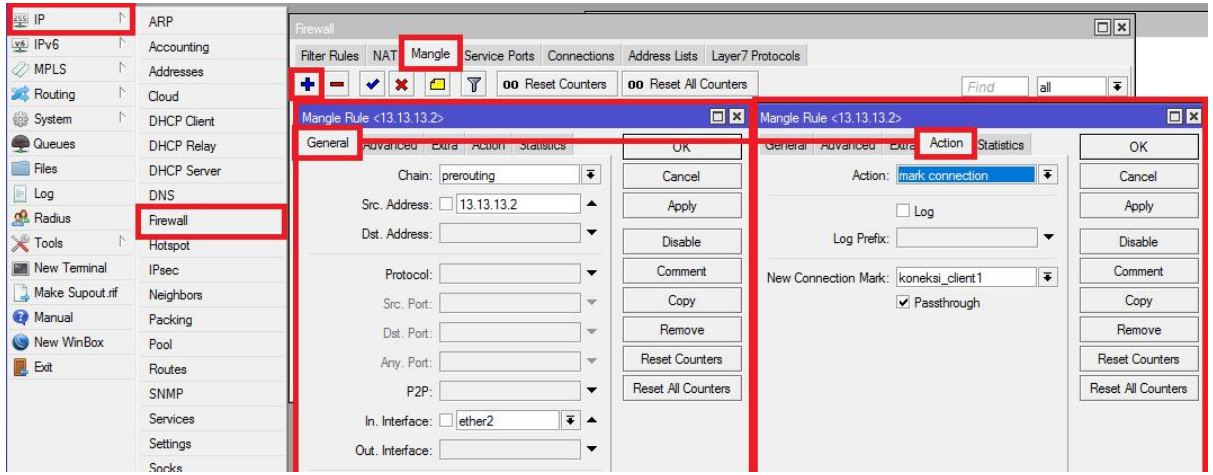
- Setelah itu, kita cek semua rule firewall mangle yang telah kita buat dengan menggunakan perintah **ip firewall mangle print detail**

```
[admin@Mikrotik2] > ip firewall mangle print detail
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=prerouting action=mark-connection new-connection-mark=koneksi_client1 passthrough=yes src-address=13.13.13.2 in-interface=ether2 log=no log-prefix=""

 1    chain=prerouting action=mark-packet new-packet-mark=upload_client1 passthrough=no in-interface=ether2 connection-mark=koneksi_client1 log=no log-prefix=""

 2    chain=prerouting action=mark-packet new-packet-mark=download_client1 passthrough=no in-interface=wlan1 connection-mark=koneksi_client1 log=no log-prefix=""

 3    chain=prerouting action=mark-connection new-connection-mark=koneksi_client2 passthrough=yes src-address=13.13.13.3 in-interface=ether2 log=no log-prefix=""

 4    chain=prerouting action=mark-packet new-packet-mark=upload_client2 passthrough=no in-interface=ether2 connection-mark=koneksi_client2 log=no log-prefix=""

 5    chain=prerouting action=mark-packet new-packet-mark=download_client2 passthrough=no in-interface=wlan1 connection-mark=koneksi_client2 log=no log-prefix=""
```

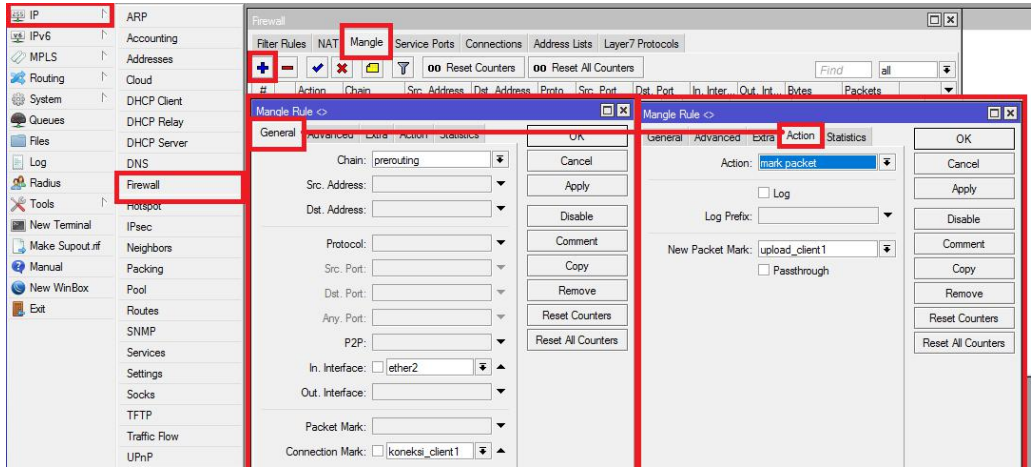
- Jika kalian ingin menggunakan Winbox (GUI) untuk mengkonfigurasi Firewall Mangle, bisa dengan klik pada menu IP Firewall Mangle + (Add) lalu konfigurasikan seperti perintah text diatas

(LAB)Packet Mark + Mark Connection

- Mark Connection

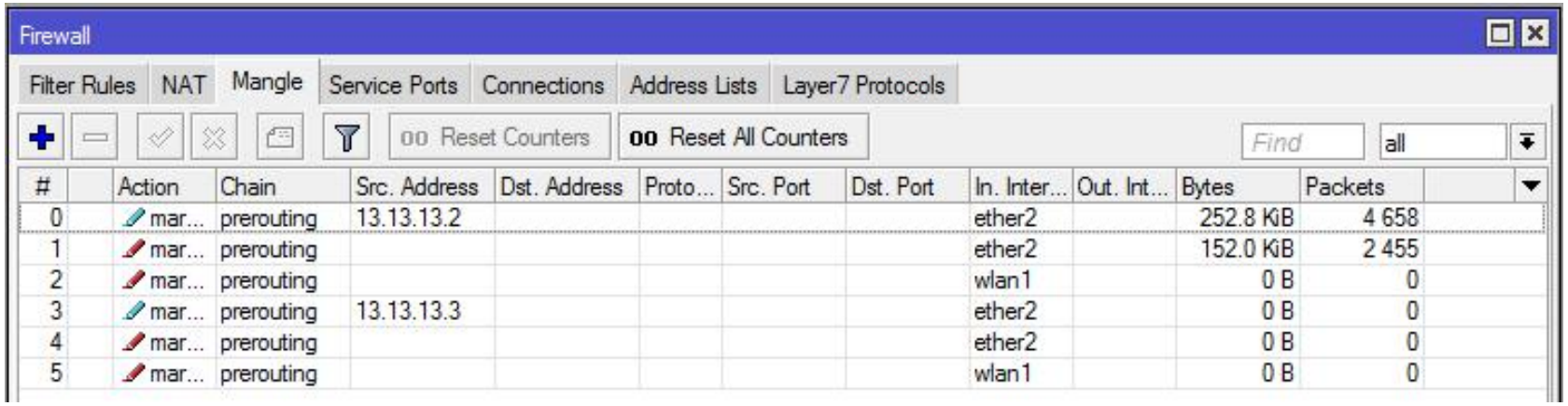


- Packet Mark



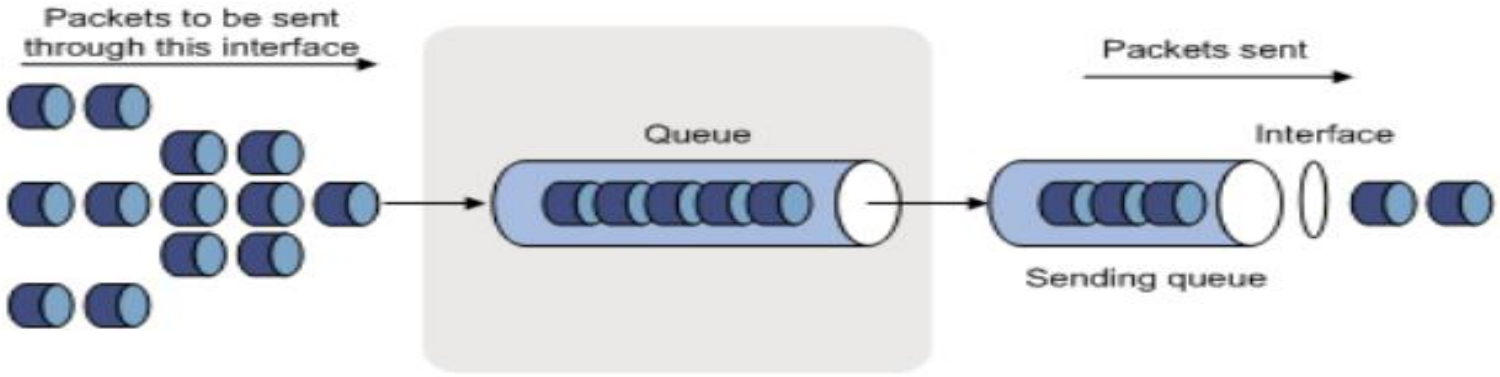
Firewall Mangle Monitoring Test

- Konfigurasi diatas sudah selesai. Sekarang, untuk melakukan monitoring, bisa kita lihat melalui Winbox (GUI) IP Firewall Mangle



Quality of Service

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



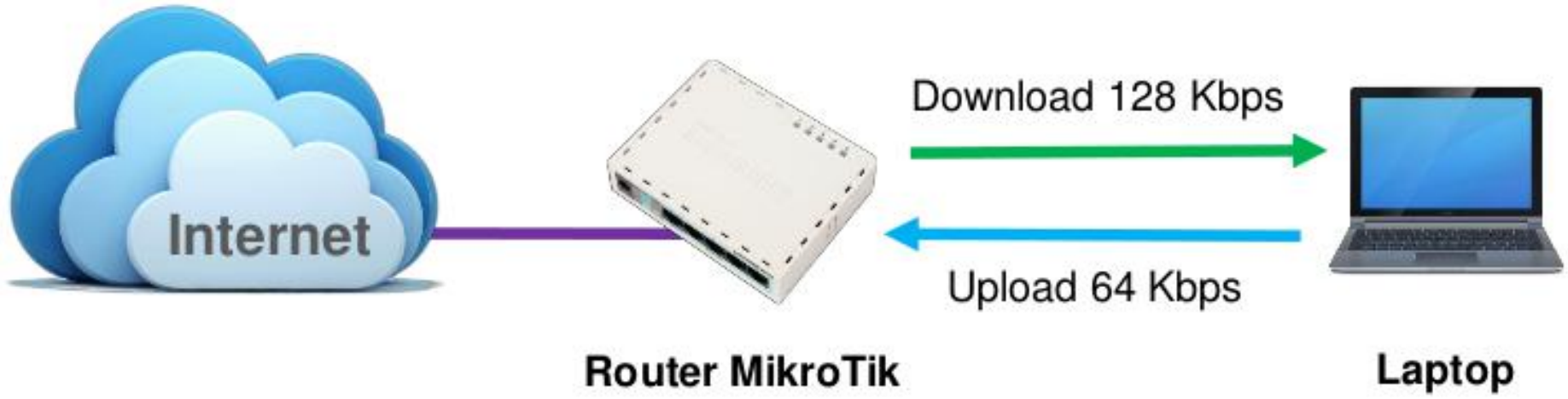
Fitur Simple Queue

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

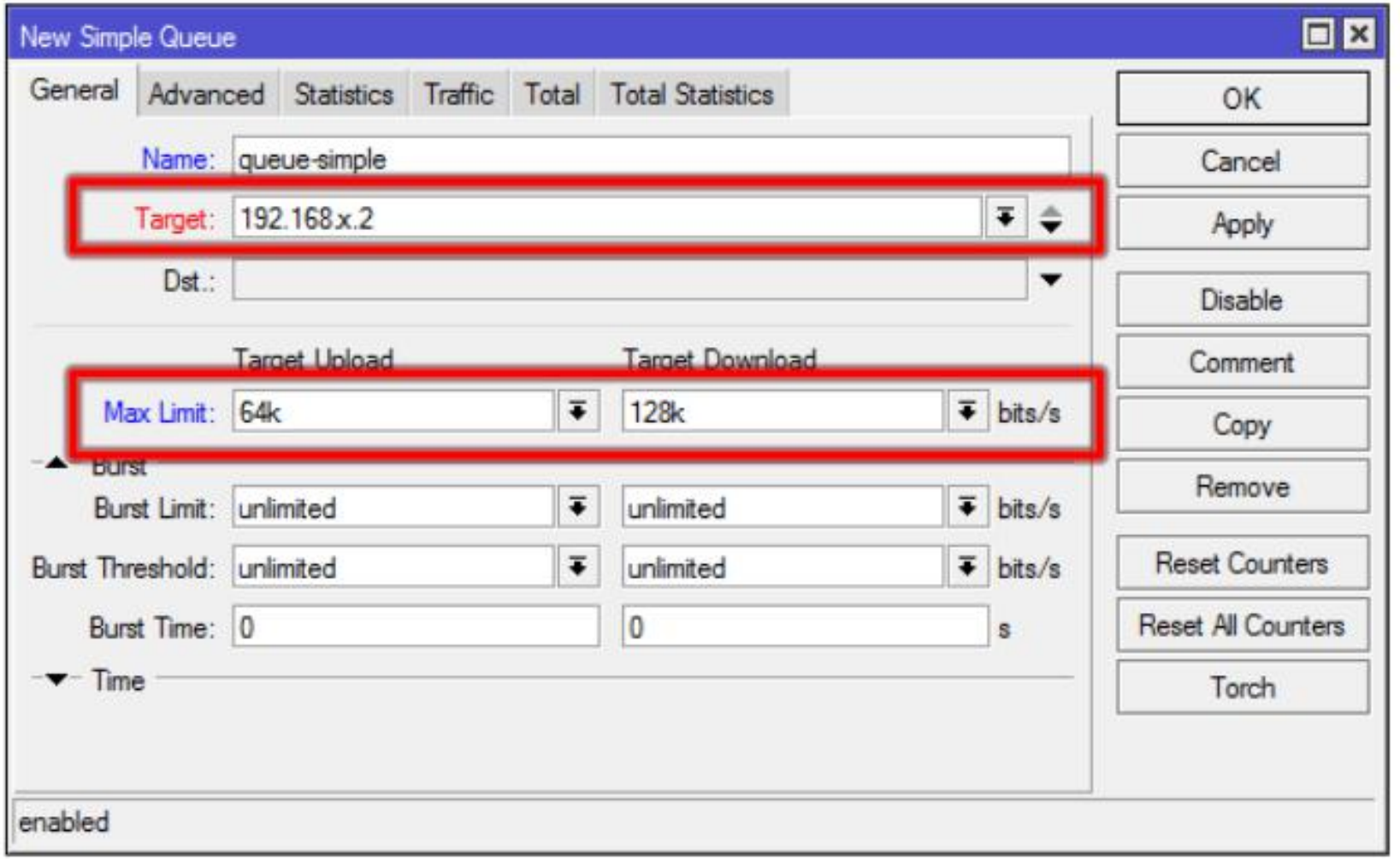
(LAB)Simple Queue

Make a simple queue for your laptop

- Downstream : 128 kbps
- Upstream : 64 kbps



(LAB)Simple Queue



Simple Queue Target

- Target Address harus diisi
- Parameter target address bisa berupa IP Address, Interface, dan Network
- Multiple Target Address untuk target yang lebih dari satu

Simple Queue Max Limit

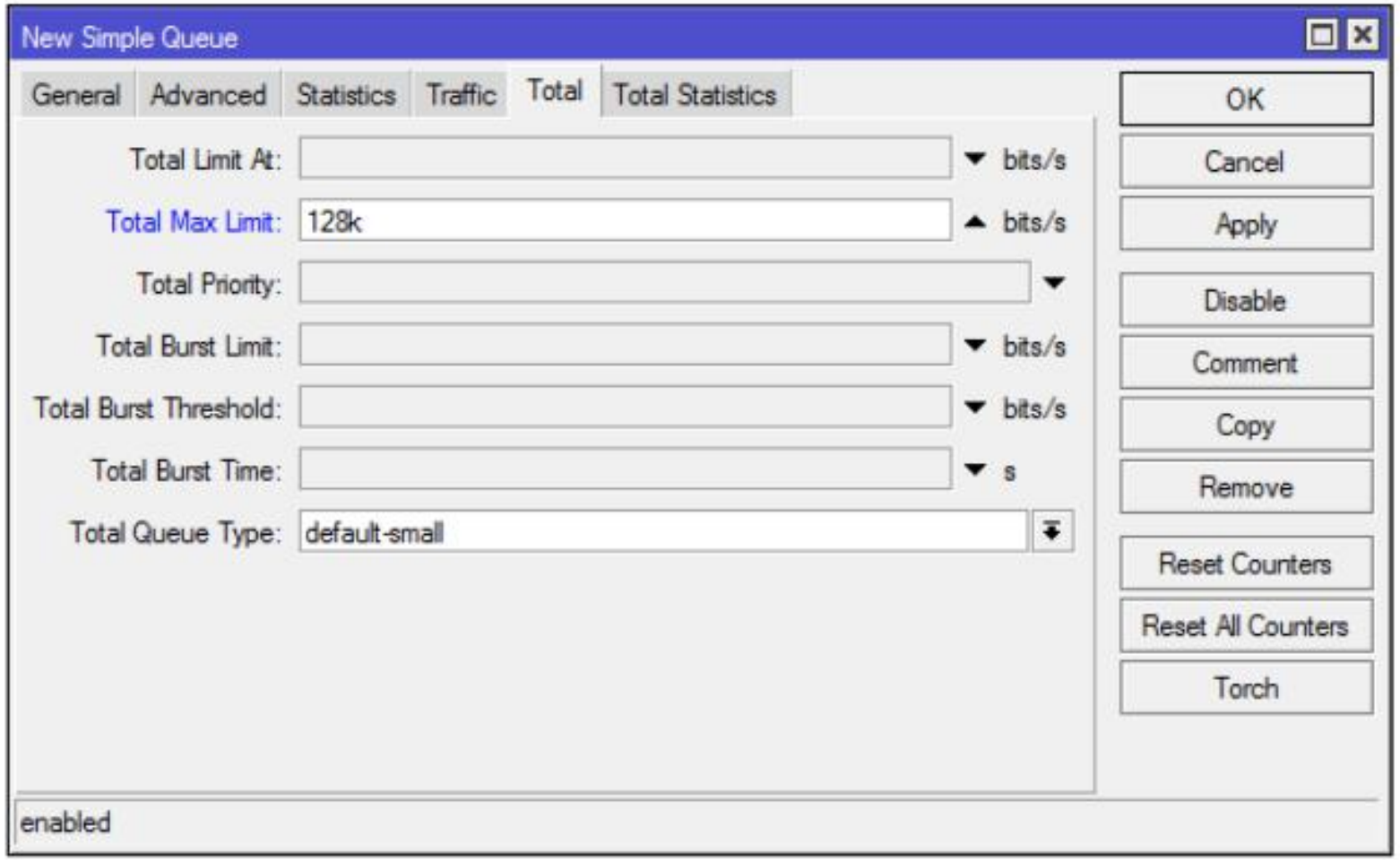
- Sebaiknya harus ditentukan, karena di kondisi nyata tidak ada bandwidth unlimited
- Jika max limit tidak ditentukan, bandwidth management tidak dapat berjalan sempurna

Quality of Service

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

Simple Queue Total

Akumulasi Upload dan Download

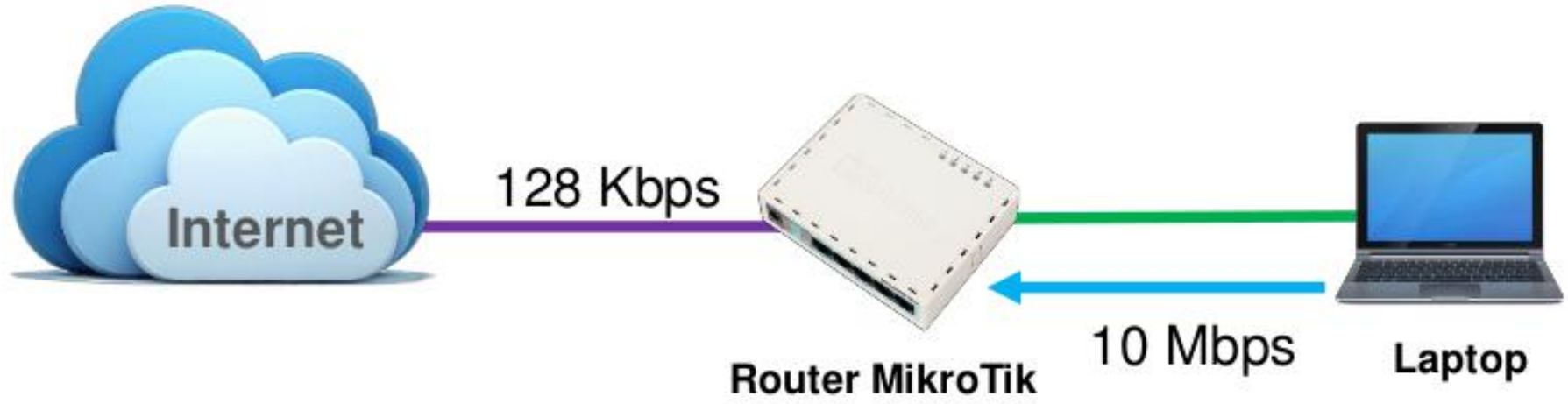


Tips

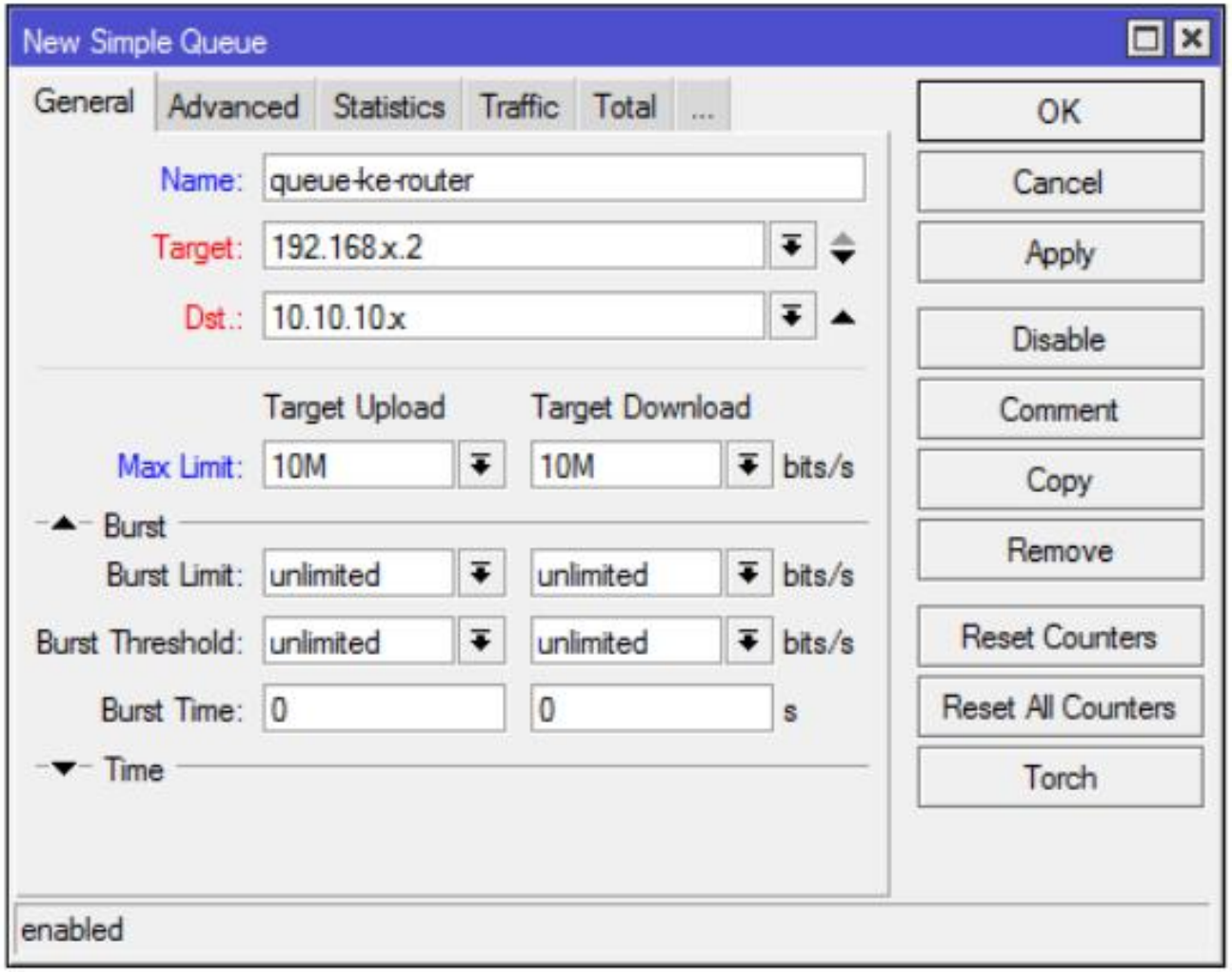
- Jika kita perhatikan, ada perubahan warna pada icon Queue rule. Maksud masing-masing warna adalah sebagai berikut :
  - Hijau : 0 – 50% bandwidth digunakan.
  - Kuning : 51 – 75% bandwidth digunakan
  - Merah : 76 – 100% bandwidth digunakan

(LAB)Destination

- Limit download laptop maksimal 128 Kbps
- Khusus koneksi ke router, boleh menggunakan bandwidth sampai 10 Mbps



Simple Queue Destination



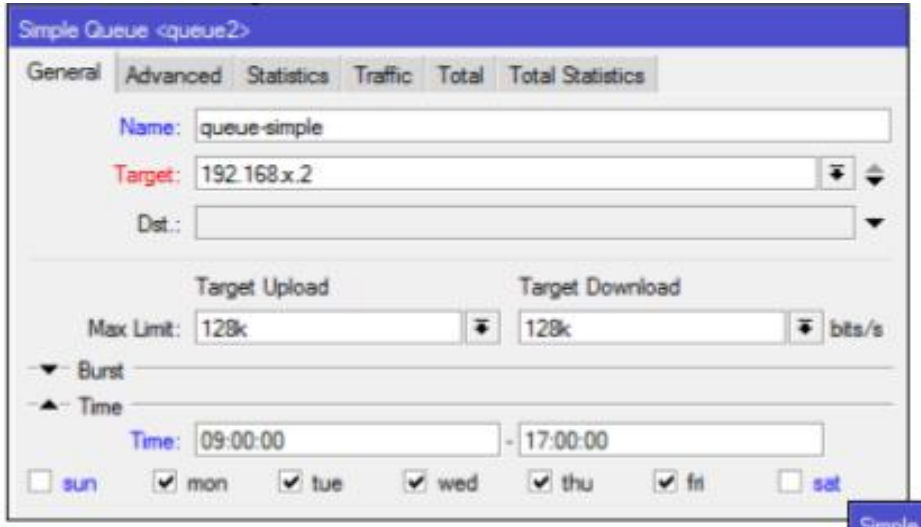
Destination

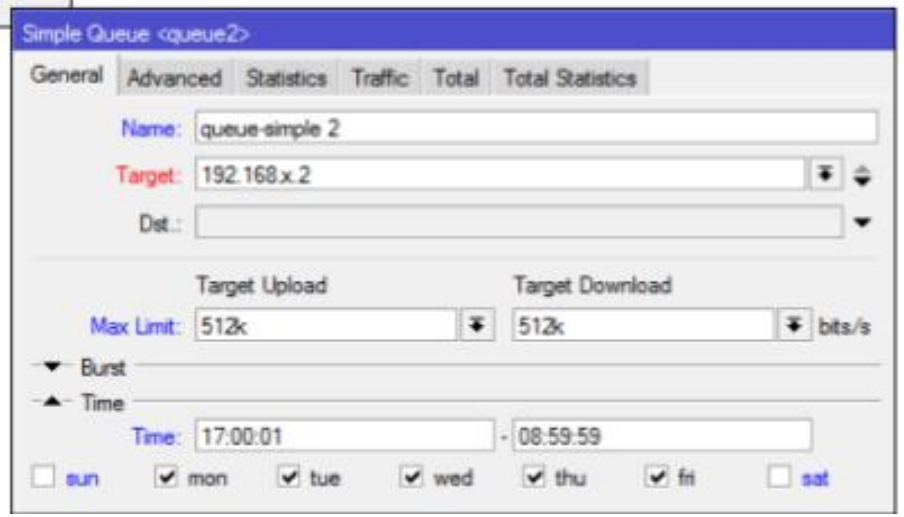
- Menentukan queue untuk traffik dengan tujuan tertentu
- Bisa diisi dengan IP Address atau Network

(LAB)Time

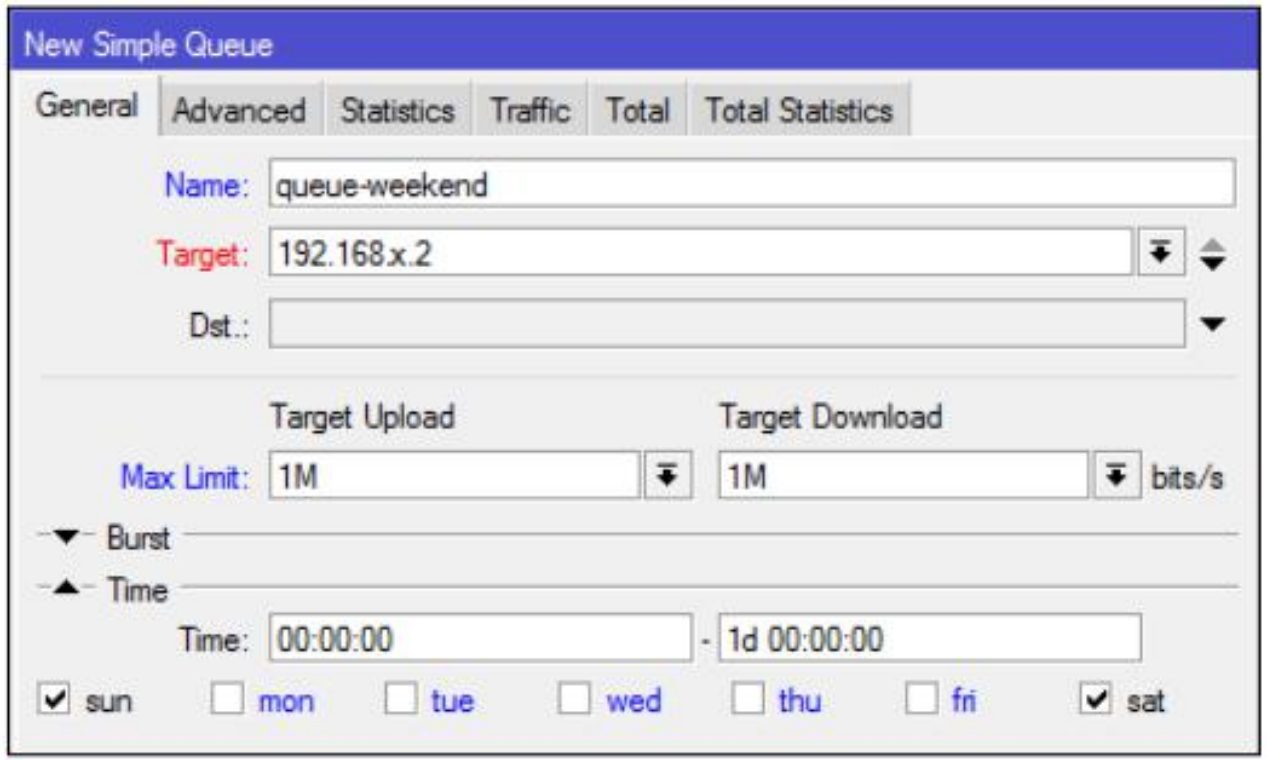
- Limit bandwidth pada jam 09:00 - 17:00 di hari kerja dengan bandwidth 128 Kbps
- Kemudian limit bandwidth pada jam 17:00 - 09:00 di hari kerja dengan bandwidth 512 Kbps
- Untuk sabtu - minggu boleh menggunakan bandwidth sampai 1 Mbps

(LAB)Simple Queue Time





(LAB)Simple Queue Time



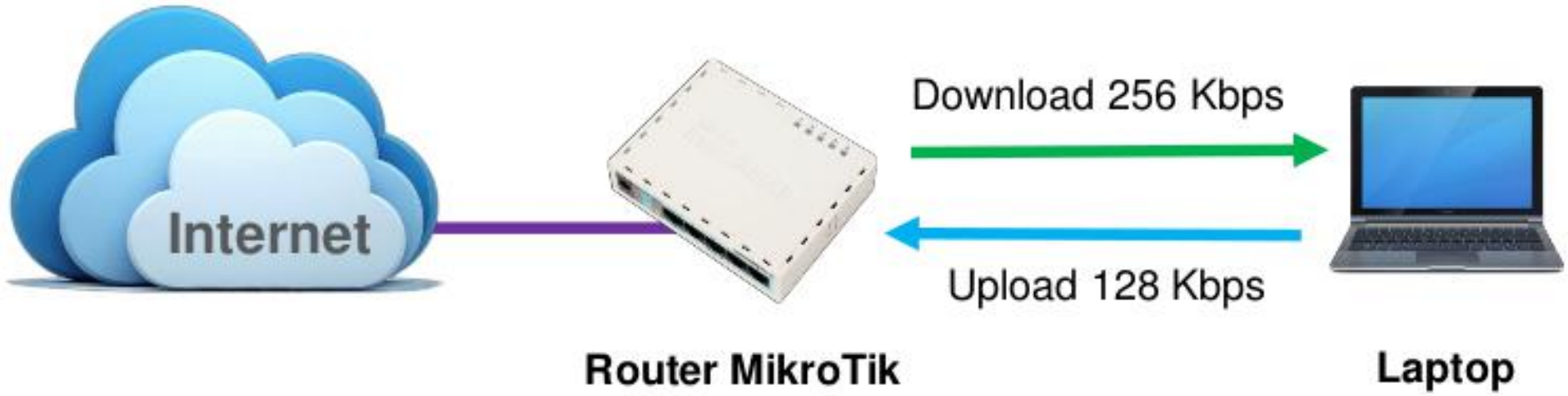
Sebelum setting parameter Time, pastikan sudah setting NTP Client dan clock router sudah sesuai dengan kondisi real

Burst

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

Topologi Simple Queue Burst

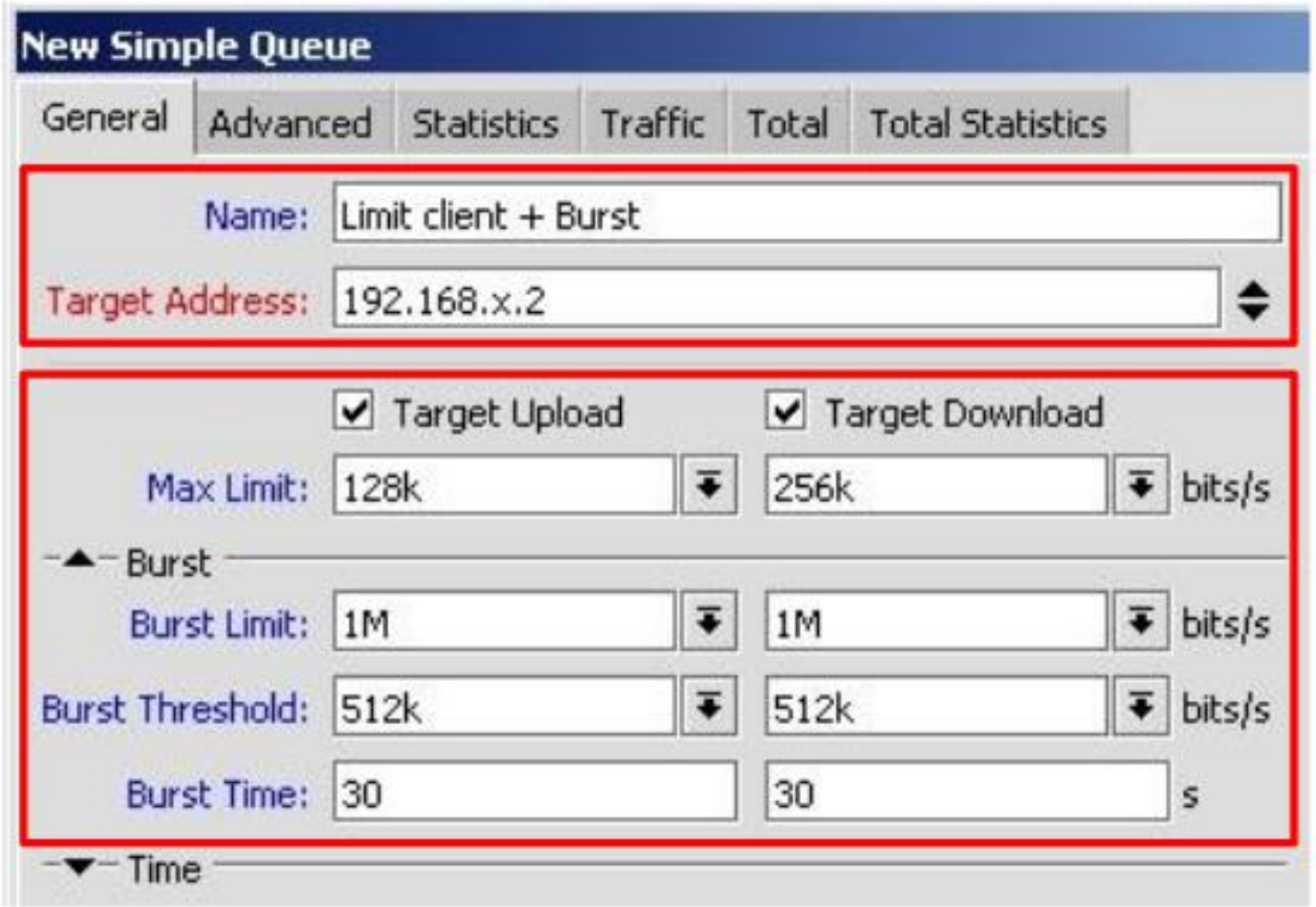
- Pada kondisi tertentu, user diijinkan untuk menggunakan bandwidth melebihi max limit



(LAB)Simple Queue Burst

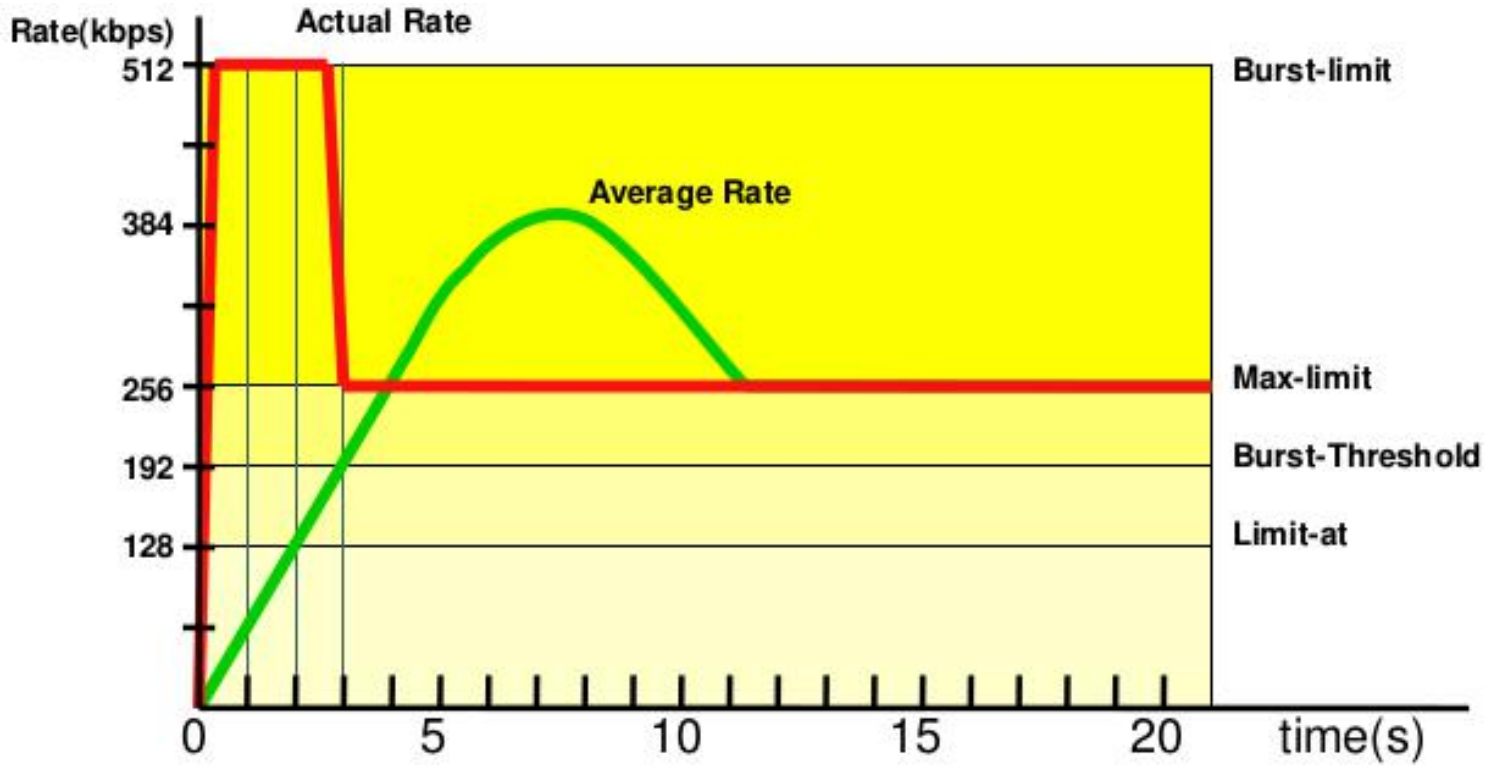
- Make a simple queue for your laptop
  - Downstream max-limit=256k
  - Upstream max-limit=128k
- Try Using Burst
  - Burst-limit=1M
  - Burst-treshold=512K
  - Burst-time=30s

(LAB)Simple Queue Burst



Contoh Burst

Max-limit=256kbps, **burst-time**=8,
burst-threshold=192kbps, **burst-limit**=512kbps.

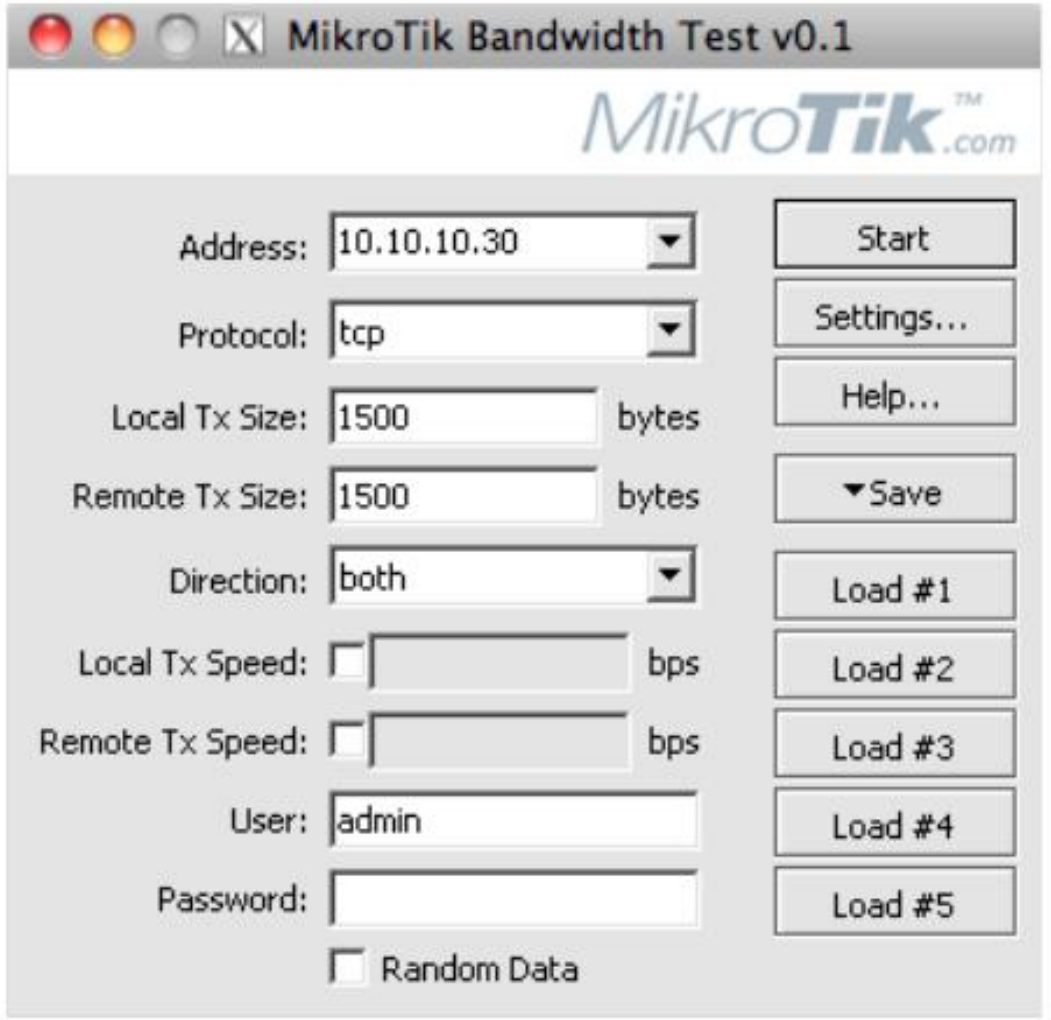


Contoh Burst

- Pada awalnya, data rate rata-rata dalam 8 detik terakhir adalah 0 kbps. Karena data rate rata-rata ini lebih kecil dari burst-threshold, maka burst dapat dilakukan
- Setelah 1 detik, data rate rata-rata adalah (0+0+0+0+0+0+0+512)/8=64kbps, masih lebih kecil dari **burst-threshold**. Burst dapat dilakukan
- Demikian pula untuk detik kedua, data rate rata-rata adalah (0+0+0+0+0+0+512+512)/8=128kbps
- Setelah 3 detik, tibalah pada saat dimana data rate rata-rata lebih besar dari **burst-threshold**. Burst tidak dapat lagi dilakukan, dan data rate turun menjadi **max-limit** (256kbps

Simple Queue Bandwidth Test

- **Address** :
  - IP Address test serve
- **Direction** :
  - Upload
  - Download
  - Upload & Download
- **Protocol** :
  - TCP / UDP
- **User & Password** :
  - Autentikasi

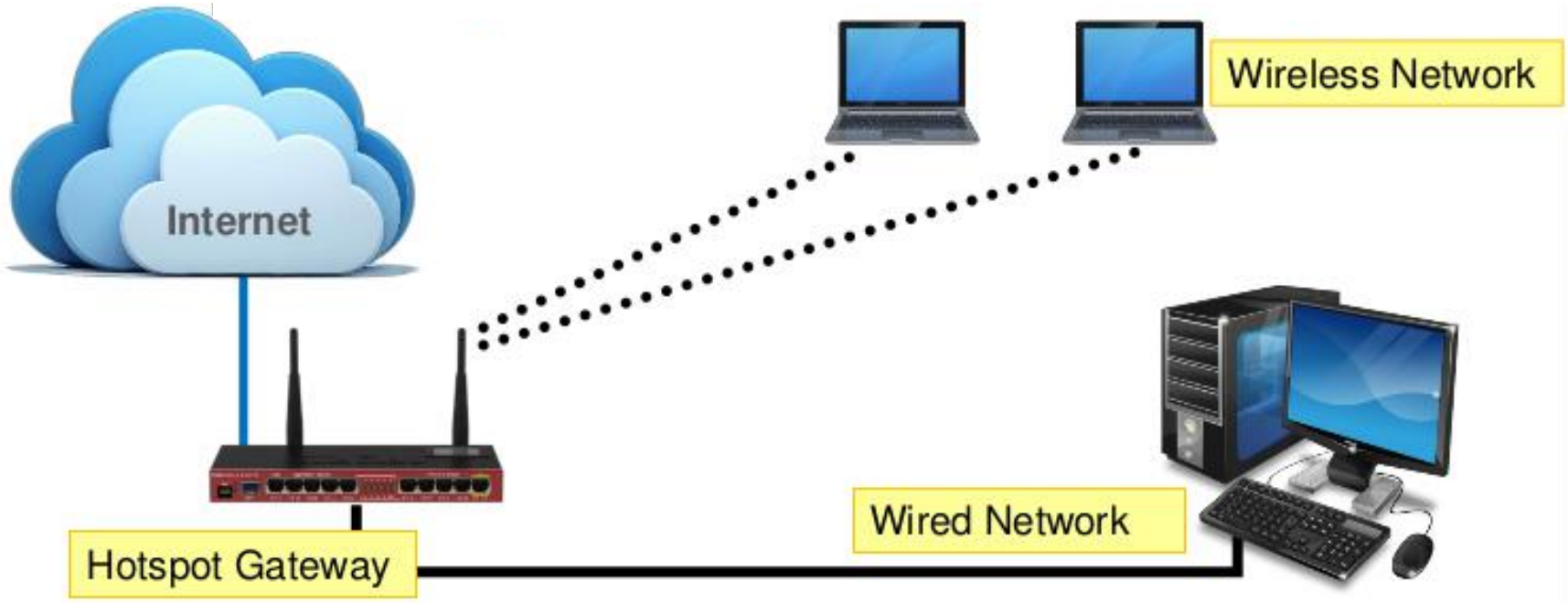


About Hotspot?

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

Example Hotspot Network

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



Hotspot Features

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

(LAB)Hotspot Setup Wizard

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

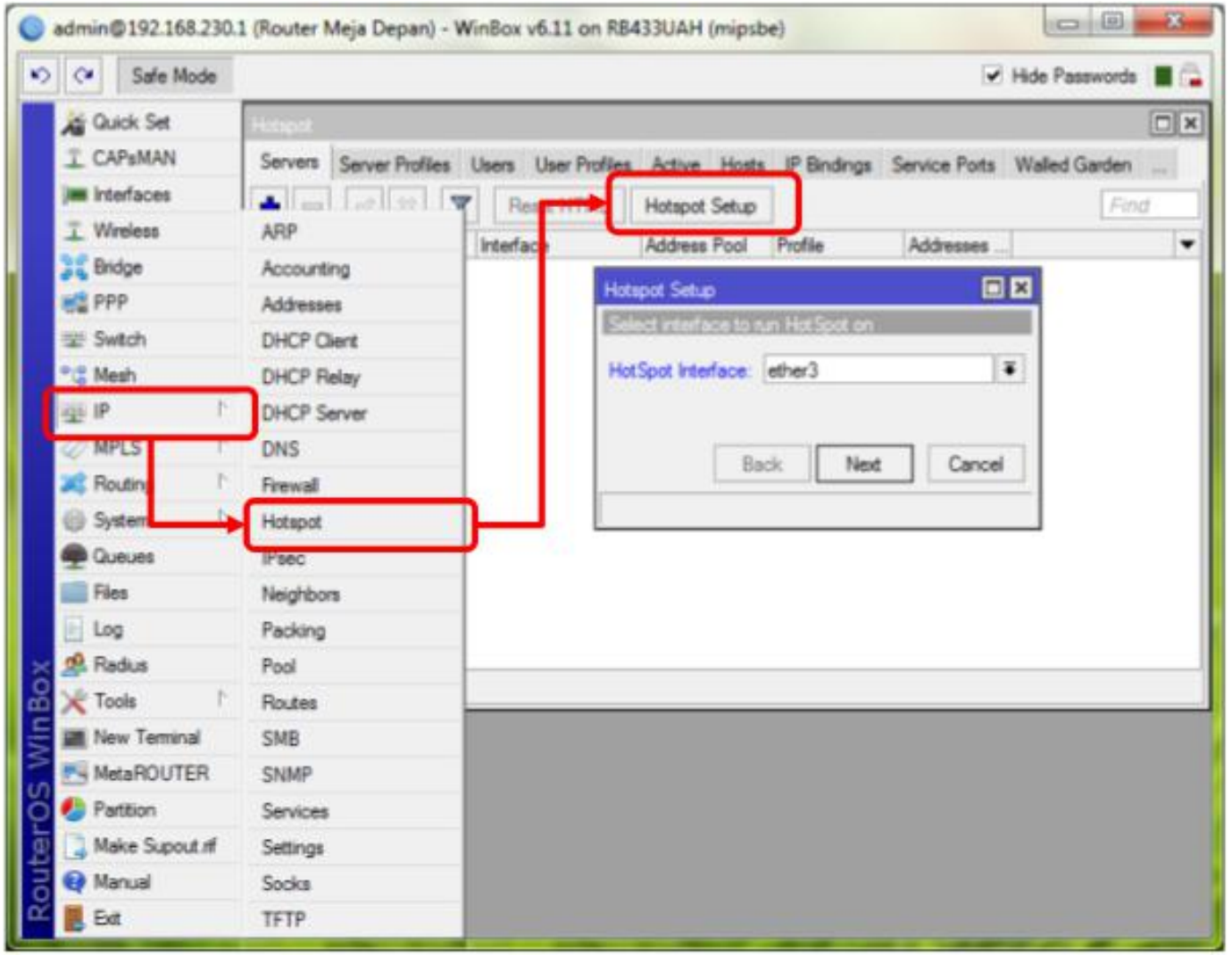
(LAB)Hotspot Setup Wizard

- Pada Langkah awal Tentukan Interface mana yang akan digunakan untuk menjalankan Hotspot System :
  - *hotspot interface : (ex:ether1,wlan1,bridge1,vlan1)*
- Tentukan Alamat IP untuk Interface Hotspot :
  - *Local address of hotspot network : (ex:10.10.10.1/24)*
- Opsi Hotspot Network akan NAT atau Routing :
  - *masquerade hotspot network : yes*
- Tentukan IP-Pool untuk jaringan Hotspot :
  - *address pool of hotspot network : 10.10.10.50-10.10.10.254*
- Menggunakan SSL-Certificate jika ingin menggunakan Login-By HTTPS :
  - *select certificate : none*

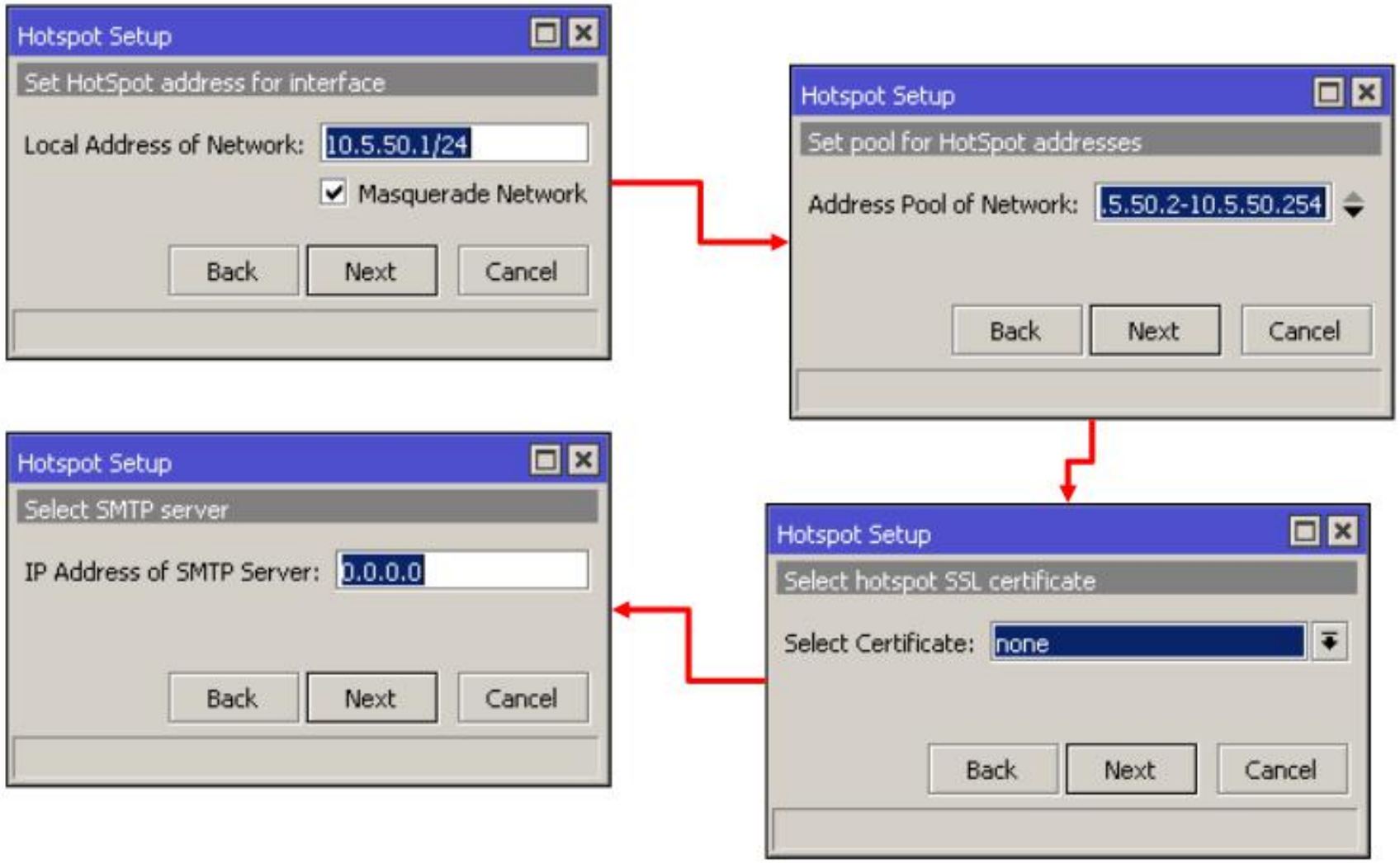
(LAB)Hotspot Setup Wizard

- Jika diperlukan SMTP Server khusus untuk Server hotspot bisa ditentukan, sehingga Server bisa mengirimkan email (misal email notifikasi). Konfigurasi SMTP Server :
  - *Ip address of smtp server : 0.0.0.0 (ex : 168.125.154.190)*
- Konfigurasi DNS Server yang akan digunakan oleh user Hotspot :
  - *dns server : 158.149.180.192, 185.154.85.23*
- Konfigurasi DNS-name dari router Hotspot. Hal ini digunakan jika Router memiliki DNS-Name yang valid (FQDN), Jika tidak ada biarkan kosong
- Langkah terakhir dari wizard adalah pembuatan sebuah user hotspot :
  - *name of local hotspot user : admin*
  - *password for the user : admin*

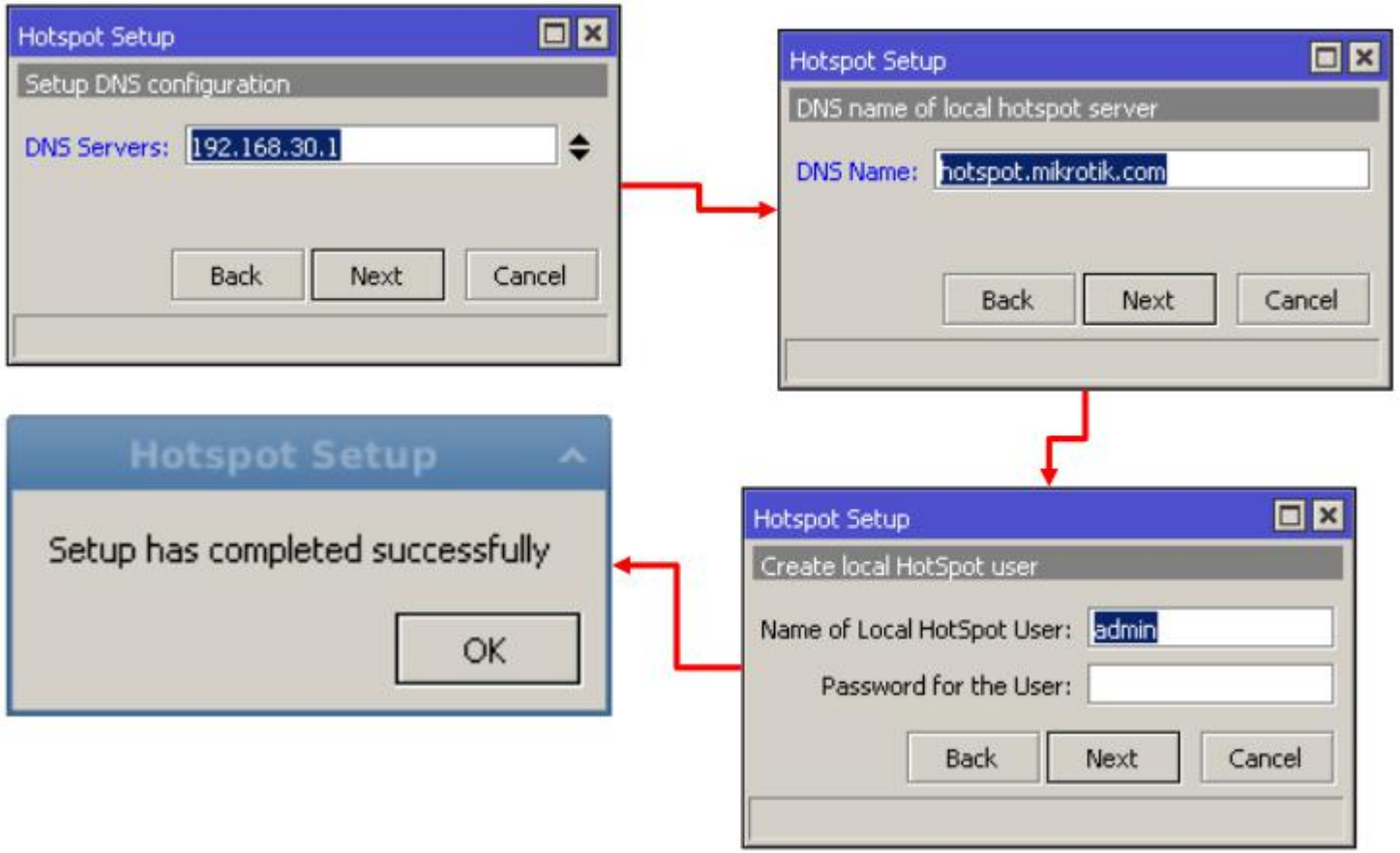
(LAB)Hotspot Setup Wizard (Step 1)



(LAB)Hotspot Setup Wizard (Step 2-5)



(LAB)Hotspot Setup Wizard (Step 6-9)



How does it work?

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

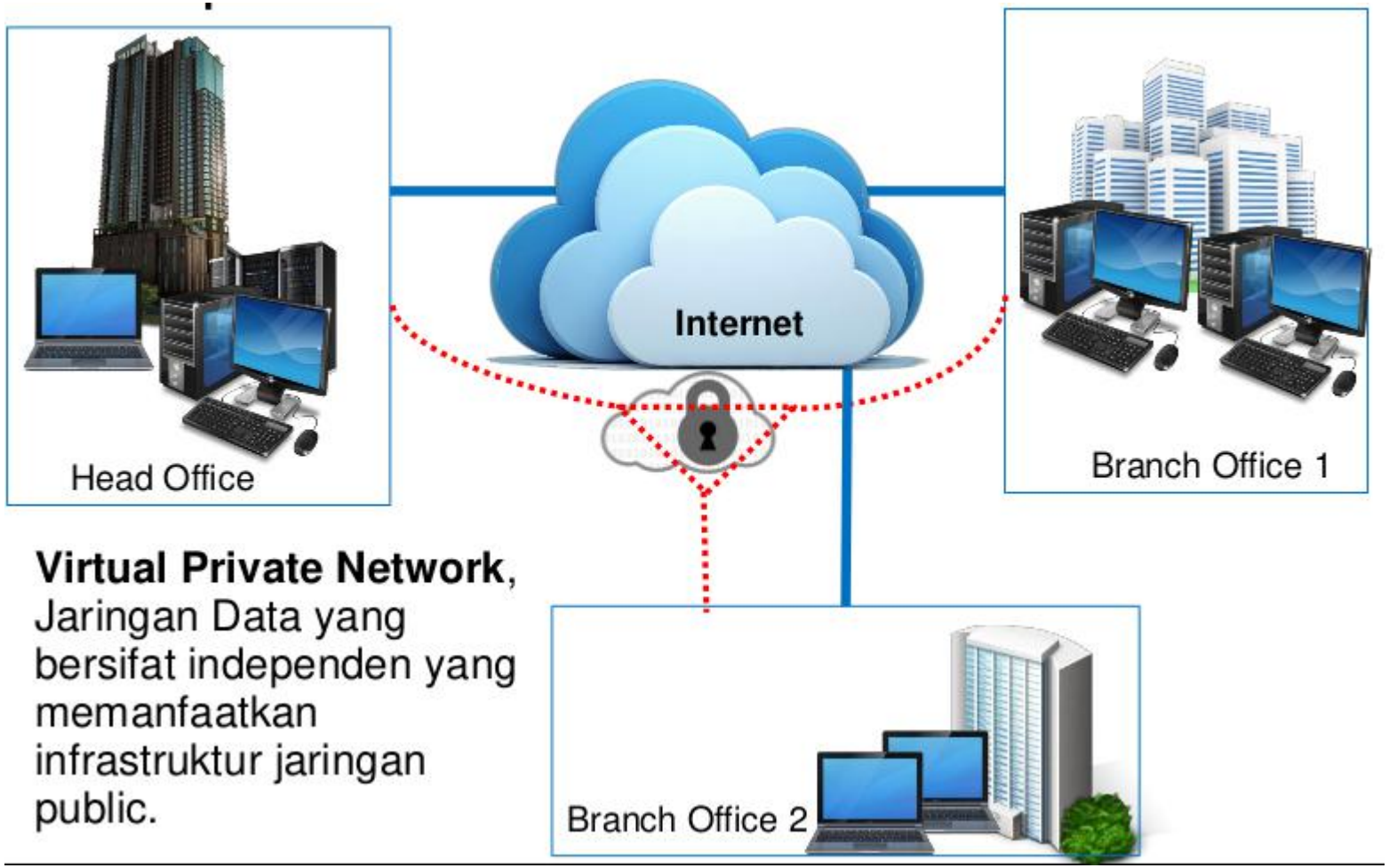
How does it work?

- Jika informasi login sudah tepat, router akan :
  - Mengautentikasi client di Hotspot System
  - Membuka halaman web yang diminta sebelumnya
  - Membuka pop-up halaman status
- User dapat menggunakan akses jaringan

Virtual Private Network

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

VPN Networks



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

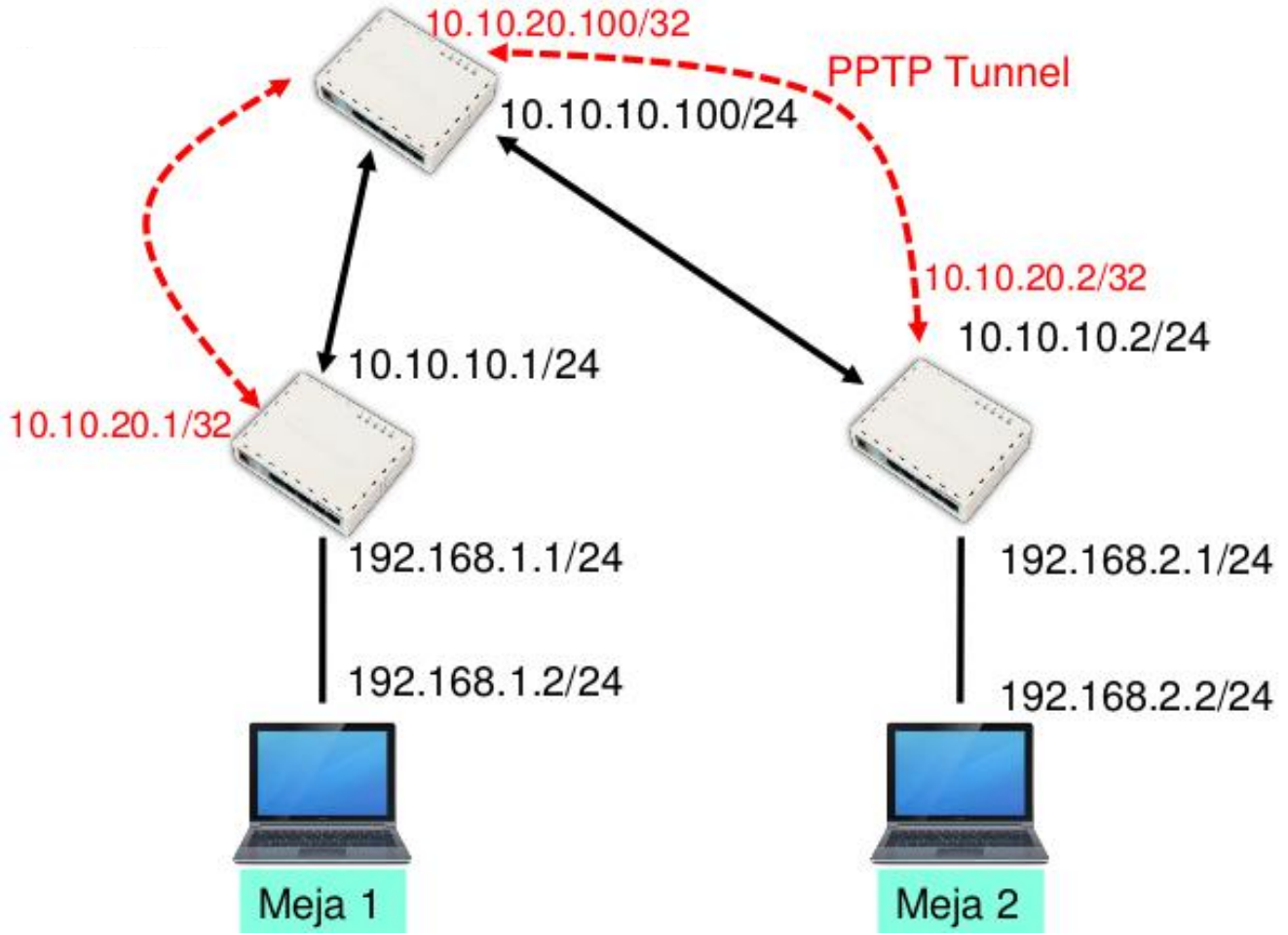
VPN Type

VPN bisa diimplementasikan di berbagai tipe network :

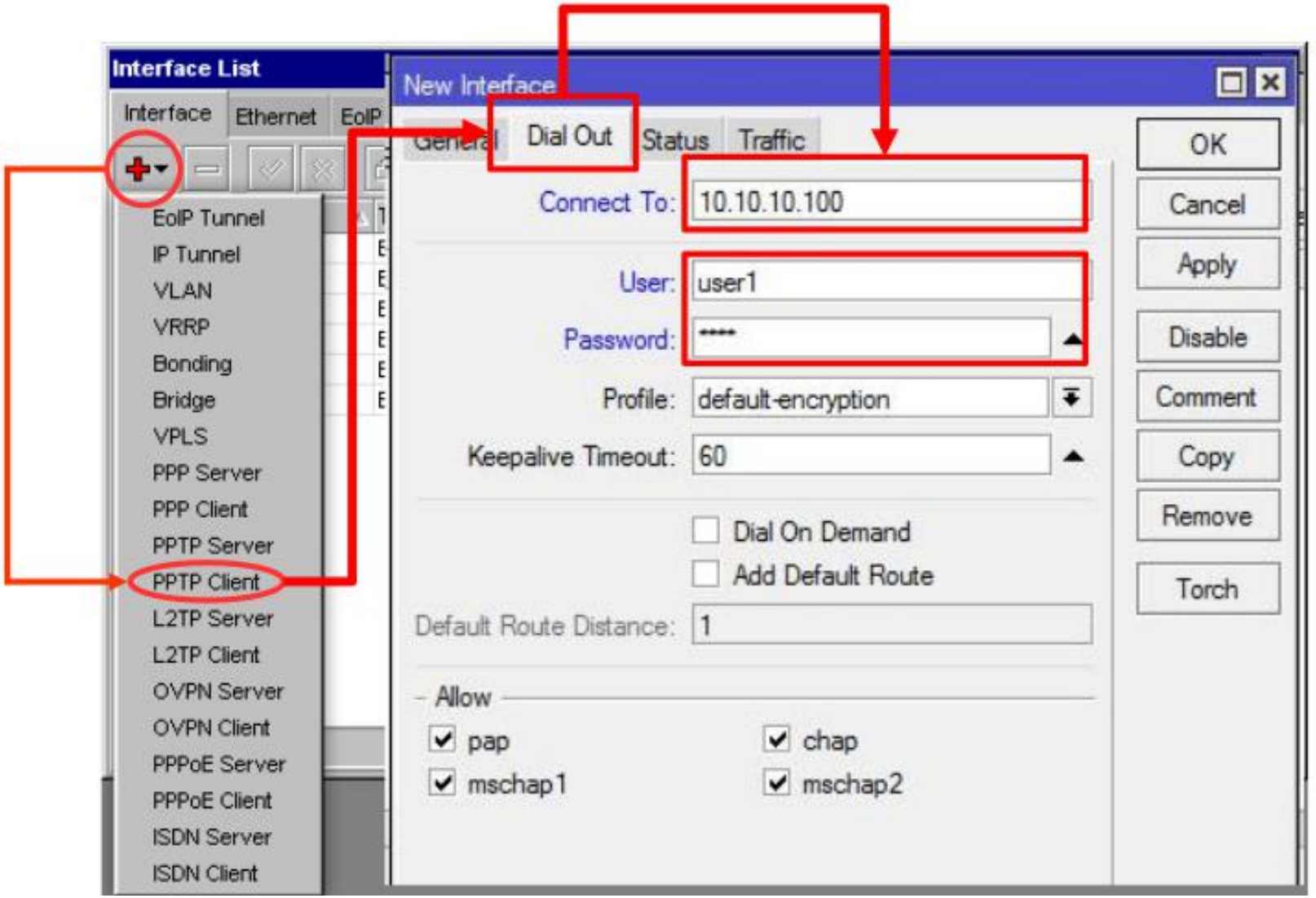
- Routed Network :
  - VPN yang dilakukan di network yang sudah melewati multi hop router atau melewati internet. Contohnya penggunakan **PPTP**
- Bridge Network :
  - VPN yang diimplementasikan di network yang masih satu switch (satu network bridge). Contohnya penggunaan **PPPoE**

(LAB)PPTP Tunnels Client

- Contoh Topologi



(LAB)PPTP Tunnels Client



(LAB)PPTP Tunnels Client

Membuat PPTP-Client :

- **Username** dan **Password** : Sesuaikan dengan konfigurasi server
- **Connect-to** : Parameter Alamat IP dari PPTP-Server
- **Add-Default-Route** : Jika akan menggunakan koneksi PPTP sebagai gateway utama
- **Dial on Demand** : Jika diaktifkan(centang), koneksi PPTP hanya akan aktif ketika digunakan(terdapat traffik)

Membuat PPTP-Client Interface :

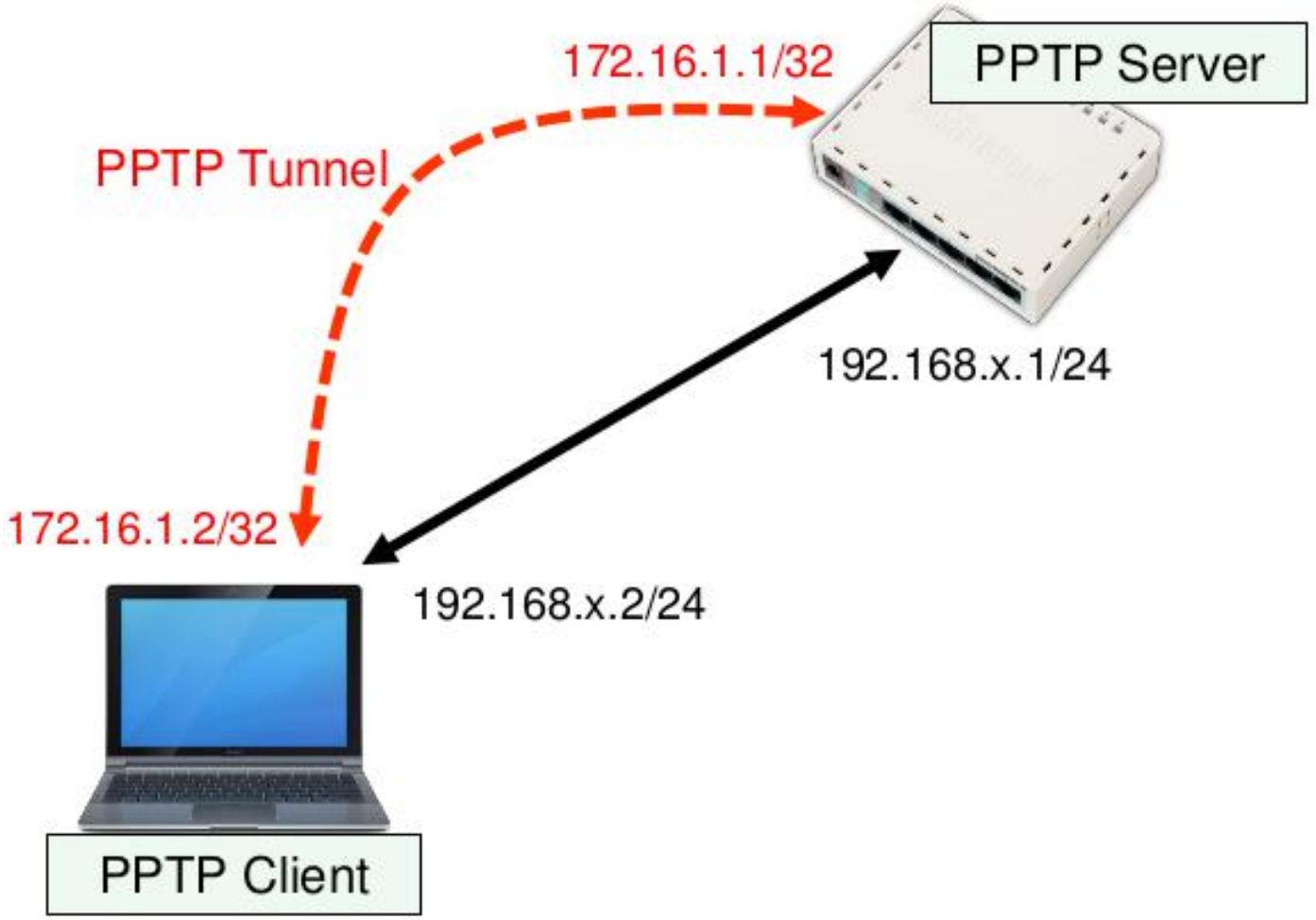
```
/interface pptp-client add name=pptp-out1 connect-to=10.10.10.100
user=user1 password=test
```

Point to Point Tunnel Protocol

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

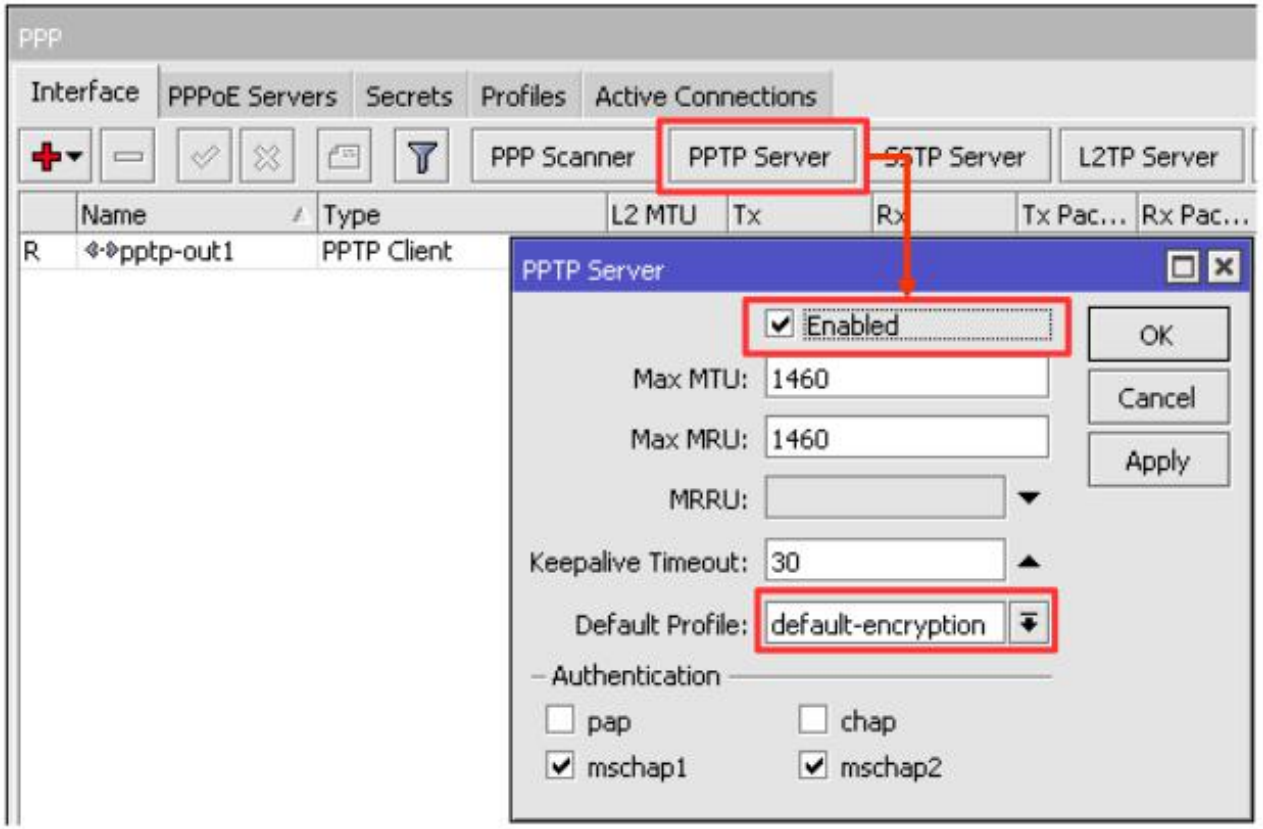
(LAB)PPTP Server

Laptop dial PPTP ke router



(LAB)PPTP Tunnels Server

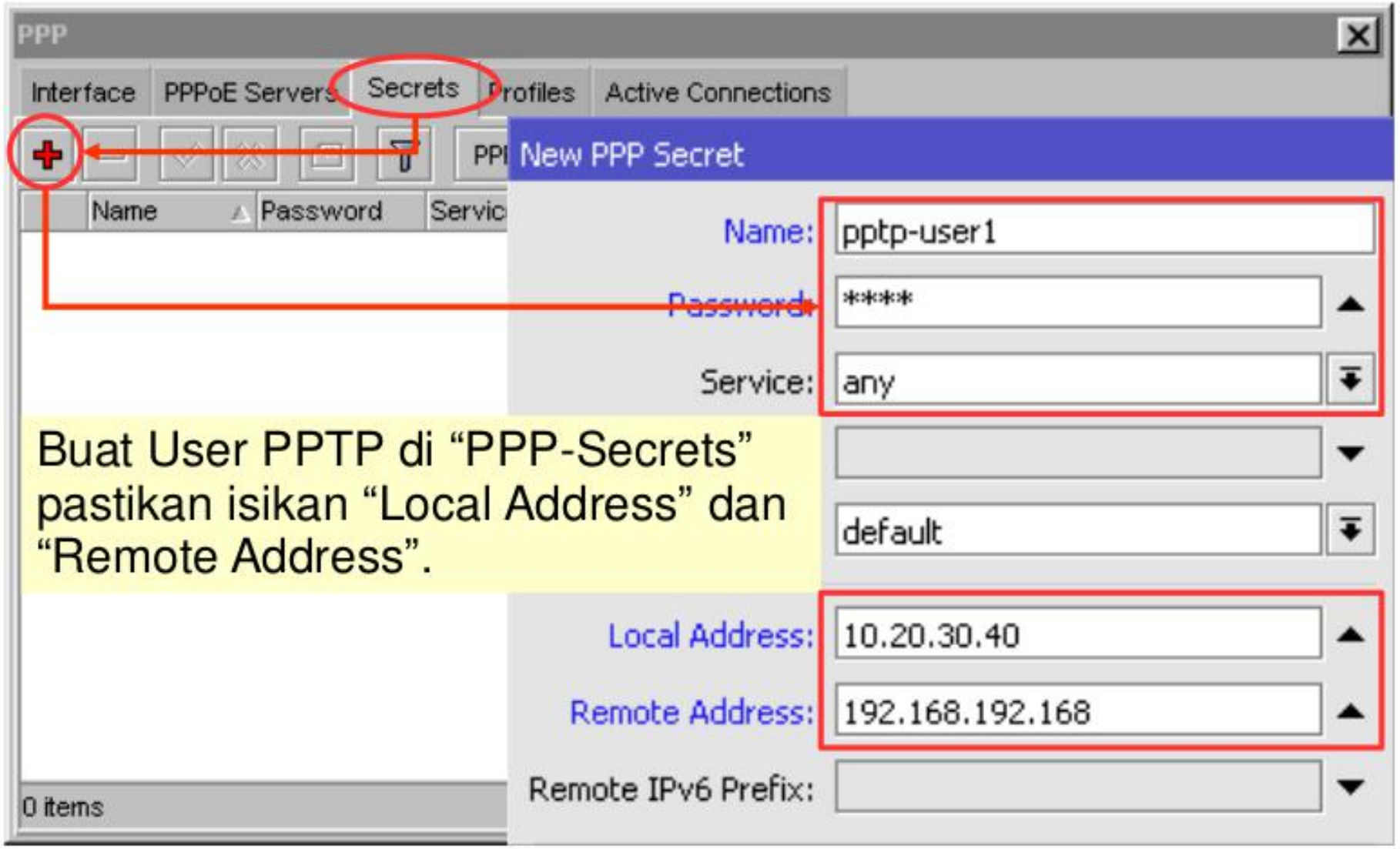
Aktifkan PPTP Server, pastikan menggunakan profile "default-encryption" supaya link VPN terenkripsi



PPTP Server Configuration

- **Service** PPTP Server bisa diaktifkan pada PPP Configuration
- **Default Profile** digunakan untuk menentukan group dan memberikan konfigurasi dasar seperti IP Address, penggunaan enkripsi, dan juga limitasi user
- Default Profile digunakan untuk user-user yang tidak terdapat di database local router contohnya jika autentikasi user menggunakan Radius

(LAB)PPTP Tunnels Server



PPP Secret

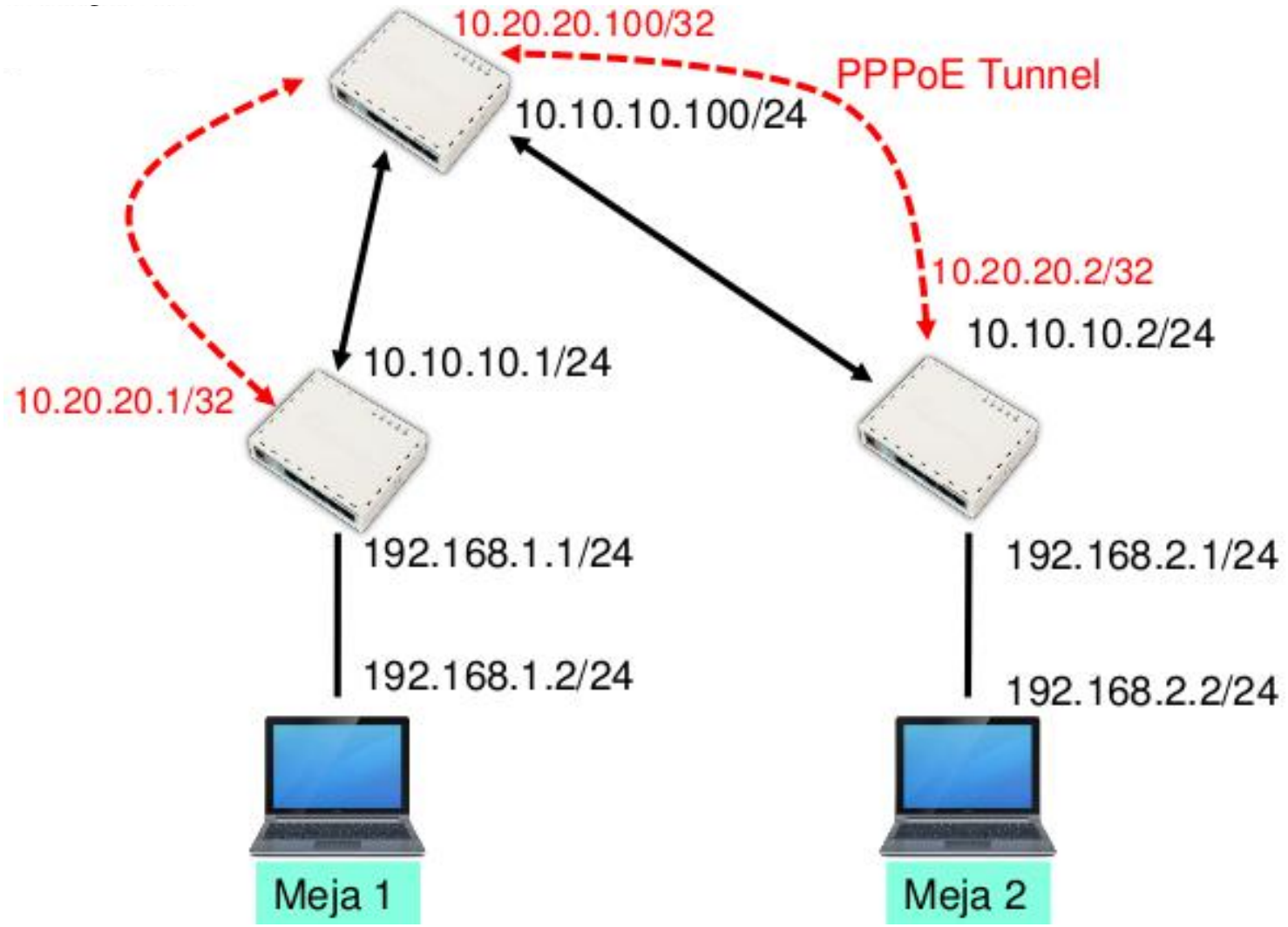
- PPP Secret adalah data user untuk Service VPN (PPTP, PPPoE, OpenVPN, dll) yang ada di local database router, semua konfigurasi user seperti username, password, alokasi IP Address, profile, dan limitasi bisa dilakukan disini
- Ada dua pilihan melakukan assign IP ke user yaitu menggunakan setting di secret (fix IP) atau menggunakan profile (IP Pool)
- VPN User juga bisa menggunakan database user external yaitu menggunakan Radius seperti UserManager atau FreeRadius

Point to Point Protocol over Ethernet

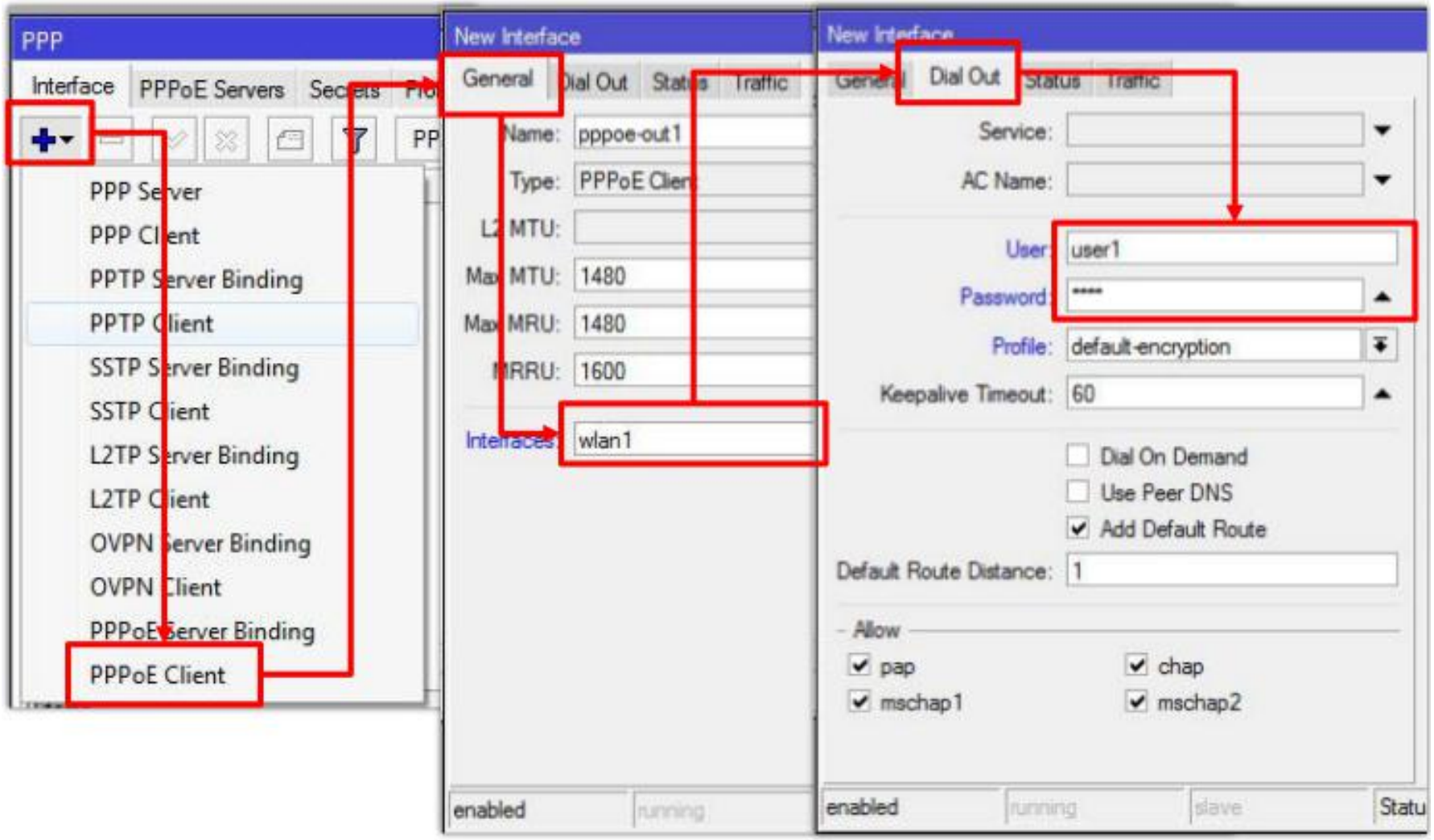
- Penggunaan PPPoE Tunnel :
  - Koneksi antar Client dan Router yang bersifat secure
  - Untuk digunakan sebagai koneksi internet bersifat secure di jaringan local (LAN)
- Sebuah Koneksi PPPoE
  - MikroTik RouterOS bisa berfungsi sebagai PPPoE Server maupun PPPoE Client atau gabungan dari keduanya
- Koneksi PPPoE menggunakan Ethernet frame sebagai protokol transportnya
- Fungsi PPPoE Clients sudah tersedia atau termasuk dalam sebagian besar Sistem Operasi

(LAB)PPPoE Client

Topologi



(LAB)PPPoE Client Configuration



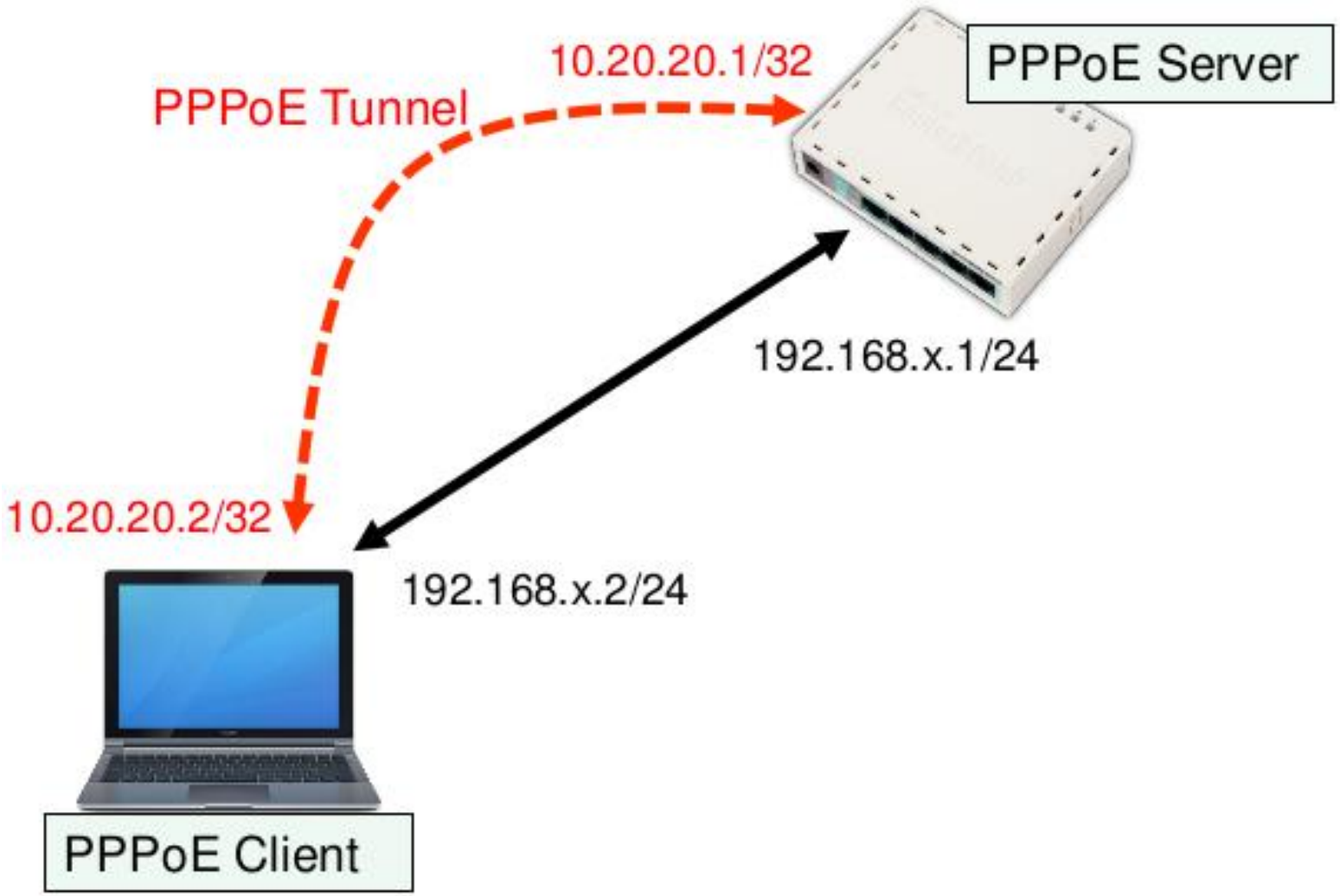
(LAB)PPPoE Client Configuration

Membuat PPPoE-Client pada RouterOS :

- **Interface** : Interface yang terhubung langsung dengan PPPoE Server
- **Username** dan **Password** : Sesuaikan dengan konfigurasi Server
- **Add Default Route** : Aktifkan jika akan menggunakan koneksi PPPoE sebagai Gateway utama
- **Dial on Demand** : Jika diaktifkan, koneksi PPPoE hanya akan aktif ketika digunakan (ada traffik)
- **Use Peer DNS** : Jika akan menggunakan DNS sesuai informasi pada PPPoE Server

(LAB)PPPoE Server

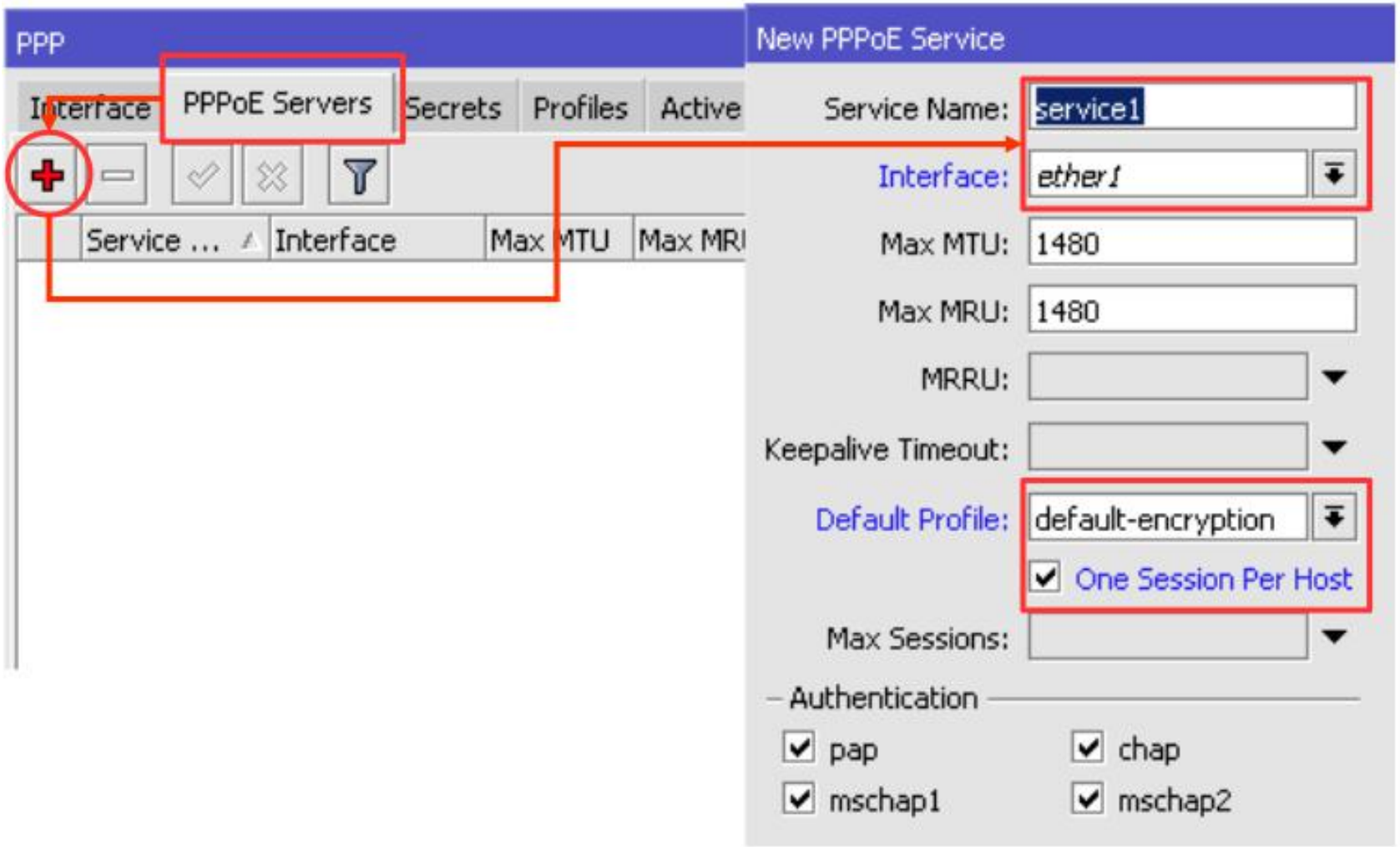
Topologi



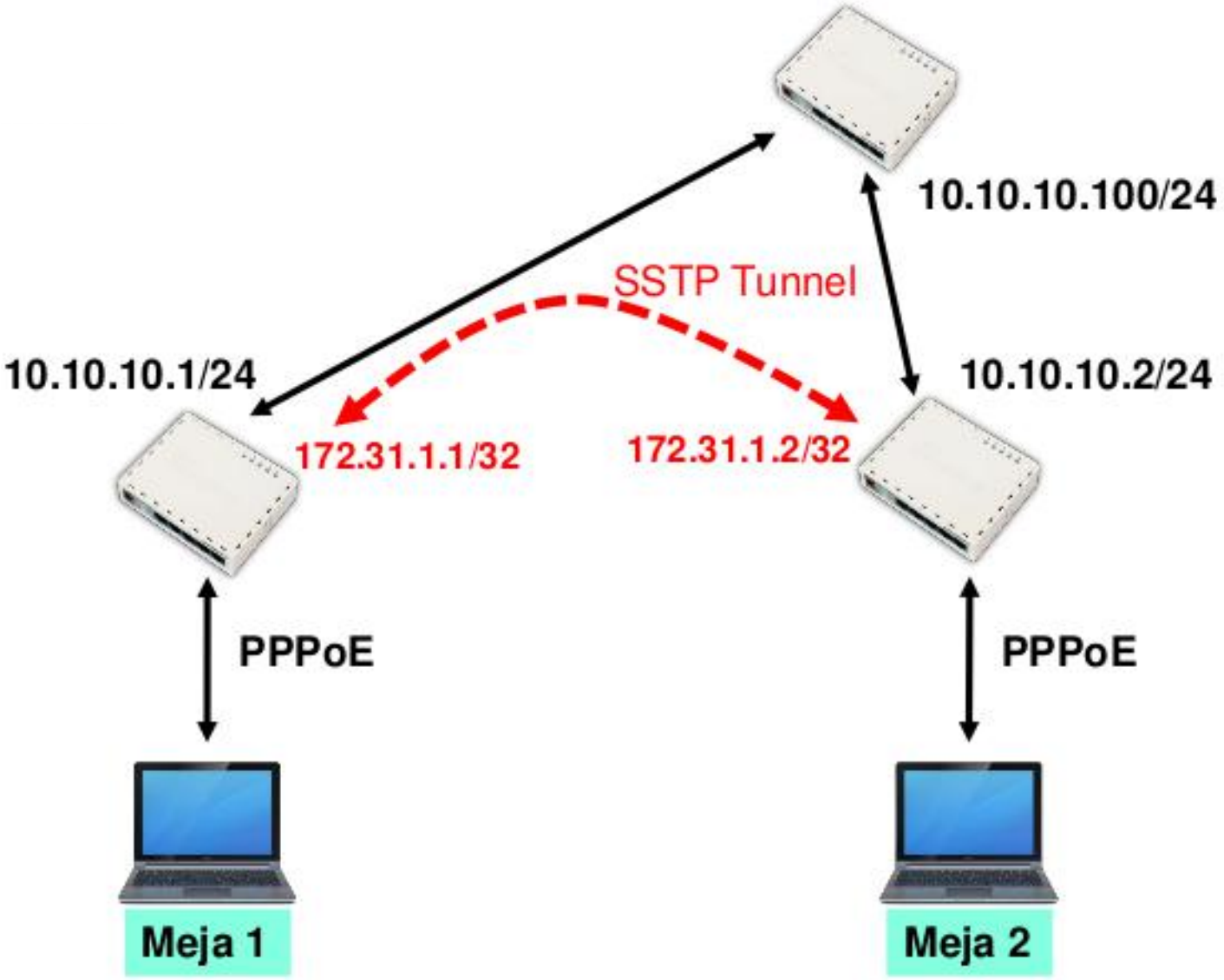
(LAB)PPPoE Server Configuration

- Aktifkan PPPoE Server pada Interface
- Buat PPP Secret untuk PPPoE Client(Langkahnya hampir sama dengan konfigurasi pada Lab PPTP)
- Dial PPPoE dari Laptop

(LAB)PPPoE Server Configuration



Topologi

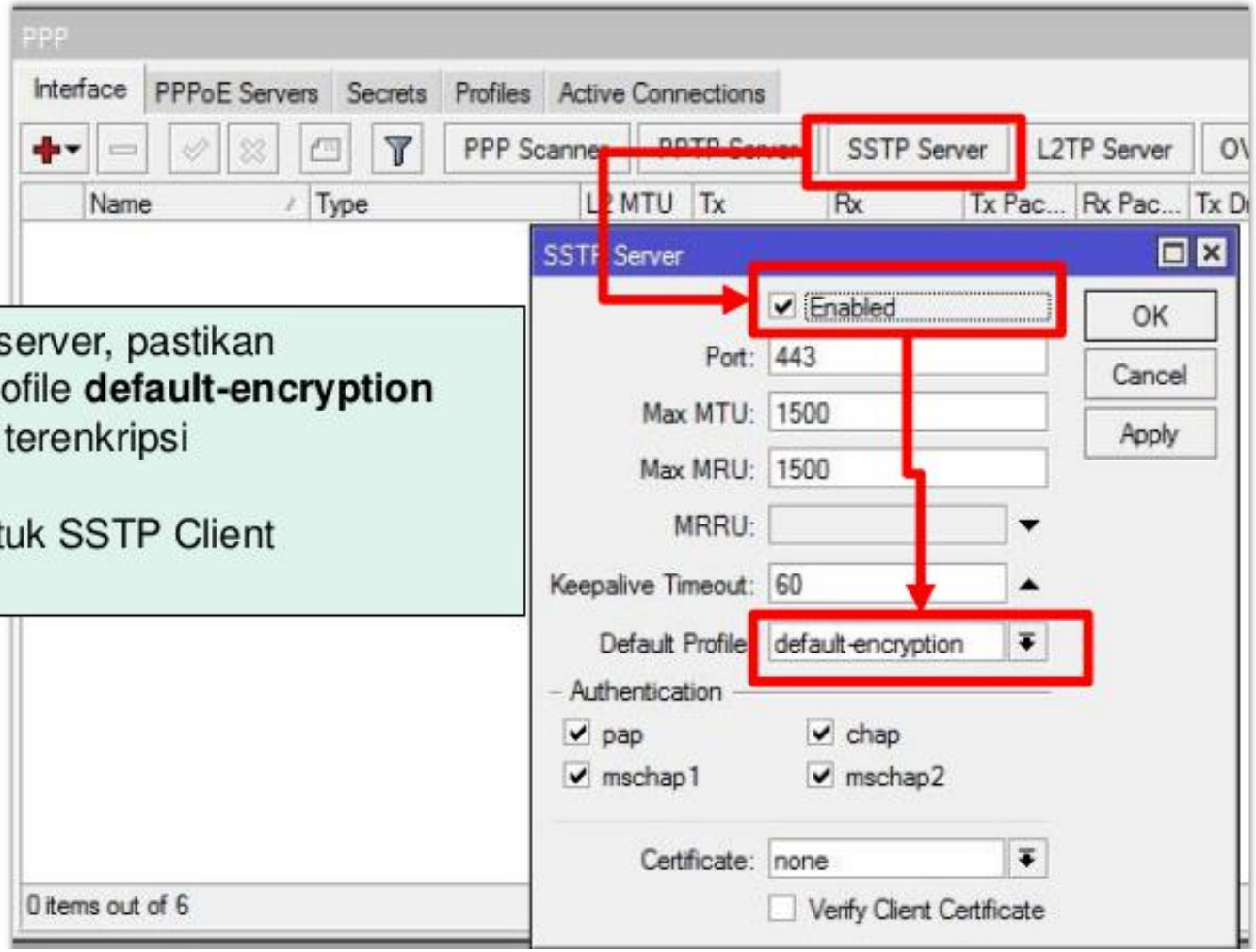

10.10.10.100/24
SSTP Tunnel
10.10.10.1/24
10.10.10.2/24
172.31.1.1/32
172.31.1.2/32
PPPoE
PPPoE
Meja 1
Meja 2

(LAB)SSTP

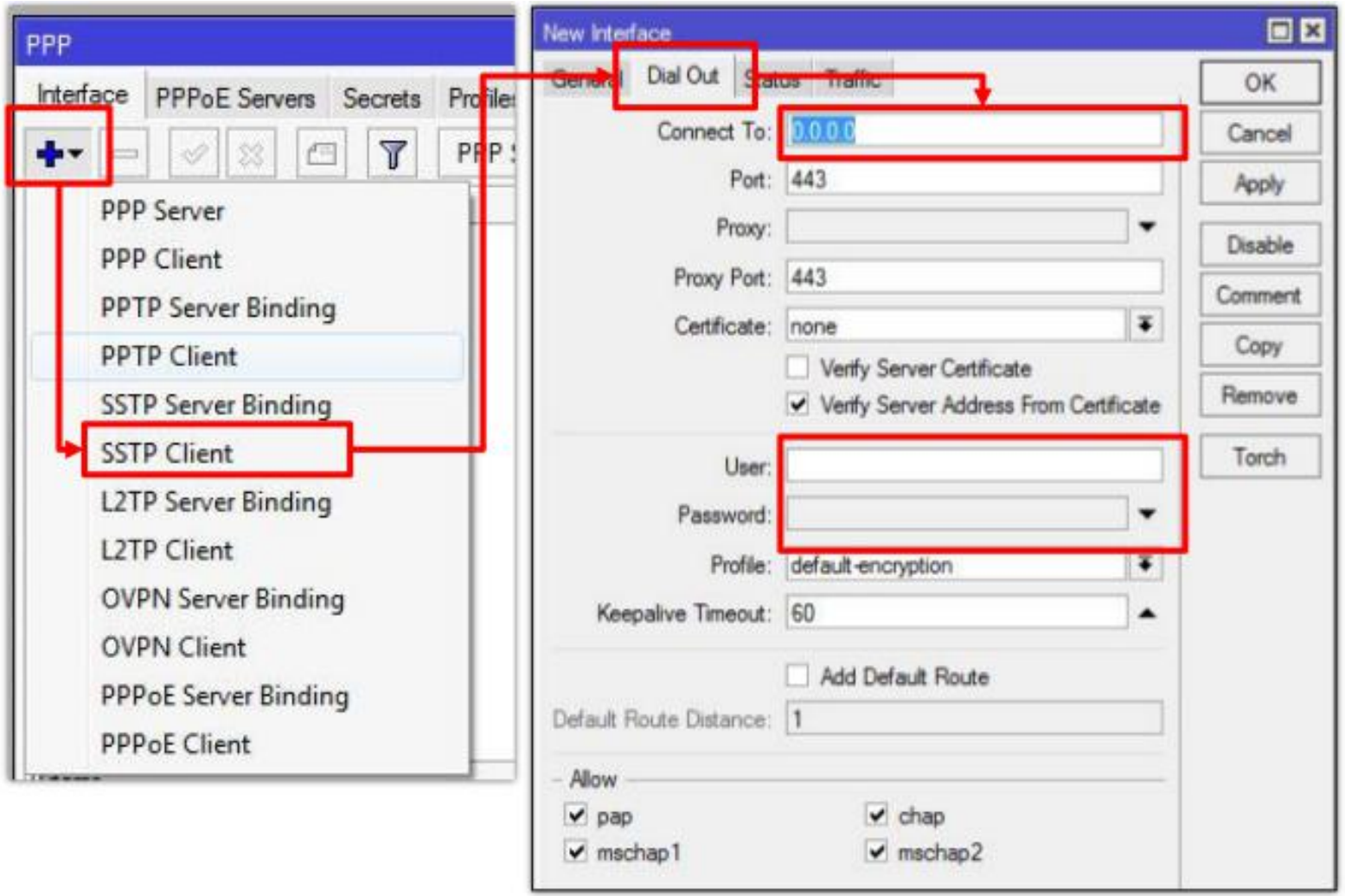
- Buatlah SSTP Tunnel tanpa certificate antar Router, bekerja sama dengan rekan semeja
- Koneksikan laptop dengan Router menggunakan service PPPoE pada masing-masing meja
- Buatlah Static Route agar laptop bisa saling berkomunikasi

(LAB)SSTP Server

- Aktifkan SSTP server, pastikan menggunakan profile **default-encryption** supaya link VPN terenkripsi
- Buat Secret untuk SSTP Client



(LAB)SSTP Client



Secure Socket Tunneling Protocol

- PPP Tunnel over SSL
- MikroTik RouterOS bisa berfungsi sebagai SSTP Server maupun SSTP Client atau gabungan dari keduanya
- Dibutuhkan SSL Certificate untuk dapat terkoneksi, baik ada Server maupun Client(tidak berlaku jika keduanya MikroTik RouterOS)
- Koneksi SSTP menggunakan TCP port 443

VPN Monitoring

- Pada sisi Server bisa dilihat berapa banyak koneksi VPN yang terbentuk (aktif)