

# **HOW TO BASIC MIKROTIK MTCNA**

**MUHAMMAD ADIB AULIA NURKHAFIF**

# KATA PENGANTAR

Bismillahirrahmanirrahim,

Pertama-tama saya ucapkan puji syukur kepada Allah yang maha kuasa, berkat rahmat-Nya saya dapat menyelesaikan buku saya yang pertama yaitu **HOW TO BASIC MIKROTIK MTCNA**.

Tak lupa pula kita aturkan sholawat dan salam kepada Nabi Muhammad SAW. Idola kita, dan suri tauladan terbaik di dunia ini.

Alhamdulillah, setelah lama perjuangan saya menyelesaikan buku ini, akhirnya selesai juga. Buku ini ditujukan kepada kedua orangtua yang telah membesarkan saya dengan penuh kasih sayang, dan kepada guru TKJ saya yang telah mengajarkan kepada saya semua hal tentang MikroTik MTCNA.

Pada buku saya yang pertama ini tentang MikroTik MTCNA, semoga kalian semua dapat mengambil ilmu/pelajaran yang saya tulis dalam buku ini. Semoga dapat membawa berkah dan dapat menjadi langkah kalian dalam menguasai MikroTik MTCNA.

Saya masih menyadari banyaknya kesalahan dalam buku ini, jika kalian mau memberi kritik/saran kalian bisa menghubungi saya di email: [adibnk11@gmail.com](mailto:adibnk11@gmail.com).

Selamat belajar dan membaca!

Sekian,

Bogor, Jawa barat, Desember 2019

Muhammad Adib Aulia Nurkhafif

# DAFTAR ISI

Kata Pengantar.....	i
Daftar Isi.....	ii
Sejarah Mikrotik.....	vi
Pengenalan Mikrotik.....	vii
A. Jenis Mikrotik.....	vii
B.Tipe Routerboard.....	viii
C.Fitur Mikrotik .....	ix
D.Lisensi Mikrotik.....	ix
E.Sertifikasi Mikrotik.....	xii
Bab 1 Dasar .....	xiii
Akses Router Mikrotik .....	- 1 -
Melihat Versi Mikrotik.....	- 14 -
Melihat Fitur Mikrotik .....	- 18 -
Enable/Disable Fitur Mikrotik.....	- 21 -
Enable Fitur.....	- 21 -
Disable Fitur .....	- 29 -
Uninstall Fitur .....	- 36 -
Upgrade Fitur Mikrotik.....	- 38 -
Drag & Drop.....	- 41 -
Upload File.....	- 43 -
Check For Updates.....	- 44 -
Downgrade Fitur Mikrotik.....	- 46 -
User Management.....	- 48 -
Export, Import, Backup, And Restore .....	- 55 -
Backup & Restore.....	- 56 -
Export & Import.....	- 57 -

Router Identity .....	- 59 -
<b>Menyimpan Dan Mengupload Hasil Backup/Export .....</b>	<b>- 61 -</b>
Drag & Drop.....	- 61 -
Upload.....	- 62 -
<b>Soft Dan Hard Reset.....</b>	<b>- 63 -</b>
Soft Reset .....	- 63 -
Hard Reset .....	- 65 -
<b>Internet Via Lan.....</b>	<b>- 66 -</b>
<b>Internet Via Wlan .....</b>	<b>- 70 -</b>
<b>Network Time Protocol (Ntp).....</b>	<b>- 77 -</b>
Bab 2 Firewall.....	- 80 -
<b>Pengenalan Firewall.....</b>	<b>- 81 -</b>
Overview.....	- 81 -
Firewall Filter Rule .....	- 81 -
Firewall Nat.....	- 82 -
Firewall Mangle.....	- 83 -
Prinsip "If" Kemudian "Then".....	- 84 -
Packet Flow.....	- 85 -
<b>Firewall Filter Rule .....</b>	<b>- 86 -</b>
Content: .....	- 86 -
Kasus.....	- 88 -
<b>Firewall Logging .....</b>	<b>- 93 -</b>
<b>Memblokir Situs.....</b>	<b>- 95 -</b>
Overview.....	- 95 -
Dengan Filter Rule.....	- 95 -
Dengan Address List.....	- 97 -
Dengan Layer 7 Protocol.....	- 99 -
Pemblokiran Konten.....	- 101 -
Pemblokiran Dengan Dns.....	- 103 -
<b>Connection Tracking &amp; State .....</b>	<b>- 105 -</b>
Bab 3 Wireless .....	- 109 -
<b>Pengenalan Wireless .....</b>	<b>- 110 -</b>

Content:.....	- 110 -
<b>Wireless Lab:.....</b>	<b>- 117 -</b>
Simple Interkoneksi Wireless.....	- 118 -
Virtual Access Point (Vap) .....	- 121 -
Nstreme .....	- 123 -
Mac Address Filtering .....	- 127 -
Wireless Bridge .....	- 132 -
WDS (Wireless Distribution System).....	- 136 -
WDS Dynamic .....	- 138 -
WDS Static.....	- 143 -
Wireless Repeater .....	- 148 -
Bab 4 Quality Of Service (QoS) .....	- 154 -
<b>Pengenalan Qos.....</b>	<b>- 155 -</b>
Simple Queue.....	- 157 -
Burst.....	- 157 -
Per Connection Queue.....	- 158 -
Queue Tree & Mangle .....	- 158 -
<b>Queue Lab:.....</b>	<b>- 159 -</b>
Simple Queue.....	- 160 -
Queue Burst .....	- 163 -
Pcq (Per-Connection Queue).....	- 166 -
Pcq With Rate.....	- 170 -
Queue Tree .....	- 174 -
Bab 5 Network Management.....	- 183 -
Pengenalan Network Management.....	- 184 -
Overview.....	- 184 -
Dhcp.....	- 185 -
Web Proxy.....	- 196 -
Arp .....	- 204 -
Hotspot .....	- 210 -
Walled Garden.....	- 232 -
Walled Garden Ip List.....	- 233 -

Tentang Penulis ..... - 235 -

# SEJARAH MIKROTIK

MikroTik adalah perusahaan vendor jaringan besar yang sudah terkenal diseluruh dunia. Yang kini sudah memiliki client ribuan dan bahkan jutaan dan tersebar keseluruh dunia.

MikroTik ini ditemukan oleh dua orang yang bernama John Trully (Sebelah kiri) dan Arnis Riekstins (Sebelah kanan). MikroTik ini ditemukan di kota Riga, Latvia. Negara tempat pusat Mikrotik dari seluruh dunia sekarang, yang dulunya merupakan tempat uji coba MikroTik pertama kali dan termasuk negara pecahan dari Uni Soviet.



MikroTik ditemukan ditahun 1996 dan awal mula mereka memulai, mereka membuat sebuah sistem operasi gabungan antara Linux dan MS-DOS yang dikombinasikan dengan wireless LAN (WLAN) yang berkecepatan 2Mbps. Awal mula usaha dimulai, klien yang mereka miliki hanya sekitar 10-20 orang.

Disitulah timbul sebuah motto khas MikroTik yang menjadi dasar mereka, yakni “Routing the World.”. Membuat sebuah perangkat router yang pintar dan dapat disebarluaskan ke seluruh dunia. Mulai dari situ, MikroTik bangkit dan menciptakan lagi sebuah sistem operasi yang bisa mengkonfigurasi router dengan baik yang dinamakan ‘RouterOS’ dengan menggunakan Linux kernel 2.2. Lamban laun usaha mereka meningkat dan mulai dikenal di negara-negara maju diseluruh dunia.

# PENGENALAN MIKROTIK

## A. Jenis MikroTik

### 1. Mikrotik RouterOS™

Suatu sistem operasi dan perangkat lunak buatan MikroTik yang fungsinya untuk merubah computer menjadi sebuah router network yang pintar, yang terdapat banyak fitur yang digunakan untuk ip network dan jaringan wireless.

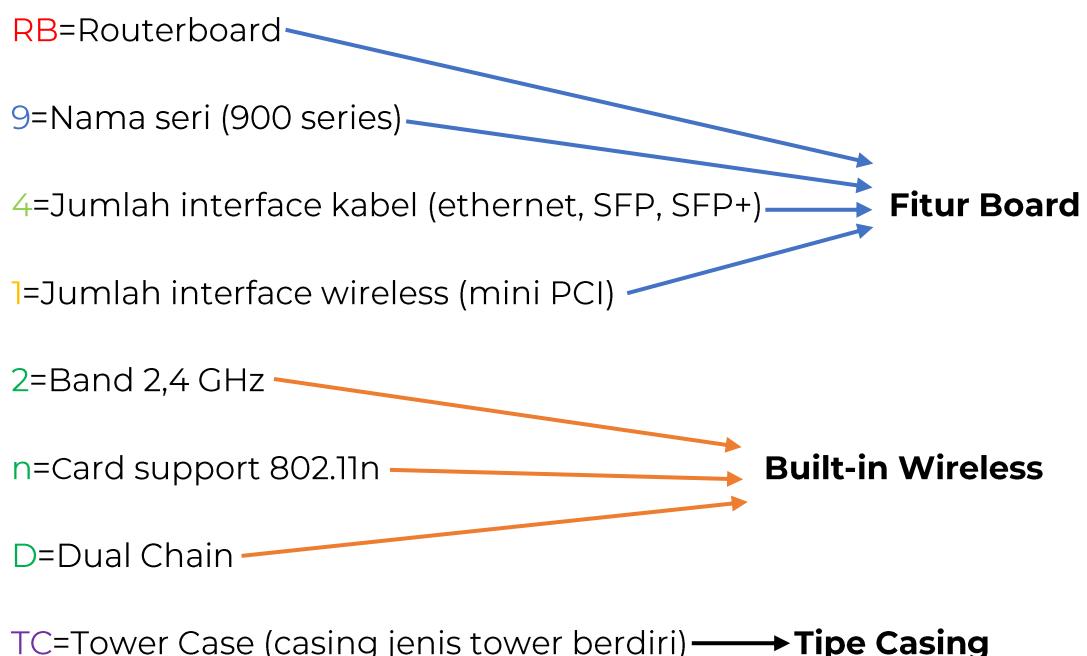
### 2. MikroTik RouterBOARD

RouterBOARD merupakan hardware (Router) yang didesain oleh MikroTik. RouterBOARD memiliki beragam seri dan interface yang disesuaikan dengan kebutuhan. RouterBOARD menggunakan RouterOS sebagai software / sistem operasinya. Beberapa contoh Routerboard ini diantaranya adalah RB400, RB600, R52H, R52N, R2N yang merupakan Wireless board dan RB750, RB450G, RB1000 yang merupakan Embeded (sistem minimum) Router.

## B.Tipe RouterBoard

Setiap produk Mikrotik pasti memiliki kode produk unik yang memiliki artinya tersendiri, contohnya seperti router hAP lite yang saya gunakan untuk membuat lab mikrotik.

hAP lite memiliki kode produk **RB941-2nD-TC**.



## C.Fitur Mikrotik

1. Router OS apabila diinstall pada PC/Virtual machine, akan support driver perangkat:

- Ethenet, Wireless Card, V35, ISDN, USB Mass Storage, USB 3G Modem, E1/T1.

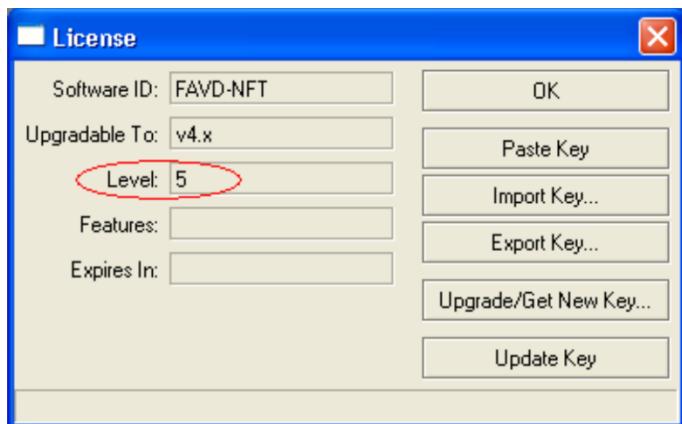
2. Memiliki fitur yang melebihi sebuah “router” :

- User Management (DHCP, Hotspot, Radius, dll).
- Routing (RIP, OSPF, BGP, RIPng, OSPFv3).
- Firewall & NAT (Kustomisasi sendiri).
- QoS/Bandwidth limiter (Burst, PCQ, RED, dll).
- Tunnel (EoIP, PPTP, L2TP, PPPoE, SSTP, OpenVPN).
- Real-time Tools (Torch, watchdog, mac-ping, MRTG, sniffer).

## D.Lisensi Mikrotik

MikroTik adalah sebuah perangkat lunak yang dapat mengkonfigurasi jaringan namun, tidak semua fitur di Mikrotik yang bisa kita konfigurasi. Karena ada fitur-fitur yang tidak terbuka atau terbatasi. Didalam Mikrotik, ada sebuah istilah yang dinamakan lisensi, setiap tingkatan dalam lisensi itu, ada fitur-fitur tertentu yang terbuka atau terbatasi, dari lisensi level 0 – lisensi level 6. Jika kita meng-upgrade lisensi Mikrotik kita, maka fitur itu akan terbuka.

Pada MikroTik RouterOs, jika kita ingin melihat lisensi,



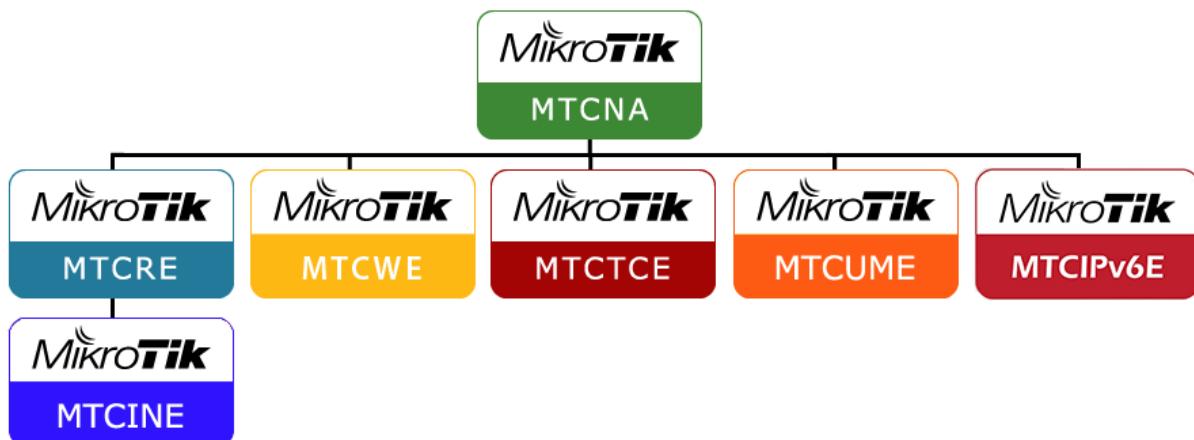
>System>Licence

- Level 0 (gratis); tidak membutuhkan lisensi untuk menggunakannya dan penggunaan fitur hanya dibatasi selama 24 jam setelah instalasi dilakukan.
- Level 1 (demo); pada level ini kamu dapat menggunakannya sebagai fungsi routing standar saja dengan 1 pengaturan serta tidak memiliki limitasi waktu untuk menggunakannya.
- Level 3; sudah mencakup level 1 ditambah dengan kemampuan untuk menajemen segala perangkat keras yang berbasiskan Kartu Jaringan atau Ethernet dan pengelolan perangkat wireless tipe klien.
- Level 4; sudah mencakup level 1 dan 3 ditambah dengan kemampuan untuk mengelola perangkat wireless tipe akses poin.
- Level 5; mencakup level 1, 3 dan 4 ditambah dengan kemampuan mengelola jumlah pengguna hotspot yang lebih banyak.
- Level 6; mencakup semua level dan tidak memiliki limitasi apapun.

Untuk detail lebih jelas, bisa cek ditabel dibawah ini:

Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
<b>Price</b>	no key 	registration required 	do not sell	\$45	\$95	\$250
<b>Initial Config Support</b>	-	-	-	15 days	30 days	30 days
<b>Wireless AP</b>	24h trial	-	-	yes	yes	yes
<b>Wireless Client and Bridge</b>	24h trial	-	yes	yes	yes	yes
<b>RIP, OSPF, BGP protocols</b>	24h trial	-	yes(*)	yes	yes	yes
<b>EoIP tunnels</b>	24h trial	1	unlimited	unlimited	unlimited	unlimited
<b>PPPoE tunnels</b>	24h trial	1	200	200	500	unlimited
<b>PPTP tunnels</b>	24h trial	1	200	200	500	unlimited
<b>L2TP tunnels</b>	24h trial	1	200	200	500	unlimited
<b>OVpn tunnels</b>	24h trial	1	200	200	unlimited	unlimited
<b>VLAN interfaces</b>	24h trial	1	unlimited	unlimited	unlimited	unlimited
<b>HotSpot active users</b>	24h trial	1	1	200	500	unlimited
<b>RADIUS client</b>	24h trial	-	yes	yes	yes	yes
<b>Queues</b>	24h trial	1	unlimited	unlimited	unlimited	unlimited
<b>Web proxy</b>	24h trial	-	yes	yes	yes	yes
<b>User manager active sessions</b>	24h trial	1	10	20	50	Unlimited
<b>Number of KVM guests</b>	none	1	Unlimited	Unlimited	Unlimited	Unlimited

## E.Sertifikasi Mikrotik



**MTCNA= MikroTik Certified Network Associate**

Sertifikat ini mempelajari dasar-dasar MikroTik.

**MTCRE= MikroTik Certified Routing Engineer**

Sertifikat yang hanya bisa didapatkan setelah MTCNA, dalam sertifikat ini, kita belajar tentang protocol-protokol routing di MikroTik.

**MTCWE=MikroTik Certified Wireless Engineer**

Sertifikat ini mempelajari tentang wireless lebih dalam.

**MTCTCE=MikroTik Certified Traffic Control Engineer**

Sertifikat ini berhubungan dengan pengaturan lalu lintas bandwidth.

**MTCUME=MikroTik Certified User Management Engineer**

Sertifikat ini berhubungan dengan hotspot dan tunneling.

**MTCIPv6E=MikroTik Certified IPv6 Engineer**

Sertifikat ini berhubungan dengan IPv6

**MTCINE=MikroTik Certified Inter Network Engineer**

Sertifikat ini merupakan yang paling tinggi tingkatnya. Dan membahas tentang BGP, MPLS, dan Traffic Engineering.



# AKSES ROUTER MIKROTIK

Perangkat MikroTik yang kita punya pasti sebelum menggunakannya kita harus mengonfigurasi terlebih dahulu, oleh karena itu kita harus mengakses perangkat tersebut untuk mengkonfigurasi. Ada banyak cara untuk mengakses MikroTik, ada yang berbasis teks, dan ada yang berbasis GUI (Graphical Unit Interface) atau antarmuka sistem menggunakan grafis yang mempermudah kita mengonfig MikroTik, jadi kita tinggal klik saja, tidak perlu mengetik seperti didalam telnet. telnet

Lebih jelasnya ada ditabel berikut:

Akses Via	Basis Teks	GUI
Telnet	yes	no
SSH	yes	no
Webfig	yes	yes
Winbox	yes	yes

Sebenarnya masih banyak lagi, cara mengakses MikroTik, namun sebagai contoh saja, saya pilih 4 cara yang biasanya digunakan untuk kita praktekkan.

Dan di Lab kali ini, saya akan menggunakan router yang masih memiliki setelan default (Factory Setting).

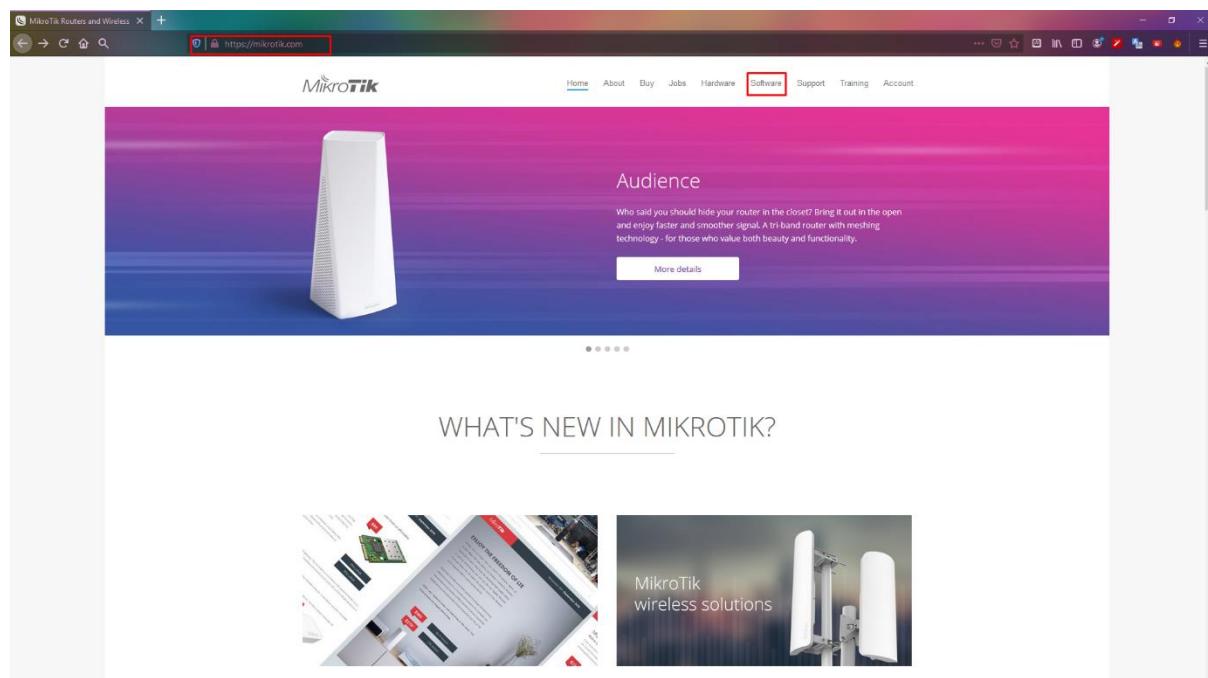
Yaitu IP interface ether1-nya=192.168.88.1

Dan user login-nya= Admin

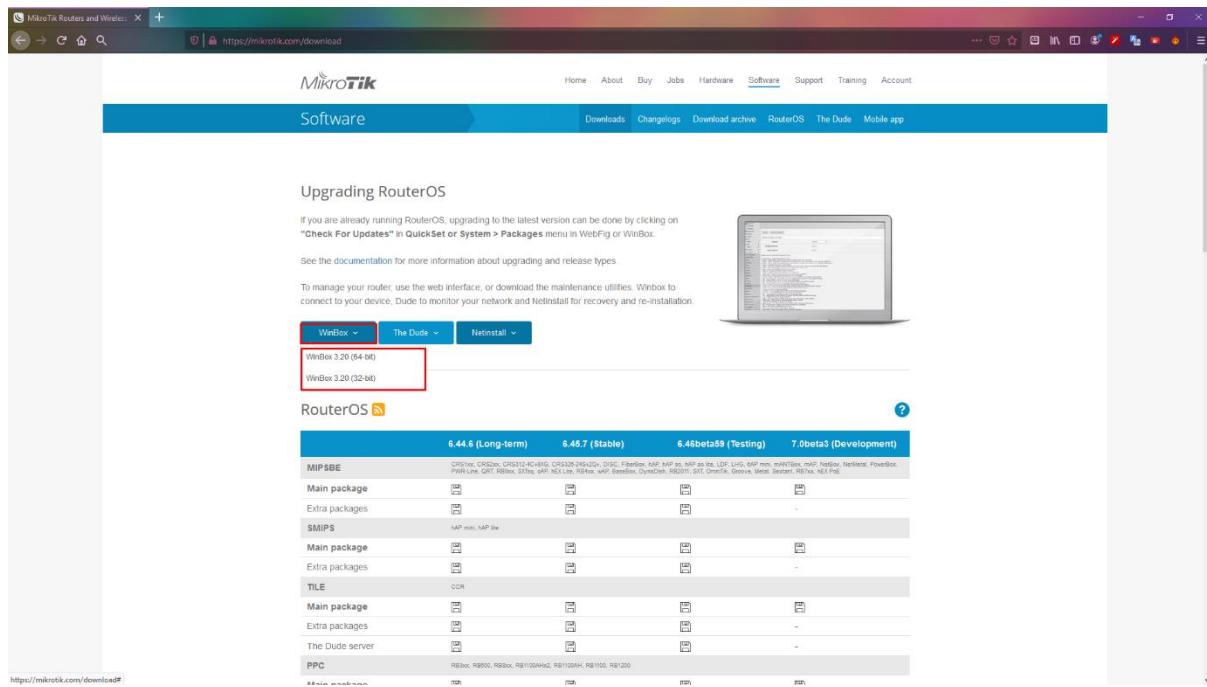
Password=(kosong)

## 1. Via Winbox

Langkah pertama yang paling mudah menurut saya untuk mengkonfigurasi MikroTik adalah via Winbox, apa itu Winbox? Winbox adalah aplikasi resmi dari MikroTik yang digunakan untuk mengkonfigurasi router MikroTik. Winbox ini, bisa berbasis GUI atau teks (terminal). Jika kalian belum memiliki Winbox, bisa diunduh di [www.mikrotik.com](https://www.mikrotik.com).

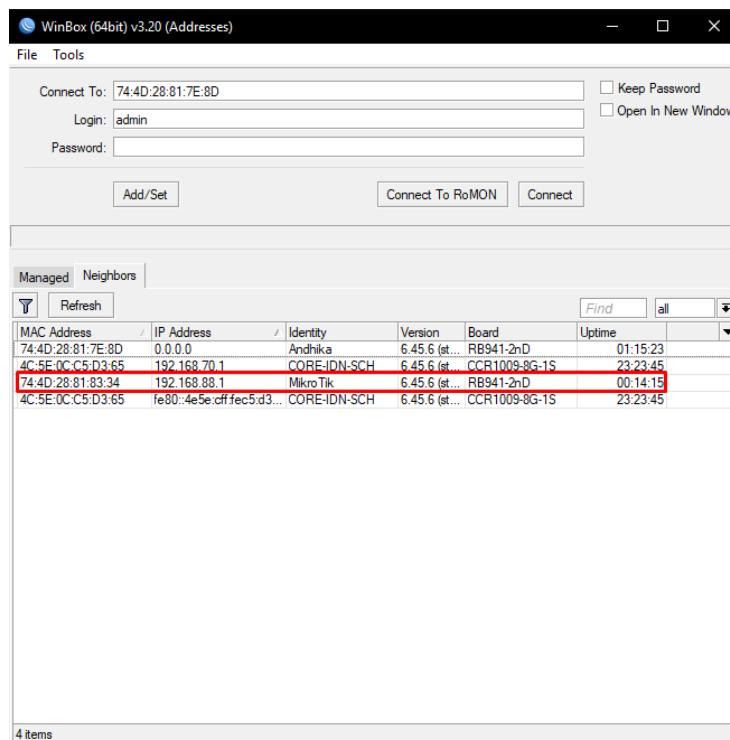


Lalu pilih 'software' dibagian atas.



Kemudian pilih Winbox, dan pilih versi -bit yang sesuai dengan windows.

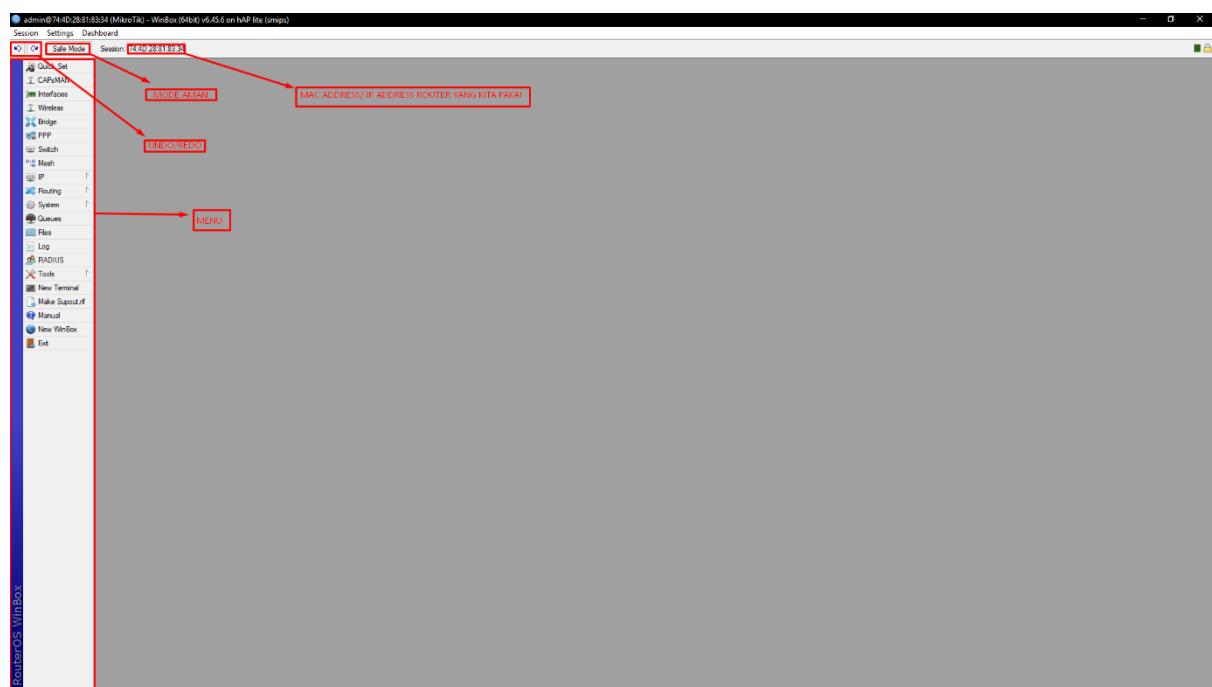
Jika sudah kita buka Winbox yang barusan kita download.



Beginilah tampilan awal Winbox, yang dilingkari merah adalah router kita.

Kita bisa mengakses lewat IP address maupun MAC address.

- Pertama-tama kita klik 'neighbors' lalu klik refresh.
- Pastikan juga kabel lan sudah terhubung dengan baik dan router dalam keadaan menyala.
- Jika sudah, kita isi kolom login dengan konfigurasi default.
- Login=admin
- Password=(kosong)
- Lalu kita klik 'connect'.



Beginilah isi dari Winbox, dari sini kita bisa mengonfigurasi Router MikroTik kita dengan Winbox.

## 2. Via Webfig

Webfig adalah alat untuk mengonfigurasi Router MikroTik menggunakan web browser. Webfig dapat diakses langsung dari router tanpa menggunakan aplikasi tambahan apapun, kecuali web browser untuk konfigurasi.

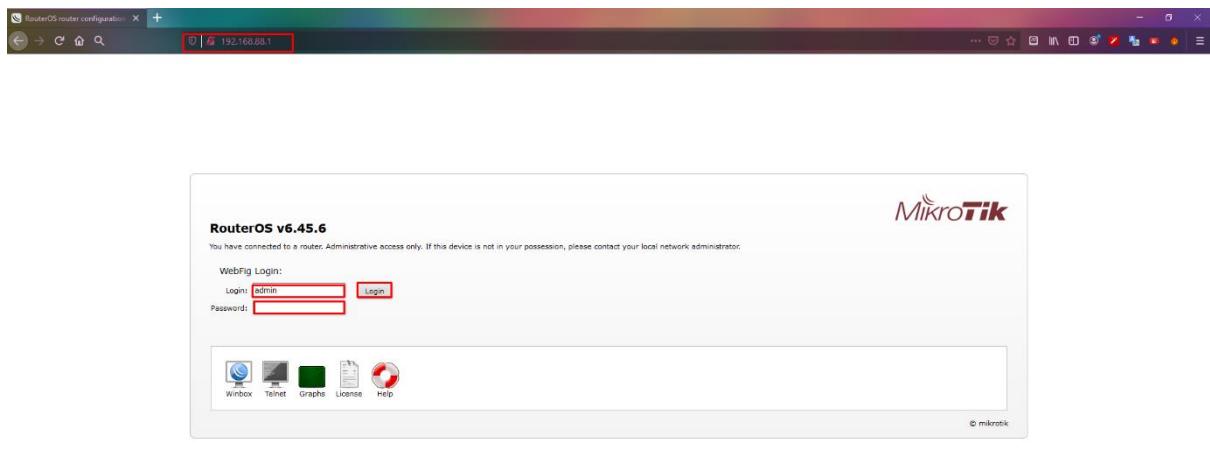
Webfig dapat diakses diberbagai platform web browser karena sifatnya yang independent, jadi kita dapat mengakses webfig di Firefox, Safari, Chrome, dll. Asalkan terhubung ke router.

Webfig juga dibuat sedemikian rupa agar menjadi pengganti Winbox, dengan fitur yang hampir sama seperti Winbox.

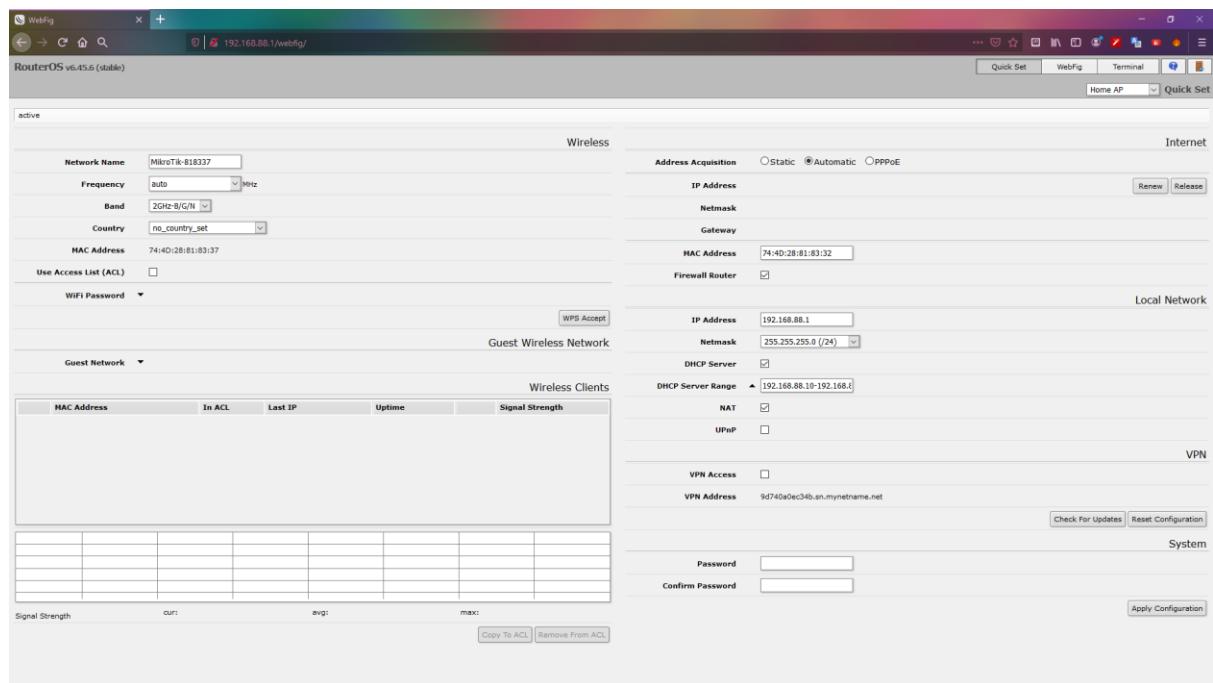
Webfig dapat dijalankan dengan cara memasukkan IP Address router di search bar browser.

Langsung saja kita masuk ke Lab nya.

Pertama-tama kita buka dulu browser-nya.



- Lalu kita ketikkan IP address Router kita di search bar=192.168.88.1
- Isi webfig login dengan login=admin, password=(kosong)
- Lalu klik login.



Seperti inilah tampilan awal dari webfig.

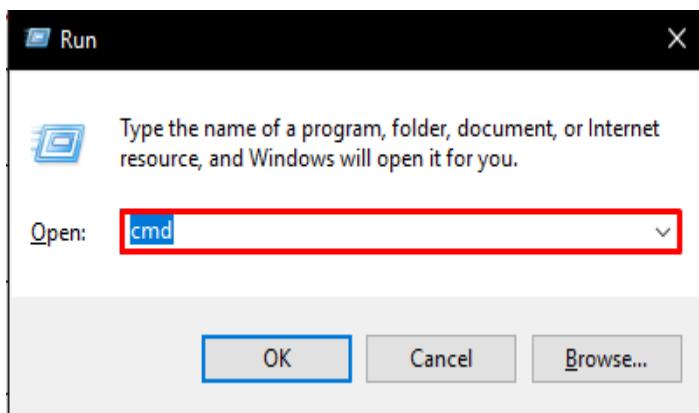
Di webfig ini ada 3 mode (Quick Set, Webfig, Terminal)

1. Quick Set: Mengonfigurasi MikroTik dengan cepat dan otomatis.
  2. Webfig: Mode ini sama saja seperti winbox, dengan tool yang hamper sama.
  3. Terminal: Di mode ini, kita mengonfigurasi MikroTik dengan basis teks atau CLI (Command Line Interface)
3. Via Telnet

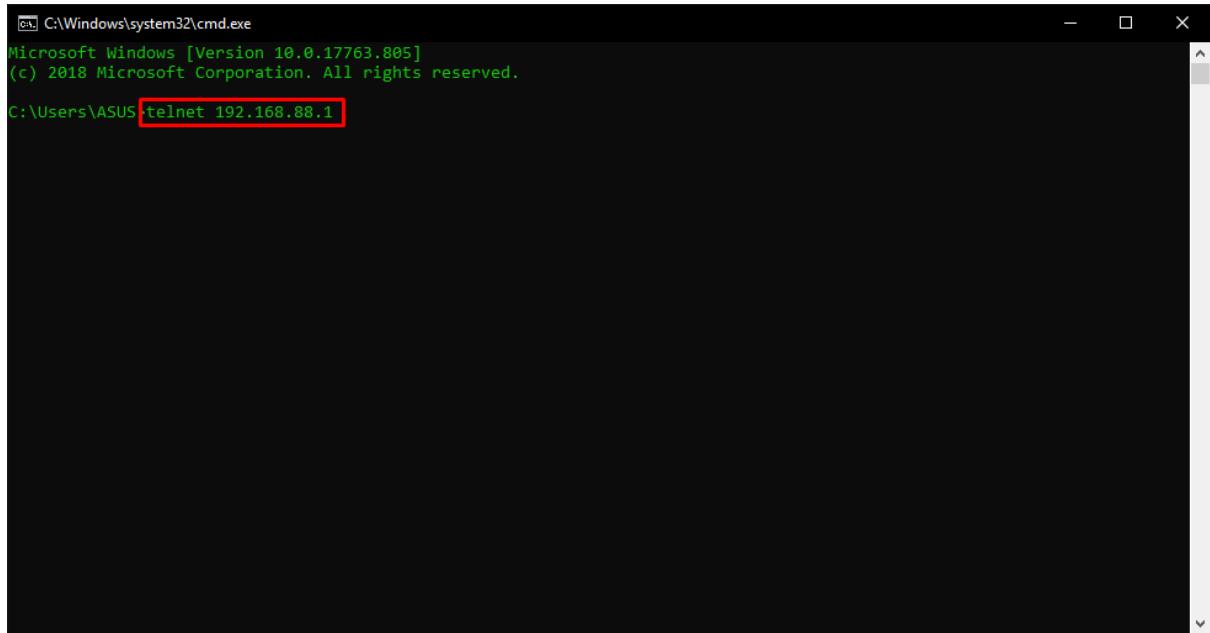
Telnet adalah singkatan dari Telecommunications Network Protocol, merupakan cara mengonfigurasi yang terjadi di jaringan internet dengan adanya servis dari Telnet. Dengan adanya Telnet, memungkinkan penggunanya untuk mengakses MikroTik lewat jaringan internet, Telnet menggunakan protocol Transmission Control Protocol (TCP) port 23.

Langsung lanjut ke Lab nya

- Pertama-tama kita buka CMD, tekan  + R pada keyboard.



- Kita isikan open=cmd
- Kemudian klik 'ok'



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ASUS>telnet 192.168.88.1
```

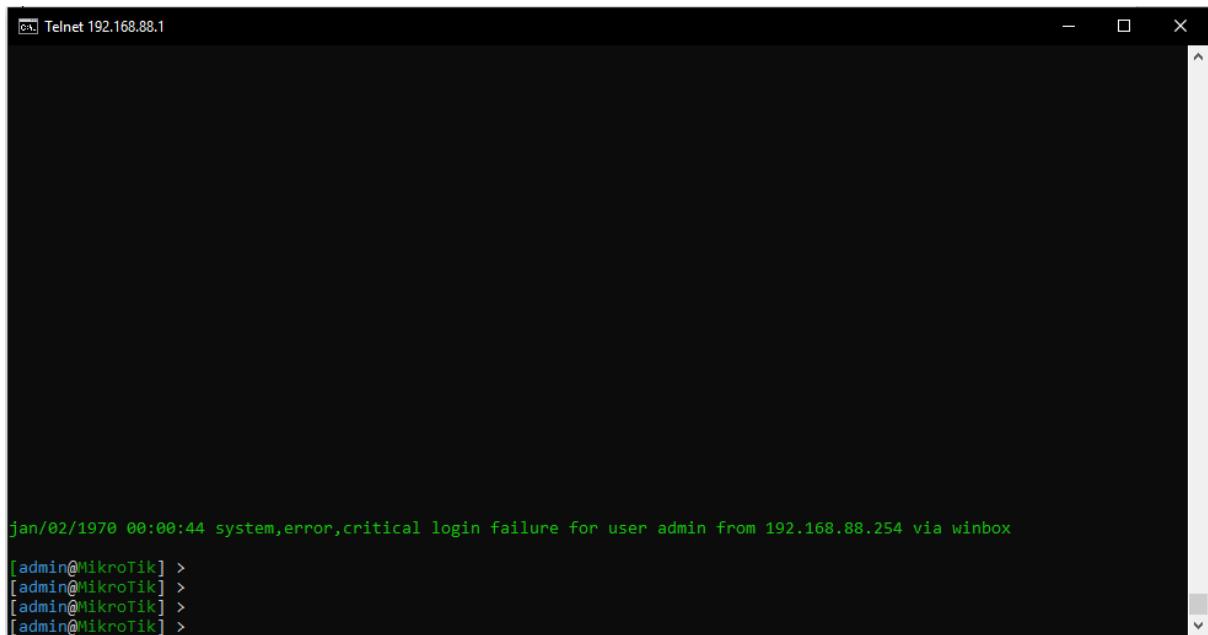
- Kemudian kita ketik ‘telnet 192.168.88.1’ (IP default router kita)



```
ca. Telnet 192.168.88.1

MikroTik v6.45.6 (stable)
Login: admin
Password: -
```

- Akan muncul MikroTik login page, kemudian kita isikan dengan pengaturan default. Login=admin, password=(kosong)

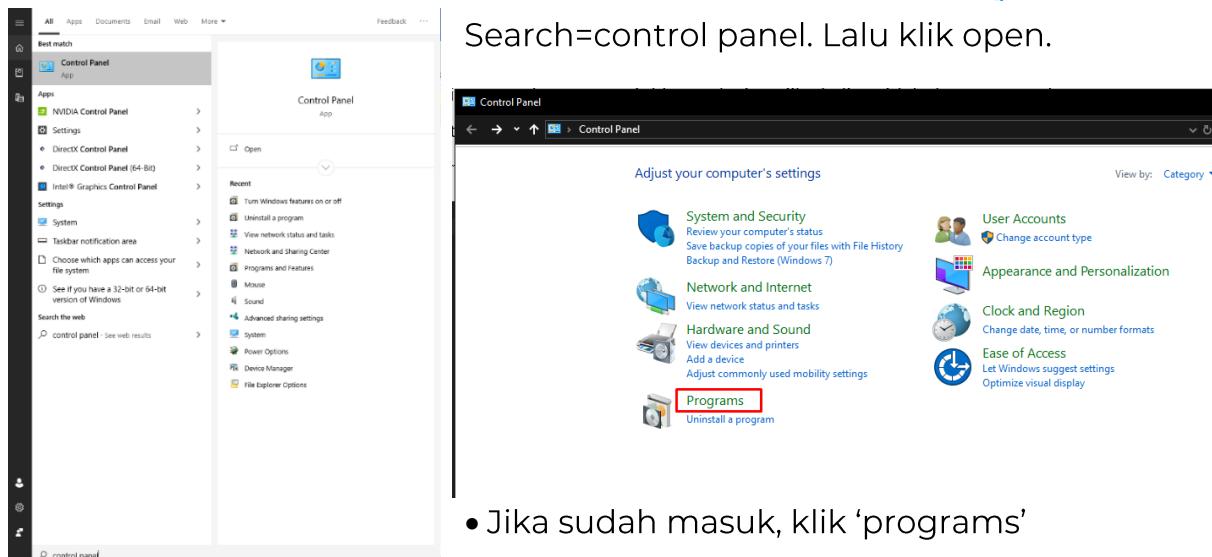


```
jan/02/1970 00:00:44 system,error,critical login failure for user admin from 192.168.88.254 via winbox  
[admin@MikroTik] >  
[admin@MikroTik] >  
[admin@MikroTik] >  
[admin@MikroTik] >
```

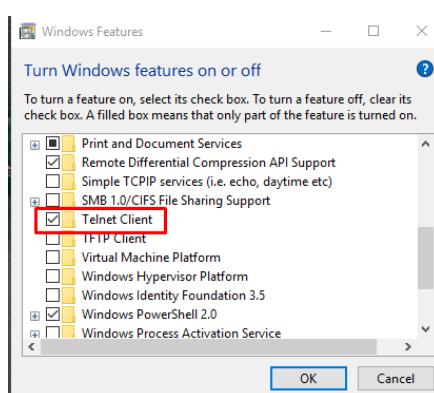
- Kita sudah memasuki telnet, dari sini kita bisa mengonfig router kita menggunakan telnet yang berbasis teks atau CLI.

Namun, ada beberapa pengguna yang tidak dapat menggunakan telnet, hal ini dikarenakan servis telnet di windows belum diaktifkan, oleh karena itu saya akan menunjukkan solusinya jika kalian tidak dapat mengakses telnet.

- Pertama-tama buka control panel terlebih dahulu.  + S.



- Jika sudah masuk, klik 'programs'
- Klik 'Turn Windows features on or off'

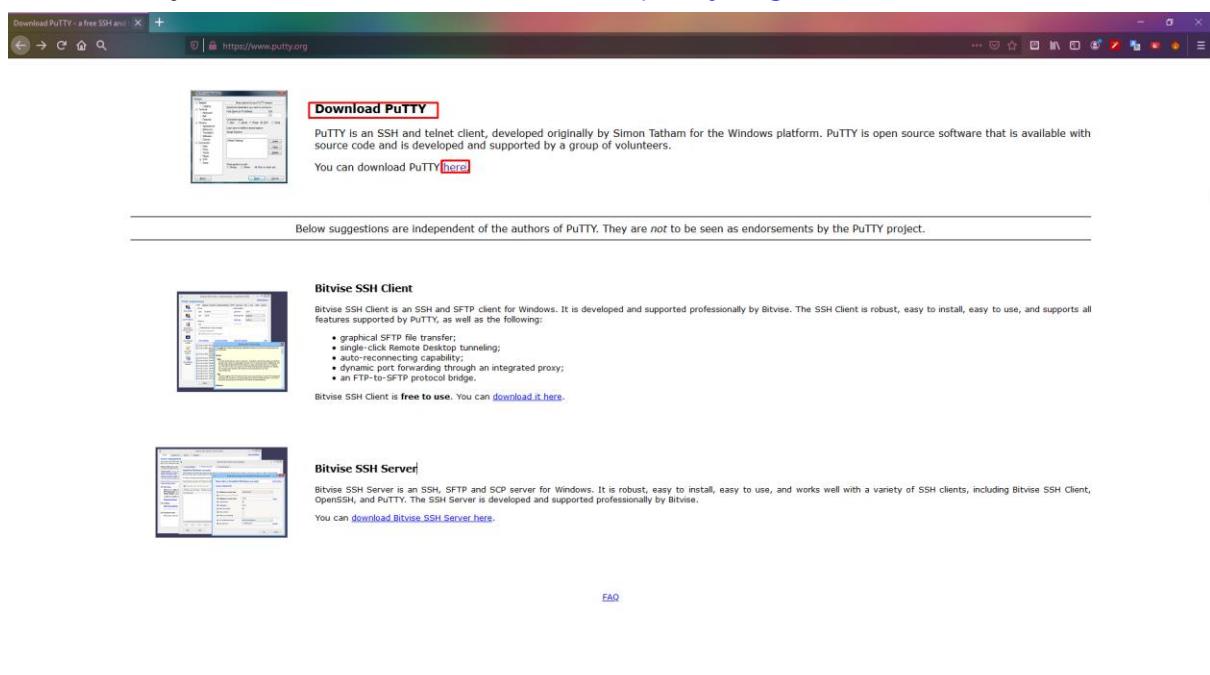


- Enable Telnet client, tunggu hingga prosesnya selesai
- Barulah kita bisa mengakses telnet.

#### 4. Via SSH

SSH merupakan singkatan dari Secure Shell yang merupakan sebuah protocol jaringan yang memanfaatkan kriptografi untuk mengonfigurasi router lebih aman karena telnet, rlogin, ftp dan rsh sangat rawan pencurian data, oleh karena itu digunakanlah SSH untuk mengonfigurasi jaringan dengan aman. SSH menggunakan TCP port 22.

SSH yang saya gunakan disini adalah PuTTY. Jika kalian belum memilikinya kalian bisa unduh di [www.putty.org](https://www.putty.org).



- Jika kalian sudah masuk, klik '[here](#)' yang berwarna biru dibagian 'You can download Putty here'.

## Package files

You probably want one of these. They include versions of all the PuTTY utilities.

(Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

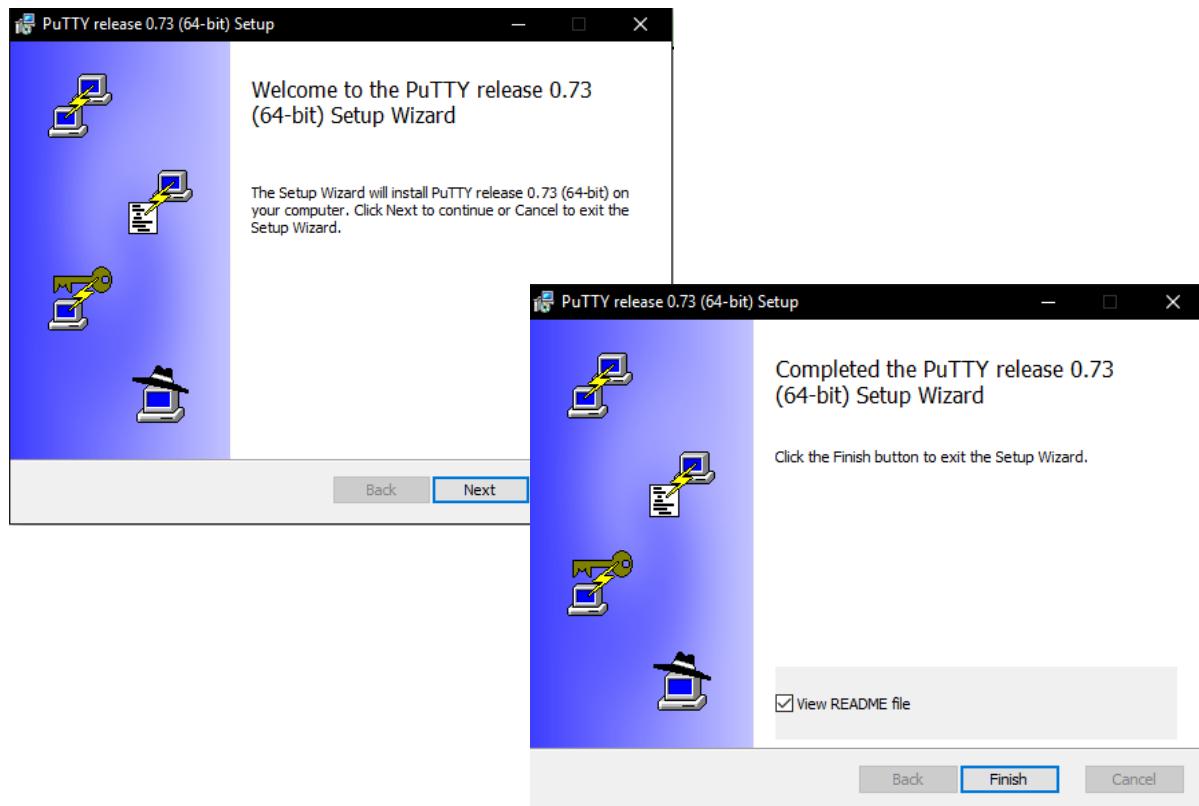
### MSI ('Windows Installer')

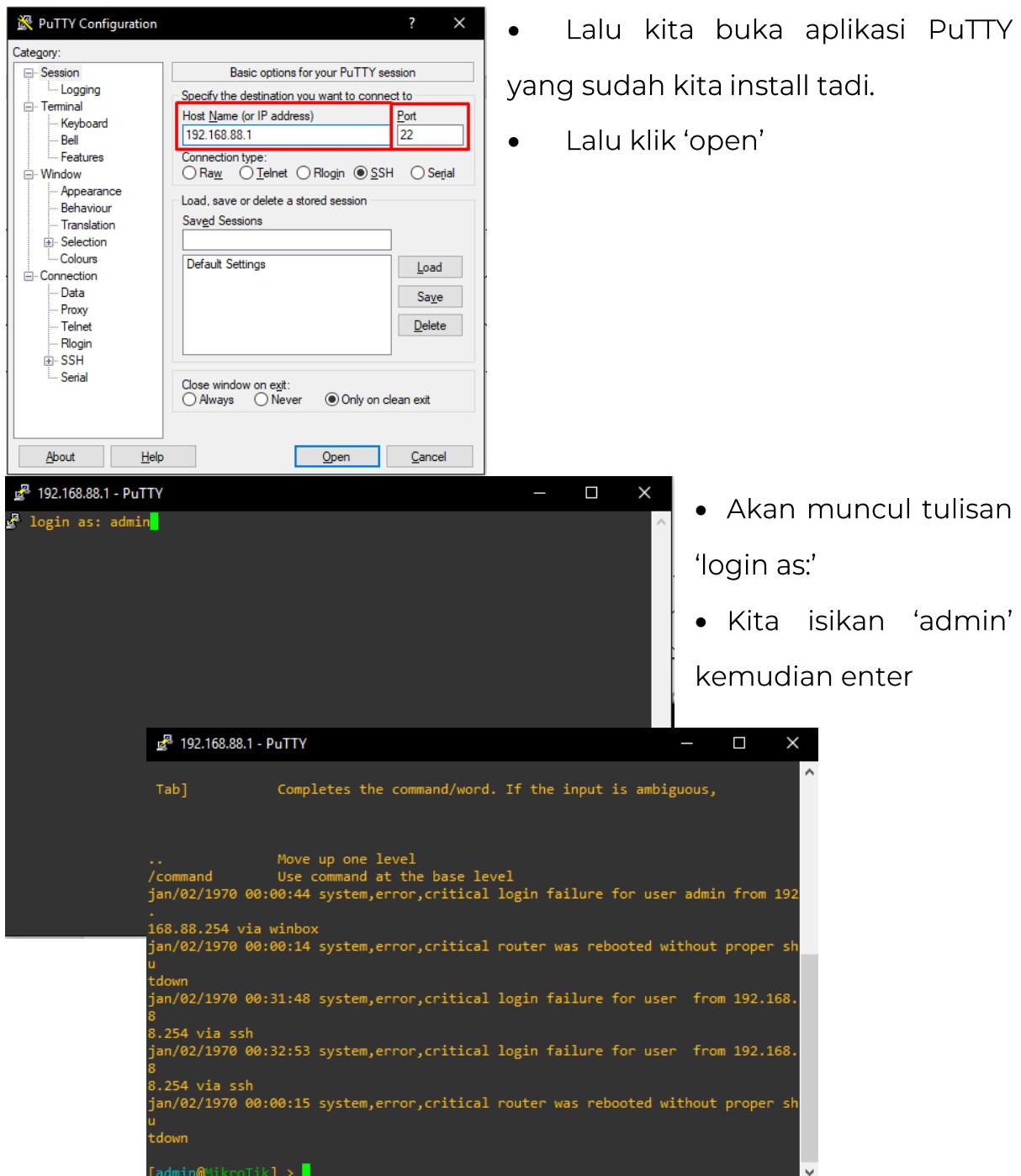
32-bit:	<a href="#">putty-0.73-installer.msi</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>
64-bit:	<a href="#">putty-64bit-0.73-installer.msi</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>

### Unix source archive

.tar.gz:	<a href="#">putty-0.73.tar.gz</a>	<a href="#">(or by FTP)</a>	<a href="#">(signature)</a>
----------	-----------------------------------	-----------------------------	-----------------------------

- Pilih yang sesuai dengan arsitektur windows kalian 32-bit atau 64-bit. Lalu unduh.
- Jalankan setup seperti biasa, tinggal next dan ok.





- Kita akan masuk kedalam SSH yang berbasis teks atau CLI.
- Dari sini kita bisa mengonfigurasi sesuai kebutuhan kita.

NOTE: Untuk Telnet dan SSH. Pada CLI, kita bisa tekan 'tab' pada keyboard jika kita tidak tahu command apa yang harus kita pakai/gunakan.

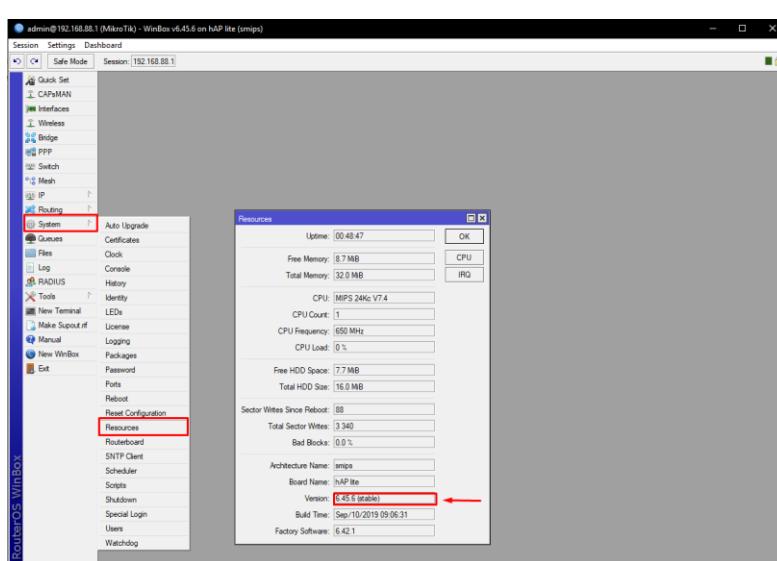
# MELIHAT VERSI MIKROTIK

Setiap Router MikroTik yang kita punya pasti memiliki versi RouterOS nya masing-masing, seperti router hAP-lite yang saya miliki.

Ada banyak cara untuk melihat versi MikroTik, mulai dari yang paling mudah menggunakan winbox/webfig yang berbasis GUI, sampai menggunakan Telnet/SSH yang berbasis teks atau CLI.

## 1. Via Winbox

Menggunakan Winbox adalah cara yang paling mudah, karena sudah menggunakan GUI yang mempermudah kita jadi tinggal klik-klik saja, tidak perlu mengetik seperti di Telnet atau SSH. Baiklah kita langsung coba.



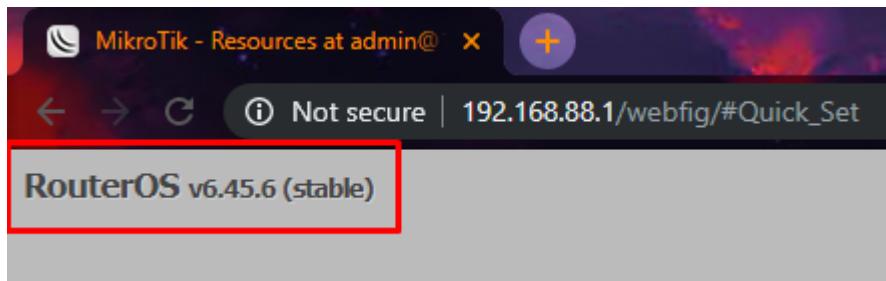
- Pertama-tama kita buka Winbox dan hubungkan kepada router yang ingin kita cek, lalu kita masuk ke Winbox nya

- Untuk mengeceknya klik 'System>Resources>Version'
- Di table Resource tertulis 'Version: 6.45.6 (stable)'. 6.45.6 adalah versi RouterOS router hAP-lite milik saya.

## 2. Via Webfig

Menggunakan webfig juga sangat mudah, disamping tidak perlu menggunakan aplikasi tambahan seperti Winbox karena harus diunduh terlebih dahulu, Webfig dapat digunakan disemua browser (karena memang digunakan di browser). Baiklah langsung kita coba.

- Pertama-tama kita buka webfig dibrowser dan masuk.



- Dipojok kiri atas sudah tertera versi dari RouterOS nya, untuk milik saya yaitu versi 6.45.6(stable)

### 3. Via Telnet

Jika menggunakan telnet kita melihat versi MikroTik ini dengan cara mengetik command nya di CLI, memang agak susah, tidak seperti di Winbox/Webfig yang mudah karena menggunakan GUI.

- Pertama kita buka telnet ke IP router kita, seperti di Lab sebelumnya.
- Jika sudah masuk ke CLI, ketikkan ‘system resource print’

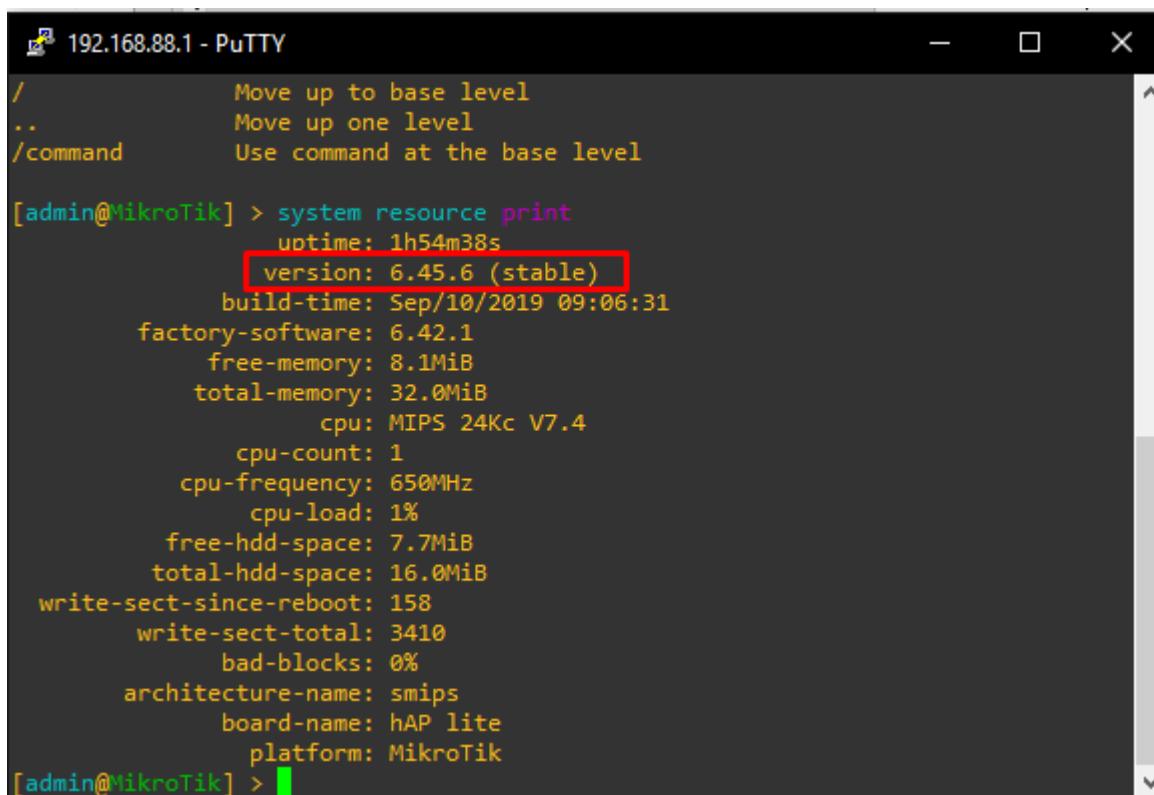
```
[admin@MikroTik] > system resource
[admin@MikroTik] /system resource>
cpu irq export get monitor print
[admin@MikroTik] /system resource> print
    uptime: 1h40m6s
        version: 6.45.6 (stable)
            build-time: Sep/10/2019 09:06:31
                factory-software: 6.42.1
                    free-memory: 8.2MiB
                        total-memory: 32.0MiB
                            cpu: MIPS 24Kc V7.4
                                cpu-count: 1
                                    cpu-frequency: 650MHz
                                        cpu-load: 2%
                                            free-hdd-space: 7.7MiB
                                                total-hdd-space: 16.0MiB
                                                    write-sect-since-reboot: 147
                                                        write-sect-total: 3399
                                                            bad-blocks: 0%
                                                                architecture-name: smips
                                                                    board-name: hAP lite
                                                                        platform: MikroTik
[admin@MikroTik] /system resource>
```

- Disitu tertulis ‘version: 6.45.6 (stable)’ dan itu adalah versi MikroTik di router saya.

#### 4. Via SSH

Menggunakan SSH tidak jauh beda dengan menggunakan Telnet karena sama-sama menggunakan CLI, command yang digunakan pun sama persis. Namun, fungsi antara SSH dan Telnet berbeda, Telnet sangat rawan untuk pencurian data, oleh karena itu digunakanlah SSH agar lebih aman.

- Pertama-tama kita buka PuTTY yang telah kita unduh dan masuk menggunakan IP router kita.
- Ketikkan command 'system resource print'.



The screenshot shows a PuTTY terminal window titled '192.168.88.1 - PuTTY'. The command 'system resource print' has been entered, and its output is displayed. The output includes various system parameters such as uptime, version, build-time, factory-software, memory details, CPU information, and disk space. The 'version' line is highlighted with a red rectangle. The terminal prompt '[admin@MikroTik] >' appears at the bottom.

```
/           Move up to base level
..          Move up one level
/command    Use command at the base level

[admin@MikroTik] > system resource print
    uptime: 1h54m38s
    version: 6.45.6 (stable) version: 6.45.6 (stable)
    build-time: Sep/10/2019 09:06:31
    factory-software: 6.42.1
        free-memory: 8.1MiB
        total-memory: 32.0MiB
            cpu: MIPS 24Kc V7.4
            cpu-count: 1
            cpu-frequency: 650MHz
            cpu-load: 1%
        free-hdd-space: 7.7MiB
        total-hdd-space: 16.0MiB
    write-sect-since-reboot: 158
        write-sect-total: 3410
        bad-blocks: 0%
    architecture-name: smips
        board-name: hAP lite
        platform: MikroTik
[admin@MikroTik] >
```

# MELIHAT FITUR MIKROTIK

MikroTik memiliki banyak sekali fitur-fitur. Seperti yang sudah saya jelaskan diawal buku, nah sekarang kita akan melihat, fitur apa sajakah yang ada dirouter kita.

Untuk caranya sendiri ada banyak, seperti dengan GUI (Winbox, Webfig) dan CLI (Telnet, SSH).

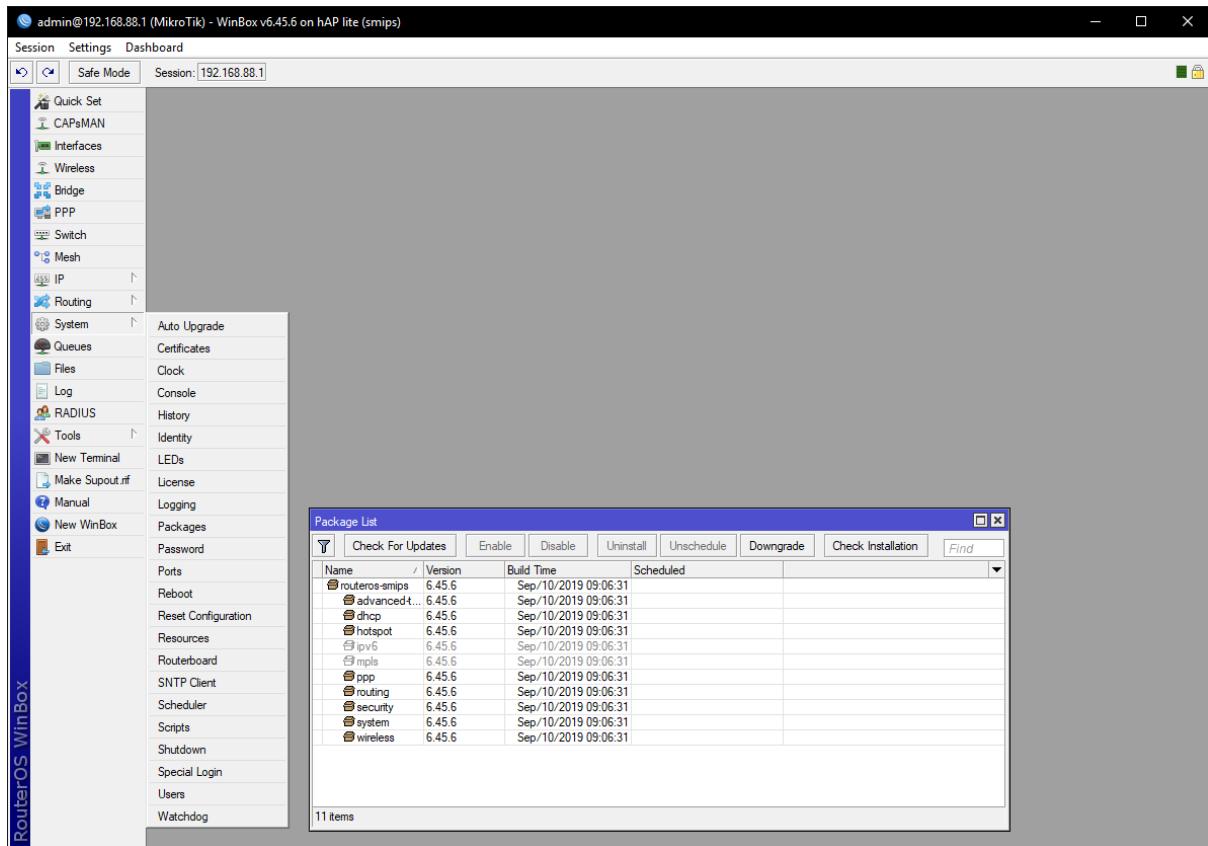
Untuk Via GUI kita tinggal klik di 'system>packages'

## 1. Via Webfig

The screenshot shows the RouterOS v6.45.6 (stable) interface in Webfig mode. The left sidebar has a tree view with 'System' selected. Under 'System', 'Packages' is also selected and highlighted with a red box. The main content area shows a table titled 'Package List' with 11 items. The table has columns: Name, Version, Build Time, and Scheduled. The packages listed are: advanced-tools, dhcp, hotspot, l3fwd, l3fwd-ipv6, l3fwd-ospf, ip, ipsec, routeros-empis, routing, security, system, and wireless. All packages are version 6.45.6 and were built on Sep/10/2019 09:06:32.

Name	Version	Build Time	Scheduled
advanced-tools	6.45.6	Sep/10/2019 09:06:32	
dhcp	6.45.6	Sep/10/2019 09:06:32	
hotspot	6.45.6	Sep/10/2019 09:06:32	
l3fwd	6.45.6	Sep/10/2019 09:06:32	
l3fwd-ipv6	6.45.6	Sep/10/2019 09:06:32	
l3fwd-ospf	6.45.6	Sep/10/2019 09:06:32	
ip	6.45.6	Sep/10/2019 09:06:32	
ipsec	6.45.6	Sep/10/2019 09:06:32	
routeros-empis	6.45.6	Sep/10/2019 09:06:32	
routing	6.45.6	Sep/10/2019 09:06:32	
security	6.45.6	Sep/10/2019 09:06:32	
system	6.45.6	Sep/10/2019 09:06:32	
wireless	6.45.6	Sep/10/2019 09:06:32	

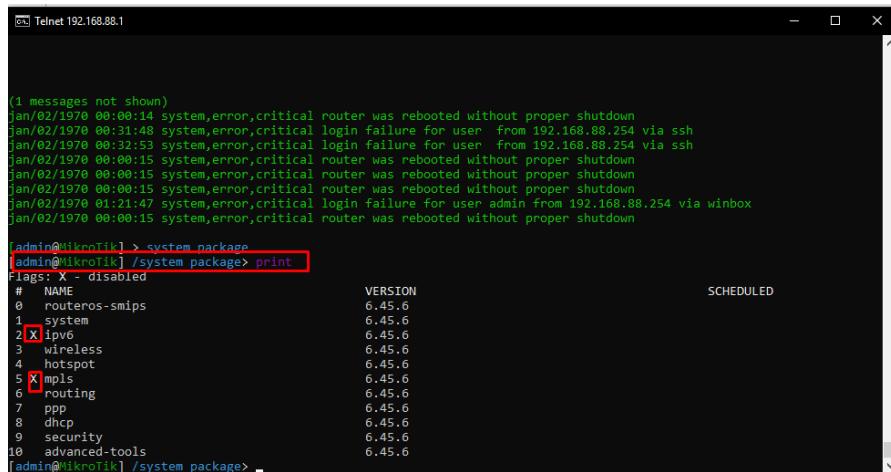
## 2. Via Winbox



- Disitu terlihat bahwa IPv6 dan MPLS berwarna abu-abu, yang berarti ter-disabled, dan untuk Lab selanjutnya, kita akan meng-enable paket/fitur yang ada di MikroTik.

Sedangkan untuk Via CLI seperti Telnet dan SSH, tinggal ketikkan command 'system package' di CLI.

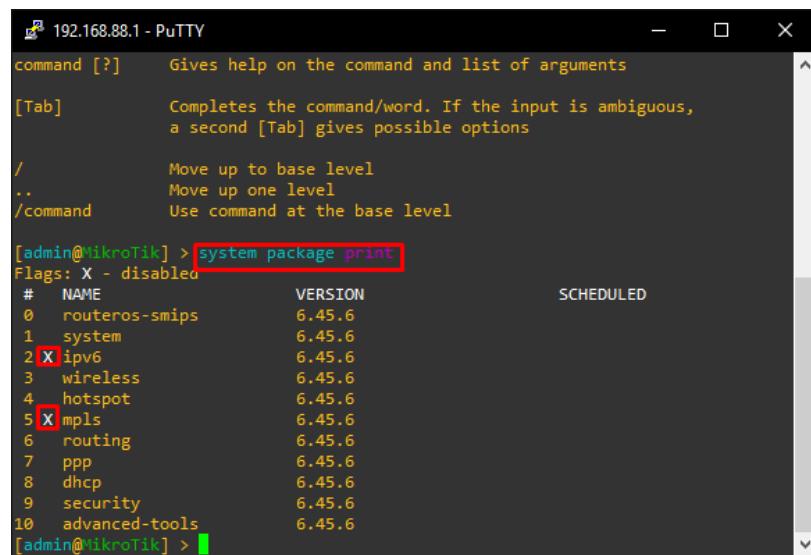
### 3. Via Telnet



```
(1 messages not shown)
jan/02/1970 00:00:14 system,error,critical router was rebooted without proper shutdown
jan/02/1970 00:31:48 system,error,critical login failure for user from 192.168.88.254 via ssh
jan/02/1970 00:32:53 system,error,critical login failure for user from 192.168.88.254 via ssh
jan/02/1970 00:00:15 system,error,critical router was rebooted without proper shutdown
jan/02/1970 00:00:15 system,error,critical router was rebooted without proper shutdown
jan/02/1970 00:00:15 system,error,critical router was rebooted without proper shutdown
jan/02/1970 01:21:47 system,error,critical login failure for user admin from 192.168.88.254 via winbox
jan/02/1970 00:00:15 system,error,critical router was rebooted without proper shutdown

[admin@MikroTik] > system package
[admin@MikroTik] /system package> print
Flags: X - disabled
#  NAME          VERSION      SCHEDULED
0  routertos-smips  6.45.6
1  system        6.45.6
2  X ipv6        6.45.6
3  wireless      6.45.6
4  hotspot        6.45.6
5  X mpls        6.45.6
6  routing        6.45.6
7  ppp            6.45.6
8  dhcp            6.45.6
9  security        6.45.6
10 advanced-tools 6.45.6
[admin@MikroTik] /system package> _
```

### 4. Via SSH (PuTTY).



```
command [?]      Gives help on the command and list of arguments
[Tab]           Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options
/
..              Move up one level
/command        Use command at the base level

[admin@MikroTik] > system package print
Flags: X - disabled
#  NAME          VERSION      SCHEDULED
0  routertos-smips  6.45.6
1  system        6.45.6
2  X ipv6        6.45.6
3  wireless      6.45.6
4  hotspot        6.45.6
5  X mpls        6.45.6
6  routing        6.45.6
7  ppp            6.45.6
8  dhcp            6.45.6
9  security        6.45.6
10 advanced-tools 6.45.6
[admin@MikroTik] > _
```

Dikedua contoh diatas, terdapat tanda 'X' pada IPv6 dan MPLS, dan 'X' tersebut berarti paket yang tertandai itu ter-disable.

# ENABLE/DISABLE FITUR MIKROTIK

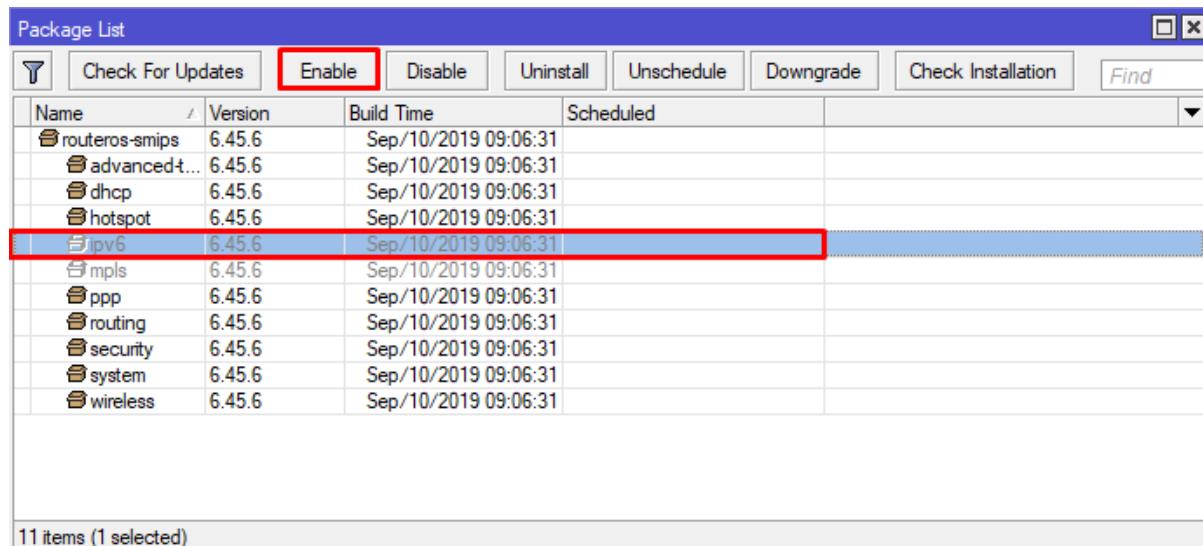
Seperti yang sebelumnya kita bahas, ada fitur di mikrotik yang secara default ter-disable yaitu IPv6 dan MPLS. Nah kali ini, kita akan membahas bagaimana caranya meng-enable dan men-disable.

Seperti biasa, ada 2 cara untuk meg-enable/men-disable fitur di MikroTik yaitu GUI dan CLI

## Enable Fitur

### 1. Via Winbox

- Pertama-tama buka Winbox, klik menu 'system>package'



Name	Version	Build Time	Scheduled
routeros-smips	6.45.6	Sep/10/2019 09:06:31	
advancedt...	6.45.6	Sep/10/2019 09:06:31	
dhcp	6.45.6	Sep/10/2019 09:06:31	
hotspot	6.45.6	Sep/10/2019 09:06:31	
ipv6	6.45.6	Sep/10/2019 09:06:31	
mpls	6.45.6	Sep/10/2019 09:06:31	
ppp	6.45.6	Sep/10/2019 09:06:31	
routing	6.45.6	Sep/10/2019 09:06:31	
security	6.45.6	Sep/10/2019 09:06:31	
system	6.45.6	Sep/10/2019 09:06:31	
wireless	6.45.6	Sep/10/2019 09:06:31	

11 items (1 selected)

- Didalam package list, klik fitur yang ter-disabled, paket yang ter-disable berwarna abu. Contoh saya akan meng-enable IPv6.
- Kemudian klik enable tab atas.

Package List

Package List					
	Name	Version	Build Time	Scheduled	
↳	routeros-smips	6.45.6	Sep/10/2019 09:06:31		
↳	advancedt...	6.45.6	Sep/10/2019 09:06:31		
↳	dhcp	6.45.6	Sep/10/2019 09:06:31		
↳	hotspot	6.45.6	Sep/10/2019 09:06:31		
↳	↳ ipv6	6.45.6	Sep/10/2019 09:06:31	scheduled for enable	
↳	mpls	6.45.6	Sep/10/2019 09:06:31		
↳	ppp	6.45.6	Sep/10/2019 09:06:31		
↳	routing	6.45.6	Sep/10/2019 09:06:31		
↳	security	6.45.6	Sep/10/2019 09:06:31		
↳	system	6.45.6	Sep/10/2019 09:06:31		
↳	wireless	6.45.6	Sep/10/2019 09:06:31		

11 items (1 selected)

The Winbox interface shows the following navigation tree on the left:

- System
  - Queues
  - Files
  - Log
  - RADIUS
  - Tools
    - New Terminal
    - Make Supout.if
    - Manual
    - New WinBox
    - Exit
- IP
  - ↳ IPv6
- Routing
- System
  - Queues
  - Files
  - Log
  - RADIUS
  - Tools
    - New Terminal
    - Make Supout.if

The 'Reboot' option under the 'System' menu is highlighted with a red box.

The main window displays the 'Package List' with the following table:

Package List					
	Name	Version	Build Time	Scheduled	
↳	routeros-smips	6.45.6	Sep/10/2019 09:06:31		
↳	advancedt...	6.45.6	Sep/10/2019 09:06:31		
↳	dhcp	6.45.6	Sep/10/2019 09:06:31		
↳	hotspot	6.45.6	Sep/10/2019 09:06:31		
↳	↳ ipv6	6.45.6	Sep/10/2019 09:06:31		
↳	mpls	6.45.6	Sep/10/2019 09:06:31		
↳	ppp	6.45.6	Sep/10/2019 09:06:31		
↳	routing	6.45.6	Sep/10/2019 09:06:31		
↳	security	6.45.6	Sep/10/2019 09:06:31		
↳	system	6.45.6	Sep/10/2019 09:06:31		
↳	wireless	6.45.6	Sep/10/2019 09:06:31		

11 items

- Akan ada tulisan ‘Scheduled for Enable’ yang berarti kita harus me-reboot Router kita agar fitur itu aktif, klik ‘system>reboot’
- Kita masuk lagi kedalam Winbox, disitu akan terlihat fitur IPv6 dibawah IP dan jika kita lihat di package list, tulisan IPv6 tidak berwarna abu lagi.

## 2. Via Webfig

- Pertama-tama kita buka webfig, klik 'system>package'

	Name	Version	Build Time
	advanced-tools	6.45.6	Sep/10/2019
	dhcp	6.45.6	Sep/10/2019
	hotspot	6.45.6	Sep/10/2019
	ipv6	6.45.6	Sep/10/2019
X	<b>mpls</b>	6.45.6	Sep/10/2019
	ppp	6.45.6	Sep/10/2019
	routeros-smips	6.45.6	Sep/10/2019
	routing	6.45.6	Sep/10/2019
	security	6.45.6	Sep/10/2019
	system	6.45.6	Sep/10/2019
	wireless	6.45.6	Sep/10/2019

- Lalu kita klik fitur yang akan kita enable, disini saya akan meng-enable MPLS

<input type="button" value="Close"/>	<input style="outline: 2px solid red; border-radius: 5px; padding: 2px 10px;" type="button" value="Enable"/>	<input type="button" value="Disable"/>	<input type="button" value="Uninstall"/>	<input type="button" value="Unschedule"/>
<b>Enabled</b> <input type="checkbox"/>				
<b>Name</b> mpls				
<b>Version</b> 6.45.6				
<b>Build Time</b> Sep/10/2019 09:06:31				
<b>Scheduled</b> scheduled for enable				

- Kita klik 'enable', lalu akan muncul tulisan 'scheduled for enable' berarti kita harus me-reboot agar fitur itu aktif

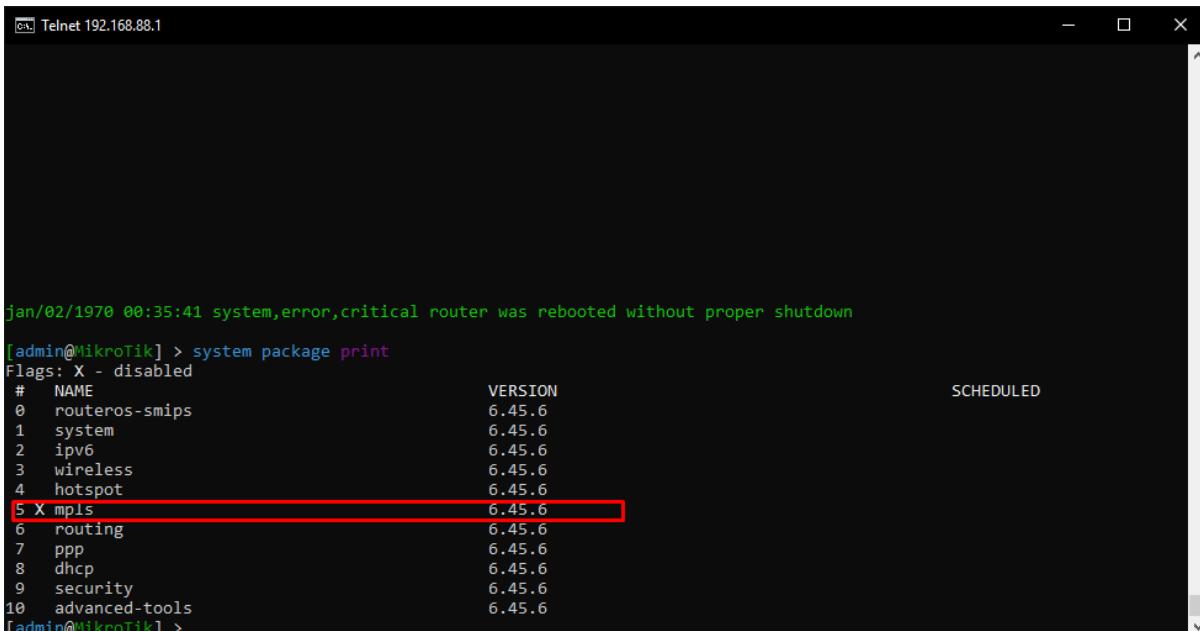
• Kita reboot Router kita di 'System>Reset Configuration' setelah itu klik 'yes'.

• Lalu kita bisa lihat fitur MPLS yang sudah aktif dibawah fitur IP, dan warna tulisannya sudah tidak abu lagi.

	<b>Name</b>	<b>Version</b>	<b>Build Time</b>	<b>S</b>
	advanced-tools	6.45.6	Sep/10/2019 09:06:31	
	dhcp	6.45.6	Sep/10/2019 09:06:31	
	hotspot	6.45.6	Sep/10/2019 09:06:31	
	ipv6	6.45.6	Sep/10/2019 09:06:31	
	<b>mpls</b>	<b>6.45.6</b>	<b>Sep/10/2019 09:06:31</b>	
	ppp	6.45.6	Sep/10/2019 09:06:31	
	routeros-smips	6.45.6	Sep/10/2019 09:06:31	
	routing	6.45.6	Sep/10/2019 09:06:31	
	security	6.45.6	Sep/10/2019 09:06:31	
	system	6.45.6	Sep/10/2019 09:06:31	
	wireless	6.45.6	Sep/10/2019 09:06:31	

### 3. Via Telnet

- Pertama-tama kita buka Telnet, lalu ketikkan di CLI, 'system package print' untuk melihat isi fitur MikroTik.



```
jan/02/1970 00:35:41 system,error,critical router was rebooted without proper shutdown
[admin@MikroTik] > system package print
Flags: X - disabled
#  NAME                      VERSION          SCHEDULED
0  routeros-smips            6.45.6
1  system                     6.45.6
2  ipv6                      6.45.6
3  wireless                  6.45.6
4  hotspot                    6.45.6
5 X mpls                     6.45.6
6  routing                   6.45.6
7  ppp                       6.45.6
8  dhcp                      6.45.6
9  security                  6.45.6
10 advanced-tools            6.45.6
[admin@MikroTik] >
```

- Dirouter saya, MPLS ter-disable, untuk mengetahuinya bisa dilihat dari tanda 'X' yang berada disamping tulisan MPLS.

- Untuk mengaktifkannya, ketik ‘system package enable mpls’.  
Kita bisa mengganti nama MPLS dengan nama fitur lain, asalkan fitur itu dalam posisi ter-disable. Contoh: ‘system package enable dhcp’ berarti kita meng-enable fitur DHCP, namun sebelumnya fitur DHCP harus dalam keadaan ter-disable.

```
[admin@mikrotik] > system package enable mpls
[admin@mikrotik] > system package print
Flags: X - disabled
#  NAME                      VERSION          SCHEDULED
0  routeros-smips            6.45.6
1  system                     6.45.6
2  ipv6                      6.45.6
3  wireless                  6.45.6
4  hotspot                   6.45.6
5 X mpls                     6.45.6          scheduled for enable
6  routing                   6.45.6
7  ppp                       6.45.6
8  dhcp                      6.45.6
9  security                  6.45.6
10 advanced-tools            6.45.6
[admin@mikrotik] >
```

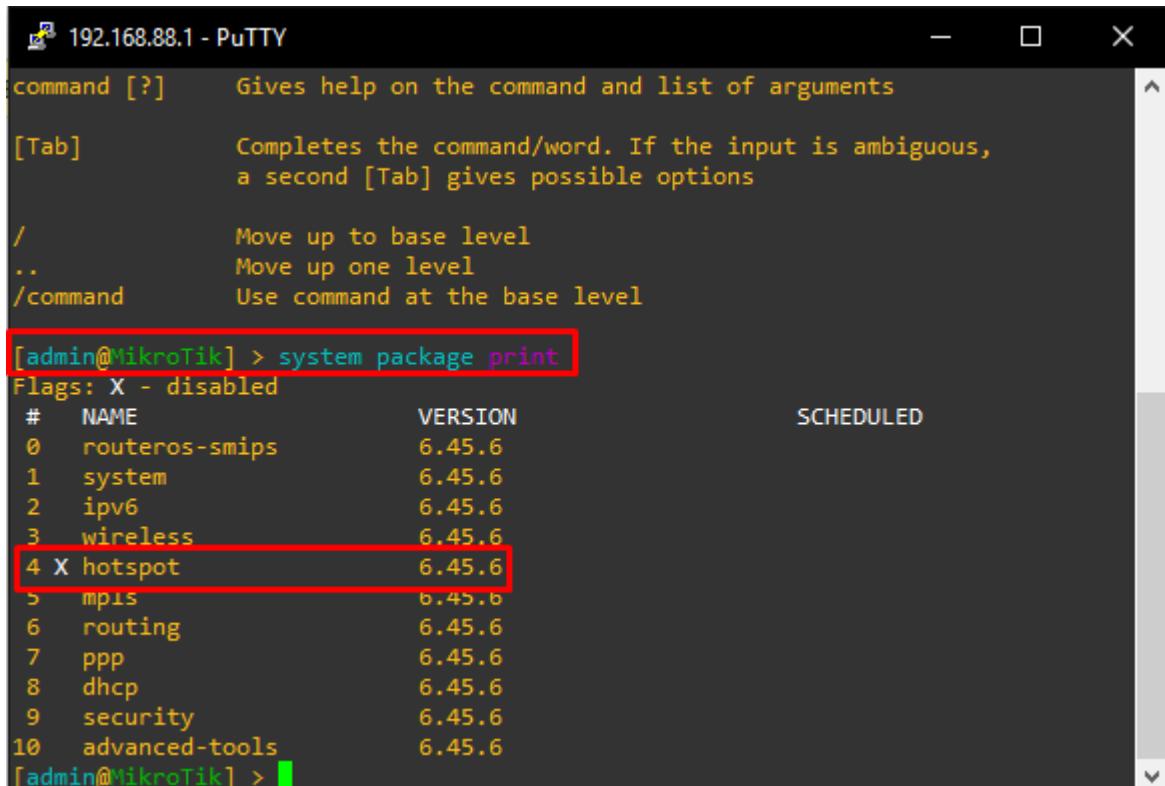
- Untuk mengeceknya, ketikkan kembali ‘system package print’ disitu tertulis ‘scheduled for enable’ pada MPLS, kita tinggal reboot untuk mengaktifkan fitur tersebut.

```
[admin@mikrotik] > system reboot
Reboot, yes? [y/N]:
y
system will reboot shortly
```

- Lalu kita reboot router kita dengan menggunakan command ‘system reboot’. Akan ada pilihan **yes** or **no**, kita pilih **yes**.
- Saat kita sudah masuk ke Telnet setelah reboot, ketikkan command ‘system package print’. Disitu akan terlihat, disebelah MPLS tidak ada tanda ‘X’. yang berarti fitur MPLS sudah aktif dan bisa digunakan.

#### 4. Via SSH

- Pertama-tama kita masuk dahulu kedalam SSH PuTTY. Dengan cara yang sama seperti di Telnet, ketikkan ‘system package print’



```
192.168.88.1 - PuTTY

command [?]      Gives help on the command and list of arguments
[Tab]           Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options
/
..             Move up one level
/command       Use command at the base level

[admin@mikrotik] > system package print
Flags: X - disabled
#  NAME          VERSION          SCHEDULED
0  routeros-smips  6.45.6
1  system         6.45.6
2  ipv6          6.45.6
3  wireless      6.45.6
4 X hotspot       6.45.6
5  mpis          6.45.6
6  routing        6.45.6
7  ppp            6.45.6
8  dhcp           6.45.6
9  security       6.45.6
10 advanced-tools 6.45.6
[admin@mikrotik] >
```

- Disitu bisa terlihat bahwa fitur Hotspot ter-disable, terlihat dari tanda ‘X’ yang ada disebelahnya.

- Lalu kita enable dengan mengetik command ‘system package enable hotspot’. Sama seperti telnet, Kita bisa mengganti nama Hotspot dengan nama fitur lain, asalkan fitur itu dalam posisi ter-disable. Contoh: ‘system package enable dhcp’ berarti kita meng-enable fitur DHCP, namun sebelumnya fitur DHCP harus dalam keadaan ter-disable.

```
[admin@MikroTik] > system package enable hotspot
[admin@MikroTik] > system package print
Flags: X - disabled
#  NAME          VERSION      SCHEDULED
0  routeros-smips 6.45.6
1  system        6.45.6
2  ipv6          6.45.6
3  wireless      6.45.6
4 X hotspot       6.45.6
5  mpls          6.45.6
6  routing        6.45.6
7  ppp            6.45.6
8  dhcp           6.45.6
9  security       6.45.6
10 advanced-tools 6.45.6
[admin@MikroTik] >
```

scheduled for enable

- Untuk mengeceknya, ketikkan kembali ‘system package print’ disitu tertulis ‘scheduled for enable’ pada Hotspot, kita tinggal reboot untuk mengaktifkan fitur tersebut.

```
[admin@MikroTik] > system reboot
Reboot, yes? [y/N]:
y
system will reboot shortly
```

- Lalu kita reboot router kita dengan menggunakan command ‘system reboot’. Akan ada pilihan **yes** or **no**, kita pilih **yes**.

4 hotspot 6.45.6

- Saat kita sudah masuk ke Telnet setelah reboot, ketikkan command 'system package print'. Disitu akan terlihat, disebelah Hotspot tidak ada tanda 'X'. yang berarti fitur Hotspot sudah aktif dan bisa digunakan.

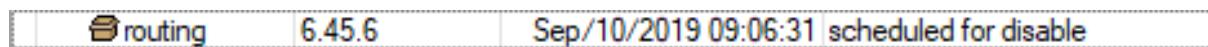
## Disable Fitur

### 1. Via Winbox

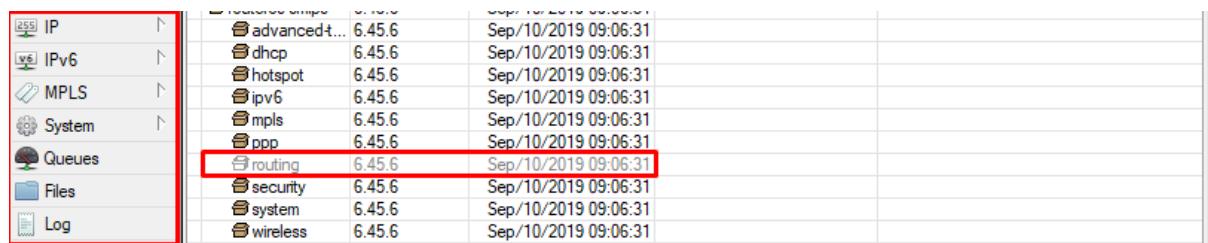
- Pertama-tama buka Winbox, klik fitur 'system>package'

Package List				
	Name	Version	Build Time	Scheduled
	Check For Updates	Enable	Disable	Uninstall
	routeros-smips	6.45.6	Sep/10/2019 09:06:31	
	advancedt...	6.45.6	Sep/10/2019 09:06:31	
	dhcp	6.45.6	Sep/10/2019 09:06:31	
	hotspot	6.45.6	Sep/10/2019 09:06:31	
	ipv6	6.45.6	Sep/10/2019 09:06:31	
	mpls	6.45.6	Sep/10/2019 09:06:31	
	ppp	6.45.6	Sep/10/2019 09:06:31	
	routing	6.45.6	Sep/10/2019 09:06:31	
	security	6.45.6	Sep/10/2019 09:06:31	
	system	6.45.6	Sep/10/2019 09:06:31	
	wireless	6.45.6	Sep/10/2019 09:06:31	
11 items (1 selected)				

- Kita klik fitur yang akan kita disable, misal fitur Routing.
- kemudian klik 'disable' di tab atas.



- Akan ada tulisan 'Scheduled for Enable' yang berarti kita harus me-reboot Router kita agar fitur itu aktif, klik 'system>reboot'
- Kita masuk lagi kedalam Winbox, di tab fitur, fitur Routing yang sebelumnya ada dibawah MPLS akan mengilang dan warna tulisan Routing di 'system package' akan berubah menjadi abu.

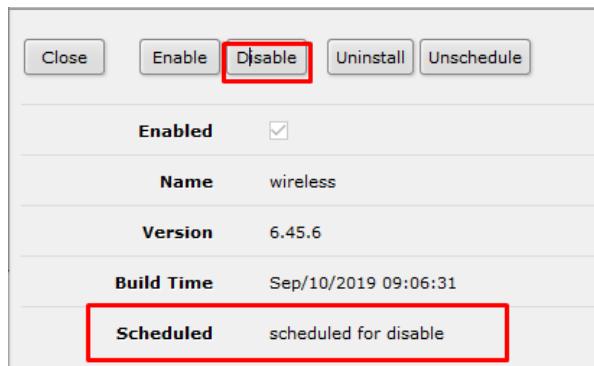


## 2. Via Webfig

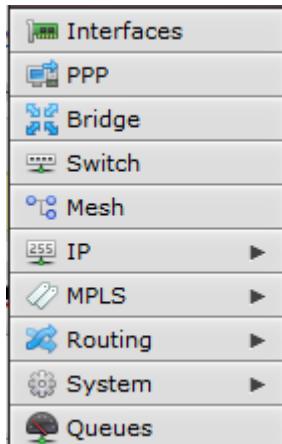
- Pertama-tama buka Webfig terlebih dahulu.
- Kemudian buka fitur 'system package'.



- Disini kita akan men-disable fitur Wireless, klik 'wireless'



- Pilih ‘disable’, lalu akan muncul tulisan ‘scheduled for disable’ yang berarti kita harus me-reboot router kita agar fitur tersebut bisa berjalan.



- Setelah kita reboot, kita bisa melihat bahwa fitur Wireless sudah hilang karena kita telah men-disable fiturnya.

### 3. Via Telnet.

- Pertama kita buka telnet ke IP router kita.
- Lalu ketikkan command ‘system package print’ untuk melihat daftar fitur di router kita.

```
[admin@MikroTik] > system package print
Flags: X - disabled
#   NAME                               VERSION
0   routeros-smips                      6.45.6
1   system                             6.45.6
2   ipv6                                6.45.6
3   wireless                           6.45.6
4   hotspot                            6.45.6
5   mpls                                6.45.6
6   routing                            6.45.6
7   ppp                                 6.45.6
8   dhcp                                6.45.6
9   security                           6.45.6
10  advanced-tools                     6.45.6
[admin@MikroTik] >
```

- Misalkan kita akan men-disable fitur PPP, maka kita harus mengetik command ‘system package disable ppp’.

```
[admin@MikroTik] > system package disable ppp
[admin@MikroTik] > system package pr
Flags: X - disabled
#   NAME                               VERSION          SCHEDULED
0   routeros-smips                      6.45.6
1   system                             6.45.6
2   ipv6                                6.45.6
3   wireless                           6.45.6
4   hotspot                            6.45.6
5   mpls                                6.45.6
6   routing                            6.45.6
7   ppp                                 6.45.6
8   uncp                                6.45.6
9   security                           6.45.6
10  advanced-tools                     6.45.6
[admin@MikroTik] >
```

- Lalu akan muncul tulisan ‘scheduled for disable’ yang berarti kita harus me-reboot router kita agar fitur tersebut bisa berjalan.

```
[admin@MikroTik] > system reboot
Reboot, yes? [y/N]:
y
system will reboot shortly
```

- Setelah itu ketik ‘system reboot’ ketik ‘y’.

```
[admin@MikroTik] > system package print
Flags: X - disabled
#  NAME                                VERSION
0  routeros-smips                      6.45.6
1  system                               6.45.6
2  ipv6                                 6.45.6
3  wireless                            6.45.6
4  hotspot                              6.45.6
5  mpls                                 6.45.6
6  routing                             6.45.6
7 X ppp                                6.45.6
8  dnncp                               6.45.6
9  security                            6.45.6
10 advanced-tools                     6.45.6
[admin@MikroTik] >
```

- Lalu ketikkan ‘system package print’ untuk mengecek apakah fitur yang tadi kita disable benar-benar sudah ter-disable.
- Jika sebelah tulisannya ada tanda (flag) ‘X’ berarti fitur itu sudah ter-disable dan tidak bisa digunakan.

#### 4. Via SSH

- Pertama-tama kita masuk ke SSH IP router kita.
- Lalu ketikkan command ‘system package print’ untuk melihat daftar fitur di router kita.

```
[admin@MikroTik] > system package print
Flags: X - disabled
#  NAME                      VERSION
0  routeros-smips            6.45.6
1  system                     6.45.6
2  ipv6                      6.45.6
3  wireless                  6.45.6
4  hotspot                    6.45.6
5  mpls                      6.45.6
6  routing                    6.45.6
7  ppp                       6.45.6
8  dhcp                      6.45.6
9  security                   6.45.6
10 advanced-tools            6.45.6
[admin@MikroTik] > system package disable ppp
```

- Lalu misalnya kita mau men-disable fitur PPP, maka ketikkan ‘system disable ppp’

```
[admin@MikroTik] > system package print
Flags: X - disabled
#  NAME                      VERSION          SCHEDULED
0  routeros-smips            6.45.6
1  system                     6.45.6
2  ipv6                      6.45.6
3  wireless                  6.45.6
4  hotspot                    6.45.6
5  mpls                      6.45.6
6  routing                    6.45.6
7  ppp                       6.45.6
8  dhcp                      6.45.6
9  security                   6.45.6
10 advanced-tools            6.45.6
[admin@MikroTik] >
```

- Lalu akan muncul tulisan ‘scheduled for disable’ yang berarti kita harus me-reboot router kita agar fitur tersebut bisa berjalan.

```
[admin@MikroTik] > system reboot
Reboot, yes? [y/N]:
y
system will reboot shortly
```

- Ketik ‘system reboot’ untuk me-reboot router kita.

```
[admin@MikroTik] > system package print
Flags: X - disabled
#   NAME           VERSION
0   routeros-smips 6.45.6
1   system          6.45.6
2   ipv6            6.45.6
3   wireless        6.45.6
4   hotspot          6.45.6
5   mpls             6.45.6
6   routing          6.45.6
7 X ppp              6.45.6
8   dhcpc            6.45.6
9   security          6.45.6
10  advanced-tools   6.45.6
[admin@MikroTik] >
```

Lalu ketikkan ‘system package print’ untuk mengecek apakah fitur yang tadi kita disable benar-benar sudah ter-disable.

- Jika sebelah tulisannya ada tanda (flag) ‘X’ berarti fitur itu sudah ter-disable dan tidak bisa digunakan.

## Uninstall Fitur.

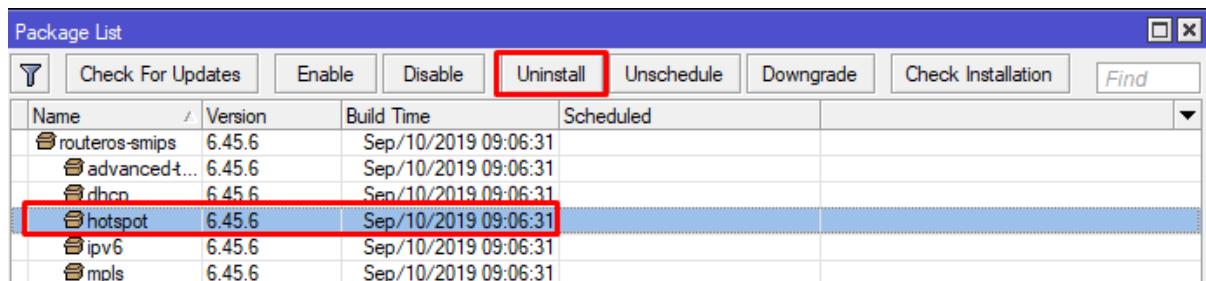
Untuk meng-uninstall fitur ini tidak jauh beda dengan men-disable, hanya saja, perbedaannya adalah:

- Disable= Menghilangkan fitur sementara sampai diaktifkan kembali.
- Uninstall= Menghilangkan fitur selamanya (permanen).

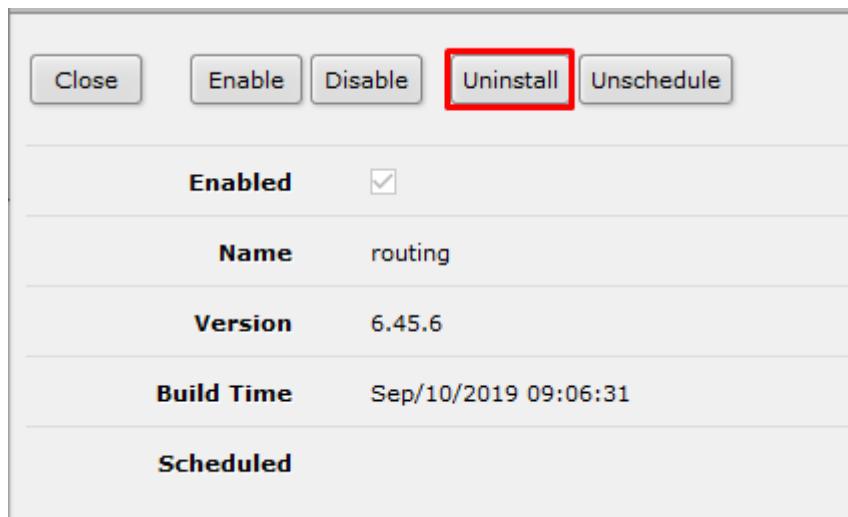
Ada 2 cara untuk uninstall, via GUI dan CLI.

### Via GUI

- Jika di Winbox, kita bisa meng-uninstall di package list, di tab atas ada tombol uninstall.



- Jika di Webfig, kita tinggal klik fitur mana yang mau kita uninstall di system package, lalu klik 'uninstall'.



## Via CLI

- Jika lewat CLI, meskipun itu SSH ataupun Telnet, commandnya tetap sama.

```
[admin@MikroTik] > system package print
Flags: X - disabled
#   NAME                      VERSION
0   routeros-smips            6.45.6
1   system                     6.45.6
2   ipv6                      6.45.6
3   wireless                  6.45.6
4   hotspot                    6.45.6
5   mpls                      6.45.6
6   routing                    6.45.6
7 X  ppp                      6.45.6
8   dhcp                      6.45.6
9   security                  6.45.6
10  advanced-tools            6.45.6
[admin@MikroTik] > system package uninstall mpls
```

- Pertama-tama ketik 'system package print' untuk melihat daftar fitur.
- Kemudian ketik 'system package uninstall mpls' jika misalnya kita ingin menghapus fitur MPLS dari router kita.

Note=SSH dan Telnet itu sama, karena basisnya sama-sama CLI. Jadi seluruh command yang ada di Telnet bisa digunakan juga di SSH, yang membedakan hanyalah fungsinya.

# UPGRADE FITUR MIKROTIK

MikroTik selalu meng-update fitur-fiturnya, hal ini bertujuan agar memperbaiki bug/error yang terjadi di versi RouterOS MikroTik sebelumnya, selain memperbaiki update MikroTik dilakukan untuk memperbarui fitur-fitur yang ada menjadi lebih baik lagi.

Untuk mengunduh pembaruan tersebut, kita bisa unduh di website MikroTik: [www.mikrotik.com/download](http://www.mikrotik.com/download).

The screenshot shows the MikroTik Software download page. The RouterOS section is highlighted. It lists several architecture categories: MIPSBE, Main package, Extra packages, SMIPS, Main package, Extra packages, TILE, Main package, Extra packages, The Dude server, PPC, Main package, Extra packages, ARM, Main package, Extra packages, The Dude server, X86, Main package, Extra packages, CD Image, The Dude server, MMIPS, Main package. Each category has four columns representing different software versions: 6.44.6 (Long-term), 6.45.7 (Stable), 6.46beta59 (Testing), and 7.0beta3 (Development). Each column contains a list of specific router models or components that support that version.

Di website tersebut, kita tinggal cari versi RouterOS yang terbaru dan sesuai dengan arsitektur router kita. Misal router yang saya punya, hAP lite yang berarsitektur SMIPS. Maka kita cari arsitektur SMIPS di web itu.

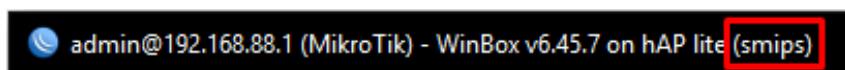
Ada 2 tipe download: Main Package dan Extra Package.

Main Package= Seluruh data fitur-fitur MikroTik yang dikumpulkan menjadi satu dalam format (.npk).

Extra Package= Data fitur-fitur MikroTik yang dipisah tiap fitur namun disatukan dalam format (.zip).

Bagaimana jika kita tidak tahu arsitektur router kita?

- Kita bisa mengetahuinya lewat Winbox
- Setelah kita login ke Winbox, dibagian tab paling atas, tertuliskan arsitektur router kita.



- Dari situ kita bisa tahu arsitektur router kita.

Dibawah ini daftar [Arsitektur MikroTik](#):

MIPSBE= CRS1xx, CRS2xx, DISC, LDF, LHG, NetBox, NetMetal, PowerBox, QRT, RB9xx, hAP, hAP ac, hAP ac lite, mANTBox, mAP, RB4xx, cAP, hEX Lite,wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7x

- SMIPS= hAP mini, hAP lite

- TILE = CCR series

- PPC = RB3xx, RB600, RB8xx, RB1100AHx2, RB1100AH, RB1100, RB1200
- ARM= LDF ac, LHG ac, SXTsq (ac series), Wireless Wire, cAP ac hAPac<sup>2</sup>, CRS3xx, RB3011, RB1100AHx4
- x86= PC / X86, RB230 series
- MIPSLE= RB1xx, RB5xx, Crossroads
- MMIPS= RBMxx, hEX , RB750Gr3

- **Upgrade Fitur MikroTik**

Upgrade MikroTik ini memiliki 3 cara:

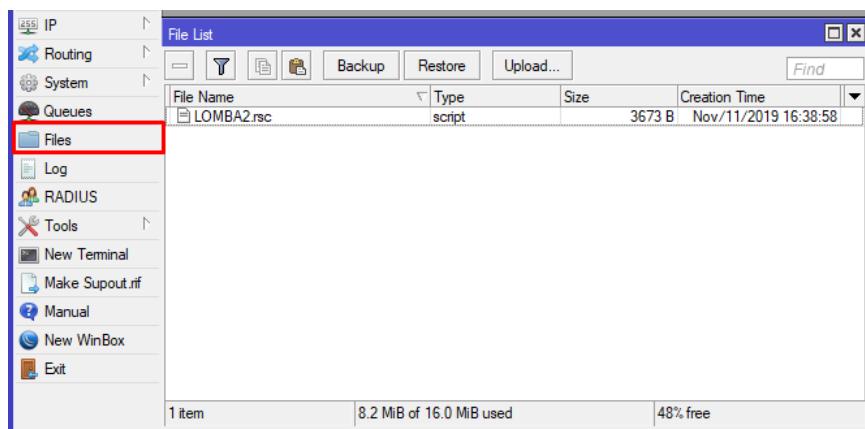
1. Drag & Drop.
2. Upload File.
3. Check for Update.

Kita langsung menuju Labnya, untuk utility yang digunakan, mulai Lab ini dan seterusnya kita akan menggunakan Winbox sebagai GUI dan Telnet sebagai CLI.

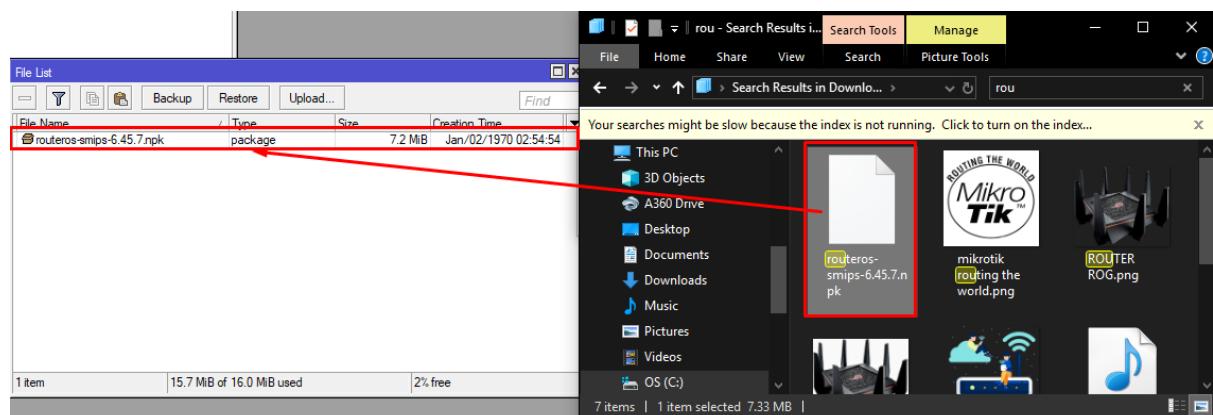
## Drag & Drop.

Drag & Drop merupakan cara termudah untuk meng-upgrade versi RouterOS MikroTik, karena langkah-langkahnya yang simpel.

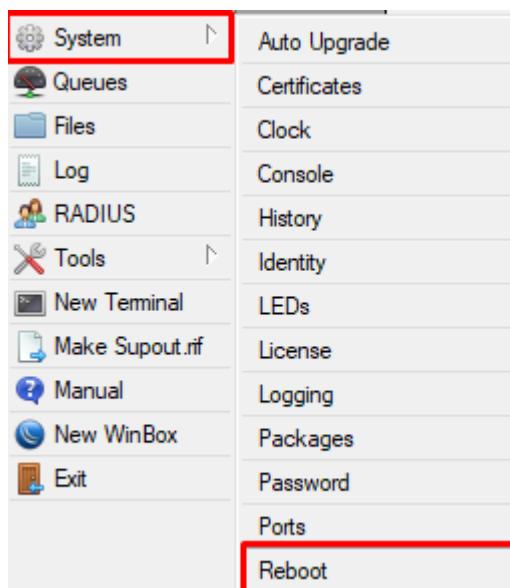
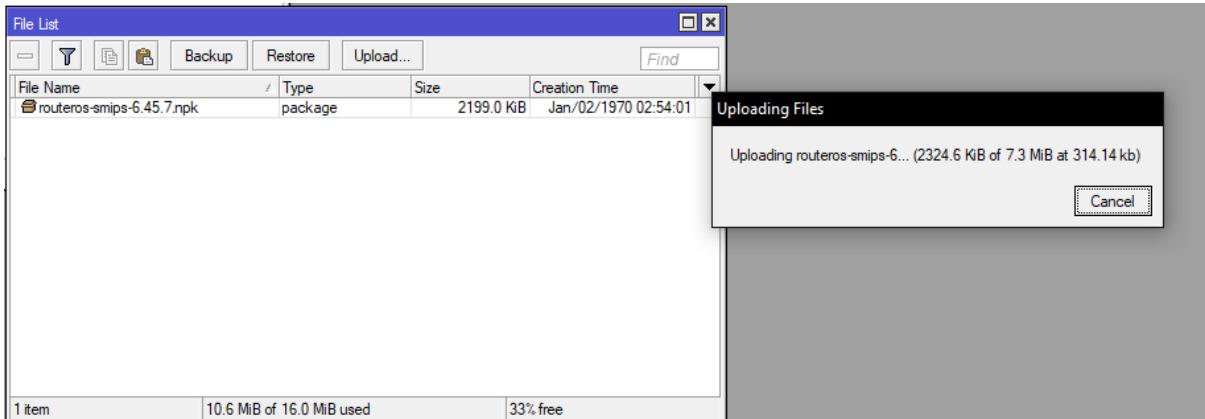
- Pertama-tama buka Winbox-nya, lalu klik fitur ‘files’.



- Lalu kita buka folder yang berisi RouterOS baru, yang kita unduh di web MikroTik.



- Kita ‘drag’ file RouterOS-nya ke File list di Winbox. Kemudian akan meng-upload.



- Jika sudah, kita tinggal Reboot untuk memulai upgrade RouterOS.
- Setelah reboot, bisa kita lihat hasilnya di 'system>resource'

Architecture Name:	smips
Board Name:	hAP lite
Version:	6.45.7 (stable)
Build Time:	Oct/24/2019 08:44:35
Factory Software:	6.42.1

- Kita berhasil upgrade RouterOS ke

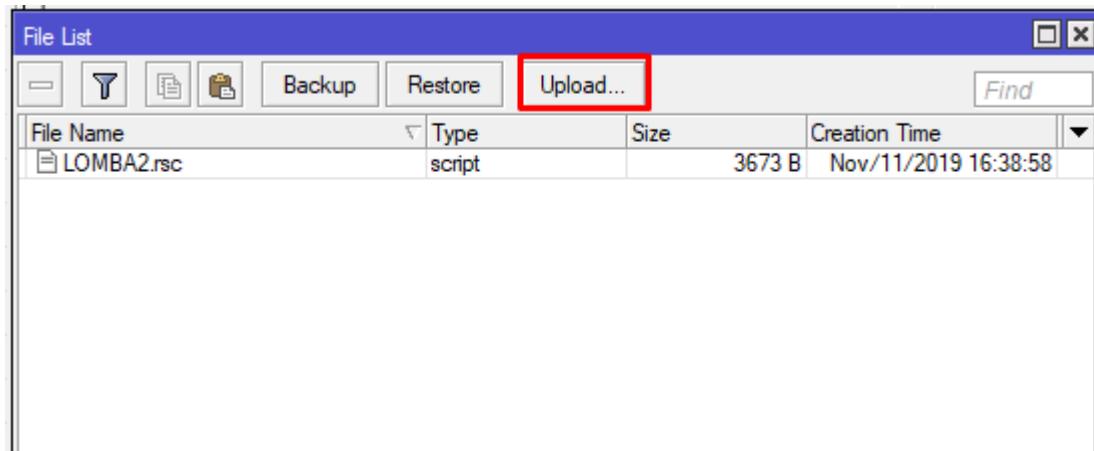
V6.45.7 (stable) dari yang sebelumnya V.6.45.6 (stable)

Untuk Drag & Drop, hanya bisa dilakukan di GUI.

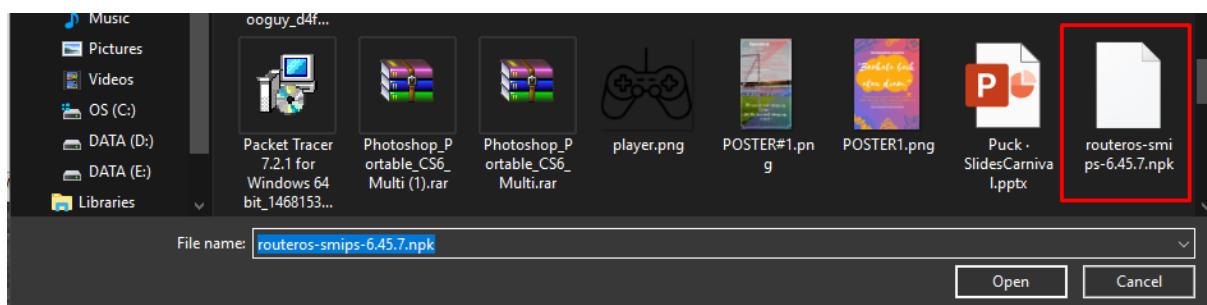
## Upload File.

Cara lain, selain Drag & Drop adalah Upload file.

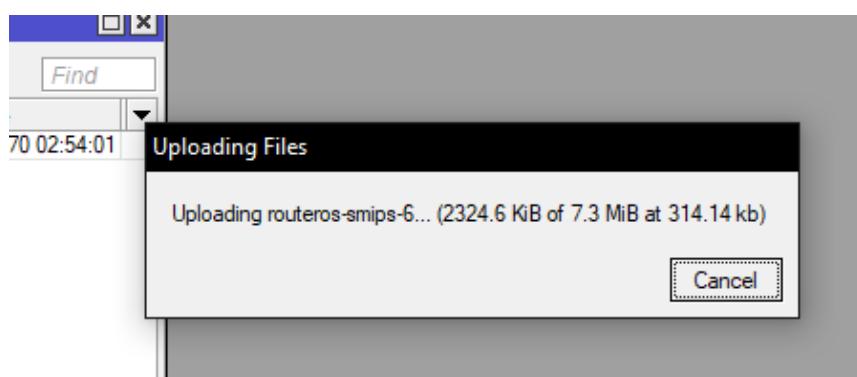
- Buka Winbox, buka fitur ‘files’.



- Di tab atas, klik ‘upload’ untuk mengupload file RouterOS-nya.



- Pilih file RouterOS-nya.



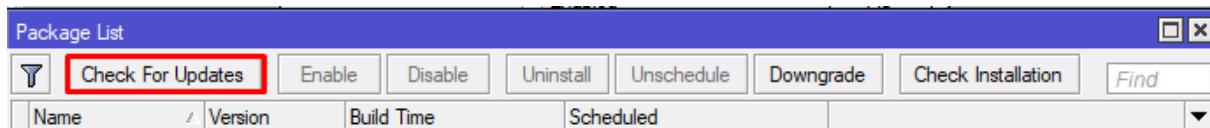
- Setelah upload selesai, reboot router untuk mulai upgrade.

Note : Cara ini hanya bisa digunakan di GUI.

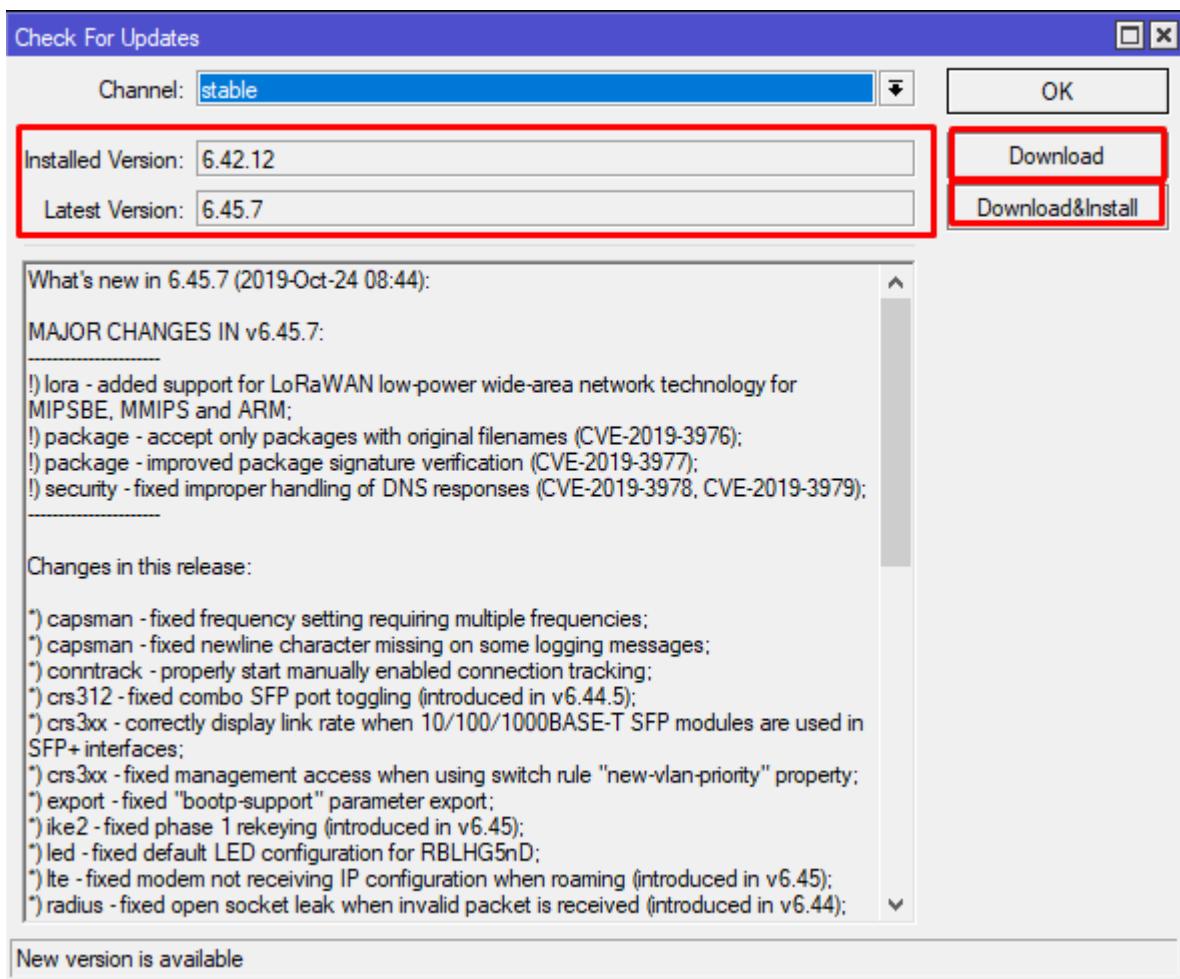
## Check for Updates.

Fitur ini ada didalam winbox, jadi winbox melakukan check update RouterOS yang ter-install.

- Untuk mengaksesnya, kita bisa menuju 'system>packages'



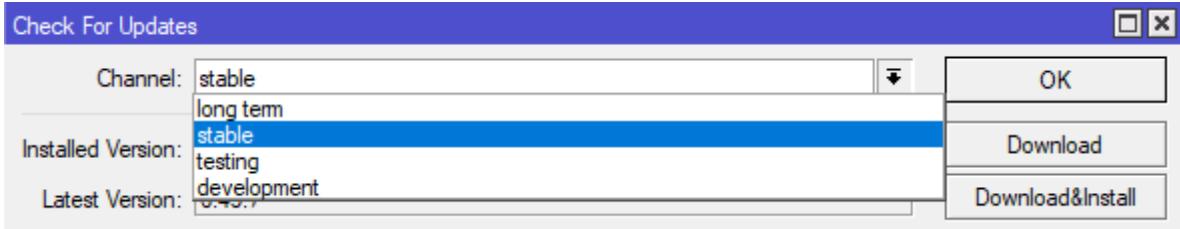
- Pada tab atas ada 'Check For Updates' kita klik.



- Beginilah tampilannya, disitu tertulis:

- Router OS yang terinstall adalah versi 6.42.12,
- Sementara versi terbaru yang stabil adalah V.6.45.7

- Kita juga bisa mengganti channel/tipe RouterOS yang mau kita download.



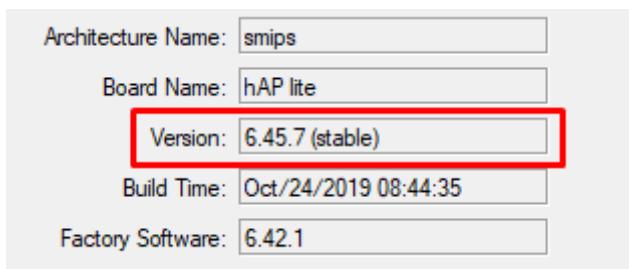
- Stable: Versi RouterOS ini sudah layak dan jarang terjadi bug.
- Long Term: Versi RouterOS yang sangat layak dan tidak ada bug.
- Testing: Versi RouterOS yang masih dalam tahap percobaan untuk menyempurnakan fitur-fiturnya
- Development: Versi RouterOS yang masih dalam tahap pengembangan/belum jadi.



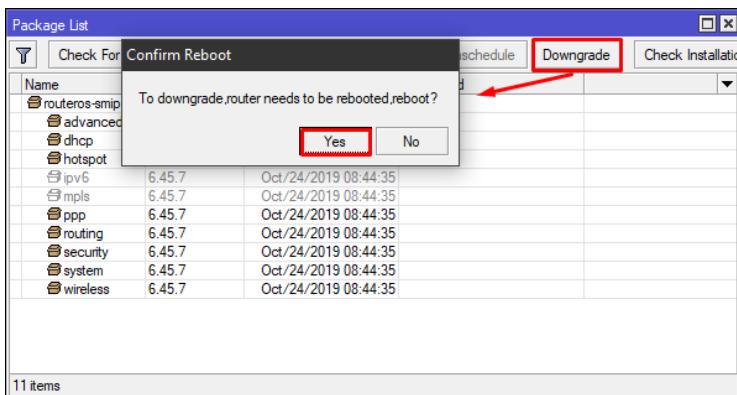
- Download: Hanya mengunduh file RouterOS nya dan menaruhnya di Files.
- Download & Install: Mengunduh file, sekaligus mengintallnya.

# DOWNGRADE FITUR MIKROTIK

Kadangkala MikroTik RouterOS yang kita install, banyak memiliki masalah; tidak kompatibel; banyak bug. Oleh karena itu, dibutuhkannya downgrade agar RouterOS-nya bisa kompatibel dan bekerja dengan baik.

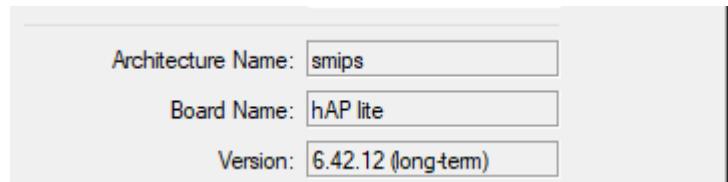


- Sebelumnya RouterOS saya versinya 6.45.7, lalu saya akan coba downgrade.
- Pertama-tama buka Winbox terlebih dahulu.
- Lalu menuju ke menu 'system>packages'



- Klik 'downgrade' pada tab atas, kemudian klik 'yes' untuk menjalankan proses downgrade.

- Jika kita sudah berhasil masuk lagi, maka versi RouterOS kita sudah diturunkan.
- Untuk mengeceknya klik 'system>resources'



- Versi RouterOS saya turun menjadi V.6.42.12

# USER MANAGEMENT

User Management adalah fitur MikroTik yang digunakan untuk membuat user/pengguna yang dapat mengakses router kita dan dapat mengonfigurasinya.

Untuk lebih detail, setiap user pada MikroTik ini memiliki grup yang pada grup ini ada hak-hak atau kebijakannya sendiri. Ada 3 grup yang memiliki kebijakan/hak berbeda:

## **1. Full**

Grup ini memiliki akses penuh pada MikroTik, yang dimana dia bisa mengedit, menambahkan, konfigurasi dan menambah/menghapus user.

## **2. Write**

Grup ini memiliki akses untuk mengonfig semua fitur/hampir sama dengan user Full, namun bedanya tidak dapat melakukan backup/export konfigurasi dan menambah/menghapus user lain.

## **3. Read**

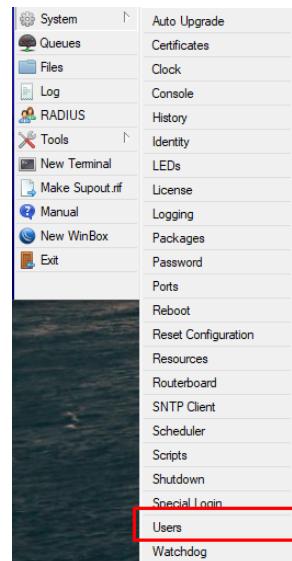
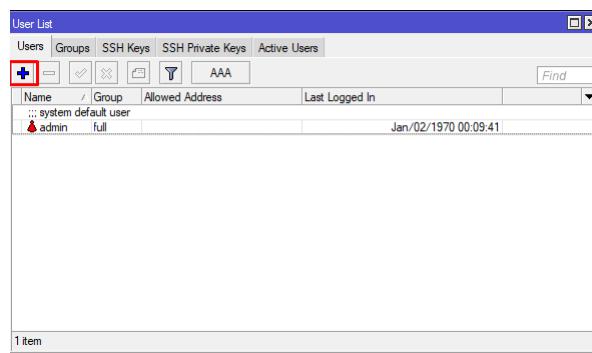
Grup ini hanya memiliki akses untuk melihat-lihat konfigurasi di Router tidak dapat menambah, menghapus, maupun mengedit konfigurasi, dan tidak dapat menambah/menghapus user.

Secara default, Router MikroTik, jika kita tidak membuat user, kita sudah memiliki user default/admin dan passwordnya=(kosong)

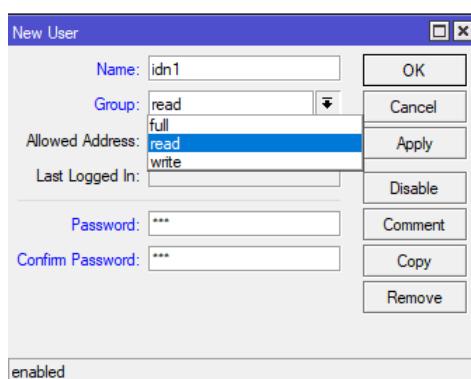
Cara membuat user management ini bisa dilakukan via GUI dan CLI.

### 1. Via GUI

- Masuk kedalam Winbox, buka ‘system>users’.

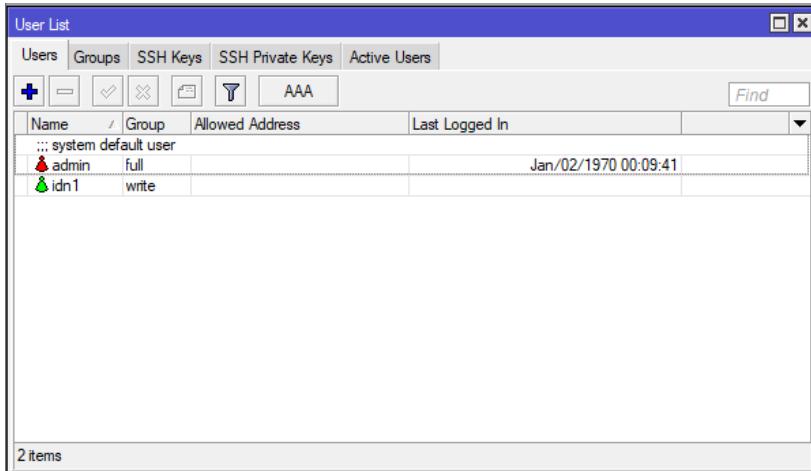


- Disitu sudah tertulis user admin sebagai user default.
- Jika kita ingin menambahkan, klik tombol ‘+’ di pojok kiri atas.



- Konfigurasi=
  - Name= (bebas) contoh= idn1
  - Group= Pilih, antara Full, Read, dan Write, contoh= Write
  - Password= (bebas) contoh= 123
- Jika sudah klik ‘apply’ dan ‘ok’

- Hasilnya sebagai berikut:

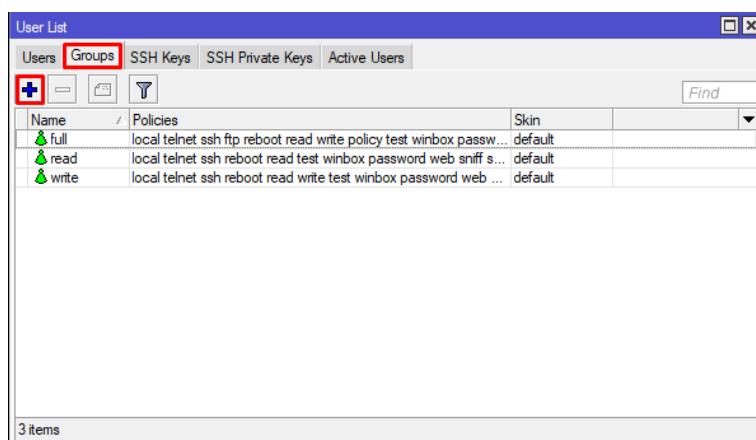


- Kita bisa login menggunakan user tersebut di Winbox.

Kita juga bisa mengubah-ubah hak/kebijakan user tersebut dengan membuat grup baru.

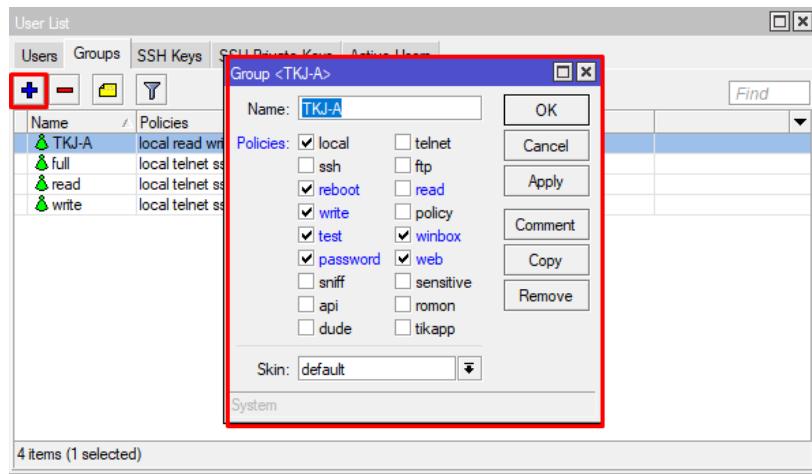
Caranya :

- Buka 'system>users'
- Didalam user list, klik 'group' pada tab atas.

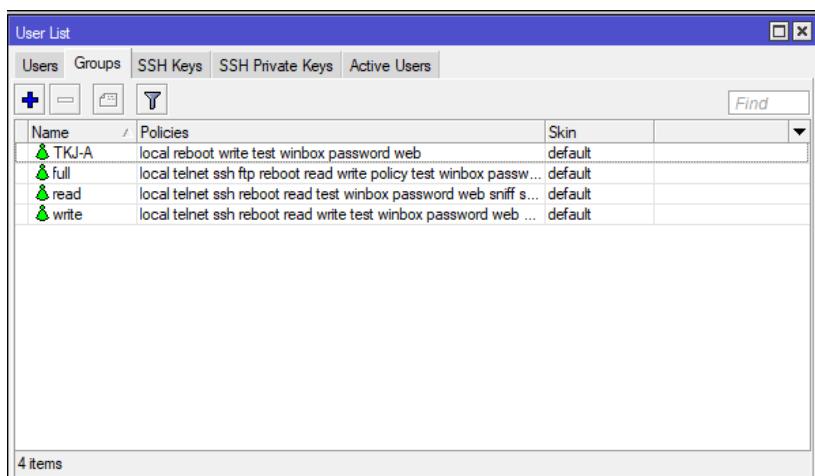


Disitu sudah tertulis grup default (full, read, write), kita akan membuat grup kita sendiri.

- Klik tombol ‘+’ di pojok kiri atas.



- Kita isi:
  - Nama : (bebas), contoh= TKJ-A
  - Policies : (kita isi sesuai keinginan kita)
- Lalu klik ‘apply’ dan ‘ok’



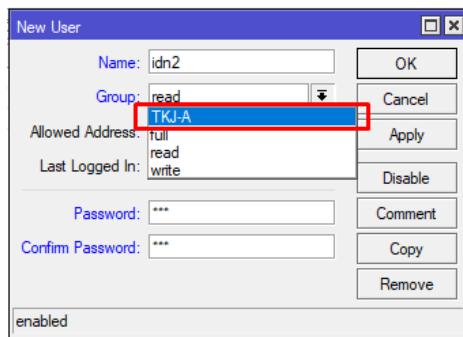
Sebelum lanjut, saya ingin memberitahu fungsi Policies yang ada:

1. **Local**= Kebijakan yang mengijinkan user login via local console (keyboard, monitor)
2. **Telnet**= Kebijakan yang mengijinkan user login secara remote via telnet
3. **SSH**= Kebijakan yang mengijinkan user login secara remote via secure shell protocol
4. **FTP**= Kebijakan yang mengijinkan hak penuh login via FTP, termasuk transfer file dari/menuju router. User dengan kebijakan ini memiliki hak read, write, dan menghapus files.
5. **Reboot**= Kebijakan yang mengijinkan user me-restart router.
6. **Read**= Kebijakan yang mengijinkan untuk melihat Konfigurasi router. Semua command console yang tidak bersifat konfigurasi bisa diakses.
7. **Write**= Kebijakan yang mengijinkan untuk melakukan konfigurasi router, kecuali user management. Policy ini tidak mengijinkan user untuk membaca konfigurasi router, user yang diberikan policy write ini juga disarankan juga diberikan policy read.
8. **Policy**= Kebijakan yang memberikan hak untuk management user.
9. **Test**= Kebijakan yang memberikan hak untuk menjalankan ping, traceroute, bandwidth-test, wireless scan, sniffer, snooper dan test commands lainnya. .
10. **Web**= Kebijakan yang memberikan hak untuk remote router via Webfig

11. **Winbox**= Kebijakan yang memberikan hak untuk remote router via Winbox
12. **Password**= Kebijakan yang memberikan hak untuk mengubah password
13. **Sensitive**= Kebijakan yang memberikan hak untuk melihat informasi sensitif router, misal secret radius, authentication-key, dll.
14. **API**= Kebijakan yang memberikan hak untuk remote router via API.
15. **Sniff**= Kebijakan yang memberikan hak untuk menggunakan tool packet sniffer.

Selanjutnya kita akan memasukkan user kedalam grup yang kita buat

- Setelah kita membuat grup baru, kita tinggal tambahkan user.
- Klik ‘users’ di tab atas, kemudian kita tambahkan user baru.



- Kita isi:
  - Name= (bebas) contoh: idn2
  - Group= (disini, kita isi grup yang tadi baru kita buat)
  - Klik ‘apply’ lalu ‘ok’.

User List				
Users		Groups	SSH Keys	SSH Private Keys
AAA <input type="text" value="Find"/>				
Name	/	Group	Allowed Address	Last Logged In
...; system default user				
admin		full		Jan/02/1970 00:04:10
idn1		write		
idn2		TKJ-A		

3 items

- Kita sudah membuat user baru dengan grup yang kita buat sendiri, kita bisa login menggunakan user tersebut.

# EXPORT, IMPORT, BACKUP, AND RESTORE

Pada Lab ini, kita akan membahas tentang Backup, Export, dan Import konfigurasi MikroTik yang telah kita buat.

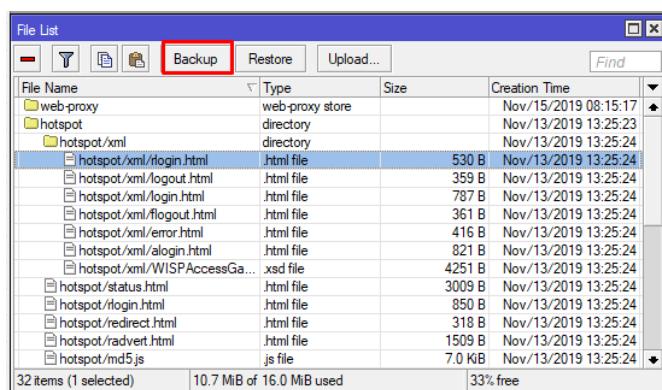
Apa itu Backup, Export, Import, dan Restore?

- Backup= Merupakan pencadangan/backup semua konfigurasi MikroTik yang telah kita konfigurasi. File backup ber-ekstensi (.backup)
- Export= Menyimpan seluruh konfigurasi MikroTik kita/mengekspor kedalam ekstensi (.rsc)
- Import= Meng-upload settingan export yang sudah pernah kita buat.
- Restore= Me-restore settingan backup yang sudah pernah kita buat.

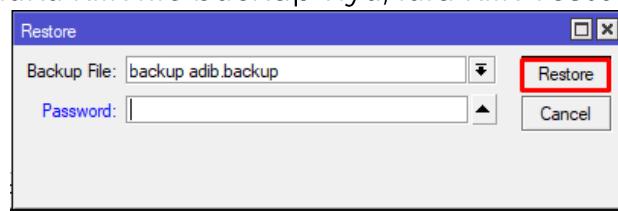
Kita simak bagaimana cara membuat **Backup** dan **Export**, lalu diimplementasikan kembali pada **Import** dan **Restore**.

## Backup & Restore.

- Pertama-tama kita menuju menu files di Winbox.
- Lalu klik ‘backup’ untuk mem-backup semua konfigurasi dalam ekstensi (.backup)
- Lalu akan ada opsi backup, kita isikan:
  - Name: (bebas), misal “backup adib”
  - Password: (bebas), jika tidak ingin menggunakan password, maka centang ‘Don’t Encrypt’
- Jika sudah, kita klik ‘backup’. Lalu hasilnya akan muncul di files.



- Lalu, jika kita ingin mengembalikan semua settingan backup yang kita buat, maka klik file backup-nya, lalu klik ‘restore’.



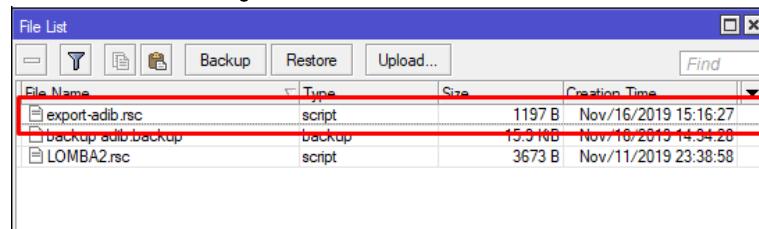
- Semua konfigurasi yang telah kita simpan akan di dimuat dan diimplementaskan.

## Export & Import.

- Untuk export, hanya bisa di akses lewat CLI, yang berarti kita harus mengetik commandnya di terminal: 'export file=(nama filenya)' contoh 'export file=export-adib'

```
[admin@MikroTik] > export file=export-adib
[admin@MikroTik] >
```

- Kita tunggu export-nya hingga selesai.
- Untuk melihat hasilnya bisa kita lihat di menu files.



- Sementara itu, jika kita ingin mengembalikan semua settingan export yang telah kita buat, kita harus menggunakan import, dan untuk menggunakan import, kita harus mengetikkan commandnya, karena import hanya ada di CLI. Ketikkan command:

'import (nama file)' contoh: 'import export-adib.rsc' (nama file yang kita

```
[Adib@Aulia] > import export-adib.rsc
Script file loaded and executed successfully
[Adib@Aulia] >
```

export tadi.

- Jika sudah selesai, maka settingan akan kembali.

**NOTE:**

- File Export dan Backup, bisa dibuka menggunakan notepad, namun perbedaan antara Export (.rsc) atau Backup (.backup) yaitu:
    - File export, ketika dibuka di Notepad, susunan teks nya beraturan dan kita bisa mengeditnya.

```
# export-adib.rsc - Notepad
File Edit Format View Help
# nov/16/2019 13:54:46 by RouterOS 6.45.7
# software id = ICX8-ZYPX
#
# model = R8941-2nD
# serial number = 9D740A0EC34B
#interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
add authentication-types=wpa-psk,wpa2-psk,wpa,wpa2-eap group-ciphers=\
    tkip,aes-ccm management-protection=allowed mode=dynamic-keys name=as \
    supplicant-identity="" unicast-ciphers=tkip,aes-ccm wpa-pre-shared-key=\
        Mamamialezatos wpa2-pre-shared-key=Mamamialezatos
#interface wireless
set [ find default-name=wlan1 ] band=2ghz/b/g disabled=no frequency=2437 \
    security-profile=as ssid="SAMSUNG NOTE 10"
#ip address
add address=12.12.12.1/24 interface=ether2 network=12.12.12.0
#ip dhcp-client
add dhcp-options=hostname,clientid disabled=no interface=wlan1
#ip firewall address-list
add address=www.youtube.com list=ytup
#ip firewall filter
add action=add-src-to-address-list address-list=NAKAL address-list-timeout=\
    none-dynamic chain=forward protocol=icmp
add action=drop chain=forward dst-address-list=ytup
#ip firewall nat
add action=masquerade chain=srccnat out-interface=wlan1
#system clock
set time-zone-name=Asia/Jakarta
```

- File backup, ketika dibuka di Notepad, susunan teks nya tidak beraturan dan tidak bisa diedit.

- Proses Export **lebih lama**, dibandingkan Backup.
  - Proses Import, **tidak perlu** melakukan reboot, sementara Restore wajib.
  - Proses Export/Import hanya bisa diakses di CLI, sementara Backup/Restore bisa diakses di GUI.

# ROUTER IDENTITY

Di Lab kali ini, kita akan menamai router kita atau router identity.

Mengapa router identity itu penting?

- Agar router kita tidak tertukar dan mempermudah manajemen jaringan.

Pada dasarnya, default nama router yaitu MikroTik, jika semua router bernama MikroTik, bagaimana jika ada masalah disalah satu router namun kita tidak tahu router yang mana yang bermasalah. Itulah kenapa router identity itu penting.

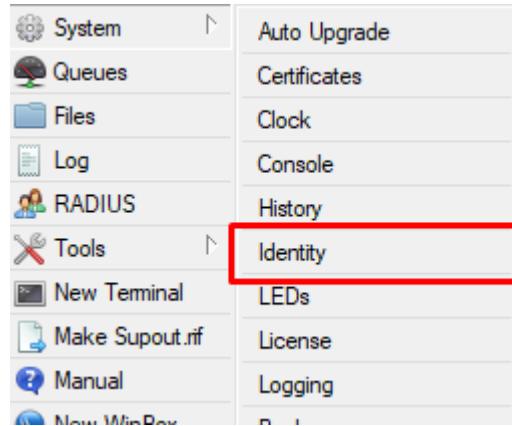
Dan juga ketika kita dalam perusahaan, kita mau membagi router sesuai dengan wilayah jangkauannya, jika semua router beridentitas sama, kita akan kewalahan untuk memanajemen router itu karena identitasnya sama. Maka dibutuhkanlah router identity untuk menamai router tersebut agar ktaia lebih mudah untuk mengaturnya.

Langsung saja kita menuju Labnya

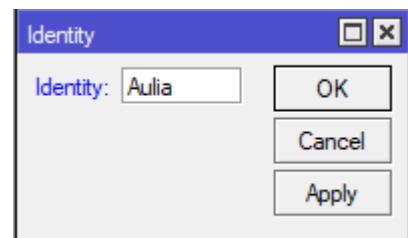
Untuk menamai router, caranya sangat mudah, bisa diakses dengan CLI maupun GUI.

## 1. Via GUI.

- Caranya cukup klik menu ‘system’ pada winbox, kemudian klik ‘identity’.



- Kita isikan nama yang kita inginkan.
- Misal saya ‘Aulia’
- Kemudian klik ‘apply’ lalu ‘ok’
- Secara otomatis nama router kita akan berganti.



admin@74:4D:28:81:83:34 (Aulia) -

## 2. Via CLI.

```
[Adib@MikroTik] > system identity set name=Aulia  
[Adib@Aulia] >
```

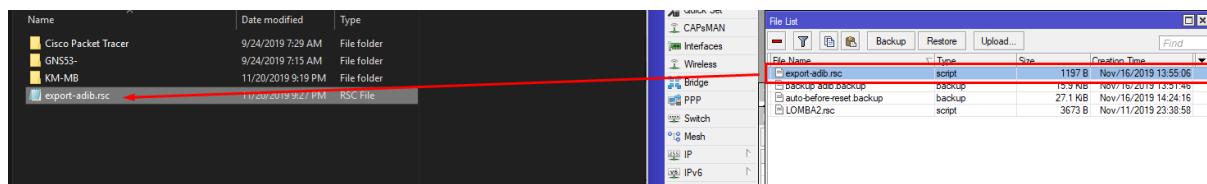
- Caranya cukup ketik command ‘system identity set name=(nama router)’ contoh ‘system identity set name=Aulia’
- Secara otomatis nama router akan berganti.

# MENYIMPAN DAN MENGUPLOAD HASIL BACKUP/EXPORT

Selain itu, kita juga bisa memindahkan file hasil backup atau export kita ke PC kita. Caranya ada 2, bisa dengan **Drag & Drop** atau **Upload**.

## Drag & Drop.

- Untuk step-nya mudah saja, kita tinggal pilih filenya (backup/export) di menu Files, kemudian kita **drag** ke folder yang dituju, lalu kita **drop**.



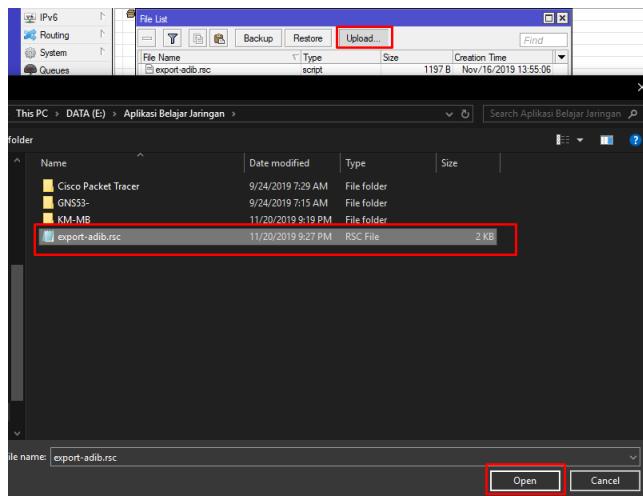
- Maka file tersebut akan secara otomatis tersalin.

Atau sebaliknya, kita juga bisa menyalin hasil export/upload yang berada di folder ke dalam MikroTik.

- Untuk step-nya sama seperti sebelumnya, hanya saja terbalik.
- Kita **drag** file (export/backup) yang berada difolder, lalu kita **drop** kedalam files list di menu files winbox.

## Upload.

- Untuk step-nya, sangat mudah juga.
- Kita tinggal menuju file list di menu files, lalu klik ‘upload’ di bar atas.



- Maka file yang kita upload tadi, akan muncul di file list.

Note: Untuk cara **Drag & Drop dan Upload**, hanya bisa digunakan di Winbox.

# SOFT DAN HARD RESET

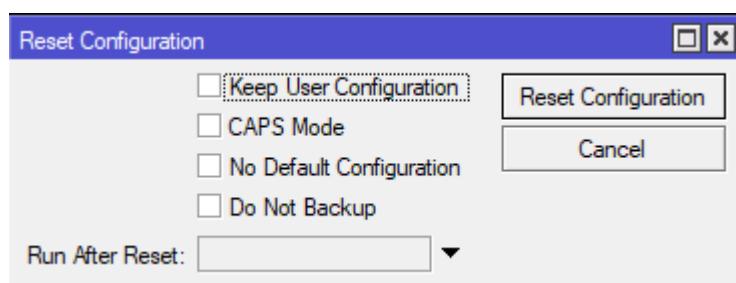
Ada waktunya, dimana kita membutuhkan sesuatu yang bernama 'reset' atau mengembalikan. Nah, ada kalanya kita membutuhkan reset pada router kita, misalnya kita ingin menghapus semua konfigurasi dan ingin membuat konfigurasi baru tanpa harus menghapus satu-satu, kita bisa gunakan **soft reset**. Atau ketika kita tidak dapat mengakses router karena lupa user/password router, kita dapat gunakan **hard reset** untuk mengembalikan semua konfigurasi dari awal (default configuration).

Langsung saja kita bahas satu-satu.

## Soft Reset

Kita mereset semua konfigurasi yang ada di router melalui aplikasi, baik GUI maupun CLI.

- Jika menggunakan Winbox (GUI), kita tinggal menuju menu 'system>reset configuration'



- Disitu ada beberapa fitur tambahan:

### **1. Keep User Configuration**

Jika kita centang menu ini maka ketika router melakukan reset configuration tidak akan menghapus konfigurasi yang telah di setting oleh user.

### **2. Caps Mode**

Menu ini digunakan ketika kita menggunakan Capsman untuk manajemen wireless kita.

### **3. No Default Configuration**

Jika kita pilih menu ini maka mikrotik akan reset total tanpa ada konfigurasi IP default mikrotik.

### **4. Do Not Backup**

Jika kita pilih Do Not Backup, maka mikrotik hanya akan melakukan reset tanpa melakukan backup sebelum proses reset di lakukan.

- Jika kita sudah memilih fitur yang kita perlukan, klik 'Reset Configuration' untuk memulai reset router kita.

- Jika menggunakan Telnet (CLI) kita cukup ketikkan command '**system reset configuration**', jika kita ingin menambahkan fitur, maka kita tambahkan command lagi, contoh :  
**'system reset-configuration no-defaults=yes'**

```
[Adib@Aulia] > system reset-configuration  
caps-mode keep-users no-defaults run-after-reset skip-backup  
[Adib@Aulia] > system reset-configuration
```

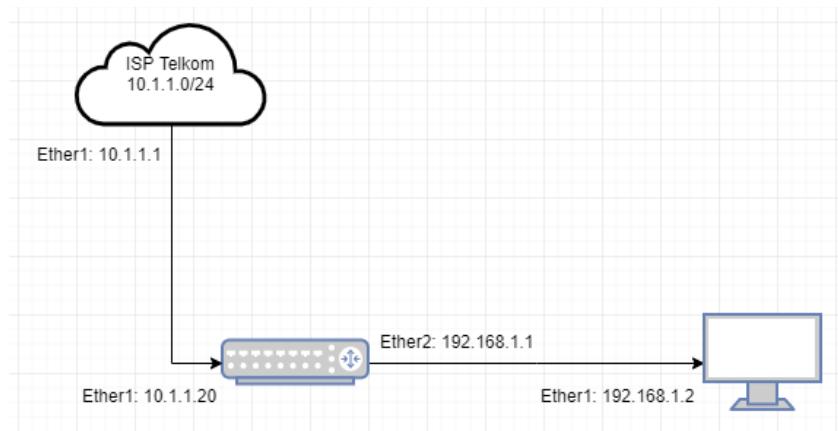
- Jika kita tidak tahu command apa yang ingin kita tambah, cukup tekan keyboard 'tab'. Lalu enter jika sudah tekan enter.

## Hard Reset

Mereset semua konfigurasi yang ada di router langsung dari router, tanpa menggunakan aplikasi seperti winbox/telnet. Dan disini kita akan mereset router hAP-lite.

1. Siapkan router yang mau kita reset, pastikan tidak menyala (kabel power tidak tercolok).
2. Lalu tekan dan tahan tombol reset sambil menyolokkan kabel power.
3. Tetap tekan tombol reset, dan tunggu lampu LED berkedip 10 kali.
4. Jika sudah coba akses kedalam router, jika berhasil, di Winbox, default IP addressnya menjadi 0.0.0.0.

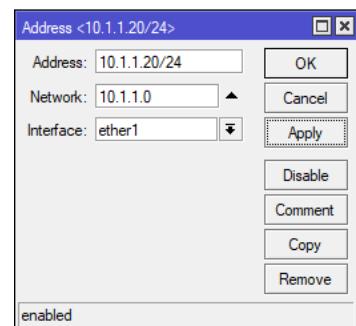
# INTERNET VIA LAN



Berdasarkan topologi diatas, kita akan mencoba untuk menghubungkan router kita dengan internet melalui LAN, (Local Area Network). Caranya dengan mengonfigurasi router yang terhubung ke internet dan PC klien.

Kita langsung terapkan.

- Buka Winbox terlebih dahulu. Lalu kita tambahkan IP address di ether1: 10.1.1.20/24 agar kita bisa terhubung dengan ISP Telkom.
- Kemudian kita pastikan bahwa kita sudah terhubung dengan ISP. Ping 10.1.1.1 di router.

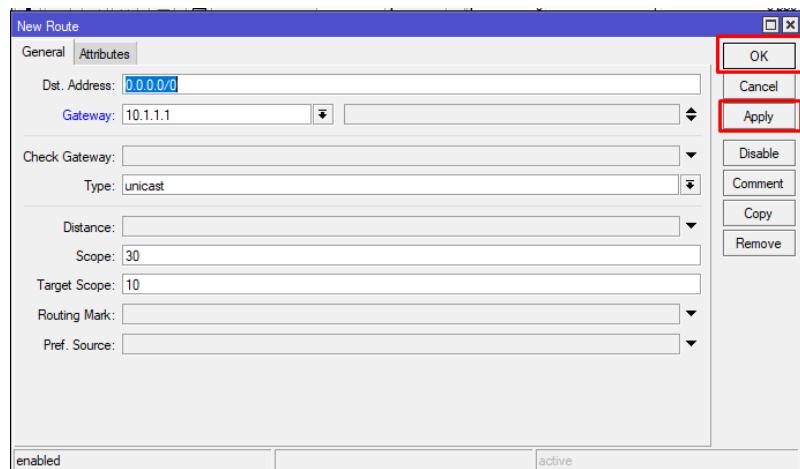


A terminal window showing the output of a ping command. The host is 10.1.1.1 and the sequence numbers range from 0 to 5. The ping results show a size of 56 bytes, a TTL of 128, and a time of 0ms for each packet.

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	10.1.1.1	56	128	0ms	
1	10.1.1.1	56	128	0ms	
2	10.1.1.1	56	128	0ms	
3	10.1.1.1	56	128	0ms	
4	10.1.1.1	56	128	0ms	
5	10.1.1.1	56	128	0ms	

- Jika sudah ada reply, maka router sudah terhubung, namun kita harus menambahkan routing ke IP 0.0.0.0/0 (default route) atau IP yang mewakili seluruh IP yang ada didunia agar kita bisa mengakses internet.

- Klik 'IP>Routes'. Masukkan=
  - Dst. Address: 0.0.0.0/0
  - Gateway: 10.1.1.1 (IP ISP)
- Klik 'apply' lalu 'ok'.

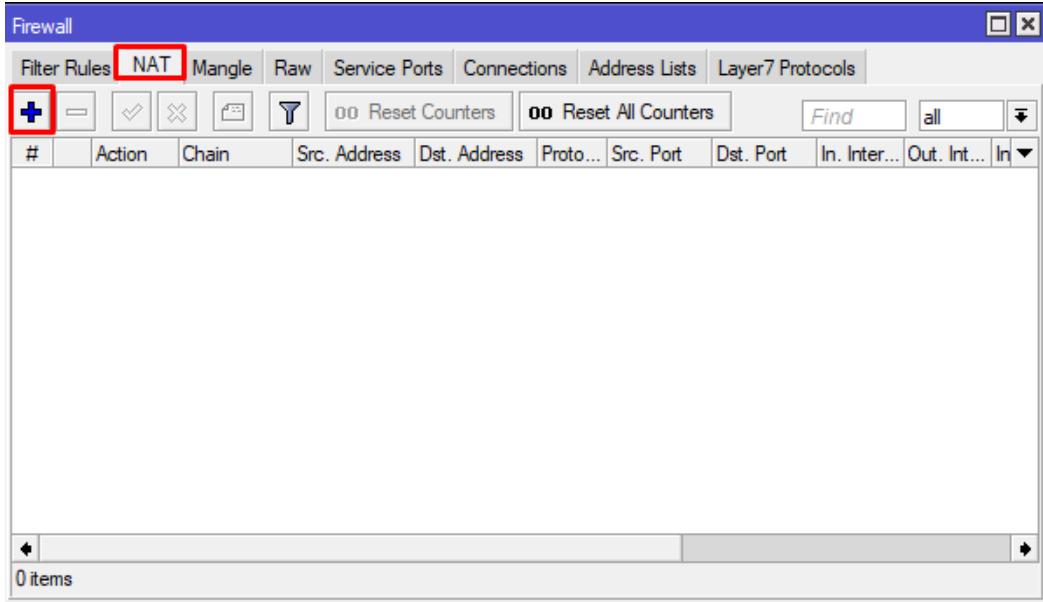


- Dengan begini, router kita dapat terhubung ke internet. Kita dapat mengeceknya dengan ping ke 8.8.8.8.

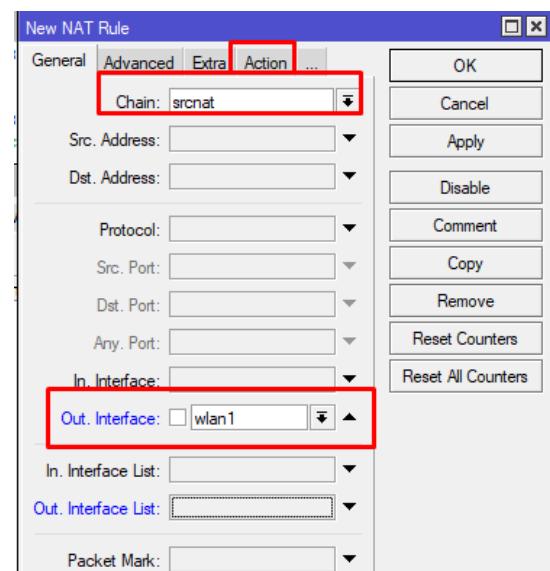
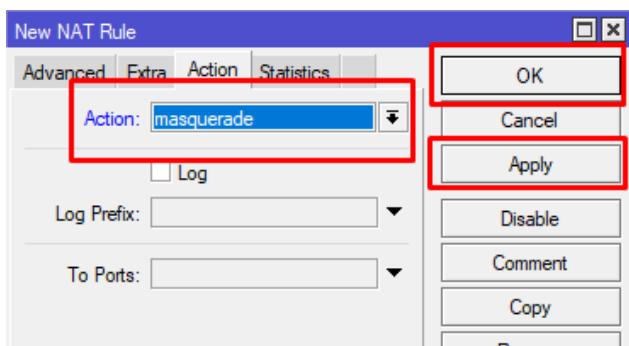
```
[Adib@Aulia] > ping 8.8.8.8
SEQ HOST SIZE TTL TIME STATUS
 0 8.8.8.8 56 45 26ms
 1 8.8.8.8 56 45 25ms
 2 8.8.8.8 56 45 26ms
 3 8.8.8.8 56 45 25ms
 4 8.8.8.8 56 45 24ms
```

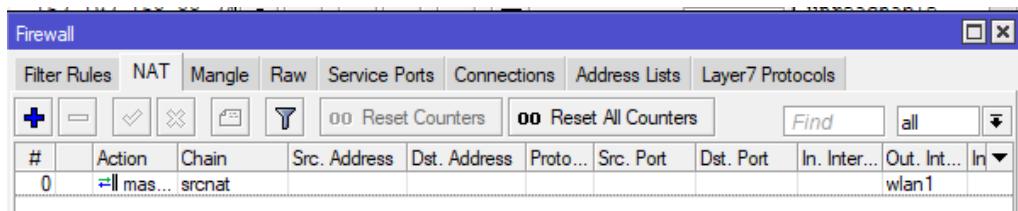
- Router kita sudah memiliki akses internet, hanya saja PC kita belum, maka kita harus membuat IP menuju PC dan konfigurasi NAT (Network Address Translator) untuk menerjemahkan IP Public ke IP Private.

- Pertama-tama kita menuju menu 'IP>Firewall>NAT' lalu kita add '+'



- Di tab tersebut kita isikan:
  - Chain: srcnat
  - Out. Interface: wlan 1
- Lalu pada tab Action, kita isikan:
  - Action: masquerade
  - Jika sudah 'apply' lalu 'ok'.





- Jika konfigurasi NAT sudah, maka sambungan koneksi antara PC dan router bisa mengakses internet.

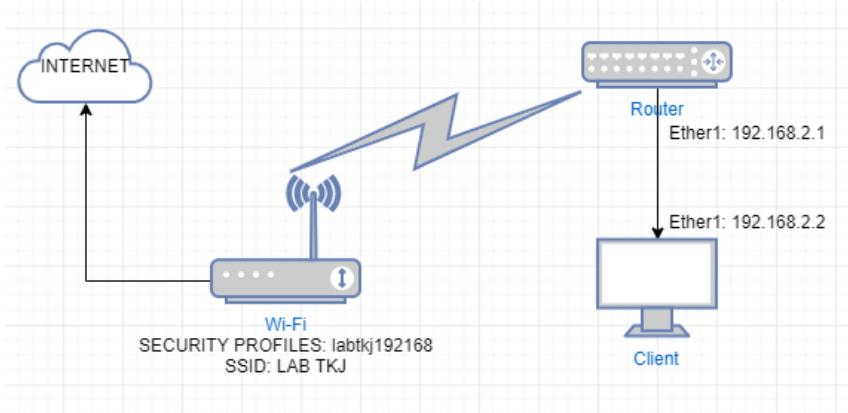
```
C:\Users\ASUS>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=164ms TTL=47
Reply from 8.8.8.8: bytes=32 time=129ms TTL=47
Reply from 8.8.8.8: bytes=32 time=380ms TTL=47
Reply from 8.8.8.8: bytes=32 time=98ms TTL=47
```

- Untuk mengecek apakah PC sudah terhubung atau belum, kita bisa melakukan ping ke 8.8.8.8.

- Jika sudah ada reply, maka PC bisa mengakses internet.

# INTERNET VIA WLAN

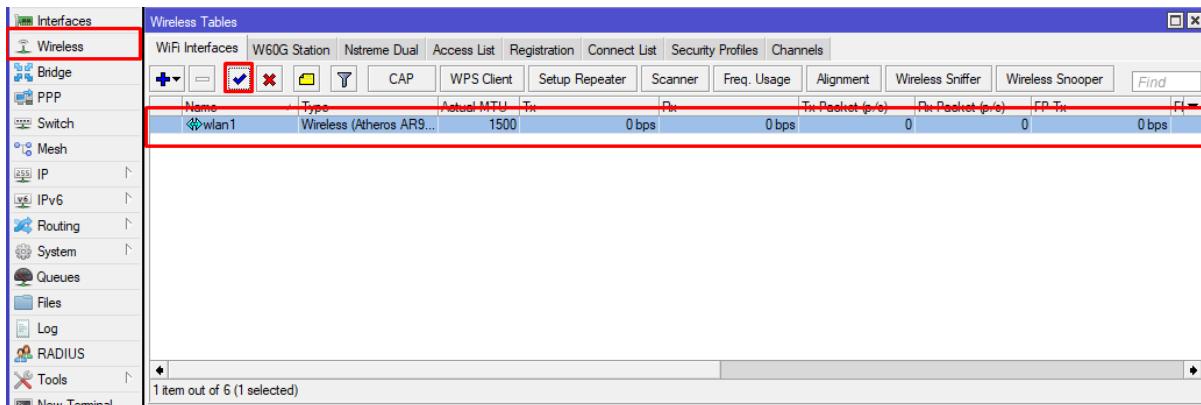


Pada lab sebelumnya, kita berhasil menghubungkan internet ke PC lewat LAN, nah pada lab kali ini, kita akan mencoba menghubungkan internet ke PC namun lewat WLAN atau biasa disebut dengan WiFi atau Access Point.

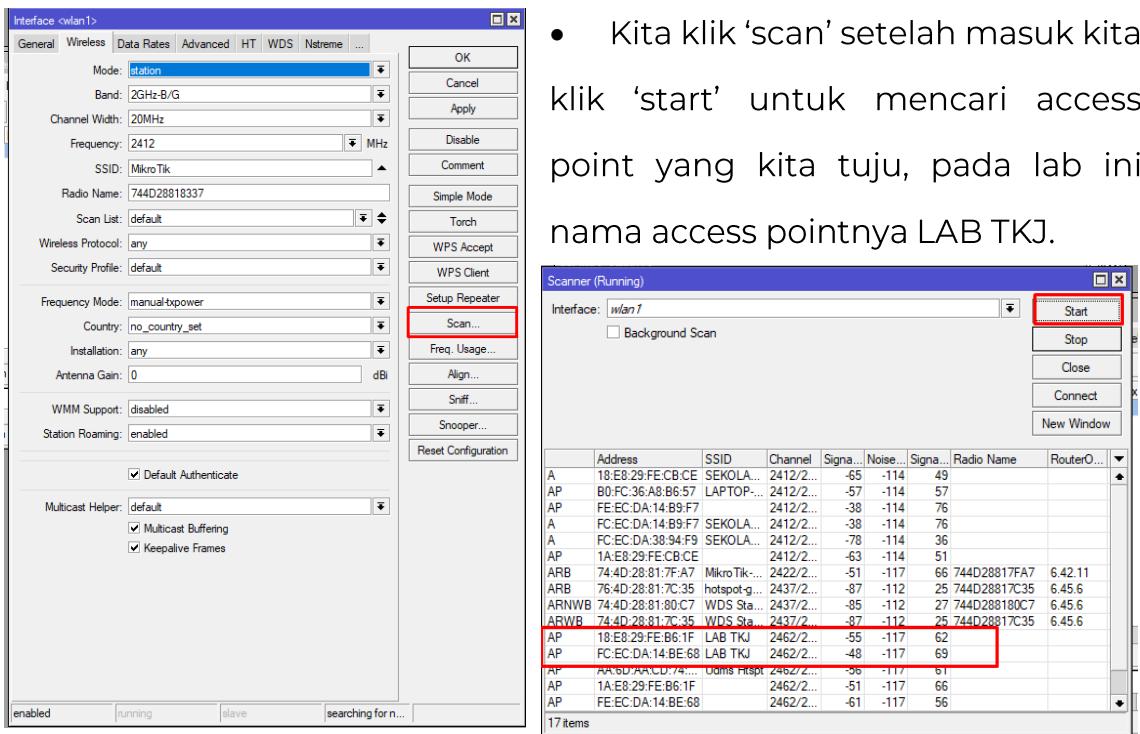
Seperti di topologi diatas, kita akan mencoba menghubungkan Client lewat router yang mengakses internet dari Access Point LAB TKJ.

Kita langsung coba.

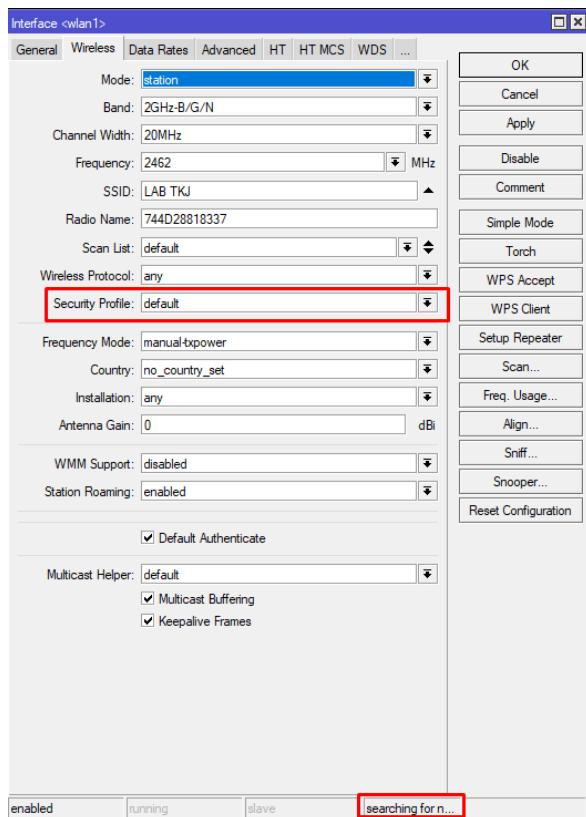
- Buka winbox, kita menuju menu wireless.



- Disitu akan ada interface wlan1 jika kalian menggunakan router hAP-lite. Jika interface nya ter-disable, kita harus meng-enable nya dengan cara: klik wlan1, kemudian klik tanda centang di tab atas.



- Jika ada 2 seperti diatas, kita pilih AP (Access Point) dengan signal terkecil. Di gambar ada 2 AP LAB TKJ, ada signal -55 dan -48. Kita pilih yang -48 karena lebih kecil dan lebih cepat dari -55.
- Jika sudah kita klik 'connect'

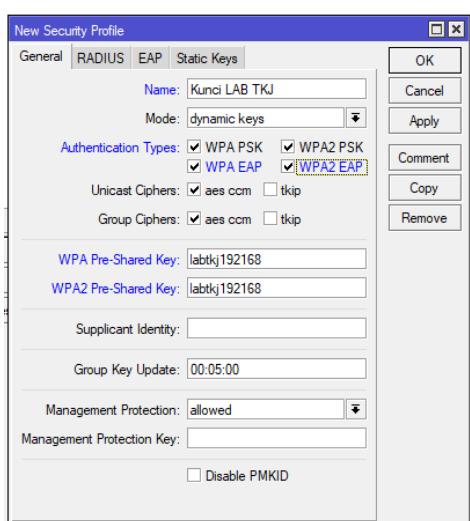
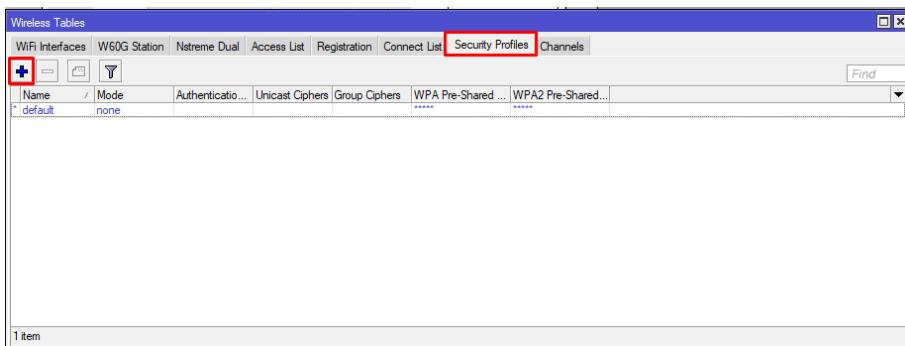


- Kita klik 'scan' setelah masuk kita klik 'start' untuk mencari access point yang kita tuju, pada lab ini nama access pointnya LAB TKJ.

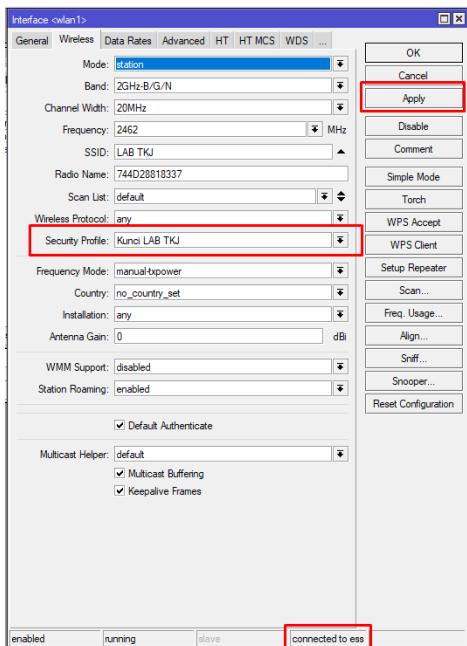
Scanner (Running)							
Interface: wlan1							
Start							
<input type="checkbox"/> Background Scan							
Freq. Usage...							
Align...							
Sniff...							
Snooper...							
Reset Configuration							
17 items							

- Kita lihat dibagian bawah, "Searching for network" yang artinya masih ada konfigurasi yang kurang. Jika kita lihat di topologi, access point LAB TKJ memiliki password: labtkj192168. Nah untuk memasukkan password tersebut, kita harus buat security profiles agar bisa terhubung.

- Kita kembali pada wireless table, disitu kita menuju security profiles, kemudian klik add ‘+’



- Pada new security profiles, kita isikan:
  - Name: (bebas) contoh: Kunci LAB TKJ
  - Authentication Types: (bebas) tergantung enkripsi apa yang ingin kita pakai.
    - WPA Pre-shared Key: (password yang akan kita gunakan) labtkj192168
    - WPA2 Pre-shared Key: (password yang akan kita gunakan) labtkj192168
  - Jika sudah klik 'apply' kemudian 'ok'



- Lalu kita setting lagi pada interface wlan1.
- Disitu kita masukkan security profiles yang kita buat tadi.
- Lalu kita apply, dan akhirnya bisa terkoneksi “connected to ess”.
- Namun belum selesai disitu, kita harus menambahkan beberapa konfigurasi lagi.

**DHCP Client**

DHCP Client Options					
Interface	/	Use P...	Add D...	IP Address	Expires After
wlan1	/	yes	yes	100.100.100.40/24	00:09:47

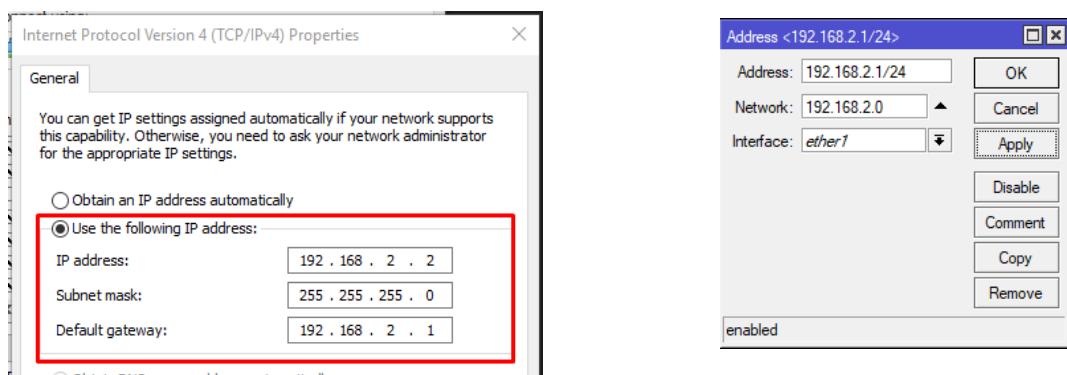
**New DHCP Client**

DHCP Client Options					
Interface:	OK				
wlan1	OK				
<input checked="" type="checkbox"/> Use Peer DNS	Cancel				
<input checked="" type="checkbox"/> Use Peer NTP	Apply				
Add Default Route: yes	Disable				
	Comment				
	Copy				
	Remove				
	Release				
	Renew				

- Kita harus menambahkan IP DHCP Client agar kita bisa mendapatkan IP dari WiFi.
- Kita menuju menu IP>DHCP Client.
- Kita add ‘+’ disitu kita cukup isikan Interface:wlan1 lalu ‘apply’ kemudian ‘ok’.
- Lalu kita tunggu proses requesting ke access point, tunggu hingga bound.
- Jika sudah bound kita mendapatkan IP dari Access point agar antara router dan access point bisa saling terhubung.

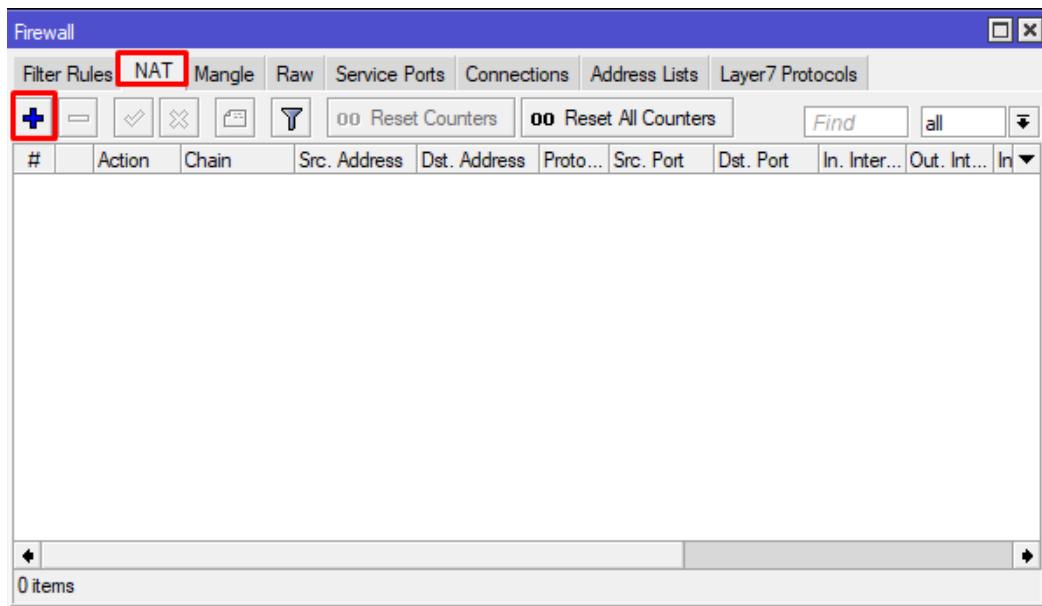
Tidak lupa, kita harus membuat router dan client tetap terhubung dengan membuat IP address antara router dan client.

- Kita buat IP address 192.168.2.1/24 pada ether1 di router.
- Dan kita membuat IP address 192.168.2.2/24 pada client

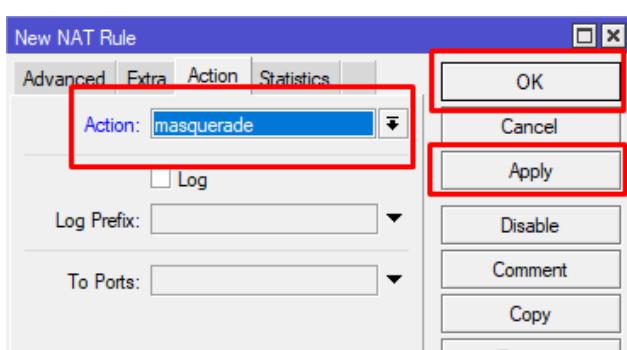
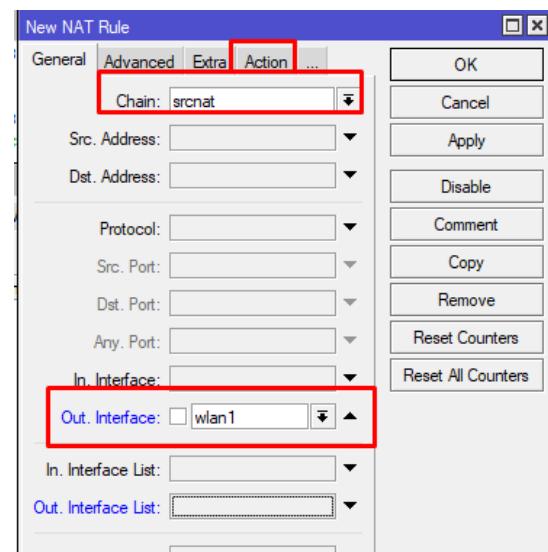


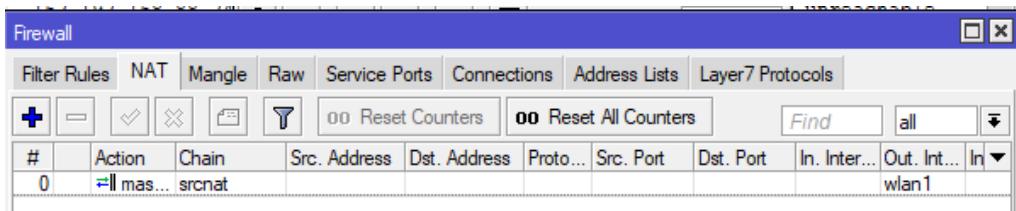
Kemudian kita konfigurasi NAT (Network Address Translation) konfigurasinya sama seperti di lab sebelumnya. Menu IP>Firewall>NAT>add (+).

- Pertama-tama kita menuju menu ‘IP>Firewall>NAT’ lalu kita add ‘+’



- Di tab tersebut kita isikan:
  - Chain: srcnat
  - Out. Interface: wlan 1
- Lalu pada tab Action, kita isikan:
  - Action: masquerade
- Jika sudah ‘apply’ lalu ‘ok’.





- Jika konfigurasi NAT sudah, maka sambungan koneksi antara PC dan router bisa mengakses internet.

```
C:\Users\ASUS>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=164ms TTL=47
Reply from 8.8.8.8: bytes=32 time=129ms TTL=47
Reply from 8.8.8.8: bytes=32 time=380ms TTL=47
Reply from 8.8.8.8: bytes=32 time=98ms TTL=47
```

- Untuk mengecek apakah PC sudah terhubung atau belum, kita bisa melakukan ping ke 8.8.8.8.

- Jika sudah ada reply, maka PC bisa mengakses internet.

# NETWORK TIME PROTOCOL (NTP)

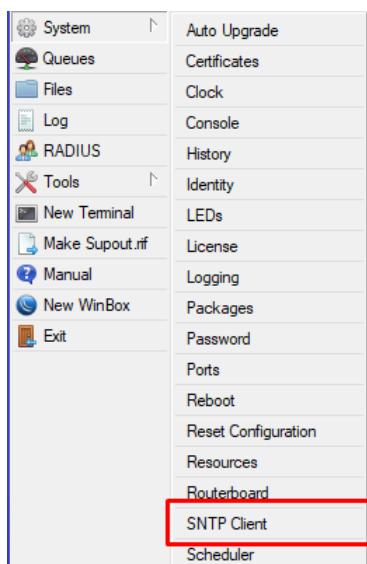
Jika kalian mengamati, setting waktu pada router MikroTik secara defaultnya adalah jam 00:00:00, 02 Januari tahun 1970. Setting waktu pada MikroTik ini sangatlah penting untuk keamanan dan konfigurasi yang bersangkutan. Karena jika tidak, akan terjadi kesalahan maupun kegagalan pada konfigurasi yang menggunakan waktu/NTP.

Apa itu NTP?

NTP merupakan singkatan dari Network Time Protocol. Yang fungsinya memungkinkan router kita melakukan sinkronisasi terhadap waktu dengan jaringan, router kita dapat digunakan menjadi NTP Server maupun NTP Client. Dengan begitu waktu yang tadinya default (tahun 1970) jadi tahun waktu buku ini dibuat (2019).

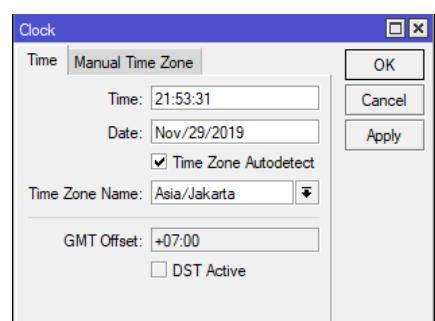
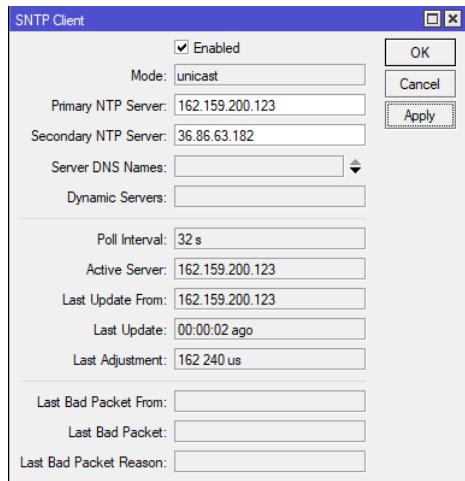
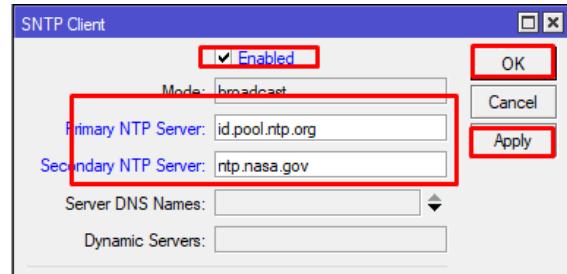
Jika ingin melihat daftar NTP, bisa kita cari di [www.pool.ntp.org](http://www.pool.ntp.org)

Langsung kita terapkan di router kita, sebelumnya pastikan router terhubung ke internet.



- Pertama-tama buka Winbox, klik 'system>SNTP client'

- Kita centang Enabled, kemudian kita isi:
  - Primary NTP Server: id.pool.ntp.org
  - Secondary NTP Server: ntp.nasa.gov
- Kemudian ‘apply’ lalu ‘ok’
- Secara otomatis, modenya akan berganti menjadi unicast dan nama NTP servernya akan menjadi IP Address.
- Untuk mengecek waktunya sudah benar ataukah belum, kita bisa mengeceknya di ‘system>clock’
- Jika benar, maka jam, tanggal, dan zona waktu nya akan sesuai dengan keadaan kita sekarang ini.



## Catatan:

**BAB KEDUA**

**FIREWALL**

**HOW TO BASIC-MTCNA**

# PENGENALAN FIREWALL

## Overview

Untuk melindungi router dari luar, baik dari berasal dari WAN (internet) maupun dari client (local). Untuk melindungi netwok dari netwok lain yang melewati router. Dalam MikroTik firewall, ada banyak fitur yang semuanya dimasukkan dalam menu ‘IP>Firewall’. Firewall basic di MikroTik ada di ‘IP>Firewall>Filter Rule.’

## Firewall Filter Rule

Setiap Firewall Filter rule diorganisir dalam chain (rantai) yang berurutan. Setiap aturan chain yang dibuat akan dibaca oleh router dari atas ke bawah. Di Firewall Filter Rule ada 3 default chain (input,forward, output). Kita juga boleh membuat nama chain sesuai dengan keinginan kita. Paket dicocokkan dengan kriteria/persyaratan dalam suatu chain, apabila cocok paket akan melalui kriteria/persyaratan chain berikutnya/ di bawahnya.

## Firewall NAT

Network Address Translation (NAT) adalah proses penulisan ulang (masquerade) pada alamat IP asal (source) dan/atau alamat IP tujuan (destination), setelah melalui router atau firewall. NAT digunakan pada jaringan dengan workstation yang menggunakan IP private supaya dapat terkoneksi ke Internet dengan menggunakan satu atau lebih IP public. Sederhananya, NAT adalah firewall yang berfungsi untuk menerjemahkan IP Public yang berasal dari ISP menjadi IP Private agar computer yang menggunakan IP Private bisa terhubung ke internet.

Secara default, ada 2 chain pada NAT:

1. Srcnat/Source NAT, digunakan untuk menyembunyikan asal paket-paket dengan melakukan pemetaan alamat asal paket-paket yang akan menuju jaringan eksternal ke suatu IP address atau range address tertentu. Dengan kemampuan seperti ini, srcnat bisa digunakan sebagai server Masquerader.
2. Dstnat/destination NAT, sering digunakan untuk me-redirect secara transparan paket-paket yang masuk ke suatu lokasi/tujuan, misalnya diarahkan ke mesin yang berfungsi sebagai server proxy, dll,

## Firewall Mangle

Mangle adalah suatu cara yang digunakan untuk menandai atau mark paket data dan suatu koneksi yang bisa diterapkan pada fitur fitur mikrotik yang lain, contoh pada routes, pemisahan bandwidth pada queues, NAT dan filter rules. mangle padamikrotik hanya dapat dipakai pada mikrotik itu sendiri. Dan yang penting proses pembacaan rule mangle ini dilakukan dari urutan pertama ke bawah.

Ada jenis jenis penandaan atau mark pada Mangle yaitu:

### **Packet Mark, Connection Mark, dan Routing Mark.**

- **Packet Mark:** Menandai paket yang masuk maupun keluar, seperti upload/download
- **Connection Mark:** Menandai koneksi yang terhubung pada router.
- **Routing Mark:** Menandai routing yang masuk maupun keluar router.

Secara default mangle terbagi menjadi beberapa chain, yaitu :

- Chain Input digunakan untuk menandai trafik yang masuk menuju ke router mikrotik serta hanya dapat menentukan In. Interface saja.
- Chain Output digunakan untuk menandai trafik yang keluar melewati router mikrotik serta hanya bisa memilih Out. Interface saja.
- Chain Forward digunakan untuk menandai trafik yang keluar masuk melalui router dan dapat memilih In dan Out Interface.

- Chain Prerouting dipakai untuk menandai trafik yang masuk mengarah serta melalui router (trafik download). Chain ini hanya dapat memilih Out. Interface saja.
- Chain Postrouting digunakan untuk menandai trafik yang keluar serta melalui router (trafik unggah) serta hanya dapat memilih In. Interface saja.

## Prinsip “IF” Kemudian “THEN”

**IF** (jika) packet memenuhi syarat kriteria yang kita buat.

**THEN** (maka) action apa yang akan dilakukan pada packet tersebut.

## FIREWALL -IF

The screenshot shows the 'New Firewall Rule' configuration window with several fields highlighted by red boxes:

- Chain:** Forward
- Src. Address:** [Field] → **Source IP (IP client)**
- Dst. Address:** [Field] → **Destination IP (IP internet)**
- Protocol:** [Field] → **Protocol (TCP/UDP/ICMP, dll)**
- Src. Port:** [Field] → **Source port (biasanya port dari client)**
- Dst. Port:** [Field] → **Destination port (service port tujuan)**
- In. Interface:** [Field] → **Interface (traffik masuk atau keluar)**
- Out. Interface:** [Field]
- In. Interface List:** [Field]
- Out. Interface List:** [Field]
- Packet Mark:** [Field] → **Paket yang sebelumnya telah ditandai**
- Connection Mark:** [Field]
- Routing Mark:** [Field]
- Routing Table:** [Field]

## Firewall-Then

	Advanced	Extra	Action	Statistics
n:	accept accept add dst to address list <b>add src to address list</b>			<p><b>accept</b> - accept the packet. Packet is not passed to next firewall rule.</p> <p><b>add-dst-to-address-list</b> - add destination address to <a href="#">address list</a> specified by address-list parameter</p> <p><b>add-src-to-address-list</b> - add source address to <a href="#">address list</a> specified by address-list parameter</p> <p><b>drop</b> - silently drop the packet</p> <p><b>fasttrack connection</b></p> <p><b>jump</b></p> <p><b>log</b></p> <p><b>passthrough</b></p> <p><b>reject</b></p> <p><b>return</b></p> <p><b>tarpit</b></p>
x:	drop fasttrack connection jump log passthrough reject return tarpit			

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

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

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

**drop** - silently drop the packet

**fasttrack connection**

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

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

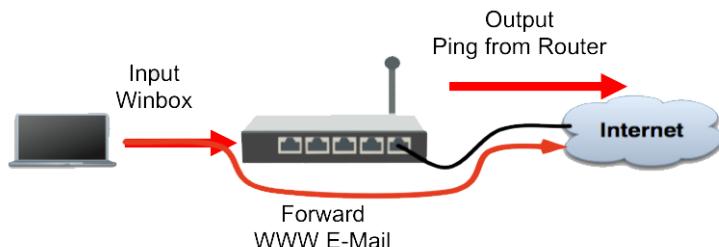
**passthrough** - ignore this rule and go to next one (useful for statistics).

**reject** - drop the packet and send an ICMP reject message

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

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

## Packet Flow



Tiga aturan dasar packet flow

INPUT: Packet menuju ke router.

OUTPUT: Packet keluar dari router.

FORWARD: Packet melewati router.

# **FIREWALL FILTER RULE**

## **CONTENT:**

- 1. OVERVIEW**
- 2. KASUS#1**
- 3. KASUS#2**
- 4. KASUS#3**

## **Overview**

Kalian pasti tahu yang namanya hacker kan? Hacker dikenal bisa membobol jaringan, apa yang terjadi jika hacker membobol router kita? Maka dari itu, kita harus memasang firewall agar router kita aman dari hacker maupun ancaman lain, salah satunya kita bisa mengamankan dengan fitur ‘Filter Rule’ pada firewall.

Pada lab ini, kita akan beberapa kasus tentang filter rule:

1. Blok IP yang akan melakukan PING ke router.
2. Blok IP yang akan meremote winbox lewat IP address, kecuali IP kita.
3. Mencatat semua IP yang melakukan PING terhadap router

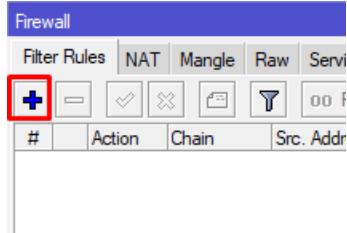
## KASUS#1

Pada kasus firewall kali ini kita akan mencoba blok PC kita, agar tidak bisa melakukan ping terhadap router.(IP PC: 192.168.1.2/24. IP router:192.168.1.1/24)

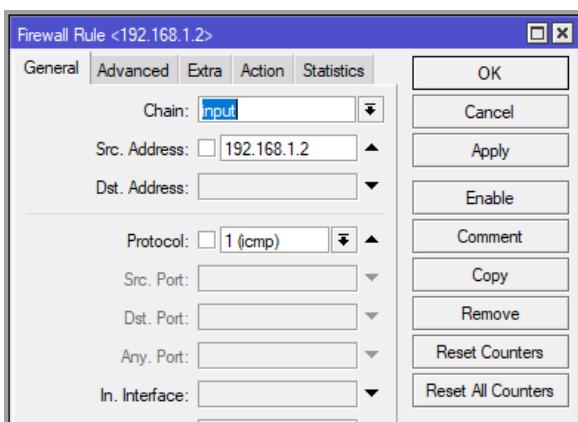
Beginilah penyelesaiannya:

```
C:\Users\ASUS>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
```

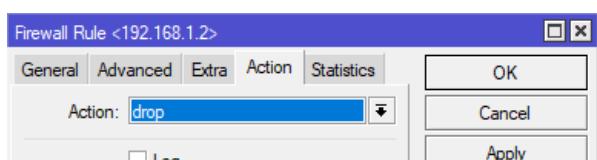
- Sebelumnya kita mencoba ping terlebih dahulu PING ke router.



- Buka winbox, kemudian klik menu 'IP > Firewall'
- Kita menuju menu filter rules, lalu klik '+' untuk menambah rule.
- Kita isikan:



- Chain: Input (karena masuk melewati router)
- Src. Address: 192.168.1.2 (IP PC kita, kita isikan Src. Address karena sumber IP nya berasal dari IP PC kita)
- Protocol: 1 ICMP (protocol PING adalah ICMP)



- Lalu kita pindah ke tab Action kita isikan: drop (membuang paket)
- Jika sudah 'apply' lalu 'ok'

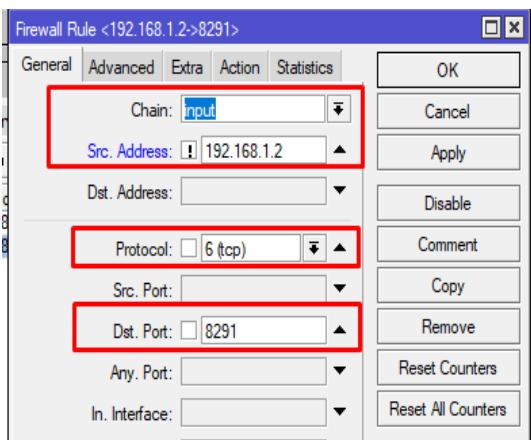
- Kita bisa lihat, hasilnya timeout karena kita sudah memblokir akses IP

```
C:\Users\ASUS>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```

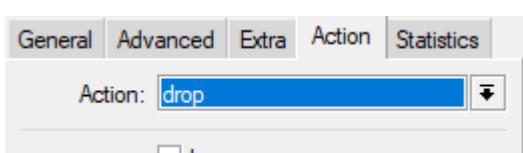
## KASUS#2

Di kasus ini, kita mencoba blok semua IP yang mencoba mengakses winbox lewat IP address, kecuali kita, jadi hanya IP kita yang bisa mengakses winbox.

- Pertama-tama kita masuk winbox, lalu kita tambahkan rule baru di firewall>filter rule.
- Kita isikan:

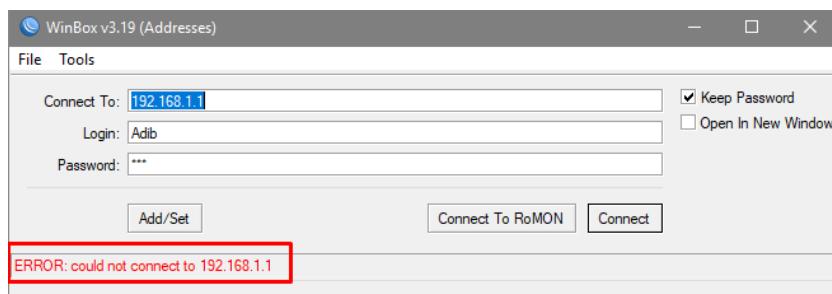


- Chain: Input
- Src. Address: !192.168.1.2 (tanda ! [seru] berfungsi untuk mengecualikan)
- Protocol: 6 TCP, (karena port winbox menggunakan protocol tcp)
- Dst. Port: 8291 (port winbox)
- Lalu kita menuju tab Action
- Kita isikan, Action:drop



Jika sudah bisa kita uji coba.

- Jika kita mengakses winbox menggunakan IP dan PC kita menggunakan IP 192.168.1.2, maka kita bisa mengakses.
- Namun, jika kita mengganti IP address PC kita menjadi 192.168.1.5 maka kita tidak bisa mengaksesnya.



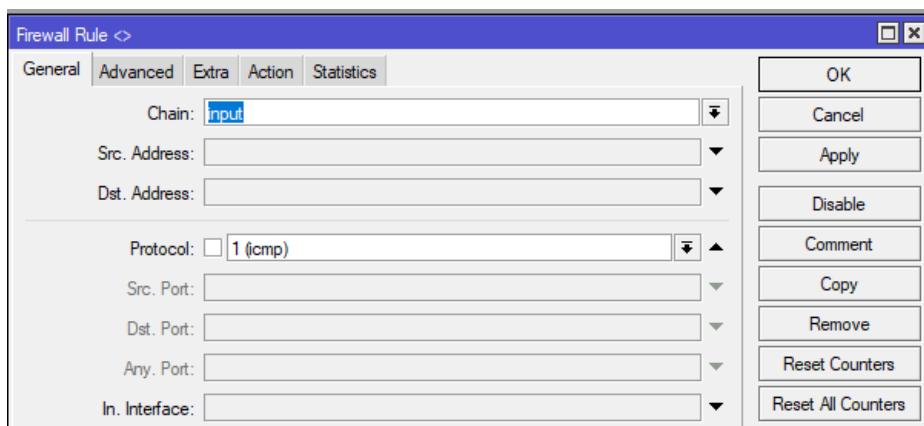
Hanya saja, ada beberapa kekurangan:

1. Meskipun kita sudah blok IP address, tetap saja kita masih bisa mengakses lewat mac address.
2. IP yang harus kita pasang antara PC dan router harus satu network, misal PC network 10.10.10.0, maka router juga harus network 10.10.10.0.

## KASUS#3

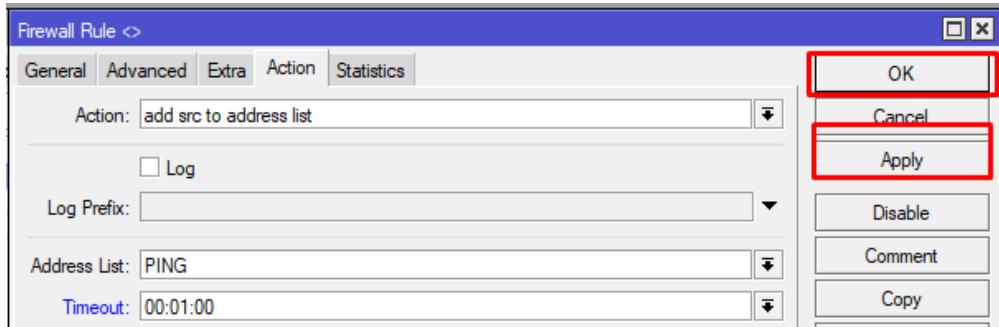
Pada kasus ini, kita akan mencari tahu caranya agar kita bisa mencatat semua IP yang melakukan PING terhadap router.

- Pertama-tama buka winbox, menu IP>firewall, kita tambahkan filter rule.



- Kita isikan:
  - Chain: Input
  - Protocol: ICMP (default protocol PING)

- Lalu kita menuju tab Action



- Kita isikan:
  - Action: add src to address list
  - Address List: PING
  - Timeout: 1 menit (dalam waktu 1 menit, IP yang bernama PING di address list akan hilang.) pilihan ini opsional.
  - Jika sudah 'apply' kemudian 'ok'
- Lalu kita mencoba untuk melakukan PING dari PC ke router.
- IP PC yang tadi melakukan PING akan tercatat dan terdaftar di address list.

	Name	Address	Timeout	Creation Time
D	PING	192.168.1.2		Jan/02/1970 01:...
D	PING	192.168.45.56	00:00:44	Jan/02/1970 02:...

Kesimpulan:

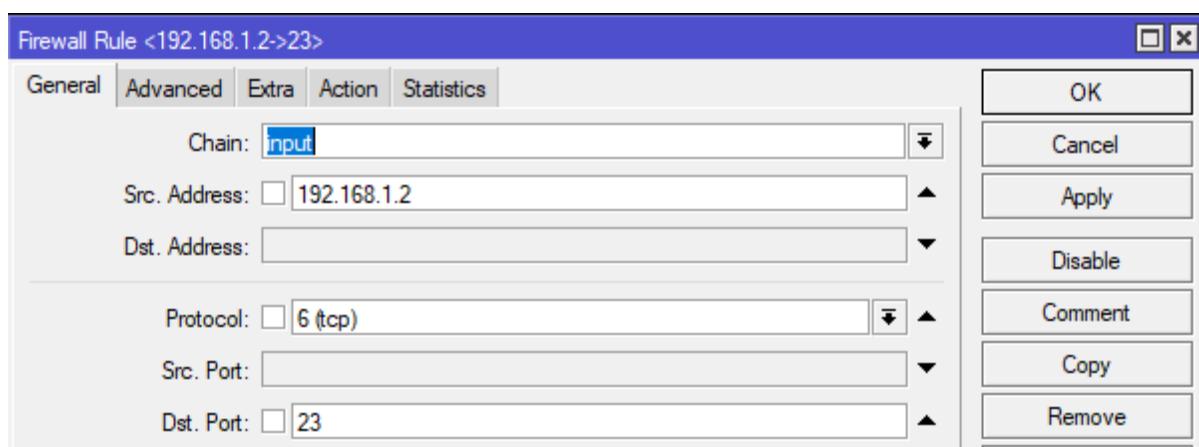
Kita bisa merubah rule yang kita buat, misal kita akan blok Telnet, maka pada protocol, kita isi TCP and dst. portnya 23.

# FIREWALL LOGGING

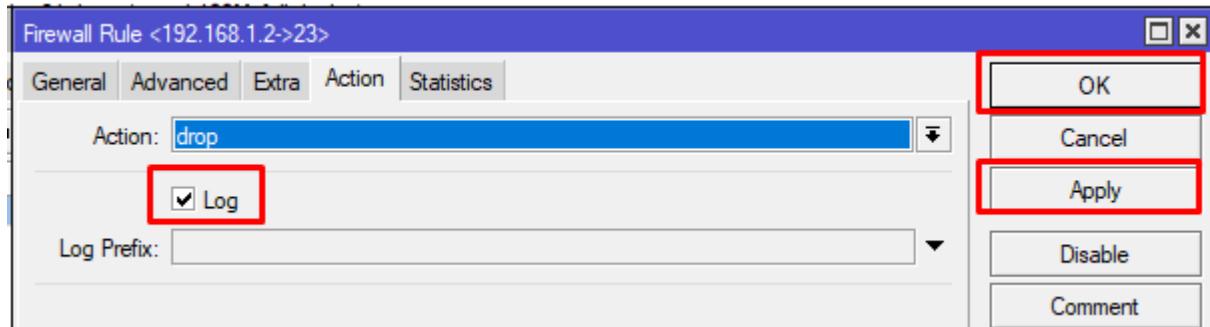
Pada firewall, kita juga bisa melihat history/riwayat kejadian firewall yang terjadi, namun fitur itu hanya dapat kita akses jika kita mengaktifkan 'log' pada tab Action di firewall. Kita coba contohkan.

Contoh pada kali ini, kita akan mencoba memblokir akses telnet dengan filter rule.

- Pertama-tama buka menu firewall dan tambahkan filter rule



- Kita isikan:
  - Chain: Input
  - Src. Address: 192.168.1.2 (IP PC)
  - Protocol: TCP
  - Dst. Port: 23



- Lalu kita menuju tab Action dan isikan:
  - Action: drop
  - Centang log
  - Lalu ‘apply’ dan ‘ok’
- Jika sudah kita coba untuk melakukan telnet ke IP router

```
C:\Users\ASUS>telnet 192.168.1.1
Connecting To 192.168.1.1...Could not open connection to the host, on port 23: Connect failed
```

- Hasilnya gagal, dan sudah tercatat pada menu log.

Jan/02/1970 03:04:20	memory	firewall, info	input: in:ether2 out:(unknown 0), src-mac 04:d4:c4:69:5c:a6, proto TCP (SYN), 192.168.1.2:55951->192.168.1.1:23, len 52
Jan/02/1970 03:04:23	memory	firewall, info	input: in:ether2 out:(unknown 0), src-mac 04:d4:c4:69:5c:a6, proto TCP (SYN), 192.168.1.2:55951->192.168.1.1:23, len 52
Jan/02/1970 03:04:29	memory	firewall, info	input: in:ether2 out:(unknown 0), src-mac 04:d4:c4:69:5c:a6, proto TCP (SYN), 192.168.1.2:55951->192.168.1.1:23, len 52
Jan/02/1970 03:16:01	memory	firewall, info	input: in:ether2 out:(unknown 0), src-mac 04:d4:c4:69:5c:a6, proto TCP (SYN), 192.168.1.2:56032->192.168.1.1:23, len 52
Jan/02/1970 03:16:04	memory	firewall, info	input: in:ether2 out:(unknown 0), src-mac 04:d4:c4:69:5c:a6, proto TCP (SYN), 192.168.1.2:56032->192.168.1.1:23, len 52
Jan/02/1970 03:16:10	memory	firewall, info	input: in:ether2 out:(unknown 0), src-mac 04:d4:c4:69:5c:a6, proto TCP (SYN), 192.168.1.2:56032->192.168.1.1:23, len 52

# MEMBLOKIR SITUS

## Overview

Jika didalam rumah, warnet, perusahaan, dll. Pasti butuh sesuatu yang bernama blokir situs, seperti perusahaan yang memblokir website youtube dari pukul 7 pagi-6 sore (jam kerja) agar pegawainya tidak lalai dalam bekerja. Lalu di warnet, diblokir situs yang berkonten negative agar anak-anak tidak dapat mengaksesnya, dsb. Namun, kita juga bisa mengatur yang mana klien yang mau kita blok, dan pembagiannya.

Untuk caranya tersendiri ada bermacam-macam:

## Dengan Filter Rule.

Banyak sekali cara untuk memblokir situs, namun untuk cara mudah yang paling dasarnya adalah menggunakan filter rule, dan untuk konfigurasinya kita hanya butuh mencari IP situsnya tersebut, kemudian menambahkan action=drop untuk memblokirnya.

Beginilah langkah-langkahnya:

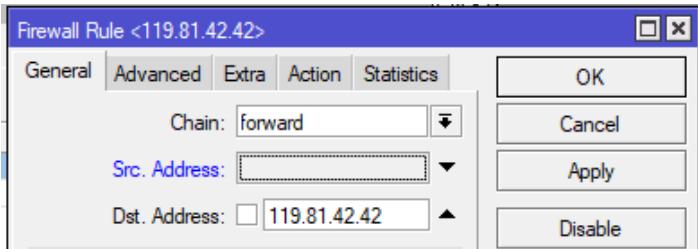
- Kita cari IP Address dari situs yang ingin kita blok, dengan cara buka CMD, ketikkan ‘nslookup 1cak.com’ misalkan kita akan memblokir 1cak.
- Untuk permulaan, kita coba blokir dengan situs yang hanya terdapat

```
C:\Users\ASUS>nslookup 1cak.com
Server:  dns.google
Address: 8.8.8.8

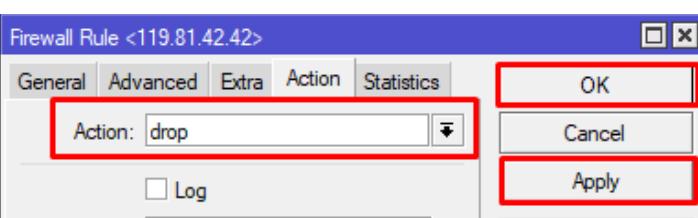
Non-authoritative answer:
Name: 1cak.com
Address: 119.81.42.42
```

1 IP Address, seperti 1cak.

- Kemudian kita tambahkan rule untuk memblokirnya. Isi:



- Chain: Forward
- Dst. Address: 119.81.42.42



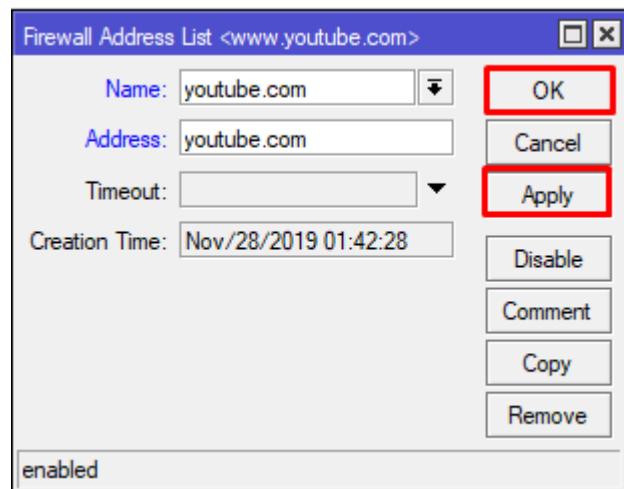
- kita menuju tab Action, isikan:
- Action: drop
- Lalu 'apply' kemudian 'ok'

Dengan begini, akses kita menuju situs lcak akan gagal karena sudah kita blokir.

## Dengan Address List.

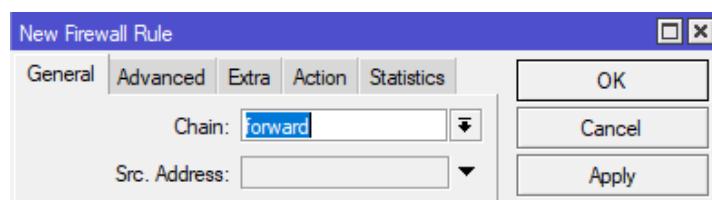
Kita akan memblokir situs Youtube dengan Address List, caranya sederhana.

- Pertama-tama kita buka winbox, menuju IP>firewall>address list lalu kita add ‘+’
- Kita isikan:
  - Name: (bebas)
  - Address: youtube.com
  - Lalu ‘apply’ dan ‘ok’

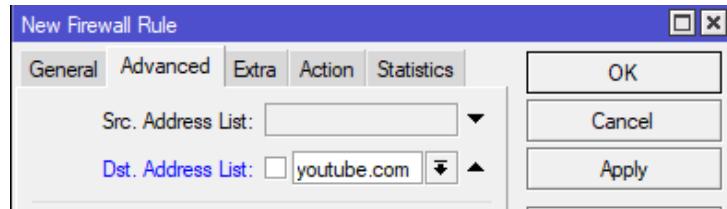


Firewall				
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols				
Name	Address	Timeout	Creation Time	
youtube.c...	youtube.com		Nov/28/2019 08:...	
D :: youtube.com				
D :: youtube.com	74.125.68.91		Nov/28/2019 08:...	
D :: youtube.com	74.125.68.93		Nov/28/2019 08:...	
D :: youtube.com	74.125.68.190		Nov/28/2019 08:...	
D :: youtube.com	74.125.68.136		Nov/28/2019 08:...	

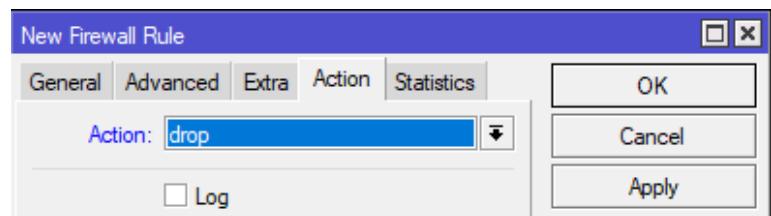
- Deretan address Youtube sudah bisa terlihat.
- Selanjutnya kita blok menggunakan filter rule.
- Kita buat rule baru, isikan Chain: Forward



- Lalu pada tab Advanced, isikan Dst. Address List: youtube.com



- Lalu pada tab Action, isikan Action: drop



- Jika sudah, maka situs youtube.com sudah terblokir.
- Untuk memastikannya, kita buka situs Youtube dan kemudian lihat statistic pada filter rules, jika berjalan dan ada paket yang masuk, maka pemblokiran sudah berhasil.

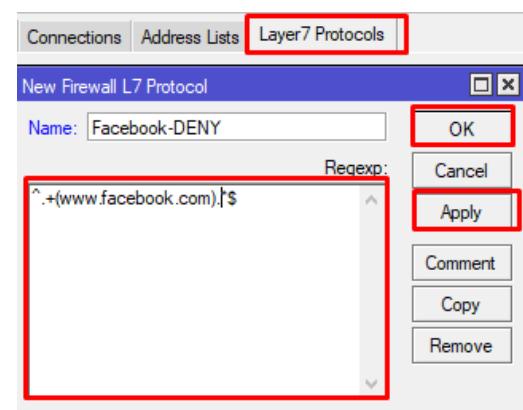
Note: untuk website yang akan kita blok, jika Youtube masih bisa mengakses padahal sudah kita blok, coba gunakan website selain Youtube, karena Youtube memang susah untuk diblokir.

## Dengan Layer 7 Protocol.

Blok pada layer 7 bisa tergolong sangat ampuh karena cara kerja Layer 7 adalah mencocokan (mathcer) 10 paket koneksi pertama atau 2KB koneksi pertama dan mencari pola/pattern data yang sesuai dengan yang tersedia. Jika pola ini tidak ditemukan dalam data yang tersedia, matcher tidak memeriksa lebih lanjut. Dan akan dianggap unknown connections. Anda harus mempertimbangkan bahwa banyak koneksi secara signifikan akan meningkatkan penggunaan memori pada RB maupun PC Router anda. Untuk menghindari itu tambahkan regular firewall matchers (pattern) untuk mengurangi jumlah data yang dikirimkan ke layer-7 filter.

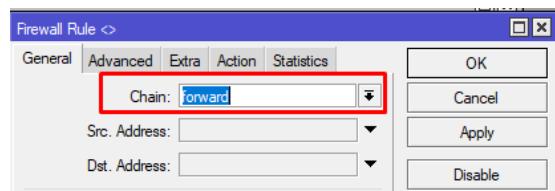
Caranya sebagai berikut:

- Misalkan kita akan mencoba memblokir Facebook dengan Layer 7 protocol.
- Pertama-tama kita menuju ke menu ‘firewall>layer7 Protocols’ lalu kita buat baru ‘+’
- Di tabel Layer7 kita isi:
  - Name: (bebas), saya isi: Facebook-DENY
  - Pada tabel Regexp kita isi : $^.+(www.facebook.com).*$$ .
  - Saya isi:
- Jika sudah diisi klik ‘apply’ lalu ‘ok’

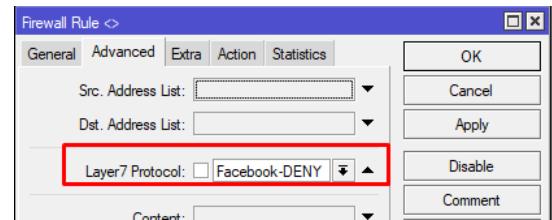


$^.+(www.facebook.com).*$$  karena saya ingin memblokir Facebook.

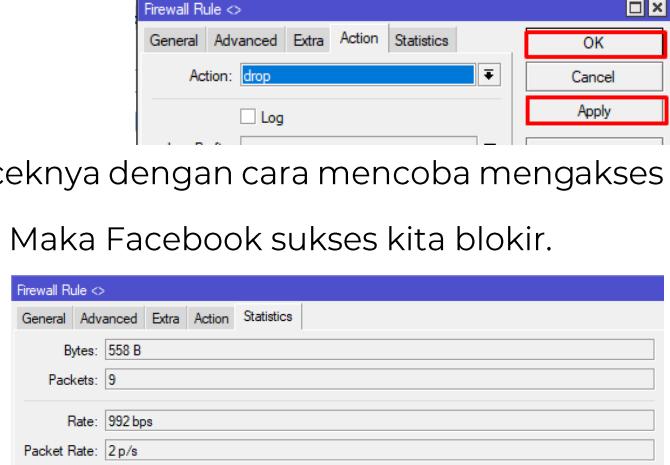
- Skrip layer 7 protocol sudah jadi, namun jika kita buka situs Facebook masih bisa dibuka. Hal ini karena kita belum memberi Action=drop untuk skrip layer 7 protocol tadi.
- Untuk memberi action, kita tambahkan rule di firewall. Kita isikan Chain: Forward.



- Kemudian ke tab Advanced. Kita isikan Layer7 protocol dengan yang kita buat tadi: Facebook-DENY.



- Kita beri Action=drop.
- Lalu 'apply' dan 'ok'
- Jika sudah kita bisa mengeceknya dengan cara mencoba mengakses situs Facebook, jika tidak bisa. Maka Facebook sukses kita blokir.
- Kita juga bisa melihat pada statistic rule layer 7 protocol tadi.
- Jika ada bytes dan packet yang masuk, maka pemblokiran sukses.

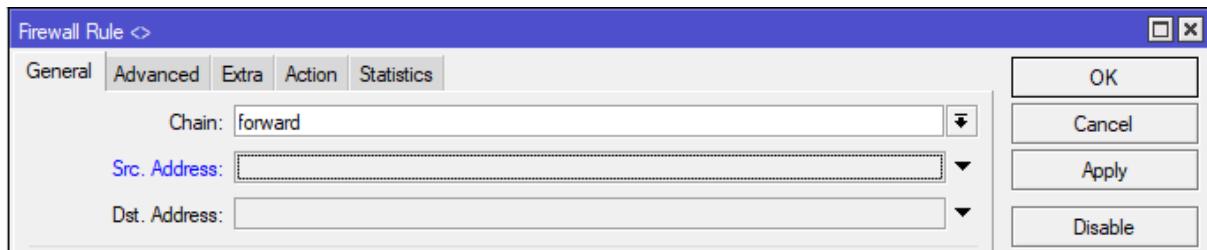


## Pemblokiran Konten

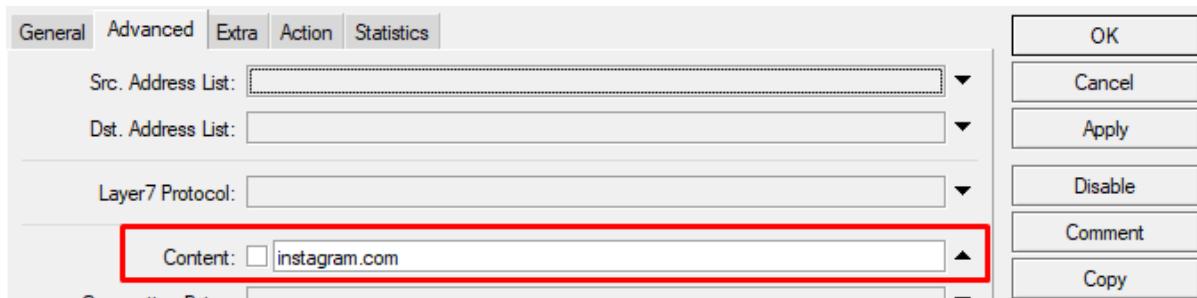
Blokir konten berarti memblokir seluruh akses terhadap internet mengenai segala hal yang terkait dengan konten tersebut, misalkan kita mencoba memblokir konten tentang Instagram, maka seluruh hal yang berkaitan atau mengandung unsur Instagram terblokir.

Untuk penerapannya:

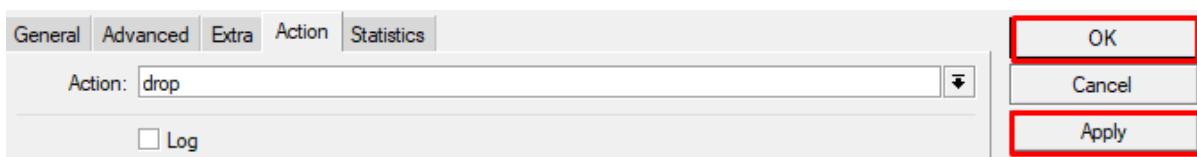
- Kita tambahkan firewall rule, kemudian isikan Chain:forward



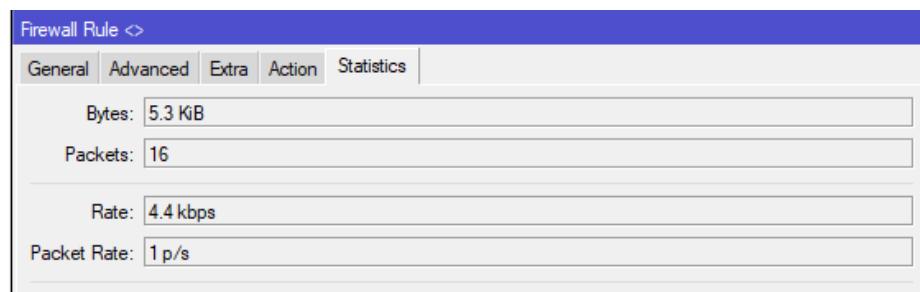
- Kemudian pada tab Advanced kita isikan pada tabel content: 'instagram.com' karena kita akan memblokir Instagram.



- Kemudian pada tab Action, kita isikan Action:drop



- Setelah itu cobalah membuka situs Instagram, jika tidak bisa maka pemblokiran berhasil. Kemudian cek statistic pada rulenya, jika ada bytes/packets yang masuk, berarti pemblokiran berhasil.



## Pemblokiran dengan DNS.

Didalam internet banyak sekali bertebaran website-website maupun hal-hal yang berkonten negatif, dan jika kita ingin memblokirnya, pasti akan lelah jika kita memblokir semua websitenya secara satu-persatu. Oleh karena itu, kita gunakan DNS agar lebih mudah dalam melakukan pemblokiran, jadi kita tidak perlu memblokir satu-demi satu karena akan banyak memakan rule dan waktu, cukup satu rule, yaitu DNS. Semua website yang diblokir sudah dikonfigurasikan oleh DNS, jadi kita tidak perlu repot memblokir satu-satu.

Beginilah konfigurasinya:

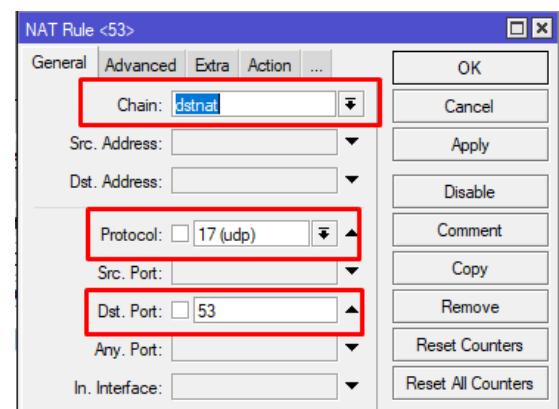
- Kita buka website [www.dnsbersih.id](http://www.dnsbersih.id)

### DNS NAWALA

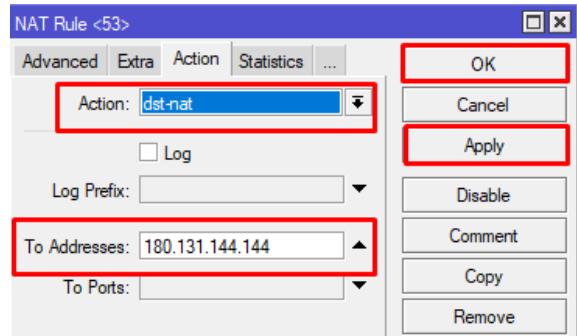
DNS Nawala adalah layanan DNS yang bebas digunakan oleh pengguna akhir atau penyedia jasa internet untuk mendapatkan akses internet bersih dan aman.

NS #1 : 180 . 131 . 144 . 144  
NS #2 : 180 . 131 . 145 . 145

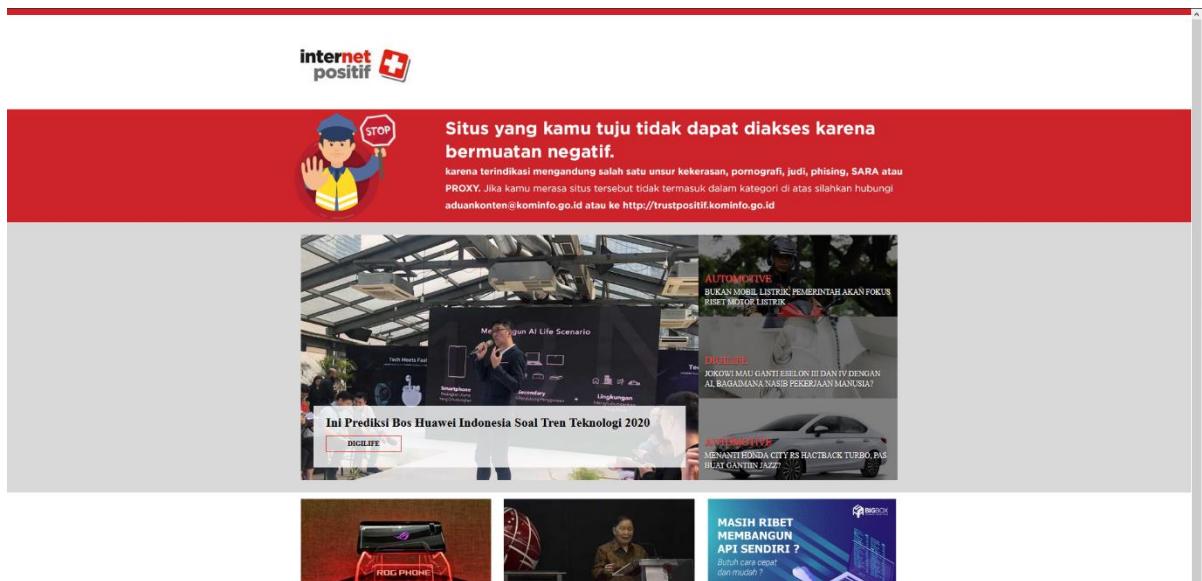
- Disitu akan ada IP DNS, kita pilih salah satu untuk di-copy.
- Kemudian kita tambahkan rule NAT. 'IP>Firewall>NAT' kita isikan:
  - Chain: dstnat
  - Protocol: udp (karena protocol DNS itu udp)
  - Dst. Port: 53 (Portnya DNS=53)



- Kemudian pada tab Action, kita isi:
  - Action: dst-nat
  - To Addresses: 180.131.144.144 (IP DNS tadi)



- Jika sudah, maka DNS sudah aktif, jika kita mencoba mengakses situs negatif, maka Internet Positif akan muncul.



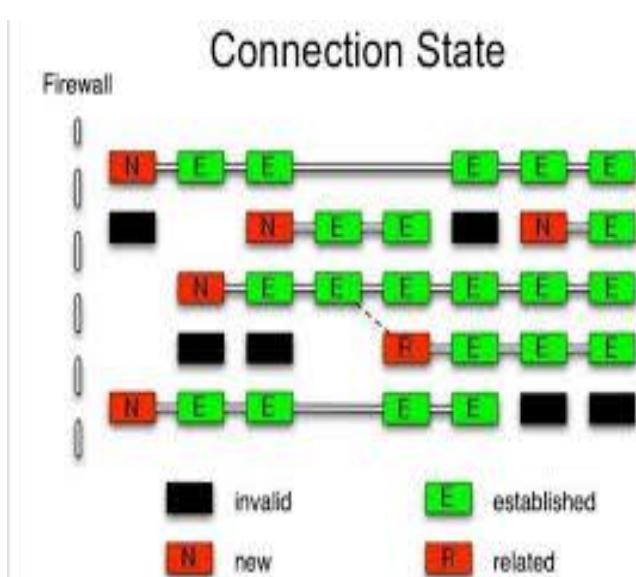
# CONNECTION TRACKING & STATE

Connection Tracking merupakan sebuah fitur yang digunakan untuk melihat informasi yang melewati router, masuk router, maupun keluar router seperti dst-address dan src-address yang sedang digunakan. Untuk mengeceknya kita bisa klik menu ‘IP>Firewall>Connections’

The screenshot shows the Winbox Firewall interface with the 'Connections' tab selected. The table displays various network connections with columns for Src. Address, Dist. Address, Reply Src. Address, Protocol, Connecti..., Connecti..., P2P, Timeout, TCP State, and ICMP Type. A red box highlights the 'Tracking' button in the toolbar above the table.

Src. Address	Dist. Address	Reply Src. Address	Protocol	Connecti...	Connecti...	P2P	Timeout	TCP State	ICMP Type
A 10.5.8.208.55337	66.228.113.24.8291	66.228.113.24.8291	6 (tcp)				00:04:23	established	
U 10.10.0.3	224.0.0.5	224.0.0.5	89 (ospf)				00:09:17		
A 10.10.0.3.47445	66.228.113.24.161	66.228.113.24.161	17 (udp)				00:02:23		
A 10.10.0.3.51186	66.228.113.24.23	66.228.113.24.23	6 (tcp)				00:00:05	close	
A 10.10.0.3.51997	66.228.113.24.80	66.228.113.24.80	6 (tcp)				00:00:03	time wait	
A 10.10.0.3.55102	66.228.113.24.8291	66.228.113.24.8291	6 (tcp)				23:59:20	established	
A 10.10.0.3.56727	66.228.113.24.22	66.228.113.24.22	6 (tcp)				00:00:04	close	
A 10.10.0.3.59423	66.228.113.24.21	66.228.113.24.21	6 (tcp) ftp				00:00:06	time wait	
U 66.228.113.24	224.0.0.5	224.0.0.5	89 (ospf)				00:09:24		
U 66.228.113.24.22	159.148.172.205.1631	159.148.172.205.1631	6 (tcp)				07:41:27	established	
U 66.228.113.24.23	159.148.172.205.4566	159.148.172.205.4566	6 (tcp)				06:03:50	established	
U 66.228.113.24.80	61.247.26.243.1177	61.247.26.243.1177	6 (tcp)				21:59:32	established	
U 66.228.113.24.80	41.234.95.3.12701	41.234.95.3.12701	6 (tcp)				06:52:49	established	
U 66.228.113.24.80	58.96.34.68.4304	58.96.34.68.4304	6 (tcp)				01:43:51	established	
U 66.228.113.24.80	41.234.129.149.13058	41.234.129.149.13058	6 (tcp)				12:29:52	established	
U 66.228.113.24.80	125.160.169.179.51...	125.160.169.179.51566	6 (tcp)				22:27:30	established	
U 66.228.113.24.80	77.48.235.215.8530	77.48.235.215.8530	6 (tcp)				05:49:42	established	
U 66.228.113.24.80	41.234.95.3.12700	41.234.95.3.12700	6 (tcp)				06:52:46	established	
U 66.228.113.24.80	217.52.99.170.3269	217.52.99.170.3269	6 (tcp)				06:17:51	established	
U 66.228.113.24.80	65.5.222.47.50726	65.5.222.47.50726	6 (tcp)				10:42:12	established	
U 66.228.113.24.8291	41.233.48.14.50087	41.233.48.14.50087	6 (tcp)				19:54:00	established	
U 66.228.113.24.8291	189.58.32.236.1484	189.58.32.236.1484	6 (tcp)				19:54:28	established	
U 66.228.113.24.8291	41.236.252.35.52727	41.236.252.35.52727	6 (tcp)				15:57:36	established	
U 66.228.113.24.8291	189.58.32.236.1478	189.58.32.236.1478	6 (tcp)				19:53:32	established	
U 66.228.113.25	224.0.0.5	224.0.0.5	89 (ospf)				00:09:24		
A 80.93.248.214.2050	66.228.113.24.8291	66.228.113.24.8291	6 (tcp)				06:54:20	established	
A 80.93.248.214.54899	66.228.113.24.8291	66.228.113.24.8291	6 (tcp)				23:57:55	established	
A 80.93.249.97.3687	66.228.113.24.8291	66.228.113.24.8291	6 (tcp)				02:08:30	established	
A 159.148.172.205.3160	66.228.113.24.161	66.228.113.24.161	17 (udp)				00:02:24		
A 159.148.172.205.4177	66.228.113.24.23	66.228.113.24.23	6 (tcp)				00:00:00	close	
A 159.148.172.205.4336	66.228.113.24.22	66.228.113.24.22	6 (tcp)				00:00:02	close	
A 159.148.172.205.4403	66.228.113.24.21	66.228.113.24.21	6 (tcp) ftp				00:00:04	close	
A 159.148.172.205.4512	66.228.113.24.80	66.228.113.24.80	6 (tcp)				00:00:04	time wait	
A 159.148.172.205.4939	66.228.113.24.8291	66.228.113.24.8291	6 (tcp)				23:55:23	established	
A 193.189.117.122.42...	66.228.113.24.161	66.228.113.24.161	17 (udp)				00:01:40		
A 193.189.117.122.42...	66.228.113.24.161	66.228.113.24.161	17 (udp)				00:01:40		

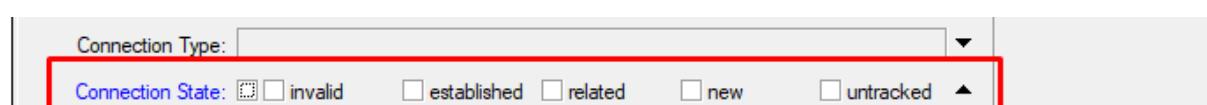
Status dalam connection Tracking :



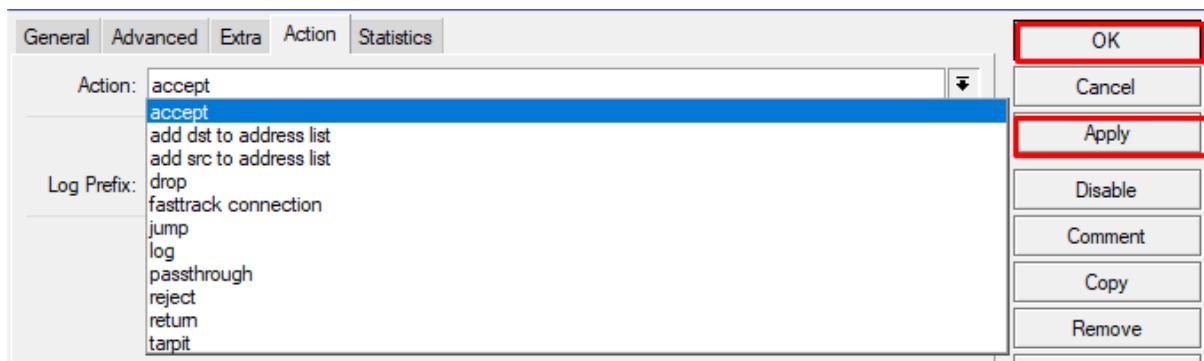
- Established : Paket data bagian dari yang sudah dikenali
- New : Paket baru yang memulai koneksi.
- Related : Paket yang memulai koneksi baru tetapi sudah terkait dengan koneksi yang sudah ada sebelumnya.
- Invalid : Paket tidak memiliki koneksi apapun

Kita juga dapat membuat rule untuk Connection State, caranya:

- Pertama-tama kita tambahkan rule baru, kita isikan pada tab general:
  - Chain: Forward
  - Connection State: kita isikan terserah kita, namun kita juga harus menyamakannya dengan Action:



- Established : Accept
- Related : Accept
- New : Passthrough
- Invalid : Drop



- Jika kita sudah memilih yang sesuai, maka tinggal 'apply' lalu 'ok'.

2	✓ acc...	forward					established
3	✓ acc...	forward					related
4	✗ pas...	forward					new
5	✗ drop	forward					invalid

## Catatan:



# PENGENALAN WIRELESS

## CONTENT:

- 1. OVERVIEW**
- 2. SIMPLE INTERKONEKSI WIRELESS**
- 3. VIRTUAL ACCESS POINT**
- 4. NSTREME**
- 5. MAC ADDRESS FILTERING**
- 6. WDS DYNAMIC**
- 7. WDS STATIC**
- 8. WIRELESS BRIDGE**
- 9. WIRELESS MULTIFUNGSI**
- 10. WIRELESS REPEATER**

## Overview

Apa yang dimaksud dengan Pengertian Wireless?

Pengertian Wireless yakni sebuah jaringan nirkabel atau tanpa kabel yang menggunakan udara sebagai media penghubung transmisinya guna menghantarkan gelombang elektromagnetik maupun data.

### Wireless Pada MikroTik.

RouterOS mendukung beberapa modul radio (wireless card) untuk jaringan WLAN atau Wi-Fi (Wireless Fidelity).

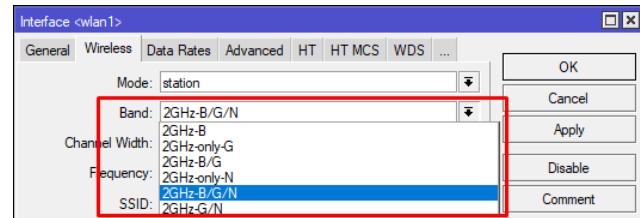
Wi-Fi memiliki standar & spesifikasi IEEE 802.11 dan menggunakan frekuensi 2,4GHz dan 5,8GHz.

MikroTik mendukung standar IEEE 802.11a/b/g/n

- 802.11a – frekuensi 5GHz, 54Mbps.
- 802.11b – frekuensi 2,4GHz, 11 Mbps.
- 802.11g – frekuensi 2,4GHz, 54Mbps.
- 802.11n (Level 4 keatas) – frekuensi 2,4GHz atau 5GHz, 300Mbps

## Wireless Band

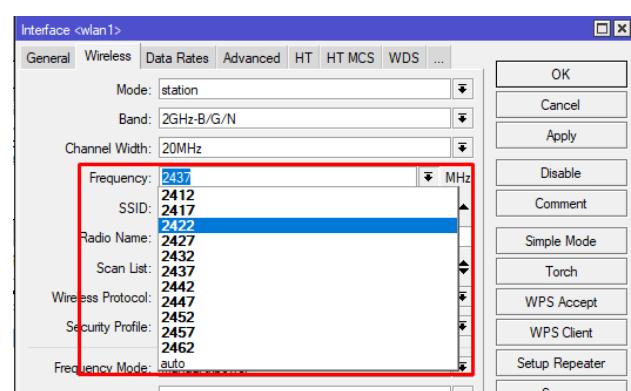
Band merupakan mode kerja frekuensi dari suatu perangkat wireless. Untuk menghubungkan 2 perangkat, keduanya harus bekerja pada band frekuensi yang sama.



## Wireless Frequency Channel

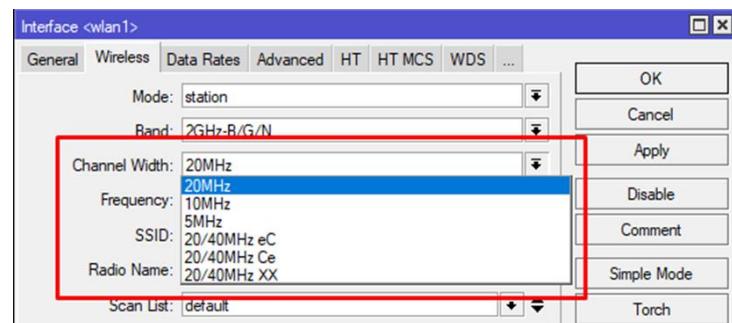
Frequency channel adalah pembagian frekuensi dalam suatu band dimana Access Point (AP) beroperasi. Nilai-nilai channel bergantung pada band yang dipilih, kemampuan wireless card, danaturan/regulasi frekuensi suatu negara. Range frequency channel untuk masing-masing band adalah sbb:

- 2,4Ghz = 2412 s/d 2499MHz
- 5GHz = 4920 s/d 6100MHz



## Wireless Channel Width

Channel Width/Lebar Channel adalah rentang frekuensi batas bawah dan batas atas dalam 1 channel. MikroTik dapat mengatur berapa lebar channel yang akan digunakan. Default lebar channel yang digunakan adalah 22Mhz (ditulis 20MHz). Lebar channel dapat dikecilkan (5MHz) untuk meminimalkan frekuensi, atau dibesarkan (40MHz) untuk mendapatkan throughput yang lebih besar.



## Frequency Regulation

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

Frequency Mode:	manual-txpower	
Country:	no_country_set	
Installation:	any	
Antenna Gain:	0	dBi

**Frequency Mode:**

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

**Country:** Pemilihan negara.

**Installation:**

1. Indoor: Pemasangan wireless didalam ruangan.
2. Outdoor: Pemasangan wireless diluar ruangan.

**Antena Gain:** Default 0, akan otomatis menyesuaikan agar tidak melebihi EIRP country regulation.

## Interface Wireless Mode

### 1. AP Mode

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

### 2. Station Mode

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

## Interface Wireless Special-Mode

- alignment-only: Mode transmit secara terusmenerus digunakan untuk positioning antena jarak jauh.
- nstreme-dual-slave: Digunakan untuk sistem nstreme-dual.
- WDS-slave: Sama seperti ap-bridge, namun melakukan scan ke AP dengan SSID yang sama dan melakukan koneksi dengan WDS. Apabila link terputus, akan melanjutkan scanning.

# **WIRELESS LAB:**

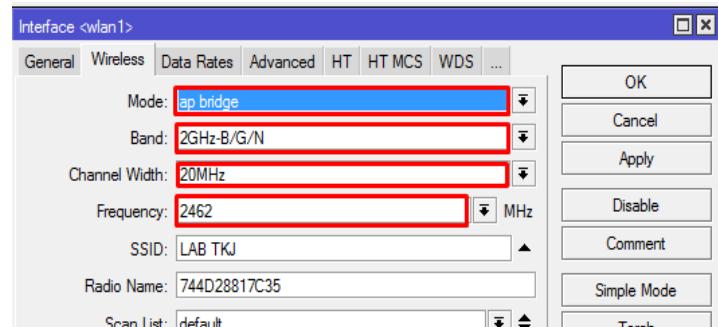
- 1. SIMPLE INTERKONEKSI WIRELESS**
- 2. VIRTUAL ACCESS POINT**
- 3. NSTREME**
- 4. MAC ADDRESS FILTERING**
- 5. WDS DYNAMIC**
- 6. WDS STATIC**
- 7. WIRELESS BRIDGE**
- 8. WIRELESS REPEATER**

# SIMPLE INTERKONEKSI WIRELESS

Kita akan mencoba menghubungkan dua RouterBoard dengan menggunakan Wireless, sebenarnya konsep nya sama dengan cara mengkoneksikan Router ke Internet tapi beda nya adalah Access Point yang digunakan menggunakan perangkat MikroTik.

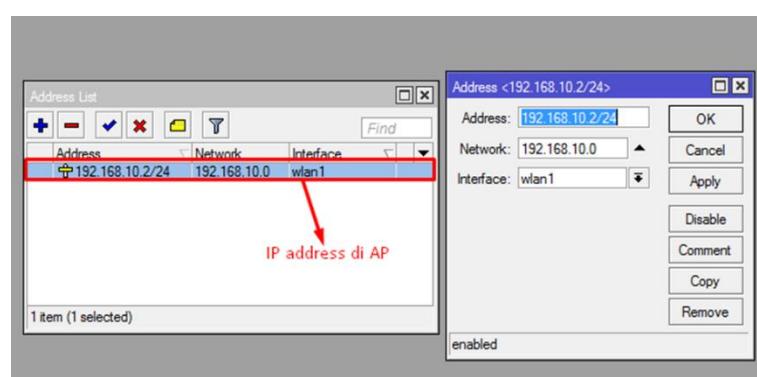
Pertama Kita harus mengonfigurasi router yang kita fungsikan sebagai **Access Point.**

- Klik Menu Wireless > Interface Wireless> Tab Wireless
- Pilih Mode=Ap Bridge  
Band=(terserah)2GHz-B  
Channel Width=20MHz  
Frekuensi=2462
- SSID=(terserah)Wireless  
LABTKJ
- Security Profile=di isi jika Access Point ingin di beri Security Wireless.



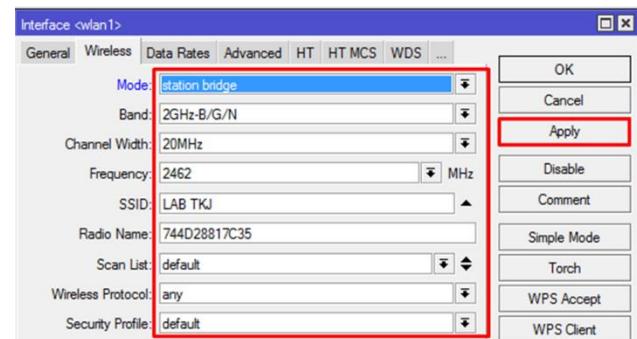
Kemudian kita buat Address untuk Access Point dan sebagai gateway untuk client.

- Klik Menu IP > Address > Add (+)
- Isi Address=(terserah)192.168.10.1/24 ,Interface=Wlan
- Lalu Apply dan OK

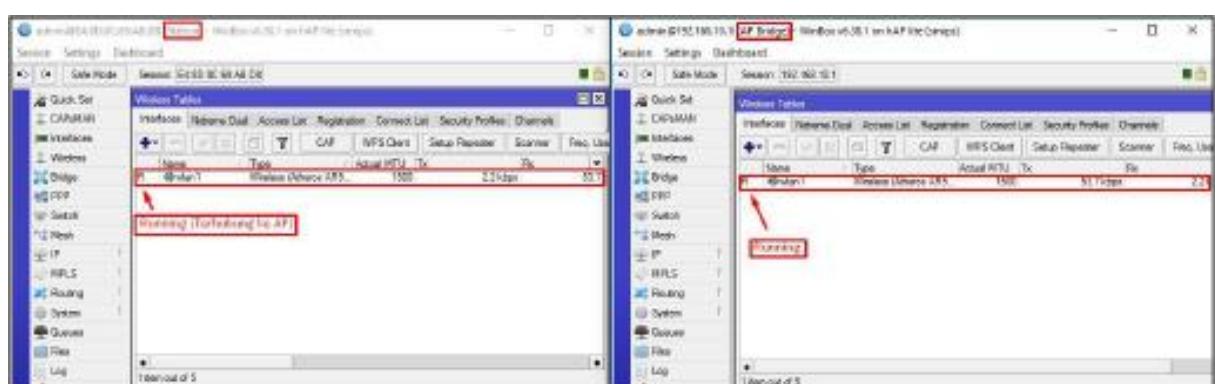


Jika sudah, kita ganti konfigurasi ke router yang menjadi **Station**.

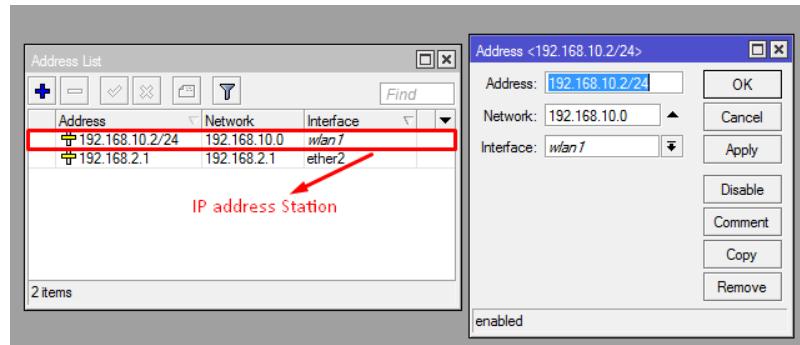
- Klik Menu Wireless >Interface Wireless> Tab Wireless
- Pilih Mode=Station Bridge,  
Band=2GHz-BChannel  
Width=20MHz  
Frekuensi=2462
- SSID= LABTKJ
- Security Profile=di isi jika Access Point di Password



Setelah kita apply, maka secara otomatis interface wlan antara dua router akan berjalan dengan status R (Running).

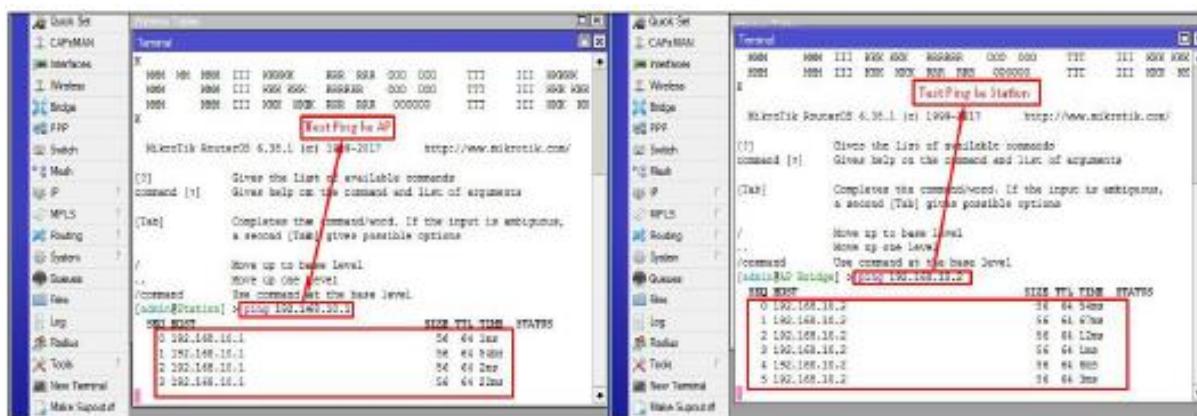


Selanjutnya kita akan meng-Konfigurasikan IP address untuk Interface Wireless secara Static.



- Klik Menu IP > Address > Add (+)
- Isi Address=192.168.10.2/24 ,Interface=Wlan1
- Lalu Apply dan OK

Jika sudah, maka antara Access Point dan Station sudah terhubung. Untuk mengetesnya kita bisa melakukan ping satu sama lain.



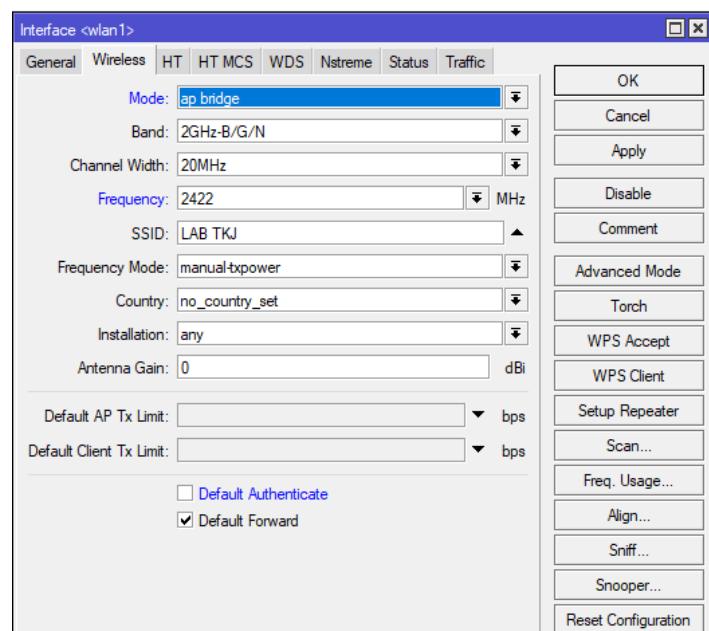
# VIRTUAL ACCESS POINT (VAP)

Multiple SSID adalah salah satu fitur yang sering digunakan dalam distribusi akses jaringan melalui media nirkabel/wireless. Metode ini memungkinkan sebuah perangkat yang secara fisik hanya memiliki satu interface wireless dapat memancarkan lebih dari satu SSID dengan service yang berbeda. Fitur ini sering digunakan untuk memenuhi kebutuhan berbagai instansi mulai dari kantor, sekolah dsb.

Maka dari itu, kita akan coba terapkan.

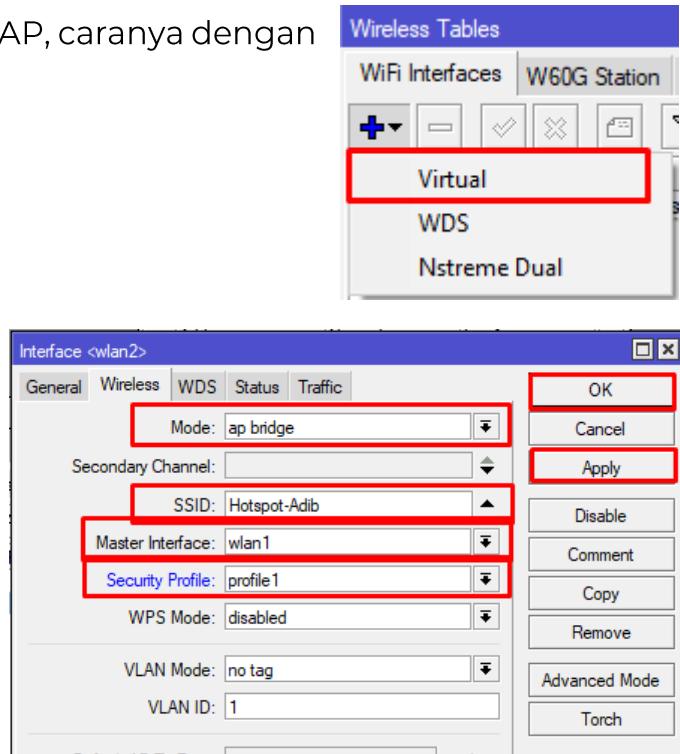
Pertama-tama kita buat router kita menjadi Access Point.

- Klik menu ‘Wireless>Interface wlan’
- Kemudian konfig interface wlan sebagai berikut:
  - Mode: AP Bridge
  - Band:2GHz-B/G/N
  - Channel:20MHz
  - Frekuensi:2422
  - SSID: LAB TKJ (Bebas)

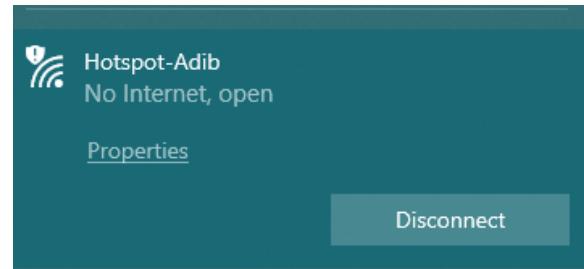


Kemudian, kita akan membuat VAP, caranya dengan klik add '+' pada wireless. Kita isi:

- Mode: AP Bridge
- SSID: Hotspot-Adib
- Master Interface: wlan1
- Security Profiles:  
(tambahkan jika butuh password)



Jika kita sudah membuat maka VAP akan aktif dan kita bisa terhubung dengan VAP tersebut.



**Catatan:** Semakin Banyak Virtual AP yang kita buat akan semakin padat traffic yang ada di Frekuensi tersebut,karna Frekuensi VAP mengikuti Frekuensi Master Interface Wireless.

# NSTREME

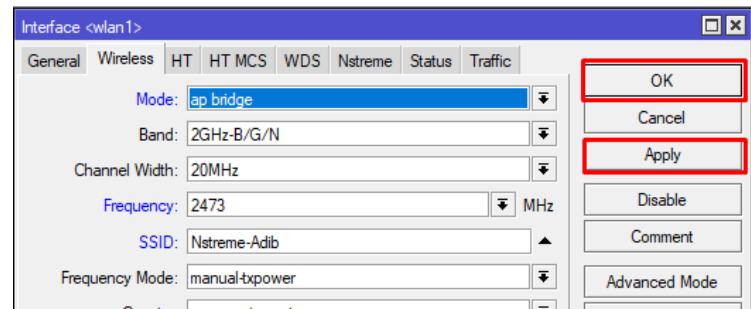
Nstreme adalah MikroTik proprietary, protokol nirkabel dibuat untuk mengatasi keterbatasan kecepatan dan jarak IEEE 802.11 standar dan untuk memperpanjang point-topoint dan point point-to-multi kinerja wireless link. Protokol Nstreme-dual baru yang dirancang untuk menyediakan komunikasi real full-duplex pada wireless dengan sepasang kartu nirkabel - satu untuk transmisi data dan satu untuk menerima,Bisa dibilang Nstreme berfungsi untuk memfokuskan Sinyal ke beberapa Device.

Beginilah caranya:

Pastikan terlebih dahulu, ada dua router, station dan Access Point.

Pertama-tama kita konfigurasi terlebih dahulu **Access Point**.

- Klik menu ‘Wireless>interface wireless’
- Kita isi pada tab wireless:
  - Mode=Ap Bridge
  - Band=(bebas)2GHz-B/G/N
  - Channel=20MHz
  - Frekuensi=(bebas)2473
  - SSID=(bebas)Nstreme-Adib

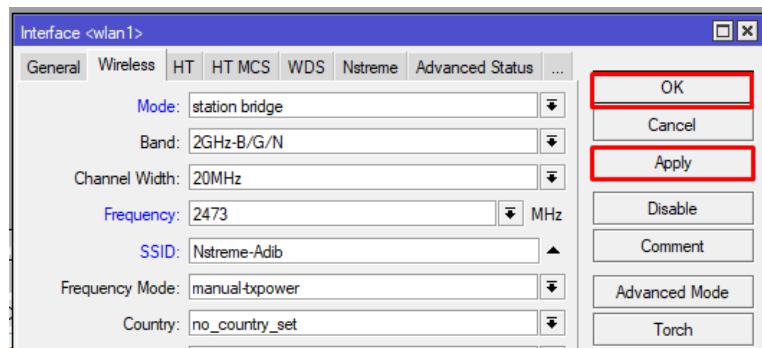


Selanjutnya kita buat IP Address untuk wlan1:

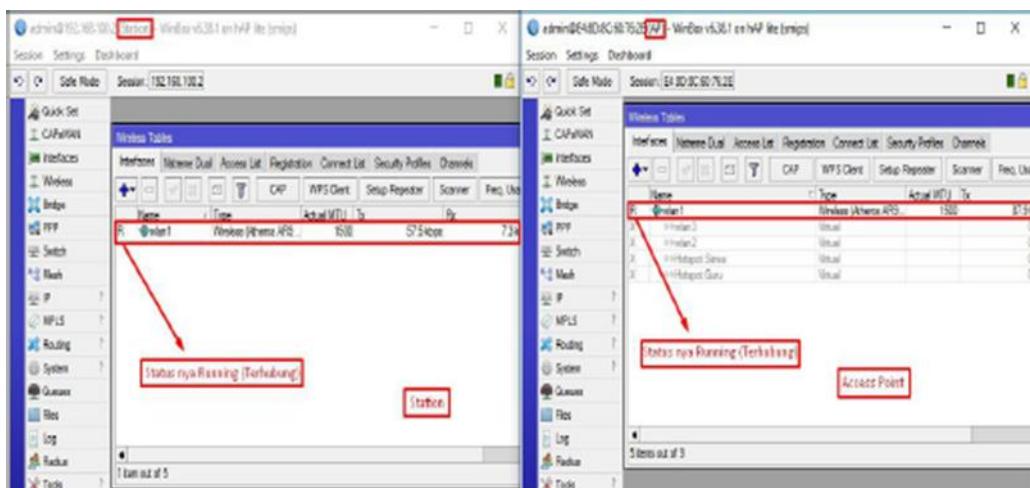
- IP Address: 192.168.100.1/24
- Interface: wlan1
- Jika sudah ‘apply’ lalu ‘ok’

Kemudian kita konfigurasi router yang menjadi **Station**.

- Klik menu ‘Wireless> interface wlan’
- Kita isikan pada tab wireless:
  - Mode: station bridge
  - Band=2GHz-B/G/N
  - Channel=20MHz
  - Frekuensi=2437
  - SSID: Nstreme-Adib  
(samakan dengan AP)
- Jika sudah klik ‘apply’ kemudian ‘ok’



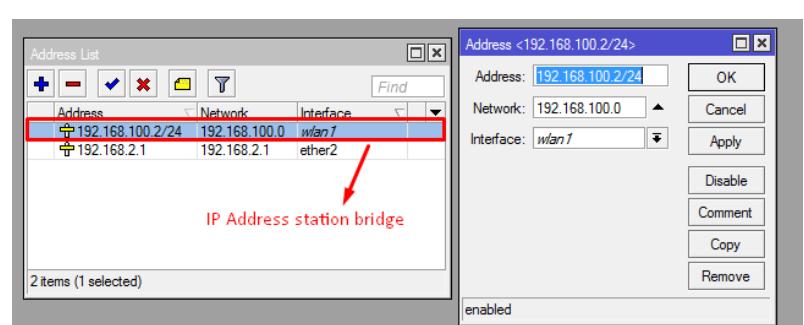
Jika sudah, maka status antara kedua interface wlan adalah R (running)



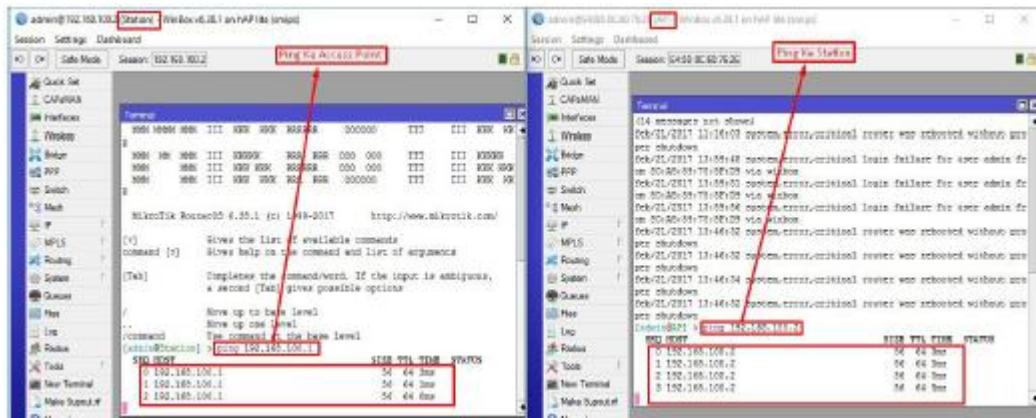
Lalu selanjutnya kita buat IP Address untuk Station agar dapat terhubung dengan AP.

Kita isikan:

- Address:192.168.100.2/24
- Interface:wlan1

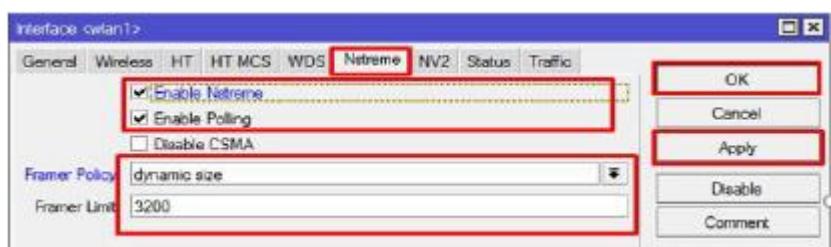


Dengan mengonfigurasi IP, maka antara AP dan Station sudah dapat terhubung, kemudian kita coba PING.

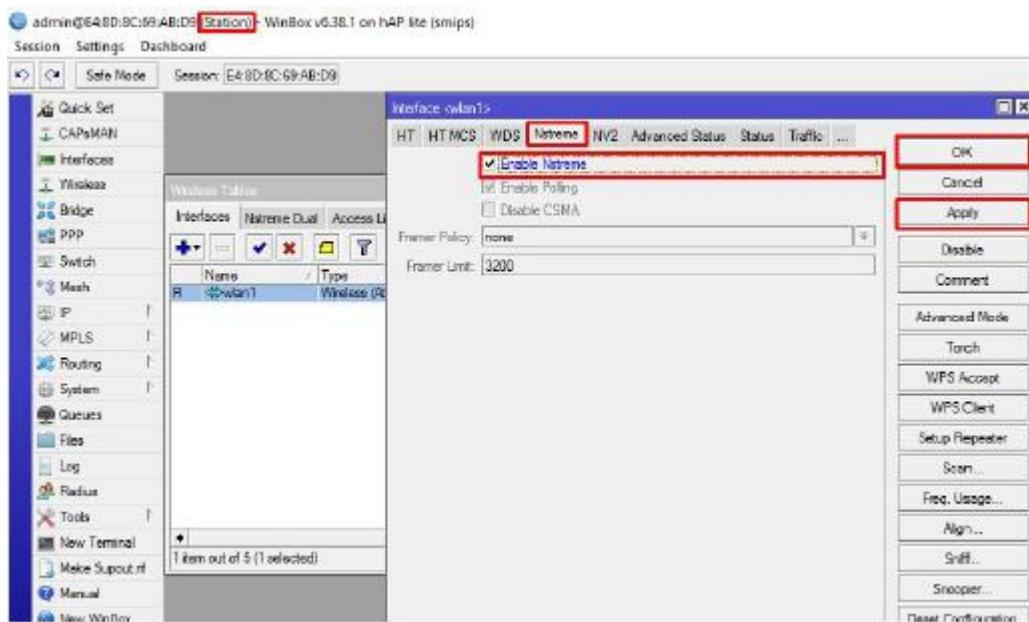


Jika kedua router sudah terhubung, kita tinggal mengaktifkan fitur Nstreme.

- Pada **Access Point**, kita klik menu ‘wireless>interface wlan’
- Lalu kita klik tab ‘Nstreme’ pada wireless settings.
- Kita centang:
  - Enable Nstreme, Enable Polling.
  - Kita isi:
    - Framer Policy: dynamic size
    - Framer limit: 3200
  - Jika sudah, ‘apply’ lalu ‘ok’



- Pada **Station**, klik menu ‘wireless>interface wlan’
- Pada tab Nstreme, kita centang
- Kemudian ‘apply’ lalu ‘ok’



# MAC ADDRESS FILTERING

Apa Mac Address Filtering?

Fungsinya untuk menyaring Mac Address yang dapat terhubung/terkoneksi dengan router kita. Contohnya, ada dua buah atau bahkan lebih access point yang memiliki SSID yang sama, sementara itu, bagaimana caranya station yang menjadi penerima bisa terkoneksi dengan access point yang dituju sementara banyak access point ber SSID sama?

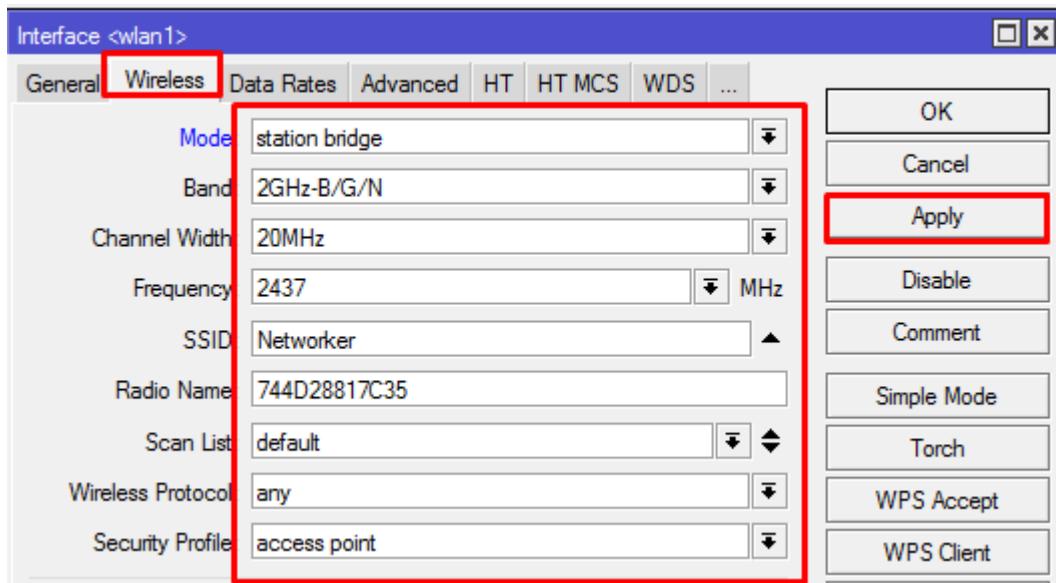
Caranya dengan menggunakan **Mac Address Filtering**.

Beginilah caranya:

Mula-mula kita perlu mengonfigurasi router yang menjadi access point.

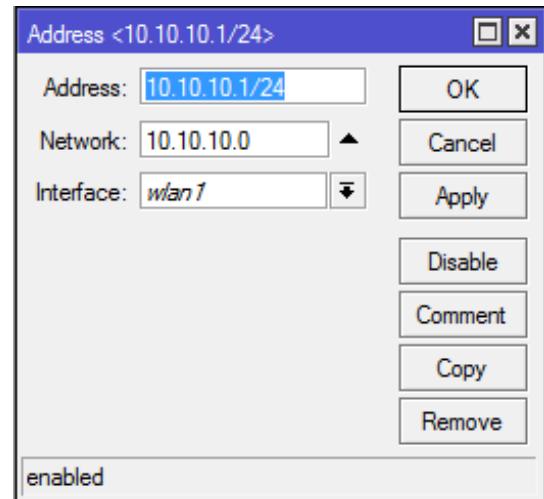
- Seperti biasanya kita perlu mengonfigurasi interface wireless:
  - Mode: AP Bridge
  - Band, Channel, dan Frekuensi: menyesuaikan antara AP dan Station
  - SSID: Networker

- Jika sudah ‘apply’ lalu ‘ok’



Kemudian kita buat IP Address untuk interface wireless. Isikan:

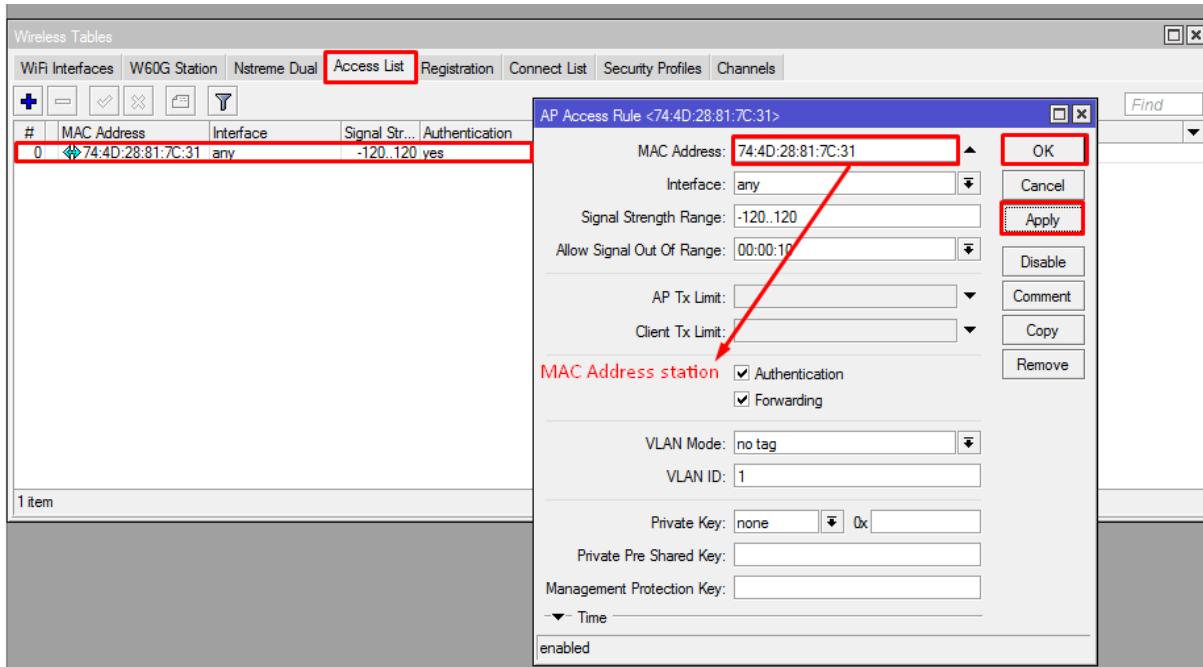
- IP Address: 10.10.10.1/24
- Interface: wlan1
- Kemudian ‘apply’ lalu ‘ok’



Kemudian kita masukkan MAC-address station pada **Access List**, yang berfungsi sebagai penyaringan autentikasi untuk sebuah AP terhadap client yang akan terkoneksi. Caranya:

- Klik ‘Access List’ pada menu wireless, kemudian kita add ‘+’
- Kita isikan:

- MAC Address: (isikan MAC Address station) contoh:  
74:4D:28:81:7C:31



- Interface: wlan1 (karena disini kita menggunakan wlan1)
- Jika sudah 'apply' lalu 'ok'

Selanjutnya kita mengkonfigurasi router yang menjadi station.

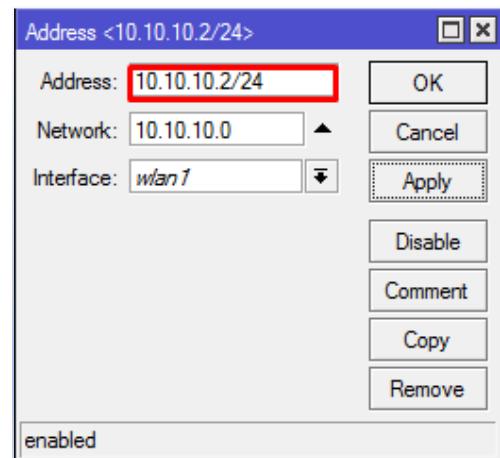
- Pertama-tama kita setting interface wireless, kita isikan:
  - Mode: Station Bridge
  - Band, Channel, dan Frekuensi: menyesuaikan antara AP dan Station
  - SSID: Adib-AP

- Jika sudah ‘apply’ lalu ‘ok’

Kemudian kita buat IP Address untuk interface wlan. Isikan:

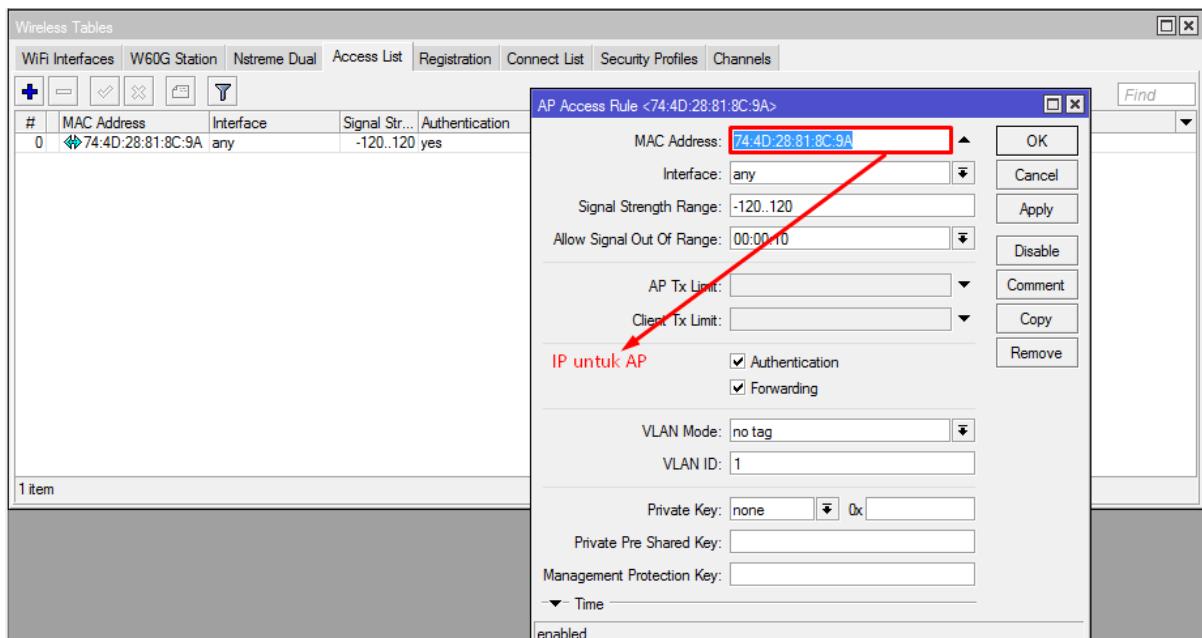
- IP Address: 10.10.10.2/24
- Interface: wlan1

Pastikan IP Address antara AP dan Station satu network.



Lalu kita harus memasukkan MAC-address AP di Access List yang berfungsi agar station langsung bisa terkoneksi ke AP. Caranya:

- Klik ‘Access List’ pada menu wireless, kemudian kita add ‘+’
- Kita isikan:
  - MAC Address: (isikan MAC Address AP) contoh 74:4D:28:81:8C:9A
  - Interface: wlan1 (karena disini kita menggunakan wlan1)
  - Jika sudah ‘apply’ lalu ‘ok’



Jika sudah, maka kedua router sudah terhubung meskipun banyak AP lain yang SSID nya sama.

# WIRELESS BRIDGE

Sebelum kita memasuki lab, saya akan memberikan penjelasan singkat tentang bridge.

Apa itu bridge?

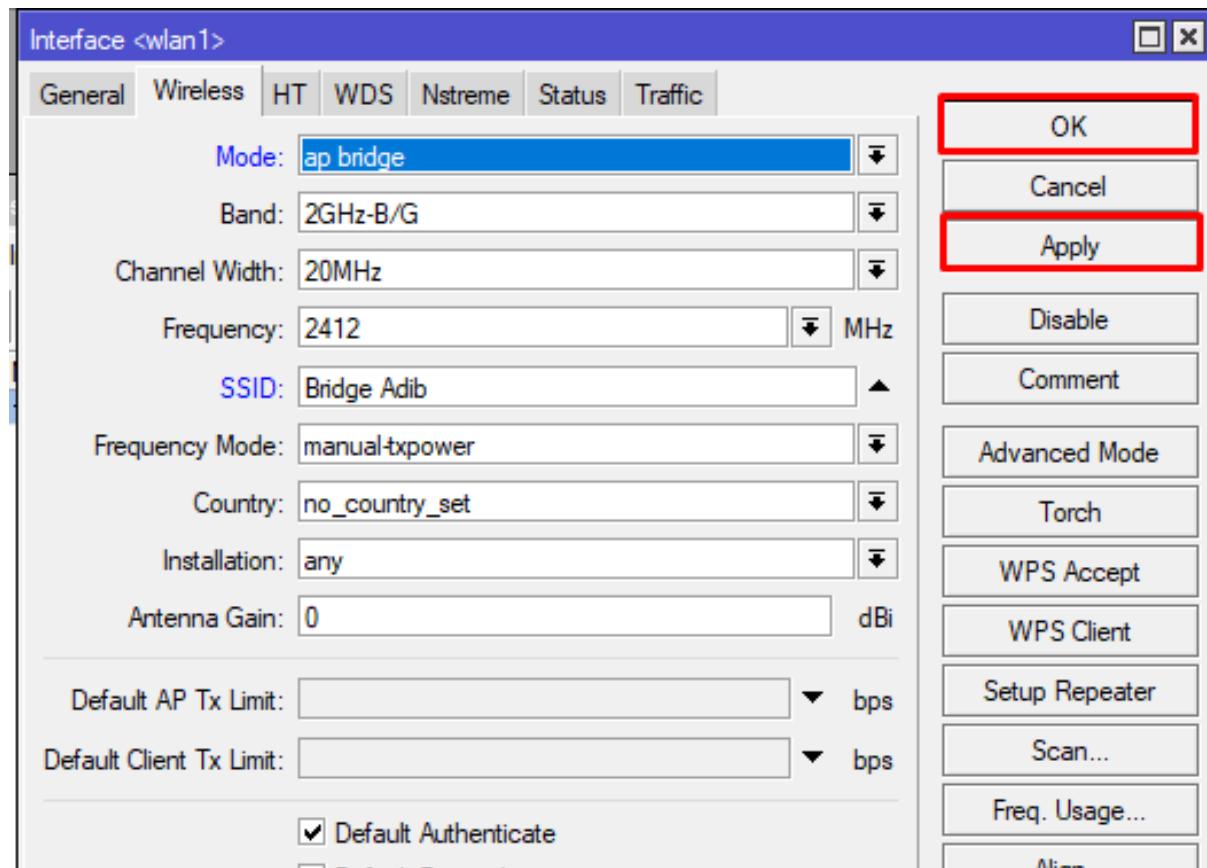
- Menggabungkan 2 atau lebih interface seolah-olah berada dalam 1 segmen network yang sama.
- Bridge juga dapat berjalan pada jaringan wireless.
- Proses bridge berjalan pada layer data link (layer 2).
- Interface bridge adalah interface virtual, dimana kita dapat membuat sebanyak yang kita inginkan.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

Meskipun begitu, Bridge juga memiliki kelemahan, yaitu:

- Sulit untuk mengatur trafik broadcast (misalnya akibat virus,dll) Permasalahan pada satu port/segmen akan membuat masalah di port/segmen pada bridge yang sama
- Peningkatan beban trafik akibat terjadinya akumulasi traffic broadcast

Beginilah caranya membuat wireless bridge:

Kita memerlukan 1 Router yang menjadi Access Point

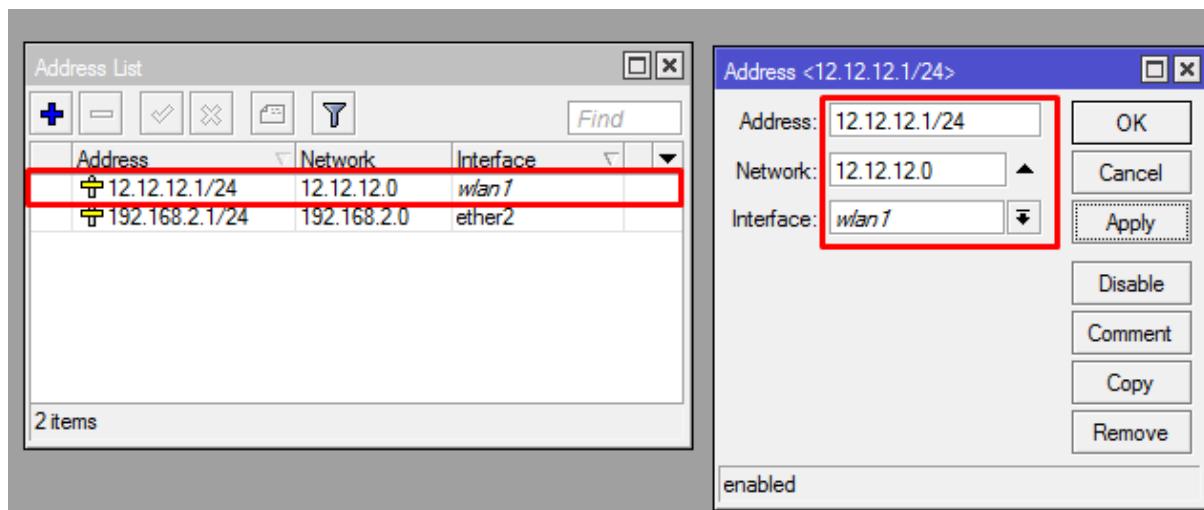


Isikan:

- Mode: AP Bridge
- Band, Channel, dan Frekuensi: menyesuaikan antara AP dan Station
- SSID: (bebas) Bridge Adib
- Jika sudah 'apply' lalu 'ok'

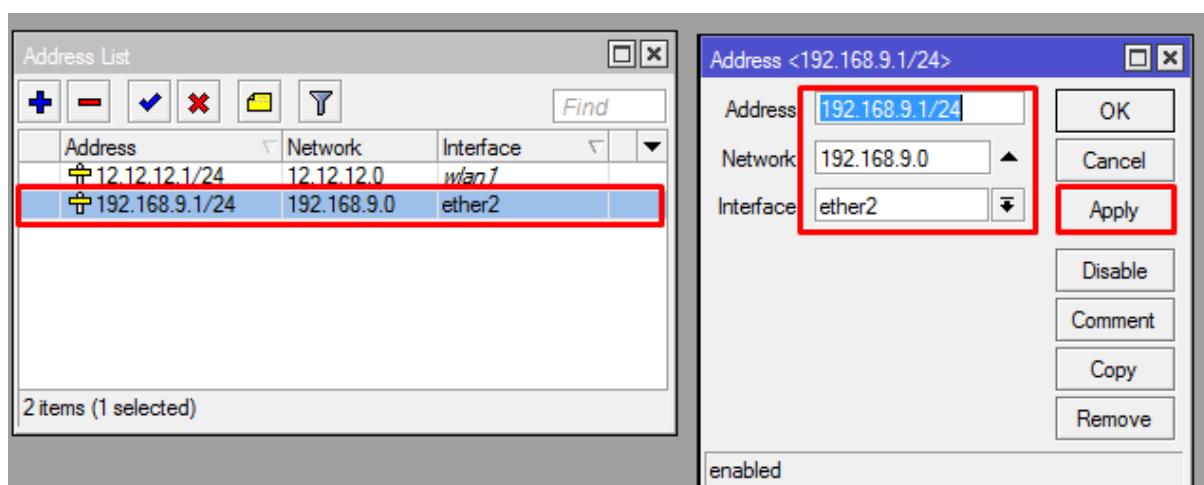
Langkah selanjutnya kita buat IP Address untuk interface wlan dan interface ether (LAN).

- Klik menu 'IP> Address> add '+. Isikan:
  - IP Address: 12.12.12.1/24
  - Interface: wlan1



Lalu buat IP Address lagi untuk interface LAN (ether)

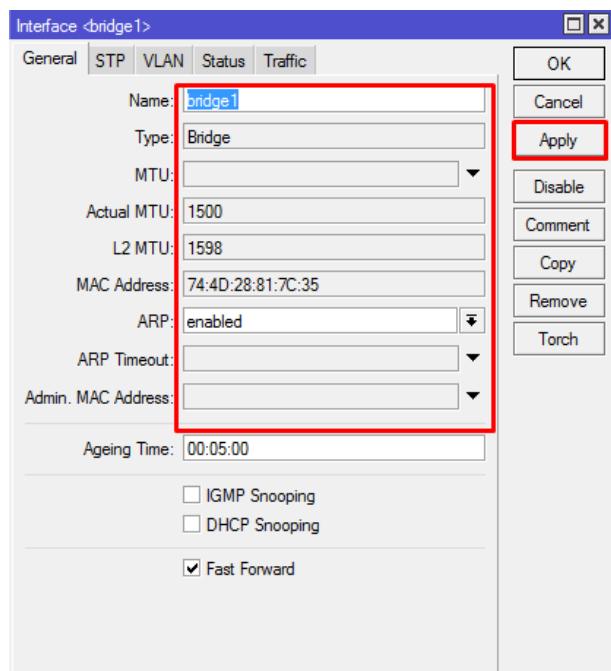
- Klik menu 'IP> Address> add '+. Isikan:
  - IP Address: 192.168.1.1/24
  - Interface: ether2 (LAN yang terkoneksi pada router)



Jika sudah, kita harus mengonfigurasi IP Address pada PC kita agar bisa terhubung ke router. IP: 192.168.9.2/24 Gateway: 192.168.9.1

Jika sudah, kita buat bridge agar kedua interface tersebut bisa terhubung

- Pertama-tama klik menu 'bridge' kemudian kita add '+'
- Kita isi: name: (bebas)
- Kemudian 'apply' lalu 'ok'



Kemudian kita masukkan interface wlan dan interface LAN (ether) kedalam bridge port.

- Bridge>Port>add '+'
- Isi:
- Interface: wlan1
- Bridge: bridge1



buat new port lagi, isi:

- Interface: ether2
- Bridge: bridge1



Jika langkahnya tadi sudah, maka PC sudah bisa terhubung ke Access Point karena jaringannya sudah menjadi satu segmen karena bridge tadi. Kita dapat mengetesnya dengan melakukan ping.

# **WDS (WIRELESS DISTRIBUTION SYSTEM)**

Di era modern kebutuhan akan koneksi internet hampir bisa dikatakan kebutuhan yang penting. Banyak perusahaan atau instansi pendidikan kemudian mencoba memberikan akses internet di area terbuka sehingga pengguna bisa jauh lebih nyaman. Kasus yang muncul adalah dengan kebutuhan cover area yang luas seperti sekolah, kampus atau area terbuka, terkadang tidak dapat dijangkau dengan satu perangkat wireless. Terlebih user wireless yang bersifat mobile atau berpindah - pindah. MikroTik memberikan solusi kebutuhan roaming wireless dengan fitur WDS.

Apa itu WDS?

WDS (Wireless Distribution System) adalah sistem yang memungkinkan interkoneksi antar Access point (AP). Sistem ini digunakan untuk memperluas jangkauan area wireless, dengan menggunakan beberapa perangkat AP Untuk Menjadi satu, tanpa membangun backbone jaringan atau WDS itu bisa di fungsikan sebagai Repeater yang berfungsi untuk memperluas jangkauan sinyal sebuah jaringan wireless.

WDS sendiri ada dua, WDS Dynamic yang bisa kita konfigurasikan secara otomatis dan WDS Static yang perlu kita konfigurasikan satu-persatu, memang secara konfigurasi sedikit lebih rumit, namun koneksi tidak mudah berganti - ganti jika signal turun.

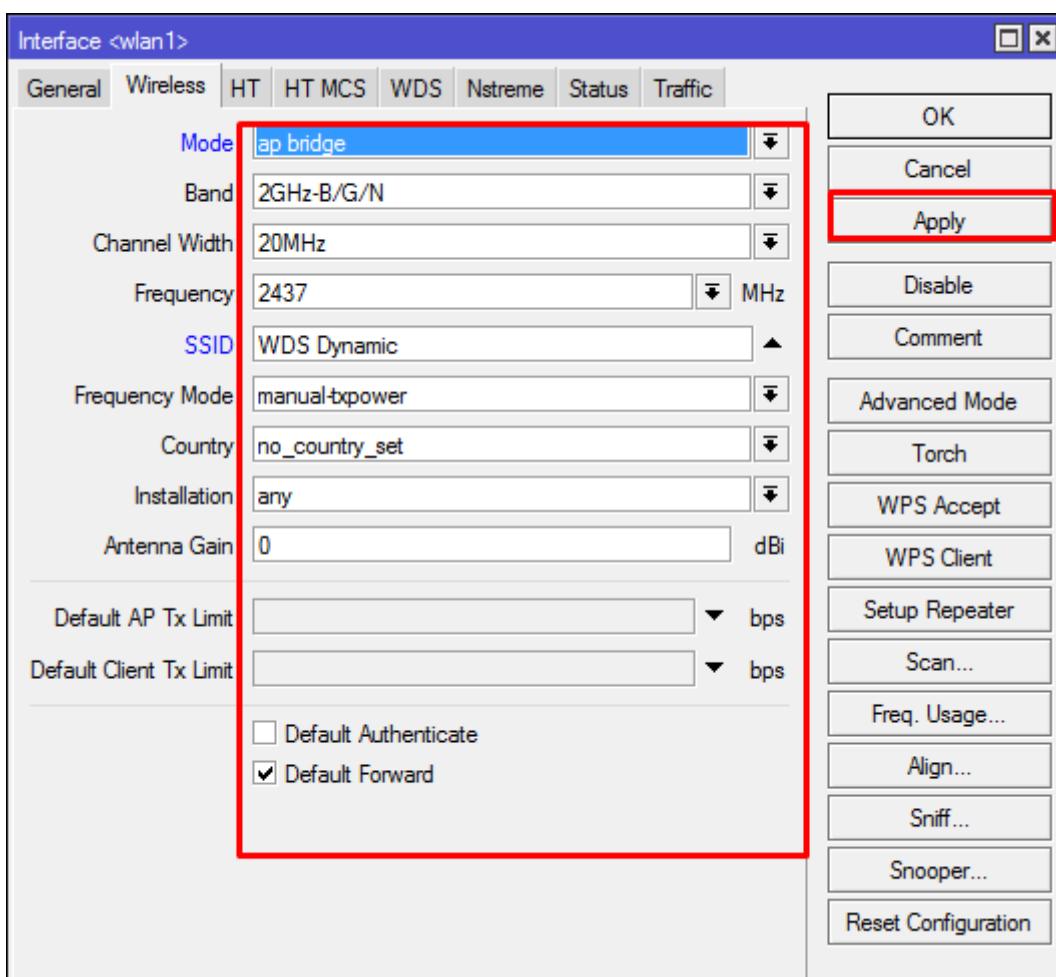


# WDS DYNAMIC

Setelah membaca penjelasan tentang WDS tadi, kita akan mencoba membuat WDS tersebut, kita mulai dari WDS Dynamic.

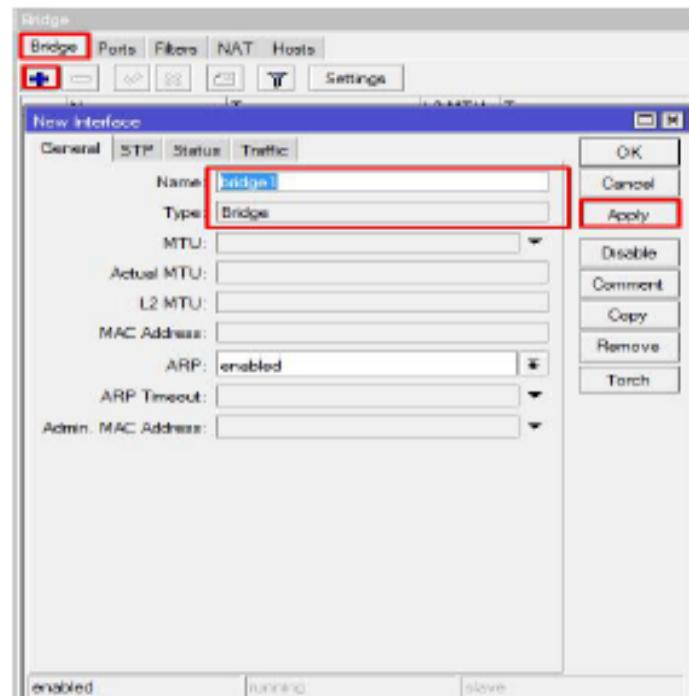
Pertama-tama kita perlu mengonfigurasi router yang menjadi Access Point. Seperti biasa kita harus mengonfig interface wirelessnya. Isikan:

- Mode: AP Bridge
- Band, Channel, Frekuensi: Menyesuaikan antara AP dan Station
- SSID: WDS Dynamic
- Jika sudah ‘apply’ lalu ‘ok’



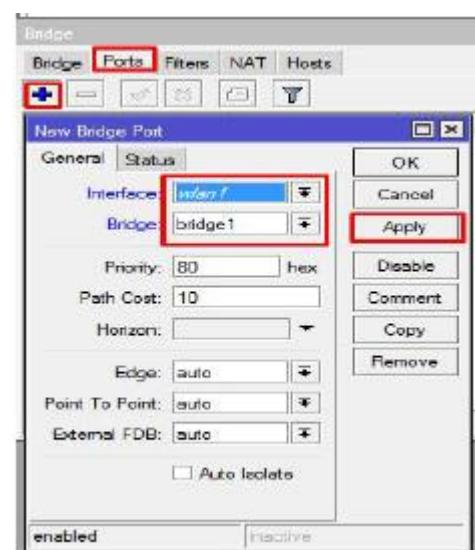
Selanjutnya, kita memerlukan bridge antara AP dan Station agar WDS nya dapat terhubung.

- Klik menu ‘bridge’ kemudian kita add ‘+’ bridge baru
- Isikan, name: bebas/bisa memilih default (bridge1)
- Jika sudah ‘apply’ lalu ‘ok’



Selanjutnya, kita tambahkan port interface wireless kedalam bridge tadi.

- Klik tab ‘port’ pada menu bridge
- Lalu kita add ‘+’
- Isi:
  - Interface: wlan1
  - Bridge: bridge1
- Lalu ‘apply’ kemudian ‘ok’



Terakhir, kita perlu mengonfigurasi WDS Dynamic pada menu wireless.

- Klik interface wireless. (wlan1)
- Lalu kita klik tab ‘WDS’ kemudian isikan:

- WDS Mode:

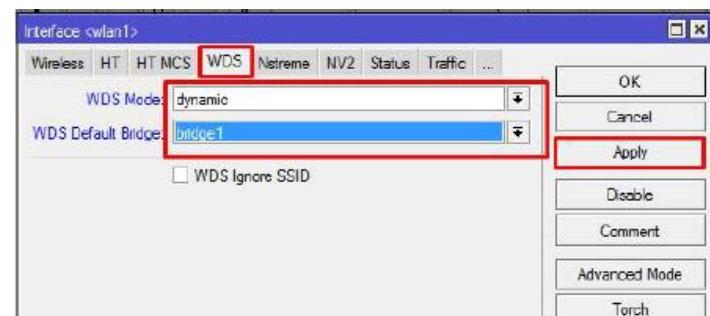
Dynamic

- WDS Default Bridge:

Bridge: Bridge1 (bridge yang kita buat tadi)

- Jika sudah ‘apply’

lalu ‘ok’



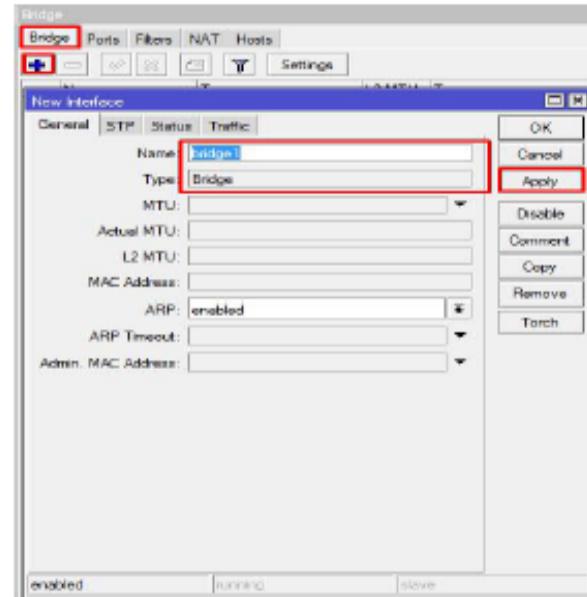
Kemudian kita perlu mengonfigurasi router yang menjadi station.

Pada tab wireless di wireless interface, kita isikan:

- Mode: Station WDS
- Band, Frekuensi, Channel: sesuaikan dengan AP
- SSID: WDS Dynamic (sama dengan AP)
- Jika sudah ‘apply’ lalu ‘ok’

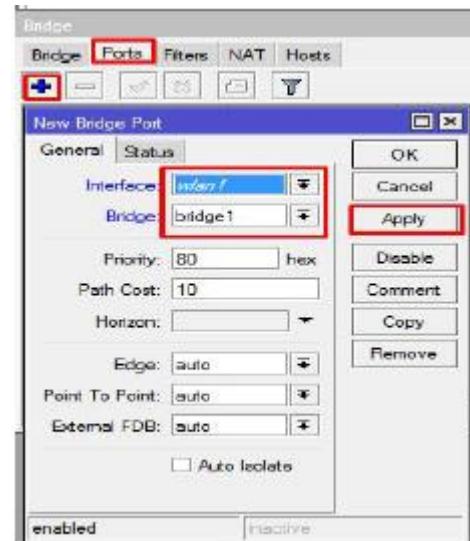
Jika sudah, konfigurasi selanjutnya kita buat interface bridge.

- Klik menu ‘bridge’ kemudian kita add ‘+’ bridge baru
- Isikan, name: bebas/bisa memilih default (bridge1)
- Jika sudah ‘apply’ lalu ‘ok’



Selanjutnya, kita tambahkan port interface wireless kedalam bridge tadi.

- Klik tab ‘port’ pada menu bridge
- Lalu kita add ‘+’
- Isi:
  - Interface: wlan1
  - Bridge: bridge1
- Lalu ‘apply’ kemudian ‘ok’



Selanjutnya kita konfigurasi WDS pada station agar aktif, caranya:

- Klik interface wireless. (wlan1)
- Lalu kita klik tab ‘WDS’ kemudian isikan:

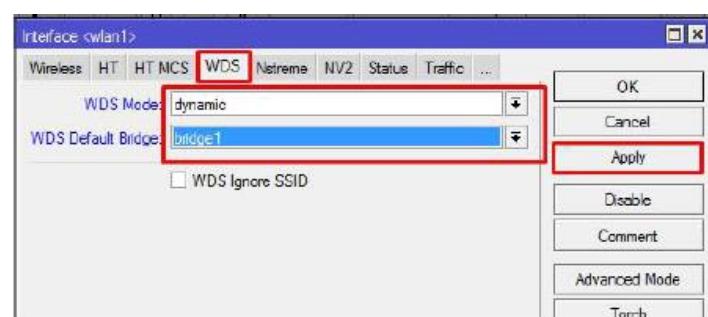
- WDS Mode:

Dynamic

- WDS Default Bridge:

Bridge: Bridge1 (bridge yang kita buat tadi)

- Jika sudah ‘apply’ lalu ‘ok’



Jika sudah kita buat maka WDS antara 2 router akan aktif dengan status wlan1 **RS** (Running, Slave)

dan status WDSnya **DRS** (Dynamic, Running, Slave)

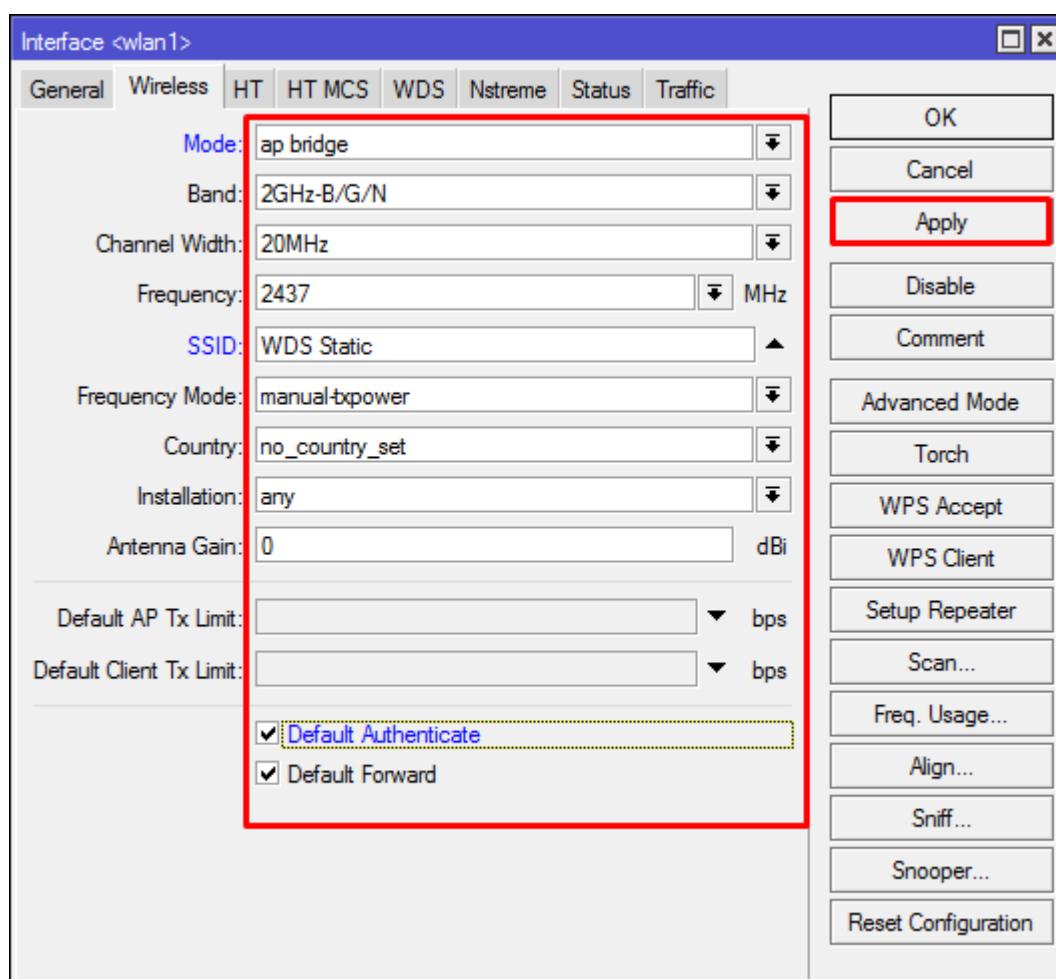
Name	Type	Actual NTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
RS - wlan1	Wireless (Atheros AR9)	1500	0 bps	0 bps	0	0
DRS - hwdsl6	WDS	1500	0 bps	0 bps	0	0

# WDS STATIC

Jika sebelumnya kita mengonfigurasi WDS secara Dynamic atau Otomatis, maka sekarang kita akan mengonfigurasi secara manual.

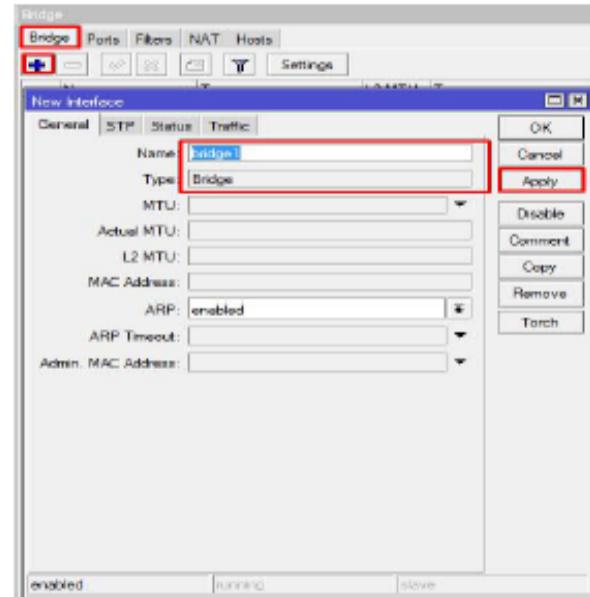
Pertama-tama kita konfigurasi interface wireless pada router yang menjadi Access Point. Kita isikan pada wireless menu:

- Mode: AP Bridge
- SSID: WDS Static (nama bebas, hanya untuk memudahkan)
- Band, Channel, Frekuensi: menyesuaikan antara AP dan Station
- Jika sudah ‘apply’ lalu ‘ok’



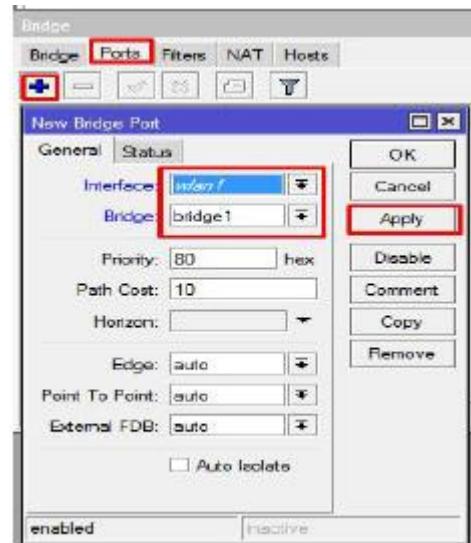
Jika sudah konfigurasi selanjutnya kita buat interface bridge.

- Klik menu ‘bridge’ kemudian kita add ‘+’ bridge baru
- Isikan, name: bebas/bisa memilih default (bridge1)
- Jika sudah ‘apply’ lalu ‘ok’

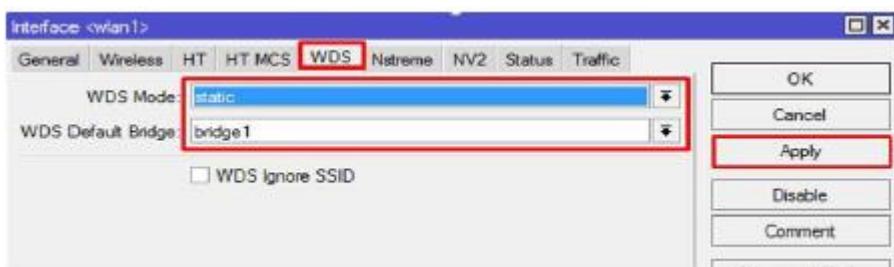


Selanjutnya, kita tambahkan port interface wireless kedalam bridge tadi.

- Klik tab ‘port’ pada menu bridge
- Lalu kita add ‘+’
- Isi:
  - Interface: wlan1
  - Bridge: bridge1
- Lalu ‘apply’ kemudian ‘ok’



Kemudian kita konfig WDS di Access Point dengan WDS Static, isi:



- WDS Mode: Static
- WDS Default Bridge: bridge1

Kemudian kita buat interface WDS-nya secara manual karena kita menggunakan WDS static.

- Klik menu ‘wireless> kita add ‘+’ interface> WDS

The 'Wireless Tables' window shows the following table:

		Actual M...	Tx	Rx	Tx Packet
Virtual	ess (Atheros AR9...)	1500	0 bps	0 bps	
WDS		1500	0 bps	0 bps	
Nstreme Dual					

- Kita isikan:
- Master Interface: wlan1
- WDS Address: 74:4D:28:81:7C:31 (Mac Address Station)
- Jika sudah ‘apply’ lalu ‘ok’

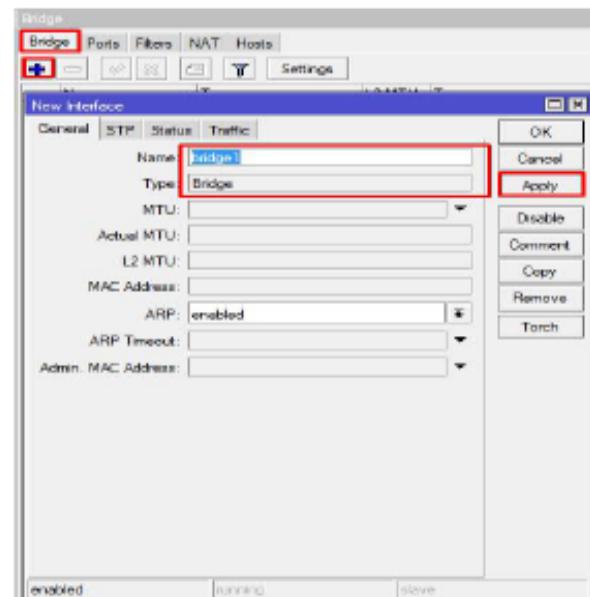
Konfigurasi WDS di AP sudah selesai, selanjutnya kita pindah konfigurasi ke Station.

Pertama-tama kita konfigurasi interface wireless pada Station, kita isi:

- Mode: Station WDS
- Band, Frekuensi, Channel: Sesuaikan dengan AP
- SSID: WDS Static (samakan dengan AP, agar lebih mudah)
- Jika sudah 'apply' lalu 'ok'

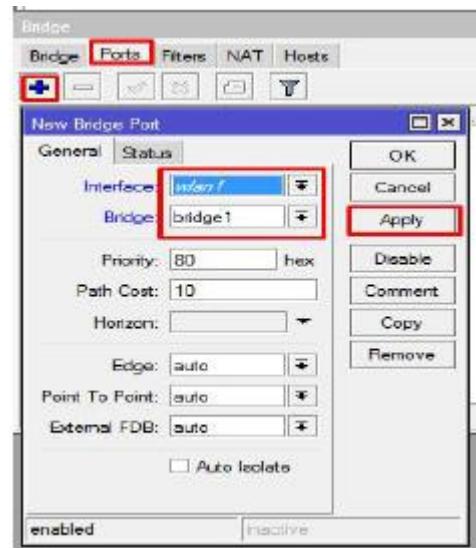
Jika sudah, konfigurasi selanjutnya kita buat interface bridge.

- Klik menu 'bridge' kemudian kita add '+' bridge baru
- Isikan, name: bebas/bisa memilih default (bridge1)
- Jika sudah 'apply' lalu 'ok'



Selanjutnya, kita tambahkan port interface wireless kedalam bridge tadi.

- Klik tab ‘port’ pada menu bridge
- Lalu kita add ‘+’
- Isi:
  - Interface: wlan1
  - Bridge: bridge1
- Lalu ‘apply’ kemudian ‘ok’



Jika bridge sudah kita buat, maka fungsi WDS antara Access Point dan Station akan bekerja, ditandai dengan status **RS** (Running, Slave) pada interface wlan1. Dan status **RSA** (Running, Static, Active) pada interface WDS.

The screenshot shows the 'Wireless Tables' interface with the 'Interfaces' tab selected. The table displays the following information:

Name	Type	Actual MTU	Tx	Px	Tx Packet (p/s)	Rx Packet (p/s)
RS wlan1	Wireless /Atheros AR9..	1500	848 bps	0 bps	2	0
RSA wds1	WDS	1500	424 bps	0 bps	1	0

A red arrow points from a label 'Status di AP' to the wlan1 row in the table.

# WIRELESS REPEATER

Pada sesi kali ini, kita akan memfungsikan router kita sebagai repeater,

Apa itu repeater?

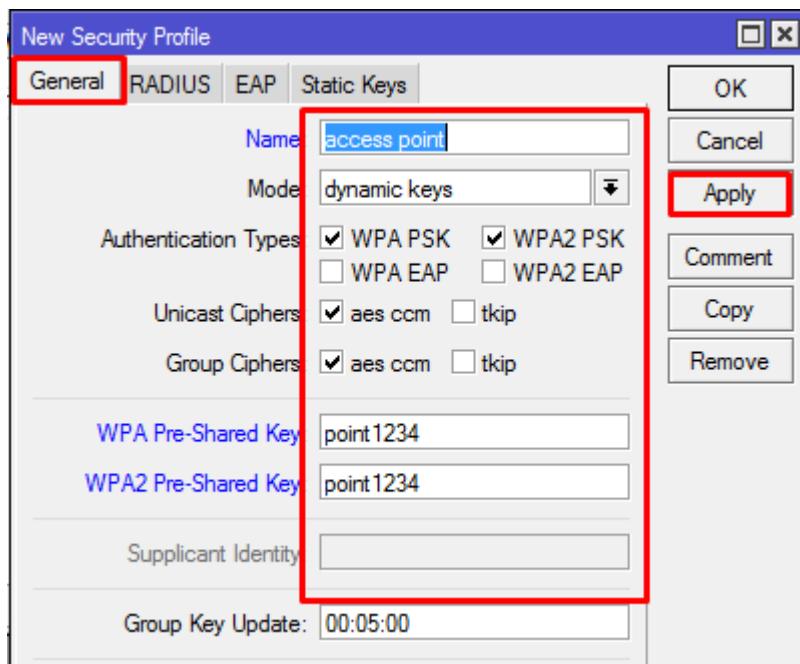
Repeater merupakan sebuah perangkat jaringan yang berfungsi untuk menguatkan, kemudian menyebarkan ulang sinyal sehingga daerah jangkauannya semakin besar.

Secara umum, fungsinya memang sangat mirip dengan WDS. Fitur Wireless Repeater ini baru dikenalkan pada MUM di eropa tahun 2016. Dan hanya router dengan RouterOS versi 6.35 yang dapat mengaksesnya. Bedanya dengan WDS adalah dalam hal konfigurasi. Wireless Repeater memang lebih mudah, sementara WDS lumayan susah.

Beginilah caranya:

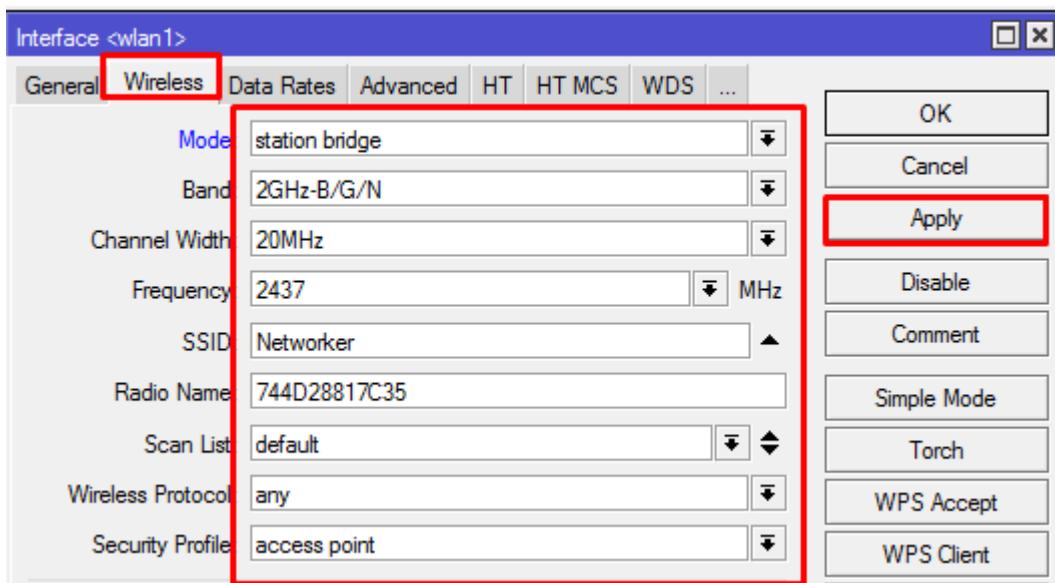
Kita gunakan 2 router, yang pertama menjadi AP dan yang kedua menjadi Repeater.

Pertama-tama, kita akan menambahkan password pada AP, kita buat di menu 'security profiles' pada wireless.



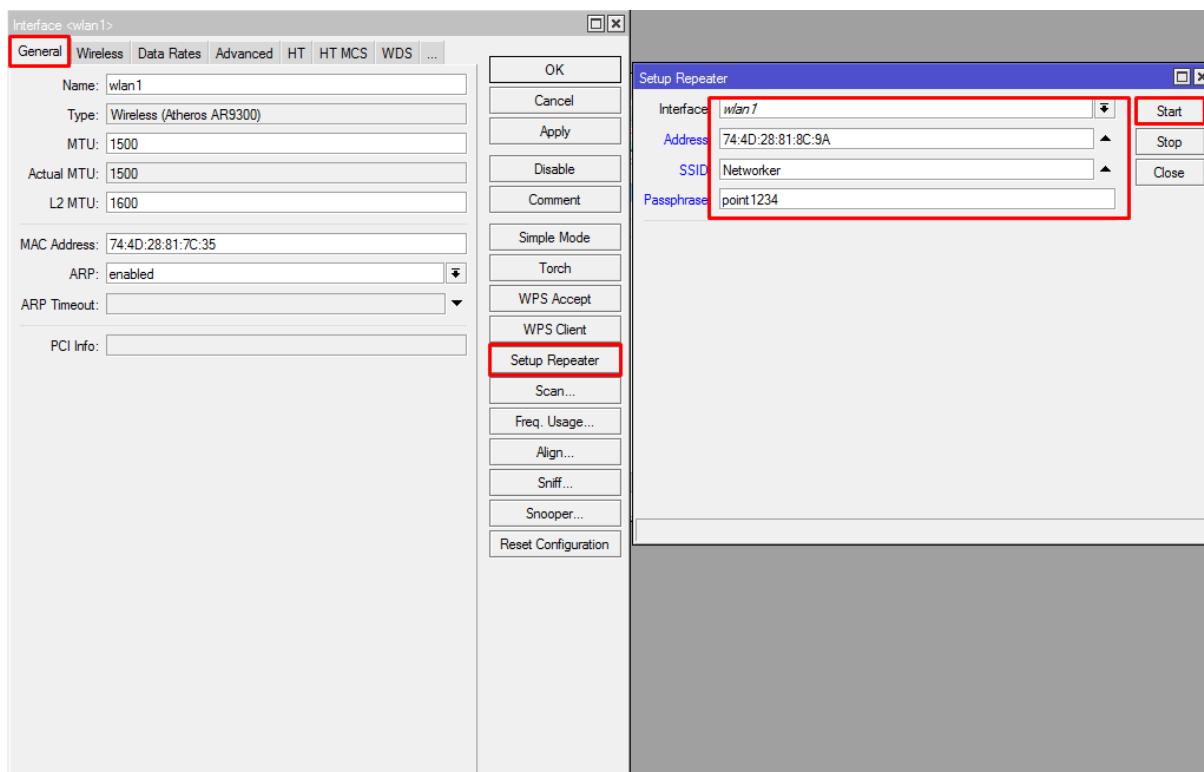
Lalu seperti biasanya kita perlu mengonfigurasi interface wireless, isikan:

- Mode: AP Bridge
- Band, Channel, dan Frekuensi: menyesuaikan antara AP dan Station
- SSID: Networker
- Security Profile: access point (masukkan security profile tadi)
- Jika sudah ‘apply’ lalu ‘ok’



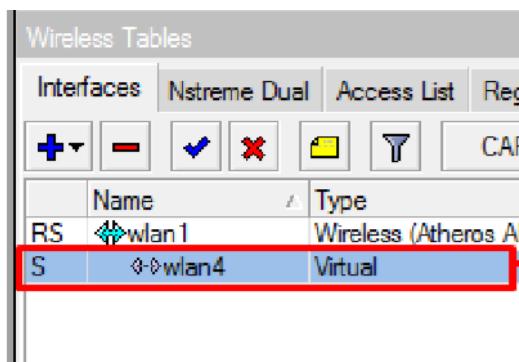
Selanjutnya kita konfigurasi router yang menjadi Station agar bisa menjadi Repeater.

- Kita masuk ke interface wlan, kemudian klik ‘setup repeater’
- Isikan:
  - Interface: wlan1



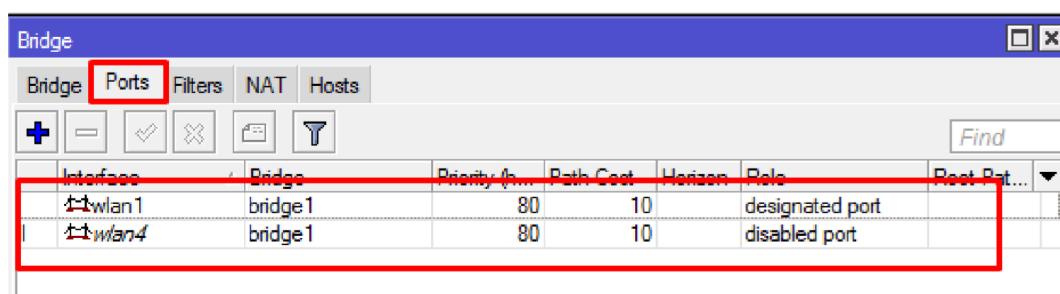
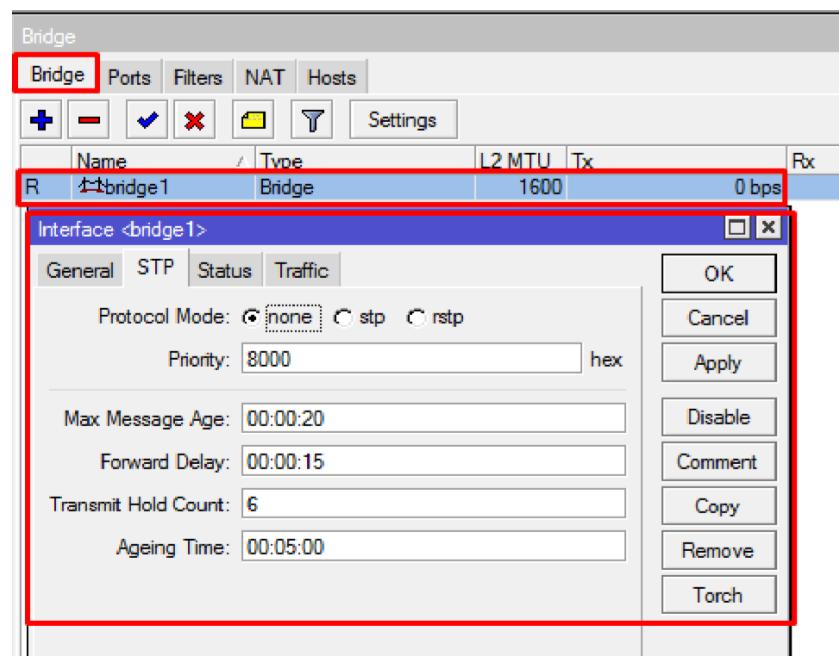
- Address: 74:4D:28:81:8C:9A (MAC Address AP)
- SSID: Networker
- Passphrase: point1234 (Password AP yang tadi kita buat di security profiles)
- Jika sudah klik ‘start’

Jika langkah-langkah tadi sudah selesai, maka Station berhasil menjadi repeater.



Setelah berhasil, di station akan terbentuk Virtual Access Point.

Juga secara otomatis akan terbentuk bridge dan portnya



## Catatan:



# PENGENALAN QOS

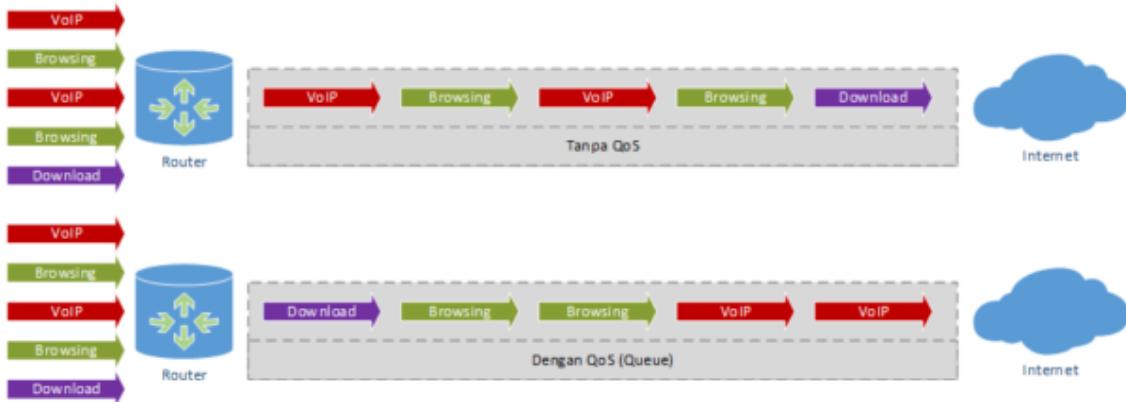
Apa itu QoS?

QoS merupakan singkatan dari **Quality of Service** atau dalam Bahasa Indonesia diartikan sebagai **Kualitas Layanan**.

QoS digunakan untuk menjaga layanan jaringan tetap pada batas minimalnya, contohnya, ketika banyak klien yang menggunakan layanan jaringan yang menyebabkan traffic penuh dan menyebabkan penurunan pada kualitas layanan jaringan.

Oleh sebab itu perlu ada pengaturan untuk menjamin bahwa layanan tetap bisa berjalan dengan optimal. QoS tidak selalu berarti pembatasan bandwidth sebuah komputer. QoS juga bisa digunakan untuk mengatur prioritas berdasarkan parameter-parameter yang diberikan dan menghindari terjadinya monopoli sebuah traffic terhadap seluruh bandwidth yang tersedia.

Ketika tanpa menggunakan QoS, sebuah traffic akan secara acak memenuhi/menggunakan bandwidth yang tersedia. Akibatnya, beberapa aplikasi yang membutuhkan data lebih cepat tidak terpenuhi dengan semestinya. Pada kasus traffic VoIP, akan terjadi delay yang lumayan lama yang dapat menyebabkan terganggunya komunikasi antara dua orang yang menggunakan layanan tersebut.



Ilustrasi Penggunaan QoS

Dengan menggunakan QoS, sebuah traffic akan disusun berdasarkan skala prioritas dalam sebuah sistem antrian atau biasa disebut Queue. dengan adanya sistem prioritas, traffic yang mempunyai prioritas lebih tinggi akan diproses oleh router terlebih dahulu, dibandingkan traffic dengan prioritas yang lebih kecil. Pada kasus traffic VoIP misalnya, traffic tersebut akan diproses terlebih dahulu oleh router agar proses komunikasi dapat tetap nyaman antara kedua orang yang menggunakan layanan tersebut. Selain itu dengan menggunakan QoS, sebuah traffic dapat dibatasi penggunaan bandwidth-nya.

Dalam MikroTik RouterOS terdapat beberapa jenis QoS yang dapat digunakan. Masing-masing jenis QoS mempunyai mekanisme sendiri sendiri, berikut adalah macam-macam jenis QoS dalam MikroTik RouterOS.

## 1. Simple Queue

Pembatasan trafik tidak dapat dilakukan pada suatu interface. Satu-satunya cara untuk mengontrol adalah dengan buffering (menahan sementara). Selain itu jika paket yang berada dalam buffer telah melampaui limit buffer, akan dilakukan drop pada paket tersebut. Pada paket TCP, cara ini cukup efektif karena paket yang didrop akan dikirimkan ulang. Sehingga tidak ada kehilangan paket data. Cara termudah melakukan queue di RouterOS adalah menggunakan simple queue. Dengan menggunakan simpel queue, sebuah traffic dapat dilimit tx-rate-nya (untuk upload), rx-rate-nya (untuk download) dan tx+rx-rate-nya (akumulasi).

## 2. Burst

Burst adalah salah satu cara menjalankan QoS yang 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. Perlu diingat bahwa burst time tidak sama dengan waktu yang diijinkan oleh router untuk melakukan burst. Dalam Burst dikenal beberapa istilah penting yaitu burst-limit & burst-threshold

### 3. Per Connection Queue

Untuk kondisi client yang sangat banyak dan sangat merepotkan jika harus membuat banyak rule maka bisa menggunakan metode PCQ. PCQ dibuat sebagai penyempurnaan dari metode SFQ. Kelebihan PCQ adalah bisa membatasi bandwith untuk masing-masing client secara merata. Namun PCQ mempunyai kekurangan yaitu PCQ membutuhkan memori yang cukup besar.

### 4. Queue Tree & Mangle

QueueTree adalah tool pada MikroTik RouterOS yang memiliki kemampuan untuk melimitasi bandwith yang lebih lengkap dibandingkan dengan simple-queue. Dengan QueueTree dimungkinkan untuk melakukan limitasi yang lebih fleksibel. Agar sebuah QueueTree dapat berjalan maka harus menggunakan Mangle yang diconfigurasikan terlebih dahulu.

Dalam bab ini, kita akan bahas satu-satu QoS yang ada di MikroTik

# **QUEUE LAB:**

**1.SIMPLE QUEUE**

**2.QUEUE BURST**

**3.PCQ (PER- CONNECTION QUEUE)**

**4.PCQ WITH RATE**

**5.QUEUE TREE**

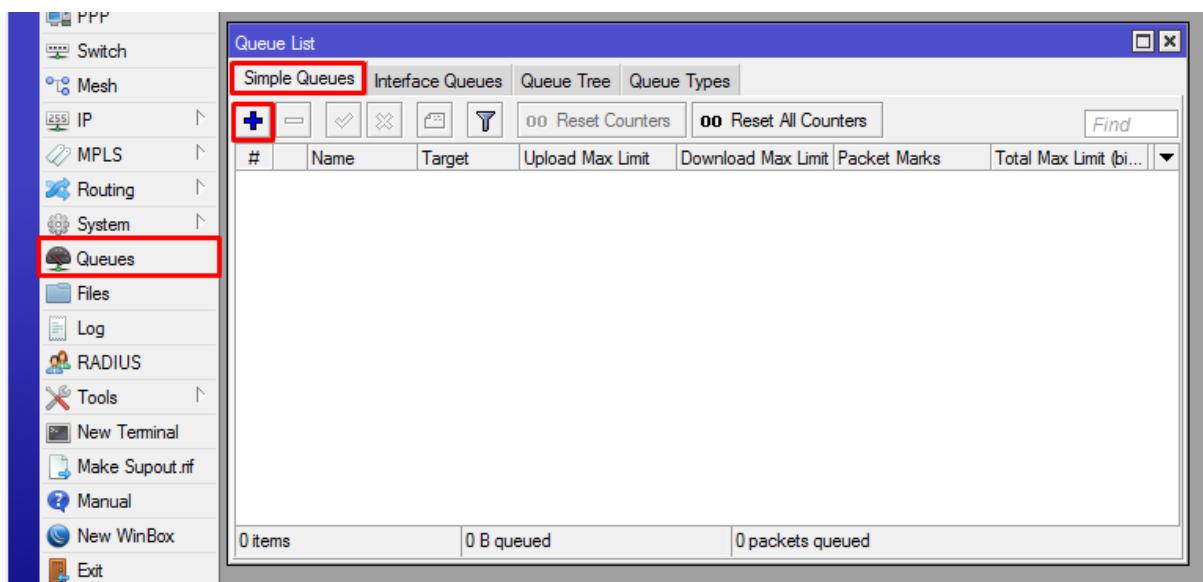
# SIMPLE QUEUE

Simple Queue singkatnya adalah queue yang melimitasi batas upload dan download klien secara sederhana dan berbasis pada IP Address.

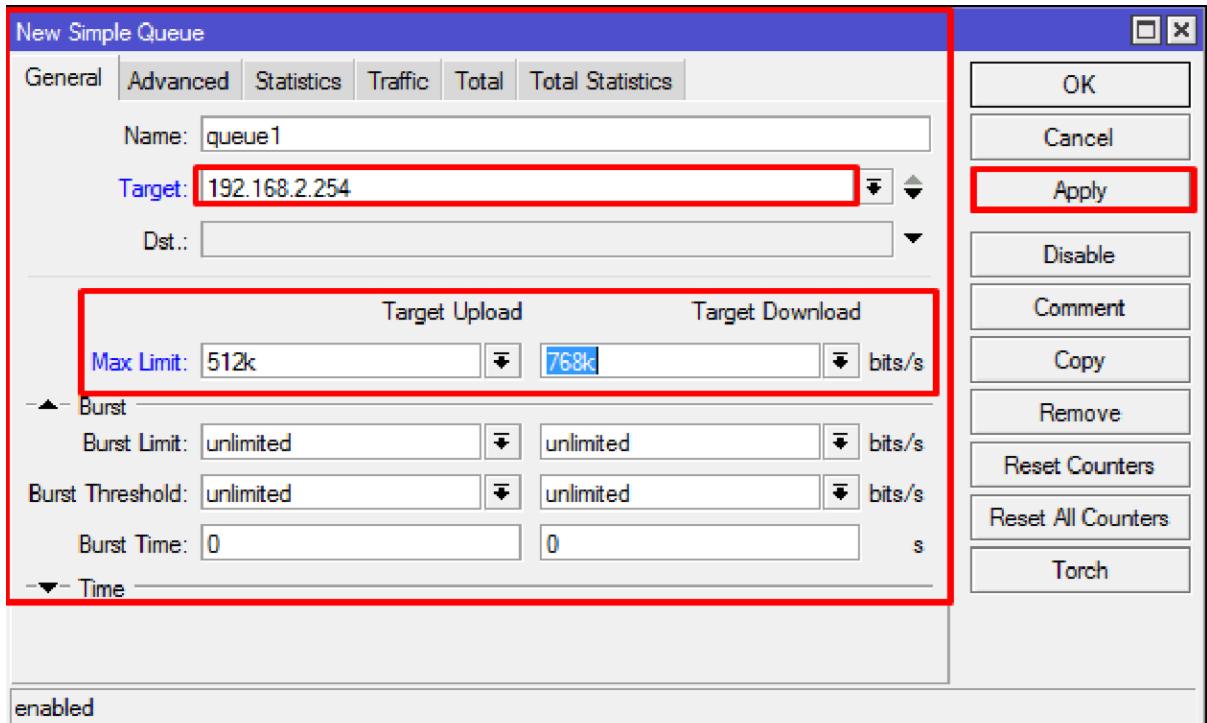
Beginilah caranya:

Pastikan terlebih dahulu router terhubung ke internet.

- Klik menu ‘queue’ lalu kita menuju tab ‘simple queue’ dan buatlah queue baru ‘+’



- Beginilah tab simple queue, disini kita isikan:

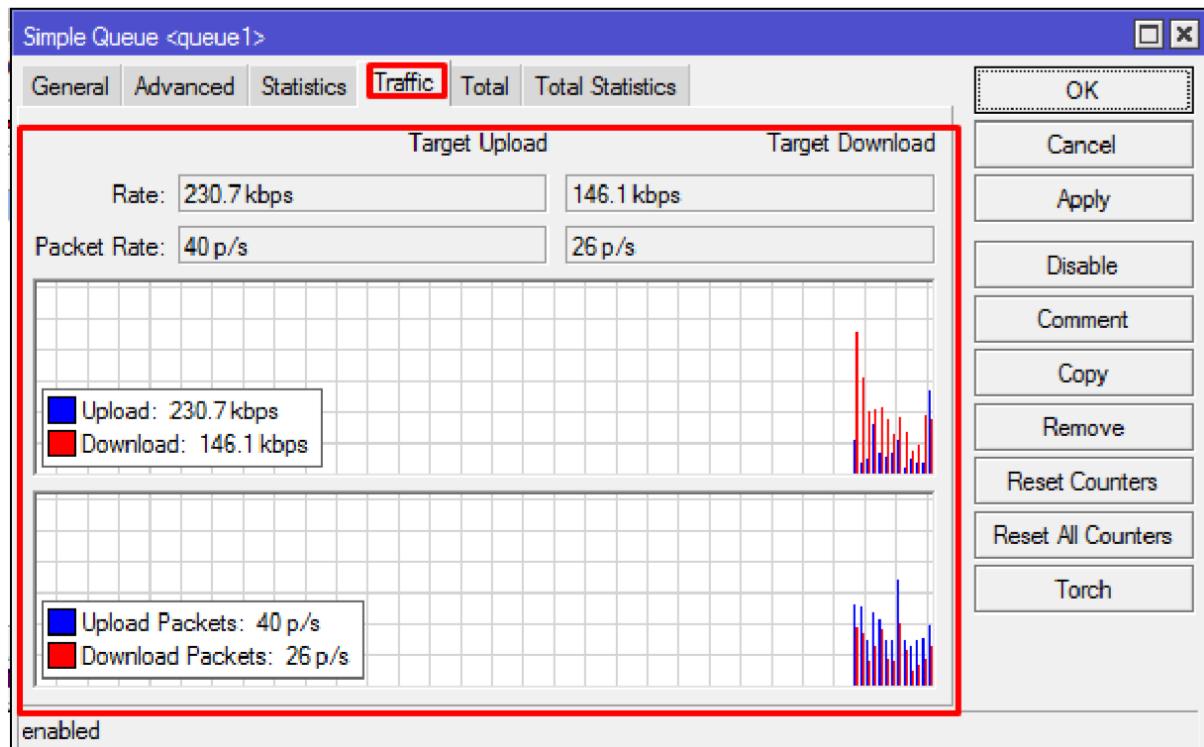


- Name: (bebas)
- Target: (IP Address Klien yang dituju)  
=192.168.2.254
- Max Limit: Batas maksimal pada **Target Upload** (batas upload) dan **Target Download** (batas download) pada klien. Misalkan kita isi:
  - Target Upload: 512k= yang berarti klien tidak dapat melakukan upload dengan kecepatan bandwith diatas 512 kb
  - Target Download: 768k= yan berarti klien tidak bisa melakukan download dengan kecepatan bandwith diatas 768 kb
- Jika sudah, 'apply' kemudian 'ok'

Queue List						
Simple Queues		Interface Queues	Queue Tree	Queue Types		
#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Max Lim
0	queue1	192.168.2.254	512k	768k		

Jika kita ingin melihat hasilnya, cobalah pada melakukan download/upload pada klien yang tadi kita targetkan. Pasti upload dan downloadnya tidak akan melebihi standar yang kita buat dengan queue tadi.

Lalu untuk melihat grafiknya bisa kita lihat di queue yang tadi kita buat pada tab traffic.



Disitu akan terlihat kecepatan bandwith klien. Kecepatannya tidak akan melebihi batas yang sudah ditentukan dengan simple queue.

# QUEUE BURST

Seperti yang sudah saya jelaskan diawal tentang queue burst, yaitu queue yang memungkinkan klien untuk menggunakan data-rate yang melebihi max-limit untuk periode waktu tertentu. Namun akan kita dalami lagi fitur-fitur dalam queue burst.

Ada 3 fitur dalam Queue Burst:

## 1. **Burst limit**

Nilai bandwidth maksimum yang akan diterima user apabila terjadi Burst. Nilai burst limit harus lebih besar dari Max-limit yang di berikan

## 2. **Burst Time**

Periode waktu yang digunakan untuk menghitung data rate. Burst time bukan menghitung lamanya burst.

## 3. **Burst Threshold**

Nilai ini menentukan kapan burst di jalankan dan kapan burst dihentikan.

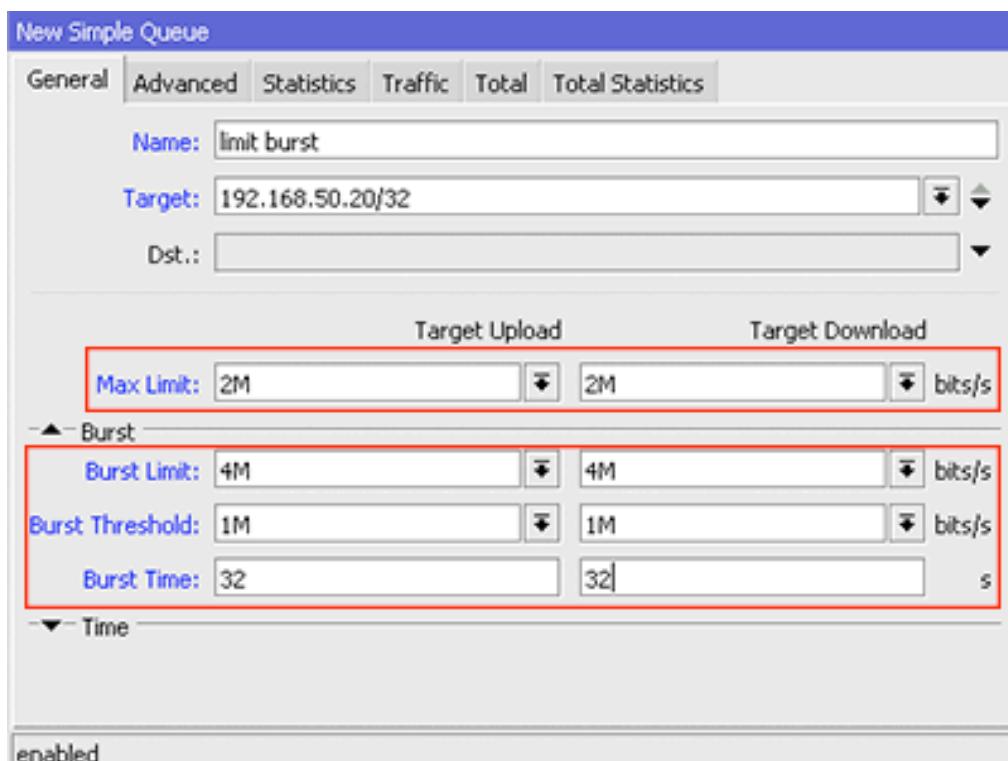
Ada juga rumus untuk menghitung lamanya user mendapatkan burst pada saat pertama kali menggunakan alokasi bandwidth :

$$\text{Lama Burst di jalankan} = (\text{burst-threshold} / \text{burst-limit}) \times \text{burst-time}$$

Beginilah cara konfigurasinya:

Pertama-tama kita pastikan terlebih dahulu router kita terhubung ke internet dan memiliki klien.

- Klik menu ‘queue’ dan tambahkan queue baru pada tab ‘simple queue’ lalu isikan:



- Name: (bebas)
- Target: 192.168.50.20/32 (IP Address klien)
- Max limit upload/download: 2M/2M
- Burst limit upload/download: 4M/4M
- Burst Threshold upload/download: 1M/1M
- Burst Time upload/download: 32s/32s
- Jika sudah klik ‘apply’ kemudian ‘ok’

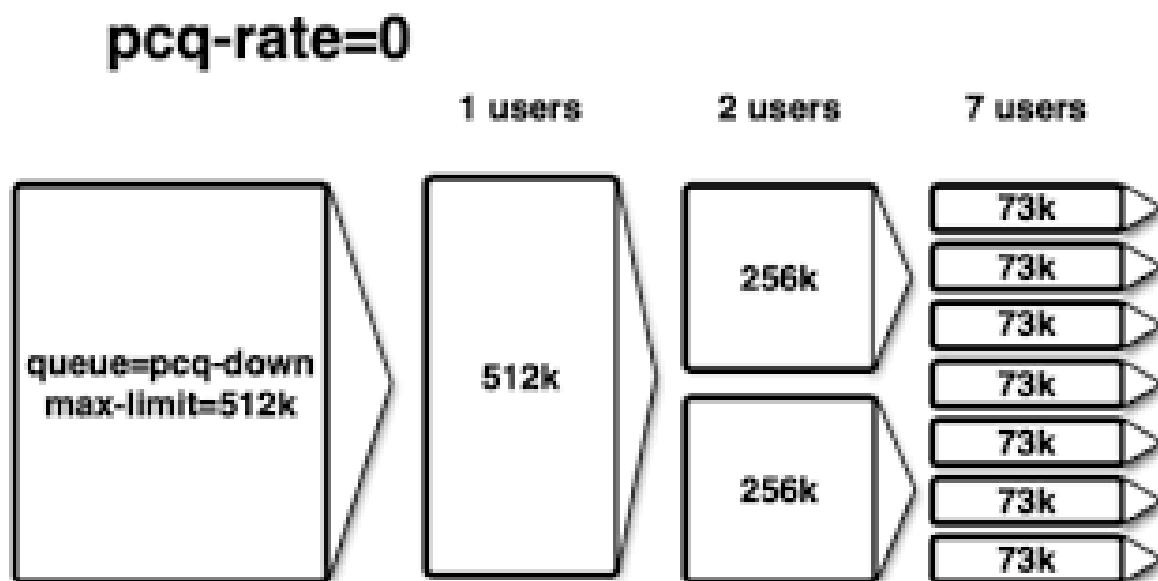
Semua konfigurasi diatas jika dijelaskan akan menjadi seperti ini:

Pertama-tama kita batasi upload/download klien sebesar 2Mb/2Mb lalu kemudian, pada waktu tertentu **burst** akan berjalan, selama **32 detik (burst time)** kecepatan upload/download akan mengalami kenaikan secara signifikan melebihi batas (2Mb) menjadi **4Mb download dan 4Mb upload**. **(burst limit)** kemudian jika waktu sudah 32 detik, maka secara otomatis kecepatan bandwidth akan menurun secara drastis hingga **1Mb upload dan 1Mb download (burst threshold)**. Lalu kemudian bandwidth akan normal kembali menjadi 2Mb upload dan 2Mb download, setelah beberapa saat akan terjadi kenaikan bandwidth lagi **(burst limit)** selama 32 detik **(burst time)** dan jika sudah 32 detik, maka akan turun lagi secara drastis **(burst threshold)**, kemudian bandwidth akan normal kembali (2Mb) lalu setelah beberapa saat akan terjadi **burst** lagi, dan begitulah seterusnya.

# PCQ (PER-CONNECTION QUEUE)

PCQ atau Per Connection Queue merupakan metode queue dalam MikroTik yang berfungsi untuk membagi rata suatu bandwidth yang diberikan. Misalkan kita punya bandwidth 512 kb, lalu kita akan membagi rata bandwidth tersebut ke 2 PC, bahkan 7 PC. Kita cukup menggunakan 1 rule PCQ tanpa harus menggunakan 7 rule simple queue. PCQ bekerja dengan membuat sub-stream berdasarkan parameter pcq-classifier yang dapat berupa IP Address pengirim berdasarkan pengirim (src-address), IP Address tujuan (dst-address), Port pengirim (src-port) maupun Port tujuan (dst-port).

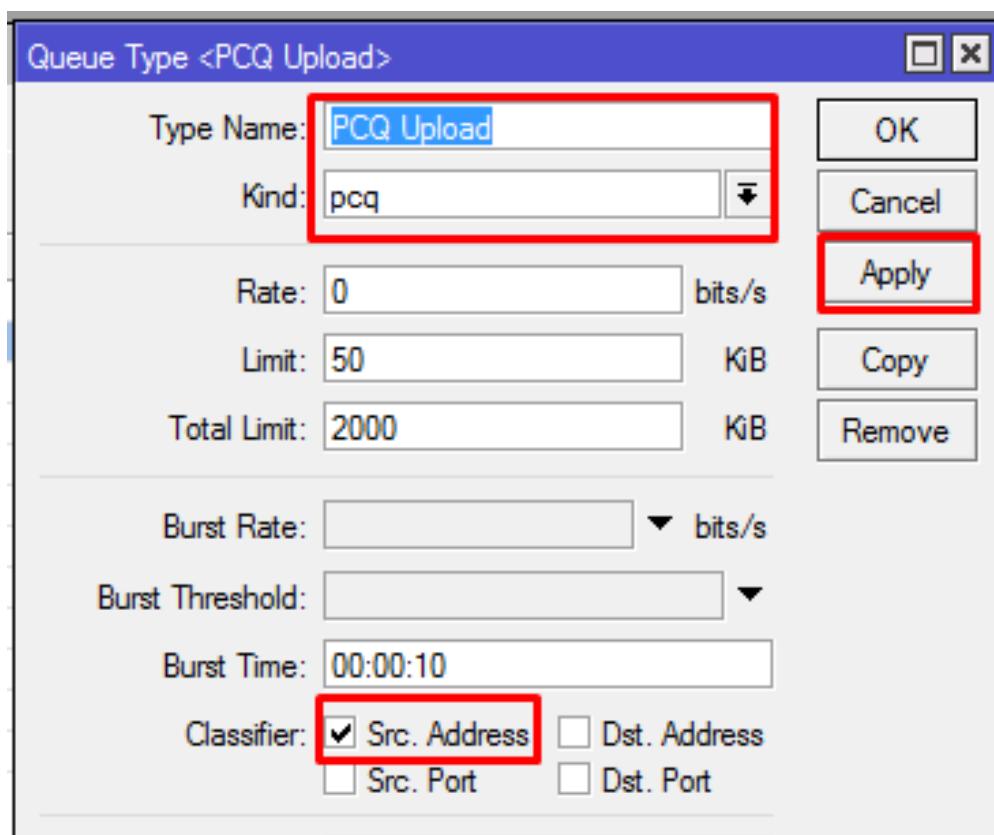
Dibawah ini contoh dari PCQ:



Beginilah caranya:

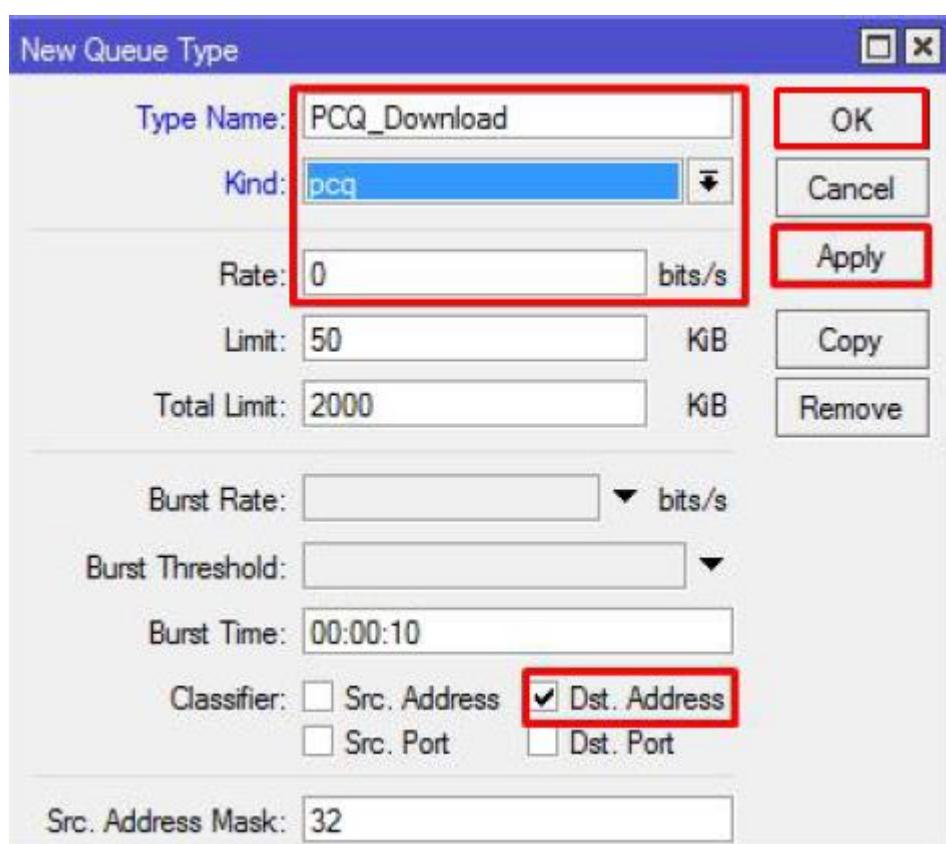
Pertama-tama kita buat queue-type untuk upload:

- Klik 'queue>queue type> add (+)', isikan:
  - Type Name: PCQ\_Upload ,
  - Kind: Pcq
  - Rate: 0
  - Classifier: Src. Address



kemudian kita buat queue type untuk download terlebih dahulu

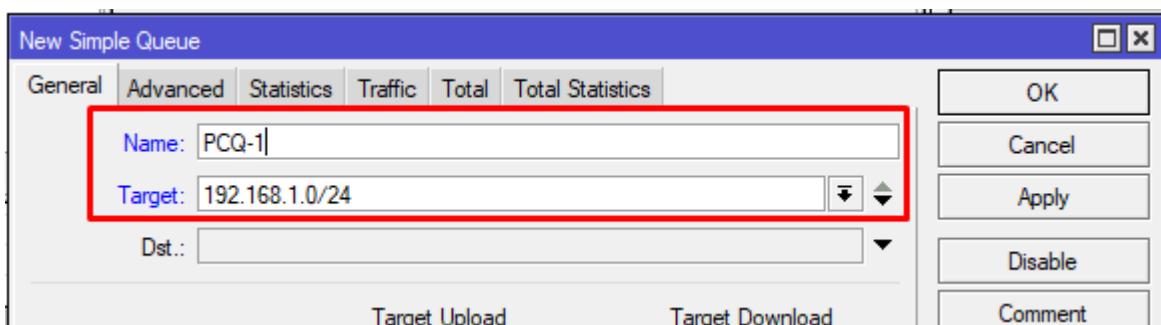
- Klik 'queue>queue type> add (+), isikan:
  - Type Name: PCQ\_Download ,
  - Kind: Pcq
  - Rate: 0
  - Classifier: Dst. Address



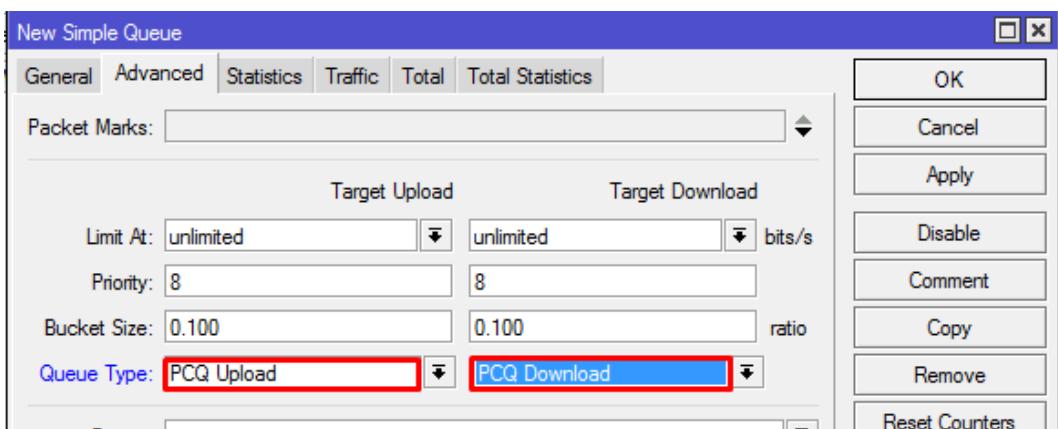
Jika sudah, urutan rule akan seperti ini:

Type	Name
PCQ Download	pcq
PCQ Upload	pcq

Lalu kita akan simple queue dan memasukkan PCQ kedalamnya.



- Klik menu ‘queue>simple queue>add ‘+’ kita isikan:
  - Name: (bebas)
  - Target: 192.168.1.0 (Target network yang akan kita buat queue PCQ)
- Kemudian klik tab ‘advanced’ kita isikan pada ‘queue type’ :



- Queue type upload/download: PCQ\_Uplod/PCQ\_Download
- Jika sudah ‘apply lalu ‘ok’

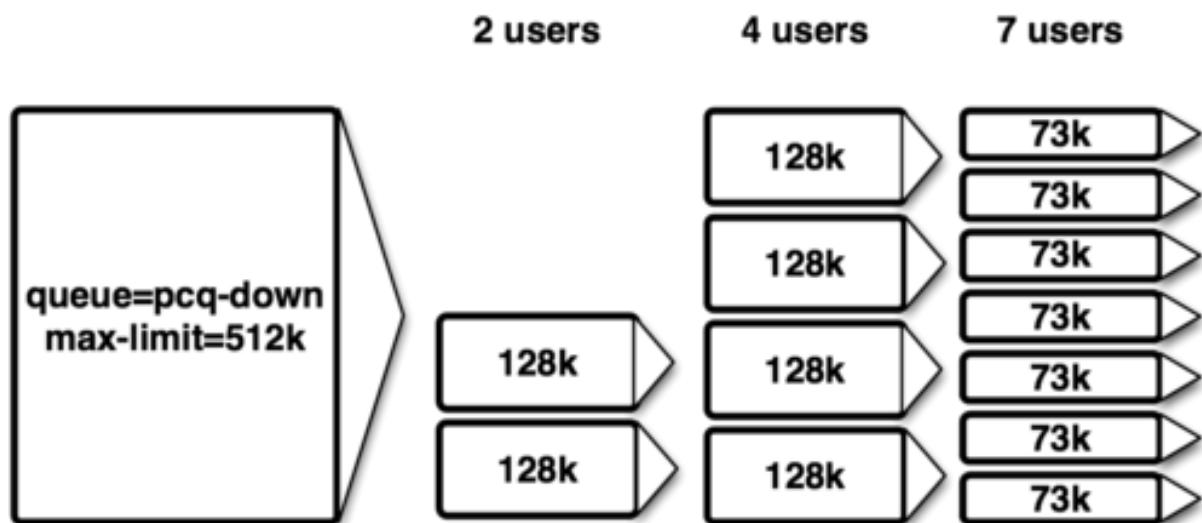
Jika sudah selesai, maka bandwidth pada network 192.168.1.0/24 akan terbagi dengan rata secara otomatis

# PCQ WITH RATE

Dalam PCQ kita juga bisa menggunakan Parameter PCQ Rate, Parameter pcq-rate: dapat digunakan untuk membatasi bandwidth maksimum yang bisa didapatkan oleh tiap sub-stream. Jika parameter yang digunakan adalah pcq-rate=0 maka setiap sub-stream bisa saja mendapatkan bandwidth maksimum yang nantinya diberikan oleh Simple Queue.

Lebih detailnya bisa di lihat gambar di bawah ini yang menggunakan pcq-rate=12800 atau 128kb

## pcq-rate=128000

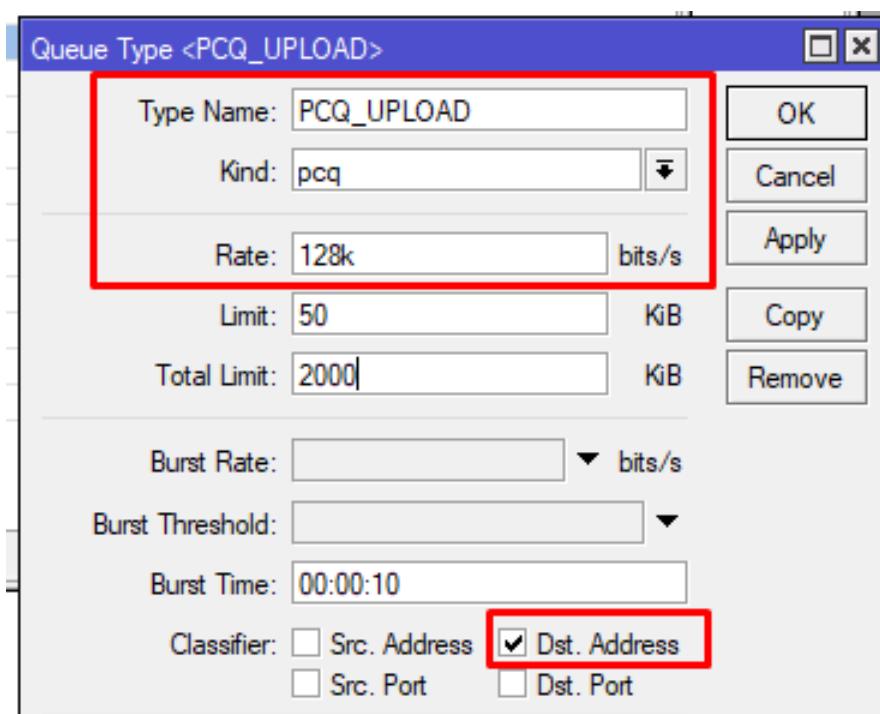


Berdasarkan gambar diatas, kita bisa melihat bahwa bandwidth tiap user menjadi rata 128 kb jika menggunakan PCQ rate. Padahal bandwidth aslinya ada 512 kb

Beginilah caranya:

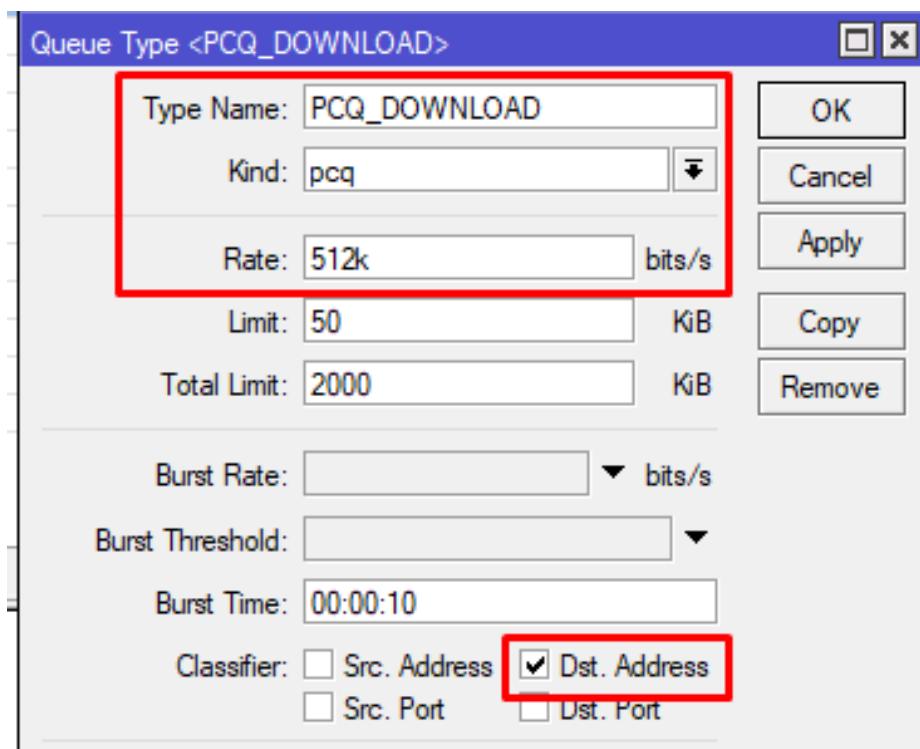
Pertama-tama kita buat queue type untuk upload terlebih dahulu

- Klik 'queue>queue type> add (+), isikan:
  - Type Name: PCQ\_Upload
  - Kind: pcq
  - Rate: 128k (kita akan membagi rata semua bandwidth upload menjadi 128kb)
  - Classifier: Src. Address



Selanjutnya kita buat queue-type untuk download:

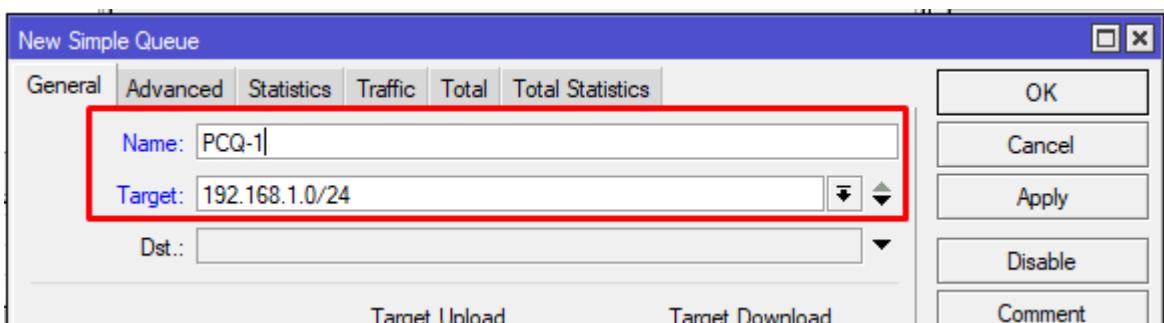
- Klik 'queue>queue type> add (+), isikan:
  - Type Name: PCQ\_Download
  - Kind: pcq
  - Rate: 512k (kita akan membagi rata semua bandwidth download menjadi 512kb)
  - Classifier: Dst. Address



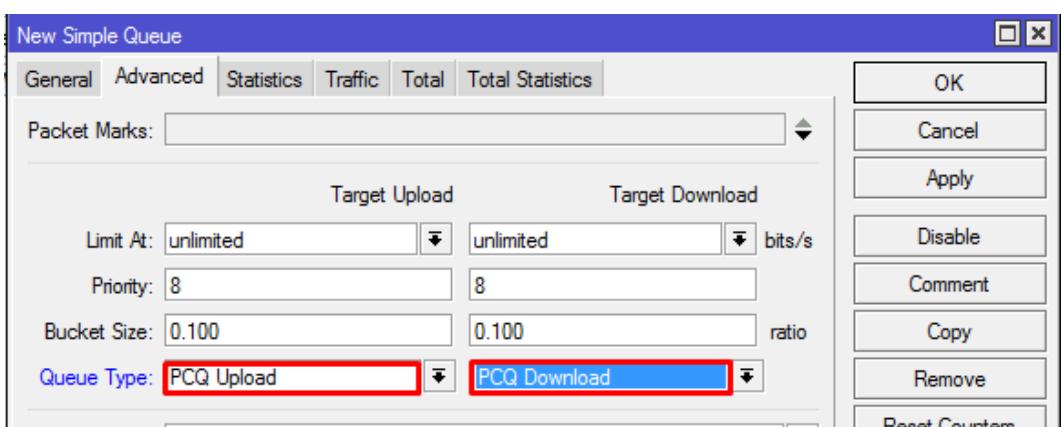
Jika sudah, urutan rule akan seperti ini:

Type	Name	Kind
PCQ Download	pcq	
PCQ Upload	pcq	

Lalu kita akan simple queue dan memasukkan PCQ kedalamnya.



- Klik menu 'queue>simple queue>add '+' kita isikan:
  - Name: (bebas)
  - Target: 192.168.1.0 (Target network yang akan kita buat queue PCQ)
- Kemudian klik tab 'advanced' kita isikan pada 'queue type' :



- Queue type upload/download: PCQ\_Uplod/PCQ\_Download
- Jika sudah 'apply lalu 'ok'

Jika sudah selesai, maka bandwidth upload/download pada network 192.168.1.0/24 akan terbagi menjadi 128kb/512kb meskipun banyak klien.

# QUEUE TREE

Apa itu Queue Tree?

Merupakan fitur bandwidth management di Mikrotik yang sangat fleksibel dan cukup kompleks. Pendefinisian target yang akan dilimit pada Queue Tree tidak dilakukan langsung saat penambahan rule Queue namun dilakukan dengan melakukan marking paket data menggunakan Firewall Mangle. Inilah yang menjadikan penerapan Queue Tree menjadi lebih kompleks.

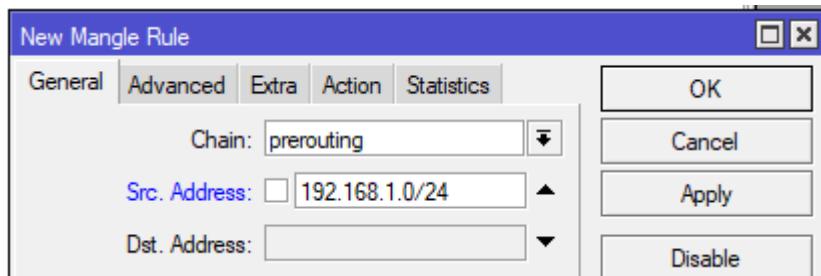
Langkah ini menjadi tantangan tersendiri, sebab jika salah pembuatan Mangle bisa berakibat Queue Tree tidak berjalan.

Namun disisi lain penggunaan Mangle Packet-Mark ini juga menguntungkan, sebab akan lebih fleksible dalam menentukan traffic apa yang akan dilimit, bisa berdasar IP Address, Protocol, Port dan sebagainya. Setiap service pada jaringan dapat diberikan kecepatan yang berbeda.

Kita langsung kita coba ya!

Pertama-tama kita buat firewall mangle mark seperti yang ada dipenjelasan tadi.

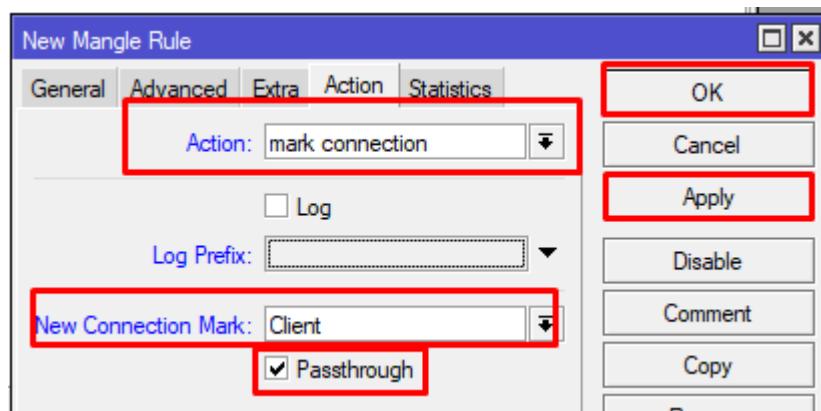
- Klik ‘ip>firewall>mangle’ lalu kita buat baru, klik ‘+’ isikan:



- Chain: prerouting
- Src. Address: 192.168.1.0/24 (Network tujuan/klien)

Kemudian klik tab ‘Action’ isikan:

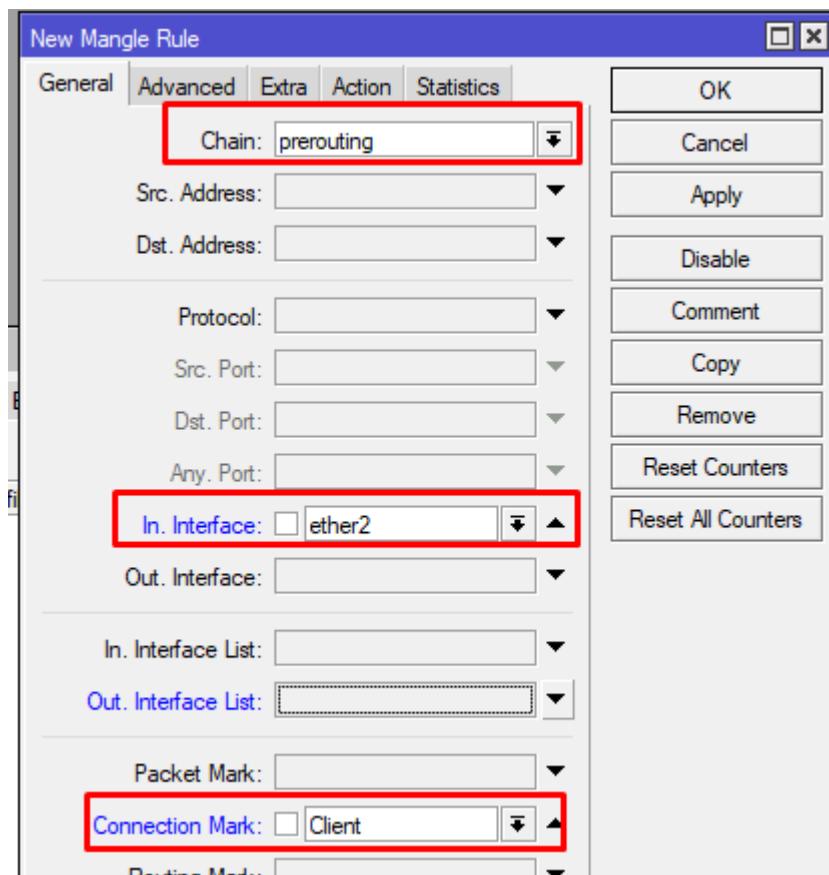
- Action: Mark Connection
- New Connection Mark: Client
- Centang Passthrough



Jika sudah ‘apply’ kemudian ‘ok.

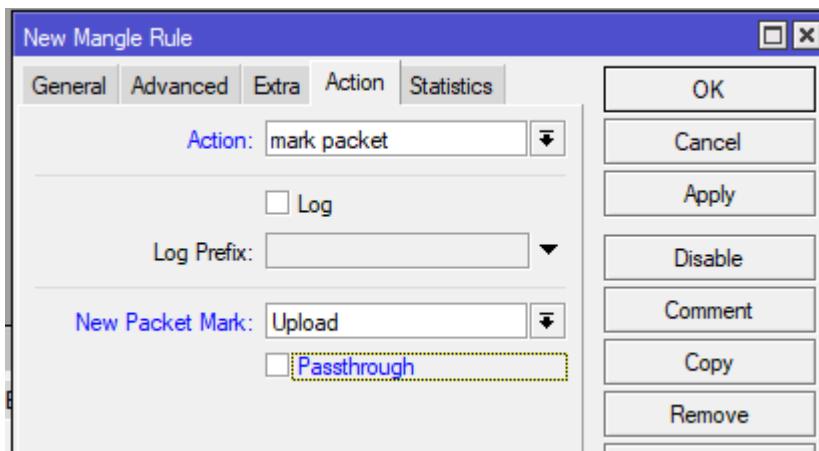
Setelah menandai koneksi klien, sekarang kita buat mangle untuk menandai traffic upload dari klien.

Masih di 'IP>Firewall>Mangle>add'+' kita isikan:



- Chain: prerouting
- In. Interface: ether2 (karena jika upload yang dilewati pertama adalah ether)
- Connection Mark: Client (yang tadi kita buat)

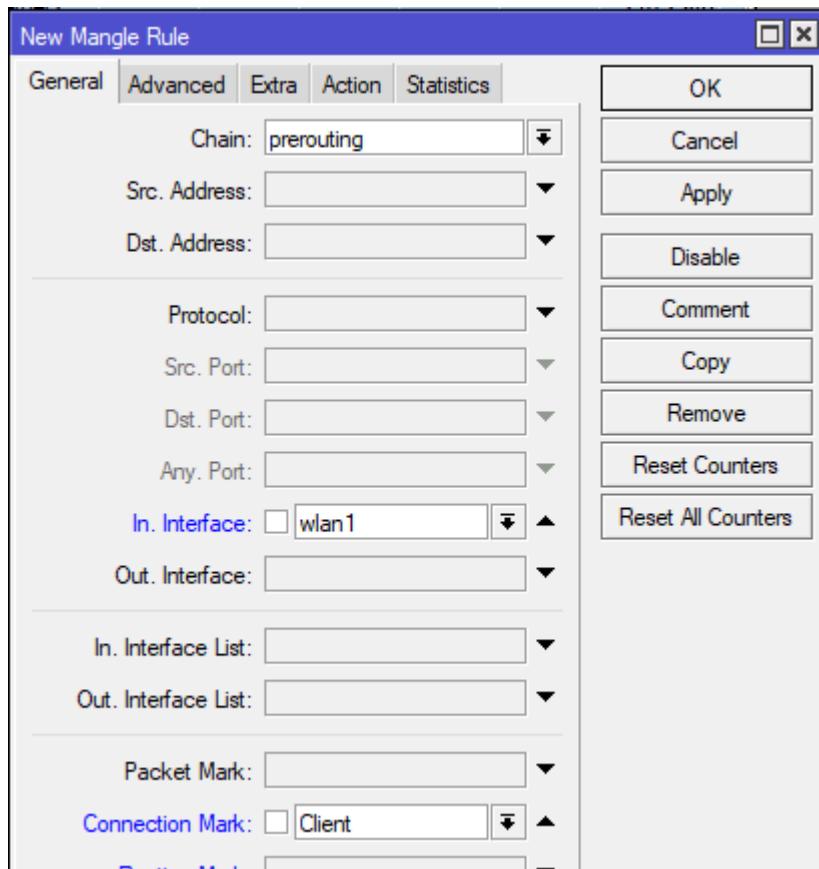
Lalu klik tab ‘Action’ kita isikan:



- Action: mark packet
- New Packet Mark: Upload
- Kita hilangkan centang pada Passthrough
- Jika sudah ‘apply’ lalu ‘ok’

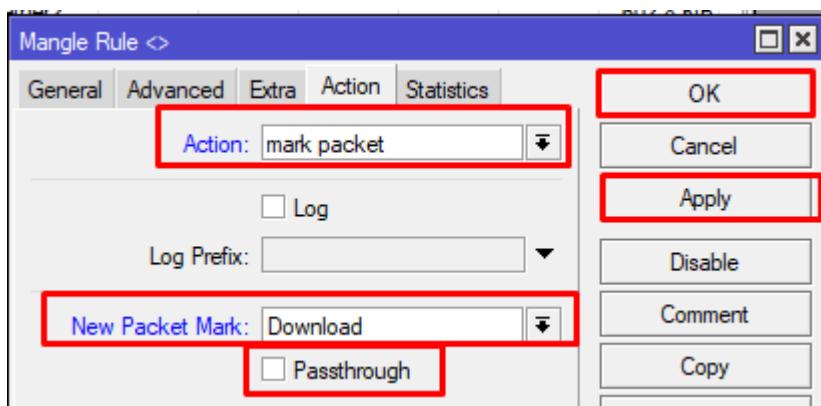
Selanjutnya kita buat firewall mangle untuk menandai download klien.

Masih di 'IP>Firewall>Mangle>add'+' kita isikan:



- Chain: prerouting
- In. Interface: wlan1 (karena jika kita download pasti akan melalui wlan terlebih dahulu, karena sumber internet dari wlan)
- Connection Mark: Client

Lalu klik tab ‘Action’ kita isikan:



- Action: mark packet
- New Packet Mark: Download
- Kita hilangkan centang pada Passthrough
- Jika sudah ‘apply’ lalu ‘ok’

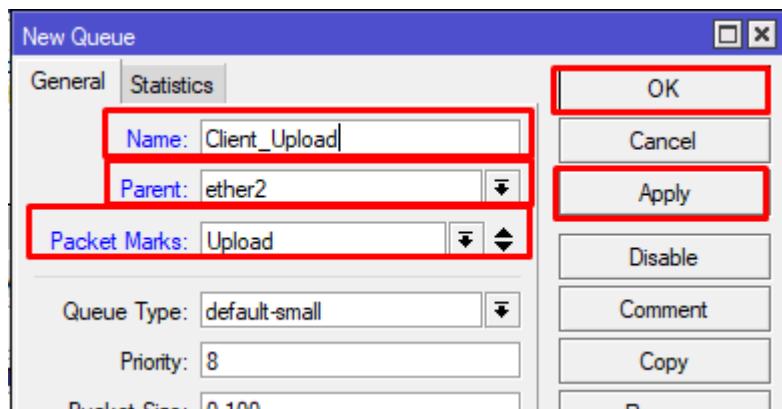
Jika kita sudah, maka pada firewall mangle table, akan seperti ini:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes
0	mark...	prerouting	192.168.1....											965.7 KB
1	mark...	prerouting												675.1 KB
2	mark...	prerouting												3890 B

Selanjutnya, kita akan membuat queue tree-nya

Pertama-tama kita buat queue tree untuk upload terlebih dahulu

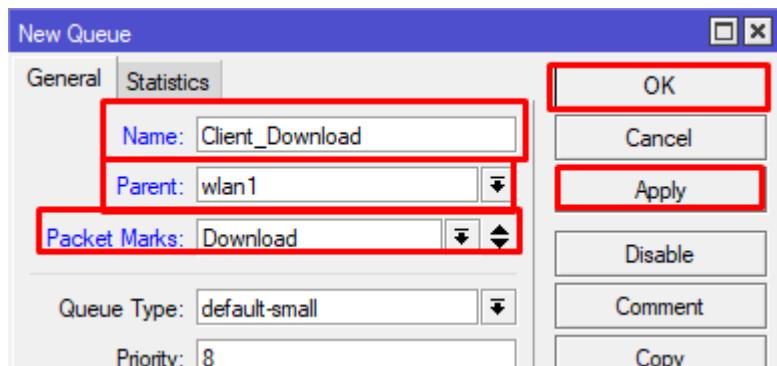
- Klik 'queue>queue tree> kita buat baru '+, kita isikan:



- Name: Client\_Upload (bebas)
- Parent: ether2
- Packet Marks: Upload (mangle yang tadi kita buat)
- Jika sudah 'apply' kemudian 'ok'

Kemudian kita buat queue tree untuk downloadnya:

- Klik 'queue>queue tree> kita buat baru '+, kita isikan:



- Name: Client\_Download
- Parent: wlan1
- Packet Marks: Download (Mangle yang tadi kita buat)
- Jika sudah 'apply' kemudian 'ok'

Jika langkah ini Sudah maka konfigurasi queue tree sudah selesai dan semua klien akan mendapat bandwidth yang rata, kemudian juga akan ditandai berapa banyak sudah melakukan upload dan download dengan mangle.

## Catatan:



# PENGENALAN NETWORK MANAGEMENT

## Overview

Manajemen jaringan adalah proses mengatur dan mengelola jaringan komputer. Layanan yang disediakan oleh disiplin ini meliputi analisis kesalahan, manajemen kinerja, penyediaan jaringan, dan menjaga kualitas layanan.

Didalam network management terdapat beberapa layanan:

- 1. DCHP**
- 2. Web Proxy**
- 3. Transparent Proxy**
- 4. ARP**
- 5. Hotspot**
- 6. IP Binding**
- 7. Walled Garden**

Untuk pengertian, fungsi dan prakteknya, saya akan jelaskan pada masing-masing lab.

# DHCP

Apa itu DHCP?

DHCP merupakan singkatan dari **Dynamic Host Configuration Protocol**. adalah protokol yang berbasis arsitektur client/server yang dipakai untuk memudahkan pengalokasian alamat IP dalam satu jaringan.

Fungsinya adalah untuk mempermudah pendapatkan IP Address pada suatu jaringan. Misalnya jika pada suatu jaringan tidak dipasang DHCP Server, maka pengalaman pada klien harus dikonfigurasi secara manual, sedangkan jika kita pasang DHCP Server pada suatu jaringan, maka klien akan mendapatkan IP Address secara otomatis dari DHCP Server tanpa harus mengkonfigurasi secara manual.

Pada DHCP terdapat 2 peran, yaitu:

## 1. **DHCP Server**

DHCP Server berfungsi untuk membuat daftar IP Address (IP Pool) dan kemudian memberikannya kepada klien.

## 2. **DHCP Client**

DCHP Client berfungsi untuk menerima IP Address yang diberikan oleh DHCP Server.

Beginilah proses yang terjadi pada DHCP antara Server dan Client

### **1. IP Least Request**

Komputer client meminta alamat IP ke server

### **2. IP Least Offer**

DHCP server yang memiliki list alamat IP memberikan penawaran kepada komputer client

### **3. IP Lease Selection**

Komputer client memilih/ menyeleksi penawaran yang pertama kali diberikan DHCP, kemudian melakukan broadcast dengan mengirim pesan bahwa komputer client menyetujui penawaran tersebut

### **4. IP Lease Acknowledge**

Pada tahap ini DHCP server menerima pesan tersebut dan mulai mengirim suatu paket acknowledge (DHCPACK) kepada client.

Paket tersebut berisi berapa lama komputer client bisa menggunakan alamat IP tersebut (yang diberikan DHCP server) beserta konfigurasi lainnya. Dan komputer client pun dapat terhubung ke jaringan.

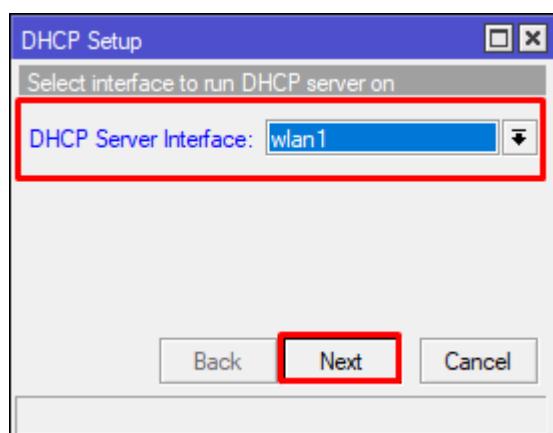
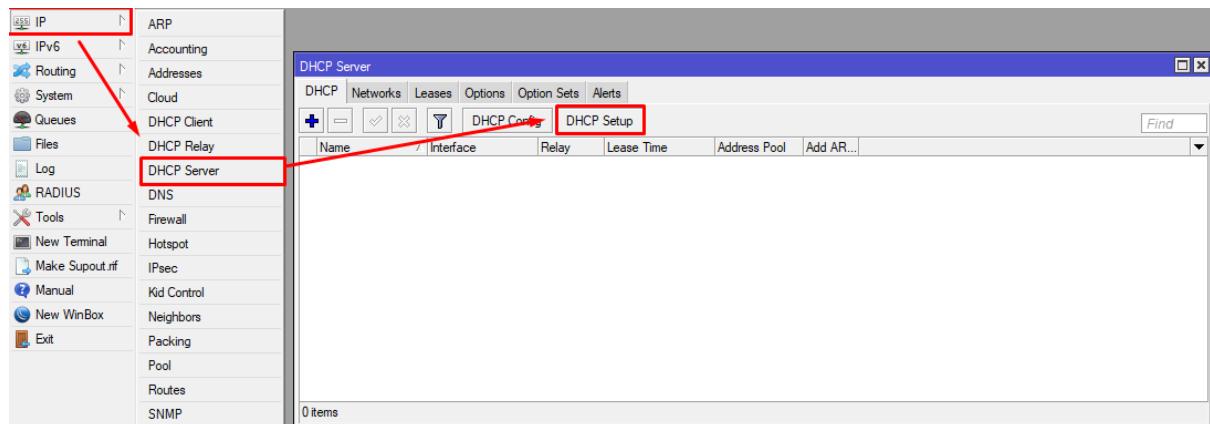
## Setting DHCP Server

Cara untuk membuat DHCP Server ada 2, dengan DHCP Setup, maupun dengan cara setting secara manual.

### 1. Setting DHCP Otomatis (DHCP Setup)

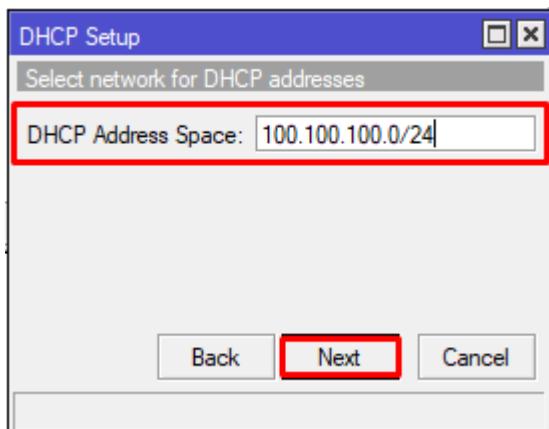
Pertama-tama kita langsung menuju menu DHCP Server.

- Klik 'IP>DHCP Server>DHCP Setup'



DHCP Server Interface: wlan1

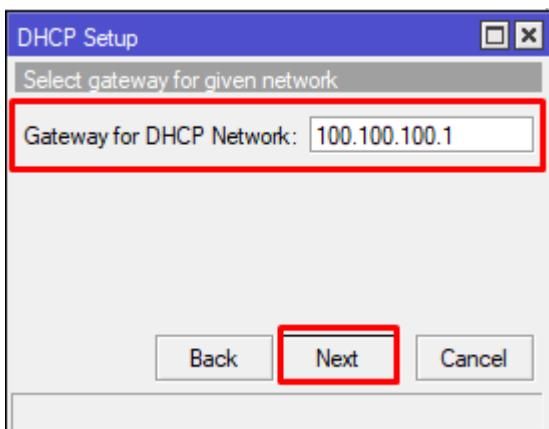
Dimana DHCP Server akan berjalan



### DHCP Address Space:

**100.100.100.0/24**

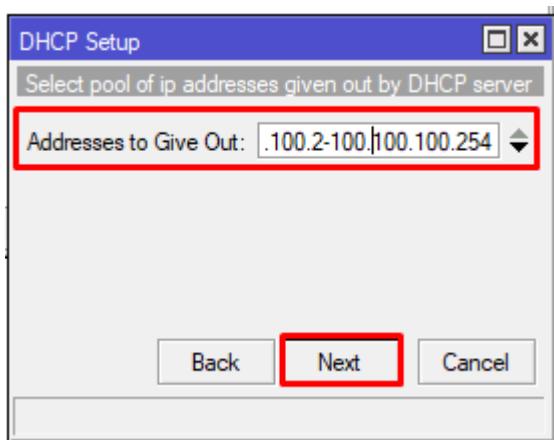
Network yang digunakan pada DHCP Server



### Gateway for DHCP Network:

**100.100.100.1**

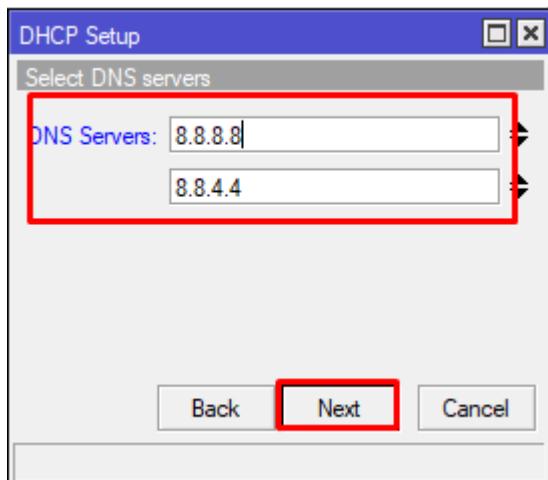
Gateway yang digunakan pada DHCP (IP Address interface yang digunakan untuk DHCP)



**Address to Give Out: 100.100.100.2 –**

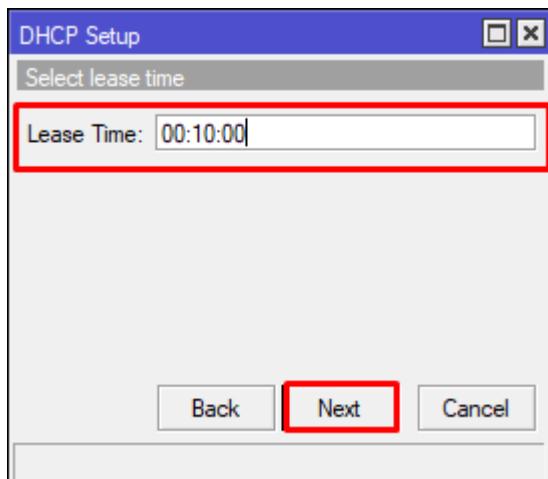
**100.100.100.254**

Daftar IP Address yang akan diberikan kepada klien, yaitu antara 100.100.100.2, 100.100.100.3 seterusnya hingga 100.100.100.254.



### DNS Servers: 8.8.8.8, 8.8.4.4.

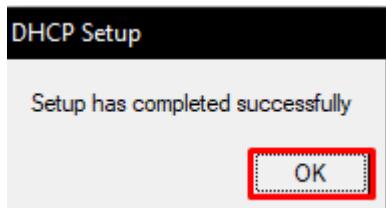
DNS Servers yang akan diberikan kepada klien



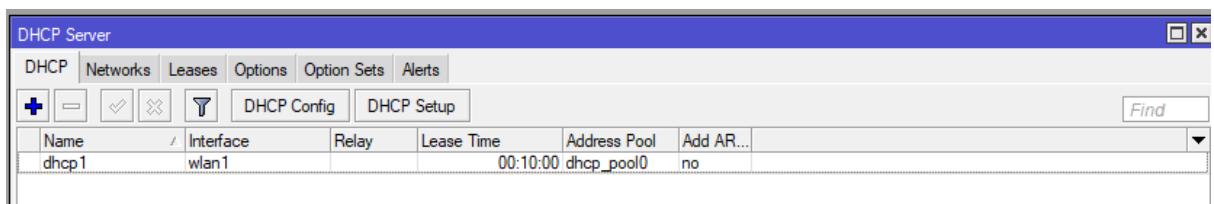
### Lease Time: 00:10:00

Waktu yang klien punya untuk bisa menggunakan IP yang diberikan oleh DHCP server, jika waktu Lease telah habis, maka IP yang sebelumnya dipakai akan kadaluarsa dan klien akan meminta IP baru lagi dari server

Jika sudah, konfigurasi DHCP Server sudah selesai dan kita bisa lihat



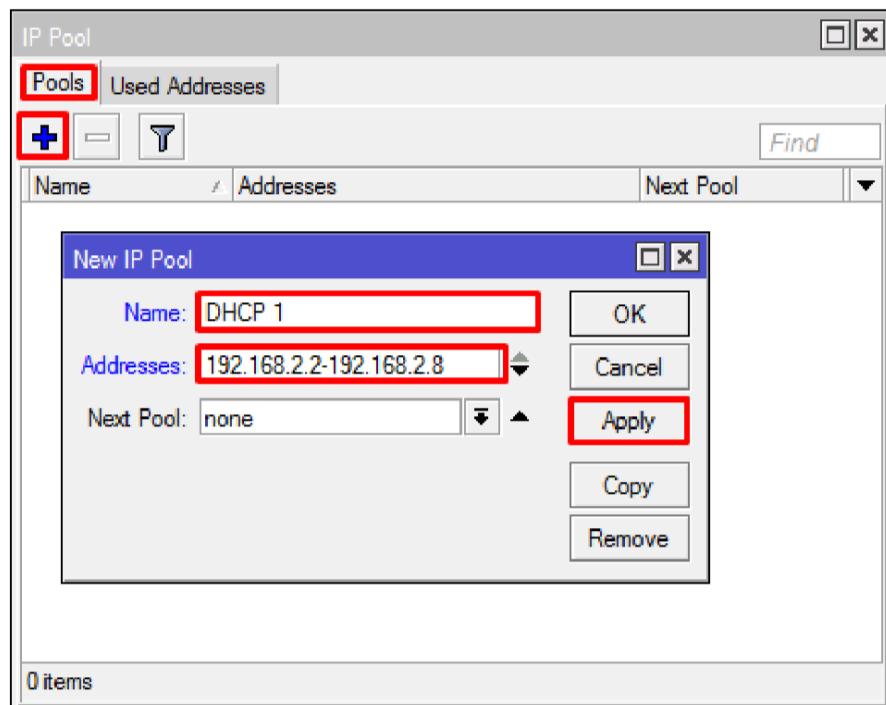
hasilnya di 'IP>DHCP Server>DHCP'



## 2. Setting DHCP Manual

Pertama-tama kita buat IP Pool (daftar IP Address yang nantinya akan diberikan kepada klien).

- klik 'IP>Pool' lalu kita buat baru '+' kita isikan:

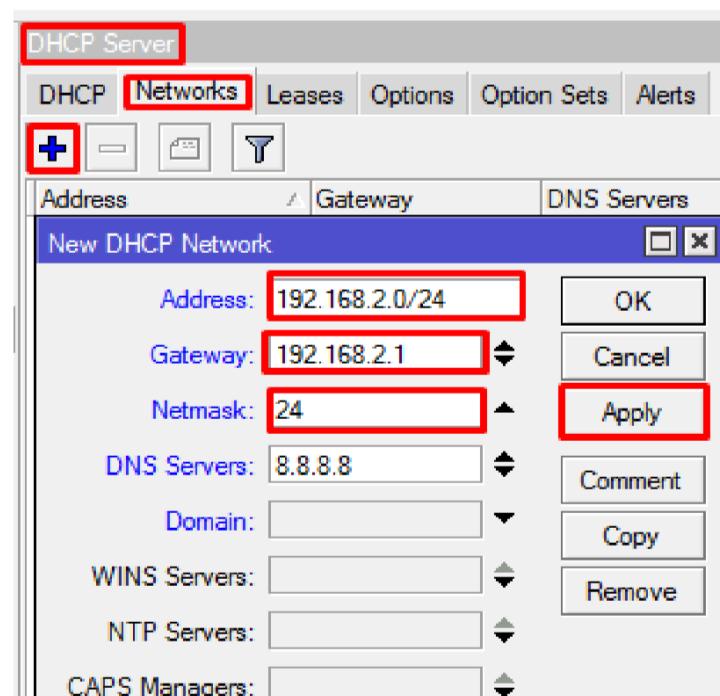


- Name: DHCP 1 (bebas)
- Addresses: 192.168.2.2 – 192.168.2.8
- Jika sudah 'apply' kemudian 'ok'

Maksud dari IP Pool ini adalah: kita memberikan IP 192.168.2.2, 192.168.2.3 dan seterusnya hingga IP 192.168.2.8 kepada klien.

Selanjutnya kita buat DCHP Server Networknya.

- Klik 'IP>DHCP Server>Networks' lalu kita buat baru '+' kita isikan:



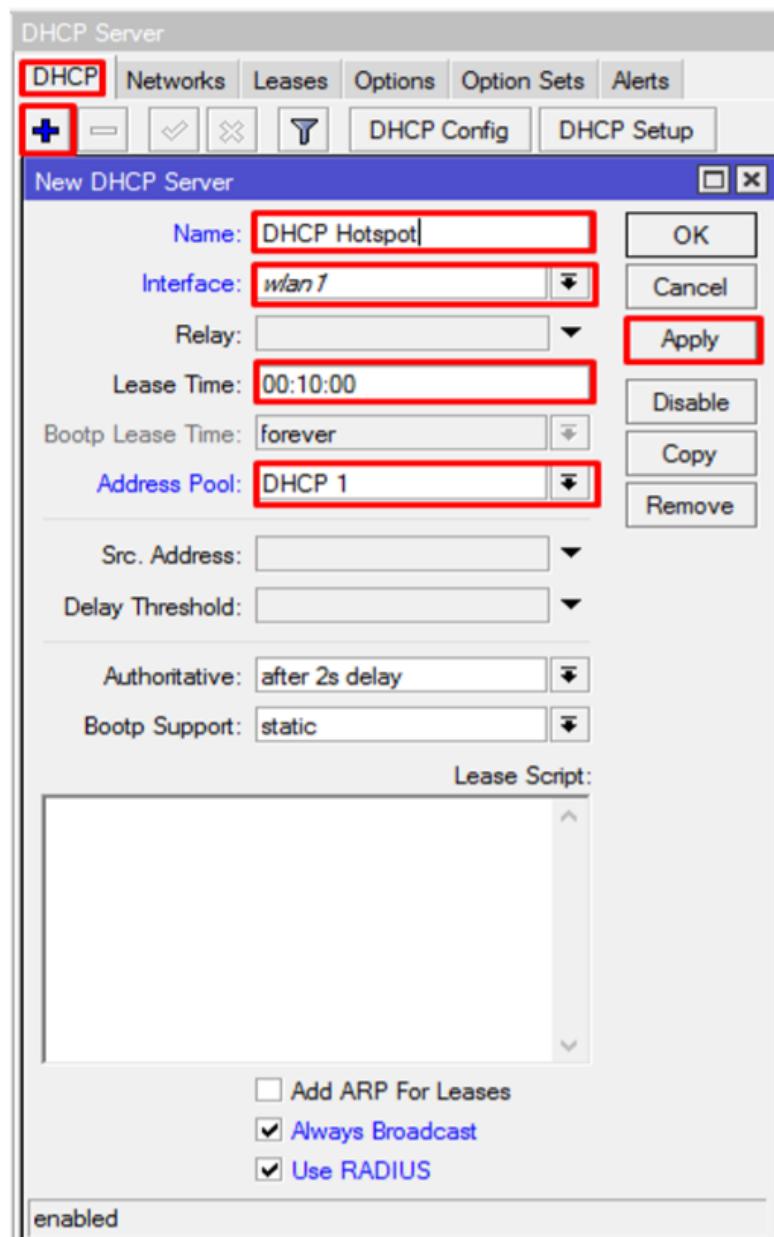
- Addresses: 192.168.2.0/24
- Gateway: 192.168.2.1
- Netmask: 24 (karena kita menggunakan prefix /24)
- DNS Server: 8.8.8.8 (bebas)
- Jika sudah 'apply' lalu 'ok'

Jika sudah, maka pada table DHCP Server Networks akan seperti ini:

DHCP Server					
DHCP	Networks	Leases	Options	Option Sets	Alerts
				Address: 192.168.2.0/24 Gateway: 192.168.2.1 DNS Servers: 8.8.8.8	Domain:      WINS Servers:      NTP Servers:      CAPS Managers:

Selanjutnya, kita buat DHCP Server

- Klik 'IP>DHCP Server>DHCP' kemudian kita buat baru '+' kita isikan:



Name: DHCP Hotspot

Interface: wlan1

Lease time: 00:10:00

Address Pool: DHCP 1

Centang: Always

Broadcast dan Use  
Radius

Jika sudah 'apply' lalu 'ok'

**Maksudnya:**

**Interface: wlan1**

Karena kita akan membuat DHCP server pada interface wlan1

**Lease time: 00:10:00**

Waktu yang klien punya untuk bisa menggunakan IP yang diberikan oleh DHCP server, jika waktu Lease telah habis, maka IP yang sebelumnya dipakai akan kadaluarsa dan klien akan meminta IP baru lagi dari server

**Address Pool: DHCP 1**

Daftar IP yang tadi sudah kita buat

**Centang: Always Broadcast dan Use Radius**

Selalu membroadcast IP ke semua klien dan dapat menggunakan Radius.

Jika sudah, maka DHCP Server telah terbentuk pada interface wlan1

DHCP Server						
DHCP		Networks		Leases		Options
+ -		✓ ✘		✖		Filter
DHCP Config		DHCP Setup				
Name	Interface	Relay	Lease Time	Address Pool	Add AR...	
DHCP Hotspot	wlan1		00:10:00	DHCP 1	no	

# WEB PROXY

## OVERVIEW

Proxy adalah server yang menyediakan suatu layanan untuk meneruskan setiap permintaan user kepada server lain yang terdapat di internet. Atau definisi proxy server yang lainnya yaitu suatu server atau program komputer yang mempunyai peran sebagai penghubung antara suatu komputer dengan internet.

Bagaimanakah Proxy bekerja?

Sebenarnya prinsip kerja proxy server sangatlah sederhana, saat user menggunakan layanan suatu proxy lalu meminta file atau data yang terdapat di public server (internet) maka proxy akan meneruskannya ke internet jadi seolah-olah proxy tersebut yang memintanya. Dan saat proxy server telah mendapatkan apa yang diminta oleh user, proxy akan memberikan respon kepada user jadi seolah-olah dia adalah public servernya.

## **FUNGSI PROXY**

Lalu apa saja fungsi dari proxy?

### **1. Fungsi connecting sharing**

Salah satu fungsi proxy adalah sebagai connecting sharing yaitu sebagai penghubung atau perantara pengambilan data dari suatu alamat IP dan diantarkan ke alamat IP lainnya ataupun kepada IP komputer user.

### **2. Fungsi filtering**

Terdapat beberapa proxy yang dilengkapi dengan firewall yang dapat memblokir beberapa atau sebuah alamat IP yang tidak diinginkan,

sehingga beberapa website tidak dapat diakses dengan memakai proxy tersebut. Itulah salah satu fungsi dari proxy sebagai filtering.

### **3. Fungsi caching**

Dan fungsi proxy yang lainnya yaitu sebagai fungsi caching, disini maksudnya proxy juga dilengkapi dengan media penyimpanan data dari suatu web, dari query ataupun permintaan akses user. Misalnya permintaan untuk mengakses suatu web dapat lebih cepat jika telah ada permintaan akses ke suatu web pada pemakai proxy sebelumnya. Itulah fungsi proxy sebagai caching.

## **JENIS PROXY**

### **1. Web Proxy.**

Proxy yang harus dikonfigurasi secara manual pada browser yang kita gunakan, jadi setelah kita selesai membuat konfigurasi di MikroTik, kita juga harus mengonfigurasi ulang di browser. Namun jika ada 2 browser misalkan Chrome dan Firefox, maka kita harus mengonfigurasi kedua browser tersebut agar dapat terhubung ke proxy. Dan kita perlu mengonfigurasi browser pada tiap klien agar dapat terhubung ke proxy

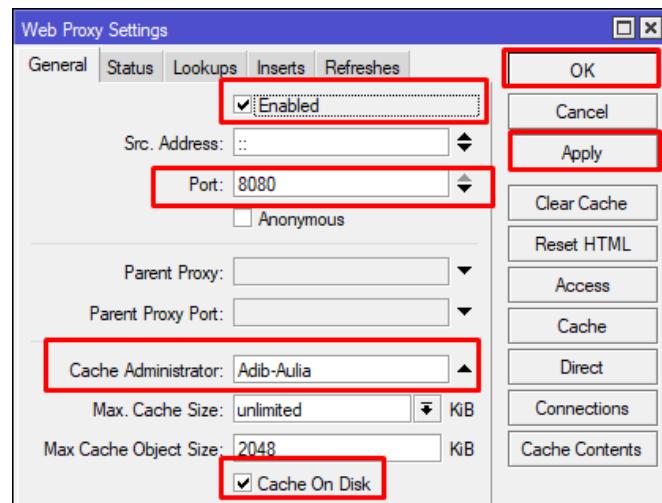
### **2. Transparent Proxy.**

Proxy yang secara otomatis bisa terhubung tanpa harus mengonfigurasi proxy pada browser, kita cukup menggunakan NAT untuk perintahnya. Dengan Transparent proxy ini, kita bisa menggunakan proxy disemua browser dan semua klien.

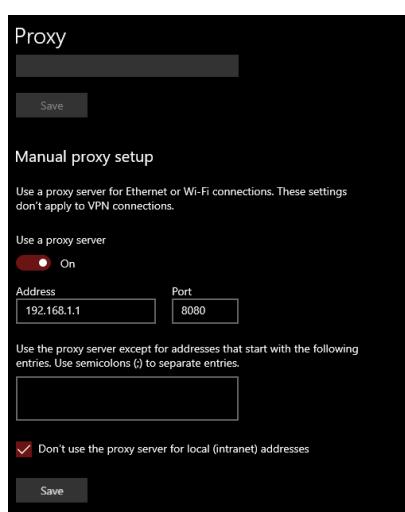
## KONFIGURASI WEB PROXY

- Pertama-tama buka winbox, klik menu ‘IP>Web Proxy’
- Lalu pada Web Proxy settings, isi konfigurasi seperti berikut:

- Centang (enabled)
- Port: 8080
- Cache Administrator:  
(bebas) Adib-Aulia
- Centang (Cache On Disk)  
agar menyimpan cachenya dalam files.
- Lalu ‘apply’ dan ‘ok’



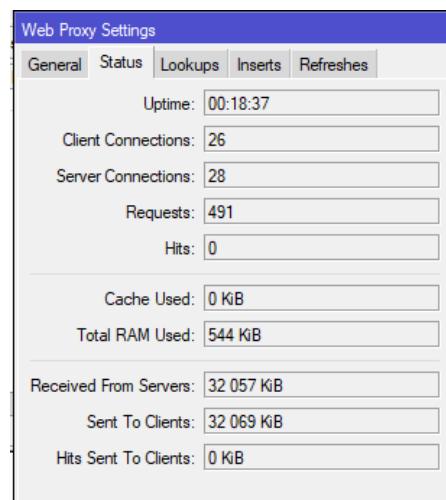
- Selanjutnya kita setting proxy pada browser/windows.
- Kita menuju windows 10 setting (bagi yang windows 10)
- Kita cari di search table: proxy



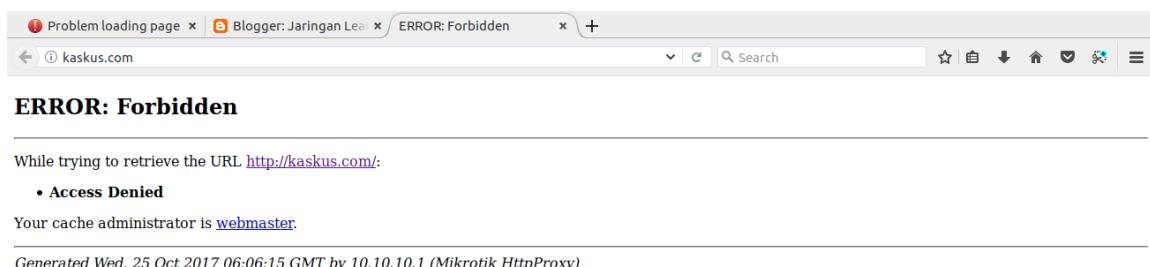
- Lalu klik ‘Proxy settings’
- Disitu klik klik ‘on’ use a proxy server. Kita isikan:
  - Address: 192.168.1.1 (address router)
  - Port: 8080 (port web proxy)
  - Lalu klik ‘save’

Dengan begitu Web Proxy sudah aktif, untuk mengeceknya sudah berjalan atau belum, kita bisa lihat di status pada Web Proxy.

Lalu kita coba mengecknya juga dengan browsing di browser yang sudah kita setting Web proxy.

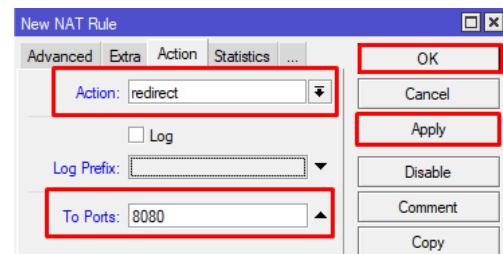
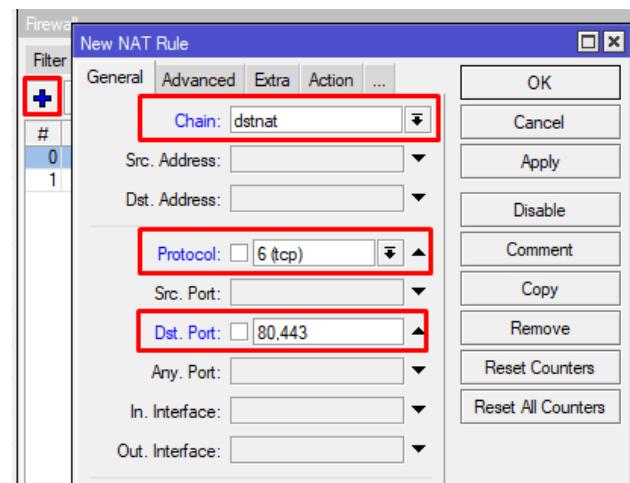


Hasilnya adalah terblokir.



## KONFIGURASI TRANSPARENT PROXY

- Pertama-tama kita konfigurasikan Web Proxy (konfigurasinya sama seperti web proxy)
- Jika Web Proxy sudah kita buat, maka selanjutnya kita buat NAT untuk meredirect ke port proxy. Kita isikan:
  - Chain: dstnat
  - Protocol: tcp
  - Dst. Port: 80, 443 (port HTTP dan HTTPS)
- Kemudian pada tab Action kita isikan:
  - Action: redirect
  - To Port: 8080 (port web proxy)
  - Jika sudah ‘apply’ lalu ‘ok’



Dengan begini Transparent Proxy sudah aktif dan kita bisa menjalankannya secara langsung ke semua klien.

## KONFIGURASI PEMBLOKIRAN SITUS DENGAN PROXY.

Didalam proxy, kita juga bisa menyaring situs-situs dan mengubah perintahnya, misalkan kita mau mengakses 1cak, namun karena kita terhubung dengan proxy, yang tadinya kita akan mengakses 1cak, menjadi teralihkan dan malah mengakses situs islampos.

Beginilah caranya.

- Kita buat dulu Web Proxy/Transparent Proxy.

● Jika sudah, kita ke menu Access pada web proxy settings.

- Lalu buat web proxy rule baru ‘+’

- Kita isikan:

- Dst Port: 80, 443 (port HTTP dan HTTPS)

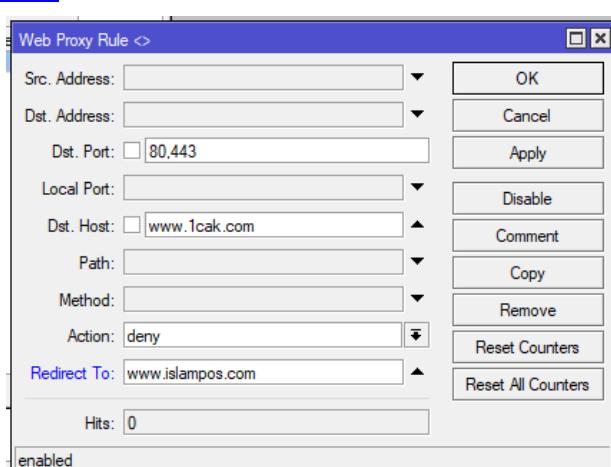
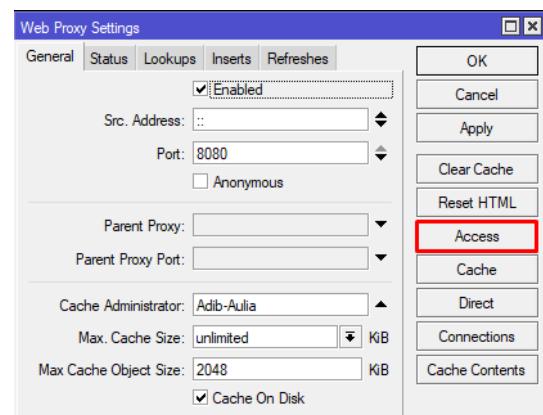
- Dst. Host: [www.1cak.com](http://www.1cak.com)

(situs yang akan kita alihkan)

- Action: deny

- Redirect To:

[www.islampos.com](http://www.islampos.com) (situs yang ingin kita tuju)



Kemudian kita coba untuk mengakses 1cak, hasilnya akan teralihkan dan akan mengakses islampos.



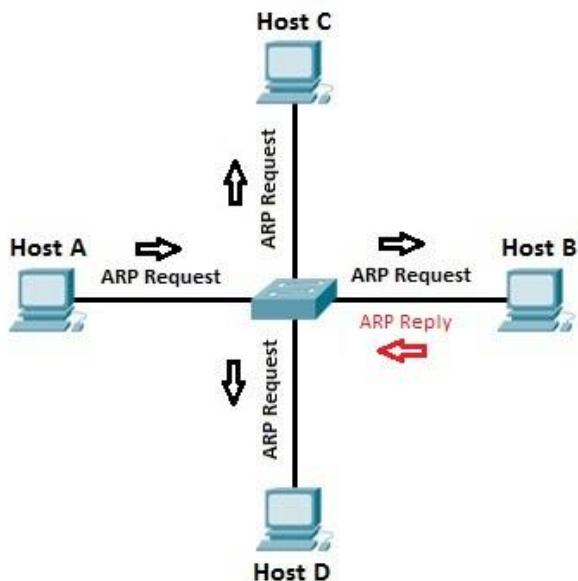
# ARP (ADDRESS RESOLUTION PROTOCOL)

## Overview

Apa itu ARP?

ARP (Address Resolution Protocol) adalah protokol jaringan yang digunakan untuk mengetahui alamat perangkat keras (MAC) dari suatu perangkat dari alamat IP. Ini digunakan ketika perangkat ingin berkomunikasi dengan beberapa perangkat lain di jaringan lokal (misalnya pada jaringan Ethernet yang membutuhkan alamat fisik untuk diketahui sebelum mengirim paket). Perangkat pengirim menggunakan ARP untuk menerjemahkan alamat IP ke alamat MAC. Perangkat mengirim pesan permintaan ARP yang berisi alamat IP perangkat penerima. Semua perangkat di segmen jaringan lokal melihat pesan, tetapi hanya perangkat yang memiliki alamat IP tersebut yang merespons dengan pesan balasan ARP yang berisi alamat MAC-nya. Perangkat pengiriman sekarang memiliki cukup informasi untuk mengirim paket ke perangkat penerima.

## Cara Kerja ARP



Katakanlah bahwa Host A ingin berkomunikasi dengan host B.

- Host A mengetahui alamat IP host B, tetapi tidak tahu alamat MAC host B. Untuk mengetahui alamat MAC host B, host A mengirim permintaan ARP, mencantumkan alamat IP host B sebagai alamat IP tujuan dan alamat MAC dari FF: FF: FF: FF: FF: FF (broadcast Ethernet).
- Switch akan meneruskan frame keluar semua antarmuka (kecuali antarmuka masuk). Setiap perangkat di segmen ini akan menerima paket, tetapi karena alamat IP tujuan adalah alamat IP host B, hanya host B yang akan membalas dengan paket balasan ARP, yang mencantumkan alamat MAC-nya.
- Host A sekarang memiliki informasi yang cukup untuk mengirim traffic ke host B.

## **ARP Mode**

ARP juga memiliki mode-mode tersendiri:

### **1. Enable**

Mode ini default enable pada semua interface di MikroTik. Semua ARP akan ditemukan dan secara dinamik ditambahkan dalam ARP tabel

### **2. Proxy ARP**

Router dengan mode ARP proxy akan bertindak sebagai transparan proxy ARP antara dia atau lebih jaringan yang terhubung langsung.

### **3. Reply Only**

ARP reply-only memungkinkan router hanya akan mereply ARP statis ditemukan di tabel ARP, akses ke router dan ke jaringan di belakang router hanya dapat diakses oleh kombinasi Ip dan mac address yang ditemukan ditabelARP.

### **4. Disable**

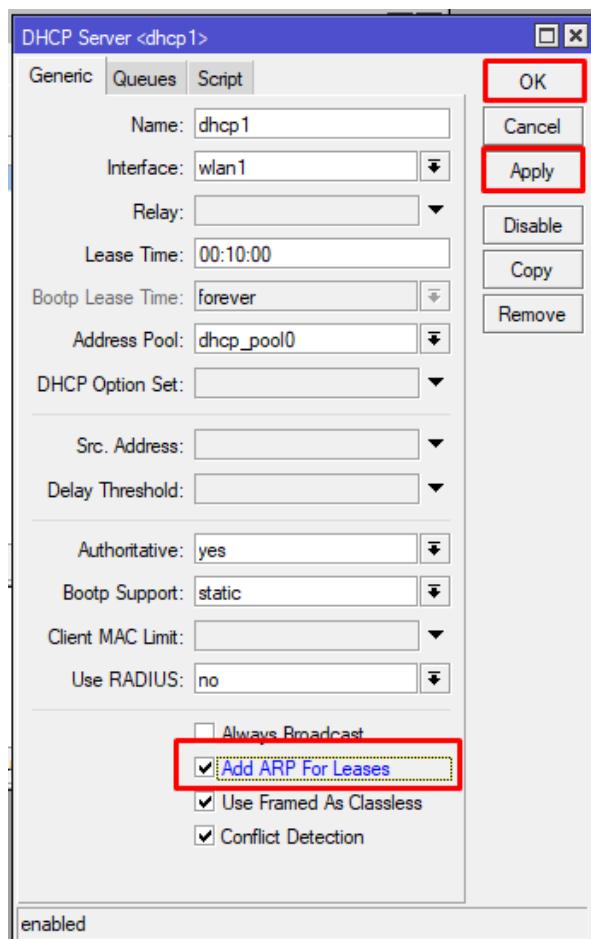
permintaan ARP dari klien tidak dijawab oleh router.

## Fungsi ARP

Sekarang ini, ada aplikasi yang bernama NetCut, yang fungsinya untuk memutus klien yang terhubung pada satu jaringan LAN, hal ini dikarenakan orang ingin mendapatkan bandwidth yang besar dibandingkan orang lain. Mikrotik memiliki cara tersendiri untuk mencegah terjadinya NetCut tersebut, caranya dengan merubah **ARP** menjadi **Reply only**.

Beginilah contohnya:

- Pertama-tama, pastikan ada yang menjadi klien dan server.
- Lalu buat DHCP Server. (bebas menggunakan Setup maupun manual)



- Jika sudah, kita aktifkan fitur ARP pada DHCP Server.
- Klik 'IP>DHCP Server>DHCP> (DHCP Server yang dibuat)'
- Lalu 'apply' dan 'ok'

Jika kita sudah mengaktifkannya di DHCP Server, langkah selanjutnya kita perlu mengaktifkannya juga pada interface yang menjadi DHCP Server.

- Klik menu 'interface>interface wlan1 (interface yang menjadi DHCP Server)'

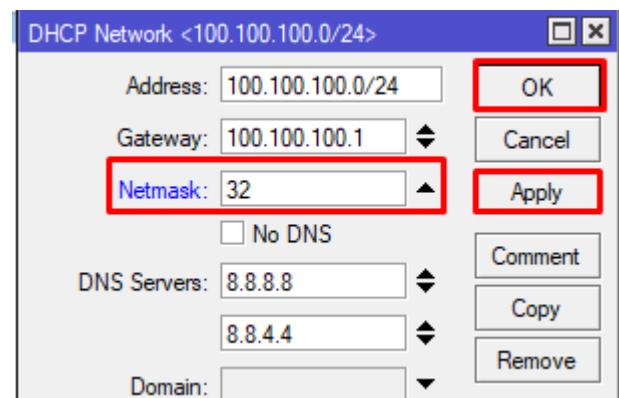
Name	Type	Actual MTU	L2 MTU	Trx	Px
R wlan1	Wireless (Atheros AR9300)	1500	1600	4.2 kbps	19.1 k
♦ pwr-line 1	PWR	1500	1598	0 bps	0
♦ ether4	Ethernet	1500	1598	0 bps	0
♦ ether3	Ethernet	1500	1598	0 bps	0
R ether2	Ethernet	1500	1598	105.6 kbps	19.9 k
♦ ether1	Ethernet	1500	1598	0 bps	0

- Pada menu general, kita isikan:
- ARP: reply-only

Name:	wlan1
Type:	Wireless (Atheros AR9300)
MTU:	1500
Actual MTU:	1500
L2 MTU:	1600
MAC Address:	74:4D:28:81:83:37
ARP:	reply-only
ARP Timeout:	[empty]

Kemudian, kita edit lagi DHCP Server Networknya

- Klik menu 'IP>DHCP Server>Networks> (Networks yang kita buat)
- Edit Netmask menjadi: 32
- Jika sudah 'apply' lalu 'ok'



Jika sudah, maka router Mikrotik kita akan aman dari serangan NetCut.

# HOTSPOT

## OVERVIEW

Apa itu Hotspot?

Kebanyakan orang menyebut jika terdapat akses internet yg di sebarluaskan via wireless di public area (cafe,mall,dsb) itu adalah layanan Hotspot, Sedangkan sebenarnya Hotspot di Mikrotik adalah sebuah system untuk memberikan fitur autentikasi pada user yang akan menggunakan jaringan. Jadi untuk bisa akses ke jaringan, client diharuskan memasukkan username dan password pada login page disediakan.

Hotspot dan WiFi pada Mikrotik itu berbeda.

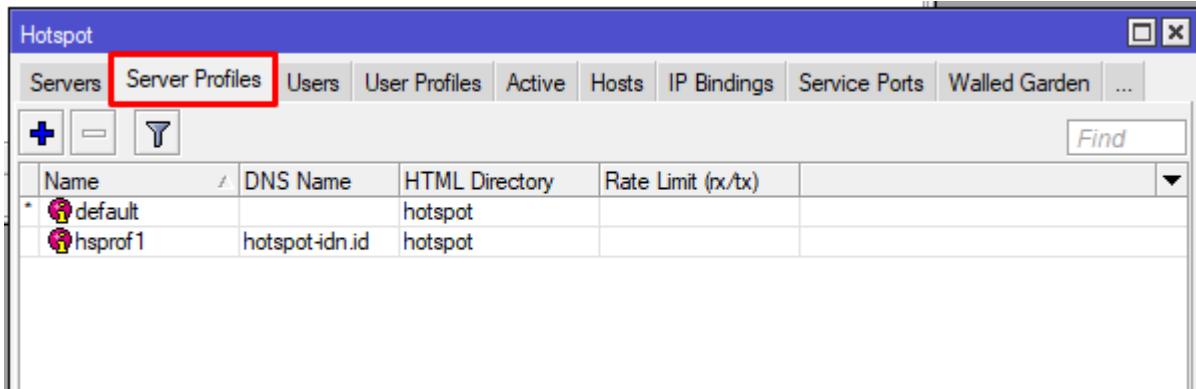
**WiFi:** Suatu fitur wireless yang digunakan untuk membagikan layanan internet. Bisa diakses di MikroTik dengan membuat Access Point pada interface wireless.

**Hotspot:** Suatu fitur wireless dalam MikroTik yang fungsinya hampir sama seperti wifi, yaitu untuk membagikan layanan internet, hanya saja hotspot dapat dibagikan juga lewat interface LAN/ether tidak hanya interface wireless. Namun untuk dapat mengakses internet, klien harus melewati autentikasi hotspot yang berupa user hotspot dan passwordnya yang diisi pada hotspot gateway.

Didalam hotspot, terdapat beberapa konfigurasi yang kita gunakan untuk mempermudah dalam pelayanan hotspot

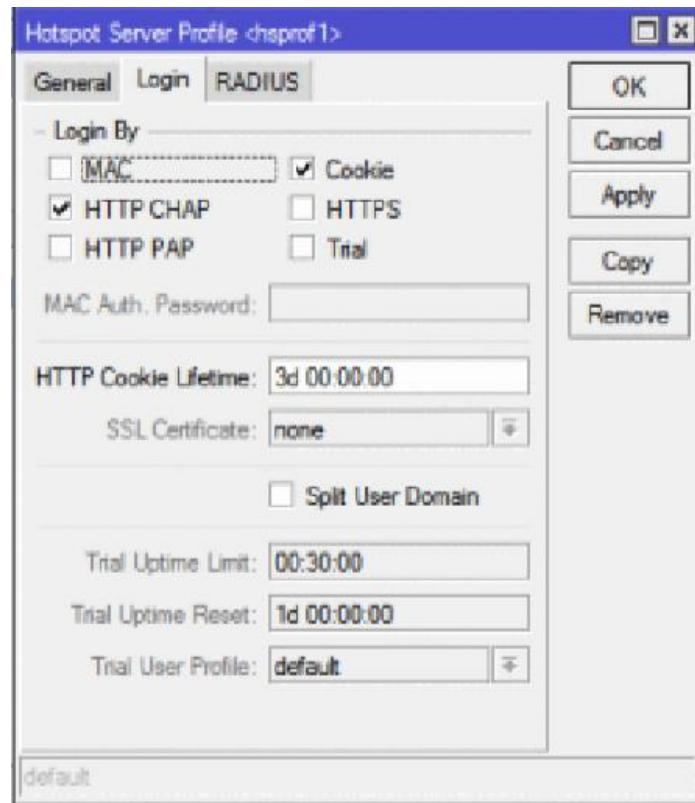
## FITUR-FITUR HOTSPOT:

### 1. Server Profiles



Fungsi dari server profiles, yaitu menyimpan konfigurasi umum pada suatu hotspot servers atau lebih.

Didalam server profiles, terdapat konfigurasi login/metode autentikasi pada klien. Terdapat 6 cara:



**MAC Address:** metode ini akan mengautentikasi user mulai dari user tersebut muncul di ‘host-list’, dan menggunakan MAC address dari client sebagai username dan password.

**HTTP CHAP:** metode standard yang mengintegrasikan proses CHAP pada proses login.

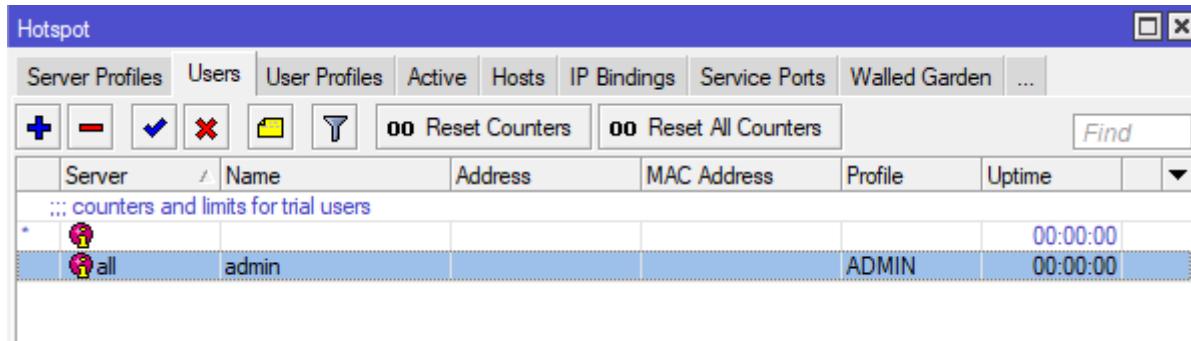
**HTTP PAP:** metode autentikasi yang paling sederhana, yaitu menampilkan halaman login dan mengirimkan info login berupa plain text.

**HTTPS:** menggunakan Enkripsi Protocol SSL untuk Autentikasi.

**HTTP Cookie:** setelah user berhasil login data cookie akan dikirimkan ke webbrowser dan juga disimpan oleh router di ‘Active HTTP cookie list’ yang akan digunakan untuk autentikasi login selanjutnya.

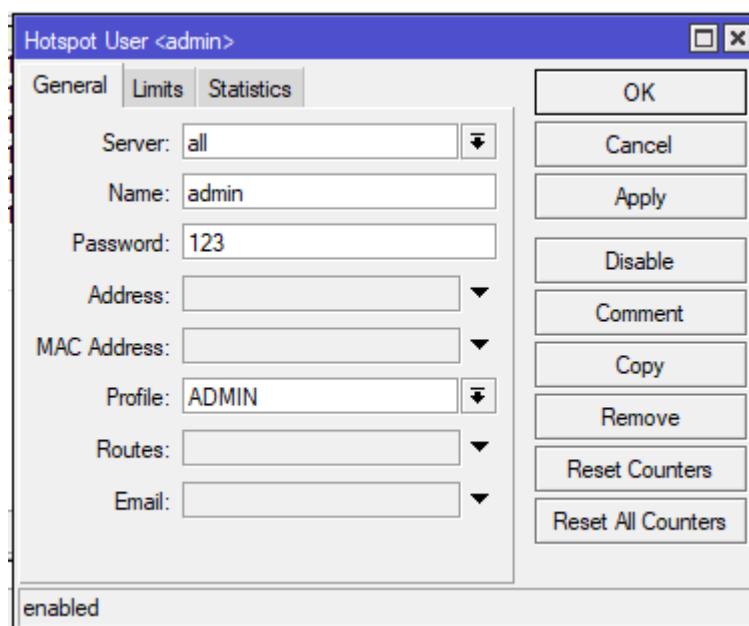
**Trial:** User tidak memerlukan autentikasi pada periode waktu yang sudah ditentukan.

## 2. Users



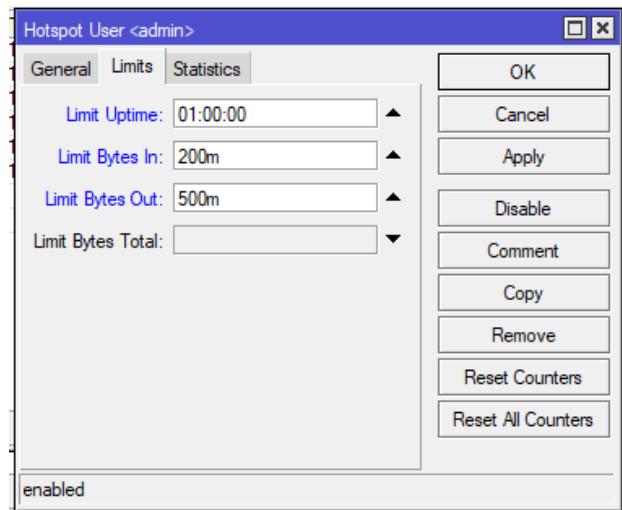
Pada menu hotspot ini, kita bisa membuat dan memanajemen user/klien yang dapat terhubung kedalam hotspot.

Jika kita klik users tersebut, didalamnya akan ada 3 menu:



**A. General:** Berisi tentang konfigurasi dasar pada user hotspot tersebut.

Seperti server yang user tersebut gunakan, nama user dan passwordnya



**B. Limit:** Berisi tentang pembatasan yang dapat kita atur pada user.

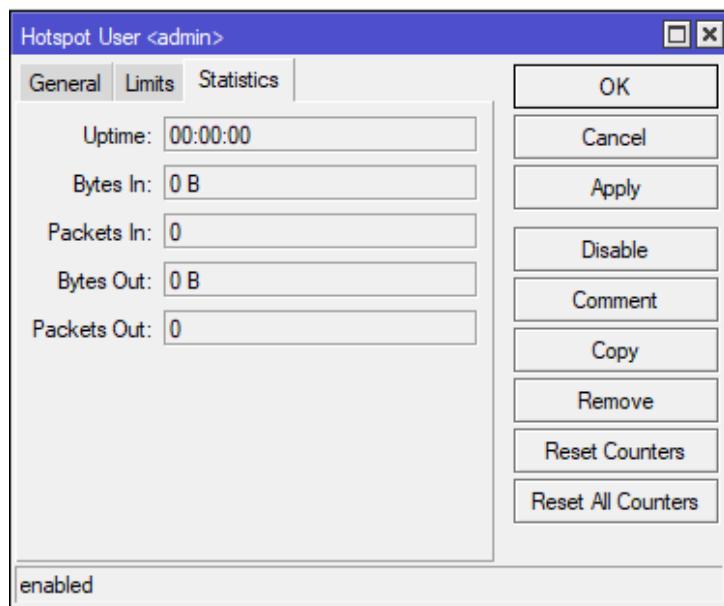
**Limit Uptime:** Pembatasan waktu pada user. Jika waktu yang ditentukan sudah habis, maka user tersebut akan ter-disable secara otomatis.

**Limit Bytes In:** Pembatasan packet upload

**Limit Bytes Out:** Pembatasan packet download

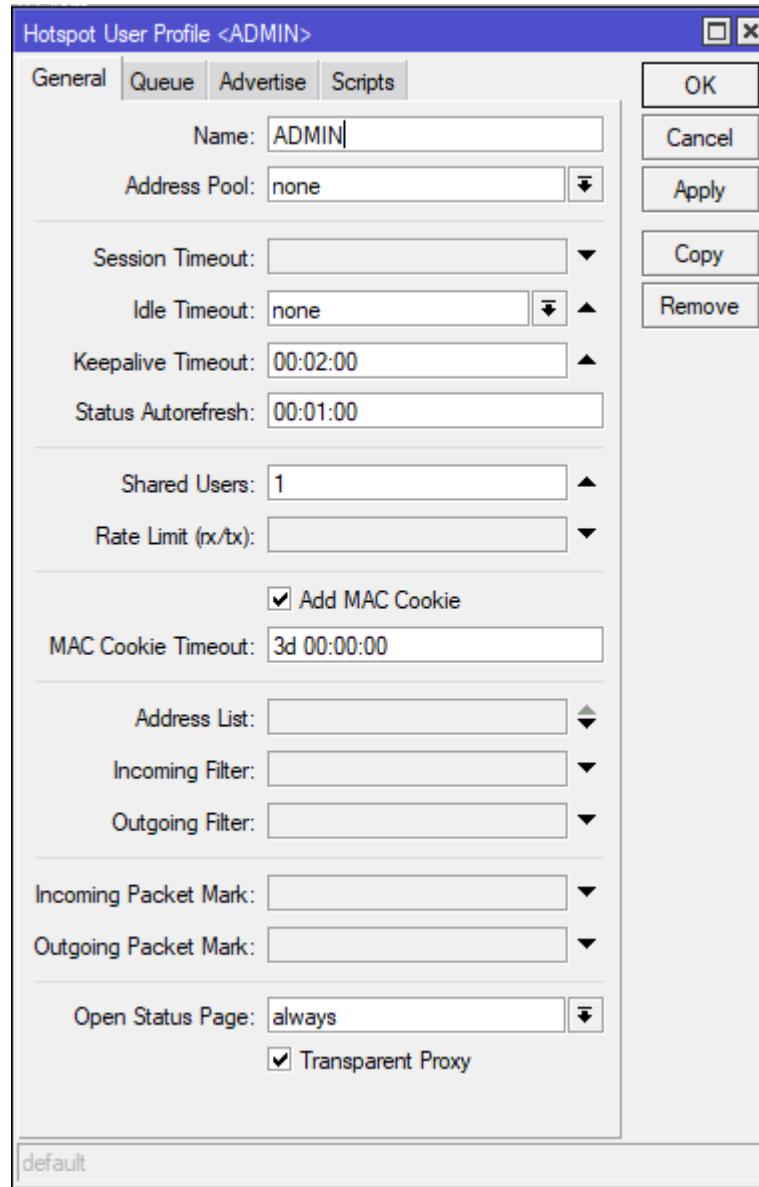
**Limit Bytes Total:** Total pembatasan antara upload dan download.

**C. Statistics:** Berisi tentang statistik penggunaan user tersebut.



### 3. User Profiles

User Profiles, merupakan konfigurasi dasar dalam sebuah user yang berbentuk profil. User profiles ini dapat digunakan oleh satu user/lebih.



**Keterangan:**

**General:** digunakan untuk mengkonfigurasi User

**Address pool:** Daftar IP yang akan dibagikan ke pengguna user

**Time-out:** Untuk mencegah monopoli oleh user

**Data rate:** Kecepatan akses

**Session time:** Sesi akses

**Shared Users:** Mensharing banyak user yang dapat menggunakan Hotspot tersebut dengan satu akun

**Address List:** IP user akan ditambahkan ke dalam firewall addresslist sesuai list yang ditentukan

**Incoming Filter:** Nama chain baru untuk trafik yang berasal dari IP user (trafik upload)

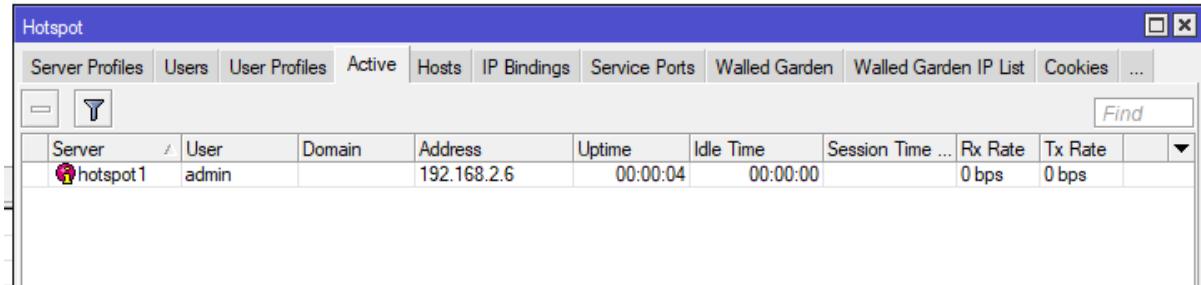
**Outgoing Filter:** Nama chain baru untuk trafik yang menuju IP user (trafik download)

**Incoming Packet Mark:** Nama packet-mark untuk trafik yang berasal dari IP user (trafik upload)

**Outgoing Packet Mark:** Nama packet-mark untuk trafik yang menuju IP user (trafik download)

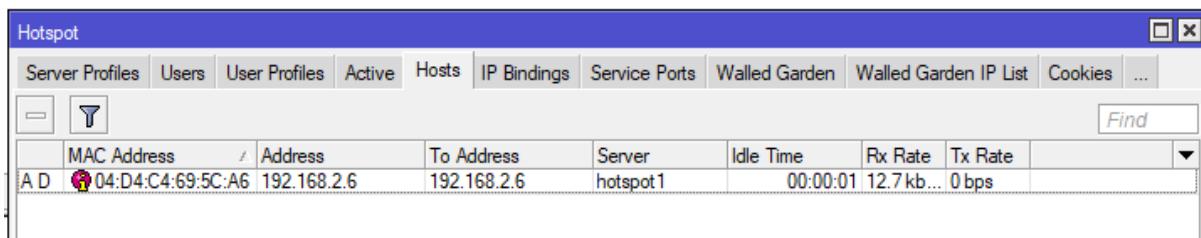
**Advertise:** Dengan menggunakan fitur advertisement pada Hotspot server, berfungsi untuk menampilkan popup halaman sebuah web ke user dan popup-popup yang akan muncul bisa anda atur intervalnya.

**4. Active:** Berisi informasi users yang sedang aktif namun belum mendapat IP (terhubung)



Server	User	Domain	Address	Uptime	Idle Time	Session Time ...	Rx Rate	Tx Rate
hotspot1	admin		192.168.2.6	00:00:04	00:00:00		0 bps	0 bps

**5. Host:** Berisi informasi users yang aktif dan sudah terhubung kedalam hotspot.



MAC Address	Address	To Address	Server	Idle Time	Rx Rate	Tx Rate
A D 04:D4:C4:69:5C:A6	192.168.2.6	192.168.2.6	hotspot1	00:00:01	12.7 kb... 0 bps	

Keterangan/flag user dalam hotspot:

**S:** User sudah ditentukan IP nya didalam IP binding

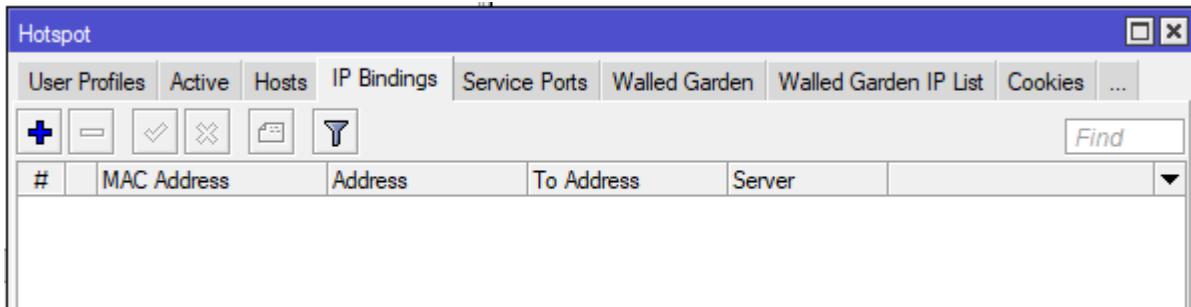
**H:** User menggunakan IP DHCP

**D:** User menggunakan IP static

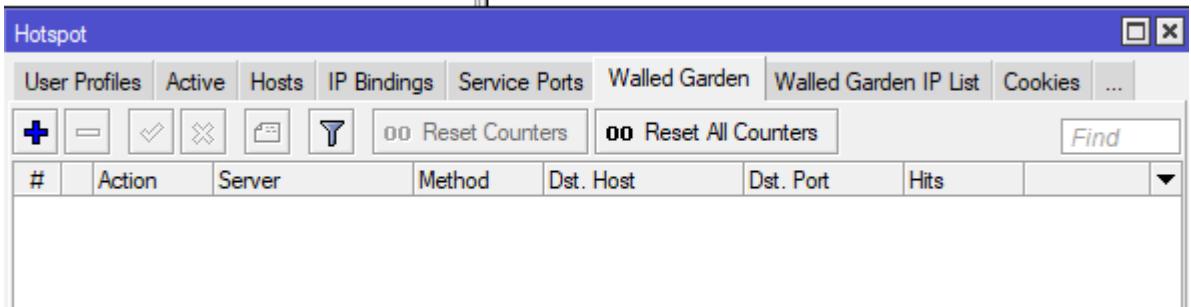
**A:** User sudah melakukan login / Autentikasi

**P:** User di bypass pada IP binding

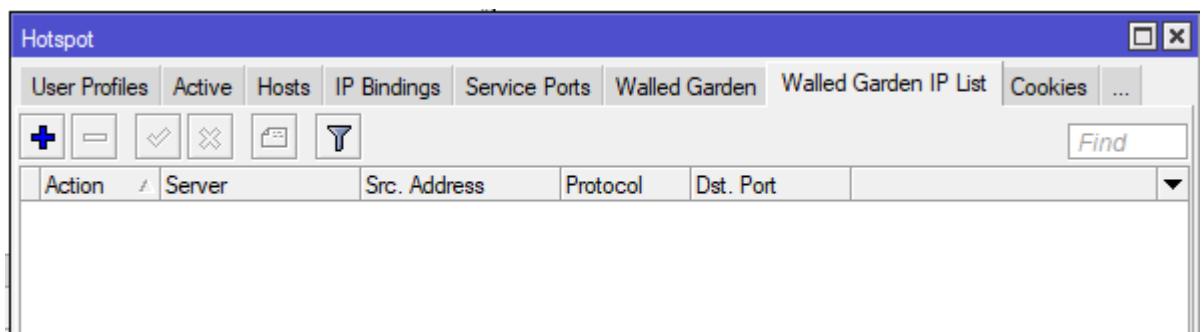
**6. IP Binding:** Bypass host terhadap authentication, block akses dari host tertentu berdasarkan mac address/ip address asli .



**7. Walled Garden:** Walled garden itu sebuah sistem yang memungkinkan untuk user yang belum terautentikasi menggunakan bypass beberapa resource jaringan tertentu tetapi tetap memerlukan autentikasi jika ingin menggunakan resource yang lain.



**8. Walled Garden IP List:** Walled garden ip-list mampu melakukan bypass terhadap resource yang lebih spesifik pada protocol dan port tertentu. Biasanya digunakan untuk melakukan bypass terhadap server local yang tidak memerlukan autentikasi.

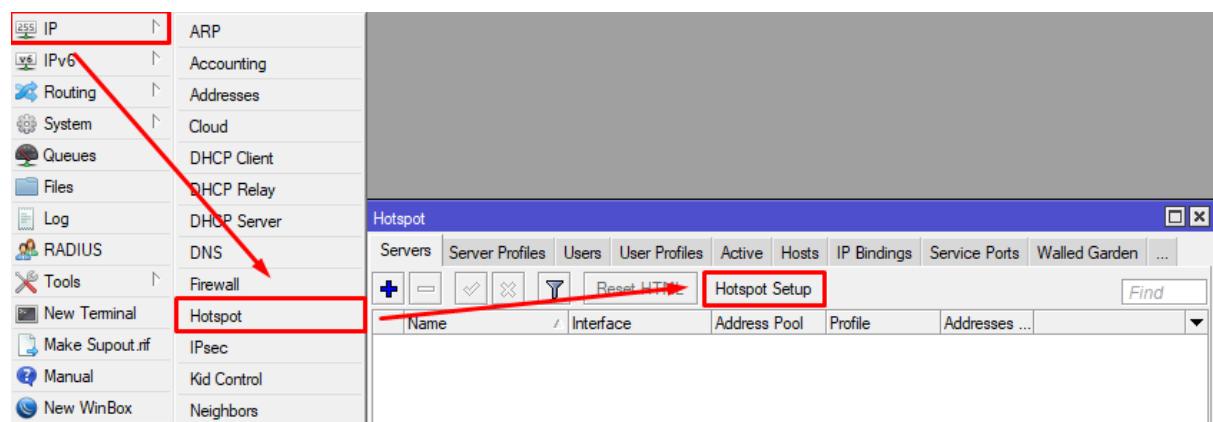


## HOTSPOT SETTING

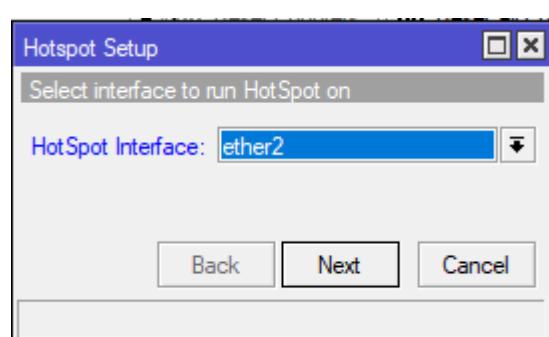
Untuk cara pembuatan hotspot, tidak jauh berbeda dengan membuat DHCP Server, ada yang manual dan ada yang otomatis (hotspot setup). Kita mulai dengan yang otomatis terlebih dahulu.

### 1. Setting Hotspot Otomatis (Hotspot Setup)

Pertama klik 'IP>Hotspot>Hotspot Setup'

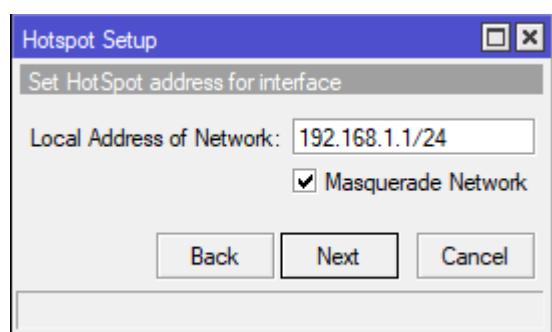


Kemudian kita ikuti setup nya.



#### Hotspot Interface: ether2

Interface yang akan kita pilih untuk dijadikan hotspot.

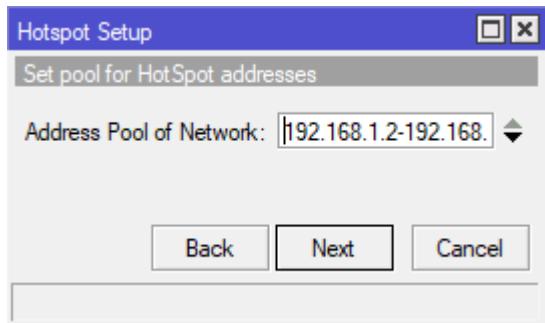


#### Local Address of Network:

**192.168.1.1/24**

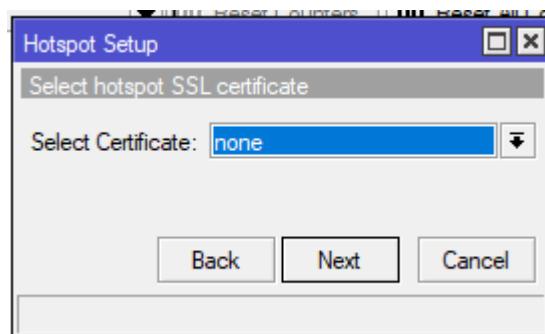
IP Address router/ IP Address yang akan menjadi gateway hotspot.

Centang **Masquerade Network**



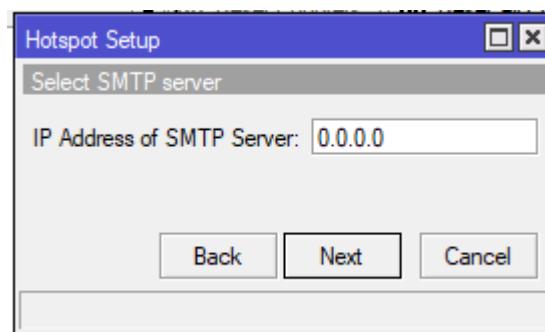
**Address Pool of Network: 192.168.1.2 – 192.168.1.254**

Daftar IP Address yang akan diberikan kepada klien



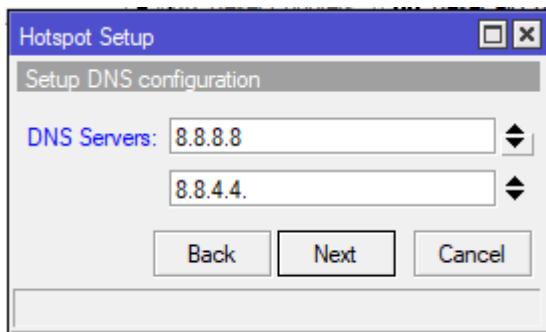
**Select Certificate: none**

Sertifikat yang akan dipasang pada hotspot. Jika tidak ada, cukup isikan none.



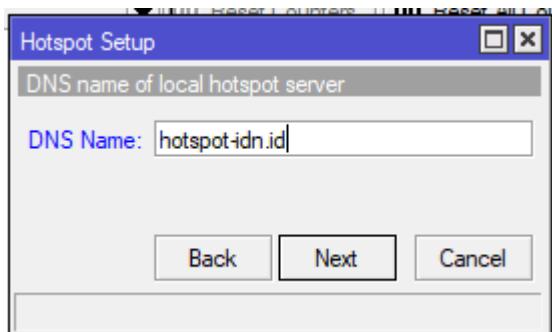
**IP Address of SMTP Server: 0.0.0.0**

IP Address dari SMTP (Simple Mail Transfer Protocol) yang akan digunakan pada hotspot



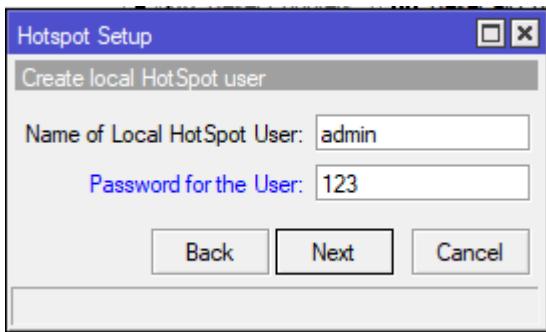
### DNS Servers: 8.8.8.8, 8.8.4.4.

DNS Servers yang akan diberikan kepada klien



### DNS Name: hotspot-idn.id

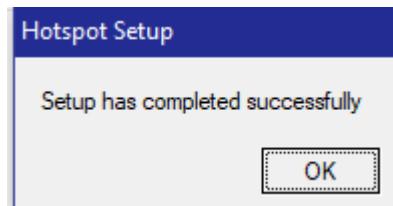
Domain dari hotspot gateway yang akan kita gunakan.



### Name of Local HotSpot User: admin

### Password for User: 123

User dan password yang akan kita gunakan di Hotspot. (kita juga bisa mengosongi password)



Jika sudah, maka konfigurasi hotspot secara dasar sudah kita buat.

Agar klien bisa mengakses internet perlu memasuki hotspot gateway terlebih dahulu.

Ketikkan DNS hotspot yang tadi kita sudah buat. '**hotspot-idn.id**' di browser.



Lalu kita akan memasuki hotspot gateway MikroTik. Kita isikan user yang tadi kita buat pada login dan password:

Please log on to use the internet hotspot service

- Login: admin
- Password: 123

Jika sudah klik 'ok'

A simple login form with two text input fields and one button. The first field is labeled 'login' and contains 'admin'. The second field is labeled 'password' and contains three dots ('•••'). Below the fields is a button labeled 'OK'.

### HOTSPOT GATEWAY

powered by **MikroTik**

Powered by MikroTik RouterOS

Welcome admin!

IP address:	192.168.1.2
bytes up/down:	50 B / 0 B
connected:	0s
status refresh:	1m

log off

Maka kita akan dapat mendapat IP dan dapat mengakses internet.

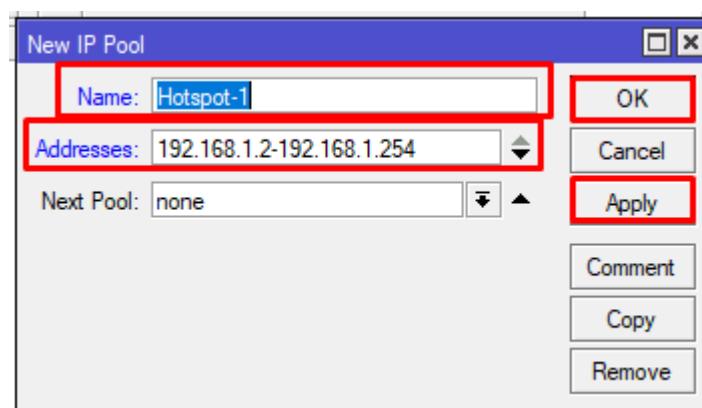
## **2. Setting Hotspot Manual.**

Hal-hal yang perlu kita buat dalam setting manual adalah :

1. Hotspot Server
2. Hotspot Profiles
3. User
4. User Profiles
5. IP Pool
6. DNS

Pertama-tama kita buat IP Pool (daftar IP Address yang nantinya akan diberikan kepada klien).

- klik 'IP>Pool' lalu kita buat baru '+' kita isikan:

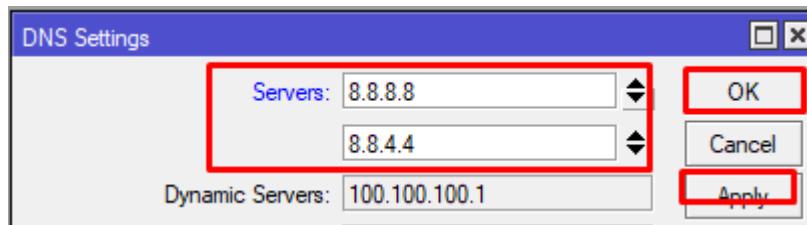


- Name: Hotspot-1 (bebas)
- Addresses: 192.168.1.2 – 192.168.1.254
- Jika sudah 'apply' kemudian 'ok'

Maksud dari IP Pool ini adalah: kita memberikan IP 192.168.1.2, 192.168.1.3 dan seterusnya hingga IP 192.168.1.254 kepada klien.

Selanjutnya kita setting DNS Server yang akan digunakan oleh Hotspot.

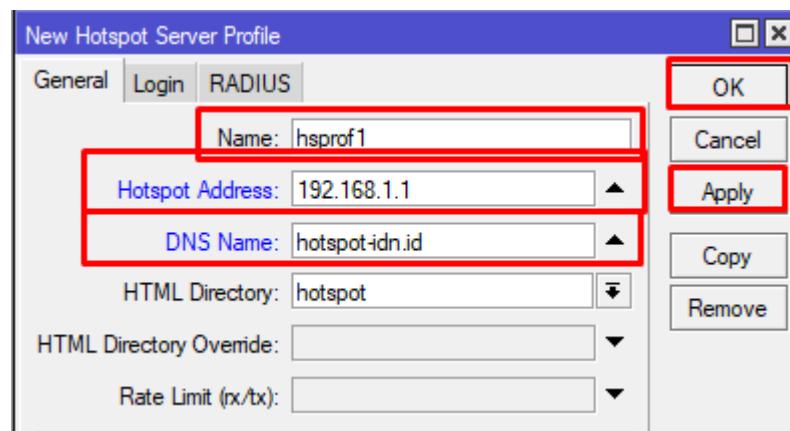
Klik 'IP>DNS' isikan:



- Servers: 8.8.8.8, 8.8.4.4.
- Jika sudah 'apply' lalu 'ok'

Selanjutnya kita buat Server Profiles dahulu sebelum kita membuat Hotspot Server.

Klik 'IP>Hotspot>Server Profiles> add '+' kita isikan:



- Name: hsprof1
- Hotspot Address: 192.168.1.1 (yang berfungsi menjadi hotspot gateway/ IP Address interface yang menjadi hotspot)
- DNS Name: hotspot-idn.id (Domain dari hotspot gateway yang akan kita gunakan.)

Lalu baru kita buat Hotspot Servernya.

Klik 'IP>Hotspot>Servers>add '+' kita isikan:



- Name: Hotspot IDN (bebas)
- Interface: ether2 (interface yang akan menjadi hotspot server)
- Address Pool: Hotspot-1 (ip address yang akan dibagikan kepada klien)
- Profile: hsprof1 (hotspot profiles yang tadi kita buat)
- Jika sudah 'apply' lalu 'ok'

Beginilah hasilnya:

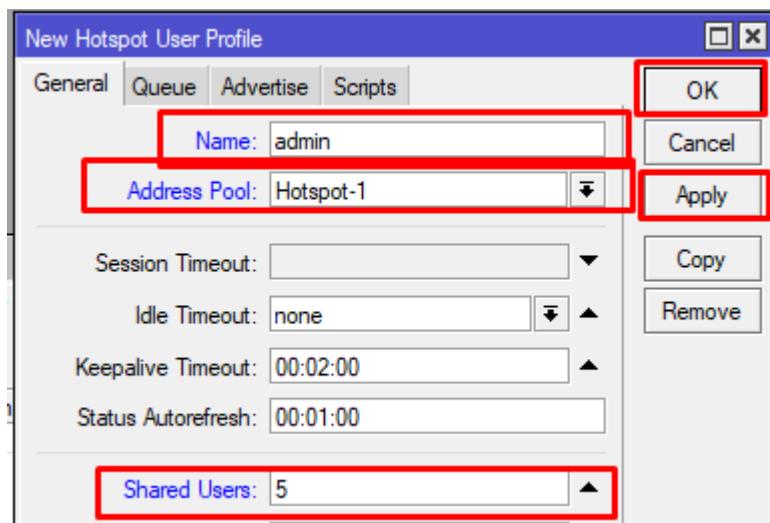
Servers	Server Profiles	Users	User Profiles	Active	Hosts	IP Bindings	Service Ports	Walled Garden	Walled Garden IP List	...
<a href="#">Reset HTML</a>	<a href="#">Hotspot Setup</a>								<a href="#">Find</a>	

Name	Interface	Address Pool	Profile	Addresses ...
Hotspot IDN	ether2	Hotspot-1	hsprof1	

Langkah selanjutnya, kita perlu membuat user profiles terlebih dahulu sebelum membuat user.

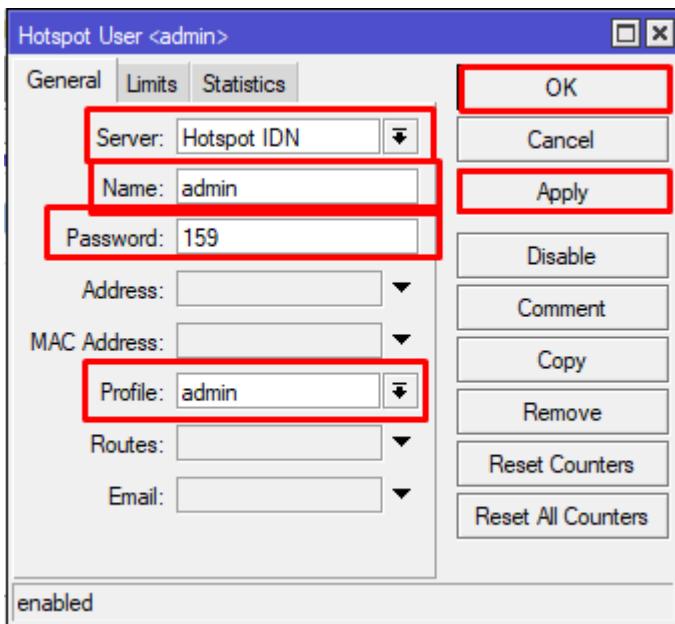
Klik 'IP>hotspot>User Profiles>add '+' kita isikan:



- Name: admin (bebas)
- Address Pool: Hotspot-1 (IP Pool yang tadi kita buat)
- Shared User: 5 (jumlah klien yang bisa menggunakan user admin)
- Jika sudah 'apply' lalu 'ok'

Kemudian barulah kita membuat user untuk hotspotnya.

Klik 'IP>hotspot>users>add '+' kita isikan:



- Server: Hotspot IDN (hotspot server yang tadi kita buat)
- Name: admin (nama user)
- Password: 159 (password untuk user admin)
- Profile: admin (user profiles yang tadi kita sudah buat)
- Jika sudah 'apply' lalu 'ok'

Kita sudah berhasil membuat hotspot dengan cara manual.

Agar klien bisa mengakses internet perlu memasuki hotspot gateway terlebih dahulu.

Ketikkan DNS hotspot yang tadi kita sudah buat. '**hotspot-idn.id**' di browser.



Lalu kita akan memasuki hotspot gateway MikroTik. Kita isikan user yang tadi kita buat pada login dan password:

Please log on to use the internet hotspot service

- Login: admin
- Password: 159

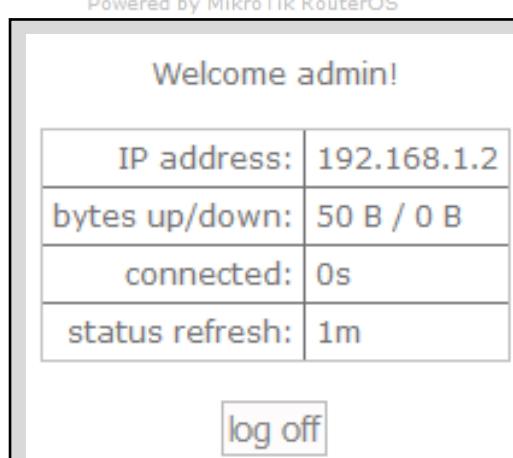
Jika sudah klik 'ok'

A simple login form with two text input fields and one button. The first field is labeled 'login' and contains 'admin'. The second field is labeled 'password' and contains three dots ('•••'). Below the fields is a button labeled 'OK'.

HOTSPOT GATEWAY

powered by **MikroTik**

Maka kita akan dapat mendapat IP



## **IP BINDING**

Seperti yang sudah saya jelaskan sebelumnya pada **Fitur-fitur Hotspot**.

Fungsi dari IP Binding yaitu mengizinkan klien lewat IP Address/Mac Address agar dapat langsung terkoneksi ke internet tanpa harus melewati hotspot gateway pada saat terkoneksi, selain mengizinkan, kita juga bisa menolaknya.

IP-Binding adalah menu HotSpot yang memungkinkan untuk setup statis One-to-One NAT translation, memungkinkan untuk memotong klien HotSpot tertentu tanpa otentikasi apapun, dan juga memungkinkan untuk memblokir host tertentu dan subnet dari jaringan HotSpot,

### **TYPE IP BINDING:**

**Blocked:** IP Address/Mac address yang didaftarkan dengan type ini otomatis tidak akan mendapatkan layanan hotspot.

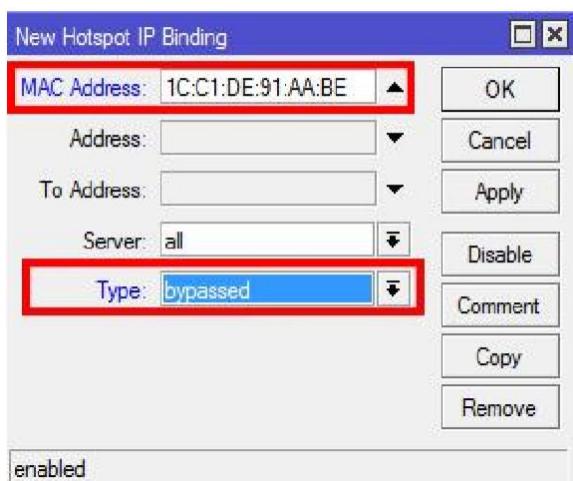
**Bypassed:** IP Address/Mac address yang didaftarkan dengan type ini akan dibypass sehingga tidak perlu melewati proses autentikasi.

**Regular:** IP Address/Mac address yang didaftarkan dengan type ini akan melewati proses autentikasi seperti user biasa, misalkan digunakan hanya untuk mengalokasikan ip address khusus ke host tertentu.

## Contohnya:

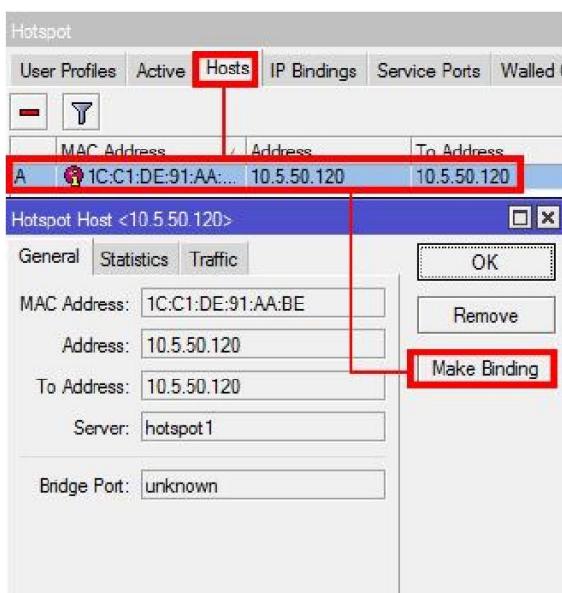
Kita akan membuat klien dengan Mac Address '1C:C1:DE:91:AA:BE' dapat mengakses internet tanpa harus melewati hotspot gateway.

- Klik 'IP>Hotspot>IP Binding' kita buat baru '+' lalu kita isikan:



- MAC Address: 1C:C1:DE:91:AA:BE
- Type: bypasses
- Jika sudah 'apply' lalu 'ok'

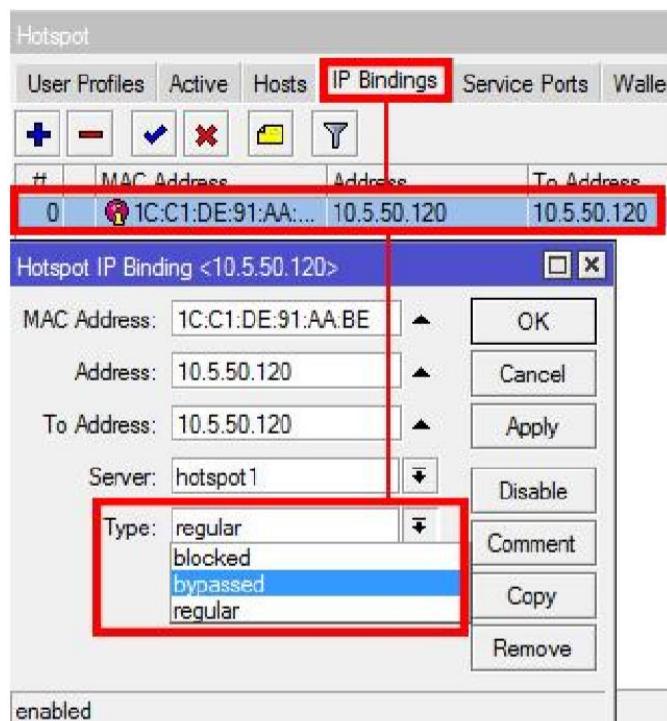
Jika konfigurasi sudah, maka klien dengan MAC Address 1C:C1:DE:91:AA:BE sudah dapat terkoneksi ke internet tanpa harus melewati hotspot gateway.



Selain itu, kita juga dapat membuat IP Binding dengan klien yang sedang terkoneksi pada hotspot.

- Caranya klik 'host>lalu klik host yang aktif'
- Pilih Make Binding

Selanjutnya kita hanya perlu mengonfigurasi type ip bindingnya.



- Klik 'IP Binding>pilih klien yang sudah ter-binding tadi'
- Pilih type: bypassed

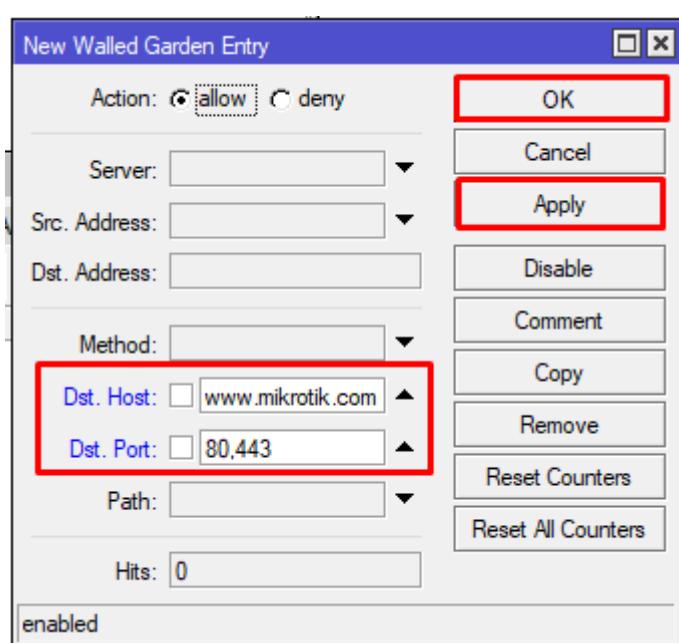
Jika sudah, maka klien tersebut tidak perlu login lagi untuk mengakses internet hotspot.

## Walled Garden

Sama seperti yang saya jelaskan pada **Fitur-fitur Hotspot**. Fungsi dari Walled Garden, yaitu bisa membuat user yang belum login ke hotspot gateway namun sudah terhubung ke hotspot dapat mengakses internet namun hanya pada settingan tertentu, seperti akses situs.

Contohnya kita akan membuat klien yang belum login dapat mengakses situs mikrotik.com

- Klik menu 'IP>Hotspot>Walled Garden' kita buat baru '+' kita isikan:



- Dst. Host:  
[www.mikrotik.com](http://www.mikrotik.com)
- Dst. Port: 80, 443 (Port HTTP dan HTTPS)
- Kemudian 'apply' lalu 'ok'
- Jika sudah 'apply' lalu 'ok'

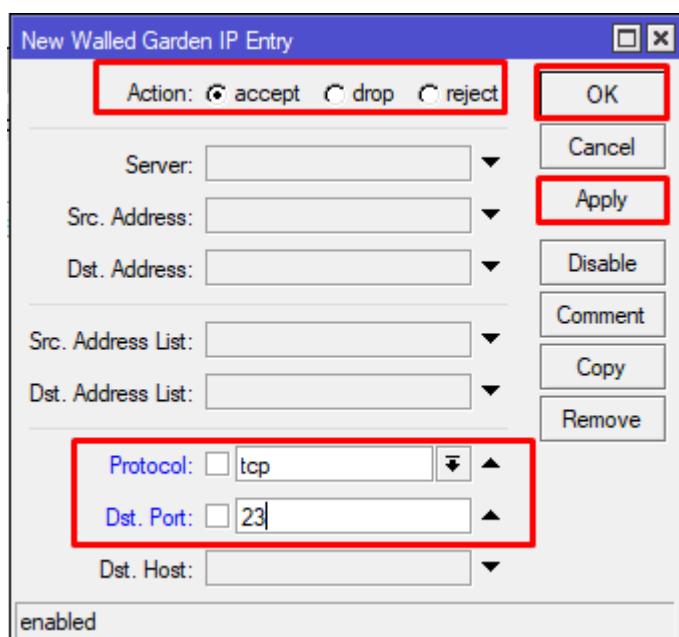
Dengan begini, klien dapat mengakses situs Mikrotik meskipun belum login kedalam hotspot.

## Walled Garden IP List

Sama seperti yang saya jelaskan di **Fitur-fitur hotspot**. Fungsinya hampir sama seperti Walled Garden tetapi dapat melakukan bypass terhadap resource yang lebih spesifik pada protocol dan port tertentu. Biasanya digunakan untuk melakukan bypass terhadap server local yang tidak memerlukan autentikasi.

Contohnya kita akan mencoba bypass trafik pada telnet.

- Klik 'IP>Hotspot>Walled Garden IP List' kita buat baru '+'



Kita isikan:

- Action: accept
- Protocol: tcp
- Dst. Port: 23 (telnet)

Jika sudah, maka akses telnet diizinkan.

## Catatan:

# TENTANG PENULIS



Beliau bernama Muhammad Adib Aulia Nurkhafif, Lahir di Pekalongan 11 April 2004. Panggilannya Adib, ia tinggal di Desa Sijono, Kecamatan Warungasem, Kabupaten Batang, usianya masih lima belas ketika menuliskan buku ini.

Sejak kecil ia sudah dikenalkan dengan berbagai macam teknologi yang menjadikan ia menyukai teknologi, hingga akhirnya pada saat lulus SMP, ia memutuskan untuk masuk kedalam SMK IDN demi memperdalam ilmunya dibidang teknologi.

Dan kini, diusianya yang masih dibilang muda, ia telah mendapatkan dua sertifikat internasional bergengsi yang pada masanya anak SMK jarang yang memiliki. Sekarang, ia masih duduk di bangku Sekolah SMK IDN dan masih kelas sepuluh.

Jika ingin bertanya atau ingin mengenal penulis lebih dalam, kalian bisa menghubunginya di:



Telepon: +6282241033809

Email: adibnk11@gmail.com

Instagram: adib\_nk

WhatsApp: +6282241033809

Facebook: Nur Khafif