

MikroTik Academy STT Terpadu Nurul Fikri



Mikrotik Certified Network
Associate
(MTCNA)

Kata Pengantar

Buku ini merupakan modul bagi siswa yang belajar di Mikrotik Academy Stt Nurul Fikri untuk materi MikroTik Certified Network Associate (MTCNA). Ucapan terima kasih kepada semua pihak yang sudah membantu dalam hal penulisan dan koreksi demi kesempurnaan buku ini. Buku ini ditulis oleh trainer dan alumni kelas MTCNA di Mikrotik Academy Stt Nurul Fikri, mereka adalah April Rustianto, SKomp, M.T, Fikri Maulana, Rachmat, Erwin Gumulya, Slamet Santoso, Moch Hafied Fajar N, Ali Imran.

Penulis berharap modul ini dapat membantu siswa dalam mempelajari materi MTCNA lebih baik sehingga dapat menambah keilmuan dari peserta training. Masukan, kritikan dan sumbangsih dalam hal penulisan sangat kami harapkan demi perbaikan materi pada modul ini.

Akhir kata selamat belajar, dan teruslah memacu diri menjadi lebih baik sesuai dengan pepatah *orang yang hari ini lebih baik dari hari kemarin adalah orang yang beruntung*



Daftar Isi

Kata Pengantar	2
Daftar Isi	3
Persiapan Awal	4
Modul 1 Introduction	5
Modul 2 DHCP	28
Modul 3 Bridging	36
Modul 4 Routing	41
Modul 5 Wireless	47
Modul 6 Firewall	69
Modul 7 Tunneling	93
Modul 8 QoS	106
Modul 9 Mikrotik RouterOS Tool	113
Testimoni	117



Persiapan Awal

Sebelum memulai training MTCNA peserta diharapkan melakukan beberapa hal dibawah ini:

1. Membuat akun mikrotik terlebih dahulu di www.mikrotik.com. Pastikan data diri yang anda masukan benar (baik huruf besar maupun kecil). Data tersebut akan digunakan sebagai referensi pada saat pembuatan sertifikat MTCNA setelah ujian akhir anda lulus.
2. Menyerahkan email masing-masing yang digunakan untuk membuat akun di website mikrotik ke trainer untuk dimasukan ke dalam kelas virtual
3. Buka email masing-masing dan cari email dari mikrotik.com untuk join ke kelas virtualnya.
4. Setelah join ke kelas virtual, peserta dapat mengerjakan latihan soal yang terdapat pada portal kelas virtual MTCNA pada website mikrotik.com

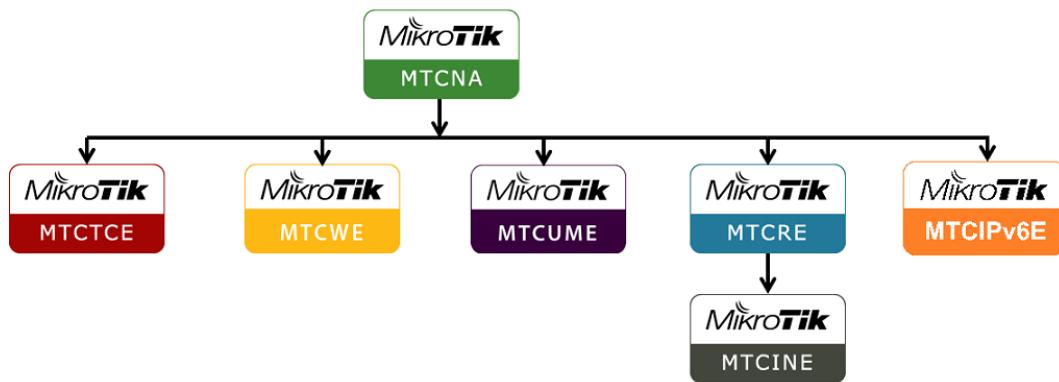
Mekanisme ujian sertifikasi MTCNA adalah sebagai berikut: ini:

1. Ujian sertifikasi MTCNA akan diadakan pada pertemuan terakhir, yaitu pertemuan ke-4 dari training
2. Ujian sertifikasi MTCNA dilakukan secara online selama 1 jam dan soal yang diberikan sebanyak 25 buah pilihan ganda.
3. Passing grade dari ujian sertifikasi MTCNA adalah 60%, jika peserta nilainya berada pada rentang 50%-59% dapat mengulang ujian sertifikasi MTCNA pada hari yang sama.
4. Peserta yang nilainya dibawah 50% tidak dapat mengulang ujian sertifikasi MTCNA pada hari yang sama dan harus mengikuti kelas selanjutnya.

Modul 1 Introduction

Sertifikasi MikroTik

Berikut ini merupakan track sertifikasi MikroTik RouterOS terbaru yang dapat diambil:



Berikut ini kepanjangan dari masing-masing sertifikasinya:

- MTCNA: MikroTik Certified Network Associate
- MTCRE : MikroTik Certified Routing Engineer
- MTCTCE : MikroTik Certified Traffic Control Engineer
- MTCWE : MikroTik Certified Wireless Engineer
- MTCUME : MikroTik Certified User Management Engineer
- MTCINE : MikroTik Certified Inter-networking Engineer
- MTCIPv6E : MikroTik Certified IPv6 Engineer

Masing-masing sertifikasi tersebut expire setelah 3 tahun, dan harus diperpanjang satu persatu dari level MTCNA, hingga level professional seperti MTCRE, dan MTCTCE.

Tentang MikroTik

MikroTik berdiri pada tahun 1996 yang berlokasi di Latvia. Pada awalnya di tahun 1997 MikroTik fokus membuat software untuk PC berbasis x86 yang dinamakan RouterOS yang berbasis Linux. Pada awal tahun ini belum tersedia

perangkat khusus dari MikroTik seperti RouterBoard. MikroTik baru mengeluarkan perangkat sendiri pada tahun 2002 yang dinamakan RouterBoard.

MikroTik RouterOS mempunyai banyak sekali fitur. Fitur-fitur yang dimiliki diantaranya adalah:

- Mendukung WiFi 802.11 a/b/g/n/ac
- Firewall dan bandwidth shaping
- Point-to-Point Tunneling (PPTP, PPPoE, SSTP, OpenVPN)
- DHCP, Procy, dan HotSpot
- Detil fitur dari MikroTik RouterOS dapat dilihat di wiki.mikrotik.com

Cara mengakses mikrotik

Terdapat beberapa cara untuk mengakses mikrotik yaitu melalui ssh, winbox, telnet, Dan web based (webfig).

1. Akses MikroTik via ssh



Berikut ini langkah-langkah untuk mengakses mikrotik menggunakan SSH:

1. Reset mikrotik jika sudah ada konfigurasi nya dengan cara hard reset / via software .
2. Koneksikan mikrotik ke laptop menggunakan kabel melalui ether 2
3. Pastikan ethernet pada laptop sudah satu jaringan dengan mikrotik, dan bisa melakukan ping ip ke router (192.168.88.1). Jika laptop tidak mendapatkan ip secara otomatis, atur ip nya secara manual menggunakan

ip address **192.168.88.2**, subnet mask **255.255.255.0**, dan default gateway **192.168.88.1**.

Network Connection Details

Property	Value
Connection-specific DN...	
Description	VMware Virtual Ethernet Adapter for VMn
Physical Address	00-50-56-C0-00-01
DHCP Enabled	No
IPv4 Address	192.168.88.2
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.88.1
IPv4 DNS Server	
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::14a7:53e1:2d21:5ef1%16
IPv6 Default Gateway	fec0:0:0:ffff::1%1
IPv6 DNS Servers	fec0:0:0:ffff::2%1 fec0:0:0:ffff::3%1

C:\WINDOWS\system32\cmd.exe

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

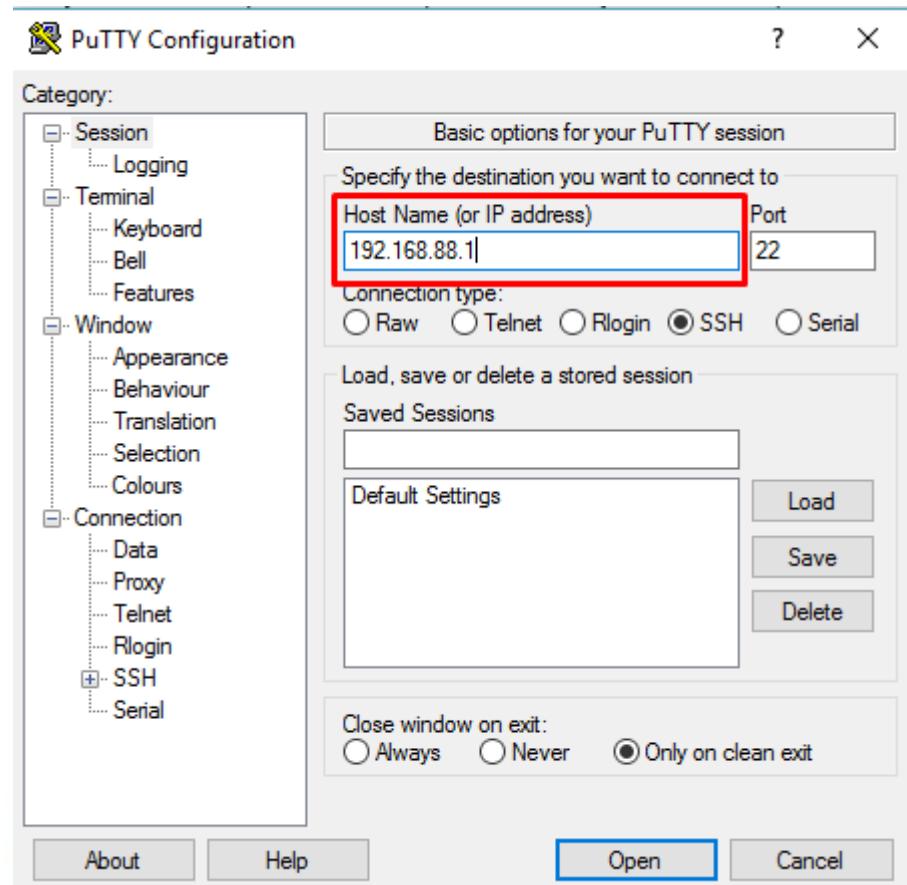
C:\Users\Fikri>ping 192.168.88.1

Pinging 192.168.88.1 with 32 bytes of data:
Reply from 192.168.88.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.88.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

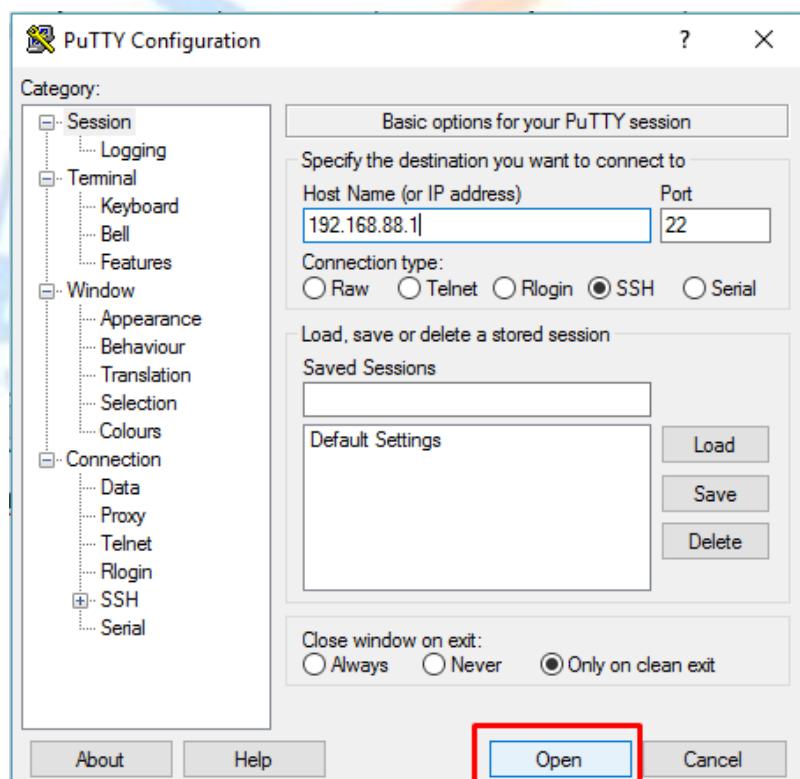
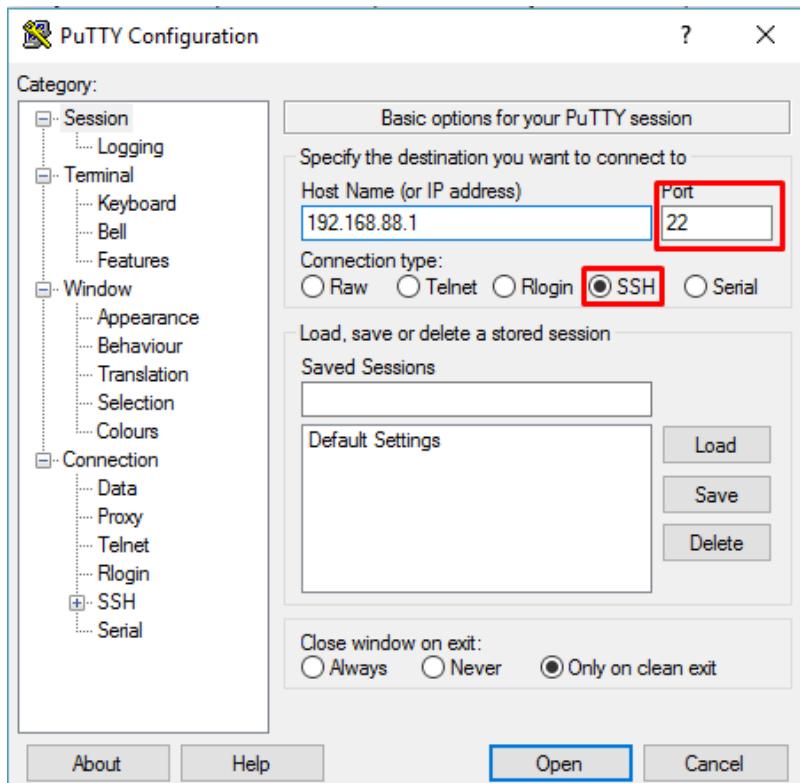
C:\Users\Fikri>
```

4. Untuk mengakses via ssh disini perlu software putty, pastikan laptop sudah terinstall putty.
5. Buka putty, dan masukan ip router (192.168.88.1) dan isikan port dengan 22 (port ssh)

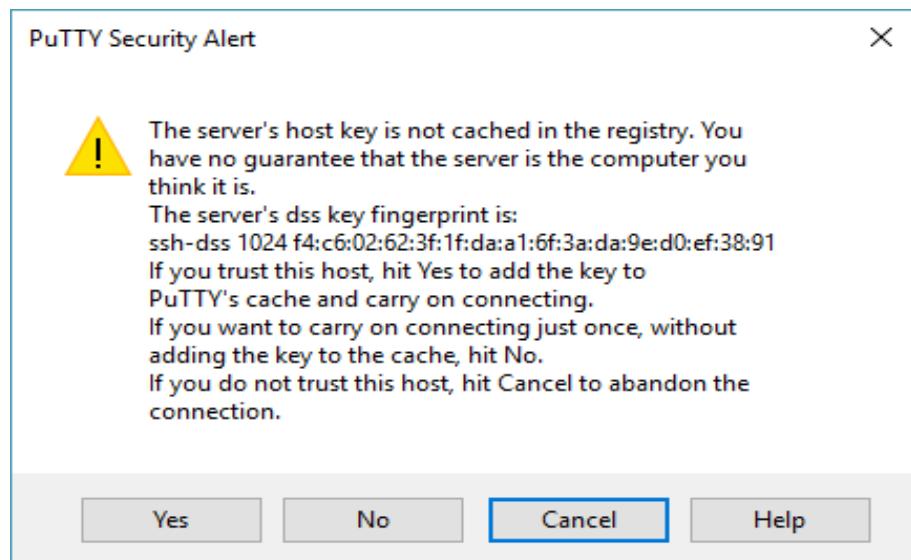


6. Pada putty, rubah connection typenya menjadi **SSH**, kemudian klik open

Sekolah Tinggi Terpadu NURUL FIKR



7. Maka tampilan nya akan seperti berikut.
8. Pilih yes, untuk masuk ke terminal mikrotik via SSH



9. Masukkan username dan password mikrotik (default user: admin password: (kosong)).



```
[admin@mikrotik-fikri] > [REDACTED]
```

192.168.88.1 - PuTTY

— □ X

```
MMM MMMM MMM III KKK KKK RRRRRR 000000 TTT III KKK KKK
MMM MM MMM III KKKKKK RRR RRR 000 000 TTT III KKKKKK
MMM MMM III KKK KKK RRRRRR 000 000 TTT III KKK KKK
MMM MMM III KKK KKK RRR RRR 000000 TTT III KKK KKK
```

MikroTik RouterOS 5.20 (c) 1999-2012 http://www.mikrotik.com/

ROUTER HAS NO SOFTWARE KEY

You have 19h22m to configure the router to be remotely accessible,
and to enter the key by pasting it in a Telnet window or in Winbox.
See www.mikrotik.com/key for more details.

Current installation "software ID": W5EY-LHT9
Please press "Enter" to continue!

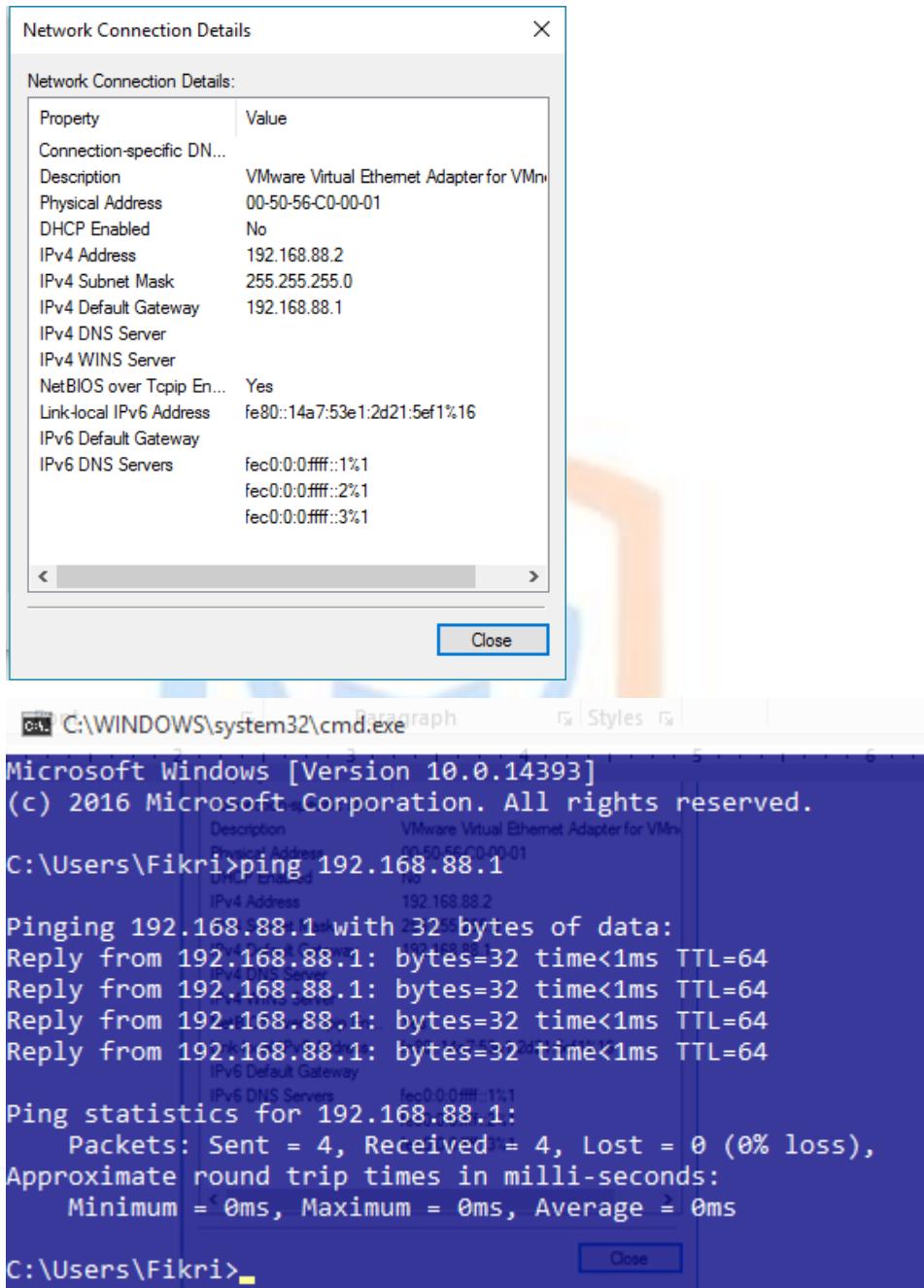
```
[admin@mikrotik-fikri] > [REDACTED]
```

2. Akses mikrotik via webfig



Berikut ini langkah-langkah untuk mengakses mikrotik menggunakan webfig:

1. Reset mikrotik jika sudah ada konfigurasi nya dengan cara hard reset / via software .
 2. Koneksikan mikrotik ke laptop menggunakan kabel melalui ether 2
 3. Pastikan ethernet sudah satu jaringan dengan mikrotik, dan bisa melakukan ping ke ip router (192.168.88.1)



4. Jika sudah terkoneksi ke router, buka browser dan ketik pada url alamat 192.168.88.1.
5. Maka tampilannya akan seperti berikut.

	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx
;;: defconf										
[D]	R	bridge	Bridge	1500	1598	144.8 kbps	23.1 kbps	20	21	0 bps
[D]	RS	ether1	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps
[D]	S	ether2	Ethernet	1500	1598	76.5 kbps	9.6 kbps	11	10	144.8 kbps
[D]	S	ether3	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps
[D]	S	ether4	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps
[D]	S	wlan1	Wireless (Atheros AR9)	1500	1600	0 bps	0 bps	0	0	0 bps

3. Akses mikrotik via winbox

Langkah – langkah untuk mengakses mikrotik via Winbox adalah sebagai berikut:

1. Reset mikrotik untuk menghapus konfigurasi yang sudah ada, dengan cara menekan tombol reset dan mencolokan kabel power ke mikrotik hingga panel lamput act yang terdapat pada mikrotik berkedip hingga selesai .
2. Download winbox pada laman web mikrotik.com
3. Sebelum membuka winbox, ada beberapa hal yang harus kita pastikan yaitu kita sudah harus mendapatkan ip dari mikrotik. Dengan cara **win + r** > **control panel > network and internet > network and sharing center > change adapter setting > klik kanan pada Ethernet > status > details** .

Network Connection Details	
Network Connection Details:	
Property	Value
Connection-specific DN...	
Description	Realtek PCIe GBE Family Controller
Physical Address	30-65-EC-11-98-2B
DHCP Enabled	Yes
IPv4 Address	192.168.88.251
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Monday, September 4, 2017 09:02:27
Lease Expires	Monday, September 4, 2017 09:27:28
IPv4 Default Gateway	192.168.88.1
IPv4 DHCP Server	192.168.88.1
IPv4 DNS Server	192.168.88.1

4. Kemudia kita ping ip default mikrotik apa sudah terkoneksi atau belum.

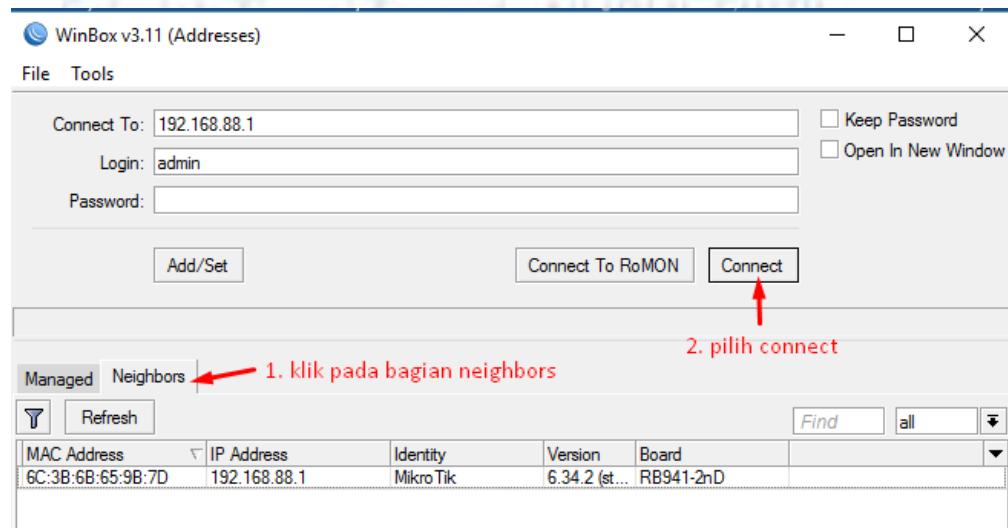
Buka cmd dan ping 192.168.88.1

```
Pinging 192.168.88.1 with 32 bytes of data: Wi-Fi
Reply from 192.168.88.1: bytes=32 time<1ms TTL=64
Reply from 192.168.88.1: bytes=32 time<1ms TTL=64
Reply from 192.168.88.1: bytes=32 time=1ms TTL=64
Reply from 192.168.88.1: bytes=32 time=1ms TTL=64

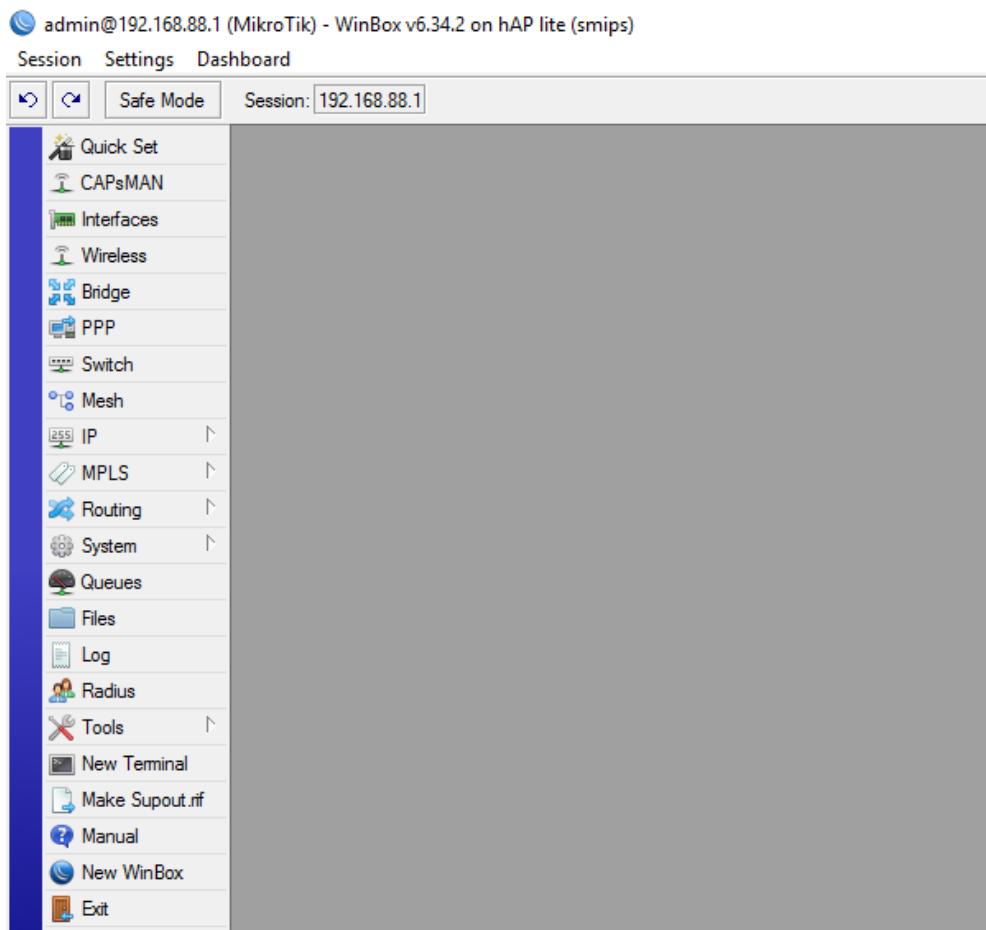
Ping statistics for 192.168.88.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Fikri>
```

5. Jika sudah terkoneksi, buka winbox dan pilih neighbors, kemudian isi login menggunakan: **admin** dan **kosongkan** password lalu connect .



6. Ini merupakan tampilan jika sudah berhasil ke mikrotik.



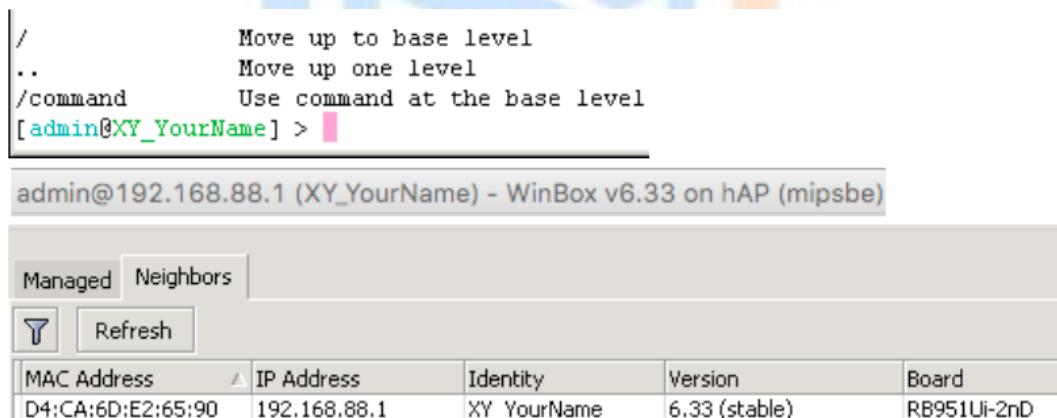
4. Akses Mikrotik via Command Line Interface (CLI)

Selain menggunakan winbox, MikroTik RouterOS juga dapat diakses menggunakan CLI. Perintah yang terdapat pada CLI dapat dilihat dengan melakukan double tab. Jika kita ingin menampilkan help dari suatu perintah dapat menggunakan karakter (?). Perintah yang tidak lengkap juga dapat dilengkapi secara otomatis jika kita melakukan tab. Berikut ini tampilan CLI pada Mikrotik RouterOS

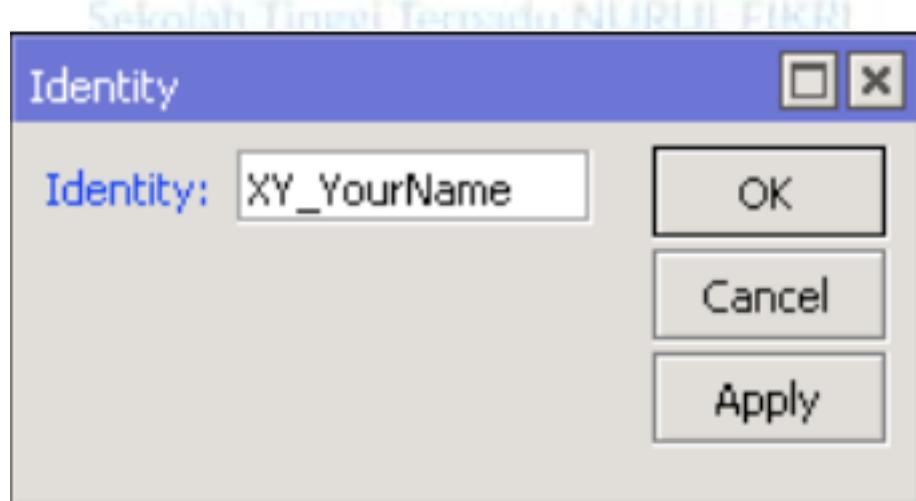
```
[admin@MikroTik] > /interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#      NAME                      TYPE      ACTUAL-MTU L2MTU
0      S ether1-gateway          ether      1500     1598
1      RS ether2-master-local    ether      1500     1598
2      S ether3-slave-local     ether      1500     1598
3      RS ether4-slave-local    ether      1500     1598
4      R  wlan1                  wlan      1500     1600
5      R  bridge-local           bridge    1500     1598
[admin@MikroTik] >
```

Router Identity

Router Identity merupakan nama atau hostname dari sebuah router. Nama sebuah router sangat diperlukan untuk memudahkan identifikasi perangkat. Berikut ini tampilan identity pada Mikrotik RouterOS



Router identity dapat dikonfigurasi dari menu System → identity. Tampilan menu Router identity dapat dilihat pada gambar dibawah ini



Reset Konfigurasi

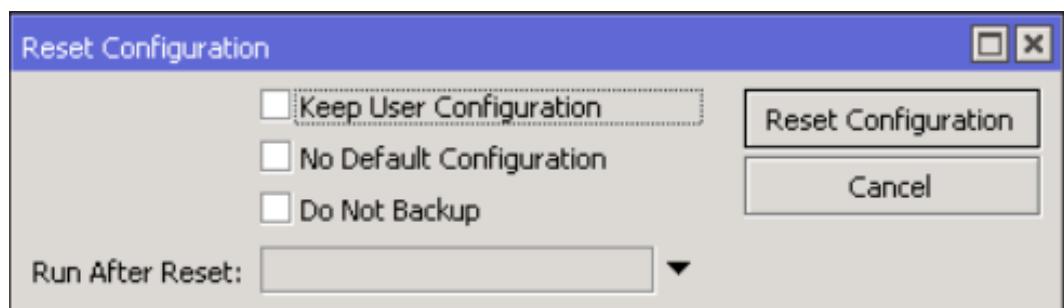
Terdapat dua cara untuk mereset konfigurasi pada MikroTik RouterOS, yaitu menggunakan hardreset dan softreset. Cara melakukan Hardreset pada MikroTik RouterOS adalah sebagai berikut:

- Cabut kabel power MikroTik
- Tekan tombol reset yang terdapat pada perangkat RouterBoard dan sambil colok kembali kabel power ke perangkat RouterBoard.
- Lepas tombol reset pada perangkat RouterBoard setelah lampu indikator berkedip



Cara melakukan softreset / reset konfigurasi lewat perintah di RouterOS adalah sebagai berikut:

- Masuk ke menu system → reset configuration
- Klik tombol reset configuration untuk mereset konfigurasi kembali ke default



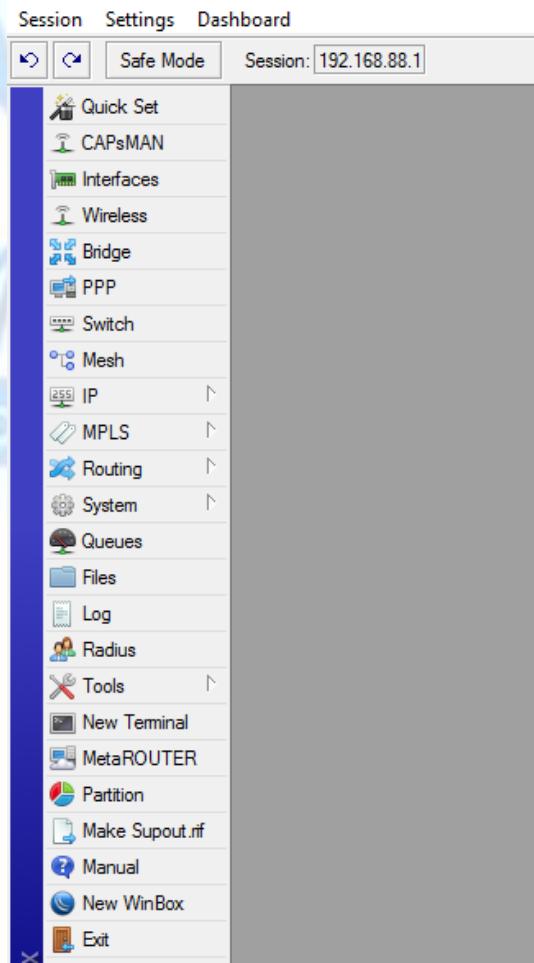
Beberapa pilihan pada menu reset configuration adalah sebagai berikut:

- Keep user configuration : Pada saat mereset konfigurasi user dan password tidak ikut dihapus
- No default configuration : Pada saat mereset konfigurasi tidak meload kembali konfigurasi default
- Do not backup : backup otomatis tidak dilakukan pada saat melakukan reset konfigurasi

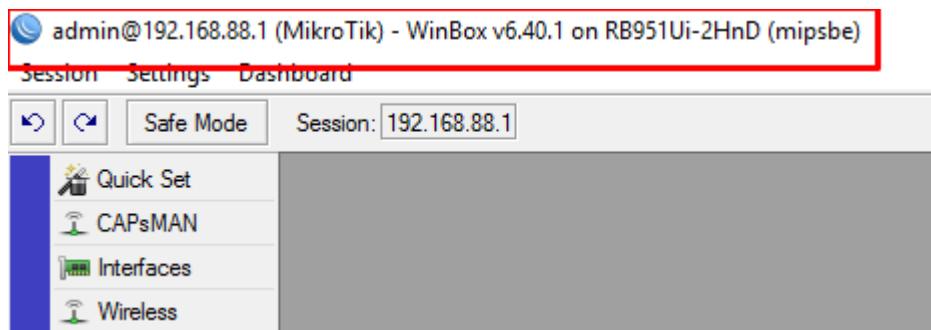
Upgrade dan Downgrade Firmware

Firmware pada MikroTik RouterOS dapat di upgrade maupun di downgrade sesuai kebutuhan. Berikut ini merupakan langkah-langkah dalam melakukan upgrade firmware di mikroTik RouterOS:

1. Koneksikan winbox ke mikrotik



2. Cek versi mikrotik sebelum di upgrade



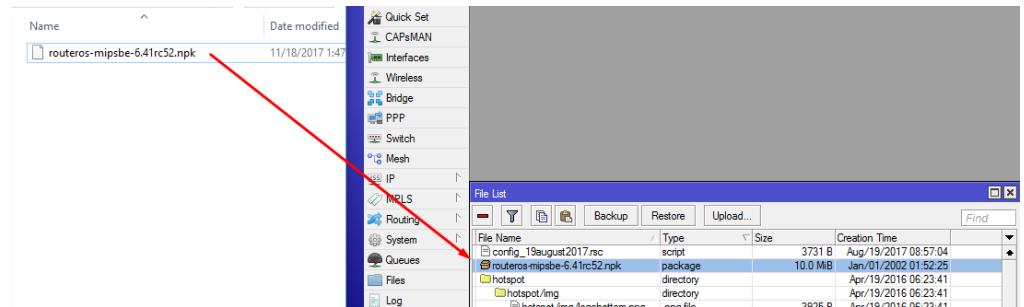
3. Siapkan firmware untuk melakukan upgrade

Name	Date modified	Type	Size
routeros-mipsbe-6.41rc52.npk	11/18/2017 1:47 PM	NPK File	10,279 KB

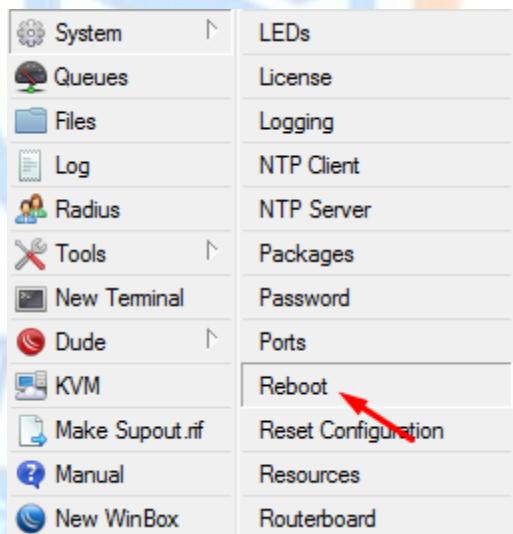
4. Buka menu file lalu *Drop n drag* firmware mikrotik yg berekstensi .npk

File List				
		Backup	Restore	Upload...
File Name	Type	Size	Creation Time	
skins	directory		Nov/18/2017	
um-before-migration.tar	.tar file	15.5 kB	Nov/18/2017	
user-manager	directory		Nov/18/2017	
user-manager/logsqldb	file	6.0 kB	Nov/18/2017	
user-manager/sqldb	file	80.0 kB	Nov/18/2017	

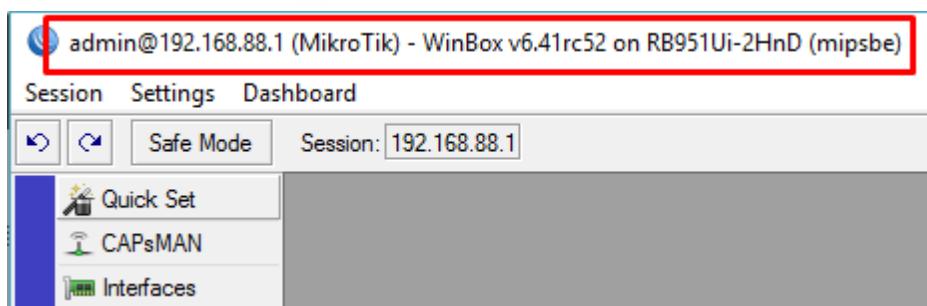
5 items 88.6 MiB of 2000.4 MiB used 95% free



5. Reboot Router

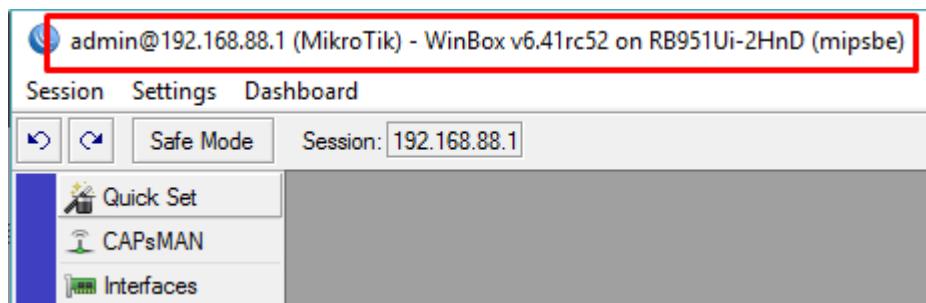


6. Verifikasi

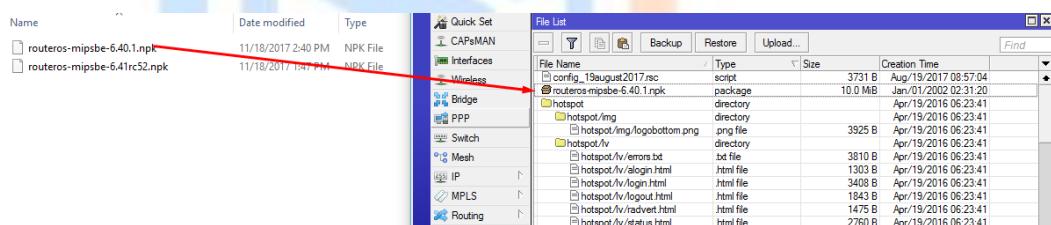


Berikut ini merupakan langkah-langkah untuk melakukan downgrade di MikroTik RouterOS:

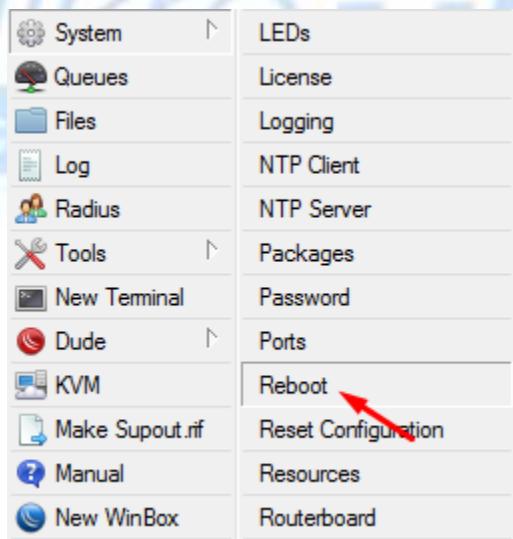
1. Cek versi mikrotik



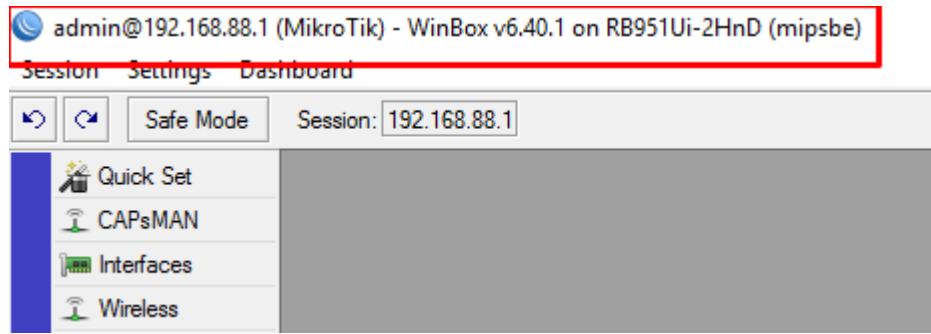
2. Drop and drag firmware mikrotik yg berekstensi .npl kedalam file list



3. Reboot Router

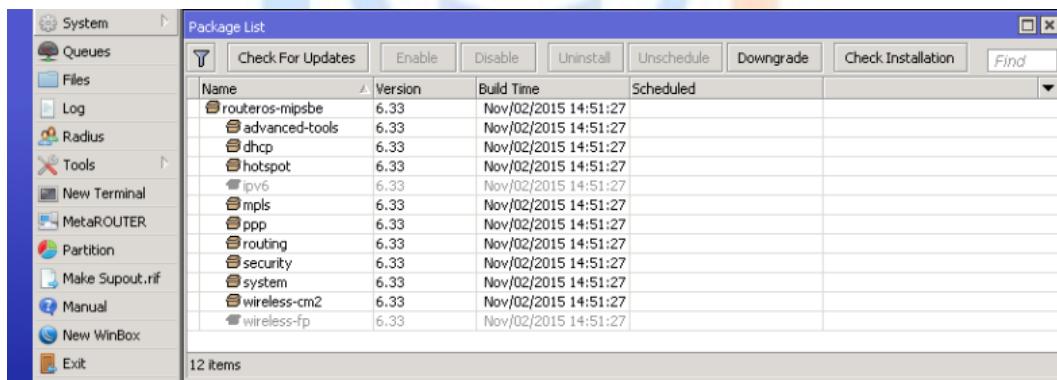


4. Verifikasi versi mikrotik yang telah di downgrade



Package Management

RouterOS memiliki berbagai macam fitur. Fitur-fitur tersebut dapat ditambah ataupun dikurangi. Untuk melihat fitur-fitur apa saja yang terdapat pada RouterOS dapat dilihat pada menu **System → Packages**



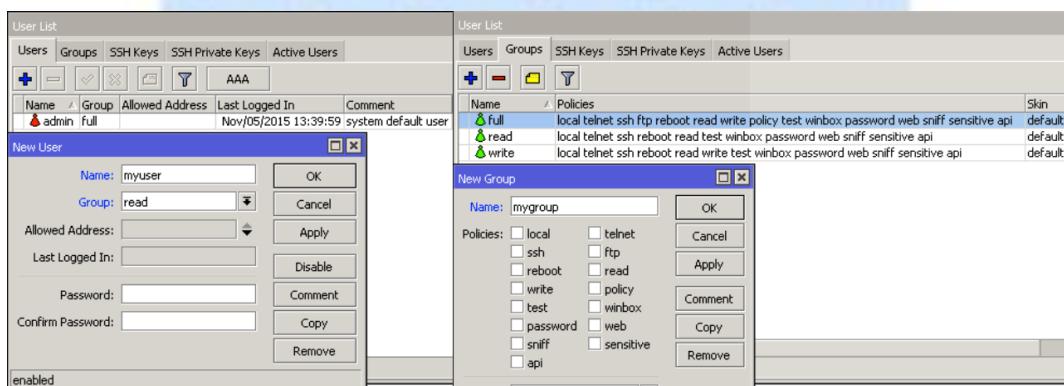
Berikut ini beberapa package yang sudah terdapat pada package management

Package	Functionality
advanced-tools	Netwatch, wake-on-LAN
dhcp	DHCP client and server
hotspot	HotSpot captive portal server
ipv6	IPv6 support
ppp	PPP, PPTP, L2TP, PPPoE clients and servers
routing	Dynamic routing: RIP, BGP, OSPF
security	Secure WinBox, SSH, IPsec
system	Basic features: static routing, firewall, bridging, etc.
wireless-cm2	802.11 a/b/g/n/ac support, CAPsMAN v2

selain package default yang sudah terdapat pada package management, RouterOS juga bisa ditambahkan package lain seperti GPS, ntp, dl. Package tambahan bisa di download di website mikrotik (www.mikrotik.com). Cara menambahkan package kedalam RouterOS adalah dengan mengupload file tambahan tersebut kedalam package management kemudian reboot RouterBoard

RouterOS User

Default user dari MikroTik RouterOS adalah **Admin** dan group **Full**. Default group yg lainnya adalah read dan write. Kita dapat menambahkan user lagi dan mengkustomisasi group di menu **System → users**



RouterOS Service

Terdapat beberapa RouterOS service yang secara default berjalan. Servicenya tersebut diantaranya adalah ftp, ssh, telnet, winbox, dan www. Service yang berjalan di MikroTik RouterOS dapat dilihat pada **menu IP → services**

IP Service List					
	Name	Port	Available From	Certificate	
X	• api	8728			
X	• api-ssl	8729		none	
	• ftp	21	192.168.88.5		
	• ssh	22			
	• telnet	23			
	• winbox	8291			
	• www	80			
X	• www-ssl	443		none	
8 items					

Beberapa fungsi dari service yang berjalan di MikroTik RouterOS adalah sebagai berikut:

- SSH : digunakan untuk akses secure CLI
- Telnet : digunakan untuk akses CLI, namun kurang aman dikarenakan tidak adanya enkripsi
- WinBox : Digunakan untuk akses GUI dari MikroTik RouterOS
- WWW : Digunakan untuk akses MikroTik RouterOS dari Web browser.

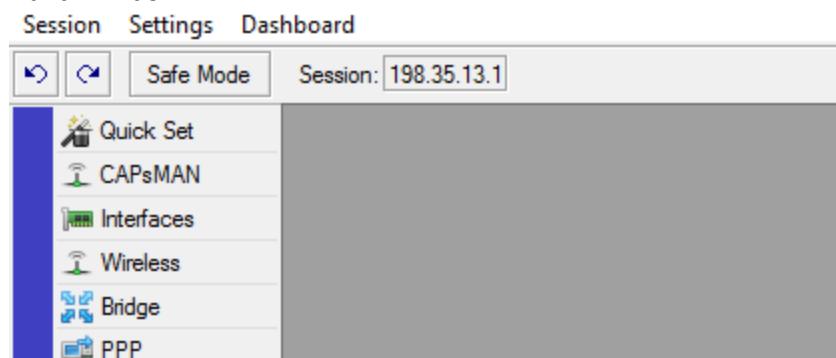
Demi keamanan perangkat apabila sudah masuk ke production sebaiknya disable beberapa service yang tidak perlu.

Backup Di Mikrotik

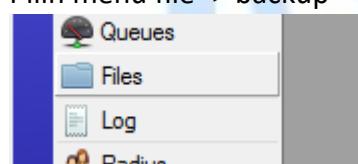
Terdapat dua jenis backup di MikroTik, yaitu backup file (.backup) yang digunakan untuk restore konfigurasi pada router yang sama dan export file (.rsc) yang digunakan untuk memindahkan config mikrotik ke router lain.

Mikrotik dapat melakukan backup seluruh konfigurasi. File hasil backup juga dapat di enkripsi untuk menjaga kerahasiaanya. Berikut ini langkah-langkah untuk melakukan backup di mikrotik:

1. Buka winbox



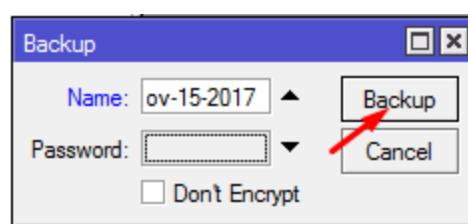
2. Pilih menu file -> backup



A screenshot of the Winbox file list window. The title bar says 'File List'. Below it is a toolbar with icons for back, forward, filter, file list, backup, restore, and upload. The 'Backup' button is highlighted with a red arrow. The main area is a table showing a list of files and directories:

File Name	Type	Size
skins	directory	
um-before-migration.tar	.tar file	15
user-manager	directory	
user-manager/logsqldb	file	6
user-manager/sql ldb	file	80

3. Beri nama file



4. Cek hasil backup di menu file

File List				
			Backup	Restore
File Name	Type	Size	Creation Time	
backup-nov-15-2017.backup	backup	8.2 KB	Nov/15/2017 17:49:21	
skins	directory		Nov/15/2017 17:26:32	
um-before-migration.tar	tar file	15.5 KB	Nov/15/2017 17:26:37	
user-manager	directory		Nov/15/2017 17:26:37	
user-manager/logsqldb	file	6.0 KB	Nov/15/2017 17:26:36	
user-manager/sqldb	file	80.0 KB	Nov/15/2017 17:26:37	

Backup selanjutnya adalah menggunakan export (.rsc). Export hanya dapat digenerate menggunakan CLI. File hasil export konfigurasi bisa di edit menggunakan notepad. File hasil export tersimpan pada file list

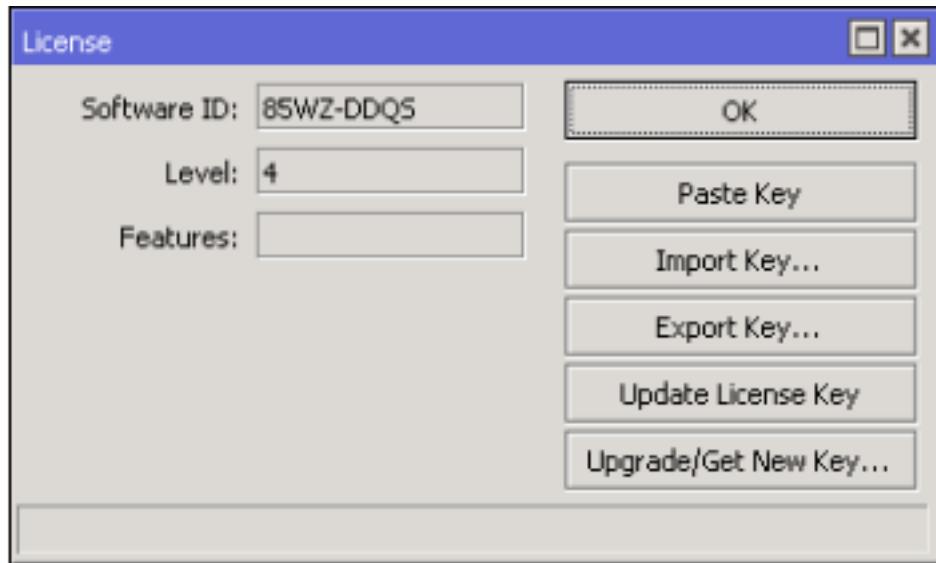
```
[admin@XY_YourName] > /export file=flash/router_conf_20151106
[admin@XY_YourName] > /file print
# NAME TYPE SIZE CREATION-TIME
0 flash disk jan/01/1970 02:00:00
1 flashskins directory jan/01/1970 02:00:01
2 flash/XY_YourName-20151106-0939.backup backup 37.6KiB nov/06/2015 09:39:10
3 flash/router_conf_20151106.rsc script 3595 nov/06/2015 09:40:35
[admin@XY_YourName] >
```

File export dapat di restore ke router lain dengan cara mengetik perintah *import* pada CLI.

```
[admin@XY_YourName] > /import flash/router_conf_20151106.rsc
Script file loaded and executed successfully
[admin@XY_YourName] >
```

Lisensi RouterOS

Setiap MikroTik RouterOS dilengkapi dengan lisensi. Lisensi MikroTik RouterOS dapat dilihat pada menu **System → License**. Lisensi pada RouterOS berlaku seumur hidup. Lisensi RouterOS dapat diupgrade dengan cara membelinya di situs mikrotik.com



MikroTik RouterOS memiliki beberapa tingkatan lisensi, berikut ini detail dari lisensi di MikroTik

Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key ↗	registration required ↗	volume only ↗	\$45	\$95	\$250
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h trial	-	yes(*)	yes	yes	yes
EoIP tunnels	24h trial	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited
L2TP tunnels	24h trial	1	200	200	500	unlimited
OVPN tunnels	24h trial	1	200	200	unlimited	unlimited
VLAN interfaces	24h trial	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h trial	1	1	200	500	unlimited
RADIUS client	24h trial	-	yes	yes	yes	yes
Queues	24h trial	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h trial	-	yes	yes	yes	yes
User manager active sessions	24h trial	1	10	20	50	Unlimited
Number of KVM guests	none	1	Unlimited	Unlimited	Unlimited	Unlimited

Modul 2 DHCP

Dynamic host configuration protocol (DHCP) adalah merupakan service yang memungkinkan sebuah perangkat dapat mendistribusikan atau assign IP address secara otomatis di dalam sebuah jaringan computer. Jadi ketika ada request yang di kirimkan oleh user yang berfungsi sebagai DHCP client maka akan di response oleh router mikrotik yang bertugas sebagai DHCP Server.

Ketika reponse DHCP Client sudah di terima oleh DHCP Server maka DHCP server akan memberikan informasi berupa IP ADDRESS,Netmask,Default Gateway,Dns Server dan juga NTP server kepada DHCP Client yang me-request tadi.

Router Mikrotik sendiri dapat digunakan sebagai DHCP Server maupun DHCP CLinet,bahkan Router mikrotik dapat difungsikan sebagai DHCP Server dan juga DHCP Client dalam waktu yang bersamaan

Perbedaan Antara DHCP Server dan DHCP Client

Di dalam protocol DHCP sendiri terbagi menjadi 2 (dua) Fungsi, yaitu;

- DHCP SERVER, adalah kondisi dimana router (mikrotik) bertugas memberikan atau assign IP address secara otomatis kepada user didalam sebuah jaringan. Tujuannya agar si user tidak perlu men-setup PCnya menggunakan IP Statik., Biasanya DHCP server di implementasikan pada jaringan Wifi,Hotspot area atau di jaringan LAN yang memiliki jumlah user yang banyak .
- DHCP CLIENT, adalah kondisi dimana perangkat didalam sebuah jaringan pc, laptop. Access point maupun router bergunci sebagai ip dhcp atau ip otomatis dari DHCP server.

Cara Konfigurasi DHCP SERVER Di MIKROTIK

Untuk setting DHCP SERVER di mikrotik pastikan kalian harus sudah memberikan IP ADDRESS untuk interface yang menjalankan DHCP SERVER adalah interface ether2 dengan IP ADDRESS

192.168.1.0/24,nah kalian tau knp harus ether2 ??

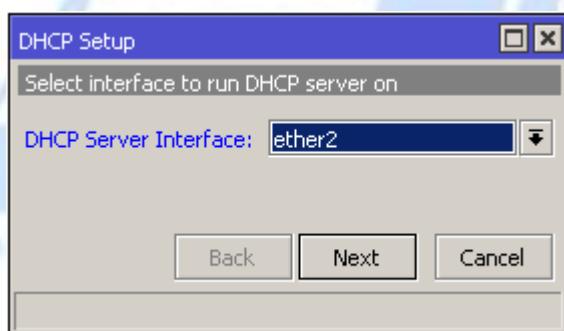
Karena kondisi dijaringan saya interface ether2 router mikrotik terhubung langsung ke switch yang berfungsi sebagai center point untuk menghubungkan semua user yang ada di jaringan, jika dijaringan kalian berbeda dengan topology saya yah tinggal disesuaikan saja.

Gunakan winbox untuk login ke router mikrotik anda dan klik menu **IP > DHCP SERVER > TAB DHCP** klik menu **DHCP SETUP**,nanti akan muncul wizard serperti gambar dibawah ini.

Select Interface to run **DHCP SERVER ON**

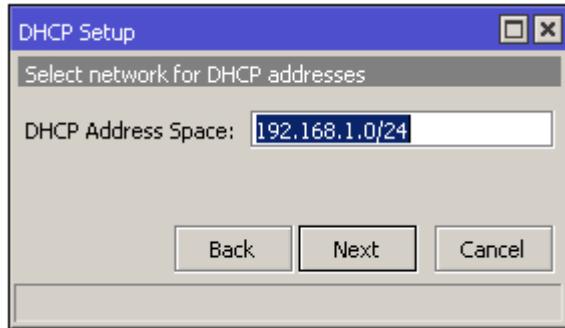
Ditahap ini kita akan menentukan interface mana yang akan menjalankan service DHCP SERVER,

Silahkan kalian pilih interface yang akan di setup sebagai DHCP SERVER pada opsi DHCP SERVER interface kemudian klik tombol **NEXT**.



Select network for DHCP ADDRESSES

Nah disini kita bisa menentukan jumlah IP ADDRESS yang akan dialokasikan oleh DHCP SERVER kepada user didalam jaringan berdasarkan jumlah subnet pada opsi DHCP ADDRESS SPACE. Namun biasanya jumlah ip yang akan muncul akan mengikuti konfigurasi pengalamatan IP ADDRESS yang kita konfig sebelumnya di menu > **IP > ADDRESS**, jadi tinggal langsung kita klik NEXT saja



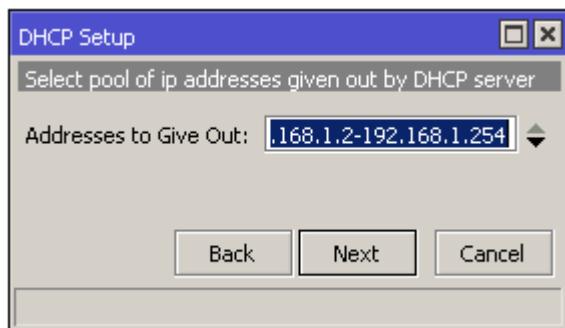
Select gateway for given network

Di menu ini kita diminta untuk menentukan alamat IP GATEWAY yang akan diberikan kepada user pada opsi **GATEWAY for DHCP NETWORK**. Kalau kalian tidak ingin mengubah konfigurasi ip gateway nya tinggal klik NEXT saja.



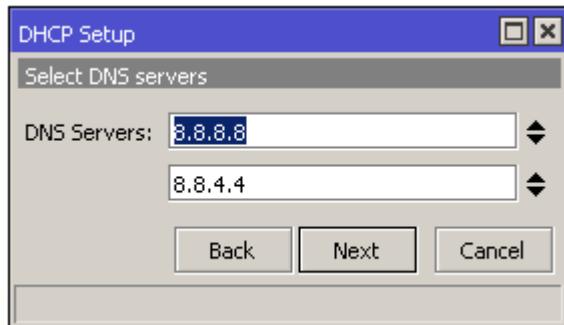
Select pool of ip address given out by DHCP SERVER

Kalian bisa menentukan berapa RANGE IP ADDRESS yang akan diberikan secara otomatis Oleh DHCP SERVER kepada user pada tahap ini . klik NEXT untuk melanjutkan ketahap selanjutnya.



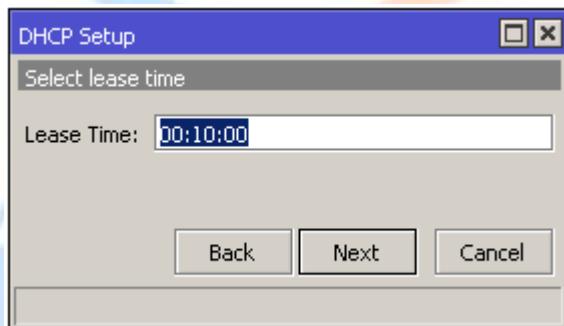
Select DNS SERVERs

Kalau kita sudah men-setup DHCP SERVER sekarang tinggal kita menambahkan DNS SERVER di mikrotik router kita ..secara standarisasinya DNS SERVER akan otomatis muncul dengan sendirinya tanpa harus di input oleh kita.

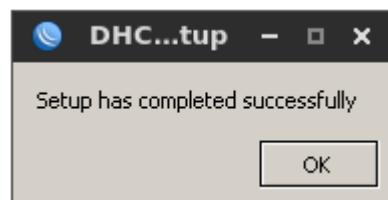


Select lease Time

Adalah waktu sewa untuk sebuah IP ADDRESS yang akan dipinjamkan oleh layanan DHCP SERVER kepada setiap user yang terkoneksi melalui proses DHCP

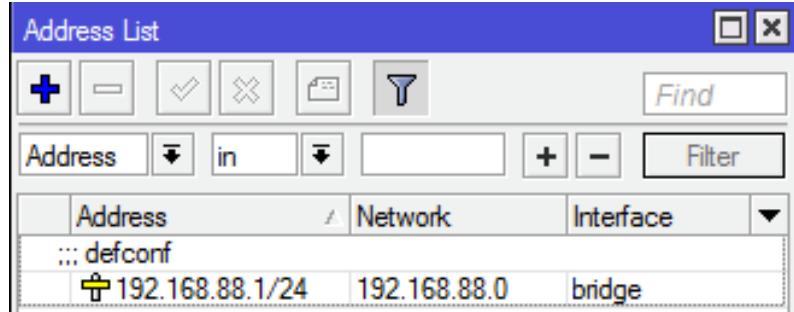


Jika semua tahap yang kita konfig sudah benar maka akan muncul notifikasi "SETUP HAS COMPLETED SUCCESSFULLY" seperti gambar dibawah ini.

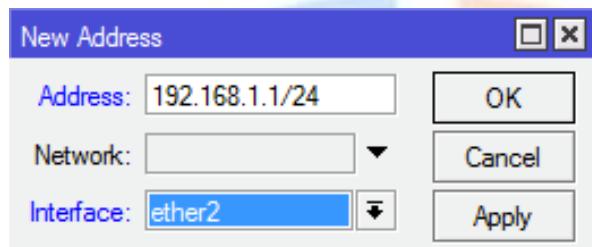


Setelah itu kita perlu menambahkan ip address default routernya di MikroTik RouterBoard. Caranya adalah sebagai berikut:

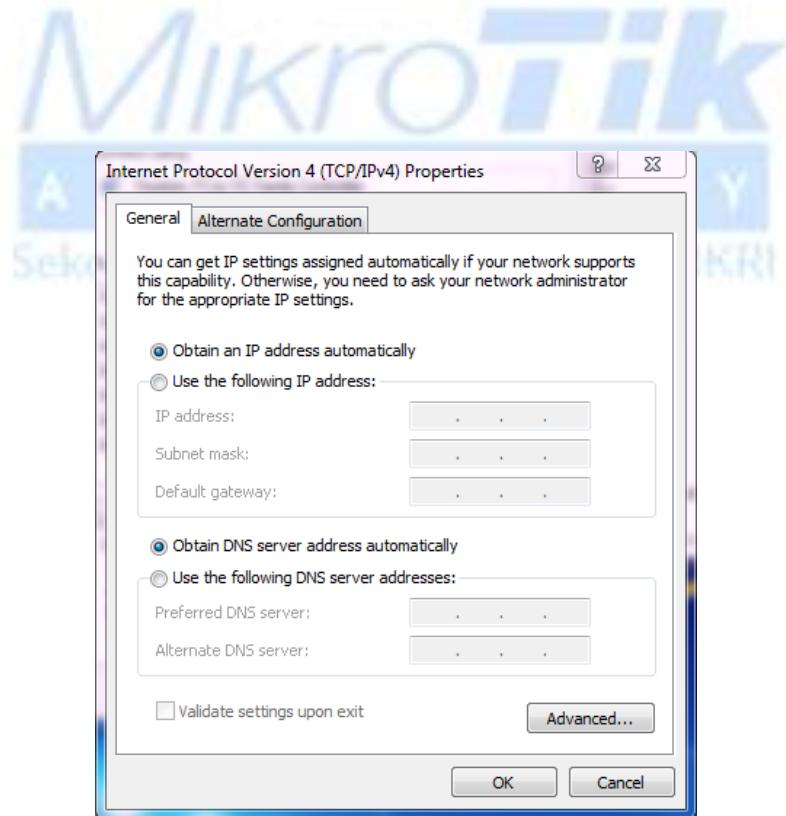
- Masuk ke menu IP → address



- Tekan tombol (+) untuk menambahkan IP address. Masukkan address



Sekarang tinggal kita ubah pengaturan IP address di PC /LAPTOP kalian secara automatic apabila masih di set static , untuk mengubah konfigurasi ip address klik kanan icon network pada PC/LAPTOP kalian dan pilih **Open Network and Sharing Center**.Pilih change adapter setting, kemudian klik kanan interface

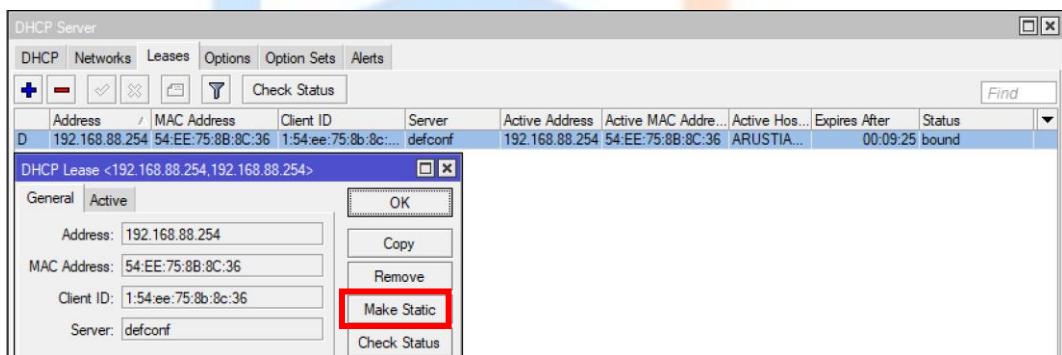


Local Area Connection pilih **properties**, lalu doble klik pada opsi **Internet Protocol Version 4 (IPv4)**. setelah itu IP ADDRESS dan DNS SERVER nya di obtain agar mendapatkan IP ADDRESS AUTOMATIC atau DHCP dari router mikrotik.

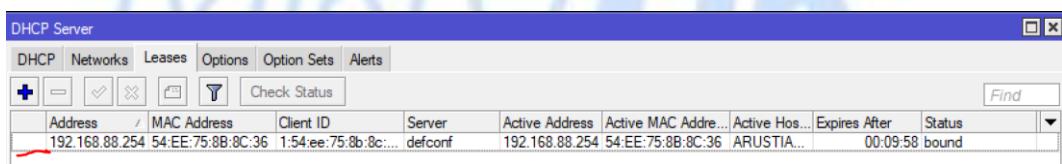
DHCP Static

Request ip dynamic menggunakan DHCP dapat juga di static kan sehingga laptop dapat mendapatkan address DHCP sama terus menerus. Langkah-langkah konfigurasinya adalah sebagai berikut:

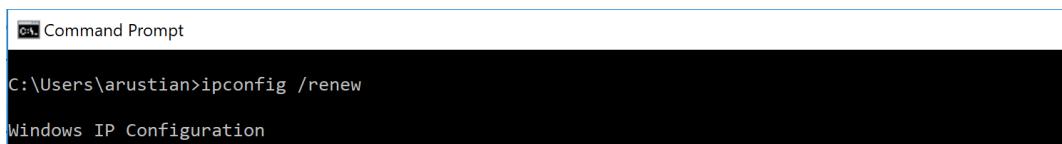
1. Masuk ke menu IP → DHCP Server → Lease
2. Double klik IP address pada table Leases dan klik make static



3. Atribut **D** akan hilang pada table Leases yg menandakan ip tersebut yg akan selalu didapatkan oleh PC ARUSTIAN



4. Coba renew ip address anda yg didapat dari DHCP server. Caranya masuk ke command prompt trus ketik perintah **ipconfig /renew**

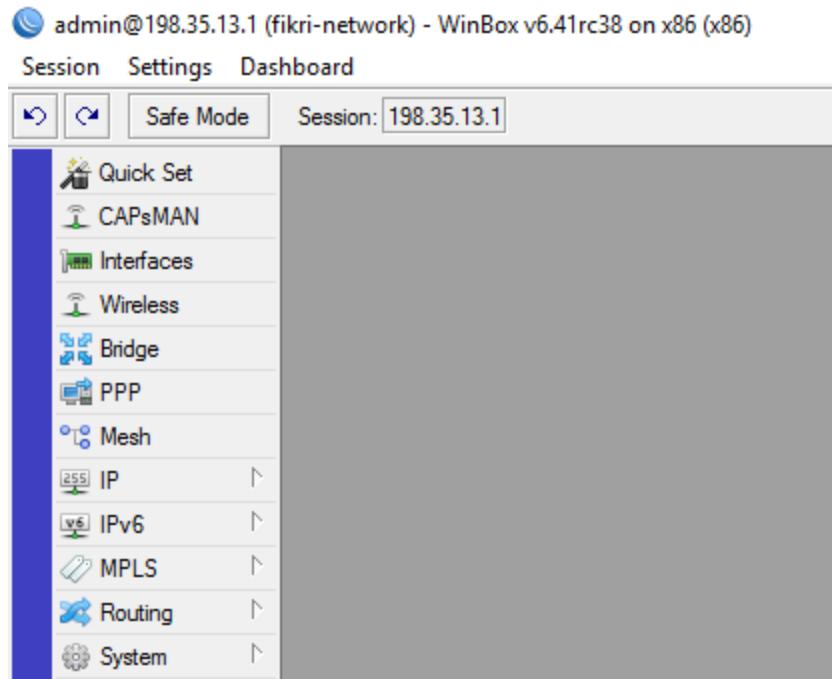


5. Cek Kembali IP address pada laptop anda apakah tetap sama?

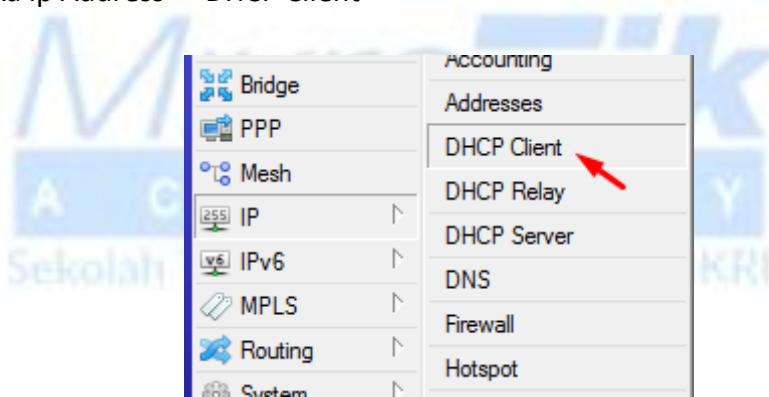
Setting DHCP Client Di Mikrotik

Mikrotik juga dapat dikonfigurasikan sebagai DHCP client, langkah-langkah untuk mengkonfigurasikan DHCP client di mikrotik adalah sebagai berikut:

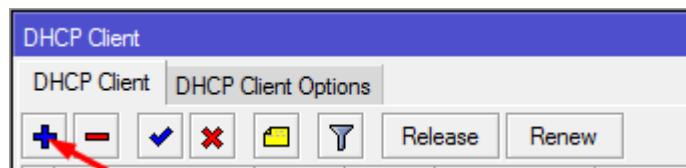
1. Koneksikan Mikrotik ke Winbox

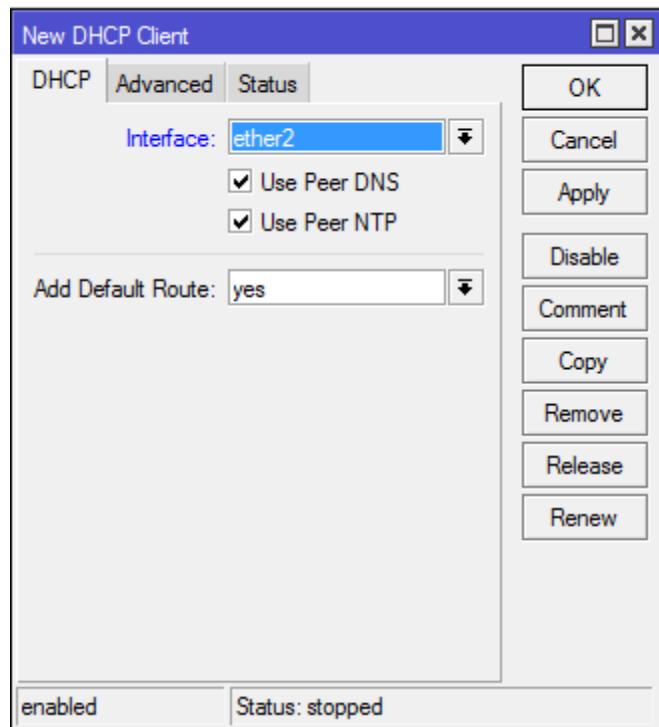


2. Buka ip Address -> DHCP Client



3. Tambahkan dhcp client baru



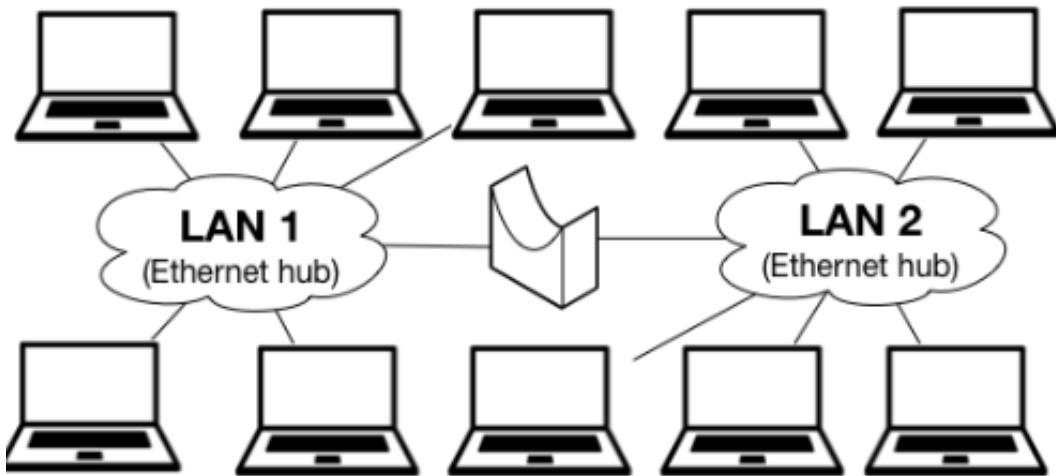


4. Verifikasi

DHCP Client						
DHCP Client		DHCP Client Options				
		+	-	✓	✗	✖
		Release	Renew	Find		
	Interface	Use P...	Add D...	IP Address	Expires After	Status
	ether2	yes	yes	10.0.3.15/24	23:58:27	bound

Modul 3 Bridging

Bridging pada Mikrotik RouterOs merupakan cara menggabungkan dua segment network menjadi sebuah network yang memiliki broadcast domain yg sama dengan mekanisme software bridge. Bridge sendiri merupakan perangkat layer 2 pada OSI model yang berfungsi sebagai transparent device yang membagi collision domain menjadi dua bagian seperti gambar dibawah ini.



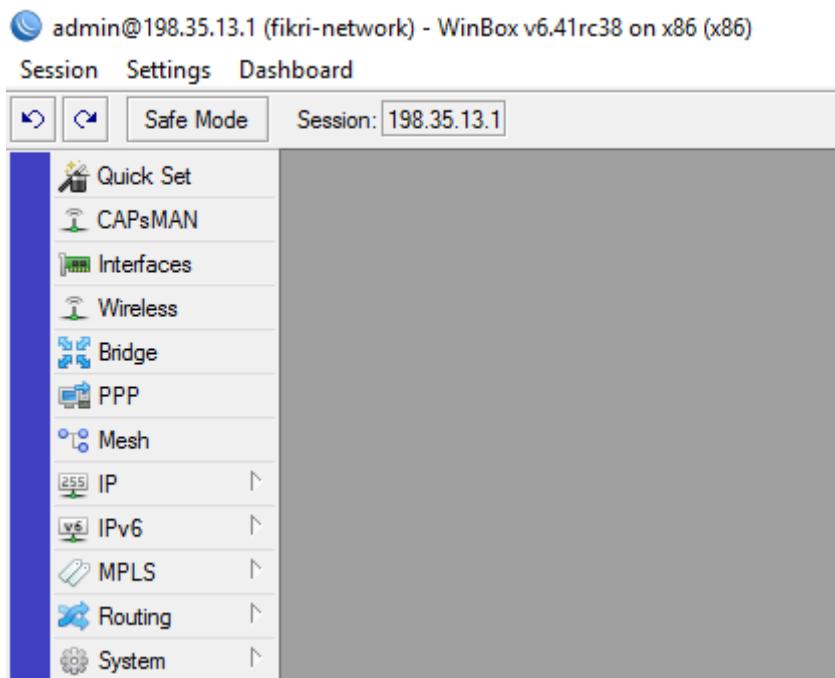
interface Ethernet, SFP, wireless, dan tunnel dapat ditambahkan kedalam sebuah bridge. Pada interface ether 3-5 biasanya menjadi slave dari master port ether 2. Konfigurasi tersebut membuat ether 2-5 menjadi seolah-olah sebuah switch yang melakukan switching frame (nama PDU di layer 2). Konfigurasi tersebut juga lebih hemat CPU usage dikarenakan menggunakan switch chip sendiri.

Terdapat beberapa limitasi pada bridging wireless, yaitu wireless client (mode station) tidak support bridge. Untuk mengatasi tersebut pada RouterOS terdapat beberapa mode wireless station yang mendukung bridge, yaitu:

- Station bridge : bridge antar RouterOS
- Station pseudobridge : bridge antara RouterOS dengan perangkat lain
- Station wds (wireless distribution system) : bridge antar RouterOS

Berikut ini merupakan langkah-langkah membuat bridge di mikrotik

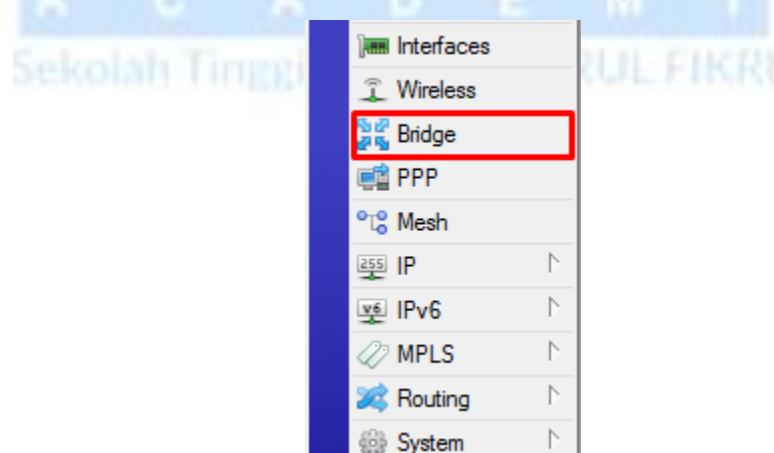
1. Koneksikan mikrotik ke winbox



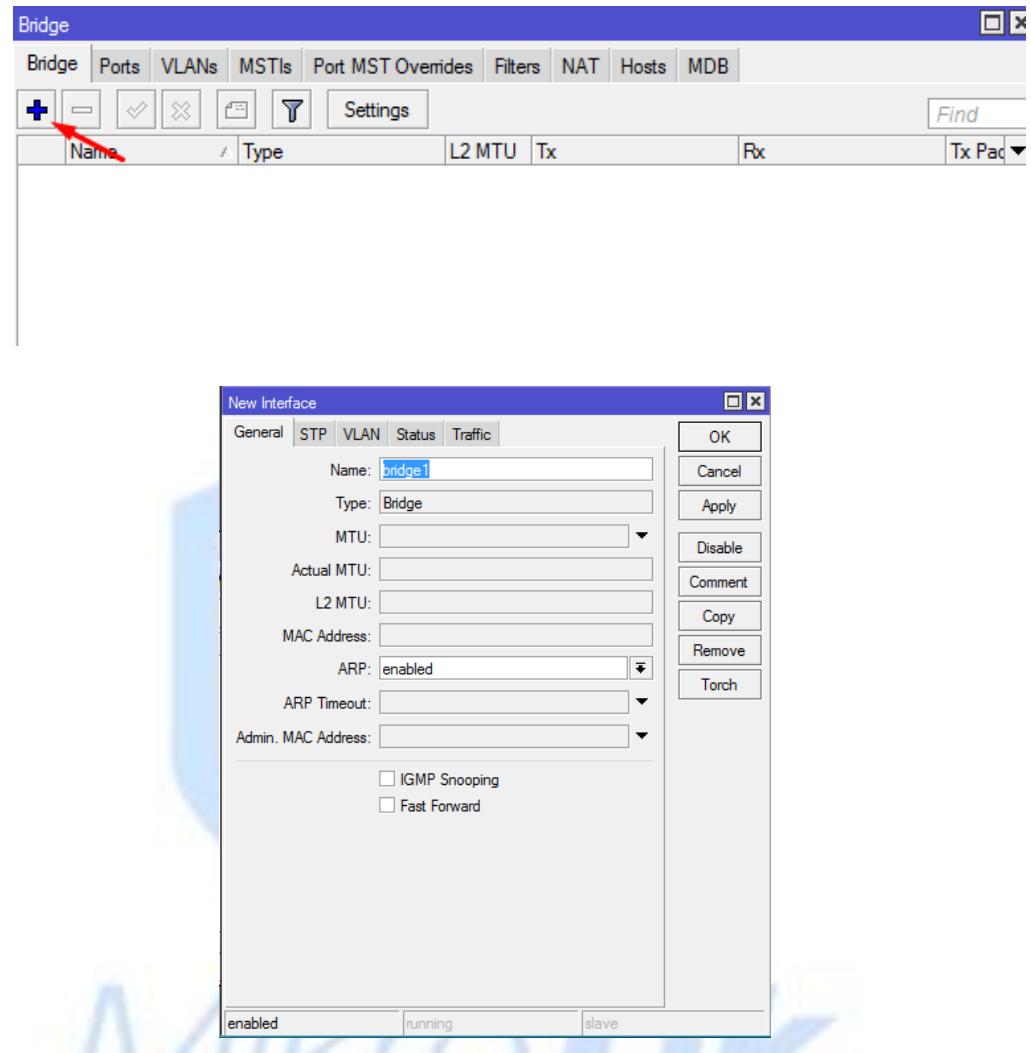
2. Cek interface yang akan di Bridge

Interface List	
	Name
R	♦♦ether2
R	♦♦wireless

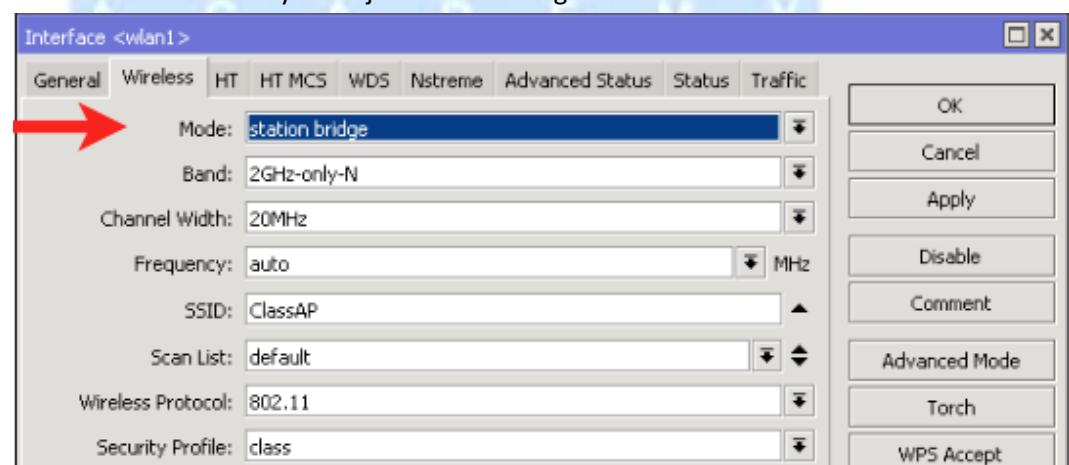
3. Buka menu bridge



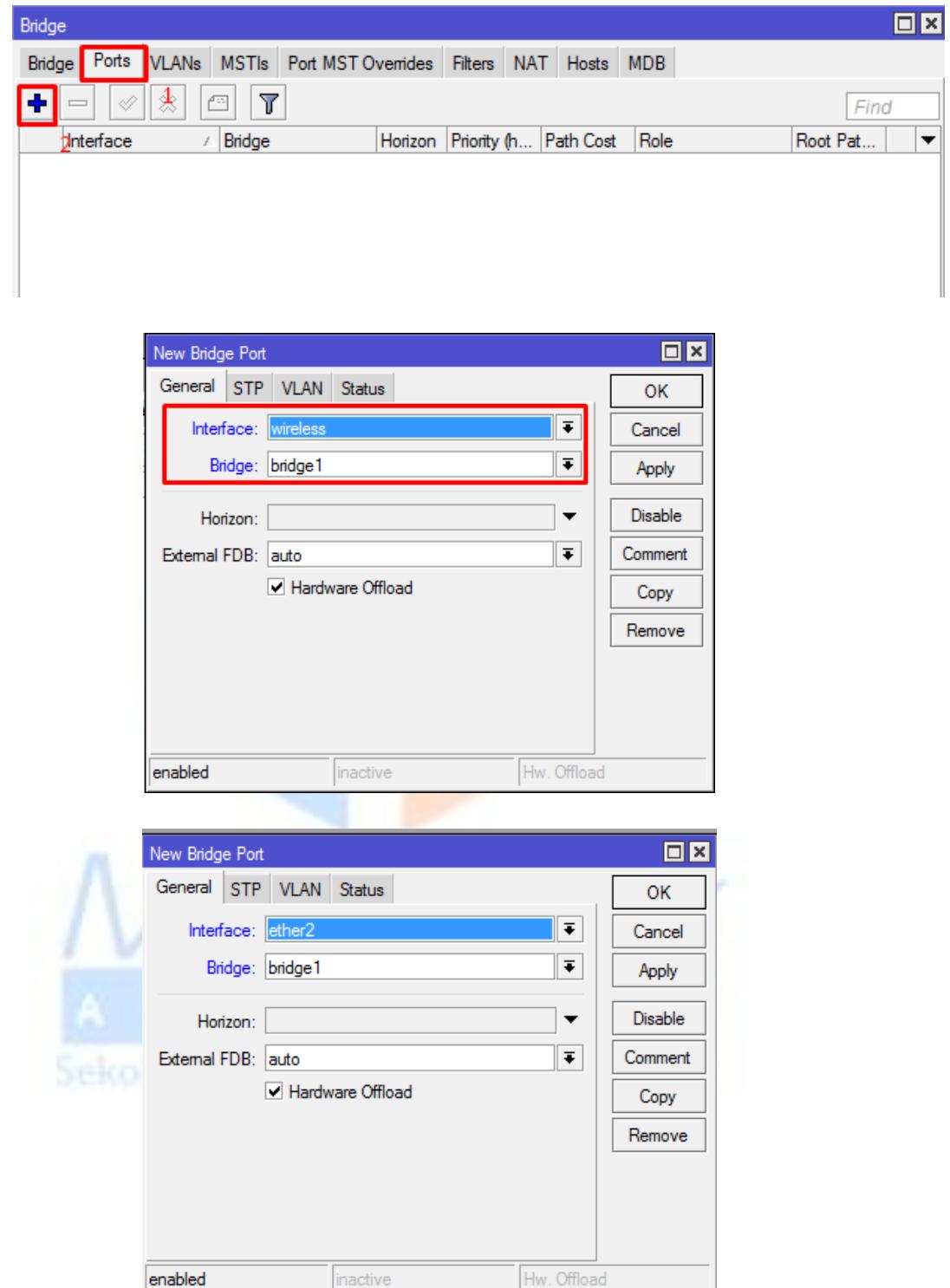
4. Buat bridge



5. Ganti mode wireless nya menjadi station bridge



6. Daftarkan interface ke bridge yang sudah di buat



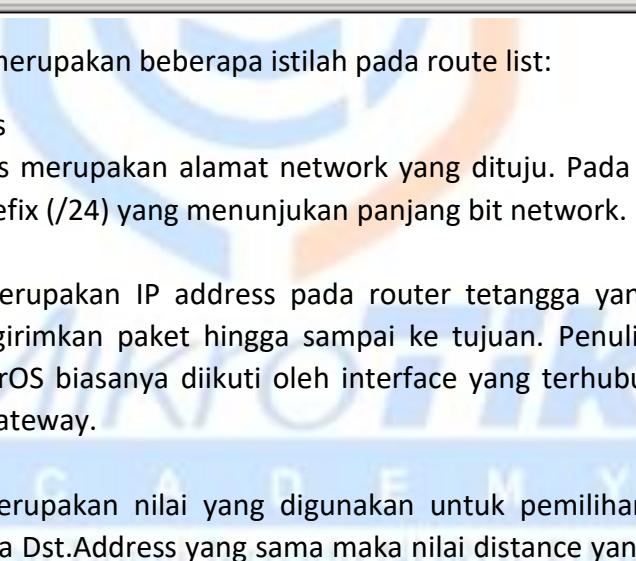
7. Verifikasi bridge dan interface

Bridge			
Bridge		Ports	VLANs
Bridge		MSTIs	Port MST Overrides
Interface	Bridge	Horizon	
Ether2	bridge1		
wireless	bridge1		



Modul 4 Routing

Routing bekerja pada layer 3 OSI model. Routing pada RouterOS digunakan untuk mendefinisikan kemana paket akan dikirimkan. Ibarat sebuah surat, routing merupakan alamat tujuan kemana surat harus dikirimkan. Routing table dari RouterOS dapat diakses dari menu **IP → routes**



Route List					
Routes		Nexthops	Rules	VRF	
Dst. Address	Gateway	Distance	Routing Mark	Pref. Source	
DAS ➤ 0.0.0.0/0	10.5.120.1 reachable wlan1	0			
DAC ➤ 10.5.120.0/24	wlan1 reachable	0	10.5.120.243		
DAC ➤ 192.168.88.0/24	bridge-local reachable	0	192.168.88.1		

Berikut ini merupakan beberapa istilah pada route list:

1. Dst. Address

Dst. Address merupakan alamat network yang dituju. Pada Dst. Address terdapat prefix (/24) yang menunjukkan panjang bit network.

2. Gateway

Gateway merupakan IP address pada router tetangga yang digunakan untuk mengirimkan paket hingga sampai ke tujuan. Penulisan gateway pada RouterOS biasanya diikuti oleh interface yang terhubung langsung dengan IP gateway.

3. Distance

Distance merupakan nilai yang digunakan untuk pemilihan route. Jika terdapat dua Dst.Address yang sama maka nilai distance yang paling kecil menang. Nilai distance default bagi masing-masing tipe route adalah:

- Connected routes: 0
- Static route: 1
- eBGP: 20
- OSPF: 110
- RIP : 120
- MME : 130
- iBGP : 200

4. Routing Mark

Routing mark (vrf) merupakan nama routing table. Routing table dikelompokan berdasarkan namanya. Routing table yang tidak mempunyai routing-mark dikelompokkan kedalam main routing table.

5. Pref.Source

Pref.Source adalah connected route yang merupakan IP address dari interface yang menjadi gateway dari sebuah dst.address.

6. Scope dan Target Scope

Scope digunakan untuk mencari nexthop. Sebuah route dapat mencari Nexthopnya hanya jika nilai **scope** lebih kecil atau sama dengan **target-scope**.

Pemilihan Best Path

Beberapa kriteria pemilihan Best Path pada routing table adalah sebagai berikut:

1. Routing table yang paling spesifik

Sebagai contoh jika terdapat dua routing table sebagai berikut:

- Dst 192.168.1.0/24 gateway: 1.2.3.4
- Dst 192.168.1.0/25 gateway: 10.10.10.1

Jika paket ingin diteruskan ke 192.168.1.10 maka dari kedua routing table tersebut paket ternyata akan di teruskan ke gateway 10.10.10.1 dikarenakan dst 192.168.1.0/25 memiliki prefix yang lebih spesifik

2. Distance

Distance menjadi penentu jika terdapat dua routing table sebagai berikut

- Dst 192.168.1.0/24 gateway: 1.2.3.4 distance 1
- Dst 192.168.1.0/24 gateway: 10.10.10.1 distance 10

Paket akan diteruskan ke gateway 1.2.3.4 dikarenakan memiliki distance paling kecil diantara dua routing table yang sama.

3. Default Gateway

Default gateway merupakan routing dengan alamat network 0.0.0.0/0. Default gateway atau default route menjadi pilihan terakhir pemilihan jalur jika tidak ada network yang cocok pada routing table.

Route Flags

Route flags pada RouterOS diberikan otomatis pada routing table, beberapa route flags adalah sebagai berikut:

- Dynamic (D) : route flags dynamic menunjukkan routing tersebut ditambahkan secara dinamis oleh routing protocol atau direct connect interface
- Active (A) : route flags active menunjukkan route tersebut digunakan untuk meneruskan paket
- Connected (C) : route flags connected menunjukkan connected route

- Static (S) : route flags static menunjukkan routing tersebut merupakan static route
- Disable (X) : route flags disable menunjukkan routing tersebut di disable dan tidak digunakan untuk meneruskan paket
- Ospf (o) : route flags ospf menunjukkan routing table tersebut berasal dari dynamic routing protocol OSPF

Contoh route flags pada routing table di RouterOS dapat dilihat pada gambar dibawah ini:

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source	
A5	▶ 0.0.0.0/0	10.5.120.1 reachable wlan1	1			
DAC	▶ 10.5.120.0/24	wlan1 reachable	0		10.5.120.243	
DAC	▶ 192.168.88.0/24	bridge-local reachable	0		192.168.88.1	

3 items

Static Route

Static route merupakan route yang secara manual di input pada RouterOS. Static route digunakan untuk routing paket ke alamat tujuan. Cara membuat static route adalah sebagai berikut:

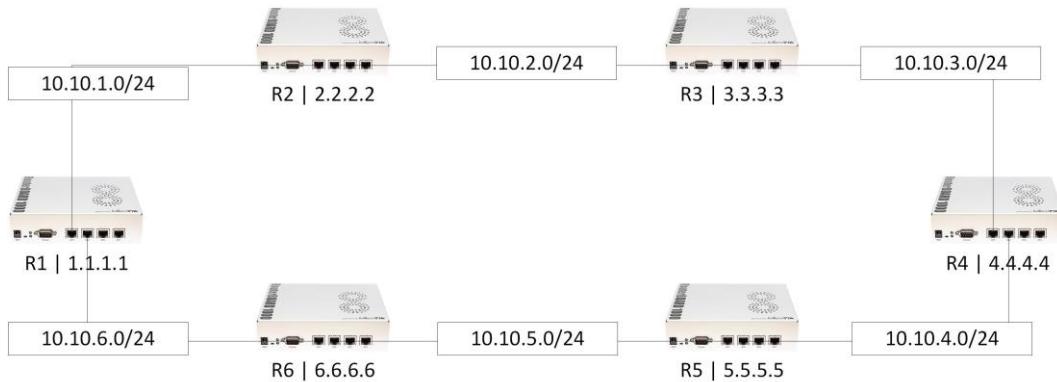
- Masuk ke menu IP → routes
- Tambahkan route baru dengan menekan tombol (+), maka akan muncul menu seperti dibawah ini.

General	Attributes
Dst. Address:	192.168.90.0/24
Gateway:	192.168.89.5
Check Gateway:	
Type:	unicast
Distance:	
Scope:	30
Target Scope:	10
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/> <input type="button" value="Disable"/> <input type="button" value="Comment"/> <input type="button" value="Copy"/> <input type="button" value="Remove"/>	

- Masukkan Dst.Address (network tujuan) beserta prefixnya, dan gateway
- Tekan tombol OK, jika sudah memasukan parameter tersebut

Lab Static Route

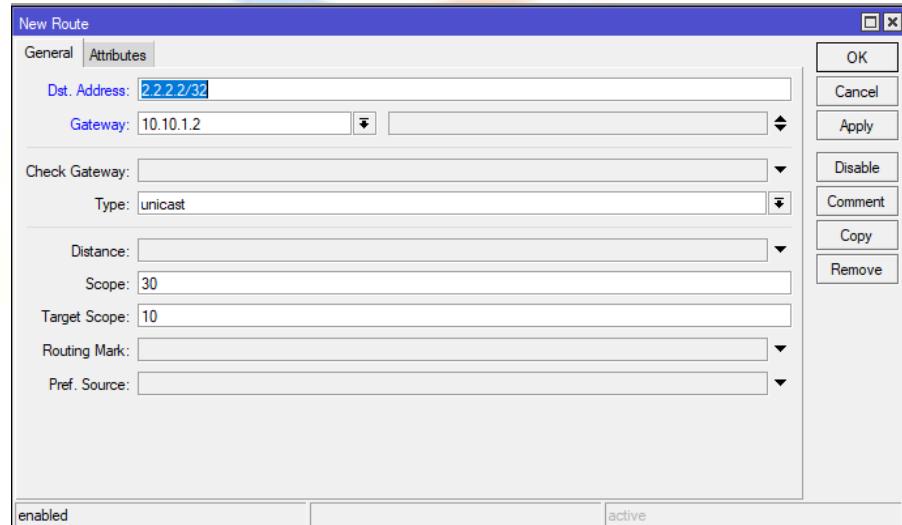
Buatlah Topologi seperti dibawah ini, dan beri IP address sesuai dengan topologi



Buatlah static route pada masing-masing router agar semua router dapat saling ping ke ip Loopback masing-masing

Dalam melakukan praktik dari studi kasus diatas, dapat dilakukan dengan cara cara berikut:

1. Buat terlebih dulu seperti keadaan topologi diatas
2. Jika sudah terhubung seperti diatas, lakukan konfigurasi di masing masing RB, contoh disini pakai R1 mau menghubungkan ke RB2

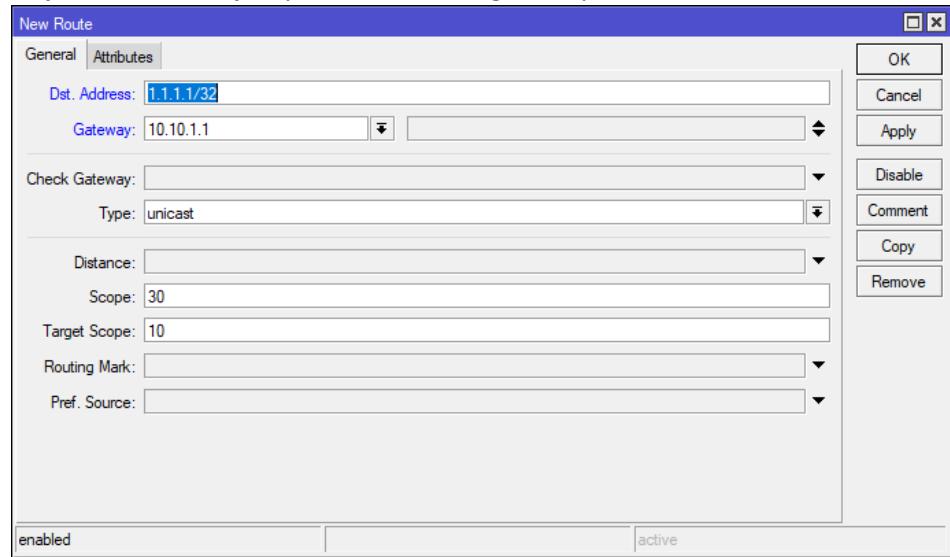


Penjelasan dari maksud konfigurasi routing static diatas adalah:

Dst.address : ip network tujuan yang ingin kita hubungkan (alamat ip loopback R2)

Gateway : masukan ip nexthopnya yang melewati dari R1 ke R2

3. jika sudah selanjutnya lakukan routing static pada RB2 ke RB1

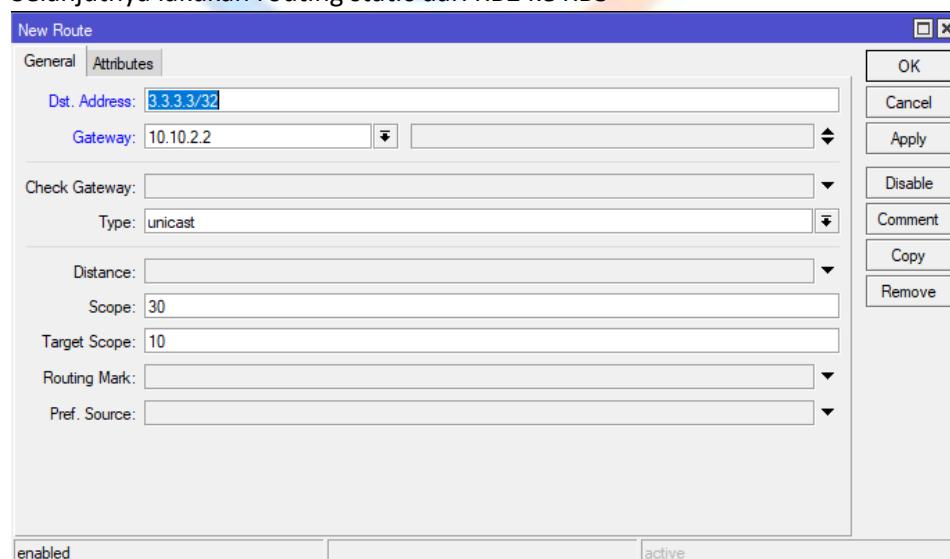


Penjelasan dari maksud konfigurasi routing static diatas adalah:

Dst.address : ip network tujuan yang ingin kita hubungkan (alamat ip loopback R1)

Gateway : masukan ip nexthopnya yang melewati dari R2 ke R1

2. Selanjutnya lakukan routing static dari RB2 ke RB3

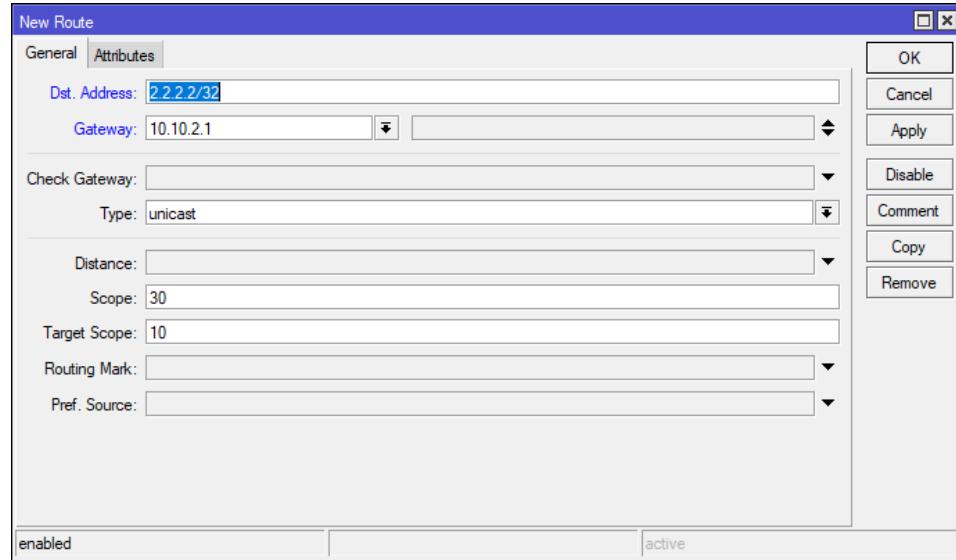


Penjelasan dari maksud konfigurasi routing static diatas adalah:

Dst.address : ip network tujuan yang ingin kita hubungkan (alamat ip loopback R3)

Gateway : masukan ip nexthopnya yang melewati dari R2 ke R3

3. Selanjutnya lakukan routing static dari RB3 ke RB2:

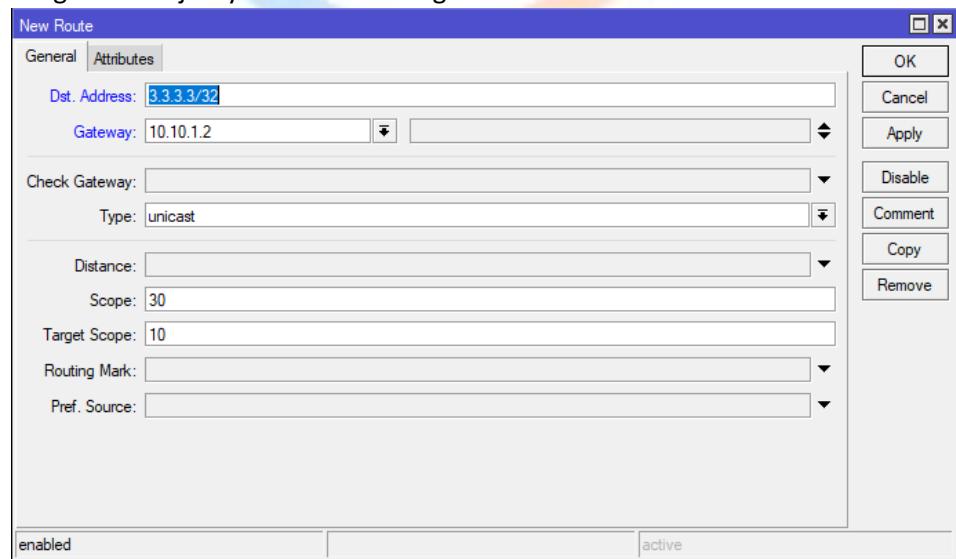


Penjelasan dari maksud konfigurasi routing static diatas adalah:

Dst.address : ip network tujuan yang ingin kita hubungkan (alamat ip loopback R2)

Gateway : masukan ip nexthopnya yang melewati dari R3 ke R2

4. Langkah selanjutnya lakukan routing static dari RB1 ke RB3:



Penjelasan dari maksud konfigurasi routing static diatas adalah:

Dst.address : ip network tujuan yang ingin kita hubungkan (alamat ip loopback R3)

Gateway : masukan ip nexthopnya yang melewati dari R1 ke R2

Modul 5 Wireless

Wireless pada Mikrotik

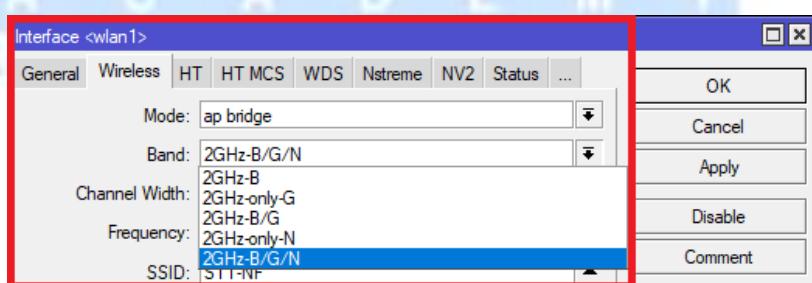
- RouterOS mendukung beberapa modul radio (wireless card) untuk jaringan WLAN atau Wi-Fi (Wireless Fidelity).
- Wi-Fi memiliki standar & spesifikasi IEEE 802.11 dan menggunakan frekuensi 2,4GHz dan 5,8GHz.
- MikroTik mendukung standar IEEE 802.11a/b/g/n
 - 802.11a – frekuensi 5GHz, 54Mbps
 - 802.11b – frekuensi 2,4GHz, 11 Mbps
 - 802.11g – frekuensi 2,4GHz, 54Mbps
 - 802.11n – frekuensi 2,4GHz dan 5GHz, sampai 450 Mbps*
 - 802.11ac – frekuensi 5GHz sampai 1300 Mbps*

IEEE Standard	Frequency	Speed
802.11a	5GHz	54Mbps
802.11b	2.4GHz	11Mbps
802.11g	2.4GHz	54Mbps
802.11n	2.4 and 5GHz	Up to 450 Mbps*
802.11ac	5GHz	Up to 1300 Mbps*

* Depending on RouterBOARD model

Wireless Band

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



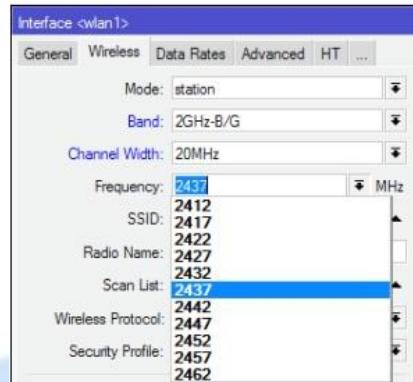
Wireless – Frequency Channel

- Frequency channel adalah pembagian frekuensi dalam suatu band dimana Access Point (AP) beroperasi.

Nilai-nilai channel bergantung pada band yang dipilih, kemampuan wireless card, dan aturan/regulasi frekuensi suatu negara.

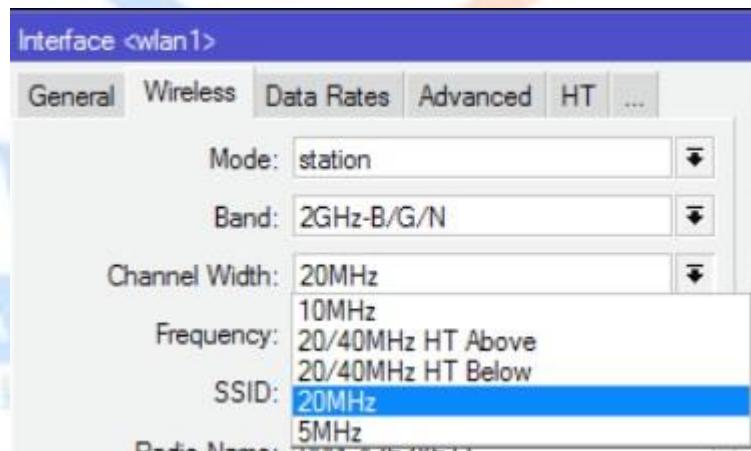
- Range frequency channel untuk masing-masing band adalah sbb:

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



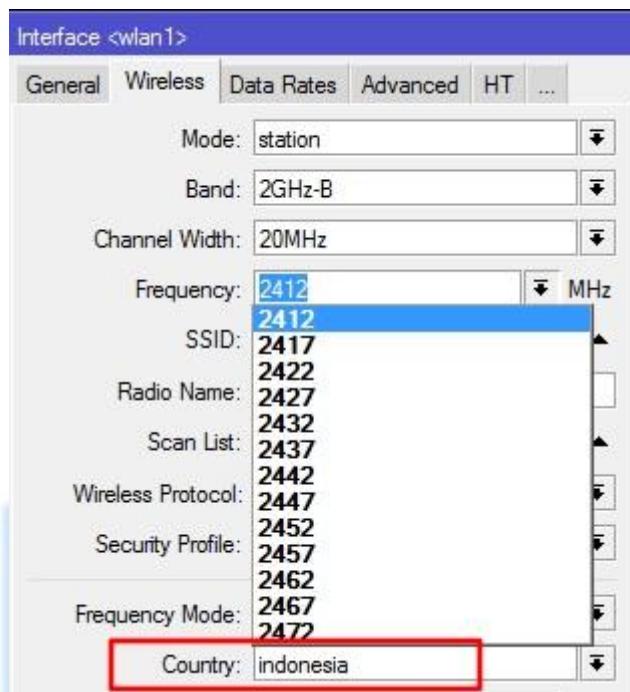
Wireless – Lebar Channel

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

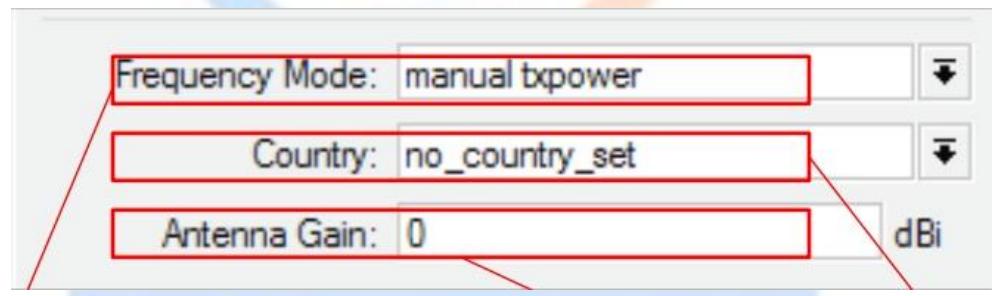


Wireless – Regulasi Frekuensi

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



Regulasi Frekuensi



Keterangan :

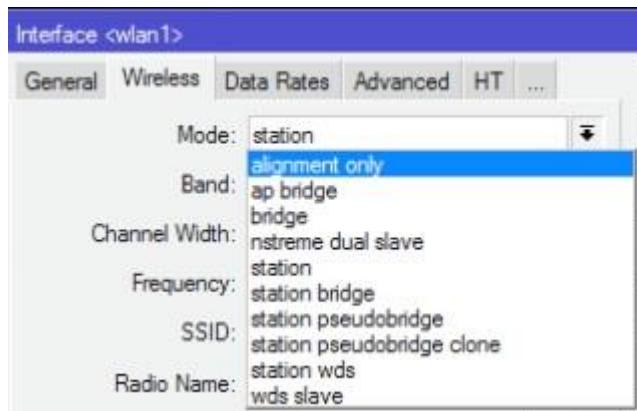
- Frequency Mode :
 1. manual-tx-power : Transmit power diatur manual (tidak menyesuaikan dengan negara tertentu).
 2. regulation-domain : Frekuensi channel disesuaikan dengan frekuensi-frekuensi yang diijinkan di suatu negara.
 3. Superchannel : Membuka semua frekuensi yang bisa disupport oleh wireless card
- Country : Pemilihan Country/Negara
- Antenna Gain : Default 0, akan otomatis menyesuaikan agar tidak melebihi EIRP country regulation

Konsep Koneksi Wireless

- Kesesuaian Mode: (AP-Station, AP-Repeater, RepeaterRepeater)

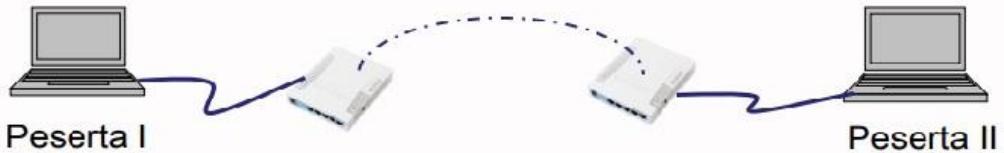
- Kesesuaian BAND
- Kesesuaian SSID
- Kesesuaian enkripsi dan authentifikasi
- Frekuensi channel tidak perlu sama, station secara otomatis akan mengikuti channel frekuensi pada AP.

Mode interface wireless



Keterangan :

1. alignment-only – mode transmit secara terusmenerus digunakan untuk positioning antena jarak jauh.
2. AP-bridge : wireless difungsikan sebagai Akses Poin.
3. nstream-dual-slave – digunakan untuk sistem nstream-dual.
4. Bridge - hampir sama dengan AP-bridge, namun hanya bisa dikoneksi oleh 1 station/client, mode ini biasanya digunakan untuk point-to-point.
5. Station – scan dan connect AP dengan frekuensi & SSID yang sama, mode ini TIDAK DAPAT di BRIDGE
6. Station-bridge – sama seperti station, mode ini adalah MikroTik proprietary. Mode untuk L2 bridging, selain wds.
7. Station-wds – sama seperti station, namun membentuk koneksi WDS dengan AP yang menjalankan WDS.
8. station-pseudobridge – sama seperti station, dengan tambahan MAC address translation untuk bridge.
9. station-pseudobridge-clone – Sama seperti station-pseudobridge, menggunakan station-bridge-clone-mac address untuk koneksi ke AP.
10. 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.



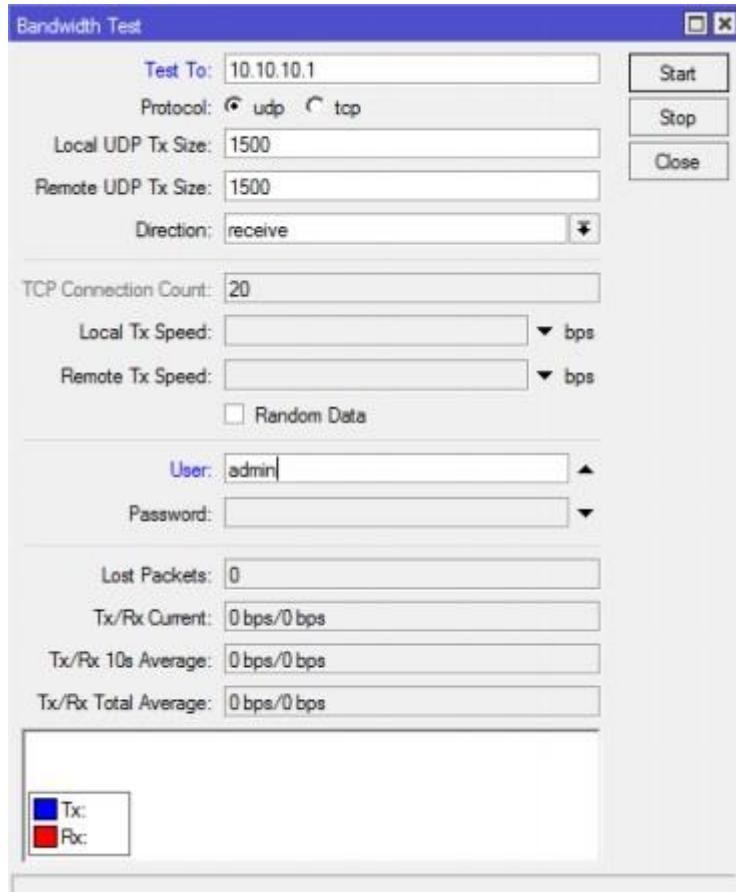
Konfigurasi	Peserta I	Peserta II
Mode	AP-Bridge/Bridge	Station
Band	Samakan	
SSID	Samakan (unik untuk tiap pasangan)	
Frequensi	Pilih	Tidak harus sama
Security Profile	Samakan	
IP address wlan1	10.10.10.1/24	10.10.10.2/24

LAB – Wireless AP & Station

- Satu peserta menjadi Access Point, satunya menjadi Station (wireless mode)
- Samakan SSID, band dan security profile.
- Setting IP Address interface wlan: IP AP= 10.10.10.1/24 IP station = 10.10.10.2/24
- Pastikan koneksi wireless (layer 1) terhubung, baru dapat dilakukan ping antar IP (layer 3)
- Lakukan ping dari masing-masing MikroTik.
- Lakukan bandwidth test antar Mikrotik

Bandwidth Test

- Bandwidth test digunakan untuk mengukur seberapa besar link dapat mendeliver bandwidth
- Untuk menjamin keakuratan, Bandwidth test hanya dijalankan disatu sisi
- Test to = IP lawan kita
- User & password = user password router yang kita test



LAB – Wireless AP & Station

- Coba gantilah frekuensi untuk mendapatkan signal terbaik.

Keterangan :

- Signal yang dikirim dan diterima oleh antena
- Client Connection Quality (CCQ) yaitu nilai yang menyatakan seberapa efektifkah kapasitas bandwidth yang dapat digunakan

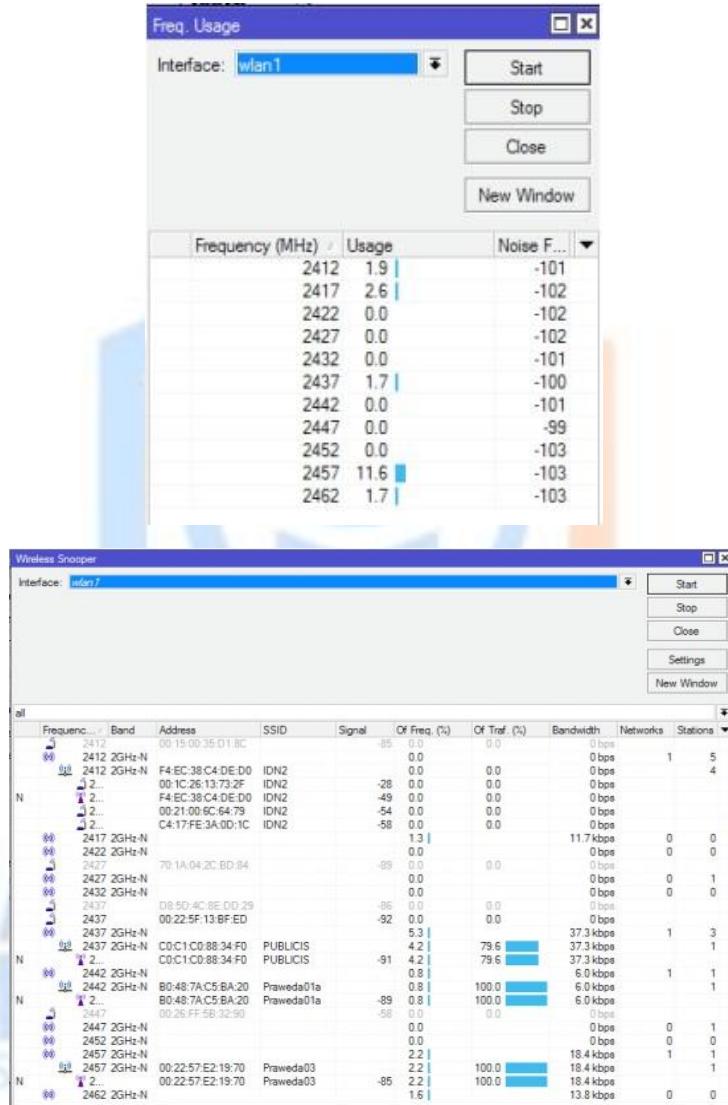
Wireless Tools

Ada beberapa tool dalam wireless MikroTik yang dapat digunakan untuk optimasi link.

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

LAB – Wireless Tools

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

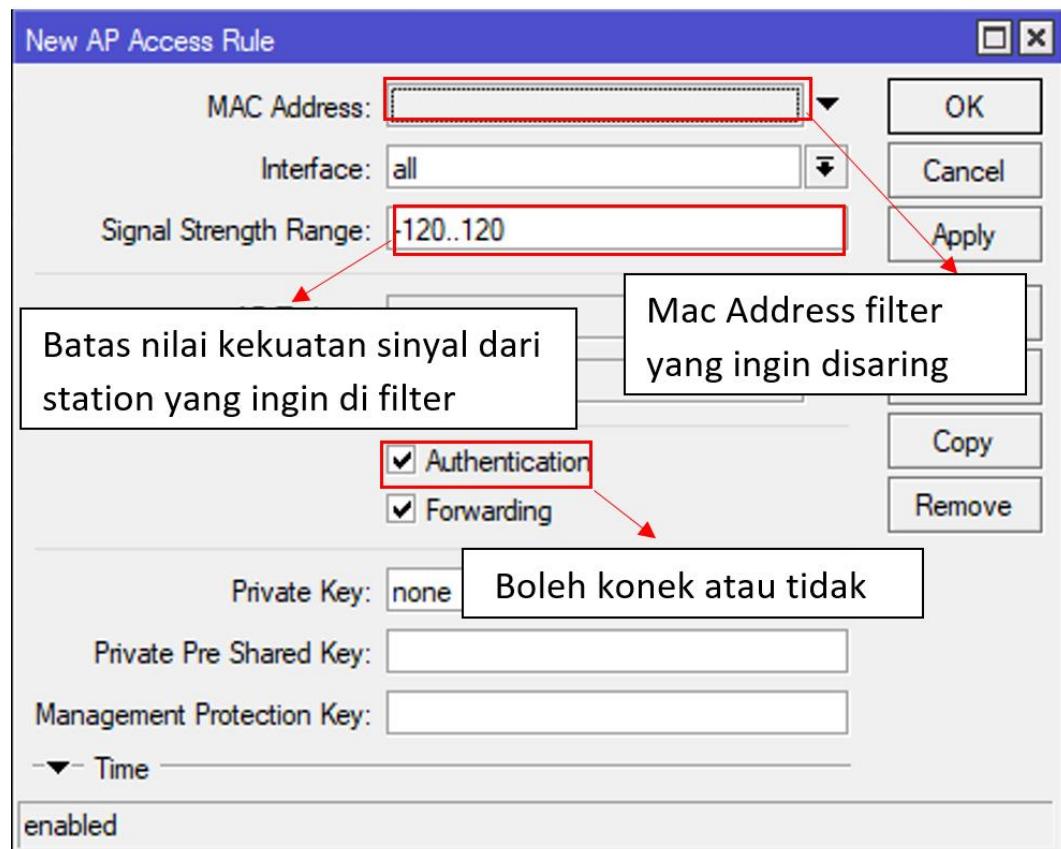


Wireless MAC Filtering

- Access Point, dapat dilakukan pembatasan hak akses dimana AP hanya dapat dikonek oleh station yang sudah kita tentukan
- Station, juga dapat dilock agar terkoneksi dengan AP yg sudah ditentukan.
- Mac filtering AP ada di Access List
- Mac filtering Station ada di Connect List.

Access Point – Access List

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



Keterangan :

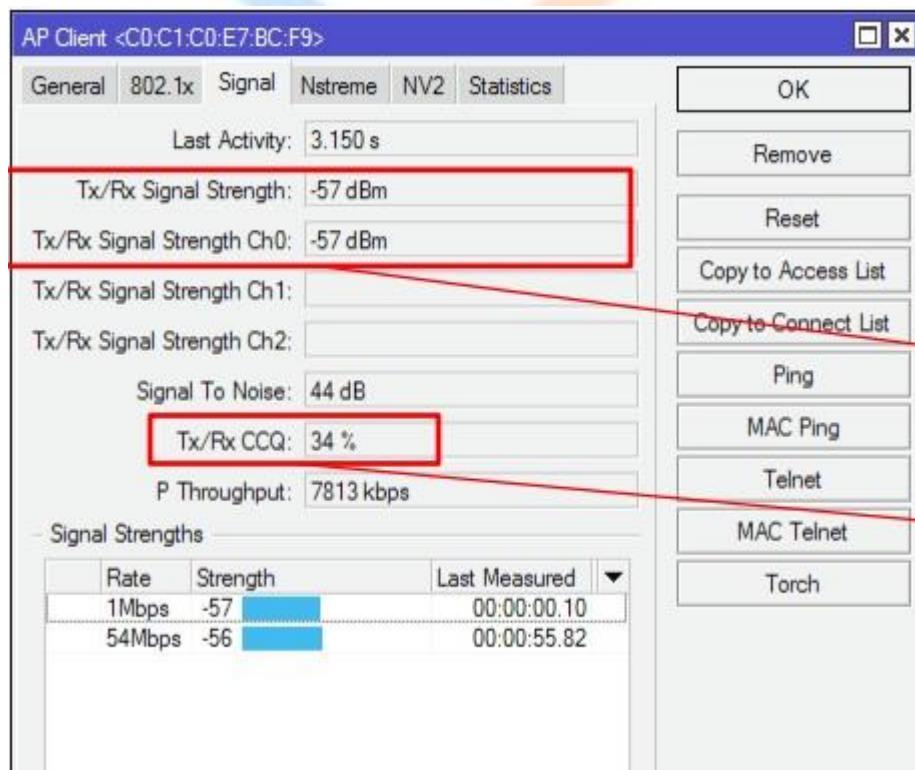
- MAC Address station yang ingin difilter
- Batas nilai kekuatan signal dari station yang ingin difilter
- Boleh koneksi atau tidak

Access Point – Default Authenticate



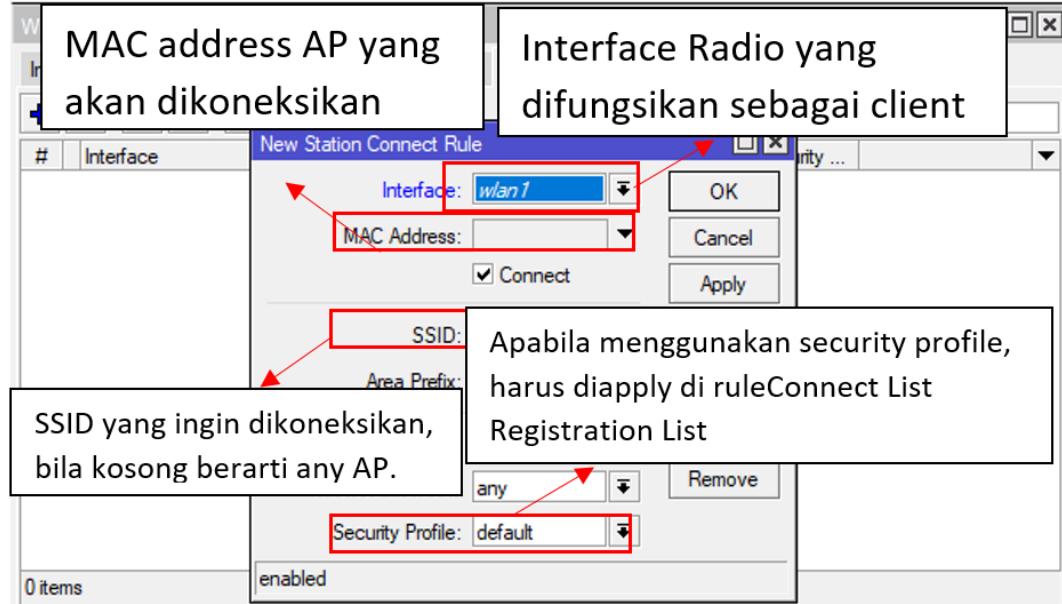
SSID:	STT-NF	Comment
Radio Name:	4C5E0CC3A651	Simple Mode
Scan List:	default	Torch
Wireless Protocol:	any	Scan...
Security Profile:	profile1	Freq. Usage...
Frequency Mode:	manual-txpower	Align...
Country:	no_country_set	Sniff...
Antenna Gain:	0 dBi	Snooper...
DFS Mode:	none	Reset Configuration
Proprietary Extensions:	post-2.9.25	
WMM Support:	disabled	
Bridge Mode:	enabled	
Default AP Tx Rate:	[] bps	
Default Client Tx Rate:	[] bps	
<input type="checkbox"/> Default Authenticate <input type="checkbox"/> Default Forward <input type="checkbox"/> Hide SSID		

Access List dapat berfungsi apabila wireless default authenticate di non aktifkan (unchecked). Artinya by default station tidak akan bisa koneksi ke AP apabila tidak di allow di Access List.



Station – Connection List

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

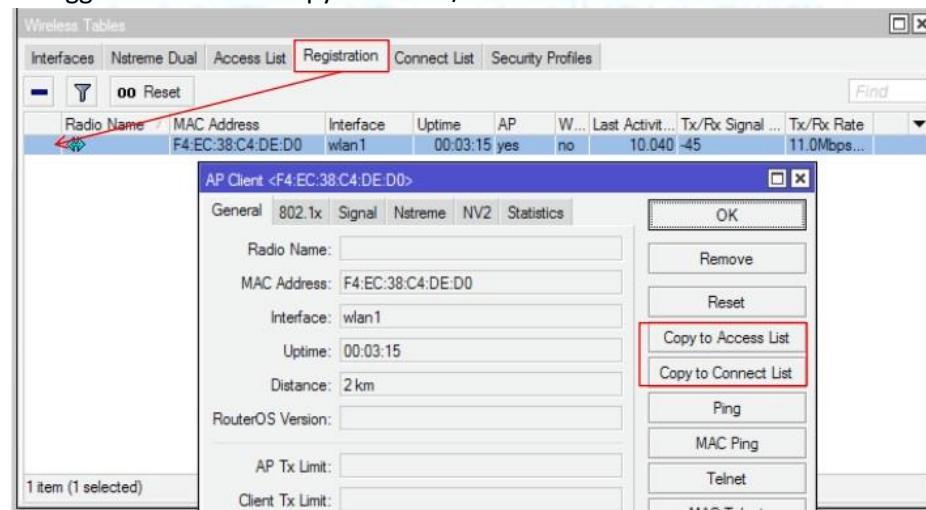


Keterangan :

- Interface radio yang difungsikan sebagai client
- MAC address AP yang akan dikoneksikan.
- Boleh / tidak boleh koneksi dengan MAC diatas
- SSID yang ingin dikoneksikan, bila kosong berarti any AP.
- Apabila menggunakan security profile, harus diapply di ruleConnect List

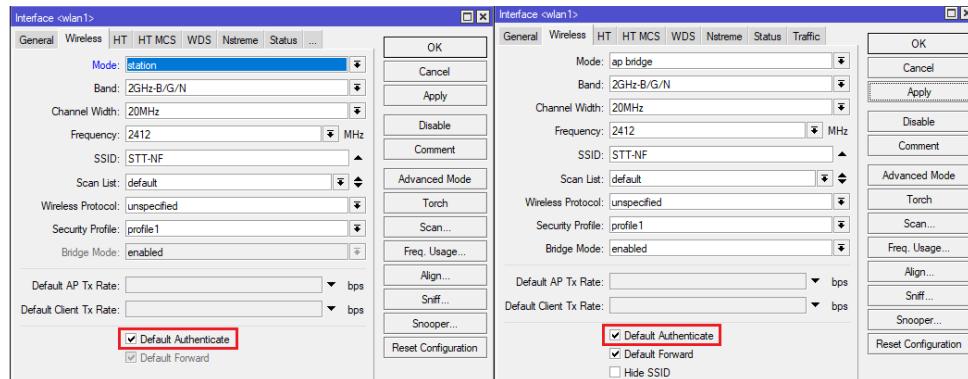
Registration List

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



Default Authenticated

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

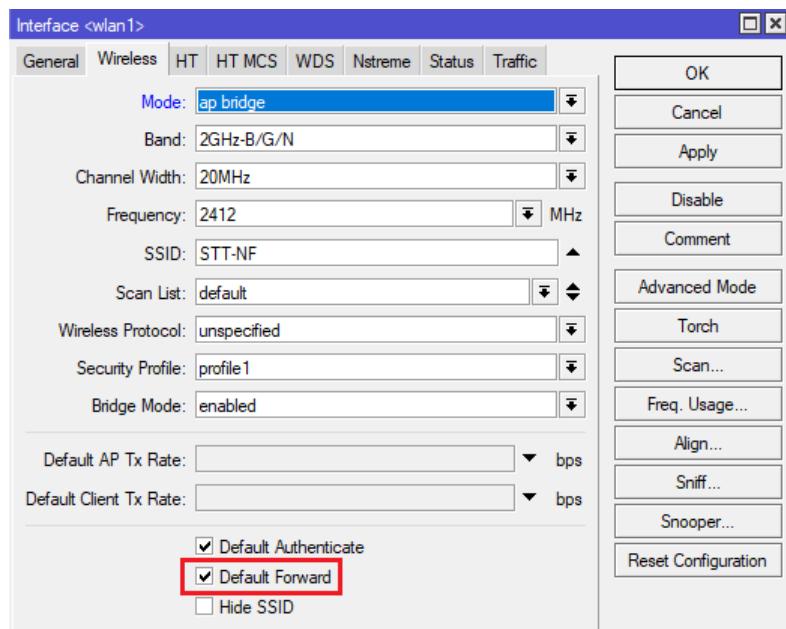


LAB – MAC Filtering

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

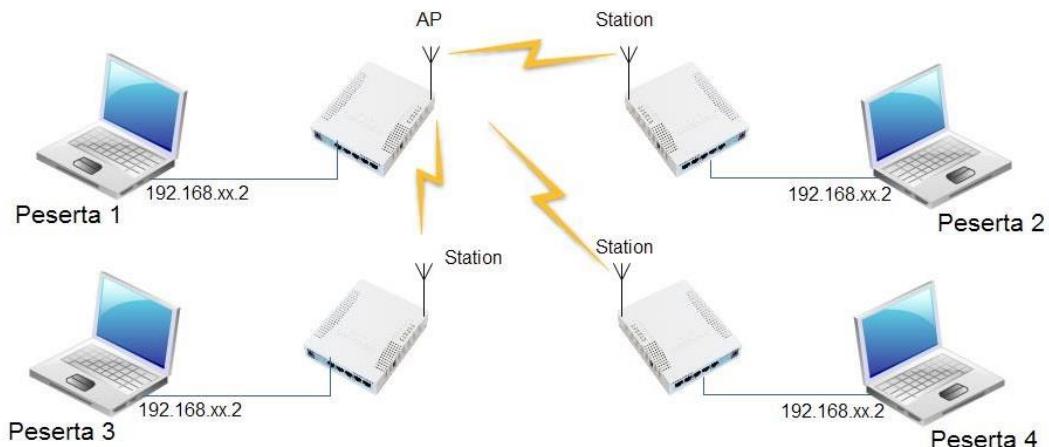
Drop Koneksi Antar Client

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



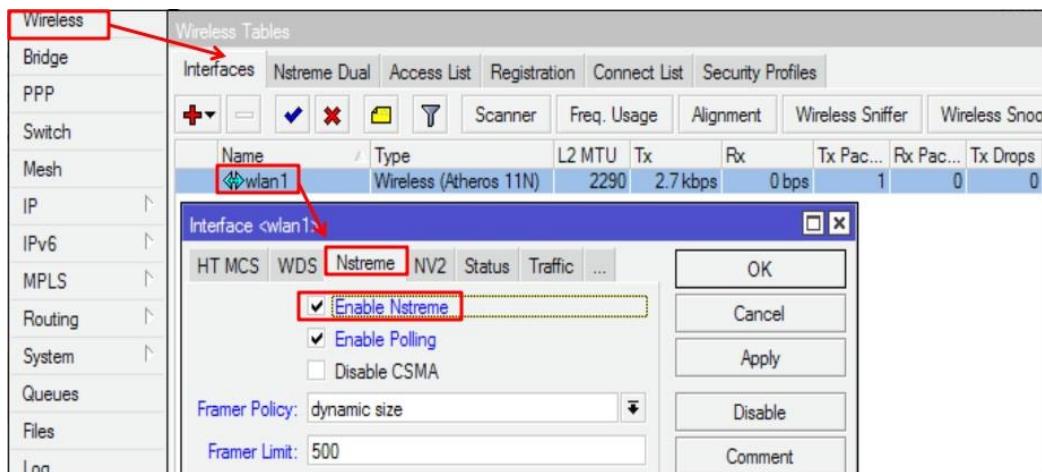
- Default forward biasanya didisable untuk alasan keamanan.
- Sesama station tidak dapat berkomunikasi, apabila default forward di uncheck

LAB – Default Fowarding



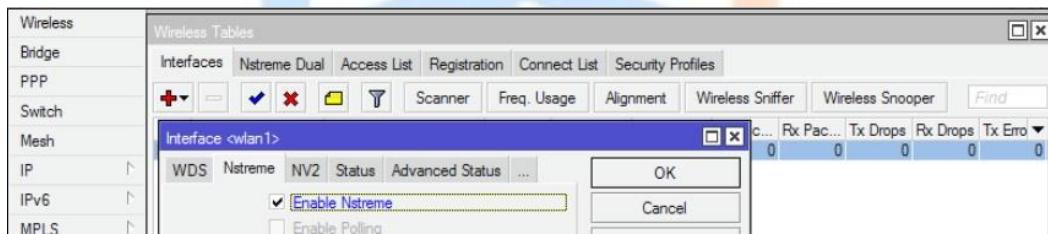
- Cobalah ping antar peserta ketika default fowarding check dan uncheck Nstreme
- Nstreme adalah protocol wireless proprietary Mikrotik
- Meningkatkan perfomance link wireless jarak jauh.
- Untuk koneksi Nstreme harus diaktifkan baik di sisi AP maupun station
- Konfigurasi Nstreme hanya di sisi AP, client hanya meng-enable-kan saja

LAB - Wireless Nstreme



Keterangan : Setting di AP

LAB - Wireless Nstreme



Keterangan : Setting di station

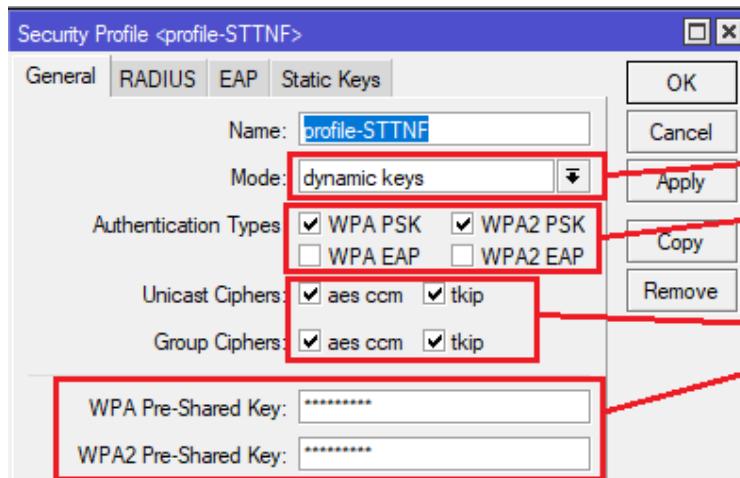
- Cobalah koneksi dengan Laptop ke AP yang mengaktifkan feature nstream

Wireless Security

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

Wireless Encryption – WPA

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

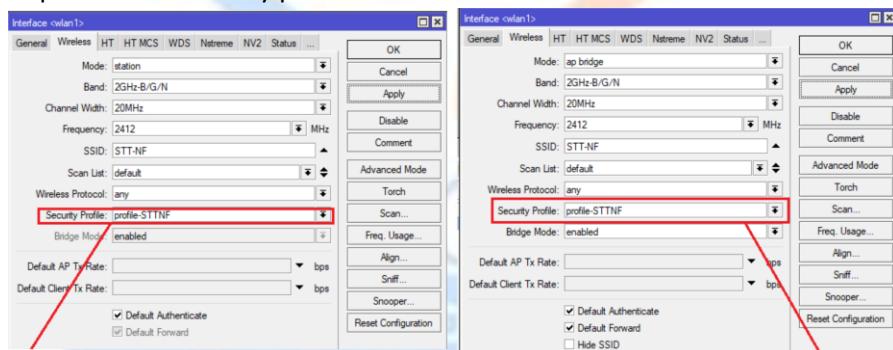


Keterangan :

- Dynamic key = WPA Static Key = WEP (lama)
- Jenis Authentifikasi
- Model Enkripsi
- Key Authentifikasi / password

Wireless Encryption

- Implementasi security profile



Keterangan :

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

WEP Encryption

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

LAB-WEP Encryption

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

LAB-WEP Encryption

LAB - Virtual Access Point

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



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

HotSpot

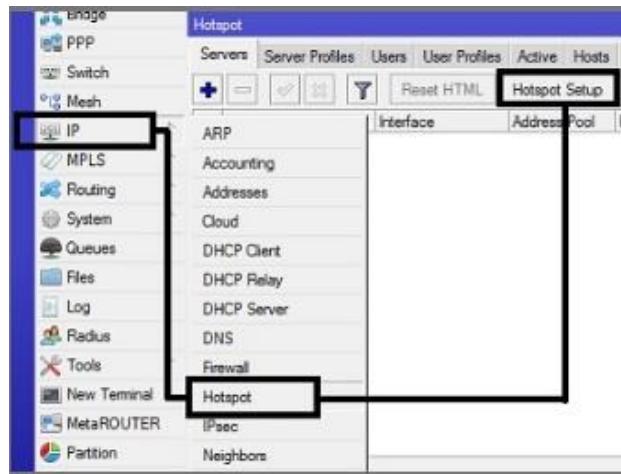
Router Mikrotik memiliki banyak fitur, salah satu fitur yang cukup populer dan banyak digunakan adalah Hotspot. Kelebihan Hotspot adalah kita dapat mengkonfigurasi jaringan yang hanya bisa digunakan dengan username dan password tertentu. Kita juga dapat melakukan manajemen terhadap user-user tersebut. Misalnya, mengatur durasi total penggunaan hotspot per user, membatasi berapa besar data yang dapat di download tiap user, mengatur konten apa saja yang boleh diakses user, dll.

Hotspot merupakan fitur gabungan dari berbagai service yang ada di Mikrotik, antara lain :

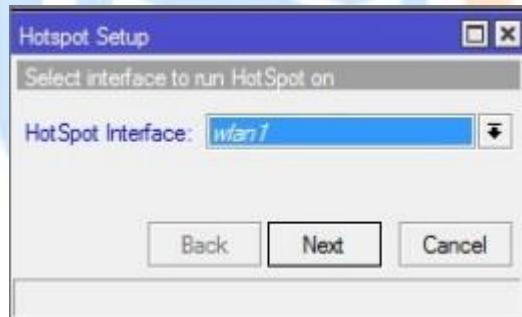
- DHCP server, digunakan untuk memberi layanan IP otomatis ke user
- Firewall NAT, untuk mentranslasi IP user ke IP yang bisa dikenali ke internet
- Firewall filter, untuk memblock user yang belum melakukan login
- Proxy, untuk memberikan tampilan halaman login
- dan sebagainya

Berikut cara setting dasar hotspot MikroTik :

Buka di menu **IP > Hotspot > Hotspot Setup**.



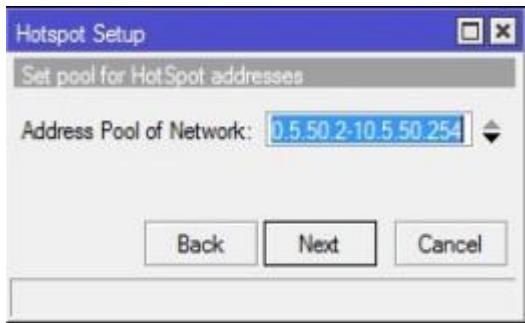
Dengan menekan tombol Hotspot Setup, wizard Hotspot akan mengarahkan kita untuk melakukan setting dengan menampilkan kotak-kotak dialog pada setiap langkah nya.



1. Kita diminta untuk menentukan interface mana Hotspot akan diaktifkan. Pada kasus kali ini, Hotspot diaktifkan pada wlan1, dimana wlan1 sudah kita set sebagai access point (ap-bridge). Selanjutnya klik Next.



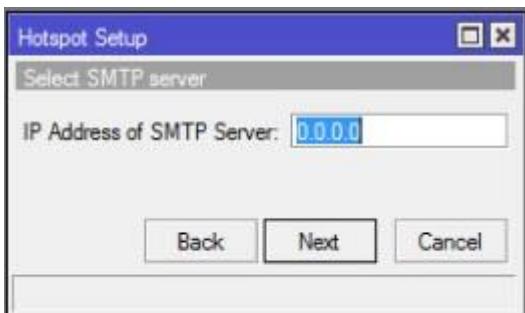
2. Jika di interface wlan1 sudah terdapat IP, maka pada langkah kedua ini, secara otomatis terisi IP Address yang ada di wlan1. Tetapi jika belum terpasang IP, maka kita bisa menentukan IP nya di langkah ini. Kemudian Klik Next.



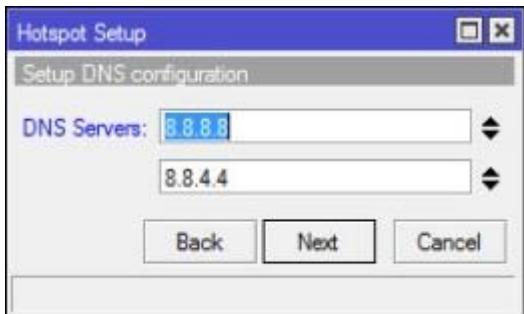
3. Tentukan range IP Address yang akan diberikan ke user (DHCP Server). Secara default, router otomatis memberikan range IP sesuai dengan prefix/subnet IP yang ada di interface. Tetapi kita bisa merubahnya jika dibutuhkan. Lalu klik Next.



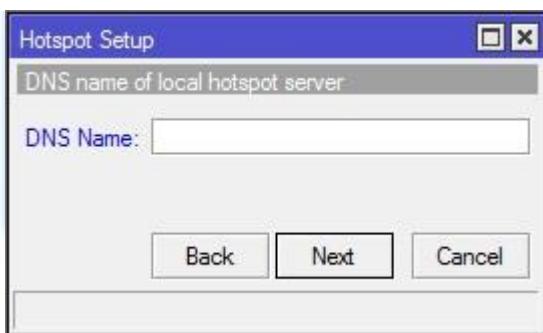
4. Menentukan SSL Certificate jika kita akan menggunakan HTTPS untuk halaman loginnya. Tetapi jika kita tidak memiliki sertifikat SSL, kita pilih none, kemudian klik Next.



5. Jika diperlukan SMTP Server khusus untuk server hotspot bisa ditentukan, sehingga setiap request SMTP client diredirect ke SMTP yang kita tentukan. Karena tidak disediakan smtp server, IP 0.0.0.0 kami biarkan default. Kemudian klik Next.



6. Di langkah ini, kita menentukan alamat DNS Server. Anda bisa isi dengan DNS yang diberikan oleh ISP atau dengan open DNS. Sebagai contoh, kita menggunakan DNS Server Google. Lalu klik Next.

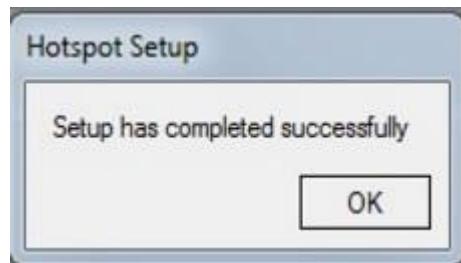


7. Selanjutnya kita diminta memasukkan nama DNS untuk local hotspot server. Jika diisi, nantinya setiap user yang belum melakukan login dan akan akses ke internet, maka browser akan diblokkan ke halaman login ini. Disini DNS name sebaiknya menggunakan format FQDN yang benar. Jika tidak diisi maka di halaman login akan menggunakan url IP address dari wlan1. Pada kasus ini, nama DNS-nya diisi "hotspot.AcademySTTNF". Lalu klik Next.



8. Langkah terakhir, tentukan username dan pasword untuk login ke jaringan hotspot Anda. Ini adalah username yang akan kita gunakan untuk mencoba jaringan hotspot kita. Sampai pada langkah ini, jika di klik Next

maka akan muncul pesan yang menyatakan bahwa *setting* Hotspot telah selesai.

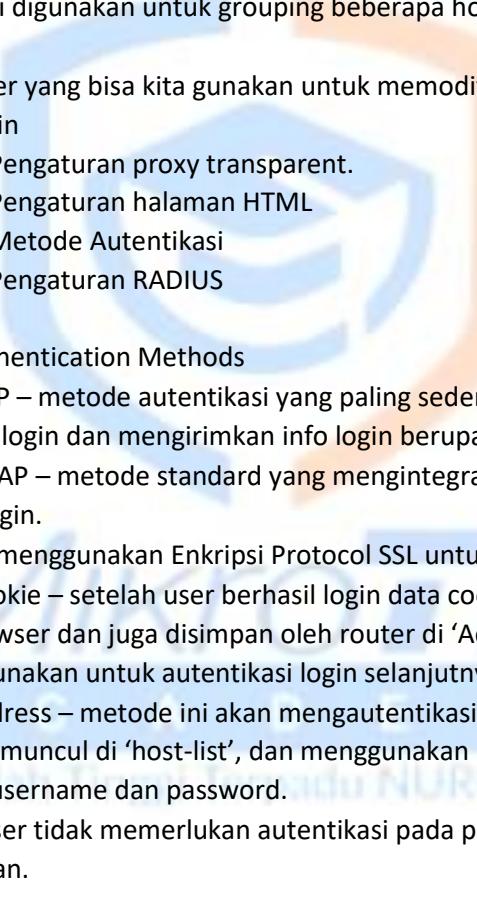


9. Selanjutnya kita akan mencoba mengkoneksikan laptop ke wifi hotspot yang sudah kita buat. Kemudian buka browser dan akses web sembarang (pastikan Anda mengakses web yang menggunakan protokol http, karena hotspot mikrotik belum mendukung untuk redirect web yang menggunakan https), maka Anda akan dialihkan ke halaman login hotspot seperti pada gambar berikut ini:



Untuk mencobanya, silahkan coba login dengan username dan password yang telah Anda buat pada langkah sebelumnya. Jika berhasil login maka akan membuka halaman web yang diminta dan membuka popup halaman status Hotspot.

Fitur – Fitur dalam Hotspot

- 
- 1) Hotspot Server
 - Didalam sebuah router bisa dibangun banyak hotspot server, dengan catatan dalam 1 interface hanya bisa untuk 1 hotspot server.
 - Di menu ini kita bisa mengaktifkan One to One Nat / universal client.
 - Kita bisa mengatur untuk timeout user yang belum melakukan login sehingga IP bisa dialokasikan ke user yang lain.
 - Selain itu kita juga bisa membatasi jumlah MAC sama yang melakukan request akses. Hal ini berguna untuk mencegah DHCP starvation.
 - 2) Hotspot Server Profile
 - Hotspot Server Profile digunakan untuk menyimpan konfigurasi-konfigurasi umum dari beberapa hotspot server.
 - Profile ini digunakan untuk grouping beberapa hotspot server dalam satu router.
 - Parameter yang bisa kita gunakan untuk memodifikasi hotspot server kita antara lain
 - Pengaturan proxy transparent.
 - Pengaturan halaman HTML
 - Metode Autentikasi
 - Pengaturan RADIUS
 - 3) Hotspot Authentication Methods
 - HTTP-PAP – metode autentikasi yang paling sederhana, yaitu menampilkan halaman login dan mengirimkan info login berupa plain text.
 - HTTP-CHAP – metode standard yang mengintegrasikan proses CHAP pada proses login.
 - HTTPS – menggunakan Enkripsi Protocol SSL untuk Autentikasi.
 - HTTP Cookie – setelah user berhasil login data cookie akan dikirimkan ke web-browser dan juga disimpan oleh router di ‘Active HTTP cookie list’ yang akan digunakan untuk autentikasi login selanjutnya.
 - MAC Address – metode ini akan mengautentikasi user mulai dari user tersebut muncul di ‘host-list’, dan menggunakan MAC address dari client sebagai username dan password.
 - Trial – User tidak memerlukan autentikasi pada periode waktu yang sudah ditentukan.
 - 4) HotSpot User
 - Halaman dimana parameter username, password dan profile dari user disimpan.
 - Beberapa limitasi juga bisa ditentukan di halaman user seperti uptime-limit dan bytes-in/bytes-out. Jika limitasi sudah tercapai maka user tersebut akan expired dan tidak dapat digunakan lagi.
 - IP yang spesifik juga bisa ditentukan di halaman ini sehingga user akan mendapat ip yang sama.
 - User bisa dibatasi pada MAC-address tertentu.
 - 5) Hotspot – Active

- Tabel active digunakan untuk memonitoring client yang sedang aktif / terautentikasi di hotspot server kita secara realtime.

6) Hotspot – Host

Tabel host digunakan untuk memonitoring semua perangkat yang terhubung dengan hotspot server baik yang sudah login ataupun belum

Flag yang tersedia didalam tabel Host

S : User sudah ditentukan IP nya didalam IP binding

H : User menggunakan IP DHCP

D : User menggunakan IP statik

A : User sudah melakukan login / Autentikasi

P : User di bypass pada IP binding.

7) Hotspot – IP bindings

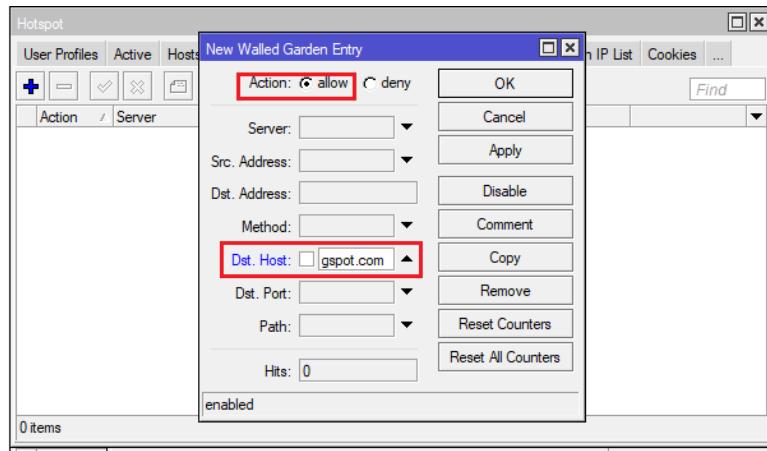
- One-to-one NAT bisa dikonfigurasi secara static berdasarkan
- Original IP Host
- Original MAC Address
- Bypass host terhadap Hotspot Authentication bisa dilakukan menggunakan IP-Bindings.
- Block Akses dari host tertentu (Berdasarkan Original MAC-address atau Original IP-Address) juga bisa dilakukan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

8) Hotspot – Service port

Sama seperti untuk klasik NAT, HotSpot tertanam satu-ke-satu ‘istirahat’ NAT beberapa protokol yang tidak kompatibel dengan terjemahan alamat. Untuk meninggalkan protokol ini konsisten, modul penolong harus digunakan. Untuk satu-ke-satu NAT satunya modul tersebut adalah untuk protokol FTP.

9) Hotspot – WalledGarden

WalledGarden adalah sebuah system yang memungkinkan untuk user yang belum terautentikasi menggunakan (Bypass!) beberapa resource jaringan tertentu tetapi tetap memerlukan autentikasi jika ingin menggunakan resource yang lain.



10) Hotspot – IP-WalledGarden list

IP-WalledGarden hampir sama seperti WalledGarden tetapi mampu melakukan bypass terhadap resource yang lebih spesifik pada protocol dan port tertentu. Biasanya digunakan untuk melakukan bypass terhadap server local yang tidak memerlukan autentikasi.

11) Hotspot – Cookies

- Cookie dapat digunakan untuk otentikasi dalam layanan Hotspot
- domain (read-only: text) – nama domain (jika berpisah dari username)
- expires-in (read-only: waktu) – berapa lama cookie tersebut valid
- mac-address (read-only: alamat MAC) – MAC address pengguna



Modul 6 Firewall

Pada modul ini akan dijelaskan tentang konfigurasi firewall pada mikrotik. Disini saya akan mengkonfigurasi firewall secara ringkas. Untuk itu baiknya kita lebih mengetahui apa itu firewall.

Firewall adalah perangkat yang berfungsi untuk memeriksa dan menentukan paket data yang dapat keluar atau masuk dari sebuah jaringan. Dengan kemampuan tersebut maka firewall berperan dalam melindungi jaringan dari serangan yang berasal dari jaringan luar (outside network). Firewall mengimplementasikan packet filtering dan dengan demikian menyediakan fungsi keamanan yang digunakan untuk mengelola aliran data ke, dari dan melalui router. Sebagai contoh, firewall difungsikan untuk melindungi jaringan lokal (LAN) dari kemungkinan serangan yang datang dari Internet. Selain untuk melindungi jaringan, firewall juga difungsikan untuk melindungi komputer user atau host (host firewall).

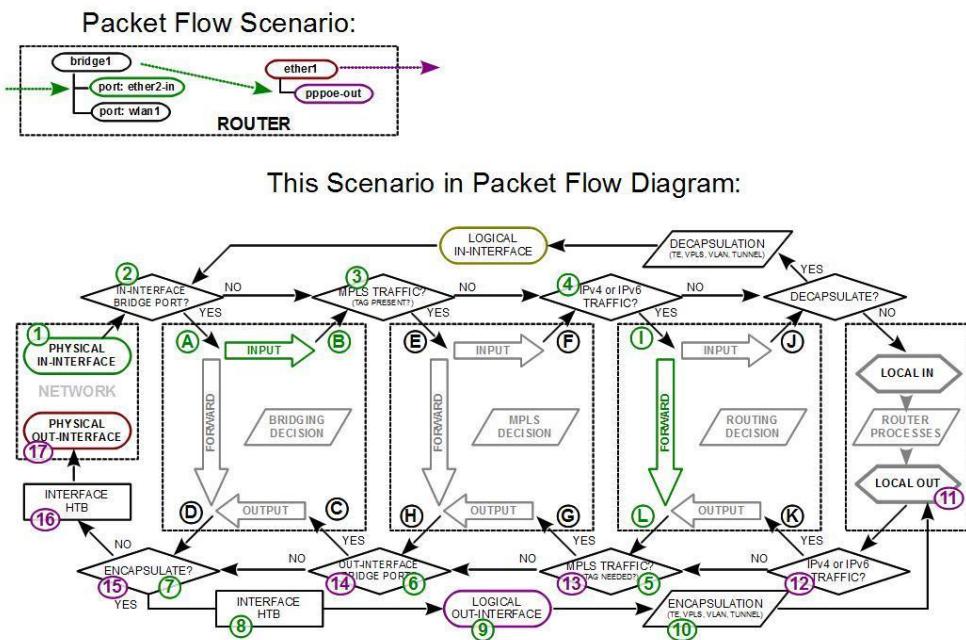
Firewall digunakan sebagai sarana untuk mencegah atau meminimalkan risiko keamanan yang melekat dalam menghubungkan ke jaringan lain. Firewall jika dikonfigurasi dengan benar akan memainkan peran penting dalam penyebaran jaringan yang efisien dan infrastrure yang aman. MikroTik RouterOS memiliki implementasi firewall yang sangat kuat dengan fitur termasuk:

- stateful packet inspection
- Layer-7 protocol detection
- peer-to-peer protocols filtering
- traffic classification by:
 - source MAC address
 - IP addresses (network or list) and address types (broadcast, local, multicast, unicast)
 - port or port range
 - IP protocols
 - protocol options (ICMP type and code fields, TCP flags, IP options and MSS)
 - interface the packet arrived from or left through
 - internal flow and connection marks
 - DSCP byte
- packet content
- rate at which packets arrive and sequence numbers
- packet size
- packet arrival time
- DLL

Chain Firewall pada Mikrotik

- 'Chain Firewall', Fitur ini biasanya banyak digunakan untuk melakukan filtering akses (Filter Rule), Forwarding (NAT), dan juga untuk menandai koneksi maupun paket dari trafik data yang melewati router (Mangle). Supaya fungsi dari fitur firewall ini dapat berjalan dengan baik, kita harus menambahkan rule-rule yang sesuai. Terdapat sebuah parameter utama pada rule di fitur firewall ini yaitu 'Chain'. Parameter ini memiliki kegunaan untuk menentukan jenis trafik yang akan di-manage pada fitur firewall dan setiap fungsi pada firewall seperti Filter Rule, NAT, Mangle memiliki opsi chain yang berbeda.

Pengisian parameter chain pada dasarnya mengacu pada skema 'Traffic Flow' dari Router. Jadi kita harus mengenali terlebih dahulu jenis trafik yang akan kita manage menggunakan firewall. chain bisa dianaloginkan sebagai tempat admin mencegat sebuah trafik, kemudian melakukan firewalling sesuai kebutuhan.



BERIKUT ADALAH ISTILAH DAN ARTI DALAM FIREWALL MIKROTIK :

FILTER RULES

Filter rule biasanya digunakan untuk melakukan kebijakan boleh atau tidaknya sebuah trafik ada dalam jaringan, identik dengan accept atau drop. Pada menu Firewall → Filter Rules terdapat 3 macam chain yang

tersedia. Chain tersebut antara lain adalah *Forward*, *Input*, *Output*. Adapun fungsi dari masing-masing chain tersebut adalah sebagai berikut:

- - **Forward** :

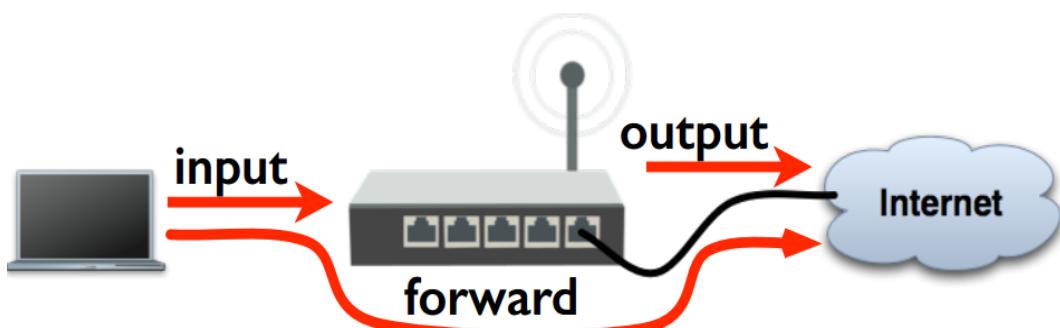
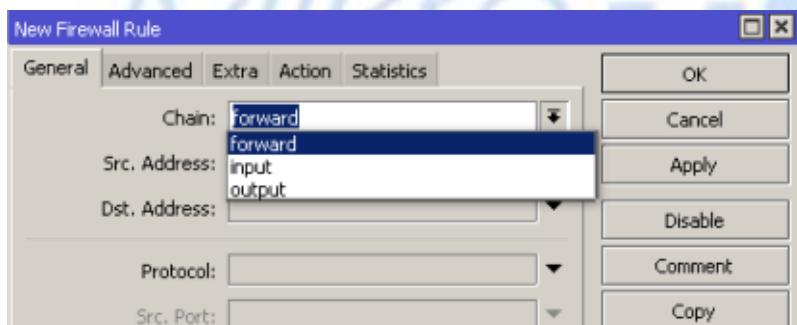
Digunakan untuk memproses trafik paket data yang hanya melewati router. Misalnya trafik dari jaringan public ke local atau sebaliknya dari jaringan local ke public, contoh kasus seperti pada saat kita melakukan browsing. Trafik laptop browsing ke internet dapat dimanage oleh firewall dengan menggunakan chain forward.

- - **Input** :

Digunakan untuk memproses trafik paket data yang masuk ke dalam router melalui interface yang ada di router dan memiliki tujuan IP Address berupa ip yang terdapat pada router. Jenis trafik ini bisa berasal dari jaringan public maupun dari jaringan lokal dengan tujuan router itu sendiri. Contoh: Mengakses router menggunakan winbox, webfig, telnet baik dari Public maupun Local.

- - **Output** :

Digunakan untuk memproses trafik paket data yang keluar dari router. Dengan kata lain merupakan kebalikan dari 'Input'. Jadi trafik yang berasal dari dalam router itu sendiri dengan tujuan jaringan Public maupun jaringan Local.Misal dari new terminal winbox, kita ping ke ip google. Maka trafik ini bisa ditangkap dichain output.



NAT (Network Address Translation)

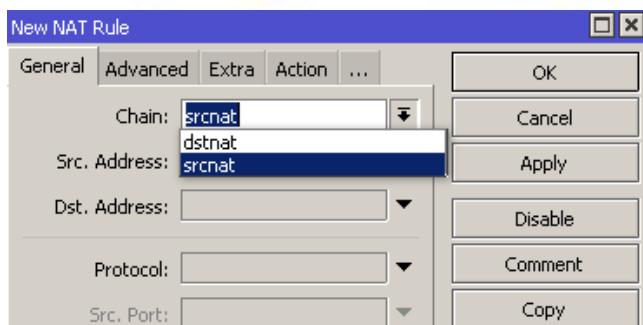
Pada menu Firewall → NAT terdapat 2 macam opsi chain yang tersedia, yaitu *dst-nat* dan *src-nat*. Dan fungsi dari NAT sendiri adalah untuk melakukan pengubahan *Source Address* maupun *Destination Address*. Kemudian fungsi dari masing-masing chain tersebut adalah sebagai berikut:

- *dstnat* :

Memiliki fungsi untuk mengubah destination address pada sebuah paket data. Biasa digunakan untuk membuat host dalam jaringan lokal dapat diakses dari luar jaringan (internet) dengan cara NAT akan mengganti alamat IP tujuan paket dengan alamat IP lokal. Jadi kesimpulan fungsi dari chain ini adalah untuk mengubah/mengganti IP Address tujuan pada sebuah paket data.

- *srcnat* :

Memiliki fungsi untuk mengubah source address dari sebuah paket data. Sebagai contoh kasus fungsi dari chain ini banyak digunakan ketika kita melakukan akses website dari jaringan LAN. Secara aturan untuk IP Address local tidak diperbolehkan untuk masuk ke jaringan WAN, maka diperlukan konfigurasi 'srcnat' ini. Sehingga IP Address lokal akan disembunyikan dan diganti dengan IP Address public yang terpasang pada router.



MANGLE

Pada menu Firewall → Mangle terdapat 4 macam pilihan untuk chain, yaitu *Forward*, *Input*, *Output*, *Prerouting*, dan *Postrouting*. Mangle sendiri memiliki fungsi untuk menandai sebuah koneksi atau paket data, yang melewati route, masuk ke router, ataupun yang keluar dari router. Pada implementasinya Mangle sering dikombinasikan dengan fitur lain seperti *Management Bandwidth*, *Routing policy*, dll. Adapun fungsi dari masing-masing chain yang ada pada mangle adalah sebagai berikut:

- Forward, Input, Output :

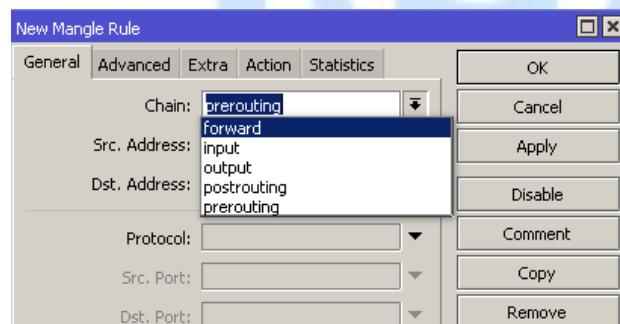
Untuk penjelasan mengenai Forward, Input, dan Output sebenarnya tidak jauh berbeda dengan apa yang telah diuraikan pada Filter rules diatas. Namun pada Mangle, semua jenis trafik paket data forward, input, dan output bisa ditandai berdasarkan koneksi atau paket data.

- Prerouting :

Merupakan sebuah koneksi yang akan masuk kedalam router dan melewati router. Berbeda dengan input yang mana hanya akan menangkap trafik yang masuk ke router. Trafik yang melewati router dan trafik yang masuk kedalam router dapat ditangkap di chain prerouting.

- Postrouting :

Kebalikan dari prerouting, postrouting merupakan koneksi yang akan keluar dari router, baik untuk trafik yang melewati router ataupun yang keluar dari router.



Address List

Address list, adalah salah satu fitur mikroTik yang fungsinya untuk memudahkan kita dalam menandai suatu konfigurasi address. Sehingga dengan address list, kita bisa membuat list address yang ingin di tandai tanpa harus mengganggu konfigurasi penting di fitur lainnya.

Fungsi lain address list adalah sebagai action pada firewall agar admin bisa menetukan address apa saja yang ingin ditandai dan dimasukan kedalam address list. Jika pada lab sebelumnya, kita menggunakan fitur log untuk membuat catatan aktifitas si Router. Bisa dibilang sama, address list juga memiliki fungsi membuat catatan seperti penanda address paket agar dimasukan kedalam address list.

Layer 7 protocols

Layer7-Protocol adalah metode pencarian pola terhadap paket data yang melewati jalur ICMP,TCP dan UDP.



L7 matcher mengumpulkan 10 paket pertama dari koneksi atau 2KB koneksi pertama dan mencari pola data yang dikumpulkan. Jika pola ini tidak ditemukan dalam data yang dikumpulkan, matcher berhenti memeriksa lebih lanjut. memori yang dialokasikan dibebaskan dan protokol dianggap sebagai tidak dikenal . Anda harus mempertimbangkan bahwa banyak koneksi secara signifikan akan meningkatkan penggunaan resource CPU dan memory . Untuk menghindari hal ini, tambahkan matchers firewall yang teratur untuk mengurangi jumlah data yang dikirimkan ke filter Layer-7 secara berulang-ulang.

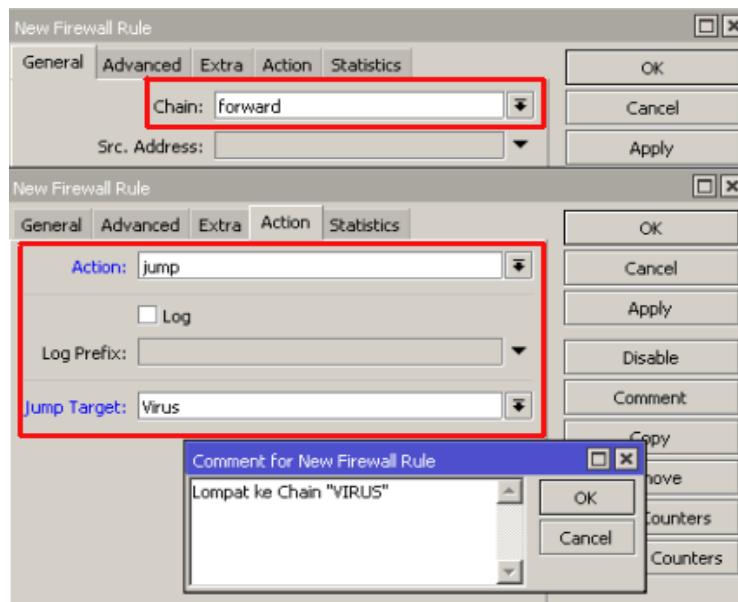
Persyaratan tambahan adalah bahwa Layer7 matcher harus melihat kedua arah lalu lintas (incoming dan outgoing). Untuk memenuhi persyaratan ini aturan L7 harus disetting pada chain **Forward**. Jika rule di set pada **Chain input/output** maka rule yang sama juga harus diset pada **Chain output/postrouting**, apabila data yang dikumpulkan mungkin tidak lengkap maka pola pencocokan akan salah.

CUSTOM CHAIN

Nah, selain jenis chain yang telah diuraikan diatas, sebenarnya ada jenis chain yang lain dimana kita bisa menambahkan atau menentukan sendiri nama dari chain tersebut selain dari forward, input, output dll. Nama chain tersebut dapat kita tentukan sendiri, namun pada prinsipnya tetap mnegacu pada chain utama yang tersedia di Firewall. Biasanya custom chain digunakan untuk menghemat resource router dan mempermudah admin jaringan dalam membaca rule firewall. By default router akan membaca rule firewall secara berurutan sesuai nomor urut rule firewall. Namun dengan fitur jump ini, admin jaringan dapat menentukan pembacaan rule firewall yang lebih efisien.

Untuk membuat *custom chain* tersebut kita memerlukan sebuah '**Action**' yaitu **Jump**. Jump sendiri berfungsi untuk melompat ke chain lain yang telah didefinisikan pada paramater **jump-target**. Sehingga kita bisa menempatkan rule dari *custom chain* yang telah kita buat pada urutan paling bawah. Ini dimaksudkan untuk mempermudah dalam pengelolaan rule-rule firewall, terlebih lagi jika kita memeliki rule-rule yang banyak. Adapun langkah-langkah pembuatan **Custom Chain** adalah sebagai berikut.

- Pada contoh kasus kali ini kita akan membuat sebuah rule yang mana akan melindungi perangkat client dari trafik yang mengandung virus. Untuk itu agar lebih mudah dalam pengelolaan kita akan membuat sebuah chain baru yang bernama “Virus” dengan jenis trafik “Forward”.
- Pertama, pilih menu **Firewall → Filter Rules**. Kemudian isikan parameter sesuai dengan tampilan gambar dibawah ini.



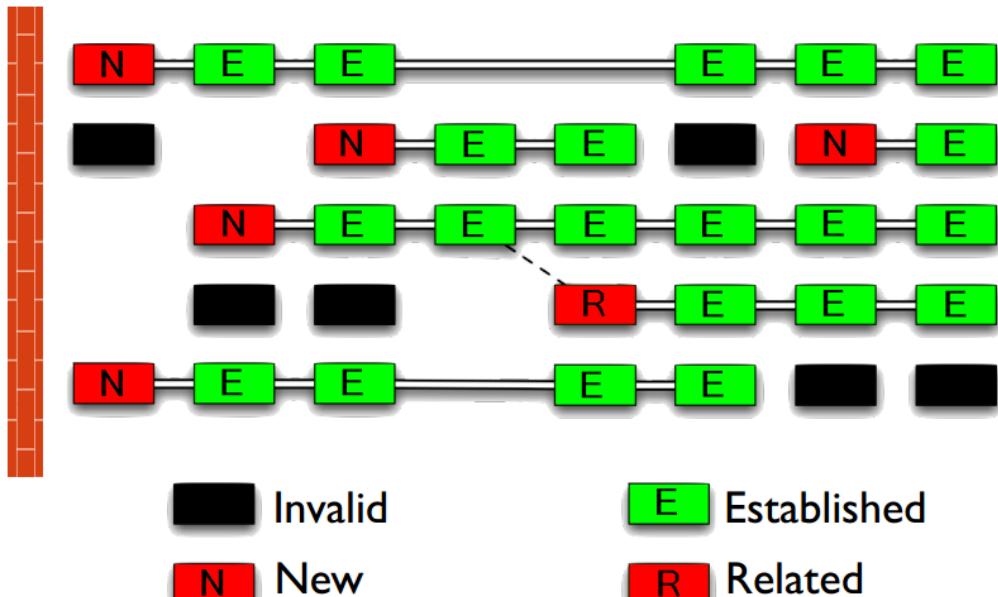
- Kemudian apabila kita telah selesai mengisikan parameter-parameter diatas maka akan tampil pada list firewall filter sebagai berikut.

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port
0	✗ drop	forward					
1	✓ acc...	forward					
::: Lompat ke Chain "VIRUS"							
2	✓ jump	forward					
::: Allow HTTP							
3	✓ acc...	forward			6 (tcp)		80
::: Allow SMTP							
4	✓ acc...	forward			6 (tcp)		25
::: allow TCP							
5	✓ acc...	forward			6 (tcp)		
::: allow ping							
6	✓ acc...	forward			1 (icmp)		
::: allow udp							
7	✓ acc...	forward			17 (udp)		
::: Chain VIRUS							
8	✗ drop	Virus			6 (tcp)		135-139
9	✗ drop	virus			17 (udp)		135-139
10	✗ drop	virus			6 (tcp)		445
11	✗ drop	virus			17 (udp)		445
12	✗ drop	virus			6 (tcp)		593
13	✗ drop	virus			6 (tcp)		1024-1099

Connection State (Status paket data yang melalui router)

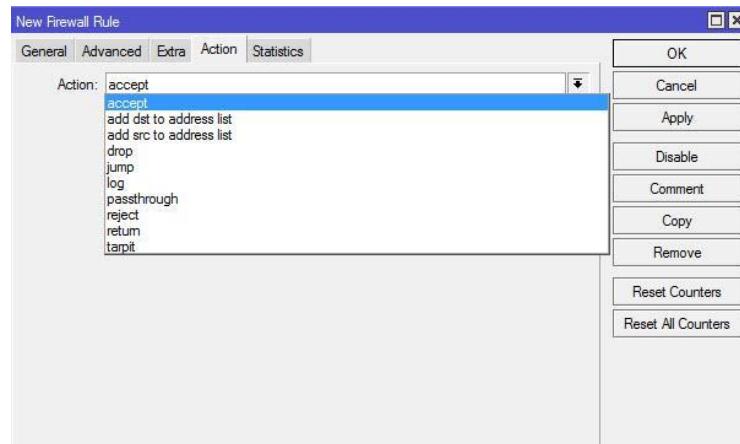
- Invalid** : paket tidak dimiliki oleh koneksi apapun, tidak berguna.
- New** : paket yang merupakan pembuka sebuah koneksi/paket pertama dari sebuah koneksi.

- **Established** : merupakan paket kelanjutan dari paket dengan status new.
- **Related** : paket pembuka sebuah koneksi baru, tetapi masih berhubungan dengan koneksi sebelumnya.



Action Filter Firewall RouterOS Mikrotik

- **Accept** : paket diterima dan tidak melanjutkan membaca baris berikutnya
- **Drop** : menolak paket secara diam-diam (tidak mengirimkan pesan penolakan ICMP)
- **Reject** : menolak paket dan mengirimkan pesan penolakan ICMP
- **Jump** : melompat ke chain lain yang ditentukan oleh nilai parameter jump-target
- **Tarpit** : menolak, tetapi tetap menjaga TCP connection yang masuk (membalas dengan SYN/ACK untuk paket TCP SYN yang masuk)
- **Passthrough** : mengabaikan rule ini dan menuju ke rule selanjutnya
- **log** : menambahkan informasi paket data ke log



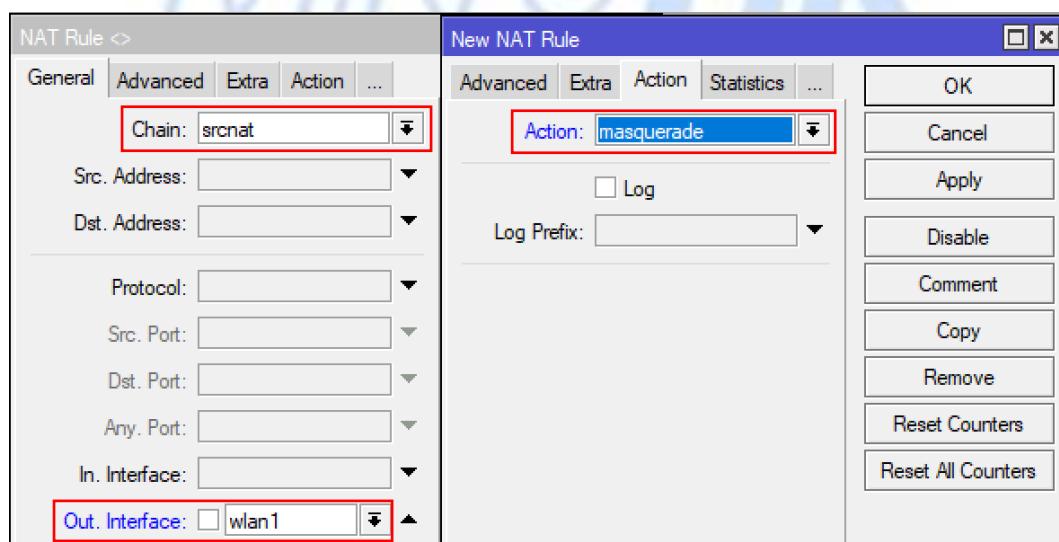
LAB Firewall

Source NAT

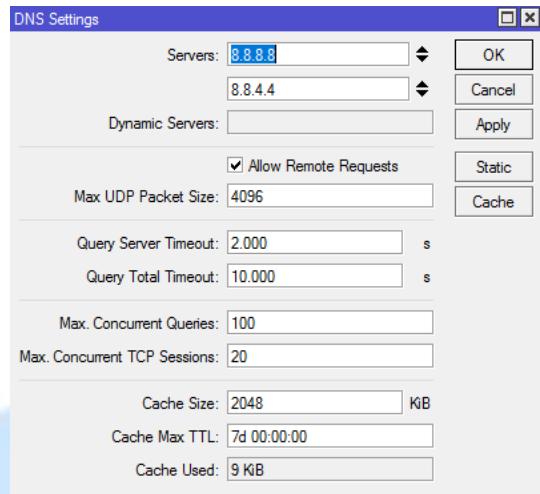
Apabila ingin menyembunyikan jaringan private LAN kita dengan alamat IP 192.168.30.0/24 dibelakang satu alamat IP 172.168.100.2 yang didapatkan dari ISP, kita bisa memanfaatkan fitur source NAT dengan action masquerade. Masquerade dapat merubah alamat IP serta port asal (source port) dari paket yang datang dari jaringan 192.168.30.0/24 ke alamat IP 172.168.100.2 saat sebelum paket keluar dari router.

Konfigurasinya seperti berikut :

1. Masuk menu IP – Firewall – NAT (+) add NAT Rule dan pilih Chain **srcnat** serta out interface **wlan1**
2. Pindah ke Tab Action – Pilih **Masquerade**



3. Pilih menu IP – DNS Setting



4. Selanjut nya Pilih IP – Route untuk menentukan IP GATEWAY

Route List						
	Dest. Address	Gateway	Distance	Routing Mark	Pref. Source	
DAS	► 0.0.0.0/0	192.168.43.1 reachable wlan1	1			
DAC	► 192.168.30.0/...	bridge reachable	0		192.168.30.1	
DAC	► 192.168.43.0/...	wlan1 reachable	0		192.168.43.44	
DAC	► 192.168.88.0/...	bridge reachable	0		192.168.88.1	

5. Dan coba test Ping ke website – Lihat Traffic pada Interface NAT tersebut sekarang Mikrotik sudah dapat ber internetan.

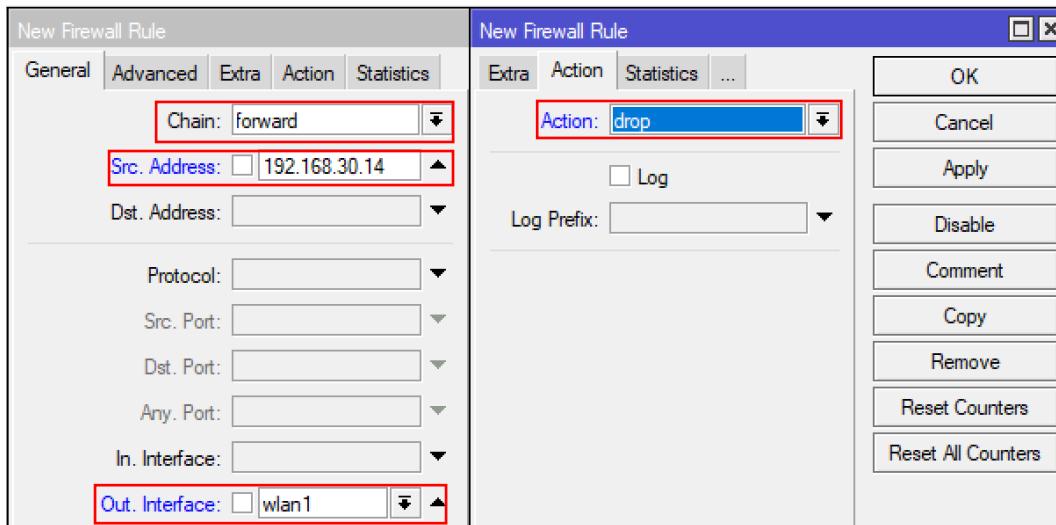
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets	
0	mas...	srcnat								ether1	426 B	6

45	103.49.221.211	56	128	43ms
46	103.49.221.211	56	128	41ms
47	103.49.221.211	56	128	47ms
48	103.49.221.211	56	128	44ms
49	103.49.221.211	56	128	42ms
50	103.49.221.211	56	128	45ms
51	103.49.221.211	56	128	39ms
52	103.49.221.211	56	128	44ms

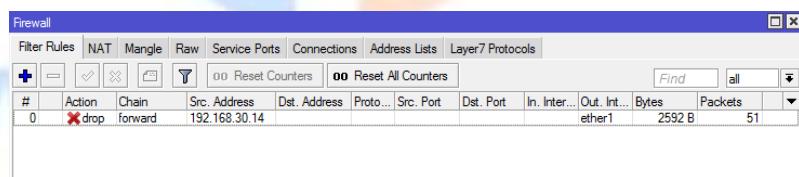
MEMBUAT FIREWALL UNTUK MEMBLOCK AKSES INTERNET DARI 1 IP ADDRESS CLIENT

- Buat New Firewall Rules, kemudian pilih “GENERAL”, pilih Chain : “FORWARD”.

2. setelah itu pilih Source Address dengan IP Address dari Client yang akan kita Block. Seperti Client dengan IP : 192.168.30.14
3. Pada pilihan Out Interface kita isi dengan interface : wlan1
4. kemudian pilih “ACTION”, dan pilih : “DROP”.
5. apabila ada Client dengan IP : 192.168.30.14 yang akan mengakses internet dengan OUTGOING melalui Interface wlan1, maka koneksi ini akan di DROP oleh Mikrotik.



6. Perhatikan Traffik dan Sekarang IP yang akan kita blokir tidak akan bisa mengakses ke Internet.

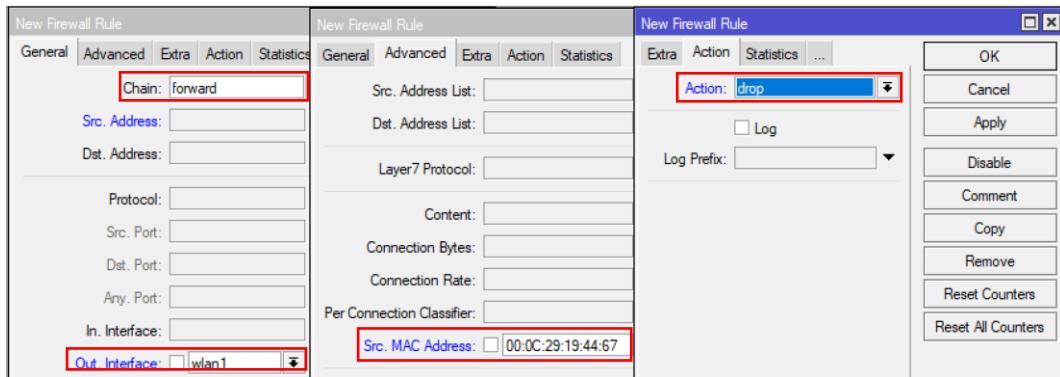


MEMBUAT FIREWALL UNTUK MEMBLOCK AKSES INTERNET DARI 1 MAC ADDRESS CLIENT

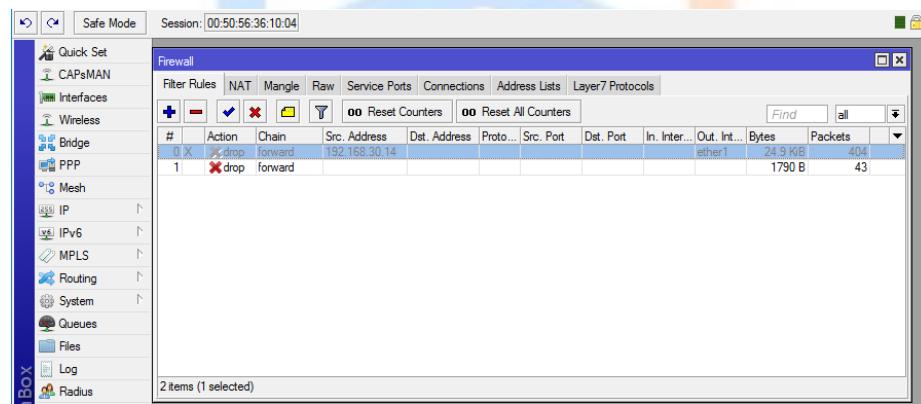
Selanjutnya adalah memblok akses internet dari 1 mac address client , untuk memblok akses internet dari 1 mac address client caranya sama yang berbeda hanya pada memblok akses internet dari 1 mac address client kita menggunakan menu advance untuk mencantumkan mac address, cara sebagai berikut:

1. Buat New Firewall Rules, kemudian pilih “GENERAL”, dan pilih Chain : “FORWARD”.
2. Out Interface kita isi dengan interface : ether1
3. Selanjutnya pilih “ADVANCED”, isikan pada “Source Mac Address” dari pada Mac Address yang dimiliki oleh Client/mac Address kita sendiri, yang akan kita Blokir akses internetnya. contohnya : **00:0C:29:19:44:67**
4. kemudian pilih “ACTION”, lalu pilih : “DROP”.

5. apabila ada Client yang mempunyai Mac Address sesuai Mac target yang akan mengakses internet dengan OUTGOING melalui Interface wlan1, maka koneksi ini akan di DROP oleh Mikrotik.



6. Perhatikan Traffik dan Sekarang IP yang akan kita blokir tidak akan bisa mengakses ke Internet.



MEMBUAT FIREWALL UNTUK MERIDIRECT Halaman Website Tertentu

1. Buat New Firewall Nat,pilih “CHAIN”,lalu pilih : “DSTNAT”.

pilih Destination Address dengan IP Address dari websites yang mau kita block. Misalnya Websites <http://www.nurulfikri.ac.id> dengan IP Public : 202.67.15.202

dikolom “ACTION”,lalu pilih:”redirect” to Port:80

The top screenshot shows the 'General' tab of a NAT rule configuration. It includes fields for Chain ('dstnat'), Source Address, Destination Address ('202.67.15.202'), Protocol ('6 (tcp)'), Source Port, and Destination Port ('80'). The bottom screenshot shows the 'Action' tab, where the 'redirect' action is selected, and the 'To Ports' field is set to '80'.

ketika ada user yang mengakses web <http://www.nurulfikri.ac.id> maka akan langsung dialihkan (redirect) webfig mikroTik

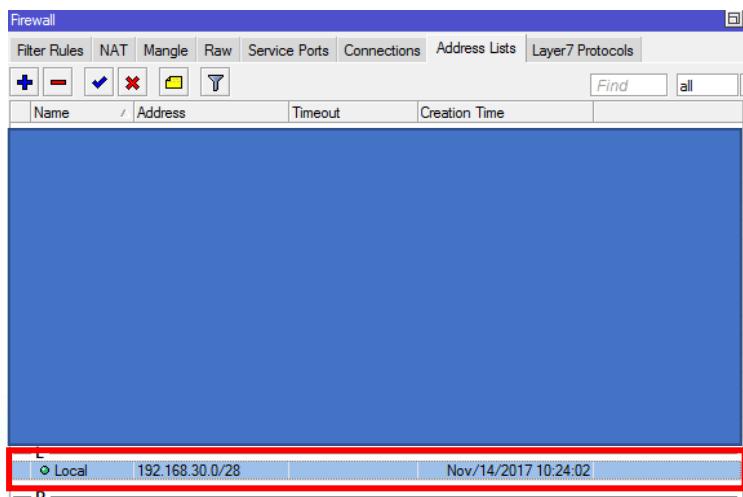
The screenshot shows the RouterOS Web Interface with the 'Interface List' tab selected. The table displays various network interfaces including bridge, ethernet, and wireless ports. The 'Name' column lists interfaces like 'bridge', 'ether1', 'ether2', 'ether3', 'ether4', 'lo0', 'test_bridge', and 'wlan1'. The 'Type' column indicates their nature (Bridge, Ethernet, Wireless). The 'Tx' and 'Rx' columns show traffic statistics. The 'Actions' column contains icons for managing each interface.

Lab Mangle

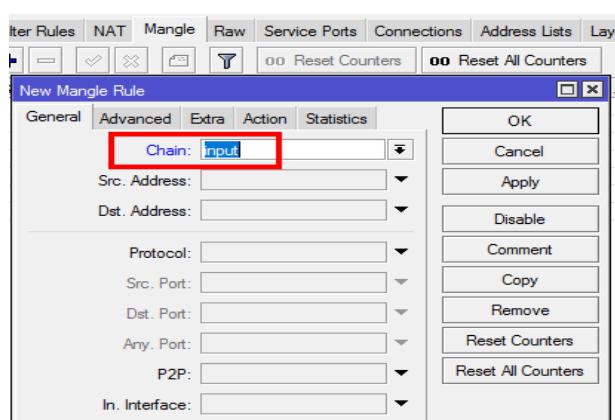
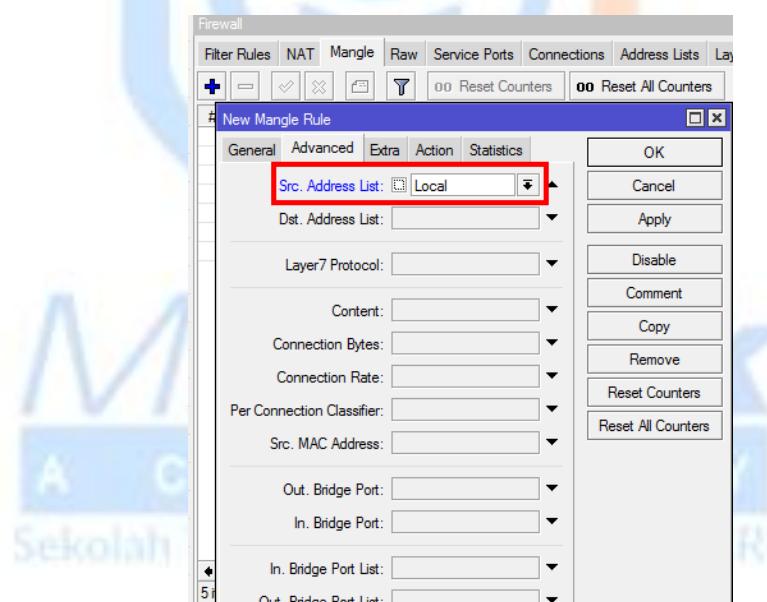
Konfigurasi firewall filter dengan mangle agar semua PC tidak dapat melakukan koneksi ke router untuk semua protocol.

1. Login ke router mikrotik dengan menggunakan winbox. Masuk ke menu IP => Firewall => Address List. Tambahkan blok ip address **LAN-Client** dalam hal ini 192.168.30.0/28 (**name=Local**)

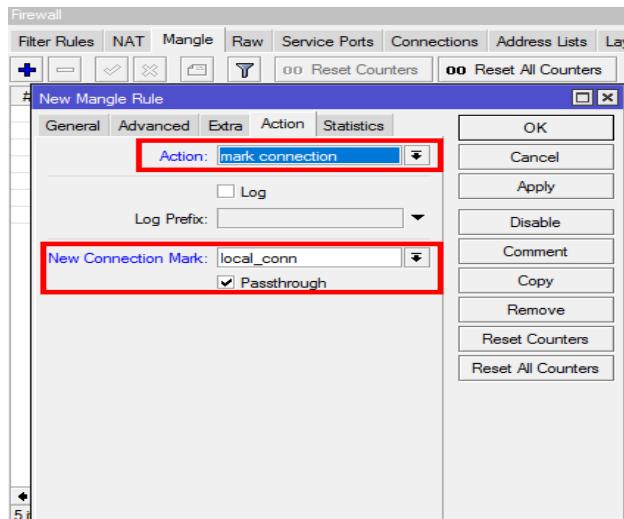
2. Tambahkan New Mangle Rule pada tab Mangle, pada tab General, pilih input pada kolom Chain.



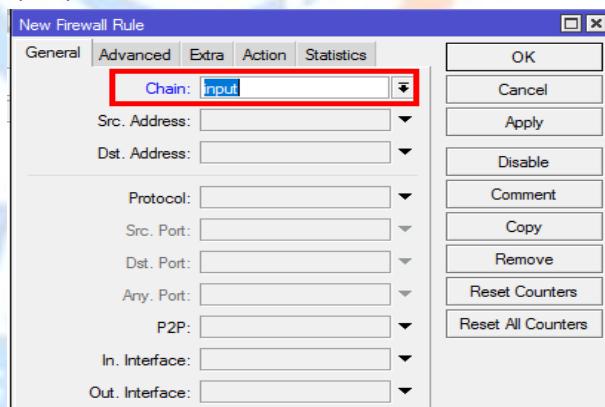
3. Pindah ke tab Advanced, pilih LAN Client pada Src. Address List.(Local)



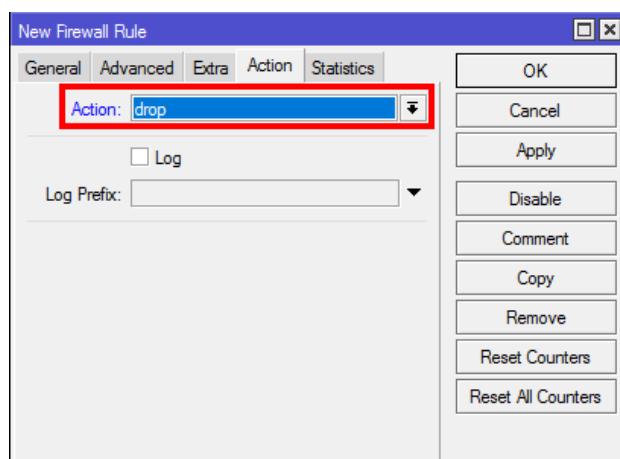
4. Pindah ke tab **Action**, pilih mark connection pada kolom **Action**, dan isikan "local_conn" pada kolom **New Connection Mark**. Dan ceklist **passthrough**.



5. Agar **LAN Client** tidak dapat melakukan koneksi ke router, masuk kembali ke menu IP => Firewall. Pada tab Filter Rules tambahkan **New Firewall Rule**. Pada tab **General**, pilih input pada kolom **Chain**.



6. Pindah ke tab **Action**, pilih **drop** pada kolom **Action**.



Mikrotik blokir web dengan membelokan ke server local

Dalam network suatu institusi diberlakukan aturan – aturan dengan alasan tertentu, kebijakan yang diberlakukan di network seperti contoh pemblokiran website tertentu agar karyawan tidak melakukan akses ke website yang dapat mengganggu pekerjaan karyawan maupun user pada penggunaan network / internet. Terdapat dua cara untuk memblokir website di MikroTIK:

- Blokir website dimikrotik dengan static dns
- Blokir website dengan membelokan ke server lokal

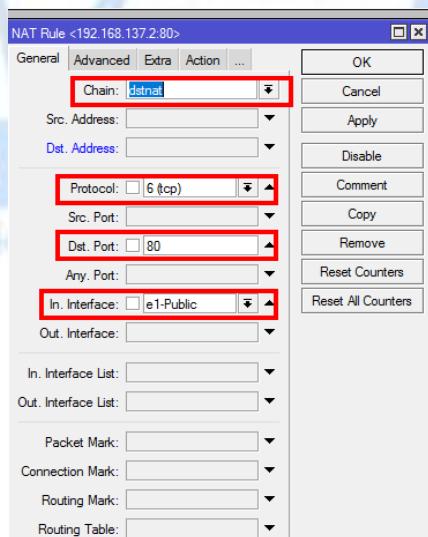
Konsep dalam pemblokiran website dengan static dns dan membelokan ke server local adalah sebagai berikut :

Saya sudah menyiapkan server local dengan web server local bisa menggunakan pc windows maupun linux dan sudah kita buat tampilan webpage yang akan muncul apabila user mengakses domain yang kita set untuk diblokkan ke server local

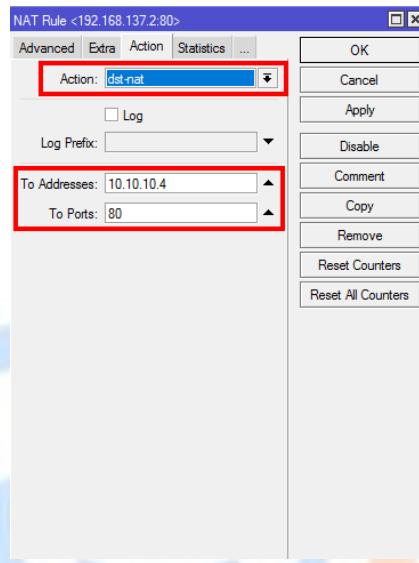
Konfigurasi Nat pada Firewall nat untuk memaksa akses dns ke dns mikrotik (dengan teknik ini user akan secara paksa menggunakan dns mikrotik walaupun user memakai dns lain).

- **Blokir website dengan membelokan ke server lokal**

Tambahkan Nat pilih **New NAT Rule**, kemudian isi **chain**, **Dst.Address** (isikan ip web server),**Protocol**, **in-interface**



Pindah ke tab **Action**, pilih mark connection pada kolom **Action**, dan isikan **To Address** dan **To Port (ip webserver)**

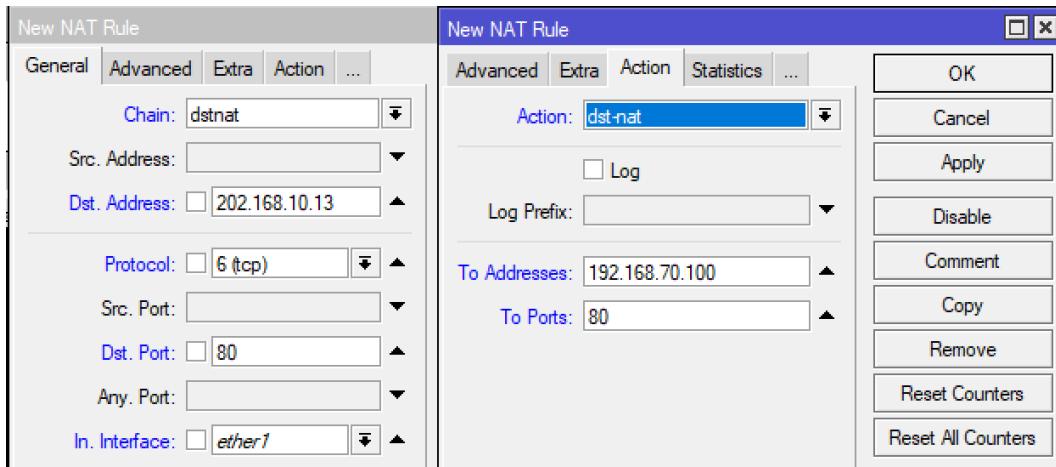


LAB DST-NAT dan SRC-NAT



Penerapannya, DST-NAT untuk WAN agar bisa di akses dari luar, sedangkan SCR-NAT untuk LAN akses dari Lokal. Misalnya saya mempunyai Web Server dengan Port 80. Saya ingin bisa diakses dari luar, cukup tambahkan rule berikut ini:

1. Buat New Firewall NAT,pilih "CHAIN", lalu pilih:"DSTNAT"
2. Pilih Destination Adresses 202.168.10.13 -> (IP Public yang kita pakai)
3. isikan Protokol "6(tcp) dan Dst.port 80
4. kemudian pilih "ACTION", kita pilih : "dst-nat" to Addresses: 192.168.70.100 (IP Lokal WebServer), to Port 80 (Port Web Server)

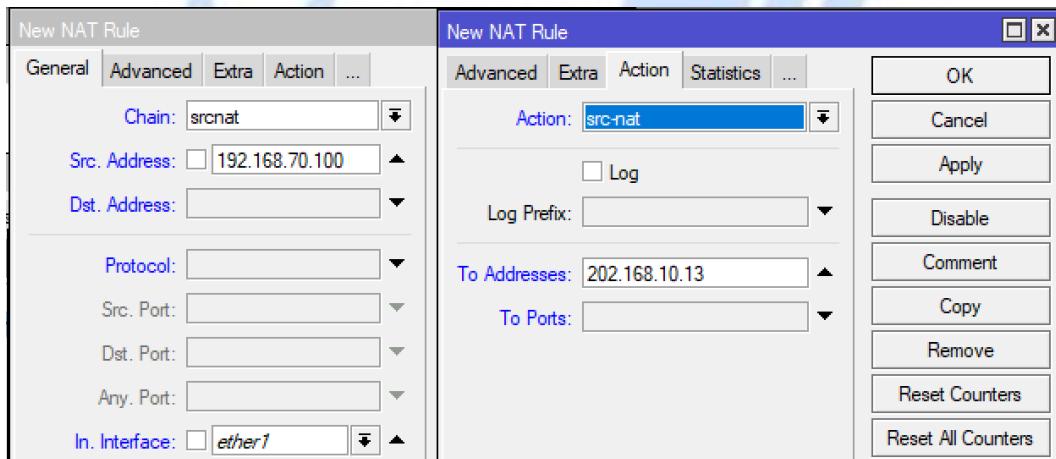


Jika konfigurasi sudah selesai, web server bisa di akses dengan mengunjungi alamat <http://202.168.10.13> (Alamat tersebut hanya bisa di akses dari luar)

Bagaimana jika web server dapat akses ke luar (internet)

Caranya hanya menggunakan teknik yang sama namun perbedaan hanya ada pada “srcnat”

- 1.Buat New Firewall NAT,pilih "CHAIN", lalu pilih:"SCRNAT"
- 2.Pilih Destination Adresses 192.168.70.100 -> (IP Local)
- 3.kemudian pilih “ACTION”, kita pilih : “src-nat” to Addresses: 202.168.10.13 (IP Public)

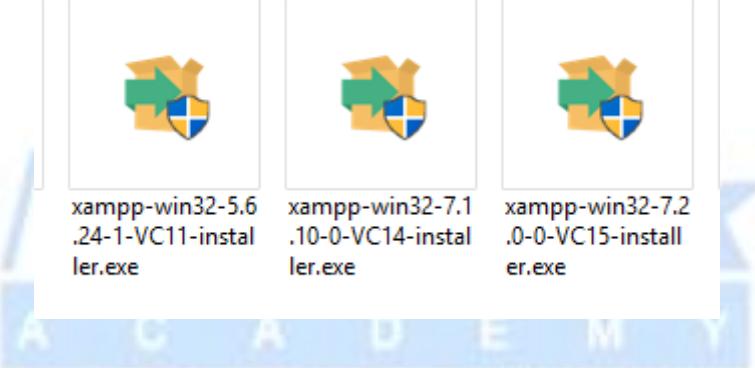


Server –Instalasi XAMPP

Persiapkan file XAMPP yang dapat di download melalui situs resmi apachefriends.org, pada gambar dibawah ini kita pilih pilih XAMPP for Windows dengan dimana Versi pada XAMPP adalah versi PHP yang kita gunakan.

The screenshot shows the Apache Friends Download page. At the top, there's a navigation bar with links like 'Secure', 'Download', 'Add-ons', 'Hosting', 'Community', 'About', 'Search', and language selection ('EN'). Below the navigation is a large 'Download' heading. To the right of the heading is a 'Documentation/FAQs' sidebar with text about the lack of a manual and links to various FAQs. The main content area displays a table for XAMPP for Windows versions 5.6.32, 7.0.26, and 7.1.12 & 7.2.0. The table includes columns for Version, Checksum (md5, sha1), and Size (110 Mb, 121 Mb). Each row has a 'Download (32 bit)' button. Below the table is a link to 'Add-ons and Themes'.

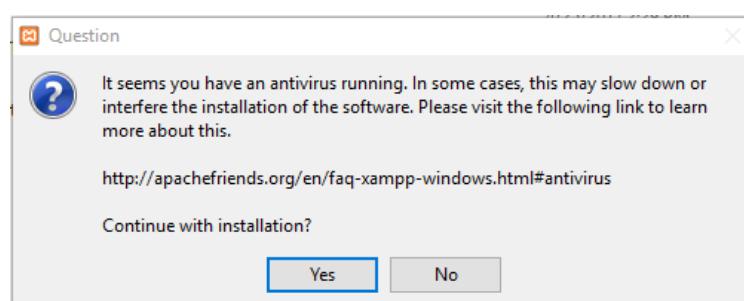
Setelah kita sudah mendapatkan file XAMPP yang selesai di download., kita doble klik / run icon XAMPP



Question saat instalasi XAMPP, Pilih Yes

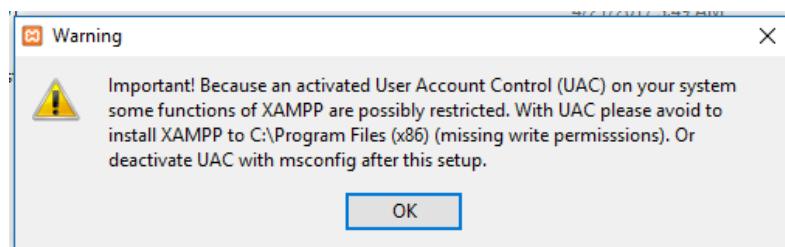
Program Antivirus sedang berjalan dimana akan membuat proses installasi XAMPP berjalan lambat.

Klik Yes to Continue

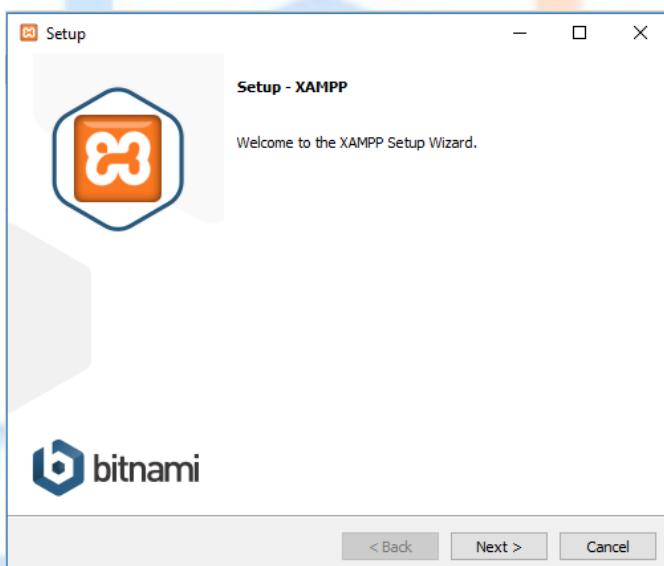


Warning saat instalasi XAMPP,
Pemberitahuan penting, bahwa Active User Account Control (UAC) pada windows,
dengan cara abaikan Install XAMPP di Folder (Permission) atau Deactive UAC setelah
setup selesai.

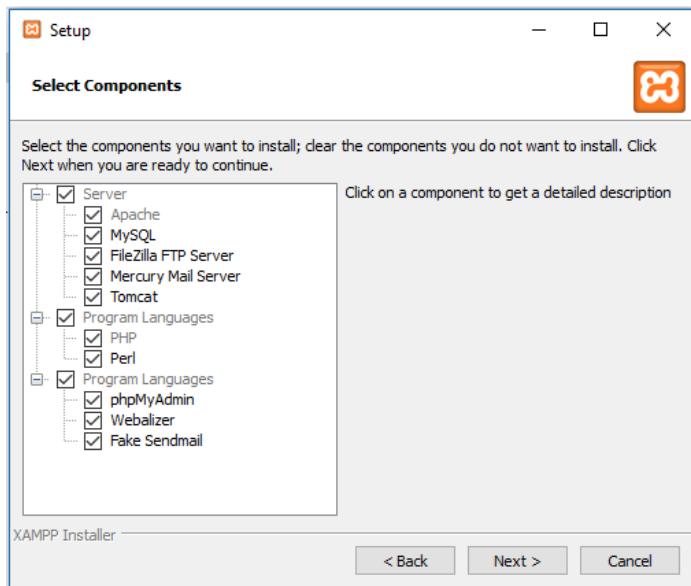
Klik Ok untuk melanjutkan.



Welcome XAMPP setup wizard., Klik Next untuk melanjutkan.

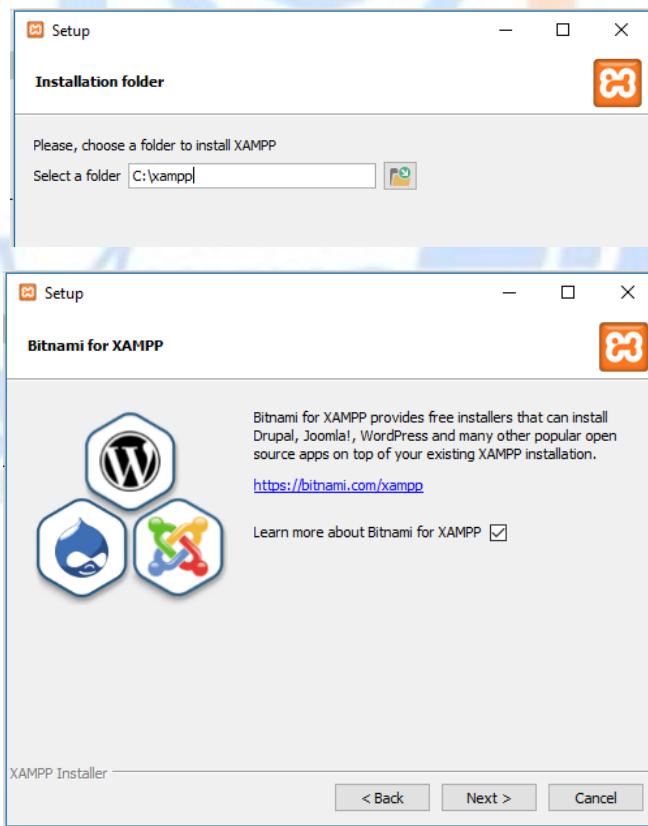


Select Components, biarkan saja default Component yang akan diinstall, Klik Next untuk
melanjutkan.

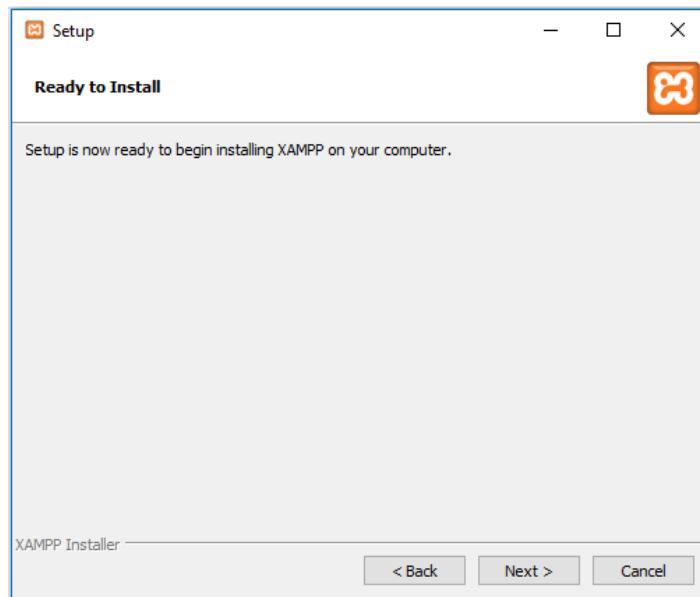


Installation Folder,

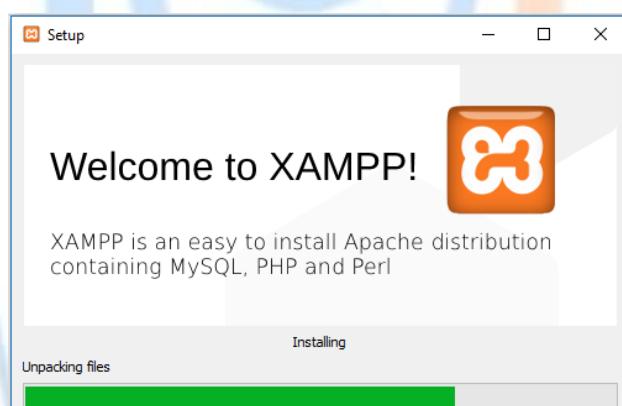
Lokasi dimana folder xampp di install, secara default pada windows akan diarahkan di C:\xampp



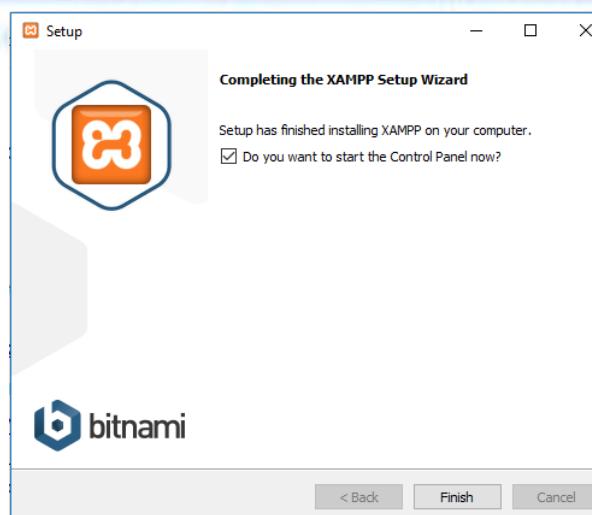
Bersiap Installasi Xampp, Klik Next untuk melanjutkan



Proses Unpacking File, tunggu hingga proses selesai.



Complting the XAMPP, setelah selesai ceklist untuk menjalankan Control Panel XAMPP, jika sudah klik FINISH..

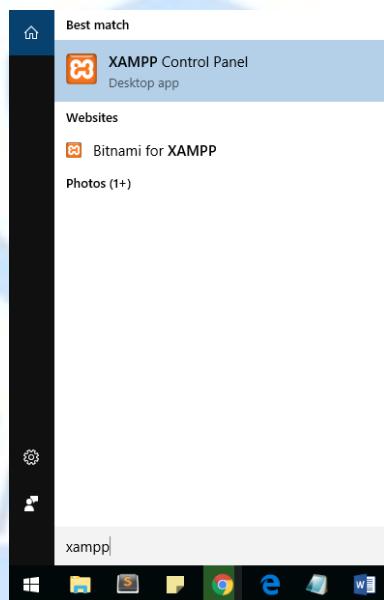


Pada awal membuka kita akan diajukan dengan pertanyaan mengenai Bahasa, pilih English(UK) untuk Bahasa default.

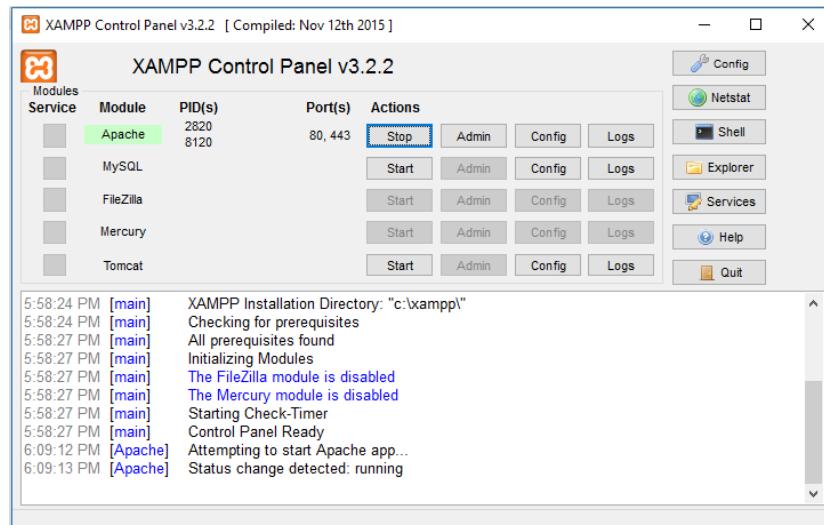


Running XAMPP

Untuk menjalankan service pada XAMPP control panel di windows kita klik Icon Windows Button, Search XAMPP maka akan muncul Launcher Aplikasi XAMPP, Double klik untuk memilih.



Setelah muncul XAMPP Control Panel kita dapat menjalankan service apache dan mysql dengan menekan Tombol ACTION start, maka akan muncul status active Apache PID 2820,8120 dengan Port 80, 443.



Modul 7 Tunneling

Tunneling di Mikrotik RouterOS ada beberapa macam yg di support, diantaranya adalah:

- EoIP
- PPTP
- SSTP
- PPPoE
- L2TP
- OVPN

Tunneling di mikrotik berada di menu PPP. Pada menu tersebut kita dapat mengkonfigurasikan client dan server dari beberapa tipe tunneling. Satu persatu tipe tunneling akan dijelaskan:

1. **EoIP** merupakan protokol pada Mikrotik RouterOS untuk membentuk sebuah network tunnel. EoIP merupakan protokol proprietary Mikrotik, sehingga jika ingin menggunakan EoIP sebagai protokol untuk membuat tunnel kedua sisi (kantor pusat dan kantor cabang) harus sama-sama menggunakan MikroTik.
2. **PPTP** (Point-to-point tunnelling protocol) menyediakan tunnel yg terenkripsi via IP. PPTP menggunakan port tcp-1723 dan ip protocol number 47. Enkripsi pada tunneling PPTP saat ini sudah gampang dijebol sehingga tidak direkomendasikan di terapkan pada production site. RouterOS support PPTP client dan server
3. **SSTP** (Secure Socket Tunnelling Protocol) merupakan penyempurnaan dari PPTP. SSTP menggunakan port tcp-443 sehingga memungkinkannya untuk ter-bypass oleh firewall dan proxy server. RouterOS mendukung SSTP client dan server
4. **PPPoE** merupakan tunneling point to point yg memungkinkan sebuah client dapat menggunakan layanan yg telah di sediakan dalam sebuah PPPoE server. PPoE client hanya dapat terkoneksi ke PPoE server yg satu broadcast domain. Contoh penggunaan PPPoE adalah pada jaringan speedy milik Telkom.

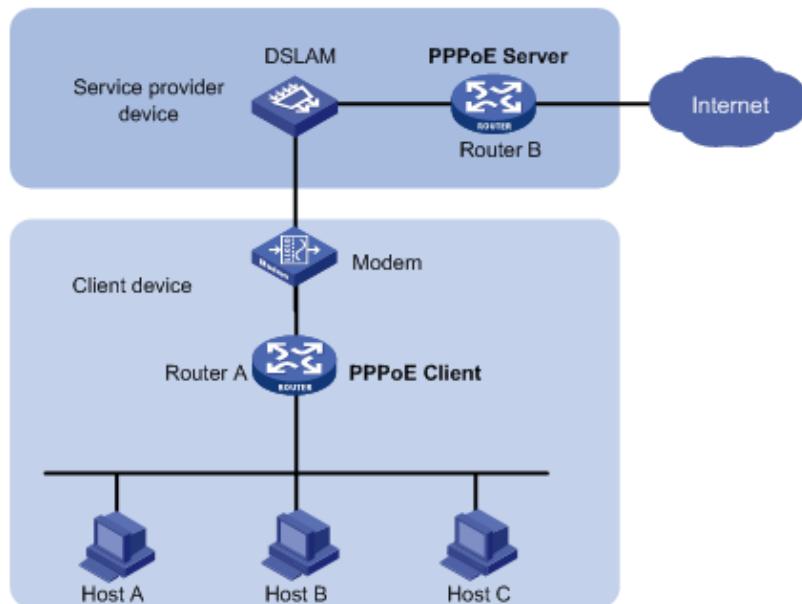


Figure 1 Topologi Koneksi PPPoE

5. **L2TP** (layer 2 Tunneling Protocol) merupakan jenis tunneling & encapsulation lain dari protocol PPP. L2TP mensupport non-TCP/IP protocol (frame relay, ATM dan Sonet). L2TP dikembangkan dengan menggabungkan fitur dari PPTP dengan protocol proprietary Cisco (Layer 2 Forwarding). L2TP dikembangkan dengan menggabungkan fitur dari PPTP dengan protocol proprietary Cisco (Layer 2 Forwarding). L2TP tidak melakukan enkripsi paket, untuk enkripsi biasanya L2TP dikombinasikan dengan IPsec. L2TP menggunakan UDP port 1701

Lab EoIP:

Buatlah tunnel EoIP sesuai dengan topologi dibawah ini agar pc kantor pusat dan ping ke pc kantor cabang:

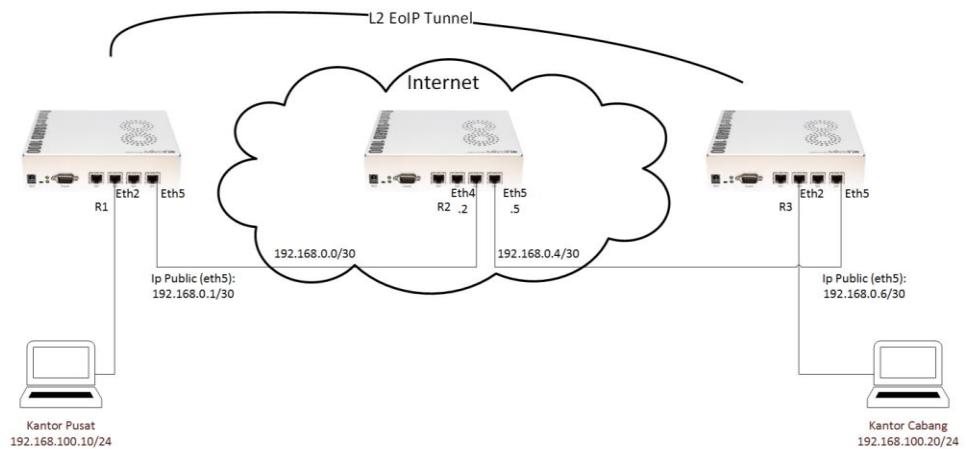


Figure 2 Topologi Lab EoIP

Langkah-langkah yg harus dikerjakan adalah:

1. Setting tiga buah mikrotik sesuai dengan topologi diatas (R2 berperan sebagai router internet)
2. Tambahkan default route (0.0.0.0/0) pada R1 dan R3 dan set gatewaynya ke arah R2
Ip → route → add new (+)

Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS ▶ 0.0.0.0/0	192.168.0.2 reachable ether2	1		
DAC ▶ 192.168.0.0/30	ether2 reachable	0		192.168.0.1

Figure 3 Default route di R1

Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS ▶ 0.0.0.0/0	192.168.0.5 reachable ether2	1		
DAC ▶ 192.168.0.4/30	ether2 reachable	0		192.168.0.6

Figure 4 Default Route di R3

3. Buat EoIP tunnel di R1 dan R3

Interface → EoIP Tunnel

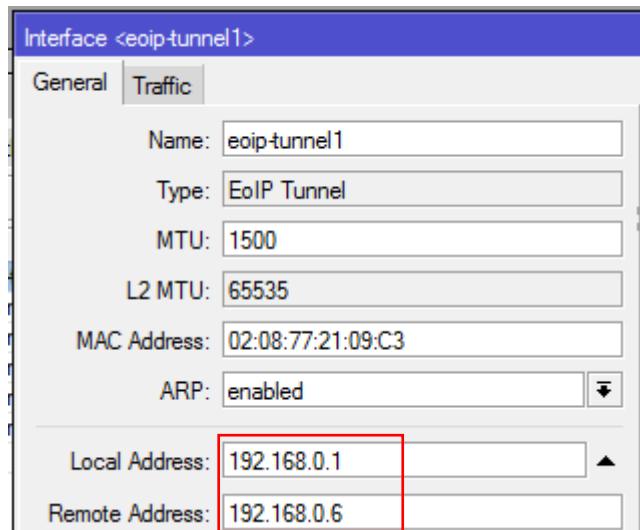


Figure 5 Konfigurasi pada R1

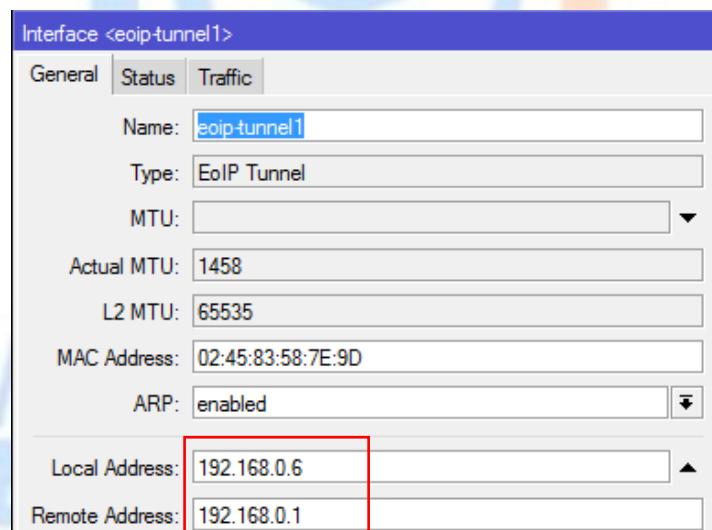


Figure 6 Konfigurasi Pada R3

4. Lakukan bridging interface Eth2 dengan interface EoIP pada R1

Bridge							
Bridge		Ports		Filters		NAT	
<input style="width: 20px; height: 20px; border: none; background-color: #ccc; border-radius: 50%;" type="button" value="+"/>		<input style="width: 20px; height: 20px; border: none; background-color: #ccc; border-radius: 50%;" type="button" value="-"/>		<input style="width: 20px; height: 20px; border: none; background-color: #ccc; border-radius: 50%;" type="button" value="✓"/>		<input style="width: 20px; height: 20px; border: none; background-color: #ccc; border-radius: 50%;" type="button" value="✗"/>	
Interface	Bridge	Priority (h...)	Path Cost	Horizon	Role	Root Pat...	
eoip-tunnel1	bridge	80	10		designated port		
Ether2-master	bridge	80	10		designated port		

Figure 7 bridge interface di R1

5. Lakukan bridging interface Eth2 dengan interface EoIP pada R2

Bridge							
Bridge		Ports	Filters	NAT	Hosts		
							Find
Interface	/	Bridge	Priority (h...)	Path Cost	Horizon	Role	Root Pat...
Eoiptunnel1		bridge	80	10		designated port	
Ether2-master		bridge	80	10		designated port	

Figure 8 bridge interface di R3

6. Ping dari PC kantor pusat ke ip 192.168.100.20

Lab PPTP:

Buatlah tunnel menggunakan protokol PPTP dari R1 ke R3 sesuai dengan topologi dibawah ini dan lakukan traceroute ke ip 10.10.10.10 dari R1 setelah PPTP terbentuk

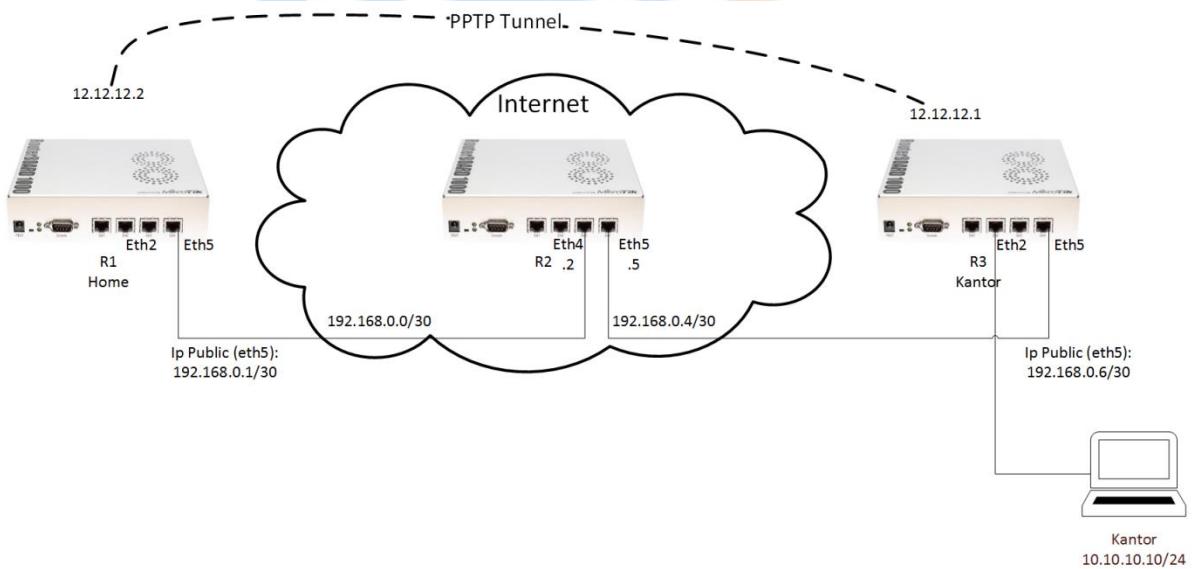


Figure 9 Topologi lab PPTP

Langkah-langkanya adalah sebagai berikut:

1. Aktifkan terlebih dahulu PPTP server di router R3 (kantor)
PPP → PPTP

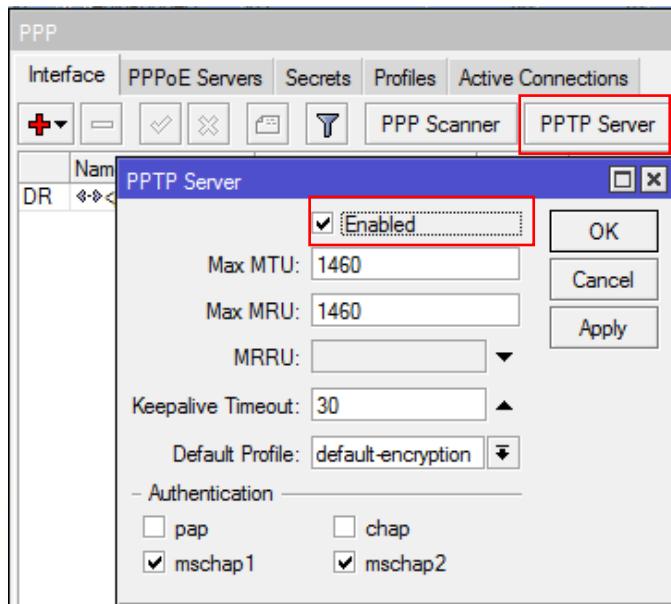
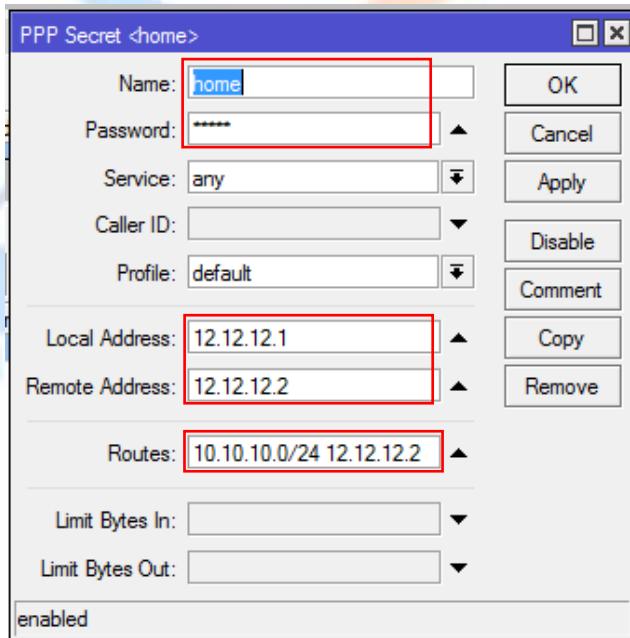


Figure 10 Enable PPTP Server di R3

2. Buat PPP secret di R3. Config dari PPP secret terlihat pada gambar dibawah ini:
PPP → secret (tab)



3. Konfigurasikan PPTP client di router R1 (home)
PPP → PPTP Client (add new (+))

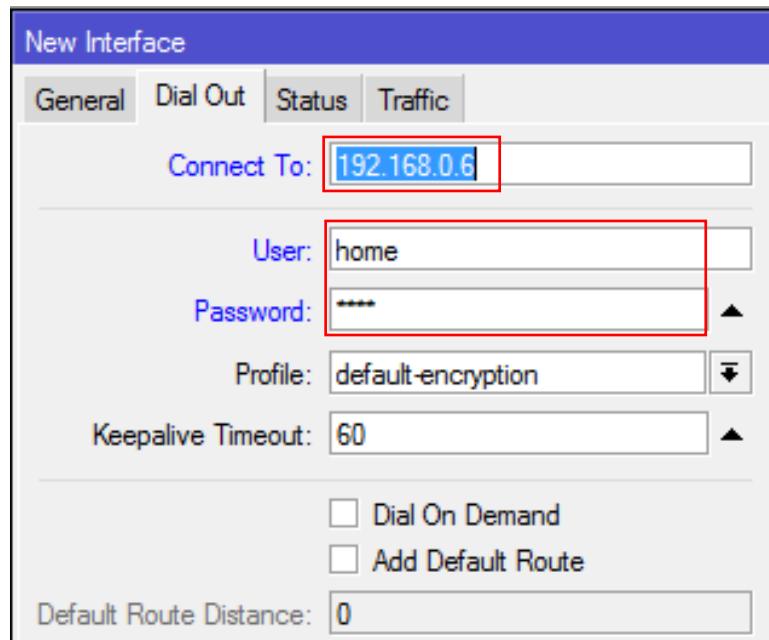
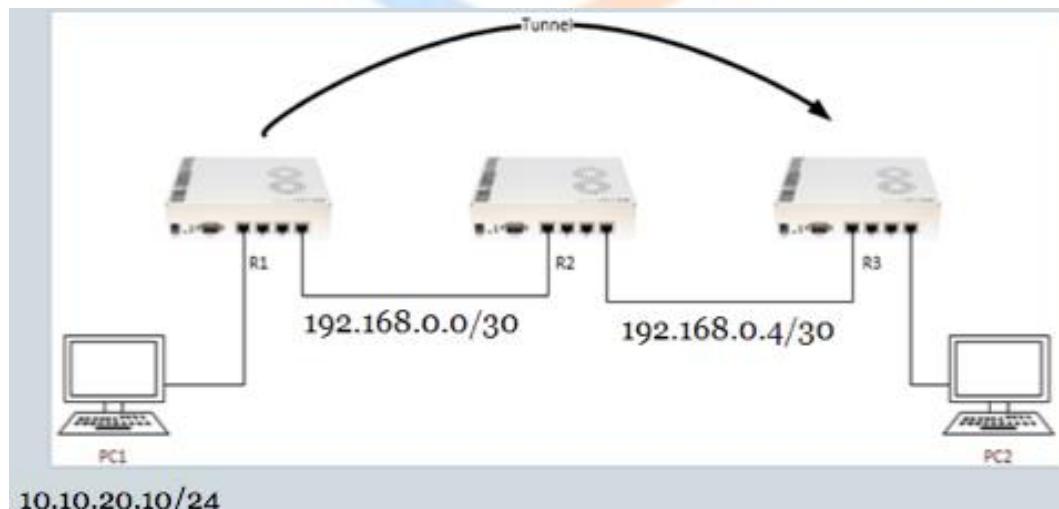


Figure 11 Konfigurasi PPTP Client di R1

Lab L2TP

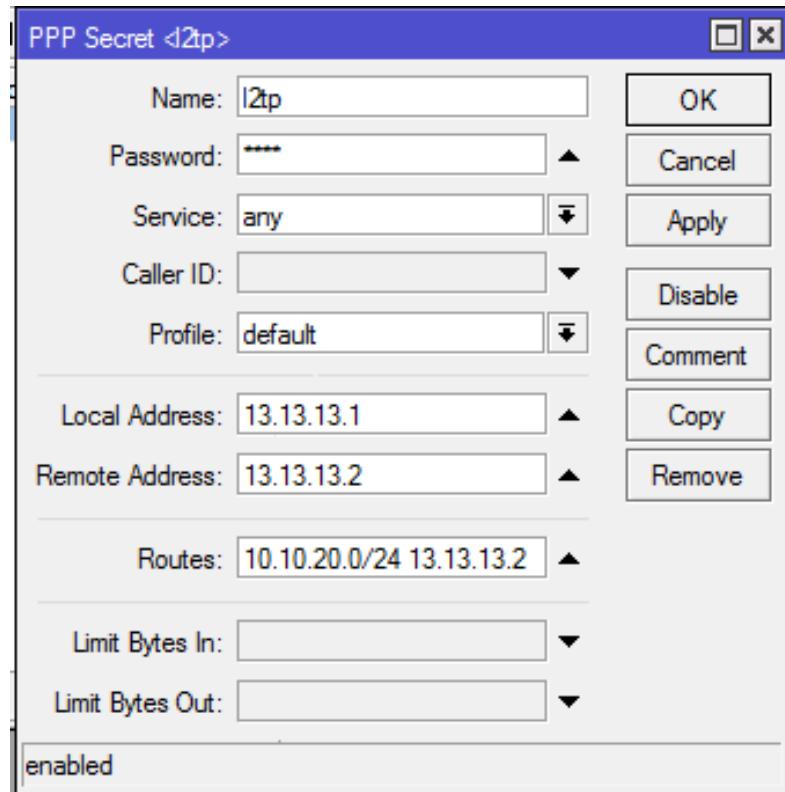
Buatlah L2TP tunnel sesuai dengan topologi dibawah ini



Berikut ini langkah-langkah yang diperlukan dalam konfigurasi L2TP

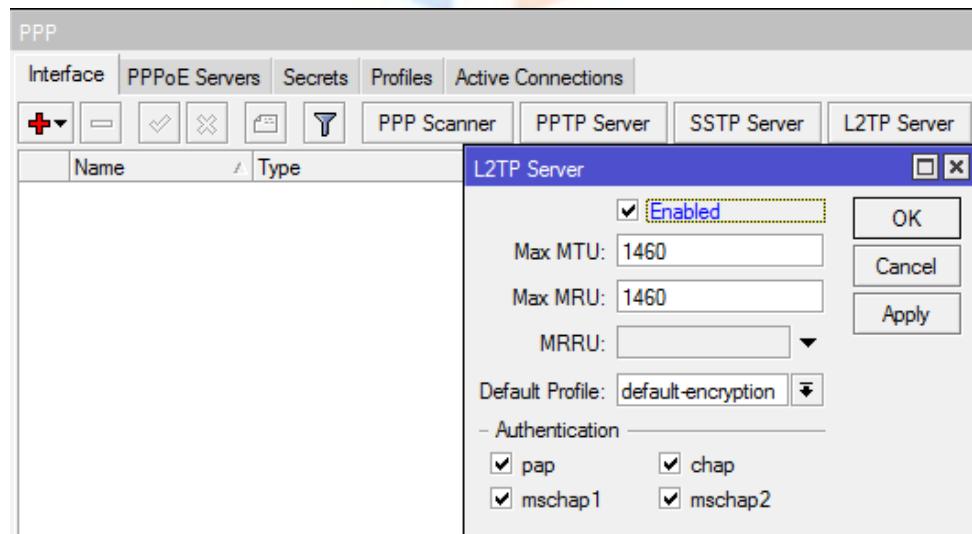
- Buatlah PPP secret di router office (R3)

PPP → secret



- Aktifkan L2TP server pada router office (R3)

PPP → L2TP server menu



- Konfigurasi L2TP client di router home (R1)

PPP → add new L2TP client (+)

New Interface

General Dial Out Status Traffic

Connect To: 192.168.0.6

User: l2tp
Password: ****
Profile: default-encryption
Keepalive Timeout: 60

Dial On Demand
 Add Default Route
Default Route Distance: 0

Allow

<input checked="" type="checkbox"/> pap	<input checked="" type="checkbox"/> chap
<input checked="" type="checkbox"/> mschap1	<input checked="" type="checkbox"/> mschap2

- Pada router home (R1) akan muncul ip address baru setelah koneksi L2TP ini berhasil

PPP

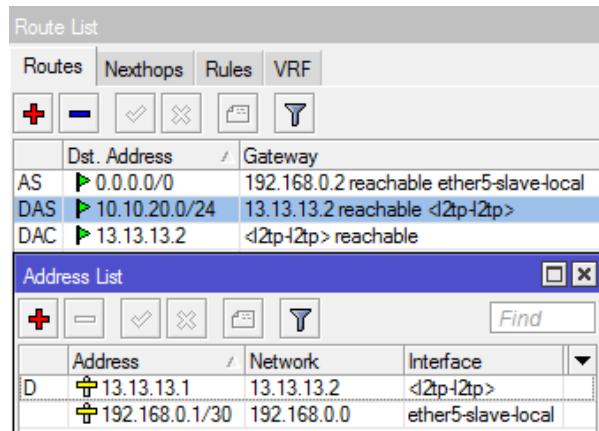
Interface PPPoE Servers Secrets Profiles Active Connections

	Name	Type	L2 MTU	Tx
R	l2tp-out1	L2TP Client		

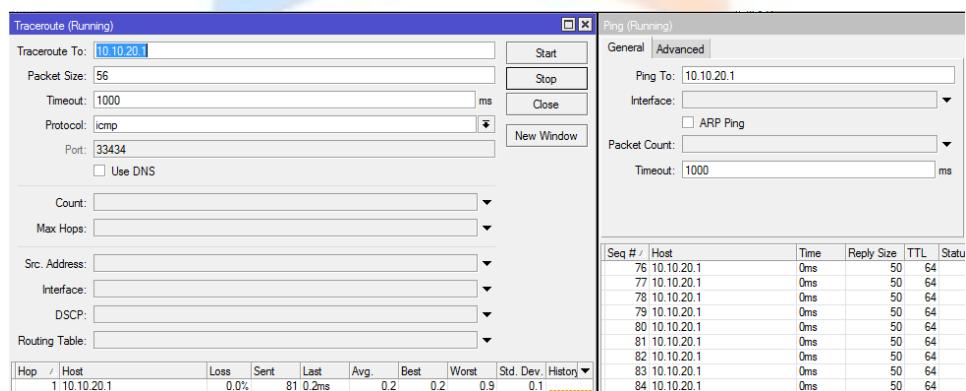
Address List

	Address	Network	Interface
D	192.168.0.6/30	192.168.0.4	ether5
D	13.13.13.2	13.13.13.1	l2tp-out1
D	192.168.100.2...	192.168.100.0	lo1
D	10.10.10.1/24	10.10.10.0	lo2

- Pada router office (R3) juga muncul ip address dan route list baru

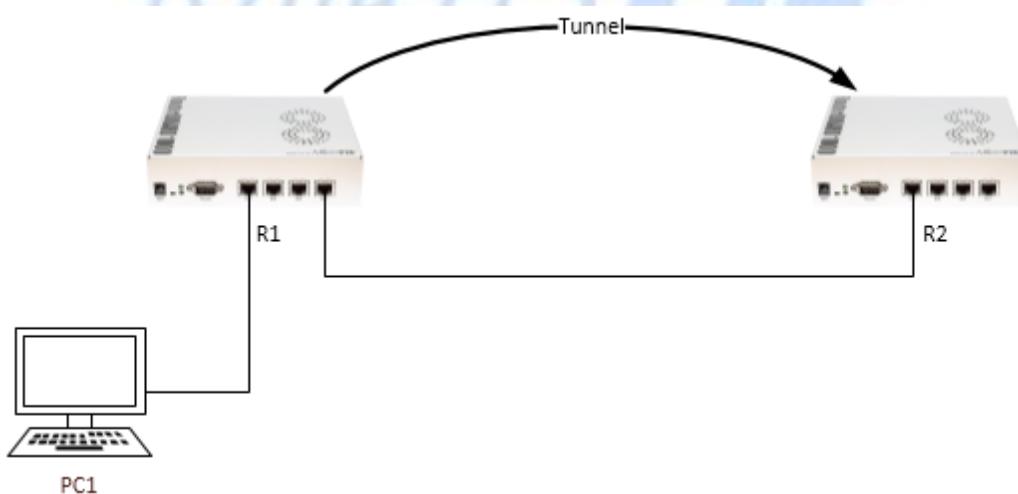


- Lakukan ping dan traceroute dari router home (R1) ke ip 10.10.20.10



Lab PPPoE

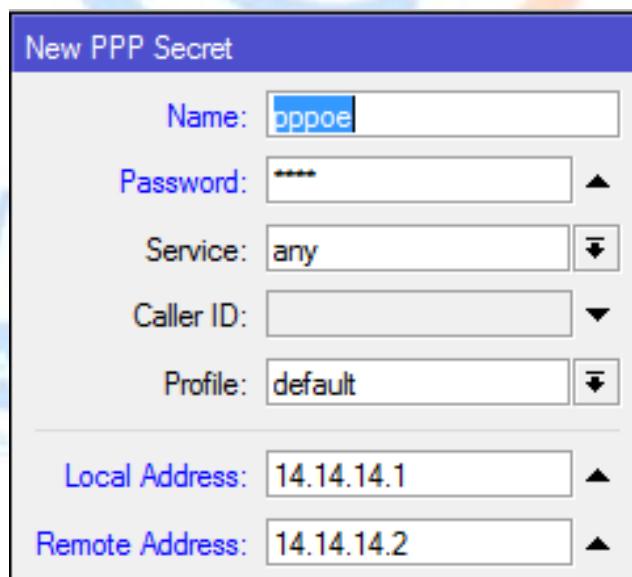
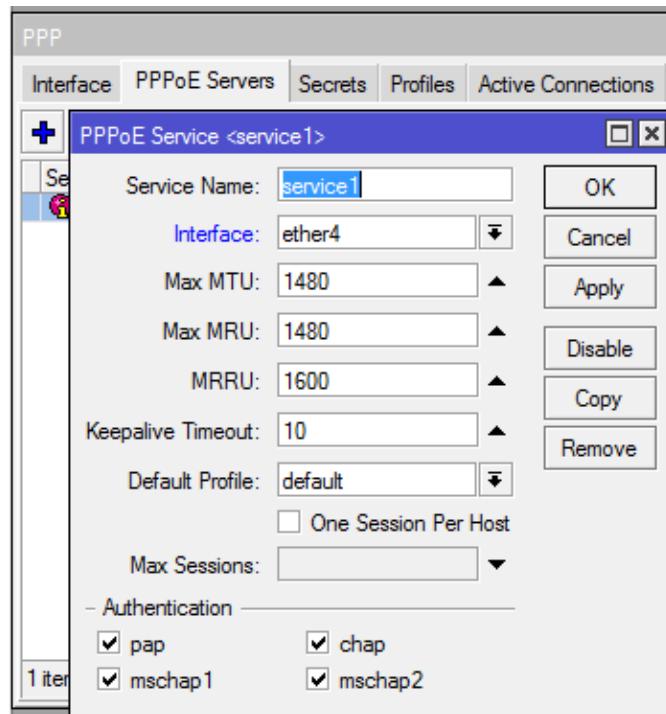
Buatlah topologi seperti dibawah ini untuk simulasi membuat PPPoE Tunneling



Berikut ini merupakan langkah-langkah dalam mengkonfigurasikan PPPoE:

- Buatlah PPPoE server di R2

PPP → add new PPPoE server (+)



- Buat interface pppoe client di R1

PPP → add new PPPoE client (+)

Interface <pppoe-out1>

General Dial Out Status Traffic

Name: pppoe-out1
Type: PPPoE Client
L2 MTU:
Max MTU: 1480
Max MRU: 1480
MRRU: 1600
Interfaces: ether5

Interface <pppoe-out1>

General Dial Out Status Traffic

Service: service1
AC Name: mikrotik_2
User: pppoe
Password: ****
Profile: default
Keepalive Timeout: 60
 Dial On Demand
 Use Peer DNS
 Add Default Route
Default Route Distance: 0
- Allow -
 pap chap
 mschap1 mschap2

- Cek ip address dan routing di R1 (PPPoE client) dan di R2 (PPPoE server)

```
[admin@mikrotik_2] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 192.168.0.2/30 192.168.0.0 ether5
1 X 192.168.0.5/30 192.168.0.4 ether4
2 192.168.88.1/24 192.168.88.0 ether2
3 D 14.14.14.1/32 14.14.14.2 <pppoe-pppoe>
[admin@mikrotik_2] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
# DST-ADDRESS PREF-SRC GATEWAY DISTANCE
0 ADC 14.14.14.2/32 14.14.14.1 <pppoe-pppoe> 0

[admin@mikrotik_3] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 192.168.100.2/24 192.168.100.0 lo1
1 10.10.20.1/24 10.10.20.0 lo2
2 D 14.14.14.2/32 14.14.14.1 pppoe-out1
[admin@mikrotik_3] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
# DST-ADDRESS PREF-SRC GATEWAY DISTANCE
0 ADS 0.0.0.0/0 14.14.14.1 0
1 ADC 10.10.20.0/24 10.10.20.1 lo2 0
2 ADC 14.14.14.1/32 14.14.14.2 pppoe-out1 0
```



Modul 8 QoS

RouterOS mengimplementasikan beberapa metode QoS sebagai berikut:

- shaping (limit bandwidth) merupakan cara membatasi trafik yg masuk dengan cara dropping packet yg melebihi batas (simple Queue)
- traffic prioritization merupakan konsep memberikan memberikan klasifikasi kelas-kelas pada trafik. Kategori trafiknya diantaranya adalah high, medium, dan low. Pengelompokan tersebut digunakan untuk memilih trafik paket mana yang didahulukan lewat di jaringan.
- dll

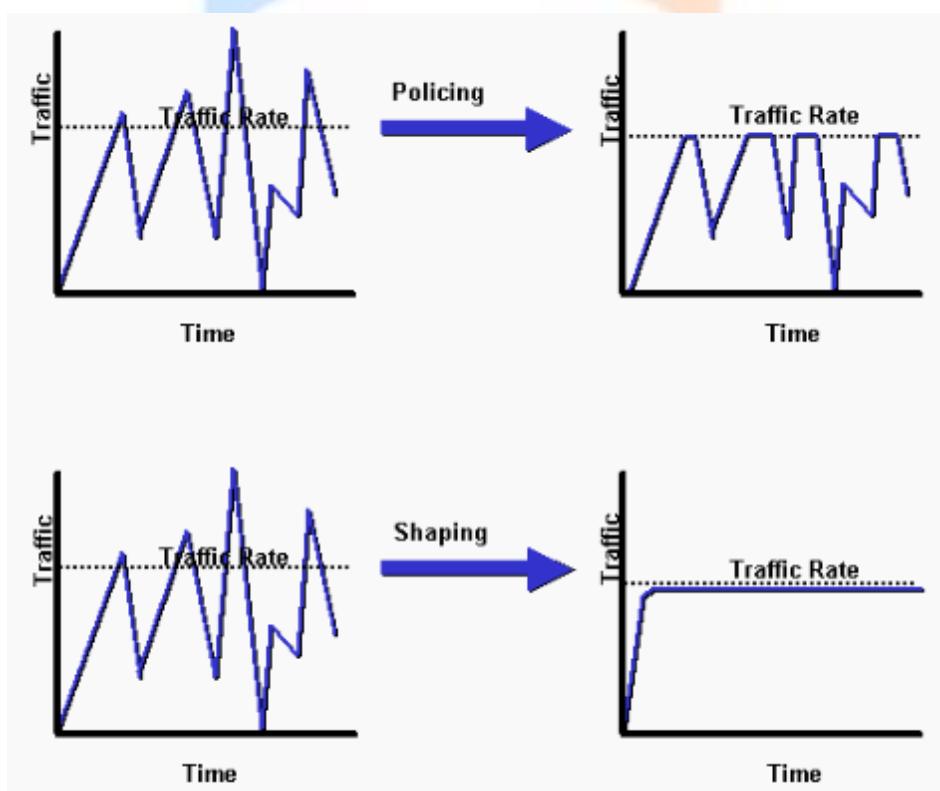


Figure 12 Contoh Penerapan QoS

Simple queue dapat digunakan untuk membatasi bandwidth. Bandwidth yang dapat dibatasi adalah sebagai berikut:

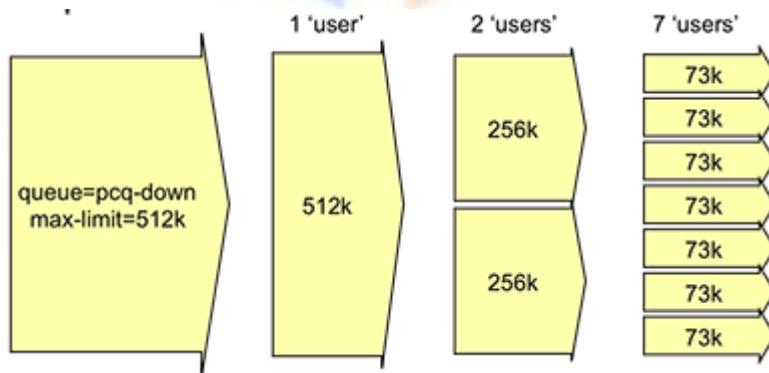
- Bandwidth download
- Bandwidth upload
- Total bandwidth

Burst memungkinkan data rate yg lebih tinggi untuk periode waktu singkat. Beberapa istilah:

- **Burst Limit** : max upload/download yg dapat dicapai selama periode burst
- **Burst time** : waktu (dalam detik) yg dibolehkan untuk burst
- **Burst threshold** : jika average date rate diatas threshold maka burst akan non aktif

Simple queue hanya membatasi upload dan download namun, jika ingin membuat pengelompokan queue diperlukan metode lain yang dinamakan HTB. HTB merupakan kepanjangan dari *Hierarchical Token Bucket*, HTB memungkinkan kita membuat queue menjadi lebih terstruktur, dengan melakukan pengelompokan-pengelompokan bertingkat. Pengelompokan tersebut misalkan, terdapat tiga client dimana masing-masing client mendapatkan prioritas 1,2,dan 3 dalam mendapatkan total bandwidth.

PCQ (Per Connection Queuing) bekerja dengan sebuah algoritma yang akan membagi bandwidth secara merata ke sejumlah client yang aktif. PCQ ideal diterapkan apabila dalam pengaturan bandwidth kita kesulitan dalam penentuan bandwidth per client. Cara kerja PCQ adalah dengan menambahkan sub-queue, berdasar classifier tertentu. Berikut gambaran cara kerja PCQ dengan parameter PCQ-Rate = 0



Lab Simple Queue

- Buatlah simple queue untuk melimit bandwidth upload 64 Kbps dan download 128 Kbps
- Coba lakukan download dan upload file ke gdrive atau akses webfig mikroTIK nya.

- Langkah-langkahnya adalah: Queue → simple Queue tab → add new (+)

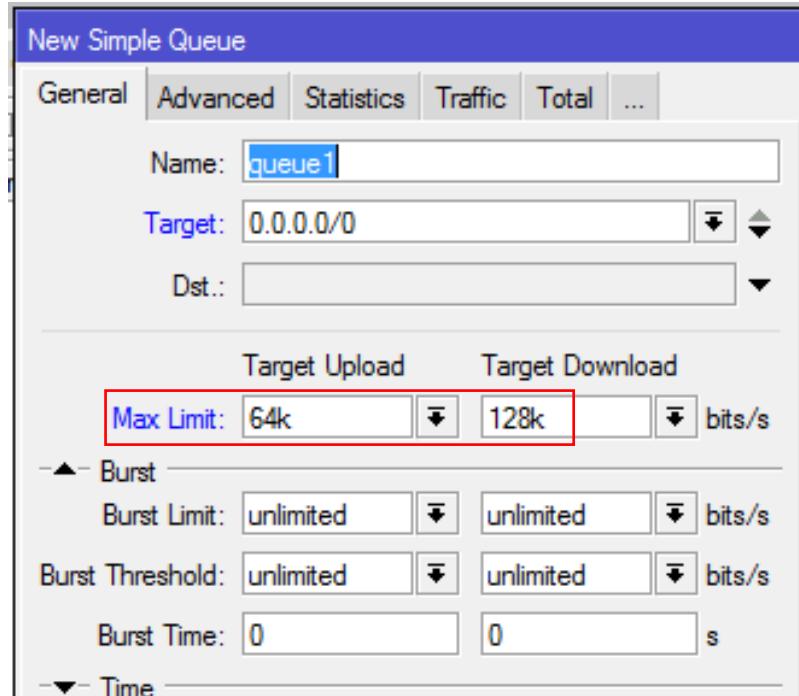


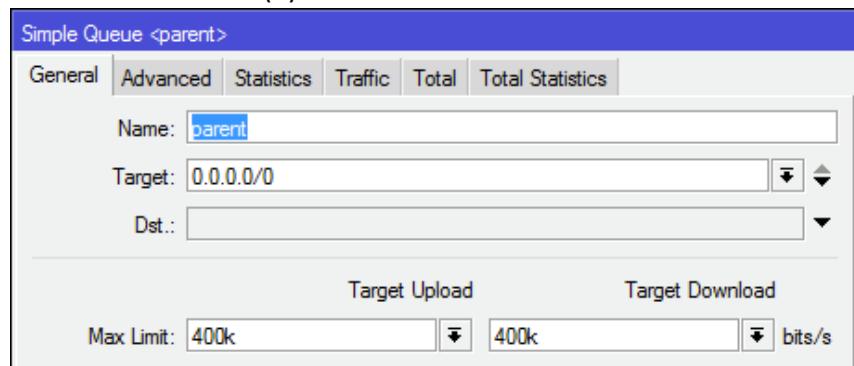
Figure 13 Konfigurasi simple Queue

LAB HTB

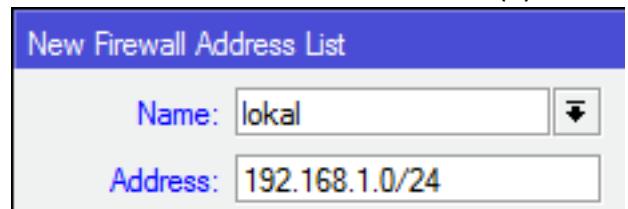
Pada lab HTB skenarionya adalah membagi total bandwidth (400 Kbps) ke tiga client, dimana masing-masing client mendapatkan prioritas bandwidth 1,2,dan 3. Maximum bandwidth yang bisa didapat masin-masing client adalah sebesar 200 Kbps dengan minimum bandwidth (CIR) adalah 75 Kbps.

Langkah-langkahnya adalah sebagai berikut:

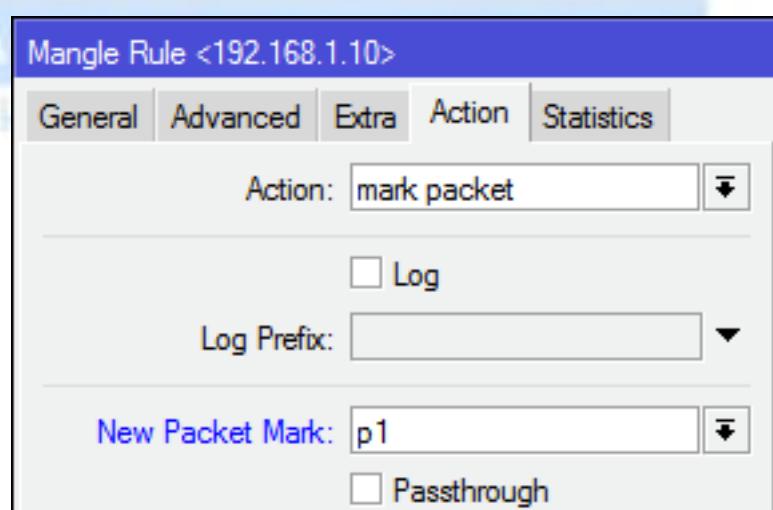
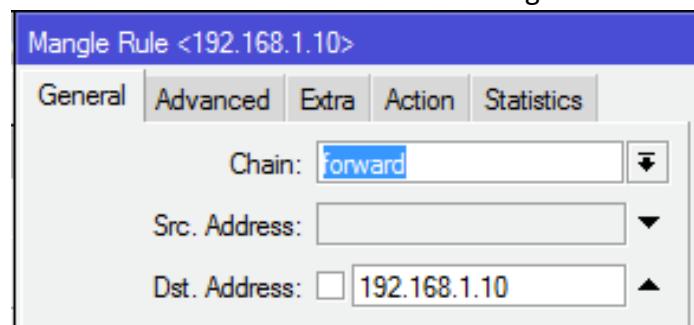
- Buat queue tree parent terlebih dahulu dengan max limit 400 Kbps
 - Queue → add new (+)



- Buat packet-mark terlebih dahulu untuk identifikasi ip client.
 - Buat address list terlebih dahulu untuk mendefinisikan ip lokalnya.
IP firewall → address list → add new (+)



- Buat mangle untuk ip client 192.168.1.10, 192.168.1.20, 192.168.1.30. IP → Firewall → tab Mangle → add new (+)



- Buat queue tree perclient dengan priority 1,2,dan 3 dengan setting max limit 200 Kbps dan limit at 75 Kbps

Simple Queue <queue1>

General	Advanced	Statistics	Traffic	Total	Total Statistics
Name: q1					
Target: 0.0.0.0/0					
Dst.:					
Target Upload		Target Download			
Max Limit: 200k		200k		bits/s	

Simple Queue <parent>

General	Advanced	Statistics	Traffic	Total	Total Statistics
Packet Marks: p1					
Target Upload		Target Download			
Limit At: 75k		75k		bits/s	
Priority: 1		1			
Bucket Size: 0.100		0.100		ratio	
Queue Type: default-small		default-small			
Parent: parent					

- Hasil akhir konfigurasinya adalah sebagai berikut:

Name	Parent	Packet Mark	Priority	Limit At ...	Max Limit...	Avg. Rate	
parent	ether3		8		400k	401.1 kbps	
q1	parent	p1	1	75k	200k	194.7 kbps	
q2	parent	p2	2	75k	200k	133.5 kbps	
q3	parent	p3	3	75k	200k	78.8 kbps	

Lab Burst

Buatlah konfigurasi burst yg membuat user bisa mendapatkan bandwidth 512 Kbps selama 15 detik

- Langkah-langkahnya adalah: Queue → simple Queue → edit simple queue

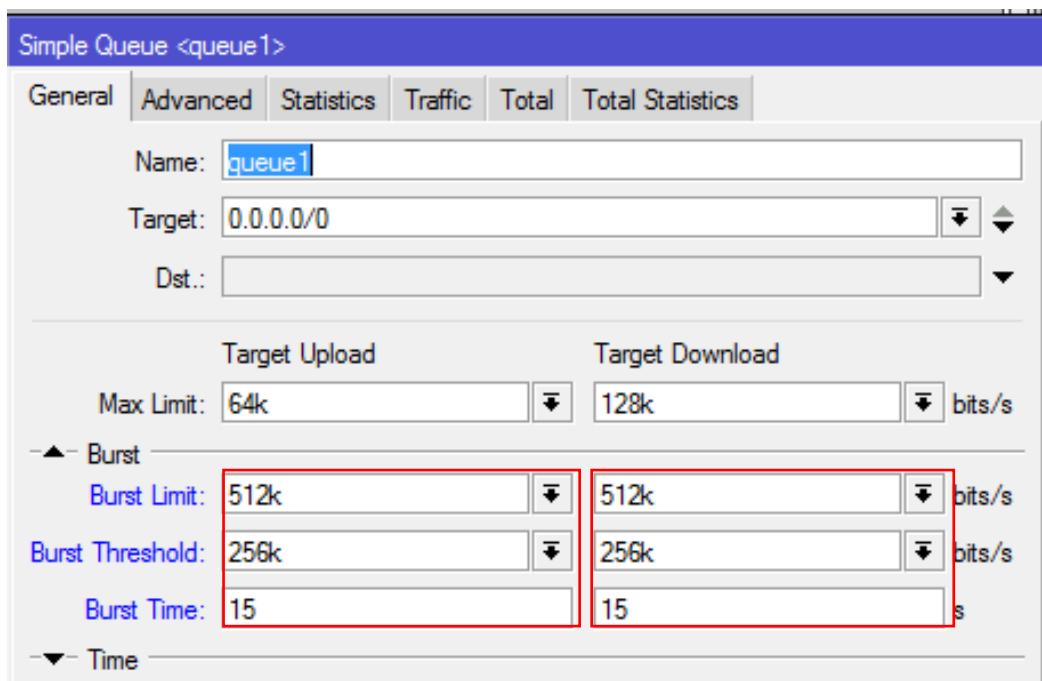


Figure 14 Konfigurasi Burst pada Mikrotik

Test browsing situs detik.com untuk melihat perbedaan kecepatannya setelah diimplementasikan burst.

Konfigurasi tersebut memungkinkan trafik dari user dapat naik hingga 512 Kbps selama 15 detik. Burst akan bekerja selama rata-rata trafik dari user tidak diatas 256 Kbps.

Lab PCQ

Buatlah PCQ yg membatasi bandwidth upload dan download sebesar 128 Kbps tiap user:

- Langkah-langkahnya adalah:
 - Queue → Queue type → add new (+)

The image shows two windows side-by-side. The left window is titled 'Queue Type <queue-download>' and the right is titled 'Queue Type <queue-upload>'. Both windows have 'Type Name' set to 'queue-download' and 'queue-upload' respectively, and 'Kind' set to 'pcq'. Under 'queue-download', 'Rate' is 128k, 'Limit' is 50, and 'Total Limit' is 2000. Under 'queue-upload', 'Rate' is 128k, 'Limit' is 50, and 'Total Limit' is 2000. Both windows have a 'Burst' section with fields for Rate, Limit, Total Limit, Burst Rate, Burst Threshold, and Burst Time (set to 00:00:10). At the bottom of each window is a 'Classifier' section with checkboxes for 'Src. Address' (checked) and 'Dst. Address' (unchecked), and 'Src. Port' (unchecked) and 'Dst. Port' (unchecked).

Apply PCQ tadi di simple queue, dan lakukan bandwidth test dari laptop.

- Caranya adalah: Queue → simple queue → tab advance

New Simple Queue

General Advanced Statistics Traffic Total Total Statistics

Packet Marks: [input field]

Target Upload Target Download

Limit At: unlimited [down arrow] unlimited [down arrow] bits/s

Priority: 8

Queue Type: queue_upload [down arrow] queue_download [down arrow]

Parent: none [down arrow]



MikroTik
A C A D E M Y
Sekolah Tinggi Terpadu NURUL FIKR

Modul 9 Mikrotik RouterOS Tool

MikroTik RouterOS menyediakan beberapa tools diantaranya:

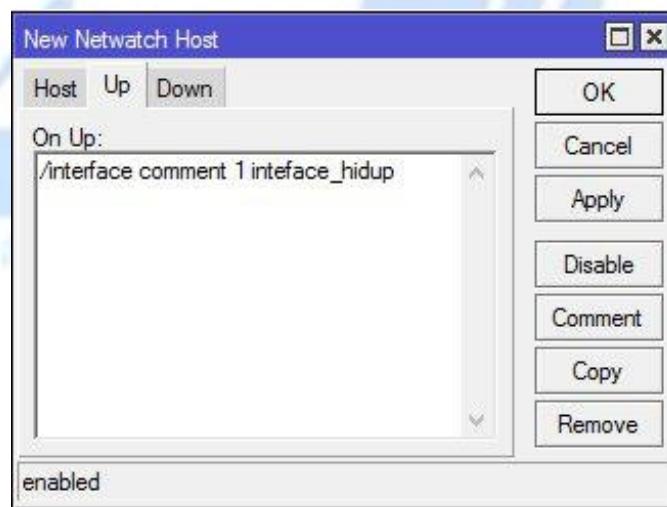
1. Netwatch

Netwatch digunakan untuk monitoring state dari host network. Monitoring dilakukan dengan cara mengirimkan ICMP echo (ping) ke list IP host yang sudah di spesifikasi. Setiap IP host yang didefinisikan dapat di atur ping interval dan ping timeoutnya. Keuntungan menggunakan netwatch adalah kemampuannya untuk **mengeksekusi perintah CLI atau console** ketika terjadi **perubahan state host**. Netwatch dapat diakses dari menu **tools → netwatch**



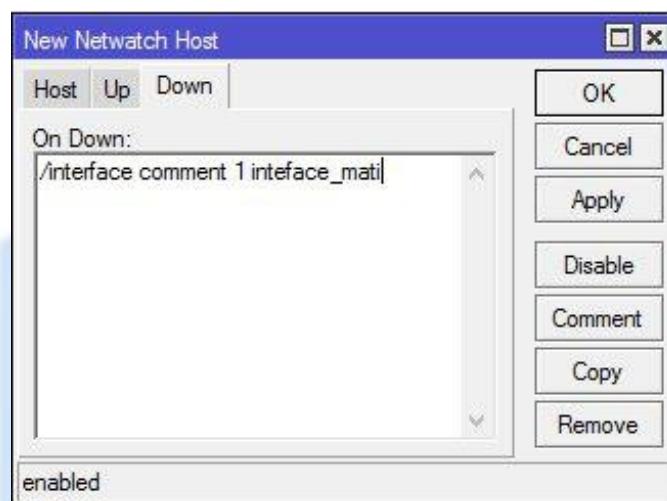
Figure 15 Netwatch pada mikrotik

- Netwatch dapat mengeksekusi script ketika host naik atau unreachable



Berikut hasil dari netwatch pada saat kondisi state hidup

Interface List								
	Interface	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding
R	ether1	Ethernet				6.2 kbps	1552 bps	1 2
R	interface_hidup							
R	ether2	Ethernet				0 bps	0 bps	0 0



Berikut hasil dari netwatch pada saat kondisi state mati

Interface List								
	Interface	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding
R	ether1	Ethernet				18.9 kbps	6.1 kbps	6
R	interface_mati							
R	ether2	Ethernet				0 bps	0 bps	0

2. Ping

ping digunakan untuk verifikasi reachability host menggunakan ICMP echo. ping dapat diakses dari menu tools → ping

3. Traceroute

- Traceroute digunakan untuk melakukan verifikasi jalur dari source ke destination
- Traceroute diakses dari menu tool → traceroute

4. Torch

Torch merupakan real-time traffic monitoring yang dapat digunakan untuk memonitor traffic flow yang melalui sebuah interface. Torch dapat memonitor traffic seperti protocol, source address, destination address, port, dll. Torch menampilkan protocol atau pilihan sesuai yang dipilih dan Tx/Rx data rate masing-masing traffic flow.

Tool → Torch

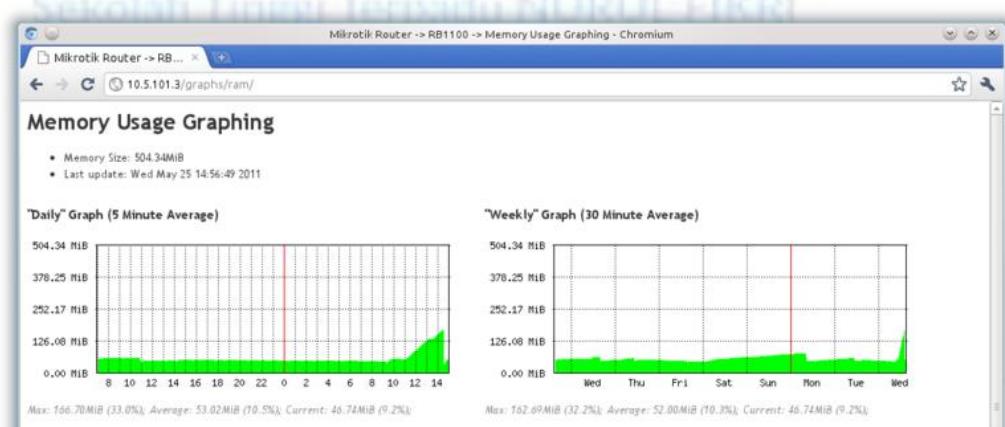
Torch							
Basic				Filters			
Interface:	afp2	Src. Address:	0.0.0.0/0	Dst. Address:	0.0.0.0/0	MAC Protocol:	all
Entry Timeout:	00:00:03	Src. Address6:	/0	Dst. Address6:	/0	Protocol:	any
- Collect		Port:	any	VLAN Id:	any	DSCP:	any
<input checked="" type="checkbox"/> Src. Address	<input type="checkbox"/> MAC Protocol	<input type="checkbox"/> Port	<input type="checkbox"/> VLAN Id	<input type="checkbox"/> DSCP			
<input checked="" type="checkbox"/> Dst. Address	<input type="checkbox"/> Src. Address6	<input type="checkbox"/> Dst. Address6	<input type="checkbox"/> VLAN Id	<input type="checkbox"/> DSCP			
<input type="checkbox"/> MAC Protocol	<input type="checkbox"/> Port	<input type="checkbox"/> VLAN Id	<input type="checkbox"/> DSCP				
<input type="checkbox"/> Protocol	<input type="checkbox"/> DSCP						
<input type="checkbox"/> DSCP							
Bth. Protocol	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate
800 (ip)	5 (tcp)	172.16.16.101.3338	103.4.3.211.63663			2.3 Mbps	75.5 Mbps
800 (ip)	17 (udp)	74.125.200.132.443 (https)	103.4.3.211.36738			153.9 k...	5.0 Mbps
800 (ip)	6 (tcp)	31.13.78.52.443 (https)	103.4.3.210.60506			149.6 k...	3.4 Mbps
800 (ip)	6 (tcp)	31.13.78.52.443 (https)	103.4.3.210.50202			109.4 k...	2.9 Mbps
800 (ip)	6 (tcp)	209.85.229.235.443 (https)	103.4.3.210.14792			88.6 kbps	2.8 Mbps
800 (ip)	6 (tcp)	188.166.216.46.119	103.4.3.210.1194			159	241
800 (ip)	17 (udp)	188.166.216.46.119	103.4.3.210.7011			148.3 k...	2.8 Mbps
800 (ip)	17 (udp)	125.200.128.443 (https)	103.4.3.210.1194			130.6 k...	2.5 Mbps
800 (ip)	6 (tcp)	74.125.200.128.443 (https)	103.4.3.211.50223			44.4 kbps	2.4 Mbps
800 (ip)	17 (udp)	140.118.136.57.11026	103.4.3.211.27292			118.5 k...	2.4 Mbps
800 (ip)	6 (tcp)	74.125.200.101.443 (https)	103.4.3.211.50170			42.7 kbps	2.0 Mbps
800 (ip)	17 (tcp)	103.128.128.124.443 (https)	103.4.3.211.57224			113.5 k...	2.0 Mbps
800 (ip)	6 (tcp)	103.6.128.128.124.443 (https)	103.4.3.211.62150			78.4 kbps	199.8 ...
800 (ip)	6 (tcp)	31.13.78.52.443 (https)	103.4.3.210.50204			77.6 kbps	1911.5 ...
800 (ip)	6 (tcp)	119.10.115.24.443 (https)	103.4.3.210.63719			43.6 kbps	1745.8 ...
800 (ip)	17 (tcp)	202.43.172.13.443 (https)	103.4.3.211.23250			73.5 kbps	1736.0 ...
800 (ip)	6 (tcp)	103.6.128.128.124.443 (https)	103.4.3.211.30203			49.2 kbps	1695.6 ...
800 (ip)	17 (tcp)	193.154.224.130.51413	103.4.3.211.46406			80.1 kbps	1559.5 ...
800 (ip)	6 (tcp)	31.13.78.52.443 (https)	103.4.3.210.50203			60.4 kbps	1401.8 ...
800 (ip)	6 (tcp)	31.13.78.52.443 (https)	103.4.3.210.50201			61.6 kbps	1358.5 ...
800 (ip)	6 (tcp)	103.6.128.128.124.443 (https)	103.4.3.211.39825			42.7 kbps	1356.5 ...
800 (ip)	17 (tcp)	170.81.200.239.35634	103.4.3.211.36171			69.4 kbps	1347.8 ...
800 (ip)	17 (tcp)	202.43.172.12.443 (https)	103.4.3.211.36554			48.7 kbps	1201.4 ...
800 (ip)	17 (tcp)	104.174.68.116.55171	103.4.3.211.49368			121.8 k...	1161.1 ...
800 (ip)	6 (tcp)	103.6.128.128.124.443 (https)	103.4.3.211.51785			22.0 kbps	985.6 ...
800 (ip)	17 (tcp)	83.223.175.247.58192	103.4.3.211.47874			44.6 kbps	985.5 ...
800 (ip)	6 (tcp)	4.10.6.128.127.443 (https)	103.4.3.211.68527			36.8 kbps	982.3 ...
10167 items (1 selected)		Total Tx: 18.7 Mbps	Total Rx: 161.7 Mbps	Total Tx Packet: 12.997	Total Rx Packet: 16.549		

5. Graphing

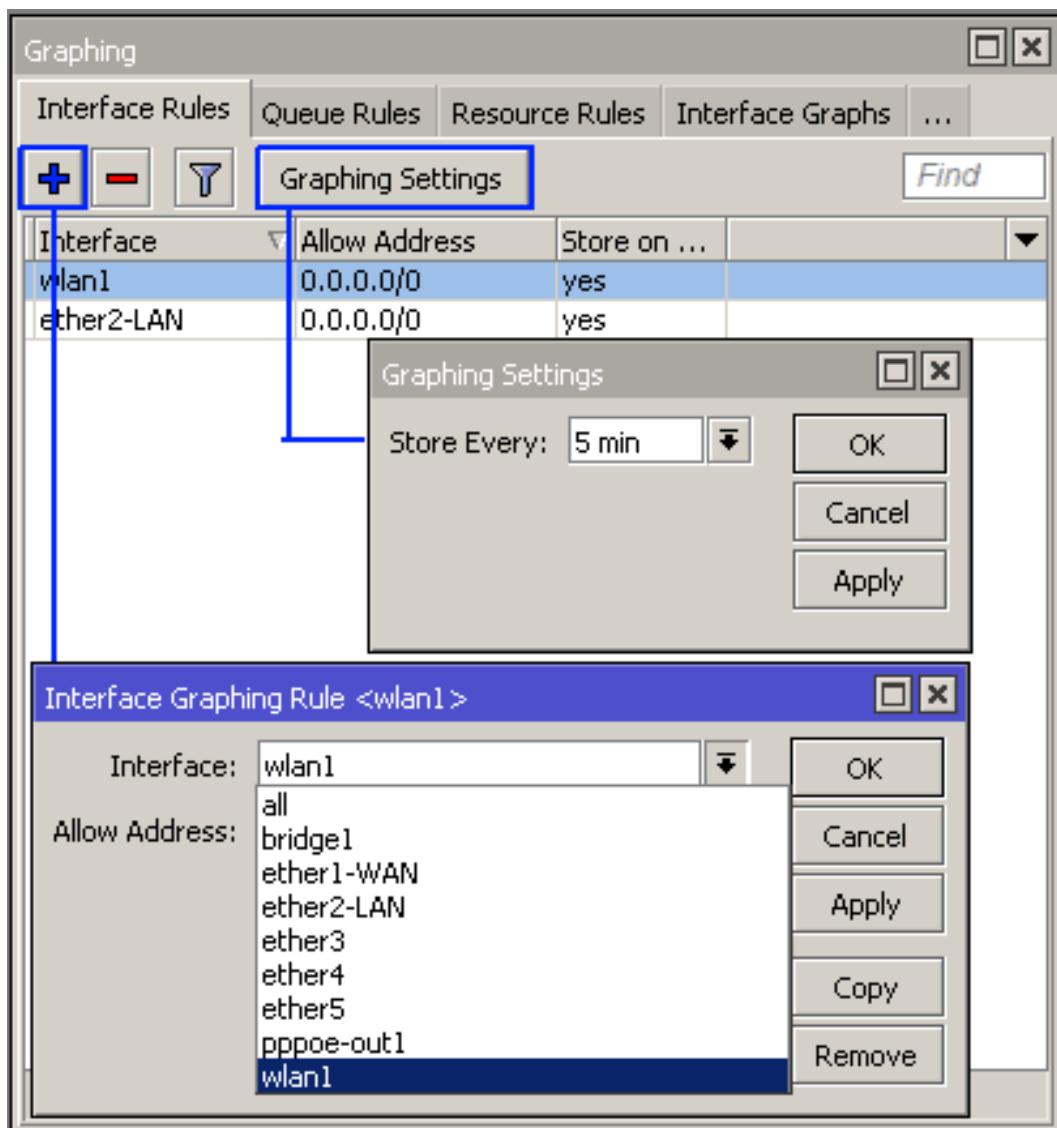
Graphing merupakan tool untuk memonitor berbagai macam parameter MikroTik RouterOS dari waktu ke waktu dan menampilkan kedalam grafik. Tool Graphing dapat menampilkan grafik sebagai berikut:

- RouterBoard Health (voltase dan teperatur)
- Penggunaan resource (CPU, Memory, dan disk usage)
- Trafik yang melewati interface
- Trafik yang melewati simple queue

Graphing terdiri dari dua bagian, bagian pertama bertugas mengumpulkan informasi dan bagian lainnya bertugas menampilkan data pada halaman web. Untuk mengakses grafik di halaman web ketik pada URL browser [http://\[ip_router\]/graphs/](http://[ip_router]/graphs/)



Graphing dapat diakses dari winbox di menu Tools → Graphing



A G A D E M Y
Sekolah Tinggi Terpadu NURUL FIKR

Testimoni

Berikut ini merupakan beberapa testimoni dari peserta pelatihan MTCNA di MikroTik Academy STT Terpadu Nurul Fikri

Dede Setiawan – Mahasiswa Semester 8 STT Nurul Fikri

“Selama mengikuti pelatihan dan sertifikasi ini, untuk materi yang disampaikan sangat lengkap dan mudah dipahami, saran saya untuk lebih banyak praktik selama proses pelatihan atau ditambah durasi dalam pelatihannya”

Ali Imron – Mahasiswa Semester 1 STT Nurul Fikri

“menambah pengetahuan banyak mengenai Mikrotik dan juga mendapatkan sertifikat dari MikroTik langsung sehingga membuat saya lebih semangat lagi untuk mencari tau mengenai Mikrotik ini, dan so pasti menambah teman yang sudah berpengalaman dalam dunia jaringan sehingga bisa saling sharing pengetahuan mengenai jaringan.”

Slamet Santoso – Mahasiswa Semester Akhir STT Nurul Fikri

“Menambah wawasan tentang Networking dan dapat diterapkan langsung di dalam Dunia Kerja dapat sertifikat internasional MTCNA dari Mikrotik”

Moch Hafied – Mahasiswa Semester 1 STT Nurul Fikri

“Mentor yang menyenangkan dan berpengalaman tentang MikroTIK. Dengan mengikuti training MTCNA ini, saya lebih ingin mendalami dan terus mengembangkan ilmu saya di bidang Mikrotik tentunya. Terimakasih kepada Bapak April Rustanto selaku mentor kami dan juga STT Nurul Fikri yang menyediakan tempat dan layanan untuk mengikuti Training MTCNA ini.”

Mujib Ahmad - Mahasiswa Semester 1 STT Nurul Fikri

“Saya sangat senang mengikuti sertifikasi MTCNA ini. Disamping mendapat sertifikat untuk menunjang pekerjaan, saya bisa tau lebih dalam tentang mikrotik. Banyak pengalaman yang sudah saya dapatkan saat training ini. Saya berharap kedepannya pesertanya bisa lebih banyak dari ini. Terimakasih”