AJEF ALMURNANDO 2019

Mikrotik MTCNA

Mikrotik
Router

Mikrotik MTCNA

Oleh
Ajef Almurnando

Biodata :
Alumni SMKN1 Banjit 2019, Way Kanan
Alumni BLC Telkom Klaten
Relawan IT SMKNet 2019
IT Support ngoprekbareng

MikroTik Certified Network Associate Training

JADWAL TRAINING MTCNA (OUTLINE)

	SESI 1	SESI 2	SESI 3	SESI 4
HARI 1	PEMAHAMAN TCP/IP DAN SUBNETTING	PENGENALAN MIKROTIK	KONFIGURASI DASAR	
HARI 2	DHCP	BRIDGE	ROUTING	WIRELESS
HARI 3	FIREWALL	QoS	TUNNELS DAN TOOLS MONITORING	TEST

WAKTU TRAINING

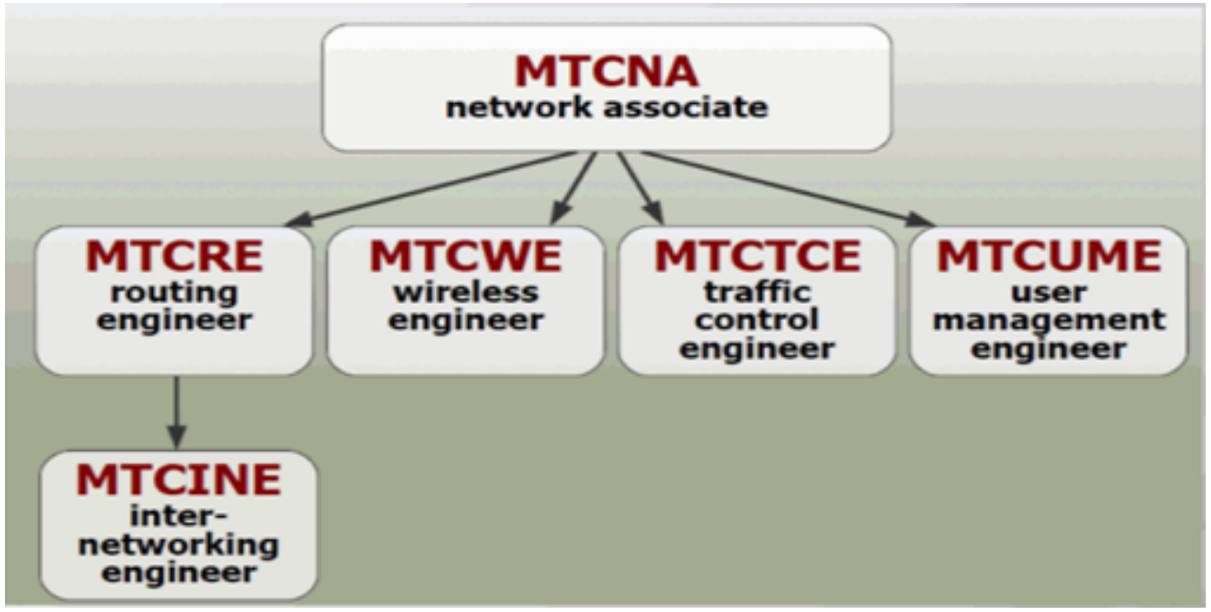
TRAINING = 09:00 - 17:00

ISTIRAHAT 30 MENIT = 10:30 & 15:00

ISTIRAHAT 1 JAM = 12:30

TEST SERTIFIKASI = HARI TERAKHIR,1 JAM

SERTIFIKASI MIKROTIK



TEST SERTIKASI

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

MikroTik

MTCNA

MikroTik Certified Network Associate Training

PENGENALAN MIKROTIK

APA ITU MIKROTIK?

- Kependekan dari mikrotikls yang dalam bahasa Latvia berarti “network kecil”
- Sebuah perusahaan kecil berkantor pusat di kota Riga, Latvia,y-ang memproduksi perangkat keras (RouterBoard) dan perangkat lunak (RouterOS)

APA ITU RouterOS?

- Produk (Software) dari mikrotik
- System operasi yang diperuntukkan sebagai network router.
- RouterOS digunakan untuk menjadikan komputer biasa menjadi router network (PC Router) yang handal,mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless.
- Diinstall pada PC biasa

APA ITU RouterBoard?

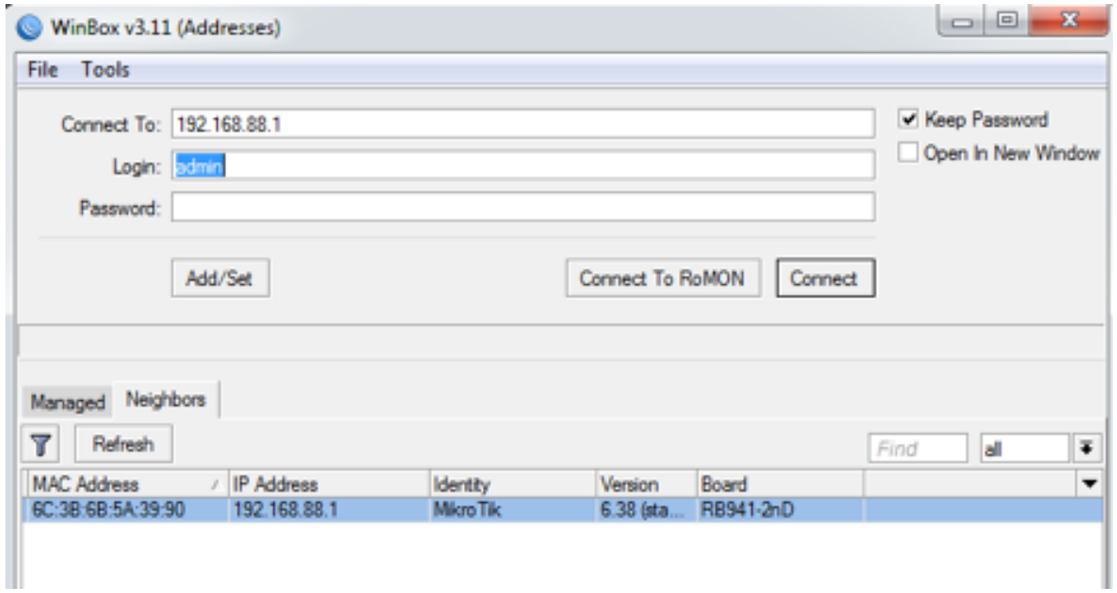
- Produk (hardware) dari mikrotik
- Sebuah router (Hardware) yang didalamnya sudah terinstal RouterOS mikrotik

- APA SAJA FITUR MIKROTIK?
- Router OS support berbagai driver perangkat
- Ethernet, Wireless Card, V35, ISDN, USB MassStorage, USB 3G Modem,
- User Management (DHCP, Hotspot, Radius, dll).
- Routing (RIP, OSPF, BGP, RIPng, OSPF V3).
- Firewall& NAT (fully-customized, linux based).
- QoS/Bandwidth limiter (fully customized, linux based).
- Tunnel (EoIP, PPTP, L2TP, PPPoE, SSTP,OpenVPN).
- Real-time Tools (Torch, watchdog, mac-ping, MRTG, sniffer).

BAGAIMANA CARA MENGAKSES MIKROTIK?

1. WINBOX

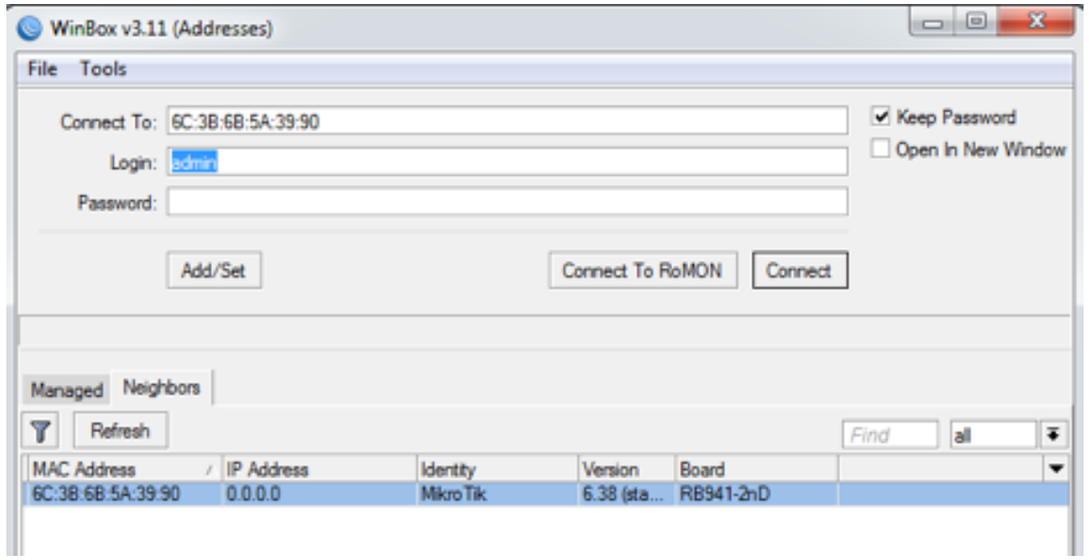
- Untuk mengakses mikrotik dapat menggunakan software winbox yang kompatible di semua OS dan bisa didapatkan di web resminya https://mikrotik.com/
- Default IP Address (LAN) = 192.168.88.1
- Username = admin
- Password = (kosong)



1. MAC WINBOX

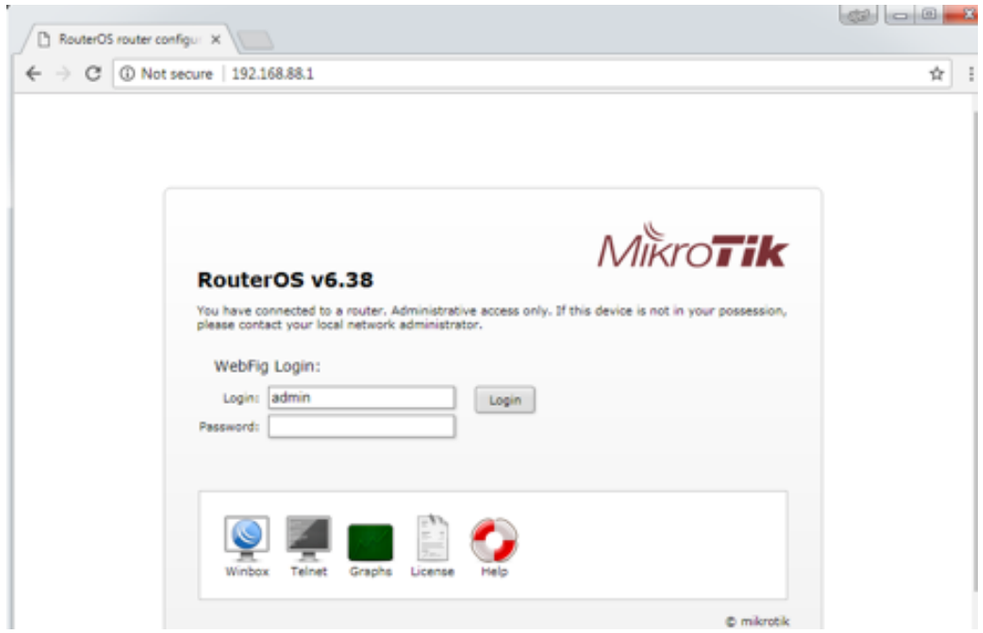
Selain menggunakan IP Default,mikrotik juga bisa diakses menggunakan mac address dari interfaces yang terhubung langsung dengan laptop.

Saat melakukan reset default configuration maka untuk akses mikrotik melalui winbox hanya bisa menggunakan mac win-box



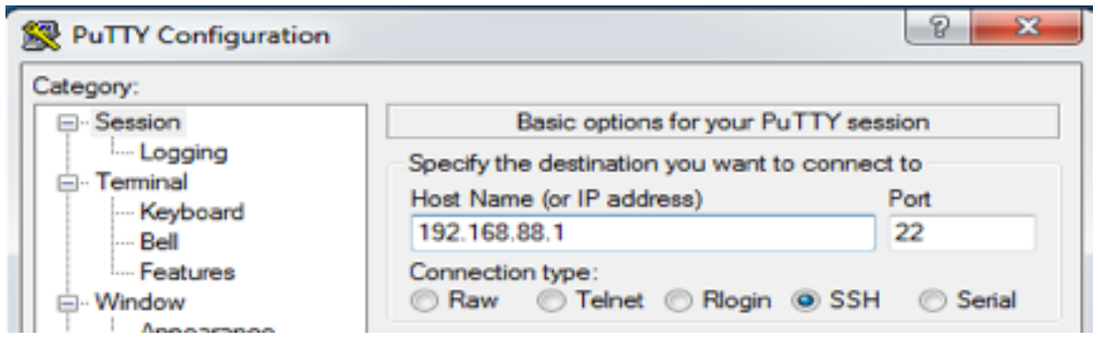
WEBFIG

Cara termudah untuk mengakses mikrotik yaitu menggu-nakan browser yang ada dilapop anda. Isikan IP Address de-fault mikrotik http://192.168.88.1



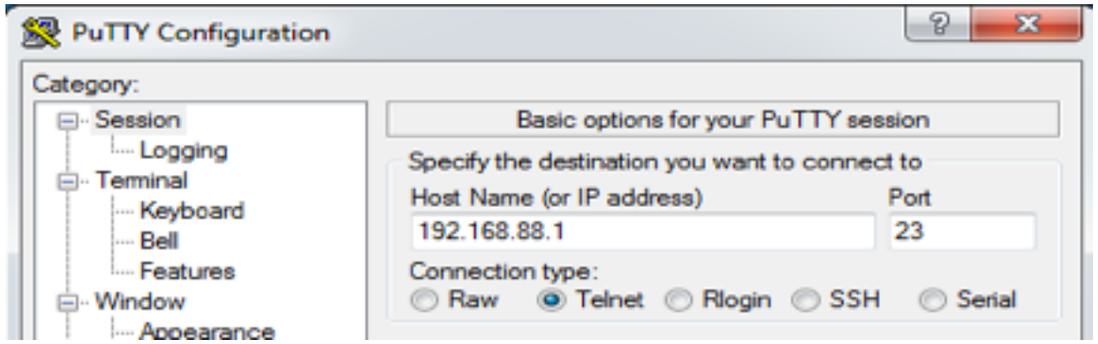
SSH

Untuk akses mikrotik melalui SSH dapat menggunakan software Putty yang bisa anda dapatkan di situs resminya https://www.putty.org



TELNET

akses mikrotik menggunakan TELNET menggunakan software putty juga sama dengan SSH namun berbeda port.

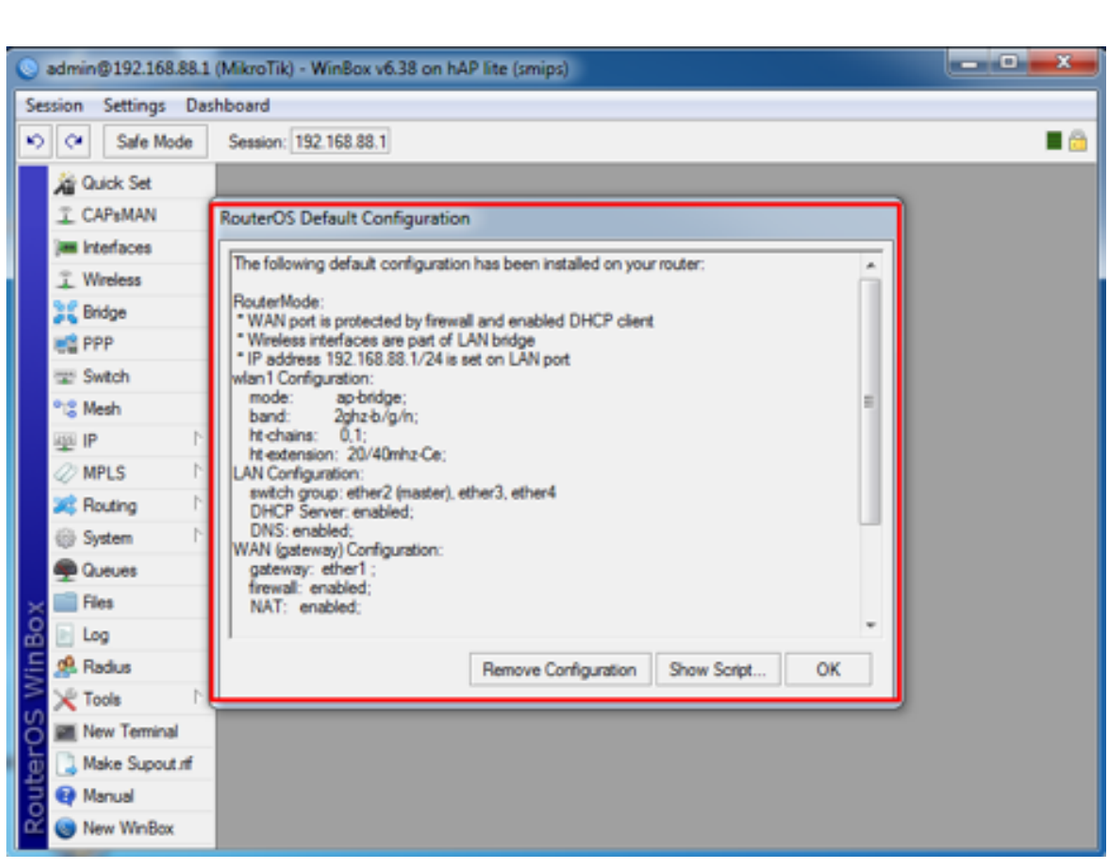


CONSOLE

Hanya dilakukan untuk RouterBoard yang mempunyai port console pada salah satu interface nya

DEFAULT CONFIGURATION

Pada dasarnya mikrotik sudah punya konfigurasi default, dimana konfigurasi tersebut sudah cukup jika mikrotik anda hanya difungsikan untuk mengakses internet dan memancarkan wifi untuk client.



Nah pada Lab pertama kita akan belajar mengkonfigurasi mikrotik kita sendiri dari awal hingga bias difungsikan untuk koneksi ke internet dan wifi ke client serta fungsi-fungsi lainnya tentunya dengan keinginan dan kebutuhan kita sendiri, dan mereset konfigurasi default dari mikrotik.

IP Address & Subnetting

IP Address

Agar unik setiap computer yang terkoneksi ke Internet diberi alamat yang berbeda.Alamat ini supaya seragam seluruh dunia maka pemberian alamat IP address diseluruh dunia diberikan oleh badan internasional Internet Assigned Number Authority (IANA), dimana IANA hanya memberikan IP address Network ID nya saja sedangkan host ID diatur oleh pemilik IP address tersebut.

Alamat yang unik terdiri dari 32 bit yang dibagi dalam 4 oktet (8 bit)

oooooooo . oooooooo . oooooooo . oooooooo

1 2 3 4

Ip address dibagi menjadi 2 bagian yaitu Network ID dan Host ID, Network ID yang akan menentukan alamat dalam jaringan (network address) sedangkan Host ID menentukan alamat dari host yang sifatnya unik untuk membedakan antara satu host dengan host lainnya.

Terdapat 2 jenis IP, yaitu IP public dan IP Privat.IP Public digunakan untuk berkomunikasi dalam jaringan luas (Internet) sedangkan IP Public digunakan untuk komunikasi dalam jaringan local (LAN).

Terdapat 3 kelas IP Private yang umum digunakan, yaitu :

Kelas A = 10.0.0.0

Kelas B = 172.16.0.0 - 172.31.0.0

Kelas C = 192.168.0.0

Dimana angka 0 bisa kita ganti dengan angka 0 – 254.Selain dari ketiga kelas IP tersebut digunakan untuk IP Public, IP Loopback, Multicast dll.

Penggunaan	IP / subnet
Self Identification	0.0.0.0/8
Localhost	127.0.0.1
Not Used	Other 127.0.0.0/8
Multicast	224.0.0.0/4
Local link/DHCP error	169.245.0.0/16
TEST-NET-1	192.0.2.0/24
TEST-NET-2	198.51.100.0/24
TEST-NET-3	203.0.113.0/24
6to4 Relay Anycast	192.88.99.0/24
Benchmark Test	198.18.0.0/15
Future Used	240.0.0.0/4
Limited Broadcast	255.255.255.255/32

RFC5735 Jan 2010: http://tools.ietf.org/html/rfc5735

Subnetting

Kita juga harus menguasai konsep subnetting untuk mendapatkan IP Address baru.Dimana dengan subnetting kita dapat membuat network ID baru dari suatu network yang dimiliki sebelumnya. Subnetting digunakan untuk memecah satu buah network menjadi beberapa network kecil.

Seharusnya kita sudah tidak familiar lagi dengan Subnetting karena materi ini merupakan materi dasar yang kita pelajari sebelum belajar jaringan khususnya mikrotik lebih dalam, namun kita akan sedikit mengulas untuk mengingat :

Contoh: 192.168.0.0/24

- Netmask : 255.255.255.0
- Prefix : /24
- IP Network : 192.168.0.0
- First HostIP: 192.168.0.1
- Last HostIP : 192.168.0.254
- Broadcast : 192.168.0.255
- HostIP : total IP di dalam Subnet (–) minus 2

Subnet Mask	Prefix	No of IP	Usable IP
255.255.255.0	/24	256	254
255.255.255.128	/25	128	126
255.255.255.192	/26	64	62
255.255.255.224	/27	32	30
255.255.255.240	/28	16	14
255.255.255.248	/29	8	6
255.255.255.252	/30	4	2
255.255.255.254	/31	2	-
255.255.255.255	/32	1	-

Selanjutnya bagaimana yang kita gunakan bukanlah prefix 24 – 32, namun kita menginginkan menggunakan prefix 23,22,21 dan seterusnya., berikut beberapa contoh subnettingnya :

1.Contoh IP : 192.168.10.1/22

Untuk menghitung jumlah range IP, karena prefix nya berada pada oktet ke-3 maka :

Jumlah range IP = /22 + 8 = /30 = 4 range IP.

Jumlah total IP = 4 x 256 atau bisa dengan rumus (2^32-22)

= 1024

IP Usable = 1024 -2 = 1022 Host yang bisa digunakan untuk klien

Range IP = 10 : 4

= 2,....

` = 2 x 4 = 8

Jadi range IP nya :

192.168.8.0 - 192.168.11.255

Dengan demikian jika ada IP yang berbeda network namun masih dalam satu range seperti hal nya diatas maka computer tetap bisa saling berkomunikasi.

2.Contoh IP : 10.10.10.1/12

Untuk menghitung jumlah range IP, karena prefixnya berada pada oktet ke-2 maka :

Jumlah Range IP = /12 + 8 + 8 = /28 = 16 Range IP

Jumlah total IP = 16 x 256 x 256 atau bisa dengan rumus (2^32-12) = 1.048.576

IP Usable = 1.048.576 - 2 = 1.048.574

Range IP = Karena jumlah range lebih besar daripada network ID maka range pasti dimulai dari 0

Jadi range IP nya : 10.0.0.0 - 10.15.255.255

Semakin luas prefix yang kita miliki maka jumlah IP serta range yang kita punya akan semakin luas, maka penguasaan perhitungan subnetting akan sangat penting untuk distribusi IP.

Selanjutnya untuk kadang kala kita diberikan sebuah IP dengan sebuah prefix tapi tanpa disebutkan apakah IP tersebut merupakan Network ID, IP Usable, atau bahkan Broadcast.

Contoh IP : 172.16.10.50/32 = 4 IP

Langkah pertama kita tentukan IP pertama :

IP Pertama = 50 : 4 = 12,..

= 12 x 4

= 48

Maka dari perhitungan tersebut kita bisa menentukan :

IP pertama = 172.16.10.48 (Network ID)

IP Usable = 172.16.10.49 & 172.16.10.50

Broadcast = 172.16.10.51

Dengan menguasai perhitungan subnetting kita bahkan bisa meringkas sebuah prefix dengan menggunakan Prefix yang lebih besar jika IP tersebut berada dalam satu range seperti pada contoh satu (1) dan contoh dua (2), Untuk perhitungan tersebut dinamakan supernetting atau teknik meringkas banyak prefix menjadi satu prefix saja.

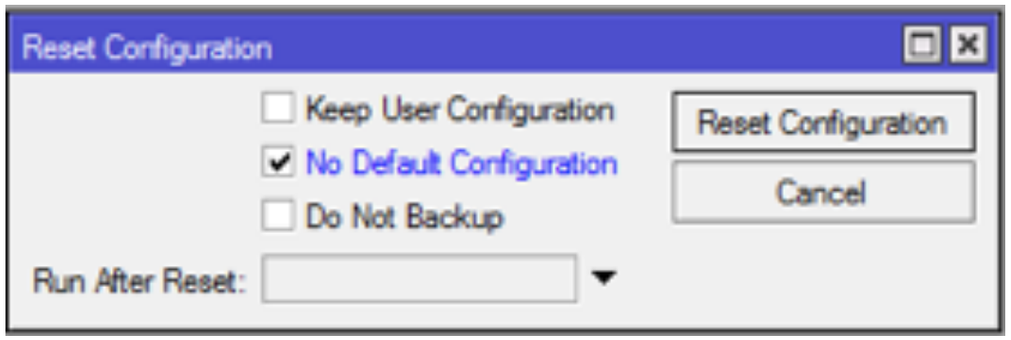
KONFIGURASI DASAR

* Topologi

Konfigurasi :

a) Reset No-Default Configuration

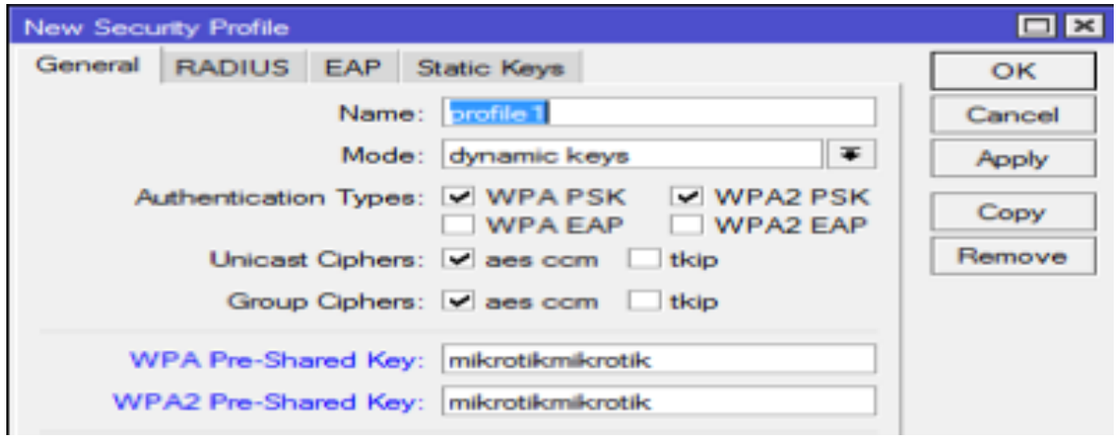
Menu System => Reset Configuration



b) Koneksikan Router Anda ke AP (Internet)

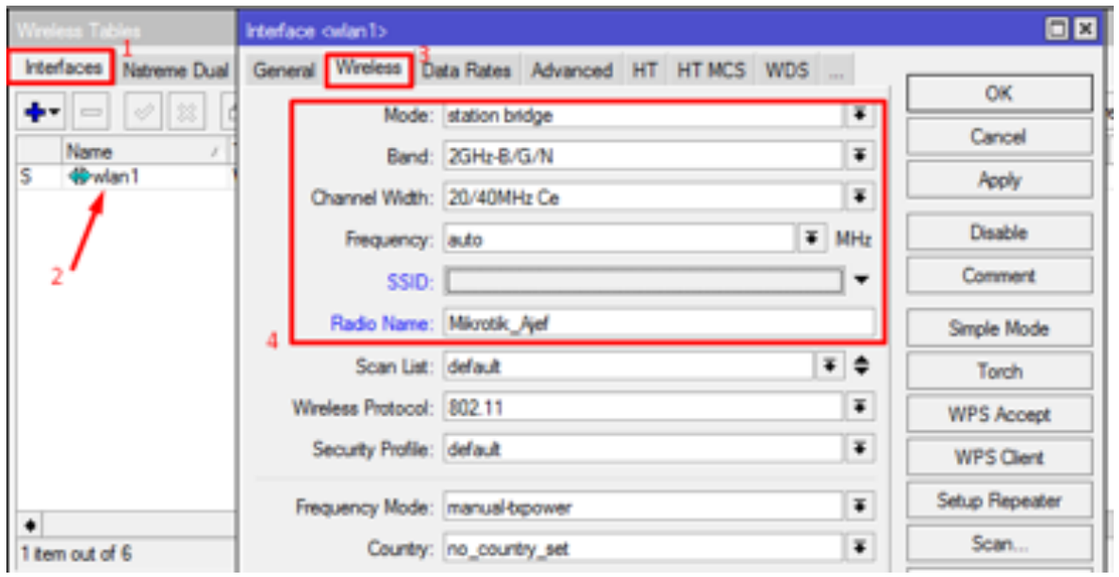
Menu Wireless =>Security Profile

Buat password sesuai dengan security dari ISP atau AP Internet,biasanya konfigurasi password menggunakan type antentikasi WPA/WPA2 PSK dan harus terdiri dari delapan (8) karakter atau lebih.

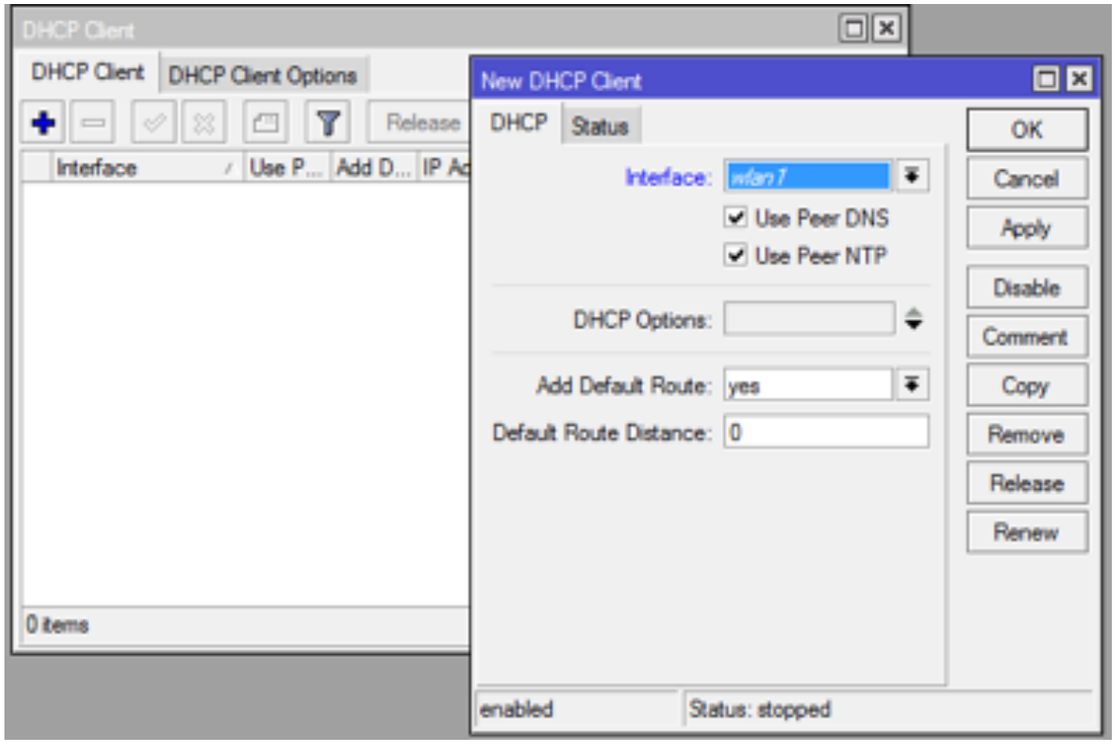


- Menu Wireless > Interfaces > Wlan > Wireless

Untuk konfigurasi wireless, Kita gunakan Mode Station Bridge,SSID harus kita kosongkan karena kita hanya sebagai station dan tidak memancarkan wifi untuk klien.Dan untuk settingan lainnya menyesuaikan setting AP Internet.



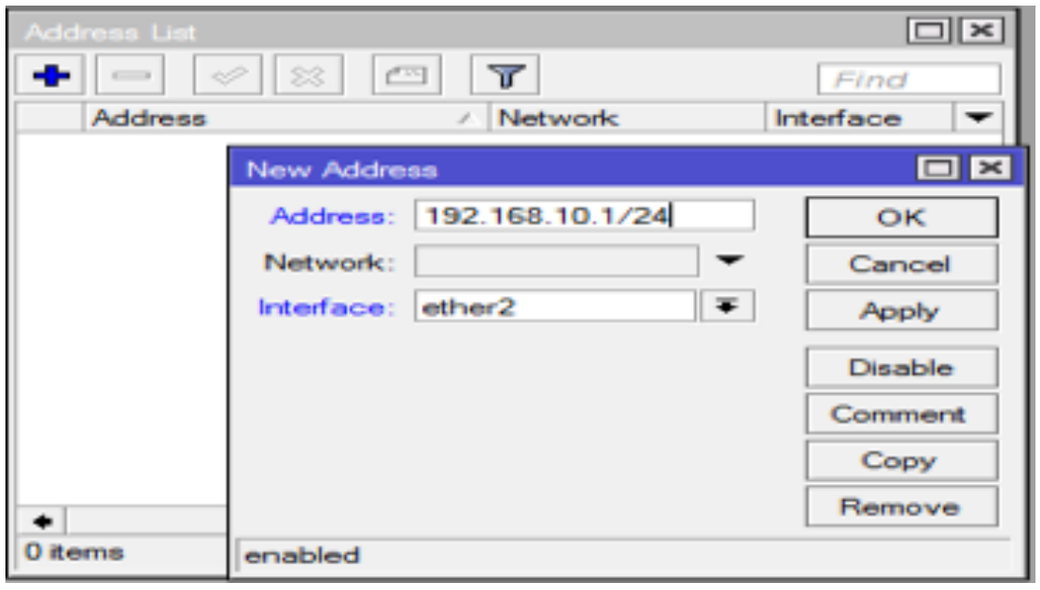
Menu IP => DHCP Client => Add (IP WAN)



Menu IP => Addresses =>Add (IP LOKAL)

a) Address = 192.168.X.X/24

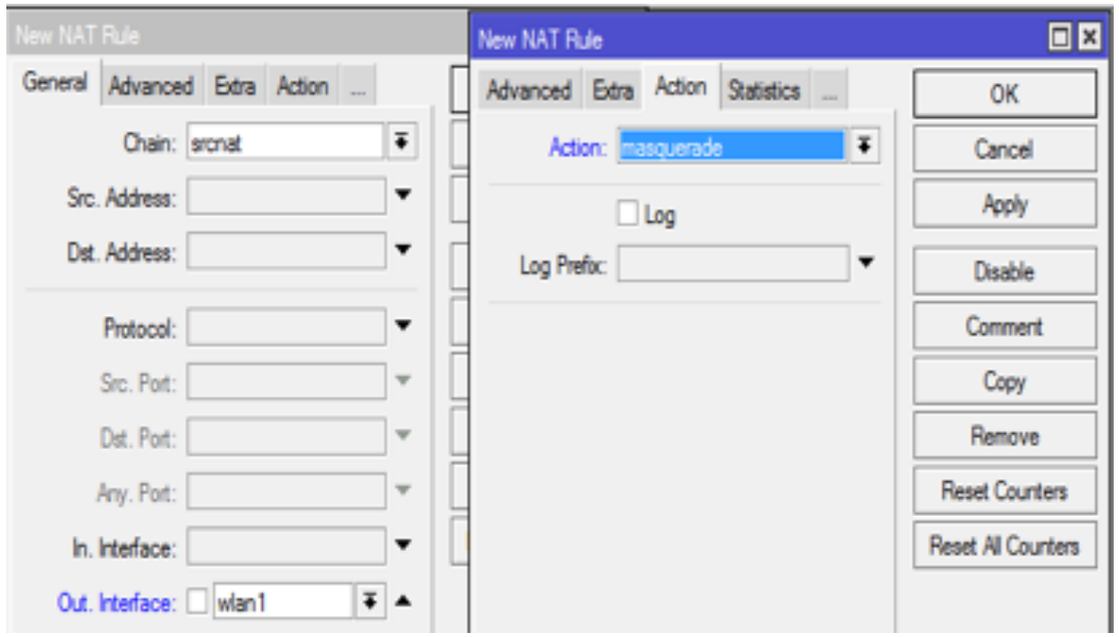
b) Interface = Ether2 (Ethernet yang terhubung dengan laptop anda)



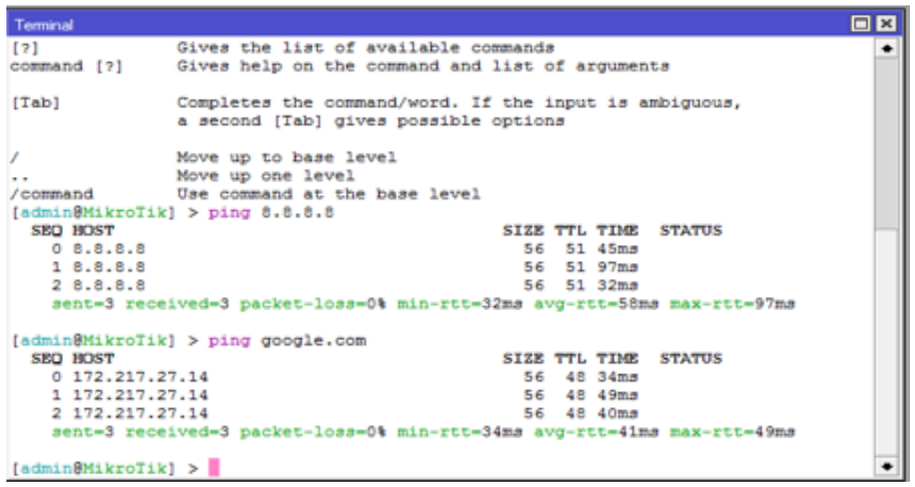
Menu IP => Firewall => NAT => Add

a) Chain = src-nat

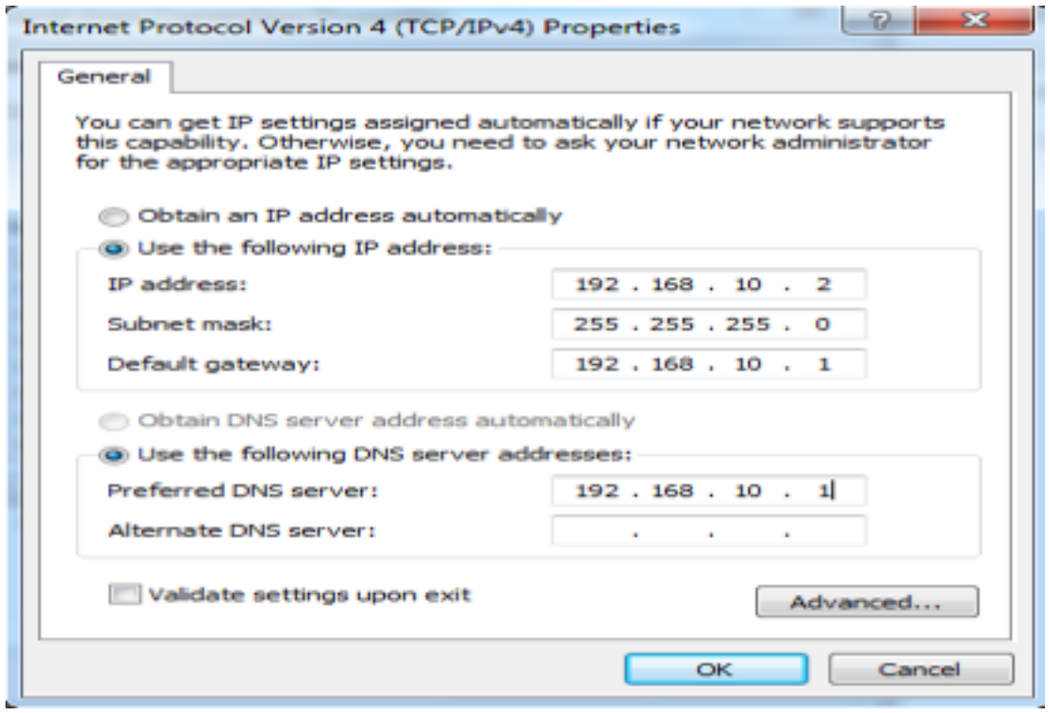
b) Out.Interface = Wlan1 (Ethernet yang terhubung dengan Internet) Action = Masquarade



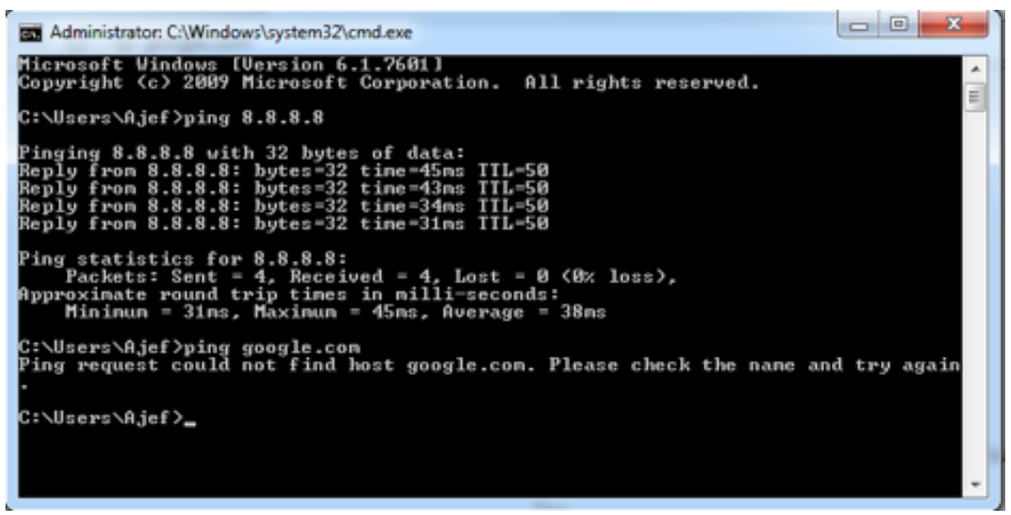
Seharusnya sampai tahap konfigurasi ini router sudah terkoneksi dengan internet.Silahkan anda test dengan ping 8.8.8.8 dan ping google.com



Agar laptop anda juga terkoneksi dengan internet,setting ip static yang berada satu segment dengan IP local yang anda buat pada router anda

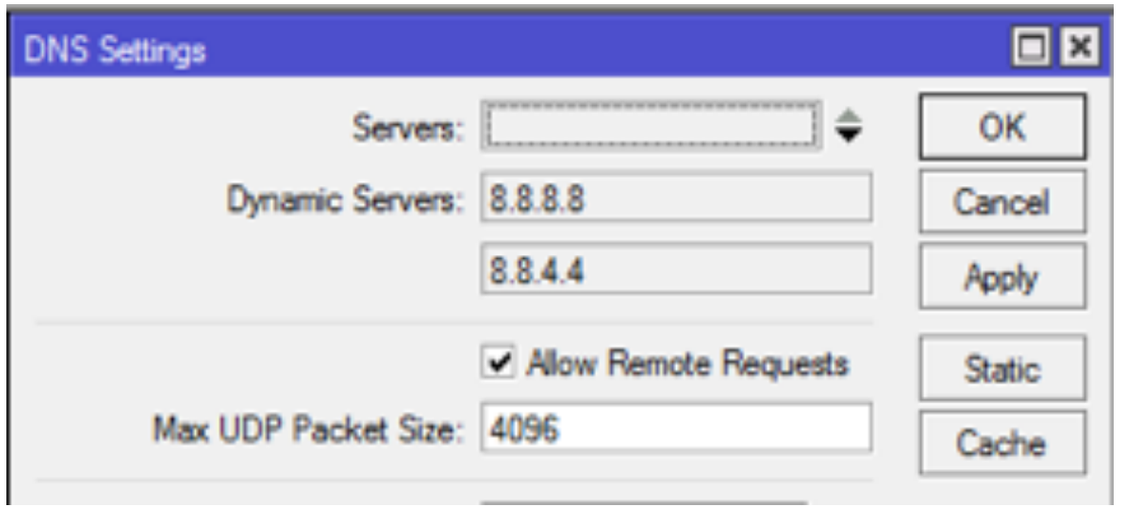


Sekarang laptop anda sudah bias mengakses internet tanpa harus terkoneksi langsung dengan Wifi(Internet) tapi menggunakan LAN pada router anda.



Seharusnya laptop anda belum bisa melakukan test ping/ mengakses menggunakan domain seperti google.com.Anda perlu set request DNS dari router anda untuk mengizinkan perangkat yang terhubung dengan LAN anda bisa mengakses internet dengan nama domain.

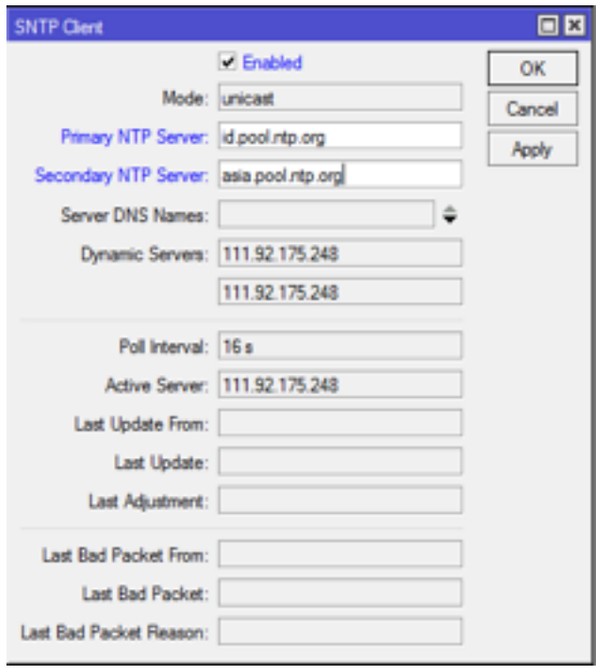
• IP => DNS

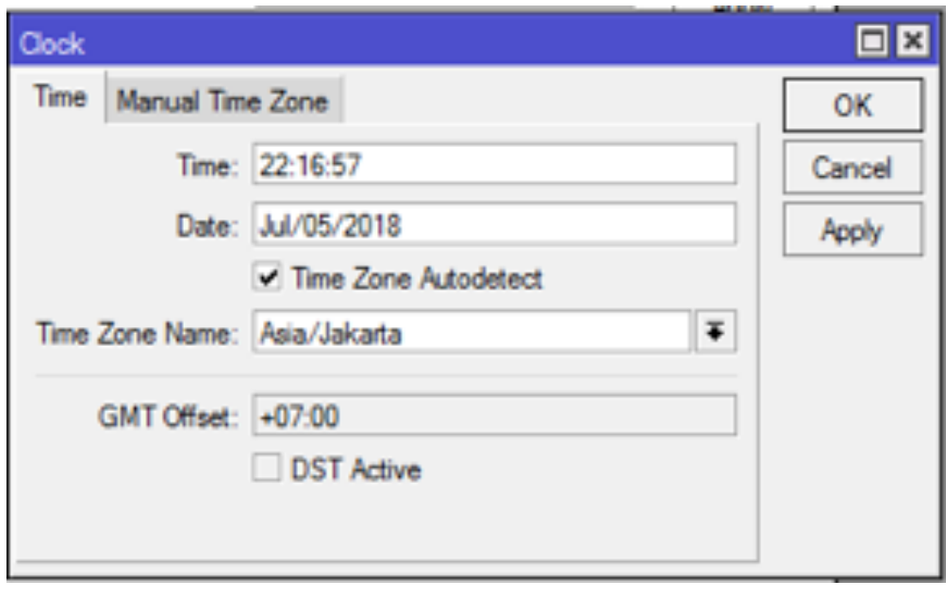


Sekarang laptop anda seharusnya sudah bisa mengakses internet dengan domain dan melakukan test ping ke google.com.Nah, Default konfigurasi waktu dari mikrotik belum sesuai dengan GMT daerah anda masing-masing, maka dari itu anda perlu melakukan konfigurasi waktu agar sesuai dengan waktu setempat.

•Menu System => SNTP Client

• Menu System => Clock





Sampai pada tahap ini Router maupun laptop anda sudah terkoneksi dengan internet baik dan waktu pada router anda sudah sesuai dengan waktu setempat.

UPGRADE & DOWNGRADE ROUTER OS

Kenapa harus UPGRADE?

- Upgrade RouterOS biasanya dilakukan karena adanya perbaikan bug dari versi sebelumnya (Terutama direkomendasikan oleh mikrotik)
- upgrade dilakukan umumnya karena adanya fitur baru yang dibutuhkan oleh user
- Adanya peningkatan kinerja dan stabilitas pada versi selanjutnya

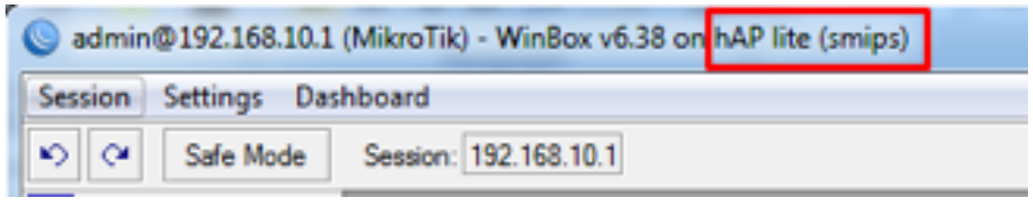
Ada beberapa tipe paket yang bisa kita pilih untuk upgrade routerOS :

- Bugfix only = Pada tipe paket ini hanya ada perbaikan bug dan tidak ada penambahan fitu-fitur baru,jadi cocok untuk anda yang masih nyaman dengan versi sekarang dan hanya ingin memperbaik bug yang ada.
- Current = Pada tipe paket ini adanya perbaikan bug dan penambahan fitur-fitur yang baru,dan untuk cara kerja system biasanya memiliki sedikit perbedaan dari versi sebelumnya.
- Legacy = Tipe paket ini digunakan untuk versi mikrotik yang dulu,sudah jarang digunakan kecuali dengan alasan tertentu, seperti ingin membandingkan versi OS yang lama dengan yang baru.
- Release candidate = Paket ini adalah versi OS yang akan diluncurkan selanjutnya(pengembangan), diperkenankan untuk mencoba namun tidak untuk digunakan sebagai OS utama yang digunakan untuk beroperasi, hal ini karena masih dikembangkan un-

tuk mencari bug dan kekurangan sehingga nanti siap diluncurkan jika sudah dianggap stabil.

- Untuk melihat apa saja fitur terbaru yang ada pada mikrotik versi terbaru bisa anda cek di Mikrotik.com, changelogs.
- Dalam Memilih package routerOS untuk upgrade hal yang terpenting dilakukan adalah mengetahui tipe arsitektur routerBoard kita agar tidak terjadi kesalahan download package.

Lihat melalui winbox



Melalui Web Dowload package

	6.40.8 (Bugfix only)	6.42.5 (Current)	5.26 (Legacy)	6.43rc42 (Release candidate)
MIPSBE	CRS1xx, CRS2xx, DISC, hAP, hAP ac, hAP ac lte, LDF, LHG, mANTBox, mAP, NetBox, NetMetal, PowerBox, QRT, RB9xx, cAP, HEX Lite, RB4xx, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx			
Main package				
Extra packages				
SMIPS	hAP mini, hAP lite			
Main package			-	
Extra packages			-	
TILE	CCR			
Main package			-	
Extra packages			-	
The Dude server			-	
PPC	RB3xx, RB600, RB8xx, RB1100AHx2, RB1100AH, RB1100, RB1200			

Bagaimana memilih package RouterOS?

Main Package = Semua Package RouterOS sudah tersedia dan bisa langsung digunakan dan diinstall.

Extra Package = Package RouterOS terpisah-pisah dan kita bisa menentukan sendiri package apa saja yang kia butuhkan di RouterOS yang akan kita gunakan.

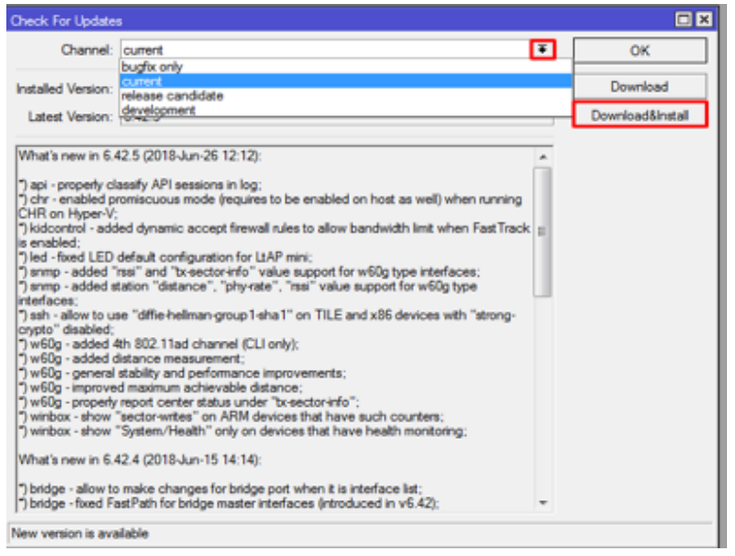
Cd Image = digunakan untuk menginsall routerOS pada PC Biasa

	6.40.8 (Bugfix only)	6.42.5 (Current)	5.26 (Legacy)	6.43rc42 (Release candidate)
MIPSBE	CRS1xx, CRS2xx, DISC, hAP, hAP ac, hAP ac lte, LDF, LHG, mANTBox, mAP, NetBox, NetMetal, PowerBox, QRT, RB9xx, cAP, HEX Lite, RB4xx, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx			
Main package				
Extra packages				
SMIPS	hAP mini, hAP lite			
Main package			-	
Extra packages			-	
TILE	CCR			
Main package			-	
Extra packages			-	
The Dude server			-	

Bagaimana cara UPGRADE ?

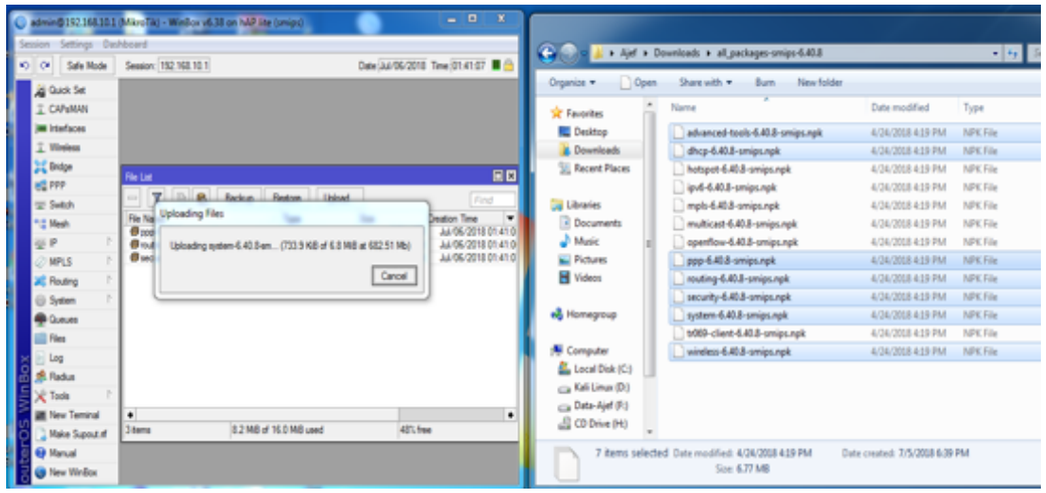
Ada beberapa cara yang bias dilakukan untuk Upgrade RouterOS :

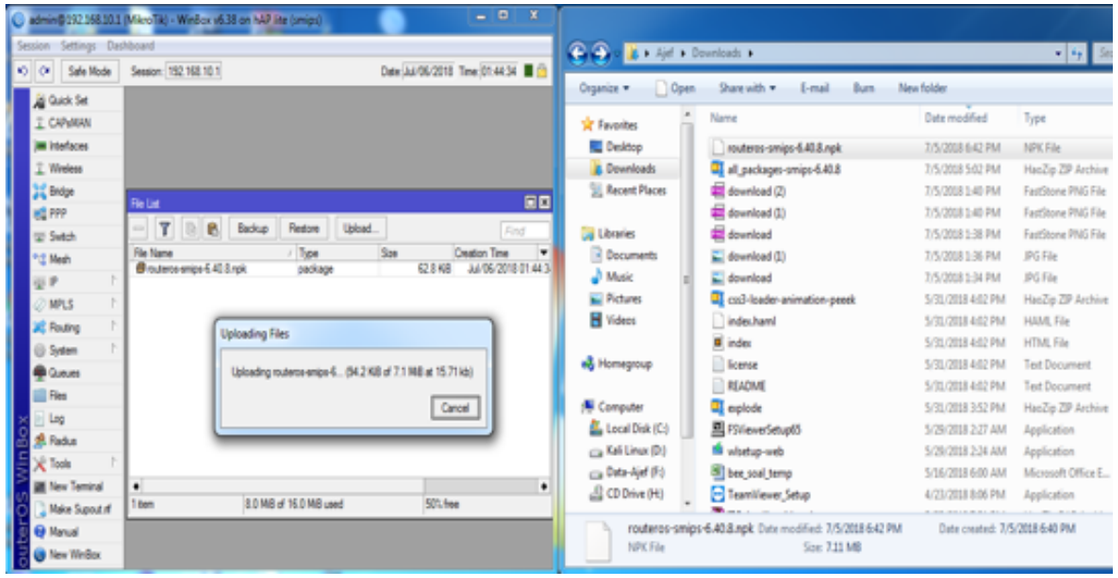
1. Menu System => Packages => Check For Updates

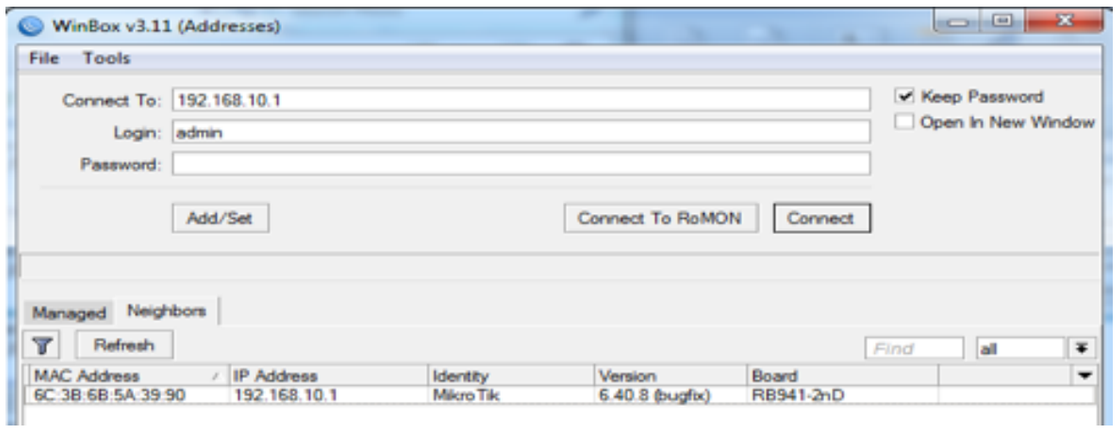


Selanjutnya router akan restart otomatis, dan versi RouterOS seharusnya sudah berubah.

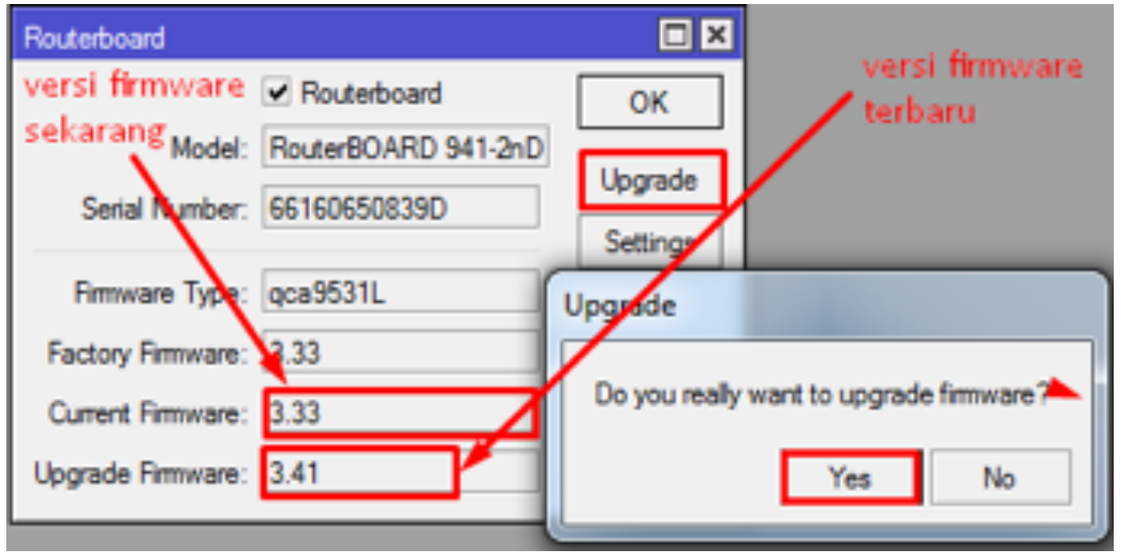
1. Download Package (Main Package/Extra Package) di web resmi mikrotik https://mikrotik.com/download, lalu lakukan drag and drop package yang sudah di download ke dalam menu File pada mikrotik anda.Dan setelah selesai proses upload,lakukan reboot pada mikrotik anda,maka otomatis versi routerOS mikrotik anda akan berubah sesuai versi OS yang kita upload.+







Selain upgrade versi routerOS kita juga perlu mengupgrade firmware/BIOD RouterBoard agar tetap selalu update yang terbaru. : System => Routerboard



Kadang kala kita tidak bisa melakukan upgrade routerOS jika firmware yang kita gunakan masih versi lawas, maka dari itu upgrade firmware merupakan salah satu syarat untuk melakukan Upgarade RouterOS.

KEAMANAN DASAR ROUTER

Keamanan adalah sesuatu yang sangat penting dan wajib diterapkan dalam setiap konfigurasi router, sebelum menerapkan sistem keamanan yang luas (Firewall,NAT,Filter Rules, dll) ada beberapa hal penting yang wajib dilakukan untuk menjaga keamanan router kita.

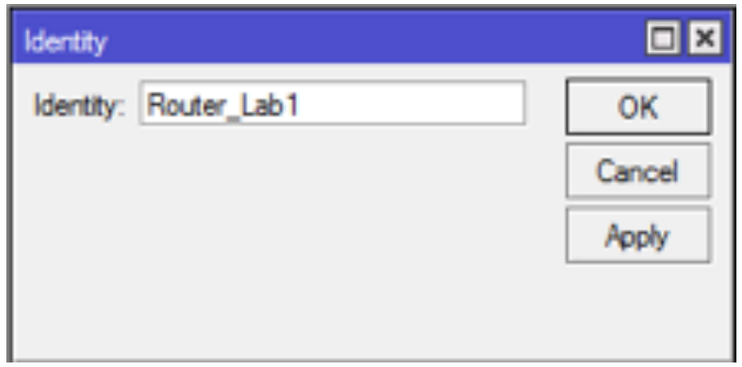
1) Identitas

Jika kita menggunakan banyak router dalam jaringan yang kita bangun, maka identitas dari sebuah router akan sangat membantu untuk manajemen troubleshoot dan perbaikan, bayangkan kita punya 100 router namun dengan nama default mikrotik.Ada dua cara untuk merubah identitas mikrotik kita,yakni menggunakan console pada mikrotik dan melalui menu system identity.

/System identiy set name = Router_Lab1

```
[admin@Router_Lab1] > system identity set name=Router_Lab1
[admin@Router_Lab1] >
```

Menu System => Identity



2) Username & Password

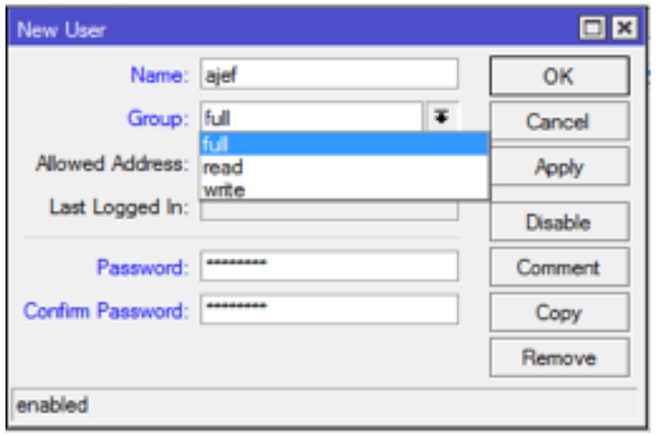
Hal yang paling penting selanjutnya adalan username dan password login router, default username dan password mikrotik yaitu username = admin dengan password = (kosong) jadi akan sangat rentan jika username dan password default tidak diganti.

Jika menggunakan console =

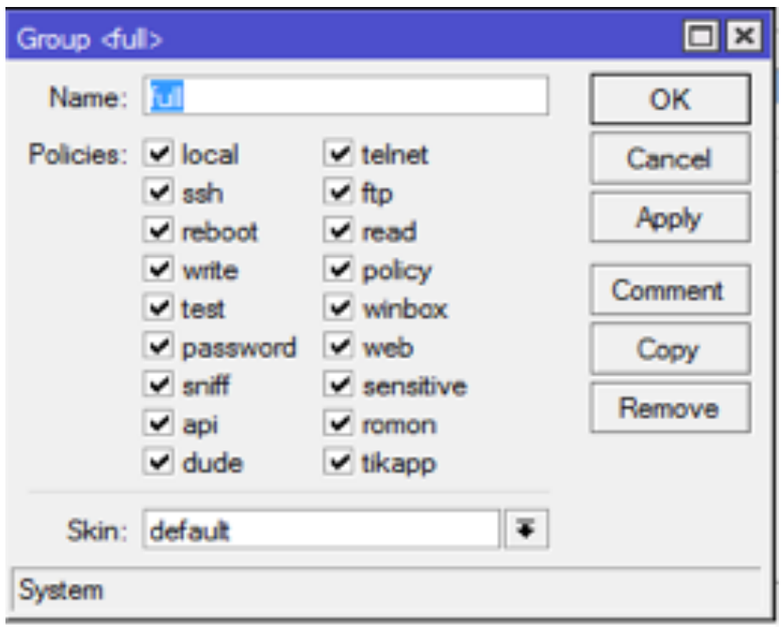
password lalu enter
old pasword : (pasword yang lama , jika baru diinstal berarti dikosongkan)
new password : (masukkan password bar)
confirm new pasword : (masukkan password baru sekali lagi)

```
[admin@Router_Lab1] > password
old-password:
new-password: ********
confirm-new-password: ********
```

)Menu System > Users > Add (Untuk pemilihan grub,silahkan pilih salah satu sesuai dengan kebutuhan)



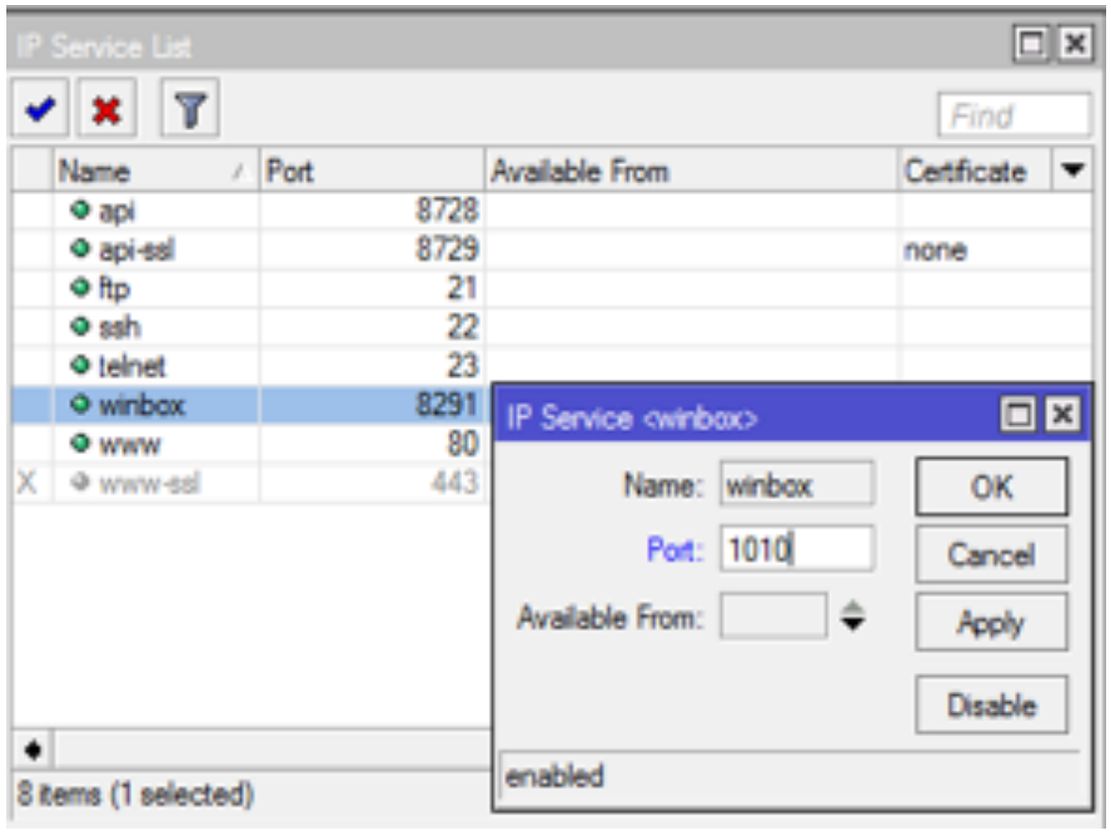
Selain group default yang sudah ditetapkan pada router, kita juga bisa mengubah kebijakan yang digunakan sesuai dengan yang diinginkan dan bisa membuat group baru sesuai kebutuhan untuk router



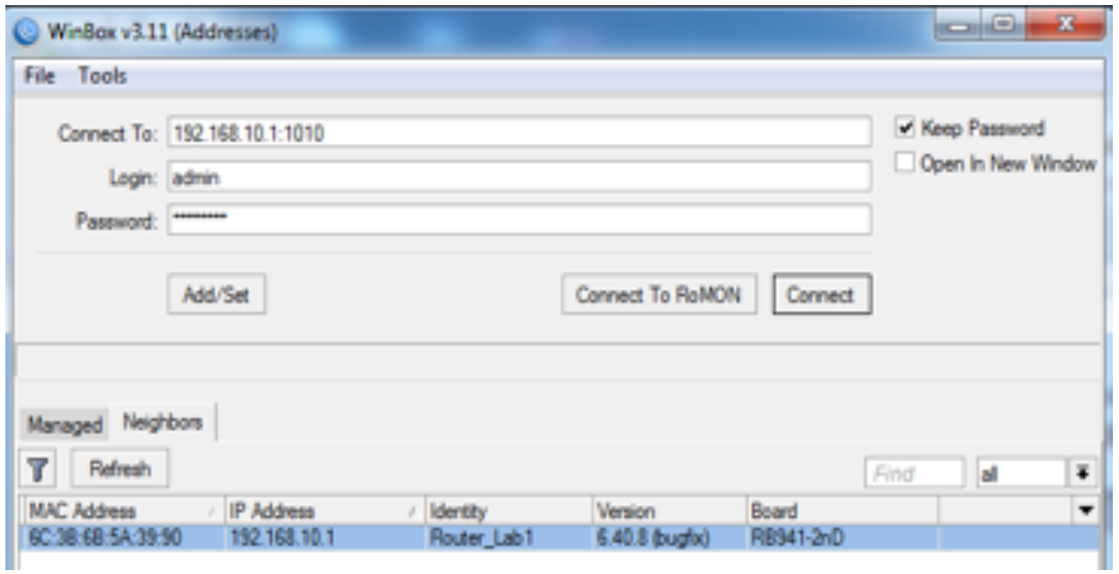
3) Manajemen Port

Untuk mengakses mikrotik kita menggunakan beberapa layanan service protocol dan menggunakan port default yang sudah ditentukan, untuk menjaga keamanan router akan sangat membantu jika kita merubah port untuk mengakses router agar tidak sembarang orang bisa mencoba untuk login. Untuk port yang tidak dipakai atau tidak aman by default harus di disable.Untuk yang masih dipakai, default port harus diganti.

Menu IP > Services (Anda bisa merubah port sesuai keinginan dengan syarat port yang digunakan tidak dipakai oleh service yang lain)



Jika kita merubah port dari sebuah winbox atau www, maka untuk mengakses mikrotik kita perlu menyertakan port yang kita buat saat ingin login ke router kita.

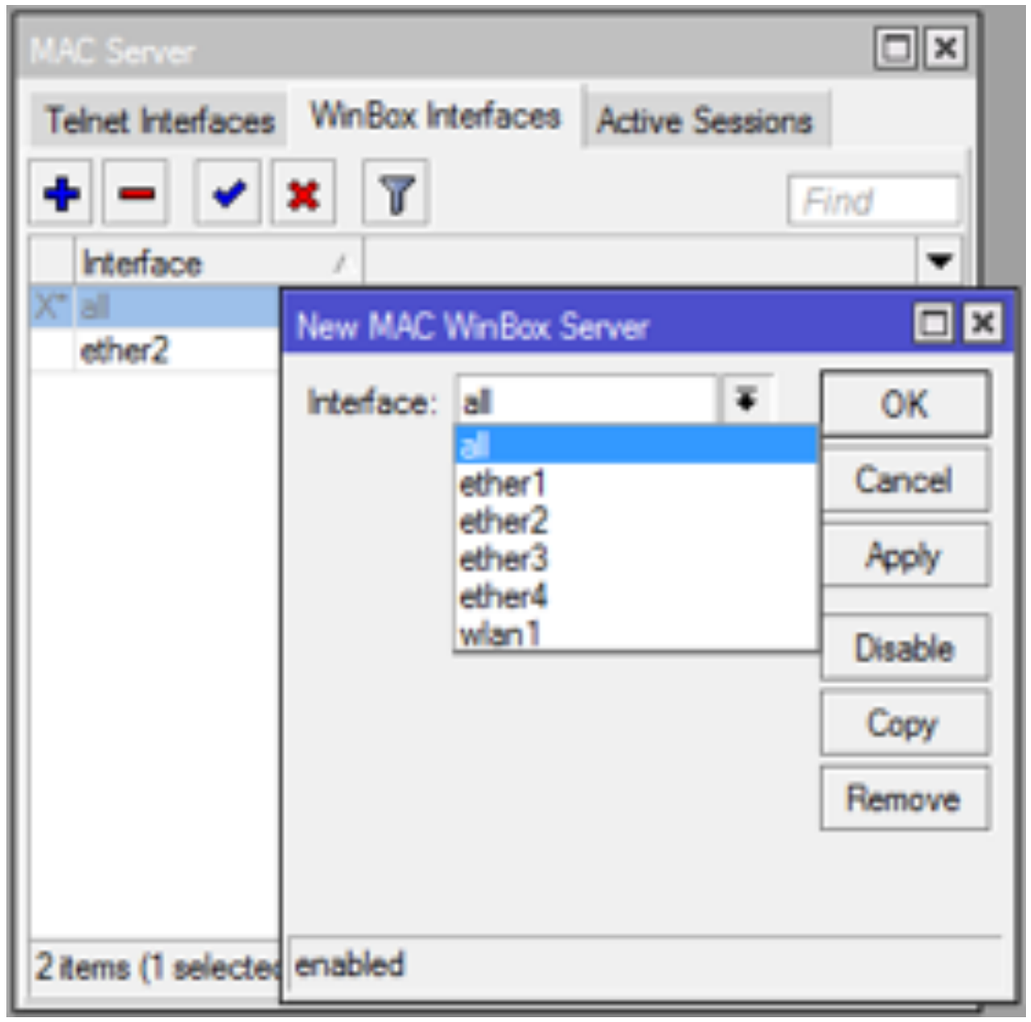


4) Manajemen Mac Server

Pada defaultnya kita bisa login ke router melalui semua Ethernet yang ada pada mikrotik, untuk keamanan selanjutnya kita bisa memanagemen Ethernet mana saja yang bisa digunakan untuk login ke router.

Menu Tools > Mac Server > Add

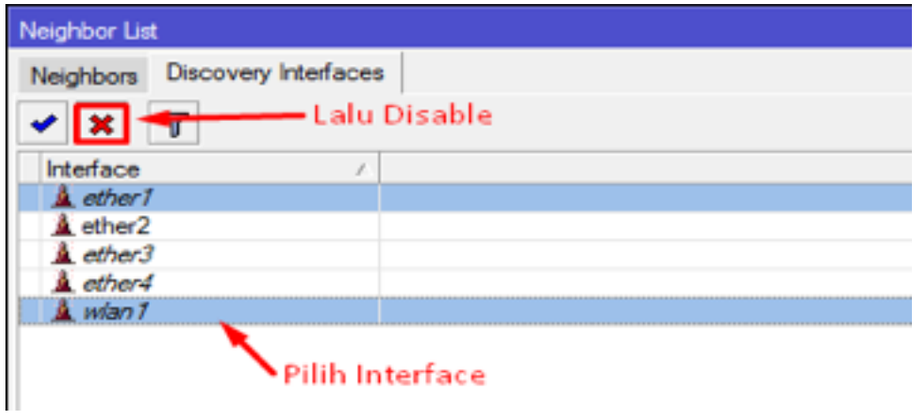
Note : “Setelah memilih Ethernet mana yang bisa digunakan untuk mengakses router pastikan rule yang menyatakan semua Ethernet bisa digunakan(all) anda disable”



5) Manajemen Discovery Protocol

Dengan adanya fitur neighbor, kita bisa melihat perangkat lain yang terhubung dengan mikrotik kita, mulai dari Radio Name,IP address,Mac Address dan lainya bisa kita lihat pada neighbor.Untuk mencegah mikrotik agar tidak masuk neighbor mikrotik lain maka kita bisa mengatur Ethernet mana saja yang bisa dibaca oleh neighbor di mikrotik.

Menu IP => Neighbor => Discovery Interfaces



Backup-Restore & Export-Import

Kenapa harus backup?

- Jika kita akan mengkonfigurasi banyak router dengan konfigurasi yang sama maka cara terbaik yang dilakukan adalah dengan backup konfigurasi, keuntungannya kita hanya perlu meng konfigurasi satu router dan untuk router lainnya hanya perlu restore konfigurasi yang sudah kita backup.
- Untuk antisipasi jika suatu saat terjadi kerusakan hardware yang mengharuskan kita mengganti perangkat router kita.

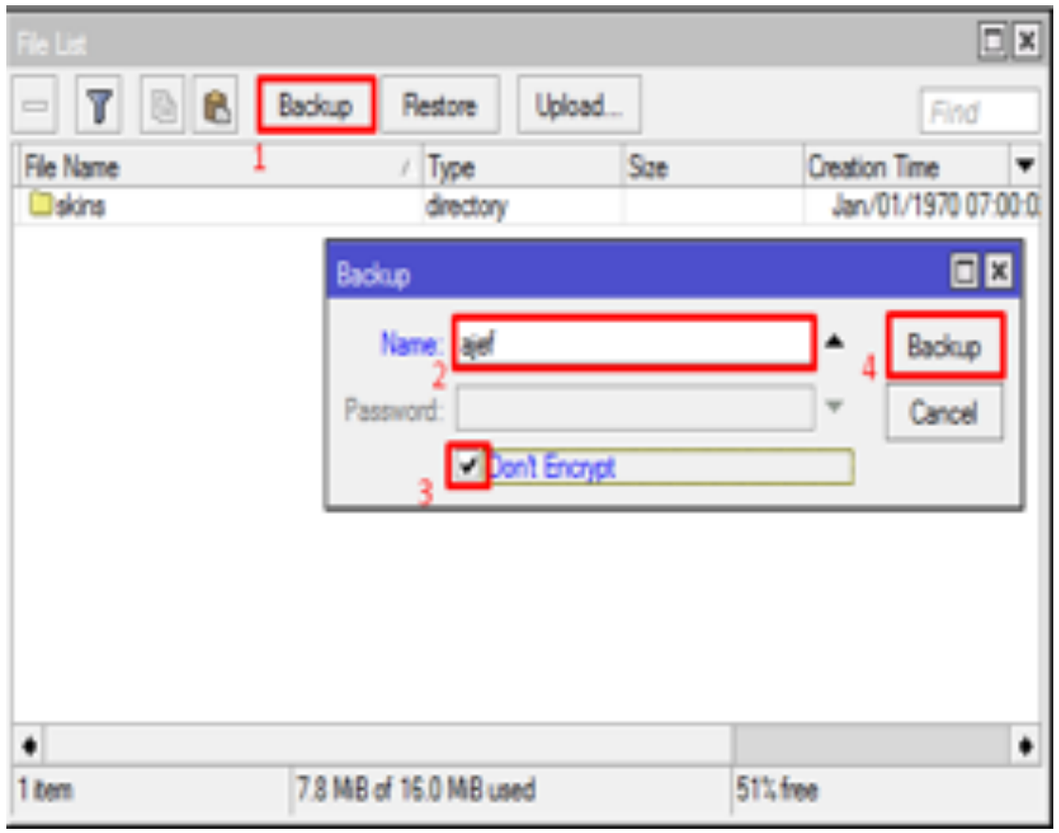
Bagaimana cara backup konfigurasi di router ?

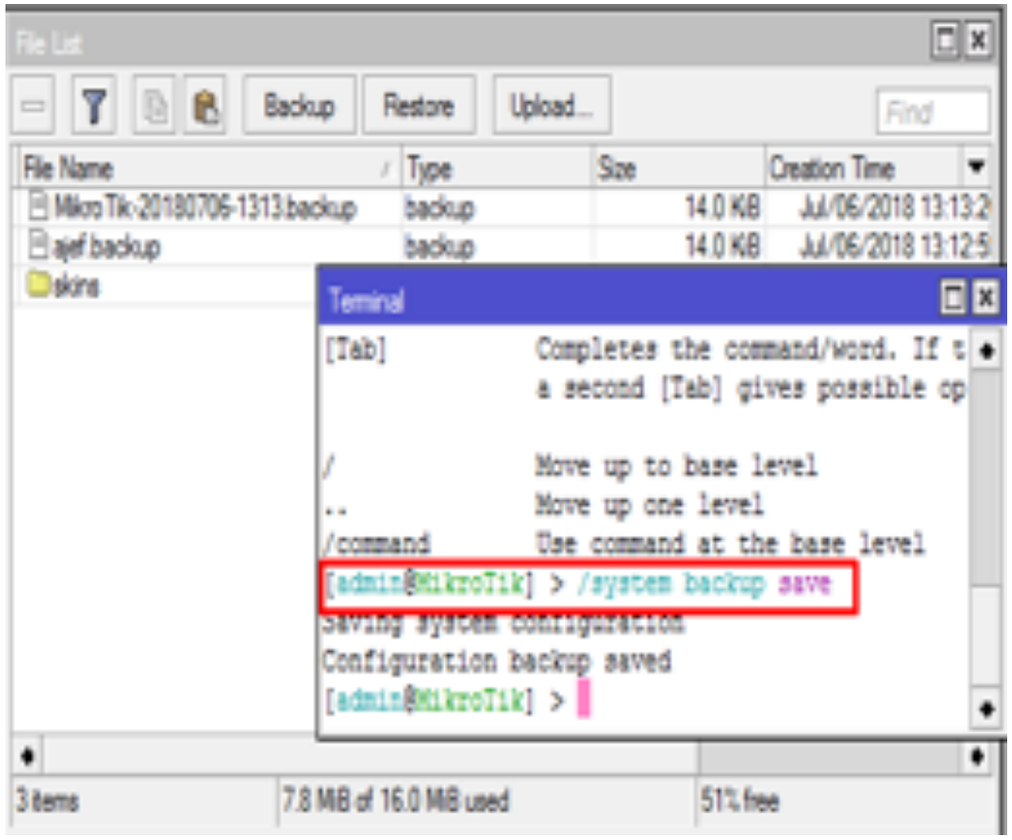
Backup terbagi menjadi dua =

1. /System backup save name=nama_filedon't encrypt=yes atau fitur backup dimenu file pada router anda.

- Outputnya single binary
- Tidak bisa diedit
- Backup seluruh konfigurasi termasuk username dan password
- Hanya bisa di restore di perangkat itu sendiri

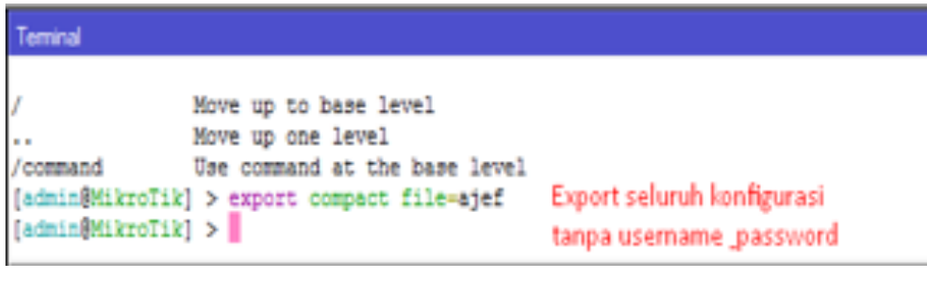
Note : "Pembuatan backup tanpa password jangan lupa don't encrypt diaktifkan"





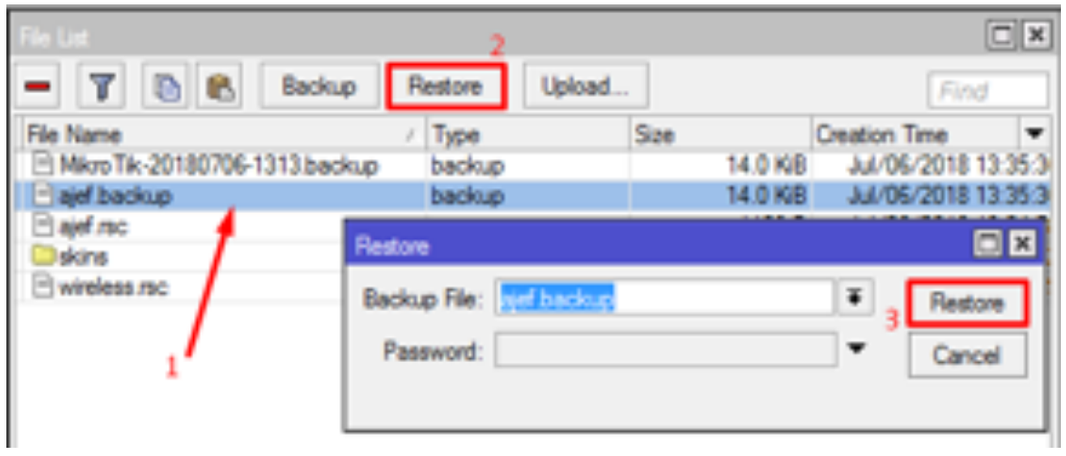
2. Perintah /Export File=.....

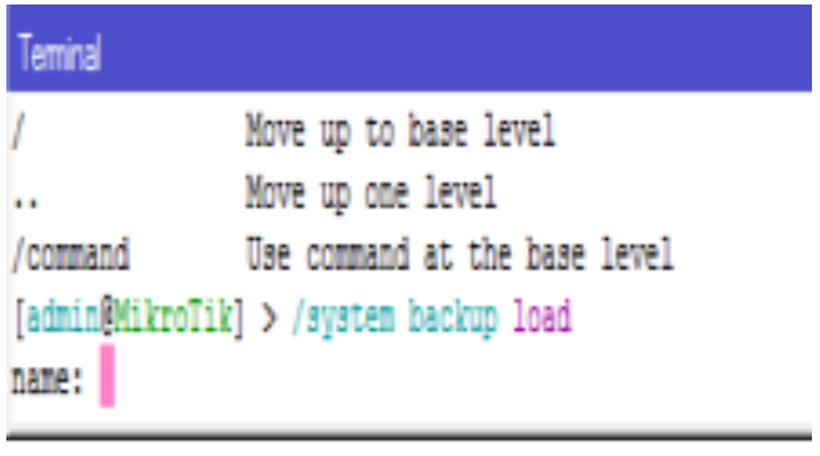
- File backup dalam format script
- Bisa diedit
- Backup hampir seluruh konfigurasi (tidak termasuk username & password)
- Backup bisa dilakukan secara parsial



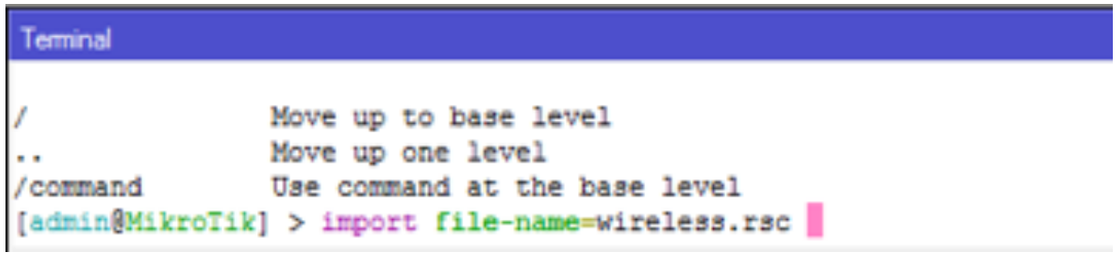
Bagaimana restore konfigurasi di router

1. Untuk file backup dengan cara pertama bisa dengan /system backup load atau tombol restore di menu file.(File backup harus sudah diupload ke root directorymenu file)





2. Untuk file backup dengan cara kedua import menggunakan CLI pata terminal router



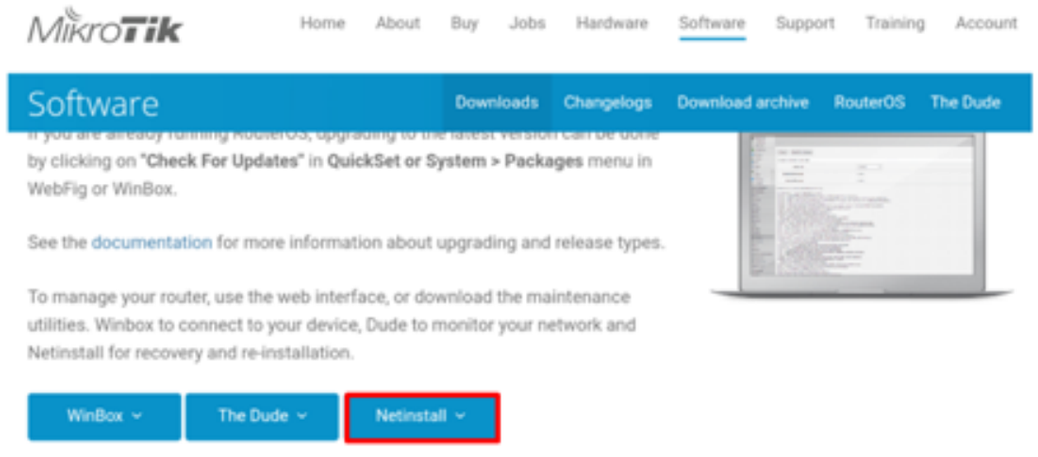
NETINSTALL

Kenapa harus melakukan NETINSTALL ?

Netinstal biasa digunakan untuk melakukan install ulang RouterBoard / PC Router yang sudah support net-boot dan menjaga agar lisensi yang ada tidak hilang.Biasanya masalah seperti lupa username atau password login router namun kita tidak bisa melakukan hardreset pada mikrotik maka jalan satu-satunya yang bisa dilakukan adalah dengan Install ulang router anda.Selain itu karena ada masalah pada router seperti tidak berfungsinya beberapa Ethernet dan lain lain, maka solusi terakhir yang bisa dilakukan adalah netinstall.

Langkah-langkah melakukan netinstall :

1. Download program netinstall dan package yang dibutuhkan, pada situs resmi mikrotik.com/download

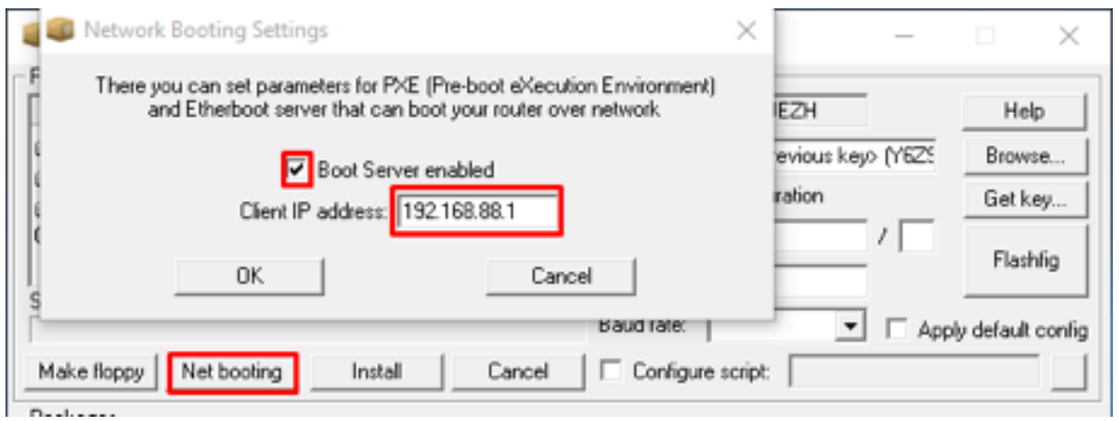


1.

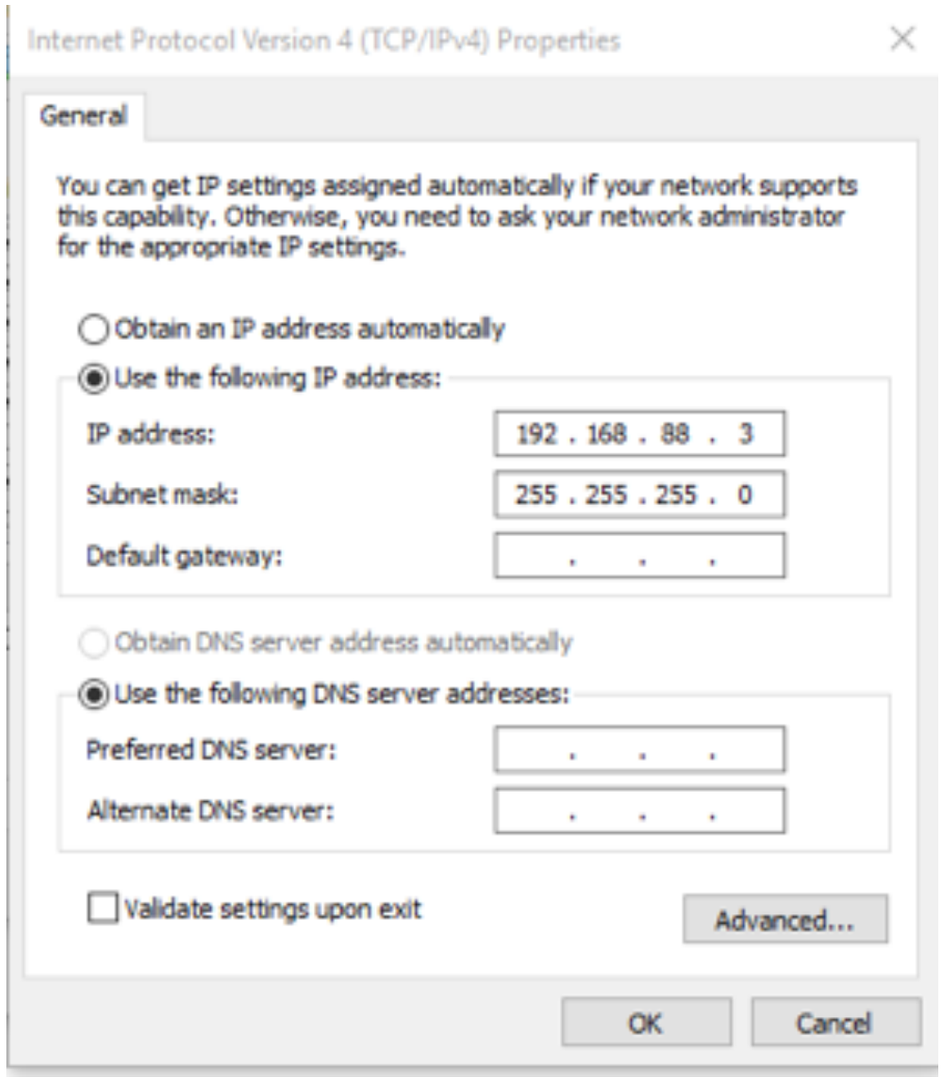
2) Hubungkan Ethernet laptop anda via Ethernet 1 atau boot interface (console) pada router anda.

3) Jalankan program Netinstall.exe yang sudah anda download, lalu aktifkan Netboot Protocol (BootTP)

- Isikan IP untuk Router untuk Boot melalui ethernet.



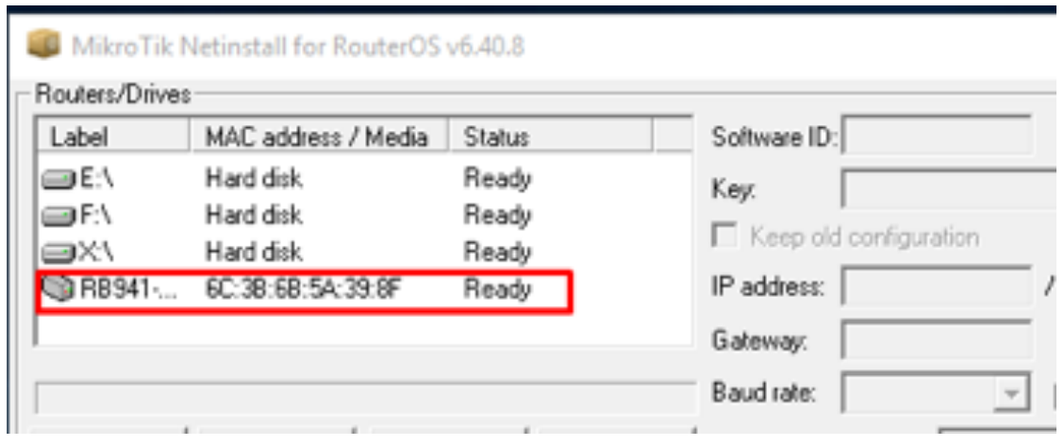
- Lalu konfigurasi IP lapto anda satu segment dengan IP Router yang anda tentukan pada Net Booting



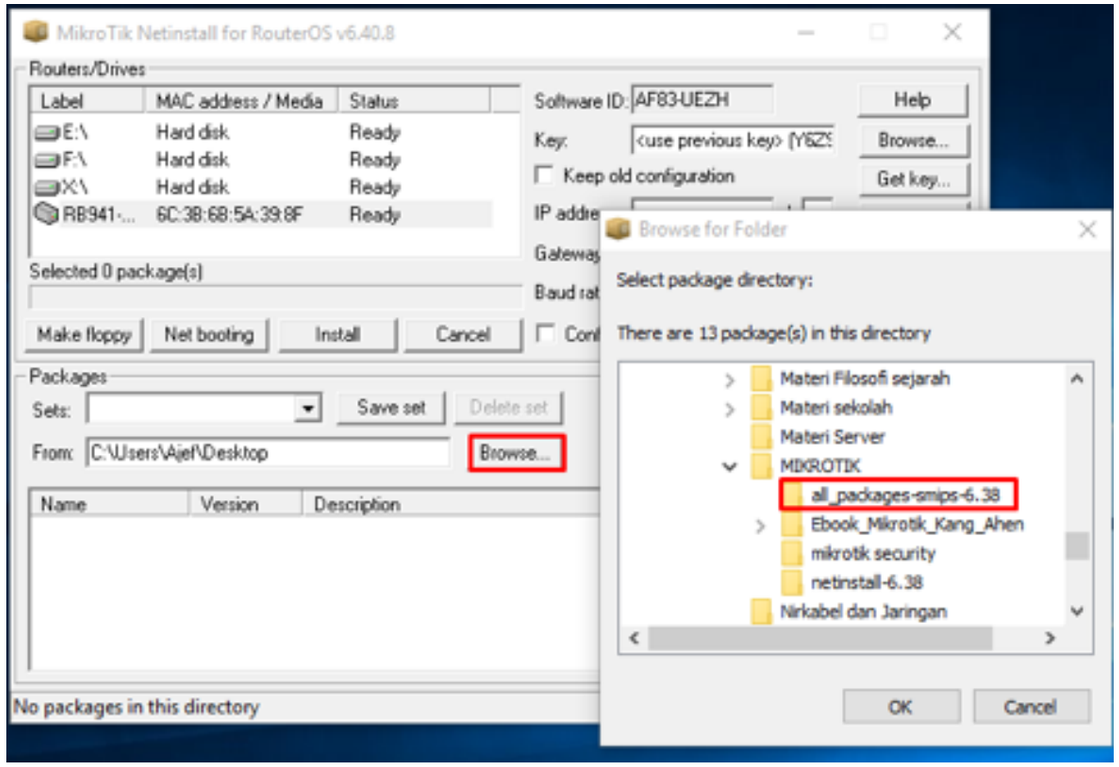
4) Reset router untuk masuk mode netinstall

- Tekan tombol reset selama 15 detik
- Untuk router yang memiliki console port,boot sequence diru-bah menjadi boot to ether melalui firmware/BIOS

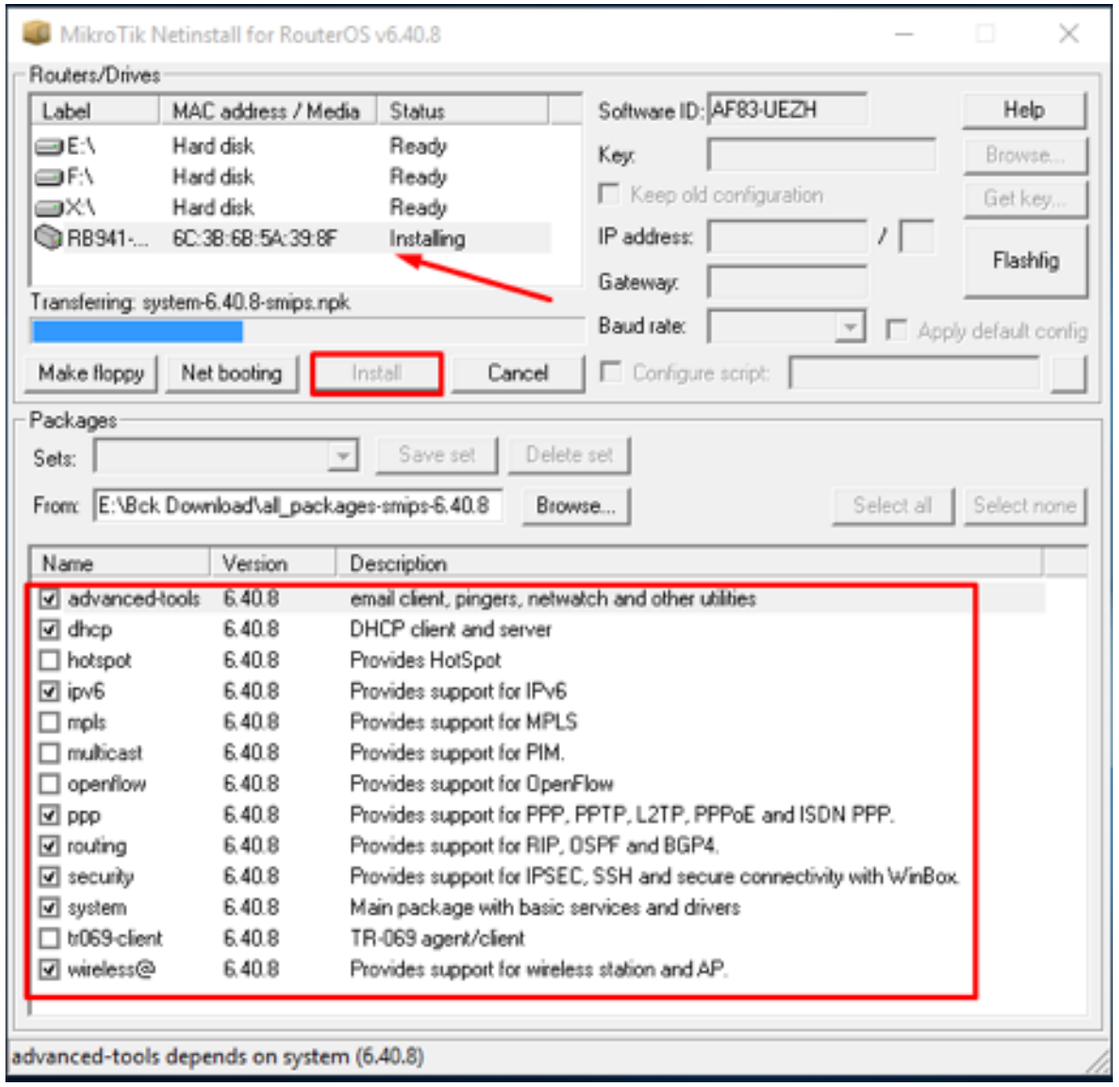
- Pastikan Storage dari Router anda muncul, jika tidak muncul, disable firewaal pada laptop anda dan matikan antivirus yang terpasang pada laptop anda



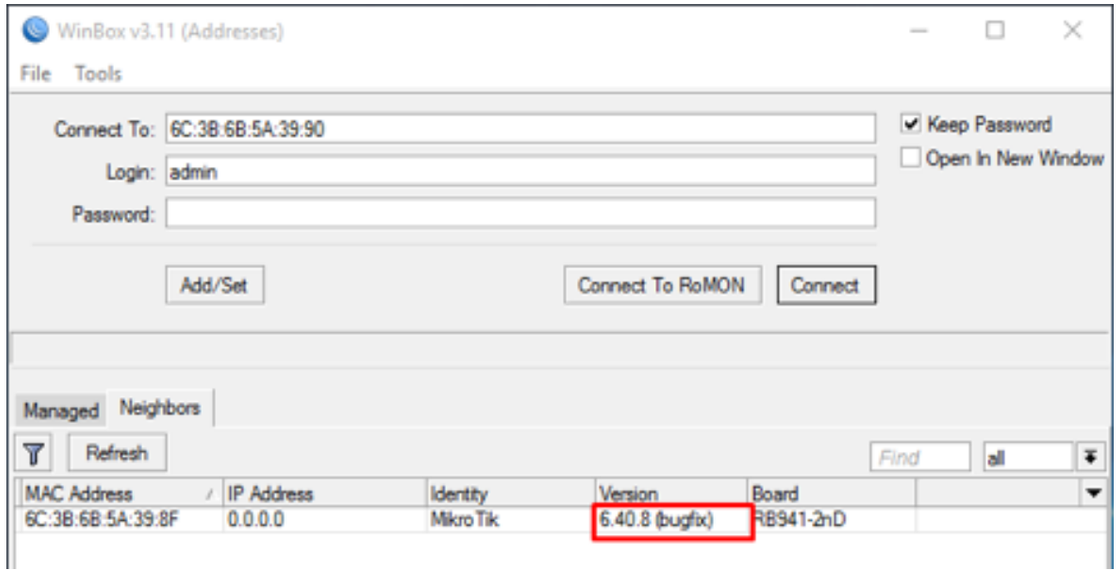
5) Setelah router anda muncul di aplikasi netinstall,pilih perangkat lalu browse ke folder RouterOS yang akan diinstall disimpan.Pilih package yang akan diinstall,kemudian klik tombol install.



6) Selanjutnya pilih paket yang ingin anda install, lalu klik Install dan Tunggu proses hingga selesai, router anda akan restart



7) Masuk kembali ke winbox dan anda bisa melihat versi routerOS anda sudah berubah.Login sebagai admin dan restore konfigurasi (Jika ada backupnya)



Beberapa kendala yang umumnya ditemui saat melakukan netinstall biasanya :

- Storage routerOS tidak muncul biasanya disebabkan karena windows firewall dan windows defender pada laptop anda masik aktif, pada sebagian laptop setelah kita disable namun masih tetap tidak muncul perlu dilakukan restart computer.Selain itu Adanya antivirus yang terpasang pada laptop anda perlu anda disable terlebih dahulu.
- Proses Install tidak berjalan biasanya disebabkan karena versi netinstall kita terlalu lama, atau versi netinstall tidak sesuai dengan package RouterOS yang akan kita install.

Lisensi Mikrotik

Mikrotik OS sesungguhnya adalah gratis, tapi gratis disini hanya diberikan kemampuan-kemampuan tertentu. Untuk mendapatkan fitur-fitur mikrotik secara penuh kita harus membeli sebuah lisensi. Dan agar lisensi mikrotik lebih ter-

jangkau, maka lisensi ini pun dibagi menjadi beberapa level yang disesuaikan dengan kebutuhan pengguna mikrotik.

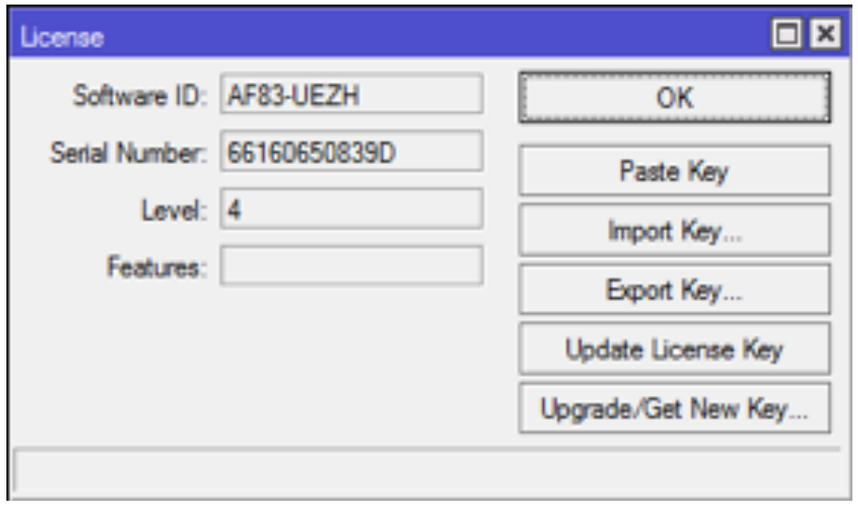
- Level 0 (gratis) tidak membutuhkan lisensi untuk menggunakannya dan penggunaan fitur hanya dibatasi selama 24 jam setelah instalasi dilakukan.
- Level 1 (demo) pada level ini kamu dapat menggunakannya sebagai fungsi routing standar saja dengan 1 pengaturan serta tidak memiliki limitasi waktu untuk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

Untuk aplikasi hotspot, bisa digunakan level 4 (200 user), level 5 (500 user) dan level 6 (unlimited user). Detail perbedaan masing-masing level dapat dilihat pada tabel di bawah ini: Anda bisa melakukan generate licensi, pada mikrotik.com pada menu make a demo key.

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

Untuk melihat lisensi yang anda gunakan di mikrotik anda, bisa cek dengan cara :

Menu System => Licensi



Namun Untuk Lisensi cloud hosted router yang dibatasi adalah kecepatan bandwidth nya, berdasarkan perpetual.

Perlu diperhatikan bahwa licensi melekat pada storage jadi jika perangkat storage rusak atau kita melakukan install ulang maka licensi bisa saja hangus.

MikroTik

MTCNA

MikroTik Certified Network Associate Training

DHCP

Dynamic Host Control Protocol

Dynamic host control protocol atau yang lebih sering disebut DHCP adalah layanan yang digunakan untuk memberikan IP secara otomatis dalam sebuah jaringan.IP Address dan net-mask IP Address default gateway Konfigurasi DNS dan NTP ServerDan masih banyak lagi custom option (tergantung apakah DHCP client bisa support).

Ada dua macam DHCP yaitu DCHP Server dan DHCP Client, DHCP Server adalah perangkat yang memberikan layanan sedangkan DHCP Client adalah perangkat yang menerima layanan DHCP Server.

Proses DHCP melewati 4 tahap saat menetapkan alamat IP ke klien. Tahapan-tahapan ini sering disingkat DORA, Discovery, Offer, Request dan Acknowledgement.

DHCP Server & DHCP Client

- DHCP Discovery

Klien mengirim pesan siaran di subnet jaringan menggunakan alamat tujuan 255.255.255.255 atau alamat siaran subnet spesifik.

- DHCP Offer

Ketika server DHCP menerima pesan DHCP DISCOVER dari klien, yang merupakan permintaan sewa alamat IP, server menyimpan alamat IP untuk klien dan membuat tawaran sewa dengan mengirimkan pesan DHCP OFFER ke klien. Pesan ini berisi alamat MAC klien, alamat IP yang ditawarkan server, subnet mask, durasi sewa, dan alamat IP server DHCP yang membuat penawaran.

- DHCP Request

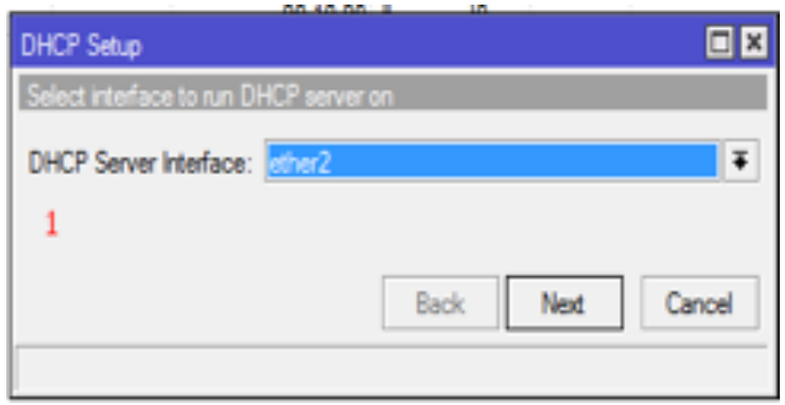
Sebagai tanggapan atas penawaran DHCP, klien membalas dengan permintaan DHCP, menyiarkan ke server, meminta alamat yang ditawarkan. Klien dapat menerima penawaran DHCP dari beberapa server, tetapi hanya akan menerima satu penawaran DHCP. Berdasarkan opsi identifikasi server yang diperlukan dalam permintaan dan penyiaran pesan, server diberitahu yang tawarannya telah diterima klien. Ketika server DHCP lain menerima pesan ini, mereka menarik semua penawaran yang mungkin telah mereka buat ke klien dan mengembalikan alamat yang ditawarkan ke kumpulan alamat yang tersedia.

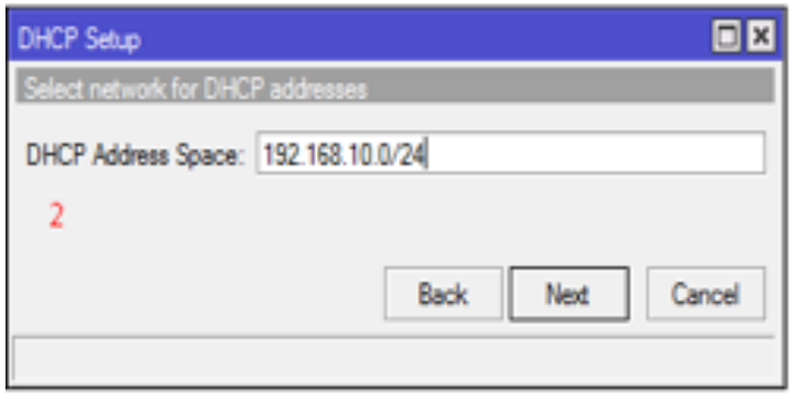
- DHCP Acknowledgement

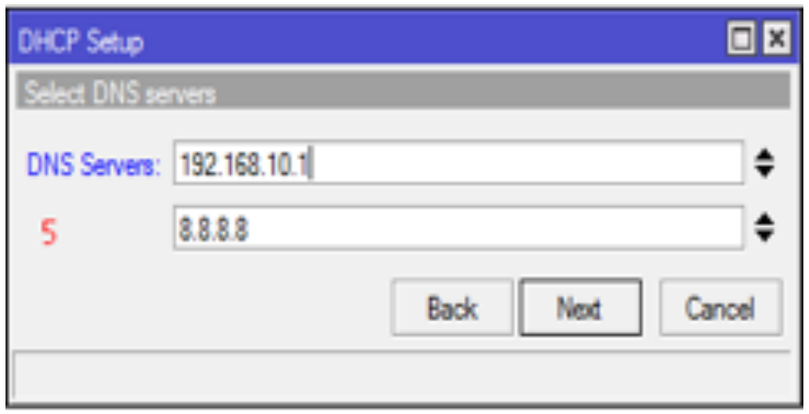
Ketika server DHCP menerima pesan DHCP REQUEST dari klien, proses konfigurasi memasuki tahap akhir. Tahap Acknowledgement melibatkan pengiriman paket DHCP ACKNOWLEDGEMENT ke klien. Paket ini mencakup durasi sewa dan informasi konfigurasi lainnya yang mungkin diminta oleh klien. Pada titik ini, proses konfigurasi IP selesai.Untuk lab DHCP Client sudah kita praktekan saat kita melakukan konfigurasi dasar untuk terhubung dengan internet.Selanjutnya tahap konfigurasi DHCP Server.

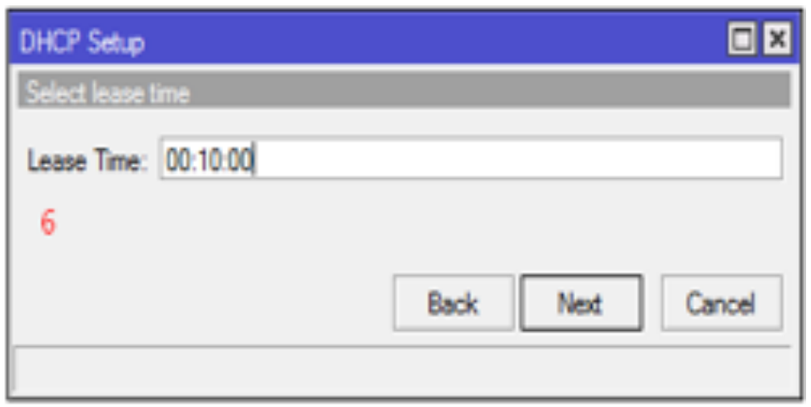
DHCP Server Network Konfigurasi

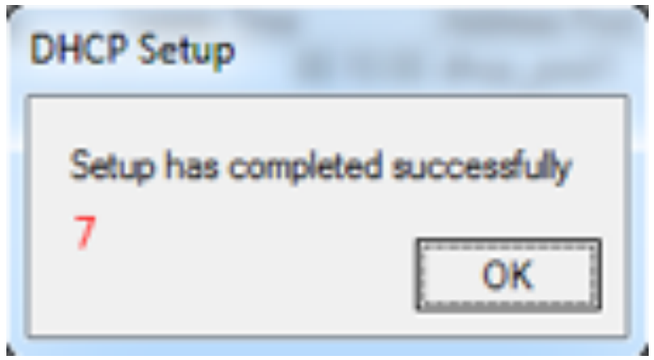
IP => DHCP Server => DHCP Setup





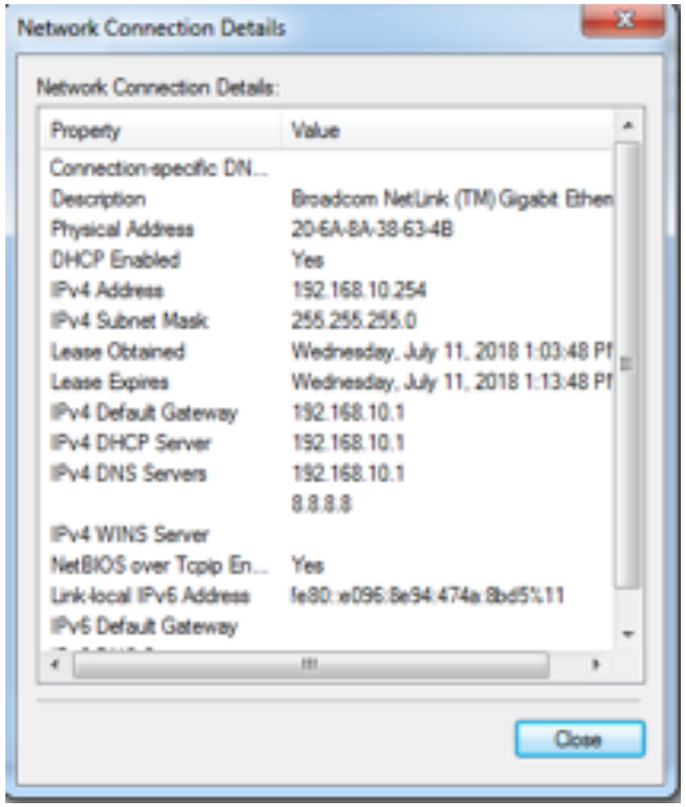






Keterangan:

1. Pilih Interface mana yang akan dijadikan DHCP Server
2. Tentukan network yang akan diberikan kepada klien
3. Pilih Gateway yang akan diberikan pada klien
4. Tentukan IP Pool/range IP yang akan diberikan (Selain IP Router)
5. Tentukan DNS yang akan diberikan dan dipakai oleh klien
6. Tentukan berapa lama waktu yangdiberikan kepada klien dalam menggunakan IP yang dipakai, jika dalam 10 menit perangkat tersebut masih aktif maka lease time akan diper-panjang otomatis, namun jika perangkat tersebut non-aktif maka IP yang dipakai akan diberikan untuk perangkat lain yang memberikan request. Untuk test DHCP Server, silah-kan ubah konfigurasi IP pada laptop anda menjadi dynamic/Otomatis, dan lihat berapa IP yang didapat dari DHCP Server router.

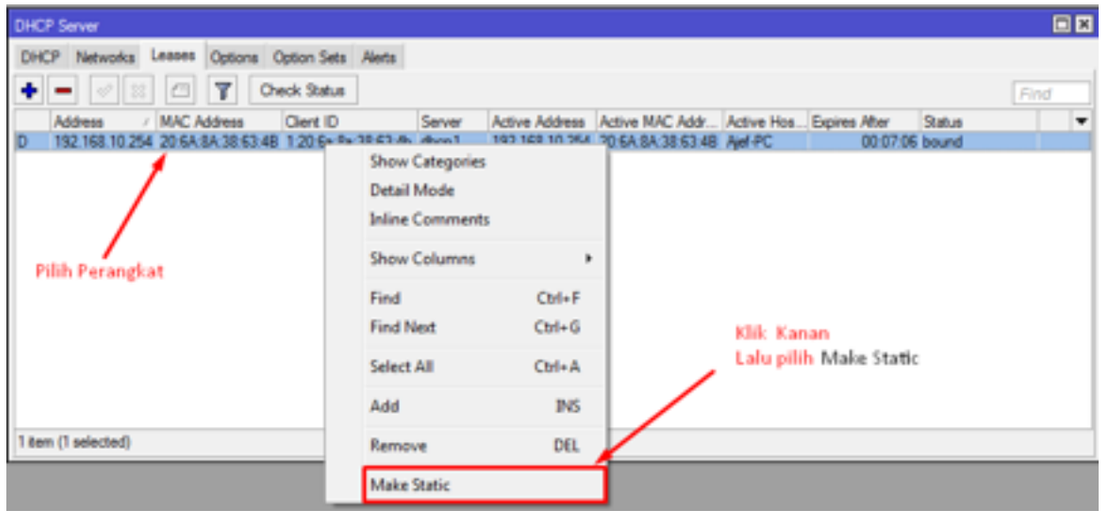


Manajemen Lease

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

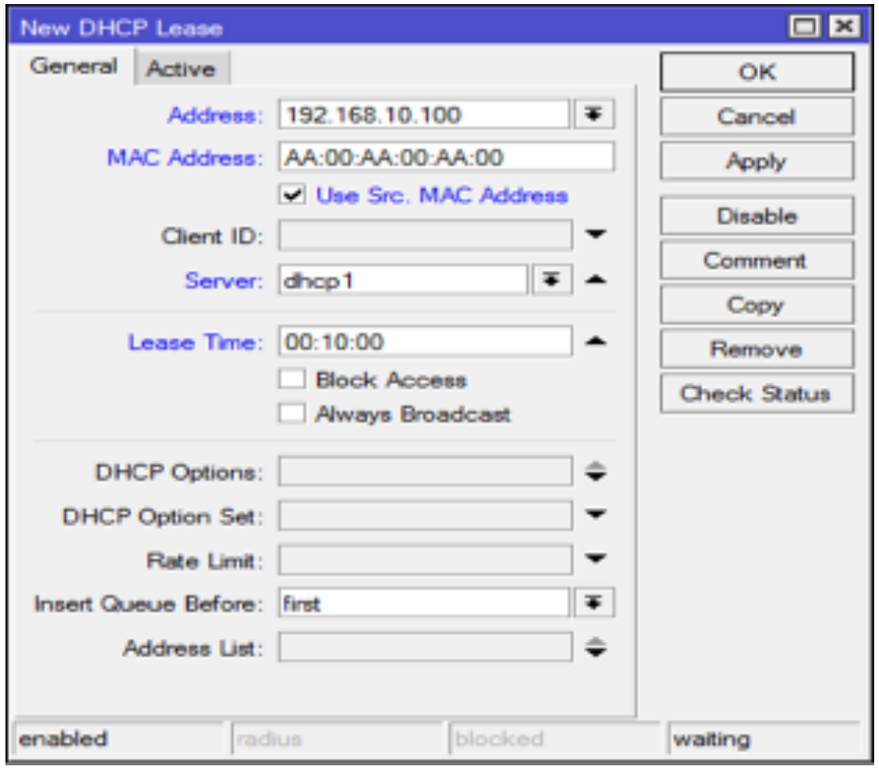
DHCP Server Setup Configuration

IP Pool - > IP DHCP ADD - > IP DHCP NETWORK



Anda juga bisa menambahkan secara manual IP,

IP => DHCP Server => Leases => Add



Manajemen Address Resolution Protocol (ARP)

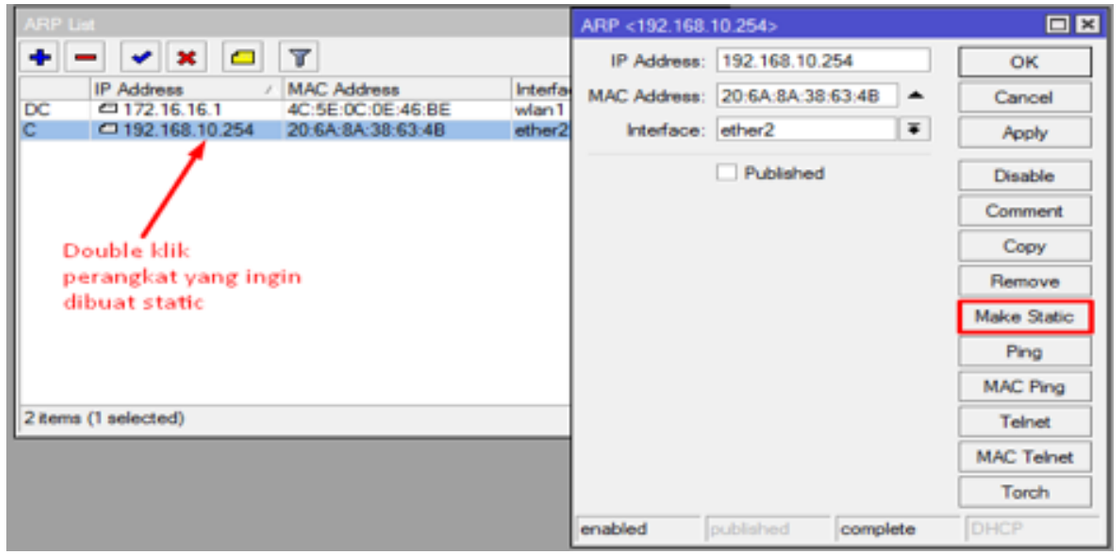
ARP atau Address Resolution Protocol merupakan table yang berisi suatu informasi daftar Alamat user yang terhubung dalam router mikrotik tersebut. Didalam ARP list Terdapat Informasi daftar info Address/ alamat yang terhubung didalam jaringan kita, Seperti IP Address dan Mac Address Client.Maka dari itu kita bisa memanfaatkan fitur ARP untuk keamanan jaringan kita.

Kelemahan ARP jumlah entrinya terbatas hanya sampai 80192 entri sehingga menyebabkan CLient lain tidak bisa terkoneksi.

Berikut Beberapa Fungsi Dari ARP List :

1. Mengetahui Info IP Address dan Mac Address yang mana saja Terhubung
2. Dapat Menstatic (Tetap) IP address yang DHCP (auto)
3. Mencegah DHCP Starvation (Kekurangan IP Address)
4. Mencegah Lolosnya Penetapan Limit Bandwith (Speed Network)
5. Memaksa klient menggunakan protocol DHCP

IP => ARP



Setelah IP address dan Mac Address perangkat tersebut dibuat static, maka perangkat itu tidak bisa lagi mengganti IP Address jika ingin tetap terkoneksi dengan internet, jika IP Address perangkat tersebut diganti atau digunakan pada perangkat lain maka perangkat tersebut tetap tidak akan bisa terkoneksi dengan internet.

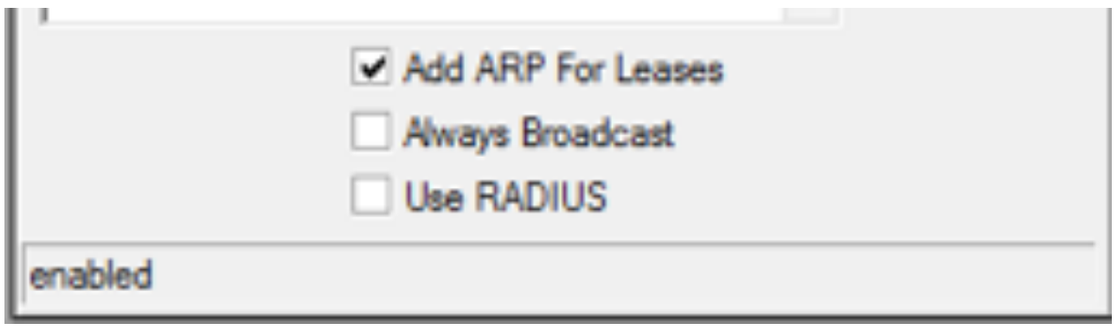
Keterangan :

D = Dynamic berarti IP tersebut bisa digunakan dan diganti orang lain tanpa se izin admin.

C = Complete berarti untuk merubah IP dari perangkat tersebut harus melalui izin admin

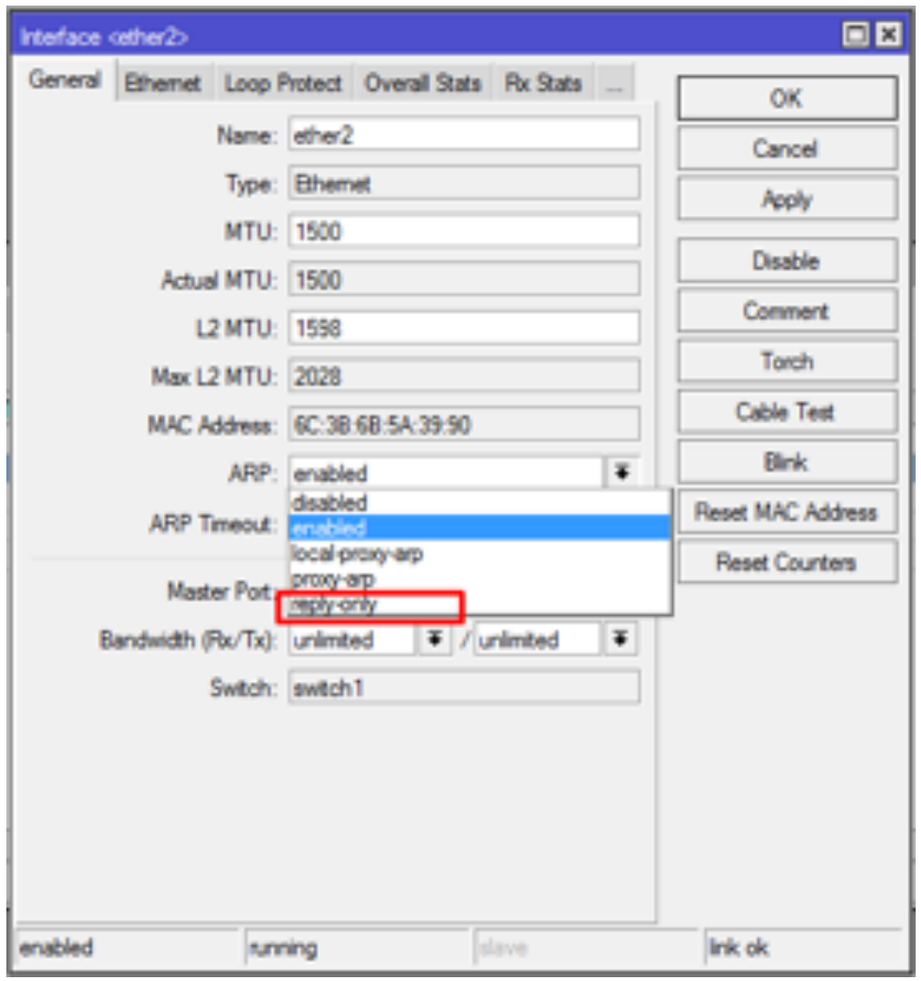
Namun IP Address yang sudah kita buat static akan tetap berjalan pada perangkay lain jika kita mengganti IP Address dari perangkat dengan IP Address yang lain dalam satu network.Jika kita ingin memaksa seluruh IP yang kita static tetap bisa berjalan menerapkan fungsi ARP, maka kita bisa mengkombinasikan fungsi DHCP Server dengan ARP dan memaksa semua client yang ingin terkoneksi dengan internet harus mendapat IP DHCP Server dari router sesuai dengan IP yang sudah dialokasikan.

* Supaya setiap perangkat hanya bisa terkoneksi hanya dengan alokasi IP Address dari DHCP Server kita perlu mengaktifkan opsi 'Add ARP for Leases'. Caranya klik dua kali pada DHCP Server dan centang opsi tersebut yang terletak di bagian bawah.



Selain itu pada interface router dimana DHCP Server berada kita ubah parameter 'ARP' dengan opsi 'reply-only'. Hal ini ditujukan supaya router tidak akan melakukan update secara otomatis pada tabel ARP List ketika ada client yang terkoneksi menggunakan IP Address Static.

Menu Interface=>Ether2 (Ethernet DHCP Server) => ARP (Reply Only)



konfigurasi diatas akan membuat router hanya mengijinkan interkoneksi client yang mendapatkan ip address dari proses

DHCP. User yang melakukan setting ip address manual justru tidak bisa interkoneksi ke router.

Jadi dengan menerapkan ARP Mode REply only dan DHCP Server Add ARP for leases maka client tidak akan bisa terkoneksi ke router selain dengan cara laptop mendapat dhcp client dari router, dan seperti yang sudah dibahas bahwa hal ini mencegah DHCP Starvation.

MikroTik

MTCNA

MikroTik Certified Network Associate Training

BRIDGE

BRIDGE

Merupakan perangkat yang bekerja di layer 2 (DataLink).Dahulu mikrotik digunakan sebagai solusi karena terjadi collision domain dalam pengiriman paket dalam satu hub, maka ditambahkan perangkat bridge agar berfungsi untuk memecah collision domain menjadi 2.Dalam perkembangannya bridge berkembang menjadi multiport bridge atau lebih dikenal dengan nama switch.

Konsep bridge pada mikrotik :

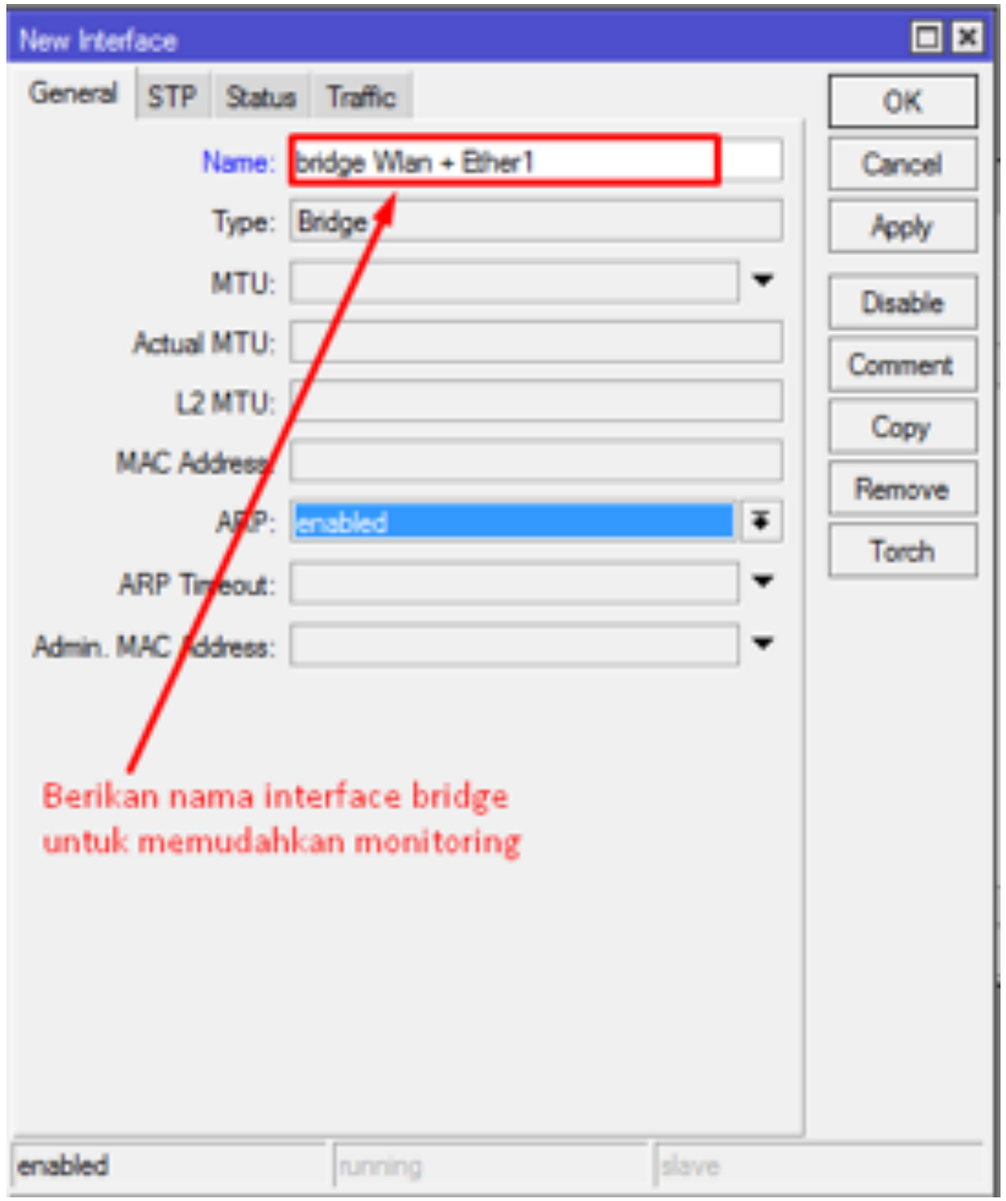
- Menggabungkan 2 atau lebih interface yang bertipe ethernet, wireless, FO, Tunnel atau sejenisnya, seolah-olah berada dalam 1 segmen network yang sama.

- Proses penggabungan ini terjadi pada layer data link.
- Mengaktifkan bridge pada 2 buah interface akan menonaktifkan fungsi routing di antara kedua interface tersebut.
- Mengemulasi mode switch secara software pada dua atau lebih interface.
- Memanfaatkan port-port pada Routerboard untuk menghubungkan perangkat-perangkat jaringan supaya berada dalam satu subnet / bridge network yang sama layaknya seperti Switch.

Untuk Konfigurasi :

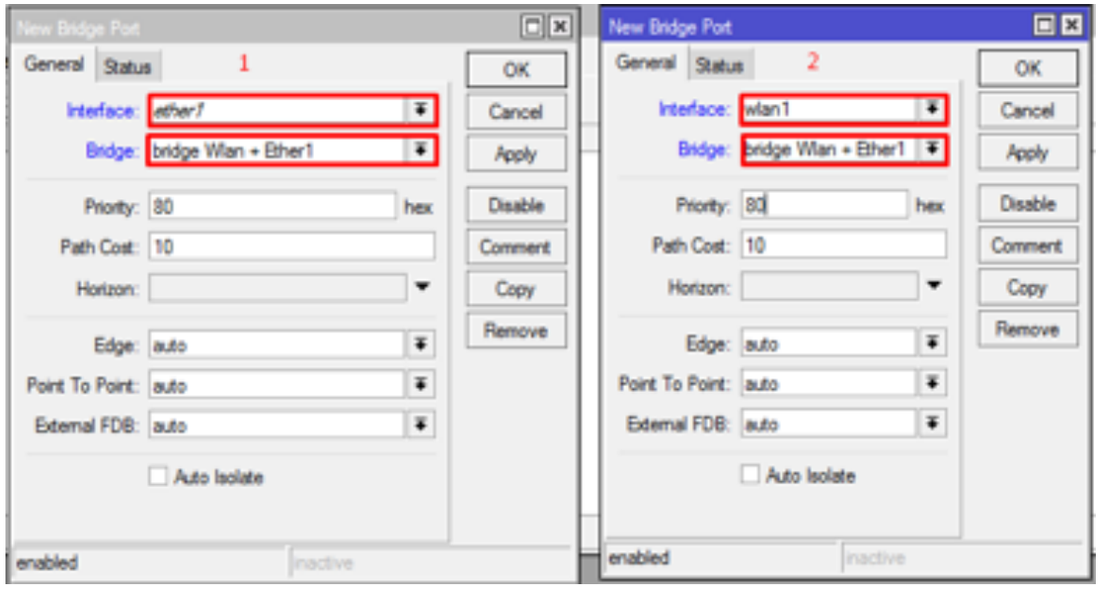
Buat Interface Bridge

Menu => Bridge=> Bridge=> Add



Selanjutnya tambahkan port ke interfaces bridge yang sudah dibuat, yaitu interface Ether1 & Wlan.Untuk port yang ingin ditambahkan bisa berupa Ethernet, wireless, SFP, Tunnel (Syarat dan ketentuan berlaku)

Menu Bridge => Ports => Add



Pastikan interface yang kita bridge merupakan interface yang belum mempunyai konfigurasi IP, dan saat suatu interface kita bridge maka konfigurasi IP dilakukan pada interface bridge yang kita buat.

MikroTik

MTCNA

MikroTik Certified Network Associate Training

ROUTING

ROUTING

Routing adalah proses pengiriman paket dari satu jaringan ke jaringan lainnya dengan memilih jalur terbaik dalam multiple jaringan.

Fungsi routing sudah menjadi satu paket dengan system package routerOS, artinya saat kita menginstall routerOS maka otomatis fungsi routing sudah dapat digunakan.Routing dibedakan menjadi dua yaitu routing statik dan routing dinamis :

- Routing Static, adalah router yang memiliki kabel routing statis yang settingannya diatur oleh administrasi jaringan secara manual.

- Routing Dynamic, adalah router yang membuat tabel routing secara otomatis, dengan membaca lalu lintas jaringan dan tentu juga dengan saling berhubungan dengan router yang lain.

Ada beberapa mekanisme bagaimana router memilih jalur routing yaitu antara lain sebaga berikut :

- Rule routing yang paling spesifik (Misal, 192.168.1.128/26 lebih spesifik dari 192.168.1.1/24).
- Distance (Router akan memilih nilai distance yang paling kecil).
- Round Robin (Random. Apabila Rule tersebut sama-sama spesifik dan memiliki nilai distance yang sama).

Distance

DIstance beripa nilai yang digunakan untuk menentukan jalur routing mana yang menjadi prioritas dan yang menjadi sebuah jalur backup. Secara default nilai distance pada MikroTik dari 0 (Nol) - 8 (Delapan). Semakin kecil nilai distance maka rule tersebut akan semakin diprioritaskan.

Check Gateway

Digunakan untuk Mekanisme pengecekan gateway menggunakan ARP Request atau Test Ping yang akan dikirimakan setiap 10 detik. Sebuah link akan dianggap sebagai "Gateway Time-Out" apabila tidak menerima respon selama kurang lebih 10 detik dari mesin gateway. Dan akan dianggap "Unreachable" jika terjadi 2 kali gateway time-out secara berurutan.

Scope & Target Scope

Digunakan untuk melakukan pengecekan koneksi yang berada diatas router gateway atau yang tidak terhubung langsung (recursive).Secara default router akan memberikan niali dari scope dan target scope untuk masing-masing type routing yang nilainya juga berbeda.Untuk penerapan dan pembahasan lebih lanjut nanti akan dibahas pada materi MTCRE.

Parameter Routing Type

Selain fungsi-fungsi diatas, ada lagi sebuah fungsi routing yang bisa digunakan untuk kebutuhan keamanan jaringan. Kita bisa mengaturnya pada pamarameter Type.

Pada parameter tersebut kita bisa melihat beberapa macam opsi. Untuk fungsi keamanan jaringan kita bisa memilih beberapa parameter berikut:

- Blackhole (Melakukan blocking secara diam-diam).
- Prohibit (Melakukan blocking dan mengirimkan pesan error ICMP "Administratively prohibited atau Packet filtered "
- Unreachable (Melakukan blocking dan mengirimkan pesan error ICMP "Host Unreachable".

Artinya, apabila kita menggunakan ketiga parameter diatas, kita tidak memerlukan untuk mendefinisikan gateway. Misal,

jika kita ingin melakukan blocking IP address tujuan tertentu, maka kita hanya mengisi parameter "Dst. Address" dan kita tentukan parameter "type".Sebagai contoh kita akan melakukan blocking koneksi ke tujuan IP Address 192.168.1.2 dengan type "Prohibit". Sehingga perangkat dengan IP Address tersebut tidak dapat diakses oleh perangkat lain di jaringan lokal kita.

Route Flags

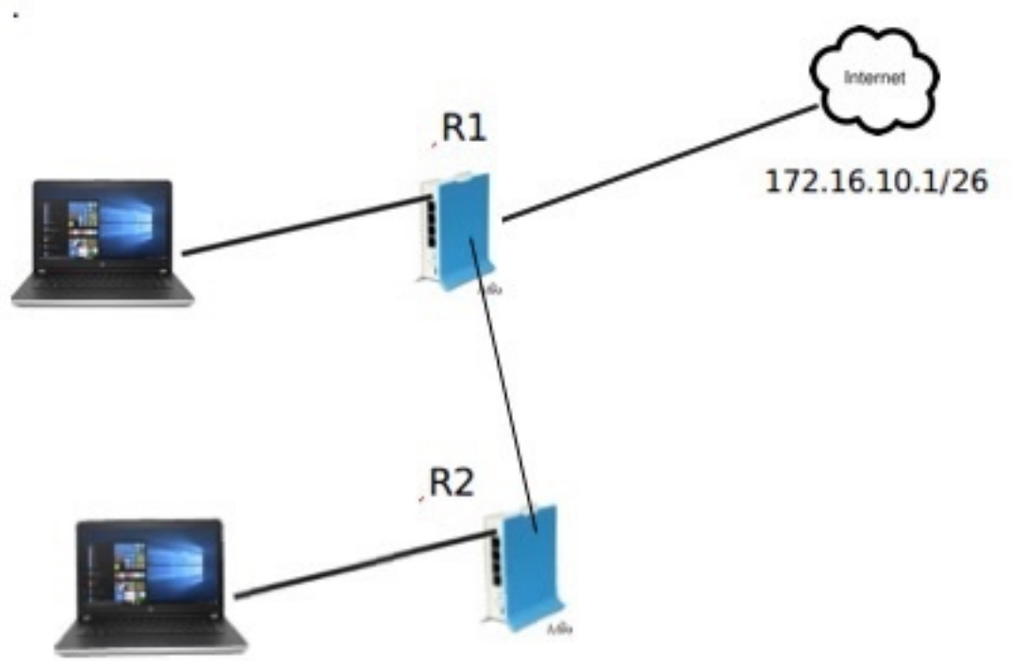
Flags pada routing menunjukan status routing yang kita buat baik itu routing static maupun routing dinamic.Ada beberapa Flags pada routing yang perlu diketahui :

```
[ admin@MikroTik ] > ip route print
Flags: X - disabled, A - active, D - dynami
C - connect, S - static, r - rip, b - bgp,
B - blackhole, U - unreachable, P - prohibi
#  DST-ADDRESS  PREF-SRC
0  ADC 10.10.10.0/24  10.10.10.100
1  ADC 172.16.10.0/29  172.16.10.2
[ admin@MikroTik ] >
```

X Disabled, **A** Active, **D** Dynamic, **C** Connect, **S** Static, **r** Rip, **b** Bgp, **o** Ospf, **B** Blackhole, **U** Unreachable, **P** Prohibit

Routing Static

Pada lab routing statik, kita akan menghubungkan klien yang berada pada 2 router untuk dapat saling berkomunikasi.



Konfigurasi R1 :

Ether1 = 172.16.10.2/26

Ether2 = 192.168.11.1/24

Ether3 = 10.10.10.1/30

Konfigurasi R2 :

Ether1 = 10.10.10.2/30

Ether2 = 192.168.12.1/24

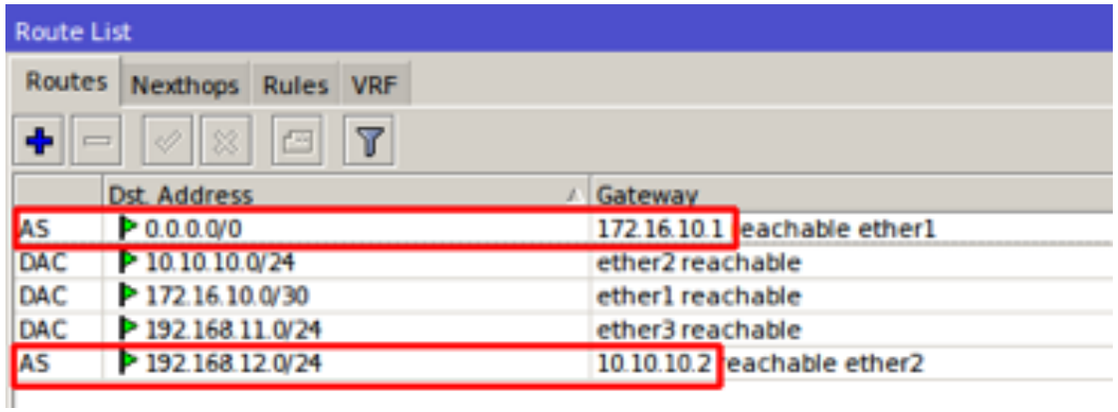
Untuk menambahkan routing :

IP Route Add

Routing R1 :

Dst-Nat 192.168.12.0/24 Gateway 10.10.10.2

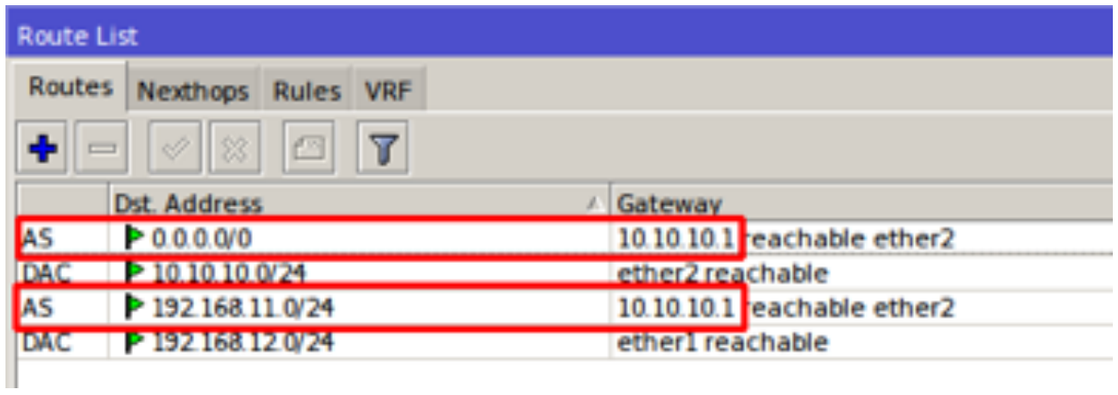
Dst-nat 0.0.0.0/0 Gateway 172.16.10.1



Routing R2 :

Dst-Nat 192.168.11.0/24 Gateway 10.10.10.1

Dst-nat 0.0.0.0/0 Gateway 10.10.10.1



Untuk pengujian silahkan lakukan ping antar klien, seharusnya kedua klien sudah bisa berkomunikasi.Dan lakukan ping ke internet melalui klien R2 pastikan bisa terkoneksi ke internet.

Selain menggunakan topologi diatas, static routing 2 router juga bisa dilakukan dengan perantara wireless, namun secara konfigurasi tetap sama.

MikroTik

MTCNA

MikroTik Certified Network Associate Training

WIRELESS

WIRELESS

Dalam membangun jaringan wireless, salah satu hal paling dasar dan harus dipahami adalah menguasai spesifikasi dari peralatan Wifi yang hendak digunakan. Biasanya pada daftar spesifikasi dari peralatan wireless wifi akan tercantum kode IEEE 802.11 a/b/g/n/ac. Kelima kode huruf di belakang kode IEEE 802.11 tersebut menandakan spesifikasi yang berbeda-beda. Dan yang merupakan teknologi paling baru adalah IEEE 802.11 ac.

Berikut adalah daftar data rate dan frekuensi yang dimiliki oleh masing-masing kode IEEE 802.11:

1. IEEE 802.11 - b Wireless Lan yang menggunakan Frequency 2.4Ghz berkecepatan transfer data 11 Mbps
2. IEEE 802.11 - b/g Wireless Lan yang menggunakan Frequency 2.4Ghz berkecepatan transfer data 54 Mbps
3. IEEE 802.11 - b/g/n Wireless Lan yang menggunakan Frequency 2.4Ghz berkecepatan transfer data 100 – 500 Mbps
4. IEEE 802.11 - a Wireless Lan yang menggunakan Frequency 5 Ghz berkecepatan transfer data 54Mbps
5. IEEE 802.11 – ac Wireless Lan yang menggunakan Frequency 5 Ghz berkecepatan transfer data 1300 Mbps atau 1.3 Gb

Band

Memilih band merupakan cara untuk menentukan standart protokol yang akan digunakan oleh wireless interface. Selain menentukan standart protokol, band juga menentukan data rates yang bisa dilewatkan, channel frequencies dan lebar channel. Ada beberapa band di router mikrotik.

- 2Ghz-b, bekerja di frekuensi 2,4Ghz. Menggunakan protokol 802.11b dengan data rate maksimum 11 Mbit/s.
- 2Ghz-b/g, juga bekerja di frekuensi 2,4Ghz. Menggunakan protokol 802.11b dan 802.11g. protokol 802.11g hampir sama seperti 802.11b akan tetapi melakukan transmisi dengan basis OFDM seperti 802.11a sehingga protokol 802.11g bisa mencapai 54 Mbit/s.

- 2Ghz-b/g/n, bekerja di frekuensi 2,4Ghz. Menggunakan protokol 802.11b, 802.11g dan 802.11n. secara teori maksimal data rate yang bisa dicapai adalah 300 Mbit/s.
- 2Ghz-only G, bekerja di frekuensi 2,4Ghz, hanya menggunakan protokol 802.11g.
- 2Ghz-only N, bekerja di frekuensi 2,4Ghz, hanya menggunakan protokol 802.11n.
- 5Ghz-a, bekerja di frekuensi 5 Ghz. Menggunakan protokol 802.11a, maximum data rate yang bisa dicapai adalah 54 Mbit/s.
- 5Ghz-a/n, bekerja di frekuensi 5 Ghz. Menggunakan protokol 802.11a dan 802.11n.
- 5Ghz-only N, bekerja di frekuensi 5 Ghz dan hanya menggunakan protokol 802.11n.

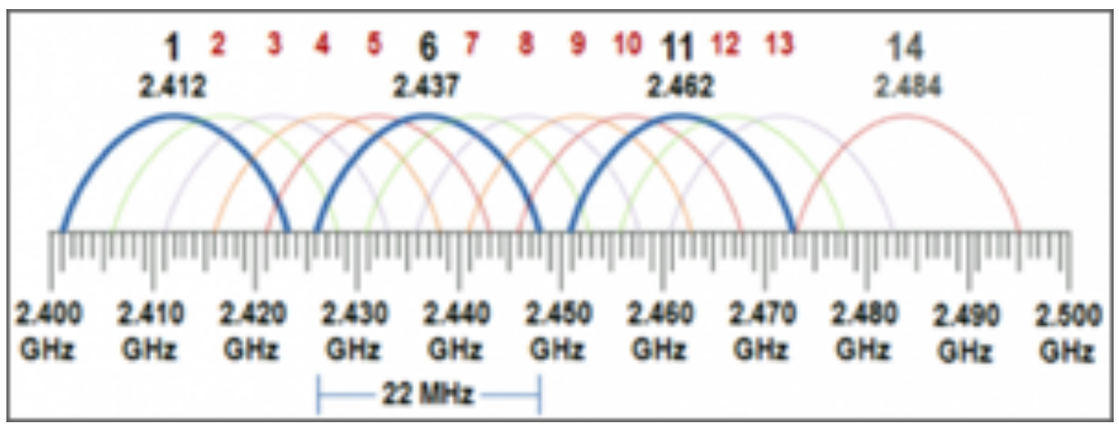
Jika kita perhatikan, ada beberapa pilihan band yang menggunakan lebih dari satu protokol. Jika kita setting sebuah interface wireless dengan band yang menggunakan lebih dari satu protokol, maka interface wireless tersebut memberikan pilihan kepada client, protokol mana yang support dengan perangkat client tersebut.

Frekuensi

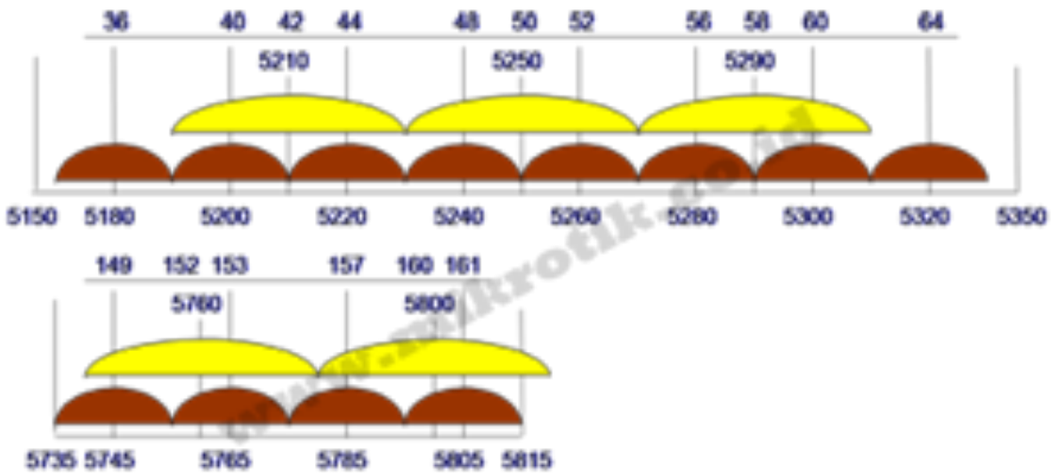
Wireless LAN menggunakan radio frekuensi yang membutuhkan media rambat yang juga harus bersih atau tanpa gangguan. Gangguan bisa berupa halangan seperti pohon,gedung,tembok,kaca atau interferensi frekuensi dari perangkat lain di sekitarnya.

Agar terbentuk link wireless yang bagus, gangguan ini harus dihindari. hal pertama yang harus dilakukan dilakukan adalah site survey terlebih dahulu untuk mengetahui kondisi lapangan secara fisik maupun penggunaan frekuensi yang sudah ada. Misalnya, adanya halangan berupa bukit, gedung, pohon, tembok, kaca dsb yang harus dihindari. Kita harus mengetahui juga frekuensi - frekuensi yang ada disekitar. jadi nantinya bisa dihindari penggunaanya agar tidak interferensi/overlapping.

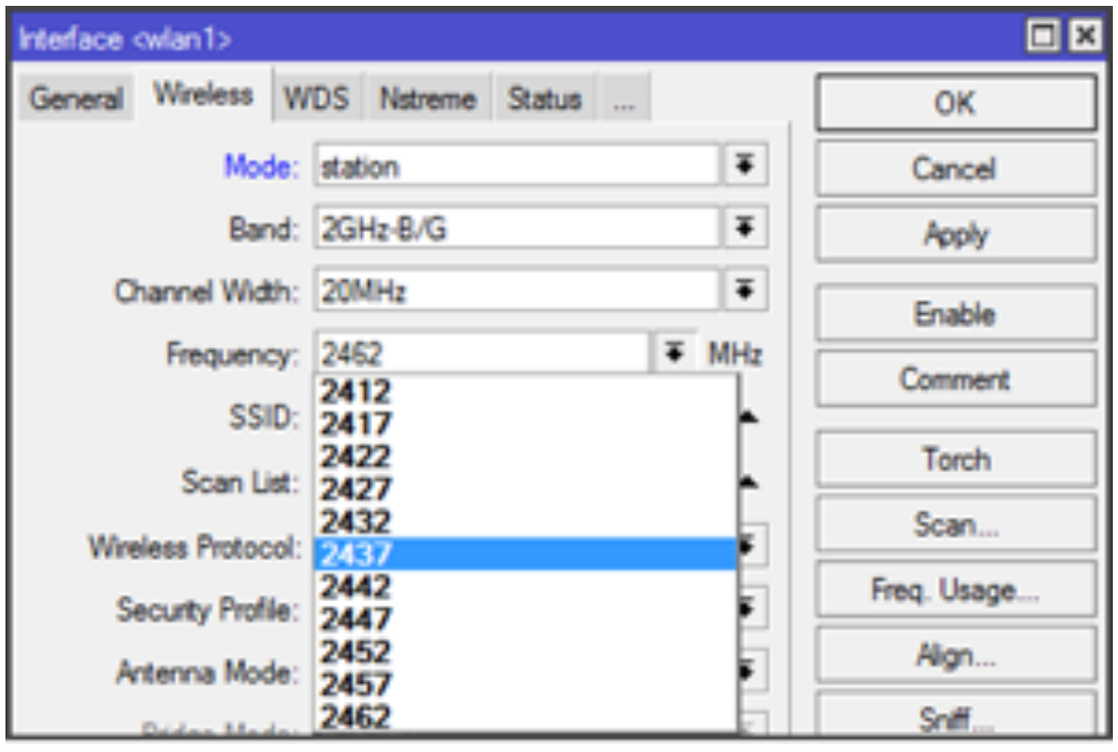
Alokasi frekuensi sudah diatur dalam regulasi di setiap wilayah dan negara. Di Indonesia, untuk keperluan wireless LAN sudah dalokasikan dalam ISM Band pada frekuensi 2,4GHz dan 5,8GHz. Lebih detail nya, untuk 2,4GHz dibagi dalam beberapa channel dengan lebar channel masing - masing 22MHz.



Begitu juga dengan yang 5GHz. Frekuensi 5Ghz juga dibagi menjadi beberapa channel.



Di mikrotik, tiap channel ditampilkan dengan nilai tengah frekuensi-nya. Misal pada band 2,4GHz, channel1 = 2412 ,dsb.



Kebanyakan perangkat seperti laptop, gadget sebelumnya memang hanya support untuk 2,4GHz saja. Akan tetapi beberapa gadget saat ini sudah support 5GHz. Begitu juga untuk link perangkat wireless LAN saat ini juga sudah banyak yang beralih ke 5GHz. Berbeda dengan pembagian channel pada 2,4GHz, pembagian channel pada 5GHz tidak ada yang saling overlapping. Untuk mengcover laptop atau gadget, bisa gunakan frek 5725 - 5785 MHz. Kebanyakan gadget saat ini support di frekuensi tersebut. Produk Mikrotik juga sudah support baik untuk band 2,4GHz atau 5GHz. Support juga untuk custom freq dan custom channel width. Tapi sekali lagi, gunakan frekuensi dengan bijak. Jangan menyalahi regulasi

Wireless Manajemen Tool

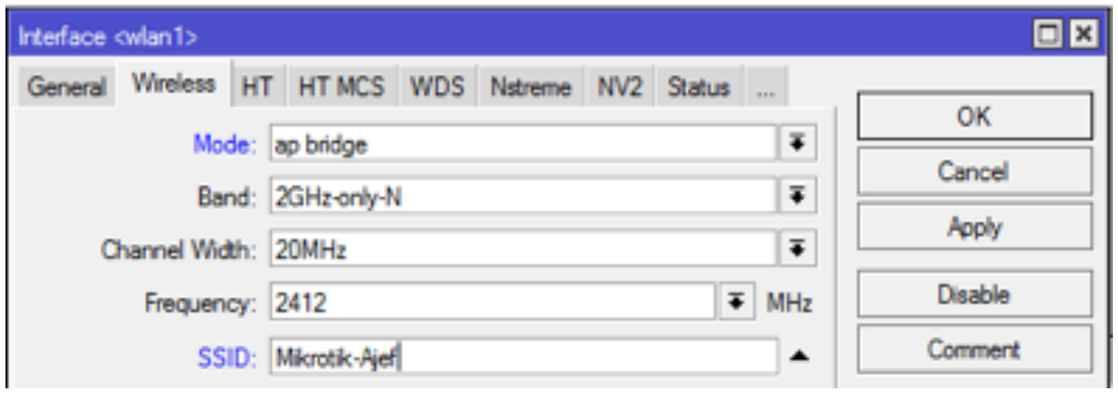
Didalam menu wireless MikroTik terdapat berbagai macam tool-tool yang digunakan untuk mendukung kinerja dari fitur wireless. Dan disini kita akan membahas beberapa wireless tools diantaranya yaitu Access List (AP) dan Connect list (Station). Kedua tool tersebut merupakan bagian dari manajemen wireless, dimana kita bisa membuat kebijakan interkoneksi jaringan wireless sesuai dengan parameter yang kita buat. Dengan demikian kita dapat meminimalisir akan miss-connection terutama dari perangkat client yang akan terkoneksi ke AP (Access Point). Selain itu, dengan tool ini kita dapat melakukan pembatasan (filtering) terhadap koneksi dari perangkat AP maupun client.

Contoh implementasi, misalnya pada sebuah jaringan, admin jaringan ingin membuat kebijakan hanya Client Adan Client B yang boleh terkoneksi, sedangkan client lain tidak dapat terkoneksi.

Access List (AP)

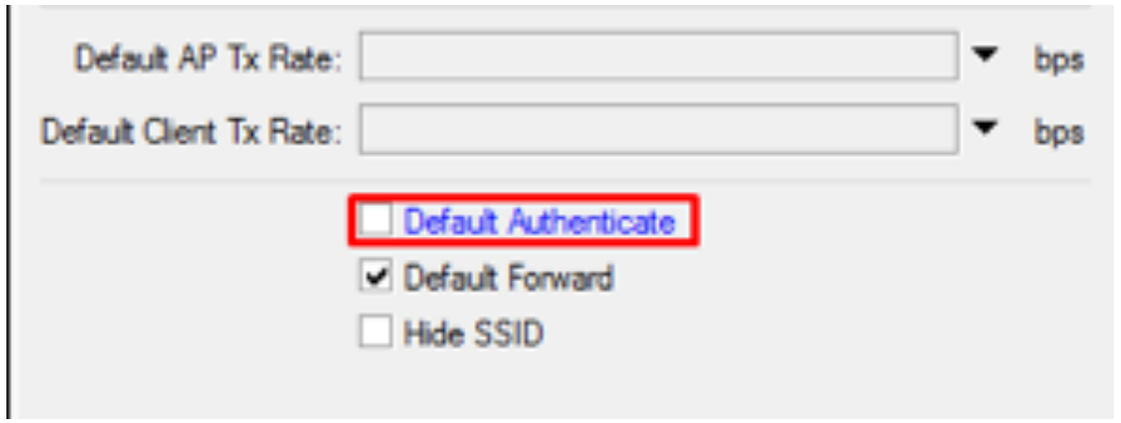
Access List merupakan sebuah tool yang digunakan di sisi AP (Access Point) untuk melakukan filtering koneksi dari client. Sehingga AP dapat menentukan client mana saja yang bisa terkoneksi berdasarkan MAC Address.

Untuk langkah-langkah konfigurasi dasar, pertama setting terlebih dahulu interface wireless sebagai access point.



Dengan setting diatas, interface wireless akan berkerja sebagai access point dengan SSID "Mikrotik-Ajef". Selanjutnya kita akan melakukan management terhadap interkoneksi client agar bisa terkoneksi berdasarkan mac-address. dengan kata lain, client bisa terkoneksi jika mac-address sudah terdaftar. Bagi mac-address yang belum terdaftar, tidak dapat terkoneksi. Disini, kita akan menggunakan fitur Access List, atau kadang dikenal dengan sebutan ACL.

Agar router menggunakan kebijakan (policy) yang dibuat di access-list, maka kita setting default-policy interface wireless terlebih dahulu. Double klik interface wireless, kemudian masuk ke tab "Wireless".



Karena hanya mac-address yang terdaftar di access list yang boleh terkoneksi, maka hilangkan centang pada opsi "Default Authenticate" pada properties interface wireless. Dengan begitu, ketika ada client wireless yang hendak terkoneksi, router tidak akan langsung mengijinkan client tadi interkoneksi, namun router akan melihat kedalam tabel access-list untuk mengecek apakah ada kebijakan yang diterapkan untuk client tadi.

Sedangkan "Default Foward" untuk menentukan kebijakan apakah antar client wireless akan diijinkan untuk saing interkoneksi atau tidak. Terkadang untuk alasan security admin perlu mematikan opsi default-foward. Misal untuk menangkal NetCut, netcut berkerja dengan menyerang perangkat client lain yang sudah terkoneksi, dengan mematikan opsi default-foward, netcut tidak akan bisa menyerang client lain yang masih dalam 1 AP.

Di dalam access-list, kebijakan (policy) dibuat berdasarkan

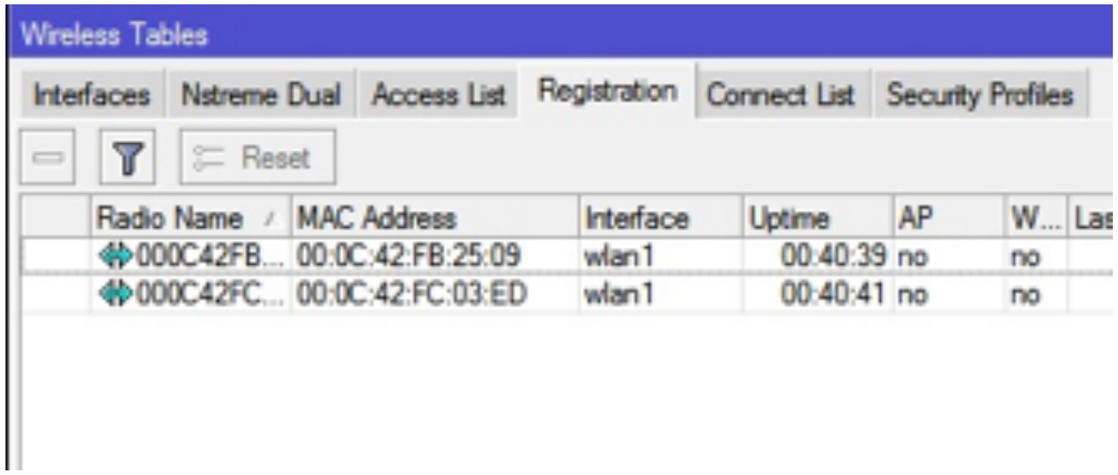
mac-address client. Untuk membuat kebijakan tersebut, klik menu Wireless -> Access List -> kemudian akan muncul tampilan seperti berikut.

Tentukan MAC Address client yang diizinkan untuk terkoneksi (misal, jika diimplementasikan pada topologi diatas, maka kita masukkan MAC Address dari client A dan client B). pada properties access-list ini, admin jaringan juga bisa membuat kebijakan dengan menentukan beberapa parameter.

- Interface : Di interface mana access-list ini berlaku. Jika misalnya ada beberapa interface yang berjalan sebagai access point. Jika dipilih "all" maka akan berlaku di semua interface.
- Signal Strength Range : Range signal client yang diijinkan untuk terkoneksi. Contoh kasus misalnya signal client yang buruk, akan menganggu client lain yang sudah terkoneksi karena interface wireless akan mencoba mencari modulasi terbaik untuk client tersebut agar bisa mendapatkan signal yang bagus. Admin bisa membuat kebijakan agar hanya client yang mendapatkan signal yang bagus yang bisa terkoneksi sehingga wireless bisa lebih stabil.
- AP Tx Limit : Membatasi throughput wireless ketika access-point mengirim data ke client.
- Client Tx limit : Membatasi throughtput client ketika transmit ke access point.
- Authentication : Menentukan kebijakan apakah client boleh terkoneksi ke access point atau tidak.
- Fowarding : Menentukan kebijakan apakah antar client wireless bisa interkoneksi atau tidak.
- Private key, Pre-Shared Key, dan Management Protection Key : Menentukan security key yang hanya berlaku untuk client tersebut. Dikombinasikan dengan fitur wireless security.
- Time : Untuk menentukan kapan rule access-list tadi dijalankan. Admin jaringan bisa membuat kebijakan kapan

user bisa terkoneksi dengan access point, dan kapan akan diputus dari access-point.

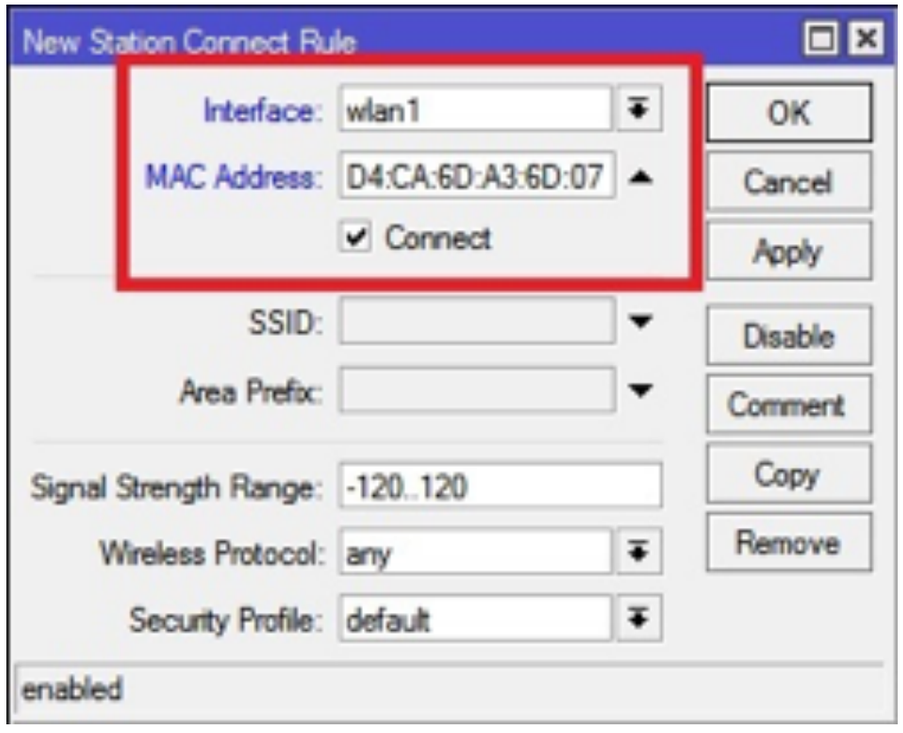
Terakhir cek di tabel "Registration" pada menu Wireless untuk melihat client yang sudah terkoneksi dengan interface wireless



Connect List (Station / Client)

Connect List merupakan tool yang memiliki fungsi kebalikan dari Access List, yaitu digunakan disisi wireless client (station) untuk membatasi (filtering) koneksi terhadap AP (Access Point). Sehingga client dapat menentukan AP (Access Point) mana wireless client akan terkoneksi berdasarkan Mac Address access point. Sehingga wireless client tidak akan berpindah ke access point lain, walaupun access point tersebut memiliki SSID yang sama. Namun dengan catatan Default Authenticate di non-aktifkan Untuk langkah-langkah konfigurasi dasar, setting terlebih dahulu interface wireless sebagai wireless client.

Selanjutnya untuk menentukan policy disisi wireless client, klik menu Wireless -> Connect List -> kemudian akan muncul tampilan seperti berikut.



Tentukan interface untuk koneksi ke AP, kemudian isikan MAC Address dari AP yang akan terkoneksi. Kemudian Klik OK. (Untuk topologi diatas, maka hal ini dilakukan pada masing-masing client, yaitu client A dan client B). Disini kita juga bisa menentukan beberapa parameter misalnya Signal Strength Range, Wireless Protokol yang digunakan, dll. Fungsi access list ini juga bisa digunakan untuk mencegah wireless client terkoneksi ke access point dengan mac-address tertentu, dengan cara menghilangkan centang pada parameter "Connect"

Baik menggunakan Access List maupun Connect List, kita dapat melihat client mana atau AP mana yang sedang terkoneksi pada Tab Registration.

Jadi kesimpulannya adalah agar koneksi wireless lebih aman dan stabil, baik Access Point maupun Client, kita dapat memanfaatkan wireless tool dari MikroTik yaitu Access List dan Connect List.

MikroTik

MTCNA

MikroTik Certified Network Associate Training

FIREWALL

FIREWALL

Pada routerOS mikrotik terdapat sebuah fitur yang disebut dengan FIREWALL.Fitur ini biasanya banyak digunakan untuk melakukan filtering (Filter Rule) dan Forwarding (NAT), Dan juga untuk menandai koneksi maupun paket dari trafik data yang melewati router(Mangle).Supaya fungsi firewall ini dapat berjalan dengan baik, kita harus menambahkan rule yang sesuai.

Terdapat sebuah parameter utama pada rulefitur firewall ini yaitu “Chain”.Parameter ini memiliki kegunaan untuk menentukan jenis trafik yang akan di manage pada fitur firewal, dan setiap fungsi pada firewall seperti Filter Rule, NAT, Mangle memiliki opsi chain yang berbeda.

FIREWALL Filter Rules

Filter Rule biasanya digunakan untuk melakukan kebijakan boleh atau tidaknya sebuah trafik ada dalam sebuah jaringan.Pada Filter Rule terdapat tiga buah chain yaitu Input, Output, dan Forward.Adapun fungsi dari masing-masing chain tersebut :

Input

Digunakan untuk memproses trafik paket data yang masuk atau menuju ke router melalui interface yang ada di router.Jenis trafik paket data yang masuk bisa berasal dari jaringan publik maupun jarigan lokal dengan tujuan router.Contohnya, mengakses router menggunakan winbox, webfig, telnet, ssh baik dari lokal mapun public, Melakukan Ping ke Router.

Output

Digunakan untuk memprose trafik atau paket data yang keluar atau berasal dari router.Trafik yang berasal dari router bisa menuju jaringan publik atau lokal LAN router itu sendiri.Contohnya kita melakukan ping ke google atau new terminal di winbox.

Forward

Digunakan untuk memproses trafik atau paket data yang hanya melewati router, jadi ip source maupun destination bukanlah berasal dari router.Misalnya saat kita melakukan browsing, request berasal dari laptop yang melakukan browsing dan tujuannya adalah internet.

CONNETION TRACKING DAN CONNECTION STATE

Selain parameter chain, terdapat paramete yang juga penting untuk dimanfaatkan, yaitu connection tracking.Connection tracking merupakan fitur yang digunakan untuk melihat informasi dan status paket yang melewati router, masuk router, maupun keluar router seperti dst-address dan src-address yang sedang digunakan.Untuk membuat rule connection tracking kita menggunakan connection state, beberapa status dalam connection state :

New : Merupakan paket pembuka sebuah koneksi/paket pertama dari sebuah koneksi

Established : Merupakan paket kelanjutan dari paket dengan status new.

Related : Paket yang memulai koneksi baru namun masih berhubungan dengan paket Sebelumnya

Invalid : Paket yang tidak memiliki koneksi apapun.

FIREWALL ACTION

Pada menu action, kita bisa memutuskan atau menentukan suatu trafik atau paket data tersebut di perbolehkan (Accept), di larang (Drop) atau kebijakan lainnya.Terdapat beberapa action yang bisa dipilih :

Accept : Paket diterima dan tidak melanjutkan membaca baris berikutnya

Drop : Menolak paket secara diam-diam (Tidak mengirimkan pesan penolakan ICMP)

Reject : Menolak paket namun tetap mengirimkan pesan penolakan ICMP

Jump: Melompat ke chain lain yang ditentukan oleh nilai parameter jump-target

Tarpit: Menolak tapi tetap menjaga TCP Connection yang masuk (Tetap membalas namun tidak sampai pada tujuan)

Passtrough : Mengabaikan rule ini dan menuju rule selanjutnya

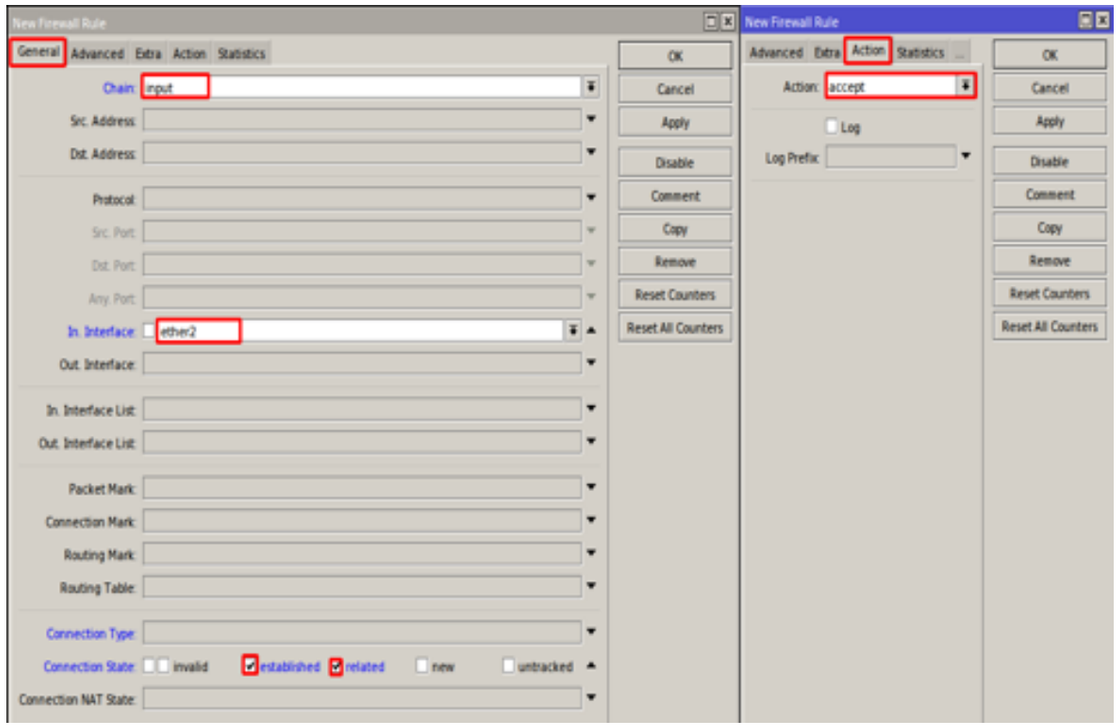
Log : Menambahkan informasi paket data ke log

Dalam menerapkan firewall Filter Rules ada dua skenario atau strategi yang bisa kita gunakan, yaitu “drop all allow some” artinya tutup semua port dan semua akses ke router dan izinkan beberapa sesuai yang kita definisikan atau “allow all drop some” artinya semua port dan akses ke router diizinkan lalu tutup beberapa port yang tidak diperlukan.

Untuk contoh penerapan kita akan menggunakan skenario “drop all accept some” :

Buka menu IP => Firewall => Filter Rules => Add

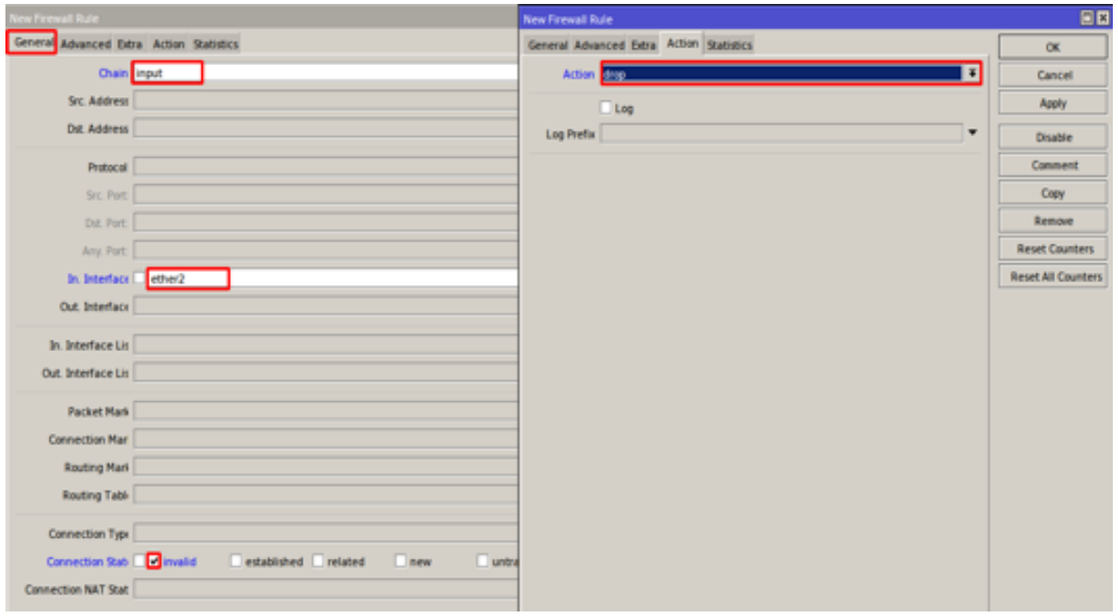
Pada parameter General, chain kita gunakan input karena paket atau request berasal dari lan menuju router, selanjutnya kita perlu menentukan interface mana rule yang kita buat akan berjalan atau bekerja karena jika tidak ditentukan maka defaultnya rule yang kita buat berlaku pada semua interface, lalu status paket (Connection State) kita pilih Edtablished dan Related dan terakhir pada parameter action kita pilih accept.Artinya rule yang kita buat berfungsi untuk mengizinakan jika ada paket yang masuk melalui interface ether2 (Ether yang ditentukan) dengan status paket established related.



Buka menu IP => Firewall => FIlter Rules => Add

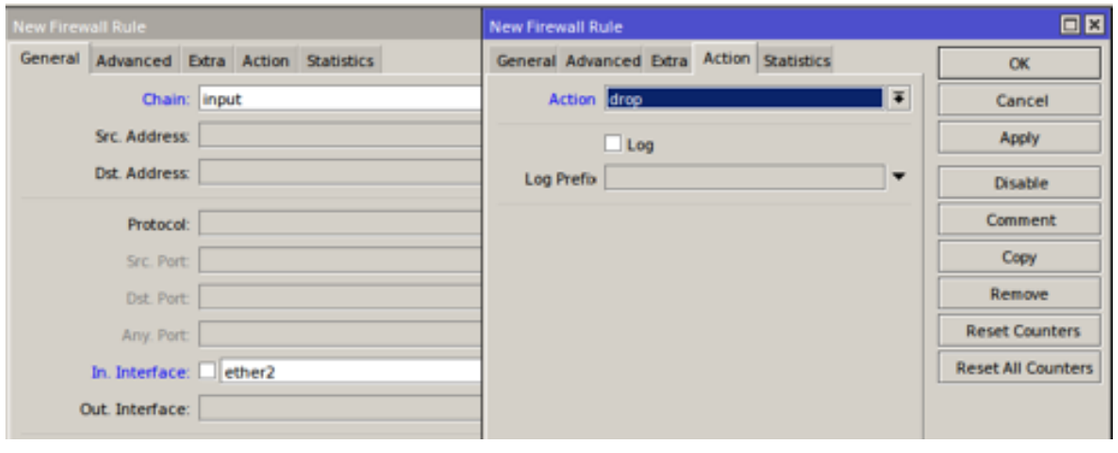
Selanjutnya kita buat rule yang kedua yang difungsikan untuk menolak paket yang statusnya invalid untuk melewati router.Sama seperti langkah diatas dengan chain input, pada

interface dari LAN, dengan connection state “Invalid” maka action kita gunakan DROP



Buka menu IP => Firewall => Filter Rules => Add

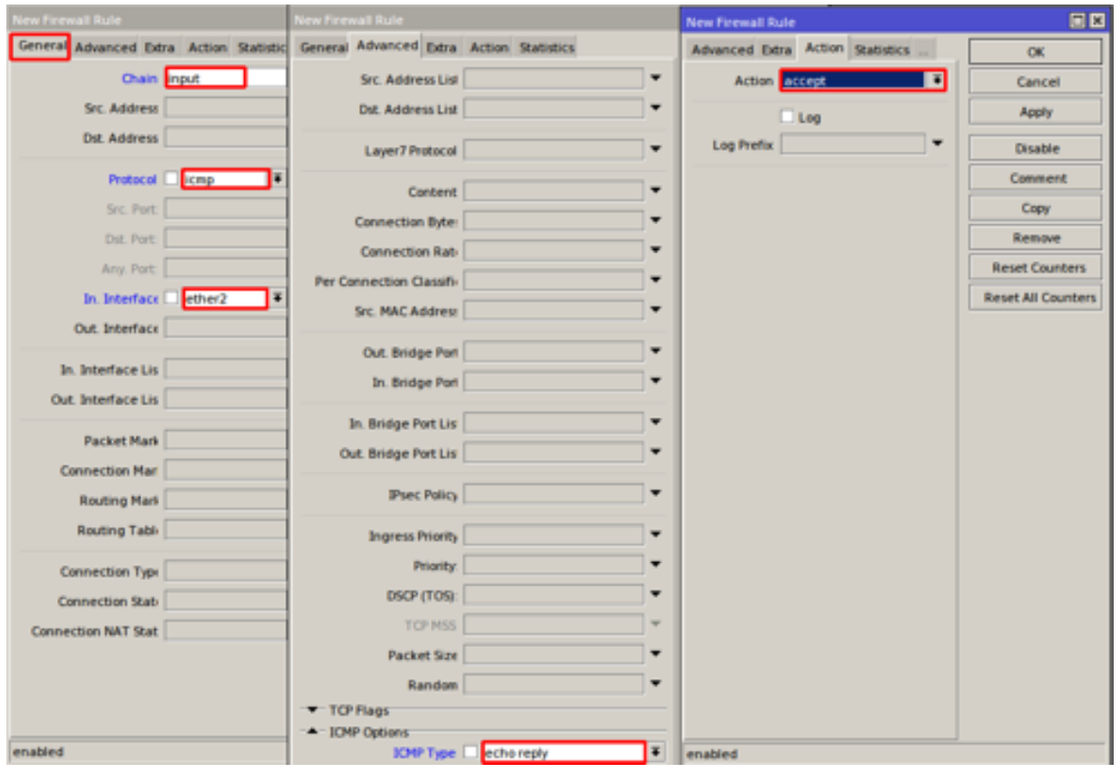
Selanjutnya untuk rule ketiga kita tutup semua request dan akses dari ether2 menuju router agar router dapat membaca rule yang kita buat pada tahap 1 dan 2 diatas.



Seharusnya pada tahap ini Client tidak bisa lagi melakukan akses maupun ping ke router dengan IP Address, jika tadi anda login winbox menggunakan IP winbox sekarang anda akses router menggunakan mac winbox.

Buka menu IP => Firewall => Filter Rules => Add

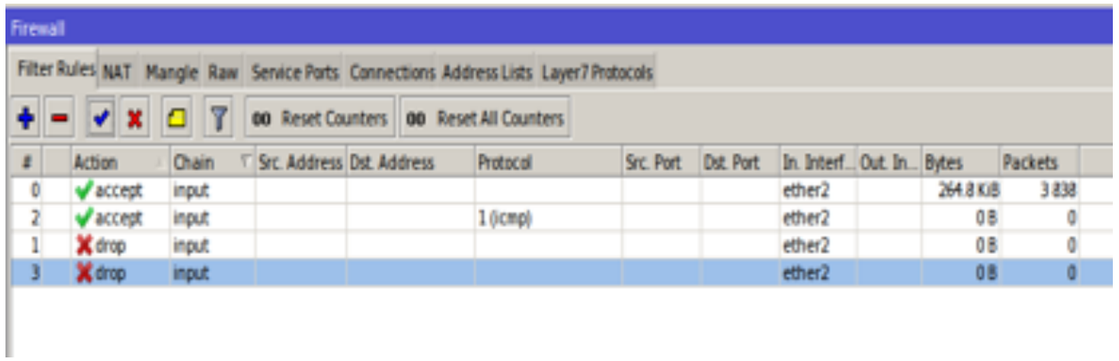
Selain rule diatas kita juga bisa menerapkan aturan-aturan yang ingin kita buat sendiri, misalnya semua koneksi dari LAN sudah kita DROP supaya rule router membaca rule diatasnya,



namun kita ingin agar client tetap bisa melakukan ping ke router tapi tidak untuk lainnya.Pada tab general kita gunakan chain Input, lalu kita tentukan protokolnya ICMP, dan juga tentukan interfaceny, kemudian pada tab Advanced kita pilih

ICMP type = Echo Replay, dan terakhir action kita pilih accept.

Selanjutnya setelah kita membuat rule yang keempat kita sudah bisa melakukan ping ke router, namun karena urutan rule pada tabel firewall itu berpengaruh maka rule terakhir yang kita buat kita naikan diatas rule yang digunakan untuk menolak semua akses ke router (Rule 2), karena pada prinsip kerjanya firewall akan membaca tabel dari rule yang paling atas. Jadi seharusnya urutan rule yang benar adalah :

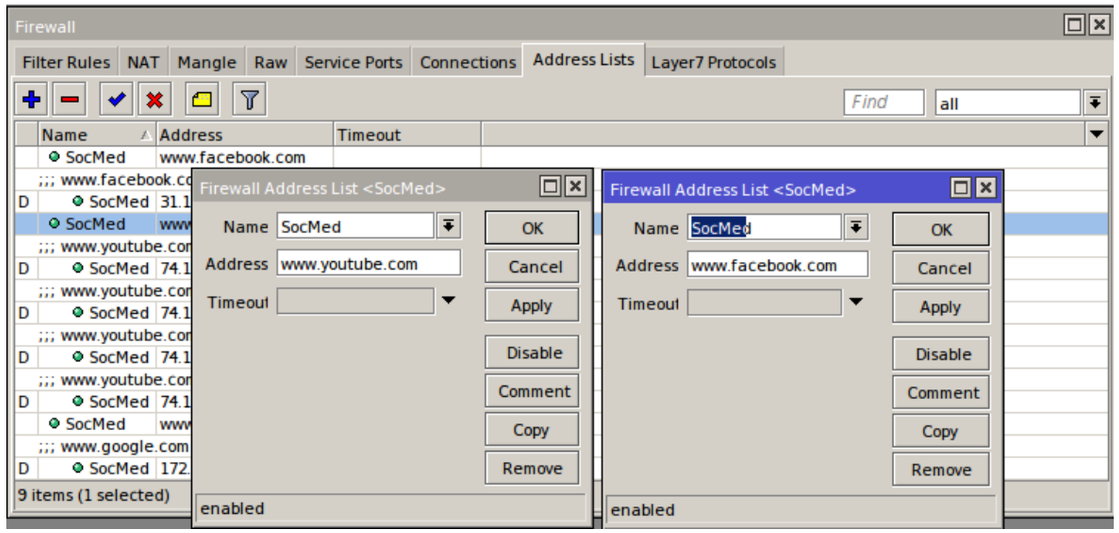


Seharusnya Sekarang klien dari Ether2 sudah bisa melakukan ping ke router.

Selanjutnya pada versi routerOS mulai dari Versi 6.36 sampai ke versi yang terbaru sekarang kita bisa mengkombinasikan fungsi firewall filter rules dengan menu Address List yang digunakan untuk melakukan drop untuk situs-situs yang menggunakan securing (https://).

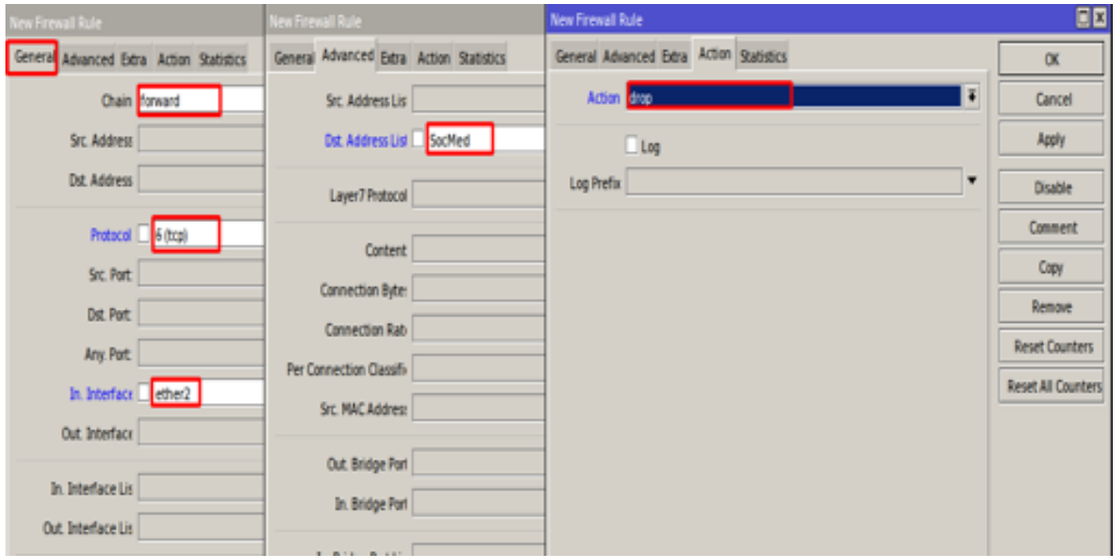
Pada menu IP => Firewall => Address List => Add

Tambahkan IP dari semua situs yang ingin kita batasi akses nya, Namun kita tahu IP pada situs diinternet terlalu banyak untuk dimuat satu persatu, maka pada fitur address list ini juga mendukung pemilihan situs menggunakan nama domain.Jadi kita bisa melakukan Drop situs berdasarkan nama domainnya dan nantinya router akan memetakan sendiri IP yang digunakan oleh situs tersebut.

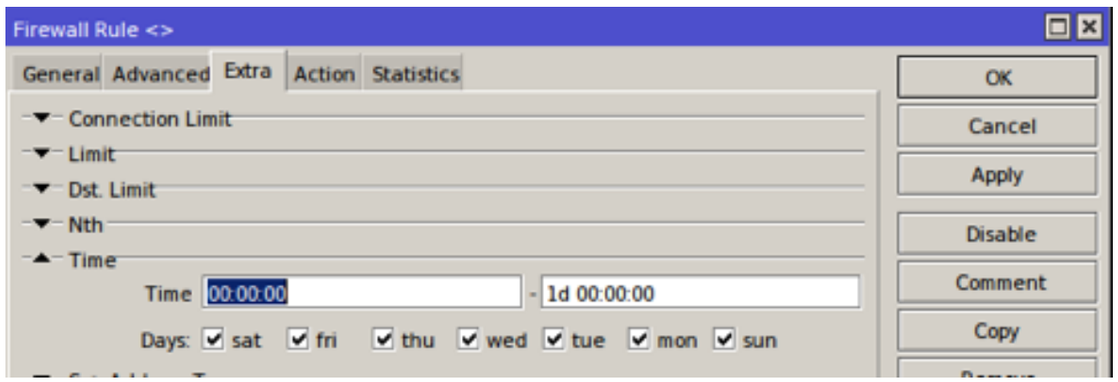


Lalu buat rule di filter rules untuk drop situs-situs yang sudah kita tambahkan pada Address List.Dengan chain “Forward” melalui protokol “tcp” lalu tentukan interface nya, selanjutnya pada tab Advanced tambahkan paket yang kita tandai di Address List pada parameter “Dst-Address List”

Kemudian gunakan Action “DROP”.



Kita juga bisa menggunakan parameter time untuk membatasi waktu kapan saja situs tersebut bisa diakses dan di-Drop, pada tab “Extra” parameter Time, kita bisa menentukan waktu dan hari berlakunya rule tersebut



FIREWALL NAT (Network Addressing Translation)

Selain Filter Rule, pada menu firewall opsi yang wajib kita gunakan adalah NAT.Firewall NAT berfungsi untuk mengubah atau memodifikasi Source Address ataupun Destination Address.Contohnya pada saat kita ingin komputer klien pada LAN kita ingin dapat mengakses internet maka kita buat rule source address yang berasal dari LAN kita buat dengan konfigurasi Src-nat, agar dapat mengakses internet.Karena pada prinsipnya IP Private tidak bisa berkomunikasi langsung dijaringan global jadi harus menggunakan IP Publik.Maka dari itu untuk melakukan browsing komputer client mengirimkan request ke router lalu oleh router request dari client yang menggunakan IP Private akan dimodifikasi seoala-olah yang melakukan request adalah router yang punya IP Public agar bisa berhubungan dengan jaringan luar lalu reply dari internet akan diteruskan kembali ke client sesuai requestnya, biasanya ditambahkan

port number pada setiap reply untuk menandai jika banyak client yang melakukan request.Ada dua chain pada NAT masing-masing fungsinya adalah :

1.Dst-nat :

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.

2.Src-nat :

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.

Sedangkan untuk opsi Action ada beberapa pilihan fungsi sesuai yang kita butuhkan :

Masquerade: Berfungsi untuk modifikasi IP Private ke IP Public dalam jumlah banyak

Dst-nat : Menggantikan alamat tujuan dari sebuah paket ke IP yang ditentukan pada nilai-nilai To-Address dan parameter To-Port.

Jump : Digunakan untuk lompat ke rule yang sudah ditentukan pada Jump-target

Netmap Digunakan untuk melakukan pemetaan 1:1 statis dari satu set alamat IP satu sama lain. Sering digunakan untuk mendistribusikan alamat IP Publik untuk host di jaringan pribadi.

Passtrough : Untuk mengabaikan rule dan lanjut pada rule selanjutnya

Redirect: Digunakan untuk menggantikan alamat IP tujuan ke alamat lainnya sesuai yang ditentukan.

Return : Digunakan untuk kembali memproses rule pertama-dari aturan yang kita buat

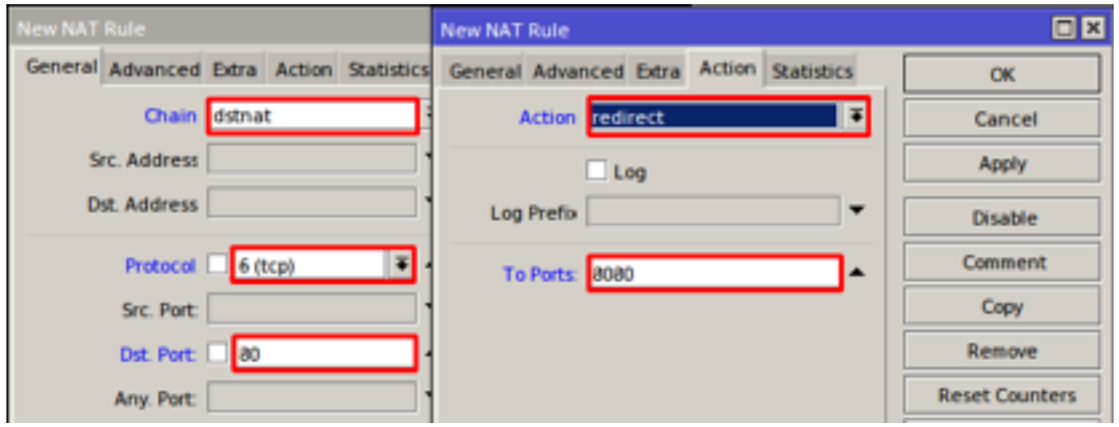
Src-nat : Menggantikan alamat sumber dari sebuah paket ke IP yang ditentukan pada nilai-nilai To-Address dan parameter To-Port.

Untuk penerapan menggunakan chain src-nat sebenarnya sudah kita terapkan di pembahasan awal saat melakukan konfigurasi dasar.Nah, sekarang kita akan menerapkan menggunakan chain dst-nat yang fungsinya untuk membuat transparent proxy, forwarding, CCTV dll.

Untuk membuat tranparen proxy :

Buka menu IP -> Firewall => NAT => Add

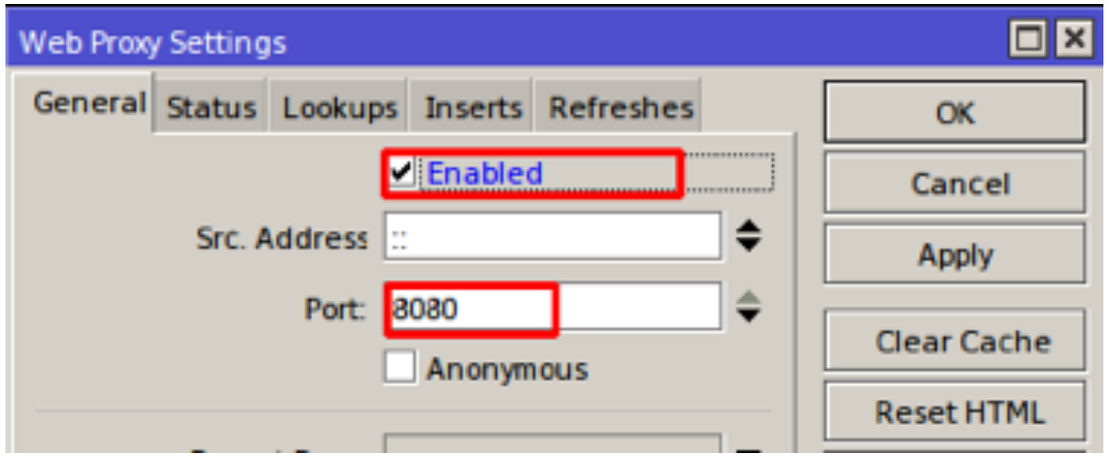
Pada tab menu genral kita gunakan chain “dst-nat”, dengan protokol “6 tcp” dengan tujuan port “80”, lalu kita gunakan Action “Redirect” untuk mengalihkan traffik yang menggunakan protokol http (80) agar melalui protokol proxy yang menggunakan port “8080”.



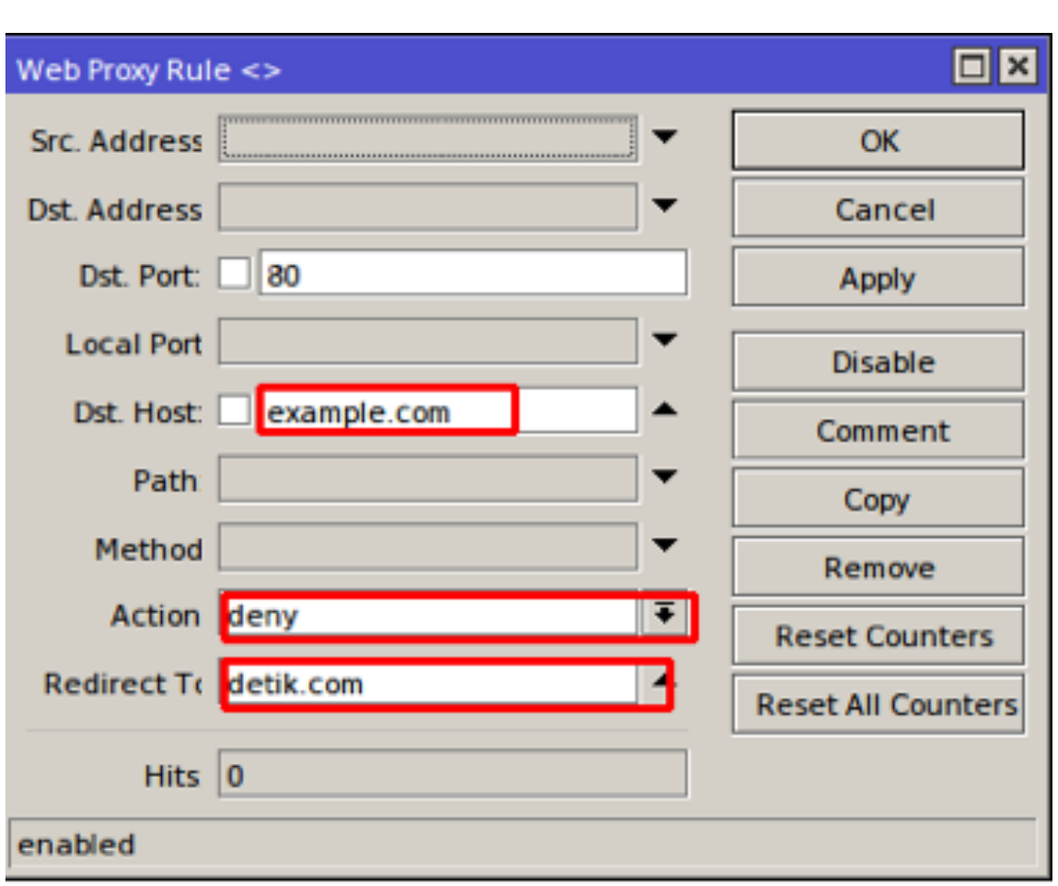
Selanjutnya kita konfigurasikan web proxy pada menu :

IP => Web Proxy

aktifkan web proxy dengan memberi centang pada “Enabled” dan pastikan port nya 8080.



Untuk pengujian kita bisa masukan url yang kita inginkan pada tab menu “Dst.Host” dengan Action “Deny” lalu silahkan tambahkan Destination yang baru untuk meredirect url tersebut



Konfigurasi diatas berarti, saat kita mengakses “example.com” maka akan otomatis di alihkan ke situs “detik.com”.

MikroTik

MTCNA

MikroTik Certified Network Associate Training

FIREWALL

TUNNELS

Tunnels digunakan untuk berkomunikasi antar jaringan lokal yang mempunyai jarak yang jauh melalui infrastruktur pihak ketiga (Internet).Dengan tunnel kita membuat terowongan sendiri dalam sebuah jaringan yang bisa kita gunakan untuk bertukar data seolah berada pada jaringan lokal.Dalam teknik Tunneling ini, nantinya paket data yang dikirim akan dilakukan proses encapsulation (enkapsulasi). Paket data ini nantinya akan dibungkus, dan akan menghasilkan paket data baru oleh protocol lain. Setelah itu, Paket data yang baru tersebut akan dikirim melalui tunnel tadi. Ada banyak jenis tunnel yang bias kita gunakan , diantaranya OVPN,EOIP,PPP,PPTP,SSTP,L2TP,PPPoE, GRE Tunnel, IP Tunnel.

PPPoE Server & PPPoE Client

Point-to-Point Protocol over Ethernet (PPPoE) adalah protokol jaringan untuk mengenkapsulasi Point-to-Point Protocol (PPP) frame dalam frame ethernet.

Beberapa kelebihan menggunakan tunneling ini, data lebih secure :

- Authenticate
- Enkripsi
- Compression
- Ip Distribution

Pada topologi kali ini kita akan menghubungkan router dengan router menggunakan Tunneling PPPoE.

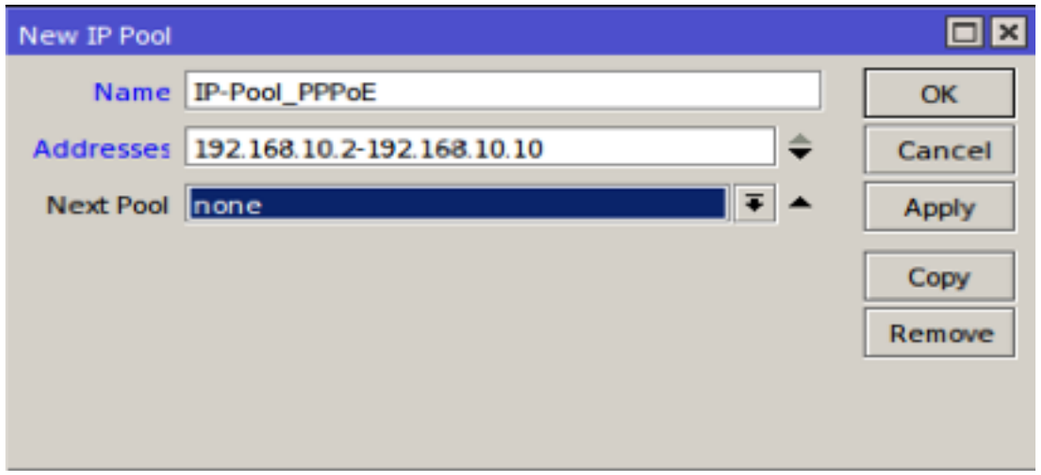
Konfigurasi R1 (PPPoE Server) :

Ether1 : 172.16.10.2/30

Ether2 : 192.168.10.1/24

Buat range IP pada menu IP => Pool => Add

Kita buat PPPoE Server pada ether2, dan range IP yang diberikan untuk PPPoE klien kita tentukan pada IP Pool.

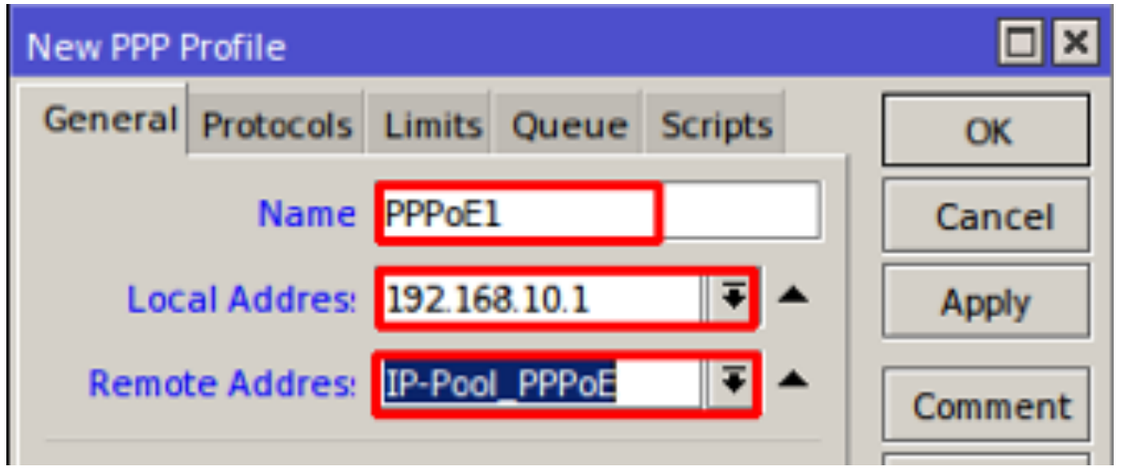


Buka menu PPP => Profiles => Add

Buat profile untuk user PPPoE Server :

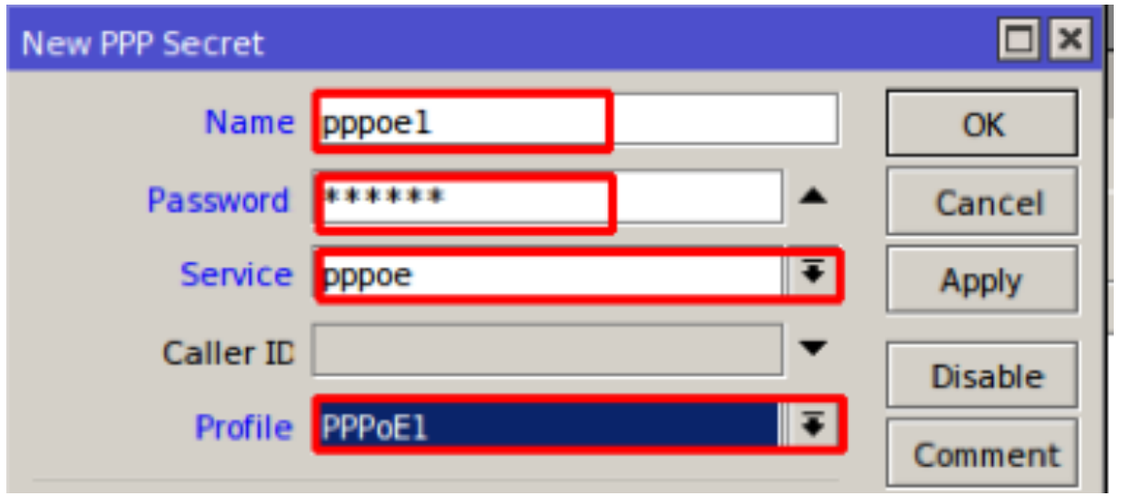
Local Address = Gateway yang akan diberikan untuk User PPPoE Client

Remote Address = IP yang akan diberikan untuk user PPPoE Client, Gunakan Pool yang sudah kita buat tadi atau kita bisa menentukan sendiri IP yang akan diberikan untuk klien



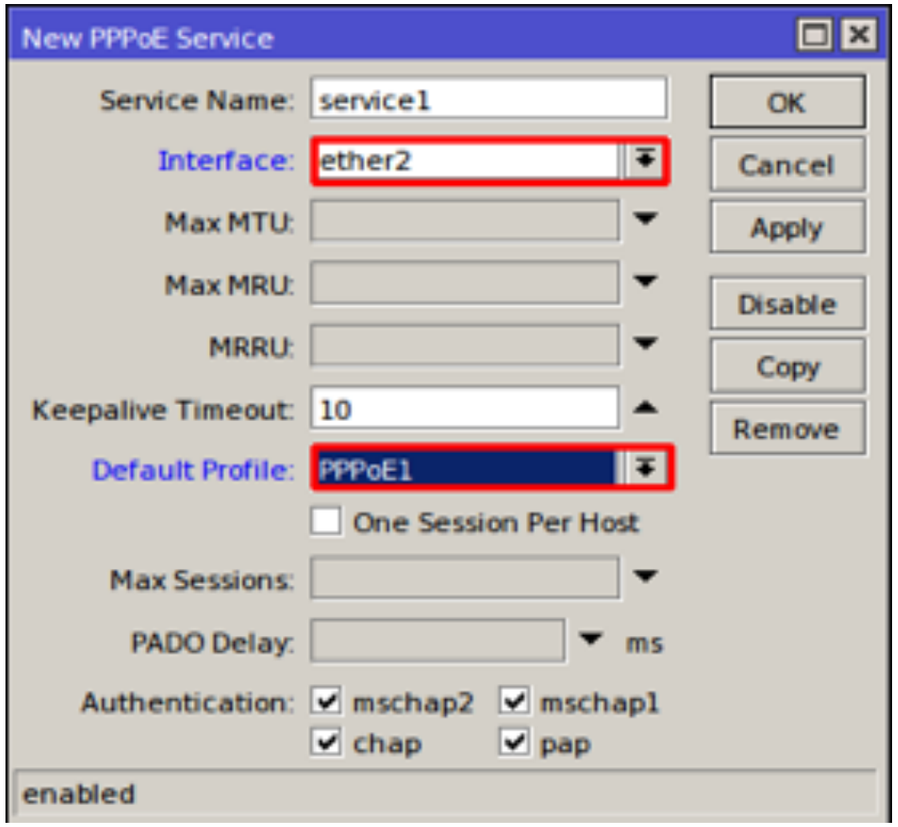
Buka menu PPP => Secret => Add

Tambahkan Username & Password untuk klien sesuai jumlah klien yang ada.



Buka menu PPP => PPPoE Server => Add

Aktifkan PPPoE server yang kita buat tadi.Tambahkan Interface dan Default Profile yang sudah kita buat tadi.



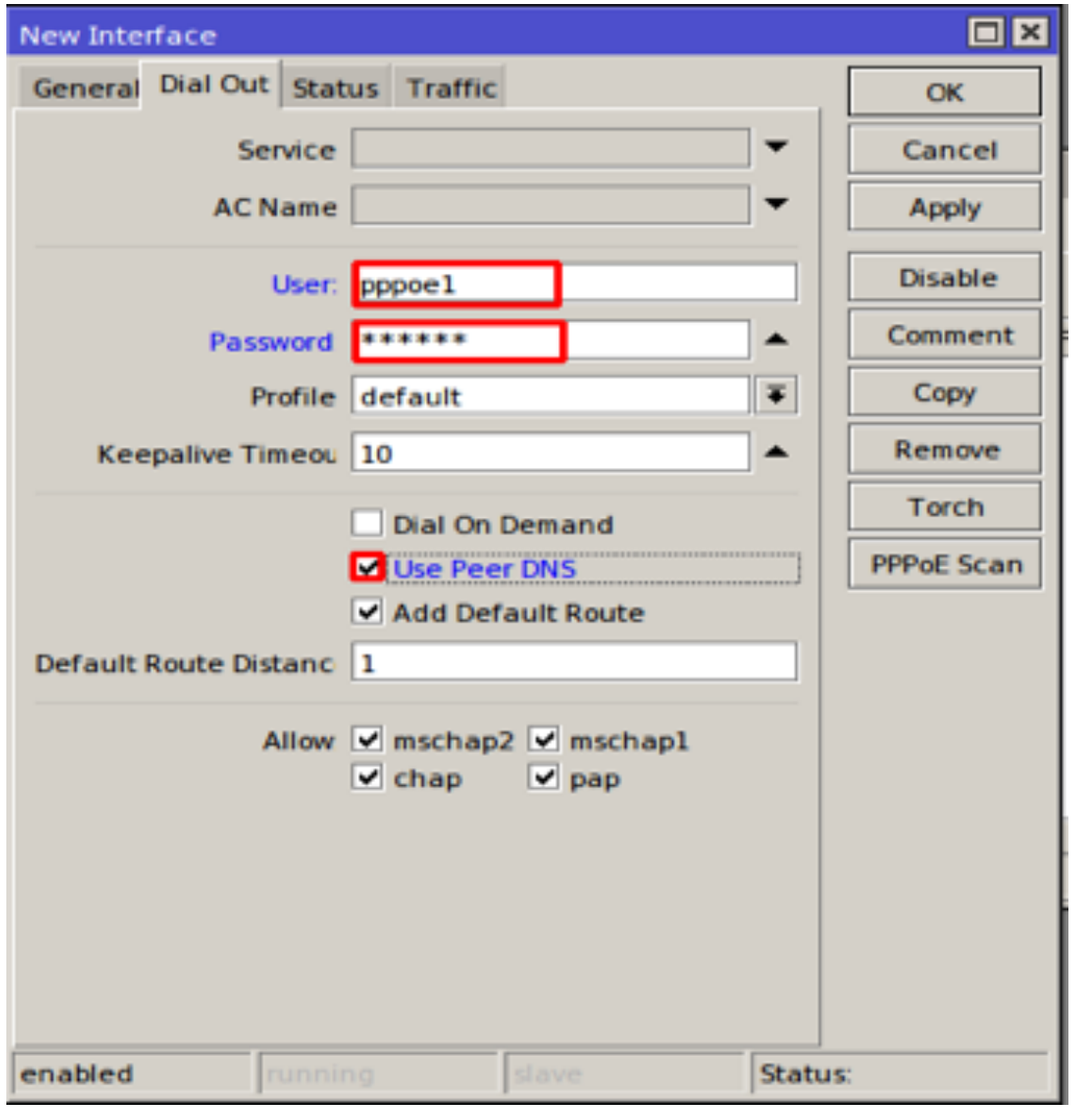
Konfigurasi R2 (PPPoE Client) :

Ether1 = PPPoE Client

Ether2 = 10.10.10.1/24

Buka Menu PPP => Interface => Add => PPPoE Client

Untuk konfigurasi PPPoE Client, kita cukup mengisi username dan password yang dibuat pada PPPoE Server tadi.Centang Add Default Route agar secara otomatis membuat default route pada routing table, Serta Centang Use Peer DNS untuk request DNS dari PPPoE Server.



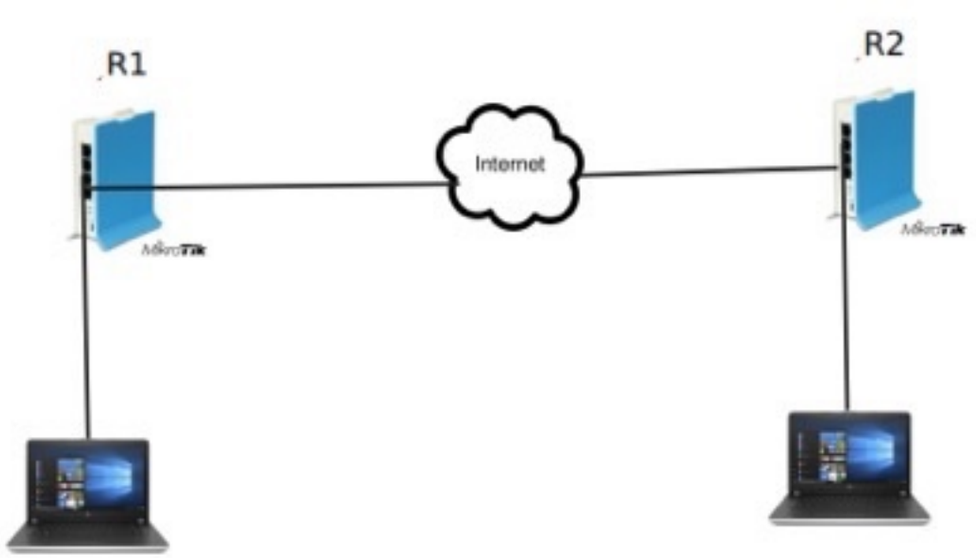
Dan jika anda cek pada IP Addresses maka akan otomatis dapat IP dari ranga yang dibuat pada PPPoE Server, serta pada tabel routing sudah otomatis default route dengan gateway interface PPPoE Server.Dan router 2 sudah terkoneksi dengan internet.

PPTP Server & PPTP Client

PPTP membentuk tunnel PPP antar IP mengunakan protocol TCP dan GRE (Generic Routing Encapsulation).Menggunakan

enkripsi MPPE (Microsoft Point-to-Point Encryption), PPTP menggunakan port TCP 1723 dan banyak digunakan karena hampir semua OS dapat menjalankan PPTP client.

Pada topologi kali ini kita akan menghubungkan router dengan router menggunakan Tunneling PPTP.



Konfigurasi R1 (PPTP Server) :

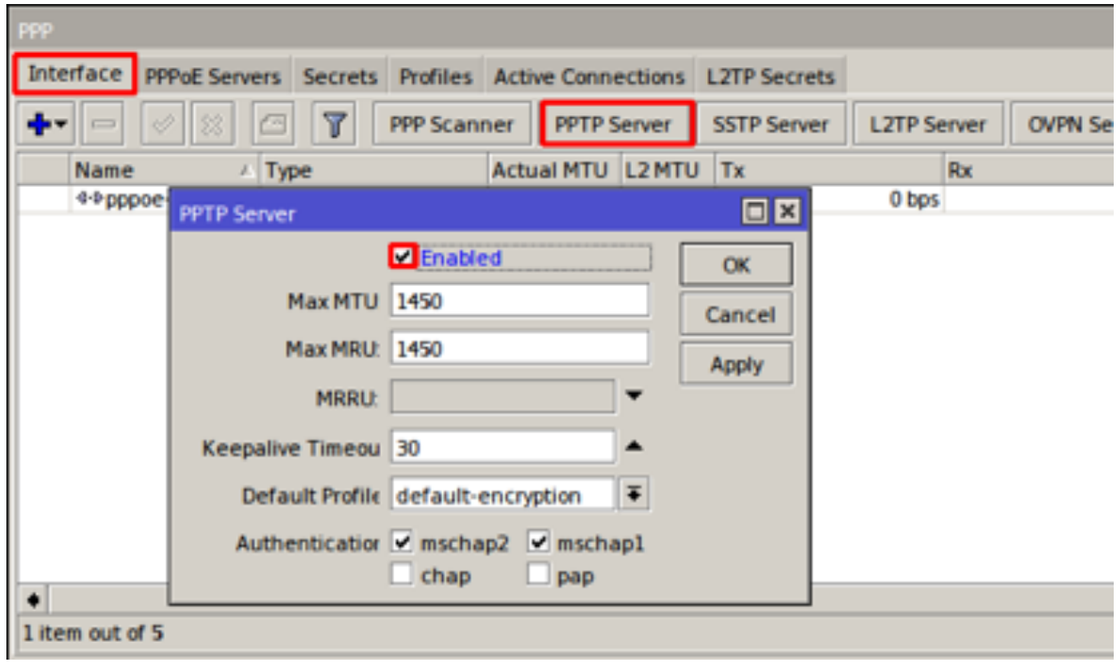
Ether1 = 172.16.10.10/26

Ether2 = 192.168.1.1/24

IP Tunnel = 10.10.10.1/30

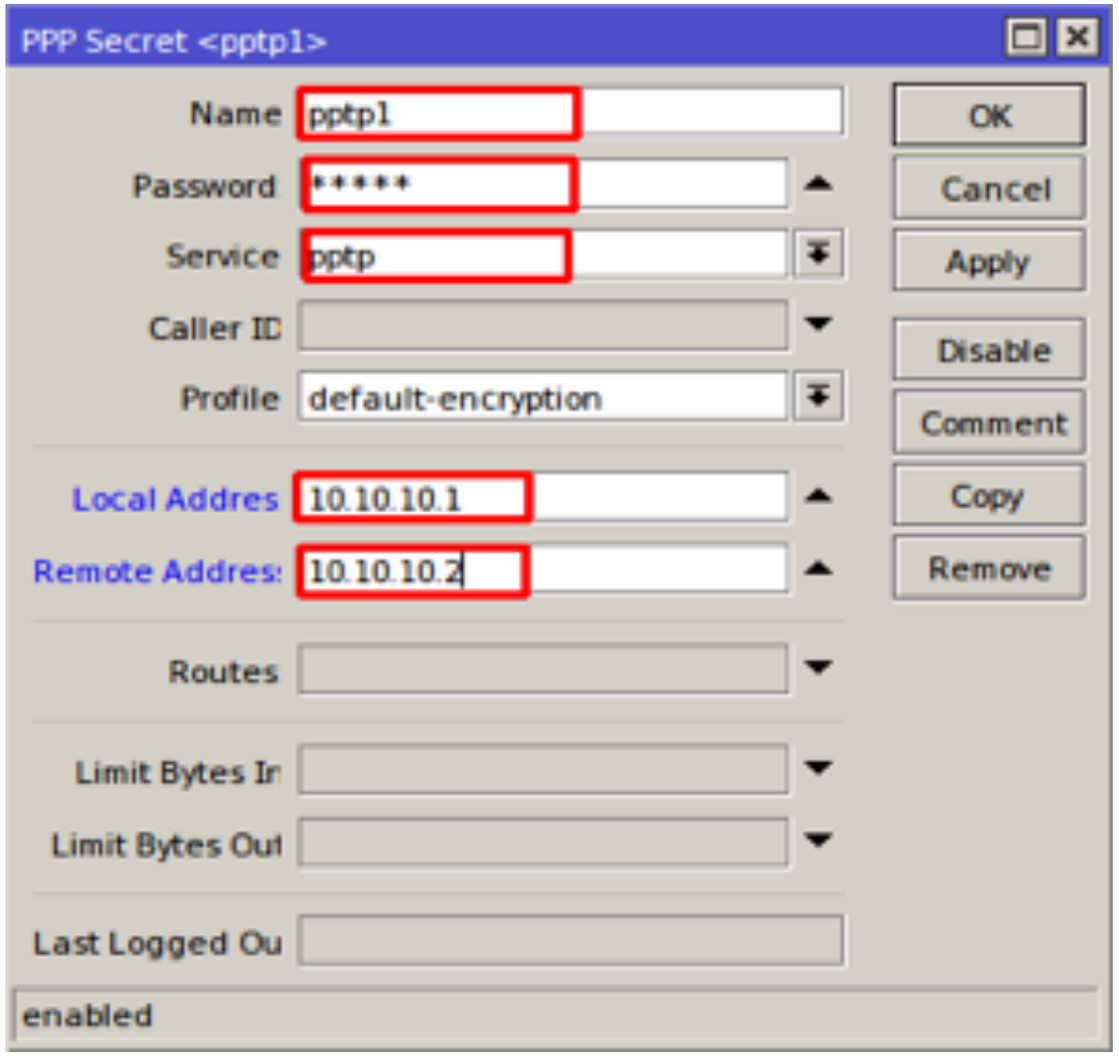
Buka menu PPP => Interfaces => PPTP Server

Aktifkan PPTP Server dengan mencentang “Enable” pada menu PPTP Server



Buka Menu PPP => Secret => Add

Selanjutnya sama seperti pada PPPoE Server, kita buat username dan password untuk user klien PPTP, serta tambahkan IP Tunnel yang akan diberikan untuk user klien.Buat user sesuai dengan jumlah klien yang ada.



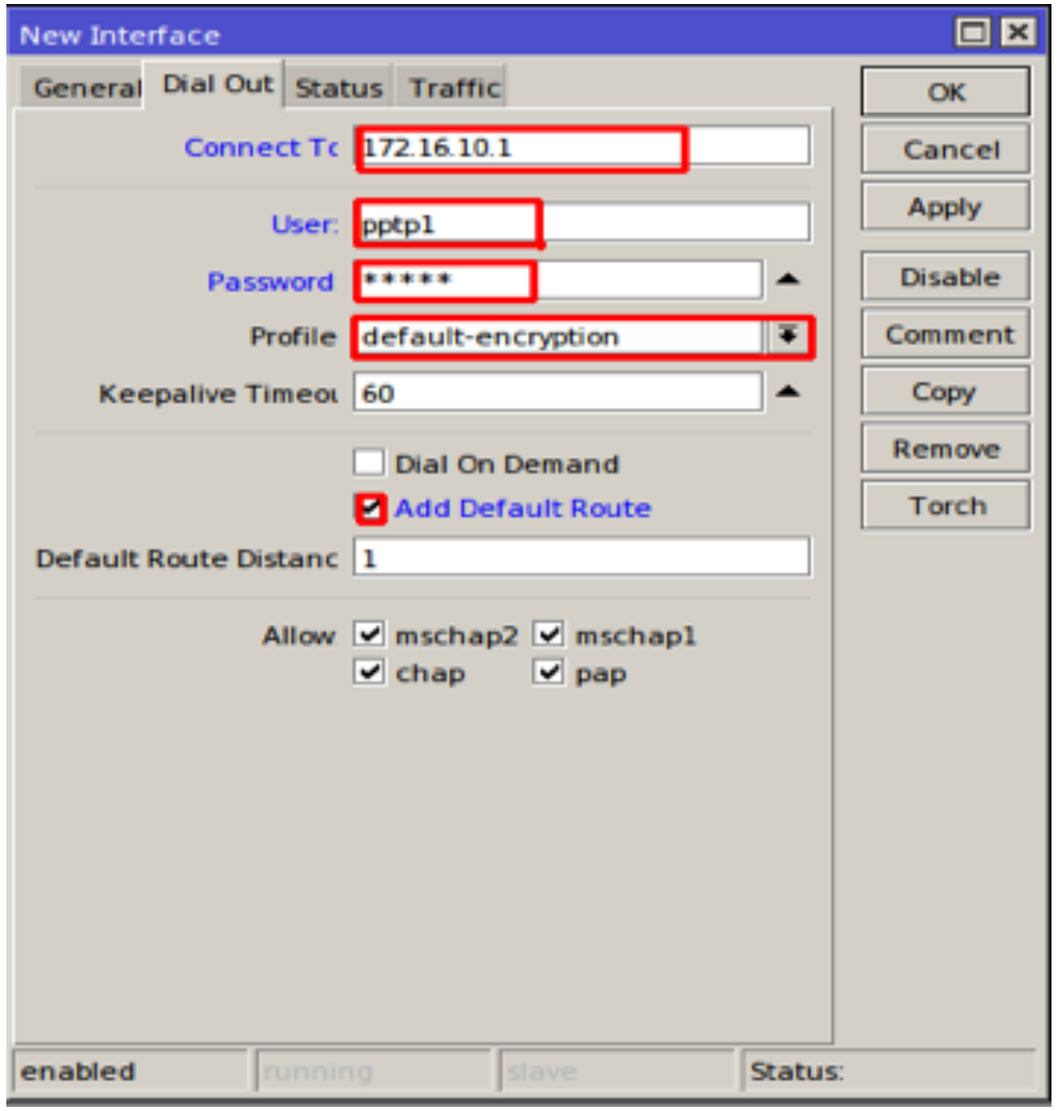
Konfigurasi R2 (PPTP Client)

Ether1 = 172.16.10.20/26

Ether2 = 192.168.2.1/24

Buka menu PPP => PPTP Client => Dial out

Pada bagian Connect to isi dengan IP Public pada Router1, lalu username & password sesuai dengan yang ditambahkan pada PPTP Server.Centang Add Default Route jika ingin default route otomatis ditambahkan pada routing table.



Untuk pengujian kita bisa melakukan traceroute dari router2 menuju router1 seharusnya router terhubung menggunakan IP Tunnel.Jika kita ingin menguji dari laptop klien silahkan tambahkan static routing pada kedua router.

MikroTik

MTCNA

MikroTik Certified Network Associate Training

Quality of Service (QoS)

Quality of Service (QoS)

QoS (kualitas layanan) adalah metode untuk menjaga kualitas layanan tetap pada batas minimal yang ditentukan. Ketika banyak layanan yang menggunakan jaringan secara bersama-sama tentu saja akan terjadi penurunan troughput yang didapat dari tiap-tiap layanan. Oleh sebab itu perlu ada pengaturan untuk menjamin bahwa layanan tetap bisa berjalan dengan optimal. QoS tidak selalu berarti pembatasan bandwidth sebuah komputer. QoS juga bisa digunakan untuk mengatur prioritas berdasarkan parameter-parameter yang diberikan dan menghindari terjadinya monopoli sebuah traffic terhadap seluruh bandwidth yang tersedia.Pada Mikrotik sendiri, penerapan Bandwith manajemen bisa menggunakan fitur Queue. Queue sendiri terbagi 2, yaitu Simple Queue & Queue Tree.Pada saat menerapkan Queue pada jaringan, akan ada 2 jenis Rate, yaitu MIR dan CIR :

MIR (Maximum Information Rate) atau (Max Limit) adalah Bandwidth Maksimal yang akan di dapatkan oleh Client ketika jaringan sedang tidak sibuk (tidak digunakan User Lain)

CIR (Committed Information Rate) atau (Limit At) adalah Bandwidth pasti yang akan di dapatkan saat kondisi jaringan (traffic) penuh / sibuk. Tetapi, tidak akan mendapatkan Bandwidth dibawah CIR.

Melakukan manajemen bandwidth dengan Simple Queue adalah cara paling sederhana. Pada simple queue kita bisa melimit Bandwidth berdasarkan IP Address Client. Baik itu bandwidth Download ataupun Upload.

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

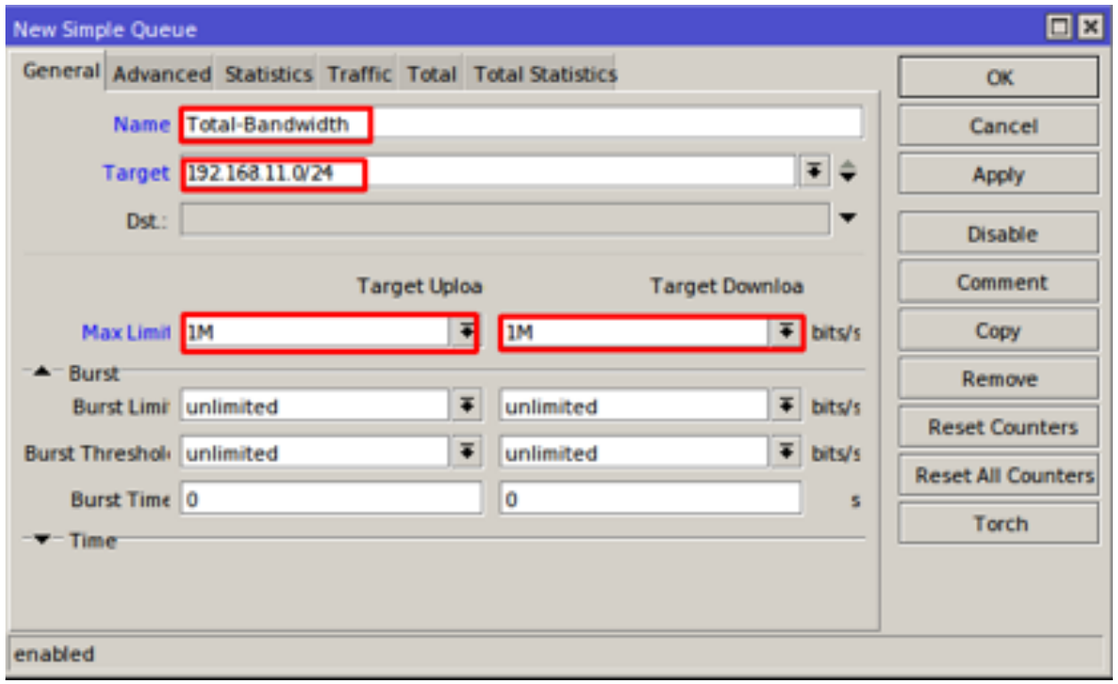
Simple Queue

Cara termudah melakukan queue di RouterOS adalah menggunakan simple queue. Dengan menggunakan simpel queue, sebuah traffic dapat kita limit tx-rate-nya (untuk upload), rx-rate-nya (untuk download) dan tx+rx-rate-nya (akumulasi).

Untuk penerapan simple queue, silahkan cek terlebih dahulu berapa bandwidth yang anda miliki melalui bandwidth test bisa dari ocla atau situs lainnya.Pada lab kali ini kita akan menerapkan MIR dan CIR untuk client.

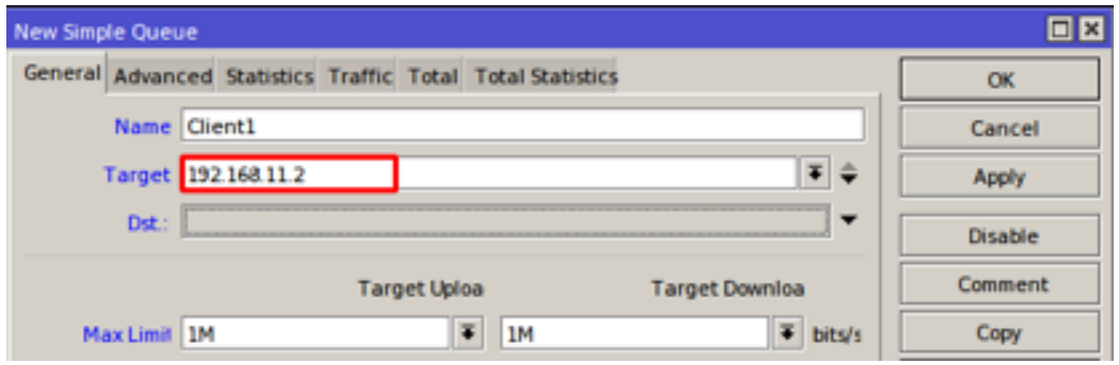
Buka menu Queue => Add

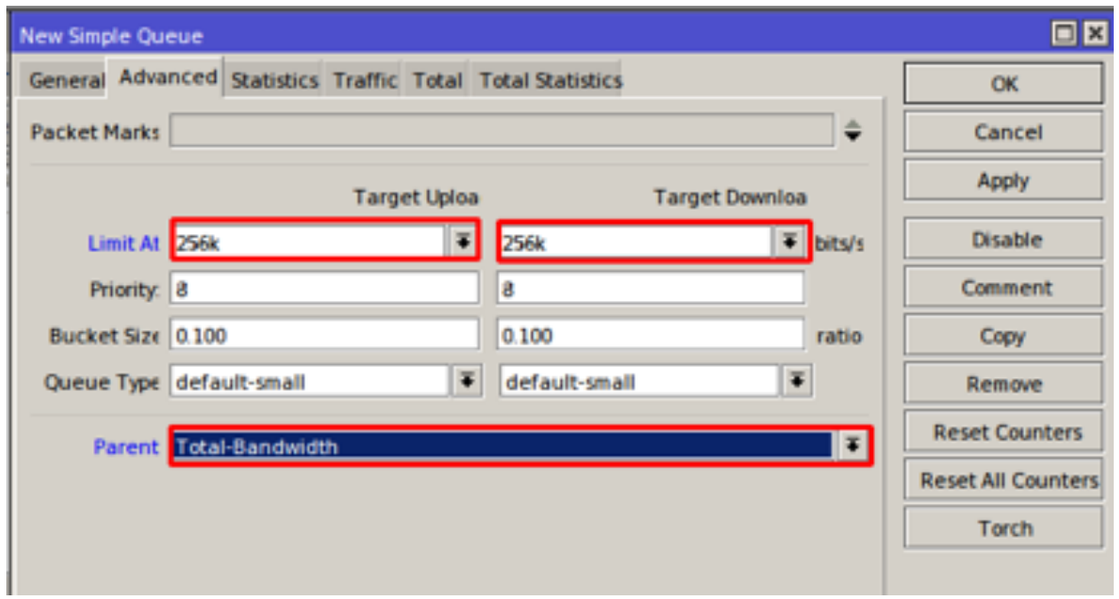
Pada skenario lab kali ini kita akan limitasi bandwidth untuk 4 client dengan bandwith 1 Mb untuk upload maupun download, dengan menentukan Parent (Bandwidth maksimal).Pada tab General tentukan Target Host yang akan kita limit bandwidth nya bisa ditentukan dengan IP Spesifik, Range IP, Network IP, atau berdasarkan Ethernet.Selanjutnya pada Max Limit tentukan Bandwidth maksimal yang kita punya (Cek by Ookla atau speedtest lainnya).



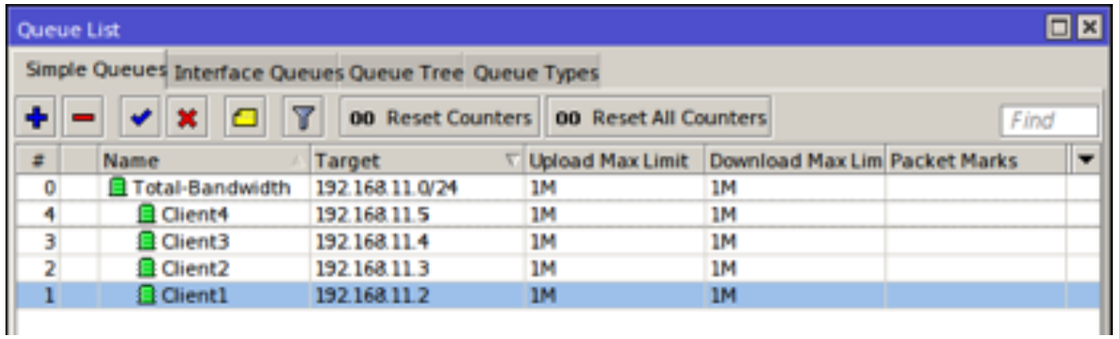
Buka menu Queue => Add

Selanjutnya Pada tab general, kita tambahkan IP dari Klien atau host yang ingin kita limit bandwidthnya, dengan Max Limit yang kita punya.Lalu pada tab Advanced tentukan Limit At untuk Upload dan Download nya,dan pada pilihan parent gunakan parent yang kita buat tadi.Untuk menghitung jumlah Limit At, Jumlah bandwidth dibagi dengan jumlah client yang ada.Buat 3 rule yang sama untuk 3 Host atau klien dengan Parent yang sama,





Buat 3 rule yang sama untuk 3 Host atau klien dengan Parent yang sama,



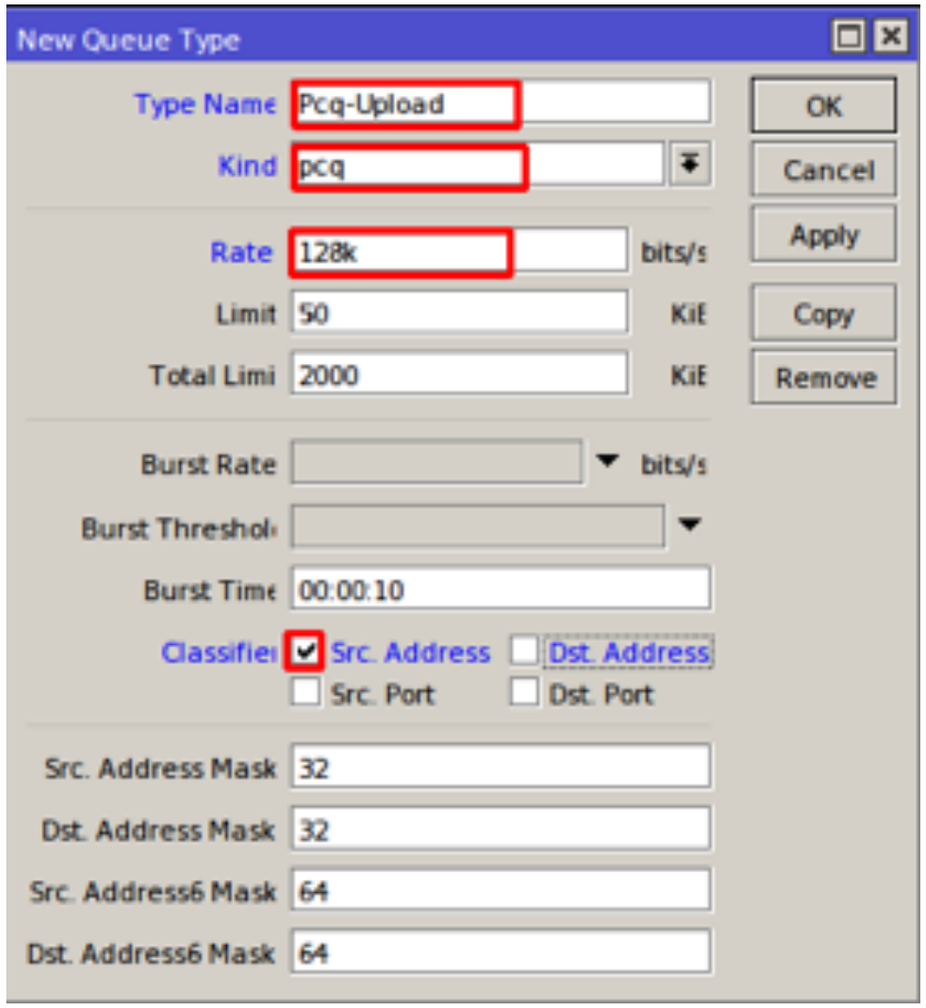
Dengan konfigurasi limitasi bandwidth diatas, jika hanya 1 user yang menggunakan jaringan, nantinya Client1 akan mendapatkan bandwidth full 1Mbps. Ketika jaringan sibuk, 4 client tersebut menggunakan jaringan maka semuanya akan mendapatkan kecepatan minimum atau yang ditentukan pada Limit At (CIR).

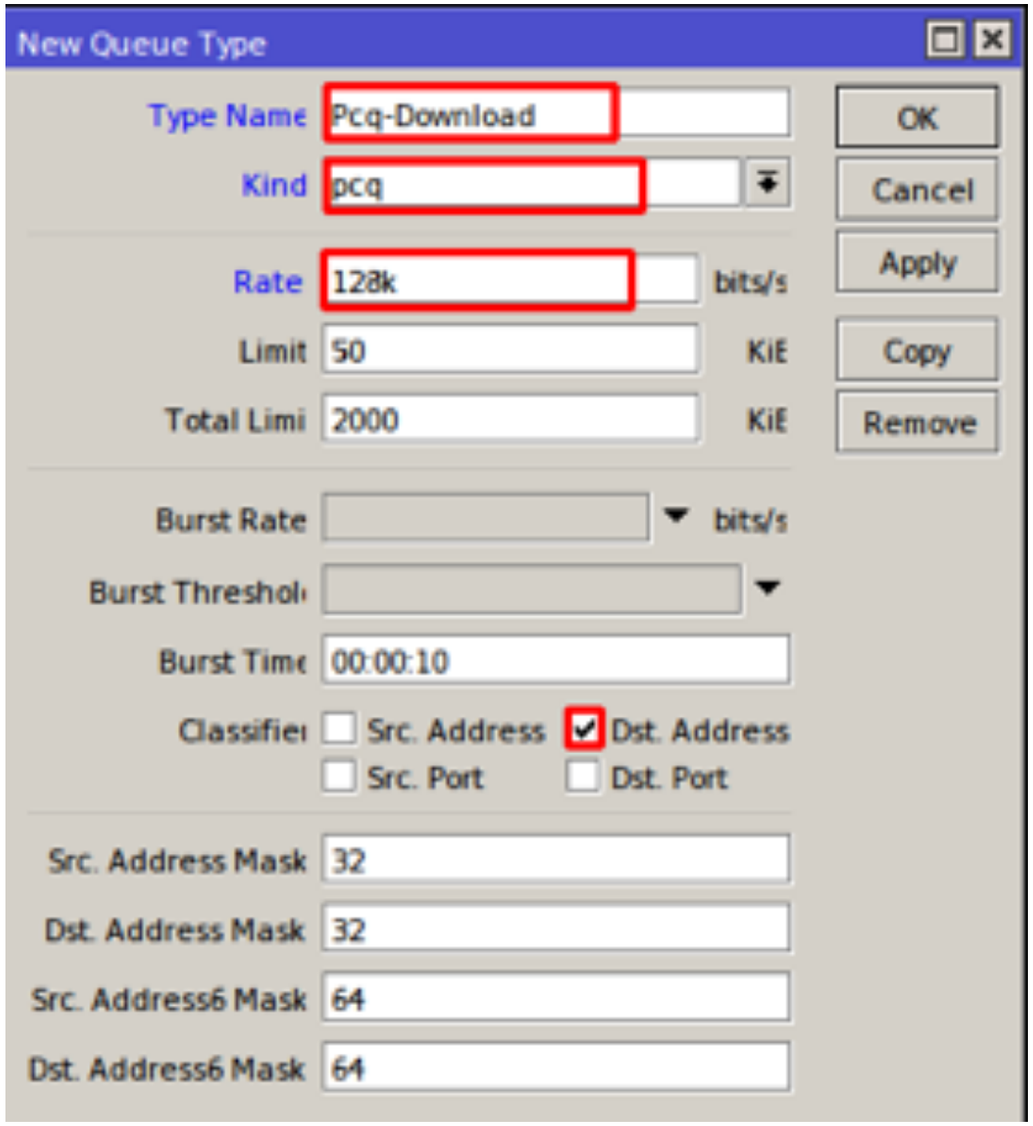
Per Connection Queue (PCQ)

Dengan menerapkan Simple Quue diatas akan efektif jika client pada jaringan kita tidak dalam jumlah yang banyak, namun bagaimana jika klien kita berjumlah ratuasan, akan menjadi sangat repot jika kita harus membuat ratusan rule untuk semua klien.Untuk kondisi client yang sangat banyak dan sangat merepotkan jika harus membuat banyak rule maka bisa menggunakan metode PCQ.Kelebihan PCQ adalah bisa membatasi bandwith untuk masing-maing client secara merata. Namun PCQ mempunyai kekurangan yaitu PCQ membutuhkan memori yang cukup besar.

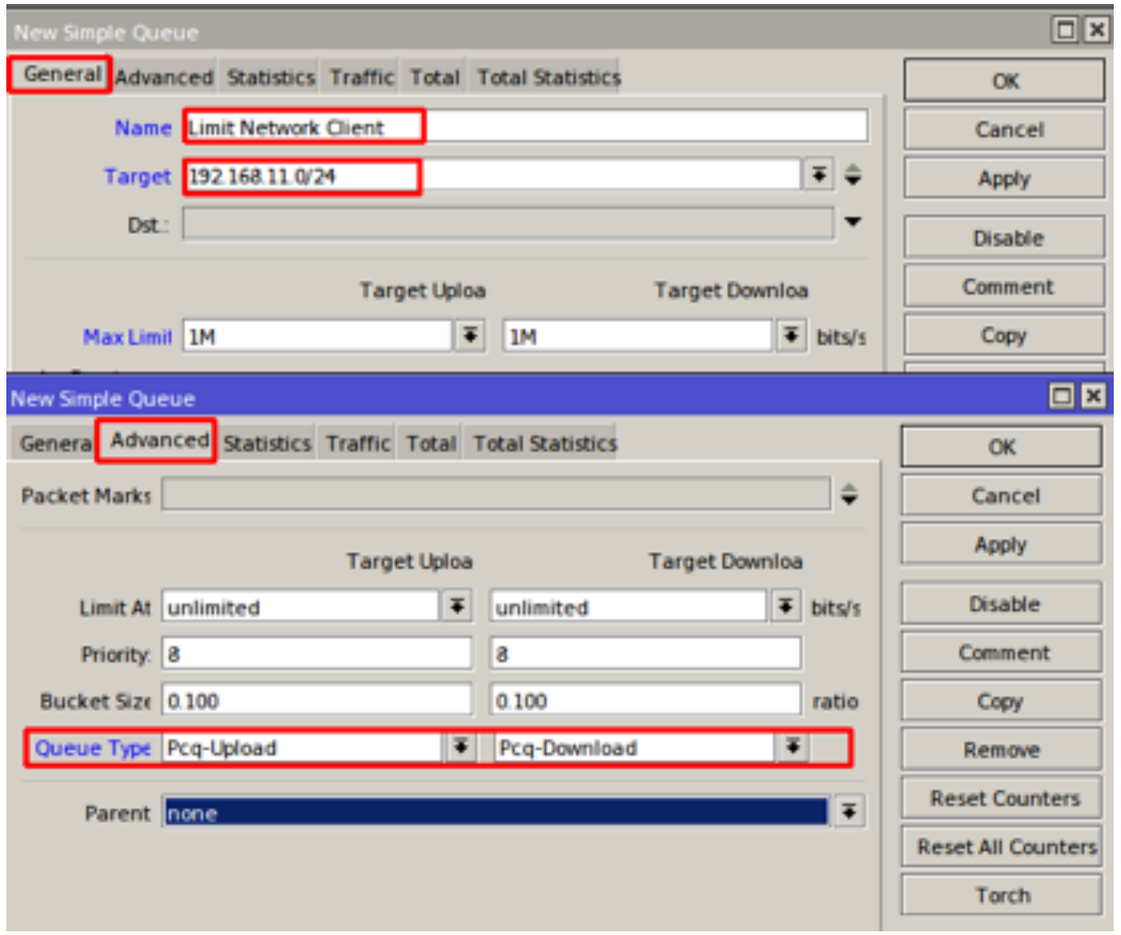
Buka menu Queue => Queue Types => Add

Pertama kita tentukan PCQ Upload dan PCQ Download, dengan menentukan Rate atau sama dengan Limit At (Jumlah Bandwidth dibagi Jumlah Client).Untuk PCQ gunaka Classified Dst.Address sedangkan untuk PCP-Upload gunakan Classified Src.Address.





Selanjutnya untuk penerapan pada klien kita bisa kombinasikan PCQ dengan simple queue, Setelah kita tentukan target klien, pada tab Advanced kita tidak perlu menentukan Limit At dan Parent lagi tetapi pada Type Queue kita gunakan PCQ yang sudah kita buat pada Queue Type



Jika kita menerapkan PCQ kita tidak bisa menentukan priority untuk klien tertentu karena semua bandwidth dibagi rata sesuai dengan jumlah klien yang aktif.Untuk pengujian silakan minta beberapa teman anda untuk terhubung pada jaringan yang anda limit dan lakukan test bandwidth saat 2 klien yang aktif dan pada saat lebih banyak klien yang aktif.

3. Burst

Burst adalah salah satu cara menjalankan QoS yang memungkinkan penggunaan data-rate yang melebihi max-limit untuk periode waktu tertentu. Jika data rate lebih kecil dari burst-threshold, burst dapat dilakukan hingga data-rate men-

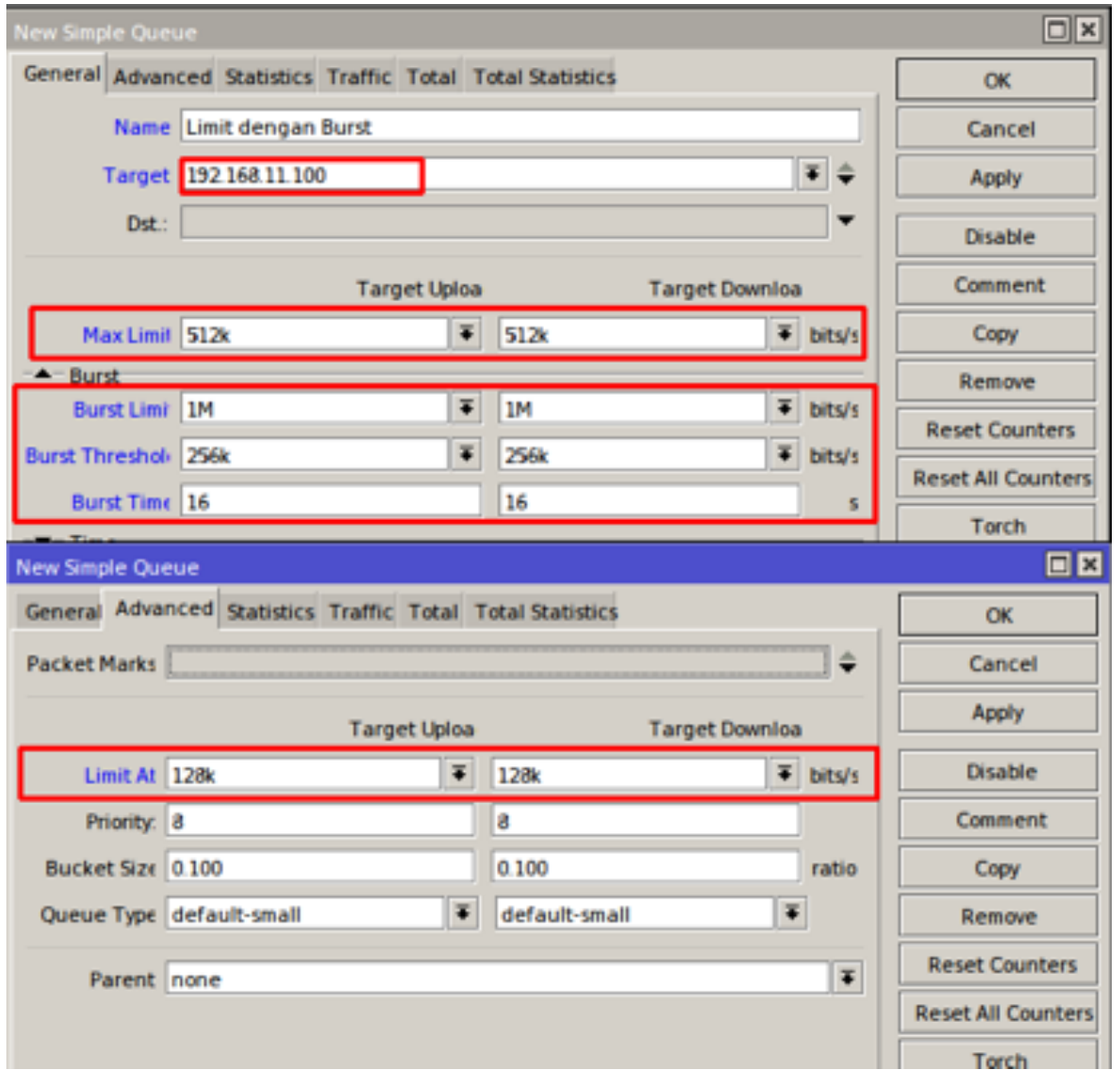
capai burst-limit. Setiap detik, router mengkalkulasi data rate rata-rata pada suatu kelas queue untuk periode waktu terakhir sesuai dengan burst-time. Perlu diingat bahwa burst time tidak sama dengan waktu yang diijinkan oleh router untuk

melakukan burst. Dalam Burst dikenal beberapa istilah penting yaitu burst-limit, burst-threshold dan Burst Time.

- Burst Limit adalah jumlah Bandwidth mkasimum yang akan diterima user dan melebihi bandwidth max limit saat burst terjadi

- Burst Threshold adalah Nilai bandwidth yang ditentukan kapan burst bisa dijalankan dan kapan burst harus dihentikan.Nilai Burst threshold umumnya ¾ dari nilai Max-Limit.

- Burst Time adalah Periode waktu yang digunakan untuk menghitung data rate rata-rata.Burst time bukan menunjukan berapa lama terjadi burst.



Untuk penerapan Burst Time umumnya pada jaringan yang mayoritas klien banyak melakukan browsing, karena burst time yang hanya terjadi hanya beberapa detik.Burst akan berjalan jika nilai data rate rata-rata lebih rendah dari burst threshold yang kita tentukan, namun pada saat nilai rata-rata data rate sama atau melebihi burst threshold maka burst akan dihentikan.Untuk menghitung berapa lama terjadi Burst, kita dapat menggunakan rumus :

(Lama Burst dijalankan = (Burst-Threshold/Burst Limit) x Burst Time)

Dengan konfigurasi diatas berarti :

Lama Burst dijalankan = (256/1024) x 16 = 4 Detik

4. Queue Tree & Mangle

QueueTree adalah tool pada MikroTik RouterOS yang memiliki kemampuan untuk melimitasi bandwith yang lebih lengkap dibandingkan dengan simple-queue. Dengan QueueTree dimungkinkan untuk melakukan limitasi yang lebih fleksibel. Agar sebuah QueueTree dapat berjalan maka harus menggunakan Mangle yang dikonfigurasikan terlebih dahulu.Selain itu kita bisa menandai koneksi maupun paket yang ingin kita limit, misalnya kita hanya ingin membatasi penggunaan Youtube dan Facebook saja, atau kita ingin membatasi Bandwidth hanya untuk 1 IP atau 1 Network saja.Untuk Lab dan pembahasan lebih lanjut akan dibahas pda saat materi MTCRE.

Tools Monitoring

Tugas seorang admin jaringan saat selesai melakukan instalasi jaringan adalah monitoring lalu lintas traffic jaringan, memastikan semua berjalan normal, mengatasi jika ada aktifitas mencurigakan didalam jaringan.Untuk monitoring lalu lintas jaringan pada mikrotik dapat dilakukan dengan Aplikasi monitoring yang sudah disediakan oleh mikrotik yaitu The Dude yang bisa anda dapatkan di situs resmi mikrotik (mikrotik.com/download).

Namun pada RouterOS sendiri sudah dilengkapi dengan fitur monitoring yang sudah cukup lengkap dapat kita gunakan dengan mudah, Diantaranya adalah :

1. Netwatch

adalah salah satu fitur Mikrotik yang digunakan untuk monitoring uptime router Mikrotik kita. Fitur ini dapat anda temukan pada Winbox anda di menu Tools Netwatch.

Di sini kita dapat menentukan host yang akan dipantau, sebagai contoh host di atas diisi dengan IP Google. Masalahnya adalah kita tidak mungkin selalu melihat Netwatch untuk melakukan aktivitas monitor jaringan. Maka kita bisa setting agar router secara otomatis mengirim email saat terjadi downtime.

2. Email

Untuk melakukan monitoring yang dapat dipantau melalui notifikasi email, bisa dikombinasikan dengan netwatch.

3. Tourch

merupakan tool yang digunakan untuk memonitor lalulintas data secara realtime, tourch bisa di custom berdasarkan ip address pengirim maupun ip address tujuan :

Keterangan :

TX menunjukan kecepatan lalulintas data yang keluar melalui interface tersebut, bisa dikatakan data keluar dari interface (transfer, upload)

RX menunjukan kecepatan lalulintas data yang masuk melalui interface tersebut, bisa dikatakan data diterima melalui interface tersebut (recieve, download)

TX-PACKET menunjukan banyaknya paket yang keluar melalui interface tersebut

RX-PACKET menunjukan banyaknya paket yang diterima melalui interface tersebut

4. Graphs

Dengan tools graph, kita bisa melakukan monitoring terhadap beberapa parameter pada router dan menyajikannya dalam bentuk grafik. Grafik ini bisa dilihat dengan melakukan akses router via web, dengan format alamat http://[ip router]/graphs.

By default, tool graph ini belum melakukan perekaman data apapun, jika dilihat via web browser belum terdapat data apapun. Dibutuhkan pengaturan parameter apa saja yang akan direkam serta tambahan policy jika dibutuhkan.

Selain interface router, graph juga bisa merekam Resource Hardware seperti CPU, Memory dan RAM, atau bisa juga untuk merekam Queue.

5. SNMP

Simple Network Management Protocol (SNMP) adalah protokol standar Internet untuk mengelola perangkat pada jaringan. SNMP dapat digunakan untuk berbagai data grafik. Contoh penggunaan nya pada The Dude dan aplikasi sejenisnya Agar Mikrotik dapat dikelola, maka SNMP harus diaktifkan. Caranya cukup mudah, mengaktifkan SNMP pd Mikrotik, bisa dengan command : /snmp set enabled=yes.

6. Logging

Secara default router akan mencatat semua aktifitas yang dilakukan router, namun untuk memudahkan melihat log kita bisa melakukan pengaturan topic apa saja yang akan dicatat serta akan disimpan atau ditampilkan dimana log tersebut.

7. Ping

8. Traceroute

9. CPU Load

Menjadi seorang network enginering bukan hanya tentang bagaimana keterampilan kita dalam membuat jaringan, namun disan kita juga belajar seni baik itu tentang kerapihan, SOP, Keindahan dalam sebuah rangkaian jaringan.Selain itu yang terpenting dalam sebuah jaringan bukan hanya proses pembuatan namun bagaimana kita bisa membuat jaringan yang kita buat dapat selalu berjalan stabil (Bukan berarti tidak ada masalah sama sekali), dan setiap ada masalah kita selalu siap dan sudah menyiapkan solusi untuk kemungkinan terburuk yang akan terjadi.