Modul Workshop Mikrotik Dasar:

Pengenalan Mikrotik dan Perintah-perintah Dasar

Disusun oleh:

Helmi Prasetyo, S.Kom
Herika Hayurani, M.Kom
Sri Puji Utami A., M.T

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS YARSI
SEPTEMBER 2014

Jl. Letjen. Suprapto, Cempaka Putih
Jakarta Pusat 10510 - Telp/Fax : (021) 4269301
Website : www.yarsi.ac.id

DAFTAR ISI

BAB I
PENGENALAN MIKROTIK

Tujuan :

- Peserta mengenal dan mengetahui apa itu Mikrotik
- Peserta mengetahui fitur dan istilah pada Mikrotik
- Peserta mengetahui cara akses dan mampu mengakses Mikrotik

1.1 Sejarah Mikrotik

Mikrotik adalah sebuah perusahaan kecil berkantor pusat di Latvia, bersebelahan dengan Rusia. Pembentukannya diprakarsai oleh John Trully dan Arnis Riekstins. John Trully adalah seorang berkewarganegaraan Amerika yang berimigrasi ke Latvia. Di Latvia ia bejumpa dengan Arnis, Seorang sarjana Fisika dan Mekanik sekitar tahun 1995.

John dan Arnis mulai me-routing dunia pada tahun 1996 (misi Mikrotik adalah me-routing seluruh dunia). Mulai dengan sistem Linux dan MS-DOS yang dikombinasikan dengan teknologi Wireless-LAN (WLAN) Aeronet berkecepatan 2 Mbps di Moldova, negara tetangga Latvia, baru kemudian melayani lima pelanggannya di Latvia.

Prinsip dasar mereka bukan membuat Wireless ISP (W-ISP), tetapi membuat program router yang handal dan dapat dijalankan diseluruh dunia. Latvia hanya merupakan tempat eksperimen John dan Arnis, karena saat ini mereka sudah membantu negara-negara lain termasuk Srilanka yang melayani sekitar 400 pengguna.

Linux yang pertama kali digunakan adalah Kernel 2.2 yang dikembangkan secara bersama-sama denag bantuan 5-15 orang staff Research and Development (R&D) Mikrotik yang sekarang menguasai dunia routing di negara-negara berkembang. Menurut Arnis, selain staf di lingkungan Mikrotik, mereka juga merekrut tenega-tenaga lepas dan pihak ketiga yang dengan intensif mengembangkan Mikrotik secara marathon.

1.2 Routers OS

Mikrotik RouterOS™ adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer manjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless, cocok digunakan oleh ISP

dan provider hotspot. Untuk instalasi Mikrotik tidak dibutuhkan piranti lunak tambahan atau komponen tambahan lain. Mikrotik didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks sekalipun.

Mikrotik bukanlah perangkat lunak yang gratis jika anda ingin memanfaatkannya secara penuh, dibutuhkan lisensi dari Mikrotiks untuk dapat menggunakanya alias berbayar. Mikrotik dikenal dengan istilah Level pada lisensinya. Tersedia mulai dari Level 0 kemudian 1, 3 hingga 6, untuk Level 1 adalah versi Demo Mikrotik dapat digunakan secara gratis dengan fungsi-fungsi yang sangat terbatas. Tentunya setiap level memilki kemampuan yang berbeda-beda sesuai dengan harganya, Level 6 adalah level tertinggi dengan fungsi yang paling lengkap. Secara singkat dapat digambarkan jelaskan sebagai berikut:

- 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 sbg 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.

1.3 Routerboard

RouterBoard adalah router embedded produk dari Mikrotik. Routerboard seperti sebuah pc mini yang terintegrasi karena dalam satu board tertanam prosesor, ram, rom, dan memori flash. Routerboard menggunakan os RouterOS yang berfungsi sebagai router jaringan, bandwidth management, proxy server, dhcp, dns server dan bisa juga berfungsi sebagai hotspot server.

Ada beberapa seri routerboard yang juga bisa berfungsi sebagai wifi. sebagai wifi access point, bridge, wds ataupun sebagai wifi client. seperti seri RB411, RB433, RB600. dan sebagian besar ISP wireless menggunakan routerboard untuk menjalankan fungsi wirelessnya baik sebagai ap ataupun client. Dengan routerboard Anda bisa menjalankan fungsi sebuah router tanpa tergantung pada PC lagi. karena semua fungsi pada router sudah ada dalam routerboard. Jika dibandingkan dengan pc yang diinstal routerOS, routerboard ukurannya lebih kecil, lebih kompak dan hemat listrik karena hanya menggunakan adaptor. untuk digunakan di jaringan wifi bisa dipasang diatas tower dan menggunakan PoE sebagai sumber arusnya.

Mikrotik pada standar perangkat keras berbasiskan Personal Computer (PC) dikenal dengan kestabilan, kualitas kontrol dan fleksibilitas untuk berbagai jenis paket data dan penanganan proses rute atau lebih dikenal dengan istilah routing. Mikrotik yang dibuat sebagai router berbasiskan PC banyak bermanfaat untuk sebuah ISP yang ingin menjalankan beberapa aplikasi mulai dari hal yang paling ringan hingga tingkat lanjut. Contoh aplikasi yang dapat diterapkan dengan adanya Mikrotik selain routing adalah aplikasi kapasitas akses (bandwidth) manajemen, firewall, wireless access point (WiFi), backhaul link, sistem hotspot, Virtual Private Network (VPN) server dan masih banyak lainnya.

1.4 Fitur Mikrotik

- Address List : Pengelompokan IP Address berdasarkan nama
- Asynchronous : Mendukung serial PPP dial-in / dial-out, dengan otentikasi CHAP, PAP, MSCHAPv1 dan MSCHAPv2, Radius, dial on demand, modem pool hingga 128 ports.
- Bonding : Mendukung dalam pengkombinasian beberapa antarmuka ethernet ke dalam 1 pipa pada koneksi cepat.
- Bridge : Mendukung fungsi bridge spinning tree, multiple bridge interface, bridging firewalling.
- Data Rate Management : QoS berbasis HTB dengan penggunaan burst, PCQ, RED, SFQ, FIFO queue, CIR, MIR, limit antar peer to peer
- DHCP : Mendukung DHCP tiap antarmuka; DHCP Relay; DHCP Client, multiple network DHCP; static and dynamic DHCP leases.

- Firewall dan NAT : Mendukung pemfilteran koneksi peer to peer, source NAT dan destination NAT. Mampu memfilter berdasarkan MAC, IP address, range port, protokol IP, pemilihan opsi protokol seperti ICMP, TCP Flags dan MSS.
- Hotspot : Hotspot gateway dengan otentikasi RADIUS. Mendukung limit data rate, SSL ,HTTPS.
- IPSec : Protokol AH dan ESP untuk IPSec; MODP Diffie-Hellmann groups 1, 2, 5; MD5 dan algoritma SHA1 hashing; algoritma enkirpsi menggunakan DES, 3DES, AES-128, AES-192, AES-256; Perfect Forwarding Secresy (PFS) MODP groups 1, 2,5
- ISDN : mendukung ISDN dial-in/dial-out. Dengan otentikasi PAP, CHAP, MSCHAPv1 dan MSCHAPv2, Radius. Mendukung 128K bundle, Cisco HDLC, x751, x75ui, x75bui line protokol.
- M3P : Mikrotik Protokol Paket Packer untuk wireless links dan ethernet.
- MNDP : Mikrotik Discovery Neighbour Protokol, juga mendukung Cisco Discovery Protokol (CDP).
- Monitoring / Accounting : Laporan Traffic IP, log, statistik graph yang dapat diakses melalui HTTP.
- NTP : Network Time Protokol untuk server dan clients; sinkronisasi menggunakan system GPS.
- Poin to Point Tunneling Protocol : PPTP, PPPoE dan L2TP Access Consentrator; protokol otentikasi menggunakan PAP, CHAP, MSCHAPv1, MSCHAPv2; otentikasi dan laporan Radius; enkripsi MPPE; kompresi untuk PPoE; limit data rate.
- Proxy : Cache untuk FTP dan HTTP proxy server, HTTPS proxy; transparent proxy untuk DNS dan HTTP; mendukung protokol SOCKS; mendukung parent proxy; static DNS.
- Routing : Routing statik dan dinamik; RIP v1/v2, OSPF v2, BGP v4.
- SDSL : Mendukung Single Line DSL; mode pemutusan jalur koneksi dan jaringan.
- Simple Tunnel : Tunnel IPIP dan EoIP (Ethernet over IP).
- SNMP : Simple Network Monitoring Protocol mode akses read-only.
- Synchronous : V.35, V.24, E1/T1, X21, DS3 (T3) media ttypes; sync-PPP, Cisco HDLC; Frame Relay line protokol; ANSI-617d (ANDI atau annex D) dan Q933a (CCITT atau annex A); Frame Relay jenis LMI.

- Tool : Ping, Traceroute; bandwidth test; ping flood; telnet; SSH; packet sniffer; Dinamik DNS update.
- UPnP : Mendukung antarmuka Universal Plug and Play.
- VLAN : Mendukung Virtual LAN IEEE 802.1q untuk jaringan ethernet dan wireless; multiple VLAN; VLAN bridging.
- VoIP : Mendukung aplikasi voice over IP.
- VRRP : Mendukung Virtual Router Redudant Protocol.
- WinBox : Aplikasi mode GUI untuk meremote dan mengkonfigurasi Mikrotik RouterOS.

1.5 Istilah di Mikrotik dan Networking

Berikut ini adalah kumpulan istilah-istilah dalam Mikrotik yang sering muncul menu-menu Mikrotik :

- System, paket yang wajib diinstal karena merupakan inti dari Mikrotik
- PPP(Point to Point Protocol), merupakan paket yang memuat protokol PPP. Paket ini diperlukan untuk fitur komunikasi serial dengan menggunakan PPP, ISDN PPP, L2TP, dan PPTP serta komunikasi PPP on Ethernet(PPPoE). Paket PPP digunakan untuk komunikasi Wide Area Network dengan menggunakan komunikasi serial mode asyncronous maupun mode synchronous.
- DHCP(Dynamic Host Configuration Protocol), paket yang memuat fitur DHCP baik yang diperlukan untuk menjadi client maupun server.
- Advanced –tools, memuat fitur e-mail client, ping, netwatch, traceroute, bandwidth tester, traffic monitoring, mrtg, dan utility yang lain, yang sering diperlukan untuk mengetahui kondisi router maupun jaringan. Fitur Netwatch merupakan salah satu fitur yang memungkinkan Mikrotik menjadi lebih pintar dan dapat memilih konfigurasi berdasarkan script(urutan perintah) sesuai kondisi jaringan (netwatch).
- Arlan, merupakan dukungan Mikrotik untuk penggunaan card ISA arlan 655 Wireless Interface agar dapat secara transparan berkomunikasi dengan lawannya.
- GPS, Mikrotik dapat menggunakan penerima Global Poasitioning System(GPS) sebagai referensi waktu Network Time Protokol (NTP) dan lokasi.
- Hotspot, digunakan untuk melakukan authentication, authorization dan accounting pengguna yang melakukan access jaringan melalui gerbang hotspot. Pengguna hotspot

sebelum melakukan access jaringan perlu melakukan authentication melalui web browser baik dengan protokol http maupun https (secure http).

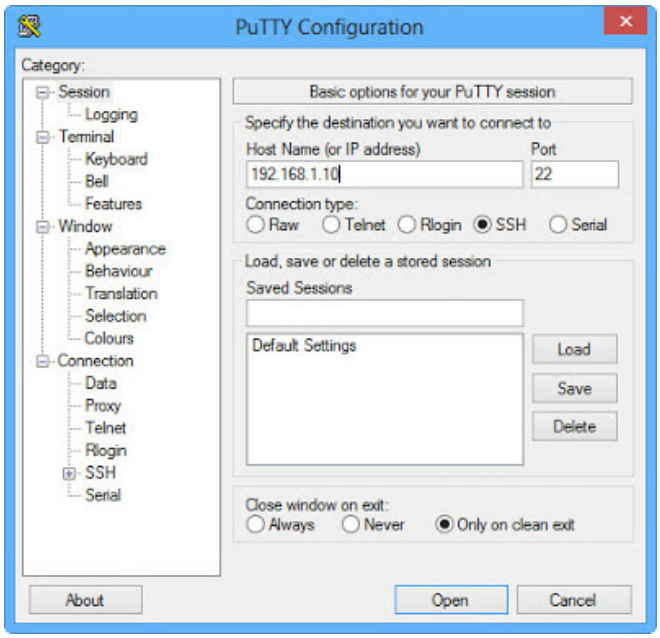
- ISDN, Mikrotik router dapat berfungsi sebagai ISDN client maupun server. Fungsi dial- up dapat diatur secara permanen ataupun dial-on- demand. IP address yang diberikan ISP dapat digunakan sebagai default route table.
- LCD, digunakan untuk menampilkan informasi kondisi sistem Mikrotik melalui layer LCD mini yang tersambung ke paralel ataupun USB.
- NTP (Network Time Protocol), digunakan untuk menyelaraskan sistem waktu komputer dalam jaringan.
- Radio LAN, Mikrotik mendukung penggunaan wireless radio LAN.
- Router Board, digunakan untuk mendukung penggunaan Mikrotik pada papan rangkaian khusus. Papan rangkaian khusus tersebut pada dasarnya merupakan computer minimum (tanpa harddisk controller, vga dan sound) dengan kartu jaringan, catu daya lebih sederhana(cukup + 12 VDC) dan performa yang sangat minimum. Router board yag dapat digunakan Mikrotik adalah router board 200 dan 500
- Routing, diperlukan jika jaringan menggunakan routing dynamic. Mikrotik dapat menggunakan RIP, OSPF, maupun BGP versi 4.
- Security, berisikan dukungan untuk keamanan komunikasi. Paket ini diperlukan oleh Mikrotik untuk menjalankan IP security(IP Sec), Secure Shell, dan untuk menjalankan Win Box pada mode aman (secure).
- Telepony, berguna untuk mengatur layanan komunikasi dengan menggunakan Voice Over IP (VoIP). Paket ini selain memberikan fungsi gatekeeper juga mendukung penggunaan beberpa hardware VoIP terpasng pada Mikrotik Router OS.
- UPS, fitur ini memudahkan administrator memonitor dan mengamankan router dari kerusakan akibat gangguan catu daya. Untuk melakukan pengamanan tersebut router akan selalu memonitor kondisi baterai UPS saat catu daya utama tidak terdsedia. Jika kondisi baterai UPS dibawah 10% maka fitur ini memerintahkan rauter telah pada kondisi hibernate dan siap untuk kembali aktif saat catu daya utama kembali.
- Mikrotik web proxy, dalam saat yang bersamaan dapat difungsikan sebagai proxy HTTP normal maupun transparant.

1.6 Cara akses Mikrotik

Perangkat Mikrotik dapat diakses dengan menggunakan berbagai media, dan cara akses Mikrotik-nya pun berbeda-beda. Ada 4 cara mengakses Mikrotik Router, antara lain :

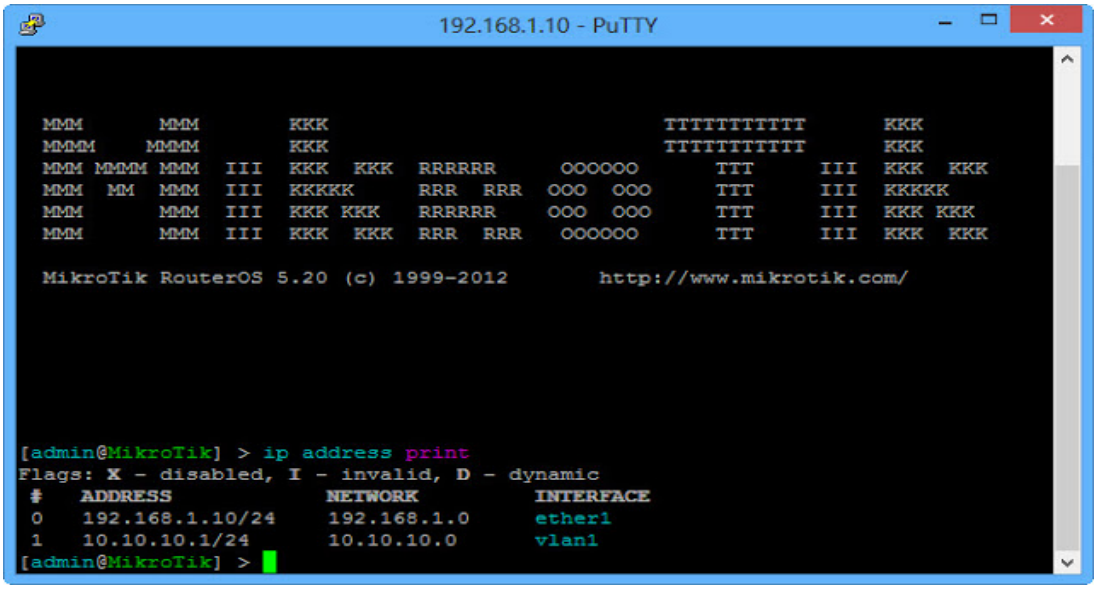
1. Via Console/Command Mikrotik

Mikrotik bisa kita akses langsung via console/shell maupun remote akses menggunakan PUTTY (www.putty.nl). Caranya tinggal masukkan alamat IP Mikrotik ke kolom Host Name nya PuTTY.



Tips Command : "Manfaatkan auto complete" (mirip bash auto complete di linux) Tekan Tombol TAB di keyboard untuk mengetahui/melengkapi daftar perintah selanjutnya. Jadi perintah yang panjang tidak perlu kita ketik lagi, cukup ketikkan awal perintah itu, lalu tekan TAB-TAB maka otomatis Shell akan menampilkan/melengkapi daftar perintah yang kita maksud.

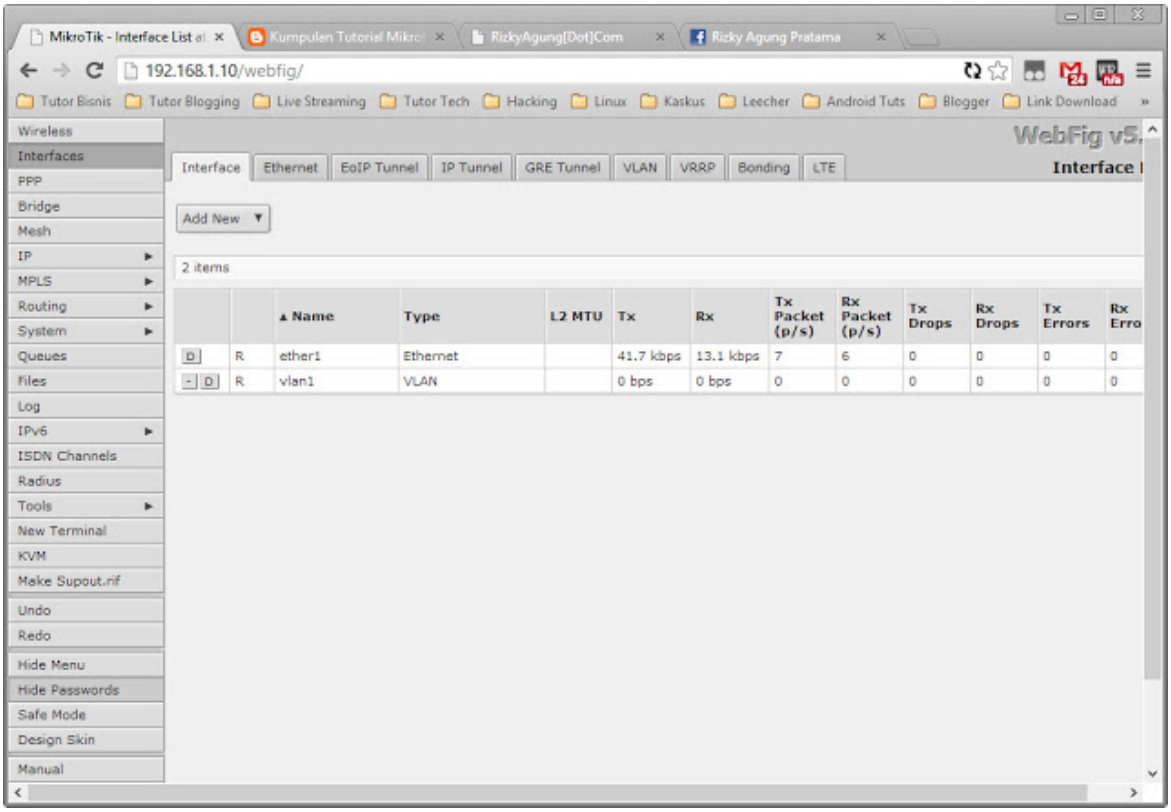
Contoh:



Cukup ketikkan Ip Fir >>> lalu tekan TAB >>> maka otomatis shell akan melengkapi menjadi Ip Firewall. Lalu ketik ".." (titik dua) untuk kembali ke sub menu diatasnya, dan ketik "/" untuk kembali ke root menu.

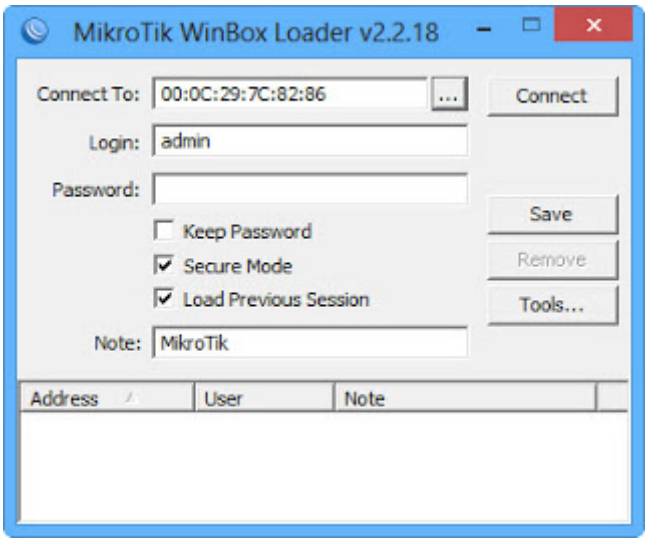
2. Via Web Browser

Mikrotik bisa juga diakses via web/port 80 pada browser. Contoh : ketik di browser IP Mikrotik kita: 192.168.1.10.

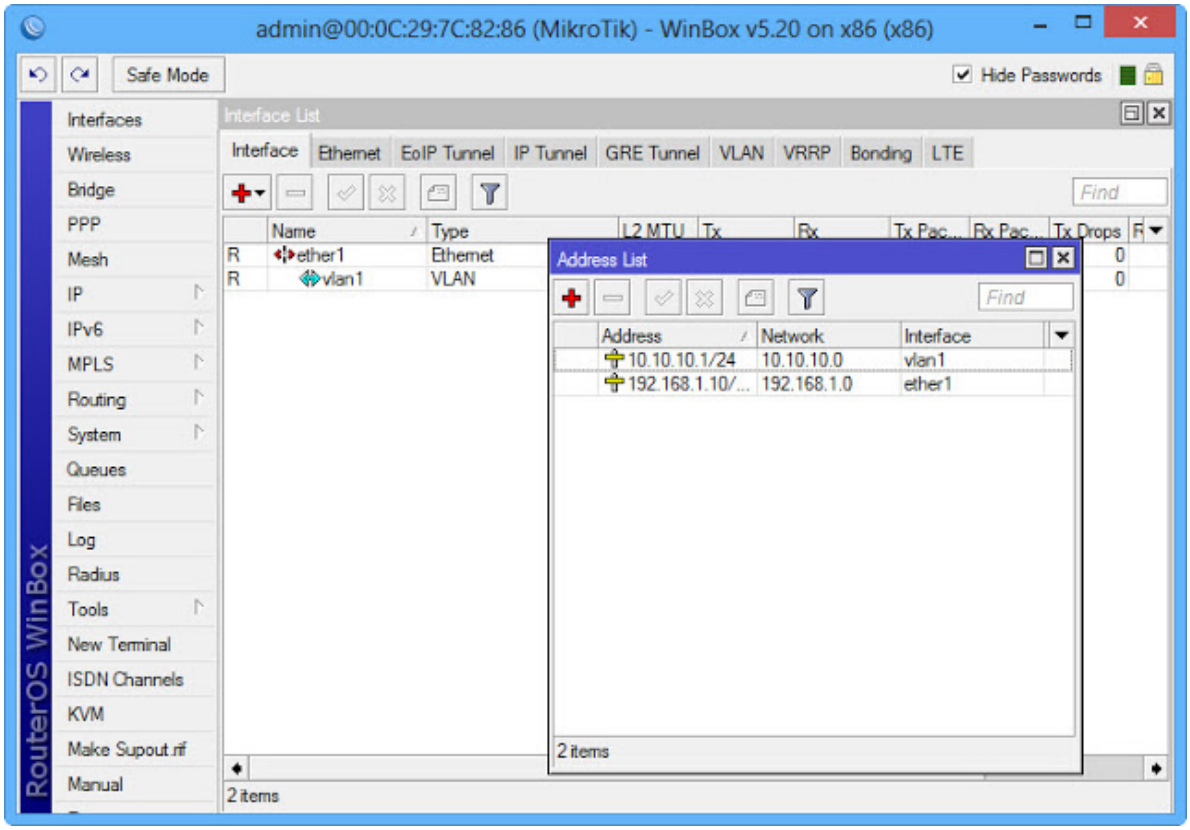


3. Via Winbox

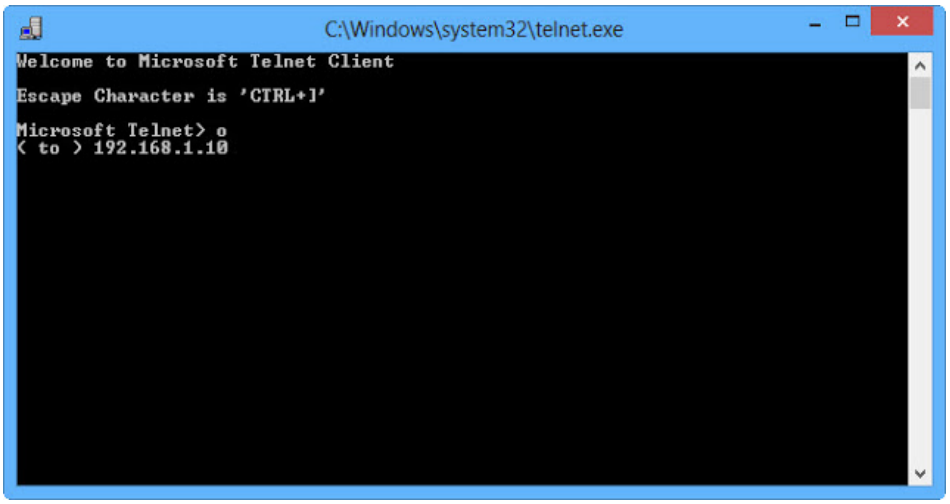
Mikrotik bisa juga diakses/remote menggunakan tool winbox (utility kecil di windows yang sangat praktis dan cukup mudah digunakan). Winbox merupakan tool untuk meremote Mikrotik yang paling populer karena selain mudah juga dapat menampilkan menu-menu pada Mikrotik secara GUI. Tampilan awal mengaktifkan winbox seperti ini :



Winbox bisa mendeteksi Mikrotik yang sudah di install asal masih dalam satu network, yaitu dengan mendeteksi MAC address dari ethernet yang terpasang di Mikrotik. Untuk bisa mengakses Mikrotik menggunakan winbox bisa dengan menggunakan IP Address Mikrotik maupun MAC Address nya.

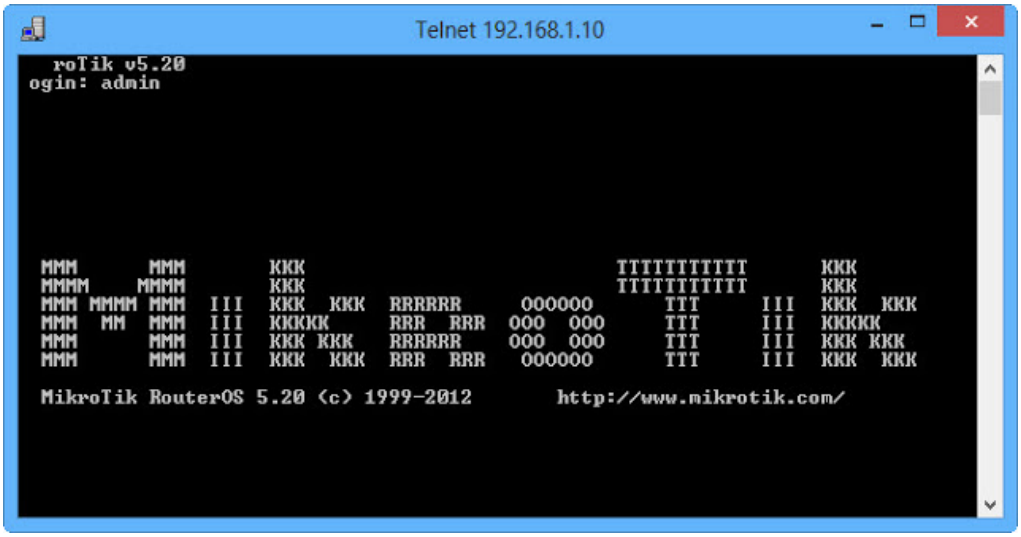


4. Via Telnet



Kita dapat me-remote Mikrotik menggunakan telnet melalui program aplikasi ”command prompt” (cmd) yang ada pada windows yang fitur Telnet nya sudah diaktifkan. Namun, penggunaan telnet tidak dianjurkan dalam jaringan karena masalah keamanannya.

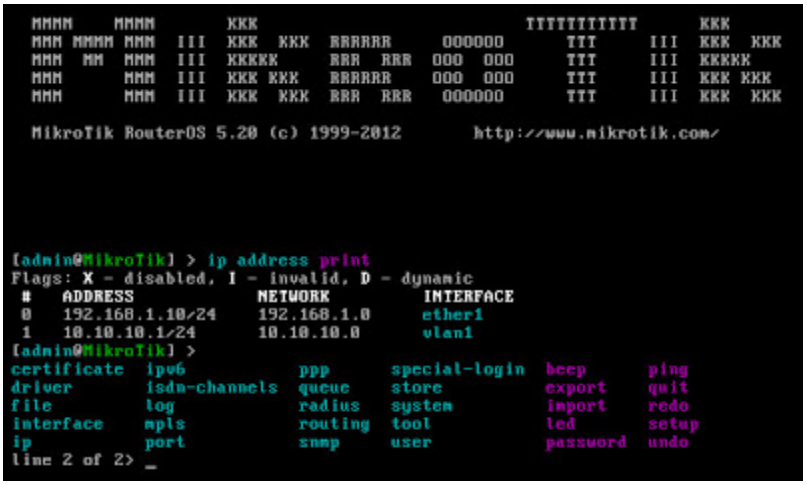
Contoh :



Itulah tadi 4 cara dalam mengakses Mikrotik. Bagi anda yang sedang belajar Mikrotik bisa mencoba-coba menggunakan masing-masing cara di atas untuk latihan. Selamat Mencoba :)

1.7 Perintah dasar Mikrotik

Bagi anda yang baru belajar menggunakan Mikrotik pasti masih bingung dengan perintah (command line) yang digunakan pada RouterOS. Padahal banyak perintah-perintah dasar Mikrotik yang penting dan wajib diketahui agar anda dapat menggunakan Mikrotik RouterOS dengan baik. Sebenarnya perintah–perintah dasar Mikrotik RouterOS tidak jauh berbeda dengan perintah dasar pada linux umumnya. Karena sebetulnya Mikrotik ini merupakan perkembangan dari kernel linux Debian.



Perintah shell Mikrotik RouterOS sama dengan linux, seperti penghematan perintah, cukup menggunakan tombol TAB di keyboard maka perintah yang panjang, tidak perlu lagi

diketikkan, hanya ketikkan awal nama perintahnya, nanti secara otomatis Shell akan menampilkan sendiri perintah yang berkenaan. Misalnya perintah IP ADDRESS di Mikrotik. Cukup hanya mengetikkan IP ADD spasi tekan tombol TAB, maka otomatis shell akan mengenali dan menterjemahkan sebagai perintah IP ADDRESS.

Berikut ini merupakan perintah perintah dasar Mikrotik yang umum digunakan :

1. Perintah untuk shutdown dan restart computer , ketikkan :

[admin@Mikrotik]>system shutdown (Untuk shutdown komputer)

[admin@Mikrotik]>system reboot (Untuk restart computer)

[admin@Mikrotik]>system reset (Untuk meret konfigurasi yang sudah dibuat sebelumnya). Dan perlu diperhatikan bahwa perintah – perintah tersebut harus dilakukan pada direktori admin.

2. Perintah untuk merubah nama mesin Mikrotik , ketikkan :

[admin@Mikrotik]>/system identity

[admin@Mikrotik]>system identity > set name=proxy

Untuk melihat hasil konfigurasi , ketikkan “print” atau “pr”

Lalu console berubah menjadi **[admin@proxy]**

3. Perintah merubah password mesin Mikrotik , ketikkan

[admin@proxy]>/ password

[admin@proxy]password>old password (jika sebelumnya anda belum mengeset password maka ketikkan kosong)

[admin@proxy]password>new password :…….(ketikkan password yang baru)

[admin@proxy]password>retype new password: ……..(masukkan sekali lagi passowrdnya)

Sebagai contoh :

Jika password lama kosong dan password baru ABCD, maka perintahnya adalah sebagai berikut :

[admin@proxy]>/password

[admin@proxy]password>old password

[admin@proxy]password>new password ABCD

[admin@proxy]password>retype new password ABCD

4. Perintah untuk melihat kondisi interface pada Mikrotik Router :

[admin@Mikrotik] > interface print

Flags: X – disabled, D – dynamic, R – running

#	NAME	TYPE	RX-RATE	TX-RATE	MTU
0	R ether1	ether	0	0	1500
1	R ether2	ether	0	0	1500

[admin@Mikrotik]>

Jika interfacenya ada tanda X (disabled) setelah nomor (0,1), maka periksa lagi etherned cardnya, seharusnya R (running).

a. Mengganti nama interface

[admin@Mikrotik] > interface(enter)

b. Untuk mengganti nama Interface ether1 menjadi Public (atau terserah),maka:

[admin@Mikrotik] interface> set 0 name=Public

c. Begitu juga untuk ether2, misalkan namanya diganti menjadi Local, maka

[admin@Mikrotik] interface> set 1 name=Local

d. atau langsung saja dari posisi root direktori, memakai tanda "/", tanpa tanda kutip

[admin@Mikrotik] > /interface set 0 name=Public

e. Cek lagi apakah nama interface sudah diganti.

[admin@Mikrotik] > /interface print

Flags: X – disabled, D – dynamic, R – running

#	NAME	TYPE	RX-RATE	TX-RATE	MTU

0	R Local	ether	0	0	1500
1	R Public	ether	0	0	1500

5. Perintah untuk melihat paket sofware Mikrotik OS :

[admin@proxy]>/system package

[admin@proxy]system package><ketikkan print atau pr>

Dengan perintah di atas maka akan tampil paket softwore yang ada dalam Mikrotik OS
Contoh :

[admin@Mikrotik system package> pr

Flags : x – disabled

#	Name	VERSION	SCHEDULED
0	X routing – test	2.9.27	
1	dhcp	2.9.27	
2	radiolan	2.9.27	
3	user-menejer	2.9.27	
4	X webproxy-test	2.9.27	
5	arlan	2.9.27	
6	isdn	2.9.27	
7	hotspot-fix	2.9.27	
8	ppp	2.9.27	
9	wireless	2.9.27	
10	web-proxy	2.9.27	
11	hotspot	2.9.27	
12	advanced-tools	2.9.27	

13 security 2.9.27

14 Telephony 2.9.27

15 routing 2.9.27

16 synchronous 2.9.27

17 system 2.9.27

18 routerboard 2.9.27

19 rstp-bridge-test 2.9.27

20 X wireless-legecy 2.9.27

Untuk melihat lebih detailnya, ketikan :

[admin@proxy]system package > pr detail fl gs : x – disabled

0 x name=”routing-test” version=”2.9.27” build – time =jul/03/2006 10:57:53 scheduled

1 name =”system”version =”2.9.27” build – time=jul/03/2006 10 :56:37 schedule

2 name =”system”version =”2.9.27” build – time=jul/03/2006 10 :56: 44 schedule

3 name=”web-proxy” version=”2.9.27” build-time=jul/03/2006 10:`58 :03 schedule

4 name=”advanced –tools” version=”2.9.27” build –time=jul /03/2006 10:56 : 41 scheduled=””

5 name=”dhcp” version=”2.9.27” build-time=jul/03/2006 10:56:45 scheduled=””

6 name =”hotspot”version=”2.9.27”build-time=jul/03/2006 10:56:58 scheduled=””

7 x name=”webproxy-test” version=”2.9.27” build-time=jul / 03 /2006 10:57:52 scheduled

8 name=”routerboard” version =”2.9.27” build-time=jul / 03 / 2006 10: 57 : 17 –[q quit | D dump | up | down]

6. Perintah setting IP address pada mesin Mikrotik OS :

[admin@proxy]> ip address

[admin@proxy]ip address> Add interface=<nama interface>anddress= (ketikkan IP address/subnet mask interface)

Contoh :

Jika nama interfacenya “lan” dan IP address yang dikehendaki : 192.168.8.1 dan subnet mask : 255.255.255.0, maka perintahnya sebagai berikut

[admin@proxy]>/ ip address

[admin@proxy]ip address > Add interface=lan address = 192.168.8.1/24

7. Memeriksa IP Address

[admin@proxy]> ip address print

8. Menghapus IP Address

[admin@proxy]>ip address remove 1

INGAT: angka 1 adalah nomor index dari output interface print. Perhatikan baik-baik sebelum menghapus IP Address.

9. Mengedit atau mengubah IP Address

[admin@proxy]> ip address edit 1

10. Menonaktifkan IP Address

[admin@proxy]>ip address disable 1

BAB II
INSTALASI DAN KONFIGURASI DASAR MIKROTIK

Tujuan:

- Peserta dapat menginstal sendiri RouterOS
- Peserta mampu memberikan licence pada RouterOS
- Peserta mampu mengkonfigurasi dasar pada Mikrotik.

2.1 Instalasi Mikrotik RouterOS

2.1.1 Instalasi dengan Netinstall

Instalasi Mikrotik dapat dilakukan dengan beberapa macam cara. Sebelumnya juga sudah pernah dibahas tentang apa saja cara install Mikrotik Salah satu cara install Mikrotik yaitu dengan Netinstall.

Netinstall adalah program yang berjalan pada komputer Windows yang memungkinkan Anda untuk menginstal Mikrotik RouterOS ke PC atau ke RouterBoard melalui jaringan Ethernet. Netinstall juga digunakan untuk menginstal ulang RouterOS dalam kasus di mana instalasi sebelumnya gagal, menjadi rusak atau password akses hilang.

Perangkat Anda harus mendukung boot dari ethernet, dan harus ada link ethernet langsung dari komputer netinstall ke perangkat target. Semua RouterBOARD dukungan untuk PXE boot jaringan, harus diaktifkan baik di dalam menu RouterOS "Routerboard" jika RouterOS yang beroperasi, atau dalam pengaturan bootloader. Untuk ini, Anda akan membutuhkan kabel serial.

Untuk perangkat RouterBOARD tanpa port serial, dan tidak ada akses RouterOS, tombol reset juga dapat memulai modus PXE boot. Lihat RouterBOARD petunjuk PDF untuk rincian. Misalnya RB750 PDF Netinstall juga dapat langsung menginstal RouterOS pada disk (USB / CF / IDE / SATA) yang terhubung ke mesin Windows netinstall. Setelah instalasi hanya memindahkan disk untuk mesin Router dan boot dari itu.

Netinstall bisa digunakan untuk mereset password Mikrotik ketika kita lupa password Mikrotik nya dan juga ketika terjadi kegagalan sistem pada proses instalasi

sebelumnya. Lalu kenapa harus menggunakan Netinstall? Kenapa tidak langsung upgrade saja terus di reset?

Sekarang langsung saja kita coba cara install Mikrotik dengan netinstall.Bagaimana cara melakukan NetInstall? Perlengkapan :

1. Software NetInstall (download dari http://Mikrotik.co.id/download.php)

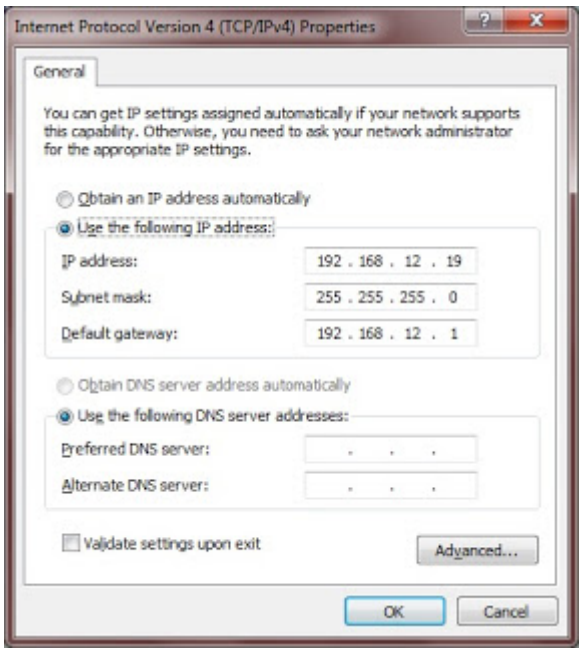
2. Kabel UTP

3. File software Mikrotik sesuai dengan jenisnya (x86,mpsbe,mipsle)

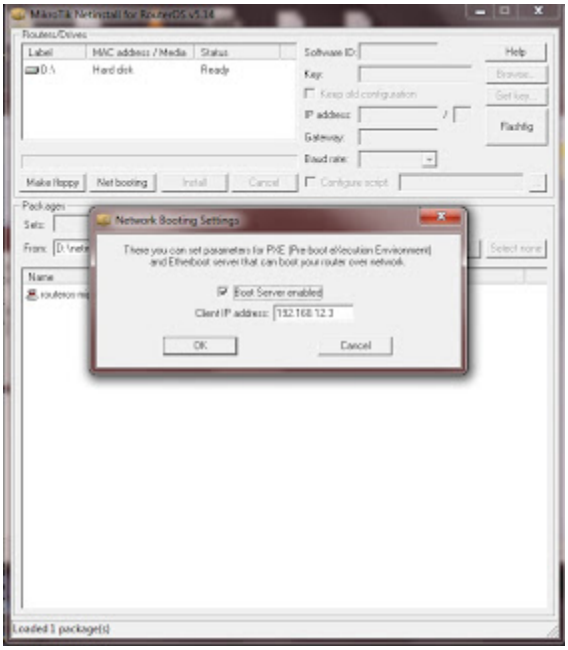
Dibeberapa literasi harus ada kabel serial, namun saya telah mencoba tanpa kabel serial dan berhasil. Fungsi kabel serial ini nantinya adalah untuk merubah alur booting dari device yang secara default booting dari disk internal menjadi boot dari network.

- Download program Netinstall dari halaman http://Mikrotik.co.id/download.php
- Download combined package routerOS dari halaman http://Mikrotik.co.id/download.php, sesuaikan dengan tipe router anda dan versi yang ingin anda gunakan.

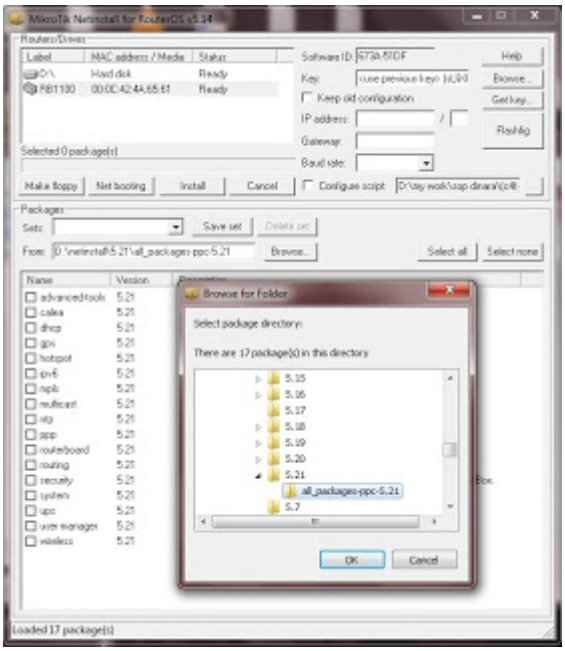
Setting PC anda menggunakan IP statik. (misalnya: IP 192.168.12.19 netmask 255.255.255.0) dan tancapkan kabel ethernet dari PC anda ke port ether1 router anda.



Jalankan program Netinstall dan tekan tombol Net booting, kemudian anda aktifkan / centang Boot Server enabled, lalu isikan Client IP address dengan IP yang satu subnet dengan IP statik PC anda (misalnya : 192.168.12.3) dan tekan tombol OK.



Tekan tombol browse lalu pilih folder dimana anda menyimpan file *.npk yang sudah anda download di langkah ke-2. dalam kasus ini karena yang akan saya net install adalah untuk jenis RB1000 series maka packet yang digunakan adalah mipsle jika yang akan anda netinstall adalah jenis RB400 series atau RB750 series maka gunakan yang mipsbe



- Cabut power adaptor router anda
- Tekan tombol reset kecil yang ada di router anda, dan anda tahan.
- Sambil tetap ditahan, anda nyalakan power adaptornya
- Tunggu beberapa saat, nanti di program Netinstall anda akan muncul mac-address dari router anda.
- Lepaskan tombol reset, kemudian anda tekan mac-address router anda di program Netinstall dan pilih paket yang akan anda gunakan untuk instalasi (tercentang)
- Tekan tombol install, nanti proses instalasi akan ditampilkan di program Netinstall.
- Jika proses instalasi sudah selesai, tombol Install akan berubah menjadi reboot, silahkan anda tekan tombol tersebut dan proses instalasi sudah selesai.

Catatan :
Jangan terlalu memaksa/kuat untuk menekan tombol reset karena bisa mengakibatkan tombol reset rusak. Jika router anda memiliki port serial, kami sarankan anda gunakan kabel serial untuk merubah boot-device ke port ethernet

Proses Instalasi menggunakan netinstall akan menghapus semua konfigurasi router anda, sehingga default username=admin, password=(kosong tidak perlu diisi)

2.1.2 Instalasi dengan CD menggunakan file .iso

Jika anda membeli RouterBoard Mikrotik biasanya sudah langsung bisa digunakan tanpa perlu lagi melakukan instalasi RouterOS, tinggal memasukkan lisensi saja. Namun jika anda tidak ingin menggunakan RouterBoard atau hanya ingin menggunakan PC sebagai Mikrotik tentunya anda harus melakukan instalasi Mikrotik ke PC dulu. Nah, ada beberapa cara install Mikrotik ke PC. Mikrotik dapat di install di PC dengan menggunakan beberapa cara, yaitu:

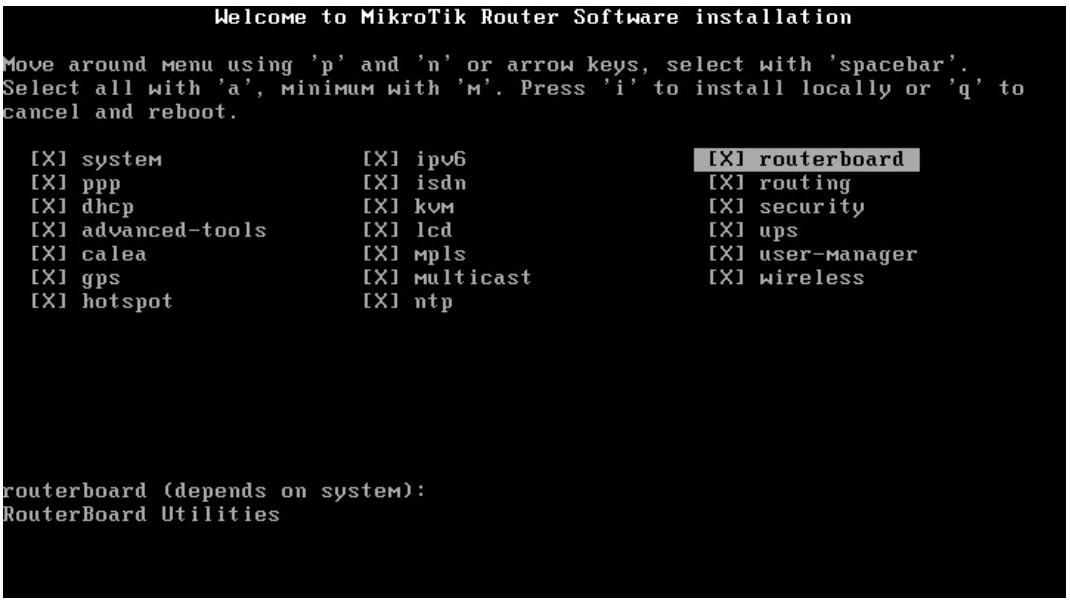
1. ISO Image: menggunakan Compact Disc (CD) instalasi. Silahkan download file berekstensi .ISO yang tersedia dan kamu harus “membakarnya” ke dalam media CD kosong.
2. NetInstall; melalui jaringan komputer (LAN) dengan Satu Disket, atau menggunakan Ethernet yang mendukung proses menyalakan komputer (booting)

komputer melalui Ethernet Card. NetInstall dapat dilakukan pada sistem operasi Windows 95/98/NT4/2000/XP.

3. Mikrotik Disk Maker: membutuhkan beberapa buah disket ukuran 3,5″ yang nant inya akan disalin pada hard disk saat instalasi dilakukan. Dengan menggunakan tools FloppyMaker.exe.

Dari ketiga cara tersebut, cara pertama yang menggunakan CD ISO image yang paling populer dan paling banyak digunakan. Jadi kali ini kita akan membahas cara yang pertama dulu. Cara instalasi Mikrotik menggunakan ISO image memang cukup mudah dilakukan. Anda hanya perlu mendownload file ISO Mikrotik RouterOS, burn ke CD, boot ke CD itu dan install Mikrotik nya. Oke Sekarang kita akan mulai bahas cara install Mikrotik RouterOS di PC, silahkan simak cara berikut ini :

- Download file ISO Mikrotik nya. Kalian bisa download disini http://Mikrotik.co.id/download.php dan Burn file ISO nya ke CD.
- Masukkan cd Mikrotik ke dalam cd/dvd room.
- Setting bios komputer anda, pada booting awal (first boot)nya adalah cd/dvd room anda.
- Setelah di setting maka komputer anda akan booting pertama kali ke cd/dvd room anda. Jika berhasil maka akan muncul tampilan seperti dibawah ini.



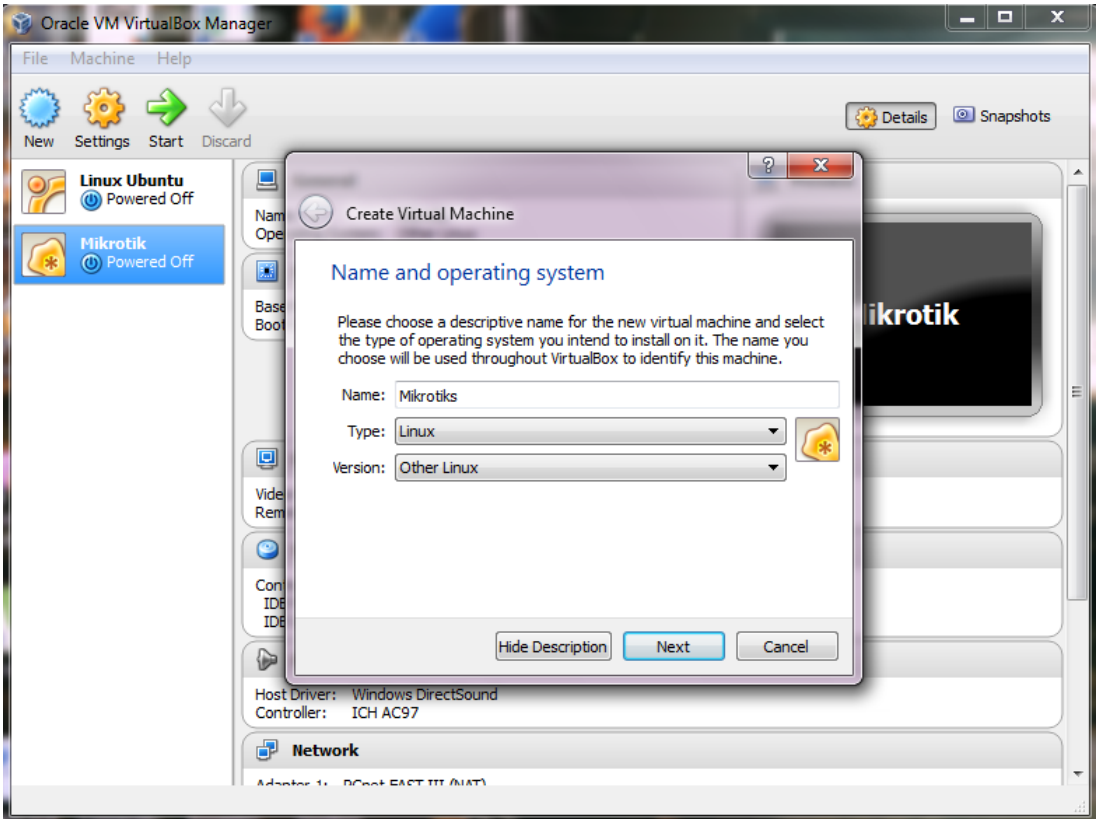
2.1.3 Instalasi RoutersOS pada VirtualBox

Disini kita menggunakan VirtualBox untuk menjalankan RouterOS Mikrotik secara virtual. Tujuannya adalah agar kita tetap bisa belajar dan oprek-oprek Mikrotik tanpa harus punya RouterBoard nya. Langsung saja, langkah-langkah nya sebagai berikut.

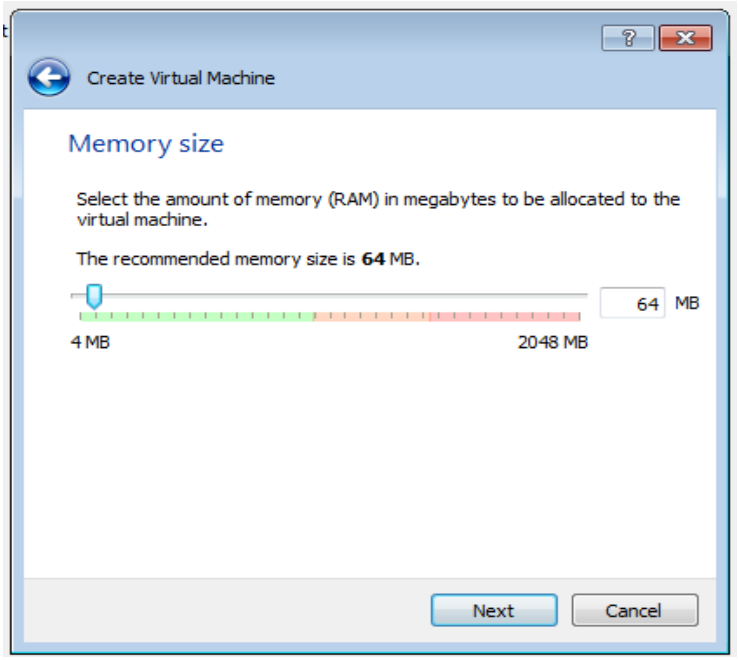
Langkah Instalasi :

1) Langkah awal yang harus diambil adalah dengan double klik pada Icon Oracle VM VirtualBox

2) Maka akan muncul tampilan awal pada Oracle VM VirtualBox seperti gambar dibawah ini yang siap untuk digunakan, lalu klik New kemudian akan muncul kotak dialog dan anda dapat mengisikan Name dengan nama Virtual Machine, disini saya mengisikan dengan nama "Mikrotik". Lalu pilih Other untuk sistem operasinya dan pilih Other untuk versinya, jika sudah selesai pilih Next .

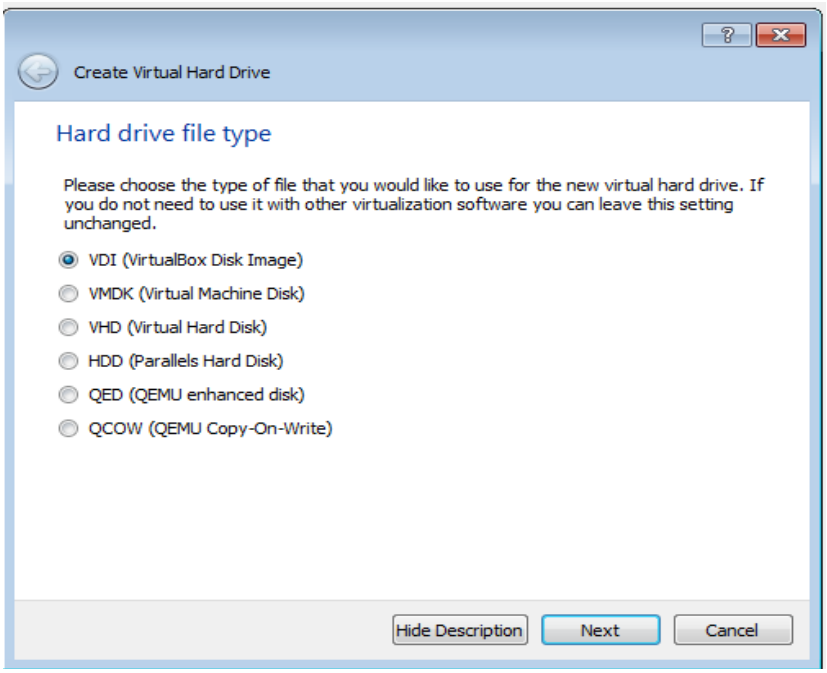


3) Langkah selanjutnya, akan muncul kotak dialog untuk mengatur berapa besar RAM yang akan digunakan untuk mesin virtual kita. Saya disini mengalokasikan sekitar 64 MB, lalu klik Next

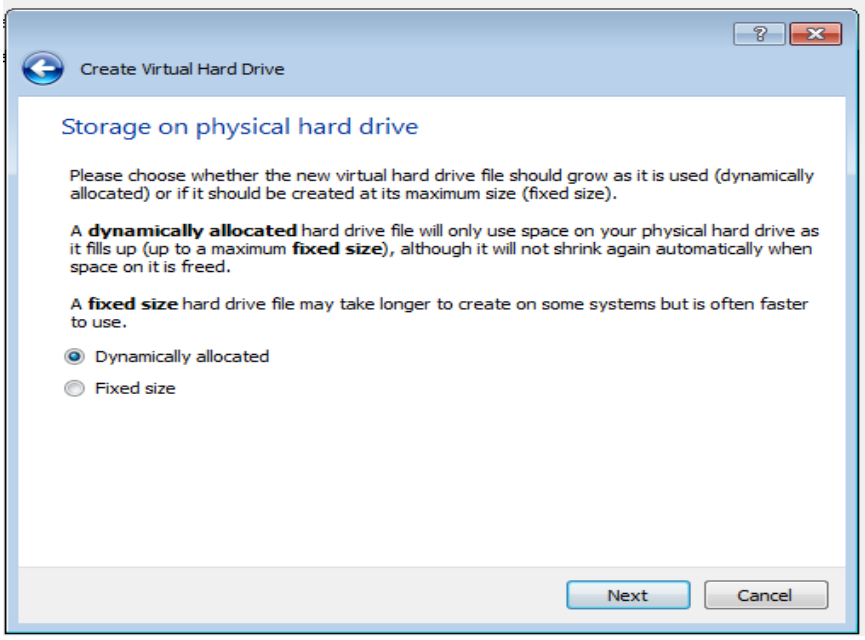


4) VirtualBox menyediakan opsi untuk membuat hasrddisk baru atau menggunakan harddisk yang ada sebagai Disk Start-Up. Secara default, sudah diatur untuk membuat Harddisk baru. Maka biarkan saja secara default, lalu Next

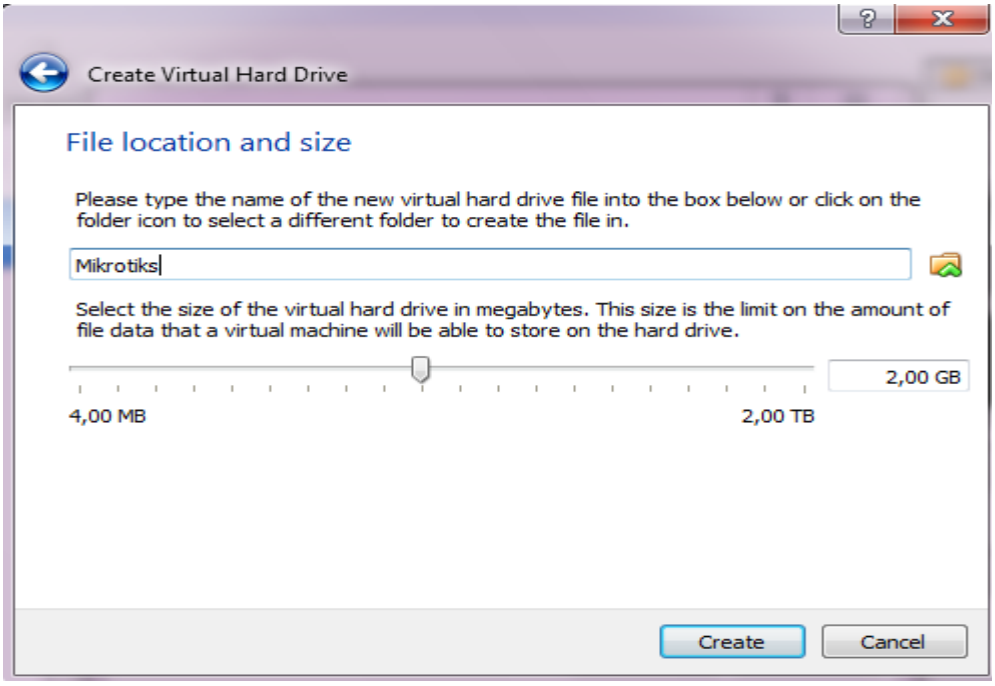
5) Pada kotak dialog selanjutnya, pilih VDI (Virtualbox Disk Image), lalu pilih Next



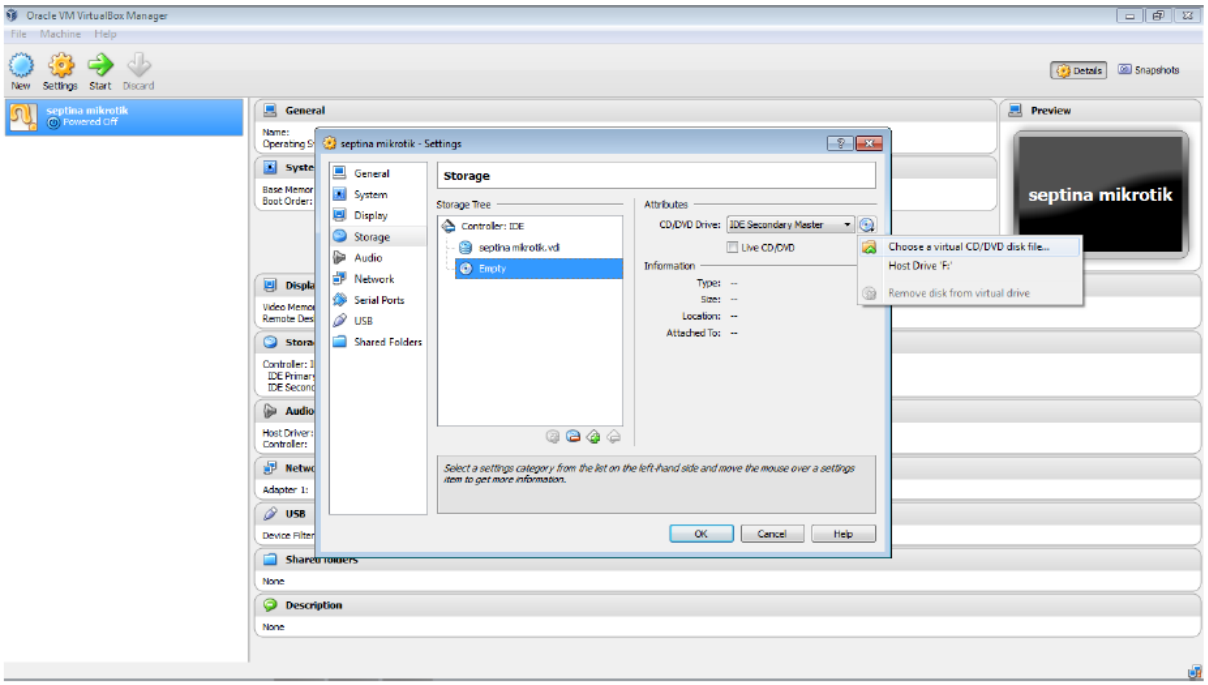
6) Kemudian pada kotak dialog selanjutnya terdapat dua opsi untuk memilih ukuran Fixed size (ukuran tetap) atau Dynamically allocates (ukuran dinamis) yang dialokasikan sesuai kebutuhan anda, kalau saya memilih ukuran Dynamically alocated, lalu pilih Next



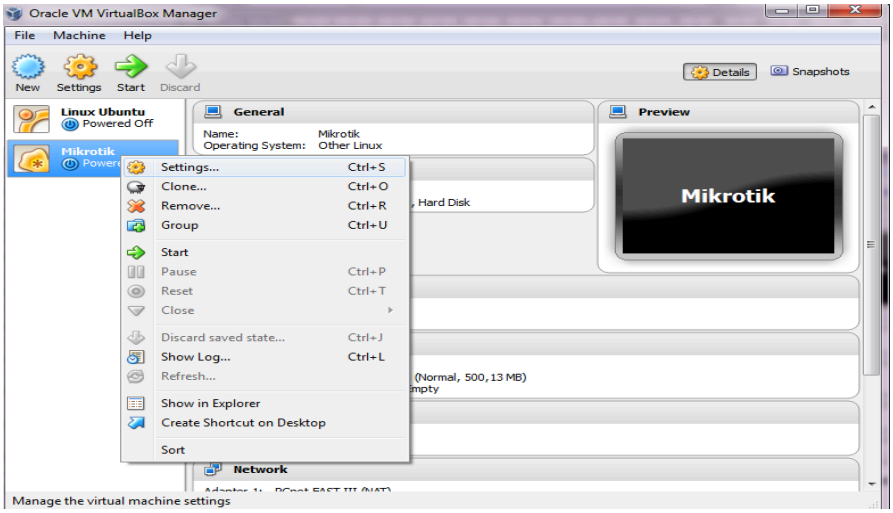
7) Pada kotak dialog berikutnya untuk mengatur ukuran Virtual Disk, namun secara default VirtualBox mengalokasikan ruang disk 2GB untuk sistem baru. Lalu pilih Create



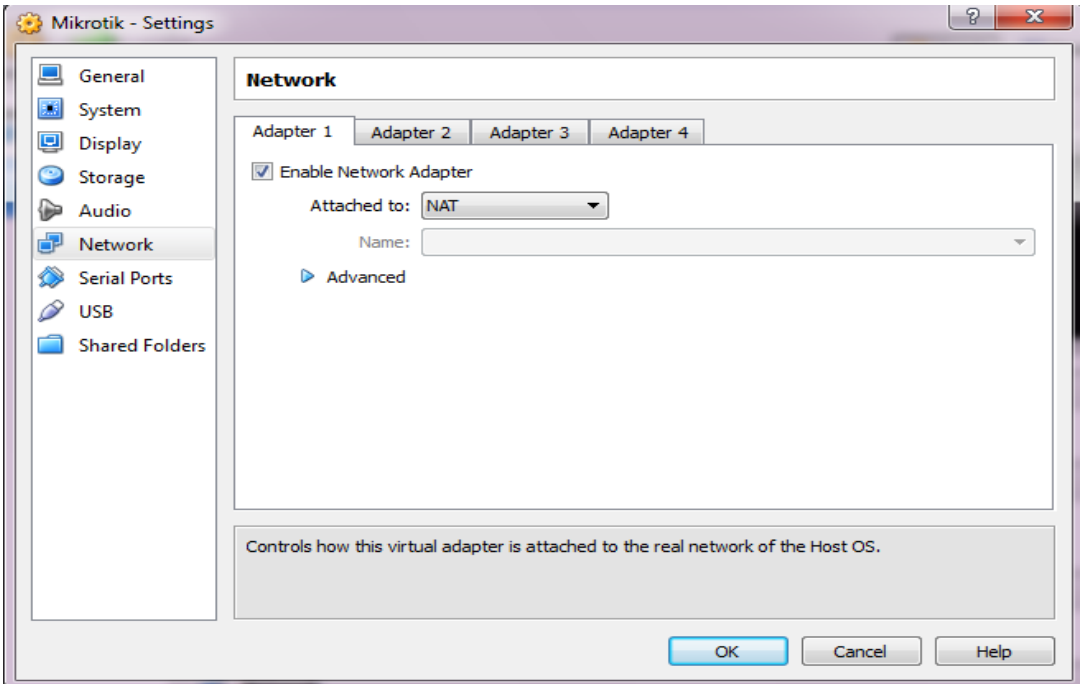
8) Selanjutnya mesin Virtual siap digunakan, lalu pilih Setting. Maka akan muncul jendela, lalu pilih Storage dan klik pada Controller IDE , gambar Disk (empty) kemudian Add Master Mikrotik lalu klik pada gambar Disk dan pilih Choose a virtual CD/DVD disk file untuk mencari dimana lokasi master Mikrotiknya



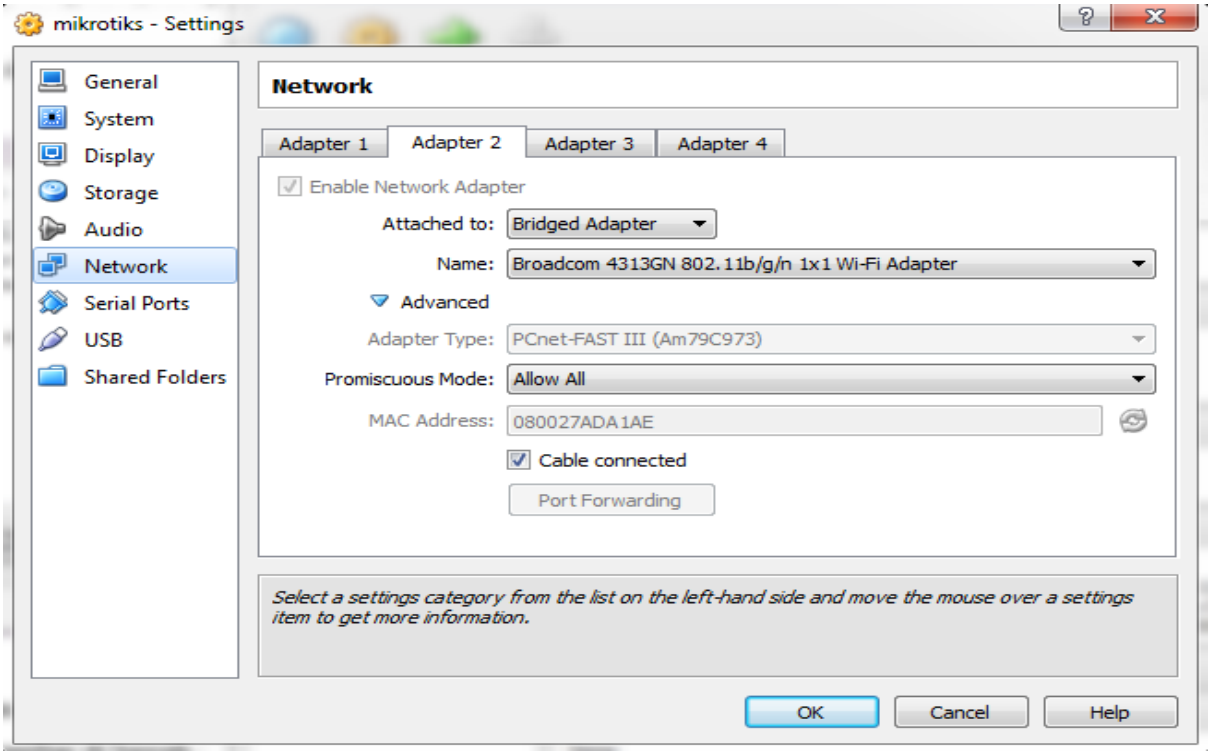
Sebelum melakukan Instalasi RoutersOS terlebih dahulu esetting slot Ethernet pada Virtual Mikrotik. Klik kanan pada Mikrotik lalu Settings :



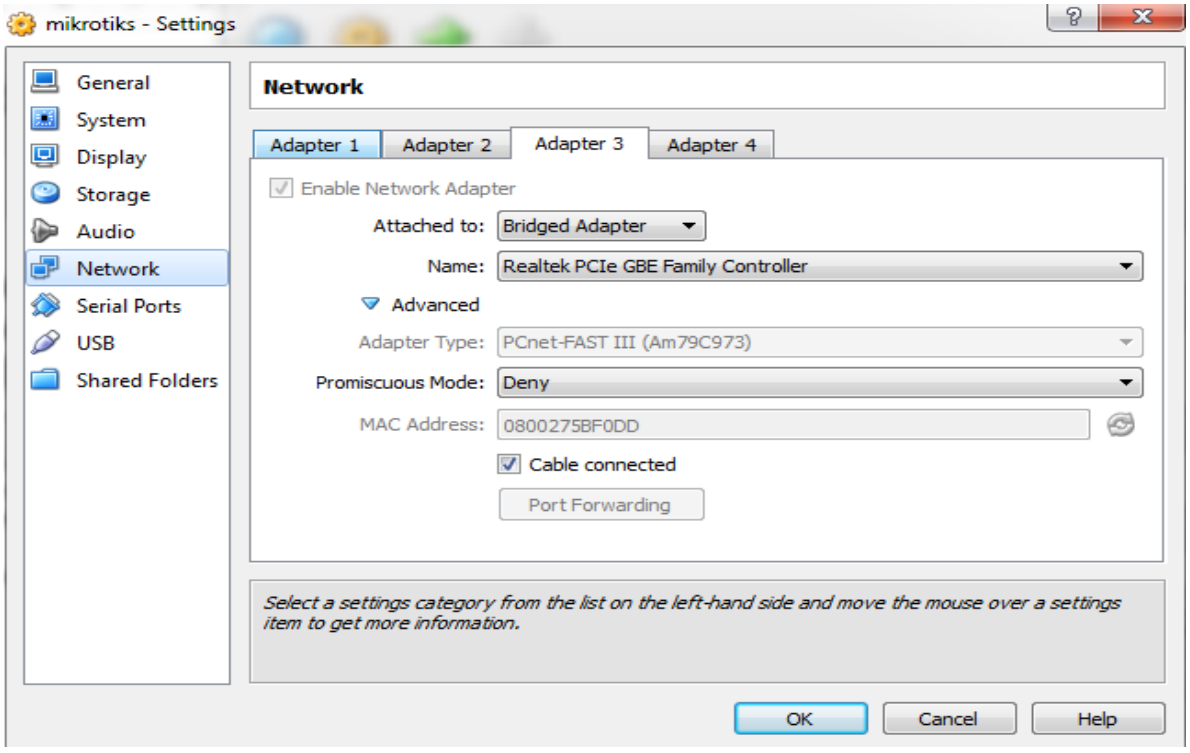
Akan tampil seperti gambar di bawah, klik pada tab Network di sebelah kiri, lalu Setting Adapter 1 Sebagai NAT (sumber internet Mikrotik).

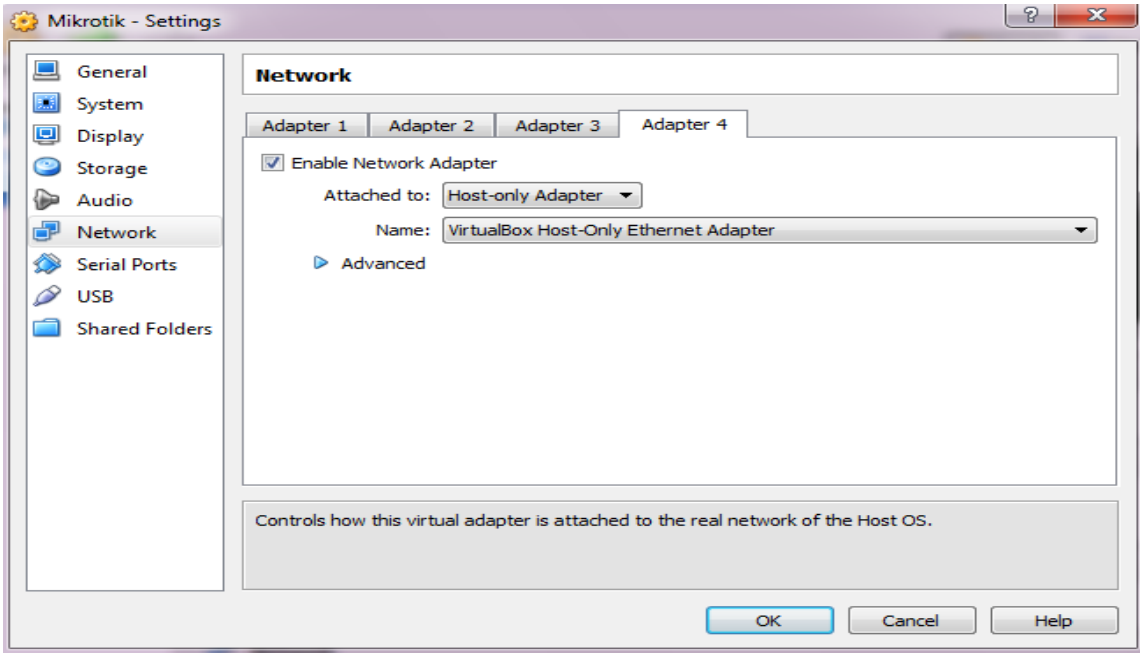


Selanjutnya pada Adapter 2, aktifkan dengan menceklist enable Network lalu ubah Attached to Bridged Adapter dan sesuaikan adapter networknya ,

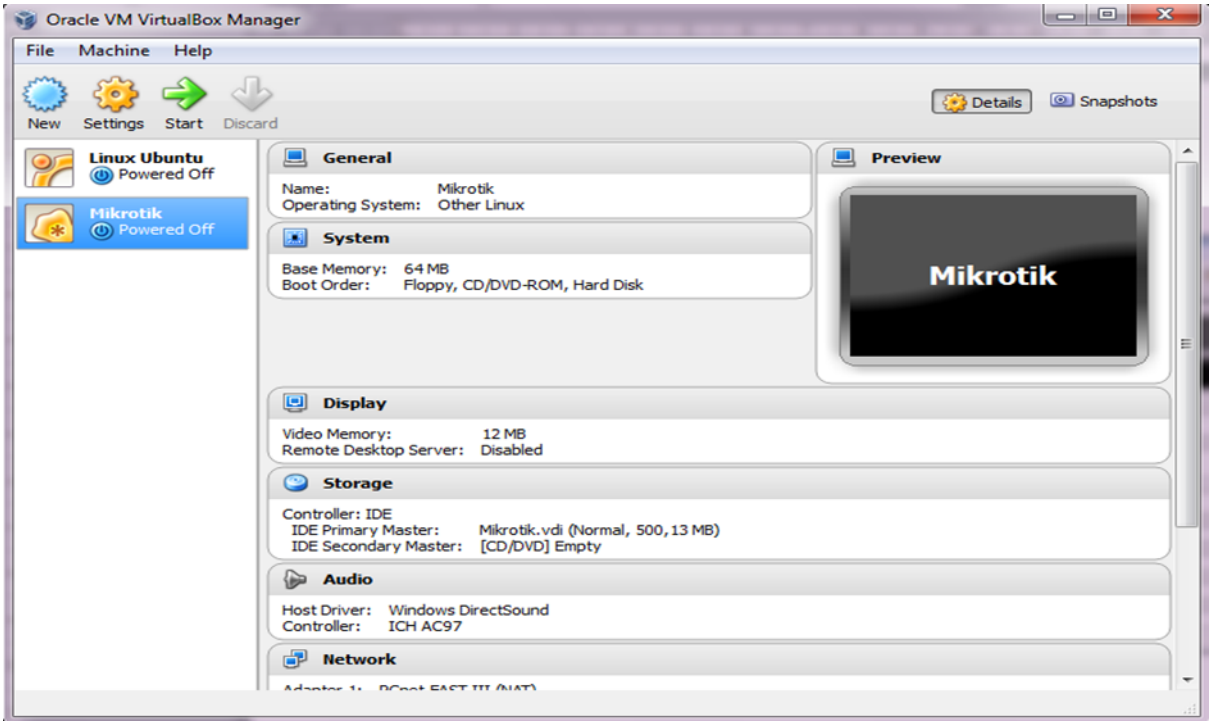


Pada Adapter 3 juga pilih Bridged Adapter dan pada Adapter 4 sebagai Hosts-only Adapter (Agar dapat di akses oleh Winbox). Seperti pada gambar di bawah :

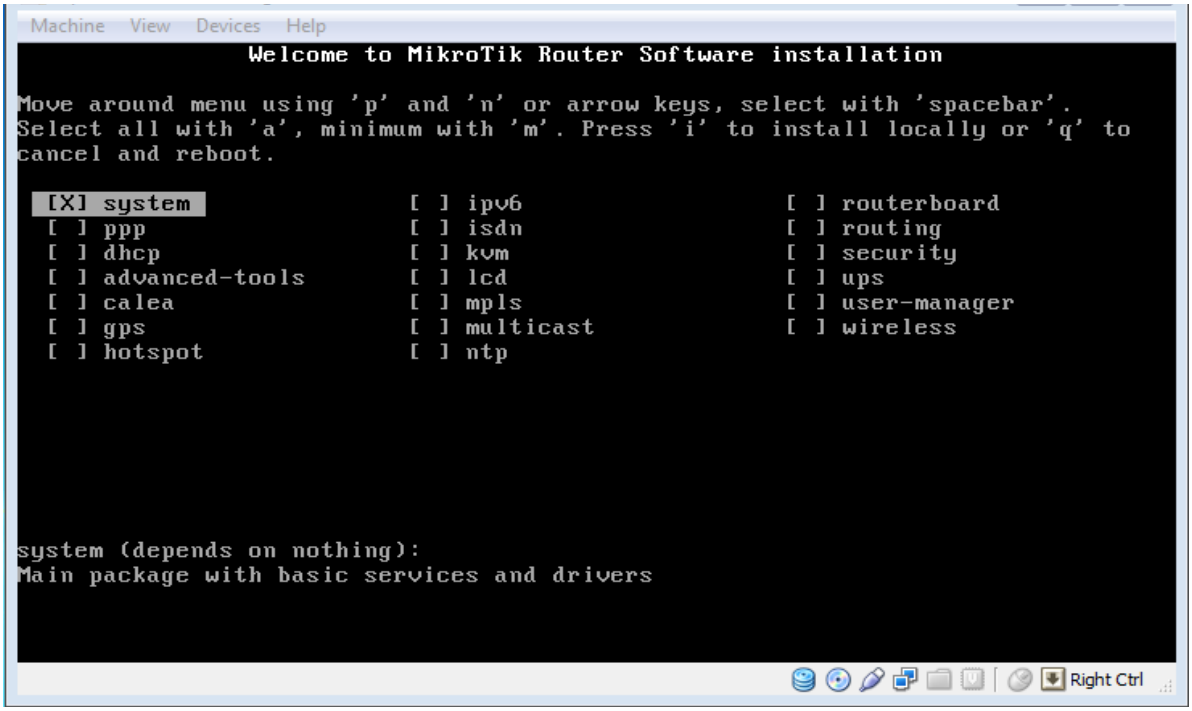




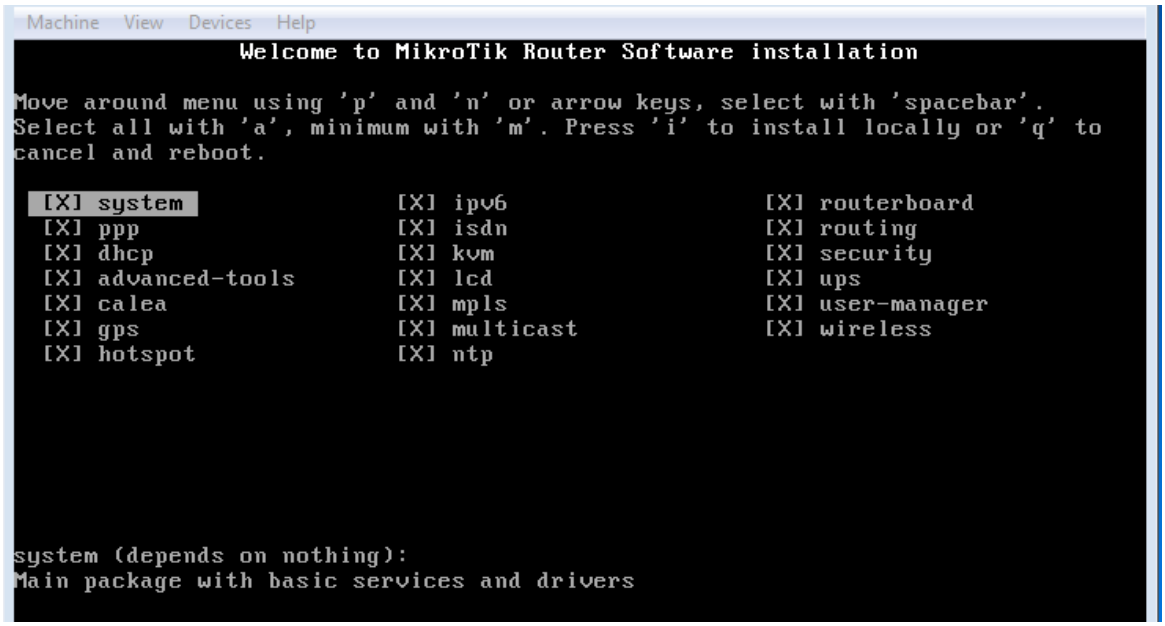
9) Selanjutnya klik Start untuk memulai menginstalasi Mikrotiknya

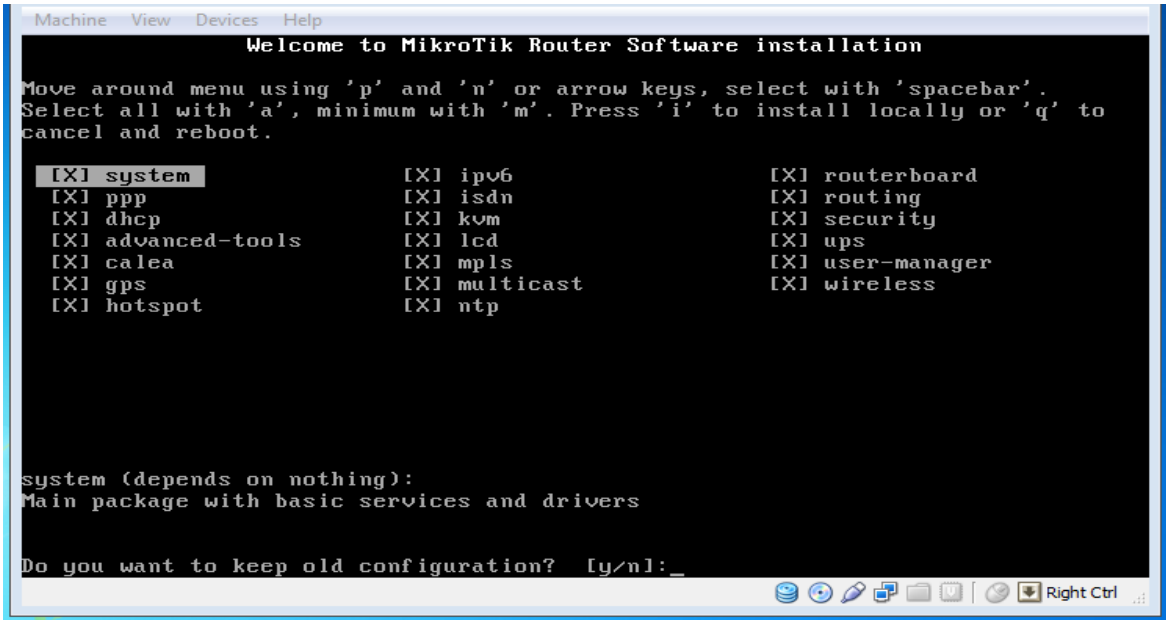


10) Kemudian akan muncul kotak dialog “Welcome to Mikrotik Router Software Installation”

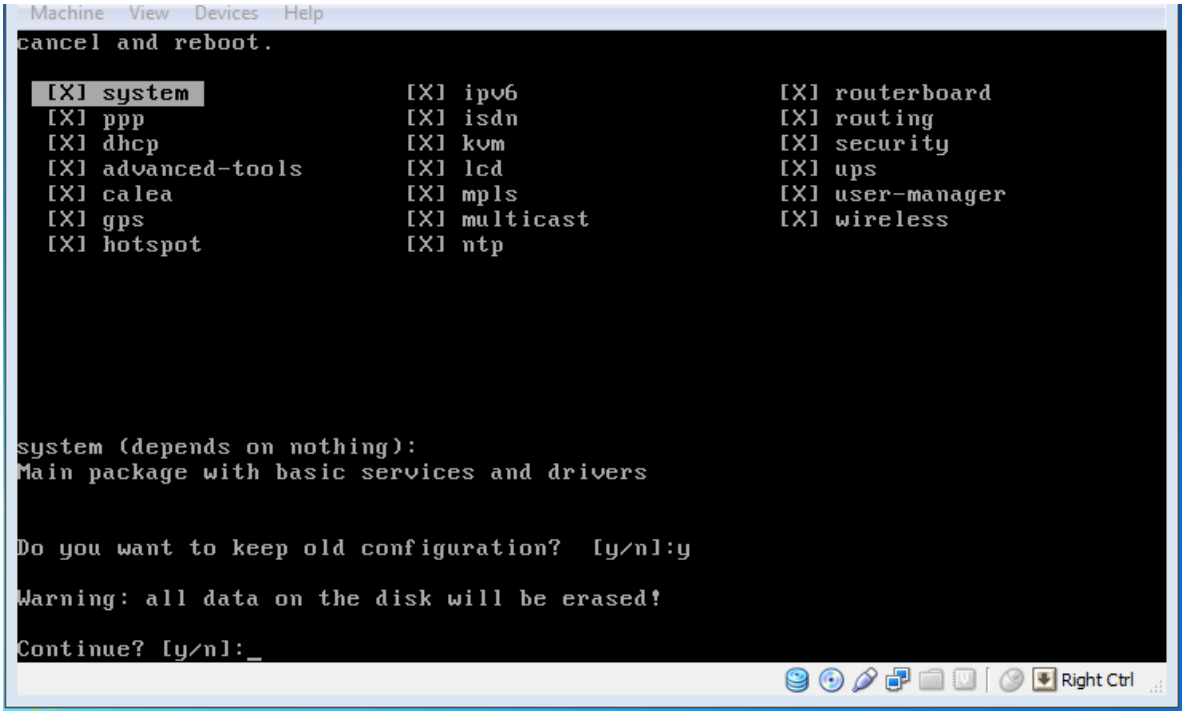


11) Lalu ketikkan “a” untuk memberikan tanda pada semua opsi yang disediakan

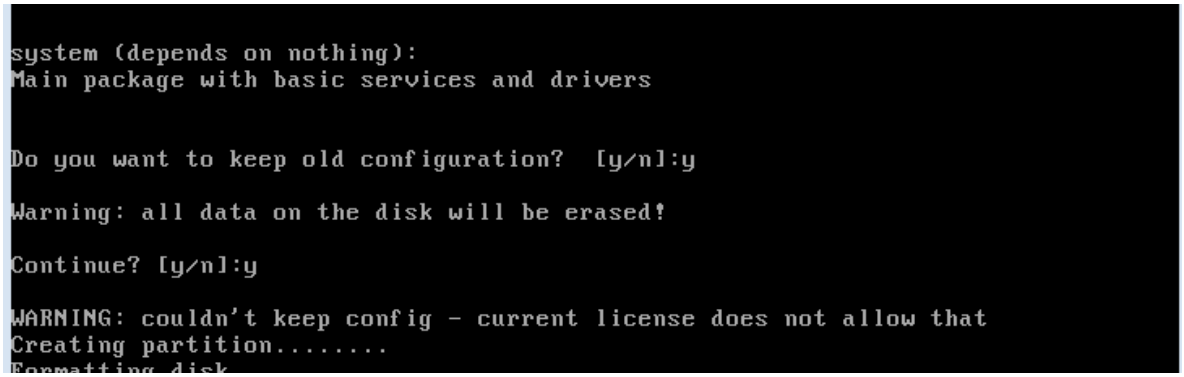



Machine View Devices Help
Welcome to MikroTik Router Software installation
Move around menu using 'p' and 'n' or arrow keys, select with 'spacebar'.
Select all with 'a', minimum with 'm'. Press 'i' to install locally or 'q' to
cancel and reboot.
[X] system
[X] ppp
[X] dhcp
[X] advanced-tools
[X] calea
[X] gps
[X] hotspot
[X] ipv6
[X] isdn
[X] kvm
[X] lcd
[X] mpls
[X] multicast
[X] ntp
[X] routerboard
[X] routing
[X] security
[X] ups
[X] user-manager
[X] wireless
system (depends on nothing):
Main package with basic services and drivers
Do you want to keep old configuration? [y/n]:_
Right Ctrl

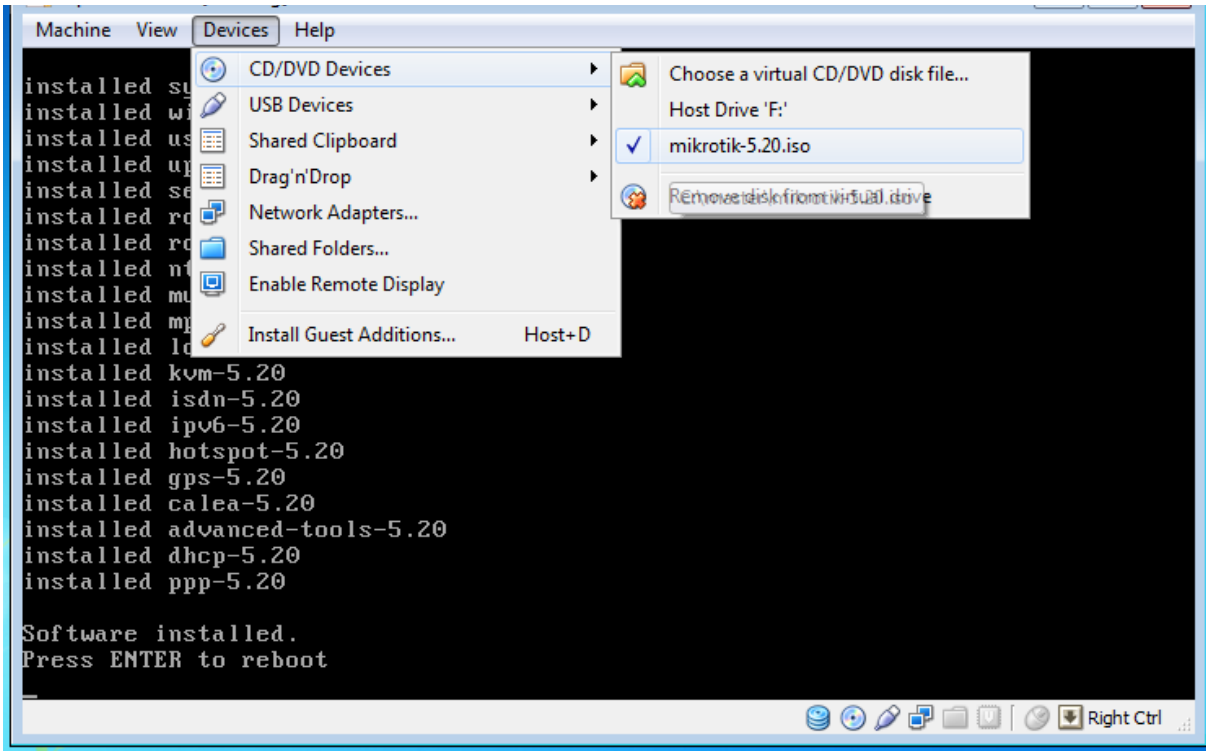
12) Setelah itu, untuk melanjutkan proses instalasi ketikkan “y”

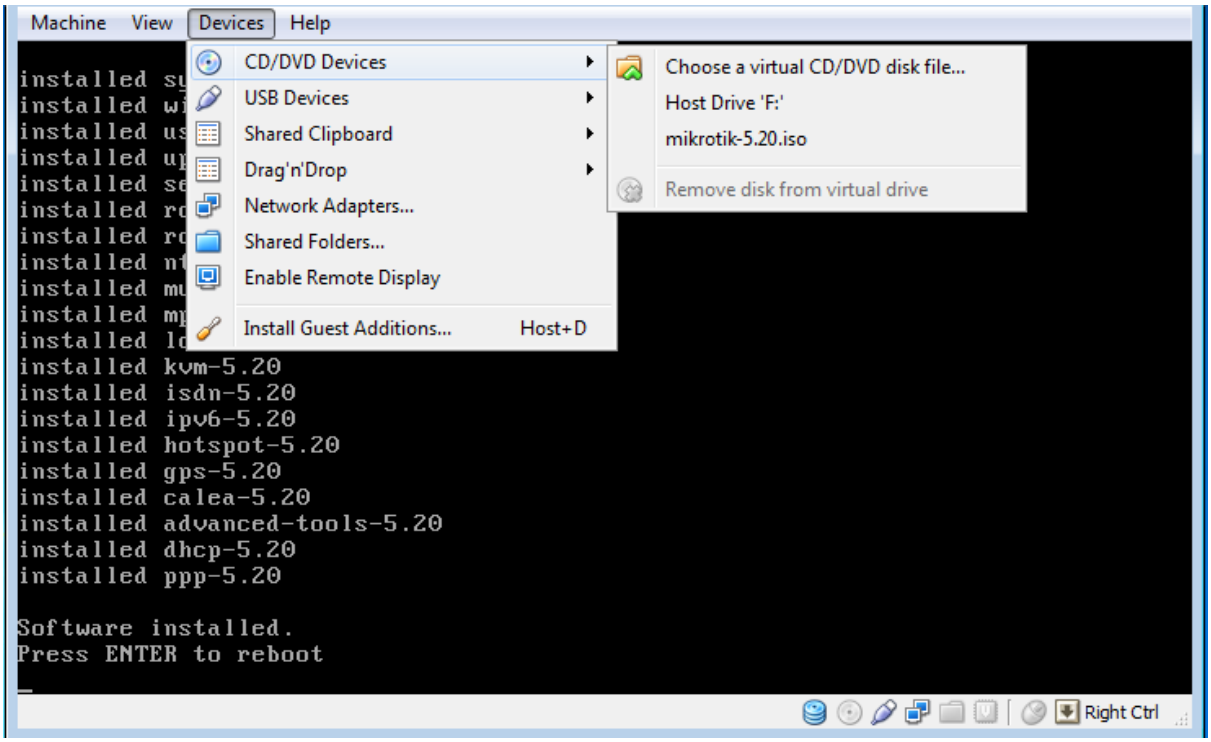


13) Tunggu sebentar hingga proses instalasi selesai dilakukan

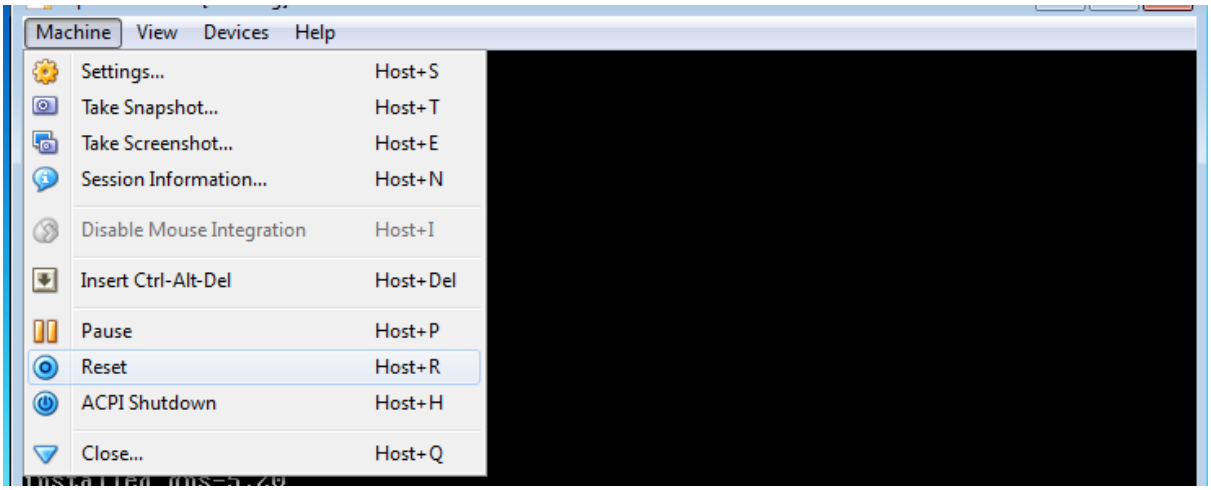


14) Jika proses sudah berhenti *jangan tekan Enter karena akan me-restart dari awal" , pilih Device → CD/DVD Devices → hilangkan tanda centang pada Mikrotik-5.20.iso

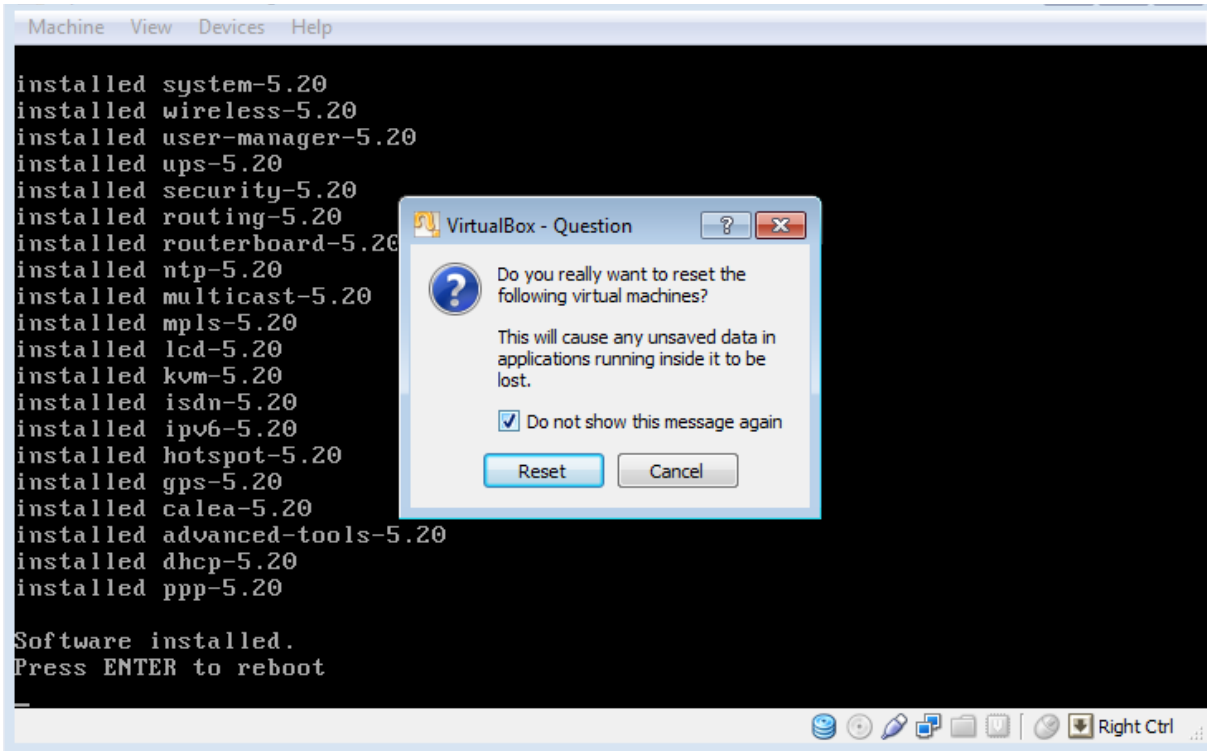




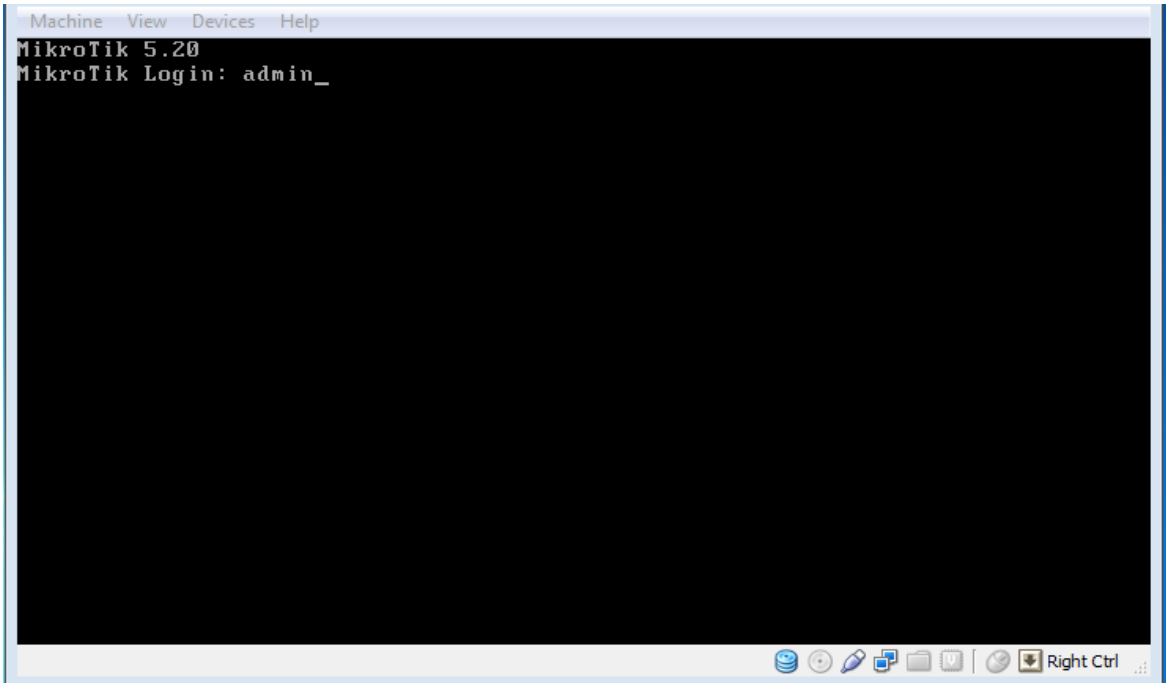
15) Kemudian pilih Machine → Reset



16) Maka muncul kotak dialog, berikan tanda centang pada "Do not show this message again" agar tidak ditampilkan pemberitahuan tersebut lagi. Lalu pilih Reset



17) Tunggu sampai muncul kotak dialog login, kemudian pada Mikrotik Login ketikkan admin



18) Maka akan muncul tampilan awal pada Mikrotik

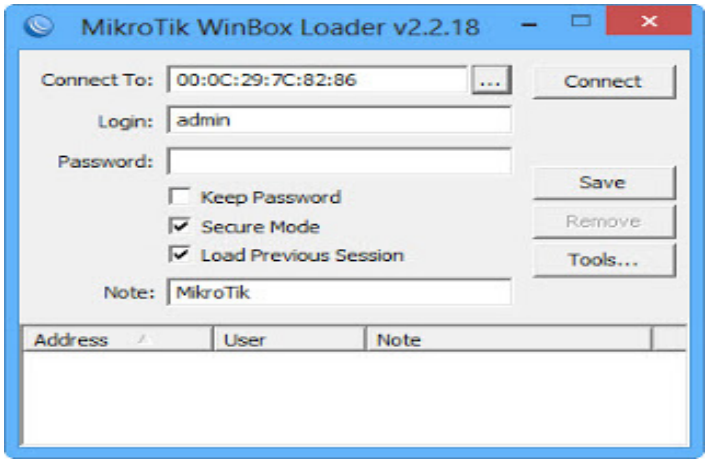
Lalu tekan enter, dan Mikrotik siap untuk digunakan J Selesai

Sekarang Mikrotik RouterOS nya sudah terinstall di PC anda. Namun Mikrotik nya hanya bisa digunakan selama 24 jam saja karena masih dalam masa trial. Untuk bisa membuatnya full versi, perlu dilakukan registrasi lisensi dulu.

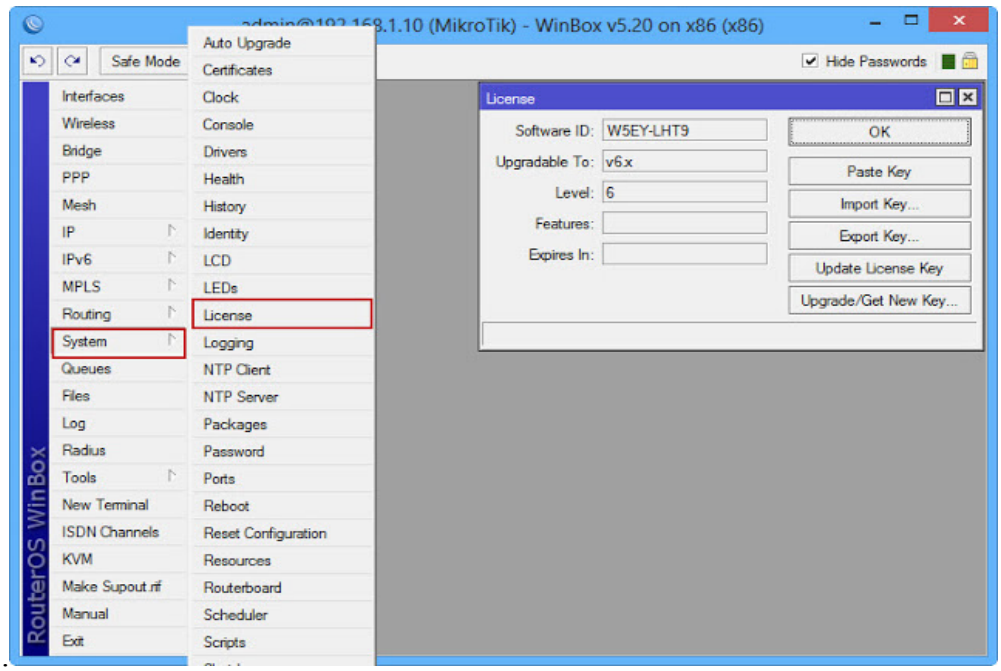
2.1.4 Memasukan lisence menggunakan winbox

Cara Registrasi Lisensi Mikrotik yaitu Koneksikan PC Mikrotik nya dengan PC lainnya atau Laptop anda menggunakan kabel UTP.

- Buka Winbox (Jika belum punya Winbox silahkan **download Winbox disini**)
- Login ke Mikrotik menggunakan Winbox.



- Di halaman utama Winbox **"RouterOs Welcome"** dengan berita router anda tidak memiliki key dan router akan di stop dalam waktu 23 jam 50 menit.
- Di halam Utama Winbox klik **"System"** dan klik **"Licence"**
- Kemudian klik "Import Key" dan pilih file lisensi level 6 yang ada di folder ISO tadi
- **Router now?** klik **"OK"** maka router akan restart dan disconnect.
- Login lagi ke Mikrotik nya via Winbox, buka menu System → License, maka akan muncul tampilan bahwa Mikrotik sudah berhasil diregistrasi dengan lisensi level



Selamat sekarang Mikrotik Anda lisensi nya sudah menjadi level 6. Anda dapat mencoba menyeting Mikrotik PC anda ini.

2.2 Konfigurasi Dasar

2.2.1 Setting username dan password login

Secara default di Router Mikrotik sudah terdapat satu user yang dapat mengakses RouterOS yaitu user dengan username : admin dan tanpa password. Username inilah yang awalnya kita gunakan untuk login ke RouterOS Mikrotik seperti login di Winbox. Tutorial selanjutnya akan membahas tentang penjelasan kategori akses user dan penambahan user di router Mikrotik.

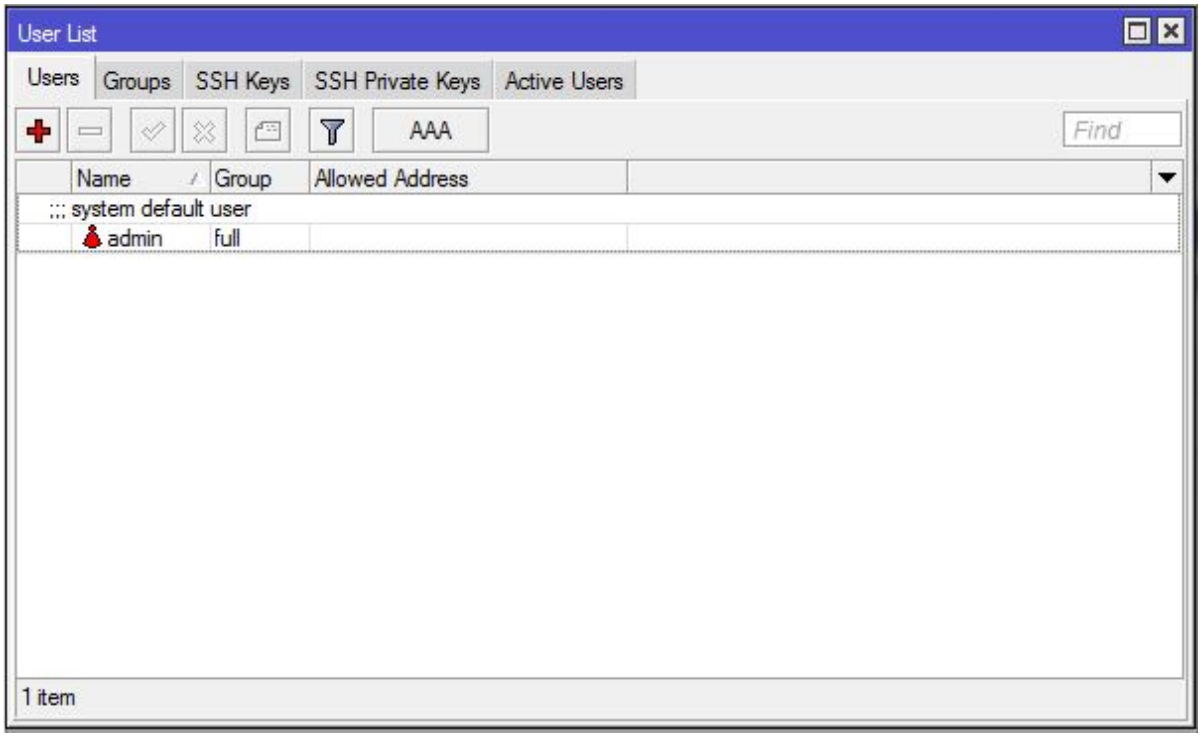
User yang dapat login ke Router Mikrotik dapat dikelompokkan menjadi 3 kategori, yaitu :

- Full --> user yang memiliki akses ini merupakan user dengan pangkat tertinggi, yang dapat melakukan konfigurasi seperti menghapus konfigurasi, menambahkan konfigurasi, sampai dengan menambahkan user baru ke dalam sistem Mikrotik.
- Write --> user ini memiliki akses konfigurasi seperti pada user yang memiliki akses full, namun tidak dapat menambahkan user baru, dan juga tidak dapat melakukan proses backup konfigurasi.
- Read --> user dengan akses ini hanya mampu melakukan monitoring pada sistem, tidak mampu melakukan konfigurasi seperti pada user dengan level Write maupun Full.

Untuk melihat daftar user dalam sistem Mikrotik, dapat menggunakan perintah command line :

[admin@Mikrotik] > **user print**

Atau melalui winbox dengan menu | **System --> users**



Jika anda hanya ingin mengganti password tanpa mengganti username ,misalkan password barunya adalah "rahasia ",maka perintahnya adalah:

[admin@Mikrotik] **> user set admin password=rahasia**

Jika ingin menambahkan username dan password sekaligus,maka perintahnya:

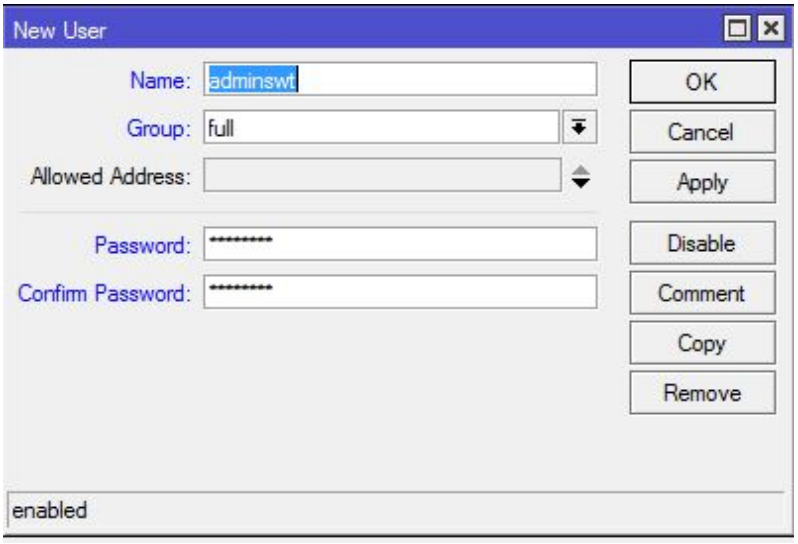
[admin@Mikrotik] **> user add name=adminswt password=rahasia**

Jika ingin mengganti username dan password sekaligus, maka perintahnya :

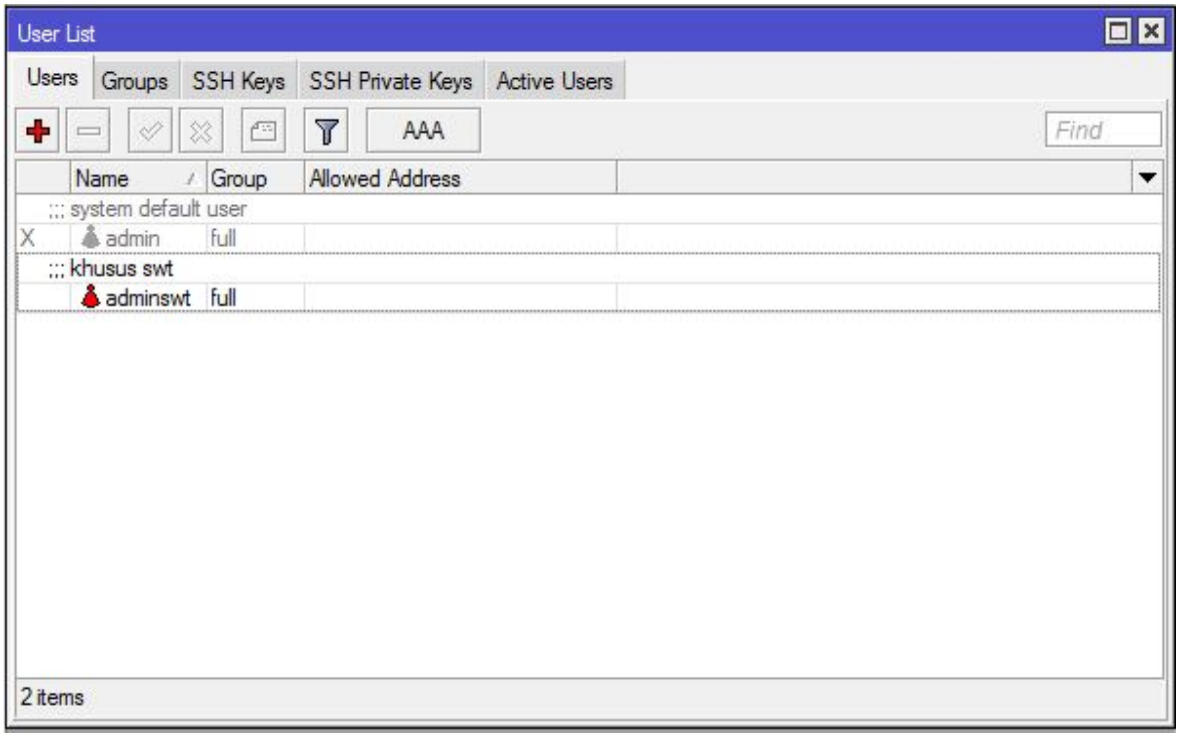
[admin@Mikrotik] **> user set admin name=adminswt password=rahasia**

Pada winbox untuk menambahkan user baru klik icon +, masukkan username, pilih kategori akses pada kotak Group, isikan juga password.

Opsi *Allowed Address* digunakan jika user yang dibuat hanya boleh login melalui alamat IP tertentu, misalnya user hanya boleh login melalui interface ether1 maka isikan dengan IP address ether1 misal : 192.168.100.0/24. Namun jika tidak diisi maka user dapat mengakses dari interface mana saja.



Jika sudah, maka akan muncul user baru di menu System --> users

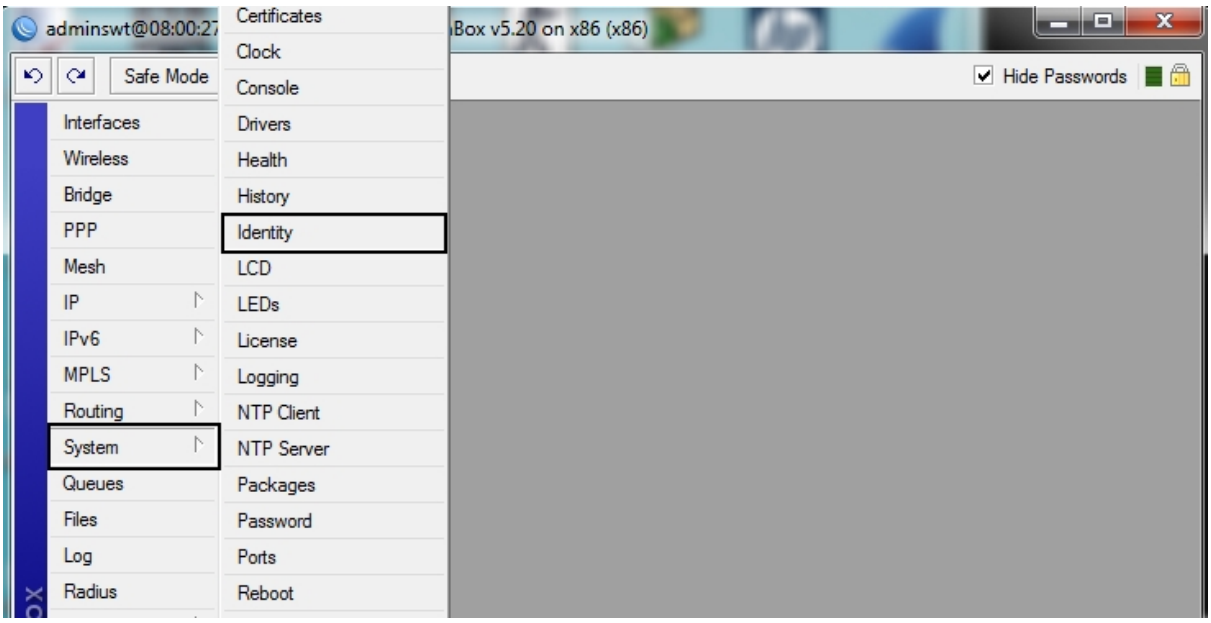


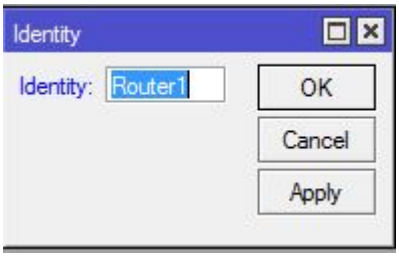
2.2.2 Mengganti Identity Router

Identity router adalah nama yang muncul pada command promt, identity tentunya untuk memudahkan kita mengingat nama router sebagai identitas daripada kita mengingat ip addressnya. Untuk mengganti identity router, misalkan akan diganti menjadi "Router1 perintahnya adalah:

[admin@Mikrotik] **> system Identity set name=Router1**

Pada winbox : **System | Identity**





Setelah diganti, maka identity router tersebut akan berubah menjadi:

[admin@**Router**1] >

2.2.3 Setting waktu pada Mikrotik

Apa itu NTP? Pasti banyak yang belum tau apa itu Network Time Protocol. NTP memang terdengar asing bagi orang yang belum begitu paham tentang jaringan komputer. untuk mempelajari lebih lanjut tentang Apa itu NTP (Network Time Protocol) dan penerapannya di Mikrotik silahkan simak pengertian NTP berikut ini :

Network Time Protocol atau lebih sering disebut dengan istilah NTP adalah sebuah mekanisme atau protokol yang digunakan untuk melakukan sinkronisasi terhadap penunjuk waktu dalam sebuah sistem komputer dan jaringan. Proses sinkronisasi ini dilakukan di dalam jalur komunikasi data yang biasanya menggunakan protokol komunikasi TCP/IP. Sehingga proses ini sendiri dapat dilihat sebagai proses komunikasi data biasa yang hanya melakukan pertukaran paket-paket data saja.

NTP menggunakan port komunikasi UDP nomor 123. Protokol ini memang didesain untuk dapat bekerja dengan baik meskipun media komunikasinya bervariasi, mulai dari yang waktu latensinya tinggi hingga yang rendah, mulai dari media kabel sampai dengan media udara. Protokol ini memungkinkan perangkat-perangkat komputer untuk tetap dapat melakukan sinkronisasi waktu dengan sangat tepat dalam berbagai media tersebut. Biasanya dalam sebuah jaringan, beberapa node dilengkapi dengan fasilitas NTP dengan tujuan untuk membentuk sebuah subnet sinkronisasi. Node-node tersebut kemudian akan saling berkomunikasi dan ber sinkronisasi menyamakan waktu yang direkam mereka. Meskipun ada beberapa node yang akan menjadi master (primary server), protokol NTP tidak membutuhkan mekanisme pemilihan tersebut.

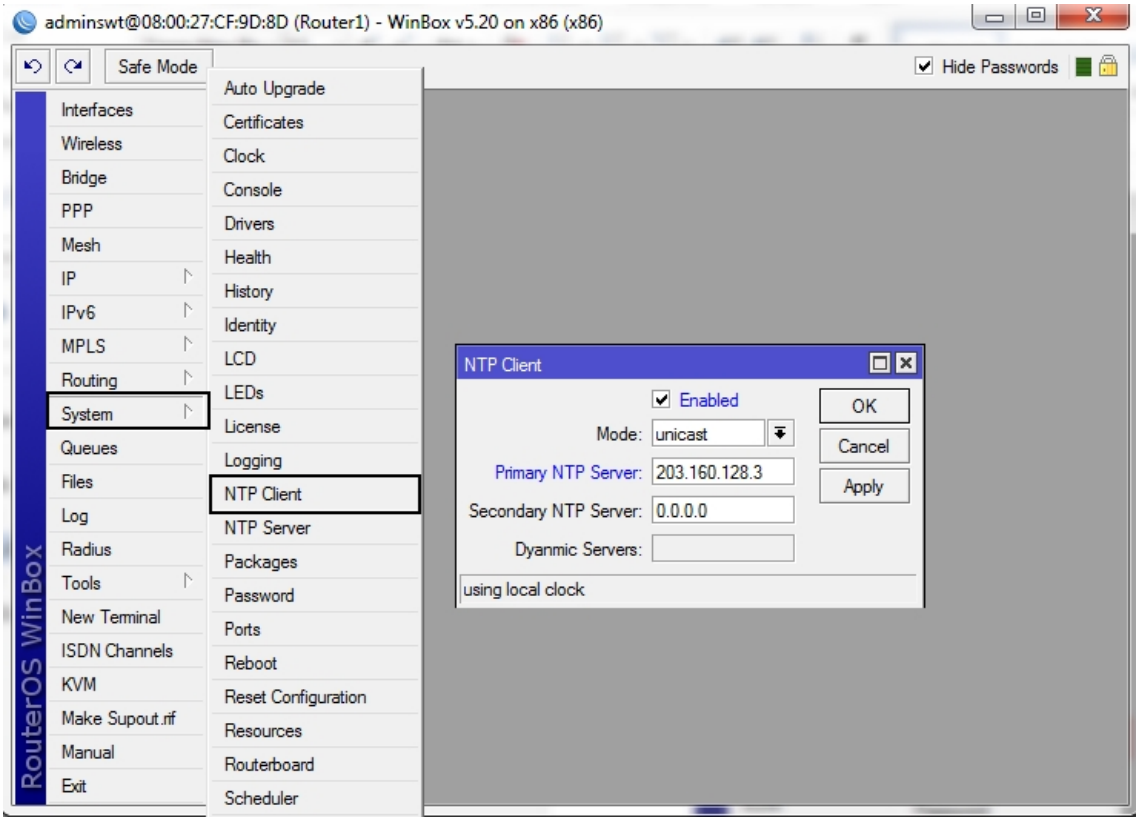
Oke sudah tau kan apa itu NTP? Kalo sudah jelas tentang NTP sekarang lanjut ke setting NTP pada Mikrotik mari kita Belajar Mikrotik lebih dalam lagi tentang NTP.

- Setting Network Time Protocol Client di Mikrotik

Dalam kondisi tertentu Router Mikrotik harus bekerja berdasarkan waktu, baik tanggal, hari, maupun jam. Misalnya saja jika Anda ingin memblokir akses internet di luar jam kerja atau memblokir beberapa situs pada jam-jam tertentu. Jika anda menggunakan PC sebagai Router Mikrotik ini tentu bukan masalah, karena di Motherboard komputer sudah terpasang baterai yang dapat mempertahankan konfigurasi waktu. Namun pada RouterBoard Mikrotik yang tidak memiliki barerai internal maka konfigurasi waktu akan kacau tiap kali router mengalami restart.

Nah, untuk menghindari ketidakakuratan konfigurasi waktu inilah, maka pada Router Mikrotik perlu dikonfigurasikan Network Time Protocol (NTP). Router Mikrotik perlu mengetahui NTP Server yang ada di Internet dan akan berusaha menyesuaikan dengan konfigurasi waktu yang ada di NTP Server tersebut. Untuk sinkronisasi konfigurasi waktu pada Router Mikrotik, Anda dapat menggunakan NTP Server untuk Indonesia dengan IP Address 203.160.128.3.

Untuk lebih mudahnya silahkan anda gunakan Winbox untuk menyeting NTP Client nya. Buka Winbox, masuk ke menu System --> NTP Client, seperti gambar berikut :

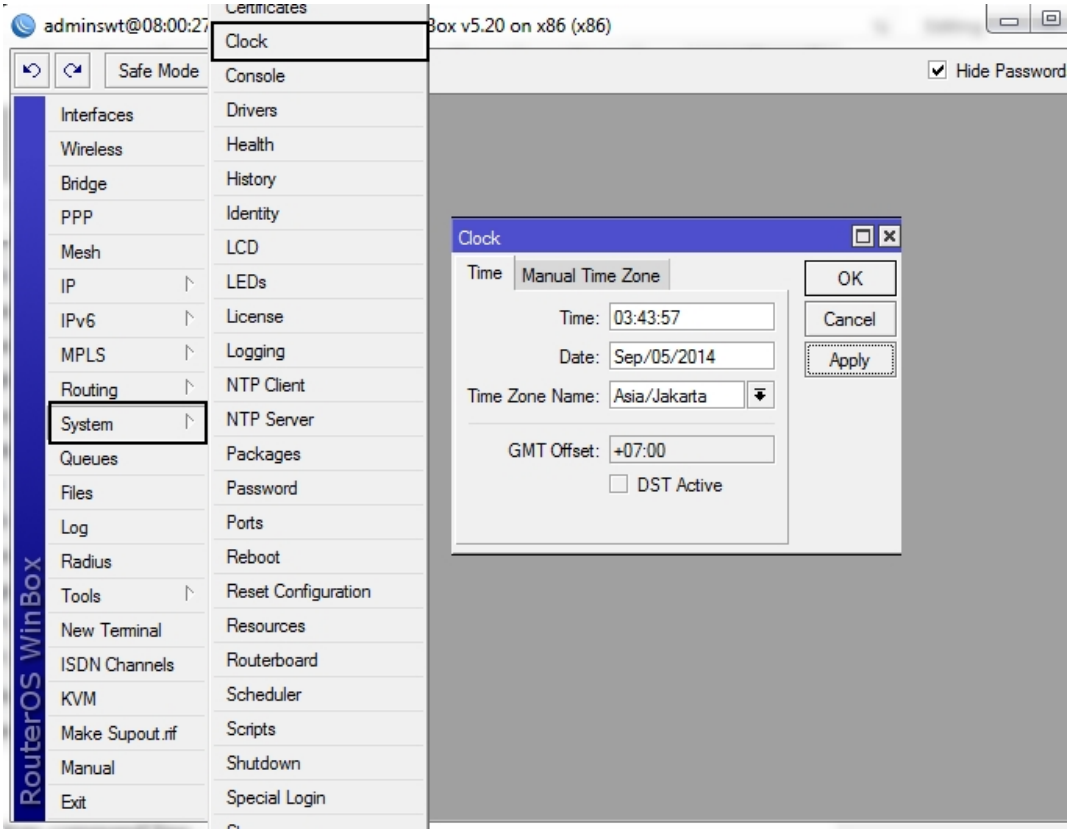


Centang opsi Enabled --> Mode : unicast --> Primary NTP Server : 203.160.128.3

Atau bisa juga menggunakan command line :

[admin@Mikrotik] > **system ntp client set primary-ntp=203.160.128.3 enabled=yes mode=unicast**

Selanjutnya setting waktu pada Mikrotik nya dengan masuk ke menu System --> Clock, seperti gambar di bawah ini :



Atau bisa juga menggunakan command line :

[admin@Mikrotik] > system clock set time-zone-name=Asia/Jakarta

Sekarang konfigurasi waktu Router Mikrotik anda sudah sesuai.

2.2.4 Mengganti nama interface

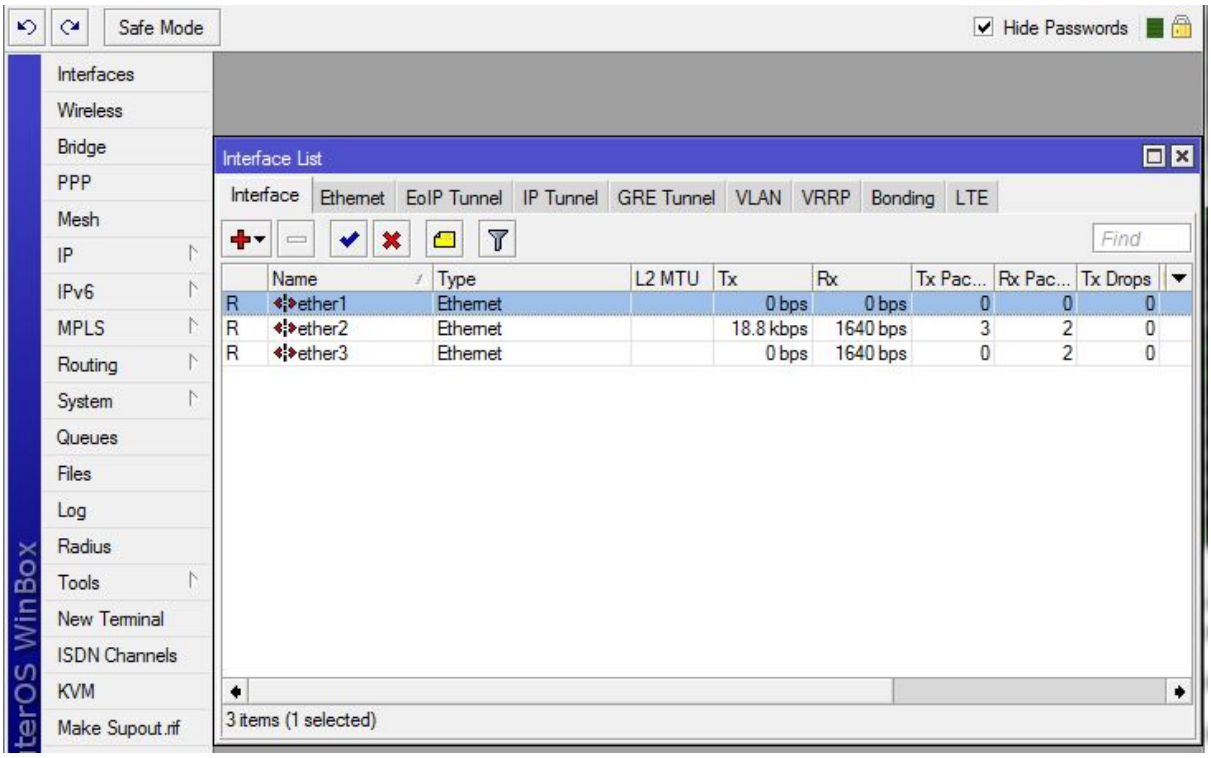
Default nama interface pada Mikrotik adalah ether untuk interface Ethernet dan wlan untuk interface wireless,jika ada lebih dari satu interface maka nama deefaultnya akan ditambahkan angka pada belakangnya dengan dimulai dari angka 1, contoh : ether 1, ether2, wlan2, wlan2,dst. Jika kita ingin menamakannya sesuai dengan fungsi interface yang kita akan konfigurasikan , maka cara menggantikanya adalah sebagai berikut:

Pertama, kita lihat nama interface default dengan perintah berikut :

[admin@Mikrotik] > **interface print**

```
[admin@Router1] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                TYPE                MTU L2MTU  MAX-L2MTU
 0  R  ether1                              ether              1500
 1  R  ether2                              ether              1500
 2  R  ether3                              ether              1500
[admin@Router1] > _
```

Jika menggunakan winbox adalah Interface,maka akan muncul tampilan seperti dibawah ini



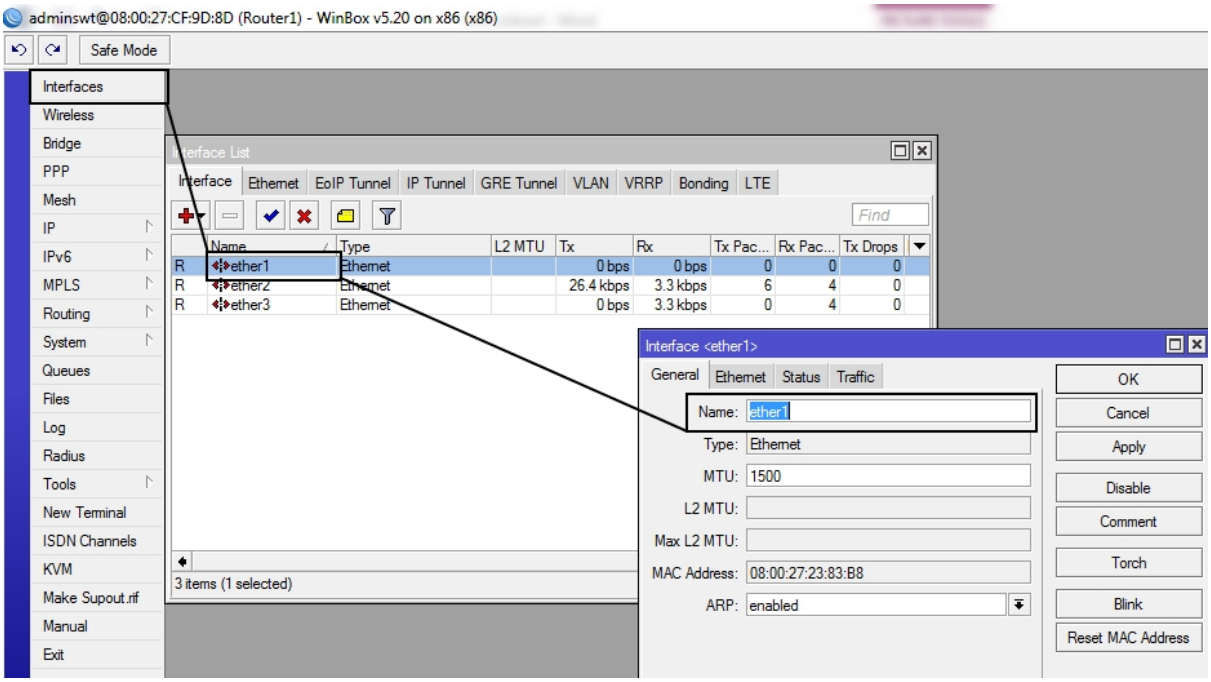
Pada contoh diatas ada dua interface Ethernet, misalkan kita ingin menggunakan ether1 untuk koneksi ke public/internet, dan ether2 untuk koneksi locak, maka kita namakan sesuai dengan fungsinya

[admin@Mikrotik] > **interface set 0 name=Public**

[admin@Mikrotik] > **interface set 1 name=Local**

0 dan 1 adalah nomor urut interface tersebut sebagaimana ditampilkan pada perintah Interface Print diatas.

Jika menggunakan winbox adalah Interface | ether1 | Name: ether1 , ganti ether1 menjadi Public dengan cara double click baris ether1 lalu ganti nama ether satu menjadi Public, demikian juga pada ether2. Ganti menjadi Locak, lalu klik Apply

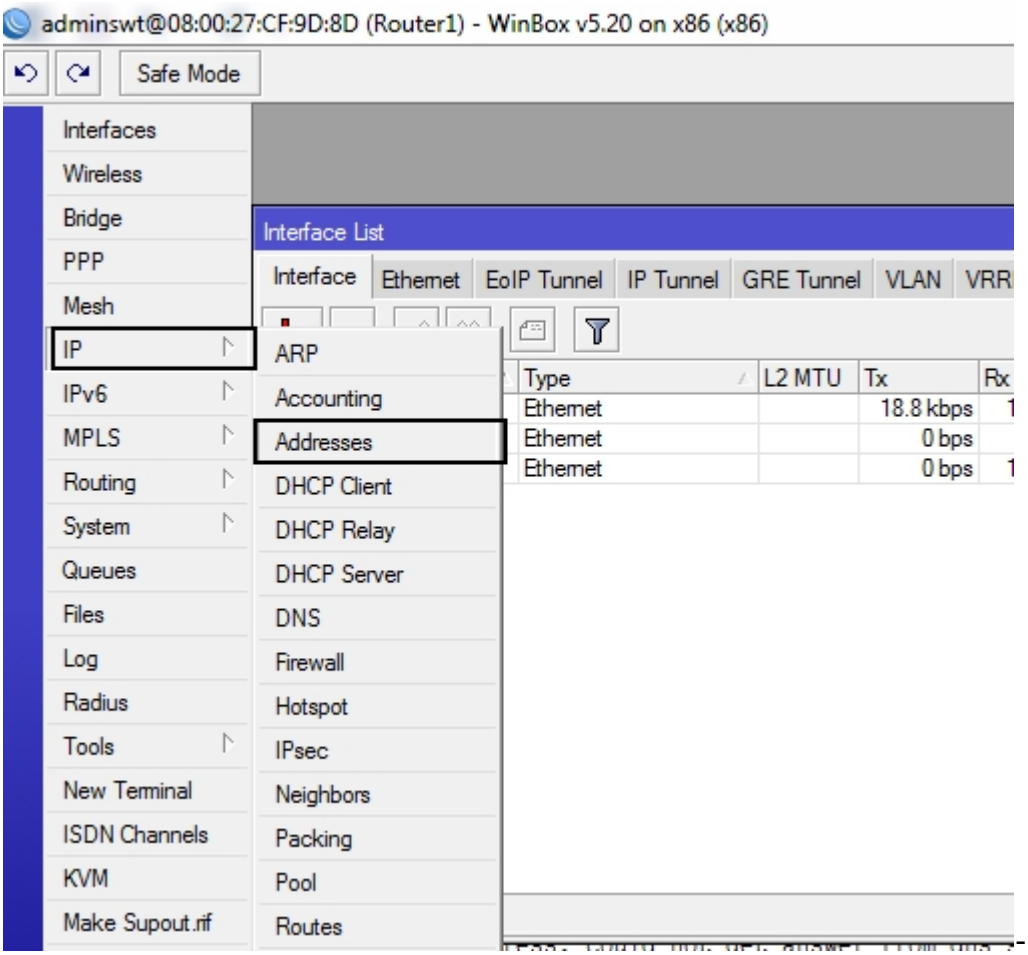


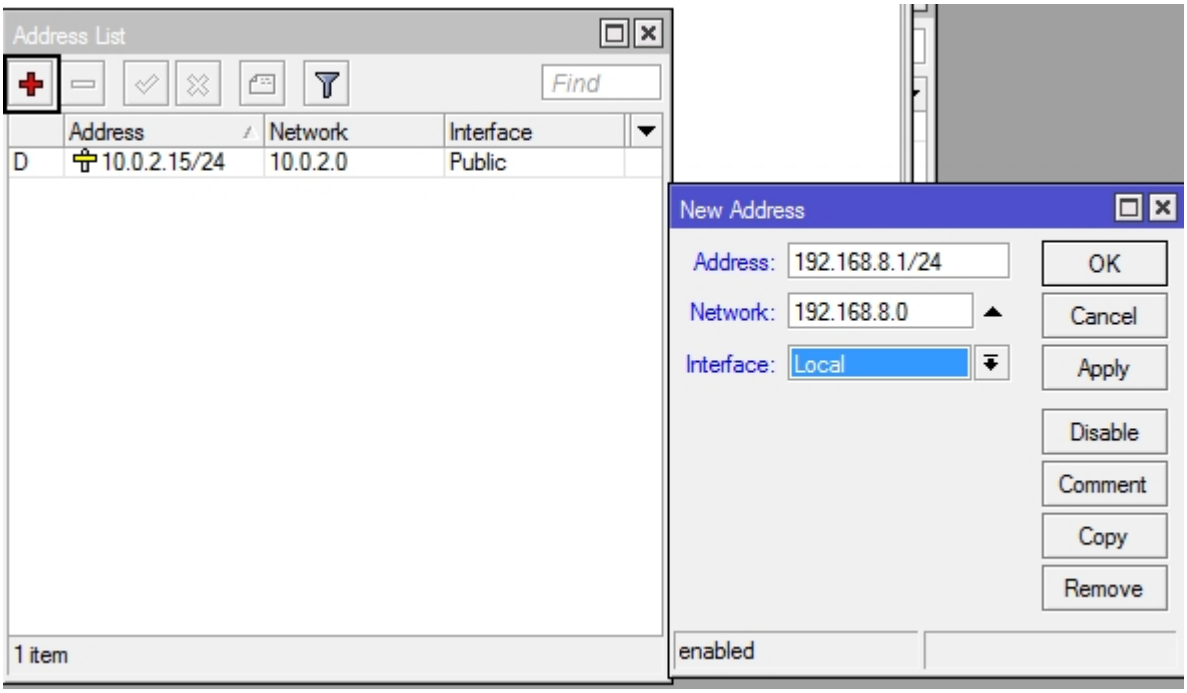
2.2.5 Setting IP Address

Misalkan kita akan mensetting IP private 192.168.8.1/24 pada interface Local. Command nya adalah:

[admin@Mikrotik] **> ip address add address=192.168.8.1/24 interface=Local**

Jika menggunakan winbox: ***IP*** **|** ***Addresses***, double click baris interface yang akan dimasukan ip addreess,lalu isikan ip address nya


adminswt@08:00:27:CF:9D:8D (Router1) - WinBox v5.20 on x86 (x86)
Safe Mode
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Make Supout.rif
ARP
Accounting
Addresses
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Neighbors
Packing
Pool
Routes
Interface List
Interface
Ethernet
EoIP Tunnel
IP Tunnel
GRE Tunnel
VLAN
Type
L2 MTU
Tx
Rx
Ethernet
18.8 kbps
Ethernet
0 bps
Ethernet
0 bps

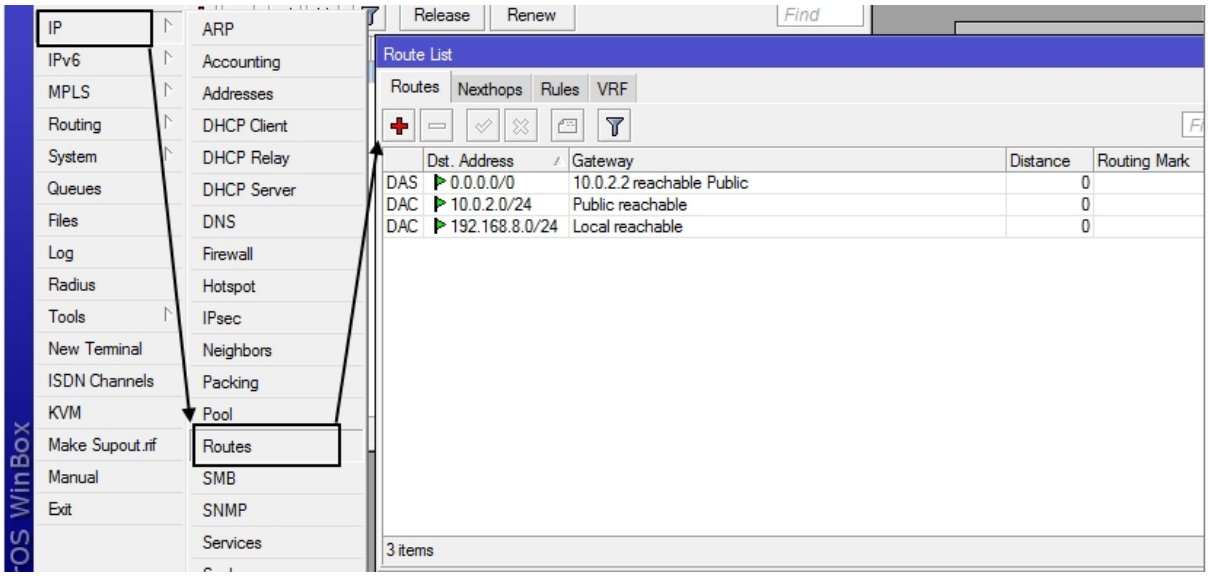

Address List
Find
Address
Network
Interface
D
10.0.2.15/24
10.0.2.0
Public
1 item
New Address
Address:
192.168.8.1/24
Network:
192.168.8.0
Interface:
Local
OK
Cancel
Apply
Disable
Comment
Copy
Remove
enabled

2.2.6 Setting Default Gateway

Setelah setting IP Address pada interface yang akan digunakan, setting yang perlu dilakukan selanjutnya adalah Default Gateway, yaitu gerbang untuk penghubung antara jaringan local dengan jaringan internet. IP Address yang akan dijadikan sebagai Default Gateway adalah IP Address yang diberikan oleh ISP, dalam contoh IP Address nya adalah 62.10.10.2/29. Cara settinganya adalah :

[admin@Mikrotik] **> ip route add dst-address=0.0.0.0/0 gateway=62.10.10.2**

Jika menggunakan winbox : **IP | Routeres** | +



2.2.7 Setting DNS server

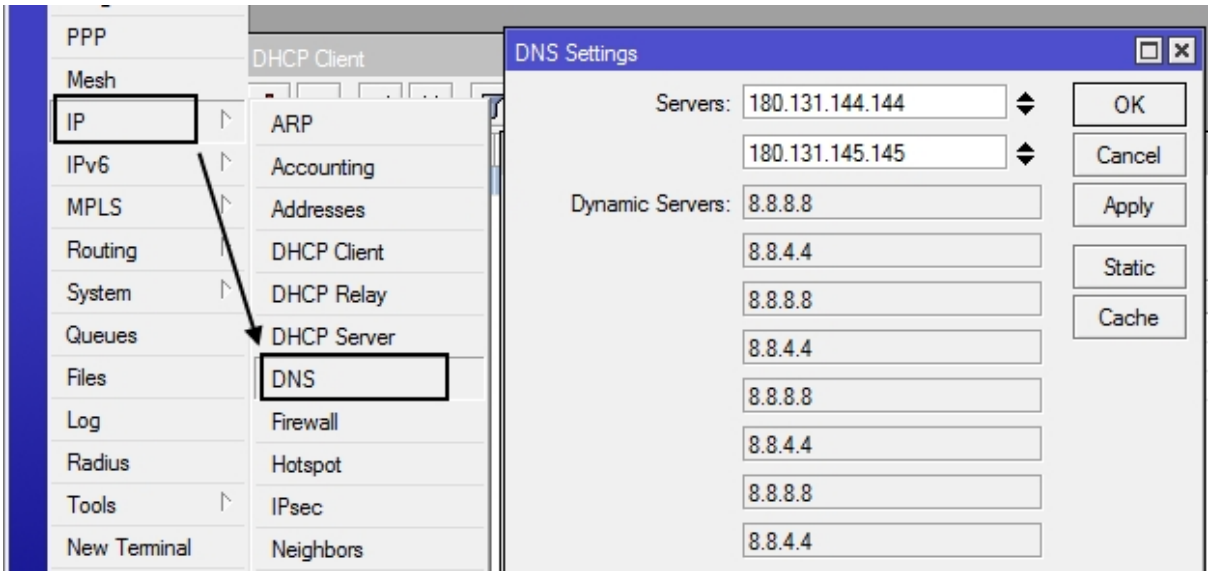
Setelah IP Address dan Default Gateway,konfigurasi berikutnya yang perlu di setting adalah DNS Server agar dapat mengakses internet, karena DNS Server adalah berfungsi me-resolve domain name ke IP Address, Cara settingnya adalah:

[admin@Mikrotik] **> ip dns set server=62.10.10.1 allow-remote-requests=yes**

Setting ini adalah jika router Mikrotik kita difungsikan juga sebagai DNS server local, dan parameter allow-remote=reques=yes adalah untuk menjadikan Mikrotik sebagai DNS local yang berfungsi menerima request tentang resolve domain. Jika ingin men-setting lebih dari satu ip address DNS server,bisa dilakukan dengan menambahkan tanda koma sebagai pemisahnya, contoh:

[admin@Mikrotik] **> ip dns set server=62.10.10.1,8.8.8.8,8.8.4.4 allow-remote-requests=yes**

Jika menggunakan winbox: **IP | DNS | Servers**

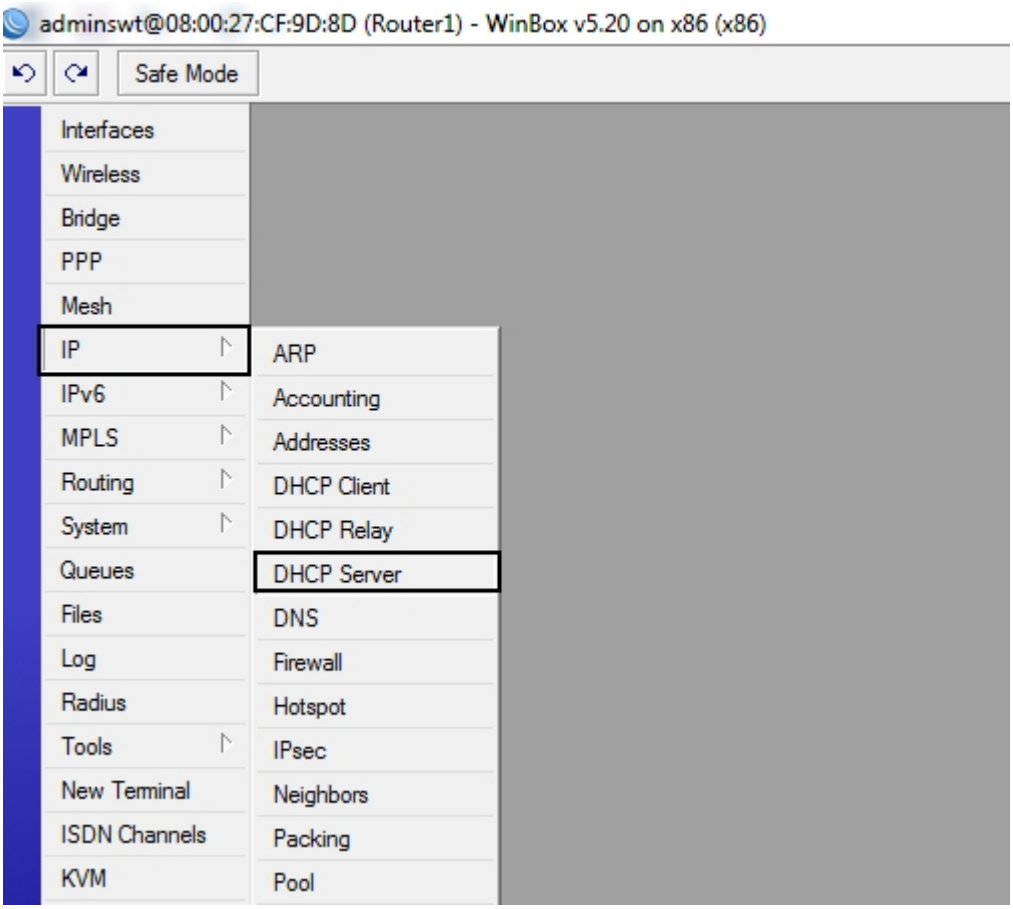


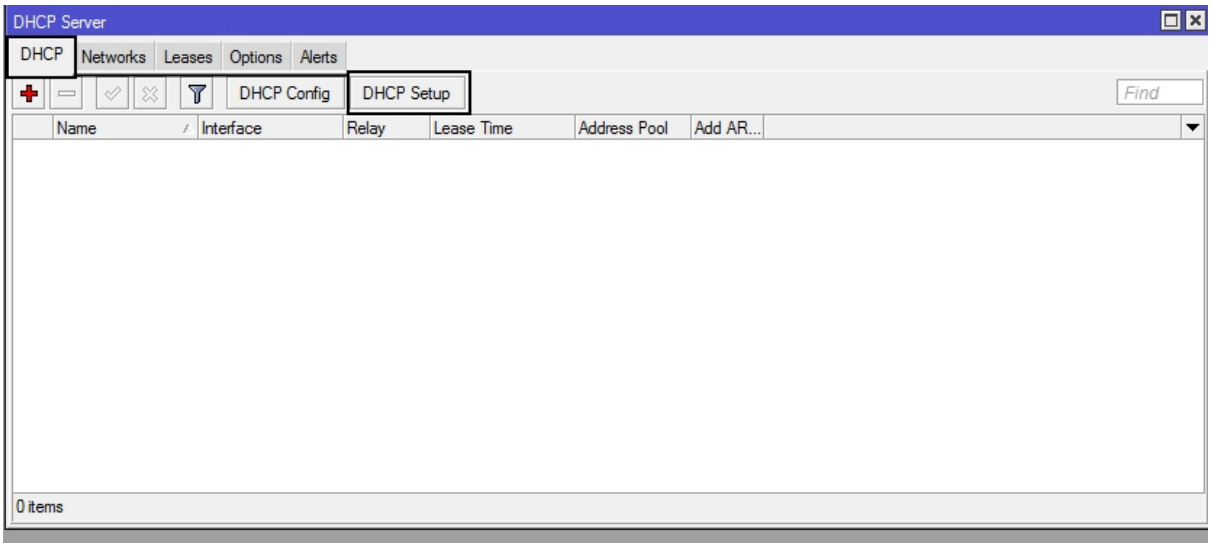
2.2.8 Setting DHCP Server

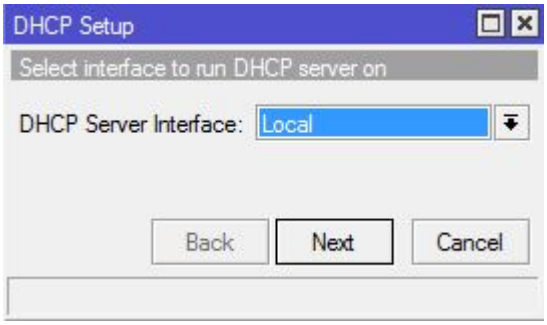
DHCP (Dynamic Host Configuration Protocol) server adalah berfungsi untuk memberikan secara otomatis konfigurasi yang di butuhkan oleh computer client untuk bisa terhubung dalam LAN sehingga computer client tidak perlu men-setting konfigurasi yang dibuthkan itu secara manual. Konfigurasi yang dapat diberikan oleh DHCP server adalah : IP Address, Gateway , dan DNS server. Cara settingnya adalah:

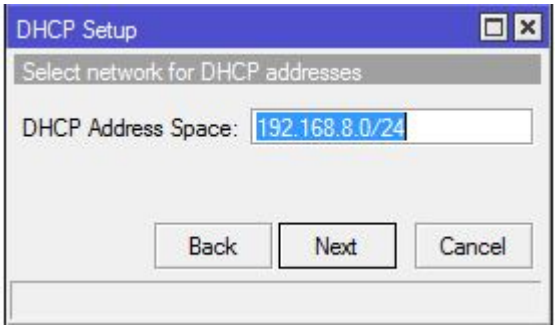
[admin@Mikrotik] **> ip dhcp-server setup**

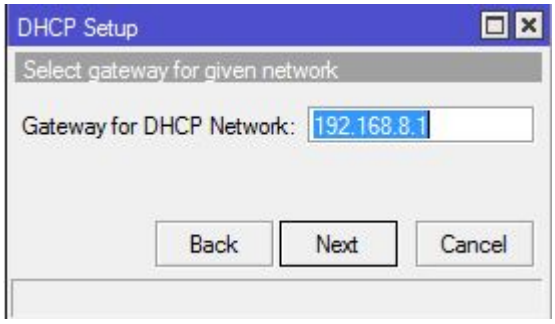
Jika menggunakan winbox: **IP | DHCP Server | DHCP | DHCP Setup**, lalu ikuti langkah-langkah pada wizard seperti tampilan di bawah ini, isi sesuai dengan konfigurasi yang kita miliki.

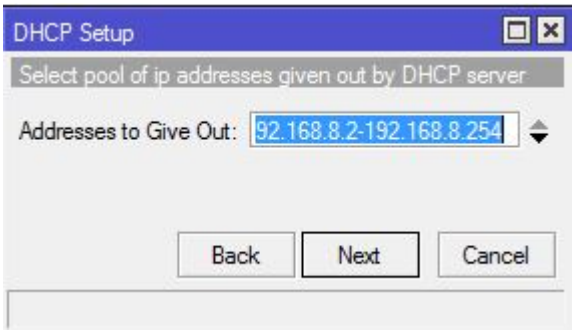

adminswt@08:00:27:CF:9D:8D (Router1) - WinBox v5.20 on x86 (x86)
Safe Mode
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
ARP
Accounting
Addresses
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Neighbors
Packing
Pool


DHCP Server
DHCP
Networks
Leases
Options
Alerts
DHCP Config
DHCP Setup
Find
Name
Interface
Relay
Lease Time
Address Pool
Add AR...
0 items









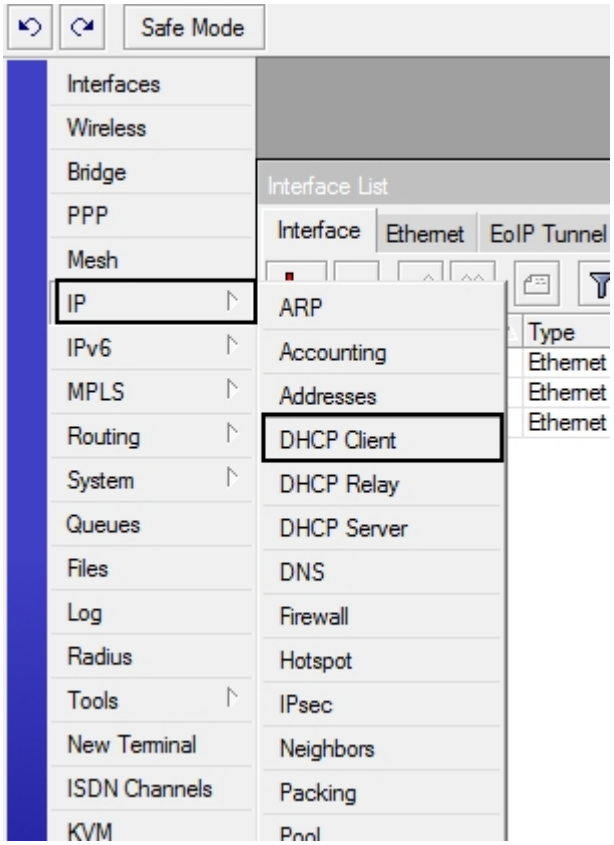
Sampai disini , konfigurasi dasar router Mikrotik sudah selesai, router sudah dapat mengakses internet, demikan juga komputer client yang ingin mengakses internet melalui router Mikrotik.

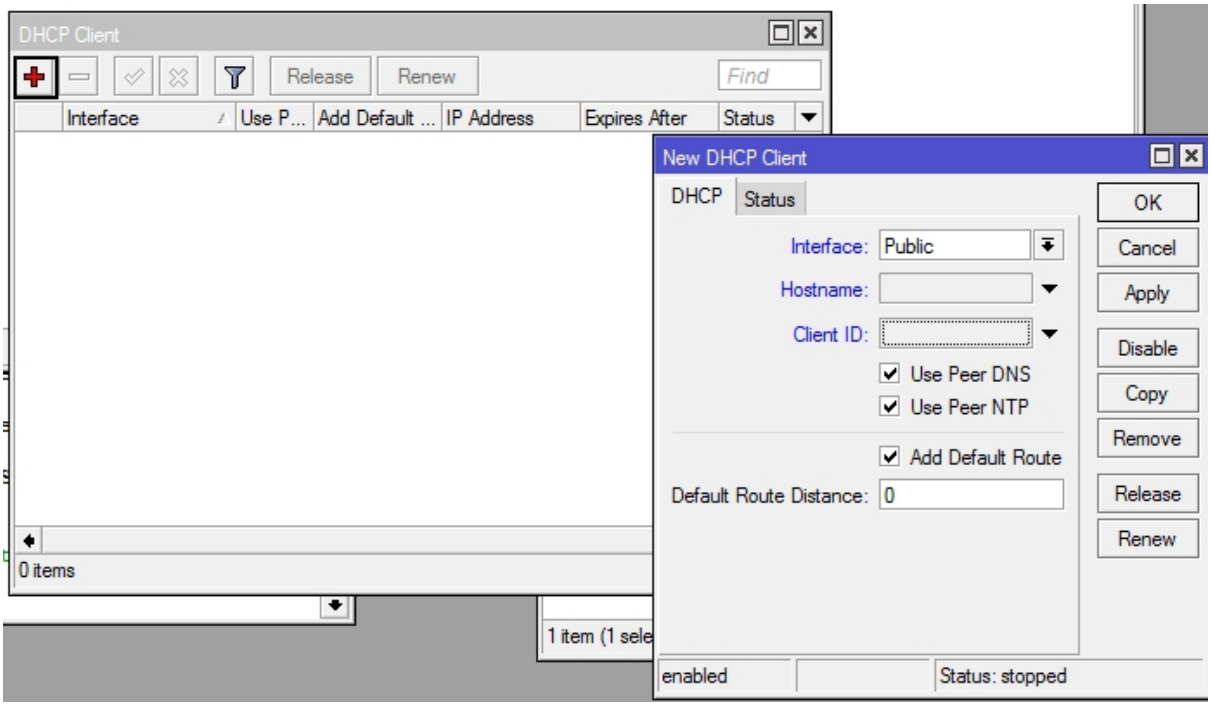
2.2.9 Setting DHCP Client

Khusus untuk interface “ether1” atau tadi yang sudah di ubah menjadi Public akan menggunakan alamat IP dinamis (DHCP) karena interface tersebut terkoneksi lewat “NAT VirtualBox” yang telah menyediakan layanan” DHCP Server” .

[admin@Mikrotik] **> ip dhcp-client add interface=Public disabled=no**

Jika menggunakan Winbox: **IP | DHCP Client |** +


Safe Mode
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels
KVM
Interface List
Interface
Ethernet
EoIP Tunnel
ARP
Accounting
Addresses
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Neighbors
Packing
Pool
Type
Ethernet
Ethernet
Ethernet


DHCP Client
Release
Renew
Find
Interface
Use P...
Add Default ...
IP Address
Expires After
Status
0 items
1 item (1 sele
New DHCP Client
DHCP
Status
Interface: Public
Hostname:
Client ID:
Use Peer DNS
Use Peer NTP
Add Default Route
Default Route Distance: 0
OK
Cancel
Apply
Disable
Copy
Remove
Release
Renew
enabled
Status: stopped

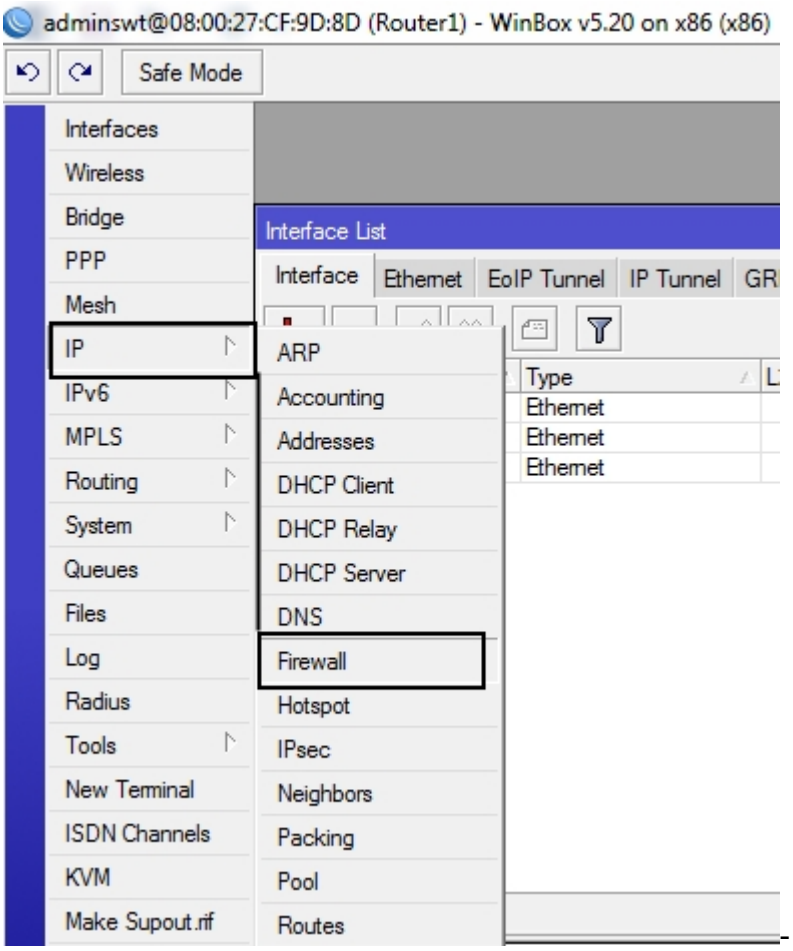
2.2.10 Setting Network Address Translation Masquerade

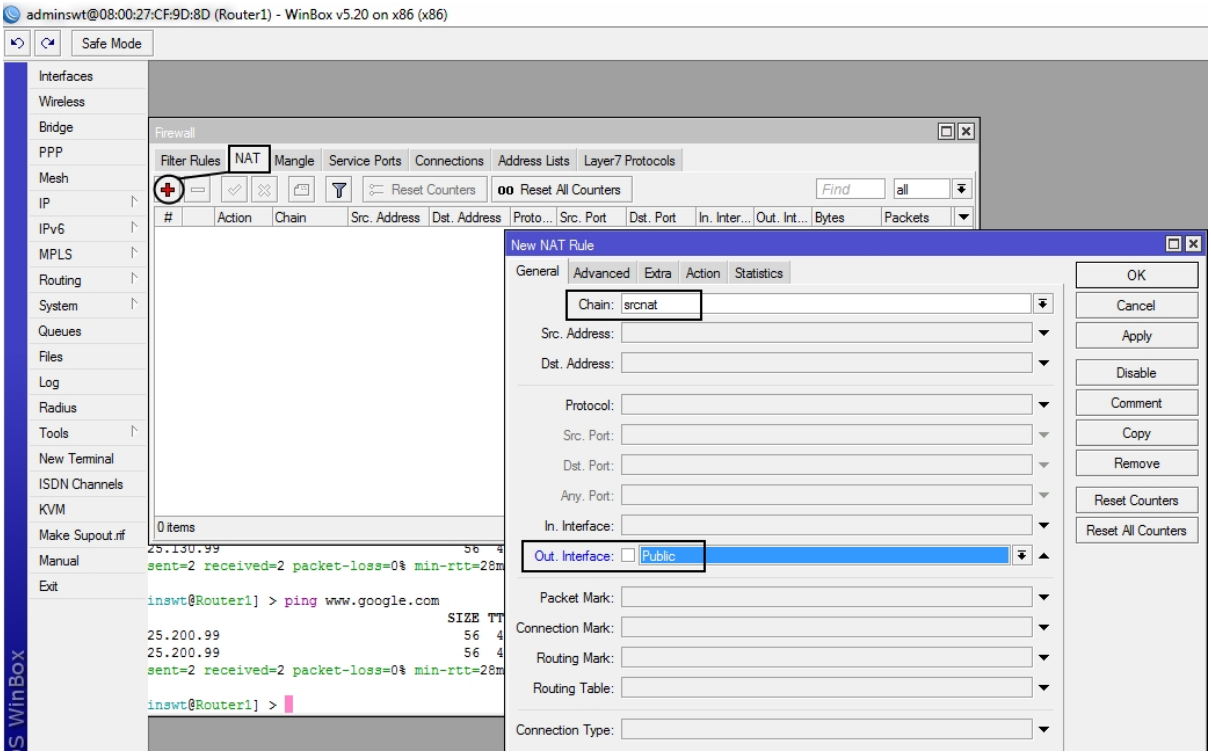
Selanjutnya perlu di setting agar komputer client bisa berkomunikasi dengan jaringan internet melalui router Mikrotik adalah NAT (Network Address Translation), yaitu untuk menterjemahkan IP Address yang dapat dikenali oleh jaringan internet.

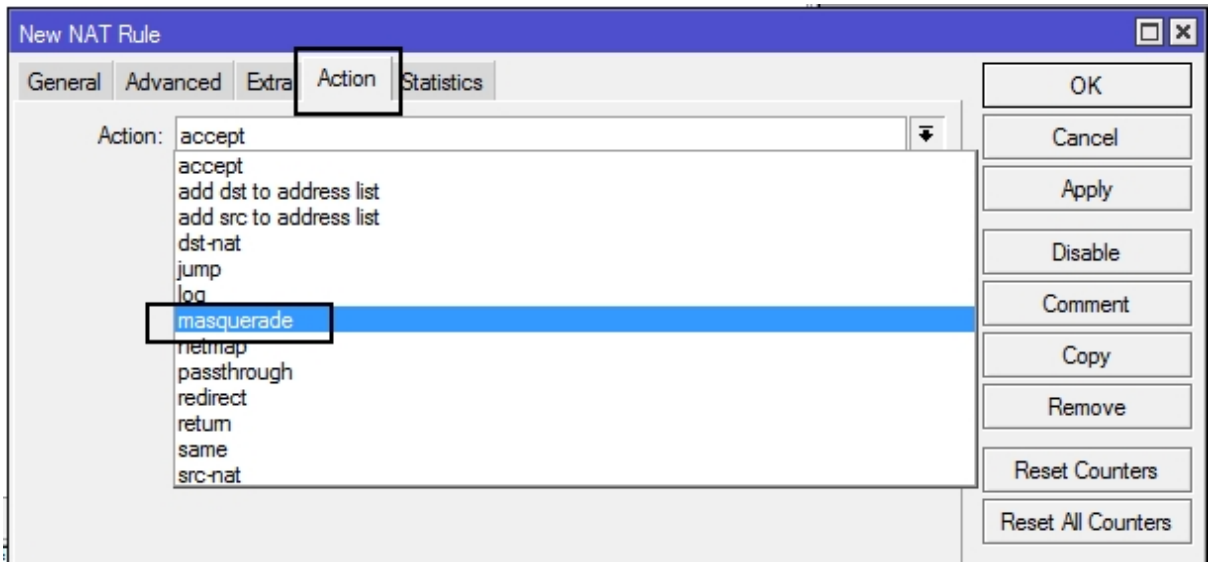
Cara settingnya adalah:

[admin@Mikrotik] **> ip firewall nat add chain=srcnat out-interface=Public action=masquerade**

Jika menggunakan winbox : **IP | Firewall | NAT | +**







2.2.11 Address List

Address List adalah fitur pada firewall yang digunakan untuk mengelompakan ip address berdasarkan nama tertentu, contohnya dalam suatu LAN dengan network yang sama terdapat beberapa department yang berbeda dengan penggunaan ip statik, maka kita dapat mengelompokan semua atau sebagian ip address tersebut dengan nama tertentu.

Misalkan ip address 192.168.8.11 – 192.168.8.13 adalah milik Staff IT , ip address 192.168.8.14 – 192.168.8.16 adalah milik Staf Perpus . Commandnya adalah :

[admin@Mikrotik] **> ip firewall address-list add list=”Staf IT” address=192.168.8.11**

[admin@Mikrotik] **> ip firewall address-list add list=”Staf IT” address=192.168.8.12**

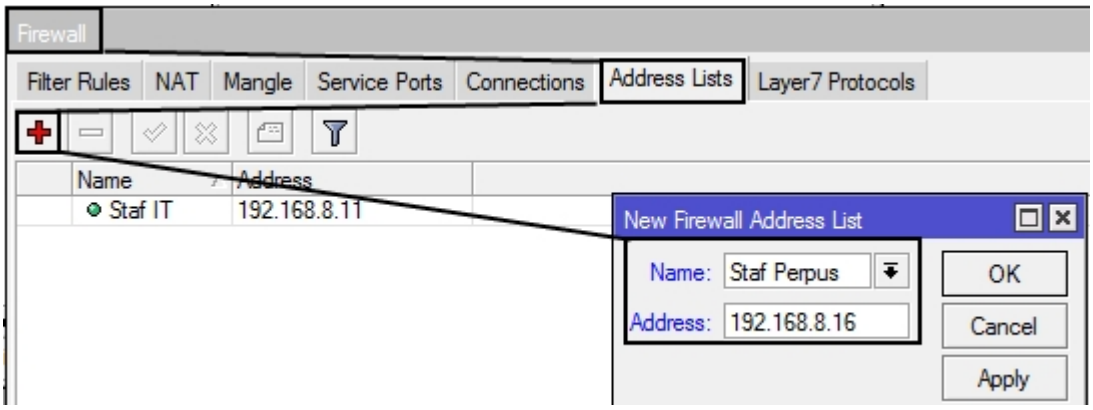
[admin@Mikrotik] **> ip firewall address-list add list=”Staf IT” address=192.168.8.13**

[admin@Mikrotik] **> ip firewall address-list add list=”Staf Perpus” address=192.168.1.14**

[admin@Mikrotik] **> ip firewall address-list add list=”Staf Perpus” address=192.168.8.15**

[admin@Mikrotik] **> ip firewall address-list add list=”Staf Perpus” address=192.168.8.16**

Jika menggunakan winbox adalah **: IP :Firewall | address Lists |** +



2.2.12 Backup dan Restore

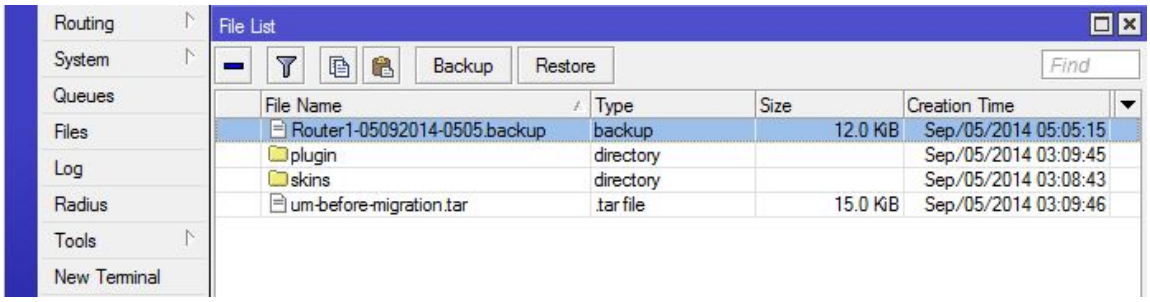
Konfigurasi Router Mikrotik dapat di-backup dan restore untuk mencegah pekerjaan konfigurasi ulang jika suatu saat router diganti atau rusak. Fitur Backup juga berguna ketika anda melakukan kesalahan konfigurasi dan ingin kembali ke konfigurasi sebelumnya. Konfigurasi yang di-backup ini akan disimpan dalam bentuk file dan dapat di download atau copy ke harddisk PC/laptop anda.

Cara Backup Konfigurasi Mikrotik

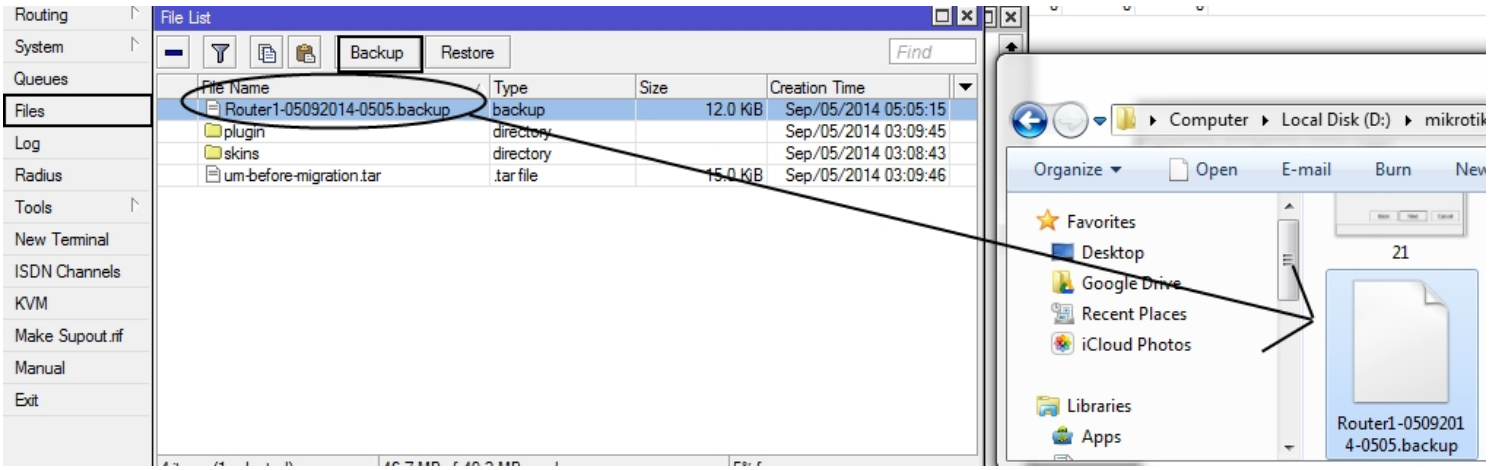
Untuk melakukan backup konfigurasi, anda dapat melakukannya via command line ataupun winbox, dengan perintah :

[admin@Mikrotik] > system backup save

Jika menggunakan winbox, masuk ke menu Files --> klik Backup. Maka akan muncul file baru dengan ekstensi .backup.



Kemudian untuk mengcopy atau download file .backup tersebut ke komputer tinggal drag and drop aja file nya ke Windows Explorer seperti gambar berikut :



Perhatikan nama file di kotak yaitu Router1-05092014-0505.backup ,maka maksudnya adalah:

- Router1 : nama identitas router Mikrotik (router identity)
- 05092014 : backup ini dilakukan pada tanggal 05 bulan 09 (September) tahun 2014
- 0505 : backup ini dilakukan pada jam 05.05
- .backup : jenis ekstensi setiap file backup

Tapi kita juga bisa menentukan nama file untuk file backup, hanya saja penentuan nama file saat melakukan backuo hanya bisa dilakukan melalui command line, tidak bisa melalui winbox,contohnya adalah :

[Router1@adminswt]> **system backup save name=backup-Mikrotik-bulan-september**

Dengan command tersebut, maka file backup akan tersimpan dengan nama **backup-Mikrotik-bulan-september.backup** .

Backup Sebagian Konfigurasi :

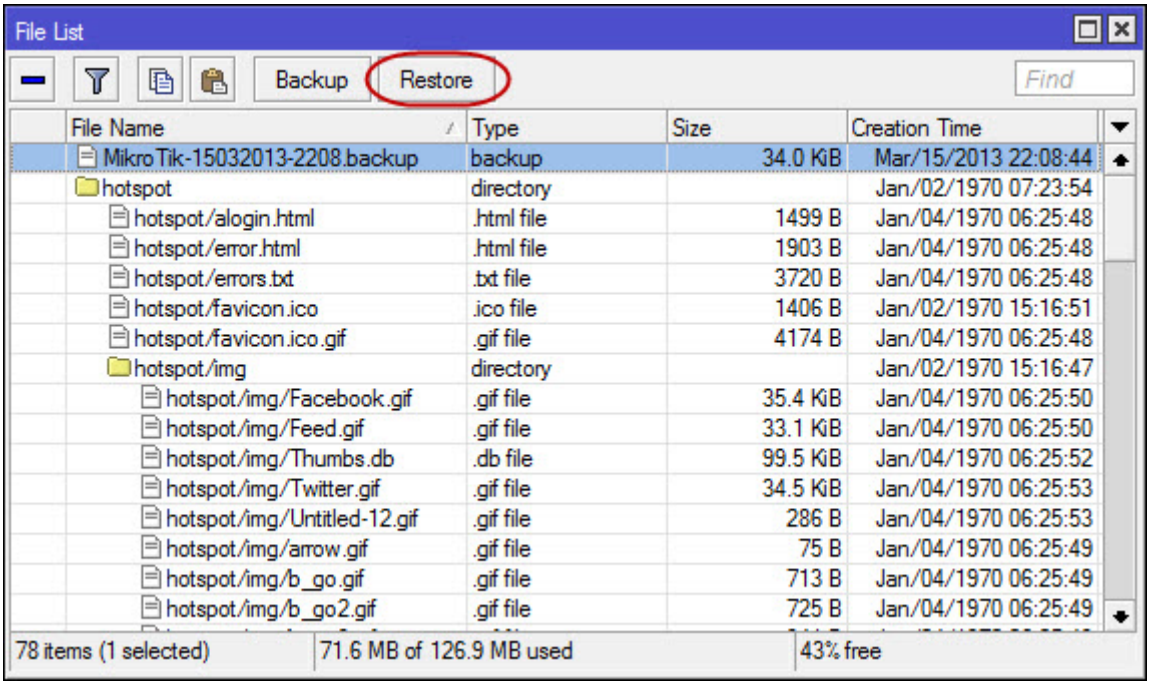
Pada pembahasan sebelumnya kita telah mengetahui cara melakukan backup keseluruhan konfigurasi, kali ini kita akan mebahas tentang cara membackup sebagian konfigurasi saja. Caranya agak sedikit berbeda, yaitu dengan meng-export script. Misalkan kita hanya ingin membackup konfigurasi ip address saja, maka commandnya adalah sebagian berikut :

[Router1@adminswt]> **ip address export file=nama-script**

Ganti "**nama-script**" pada baric command tersebut dengan nama yang kita ingin dan file akan tersimpan dengan ekstensi **.rsc** , metode backup ini hanya dilakukan melalui command line, tidak bisa dilakukan melalui winbox.

Cara Restore Konfigurasi Mikrotik

Untuk mengembalikan konfigurasi yang sudah di-backup sebelumnya masuk ke manu Files. Copy file backup dari komputer ke router Mikrotik dengan drag dan drop seperti sebelumnya. Pilih file backup yang mau di-restore. klik Restore.



Setelah memilih restore seluruh konfigurasi,maka akan ada permintaan untuk Reboot, pilih Yes maka router akan reboot dan setelah itu akan langsung menggunakan konfigurasi hasil Restore. Sekarang konfigurasi router Mikrotik sudah kembali seperti sebelumnya.

Untuk melakukan restore file hasil backup sebagian konfigurasi yang merupakan script, caranya dengan melakukan import file script yang berektensi .src , yaitu dengan command berikut ini :

[Router1@adminswt]> **import nama-script.rsc**

BAB III
KONFIGURASI TAMBAHAN PADA MIKROTIK

Tujuan:

- Peserta dapat mengatur Bandwidth sederhana di Mikrotik
- Peserta dapat memblok port Virus di Mikrotik
- Peserta mampu memblokir situs tertentu menggunakan Web Proxy Mikrotik
- Peserta mampu menggunakan DNS Nawala untuk memblokir Situs-Situs Dewasa pada Mikrotik

3.1 Membagi Bandwidth Sederhana

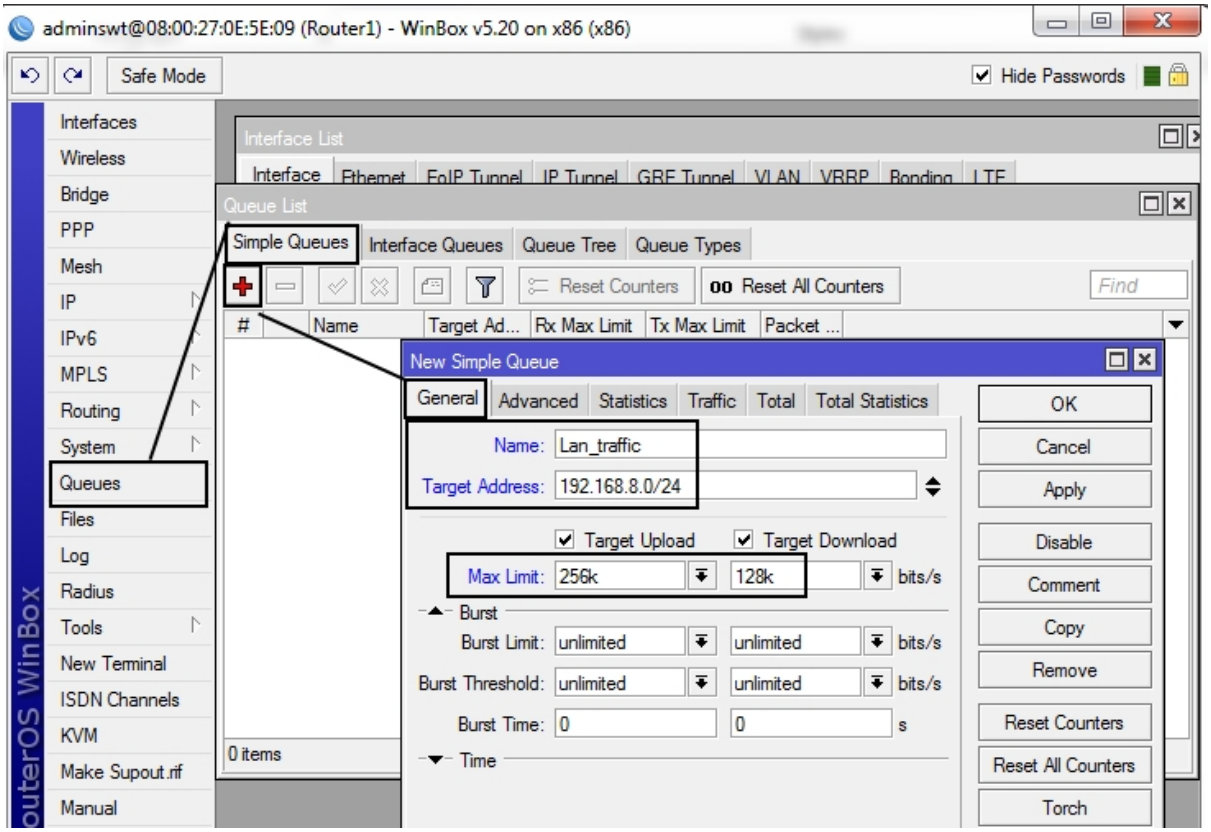
Mikrotik RouterOS memiliki fitur yang berfungsi melakukan management bandwidth yang dinamakan Queue Simple dan Queue Tree.

- Queues Simple – yaitu di desain untuk konfigurasi sederhana, misalnya pembatasan/pembagian bandwidth per client atau p2p traffic dan yang lainnya.
- Queue Tree – adalah fitur untuk penerapan bandwidth management yang lebih kompleks daripada Queue Simple, penerapan Queue Tree memerlukan markin dari fitur Mangle yang ada pada menu Firewall.

Cara yang paling mudah untuk membatasi bandwidth IP Address atau subnet yang spesifik adalah dengan menggunakan simple queue. Berikut ini yang akan kita coba konfigurasikan bandwidth managementnya dengan Queue Simple, kita akan membatasi bandwidth untuk download dan upload pada jaringan local dengan limitasi download = 256Kbps dan upload = 128Kbps. Misalkan nama untuk aturan ini adalah LAN_traffic, commandnya adalah :

[Router1@adminswt]> **queue simple add name=LAN_traffic target-addresses=192.168.8.0/24 max-limit=256/128K interface=Local**

Jika menggunakan winbox adalah: **Queues | Simple Queues | +**

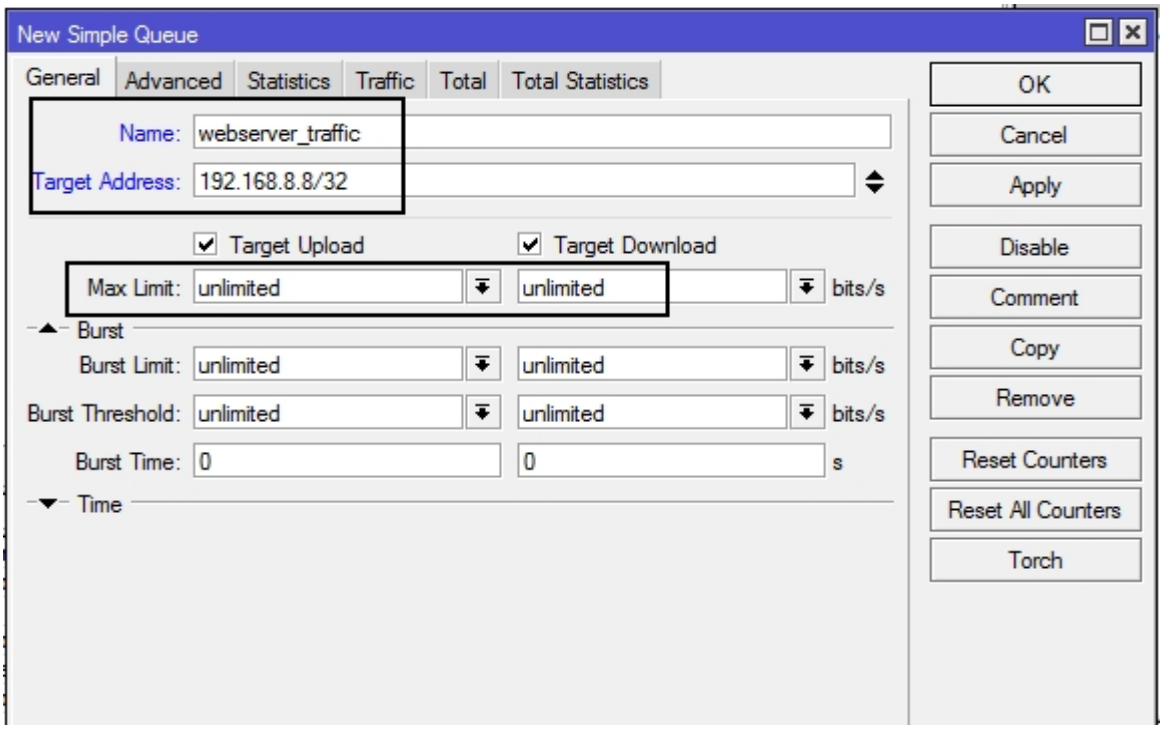


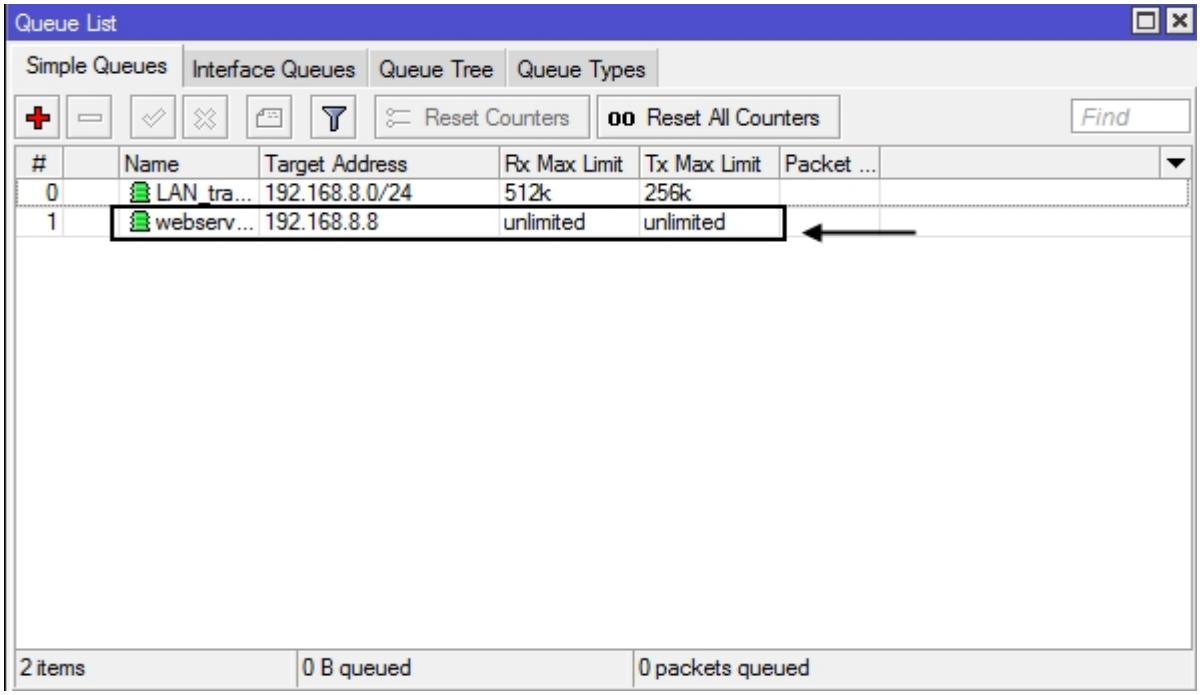
Dengan konfigurasi tersebut maka berapapun bandwidth yang tersedia, bagi ip address dalam network 192.168.8.0/24 tetap akan mendapatkan bandwidth maksimal 256Kbps untuk upload dan 128Kbps untuk download. Jika kita ingin ip address tertentu dalam network tersebut (misalkan web server) agar tidak terkena limitasi yang telah kita buat, maka caranya adalah dengan membuat konfigurasi simple queue yang baru (misalkan dengan nama webserver_traffic) dengan max-limit 0 (unlimited), kemudian konfigurasi tersebut di posisikan di atas konfigurasi LAN_traffic. Commandnya adalah :

[Router1@adminswt]> **queue simple add name=webserver_traffic target-addresses=192.168.8.8/32 max-limit=0/0**

[Router1@adminswt]> **queue simple move webserver_traffic destimation=0**

Jika menggunakan winbox adalah :





3.2 Memblokir Situs menggunakan Web Proxy Mikrotik

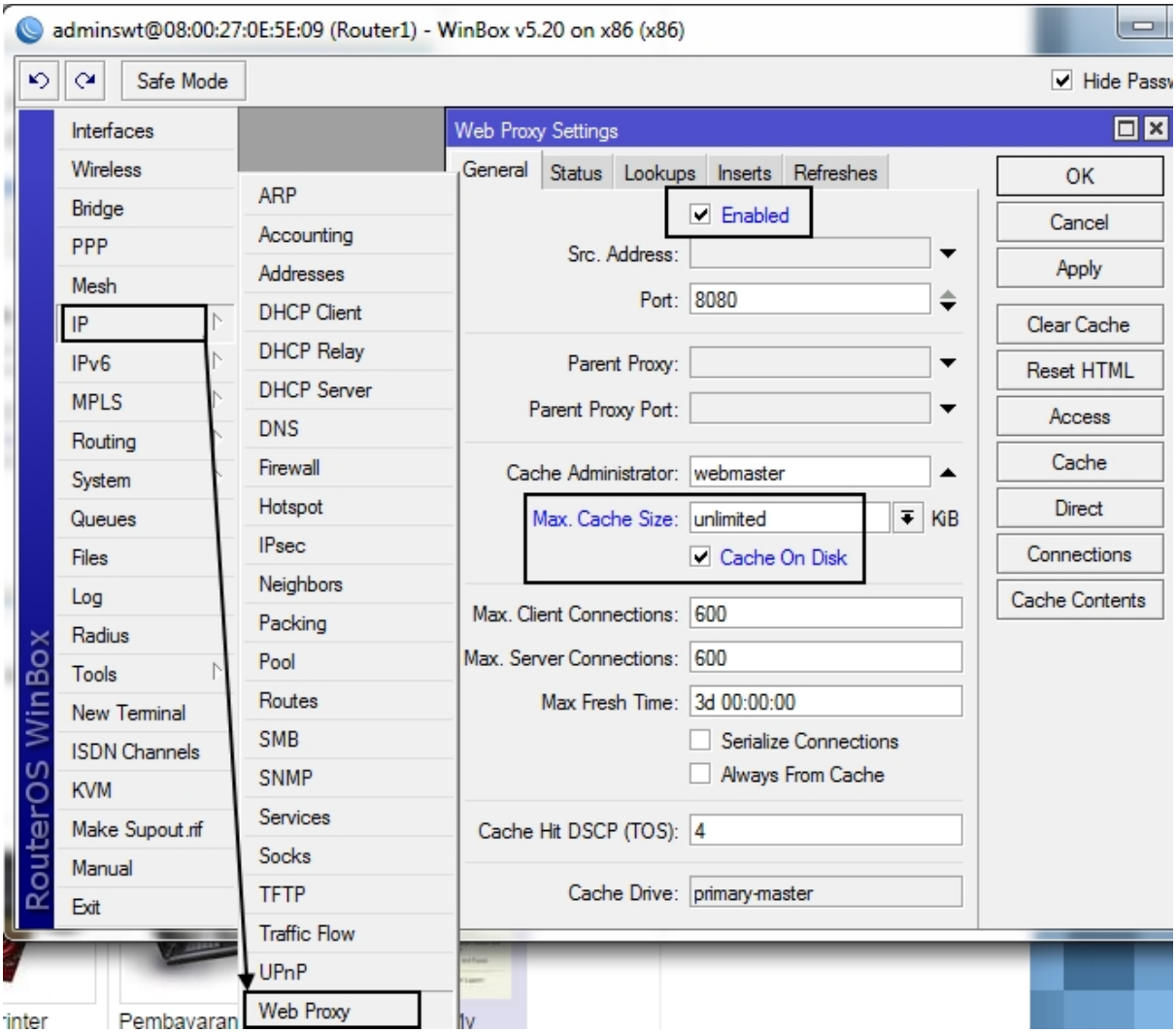
Penggunaan Web Proxy diantaranya adalah untuk menerapkan caching content yaitu web proxy akan menyimpan kontek website yang pernah di akses yang mana konten tersebut akan tersimpan selama waktu yang ditentukan untuk di akses oleh client Mikrotik yang membuka halaman website yang sama, hal ini dapat menghemat website karena client tidak perlu terhubung langsung ke halaman sumber website tersebut, tapi cukup ke web proxy yang ada di Mikrotik.

Kegunaan lain dari web proxy adalah dapat mengatur website yang boleh dan yang tidak boleh di akses atau bahkan men-redirect halaman website tertentu ke halaman yang kita inginkan. Perlu di perhatikan bahwa penggunaan web proxy dapat cukup memperbesar pengunaan resources router Mikrotik, maka jika anda menggunakan Mikrotik dengan spec yang rencah sebaiknya tidak mengaktifkan fungsi web proxy , jika ingin menggunakan web proxy sebaiknya pada Mikrotik yang diinstall pada PC Router dengan spec yang memadai.

Cara konfiguras web proxy cukup sederhanya, commandnya adalah:

[admin@Mikrotik] **> ip proxy set enabled=yes port=8080 max-cache-size=unlimited cache-on-disk=yes**

Jika menggunakan winbox : **IP | Web Proxy**



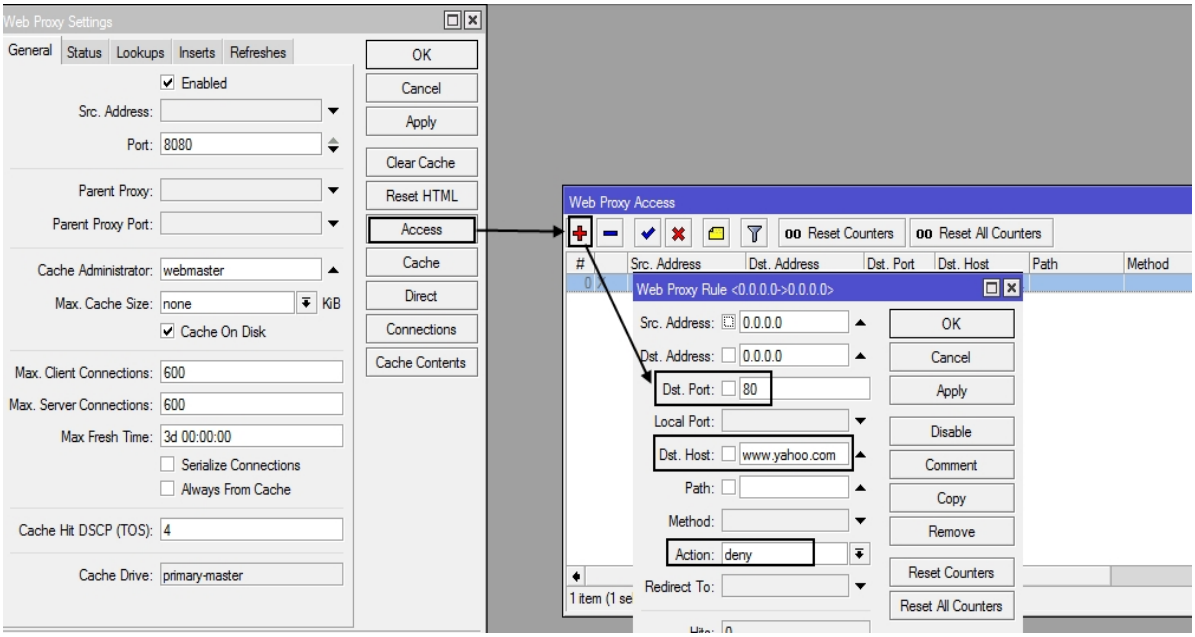
Selanjutnya kita akan coba memblokir sebuah situs tertentu menggunakan fitur filtering Web Proxy ini. Pastikan Transparent Web Proxy Mikrotik sudak aktif. Jika belum silahkan anda setting sesuai tutorial berikut ini :

1. Login ke Mikrotik dengan Winbox
2. Masuk ke menu IP --> Web Proxy --> Access --> Add rule baru
3. Masukkan detail website yang mau di blok

   > Dst. Port : isikan port http 80

   > Dst. Host : isikan alamat website yang mau di blok misalnya www.yahoo.com

   > Action : pilih deny untuk memblokir akses nya



4. Kita juga bisa memodifikasi rule nya dengan me-redirect ke situs lain. Misalnya ketika ada user yang mengakses web www.yahoo.com maka akan langsung dialihkan (redirect) ke www.google.com Tinggal isikan saja alamat website-nya di kolom Redirect To :

3.3 Cara Mudah Memblokir Situs-situs Dewasa dengan DNS

Memblokir Situs-situs Dewasa dengan Mudah di Mikrotik. Menciptakan suasana internet yang sehat itu penting. Apalagi jika banyak client dari jaringan kita adalah anak-anak atau anak sekolah yang belum boleh mengakses konten dewasa. Masalahnya, banyak sekali situs-situs dewasa yang beredar di internet. Hal ini akan menjadi susah jika kita harus memblokir situsnya satu per satu.

Untuk dapat memblokir situs atau konten terentu di internet pada Mikrotik dapat dilakukan dengan cara :

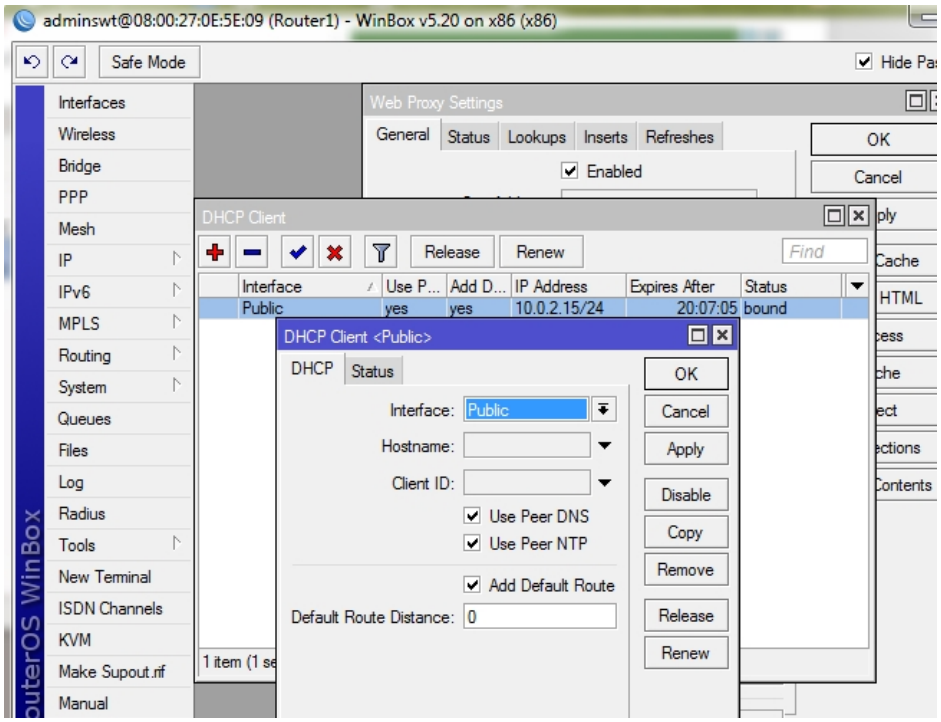
1. Web Proxy
2. DNS Static
3. Firewall

Ketiganya harus memasukkan daftar situs yang akan diblokir secara manual satu per satu. Hal ini tentu akan sangat merepotkan jika jumlah situs yang akan diblokir sampai ratusan bahkan ribuan. Kendala lainnya adalah kita tidak tahu situs apa saja yang harus diblokir. Oleh karena itu solusi yang cocok adalah dengan menggunakan DNS Static. Dalam hal ini kita dapat

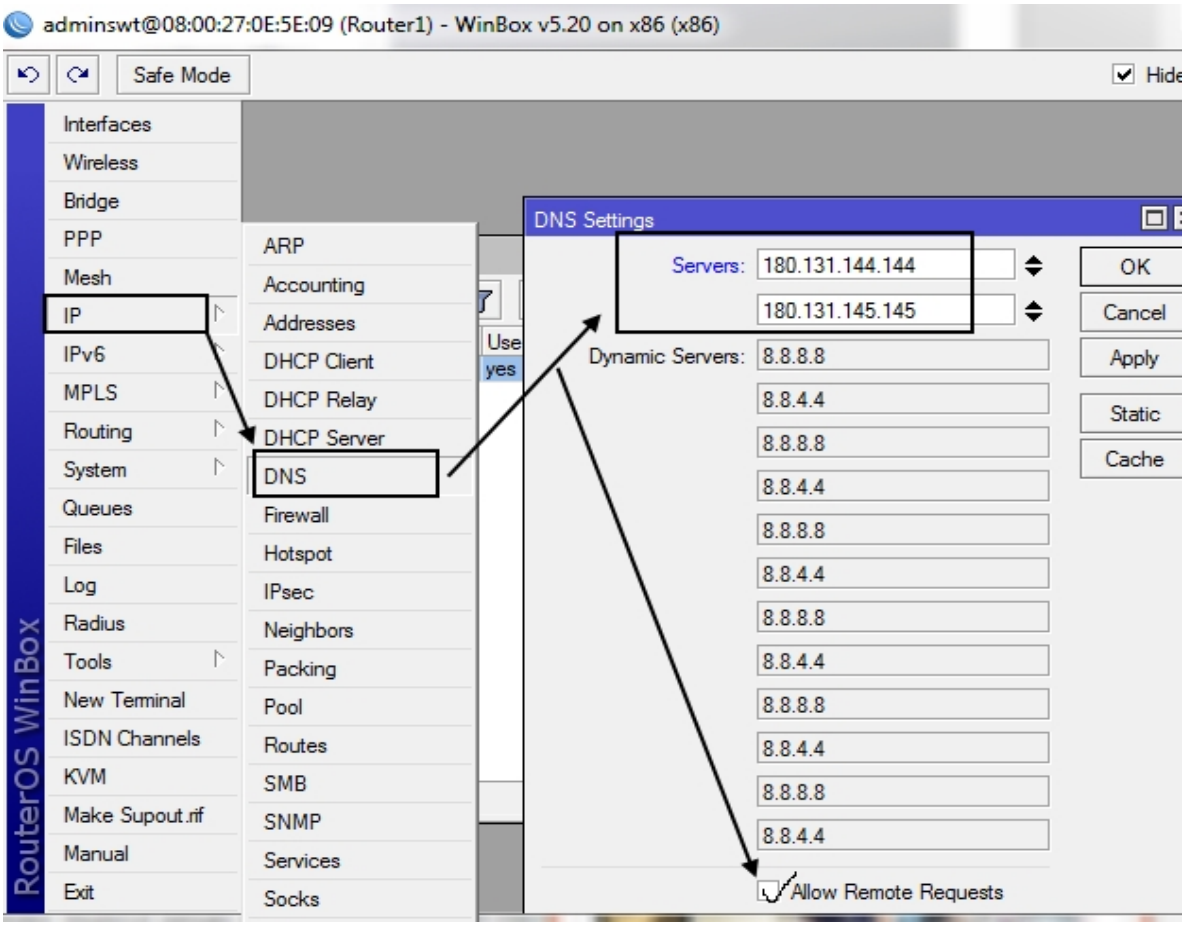
menggunakan DNS Gratis dari Nawala atau OpenDNS yang sudah memfilter konten berbahaya. Jadi kita tidak perlu lagi repot-repot memfilter manual semua situs-situs berbahaya tersebut. Caranya sangat mudah, silahkan anda login ke Mikrotik via Winbox.

1. Jika anda menggunakan DHCP Client, misalnya menggunakan internet dari speedy atau modem GSM maka anda harus menonaktifkan fitur "Use Peer DNS"

   Masuk ke menu IP → DHCP Client → Buka DHCP client nya → unchecklis "Use Peer DNS"



2. Masuk ke menu IP → DNS → Masukkan DNS Server nya di kolom Servers → checklis Allow Remote Request



- DNS Nawala (gratis tanpa register) :

  - 180.131.144.144
  - 180.131.145.145

- DNS OpenDNS (gratis register dulu) → opendns.com

Bedanya jika menggunakan DNS Nawala jika masuk ke situs yang terblokir akan muncul pesan tetapi tidak dapat diganti. Sedangkan kalo OpenDNS bisa kita masukkan pesan tertentu sesuai keinginan seperti pada gambar pertama diatas.

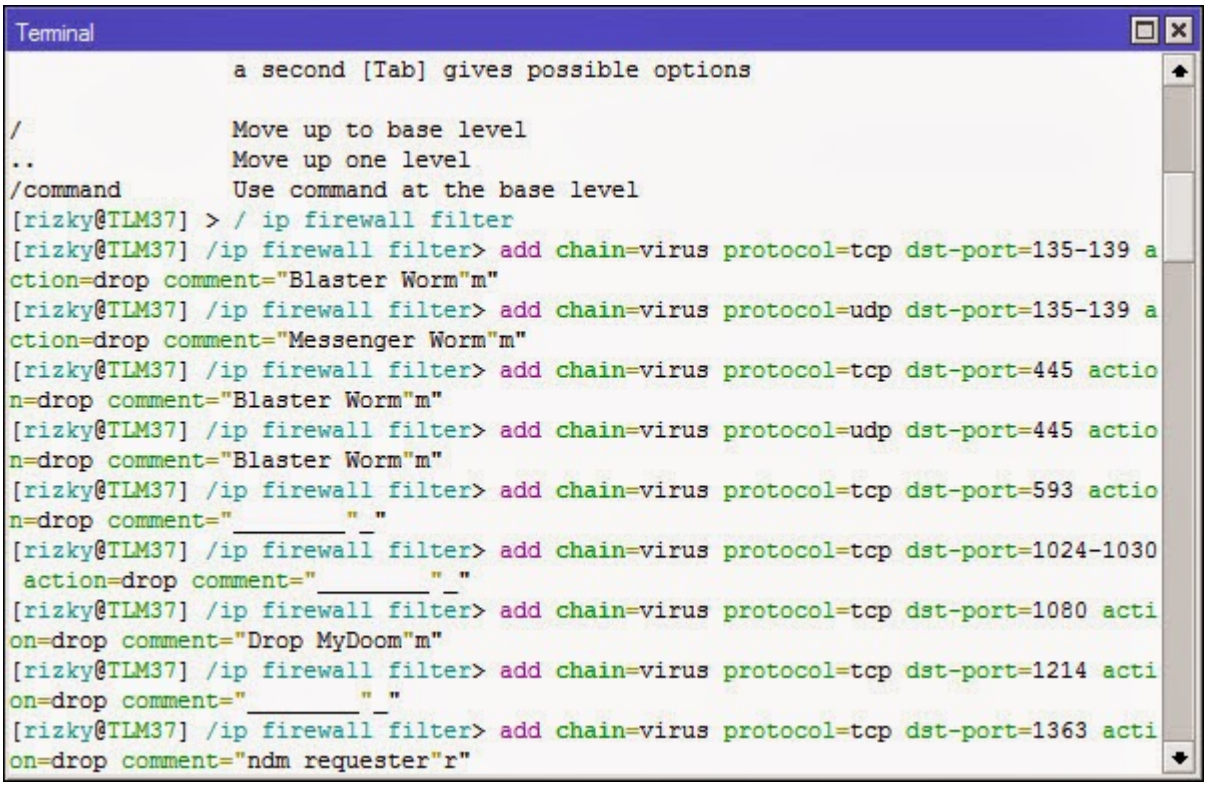
Selain itu, jika menggunakan DNS Nawala kita ga bisa menambahkan atau mengurangi situs yang diblokir, sedangkan kalo menggunakan DNS OpenDNS bisa diatur situs apa saja yang mau diblokir. Namun jika menggunakan OpenDNS harus register dulu.

3. Setelah diganti DNS nya, jangan lupa untuk Flush DNS Cachenya. Pada menu DNS Settings → Cache → Flush Cache

3.4 Memblokir Port Virus di Mikrotik Menggunakan Firewall

Penyebaran virus dan malware di jaringan dapat terjadi jika kita tidak selektif dalam mengaktifkan port apa saja yang digunakan. Untuk mengamankan jaringan dari penyebaran virus dan malware, kita dapat menutup port komunikasi yang tidak digunakan dan rentan dimanfaatkan oleh virus. Caranya dengan menggunakan rule firewall Mikrotik untuk men-drop paket yang masuk ke port yang tidak digunakan.

Caranya sangat mudah, silahkan anda copy paste perintah berikut ini ke terminal Mikrotik :



/ ip firewall filter
add chain=virus protocol=tcp dst-port=135-139 action=drop comment="Blaster Worm"
add chain=virus protocol=udp dst-port=135-139 action=drop comment="Messenger Worm"
add chain=virus protocol=tcp dst-port=445 action=drop comment="Blaster Worm"
add chain=virus protocol=udp dst-port=445 action=drop comment="Blaster Worm"
add chain=virus protocol=tcp dst-port=593 action=drop comment="_____"
add chain=virus protocol=tcp dst-port=1024-1030 action=drop comment="_____"

add chain=virus protocol=tcp dst-port=1080 action=drop comment="Drop MyDoom"
add chain=virus protocol=tcp dst-port=1214 action=drop comment="_____"
add chain=virus protocol=tcp dst-port=1363 action=drop comment="ndm requester"
add chain=virus protocol=tcp dst-port=1364 action=drop comment="ndm server"
add chain=virus protocol=tcp dst-port=1368 action=drop comment="screen cast"
add chain=virus protocol=tcp dst-port=1373 action=drop comment="hromgrafx"
add chain=virus protocol=tcp dst-port=1377 action=drop comment="cichlid"

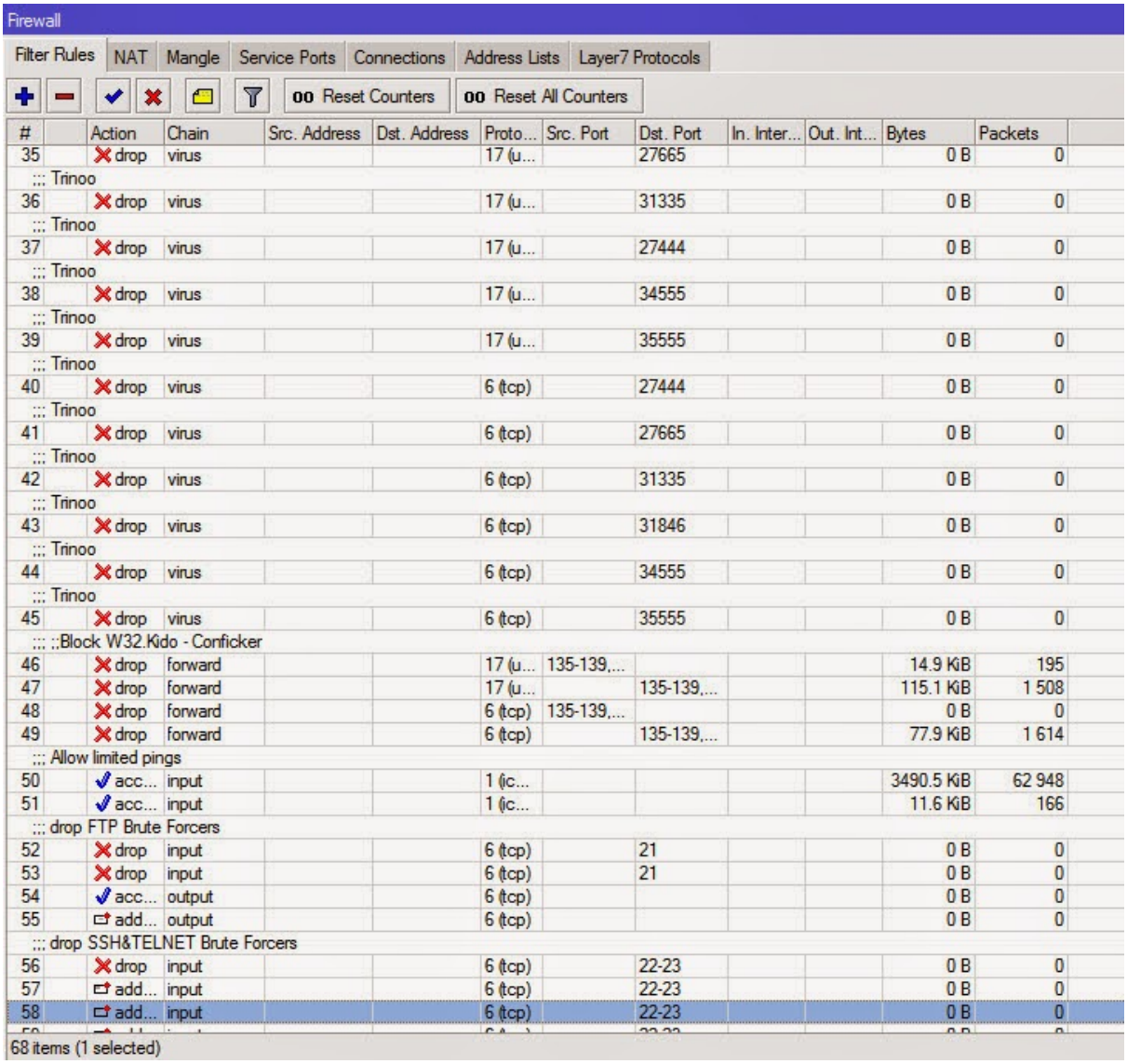
add chain=virus protocol=tcp dst-port=2745 action=drop comment="Bagle Virus"
add chain=virus protocol=tcp dst-port=2283 action=drop comment="Dumaru.Y"
add chain=virus protocol=tcp dst-port=2535 action=drop comment="Beagle"
add chain=virus protocol=tcp dst-port=2745 action=drop comment="Beagle.C-K"
add chain=virus protocol=tcp dst-port=3127-3128 action=drop comment="MyDoom"
add chain=virus protocol=tcp dst-port=3410 action=drop comment="Backdoor OptixPro"
add chain=virus protocol=tcp dst-port=4444 action=drop comment="Worm"
add chain=virus protocol=udp dst-port=4444 action=drop comment="Worm"
add chain=virus protocol=tcp dst-port=5554 action=drop comment="Drop Sasser"
add chain=virus protocol=tcp dst-port=8866 action=drop comment="Drop Beagle.B"
add chain=virus protocol=tcp dst-port=9898 action=drop comment="Drop Dabber.A-B"
add chain=virus protocol=tcp dst-port=10000 action=drop comment="Drop Dumaru.Y"
add chain=virus protocol=tcp dst-port=10080 action=drop comment="Drop MyDoom.B"
add chain=virus protocol=tcp dst-port=12345 action=drop comment="Drop NetBus"
add chain=virus protocol=tcp dst-port=17300 action=drop comment="Drop Kuang2"
add chain=virus protocol=tcp dst-port=27374 action=drop comment="Drop SubSeven"
add chain=virus protocol=tcp dst-port=65506 action=drop comment="Drop PhatBot,Agobot, Gaobot"
add chain=virus protocol=udp dst-port=12667 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=udp dst-port=27665 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=udp dst-port=31335 action=drop comment="Trinoo"

disabled=no
add chain=virus protocol=udp dst-port=27444 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=udp dst-port=34555 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=udp dst-port=35555 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=tcp dst-port=27444 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=tcp dst-port=27665 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=tcp dst-port=31335 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=tcp dst-port=31846 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=tcp dst-port=34555 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=tcp dst-port=35555 action=drop comment="Trinoo" disabled=no
add action=drop chain=forward comment=";;Block W32.Kido - Conficker" disabled=no protocol=udp src-port=135-139,445
add action=drop chain=forward comment="" disabled=no dst-port=135-139,445 protocol=udp
add action=drop chain=forward comment="" disabled=no protocol=tcp src-port=135-139,445,593
add action=drop chain=forward comment="" disabled=no dst-port=135-139,445,593 protocol=tcp
add action=accept chain=input comment="Allow limited pings" disabled=no limit=50/5s,2 protocol=icmp
add action=accept chain=input comment="" disabled=no limit=50/5s,2 protocol=icmp
add action=drop chain=input comment="drop FTP Brute Forcers" disabled=no dst-port=21 protocol=tcp src-address-list=FTP_BlackList
add action=drop chain=input comment="" disabled=no dst-port=21 protocol=tcp src-address-list=FTP_BlackList
add action=accept chain=output comment="" content="530 Login incorrect"

disabled=no dst-limit=1/1m,9,dst-address/1m protocol=tcp
add action=add-dst-to-address-list address-list=FTP_BlackList address-list-timeout=1d chain=output comment="" content="530 Login incorrect" disabled=no protocol=tcp
add action=drop chain=input comment="drop SSH&TELNET Brute Forcers" disabled=no dst-port=22-23 protocol=tcp src-address-list=IP_BlackList
add action=add-src-to-address-list address-list=IP_BlackList address-list-timeout=1d chain=input comment="" connection-state=new disabled=no dst-port=22-23 protocol=tcp src-address-list=SSH_BlackList_3
add action=add-src-to-address-list address-list=SSH_BlackList_3 address-list-timeout=1m chain=input comment="" connection-state=new disabled=no dst-port=22-23 protocol=tcp src-address-list=SSH_BlackList_2
add action=add-src-to-address-list address-list=SSH_BlackList_2 address-list-timeout=1m chain=input comment="" connection-state=new disabled=no dst-port=22-23 protocol=tcp src-address-list=SSH_BlackList_1
add action=add-src-to-address-list address-list=SSH_BlackList_1 address-list-timeout=1m chain=input comment="" connection-state=new disabled=no dst-port=22-23 protocol=tcp
add action=drop chain=input comment="drop port scanners" disabled=no src-address-list=port_scanners
add action=add-src-to-address-list address-list=port_scanners address-list-timeout=2w chain=input comment="" disabled=no protocol=tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg
add action=add-src-to-address-list address-list=port_scanners address-list-timeout=2w chain=input comment="" disabled=no protocol=tcp tcp-flags=fin,syn
add action=add-src-to-address-list address-list=port_scanners address-list-timeout=2w chain=input comment="" disabled=no protocol=tcp tcp-flags=syn,rst
add action=add-src-to-address-list address-list=port_scanners address-list-timeout=2w chain=input comment="" disabled=no protocol=tcp tcp-flags=fin,psh,urg,!syn,!rst,!ack
add action=add-src-to-address-list address-list=port_scanners address-list-timeout=2w chain=input comment="" disabled=no protocol=tcp tcp-flags=fin,syn,rst,psh,ack,urg
add action=add-src-to-address-list address-list=port_scanners address-list-

timeout=2w chain=input comment="" disabled=no protocol=tcp tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg

Hasilnya akan jadi seperti ini :



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
35	drop	virus			17 (u...		27665			0 B	0
;;; Trinoo											
36	drop	virus			17 (u...		31335			0 B	0
;;; Trinoo											
37	drop	virus			17 (u...		27444			0 B	0
;;; Trinoo											
38	drop	virus			17 (u...		34555			0 B	0
;;; Trinoo											
39	drop	virus			17 (u...		35555			0 B	0
;;; Trinoo											
40	drop	virus			6 (tcp)		27444			0 B	0
;;; Trinoo											
41	drop	virus			6 (tcp)		27665			0 B	0
;;; Trinoo											
42	drop	virus			6 (tcp)		31335			0 B	0
;;; Trinoo											
43	drop	virus			6 (tcp)		31846			0 B	0
;;; Trinoo											
44	drop	virus			6 (tcp)		34555			0 B	0
;;; Trinoo											
45	drop	virus			6 (tcp)		35555			0 B	0
;;; ;;Block W32.Kido - Conficker											
46	drop	forward			17 (u...	135-139,...				14.9 KiB	195
47	drop	forward			17 (u...		135-139,...			115.1 KiB	1 508
48	drop	forward			6 (tcp)	135-139,...				0 B	0
49	drop	forward			6 (tcp)		135-139,...			77.9 KiB	1 614
;;; Allow limited pings											
50	acc...	input			1 (ic...					3490.5 KiB	62 948
51	acc...	input			1 (ic...					11.6 KiB	166
;;; drop FTP Brute Forcers											
52	drop	input			6 (tcp)		21			0 B	0
53	drop	input			6 (tcp)		21			0 B	0
54	acc...	output			6 (tcp)					0 B	0
55	add...	output			6 (tcp)					0 B	0
;;; drop SSH&TELNET Brute Forcers											
56	drop	input			6 (tcp)		22-23			0 B	0
57	add...	input			6 (tcp)		22-23			0 B	0
58	add...	input			6 (tcp)		22-23			0 B	0

3.5 Menangkal Netcut dengan Mikrotik

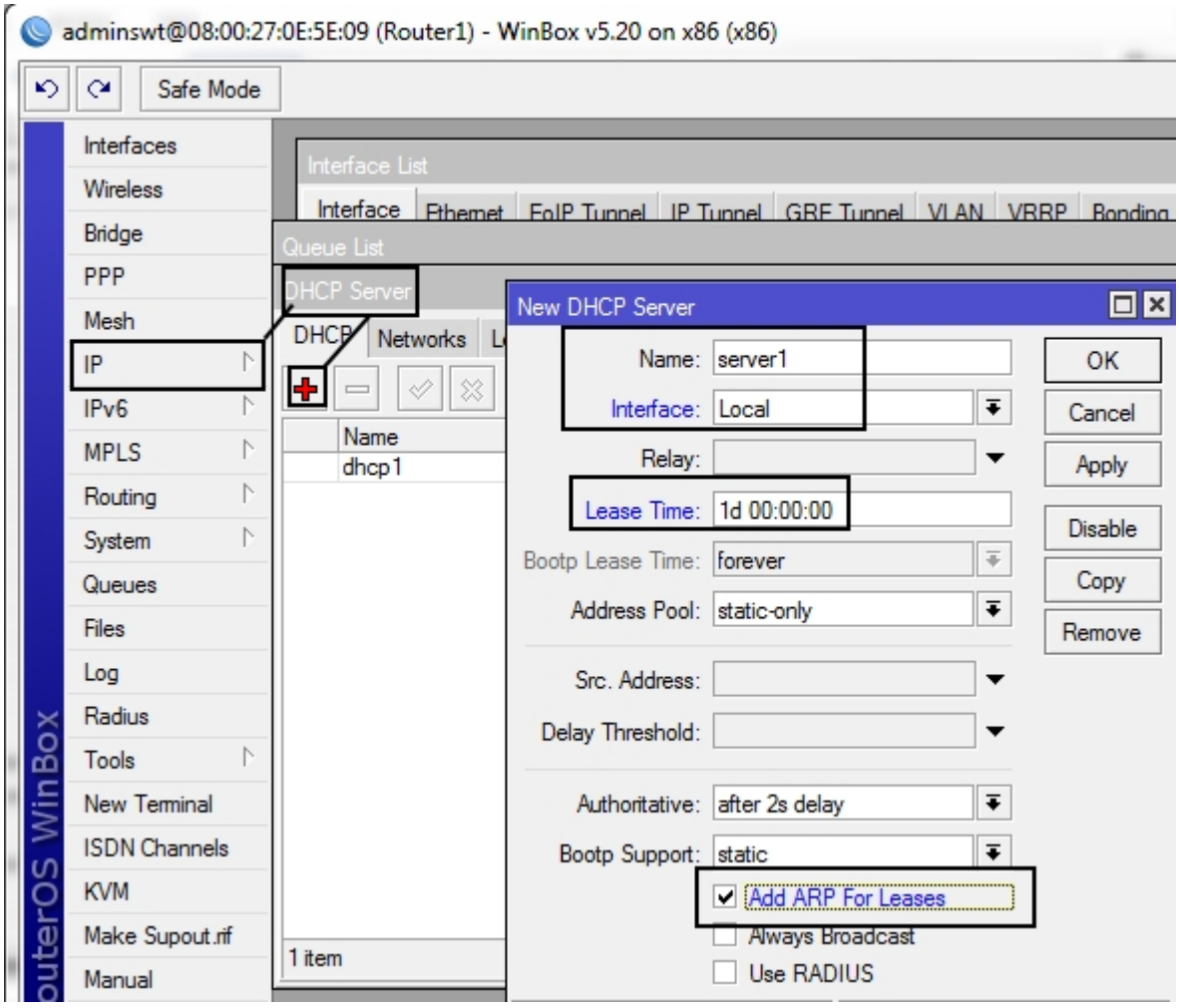
Cara menangkal dan mengatasi Netcut dengan Mikrotik Ini bisa digunakan ketika jaringan anda misalnya hotspot diputuskan oleh orang jahil yang menggunakan Netcut. Netcut adalah sebuah tool yang dapat digunakan untuk memutus koneksi pada jaringan.

Misalnya kita mau memutus koneksi internet di jaringan hotspot supaya bisa memakai semua bandwidth di hotspot itu.

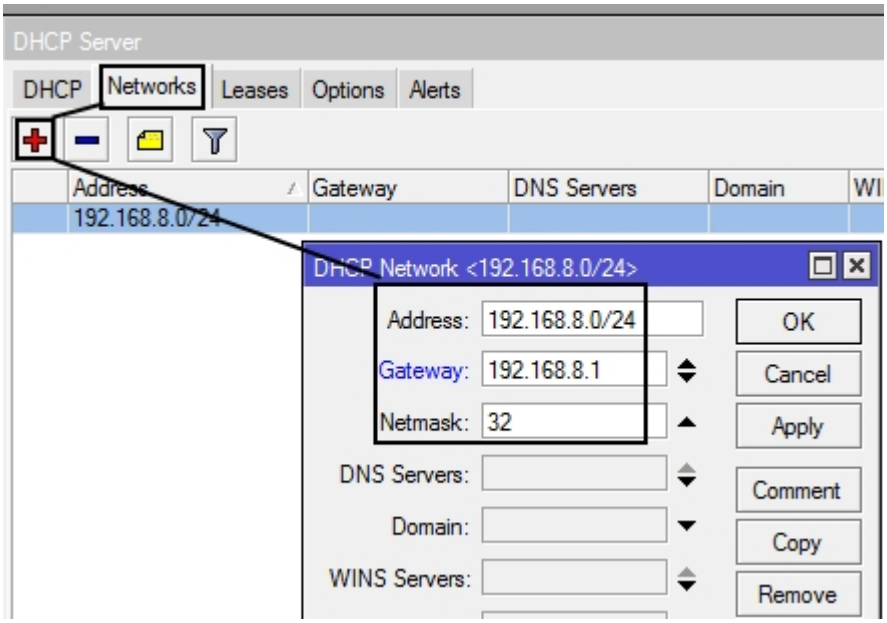
Cara mengatasi netcut menggunakan Mikrotik, lakukan langkah-langkah berikut ini :

1. Masuk ke IP --> DHCP Server
2. Pilih konfigurasi DHCP yang digunakan untuk hotspot anda,
3. Ganti waktu sewa (lease time) IP menjadi 1 hari
4. Dan yang paling penting, aktifkan opsi Add ARP for Leases, opsi ini untuk mencegah ARP Spoofing oleh NetCut

   Untuk lebih jelasnya lihat gambar di bawah ini :



5. Tambahkan netmask /32 untuk single host (255.255.255.255) contonya seperti gambar di bawah ini:



Sampai sini sudah selesai settingan untuk menghindari tangan-tangan jahil.

3.6 Limited Download dan Unlimited Browsing

Pada sub bab ini membahas salah satu teknik manajemen Bandwidth yang efektif untuk membagi bandwidth secara adil. Karena, jika bandwidth download tidak dibatasi, maka akan menggangu kecepatan internet pengguna lain dalam satu jaringan. Akibatnya, jika ada beberapa pengguna yang melakukan download apalagi menggunakan IDM, maka pengguna lain yang cuma browsing tidak kebagian bandwidth.

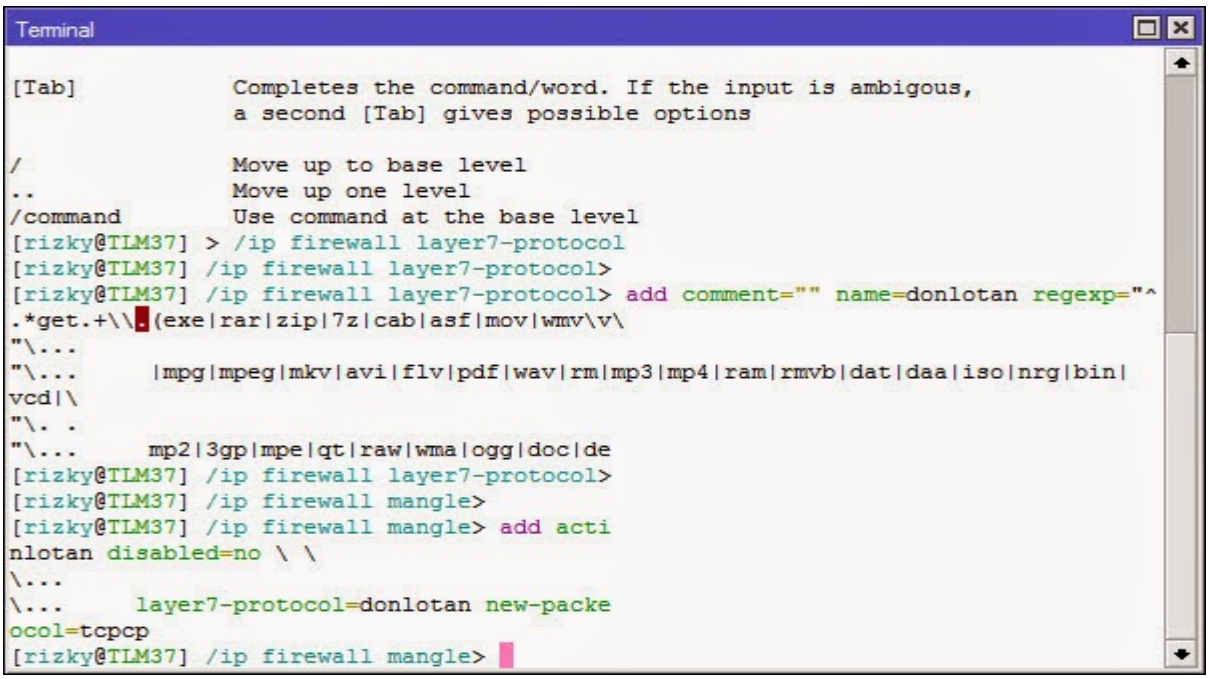
Untuk mengatasi hal ini, maka teknik Limited Download dan Unlimited Browsing ini kita terapkan. Pada Mikrotik, teknik ini bisa dilakukan dengan banyak cara. Salah satu cara yang simpel dan efektif adalah menggunakan filter Layer 7 Protocol. Langkahnya sebagai berikut :

1. Buat daftar ekstensi file yang masuk filter download di Layer 7 protocol. Silahkan copy dan paste script berikut ke Terminal Mikrotik kemudian tekan enter. Jika ekstensi file nya dirasa kurang banyak silahkan ditambahkan sendiri.

```
/ip firewall layer7-protocol

add                              comment=""                                  name=donlotan
regexp="^.*get.+\\.(exe|rar|zip|7z|cab|asf|mov|wmv\

    |mpg|mpeg|mkv|avi|flv|pdf|wav|rm|mp3|mp4|ram|rmvb|dat|daa|iso|nrg|bin|vcd|\

    mp2|3gp|mpe|qt|raw|wma|ogg|doc|deb|tar|bzip|gzip|gzip2|0[0-9][0-9]).*\$"
```

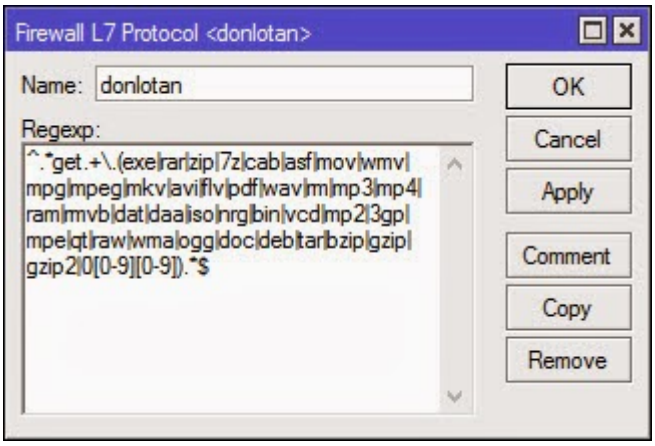
2. Buat Firewall Mangle untuk menandai paket yang mau dilimit. Silahkan copy paste juga script berikut ini ke Terminal dan tekan enter.

```
/ip firewall mangle

add action=mark-packet chain=forward comment=Donlotan disabled=no \

    layer7-protocol=donlotan     new-packet-mark=paket-donlot     passthrough=no
protocol=tcp
```

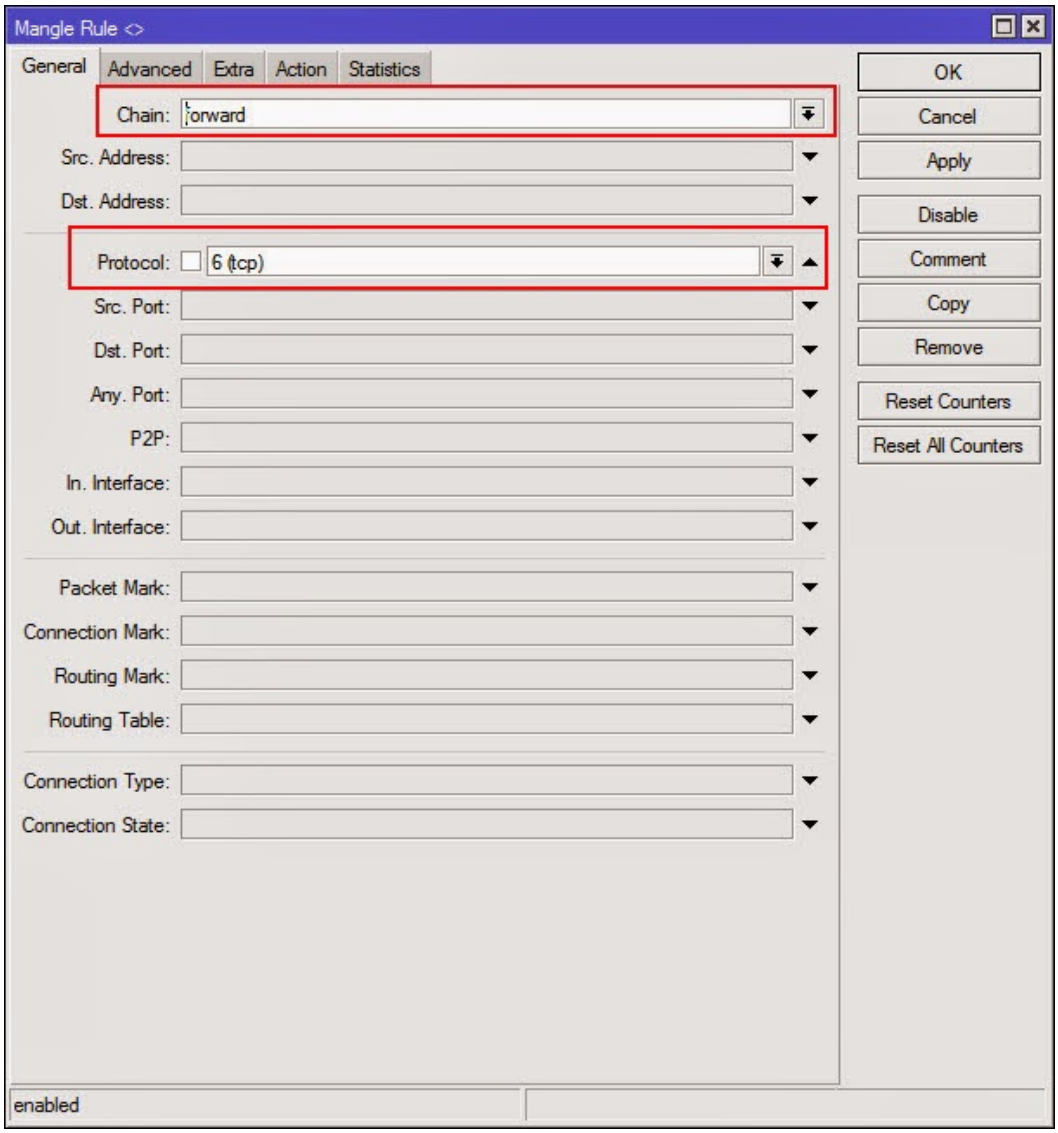


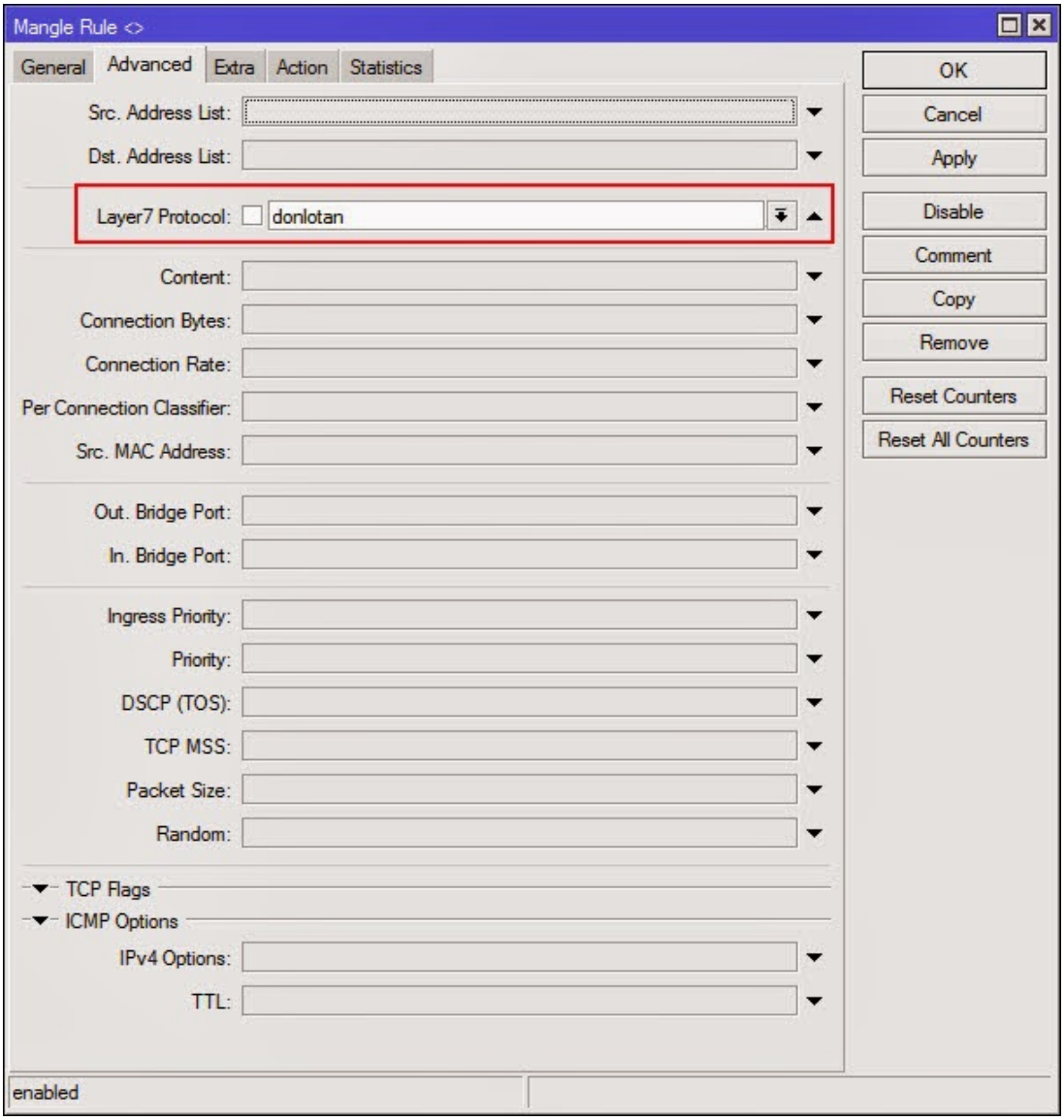
3. Silahkan cek apakah script tadi berhasil dieksekusi menjadi settingan atau tidak.

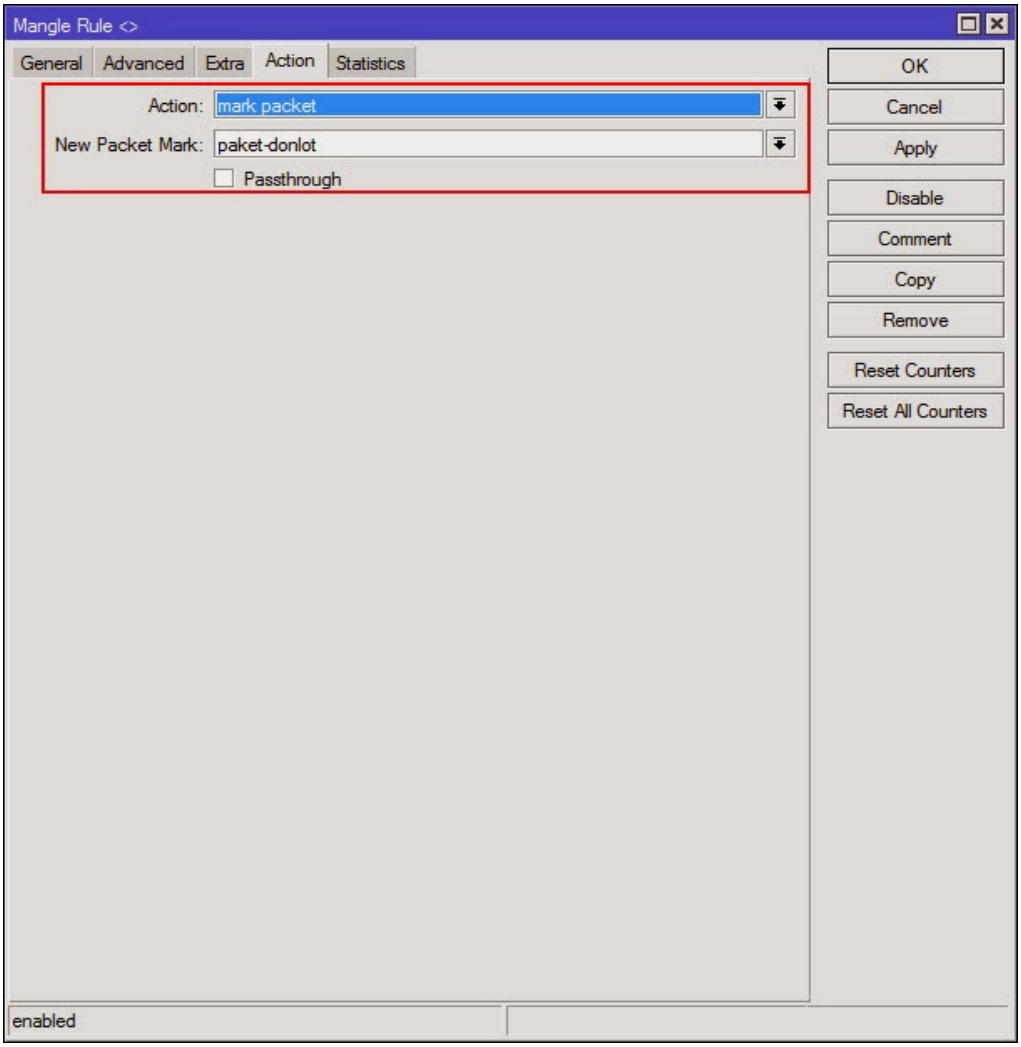
   Cek Settingan Layer 7 protocol : IP → Firewall → Layer7 Protocol



Cek Settingan Mangle : IP → Firewall -→ Mangle




Mangle Rule <>
General
Advanced
Extra
Action
Statistics
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Src. Address List:
Dst. Address List:
Layer7 Protocol:
donlotan
Content:
Connection Bytes:
Connection Rate:
Per Connection Classifier:
Src. MAC Address:
Out. Bridge Port:
In. Bridge Port:
Ingress Priority:
Priority:
DSCP (TOS):
TCP MSS:
Packet Size:
Random:
TCP Flags
ICMP Options
IPv4 Options:
TTL:
enabled



4. Selanjutnya buat limit bandwidth nya dengan Queue.

   Queue Type : Masuk ke Queue → Queue Types → add

   - Beri nama limit dl

   - Kind : pcq

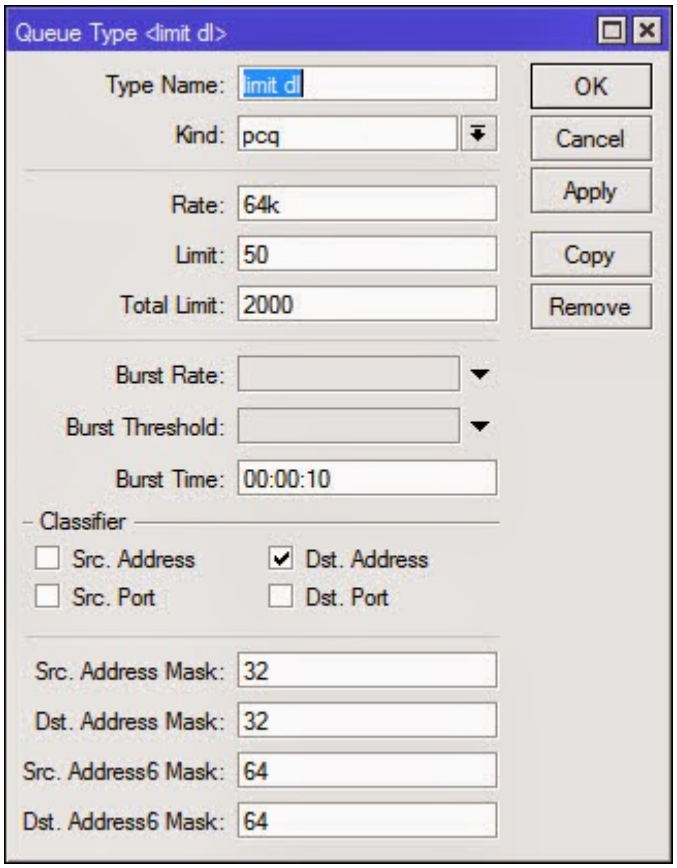
   - Rate : 64k (silahkan sesuaikan dengan keinginan berapa max speed download nya)

   jika diisi 64k, maksudnya membatasi kecepatan download 64 kbps dibagi 8 → 8 KB/s

   jika ingin lebih tinggi bisa saja diisi 256k sehingga throughput : 256/8 = 32 KB/s

   NB : ingat 1 byte = 8 bit

Silahkan diisi sesuai keinginan anda. Settingan lainnya biarkan saja, lihat gambar berikut ini :



Queue Tree : masuk ke Queue → Queue Tree → add

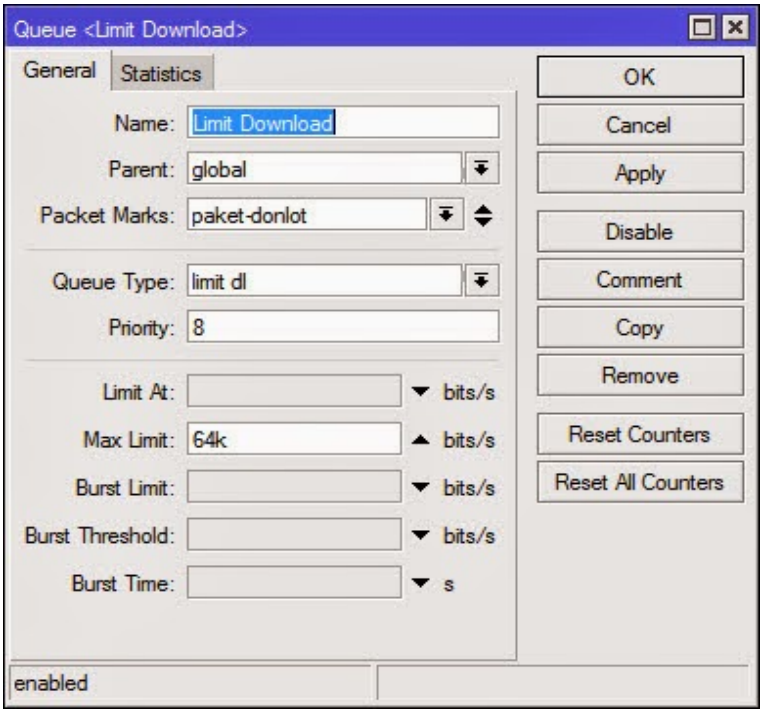
- Beri nama : Limit Download

- Parent : global (Router OS saya versi 6, cuma ada satu parent global)

- Packet Marks : paket-donlot

- Queue Type : limit dl

- Max Limit : 64k (Sesuaikan dengan kebutuhan anda)



5. Settingan selesai. Jadi settingan di atas membatasi bandwidth download sebesar 64kbps = 8KB/s.

BAB IV
RouterOS TOOLS

Tujuan:

- Peserta mengenal dan mengetahui Tools RouterOS
- Peserta dapat menggunakan Tools RouterOS

Mikrotik RouterOS memiliki banyak tools yang berfungsi untuk pengecekan dan monitoring jaringan yang terhubung dengannya. Tools yang akan dibahas disini adalah :

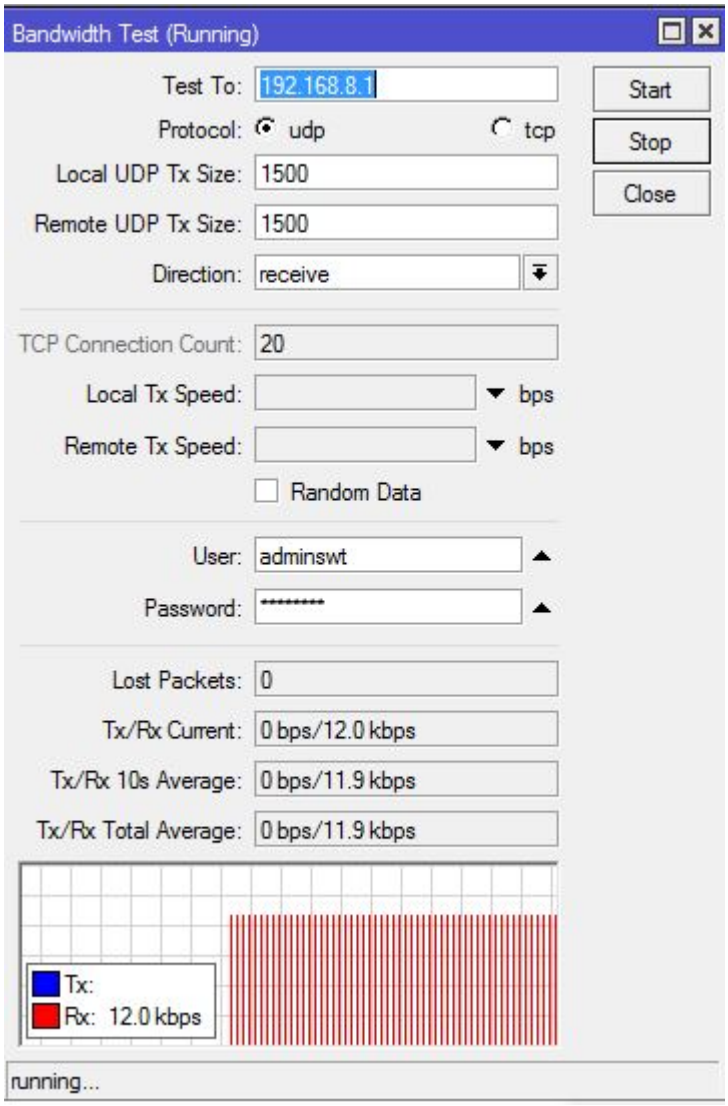
- Bandwith Test
- Flood Ping
- Graphing
- IP-Scan
- Netwatch
- Packet Sniffer
- Torch
- Tracerouter

4.1 Bandwidth Test

Ini adalah fitur untuk melakukan test bandwidth antara dua router Mikrotik dengan cara salah satunya dijadikan Btest Server kemudian yang satu lagi melakukan test bandwidth yang ditujukan ke Btest Server untuk mendapatkan hasil test. Melakukan bandwidth dedicated line site-to-site.

Berikut ini contoh command dan hasil bandwidth test

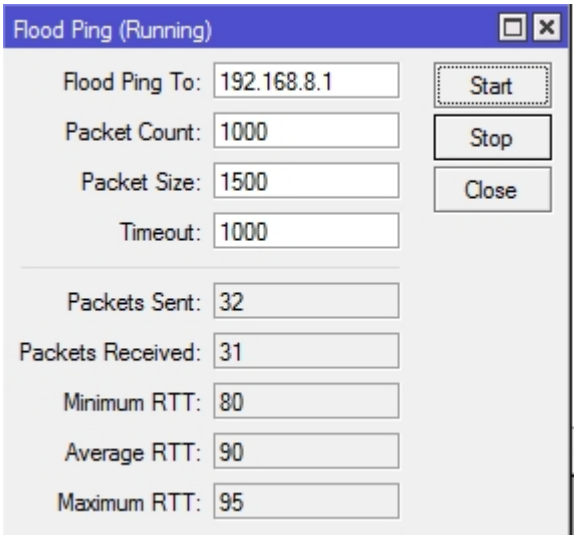
[Router1@adminswt]> **tool bandwidth-test 192.168.8.1 duration=15s direction=both local-dup-tx-size=1000 protocol=udp remote-udp remote-udp-rx-size=1500 user=admin password=passwd**



4.2 Flood Ping

Flood Ping adalah tool untuk mengirimkan paket ICMP (Internet Control Message Protocol) echo request ke remote hosts sebagamana penggunaan ping pada umumnya seperti biasa, hanya saja bedanya tool ini bisa menentukan berapa besar ukuran paket yang dikirim dan berapa banyak jumlah paket yang akan dikirim, sehingga request ICMP dilakkukan secara terus-menerus hingga mencapai jumlah paket yang kita tentukan.

[Router1@adminswt]> **tool flood-ping address=8.8.8.8**

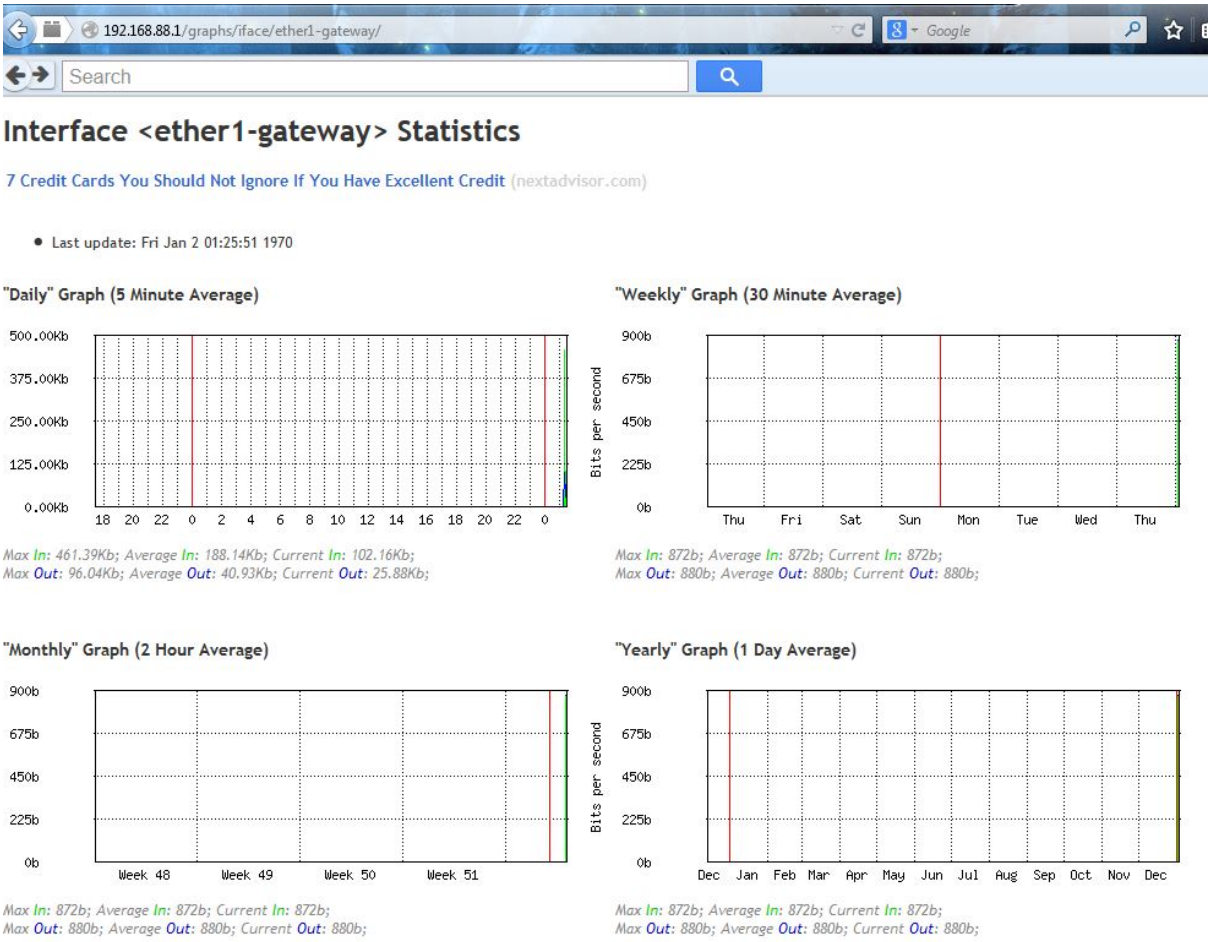


4.3 Graphing

Graphing adalah tool untuk monitoring beberapa resources RouterOS menampilkannya dalam bentuk grafik/gambar. Tool ini dapat menampilkan grafik mengenai :

- Roureboard health (voltage and temperature)
- Resource usage (CPU, Memory and Disk Usage)
- Traffic which is passed through interfaces
- Traffic which is passed throught simple queues

Untuk melihat tampilan grafiknya adalah dengan cara mengakses melalui browser ke http://ip-address-Mikrotik/graphs, berikut ini contoh tampilan grafik mengenai PCU usage dari router Mikrotik.

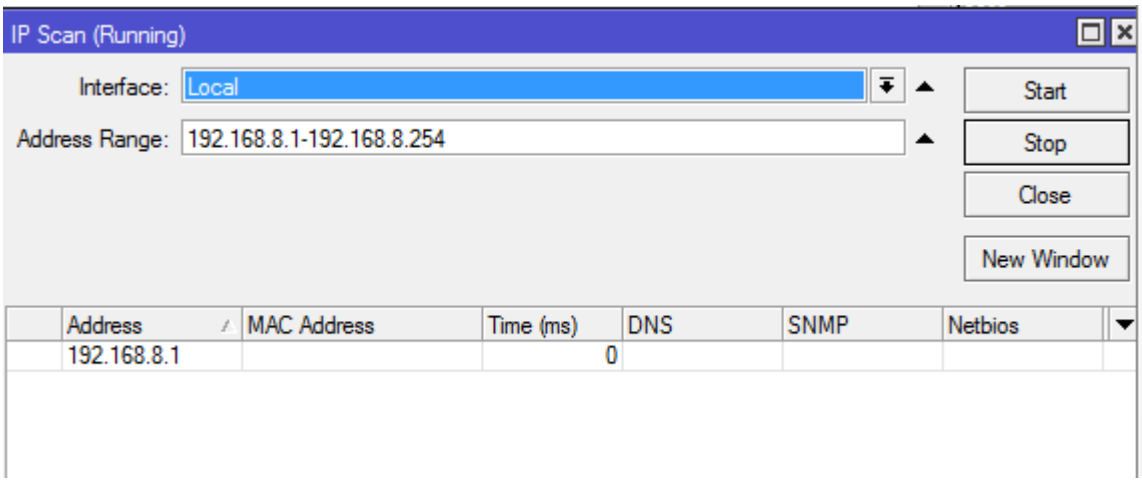


4.4 IP Scan

IP Scan adalah tool yang fungsinya sama dengan software ip scan pada umumnya, yaitu untuk melakukan pemindaian/scanning range IP Address dan menampilkan hasilnya dengan disertai mac address dan netbios host yang berhasil di scan. Commandnya adalah :

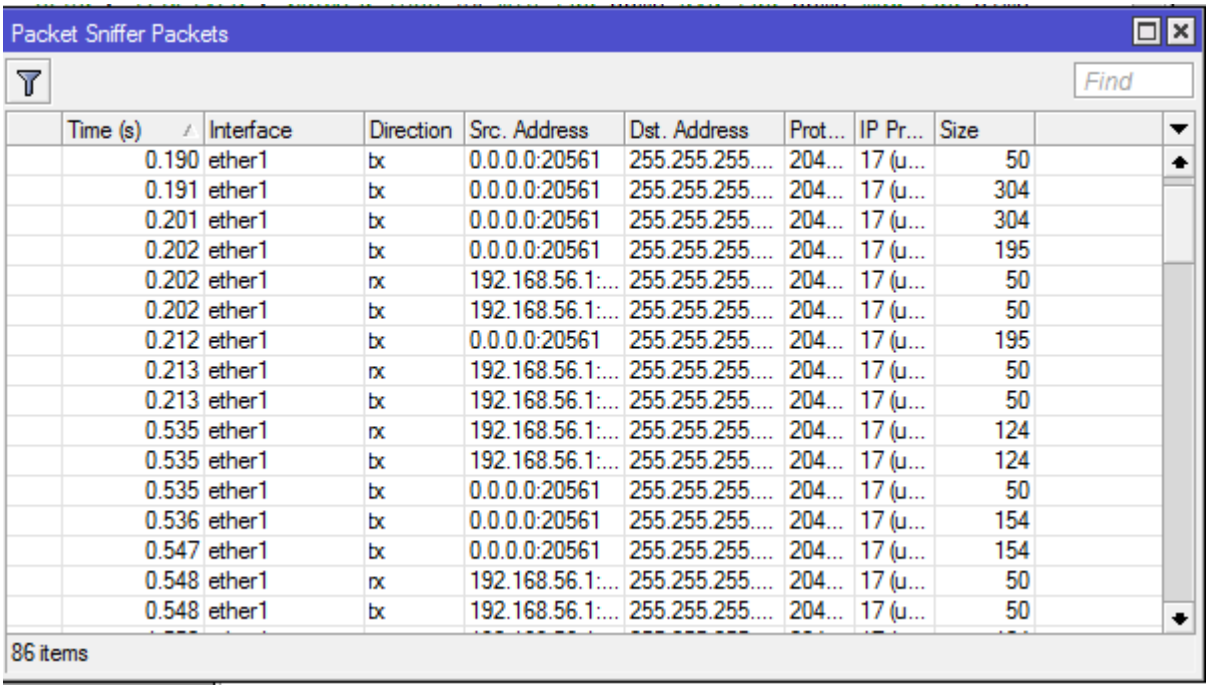
[Router1@adminswt]> **tool ip-scan interface=Local address-range=192.168.8.1-192.168.8.254**

Jika menggunakan winbox: **Tools | IP Scan**



4.5 Packet Sniffer

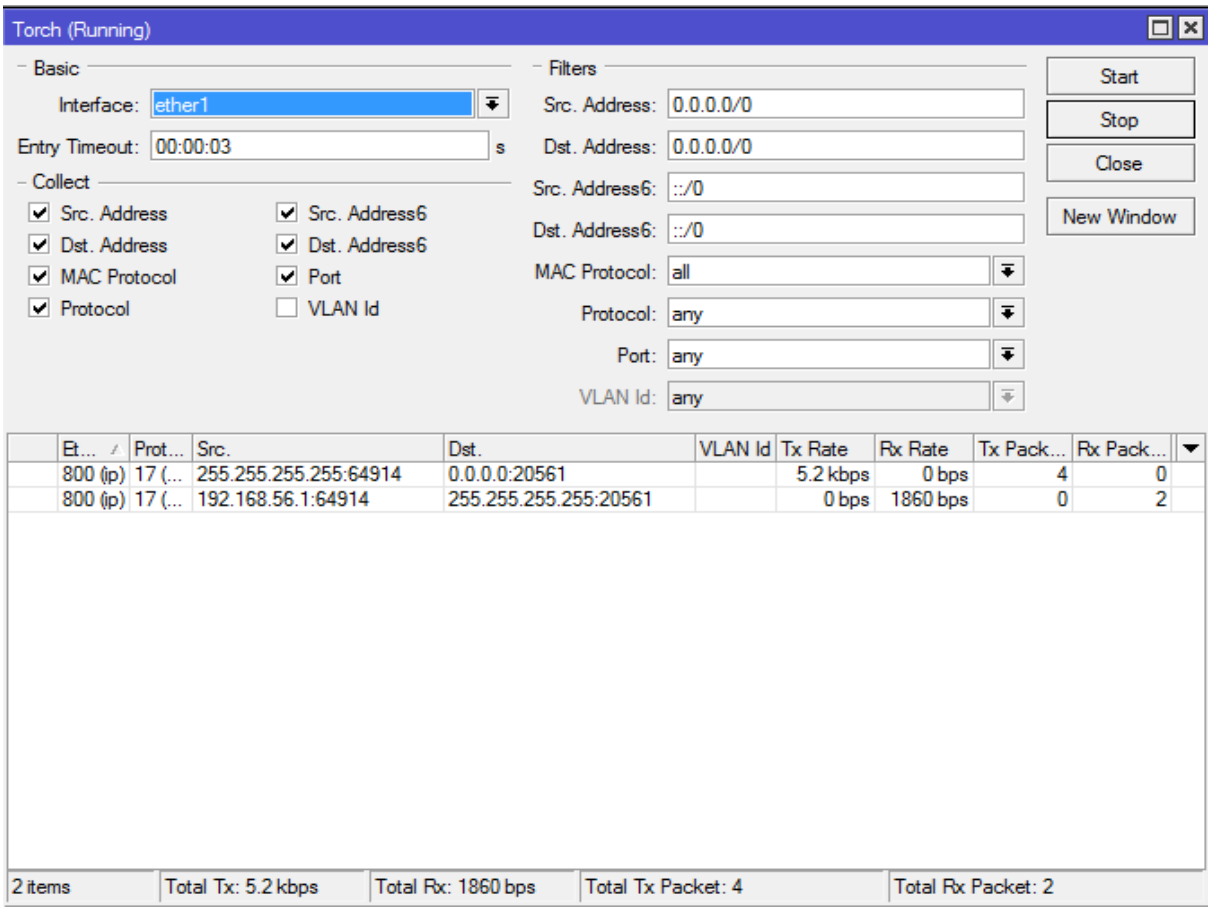
Ini adalah tool yang fungsinya untuk melakukan sniffing/penyadapan paket traffic yang melewati interface yang di sadap, tool ini bermanfaat untuk menganalisa pake traffic, fungsi ini hampir sama dengan tool netstat dan tcpdump. Berikut ini contoh tampilan paket hasil sniffing pada winbox :



4.6 Torch

Torch adalah tool monitoring traffic realtime yang melewati suatu interface dalam kondisi realtime, tool ini bermanfaat untuk menganalisa traffic sekaligus besar bandwidth

yang terpakai oleh ip address tertentu maupun oleh interface. Berikut ini contoh tampilan torch pada winbox : **Tool |Torch | Start**



DAFTAR PUSTAKA

Rizky Agung Pratama , Tutorial Mikrotik : http://Mikrotikindo.blogspot.com/

Mikrotik Fundamental. PT.Excellent Infotama Kreasindo.

Untuk informasi lebih lanjut, silakan menghubungi:

Program Studi Teknik Informatika
Fakultas Teknologi Informasi
Universitas YARSI

1. Helmi Prasetyo, S.Kom
   E-mail : swtprasz8888@gmail.com

2. Sri Puji Utami A., M.T
   E-mail : puji.atmoko@yarsi.ac.id

3. Herika Hayurani, M.Kom
   E-mail : herika.hayurani@yarsi.ac.id