

[Step by Step]

Buat Router Mudah Dengan MikroTik

(It's Very Simple & Komprehensif)

*Siapa bilang buat router itu susah, sudah nggak zamanya lagi
Dan kebetulan fungsi routing memang paling dibutuhkan dan sering ditanyakan jika
berkaitan dengan networking ☺*

Kali ini ana sekali-kali buat tutorial praktis (orientasi praktek langsung) tentang jaringan namun komprehensif ☺

Sekaligus sebagai log, sebab kemarin habis ngerjain router mikrotik punya teman

Syarat yang dibutuhkan disini hanyalah: "**Mau belajar dan nggak takut duluan :)**"

Semoga bermanfaat...

Pengantar Mikrotik

Mikrotik RouterOS adalah sebuah mesin linux yang dirancang secara khusus untuk keperluan networking.

Mikrotik ini begitu menarik saat ini, karena dengan fiturnya yang begitu lengkap serta kemudahan dalam penggunaannya dan juga relatif lebih murah (apalagi dibanding Cysco)

Dan dalam networking, mikrotik hampir dibilang lebih dari yang lain (meski kita ingin membuat jaringan yang kompleks), kelemahannya cuma dalam performance proxy (dibanding squid) serta jika routerboard-nya dibanding cysco kalah dalam hardware yang digunakan

Jika kita sudah memahami konsep jaringan dengan baik maka akan begitu mudah menerapkan di MikroTik dengan tool GUI-nya (winbox), sehingga kita tak perlu menghafal command untuk melakukan setting

Step By Step:

Minimum Hardware:

Standard PC yang kita jadikan router tidak butuh resource yang besar, apalagi untuk penggunaan standard (gateway misalnya)

Namun untuk beban yang besar (network kompleks atau routing yang rumit) bagus untuk mempertimbangkan memilih resource PC memadai

Pentium I, II, III, AMD, Cyrix dll

Asal bukan multi-prosesor/hyper threading

RAM 64 MB (Minimum 32 MB)

Kalau sekalian untuk proxy 1GB sangat dianjurkan

Harddisk **IDE** 400 Mb

Minimal 128MB parallel ATA atau Compact Flash

Tidak dianjurkan menggunakan UFD, SCSI, dan juga S-ATA (menunggu update Versi terbaru)

NIC 10/100 atau 100/1000

Instalasi

Boot dari CDROM >>>

Masukkan CD MIKROTIK >>>

Akan muncul seperti ini....

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 'r' to
install remote router or 'q' to cancel and reboot.

```
[X] system          [ ] lcd             [ ] telephony
[ ] ppp             [ ] ntp             [ ] ups
[ ] dhcp           [ ] radiolan        [ ] user-manager
[ ] advanced-tools [ ] routerboard     [ ] web-proxy
[ ] arlan          [ ] routing         [ ] webproxy-test
[ ] gps            [ ] routing-test    [ ] wireless
[ ] hotspot        [ ] rstp-bridge-test [ ] wireless-legacy
[ ] hotspot-fix    [ ] security
[ ] isdn           [ ] synchronous
```

system (depends on nothing):
Main package with basic services and drivers

[x] Keterangan beberapa yang penting diantaranya:

- System : Packet wajib install (inti system mikrotik/paket dasar), berisi Kernel Mikrotik
- PPP : Untuk **membuat Point to Point Protocol Server**
Point-to-Point tunneling protocols - PPTP, PPPoE and L2TP Access Concentrators and clients; PAP, CHAP, MSCHAPv1 and MSCHAPv2 authentication protocols; RADIUS authentication and accounting; MPPE encryption; compression for PPPoE; data rate limitation; differentiated firewall; PPPoE dial on demand
- Dhcp : Packet yang dibutuhkan apabila ingin **membuat dhcp-server** (agar client bisa mendapatkan ip address otomatis -dynamic IP)
* DHCP - DHCP server per interface; DHCP relay; DHCP client; multiple DHCP networks; static and dynamic DHCP leases; RADIUS support
- Advanced tool : **Tools tambahan untuk administrasi jaringan seperti ip-scan, bandwidth test, Scanning, Nslookup** dll
- Arlan : Packet untuk **konfigurasi chipset wireless aironet arlan**
- Gps : Packet untuk **support GPS Device**
- Hotspot : Packet untuk **membuat hotspot gateway, seperti authentication , traffic quota dan SSL**
HotSpot Gateway with RADIUS authentication and accounting; true Plug-and-Play access for network users; data rate limitation; differentiated firewall; traffic quota; real-time status information; walled-garden; customized HTML login pages; iPass support; SSL secure authentication; advertisement support
- Hotspot -fix: **Tambahan packet hotspot**
- Security : Berisi fasilitas yang mengutamakan Keamanan jaringan, seperti Remote Mesin dengan SSH, Remote via MAC Address
- Web-proxy : Untuk menjalankan service Web proxy yang akan menyimpan cache agar traffik ke Internet bisa di reduksi sehingga sensasi browsing lebih cepat

FTP and HTTP caching proxy server; HTTPS proxy; transparent DNS and HTTP proxying; SOCKS protocol support; DNS static entries; support for caching on a separate drive; access control lists; caching lists; parent proxy support

- Isdn : Packet **untuk isdn server dan isdn client** membutuhkan packet PPP
- Lcd : Packet untuk **customize port lcd**
- Dll

[x] Umumnya Paket Mikrotik untuk Warnet, Kantor atau SOHO (sebagai fungsi router, transparent dan Dhcp) adalah :

System, Dhcp, Advance Tools, RouTing, Security, Web-Proxy

Tapi kalo kita bingung mending centang saja semua apalagi installernya kecil dan installnya sangat cepat, juga besoknya bisa kita uninstall/disable paket itu

[x] Kita pilih service apa saja yang ingin kita install

[x] Tekan:

'a' = semua service akan terpilih

'n' = bila kita menginstall baru

'y' = bila kita hanya ingin menambah service baru (konfigurasi sebelumnya tidak akan hilang)

[x] Lalu ketik " i " untuk memulai instalasi, maka proses berlanjut...

"proses format dan pengkopian file-file yang dibutuhkan akan berjalan otomatis"

```
system (depends on nothing):  
Main package with basic services and drivers
```

```
Do you want to keep old configuration? [y/n]:n
```

```
Warning: all data on the disk will be erased!
```

```
Continue? [y/n]:y
```

```
Creating partition.....  
Formatting disk.....
```

```
installed system-2.9.27  
installed hotspot-fix-2.9.27  
installed hotspot-2.9.27  
installed ppp-2.9.27  
installed routing-test-2.9.27  
installed advanced-tools-2.9.27  
installed arlan-2.9.27  
installed dhcp-2.9.27  
installing gps-2.9.27 [*****]
```

[x] Setelah selesai, tekan Enter untuk reboot...

[x] Setelah komputer booting maka akan ada pilihan untuk melakukan check system disk, tekan " y " (tekan "n", jika yakin Hardisk kita tidak ada badsector)

[x] lalu akan tampil user login dan password:

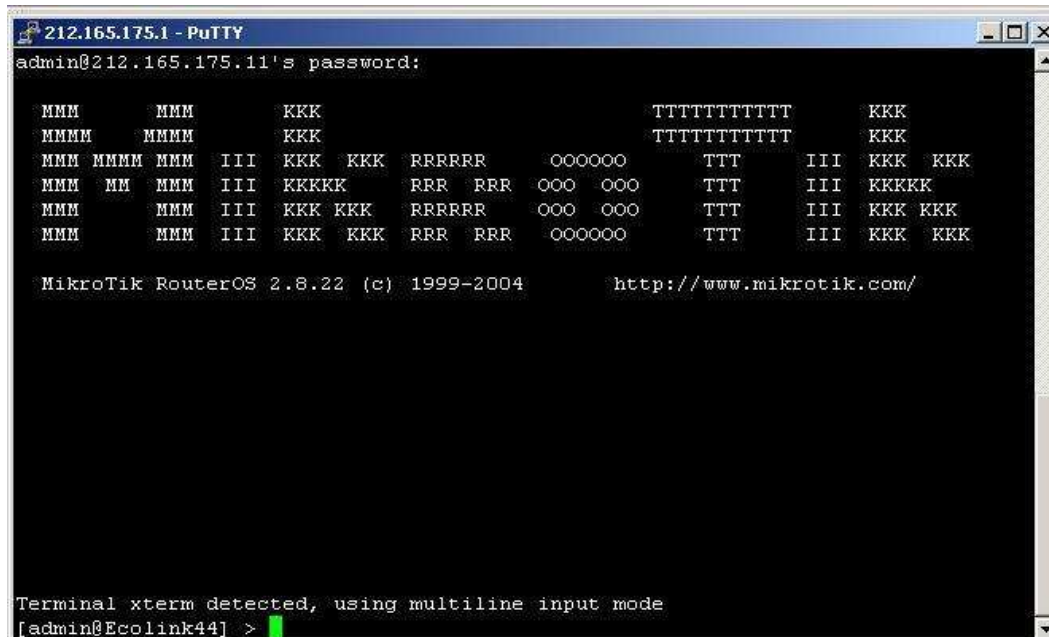
Mikrotik 2.9.27

Mikrotik Login:

Default user = admin dan password kosong (langsung Enter saja)

[x] Untuk software license tekan " y " . Lalu enter beberapa kali sampai

muncul prompt untuk command line
[x] Setelah login akan tampil seperti ini:



```
212.165.175.1 - PuTTY
admin@212.165.175.11's password:

MMM      MMM      KKK      TTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTT      KKK
MMM MMMM MMM III  KKK  KKK  RRRRRR   000000   TTT   III  KKK  KKK
MMM MM  MMM  III  KKKKK  RRR  RRR  000  000   TTT   III  KKKKK
MMM     MMM  III  KKK  KKK  RRRRRR   000  000   TTT   III  KKK  KKK
MMM     MMM  III  KKK  KKK  RRR  RRR  000000   TTT   III  KKK  KKK

MikroTik RouterOS 2.8.22 (c) 1999-2004      http://www.mikrotik.com/

Terminal xterm detected, using multiline input mode
[admin@Ecolink44] >
```

Nah, setelah proses diatas kita sudah mulai bisa menggunakan tool winbox *sehingga jadi lebih mudah*

3 Cara Akses Mikrotik:

1. Via Console/Command

Mikrotik (Jenis router board maupun PC) bisa kita akses langsung via console/shell maupun remote akses menggunakan putty (www.putty.nl)

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

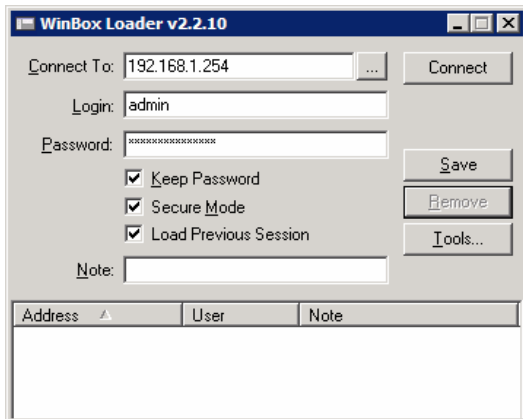
Mikrotik bisa juga diakses via web/port 80 di browser

Contoh ketik di browser IP mikrotik kita: 192.168.0.18

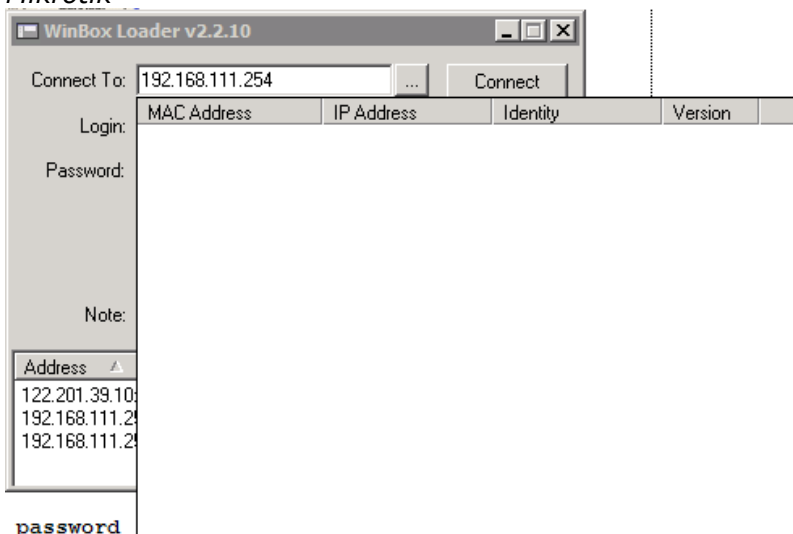
3. Via Winbox

Mikrotik bisa juga diakses/remote menggunakan tool winbox (utility kecil di windows yang sangat praktis dan kerenz)

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



password

>>> Maka kita tinggal pilih MAC address yang sudah terdeteksi dan klik tombol Connect

Kita Ubah Password Defaultnya (biar aman):

Command:

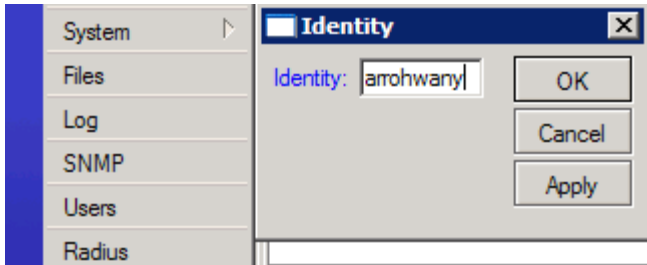
```
[admin@Mikrotik] > password
old password: (Enter)
new password: ***** (ketik password baru kita)
retype new password: *****
[admin@ Mikrotik] > _
```

Ganti Nama System Kita:

Via Command:

```
[admin@bismillah] > system identity set name=bismillah
(Bismillah = contoh saja)
>>> Lalu tekan Ctr-O untuk menyimpan dan keluar dari editor
>>> Maka prompt shell akan berubah jadi:
[admin@ bismillah] > _
```

Via winbox:



Aktifkan Kedua Lancard (ethernet) Kita (jika belum aktif)

Check dulu; siapa tahu belum ke-detect/belum aktif:

```
[admin@ bismillah] > /interface print
Flags: X - disabled, D - dynamic, R - running
#   NAME      TYPE      RX-RATE  TX-RATE  MTU
0   X ether1    ether    0         0        1500
1   R ether2    ether    0         0        1500
```

Jika belum ke-detect, mungkin karna 2 sebab:

- [x] LAN Card yang kita pasang rusak
- [x] Driver LAN Card itu belum tersupport

Jika interfacenya ada tanda X (disabled) setelah nomor (0,1), maka kita enabled dulu hingga hurufnya jadi R (running)

Command:

```
[admin@bismillah] >interface ethernet enable ether1
```

Via winbox:

	Name	Type	MTU	Tx Rate	Rx Rate	Tx Pac...	Rx Pac...
R	ether1	Ethernet	1500	998 bps	3.1 kbps	2	2
R	ether2	Ethernet	1500	13.2 kbps	8.5 kbps	6	9

Beri Nama Ethernet Itu (untuk mudah menghafal & mendefinisikan)

Via Command:

```
[admin@bismillah] >interface Ethernet set ether1 name=public
```

[x] Misal ini yang akan connect ke internet (nyambung ke ISP kita)

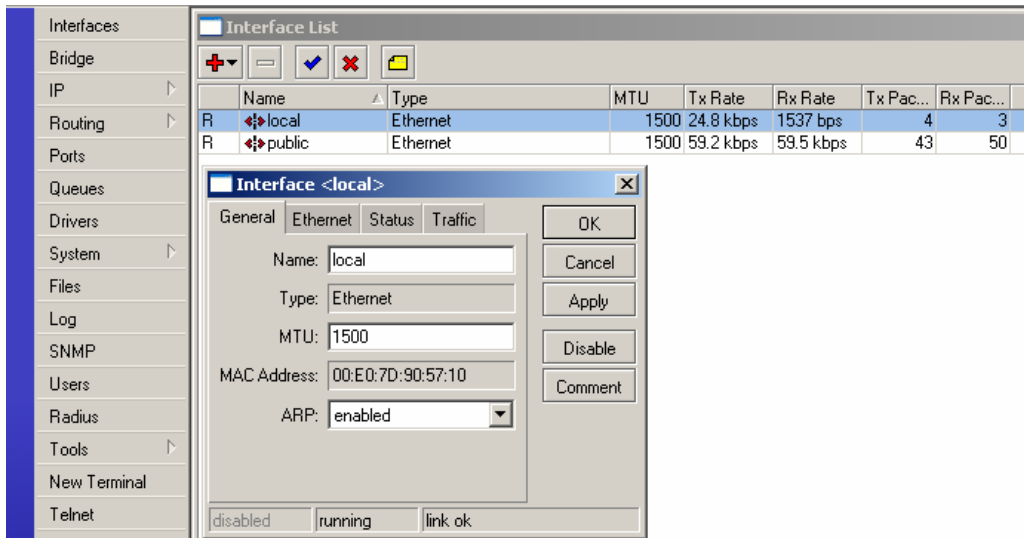
```
[admin@bismillah] >interface ethernet set ether2 name=local
```

[x] Misal ini yang terhubung ke jaringan lokal kita (ke switch/Hub)

[x] Lalu kita lihat lagi:

```
[admin@ bismillah] > /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
```

Via winbox:



Setting IP Address

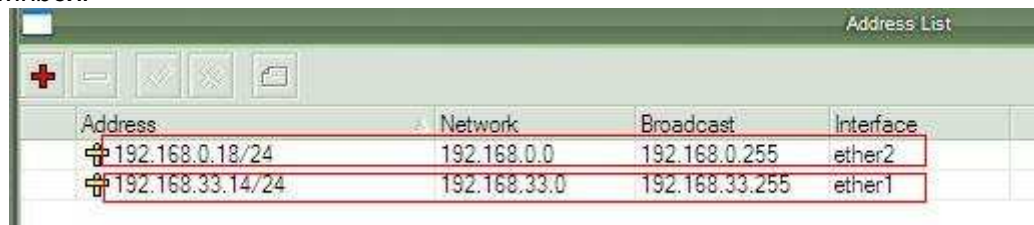
Via Command:

```
[admin@bismillah]>ip address add interface=public
address=192.168.33.14/255.255.255.0 comment=ip-public
[x] 192.168.33.212/255.255.255.0 = ini hanya contoh, ganti dengan IP
address yang diberi ISP kita)
[admin@bismillah] >ip address add interface=local address=
192.168.0.18/255.255.255.0 comment=gateway-lokal
[x] 192.168.0.18/255.255.255.0 = IP address jaringan lokal (LAN) kita
```

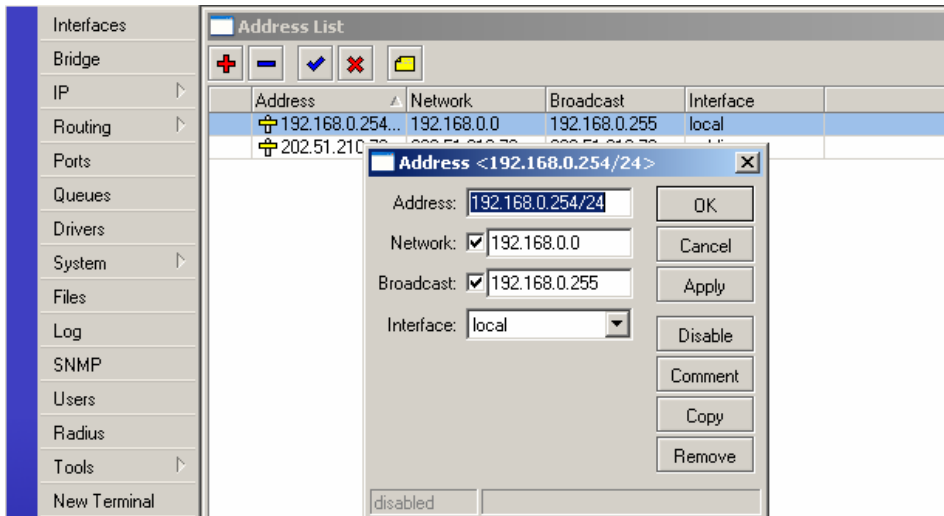
>>> **Lalu kita lihat konfigurasi IP address yang sudah kita berikan**

```
[admin@bismillah] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK BROADCAST INTERFACE
0 192.168.0.18/24 192.168.0.0 192.168.0.255 local
1 192.168.0.254/24 192.168.33.0 192.168.33.255 public
```

Via winbox:



Klik tanda +



Memasukkan IP Gateway

(Fungsi Router: Agar bisa connect ke internet lewat pintu gerbang IP Gateway yg diberi ISP kita)

Via Command:

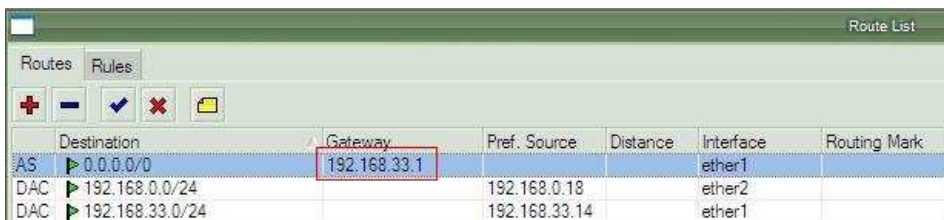
```
[admin@bismillah] > ip route add gateway=192.168.33.1
[x] 192.168.33.1 = Ganti dengan IP Gateway yang diberikan ISP kita
```

[x] **Lalu lihat Tabel routing kita:**

```
[admin@bismillah] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf
# DST-ADDRESS PREFSRC G GATEWAY DISTANCE INTERFACE
0 ADC 192.168.33.0/24 192.168.33.14 public
1 ADC 192.168.0.0/24 192.168.0.18 local
2 A S 0.0.0.0/0 r 192.168.33.1 public
```

Via winbox:

Klik tanda +



Ket:

[x] Bagian Destination diisi 0.0.0.0/0 artinya adalah;

"Semua routing kemanapun tujuannya diarahkan menuju Ip gatewaynya"

[x] Router adalah sebuah device yang fungsinya untuk:

"Meneruskan paket-paket dari sebuah network ke network yang lain (baik LAN ke LAN atau ke WAN atau internet) sehingga host-host yang ada pada sebuah network bisa berkomunikasi dengan host-host yang ada di network yang lain"

[x] Tujuan routing adalah:

"Agar paket IP yang dikirim sampai pada target, begitu juga paket IP"

yang ditujukan untuk kita sampai pada kita dengan baik"

Target atau destination ini bisa berada dalam 1 jaringan ataupun berbeda jaringan (baik secara topologis maupun geografis)

[x] Contoh Penerapan di Mikrotik:

a. Routing Static

Contoh:

```
ip route add dst-address=192.168.77.0/24 gateway=192.168.33.1
```

>>> Artinya tujuan network 192.168.0.0/24 lewat gateway 172.99.77.2

```
ip route add dst-address=212.165.1.2 gateway=203.77.33.7
```

>>> Artinya tujuan host 212.165.1.2 lewat gateway 203.33.45.6

b. Routing untuk 2 ISP atau lebih (misalnya menggunakan 2 atau lebih koneksi)

2 Metode jika ISP pertama dan kedua memberi jatah bandwidth yang berbeda

[x] Menggunakan semua jalur gateway yang tersedia (teknik load-balancing)

```
ip route add gateway=203.77.33.7,192.168.33.1,192.168.33.1
```

>>> "Besarnya pemakaian bandwidth dari gateway 192.168.33.1 lebih besar 2 kali lipat dari bandwidth yang digunakan dari gateway 203.77.33.7"

[x] Menjadikan salah satunya sebagai back-up (teknik fail-over)

Contoh asumsi jalur utama melalui 192.168.33.1 dan jalur 203.77.33.7 sebagai back-up bila jalur utama tidak bisa dilalui:

```
> /ip firewall mangle add chain=prerouting src-address=192.168.0.0/24 action=mark-routing new-routing-mark=jalur1
```

```
> /ip route add gateway=192.168.33.1 routing-mark=jalur1 check-gateway=ping
```

```
> /ip route add gateway=203.77.33.7
```

[x] Kemudian **Test Ping ke Gateway** untuk memastikan konfigurasi benar

```
[admin@bismillah] > ping 192.168.33.1
```

```
192.168.0.254 64 byte ping: ttl=64 time<1 ms
```

```
192.168.0.254 64 byte ping: ttl=64 time<1 ms
```

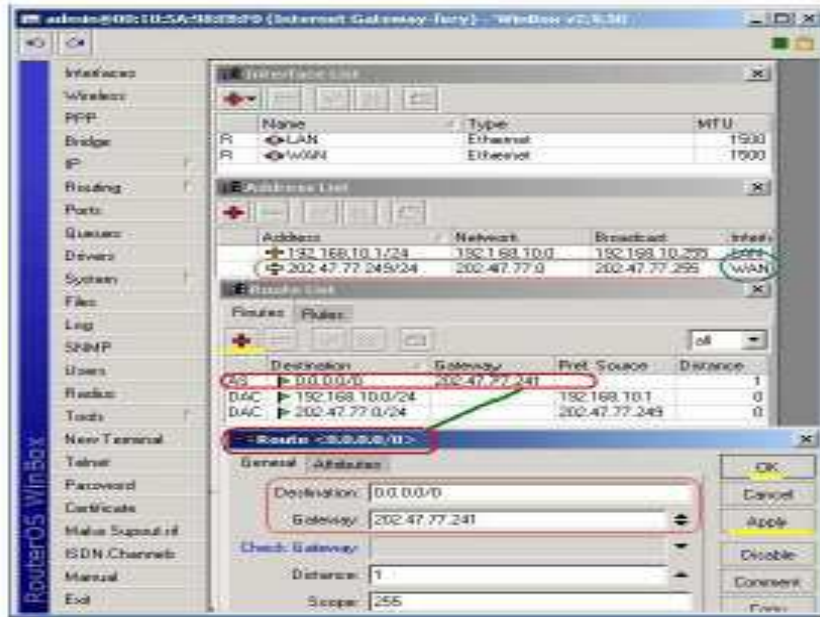
```
2 packets transmitted, 2 packets received, 0% packet loss
```

```
round-trip min/avg/max = 0/0.0/0 ms
```

[x] Test Tracing; Untuk melihat jalur Gateway mana yang digunakan, kemana saja jalur yang dilewati dan seberapa jauh (hop) menuju situs tujuan

```
[admin@bismillah] >
```

Maka sampai disini kita telah melakukan ini:



SETTING DNS

Isi DNS sesuai rekomendasi yang diberi ISP kita

Via Command:

```
[admin@bismillah] > ip dns set primary-dns=192.168.33.1 allow-remoterequests=yes
```

```
[admin@bismillah] > ip dns set secondary-dns=192.168.33.77 allow-remoterequests=yes
```

Maksud allow-remote-requests = yes

Adalah membuat **"router kita juga menjadi DNS forwarder"**

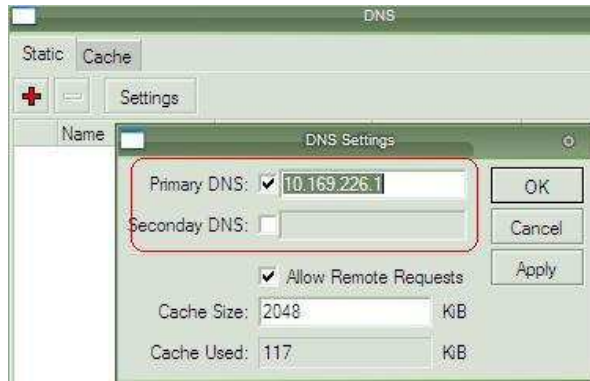
Yaitu fungsi melakukan penyimpanan cache DNS juga (menjadi server DNS);

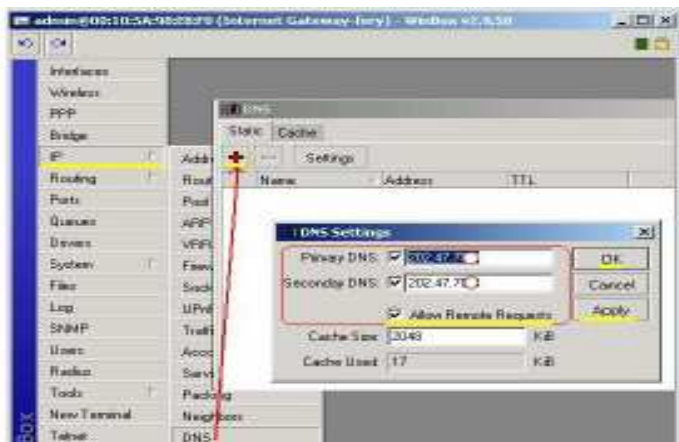
Sehingga client dalam LAN akan terasa lebih cepat browsing sebab cukup mengambil cache DNS di router Mikrotik (jadi cuma local; client tak perlu jauh-jauh meresolve DNS pada Server DNS ISP)

Cara menyetting di client:

Setting DNS primary cukup diisi IP Address Mikrotik kita dan secondary DNS biarkan kosong saja

Via winbox:





[x] **Melihat konfigurasi DNS**

```
[admin@bismillah] > ip dns print
primary-dns: 192.168.33.1
secondary-dns: 192.168.33.77
allow-remote-requests: yes
cache-size: 2048KiB
cache-max-ttl: 1w
cache-used: 16KiB
```

[x] **Tes akses domain; "ping nama domain"...**

```
[admin@bismillah] > ping yahoo.com
216.109.112.135 64 byte ping: ttl=48 time=250 ms
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 571/571.0/571 ms
```

>>> Jika **sudah berhasil reply berarti seting DNS sudah benar**

Source NAT (Network Address Translation) / Masquerading

Agar client computer di lokal network bisa terkoneksi ke internet

Dengan NAT ini maka kita bisa meng-*share* suatu nomor IP address public ke komputer client (IP lokal)

Keuntungan:

[x] *Menghemat IP public kita (cukup satu sebagai gateway lokal)*

[x] *Jaringan local (LAN) kita akan tersembunyi dibelakang IP publik yang diberikan ISP sehingga relatif lebih aman*

*Sebab dengan Masquerading maka akan **merubah paket-paket data IP address asal dan port dari network lokal ke publik (gateway) yang selanjutnya baru diteruskan ke jaringan internet***

Via Command:

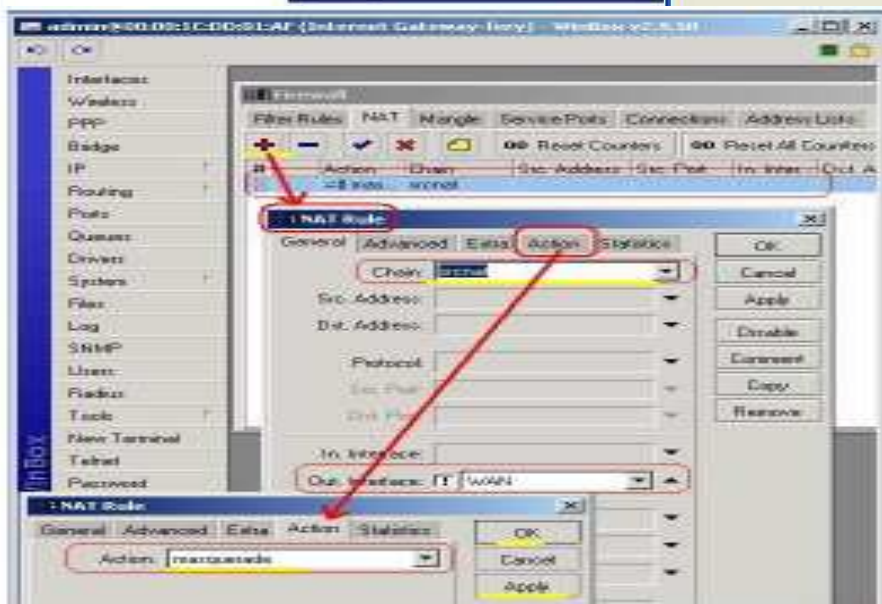
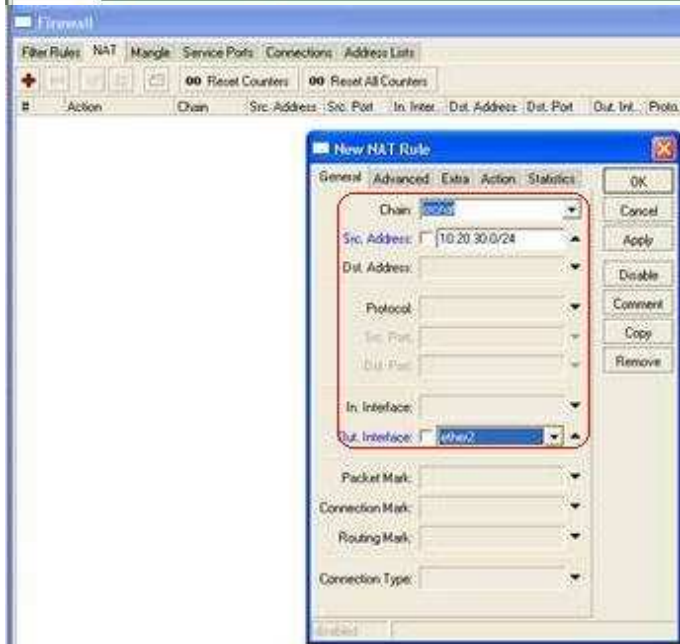
```
[admin@bismillah]> ip firewall nat add chain=srcnat  
action=masquerade out-interface=public
```

Ket:

*out-interface= **interface yang keluar** (ip publik dari isp - yang terhubung ke internet)*

Via winbox:

#	Action	Chain	Src. Address	Src. Port	In. Inter...	Dst. Address	Dst. Port	Out. Interface	Proto...	Bytes	Packets
1	masquerade	srcnat						ether1		35.6 KiB	380
2	redirect	dstnat					80		6 (tcp)	7.2 KiB	155
3	redirect	dstnat					3128		6 (tcp)	0 B	0
4	redirect	dstnat					8000		6 (tcp)	0 B	0



[x] Melihat konfigurasi Masquerading (NAT) kita
 [admin@bismillah]> ip firewall nat print
 Flags: X - disabled, I - invalid, D - dynamic
 0 chain=srcnat out-interface=public action=masquerade

[x] Tes akses domain dari kompi client; jika ada reply berarti setting masquerade kita sudah benar

c:\>ping yahoo.com

```
216.109.112.135 64 byte ping: ttl=48 time=250 ms
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 571/571.0/571 ms
```

>>> Dan berarti sampai tahap ini kita telah berhasil menginstal Mikrotik sebagai Gateway server (fungsi sebagai Router)

[x] Beberapa Contoh Penerapan NAT Lainnya:

[x] Me-redirect port web menjadi transparent proxy

Mengarahkan semua trafik yang menuju Port 80,3128,8000 dibelokkan menuju port 8080 yaitu portnya Web-Proxy

```
/ip firewall nat add chain=dstnat protocol=tcp dst-port=80
action=redirect to-ports=8080
```

>>> Redirect port 80 to 8080 for proxy server

```
/ip firewall nat add chain=dstnat protocol=tcp dst-port=3128
action=redirect to-ports=8080
```

>>> Redirect port 3128 to 8080 for proxy server

```
/ip firewall nat add chain=dstnat protocol=tcp dst-port=8080
action=redirect to-ports=8080
```

>>> Redirect port 8080 to 8080 for proxy server

[x] Membuat traffic harus melewati proxy server

Maksudnya menuju server proxy lain yang dedicated terinstall squid

Firewall di linux misalnya:

```
iptables -A PREROUTING -t nat -p tcp -s 192.168.77.0/24 -i eth2
-d \! 192.168.77.0/24 --dport 80 -j REDIRECT --to 8080
```

>>> Mikrotik punya Ip ini (192.168.77.0/24 = contoh)

>>> Mikrotik membuang semua service web menuju port 80 ke linux

>>> Squid di linux open (menerima) service port 8080

[x] KONFIGURASI FIREWALL LAINYA

```
ip firewall nat add action=masquerade chain=srcnat
ip firewall filter add chain=input connection-state=invalid
action=drop
ip firewall filter add chain=input protocol=udp action=accept
ip firewall filter add chain=input protocol=icmp action=accept
Ip firewall filter add chain=input in-interface=local
action=accept
```

>>> bagian yang ke jaringan lokal

```
ip firewall filter add chain=input in-interface=public
action=accept
```

>>> bagian yang nyabung langsung ke internet

```
ip firewall filter add chain=input action=drop
```

[x] FILTERING :

Sumber: <http://www.mikrotik.com/testdocs/ros/2.9/ip/filter.php>

```
ip firewall filter
add chain=input connection-state=invalid action=drop
\comment="Drop Invalid connections"
add chain=input connection-state=established action=accept
\comment="Allow Established connections"
add chain=input protocol=udp action=accept \
```

```

comment="Membolehkan paket UDP"
add chain=input protocol=icmp action=accept \
comment="Membolehkan paket ICMP (Ping)"
add chain=input src-address=192.168.0.0/24 action=accept \
comment="Allow access to router from known network"
add chain=input action=drop comment="Drop anything else"

```

[x] ANTI VIRUS UNTUK MICROTIK

```

add chain=forward action=jump jump-target=virus comment="jump
to the virus chain"
+++++
add chain=forward protocol=icmp comment="allow ping"
add chain=forward protocol=udp comment="allow udp"
add chain=forward action=drop comment="drop everything else"

```

[x] SECURITY ROUTER MICROTIK KITA

```

/ ip firewall filteradd chain=input connection-
state=established comment="Accept established connections" add
chain=input connection-state=related comment="Accept related
connections" add chain=input connection-state=invalid
action=drop comment="Drop invalid connections" add chain=input
protocol=udp action=accept comment="UDP" disabled=no add
chain=input protocol=icmp limit=50/5s,2 comment="Allow limited
pings" add chain=input protocol=icmp action=drop
comment="Drop excess pings" add chain=input protocol=tcp dst-
port=22 comment="SSH for secure shell" add chain=input
protocol=tcp dst-port=8291 comment="winbox" # Edit rules ini
berdasar IP yang ada di network kita! # add chain=input src-
address=192.168.33.14/24 comment="From Mikrotiks network"
add chain=input src-address=192.168..0.0/24 comment="From our
private LAN"# End of Edit #add chain=input action=log log-
prefix="DROP INPUT" comment="Log everything else" add
chain=input action=drop comment="Drop everything else"
"http://wiki.mikrotik.com/wiki/Securing\_your\_router"

```

[x] SETTING KEAMANAN JARINGAN HANYA UNTUK LOKAL AREA KITA

```

/ip firewall filteradd chain=forward connection-
state=established comment="allow established connections" add
chain=forward connection-state=related comment="allow related
connections" add chain=forward connection-state=invalid
action=drop comment="drop invalid connections"
add chain=virus protocol=tcp dst-port=135-139 action=drop
comment="Drop Blaster Worm" add chain=virus protocol=udp dst-
port=135-139 action=drop comment="Drop Messenger Worm" add
chain=virus protocol=tcp dst-port=445 action=drop
comment="Drop Blaster Worm" add chain=virus protocol=udp
dst-port=445 action=drop comment="Drop 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=1433-1434 action=drop
comment="Worm" add chain=virus protocol=tcp dst-port=2745
action=drop comment="Bagle Virus" add chain=virus protocol=tcp
dst-port=2283 action=drop comment="Drop Dumaru.Y" add
chain=virus protocol=tcp dst-port=2535 action=drop
comment="Drop Beagle" add chain=virus protocol=tcp dst-
port=2745 action=drop comment="Drop Beagle.C-K" add chain=virus
protocol=tcp dst-port=3127-3128 action=drop comment="Drop
MyDoom" add chain=virus protocol=tcp dst-port=3410 action=drop
comment="Drop 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"
+++++

```

[x] Matikan Port yang Biasa Dipakai Spam

```

/ip firewall filter add chain=forward dst-port=135-139
protocol=tcp action=drop
/ip firewall filter add chain=forward dst-port=135-139
protocol=udp action=drop
/ip firewall filter add chain=forward dst-port=445 protocol=tcp
action=drop
/ip firewall filter add chain=forward dst-port=445 protocol=udp
action=drop
/ip firewall filter add chain=forward dst-port=593 protocol=tcp
action=drop
/ip firewall filter add chain=forward dst-port=4444
protocol=tcp action=drop
/ip firewall filter add chain=forward dst-port=5554
protocol=tcp action=drop
/ip firewall filter add chain=forward dst-port=9996
protocol=tcp action=drop
/ip firewall filter add chain=forward dst-port=995-999
protocol=udp action=drop
/ip firewall filter add chain=forward dst-port=53 protocol=tcp
action=drop
/ip firewall filter add chain=forward dst-port=55 protocol=tcp

```

```
action=drop
/ip firewall filter add chain=forward dst-p
```

Silahkan cek referensi seperti di:

http://www.mikrotik.com/documentation/manual_2.7

<http://www.mikrotik.com/docs/ros/2.9/ip/webproxy>

DHCP Server (Dynamic Host Configuration Protocol) Server

Jika kita ingin client mendapat IP address secara otomatis (pengaturan IP Address dilakukan terpusat di server)

Sehingga juga akan mempermudah administrator memberi pengalamatan ip untuk client (nggak perlu menyetting IP secara manual)

Step by step Via Command:

1. Buat IP address pool (rentang jatah pengalamatan IP)

```
/ip pool add name=dhcp-pool ranges=192.168.3.33-192.168.33.212
```

2. Menambahkan DHCP Network dan gatewaynya yang akan kita distribusikan ke client (Pada contoh ini networknya adalah 192.168.33.0/24 dan gatewaynya 192.168.33.1)

```
/ip dhcp-server network add address=192.168.33.0/24 gateway=192.168.33.1
```

3. Tambahkan DHCP Server (pada contoh ini dhcp diterapkan pada interface local)

```
/ip dhcp-server add interface=local address-pool=dhcp-pool
```

4. Check status DHCP server

```
[admin@bismillah]> ip dhcp-server print
```

```
Flags: X - disabled, I - invalid
```

```
# NAME INTERFACE RELAY ADDRESS-POOL LEASE-TIME ADD-ARP
```

```
0 X dhcp1 ether2
```

Tanda X menyatakan bahwa DHCP server belum enable maka kita **enablekan dulu:**

```
/ip dhcp-server enable 0
```

Lalu cek lagi >>> sudah aktif belum (R=Running)

6. Tes Ping Dari Client

```
c:\>ping www.yahoo.com
```

Membuat Transparent web proxy

Fungsi utama proxy adalah untuk menyimpan cache

Apabila sebuah LAN menggunakan proxy untuk berhubungan dengan Internet, maka ketika browser di client (port web) mengakses sebuah url sebuah web maka mengambil request tersebut di proxy server

Dan jika data itu belum ada di proxy server maka proxy mengambil langsung dari web bersangkutan

Lalu request tersebut juga disimpan di cache proxy

*Maka **jika ada lagi client yang melakukan request ke url yang sama, maka akan diambilkan dari cache itu** (dalam jaringan lokal berarti)*

Sehingga ini akan membuat akses ke Internet terasa lebih cepat

Dan Transparent proxy kita buat untuk memastikan setiap pengguna mengakses Internet melalui web proxy yang telah kita aktifkan (diatas)

Sebab setiap request dari Browser client yang menggunakan gateway kita secara otomatis akan dilewatkan ke proxy

Jadi dengan hal ini juga akan mempermudah administrasi client:

Tidak perlu lagi melakukan setup proxy ditiap browser client

(karena dilakukan redirection otomatis disisi server)

[x] Set Proxy

Via Command:

IP Proxy

/ip proxy set enabled=yes

>>> Mengaktifkan fitur web proxy

maximal-client-connections=1000

maximal-server-connections=1000

IP Web-Proxy

/ ip web-proxy set enabled=yes

>>> Mengaktifkan web proxy (adanya IP Proxy dan IP Web-Proxy tergantung versi mikrotik kita)

set src-address=0.0.0.0

>>> address yang akan kita gunakan untuk koneksi ke parent proxy (defaultnya 0.0.0.0)

set port=8080

>>> Port yang mau digunakan untuk web proxy

set hostname="proxy.bismillah.com"

>>> Nama Hostname untuk Web Proxy (optional)

set transparent-proxy=yes

>>> Mengaktifkan transparant proxy

set parent-proxy=0.0.0.0:0

>>> Diisi jika kita ingin menggunakan parent proxy (optional)

set cache-administrator="arohwany@bismillah.com"

>>> email administrator support yang akan dikirim status, seperti jika proxy error

set max-object-size=8192KiB

>>> ukuran maximal file yang akan disimpan sebagai cache (default 4096Kilobytes)

set cache-drive=system

>>> drive tempat penyimpanan cache

set max-cache-size=unlimited

>>> ukuran maximal hardisk yang akan dipakai sebagai penyimpan file cache (misalnya 3 kali total RAM atau unlimited)

set max-ram-cache-size=unlimited

>>> maximal ram yang akan digunakan untuk cache

[x] Membuat Rule NAT untuk transparent proxy

Me-redirect port web ke transparent proxy:

"Mengarahkan semua trafik yang menuju Port 80,3128,8000 kita belokkan menuju port 8080, yaitu portnya Web-Proxy"

```
/ip firewall nat add chain=dstnat protocol=tcp dst-port=80  
action=redirect to-ports=8080  
>>> Redirect port 80 to 8080 for proxy server
```

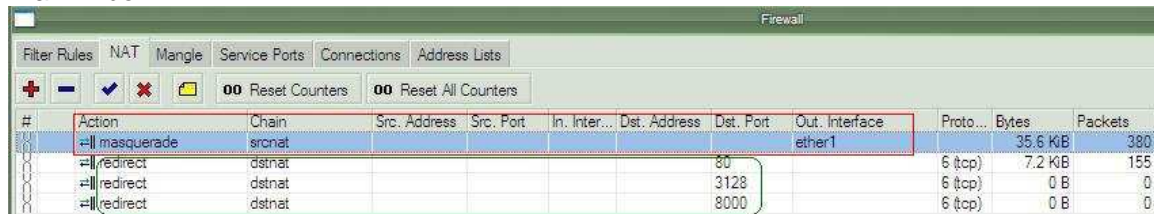
```
/ip firewall nat add chain=dstnat protocol=tcp dst-port=3128  
action=redirect to-ports=8080  
>>> Redirect port 3128 to 8080 for proxy server
```

```
/ip firewall nat add chain=dstnat protocol=tcp dst-port=8080  
action=redirect to-ports=8080  
>>> Redirect port 8080 to 8080 for proxy server
```

[x] Coba kita lihat Tabel NAT

```
[admin@bismillah] > /ip firewall nat print  
Flags: X - disabled, I - invalid, D - dynamic  
0 chain=srcnat out-interface=public action=masquerade  
1 chain=dstnat in-interface=local src-address=192.168.0.0/24  
protocol=tcp dst-port=80 action=redirect to-ports=3128
```

Via Winbox:



#	Action	Chain	Src. Address	Src. Port	In. Inter...	Dst. Address	Dst. Port	Out. Interface	Proto...	Bytes	Packets
0	masquerade	srcnat						ether1		35.6 KiB	380
1	redirect	dstnat					80		6 (tcp)	7.2 KiB	155
2	redirect	dstnat					3128		6 (tcp)	0 B	0
3	redirect	dstnat					8080		6 (tcp)	0 B	0

[x] Check Web Proxy:

```
[admin@bismillah] > /ip web-proxy print  
enabled: yes  
src-address: 0.0.0.0  
port: 8080  
hostname: "proxy.bismillah.com"  
transparent-proxy: yes  
parent-proxy: 0.0.0.0:0  
cache-administrator: "arohwany@bismillah.com"  
max-object-size: 8192KiB  
cache-drive: system  
max-cache-size: unlimited  
max-ram-cache-size: unlimited  
status: running  
reserved-for-cache: 4733952KiB  
reserved-for-ram-cache: 2048KiB
```

[x] Melihat hasil konfigurasi web-proxy

```
/ip web-proxy print
```

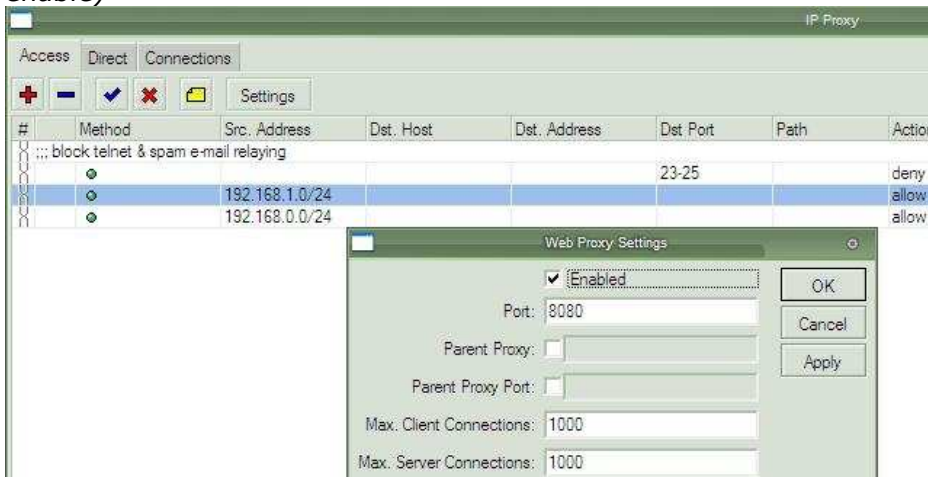
[x] Memonitoring kerja web-proxy

```
/ip web-proxy monitor
```

Via Winbox:

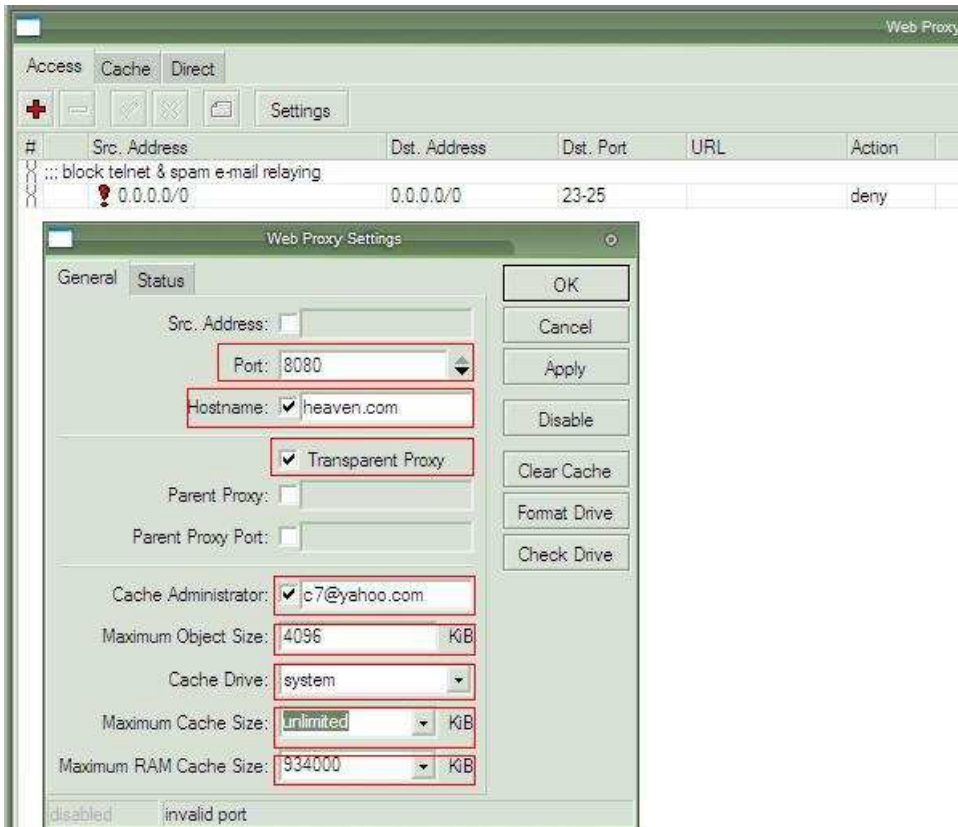


[x] mengaktifkan web proxy pada menu IP>Proxy>Access>**Setting** (check box enable)

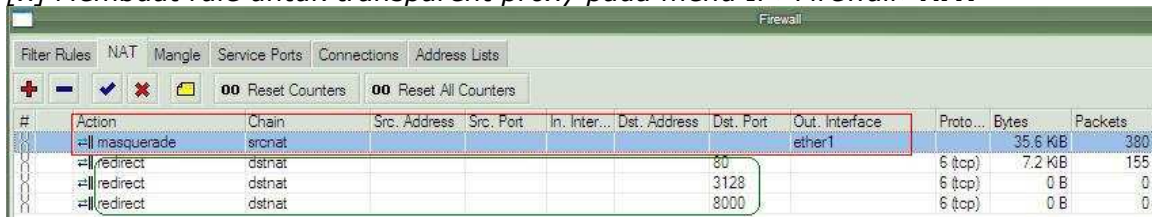


[x] Setting parameter pada menu IP>Web Proxy>Access >**Setting**>General





[x] Membuat rule untuk transparent proxy pada menu IP>Firewall>**NAT**



Silahkan baca referensi utama disini juga:

<http://harrychanputra.wordpress.com/2007/04/15/setting-mikrotik>

<http://www.forummikrotik.com>

<http://forum.mikrotik.com>

<http://mikrotik.co.id/artikel.php>

<http://www.mikrotik.com/testdocs/ros/2.9>

http://wiki.mikrotik.com/wiki/Main_Page

<http://www.tiktube.com>

http://www.youtube.com/results?search_query=mikrotik&search=Search

Dan juga artikel,penyerta yang ana sertakan dalam attachment dibawah ini (silahkan download):

Rabu, 11 Juni 2008

Muhammad Ulinnuha

(To Connect our live)

(Project pribadi, siap di convert dalam bentuk web. PR:"sebelum belakangan nanti terlalu sibuk dan nggak jadi-jadi juga")

Project Buku Selanjutnya yang insya Allah akan menyusul:

[1] "*[Step by Step] FreeBSD to Easy*"

[2] "*[Step by Step] Menjadi Blogger Hebat!*"

[3] "*[Step by Step] Blog Business*"