

## DAFTAR ISI

1. How to limit traffic download RapidShare .....	2
2. Implementasi Penggunaan PCQ Bagi ISP Untuk Mendapatkan Hasil Yang Maksimal .....	7
3. Detect dan shapping download dengan connetion byte .....	9
4. Memisahkan Gateway Internasional dan IIX dengan 3 NIC (Bagian 2) .....	11
5. Bandwidth management di Hotspot Area .....	12
6. Memisahkan IIX ke ISP wireless dan Internasional ke speedy .....	14
7. How To Block Traceroute .....	15
8. HOWTO: Menghindari Port Scanner dari Hacker .....	16
9. HOW TO : Melindungi Pelanggan/User Anda .....	17
10. Load-balancing & Fail-over di MikroTik .....	19
11. Redirect Mikrotik ke Komputer Proxy Squid (tanpa parent proxy MT) .....	21
12. Delaypool rasa Mikrotik .....	23
13. 2 Isp In 1 Router With Loadbalancing .....	26
14. Tutz Load Balancing Plus plus [Chaozz version] (Route Rule) .....	28
15. SETUP MIKROTIK (base 1) .....	30
16. TUTORIAL SETUP HOTSPOT + USERMANAGER .....	31
17. TUTORIAL 2 ISP IN 1 ROUTER WITH LOADBALANCING .....	32
18. SETUP QUEUE .....	34
19. TUTORIAL MISAHIN BW LOKAL DAN INTERNATIONAL .....	35
20. TUTORIAL SETING IP-PROXY & CONTOH PENGGUNANNYA (BASIC) .....	36
21. SETING PPTP SERVER & CLIENT .....	37
22. HOWTO: Menghindari Port Scanner dari Hacker .....	38
23. Wireless Bridge (client) dengan AP tanpa WDS .....	39
24. Setting Point To Multi Point .....	39
25. Pengamanan Mikrotik dari Scan Winbox dan Neighbour .....	40
26. Transparent Traffic Shaper .....	41
27. Pengamanan Mikrotik dari Scan Winbox dan Neighbour .....	43
28. Script Bikin Queues Tree B/W Limiter .....	44
29. Update Otomatis nice.rsc .....	46
30. [Share] Script u/ membatasi BW jika suatu traffic client melewati batas tertentu .....	51
31. Hotspot Mikrotik .....	53
32. [tutorial] Mikrotik Load Balancing - Winbox version .....	56
33. Konfigurasi SMS saat Internet down .....	62
34. Mikrotik dengan SquidBox .....	63
35. <ask> bagaimana cara install mikrotik di Router Board .....	65
36. Load Balance + Fail Over dengan script .....	66
37. Load Balancing nth buat Mikrotik Ver 3.xx dan 2.9xx .....	69
38. MikroTik Password Recovery .....	71
39. Howto : Bypass traceroute traffic.....	76
40. Cara copy torch atau LOG ke file ---caranya? .....	77
41. MikroTik Password Recovery .....	78
42. [Script] HTML Project for HotSpot Voucher.....	79
43. Ringtone Mikrotik .....	83
44. Editing Hotspot login Page .....	90
45. Memisahkan antara download dan browsing dengan mikrotik .....	93
46. backup database radius server hotspot .....	94
47. CATATAN LAIN-LAIN.....	95

---

## How To : Limit Traffic Download Rapidshare

Artikel singkat berikut akan menerangkan cara untuk membatasi traffic download dari rapidshare.

Hal yang harus diperhatikan adalah, how to ini meutilisasi penggunaan script untuk mendeteksi DNS Cache...Jadi penggunaan DNS Mikrotik untuk How To ini merupakan kewajiban...

### 1. Script

Pada dasarnya script dibawah saat dijalankan akan memeriksa DNS Cache, dan mencari entry yang terdapat kata 'rapidshare'...kemudian membuat log entry...lalu menempatkan IP yang didapat ke Address List di list 'rapidshare'

Code:

```
:foreach i in=[/ip dns cache find] do={
:if ([[:find [/ip dns cache get $i name] "rapidshare"] > 0) do={
:log info ("rapidshare: " . [/ip dns cache get $i name] . " (ip address " . [/ip dns
cache get $i address] . ")")
/ip firewall address-list add address=[/ip dns cache get $i address] list=rapidshare
disabled=no
}
}
```

### 2. Jalankan Script

Script diatas harus dijalankan secara periodik dengan **scheduler** untuk mendapatkan hasil yang terbaik...bisa diset untuk jalan 1 menit sekali atau 5 menit sekali atau 1 jam sekali...semua terserah anda dan kondisi yang ada...

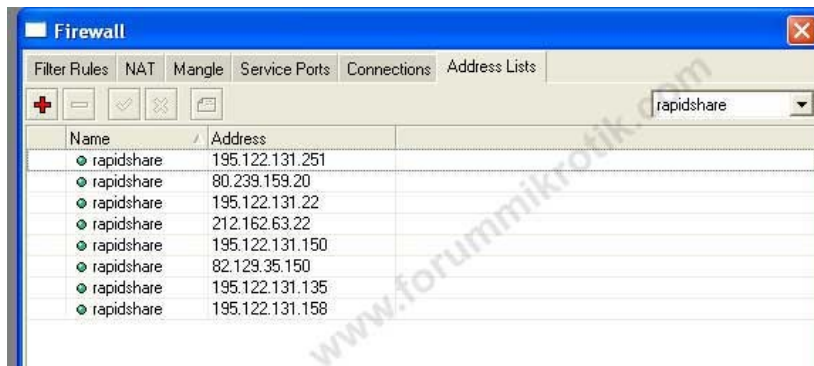
buat entry baru pada scheduler :



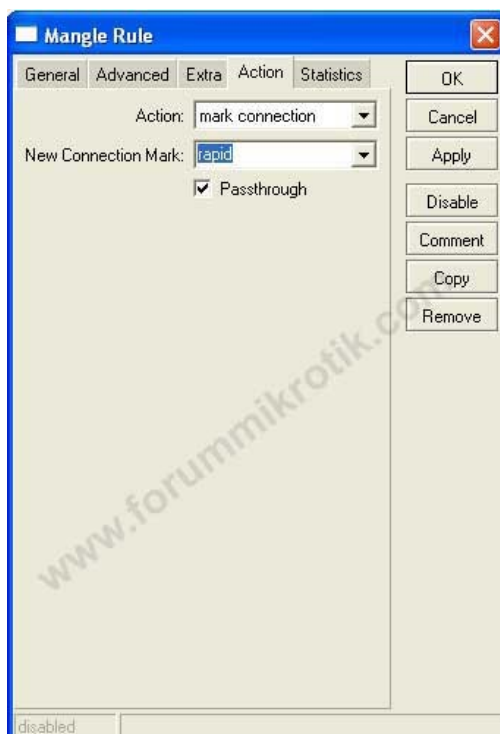
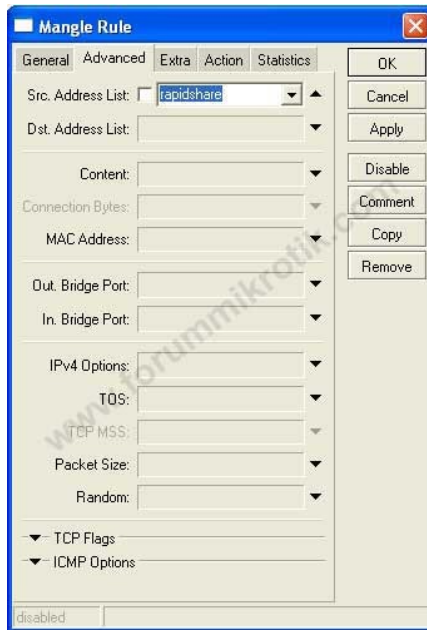
Start Date dan Time di set sesuai dengan waktu yang anda inginkan

### 3. Mangle

Pada saat ini seharusnya telah terdapat address list baru



Lalu buat rule mangle baru untuk mark-conn



kemudian, buat rule mangle baru untuk mark-packet

**Mangle Rule**

General | Advanced | Extra | Action | Statistics

Chain: **prerouting**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark: ☒ **rapid**

Routing Mark:

Connection State:

Connection Type:

disabled

OK | Cancel | Apply | Disable | Comment | Copy | Remove

**Mangle Rule**

General | Advanced | Extra | Action | Statistics

Action: **mark packet**

New Packet Mark: **rapid**

☐ Passthrough

disabled

OK | Cancel | Apply | Disable | Comment | Copy | Remove

#### 4. Queue

Akhirnya, kita dapat melakukan pembatasan traffik...contoh penerapan menggunakan simple queue dapat dilihat dibawah...

**Simple Queue <rapid>**

General | Advanced | Statistics | Traffic | Total | Total Statistics

P2P:

Packet Mark: **rapid**

Dst. Address:

Interface: **all**

Target Upload: Limit At: **10k** bits/s

Target Download: Limit At: **10k** bits/s

Queue Type: **default-small**

Parent: **none**

Priority: **8**

disabled

OK | Cancel | Apply | Enable | Copy | Remove

Untuk percobaan silahkan coba lakukan proses download dari rapidshare, lalu enable dan disable rule queue-nya dan rasakan perbedaannya...



Selamat mencoba....

heh tapi ati2 bro.... soalnya ada kejadian kaya gini (ip dibawah cache DNS yg dobel ga masuk ke address-list), perhatikan en lihat tulisan tebal dan miring, tidak masuk dalam daftar address-list:

Code:

```
[admin@Mikrotik] > ip dns cache print
Flags: S - static
# NAME ADDRESS TTL

.....
55 ns1.rapidshare.com 195.122.131.250 1d19h59m
56 ns2.rapidshare.com 80.237.244.50 1d19h59m
81 rapidshare.com 195.122.131.2 13m10s
82 rapidshare.com 195.122.131.3 13m10s
83 rapidshare.com 195.122.131.4 13m10s
84 rapidshare.com 195.122.131.5 13m10s
85 rapidshare.com 195.122.131.6 13m10s
86 rapidshare.com 195.122.131.7 13m10s
87 rapidshare.com 195.122.131.8 13m10s
88 rapidshare.com 195.122.131.9 13m10s
89 rapidshare.com 195.122.131.10 13m10s
90 rapidshare.com 195.122.131.11 13m10s
91 rapidshare.com 195.122.131.12 13m10s
92 rapidshare.com 195.122.131.13 13m10s
93 rapidshare.com 195.122.131.14 13m10s
94 rapidshare.com 195.122.131.15 13m8s
95 rapidshare.com 195.122.131.250 13m8s :!: 96 rs144cg.rapidshare.com 82.129.39.145
13m8s
97 rs26cg.rapidshare.com 82.129.39.27 13m18s
98 rs91cg.rapidshare.com 82.129.39.92 13m29s
99 rs67cg.rapidshare.com 82.129.39.68 13m50s
100 rs140cg.rapidshare.com 82.129.39.141 13m58s
.....

[admin@Mikrotik] > ip firewall address-list print
Flags: X - disabled, D - dynamic
# LIST ADDRESS

.....
53 rapidshare 195.122.131.250
54 rapidshare 80.237.244.50
55 rapidshare 195.122.131.2
56 rapidshare 195.122.131.3
57 rapidshare 195.122.131.4
58 rapidshare 195.122.131.5
59 rapidshare 195.122.131.6
60 rapidshare 195.122.131.7
61 rapidshare 195.122.131.8
62 rapidshare 195.122.131.9
63 rapidshare 195.122.131.10
64 rapidshare 195.122.131.11
65 rapidshare 195.122.131.12
66 rapidshare 195.122.131.13
67 rapidshare 195.122.131.14
68 rapidshare 195.122.131.15 :!:
```

dengan penyempurnaan script diatas (scheduler), jikalau ada ip yang masuk dobel di dns agar ip berikutnya masuk ke address-list:

Code:

```
:foreach i in[/ip dns cache find] do={
    :local bNew "true";
#   check if dns name contains rapidshare
    :if ([:find [/ip dns cache get $i name] "rapidshare"] != 0) do={
        :local tmpAddress [/ip dns cache get $i address] ;
#---- if address list is empty do not check ( add address directly )
        :if ( [/ip firewall address-list find ] = "") do={
            /ip firewall address-list add address=$tmpAddress list=rapidshare
disabled=no;
        } else={
#----- check every address list entry
            :foreach j in[/ip firewall address-list find ] do={
#----- set bNew variable to false if address exists in address list
                :if ( [/ip firewall address-list get $j address] = $tmpAddress )
do={
                    :set bNew "false";
                }
            }
#----- if address is new then add to address list
            :if ( $bNew = "true" ) do={
                /ip firewall address-list add address=$tmpAddress list=rapidshare
disabled=no
            }
        }
    }
}
```

## Implementasi Penggunaan PCQ Bagi ISP Untuk Mendapatkan Hasil Yang Maksimal

Melihat banyaknya pertanyaan mengenai pembagian sharing bandwidth yang adil dan yang pasti bisa membatasi semua jenis trafik baik IDM maupun P2P sehingga gak perlu takut kecolongan, saya coba untuk mensharing CMIW 🤪

Konfigurasi Jaringan :

Public --- (10.0.0.1/24) MT (192.168.1.1/24)--- Local

Skenarionya kaya gini :

Client 192.168.1.10 --- Bandwidth 512kbps 1:1 (corporate)  
(512k up / 512 down)

Client 192.168.1.20, 21, 22, 23 --- Bandwidth 384kbps 1:4 (personal)  
(64k up / 384 down)

Pertama-tama lakukan mangle :

Untuk trafik upload corporate

```
/ip firewall mangle add chain=prerouting src-address=192.168.1.10 in-interface=Local action=mark-packet new-packet-mark=corporate-up passthrough=no
```

Untuk trafik download corporate

```
/ip firewall mangle add chain=forward src-address=192.168.1.10 action=mark-connection new-connection-mark=corporate-conn passthrough=yes
```

```
/ip firewall mangle add chain=forward connection-mark=corporate-conn in-interface=Public action=mark-packet new-packet-mark=corporate-down passthrough=no
```

Untuk trafik upload personal

```
/ip firewall mangle add chain=prerouting src-address=192.168.1.20 in-interface=Local action=mark-packet new-packet-mark=personal-up passthrough=no
```

```
/ip firewall mangle add chain=prerouting src-address=192.168.1.21 in-interface=Local action=mark-packet new-packet-mark=personal-up passthrough=no
```

```
/ip firewall mangle add chain=prerouting src-address=192.168.1.22 in-interface=Local action=mark-packet new-packet-mark=personal-up passthrough=no
```

```
/ip firewall mangle add chain=prerouting src-address=192.168.1.23 in-interface=Local action=mark-packet new-packet-mark=personal-up passthrough=no
```

Untuk trafik download personal

```
/ip firewall mangle add chain=forward src-address=192.168.1.20 action=mark-connection new-connection-mark=personal-conn passthrough=yes
```

```
/ip firewall mangle add chain=forward src-address=192.168.1.21 action=mark-connection new-connection-mark=personal-conn passthrough=yes
```

```
/ip firewall mangle add chain=forward src-address=192.168.1.22 action=mark-connection new-connection-mark=personal-conn passthrough=yes
```

```
/ip firewall mangle add chain=forward src-address=192.168.1.23 action=mark-connection new-connection-mark=personal-conn passthrough=yes
```

```
/ip firewall mangle add chain=forward connection-mark=personal-conn in-interface=Public action=mark-packet new-packet-mark=personal-down passthrough=no
```

Harpa diperhatikan untuk mark-packet maka passthrough=no sedangkan untuk mark-connection passthrough=yes

Nah setelah beres urusan mangling ini, kita lanjut ke pembuatan queue tree :

```
/queue tree add name=down parent=Local queue=default
```

```
/queue tree add name=up parent=global-in queue=default
```

untuk download kita menggunakan in-interface kita dalam hal ini Local, sedangkan untuk upload kita menggunakan global-in

selanjutnya kita tambahkan type baru di queue kita :

yang harus kita tambahkan melihat skenario diatas adalah PCQ untuk paket corporate 512kbps (1:1) dan paket personal 384kbps (1:4).

Untuk paket corporate kita langsung menetapkan angka 512kbps, sedangkan untuk personal kita tidak dapat menetapkan angka disini karena bandwidth yang akan diterima oleh paket personal tergantung seberapa banyak user yang online, jadi jika hanya 1 orang online akan mendapatkan bw penuh 384kbps, kalau 2 orang online maka masing-masing akan mendapatkan 192kbps dan seterusnya.

```
/queue type add name=512-down kind=pcq pcq-rate=512k pcq-classifier=dst-address pcq-total-limit=2000
```

```
/queue type add name=512-up kind=pcq rate=512k pcq-classifier=src-address pcq-total-limit=2000
```

```
/queue type add name=auto-down kind=pcq pcq-rate=0 pcq-classifier=dst-address pcq-total-limit=2000
```

```
/queue type add name=auto-up kind=pcq rate=0 pcq-classifier=src-address pcq-total-limit=2000
```

kita menggunakan 0 pada paket personal karena MT akan menghitung berapa besar bw yang tersedia pada saat client melakukan koneksi.

Nah setelah itu kita kembali ke queue tree dan menambahkan :

Paket corporate

```
/queue tree add name=corp-down packet-mark=corporate-down parent=down queue=512-down
```

```
/queue tree add name=corp-up parent=up packet-mark=corporate-up queue=512-up
```

Paket personal

```
/queue tree add name=per-down packet-mark=personal-down parent=down queue=auto-down max-limit=384k
```

```
/queue tree add name=per-up parent=up packet-mark=personal-up queue=auto-up max-limit=64k
```

Done.

Setelah melakukan semua hal ini silahkan dicoba gunakan aplikasi P2P ataupun downloader, seharusnya semuanya sudah dapat ter-shaping dengan baik 😁

Settingan diatas cocok diterapkan buat konfigurasi seperti diterangkan diatas, tanpa menggunakan proxy internal MT dan hanya 2 interface, untuk menggunakan proxy internal dan lebih banyak interface diperlukan sedikit perubahan dan penambahan pada script diatas 😁



## Detect dan shapping download dengan connetion byte

Sehubungan dengan banyaknya pertanyaan mengenai cara membatasi download aktifitas, berikut ada trik lain selain "delaypool rasa mikrotik".

Adapun trik ini adalah dengan memanfaatkan fasilitas "connection bytes" pada mangle.

Mengenai fungsi connection bytes kalo tidak salah adalah : mendeteksi jumlah bytes yang telah tertransfer dalam satu koneksi antar dua pihak.

Sebagai contoh :

ip 192.168.10.12 melakukan koneksi ke 202.1.2.xx. Nah selama koneksi ini terjadi, connection bytes akan mencatat traffic bandwidth yang terjadi dalam koneksi ini. dari 0 byte sampai tak terhingga. dan penghitungan akan dihentikan setelah koneksi terputus.

Dan untuk connection bytes ini akan mumpuni jika dilakukan pada queue tree. untuk queue simple saya belum pernah mencoba.

Baik sekarang dimulai:

Sebagai ilustrasi, saya akan membatasi client dengan ip 192.168.10.12.

Jika melakukan koneksi pada satu web dengan jumlah bytes masih antara 0-128 KB, maka koneksi ini diberi prioritas 1, dan diberi jatah bandwidth 128kbps. namun setelah bytes lebih dari 128KB pada koneksi itu, maka priority akan diturunkan menjadi prio 8 dan bandwidth akan dicekek ke 32kbps.

Mangle :

Pertama lakukan mark connection pada setiap aktifitas LAN ke luar

Quote:

```
chain=postrouting out-interface=ether1 dst-address=192.168.10.0/24 protocol=tcp src-port=80 action=mark-connection new-connection-mark=http_conn passthrough=yes
```

Selanjutnya menangkap bytes yang tertransfer dari suatu web ke ip 192.168.10.12. dimana pada mangle pertama mendeteksi hanya pada transfer antara 0-128KB. jika lebih dari itu maka akan ditangani oleh mangle kedua.

Quote:

```
chain=postrouting out-interface=ether1 dst-address=192.168.10.12 connection-mark=http_conn connection-bytes=0-131072 action=mark-packet new-packet-mark=client12_browsing passthrough=no
chain=postrouting out-interface=ether1 dst-address=192.168.10.12 connection-mark=http_conn connection-bytes=131073-4294967295 action=mark-packet new-packet-mark=client12_download passthrough=no
```

Selesai dimangle sekarang kita lakukan shaping pada kedua mangle tersebut dengan queue tree. Pada queue tree ini kita memanfaatkan queue type pcq, dan untuk byte antara 0-128KB kita beri rate 128kbps, sementara jika lebih dari 128KB maka akan diberi rate 32kbps.

queue type :

Quote:

```
name="browsing" kind=pcq pcq-rate=128000 pcq-limit=50 pcq-classifier=dst-address pcq-total-limit=2000
name="download" kind=pcq pcq-rate=32000 pcq-limit=50 pcq-classifier=dst-address pcq-total-limit=2000
```

Selanjutnya masuk ke queue tree:

queue tree :

Pertama bikin parent queue

Quote:

```
name="choi" parent=ether1 packet-mark="" limit-at=1024000 queue=default priority=3 max-limit=1024000 burst-limit=0 burst-threshold=0 burst-time=0s
```

Selanjutnya bikin child queue khusus untuk ip 192.168.10.12 tersebut dimangle diatas

Quote:

```
name="client12_browsing" parent=choi packet-mark="client12_browsing" limit-at=0 queue=browsing priority=1 max-limit=0 burst-limit=0 burst-threshold=0
```

```
name="client12_download" parent=choi packet-mark="client12_download" limit-at=0 queue=download
priority=8 max-limit=0 burst-limit=0 burst-threshold=0
```

Selesai...

Silahkan di uji coba...

maaf ada kesalahan dikit :

Quote:

```
chain=postrouting out-interface=ether1 dst-address=192.168.10.0/24 protocol=tcp dst-port=80 action=mark-
connection new-connection-mark=http_conn passthrough=yes
```

untuk dst-port harap diganti dengan src-port=80....

Saya coba modifikasi sedikit sehingga arah setingannya lebih 'global' tidak hanya berdasarkan ip client, menggunakan webproxy dan sejauh ini berjalan dengan baik. (menggunakan list nice, sehingga aktifitas browsing/download IIX tidak dibatasi). Saya juga menggunakan **prerouting** pada manglenya.

di *mangle*

Code:

```
chain=prerouting protocol=tcp dst-port=80 dst-address-list=!nice action=mark-
connection new-connection-mark=http_conn passthrough=yes

chain=prerouting connection-mark=http_conn connection-bytes=0-131072 action=mark-
packet new-packet-mark=browsing passthrough=no

chain=output connection-mark=http_conn connection-bytes=0-131072 action=mark-packet
new-packet-mark=browsing passthrough=no

chain=prerouting connection-mark=http_conn connection-bytes=131073-4294967295
action=mark-packet new-packet-mark=download passthrough=no

chain=output connection-mark=http_conn connection-bytes=131073-4294967295
action=mark-packet new-packet-mark=download passthrough=no
```

pada *queue type*

Code:

```
name="browsing" kind=pcq pcq-rate=512000 pcq-limit=50 pcq-classifier=dst-address
pcq-total-limit=2000

name="download" kind=pcq pcq-rate=32000 pcq-limit=50 pcq-classifier=dst-address pcq-
total-limit=2000
```

pada *queue tree*

Code:

```
name="clovanzo" parent=LAN packet-mark="" limit-at=10000000 queue=default priority=3
max-limit=10000000 burst-limit=0 burst-threshold=0 burst-time=0s

name="client_browsing" parent=clovanzo packet-mark=browsing limit-at=0
queue=browsing priority=1 max-limit=0 burst-limit=0 burst-threshold=0 burst-time=0s

name="client_download" parent=clovanzo packet-mark=download limit-at=0
queue=download priority=8 max-limit=0 burst-limit=0 burst-threshold=0 burst-time=0s
```

kalo ada salah mohon bantuan revisinya

## Memisahkan Gateway Internasional dan IIX dengan 3 NIC (Bagian 2)

Pada eksperimen saya ini, router mikrotik kita juga akan berfungsi sebagai limiter internasional & IIX, tapi untuk mendukung ini kita membutuhkan 3 NIC, dengan fungsi 1 sebagai interface traffic internasional, 1 sebagai interface traffic local dan 1 sebagai interface distribusi

Saya asumsikan kondisi address-list sudah memuat semua blok IP IIX dan supaya tidak pusing kita rubah nama-nama interface menjadi :

1. Internasional
2. Lokal
3. Distribusi

selanjutnya kita configure ip address masing2 interface

Code:

```
/ip address
add address=192.168.7.1/24 interface=distribusi comment="ip trafik distribusi"
disabled=no
add address=203.89.26.50/30 interface=Internasional comment="ip trafik
internasional" disabled=no
add address=203.89.26.46/30 interface=Lokal comment="ip trafik IIX" disabled=no
```

dan kita tandai paket yang menuju IIX dari interface distribusi

Code:

```
/ip firewall mangle
add chain=prerouting in-interface=distribusi dst-address-list=nice action=mark-
routing new-routing-mark=nice2 passthrough=yes comment="mark nice trafic"
disabled=no
```

perbedaan dengan tutorial yang lalu adalah sekarang kita memberi mangle dengan chain prerouting dan hanya melakukan mangle di traffic yang datang melalui interface distribusi

sekarang membuat ip route dengan command

Code:

```
/ip route
add dst-address=0.0.0.0/0 gateway=203.89.26.49 scope=255 target-scope=10
comment="gateway traffic internasional" disabled=no
add dst-address=0.0.0.0/0 gateway=203.89.26.45 scope=255 target-scope=10
comment="gateway traffic IIX" mark=nice2 disabled=no
```

Next .. kita buat queue untuk setiap client ..

Code:

```
/queue simple
add name="IIX-Client-01" max-limit=256000/256000 dst-address="192.168.7.212"
interface=lokal
add name="INT-Client-01" max-limit=64000/64000 dst-address="192.168.7.212"
interface=internasional
```

proses limit bandwidth akan dilakukan hanya untuk client dengan ip 192.168.7.212 yang trafiknya melalui interface lokal / internasional, dimana traffic yang melewati interface ini telah kita pisah pada ip route diatas

## Bandwidth management di Hotspot Area

Banyak para pemakai selalu menanyakan sekitar bagaimana caranya memprioritaskan lalu lintas trafik menggunakan layanan Mikrotik RouterOS Hotspot.

Metoda yang berikut membantu ke arah mengatur lalu lintas jaringan dan menyesuaikan nya cara Anda ingin. Itu juga memastikan untuk menyediakan layanan yang benar untuk suatu penggunaan yang spesifik di suatu jaringan yang besar, memberi prioritas untuk VIPs, Para Pemakai atau jasa khusus di suatu jaringan yang terlampau banyak.

Juga, anda dapat menggunakan metoda yang sama jika anda ingin pastikan para user bahwa mestinya tidak men-download-an atau upload file karena periode lama untuk selamatkan sisa tersedia lalu lintas untuk para pemakai yang ringan yang sedang mencari kecepatan baik untuk browsing. Ini dapat diterapkan dengan memakasi burst limit atau suatu kombinasi limit-at dan burst limit dengan prioritas.

Triknya dengan menggunakan Users Profiles bandwidth management, dan menugaskan jenis kecepatan-kecepatan berbeda yang dihubungkan dengan suatu kelompok khusus.

Nah untuk menseting traffiknya, kita dapat menggunakan rumus sbb:

**x1k/y1k x2k/y2k x3k/y3k x5/y5 P x6k/y6k** yang diletakkan di Rate Limit di user profile dimana:

x1k/y1k: Rate (txrate/rxrate i.e 128k/1024k)

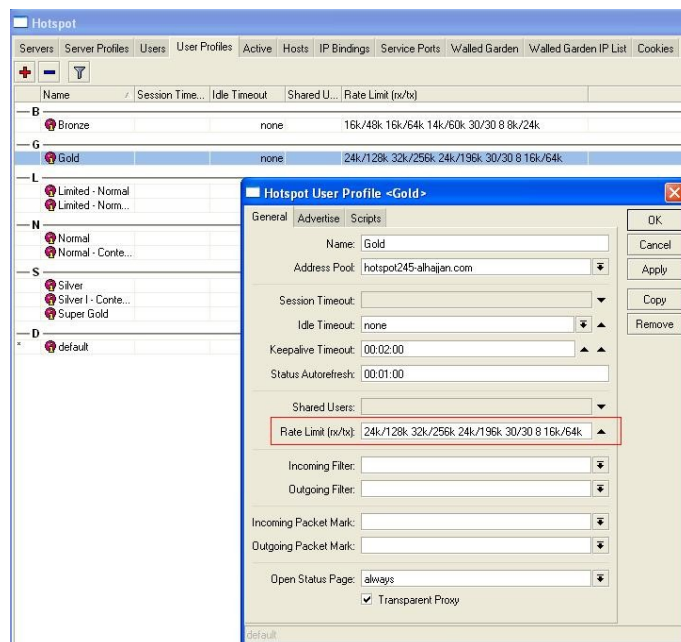
x2k/y2k: Burst Rate (i.e 256k/2048k)

x3k/y3k: Burst Threshold (i.e 160k/1280k)

x5/y5: Burst Time (in seconds i.e: 60/60)

Priority: P (use integer from 1-8)

Minimum rate: x6k/y6k (i.e 32k/256k)



Nah ini screenshotnya:

arti setting diatas:

Rate:24k/128k

Burst Rate: 32k/256k

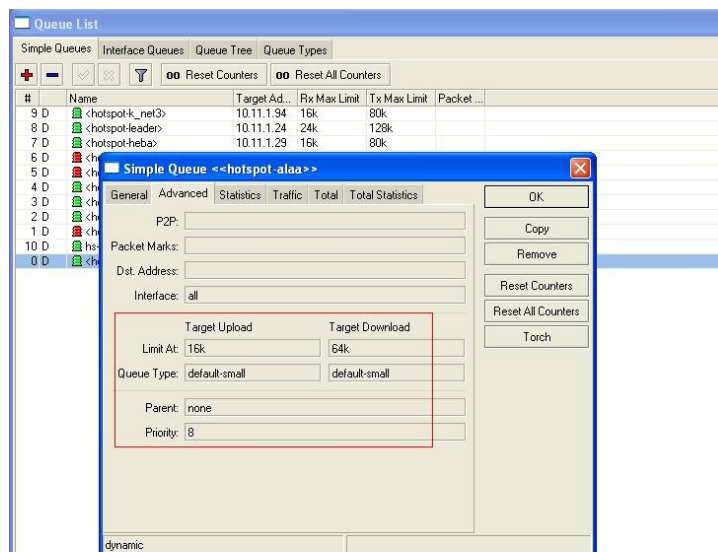
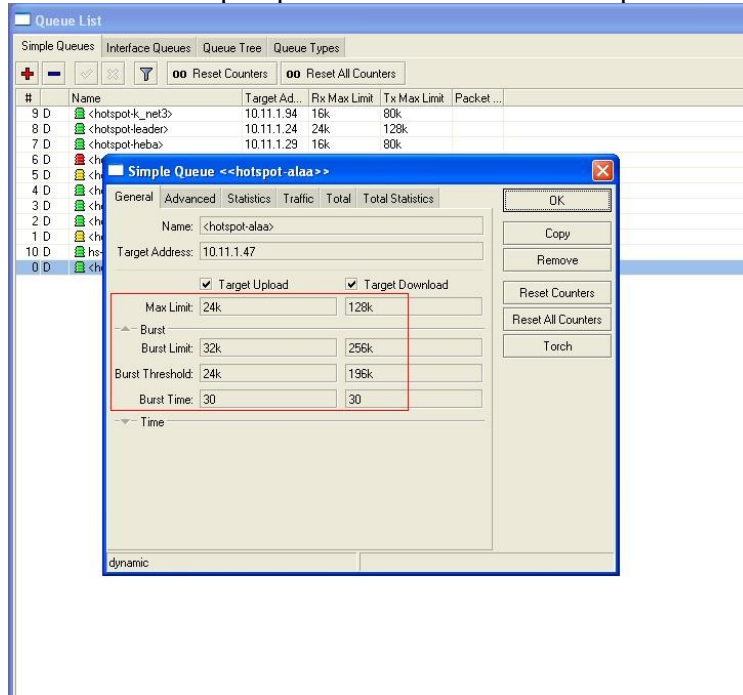
Burst Threshold: 24k/196k

Burst Time: 30/30

Priority: 8

Minimum rate: 16k/64k

Nah nanti di simple queue akan terlihat sama seperti settingan di hotspotnya:



Nah untuk mengecek prioritasnya lihat ini:

Selamat mencoba.....

ditranslate bebas dari:

[http://wiki.mikrotik.com/wiki/Hotspot\\_configuration\\_priorities](http://wiki.mikrotik.com/wiki/Hotspot_configuration_priorities)

## Memisahkan IIX ke ISP wireless dan Internasional ke speedy ...

```
/ ip firewall mangle
add chain=prerouting src-address=10.0.0.0/24 dst-address-list=nice \
action=mark-connection new-connection-mark=mark-con-indonesia \
passthrough=yes comment="" disabled=no
add chain=prerouting src-address=10.0.0.0/24 dst-address-list=!nice \
action=mark-connection new-connection-mark=mark-con-overseas \
passthrough=yes comment="" disabled=no
add chain=prerouting connection-mark=mark-con-indonesia action=mark-packet \
new-packet-mark=indonesia passthrough=yes comment="" disabled=no
add chain=prerouting connection-mark=mark-con-overseas action=mark-packet \
new-packet-mark=overseas passthrough=yes comment="" disabled=no
add chain=prerouting in-interface="Atas - Lan" packet-mark=overseas \
action=mark-routing new-routing-mark=speedy passthrough=no comment="" \
disabled=no
```

```
/ ip route
add dst-address=0.0.0.0/0 gateway=222.222.222.1 scope=255 target-scope=10 \
comment="ISP Wireless" disabled=no
add dst-address=0.0.0.0/0 gateway=192.168.1.1 scope=255 target-scope=10 \
routing-mark=speedy comment="Speedy" disabled=no
```

```
add name="LAN" target-addresses=10.0.0.0/24 dst-address=10.0.0.0/24 \
interface=all parent=none direction=both priority=8 \
queue=default-small/default-small limit-at=0/0 max-limit=0/0 \
total-queue=default-small disabled=no
add name="Billing iix" target-addresses=10.0.0.2/32 dst-address=0.0.0.0/0 \
interface=all parent=none packet-marks=indonesia direction=both priority=8 \
queue=default-small/default-small limit-at=0/0 max-limit=128000/128000 \
total-queue=default-small disabled=no
add name="Billing int" target-addresses=10.0.0.2/32 dst-address=0.0.0.0/0 \
interface=all parent=none packet-marks=overseas direction=both priority=8 \
queue=default-small/default-small limit-at=0/0 max-limit=64000/64000 \
total-queue=default-small disabled=no
```

nat nya dibagi dua juga ga bos? apa di masquerade aja.

satu global nat pake masquerade tanpa menyebutkan out interface boleh.

dua global nat dengan masquerade dengan menyebutkan out interface juga boleh.

dua src-nat dengan menyebutkan src-address dan to-address juga boleh.

gunakan lah yang sesuai dengan ilmu yang di miliki... biar gampang ngebenerinnya klo kenapa2 🤔

## How To Block Traceroute

cuma mau nambahin buat blok traceroute dan ping  
soanya kadang2 ada user yang "jago" dia bisa dapat ip yang sejajar dengan interface yang langsung menuju ke internet

=====

contoh :

ISP----MIKROTIK---CLIENT

tetapi dengan trace route dia bisa dapat nomor ip yang sejajar dengan Interface mikrotik yang menuju internet, seperti ini

ISP-----MIKROTIK-----CLIENT  
-----CLIENT"JAGO"

=====

nah untuk menanggulangi kita bisa bikin rule pada firewall seperti ini

```
/ip firewall filter add chain=forward protocol=icmp icmp-options=11:0 action=drop comment="Drop Traceroute"  
/ip firewall filter add chain=forward protocol=icmp icmp-options=3:3 action=drop comment="Drop Traceroute"
```

nah untuk membatasi ping, kadang2 ada client yang sukanya iseng menuhin traffic dengan picg yang gak jelas,ada baiknya kita batasi ping-nya

```
/ip firewall filter add chain=input action=accept protocol=icmp limit=50/5s,2
```

## HOWTO: Menghindari Port Scanner dari Hacker

di bagian filter:

Code:

```
/ip firewall filter
add chain=input protocol=tcp psd=21,3s,3,1 action=add-src-to-address-list address-
list="port scanners" address-list-timeout=2w comment="Port scanners to list "
disabled=no
```

Chain ini dipakai untuk mendaftar ip ke black-list address list

Chain selanjutnya untuk mendeteksi apakah ada indikasi aktifitas port scanner:

Code:

```
add chain=input protocol=tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg action=add-src-
to-address-list address-list="port scanners" address-list-timeout=2w comment="NMAP
FIN Stealth scan"

add chain=input protocol=tcp tcp-flags=fin,syn action=add-src-to-address-list
address-list="port scanners" address-list-timeout=2w comment="SYN/FIN scan"

add chain=input protocol=tcp tcp-flags=syn,rst action=add-src-to-address-list
address-list="port scanners" address-list-timeout=2w comment="SYN/RST scan"

add chain=input protocol=tcp tcp-flags=fin,psh,urg,!syn,!rst,!ack action=add-src-to-
address-list address-list="port scanners" address-list-timeout=2w
comment="FIN/PSH/URG scan"

add chain=input protocol=tcp tcp-flags=fin,syn,rst,psh,ack,urg action=add-src-to-
address-list address-list="port scanners" address-list-timeout=2w comment="ALL/ALL
scan"

add chain=input protocol=tcp tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg action=add-src-
to-address-list address-list="port scanners" address-list-timeout=2w comment="NMAP
NULL scan"
```

jika ada tanda tanda dari kejadian di atas, maka harus didrop scanning IPnya pakai perintah ini:

Code:

```
add chain=input src-address-list="port scanners" action=drop comment="dropping port
scanners" disabled=no
```

sumber:

HTML Code:

```
http://wiki.mikrotik.com/wiki/Drop\_port\_scanners
```



## HOW TO : Melindungi Pelanggan/User Anda

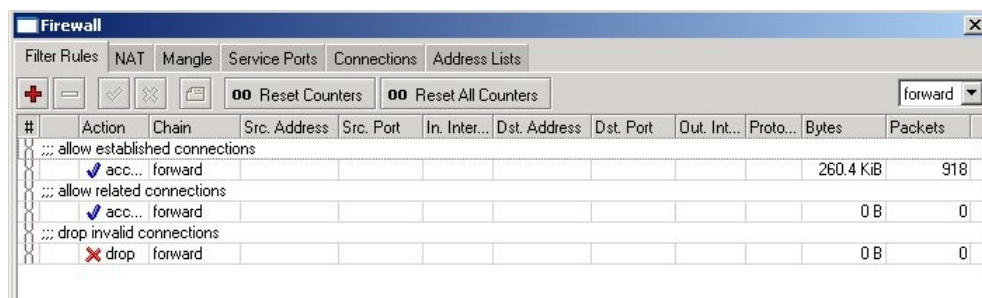
Untuk melindungi network pelanggan/user anda, kita harus memeriksa semua traffic yang melewati router dan blok yang tidak diinginkan.

Untuk traffic ICMP, TCP, UDP kita akan membuat chain dimana akan melakukan DROP untuk paket-paket yang tidak diinginkan. Untuk awalnya kita dapat meng-copy dan paste command dibawah ini melalui terminal console pada RouterOS kita :

Code:

```
/ip firewall filter
add 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"
```

Pada rule diatas, 2 rule pertama berurusan dengan paket untuk koneksi telah terbuka dan berhubungan dengan koneksi lainnya. Kita mengasumsikan bahwa paket tersebut tidak bermasalah. Pada rule selanjutnya kita akan melakukan DROP pada paket dari koneksi yang Invalid.



#	Action	Chain	Src. Address	Src. Port	In. Inter...	Dst. Address	Dst. Port	Out. Int...	Proto...	Bytes	Packets
1	allow established connections										
2	✓ acc...	forward								260.4 KiB	918
3	allow related connections										
4	✓ acc...	forward								0 B	0
5	drop invalid connections										
6	✗ drop	forward								0 B	0

Selanjutnya, kita akan mem-filter dan melakukan DROP pada paket-paket yang kelihatannya berasal dari HOST yang terinfeksi Virus.

Daripada kita menambah rule-rule dibawah ke forward chain, yang berakibat chain forward terlalu penuh dengan rule sehingga sulit melakukan troubleshooting. Kita dapat menambah chain tersendiri, dan dapat diberi nama **Virus**. Dan rule-rule dibawah kita masukkan ke chain tersebut.

Code:

```
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 Dumar.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"
```

Here, we list all those well known "bad" protocols and ports, used by various trojans and viruses when they take over your computer. This list is incomplete; we should add more rules to it! We can jump to this list from the forward chain by using a rule with action=jump:

Diatas kita telah dapatkan daftar rule untuk memfilter paket-paket dari protocol dan posrt yang merupakan berasal dari Virus ataupun Trojan. Daftar diatas belum komplit, kita bisa mendapatkan rule-rule tambahan dari berbagai sumber, tapi setidaknya rule diatas dapat menjadi awal.

Agar paket dari chain **forward** dapat menuju ke chain **virus** kita dapat menererapkan **action=jump**, seperti rule dibawah ini :

Code:

```
add chain=forward action=jump jump-target=virus comment="jump to the virus chain"
```

Chain Forward kita akan nampak seperti dibawah ini :

#	Action	Chain	Src. Address	Src. Port	In. Inter...	Dst. Address	Dst. Port	Out. Int...	Proto...	Bytes	Packets
1	allow established connections	forward								1390.3 KiB	5052
2	allow related connections	forward								1248 B	12
3	drop invalid connections	forward								0 B	0
4	jump to the virus chain	forward								48 B	1

Bila paket yang ter-jump ke chain **virus** tidak ter-filter, maka paket tersebut akan dikembalikan ke chain **forward**.

Kita dapat dengan mudah menambahkan rule yang membolehkan **udp** dan **ping** dan drop yang lainnnya (jika tidak ada service pada network user yang perlu diakses dari network luar) :

Code:

```
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"
```

Demikian tutorial ini, semoga bermanfaat bagi kita semua

Ditranslasikan secara bebas dari : [http://wiki.mikrotik.com/wiki/Protecting\\_your\\_customers](http://wiki.mikrotik.com/wiki/Protecting_your_customers)

## Load-balancing & Fail-over di MikroTik

Kondisi : ISP dimana kita bekerja sebagai Administrator menggunakan lebih dari satu gateway untuk terhubung ke Internet. Semuanya harus dapat melayani layanan upstream & downstream. Karena akan beda kasusnya apabila salah satunya hanya dapat melayani downstream, contohnya jika menggunakan VSAT DVB One-way.

Untuk kasus ini dimisalkan ISP memiliki 2 jalur ke Internet. Satu menggunakan akses DSL (256 Kbps) dan lainnya menggunakan Wireless (512 Kbps). Dengan rasio pemakaian DSL:Wireless = 1:2 .

Yang akan dilakukan :

1. Menggunakan semua jalur gateway yang tersedia dengan teknik load-balancing.
2. Menjadikan salah satunya sebagai back-up dengan teknik fail-over.

OK, mari saja kita mulai eksperimennya :

1. IP address untuk akses ke LAN :

```
> /ip address add address=192.168.0.1/28 interface=LAN
```

IP address untuk akses ke jalur DSL :

```
> /ip address add address=10.32.57.253/29 interface=DSL
```

IP address untuk akses ke jalur Wireless :

```
> /ip address add address=10.9.8.2/29 interface=WIRELESS
```

Tentukan gateway dengan rasionya masing-masing :

```
> /ip route add gateway=10.32.57.254,10.9.8.1,10.9.8.1
```

2. Pada kasus untuk teknik fail-over. Diasumsikan jalur utama melalui Wireless dengan jalur DSL sebagai back-up apabila jalur utama tidak dapat dilalui. Untuk mengecek apakah jalur utama dapat dilalui atau tidak, digunakan command ping.

```
> /ip firewall mangle add chain=prerouting src-address=192.168.0.0/28 action=mark-routing new-routing-mark=SUBNET1-RM
```

```
> /ip route add gateway=10.9.8.1 routing-mark=SUBNET1-RM check-gateway=ping
```

```
> /ip route add gateway=10.32.57.254
```

## Another Load Balancing Tutorial

### 1. Masalah IP Address silahkan di definisikan sendiri.

### 2. Bikin Mangle :

```
add chain=prerouting in-interface=LocalHost connection-state=new nth=2,1,0 \
```

```
action=mark-connection new-connection-mark=one passthrough=yes \
```

```
comment="Load Balancing - 3 Gateway by Raden Dody uhuy" disabled=no
```

```
add chain=prerouting in-interface=LocalHost connection-mark=one \
```

```
action=mark-routing new-routing-mark=one passthrough=no comment="" \
```

```
disabled=no
```

```
add chain=prerouting in-interface=LocalHost connection-state=new nth=2,1,1 \
```

```
action=mark-connection new-connection-mark=two passthrough=yes comment="" \
```

```
disabled=no
```

```
add chain=prerouting in-interface=LocalHost connection-mark=two \
```

```
action=mark-routing new-routing-mark=two passthrough=no comment="" \
```

```
disabled=no
```

```
add chain=prerouting in-interface=LocalHost connection-state=new nth=2,1,2 \
```

```
action=mark-connection new-connection-mark=three passthrough=yes comment="" \
```

```
disabled=no
```

```
add chain=prerouting in-interface=LocalHost connection-mark=three \
```

```
action=mark-routing new-routing-mark=three passthrough=no comment="" \
```

```
disabled=no
```

### 3. Bikin NAT

```
/ip firewall nat
```

```
add chain=srcnat out-interface=[nama interface 1] connection-mark=one \
action=masquerade comment="NAT for Load Balancing by Mbah Dody au ah gelap" disabled=no
add chain=srcnat out-interface=[nama interface 2] connection-mark=two \
action=masquerade comment="" disabled=no
add chain=srcnat out-interface=[nama interface 3] connection-mark=three \
action=masquerade comment="" disabled=no
```

#### 4. Bikin Routing

```
/ ip route
add dst-address=0.0.0.0/0 gateway=[IP Interface 1] scope=255 target-scope=10 \
routing-mark=one comment="Route for Load Balancing by Ki Dody oye" disabled=no
add dst-address=0.0.0.0/0 gateway=[IP Interface 2] scope=255 target-scope=10 \
routing-mark=two comment="" disabled=no
add dst-address=0.0.0.0/0 gateway=[IP Interface 3] scope=255 target-scope=10 \
routing-mark=three comment="" disabled=no
```

Sudah saya coba dan sukses, dulu ada dan banyak website yg tidak mau menerima koneksi dari client yg load balancing terutama website yg mengandung banyak security, tapi sudah saya coba utk akses [www.klikbca.com](http://www.klikbca.com), buka email nggak masalah, cuman tetep ada masalah ... kenapa saldo saya nggak

nambah-nambah ya ? 😊. sory ngelantur.

Tapi tetep nanti akan ketemu website yg nggak mau menerima , utk itu perlu dibuatkan mangle khusus utk web yg nggak mau tsb, berikut scriptnya :

```
/ ip firewall mangle
add chain=prerouting in-interface=LocalHost dst-address-list=Nggak Doyan Load Balancing \
action=mark-routing new-routing-mark=one passthrough=yes comment="Ora \
Doyan Load Balancing" disabled=no
```

**Perhatian :** Script tersebut harap di letakkan sebelum script load balancing.

#### 5. Buat Address List website yg nggak mau menerima client Load Balancing.

```
/ ip firewall address-list
add list=Nggak Doyan Load Balancing address=[IP Addressnya berapa ?] comment="" disabled=no
Quote:
```

Originally Posted by **jhoe** 📧

*Salam kenal bro q jhoe,*

*Gimana cara nyeting DNS untuk 2 ISP, kan gini bos q pkai IM2 dan dapat jatah dari kampus yang DNS nya beda.*

bukannya tinggal di set di DNS nya mikrotik aja?

contoh yg punya gw pake speedy (192.168.1.1 -- dns dari modem) dan cbn (202.158.3.6)

Code:

```
[admin@MikroTik] > /ip dns print
primary-dns: 192.168.1.1
secondary-dns: 202.158.3.6
allow-remote-requests: yes
cache-size: 8192KiB
cache-max-ttl: 1w
cache-used: 3430KiB
```

## **Redirect Mikrotik ke Komputer Proxy Squid (tanpa parent proxy MT)**

Begini Saya meredirect Mikrotik (MT) ke squid Proxy tanpa menghidupkan web-proxy yang ada di MT nya, saya sempat kesulitan mencari solusi supaya dapat me redirect port 80, 8080, ke port 3128 (transparent proxy), karena kalau saya pakai web-proxy MT internet saya jadi lemot koneksinya, pernah saya pakai parent proxy MT redirect ke squid tapi hasilnya gak maksimal internet kadang masih lemot karena web-proxy di hidupkan (enable), makanya saya mencoba meng kotak-kotak eh meng kotak-katik akhirnya dapet referensi dari <http://tldp.org/HOWTO/TransparentProxy-6.html>, yang intinya bisa redirect port 80 ke 3128 tanpa menghidupkan web-proxy mikrotik. Topology yang saya gunakan adalah sebagai berikut :

Client⇄ Switch ⇄ Mikrotik ⇄ ISP -

..... |  
.....Squid-Box

Di mikrotik ada 3 LAN card terus saya namai lan, wan, proxy

Lan = 192.168.1.1

Wan = 202.114.12.112

Proxy = 192.168.0.1

Squid (Ubuntu 7.10 server) Eth0 = 192.168.0.2

Untuk settingan awal MT gak perlu saya tulis disini ya, termasuk pembagian bandwidth nya, serta konfigurasi squidnya. saya langsung saja cara translasinya

## **Buat NAT nya dulu di IP firewall NAT (sharing internet)**

```
/ip firewall nat add chain=srcnat out-interface=wan action=masquerade
```

## **Terus buat nat untuk redirect ke squid**

```
/ip firewall nat add chain=dst-nat src-address=192.168.0.2 protocol=tcp dst-port=80 in-interface=lan  
action=dst-nat to-address=192.168.0.2 to-port=3128
```

```
/ip firewall nat add chain=dst-nat src-address=192.168.0.2 protocol=tcp dst-port=8080 in-interface=lan  
action=dst-nat to-address=192.168.0.2 to-port=3128
```

```
/ip firewall nat add chain=src-nat src-address=192.168.1.0 out-interface=lan action=srcnat src-  
address=192.168.1.1 to-port=3128
```

## **Terus buat filter rules nya**

```
/ip firewall filter add chain=forward src-address=192.168.1.0 dst-address=192.168.0.2 dst-port=3128 in-  
interface=lan out-interface=wan action=accept
```

Nah sekarang coba deh, jadi bisa simpan cache di squid-proxy external tanpa harus lewat parent proxy nya mikrotik... Kalau ada kendala coba di ubuntu servernya di tambahin ini (sebaiknya jgn diisi dulu di Ubuntunya kalau belum bisa konek baru isi iptables dibawah ini) :

```
iptables -t nat -A PREROUTING -I eth0 -s ! SQUID - tcp -dport 80 -j DNAT -to SQUID:3128
```

```
iptables -t nat -A PREROUTING -I eth0 -s ! SQUID - tcp -dport 8080 -j DNAT -to SQUID:3128
```

```
iptables -t nat -A POSTROUTING -o eth0 -s LAN -d SQUID -j SNAT -to iptables-box
```

```
iptables -A FORWARD -s LAN -d SQUID -i eth0 -p tcp -dport 3128 -j ACCEPT
```

sekali lagi mohon ma`af rekan-rekan semua, karena masih tahap belajar, mungkin kalau ada kesalahan mohon dikoreksi, atau ada tambahan mohon di benahi..

-----  
kalau bobol limiter bwnya itu akibat NAT/Masquerading pada Mikrotik maupun akibat redirecting pada Proxy servernya sehingga pada server limiter akan kebaca IP Mikrotik ataupun Ip Proxy server.

Paling aman adalah sampeyan tinggal menggunakan mikrotik sebagai bandwidth management dan sebagai

router pembelok Policy routing dimana setiap packet dari client yang memiliki protocol TCP dan tujuan portnya 80 dibelokkan dulu ke IP Proxy tanpa melalui proses NAT dan tidak mengubah header IP sourcenya. Kemudian di proxy baru sampeyan redirect port 80 tadi kedalam port proxynya misal 8080.

Cara ini berlaku untuk Mikrotik berfungsi sebagai hotspot maupun sebagai router/gateway biasa. contoh Perintah untuk membelokkan routing (Cara ini berlaku untuk Mikrotik berfungsi sebagai hotspot tanpa transparent proxy maupun Mikrotik sebagai router/gateway biasa) :

Asumsi 1 : IP Network LAN 192.168.1.0/24

Asumsi 2 : IP Proxy server 192.168.1.254

Asumsi 3 : PC router/Gateway menggunakan Mikrotik 😁

1. Pertama kita definisikan dulu IP mana yang harus kena policy routing atau dengan kata lain mau kita belokkan ke Proxy untuk kita redirect

```
/ip firewall address-list add list=Source-IP-belok-ke-Proxy address=192.168.1.0/24 comment="Blok Source/asal Ip yang harus dibelokin ke Proxy" disabled=no
```

2. Kedua kita kita definisikan list IP yang dimana kalau client mengakses IP yang kita definisikan tersebut tidak boleh kena Proxy (contohnya Ip Proxy itu sendiri)

```
/ip firewall address-list add list=Destination-IP-Ngga-Boleh-Kena-Proxy address=192.168.1.254 comment="IP Proxy yang ngga boleh dibelokin kembali ke proxy" disabled=no
```

3. Langkah ketiga kita marking packet dulu yang dimana paket tersebut merupakan paket berasal dari Client dengan protocol TCP dan dst-port 80 melalui mangle dengan nama proxy-route

```
/ip firewall mangle add chain=prerouting action=mark-routing new-routing-mark=proxy-route passthrough=no dst-port=80 protocol=tcp src-address-list=Source-IP-belok-ke-Proxy dst-address-list=! Destination-IP-Ngga-Boleh-Kena-Proxy
```

4. Kemudian kita tambahkan routing dengan ketentuan Policy routing pada mikrotik kita sebagai berikut

```
/ip route add dst-address=0.0.0.0/0 gateway=192.168.1.254 routing-mark=proxy-route comment="" disabled=no
```

5. Kemudian di Server Proxy Kita kita tambahkan dengan Perintah redirecting paket yang mempunyai tujuan protocol TCP dst-port 80 kedalam Port daemon Proxy kita (contohnya 8080). Contoh pada Linux adalah :

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080
```

6. Nah untuk Bandwidth management pada mikrotik yang menggunakan simple queue ngga masalah, tapi kalau menggunakan Queue tree perlu lihat dulu apakah mikrotiknya berfungsi sebagai NAT atau tidak. Tapi pada prinsipnya kalau settingan di Ip firewall manglenya benar, tidak akan menjadi masalah.

## Delaypool rasa Mikrotik

Tutorial sederhana ( hanya 3 langkah ) ini sangat bermanfaat bagi RT/RW net atau warnet yang ingin melakukan optimalisasi bandwidth dengan melakukan queue traffic download dari file-file tertentu.

Sudah menjadi masalah klasik ketika bandwidth warnet / RT/RW net harus habis karena ada salah satu client/user rakus bandwidth melakukan downloading .

Tentunya dengan simpe queue sederhana hal ini bisa diatasi.

Tapi bagaimana jika client awam tetap ingin browsing itu lancar meskipun mereka sedang download file.

Client yang aneh ...

Berikut tutorial untuk melakukan limitasi bandwidth dari DataUtamaNet untuk melimit traffic download extension file2 tertentu.

Disini saya akan memanfaatkan fasilitas content, address list, mangle dan simple queue dari mikrotik.

Saya asumsikan Router Mikrotiik sudah terinstall dengan baik, dalam artian client kita sudah bisa akses internet dengan lancar.

### Langkah 1

Kita masukan rule di firewall untuk mendapatkan IP dari download server dan memasukan IP tersebut ke dalam address list

```
/ip firewall filter add chain=forward \
```

```
src-address=192.168.10.0/24 protocol=tcp content=.mp3 \
```

```
action=add-dst-to-address-list address-list=downloads \
```

```
address-list-timeout=01:00:00
```

```
/ip firewall filter add chain=forward \
```

```
src-address=192.168.10.0/24 protocol=tcp content=.exe \
```

```
action=add-dst-to-address-list address-list=downloads \
```

```
address-list-timeout=01:00:00
```

Rule diatas akan menangkap semua traffic dengan content .mp3 dan .exe yang berasal dari blok IP LAN dan memasukkannya ke addres list downloads selama 1 jam.

Variable diatas dapat dirubah sesuai dengan topology dan kebutuhan anda sendiri.

## Langkah 2

Kita lakukan mangle untuk marking paket yang berasal dari address list yang telah kita dapat dari Langkah 1

```
/ip firewall mangle add chain=forward \  
protocol=tcp src-address-list=downloads \  
action=mark-packet new-packet-mark=download-paket
```

Mangle ini kita perlukan untuk melabeli paket sehingga simple queue dapat menangkap traffic dari IP-IP yang telah terdapat pada address list “downloads”

## Langkah 3

Langkah terakhir kita masukkan simple queue dari paket mark yang telah kita dapat dari langkah 2

```
/queue simple add name=download-files \  
max-limit=64000/64000 packet-marks=download-paket
```

Letakan queue di urutan paling atas supaya dibaca dulu oleh mikortik

That's it ..

Kita sudah berhasil mengalokasikan bandwidth untuk traffic download file2 yang kita inginkan, dan browsing tetap lancar .. meskipun browsing ke server yang sudah pada address list menjadi lambat karena ikut ke limit ;- ) at least for the next 1 hour J

FYI saya sudah pernah melakukan marking paket dengan memasukan langsung content pada rule mangle tapi pada prakteknya ketika kita mendownload file dengan extension yang sama secara simultan Queue tidak berjalan efektif 100%

Coba ini:

Quote:

```
/ip firewall ma  
add chain=forward protocol=tcp content=.exe \  
action=mark-connection new-connection-mark=con-dowloader passthrough=yes \  
comment="" disabled=no  
add chain=output protocol=tcp content=.exe \  
action=mark-connection new-connection-mark=con-dowloader passthrough=yes \  
comment="" disabled=no  
add chain=forward protocol=tcp content=.avi \  
action=mark-connection new-connection-mark=con-dowloader passthrough=yes \
```



```
comment="" disabled=no
add chain=output protocol=tcp content=.avi \
action=mark-connection new-connection-mark=con-downloader passthrough=yes \
comment="" disabled=no
add chain=forward protocol=tcp content=.zip \
action=mark-connection new-connection-mark=con-downloader passthrough=yes \
comment="" disabled=no
add chain=output protocol=tcp content=.zip \
action=mark-connection new-connection-mark=con-downloader passthrough=yes \
comment="" disabled=no
add chain=output connection-mark=con-downloader action=mark-packet \
new-packet-mark=downloader-pkt passthrough=no comment="" disabled=no
add chain=forward connection-mark=con-downloader action=mark-packet \
new-packet-mark=downloader-pkt passthrough=no comment="" disabled=no
```

\*tambahin sendiri ext pa ja sampe puaas taro diatas

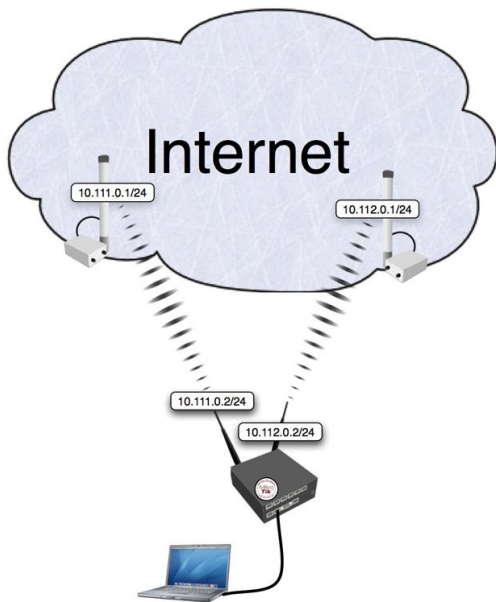
queuenya

Quote:

```
/queue simple
add name="downloader" dst-address=0.0.0.0/0 interface=all \
packet-marks=downloader-pkt direction=both priority=8 \
queue=default-small/default-small limit-at=0/64000 max-limit=0/64000 \
burst-limit=/128000 burst-threshold=/96000 burst-time=/10s \
total-queue=default-small disabled=no
```

semoga membantu  
terima kasih

## 2 ISP IN 1 ROUTER WITH LOADBALANCING



```
/ ip address
add address=192.168.0.1/24 network=192.168.0.0 broadcast=192.168.0.255 interface=Local comment="" \
disabled=no
add address=10.111.0.2/24 network=10.111.0.0 broadcast=10.111.0.255 interface=wlan2 \
comment="" disabled=no
add address=10.112.0.2/24 network=10.112.0.0 broadcast=10.112.0.255 interface=wlan1 \
comment="" disabled=no
/ ip firewall mangle
add chain=prerouting in-interface=Local connection-state=new nth=1,1,0 \
action=mark-connection new-connection-mark=odd passthrough=yes comment="" \
disabled=no
add chain=prerouting in-interface=Local connection-mark=odd action=mark-routing \
new-routing-mark=odd passthrough=no comment="" disabled=no
add chain=prerouting in-interface=Local connection-state=new nth=1,1,1 \
action=mark-connection new-connection-mark=even passthrough=yes comment="" \
disabled=no
add chain=prerouting in-interface=Local connection-mark=even action=mark-routing \
new-routing-mark=even passthrough=no comment="" disabled=no
/ ip firewall nat
add chain=srcnat connection-mark=odd action=src-nat to-addresses=10.111.0.2 \
to-ports=0-65535 comment="" disabled=no
add chain=srcnat connection-mark=even action=src-nat to-addresses=10.112.0.2 \
to-ports=0-65535 comment="" disabled=no
/ ip route
add dst-address=0.0.0.0/0 gateway=10.111.0.1 scope=255 target-scope=10 routing-mark=odd \
comment="" disabled=no
add dst-address=0.0.0.0/0 gateway=10.112.0.1 scope=255 target-scope=10 routing-mark=even \
comment="" disabled=no
add dst-address=0.0.0.0/0 gateway=10.112.0.1 scope=255 target-scope=10 comment="" \
disabled=no
```

***Mangle***

```
/ ip address
add address=192.168.0.1/24 network=192.168.0.0 broadcast=192.168.0.255 interface=Local comment="" \
disabled=no
add address=10.111.0.2/24 network=10.111.0.0 broadcast=10.111.0.255 interface=wlan2 \
comment="" disabled=no
add address=10.112.0.2/24 network=10.112.0.0 broadcast=10.112.0.255 interface=wlan1 \
comment="" disabled=no
```

*router punya 2 upstream (WAN) interfaces dengan ip address 10.111.0.2/24 and 10.112.0.2/24. dan interface LAN dengan nama interface "Local" dan ip address 192.168.0.1/24.*

```
/ ip firewall mangle
```

```
add chain=prerouting in-interface=Local connection-state=new nth=1,1,0 \
action=mark-connection new-connection-mark=odd passthrough=yes comment="" \
disabled=no
```

```
add chain=prerouting in-interface=Local connection-mark=odd action=mark-routing \
new-routing-mark=odd passthrough=no comment="" disabled=no
```

```
add chain=prerouting in-interface=Local connection-state=new nth=1,1,1 \
action=mark-connection new-connection-mark=even passthrough=yes comment="" \
disabled=no
add chain=prerouting in-interface=Local connection-mark=even action=mark-routing \
new-routing-mark=even passthrough=no comment="" disabled=no
```

### ***NAT***

```
/ ip firewall nat
add chain=srnat connection-mark=odd action=src-nat to-addresses=10.111.0.2 \
to-ports=0-65535 comment="" disabled=no
add chain=srnat connection-mark=even action=src-nat to-addresses=10.112.0.2 \
to-ports=0-65535 comment="" disabled=no
```

### ***Routing***

```
/ ip route
add dst-address=0.0.0.0/0 gateway=10.111.0.1 scope=255 target-scope=10 routing-mark=odd \
comment="" disabled=no
add dst-address=0.0.0.0/0 gateway=10.112.0.1 scope=255 target-scope=10 routing-mark=even \
comment="" disabled=no
add dst-address=0.0.0.0/0 gateway=10.112.0.1 scope=255 target-scope=10 comment="" \
disabled=no comment="gateway for the router itself"
```

## Tutz Load Balancing Plus plus [Chaozz version]

This is my first tutz i post in this forum. i hope this tutz is useful for all of you. i think this tutz is almost

same with other but this is my version. bukan forum english ne. pk bhs indo aja ar..



ISP 1 IIX : 10.0.68.1

ISP 2 Vsat : 10.0.32.1 <- internasional

ISP 3 Speedy : 10.0.22.1 <- internasional



Contoh aja

IP router ether1 (IIX) : 10.0.68.2/29

IP router ether2 (Vsat) : 10.0.32.2/29

IP router ether3 (Speedy) : 10.0.22.2/29

IP router ether4 (ke lan) : 192.168.1.1/24

Mangle

```
/ip fi ma add chain=prerouting src-address list=Vsat action=mark-routing new-routing-mark=Game  
comment=Vsat
```

```
/ip fi ma add chain=prerouting src-address list=Vsat dst-address list=nice action=mark-routing new-routing-  
mark=Vsat-iix comment=Vsat-iix
```

```
/ip fi ma add chain=prerouting src-address list=Speedy action=mark-routing new-routing-mark=Game  
comment=Speedy
```

```
/ip fi ma add chain=prerouting src-address list=Speedy dst-address list=nice action=mark-routing new-  
routing-mark=Speedy-iix comment=Speedy-iix
```

```
/ip fi address-list add address=x.x.x.x list=nice (masukin ip iix)
```

<http://ixp.mikrotik.co.id/download/nice.rsc>

NAT

```
/ip fi nat
```

```
add chain=srcnat action=src-nat to-addresses=10.0.32.2 to-ports=0-65535  
out-interface=ether2 routing-mark=Vsat
```

```
add chain=srcnat action=src-nat to-addresses=10.0.68.2 to-ports=0-65535  
out-interface=ether2 routing-mark=Vsat-iix
```

```
add chain=srcnat action=src-nat to-addresses=10.0.22.2 to-ports=0-65535  
out-interface=ether3 routing-mark=Speedy
```

```
chain=srcnat action=src-nat to-addresses=10.0.68.3 to-ports=0-65535  
out-interface=ether3 routing-mark=Speedy-iix
```

```
/ip ro add dst-address=0.0.0.0/0 gateway=10.0.68.1
/ip ro add dst-address=0.0.0.0/0 gateway=10.0.32.1 mark=Vsat
/ip ro add dst-address=0.0.0.0/0 gateway=10.0.68.1 mark=Vsat-iix
/ip ro add dst-address=0.0.0.0/0 gateway=10.0.22.1 mark=Speedy
/ip ro add dst-address=0.0.0.0/0 gateway=10.0.68.1 mark=Speedy-iix
```

Sekarang da siap ne..

tinggal masukin ip mana yg anda mo di kasi akses internet (klo ga ga di address-list ya gak jln hehe ) di masukin ke Vsat,Speedy di Address-list

Contoh:

```
/ip fi address-list add address=192.168.1.2 list=Vsat
/ip fi address-list add address=192.168.1.3 list=Speedy
/ip fi address-list add address=192.168.1.4 list=Speedy
/ip fi address-list add address=192.168.1.5 list=Speedy
/ip fi address-list add address=192.168.1.6 list=Vsat
/ip fi address-list add address=192.168.1.7 list=Speedy
/ip fi address-list add address=192.168.1.8 list=Vsat
/ip fi address-list add address=192.168.1.9 list=Speedy
```



Akhirnya Siap juga



mohon maaf klo ada yg salah.

---

Let's click "thank" if this posting is usefull.. Thank you

---

## # SETUP MIKROTIK (base 1)

1. setelah mikrotik terinstall dengan baik dan benar jalankan mikrotik anda
2. masukkan username & password, dalam hal ini karena masih baru maka default usernam : admin password : *blank*
3. ganti nama ethernet anda jika anda mau, dalam hal ini anda dapat memberikan nama apa saja =  
[kucing@mikrotik] >interface  
[kucing@mikrotik] interface >print (melihat dulu berapa banyak ethernet yg terpasang)  
[kucing@mikrotik] interface >set 0 name=LAN  
[kucing@mikrotik] interface >set 1 name=WAN
4. kemudian nambahkan ip addressnya  
[kucing@mikrotik] >ip address  
[kucing@mikrotik] ip address >add address=192.168.0.1/255.255.0.0 interface=LAN ----> ini untuk ip interface lokal  
[kucing@mikrotik] ip address >add address=203.90.1.1/255.255.255.240 interface=WAN ----> ini untuk ip global yg di dapet dari ISP
5. kemudian masukin gatewaynya  
[kucing@mikrotik] > ip route  
[kucing@mikrotik] ip route >add gateway=xxx.xxx.xxx.xxx/xxx.xxx.xxx.xxx ----> ini merupakan gateway untuk keluar
6. kemudian setup webproxy  
[kucing@mikrotik] >ip web-proxy  
[kucing@mikrotik] ip web-proxy >set enable=yes  
[kucing@mikrotik] ip web-proxy >set transparent-proxy=yes  
[kucing@mikrotik] ip web-proxy >set max-object-size=1200KiB ----> ini supaya nge loadnya ngacir si web



proxy

7. kemudian tambahkan rule supaya si client yg menggunakan port 80 akan di oper ke web-proxy  
[kucing@mikrotik] >ip firewall nat  
[kucing@mikrotik] ip firewall nat >add chain=dstnat protocol=tcp dst-port=80 action=redirect to-ports=3128
8. kemudian masukan dns nya  
[kucing@mikrotik] >ip dns  
[kucing@mikrotik] ip dns >set primary-dns=xxx.xxx.xxx.xxx  
[kucing@mikrotik] ip dns >set secondary-dns=xxx.xxx.xxx.xxx
9. Sekarang masqrade interface WANnya  
[kucing@mikrotik]>ip firewall nat  
[kucing@mikrotik] ip firewall nat>add chain=srcnat out-interface=WAN action=masquerade
10. sekarang coba ping ke gateway & dns dari mikrotik, kalo REPLY berarti dah konek



11. heuehuueeuhehehueuheuh selesai juga dah tutorial ke 2 gw

## ----TUTORIAL SETUP HOTSPOT----



- 1.[kucing@mikrotik]>ip hotspot
- 2.[kucing@mikrotik] ip hotspot>setup  
hotspot interface:LAN  
local address of network:xxx.xxx.xxx.xxx/xx -->ip dari inteface LAN  
masqurade network:yes  
address pool of network:xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx  
select certificate:none  
ip address of SMTP server:0.0.0.0  
DNS server:  
DNS name:  
name of local hotspot user: admin ----> user untuk masuk ke halaman hotspot  
password for the user:
3. sekarang buka web browser, ketikan ip addressnya hotspot
- 4.masukan username yg telah di buat tadi
- 5.walah berhasil kan.....

## -----TUTORIAL USER MANAGER WITH HOTSPOT-----

1. enable dulu use-radius di hotspot  
[kucing@mikrotik]>ip hotspot profile
2. [kucing@mikrotik] ip hotspot profile>print
3. akan terlihat profile2 yg telah di buat, kemudian tentukan profile mana yg akan di pake di use-radius  
[kucing@mikrotik]ip hotspot profile> set 0 use-radius=yes  
0 = merupakan nomor profile
- 4.sekarang bikin radiusnya  
[kucing@mikrotik]>radius  
[kucing@mikrotik]radius>add address=127.0.0.1  
[kucing@mikrotik]radius>print  
[kucing@mikrotik]radius>set 0 service=hotspot, secret=12345678
- 5.sekarang bikin owner untuk di usermanager  
[kucing@mikrotik]>/ tool user-manager customer add login=admin password=admin123456789  
permissions=owner
- 6.sekarang bikin penghubung/supaya si mikrotik ngeroute ke usermanager  
[kucing@mikrotik]>/ tool user-manager router add subscriber=admin ip-address=127.0.0.1 shared-secret=12345678
- 7.nah setelah ini smua dah di buat, sekarang untuk ngetes apakah usermanager dah konek apa blom
- 8.buka web browser ketik " 127.0.0.1/userman "
- 9.akan tampil halaman login userman, masukin dah tuh username=test password=test
- 10.huehuehuehuehuehuehue.....akhirnya kelar juga tutorial usermanagernya

## -----TUTORIAL 2 ISP IN 1 ROUTER WITH LOADBALANCING-----

```
/ ip address
add address=192.168.0.1/24 network=192.168.0.0 broadcast=192.168.0.255 interface=Local comment="" \
disabled=no
add address=10.111.0.2/24 network=10.111.0.0 broadcast=10.111.0.255 interface=wlan2 \
comment="" disabled=no
add address=10.112.0.2/24 network=10.112.0.0 broadcast=10.112.0.255 interface=wlan1 \
comment="" disabled=no
/ ip firewall mangle
add chain=prerouting in-interface=Local connection-state=new nth=1,1,0 \
action=mark-connection new-connection-mark=odd passthrough=yes comment="" \
disabled=no
add chain=prerouting in-interface=Local connection-mark=odd action=mark-routing \
new-routing-mark=odd passthrough=no comment="" disabled=no
add chain=prerouting in-interface=Local connection-state=new nth=1,1,1 \
action=mark-connection new-connection-mark=even passthrough=yes comment="" \
disabled=no
add chain=prerouting in-interface=Local connection-mark=even action=mark-routing \
new-routing-mark=even passthrough=no comment="" disabled=no
/ ip firewall nat
add chain=srcnat connection-mark=odd action=src-nat to-addresses=10.111.0.2 \
to-ports=0-65535 comment="" disabled=no
add chain=srcnat connection-mark=even action=src-nat to-addresses=10.112.0.2 \
to-ports=0-65535 comment="" disabled=no
/ ip route
add dst-address=0.0.0.0/0 gateway=10.111.0.1 scope=255 target-scope=10 routing-mark=odd \
comment="" disabled=no
add dst-address=0.0.0.0/0 gateway=10.112.0.1 scope=255 target-scope=10 routing-mark=even \
comment="" disabled=no
add dst-address=0.0.0.0/0 gateway=10.112.0.1 scope=255 target-scope=10 comment="" \
disabled=no
```

### ***Mangle***

```
/ ip address
add address=192.168.0.1/24 network=192.168.0.0 broadcast=192.168.0.255 interface=Local comment="" \
disabled=no
add address=10.111.0.2/24 network=10.111.0.0 broadcast=10.111.0.255 interface=wlan2 \
comment="" disabled=no
add address=10.112.0.2/24 network=10.112.0.0 broadcast=10.112.0.255 interface=wlan1 \
comment="" disabled=no
```

*router punya 2 upstream (WAN) interfaces dengan ip address 10.111.0.2/24 and 10.112.0.2/24. dan interface LAN dengan nama interface "Local" dan ip address 192.168.0.1/24.*

```
/ ip firewall mangle
```

```
add chain=prerouting in-interface=Local connection-state=new nth=1,1,0 \
action=mark-connection new-connection-mark=odd passthrough=yes comment="" \
disabled=no

add chain=prerouting in-interface=Local connection-mark=odd action=mark-routing \
```



```
new-routing-mark=odd passthrough=no comment="" disabled=no
```

```
add chain=prerouting in-interface=Local connection-state=new nth=1,1,1 \  
action=mark-connection new-connection-mark=even passthrough=yes comment="" \  
disabled=no  
add chain=prerouting in-interface=Local connection-mark=even action=mark-routing \  
new-routing-mark=even passthrough=no comment="" disabled=no
```

## ***NAT***

```
/ ip firewall nat  
add chain=srcnat connection-mark=odd action=src-nat to-addresses=10.111.0.2 \  
to-ports=0-65535 comment="" disabled=no  
add chain=srcnat connection-mark=even action=src-nat to-addresses=10.112.0.2 \  
to-ports=0-65535 comment="" disabled=no
```

## ***Routing***

```
/ ip route  
add dst-address=0.0.0.0/0 gateway=10.111.0.1 scope=255 target-scope=10 routing-mark=odd \  
comment="" disabled=no  
add dst-address=0.0.0.0/0 gateway=10.112.0.1 scope=255 target-scope=10 routing-mark=even \  
comment="" disabled=no  
add dst-address=0.0.0.0/0 gateway=10.112.0.1 scope=255 target-scope=10 comment="" \  
disabled=no comment="gateway for the router itself"
```



*thanks to mbah WIKI yg udah nyedian info*

## # SETUP QUEUE

*mungkin banyak tersebar dimana2 bagaimana cara untuk membatasi BW, tapi kali ini saya mau mencoba memberikan tutorial yg sudah saya uji terlebih dahulu selama 40 jam 30 menit 100 detik dan berfungsi*



*100% dengan sempurna*

oke kita mulai saja=

1. kita bikin/setup mangle dulu =

```
[Kucing@mikrotik] > ip firewall mangle print
```

Flags: X - disabled, I - invalid, D - dynamic

0 UP LOAD

```
chain=prerouting in-interface=LAN
```

```
src-address=xxx.xxx.xxx.xxx/xx action=mark-packet
```

```
new-packet-mark=test-up passthrough=no
```

1 MARK-KONEKSI

```
chain=forward src-address=xxx.xxx.xxx.xxx/xx
```

```
action=mark-connection
```

```
new-connection-mark=test-conn passthrough=yes
```

2 ;;; DOWN DIRECT KONEKSI

```
chain=forward in-interface=WAN
```

```
connection-mark=test-conn action=mark-packet
```

```
new-packet-mark=test-down passthrough=no
```

3 ;;; DOWN VIA PROXY

```
chain=output out-interface=LAN
```

```
dst-address=xxx.xxx.xxx.xxx/xx action=mark-packet
```

```
new-packet-mark=test-down passthrough=no
```

2. Tahap terakhir adalah membuat queue tree=

```
[Kucing@mikrotik] > queue tree pr
```

Flags: X - disabled, I - invalid

```
0 name="download" parent=LAN packet-mark=test-down
```

```
limit-at=32000 queue=default priority=8
```

```
max-limit=32000 burst-limit=0
```

```
burst-threshold=0 burst-time=0s
```

```
1 name="UPLOAD" parent=global-in
```

```
packet-mark=test-up limit-at=32000
```

```
queue=default priority=8
```

```
max-limit=32000 burst-limit=0
```

```
burst-threshold=0 burst-time=0s
```

di sini saya menggunakan queue typenya adalah **PCQ** kenapa, karena **PCQ** bisa secara otomatis membagi



*trafik per client*

## TUTORIAL MISAHIN BW LOKAL DAN INTERNATIONAL

1. Bikin src-address list dengan nama nise

2. atau dengan copy-paste src-address yg di sediain oleh nise

<http://www.datautama.net.id/harijant...utama-nice.php>

copy-paste bisa di lakukan dari putty.exe

3. Bikin mangel / supaya tau itu koneksi & paket nya dateng dari lokal ato international  
/ ip firewall mangle

- add chain=forward src-address-list=nice action=mark-connection \  
new-connection-mark=con-indonesia passthrough=yes comment="mark all \  
indonesia source connection traffic" disabled=no ----> **untuk lokal**

- add chain=forward dst-address-list=nice action=mark-connection \  
new-connection-mark=con-indonesia passthrough=yes comment="mark all \  
indonesia destination connection traffic" disabled=no ----> **untuk lokal**

- add chain=forward src-address-list=!nice action=mark-connection \  
new-connection-mark=con-overseas passthrough=yes comment="mark all \  
overseas source connection traffic" disabled=no ---> **Untuk International**

- add chain=forward dst-address-list=!nice action=mark-connection \  
new-connection-mark=con-overseas passthrough=yes comment="mark all \  
overseas destination connection traffic" disabled=no

- add chain=prerouting connection-mark=con-indonesia action=mark-packet \  
new-packet-mark=indonesia passthrough=yes comment="mark all indonesia \  
traffic" disabled=no ---> **paket lokal**

- add chain=prerouting connection-mark=con-overseas action=mark-packet \  
new-packet-mark=overseas passthrough=yes comment="mark all overseas \  
traffic" disabled=no ----> **paket international**

4. Bikin simple queue =

/ queue simple

- add name="test-indonesia" target-addresses=xxx.xxx.xxx.xxx/xx \  
dst-address=0.0.0.0/0 interface=all parent=none packet-marks=indonesia \  
direction=both priority=8 queue=default/default limit-at=0/0 \  
max-limit=256000/256000 total-queue=default disabled=no ---> **256 UPLOAD & DOWNLOAD (LOKAL)**

- add name="test-overseas" target-addresses=xxx.xxx.xxx.xxx/xx \  
dst-address=0.0.0.0/0 interface=all parent=none packet-marks=overseas \  
direction=both priority=8 queue=default/default limit-at=0/0 \  
max-limit=128000/128000 total-queue=default disabled=no ----> **256 UPLOAD & DOWNLOAD (INTERNATIONAL)**

5. Untuk mengetahui benar ato tidaknya silahkan mengunjungi

<http://www.sijiwae.net/speedtest/> ---> liat di kolom kecepatan koneksi

## TUTORIAL SETING IP-PROXY & CONTOH PENGGUNANNYA (BASIC)

1. Mulai dengan mengkonfigure ip-proxy

```
/ip proxy
enabled: yes
src-address: 0.0.0.0
port: 8080 ---> bisa menggunakan port selain 8080
parent-proxy: 0.0.0.0:0
parent-proxy-port : 3128 ---> kalo ada lebih dari satu proxy
cache-drive: system
cache-administrator: "TESTING"
max-disk-cache-size: none
max-ram-cache-size: none
cache-only-on-disk: no
maximal-client-connections: 1000
maximal-server-connections: 1000
max-object-size: 512KiB
max-fresh-time: 3d
```

2. Sekarang buat supaya proxynya jadi transparan

```
/ip firewall nat
chain=dstnat protocol=tcp dst-port=80 action=redirect to-ports=8080 ---> letakkan setelah masquarade
```

3. Pastiin supaya proxy ente2 ga ada yg pake

```
/ip firewall filter
chain=input in-interface=PUBLIC-INTERFACE src-address=0.0.0.0/0 protocol=tcp dst-port=8080
action=drop
```

4. Contoh untuk memblok suatu site

```
/ip proxy access
dst-host=www.google.com action=deny
bisa juga memblok per ip, dengan memasukan src-address
```

5. Contoh untuk memblok/memberhentikan suatu jenis file

```
/ip proxy access
path=*.exe action=deny
path=*.mp3 action=deny
path=*.zip action=deny
path=*.rar action=deny.
```

6. Contoh lain

```
/ip proxy access
dst-host=:sex action=deny ---> akan memblok semua site yg ada kata SEX
```

Menurut sumber yg ada (*dah kaya wartawan aja*) IP-PROXY itu adalah merupakan proxy yg di buat sendiri oleh orang2 pendiri mikrotik, dan IP-PROXY ini tidak menggunakan engine *SQUID* tapi mencontoh engine *SQUID*. Makanya web-proxy ( *SQUID engine* ) di versi 3 ke atas rencananya mo di apus dan akan di gantikan oleh IP-PROXY sepenuhnya, yg menurut saya itu merupakan terobosan yg sangat luar biasa



walaupun ada sisi jeleknya sedikit .

Bisa di liat contoh2 di atas yg dimana contoh2 di atas ga bisa di lakukan oleh web-proxy ( walaupun menggunakan engine *SQUID* ). Sekali lagi angkat jempol buat para pendiri MIKROTIK

## SETING PPTP SERVER & CLIENT

langkah 1:

1. buka winbox
2. klik interface
3. klik add PPTP client
4. masukkan server address (ip publik mikrotik)
5. user (user yg akan konek ke mikrotik)
6. password (passwordnya)
7. profile (default)
8. allow (centang semua)

langkah 2:

1. buka PPP
2. klik PPTP Server
3. klik enabled
4. authentication (klik smuanya)
5. klik secret
6. klik add
7. masukan name & password
8. service PPTP
9. routes ip lokal gateway (ip lokal si mikrotik)
10. local address (ip pptp server lokal yg bakal di add di ip address, terserah yg penting ip nya blom ada di jaringan)
11. remote address (ip yg bakal di pake untuk meremote di jaringan lokal, terserah juga)

langkah 3:

1. bikin koneksi VPN PPTP di windows

Quote:



ingat...!!!! username & password musti sama di PPTP client (interface) dengan PPP Secret

done....!!!!

semoga bermanfaat, kl mau tau fungsinya apa bisa kok di coba2 googling

## HOWTO: Menghindari Port Scanner dari Hacker

di bagian filter:

Code:

```
/ip firewall filter
add chain=input protocol=tcp psd=21,3s,3,1 action=add-src-to-address-list address-
list="port scanners" address-list-timeout=2w comment="Port scanners to list "
disabled=no
```

Chain ini dipakai untuk mendaftar ip ke black-list address list

Chain selanjutnya untuk mendeteksi apakah ada indikasi aktifitas port scanner:

Code:

```
add chain=input protocol=tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg
action=add-src-to-address-list address-list="port scanners"
address-list-timeout=2w comment="NMAP FIN Stealth scan"

add chain=input protocol=tcp tcp-flags=fin,syn
action=add-src-to-address-list address-list="port scanners"
address-list-timeout=2w comment="SYN/FIN scan"

add chain=input protocol=tcp tcp-flags=syn,rst
action=add-src-to-address-list address-list="port scanners"
address-list-timeout=2w comment="SYN/RST scan"

add chain=input protocol=tcp tcp-flags=fin,psh,urg,!syn,!rst,!ack
action=add-src-to-address-list address-list="port scanners"
address-list-timeout=2w comment="FIN/PSH/URG scan"

add chain=input protocol=tcp tcp-flags=fin,syn,rst,psh,ack,urg
action=add-src-to-address-list address-list="port scanners"
address-list-timeout=2w comment="ALL/ALL scan"

add chain=input protocol=tcp tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg
action=add-src-to-address-list address-list="port scanners"
address-list-timeout=2w comment="NMAP NULL scan"
```

jika ada tanda tanda dari kejadian di atas, maka harus didrop scanning IPnya pakai perintah ini:

Code:

```
add chain=input src-address-list="port scanners" action=drop comment="dropping port
scanners" disabled=no
```

sumber:

HTML Code:

```
http://wiki.mikrotik.com/wiki/Drop\_port\_scanners
```

## Wireless Bridge (client) dengan AP tanpa WDS

Bersyukur sekali karena Mikrotik, selalu melakukan upgrade operating system-nya dengan mengakomodasi kebutuhan atau mungkin keluhan penggunaannya.

Mungkin msh ada temen2 disana yang pernah mengalami kesulitan seperti pernah saya alami, yaitu wireless bridging mikrotik dengan AP tanpa fasilitas WDS, untuk itulah saya membuat tutor ini sekaligus sarana belajar menulis di forum ini.

Langkah-langkah untuk membuat koneksi Wireless Bridge pada mikrotik sbb:

1. Untuk anda yang msh menggunakan RBxxx dengan MT v2.9.x silahkan upgrade dengan versi terbaru v3.10 bisa download di [www.mikrotik.co.id](http://www.mikrotik.co.id), cara upgrade tinggal drag n drop pada Files di winbox.
2. Set wlan1 pada mode station pseudobridge, trus tentukan channel, tentukan SSID atau scan en connect pada AP yang diinginkan.
3. Buat (add) interface bridge1, dan masukan wlan1 dan ether1 pada tab port bridge1.
4. Buat (add) IP pada interface bridge1 se-subnet dengan IP-nya AP.
5. Untuk test, silahkan sambungkan PC dengan pada ether1, set IP satu subnet dengan AP, lalu ping AP atau gateway, insaallah tembusss...

## Setting Point To Multi Point

### Konfigurasi pada wireless Access Point

1. Buatlah sebuah Interface bridge yang baru, berilah nama wds bridge atau terserah anda namanya
  2. Masukkan ethernet dan wlan ke dalam interface port bridge
  3. Selanjutnya adalah setting wireless interface. Kliklah pada menu wireless. (1). pilih pada tab Security Profiles (2). Cek list WPA PSK pada Authentication Types (3). cel list juga tkip, aes ccm pada Unicast Ciphers dan Group Ciphers (4) Isikan password pada WPA Pre-Shares Key (5) klik Apply OK
  4. Selanjutnya klik tab Connect list (1). pada interface pilihlah wlan yang akan digunakan (2). tentukan ssid (3) dan pada Security Profile arahkan ke profile1 (4) klik Apply OK
  5. dan selanjutnya (1) klik tab interface (2) double klik pada nama wireless yang akan digunakan (3). pilihlah mode ap bridge (4). tentukan ssid seperti pada security profile tadi (5). band (6). dan frequency yang digunakan (7). pada Security Profile tujukan ke profile1 (8). dan pada Frequency Mode tujukan ke manual txpower (9). jangan lupa aktifkan Default Authentication dan Default Forward (10) lalu aktifkan interface wirelessnya (11) klik apply OK
  6. Berikutnya konfigurasi wds pada wireless interface yang digunakan, bukalah kembali konfigurasi wireless seperti langkah terdahulu. (1). pilihlah tab wds (2) tentukanlah WDS Mode ke dynamic (3). pilihlah wds-bridge pada WDS Default Bridge (4) klik Apply OK
- nah seting access point nya udah kelar, tinggal seting wireless stationnya tapi saya belum edit gambar untuk wireless stationnya, tapi pada dasarnya setting stationnya sama seperti access point cuma mode di tentukan ke station wds dan frequency mode ke super channel nah tinggal scan, di tabel akan terlihat ssid access point yg kita buat klik connect klik ok udah sep.....kan semoga bermanfaat. untuk melihat gambarnya <http://www.warnet-cinta.blogspot.com>

## Pengamanan Mikrotik dari Scan Winbox dan Neighbour

Kadang kala para ISP atau penyedia jasa layanan tidak terlalu jeli untuk melindungi customernya. Terutama ketika melindungi router pelanggan yang menggunakan Mikrotik RouterOS(tm). Dengan menjalankan IP >> Neighbor kita bisa melihat router mikrotik lainnya yang secara fisik terhubung dengan router kita melalui jaringan di provider kita.

Untuk itu kita bisa melindunginya dengan berbagai cara misalnya memblok scan dari winbox dan neighbor kita. Berikut adalah cara yang paling mudah :

Code:

```
admin@mikrotik] interface bridge> filter print
Flags: X - disabled, I - invalid, D - dynamic
0 ;;; block discovery mikrotik
chain=forward in-interface=ether1 mac-protocol=ip dst-port=5678
ip-protocol=udp action=drop
1 ;;; block discovery mikrotik
chain=input in-interface=ether1 mac-protocol=ip dst-port=5678
ip-protocol=udp action=drop
2 ;;; block discovery mikrotik
chain=output mac-protocol=ip dst-port=5678 ip-protocol=udp action=drop
3 ;;; block discovery mikrotik
chain=input in-interface=ether1 mac-protocol=ip dst-port=8291
ip-protocol=tcp action=drop
4 ;;; block winbox mikrotik
chain=forward in-interface=ether1 mac-protocol=ip dst-port=8291
ip-protocol=tcp action=drop
5 ;;; block request DHCP
chain=input mac-protocol=ip dst-port=68 ip-protocol=udp action=drop
6 ;;; block request DHCP
chain=forward mac-protocol=ip dst-port=68 ip-protocol=udp action=drop
7 ;;; block request DHCP
chain=output mac-protocol=ip dst-port=68 ip-protocol=udp action=drop
```

Dengan perintah tersebut kita bisa menutup beberapa scan terutama yang menggunakan winbox dan ip neighbor. Port diatas adalah bagian dari share Mikrotik RouterOS yang memang di perlukan untuk monitoring.

Sumber: <http://tutorial.multisolusi.com>



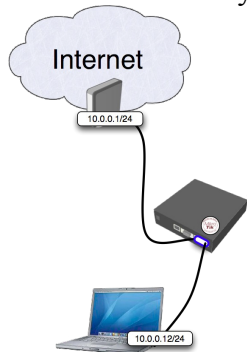
Maap klo udah ada yang posting, bagi yang belum tau aja



## Transparent Traffic Shaper

### Pendahuluan

Contoh kali ini akan memperlihatkan bagaimana cara mengkonfigurasi Transparent Traffic Shaper. Transparent Traffic Shaper pada dasarnya adalah bridge yang dapat membedakan dan memprioritaskan traffic data yang melewatinya. Lihat Network Layout dibawah ini :



Kita akan mengkonfigurasi 1 (satu) queue yang membatasi total throughput ke client dan 3 (tiga) sub-queues yang akan membatasi HTTP, P2P dan traffic lainnya secara terpisah. Traffic HTTP akan mendapatkan prioritas diatas traffic lainnya.

### Konfigurasi

Konfigurasi yang akan digunakan adalah

Code:

```
/ interface bridge
add name="bridge1"
/ interface bridge port
add interface=ether2 bridge=bridge1
add interface=ether3 bridge=bridge1

/ ip firewall mangle
add chain=prerouting protocol=tcp dst-port=80 action=mark-connection \
    new-connection-mark=http_conn passthrough=yes
add chain=prerouting connection-mark=http_conn action=mark-packet \
    new-packet-mark=http passthrough=no
add chain=prerouting p2p=all-p2p action=mark-connection \
    new-connection-mark=p2p_conn passthrough=yes
add chain=prerouting connection-mark=p2p_conn action=mark-packet \
    new-packet-mark=p2p passthrough=no
add chain=prerouting action=mark-connection new-connection-mark=other_conn \
    passthrough=yes
add chain=prerouting connection-mark=other_conn action=mark-packet \
    new-packet-mark=other passthrough=no

/ queue simple
add name="main" target-addresses=10.0.0.12/32 max-limit=256000/512000
add name="http" parent=main packet-marks=http max-limit=240000/500000
add name="p2p" parent=main packet-marks=p2p max-limit=64000/64000
add name="other" parent=main packet-marks=other max-limit=128000/128000
```

### Penjelasan

Dibawah ini kita akan mencoba melihat kode-kode tersebut perbagian.

**Bridge :** Code:

```
/ interface bridge
add name="bridge1"
/ interface bridge port
add interface=ether2 bridge=bridge1
add interface=ether3 bridge=bridge1
```

Kita membuat satu interface Bridge dan meng-assign 2 (dua) interface ethernet ke interface Bridge tersebut. Oleh karena ini, maka traffic shaper yang akan dijalankan akan sepenuhnya transparan oleh klien.

**Mangle : Code:**

```
/ ip firewall mangle
add chain=prerouting protocol=tcp dst-port=80 action=mark-connection \
    new-connection-mark=http_conn passthrough=yes
add chain=prerouting connection-mark=http_conn action=mark-packet \
    new-packet-mark=http passthrough=no
```

Seluruh traffic yang menuju ke TCP Port 80 kemungkinan besar adalah traffic HTTP dan oleh karena itu akan ditandai dengan packet mark **http**. Perhatikan, pada rule pertama terdapat **passthrough=yes** sementara pada rule kedua terdapat **passthrough=no**.

**Code:**

```
/ ip firewall mangle
add chain=prerouting p2p=all-p2p action=mark-connection \
    new-connection-mark=p2p_conn passthrough=yes
add chain=prerouting connection-mark=p2p_conn action=mark-packet \
    new-packet-mark=p2p passthrough=no
add chain=prerouting action=mark-connection new-connection-mark=other_conn \
    passthrough=yes
add chain=prerouting connection-mark=other_conn action=mark-packet \
    new-packet-mark=other passthrough=no
```

Sama dengan diatas, traffic P2P ditandai dengan packet mark **p2p** dan traffic lainnya ditandai dengan packet mark **other**.

**Queues : Code:**

```
/ queue simple
add name="main" target-addresses=10.0.0.12/32 max-limit=256000/512000
```

Kita membuat queue yang membatasi seluruh traffic yang akan menuju / datang dari klien (spesifik di **target-address**) sebesar 256k/512k

**Code:**

```
/ queue simple
add name="http" parent=main packet-marks=http max-limit=240000/500000
add name="p2p" parent=main packet-marks=p2p max-limit=64000/64000
add name="other" parent=main packet-marks=other max-limit=128000/128000
```

All sub-queues have the main queue as the parent, thus the aggregate data rate could not exceed limits specified in the main queue. Note, that http queue has higher priority than other queues, meaning that HTTP downloads are prioritized.

Seluruh sub-queues memiliki **main** sebagai parent-nya, oleh karena itu seluruh data rate tidak dapat melampaui batas yang telah dispesifikasikan pada queue **main**. Perhatikan bahwa queue **http** memiliki prioritas lebih besar dari queue lainnya, berarti bahwa HTTP Downloads akan lebih diprioritaskan.

## Pengamanan Mikrotik dari Scan Winbox dan Neighbour

Kadang kala para ISP atau penyedia jasa layanan tidak terlalu jeli untuk melindungi customernya. Terutama ketika melindungi router pelanggan yang menggunakan Mikrotik RouterOS(tm). Dengan menjalankan IP >> Neighbor kita bisa melihat router mikrotik lainnya yang secara fisik terhubung dengan router kita melalui jaringan di provider kita.

Untuk itu kita bisa melindunginya dengan berbagai cara misalnya memblok scan dari winbox dan neighbor kita. Berikut adalah cara yang paling mudah :

Code:

```
admin@mikrotik] interface bridge> filter print
Flags: X - disabled, I - invalid, D - dynamic
0 ;;; block discovery mikrotik
chain=forward in-interface=ether1 mac-protocol=ip dst-port=5678
ip-protocol=udp action=drop
1 ;;; block discovery mikrotik
chain=input in-interface=ether1 mac-protocol=ip dst-port=5678
ip-protocol=udp action=drop
2 ;;; block discovery mikrotik
chain=output mac-protocol=ip dst-port=5678 ip-protocol=udp action=drop
3 ;;; block discovery mikrotik
chain=input in-interface=ether1 mac-protocol=ip dst-port=8291
ip-protocol=tcp action=drop
4 ;;; block winbox mikrotik
chain=forward in-interface=ether1 mac-protocol=ip dst-port=8291
ip-protocol=tcp action=drop
5 ;;; block request DHCP
chain=input mac-protocol=ip dst-port=68 ip-protocol=udp action=drop
6 ;;; block request DHCP
chain=forward mac-protocol=ip dst-port=68 ip-protocol=udp action=drop
7 ;;; block request DHCP
chain=output mac-protocol=ip dst-port=68 ip-protocol=udp action=drop
```

Dengan perintah tersebut kita bisa menutup beberapa scan terutama yang menggunakan winbox dan ip neighbor. Port diatas adalah bagian dari share Mikrotik RouterOS yang memang di perlukan untuk monitoring.

Sumber: <http://tutorial.multisolusi.com>



Maap klo udah ada yang posting, bagi yang belum tau aja

## Script Bikin Queues Tree B/W Limiter

maap baru gabung, ni coba posting script bikin queues tree buat B/W limiter. semoga bermanfaat.

1. bikin mangle ya dulu, pake script seperti di bawah. (range IP 2 s/d 11)

```
:for e from 2 to 11 do={
/ip firewall mangle add chain=prerouting src-address=(192.168.224. . $e) action=mark-connection new-connection-mark=($e . indosatcon )
/ip firewall mangle add chain=prerouting connection-mark=($e . indosatcon ) protocol=!1 action=mark-packet new-packet-mark=($e . indosatflow ) passthrough=no
}
```

2. trus bikin queues nya, seperti ini.

```
:for e from 2 to 11 do={
/queue tree add name=("STREAM-DOWN-" . $e) parent=STREAM-DOWN packet-mark=($e . indosatflow)
/queue tree add name=("STREAM-UP-" . $e) parent=STREAM-UP packet-mark=($e . indosatflow)
}
```

tinggal copy paste di terminal nya... enter...

1. kita bikin queue di queue tree dengan name=STREAM-DOWN untuk parrent=global-in
2. bikin lagi queue di queue tree dengan name=STREAM-UP untuk parrent=global-out
- 3.membuat mangle pada /ip firewall. dengan menjalankan script seperti di bawah pada **terminal**

untuk mikrotik v 2.9.xx

```
:for e from 2 to 11 do={
/ip firewall mangle add chain=prerouting src-address=(192.168.224. . $e) action=mark-connection new-connection-mark=($e . indosatcon )
/ip firewall mangle add chain=prerouting connection-mark=($e . indosatcon ) protocol=!1 action=mark-packet new-packet-mark=($e . indosatflow ) passthrough=no
}
```

untuk mikrotik v 3.x

```
:for e from=2 to=11 do={
/ip firewall mangle add chain=prerouting src-address="192.168.224.$e" action=mark-connection new-connection-mark="$e. indosatcon"
/ip firewall mangle add chain=prerouting connection-mark="$e. indosatcon" protocol=!1 action=mark-packet new-packet-mark="$e. indosatflow" passthrough=no
}
```

cek pada /ip firewall mangle memastikan bahwa script nya berjalan.

4. kemudian kita buat queue tree nya dengan menjalan kan script seperti di bawah.

untuk mikrotik v 2.9.xx

```
:for e from 2 to 11 do={
/queue tree add name=("STREAM-DOWN-" . $e) parent=STREAM-DOWN packet-mark=($e. indosatflow)
```

```
/queue tree add name=( "STREAM-UP-" . $e) parent=STREAM-UP packet-mark=($e. indosatflow)
}
```

untuk mikrotik v 3.xx

```
:for e from=2 to=20 do={
/queue tree add name="STREAM-DOWN-.$e" parent=STREAM-DOWN packet-mark="$e.
indosatflow"
/queue tree add name="STREAM-UP-. $e" parent=STREAM-UP packet-mark="$e. indosatflow"
}
```

cek juga pada queue tree nya apa kah sudah ada list queue nya.

5. coba melimit salah satu ip dan amati... apakah sudah benar berjalan.

supaya ip lokal tidak bisa internet

BLOCKING IP  
Setting dengan WinBox  
New Terminal >

```
SCRIPT 1
# Start of Script1
/ip firewall filter add chain=forward src-address=192.168.1.0/24 action=jump jump-target=BlockingIP
comment="BlockingIP 192.168.1.x"
# End of Script1
```

```
SCRIPT 2
# Start of Script2
:for e from 1 to 254 do={
/ip firewall filter add chain=BlockingIP src-address=(192.168.1 . . $e) action=reject \ comment=($e)
}
/ip firewall filter add chain=BlockingIP action=return comment="Return the packet"
# End of Script2
```

1. a. Menu ip > firewall > filter rules
  - b. liat bagian chain Forward
  - c. Cari rule dengan comment "BlockingIP 192.168.1.x"
  - d. Drag Drop Rule itu ke paling atas
  2. a. Menu ip > firewall > filter rules
  - b. liat bagian chain BlockingIP
  - c. ada comment 1-254
  - d. tinggal disable atau enable aja...
    - disable berarti gak di block
    - enable berarti di block
  - e. Rule yang paling bawah.. dengan Comment "Return the packet"
- HARUS SELALU ENABLE

## Update Otomatis nice.rsc

Sudah beberapa tahun terakhir, banyak pengguna Mikrotik di Indonesia yang melakukan routing dan pengaturan bandwidth menggunakan dasar IP Address List NICE. Di website Mikrotik Indonesia, disediakan script nice.rsc ini yang terupdate secara rutin setiap hari, yang datanya langsung bersumber dari BGP Router OIXP dan IIX2-JKT. Data tersebut juga sudah dinormalisasi dan dicek over-subnet nya sehingga tidak akan menimbulkan error saat diimport dan lebih menghemat resources karena jumlah barisnya hanya 1/5 dari data yang asli.

Dengan keluarnya Mikrotik RouterOS versi 3.0, sekarang kita bisa update otomatis pada script nice-rsc ini.

Yang perlu kita lakukan hanya membuat scheduler dan script seperti berikut.

```
/system scheduler
add comment=update-nice disabled=no interval=1d name=update-nice-rsc on-event=":if
([:len [/file find name=nice.rsc\
]] > 0) do={ /file remove nice.rsc }; /tool fetch address=ixp.mikrotik.co.id
path=/download/nice.rsc;/import ni\
ce.rsc" start-date=jan/01/2008 start-time=00:06:00
```

Script di atas akan dilakukan 1 kali setiap 24 jam setiap pukul 6 pagi.

---

Ini hasil eksperimen hari ini supaya daftar nice di mikrotik bisa terupdate lewat script.

NB: tapi autodownload dari link mikrotik.co.id belum bisa. karena gue baca betul betul dari quote:

Quote:

Proses upload ini dapat juga dilakukan secara otomatis jika Anda memiliki pengetahuan scripting. Misalnya Anda membuat shell script pada Linux untuk melakukan download secara otomatis dan mengupload file secara otomatis setiap pk 06.00 pagi. Kemudian Anda tinggal membuat scheduler pada router untuk melakukan import file.

ini kayanya harus dari luar mikrotik box (lewat linux-box, yg mungkin bisa dari squidbox yg online 24jam terus)

Script:

```
/ip sys scr pr
name="scriptdelnice" owner="admin"
policy=ftp,reboot,read,write,policy,test,winbox,pa ssword
last-started=jul/09/2007 10:19:59 run-count=1
source=
/ip firewall address-list remove [find list="nice"]
name="scriptimpnice" owner="admin"
policy=ftp,reboot,read,write,policy,test,winbox,pa ssword
last-started=jul/09/2007 10:19:59 run-count=1
source=
/import nice.rsc
```

Schedule:

```
# NAME ON-EVENT START-DATE START-TIME INTERVAL RUN-COUNT
4 schdelnice scriptdelnice apr/16/2007 06:05:00 1d 0
4 schimpnice scriptimpnice apr/16/2007 06:05:05 1d 0
```

gue bagi 2 scriptnya supaya mikrotik ada delay 5 detik menghapus daftar nice yang panjang, lalu

mengimport lagi filenya. (kalo diupdate langsung tanpa meremove daftar sebelumnya bisa apa enggak gue lum tau) eksperimen sendiri yah ^^, kalau ada script lebih bagus di revisi dibawah boleh2 aja.

mungkin rekan2 laen bisa menambahkan script di linux biar bisa donlot halaman web terus disimpan ke file nice.rsc, lalu upload lewat ftp ke mikrotik box

karena sampai sini gue ga paham betul script linux. (pake mikrotik aja barusan 6 bulan gara2 provider ngasi mikrotik, kalo ga gue ga belajar mikrotik hihihihhi).

### [How-to] Auto Update Address-List IIX di Router Mikrotik

How to sederhana mengenai bagaimana melakukan auto update address-list IIX di Router mikrotik dengan bantuan sebuah mesin linux yang melakukan download dan upload otomatis, meskipun rada cupu semoga bisa berguna;

Sebelumnya di tulis di [blog saya](#) dan di [Forum RTRW](#)

Berikut adalah metode sederhana yang saya lakukan untuk melakukan auto update address-list IIX yang saya perlukan dalam melakukan mangling untuk kemudian digunakan oleh queue pada Router yang menggunakan Mikrotik RouterOS.

Untuk proses download dan upload otomatis saya menggunakan sebuah mesin linux yang juga melayani fungsi web server untuk keperluan internal.

Secara garis besar yang dilakukan terbagi ke dalam 4 langkah sebagai berikut;

**1. Download otomatis**, dengan menggunakan cron dan wget linuxbox mendownload file yang berisikan script address-list iix secara otomatis pada waktu-waktu tertentu, dalam hal ini file yang di download adalah nice.rsc dari <http://ixp.mikrotik.co.id/download/nice.rsc>, waktu download adalah setiap hari pada pukul 05.00 pagi. Di RouterOS 3.0rcx ada tool yang berjudul fetch, meskipun saya belum bisa menggunakannya sepertinya ini adalah tool untuk mengambil file otomatis dari web server, sehingga besar kemungkinan proses auto update ini nantinya bisa dilakukan sendiri oleh Mikrotik RouterOS tanpa bantuan dari sebuah mesin linux.

Fullpath ke wget;

Code:

```
vinson:/# which wget
/usr/bin/wget
```

Perintah wget;

Code:

```
/usr/bin/wget -q http://ixp.mikrotik.co.id/download/nice.rsc -O
/path/ke/direktori/lokal/nice.rsc
```

-q untuk mematikan verbose perintah wget

-O untuk menyimpan file yang di download ke dalam direktori tertentu

Masukkan ke dalam crontab;

Code:

```
#touch croniix.txt
```

Masukkan perintah cron ke dalam file tersebut dengan menggunakan text editor favorit anda; Sesuaikan /path/ke/direktori/lokal/ dengan full path ke direktori lokal yang anda gunakan.

Code:

```
0 5 * * * /usr/bin/wget -q http://ixp.mikrotik.co.id/download/nice.rsc -O
/path/ke/direktori/lokal/nice.rsc
```

Masukkan cron tersebut ke dalam crontab;

Code:

```
# crontab croniix.txt
```

Pastikan bahwa cron tersebut sudah masuk dan aktif;

Code:

```
# crontab -l
```

**2. Kemudian lakukan penyesuaian isi file nice.rsc** sesuai dengan kebutuhan kita. Dalam kasus saya adalah mengganti nama address-list=nice menjadi address-list=iix-ip melalui perl dan menghapus baris yang berisi komentar (#) (untuk tujuan penyederhanaan - bukan untuk menghilangkan nama pembuat script yang sudah kita ketahui bersama dibuat oleh Om Valens Riyadi Valens Riyadi @ [www.mikrotik.co.id](http://www.mikrotik.co.id)), juga menghapus baris yang berisi perintah /sys note. Hal ini dilakukan dengan menggunakan perintah sed yang disatukan ke dalam sebuah batch file. Sesuaikan nama address-list IIX dengan nama list yang anda gunakan di router anda.

Buat file script yang akan dijalankan untuk melakukan modifikasi

Code:

```
# touch modifnice.batch
# chmod 0777 modifnice.batch
```

Masukkan baris berikut ke dalam file script tersebut;

Code:

```
# Untuk melakukan modifikasi terhadap nice.rsc

# menghapus baris 1-10 yang berisikan komentar dan /sys note dari file nice.rsc dan
menyimpan hasilnya di dalam file iix-ip.rsc
sed -e '1,10d' /path/ke/direktori/lokal/nice.rsc > /path/ke/direktori/lokal/iix-
ip.rsc

# merubah address-list=nice menjadi address-list=iix-ip
perl -pi -e "s/nice/iix-ip/g;" /path/ke/direktori/lokal/iix-ip.rsc
```

**3. Mengupload file tersebut ke router-router mikrotik** yang ingin kita update secara otomatis address-list IIX nya, terlebih dahulu di masing-masing router kita buat sebuah group yang hanya memiliki privilege untuk melakukan ftp ke router tersebut dan membuat user terkait dengan grup tersebut serta menentukan password aksesnya. Hal ini dilakukan melalui perintah ncftpput.

Tambahkan baris berikut ke dalam batch file yang telah kita buat sebelumnya;

Code:

```
# mengupload file iix-ip.rsc ke router-router yang kita inginkan
# masukkan ip router, username, dan password
ncftpput -b -u username -p password 117.xxx.xxx.38 / /path/ke/direktori/lokal/iix-
ip.rsc
```



```
ncftpput -b -u username -p password 117.xxx.xxx.14 / /path/ke/direktori/lokal/iix-  
ip.rsc  
ncftpput -b -u username -p password 117.xxx.xxx.34 / /path/ke/direktori/lokal/iix-  
ip.rsc  
ncftpput -b -u username -p password 10.xxx.xxx.3 / /path/ke/direktori/lokal/iix-  
ip.rsc  
ncftpput -b -u username -p password 117.xxx.xxx.19 / /path/ke/direktori/lokal/iix-  
ip.rsc
```

Rubah IP Address, username, dan password sesuai dengan username, password dan IP Address router anda, sebaiknya dibuat username terpisah yang hanya memiliki privilege ftp.

Tambahkan file batch ke dalam crontab, melalui baris di croniix.txt

Code:

```
30 5 * * * /path/ke/direktori/lokal/modifniece.batch
```

Aktifkan crontab

Code:

```
#crontab croniix.txt
```

File batch modifniece.batch akan dijalankan pukul 05:30 setiap hari.

Buat user di Router mikrotik untuk keperluan upload ftp dari mesin linux;

Buat group ftponly

Code:

```
/ user group  
add name="ftponly" policy=ftp,!local,!telnet,!ssh,!reboot,!read,!write,!policy,!  
test,!winbox,!password,!web  
/ user  
add name="username" group=ftponly address=0.0.0.0/0 comment="" disabled=no
```

Berikan password untuk user "username";

Buka service FTP di setiap router dan pastikan tidak ada rule firewall yang menghalangi koneksi pada port 21

Code:

```
/ ip service  
set ftp port=21 address=0.0.0.0/0 disabled=no
```

Memastikan bahwa koneksi ftp pada port tersebut bisa dilakukan melalui telnet

Code:

```
# telnet 117.xxx.xxx.34 21  
Trying 117.xxx.xxx.34...  
Connected to 117.xxx.xxx.34.  
Escape character is '^]'.  
220 rt.distrib.dursaw.netsol FTP server (MikroTik 3.0rc13) ready
```

**4. Membuat schedule di masing-masing router mikrotik** untuk menjalankan script yang sudah diupload sebelumnya dan menghapus file tersebut setelah script dijalankan dengan menggunakan scheduler.

Buat script untuk melakukan import dan melakukan penghapusan dan kemudian buat system scheduler untuk menjalankan kedua script tersebut dengan jeda waktu 30 menit;

Code:

```
/ system script
```

```
add name="import-iix-ip" source="/import iix-ip.rsc"
policy=ftp,reboot,read,write,policy,test,winbox,password
add name="rem-iix-ip" source="/file rem iix-ip.rsc"
policy=ftp,reboot,read,write,policy,test,winbox,password
/ system scheduler
add name="UpdateIIX" on-event=import-iix-ip start-date=jan/13/2008 start-
time=06:30:00 interval=1d comment="" disabled=no
add name="Remove-Addr" on-event=rem-iix-ip start-date=jan/13/2008 start-
time=07:00:00 interval=1d comment="" disabled=no
```

Hal yang perlu diperhatikan adalah sinkronisasi waktu antar server dan router-router terkait apabila kita menginginkan proses autoupdate terjadi tepat pada waktu yang kita inginkan.

## Referensi:

Sumber nice.rsc <http://mikrotik.co.id>

[Mengenai Cron](#)

[Mengenai modifikasi isi file dengan perl secara sederhana](#)

[Mengenai ncftpput](#)

HASIL KHUSUS :

**/tool fetch address=ixp.mikrotik.co.id src-path=/download/nice.rsc**

**/import nice.rsc**

**:log info "Update route to IIX done"**

## [Share] Script u/ membatasi BW jika suatu traffic client melewati batas tertentu

Misalkan kita punya script simple queue seperti bawah ini:

Code:

```
add name="Isp" target-addresses=192.111.111.99/32 dst-address=0.0.0.0/0 \  
  interface=all parent=none direction=both priority=8 \  
  queue=default-small/share-ni-down limit-at=0/0 max-limit=32000/64000 \  
  burst-limit=/128000 burst-threshold=/30000 burst-time=/10s \  
  total-queue=default-small disabled=no
```

dan kita menginginkan membatasi bandwidth-nya jika traffiknya sudah melewati misalkan 500MB dalam satu hari, maka kita bisa membuat script dibawah ini:

Code:

```
add name="trafwatcher01" source="  
/queue simple  
:local traf;  
:set traf [get [find name="Isp"] total-bytes]  
:if ($traf > 500000000) do = {  
set [find name="Isp"] max-limit= 32000/32000  
:log info "isp traffic exceeding 500MB"}  
policy=ftp,reboot,read,write,policy,test,winbox,password
```

variabel traf fungsinya untuk menampung sementara nilai total traffic

buat scheduler untuk mengecek traffic script-nya, misalnya dibuat setiap 1/2 jam untuk mengeceknya.

Code:

```
add name="trafisp" on-event=trafwatcher01 start-date=jan/01/1970 \  
  start-time=11:00:00 interval=30m comment="" disabled=no
```

nah itu untuk script untuk membatasinya, tinggal membuat script satu lagi jika sudah melewati satu hari (misal jam 12 malam), counternya mereset total traffic queue client tsb dan mereset bandwidthnya normal ke 64 kbps lagi.

GOODLUCK

sumber: wiki dan howto-script mikrotik

## Advanced Script 1

Biar lebih sip gue utak atik lagi scriptnya, jadi 2 tingkat ato bahkan bisa lebih.

Pelajari aja code bawah ini:

Code:

```
/queue simple  
:local traf;  
:local maxi;  
:set traf [get [find name="Isp"] total-bytes]  
:set maxi [get [find name="Isp"] max-limit]  
:if ($traf < 100000000 && $maxi != "64000/96000") do = {  
set [find name="Isp"] max-limit= "64000/96000"}  
:if ($traf > 100000000 && $maxi != "64000/64000") do = {  
set [find name="Isp"] max-limit= "64000/64000"}  
:if ($traf > 1000000000 && $maxi != "64000/32000") do = {  
set [find name="Isp"] max-limit= "32000/32000"}  
/sys sched disa [find name="isp-trafwatcher"]}
```

Penjelasan:

Gue buat 2 tingkat bandwidth limiternya jadi dibawah 10MB masih sesuai limit awal, 10 - 100 MB turun jadi 64k, atas 100MB jadi 32k

biar script ngga ngulang ngulang terus di log-nya dibuat satu variabel lagi yaitu variabel maxi yang menampung setting bandwidthnya, kalo tidak sama dengan logika-nya maka que simple ga di set ulang.

di script terakhir ditambahin buat mendisable schedulernya biar scheduler ga jalan terus ( di disable).

nah biar enable lagi, perlu dibuat satu script lagi untuk men-clear counter traffiknya dan meng-enable lagi schedulernya, misalnya tiap jam 00:00

script buat enable lagi en autoclear counter. kasi nama script bebas, abis itu buat juga schedulernya

Code:

```
/ip fire filt reset-counters-all
/que tree reset-counters-all
/que sim reset-counters-all
/sys sched ena [find name="isp-trafwatcher"]
```

## Advanced Script 2

Nah kalo script di atas itu cuman deteksi traffic upload sama donlot (total trafik )

nah misalnya kita ingin melimit kalo donlotnya saja jika melebihi batas tertentu, maka kita bisa memakai built-in variable bytes.

masalahnya..... di variable bytes tersebut jika di ambil, formatnya berupa upload/download, contoh: 1000/3000

nah bagaimana caranya kita mengambil angka 3000 ini.... kita bisa menggunakan command :find , :pick dan :len ---> lebih jauh lihat sini <http://www.mikrotik.com/testdocs/ros.../scripting.php>

Code:

```
/queue simple
:local traf;
:local down;
:local maxi;
:set traf [get [find name="Isp"] bytes]
:set down [:pick $traf ([:find $traf /]+1) [:len $traf]]
:set maxi [get [find name="Isp"] max-limit]
:if ($down < 15000000 && $maxi != "0/96000") do = {
set [find name="Isp"] max-limit= "0/96000"}
:if ($down > 15000000 && $maxi != "0/72000") do = {
set [find name="Isp"] max-limit= "0/72000"}
:if ($down > 100000000 && $maxi != "0/64000") do = {
set [find name="Isp"] max-limit= "64000/64000"}
/sys sched disa [find name="isp-trafwatcher"]}
```

NB:

untuk upload tinggal di ganti aja script ini

**:set down [:pick \$traf ([:find \$traf /]+1) [:len \$traf]]** menjadi: **:set down [:pick \$traf 0 ([:find \$traf /]-1)]**

# Hotspot Mikrotik

Begitu mudahnya untuk menggunakan mikrotik. Konsep networking yang sudah anda pahami akan sangat mudah di implementasikan di operating sistem router yang berbasis kepada linux kernel ini. Kali ini kita akan praktekkan sebuah judul yang banyak di nanti orang banyak. Judul yang di ambil adalah, membuat hotspot dan user manager dengan router yang sama.

Langkah pertama adalah sbb :

1. Buat sebuah server Radius

```
/ radius add service=hotspot address=127.0.0.1 secret=123456
```

2. Buat profile dan set profile tersebut untuk menggunakan Radius Server

```
/ ip hotspot profile set hspofl use-radius=yes
```

3. Membuat scriber

```
/ tool user-manager customer add login="MikroTik" password="qwerty" permissions=owner
```

4. Tambahkan Router kita dalam hal ini localhost.

```
/ tool user-manager router add subscriber=MikroTik ip-address=127.0.0.1 shared-secret=123456
```

5. Lalu silahkan browser ke <http://routeranda/userman>

## Centralized Authentication for Hotspot user

### From MikroTik Wiki

Jump to: [navigation](#), [search](#)

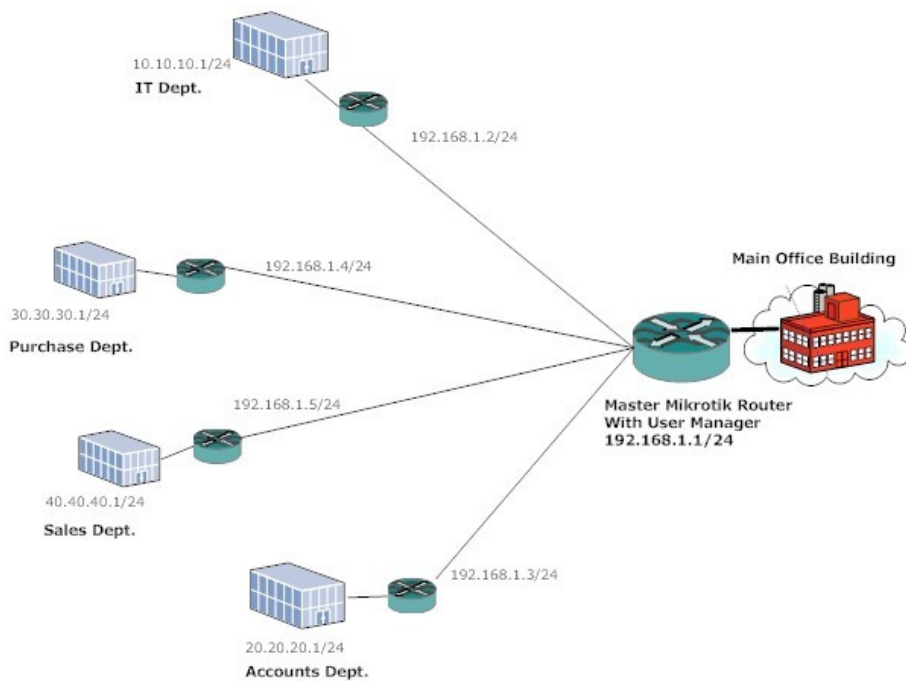
Generally we are using external Radius servers for user authentication as MikroTik is not Radius server. But here in this example we use the MikroTik User Manager which works as a Radius server and does authentication and control of your Hotspot users.

### [\[edit\]](#) Requirements

**Central location:** MikroTik OS with User Manager ([suggested License is L6](#)).

**Hotspot:** Mikrotik Routerboard with at least a L4 License

**Network** 192.168.1.0/24



R1-Hotspot Master  
 WAN IP- <Connected to Internet>  
 LAN IP - 192.168.1.1/24

R2-Hotspot IT Dept  
 WAN IP - 192.168.1.2/24  
 LAN IP - 10.10.10.1/24

R3-Hotspot Account Dept.  
 WAN IP - 192.168.1.3/24  
 LAN IP - 20.20.20.1/24

R4- Hotspot Purchase Dept  
 WAN IP - 192.168.1.4/24  
 LAN IP - 30.30.30.1/24

R5- Hotspot Sales Dept.  
 WAN IP - 192.168.1.5/24  
 LAN IP - 40.40.40.1/24

We assume that all the setup is ready and the hotspot is configured on R2, R3, R4, and R5 with local authentication.

First, we will configure R2, R3, R4 & R5 to use MikroTik user manager as a Radius server.

```
/ip hotspot profile
use-radius=yes
```

```
/radius add
service=hotspot address=192.168.1.1 secret=123456
```

This configuration will apply to all the Hotspot router.

Now, we will configure R1-Hotspot Master.

```
/tool user-manager customer add
subscriber=mikrotik login="mikrotik" password="ashish" time-zone=+05:30
permissions=owner parent=mikrotik
```

```
/tool user-manager router add  
subscriber=mikrotik name="R2" ip-address=192.168.1.2 shared-secret="123456"  
  
subscriber=mikrotik name="R3" ip-address=192.168.1.3 shared-secret="123456"  
  
subscriber=mikrotik name="R4" ip-address=192.168.1.4 shared-secret="123456"  
  
subscriber=mikrotik name="R5" ip-address=192.168.1.5 shared-secret="123456"
```

and finally add the user on R1

```
/tool user-manager user add  
username=ashish password=ashishpatel subscriber=mikrotik
```

The user name and password will work for all the remote hotspot router...a user can login from any department of the company with same ID and password and we can have all the user data centrally.

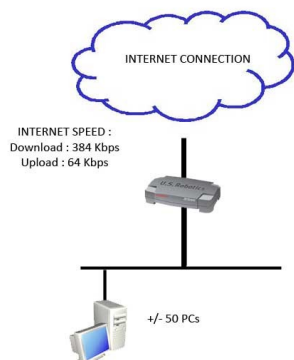
Now you can log into the User Manager web interface on the address <http://192.168.1.1/userman> and start setting up your user accounts.

More information in the [User Manager](#) section.

## [tutorial] Mikrotik Load Balancing - Winbox version

### Tutorial Mikrotik Load Balancing

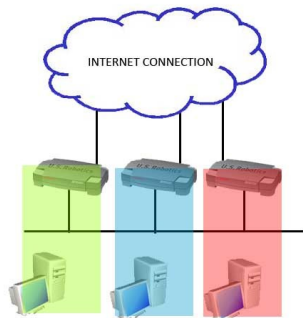
#### Konsep awal :



Di beberapa daerah, model internet seperti ini adalah bentuk yang paling ekonomis dan paling memadai, karena di beberapa daerah tidak mungkin untuk menggunakan jenis koneksi internet lain, karena cost yang akan dikeluarkan untuk biaya operasional akan menjadi sangat besar.

Lalu bagaimanakah dengan solusinya ? apakah kita bisa menggunakan beberapa line untuk menunjang kehidupan ber-internet ? Bisa, tapi harus digabung.

Contoh topologi yang tidak digabung :

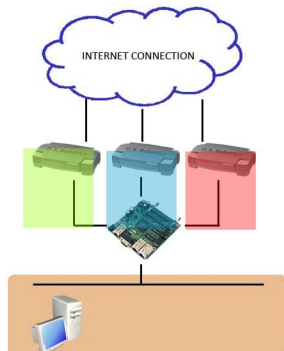


Ini adalah contoh topologi yang tidak digabung. Di perusahaan ini menerapkan 3 koneksi internet, dengan 3 modem yang berbeda, akan tetapi mereka di pecah, seakan2 mereka mempunyai 3 gerbang internet yang berbeda. Dengan topologi seperti ini, load internet tidak akan tergabung.

Model seperti ini kurang ideal untuk disebutkan sebagai load balancing.

#### Load Balancing

##### Topologi load balancing :





Dengan topologi seperti diatas, maka terjadi yang namanya Load Balancing. Jadi pada site ini, akan menggunakan 3 koneksi internet (baik itu dari ISP yang sama maupun yg berbeda) dan juga baik itu menggunakan jenis koneksi yg sama maupun yg berbeda (wireless, adsl, dialup).

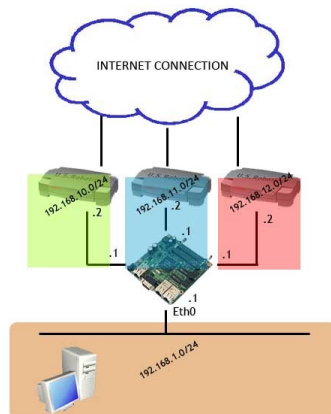
Dan semua client yang ada di jaringan, akan memiliki satu gateway, dan gateway itu yang akan menentukan packetnya akan lewat ISP yang mana.

### Konsep LoadBalancing (di Mikrotik)

1. Paket data masuk dari interface network
2. Paket data akan di berikan tanda pemisah (mangle). Misalnya di bagi jadi 3 group. :
  - paket 1 masuk group 1,
  - paket 2 masuk group 2,
  - paket 3 masuk group 3,
  - paket 4 masuk group 1,
  - paket 5 masuk group 2,
  - paket 6 masuk group 3,
  - dsb
3. Setelah paket di pisahkan, kita atur NATnya
  - a. group 1, maka akan keluar melalui interface 1,
  - b. group 2 akan keluar melalui interface 2,
  - c. group 3 akan keluar melalui interface 3.
4. Begitu juga dengan routingnya.

### Konfigurasi Load Balancing

#### Topologi lengkap :



#### Preparation

1. Configure modem-modem yg ada dengan IP management seperti yang ada di topologi
  - Modem hijau : 192.168.10.2 / 24
  - Modem biru : 192.168.20.2 / 24
  - Modem merah : 192.168.30.2 / 24
2. Configure PC Workstation yang ada di dalam jaringan dengan IP sebagai berikut :
  - IP : 192.168.1.x ( x, dari 2 – 254, karena 1 untuk gateway)
  - Netmask : 255.255.255.0
  - Gateway : 192.168.1.1

Set IP Address Interface Mikrotik (IP > Address)

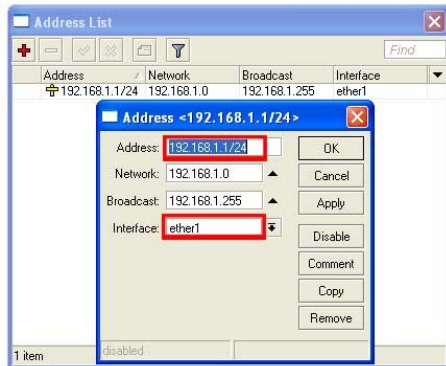
3. Konfigurasi IP address mikrotik dengan IP sebagai berikut :

Ether1 : 192.168.1.1 /24

Ether2 : 192.168.10.1/24 (interface ke modem hijau)

Ether3 : 192.168.20.1/24 (interface ke modem biru)

Ether4 : 192.168.30.1/24 (interface ke modem merah)



Note :

Setelah melakukan konfigurasi IP Address pada mikrotik, cek kembali konektifitas antara modem dengan mikrotik.

ping 192.168.10.2

ping 192.168.20.2

ping 192.168.30.2

## Mangling (IP > Firewall > Mangle)

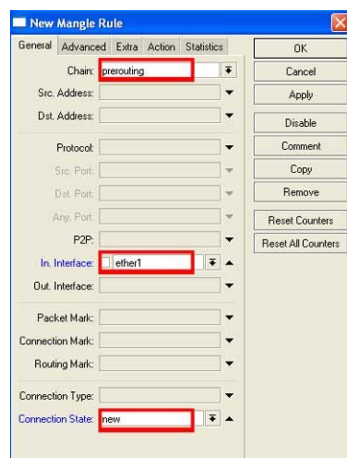
Mangle ada proses pemisahan. Pada proses mangle, sebenarnya tidak terjadi perubahan apa-apa pada paket atau data yang akan kita kirimkan, tapi pada proses ini paket hanya di berikan tanda.

## Connection Mark

Pertama kita akan lakukan connection mark.

### 1. General

- Add chain : prerouting
- In Interface : Eth 1 (interface jaringan local)
- Connection State : new

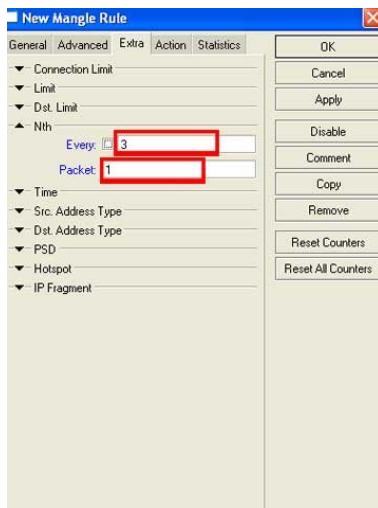


### 2. Extra - nth

- Nth

a. Every : 3

b. Packet : 1



Note :

Bagian Nth ini yang menentukan apakah paket akan masuk ke group 1, group 2 atau group 3. Untuk 3 line, maka nanti akan di buat 3 rule dengan Nth 31, 32 dan 33.

### 3. Action

- Action : mark connection
- New Connection mark : conn\_1
- Passthrough : yes



Note :

Pada bagian ini kita akan memberi nama koneksi kita. Conn\_1 adalah koneksi pertama, Conn\_2, untuk koneksi kedua, dan Conn\_3 untuk koneksi ke 3.

Note :

Lakukan connection marking ini sebanyak 3 kali, masing2 dengan NTH 31, 32 dan 33, dengan nama Conn\_1, Conn\_2 dan Conn\_3

## Route Mark

### 4. General

- Add chain : prerouting
- In Interface : Eth 1 (interface jaringan local)
- Connection mark : conn\_1

General Advanced Extra Action Statistics

Chain: **prerouting**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface: **ether1**

Out. Interface:

Packet Mark:

Connection Mark: **conn\_1**

Routing Mark:

Connection Type:

Connection State:

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

## 5. Action

- Action : mark routing
- New Connection mark : route\_1
- Passthrough : no

Note :

Pada bagian ini kita akan memberi nama pada routing kita. route\_1 adalah route pertama, route\_2, untuk route kedua, dan route\_3 untuk routing ke 3.

Note :

General Advanced Extra Action Statistics

Action: **mark routing**

New Routing Mark: **route\_1**

☐ Passthrough

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

Lakukan routing marking ini sebanyak 3 kali, masing2 untuk Conn\_1, Conn\_2 dan Conn\_3, dengan nama route\_1, route\_2 dan route\_3

## NAT (IP > Firewall > NAT)

NAT, Network Address Translation, adalah suatu proses perubahan pengalamatan. Ada beberapa jenis NAT, yang akan digunakan pada proses ini adalah src-nat (source nat).

Src-nat adalah perubahan pada bagian source dari suatu paket.

### 1. General

- Chain : src nat
- In Interface : Eth 1 (interface jaringan local)
- Connection mark : conn\_1

New NAT Rule

General Advanced Extra Action Statistics

Chain: **srcnat**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface: **ether1**

Out. Interface:

Packet Mark:

Connection Mark: **conn\_1**

Routing Mark:

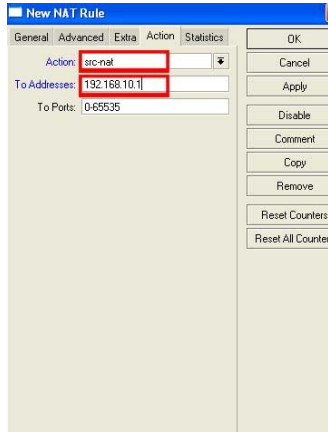
Connection Type:

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

## 2. Action

- Action : src nat

- To address : 192.168.10.1



Note :

Lakukan src-nat ini sebanyak 3 kali dengan rule sebagai berikut :

Conn\_1 == > 192.168.10.1

Conn\_2 == > 192.168.20.1

Conn\_3 == > 192.168.30.1

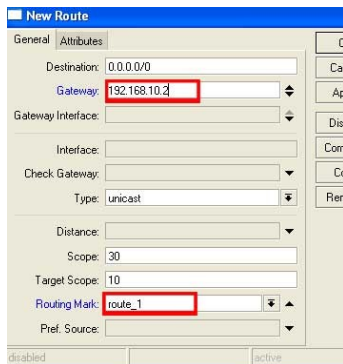
## Routing Policy (IP > Route)

Routing policy adalah bagian pengaturan routing. Pada bagian ini diatur gateway atau jalur keluar untuk setiap group

### 1. General

- gateway : 192.168.10.2

- Routing mark : route\_1



Note :

Lakukan src-nat ini sebanyak 4 kali dengan rule sebagai berikut :

route\_1 == > 192.168.10.2

route\_2 == > 192.168.20.2

route\_3 == > 192.168.30.2

default == > 192.168.10.2

=====

di persembahkan buat mikroters indonesia  
maap kalo repost, cuma mencoba untuk berkontribusi

=====

## Konfigurasi SMS saat Internet down

Akang bikin tutor ini sesuai request salah satu member forum mikrotik ini, dan mungkin ada temen-temen disini juga yang membutuhkannya jangan segan-segan untuk di coba, and seperti biasa moto Akang, Don't Steal My Tutz without credit. Yang tidak memahami moto diatas segera tutup tutz ini dan silahkan cari yang lain

Sebelumnya Akang mohon maaf dahulu karena tidak ada screenshot seperti biasanya dikarenakan tutz ini dibuat setelah modem HSDPA Akang dibeli oleh temen Akang yang amat sangat membutuhkan. Oia, Akang modemnya Huawei E220 yang paketan Flash tapi udah di Unlock.

Fitur yang satu ini tersembunyi, tidak nampak di winbox jadi tidak banyak yang tahu, kebetulan akang tahu karena iseng bisa ga ya di pake buat SMS nih mikrotik kalo modem dah nyolok terus misal putus terus ngabarin ke HP Akang atau yang ber-kompeten untuk meng-handle. Jadi ga ada ALASAN Telat Info

### 1st Step

Cek apakah modem anda sudah terdaftar di MikroTik apa belum, jika sudah silahkan langsung tancap dan jika belum carilah yang sudah terdaftar oia sama pastikan kartu GSM anda sudah aktif atau dapat digunakan,

### 2nd Step

Pastikan port yang digunakan oleh Modem HSDPA/GPRS anda, apakah usb atau serial atau pci. Jika sudah yakin mari kita tes sms masuk apa tidak

Code:

```
[Akangage@[Ei-Ji].NET]>
/tool sms usb1 085647960*** message="Hello Akang, masuk g sms-nya?"
```

Jika HP tujuan anda bergetar ada SMS masuk maka anda telah sukses konfigurasi SMS di MikroTik

### 3rd Step

Karena ingin dijadikan momen atau "alert" jika koneksi down, maka seperti biasa donk kita mainkan netwatch

Code:

```
[Akangage@[Ei-Ji].NET]>/tool netwatch add comment="Internasional" disable=no down-
script="/tool sms send usb1 "nomor tujuan" message="Koneksi Internasional down, ini
SMS otomatis jika koneksi down. Mohon jangan di reply. Terima Kasih."
host=68.180.206.184 interval=1m timeout=500ms up-script="/tool sms send usb1 "nomor
tujuan" message="Internasional sudah UP kembali"
```

Code:

```
[Akangage@[Ei-Ji].NET]>/tool netwatch add comment="IIX" disable=no down-
script="/tool sms send usb1 "nomor tujuan" message="Koneksi IIX down, ini SMS
otomatis jika koneksi down. Mohon jangan di reply. Terima Kasih." host=202.146.4.17
interval=1m timeout=500ms up-script="/tool sms send usb1 "nomor tujuan" message="IIX
sudah UP kembali, terima kasih telah menunggu."
```

Yak segitu saja, untuk interval dan timeout silahkan di edit kembali sesuai keinginan brother2 semua!! Oia, yang udah pernah terima SMS seperti ini di forum mikrotik yaitu masemen, silahkan di tanyakan untuk bukti Akang dah pernah coba2 [Hanya untuk meyakinkan saja kalau akang sudah mencoba sendiri]

Terima Kasih atas perhatiannya, Akang menunggu respon dari rekan-rekan semua!! Salam cup2 muahhh

## Mikrotik dengan SquidBox

nah sesuai yg gue janjiin di halaman pertama di thread [Queue dengan SRC-NAT dan WEB-PROXY](#), gue hari ini eksperimen dengan squidbox, karena ga ada PC yg dibuat eksperimen gue pake aja mail server gue yg pakai MDaemon

spec:

1. PC P3 800
2. Memory 128 MB
- 3 Hardisk sekitar 12 GB 5400 rpm
4. OS Win2k Pro
5. Menggunakan squidNT (yup squid under Windows)

Topology jaringan seperti ini: ( Mikrotik hanya 2 NIC )

inet--mikrotik--- switch---> client

.....|

.....-----> MailServer+Squidbox

dengan beberapa petunjuk dari sini dan forum sebelah, akhirnya bisa juga

Setingan di Mikrotik

Code:

```
#
/ ip firewall nat
add chain=srcnat out-interface=wan src-address=192.111.111.0/24 \
    action=masquerade comment="" disabled=no
add chain=dstnat in-interface=local src-address=!192.111.111.120 protocol=tcp \
    dst-port=80 src-address-list=iplist action=redirect to-ports=8082 \
    comment="transparent web" disabled=yes
```

ip lokal: 192.111.111.0/24

ip squidbox+mailserver: 192.111.111.120

iplist: ip yg boleh mengakses ke proxysquid (di daftar dulu ke address list)

.....jika semua client yg tersambung ke mikrotik boleh akses internet boleh

.....aja ip list ga dipake (gue pakai ini, karena.... lihat posting2an awal gue

...../ postingan di thread laen yg ada trouble dengan web-proxy).

gue pake port web-proxy 8082 karena menghindari adanya penyusup dari luar, (yg meng-generalisasikan bahwa port 8080 biasanya port proxy),meskipun udah ada firewall rulanya yg memblok port 8080 dan 8082 juga sih.

dibawah setingan web-proxy gue:

Code:

```
set enabled=yes src-address=0.0.0.0 port=8082 hostname="router" \
    transparent-proxy=yes parent-proxy=192.111.111.120:3128 \
    cache-administrator="webmaster" max-object-size=4096KiB cache-drive=system \
    max-cache-size=131072KiB max-ram-cache-size=unlimited
```

nah sampai sini 50% selesai.

sekarang menset squidBoxnya, karena gue tulis thread ini di rumah setingan squidbox lupa semua mohon maaf.

1. install squidbox for winNT dari: <http://www.serassio.it/SquidNT.htm>

di bagian squid.conf beri acl untuk membypass jika ada input dari ip mikrotik (ip lokal mikrotik gue 192.111.111.3)

Code:

```
http_port 3128

acl mikrotik src 192.111.111.3
acl blocker dstdomain -i "c:\squid\etc\blocklist.txt" <--funksinya sebagai web filter
http_access deny blocker
http_access allow mikrotik
```

3. lalu buat swap squidbox pake perintah c:\squid>squid -z  
..... tunggu beberapa detik dulu biar nanti swapnya selesai dibuat

4. install sebagai servis di windows , kalo ingin setiap PC diidupin langsung meload squid-nya pakai perintah .... (lupa gue nih,coba pake perintah squid -?, ada kok commandnya)

setelah gue jalanin udah bisa diarahkan ke squidbox, tp ternyata hasil dari web browser kena blok. setelah gue lihat access lognya ternyata keluarnya:

Code:

```
tanggal [kode kode tdk tau gue] [ip_public_gue] HTTP_DENIED http:\\forummikrotik.com
tanggal [kode kode tdk tau gue] [ip_public_gue] HTTP_DENIED http:\\forummikrotik.com
tanggal [kode kode tdk tau gue] [ip_public_gue] HTTP_DENIED http:\\forummikrotik.com
```

ga tau nih bisa begini aneh 🤔 masa ip public mikrotik gue bisa masuk ke lognya squid

nah akhirnya gue tambahkan disini acl ip public gue sperti gini:

Code:

```
http_port 3128

acl mikrotik src 192.111.111.3 [ip_public_gue]
acl dstdomain blocker -i regex "c:\squid\etc\blocklist.txt" <----- ini gue lupa, fungsinya sebagai web filter
http_access deny blocker
http_access allow mikrotik
```

gue restart lagi servis squidbox-nya langsung semua berjalan dengan sempurna. meskipun agak lelet karena kondisi hdd-nya yg sudah agak parah berbunyi aneh kletek keletek tapi anehnya windowsnya ngga hang 😊 biasanya kalo udah gitu udah koit hdd-nya, mungkin tinggal menunggu waktu. dan juga gue belum maksimalin settingan squidnya, (masih quickstart nih)

nah dari sini kita bisa mengganti squidboxnya dengan linux, yg mestinya lebih mantap



## **<ask> bagaimana cara install mikrotik di Router Board**

Pakai net install saja,

Pertama cari kebal serial null modem, matikan rb

- pakai hyperterminal set baut rate 115, data bit 8, parity none, stop bit 1, flow control, none
- nyalakan rb sebelum 2 detik tekan sembarang
- pilih O (pilih boot device) dan pilih ethernet.
- jalankan netinstall versi yang routerboard (nggak akan jalan kalau netinstall versi x86)
- klik netbooting isi dengan ip yang satu group dengan komp kita
- pilih paket yang mau diinstall
- klik install, tunggu prosesnya
- reboot kembali ke hyperterminal kembalikan lagi boot ke Nand
- selesai

meskipun kita melakukan format di Nand. license tidak terhapus, jadi kalau kita beli rb default level 4 akan tetep level 4 dan software id tidak berubah.

Semoga membantu.

Untuk install baru/ reinstall dengan netinstall mesti download packetnya dulu di

[http://www.mikrotik.com/download/all...\\_2.9.45-ns.zip](http://www.mikrotik.com/download/all..._2.9.45-ns.zip) terus jalankan software netinstallnya. jadi semua bisa offline.

Untuk upgrade bisa 2 cara secara online,

cara kedua download separete packet, kemudian pakai ftp kita upload ke routerboard setelah itu refresh, (/syst upgrad refre) dan reboot RB anda.

## Load Balance + Fail Over dengan script

Contoh Topologi yang dipakai pada script

```
ISP1-512kbps-----`interface WARNET1
`!`!
SPEEDY1-384kbps--SWITCH HUB--->MIKROTIK---interface WARNET2
`!`!
SPEEDY2-384kbps-----`interface WARNET3
```

ket:

- Masing-masing warnet menggunakan satu interface
- Modem ADSL speedy diset ke mode ROUTER/NAT
- Interface Input digabung menggunakan SWITCH/HUB untuk menghemat port ethernet

Oleh karena terdapat perbedaan kecepatan ISP, maka mangle aku set 4:3:3. Untuk penggunaan konfigurasi berbeda, silahkan disesuaikan pada scriptnya, ntar aku kasih tanda deh parameter yang harusnya disesuaikan.

Baiklah, kita teruskan ke pembahasan berikutnya. Ini adalah contoh dari interface yang ada sesuai topologi di atas, namun dengan sedikit perubahan, dikarenakan kalau jalur ISP1 dan Speedy digabung, bandwidth akan dengan mudah dicuri maka yang digabung hanya dua Speedy dan ISP1 menggunakan interface sendiri

Code:

```
/interface print
Flags: X - disabled, D - dynamic, R - running
#      NAME                                TYPE                RX-RATE    TX-RATE
MTU
 0  R warnet1                            ether                0           0
1500
 1  R warnet2                            ether                0           0
1500
 2  R warnet3                            ether                0           0
1500
 3  R ISP1                                ether                0           0
1500
 4  R Speedy                              ether                0           0
1500
```

Untuk membuat mangle yang demikian banyak (parameter dapat diubah/disesuaikan) memakan banyak waktu, karena itu bisa disederhanakan dengan script berikut ini:

Code:

```
:for t from=1 to=10 do={
:local e "ISP1","ISP1","ISP1","Spd1","Spd1","Spd1","Spd2","Spd2","Spd2"
/ip fire mangle add chain=prerouting in-interface="warnet1" \
connection-state=new nth=("9,1," . (($t)-1)) action=mark-connection \
new-connection-mark=("Net" . ($t)) passthrough=yes \
comment=("paketa" . ($t))
/ip fire mangle add chain=prerouting in-interface="warnet2" \
connection-state=new nth=("9,2," . (($t)-1)) action=mark-connection \
new-connection-mark=("Net" . ($t)) passthrough=yes \
comment=("paketb" . ($t))
```

```

/ip fire mangle add chain=prerouting in-interface="warnet3" \
connection-state=new nth=9,3," . (($t)-1)) action=mark-connection \
new-connection-mark=("Net" . ($t)) passthrough=yes \
comment=("paketc" . ($t))
/ip firewall mangle add chain=prerouting in-interface="warnet1" \
connection-mark=("Net" . ($t)) action=mark-routing \
new-routing-mark=[:pick $e (($t)-1)] comment=("routing" . ($t))
/ip firewall mangle add chain=prerouting in-interface="warnet2" \
connection-mark=("Net" . ($t)) action=mark-routing \
new-routing-mark=[:pick $e (($t)-1)] comment=("routing" . ($t))
/ip firewall mangle add chain=prerouting in-interface="warnet3" \
connection-mark=("Net" . ($t)) action=mark-routing \
new-routing-mark=[:pick $e (($t)-1)] comment=("routing" . ($t))
}

```

Parameter yang berwarna biru dapat diubah sesuai kebutuhan perbandingan bandwidth. Disini nth menggunakan counter yang berbeda untuk interface yang berbeda, sekedar untuk menjelaskan penggunaan counter. Dengan counter berbeda-beda tersebut maka tiap paket dari masing2 warnet akan menghitung sendiri-sendiri nth-nya. Apabila diinginkan topologi ke lokal hanya menggunakan 1 jalur, maka mangle connection cukup diberi satu saja, mis. paketa\* (untuk paketb\* dan paketc\* bisa dihapus).

Untuk Routing bisa menggunakan sbb:

Code:

```

/ip route add dst-address=0.0.0.0/0 gateway=[IP ISP1] \
scope=255 target-scope=10 routing-mark="ISP1" disabled=no
/ip route add dst-address=0.0.0.0/0 gateway=[IP Speedy1] \
scope=255 target-scope=10 routing-mark="Spd1" disabled=no
/ip route add dst-address=0.0.0.0/0 gateway=[IP Speedy 2] \
scope=255 target-scope=10 routing-mark="Spd2" disabled=no

```

untuk NAT-nya bisa pake NAT masquerade biasa

Pertama kita buat script, misalnya dengan nama "failover" dengan kode sbb:

Code:

```

:set route1 [/tool netwatch get [/tool netwatch find comment="ISP1"] status]
:set route2 [/tool netwatch get [/tool netwatch find comment="Spd1"] status]
:set route3 [/tool netwatch get [/tool netwatch find comment="Spd2"] status]
:if ($route1="up") \
# Untuk baris berikut ini silahkan diganti angka-angka sesuai dengan rasio
# v1/v2/v3 sesuaikan angka rasionya kecuali yang angka 0 tetap 0
# w1/w2/w3 diberi angka 1 atau 0 sesuai dengan rasionya
do={:global v1 4; :global w1 1,1,1,1} \
else {:global v1 0; :global w1 0,0,0,0}
:if ($route2="up") \
do={:global v2 3; :global w2 1,1,1} \
else {:global v2 0; :global w2 0,0,0}
:if ($route3="up") \
do={:global v3 3; :global w3 1,1,1} \
else {:global v3 0; :global w3 0,0,0}
:global v ($v1 + $v2 + $v3 - 1)
:global w ($w1 . $w2 . $w3)
:local M 0
# untuk to disesuaikan penjumlahan semua rasionya
:for Z from=1 to=10 do={
:if ([:pick ($w) (($Z)-1)]="1") do={
/ip fire mangle enable [/ip fire mangle find \
comment=("paketa" . $Z)]
/ip fire mangle enable [/ip fire mangle find \
comment=("paketb" . $Z)]

```

```

/ip fire mangle enable [/ip fire mangle find \
comment=("paketc" . $Z)]
/ip fire mangle enable [/ip fire mangle find \
comment=("routing" . $Z)]
/ip fire mangle set [/ip fire mangle find \
comment=("paketa" . $Z)] nth=($v . ",1," . $M)
/ip fire mangle set [/ip fire mangle find \
comment=("paketb" . $Z)] nth=($v . ",2," . $M)
/ip fire mangle set [/ip fire mangle find \
comment=("paketc" . $Z)] nth=($v . ",3," . $M)
:set M ($M+1)
} else={
/ip fire mangle disable [/ip fire mangle find \
comment=("paketa" . $Z)]
/ip fire mangle disable [/ip fire mangle find \
comment=("paketb" . $Z)]
/ip fire mangle disable [/ip fire mangle find \
comment=("paketc" . $Z)]
/ip fire mangle disable [/ip fire mangle find \
comment=("routing" . $Z)]
}
}

```

Kode diatas akan mendeteksi netwatch masing2 ISP/Speedy dan secara otomatis mengubah nilai nth sesuai dengan ISP yang sedang aktif. Misalnya Speedy 1 tidak aktif maka routing & paket\*5,6,7 akan di disable dan akan dihitung paket total yang aktif untuk mengisi nilai nth.

Langkah terakhir adalah membuat netwatch untuk masing2 ISP/Speedy, kemudian pada masing2 trigger (semua baik up maupun down) diberi pemanggil ke script ini

Code:

```

/tool netwatch
add host=[IP ISP1] disabled=no interval=20s comment="ISP1" \
up-script="failover" down-script="failover"
add host=[IP Speedy1] disabled=no interval=20s comment="Spd1" \
up-script="failover" down-script="failover"
add host=[IP Speedy2] disabled=no interval=20s comment="Spd2" \
up-script="failover" down-script="failover"

```

Demikian sedikit sharing dari saya. Jikalau ada kesalahan mohon dikoreksi.

Yah, walaupun sudah banyak yang membahas tentang Load Balance + Fail Over, tetapi kelihatannya belum ada yang dengan pendekatan script seperti ini, jadi walaupun tidak ada yang respons tetap aku uploadkan ke forum ini, semoga bisa menambah ilmu kita semua.

## Load Balancing nth buat Mikrotik Ver 3.xx dan 2.9xx

Sebelumnya saya minta maaf dulu yach kalo seandainya **REPOST**



:th\_being\_funny2 :

Hampir setiap hari saya bolak balik di forum ini dan membaca, rupanya masih banyak member yang sering menanyakan cara load balancing atau pun cara mengabungkan 2 line speedy.

disini saya ingin membagikan contoh load balancing nth yang saya pakai di server saya.

settingan pppoe speedy saya sudah saya tanam di dalam modem jadi saya gak pakai pppoe di mikrotik.

berikut contohnya buat mikrotik versi 3.xx (saya pakai di mikrotik 3.16) :

Ip Modem 01 : 192.168.1.1 interface=speedy1

IP Modem 02 : 192.168.2.1 interface=speedy2

IP Local : 10.18.92.1 interface=Local

### Setting Buat Mangle

```
/ip firewall mangle
```

```
add chain=prerouting action=mark-connection new-connection-mark=Santaria1 \
passthrough=yes connection-state=new in-interface=Local nth=2,1 \
comment="" disabled=no
```

```
add chain=prerouting action=mark-routing new-routing-mark=Santaria1 passthrough=no \
in-interface=HotSpot connection-mark=Santaria1 comment="" disabled=no
```

```
add chain=prerouting action=mark-connection new-connection-mark=Santaria2 \
passthrough=yes connection-state=new in-interface=Local nth=1,1 \
comment="" disabled=no
```

```
add chain=prerouting action=mark-routing new-routing-mark=Santaria2 passthrough=no \
in-interface=HotSpot connection-mark=Santaria2 comment="" disabled=no
```

### Setting NAT

```
/ip firewall nat
```

```
add chain=srcnat action=masquerade out-interface=speedy1
```

```
add chain=srcnat action=masquerade out-interface=speedy2
```

```
add chain=srcnat action=masquerade src-address="10.18.92.0/24"
```

### Setting Routenya

```
/ ip route
```

```
add dst-address=0.0.0.0/0 gateway=192.168.1.1 scope=255 target-scope=10 \
routing-mark=Santaria1 comment="" disabled=no
```

```
add dst-address=0.0.0.0/0 gateway=192.168.2.1 scope=255 target-scope=10 \
routing-mark=Santaria2 comment="" disabled=no
```

```
add dst-address=0.0.0.0/0 gateway=192.168.1.1 scope=255 target-scope=10 \
comment="primary connection" disabled=no
```

Berikut scripting Load Balancing dengan konfigurasi 2 Line untuk Mikrotik versi 2.9.27

Sesuaikan IP masing-masing interface menurut network kita.

Note : 10.11.90.1 = IP Local

192.168.1.1 = IP Modem Speedy 1

192.168.2.1 = IP Modem Speedy 2

By JoySolutions.

```
/ ip address
```

```
add address=10.11.90.1/24 network=10.11.90.0 broadcast=10.11.90.255 \
```

```
interface=local comment="" disabled=no
```

```
add address=192.168.1.254/24 network=192.168.1.0 broadcast=192.168.1.255 \
```

```
interface="Internet" comment="" disabled=no
```

```
add address=192.168.2.254/24 network=192.168.2.0 broadcast=192.168.2.255 \
```

```
interface="Speedy" comment="" disabled=no
```

```
/ ip firewall mangle
```

```
add chain=prerouting in-interface=local connection-state=new nth=1,1,0 \
```

```
action=mark-connection new-connection-mark=santaria1 passthrough=yes \
```

```
comment="Load Balancing Client" disabled=no
```

```
add chain=prerouting in-interface=local connection-mark=santaria1 \
```

```
action=mark-routing new-routing-mark=santaria1 passthrough=no comment="" \
```

```
disabled=no
```

```
add chain=prerouting in-interface=local connection-state=new nth=1,1,1 \
```

```
action=mark-connection new-connection-mark=santaria2 passthrough=yes \
```

```
comment="" disabled=no
```

```
add chain=prerouting in-interface=local connection-mark=santaria2 \
```

```
action=mark-routing new-routing-mark=santaria2 passthrough=no comment="" \
```

```
disabled=no
```

```
/ ip firewall nat
```

```
add chain=srcnat out-interface="Internet" action=masquerade comment="" \
```

```
disabled=no
```

```
add chain=srcnat out-interface="Speedy" action=masquerade comment="" \
```

```
disabled=no
```

```
/ ip route
```

```
add dst-address=0.0.0.0/0 gateway=192.168.2.1 scope=255 target-scope=10 \
```

```
routing-mark=santaria1 comment="" disabled=no
```

```
add dst-address=0.0.0.0/0 gateway=192.168.1.1 scope=255 target-scope=10 \
```

```
routing-mark=santaria2 comment="" disabled=no
```

```
add dst-address=0.0.0.0/0 gateway=192.168.1.1 scope=255 target-scope=10 \
```

```
comment="primary connection" disabled=no
```

# MikroTik Password Recovery

**last update: 2008-02-06**

**WARNING: The author makes no guarantees and holds no responsibility for any damage, injury or loss of property that may result after reading this page. Following text is for education purposes only!**

According to information on [MikroTik's wiki page](#), it is not possible to recovery the password. It is not true - i'll try to proof that below :)

## News

2008-01-23: new mtpass release: [mtpass-0.2.tar.bz2](#) (now it can decrypt passwords for all users)

## Hardware needed

- computer (laptop is a good choice for hard conditions) :)
- RouterBoard (i've tested it on versions: 532 and 532A - but should work on all [OpenWrt-supported](#) RouterBoards)
- serial console cable
- patch-cord

## Soft needed

- Due the fact that i don't like the big bill's operating system, so this tutorial will be based on linux, the distribution should not matter, but it's based on debian
- dhcp server (isc dhcp was used)
- tftp server (tftp-hpa was used)
- minicom (for serial communication)
- netcat
- ... and my [mtpass](#) tool :)

## So here we go...

Our goal is to set the RouterBoard BIOS to boot the system via network. In this way we will load our custom kernel. With that kernel we will be able to send to computer a file with MikroTik passwords. Then we will be able to decrypt the password.

### 1. Minicom configuration

If we don't chage default settings - the RouterBoard's console port should be accessible with the following transmission parameters: 115200, 8N1. So we need to set MikroTik like that. If minicom is launched for the first time, there's need to setup: `# minicom -s` Select "Serial port setup" and a window with parameters should appear. In my case i set:

```
A - Serial Device      : /dev/ttyUSB0
E - Bps/Par/Bits       : 115200 8N1
F - Hardware Flow Control : Yes
G - Software Flow Control : No
```

I've set the /dev/ttyUSB0 as serial port, due using a USB<->RS232 converter. In the case of computer with a standard COM1/COM2 port, so you should of course set the path to /dev/ttyS0 or /dev/ttyS1

After setting, you need to accept these values with hit the Enter key, then you'll return to main menu. Now you need to save minicom configuration as default:

"Save setup as dfl" and we're ready with minicom.

## 2. dhcp and tftp server configuration

You should setup dhcp to assign the IP address to MikroTik and then to pass the server and path to kernel image, which will be booted. How to configure the dhcp server is a topic for different kind of article, so I'll confine to minimum needed information :)

i used the following dhcpd.conf file:

```
default-lease-time 21600;
max-lease-time 43200;
option domain-name-servers 10.0.0.1;
option netbios-name-servers 10.0.0.1;
option netbios-node-type 8;
option www-server 10.0.0.1;
authoritative;
allow booting;
allow bootp;

subnet 10.0.0.0 netmask 255.255.255.0
{
    option routers 10.0.0.1;
    option subnet-mask 255.255.255.0;
    option broadcast-address 10.0.0.255;
    filename "/tftpboot/linuxrc";
    range 10.0.0.10 10.0.0.100;
}
```

You need to copy the [linuxrc](#) file to /tftpboot/ directory. This file is a kamikaze [OpenWrt](#) firmware. I've compiled it with ramdisk support - it doesn't need to put on CompactFlash, because this is the not point (I don't want to make changes to MikroTik filesystem itself - so i need to boot the OpenWrt from ramdisk). The image has also hardcoded IP address for eth0 interface (10.0.0.10).

Now it's time to much thanks to Drasar (a guy from Czech Republic). He gave me a lot info about kernels, booting etc. Thank you for support and time :)

Also big thanks to Andrew Griffiths for help. He inspire me a lot - links to his articles are below (first three) :)

If you want to compile the kernel and OpenWrt by yourself here is a link for a configuration file: [.config](#) (prepared and build with [kamikaze](#) version 7.09)

## 3. Let's do it :)

The following text is based on RouterBoard 532 (i've also tested it on 532A).

We connect the mikrotik with computer via serial console cable and via patch-cord, but we have to connect it to main ethernet adapter - in my RB there's a "PoE" sticker. If you have not do that already it's time to configure ethernet interface and launch the dhcp server on computer:

```
# ifconfig eth0 10.0.0.1 up
# invoke-rc.d dhcp start
```

Now it's time to run a minicom without modem initialization (this is not needed at all):

```
# minicom -o
```

If MikroTik is now running you need to reboot it, and if doesn't you need to power it up - short after that you should see on console the RouterBoard's BIOS:

```
RouterBOOT booter 1.5
```

```
RouterBoard 532
```

```
CPU frequency: 264 MHz
Memory size: 32 MB
```

```
Press any key within 1 seconds to enter setup
```

You have a short time to hit any key (default: one second - can be changed later) and than you'll see:

```
RouterBOOT-1.5
```

```
What do you want to configure?
```

```
d - boot delay
k - boot key
```



```
s - serial console
o - boot device
u - cpu mode
f - try cpu frequency
c - keep cpu frequency
r - reset configuration
g - upgrade firmware
i - board info
p - boot protocol
t - do memory testing
x - exit setup
your choice:
press o:
your choice: o - boot device
```

```
Select boot device:
  e - boot over Ethernet
* n - boot from NAND
  c - boot from CF
  1 - boot Ethernet once, then NAND
  2 - boot Ethernet once, then CF
  b - boot chosen device
your choice:
```

If you have a system on NAND memory you need to choose:

boot Ethernet once, then NAND - (1)

else - if you boot from CF (asterisk next to 'c' selection) then you need to press 2.

In my case i've pressed 1 and i was back in main menu.

Then i've selected the boot protocol configuration (p):

RouterBOOT-1.5

What do you want to configure?

```
d - boot delay
k - boot key
s - serial console
o - boot device
u - cpu mode
f - try cpu frequency
c - keep cpu frequency
r - reset configuration
g - upgrade firmware
i - board info
p - boot protocol
t - do memory testing
x - exit setup
your choice: p - boot protocol
```

**and i've selected dhcp (2):**

Choose which boot protocol to use:

```
  1 - bootp protocol
*  2 - dhcp protocol
your choice: 2 - dhcp protocol
```

After return to main menu you need to press x to save settings and reboot the kernel from your computer:

RouterBOOT-1.5

What do you want to configure?

```
d - boot delay
k - boot key
s - serial console
o - boot device
u - cpu mode
f - try cpu frequency
c - keep cpu frequency
r - reset configuration
g - upgrade firmware
i - board info
p - boot protocol
```



You need to run netcat on computer in listening mode - i.e. on port 7878: `/bin/netcat -l -p 7878 > user.dat ...` and from MikroTik you can send a file: `cat /mnt/nova/store/user.dat|nc 10.0.0.1 7878` In this simple way we have on computer the interested file. The next boot of mikrotik should be the standard way - from that medium we set before.  
Now you can disconnect cables from MikroTik :)

## 5. 0xfe239cda3d56 - what the hell is going on... :)

The passwords in the send file are crypted - fortunately it's not too hard to decrypt it - after my analysis I figured out that the passwords are crypted with XOR method. Every account has a different crypt-key. I wrote a small tool, which take filename with passwords as first argument (user.dat in our case), then it writes a passwords to standard output. The tool was tested on three different MikroTiks and it seems that is working correctly - but i don't guarantee that the RouterOS crypting algorithm will not change in the future and even with different versions. If it doesn't work in your case please mail me - i'll try to check why in my spare time.

Unfortunately for now i still don't know the crypt-key algorithm so my tool include known keys only - if you're in luck you'll see decrypted passwords - or strange characters otherwise.

Sources of this tool are available here: [mtpass-0.2.tar.bz2](#), therefore you need to unpack, compile and run it. Update: current version (will be in next release 0.3) of mtpass (only main cpp) file you can download here: [mtpass.cpp](#)

Finally - you can launch my tool like that:

```
# ./mtpass user.dat
mtpass v0.2 - MikroTik RouterOS password recovery tool, (c) 2008 by Manio
```

```
Reading file user.dat, 166 bytes long
```

Rec#	Username	Password	Disable flag	User comment
1	admin	secretpass		system default user

And you have what you're looking for :)

I hope this tutorial was helpful and you have your NAND ok after that :)

Best regards. And for happy ending a several links...

## Links:

- [MikroTik Router Security Analysis: Insecure Network Protocol](#)
- [MikroTik Router Security Analysis: Uncovering a hidden kernel module in a binary](#)
- [MikroTik Router Security Analysis: Weak password storage / encryption](#)
- [OpenWrt](#)
- [RouterBOARD 500](#)
- [RB500 Linux SDK](#)
- [Installation of Debian Sarge on Rouborboard 532](#)

## Contact:

Feel free to mail me if you have any information/suggestions:

e-mail/jabber: [manio@skyboo.net](mailto:manio@skyboo.net)

## Howto : Bypass traceroute traffic

Yang masih populer di kalangan pemakai internet adalah membuat ping time kecil walau traffic sudah full. Hal ini juga saya lakukan di mesin saya.

Tapi sempat terheran-heran ketika mencoba traceroute hasilnya berbeda dengan hasil ping, pada saat bw

full. 

Setelah sempat membaca di milist linux, dan membuka manpage dari traceroute akhirnya tahu kalau default dari aplikasi traceroute akan membuka sesi udp.

Berangkat dari pengalaman itu, maka mulai experiment untuk membaypass traceroute. Silakan dibaca scriptnya di bawah.

Code:

```
/ip firewall mangle

add chain=prerouting action=mark-connection \
    new-connection-mark=trace-con passthrough=yes \
    src-address=192.168.1.0/24 dst-port=33434-33534 \
    protocol=udp comment="" disabled=no

add chain=prerouting action=mark-packet \
    new-packet-mark=tracert passthrough=no \
    connection-mark=trace-con comment="" \
    disabled=no
```

Letakkan perintah firewall tersebut, diatas rule mangle untuk limiter perklient, agar rule dibaca terlebih dahulu.

Lalu tambahkan rule untuk queue simplenya, untuk aplikasi di queue tree silakan di coba coba sendiri



Code:

```
/ queue simple
add name="traceroute" dst-address=0.0.0.0/0 \
    interface=all parent=none \
    packet-marks=tracert direction=both priority=8 \
    queue=default-small/default-small \
    limit-at=0/0 max-limit=0/0 \
    total-queue=default-small disabled=no
```

Perhatikan juga penempatan queue simplenya.

artikel ini juga dapat di baca di blog saya di [mikrotik.web.id](http://mikrotik.web.id).

## Cara copy torch atau LOG ke file ---caranya ?

Salam kemal sebelumnya,

mohon infonya dari para sesepuh nich

saya pake winbox trus di menu tools torch, keluar deh ip dan ip desnya berserta tx dan rxnya

ada nda cara agar file itu dapat tercopy secara otomatis (tidak cospaste lagi) dimana data itu saya perlukan selama 1 bulan

mohon pencerahannya

terimakasih



mama\_nath

---

JAWABAN :

Kalau mau merekam koneksi ke file bisa pake perintah:

Code:

```
/ip firewall connection print file=filename
```

kalo mau dibikin otomatis per berapa menit, bisa diset di scheduler, dengan perintah script berikut:

Code:

```
/ip firewall connection print file=([:pick [/system clock get date] 0 3] . [:pick  
[/system clock get date] 4 6] . "-" . [:pick [/system clock get time] 0 2] . [:pick  
[/system clock get time] 3 5])
```

Nama file dibuat otomatis sesuai tanggal+jam (tanpa tahun dan detik).

Hati-hati, karena bisa memenuhi DOM/Flash dan agak memakan resource...

N.B. hasil export masuk ke files dan bisa dibuka pake wordpad (karena kalau pake notepad agak kacau)

oke, dah nemu cara masukin log informasi ke file, baru coba2 hari ini...

bikin di scheduler tiap berapa menit gitu, script dibuat gini:

Code:

```
/queue simple print stats file="stats-" . [:pick [/system clock get date] 0 3] .  
[:pick [/system clock get date] 4 6] . "-" . [:pick [/system clock get time] 0 2] .  
[:pick [/system clock get time] 3 5])
```

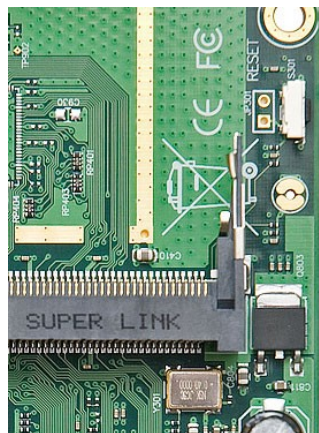
Code:

```
/queue simple print rate file="rate-" . [:pick [/system clock get date] 0 3] .  
[:pick [/system clock get date] 4 6] . "-" . [:pick [/system clock get time] 0 2] .  
[:pick [/system clock get time] 3 5])
```

kalo mo client tertentu aja bisa ditambah where name=namaqueue di belakangnya. Nama file ngikutin tanggal+jam nya.

# MikroTik Password Recovery

RouterOS password can only be reset by reinstalling the router, or using the reset jumper (or jumper hole) in case the hardware is RouterBOARD. For RouterBOARDS just close the jumper and boot the board until the configuration is cleared. For some RouterBOARDS there is not a jumper, but a jumper hole - just put a metal object into the hole, and boot the board.



To reset RouterOS config  
Hold metal object in here  
while the board boots.

Or.. if you use PC : Thing that you must have for this password recovery procedure are linux live CD (I use Ubuntu Live CD) and linux system with g++ compiler.

First step, boot your mikrotik PC router using linux live CD and mount the mikrotik drive (it should be ext3 file system), after successfully mounted, copy the 'mikrotik password file', (it located in /mnt/nova/store/user.dat) to USB flash drive, we will decode the password file.

The file path is relative, depend where you mount the mikrotik drive, for example if you mount your mikrotik drive in /mnt/media, the mikrotik password file should be /mnt/media/mnt/nova/store/user.dat

In Ubuntu Live, if you can not copy the file, may be you need to become root, use this command below :  
\$sudo su

After become 'root' copy the 'mikrotik password file' in to USB flash drive, The USB flash drive should be 'plug and play' in Ubuntu Live.

After we got password file, we can decode it, download the the password decoder <http://a3-system.info/blog/files/mtpass-0.2.tar.bz2>

After extract the decoder file you can compile it using g++ compiler, or you can use my binary version. I compile it on debian linux, using g++ version 4.1, you may need issue chmod +x in tho this binary file. You can download: <http://a3-system.info/blog/files/mtpass>

Here the some password decode process :

```
192.168.1.2 - PuTTY
debian:~# ./mtpass user.dat
mtpass v0.2 - MikroTik RouterOS password recovery tool, (c) 2008 by Manio

Reading file user.dat, 166 bytes long

Rec# | Username | Password | Disable flag | User comment
-----|-----|-----|-----|-----
1 | admin | [REDACTED] | | system default user

debian:~#
```

Sorry I make the password 'blury' 😊

Ok you got the password now, you can login into mikrotik pc router now 😊

## [Script] HTML Project for HotSpot Voucher

Hi..hi.... akhirnya sukses juga!!! Akang bagi2 Script bikin Voucher HotSpot di MikroTik dengan bantuan UserMan, silahkan di copy paste dan jangan lupa di Edit, takut ga pas atau takut ga cocok

Paste di text editor aja, trus simpan dengan ekstensi html/htm, trus masukkan lewat ftp atau /files di winbox ke direktori hotspot.

Yak.. putaran pertama

Code:

```
<table style="color: black; font-size: 11px;" border="2" height="10">
<tr>
  <td colspan="2" bordercolorlight="#000000" bordercolordark="#000000"><b><font
size="2" face="Arial">BIU Tech Airforce1 Wireless</font></b></td>
</tr>
<tr>
  <td bordercolorlight="#000000" bordercolordark="#000000"><b><font size="2"
face="Arial">Time:</font></b></td>
  <td bordercolorlight="#000000" bordercolordark="#000000"></font><b><font size="2"
face="Arial">%u_limit_uptime%</font></b></td>
</tr>
<tr>
  <td bordercolorlight="#000000" bordercolordark="#000000">
    <font face="Arial" size="2"><b>Validity</b></font></td>
  <td bordercolorlight="#000000" bordercolordark="#000000"><b><font size="2"
face="Arial">%u_prep_time%</font></b></td>
</tr>
<tr>
  <td bordercolorlight="#000000" bordercolordark="#000000"><b><font size="2"
face="Arial">Price:</font></b></td>
  <td bordercolorlight="#000000" bordercolordark="#000000"></font><b><font size="2"
face="Arial">%u_tot_price%</font></b></td>
</tr>
<tr>
  <td bordercolorlight="#000000" bordercolordark="#000000"><b><font size="2"
face="Arial">Username:</font></b></td>
  <td bordercolorlight="#000000" bordercolordark="#000000"></font><b><font size="2"
face="Arial">%u_username%</font></b></td>
</tr>
<tr>
  <td bordercolorlight="#000000" bordercolordark="#000000"><b><font size="2"
face="Arial">Password:</font></b></td>
  <td bordercolorlight="#000000" bordercolordark="#000000"><font
face="Arial"><b><font size="2">%u_password%</font></b></font></td>
</tr>
</table>
```

Putaran ke-2

Code:

```
</head>
<body bgcolor="#FFFFFF" text="#000000">
<div id="wb_Table1"
style="position:absolute;left:30px;top:17px;width:299px;height:294px;z-index:1"
align="left">
<table width="100%" border="0" cellpadding="0" cellspacing="1" id="Table1">
<tr>
<td align="center" valign="top" colspan="2" height="82"><font style="font-size:19px"
color="#000000" face="Times New Roman"><b>[Ei-Ji].NET HotSpot Internet Cafe<br>
```

```

</b></font><font style="font-size:15px" color="#000000" face="Times New Roman">Jl.
Gn. Muria 90 Grendeng Purwokerto 53122<br>
Banyumas - Jawa Tengah - Indonesia<br>
Telp. (0281) 630604</font></td>
</tr>
<tr>
<td align="left" valign="top" width="148" height="40"><font style="font-size:16px"
color="#000000" face="Times New Roman">Acces Time</font><font style="font-size:13px"
color="#000000" face="Times New Roman"><br>
</font></td>
<td align="right" valign="top" width="148" height="40"><font style="font-size:16px"
color="#000000" face="Times New Roman">Price</font><font style="font-size:15px"
color="#000000" face="Times New Roman"><br>
</font></td>
</tr>
<tr>
<td align="center" valign="top" colspan="2" height="46"><font style="font-size:15px"
color="#000000" face="Arial">SSID Wireless Network Name<br>
</font><font style="font-size:24px" color="#000000" face="Times New Roman"><b>[Ei-
Jil].NET HotSpot</b></font></td>
</tr>
<tr>
<td align="left" valign="top" width="148" height="40"><font style="font-size:16px"
color="#000000" face="Times New Roman">User Name<br>
</font></td>
<td align="right" valign="top" width="148" height="40"><font style="font-size:16px"
color="#000000" face="Times New Roman">Password<br>
</font></td>
</tr>
<tr>
<td align="center" valign="top" colspan="2" height="80"><font style="font-size:16px"
color="#000000" face="Times New Roman"><b><u>Terima Kasih atas Kunjungan Anda<br>
</u></b></font><font style="font-size:15px" color="#000000" face="Times New
Roman">Thank You for Using Our Services</font><font style="font-size:11px"
color="#000000" face="Arial"><br>
<br>
</font><font style="font-size:11px" color="#000000" face="Arial">System created by
Akanage<br>
</font><font style="font-size:11px" color="#000000" face="Arial Baltic">© [Ei-
Jil].NET HotSpot Internet Cafe 2008</font></td>
</tr>
</table></div>
</body>

```

Pesan Akang!!! Aja kelalen di Edit nyakkkk



maaf pertanyaan oot kang. nih script taruhnya di mana, biar bisa di gunakan  
buka browser.. masukan IP Userman anda, lalu masuk ke Customer, pilih ID-nya terus klik Voucher



boss.. script yg putaran ke dua, bikin browser saya (IE + firefox) jadi error scripting..

tapi yg putaran pertama emang mantep kok...



OK!! Boz... coba yang ini

Code:

```
<body>
<table style="text-align: left; width: 305px; height: 332px;" border="0"
cellpadding="2" cellspacing="2">
  <tbody>
    <tr align="center">
      <td colspan="2" rowspan="1" style="width: 30px; height: 10px;"><big><span
style="font-weight: bold;">[Ei-Ji].NET HotSpot Internet Caf</span><span style="font-
weight: bold;">e</span></big><br>
      <span style="font-weight: bold; font-style: italic;">Jl.
Gn. Muria No. 90 Grendeng Purwokerto</span><br>
      <span style="font-style: italic;">Telp. (0281) 630604</span></td>
    </tr>
    <tr align="center">
      <td style="width: 25%; height: 10%;">Access Time :<br>
%u_limit_uptime% </td>
      <td style="width: 25%; height: 10%;">Harga :<br>
%u_tot_price%<br>
      </td>
    </tr>
    <tr align="center">
      <td style="height: 10%;" colspan="2" rowspan="1">SSID
Wireless Network Name :<br>
      <big><big><span style="font-weight: bold;">[Ei-Ji].NET
HotSpot</span></big></big></td>
    </tr>
    <tr>
      <td style="height: 10%; width: 25%; text-align: center;">User Name :<br>
%u_username%<br>
      </td>
      <td style="height: 10%; width: 25%; text-align: center;">Password :<br>
%u_password%<br>
      </td>
    </tr>
    <tr align="center">
      <td style="height: 5%;" colspan="2" rowspan="1"><span style="font-weight:
bold; text-decoration: underline;">Terima
Kasih atas Kunjungan Anda</span><br>
      <span style="font-style: italic;">Thank You for
Using our Services</span><br>
      <br>
      Design & System Created by Akangage<br>
      (c) 2008 by [Ei-Ji].NET</td>
    </tr>
  </tbody>
</table>
<br>
<br>
</body>
```

Coba bisa ga???



Akhirnya dapet juga script yang bagus!!! Boleh di coba....

Code:

```
<body>
<table style="text-align: left; width: 285px; height: 268px;"
border="0" cellpadding="2" cellspacing="2">
```

```

<tbody>
  <tr align="center">
    <td colspan="2" rowspan="1" valign="undefined"><big><span
style="font-weight: bold;">[Ei-Ji].NET HotSpot Internet Cafe</span></big><br>
    <small>Jl. Gn. Muria No. 90 Grendeng Purwokerto 53122<br>
Banyumas - Jawa Tengah - Indonesia<br>
Telp. (0281) 630604</small></td>
  </tr>
  <tr>
    <td align="undefined" valign="undefined"><small>Access
Time<br>
%u_limit_uptime%</small></td>
    <td style="text-align: right;" valign="undefined"><small>Price
(Tarif)<br>
%u_tot_price%</small></td>
  </tr>
  <tr align="center">
    <td colspan="2" rowspan="1" valign="undefined"><big>SSID
Wireless Network Name<br>
    </big><big><big><span
style="font-weight: bold;">[Ei-Ji].NET HotSpot</span></big></big></td>
  </tr>
  <tr>
    <td align="undefined" valign="undefined"><small>User
Name<br>
%u_username%</small></td>
    <td style="text-align: right;" valign="undefined"><small>Password<br>
%u_password%</small></td>
  </tr>
  <tr align="center">
    <td colspan="2" rowspan="1" valign="undefined"><small><span
style="font-weight: bold; text-decoration: underline;">Terima
Kasih atas Kunjungan Anda</span><br>
Thank You for Using our Services</small></td>
  </tr>
  <tr align="center">
    <td colspan="2" rowspan="1"><small><small
style="font-weight: bold;">(c) [Ei-Ji].NET 2008 by Akangage</small></small></td>
  </tr>
</tbody>
</table>
<br>
</body>

```

Indah bangedd..... seneng liat-nya



## Ringtone Mikrotik



Buat refreshing nih boss, juga bisa buat ngebel yang ada di dekat mesin mikrotiknya

Code:

```
:beep length=400ms frequency=1046.5022612024
:delay 400ms
:beep length=200ms frequency=880
:delay 200ms
:beep length=200ms frequency=783.9908719635
:delay 200ms
:beep length=200ms frequency=659.2551138257
:delay 200ms
:beep length=200ms frequency=783.9908719635
:delay 200ms
:beep length=200ms frequency=880
:delay 200ms
:beep length=600ms frequency=1046.5022612024
:delay 600ms
:beep length=200ms frequency=880
:delay 200ms
:beep length=200ms frequency=783.9908719635
:delay 200ms
:beep length=200ms frequency=659.2551138257
:delay 200ms
:beep length=200ms frequency=783.9908719635
:delay 200ms
:beep length=400ms frequency=880
:delay 400ms
:beep length=400ms frequency=1046.5022612024
:delay 400ms
:beep length=200ms frequency=880
:delay 200ms
:beep length=200ms frequency=783.9908719635
:delay 200ms
:beep length=200ms frequency=659.2551138257
:delay 200ms
:beep length=200ms frequency=783.9908719635
:delay 200ms
:beep length=200ms frequency=880
:delay 200ms
:beep length=600ms frequency=1046.5022612024
:delay 600ms
:beep length=200ms frequency=880
:delay 200ms
:beep length=200ms frequency=783.9908719635
:delay 200ms
:beep length=200ms frequency=659.2551138257
:delay 200ms
:beep length=200ms frequency=246.9416506281
:delay 400ms
:beep length=200ms frequency=261.6255653006
:delay 400ms
```

Itu intro lagu Bendera - Coklat

Yang lagu Jablay coba ringtone ini:

Quote:

:beep length=300ms frequency=1046.5022612024  
:delay 350ms  
:beep length=300ms frequency=1318.5102276515  
:delay 350ms  
:beep length=300ms frequency=1318.5102276515  
:delay 350ms  
:beep length=300ms frequency=1174.6590716696  
:delay 350ms  
:beep length=300ms frequency=1046.5022612024  
:delay 350ms  
:beep length=650ms frequency=987.7666025122  
:delay 700ms  
:beep length=300ms frequency=987.7666025122  
:delay 350ms  
:beep length=300ms frequency=1046.5022612024  
:delay 350ms  
:beep length=300ms frequency=1174.6590716696  
:delay 350ms  
:beep length=300ms frequency=1318.5102276515  
:delay 350ms  
:beep length=175ms frequency=1046.5022612024  
:delay 175ms  
:beep length=175ms frequency=1174.6590716696  
:delay 175ms  
:beep length=175ms frequency=987.7666025122  
:delay 175ms  
:beep length=175ms frequency=1046.5022612024  
:delay 175ms  
:beep length=650ms frequency=880  
:delay 1050ms  
:beep length=300ms frequency=1046.5022612024  
:delay 350ms  
:beep length=300ms frequency=1318.5102276515  
:delay 350ms  
:beep length=300ms frequency=1318.5102276515  
:delay 350ms  
:beep length=300ms frequency=1174.6590716696  
:delay 350ms  
:beep length=300ms frequency=1046.5022612024  
:delay 350ms  
:beep length=650ms frequency=987.7666025122  
:delay 700ms  
:beep length=300ms frequency=987.7666025122  
:delay 350ms  
:beep length=300ms frequency=1046.5022612024  
:delay 350ms  
:beep length=300ms frequency=1174.6590716696  
:delay 350ms  
:beep length=300ms frequency=1318.5102276515  
:delay 350ms  
:beep length=175ms frequency=1046.5022612024  
:delay 175ms

```
:beep length=175ms frequency=1174.6590716696
:delay 175ms
:beep length=175ms frequency=987.7666025122
:delay 175ms
:beep length=175ms frequency=1046.5022612024
:delay 175ms
:beep length=650ms frequency=880
```

### **Sirine:**

Quote:

```
:for t from=1000 to=2000 step=20 do={:beep frequency=$t length=10ms; :delay 10ms}
:for t from=2000 to=1000 step=-20 do={:beep frequency=$t length=10ms; :delay 10ms}
:for t from=1000 to=2000 step=20 do={:beep frequency=$t length=10ms; :delay 10ms}
:for t from=2000 to=1000 step=-20 do={:beep frequency=$t length=10ms; :delay 10ms}
:for t from=1000 to=2000 step=20 do={:beep frequency=$t length=10ms; :delay 10ms}
:for t from=2000 to=1000 step=-20 do={:beep frequency=$t length=10ms; :delay 10ms}
```

kalo mo gaya lain tinggal coba dirubah-rubah parameternya oke...

Selanjutnya, Balonku dua lima (eh kebanyakan, ada lima aja deh)

Quote:

```
:beep length=200ms frequency=1318.5102276515
:delay 200ms
:beep length=200ms frequency=1396.9129257320
:delay 200ms
:beep length=400ms frequency=1567.9817439270
:delay 400ms
:beep length=400ms frequency=2093.0045224048
:delay 400ms
:beep length=400ms frequency=1567.9817439270
:delay 400ms
:beep length=400ms frequency=1318.5102276515
:delay 400ms
:beep length=800ms frequency=1567.9817439270
:delay 1200ms
:beep length=200ms frequency=1174.6590716696
:delay 200ms
:beep length=200ms frequency=1318.5102276515
:delay 200ms
:beep length=400ms frequency=1396.9129257320
:delay 400ms
:beep length=400ms frequency=1174.6590716696
:delay 400ms
:beep length=400ms frequency=1567.9817439270
:delay 400ms
:beep length=400ms frequency=1396.9129257320
:delay 400ms
:beep length=800ms frequency=1318.5102276515
:delay 1200ms
:beep length=190ms frequency=1046.5022612024
```

```

:delay 200ms
:beep length=200ms frequency=1046.5022612024
:delay 200ms
:beep length=390ms frequency=1760
:delay 400ms
:beep length=400ms frequency=1760
:delay 400ms
:beep length=400ms frequency=1975.5332050245
:delay 400ms
:beep length=400ms frequency=2093.0045224048
:delay 400ms
:beep length=800ms frequency=1567.9817439270
:delay 1200ms
:beep length=200ms frequency=1318.5102276515
:delay 200ms
:beep length=200ms frequency=1396.9129257320
:delay 200ms
:beep length=400ms frequency=1567.9817439270
:delay 400ms
:beep length=400ms frequency=1396.9129257320
:delay 400ms
:beep length=400ms frequency=1318.5102276515
:delay 400ms
:beep length=400ms frequency=1174.6590716696
:delay 400ms
:beep length=800ms frequency=1046.5022612024

```

Setelah mempelajari tipe data di Mikrotik, kayaknya angka di belakang titik (ind: koma) pada frequency tidak perlu dicantumkan karena Mikrotik hanya support integer dan bilangannya mending dibulatkan. Aku coba memasukkan rumus perhitungan frekuensi nada ternyata tidak bisa karena Mikrotik juga tidak support perpangkatan. Ntar aku mau coba pake :foreach aja biar lebih sederhana dan tidak terlalu panjang, cuman masih bermasalah pada durasi yang dinamis...

Nih hasil percobaan sementara untuk menyederhanakan perintah. Lagu= "Satu satu aku sayang ibu"  
Quote:

```

:local T 784,200ms,1047,400ms,1319,400ms,1568,600ms,\
1319,200ms,1760,200ms,1568,200ms,1397,200ms,\
1319,200ms,1175,600ms,784,200ms,988,400ms,\
1175,400ms,1397,600ms,1760,200ms,1568,200ms,\
1760,200ms,1568,200ms,1397,200ms,1319,600ms,\
784,200ms,1047,400ms,1319,400ms,1568,600ms,\
1319,200ms,1397,200ms,1319,200ms,1397,200ms,\
1568,200ms,1760,600ms,1760,600ms,1976,200ms,\
2093,200ms,1568,400ms,1318,400ms,1568,200ms,\
1397,200ms,1319,200ms,1175,200ms,1046,600ms
:for C from=0 to=(([:len $T]/2)-1) \
do={:beep frequency=[:pick $T ($C*2)] \
length=[:pick $T (($C*2)+1)]; :delay [:pick $T (($C*2)+1)]}

```

oke... lagu berikutnya:

Code:

```
:local T 784,350ms,1047,700ms,1047,350ms,1047,700ms,\
1175,350ms,1319,350ms,1319,350ms,1319,350ms,1047,700ms,\
1397,350ms,1319,700ms,1175,350ms,988,350ms,1047,350ms,\
1175,350ms,1047,1050ms,20000,700ms,\
784,350ms,1047,700ms,1047,350ms,1047,700ms,\
1175,350ms,1319,350ms,1319,350ms,1319,350ms,1047,700ms,\
1397,350ms,1319,700ms,1175,350ms,988,350ms,1047,350ms,\
1175,350ms,1047,1050ms
:for C from=0 to=(([:len $T]/2)-1) \
do={:beep frequency[:pick $T ($C*2)] \
length[:pick $T (($C*2)+1)]; :delay [:pick $T (($C*2)+1)]}
```

Oke... lagu berikutnya:

Code:

```
:local T 784,300ms,1047,300ms,262,150ms,1047,150ms,\
1319,300ms,784,300ms,1047,300ms,262,150ms,392,150ms,\
1047,150ms,523,150ms,1319,150ms,392,150ms,1175,\
300ms,294,150ms,1175,150ms,1047,300ms,988,300ms,\
1047,300ms
:for C from=0 to=(([:len $T]/2)-1)\
do={:beep frequency[:pick $T ($C*2)] \
length[:pick $T (($C*2)+1)]; :delay [:pick $T (($C*2)+1)]}
```



Hmm... okelah, tapi kalo pas aku senggang aja ya, soalnya akhir2 ini aku agak sibuk mikirin load balance yang kurang sempurna...

Anyway, buat yang merasa dirinya kreatif mungkin bisa bikin sendiri trus di postingkan ke sini pake script yang aku buat. Cuman script itu masih ada kelemahannya sih, cuman bisa muter sampe berapa nada gitu, entah masalah apanya, soalnya kalo aku debug dan diganti 🤔, tulisannya bisa sampe kompli, tapi kalo pake :beep kok cuman terbatas yah...

Oke... sedikit penjelasan script buat yang mo nyoba-nyoba sendiri:

buat variabel dengan

Code:

```
:local T frekuensi nada 1,lama nada diputar 1,frekuensi nada 2,lama nada diputar
2, ..., ... dst
```

trus copy paste script kayak diatas

Code:

```
:for C from=0 to=(([:len $T]/2)-1)\
do={:beep frequency[:pick $T ($C*2)] \
length[:pick $T (($C*2)+1)]; :delay [:pick $T (($C*2)+1)]}
```

untuk referensi frekuensi nada bisa dilihat di:

<http://www.borg.com/~jglatt/tutr/notefreq.htm>

kalo ternyata lom sampe selesai udah macet nadanya coba dipotong jadi dua bagian (setelah set variabel, set pemanggil, set variabel lagi, set pemanggil). Coba liat, siapa yang bisa kasih ringtone paling keren disini



Next ringtone in playlist :

Code:

```
:local T 1319,250ms,1568,250ms,1568,500ms,1319,250ms,1568,250ms,\
1568,375ms,1568,125ms,1319,250ms,1568,250ms,\
1760,250ms,1568,250ms,1319,250ms,1175,250ms,1175,375ms,\
1568,125ms,1319,250ms,1568,250ms,1568,375ms,1568,125ms,\
1319,250ms,1568,250ms,1568,375ms,1568,125ms,1319,250ms,\
1568,250ms,1760,250ms,1568,250ms,1175,250ms,1047,250ms,\
1047,250ms
:for C from=0 to=(([:len $T]/2)-1) \
do={:beep frequency[:pick $T ($C*2)] \
length[:pick $T (($C*2)+1)]; :delay [:pick $T (($C*2)+1)]}
```

FF menang lawan monster (kalo nggak salah, udah lama gak maen sih):

Code:

```
:local T 1047,250ms,1047,125ms,1047,125ms,1047,500ms,\
831,500ms,932,500ms,1047,375ms,932,125ms,1047,500ms
:for C from=0 to=(([:len $T]/2)-1) \
do={:beep frequency[:pick $T ($C*2)] \
length[:pick $T (($C*2)+1)]; :delay [:pick $T (($C*2)+1)]}
```

Kangen Band (seingatnya aja ya bro):

Code:

```
:local T 784,300ms,1319,600ms,1319,600ms,1175,600ms,988,600ms,\
1047,600ms,20000,300ms,988,150ms,1047,150ms,988,450ms,\
988,150ms,1319,300ms,1568,300ms,1047,600ms,20000,300ms,\
880,300ms,784,300ms,784,300ms,1047,300ms,1319,300ms,\
1397,600ms,1319,600ms,1175,600ms
:for C from=0 to=(([:len $T]/2)-1) \
do={:beep frequency[:pick $T ($C*2)] \
length[:pick $T (($C*2)+1)]; :delay [:pick $T (($C*2)+1)]}
```

ya sdh di coba bgtu, tp saat diskonek bunyi sirene nya hanya sekali saja..kan sharusnya bunyi terus sampai koneksi tersambung lagi.

netwatchnya sperti ini:

```
# /tool netwatch> pr detail
```

Flags: X - disabled

0 host=202.xxx.xxx.xxx timeout=5s interval=1s since=mar/17/2008 22:13:06

status=up up-script="" down-script=sirens

-----

Nih buat yang mo sirine alarm kalo koneksi putus...

Bikin script dengan nama misalnya "watch", source-nya seperti ini:

Code:

```
:do {
:for t from=1000 to=2000 step=20 do={:beep frequency=$t length=10ms; :delay 10ms}
:for t from=2000 to=1000 step=-20 do={:beep frequency=$t length=10ms; :delay 10ms}
} while ([/tool netwatch get [/tool netwatch find comment="check"] status]="down")
```



Trus bikin netwatch nya:

Code:

```
/tool netwatch add disabled=no interval=15s down-script="watch"
comment="check" host=xxx.xxx.xxx.xxx
```

Anyway, nih Yovie & Nuno yang di request:

Code:

```
:local T 1047,200ms,1047,200ms,1047,200ms,1397,400ms,\
1319,400ms,20000,200ms,1319,200ms,1319,200ms,1319,200ms,\
1319,400ms,1175,400ms,20000,200ms,1175,200ms,1175,200ms,\
1175,200ms,1397,400ms,1319,400ms,20000,200ms,1319,200ms,\
1319,200ms,1319,200ms,1319,400ms,1175,400ms,20000,200ms,\
1047,200ms,1047,200ms,1047,200ms,1047,400ms,1760,400ms,\
20000,200ms,1047,200ms,1047,200ms,1047,200ms,1047,400ms,\
1568,400ms,20000,200ms,1047,200ms,1047,200ms,1047,200ms,\
1047,400ms,1397,400ms,1319,400ms,1175,400ms,1047,400ms,\
1319,800ms,1175,400ms
:for C from=0 to=(([:len $T]/2)-1) \
do{:beep frequency[:pick $T ($C*2)] \
length[:pick $T (($C*2)+1)]; :delay [:pick $T (($C*2)+1)]}
```

kwik update :

pake script pak yosan yang melibatkan netwatch berjalan mulus. Tapi aye salah masukin time interval (15s). Nyetel di winbox malah 15 menit (00:15:00). Hasilnya sirine meraung2 lamaaa... Sampe si OP kalang kabut



nelpon aye ke rumah..Katanya "Mas ! ini ruter kog bunyi seh! takut nih kaya mau meledak!"  
sekarang aye pake script ini ajah :

```
/tool netwatch add disabled=no interval=15s down-script="watch"
comment="check" host=209.85.175.147 ==> IP Google
```

```
:do {
:beep length=1s frequency=150
:delay 2s
} while ([/tool netwatch get [/tool netwatch find comment="check"] status]="down")
```

Jadi suaranya cuma teet-teet frekuensi rendah. Nggak melengking en kedengerannnya elegan bin



profesional gitu lox

## Editing Hotspot login Page

allow all

Mungkin ini pernah di bahas sebelumnya cmn ngga lengkap ..jadi saya cmn mo lengkapin aja , jadi buad bang momod kalu emang udah ada tinggal di pindah aja ....

..sebenarnya yang kita perlukan hanya 3 scipt yang bisa di paste di htmlnya

### Dibawah body :

```
$(if chap-id)
<form name="sendin" action="$(link-login-only)" method="post">
<input type="hidden" name="username" />
<input type="hidden" name="password" />
<input type="hidden" name="dst" value="$(link-orig)" />
<input type="hidden" name="popup" value="true" />
</form>

<script type="text/javascript" src="/md5.js"></script>
<script type="text/javascript">
<!--
function doLogin() {
document.sendin.username.value = document.login.username.value;
document.sendin.password.value = hexMD5('$(chap-id)' + document.login.password.value + '$(chap-
challenge)');
document.sendin.submit();
return false;
}
//-->
</script>
$(endif)
```

---

### Form Login & Password

```
$(if trial == 'yes')Free trial available, <a style="color: #FF8080"href="$(link-login-only)?dst=$(link-orig-
esc)&username=T-$(mac-esc)">click here</a>.$(endif)
```

```
<form name="login" action="$(link-login-only)" method="post"
$(if chap-id) onSubmit="return doLogin()" $(endif)>
<input type="hidden" name="dst" value="$(link-orig)" />
<input type="hidden" name="popup" value="true" />
<table width="100" align="center" background="images/login_05.gif" style="background-color: #ffffff">
<tr>
<td align="right">login</td>
<td><input style="width: 80px" name="username" type="text" value="$(username)" /></td>
</tr>
<tr>
<td align="right">password</td>
<td><input style="width: 80px" name="password" type="password" /></td>
</tr>
<tr>
<td>&nbsp;</td>
<td><input name="submit" type="submit" value="OK" /></td>
```

```
</tr>
</table>
</form>
```

### Tempatkan di atas body close tag

```
<script type="text/javascript">
<!--
document.login.username.focus();
//-->
</script>
```



DONE !!!

Trus kalau kalian2 mau ganti tuh template & gak mau repot2 bikin sendiri .. gampang aja sambangin situs yg satu ini [www.webgraf.ru](http://www.webgraf.ru) disitu ada ratusan webtemplate tinggal download .. tambahin + modifikasi dengan script di atas ... kalian sudah punya login page yg manizzz .... (templatennya lengkap , mulai dari file PSD , versi Html & flash..jadi image bisa di ganti sesuai keinginan ) monggo di kreasi .....

Ps.ogh iya jgn lupa daftar dulu supaya url buat download'nya keliatan

semoga bermanfaat

ogh iya ini salah satu contoh template yg udh sempat saya kreasi



## Memisahkan antara download dan browsing dengan mikrotik

---

Sekedar share settingan, siapa tahu dengan adanya masukan-masukan dari rekan-rekan sekalian dapat lebih memaksimalkan setting mikrotik saya;

Settingan ini adaah hasil dari membaca tutor 'delaypoll rasa mikrotik' post dari bro 'niplux'... thank's banget mas atas tutornya;

Seperti tutor yang saya sebut diatas, pertama kita buat list filter di "/ip firewall filter" yang akan menangkap setiap request yang berisi contents file-file yang biasa di download; seperti .exe .rar .zip dan website-website yang biasa ngabisin bandwidth; seperti youtube, megarotic dll..

Dan setelah di tangkap, maka ip address si website yang didownload tersebut akan kita masukkan kedalam list tersendiri; yang didalam contoh ini saya bikin list "yes\_no".

berikut adalah hasil dari perintah yang dibikin (maaf saya tampilkan hasil jadinya saja, karena saya bikin di winbox...)

Quote:

```
chain=forward protocol=tcp dst-port=80 content=.exe src-address-list=x_z_1_download action=add-dst-to-address-list address-list=yes_no address-list-timeout=1d
```

Disini setiap website yang diakses oleh list address "x\_z\_1\_download" akan dimasukkan dalam list "yes\_no" selama satu hari; (perkiraan download paling lama)

kemudian bikin satu mangle untuk menangkap client yang melakukan download;

Quote:

```
chain=postrouting out-interface=ether1 connection-mark=http_conn src-address-list=yes_no dst-address-list=_best action=mark-packet new-packet-mark=http_clients_down passthrough=no
```

Setiap aksi dari list address "\_best" yang bertujuan ke list address "yes\_no" pada port '80' akan dimark packet dengan nama "http\_clients\_down";

filtering dan marking packet udah selesai; sekarang kita bikin "queue tree"-nya untuk membatasi bandwidth download ini :

bikin dulu "queue type" pcq dengan nama "\_d\_best\_down" dan rate-nya diset 64000 (8 KB/s);

Quote:

```
name="_d_best_down" kind=pcq pcq-rate=64000 pcq-limit=50 pcq-classifier=dst-address pcq-total-limit=2000
```

Dengan rate ini, sebesar-besarnya client download; mereka hanya akan mendapatkan max 8 KB/s; meskipun dia menggunakan IDM atau apapun namanya.

Selanjutnya bikin queue tree;

Quote:

```
name="In_best_down" parent=2_In_best packet-mark=http_clients_down limit-at=0 queue=_d_best_down priority=8 max-limit=320000 burst-limit=0 burst-threshold=0 burst-time=0s
```

Diberi nama "In\_best\_down" dengan parent "2\_In\_best" yang menangani packet mark yang sudah kita buat diatas; yakni "http\_clients\_down" dengan priority paling bontot=8; rate 0 dan max 320kbps; (perkiraan dalam waktu bersamaan yang download 5 user).

mengenai priority; untuk browsing biasa diberi priority yang lebih tinggi, semisal "2" atau "3", sehingga jika ada user yang sedang download, pada saat juga melakukan browsing, maka download istirahat sejenak, nunggu browsing-nya selesai and setelah itu download lanjut lagi...

Selesai....

Tapi ada permasalahan sedikit; dimana apabila website yang sudah ditangkap dan dimasukan ke

dalam list "yes\_no" itu ternyata adalah website penting seperti "yahoo", "google" dll.. maka dia akan tetap kelimit selama satu hari.. wah.....

Untuk mengatasi ini, kita membuat scripts yang khusus melakukan checking pada website-website penting tersebut; dimana jika ditemukan website itu tertangkap, maka secara otomatis akan dihapus dari list "yes\_no" agar tidak terlimit. Jadi khusus untuk website penting ini aja download bebas melalui jalur browsing biasa.. gpp-lah... kan jarang-jarang juga client download attachment dari email. pertama bikin dulu fiternya untuk nangkap website penting tersebut:

Quote:

```
chain=forward protocol=tcp dst-port=80 content=yahoo.co src-address-list=x_z_1_download  
action=add-dst-to-address-list address-list=penting address-list-timeout=1d
```

Setiap aksi dari list address "x\_z\_1\_download" yang berisi contents "yahoo.co" akan dimasukkan kedalam list "penting". (bukan "yes\_no") karena ini akan kita gunakan sebagai dasar untuk melakukan pengecekan pada script kita;

dan selanjutnya bikin scripts :

Quote:

```
:foreach i in=[/ip firewall address-list find list=penting dynamic=yes] do={/ip firewall address-list remove  
[find address=[/ip firewall address-list get $i address]]}
```

Semua ip yang terdapat dalam list "penting" akan dihapus, termasuk yang berada di list "yes\_no" dll... bikin scheduler:

Quote:

```
cek_penting penting jan/01/1970 22:29:00 5s 4417
```

Aksi dilakukan setiap 5 detik.

Selanjutnya bagaimana dengan yang sudah selesai download?

karena kita set waktu penangkapan selama 1 hari, maka ada kemungkinan di pendownload sudah selesai; dan ada baiknya website yang ada di list "yes\_no" dan sudah tidak aktif lagi melakukan koneksi dihapus saja; ini untuk menjaga agar jika ada user yang hanya sekedar browsing pada website tersebut tidak terhalang oleh priority "8" tadi, biar normal lagilah istilahnya;

Jadi secara periodik kita harus mengecek status koneksi khusus untuk list "yes\_no" saja. apakah masih ada koneksi aktif apa tidak; jika masih ada dibiarkan, jika sudah tidak ada dihapus...!!!

Bikin scripts lagi:

Quote:

```
:foreach i in=[/ip firewall address-list find list=yes_no dynamic=yes]do={:if([:len [/ip fire conn find dst-  
address=([/ip firewall address-list get $i address]. ":80")]]=0) do={/ip fire address-list remove $i}}
```

Melakukan cek koneksi yang ada pada port 80, jika ternyata si ip dalam list masih aktif koneksinya: dibiarkan, jika udah gak ada aktifitas lagi: dihapus...

Bikin scheduler-nya :

Quote:

```
cek_remove remove jan/01/1970 22:29:00 11s 1661
```

Untuk peletakan aturan dalam mangle-nya, harus pas, dimana aturan untuk download ini diletakkan diatas aturan untuk browsing biasa;

kalo ada yang janggal atau kurang pas mohon dikoreksi, yach biar makin seplah kinerja mikrotik saya...

thank's..

## backup database radius server hotspot

---

help me....

*gmna yach cara backup database radius server hotspot,  
skr2 ini kan sering mati listrik tuh.... radius server aq sering hank,  
takut nya database radius server hotspot khusu ny utk voucher bisa ilang...  
klu sampe ilang... mate deh....*

*mohon pencerahannya*

Gini maksudnya ya..

```
[admin@Radius-server] > tool user-manager database save name=voucer-tes
```

nanti tinggal ambil backup voucernya di File--kem copy ke windows

kalau perlu buatkan schedule tiap hari

```
[admin@Radius-server] >system scheduler print detail
```

```
0 name="userman" on-event=tool user-manager database save name=voucer  
start-date=sep/17/2008 start-time=06:00:00 interval=1d run-count=1  
next-run=sep/25 06:00:00
```

## CARA BACKUP ANTARMIKROTIK

Mikrotik A

backup

telnet

```
/tool user-manager database save  
name: penduduk
```

trus buka winbox Mikrotik A

/file/klik di klik rendam "file: penduduk.umb".....tarik pk mouse lalu taroh di dekstop

Mikrotik B

trus buka winbox Mikrotik B

klik file di winbox

klik rendam "file: penduduk.umb" yang ada di dekstop.....tarik pk mouse lalu taroh di file (posisi paling bawah)

restore

telnet

```
/tool user-manager database load  
name: penduduk
```



## CATATAN LAIN-LAIN :

bRo numpang share tutorial ne: Bro kucing ama gw coba blok packet yang ada isi file extension tertentu.. ni hasilnya:

```
//ip web-proxy access add url=":\.3g[p]$" src-address="(terserah)" method=any action=deny - blok paket 3gp
```

```
//ip web-proxy access add url=":\.ra[r]$" src-address="(terserah)" method=any action=deny - blok paket rar
```

```
//ip web-proxy access add url=":\.sw[f]$" src-address="(terserah)" method=any action=deny - blok paket swf
```

```
//ip web-proxy access add url=":\.mp[3g]$" src-address="(terserah)" method=any action=deny - blok paket mp3 and mpg
```

```
//ip web-proxy access add url=":\.jp[g]$" src-address="(terserah)" method=any action=deny - blok paket jpg
```

NB: rule ini taruh di paling atas

wah mo di terapin usermanager jg yah, oke gw mulai yah .....

eit sebelumnya paket usermanager sendiri musti di install dulu dan hotspotnya musti di setup dulu baru bisa pake usermanagernya.....

1. [kucing@mikrotik]> radius add service=hotspot address=127.0.0.1 secret=123456 ----> addressnya itu address dari hotspot

2. [kucing@mikrotik]> / ip hotspot profile set hspof1 use-radius=yes -----> hspof1 itu adalah profile dari hotspot

3. [kucing@mikrotik]> / tool user-manager customer add login="MikroTik" password="tes" permissions=owner -----> username ini untuk login ke userman

4. [kucing@mikrotik]> / tool user-manager router add subscriber=MikroTik ip-address=127.0.0.1 shared-secret=123456 -----> address untuk userman

5. sekarang tes login ke userman dengan buka browser, ketik 127.0.0.0/userman -----> ip userman nya

6. kalo bisa login berarti anda telah sukses menghubungkan hotspot ke userman cukup mudah kan ....., anda tidak perlu lagi menambahkan user di hotspot tapi langsung aja tambahin dari usermannya melalui browser

kalo ada tanda merah2 ato invalid bisa di karenakan salah penempatan interface / ip coba deh di cek kembali wew masa seh, udah di redirect blom di nat nya.

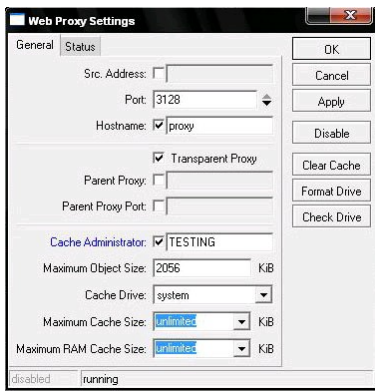
ini contoh redirect ke web-proxy dengan default port = 3128

[kucinggarong@MikroTik] ip firewall nat> add chain=dstnat action=redirect to-ports=3128(port web-proxynya) dst-port=80 protocol=tcp ---> **taro setelah masquarade ato di paling atas**

ini conto redirect ke ip-proxy dengan port = 8080

[kucinggarong@MikroTik] ip firewall nat> add chain=dstnat action=redirect to-ports=8080(port ip-proxynya) dst-port=80 protocol=tcp ---> **taro setelah masquarade ato setelah web-proxy**





just share dari salah satu blog orang indo  
nara sumber <http://indramgl.wordpress.com/2007/1...k/#comment-454>

Max-limit merupakan batasan maksimal bandwidth yang dapat dikonsumsi oleh komputer yang dikenakan limitasi.

Burst-limit merupakan batasan maksimal bandwidth yang dapat dikonsumsi dalam waktu yang singkat yang ditentukan dengan burst-time.

Burst-Thres merupakan pemicu atau trigger atau titik pembalik atau batasan bandwidth riil yang diterima sebagai pembatas burst-limit.

contoh batasan bandwidth pada komputer a:

Max-limit=64k  
Burst-limit=128k  
Burst-Thres=48k  
Burst-Time=2

Berarti komputer tersebut dapat memperoleh bandwidth 128kbps selama traffic riilnya belum mencapai 48kbps, jika dia sudah mencapai traffic riilnya maka secara otomatis bandwidth yang dia dapatkan akan berangsur-angsur turun menuju 64 kbps. Skenario seperti ini sering diterapkan oleh beberapa ISP yang menawarkan bandwidth yang burstable, atau warnet yang lebih mengutamakan klien yang browsing daripada klien yang melakukan download. Dengan menggunakan konfigurasi seperti diatas sering kali klien yang browsing akan mereka cepat karena mereka sering kali mendapatkan 128 kbps sedangkan jika mereka mulai melakukan download data dari internet maka jatah koneksi mereka akan turun menjadi 64 kbps.

rumus manajemen bandwidth

=====

Limit-at = Sesuai selera anda  
Max-limit = Sesuai selera anda  
Burst-limit =  $< 4 \times \text{Max-limit}$   
Burst-Thres =  $\frac{3}{4} \times \text{Max-limit}$   
Burst-time =  $< 12 \text{ s}$



rumusan ini belum tentu tepat,tapi cukup sebagai dasar ....

Untuk memaksa User membuka website tertentu setiap memasukkan username dan password pada halaman login hotspot :

Edit file alogin.html  
</style>

```

<script language="JavaScript">
<!--
    function startClock() {
        $(if popup == 'true')
            open('$(link-status)', 'hotspot_status',
'toolbar=0,location=0,directories=0,status=0,menubars=0,resizable=1,width=290,height=2
00');
        $(endif)
//      location.href = '$(link-redirect)'; ini bagian asli dari script alogin.html
        location.href = 'http://www.istanaku.biz';
    }
//-->
</script>
</head>
<body onLoad="startClock()">
<table width="100%" height="100%">
<tr>
    <td align="center" valign="middle">
        You are logged in
        <br><br>
//      If nothing happens, click <a href="$(link-redirect)">here</a></td>n ini bagian
asli dari script alogin.html
        If nothing happens, click <a href="http://www.istanaku.biz/">here</a></td>
</tr>

```

### “About PING”

Sebagai contoh, ada 2 host yang berbeda network seperti gambar dibawah:

Host A ————— Lab A ————— Host B

# (192.168.0.1)

(192.168.0.7) (192.168.10.3)

Ping (singkatan dari Packet Internet Groper) adalah sebuah program utilitas yang digunakan untuk memeriksa konektivitas jaringan berbasis teknologi Transmission Control Protocol/Internet Protocol (TCP/IP). Dengan menggunakan utilitas ini, dapat diuji apakah sebuah komputer terhubung dengan komputer lainnya. Hal ini dilakukan dengan cara mengirim sebuah paket kepada alamat IP yang hendak diujicoba konektivitasnya dan menunggu respons darinya. Nama “ping” datang dari sonar sebuah kapal selam yang sedang aktif, yang sering mengeluarkan bunyi ping ketika menemukan sebuah objek.

Ping sendiri awalnya diciptakan oleh Mike Muuss, pada tahun 1983. Terinspirasi dengan sifar sonar kapal selam dalam menemukan suatu objek, yaitu mengirimkan sinyal sonar dan dipantulkan kembali oleh objek. Analogi dengan ping, yaitu mengirimkan paket data dan dibalas dengan paket juga.

Karena kemampuannya untuk menguji konektivitas sepasang mesin jaringan, Ping merupakan program yang powerful dalam troubleshooting jaringan. Seringkali diagnosa awal troubleshooting jaringan menggunakan program ini. Saat ini ping merupakan program standar bawaan mesin-mesin Windows, Mac, linux, BSD dan OS lainnya. Dalam pengoperasiannya, ping dapat berjalan tanpa perlu GUI, cukup diatas command line pada cmd atau terminal.

Apabila utilitas ping menunjukkan hasil yang positif maka kedua komputer tersebut saling terhubung di dalam sebuah jaringan. Hasil statistik keadaan koneksi ditampilkan dibagian akhir. Kualitas koneksi dapat dilihat dari besarnya waktu pergi-pulang (roundtrip) dan besarnya jumlah paket yang hilang (packet loss). Semakin kecil kedua angka tersebut, semakin bagus kualitas koneksinya. (id.wikipedia.org)

Pada contoh ini, seorang user di Host A melakukan ping ke alamat IP Host B. Mari kita cermati langkah demi langkah perjalanan datanya:

1. Internet Control Message Protocol (ICMP) menciptakan sebuah payload (data) permintaan echo (di mana isinya hanya abjad di field data).

2. ICMP menyerahkan payload tersebut ke Internet Protocol (IP), yang lalu menciptakan sebuah paket. Paling sedikit, paket ini berisi sebuah alamat asal IP, sebuah alamat tujuan IP, dan sebuah field protocol dengan nilai 01h (ingat bahwa Cisco suka menggunakan 0x di depan karakter heksadesimal, jadi di router mungkin terlihat seperti 0x01). Semua itu memberitahukan kepada host penerima tentang kepada siapa host penerima harus menyerahkan payload ketika network tujuan telah dicapai – pada contoh ini host menyerahkan payload kepada protocol ICMP.

3. Setelah paket dibuat, IP akan menentukan apakah alamat IP tujuan ada di network local atau network remote.

4. Karena IP menentukan bahwa ini adalah permintaan untuk network remote, maka paket perlu dikirimkan ke default gateway agar paket dapat di route ke network remote. Registry di Windows dibaca untuk mencari default gateway yang telah di konfigurasi.

5. Default gateway dari host 192.168.0.7 (Host A) dikonfigurasi ke 192.168.0.1. Untuk dapat mengirimkan paket ini ke default gateway, harus diketahui dulu alamat hardware dari interface Ethernet 0 dari router (yang dikonfigurasi dengan alamat IP 192.168.0.1 tersebut). Mengapa demikian? Agar paket dapat diserahkan ke layer data link, lalu dienkapsulasi menjadi frame, dan dikirimkan ke interface router yang terhubung ke network 192.168.0.0. Host berkomunikasi hanya dengan alamat hardware pada LAN local. Penting untuk memahami bahwa Host A, agar dapat berkomunikasi dengan Host B, harus mengirimkan paket ke alamat MAC (alamat hardware) dari default gateway di network local.

6. Setelah itu, cache ARP dicek untuk melihat apakah alamat IP dari default gateway sudah pernah di resolved (diterjemahkan) ke sebuah alamat hardware:

\* Jika sudah, paket akan diserahkan ke layer data link untuk dijadikan frame (alamat hardware dari host tujuan diserahkan bersama tersebut).

\* Jika alamat hardware tidak tersedia di cache ARP dari host, sebuah broadcast ARP akan dikirimkan ke network local untuk mencari alamat hardware dari 192.168.0.1. Router melakukan respon pada permintaan tersebut dan menyerahkan alamat hardware dari Ethernet 0, dan host akan menyimpan (cache) alamat ini. Router juga akan melakukan cache alamat hardware dari host A di cache ARP nya.

7. Setelah paket dan alamat hardware tujuan diserahkan ke layer data link, maka driver LAN akan digunakan untuk menyediakan akses media melalui jenis LAN yang digunakan (pada contoh ini adalah Ethernet). Sebuah frame dibuat, dienkapsulasi dengan informasi pengendali. Di dalam frame ini alamat hardware dari host asal dan tujuan, dalam kasus ini juga ditambah dengan field EtherType yang menggambarkan protocol layer network apa yang menyerahkan paket tersebut ke layer data link- dalam kasus ini, protocol itu adalah IP. Pada akhir dari frame itu terdapat sebuah field bernama Frame Check Sequence (FCS) yang menjadi tempat penyimpanan dari hasil perhitungan Cyclic Redundancy Check (CRC).

8. Setelah frame selesai dibuat, frame tersebut diserahkan ke layer Physical untuk ditempatkan di media fisik (pada contoh ini adalah kabel twisted-pair) dalam bentuk bit-bit, yang dikirim satu per satu.

9. Semua alat di collision domain menerima bit-bit ini dan membuat frame dari bit-bit ini. Mereka masing-masing melakukan CRC dan mengecek jawaban di field FCS. Jika jawabannya tidak cocok, frame akan dibuang.

\* Jika CRC cocok, maka alamat hardware tujuan akan di cek untuk melihat apakah alamat tersebut cocok juga (pada contoh ini, dicek apakah cocok dengan interface Ethernet 0 dari router).

\* Jika alamat hardware cocok, maka field Ether-Type dicek untuk mencari protocol yang digunakan di layer Network.

1. Paket ditarik dari frame, dan apa yang tertinggal di frame akan dibuang. Paket lalu diserahkan ke protocol yang tercatat di field Ether-Type—pada contoh ini adalah IP.

2. IP menerima paket dan mengecek alamat tujuan IP. Karena alamat tujuan dari paket tidak sesuai dengan semua alamat yang dikonfigurasi di router penerima itu sendiri, maka router penerima akan melihat pada alamat IP network tujuan di routing table-nya.

3. Routing table harus memiliki sebuah entri di network 192.168.10.0, jika tidak paket akan dibuang dengan segera dan sebuah pesan ICMP akan dikirimkan kembali ke alamat pengirim dengan sebuah pesan “destination network unreachable” (network tujuan tidak tercapai)
4. Jika router menemukan sebuah entri untuk network tujuan di tabelnya, paket akan dialihkan ke interface keluar (exit interface)—pada contoh, interface keluar ini adalah interface Ethernet 1.
5. Router akan melakukan pengalihan paket ke buffer Ethernet 1.
6. Buffer Ethernet 1 perlu mengetahui alamat hardware dari host tujuan dan pertama kali ia akan mengecek cache ARP-nya.

\* Jika alamat hardware dari Host B sudah ditemukan, paket dan alamat hardware tersebut akan diserahkan ke layer data link untuk dibuat menjadi frame.

\* Jika alamat hardware tidak pernah diterjemahkan atau di resolved oleh ARP (sehingga tidak dicatat di cache ARP), router akan mengirimkan sebuah permintaan ARP keluar dari interface E1 untuk alamat hardware 192.168.10.3.

Host B melakukan respon dengan alamat hardwarenya, dan paket beserta alamat hardware tujuan akan dikirimkan ke layer data link untuk dijadikan frame.

1. Layer data link membuat sebuah frame dengan alamat hardware tujuan dan asal, field Ether-Type, dan field FCS di akhir dari frame. Frame diserahkan ke layer Physical untuk dikirimkan keluar pada medium fisik dalam bentuk bit yang dikirimkan satu per satu.
2. Host B menerima frame dan segera melakukan CRC. Jika hasil CRC sesuai dengan apa yang ada di field FCS, maka alamat hardware tujuan akan dicek. Jika alamat host juga cocok, field Ether-Type akan di cek untuk menentukan protocol yang akan disertai paket tersebut di layer Network—Pada contoh ini, protocol tersebut adalah IP.

saya ingin mengaplikasikan connection limit per client untuk mengatasi client yg menggunakan download manager. Code:

```
/ip firewall chain=forward in-interface=client protocol=tcp tcp-flags=syn
connection-limit=11,32 action=drop
```

untuk saat ini saya menggunakan 11 dengan asumsi memperbolehkan koneksi aktif sebanyak 10 koneksi. Saya merasa 10 koneksi tersebut masih terlalu tinggi namun untuk menurunkan angkanya, saya takut akan mengurangi kenyamanan user.

## Perintah Dasar Mikrotik OS

Perintah mikrotik sebenarnya hampir sama dengan perintah yang ada di linux, sebab pada dasarnya mikrotik ini merupakan kernel Linux, hasil pengolahan kembali Linux dari Distribusi Debian. Pemakaian perintah shellnya sama, 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. Baiklah kita lanjutkan pengenalan perintah ini. Setelah login, cek kondisi interface atau ethernet card.

–[1]– 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

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 namanya), 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

–[2]– Mengganti password default

Untuk keamanan ganti password default

```
[admin@Mikrotik] > password
```

```
old password: *****
```

```
new password: *****
```

```
retype new password: *****
```

–[3]– Mengganti nama hostname

Mengganti nama Mikrotik Router untuk memudahkan konfigurasi, pada langkah ini nama server akan diganti menjadi “routerku”

```
[admin@Mikrotik] > system identity set name=routerku
```

–[4]– Setting IP Address, Gateway, Masquareade dan Name Server

–[4.1]– IP Address

Bentuk Perintah konfigurasi

```
ip address add address={ip address/netmask} interface={nama interface}
```

a. Memberikan IP address pada interface Mikrotik. Misalkan Public akan kita gunakan untuk koneksi ke Internet dengan IP 192.168.1.2 dan Local akan kita gunakan untuk network LAN kita dengan IP 192.168.0.30 (Lihat topologi)

```
[admin@routerku] > ip address add address=192.168.1.2 \
```

```
netmask=255.255.255.0 interface=Public comment=”IP ke Internet”
```

```
[admin@routerku] > ip address add address=192.168.0.30 \
```

```
netmask=255.255.255.224 interface=Local comment = “IP ke LAN”
```

b. Melihat konfigurasi IP address yang sudah kita berikan

```
[admin@routerku] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK BROADCAST INTERFACE
0 ;; IP Address ke Internet
192.168.0.30/27 192.168.0.0 192.168.0.31 Local
1 ;; IP Address ke LAN
192.168.1.2/24 192.168.0.0 192.168.1.255 Public
```

–[4.2]– Gateway

Bentuk Perintah Konfigurasi ip route add gateway={ip gateway}

a. Memberikan default Gateway, diasumsikan gateway untuk koneksi internet adalah 192.168.1.1

```
[admin@routerku] > /ip route add gateway=192.168.1.1
```

b. Melihat Tabel routing pada Mikrotik Routers

```
[admin@routerku] > 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 192.168.0.0/24 192.168.0.30 Local
1 ADC 192.168.0.0/27 192.168.1.2 Public
2 A S 0.0.0.0/0 r 192.168.1.1 Public
[admin@routerku]>
```

c. Tes Ping ke Gateway untuk memastikan konfigurasi sudah benar

```
[admin@routerku] > ping 192.168.1.1
192.168.1.1 64 byte ping: ttl=64 time<1 ms
192.168.1.1 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
```

–[4.3]– NAT (Network Address Translation)

Bentuk Perintah Konfigurasi

ip firewall nat add chain=srcnat action=masquerade out-interface={ethernet yang langsung terhubung ke Internet atau Public}

a. Setup Masquerading, Jika Mikrotik akan kita gunakan sebagai gateway server maka agar client computer pada network dapat terkoneksi ke internet perlu kita masquerading.

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

b. Melihat konfigurasi Masquerading

```
[admin@routerku] ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=srcnat out-interface=Public action=masquerade
```

–[4.4] Name server

Bentuk Perintah Konfigurasi

```
ip dns set primary-dns={dns utama} secondary-dns={dns ke dua}
```

a. Setup DNS pada Mikrotik Routers, misalkan DNS dengan Ip Addressnya  
Primary = 202.134.0.155, Secondary = 202.134.2.5

```
[admin@routerku] > ip dns set primary-dns=202.134.0.155 allow-remoterequests=yes
[admin@routerku] > ip dns set secondary-dns=202.134.2.5 allow-remoterequests=yes
```

b. Melihat konfigurasi DNS

```
[admin@routerku] > ip dns print
primary-dns: 202.134.0.155
secondary-dns: 202.134.2.5
allow-remote-requests: no
cache-size: 2048KiB
cache-max-ttl: 1w
cache-used: 16KiB
```

c. Tes untuk akses domain, misalnya dengan ping nama domain

```
[admin@routerku] > 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.

Setelah langkah ini bisa dilakukan pemeriksaan untuk koneksi dari jaringan local. Dan jika berhasil berarti kita sudah berhasil melakukan instalasi Mikrotik Router sebagai Gateway server. Setelah terkoneksi dengan jaringan Mikrotik dapat dimanage menggunakan WinBox yang bisa di download dari Mikrotik.com atau dari server mikrotik kita. Misal Ip address server mikrotik kita 192.168.0.30, via browser buka <http://192.168.0.30>. Di Browser akan ditampilkan dalam bentuk web dengan beberapa menu, cari tulisan Download dan download WinBox dari situ. Simpan di local harddisk. Jalankan Winbox, masukkan Ip address, username dan password.

–[5]– DHCP Server

DHCP merupakan singkatan dari Dynamic Host Configuration Protocol, yaitu suatu program yang memungkinkan pengaturan IP Address di dalam sebuah jaringan dilakukan terpusat di server, sehingga PC Client tidak perlu melakukan konfigurasi IP Address. DHCP memudahkan administrator untuk melakukan pengalamatan ip address untuk client.

Bentuk perintah konfigurasi

ip dhcp-server setup  
dhcp server interface = { interface yang digunakan }  
dhcp server space = { network yang akan di dhcp }  
gateway for dhcp network = { ip gateway }  
address to give out = { range ip address }  
dns servers = { name server }  
lease time = { waktu sewa yang diberikan }

Jika kita menginginkan client mendapatkan IP address secara otomatis maka perlu kita setup dhcp server pada Mikrotik. Berikut langkah-langkahnya :

a. Tambahkan IP address pool

```
/ip pool add name=dhcp-pool ranges=192.168.0.1-192.168.0.30
```

b. Tambahkan DHCP Network dan gatewaynya yang akan didistribusikan ke client.  
Pada contoh ini networknya adalah 192.168.0.0/27 dan gatewaynya 192.168.0.30

```
/ip dhcp-server network add address=192.168.0.0/27 gateway=192.168.0.30 dns-server=192.168.0.30 \
comment=""
```

c. Tambahkan DHCP Server ( pada contoh ini dhcp diterapkan pada interface Local )

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

d. Lihat status DHCP server

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

Flags: X - disabled, I - invalid

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

```
0dhcp1 Local
```

Tanda X menyatakan bahwa DHCP server belum enable maka perlu dienablekan terlebih dahulu pada langkah e.

e. Jangan Lupa dibuat enable dulu dhcp servernya

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

kemudian cek kembali dhcp-server seperti langkah 4, jika tanda X sudah tidak ada berarti sudah aktif

f. Tes Dari client

Misalnya : D:\>ping www.yahoo.com

–[6]– Transparent Proxy Server

Proxy server merupakan program yang dapat mempercepat akses ke suatu web yang sudah diakses oleh komputer lain, karena sudah di simpan didalam caching server.Transparent proxy menguntungkan dalam



management client, karena system administrator tidak perlu lagi melakukan setup proxy di setiap browser komputer client karena redirection dilakukan otomatis di sisi server.

Bentuk perintah konfigurasi :

a. Setting web proxy :

```
- ip proxy set enable=yes
port={ port yang mau digunakan }
maximal-client-connections=1000
maximal-server-connections=1000

- ip proxy direct add src-address={ network yang akan di NAT } action=allow

- ip web-proxy set parent-proxy={proxy parent/optional}
hostname={ nama host untuk proxy/optional}
port={port yang mau digunakan}
src-address={ address yang akan digunakan untuk koneksi ke parent proxy/default 0.0.0.0}
transparent-proxy=yes
max-object-size={ ukuran maximal file yang akan disimpan sebagai cache/default 4096 in Kilobytes}
max-cache-size= { ukuran maximal hardisk yang akan dipakai sebagai penyimpanan file cache/unlimited
| none | 12 in megabytes}
cache-administrator={ email administrator yang akan digunakan apabila proxy error, status akan dikirim ke
email tersebut}
enable==yes
```

Contoh konfigurasi

a. Web proxy setting

```
/ ip web-proxy
set enabled=yes src-address=0.0.0.0 port=8080 \
hostname="proxy.routerku.co.id" transparent-proxy=yes \
parent-proxy=0.0.0.0:0 cache-administrator="support@routerku.co.id" \
max-object-size=131072KiB cache-drive=system max-cache-size=unlimited \
max-ram-cache-size=unlimited
```

Nat Redirect, perlu ditambahkan yaitu rule REDIRECTING untuk membelokkan traffic HTTP menuju ke WEB-PROXY.

b. Setting firewall untuk Transparant Proxy

Bentuk perintah konfigurasi :

```
ip firewall nat add chain=dstnat protocol=tcp dst-port=80 action=redirect to-ports={ port proxy }
```

Perintahnya:

```
/ ip firewall nat
add chain=dstnat protocol=tcp dst-port=80 action=redirect to-ports=8080 \ comment="" disabled=no
add chain=dstnat protocol=tcp dst-port=3128 action=redirect to-ports=8080 \ comment="" disabled=no
add chain=dstnat protocol=tcp dst-port=8000 action=redirect to-ports=8080 \
```

perintah diatas dimaksudkan, agar semua trafik yang menuju Port 80,3128,8000 dibelokkan menuju port 8080 yaitu portnya Web-Proxy.

## CATATAN: Perintah

```
/ip web-proxy print { untuk melihat hasil konfigurasi web-proxy}  
/ip web-proxy monitor { untuk monitoring kerja web-proxy}
```

## –[7]– Bandwidth Management

QoS memegang peranan sangat penting dalam hal memberikan pelayanan yang baik pada client. Untuk itu kita memerlukan bandwidth management untuk mengatur tiap data yang lewat, sehingga pembagian bandwidth menjadi adil. Dalam hal ini Mikrotik RouterOs juga menyertakan packet software untuk manajemen bandwidth.

Bentuk perintah konfigurasi:

```
queue simple add name={ nama }  
target-addresses={ ip address yang dituju }  
interface={ interface yang digunakan untuk melewati data }  
max-limit={ out/in }
```

Dibawah ini terdapat konfigurasi Trafik shaping atau bandwidth management dengan metode Simple Queue, sesuai namanya, Jenis Queue ini memang sederhana, namun memiliki kelemahan, kadangkala terjadi kebocoran bandwidth atau bandwidthnya tidak secara real di monitor. Pemakaian untuk 10 Client, Queue jenis ini tidak masalah.

Diasumsikan Client ada sebanyak 15 client, dan masing-masing client diberi jatah bandwidth minimum sebanyak 8kbps, dan maksimum 48kbps. Sedangkan Bandwidth totalnya sebanyak 192kbps. Untuk upstream tidak diberi rule, berarti masing-masing client dapat menggunakan bandwidth upstream secara maksimum. Perhatikan perintah priority, range priority di Mikrotik sebanyak delapan. Berarti dari 1 sampai 8, priority 1 adalah priority tertinggi, sedangkan priority 8 merupakan priority terendah.

Berikut Contoh konfigurasinya.

---

```
/ queue simple  
add name="trafikshaping" target-addresses=192.168.0.0/27 dst-address=0.0.0.0/0 \  
interface=all parent=none priority=1 queue=default/default \  
limit-at=0/64000 max-limit=0/192000 total-queue=default disabled=no  
add name="01" target-addresses=192.168.0.1/32 dst-address=0.0.0.0/0 \  
interface=all parent=trafikshaping priority=1 queue=default/default \  
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no  
add name="02" target-addresses=192.168.0.2/32 dst-address=0.0.0.0/0 \  
interface=all parent=trafikshaping priority=1 queue=default/default \  
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no  
add name="03" target-addresses=192.168.0.3/32 dst-address=0.0.0.0/0 \  
interface=all parent=trafikshaping priority=1 queue=default/default \  
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no  
add name="04" target-addresses=192.168.0.4/32 dst-address=0.0.0.0/0 \  
interface=all parent=trafikshaping priority=1 queue=default/default \  
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no  
add name="10" target-addresses=192.168.0.25/32 dst-address=0.0.0.0/0 \  
interface=all parent=trafikshaping priority=1 queue=default/default \  
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no  
add name="05" target-addresses=192.168.0.5/32 dst-address=0.0.0.0/0 \  
interface=all parent=trafikshaping priority=1 queue=default/default \  

```

```

limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no
add name="06" target-addresses=192.168.0.6/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no
add name="07" target-addresses=192.168.0.7/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no
add name="08" target-addresses=192.168.0.8/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no
add name="09" target-addresses=192.168.0.9/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no
add name="10" target-addresses=192.168.0.10/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no
add name="11" target-addresses=192.168.0.11/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no
add name="12" target-addresses=192.168.0.12/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no
add name="13" target-addresses=192.168.0.13/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no
add name="14" target-addresses=192.168.0.14/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no
add name="15" target-addresses=192.168.0.15/32 dst-address=0.0.0.0/0 \
interface=all parent=trafikshaping priority=1 queue=default/default \
limit-at=0/8000 max-limit=0/48000 total-queue=default disabled=no

```

Perintah diatas karena dalam bentuk command line, bisa juga di copy paste, selanjutnya di paste saja ke consol mikrotiknya. ingat lihat dulu path atau direktory aktif. Silahkan dipaste saja, kalau posisi direktorynya di Root.

Pilihan lain metode bandwidth manajemen ini, kalau seandainya ingin bandwidth tersebut dibagi sama rata oleh Mikrotik, seperti bandwidth 256kbps downstream dan 256kbps upstream. Sedangkan client yang akan mengakses sebanyak 10 client, maka otomatis masing-masing client mendapat jatah bandwidth upstream dan downstream sebanyak 256kbps dibagi 10. Jadi masing-masing dapat 25,6kbps. Andaikata hanya 2 Client yang mengakses maka masing-masing dapat 128kbps.

Untuk itu dipakai type PCQ (Per Connection Queue), yang bisa secara otomatis membagi trafik per client. Tentang jenis queue di mikrotik ini dapat dibaca pada manualnya di <http://www.mikrotik.com/testdocs/ros/2.9/root/queue.php>. Sebelumnya perlu dibuat aturan di bagian MANGLE. Seperti :

---

```

/ip firewall mangle add chain=forward src-address=192.168.0.0/27 \
action=mark-connection new-connection-mark=users-con
/ip firewall mangle add connection-mark=users-con action=mark-packet \
new-packet-mark=users chain=forward

```

Karena type PCQ belum ada, maka perlu ditambah, ada 2 type PCQ ini. Pertama diberi nama pcq-download, yang akan mengatur semua trafik melalui alamat tujuan/destination address. Trafik ini melewati interface Local. Sehingga semua trafik download/downstream yang datang dari jaringan 192.168.0.0/27 akan dibagi secara otomatis.

Tipe PCQ kedua, dinamakan pcq-upload, untuk mengatur semua trafik upstream yang berasal dari alamat asal/source address. Trafik ini melewati interface public. Sehingga semua trafik upload/upstream yang berasal dari jaringan 192.168.0.0/27 akan dibagi secara otomatis.

Perintah:

---

```
/queue type add name=pcq-download kind=pcq pcq-classifier=dst-address  
/queue type add name=pcq-upload kind=pcq pcq-classifier=src-address
```

---

Setelah aturan untuk PCQ dan Mangle ditambahkan, sekarang untuk aturan pembagian trafiknya. Queue yang dipakai adalah Queue Tree, Yaitu:

---

```
/queue tree add parent=Local queue=pcq-download packet-mark=users  
/queue tree add parent=Public queue=pcq-upload packet-mark=users
```

---

Perintah diatas mengasumsikan, kalau bandwidth yang diterima dari provider Internet berfluktuasi atau berubah-ubah. Jika kita yakin bahwa bandwidth yang diterima, misalkan dapat 256kbs downstream, dan 256kbps upstream, maka ada lagi aturannya, seperti :

Untuk trafik downstreamnya :

---

```
/queue tree add name=Download parent=Local max-limit=256k  
/queue tree add parent=Download queue=pcq-download packet-mark=users
```

Dan trafik upstreamnya :

---

```
/queue tree add name=Upload parent=Public max-limit=256k  
/queue tree add parent=Upload queue=pcq-upload packet-mark=users
```

–[8]– Monitor MRTG via Web

Fasilitas ini diperlukan untuk monitoring trafik dalam bentuk grafik, dapat dilihat dengan menggunakan browser. MRTG (The Multi Router Traffic Grapher) telah dibuild sedemikian rupa, sehingga memudahkan kita memakainya. Telah tersedia dipaket dasarnya.

Contoh konfigurasinya

```
/ tool graphing  
set store-every=5min  
/ tool graphing interface  
add interface=all allow-address=0.0.0.0/0 store-on-disk=yes disabled=no
```

Perintah diatas akan menampilkan grafik dari trafik yang melewati interface jaringan baik berupa Interface Public dan Interface Local, yang dirender setiap 5 menit sekali. Juga dapat diatur Alamat apa saja yang dapat mengakses MRTG ini, pada parameter allow-address.

Setelah beberapa Konfigurasi diatas telah disiapkan, tentu tidak lupa kita perhatikan keamanan dari Mesin gateway Mikrotik ini, ada beberapa fasilitas yang dipergunakan. Dalam hal ini akan dibahas tentang Firewallnya. Fasilitas Firewall ini secara prinsip serupa dengan IP TABLES di Gnu/Linux hanya saja beberapa perintah telah di sederhanakan namun berdaya guna.

Di Mikrotik perintah firewall ini terdapat dalam modus IP, yaitu

```
[admin@routerku] > /ip firewall
```

Terdapat beberapa packet filter seperti mangle, nat, dan filter.

```
[admin@routerku] ip firewall> ?
```

Firewall allows IP packet filtering on per packet basis.

```
.. — go up to ip
mangle/ — The packet marking management
nat/ — Network Address Translation
connection/ — Active connections
filter/ — Firewall filters
address-list/ —
service-port/ — Service port management
export —
```

Untuk kali ini kita akan lihat konfigurasi pada ip firewall filternya.

Karena Luasnya parameter dari firewall filter ini untuk pembahasan Firewall Filter selengkapnya dapat dilihat pada manual mikrotik, di <http://www.mikrotik.com/testdocs/ros/2.9/ip/filter.php>

Konfigurasi dibawah ini dapat memblokir beberapa Trojan, Virus, Backdoor yang telah dikenali sebelumnya baik Nomor Port yang dipakai serta Protokolnya. Juga telah di konfigurasikan untuk menahan Flooding dari Jaringan Publik dan jaringan Lokal. Serta pemberian rule untuk Access control agar, Rentang jaringan tertentu saja yang bisa melakukan Remote atau mengakses service tertentu terhadap Mesin Mikrotik kita.

#### Contoh Aplikasi Filternya

---

```
/ ip firewall filter
add chain=input connection-state=invalid action=drop comment="Drop Invalid \
connections" disabled=no
add chain=input src-address=!192.168.0.0/27 protocol=tcp src-port=1024-65535 \
dst-port=8080 action=drop comment="Block to Proxy" disabled=no
add chain=input protocol=udp dst-port=12667 action=drop comment="Trinoo" \ disabled=no
add chain=input protocol=udp dst-port=27665 action=drop comment="Trinoo" \ disabled=no
add chain=input protocol=udp dst-port=31335 action=drop comment="Trinoo" \ disabled=no
add chain=input protocol=udp dst-port=27444 action=drop comment="Trinoo" \ disabled=no
add chain=input protocol=udp dst-port=34555 action=drop comment="Trinoo" \ disabled=no
add chain=input protocol=udp dst-port=35555 action=drop comment="Trinoo" \ disabled=no
add chain=input protocol=tcp dst-port=27444 action=drop comment="Trinoo" \ disabled=no
add chain=input protocol=tcp dst-port=27665 action=drop comment="Trinoo" \ disabled=no
add chain=input protocol=tcp dst-port=31335 action=drop comment="Trinoo" \ disabled=no
```

```
add chain=input protocol=tcp dst-port=31846 action=drop comment="Trinoo" \ disabled=no
add chain=input protocol=tcp dst-port=34555 action=drop comment="Trinoo" \ disabled=no
add chain=input protocol=tcp dst-port=35555 action=drop comment="Trinoo" \ disabled=no
add chain=input connection-state=established action=accept comment="Allow \
Established connections" disabled=no
add chain=input protocol=udp action=accept comment="Allow UDP" disabled=no
add chain=input protocol=icmp action=accept comment="Allow ICMP" disabled=no
add chain=input src-address=192.168.0.0/27 action=accept comment="Allow access \
to router from known network" disabled=no
add chain=input action=drop comment="Drop anything else" disabled=no
add chain=forward protocol=tcp connection-state=invalid action=drop \
comment="drop invalid connections" disabled=no
add chain=forward connection-state=established action=accept comment="allow \
already established connections" disabled=no
add chain=forward connection-state=related action=accept comment="allow \
related connections" disabled=no
add chain=forward src-address=0.0.0.0/8 action=drop comment="" disabled=no
add chain=forward dst-address=0.0.0.0/8 action=drop comment="" disabled=no
add chain=forward src-address=127.0.0.0/8 action=drop comment="" disabled=no
add chain=forward dst-address=127.0.0.0/8 action=drop comment="" disabled=no
add chain=forward src-address=224.0.0.0/3 action=drop comment="" disabled=no
add chain=forward dst-address=224.0.0.0/3 action=drop comment="" disabled=no
add chain=forward protocol=tcp action=jump jump-target=tcp comment="" \ disabled=no
add chain=forward protocol=udp action=jump jump-target=udp comment="" \ disabled=no
add chain=forward protocol=icmp action=jump jump-target=icmp comment="" \ disabled=no
add chain=tcp protocol=tcp dst-port=69 action=drop comment="deny TFTP" \ disabled=no
add chain=tcp protocol=tcp dst-port=111 action=drop comment="deny RPC \ portmapper" disabled=no
add chain=tcp protocol=tcp dst-port=135 action=drop comment="deny RPC \ portmapper" disabled=no
add chain=tcp protocol=tcp dst-port=137-139 action=drop comment="deny NBT" \ disabled=no
add chain=tcp protocol=tcp dst-port=445 action=drop comment="deny cifs" \ disabled=no
add chain=tcp protocol=tcp dst-port=2049 action=drop comment="deny NFS" \ disabled=no
add chain=tcp protocol=tcp dst-port=12345-12346 action=drop comment="deny \ NetBus" disabled=no
add chain=tcp protocol=tcp dst-port=20034 action=drop comment="deny NetBus" \ disabled=no
add chain=tcp protocol=tcp dst-port=3133 action=drop comment="deny \ BackOrifice" disabled=no
add chain=tcp protocol=tcp dst-port=67-68 action=drop comment="deny DHCP" \ disabled=no
add chain=udp protocol=udp dst-port=69 action=drop comment="deny TFTP" \ disabled=no
add chain=udp protocol=udp dst-port=111 action=drop comment="deny PRC \ portmapper" disabled=no
add chain=udp protocol=udp dst-port=135 action=drop comment="deny PRC \ portmapper" disabled=no
add chain=udp protocol=udp dst-port=137-139 action=drop comment="deny NBT" \ disabled=no
add chain=udp protocol=udp dst-port=2049 action=drop comment="deny NFS" \ disabled=no
add chain=udp protocol=udp dst-port=3133 action=drop comment="deny \ BackOrifice" disabled=no
add chain=input protocol=tcp psd=21,3s,3,1 action=add-src-to-address-list \
address-list="port scanners" address-list-timeout=2w comment="Port \ scanners to list " disabled=no
add chain=input protocol=tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg \
action=add-src-to-address-list address-list="port scanners" \
address-list-timeout=2w comment="NMAP FIN Stealth scan" disabled=no
add chain=input protocol=tcp tcp-flags=fin,syn action=add-src-to-address-list \
address-list="port scanners" address-list-timeout=2w comment="SYN/FIN \ scan" disabled=no
add chain=input protocol=tcp tcp-flags=syn,rst action=add-src-to-address-list \
address-list="port scanners" address-list-timeout=2w comment="SYN/RST \ scan" disabled=no
add chain=input protocol=tcp tcp-flags=fin,psh,urg,!syn,!rst,!ack \
action=add-src-to-address-list address-list="port scanners" \
address-list-timeout=2w comment="FIN/PSH/URG scan" disabled=no
```

```

add chain=input protocol=tcp tcp-flags=fin,syn,rst,psh,ack,urg \
action=add-src-to-address-list address-list="port scanners" \
address-list-timeout=2w comment="ALL/ALL scan" disabled=no
add chain=input protocol=tcp tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg \
action=add-src-to-address-list address-list="port scanners" \
address-list-timeout=2w comment="NMAP NULL scan" disabled=no
add chain=input src-address-list="port scanners" action=drop comment="dropping \
port scanners" disabled=no
add chain=icmp protocol=icmp icmp-options=0:0 action=accept comment="drop \
invalid connections" disabled=no
add chain=icmp protocol=icmp icmp-options=3:0 action=accept comment="allow \
established connections" disabled=no
add chain=icmp protocol=icmp icmp-options=3:1 action=accept comment="allow \
already established connections" disabled=no
add chain=icmp protocol=icmp icmp-options=4:0 action=accept comment="allow \
source quench" disabled=no
add chain=icmp protocol=icmp icmp-options=8:0 action=accept comment="allow \
echo request" disabled=no
add chain=icmp protocol=icmp icmp-options=11:0 action=accept comment="allow \
time exceed" disabled=no
add chain=icmp protocol=icmp icmp-options=12:0 action=accept comment="allow \
parameter bad" disabled=no
add chain=icmp action=drop comment="deny all other types" disabled=no
add chain=tcp protocol=tcp dst-port=25 action=reject \
reject-with=icmp-network-unreachable comment="Sntp" disabled=no
add chain=tcp protocol=udp dst-port=25 action=reject \
reject-with=icmp-network-unreachable comment="Sntp" disabled=no
add chain=tcp protocol=tcp dst-port=110 action=reject \
reject-with=icmp-network-unreachable comment="Sntp" disabled=no
add chain=tcp protocol=udp dst-port=110 action=reject \
reject-with=icmp-network-unreachable comment="Sntp" disabled=no
add chain=tcp protocol=udp dst-port=110 action=reject \
reject-with=icmp-network-unreachable comment="Sntp" disabled=no

```

#### –[10.1]– Service dan Melihat Service yang Aktif dengan PortScanner

Untuk memastikan Service apa saja yang aktif di Mesin mikrotik, perlu kita pindai terhadap port tertentu, seandainya ada service yang tidak dibutuhkan, sebaiknya dimatikan saja.

Untuk menonaktifkan dan mengaktifkan servise, perintah adalah : Kita periksa dahulu service apa saja yang aktif

```

[admin@routerku] > ip service
[admin@routerku] ip service> print
Flags: X - disabled, I - invalid
#  NAME                PORT ADDRESS      CERTIFICATE
0 X telnet             23  0.0.0.0/0
1  ftp                 21  0.0.0.0/0
2  www                 80  0.0.0.0/0
3  ssh                 22  0.0.0.0/0
4  www-ssl             443 0.0.0.0/0      none

```

Misalkan service FTP akan dinonaktifkan, yaitu di daftar diatas terletak pada nomor 1 (lihat bagian Flags) maka : [admin@routerku] ip service> set 1 disabled=yes

Perlu kita periksa lagi,

```
[admin@routerku] ip service> print
Flags: X - disabled, I - invalid
#  NAME                PORT ADDRESS      CERTIFICATE
0 X telnet             23  0.0.0.0/0
1 X ftp                21  0.0.0.0/0
2  www                 80  0.0.0.0/0
3  ssh                 22  0.0.0.0/0
4  www-ssl             443 0.0.0.0/0      none
```

Sekarang service FTP telah dinonaktifkan. Dengan memakai tool nmap kita dapat mengecek port apa saja yang aktif pada mesin gateway yang telah dikonfigurasi.

Perintah : nmap -vv -sS -sV -P0 192.168.0.30

Hasil :

```
Starting Nmap 4.20 ( http://insecure.org ) at 2007-04-04 19:55 SE Asia Standard Time
Initiating ARP Ping Scan at 19:55
Scanning 192.168.0.30 [1 port]
Completed ARP Ping Scan at 19:55, 0.31s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:55
Completed Parallel DNS resolution of 1 host. at 19:55, 0.05s elapsed
Initiating SYN Stealth Scan at 19:55
Scanning 192.168.0.30 [1697 ports]
Discovered open port 22/tcp on 192.168.0.30
Discovered open port 53/tcp on 192.168.0.30
Discovered open port 80/tcp on 192.168.0.30
Discovered open port 21/tcp on 192.168.0.30
Discovered open port 3986/tcp on 192.168.0.30
Discovered open port 2000/tcp on 192.168.0.30
Discovered open port 8080/tcp on 192.168.0.30
Discovered open port 3128/tcp on 192.168.0.30
Completed SYN Stealth Scan at 19:55, 7.42s elapsed (1697 total ports)
Initiating Service scan at 19:55
Scanning 8 services on 192.168.0.30
Completed Service scan at 19:57, 113.80s elapsed (8 services on 1 host)
Host 192.168.0.30 appears to be up ... good.
Interesting ports on 192.168.0.30:
Not shown: 1689 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          MikroTik router ftpd 2.9.27
22/tcp    open  ssh          OpenSSH 2.3.0 mikrotik 2.9.27 (protocol 1.99)
53/tcp    open  domain?
80/tcp    open  http         MikroTik router http config
2000/tcp  open  callbook?
3128/tcp  open  http-proxy   Squid webproxy 2.5.STABLE11
3986/tcp  open  mapper-ws_ethd?
8080/tcp  open  http-proxy   Squid webproxy 2.5.STABLE11
```



2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at <http://www.insecure.org/cgi-bin/servicefp-submit.cgi> :

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====

SF-Port53-TCP:V=4.20%I=7%D=4/4%Time=4613A03C%P=i686-pc-windows-windows%r(D  
SF:NSVersionBindReq,E,"\\0\\x0c\\0\\x06\\x81\\x84\\0\\0\\0\\0\\0\\0")%r(DNSStatusR  
SF:equest,E,"\\0\\x0c\\0\\0\\x90\\x84\\0\\0\\0\\0\\0\\0");

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====

SF-Port2000-TCP:V=4.20%I=7%D=4/4%Time=4613A037%P=i686-pc-windows-windows%r  
SF:(NULL,4,"\\x01\\0\\0\\0")%r(GenericLines,4,"\\x01\\0\\0\\0")%r(GetRequest,18,"\\  
SF:x01\\0\\0\\0\\x02\\0\\0\\0d\\?\\xe4{\\x9d\\x02\\x1a\\xcc\\x8b\\xd1V\\xb2F\\xff9\\xb0")%r(  
SF:HTTPOptions,18,"\\x01\\0\\0\\0\\x02\\0\\0\\0d\\?\\xe4{\\x9d\\x02\\x1a\\xcc\\x8b\\xd1V\\x  
SF:b2F\\xff9\\xb0")%r(RTSPRequest,18,"\\x01\\0\\0\\0\\x02\\0\\0\\0d\\?\\xe4{\\x9d\\x02\\x  
SF:1a\\xcc\\x8b\\xd1V\\xb2F\\xff9\\xb0")%r(RPCCheck,18,"\\x01\\0\\0\\0\\x02\\0\\0\\0d\\?  
SF:\\xe4{\\x9d\\x02\\x1a\\xcc\\x8b\\xd1V\\xb2F\\xff9\\xb0")%r(DNSVersionBindReq,18,"\\  
SF:x01\\0\\0\\0\\x02\\0\\0\\0d\\?\\xe4{\\x9d\\x02\\x1a\\xcc\\x8b\\xd1V\\xb2F\\xff9\\xb0")%r(  
SF:DNSStatusRequest,4,"\\x01\\0\\0\\0")%r(Help,4,"\\x01\\0\\0\\0")%r(X11Probe,4,"\\  
SF:x01\\0\\0\\0")%r(FourOhFourRequest,18,"\\x01\\0\\0\\0\\x02\\0\\0\\0\\xb9\\x15&\\xf1A\\  
SF:]+\\x11\\n\\xf6\\x9b\\xa0,\\xb0\\xe1\\xa5")%r(LPDString,4,"\\x01\\0\\0\\0")%r(LDAP  
SF:BindReq,4,"\\x01\\0\\0\\0")%r(LANDesk-RC,18,"\\x01\\0\\0\\0\\x02\\0\\0\\0\\xb9\\x15&\\  
SF:\\xf1A\\]+\\x11\\n\\xf6\\x9b\\xa0,\\xb0\\xe1\\xa5")%r(TerminalServer,4,"\\x01\\0\\0\\  
SF:0")%r(NCP,18,"\\x01\\0\\0\\0\\x02\\0\\0\\0\\xb9\\x15&\\xf1A\\]+\\x11\\n\\xf6\\x9b\\xa0,  
SF:\\xb0\\xe1\\xa5")%r(NotesRPC,18,"\\x01\\0\\0\\0\\x02\\0\\0\\0\\xb9\\x15&\\xf1A\\]+\\x1  
SF:1\\n\\xf6\\x9b\\xa0,\\xb0\\xe1\\xa5")%r(NessusTPv10,4,"\\x01\\0\\0\\0");  
MAC Address: 00:90:4C:91:77:02 (Epigram)  
Service Info: Host: routerku; Device: router

Service detection performed. Please report any incorrect results at <http://insecure.org/nmap/submit/> .

Nmap finished: 1 IP address (1 host up) scanned in 123.031 seconds  
Raw packets sent: 1706 (75.062KB) | Rcvd: 1722 (79.450KB)

Dari hasil scanning tersebut dapat kita ambil kesimpulan, bahwa service dan port yang aktif adalah FTP dalam versi MikroTik router ftpd 2.9.27. Untuk SSH dengan versi OpenSSH 2.3.0 mikrotik 2.9.27 (protocol 1.99). Serta Web proxy memakai Squid dalam versi Squid webproxy 2.5.STABLE11.

Tentu saja pihak vendor mikrotik telah melakukan patch terhadap Hole atau Vulnerabilities dari Versi Protocol diatas.

## –[10.2]– Tool administrasi Jaringan

Secara praktis terdapat beberapa tool yang dapat dimanfaatkan dalam melakukan troubleshooting jaringan, seperti tool ping, traceroute, SSH, dll. Beberapa tool yang sering digunakan nantinya dalam administrasi sehari-hari adalah :

- o Telnet
- o SSH
- o Traceroute
- o Sniffer

### a. Telnet

Perintah remote mesin ini hampir sama penggunaan dengan telnet yang ada di Linux atau Windows.

```
[admin@routerku] > system telnet ?
```

Perintah diatas untuk melihat sekilas paramater apa saja yang ada. Misalnya mesin remote dengan ip address 192.168.0.21 dan port 23. Maka

```
[admin@routerku] > system telnet 192.168.0.21
```

Penggunaan telnet sebaiknya dibatasi untuk kondisi tertentu dengan alasan keamanan, seperti kita ketahui, packet data yang dikirim melalui telnet belum di enkripsi. Agar lebih amannya kita pergunakan SSH.

#### b. SSH

Sama dengan telnet perintah ini juga diperlukan dalam remote mesin, serta pringsipnya sama juga parameternya dengan perintah di Linux dan Windows.

```
[admin@routerku] > system ssh 192.168.0.21
```

Parameter SSH diatas, sedikit perbedaan dengan telnet. Jika lihat helpnya memiliki parameter tambahan yaitu user.

```
[admin@routerku] > system ssh ?
```

The SSH feature can be used with various SSH Telnet clients to securely connect to and administrate the router

<address> –

user — User name

port — Port number

Misalkan kita akan melakukan remote pada suatu mesin dengan sistem operasinya Linux, yang memiliki Account, username Root dan Password 123456 pada Address 66.213.7.30. Maka perintahnya,

```
[admin@routerku] > system ssh 66.213.7.30 user=root  
root@66.213.7.30's password:
```

#### c. Traceroute

Mengetahui hops atau router apa saja yang dilewati suatu packet sampai packet itu terkirim ke tujuan, lazimnya kita menggunakan traceroute. Dengan tool ini dapat di analisa kemana saja route dari jalannya packet. Misalkan ingin mengetahui jalannya packet yang menuju server yahoo, maka:

```
[admin@routerku] > tool traceroute yahoo.com ADDRESS STATUS
```

```
1 63.219.6.nnn 00:00:00 00:00:00 00:00:00  
2 222.124.4.nnn 00:00:00 00:00:00 00:00:00  
3 192.168.34.41 00:00:00 00:00:00 00:00:00  
4 61.94.1.253 00:00:00 00:00:00 00:00:00  
5 203.208.143.173 00:00:00 00:00:00 00:00:00  
6 203.208.182.5 00:00:00 00:00:00 00:00:00  
7 203.208.182.114 00:00:00 00:00:00 00:00:00  
8 203.208.168.118 00:00:00 00:00:00 00:00:00  
9 203.208.168.134 timeout 00:00:00 00:00:00  
10 216.115.101.34 00:00:00 timeout timeout  
11 216.115.101.129 timeout timeout 00:00:00  
12 216.115.108.1 timeout timeout 00:00:00  
13 216.109.120.249 00:00:00 00:00:00 00:00:00  
14 216.109.112.135 00:00:00 timeout timeout
```

#### d. Sniffer

Kita dapat menangkap dan menyadap packet-packet yang berjalan di jaringan kita, tool ini telah disediakan oleh Mikrotik yang berguna dalam menganalisa trafik.

```
[admin@routerku] > tool sniffer  
Packet sniffing
```

```
.. — go up to tool  
start — Start/reset sniffing  
stop — Stop sniffing  
save — Save currently sniffed packets  
packet/ — Sniffed packets management  
protocol/ — Protocol management  
host/ — Host management  
connection/ — Connection management  
print —  
get — get value of property  
set —  
edit — edit value of property  
export —
```

Untuk memulai proses sniffing dapat menggunakan perintah Start, sedangkan menghentikannya dapat menggunakan perintah Stop.

```
[admin@routerku] > tool sniffer start
```

Kalo hotspot: bikin script shutdown...

Code:

```
/system script add name="mati" source={/system shutdown}
```

trus bikin profile baru yang njalanin script shutdown kalo dia login

Code:

```
/ip hotspot user profile add copy-from="default" name="matikan" on-login=mati
```

trus bikin user yang pake profile tersebut

Code:

```
/ip hotspot user add name="user1" password="pass1" profile=matikan
```

---

rekan2 sekalian..

mau tanya dong, ada yg udah pernah bikin script untuk remove wireless registration table ketika throughput <100kbps?

soalnya lagi musim hujan, beberapa antena di klien goyang2.. (klien rumahan dengan pipa besi saja) nah, akibatnya koneksi untuk semua klien ikut2an hancur..

ketika client yg bermasalah tersebut kita remove dari registration table, koneksi menjadi bagus kembali

untuk klien ybs, dan untuk semua..

thanks in advance..

JAWABAN:

Coba script ini ditaruh di scheduler:

Code:

```
/interface wireless registration-table
:if ([get [find mac-address="xx:xx:xx:xx:xx:xx"] p-throughput] < 100) do={reset
[find mac-address="xx:xx:xx:xx:xx:xx"]}
```



atau

Code:


```
/interface wireless registration-table
:if ([get [find mac-address="xx:xx:xx:xx:xx:xx"] p-throughput] < 100) do={remove
[find mac-address="xx:xx:xx:xx:xx:xx"]}
```

tapi ini belum aku coba sendiri lho, please dicobain yah...

## Another way to block web

Iseng2 aja Akang trial eror alias coba-coba siapa tahu jadi  eh..... ga tahunya bisa  harap di maklumkan juragan!! Akang masih newbie dalam per-mikrotik-an jadinya yang simple2 aja suka miss



Ternyata menggunakan fitur "content" di /ip firewall filter bisa buat blokir web (newbie abissss  ) ternyata ga perlu proxy bisa!!! Tinggal nunggu ROSv4 buat menambahkan fitur "redirect" di action... jadi

deh!!!! MANTABBBBBB  perintahnya

Code:

```
/ip fi fi add chain=forward src-address-list="daftar ip lokal yg mau dikenakan blok"
protocol=tcp content=sex/porn/hentai dsb action=drop
```