

## DAFTAR ISI – TUTORIAL MIKROTIK BAGIAN 2

---

1. [How To] Blocked Page at Web Proxy MikroTik .....	2
2. Editing Hotspot login Page .....	4
3. misahin download dan browsing? .....	6
4. Tut FullSpeed dari cache internalnya mikrotik (untuk versin 2.9) .....	7
5. Yang Pengen Block FRIENDSTER .....	10
6. Another way to block web .....	11
7. NEW Update --> Setting PPPoE dan Load Balance Speedy --NEW UPDATE-- .....	12
8. Cara setting Web proxy 3.20 .....	15
9. NGE Limit Youtube Video Streaming di MT 3.xx .....	16
10. Script Limit Bandwidth berdasar Siang – Malam .....	18
11. Simple Load Balancing + DNS Resolver + Secret Fiture .....	19
12. Blok PTP – other way .....	20
13. Login HTTPS di Hotspot .....	22
14. mengatur prioritas trafik dari dan ke mikrotik .....	24
15. Banyak Web Server di belakang router Mikrotik .....	25
16. Routerboard 450 Repaired .....	27
17. Satu (1) Userman Banyak Hotspot .....	30
18. recovery password mikrotik .....	33
19. Cara buat PPPOE server .....	34
20. misahin download dan browsing? .....	36
21. Beberapa Konfigurasi Mikrotik dan Proxy .....	38
22. Queue dengan SRC-NAT dan WEB-PROXY .....	42
23. Mikrotik - menggunakan squid sebagai web proxy sehingga lebih optimal .....	44
24. Beda Limit Siang dan Malam secara otomatis .....	47
25. Script untuk block Conflicker Virus secara otomatis .....	48
26. VLAN di RB750 (Requested by bro Hakeem) .....	51
27. Contoh Implementasi PCQ .....	54
28. Setting Bridge dan dial PPPoE dari Mikrotik .....	56
29. The NEW LoadBalance!! More Powerfull -TESTED- .....	60
30. Membuat OSPF secara sederhana .....	65
31. NETINSTALL RB750 & RB411R Melalui PXE .....	67
32. Langkah2 membuat koneksi pppoe server berbasis winbox .....	68
33. Managemen Bandwidth Mikrotik .....	79
34. Managemen Bandwidth Mikrotik (2) .....	84
35. Netinstall Mikrotik RouterOS pada RouterBoard .....	89
36. [SHARE] agar bandwidth hotspot agan nggak bisa di share kembali di client .....	94
37. [SHARE] Hacking abal-abal: Bruteforce MT =)) .....	95
38. How To Crack Mikrotik Router Version 3.20 , 3.21, dan 3.22 .....	96
39. Trap ip berdasarkan domain .....	98
40. [Share] "Anti Netcut" Work 100% (Gak ada [NETCUT] diantara kita) .....	100

### PENUTUP :

**FAQ - Terjemahan bebas dari Wiki Mikrotik** oleh Sdr. Yosan plus sejumlah TIPS penting yang dikumpulkan dari Forum Mikrotik.

Terima kasih kepada rekan-rekan yang sudah merelakan diri melakukan sharing di Forum, saya mengumpulkan sharing tersebut di sini dengan tujuan mempermudah bagi yang membutuhkan untuk mencari, bukan bermaksud mengambil kredit atau menganggap tutorial ini milik saya. INI MILIK KITA SEMUA!

## [How To] Blocked Page at Web Proxy MikroTik

Kapan yah.... udah agak lamaan gitu ga tau sekarang masih banyak yang bertanya atau tidak, namun seingat akang dulu banyak yang bertanya cara "Merubah **blocked page**" pada blocked page web proxy mikrotik, dan



Akang juga salah satu yang bertanya



Nah... dengan tutz ini diharapkan dapat membantu menemukan



sesuatu yang baru

OK, mari kita langsung aja, kali ini pake gambar yang lebih banyak bicara yang pasti pertama kali langsung menuju ke /ip proxy lalu masuk ke /ip proxy access.

#	Src. Address	Dst. Address	Dst. Port	Dst. Host	Path	Method	Action	Redirect To	Hits
0	...	74.53.140.18	80				deny	blocked....	8
1	...	208.65.153.253	80				deny	blocked....	14
2	...	208.117.236.69	80				deny	blocked....	1
3	...	208.65.153.238	80				deny	blocked....	4
4	...	208.65.153.251	80				deny	blocked....	6
5	...	74.86.196.213	80				deny	blocked....	4
6	...	216.163.137.3	80				deny	blocked....	0
7	...	209.62.20.162	80				deny	blocked....	1
8	...	76.76.15.167					deny	blocked....	68
9	...				"memek"		deny	blocked....	4
10	...				"penis"		deny	blocked....	0
11	...				"herita"		deny	blocked....	7
12	...				"bangsal"		deny	blocked....	0
13	...				"proxy"		deny	blocked....	0
14	...				"proxies"		deny	blocked....	0

15 items (1 selected)

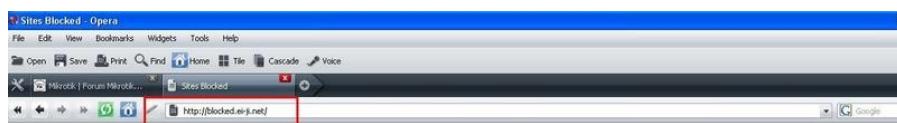
**Web Proxy Rule <>**

Src. Address:  OK  
Dst. Address:  Cancel  
Dst. Port:   Apply  
Local Port:  Disable  
Dst. Host:  "bangsal" Comment  
Path:  Copy  
Method:   
Action:  Remove  
Redirect To:  Reset Counters  
Hits: 0 Reset All Counters  
disabled

**Web Proxy Rule <209.62.20.162>**

Src. Address:  OK  
Dst. Address:  209.62.20.162 Cancel  
Dst. Port:  80 Apply  
Local Port:  Disable  
Dst. Host:  Comment  
Path:  Copy  
Method:   
Action:  Remove  
Redirect To:  Reset Counters  
Hits: 1 Reset All Counters  
disabled

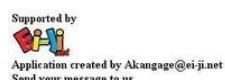
setelah itu hasilnya seperti ini.....



Sorry, This site is blocked  
Maaf, Situs ini telah diblokir



DEPKOMINFO



Nah... bagi yang tidak punya web sendiri bisa bikin lokal di taruh di pagenya mikrotik.

Code:

[Akangage \[Tutorial\] LB + Internal Proxy + HotSpot LB + Pisah IIX & Internasional LB 2 ISP or More Based IP Address PPPoE 5 Speedy + LB Full Version Setting USB Modem di MikroTik Bikin PoE Sendiri Block Webpage Redirect Memperkuat Sinyal 3G/HSDPA L7 Filtering](#)

---

Mari kita budayakan "Thanks" atas setiap jernih payah usaha seseorang agar lebih semangat lagi dalam mencari ilmu yang baru..... jangan lupa klik "Thanks"

---

## **Editing Hotspot login Page**

allow all

Mungkin ini pernah dibahas sebelumnya cuma ngga lengkap ..jadi saya cuma mo lengkapin aja , jadi buat bang momod kalau emang udah ada tinggal di pindah aja ....

(Tq to Priyo@datautama for this )

..sebenarnya yang kita perlukan hanya 3 script 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 kulu kalian2 mo 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 ....

(templatanya 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

## **misahin download dan browsing?**



maaf sebelumnya jika pernah di bahas, saya sudah coba cari cari blom ketemu , , di beberapa trit ada yg membahas memblokir IDM tp tidak bisa, pertanyaanya mungkin sedikit sama yaitu mungkin tidak jika kita pisahin jalun browsing dengan download?  
tujuan utama sih untuk melimit download dan unlimit brousing.



jadi jika pelanggan hanya sekedar brousing tidak perlu saya batasi, tp jika dalam kondisi download pelanggan saya batasi  
atau jika beberapa pelanggan sedang download tiba tiba ada pelanggan yg lain sedang rekwas untuk brousing makan jalur brousing di utamakan sementara download tidak di prioritaskan



trimakasih sebelumnya

## **JAWABAN :**

misal di buat manglenya :

```
chain=prerouting action=mark-connection  
new-connection-mark=conn-download passthrough=yes protocol=tcp  
dst-port=80 connection-bytes=1000000-0 comment="CONN-DOWNLOAD"
```

```
chain=prerouting action=mark-packet new-packet-mark=download-packet  
passthrough=yes connection-mark=conn-download
```

```
chain=prerouting action=mark-connection  
new-connection-mark=conn-browsing passthrough=yes  
protocol=tcp dst-port=80 connection-bytes=0-1000000 comment="CONN-BROWSING"
```

```
chain=prerouting action=mark-packet new-packet-mark=browsing-packet  
passthrough=yes connection-mark=conn-browsing
```

nah..setelah itu tinggal di buatin queue-tree utk prioritas dan traffict shapingnya..



bener banget!!!! deteksi pake connection bytes... tapi buat LB agak2 ribet konfigurasinya karena gerbangnya



banyak... udha gitu gabisa deteksi pake interface lagi

## Tut FullSpeed dari cache internalnya mikrotik (untuk versin 2.9)

Menggunakan internal Proxynya mikrotik versi crack(2.9) ternyata masih bisa. dari pada pakai komputer lagi mending pakai internalnya saja. cuman hasilnya memang belum seoptimal kalo pakai external proxy(terutama di bagain bandwith manjemennya) tetapi masih memuaskan.(sudah ditest cuman kadang terasa kurang memuaskan, tetapi bisa membantu meningkatkan perfoma)

1. IP Modem:

- 192.168.10.1

2. IP Mikrotik:

- 192.168.1.1 = local

- 192.168.10.2 = public/ke modem speedy

3. IP Client: 192.168.1.0/24

kita masuk ke mikrotiknya:

Quote:

```
/ ip address  
add address=192.168.10.2/24 network=192.168.10.0 broadcast=192.168.10.255 \  
interface=Public comment="" disabled=no  
add address=192.168.1.1/24 network=192.168.1.0 broadcast=192.168.1.255 \  
interface=Lan comment="" disabled=no
```

setting route:

Quote:

```
/ ip route  
add dst-address=0.0.0.0/0 gateway=192.168.10.1 scope=255 target-scope=10 \  
comment="" disabled=no
```

setting dns:

Quote:

```
/ ip dns  
set primary-dns=192.168.10.1 \  
allow-remote-requests=no cache-size=2048KiB cache-max-ttl=1w
```

Quote:

```
ip web-proxy pr  
enabled: yes  
src-address: 0.0.0.0  
port: 3128  
hostname: "proxy"  
transparent-proxy: yes  
parent-proxy: 0.0.0.0:0  
cache-administrator: "webmaster"  
max-object-size: 4096KiB  
cache-drive: system
```

```
max-cache-size: none  
max-ram-cache-size: unlimited  
status: running  
reserved-for-cache: 0KiB  
reserved-for-ram-cache: 154624KiB
```

Setting NAT:

Quote:

```
/ ip firewall nat  
add chain=dstnat src-address=192.168.1.0/24 protocol=tcp dst-port=80 \  
action=redirect to-ports=3128 comment="" disabled=no  
add chain=srcnat out-interface=Public action=masquerade comment="" disabled=no
```

Ok, sekarang mangglenya:

Quote:

```
/ ip firewall mangle  
add chain=prerouting protocol=icmp action=mark-connection \  
new-connection-mark=icmp-con passthrough=yes comment="" disabled=no  
add chain=prerouting protocol=icmp connection-mark=icmp-con\  
action=mark-packet new-packet-mark=icmp-pkt\  
passthrough=no comment="" disabled=no  
  
add chain=prerouting action=mark-connection new-connection-mark=con-up\  
passthrough=yes comment=""  
add chain=prerouting action=mark-paket new-paket-mark=all-pkt\  
conection-mark=con-up passthrough=no comment=""  
  
add chain=output content="X-Cache: HIT" action=mark-connection \  
new-connection-mark=proxy-con passthrough=yes comment=""\  
disabled=no  
add chain=output connection-mark=proxy-con action=mark-packet \  
new-packet-mark=proxy-pkt passthrough=no comment="" disabled=no  
  
add chain=forward action=mark-connection new-connection-mark=direct-con\  
passthrough=yes comment="" disabled=no  
add chain=forward protocol=tcp connection-mark=direct-con \  
action=mark-packet new-packet-mark=all-pkt passthrough=no  
comment="" disabled=no  
add chain=output protocol=tcp connection-mark=direct-con \  
action=mark-packet new-packet-mark=all-pkt passthrough=no  
comment="" disabled=no
```

setelah manggle-nya kita buat simple queuenya:

Quote:

```
add name="proxy-HIT" dst-address=0.0.0.0/0 interface=all parent=none \  
packet-marks=proxy-pkt direction=both priority=8 \
```

```
queue=default-small/default-small limit-at=0/0 max-limit=0/0 \
total-queue=default-small disabled=no comment="paling atas"
add name="Ping-queue" dst-address=0.0.0.0/0 interface=all parent=None \
packet-marks=icmp-pkt direction=both priority=2 \
queue=default-small/default-small limit-at=0/0 max-limit=0/0 \
total-queue=default-small disabled=no comment="supaya ping kecil"
add name="Parent-queue" dst-address=0.0.0.0/0 interface=all parent=None \
direction=both priority=8 queue=default-small/default-small limit-at=0/0 \
max-limit=45000/300000 total-queue=default-small disabled=no
add name="All-Trafik" target-addresses=192.168.1.0/24 \
dst-address=0.0.0.0/0 interface=all parent=Parent-queue \
packet-marks=all-pkt direction=both priority=8
queue=default-small/default-small limit-at=4500/30000
max-limit=45000/300000 total-queue=default-small disabled=no
```

untuk yang bold bisa di masukkan per ip komputer biar lebih bagus queuenya.

sudah saya coba dan hasilnya cukup memuaskan. bisa digabung dengan teknik load balancing. caranya untuk yang dari proxy-con tidak usah dibuat lagi nthnya. yang dibuat nthnya yang untuk direct-con nya saja.

maaf tidak punya screensutnya

\*Ada yang mengganjal untuk loadbalancing sampai saat ini kok susah ya biar bener2 50%:50% sudah coba tut akangge yang pakai v 3.x cuman nggak berhasil, pasti tidak imbang dengan tipologi:  
modem ---+-- mikrotik ---+-- client(Wire)  
modem ---+\*\*\*\*\* Client(Hotspot)>>= saya kurang ngerti kok nggak bisa pakai transparent proxy, selain itu jadi masalah di billingnya.

mohon feedbacknya



terima kasih sudah membaca  
semoga bisa membantu rekan-rekan semua

terima kasih banyak

## Yang Pengen Block FRIENDSTER

Sebenarnya sih saya bukanya tidak suka dengan Friendster tapi karena tuntutan tugas, yang waktu itu ketua LAB saya mendapati seisi LAB hampir semuanya Friendsteran jadi beliau marah2 karena mereka lupa fungsi dari lab itu sebenarnya, tapi biasalah anak2 walaupun gimana aja masih tetep dablek, akhirnya mereka tidak bisa diingatkan dengan mulut tapi dengan system, tapi katanya Ka Lab q tapi biarlah dari jam 15 keatas ndak papa2, wah akhirnya keluar jurus mikrotik q

Friendster setelah saya telusuri mempunya 6 IP Public untuk menampilkan websitenya:

209.11.168.112

209.11.168.113

209.11.168.122

209.11.168.123

209.11.168.133

209.11.168.121

sebelumnya masuk dulu: [lab-it@TI] ip firewall filter> setelah masuk baru ketikan ini:

```
add chain=forward src-address=209.11.168.112  
time=7h-15h,sat,fri,thu,wed,tue,mon,sun action=drop
```

```
add chain=forward in-interface=Public src-address=209.11.168.113  
time=7h-15h,sat,fri,thu,wed,tue,mon,sun action=drop
```

```
add chain=forward src-address=209.11.168.122  
time=7h-15h,sat,fri,thu,wed,tue,mon,sun action=drop
```

```
add chain=forward src-address=209.11.168.123  
time=7h-15h,sat,fri,thu,wed,tue,mon,sun action=drop
```

```
add chain=forward src-address=209.11.168.133  
time=7h-15h,sat,fri,thu,wed,tue,mon,sun action=drop
```

```
add chain=forward src-address=209.11.168.121  
time=7h-15h,sat,fri,thu,wed,tue,mon,sun action=drop
```

sedikit penjelas di atas: [www.friendster.com](http://www.friendster.com) saya block dari jam 7 pagi sampai jam 15 sore dan untuk baris kedua yaitu:

```
add chain=forward in-interface=Public src-address=209.11.168.113 time=7h-15h,sat,fri,thu,wed,tue,mon,sun  
action=drop
```

pada code diatas yaitu pada interface=Public itu di karena saya waktu itu tidak berhasil tanpa mengikutkan interfacenya akhirnya saya block dari interfacenya akhirnya berhasil jugak Friendster saya block dari jam 7-15 dan setelah jam 15 keatas Friendster bisa digunakan sejauh ini cara di atas berjalan tanpa hambatan hanya saja masalahnya hanya saja.... teman q panas pada panas ma q he....he.... sebenarnya q pengen sih friendsteran.

Di bawah ini daftar IP dari [www.youtube.com](http://www.youtube.com) yang katanya biang kerok penghabis bandwith:

208.65.153.251, 208.65.153.253, 208.65.153.238

cara di atas bisa juga digunakan untuk mengeblock situs porno dan terlarang lainnya, mungkin ini sedikit solusi untuk mengamankan lab. tapi..... kalau untuk warnet wah pada kabur semua pelanggannya nanti.he 3x....

## Another way to block web



Iseng2 aja Akang trial eror alias coba-coba siapa tahu jadi 😊 eh..... ga tahu nya 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
```

## NEW Update --> Setting PPPoE dan Load Balance Speedy --NEW UPDATE--



Dari kemarin ubek-ubek di Internet, cari sana sini, tanya sama temen2 di YM (malah diomelin ), lalu di wiki.mikrotik dan lain sebagainya akhirnya ketemu juga dan sudah Akang coba it's fully works!!!

Emang ilmu mahal harganya, dan tidak ada salahnya membagi harga mahal tersebut di Internet menjadi lebih murah dan terjangkau

### Setting PPPoE Client

Code:

```
/interface pppoe-client
add ac-name="" add-default-route=no allow=pap,chap,mschap1,mschap2 comment="" \
dial-on-demand=no disabled=no interface=Speedy-1 max-mru=1480 max-mtu=1480 \
mrru=disabled name="*****@telkom.net" password="***" profile=default \
service-name="" use-peer-dns=no user="***"

add ac-name="" add-default-route=no allow=pap,chap,mschap1,mschap2 comment="" \
dial-on-demand=no disabled=no interface=Speedy-2 max-mru=1480 max-mtu=1480 \
mrru=disabled name="*****@telkom.net" password="***" profile=default \
service-name="" use-peer-dns=no user="***"

add ac-name="" add-default-route=no allow=pap,chap,mschap1,mschap2 comment="" \
dial-on-demand=no disabled=no interface=Speedy-3 max-mru=1480 max-mtu=1480 \
mrru=disabled name="*****@telkom.net" password="***" profile=default \
service-name="" use-peer-dns=no user="***"

add ac-name="" add-default-route=no allow=pap,chap,mschap1,mschap2 comment="" \
dial-on-demand=no disabled=no interface=Speedy-4 max-mru=1480 max-mtu=1480 \
mrru=disabled name="*****@telkom.net" password="***" profile=default \
service-name="" use-peer-dns=no user="***"

add ac-name="" add-default-route=no allow=pap,chap,mschap1,mschap2 comment="" \
dial-on-demand=no disabled=no interface=Speedy-5 max-mru=1480 max-mtu=1480 \
mrru=disabled name="*****@telkom.net" password="***" profile=default \
service-name="" use-peer-dns=no user="***"
```

### Setting Mangle u/ LB

Code:

```
/ip firewall mangle
add chain=prerouting action=mark-connection new-connection-mark=ADSL-1 \
    passthrough=yes connection-state=new in-interface=HotSpot nth=*** \
    comment="" disabled=no
add chain=prerouting action=mark-routing new-routing-mark=ADSL-1 passthrough=no \
    in-interface=HotSpot connection-mark=ADSL-1 comment="" disabled=no
add chain=prerouting action=mark-connection new-connection-mark=ADSL-2 \
    passthrough=yes connection-state=new in-interface=HotSpot nth=*** \
    comment="" disabled=no
add chain=prerouting action=mark-routing new-routing-mark=ADSL-2 passthrough=no \
    in-interface=HotSpot connection-mark=ADSL-2 comment="" disabled=no
add chain=prerouting action=mark-connection new-connection-mark=ADSL-3 \
    passthrough=yes connection-state=new in-interface=HotSpot nth=*** \
    comment="" disabled=no
add chain=prerouting action=mark-routing new-routing-mark=ADSL-3 passthrough=no \
    in-interface=HotSpot connection-mark=ADSL-3 comment="" disabled=no
add chain=prerouting action=mark-connection new-connection-mark=ADSL-4 \
```

```

passthrough=yes connection-state=new in-interface=HotSpot nth=*** \
comment="" disabled=no
add chain=prerouting action=mark-routing new-routing-mark=ADSL-4 passthrough=no \
in-interface=HotSpot connection-mark=ADSL-4 comment="" disabled=no
add chain=prerouting action=mark-connection new-connection-mark=ADSL-5 \
passthrough=yes connection-state=new in-interface=HotSpot nth=*** \
comment="" disabled=no
add chain=prerouting action=mark-routing new-routing-mark=ADSL-5 passthrough=no \
in-interface=HotSpot connection-mark=ADSL-5 comment="" disabled=no

```

### Tanda Bintang

NTH untuk MT Versi 3.XX ada 2 versi, silahkan dipilih, mana aja pasti jadi

### Versi 1

Code:

```

NTH : 5.1; 5.2; 5.3; 5.4; 5.5
Untuk settingan yang "mark-routing" gunakan "passthrough" yes

```

### Versi 2

Code:

```

NTH : 5.1; 4.1; 3.1; 2.1; 0.0 atau 1.1
Untuk settingan yang "mark-routing" gunakan "passthrough" no

```

### Konfigurasi NAT

-- Ada 2 Versi, silahkan di pilih mana saja bisa --

### Versi 1

Code:

```

/ip firewall nat
add chain=srcnat action=src-nat to-addresses=[IP-Speedy-1] to-ports=0-65535 \
connection-mark=ADSL-1 comment="" disabled=no
add chain=srcnat action=src-nat to-addresses=[IP-Speedy-2] to-ports=0-65535 \
connection-mark=ADSL-2 comment="" disabled=no
add chain=srcnat action=src-nat to-addresses=[IP-Speedy-3] to-ports=0-65535 \
connection-mark=ADSL-3 comment="" disabled=no
add chain=srcnat action=src-nat to-addresses=[IP-Speedy-4] to-ports=0-65535 \
connection-mark=ADSL-4 comment="" disabled=no
add chain=srcnat action=src-nat to-addresses=[IP-Speedy-5] to-ports=0-65535 \
connection-mark=ADSL-5 comment="" disabled=no

```

### Versi 2

Code:

```

/ip firewall nat
add chain=srcnat action=masquerade src-address="Lokal"

```

### Konfigurasi Route

Code:

```

/ip route
add disabled=no distance=1 dst-address=0.0.0.0/0 gateway=PPPoE-1 \
routing-mark=ADSL-1
add disabled=no distance=1 dst-address=0.0.0.0/0 gateway=PPPoE-2 \
routing-mark=ADSL-2
add disabled=no distance=1 dst-address=0.0.0.0/0 gateway=PPPoE-3 \
routing-mark=ADSL-3

```

```

add disabled=no distance=1 dst-address=0.0.0.0/0 gateway=PPPoE-4 \
routing-mark=ADSL-4
add disabled=no distance=1 dst-address=0.0.0.0/0 gateway=PPPoE-5 \
routing-mark=ADSL-5
add disabled=no distance=1 dst-address=0.0.0.0/0 gateway=PPPoE-1, \
PPPoE-2,PPPoE-3,PPPoE-4,PPPoE-5

```

## Keterangan Warna biru --UPDATE--

Quote:

Setelah Akang amati belakangan ini terdapat perubahan pola counter speedy pada MikroTik, jika menggunakan 1 Gateway untuk default gateway, maka akan ada salah 1 line yang drop entah di menit ke-5 atau menit ke-10 padahal dulu tidak begini... nah biar lebih stabil lagi, Akang udah trial eror dan pantau belakangan ini, untuk default gateway masukan semua gateway PPPoE Speedy/ISP agar semua paket dapat tersebar secara merata.

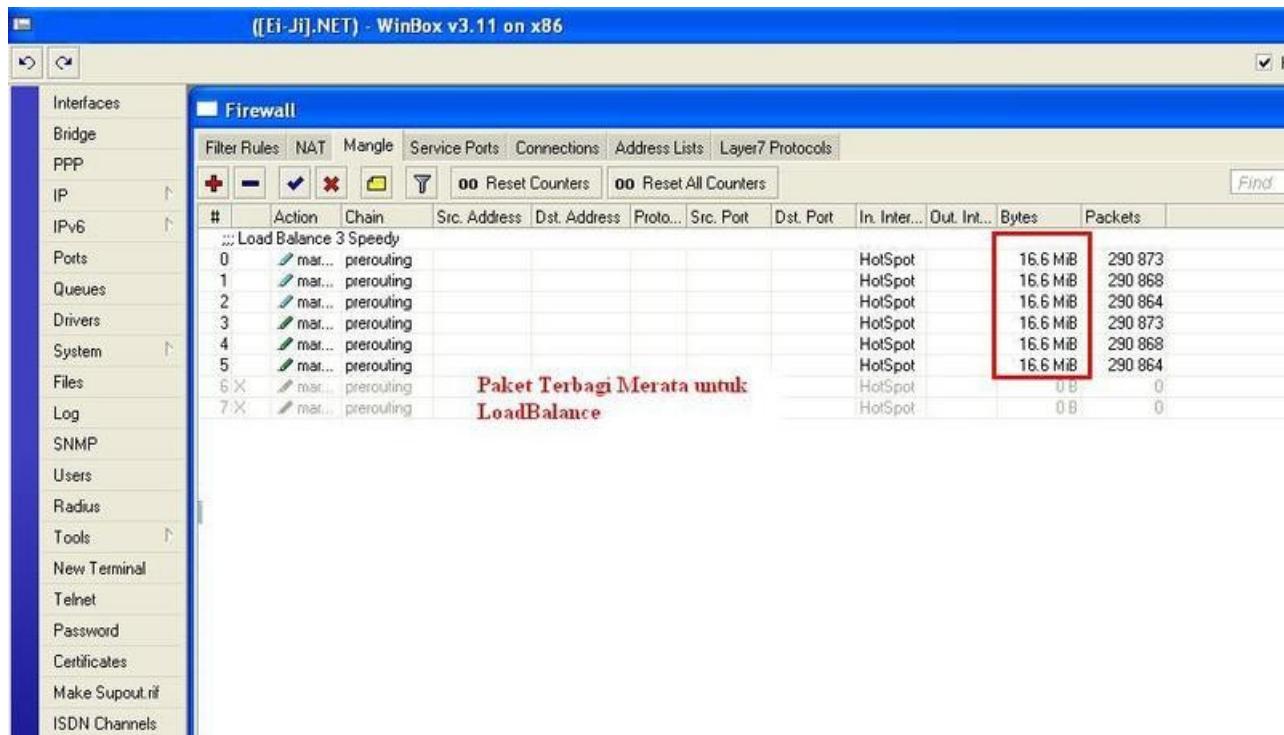


Akhirnya final juga Untuk Settingan PPPoE di MikroTik + LoadBalance, Selamat Mencoba



## Gambar LoadBalance penyebaran PAKET Merata atau BALANCE

**⚠ This image has been resized. Click this bar to view the full image. The original image is sized 799x456.**



Thanks buat brother2 semua yang membantu memecahkan solusi LB agar lebih maximal dan mantab

Code:

[Akangage \[Tutorial\] LB + Internal Proxy + HotSpot LB + Pisah IIX & Internasional LB 2 ISP or More Based IP Address PPPoE 5 Speedy + LB Full Version Setting USB Modem di](#)

[MikroTik Bikin PoE Sendiri Block Webpage Redirect Memperkuat Sinyal 3G/HSDPA L7 Filtering](#)

## Cara setting Web proxy 3.20

```
/ip proxy> pr
enabled: yes
src-address: 0.0.0.0
port: 8080
parent-proxy: 0.0.0.0
parent-proxy-port: 0
cache-administrator: "one_rule to believe"
max-cache-size: unlimited
cache-on-disk: yes
max-client-connections: 1000
max-server-connections: 1000
max-fresh-time: 3d
serialize-connections: no
always-from-cache: yes
cache-hit-dscp: 4
cache-drive: sata1
```

### NAT

```
;;; Berbagi internet ...^ ^
chain=srcnat action=masquerade out-interface=Speedy
```

```
1 ;;; lInternet lewat port ini !
chain=dstnat action=redirect to-ports=8080 protocol=tcp
src-address=192.168.0.0/24 dst-address=!192.168.0.0/16
in-interface=lokal dst-port=80
```

### Mangle

```
chain=output action=mark-packet new-packet-mark=Proxy-Hit passthrough=no
out-interface=lokal dscp=4
```

```
6 chain=prerouting action=mark-packet new-packet-mark=Test-Up passthrough=n>
src-address=192.168.0.0/24 in-interface=lokal
```

```
7 chain=forward action=mark-connection new-connection-mark=Test-Conn
passthrough=yes src-address=192.168.0.0/24
```

```
8 chain=forward action=mark-packet new-packet-mark=Test-Down passthrough=no
in-interface=Speedy connection-mark=Test-Conn
```

```
9 chain=output action=mark-packet new-packet-mark=Test-Down passthrough=no
dst-address=192.168.0.0/24 out-interface=lokal
```

coba deh... sesuain y ip nya ,



kalau berhasil lumayan looo hasilnya

## NGE Limit Youtube Video Streaming di MT 3.xx

To The Point saja

### Buat dulu http-video layer7-protocol nya

Code:

```
/ip firewall layer7-protocol  
add name=http-video regexp=http/(0\.9|1\.0|1\.1)[\x09-\x0d ][1-5][0-9][0-9][\x09-\x0d -~]* (content-type: video)
```

### Mangle Mark Packet http-video nya

Code:

```
/ip firewall mangle  
add action=mark-packet chain=prerouting comment="http-video mark-packet" \  
disabled=no layer7-protocol=http-video new-packet-mark=http-video \  
passthrough=no
```

### Queue Simple http-video nya

Code:

```
/queue simple  
add max-limit=0/64000 name=http-video packet-marks=http-video
```

Saat buka YouTube ..... kenceng, tapi saat Play Video langsung ke limit 64kbps

kalau ga jalan, mungkin proses penandaannya yang salah atau di queuenya ga sesuai atau di layer 7 nya yang kurang pas.

kalau settingan test di routerku jalan aja kok, tapi aku pake pcq ya..

cuman ya setingan seorang newbie yang ga pernah makan pojokan sekolah, kalau emang kurang pas tolong dikoreksi.

nih aku exportin, ga nolak kalau di kasih ijo ijo 😊

oh ya, aku pake MT versi 3 yang udah aku upgrade ke 3.23 dua hari lalu 😊

Code:

```
/ip firewall layer7-protocol  
add comment="" name=http-video regexp="http/(0\\.9|1\\.0|1\\.1)[\\x09-\\x0d ][1-5][0-9][0-9][\\x09-\\x0d -~]* (content-type: video)"
```

Code:

```
/ip fi ma  
add action=mark-packet chain=prerouting comment="Mark Packet HTTP Video" \  
disabled=no in-interface=ether1 layer7-protocol=http-video \  
new-packet-mark=http-video-up passthrough=no  
add action=mark-connection chain=forward comment="" disabled=no \  
layer7-protocol=http-video new-connection-mark=video-stream passthrough=\  
yes  
add action=mark-packet chain=forward comment="" connection-mark=video-stream \  
passthrough=yes
```

```
disabled=no in-interface=ether2 layer7-protocol=http-video \
new-packet-mark=http-video-down passthrough=no
```

Code:

```
/que typ
add kind=pcq name=http-video-up pcq-classifier=src-address pcq-limit=50 \
pcq-rate=0 pcq-total-limit=2000
add kind=pcq name=http-video-down pcq-classifier=dst-address pcq-limit=50 \
pcq-rate=0 pcq-total-limit=2000
```

Code:

```
/que sim
add burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s comment="" \
direction=both disabled=no dst-address=0.0.0.0/0 interface=all limit-at=\
64k/128k max-limit=64k/128k name="7. HTTP Video Traffict" packet-marks=\
http-video-up,http-video-down parent=none priority=8 queue=\
http-video-up/http-video-down total-queue=default-small
add burst-limit=0/0 burst-threshold=0/0 burst-time=0s/0s comment="" \
direction=both disabled=no dst-address=0.0.0.0/0 interface=all limit-at=\
0/0 max-limit=16k/96k name="Queue HTTP Video" packet-marks=\
http-video-up,http-video-down parent="7. HTTP Video Traffict" priority=8 \
queue=http-video-up/http-video-down target-addresses=0.0.0.0/0 \
total-queue=default-small
```



tapi sepertinya urutan peletakan menentukan prestasi

ket:

ether1 interface ke klien

ether2 interface ke ISP



## **Script Limit Bandwidth berdasar Siang - Malam**

Untuk Script Limit bandwidth malam :

- 1.Akses Router Mikrotik anda
- 2.System > Clock > kemudian perhatikan date(tgl) & time(waktu)
- 3.System > Scripts > New Script isikan data berikut :

Name : Limit Malam

Policy : Conteng Read, Policy dan Write

Source :

```
/queue simple set user1 limit-at=64000/128000 max-limit=64000/128000 total-limit-at=128000 total-max-limit=128000
```

nb:copy dan paste untuk user lainnya

4.System > Scheduler > New Schedule isikan data berikut :

Name : Malam

Start Date : (tgl mulai disesuaikan dengan tgl di mikrotik) jun/07/2007

Start Time : (waktu mulai disesuaikan kebutuhan) 19:00:00 (untuk jam 7 mlm)

Interval : 1d 00:00:00 (rolling per 1 hari)

On Event :

Limit Malam

Untuk Script Limit bandwidth siang :

- 1.System > Scripts > New Script isikan data berikut :

Name : Limit Siang

Policy : Conteng Read, Policy dan Write

Source :

```
/queue simple set user1 limit-at=32000/64000 max-limit=32000/64000 total-limit-at=64000 total-max-limit=64000
```

nb:silahkan sesuaikan pada user yg laen

2.System > Scheduler > New Schedule isikan data berikut :

Name : Siang

Start Date : (tgl mulai disesuaikan dengan tgl di mikrotik) jun/07/2007

Start Time : (waktu mulai disesuaikan kebutuhan) 07:00:00 (untuk jam 7 pagi)

Interval : 1d 00:00:00 (rolling per 1 hari)

On Event :

Limit Siang

Langkah diatas secara otomatis akan memberikan setting limit pada siang hari 32k/64k mulai jam 7 pagi s/d jam 7 mlm sedangkan limit bandwidth malam hari 64k/128k mulai jam 7 mlm s/d jam 7 pagi.

Semua setting bisa disesuaikan dengan kebutuhan, mudah-mudahan bisa dengan mudah dimengerti dan



membantu .

## **Simple Load Balancing + DNS Resolver + Secret Fitur**

**DNS Resolver ( bisa juga disebut DNS Forwarder atau apalah saya juga bingung)**

**Pake WinBox masuk ke -> IP -> DNS**

-> Klik Settings

-> masukkan Primary Dan Secondary DNS dari ISP nya

-> centang [v] allow remote requests

**Pake WinBox masuk ke -> IP -> Firewall -> NAT**

-> klik [+]-> isikan Chain : dstnat

protokol : 17(UDP)

dstport : 53

->Pindah Ke Sub Menu Action

action : redirect

to ports : 53

->Klik OK biar Kesimpel

-> Bikin Sekali lagi dengan **protokol di isi : 6(TCP)**

Sampai Disini DNS Resolvernya success

kamu bisa tambahkan sendiri Host + NS Resolution dari web web yang sering dibuka biar tambah cepet browsing nya

## **2. Settingan Gila Ala Manipulasi TOS**

anda sering gagal membuat manipulasi TOS.. pakai ini dijamin berhasil

pakai WinBox -> Ip -> Firewall -> NAT

klik [+]

isikan chain : dstnat

protocol : 1 (icmp)

in interface : ether1

-> di menu action

action : redirect

to ports : 1

klik OK

lalu silahkan coba PING atau TRACERT dan dijamin anda NGUAKAK KAK KAK KAK.

## Blok PTP – other way

kalo sya pake jurus blok semua port p2p... lumayan berhasil...

```
#yang ini membatasi akses user yang masuk ke router
add chain=input connection-state=established action=accept comment="Allow Established connections"
disabled=no
add chain=input src-address=192.168.100.0/24 dst-address=192.168.100.1 protocol=udp dst-port=53
action=accept comment="Allow UDP" disabled=no
add chain=input protocol=icmp action=accept comment="Allow ICMP" disabled=no
add chain=input src-address=192.168.100.125 dst-address=192.168.100.1 dst-port=8291 action=accept
disabled=no
add chain=input src-address=192.168.100.61 dst-address=192.168.100.1 dst-port=8291 action=accept
disabled=no
add chain=input action=drop comment="Drop anything else" disabled=no
```

#yang ini blok p2p

```
add chain=forward protocol=tcp connection-state=invalid action=drop comment="drop invalid connections"
disabled=no
add chain=forward p2p=all-p2p action=drop comment="drop p2p"
add chain=forward protocol=tcp dst-port=6346-6348 action=drop
add chain=forward protocol=tcp dst-port=41170 action=drop
add chain=forward protocol=tcp dst-port=28864-28865 action=drop
add chain=forward protocol=tcp dst-port=8888-8889 action=drop
add chain=forward protocol=tcp dst-port=8311 action=drop
add chain=forward protocol=tcp dst-port=7668 action=drop
add chain=forward protocol=tcp dst-port=6881-6889 action=drop
add chain=forward protocol=tcp dst-port=6969 action=drop
add chain=forward protocol=tcp dst-port=5500-5503 action=drop
add chain=forward protocol=tcp dst-port=4762 action=drop
add chain=forward protocol=tcp dst-port=4661-4665 action=drop
add chain=forward protocol=tcp dst-port=4329 action=drop
add chain=forward protocol=tcp dst-port=1214 action=drop
add chain=forward protocol=tcp dst-port=1044-1045 action=drop
add chain=forward protocol=tcp dst-port=412 action=drop
```

#yang ini bener-bener cuma melewatkkan port 53, selain itu drop... memang sedikit terlalu ketat...

```
add chain=forward protocol=udp dst-port=53 action=accept
add chain=forward protocol=udp action=drop
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
```

oke semoga bermanfaat.



klo saya sih pake ini

ip firewall mangle

Code:

```
add chain=prerouting p2p=all-p2p action=mark-connection new-connection-mark=P2P-conn  
passthrough=yes comment="P2P Connection" disabled=no  
add chain=prerouting connection-mark=P2P-conn action=mark-packet new-packet-mark=P2P-  
Packet passthrough=no comment="P2P Packet" disabled=no
```

ip firewall filter

Code:

```
add chain=P2P packet-mark=P2P-Packet action=drop  
add chain=P2P p2p=all-p2p action=drop  
add chain=forward action=jump jump-target=P2P  
add chain=output action=jump jump-target=P2P  
add chain=input action=jump jump-target=P2P
```

emang sih masih bisa buka list donlot tp begitu start donlot 0% terus ga jalan2 donlotnya (limewire sama  
bearshare) lom coba p2p lainnya

## Login HTTPS di Hotspot



Masih newbie nih tapi mau coba share aja, kali aja berguna..

1. Create SSL Certificate, baca manualnya di [sini](#)

Yang kita perlukan hasilnya hanyalah file server.crt dan server.key seperti contoh tersebut.

Cat: kalo bisa bikin expirednya 10 thn aja (brp hari tuh..? itung sendiri..) he..he..he maksudnya biar bisa berlaku lama... gak perlu sering2 create...

2. Kalau sudah terbentuk file server.crt dan file server.key, upload aja ke Mikrotik kita di bagian Files..

3. Masuk ke menu "/certificate import file-name=server.key" nanti ditanyakan passphrase-nya... isikan sesuai dengan ketika kita bikin SSL Certificate di atas..

4. Kalo sukses importnya, coba cek dengan perintah "/certificate print"

Munculnya kira-kira seperti ini..

Flags: K - decrypted-private-key, Q - private-key, R - rsa, D - dsa

0 KR name="hotspot" subject=C=ID,ST=DKI Jakarta,L=Jakarta,O=VILANI-Net,OU=RTRW-

Net,CN=hotspot.vilani-net.com,

emailAddress=rtrwnet@vilani-net.com

issuer=C=ID,ST=DKI Jakarta,L=Jakarta,O=VILANI-Net,OU=RTRW-Net,

CN=hotspot.vilani-net.com,emailAddress=rtrwnet@vilani-net.com

serial-number="A58341FB6D1A4C43" email=rtrwnet@vilani-net.com

invalid-before=feb/19/2007 22:47:08 invalid-after=feb/18/2010 22:47:08

ca=yes

Bisa dilihat statusnya bahwa SSL Certificatenya sudah diimport dengan nama hotspot

5. Masuk ke menu "/ip hotspot profile set hsprof1 ssl-certificate=hotspot login-by=https"

cat: hsprof1 adalah nama profile dari server hotspot kita.. "login-by" diisikan hanya https aja, karena kalau sudah https yang lain gak berlaku..

Sudah gitu aja... jangan lupa browser client harus support https juga... dan port https (443) jangan di blok ya..



Sekrinsyutnya seperti ini kira2

 This image has been resized. Click this bar to view the full image. The original image is sized 1024x768.

Vilani-Net :: Computer-Networking-Internet Solutions > LOGIN - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://hotspot.vilani-net.com/login

Vilani-Net :: SASANA A... Yahoo! Grou... klikBCA Indivi... EPCT Corpor... create ssl cer... Forum Mikroti... How to creat... aka di...

**VNet VILANI-NET**  
www.vilani-net.com

**VILANI-NET**  
Vila Nusa Indah 2 Blok BB6 No. 12A  
Jati Asih, Bekasi, Jawa Barat, 16969  
Telp: 021-82420782, Fax: 021-82402639  
Mobile: 021-92239580, 0813-10371907  
Website: <http://www.vilani-net.com>  
Email: rtrwnet@vilani-net.com

login singgahpai  
password    
OK

Provide by www.vilani-net.com

Find: altho Next Previous Highlight all Match case Done

hotspot.vilani-net.com



## **mengatur prioritas trafik dari dan ke mikrotik**

Selama ini kita concern mengatur trafik paket2 dari dan ke sisi client, mengatur prioritas paket yg mana duluan, paket mana yg belakangan. Sekarang pertanyaannya bagaimana dengan paket2 yg berasal dari mikrotik sendiri apakah otomatis mempunyai prioritas tertinggi atau terendah malah ?

Soalnya saya ingin agar paket icmp yg keluar dr mikrotik ke internet mempunyai prioritas tertinggi dari paket yg lain. Apakah perlu buat mangle dan queuenya untuk ini?

Latar belakangnya begini, saya lagi buat script untuk deteksi koneksi modem adsl router dengan cara ping ip tertentu, jalur ke ip ini telah dibuat routing statik via modem adsl tsb. Jika trafik icmp ini kalah dg trafik yg lain kemudian hasil ping reply timeout maka script akan menganggap koneksi modem adsl router tsb putus, akhirnya koneksi dilepas dari modem.

**JAWABANNYA:** Dapat script dari wiki mikrotik. Sederhana sekali. Kita tinggal buat script untuk monitor device yg lalu lintas trafiknya padat (Rx). Jika ping ke ip tertentu gagal karena trafik padat maka tinggal ambil data dari Rx apakah lebih besar dari parameter tertentu.

Code:

```
:local ip "202.134.1.10";
:local succ 0;
:local interface "public";
:for z from=1 to=3 do={ \
    :if ([/ping "$ip" count=1 size=28]=1) do { :set succ ($succ+1) }};
    /interface monitor-traffic "$interface" once do={ :if ("$received-bits-per-second" > 32000) do={:set succ ($succ+1)}};
:if ($succ>1) do { ... write some lines that connection is still up }
:if ($succ<1) do { ... write some lines that connection is down }
```

Maksud dari script di atas:

1. ip destination: 202.134.1.10
2. jumlah ping 3x
3. var succ akan ditambahkan 1 jika ping sukses
4. var succ juga akan dinaikkan bila Rx > 32000bps

Dengan script di atas, baik jika trafik padat script monitoring Rx berguna, jika no trafik, script ping berguna. Mestinya bisa pakai loop while...do. Ah, ini pr u/ nanti malam

*HASIL :*

```
:local ip "119.2.40.21";
:local succ 0;
:local interface "laxo";
:for z from=1 to=3 do={ :log info "Testing ...."; :if ([/ping "$ip" count=1 size=28]=1) do { :set succ ($succ+1) }};
/interface monitor-traffic "$interface" once do={ :if ("$rx-bits-per-second" > 32000) do={:set succ ($succ+1)}};
:if ($succ>1) do { :log info "UP" }
:if ($succ<1) do { :log info "down" }
```

## Banyak Web Server di belakang router Mikrotik

IDE GILA... (Smoga tidak bermanfaat)



Gw pernah nyoba sesuatu hal yang aneh...  
ak ga tau apakah bermanfaat apa ga? apa udah ada yang juga coba . . .

jadi konsepnya bgni,  
dengan menggunakan satu IP Public tetapi mempunyai beberapa domain

Requirement::

1 buah Router Mikrotik (klo bisa versi 3)

=> Fasilitas yang digunakan -> Proxy, DNS, DST-NAT, SRC-NAT, Firewall, dll

Internet

|

IP Public

|

Mikrotik

|

-----(LAN)-----

WEB 1 WEB 2 WEB 3

IP Public Mikrotik = 222.1.1.1

IP Local Mikrotik = 192.168.1.1

DAFTARKAN DOMAIN BERIKUT KE IP PUBLIC YANG DIMILIKI:: (222.1.1.1)

== Domain = [www.aneh.co.cc](http://www.aneh.co.cc)

== Domain = [www.gila.co.cc](http://www.gila.co.cc)

== Domain = [www.lucu.co.cc](http://www.lucu.co.cc)

====> DAFTAR AJA DI INTERNET BANYAK SEKALI (Mau yang gratis atau bayar terserah...)

NANTINYA SETIAP KOMPUTER DI BAWAH INI DAPAT DI AKSES MENGGUNAKAN NAMA BERIKUT::

WEB 1 = 192.168.1.2 ( Domain = [www.aneh.co.cc](http://www.aneh.co.cc) )

WEB 2 = 192.168.1.3 ( Domain = [www.gila.co.cc](http://www.gila.co.cc) )

WEB 3 = 192.168.1.4 ( Domain = [www.lucu.co.cc](http://www.lucu.co.cc) )

Langkah-Langkah=

1) Buat Web Proxy dengan port 3128

2) Buat DNS dan centang request dari client

3) Arahkan Web proxy agar menjadi proxy public atau bisa di akses oleh Internet (All IP dapat mengakses proxy)

4) Arahkan akses port 80 dari interface public (INPUT) ke port 3128 port proxy (Redirect)

5) BUAT / Catat nama masing - masing domain di DNS (Mikrotik)

=> [www.aneh.co.cc](http://www.aneh.co.cc) 192.168.1.2

[www.gila.co.cc](http://www.gila.co.cc) 192.168.1.3

[www.lucu.co.cc](http://www.lucu.co.cc) 192.168.1.4

6) jangan lupa buat source nat untuk ketiga komputer web server tersebut

DENGAN INI MAKA BEBERAPA WEB SERVER YANG BERADA DI LAN (Local Area Network) DAPAT DI AKSES MELALUI INTERNET DENGAN HANYA SATU IP PUBLIC DAN BEBERAPA NAMA DOMAIN YANG BERBEDA

Syarat:: Port di setiap masing-masing web server harus 80

CARA KERJA ::

Komputer yang berada di internet akan mengakses IP Public (222.1.1.1) dengan port 80 (http) kemudian router mikrotik akan mendirect ke port 3128 (Proxy)

Kemudian proxy akan melihat daftar DNS di mana nama domain tersebut berada (resolve)

Kemudian dari informasi DNS tersebut maka proxy akan mengakses komputer menurut request yang datang...

## Routerboard 450 Repaired

Selamat pagi,

Berhubung minimnya informasi/thread tentang perbaikan hw, mungkin sedikit share, siapa tau berguna buat kawan2 semua, buat yang lain juga mungkin bisa dikumpulin sharing di sini,

- Perhatian! jgn ditiru untuk yg tidak punya pengalaman solder/menyolder/electronic, dan jangan diterapin pada RB yang sehat, karena tidak worth-it memuaskan rasa ingin tau gan 😊

Begini ceritanya :

Pagi2 ini ketika bangun ternyata salah satu RB450 sy ngambek, ketika dicek kondisi lampu power biru masih menyala, dengan lampu kuning disebelahnya rada redup berkedip, kesemua lampu lan mati dengan lampu eth4 dan eth5 nyala redup..., serial port juga tidak menunjukan tanda2 kehidupan, begitu pula dengan beepnya,



router dalam kondisi koma...

Pagi itu juga segera kami pindahkan semua link yang berhubungan dengan mesin ini, dan mesin ini segera masuk ke ruang observasi dengan sedikit perasaan sedih berhubung ini harinya mencontreng para vendor



tentu lagi pada berlibur

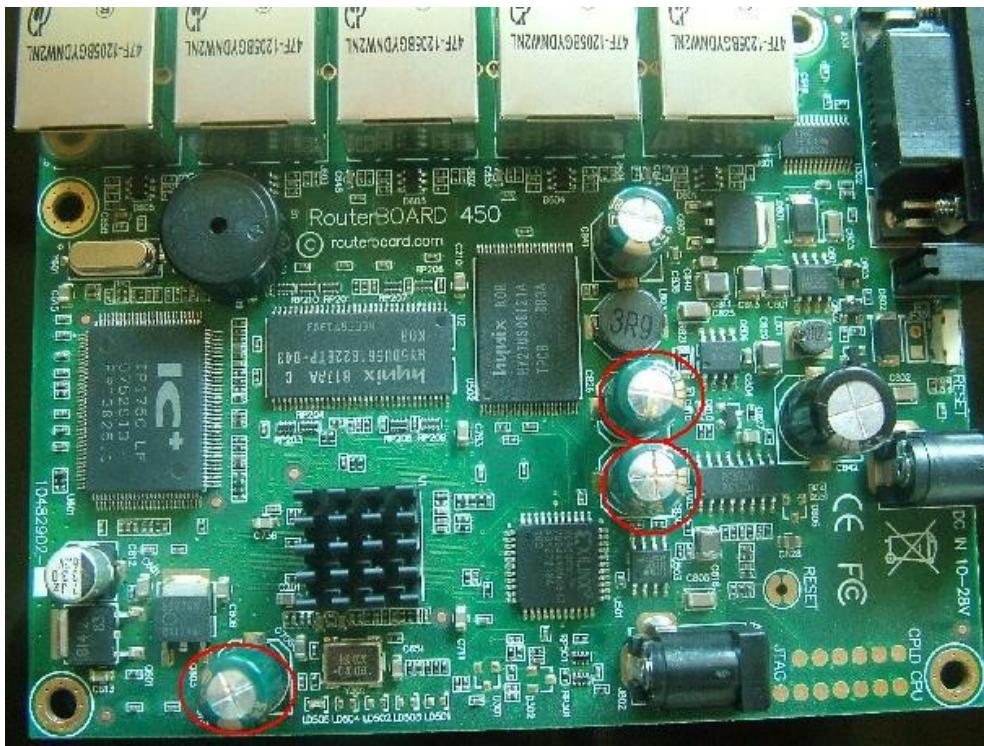


Berhubung unitnya udah berumur hampir 2 tahun, sy relakan untuk masuk ke ruang operasi , kalau masih garansi saran saya lebih baik di kontak ke vendor dulu dah,

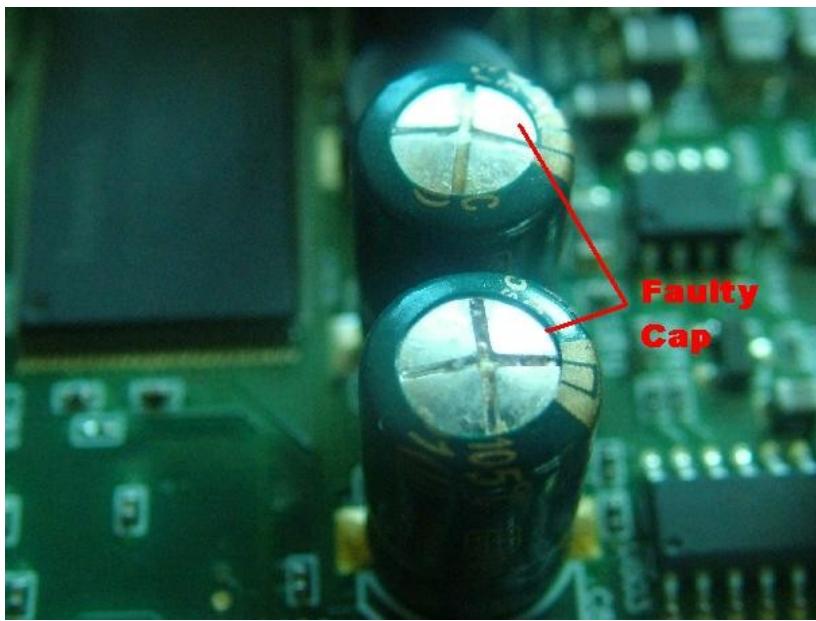
dengan membuka 4 sekrup casing luar dan 4 sekrup mounting board. pengecekan tegangan sepintas menunjukan 3,3V normal, begitu pula tegangan RAM 2,5v, namun ada satu yang menarik perhatian ternyata

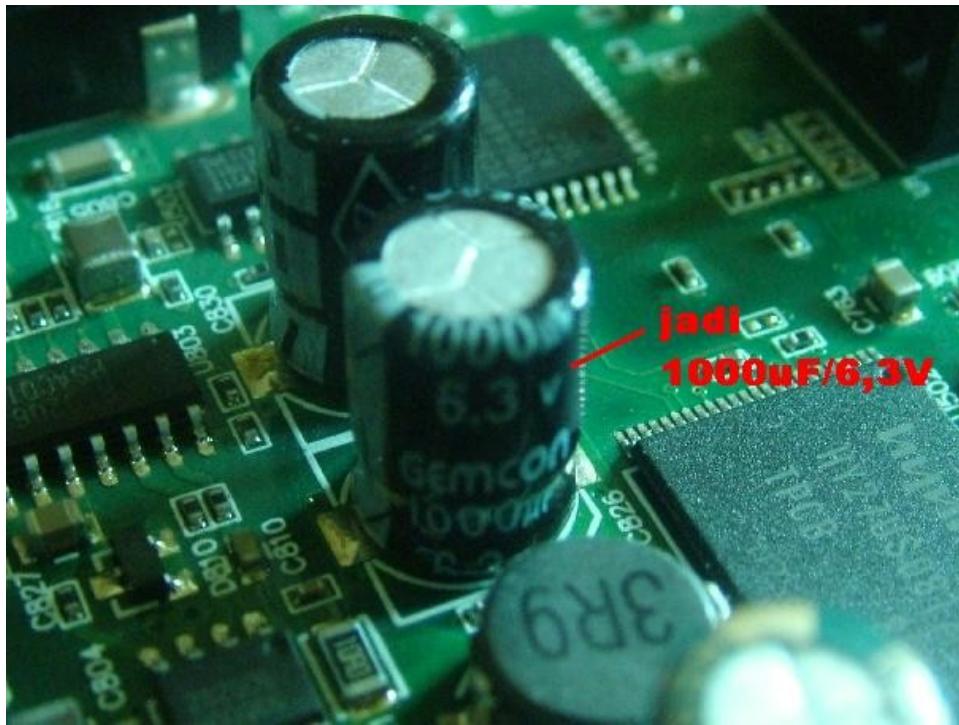


ada 3 kapasitor coupling yang sepertinya milik regulator dalam kondisi "hamil"..., pengamatan kemudian dilanjutkan, sepertinya tidak ada komponen lain yg terbakar, lampu power masih menyala, hanya unit tidak mau booting

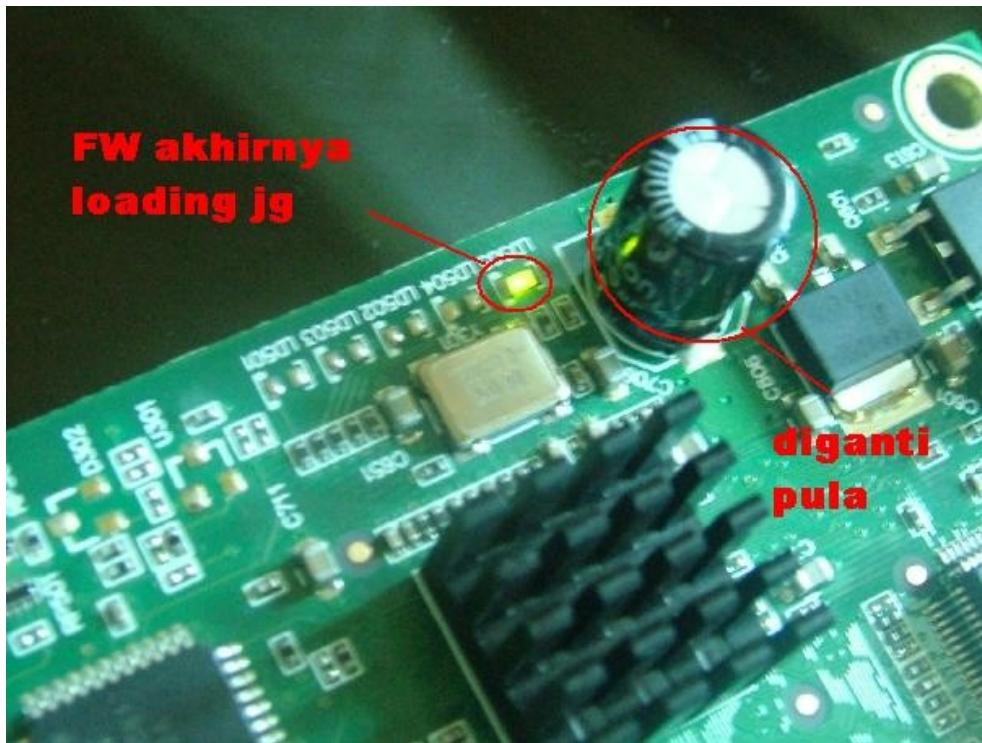


akhirnya kami putuskan untuk mencoba mengganti dl ketiga kapasitor 560uF/6.3v yg "hamil" (melengdung) ini dengan kapasitor lain dengan asumsi teg regulator mungkin tidak benar2 normal dengan performa cap tsb, setelah mengobrik abrik gudang, akhirnya berhasil nemu 3 biji 1000uF/6.3v, emang tidak sama, tp sepertinya ketiga C tersebut bukan untuk switching reg, lebih mirip Coupling tank, yah sdhlah cukup layak.. akhirnya operasi transplantasi dilakukan...





Setelah diganti ternyata unit bisa booting dengan normal, LED flash juga mulai berkedip kembali dan suara beep terdengar lagi, tanda2 kehidupan sdh nampak kembali, unit segera kami test, ternyata konfigurasi agak berubah dari aslinya karena satu dan lain hal, beruntung masih ada backup konfigurasi, unit kembali hidup..mudah2an nih RB masih bisa tahan hidup beberapa tahun lagi, semoga berguna kalau ada kasus yg mirip,



## **1 Userman Banyak Hotspot**

Kalau mau ngeset radius di mikrotik biar user2nya bisa dipakai oleh banyak server hotspot gimana ya caranya ?

Contoh:

Computer A, mau dijadikan pusat database user hotspot, juga menjalankan service hotspot

Kemudian ada computer B, yang cuma menjalankan service hotspot saja tetapi database Radiusnya ngambil ke computer A, yang di setting di computer B di apanya saja ya ?

Sudah coba router Userman di computer B diarahkan ke IP computer A, kok nggak bisa ya?  
Address radius di Computer B juga diarahkan ke IP computer A, tetap tidak bisa...

Berikut referensinya :

# **Centralized Authentication for Hotspot user**

## **From MikroTik Wiki**

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

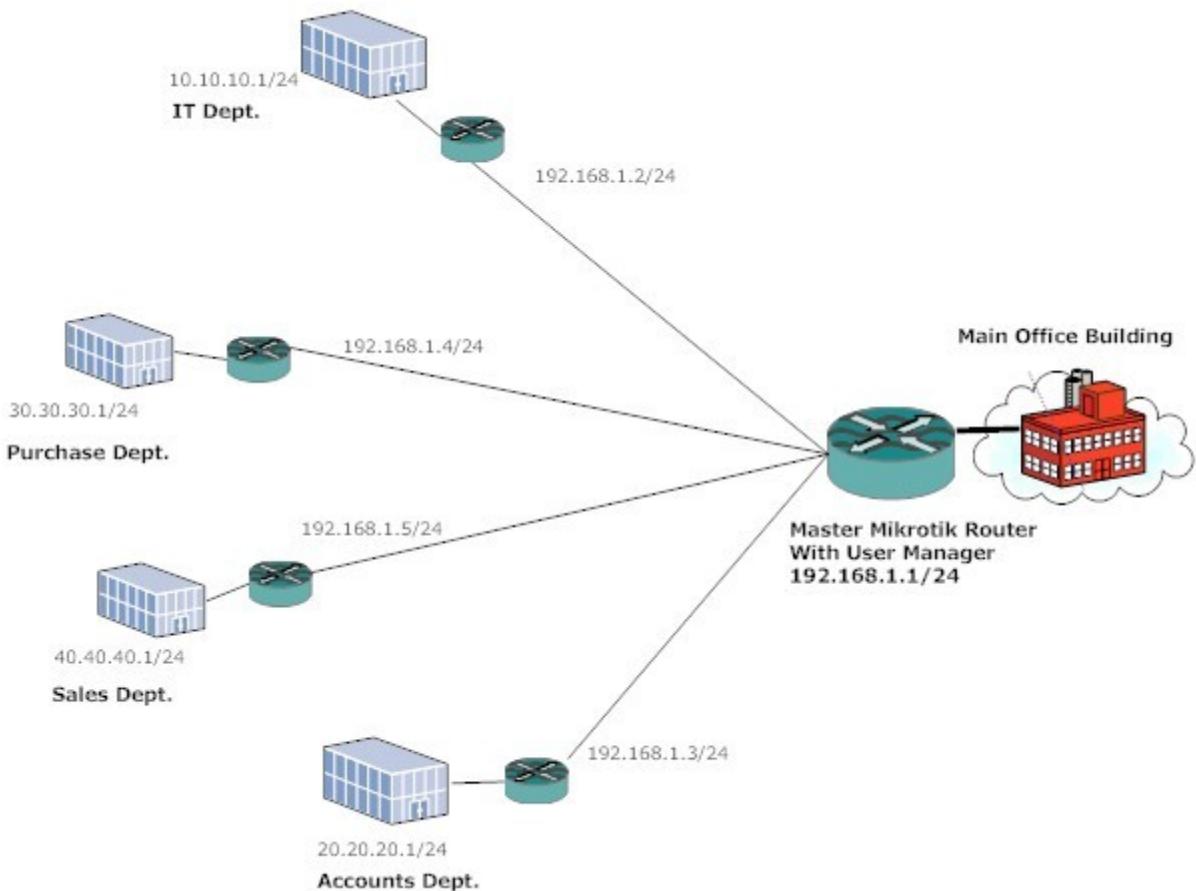
Generally we are using external Radius servers for user authentication as MikroTik is not Radius server. But here in this example we use the MikroTik User Manager which works as a Radius server and does authentication and control of your Hotspot users.

### **[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.

NEED the Solution..??? - Pl Contact.

**ASHISH PATEL - [anpatel@eitl.elecon.com](mailto:anpatel@eitl.elecon.com) - +91 2692 227275 - +91 99098 90908.**

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

## recovery password mikrotik



uda ane prakteking ternyata bisa.....

awal cerita PC router di kantor ada yang ganti passwdnya coba googling nemu tuh link mtpass v0.3, ternyata udah gagak bisa di pake tuh mtpassnya.....alhasil passwd masih tercript...trus ane coa googling lg nemu mtpass v0.5, dan hasilnya maknus passwdnya bisa terbaca semua dengan jelas...aseeeek

langkahnya :

Quote:

1. booting PC router pake cd linux live CD kayak ubuntu ato apalah yg laennya (ane sih ake ubuntu)
2. kalo uda masuk dekstopnya kemudian copy file user.dat letaknya di **/nova/store/user.dat** (copy pake flashdisk ato apalah terserah). trus reboot dan masuk mikocok lagi...
3. pindah ke PC yang ada OS linuxnya (distro terserah asal uda di install pakage **g++**, ane pake debian lenny).
4. extrak dulu file mtpass v0.5 pake perintah **tar -xvfj namafile**
5. masuk ke direktori hasil extrak trus compile file mtpass.cpp dengan perintah **g++ -lssl -lcrypto mtpass.cpp -o mtpass(nama file hasil compile)**
6. hasilnya ada file baru yaitu mtpass, trus copy file user.dat dalam folder tempat mtpass(nama file hasil compile)
7. finishing jalankan dengan perintah **./mtpass user.dat**
8. contoh hasilnya :

```
banksonk:~/home/banksonk/mtpass-0.5# g++ -lssl -lcrypto mtpass.cpp -o mtpass
banksonk:~/home/banksonk/mtpass-0.5# ./mtpass user.dat
mtpass v0.5 - MikroTik RouterOS password recovery tool, (c) 2008-2009 by manio

Reading file user.dat, 516 bytes long

Rec# | Username      | Password          | Disable flag | User comment
---+---+---+---+---+---+
1  | ok            | ok               |              |
2  | salin         | <BLANK PASSWORD> |              |
3  | salin         | joss              |              |
4  | janu2          | jevi              |              |
5  | janu           | janul             |              |
6  | kakang         | kanmas            |              |
7  | janu2          | jevi              |              |

banksonk:~/home/banksonk/mtpass-0.5#
```

\*\*yang mau mtpass v0.5 ada di <http://www.istanaku.biz> pada bagian koleksi file

thanks

banksonk

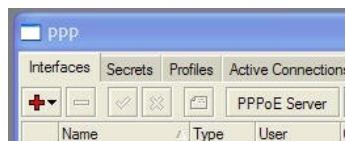
**Cara buat PPPOE server**

Cara buat PPPOE server di mikrotik :

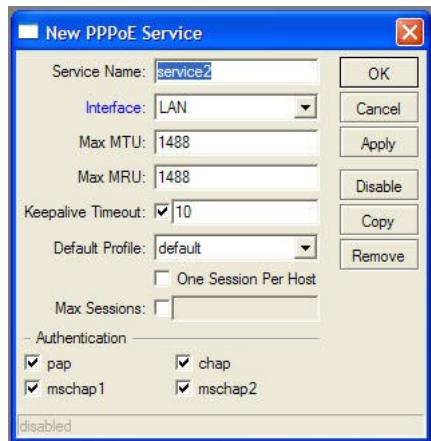
klik menu PPP



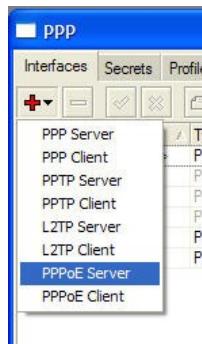
lalu klik PPPOE server



ganti interface sesuai dengan interface yang bakal di gunakan untuk koneksi PPPOE misal LAN atau ether2



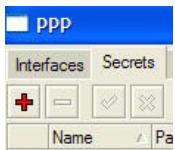
kemudian add interface PPPOE server dari PPP



kosongin aja username klik OK



add username & password buat di client, klik sub menu secret



lalu buat username & password



local address itu untuk gateway pppoe sedang remote address itu ip yang bakal di dapat klien.  
selesai pembuatan PPPOE server.

trimakasih

**misahin download dan browsing?**

## **PERTANYAAN :**



maaf sebelumnya jika pernah di bahas, saya sudah coba cari cari blom ketemu , , di beberapa trit ada yg membahas memblokir IDM tp tidak bisa, pertanyaanya mungkin sedikit sama yaitu mungkin tidak jika kita pisahin jalun browsing dengan download?

tujuan utama sih untuk melimit download dan unlimit brousing.



jadi jika pelanggan hanya sekedar brousing tidak perlu saya batasi, tp jika dalam kondisi download pelanggan saya batasi

atau jika beberapa pelanggan sedang download tiba tiba ada pelanggan yg lain sedang rekwas untuk brousing makan jalur brousing di utamakan sementara download tidak di prioritaskan

## **JAWABAN :**

misal di buat manglenya :

/ip firewall mangle

```
add chain=prerouting action=mark-connection new-connection-mark=conn-download passthrough=yes
```

```
protocol=tcp dst-port=80 connection-bytes=1000000-0 comment="CONN-DOWNLOAD"
```

```
add chain=prerouting action=mark-packet new-packet-mark=download-packet passthrough=no connection-mark=conn-download
```

```
add chain=prerouting action=mark-connection new-connection-mark=conn-browsing passthrough=yes
```

```
protocol=tcp dst-port=80 connection-bytes=0-1000000 comment="CONN-BROWSING"
```

```
add chain=prerouting action=mark-packet new-packet-mark=browsing-packet passthrough=no connection-mark=conn-browsing
```

nah..setelah itu tinggal di buatin queue-tree utk prioritas dan traffict shapingnya.. dan queue tree nya seperti ini :

/queue tree

```
add name="paket browsing" parent=global-in packet-mark=browsing-packet limit-at=0 queue=default
```

```
priority=1 max-limit=0 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
add name="paket download" parent=global-in packet-mark=download-packet limit-at=0 queue=default
```

```
priority=2 max-limit=0 burst-limit=0 burst-threshold=0 burst-time=0s
```



*NB : bener banget!!!! deteksi pake connection bytes... tapi buat LB agak2 ribet konfigurasinya karena gerbangnya banyak... udha gitu gabisa deteksi pake interface lagi.*

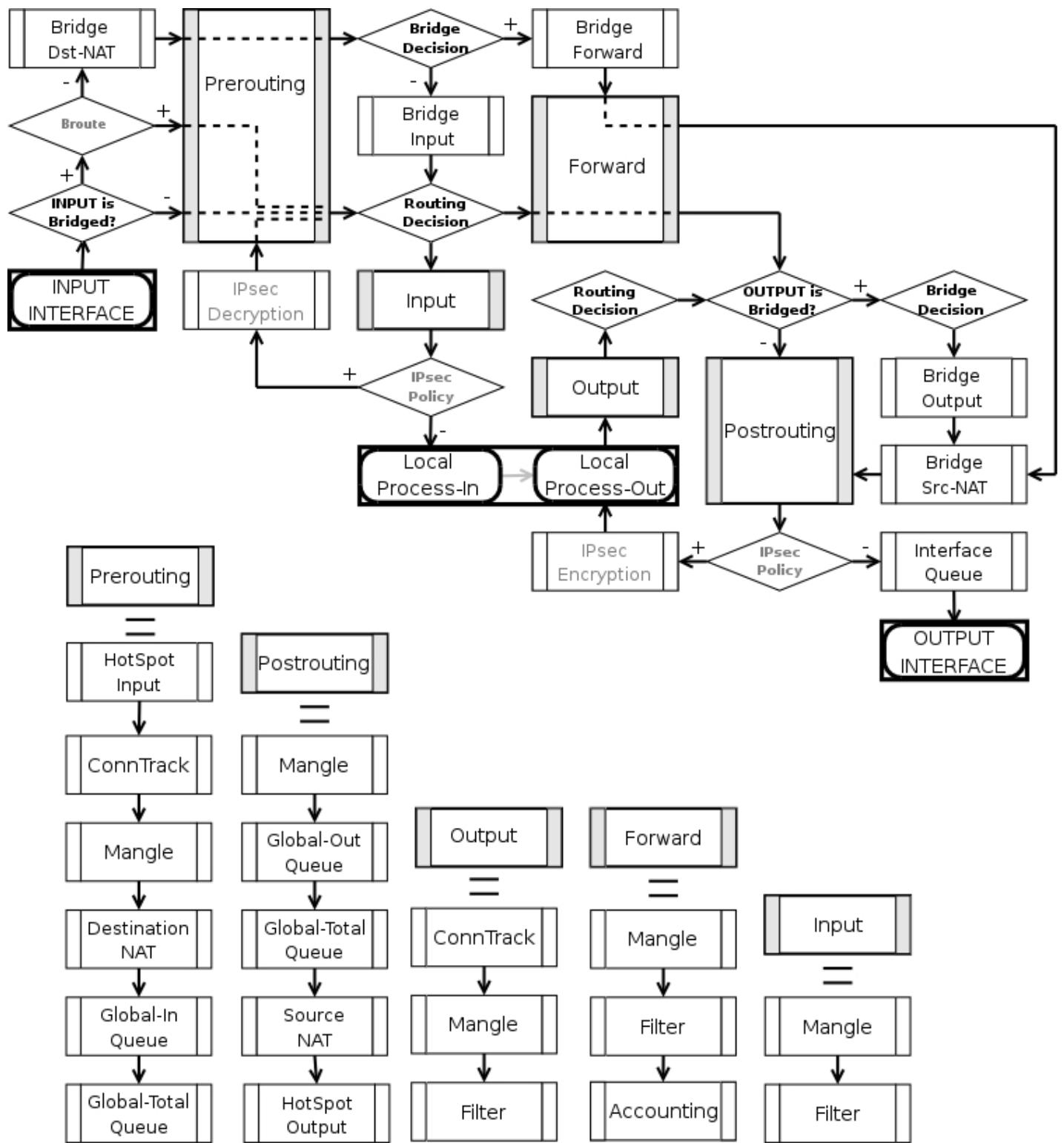
*TAPI :*

pake iface tidak bisa klo LB. tp bisa pake logical iface "global-in" (masuk dalam prerouting) untuk nerapkan prioritas. dan "global-out" ( masuk dalam postrouting) utk traffic shapingnya..

lebih jelasnya bs di lihat di packet-flow/ip-flow mikrotik.

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

GAMBAR sebagai berikut :



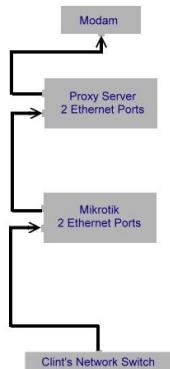
## Beberapa Konfigurasi Mikrotik dan Proxy

**Notice**, Disini hanya ditampilkan sejumlah konfigurasi proxy dan mikrotik yang mungkin dilakukan tanpa membahas mana yang lebih baik karena kondisi yang berbeda akan membutuhkan konfigurasi yang berbeda pula. Dan disini hanya akan menjelaskan konfigurasi mikrotik tanpa menjelaskan konfigurasi Proxy.

---

### Example 1

Example 1,



### Configuration:

Dalam konfigurasi ini tidak ada yang perlu dilakukan. Cukup konfigurasi mikrotik secara normal demikian pula dengan Proxy. Proxy di Mikrotik tidak perlu diaktifkan, tapi jika anda ingin mengaktifkan sebenarnya juga tidak membawa masalah. Jika web-proxy mikrotik dihidupkan, kita bisa saja melakukan redirect port 80 ke port web-proxy transparan (normalnya 3128) dengan perintah berikut :

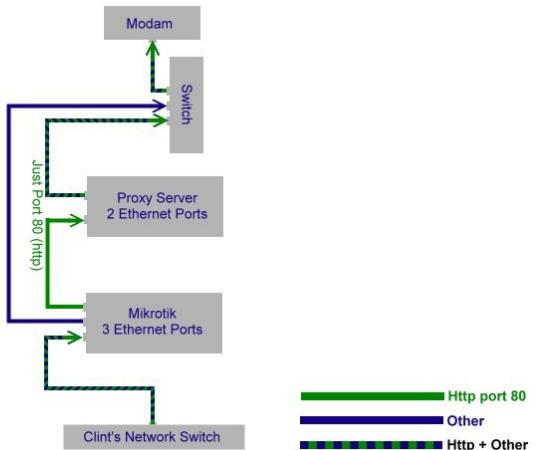
```
/ip firewall nat add chain=dstnat action=redirect to-ports=3128 protocol=tcp dst-port=80
```

---

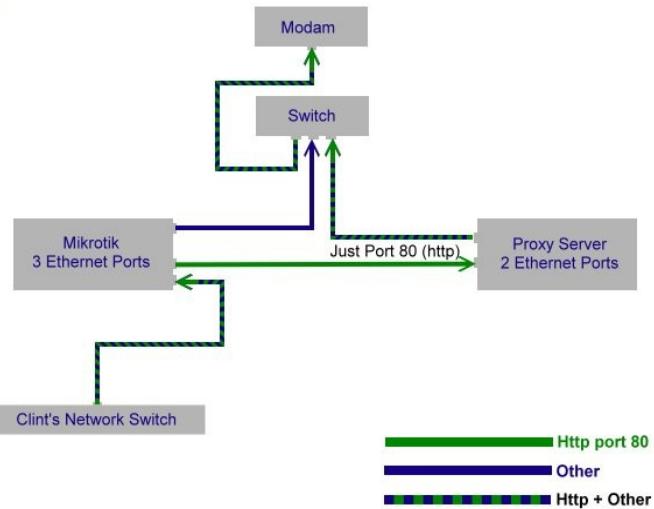
### Example 2

Hanya traffic port http (port 80) yang melalui Proxy-Server, sedangkan yang lain langsung ke modem :

Example 2, A



### Example 2.B



### Configuration:

**1st) IP Client's Network (IP Range 192.168.0.0/24 Gateway-IP 192.168.0.1)**

Mikrotik Network 3 Interface (eth1 for clients = 192.168.0.1) (eth2 for Modem = 192.168.10.2) (eth3 for Proxy-Server = 192.168.5.2)

Modem Network, IP-Address 192.168.10.1

Proxy-Server Network 2 Interface (eth1 for Mikrotik = 192.168.5.1) (eth2 for Modem (for direct internet) = 192.168.10.3)

**2nd) Mikrotik Configuration :**

**1)Firewall, /ip firewall nat add chain=dstnat dst-address=192.168.0.1 protocol=tcp dst-port=80 action=dst-nat to-addresses=192.168.5.1 to-ports=80**

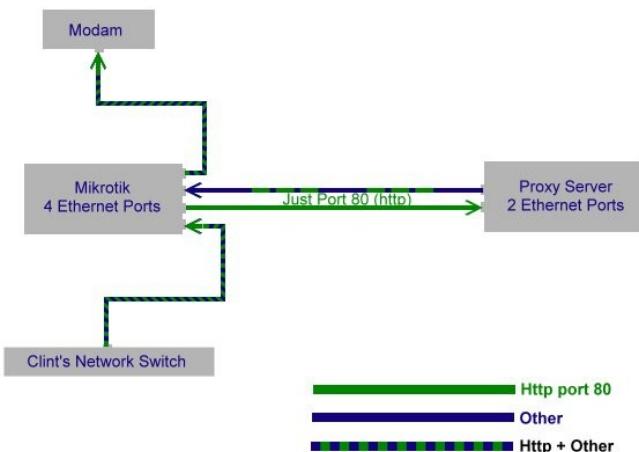
**2)Web-Proxy, bisa dihidupkan dengan Parent proxy ke (192.168.5.1 port-80)**

---

### Example 3

Hanya traffic http (port 80) yang lewat Proxy-Server, sedangkan traffic lain langsung ke modem tapi Proxy Server tetap menjadi client Mikrotik sehingga tetap bisa dikendalikan oleh Mikrotik.

### Example 3,



### **Configuration:**

#### 1st) Network IP Address Details

Client's Network (IP Range 192.168.0.0/24 Gateway-IP 192.168.0.1)

Mikrotik, 4 Interface, Interface IP-Address (eth1 for clients = 192.168.0.1) (eth2 for Modem = 192.168.10.2) (eth3 for http traffic to Proxy-Server = 192.168.5.2) (eth4 for give internet to Proxy-Server = 192.168.6.1)

Modem Network, IP-Address 192.168.10.1

Proxy-Server Network, 2 Interface, Interface IP-Address (eth1 for Mikrotik = 192.168.5.1) (eth2 for Internet Bring IN = 192.168.6.2)

#### 2nd) Mikrotik Configuration

1)**Firewall**, /ip firewall nat add chain=dstnat dst-address=192.168.0.1 protocol=tcp dst-port=80 action=dst-nat to-addresses=192.168.5.1 to-ports=80

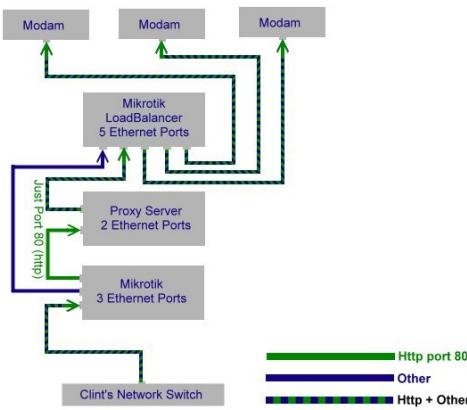
2)**Web-Proxy**, bisa dihidupkan dan pasang parent proxy ke (192.168.5.1 port-80)

---

### Example 4

Sama dengan **Example-2**, hanya kita menambahkan Core-Router With Load-Balancer, Client-Gateway Router melewaskan traffic http (port 80) ke Proxy-Server, sedangkan traffic lain langsung ke Core-Router

Example 4,



### Configuration:

#### 1st) Network IP Address Details

Client's Network (IP Range 192.168.0.0/24 Gateway-IP 192.168.0.1)

Mikrotik Network 3 Interface (eth1 for clients = 192.168.0.1) (eth2 for Core-Router = 192.168.10.2) (eth3 for http traffic to Proxy-Server = 192.168.5.2)

Core-Router, IP-Address (eth4 for Proxy-Server = 192.168.9.1) (eth5 for Mikrotik = 192.168.10.1) (eth1, eth2, eth3, for Modem's)

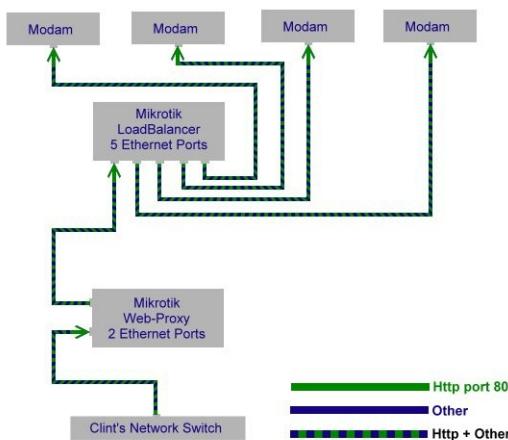
Proxy-Server Network 2 Interface (eth1 for Mikrotik = 192.168.5.1) (eth2 for Core-Router (for direct internet) = 192.168.9.2)

---

### Example 5

Mikrotik utama dengan Load-Balancer dan Mikrotik gateway dengan Web-Proxy, semua traffic dari client langsung ke Mikrotik utama (**tanpa External Proxy Server hanya menggunakan Mikrotik Web-Proxy**)

Example 5,



## Queue dengan SRC-NAT dan WEB-PROXY

Pada penggunaan queue (bandwidth limiter), penentuan CHAIN pada MANGLE sangat menentukan jalannya sebuah rule. Jika kita memasang SRC-NAT dan WEB-PROXY pada mesin yang sama, sering kali agak sulit untuk membuat rule QUEUE yang sempurna. Penjelasan detail mengenai pemilihan CHAIN, dapat dilihat pada manual Mikrotik di <http://www.mikrotik.com/docs/ros/2.9/ip/flow>

Percobaan yang dilakukan menggunakan sebuah PC dengan Mikrotik RouterOS versi 2.9.28. Pada mesin tersebut, digunakan 2 buah interface, satu untuk gateway yang dinamai PUBLIC dan satu lagi untuk jaringan lokal yang dinamai LAN.

Code:

```
[admin@instaler] > in pr
Flags: X - disabled, D - dynamic, R - running
#      NAME      TYPE    RX-RATE   TX-RATE     MTU
0  R  public    ether      0          0       1500
1  R  lan       wlan      0          0       1500
```

Dan berikut ini adalah IP Address yang digunakan. Subnet 192.168.0.0/24 adalah subnet gateway mesin ini.

Code:

```
[admin@instaler] > ip ad pr
Flags: X - disabled, I - invalid, D - dynamic
#  ADDRESS      NETWORK      BROADCAST      INTERFACE
0  192.168.0.217/24  192.168.0.0  192.168.0.255  public
1  172.21.1.1/24    172.21.1.0  172.21.1.255  lan
```

Fitur web-proxy dengan transparan juga diaktifkan.

Code:

```
[admin@instaler] > ip web-proxy pr
      enabled: yes
      src-address: 0.0.0.0
      port: 3128
      hostname: "proxy"
      transparent-proxy: yes
      parent-proxy: 0.0.0.0:0
      cache-administrator: "webmaster"
      max-object-size: 4096KiB
      cache-drive: system
      max-cache-size: none
      max-ram-cache-size: unlimited
      status: running
      reserved-for-cache: 0KiB
      reserved-for-ram-cache: 154624KiB
```

Fungsi MASQUERADE diaktifkan, juga satu buah rule REDIRECTING untuk membelokkan traffic HTTP menuju ke WEB-PROXY

Code:

```
[admin@instaler] ip firewall nat> pr
Flags: X - disabled, I - invalid, D - dynamic
0  chain=srcnat out-interface=public
   src-address=172.21.1.0/24 action=masquerade
1  chain=dstnat in-interface=lan src-address=172.21.1.0/24
   protocol=tcp dst-port=80 action=redirect to-ports=3128
```

Berikut ini adalah langkah terpenting dalam proses ini, yaitu pembuatan MANGLE. Kita akan membutuhkan 2 buah PACKET-MARK. Satu untuk paket data upstream, yang pada contoh ini kita sebut **test-up**. Dan satu lagi untuk paket data downstream, yang pada contoh ini kita sebut **test-down**.

Untuk paket data upstream, proses pembuatan manglenya cukup sederhana. Kita bisa langsung melakukannya

dengan 1 buah rule, cukup dengan menggunakan parameter SRC-ADDRESS dan IN-INTERFACE. Di sini kita menggunakan chain **prerouting**. Paket data untuk upstream ini kita namai **test-up**.

Namun, untuk paket data downstream, kita membutuhkan beberapa buah rule. Karena kita menggunakan translasi IP/masquerade, kita membutuhkan Connection Mark. Pada contoh ini, kita namai **test-conn**. Kemudian, kita harus membuat juga 2 buah rule. Rule yang pertama, untuk paket data downstream non HTTP yang langsung dari internet (tidak melewati proxy). Kita menggunakan chain **forward**, karena data mengalir melalui router.

Rule yang kedua, untuk paket data yang berasal dari WEB-PROXY. Kita menggunakan chain **output**, karena arus data berasal dari aplikasi internal di dalam router ke mesin di luar router.

Paket data untuk downstream pada kedua rule ini kita namai **test-down**.

Jangan lupa, parameter passthrough hanya diaktifkan untuk connection mark saja.

Code:

```
[admin@instaler] > ip firewall mangle print
Flags: X - disabled, I - invalid, D - dynamic
0    ;;; UP TRAFFIC
      chain=prerouting in-interface=lan
      src-address=172.21.1.0/24 action=mark-packet
      new-packet-mark=test-up passthrough=no

1    ;;; CONN-MARK
      chain=forward src-address=172.21.1.0/24
      action=mark-connection
      new-connection-mark=test-conn passthrough=yes

2    ;;; DOWN-DIRECT CONNECTION
      chain=forward in-interface=public
      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=172.21.1.0/24 action=mark-packet
      new-packet-mark=test-down passthrough=no
```

Untuk tahap terakhir, tinggal mengkonfigurasi queue. Di sini kita menggunakan queue tree. Satu buah rule untuk data downstream, dan satu lagi untuk upstream. Yang penting di sini, adalah pemilihan parent. Untuk downstream, kita menggunakan parent **lan**, sesuai dengan interface yang mengarah ke jaringan lokal, dan untuk upstream, kita menggunakan parent **global-in**.

Code:

```
[admin@instaler] > queue tree pr
Flags: X - disabled, I - invalid
0    name="downstream" 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="upstream" 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
```

Variasi lainnya, untuk bandwidth management, dimungkinkan juga kita menggunakan tipe queue PCQ, yang bisa secara otomatis membagi trafik per client.

## Mikrotik - menggunakan squid sebagai web proxy sehingga lebih optimal

untuk lebih mudah saya menggunakan 2 virtual server, yaitu :

1. IP Mikrotik:

- 192.168.10.15 = local
- 192.168.12.15 = proxy
- 192.168.5.181 = public/ke modem speedy

2. IP squid (pakai IPCop)

- 192.168.12.1 = ip green(procyy)

3. IP Client: 192.168.10.0/24

ok di ipcop disetting dulu bahwa web proxynya jalan di port 878 <= terserah anda aktifkan cachenya misal 15M atau 15000 <= untuk testing

sekarang kita masuk ke mikrotiknya:

Code:

```
/ ip address
add address=192.168.5.181/24 network=192.168.5.0 broadcast=192.168.5.255 \
    interface=Public comment="" disabled=no
add address=192.168.10.15/24 network=192.168.10.0 broadcast=192.168.10.255 \
    interface=Lan comment="" disabled=no
add address=192.168.12.15/24 network=192.168.12.0 broadcast=192.168.12.255 \
    interface=Proxy comment="" disabled=no
```

setting route:

Code:

```
/ ip route
add dst-address=0.0.0.0/0 gateway=192.168.5.15 scope=255 target-scope=10 \
    comment="" disabled=no
```

setting dns:

Code:

```
/ ip dns
set primary-dns=192.168.5.182 secondary-dns=192.168.5.205 \
    allow-remote-requests=no cache-size=2048KiB cache-max-ttl=1w
/ ip dns static
add name="192.168.5.3" address=192.168.5.3 ttl=1d
```

setting nat:

Code:

```
/ ip firewall nat
add chain=dstnat protocol=tcp dst-port=81 action=dst-nat \
    to-addresses=192.168.12.1 to-ports=81 comment="Untuk IP Cop" disabled=no
add chain=dstnat protocol=tcp dst-port=445 action=dst-nat \
    to-addresses=192.168.12.1 to-ports=445 comment="Untuk HTTPS IPCOP" \
    disabled=no
add chain=dstnat src-address=!192.168.12.0/24 protocol=tcp dst-port=80 \
    action=dst-nat to-addresses=192.168.12.1 to-ports=878 comment="" disabled=no
add chain=dstnat src-address=!192.168.12.0/24 protocol=tcp dst-port=443 \
    action=dst-nat to-addresses=192.168.12.1 to-ports=878 comment="" \
    disabled=no
add chain=srcnat out-interface=Public action=masquerade comment="" disabled=no
```

nah terus ini yang paling penting, setting mangle:

Code:

```
/ ip firewall mangle
add chain=forward content="X-Cache: HIT" action=mark-connection \
    new-connection-mark=squid_con passthrough=yes comment="" disabled=no
add chain=forward connection-mark=squid_con action=mark-packet \
    new-packet-mark=squid_pkt passthrough=no comment="" disabled=no
add chain=forward connection-mark=!squid_con action=mark-connection \
    new-connection-mark=all_con passthrough=yes comment="" disabled=no
add chain=forward protocol=tcp src-port=80 connection-mark=all_con \
    action=mark-packet new-packet-mark=http_pkt passthrough=no comment="" \
    disabled=no
add chain=forward protocol=icmp connection-mark=all_con action=mark-packet \
    new-packet-mark=icmp_pkt passthrough=no comment="" disabled=no
add chain=forward protocol=tcp dst-port=1973 connection-mark=all_con \
    action=mark-packet new-packet-mark=top_pkt passthrough=no comment="" \
    disabled=no
add chain=forward connection-mark=all_con action=mark-packet \
    new-packet-mark=test_pkt passthrough=no comment="" disabled=no
```

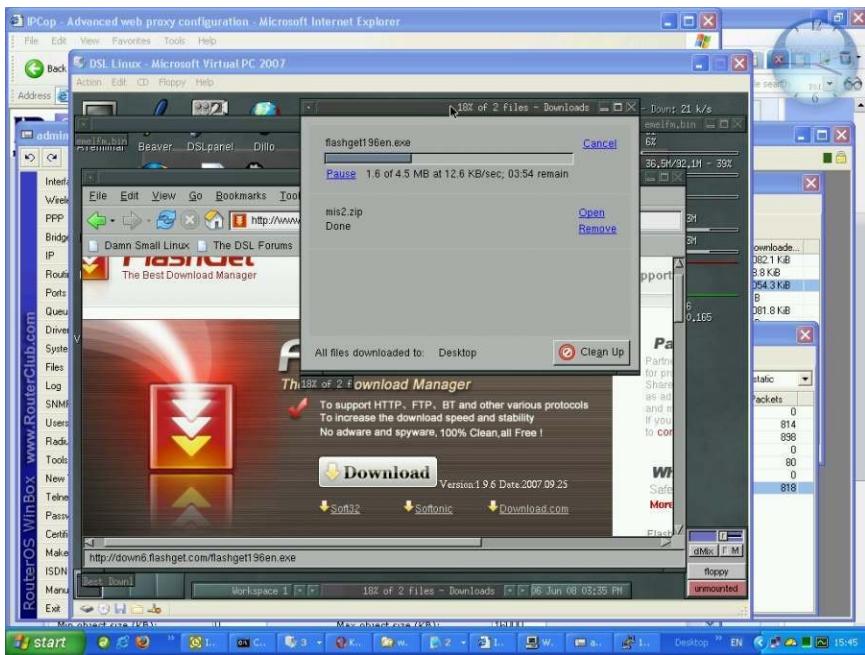
terus queue :

Code:

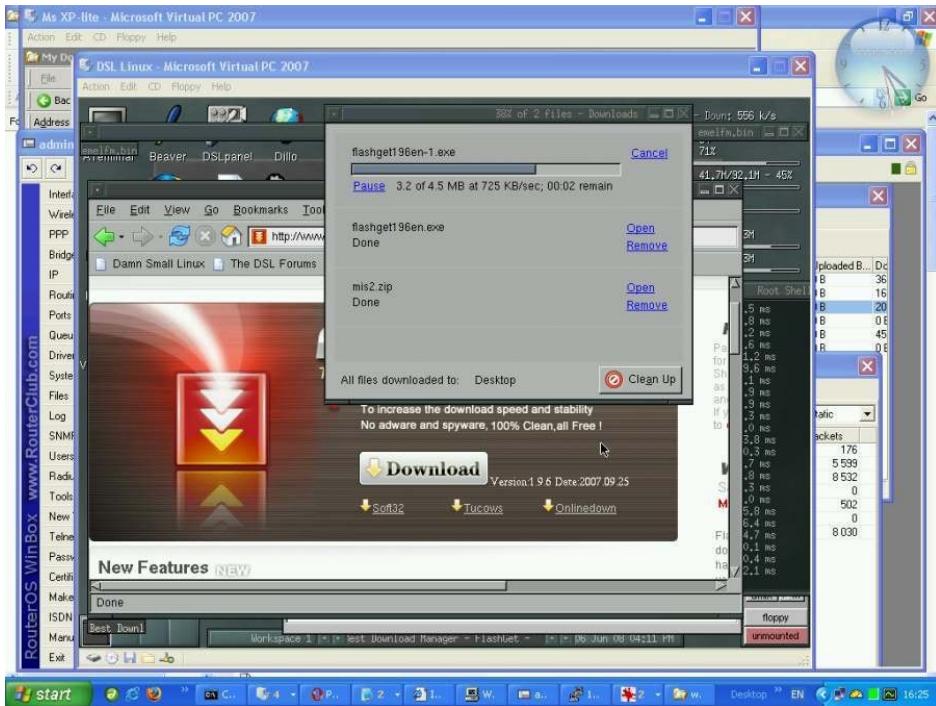
```
/ queue simple
add name="Squid_HIT" dst-address=0.0.0.0/0 interface=all parent=None \
    packet-marks=squid_pkt direction=both priority=8 \
    queue=default-small/default-small limit-at=0/0 max-limit=0/0 \
    total-queue=default-small disabled=no
add name="Main_Link" dst-address=0.0.0.0/0 interface=all parent=None \
    direction=both priority=8 queue=default-small/default-small limit-at=0/0 \
    max-limit=35000/256000 total-queue=default-small disabled=no
add name="game_tales_of_pirate" dst-address=0.0.0.0/0 interface=all \
    parent=None packet-marks=top_pkt direction=both priority=1 \
    queue=default-small/default-small limit-at=0/0 max-limit=0/0 \
    total-queue=default-small disabled=no
add name="Ping_queue" dst-address=0.0.0.0/0 interface=all parent=None \
    packet-marks=icmp_pkt direction=both priority=2 \
    queue=default-small/default-small limit-at=0/0 max-limit=0/0 \
    total-queue=default-small disabled=no
add name="The_other_port_queue" target-addresses=192.168.12.0/24 \
    dst-address=0.0.0.0/0 interface=all parent=Main_Link packet-marks=http_pkt \
    direction=both priority=8 queue=default-small/default-small \
    limit-at=5000/5000 max-limit=50000/256000 total-queue=default-small \
    disabled=no
add name="another_port" target-addresses=192.168.10.0/24 dst-address=0.0.0.0/0 \
    interface=all parent=Main_Link packet-marks=test_pkt direction=both \
    priority=8 queue=default-small/default-small limit-at=0/0 \
    max-limit=0/256000 total-queue=default-small disabled=no
```

hasilnya:

pertama mencache:



kedua hasil cachenya:



ini terinspirasi dari tutorial akange dan dari video yang aku coba tidak berhasil

NB: Maaf ya soalnya salah paste settingan NAT nya, harap maklum, masih newbie ni tadi juga kelupaan. jadi nat-nya yang di transparent port 80 dan port https 443

Selamat Mencoba ya

## Beda Limit Siang dan Malam secara otomatis

Untuk Script Limit bandwith malam :

System > Scripts > New Script isikan data berikut :

### Name : Limit Malam

Policy : Conteng Read, Policy dan Write

Source : /queue simple set user1 limit-at=64000/128000 max-limit=64000/128000 total-limit-at=128000 total-max-limit=128000

System > Scheduler > New Schedule isikan data berikut :

### Name : Malam

Start Date : (tgl mulai disesuaikan dengan tgl di mikrotik) jun/07/2007

Start Time : (waktu mulai disesuaikan kebutuhan) 19:00:00 (untuk jam 7 mlm)

Interval : 1d 00:00:00 (rolling per 1 hari)

### On Event : Limit Malam

Untuk Script Limit bandwith siang :

1.System > Scripts > New Script isikan data berikut :

### Name : Limit Siang

Policy : Conteng Read, Policy dan Write

Source : /queue simple set user1 limit-at=32000/64000 max-limit=32000/64000 total-limit-at=64000 total-max-limit=64000

2.System > Scheduler > New Schedule isikan data berikut :

### Name : Siang

Start Date : (tgl mulai disesuaikan dengan tgl di mikrotik) jun/07/2007

Start Time : (waktu mulai disesuaikan kebutuhan) 07:00:00 (untuk jam 7 pagi)

Interval : 1d 00:00:00 (rolling per 1 hari)

### On Event : Limit Siang

Langkah diatas otomatis akan memberikan limit siang 32k/64k mulai 7 pagi s/d jam 7 mlm sedangkan malam hari 64k/128k mulai 7 mlm s/d jam 7 pagi. Setting bisa disesuaikan dengan kebutuhan, untuk MT versi 3 keatas silahkan disesuaikan dengan keadaan karena berbeda sedikit.

Kendalanya kalo pake scheduler, kalo pas waktunya mesin mikrotik mati (mati lampu misalnya), lewat deh batasannya. Kalo di mikrotik v3.xx (di versi 2.xx sering bermasalah) ada cara utk menyiasati: **Hanya dibutuh 1 script, pada script, tambahkan pendekripsi waktu:**

```
:if ([/system clock get time] < [:totime 06:59:59]) do={  
/queue simple set user1 limit-at=64000/128000 max-limit=64000/128000 total-limit-at=128000 total-max-limit=128000  
}  
else {  
:if ([/system clock get time] < [:totime 19:00:00]) do={  
/queue simple set user1 limit-at=32000/64000 max-limit=32000/64000 total-limit-at=64000 total-max-limit=64000  
}  
else {  
/queue simple set user1 limit-at=64000/128000 max-limit=64000/128000 total-limit-at=128000 total-max-limit=128000  
}  
}
```

2. Pada scheduler buat interval misalkan 30 menit, dengan begini walau mati lampu pada waktu yg ditentukan, batasan malam/siang tetap terkontrol.

## Script untuk block Conflicker Virus secara otomatis

Script ini dibuat untuk mendeteksi komputer di LAN yang terinfeksi virus Conflicker. Banyak cara lain yang dipergunakan untuk mengatasi serangan virus ini, namun script ini bertujuan untuk mengidentifikasi komputer yang terkena virus tanpa melakukan tindakan pencegahan/pembersihan.

Script ini dapat di copy pastekan langsung di script mikrotik melalui winbox dan dibuatkan dalam scheduler. Karena keterbatasan huruf pada script hanya 4096 huruf, maka script ini hanya akan mem-block virus Conflicker varian A dan B.

Pada varian C, terdapat 50,000 domain lebih setiap hari sementara yang dipergunakan hanya 500. Dan walaupun kita berhasil mengidentifikasi 500 domain tersebut, jumlah karakternya tetap akan melampaui 4096 karakter, sehingga tidak dapat dibuat dalam script ini.

Saat ini versi script lain sedang dibuat untuk memblok varian C. Untuk lengkapnya, silakan baca di sini : <http://bits.blogs.nytimes.com/2009/03/19/the-conficker-worm-april-fools-joke-or-unthinkable-disaster/>.

Analysis of Conficker.C is available here - <http://mtc.sri.com/Conficker/addendumC/index.html>

domain lists (originally sourced from <http://blogs.technet.com/msrc/archive/2009/02/12/conficker-domain-information.aspx>) into daily lists as the mikrotik cannot import files above 4096 characters.

Komplet list silakan di download di sini : <http://www.epicwinrar.com/conficker/domains.txt> atau mirror copies di <http://www.epicwinrar.com/conficker/>

The lists the script below uses are ones I've cut from the original domains list and broken up into day by day sections, you're welcome to leave the script intact and download these lists with my consent. Please let me know if this has helped you out, its good to know when my work is used elsewhere :-)

The lists I've created I'm still exporting one at a time, but will eventually go up until 06/30/2009

## **[edit] The Daily IP List**

This script does the following:

- Checks todays date
- Downloads the matching domainlist file (\$month-\$day-\$year.txt)
- Confirms the file downloaded contains data (is > 0)
- Removes any current address list entries for 'daily-conficker'
- Resolves and adds todays domains into address-list 'daily-conficker'
- Deletes the downloaded text file

Note that you could easily change the script to point to a copy of the lists hosted on a more local server.

script name: daily-conficker-list

```

:local date [/system clock get date]
:local month [:pick $date 0 3]
:local day [:pick $date 4 6]
:local year [:pick $date 7 11]

#set month to numerical value
:if ([$month] = "jan") do={ :set month "01" }
:if ([$month] = "feb") do={ :set month "02" }
:if ([$month] = "mar") do={ :set month "03" }
:if ([$month] = "apr") do={ :set month "04" }
:if ([$month] = "may") do={ :set month "05" }
:if ([$month] = "jun") do={ :set month "06" }
:if ([$month] = "jul") do={ :set month "07" }
:if ([$month] = "aug") do={ :set month "08" }
:if ([$month] = "sep") do={ :set month "09" }
:if ([$month] = "oct") do={ :set month "10" }
:if ([$month] = "nov") do={ :set month "11" }
:if ([$month] = "dec") do={ :set month "12" }

#download current days domain list
/tool fetch address=www.epicwinrar.com host=www.epicwinrar.com mode=http src-path="conficker/$month-$day-$year.txt"
:log info "Download Complete"
:delay 2

#check to ensure todays file exists before deleting yesterdays list
:log info "Begining Address List Modification"
:if ( [/file get [/file find name="$month-$day-$year.txt"] size] > 0 ) do={

    /ip firewall address-list remove [/ip firewall address-list find list=daily-conficker]

    :local content [/file get [/file find name="$month-$day-$year.txt"] contents] ;
    :local contentLen [ :len $content ] ;

    :local lineEnd 0;
    :local line "";
    :local lastEnd 0;

    :do {
        :set lineEnd [:find $content "\n" $lastEnd] ;
        :set line [:pick $content $lastEnd $lineEnd] ;
        :set lastEnd ( $lineEnd + 1 ) ;

#resolve each new line and add to the address list daily-conficker. updated to list
domain as comment
        :if ( [:pick $line 0 1] != "\n" ) do={
            :local entry [:pick $line 0 ($lineEnd) ]
            :if ( [:len $entry] > 0 ) do={
                :local listip [:resolve "$entry"]
                :if ( $listip != "failure" ) do={
                    :if ((/ip firewall address-list find list=daily-conficker
address=$listip) = "") do={
                        /ip firewall address-list add list=daily-conficker address=$listip
comment=$entry
                            :log info "$listip"
                        } else={:log info "duplicate IP $entry"}
                    }
                }
            }
        }
    }
} while ($lineEnd < $contentLen)
}

```

```
:log info "Address List Modification Complete"  
#cleaning up  
/file remove "$month-$day-$year.txt"
```

Scheduler Entry (can be pasted into terminal)

```
/system scheduler  
add comment="" disabled=no interval=1d name=Conficker-daily on-event="/system script run  
daily-conficker-list" start-date=jan/01/1970 start-time=00:00:01
```

## **[edit] The Results**

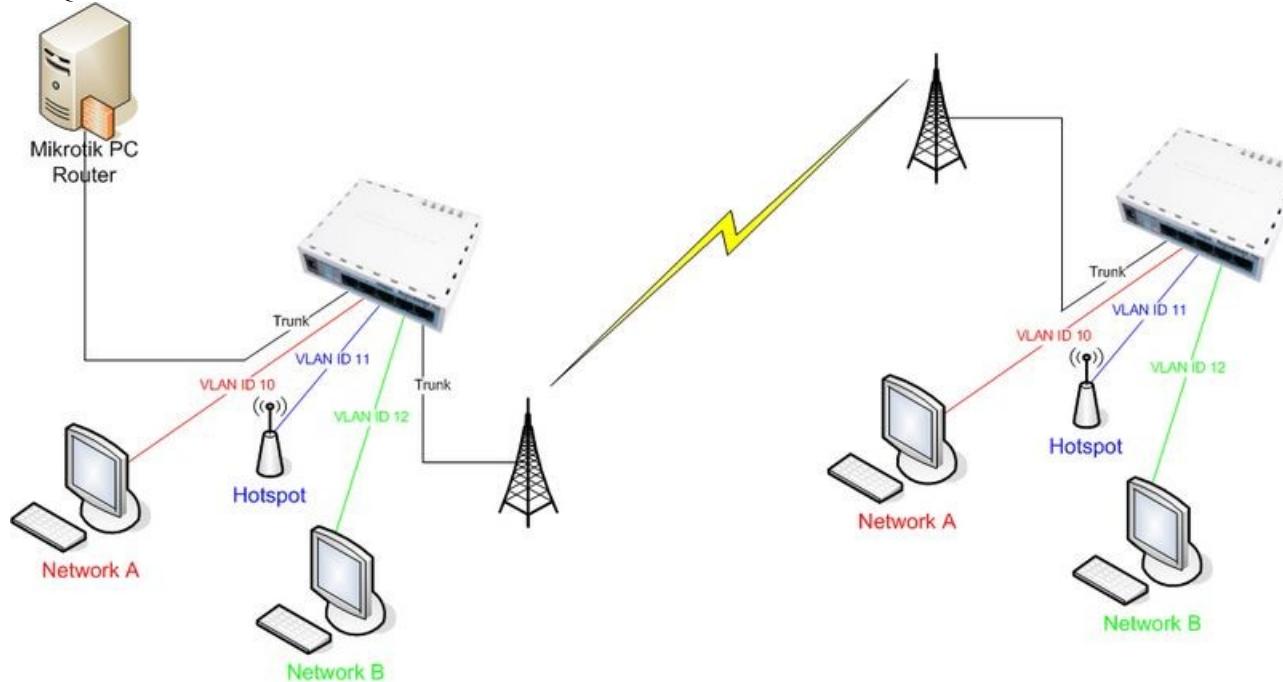
This gives you a list of the ip's that conficker will try to contact each day. What you actually use this for is up to you, but in my case I've then created a simple rule that searches for http connection to those servers and logs the src IP address for me.

```
/ip firewall filter  
add action=add-src-to-address-list address-list=conficker-infected address-list-  
timeout=1d chain=forward comment="label conficker-infected" disabled=no dst-address-  
list=\  
    daily-conficker dst-port=80 protocol=tcp
```

You could probably go one step further and have the list of these emailed to you and deleted each day but I don't have the time to go into that much detail here .. if you do however want that, feel free to leave a note on the discussion page and I'll get around to it as soon as I can.

## VLAN di RB750 (Requested by bro Hakeem)

REQUEST:



Nantinya supaya sesama vlan id yg sama akan bisa ngobrol. Tapi jika dengan vlan id yg berbeda, mereka ndak bisa saling ngobrol.

### KONFIGURASI: INTERFACE:

admin@00:0C:42:5A:73:53 (MikroTik) - WinBox v3.29 on RB750 (mipsbe)

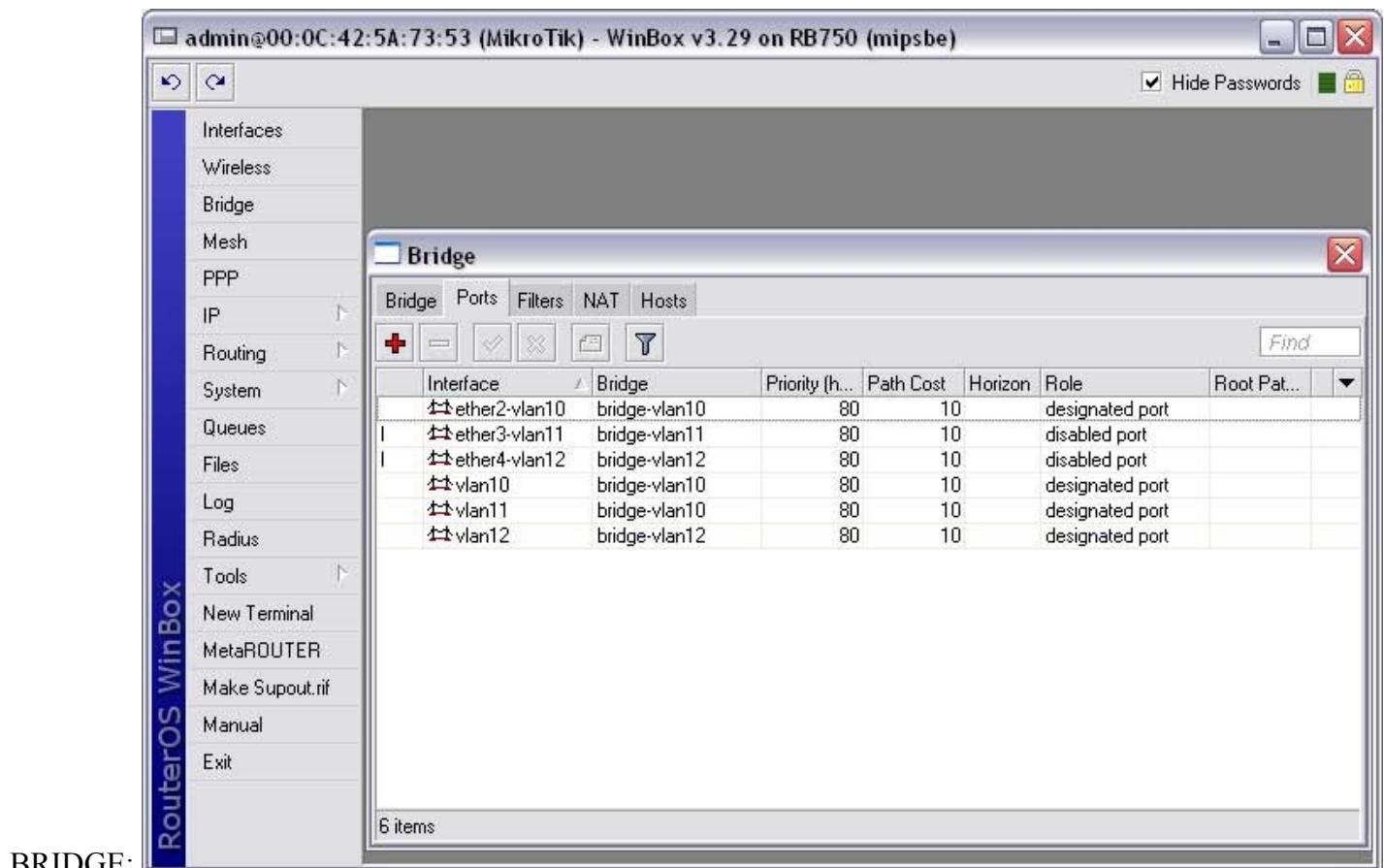
Interfaces Wireless Bridge Mesh PPP IP Routing System Queues Files Log Radius Tools New Terminal MetaROUTER Make Supout.if Manual Exit

Hide Passwords

Interface List

Interface	Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	Tx Drops
R	bridge-vlan10	Bridge	1520	0 bps	11.9 kbps	0	17	0
R	bridge-vlan11	Bridge	65535	0 bps	0 bps	0	0	0
R	bridge-vlan12	Bridge	1520	0 bps	0 bps	0	0	0
R	ether1	Ethernet	1526	0 bps	0 bps	0	0	0
R	ether2-vlan10	Ethernet	1524	110.4 kbps	7.9 kbps	26	9	0
R	ether3-vlan11	Ethernet	1524	0 bps	0 bps	0	0	0
R	ether4-vlan12	Ethernet	1524	0 bps	0 bps	0	0	0
R	ether5-trunk	Ethernet	1524	22.6 kbps	7.4 kbps	26	10	0
R	vlan10	VLAN	1520	8.2 kbps	6.3 kbps	9	10	0
R	vlan11	VLAN	1520	14.4 kbps	0 bps	17	0	0
R	vlan12	VLAN	1520	0 bps	0 bps	0	0	0

11 items [1 selected]



BRIDGE:

TEST PING:

```
Command Prompt

C:\Documents and Settings\Admin>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Documents and Settings\Admin>
```

SCRIPT:

```
/interface vlan
add arp=enabled comment="" disabled=no interface=ether5-trunk l2mtu=1520 mtu=1500 name=vlan10 use-
service-tag=no vlan-id=10
add arp=enabled comment="" disabled=no interface=ether5-trunk l2mtu=1520 mtu=1500 name=vlan11 use-
```

```
service-tag=no vlan-id=11
add arp=enabled comment="" disabled=no interface=ether5-trunk l2mtu=1520 mtu=1500 name=vlan12 use-
service-tag=no vlan-id=12

/interface bridge
add admin-mac=00:00:00:00:00:00 ageing-time=5m arp=enabled auto-mac=yes comment="" disabled=no
forward-delay=15s l2mtu=1520 max-message-age=20s mtu=1500 name=bridge-vlan10 priority=0x8000
protocol-mode=none transmit-hold-count=6
add admin-mac=00:00:00:00:00:00 ageing-time=5m arp=enabled auto-mac=yes comment="" disabled=no
forward-delay=15s l2mtu=65535 max-message-age=20s mtu=1500 name=bridge-vlan11 priority=0x8000
protocol-mode=none transmit-hold-count=6
add admin-mac=00:00:00:00:00:00 ageing-time=5m arp=enabled auto-mac=yes comment="" disabled=no
forward-delay=15s l2mtu=1520 max-message-age=20s mtu=1500 name=bridge-vlan12 priority=0x8000
protocol-mode=none transmit-hold-count=6

/interface bridge port
add bridge=bridge-vlan10 comment="" disabled=no edge=auto external-fdb=auto horizon=none
interface=ether2-vlan10 path-cost=10 point-to-point=auto priority=0x80
add bridge=bridge-vlan10 comment="" disabled=no edge=auto external-fdb=auto horizon=none
interface=vlan10 path-cost=10 point-to-point=auto priority=0x80
add bridge=bridge-vlan11 comment="" disabled=no edge=auto external-fdb=auto horizon=none
interface=ether3-vlan11 path-cost=10 point-to-point=auto priority=0x80
add bridge=bridge-vlan10 comment="" disabled=no edge=auto external-fdb=auto horizon=none
interface=vlan11 path-cost=10 point-to-point=auto priority=0x80
add bridge=bridge-vlan12 comment="" disabled=no edge=auto external-fdb=auto horizon=none
interface=ether4-vlan12 path-cost=10 point-to-point=auto priority=0x80
add bridge=bridge-vlan12 comment="" disabled=no edge=auto external-fdb=auto horizon=none
interface=vlan12 path-cost=10 point-to-point=auto priority=0x80
```

Jika ingin melakukan copy paste, mohon disesuaikan nama interfacenya.

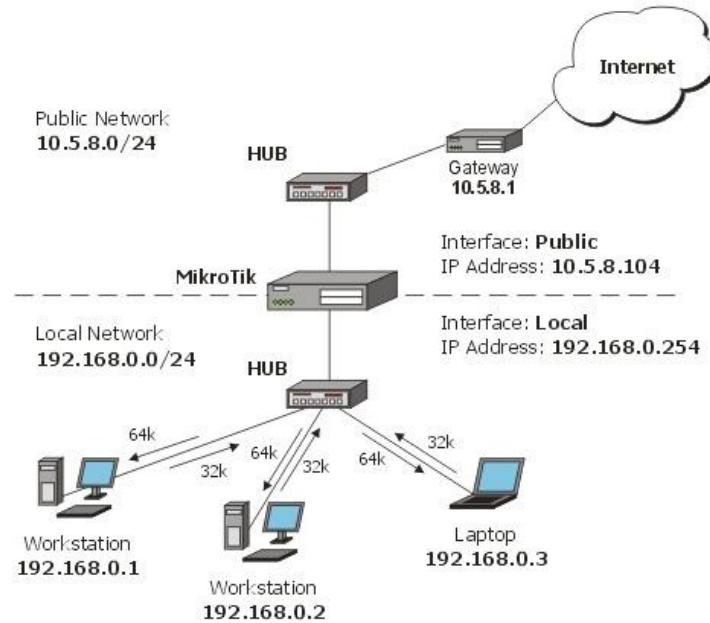
Konfigurasi untuk kedua RB sama.

## Contoh Implementasi PCQ

PCQ (Per Connection Queue) adalah jenis queue yang dapat digunakan untuk membagi atau membatasi traffic untuk multi-users secara dinamis, dengan sedikit administrasi.

### Pembagian Bandwidth Sama Rata Untuk Multi Users

Gunakan queue jenis PCQ bila kita ingin membagi bandwidth secara rata (dan mengatur max-limit) untuk beberapa user. Kita akan memberikan contoh untuk pembagian limit bandwidth download sebesar 64 kbps dan upload sebesar 32 kbps.



Ada dua cara untuk melakukan ini : Menggunakan mangle dan queue tree atau Menggunakan Simple Queue

### Dengan Mangle dan Queue Tree

1. Mark paket dengan mark-packet all :

Code:

```
/ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=all  
passthrough=no
```

2. Tambahkan 2 PCQ Type, satu untuk download dan satunya lagi untuk upload. Dst-Address adalah pengklasifikasian untuk traffic Download, sedang Src-Address adalah pengklasifikasian untuk traffic Upload :

Code:

```
/queue type add name="PCQ_download" kind=pcq pcq-rate=64000 pcq-classifier=dst-address  
/queue type add name="PCQ_upload" kind=pcq pcq-rate=32000 pcq-classifier=src-address
```

3. Akhirnya, 2 buah rule queue ditambahkan, untuk download dan upload :

Code:

```
/queue tree add parent=global-in queue=PCQ_download packet-mark=all  
/queue tree add parent=global-out queue=PCQ_upload packet-mark=all
```

## Dengan Simple Queue

Jika anda tidak suka menggunakan mangle dan queue tree, anda dapat menggunakan satu rule queue seperti dibawah ini :

Code:

```
/queue simple add queue=PCQ_upload/PCQ_download target-addresses=192.168.0.0/24
```

Sekedar tamabahn nih buat bro [a] yang nulis diatas, CMIIW yah ;-p

First of all kan marking packet yang buat up dulu nih :

**/ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=up passthrough=no**

terus buat marking yang download-an kita pake kaya gini :

**/ip firewall mangle add chain=forward action=mark-connection new-mark-connection=down-conn  
passthrought=yes**

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

jangan lupa chain di set forward, dan passthrought di set no untuk connection-mark dan di set yes untuk packet-mark

setelah itu baru deh kita buat queque typenya :

**/queue type add name="PCQ\_download" kind=pcq pcq-rate=64000 pcq-classifier=dst-address  
/queue type add name="PCQ\_upload" kind=pcq pcq-rate=32000 pcq-classifier=src-address**

ini kalo kita ingin membatasi up 32k dan down 64k, kalo kita pengen dia otomatis kaya yang bro ALOE tanyain kita bisa masukin ajah pcq-rate=0 jadi nantinya dia akan langsung menyesuaikan bandwidth yang ada dan pengguna yang ada di jaringan Local

selanjutnya tinggal bikin deh wuewue tree nya :

**/queue tree add name=upload parent=global-in  
/queue tree add name=download parent=Local**

untuk upload kita menggunakan parent global-in karena kita ingin membatasi semua yang masuk menuju router, sedangkan untuk download kita menggunakan parent Local, karena inilah interface yang menuju ke jaringan lokal kita

selanjutnya tinggal bikin ajah anakan dari tree induk yang sudah kita buat diatas:

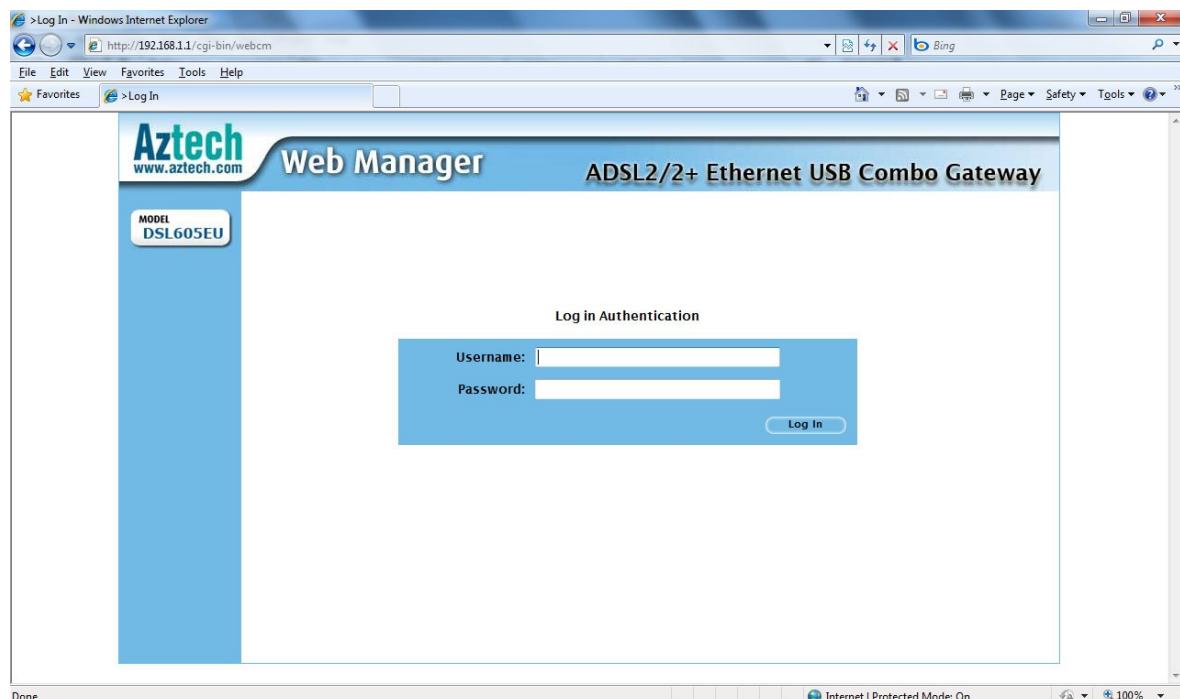
**/queue tree add name=client-upload parent=upload queue=PCQ\_upload packet-mark=up  
/queue tree add name="download" parent=Local queue=PCQ\_download packet-mark=down**

Nah sekarang setiap client kita akan mendapatkan bw 32k/64k dan kalau kita menggunakan 0 pada saat menset queue type bw akan otomatis terbagi 😊

## Setting Bridge dan dial PPPoE dari Mikrotik

Sampai saat ini, masih banyak yang bertanya bagaimana cara setting bridge untuk modem ADSL (Speedy), untuk memudahkan semuanya, berikut saya berikan tutorial dan gambar gambarnya:

Modem yang saya gunakan adalah merk Aztech, type DSL605EU (modem gratisan dari telkom). Gambar sengaja saya buat agak besar, biar jelas.



-- Connect ke IP modem

The screenshot shows a Windows Internet Explorer window with the URL <http://192.168.1.1/cgi-bin/webcm>. The title bar says "Basic> Home - Windows Internet Explorer". The main content area is titled "Aztech Web Manager" and "ADSL2/2+ Ethernet USB Combo Gateway". It displays a "Basic> Home" section with a "Connection Information" table and a "Router Information" table. The "Connection Information" table includes rows for DSL (UP), Downstream / Upstream (Kbps) (379/92), and a note to click [here](#) for quickstart. The "Router Information" table lists System Uptime (925 hours 28 minutes), Model (DSL605EU), Firmware Version (113.106.2s), Build (003), Ethernet MAC address (00:30:0A:D4:70:C7), DSL MAC address (00:30:0A:D4:70:C9), USB MAC address (00:30:0A:D4:70:C8), NAT (Enabled), and Firewall (Enabled). On the left sidebar, there are links for Basic (Home, Quick Start), Advanced (WAN, LAN, Application, QoS, Routing, Security, Status, Diagnostics, System Password, Firmware Upgrade, Save Settings, Restart Router, Restore To Default), Help (PPP Connection Help, LAN Configuration, LAN Clients Help, Firewall Help, Bridge Filters Help, QoS Help), and a "Basic" link. The status bar at the bottom shows "Done", "Internet | Protected Mode: On", and "100%".

-- Halaman utama

Basic>Home

Connection Information

DSL	UP	System Uptime	925 hours 30 minutes
	379/92	Model	DSL605EU
		Firmware Version	113.106.2s
		Build	003
		Ethernet MAC address	00:30:0A:D4:70:C7
		DSL MAC address	00:30:0A:D4:70:C9
		USB MAC address	00:30:0A:D4:70:C8
		NAT	Enabled
		Firewall	Enabled

Router Information

Local Network Information

LAN IP Address	192.168.1.1
DHCP	Disabled
DHCP Range	-
Ethernet	Connected

-- Gerakan kursor ke WAN, kemudian pilih "My Connection", kalau nggak ada, silahkan pilih "New Connection"

Advanced>WAN>MyConnection Setup

Bridged Connection

Connection Name:	MyConnection	Type:	Bridge	Sharing:	Disable
Options:		VLAN ID:	0	Priority Bits:	0

PVC Settings

PVC:	New
VPI:	0
VCI:	35
QoS:	UBR
PCR:	0 cps
SCR:	0 cps
MBS:	0 cells
CDVT:	0 usecs

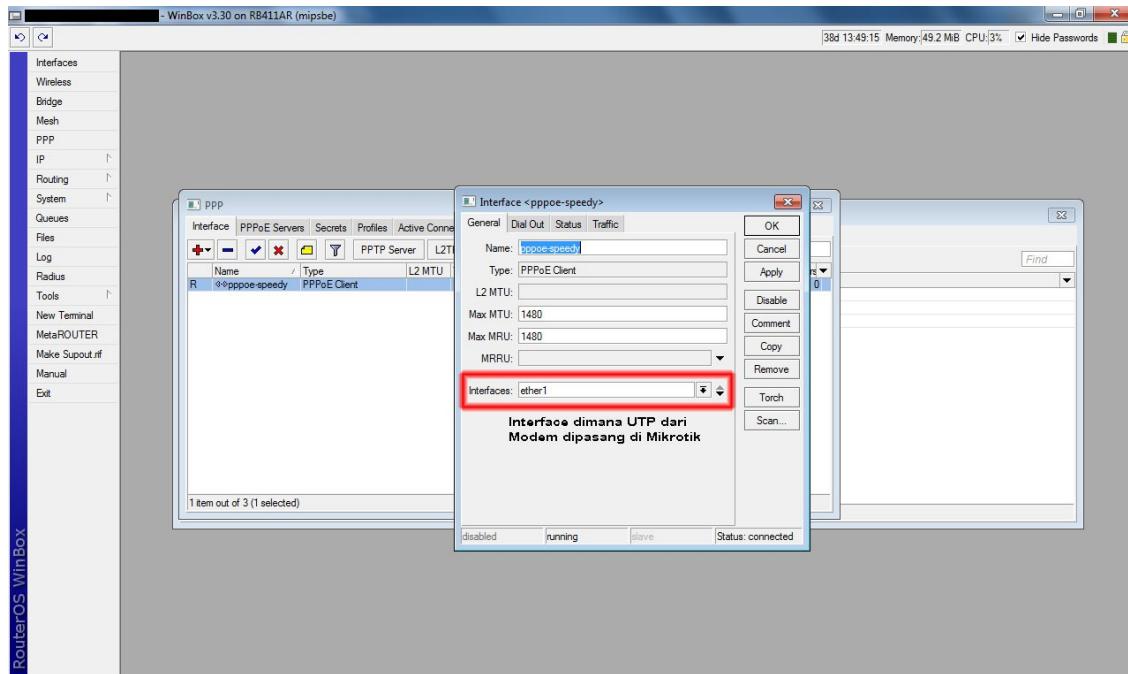
Auto PVC:

Submit   Delete

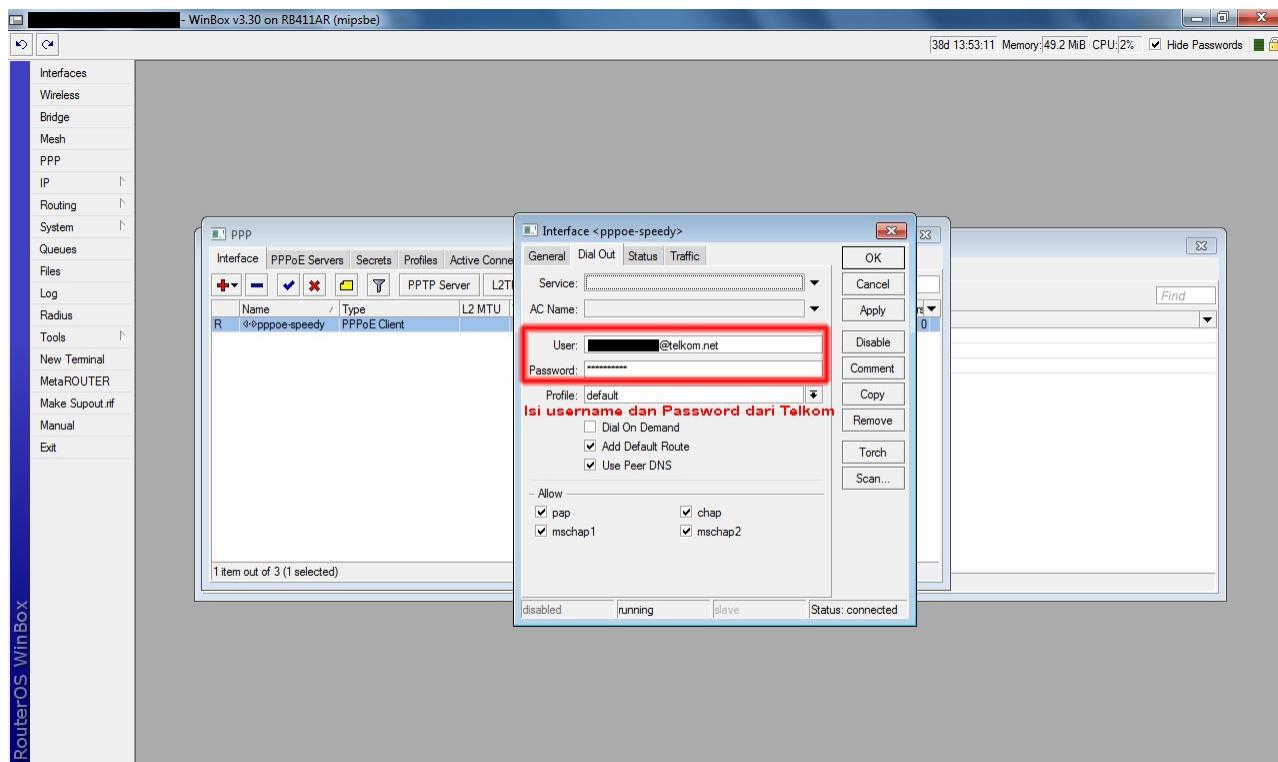
-- Hanya perlu melakukan konfigurasi type "Bridge"

Selesai, konfigurasi modem hanya seperti itu saja.

Sekarang untuk konfigurasi Mikrotik.  
Saya menggunakan RB411AR dengan OS 3.30

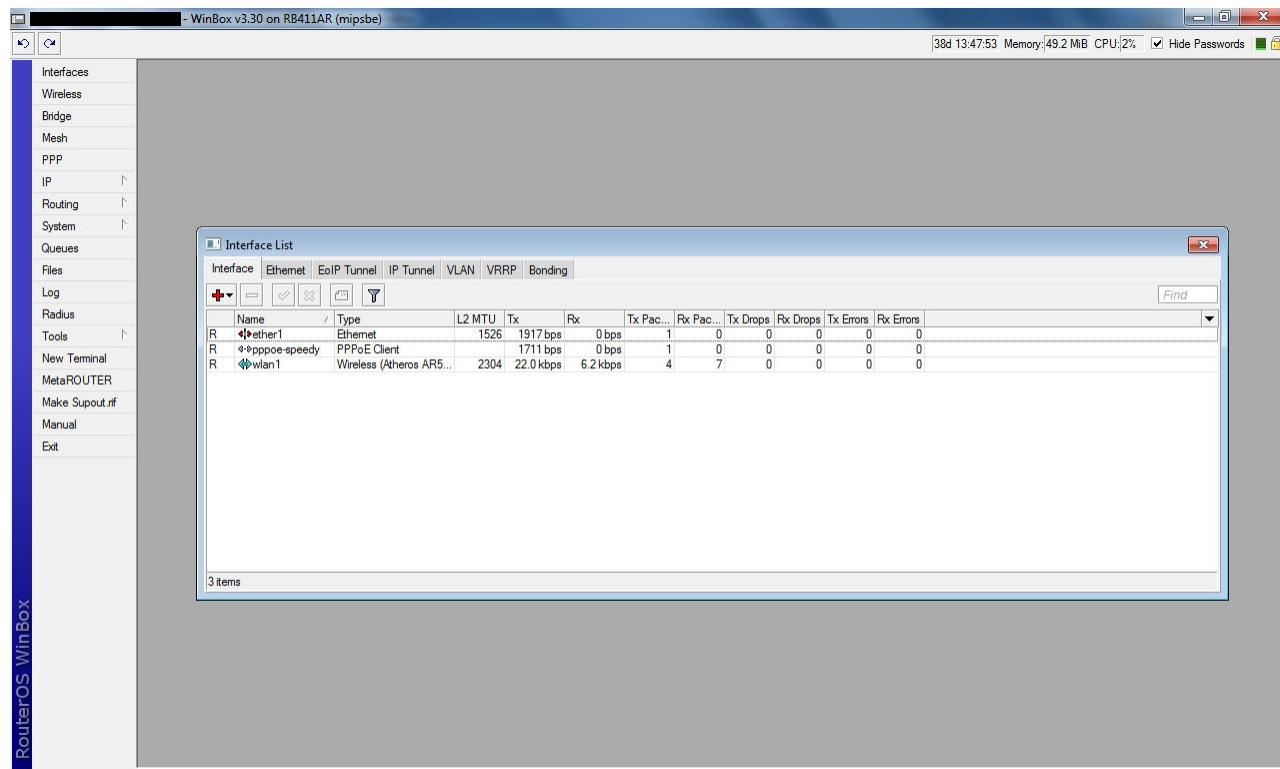


- Pilih menu PPP, kemudian pilih tanda "+", lalu pilih "PPPoE Client"
- Pada tab "General", masukkan nama yang diinginkan, kemudian pilih Interface yang akan digunakan



- Pada tab "Dial Out", masukkan "User" dan "Password" Speedy, "Dial on Demand" dan "Use Peer DNS"

bisa dicentang jika ingin digunakan



Selesai, jika sudah ada tanda "R" di depan PPPoE Client yang tadi kita buat, berarti PPPoE sudah tersambung dan anda bisa cek IP Public di bagian IP - Addresses

The NEW LoadBalance!! More Powerfull -TESTED-

## :: Tested on MikroTik 3.25 & WORKS WELL TOO on 3.24 ::

Akhirnya setelah sekian lama, tidak membuat tutz menyumbangkan lagi tutz baru, sebenarnya masih ada 3-4



tutorial lagi, tapi bertahap satu-satu dulu, dan semoga tutorial ini banyak membantu

Seperti biasa, kutipan Akang berikut ini

Quote:

### **DILARANG COPY PASTE TANPA IZIN ATAU CREDIT KE FORUMMIKROTIK**

Akang banyak menjumpai blog-blog, yang mengambil Jimplak PLEK sama persis konfigurasi disini tanpa CREDIT!! Tolong Hormati kami yang meluangkan waktu sharing konfigurasi SECARA GRATIS tanpa dipungut biaya sepeserpun, berikanlah kami CREDIT jangan asal comot, di forum manapun termasuk kaskus juga sangat membenci orang yang melakukan COPAS mentah-mentah tanpa memberikan "credit"

Ok,cukup sekilas infonya. Apa latar belakang muncul tutorial baru ini? alasannya, Akang ingin meningkatkan performa dan lebih bertenaga, dan konsep kali ini berbeda dengan sebelumnya. Perbedaan yang mencolok bagi Akang, dan sangat2 maknyusss sekali...

1. Akses video atau audio streaming menjadi 4x lebih cepat
2. Akses browsing juga sama menjadi berlipat-lipat lebih cepat
3. Stabil

Notes :

Selama Akang menggunakan konfigurasi ini, hotspot bisa berjalan lancar [kembali menggunakan UserMan, thanks buat bro [ch4rli3](#) atas info berharganya], YM juga mulus tanpa putus-putus, mIRC jalan lancar dan mulus, semuanya pokoknya MULUS tanpa gangguan sedikitpun.

**JIKA.... jika anda mengalami gangguan silahkan dipahami dan di-TELAAH dahulu  
dimana yang salah jangan asal JEPLAK**



OK,let's go to the TKP!!

Konfigurasi 5 Speedy PPPoE dan 1 Ethernet [Lokal]

**Setting PPPoE Client**, mencomot [dari sini](#) : <http://www.forummikrotik.com/9474-post1.html>

Code:

```

/interface pppoe-client
add ac-name="" add-default-route=no allow=pap,chap,mschap1,mschap2 comment="" \
dial-on-demand=no disabled=no interface=Speedy-1 max-mru=1480 max-mtu=1480 \
mrru=disabled name="PPPoE-1" user="*****@telkom.net" password="***"
profile=default \
service-name="" use-peer-dns=no user="***"

add ac-name="" add-default-route=no allow=pap,chap,mschap1,mschap2 comment="" \
dial-on-demand=no disabled=no interface=Speedy-2 max-mru=1480 max-mtu=1480 \
mrru=disabled name="PPPoE-2" user="*****@telkom.net" password="***"
profile=default \
service-name="" use-peer-dns=no user="***"

add ac-name="" add-default-route=no allow=pap,chap,mschap1,mschap2 comment="" \
dial-on-demand=no disabled=no interface=Speedy-3 max-mru=1480 max-mtu=1480 \
mrru=disabled name="PPPoE-3" user="*****@telkom.net" password="***"
profile=default \
service-name="" use-peer-dns=no user="***"

add ac-name="" add-default-route=no allow=pap,chap,mschap1,mschap2 comment="" \
dial-on-demand=no disabled=no interface=Speedy-4 max-mru=1480 max-mtu=1480 \
mrru=disabled name="PPPoE-4" user="*****@telkom.net" password="***"
profile=default \
service-name="" use-peer-dns=no user="***"

add ac-name="" add-default-route=no allow=pap,chap,mschap1,mschap2 comment="" \
dial-on-demand=no disabled=no interface=Speedy-5 max-mru=1480 max-mtu=1480 \
mrru=disabled name="PPPoE-5" user="*****@telkom.net" password="***"
profile=default \
service-name="" use-peer-dns=no user="***"

```

## New Mangle LoadBalance!!

Code:

```

/ip firewall mangle
add action=mark-connection chain=input comment="\
"NEW Load Balance" connection-state=new \
disabled=no in-interface=Speedy-1 new-connection-mark=ADSL-1 \
passthrough=yes
add action=mark-connection chain=input comment="" connection-state=new \
disabled=no in-interface=Speedy-2 new-connection-mark=ADSL-2 \
passthrough=yes
add action=mark-connection chain=input comment="" connection-state=new \
disabled=no in-interface=Speedy-3 new-connection-mark=ADSL-3 \
passthrough=yes
add action=mark-connection chain=input comment="" connection-state=new \
disabled=no in-interface=Speedy-4 new-connection-mark=ADSL-4 \
passthrough=yes
add action=mark-connection chain=input comment="" connection-state=new \
disabled=no in-interface=Speedy-5 new-connection-mark=ADSL-5 \
passthrough=yes
add action=mark-routing chain=output comment="" connection-mark=ADSL-1 \
disabled=no new-routing-mark=jalur-1 passthrough=no
add action=mark-routing chain=output comment="" connection-mark=ADSL-2 \
disabled=no new-routing-mark=jalur-2 passthrough=no
add action=mark-routing chain=output comment="" connection-mark=ADSL-3 \
disabled=no new-routing-mark=jalur-3 passthrough=no

```

```

add action=mark-routing chain=output comment="" connection-mark=ADSL-4 \
    disabled=no new-routing-mark=jalur-4 passthrough=no
add action=mark-routing chain=output comment="" connection-mark=ADSL-5 \
    disabled=no new-routing-mark=jalur-5 passthrough=no
add action=mark-connection chain=prerouting comment="" disabled=no \
    dst-address-type=!local in-interface=Lokal new-connection-mark=\
        ADSL-1 passthrough=yes per-connection-classifier=\
            both-addresses-and-ports:5/0
add action=mark-connection chain=prerouting comment="" disabled=no \
    dst-address-type=!local in-interface=Lokal new-connection-mark=\
        ADSL-2 passthrough=yes per-connection-classifier=\
            both-addresses-and-ports:5/1
add action=mark-connection chain=prerouting comment="" disabled=no \
    dst-address-type=!local in-interface=Lokal new-connection-mark=\
        ADSL-3 passthrough=yes per-connection-classifier=\
            both-addresses-and-ports:5/2
add action=mark-connection chain=prerouting comment="" disabled=no \
    dst-address-type=!local in-interface=Lokal new-connection-mark=\
        ADSL-4 passthrough=yes per-connection-classifier=\
            both-addresses-and-ports:5/3
add action=mark-connection chain=prerouting comment="" disabled=no \
    dst-address-type=!local in-interface=Lokal new-connection-mark=\
        ADSL-5 passthrough=yes per-connection-classifier=\
            both-addresses-and-ports:5/4
add action=mark-routing chain=prerouting comment="" connection-mark=ADSL-1 \
    disabled=no in-interface=HotSpot new-routing-mark=jalur-1 passthrough=yes
add action=mark-routing chain=prerouting comment="" connection-mark=ADSL-2 \
    disabled=no in-interface=HotSpot new-routing-mark=jalur-2 passthrough=yes
add action=mark-routing chain=prerouting comment="" connection-mark=ADSL-3 \
    disabled=no in-interface=HotSpot new-routing-mark=jalur-3 passthrough=yes
add action=mark-routing chain=prerouting comment="" connection-mark=ADSL-4 \
    disabled=no in-interface=HotSpot new-routing-mark=jalur-4 passthrough=yes
add action=mark-routing chain=prerouting comment="" connection-mark=ADSL-5 \
    disabled=no in-interface=HotSpot new-routing-mark=jalur-5 passthrough=yes

```

## Konfigurasi NAT

-- Ada 2 versi, silahkan pilih, suka-suka --

Code:

### **Versi ke-1**

Code:

```

/ip firewall nat
add chain=srcnat action=masquerade out-interface=PPPoE-1 comment="" disabled=no
add chain=srcnat action=masquerade out-interface=PPPoE-2 comment="" disabled=no
add chain=srcnat action=masquerade out-interface=PPPoE-3 comment="" disabled=no
add chain=srcnat action=masquerade out-interface=PPPoE-4 comment="" disabled=no
add chain=srcnat action=masquerade out-interface=PPPoE-5 comment="" disabled=no

```

### **Versi ke-2**

Code:

```
/ip firewall nat
```

```
add chain=srcnat action=masquerade src-address="IP Lokal anda"
```

## Konfigurasi Route

Code:

```
/ip route
add disabled=no distance=1 dst-address=0.0.0.0/0 gateway=PPPoE-1 \
routing-mark=Jalur-1
add disabled=no distance=1 dst-address=0.0.0.0/0 gateway=PPPoE-2 \
routing-mark=Jalur-2
add disabled=no distance=1 dst-address=0.0.0.0/0 gateway=PPPoE-3 \
routing-mark=Jalur-3
add disabled=no distance=1 dst-address=0.0.0.0/0 gateway=PPPoE-4 \
routing-mark=Jalur-4
add disabled=no distance=1 dst-address=0.0.0.0/0 gateway=PPPoE-5 \
routing-mark=Jalur-5
add comment="" disabled=no distance=1 dst-address=0.0.0.0/0 gateway=PPPoE-2
add comment="" disabled=no distance=1 dst-address=0.0.0.0/0 gateway=PPPoE-4
add comment="" disabled=no distance=1 dst-address=0.0.0.0/0 gateway=PPPoE-3
add comment="" disabled=no distance=1 dst-address=0.0.0.0/0 gateway=PPPoE-1
add comment="" disabled=no distance=1 dst-address=0.0.0.0/0 gateway=PPPoE-5
add comment="" disabled=no distance=2 dst-address=0.0.0.0/0 gateway=PPPoE-4
add comment="" disabled=no distance=3 dst-address=0.0.0.0/0 gateway=PPPoE-2
```

::: Screen Crrotttt :::

The screenshot shows the WinBox v3.25 interface on an x86 (x86) host. The main window title is "Akang@ [([Ei-Ji].NET) - WinBox v3.25 on x86 (x86)]". On the left, there's a sidebar with various network configuration tabs: Interfaces, Wireless, Bridge, Mesh, PPP, IP, IPv6, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, ISDN Channels, Make Supout.rif, Manual, and Exit. The "Firewall" tab is selected. Below it, several sub-tabs are visible: Filter Rules, NAT, Mangle, Service Ports, Connections, Address Lists, and Layer7 Protocols. Under the Filter Rules tab, there are two sections: "NEW Load Balance" and "Load Balance". The "NEW Load Balance" section contains 15 rules, each with a "mar..." icon and "input" or "prerouting" action. The last rule (ID 15) is highlighted with a blue selection bar. The "Load Balance" section contains 5 rules, all with "prerouting" action. The columns in the table include: #, Action, Chain, Src. Address, Dst. Address, Proto..., Src. Port, Dst. Port, In. Inter..., Out. Int..., Bytes, and Packets.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	mar...	input								2298.7 KB	17 219
1	mar...	input								1324.3 KB	7 391
2	mar...	input								1424.4 KB	8 411
3	mar...	input								1385.7 KB	8 435
4	mar...	output								1207.8 KB	17 867
5	mar...	output								578.6 KB	7 976
6	mar...	output								706.8 KB	8 723
7	mar...	output								2202.1 KB	10 579
8	mar...	prerouting								275.1 MiB	1 645 383
9	mar...	prerouting								338.4 MiB	2 111 837
10	mar...	prerouting								235.7 MiB	1 834 340
11	mar...	prerouting								318.2 MiB	2 078 552
12	mar...	prerouting								273.1 MiB	1 597 148
13	mar...	prerouting								336.9 MiB	2 075 649
14	mar...	prerouting								234.2 MiB	1 797 487
15	mar...	prerouting								316.8 MiB	2 042 342
16 X	mar...	prerouting								0 B	0
17 X	mar...	prerouting								0 B	0
18 X	mar...	prerouting								0 B	0
19 X	mar...	prerouting								0 B	0
20 X	mar...	prerouting								0 B	0

Penyebaran bytes dan paket merata, diangka yang tidak selisih jauh, hanya saja di Akang ada 4 line, jadi default rote di 4, sehingga di mark=output jadi besar sendiri 😊



Gambar tes download dan streaming, menyusul lagi, blm ke warnet buat di ambilin screencrotnya

# Membuat OSPF secara sederhana

Wednesday, 17 February 2010 20:29

OSPF (Open Shortest Path First) adalah metode routing yang membuat router menjadi smart dengan mencari jalan sendiri menuju router atau ip address tertentu di lokasi lain secara cepat dengan mengambil jalur terdekat yang available.

Syarat untuk menggunakan OSPF adalah semua router mikrotik terhubung langsung baik melalui wireless maupun kabel. Tidak boleh ada radio wireless lain yang bukan mikrotik yang melakukan routing diantara kedua mikrotik yang mau dihubungkan melalui OSPF.

Perintah mudah untuk memulai OSPF adalah dengan perintah :

```
routing ospf network add network=192.168.0.0/24 area=backbone
```

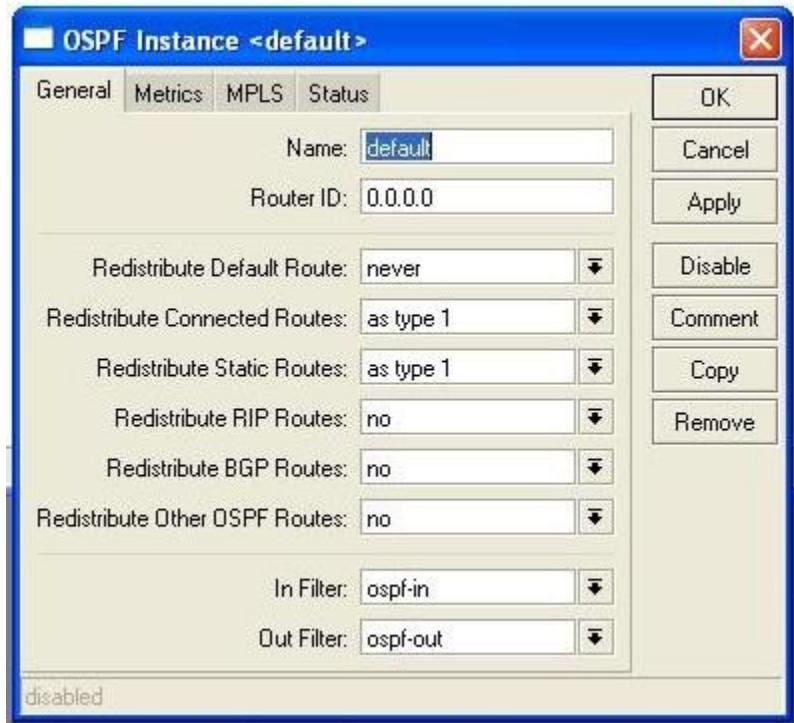
IP Address 192.168.0.0/24 boleh diganti dengan ip yang kita pakai didalam network yang kita hubungkan tersebut. Maka setelah kita memberikan perintah tersebut di TERMINAL mikrotik, maka kita akan mendapatkan kondisi dimana semua interface akan terdaftar dalam mikrotik routing seperti gambar dibawah :

OSPF											
Interfaces Instances Networks Areas Area Ranges Virtual Links Neighbors NBMA Neighbors Sham Links LSA Routes ...											
<input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="✓"/> <input type="button" value="✗"/> <input type="button" value="T"/> <input type="text" value="Find"/>											
Interface	Cost	Priority	Authentic...	Authenticatio...	Network Type	Instance	Area	Neig...	State		
D  Manyar	10	1 none	*****		broadcast	default	backbone	1	designated ro...		
D  Menanggal	10	1 none	*****		broadcast	default	backbone	1	backup		
D  ether1	10	1 none	*****		broadcast	default	backbone	0	designated ro...		

3 items out of 0

Interface Manyar dan Menanggal adalah interface wireless, sedangkan ether1 adalah interface ethernet.

Kemudian kita perlu melakukan perubahan pada tab INSTANCES menjadi seperti berikut :



Setelah itu OSPF akan segera beroperasi secara sederhana dan kita akan sudah bisa melihat OSPF bertukar routing secara otomatis jika salah satu router RING-nya terputus.

Jika kita tidak memiliki RING, maka OSPF sangat berguna bagi kita yang memiliki banyak routing di dalam network. Dengan OSPF kita tidak perlu membuat static route di semua router, namun OSPF akan melakukannya untuk kita secara otomatis.

Jika OSPF tidak berjalan sempurna, coba hapus semua static route yang sudah ada / dibuat sendiri oleh kita. Dalam kondisi normal, akan muncul routing semacam berikut ini :

**Route List**

Routes		Nexthops	Rules	VRF				
						<input type="text" value="Find"/>	<input type="button" value="all"/>	
	Dst. Address	Gateway			Distance	Routing Mark	Pref. Source	
XS	► 0.0.0.0/0	119.2.40.242			2			
XS	► 0.0.0.0/0	119.2.40.169			1	IIX		
DAo	► 0.0.0.0/0	119.2.40.169 reachable Sidoarjo			110			
DAo	► 10.88.88.252/30	119.2.40.169 reachable Sidoarjo			110			
DAo	► 10.99.99.0/29	119.2.40.169 reachable Sidoarjo			110			
DAo	► 119.2.40.20/30	119.2.40.169 reachable Sidoarjo			110			
::: Ring Manyar								
XS	► 119.2.40.132/30	119.2.40.242			1			
DAo	► 119.2.40.132/30	119.2.40.242 reachable ether1			110			
DAo	► 119.2.40.136/30	119.2.40.169 reachable Sidoarjo			110			
DAo	► 119.2.40.140/30	119.2.40.169 reachable Sidoarjo			110			
DAo	► 119.2.40.144/30	119.2.40.169 reachable Sidoarjo			110			
DAC	► 119.2.40.168/30	Sidoarjo reachable			0		119.2.40.170	
DAo	► 119.2.40.172/30	119.2.40.169 reachable Sidoarjo			110			
DAC	► 119.2.40.176/30	STTAL reachable			0		119.2.40.177	
DAo	► 119.2.40.208/30	119.2.40.169 reachable Sidoarjo			110			
DAo	► 119.2.40.212/30	119.2.40.242 reachable ether1, 119.2.40.169 reachable Sid...			110			
DAC	► 119.2.40.240/30	ether1 reachable			0		119.2.40.241	
DAo	► 119.2.41.56/29	119.2.40.169 reachable Sidoarjo			110			
DAo	► 119.2.41.160/29	119.2.40.169 reachable Sidoarjo			110			

66 items (1 selected)

Tanda DAO adalah artinya routing yang didapatkan melalui OSPF. Karena OSPF sudah membuat routing default 0.0.0.0/0 maka routing yang lama silakan untuk dihapus atau didisable saja agar tidak mengganggu.

Selamat mencoba (C) 2010 - Ayom Rahwana

## **NETINSTALL RB750 & RB411R Melalui PXE**

apabila ada masalah saat Upgrade RB750 dan RB411R yang menyebabkan RB tidak dapat di detek lewat winbox maka jalan satu-satunya Install lewat NETINSTALL.

RB750 dan RB411R tidak memiliki kabel Serial jadi untuk melakukan NETINSTALL memerlukan Trik sebagai berikut.

Persiapan :

1. Download Software NETINSTALL <http://www.mikrotik.com/download/netinstall-4.4.zip> Perhatikan Gunakan Versi 4.4 keatas, Versi 3 tidak dapat digunakan untuk RB750 dan RB411R
2. Download Paket terbaru untuk MISPBE <http://www.mikrotik.co.id/getfile.php...mipsbe-4.4.npk>

Installasi :

1. Jalankan Software NETINSTALL

2. Klik "Net Booting"

3. Centang "Boot Server Enabled"

4. Client IP Address diisi dengan IP address 1 subnet dgn PC yang kita gunakan misal PC 192.168.1.1/24 maka isi 192.168.1.2 atau s/d 192.168.1.254.

5. Pastikan Software NETINSTALL sudah dijalankan, Colok Kabel yang terkoneksi dgn PC ke Port 1 di RB750, kalo RB411R cuma 1 port.

6. Dalam Keadaan Mati colok tombol reset dengan Tusuk gigi atau Paper clip, kemudian ditahan.

7. Colok Power sambil tombol tetap di tekan.

8. Tunggu sekitar 1 menit.

9. Lepas tombol Reset setelah RB750 muncul di netinstall biasanya namanya "nstrem"

10. Klik Install deh, tungguin sampe kelar trus setelah reboot, mikrotik siap digunakan.

- Selamat mencoba -

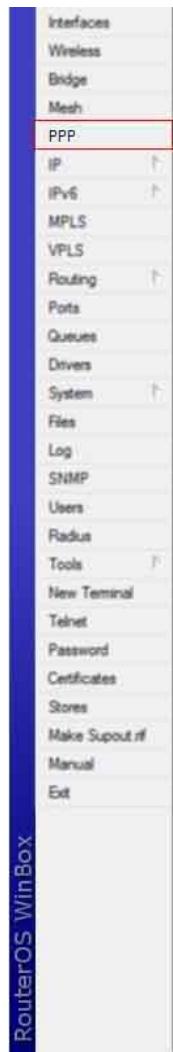
## Langkah2 membuat koneksi pppoe server berbasis winbox

Assalamualaikum Wr.wb

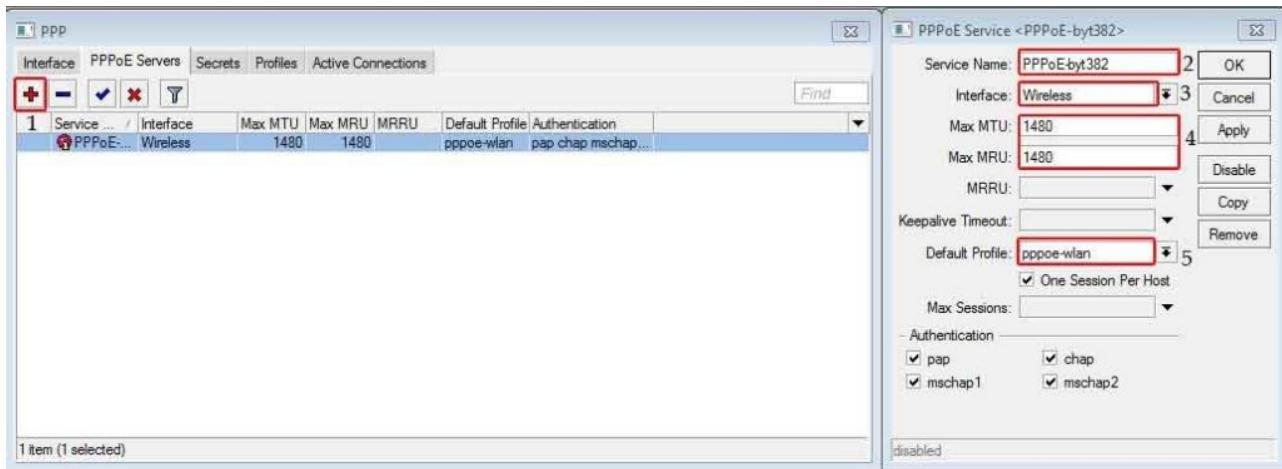
Sekian lama gabung di forum tercinta ini gw baru kali ini berniat memberikan sedikit ilmu yg gw baru pelajari. mungkin bagi sebagian yg udah paham dan mengerti ga terlalu penting tutorial ini tapi dengan semangat 45 saya di sini ingin memberikan tutorial tentang cara membuat pppoe server berbasis winbox yg tujuannya mengamankan jaringan wireless dari mac clone. saya paham dan mengerti tak ada yg sempurna dalam dunia maya. semua masih mungkin terjadi. di harapkan dengan ada tutorial ini bisa mengurangi dan mencegah orang lain yg bukan hak nya memakai jaringan kita. kepanjangan nih pidato nya. langsung aja y



cekidot



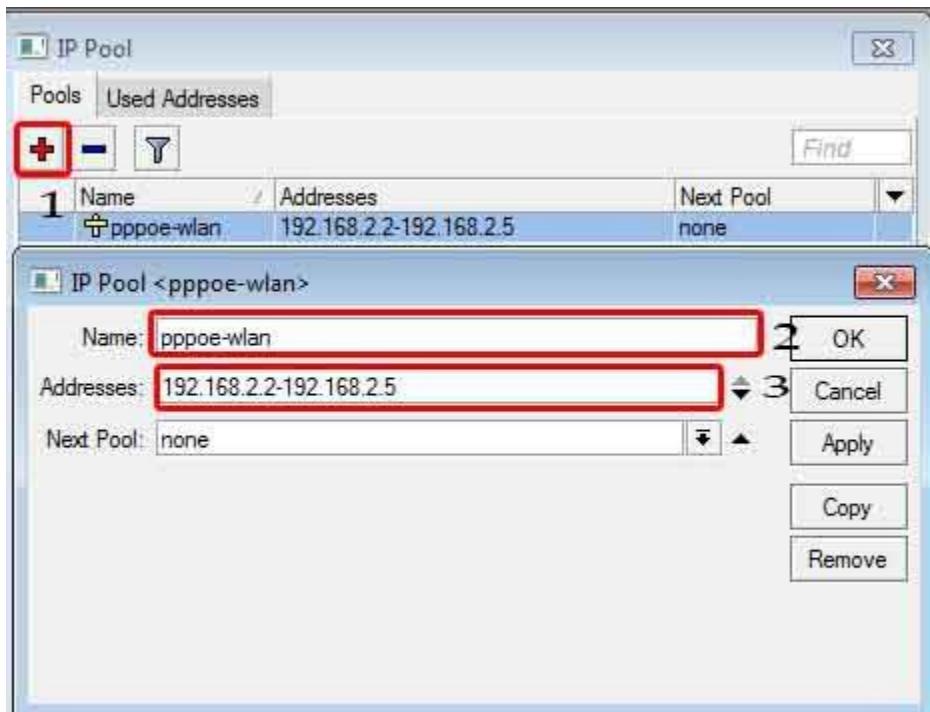
**1. Pasti dah ga asing sama tampilan ini kan. awali dengan memilih option PPP**



Akan tampil beberapa tab. di sini saya memilih tab PPPoe Server untuk langkah pertama.

1. Klik + akan muncul pop up yg ada beberapa tab, di sini saya memilih tab PPPoe server.
2. Service Name - Bebas.
3. Interface - Karena saya sedang membicarakan wireless connection maka di situ saya pilih wireless
- 4 default ( Jangan di rubah2 - Kalau udah paham benar fungsinya ga masalah 😊 )
5. Default profile - pppoe wlan ( ini adalah ip pool yg di mana terdapat range ip yg ingin di masukkan ke dalam pppoe server. )

## Cara membuat ip pool ada di sini

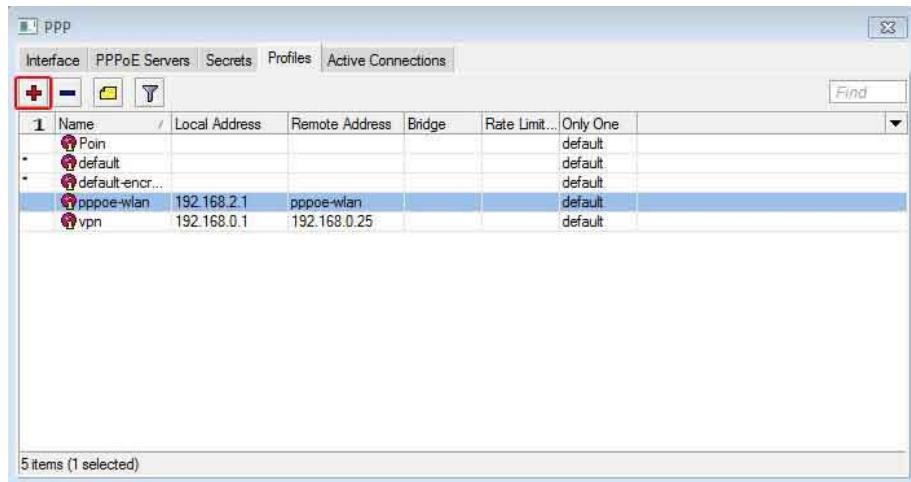


1. Klik + akan muncul pop up dan akan ada 2 tab di gambar saya memilih pool
2. Name - pppoewlan ini yg saya maksud tadi ( bebas )
3. Address - Range ip yg akan di buat untuk pppoe server. di gambar saya membuat range 192.168.2.2 - 192.168.2.5

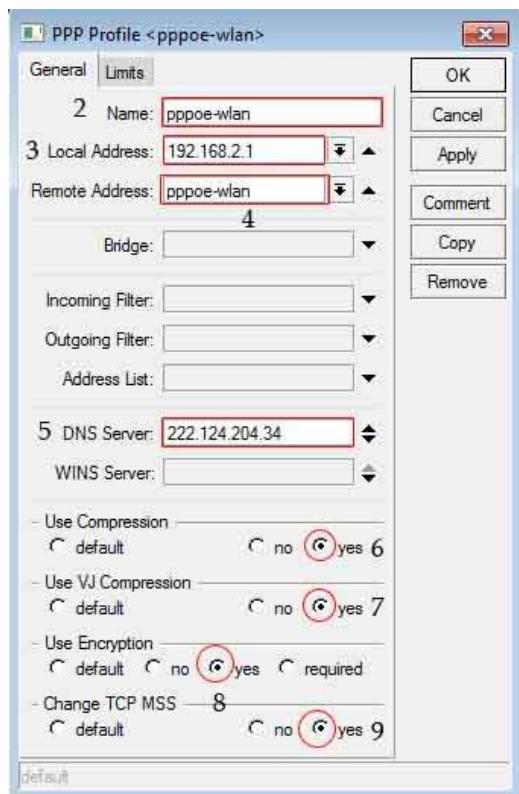
Apply.  
Ok

## 2. Membuat profile dari PPPoE server

Screenshootnya



1. klik tanda + akan muncul pop up seperti ini

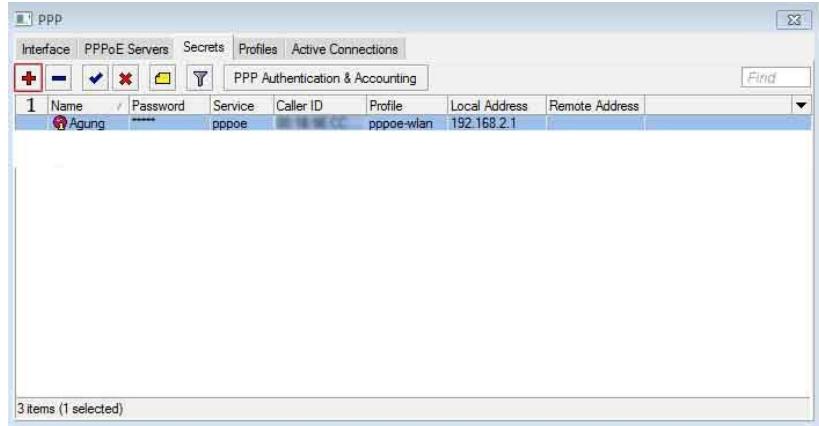


akan ada beberapa tab. di gambar saya memilih general. berikut penjelasanya

2. Name - pppoe-wlan ( bebas )

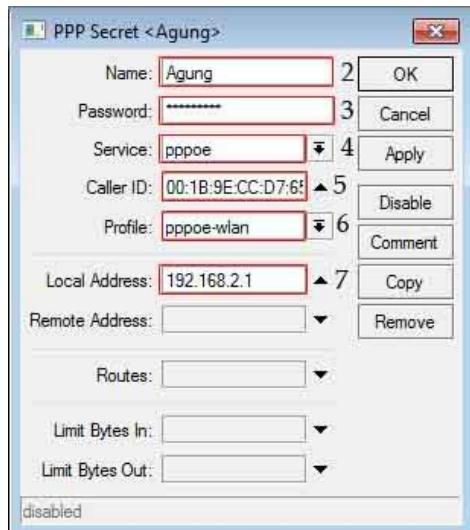
3. Local address - 192.168.2.1 ( sesuaikan dengan jaringan masing )
  4. Remote address - pilih pppoe-wlan sesuai yg sudah kita buat tadi.
  5. DNS server - DNS ISP/Provider masing2
- 6,7,8,9 saya memilih option ini namun fungsi nya saya belum tahu pasti. 🤪  
 Apply  
 ok

### 3. Membuat account client



seperti sebelumnya

1. Klik + Akan muncul pop up seperti ini



2. Name - nama client ( bebas )
3. password - password untuk client ( bebas )
4. Service - pppoe ( karena kita sedang membicarakan pppoe )
5. Callerid - macaddress client yg tercapture di wireless table masukan di sini
6. Profile - pppoe-wlan
7. local address- ip interface wireless

Apply - ok

Sampai di sini pembuatan pppoe server selesai. Sekarang tinggal dial pppoe server ini di Operating system client. Pastikan client sudah terhubung ke AP.

di gambar ini saya memakai windows XP proffesional SP3

## 1. Control panel

Pilih network connection.



## kemudian create new connection



2.

akan muncul pop up seperti ini



dan berikutnya buat nama isp ( bebas )



next.

berikutnya akan ada pilihan



pilih connect to the internet - Next



pilih option ke 2 - set up connection mannualy - next

akan muncul tampilan berikutnya



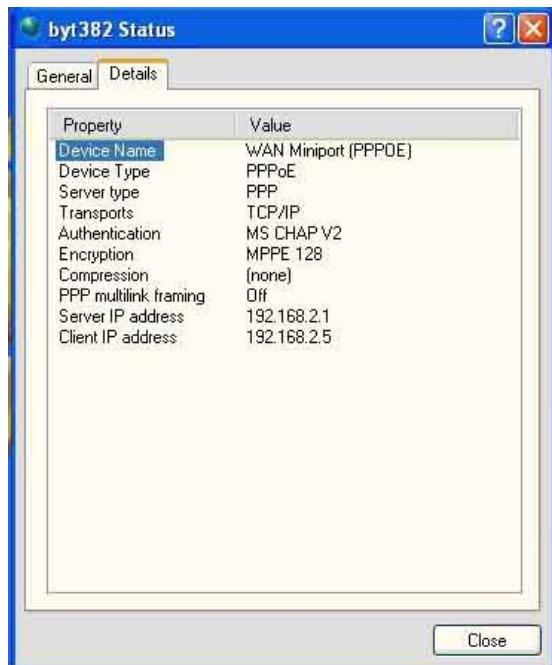
pilih connection using broadband - next

akan muncul tampilan berikutnya



isi sesuai dengan yg sudah di buat di pppoe profile tadi. - next

dan Selesai sampai di sini. coba dial dari komputer client jika sukses akan ada tampilan seperti ini



Selesai.

Berikutnya agar mac address client yg sudah masuk ke wireless table di amankan terlebih dahulu caranya seperti berikut

1. buat security profile

Name : bebas tapi Sopan 🍷

2. Masih di waktu dan jam yg sama klik tab Radius

centang mac authenticathion

Apply

ok

3. Client yg terkoneksi ke AP akan muncul di bagian registration karena saat capture ga ada yg online jadi di sini kosong 🍷 berikut penampakannya.

Wireless Tables

Interfaces Nstreme Dual Access List **Registration** Connect List Security Profiles

Find

Radio Name MAC Address Interface Uptime AP W... Last Activit... Signal Strengt... Tx/Rx Rate

0 items

nah kalau di situ sudah ada client yg terkoneksi. add client tersebut ke connect list dan access list. coba liat gambar berikut ini.

Wireless Tables

Interfaces Nstreme Dual **Access List** Registration Connect List Security Profiles

Find

#	MAC Address	Interface	Signal Str...	Authentication	Forwarding
0	00:0C:29:0B:00:00	Wireless	-120..120	yes	yes
1	00:0C:29:0B:00:01	Wireless	-120..120	yes	yes

2 items

Wireless Tables

#	Interface	MAC Address	Connect	Area Prefix	Signal Str...	Security ...
0	Wireless	00:1B:4E:00:0C:95	yes		-120..120	secwifi
1	Wireless	00:0C:42:45:23:87	yes		-120..120	secwifi

2 items

Selesai.

Mudah2 an berguna buat yg membutuhkan. maaf kalau kata2 nya ada yg membingungkan. kalau ada



kesalahan gambar atau keterangan dari gambar mohon koreksi nya. Terima kasih.

#### Tested hardware Router :

OS Router 3.23 X86 Licensi

Asus P5GD1-VM

Vgen DDR1 1 Gb PC 3200

Intel 2.8 Ghz HT

Seagate 40 Gb Sata

PSU Acbel I Power 510

Realtek Fast ethernet

Dlink Fast Ethernet

Atheros Engenius 600 Mw

Omny Hyperlink 15 db

#### Tested Software PC remote :

Windows Seven Ultimate 64 Bit

ASUS P5Q-Deluxe

Corsair Dominator 4 Gb PC 8500

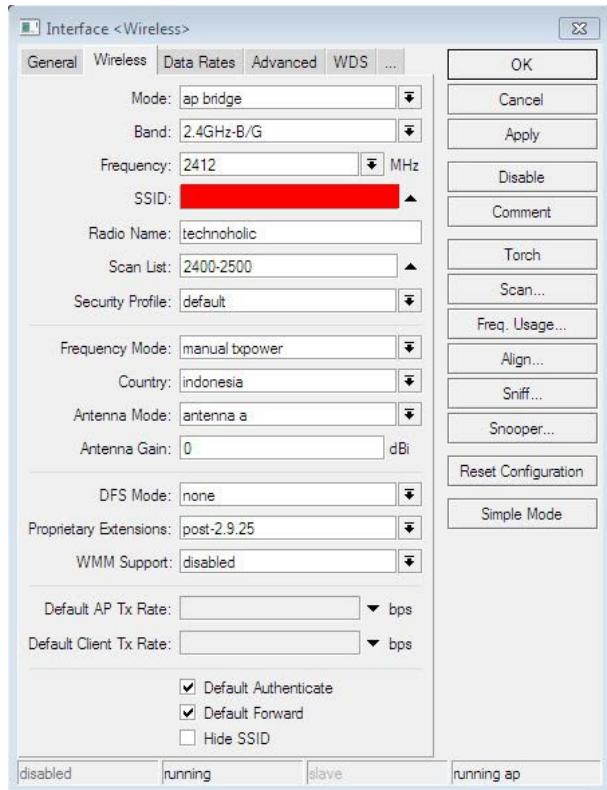
Intel Q9550 2.8 Ghz Quad Core

Seagate 320 Gb Sata

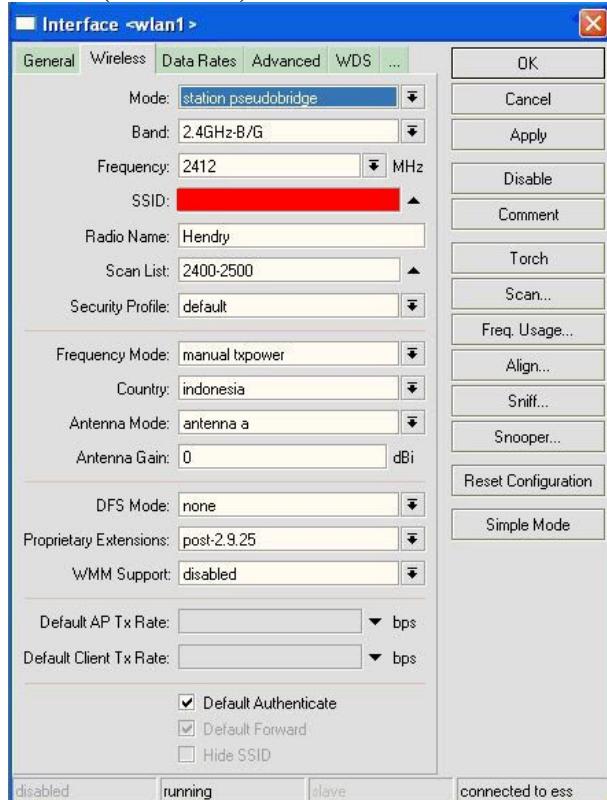
ATI Saphire 3850 256 mb 256 bit

PSU Corsair VX 450

## AP Backbone



## Client (RB411R)



# management bw mikrotik

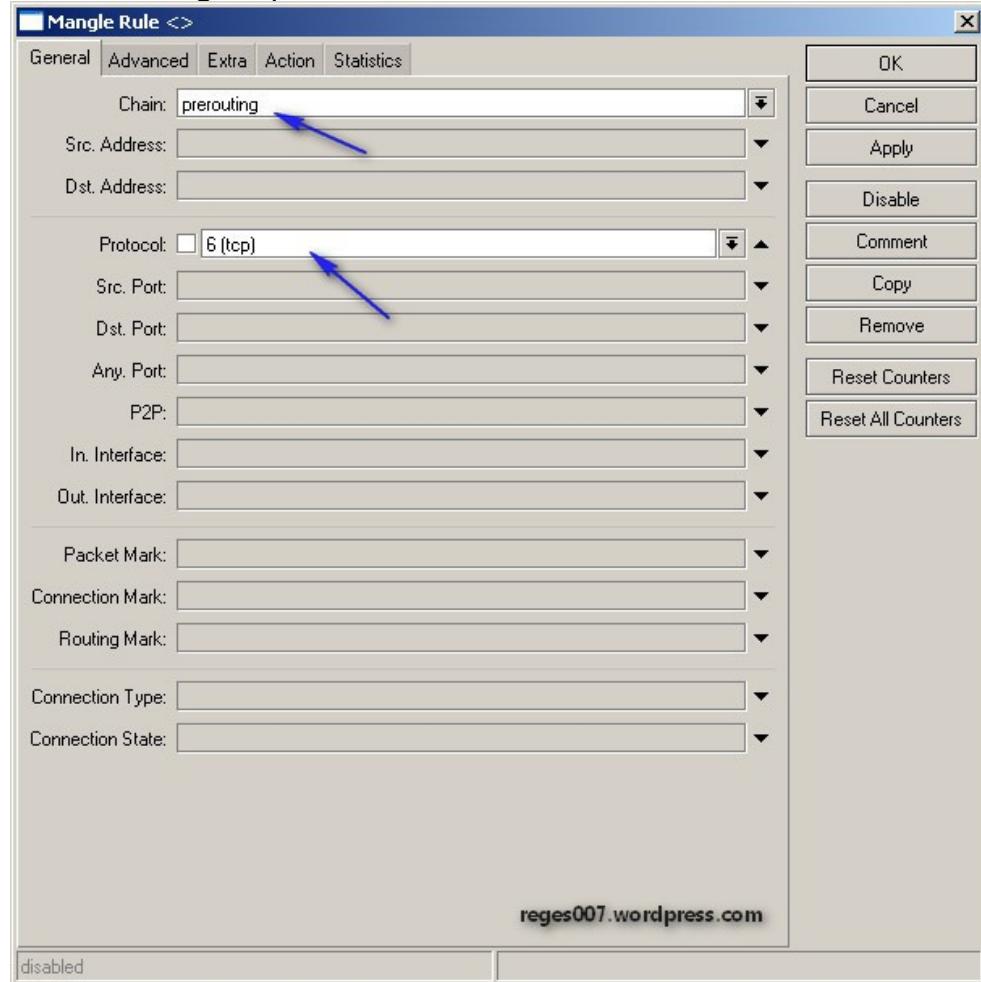
\*syarat dan ketentuan berlaku

## ***Limit pendownload dengan mangle con-bytes***

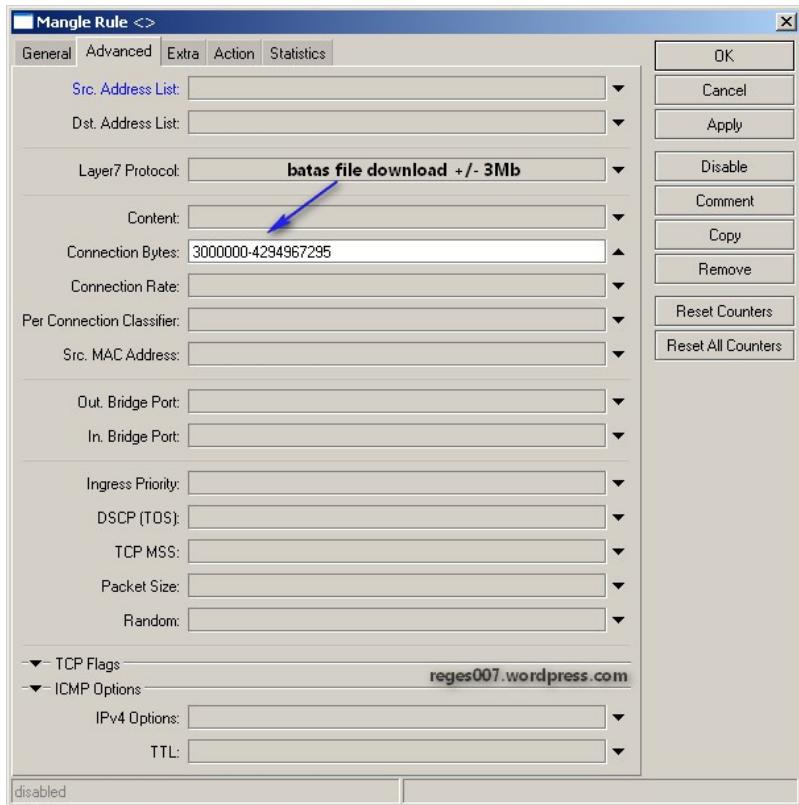
(rule berikut cocok dengan [BW Management sebuah GameNet dan Warnet](#) )

Sekarang kita akan mencoba mangle untuk men-Razia para perakus benwit di warnet kita biar mudah dan dapat di pahami saya akan mencoba membuat tutorial memakai winbox

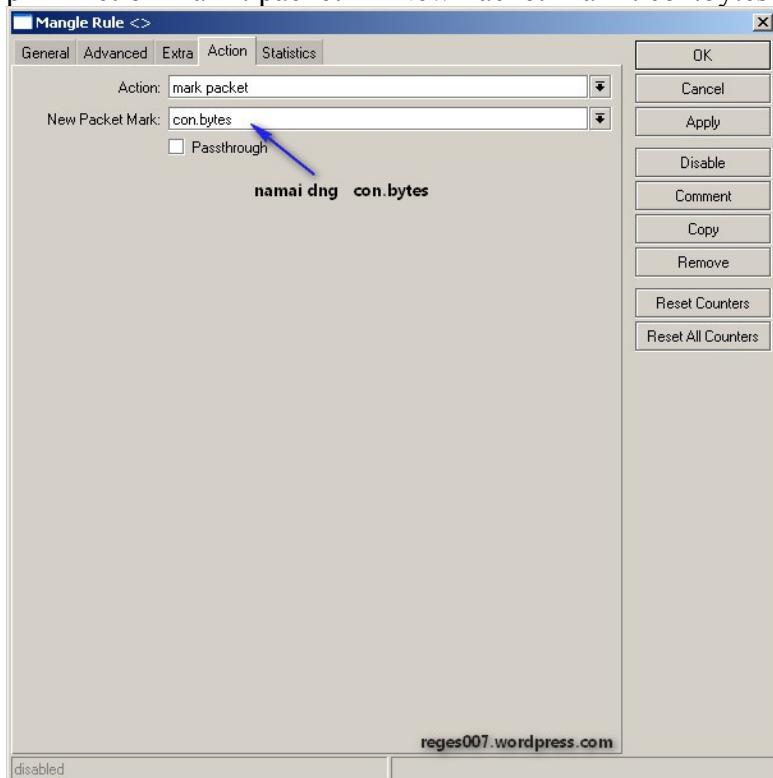
bikin rule mangle seperti ini :



ini saya ambil contoh untuk batas limit per 3Mbyte, setelah melampui itu maka akan di lemparkan ke simple queue



pilih Action mark : packet → New Packet Mark : con.bytes lalu tekan OK

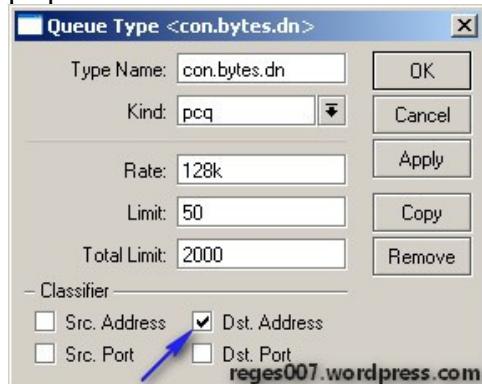


bikin queue type Kind : pcq

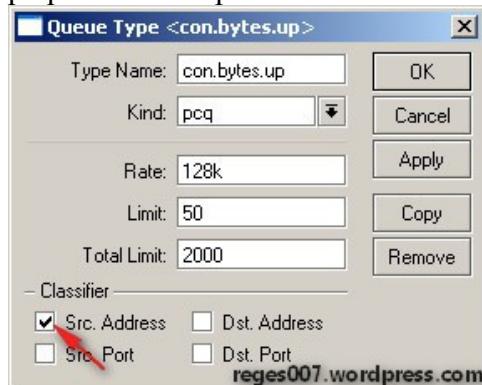
kita pake standard warnet dengan pcq-rate:128k untuk up/down saja biar simpel,bisa juga di kosongin 0 nanti

tinggal set max-limitnya sesuai network anda, misalnya kita kasih rata untuk alokasi download 384k/512k tinggal atur sesuai kondisi warnet anda.

pcq rate untuk download kita namai con.bytes.dn



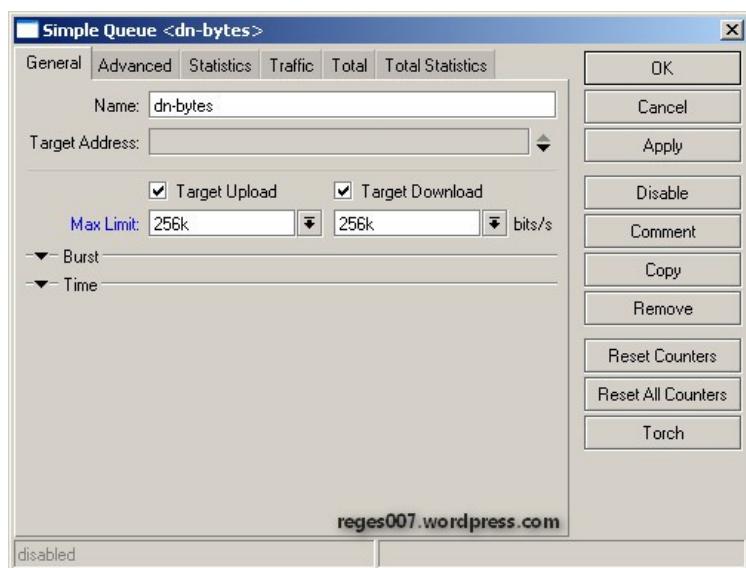
pcq rate untuk upload kita namai con.bytes.up



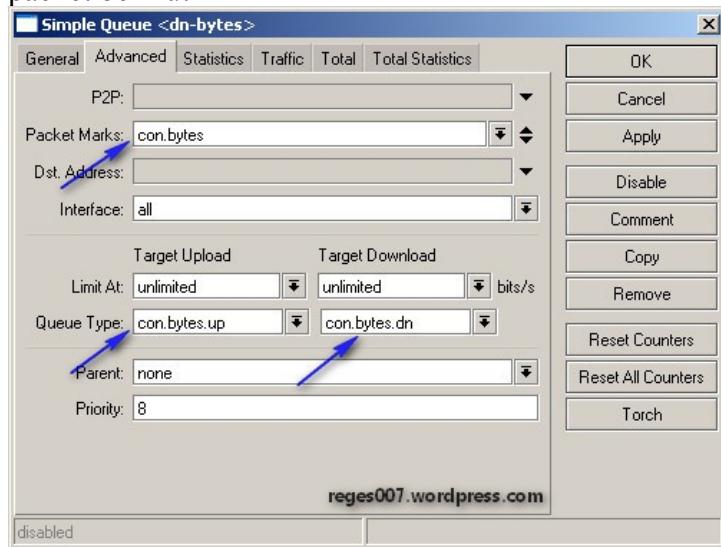
sekarang tinggal eksekusi lewat simple queue saja

disini juga bisa diatur sesuai kondisi warnet anda,jika sepi anda bisa set sampai 512k (jika warnet dengan bw 1M)

jika kondisi rame anda tinggal set 384k atau 128k jadi untuk alokasi browsing tetap aman

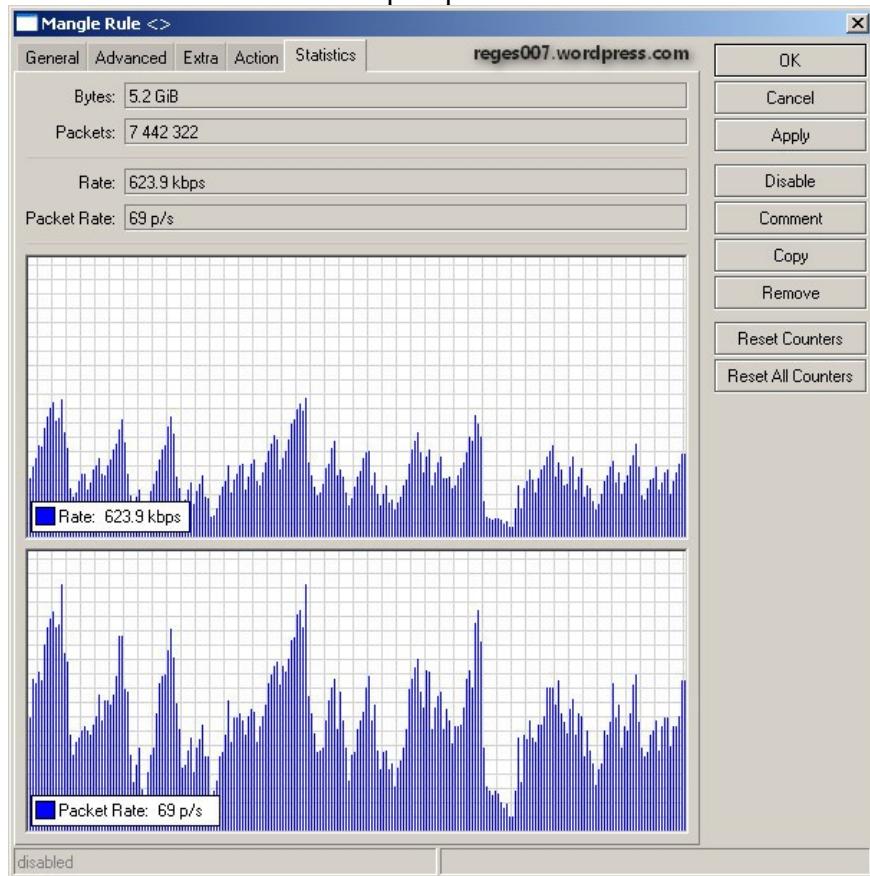


jika anda setting mangle dan queue-type dengan benar maka pada menu drop-down akan muncul packet-packet berikut

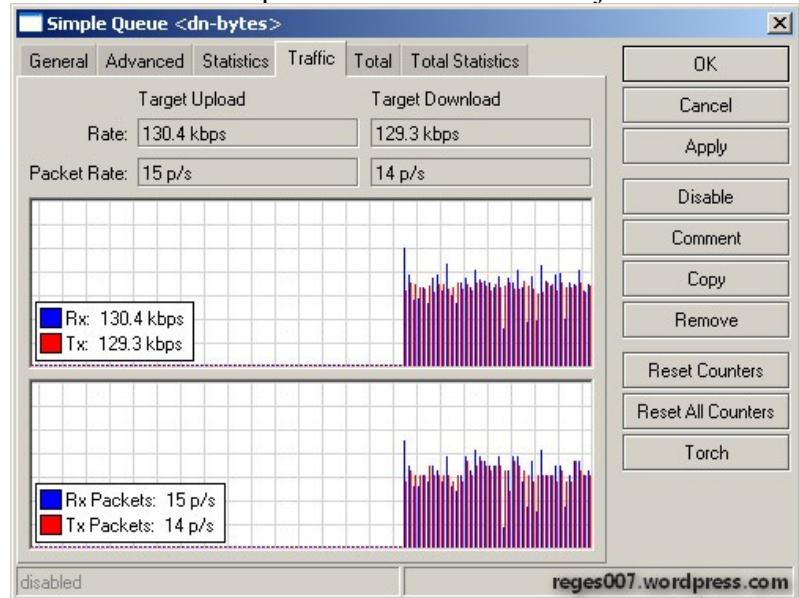


setelah itu silahkan dicoba untuk mendownload file lebih dari 3Mb, nanti traffic akan kebaca di mangle setelah melampui batas 3Mb

berikut traffic sebelum di simple-queue



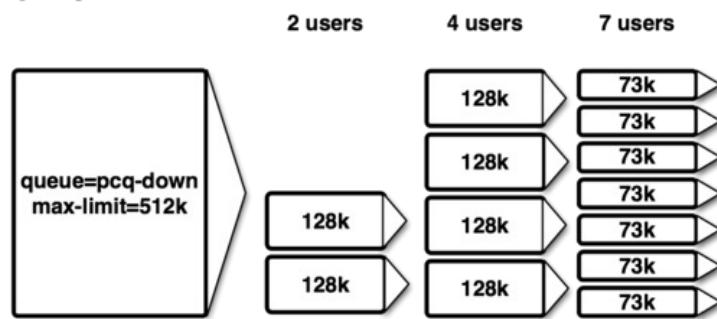
dan setelah masuk queue otomatis traffic menjadi 128k



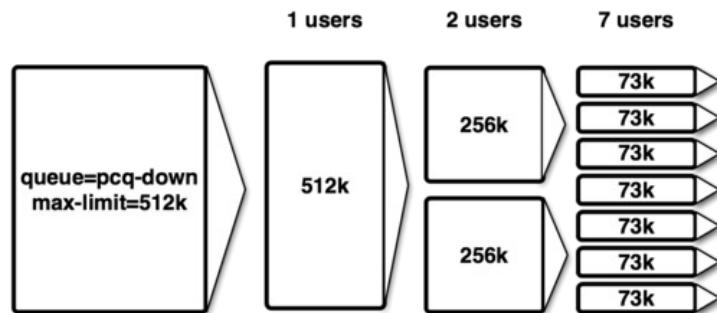
Catatan :

berikut tabel pembagian PCQ-Rate dengan Max-limit

**pcq-rate=128000**



**pcq-rate=0**



special thx for buyungsandy@kaskus

# management bw mikrotik \*syarat dan ketentuan berlaku

## **Limit pendownload dengan filter con-bytes**

Menanggapi report dari kaskuser tentang [Limit pendownload dengan mangle con-bytes](#) apabila klien menggunakan software download manager ternyata trafficnya bisa lolos dari PCQ . Maka dari itu saya buatkan rule baru untuk mengatasi problem itu.

Bikin dulu IP list bypass untuk klien kita contoh :

IP Klien 192.168.xx.xx

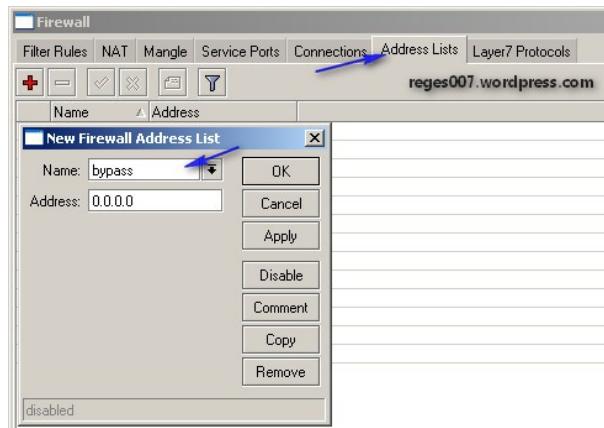
IP modem

IP Proxy external yang di pakai

IP website/homepage kita

Dll...

dengan maksud supaya tidak ikut terlimit, saya tandai dengan address-list **bypass**



lalu filter di firewall untuk deteksi connection-bytes



disini saya akan melimit traffic +/-2Mb dan mem-bypass IP klien kita supaya tidak masuk ke add-address-list

Firewall Rule <>

General Advanced Extra Action Statistics reegs007.wordpress.com

Src. Address List: [ ]

Dst. Address List: [ ] bypass

Layer7 Protocol: [ ]

Content: [ ]

Connection Bytes: 2000000-4294967295

Connection Rate: [ ]

Per Connection Classifier: [ ]

Src. MAC Address: [ ]

Out. Bridge Port: [ ]

In. Bridge Port: [ ]

Ingress Priority: [ ]

DSCP (TOS): [ ]

TCP MSS: [ ]

Packet Size: [ ]

Random: [ ]

-> TCP Flags

-> ICMP Options

IPv4 Options: [ ]

TTL: [ ]

saya masukan ke address list **Patroli**

Firewall Rule <>

General Advanced Extra Action Statistics

Action: add dst to address list

Address List: Patroli

Timeout: [ ]

reges007.wordpress.com

setelah IP masuk ke list **Patroli** sekarang kita menandai dengan packet-mark di mangle

**Mangle Rule <>**

General Advanced Extra Action Statistics reges007.wordpress.com

Chain:	forward
Src. Address:	
Dst. Address:	
Protocol:	
Src. Port:	
Dst. Port:	
Any. Port:	
P2P:	
In. Interface:	
Out. Interface:	
Packet Mark:	
Connection Mark:	
Routing Mark:	
Connection Type:	
Connection State:	

### Src.Address list pilih Patroli

**Mangle Rule <>**

General Advanced Extra Action Statistics reges007.wordpress.com

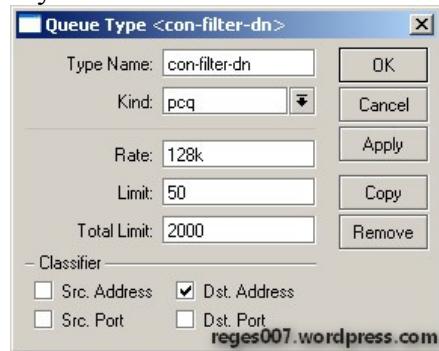
Src. Address List:	<input checked="" type="checkbox"/> Patroli
Dst. Address List:	
Layer7 Protocol:	
Content:	
Connection Bytes:	
Connection Rate:	
Per Connection Classifier:	
Src. MAC Address:	
Out. Bridge Port:	
In. Bridge Port:	
Ingress Priority:	
DSCP (TOS):	
TCP MSS:	
Packet Size:	
Random:	
-▼- TCP Flags	
-▼- ICMP Options	
IPv4 Options:	
TTL:	

saya tandai new-packet dengan nama **Razia**

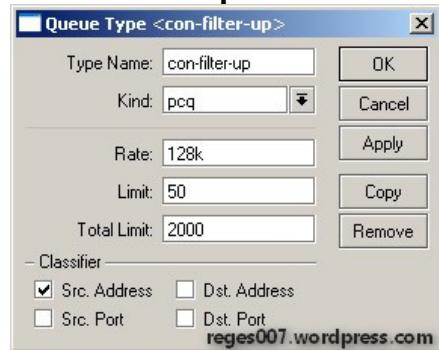


berlanjut pada queue-type untuk PCQ

saya namai **con-filter-dn**



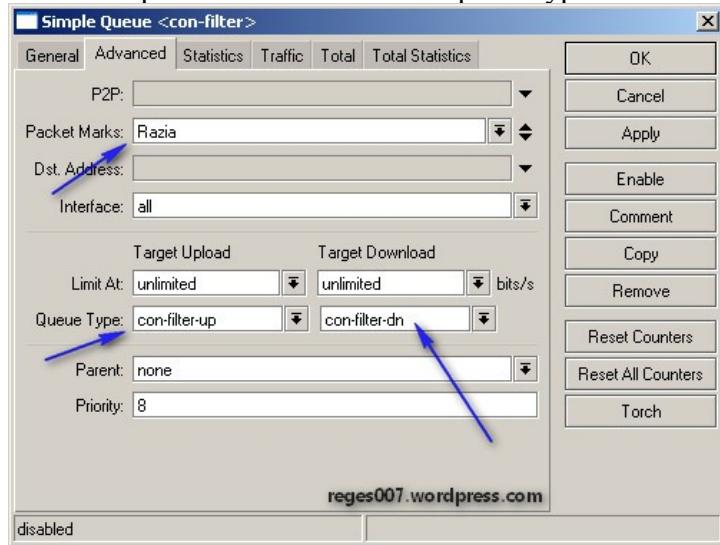
dan **con-filter-up**



terakhir bikin simple-queue



sesuaikan packet-mark **Razia** dan queue-type **con-filter-up / con-filter-dn**



rule diatas akan melimit **IP-ADDRESS** yg telah di marking oleh mangle (1 IP = 1 packet-mark) dan di PCQ classifier yg di tandai hanya dst.address dan src.address maka yang di proses untuk queue HANYA IP-ADDRES saja bukan per-Port connection seperti pada mangle con-bytes

Pertanyaannya mengapa memakai mangle con-bytes bisa lolos?

Jawabannya : karena mangle con-bytes itu menandai traffic per connection (src-port) yang dibuat oleh software download manager (pararel connection) jadi yang di tandai itu per-connection bukan per IP. Apabila software download manager telah membuat pararel connection 10 maka mangle menandai 10 packet connection setelah itu baru dikirim ke PCQ dan PCQ sekedar meng-classifier apa yang telah dikirimkan oleh mangle. apabila PCQ rate di setting 128k maka 10 packet dari mangle tersebut diberi jatah bw 128k. kenapa koq bisa sampai lolos bw nya,karena system software download manager itu mengacak koneksi untuk mendownload satu file seumpama di set 10 pararel maka dia akan membuat 10 koneksi dalam satu aksi, maka dari itu mangle hanya mengirim ke PCQ kalau masing-masing 10 koneksi itu sudah mencapai batas limit yang telah di setting connection-bytes, setelah semua (10) koneksi itu mencapai batas limit maka traffic akan menjadi 128k sesuai PCQ rate .

Nah biasanya software download manager itu mengacak koneksi (mengganti koneksi baru) supaya dia dapat port baru lagi,maka mangle otomatis bekerja dari awal lagi untuk mengirim ke PCQ setelah melampui batas connection-bytes , pasca pergantian itu otomatis traffic baru itu lolos dari queue makanya kesannya mangle con-bytes itu gk ngaruh/jebol oleh software download manager

ps:

mohon maaf apabila dalam penjelasan diatas ada kekurangannya dalam bahasa penyampaiannya karena saya ini hanyalah belajar dari otodidak yang saya temui di google maupun forum-forum.

# Netinstall Mikrotik RouterOS pada RouterBoard

Entah kenapa login di mikrotik tiba2 tidak bisa dipakai..ugh.. Bagaimana monitoringnya..? Terpaksa saya instal ulang saja router board-nya. Bagi yang mengalami hal serupa mungkin ada cara lain selain netinstall. Tinggalkan pesan dikomentar ya?

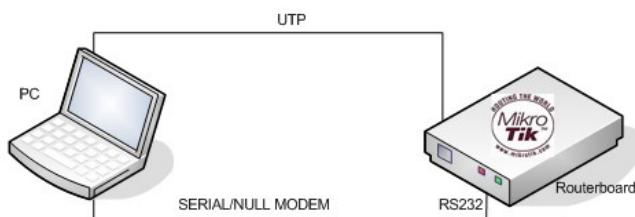
ok, kembali ke topik netinstall... bagi yg ingin mencoba silakan saja ikuti langkah-langkah berikut...

Perlu diketahui netinstall adalah program under windows yang digunakan untuk install atau upgradde Mikrotik RouterOS Operating System.

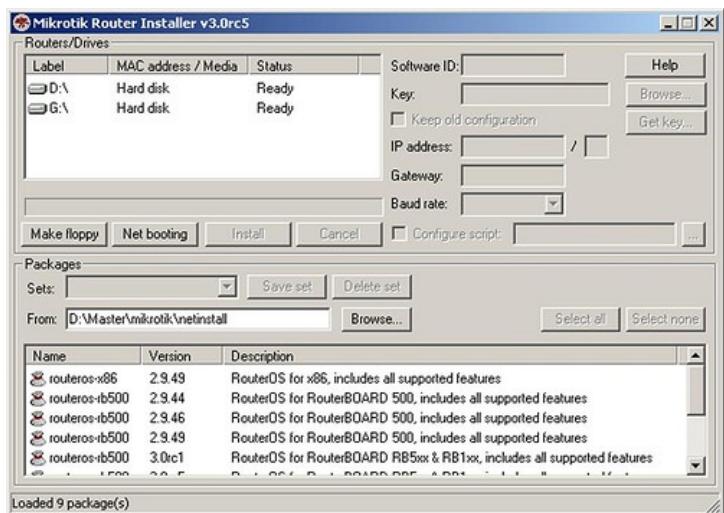
Untuk instalasi menggunakan Netinstall yang perlu di siapkan adalah :

1. PC dengan interface Ethernet dan Serial/COM
2. Kabel Null Modem.
3. Kabel UTP
4. Routerboard atau dedicated PC MIKROTIK

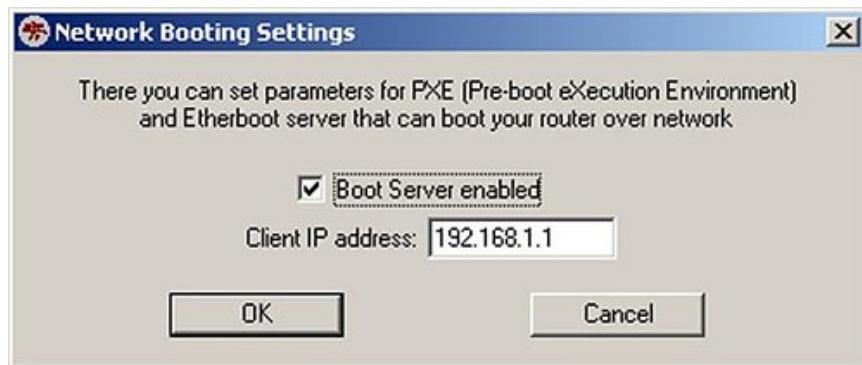
Software Neinstall, Package mikrotik yang akan di install yang bias di download di  
<http://www.mikrotik.com/download.html>



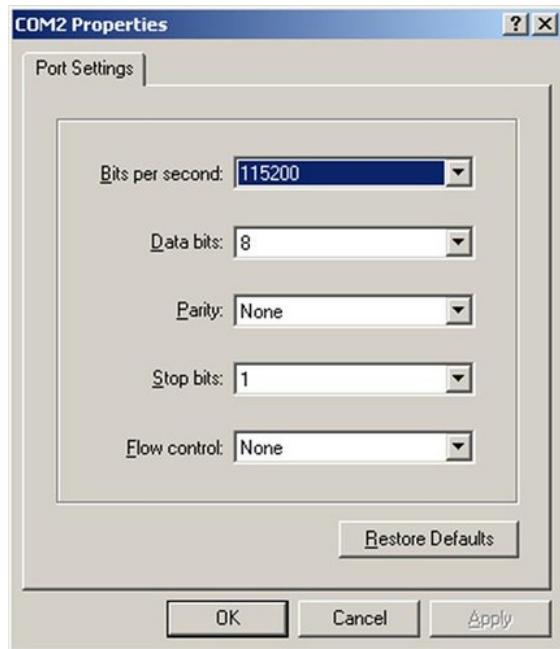
1. Konek Routerboard ke PC dengan menggunakan UTP sekaligus kabel null modem.
2. Persiapkan PC dan jalankan Netinstall.



Tekan Net booting kemudian isikan ip address routerboard yang akan di install.



1. Persiapkan Hyperteminal untuk koneksi via Serial
2. Buka Hyperteminal koneksi menggunakan COM1 atau COM2 Set Properties seperti di gambar.



Set routerboard supaya booting via Ethernet.

1. Tampilan dari hyperterminal.

RouterBoard 532A

CPU frequency: 399 MHz  
Memory size: 64 MB

Press any key within 2 seconds to enter setup..

2. Tekan sembarang tombol dalam waktu 2 detik untuk masuk ke bios routerboard

maka akan tertampil seperti dibawah.

RouterBOOT-2.9

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  
e – format nand  
g – upgrade firmware  
i – board info  
p – boot protocol  
t – do memory testing  
x – exit setup  
your choice: x – exit setup

3. Tekan o untuk , memilih sesi booting.

Select boot device:

e – boot over Ethernet  
\* n – boot from NAND, if fail then Ethernet  
c – boot from CompactFlash only  
1 – boot Ethernet once, then NAND  
2 – boot Ethernet once, then CompactFlash  
o – boot from NAND only  
b – boot chosen device  
your choice: e – boot over Ethernet

Tekan e untuk Booting via Ethernet

Kemudian tekan x untuk exit kemudian booting

1. Setelah Reboot maka akan tertampil seperti ini:

writing settings to flash... OK

RouterBOOT booter 2.9

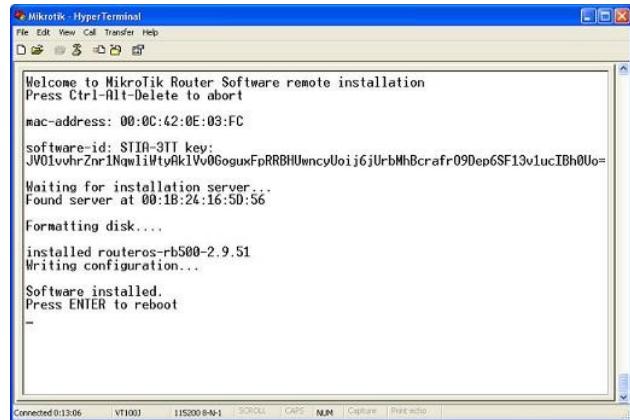
RouterBoard 532A

CPU frequency: 399 MHz

Memory size: 64 MB

Press any key within 2 seconds to enter setup..  
trying bootp protocol.... OK

Got IP address: 192.168.1.1  
resolved mac address 00:E0:29:58:34:5C  
transfer started ..... transfer ok, time=1.12s  
setting up elf i  
setting up elf i



Welcome to MikroTik Router Software remote installation  
Press Ctrl+Alt+Delete to abort

mac-address: 00:0C:42:0E:03:FC

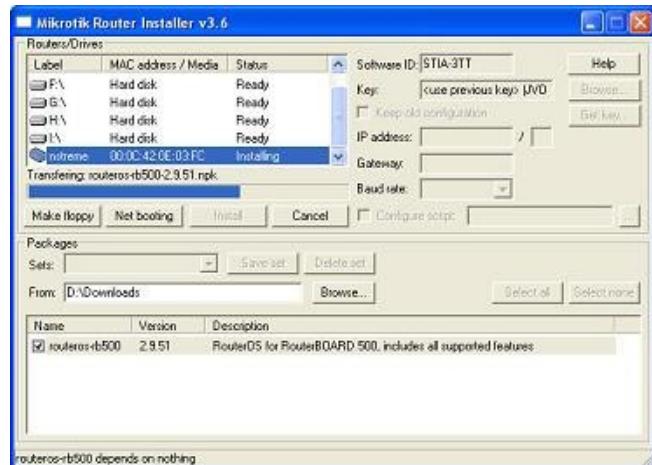
software-id: STIA-3TT key:  
JVO1vvhrZnrOHPk/4znX8nskLninMIFT..... dst

Waiting for installation server...

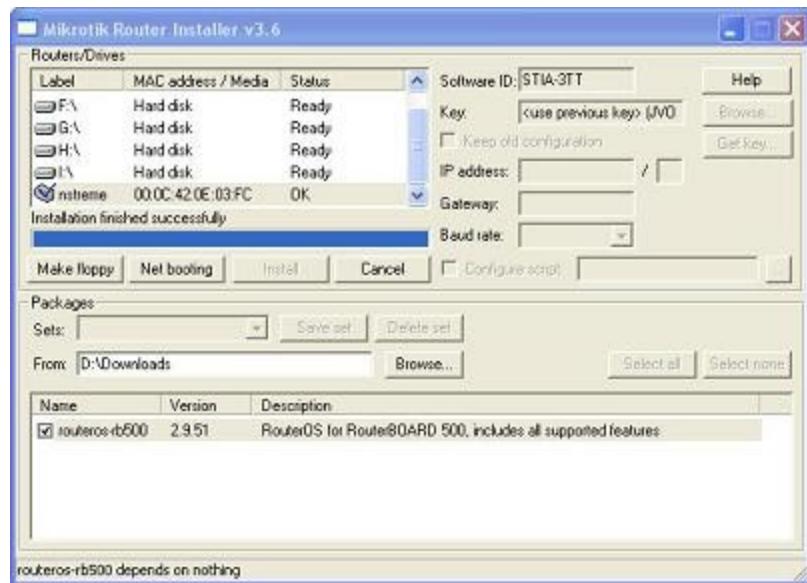
...dst

Persiapkan lagi PC dan Netinstall

Pilih routeros package yang akan di install kemudian tekan install



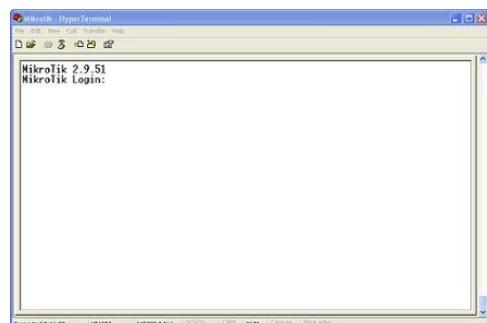
Tunggu sampai selesai...



kemudian reboot

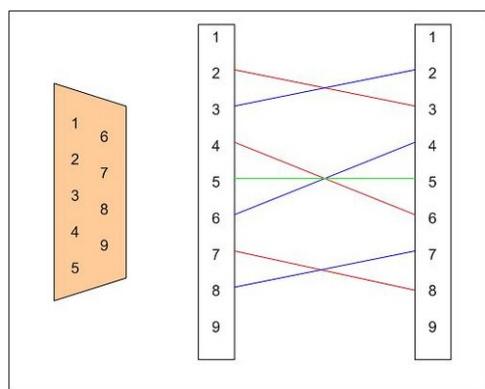
Di hyperterminal Ubah lagi sesi booting ke NAND kemudian reboot..tunggu hingga booting selesai

Routerboard telah selesai di install



Nb: Installasi tidak akan mengubah key dari mikrotik. (License tetap ada)

Konfigurasi null modem. pada port DB9 to DB9



## [SHARE] agar bandwidth hotspot agan nggak bisa di share kembali di client

Kesel rasanya apabila bandwidth hotspot kita di colong atau di share kembali di rumah client ....

Maaf newbie hanya ingin share sebuah trik bagaimana caranya agar client agan teruutama hotspot... tidak berbagi lagi (share internet di rumahnya)

yaitu dengan menset TTL ke pc client menjadi 1 😊 dengan jalan

Code:

```
/ip firewall mangle  
add action=change-ttl dst-address=192.168.1.0/24 \  
chain=forward new-ttl=set:1
```

sesuai dst address dengan client Hotspot agan 😊

saya akan coba jelaskan maksud dari mangel di atas 😊

sebuah paket yang lewat router mikrotik hanya dibuat valid untuk 1 hop berikutnya ke arah client, yang berarti hanya valid untuk 1 pc, karena begitu masuk ke PC tersebut TTL berkurang 1, sehingga menjadi 0.



semoga menjadi bermanfaat

## [SHARE] Hacking abal-abal: Bruteforce MT =))

Ane baru nyeting beberapa RB750 buat warnet, setelah internet koneksi and kwewe tree jalan senengnya minta

ampyuuunnn...

tapi malamnya....waktu mau cek settingan ulang via remote winbox, ane rada kaget...kok banyak user login

failure di terminal ane.... ane langsung kepikiran...ini pasti orang mau bruteforce MT ane

ane pun googling buat nyari skrip buat nahan itu bruteforce ...terus dapat deh scripts ini:

```
/ip firewall filter
add chain=input protocol=tcp dst-port=21 src-address-list=ftp_blacklist action=drop \
comment="drop ftp brute forcers"

add chain=output action=accept protocol=tcp content="530 Login incorrect" dst-limit=1/1m,9,dst-address/1m

add chain=output action=add-dst-to-address-list protocol=tcp content="530 Login incorrect" \
address-list=ftp_blacklist address-list-timeout=3h

add chain=input protocol=tcp dst-port=22 src-address-list=ssh_blacklist action=drop \
comment="drop ssh brute forcers" disabled=no

add chain=input protocol=tcp dst-port=22 connection-state=new \
src-address-list=ssh_stage3 action=add-src-to-address-list address-list=ssh_blacklist \
address-list-timeout=10d comment="" disabled=no

add chain=input protocol=tcp dst-port=22 connection-state=new \
src-address-list=ssh_stage2 action=add-src-to-address-list address-list=ssh_stage3 \
address-list-timeout=1m comment="" disabled=no

add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage1 \
action=add-src-to-address-list address-list=ssh_stage2 address-list-timeout=1m comment="" disabled=no

add chain=input protocol=tcp dst-port=22 connection-state=new action=add-src-to-address-list \
address-list=ssh_stage1 address-list-timeout=1m comment="" disabled=no

add chain=forward protocol=tcp dst-port=22 src-address-list=ssh_blacklist action=drop \
comment="drop ssh brute downstream" disabled=no
```



hasilnya lumayan maknyus....

## How To Crack Mikrotik Router Version 3.20 , 3.21, dan 3.22

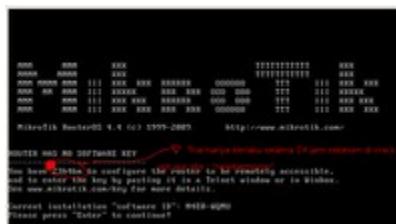
Cara Crack Mikrotik Router Versi 3.20 atau 3.21 atau 3.22, karena crack ini hanya bisa bekerja pada versi tersebut.

Persiapan :

1. Siapkan amunisi antara lain : Mikrotik V3.20/3.21/3.22...ISO , RouterOs-key.ISO, Id software-key Level3 sampai 6 (L3-L6). Jika anda installnya pada pc bukan di virtual silahkan burning image (ISO) tersebut terlebih dahulu.
2. Install mikrotiknya terlebih dahulu, jika anda memakai mikrotik v3.20 mendapati error saat instalasi,mungkin disebabkan karena tidak tersedianya paket yang diinstal. Untuk tutorial instalasi mikrotik versi 3.20 kunjungi catatan saya pada instalasi mikrotik.

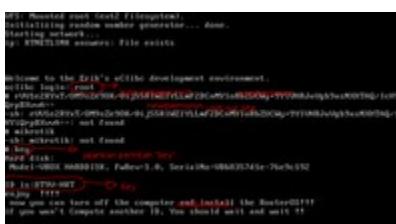
Caranya :

- Install mikrotiknya terlebih dahulu, jika instalasi berhasil akan keluar tampilan seperti berikut ini dengan status trial 24 jam.



Trial Sebelum di Crack

- Setelah instalasi berhasil selanjutnya restart dan boot RouterOS-key.ISO (crack mikrotiknya). Login sebagai "root" dan masukan perintah "key" dan tunggu beberapa menit kemudian sampai keluar Id software-key, jika Id software-key sudah keluar cek software key pada directory anda, id software-key ada pada salah satu file yang berada pada L3 sampai L6. Jika Id itu sudah cocok segeralah matikan runing RouterOs-key dengan menekan "Ctrl + C" lalu jalankan perintah "reboot" agar mikrotiknya restart dan menyimpan Id Software-key tadi.



RouterOS-key

- Cocokan Id Software-key nya, Id Software-key yang ditampilkan RouterOS-key diatas diluar level "L3-L6".

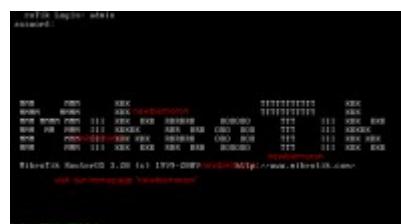


- Unmount RouterOs-key dan boot mikrotik pada mode normal
- Login mikrotik dengan winbox, masuk ke "System-->license-->import key(cari di directory mana anda menyimpannya)-->OK "



Winbox

- Selanjutnya, jika berhasil mikrotik akan meminta untuk "reboot", reboot mikrotik dan lihat apa yang terjadi



Setelah di crack

- Gambar diatas login mikrotik tidak dalam mode trial
- Selamat belajar dan mencoba
- Semoga Sukses

## Trap ip berdasarkan domain

Sebelumnya mohon maaf kepada rekan forum kalau cara yg ingin saya bagi di sini terbilang basi atau pernah ditemui dari situs lain. karena memang script ini saya lihat dari situs lain. tapi saya lupa nama situsnya, yg pasti dari situs luar sepertinya.

Ok kita mulai saja.

Tidak sedikit kita memerlukan ip adres yg mungkin kita perlukan untuk blocking, priority ataupun untuk burstable. berikut saya ingin memberikan contoh script yg digunakan untuk trap ip video dan facebook berdasarkan domain dan dari dns cache. untuk trap nya menggunakan scheduler. sehingga berkala.

Code:

```
/system scheduler
add comment="" disabled=yes interval=15m name=add-video on-event=":foreach i i\
n=[/ip dns cache find] do={\r\
\n      :local bNew \"true\";\r\
\n      :local cacheName [/ip dns cache all get \$i name] ;\r\
\n#      :put \$cacheName;\r\
\n\r\
\n      :if (([:find \$cacheName \"vimeo\"] != 0) || ([:find \$cacheName \"w\
rzuta\"] != 0) || ([:find \$cacheName \"edgesuite\"] != 0) || ([:find \$ca\
cheName \"googlevideo\"] != 0) || ([:find \$cacheName \"nba.com\"] != 0) || \
| ([:find \$cacheName \"dailymotion\"] != 0) || ([:find \$cacheName \"xtub\
e\"] != 0) || ([:find \$cacheName \"redtube\"] != 0) || ([:find \$cacheNam\
e \"youtube\"] != 0) || ([:find \$cacheName \"tube8\"] != 0) || ([:find \$\
cacheName \"pornhub\"] != 0) || ([:find \$cacheName \"youporn\"] != 0) || \
| ([:find \$cacheName \"youjizz\"] != 0) || ([:find \$cacheName \"metacafe\"]\
] != 0) || ([:find \$cacheName \"porn99\"] != 0)) do={\r\
\n\r\
\n      :local tmpAddress [/ip dns cache get \$i address] ;\r\
\n# \t:put \$tmpAddress;\r\
\n\r\
\n# if address list is empty do not check\r\
\n      :if ( [/ip firewall address-list find ] = \"\") do={\r\
\n          :log info (\"added entry: \$[/ip dns cache get \$i name] IP \
\$tmpAddress\");\r\
\n          /ip firewall address-list add address=\$tmpAddress list=yout\
ube comment=\$cacheName;\r\
\n          /ip firewall address-list add address=\$tmpAddress list=not-\\
youtube comment=\$cacheName;\r\
\n      } else={\r\
\n          :foreach j in=[/ip firewall address-list find ] do={\r\
\n              :if ( [/ip firewall address-list get \$j address] = \$tm\
pAddress ) do={\r\
\n                  :set bNew \"false\";\r\
\n                  }\r\
\n                  }\r\
\n                  :if ( \$bNew = \"true\" ) do={\r\
\n                      :log info (\"added entry: \$[/ip dns cache get \$i name]\ \
IP \$tmpAddress\");\r\
\n                      /ip firewall address-list add address=\$tmpAddress list=yout\
ube comment=\$cacheName;\r\
\n                      /ip firewall address-list add address=\$tmpAddress list=not-\\
youtube comment=\$cacheName;\r\
\n                  }\r\
\n              }\r\
\n          }\r\
\n      }
```

```

\n    }\r\
\n}\r\
\" policy=reboot,read,write,policy,test,password,sniff,sensitive \
start-date=jan/01/1970 start-time=00:00:00
add comment=facebook disabled=yes interval=15m name=add-facebook on-event=":foreal
ch i in=[/ip dns cache find] do={\r\
\n    :local bNew \"true\";\r\
\n    :local cacheName [/ip dns cache all get \$i name] ;\r\
\n#    :put \$cacheName;\r\
\n\r\
\n    :if (([:find \$cacheName \"facebook.com\"] != 0)) do={\r\
\n\r\
\n        :local tmpAddress [/ip dns cache get \$i address] ;\r\
\n#\t:put \$tmpAddress;\r\
\n\r\
\n# if address list is empty do not check\r\
\n        :if ([/ip firewall address-list find ] = \"\") do={\r\
\n            :log info ("added entry: \$[/ip dns cache get \$i name] IP \
\$tmpAddress");\r\
\n            /ip firewall address-list add address=\$tmpAddress list=face\
book comment=\$cacheName;\r\
\n        } else={\r\
\n            :foreach j in=[/ip firewall address-list find ] do={\r\
\n                :if ([/ip firewall address-list get \$j address] = \$tm\
pAddress ) do={\r\
\n                    :set bNew \"false\";\r\
\n                }\r\
\n            }\r\
\n            :if (\$bNew = \"true\") do={\r\
\n                :log info ("added entry: \$[/ip dns cache get \$i name]\
IP \$tmpAddress");\r\
\n                /ip firewall address-list add address=\$tmpAddress list=\
facebook comment=\$cacheName;\r\
\n            }\r\
\n        }\r\
\n    }\r\
\n}\r\
\" policy=reboot,read,write,policy,test,password,sniff,sensitive \
start-date=jan/01/1970 start-time=00:00:00

```

[untuk file script dapat diambil disini : http://manapegih.net/schedule.rsc](http://manapegih.net/schedule.rsc)

dari address list yg terbuat bila di gabung dengan conbyte dan priority saya rasa rekan semuanya dapat membayangkannya kan?

sedangkan selain itu ya dapat anda gunakan juga untuk yg lain. tergantung imajinasi anda.

dan bila ada yg mengatakan bila dibandingkan dengan L7 untuk trapnya bagai mana maka silahkan di coba sendiri

untuk facebook sebaiknya ditambahkan FBCDN juga

kredit hanya untuk forum.

[Share] "Anti Netcut" Work 100% (Gak ada [NETCUT] diantara kita)

He he he.. sesuai judul ane mau share2 lagi neh 😊



Netcut emang bikin pusing tapi mulai hari ini "say goodbye to users netcut".

Masalah netcut ini udah sering dibahas dithread2 sebelumnya, tapi kayaknya belum ada hasil yg memuaskan untuk pengguna (hotspot)

kalo masalah fungsi netcut yg memutuskan koneksi client kayaknya udah banyak yg solved ditrik2 sebelumnya..

**tapi masalah besarnya kalo tool netcut ini difungsikan buat nyari2 or scan mac/ip client, buat dipake gratis alias nyolong bandwidth oleh tangan usil yg tidak punya etika alias gak punya otak.**

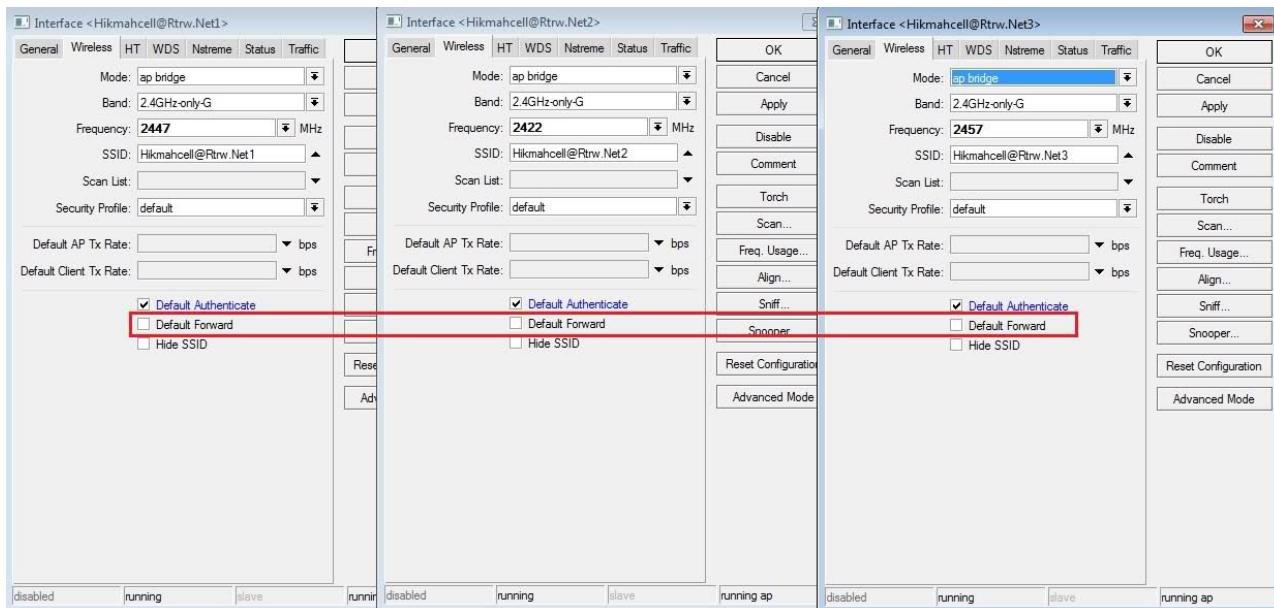


kita sebagai admin kalo pas tau bandwidth kita ada yg make gratis dengan cara cloning mac, kayak gimanaaa... gitu! dada ini sesek rasanya 😅 lho? kok malah curhat? katanya mau share?

he he.. ya udah langsung aja dah.. capek urusin user netcut saatnya kita tidur nyenyak..

Cluenya sih simple aja isolation mode! 😊

Pernah dengarkan? kalo di mikrotik khususnya seperti yg sy pake Rb433ah + 3xmpci dgn mode apbridge, kita tinggal ngilangin centang default forward pada tiap2 Interface wirelessnya, lihat gambar:



Sy pernah coba kok kayak gitu tapi tetap aja tembusss..!!! yaiyalah tembus.. kan belum selesai 😅

ok lanjut dah..

kenapa tetap bisa tembus? memang sih isolation mode untuk tiap2 Interface\_wireless udah aktif, tapi sebenarnya kita gak sadar masih ada celah yg terbuka lebar yg kita gak tau

dimana? di BRIDGE..., kenapa di BRIDGE? gini logikanya misal client[1] dan client[2] sama2 koneksi di wireless.1, dan client[3] koneksi di wireless.2 (yg udah diaktifin isolation\_mode/default\_forwardnya.) emang sih client[1] dan client[2] gak bisa saling komunikasi.. tapi sialnya lewat BRIDGE client[1] dan client[3] bisa saling komunikasi,, begitu pula client[2] dan client[3],  
Seandainya client[1] pake tool netcut untuk scan.. gimana netcut ini bisa mendapatkan informasi dari client[2]? sinetcut tinggal nanya aja ama client[3] 😅,  
begitu juga dengan client user netcut yg lain, dengan mudahnya mac/ip ini didapat, hasilnya isolation mode pun gak ada gunanya

ngerti gak dengan penjelasannya 😅? bodo ah' ngerti gak ngerti yg penting tidur nyanyak.. he he he...

nih dia biang keroknya gan, kita tinggal tutup celah masing2 Interface\_Wireless agar mereka (AP) tidak saling komunikasi (forward)

Kayak gini

#	Chain	Interfaces/In. Interface	Interfaces/Out. Interface	Action	Bytes	Packets
0	FORWARD	Hikmahcell@Rtrw.Net1	Hikmahcell@Rtrw.Net2	drop	5 988 871	54 723
1	FORWARD	Hikmahcell@Rtrw.Net1	Hikmahcell@Rtrw.Net3	drop	5 990 396	54 739
2	FORWARD	Hikmahcell@Rtrw.Net2	Hikmahcell@Rtrw.Net1	drop	771 773	7 441
3	FORWARD	Hikmahcell@Rtrw.Net2	Hikmahcell@Rtrw.Net3	drop	771 773	7 441
4	FORWARD	Hikmahcell@Rtrw.Net3	Hikmahcell@Rtrw.Net1	drop	612 819	4 745
5	FORWARD	Hikmahcell@Rtrw.Net3	Hikmahcell@Rtrw.Net2	drop	612 494	4 741

begini nih filternya sesuaikan dengan nama interface wirelesnya

Code:

```
/interface bridge filter
add action=drop chain=forward comment="" disabled=no in-interface=Wireless.1 out-
interface=Wireless.2
add action=drop chain=forward comment="" disabled=no in-interface=Wireless.1 out-
interface=Wireless.3
add action=drop chain=forward comment="" disabled=no in-interface=Wireless.2 out-
interface=Wireless.1
add action=drop chain=forward comment="" disabled=no in-interface=Wireless.2 out-
interface=Wireless.3
add action=drop chain=forward comment="" disabled=no in-interface=Wireless.3 out-
interface=Wireless.1
add action=drop chain=forward comment="" disabled=no in-interface=Wireless.3 out-
interface=Wireless.2
```

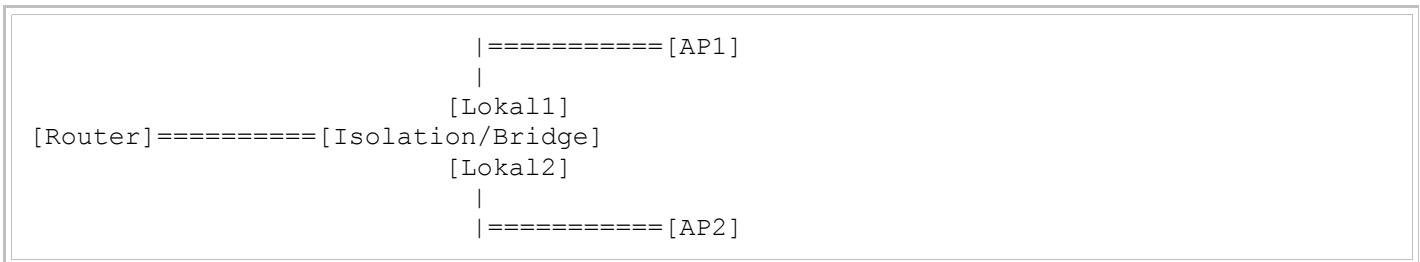
udah dah coba test scan pake netcut.. gimana ampuh gak? 😅 "biar lo tungguin ampe gondrong jg gak bakal keluar tuh mac/ipnya"

cara diatas menggunakan AP Rb433+3mpci dalam 1box

kalo dengan merk AP lain sih kurang lebih logikanya sama yaitu isolation client dan APnya.

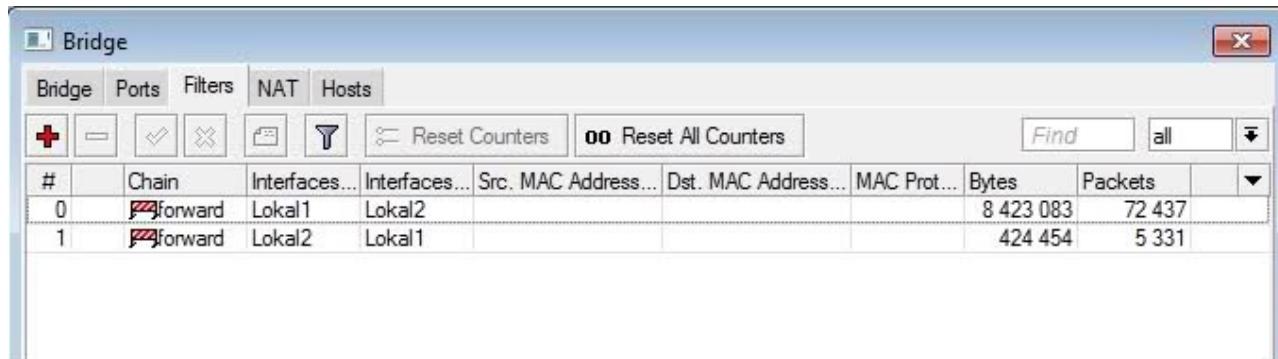
kalo misalkan topologinya kayak gini..

Code:



dibagian [Isolation/Bridge] jangan pernah pake switch yg biasa, pake yg manageable or SW250gs bisa juga, triknya sama usahakan set agar tiap2 interface yg menuju AP jangan saling komunikasi, kalo perlu pake RB skalian dengan mode Bridge dan aktifkan filternya kayak diatas..

Begini contohnya pake RB mode Bridge kurang lebih sama



Trik ini udah ane test dan hampir tiap hari ditest scan pake netcut dengan beda2 komputer saking belum yakinnya 😁, akhirnya bisa jualan dengan tenang.. 😁

Tunggu yg ampuh berikutnya 😊

## **FAQ - Terjemahan bebas dari Wiki Mikrotik**

Sumber: [http://wiki.mikrotik.com/wiki/MikroT...uestions\\_-\\_FAQ](http://wiki.mikrotik.com/wiki/MikroT...uestions_-_FAQ)

Penerjemah: yosanpro

Thread ini hanya untuk mempermudah newbie membaca FAQ yang ada pada MikroTik, dengan tambahan dari penerjemah dalam tanda --[ xxx ]--.

Tahap 1:

### **Apakah Mikrotik RouterOS itu?**

- \* Apa yang dilakukan Mikrotik RouterOS?
  - Mikrotik RouterOS adalah sistem operasi dan perangkat lunak yang mengubah Intel PC biasa atau Hardware MikroTik RouterBOARD menjadi sebuah dedicated router

- \* Bolehkan saya mencoba fungsi-fungsi MikroTik RouterOS sebelum saya membeli lisensi?

- Ya, anda dapat mendownload instalasi dari situs MikroTik dan menginstall MikroTik router sendiri. Router ini mempunyai fungsi-fungsi lengkap tanpa perlu lisensi untuk waktu berjalan total 24 jam. Cukup untuk mencoba router selama 3 hari pada penggunaan 8 jam per hari, jika anda mematikan router pada akhir dari jam ke 8 per hari.

- \* Dimana saya mendapatkan License Key?

- Buat sebuah akun pada situs MikroTik. Kartu kredit dapat digunakan untuk membayar. --[ Anda juga bisa membeli lisensi pada pedagang yang dapat dipercaya di forum ini ]--

- \* Bisakah saya menggunakan router MikroTik untuk berhubungan dengan penyedia layanan lewat T1, T3, atau koneksi kecepatan tinggi lainnya?

- Ya, anda dapat memasang bermacam-macam NIC yang didukung oleh MikroTik RouterOS dan mendapatkan edge router, backbone router, firewall, bandwidth manager, VPN server, wireless access point, Hotspot dan banyak lagi dalam satu box. Periksa daftar spesifikasi dan manual untuk interface yang didukung!

- \* Seberapa cepat router akan berjalan?

- Sebuah Intel PC lebih cepat daripada hampir semua router proprietary, dan ada banyak tenaga pemroses bahkan dalam CPU 100MHz.

- \* Bagaimana perangkat lunak ini dibandingkan dengan menggunakan router Cisco?

- Anda dapat melakukan hampir semua yang dilakukan router proprietary dengan hanya sebagian dari biaya router semacam itu dan memiliki fleksibilitas dalam mengupgrade, kemudahan manajemen dan pemeliharaan.

- \* OS apa yang dibutuhkan untuk menginstall MikroTik RouterOS?

- Tidak perlu sistem operasi. MikroTik RouterOS dipaket dengan sistem operasi dan perangkat lunaknya sendiri. OS yang digunakan berbasis kernel Linux dan sangat stabil. Hard drive anda akan dihapus seluruhnya oleh proses instalasi. Tidak ada dukungan disk tambahan, Hanya satu PRIMARY MASTER HDD atau flashdisk, kecuali untuk cache Web Proxy.

- \* Seberapa amankah router ini setelah di-setup?

- Akses ke router dilindungi oleh nama user dan password. User-user tambahan dapat ditambahkan ke router, hak-hak tertentu dapat diatur untuk group user. Akses Remote ke router dapat dibatasi berdasar user, alamat IP. Firewall filtering adalah cara termudah untuk melindungi router dan jaringan anda.

## Akses Masuk dan Kata Kunci

- \* Apa nama user dan kata kunci (password) saat memasuki router untuk pertama kali?
  - Nama user adalah 'admin', dan tidak ada password (Tekan tombol 'Enter'). Anda dapat mengubah password dengan perintah '/password'.
- 
- \* Bagaimana saya dapat mengambil password yang hilang?
  - Jika anda lupa password anda, tidak ada cara untuk mengambilnya kembali. Anda harus menginstall ulang router.
- 
- \* Setelah mati listrik router MikroTik tidak berjalan lagi
  - Jika anda tidak mematikan router anda dengan wajar, sistem file belum di-unmount dengan benar. Saat awal berjalan, RouterOS akan melakukan pemeriksaan sistem file. Tergantung dari ukuran HDD, ini bisa memakan waktu beberapa menit. Jangan mengganggu pemeriksaan sistem file! ini dapat membuat instalasi anda tidak dapat digunakan.
- 
- \* Bagaimana saya dapat mengakses router jika interface LAN telah di-disable?
  - Anda dapat mengakses router secara lokal (dengan monitor dan keyboard) maupun melalui konsol serial.

## Tentang Lisensi

- \* Berapa banyak instalasi MikroTik RouterOS yang dicakup oleh satu lisensi?
  - Lisensi adalah per instalasi RouterOS. Tiap router yang diinstall membutuhkan lisensi terpisah.
- 
- \* Apakah lisensi bisa kadaluarsa?
  - Lisensi tidak pernah kadaluarsa. Router berjalan selamanya. Namun, lisensi memiliki batasan upgrade, -- [RouterOS hanya dapat di upgrade ke versi mayor yang sama dan 1 versi mayor diatasnya. ]--
- 
- \* Bagaimana saya menginstall ulang perangkat lunak MikroTik RouterOS tanpa kehilangan lisensi?
  - Anda harus menggunakan CD, Floppy, atau prosedur NetInstall dan menginstall MikroTik RouterOS pada HDD dengan instalasi MikroTik RouterOS sebelumnya masih ada. Lisensi tersimpan dalam HDD. Jangan menggunakan utility format atau partisi, ini akan menghapus key anda! Gunakan BIOS setting yang sama (dengan waktu instalasi awal) untuk HDD anda!
- 
- \* Dapatkah saya menggunakan lisensi MikroTik RouterOS saya pada hardware berbeda?
  - Ya, anda dapat menggunakan hardware berbeda (motherboard, NIC), tetapi anda harus menggunakan HDD yang sama. Lisensi tersimpan dalam HDD kecuali utility format atau fdisk digunakan. Tidak perlu menginstall ulang sistem saat berganti ke hardware lain. Saat membayar lisensi, mohon perhatikan, bahwa ini tidak dapat digunakan pada harddrive lain daripada yang digunakan untuk instalasi. Transfer lisensi ke hard drive lain dikenai biaya 10\$. Hubungi support untuk hal ini.
- 
- \* Apa yang dilakukan, jika hard drive dengan MikroTik RouterOS saya rusak, dan saya harus menginstall lagi?
  - Jika anda telah membayar lisensi, anda harus menulis ke support[at]mikrotik.com dan menjelaskan situasinya. Kami bisa meminta anda untuk mengirim hard drive yang rusak kepada kami sebagai bukti untuk mendapatkan key pengganti. Jika anda mempunyai demo lisensi gratis, tidak ada penggantian key. Silahkan mendapatkan demo lisensi lain, atau membeli lisensi pokok.
- 
- \* Bagaimana saya memasukkan Software Key baru?
  - Memasukkan lisensi dari Console/FTP:
  - Impor file yang disertakan dengan perintah '/system license import' (anda harus mengupload file ini ke FTP

server router)

- Memasukkan lisensi dengan Console/Telnet:
  - ) Gunakan copy/paste untuk memasukkan key ke dalam jendela Telnet (tidak peduli dalam submenu apapun). Pastikan mengcopy seluruh key, termasuk baris"--BEGIN MIKROTIK SOFTWARE KEY--" dan "--END MIKROTIK SOFTWARE KEY--"
  - Memasukkan lisensi dari Winbox:
    - ) Gunakan menu 'system -> license' di Winbox untuk paste atau meng-impor key

\* Saya telah salah mengetikkan software ID saat membeli Software Key. Bagaimana saya memperbaikinya?

- Pada Account Server pilih 'work with keys', kemudian pilih key yang salah ketik, dan pilih 'fix key'.

Tentang memasukkan key, selengkapnya di halaman ini

[http://wiki.mikrotik.com/wiki/Entering\\_a\\_RouterOS\\_License\\_key](http://wiki.mikrotik.com/wiki/Entering_a_RouterOS_License_key)

Informasi lainnya tentang License Key dapat ditemukan disini

[http://wiki.mikrotik.com/wiki/All\\_about\\_licenses](http://wiki.mikrotik.com/wiki/All_about_licenses)

## Instalasi

\* Berapa besar HDD yang dapat saya gunakan untuk MikroTik RouterOS?

- MikroTik RouterOS mendukung disk lebih besar dari 8GB (biasanya hingga 120GB). Akan tetapi pastikan BIOS dari motherboard router mampu mendukung disk besar ini.

\* Dapatkah saya menjalankan MikroTik RouterOS dari sembarang hard drive di sistem saya?

- Ya

\* Adakah dukungan untuk hard drive ganda di MikroTik RouterOS?

- Drive sekunder didukung untuk web cache. Dukungan ini telah ditambahkan di versi 2.8, versi yang lebih lama tidak mendukung hard drive ganda.

\* Mengapa CD instalasi berhenti pada titik tertentu dan tidak "berjalan terus"?

- CD instalasi tidak bekerja dengan benar pada beberapa motherboard. Coba booting ulang komputer dan mulai instalasi lagi. Jika ini tidak membantu, coba gunakan hardware lain.

## Upgrade

\* Bagaimana saya menginstall paket-paket fitur tambahan?

- Anda harus menggunakan file-file paket (ekstensi .npk) dengan versi yang sama dengan paket sistem. Gunakan perintah '/system package print' untuk melihat daftar paket-paket terinstall. Periksa sisa ruang pada HDD router dengan perintah '/system resource print' sebelum meng-upload file-file paket. Pastikan anda mempunyai paling tidak sisa ruang 2MB pada router setelah anda meng-upload file-file paket!

Upload file-file paket anda dengan ftp mode BINARY ke router dan panggil perintah '/system reboot' untuk mematikan router dan booting ulang. Paket-paket tersebut diinstal (diupgrade) saat router akan dimatikan.

Anda dapat memantau proses instalasi dengan layar monitor terhubung ke router. Setelah reboot, paket-paket terinstall akan terdaftar pada '/system package print'.

\* Bagaimana saya mengupgrade?

- Untuk meng-upgrade software ini, anda harus mendownload file-file paket terbaru (\*.npk) dari website kami (paket 'system' ditambah paket yang anda butuhkan). Kemudian, upload paket-paket yang baru melalui FTP dengan menggunakan mode transfer Binary.

- \* Saya menginstall paket fitur tambahan, tetapi interface yang bersangkutan tidak muncul pada daftar '/interface print'.
    - Anda harus mendapatkan (membeli) level lisensi yang dibutuhkan atau install paket NPK untuk interface ini (contohnya paket 'wireless').
  - \* Jika saya mengupgrade RouterOS, apakah konfigurasi saya akan hilang?
    - Tidak, konfigurasi akan tetap tersimpan saat mengupgrade dalam satu tingkat versi. Saat mengupgrade tingkatan versi (contohnya, v2.5 ke v2.6) anda mungkin kehilangan konfigurasi dari beberapa fitur yang memiliki perubahan drastis. Misalnya saat mengupgrade dari v2.4, anda seharusnya mengupgrade ke versi terakhir dari 2.4 dahulu.
  - \* Berapa besar sisa ruang disk yang saya butuhkan saat mengupgrade ke versi lebih tinggi?
    - Anda membutuhkan ruang untuk paket sistem dan paket-paket tambahan yang harus diupgrade. Setelah meng-upload versi yang lebih baru ke router anda harus memiliki setidaknya sisa ruang disk 2MB. Jika tidak, jangan mencoba mengupgrade! Buang paket-paket yang tidak perlu terlebih dahulu, dan kemudian upgrade sisanya.
- ### **Downgrade (menurunkan versi)**
- \* Bagaimana saya men-downgrade instalasi MikroTik RouterOS ke versi lebih lama?
    - Anda dapat men-downgrade dengan menginstall ulang RouterOS dari media apapun. Lisensi software akan tersimpan dalam HDD selama disk tidak di partisi ulang/format ulang. Konfigurasi dari router akan hilang (Adalah mungkin untuk menyimpan konfigurasi lama, tetapi pilihan ini bisa memberi hasil yang tidak diduga saat men-downgrade dan tidak direkomendasi menggunakannya). Cara lain adalah dengan menggunakan perintah '/system downgrade'. Ini hanya bekerja jika anda men-downgrade ke versi 2.7.20 dan tidak lebih rendah. Upload paket-paket lama ke router melalui FTP dan gunakan perintah '/system downgrade'.
- ### **Pertanyaan Seputar TCP/IP**
- \* Saya mempunyai dua NIC card di Router Mikrotik dan keduanya bekerja dengan normal. Saya bisa ping kedua jaringan dari router tetapi tidak bisa ping dari satu jaringan melalui router ke jaringan lainnya dan Internet. Saya tidak mengeset firewall.
    - Ini adalah masalah yang umum, dimana anda tidak mengeset routing pada gateway Internet utama anda. Karena anda telah menambah jaringan baru, anda perlu 'memberitahu' tentang jaringan tersebut pada gateway utama anda (ISP anda). Sebuah route musti ditambahkan untuk jaringan baru anda. Alternatif lainnya, anda dapat 'menyembunyikan' jaringan baru anda dengan 'masquerade' untuk dapat mengakses Internet. Harap mempelajari Petunjuk Setup Dasar, dimana permasalahan dibahas dan solusi diberikan.
  - Berikut adalah contoh bagaimana memberi masquerade pada jaringan lokal pribadi anda:
- Code:
- ```
[admin@MikroTik] ip firewall nat> add chain=srcnat action=masquerade out-interface=Public
[admin@MikroTik] ip firewall nat> print
Flags: X - disabled, I - invalid, D - dynamic
  0  chain=srcnat out-interface=Public action=masquerade
```
- \* Bagaimana saya bisa mengubah nomor port TCP untuk layanan telnet atau http, jika saya tidak ingin menggunakan port 23 dan 80?
    - Anda dapat mengubah port yang dialokasikan dalam '/ip service'

\* Ketika saya menggunakan Alamat IP/mask dalam bentuk 10.1.1.17/24 untuk rule filter atau queue, tidak dapat digunakan.

- Rule tersebut 'tidak dapat digunakan', karena rule tersebut tidak cocok dengan paket karena alamat/mask yang salah. Bentuk yang benar seharusnya:

Code:

```
10.1.1.0/24 untuk alamat IP pada range 10.1.1.0-10.1.1.255, atau,  
10.1.1.17/32 untuk satu alamat IP 10.1.1.17 saja.
```

\* Saya ingin men-setup klien DHCP, tetapi tidak ada menu '/ip dhcp-client'.

- Fitur DHCP tidak tercakup dalam paket sistem. Anda harus menginstall paket DHCP. Upload ke router dan boot ulang!

\* Bisakah saya 'mengikat' IP ke alamat MAC melalui DHCP?

- Ya, anda dapat menambah lease static ke daftar lease DHCP server. Akan tetapi, DHCP secara default tidak aman, dan lebih baik menggunakan PPPoE untuk otentifikasi user dan pemberian alamat IP. Anda dapat meminta user untuk log on dari alamat MAC yang terdaftar juga.

--[ Pertanyaan berikutnya pada wiki tidak diterjemahkan karena tidak relevan lagi dengan versi MikroTik yang banyak dipakai di forum ]--

\* Saya tidak dapat mengakses beberapa situs saat menggunakan PPPoE.

- Gunakan '/ip firewall mangle' untuk mengubah MSS (maximum segment size) ke nilai 40 byte lebih rendah dibandingkan koneksi MTU anda. Misalnya, jika anda telah mengenkripsi PPPoE dengan MTU=1492, set rule mangle sebagai berikut:

Code:

```
/ip firewall mangle  
add chain=forward protocol=tcp tcp-flags=syn action=change-mss new-mss=1448
```

## Pertanyaan seputar Manajemen Bandwidth

\* Dapatkah saya menggunakan MikroTik sebagai bridge dan pengatur trafik dalam satu mesin?

- Ya. Anda dapat menggunakan semua fitur ekstensif manajemen queue. Atur queue ke interface dimana trafik meninggalkan router, saat melalui router. Ini bukan interface bridge! Queue pada interface bridge hanya meliputi trafik yang berasal dari router.

\* Dapatkah saya membatasi bandwidth berdasarkan MAC address?

- Untuk download:

1. Beri connection-mark semua paket dari MAC tiap klien dengan nama berbeda untuk tiap klien dengan action=passthrough

Code:

```
/ip firewall mangle add chain=prerouting src-mac-address=11:11:11:11:11:11 \  
action=mark-connection new-connection-mark=host11 passthrough=yes
```

2. Tandai lagi paket ini dengan flow-mark (sekali lagi dengan flow-mark berbeda untuk tiap connection-mark):

Code:

```
/ip firewall mangle add chain=prerouting connection-mark=host11 new-packet-  
mark=host11
```

3. Kita bisa menggunakan flow-mark ini di queue tree sekarang  
Meskipun solusi ini berfungsi, namun dasarnya tidak sempurna karena paket pertama dari tiap koneksi tidak akan terhitung.

- Untuk Upload:

Code:

```
[admin@AP] ip firewall mangle> add chain=prerouting src-mac-address=11:11:11:11:11:11  
\  
action=mark-packet new-packet-mark=upload
```

### Pertanyaan Wireless

\* Dapatkah saya mem-bridge interface wlan yang beroperasi di mode station?

- Tidak bisa

--[ Untuk MikroTik RouterOS V3.xx, anda bisa menggunakan mode station-pseudobridge ]—

MODE RADIO :

alignment-only - this mode is used for positioning antennas (to get the best direction)

ap-bridge - the interface is operating as an Access Point

bridge - the interface is operating as a bridge. This mode acts like ap-bridge with the only difference being it allows only one client

nstreme-dual-slave - the interface is used for nstreme-dual mode

station - the interface is operating as a wireless station (client)

station-pseudobridge - wireless station that can be put in bridge. MAC NAT is performed on all traffic sent over the wireless interface, so that it looks like coming from the station's MAC address regardless of the actual sender (the standard does not allow station to send packets with different MAC address from its own).

Reverse translation (when replies arrive from the AP to the pseudobridge station) is based on the ARP table. Non-IP protocols are being sent to the default MAC address (the last MAC address, which the station has received a non-IP packet from). That means that if there is more than one client that uses non-IP protocols (for example, PPPoE) behind the station, none of them will be able to work correctly

station-pseudobridge-clone - similar to the station-pseudobridge, but the station will clone MAC address of a particular device (set in the station-bridge-clone-mac property), i.e. it will change its own address to the one of a different device. In case no address is set in the station-bridge-clone-mac property, the station postpones connecting to an AP until some packet, with the source MAC address different from any of the router itself, needs to be transmitted over that interface. It then connects to an AP with the MAC address of the device that have sent that packet

station-wds - the interface is working as a station, but can communicate with a WDS peer

wds-slave - the interface is working as it would work in ap-bridge mode, but it adapts to its WDS peer's frequency if it is changed

### NAT ( Network Address Translation)

#### Aktivitas

Network Address Translation (NAT) adalah sebuah router yang mengantikan fasilitas sumber dan (atau)

alamat IP tujuan dari paket IP karena melewati jalur router. Hal ini paling sering digunakan untuk mengaktifkan beberapa host di jaringan pribadi untuk mengakses internet dengan menggunakan satu alamat IP publik.

## Spesifikasi

Paket yang diperlukan: sistem

Lisensi yang diperlukan: level1 (jumlah terbatas pada aturan 1), Level3

Standar dan teknologi: IP, RFC1631, RFC2663

Penggunaan hardware: increase with the count of rules

## NAT ada 2 jenis yaitu:

1. **Sumber(source) NAT** atau **srcnat**. Jenis NAT dilakukan pada paket yang berasal dari natted jaringan.

Router A NAT akan mengganti sumber alamat IP dari sebuah paket dengan alamat IP baru publik karena perjalanan melalui router. A setiap operasi diterapkan ke paket balasan dalam arah lainnya.

2. **Tujuan(destination) NAT** atau **dstnat**. Jenis ini dilakukan pada paket yang ditujukan ke natted jaringan. Hal ini umumnya digunakan untuk membuat host di jaringan pribadi untuk dapat diakses dari Internet. router A NAT melakukan dstnat menggantikan alamat IP tujuan dari sebuah paket IP karena perjalanan melalui router terhadap jaringan pribadi.

## NAT Drawbacks(menarik mundur)

Host di balik NAT- enabled router tidak benar end-to-end connectivity. Ada beberapa protokol internet mungkin tidak bekerja dengan skenario NAT. Pelayanan yang membutuhkan inisiasi dari koneksi TCP dari dalam atau luar jaringan status protokol seperti UDP, dapat terganggu. Terlebih lagi, beberapa protokol yang tetap bertentangan dengan NAT,

## Redirect dan Masquerade

Redirect dan masquerade adalah bentuk khusus tujuan NAT dan sumber NAT, masing-masing. Redirect adalah diutamakan dengan ke tujuan NAT biasa dengan cara yang sama seperti yang masquerade diutamakan ke sumber masquerade NAT adalah bentuk khusus sumber NAT tanpa perlu menentukan ke alamat - alamat keluar antarmuka yang digunakan secara otomatis. Yang sama adalah redirect - ia adalah satu bentuk tujuan NAT ke mana-alamat yang tidak digunakan - masuk antarmuka digunakan sebagai ganti alamat. Perlu diketahui bahwa to-port adalah makna penuh untuk redirect aturan – ini adalah port layanan pada router yang akan menangani permintaannya (contoh:webproxy)

Ketika paketnya adalah dst-natted (tidak perduli - action=nat atau action=redirect), dst alamat berubah.

Informasi tentang terjemahan alamat (termasuk alamat asli dst) disimpan dalam tabel router internal.

Transparan proxy web bekerja pada router (bila permintaan mendapatkan web redirect ke port proxy pada router) dapat mengakses informasi ini dari table internal dan mendapatkan alamat web server dari alamat IP header (dst karena alamat IP dari paket yang sebelumnya adalah alamat web server telah berubah ke alamat server proxy). Mulai dari HTTP/1.1 ada khusus di header permintaan HTTP yang berisi alamat web server, jadi server proxy dapat menggunakannya, dst, bukan alamat IP paket, jika tidak ada semacam header (HTTP versi lama pada klien), proxy server dapat tidak menentukan alamat web server dan karena itu tidak dapat bekerja.

Ini berarti, adalah mustahil untuk benar transparan redirect dari lalu lintas HTTP ke beberapa router lainnya box transparan-proxy. Hanya dengan cara yang benar adalah dengan menambahkan transparan proxy di router itu sendiri, dan konfigurasikan agar Anda "real" proxy adalah orang parent-proxy. Dalam situasi ini Anda "real" proxy tidak harus transparan lagi, sebagai proxy pada router akan transparan dan akan meneruskan permintaan proxy-style (menurut standar; permintaan ini mencakup semua informasi yang diperlukan tentang

web server) to "real" proxy.

### Keterangan Properti

**action (accept | add-dst-to-address-list | add-src-to-address-list | dst-nat | jump | log | masquerade | netmap | passthrough | redirect | return | same | src-nat; default: accept)** - untuk melakukan tindakan jika paket sesuai dengan aturan

- **accept** - menerima paket. Tidak ada tindakan yang diambil, yaitu paket yang lulus dan tidak lagi melalui aturan-aturan yang diterapkan
- **add-dst-to-address-list** - menambahkan tujuan dari sebuah alamat IP paket ke alamat yang ditentukan daftar oleh daftar alamat-parameter
- **add-src-to-address-list** - menambahkan sumber alamat IP dari sebuah paket ke alamat yang ditentukan oleh daftar daftar alamat-parameter
- **dst-nat** - menggantikan alamat tujuan dari sebuah paket ke IP ditentukan oleh nilai-nilai to-address dan parameter ke-port
- **jump** - melompat ke rantai yang ditentukan oleh nilai yang melompat-sasaran parameter
- **log** - masing-masing sesuai dengan tindakan ini akan menambah sebuah pesan masuk ke sistem
- **masquerade** - menggantikan sumber alamat IP secara otomatis ke salah satu paket ditentukan oleh fasilitas routing alamat IP
- **netmap** - membuat statis 1:1 pemetaan sekumpulan alamat IP yang lain. Sering digunakan untuk mendistribusikan publik host ke alamat IP pribadi pada jaringan
- **passthrough** - mengabaikan aturan ini pergi ke yang berikutnya atau berlanjut ke rules yg berada dibawahnya
- **redirect** - tujuan menggantikan alamat IP dari sebuah paket ke salah satu router lokal alamat
- **return** - melewati kontrol kembali ke tempat dari rantai melompat terjadi
- **same** - memberikan tertentu klien yang sama sumber / tujuan dari alamat IP yang disediakan untuk berbagai masing-masing sambungan. Hal ini paling sering digunakan untuk layanan yang mengharapkan klien alamat yang sama untuk beberapa sambungan dari klien yang sama
- **src-nat** - menggantikan sumber alamat IP dari sebuah paket ke ditentukan oleh nilai-nilai ke-alamat dan parameter ke-port

**address-list (name)** - menetapkan nama untuk mengumpulkan daftar alamat IP dari aturan yang action = add-dst-to-address-list atau action = add-src-to-address-list tindakan. Daftar alamat inikemudian digunakan untuk paket yang cocok

**address-list-timeout (time; standar: 00:00:00)** - interval waktu setelah alamat yang akan dihapus dari daftar alamat-alamat yang ditentukan oleh daftar parameter. Digunakan bersama-sama dengan tambah-dst-to-address-list-src atau menambahkan ke daftar alamat-tindakan

- **00:00:00** - meninggalkan alamat di daftar alamat selamanya

**chain (dstnat | srcnatname)** - menentukan rantai untuk meletakkan aturan tertentu ke dalam. Karena lalu lintas yang berbeda dimasukan melalui berbagai rantai, selalu berhati-hati dalam memilih yang tepat untuk rantai baru aturan. Jika input tidak sesuai dengan nama yang sudah ditetapkan rantai, rantai baru akan dibuat

- **dstnat** - aturan yang ditempatkan di rantai ini diterapkan sebelum routing. Aturan-aturan yang menggantikan tujuan alamat IP paket harus ditempatkan di sana
- **srcnat** - aturan yang ditempatkan di rantai ini akan diterapkan setelah routing. Aturan-aturan yang menggantikan sumber alamat IP paket harus ditempatkan di sana,

**comment (teks)** - Berikan komentar untuk memerintah. Komentar dapat digunakan untuk mengidentifikasi bentuk peraturan skrip

**connection-byte** (integerinteger) - sesuai paket yang diberikan hanya jika jumlah byte telah ditransfer melalui sambungan tertentu

- 0 - berarti infinity, exempli Gratia: sambungan-byte = 2000000-0 berarti jika sesuai aturan lebih dari 2MB yang ditransfer melalui sambungan relevan

**connection-limit** (integernetmask) - membatasi jumlah koneksi per alamat atau alamat blok (cocok jika ditentukan jumlah sambungan telah ditetapkan)

**connection-mark** (name) - sesuai paket ditandai melalui fasilitas ngoyakkan dengan sambungan menandai

**connection-type** (ftp | GRE | h323 | irc | mms | PPTP | quake3 | TFTP) - sesuai dari paket-paket yang terkait sambungan berdasarkan informasi dari pelacakan koneksi penolongpun. A relevan sambungan penolong harus diaktifkan di / ip firewall service-port

**conten** (teks) - teks harus berisi paket agar sesuai dengan aturan

**dscp** (integer: 0 .. 63) –DSCP (ex-KL) IP kepala bidang nilai

**dst-address** (alamat IP addressnetmaskIP addressIP) - menentukan rentang alamat IP adalah paket yg diperuntukkan untuk. Perlu diketahui bahwa konsol mengkonversi memasukkan alamat / netmask nilai jaringan ke alamat yang valid,

i.e.: 1.1.1.1/24 dikonvert ke 1.1.1.0/24

**dst-address-list** (name) - sesuai alamat tujuan dari paket yang ditetapkan pengguna terhadap daftar alamat dst-address-type (unicast | lokal | broadcast | multicast) - sesuai tujuan alamat jenis IP paket, salah satu:

- **unicast** - alamat IP yang digunakan untuk satu titik ke titik lainnya transmisi. Hanya ada satu pengirim dan penerima dalam hal ini
- **local** - sesuai alamat yang ditugaskan ke router dari interface
- **broadcast** - IP paket akan dikirim dari satu titik ke semua titik dalam IP subnetwork
- **multicast** - jenis alamat IP yang bertanggung jawab untuk transmisi atau lebih dari satu poin ke satu set lainnya

**dst-limit** (integertimeintegerdst-address | dst-port | src-addresstime) - membatasi paket per detik (pps) menilai pada tujuan per IP atau per port tujuan dasar. Yang bertentangan dengan batas cocok, setiap alamat IP tujuan / tujuan pelabuhan itu sendiri batas. Pilihannya adalah sebagai berikut (dalam urutan tampilan):

- **count** - maksimum rata-rata harga paket, diukur dalam paket per detik (pps), kecuali jika diikuti oleh waktu opsi
- **time** - menentukan interval waktu yang lebih dari paket menilai diukur
- **burst** - jumlah paket yang cocok dengan yang di burst
- **modus** - yang pengolong (-s) menilai paket untuk membatasi
- **expire** - Interval setelah menentukan alamat IP yang direkam / port akan dihapus

**dst-port** (integer: 0 .. 65535integer: 0 .. 65535) - tujuan nomor port atau range

**fragmen** (ya | tidak) - apakah paket adalah fragmen dari sebuah paket IP. Memulai paket (i.e., pertama fragmen) tidak dihitung. Catatan yang sambungan pelacakan diaktifkan, tidak akan ada fragmen karena sistem akan secara otomatis assembles setiap paket

- hotspot** (multiple choice: auth | from-client | http | lokal dst | to-client) - cocok paket diterima dari klien terhadap berbagai kondisi Hotspot. Semua nilai-nilai dapat negated
- **auth** - benar, jika paket yang berasal dari authenticated HotSpotclient
  - **from-client** - benar, jika paket yang datang dari klien Hotspot
  - **http** - benar, jika Hotspot klien mengirimkan sebuah paket ke alamat dan port sebelumnya terdeteksi sebagai server proxy (proxy teknik Universal) atau jika tujuan port 80 dan transparan proxying diaktifkan bagi klien
  - **local-dst** - benar, jika paket memiliki tujuan lokal alamat IP
  - **to-client** - benar, jika paket yang akan dikirim ke klien

**ICMP-option** (integerinteger) - cocok ICMP Jenis: Kode bidang

**in-bridge-port** (name) - interface sebenarnya paket telah dimasukkan melalui router (jika Bridged, ini kekayaan sesuai dengan sebenarnya jembatan pelabuhan, sedangkan di-interface jembatan itu sendiri)

**in-interface** (nama) - antarmuka paket yang telah dimasukkan melalui router (jika antarmuka adalah Bridged, maka akan muncul paket yang akan datang dari jembatan antarmuka sendiri)

**ingress-priority** (integer: 0 .. 63) - masuk (diterima) prioritas paket, jika diatur (0 lainnya).

Prioritas mungkin berasal dari salah satu atau VLAN WMM prioritas

**IPv4-option** (any | loose-source-routing | no-record-route | no-router-alert | no-source-routing | no-timestamp | none | record-route | router-alert | strict-source-routing | timestamp) - match ipv4 header option

- **any** - paket cocok dengan setidaknya salah satu pilihan IPv4
- **loose-source-routing** - paket cocok dengan sumber loose routing pilihan. Pilihan ini digunakan untuk rute internet datagram berdasarkan informasi yang diberikan oleh sumber
- **no-record-route** - tidak cocok dengan paket dengan catatan rute pilihan. Pilihan ini digunakan untuk rute yang internet datagram berdasarkan informasi yang diberikan oleh sumber
- **no-router-alert** - tidak cocok dengan paket router mengubah pilihan
- **no-source-routing** - tidak cocok dengan paket sumber routing pilihan
- **no-timestamp** - tidak cocok dengan paket waktu opsi
- **record-route** - paket cocok dengan catatan rute pilihan
- **router-alert** - paket cocok dengan router mengubah pilihan
- **strict-source-routing** - paket cocok dengan ketat sumber routing pilihan
- **timestamp** sesuai dengan paket

**jump-target** (dstnat | srcnatname) - nama target untuk melompat ke rantai, jika action= jump

**layer7-protokol** (name) - Layer 7 menyaring nama sebagaimana ditetapkan dalam / ip firewall layer7-protokol menu. Perhatian: ini matcher kebutuhan daya tinggi computer

**limit** (integertimeinteger) - membatasi paket cocok untuk menilai suatu batas. Berguna untuk mengurangi jumlah dari log pesan

- **count** - maksimum rata-rata harga paket, diukur dalam paket per detik (pps), kecuali jika diikuti oleh waktu opsi
- **time** - menentukan interval waktu yang lebih dari paket menilai diukur
- **burst** - jumlah paket yang cocok dengan yang di burst

**log-prefix** (teks) - semua pesan log akan ditulis ke berisi awalan ditentukan di sini. Digunakan dalam bersama-sama dengan action =log

**nth** (integerinteger: 0 .. 15integer) - cocok Nth paket tertentu yang diterima oleh aturan. Satu dari 16 counter tersedia dapat digunakan untuk menghitung paket-paket

- **every** - cocok setiap tanggal 1 setiap paket. Misalnya, jika setiap = 1 maka setiap aturan yang cocok 2. paket
- **counter** - menentukan yang digunakan. A counter akan menambahkan setiap kali berisi aturan nth cocok cocok
- **packet** - cocok diberikan pada paket nomor. Nilai dengan jelas alasan harus antara 0 dan setiap. Jika opsi ini digunakan untuk suatu counter, maka harus ada sekurang-kurangnya setiap 1 peraturan dengan opsi ini, yang meliputi semua nilai antara 0 dan setiap inclusively.

**out-bridge-port** (name) - antarmuka yang sebenarnya adalah paket meninggalkan router melalui (jika Bridged, ini kekayaan sesuai dengan sebenarnya jembatan pelabuhan, sementara out-interface - jembatan itu sendiri)

**out-interface** (name) - interface adalah paket meninggalkan router melalui (jika antarmuka adalah Bridged, maka paket akan muncul untuk meninggalkan jembatan melalui antarmuka sendiri)

**paket-mark** (teks) - sesuai paket ditandai melalui fasilitas ngoyakkan dengan paket tandai paket-size (integer: 0 .. 65535integer: 0 .. 65535) - sesuai paket yang ditentukan atau ukuran berbagai ukuran dalam byte

- **min** - menetapkan batas yang lebih rendah dari berbagai ukuran atau berdasarkan nilai
- **max** - menetapkan batas atas dari berbagai ukuran

**port** (port) - jika ada yang cocok (sumber atau tujuan) port ditentukan sesuai dengan daftar port atau port rentang (dicatat bahwa protokol harus masih dapat dipilih, seperti biasa untuk src dan dst-port-port matchers) Protocol (ddp | EGP | encap | ggp | GRE | hmp | ICMP | idrp-cmtp | igmp | ipencap | ipip | ipsec-ah | ipsec-esp | iso-tp4 | ospf | pup | rdp | rspf | st | tcp | udp | vmtcp | xns-IDP | xtpinteger) - cocok protokol IP tertentu ditentukan oleh protokol nama atau nomor. Anda harus menetapkan pengaturan ini jika Anda ingin menentukan port

**PSD** (integertimeintegerinteger) - berupaya untuk mendeteksi dan UDP TCP scans. Hal ini disarankan untuk menetapkan

menurunkan berat ke pelabuhan dengan angka tinggi untuk mengurangi frekuensi palsu positif, seperti dari pasif mode FTP transfer

- **WeightThreshold** - total berat terbaru TCP / UDP paket dengan tujuan pelabuhan yang berasal dari host yang sama untuk diperlakukan sebagai port scan urutan
- **DelayThreshold** - menunda untuk paket dengan tujuan yang berbeda yang datang dari pelabuhan yang sama tuan rumah harus dirawat sebaik mungkin port scan subsequence
- **LowPortWeight** - berat yang paket dengan privilege (<= 1024) tujuan pelabuhan
- **HighPortWeight** - berat paket dengan non-privilidged tujuan pelabuhan

**random** (integer) - sesuai dengan paket yang diberikan secara acak propability

**routing-mark** (name) - sesuai paket ditandai dengan merusak fasilitas routing mark

**same-not-by-dst** (yes | no) - untuk menentukan apakah account atau tidak untuk mencapai tujuan IP alamat yang baru ketika memilih sumber alamat IP untuk paket cocok dengan aturan oleh ation= sama

**src-address** (alamat IP addressnetmaskIP addressIP) - menentukan rentang alamat IP adalah paket berasal

dari. Perlu diketahui bahwa konsol mengkonversi memasukkan alamat / netmask nilai yang valid untuk jaringan alamat, yaitu: 1.1.1.1/24 dikonvert ke 1.1.1.0/24

**src-address-list** (nama) - sesuai alamat sumber dari paket terhadap pengguna ditetapkan daftar alamat

**src-address-type** (unicast | lokal | broadcast | multicast) - sesuai jenis sumber alamat IP paket, salah satu:

- **unicast** - alamat IP yang digunakan untuk satu titik ke titik lainnya transmisi. Hanya ada satu pengirim dan penerima dalam hal ini
- **local** - sesuai alamat yang ditugaskan ke router dari interface
- **broadcast** - IP paket akan dikirim dari satu titik ke semua titik dalam IP subnetwork
- **multicast** - jenis alamat IP yang bertanggung jawab untuk transmisi atau lebih dari satu poin ke satu set lainnya. Registered lainnya merek dagang dan merek dagang yang disebutkan di sini adalah properti dari masing-masing pemilik.
- **src-mac-address** (MAC address) - sumber alamat MAC src-port (integer: 0 .. 65535 integer: 0 .. 65535) - Nomor port sumber atau jangkauan
- **tcp-MSS** (integer: 0 .. 65.535) - TCP MSS sesuai nilai IP paket
- **time** (timetime sat | Jumat | thu | Rabu | Selasa | Senin | Minggu) - memungkinkan untuk membuat penyaring berdasarkan paket ' tiba waktu dan tanggal, atau untuk paket lokal yang dihasilkan, waktu dan tanggal keberangkatan
- **to-address** (alamat addressIP; default: 0.0.0.0) - alamat atau kisaran alamat untuk menggantikan asli alamat IP dari sebuah paket dengan
- **to-port** (integer: 0 .. 65535 integer: 0 .. 65535) - port atau jangkauan port untuk menggantikan port asli dengan sebuah IP bersama paket

## NTP Server

Setiap kali mikrotik RB kita reboot, maka jam dan tanggalnya pasti berubah lagi menjadi tanggal dan jam yang sudah lampau di tahun 1980-an. Nah, untuk menghindari hal itu terjadi, kita bisa memasang NTP-client service dengan melakukan hal ini :

Masuk ke mikrotik melalui winbox, pilih system - ntp-client - beri tanda cawang pada enable dan pilih UNICAST. Kemudian masukkan salah satu IP NTP server dibawah ini : (pilih yang bisa diakses saja)

203.160.128.6  
203.160.128.2  
202.162.32.12  
210.188.204.210  
207.46.197.32  
122.200.151.43

Pastikan port 123 dalam kondisi TIDAK TERBLOKIR untuk dapat menggunakan service NTP ini.

---

CREATE DOTA DI MIKROTIK  
Pakai script



Untuk settingannya aja  
pake script aja di >>> system >>> Script  
nanti klik + Kasih nama Dota atau apalah terserah  
nanti di kolom source nya kasih script ini

Quote:

```
{  
:local ipnya  
:set ipnya "192.168.x."  
:local iprouternya  
:set iprouternya 62  
:local publicnya  
:set publicnya "123.456.xx.xx"  
:local portnya  
:set portnya 6201  
:local startipnya  
:set startipnya 201  
:local endipnya  
:set endipnya 220  
:for i from=$startipnya to=$endipnya do={  
/ip firewall nat add chain=srcnat src-address=($ipnya . "0/24") dst-address=($ipnya . $i) protocol=tcp dst-port=($portnya) action=src-nat to-addresses=($ipnya . $iprouternya) to-ports=0-65535 comment="$portnya"  
/ip firewall nat add chain=dstnat dst-address=($publicnya) protocol=tcp dst-port=($portnya) action=dst-nat to-addresses=($ipnya . $i) to-ports=$portnya  
:set portnya ($portnya + 1)}  
}
```

jangan lupa local ip nya di sett sama ip public nya... tu yang di bold  
terus ok

kalo udah selesai tinggal di RUN aja..

nanti liat di NAT nya.. ada 6201 sampai 620xx itu portnya

dan jangan lupa juga di Dst.Address nya di ganti dengan ip perkompi biar bisa creat dota... terus port yang ada di NAT masukin ke game dotanya..

DIKUMPULKAN KEMBALI OLEH :

Ayom Rahwana

PT. Laxo Global Akses Sidoarjo

SUMBER : Forum Mikrotik Indonesia dan berbagai site referensi di Internet

Terima kasih kepada semua pihak yang telah membantu sehingga koleksi tutorial ini dapat terwujud. Mari kita berbagi untuk kemajuan kita bersama.

© 2009