

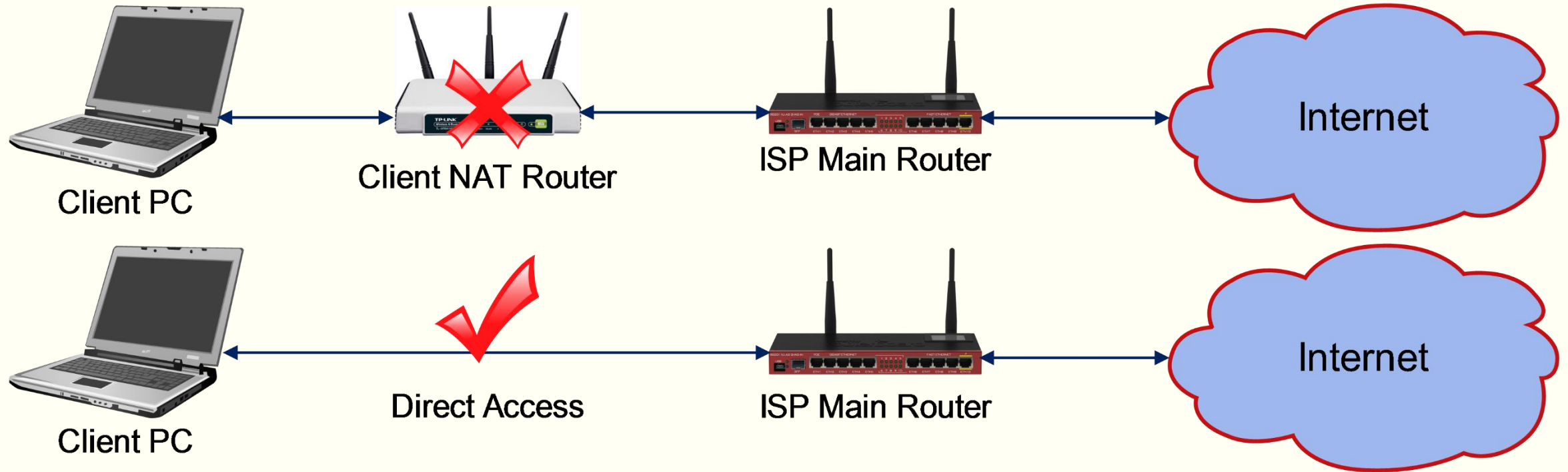


# BLOCKING CLIENT ROUTER ACCESS

By: Haydar Fadel  
May – 24 - 2014



# Theory and Logical Network Diagram



- Many clients in Iraq just buy one user name and password for their internet access and with different methods of access like PPPoE and Hotspot .
- But they share this small bandwidth among many users inside home or office i.e SOHO network.
- And other case many internet cafe or internet centers bought two or more credentials and merge them or load balance between them and provide very slow internet speed to their client .

# Theory and Logical Network Diagram

---

- The idea is how prevent popular router like (TP-Link) and other router login to internet and share it among different users ?
- And must implement this idea with different login methods (PPPoE , Dynamic IP, Static IP ..... ).
- And only accessible method to internet is by connect PC directly to ISP router .
- This can be accomplished by using MikroTik RouterOS and Firewall facilities.



# Implementation (Command Line)

---

---

- In the ISP Main router just add the following command in MikroTik new Terminal .

```
/ip firewall mangle
```

```
add action=change-ttl chain=forward comment="Block Client NAT Router/Haydar" disabled=no in-interface=LAN  
new-ttl=set:1 passthrough=no
```

- Or by using MikroTik WinBox (next pages)



# Implementation (Command Line)

```
Terminal

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

MikroTik RouterOS 6.13 (c) 1999-2014      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

/           Move up to base level
..         Move up one level
/command    Use command at the base level

[admin@Haydar-Router] > ip firewall mangle
[admin@Haydar-Router] /ip firewall mangle> add action=change-ttl chain=forward comment="Block Client NAT Router/Haydar" disabled=no in-interface=ether3 new-ttl=set :1 passthrough=no
[admin@Haydar-Router] /ip firewall mangle>
```

# Implementation (WinBox)

Mangle Rule <>

General | Advanced | Extra | Action | Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

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

enabled

Mangle Rule <>

General | Advanced | Extra | Action | Statistics

Action:

TTL Action  
 change  increment  decrement

New TTL:

Passthrough

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

enabled

# Implementation (WinBox)

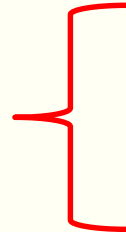
The screenshot shows the WinBox Firewall configuration interface. The window title is "Firewall". The tabs at the top are "Filter Rules", "NAT", "Mangle", "Service Ports", "Connections", "Address Lists", and "Layer7 Protocols". The "Filter Rules" tab is active. Below the tabs are several control buttons: a plus sign, a minus sign, a checkmark, a cross, a folder icon, a funnel icon, "00 Reset Counters", and "00 Reset All Counters". There is also a search field with the text "Find" and a dropdown menu with "all".

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
::: Block Client NAT Router/Haydar											
0	✓ cha...	forward						ether3		0 B	0

At the bottom of the window, it says "1 item (1 selected)".

# Verification

Before adding rule in Main ISP Router



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Haydar>ping 5.10.227.18

Pinging 5.10.227.18 with 32 bytes of data:
Reply from 5.10.227.18: bytes=32 time=45ms TTL=124
Reply from 5.10.227.18: bytes=32 time=97ms TTL=124
Reply from 5.10.227.18: bytes=32 time=39ms TTL=124
Reply from 5.10.227.18: bytes=32 time=33ms TTL=124

Ping statistics for 5.10.227.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 33ms, Maximum = 97ms, Average = 53ms

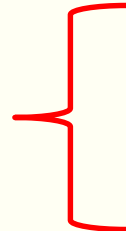
C:\Users\Haydar>ping 5.10.227.18

Pinging 5.10.227.18 with 32 bytes of data:
Reply from 5.10.227.193: TTL expired in transit.
Reply from 5.10.227.193: TTL expired in transit.
Reply from 5.10.227.193: TTL expired in transit.
Reply from 5.10.227.193: TTL expired in transit.

Ping statistics for 5.10.227.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Haydar>
```

After adding rule in Main ISP Router





# Verification

Before adding rule in Main ISP Router

After adding rule in Main ISP Router

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

MikroTik RouterOS 6.13 (c) 1999-2014      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

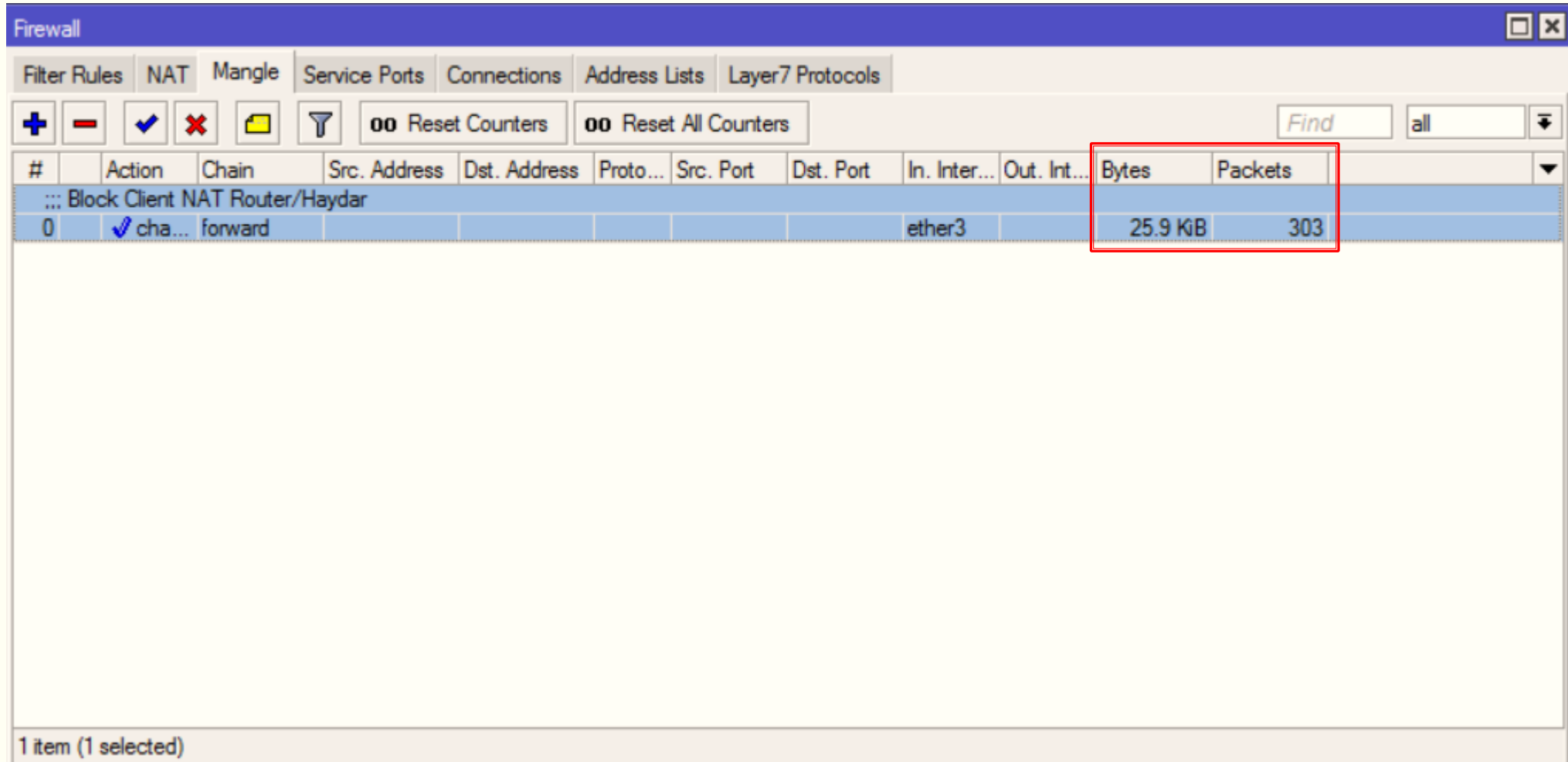
/           Move up to base level
..         Move up one level
/command   Use command at the base level

[admin@NAT/Router] > ping 5.10.227.18
HOST
5.10.227.18      SIZE TTL TIME  STATUS
5.10.227.18      56 125 51ms
5.10.227.18      56 125 133ms
5.10.227.18      56 125 43ms
5.10.227.18      56 125 46ms
5.10.227.18      56 125 34ms
sent=5 received=5 packet-loss=0% min-rtt=34ms avg-rtt=61ms max-rtt=133ms

[admin@NAT/Router] > ping 5.10.227.18
HOST
5.10.227.193    SIZE TTL TIME  STATUS
5.10.227.193    84  63 6ms   TTL exceeded
5.10.227.193    84  63 44ms  TTL exceeded
5.10.227.193    84  63 48ms  TTL exceeded
5.10.227.193    84  63 30ms  TTL exceeded
sent=4 received=0 packet-loss=100%

[admin@NAT/Router] >
```

# Verification in ISP Main Router



The screenshot shows the Mikrotik WinBox Firewall configuration window. The 'Filter Rules' tab is active. A table of firewall rules is displayed, with the first rule selected. The 'Bytes' and 'Packets' columns for this rule are highlighted with a red box.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
... Block Client NAT Router/Haydar											
0	✓ cha...	forward						ether3		25.9 KiB	303

1 item (1 selected)

THE END

Source : <https://aacable.wordpress.com/2014/03/07/blocking-client-router-access/>

