Routerboard Security

Barry Higgins
Allness IT

UK MuM 2018

Who am I?

- Barry Higgins
- Made a living from I.T. since 1996
- Started a WISP in 2009
- MikroTik consultant since 2015
- Independent UK MikroTik Trainer since 2016

- I am not a security expert
- I repeat I am not a security expert

The importance of security

The importance of Security

Why do we need to have our Routerboards secure?

Because ?

- *Audience participation.. (yeah sure, like that'll happen !)*
- *By the way, feel free to ask questions during the presentation. I'll do my best to answer there and then rather waiting till the end.*

The importance of Security

- We don’t want to be part of an attack!
- We don’t want to share all our secrets!

The importance of Security

So what do we do?

Which option to go with...

Factory Default

Or

Bespoke?

Lets start with…

Factory Default?

Factory Default

DO NOT connect your router to the internet until you have done at least the following:

1) Created an admin user Password

2) Disabled services

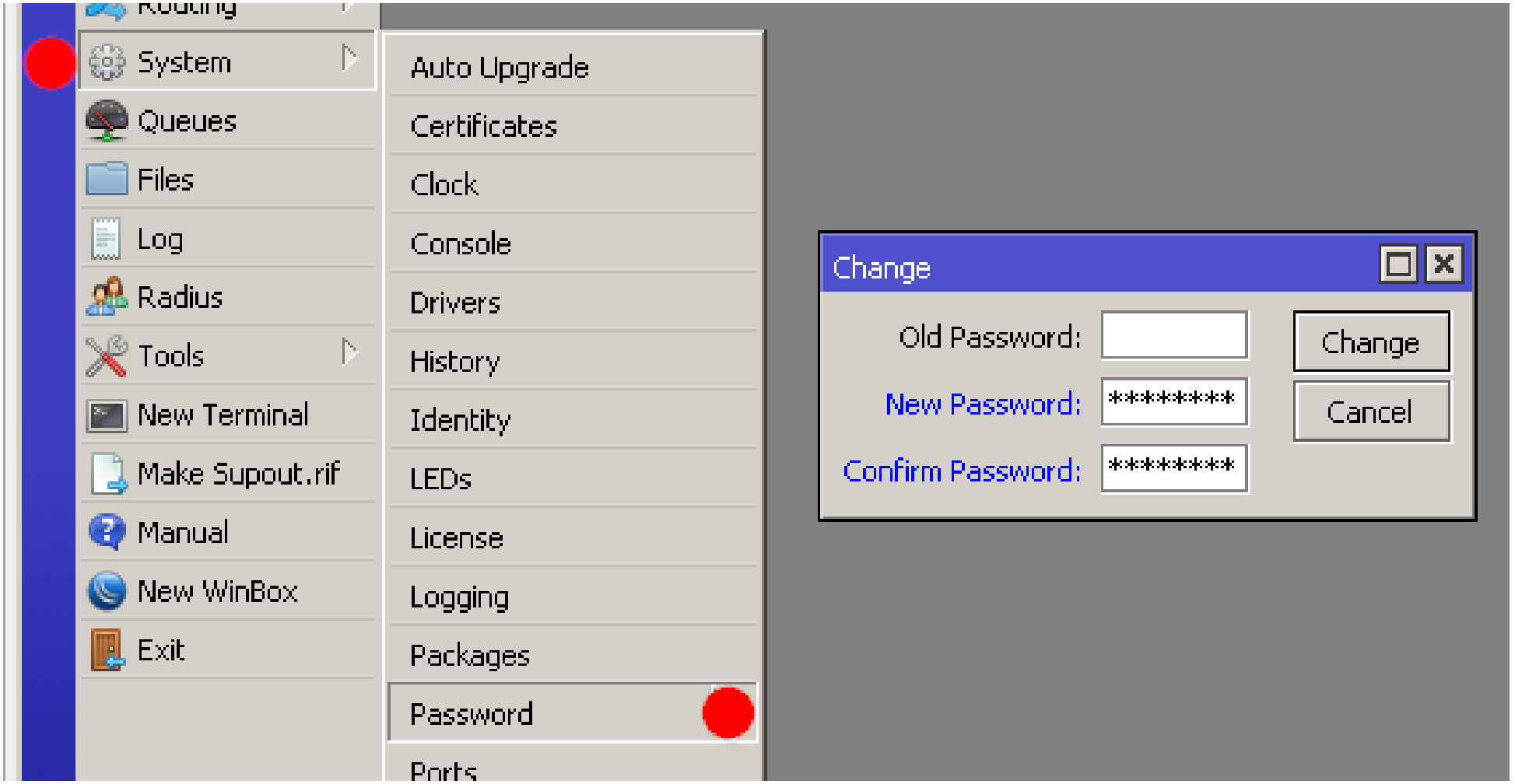
3) Updated RouterOS to the latest ‘Stable’ or ‘Long Term’ version

Factory Default

Step 1..

Set an admin user password!

Factory Default



Factory Default

Terminal/CLI..

```
[admin@MikroTik] > /password
Old-password:
New-password: ************
confirm-new-password: ************
```

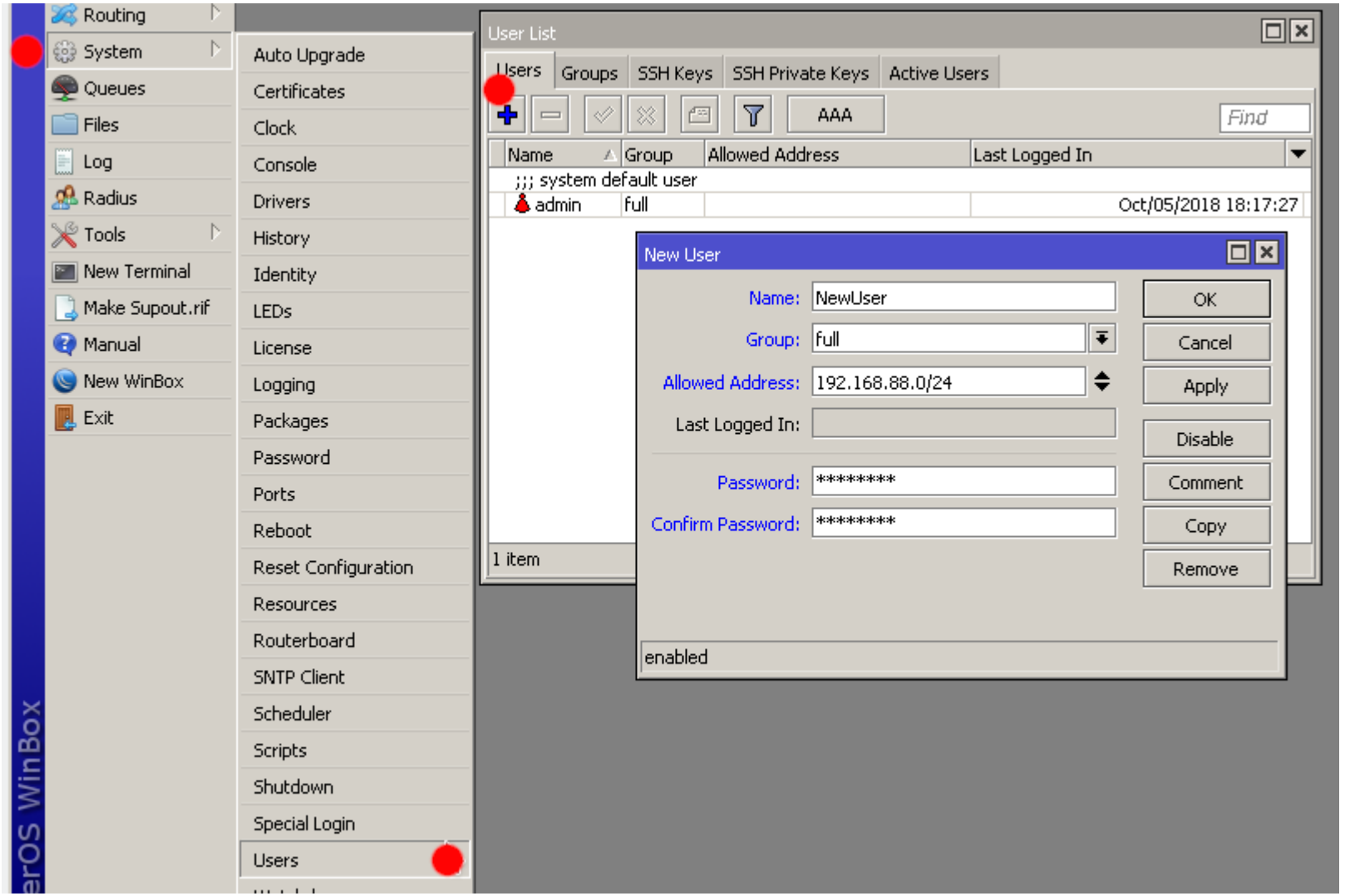
Factory Default

Lets go one stage better..

Create a new user with a password.

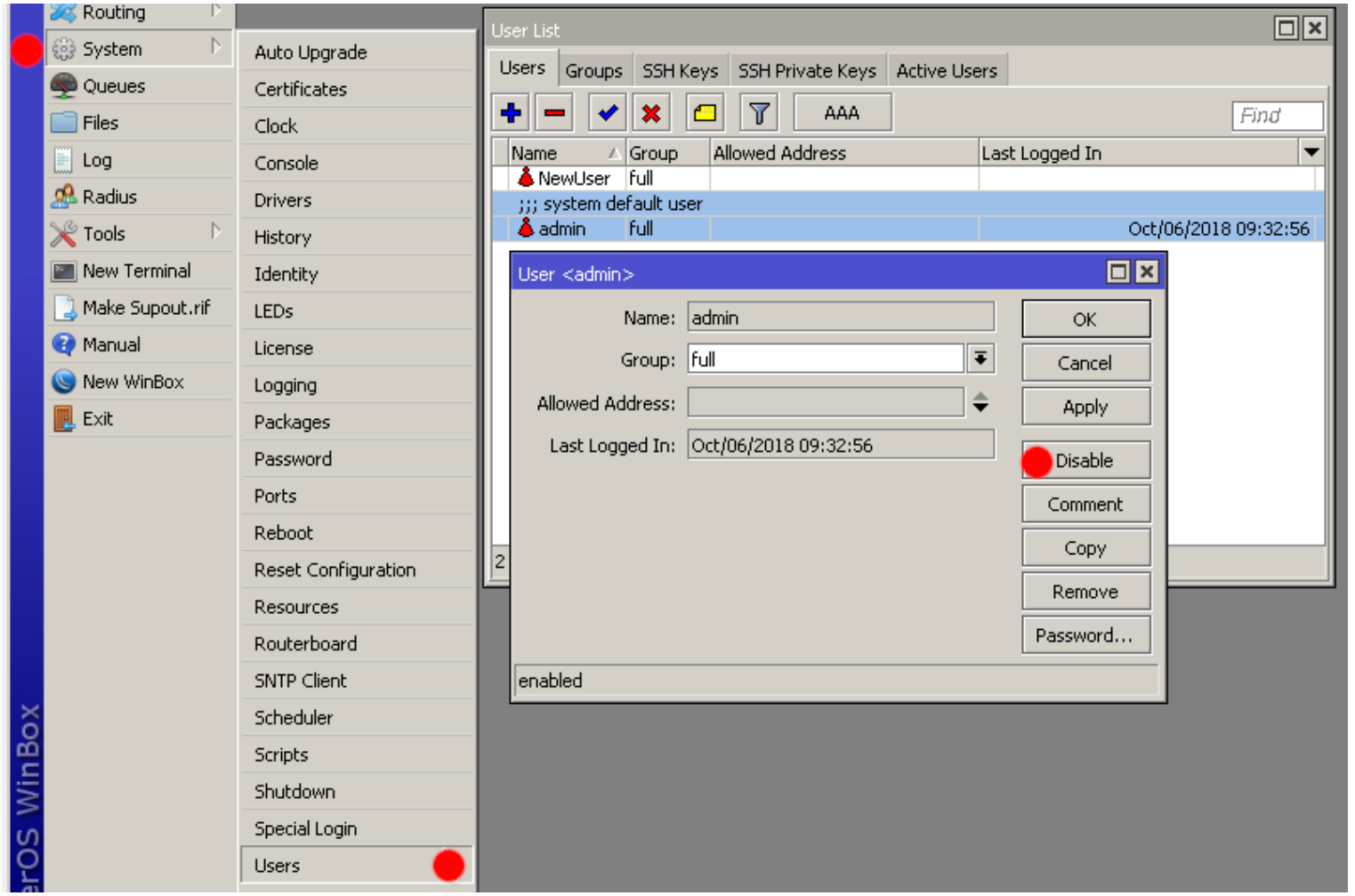
Then disable the default admin account.

Factory Default – new user



Factory Default

Logout user 'admin' and login with 'NewUser' to disable the admin account



Factory Default

Terminal/CLI..

```
[admin@MikroTik] > /user add \
name=NewUser group=full \
Password="********" \
Address=192.168.88.0/24

Now logout ‘admin’ and login as ‘NewUser’

[NewUser@MikroTik] > /user disable admin
```

Factory Default

Why? ..

.. because you have now created 2 unknowns that have to be acquired before logging in plus removing a partially known login.

Factory Default

Also note..

Adding an allowed address range has reduced the risk of unwanted logins from other networks.

Factory Default

For now that covers the more serious points that the factory default doesn't do for you.

However….

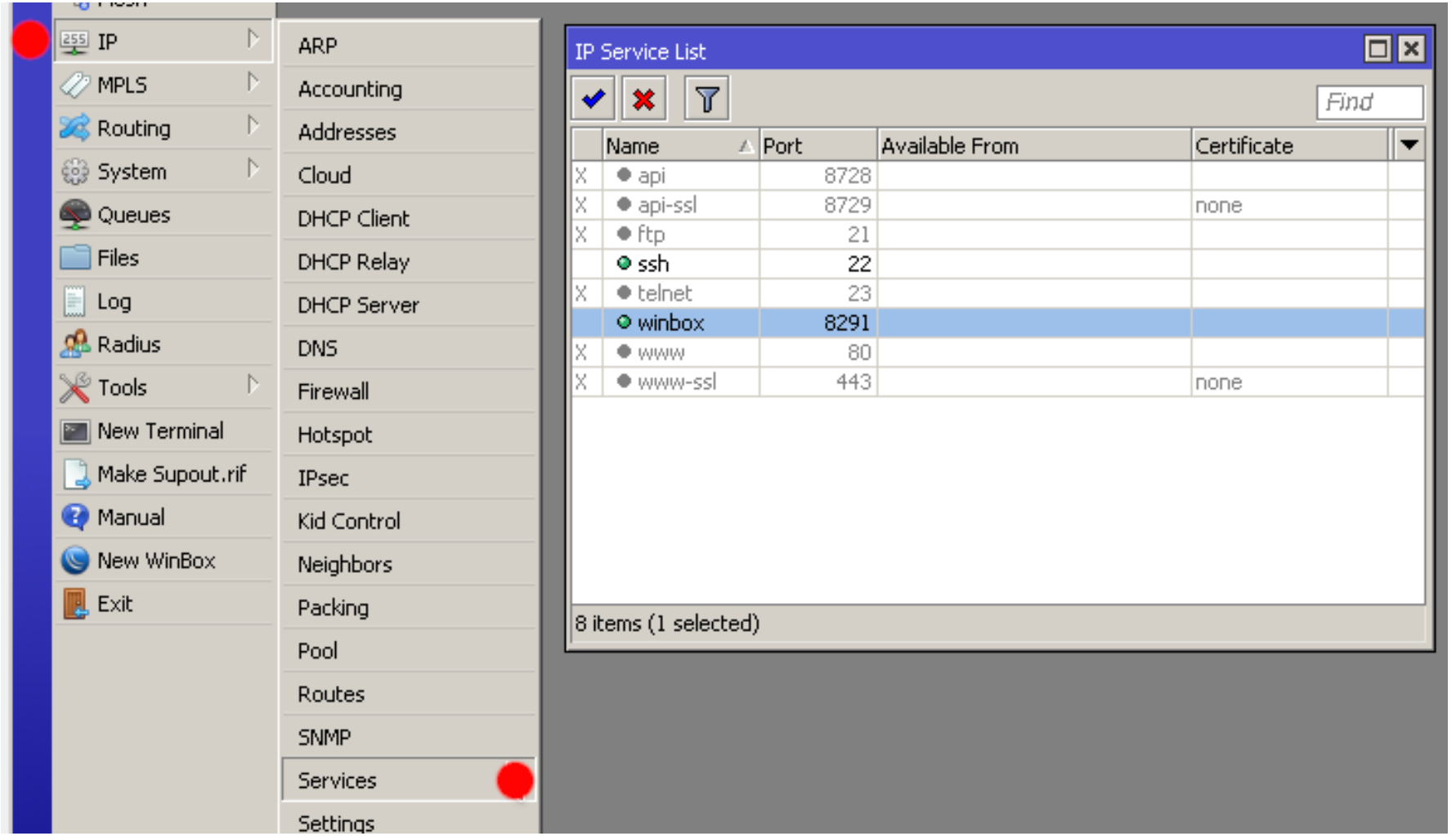
Factory Default

Consider these points if you really insist on using factory default..

/IP Services

Telnet API FTP Winbox SSH are all enabled LAN side

Factory Default – IP Services



Factory Default – IP Services

```
[NewUser@MikroTik] > /ip service disable telnet,ftp,www, \
 www-ssl,api,api-ssl

[NewUser@MikroTik] > /ip service print
Flags: X - disabled, I - invalid
 #   NAME                 PORT ADDRESS          CERTIFICATE

 0 XI telnet                 23
 1 XI ftp                    21
 2 XI www                    80
 3    ssh                    22
 4 XI www-ssl               443                  none

 5 XI api                  8728
 6    winbox               8291
 7 XI api-ssl              8729                  none
```

Factory Default

At this point we're nearly safe enough to connect to the Interent..

One last bit.

RouterOS update

Factory Default – Update RouterOS

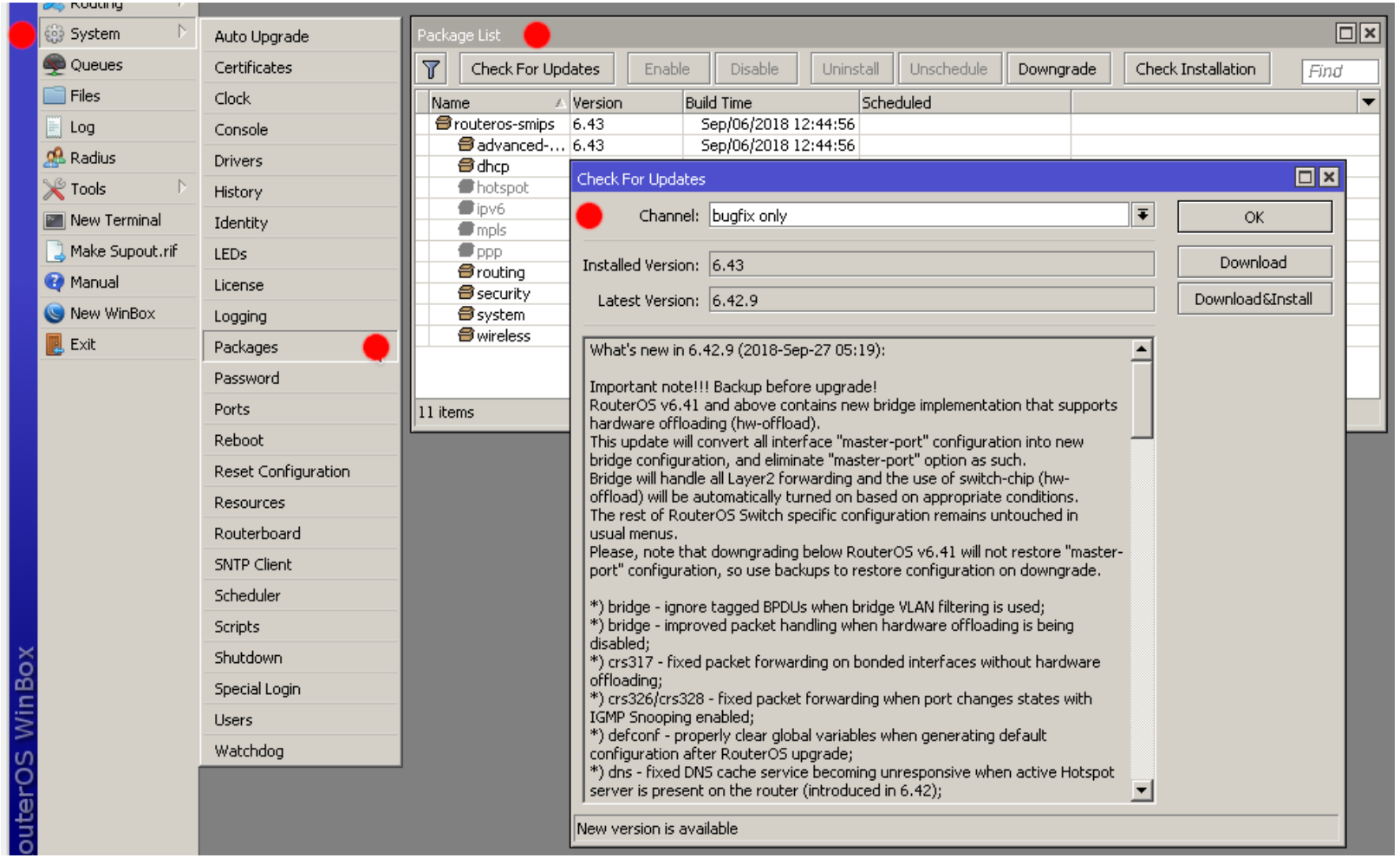
Why should you update RouterOS?

Quite simply it is one way to minimise any legacy exploits.

Update via your preferred method.

- *There is a dilemma at this point.. connect to the internet and risk a / system package update or less risky methods of downloading via an alternative device and then uploading the update to the router.*

Factory Default – Update RouterOS



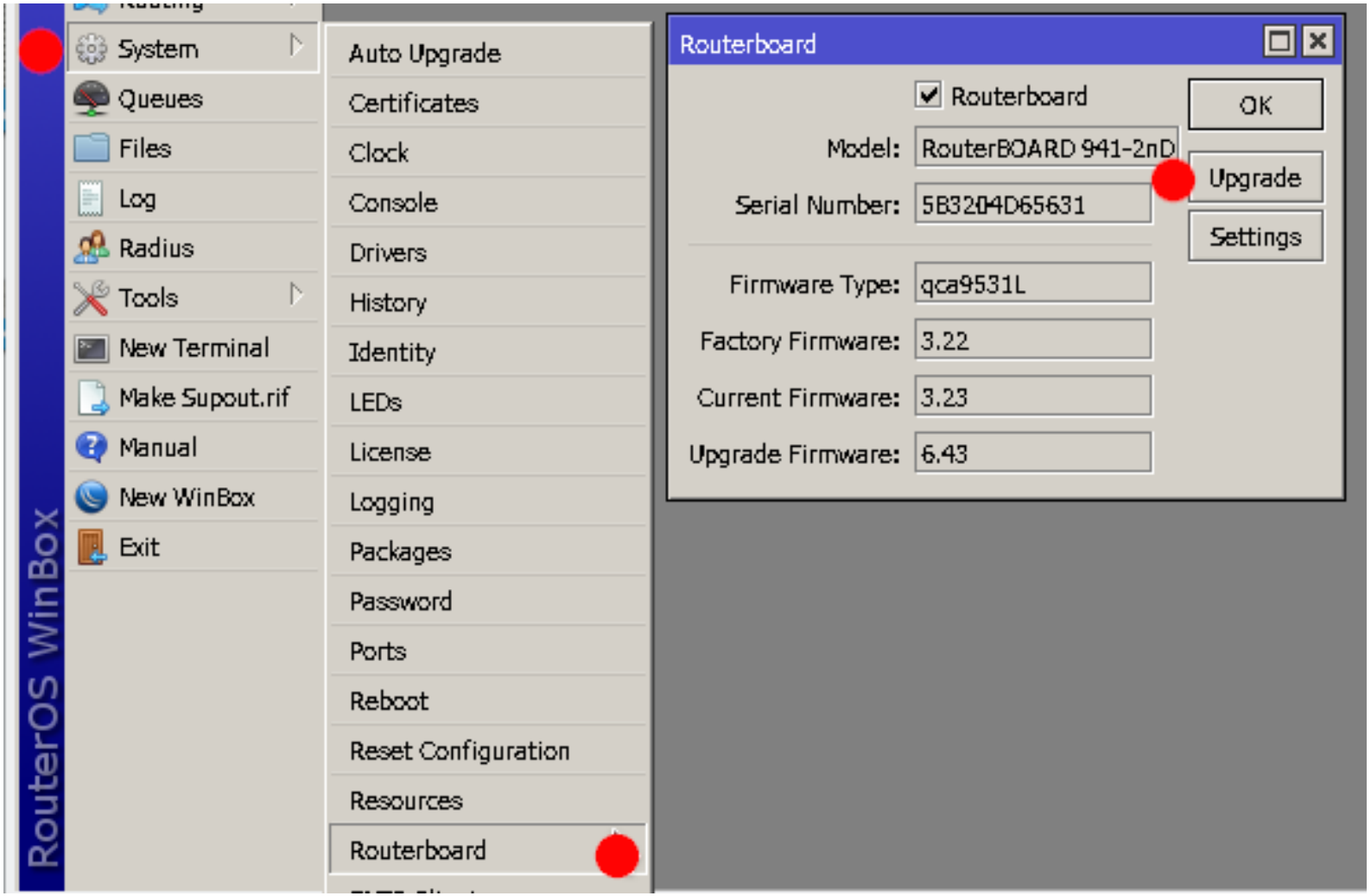
Factory Default – Update RouterOS

```
[NewUser@MikroTik] > /system package update set \
 channel=bugfix
[NewUser@MikroTik] > /system package update print
              channel: bugfix
  installed-version: 6.43
     Latest-version: 6.42.9
[NewUser@MikroTik] > /system package update install
```

Factroy Default

Don’t forget to update routerboot too!

Factory Default - Routerboot



Factory Default - Routerboot

```
[NewUser@MikroTik] > /system routerboard print
        routerboard: yes
              model: RouterBOARD 941-2nD
      serial-number: 5B3204D65631
      firmware-type: qca9531L
  factory-firmware: 3.22
  current-firmware: 3.23
  upgrade-firmware: 6.43
[NewUser@MikroTik] > /system routerboard upgrade
```

Routerboard Security

That’s it.

Thank you for listening

Factory Default

No wait...

There’s more!

Factory Default

Do you trust the LAN side?

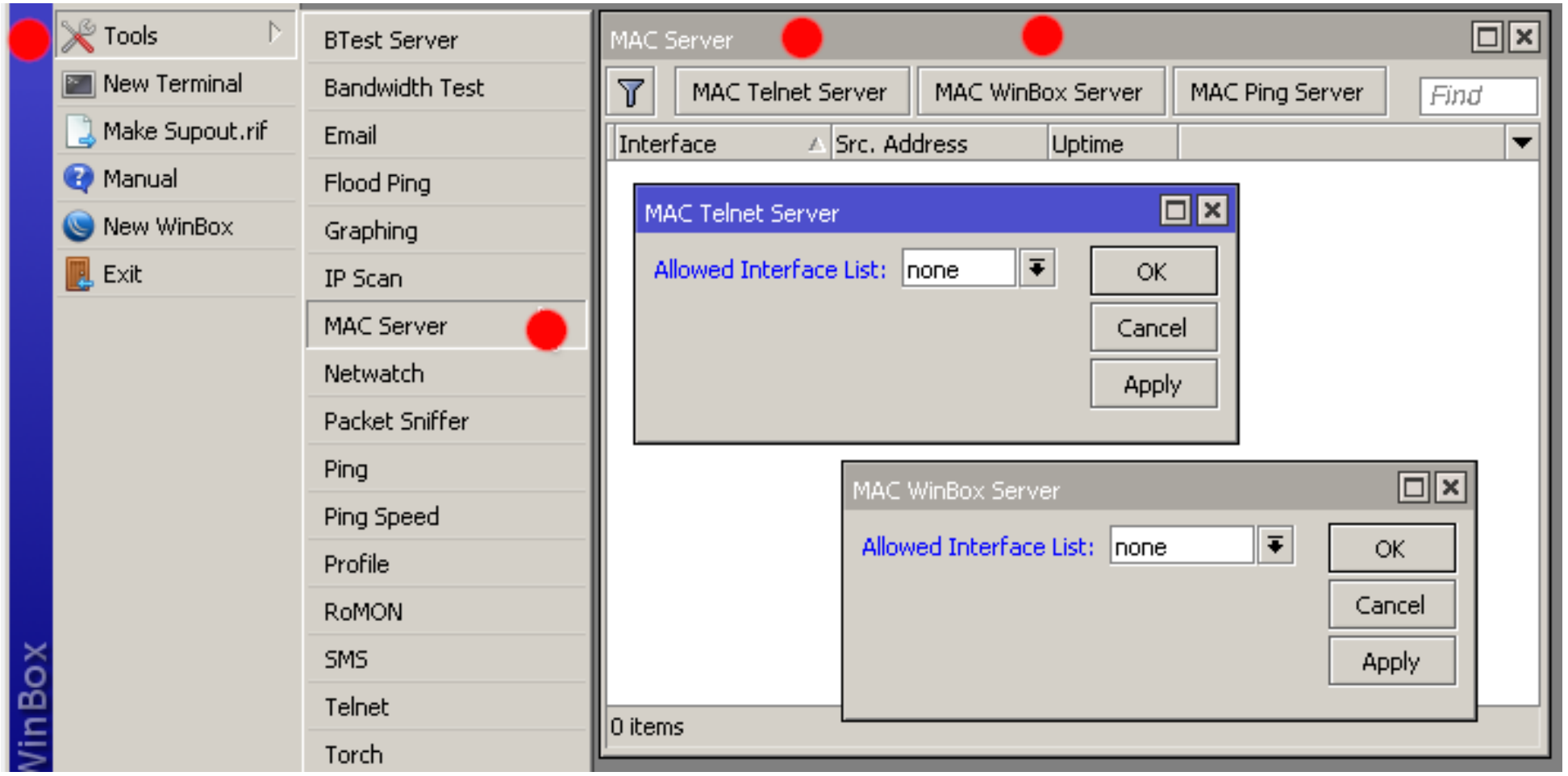
- *MAC servers*
- *Neighbo(u)r Discovery*
- *Active empty ethernet ports*
- */tool BTest server*

Factory Default – MAC servers

Why disable the MAC Servers?

The MAC servers enable connections over layer 2 via either mac-telnet or mac-winbox. Disable if you do not want them active.

Factory Default – MAC servers



Factory Default – MAC servers

```
[NewUser@MikroTik] > /tool mac-server set \
 allowed-interface-list=none

[NewUser@MikroTik] > /tool mac-server mac-winbox set \
 allowed-interface-list=none
```

Factory Default – Neighbor Discovery

Why disable the Neighbour Discovery?

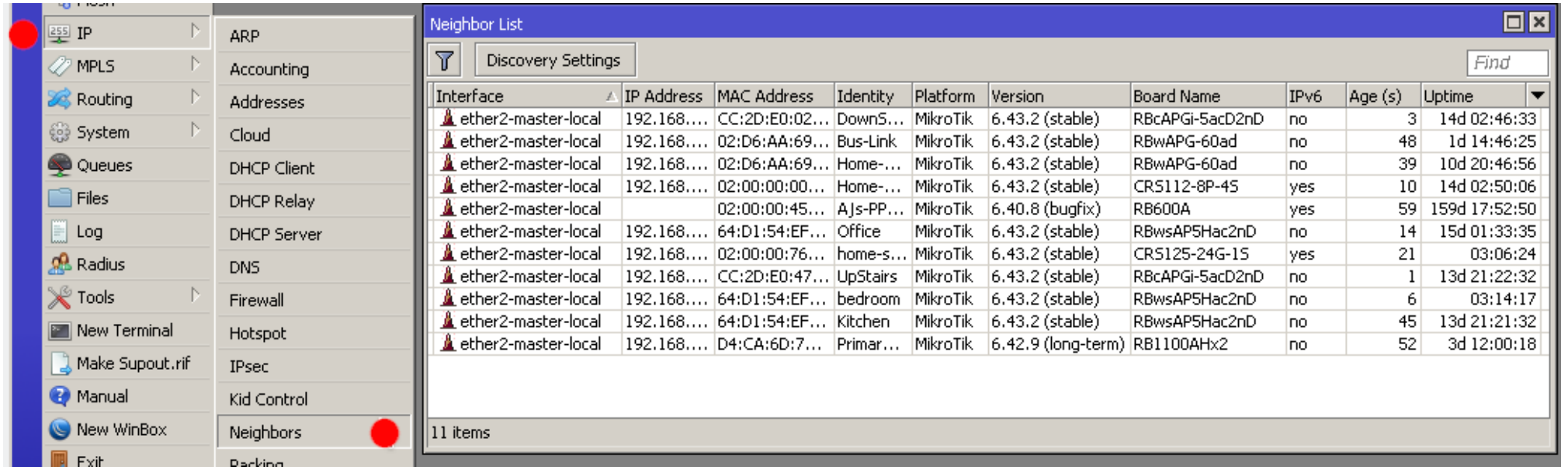
Neighbor Discovery allows your router to be seen by other devices and information of those devices seen by your device.

Neighbor Discovery Protocol (NDP)

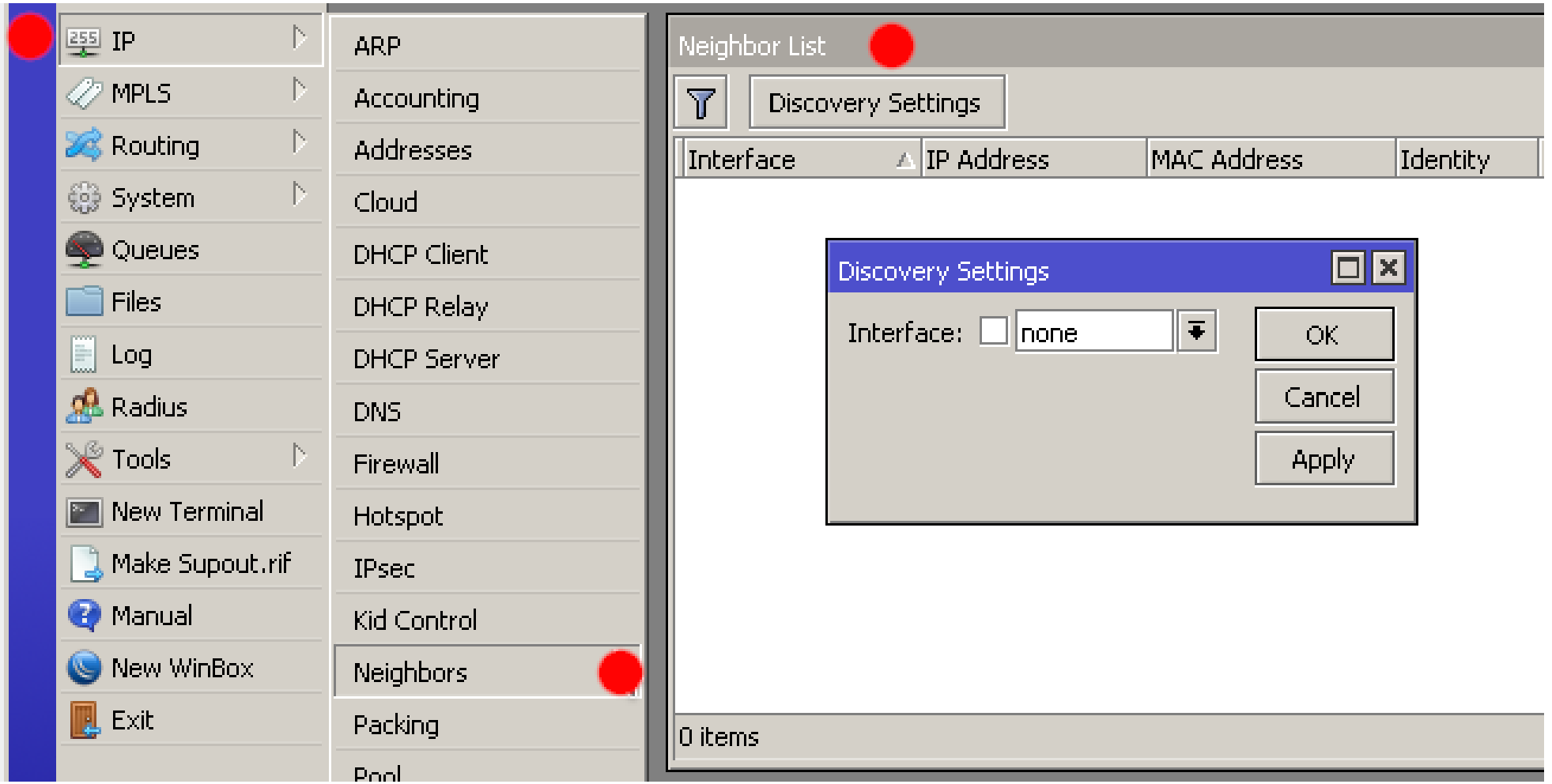
Cisco Discovery Protocol (CDP)

Neighbor Discovery

Information seen..



Factory Default – Neighbor Discovery



Factory Default – Neighbor Discovery

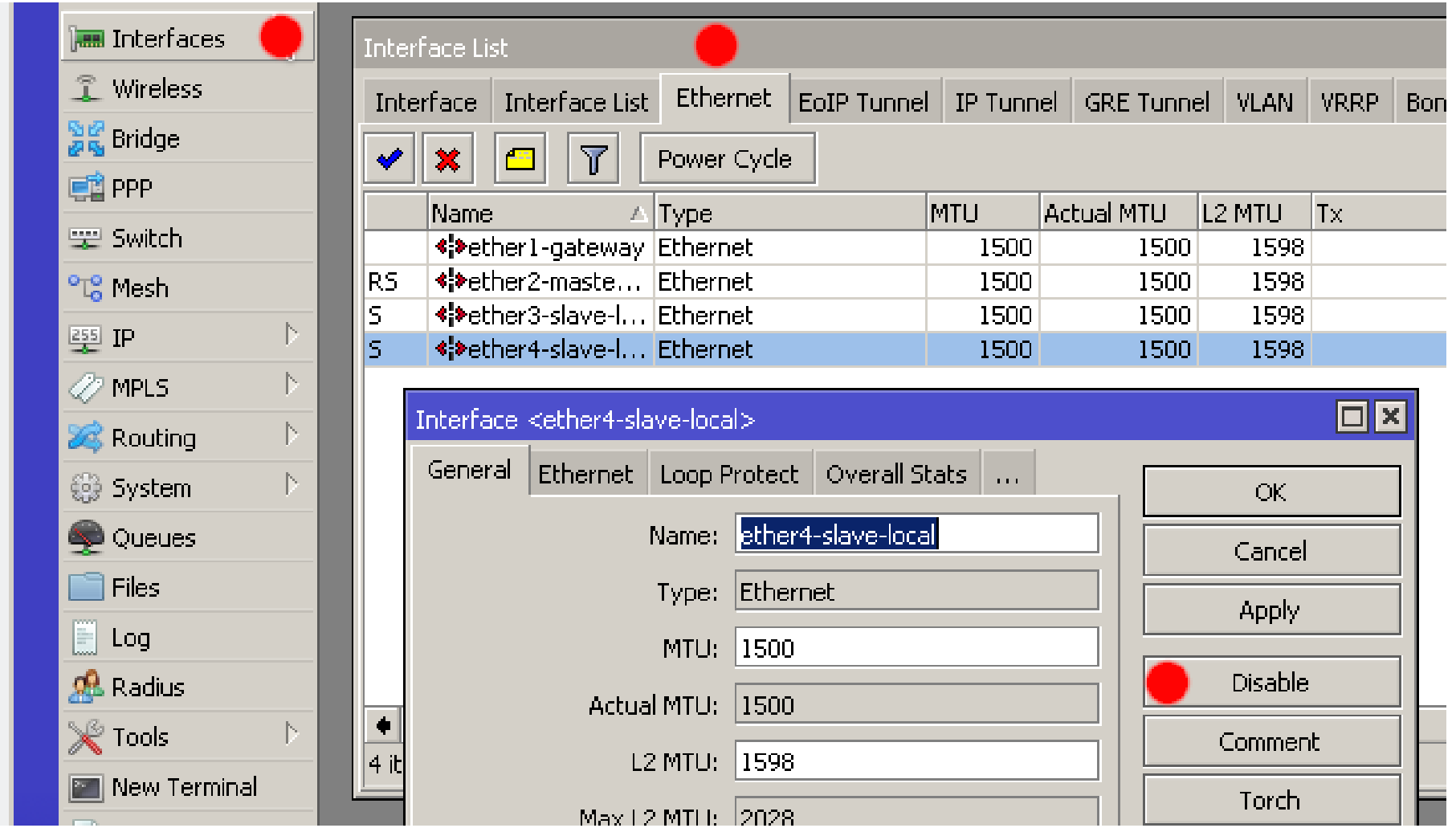
```
[NewUser@MikroTik] > /ip neighbor discovery-settings \
  set discover-interface-list=none
```

Factory Default – Disable ports

Why disable unused ports?

Disabling unused ethernet/sfp/wireless ports stops any unwanted access being obtained via those ports.

Factory Default – Disable ports



Factory Default – Disable ports

```
[NewUser@MikroTik] > /interface ethernet disable \
 ether4-slave-local
```

Factory Default - Wireless

On the subject of ports..

Wireless interface :

Its alive and accepting connections!

Factory Default - Wireless

Depending on the model..

The wireless may be open to connection without any password required!

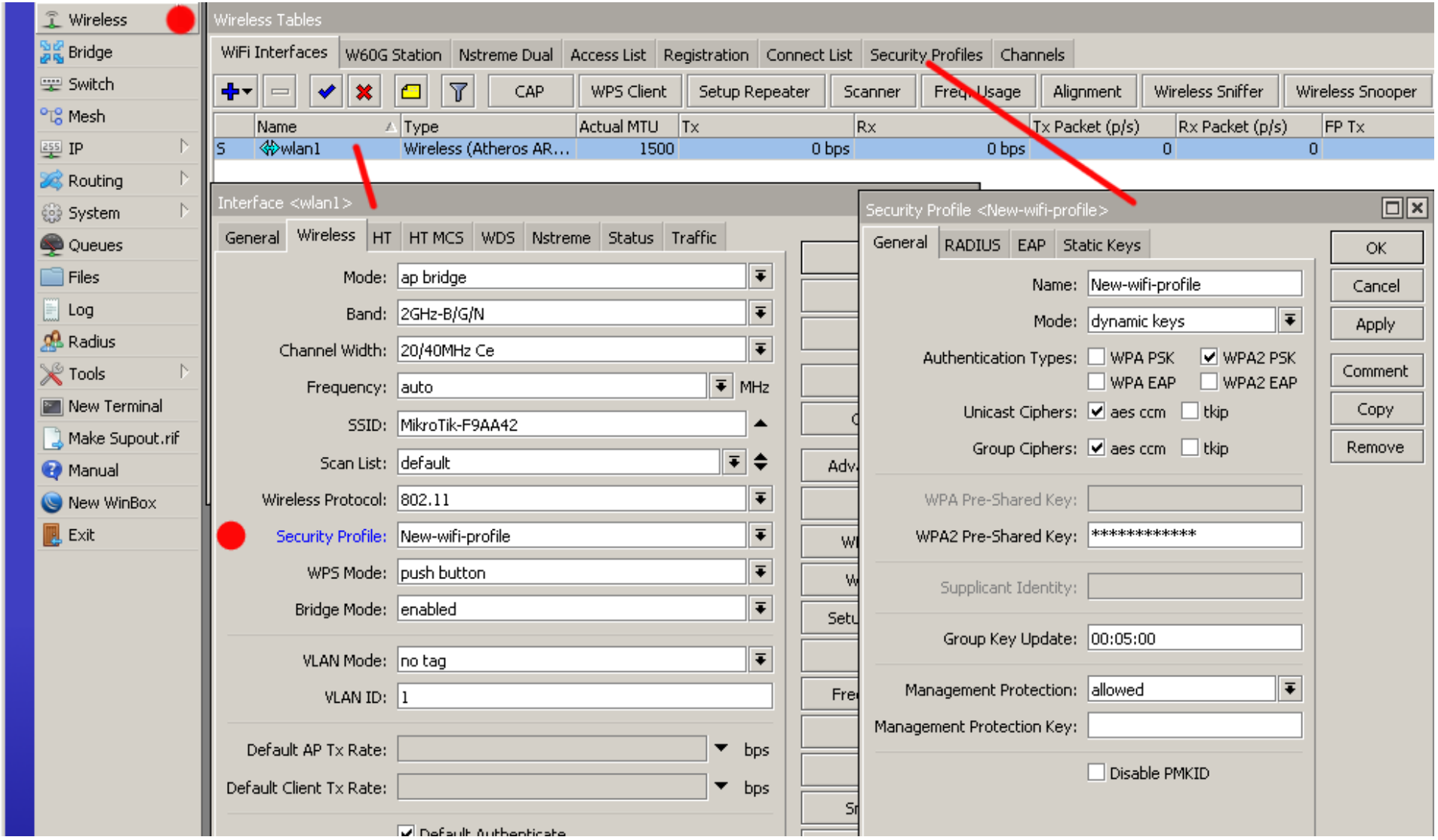
Absolute minimum add a password!

Factory Default - Wireless

How to..

Create a new security profile then assign the profile to all wireless interfaces requiring it.

Factory Default - Wireless



Factory Default - Wireless

```
[NewUser@MikroTik] > /interface wireless security-profiles \
add name=New-wifi-profile mode=dynamic-keys \
authentication-types=wpa2-psk unicast-ciphers=aes-ccm \
group-ciphers=aes-ccm wpa2-pre-shared-key=test1234

[NewUser@MikroTik] > /interface wireless set wlan1 \
security-profile=New-wifi-profile
```

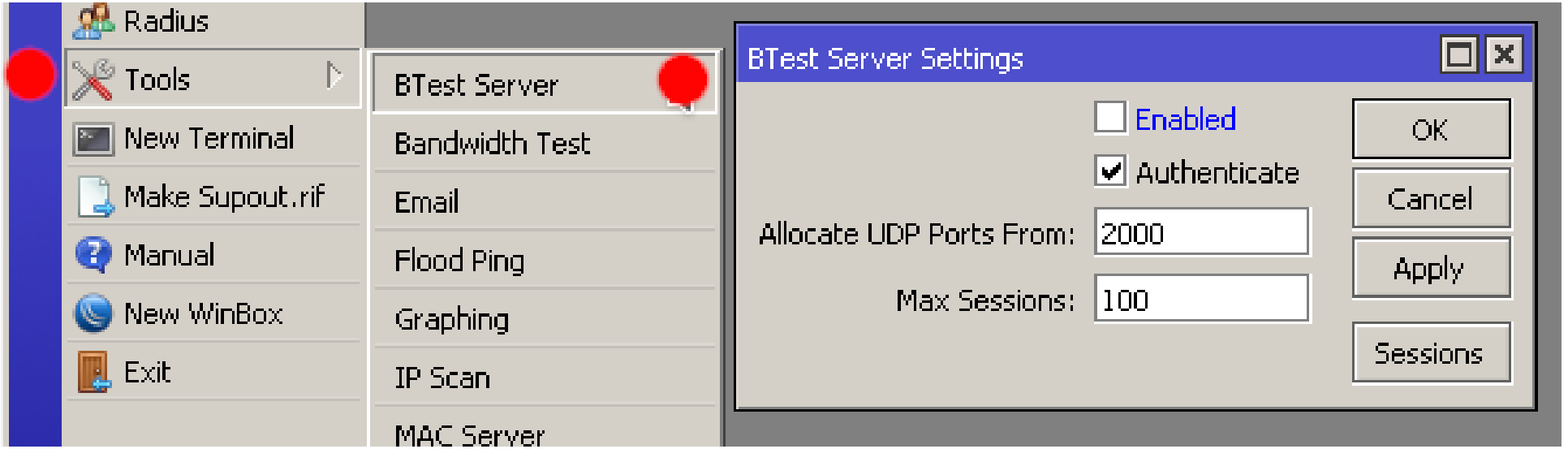
Factory Default – Btest Server

Why disable the Btest Server?

It’s a visible open port should your router be port scanned. (port 2000)

Like moths to a flame it will draw the inquisitive to your router.

Factory Default – Btest Server

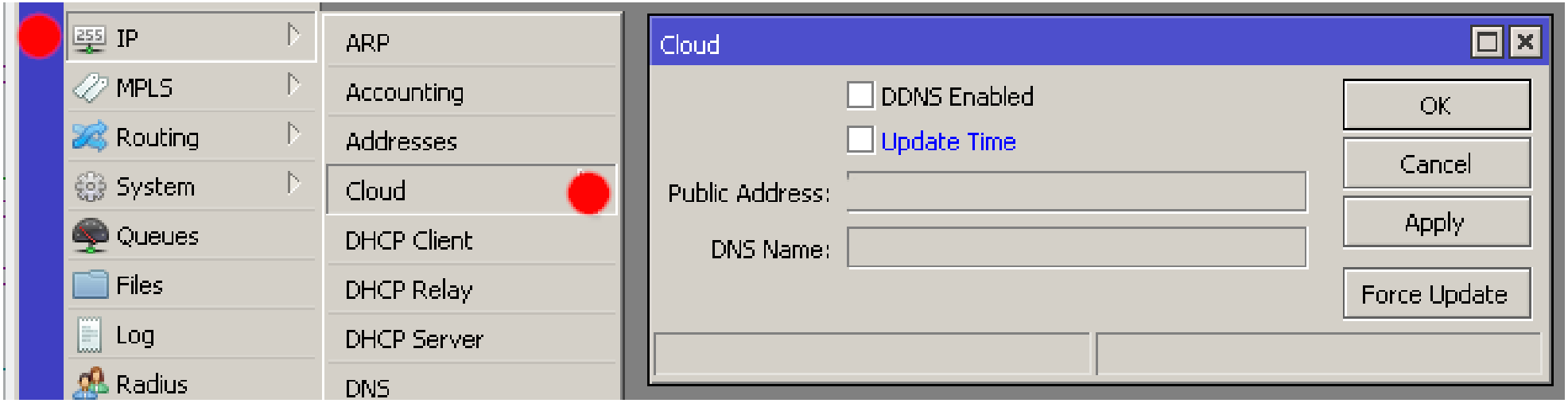



```
[NewUser@MikroTik] > /tool bandwidth-server set \
    enabled=no
```

Factory Default – NTP

Do you trust MikroTik Cloud time update?

Factory Default – NTP

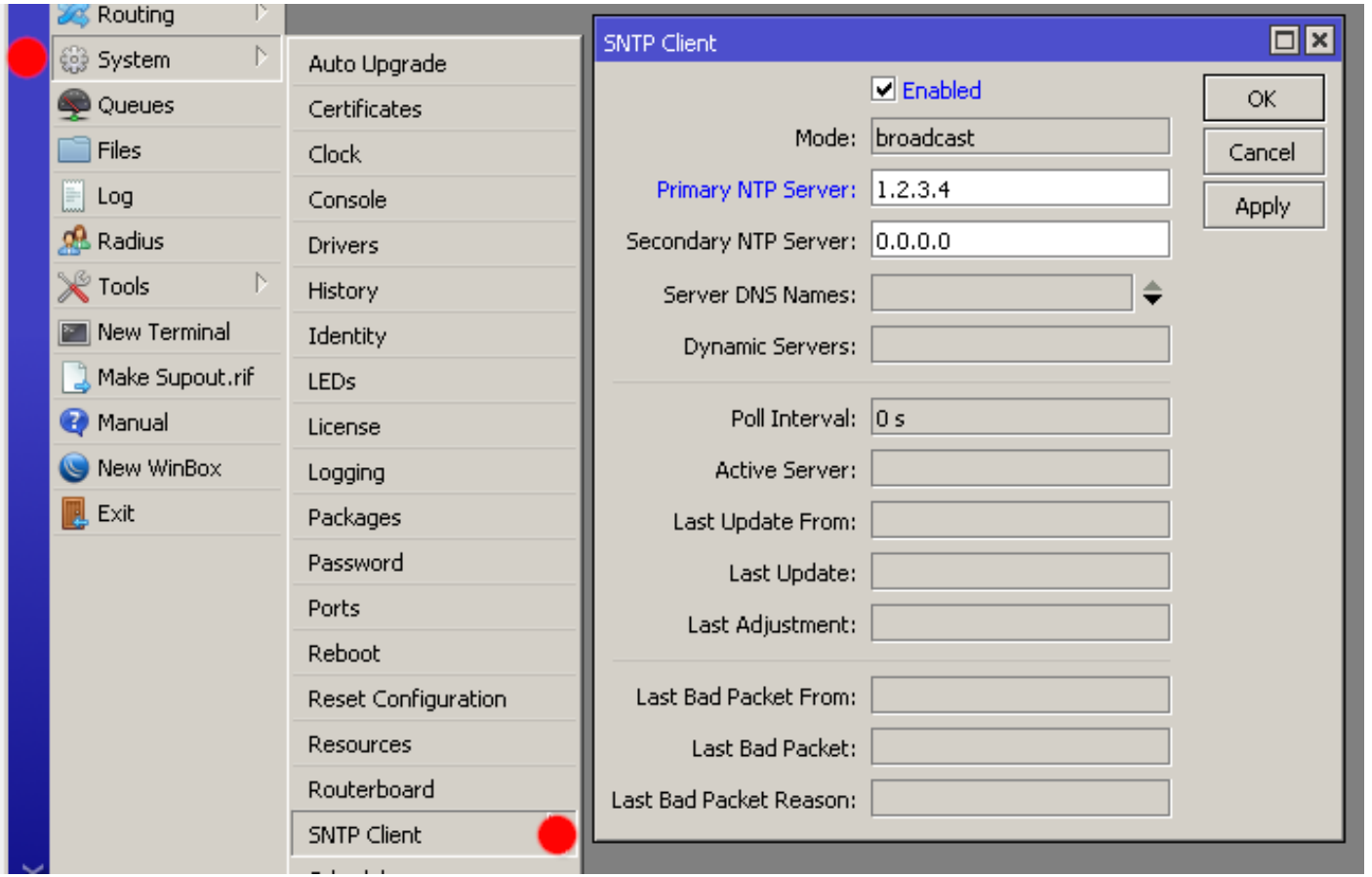



```
[NewUser@MikroTik] > /ip cloud set update-time=no
```

Factory Default - NTP

It might be better to set your own ntp client to a server you are more familiar with.

Factory Default – NTP




```
[NewUser@MikroTik] > /system ntp client set \
 enabled=yes primary-ntp=1.2.3.4
```

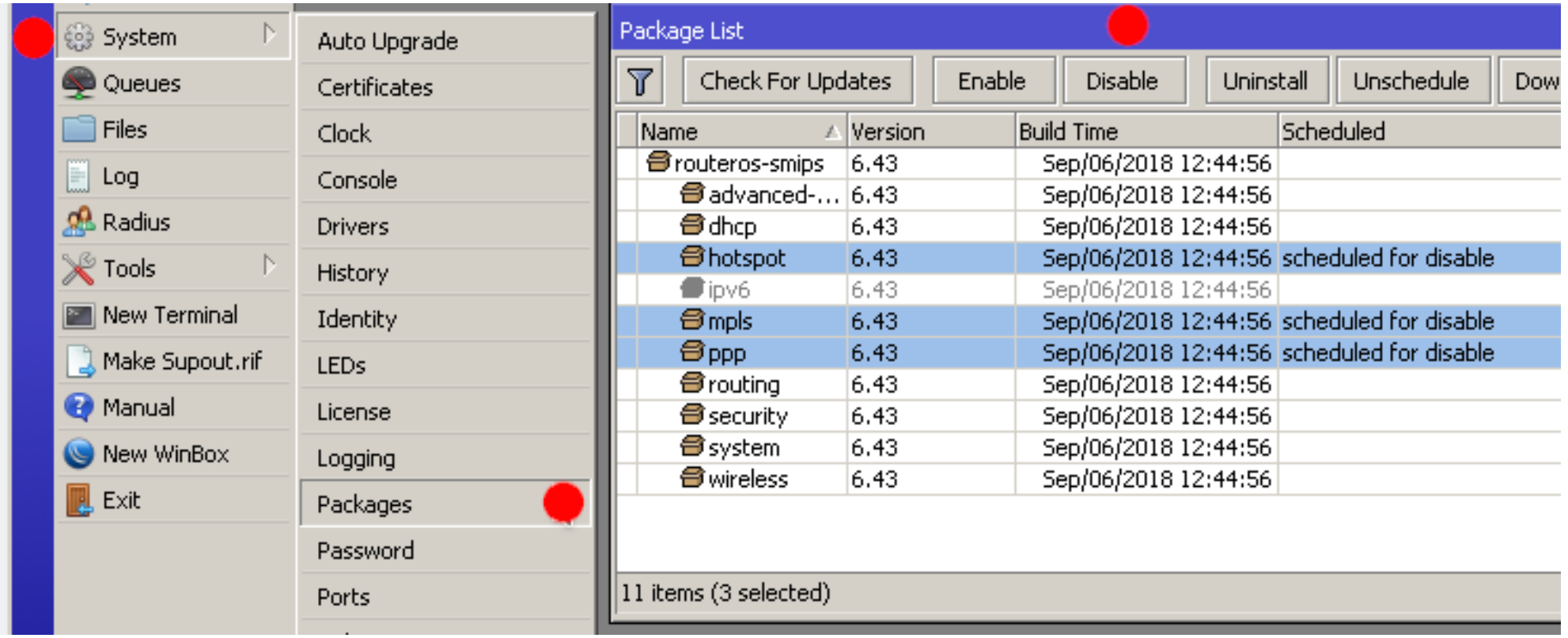
Factory Default - Packages

And finally…

If you want to be really thorough check what packages are running and decide if you really need them to be available.

Hotspot? MPLS? PPP?

Factory Default - Packages




```
[NewUser@MikroTik] > /system package disable \
 hotspot,mpls,ppp
```

Bespoke option

What if you chose not to go with the factory default?

Why?

Bespoke option

Why I personally prefer the bespoke option..

You know what the router has been configured to do!

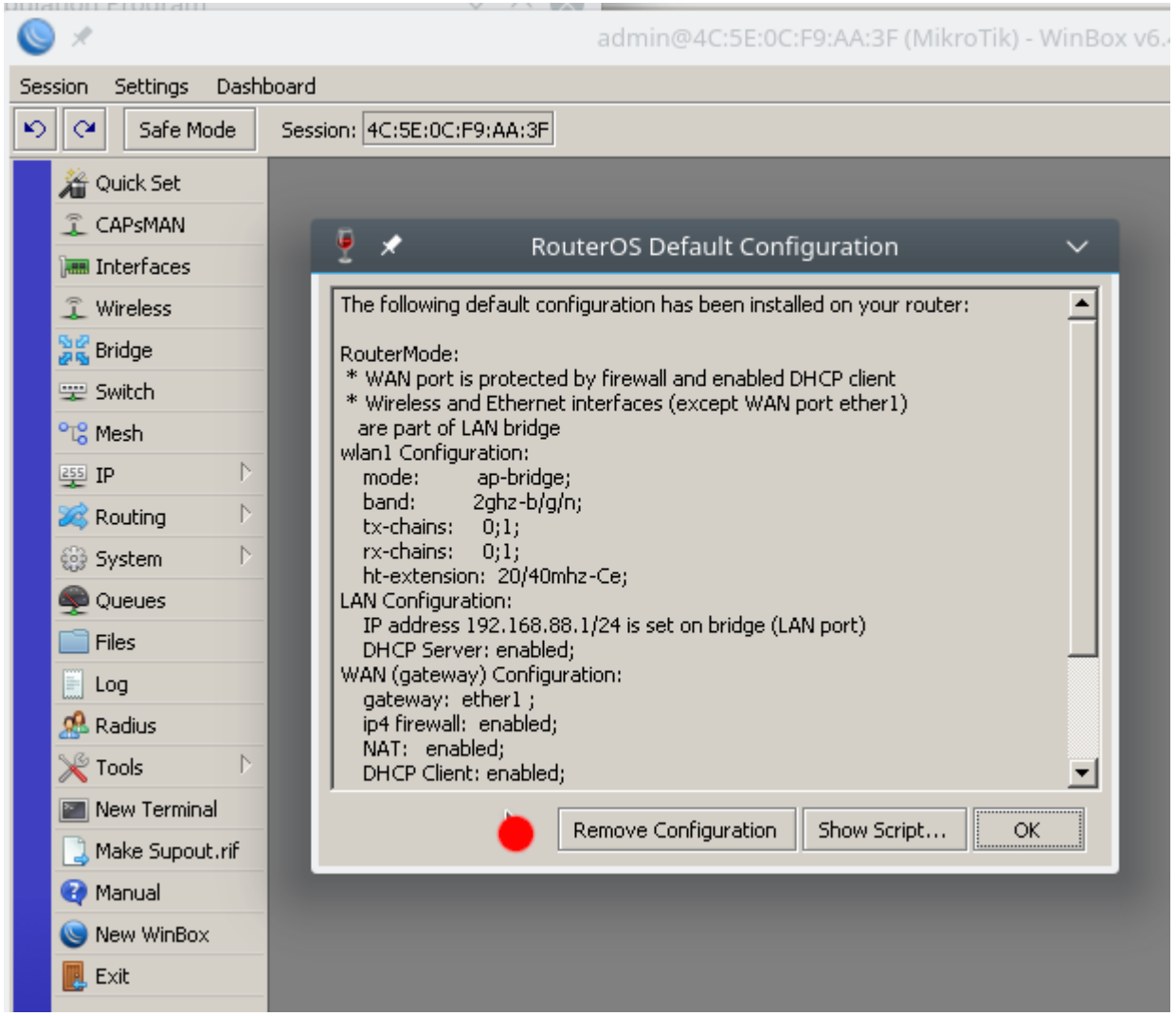
Bespoke option

It’s not for everyone though.

You are better to leave alone with factory defaults if you are unsure what you are doing.

- *Except of course changing at least the password!*
- *plus if you have just woken up please see previous slides!*

Bespoke option



Bespoke option

```
-------------------------------------------------------
You can type "v" to see the exact commands that are
used to add and remove
this default configuration, or you can view them later
with
'/system default-configuration print' command.
To remove this default configuration type "r" or hit
any other key to continue.
If you are connected using the above IP and you remove
it, you will be disconnected.
```

Bespoke option

For the brave or the experienced..

You removed configuration

The router has been cleared of defaults.

Now what?

Bespoke Option

First..

Check the all the security advice in the previous slides regarding ‘Factory default’

Bespoke Option

In brief..

1) New username and password
2) IP Services
3) RouterOS and Routerboot
4) Mac server / Bandwidth Test
5) Packages

Bespoke Option

Now to add the missing bits..

Bespoke Option

The Firewall..

The simplest approach is to add the allowed then block everything else.

Bespoke Option - Firewall

Breaking that down..

Remember the firewall can protect both the router (in/out) and any network available through it.

- Router
  - *Input chain / Output chain*
- Network
  - *Forward chain*

Bespoke Option - Firewall

Input / Output / Forward chain..

- **The sequence is this -**
  - *Allow the packets you want*
  - *Block everything else*

Bespoke Option - Firewall

Allow options..

- **Typically 3 ways to approach this -**
  - *Individual specific rules*
  - *Utilising address lists for grouping networks*
  - *New ‘chains’ combining the above*

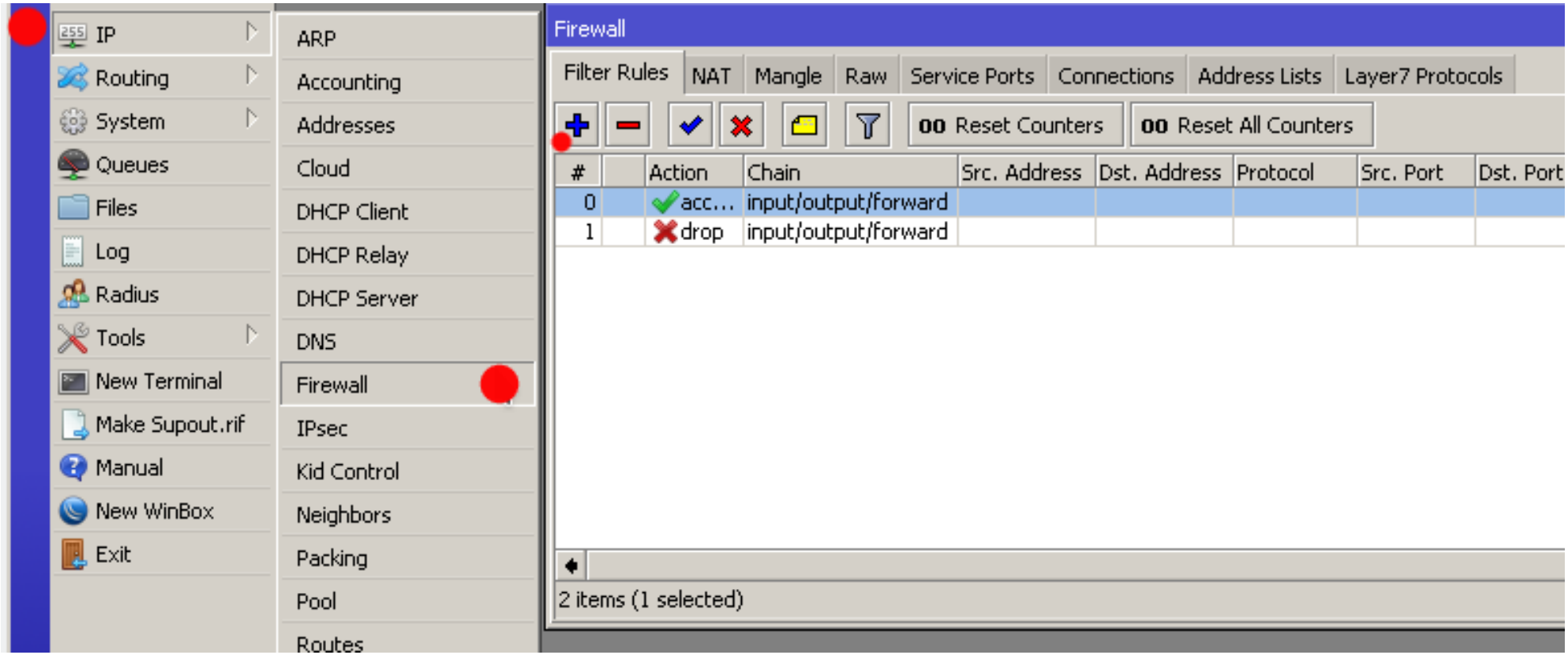
Bespoke Option

N.B the follow examples show a combined ‘input/output/forward’ chain. This is for demonstration purpose only and requires individual ‘input’ ‘output’ and ‘forward’ chains in actual use

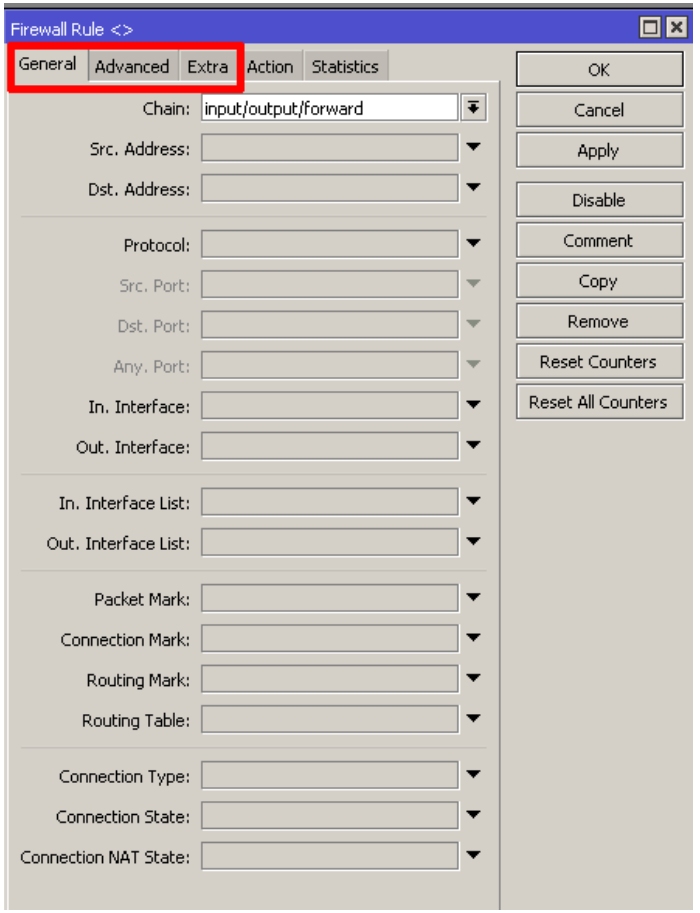
Bespoke Option - Firewall

Individual / specific rules

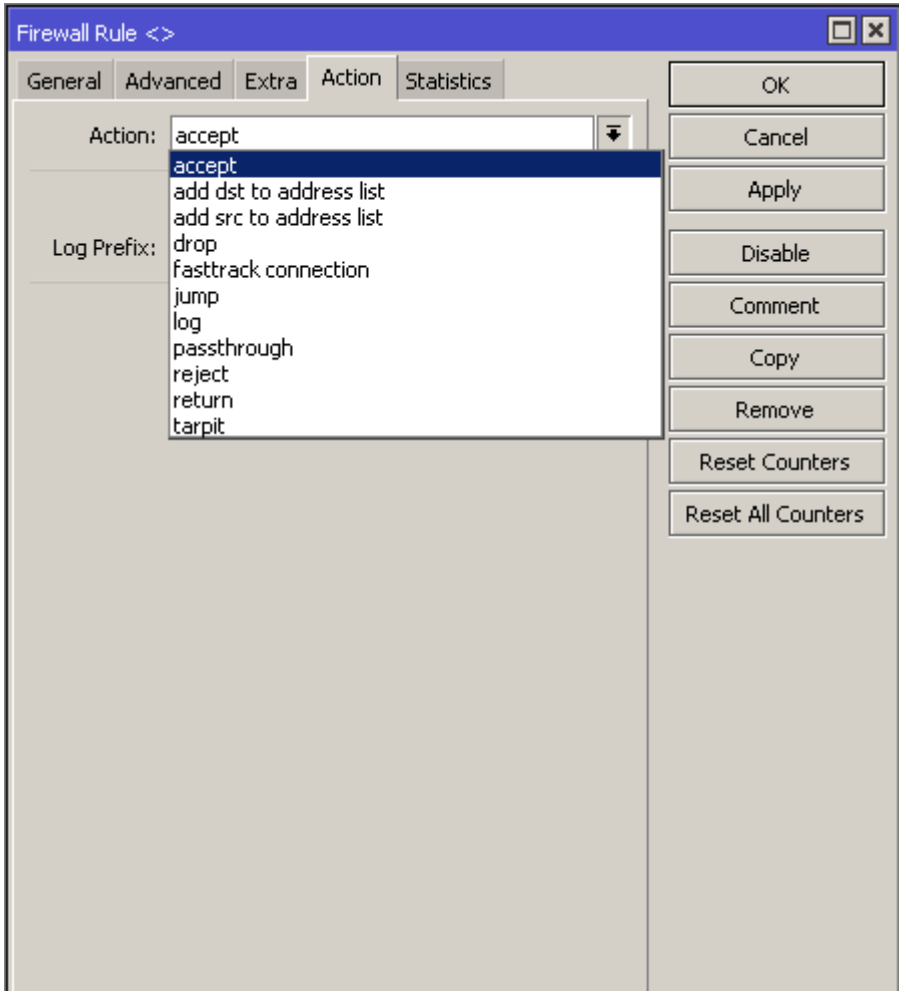
Bespoke Option – Firewall



Bespoke Option – Firewall (matcher)



Bespoke Option – Firewall (action)



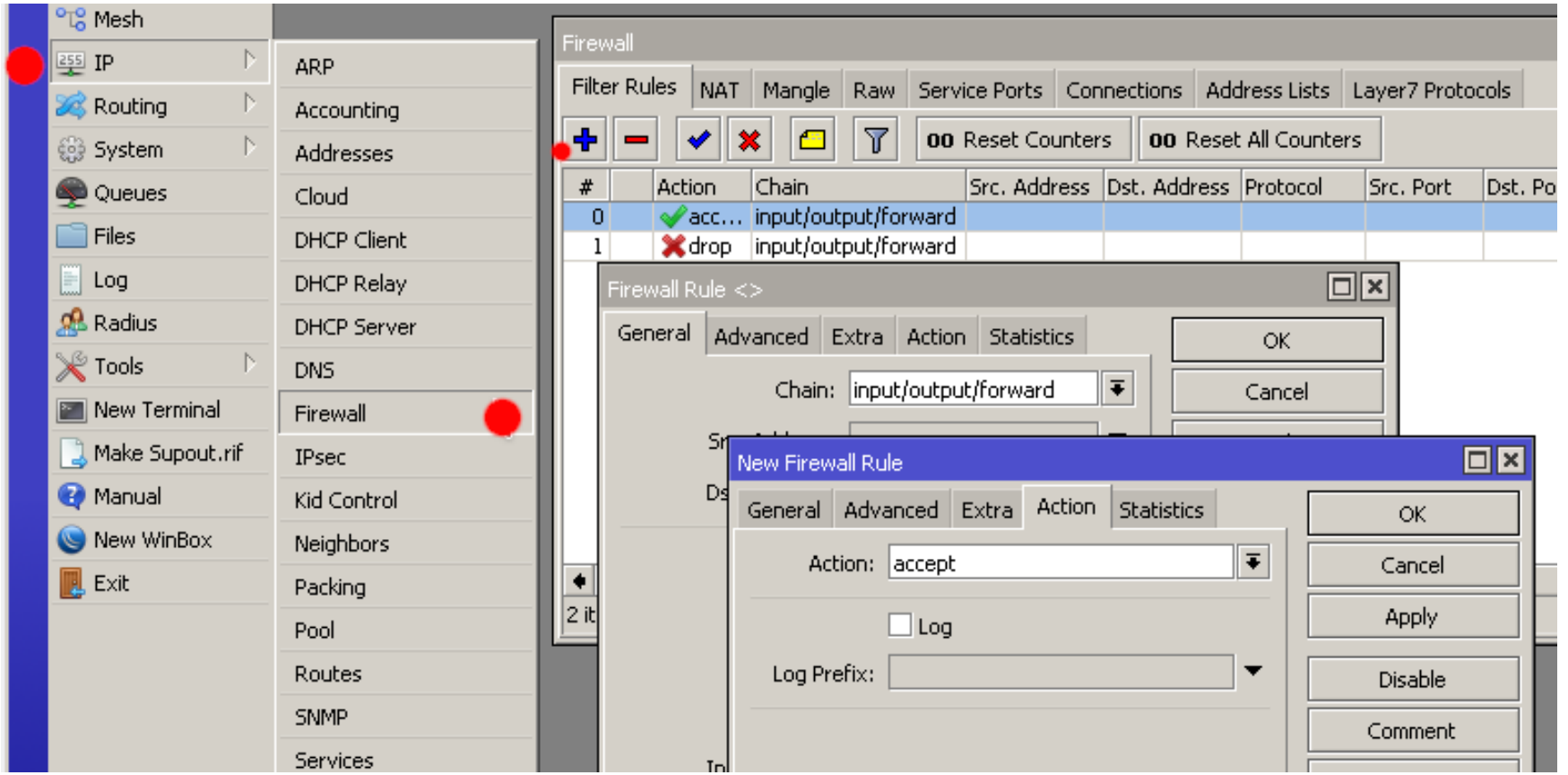
Bespoke Option – Firewall (matcher/action)

CLI/Terminal..

```
[NewUser@MikroTik] > ip firewall filter \
add chain=input/output/forward \
<matcher criteria> \
action=<accept/drop>
```

Bespoke Option – Firewall

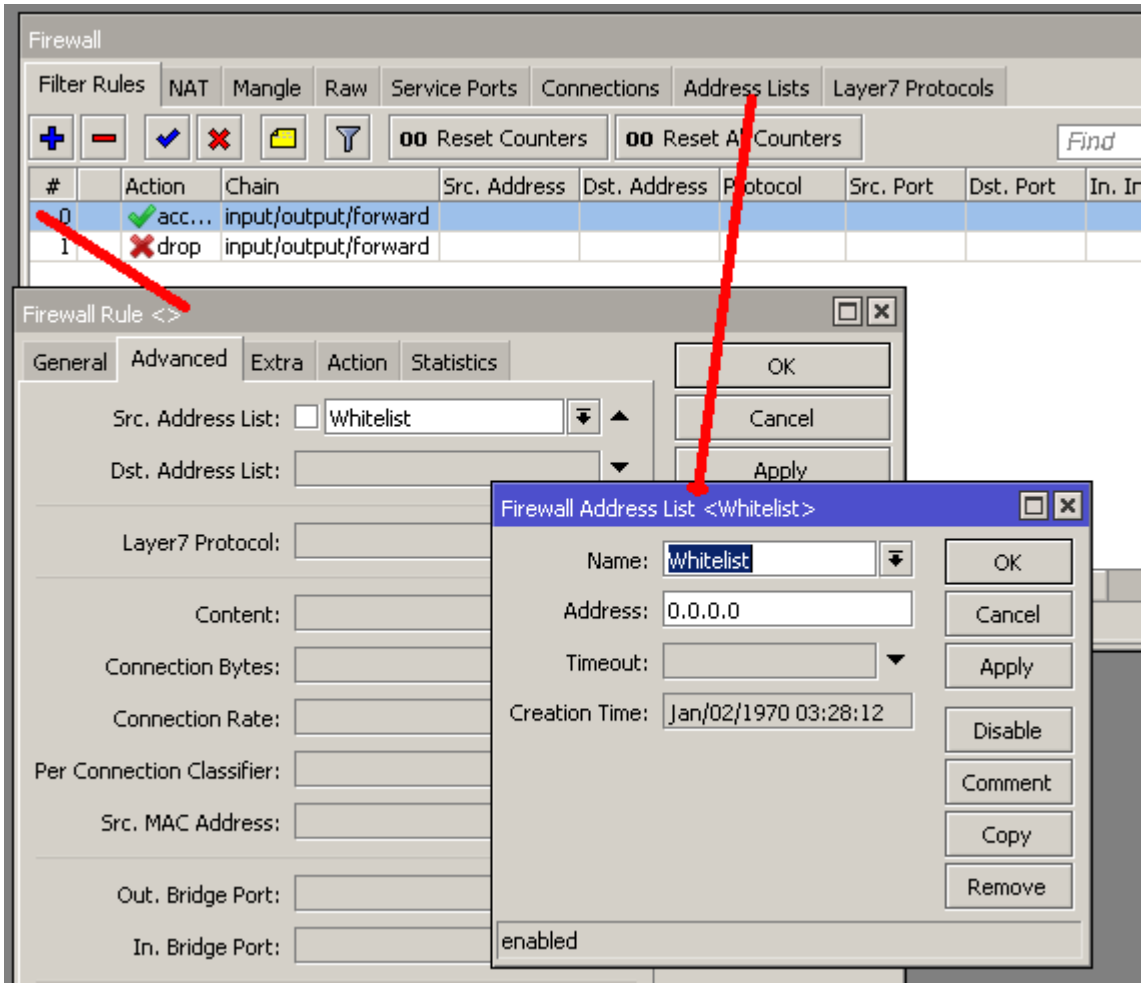
Individual accept..



Bespoke Option - Firewall

Using address lists

Bespoke Option – Firewall (address list)



Bespoke Option – Firewall (address list)

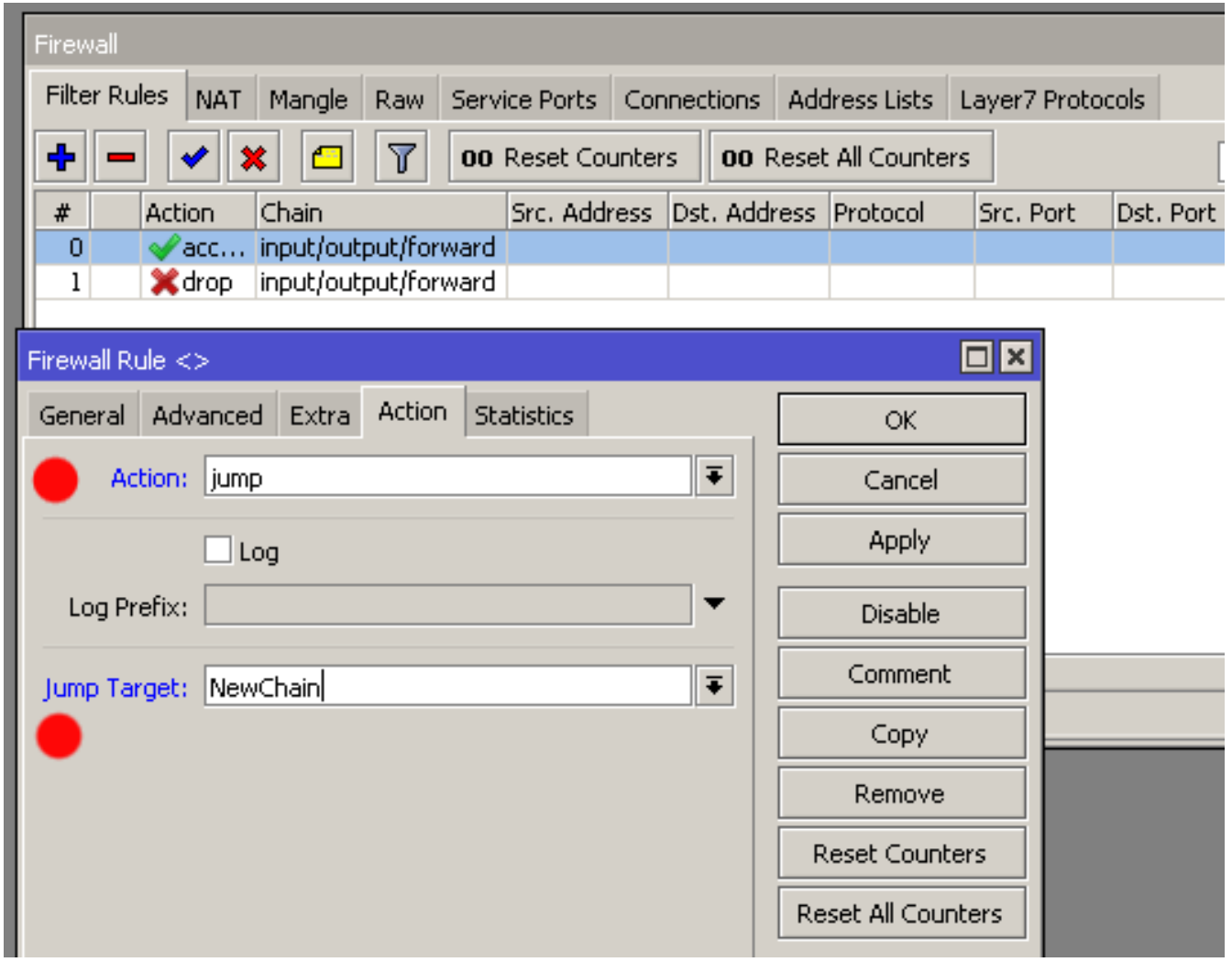
CLI/Terminal..

```
[NewUser@MikroTik] > /ip firewall filter add
chain=<input/output/forward>
<src/dst-address-list>=<address-list>
action=accept
```

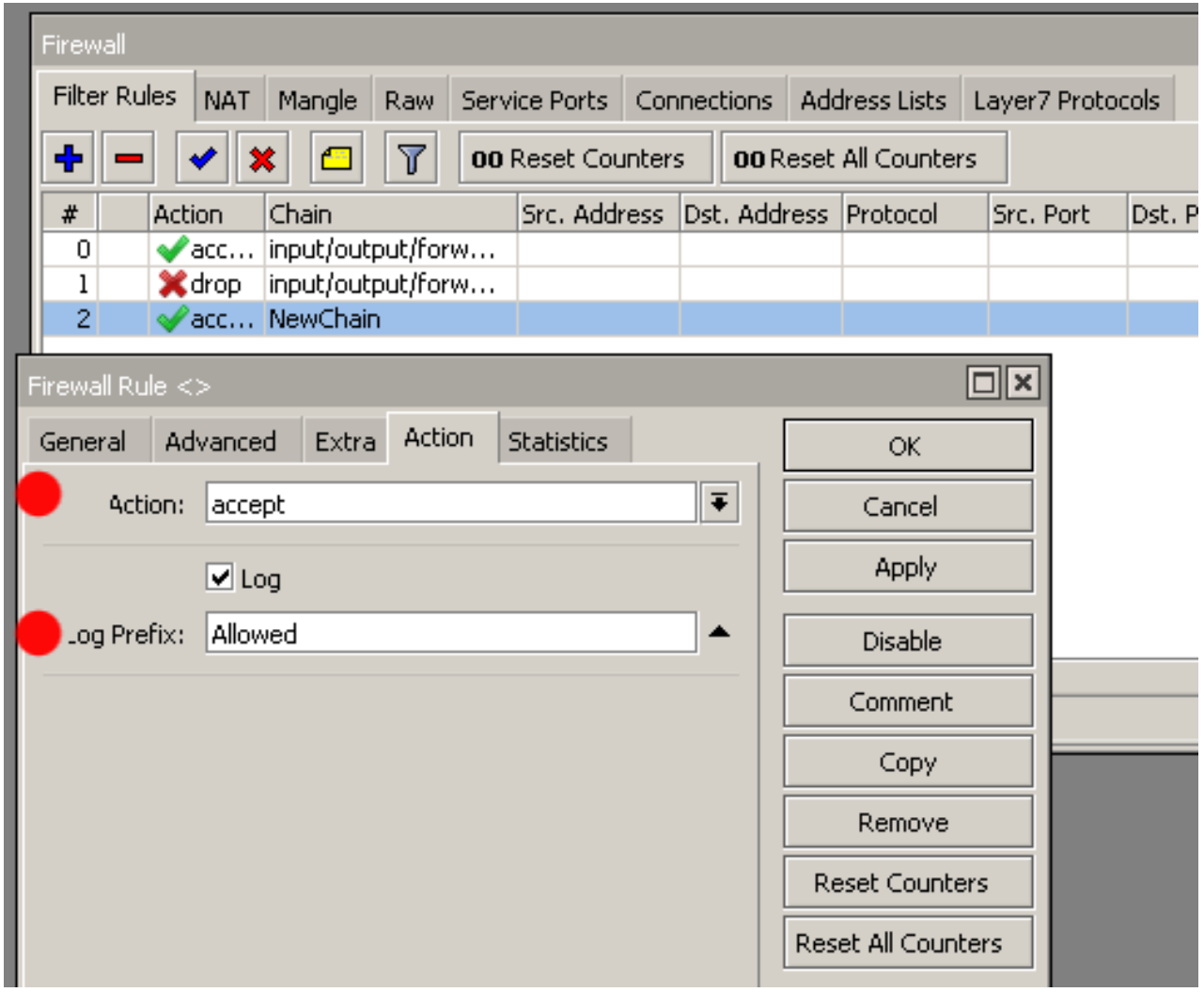
Bespoke Option - Firewall

Chains

Bespoke Option – Firewall (chain jump)



Bespoke Option – Firewall (NewChain action)



Bespoke Option – Firewall (address list)

CLI/Terminal..

```
[NewUser@MikroTik] > /ip firewall filter add \
chain=<input/output/forward> \
<matcher> \
action=jump jump-target=NewChain

[NewUser@MikroTik] > /ip firewall filter chain=NewChain \
<matcher> \
action=accept log=yes log-prefix="Allowed"
```

Bespoke Option - Firewall

Things to consider being allowed..

- Established / related packets
- Protocols
  - *ICMP & Routing*
- VPN's
  - *Management access*

Bespoke Option - Firewall

Firewall efficiency

- **Deal with the biggest bulk of packets first**
  - *Process unwanted and known bad packets/traffic*
  - *Process wanted and known good packets/traffic*
- **Deal with the unknown last**
  - *New streams*

Bespoke Option - Misc

Anything else to consider?

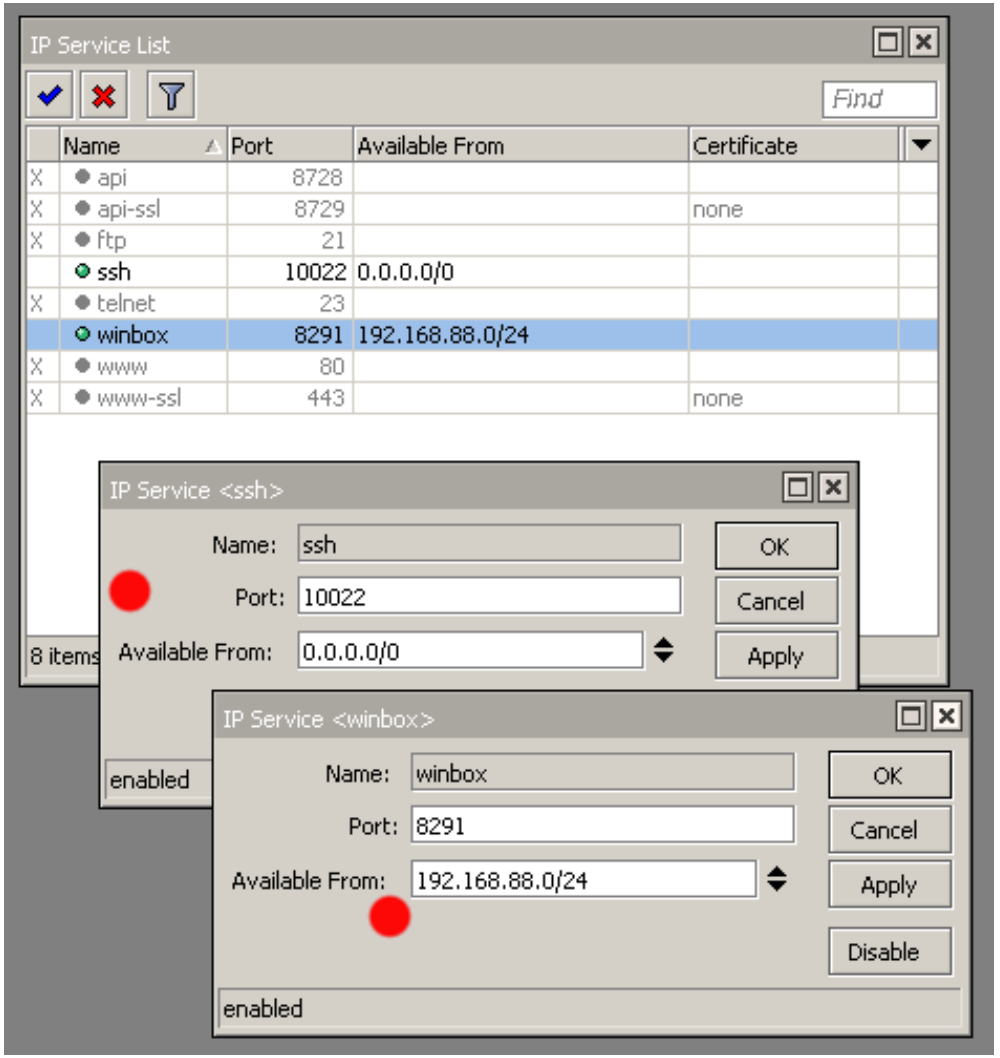
Lots of little bits!

Bespoke Option - Misc

IP Services..

- **Restrict the networks these services are allowed from.**
  - *Perhaps even contemplate changing the listening port – 'security by obscurity'*

Bespoke Option – Misc (Ip Services revisited)



Bespoke Option – Misc (Ip Services revisited)

```
[NewUser@MikroTik] > /ip service print
Flags: X - disabled, I - invalid
 #   NAME                PORT  ADDRESS         CERTIFICATE
 0 XI telnet                23
 1 XI ftp                   21
 2 XI www                   80
 3    ssh                10022 0.0.0.0/0
 4 XI www-ssl              443                  none
 5 XI api                 8728
 6    winbox              8291 192.168.88.0/24
 7 XI api-ssl             8729
[NewUser@MikroTik] > /ip service set ssh port=10022 \
address=0.0.0.0/0
[NewUser@MikroTik] > /ip service set winbox \
address=192.168.88.0/24
```

Bespoke Option – Misc (SSH)

Ssh..

Consider uprating SSH with options like

- Stronger crypto
- Larger key sizes
- Importing certificates for authentication

See wiki for more details

Bespoke Option – Misc (SSH)

```
[NewUser@MikroTik] > ip ssh set strong-crypto=yes
[NewUser@MikroTik] > ip ssh set host-key-size=4096
```

Bespole Options - Misc

Or consider..

Disabling all ip services and using a method called ‘port knocking’

A technique by which you use the firewall to monitor for a sequence of events that then trigger an access mechanism.

Again, check the wiki for information and howto’s

Bespoke Option – (Misc RP Filtering)

Reverse Path Filtering..

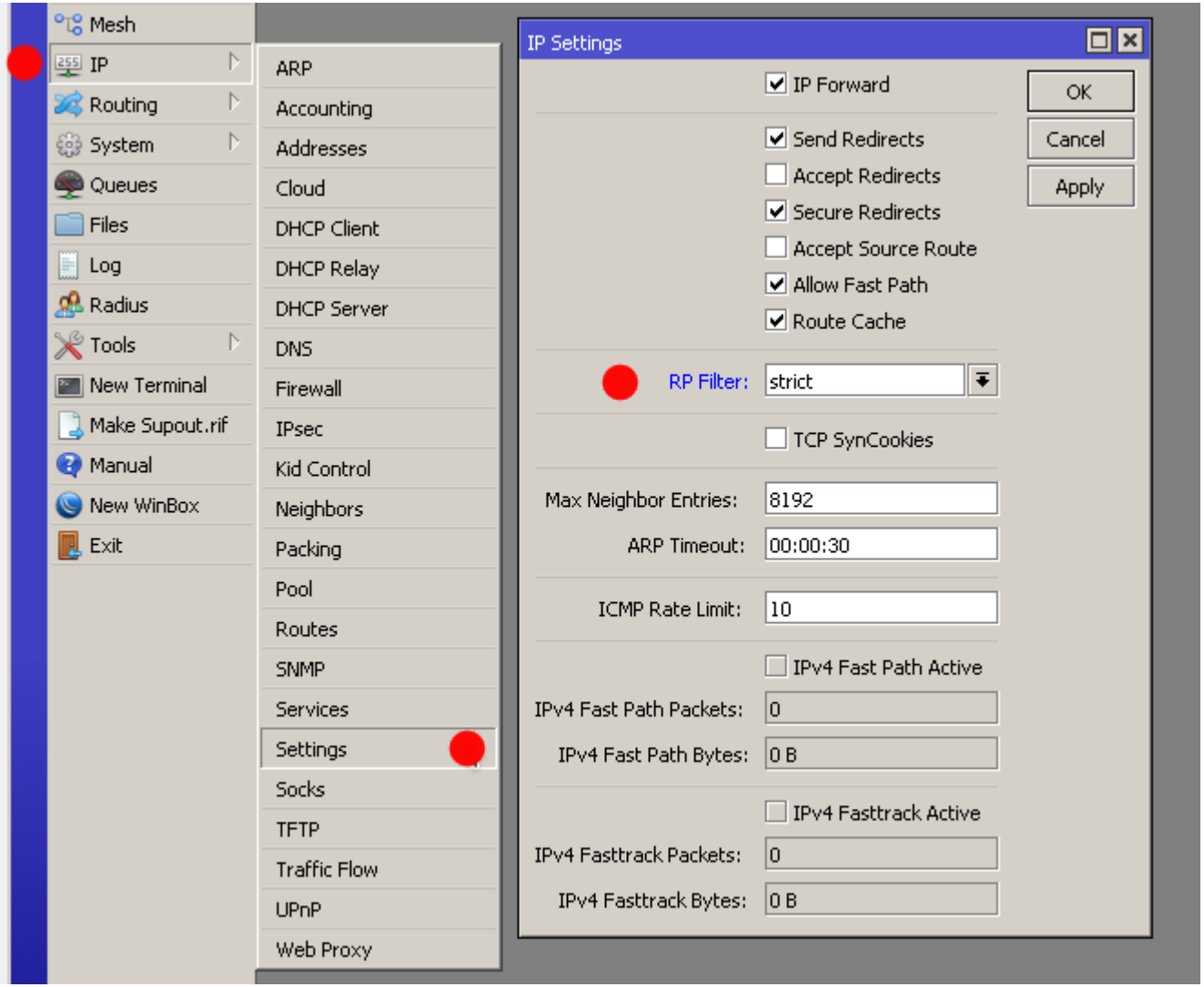
Drop packets that appear to be spoofed.

e.g. packets attempting to leave your network with incorrect source IP address.

It would indicate you have a system that's infected!

```
[NewUser@MikroTik] > /ip settings set rp-filter=strict
```

Bespoke Option – (Misc RP Filtering)



Bespoke Option – (Misc RP Filtering)

A word of caution when using RP-Filtering. It can't be implemented on individual interfaces.

It's all or nothing.

This leads rise to possible problems if the router is part of a multi-homed network.

Bespoke Option - Misc

And finally some common sense practises for the more advanced.

Bespoke Option - Misc

Routing protocols..

OSPF (v2)

- *Use authentication between routers*

  (even if it isn't that strong- MD5/password)
- *Do not broadcast OSPF on interfaces that are visible by prying eyes*

  (enable passive on the interface in question)

Bespoke Option - Misc

Routing cont..

BGP

- *Filters – Only allow the routes you want to have and to send*
- *Firewall – Only allow the peers you want to see and talk to*

Bespoke Option

Thank you for watching and listening

Any last questions?

Check list - ‘factory defualt’

1. New Username/password. disable/delete admin
2. Apply an allowed address range for the user
3. Disable services and any required ones restrict network access and/or change listening ports
4. Update RouterOS to the latest ‘Stable’ or ‘Long Term’ version
5. Don’t forget Routerboot
6. Disable MAC Services
7. Disable Neighbour Discovery
8. Disable unused interfaces/ports
9. Set at password for the WiFi plus check other security requirements
10. Disable Btest server
11. Disable MikroTik Cloud (not so urgent)
12. Add your own NTP details
13. Disable unused packages

Checklist – No factory defaults

1. Apply all the fixes from ‘factory default’
2. Firewall
3. SSH
4. Port Knocking?
5. Reverse Path Filtering
6. OSPF
7. BGP