

# 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

# 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:**

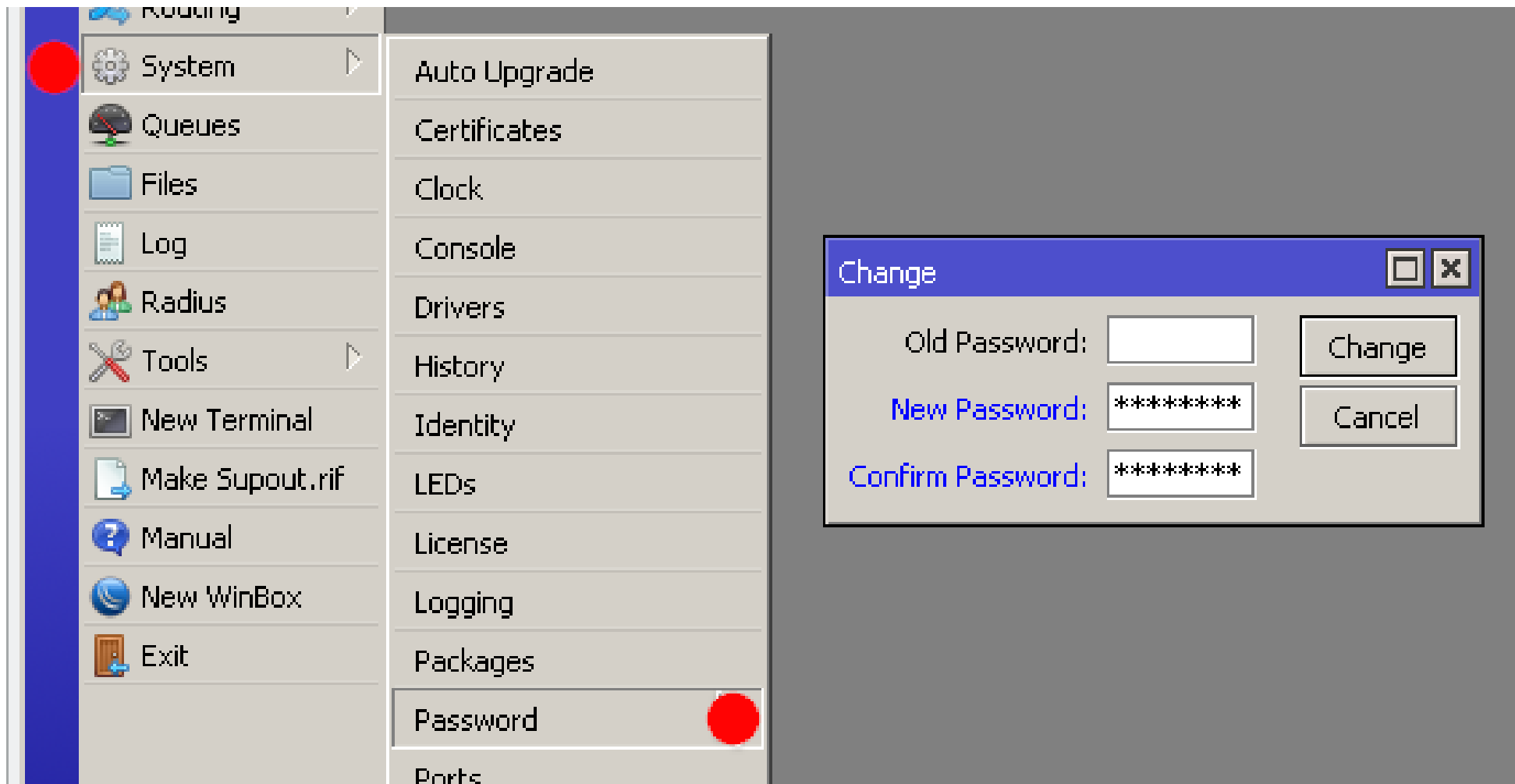
- 1) Created an admin user Password**
- 2) Disabled services**
- 3) Updated RouterOS to the latest 'Stable' or 'Long Term' version**

# Factory Default

## Step 1..

**Set an admin user password!**

# Factory Default



The image shows a screenshot of the Mikrotik WinBox interface. On the left, a vertical menu is open, displaying various system settings. The 'System' menu item is highlighted with a red circle. The 'Password' option at the bottom of this menu is also highlighted with a red circle. To the right of the menu, a 'Change' dialog box is displayed. This dialog box has a title bar with a close button and contains three input fields: 'Old Password', 'New Password', and 'Confirm Password'. The 'New Password' and 'Confirm Password' fields are filled with asterisks. There are 'Change' and 'Cancel' buttons to the right of the input fields.

# Factory Default

## Terminal/CLI..

```
[admin@MikroTik] > /password  
Old-password:  
New-password: *****(12)*****(12)  
confirm-new-password: *****(12)*****(12)
```

# Factory Default

Lets go one stage better..

Create a new user with a password.

Then disable the default admin account.

# Factory Default – new user

The screenshot displays the Mikrotik WinBox interface. On the left is a navigation tree with categories like Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, Make Supout.rif, Manual, New WinBox, and Exit. The main area shows the 'User List' window with tabs for Users, Groups, SSH Keys, SSH Private Keys, and Active Users. The 'Users' tab is active, showing a table with columns for Name, Group, Allowed Address, and Last Logged In. The table contains one entry: 'admin' in the 'full' group, with a last login of 'Oct/05/2018 18:17:27'. A 'New User' dialog box is open in the foreground, with the following fields: Name (NewUser), Group (full), Allowed Address (192.168.88.0/24), Last Logged In (empty), Password (masked with asterisks), and Confirm Password (masked with asterisks). The dialog also has buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove. The status 'enabled' is shown at the bottom of the dialog.

| Name  | Group | Allowed Address | Last Logged In       |
|-------|-------|-----------------|----------------------|
| admin | full  |                 | Oct/05/2018 18:17:27 |

New User dialog fields:

- Name: NewUser
- Group: full
- Allowed Address: 192.168.88.0/24
- Last Logged In:
- Password: \*\*\*\*\*
- Confirm Password: \*\*\*\*\*

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

Status: enabled

# Factory Default

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

The screenshot shows the Mikrotik WinBox interface. On the left is a navigation tree with categories like Routing, System, Queues, Files, Log, Radius, Tools, and Exit. The main area displays the 'User List' window. This window has tabs for Users, Groups, SSH Keys, SSH Private Keys, and Active Users. The 'Users' tab is active, showing a table with columns for Name, Group, Allowed Address, and Last Logged In. The 'admin' user is selected, and a 'User <admin>' dialog box is open over it. This dialog box contains fields for Name (admin), Group (full), Allowed Address, and Last Logged In (Oct/06/2018 09:32:56). A red circle highlights the 'Disable' button in the dialog. Other buttons include OK, Cancel, Apply, Comment, Copy, Remove, and Password... The status 'enabled' is shown at the bottom of the dialog.

| Name                    | Group | Allowed Address | Last Logged In       |
|-------------------------|-------|-----------------|----------------------|
| NewUser                 | full  |                 |                      |
| ;;; system default user |       |                 |                      |
| admin                   | full  |                 | Oct/06/2018 09:32:56 |

# 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

The screenshot shows the Mikrotik WinBox interface. On the left is a navigation tree with categories like IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, and Services. The 'Services' category is highlighted with a red dot. The main window displays the 'IP Service List' dialog, which contains a table of services and their configurations.

|   | Name    | Port | Available From | Certificate |
|---|---------|------|----------------|-------------|
| X | api     | 8728 |                |             |
| X | api-ssl | 8729 |                | none        |
| X | ftp     | 21   |                |             |
|   | ssh     | 22   |                |             |
| X | telnet  | 23   |                |             |
|   | winbox  | 8291 |                |             |
| X | www     | 80   |                |             |
| X | www-ssl | 443  |                | none        |

8 items (1 selected)

# 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 Internet..

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

The screenshot displays the Mikrotik WinBox interface. On the left is a sidebar menu with categories like System, Queues, Files, Log, Radius, Tools, and Exit. The main area is divided into a left pane with 'Packages' selected and a right pane showing the 'Package List' table. A 'Check For Updates' dialog box is open, displaying update information for RouterOS.

| Name           | Version | Build Time           | Scheduled |
|----------------|---------|----------------------|-----------|
| routeros-smips | 6.43    | Sep/06/2018 12:44:56 |           |
| advanced-...   | 6.43    | Sep/06/2018 12:44:56 |           |

**Check For Updates**

Channel: bugfix only

Installed Version: 6.43

Latest Version: 6.42.9

What's new in 6.42.9 (2018-Sep-27 05:19):

Important note!!! Backup before upgrade!  
RouterOS v6.41 and above contains new bridge implementation that supports hardware offloading (hw-offload).  
This update will convert all interface "master-port" configuration into new bridge configuration, and eliminate "master-port" option as such. Bridge will handle all Layer2 forwarding and the use of switch-chip (hw-offload) will be automatically turned on based on appropriate conditions. The rest of RouterOS Switch specific configuration remains untouched in usual menus.  
Please, note that downgrading below RouterOS v6.41 will not restore "master-port" configuration, so use backups to restore configuration on downgrade.

- \*) bridge - ignore tagged BPDUs when bridge VLAN filtering is used;
- \*) bridge - improved packet handling when hardware offloading is being disabled;
- \*) crs317 - fixed packet forwarding on bonded interfaces without hardware offloading;
- \*) crs326/crs328 - fixed packet forwarding when port changes states with IGMP Snooping enabled;
- \*) defconf - properly clear global variables when generating default configuration after RouterOS upgrade;
- \*) dns - fixed DNS cache service becoming unresponsive when active Hotspot server is present on the router (introduced in 6.42);

New version is available

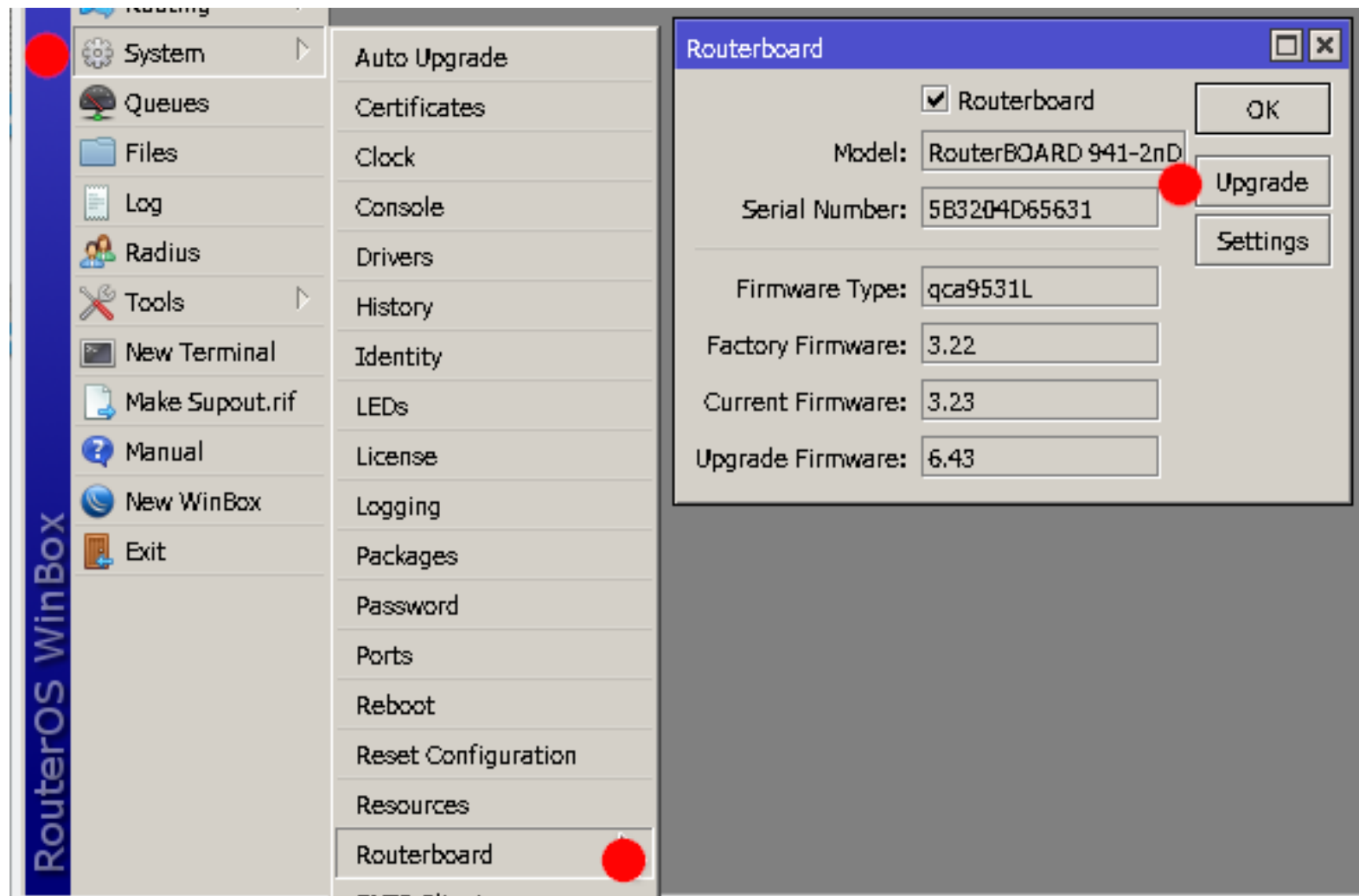
# Factory Default – Update RouterOS

```
[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
```

# Factory 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*

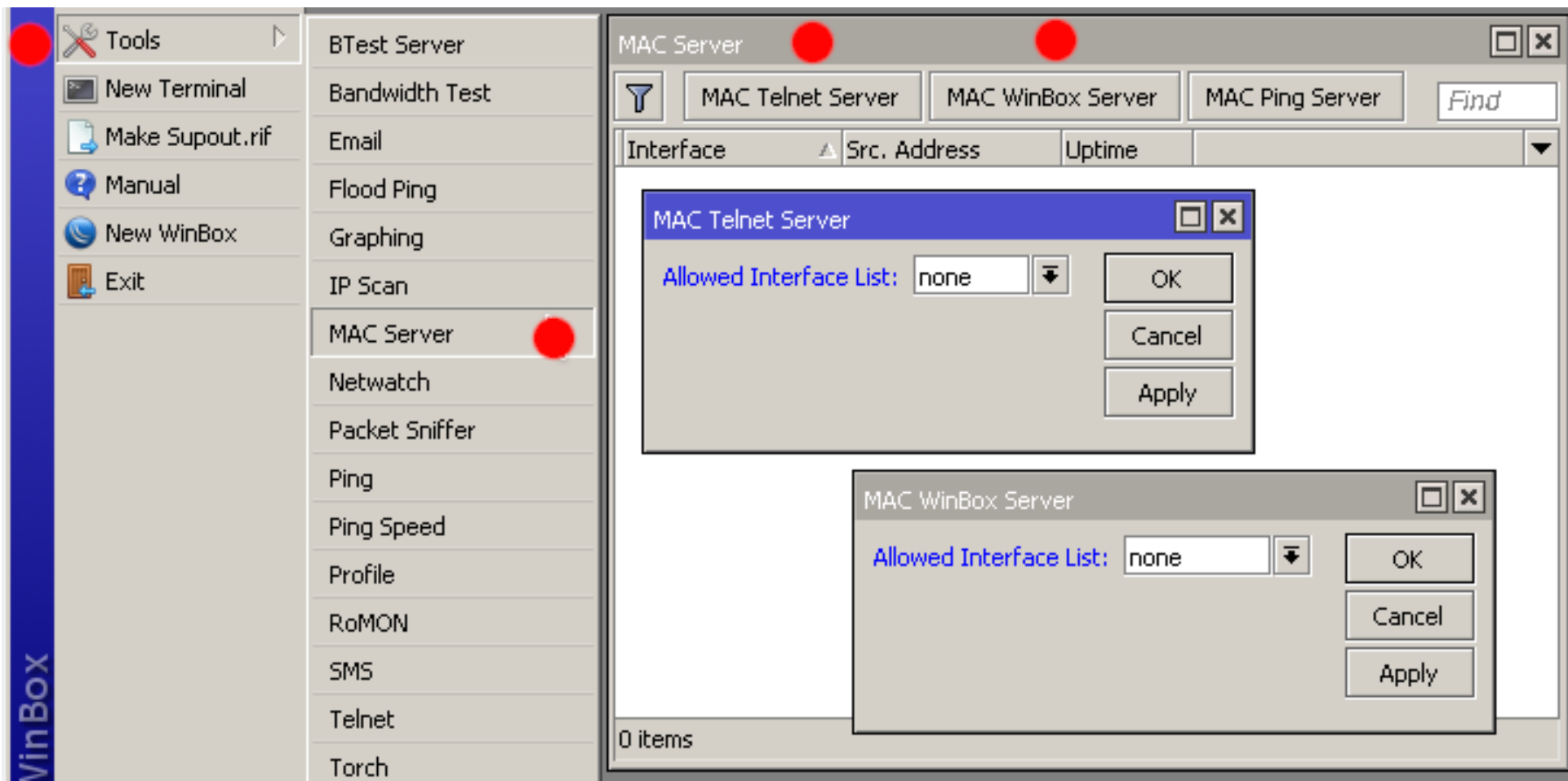


## Factory Default – MAC servers

### 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?

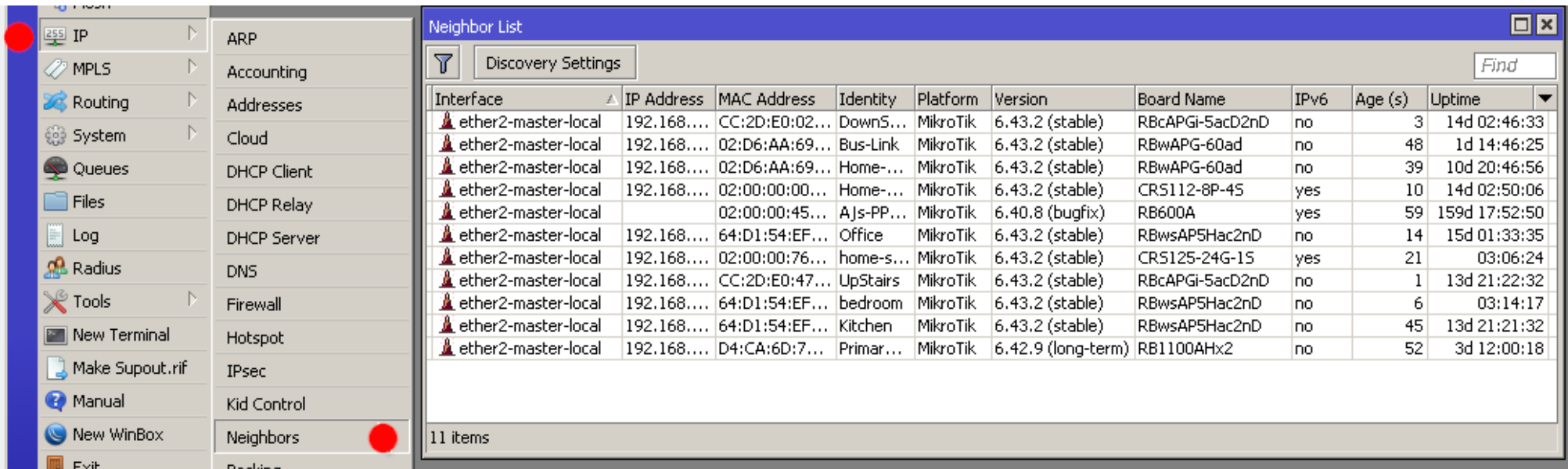
Neighbor Discovery allows your router to be seen by other devices and information of those devices seen by your device.

Neighbor Discovery Protocol (NDP)

Cisco Discovery Protocol (CDP)

# Neighbor Discovery

## Information seen..



Neighbor List

Discovery Settings

| Interface           | IP Address  | MAC Address    | Identity   | Platform | Version            | Board Name      | IPv6 | Age (s) | Uptime        |
|---------------------|-------------|----------------|------------|----------|--------------------|-----------------|------|---------|---------------|
| ether2-master-local | 192.168.... | CC:2D:E0:02... | DownS...   | MikroTik | 6.43.2 (stable)    | RBcAPGi-5acD2nD | no   | 3       | 14d 02:46:33  |
| ether2-master-local | 192.168.... | 02:D6:AA:69... | Bus-Link   | MikroTik | 6.43.2 (stable)    | RBwAPG-60ad     | no   | 48      | 1d 14:46:25   |
| ether2-master-local | 192.168.... | 02:D6:AA:69... | Home-...   | MikroTik | 6.43.2 (stable)    | RBwAPG-60ad     | no   | 39      | 10d 20:46:56  |
| ether2-master-local | 192.168.... | 02:00:00:00... | Home-...   | MikroTik | 6.43.2 (stable)    | CRS112-8P-45    | yes  | 10      | 14d 02:50:06  |
| ether2-master-local |             | 02:00:00:45... | Ajs-PP...  | MikroTik | 6.40.8 (bugfix)    | RB600A          | yes  | 59      | 159d 17:52:50 |
| ether2-master-local | 192.168.... | 64:D1:54:EF... | Office     | MikroTik | 6.43.2 (stable)    | RBwsAP5Hac2nD   | no   | 14      | 15d 01:33:35  |
| ether2-master-local | 192.168.... | 02:00:00:76... | home-s...  | MikroTik | 6.43.2 (stable)    | CRS125-24G-15   | yes  | 21      | 03:06:24      |
| ether2-master-local | 192.168.... | CC:2D:E0:47... | UpStairs   | MikroTik | 6.43.2 (stable)    | RBcAPGi-5acD2nD | no   | 1       | 13d 21:22:32  |
| ether2-master-local | 192.168.... | 64:D1:54:EF... | bedroom    | MikroTik | 6.43.2 (stable)    | RBwsAP5Hac2nD   | no   | 6       | 03:14:17      |
| ether2-master-local | 192.168.... | 64:D1:54:EF... | Kitchen    | MikroTik | 6.43.2 (stable)    | RBwsAP5Hac2nD   | no   | 45      | 13d 21:21:32  |
| ether2-master-local | 192.168.... | D4:CA:6D:7...  | Primar ... | MikroTik | 6.42.9 (long-term) | RB1100AHx2      | no   | 52      | 3d 12:00:18   |

11 items

# Factory Default – Neighbor Discovery

The screenshot displays the Mikrotik WinBox interface. On the left is a navigation tree with categories like IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, and New WinBox. The 'Neighbors' menu item is highlighted with a red dot. The main window shows the 'Neighbor List' configuration page, which includes a 'Discovery Settings' button and a table with columns for 'Interface', 'IP Address', 'MAC Address', and 'Identity'. The table currently shows '0 items'. A 'Discovery Settings' dialog box is open in the foreground, featuring an 'Interface' dropdown menu set to 'none' and buttons for 'OK', 'Cancel', and 'Apply'.

# 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

The screenshot displays the Mikrotik WinBox interface. On the left is a sidebar menu with categories like Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, and New Terminal. The main window shows the 'Interface List' configuration page. A table lists several Ethernet interfaces. The interface 'ether4-slave-local' is selected and highlighted in blue. Below the table, a configuration window for 'Interface <ether4-slave-local>' is open, showing fields for Name, Type, MTU, Actual MTU, and L2 MTU. The 'Disable' button in this window is highlighted with a red circle, indicating the goal of the tutorial.

|    | Name              | Type     | MTU  | Actual MTU | L2 MTU | Tx |
|----|-------------------|----------|------|------------|--------|----|
|    | ether1-gateway    | Ethernet | 1500 | 1500       | 1598   |    |
| RS | ether2-maste...   | Ethernet | 1500 | 1500       | 1598   |    |
| S  | ether3-slave-l... | Ethernet | 1500 | 1500       | 1598   |    |
| S  | ether4-slave-l... | Ethernet | 1500 | 1500       | 1598   |    |

Interface configuration details for 'ether4-slave-local':

- Name: ether4-slave-local
- Type: Ethernet
- MTU: 1500
- Actual MTU: 1500
- L2 MTU: 1598
- Max L2 MTU: 2028

# 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

The screenshot displays the WinBox interface for configuring a wireless interface. The left sidebar shows the navigation menu with 'Wireless' selected. The main window is divided into several panes:

- Wireless Tables:** A table listing wireless interfaces. The 'wlan1' interface is selected, showing details like Name, Type, Actual MTU, Tx, Rx, Tx Packet (p/s), Rx Packet (p/s), and FP Tx.
- Interface <wlan1>:** The 'Wireless' tab is active, showing configuration for 'ap bridge' mode on the '2GHz-B/G/N' band. The SSID is 'MikroTik-F9AA42' and the security profile is 'New-wifi-profile'.
- Security Profile <New-wifi-profile>:** The 'General' tab is active, showing 'dynamic keys' mode. Authentication types include WPA2 PSK (checked) and WPA2 EAP. Unicast and Group Ciphers are set to 'aes ccm'. The WPA2 Pre-Shared Key is masked with asterisks.

Red arrows point to the 'wlan1' interface in the table and the 'New-wifi-profile' security profile dropdown in the interface configuration pane.

# 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

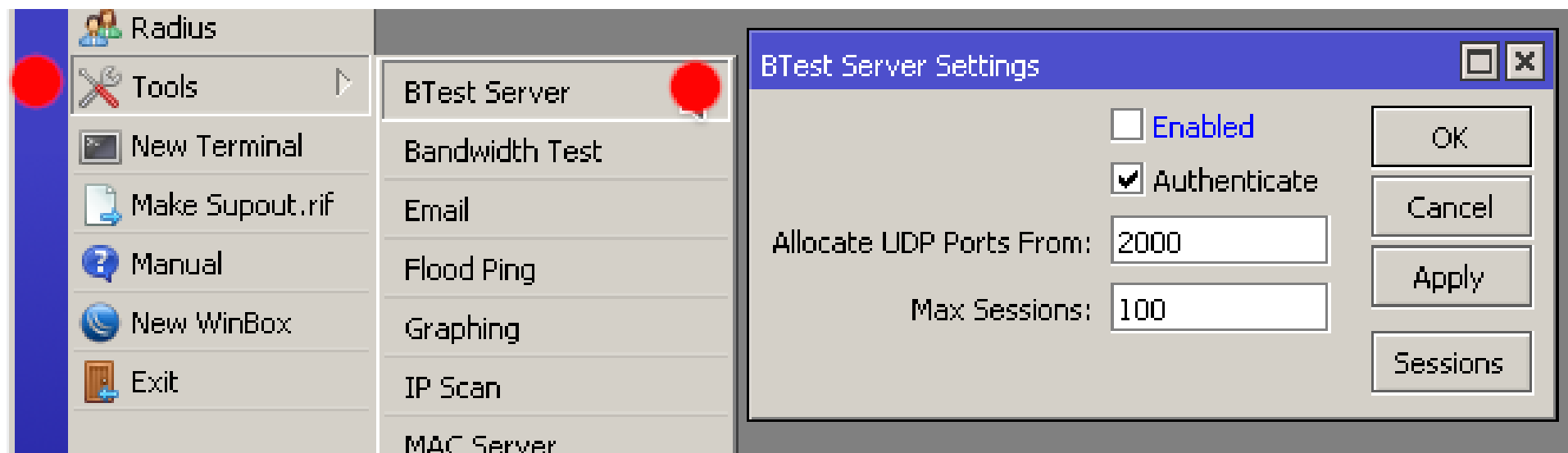
## Why disable the Btest Server?

**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

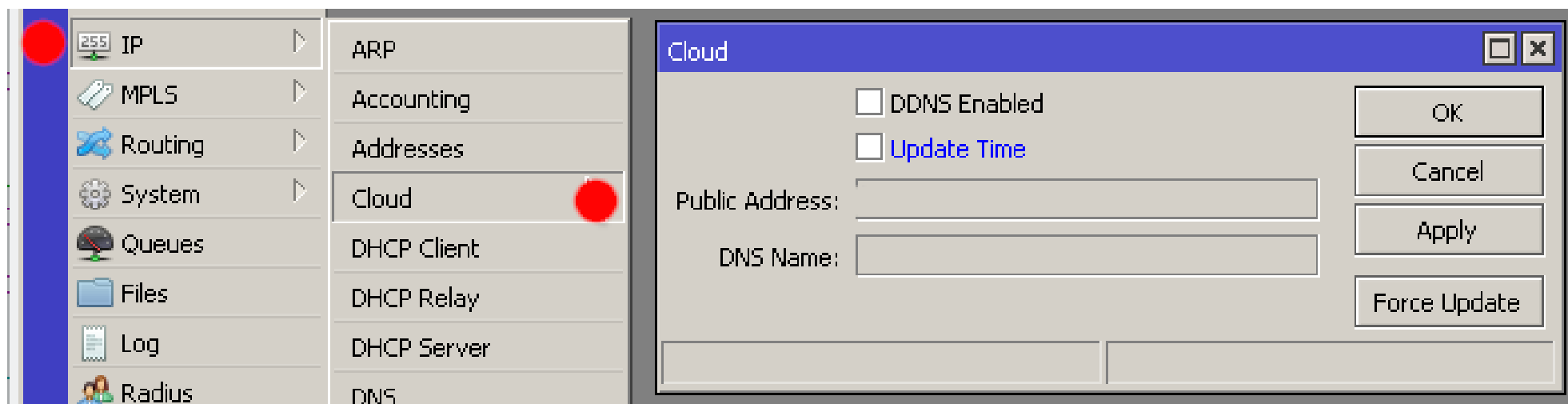


```
[NewUser@MikroTik] > /tool bandwidth-server set \  
enabled=no
```

# Factory Default – NTP

Do you trust MikroTik Cloud time update?

# Factory Default – NTP

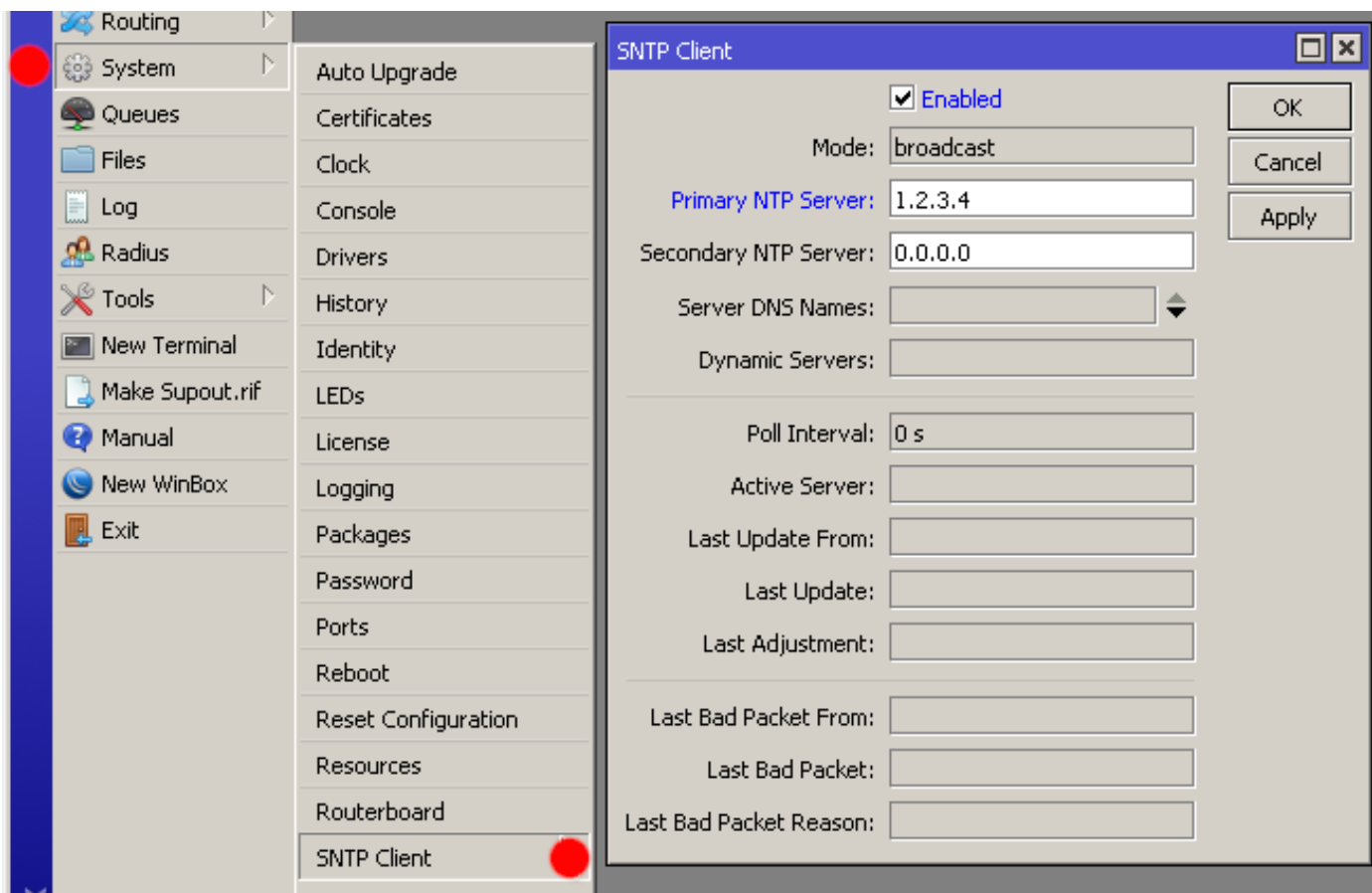


```
[NewUser@MikroTik] > /ip cloud set update-time=no
```

## 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

Package List

| Name           | Version | Build Time           | Scheduled             |
|----------------|---------|----------------------|-----------------------|
| routeros-smips | 6.43    | Sep/06/2018 12:44:56 |                       |
| advanced-...   | 6.43    | Sep/06/2018 12:44:56 |                       |
| dhcp           | 6.43    | Sep/06/2018 12:44:56 |                       |
| hotspot        | 6.43    | Sep/06/2018 12:44:56 | scheduled for disable |
| ipv6           | 6.43    | Sep/06/2018 12:44:56 |                       |
| mpls           | 6.43    | Sep/06/2018 12:44:56 | scheduled for disable |
| ppp            | 6.43    | Sep/06/2018 12:44:56 | scheduled for disable |
| routing        | 6.43    | Sep/06/2018 12:44:56 |                       |
| security       | 6.43    | Sep/06/2018 12:44:56 |                       |
| system         | 6.43    | Sep/06/2018 12:44:56 |                       |
| wireless       | 6.43    | Sep/06/2018 12:44:56 |                       |

11 items (3 selected)

```
[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!

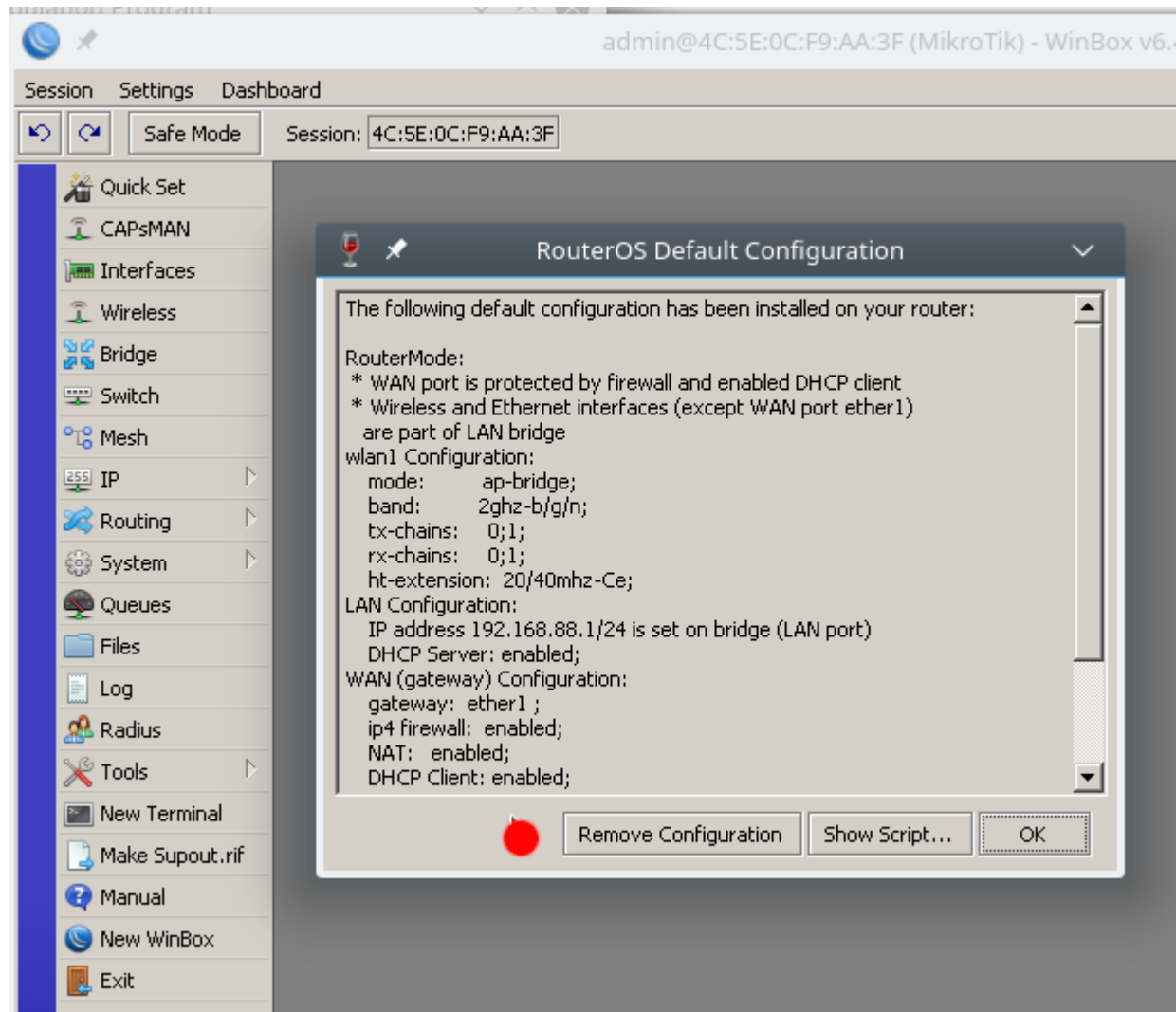
## Bespoke option

**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

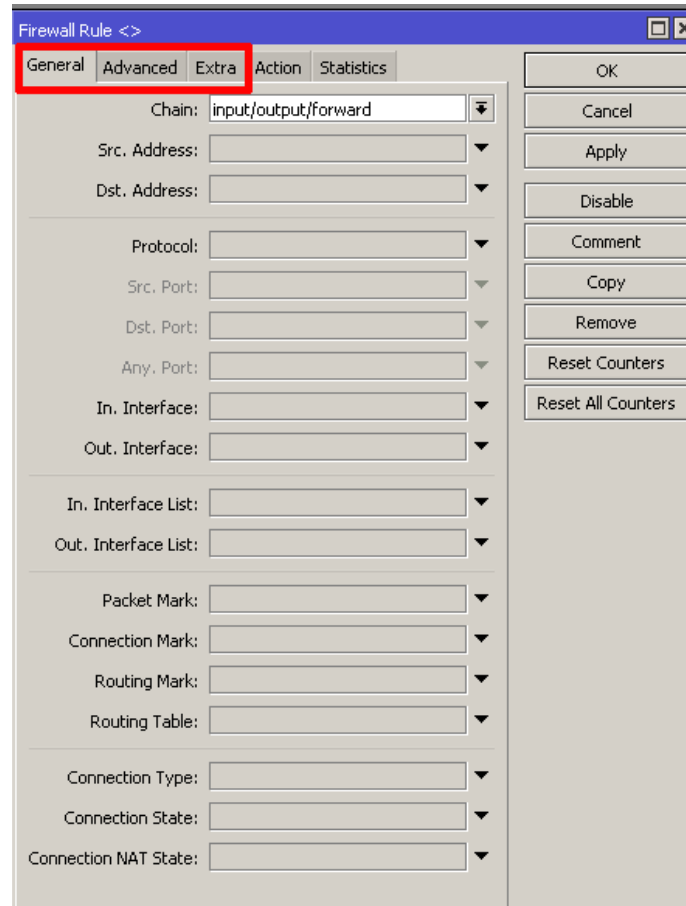
# Bespoke Option – Firewall

The screenshot shows the MikroTik WinBox interface for configuring the Firewall. The left sidebar contains a menu with 'Firewall' highlighted. The main window displays the 'Filter Rules' tab, which includes a table of rules and control buttons.

| # | Action   | Chain                | Src. Address | Dst. Address | Protocol | Src. Port | Dst. Port |
|---|----------|----------------------|--------------|--------------|----------|-----------|-----------|
| 0 | ✓ acc... | input/output/forward |              |              |          |           |           |
| 1 | ✗ drop   | input/output/forward |              |              |          |           |           |

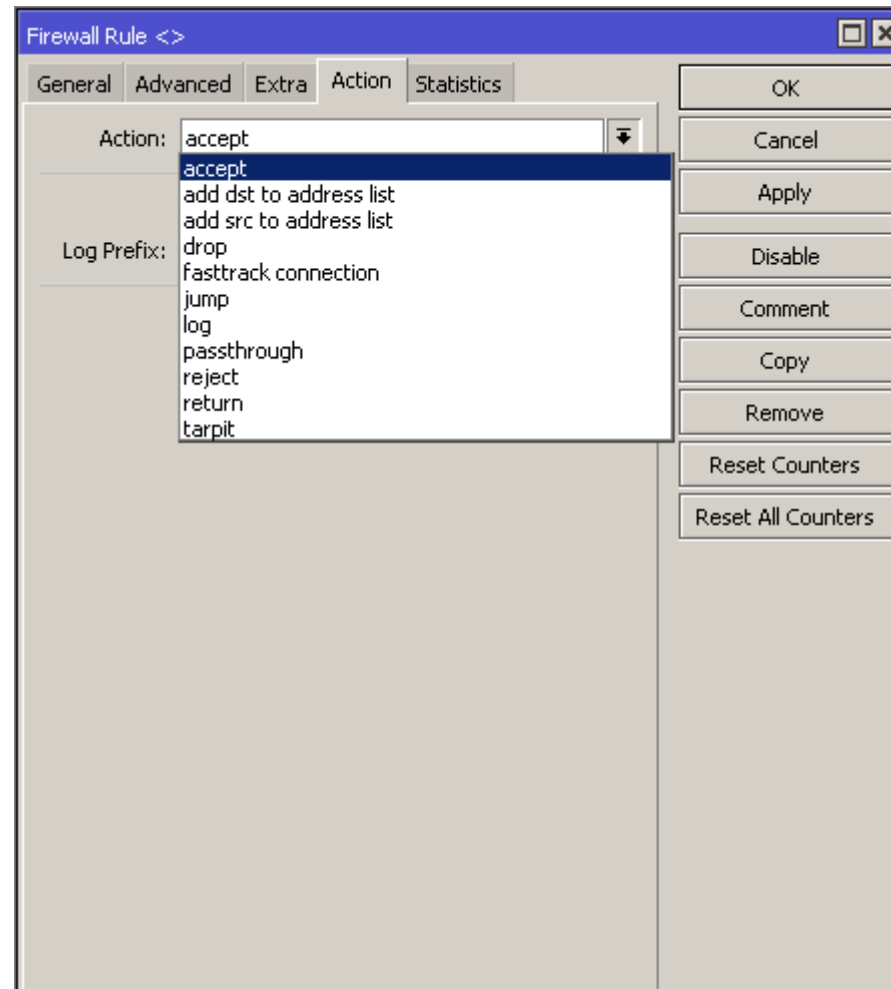
2 items (1 selected)

# 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..

The screenshot displays the Mikrotik WinBox Firewall configuration interface. On the left, a sidebar menu shows various system settings, with 'Firewall' highlighted. The main window shows the 'Filter Rules' tab, containing a table of active rules:

| # | Action   | Chain                | Src. Address | Dst. Address | Protocol | Src. Port | Dst. Po |
|---|----------|----------------------|--------------|--------------|----------|-----------|---------|
| 0 | ✓ acc... | input/output/forward |              |              |          |           |         |
| 1 | ✗ drop   | input/output/forward |              |              |          |           |         |

Below the table, two dialog boxes are visible. The top one is 'Firewall Rule <>' with the 'Chain' set to 'input/output/forward'. The bottom one is 'New Firewall Rule' with the 'Action' set to 'accept' and the 'Log' checkbox unchecked. The 'Log Prefix' field is also visible.

# Bespoke Option - Firewall

## Using address lists

# Bespoke Option – Firewall (address list)

The screenshot displays the Mikrotik WinBox Firewall configuration interface. At the top, the 'Address Lists' tab is selected. Below it, a table lists firewall rules:

| # | Action   | Chain                | Src. Address | Dst. Address | Protocol | Src. Port | Dst. Port | In. In |
|---|----------|----------------------|--------------|--------------|----------|-----------|-----------|--------|
| 0 | ✓ acc... | input/output/forward |              |              |          |           |           |        |
| 1 | ✗ drop   | input/output/forward |              |              |          |           |           |        |

A red arrow points to rule #0. Below the table, the 'Firewall Rule <>' dialog is open, showing the 'General' tab. The 'Src. Address List' is set to 'Whitelist'. A second red arrow points to the 'Whitelist' dropdown menu. In the foreground, the 'Firewall Address List <Whitelist>' dialog is open, showing the 'Name' as 'Whitelist' and the 'Address' as '0.0.0.0'. The 'Creation Time' is 'Jan/02/1970 03:28:12'. The status at the bottom is 'enabled'.

# 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)

The screenshot displays the Mikrotik WinBox Firewall configuration interface. At the top, there are tabs for Filter Rules, NAT, Mangle, Raw, Service Ports, Connections, Address Lists, and Layer7 Protocols. Below these are icons for adding, deleting, enabling, and disabling rules, along with buttons for 'Reset Counters' and 'Reset All Counters'. A table lists the active firewall rules:

| # | Action   | Chain                | Src. Address | Dst. Address | Protocol | Src. Port | Dst. Port |
|---|----------|----------------------|--------------|--------------|----------|-----------|-----------|
| 0 | ✓ acc... | input/output/forward |              |              |          |           |           |
| 1 | ✗ drop   | input/output/forward |              |              |          |           |           |

The 'Firewall Rule <>' dialog box is open, showing the configuration for rule #1. The 'Action' is set to 'jump'. The 'Log' checkbox is unchecked. The 'Log Prefix' is empty. The 'Jump Target' is set to 'NewChain'. On the right side of the dialog, there are buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.



# Bespoke Option – Firewall (NewChain action)

The screenshot displays the Mikrotik WinBox Firewall configuration interface. At the top, there are tabs for Filter Rules, NAT, Mangle, Raw, Service Ports, Connections, Address Lists, and Layer7 Protocols. Below these are buttons for adding (+), removing (-), enabling (checkmark), disabling (cross), and a filter icon. There are also buttons for '00 Reset Counters' and '00 Reset All Counters'.

| # | Action   | Chain                | Src. Address | Dst. Address | Protocol | Src. Port | Dst. P |
|---|----------|----------------------|--------------|--------------|----------|-----------|--------|
| 0 | ✓ acc... | input/output/forw... |              |              |          |           |        |
| 1 | ✗ drop   | input/output/forw... |              |              |          |           |        |
| 2 | ✓ acc... | NewChain             |              |              |          |           |        |

The 'Firewall Rule <>' dialog box is open, showing the 'Action' tab. The 'Action' dropdown is set to 'accept'. The 'Log' checkbox is checked, and the '\_log Prefix' is set to 'Allowed'. On the right side of the dialog, there are buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

# 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!

## 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)

The screenshot shows the Mikrotik WinBox interface for configuring IP services. The main window, titled "IP Service List", contains a table with the following data:

| Name        | Port  | Available From  | Certificate |
|-------------|-------|-----------------|-------------|
| X ● api     | 8728  |                 |             |
| X ● api-ssl | 8729  |                 | none        |
| X ● ftp     | 21    |                 |             |
| ● ssh       | 10022 | 0.0.0.0/0       |             |
| X ● telnet  | 23    |                 |             |
| ● winbox    | 8291  | 192.168.88.0/24 |             |
| X ● www     | 80    |                 |             |
| X ● www-ssl | 443   |                 | none        |

Two configuration windows are overlaid on the main window:

- IP Service <ssh>**: Shows Name: ssh, Port: 10022, Available From: 0.0.0.0/0. A red dot is visible on the left side of the window.
- IP Service <winbox>**: Shows Name: winbox, Port: 8291, Available From: 192.168.88.0/24. A red dot is visible on the left side of the window.

At the bottom left of the WinBox interface, the text "8 items" and "enabled" is visible.

# 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 upgrading 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
```

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)

The image shows the Mikrotik WinBox interface. On the left is a sidebar menu with categories: Mesh, IP, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, Make Supout.rif, Manual, New WinBox, and Exit. The 'IP' category is expanded, showing a list of sub-items: ARP, Accounting, Addresses, Cloud, DHCP Client, DHCP Relay, DHCP Server, DNS, Firewall, IPsec, Kid Control, Neighbors, Packing, Pool, Routes, SNMP, Services, Settings, Socks, TFTP, Traffic Flow, UPnP, and Web Proxy. A red dot is placed next to 'Settings' in this list. The 'IP Settings' dialog box is open, showing various configuration options. A red dot is placed next to the 'RP Filter' dropdown menu, which is currently set to 'strict'. Other options include checkboxes for IP Forward, Send Redirects, Accept Redirects, Secure Redirects, Accept Source Route, Allow Fast Path, Route Cache, and TCP SynCookies. Text input fields are provided for Max Neighbor Entries (8192), ARP Timeout (00:00:30), ICMP Rate Limit (10), IPv4 Fast Path Packets (0), IPv4 Fast Path Bytes (0 B), IPv4 Fasttrack Packets (0), and IPv4 Fasttrack Bytes (0 B). Buttons for OK, Cancel, and Apply are visible on the right side of the dialog.

## 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.

## 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)*



## 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 default'

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