



# Basic guidelines on RouterOS configuration and debugging

Martins Strods

MikroTik, Latvia

Ho Chi Minh City, Vietnam

April 2017

# What is the main idea of this?

“Little things matter and are very important”

# RouterOS is the same everywhere



# RouterOS management tools

# RouterOS management

- CLI (Command Line Interface)

<https://wiki.mikrotik.com/wiki/Manual:Console>

- Webfig

<https://wiki.mikrotik.com/wiki/Manual:Webfig>

- TikApp

<https://forum.mikrotik.com/viewtopic.php?t=98407>

- Winbox

<https://wiki.mikrotik.com/wiki/Manual:Winbox>

**The fastest way how to configure device**

# QuickSet

admin@192.168.88.1 (MikroTik) - WinBox v6.38.5 on hAP ac (mipsbe)

Session Settings Dashboard

Safe Mode Session:

Quick Set CAPsMAN Interfaces Wireless Bridge PPP Switch Mesh IP MPLS Routing System Queues File Log Radius Tools New Terminal MetaROUTER Faston Make Supout.rtf Manual New WinBox Exit

Home AP (Dual) Quick Set

Home AP Dual  
CAP  
CPE  
Home AP Dual  
FTP Bridge  
WSP AP

2GHz 5GHz

Network Name: MikroTik-2798E1 MikroTik-2798E2

Frequency: auto auto MHz

Band: 2GHz-B/G/N 5GHz-A/N/AC

Country: no\_country\_set

Use Access List (ACL)

WiFi Password:

WPS Access

Guest Wireless Network:

Guest Network:

Wireless Clients

MAC Address	In ACL	Last IP	Uptime	Signal Strength

Signal Strength

Copy To ACL Remove From ACL

Internet

Port: Eth1

Address Acquisition:  Static  Automatic  PPPoE

IP Address: 172.16.1.243

Netmask: 255.255.255.0 (/24)

Gateway: 172.16.1.1

MAC Address: 6C:3B:6B:27:3B:DA

Firewall Router

Local Network

IP Address: 192.168.88.1

Netmask: 255.255.255.0 (/24)

DHCP Server

DHCP Server Range: 192.168.88.10-192.168.88.254

NAT

UPnP

VPN

VPN Access

VPN Address: BT2066c72e.ar.myname.net

System

Password:

Confirm Password:

Router OS WinBox

# QuickSet

- Easy to use
- Contains the most commonly used features and should be enough for basic usage

Golden rule about QuickSet:

**“If you use QuickSet, then use QuickSet, if you leave it, then forget about it...”**



# Simple security

# Simple security

- Specify user password

```
/user set admin password=***
```

- Use different username

```
/user set admin name=martins
```

The screenshot shows the Mikrotik WinBox interface for user management. The main window displays the 'User List' with a table containing two users: 'system default user' and 'martina'. The 'martina' user is selected, and a 'User (martina)' configuration dialog is open. In this dialog, the 'Name' field is set to 'martina' and the 'Group' is set to 'full'. Below the dialog, a 'Change Password' dialog is also visible, with 'New Password' and 'Confirm Password' fields. The interface includes a sidebar with various system settings and a top navigation bar with 'Session', 'Settings', and 'Dashboard' tabs.

Name	Group	Allowed Address	Last Logged In
system default user			
martina	full		

User (martina) configuration fields:

- Name: martina
- Group: full
- Allowed Address: [empty]
- Last Logged In: [empty]

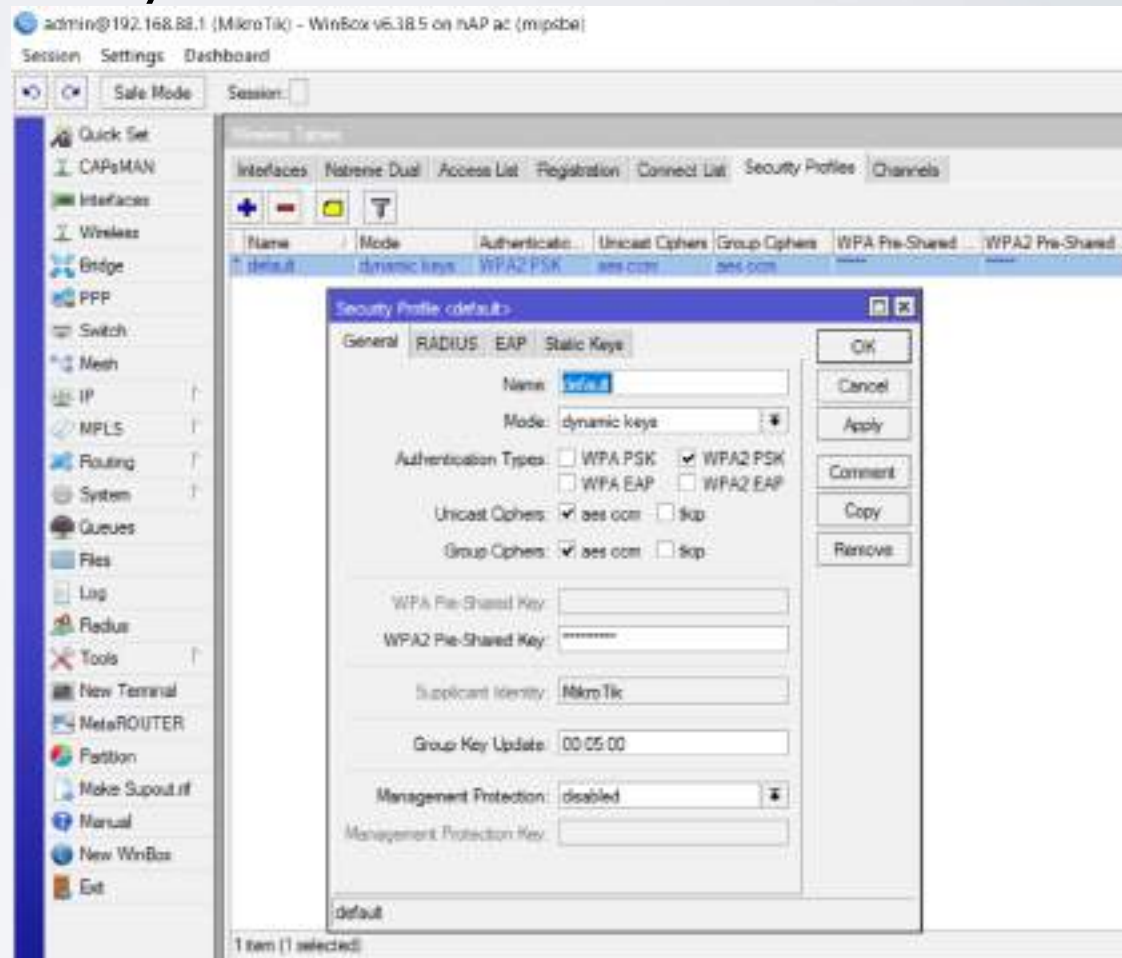
Change Password dialog fields:

- New Password: [masked]
- Confirm Password: [masked]

# Simple security

- Specify password for wireless access

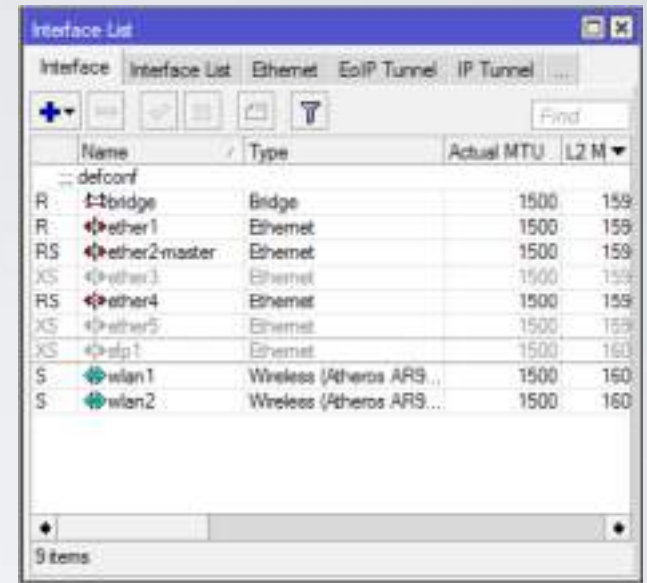
```
/interface wireless security-profiles set default authentication-types=wpa2-psk  
mode=dynamic-keys wpa2-pre-shared-key=*****
```



# Simple security

- Disable unused interfaces

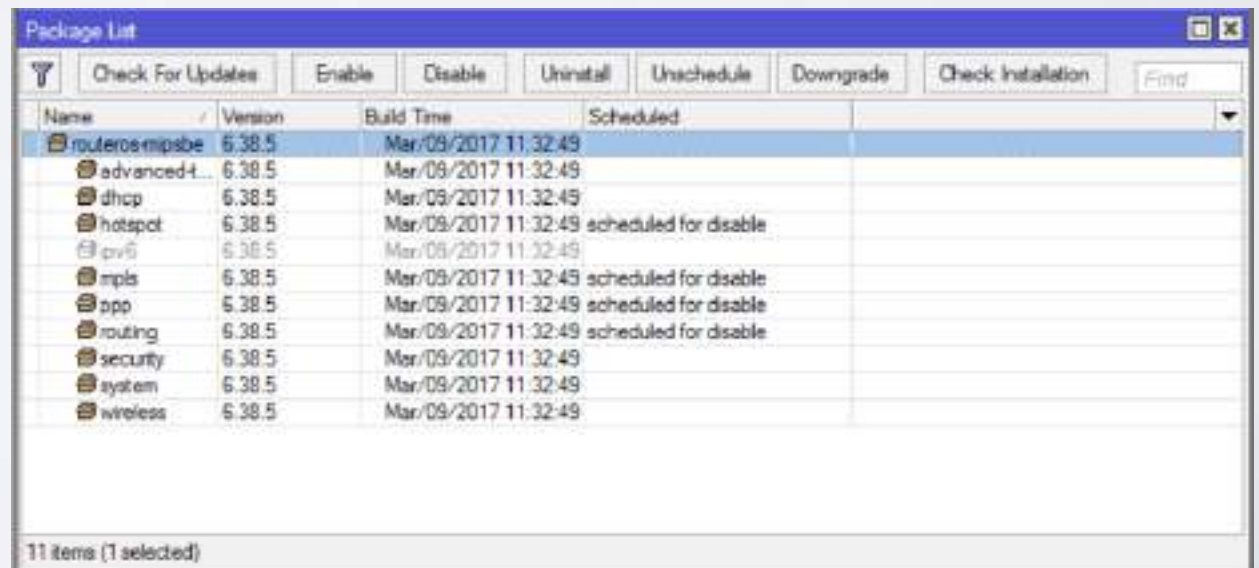
```
/interface ethernet disable ether3,ether5,sfp1
```



	Name	Type	Actual MTU	L2 MTU
	-- defconf			
R	ether1	Ethernet	1500	1500
RS	ether2-master	Ethernet	1500	1500
XS	ether3	Ethernet	1500	1500
RS	ether4	Ethernet	1500	1500
XS	ether5	Ethernet	1500	1500
XS	sfp1	Ethernet	1500	1600
S	wlan1	Wireless (Atheros ARS...)	1500	1600
S	wlan2	Wireless (Atheros ARS...)	1500	1600

- Disable unused packages (mainly IPv6)

```
/system package disable hotspot,ipv6,mpls,ppp,routing
```

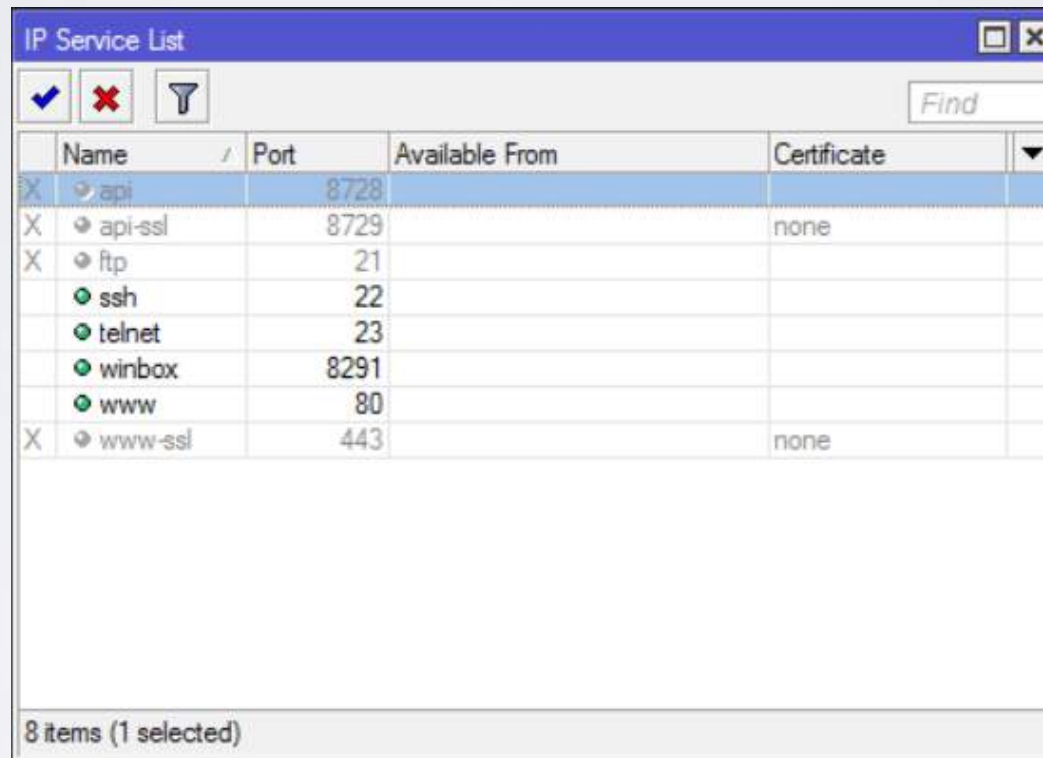


Name	Version	Build Time	Scheduled
routeros/mipsbe	6.38.5	Mar/09/2017 11:32:49	
advanced4...	6.38.5	Mar/09/2017 11:32:49	
dhcp	6.38.5	Mar/09/2017 11:32:49	
hotspot	6.38.5	Mar/09/2017 11:32:49	scheduled for disable
ipv6	6.38.5	Mar/09/2017 11:32:49	scheduled for disable
mpls	6.38.5	Mar/09/2017 11:32:49	scheduled for disable
ppp	6.38.5	Mar/09/2017 11:32:49	scheduled for disable
routing	6.38.5	Mar/09/2017 11:32:49	scheduled for disable
security	6.38.5	Mar/09/2017 11:32:49	
system	6.38.5	Mar/09/2017 11:32:49	
wireless	6.38.5	Mar/09/2017 11:32:49	

# Simple security

- Disable IP/Services

/ip service disable api,api-ssl,ftp,www-ssl



The screenshot shows a window titled "IP Service List" with a table of services. The table has columns for Name, Port, Available From, and Certificate. The 'api' service is selected and has a red 'X' in the first column, indicating it is disabled. Other services like 'api-ssl', 'ftp', 'ssh', 'telnet', 'winbox', 'www', and 'www-ssl' are also listed with their respective ports.

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

8 items (1 selected)

# Simple security

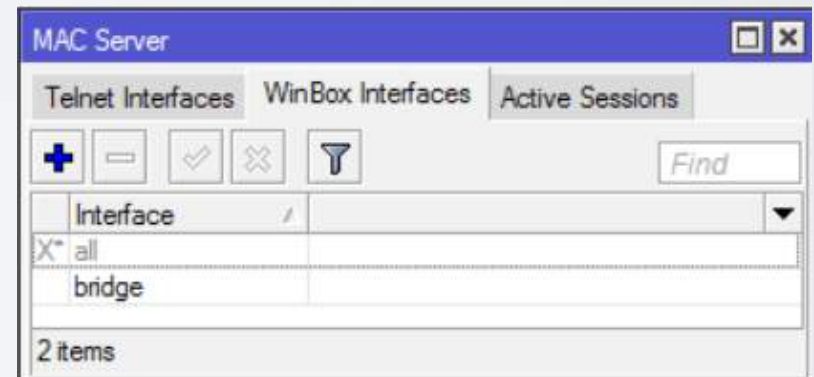
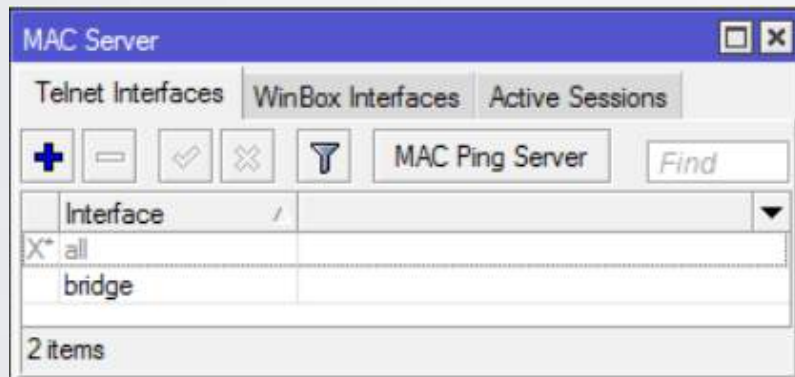
- Adjust MAC access

```
/tool mac-server set [ find default=yes ] disabled=yes
```

```
/tool mac-server add interface=bridge
```

```
/tool mac-server mac-winbox set [ find default=yes ] disabled=yes
```

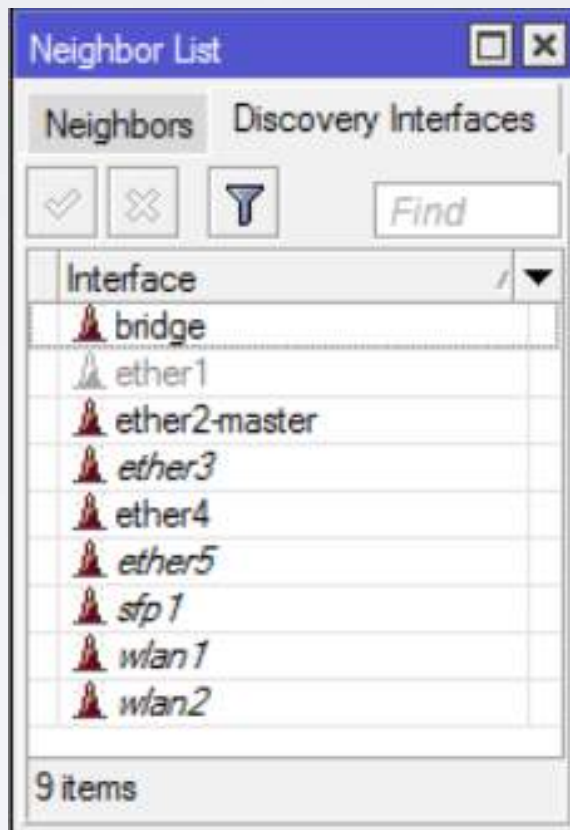
```
/tool mac-server mac-winbox add interface=bridge
```



# Simple security

- Hide device in Neighbor Discovery

```
/ip neighbor discovery set ether1 discover=no
```



# Simple security

- Disable serial port if not used (and if included)

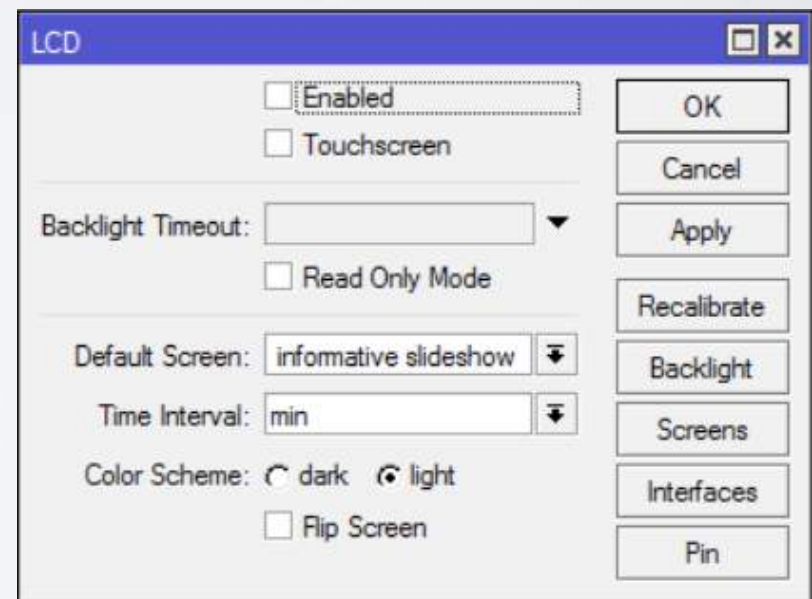
`/system console disable [find where port=serial0]`



- Disable LCD

`/lcd set enabled=no`

`/lcd set touch-screen=disabled`





# Simple security

- Protect reset button

```
/system routerboard settings set protected-routerboot=enabled reformat-hold-button=30s
```

[https://wiki.mikrotik.com/wiki/Manual:RouterBOARD\\_settings#Protected\\_bootloader](https://wiki.mikrotik.com/wiki/Manual:RouterBOARD_settings#Protected_bootloader)

# Firewall

# Firewall

## Two approaches

- Drop not trusted and allow trusted
- Allow trusted and drop untrusted

```
/ip firewall filter add chain=forward action=accept src-address=192.168.88.2 out-  
interface=ether1
```

```
/ip firewall filter add chain=forward action=drop src-address=192.168.88.0/24 out-  
interface=ether1
```

# Firewall

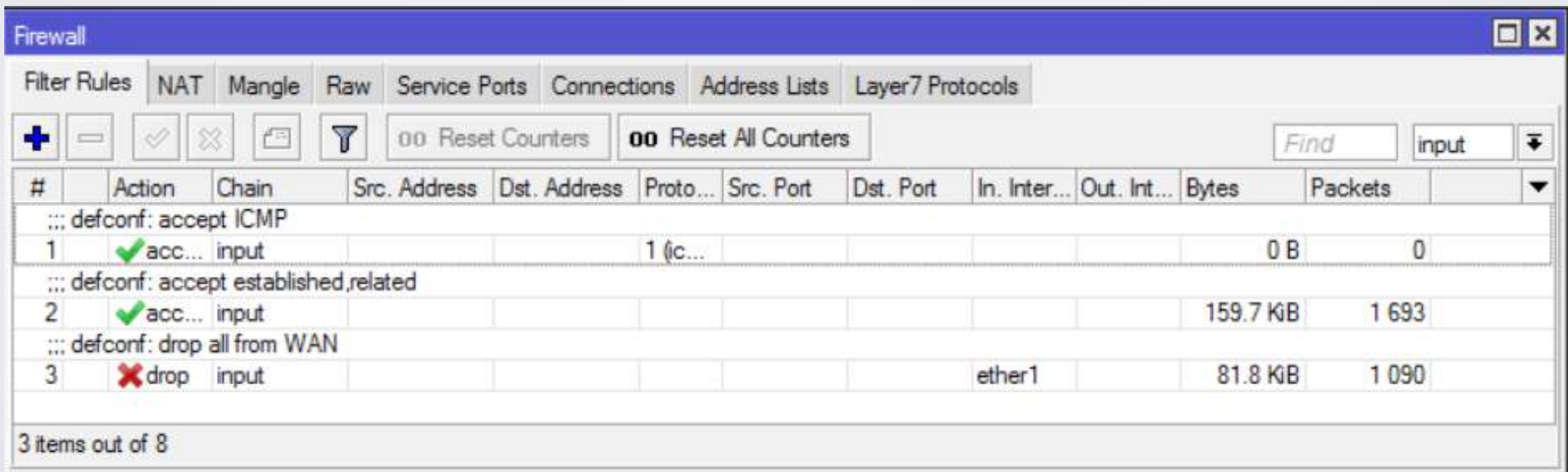
- Secure input

/ip firewall filter

add chain=input action=accept protocol=icmp

add chain=input action=accept connection-state=established,related

add chain=input action=drop in-interface=ether1



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The window title is "Firewall". The "Filter Rules" tab is selected, and the "input" chain is chosen. The table below shows the configuration of three filter rules.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
1	✓ acc...	input			1 (ic...					0 B	0
2	✓ acc...	input								159.7 KB	1 693
3	✗ drop	input						ether1		81.8 KB	1 090

3 items out of 8

# Firewall

- Secure forward

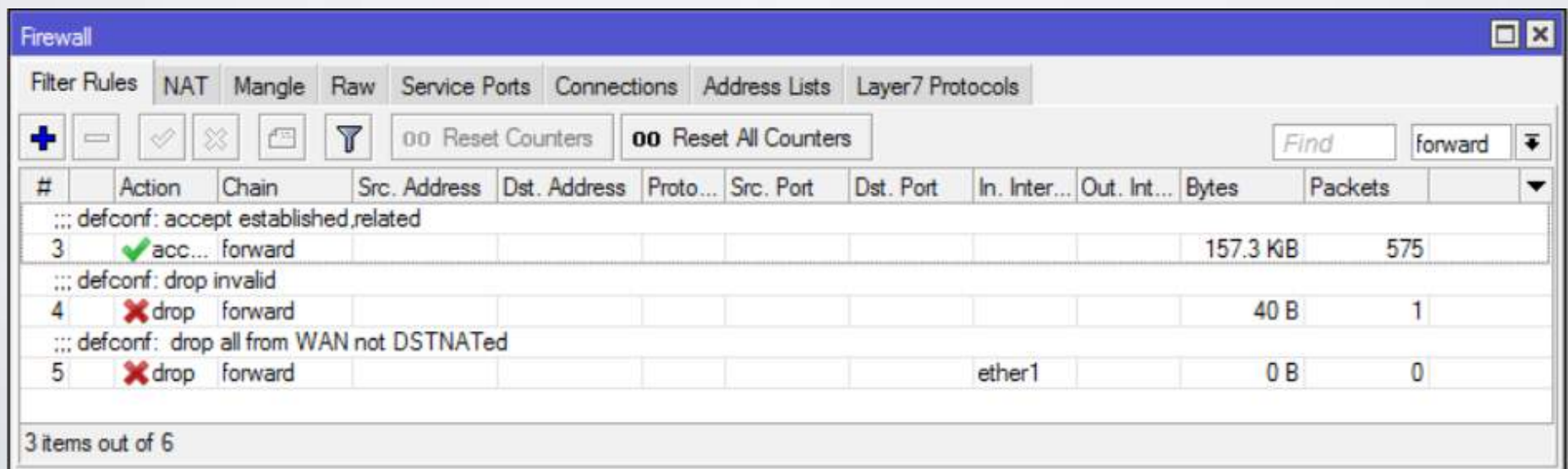
/ip firewall filter

add chain=forward action=accept connection-state=established,related

add chain=forward action=drop connection-state=invalid

add chain=forward action=drop connection-state=new connection-nat-state=!

dstnat in-interface=ether1



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The window title is "Firewall". The "Filter Rules" tab is selected, and the "forward" chain is chosen. The table below shows the configuration of three filter rules. The first rule (number 3) is "defconf: accept established,related" with an action of "accept" and a status of "checked". The second rule (number 4) is "defconf: drop invalid" with an action of "drop" and a status of "unchecked". The third rule (number 5) is "defconf: drop all from WAN not DSTNATED" with an action of "drop" and a status of "unchecked". The table also shows the number of bytes and packets for each rule.

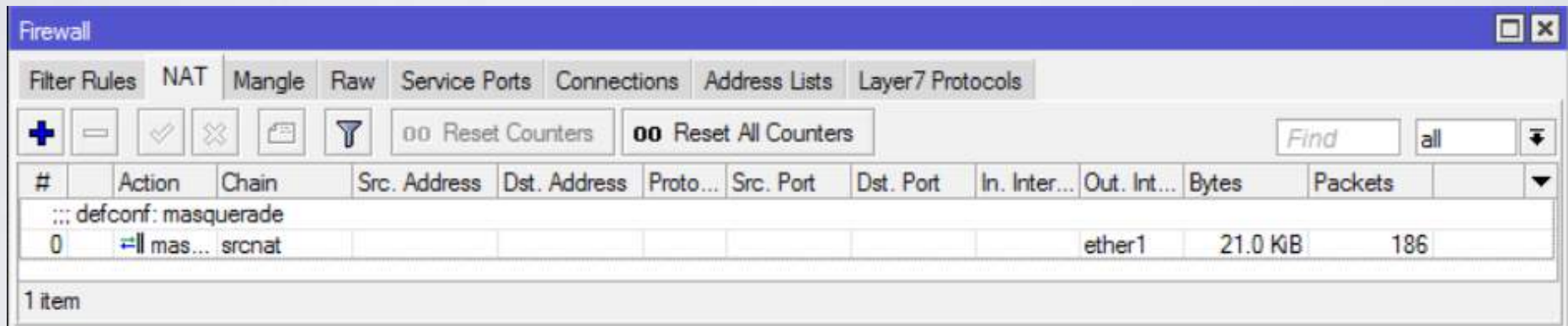
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
3	✓ acc...	forward								157.3 KiB	575
4	✗ drop	forward								40 B	1
5	✗ drop	forward						ether1		0 B	0

3 items out of 6

# Firewall

- NAT to outside (if you can, use src-nat instead of masquerade)

```
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
```



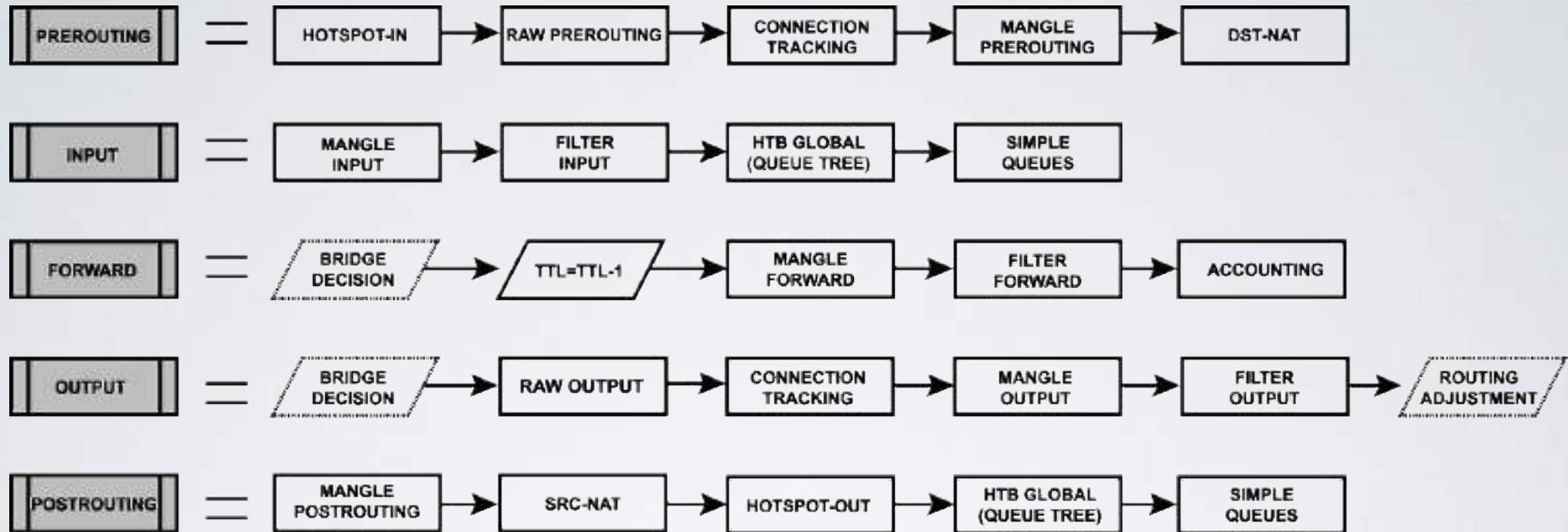
The screenshot shows the Mikrotik WinBox Firewall configuration window. The 'NAT' tab is selected. The configuration table shows a single rule with the following details:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	mas...	srcnat							ether1	21.0 KB	186

Below the table, it indicates '1 item'.

<https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/NAT#Masquerade>

# Firewall



[https://wiki.mikrotik.com/wiki/Manual:Packet\\_Flow\\_v6](https://wiki.mikrotik.com/wiki/Manual:Packet_Flow_v6)

# Firewall

- NAT to LAN

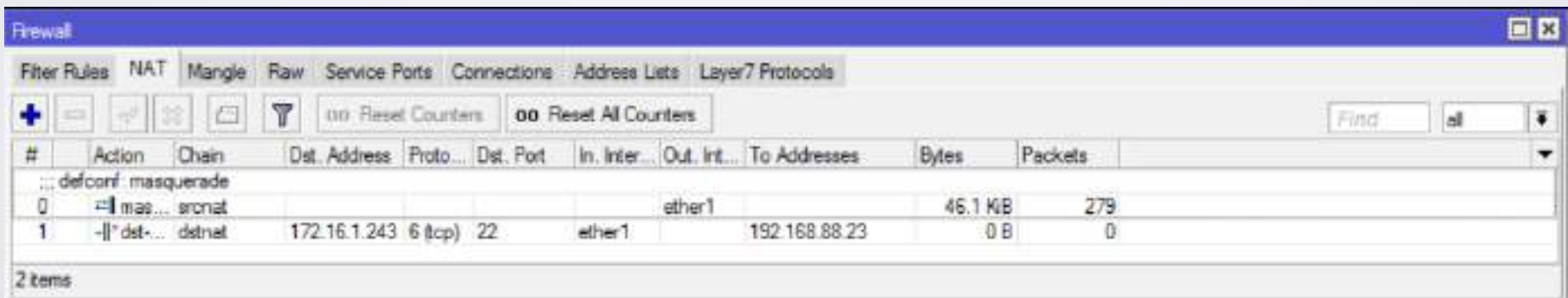
```
/ip firewall nat add chain=dstnat in-interface=ether1 protocol=tcp dst-port=22  
action=dst-nat dst-address=172.16.1.243 to-address=192.168.88.23
```

**Note:** In order to make port forwarding work you have to:

- Have dst-nat

- Have src-nat

- Accept traffic in forward chain (example in previous slides)



The screenshot shows the Mikrotik WinBox Firewall Rules configuration window. The 'Filter Rules' tab is active, and the 'dstnat' rule is selected. The rule configuration is as follows:

#	Action	Chain	Dst. Address	Proto...	Dst. Port	In. Inter...	Out. Int...	To Addresses	Bytes	Packets
0	masquerade	srcnat					ether1		46.1 KiB	279
1	dst-nat	dstnat	172.16.1.243	6 (tcp)	22	ether1		192.168.88.23	0 B	0

2 items



# Firewall

- Hairpin NAT (access local resource through public IP)

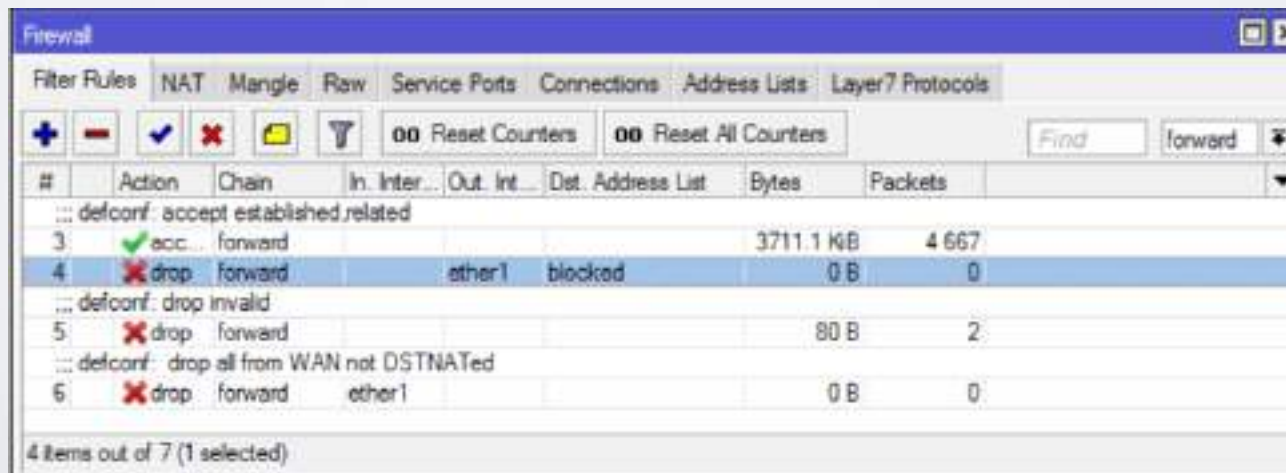
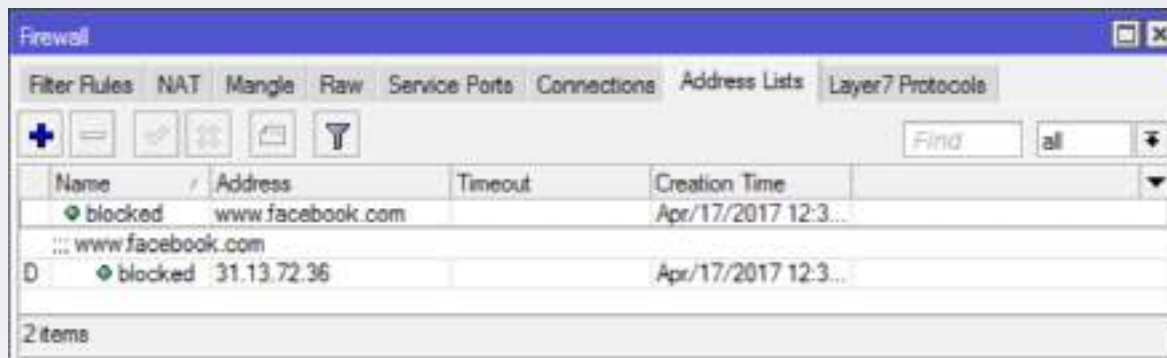
[https://wiki.mikrotik.com/wiki/Hairpin\\_NAT](https://wiki.mikrotik.com/wiki/Hairpin_NAT)

# Firewall

- Block specific traffic

```
/ip firewall address-list add list=blocked address=www.facebook.com
```

```
/ip firewall filter add chain=forward action=drop dst-address-list=blocked out-interface=ether1
```



# Firewall

- Protect device against attacks, if you allow particular access

```
/ip firewall filter
```

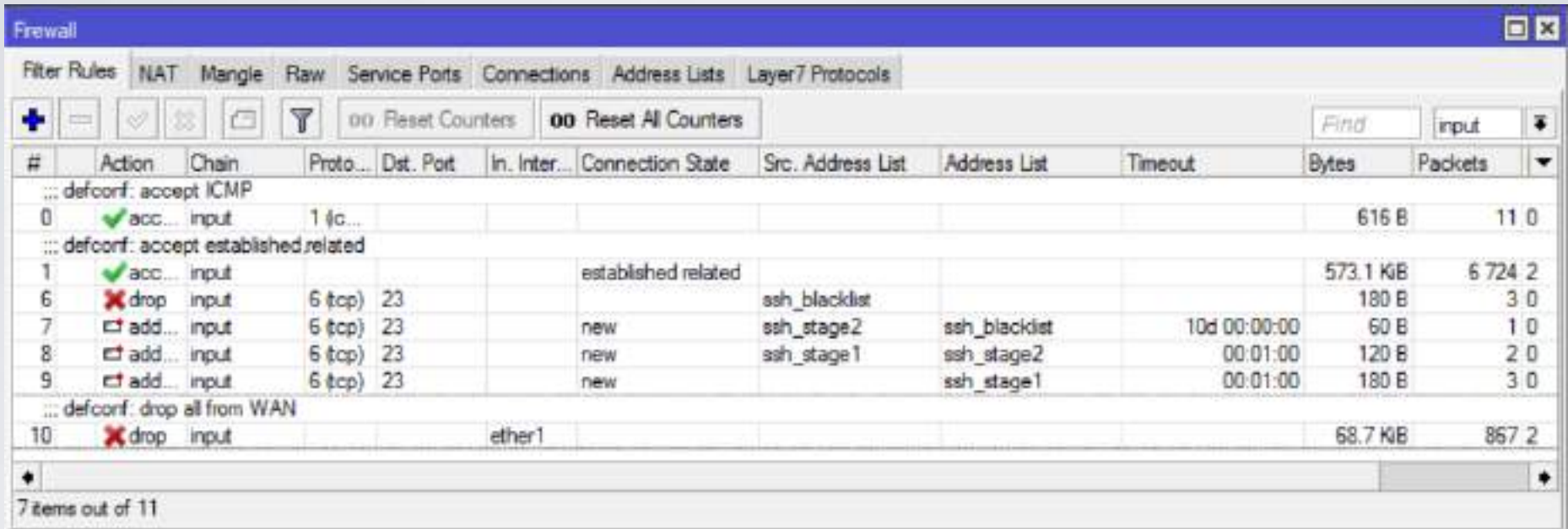
```
add chain=input protocol=tcp dst-port=23 src-address-list=ssh_blacklist  
action=drop
```

```
add chain=input protocol=tcp dst-port=23 connection-state=new src-address-  
list=ssh_stage2 action=add-src-to-address-list address-list=ssh_blacklist address-  
list-timeout=10d
```

```
add chain=input protocol=tcp dst-port=23 connection-state=new src-address-  
list=ssh_stage1 action=add-src-to-address-list address-list=ssh_stage2 address-list-  
timeout=1m
```

```
add chain=input protocol=tcp dst-port=23 connection-state=new action=add-src-  
to-address-list address-list=ssh_stage1 address-list-timeout=1m
```

# Firewall



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The window title is "Firewall". The "Filter Rules" tab is selected, and the "input" chain is chosen. The table below lists the configured rules.

#	Action	Chain	Proto...	Dst. Port	In. Inter...	Connection State	Src. Address List	Address List	Timeout	Bytes	Packets
::: defconf: accept ICMP											
0	✓ acc...	input	1 {c...							616 B	11 0
::: defconf: accept established,related											
1	✓ acc...	input				established,related				573.1 KB	6 724 2
6	✗ drop	input	6 {tcp}	23			ssh_blacklist			180 B	3 0
7	add...	input	6 {tcp}	23		new	ssh_stage2	ssh_blacklist	10d 00:00:00	60 B	1 0
8	add...	input	6 {tcp}	23		new	ssh_stage1	ssh_stage2	00:01:00	120 B	2 0
9	add...	input	6 {tcp}	23		new		ssh_stage1	00:01:00	180 B	3 0
::: defconf: drop all from WAN											
10	✗ drop	input			ether1					68.7 KB	857 2

7 items out of 11

[https://wiki.mikrotik.com/wiki/Bruteforce\\_login\\_prevention](https://wiki.mikrotik.com/wiki/Bruteforce_login_prevention)

**Handle bandwidth**

# FastTrack

- Remember this rule?

```
/ip firewall filter
```

```
add chain=forward action=accept connection-state=established,related
```

- Add FastTrack rule before previous one

```
/ip firewall filter
```

- add chain=forward action=fasttrack-connection connection-state=established,related

# FastTrack

The screenshot shows the Mikrotik WinBox Firewall configuration window. The 'Filter Rules' tab is active. A table lists firewall rules, with rule 3 selected. Rule 3 is a FastTrack rule named 'fastt...' in the 'forward' chain, with an action of 'fastt...' and a connection state of 'established related'. It has processed 675 bytes and 6 packets. Other rules include a dummy rule, a passthrough rule, and several default configuration rules.

#	Action	Chain	Proto...	Dst. Port	In. Inter...	Connection State	Src. Address List	Address List	Timeout	Bytes	Packets
::: special dummy rule to show fasttrack counters											
0	D pas...	forward								1570 B	3
::: defconf: accept established,related											
3	fastt...	forward				established related				675 B	6
::: defconf: accept established,related											
4	acc...	forward				established related				675 B	6
::: defconf: drop invalid											
5	drop	forward				invalid				0 B	0
::: defconf: drop all from WAN not DSTNATed											
6	drop	forward			ether1	new				0 B	0

5 items out of 8 (1 selected)

<https://wiki.mikrotik.com/index.php?title=Manual:IP/Fasttrack&redirect=no>

# Queues

- Add queues to limit traffic for specific resources

```
/queue simple add name=private target=192.168.88.243 max-limit=5M/5M
```

#	Name	Target	Upload Max Limit	Download Max Limit
0	queue1	192.168.88.243	5M	5M

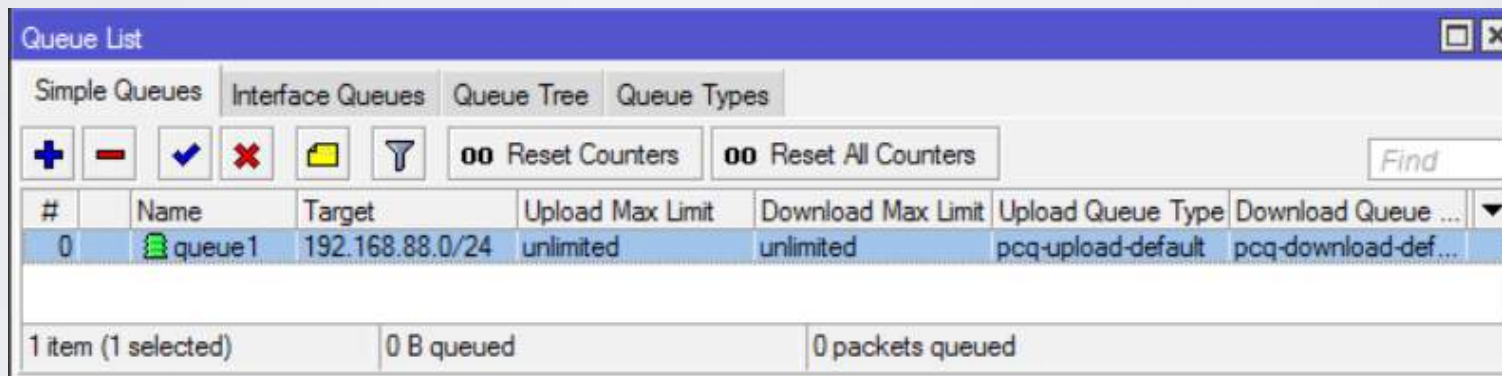
1 item      0 B queued      0 packets queued



# Queues

- Add queues to limit traffic equally (PCQ)

```
/queue simple add target-addresses=192.168.88.0/24 queue=pcq-upload-  
default/pcq-download-default
```



The screenshot shows the Mikrotik Queue List window. It has tabs for Simple Queues, Interface Queues, Queue Tree, and Queue Types. Below the tabs are several icons for adding, deleting, and filtering queues, along with buttons for 'Reset Counters' and 'Reset All Counters'. A search box labeled 'Find' is also present. The main table displays one queue configuration:

#	Name	Target	Upload Max Limit	Download Max Limit	Upload Queue Type	Download Queue ...
0	queue 1	192.168.88.0/24	unlimited	unlimited	pcq-upload-default	pcq-download-def...

At the bottom of the window, it shows '1 item (1 selected)', '0 B queued', and '0 packets queued'.

Few advices about queues

[https://wiki.mikrotik.com/wiki/Tips\\_and\\_Tricks\\_for\\_Beginners\\_and\\_Experience  
d\\_Users\\_of\\_RouterOS#Queues](https://wiki.mikrotik.com/wiki/Tips_and_Tricks_for_Beginners_and_Experience_d_Users_of_RouterOS#Queues)

**What to do when problem appears?**

# Logging

- Use logging for firewall

```
/ip firewall filter set [find where src-address-list=ssh_blacklist] log=yes log-prefix=BLACKLISTED:
```

- Use logging for debug topics

```
/system logging add topics=l2pt,debug action=memory
```

- Logging to disk or remote server

```
/system logging action set disk disk-file-name=l2tp_logs disk-file-count=5 disk-lines-per-file=1000
```

```
/system logging action set remote remote=192.168.88.3
```



# Debugging tools

- Torch

Analyse processed traffic

[https://wiki.mikrotik.com/wiki/Manual:Troubleshooting\\_tools#Torch\\_.28.2Ftool\\_to\\_rch.29](https://wiki.mikrotik.com/wiki/Manual:Troubleshooting_tools#Torch_.28.2Ftool_to_rch.29)

The screenshot shows the Mikrotik Torch interface. The 'Basic' tab is active, showing the interface 'bridge-local' and an entry timeout of '00:00:03'. The 'Collect' section has checkboxes for 'Src. Address', 'Dst. Address', 'MAC Protocol', 'Protocol', 'DSCP', 'Src. Address6', 'Dst. Address6', 'Port', and 'VLAN Id'. The 'Filters' section includes fields for 'Src. Address', 'Dst. Address', 'Src. Address6', 'Dst. Address6', 'MAC Protocol', 'Protocol', 'Port', 'VLAN Id', and 'DSCP'. On the right, there are buttons for 'Start', 'Stop', 'Close', and 'New Window'. Below the configuration is a table of traffic entries.

Et...	Prot...	Src.	Dest	VLAN id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...	
800 (p)	6 (tcp)	172.16.1.243:55392	172.16.1.1:8291 (winbox)			156.3 k...	4.9 kbps	14	7	
800 (p)	17 (...)	172.16.1.251:20148	85.234.190.33:17943			34.3 kbps	2.0 Mbps	68	178	
800 (p)	17 (...)	172.16.1.251:137 (netbios...)	172.16.1.255:137 (netbios...)			0 bps	0 bps	0	0	
800 (p)	17 (...)	172.16.1.251:20148	78.84.230.93:55480			0 bps	11.8 kbps	0	1	
800 (p)	17 (...)	255.255.255.255:5246	172.16.1.1:57768			0 bps	0 bps	0	0	
800 (p)	17 (...)	255.255.255.255:5678 (d...)	172.16.1.1:55572			0 bps	0 bps	0	0	
800 (p)	17 (...)	172.16.1.251:49541	239.255.255.250:1900			0 bps	0 bps	0	0	
800 (p)	17 (...)	172.16.1.251:49541	172.16.1.1:1900			0 bps	0 bps	0	0	

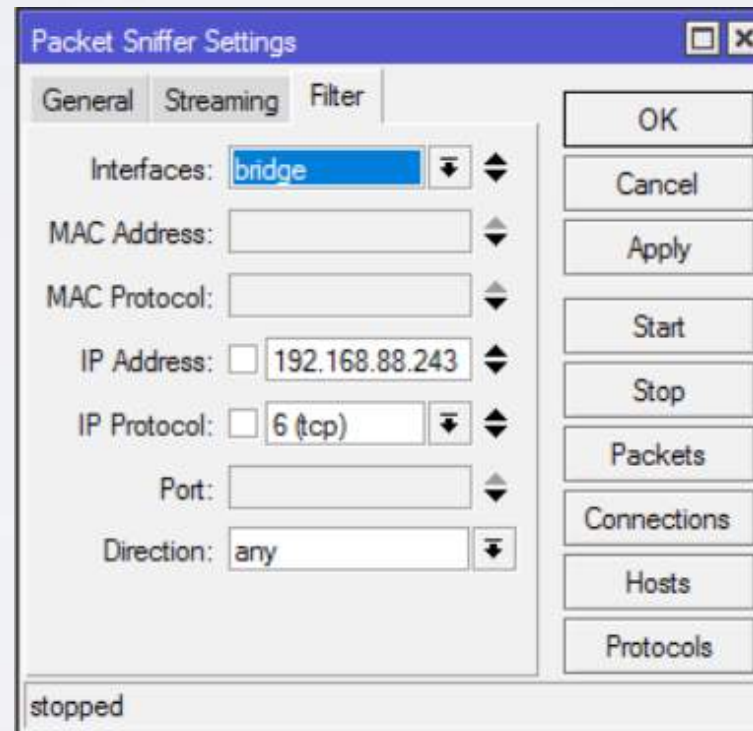
8 items    Total Tx: 190.6 kbps    Total Rx: 2.1 Mbps    Total Tx Packet: 82    Total Rx Packet: 186

# Debugging tools

- Sniffer

Analyse processed packets

[https://wiki.mikrotik.com/wiki/Manual:Troubleshooting\\_tools#Packet\\_Sniffer\\_.28.2Ftool\\_sniffer.29](https://wiki.mikrotik.com/wiki/Manual:Troubleshooting_tools#Packet_Sniffer_.28.2Ftool_sniffer.29)

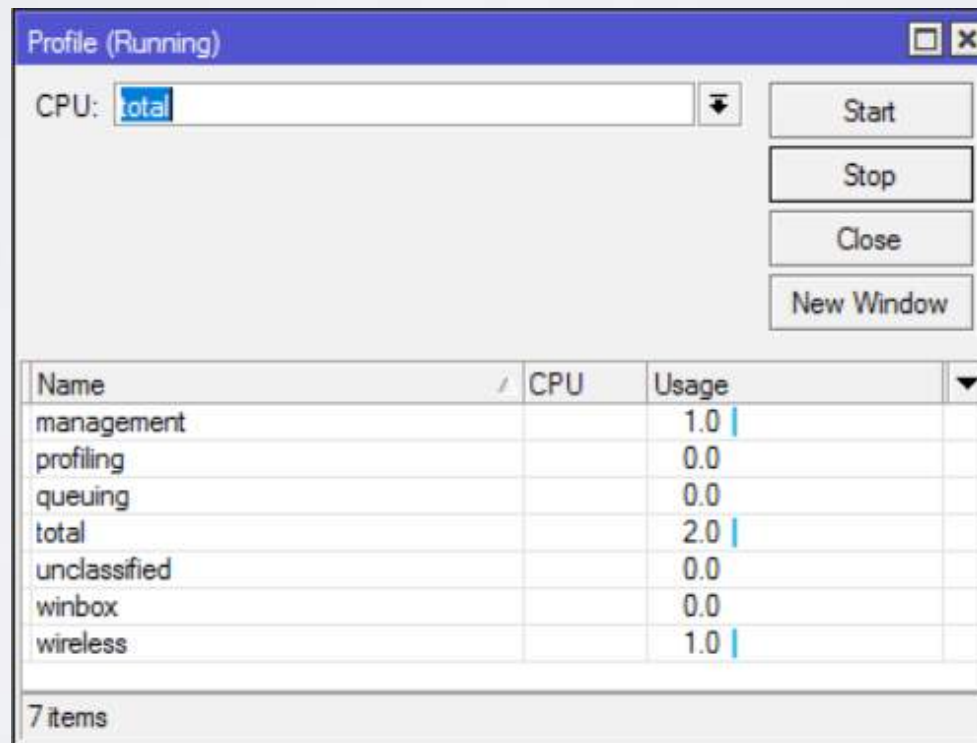


# Debugging tools

- Profiler

Find out current CPU usage

<https://wiki.mikrotik.com/wiki/Manual:Tools/Profiler>



The screenshot shows the 'Profile (Running)' window of the Mikrotik Profiler tool. At the top, there is a dropdown menu for 'CPU:' set to 'total'. To the right of this menu are four buttons: 'Start', 'Stop', 'Close', and 'New Window'. Below these controls is a table with the following data:

Name	CPU	Usage
management		1.0
profiling		0.0
queuing		0.0
total		2.0
unclassified		0.0
winbox		0.0
wireless		1.0

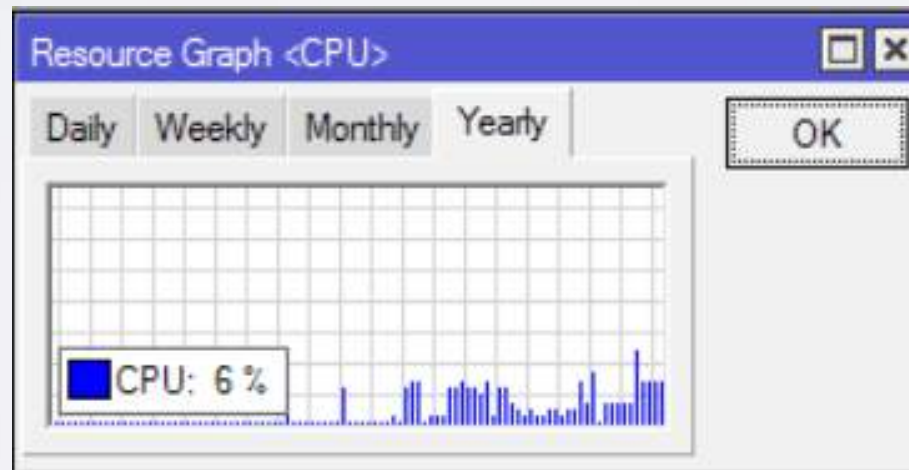
At the bottom left of the window, it indicates '7 items'.

# Debugging tools

- Graphing

Find out information about Interfaces/Queues/Resources per interval:

<https://wiki.mikrotik.com/wiki/Manual:Tools/Graphing>





# Debugging tools

- The Dude

Powerful network monitoring tool:

[https://wiki.mikrotik.com/wiki/Manual:The\\_Dude](https://wiki.mikrotik.com/wiki/Manual:The_Dude)

**Keep features and fixes up-to-date**

# Upgrade device

- Release candidate

The most up-to-date version (hardly tested) with all possible features (also half-implemented) and fixes

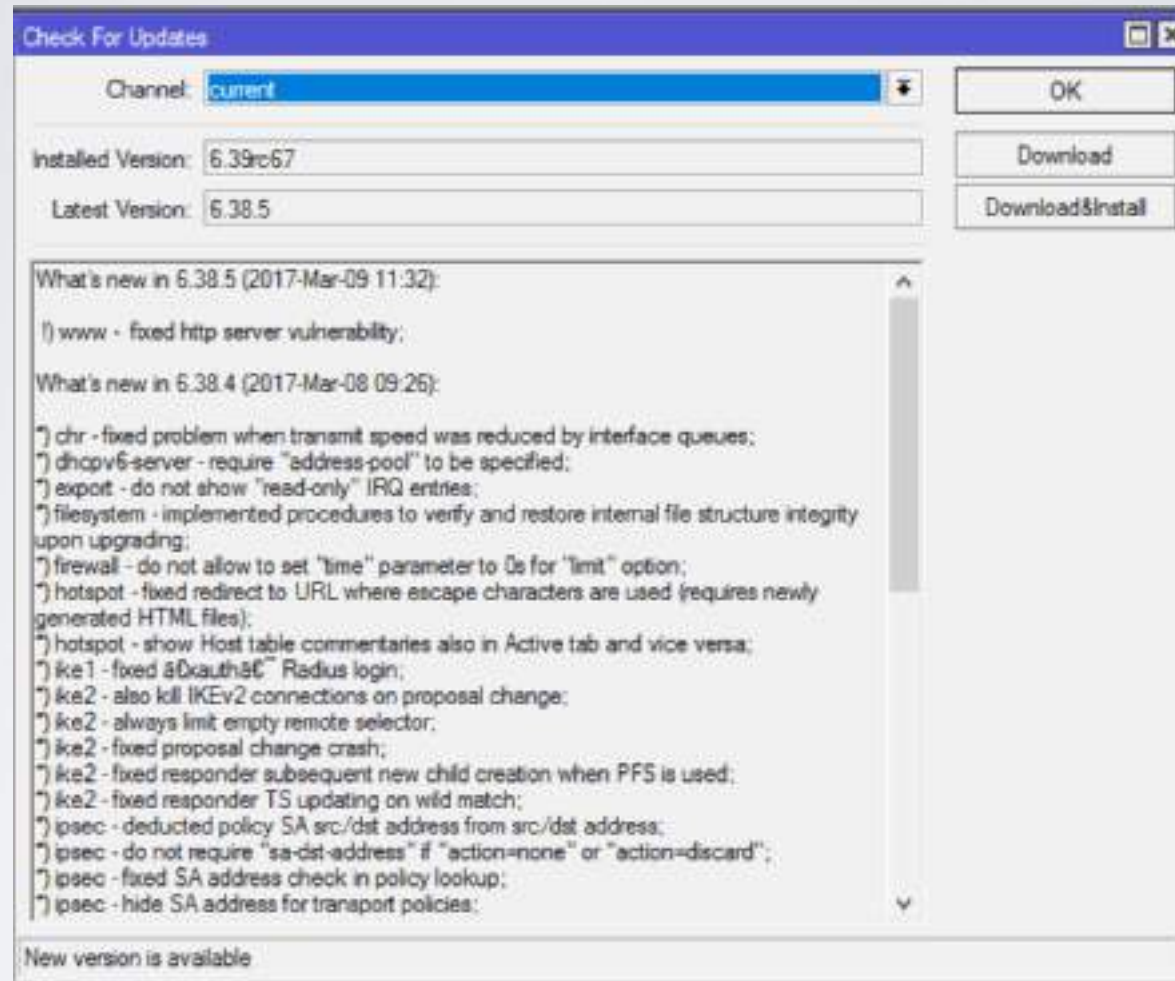
- Current

Latest full release (tested on many different scenarios for long time) with all fully implemented features

- Bugfix

Latest full release (tested on many different scenarios for long time and admitted as trustworthy) with all safe fixes

# Upgrade device



[https://wiki.mikrotik.com/wiki/Manual:Upgrading\\_RouterOS](https://wiki.mikrotik.com/wiki/Manual:Upgrading_RouterOS)

**What to do when software stops working?**

# Resolve problems

- Backup RouterBOOT

- 1) Power device off, press and hold the reset button

- 2) Power device on and after 1-2 seconds release the button

- Netinstall

- 1) Test Netinstall

<https://wiki.mikrotik.com/wiki/Manual:Netinstall>

- 2) Try to re-install any other router

- Reset device

<https://wiki.mikrotik.com/wiki/Manual:Reset>

# Resolve problems

- Serial port
  - 1) Shows all available information (also booting)
  - 2) Will work if problem is related to Layer2/Layer3 connectivity and/or interfaces themselves
- Exchange device
- Choose more powerful device (or multiple devices)

I can not figure it out by myself



# Configuration issues

- Consultants/Distributors:
  - <https://mikrotik.com/consultants>
  - <https://mikrotik.com/buy>
- Ask for help in forum:
  - <https://forum.mikrotik.com/>
- Look for an answer in manual
  - [https://wiki.mikrotik.com/wiki/Main\\_Page](https://wiki.mikrotik.com/wiki/Main_Page)

**What to do when hardware stops working?**

# Hardware issues

- Replace involved accessories
  - Power adapter
  - PoE
  - Cables
  - Interfaces (SFP modules, wireless cards, etc.)
  - Power source

Support

# Software issues

- Configuration is not working properly

Logs and supout file

[https://wiki.mikrotik.com/wiki/Manual:Support\\_Output\\_File](https://wiki.mikrotik.com/wiki/Manual:Support_Output_File)

- Out of memory

- 1) Upgrade device (mandatory)

- 2) Reboot device and generate supout file (normal situation)

- 3) When RAM is almost full generate another supout file  
(problematic situation)

# Software issues

- Device freeze
  - 1) Upgrade device (mandatory)
  - 2) Connect serial console and monitor device
  - 3) Generate supout file (problematic situation)
  - 4) Copy serial output to text file
- Any other kind of issue (for example reboot)
  - 1) Upgrade device (mandatory)
  - 2) Reproduce problem or wait for it to appear
  - 3) Generate supout file (problematic situation)

# Support

- Briefly explain what has happened
- When it happens
- What did you do to make it happen
- Send all files (mentioned in previous slides depending on problem)
- Do everything what is asked, if it is possible
- Make notes and document results (even if problem persists)
- Make new files after configuration changes
- Reply within same ticket and provide new information

Enjoy the MUM!