



Basic guidelines on RouterOS configuration and debugging

Pauls Jukonis

MikroTik, Latvia

Colombo, Sri Lanka

June 2017

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>

QuickSet

The fastest way how to configure device

The screenshot shows the Mikrotik WinBox QuickSet configuration window for a Home AP Dual. The interface is divided into several sections:

- Left Sidebar:** A navigation menu with icons for various configuration areas: Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, Partition, Make Supout.tif, Manual, New WinBox, and Exit.
- Top Bar:** Displays the user 'admin@192.168.88.1 (MikroTik) - WinBox v6.38.5 on hAP ac (mipsbe)' and navigation buttons for Session, Settings, and Dashboard. It also includes a 'Safe Mode' button and a 'Session:' field.
- Main Configuration Area:**
 - Home AP Dual:** A dropdown menu is open, showing options: CAP, CPE, Home AP Dual (selected), PTP Bridge, and WISP AP.
 - 2GHz and 5GHz Settings:** Fields for Network Name (MikroTik-279BE1 and MikroTik-279BE0), Frequency (auto), Band (2GHz-B/G/N and 5GHz-A/N/AC), and Country (no_country_set). There is a checkbox for 'Use Access List (ACL)' and a 'WPS Accept' button.
 - Guest Wireless Network:** A field for 'Guest Network:'.
 - Wireless Clients:** A table with columns: MAC Address, In ACL, Last IP, Uptime, and Signal Strength. Below the table is a 'Signal Strength:' legend.
 - Buttons:** 'Copy To ACL' and 'Remove From ACL' buttons are located at the bottom of the Wireless Clients section.
- Internet Section:**
 - Port: Eth1
 - Address Acquisition: Static, Automatic (selected), PPPoE
 - IP Address: 172.16.1.243 (with Renew and Release buttons)
 - Netmask: 255.255.255.0 (/24)
 - Gateway: 172.16.1.1
 - MAC Address: 6C:3B:6B:27:9B:DA
 - Firewall Router:
- Local Network Section:**
 - 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 Section:**
 - VPN Access:
 - VPN Address: 6f120665c726.sn.mynetname.net
- System Section:** Includes 'Check For Updates' and 'Reset Configuration' buttons.
- Bottom:** Password and Confirm Password fields.

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 configuration. The top bar indicates the user is 'admin@192.168.88.1 (MikroTik) - WinBox v6.38.5 on hAP ac (mipsbe)'. The main menu on the left includes options like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, Partition, Make Supout.rif, Manual, New WinBox, and Exit.

The 'User List' window is open, showing a table with columns: Name, Group, Allowed Address, and Last Logged In. The table contains two entries: 'system default user' and 'martins' (group: full). The 'martins' user is selected.

The 'User <martins>' configuration window is open, showing the following fields:

- Name: martins
- Group: full
- Allowed Address: (empty)
- Last Logged In: (empty)

Buttons on the right include OK, Cancel, Apply, Disable, Comment, Copy, Remove, and Password... The 'enabled' checkbox is checked.

The 'Change Password' window is also open, showing:

- New Password: (masked with dots)
- Confirm Password: (masked with dots)

Buttons on the right include OK, Cancel, and Apply. The status bar at the bottom indicates '1 item (1 selected)'.

Simple security

- Specify password for wireless access

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

The screenshot shows the Mikrotik WinBox interface. The top bar indicates the user is 'admin@192.168.88.1 (MikroTik) - WinBox v6.38.5 on hAP ac (mipsbe)'. The main window is titled 'Wireless Tables' and has several tabs: 'Interfaces', 'Nstreme Dual', 'Access List', 'Registration', 'Connect List', 'Security Profiles', and 'Channels'. The 'Security Profiles' tab is active, showing a table with columns: Name, Mode, Authentication..., Unicast Ciphers, Group Ciphers, WPA Pre-Shared..., and WPA2 Pre-Shared... The table contains one entry: 'default' with mode 'dynamic keys', authentication 'WPA2 PSK', unicast ciphers 'aes ccm', group ciphers 'aes ccm', and both WPA and WPA2 pre-shared keys set to '*****'. A dialog box titled 'Security Profile <default>' is open, showing the configuration for the 'default' profile. The 'General' tab is selected, and the 'Name' is 'default' and 'Mode' is 'dynamic keys'. Under 'Authentication Types', 'WPA2 PSK' is checked. Under 'Unicast Ciphers', 'aes ccm' is checked. Under 'Group Ciphers', 'aes ccm' is checked. The 'WPA2 Pre-Shared Key' field is filled with '*****'. The 'Supplicant Identity' is 'MikroTik' and 'Group Key Update' is '00:05:00'. 'Management Protection' is set to 'disabled'. The dialog has buttons for 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove'. The bottom status bar shows '1 item (1 selected)'.

Simple security

- Disable unused interfaces

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

Name	Type	Actual MTU	L2 M
bridge	Bridge	1500	159
ether1	Ethernet	1500	159
ether2-master	Ethernet	1500	159
ether3	Ethernet	1500	159
ether4	Ethernet	1500	159
ether5	Ethernet	1500	159
sfp1	Ethernet	1500	160
wlan1	Wireless (Atheros AR9...	1500	160
wlan2	Wireless (Atheros AR9...	1500	160

- Disable unused packages (mainly IPv6)

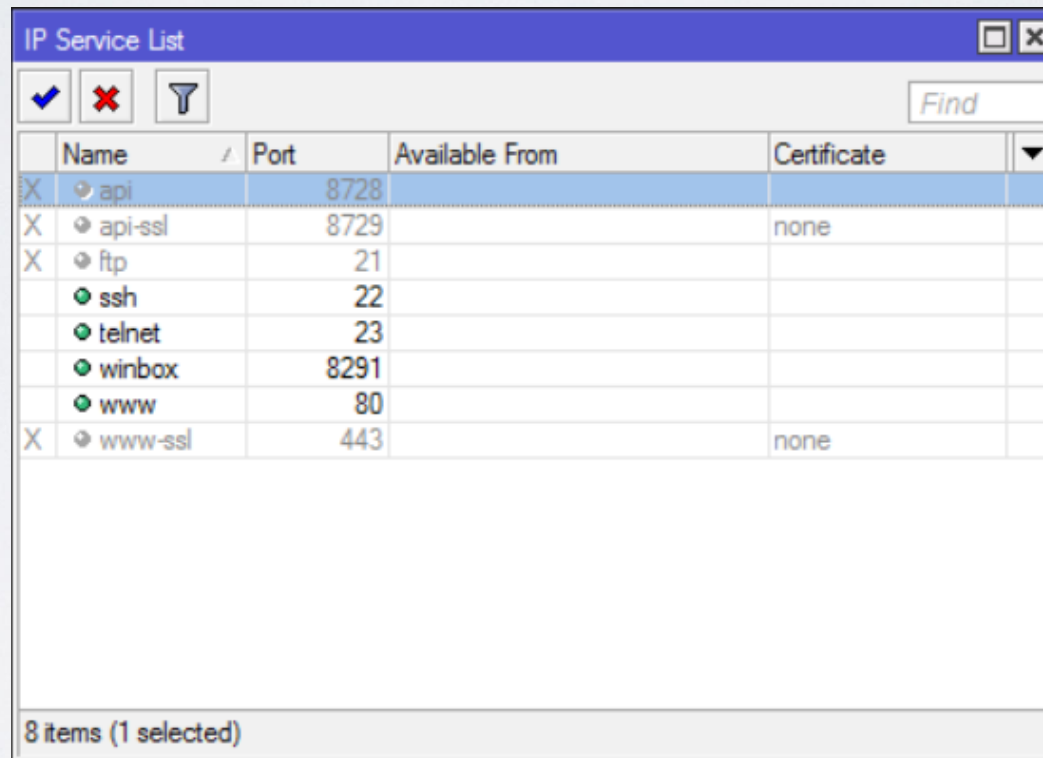
```
/system package disable hotspot,ipv6,mpls,ppp,routing
```

Name	Version	Build Time	Scheduled
routeros-mipsbe	6.38.5	Mar/09/2017 11:32:49	
advancedt...	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	
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 disabled, indicated by an 'X' in the first column. Other services like 'api-ssl', 'ftp', 'ssh', 'telnet', 'winbox', 'www', and 'www-ssl' are also listed with their respective ports. The 'Certificate' column shows 'none' for 'api-ssl' and 'www-ssl'. The status bar at the bottom indicates "8 items (1 selected)".

	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

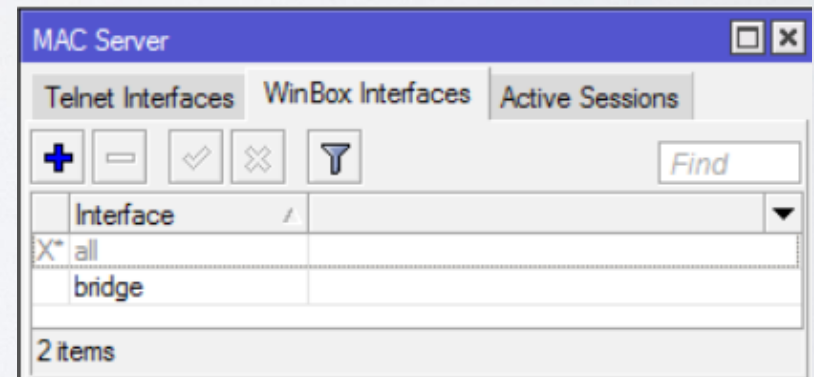
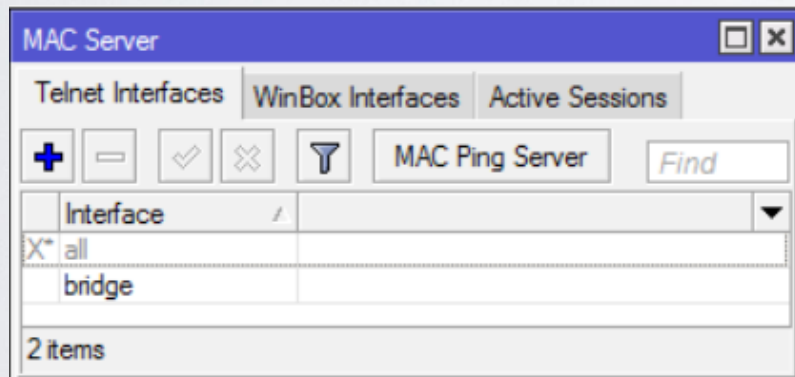
- Adjust MAC access

```
/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
```

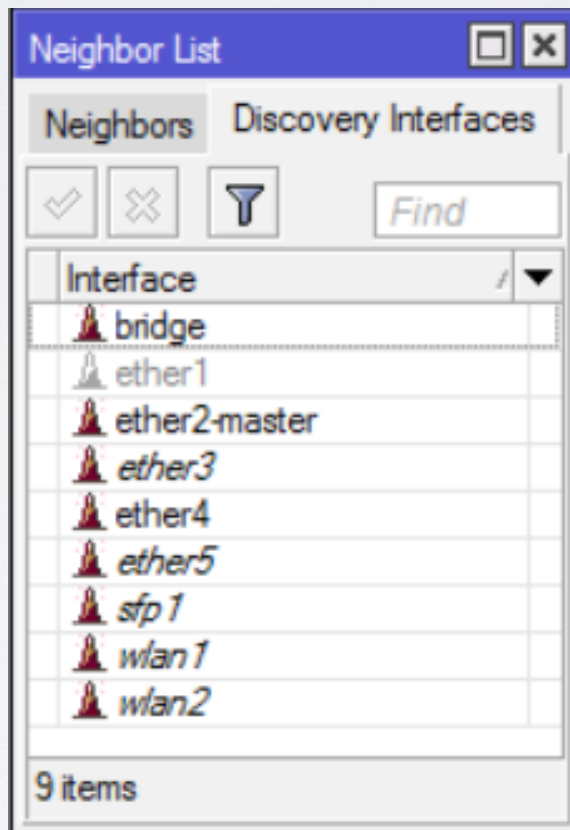
```
/tool mac-server mac-winbox add interface=bridge
```



Simple security

- Hide device in Neighbor Discovery

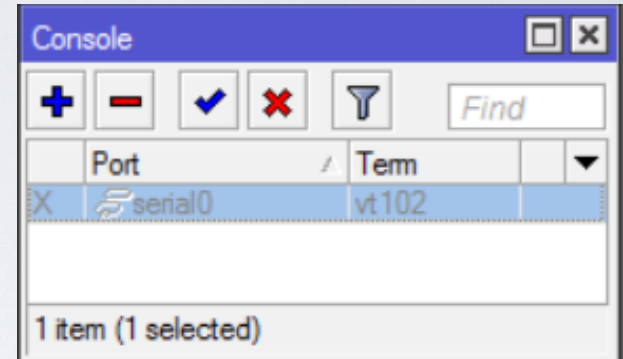
```
/ip neighbor discovery set ether1 discover=no
```



Simple security

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

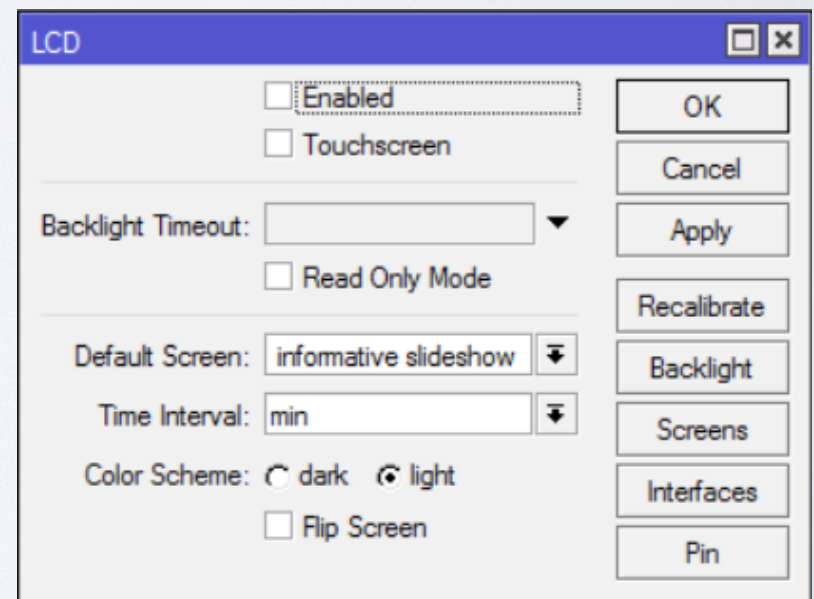
`/system console disable [find where port=serial0]`



- 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

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

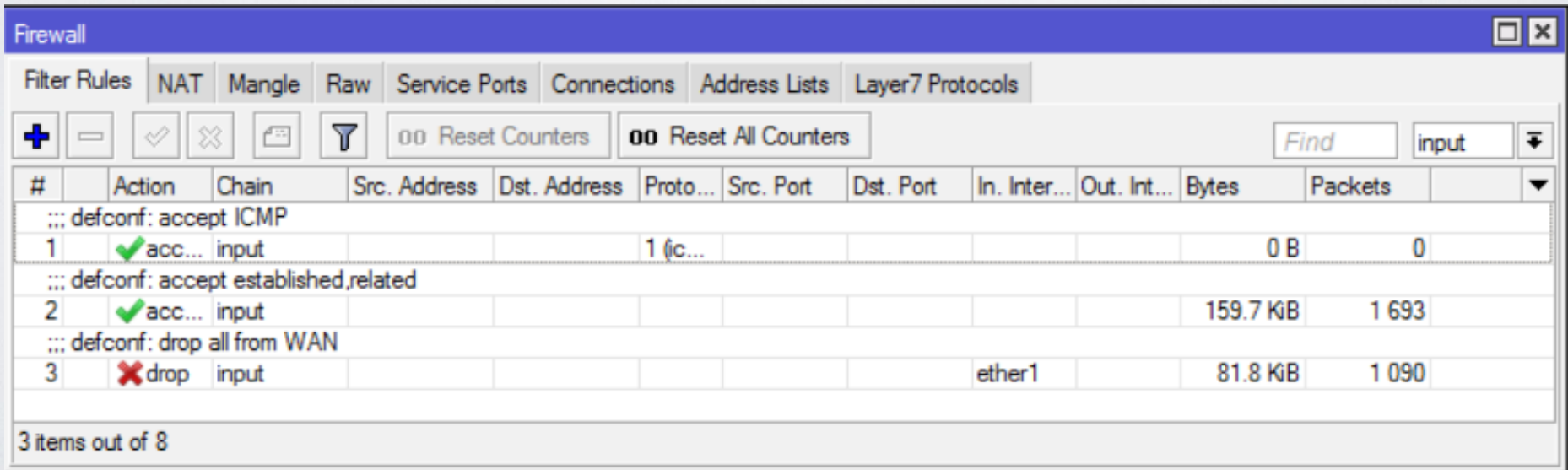
- Secure input

/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, with other tabs including NAT, Mangle, Raw, Service Ports, Connections, Address Lists, and Layer7 Protocols. The interface includes a toolbar with icons for adding, deleting, enabling, disabling, and refreshing rules, along with buttons for "Reset Counters" and "Reset All Counters". A search bar contains the text "Find" and a dropdown menu is set to "input". The main area displays a table of filter rules with the following data:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
::: defconf: accept ICMP											
1	✓ acc...	input			1 (ic...					0 B	0
::: defconf: accept established,related											
2	✓ acc...	input								159.7 KB	1 693
::: defconf: drop all from WAN											
3	✗ drop	input						ether1		81.8 KB	1 090

At the bottom of the window, it indicates "3 items out of 8".

Firewall

- Secure forward

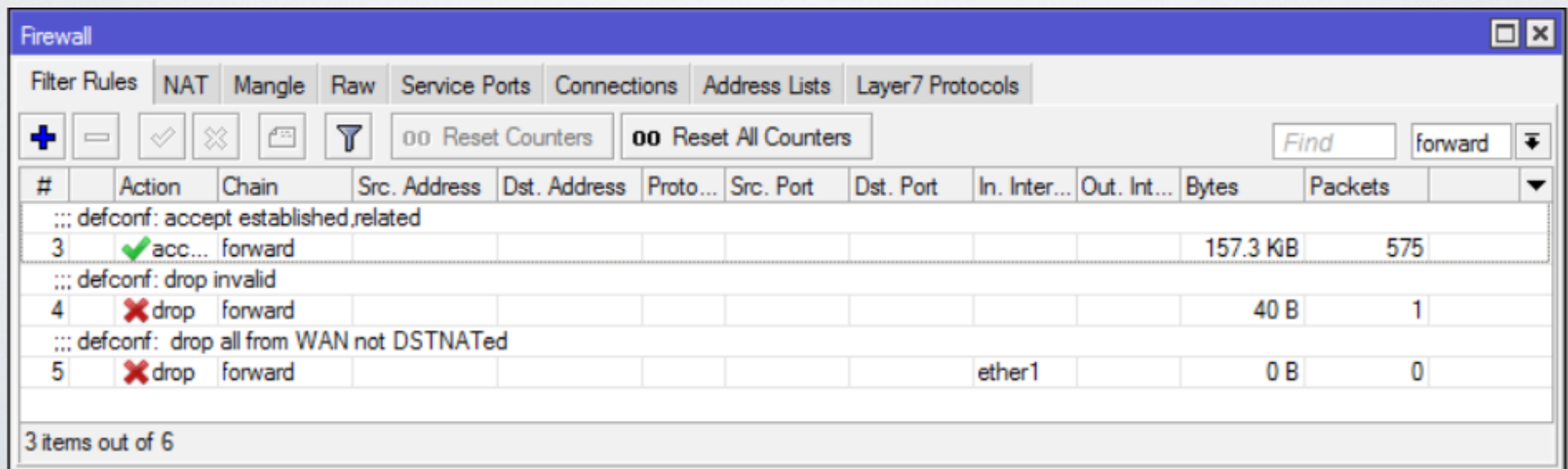
/ip firewall filter

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



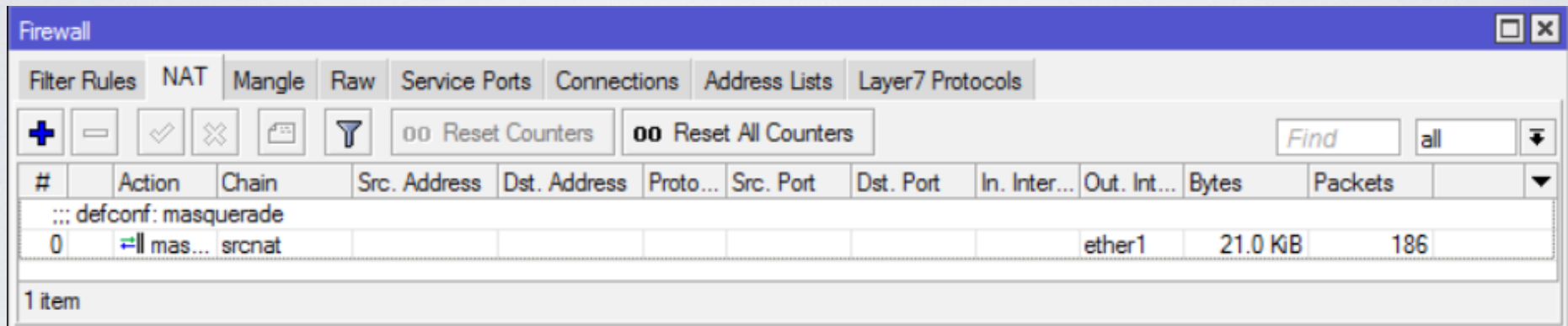
The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is active, showing a table of rules. The table has columns for #, Action, Chain, Src. Address, Dst. Address, Proto..., Src. Port, Dst. Port, In. Inter..., Out. Int..., Bytes, and Packets. Three rules are visible, with the first one selected. The status bar at the bottom indicates '3 items out of 6'.

#	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

Firewall

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

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



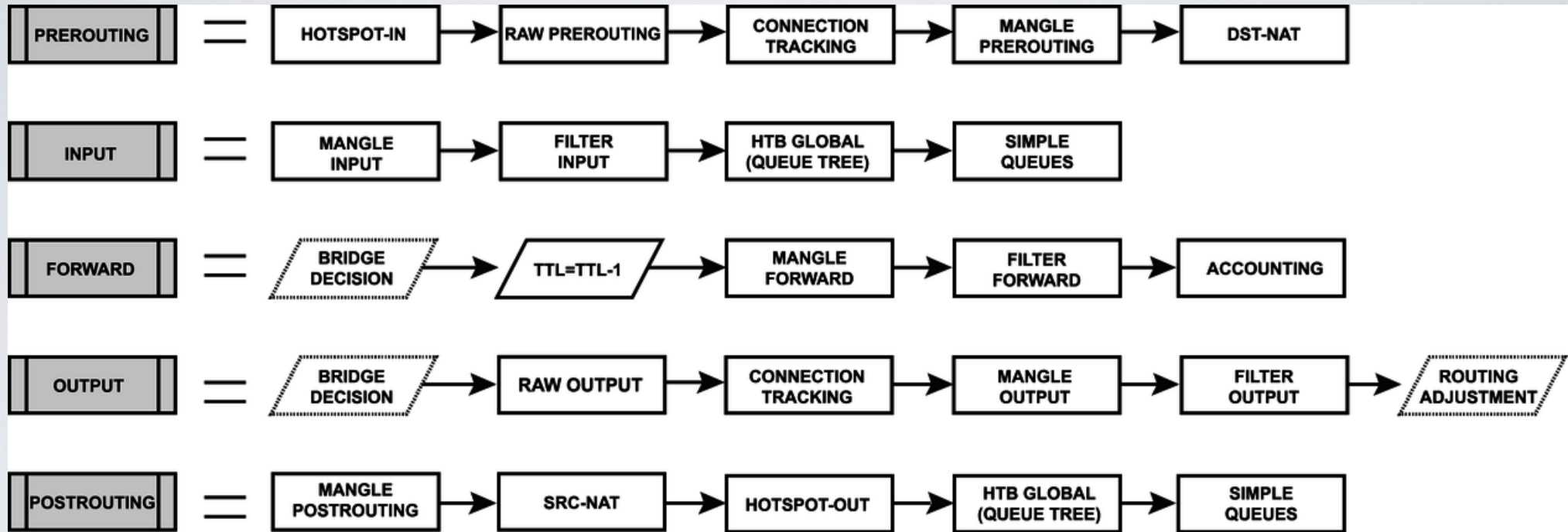
The screenshot shows the Mikrotik WinBox Firewall configuration window, specifically the NAT tab. The window title is "Firewall". The tabs include Filter Rules, NAT (selected), Mangle, Raw, Service Ports, Connections, Address Lists, and Layer7 Protocols. Below the tabs are several control buttons: a plus sign, a minus sign, a checkmark, a cross, a document icon, a funnel icon, and two buttons labeled "00 Reset Counters" and "00 Reset All Counters". There is also a search field with the text "Find" and a dropdown menu set to "all".

#	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

1 item

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

Firewall



https://wiki.mikrotik.com/wiki/Manual:Packet_Flow_v6

Firewall

- NAT to LAN

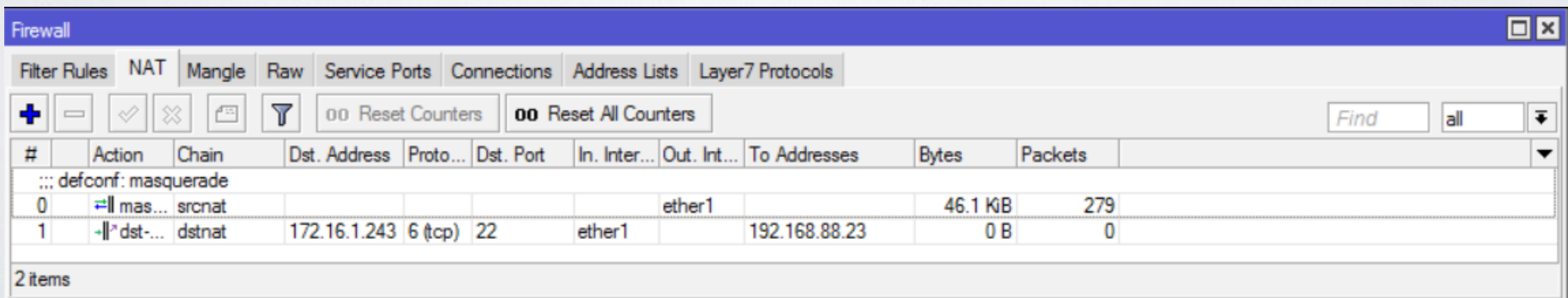
```
/ip firewall nat add chain=dstnat in-interface=ether1 protocol=tcp dst-port=22  
action=dst-nat dst-address=172.16.1.243 to-address=192.168.88.23
```

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 configuration window. The 'NAT' tab is selected. The configuration table shows two rules:

#	Action	Chain	Dst. Address	Proto...	Dst. Port	In. Inter...	Out. Int...	To Addresses	Bytes	Packets
0	masquerade	srcnat					ether1		46.1 kB	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)

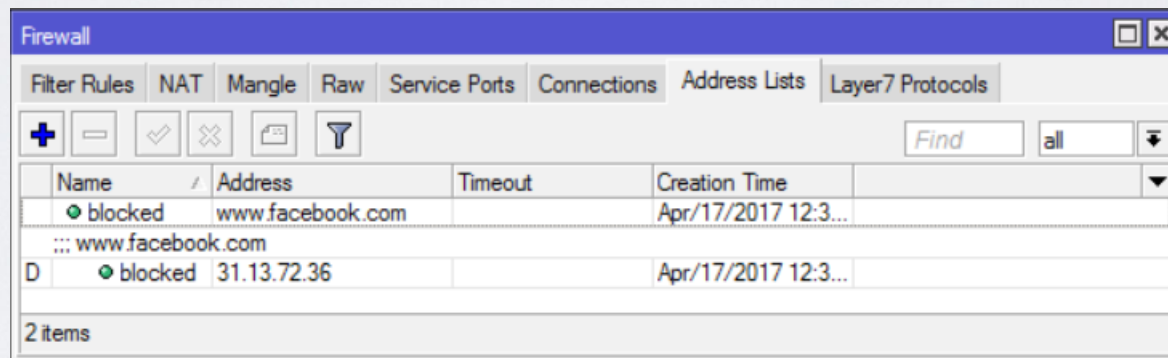
https://wiki.mikrotik.com/wiki/Hairpin_NAT

Firewall

- Block specific traffic

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

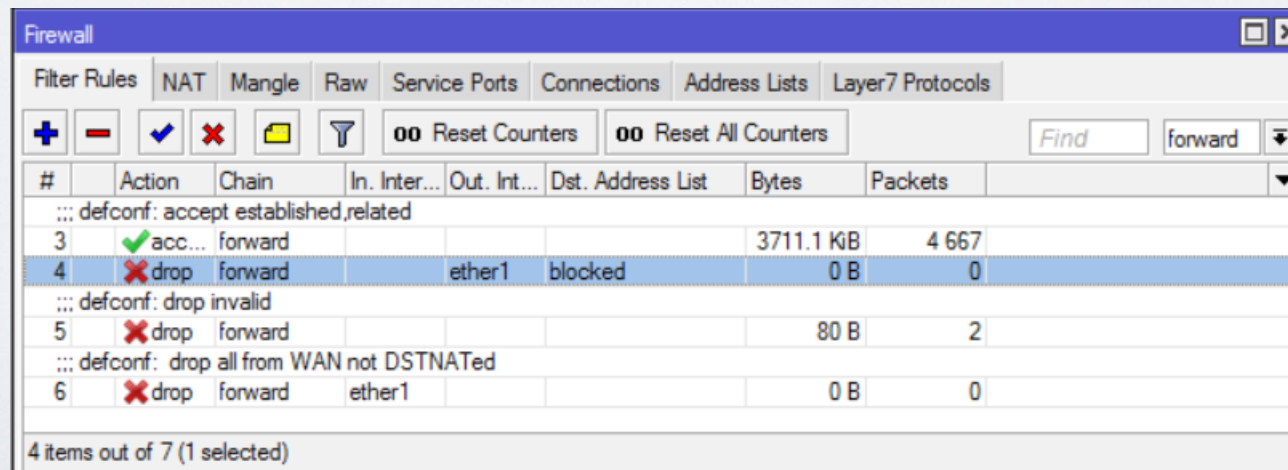
```
/ip firewall filter add chain=forward action=drop dst-address-list=blocked out-interface=ether1
```



The screenshot shows the Mikrotik WinBox Firewall configuration window, specifically the Address Lists tab. It displays two address lists:

Name	Address	Timeout	Creation Time
blocked	www.facebook.com		Apr/17/2017 12:3...
blocked	31.13.72.36		Apr/17/2017 12:3...

2 items



The screenshot shows the Mikrotik WinBox Firewall configuration window, specifically the Filter Rules tab. It displays a list of filter rules:

#	Action	Chain	In. Inter...	Out. Int...	Dst. Address List	Bytes	Packets
3	acc...	forward				3711.1 KB	4 667
4	drop	forward		ether1	blocked	0 B	0
5	drop	forward				80 B	2
6	drop	forward	ether1			0 B	0

4 items out of 7 (1 selected)

Firewall

- Protect device against attacks if you allow particular access

```
/ip firewall filter
```

```
add chain=input protocol=tcp dst-port=22 src-address-list=ssh_blacklist  
action=drop
```

```
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_blacklist address-  
list-timeout=10d
```

```
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
```

```
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
```


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

Queues

- Add queues to limit traffic for specific resources

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

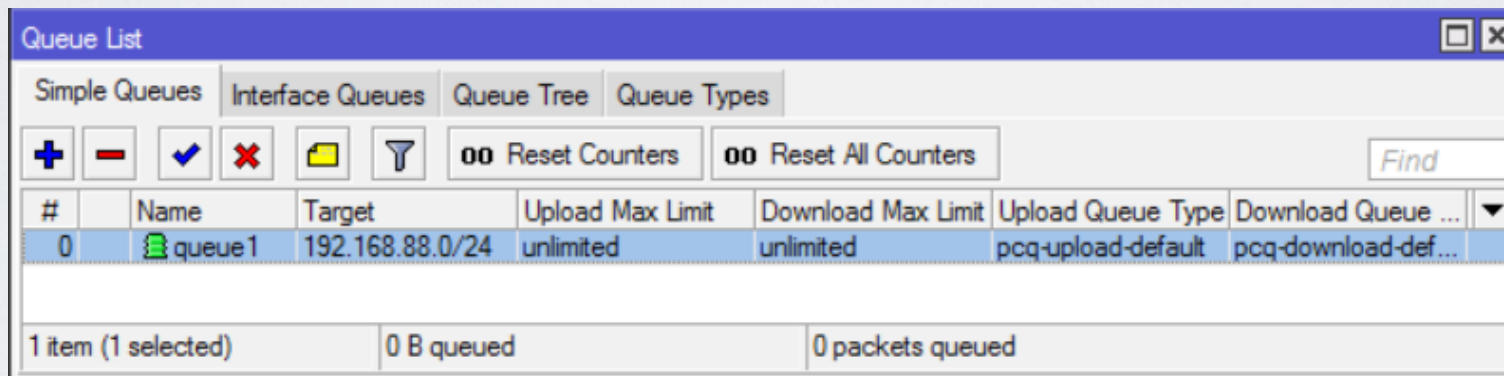
#	Name	Target	Upload Max Limit	Download Max Limit
0	queue1	192.168.88.243	5M	5M

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 'Queue List' window in Mikrotik WinBox. It has tabs for 'Simple Queues', 'Interface Queues', 'Queue Tree', and 'Queue Types'. Below the tabs are several action buttons: a plus sign, a minus sign, a checkmark, an 'X', a folder icon, a funnel icon, 'Reset Counters', and 'Reset All Counters'. A 'Find' search box is on the right. The main area contains a table with the following data:

#	Name	Target	Upload Max Limit	Download Max Limit	Upload Queue Type	Download Queue ...
0	queue1	192.168.88.0/24	unlimited	unlimited	pcq-upload-default	pcq-download-def...

At the bottom of the window, it displays '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

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

The screenshot shows the Torch application window with the following configuration:

- Basic:** Interface: bridge-local, Entry Timeout: 00:00:03 s
- Collect:** Src. Address, Dst. Address, MAC Protocol, Protocol, DSCP, Src. Address6, Dst. Address6, Port, VLAN Id
- Filters:** Src. Address: 0.0.0.0/0, Dst. Address: 0.0.0.0/0, Src. Address6: ::/0, Dst. Address6: ::/0, MAC Protocol: all, Protocol: any, Port: any, VLAN Id: any, DSCP: any

Buttons: Start, Stop, Close, New Window

Et...	Prot...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...	
800 (ip)	6 (tcp)	172.16.1.243:55392	172.16.1.1:8291 (winbox)			156.3 k...	4.9 kbps	14	7	
800 (ip)	17 (...)	172.16.1.251:20148	85.234.190.33:17943			34.3 kbps	2.0 Mbps	68	178	
800 (ip)	17 (...)	172.16.1.251:137 (netbios...)	172.16.1.255:137 (netbios...)			0 bps	0 bps	0	0	
800 (ip)	17 (...)	172.16.1.251:20148	78.84.230.93:59480			0 bps	11.8 kbps	0	1	
800 (ip)	17 (...)	255.255.255.255:5246	172.16.1.1:57768			0 bps	0 bps	0	0	
800 (ip)	17 (...)	255.255.255.255:5678 (di...)	172.16.1.1:55572			0 bps	0 bps	0	0	
800 (ip)	17 (...)	172.16.1.251:49541	239.255.255.250:1900			0 bps	0 bps	0	0	
800 (ip)	17 (...)	172.16.1.251:49541	172.16.1.1:1900			0 bps	0 bps	0	0	

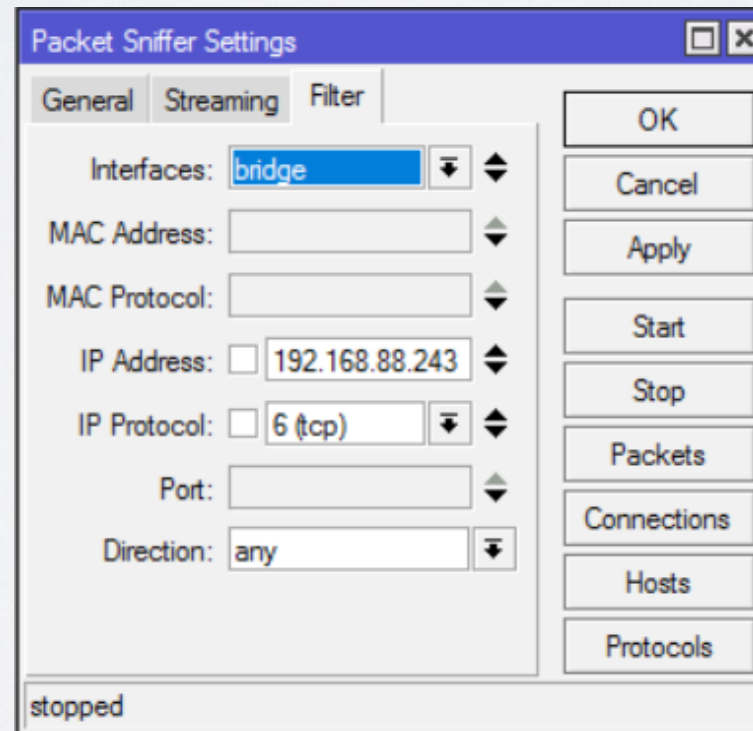
Summary: 8 items, Total Tx: 190.6 kbps, Total Rx: 2.1 Mbps, Total Tx Packet: 82, Total Rx Packet: 186

Debugging tools

- Sniffer

Analyse processed packets

https://wiki.mikrotik.com/wiki/Manual:Troubleshooting_tools#Packet_Sniffer_.28.2Ftool_sniffer.29

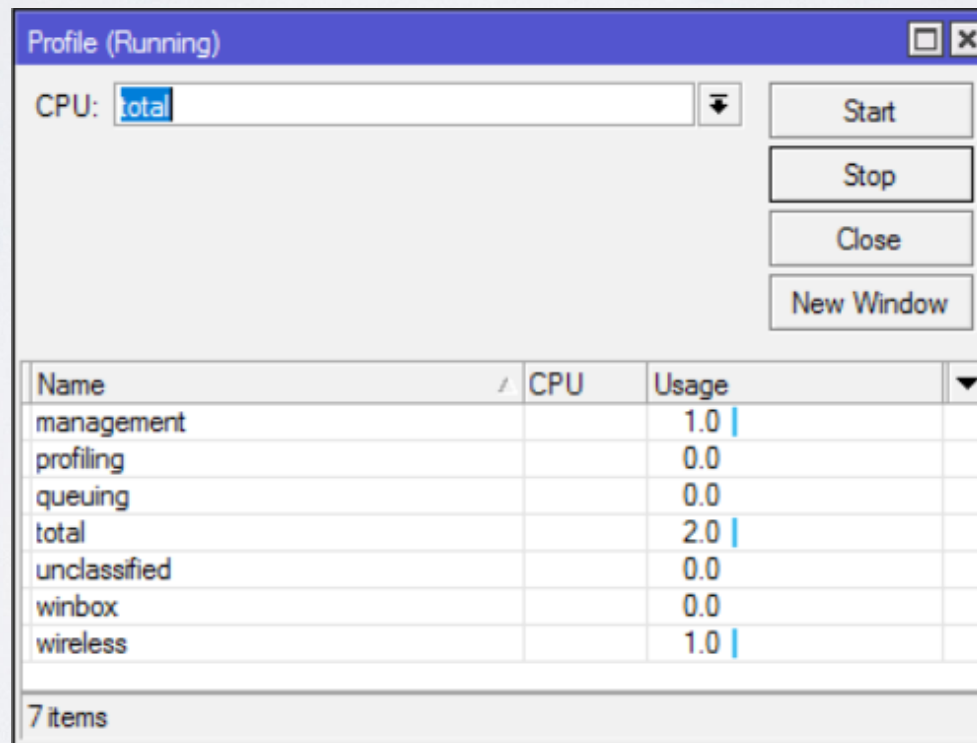


Debugging tools

- 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

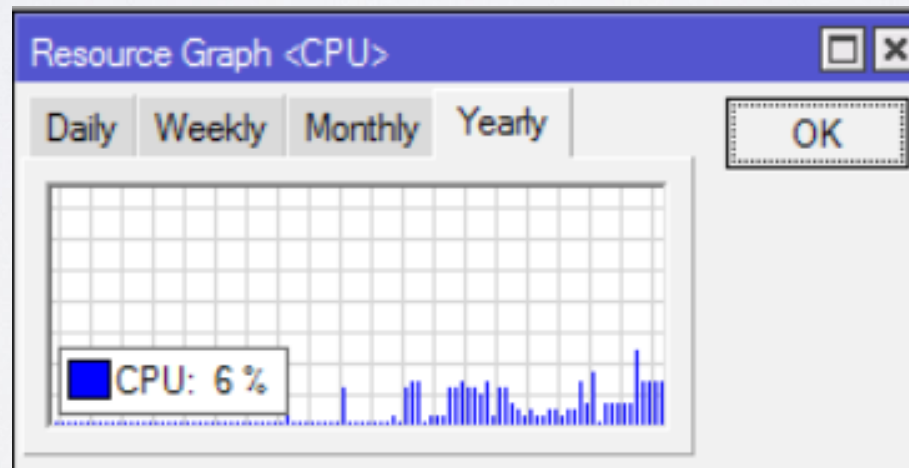
At the bottom of the window, it indicates '7 items'.

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 monitor tool:

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

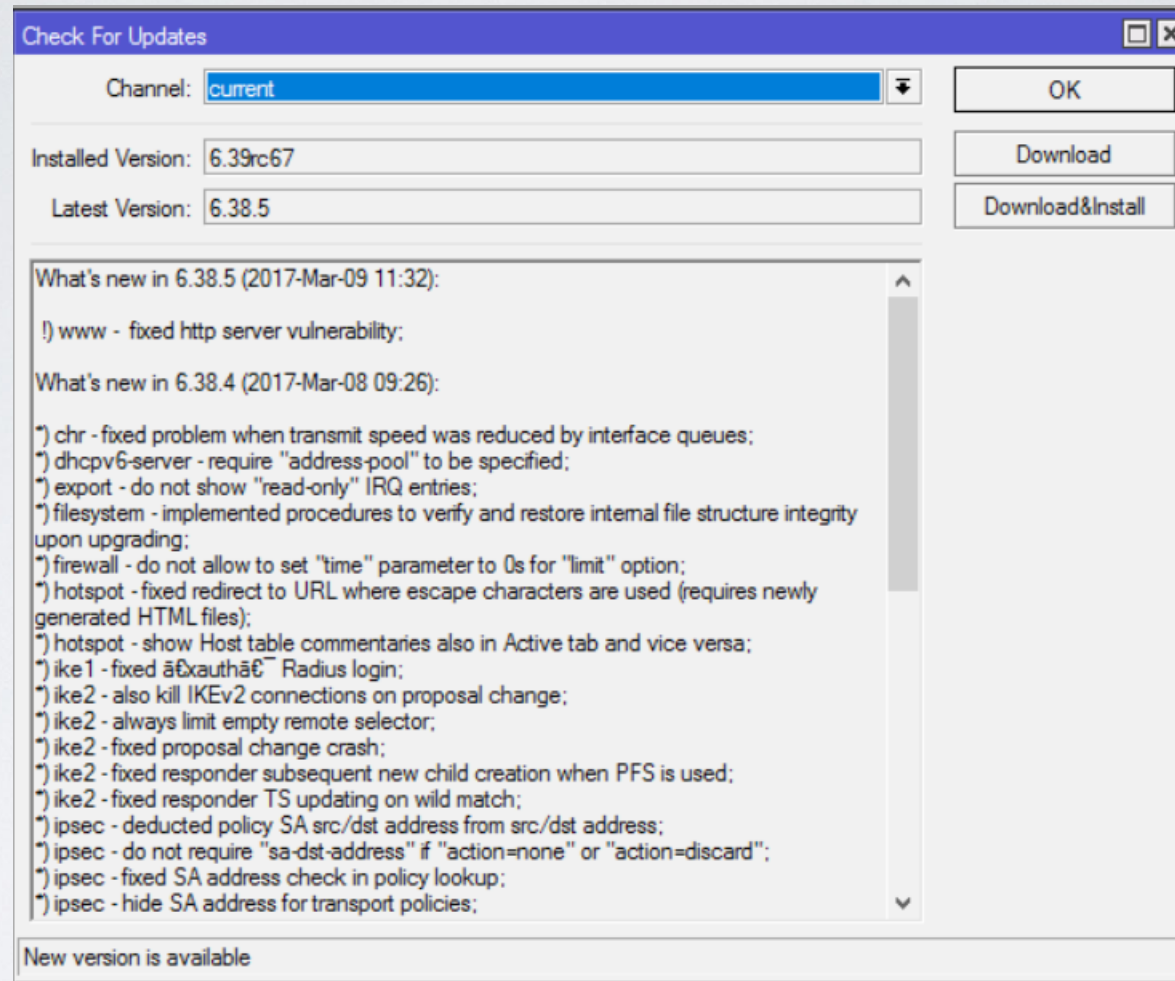
- **Current**

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

What to do when software stops working?

Resolve problems

- Backup RouterBOOT

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

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

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

- 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)

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

Feature requests?
Suggestions?

Thank you!