



Basic guidelines on RouterOS configuration and debugging

Pauls Jukonis

MikroTik, Latvia

Kathmandu, Nepal

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

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

Session Settings Dashboard

Safe Mode Session:

Quick Set

Home AP Dual

2GHz 5GHz

Network Name: MikroTik-2798E1 MikroTik-2798E0

Frequency: auto auto MHz

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

Country: no_country_set

☐ Use Access List (ACL)

WiFi Password:

WPS Accept

- 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 Renew Release

Netmask: 255.255.255.0 (/24)

Gateway: 172.16.1.1

MAC Address: 6C:3B:6B:27:98: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: 6f120665c726.sn.mynetname.net

- System -

Check For Updates Reset Configuration

Password:

Confirm Password:

OK Cancel Apply

Simple security

Simple security

- Specify user password

/user set admin password=***

- Use different username

/user set admin name=martins

The screenshot displays the MikroTik WinBox v6.38.5 interface. The top bar shows the session as 'admin@192.168.88.1 (MikroTik) - WinBox v6.38.5 on hAP ac (mipsbe)'. The left sidebar contains a menu with various system settings 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.tif, Manual, New WinBox, and Exit.

The main window is titled 'User List' and shows a table with columns: Name, Group, Allowed Address, and Last Logged In. The table contains two entries: 'system default user' and 'martins' (grouped under 'full').

A 'User <martins>' configuration dialog is open, showing fields for Name (martins), Group (full), Allowed Address, and Last Logged In. It includes buttons for OK, Cancel, Apply, Disable, Comment, Copy, Remove, and Password... The 'enabled' checkbox is checked.

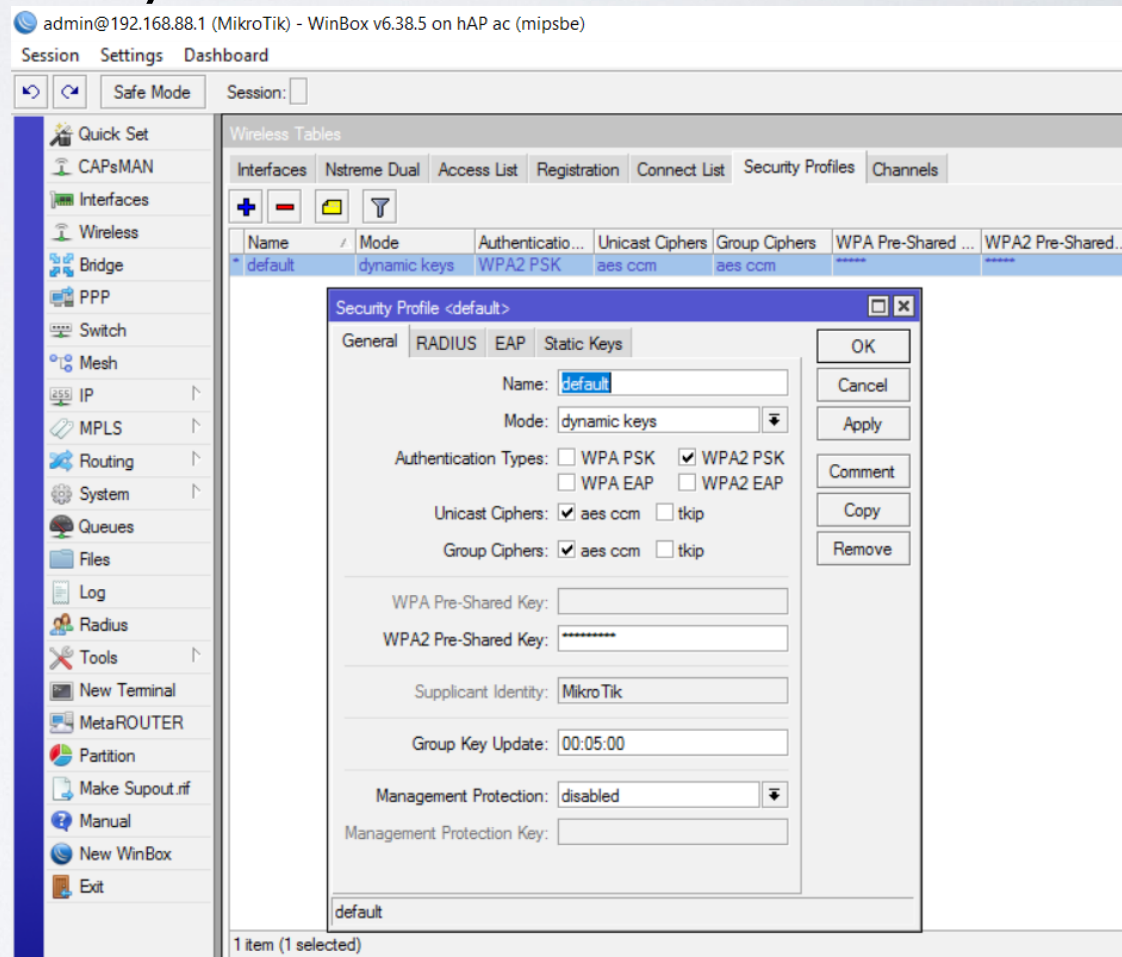
A 'Change Password' dialog is also open, showing fields for New Password and Confirm Password, with OK, Cancel, and Apply buttons.

At the bottom of the User List window, it 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=*****
```



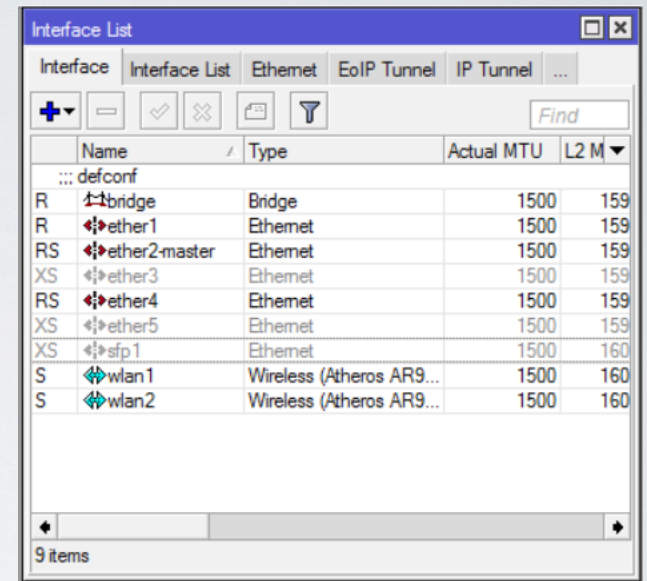
Simple security

- Disable unused interfaces

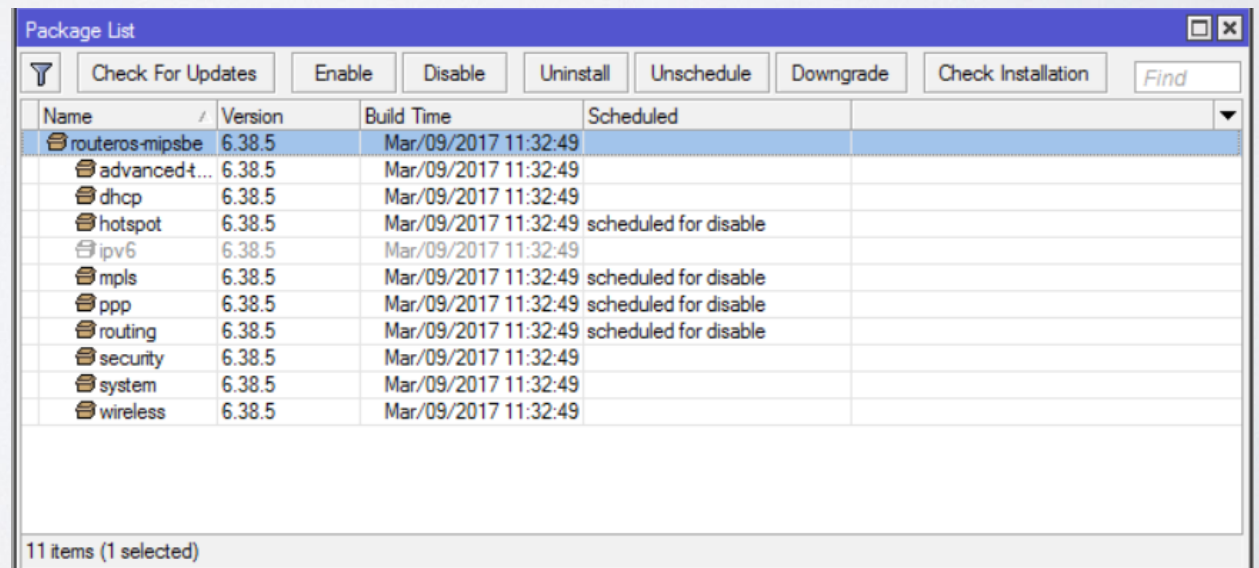
/interface ethernet disable ether3,ether5,sfp1

- Disable unused packages (mainly IPv6)

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



Name	Type	Actual MTU	L2 MTU
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

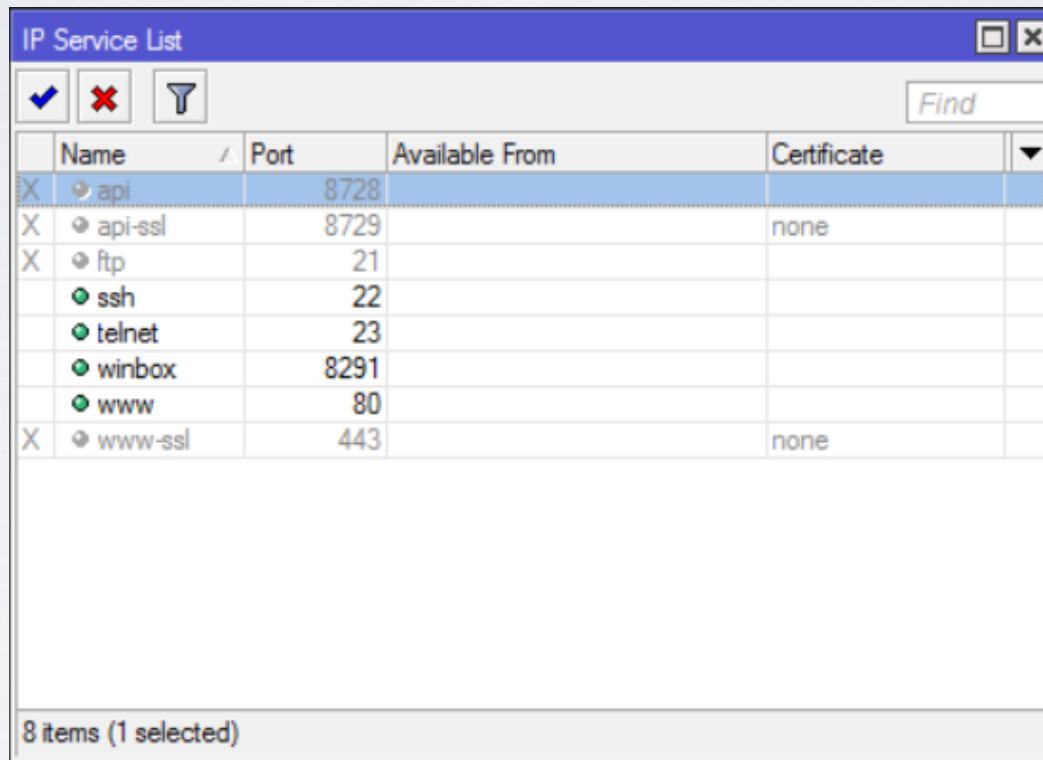


Name	Version	Build Time	Scheduled
routeros-mipsbe	6.38.5	Mar/09/2017 11:32:49	
advancedt...	6.38.5	Mar/09/2017 11:32:49	
dhcp	6.38.5	Mar/09/2017 11:32:49	
hotspot	6.38.5	Mar/09/2017 11:32:49	scheduled for disable
ipv6	6.38.5	Mar/09/2017 11:32:49	
mpls	6.38.5	Mar/09/2017 11:32:49	scheduled for disable
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 image shows a window titled "IP Service List" with a table of services. The table has columns for Name, Port, Available From, and Certificate. The first row, "api" on port 8728, is selected and has an "X" in the first column. Other rows include "api-ssl" (port 8729, certificate "none"), "ftp" (port 21), "ssh" (port 22), "telnet" (port 23), "winbox" (port 8291), "www" (port 80), and "www-ssl" (port 443, certificate "none"). The status column for "api" and "www-ssl" shows an "X", while others show a green dot. A 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

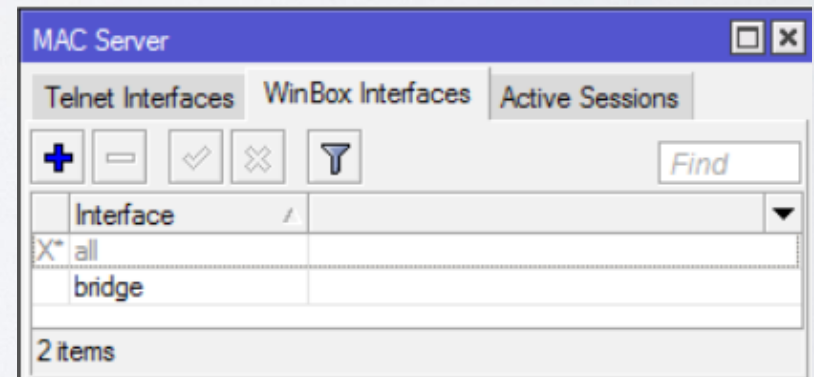
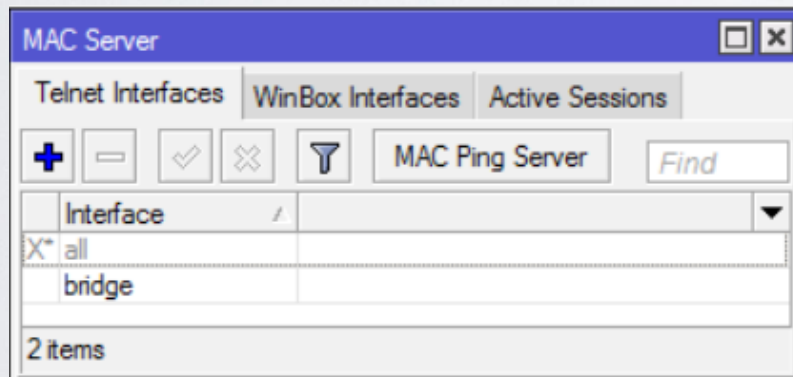
- Adjust MAC access

```
/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
```

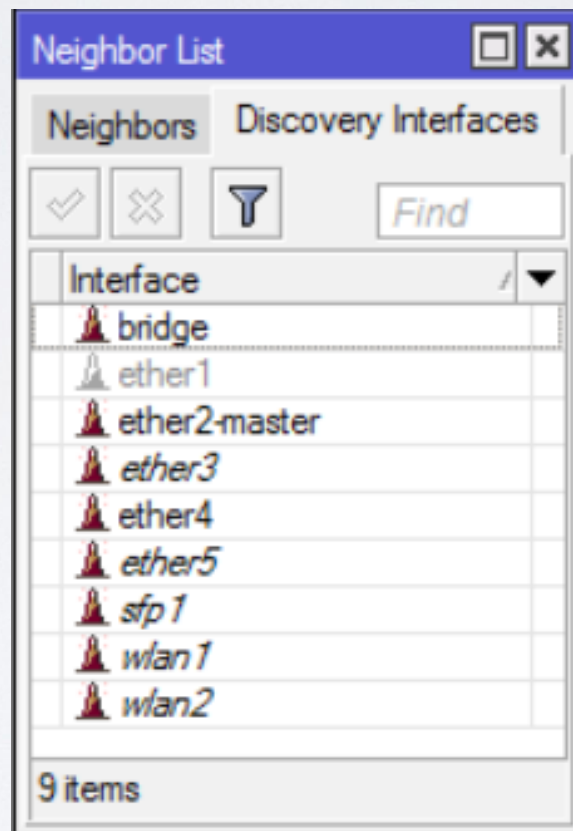
```
/tool mac-server mac-winbox add interface=bridge
```



Simple security

- Hide device in Neighbor Discovery

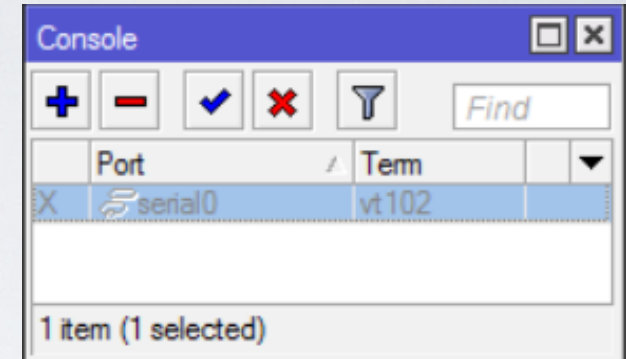
`/ip neighbor discovery set ether1 discover=no`



Simple security

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

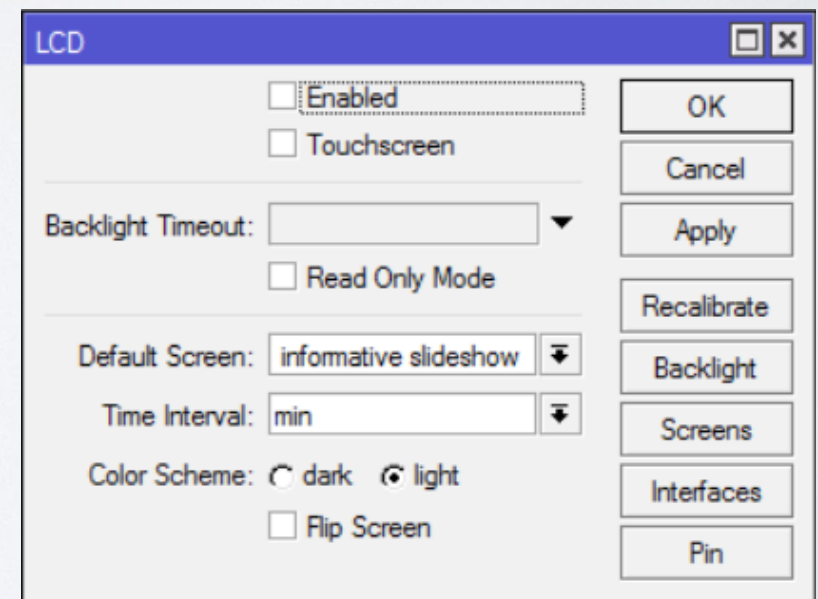
/system console disable [find where port=serial0]



- 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

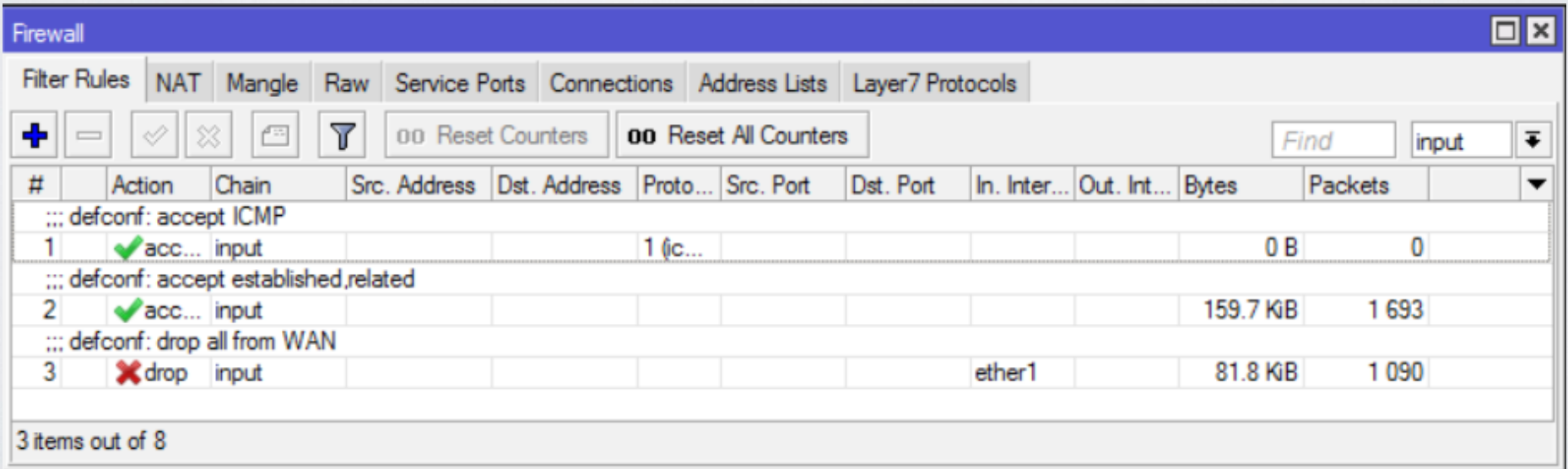
- Secure input

/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 'Filter Rules' tab is selected. The table below lists the configured rules:

#	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

3 items out of 8

Firewall

- Secure forward

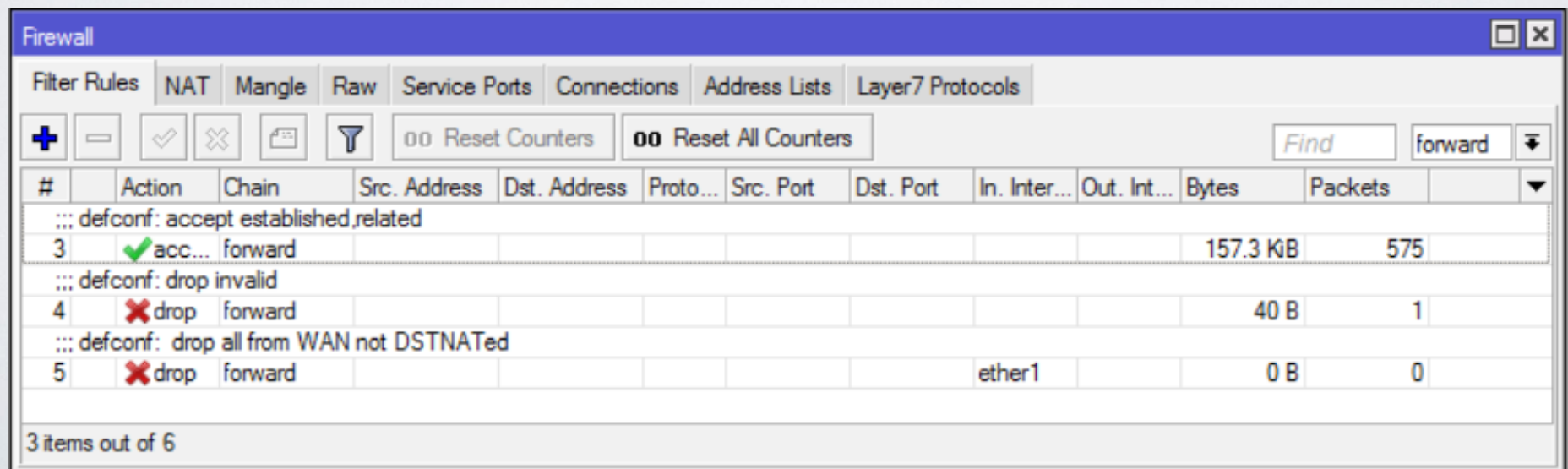
/ip firewall filter

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 selected. The table below lists the configured rules:

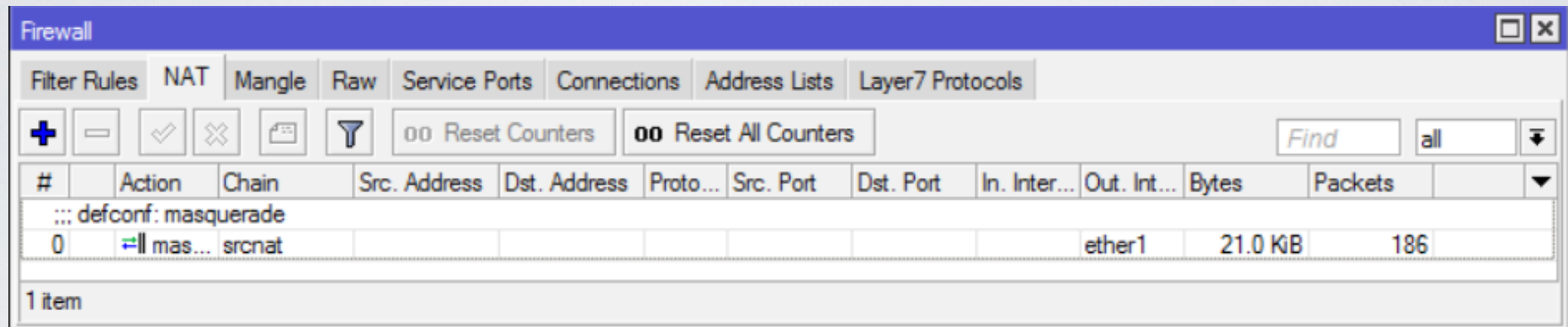
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
::: defconf: accept established,related											
3	✓ acc...	forward								157.3 KiB	575
::: defconf: drop invalid											
4	✗ drop	forward								40 B	1
::: defconf: drop all from WAN not DSTNATed											
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)

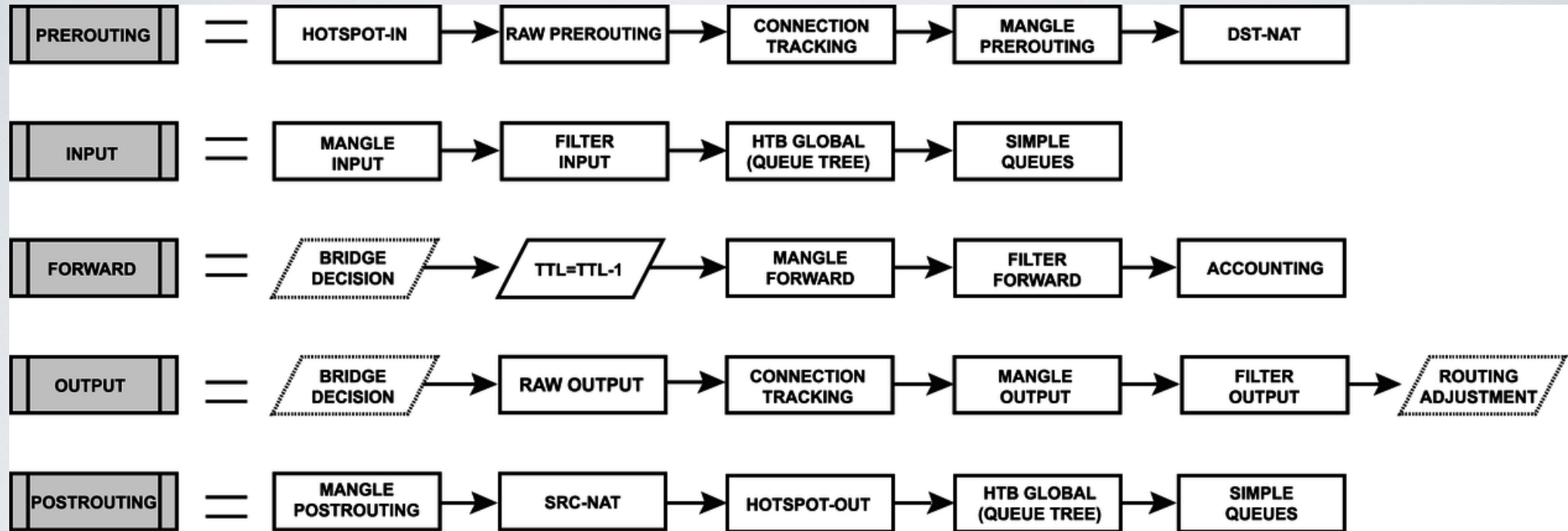
```
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
```



#	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

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

Firewall



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

Firewall

- NAT to LAN

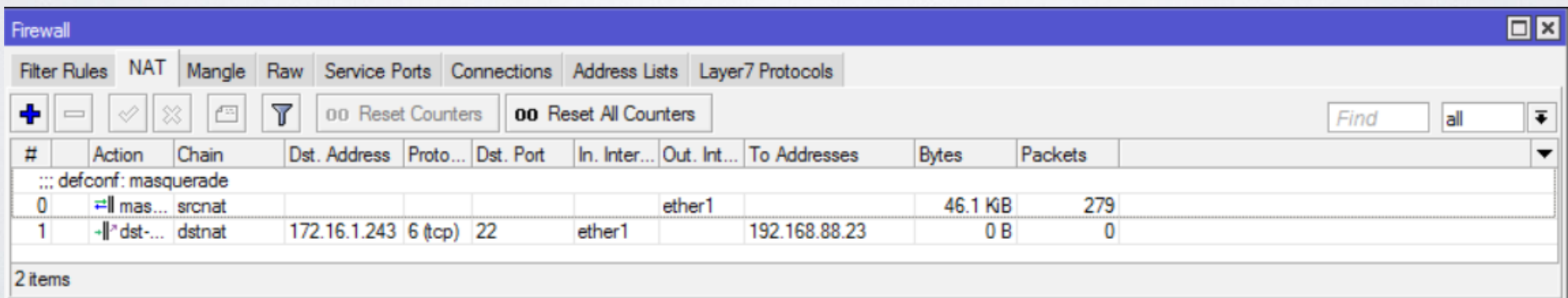
```
/ip firewall nat add chain=dstnat in-interface=ether1 protocol=tcp dst-port=22  
action=dst-nat dst-address=172.16.1.243 to-address=192.168.88.23
```

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 Rules configuration window. The 'NAT' tab is selected. The rule list contains two items:

#	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)

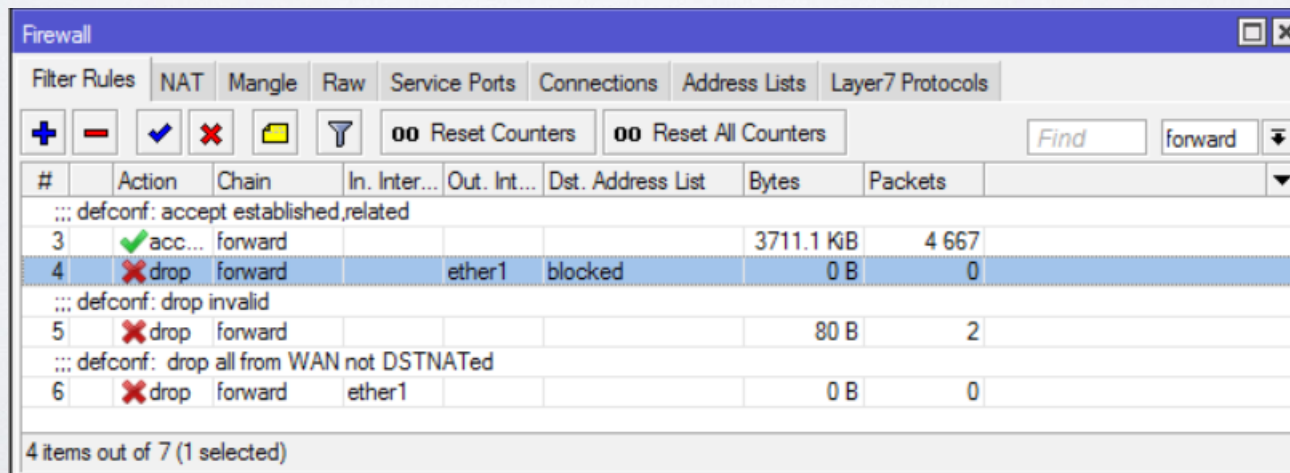
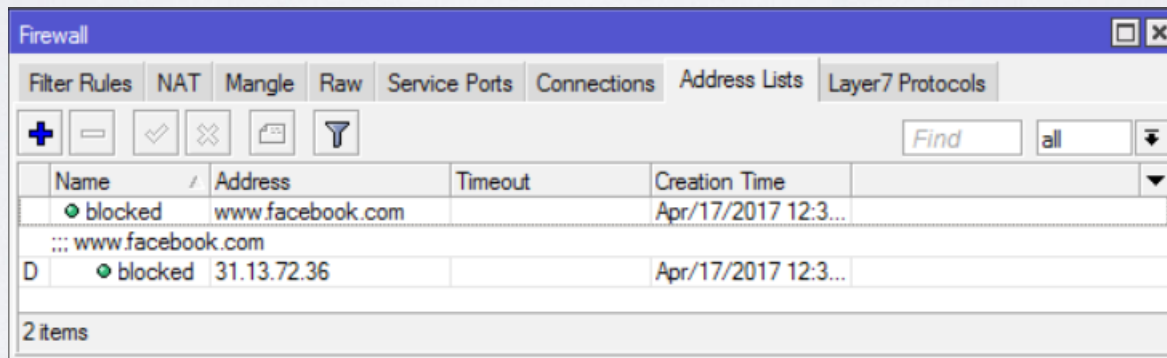
https://wiki.mikrotik.com/wiki/Hairpin_NAT

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=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

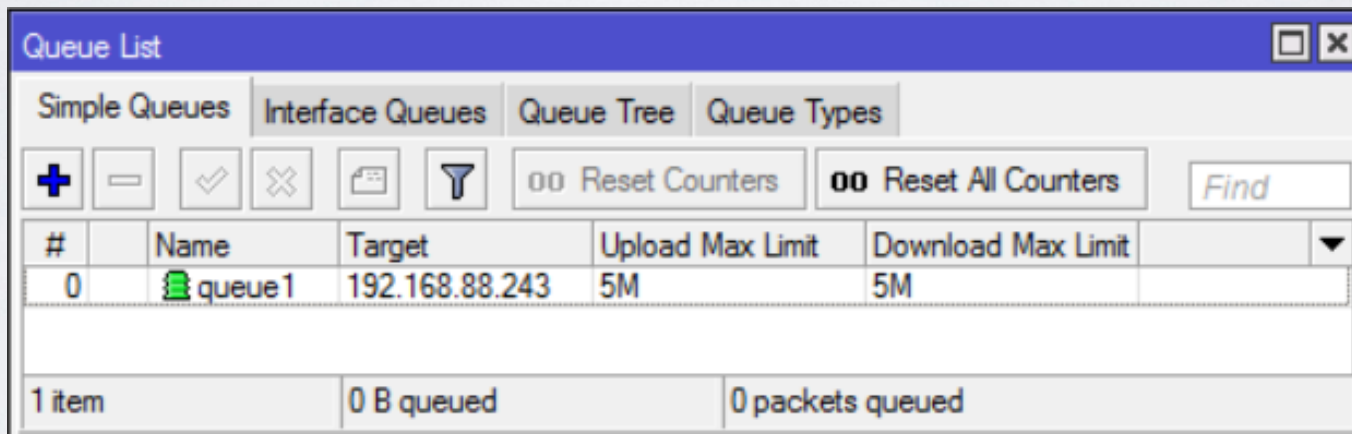
`/ip firewall filter`

- `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

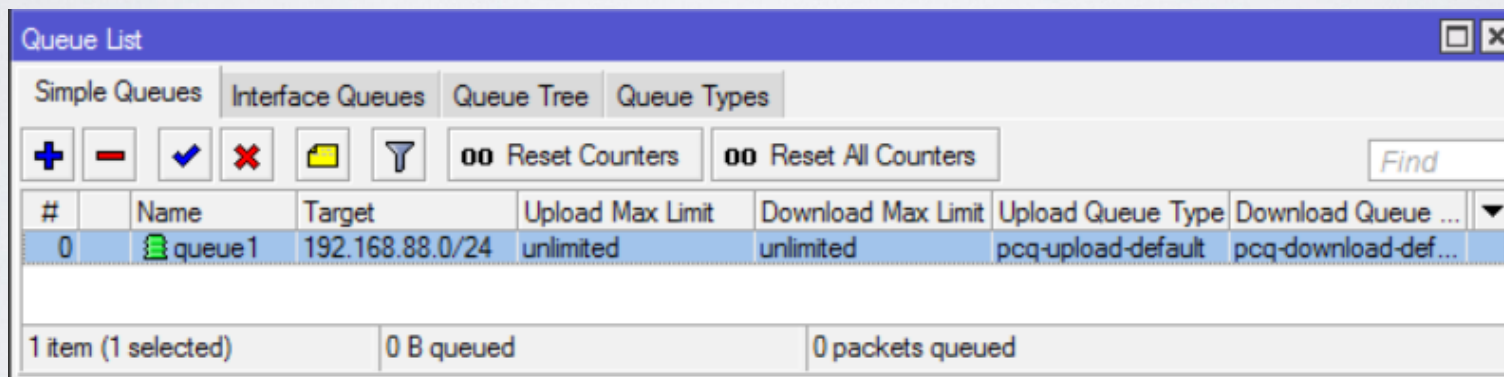


Queue List					
Simple Queues Interface Queues Queue Tree Queue Types					
+ - ✓ ✗ [Icon] [Icon] ∞ Reset Counters ∞ Reset All Counters Find					
#	Name	Target	Upload Max Limit	Download Max Limit	
0	queue1	192.168.88.243	5M	5M	
1 item 0 B queued 0 packets queued					

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



#	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...

1 item (1 selected) 0 B queued 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

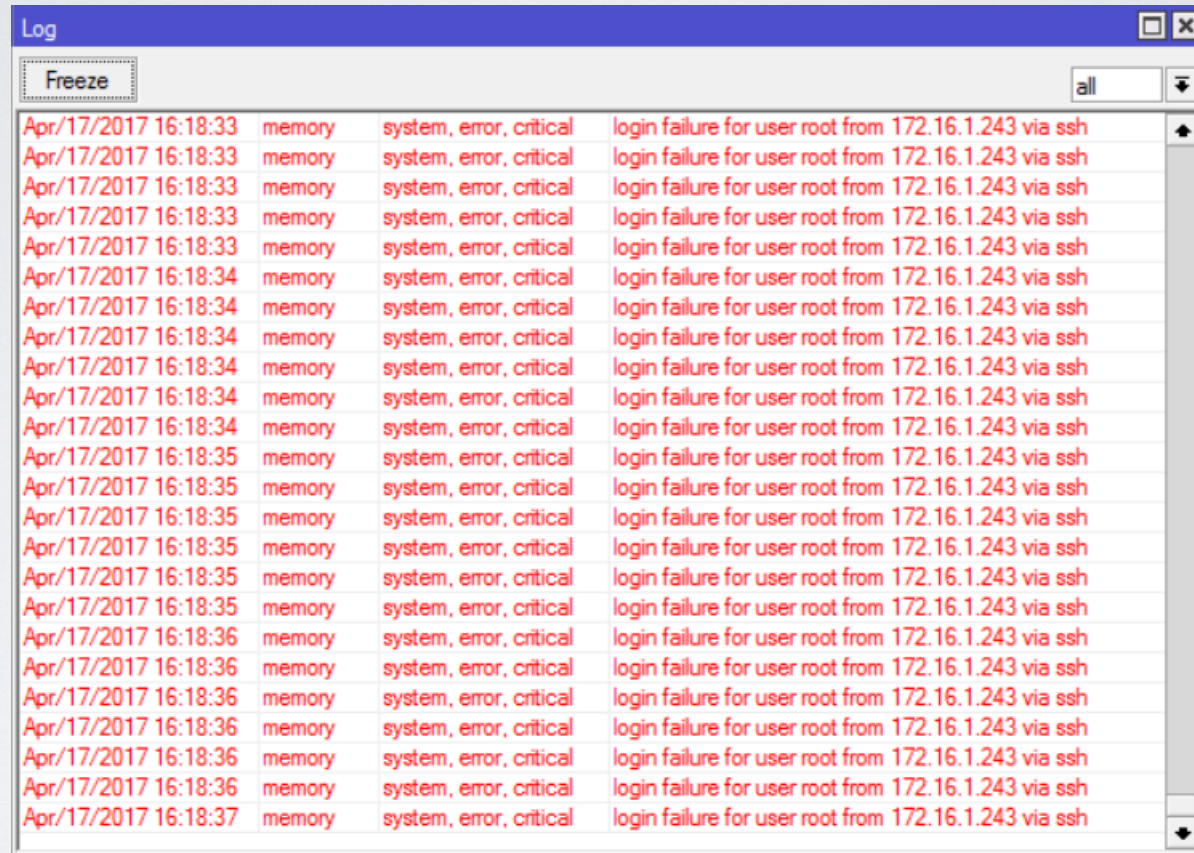
```
/system logging add topics=l2pt,debug action=memory
```

- 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
```

Logging



The screenshot shows a Mikrotik Log window with a blue title bar. Below the title bar is a toolbar with a 'Freeze' button and a dropdown menu set to 'all'. The log table contains 20 rows of entries, all of which are login failures for the user 'root' from the IP address '172.16.1.243' via 'ssh'. Each entry is timestamped 'Apr/17/2017' and includes details about the source of the log (memory, system), the error type (error, critical), and the specific event (login failure).

Time	Source	Event	Message
Apr/17/2017 16:18:33	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:33	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:33	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:33	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:33	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:34	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:34	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:34	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:34	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:34	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:34	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:35	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:35	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:35	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:35	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:35	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:35	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:36	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:36	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:36	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:36	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:36	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:37	memory	system, error, critical	login failure for user root from 172.16.1.243 via ssh

<https://wiki.mikrotik.com/wiki/Manual:System/Log>

Debugging tools

- Torch

Analyse processed traffic

https://wiki.mikrotik.com/wiki/Manual:Troubleshooting_tools#Torch_.28.2Ftool_to_rch.29

The screenshot shows the Mikrotik Torch application window. The 'Basic' tab is selected, showing the interface as '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 input 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'. At the bottom, a table displays traffic statistics.

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 statistics at the bottom:

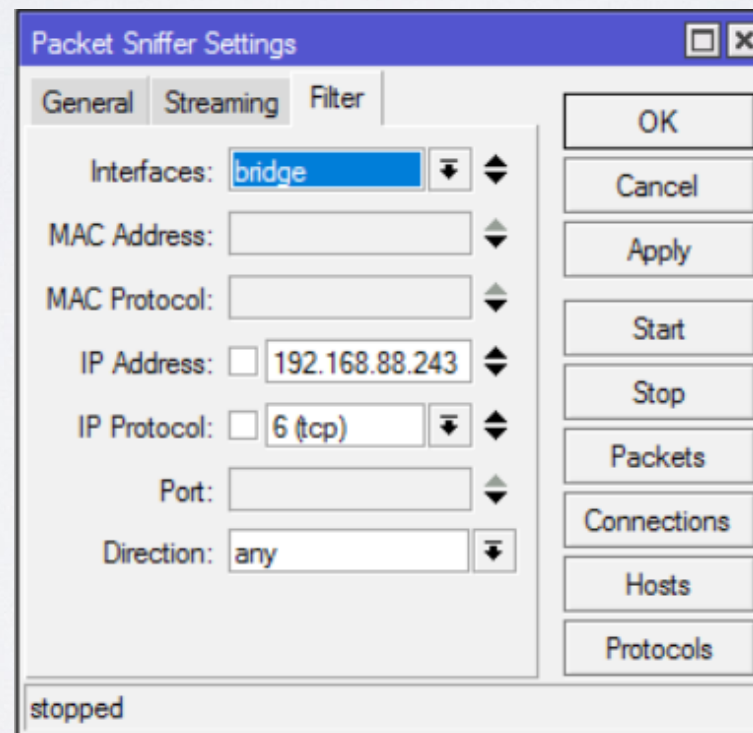
8 items	Total Tx: 190.6 kbps	Total Rx: 2.1 Mbps	Total Tx Packet: 82	Total Rx Packet: 186
---------	----------------------	--------------------	---------------------	----------------------

Debugging tools

- Sniffer

Analyse processed packets

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

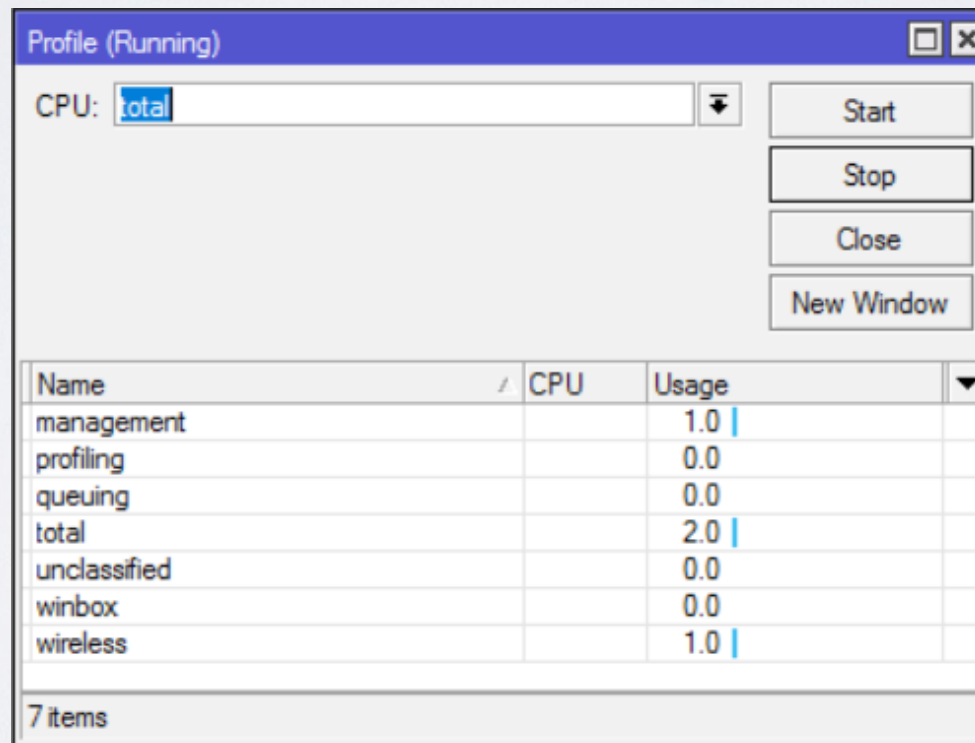


Debugging tools

- Profiler

Find out current CPU usage

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

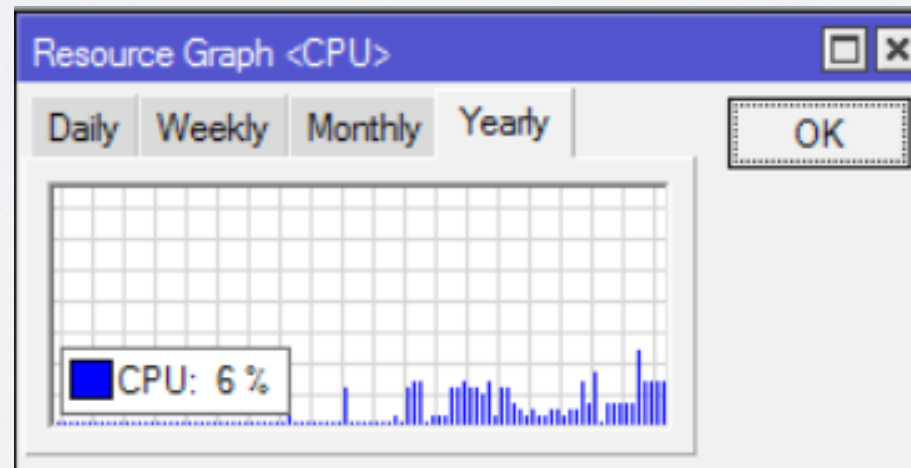


Debugging tools

- 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

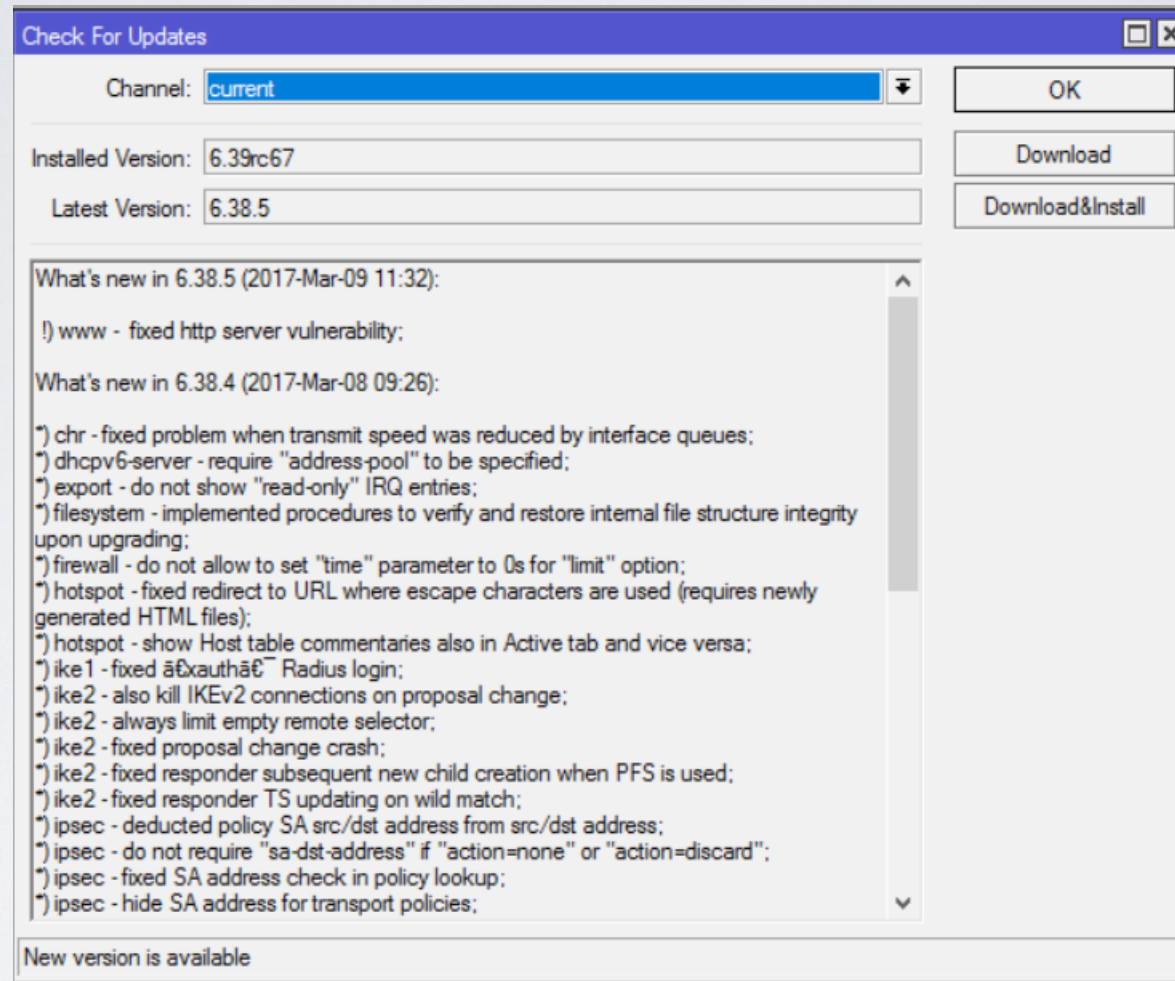
- **Current**

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!