



Basic guidelines on RouterOS
configuration and debugging

Asunción, Paraguay

June 2017

RouterOS is the **same**
everywhere



Management Tools

RouterOS Management tools

- CLI (Command Line Interface)

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

- WebFig,

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

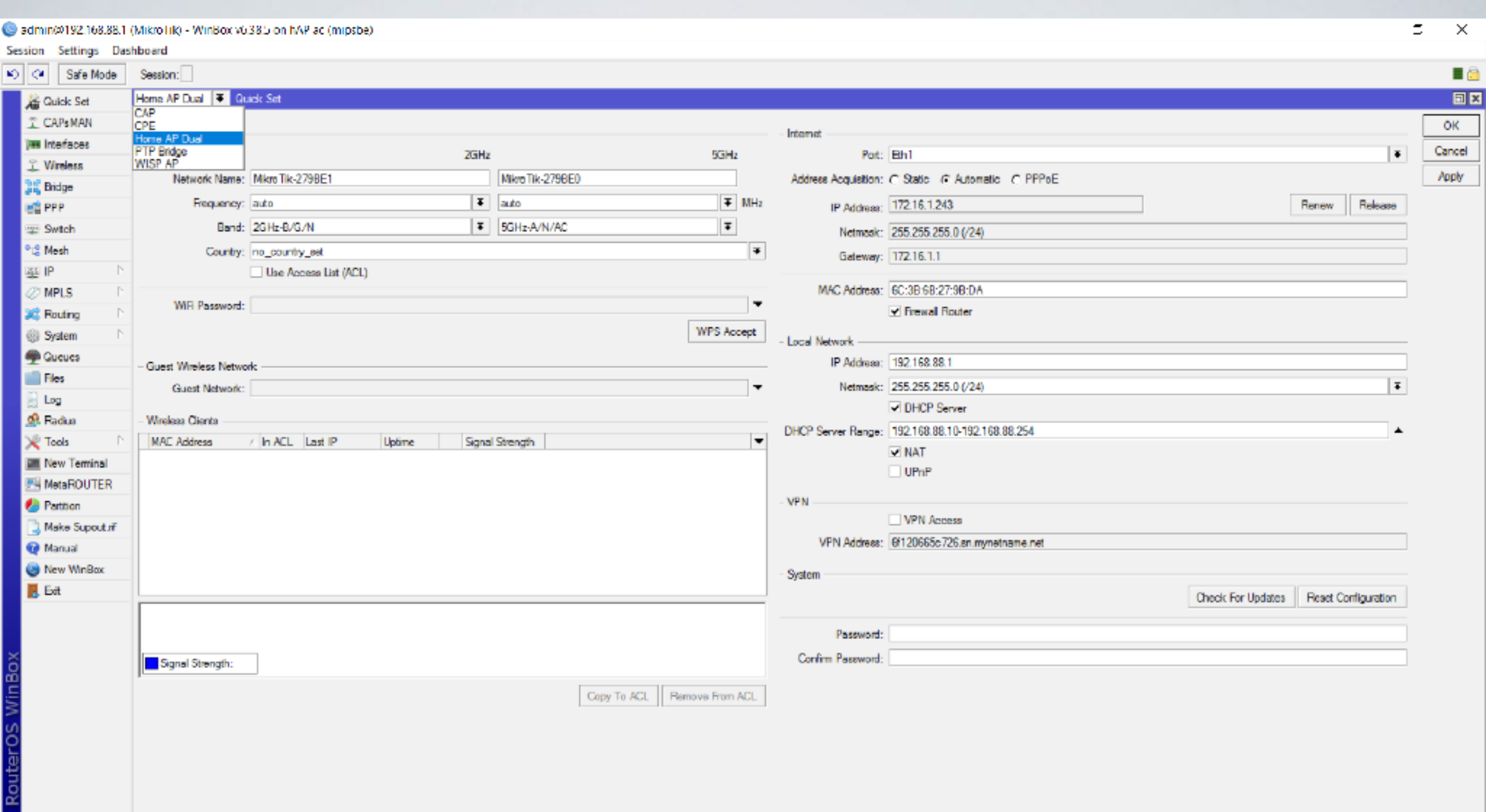
- TikApp,

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

- Winbox,

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

The fastest configuration



QuickSet

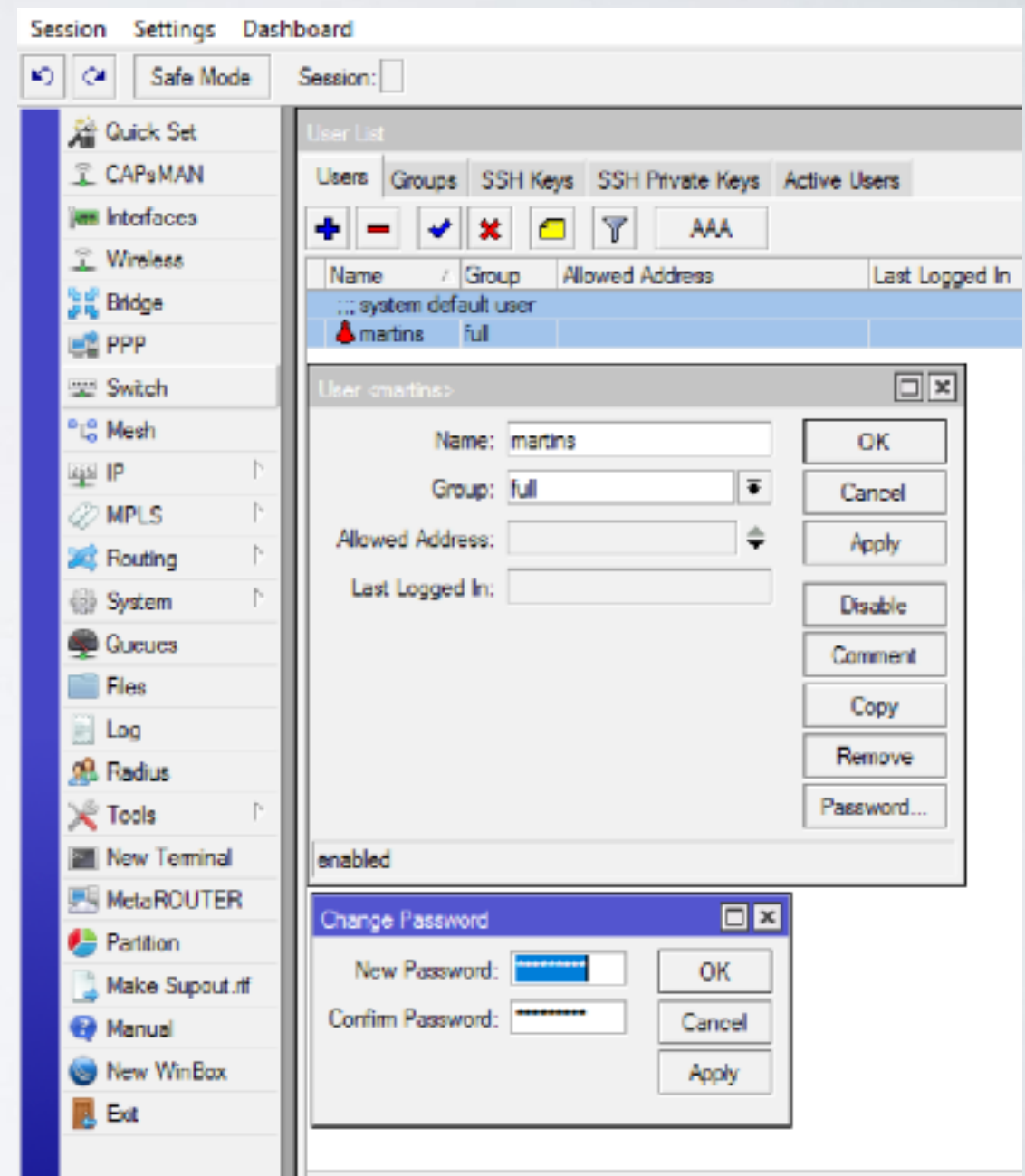
QuickSet

- Easy to use
- Contains the most commonly used features and should be enough for basic usage
- “If you use QuickSet, then use QuickSet!”

Security

Simple Security

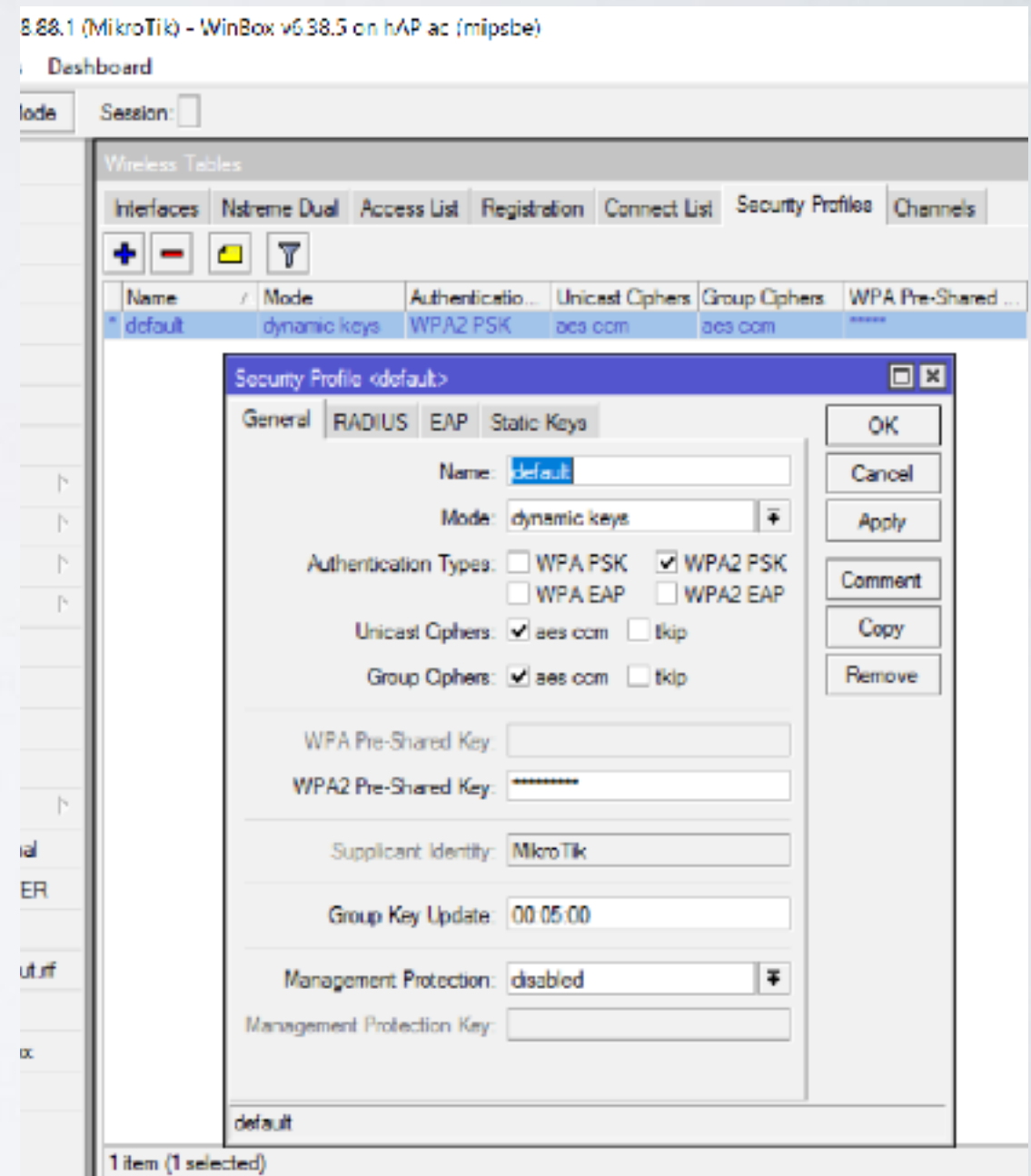
- Specify user password
/user set admin
password=***
- Use different username
/user set admin name=serg



Simple Security

- Specify password for wireless access

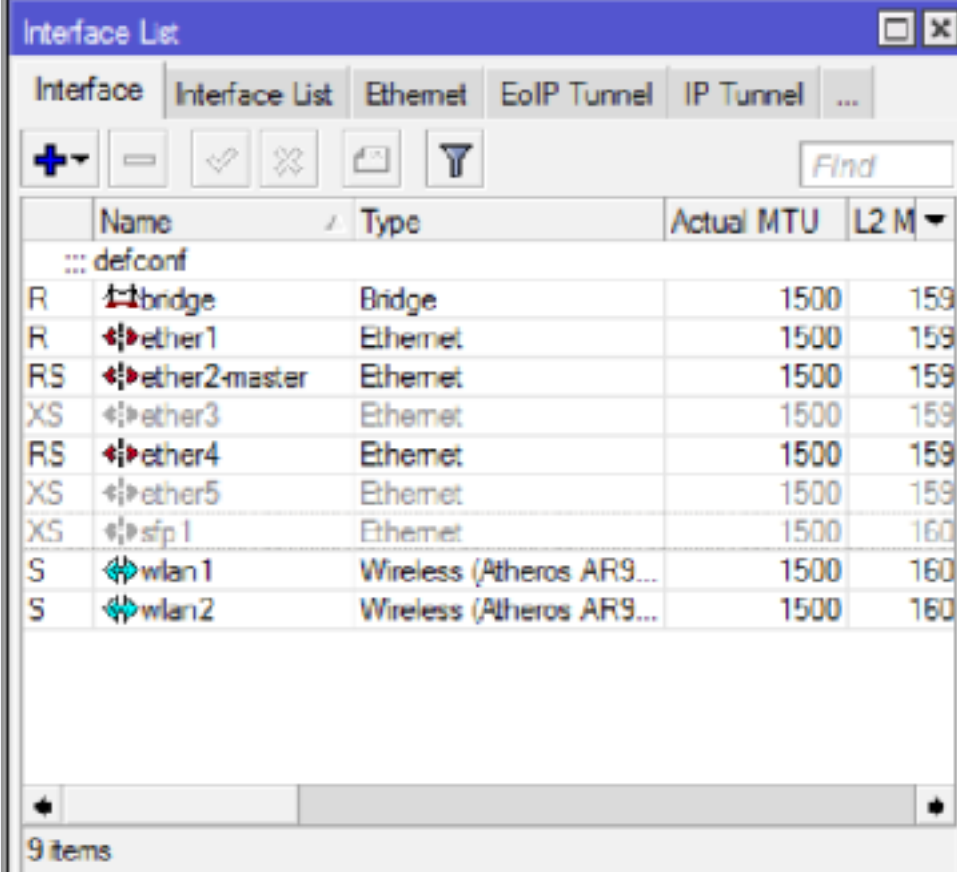
```
/interface wireless security-  
profiles set default=  
authentication-types=wpa2-  
psk mode=dynamic-keys  
wpa2-pre-shared-  
key=*****
```



Security

- Disable unused interfaces

```
/interface ethernet disable  
ether3,ether5,sfp 1
```



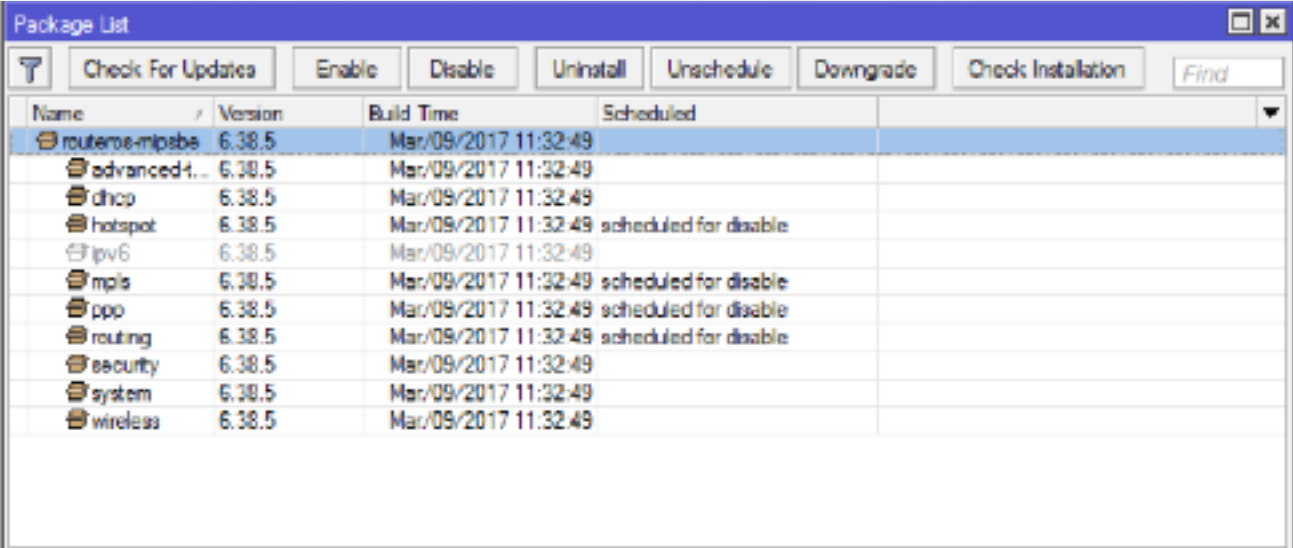
	Name	Type	Actual MTU	L2 M
...	defconf			
R	bridge	Bridge	1500	159
R	ether1	Ethernet	1500	159
RS	ether2-master	Ethernet	1500	159
XS	ether3	Ethernet	1500	159
RS	ether4	Ethernet	1500	159
XS	ether5	Ethernet	1500	159
XS	sfp 1	Ethernet	1500	160
S	wlan1	Wireless (Atheros AR9...	1500	160
S	wlan2	Wireless (Atheros AR9...	1500	160

9 items

Security

- Disable unused packages (mainly IPv6)

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



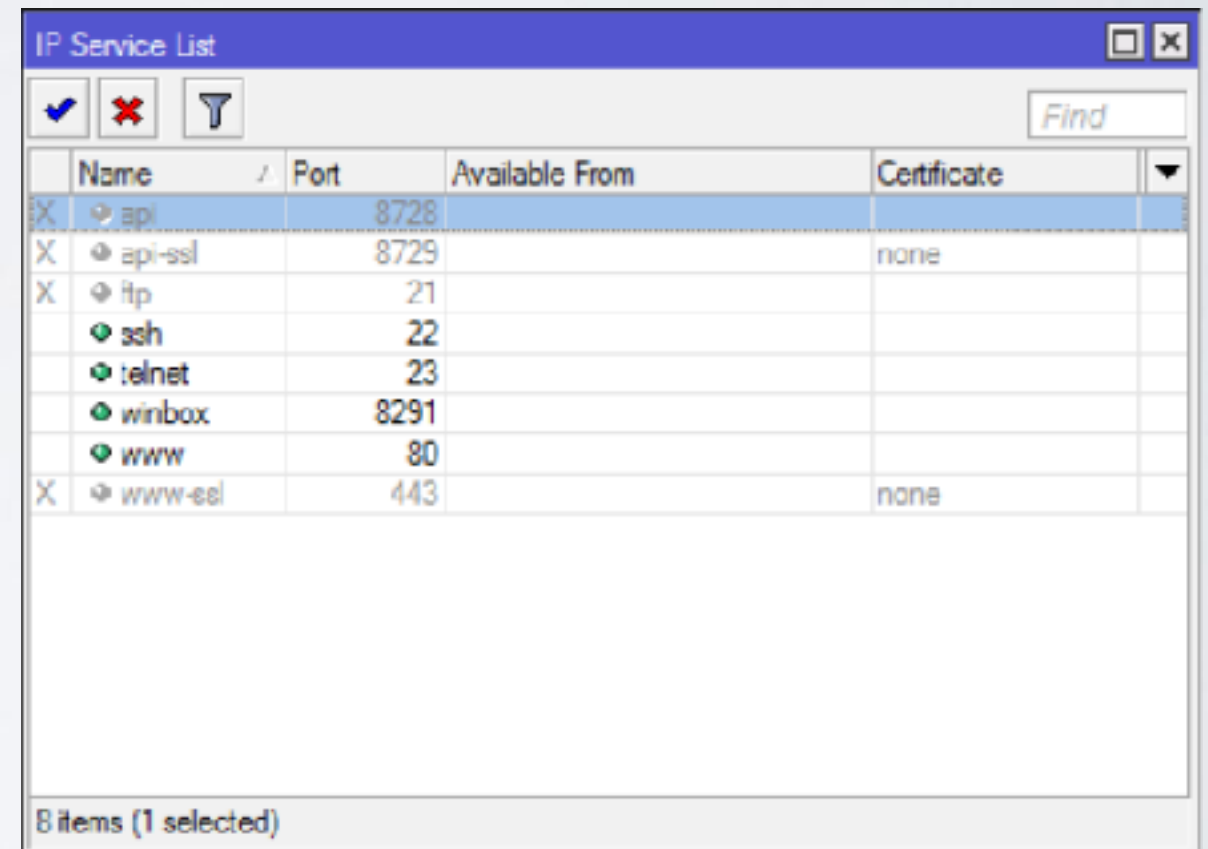
Name	Version	Build Time	Scheduled
router-mipsbe	6.38.5	Mar/09/2017 11:32:49	
advanced4...	6.38.5	Mar/09/2017 11:32:49	
dhcp	6.38.5	Mar/09/2017 11:32:49	
hotspot	6.38.5	Mar/09/2017 11:32:49	scheduled for disable
ipv6	6.38.5	Mar/09/2017 11:32:49	
mpls	6.38.5	Mar/09/2017 11:32:49	scheduled for disable
ppp	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	

11 items (1 selected)

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 first row is selected, and 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

Security

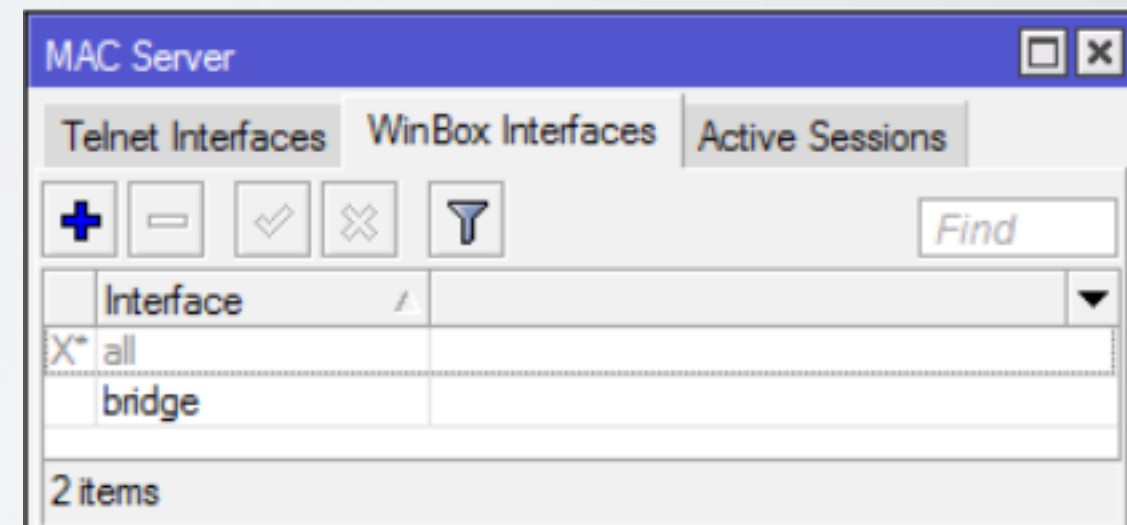
- Adjust MAC access

```
/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
```

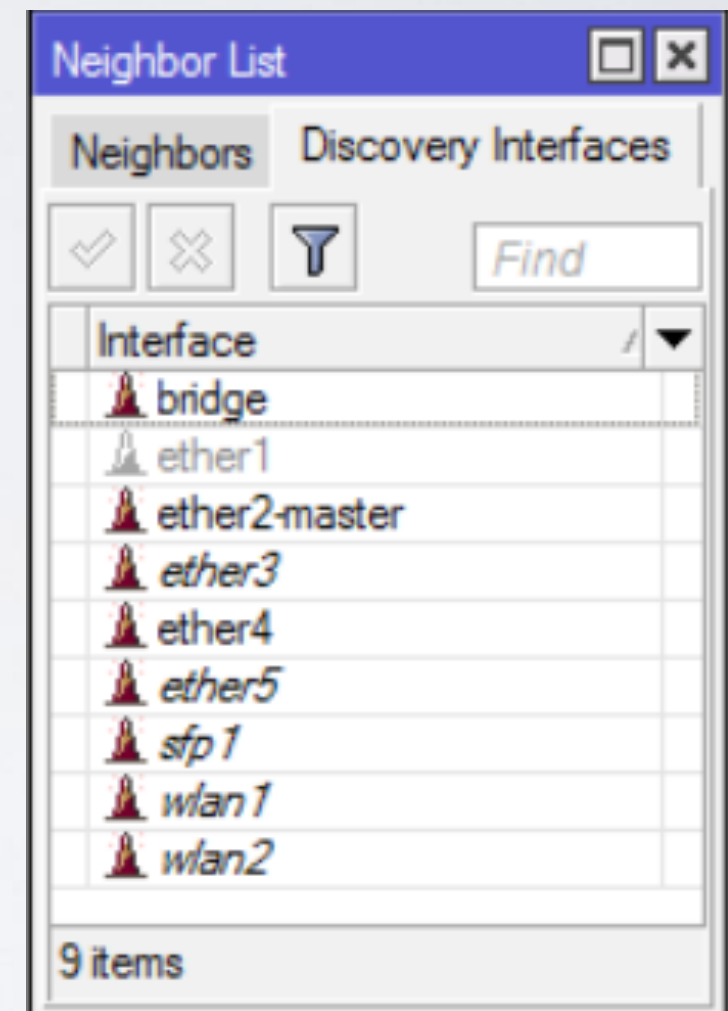
```
/tool mac-server mac-winbox  
add interface=bridge
```



Security

- Hide device in Neighbor Discovery

`/ip neighbor discovery set
ether1 discover=no`



Security

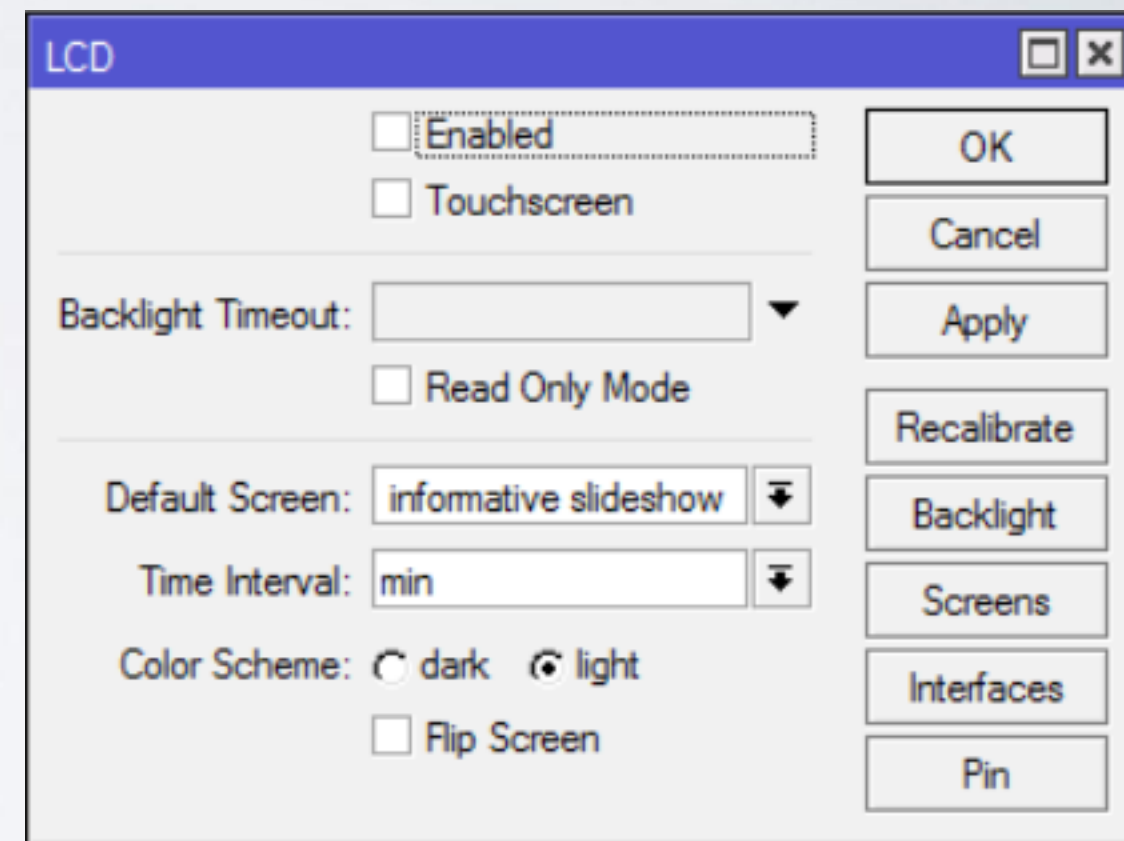
- Disable serial port if not used
(and if included)

/system console disable [find
where port=serial0]

- Disable LCD

/lcd set enabled=no

/lcd set touch-screen=disabled



Security

- Place router in secure location
- 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 most popular approaches
 - Drop untrusted and allow remaining (default accept)
 - Allow trusted and drop remaining (default drop)

```
/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 (traffic to a router)

/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

Firewall

The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is selected. The table displays the following 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

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

Firewall

- Secure forward (customers traffic through a router)

/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

Firewall

The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is selected. The rule list shows three rules:

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

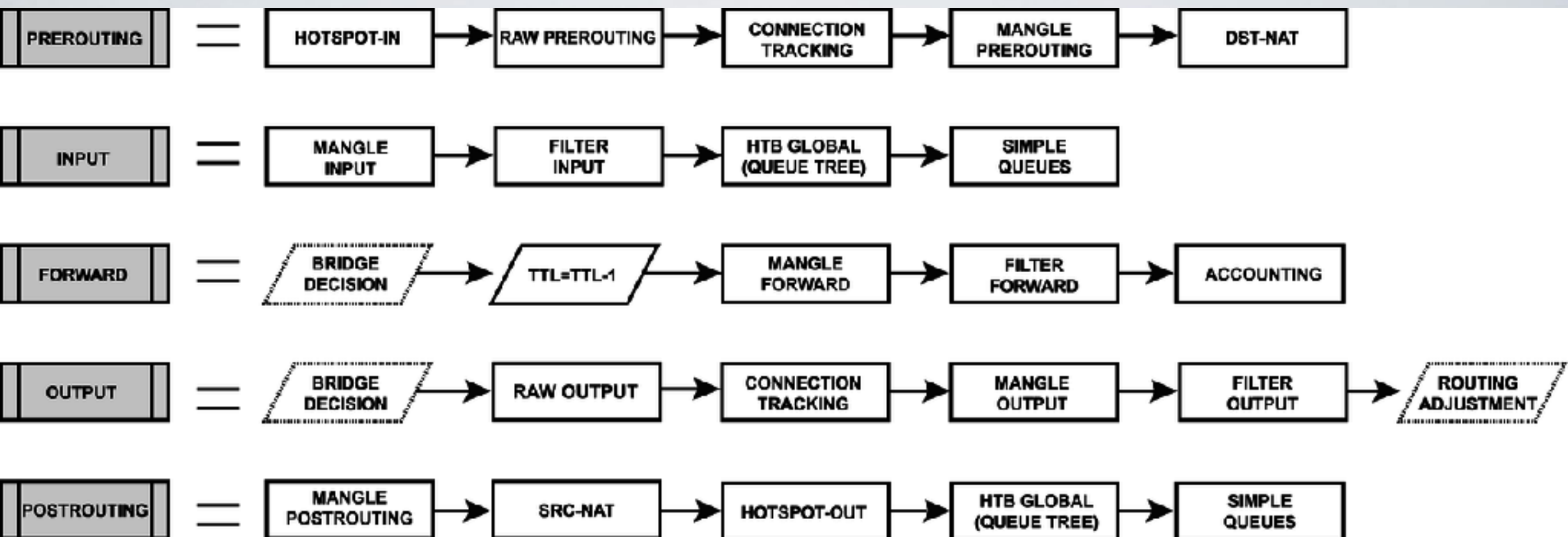
At the bottom, it indicates '3 items out of 6'.

Firewall

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

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

- [https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/
NAT#Masquerade](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:
configure dst-nat
configure src-nat
- Accept traffic in forward chain (example in previous slides)

Firewall

The screenshot shows the Mikrotik WinBox Firewall configuration window. The 'Filter Rules' tab is selected. The interface includes buttons for adding (+), removing (-), enabling (checkmark), disabling (X), and saving (floppy disk) rules. There are also buttons for 'Reset Counters' and 'Reset All Counters'. A search bar with the text 'Find' and a dropdown menu set to 'all' is present. The rule list table is as follows:

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

At the bottom left, it indicates '2 items'.

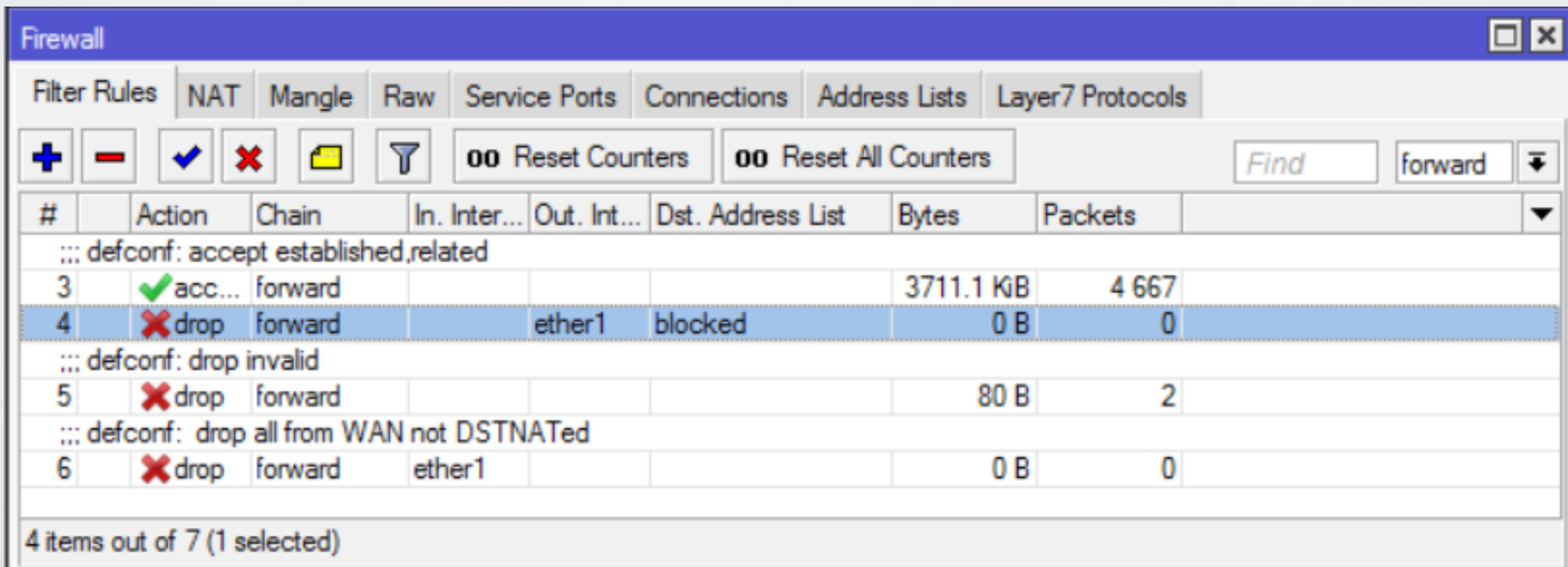
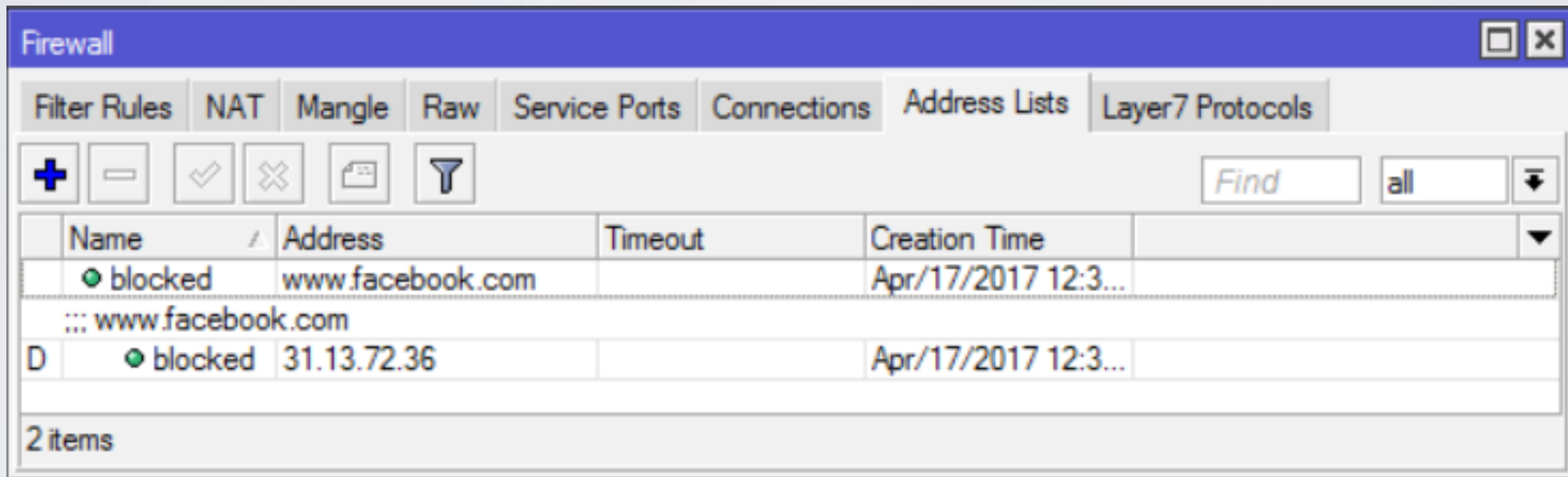
Firewall

- 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



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

#	Action	Chain	Proto...	Dst. Port	In. Inter...	Connection State	Src. Address List	Address List	Timeout	Bytes	Packets
::: defconf: accept ICMP											
0	✓ acc...	input	1 (ic...							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	867 2

7 items out of 11

Bandwidth Control

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

Firewall

Filter Rules

NAT

Mangle

Raw

Service Ports

Connections

Address Lists

Layer7 Protocols

+

-

✓

✗

📁

🔍

00 Reset Counters

00 Reset All Counters

Find

forward

⌵

#	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)

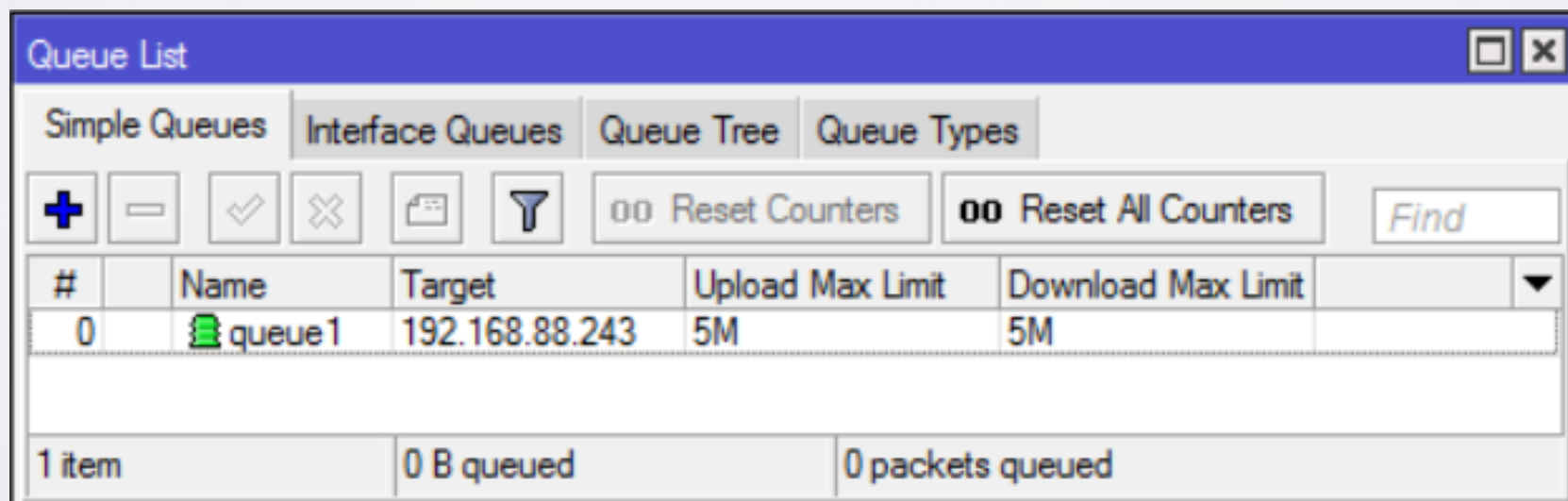
➡

Queues

- Add queues to limit traffic for specific resources

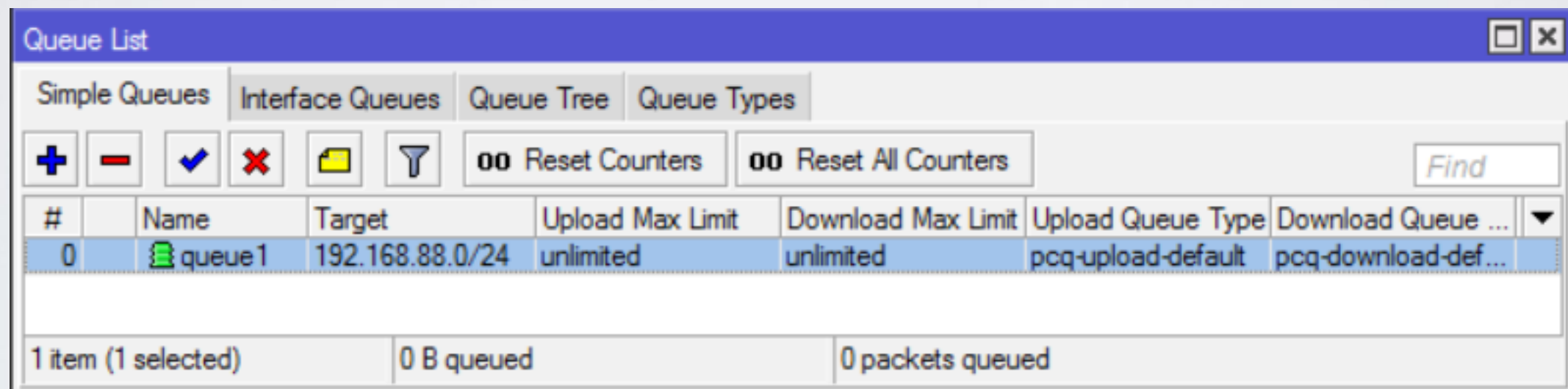
```
/queue simple add name=private
```

target=192.168.88.243 max-limit=5M/5M



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_Experienced_Users_of_RouterOS#Queues

Debugging tools

Logs

- 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

Logs

[illegible]

Debugging Tools

- Torch
- Analyse processed traffic
- https://wiki.mikrotik.com/wiki/Manual:Troubleshooting_tools#Torch_.28.2Ftool_torch.29

Debugging Tools

- Torch
- Analyse processed traffic
- https://wiki.mikrotik.com/wiki/Manual:Troubleshooting_tools#Torch_.28.2Ftool_torch.29

Debugging Tools

Torch

- Basic -
Interface:
Entry Timeout: s

- Collect -
☒ Src. Address ☐ Src. Address6
☒ Dst. Address ☐ Dst. Address6
☐ MAC Protocol ☒ Port
☒ Protocol ☐ VLAN Id
☐ DSCP

- Filters -
Src. Address:
Dst. Address:
Src. Address6:
Dst. Address6:
MAC Protocol:
Protocol:
Port:
VLAN Id:
DSCP:

Start
Stop
Close
New Window

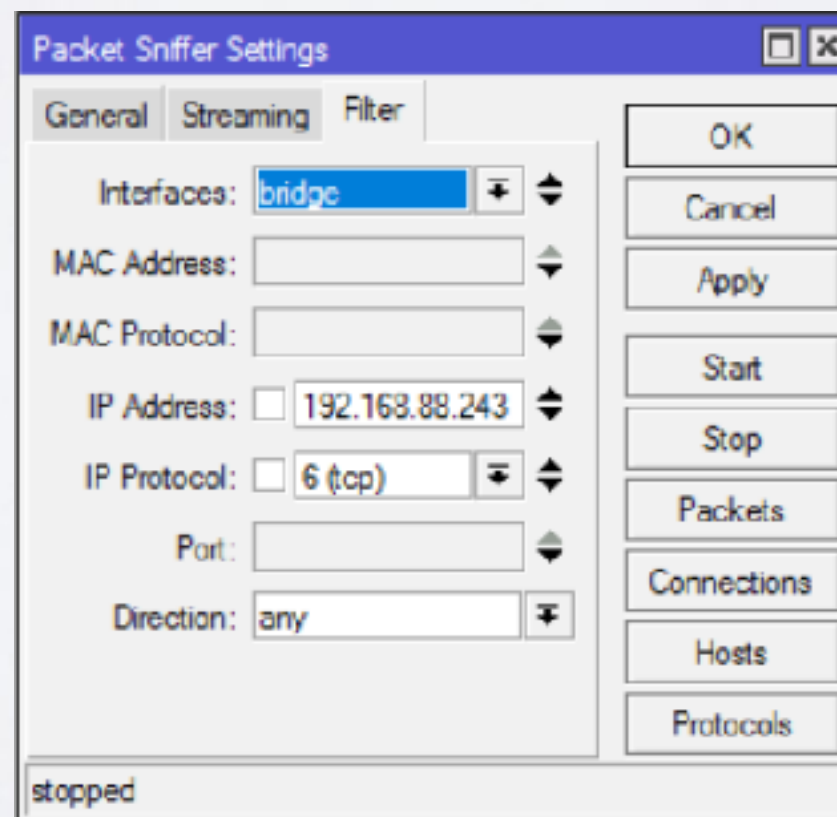
Et...	Prot...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...	
800 (ip)	6 (tcp)	172.16.1.243:55392	172.16.1.1:8291 (winbox)			156.3 k...	4.9 kbps	14	7	
800 (ip)	17 (...)	172.16.1.251:20148	85.234.190.33:17943			34.3 kbps	2.0 Mbps	68	178	
800 (ip)	17 (...)	172.16.1.251:137 (netbios...)	172.16.1.255:137 (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	

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

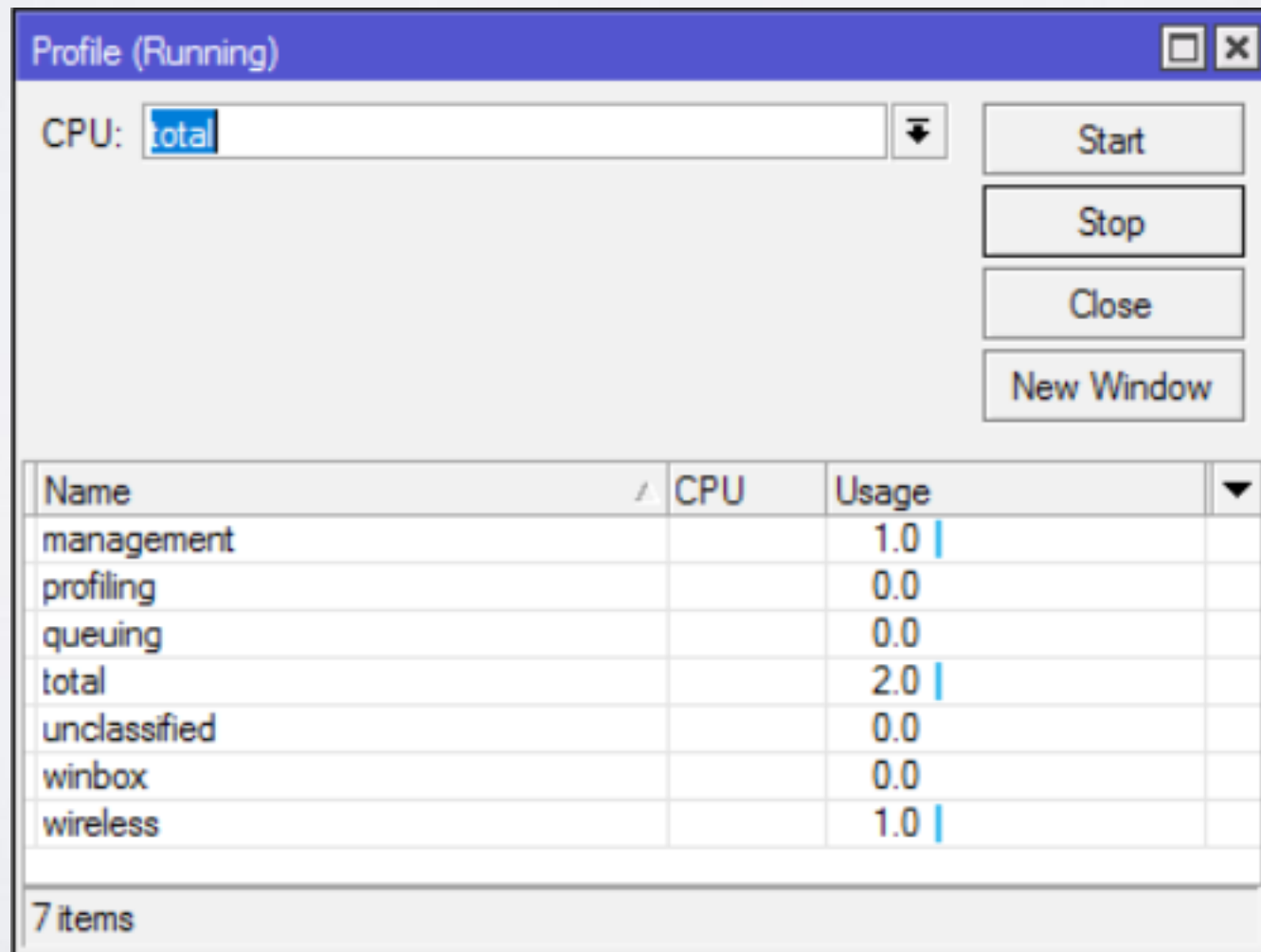
Manual:Troubleshooting_tools#Packet_Sniffer_.28.2Ftool_sniffer.29



Debugging Tools

- Profiler
- Find out current CPU usage

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



The screenshot shows the 'Profile (Running)' window from the Mikrotik Profiler tool. It features a dropdown menu for 'CPU' set to 'total', and four buttons: 'Start', 'Stop', 'Close', and 'New Window'. Below these is a table with 7 items, showing the CPU usage for different components. The 'total' usage is 2.0, with 'management' and 'wireless' each at 1.0, and 'profiling', 'queuing', 'unclassified', and 'winbox' each at 0.0.

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

7 items

Debugging Tools

- Graphing
- Find out information about Interfaces/Queues/
Resources per interval:
[https://wiki.mikrotik.com/wiki/Manual:Tools/
Graphing](https://wiki.mikrotik.com/wiki/Manual:Tools/Graphing)

Debugging Tools

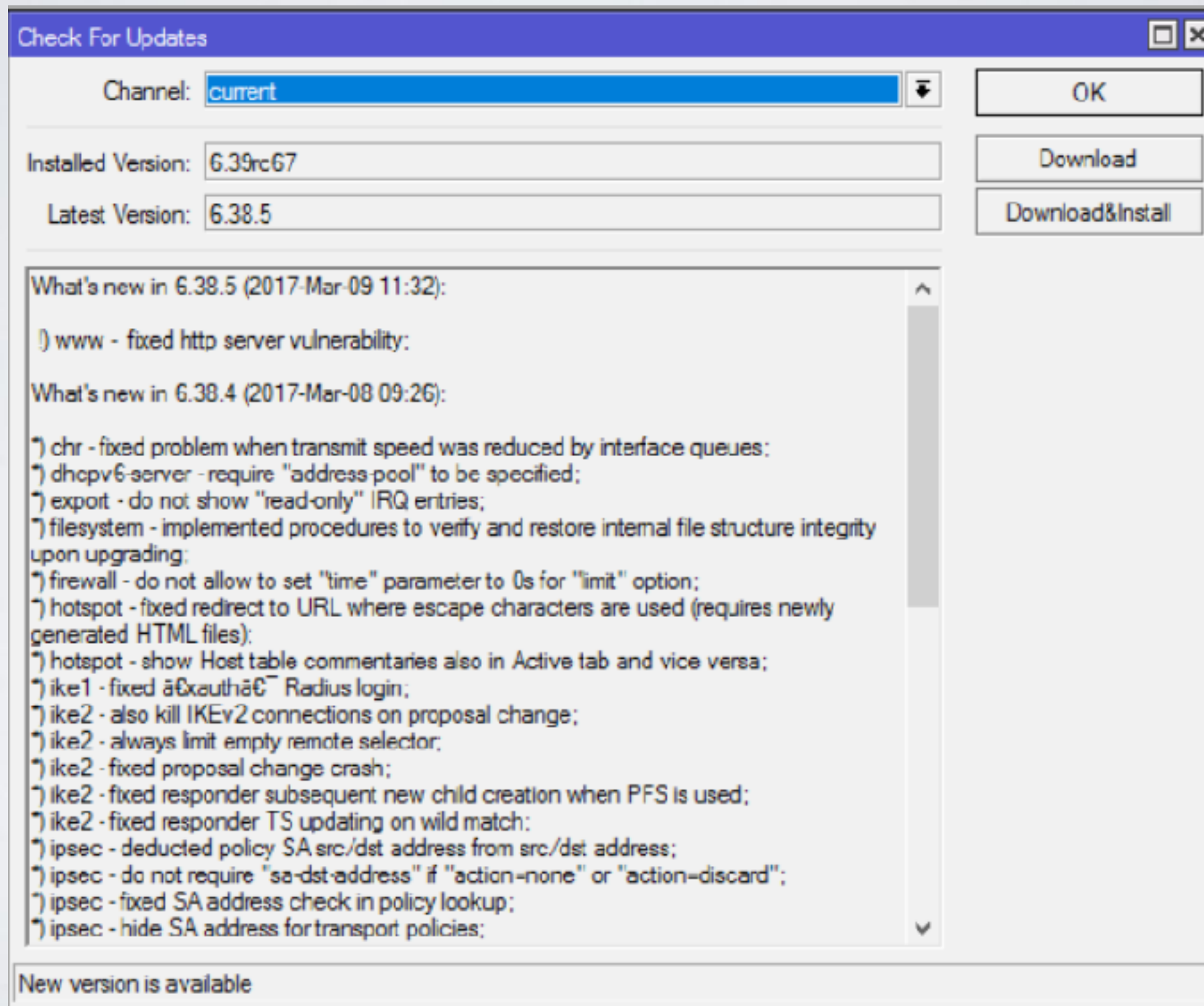
- The Dude
- Powerful network monitor tool:
https://wiki.mikrotik.com/wiki/Manual:The_Dude

Keep everything up-to-date

Upgrade Device

- Current
Latest full release (tested on many different scenarios for a long time) with all fully implemented features
- Bugfix
Latest full release (tested on many different scenarios for a long time and admitted as trustworthy) with all safe fixes

Upgrade Device



When software stops working?

Troubleshoot issue

- 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>

Troubleshoot issue

- 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 issue

- 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

Hardware Troubleshooting

Hardware Troubleshooting

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

MikroTik 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)

Software Issues

- Device freezes
 - 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 your problem
- Send all files (mentioned in previous slides depending on problem)
- Make notes and document results (even if problem persists)
- Make new files after configuration changes
- Reply within same ticket and provide new information



MikroTik

The image features the MikroTik logo, which consists of the word "Mikro" in a stylized, italicized sans-serif font, followed by "Tik" in a bold, italicized sans-serif font. Above the "i" in "Mikro" are three curved lines representing signal waves. The entire logo is rendered in a dark gray color and is positioned on a light gray background. Below the logo, there is a faint, semi-transparent reflection of the logo itself.