MikroTik

Basic guidelines on RouterOS configuration and debugging

Tokyo, Japan

May 2018

RouterOS is the **same** everywhere

Management Tools

RouterOS Management tools

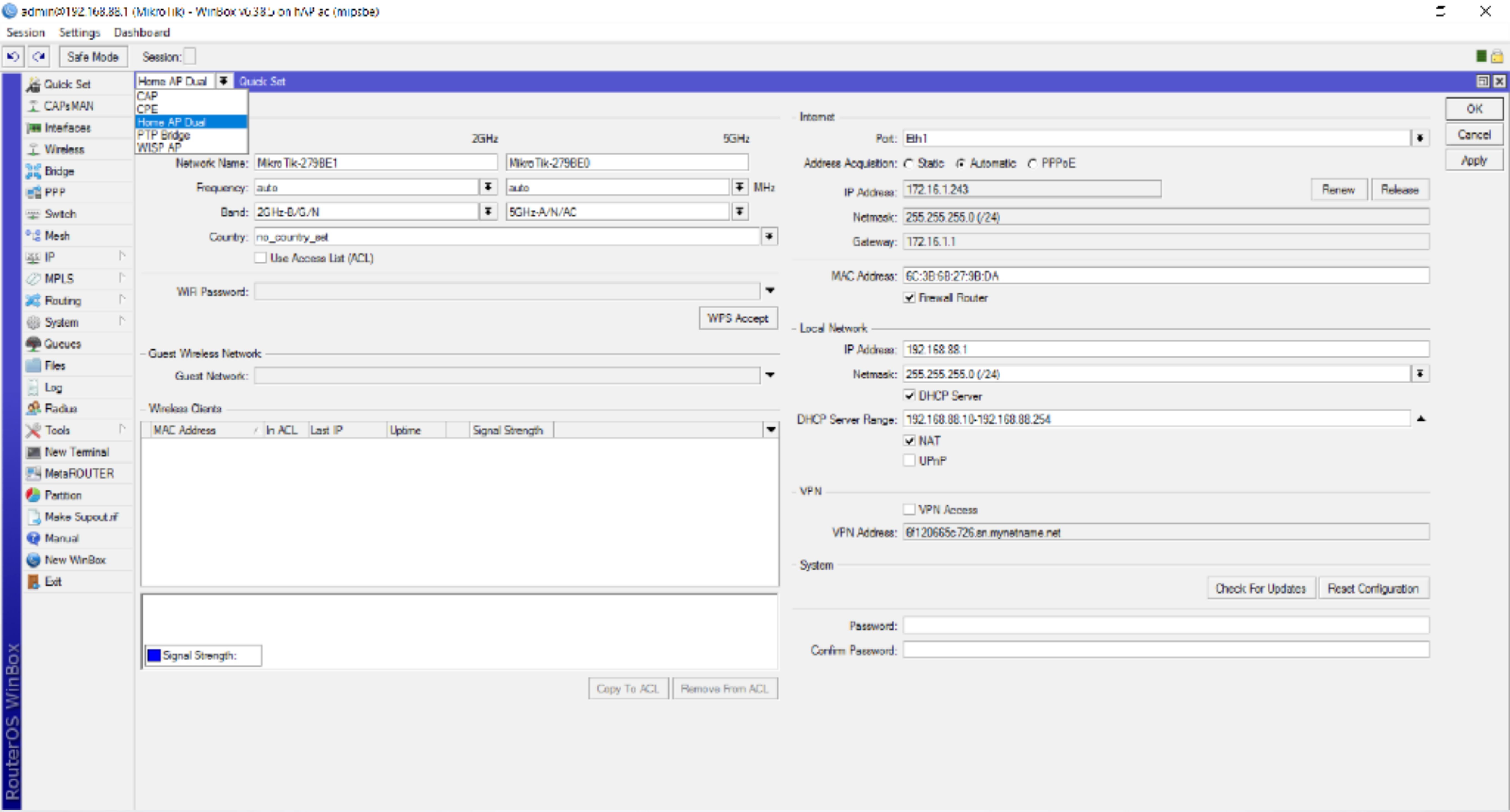
- CLI (Command Line Interface)
  https://wiki.mikrotik.com/wiki/Manual:Console

- 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



	2GHz	5GHz
Network Name:	MikroTik-279BE1	MikroTik-279BE0
Frequency:	auto	auto MHz
Band:	2GHz-B/G/N	5GHz-A/N/AC
Country:	no_country_set	

□ Use Access List (ACL)

WiFi Password:

Guest Wireless Network

Guest Network:

Wireless Clients

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:27:9B: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

Password:

Confirm Password:

QuickSet

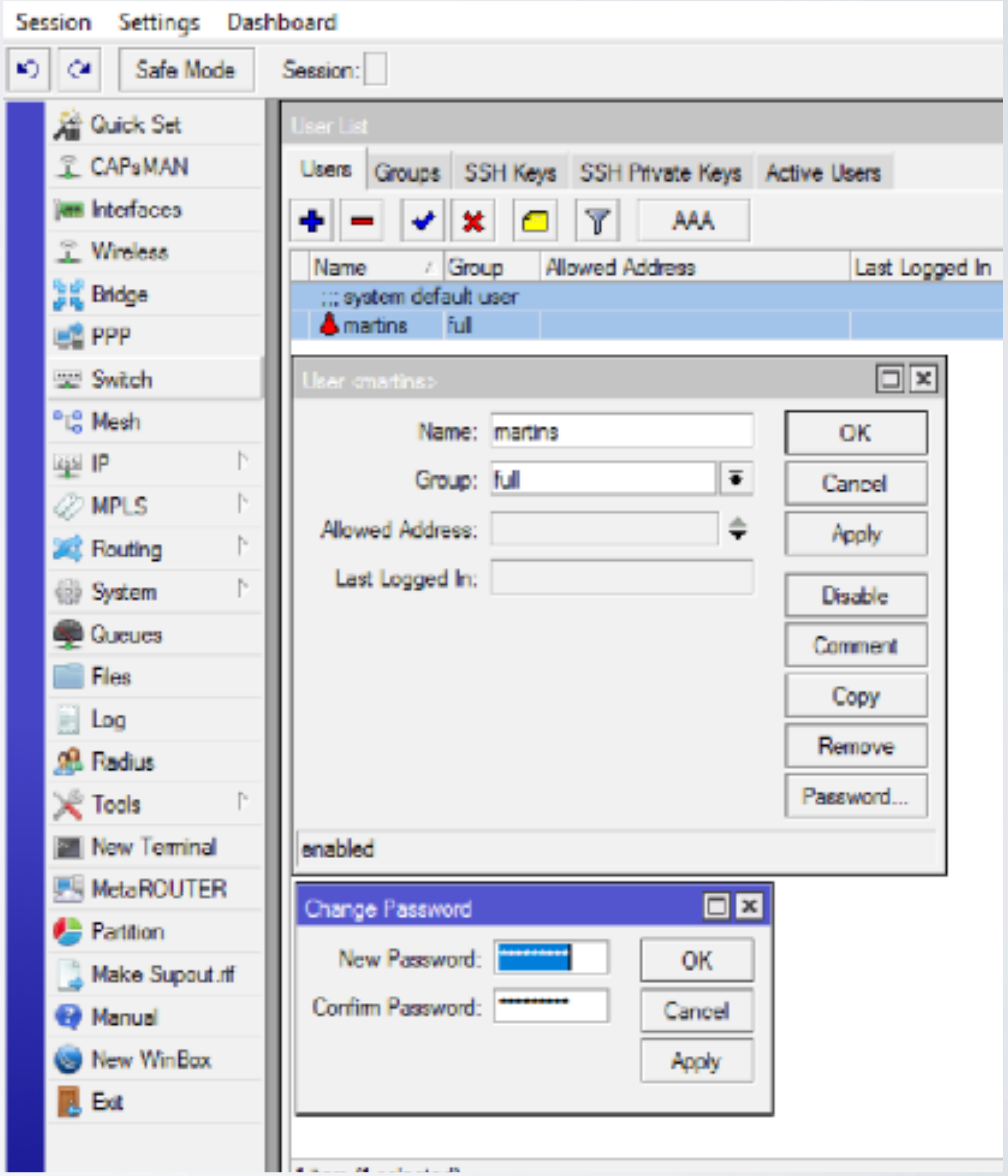
QuickSet

- 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=martins



Name	Group	Allowed Address	Last Logged In
;;; system default user			
martins	full		

User <martins>

Name: martins

Group: full

Allowed Address:

Last Logged In:

enabled

Change Password

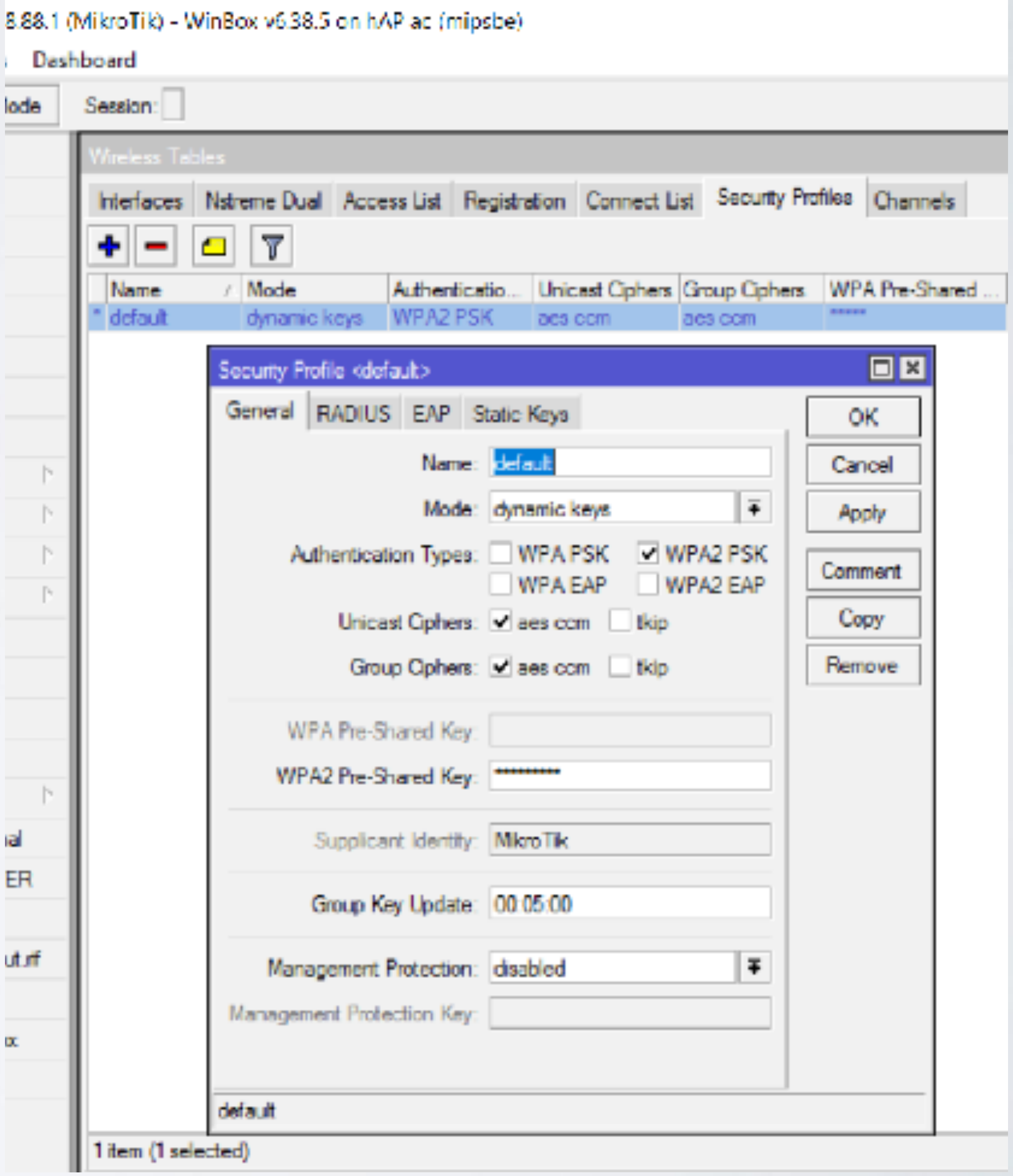
New Password: **********

Confirm Password: **********

Simple Security

- Specify password for wireless access

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



	Name	Mode	Authenticatio...	Unicast Ciphers	Group Ciphers	WPA Pre-Shared ...
*	default	dynamic keys	WPA2 PSK	aes ccm	aes ccm	*****

Name: default

Mode: dynamic keys

Authentication Types: □ WPA PSK ☑ WPA2 PSK □ WPA EAP □ WPA2 EAP

Unicast Ciphers: ☑ aes ccm □ tkip

Group Ciphers: ☑ aes ccm □ tkip

WPA Pre-Shared Key:

WPA2 Pre-Shared Key: **********

Supplicant Identity: MikroTik

Group Key Update: 00:05:00

Management Protection: disabled

Management Protection Key:

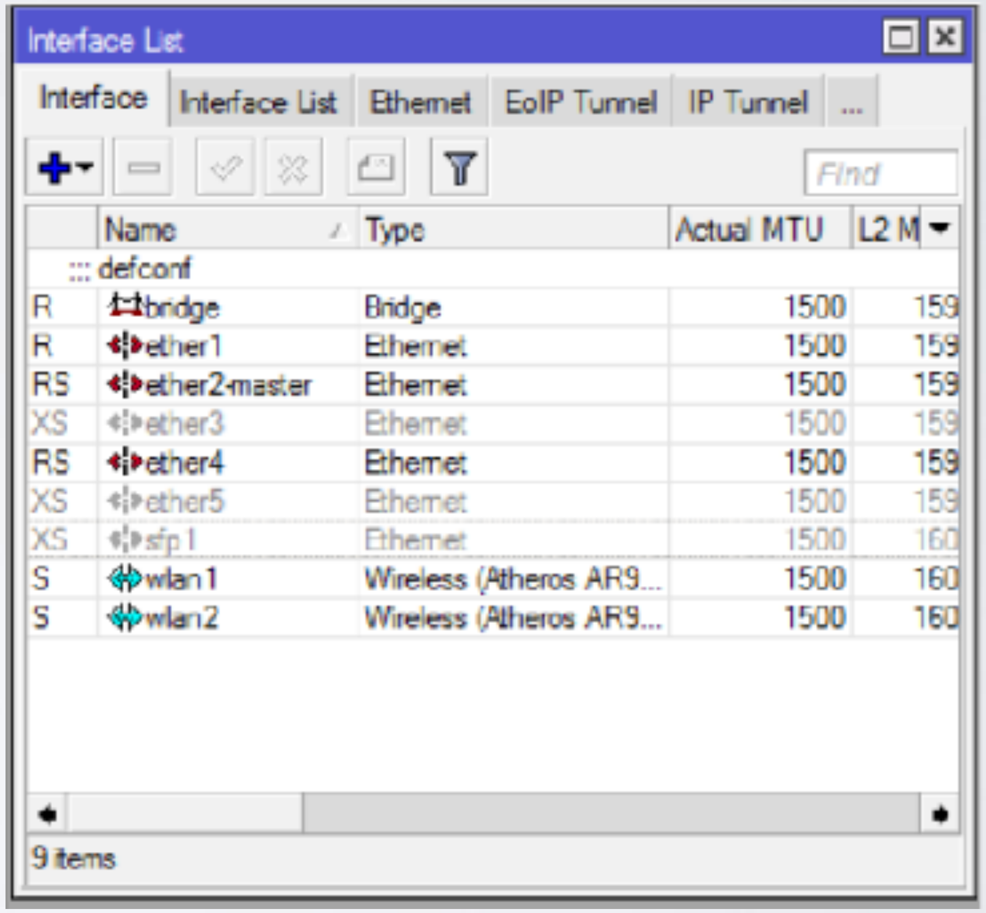
default

1 item (1 selected)

Security

- Disable unused interfaces

  /interface ethernet disable ether3,ether5,sfp1



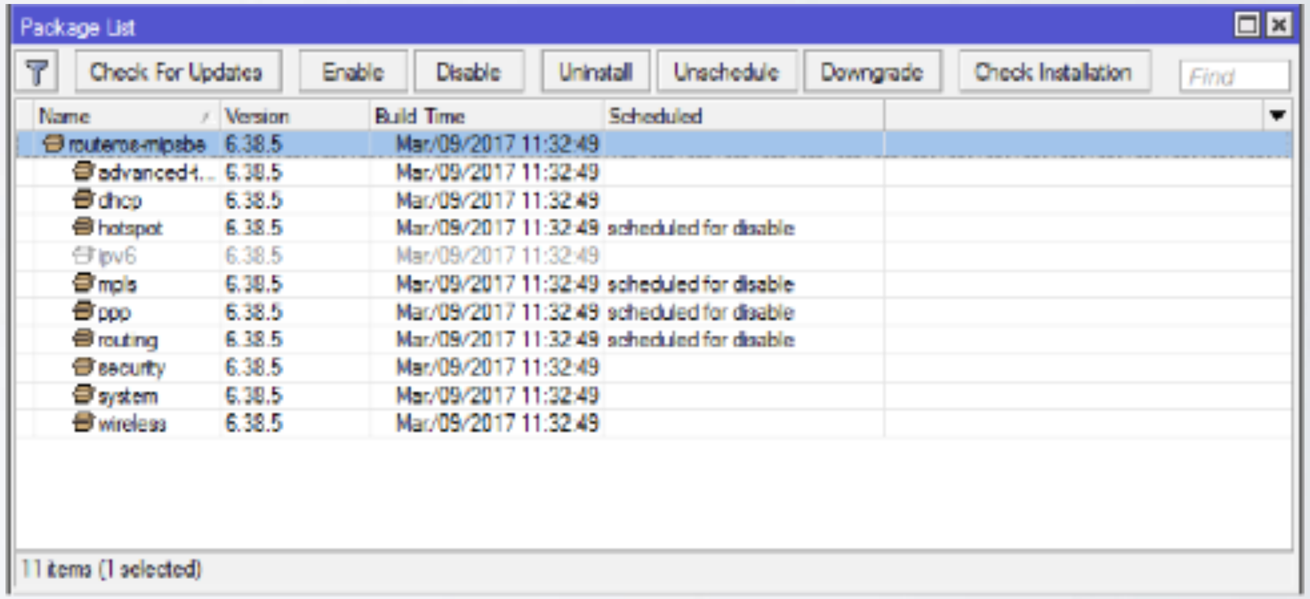
	Name	Type	Actual MTU	L2 M
	::: defconf			
R	bridge	Bridge	1500	159
R	ether1	Ethernet	1500	159
RS	ether2-master	Ethernet	1500	159
XS	ether3	Ethernet	1500	159
RS	ether4	Ethernet	1500	159
XS	ether5	Ethernet	1500	159
XS	sfp1	Ethernet	1500	160
S	wlan1	Wireless (Atheros AR9...	1500	160
S	wlan2	Wireless (Atheros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

9 items

Security

- Disable unused packages (mainly IPv6)

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



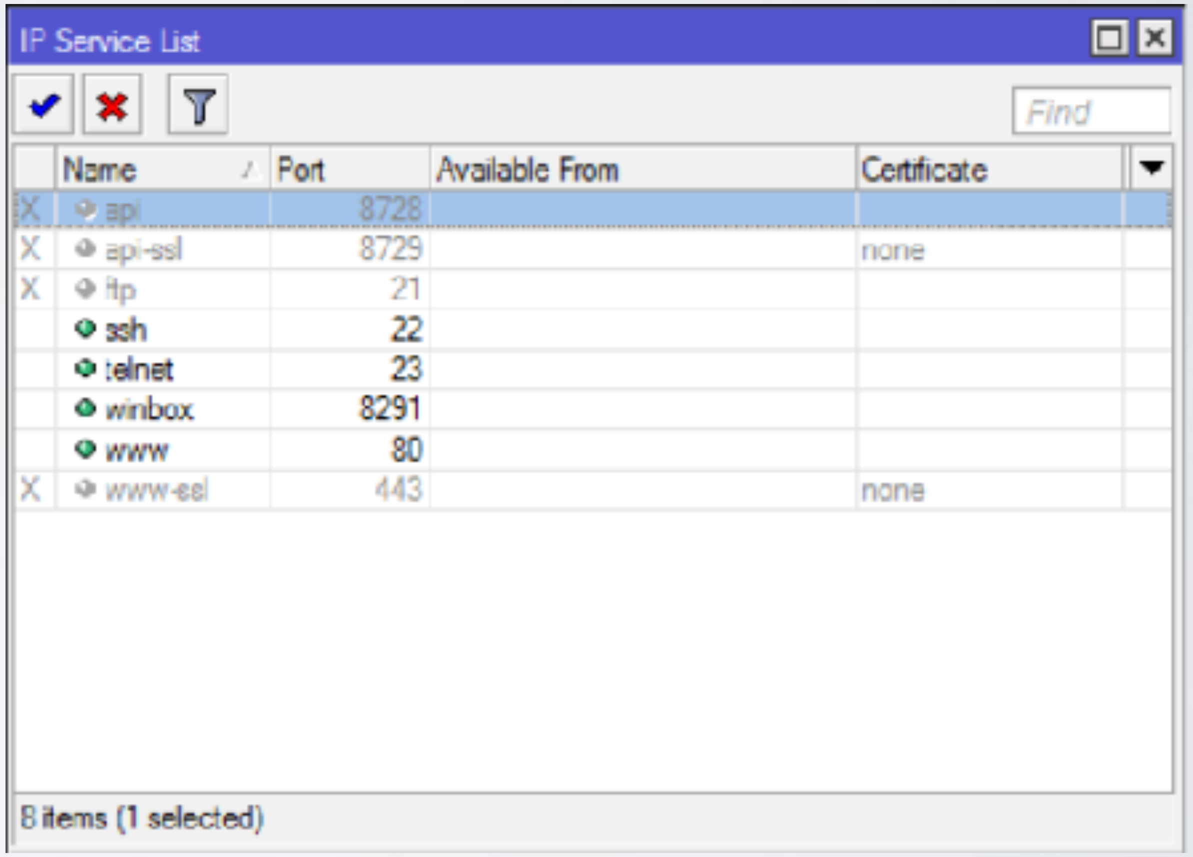
Name	Version	Build Time	Scheduled
routeros-mipsbe	6.38.5	Mar/09/2017 11:32:49	
advanced-t...	6.38.5	Mar/09/2017 11:32:49	
dhcp	6.38.5	Mar/09/2017 11:32:49	
hotspot	6.38.5	Mar/09/2017 11:32:49	scheduled for disable
ipv6	6.38.5	Mar/09/2017 11:32:49	
mpls	6.38.5	Mar/09/2017 11:32:49	scheduled for disable
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
```



IP Service List

	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)

Security

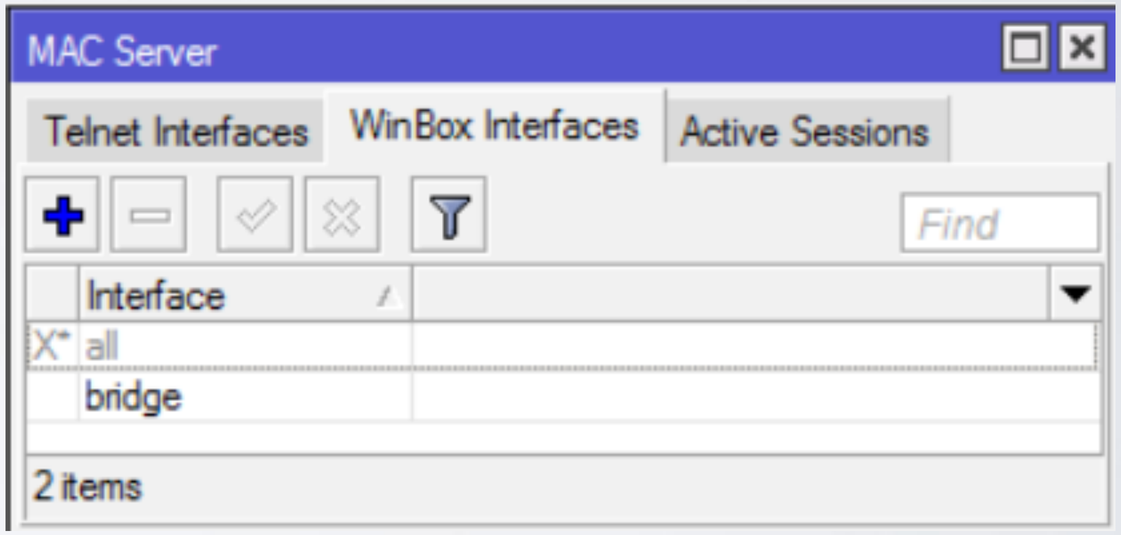
- Adjust MAC access

```
/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
```



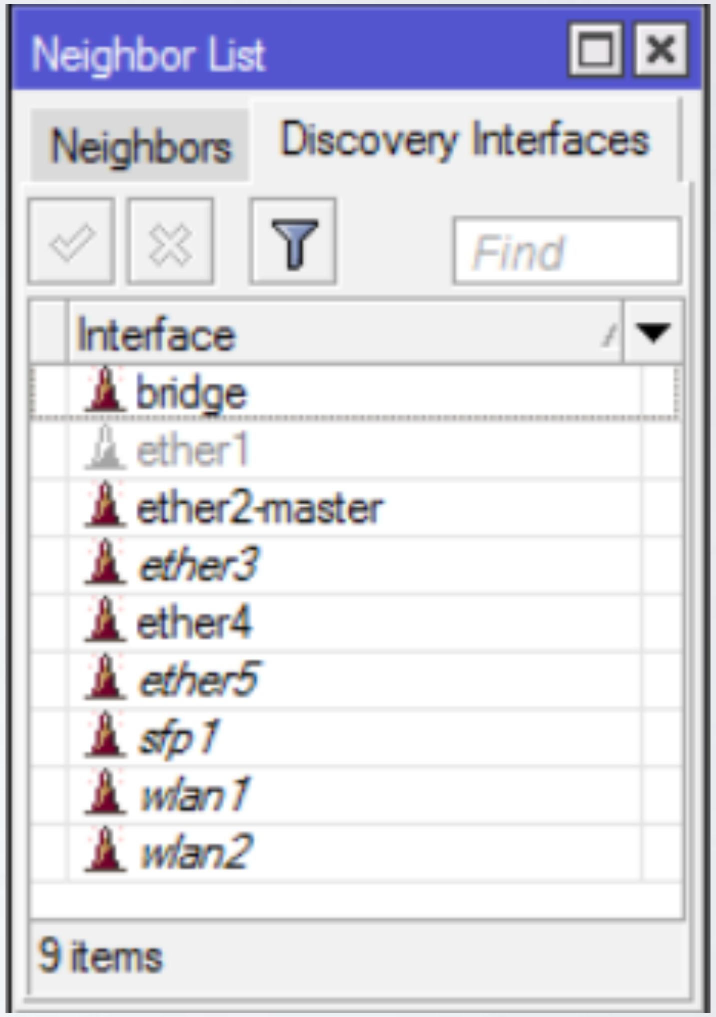
	Interface
X*	all
	bridge

2 items

Security

- Hide device in Neighbor Discovery

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



Interface
bridge
ether1
ether2-master
ether3
ether4
ether5
sfp1
wlan1
wlan2

9 items

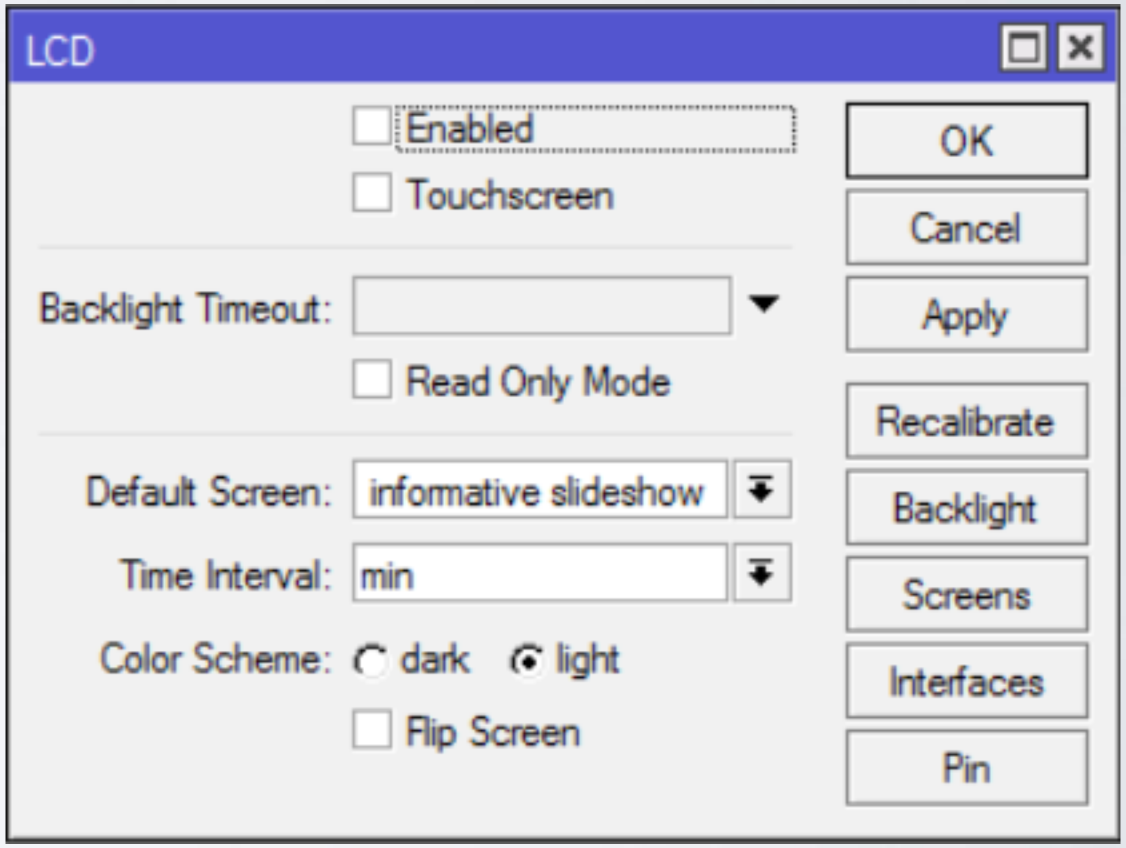
Security

- 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



LCD

□ Enabled
□ Touchscreen

Backlight Timeout:

□ Read Only Mode

Default Screen: informative slideshow

Time Interval: min

Color Scheme: ○ dark ● light

□ Flip Screen

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)

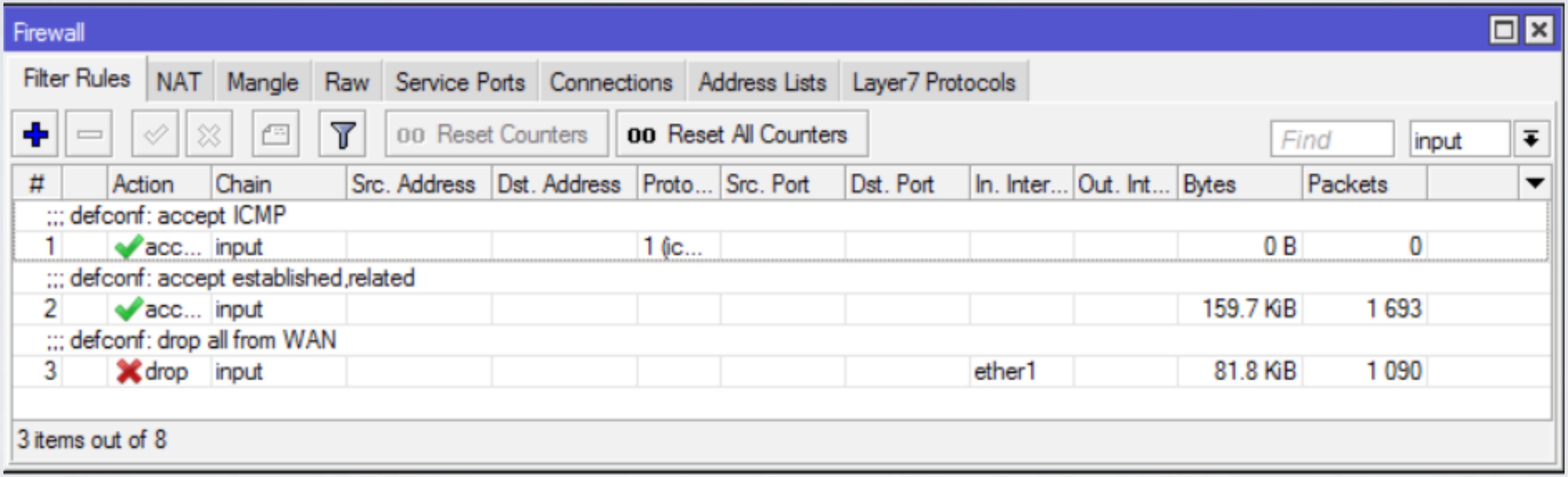
```
/ip firewall filter add chain=forward action=accept src-address=192.168.88.2 out-interface=ether1
/ip firewall filter add chain=forward action=drop src-address=192.168.88.0/24 out-interface=ether1
```

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



#		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 KiB	1 693
;;; defconf: drop all from WAN												
3		✗drop	input						ether1		81.8 KiB	1 090

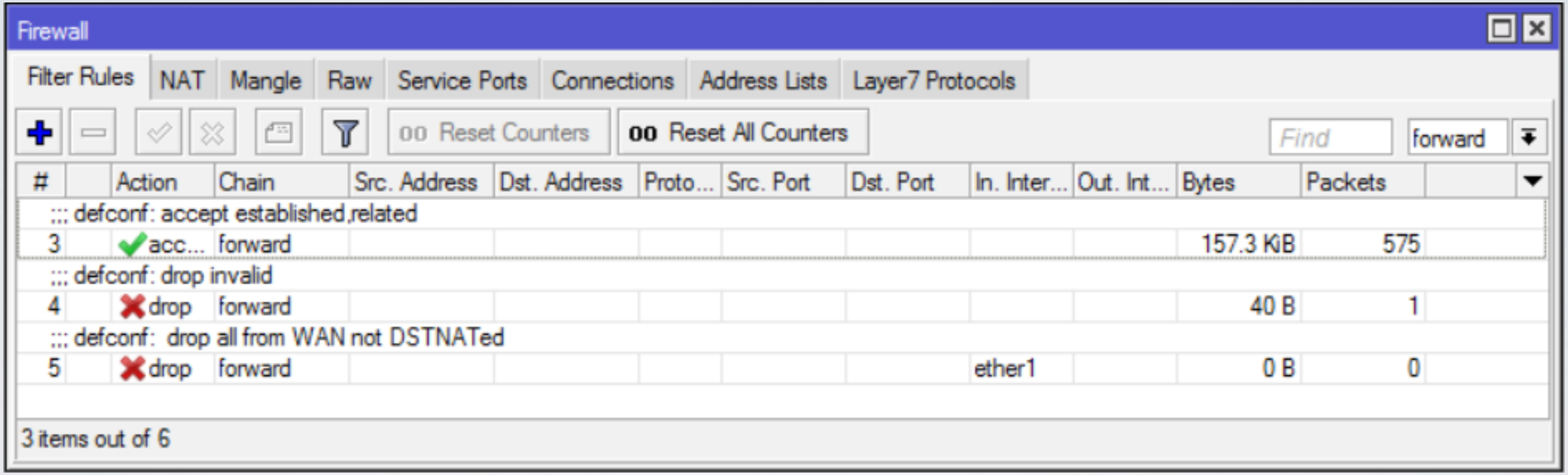
3 items out of 8

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



#		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

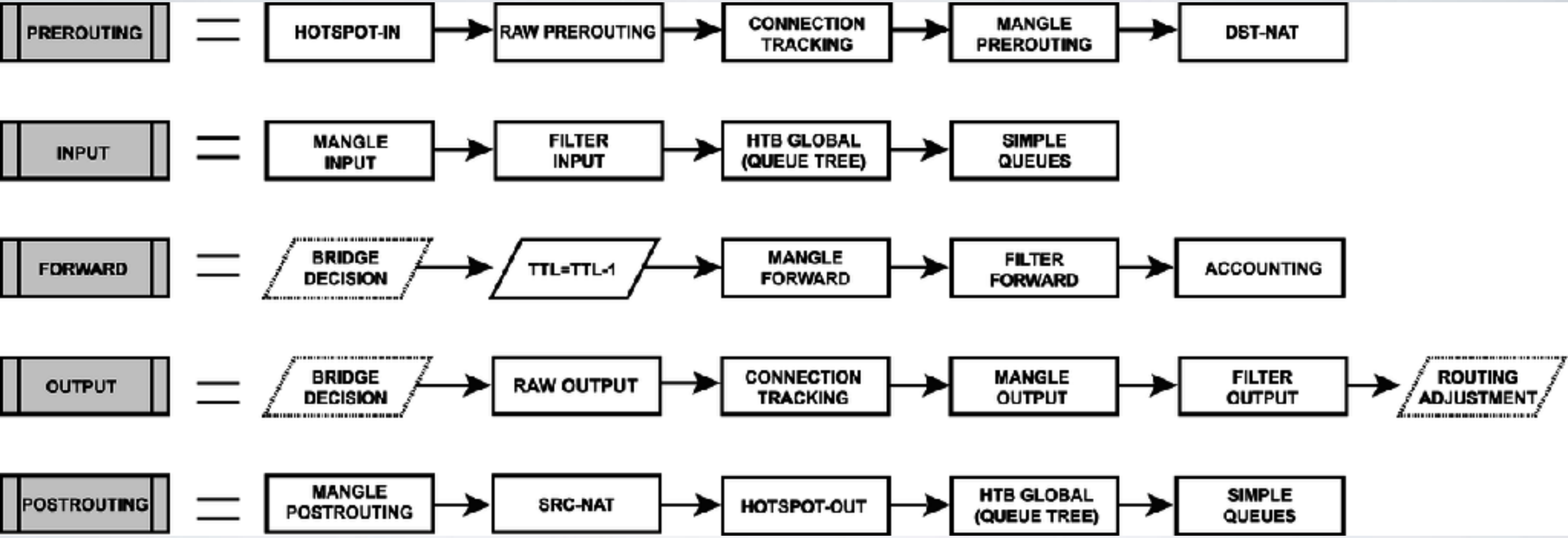
3 items out of 6

Firewall

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

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

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



Firewall

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

Firewall

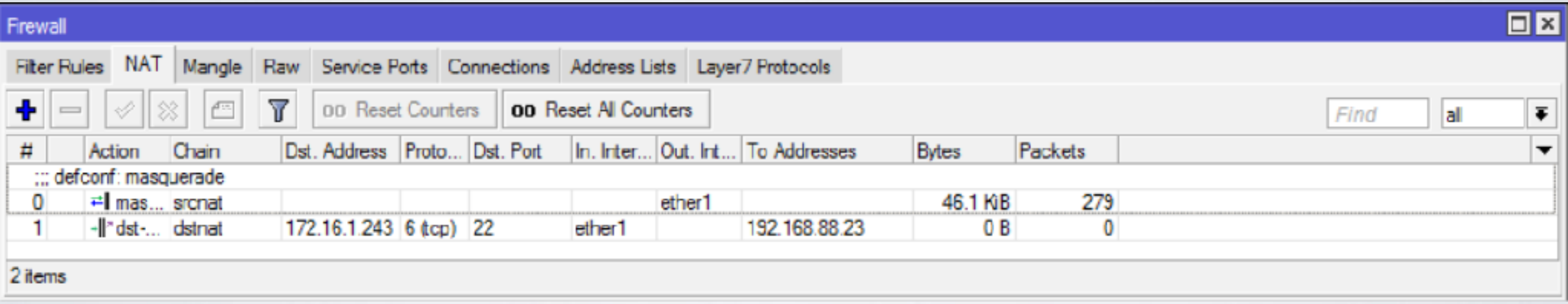
- NAT to LAN

  ```
  /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



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

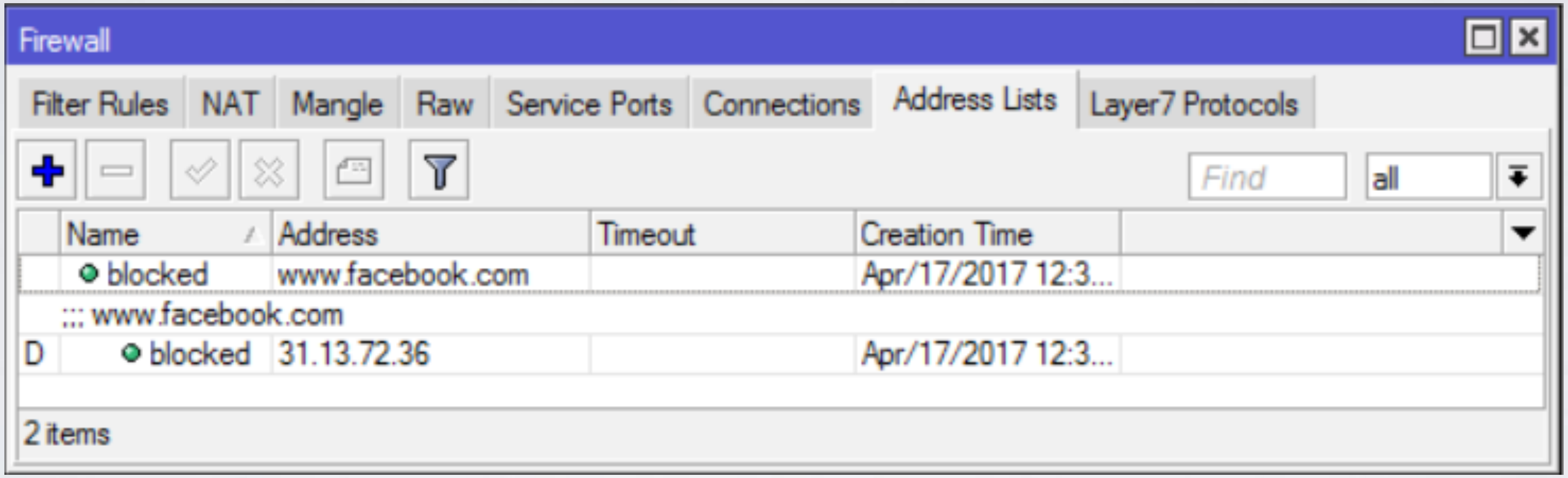
2 items

Firewall

- Block specific traffic

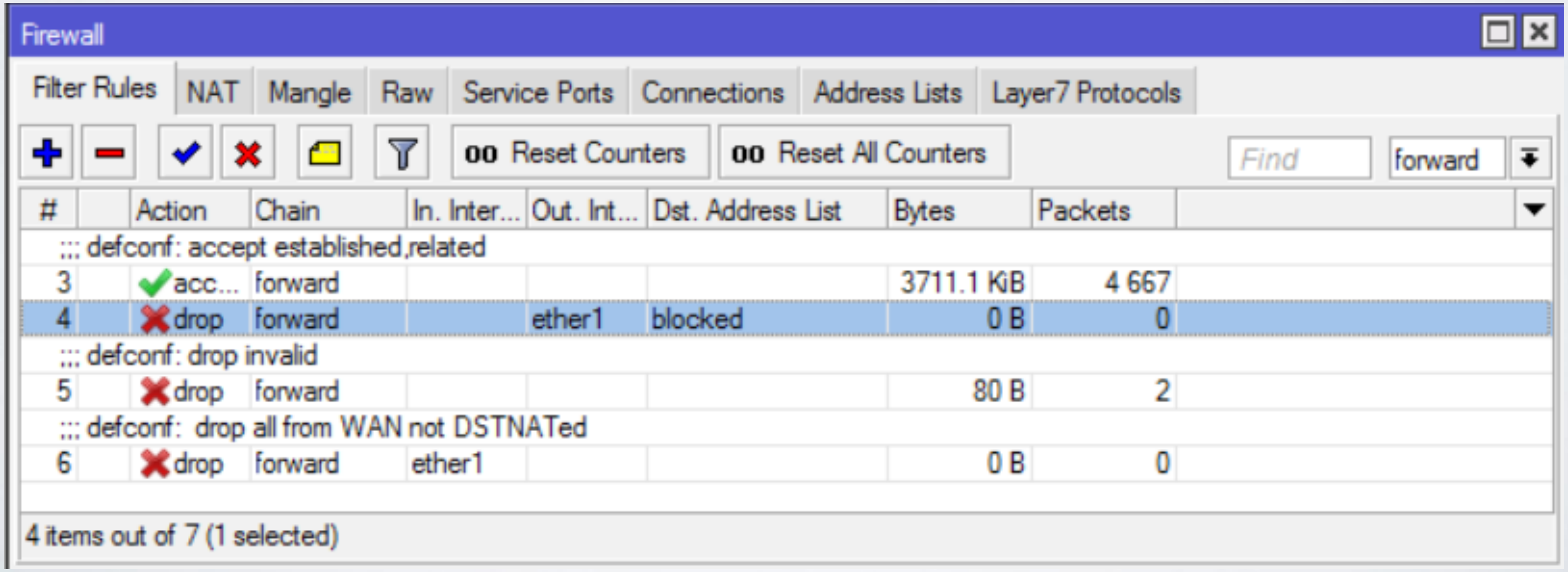
```
/ip firewall address-list add list=blocked
address=www.facebook.com
/ip firewall filter add chain=forward action=drop
dst-address-list=blocked out-interface=ether1
```

Firewall



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

2 items



#		Action	Chain	In. Inter...	Out. Int...	Dst. Address List	Bytes	Packets
;;; defconf: accept established,related								
3		✓ acc...	forward				3711.1 KiB	4 667
4		✗ drop	forward		ether1	blocked	0 B	0
;;; defconf: drop invalid								
5		✗ drop	forward				80 B	2
;;; defconf: drop all from WAN not DSTNATed								
6		✗ drop	forward	ether1			0 B	0

4 items out of 7 (1 selected)

Firewall

- Protect device against attacks if you allow particular access

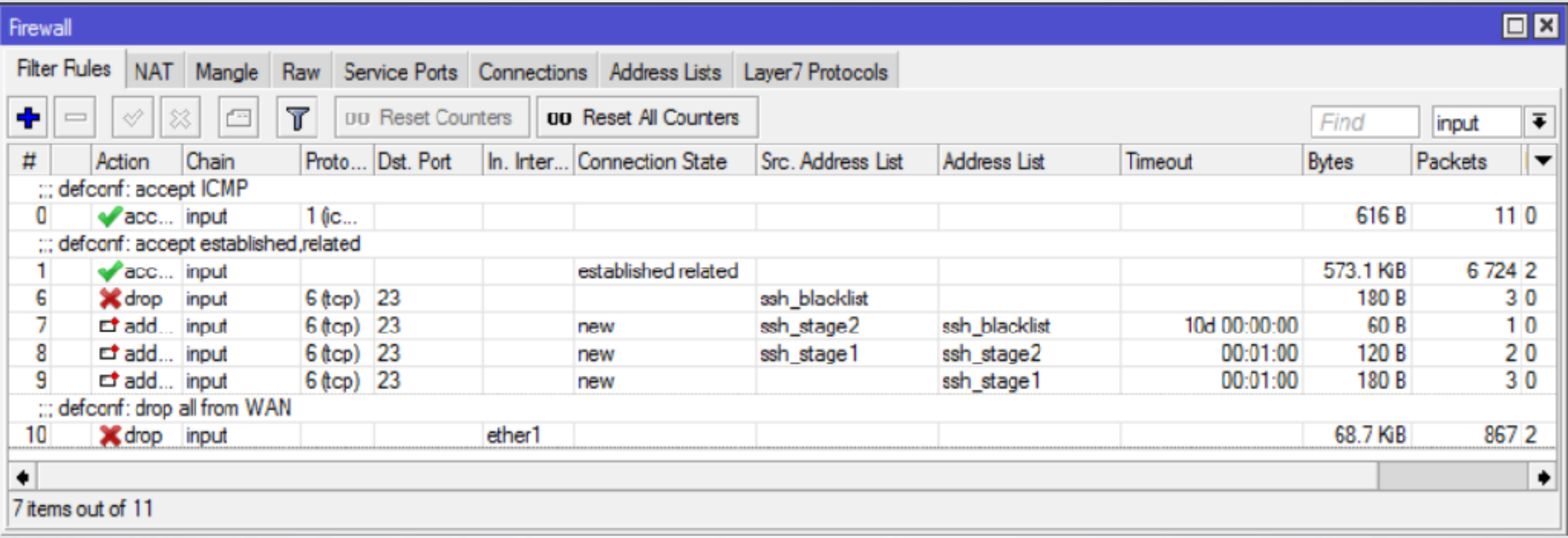
```
/ip firewall filter
add chain=input protocol=tcp dst-port=22 src-address-list=ssh_blacklist action=drop

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
```

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 KiB	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 KiB	867	2

7 items out of 11

Bandwidth Control

FastTrack

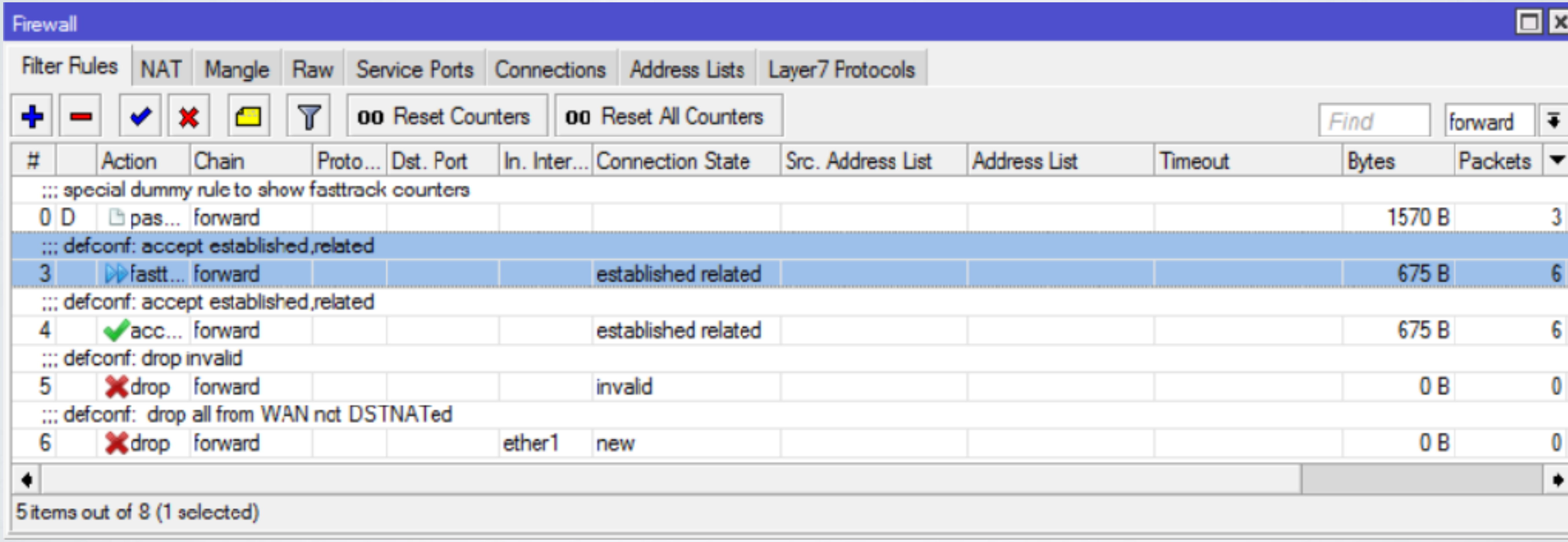
- Remember this rule?

```
/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



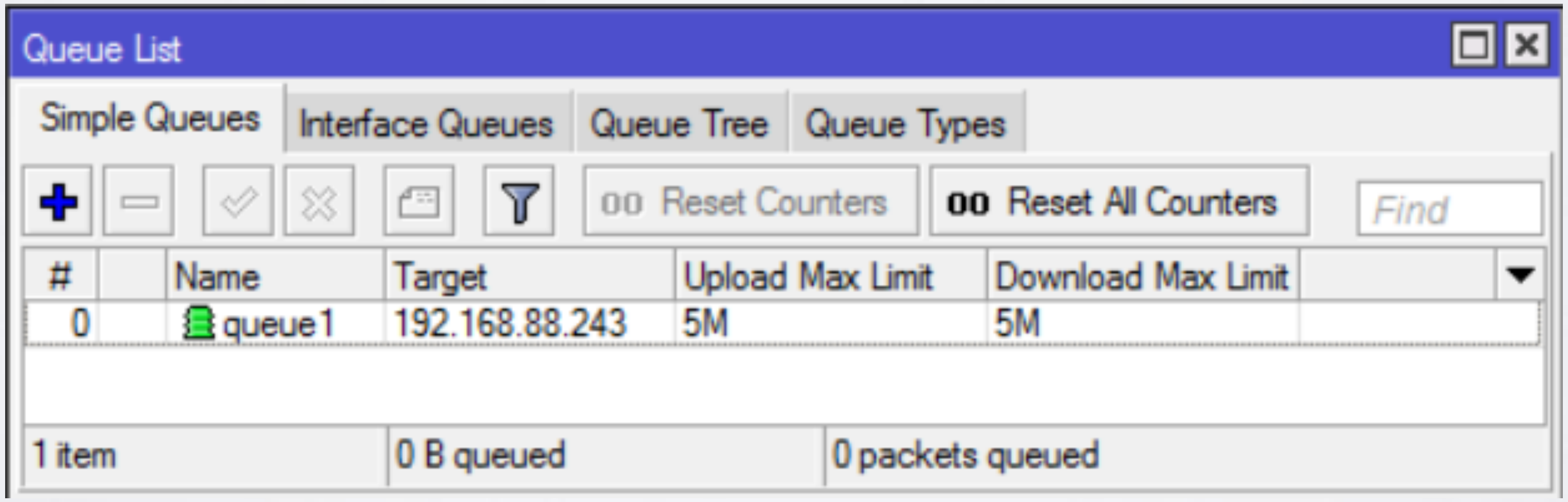
#		Action	Chain	Proto...	Dst. Port	In. Inter...	Connection State	Src. Address List	Address List	Timeout	Bytes	Packets
;;; special dummy rule to show fasttrack counters												
0	D	pas...	forward								1570 B	3
;;; defconf: accept established,related												
3		fastt...	forward				established 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
```



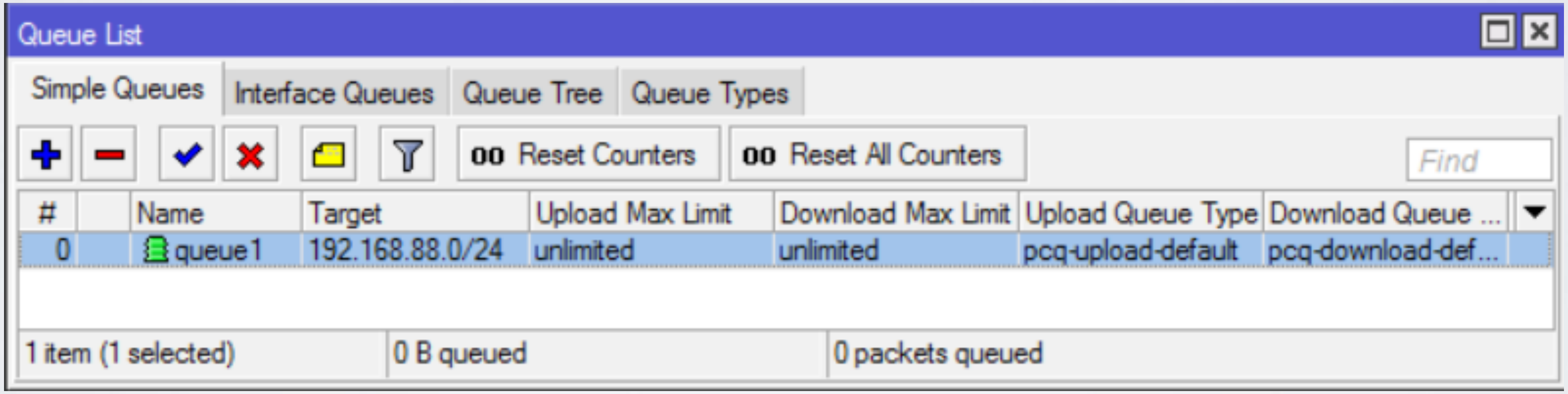
#		Name	Target	Upload Max Limit	Download Max Limit
0		queue1	192.168.88.243	5M	5M

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_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:
```

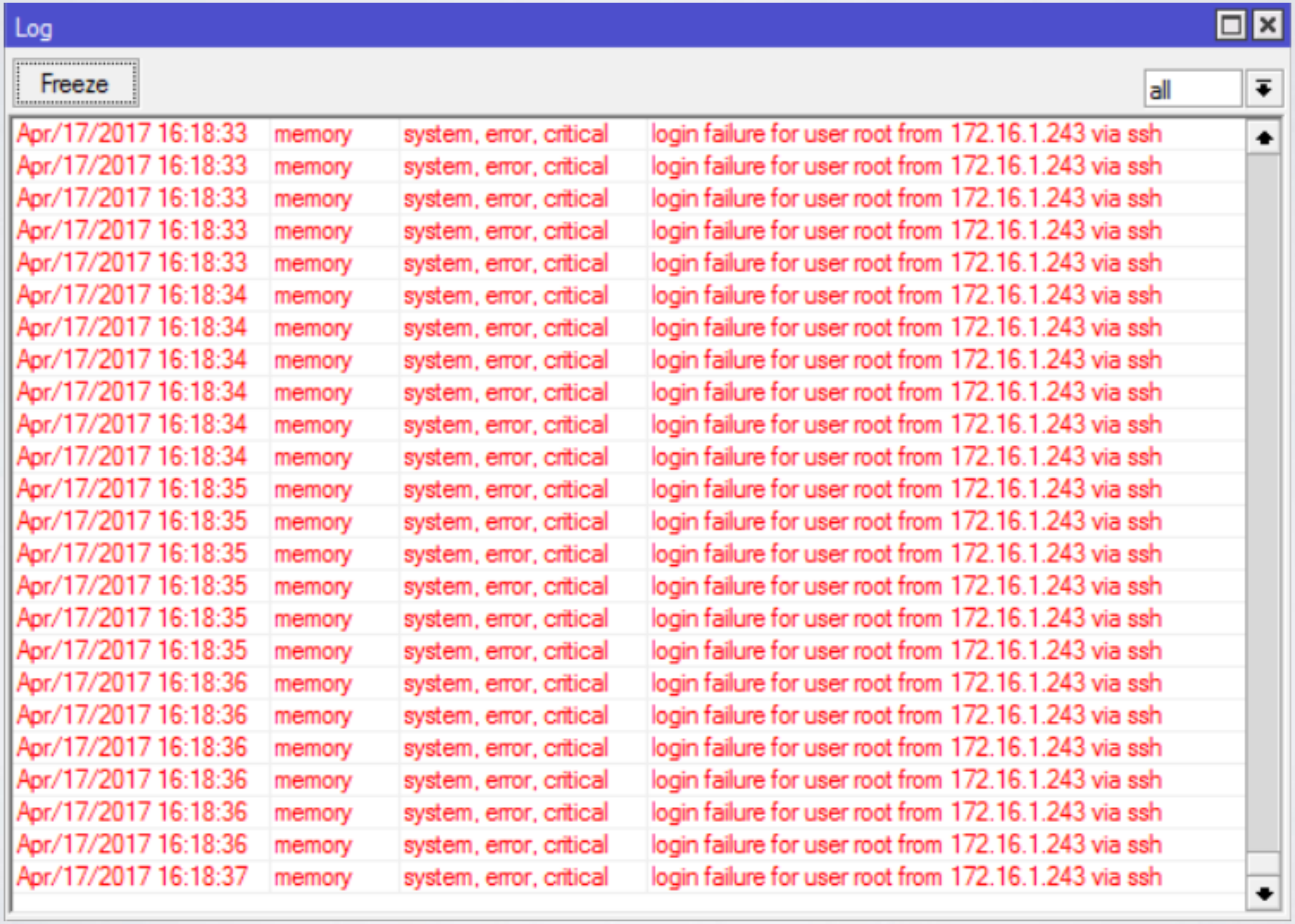
- Use logging for debug topics

```
/system logging add topics=l2tp,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

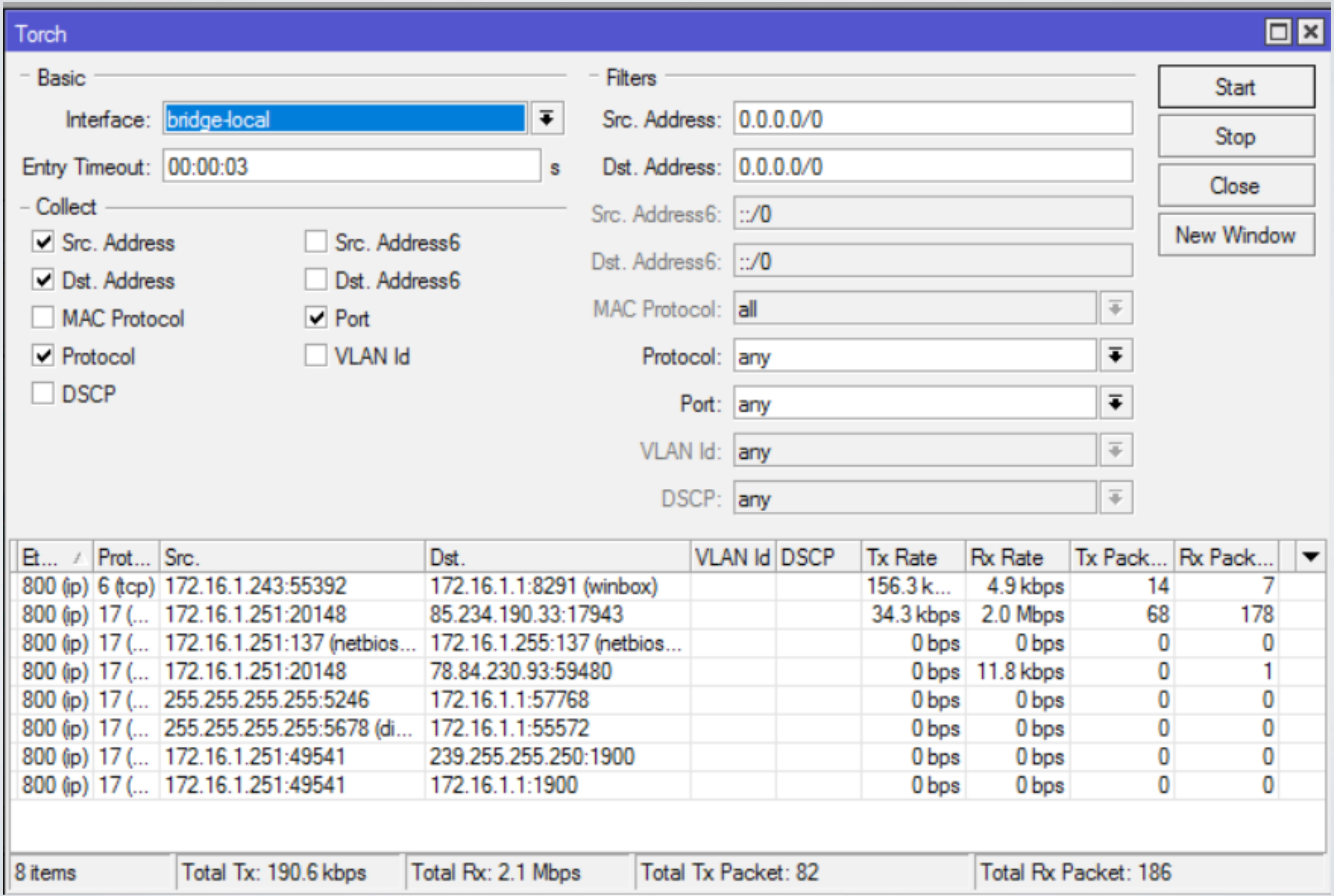


```
Apr/17/2017 16:18:33  memory  system, error, critical  login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:33  memory  system, error, critical  login failure for user root from 172.16.1.243 via ssh
Apr/17/2017 16:18:33  memory  system, error, critical  login failure for user root 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 16:18:36  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
```

Debugging Tools

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

Debugging Tools



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

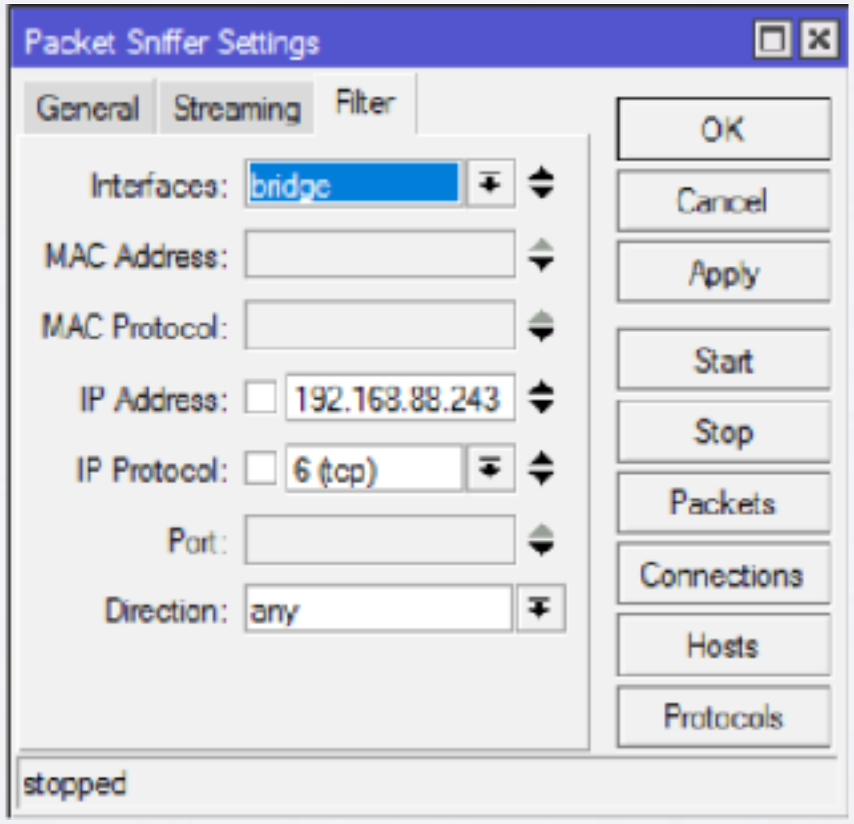
Et...	Prot...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	6 (tcp)	172.16.1.243:55392	172.16.1.1:8291 (winbox)			156.3 k...	4.9 kbps	14	7
800 (ip)	17 (...	172.16.1.251:20148	85.234.190.33:17943			34.3 kbps	2.0 Mbps	68	178
800 (ip)	17 (...	172.16.1.251:137 (netbios...	172.16.1.255:137 (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/Manual:Troubleshooting_tools#Packet_Sniffer_.28.2Ftool_sniffer.29



Interfaces: bridge

MAC Address:

MAC Protocol:

IP Address: □ 192.168.88.243

IP Protocol: □ 6 (tcp)

Port:

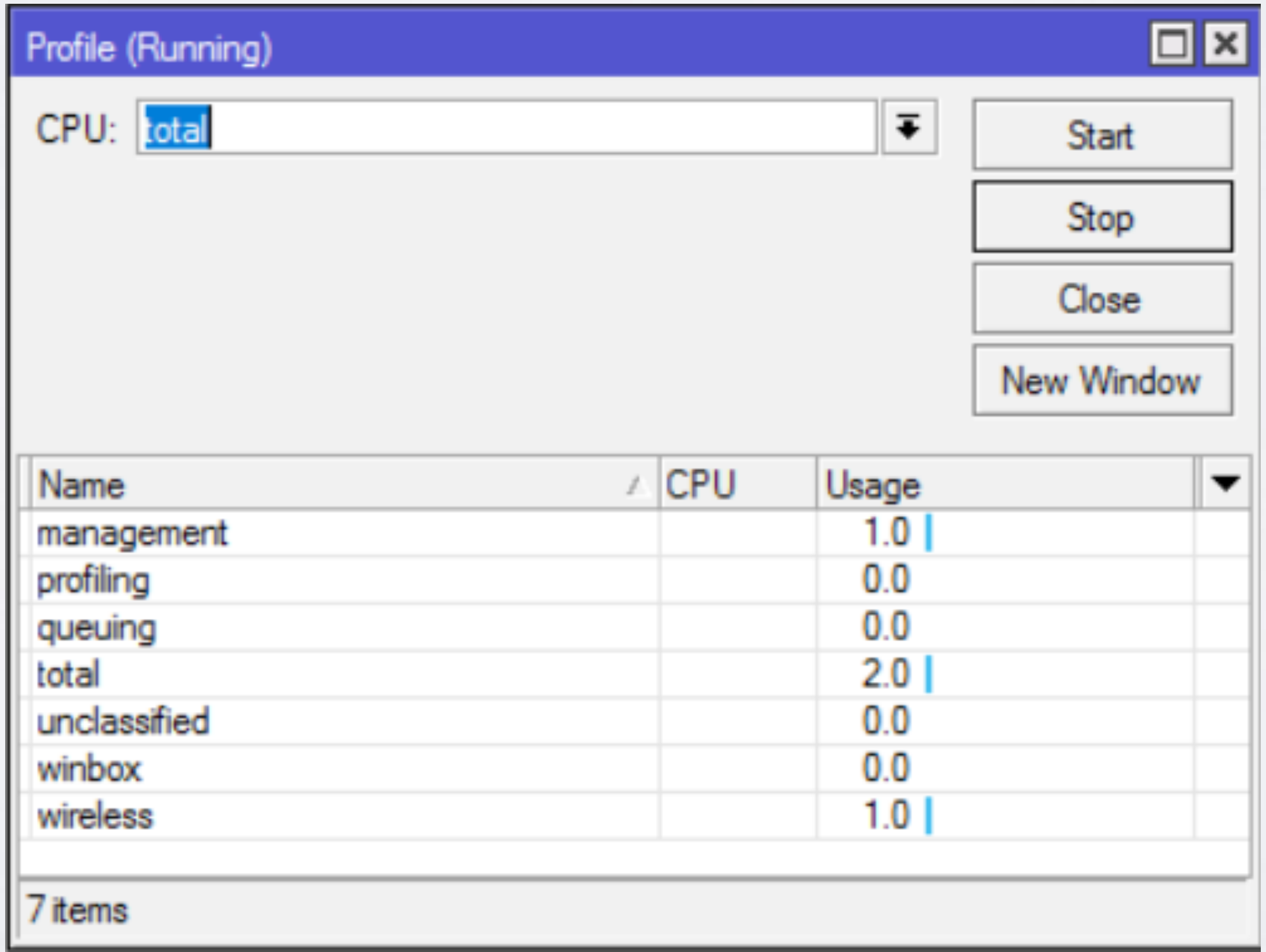
Direction: any

stopped

Debugging Tools

- Profiler

- Find out current CPU usage
  https://wiki.mikrotik.com/wiki/Manual:Tools/Profiler



CPU: total

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

Debugging Tools

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

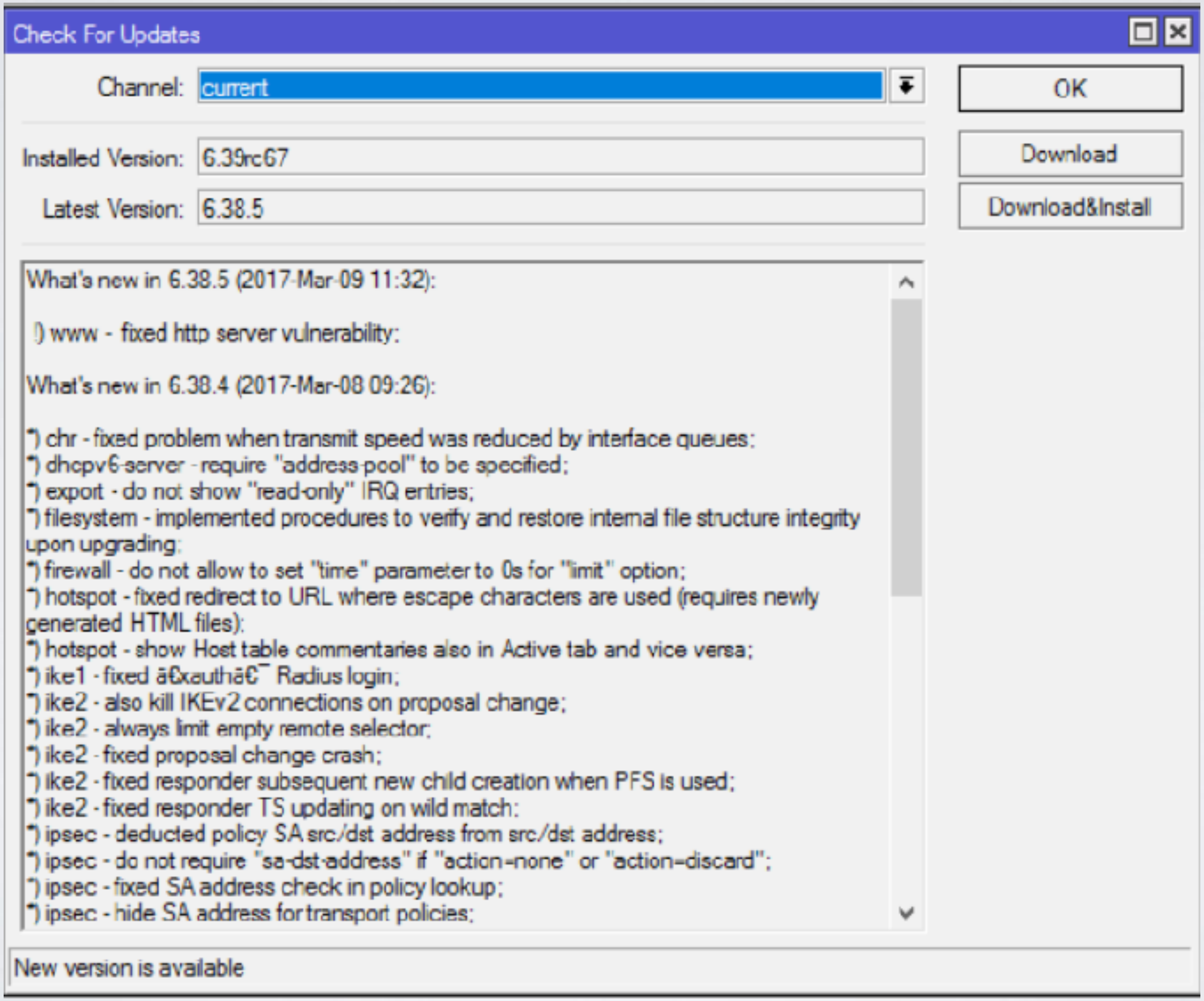
Keep everything up-to-date

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



Channel: current

Installed Version: 6.39rc67

Latest Version: 6.38.5

```
What's new in 6.38.5 (2017-Mar-09 11:32):

 !) www - fixed http server vulnerability;

What's new in 6.38.4 (2017-Mar-08 09:26):

*) chr - fixed problem when transmit speed was reduced by interface queues;
*) dhcpv6-server - require "address-pool" to be specified;
*) export - do not show "read-only" IRQ entries;
*) filesystem - implemented procedures to verify and restore internal file structure integrity
upon upgrading;
*) firewall - do not allow to set "time" parameter to 0s for "limit" option;
*) hotspot - fixed redirect to URL where escape characters are used (requires newly
generated HTML files);
*) hotspot - show Host table commentaries also in Active tab and vice versa;
*) ike1 - fixed â€œauthâ€˜ Radius login;
*) ike2 - also kill IKEv2 connections on proposal change;
*) ike2 - always limit empty remote selector;
*) ike2 - fixed proposal change crash;
*) ike2 - fixed responder subsequent new child creation when PFS is used;
*) ike2 - fixed responder TS updating on wild match;
*) ipsec - deducted policy SA src/dst address from src/dst address;
*) ipsec - do not require "sa-dst-address" if "action=none" or "action=discard";
*) ipsec - fixed SA address check in policy lookup;
*) ipsec - hide SA address for transport policies;
```

New version is available

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