Basic guidelines on RouterOS configuration and debugging

Tokyo, Japan

May 2018

RouterOS is the **same** everywhere

Management Tools

RouterOS Management tools

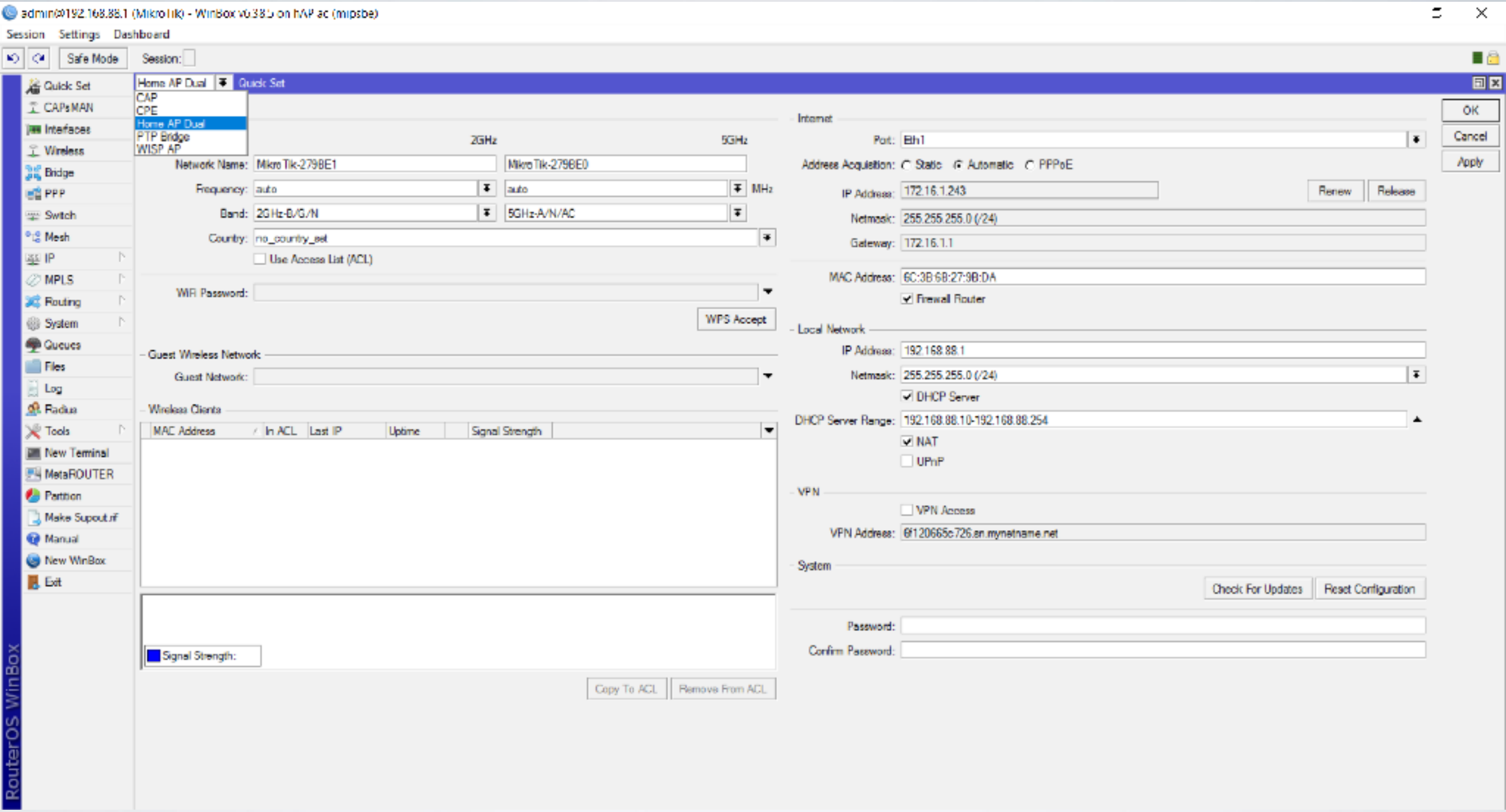
- CLI (Command Line Interface)
  https://wiki.mikrotik.com/wiki/Manual:Console

- 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


admin@192.168.88.1 (MikroTik) - WinBox v6.38.5 on hAP ac (mipsbe)
Session Settings Dashboard
Safe Mode
Session:
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit
RouterOS WinBox
Home AP Dual
CAP
CPE
Home AP Dual
PTP Bridge
WISP AP
Quick Set
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:
ether1
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:27:9B: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
Check For Updates
Reset Configuration
Password:
Confirm Password:
OK
Cancel
Apply

QuickSet

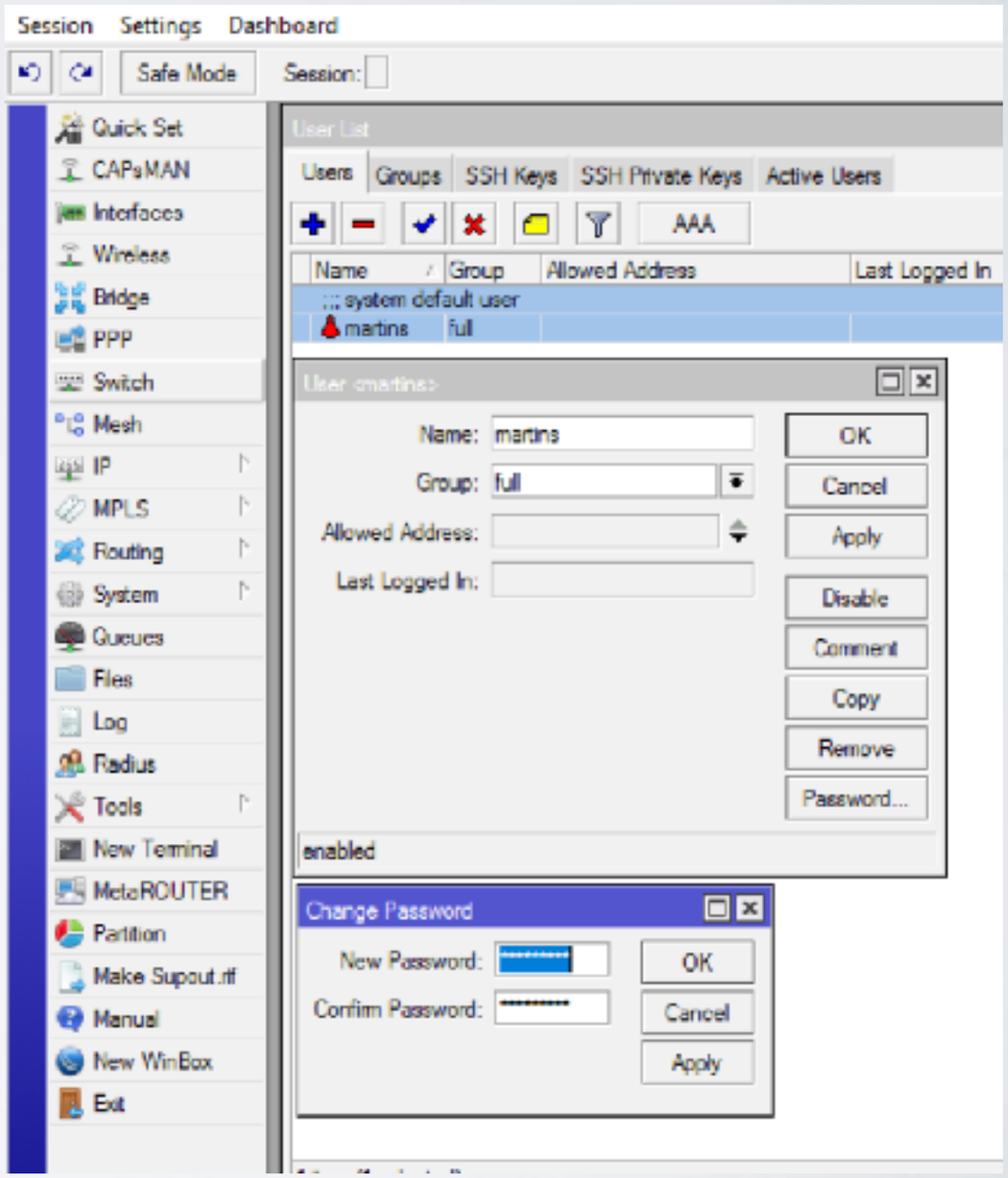
QuickSet

- 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

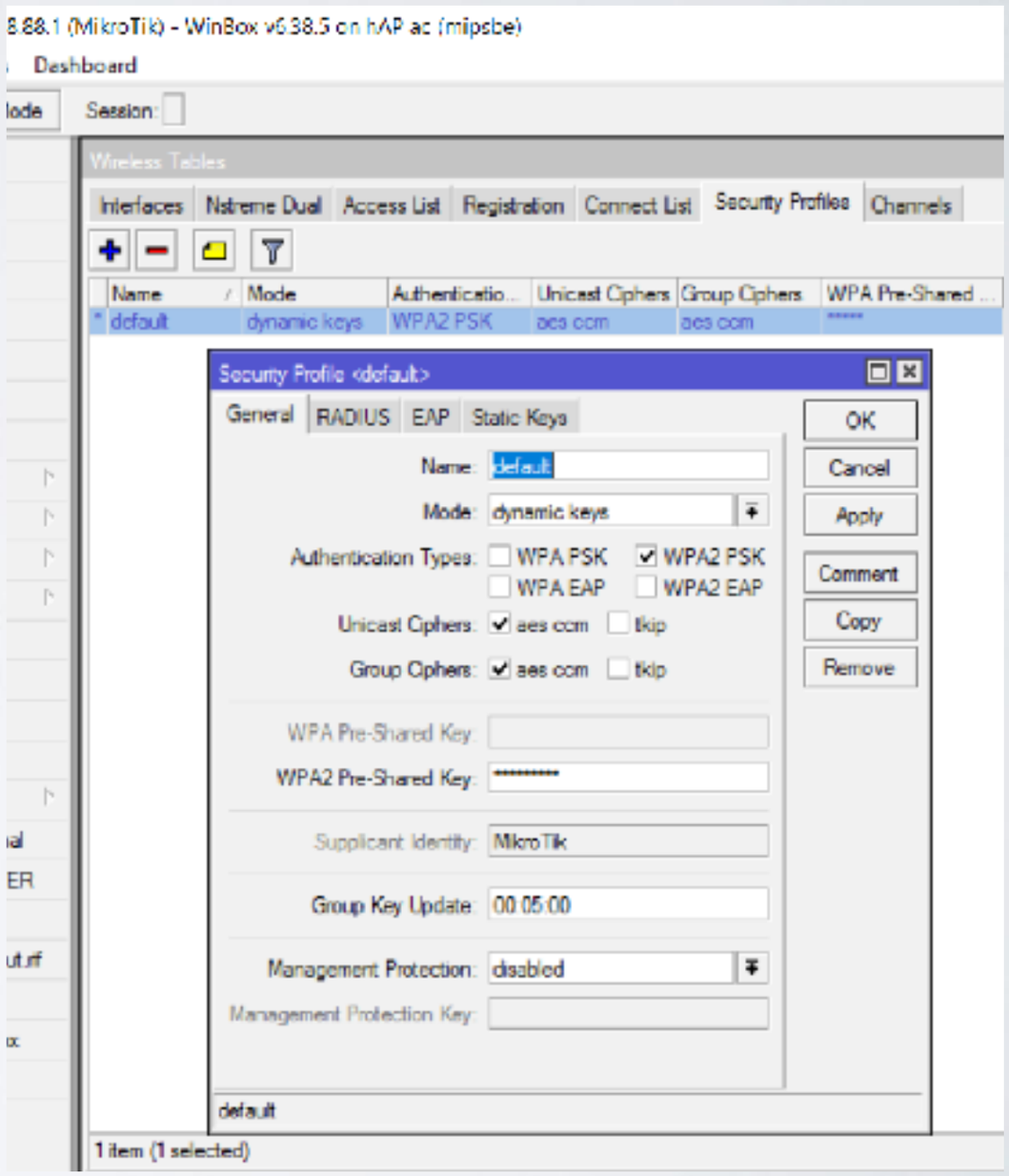
- Specify user password
  /user set admin
  password=***
- Use different username
  /user set admin
  name=martins



Simple Security

- Specify password for wireless access

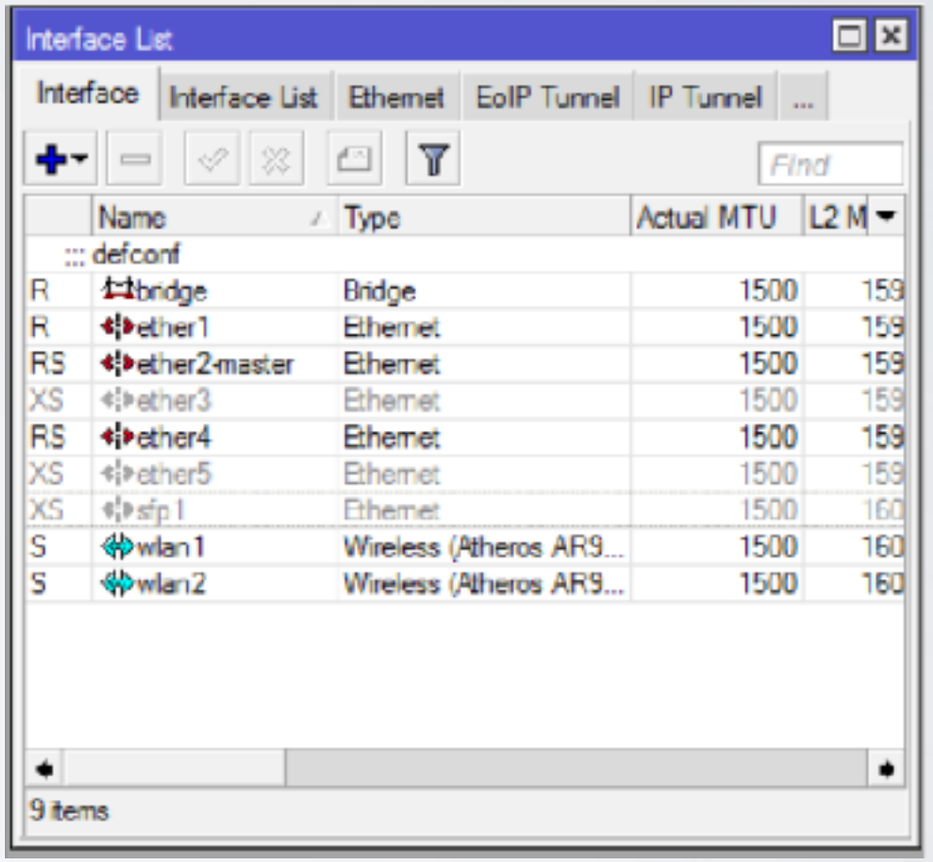
/interface wireless security-profiles set default= authentication-types=wpa2-psk mode=dynamic-keys wpa2-pre-shared-key=********



Security

- Disable unused interfaces

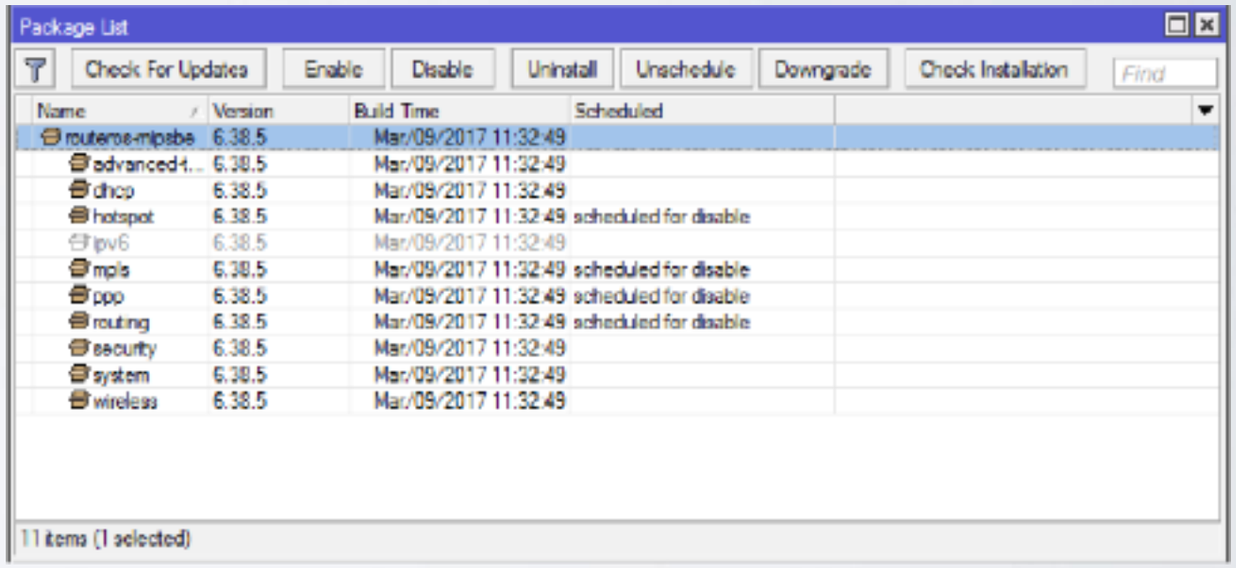
  /interface ethernet disable ether3,ether5,sfp1



Security

- Disable unused packages (mainly IPv6)

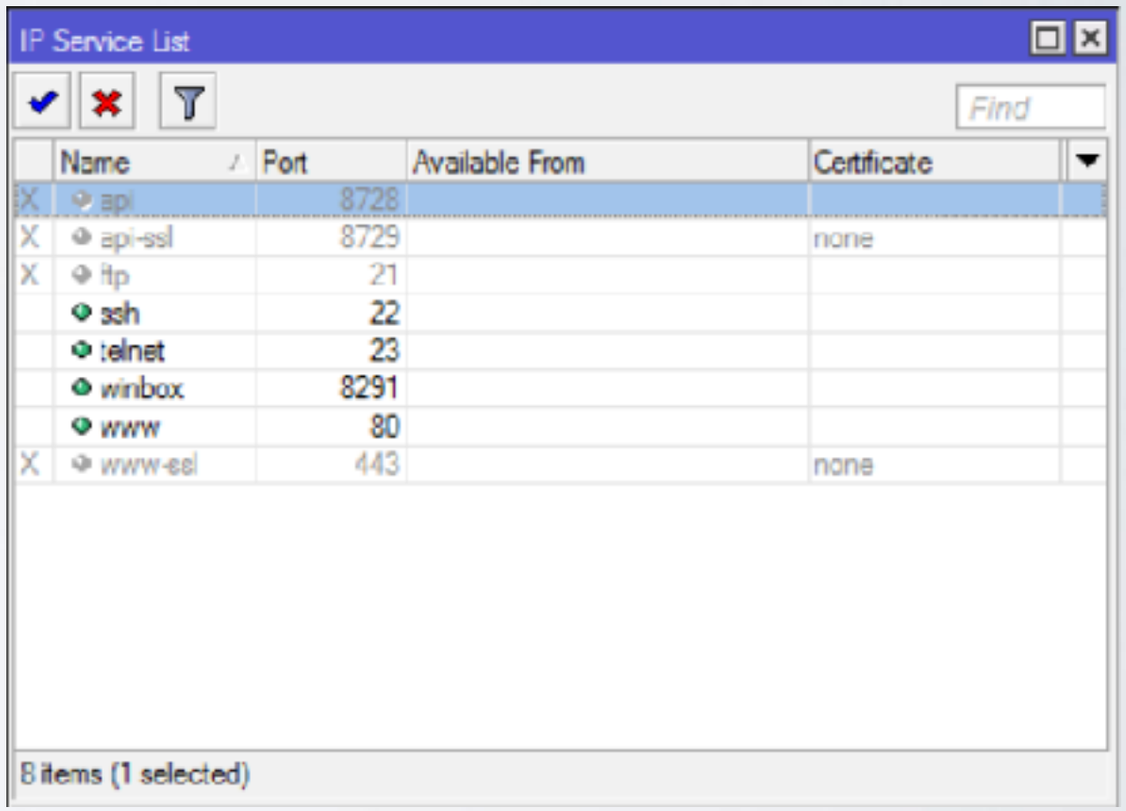
/system package disable hotspot, ipv6, mpls, ppp, routing



Security

- Disable IP/Services

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



Security

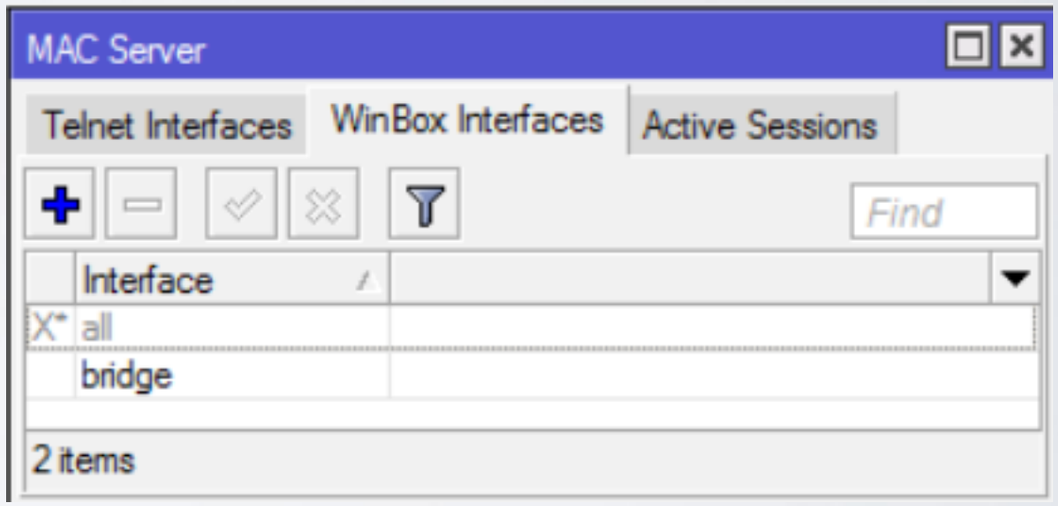
- Adjust MAC access

  /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

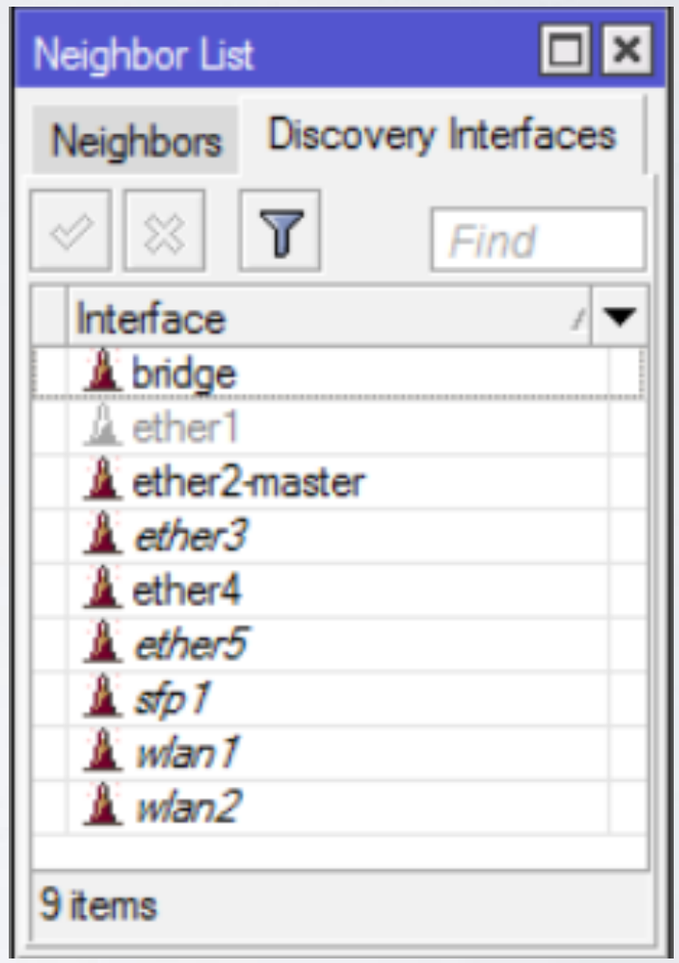
  /tool mac-server mac-winbox add interface=bridge



Security

- Hide device in Neighbor Discovery

/ip neighbor discovery set ether1 discover=no



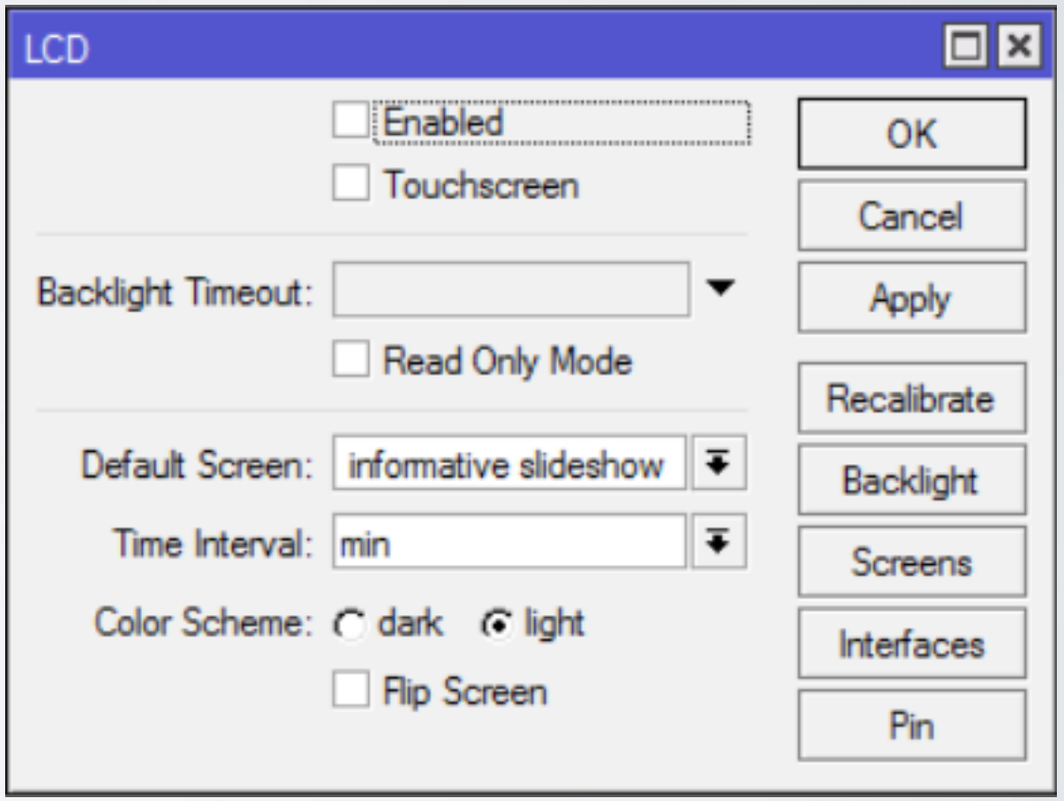
Security

- 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)

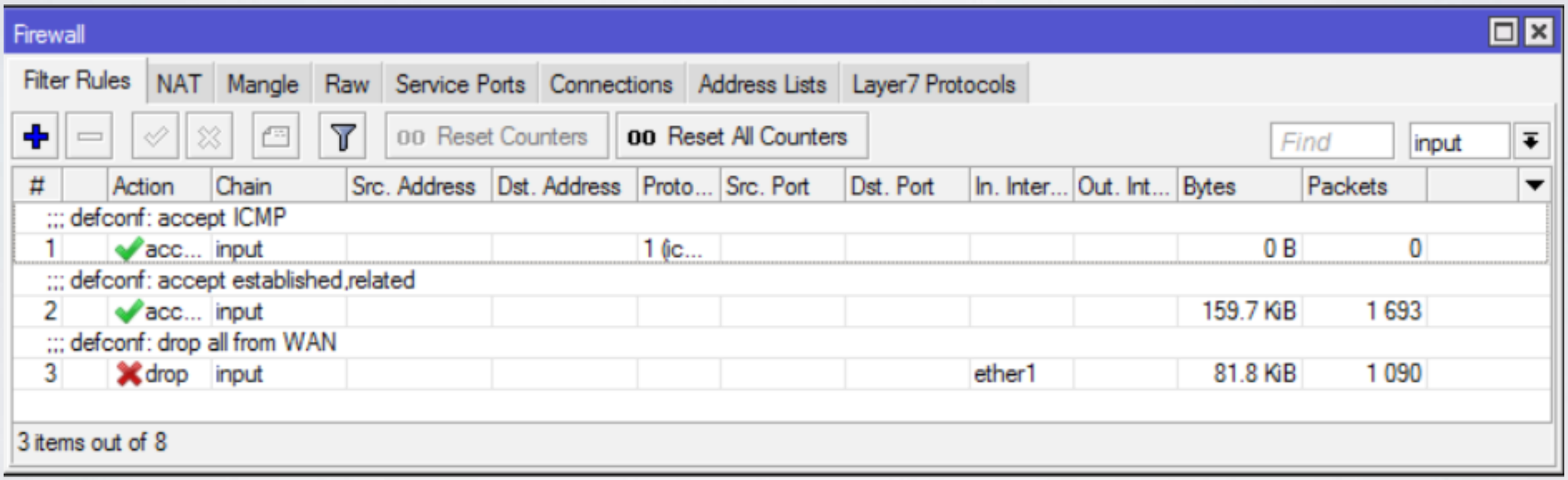
  /ip firewall filter

  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

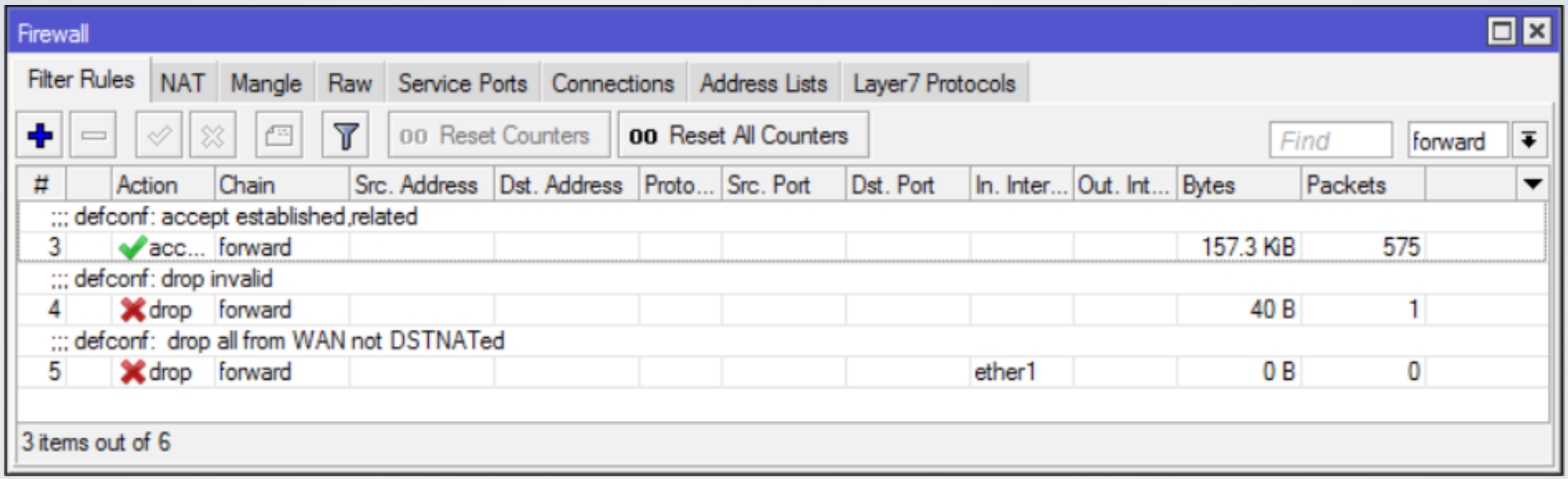

Firewall
Filter Rules
NAT
Mangle
Raw
Service Ports
Connections
Address Lists
Layer7 Protocols
Reset Counters
Reset All Counters
Find
input
Action Chain Src. Address Dst. Address Proto... Src. Port Dst. Port In. Inter... Out. Int... Bytes Packets
;;; defconf: accept ICMP
1 acc... input 1 (ic... 0 B 0
;;; 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

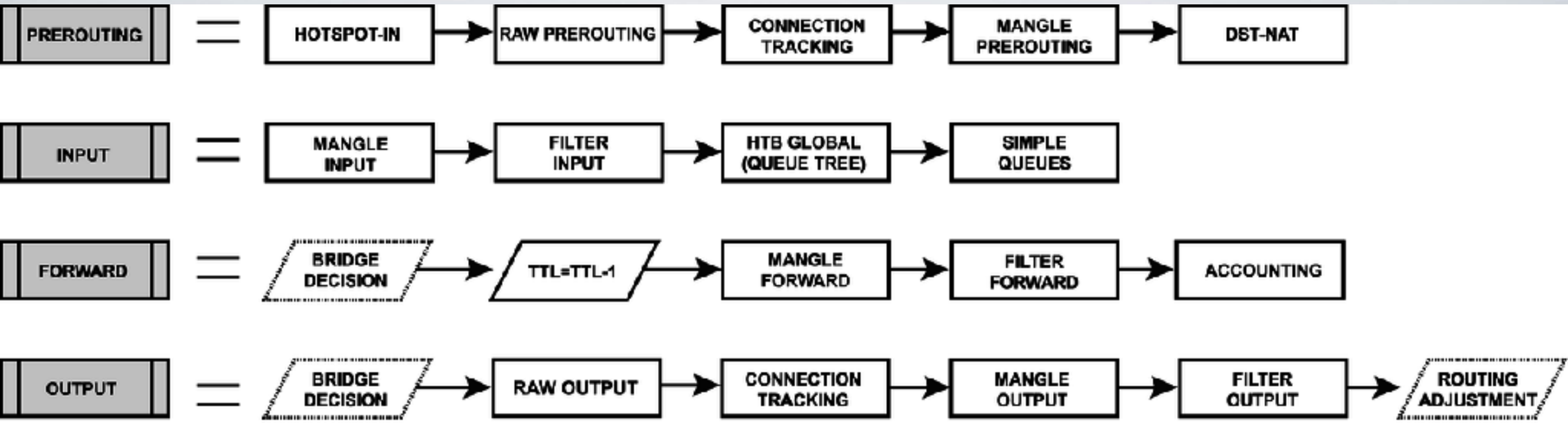

Firewall
Filter Rules
NAT
Mangle
Raw
Service Ports
Connections
Address Lists
Layer7 Protocols
00 Reset Counters
00 Reset All Counters
Find
forward
| Action | Chain | Src. Address | Dst. Address | Proto... | Src. Port | Dst. Port | In. Inter... | Out. Int... | Bytes | Packets
;;; defconf: accept established,related
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

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

oo Reset Counters | oo Reset All Counters | Find | all

#		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

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

Find | all

	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

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

00 Reset Counters | 00 Reset All Counters | Find | forward

#		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

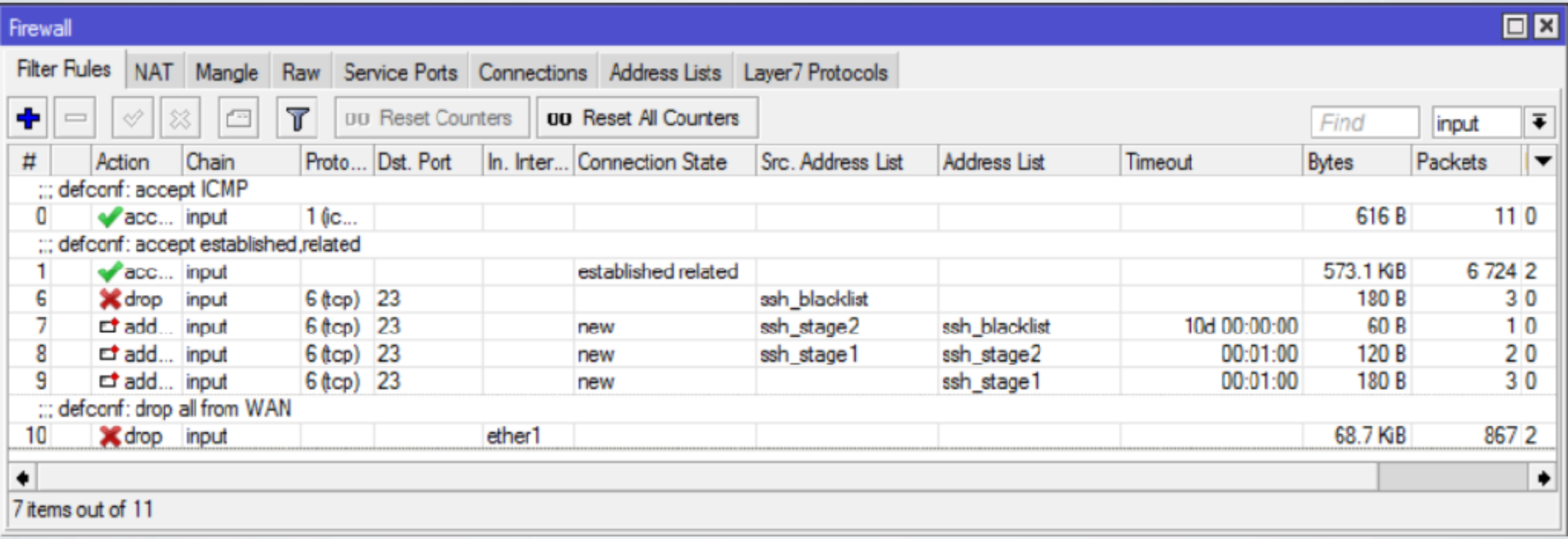
  /ip firewall filter
  add chain=input protocol=tcp dst-port=22 src-address-list=ssh_blacklist action=drop

  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


Firewall
Filter Rules
NAT
Mangle
Raw
Service Ports
Connections
Address Lists
Layer7 Protocols
Reset Counters
Reset All Counters
Find
input
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

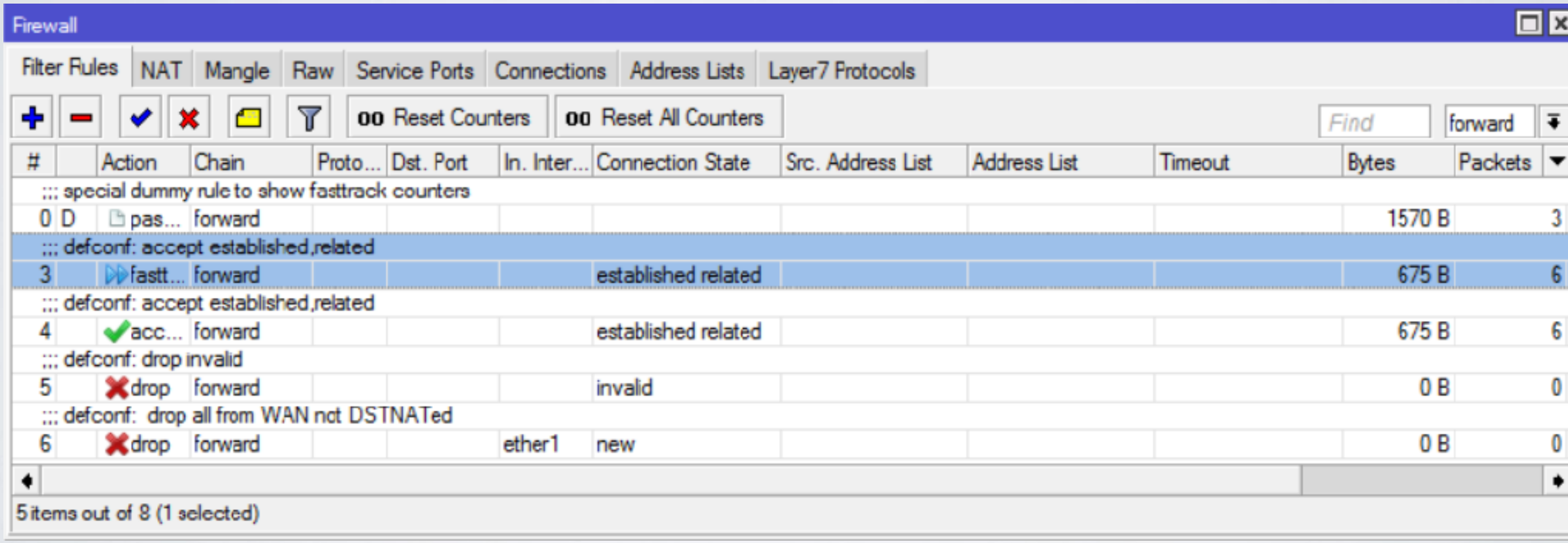
Bandwidth Control

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

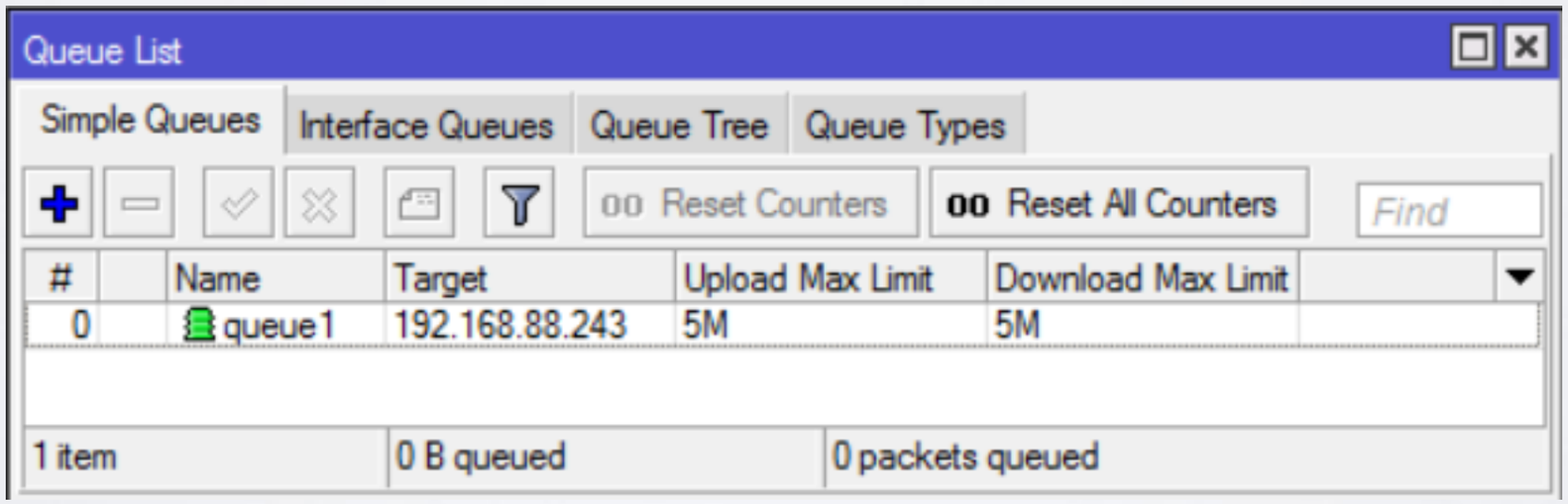
FastTrack


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

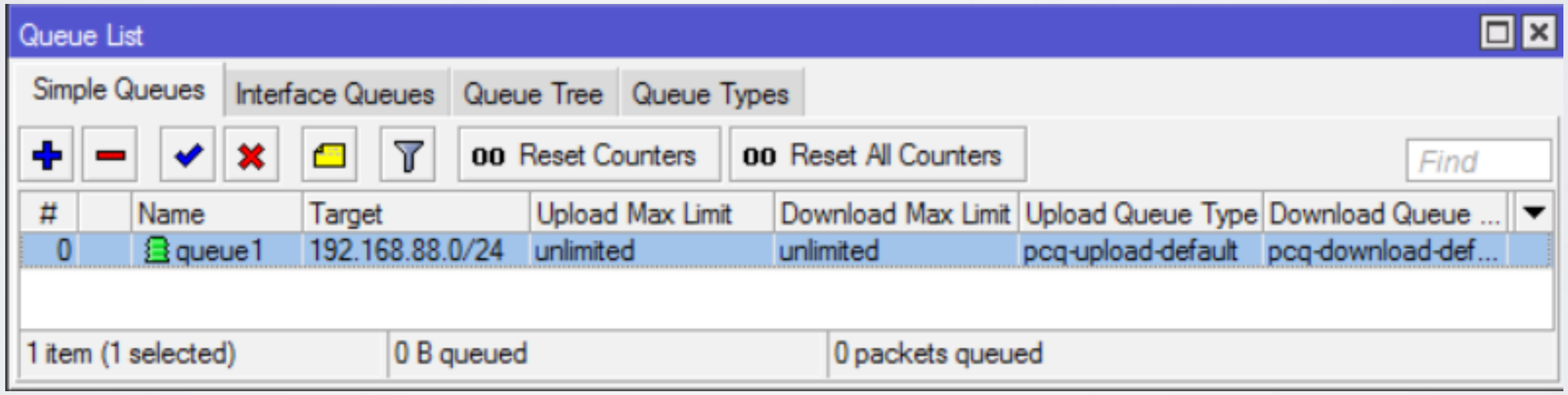
- Add queues to limit traffic for specific resources

/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



- 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

Log

Freeze

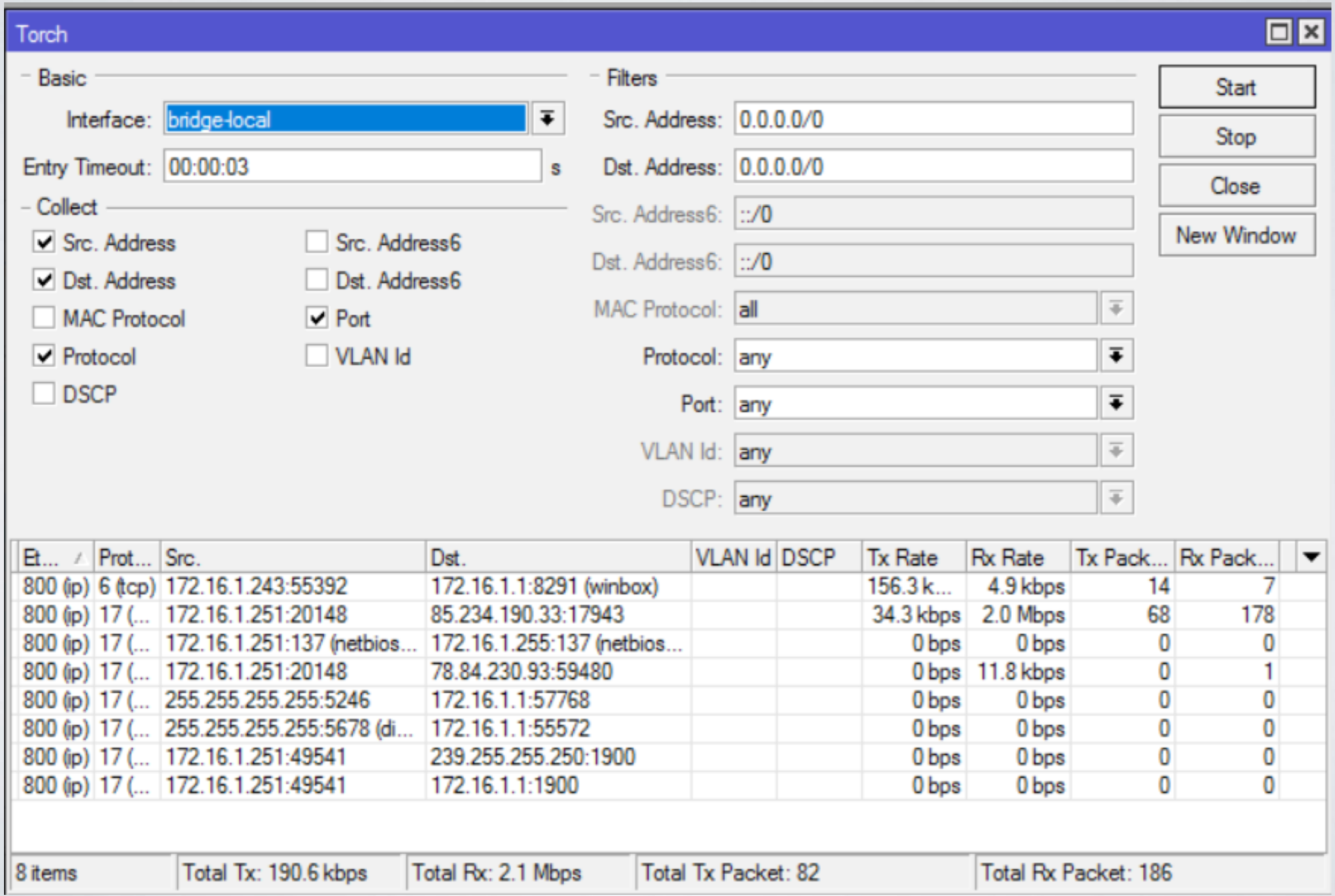
all

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

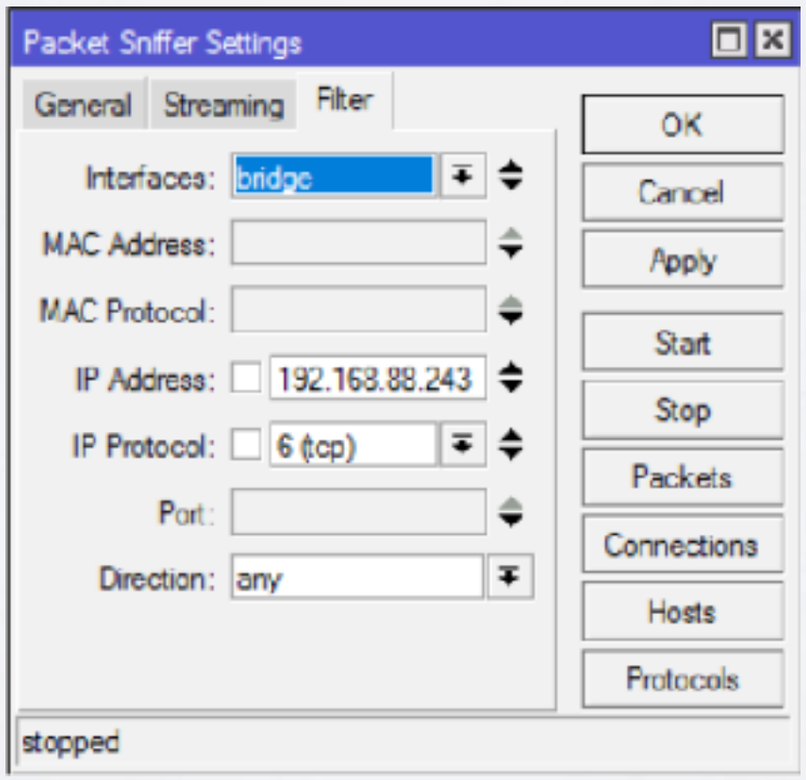
Debugging Tools



Debugging Tools

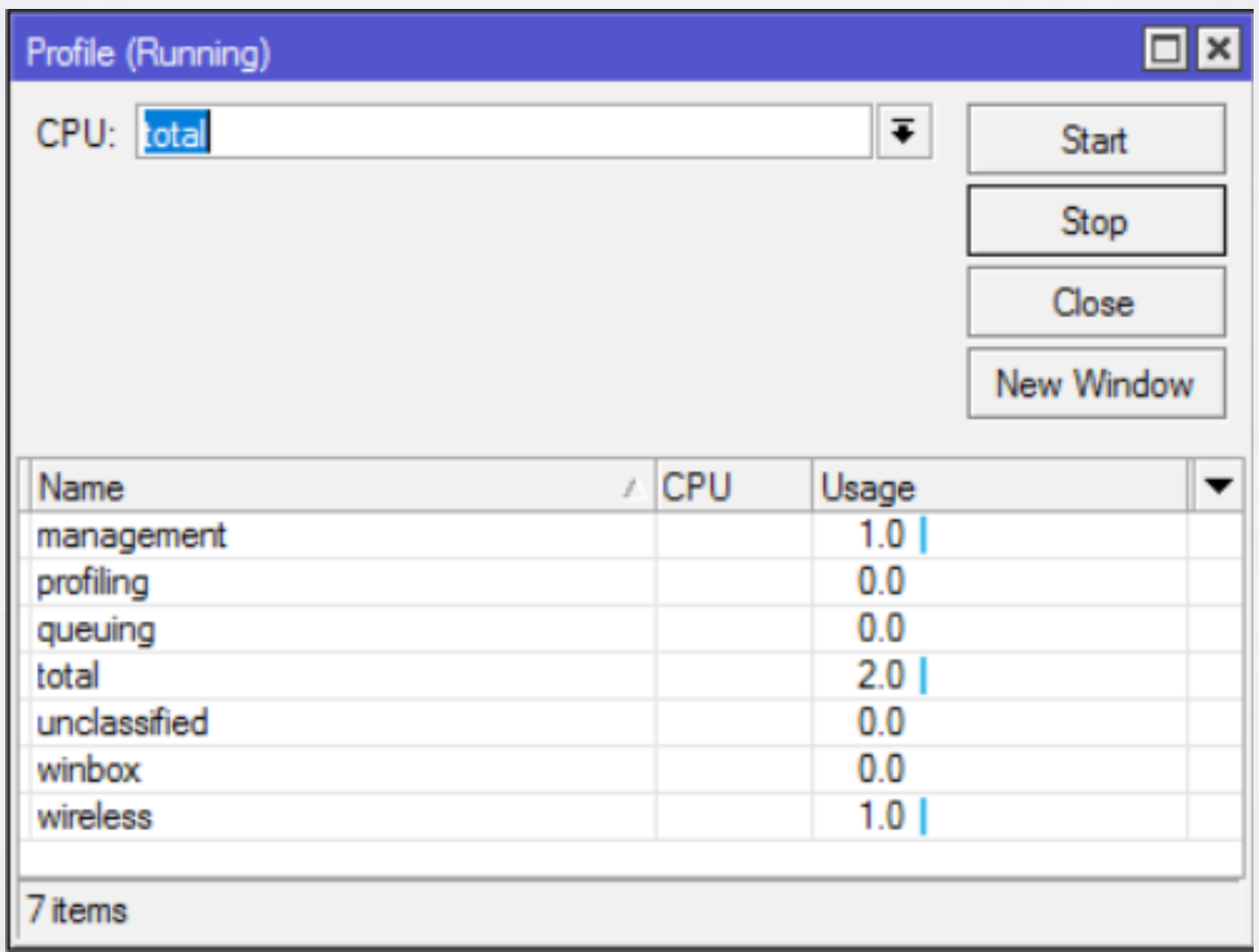
- Sniffer

- 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

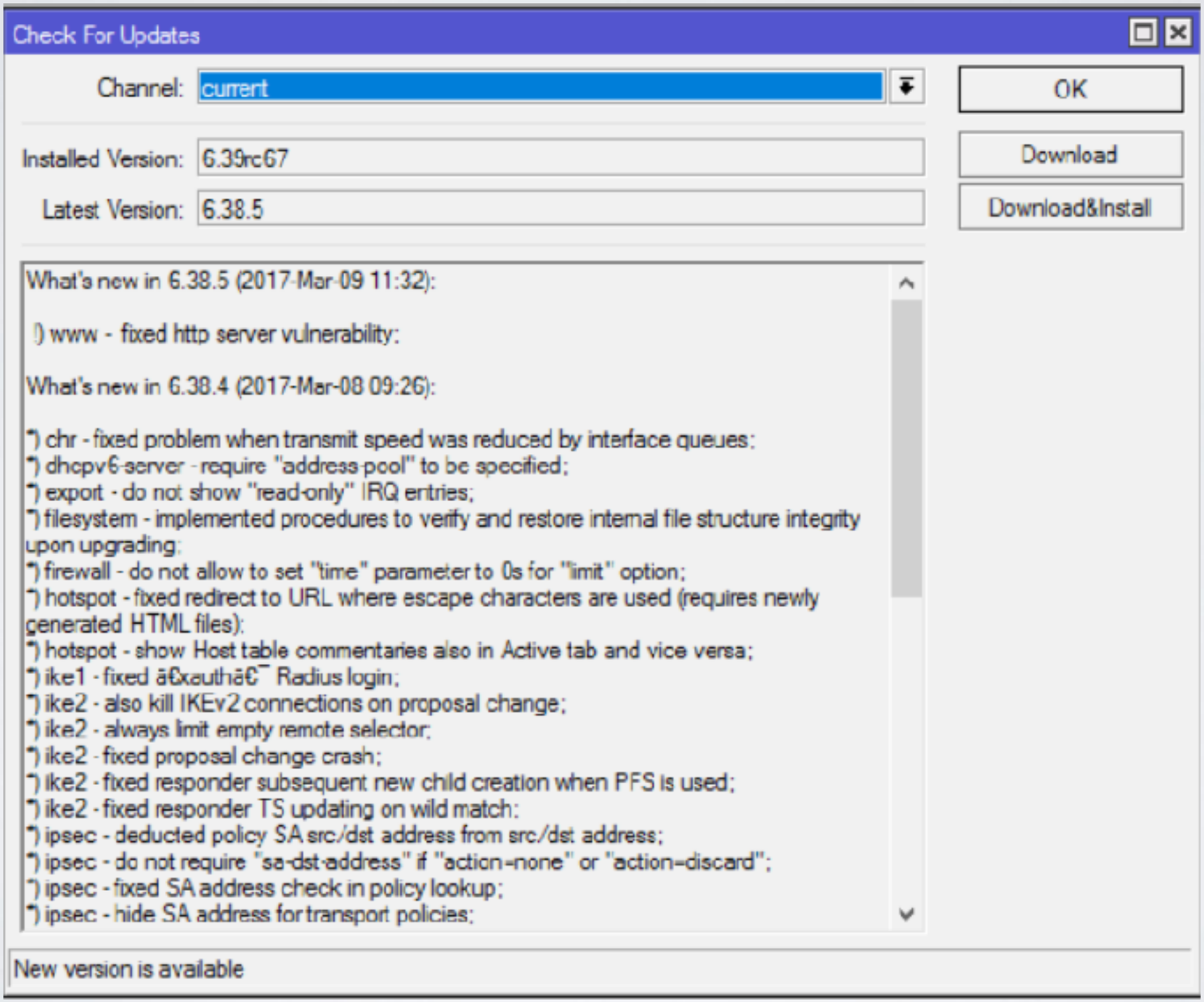
Keep everything up-to-date

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