Basic guidelines on RouterOS configuration and debugging

Martins Strods

MikroTik, Latvia

Ho Chi Minh City, Vietnam

April 2017

What is the main idea of this?

"Little things matter and are very important"

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

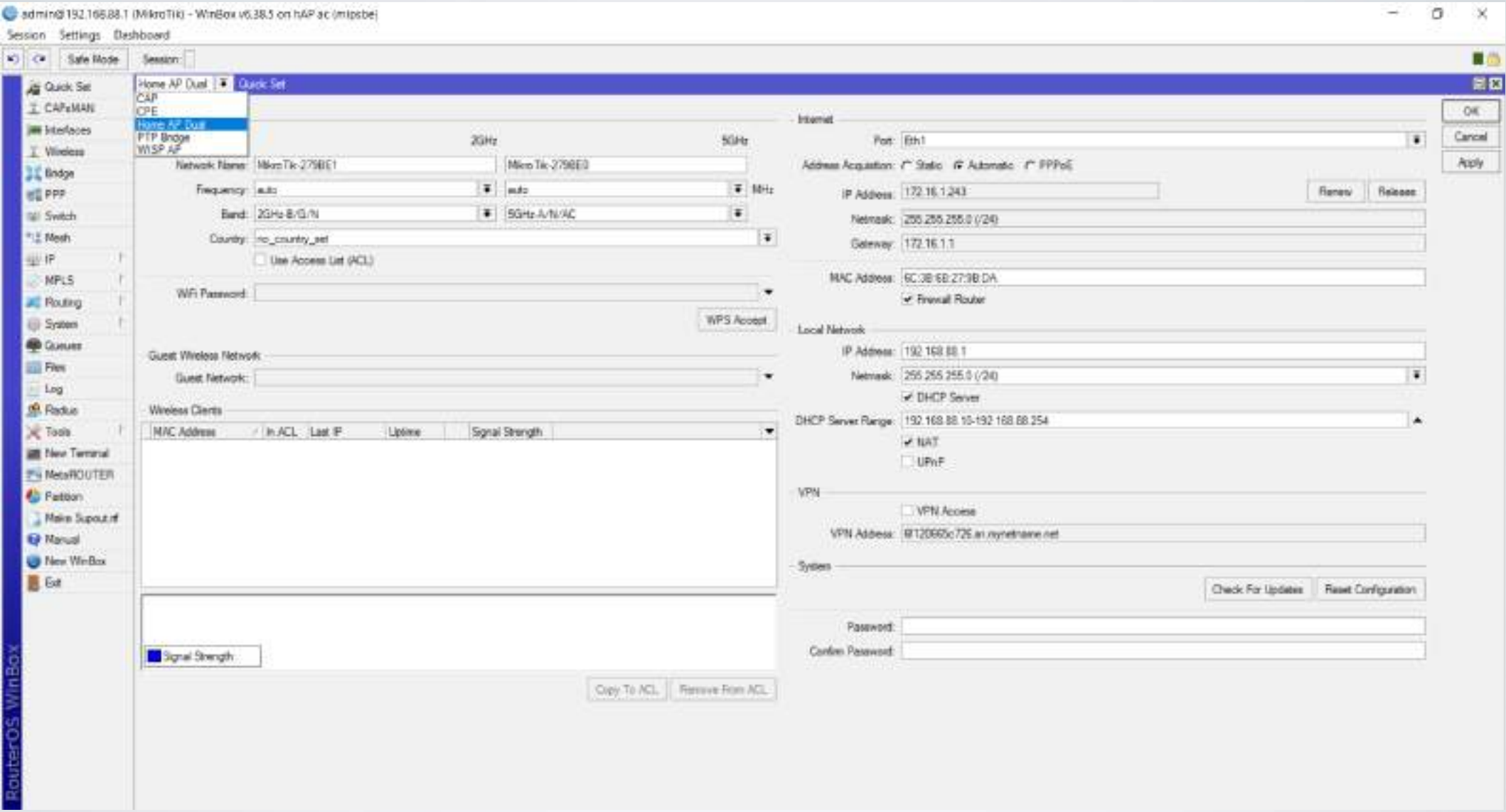
  https://forum.mikrotik.com/viewtopic.php?t=98407

- Winbox

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

The fastest way how to configure device

QuickSet


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-279BE1
MikroTik-279BE0
Frequency:
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:27:9B: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:
System
Check For Updates
Reset Configuration
Password:
Confirm Password:
OK
Cancel
Apply

QuickSet

- Easy to use
- Contains the most commonly used features and should be enough for basic usage

Golden rule about QuickSet:

“If you use QuickSet, then use QuickSet, if you leave it, then forget about it...”

Simple security

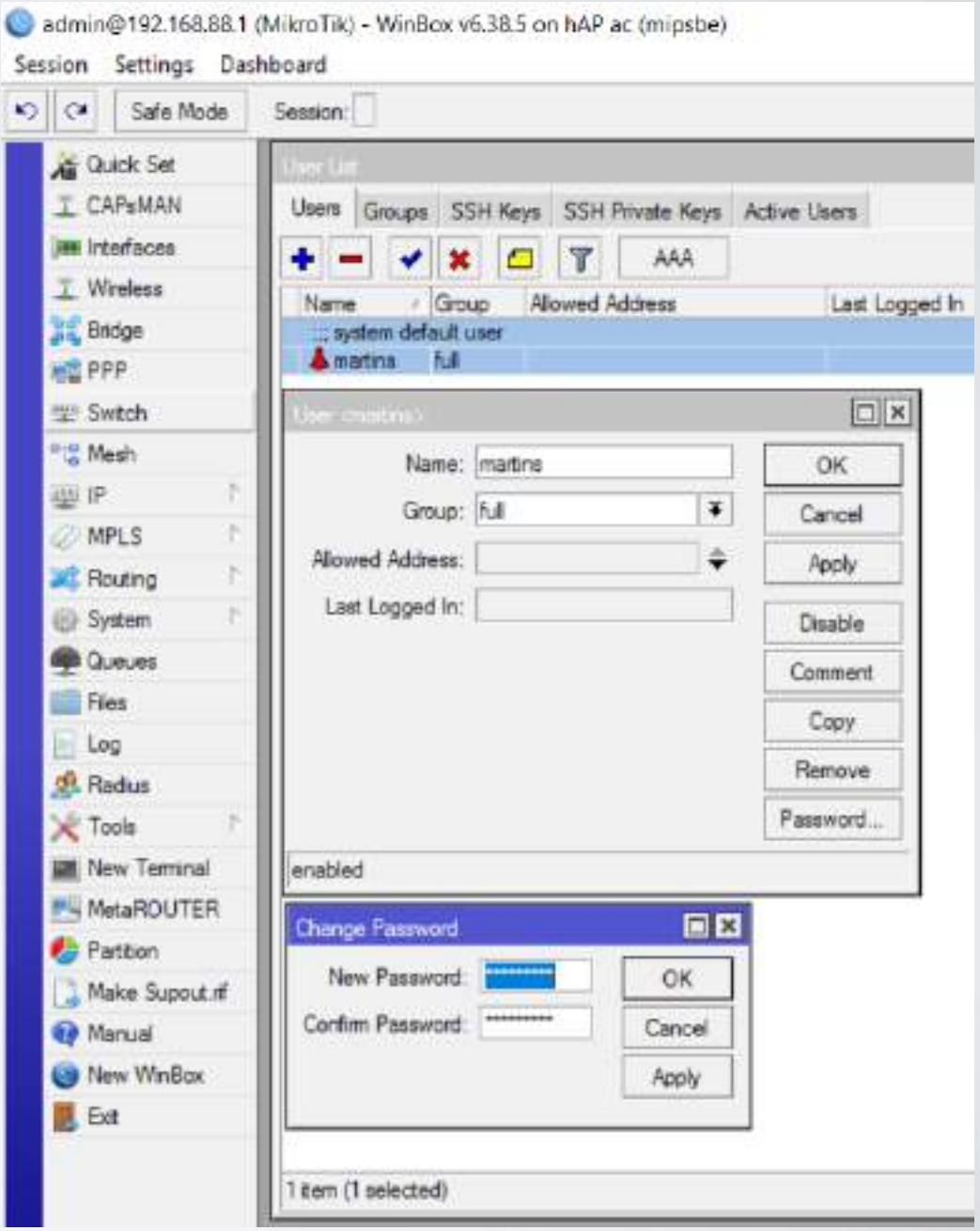
Simple security

- Specify user password

  /user set admin password=***

- Use different username

  /user set admin name=martins

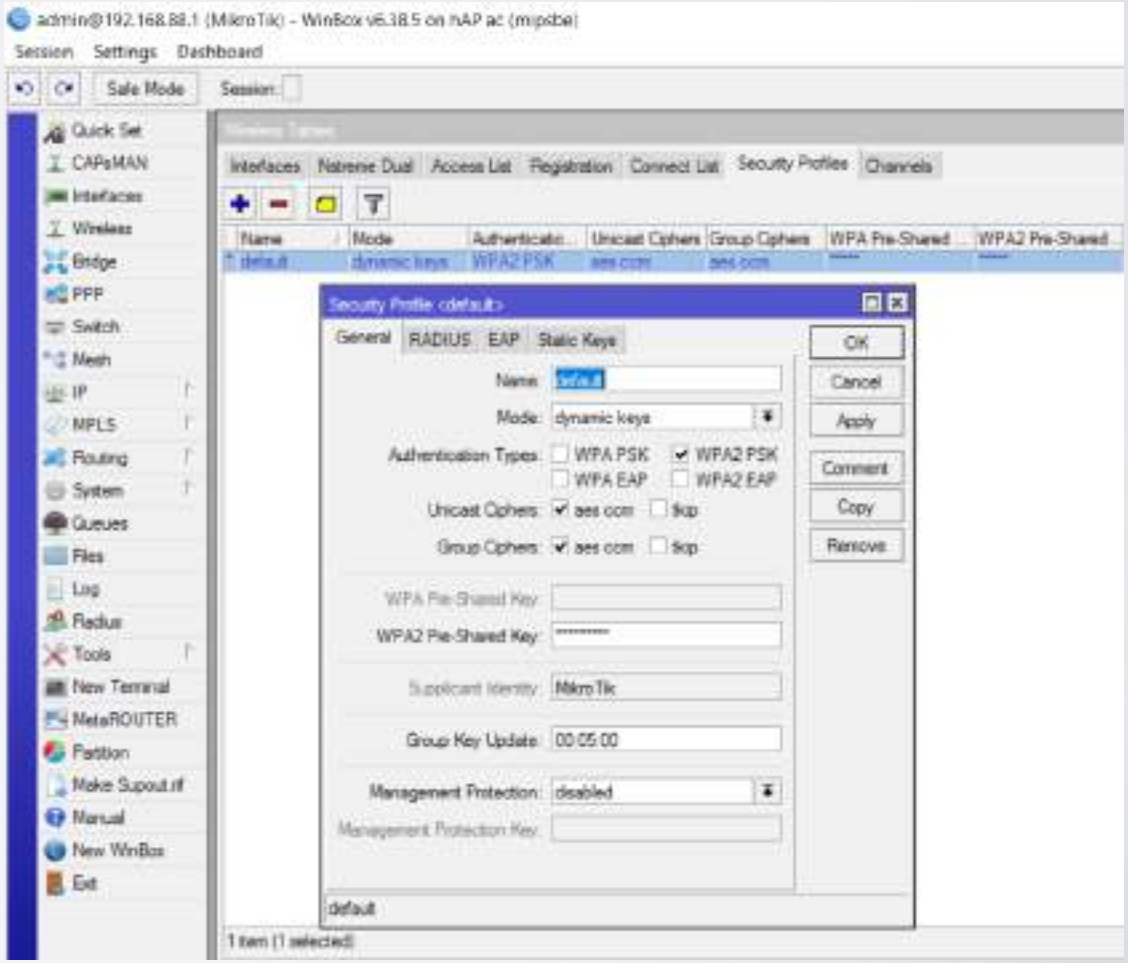


Simple security

- Specify password for wireless access

  /interface wireless security-profiles set default authentication-types=wpa2-psk

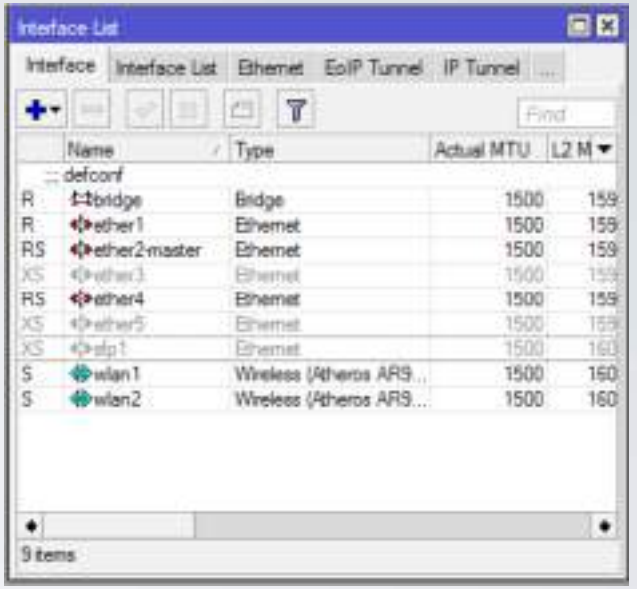
  mode=dynamic-keys wpa2-pre-shared-key=********



Simple security

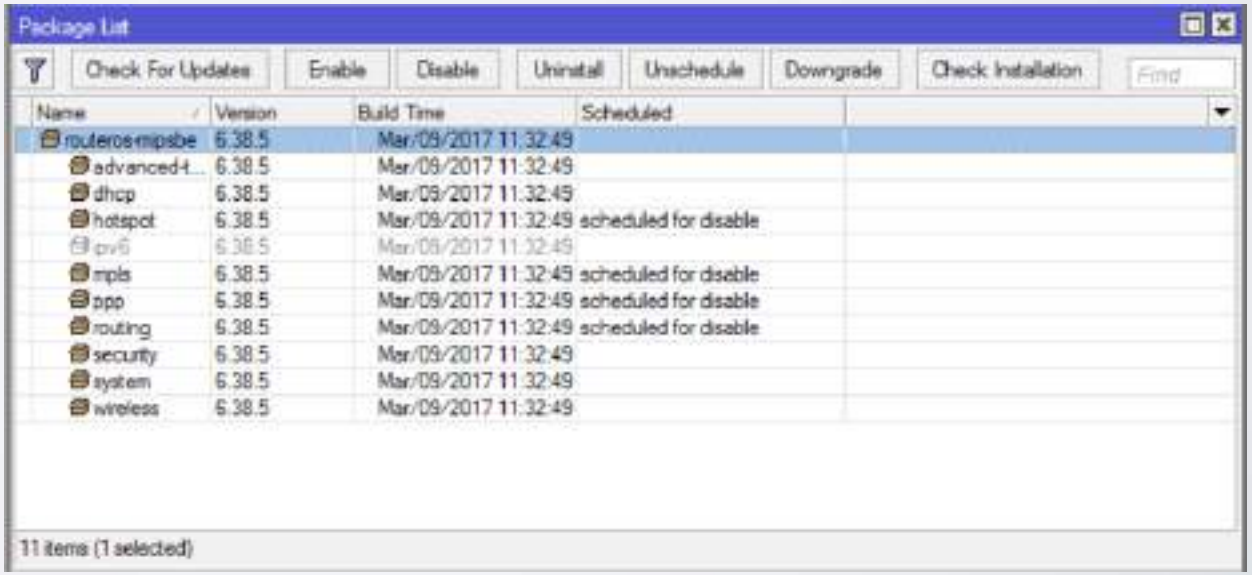
- Disable unused interfaces

  /interface ethernet disable ether3,ether5,sfp1



- Disable unused packages (mainly IPv6)

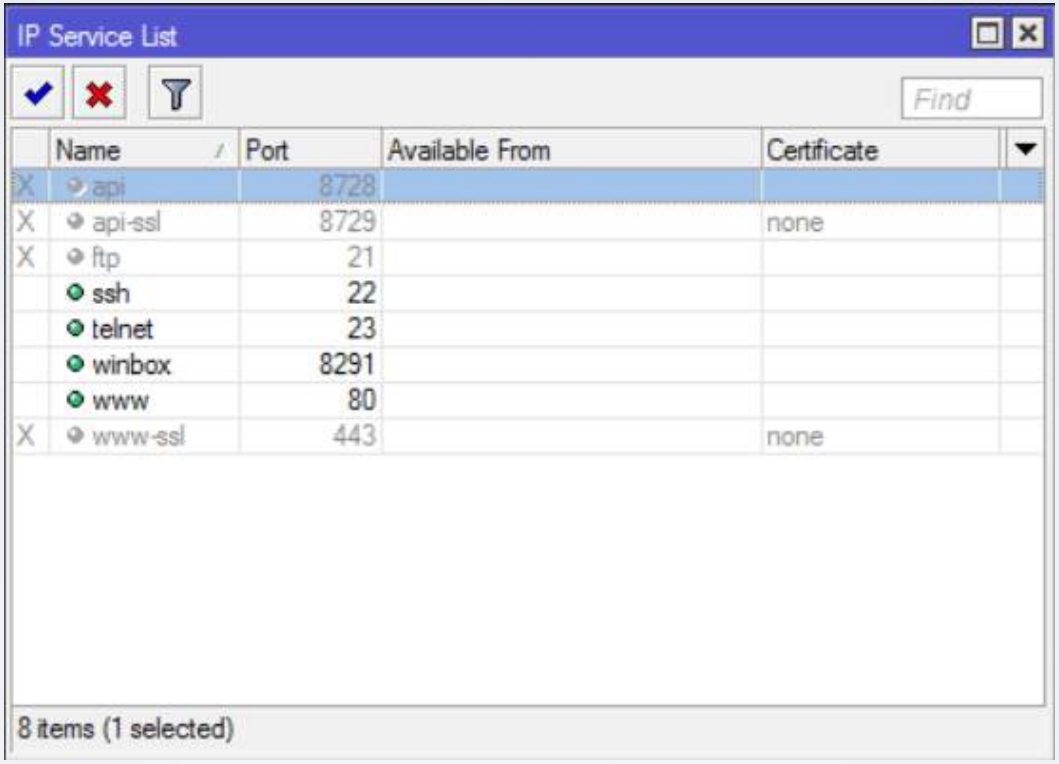
  /system package disable hotspot,ipv6,mpls,ppp,routing



Simple security

- Disable IP/Services

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



Simple security

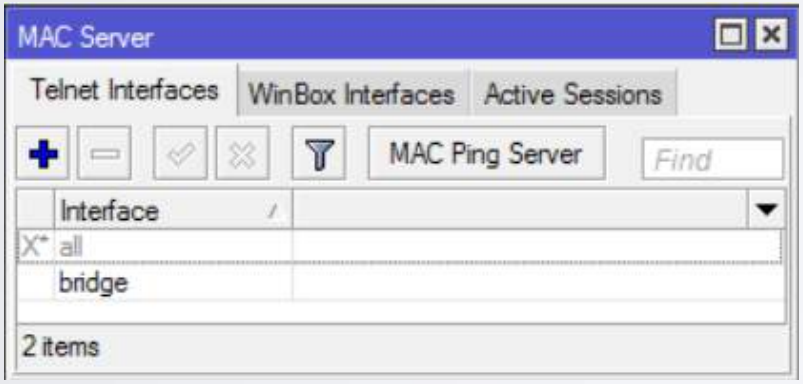
- Adjust MAC access

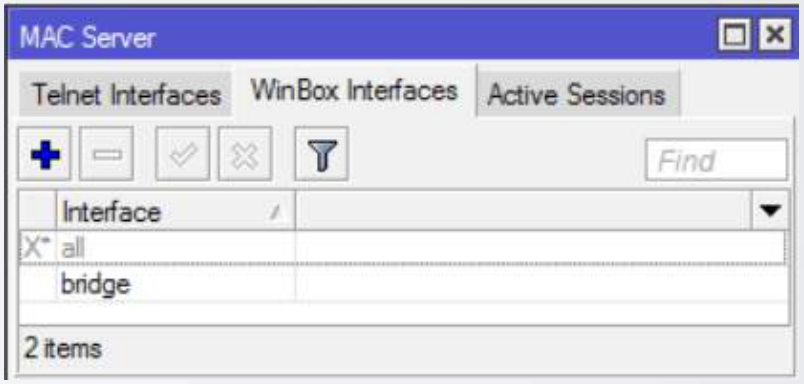
/tool mac-server set [find default=yes] disabled=yes

/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

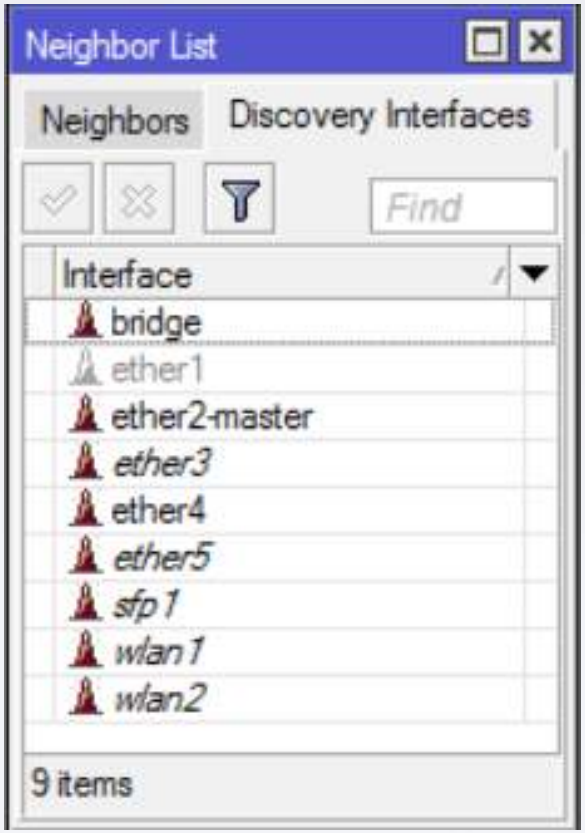




Simple security

- Hide device in Neighbor Discovery

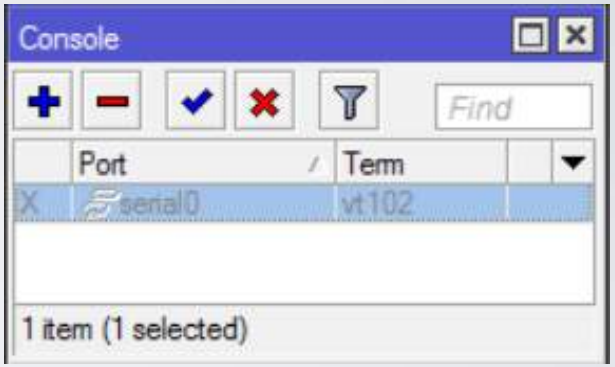
  /ip neighbor discovery set ether1 discover=no



Simple security

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

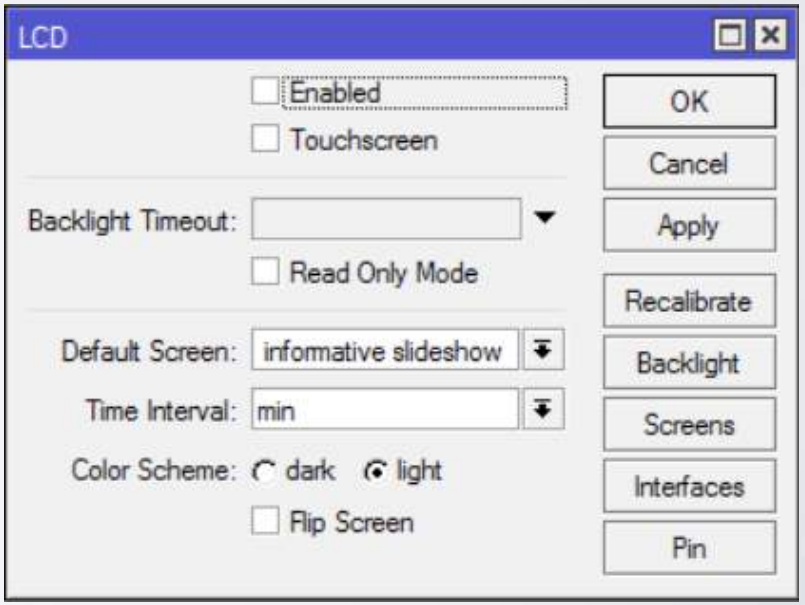
  /system console disable [find where port=serial0]



- 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

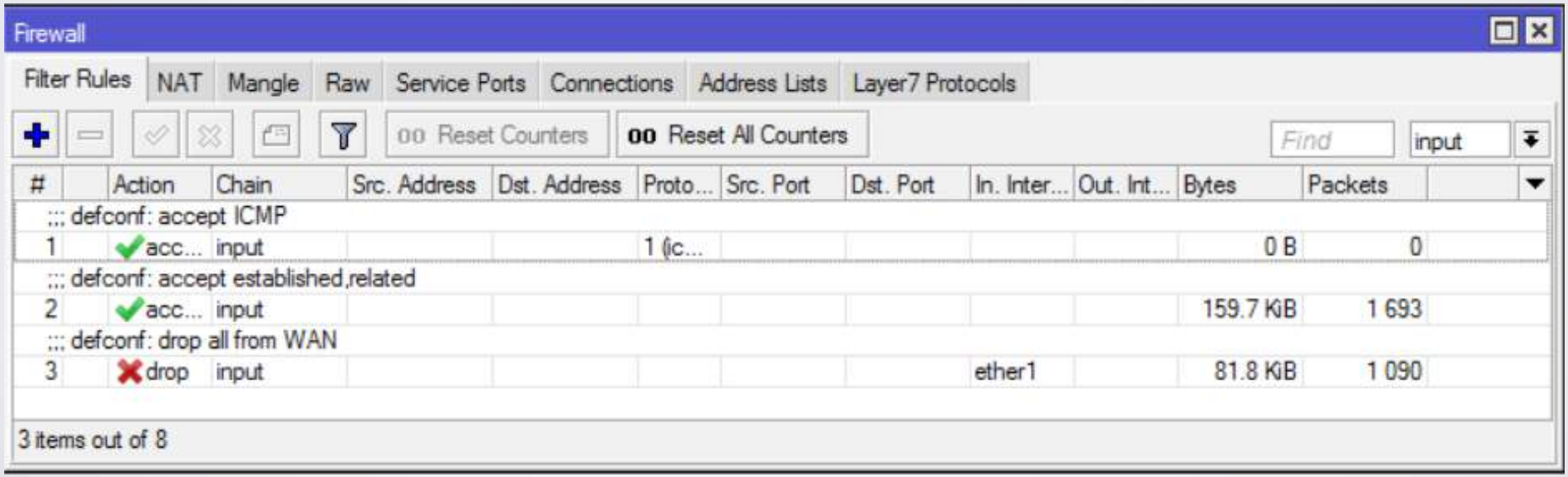
- Secure input

  /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



Firewall

- Secure forward

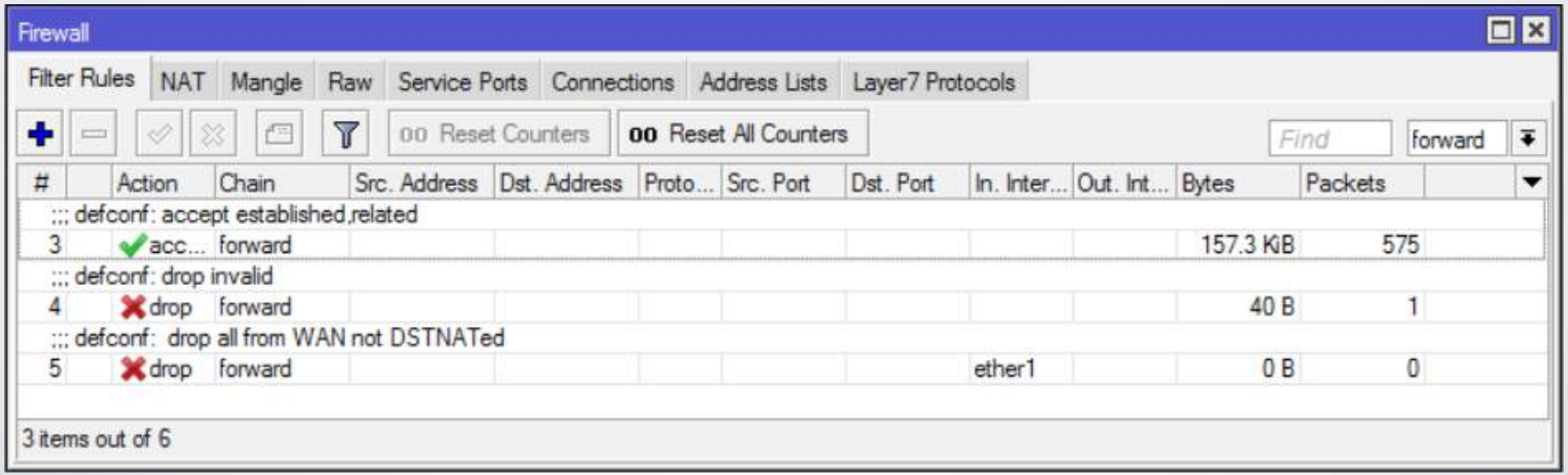
  /ip firewall filter

  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=!

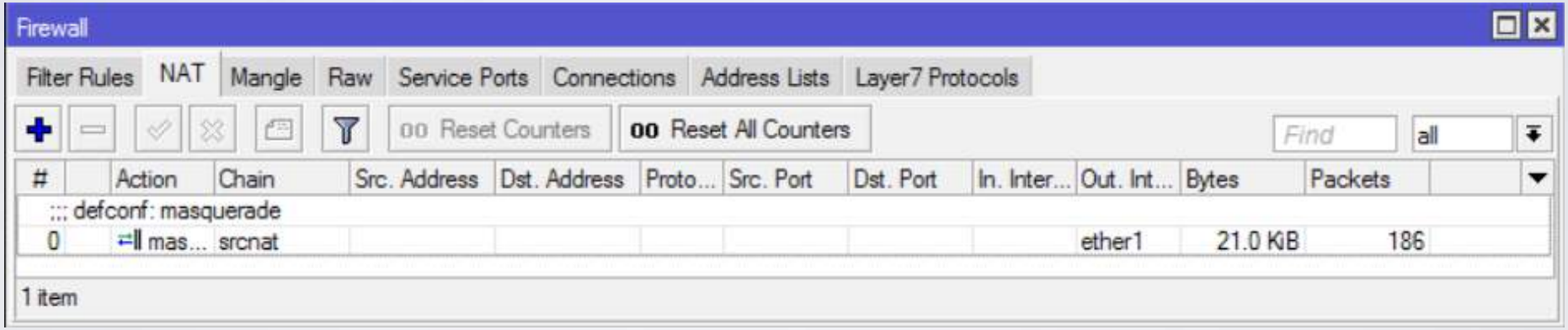
  dstnat in-interface=ether1



Firewall

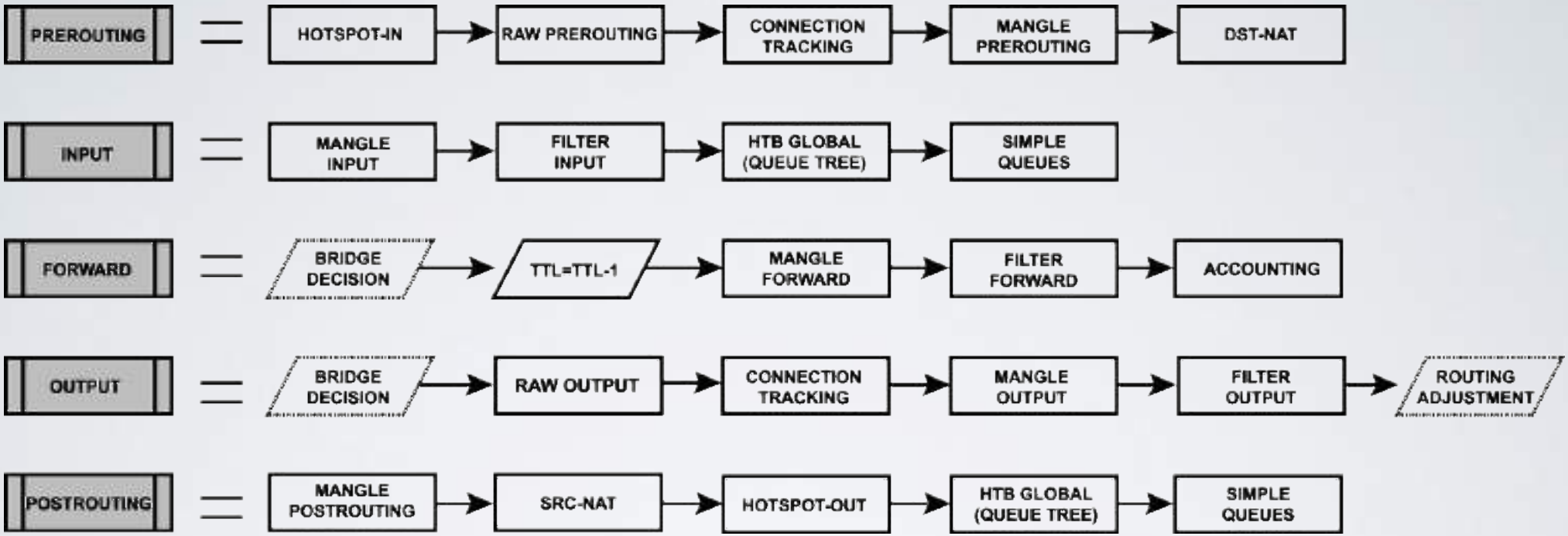
- NAT to outside (if you can, use src-nat instead of masquerade)

  /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

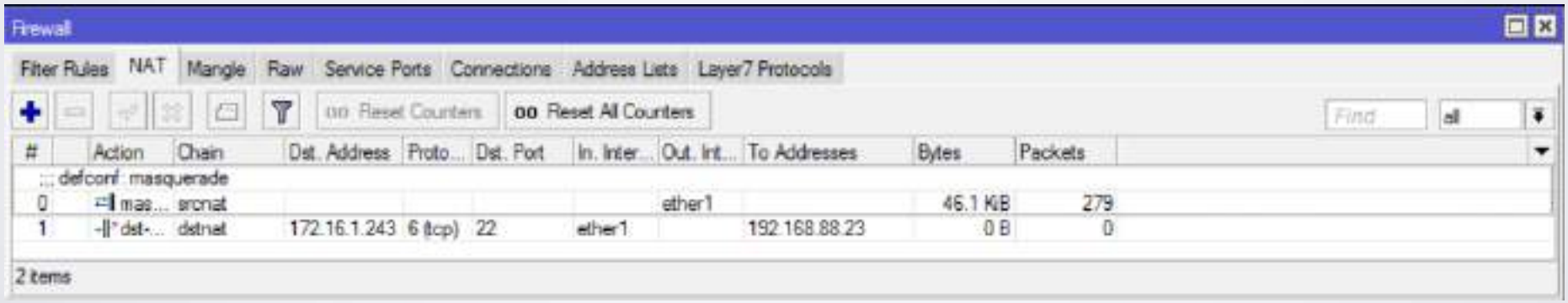
/ip firewall nat add chain=dstnat in-interface=ether1 protocol=tcp dst-port=22 action=dst-nat dst-address=172.16.1.243 to-address=192.168.88.23

Note: In order to make port forwarding work you have to:

Have dst-nat

Have src-nat

Accept traffic in forward chain (example in previous slides)



Firewall

- Hairpin NAT (access local resource through public IP)

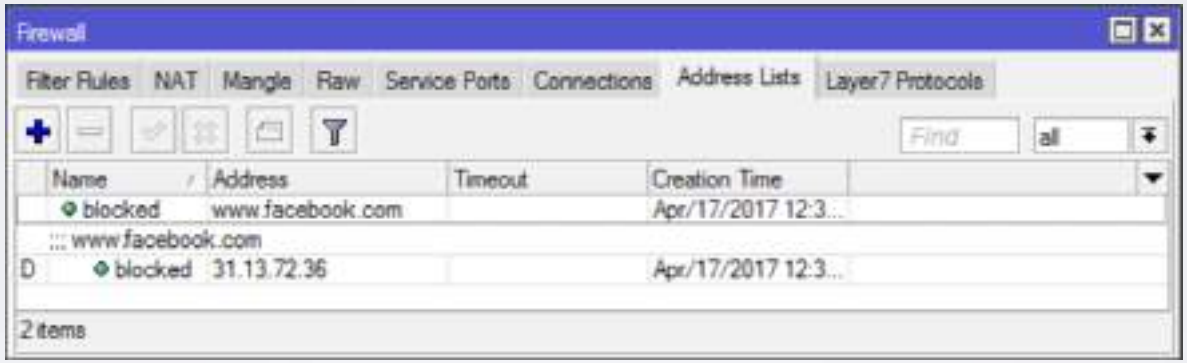
  https://wiki.mikrotik.com/wiki/Hairpin_NAT

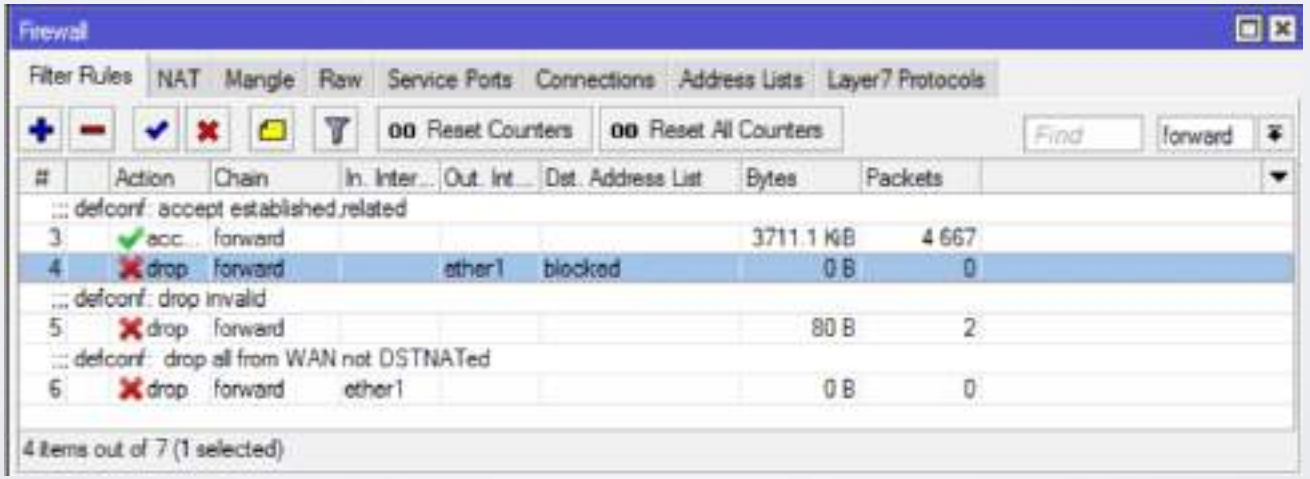
Firewall

- 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

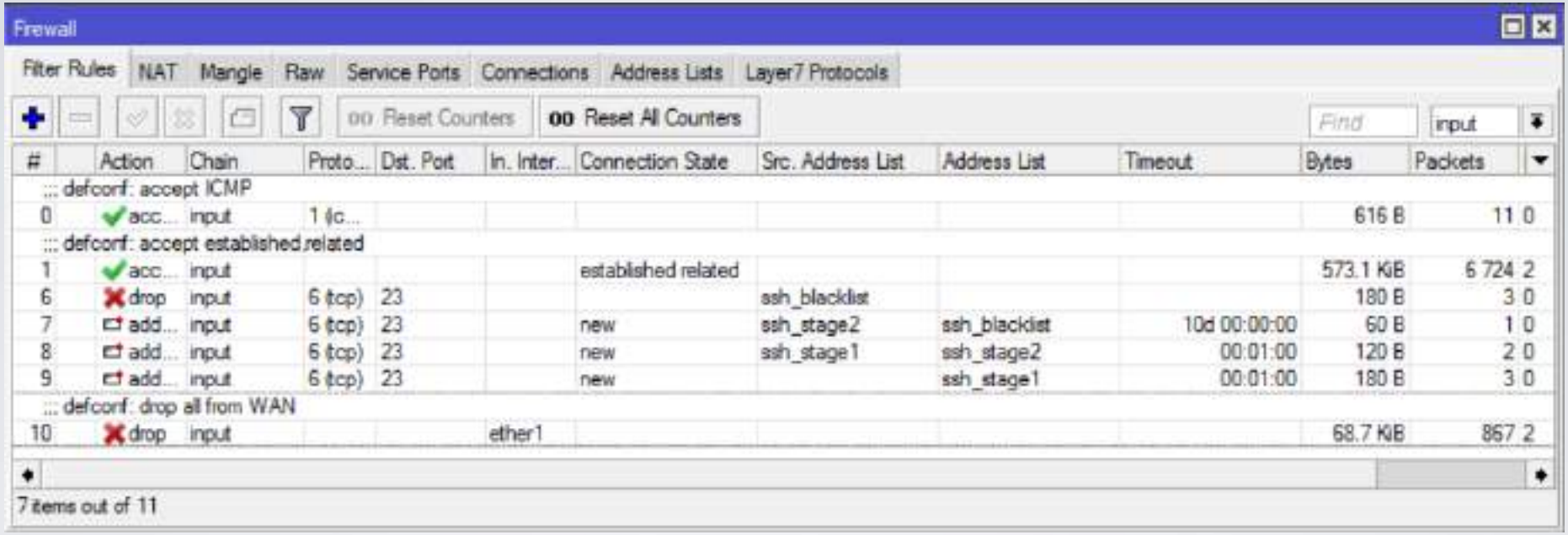
add chain=input protocol=tcp dst-port=23 src-address-list=ssh_blacklist action=drop

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



https://wiki.mikrotik.com/wiki/Bruteforce_login_prevention

Handle bandwidth

FastTrack

- Remember this rule?

  /ip firewall filter

  add chain=forward action=accept connection-state=established,related

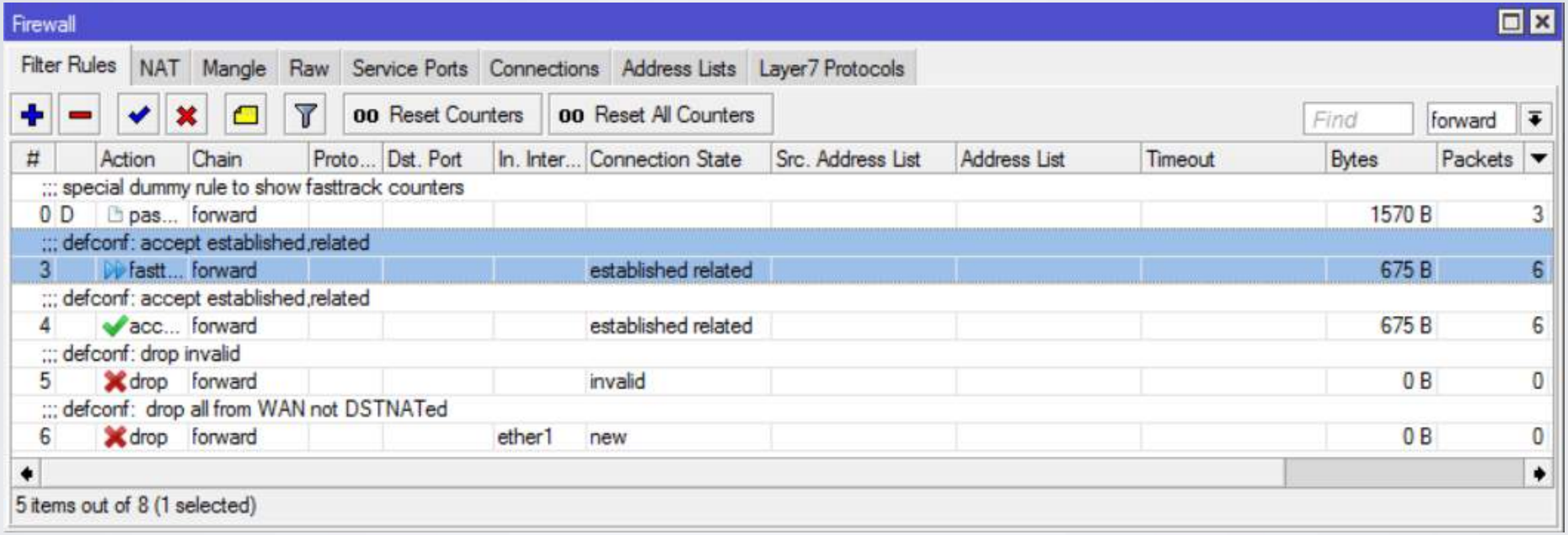
- Add FastTrack rule before previous one

  /ip firewall filter

- add chain=forward action=fasttrack-connection connection-

  state=established,related

FastTrack

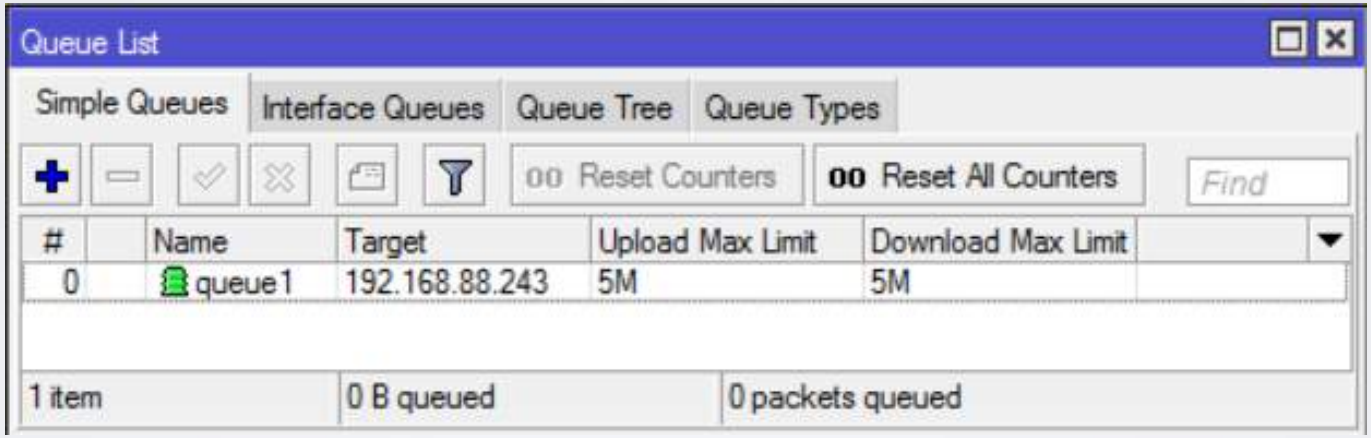


https://wiki.mikrotik.com/index.php?title=Manual:IP/Fasttrack&redirect=no

Queues

- Add queues to limit traffic for specific resources

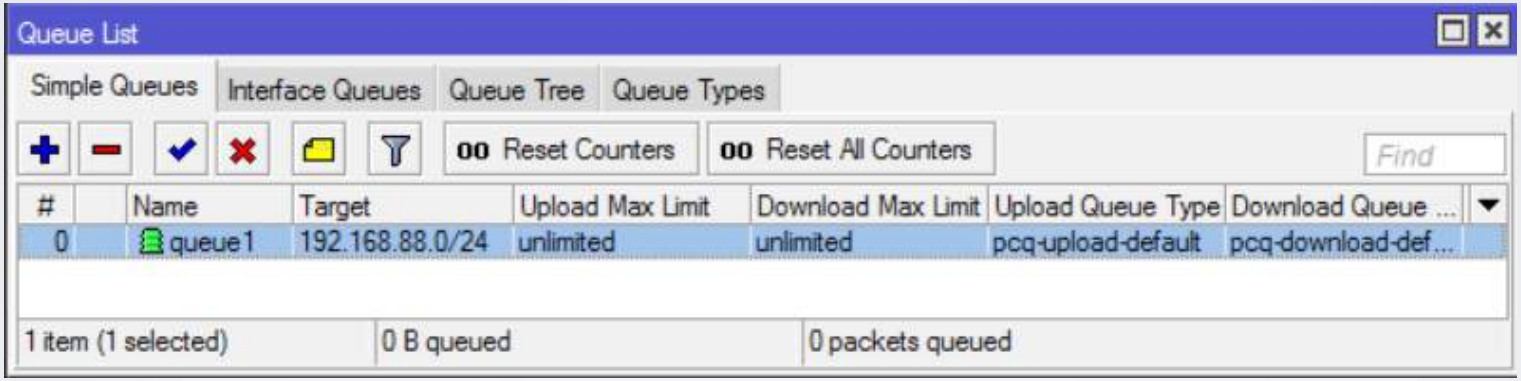
  /queue simple add name=private target=192.168.88.243 max-limit=5M/5M



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

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

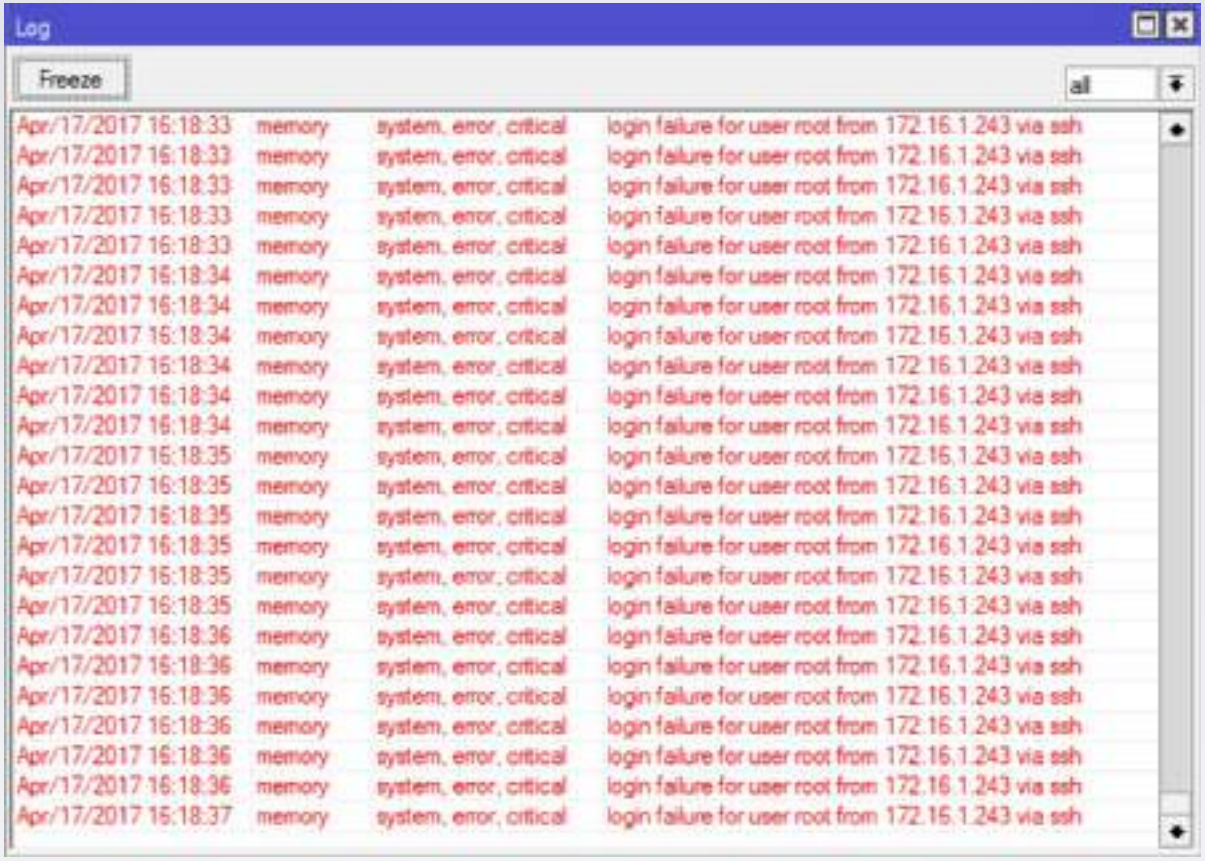
  /system logging add topics=l2pt,debug action=memory

- 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



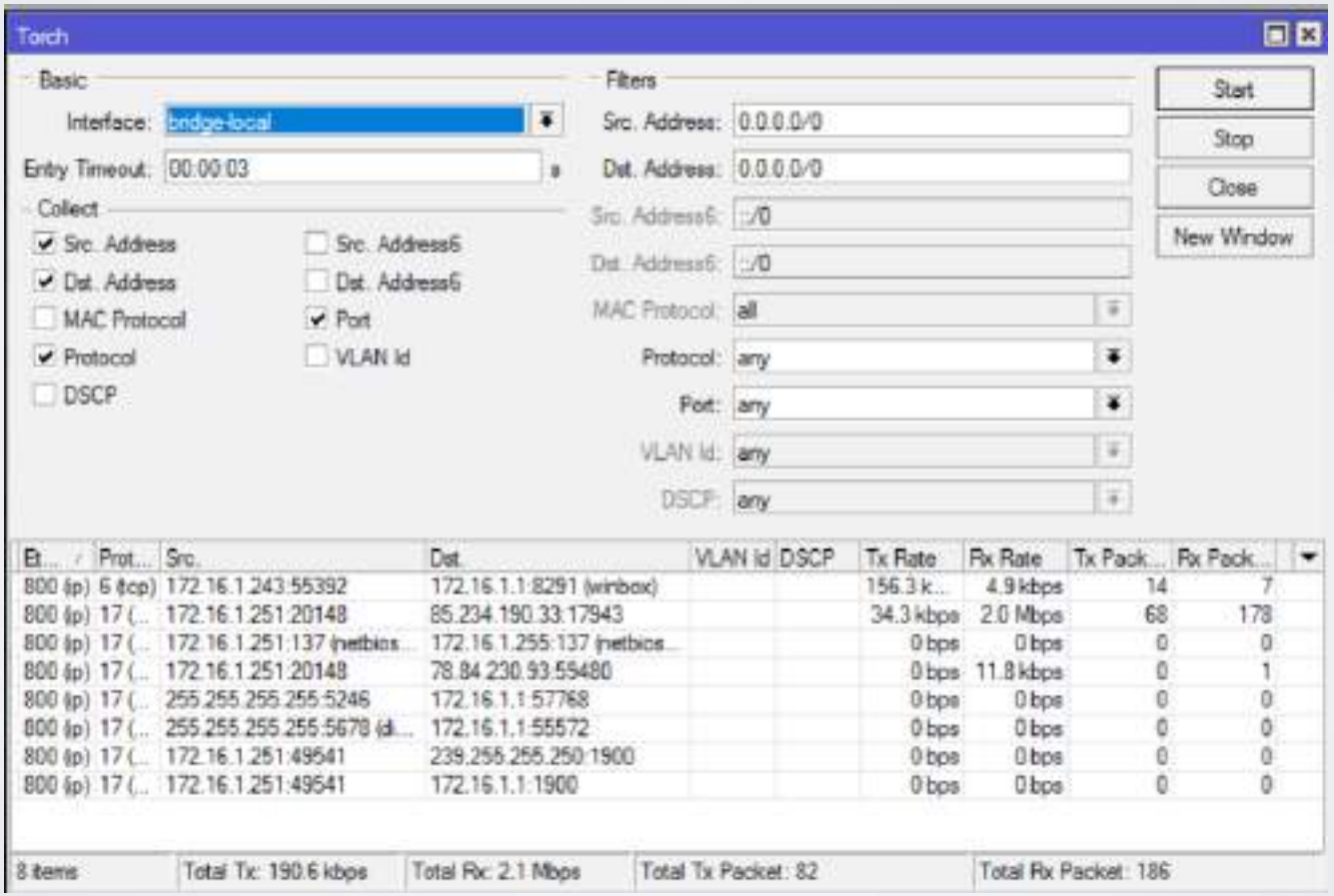
https://wiki.mikrotik.com/wiki/Manual:System/Log

Debugging tools

- Torch

  Analyse processed traffic

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

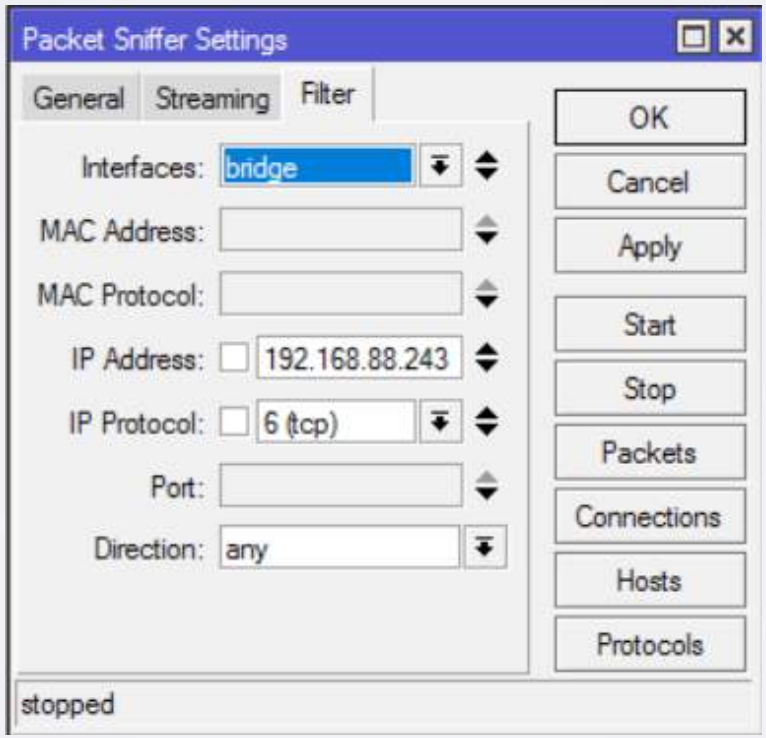


Debugging tools

- Sniffer

  Analyse processed packets

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

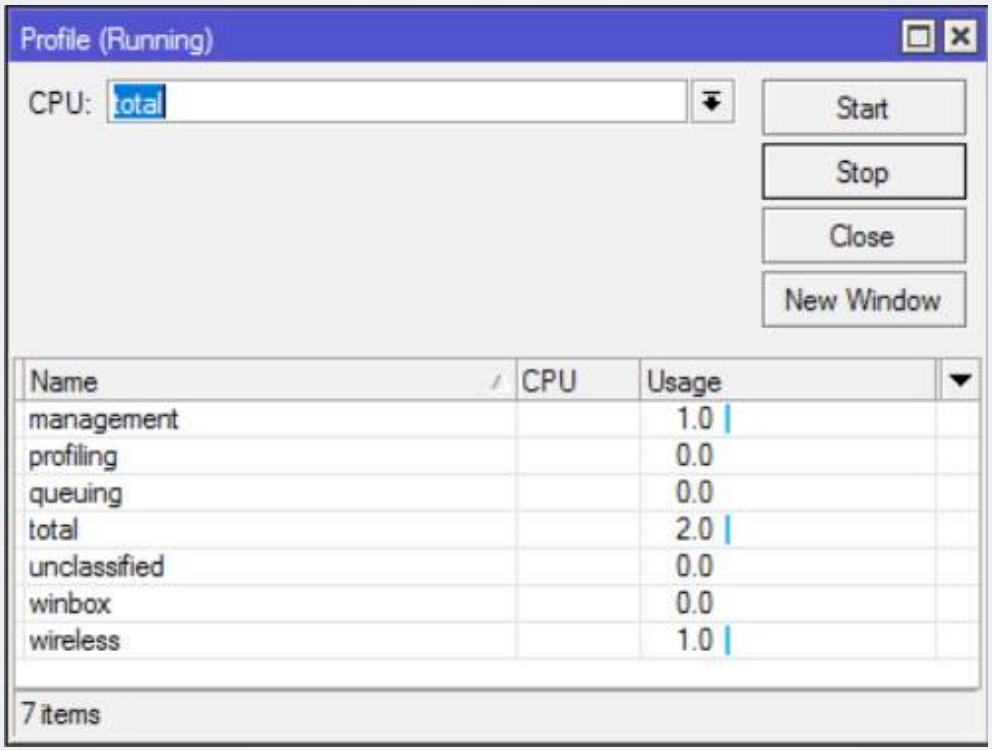


Debugging tools

- Profiler

  Find out current CPU usage

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

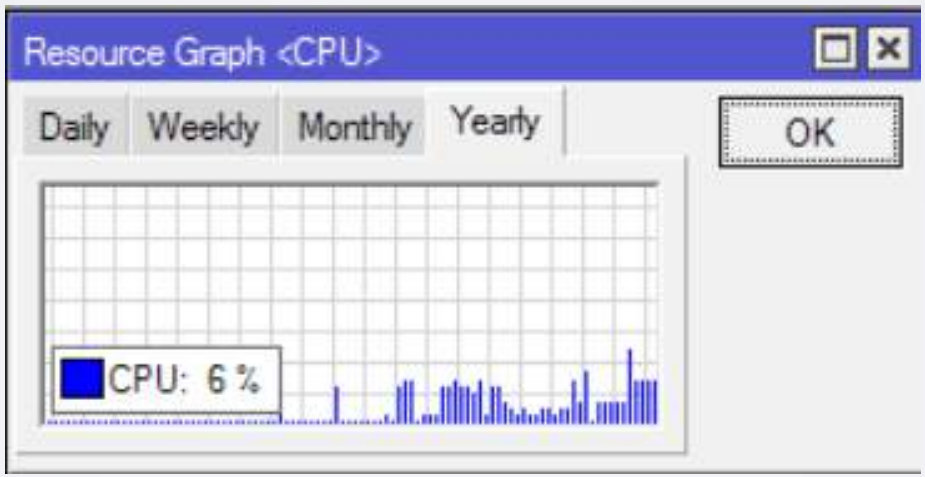


Debugging tools

- Graphing

  Find out information about Interfaces/Queues/Resources per interval:

  https://wiki.mikrotik.com/wiki/Manual:Tools/Graphing



Debugging tools

- The Dude

  Powerful network monitoring 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

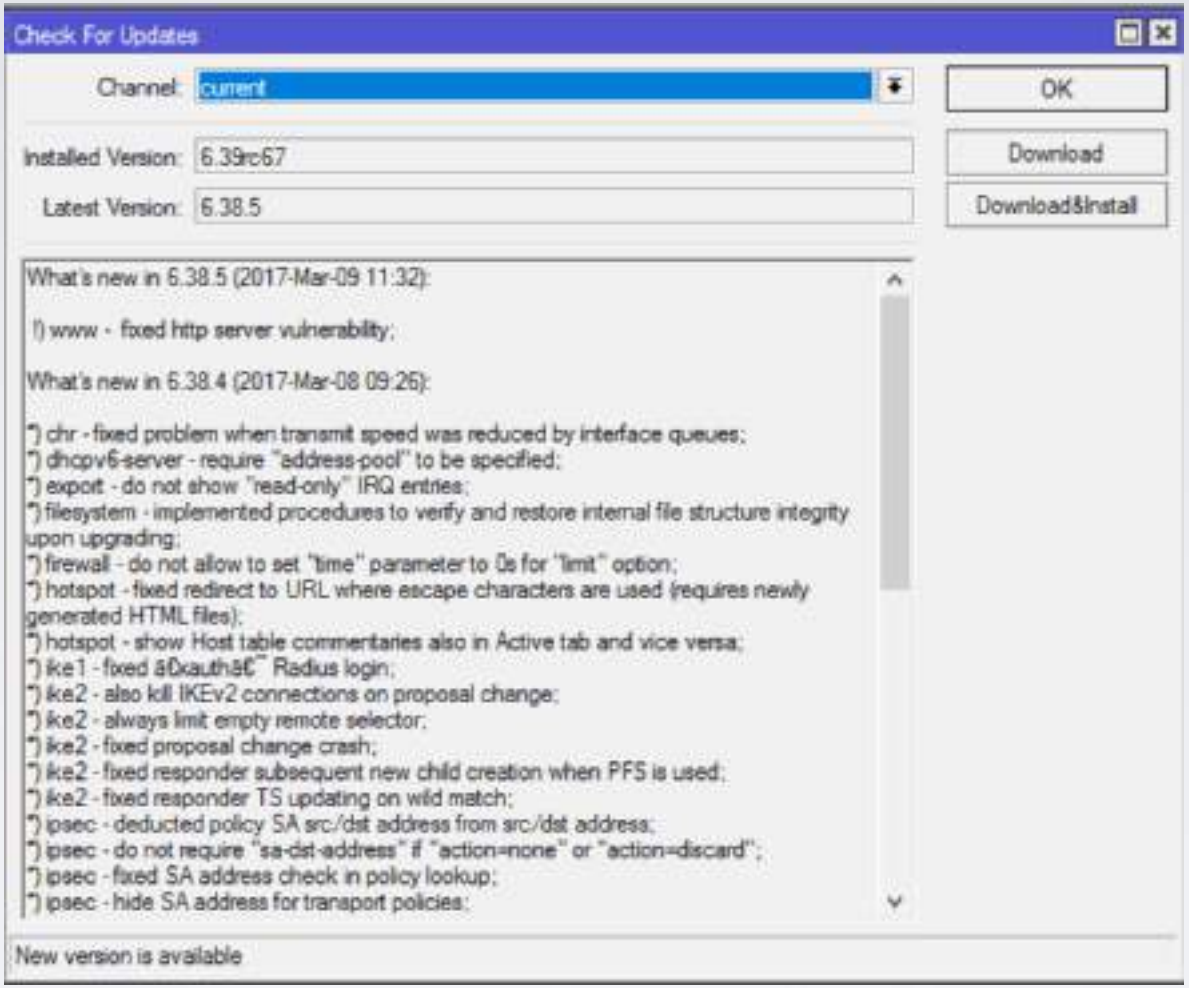
- Current

  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 the reset button

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

Software issues

- Device freeze
  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 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

Enjoy the MUM!