Effective work with Mikrotik

Эффективная работа с Mikrotik

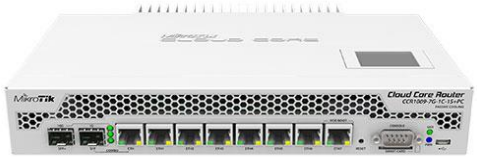
MUM in Kiev, Ukraine, June 08, 2018

Об авторе

- системный администратор более 10 лет
- настройка Windows, Linux
- виртуализация на основе VmWare (ESXi)
- сетевой инженер: Mikrotik, L2-L3 свитчи Cisco, D-Link, Edge-core etc.
- IP PBX (Asterisk) - open source программная АТС
- проектирование IT инфраструктуры заказчика и реализация проекта “под ключ”
- работа с Mikrotik более 8 лет (от hAP Lite до CCR)

Mikrotik это:

=

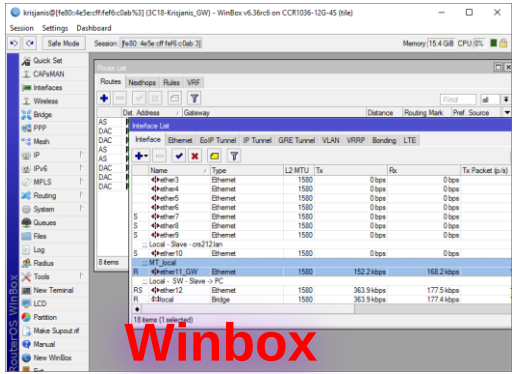


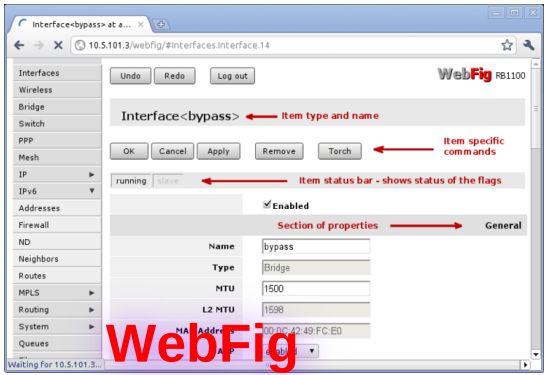
Можно сделать качественное решение

Дано:

или

Варианты настройки Mikrotik



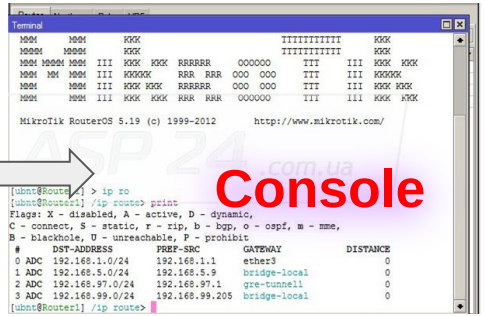


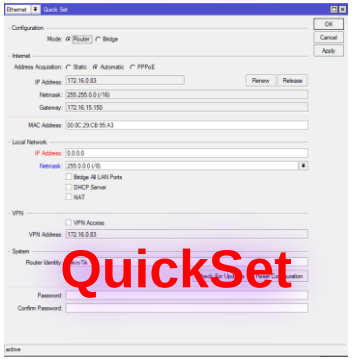
Initial login

```
/login
!done
=ret=ebddd18303a54111e2dea05a92ab46b4
/login
=name=admin
=response=001ea726ed53ae38520c8334f82d44c9f2
!done
```

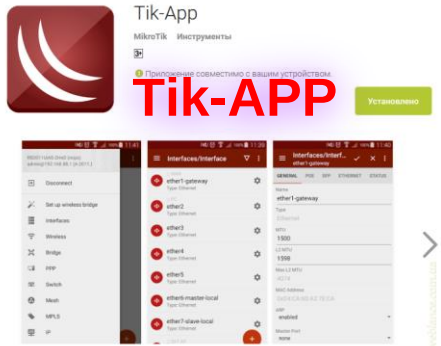
API

winbox
telnet
ssh
WebFig

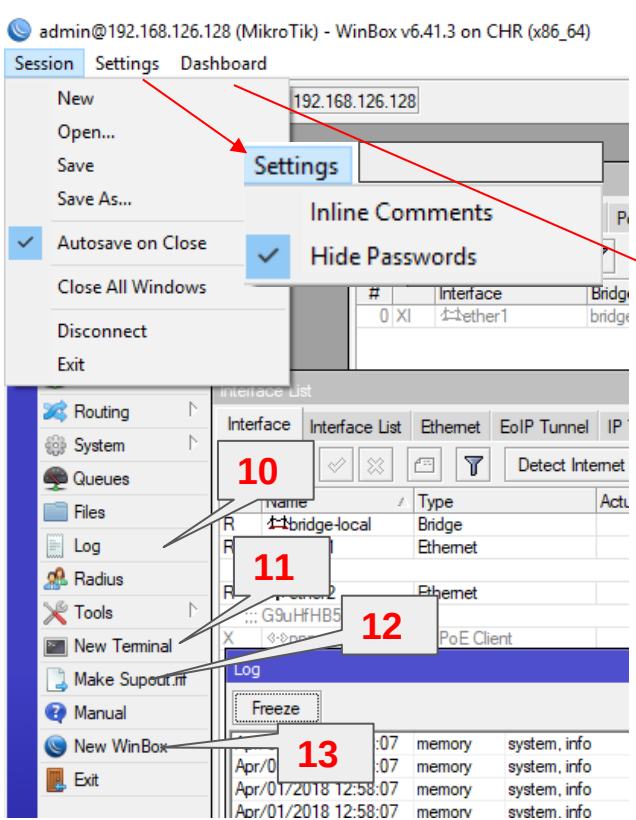


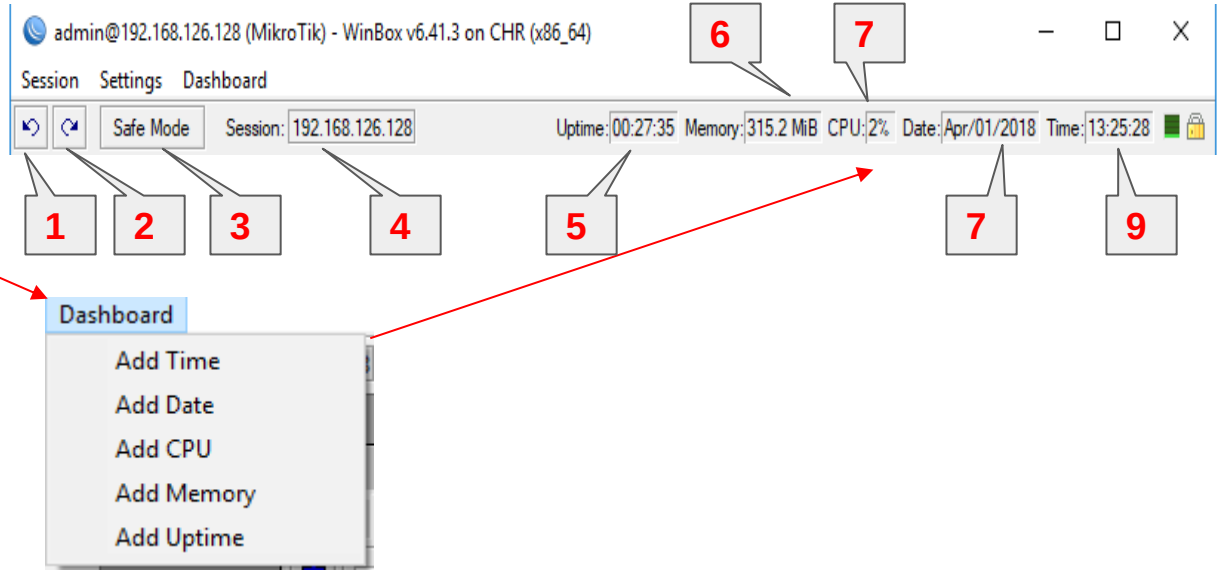


winbox
WebFig

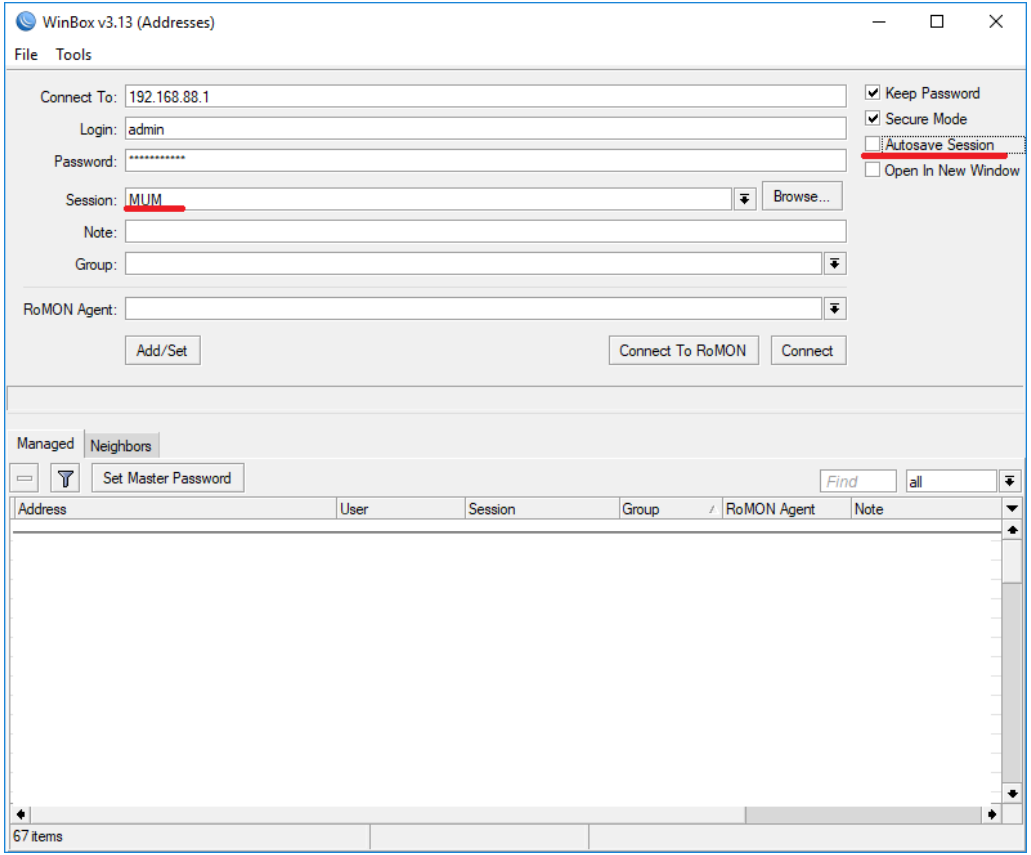


Winbox

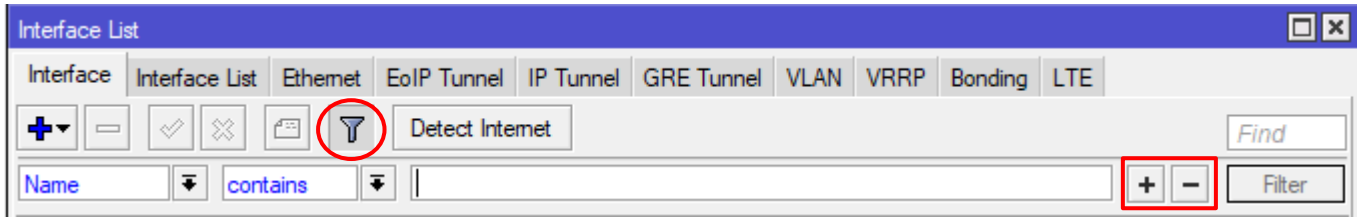

admin@192.168.126.128 (MikroTik) - WinBox v6.41.3 on CHR (x86_64)
Session
Settings
Dashboard
New
Open...
Save
Save As...
Autosave on Close
Close All Windows
Disconnect
Exit
Settings
Inline Comments
Hide Passwords
192.168.126.128
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
Make Supout.rif
Manual
New WinBox
Exit
Interface
Interface List
Ethernet
EoIP Tunnel
Detect Internet
Type
Bridge
Ethernet
PoE Client
Log
Freeze
memory
system, info
10
11
12
13

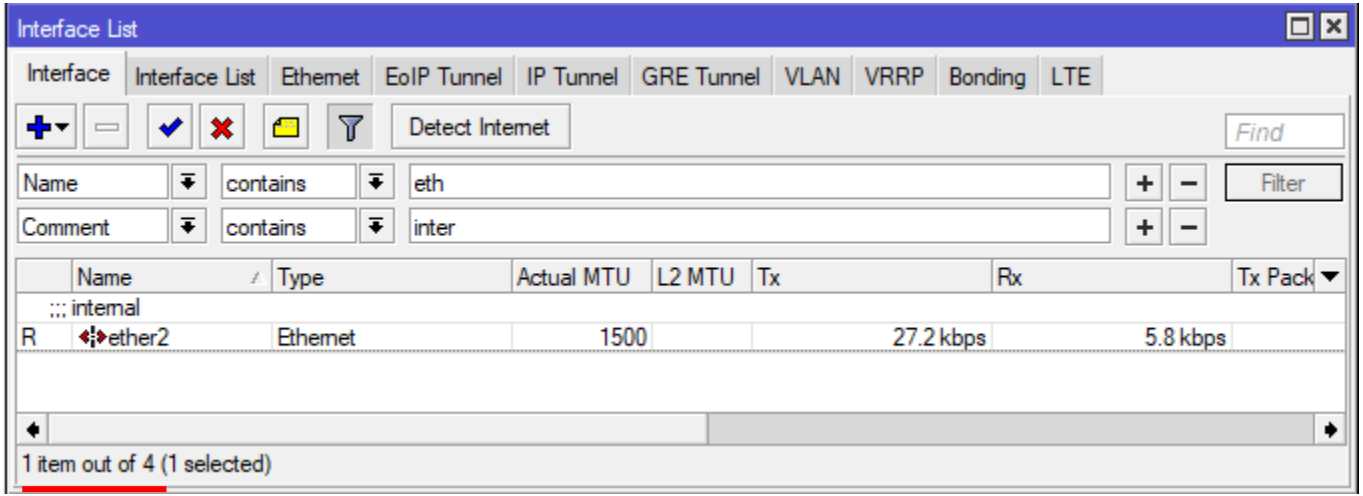

admin@192.168.126.128 (MikroTik) - WinBox v6.41.3 on CHR (x86_64)
Session
Settings
Dashboard
Safe Mode
Session: 192.168.126.128
Uptime: 00:27:35
Memory: 315.2 MiB
CPU: 2%
Date: Apr/01/2018
Time: 13:25:28
1
2
3
4
5
6
7
7
9
Dashboard
Add Time
Add Date
Add CPU
Add Memory
Add Uptime

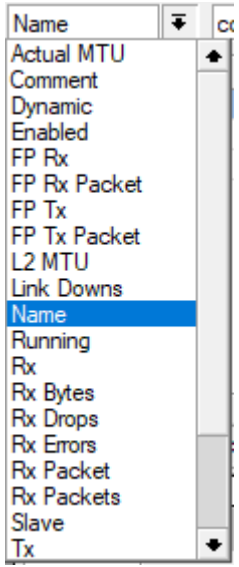
Winbox


WinBox v3.13 (Addresses)
File
Tools
Connect To:
192.168.88.1
Login:
admin
Password:
Session:
MUM
Browse...
Note:
Group:
RoMON Agent:
Add/Set
Connect To RoMON
Connect
Keep Password
Secure Mode
Autosave Session
Open In New Window
Managed
Neighbors
Set Master Password
Find
all
Address
User
Session
Group
RoMON Agent
Note
67 items

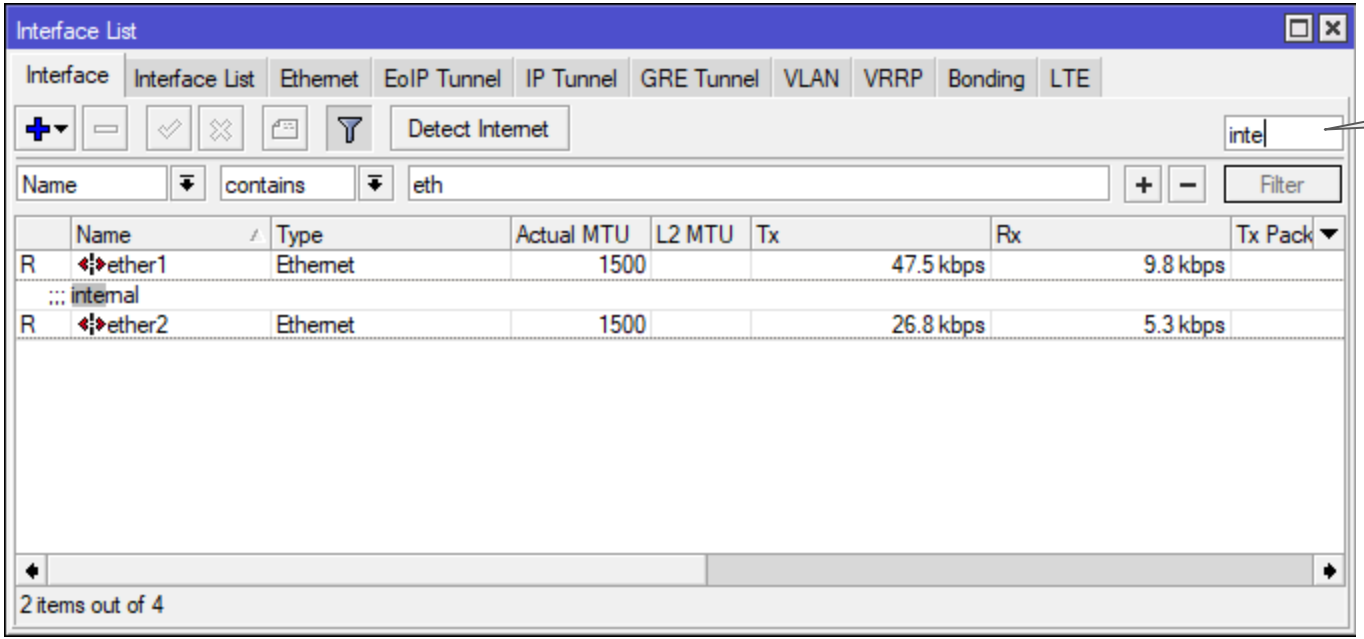
Используем фильтры







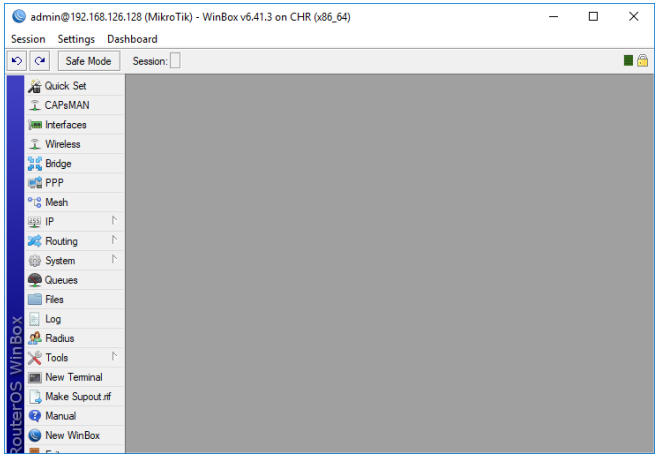
Инструменты поиска

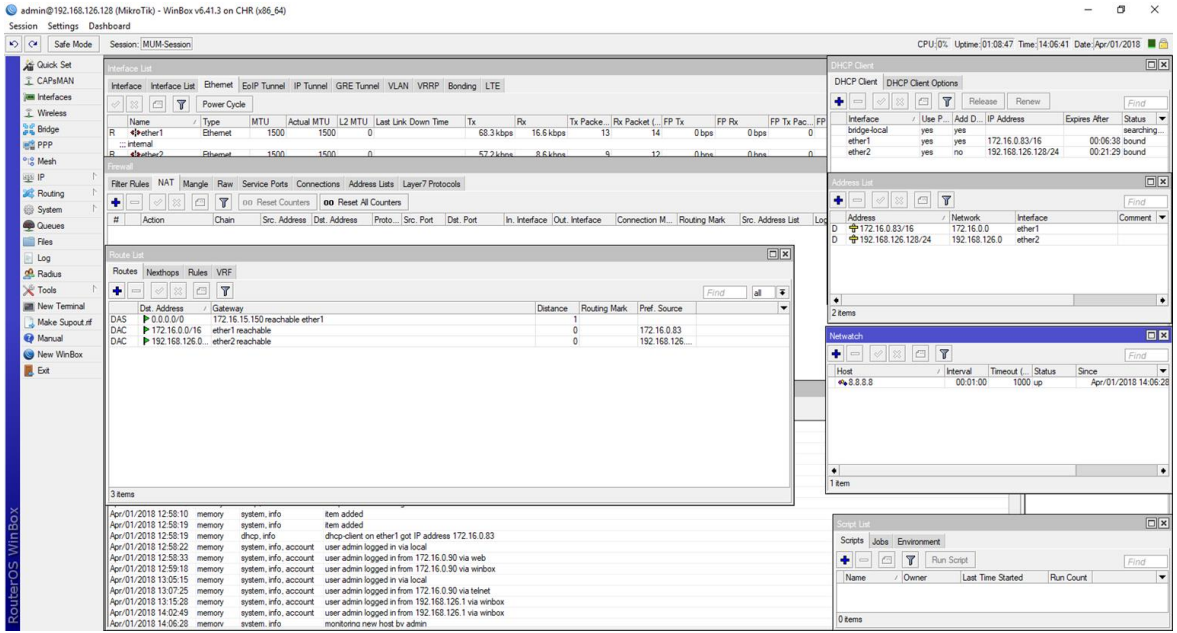


строка поиска

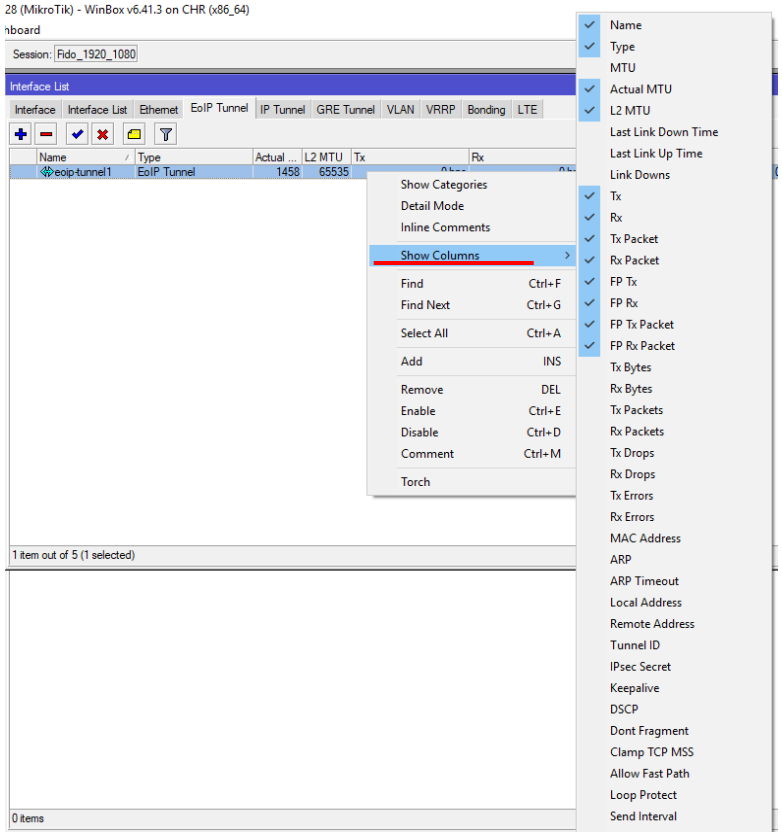
Ctrl-F
Ctrl-G

Использование сессий





Добавление/удаление “своих” колонок



Используя сессии:

Interface List

Interface | Interface List | Ethernet | EoIP Tunnel | IP Tunnel | GRE Tunnel | VLAN | VRRP | Bonding | LTE

RT1

Name	Type	Actual ...	L2 MTU	Tx	Rx	Tx Packet (...	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Pa...	FP Rx Pa...	Local Address	Remote Address	Tunnel ID
eoip-tunnel1	EoIP Tunnel	1458	65535	0 bps	0 bps	0	0	0 bps	0 bps	0	0	1.1.1.1	1.1.1.2	10

RT2

Name	Type	Actual ...	L2 MTU	Tx	Rx	Tx Packet (...	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Pa...	FP Rx Pa...	Local Address	Remote Address	Tunnel ID
eoip-tunnel1	EoIP Tunnel	1458	65535	0 bps	0 bps	0	0	0 bps	0 bps	0	0	1.1.1.2	1.1.1.1	1

Стандартные настройки колонок:

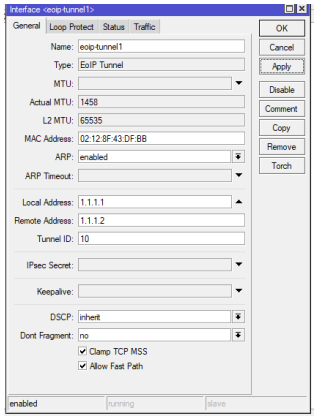
RT1

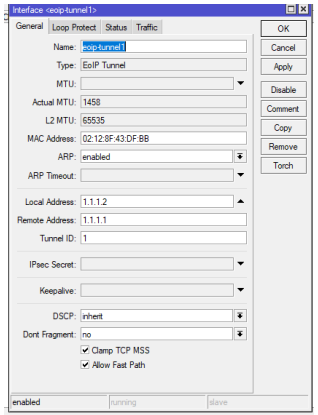
Name	Type	Actual ...	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)	FP Rx Packet (p/s)
eoip-tunnel1	EoIP Tunnel	1458	65535	0 bps	0 bps	0	0	0 bps	0 bps	0	0

нет отличий

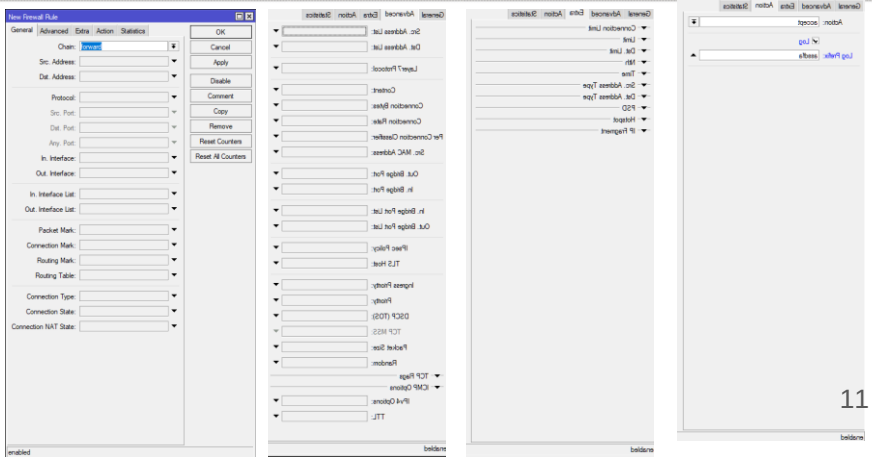
RT2

Name	Type	Actual ...	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)	FP Rx Packet (p/s)
eoip-tunnel1	EoIP Tunnel	1458	65535	0 bps	0 bps	0	0	0 bps	0 bps	0	0

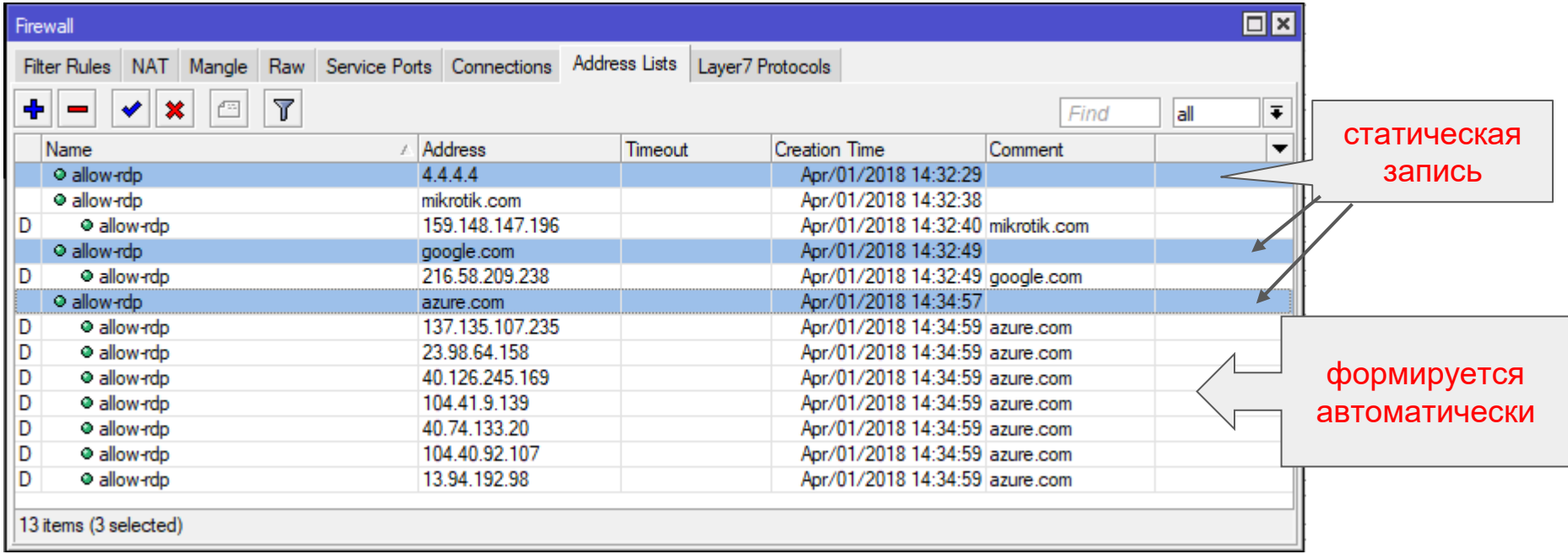




Обычный подход

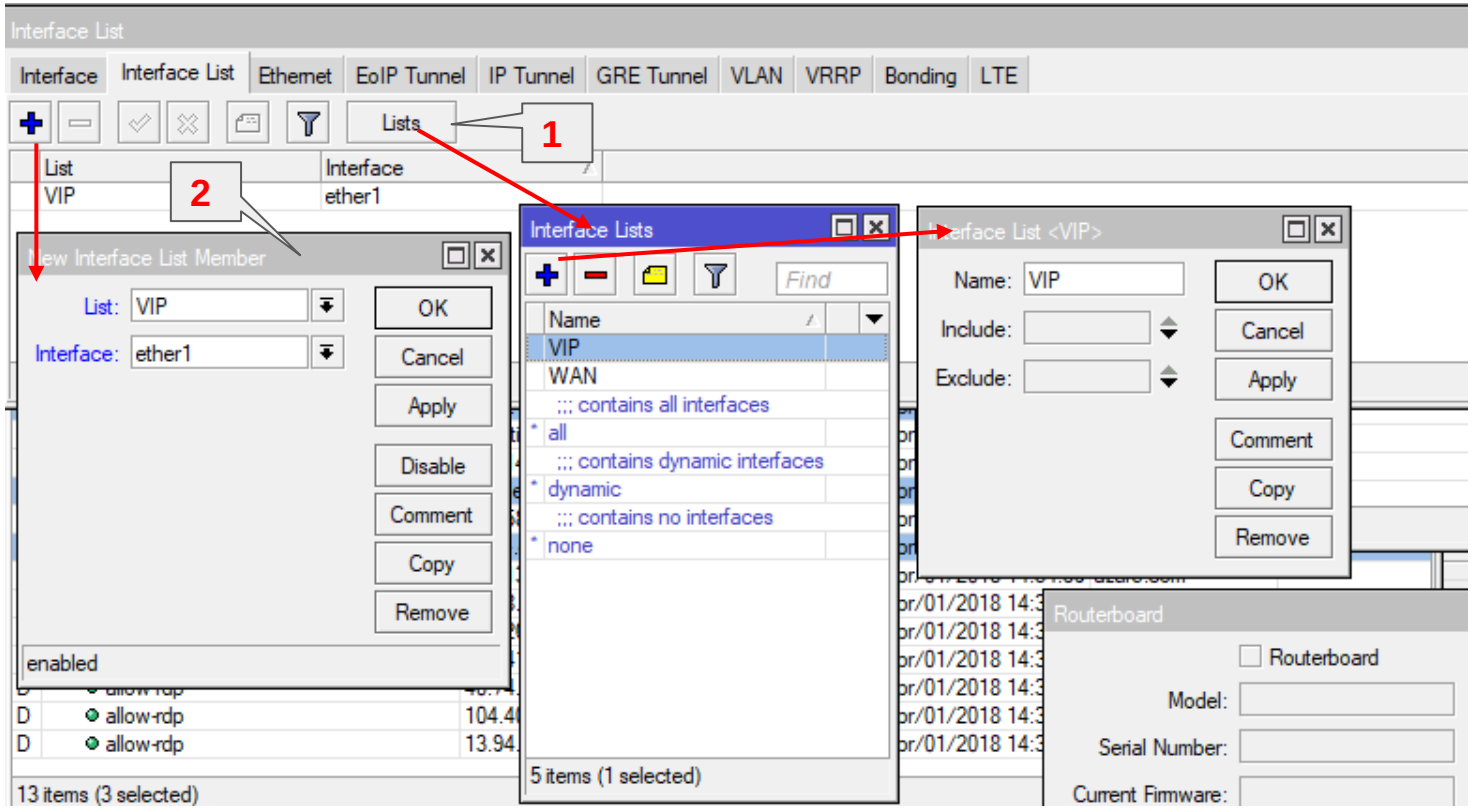


Address Lists



Используя Address List - в Firewall будет всего ОДНО правило, а не 10. Не нужно следить за изменениями IP адресов

Interface List



Права пользователей

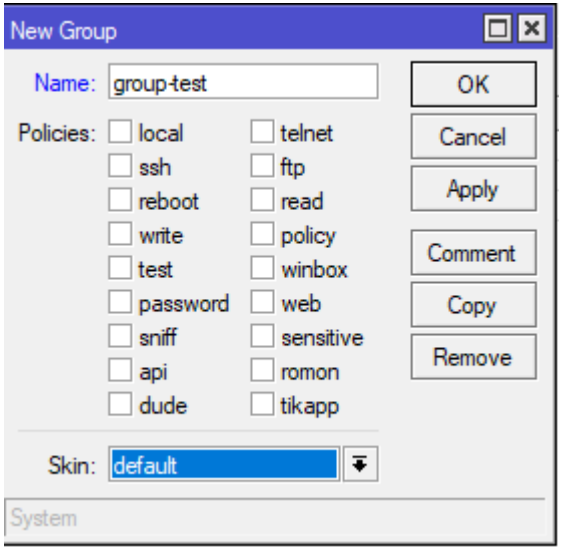
Гранулированные права доступа на основе групп
/system users groups

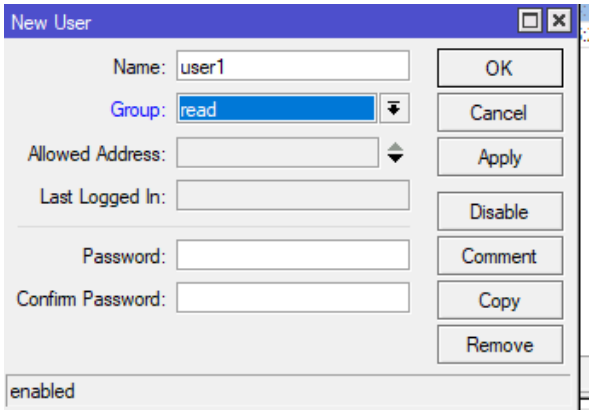
Стандартные full, read, write

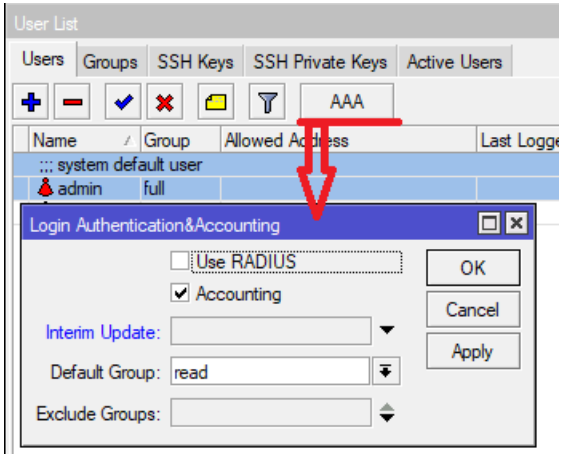
Категории прав:

Login policies: local, telnet, ssh, web, winbox, password, api, dude

Config Policies: ftp, reboot, read, write, policy, test, sensitive, sniff, romon





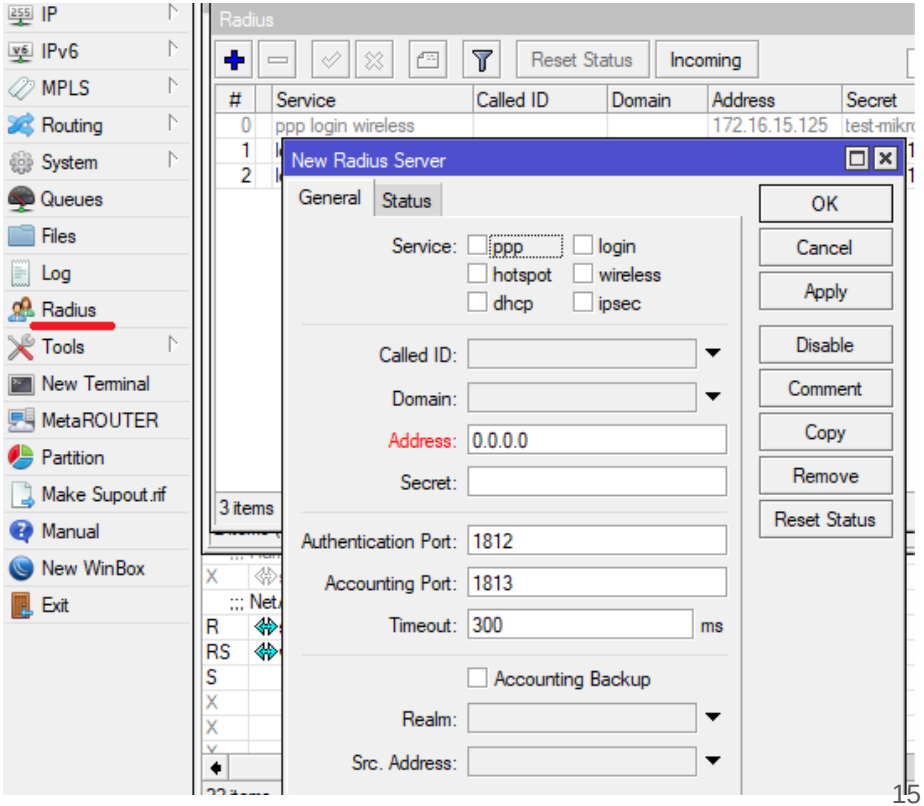


RADIUS

Единая точка хранения данных аутентификации, авторизации и аккаунтинга (при необходимости)

RADIUS можно использовать для аутентификации служб:

login, ppp, hotspot, dhcp (MAC), wireless (MAC), ipsec



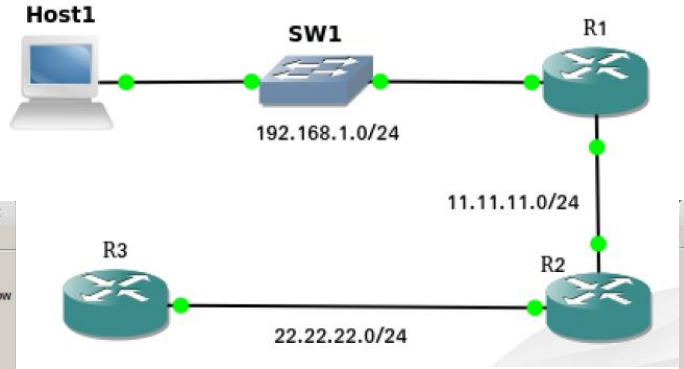
А Вы используете RoMON?

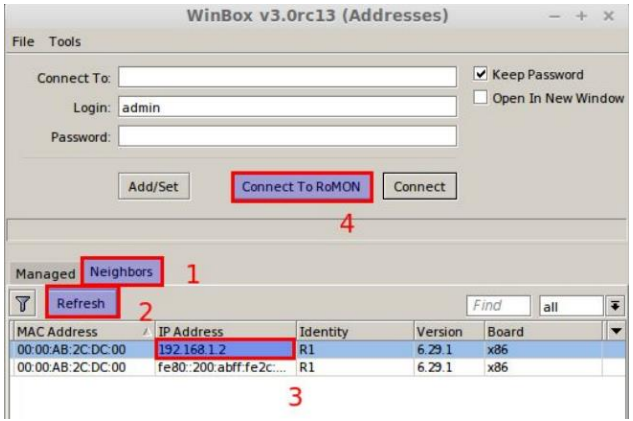
"Router Management Overlay Network" - возможность достучаться до роутера, когда сеть не работает

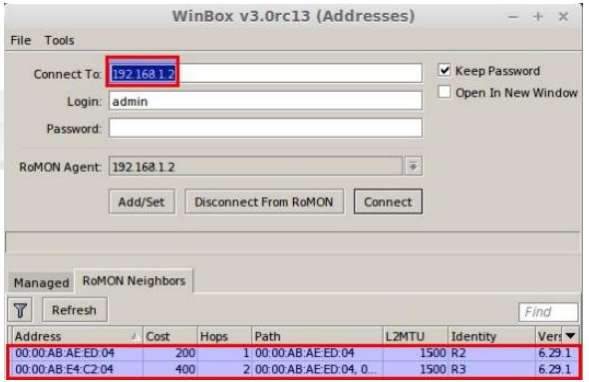
https://wiki.mikrotik.com/wiki/Manual:RoMON

https://mum.mikrotik.com/presentations/ID15/presentation_2841_1447681048.pdf

появился в ROS 6.28







Родительский контроль

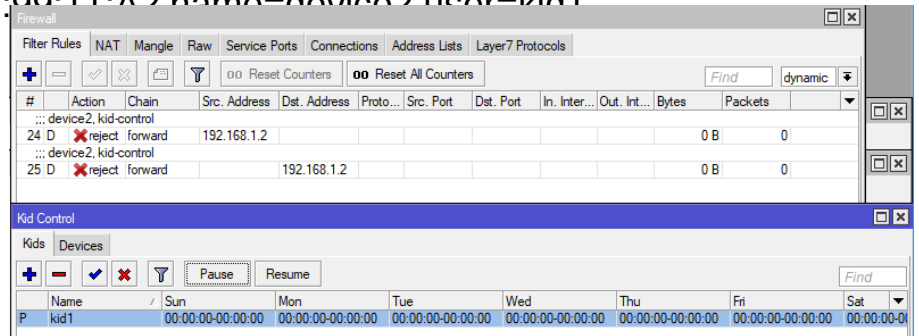
/ip kid-control Работает на ROS >6.42. Хотя на wiki указано 6.41+

Блокируем или ограничиваем по скорости устройства “детей”

Каждому MAC адресу задается принадлежность к владельцу

Одной командой разрешаем/запрещаем/задаем параметры доступа в интернет сразу на ВСЕ устройства

```
/ip kid-control add name=kid1 fri=7h-22h mon="" sat=6h-22h sun="" \
    thu="" time-rate-limited="" tue="" wed="" rate-limit=10k time-rate-limited=0s-0s
/ip kid-control device add mac-address=AA:AA:F1:99:11:A1 name=device1 user=kid1
/ip kid-control device add mac-address=AA:AA:F1:99:11:A2 name=device2 user=kid1
/ip kid-control pause kid1
/ip kid-control resume kid1
```



MetaRouter

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

MetaRouter is a new feature in RouterOS 4.0 beta 1 and RouterOS v3.21

Currently MetaRouter can be used on

- **RB400**, **RB700 series** except models with SPI flash, **RB900 series** except models with SPI flash, **RB2011** boards
- Listed PPC boards: **RB1000, RB1100, RB1100AH and RB800**.

MetaRouter - виртуальная машина. Можно поставить Open-WRT и там уже настроить SQUID, Asterisk

Нужно от 16Мб ОЗУ

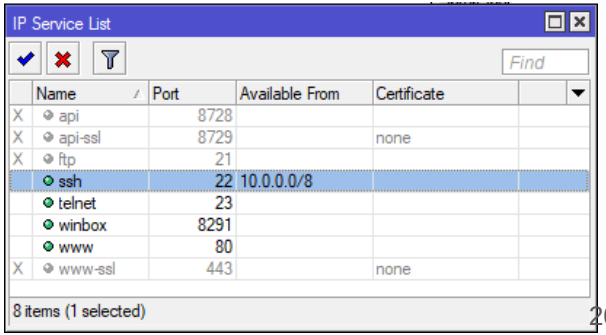
https://netflow.by/blog/net/629-zapusk-asterisk-na-mikrotik-s-pomoshchyu-metarouter-i-open-wrt
https://habrahabr.ru/post/180889/
http://asp24.com.ua/blog/virtualnaja-mashina-metarouter-i-zapusk-openwrt-na-marshrutizatorah-mikrotik/

Рекомендации:

- Address Lists
- Interface List (static, dynamic)
- DNS имена в address-list (> 6.36), туннельных интерфейсах и т.д.
- регулярно обновляем ROS и firmware (software “*/system package*”, firmware “*/system routerboard* ”).
- В 6.42 появилось /system routerboard settings set **auto-upgrade**=yes routerboard - added RouterBOOT "auto-upgrade" after RouterOS upgrade (extra reboot required);

Рекомендации (продолжение):

- /ip firewall layer7-protocol - используем аккуратно. Сильно грузит CPU
- /ip service - отключаем ненужное, ограничиваем разрешенные IP
- /ip cloud - Dynamic DNS от Mikrotik (появилось в 6.27)
  имя вида *529c0491d41c*.sn.mynetname.net
- Safe mode - бережем свои нервы и ноги !!!
- не забываем о бекапах (*.rsc and *.backup)
- bridge - admin mac address



Продвинутые возможности:

- remote log, topic log
- users: group right (full, read, write and custom), allow address, SSH keys
- TFTP сервер (загрузка по сети, конфигурация устройств)
- /ip service - меняем порты на нестандартные
- /system watchdog - перезагрузка роутера, если узел недоступен
- /system scheduler - планировщик (on boot, on time, repeat interval)
- AAA, remote radius, user manager
- /tool bandwidth-test - тест пропускной способности канала
- динамическая маршрутизация
- NTP server
- NTP client

Продвинутые возможности (продолжение):

- auto upgrade (one mikrotik as packages repository, from DUDE)

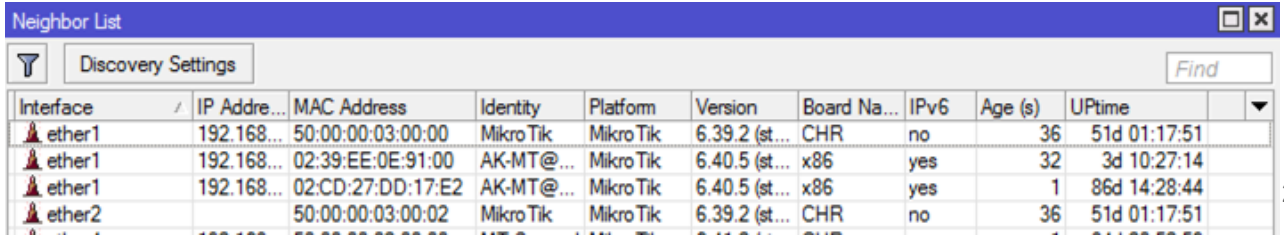
  System -> Auto Upgrade
  https://wiki.mikrotik.com/wiki/Manual:Upgrading_RouterOS

- QoS - приоритезация трафика (simple queue, queue tree)
- /tool mac-telnet
- шифрование (IPSec, GRE, OpenVPN, L2TP, EoIP т.д.) в т.ч. аппаратное в некоторых моделях н.р. hEX (RB750Gr3)
- Scripting (https://wiki.mikrotik.com/wiki/Manual:Scripting)
- /ip settings set rp-filter=strict - игнорируем пакеты с неправильным src (защита от bogon/bogus networks - немаршрутизируемые в интернет сети https://www.securitylab.ru/blog/personal/aodugin/305208.php)

Продвинутые возможности (продолжение):

- /ip neighbor - ищем устройства в сети. Нас тоже могут обнаружить!!! подобней https://habr.com/post/312236/

```
/interface bridge filter
add action=drop chain=output dst-mac-address=01:00:0C:CC:CC:CC/FF:FF:FF:FF:FF:FF \
    out-interface=ether1-gateway comment=”MNDP, CDP”
add action=drop chain=output comment="LLDP" \
    dst-mac-address=01:80:C2:00:00:0E/FF:FF:FF:FF:FF:FF out-interface=ether1-gateway
/ip firewall filter
add action=drop chain=output comment=Discovery dst-port=5678 \
    out-interface=ether1-gateway protocol=udp
```



Методы отладки (troubleshooting):

- /tool ping
- /tool traceroute
- /tool torch
- /log, /system logging - логируем нужное подробно
- /tool sniffer - захватываем и анализируем пакеты.
  Складываем локально или отправляем по протоколу TZSP и смотрим в real time в Wireshark (udp.port == 37008)

Нужна помощь, интернет не работает?

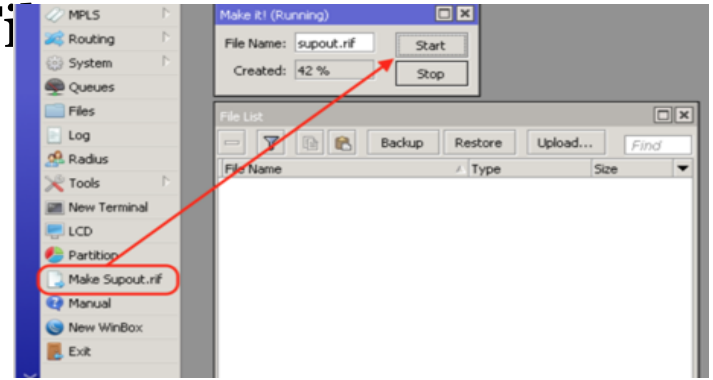
Support Output Fi

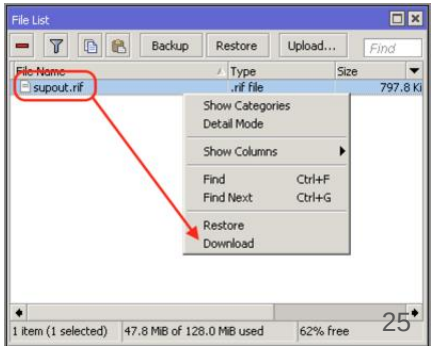
доступно создание из Winbox, Webfig, Console

/system sup-output name=supout.rif

Копируем файл к себе и передаем другу или в техподдержку. В нем содержится: логи, конфигурация, текущее состояние

Посмотреть содержимое файла можно на сайте https://mikrotik.com/client/supout





Нужна помощь, инетрет не работает?

Support Output File

address	instchk	queue
address6	interface	queue-bytes
arp	ippool	queue-packets
bfd	ipsec	queue-stats
bgp	license	resource
bridge	log	route
certificate	mesh	route6
dhcp	mme	routerboard
export	mpls	store
firewall	neighbor	switch
firewall-bytes	neighbor6	usb
firewall-packets	nexthop	web-proxy
firewall-stats	ospf	webproxy
firewall6	package	webproxy-test
firewall6-stats	pci	wireless
health	port	
hotspot	ppp	

Полезные ссылки и контакты:

- https://mikrotik.com/download
- https://wiki.mikrotik.com/wiki/Manual:TOC
- mikrotik backup and configure system - Ansible (http://mum.mikrotik.com/presentations/RU16/presentation_3841_1476092869.pdf, https://youtu.be/-NfES26eE-c)
- https://mum.mikrotik.com/archive
- https://wiki.mikrotik.com/wiki/Manual:Packet_Flow

e-mail: Mihail.MUM@gmail.com