

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:



Дано:



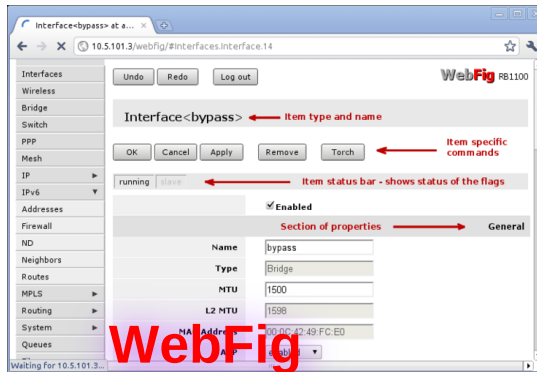
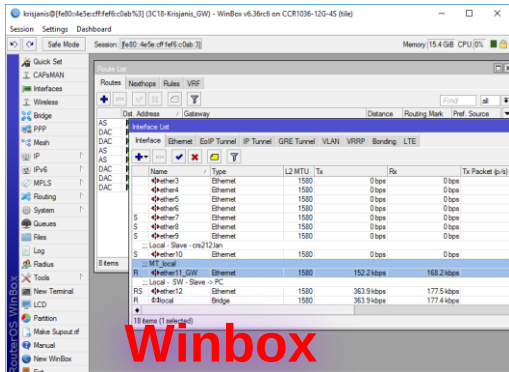
Можно сделать качественное решение



ИЛИ



Варианты настройки Mikrotik



Initial login

```
/login
```

!done

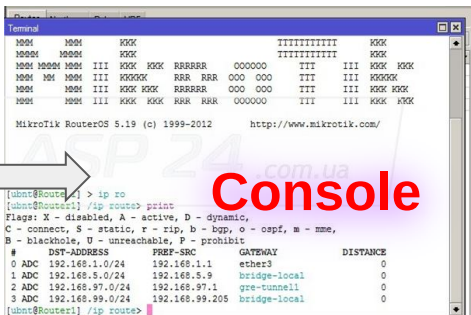
```
=ret=ebddd18303a54111e2dea05a92ab46b4
```

```
/login
```

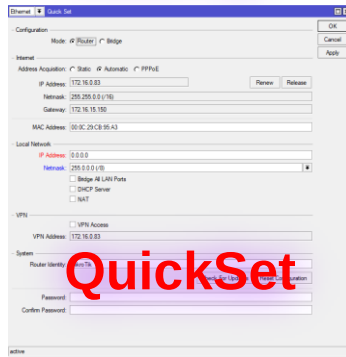
```
=name=admin
```

```
=response=001ea726ed53ae38520c8334f82d44c9f2
```

!done



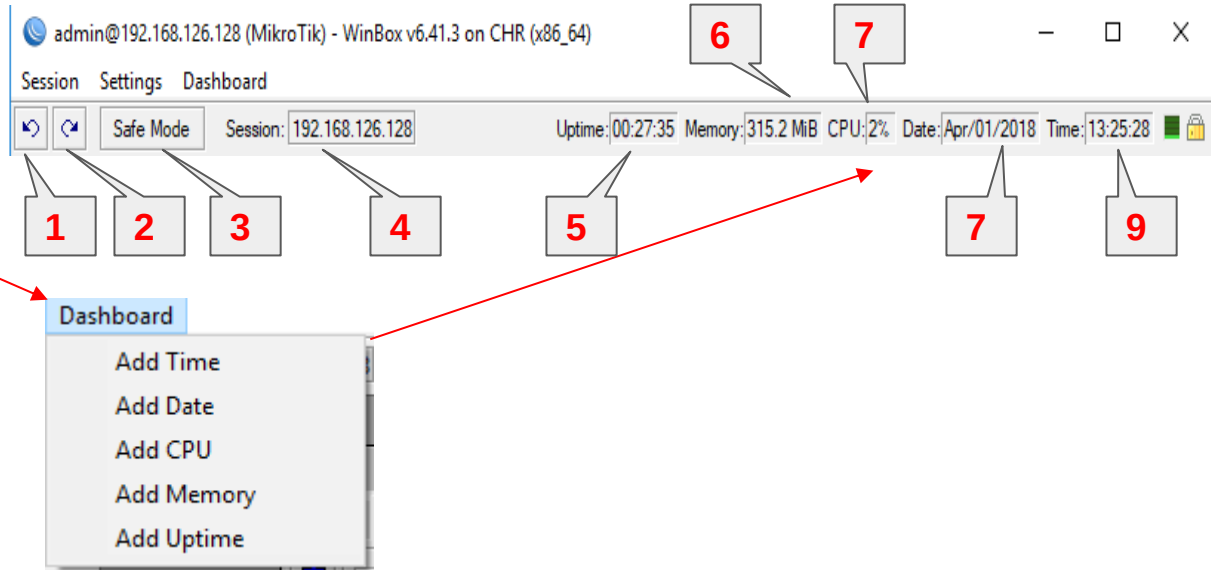
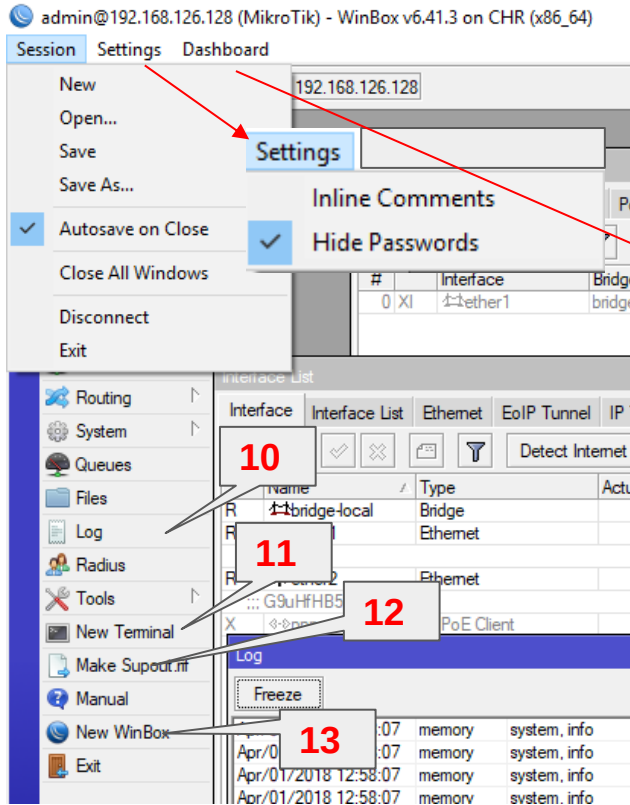
- winbox
- telnet ☐
- ssh
- WebFig



winbox
WebFig



Winbox



Winbox

WinBox v3.13 (Addresses)

File Tools

Connect To: 192.168.88.1

Login: admin

Password: *****

Session: MUM Browse...

Note:

Group:

RoMON Agent:

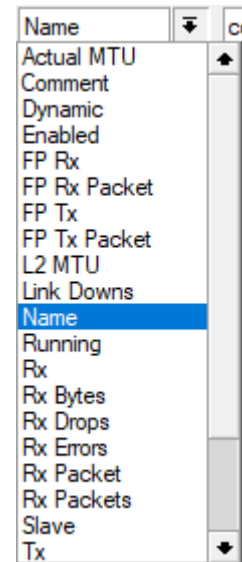
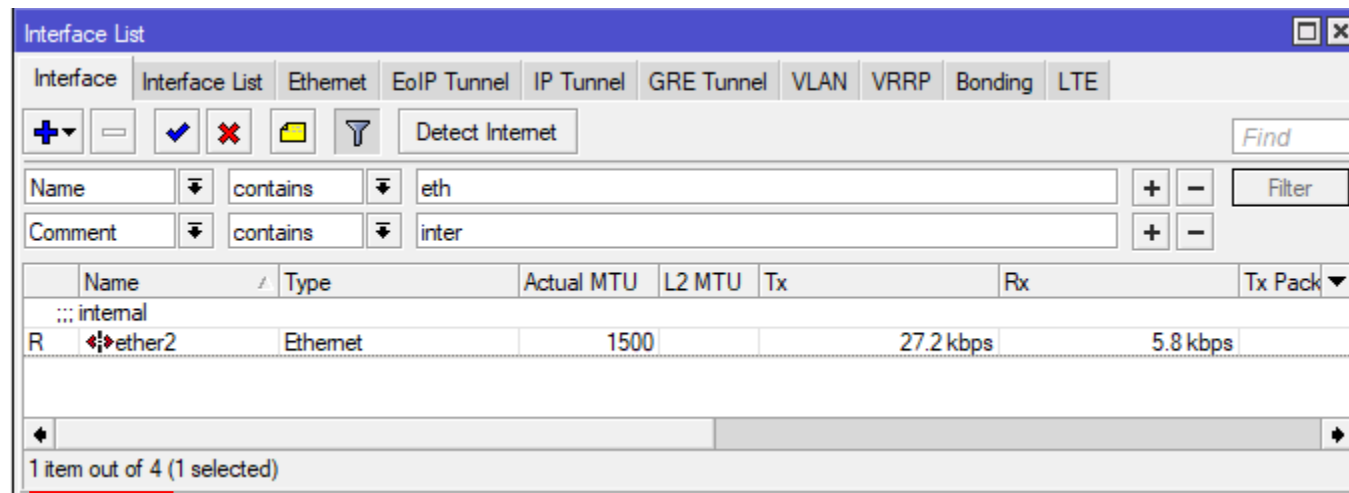
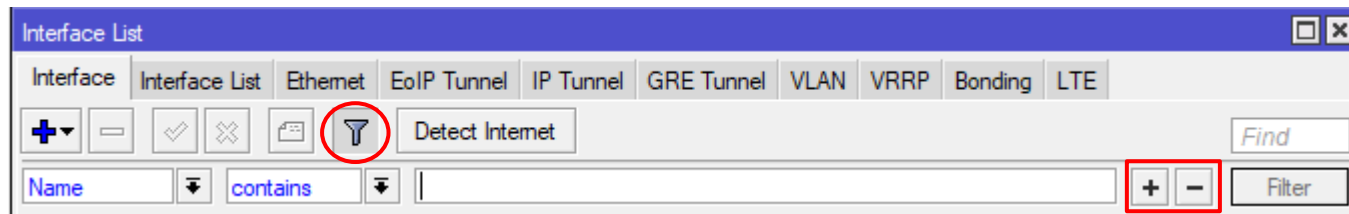
Add/Set Connect To RoMON Connect

Managed Neighbors

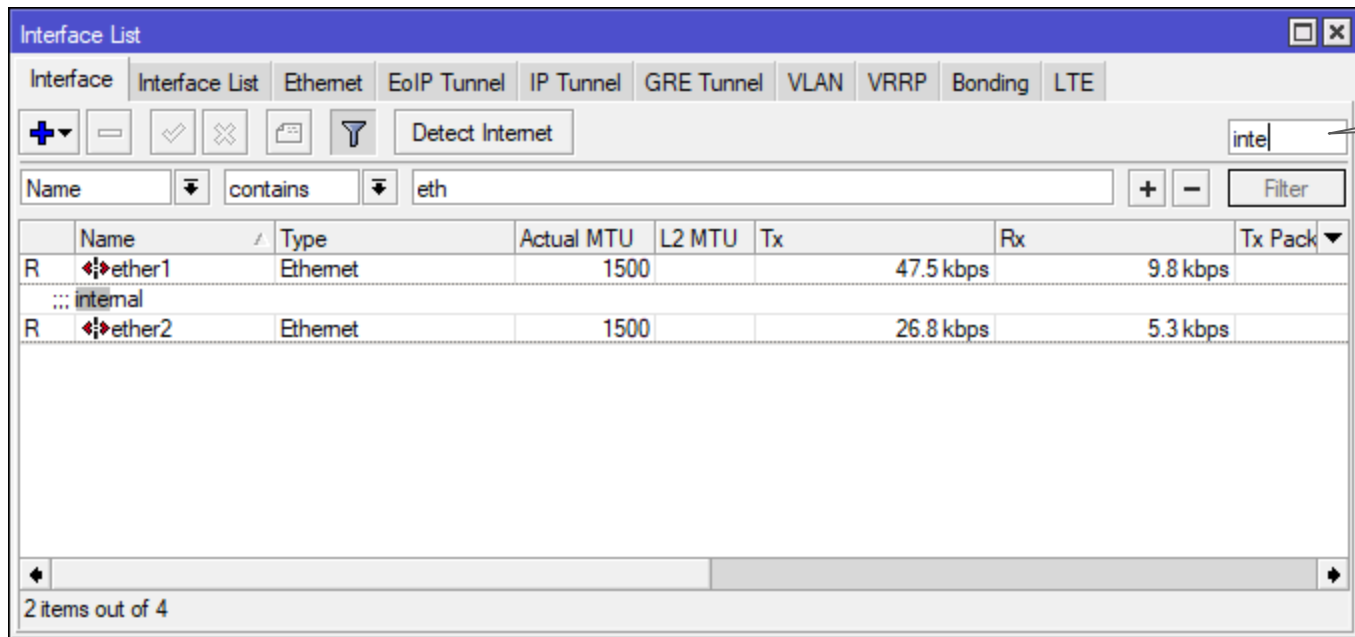
Set Master Password Find all

Address	User	Session	Group	RoMON Agent	Note
67 items					

Используем фильтры



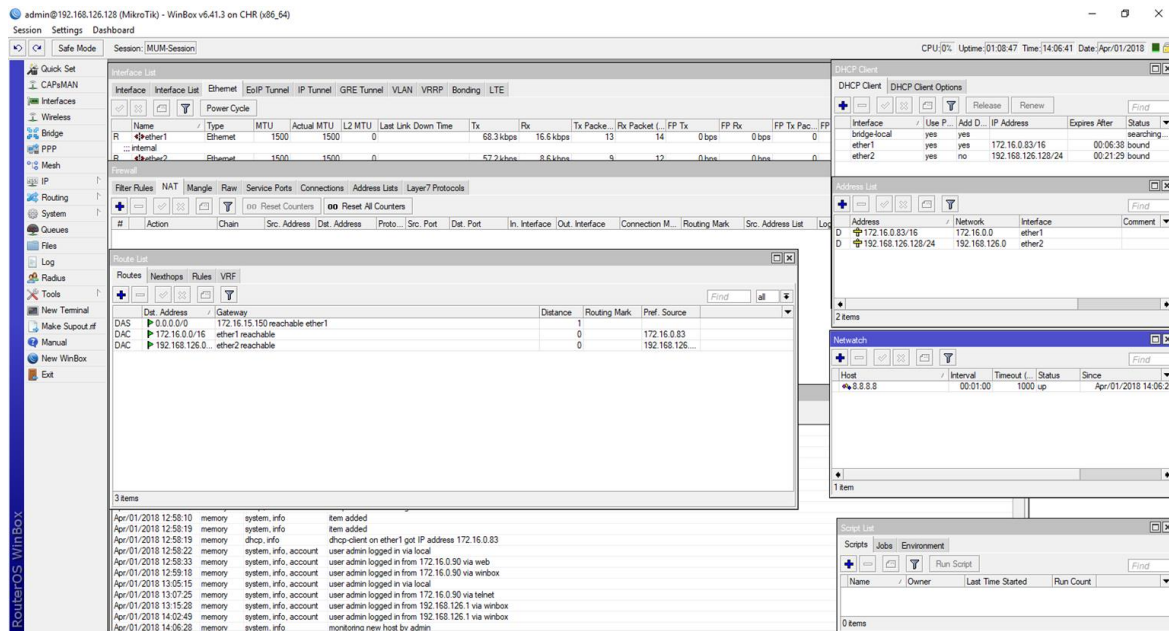
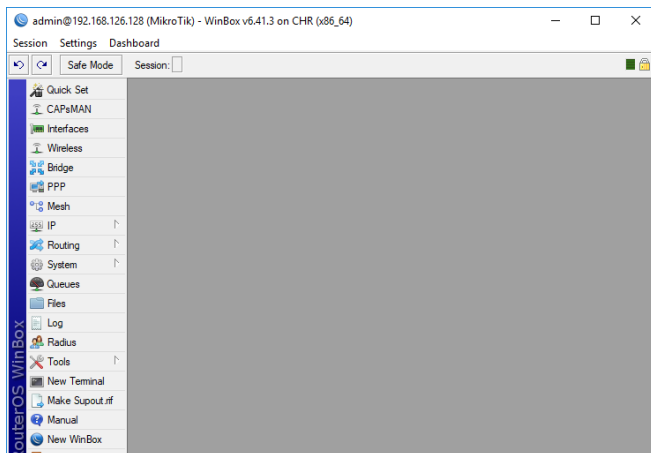
Инструменты поиска



строка поиска

Ctrl-F
Ctrl-G

Использование сессий



Добавление/удаление “своих” колонок

28 (MikroTik) - WinBox v6.41.3 on CHR (x86_64)

nboard

Session: [Fido_1920_1080]

Interface List

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

+ - ✓ ✗ 🗑️ 🔍

Name	Type	Actual ...	L2 MTU	Tx	Rx
eoip-tunnel1	EoIP Tunnel	1458	65535		

1 item out of 5 (1 selected)

0 items

Show Categories
Detail Mode
Inline Comments
Show Columns >
Find Ctrl+F
Find Next Ctrl+G
Select All Ctrl+A
Add INS
Remove DEL
Enable Ctrl+E
Disable Ctrl+D
Comment Ctrl+M
Torch

- ✓ Name
- ✓ Type
- MTU
- ✓ Actual MTU
- ✓ L2 MTU
- Last Link Down Time
- Last Link Up Time
- Link Downs
- ✓ Tx
- ✓ Rx
- ✓ Tx Packet
- ✓ Rx Packet
- ✓ FP Tx
- ✓ FP Rx
- ✓ FP Tx Packet
- ✓ FP Rx Packet
- ✓ Tx Bytes
- Rx Bytes
- Tx Packets
- Rx Packets
- Tx Drops
- Rx Drops
- Tx Errors
- Rx Errors
- MAC Address
- ARP
- ARP Timeout
- Local Address
- Remote Address
- Tunnel ID
- IPsec Secret
- Keepalive
- DSCP
- Dont Fragment
- Clamp TCP MSS
- Allow Fast Path
- Loop Protect
- Send Interval

Используя сессии:

Interface List

Interface

Interface List

Ethernet

EoIP Tunnel

IP Tunnel

GRE Tunnel

VLAN

VRRP

Bonding

LTE

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

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	1.1.1.2	1.1.1.1	1

RT2

Стандартные настройки колонок:

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		

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		

RT2

нет отличий

Interface: eoip-tunnel1

General

Name: eoip-tunnel1

Type: EoIP Tunnel

MTU: 1458

Actual MTU: 1458

L2 MTU: 65535

MAC Address: 02:12:8F:43:DF:BB

ARP: enabled

ARP Timeout: 30

Local Address: 1.1.1.1

Remote Address: 1.1.1.2

Tunnel ID: 10

IPsec Secret:

Keepalive: inherit

Dont Fragment: no

Clamp TCP MSS

Allow Fast Path

enabled

turning

save

Interface: eoip-tunnel1

General

Name: eoip-tunnel1

Type: EoIP Tunnel

MTU: 1458

Actual MTU: 1458

L2 MTU: 65535

MAC Address: 02:12:8F:43:DF:BB

ARP: enabled

ARP Timeout: 30

Local Address: 1.1.1.2

Remote Address: 1.1.1.1

Tunnel ID: 1

IPsec Secret:

Keepalive: inherit

Dont Fragment: no

Clamp TCP MSS

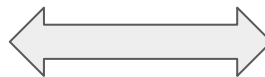
Allow Fast Path

enabled

turning

save

Обычный подход



New Firewall Rule

General

Chain: input

Src Address:

Dst Address:

Protocol:

Src Port:

Dst Port:

Any Port:

In Interface:

Out Interface:

In Interface List:

Out Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Interface: eoip-tunnel1

General

Name: eoip-tunnel1

Type: EoIP Tunnel

MTU: 1458

Actual MTU: 1458

L2 MTU: 65535

MAC Address: 02:12:8F:43:DF:BB

ARP: enabled

ARP Timeout: 30

Local Address: 1.1.1.1

Remote Address: 1.1.1.2

Tunnel ID: 10

IPsec Secret:

Keepalive: inherit

Dont Fragment: no

Clamp TCP MSS

Allow Fast Path

enabled

turning

save

Interface: eoip-tunnel1

General

Name: eoip-tunnel1

Type: EoIP Tunnel

MTU: 1458

Actual MTU: 1458

L2 MTU: 65535

MAC Address: 02:12:8F:43:DF:BB

ARP: enabled

ARP Timeout: 30

Local Address: 1.1.1.2

Remote Address: 1.1.1.1

Tunnel ID: 1

IPsec Secret:

Keepalive: inherit

Dont Fragment: no

Clamp TCP MSS

Allow Fast Path

enabled

turning

save

Interface: eoip-tunnel1

General

Name: eoip-tunnel1

Type: EoIP Tunnel

MTU: 1458

Actual MTU: 1458

L2 MTU: 65535

MAC Address: 02:12:8F:43:DF:BB

ARP: enabled

ARP Timeout: 30

Local Address: 1.1.1.1

Remote Address: 1.1.1.2

Tunnel ID: 10

IPsec Secret:

Keepalive: inherit

Dont Fragment: no

Clamp TCP MSS

Allow Fast Path

enabled

turning

save

Address Lists

Firewall

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

Find all

Name	Address	Timeout	Creation Time	Comment
allow-rdp	4.4.4.4		Apr/01/2018 14:32:29	
allow-rdp	mikrotik.com		Apr/01/2018 14:32:38	
D allow-rdp	159.148.147.196		Apr/01/2018 14:32:40	mikrotik.com
allow-rdp	google.com		Apr/01/2018 14:32:49	
D allow-rdp	216.58.209.238		Apr/01/2018 14:32:49	google.com
allow-rdp	azure.com		Apr/01/2018 14:34:57	
D allow-rdp	137.135.107.235		Apr/01/2018 14:34:59	azure.com
D allow-rdp	23.98.64.158		Apr/01/2018 14:34:59	azure.com
D allow-rdp	40.126.245.169		Apr/01/2018 14:34:59	azure.com
D allow-rdp	104.41.9.139		Apr/01/2018 14:34:59	azure.com
D allow-rdp	40.74.133.20		Apr/01/2018 14:34:59	azure.com
D allow-rdp	104.40.92.107		Apr/01/2018 14:34:59	azure.com
D allow-rdp	13.94.192.98		Apr/01/2018 14:34:59	azure.com

13 items (3 selected)

статическая запись

формируется автоматически

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

Interface List

The screenshot displays the Mikrotik WinBox interface for configuring the Interface List. The 'Interface List' window is open, showing tabs for Interface, Interface List, Ethernet, EoIP Tunnel, IP Tunnel, GRE Tunnel, VLAN, VRRP, Bonding, and LTE. The 'Interface List' tab is selected, and the 'Lists' button is highlighted with a red arrow and the number '1'. A second red arrow and the number '2' point to the 'New Interface List Member' dialog box, which is open for the 'VIP' list and 'ether1' interface. The 'Interface Lists' window shows a list of lists including 'VIP', 'WAN', 'all', 'dynamic', and 'none'. The 'Interface List <VIP>' dialog box is also visible, showing fields for Name, Include, and Exclude. The 'Routerboard' dialog box is partially visible at the bottom right.

Interface List

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

List VIP Interface ether1

New Interface List Member

List: VIP Interface: ether1

OK Cancel Apply Disable Comment Copy Remove

enabled

Interface Lists

Name

VIP

WAN

... contains all interfaces

* all

... contains dynamic interfaces

* dynamic

... contains no interfaces

* none

5 items (1 selected)

Interface List <VIP>

Name: VIP

Include:

Exclude:

OK Cancel Apply Comment Copy Remove

Routerboard

☐ Routerboard

Model:

Serial Number:

Current Firmware:

Права пользователей

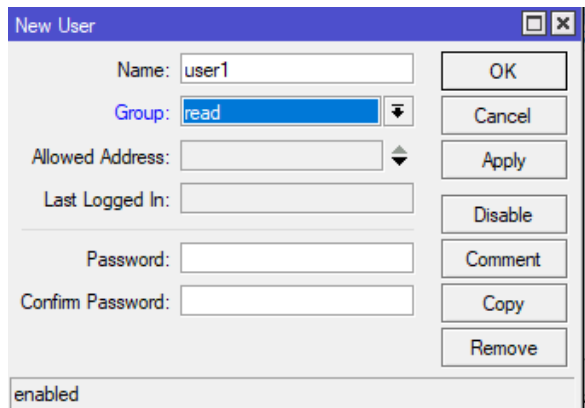
Гранулированные права доступа на основе групп
/system users groups

Стандартные full, read, write

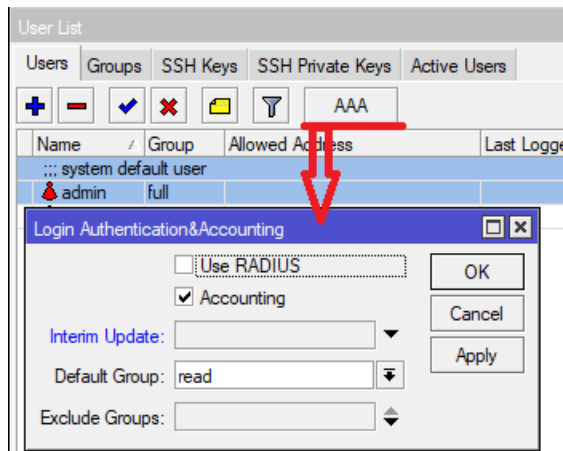
Категории прав:

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

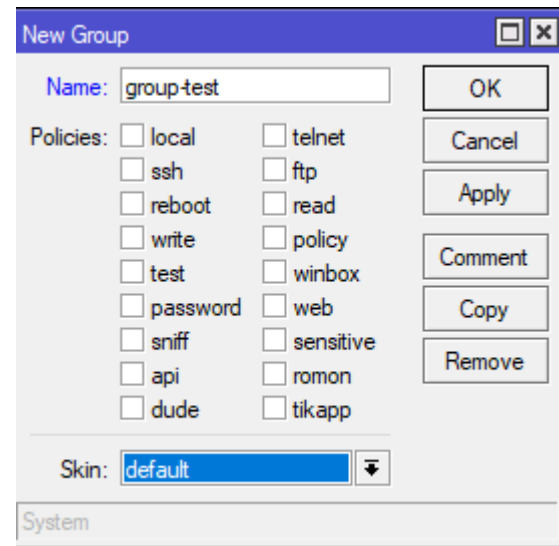
Config Policies: ftp, reboot, read, write, policy, test, sensitive, sniff, romon



New User dialog box. Fields: Name: user1, Group: read (selected), Allowed Address: (empty), Last Logged In: (empty), Password: (empty), Confirm Password: (empty). Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove. Status: enabled.



User List dialog box. Tabs: Users, Groups, SSH Keys, SSH Private Keys, Active Users. Table with columns: Name, Group, Allowed Address, Last Logged In. Row 1: system default user, Group: default, Allowed Address: (empty), Last Logged In: (empty). Row 2: admin, Group: full, Allowed Address: (empty), Last Logged In: (empty). A red arrow points from the 'full' group to the 'Login Authentication & Accounting' dialog box. Login Authentication & Accounting dialog box. Fields: Use RADIUS (unchecked), Accounting (checked), Interim Update: (empty), Default Group: read (selected), Exclude Groups: (empty). Buttons: OK, Cancel, Apply.



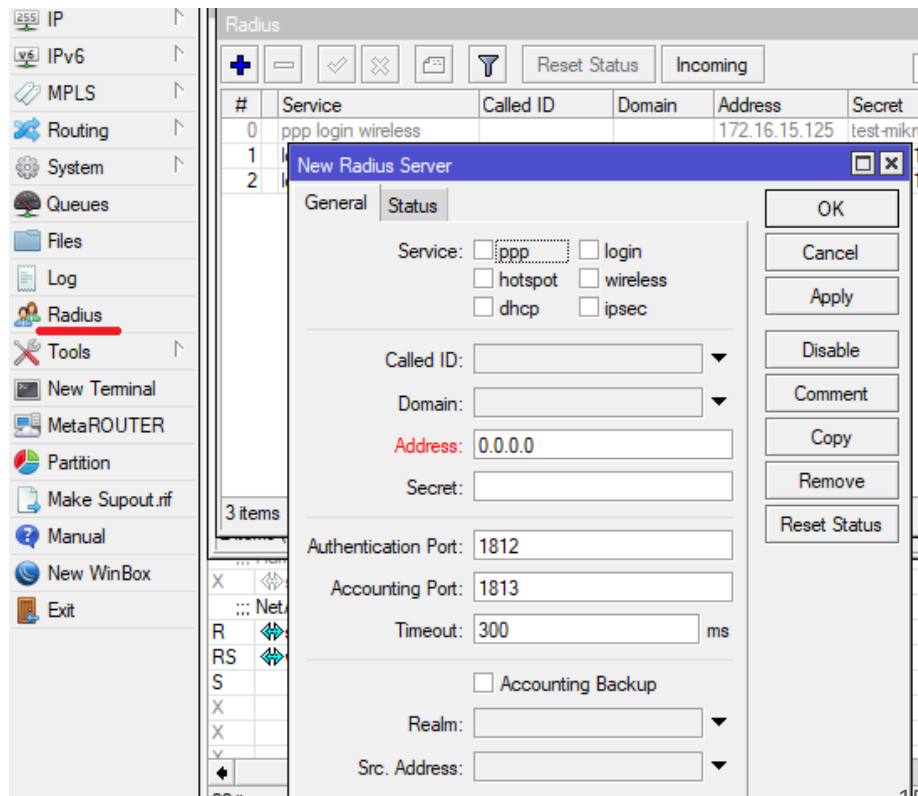
New Group dialog box. Fields: Name: group-test, Policies: local, telnet, ssh, ftp, reboot, read, write, policy, test, winbox, password, web, sniff, sensitive, api, romon, dude, tikapp. Buttons: OK, Cancel, Apply, Comment, Copy, Remove. Skin: default.

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



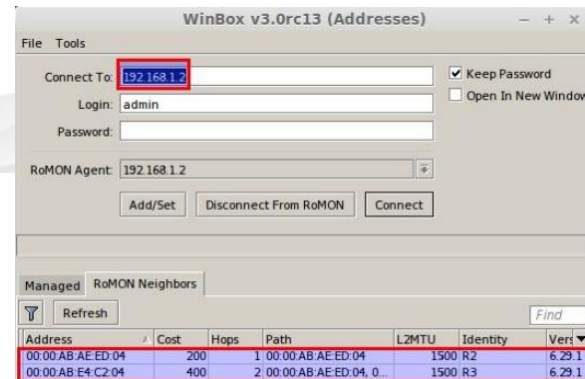
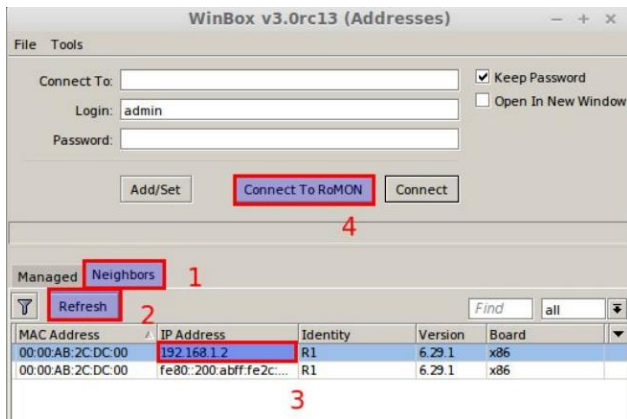
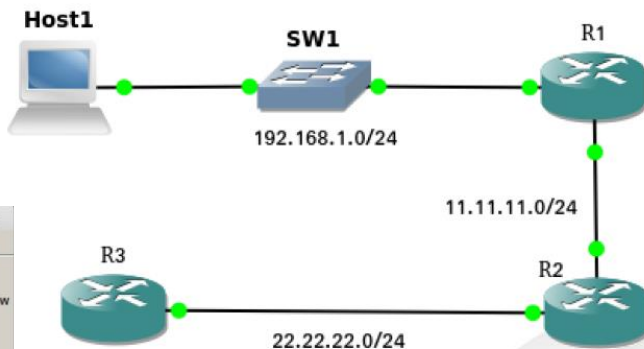
А Вы используете RoMON?

"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 BCE устройства

```
/ip kid-control add name=kid1 fri=7h-22h mon="" sat=6h-22h sun="" \
```

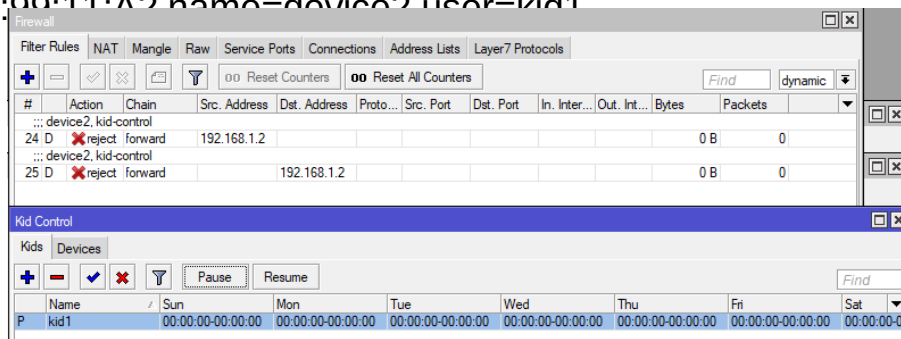
```
thu="" time-rate-limited="" tue="" wed="" rate-limit=10k time-rate-limited=0s-0s
```

```
/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/>

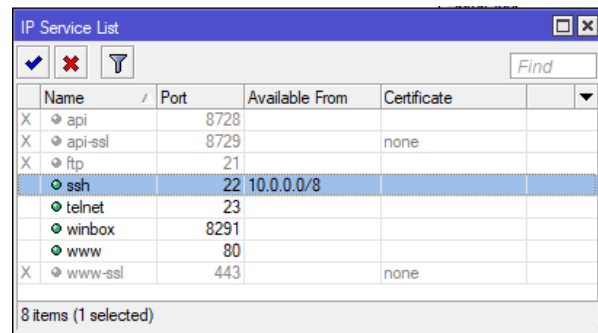
<http://asp24.com.ua/blog/virtualnaja-mashina-metarouter-i-zapusk-openwrt-na-marshrutizatorah-mikrotik/>

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



	Name	Port	Available From	Certificate
X	api	8728		
X	api-ssl	8729		none
X	ftp	21		
	ssh	22	10.0.0.0/8	
	telnet	23		
	winbox	8291		
	www	80		
X	www-ssl	443		none

8 items (1 selected)

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/>

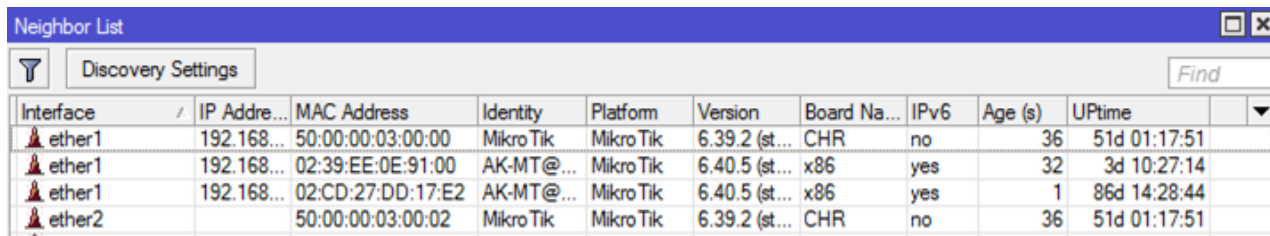
/interface bridge filter

```
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
```



Interface	IP Address	MAC Address	Identity	Platform	Version	Board Name	IPv6	Age (s)	Uptime
ether1	192.168...	50:00:00:03:00:00	MikroTik	MikroTik	6.39.2 (st...	CHR	no	36	51d 01:17:51
ether1	192.168...	02:39:EE:0E:91:00	AK-MT@...	MikroTik	6.40.5 (st...	x86	yes	32	3d 10:27:14
ether1	192.168...	02:CD:27:DD:17:E2	AK-MT@...	MikroTik	6.40.5 (st...	x86	yes	1	86d 14:28:44
ether2		50:00:00:03:00:02	MikroTik	MikroTik	6.39.2 (st...	CHR	no	36	51d 01:17:51

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?

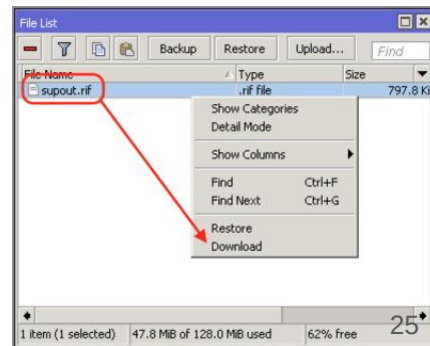
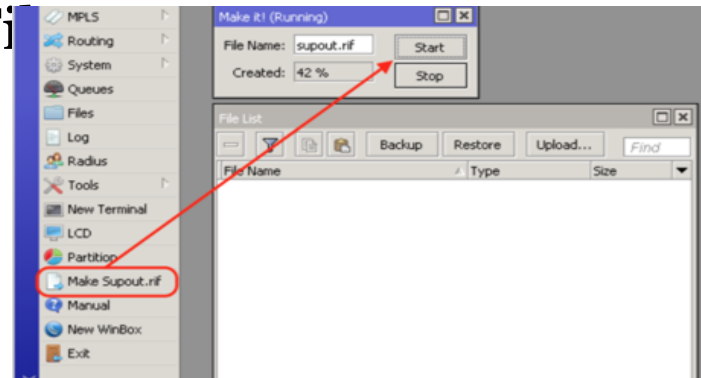
Support Output File

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, интернет не работает?

Support Output File

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

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