

The logo for MicroTik, featuring the word "Micro" in a stylized, italicized font with a crescent-like shape above the 'i', and "Tik" in a bold, blocky font with horizontal lines through the 'T' and 'i'.

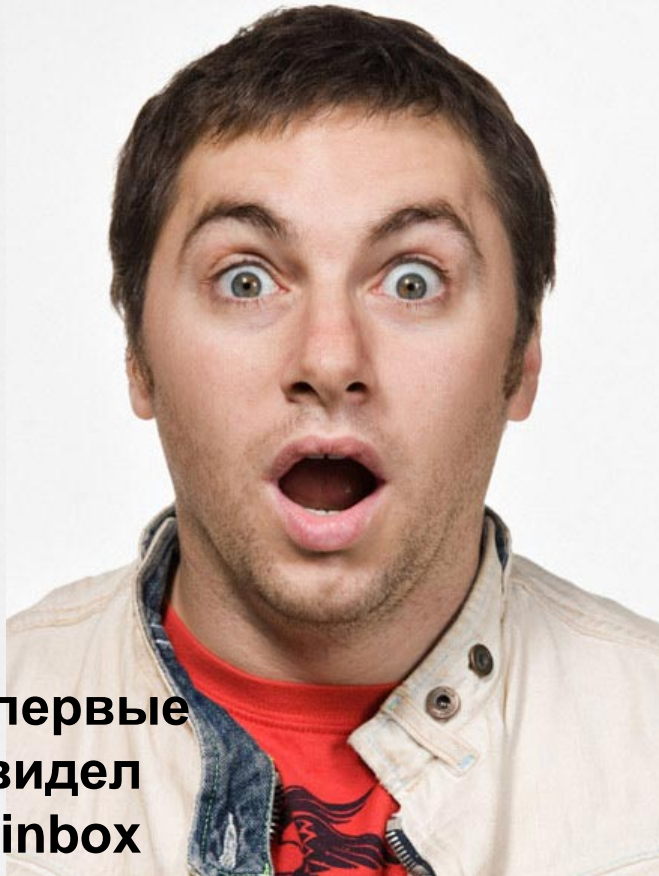
*Micro***Tik**

Начало работы
и рекомендации по настройке
на примерах из жизни.

Давайте знакомиться:

- o **Александр Романов**, Нижний Новгород
- o **8 лет** работы в маленьких и больших провайдерах в отделе широкополосного доступа
- o **МТСНА, МТСРЕ**
- o **Telegram:** *@moneron*
- o **Канал:** https://telegram.me/mikrotik_rus

Первое знакомство с Mikrotik

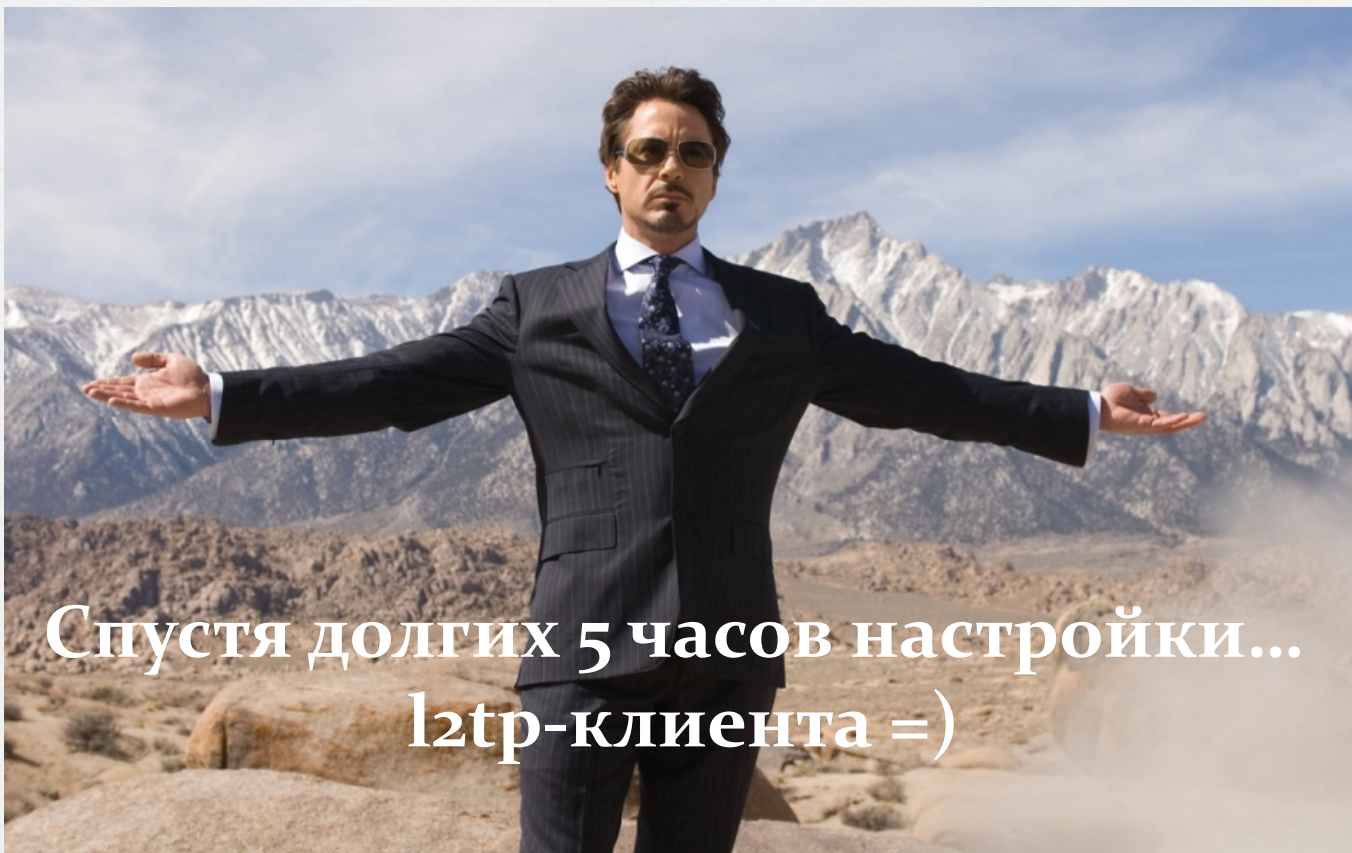


**Впервые
увидел
Winbox**



**Через три
часа
настройки**

Первое знакомство с Mikrotik



Спустя долгих 5 часов настройки...
l2tp-клиента =)

О чём пойдёт речь?

- o Первоначальные настройки безопасности
- o Принципы работы фаервола на примере конфигурации по умолчанию
- o Как облегчить жизнь самому себе? (Полезные советы и Best Practice)
- o Командная строка – это просто

Безопасность в *blank*-конфигурации:

1. Стандартный пользователь *admin* без пароля
2. *Neighbor Discovery* на всех интерфейсах
3. *MAC-server* на всех интерфейсах
4. *Firewall* выключен

Безопасность в *default*-конфигурации:

1. Стандартный пользователь *admin* без пароля
2. *Neighbor Discovery* на *ether1* выключен
3. *MAC-server* на *ether1* выключен
4. *Firewall* запрещает подключения с *ether1*

Создание пользователя с другим именем и отключение admin

The screenshot displays the Mikrotik WinBox interface. On the left, the 'System' menu is highlighted with a red circle, and a red arrow points to the 'Users' option at the bottom of the menu. In the main window, the 'User List' tab is active, showing a table with one user: 'admin' in the 'full' group, last logged in on 'Jan/02/1970 00:47'. A red plus sign icon is highlighted with a red circle, and a red arrow points to it. A 'New User' dialog box is open in the foreground, with the following fields:

- Name: nickname
- Group: full
- Allowed Address: 192.168.77.16/28, 78.95.16.1, 10.55.0.0/16 (highlighted with a blue box)
- Last Logged In: (empty)
- Password: (masked with asterisks)
- Confirm Password: (masked with asterisks)

Buttons in the dialog include OK, Cancel, Apply, Disable, Comment, Copy, and Remove. The 'enabled' checkbox is checked.

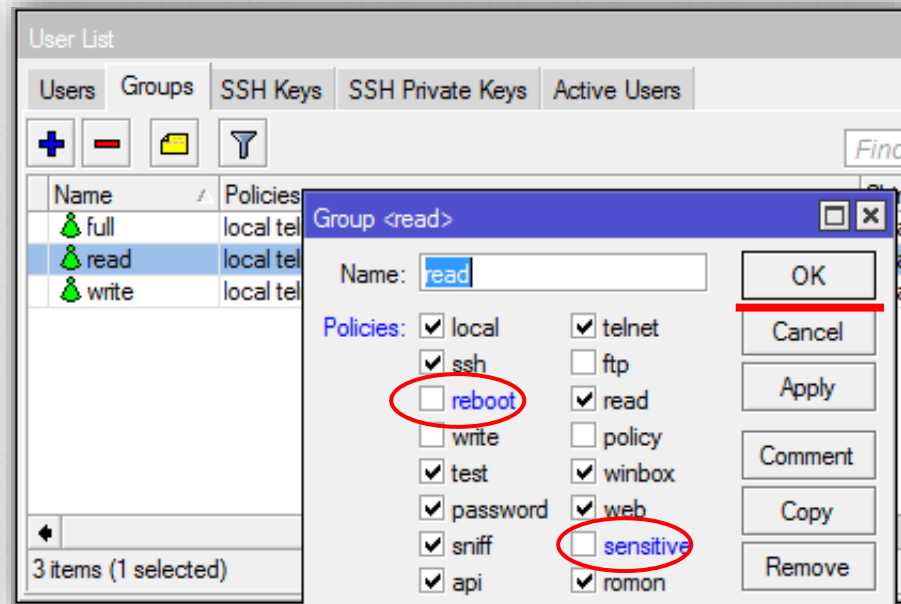
Создание пользователя

- o `/user add address=192.168.77.16/28, 78.95.16.1/32,10.55.0.0/16 group=full name=nickname password=MySuperP@$$`
Теперь пользователя **admin** можно отключать либо удалять.
- o Указание разрешённых ip-адресов для пользователя не обязательно, но оно существенно повысит безопасность.

Группа read и её возможности

- По умолчанию, в группе read включено **reboot** и **sensitive** policies. Чтобы не доставляло неприятностей, отключаем.

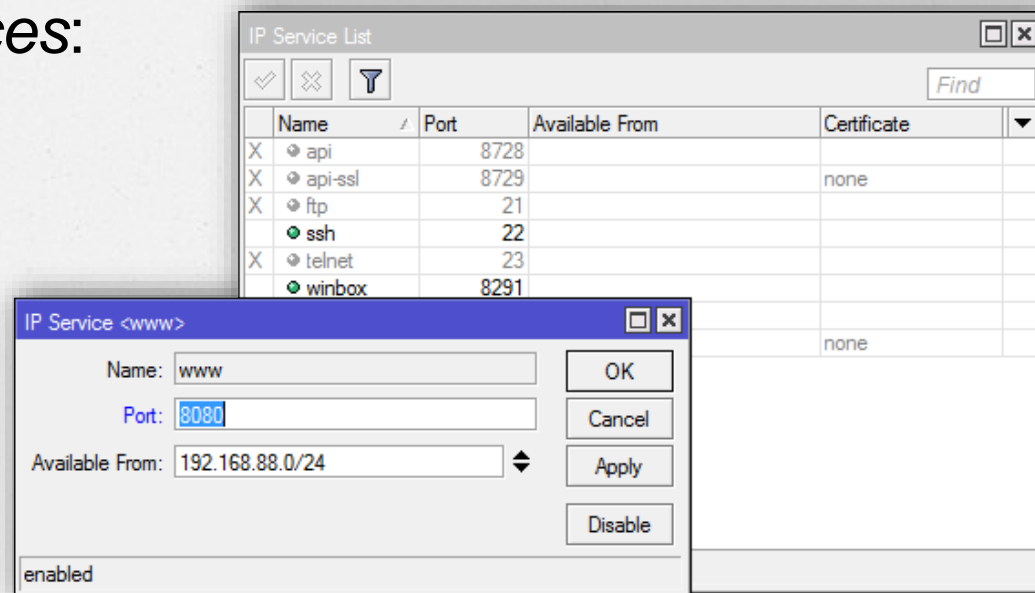
System – Users:



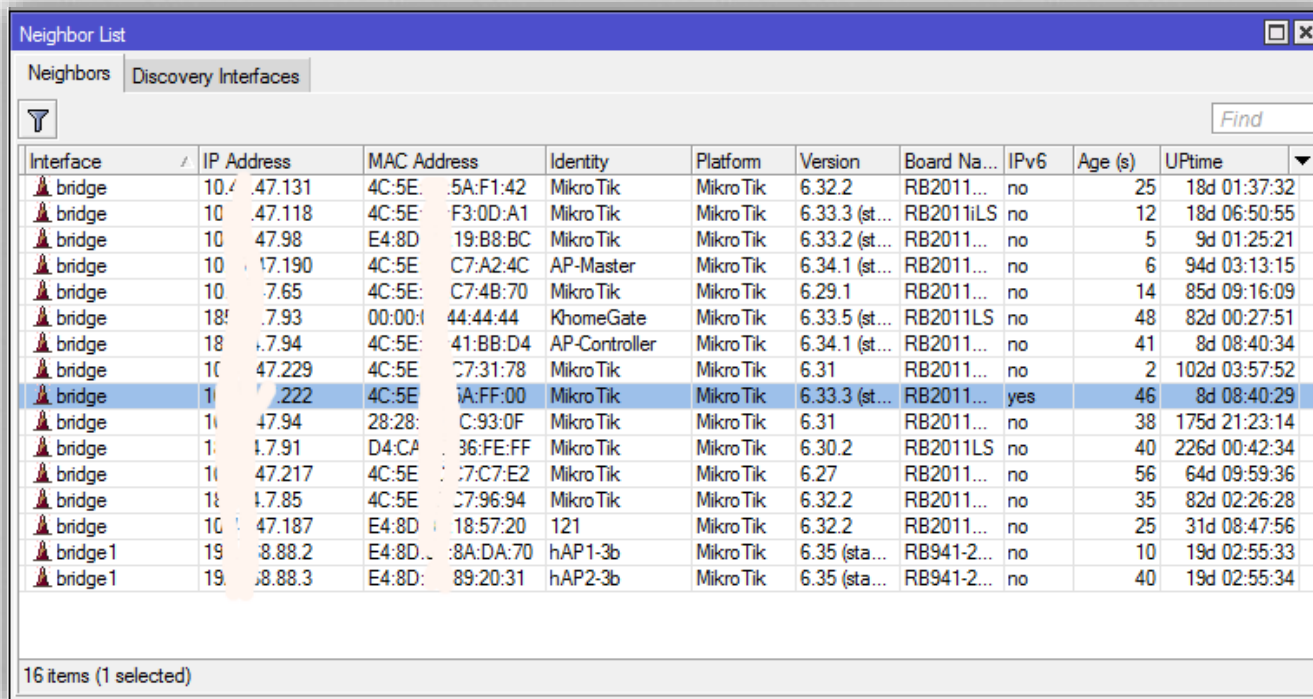
Сервисы:

Запущенные сервисы создают дополнительные уязвимости. Отключите ненужные сервисы, а необходимые также можно ограничить списком разрешённых адресов и изменить стандартный порт подключения.

IP-Services:



Пример с живой сети:



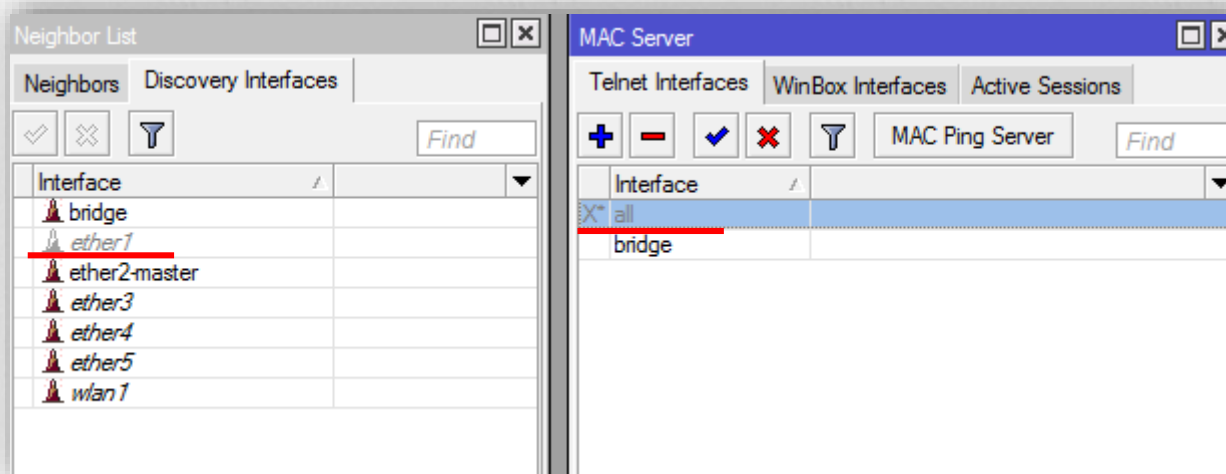
Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6	Age (s)	Uptime
bridge	10.4.47.131	4C:5E:5A:F1:42	Mikro Tik	Mikro Tik	6.32.2	RB2011...	no	25	18d 01:37:32
bridge	10.47.118	4C:5E:F3:0D:A1	Mikro Tik	Mikro Tik	6.33.3 (st...	RB2011iLS	no	12	18d 06:50:55
bridge	10.47.98	E4:8D19:B8:BC	Mikro Tik	Mikro Tik	6.33.2 (st...	RB2011...	no	5	9d 01:25:21
bridge	10.47.190	4C:5E:C7:A2:4C	AP-Master	Mikro Tik	6.34.1 (st...	RB2011...	no	6	94d 03:13:15
bridge	10.47.765	4C:5E:C7:4B:70	Mikro Tik	Mikro Tik	6.29.1	RB2011...	no	14	85d 09:16:09
bridge	18.47.793	00:00:14:44:44	KhomeGate	Mikro Tik	6.33.5 (st...	RB2011LS	no	48	82d 00:27:51
bridge	18.47.794	4C:5E:41:BB:D4	AP-Controller	Mikro Tik	6.34.1 (st...	RB2011...	no	41	8d 08:40:34
bridge	10.47.229	4C:5E:C7:31:78	Mikro Tik	Mikro Tik	6.31	RB2011...	no	2	102d 03:57:52
bridge	10.47.222	4C:5E:1A:FF:00	Mikro Tik	Mikro Tik	6.33.3 (st...	RB2011...	yes	46	8d 08:40:29
bridge	10.47.94	28:28:C:93:0F	Mikro Tik	Mikro Tik	6.31	RB2011...	no	38	175d 21:23:14
bridge	10.47.91	D4:CA:36:FE:FF	Mikro Tik	Mikro Tik	6.30.2	RB2011LS	no	40	226d 00:42:34
bridge	10.47.217	4C:5E:17:C7:E2	Mikro Tik	Mikro Tik	6.27	RB2011...	no	56	64d 09:59:36
bridge	10.47.85	4C:5E:C7:96:94	Mikro Tik	Mikro Tik	6.32.2	RB2011...	no	35	82d 02:26:28
bridge	10.47.187	E4:8D18:57:20	121	Mikro Tik	6.32.2	RB2011...	no	25	31d 08:47:56
bridge1	19.48.88.2	E4:8D:8A:DA:70	hAP1-3b	Mikro Tik	6.35 (sta...	RB941-2...	no	10	19d 02:55:33
bridge1	19.48.88.3	E4:8D:89:20:31	hAP2-3b	Mikro Tik	6.35 (sta...	RB941-2...	no	40	19d 02:55:34

16 items (1 selected)

- К некоторым роутерам удалось подключиться по MAC-telnet и Winbox

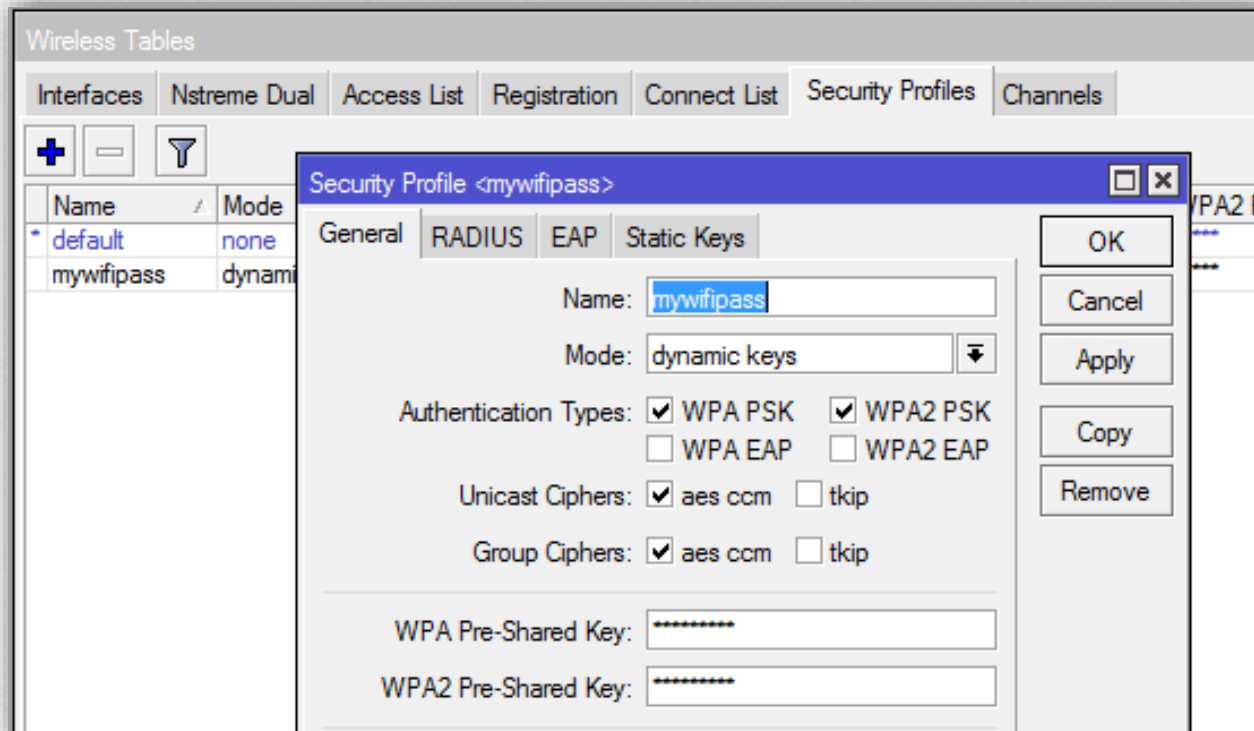
Чтобы не стать жертвой атаки:

- Отключите Neighbors Discovery и MAC Server на внешних и неиспользуемых интерфейсах (*IP-Neighbors* и *Tools-MAC Server*).



Защита Wi-Fi

- По умолчанию открытая сеть.
- Для защиты необходимо создать профиль безопасности (*Wireless – security profiles*)



Защита Wi-Fi

The screenshot displays the Mikrotik WinBox configuration window for the wireless interface `wlan1`. The interface is configured as an `ap bridge` operating on the `2GHz-B/G/N` band with a `20/40MHz Ce` channel width. The SSID is `MikroTik-7CD55F` and the security profile is `mywifipass`. The `Default Forward` checkbox is checked, indicating that the interface is configured for security. The `Default Authenticate` checkbox is also checked, while `Hide SSID` is unchecked. The interface name `wlan1` and the `Security Profile` field are highlighted with red lines.

Interface <wlan1>

General | **Wireless** | HT | HT MCS | WDS | Nstreme | Status | Traffic

Mode: `ap bridge`

Band: `2GHz-B/G/N`

Channel Width: `20/40MHz Ce`

Frequency: `auto` MHz

SSID: `MikroTik-7CD55F`

Scan List: `default`

Wireless Protocol: `802.11`

Security Profile: `mywifipass`

WPS Mode: `push button`

Bridge Mode: `enabled`

VLAN Mode: `no tag`

VLAN ID: `1`

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

Buttons: OK, Cancel, Apply, Disable, Comment, Advanced Mode, Torch, WPS Accept, Scan..., Freq. Usage..., Align..., Sniff..., Snooper..., Reset Configuration

Рассматриваемые вопросы

- Первоначальные настройки безопасности
- Принципы работы фаервола на примере конфигурации по умолчанию
- Как облегчить жизнь самому себе? (рекомендации по настройке)
- Командная строка – это просто
- Полезные советы и Best Practice

Firewall – что это?

Фаервол, сетевой экран — это комплекс аппаратных и программных средств в компьютерной сети, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

©Wikipedia



Firewall в конфигурации по умолчанию

The screenshot shows the Mikrotik WinBox Firewall configuration window. The 'Filter Rules' tab is active. The table below lists the default rules. Two rules are highlighted with red boxes: rule 3, 'defconf: drop all from WAN', and rule 7, 'defconf: drop all from WAN not DSTNATed'. Both are set to 'drop' action on the 'input' chain.

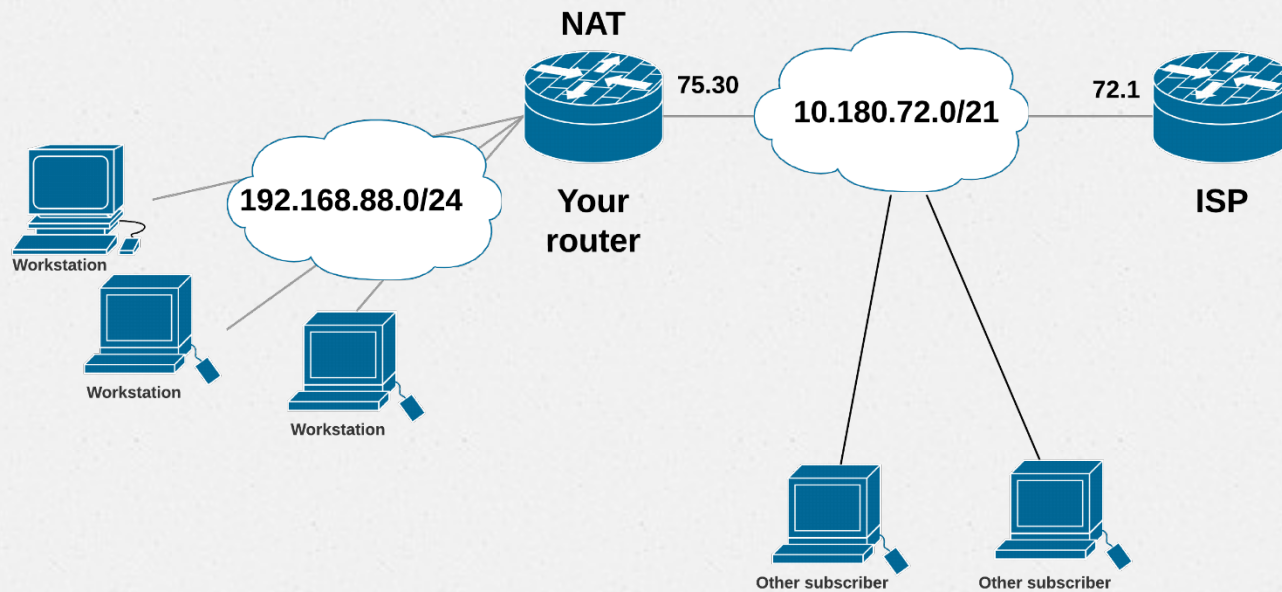
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
::: special dummy rule to show fasttrack counters											
0	D	✓ acc...	forward							0 B	0
::: defconf: accept ICMP											
1		✓ acc...	input		1 (ic...					0 B	0
::: defconf: accept established,related											
2		✓ acc...	input							0 B	0
::: defconf: drop all from WAN											
3		✗ drop	input					ether1		0 B	0
::: defconf: fasttrack											
4		▶▶ fastt...	forward							0 B	0
::: defconf: accept established,related											
5		✓ acc...	forward							0 B	0
::: defconf: drop invalid											
6		✗ drop	forward							0 B	0
::: defconf: drop all from WAN not DSTNATed											
7		✗ drop	forward					ether1		0 B	0

8 items (1 selected)

Firewall в конфигурации по умолчанию

```
/ip firewall filter
add action=accept chain=input comment="defconf: accept ICMP" protocol=icmp
add action=accept chain=input comment="defconf: accept established,related" \
connection-state=established,related
add action=drop chain=input comment="defconf: drop all from WAN" \
in-interface=ether1
add action=fasttrack-connection chain=forward comment="defconf: fasttrack" \
connection-state=established,related
add action=accept chain=forward comment="defconf: accept established,related" \
connection-state=established,related
add action=drop chain=forward comment="defconf: drop invalid" \
connection-state=invalid
add action=drop chain=forward comment=\
"defconf: drop all from WAN not DSTNATed" connection-nat-state=!dstnat \
connection-state=new in-interface=ether1
[nickname@MikroTik] > |
```

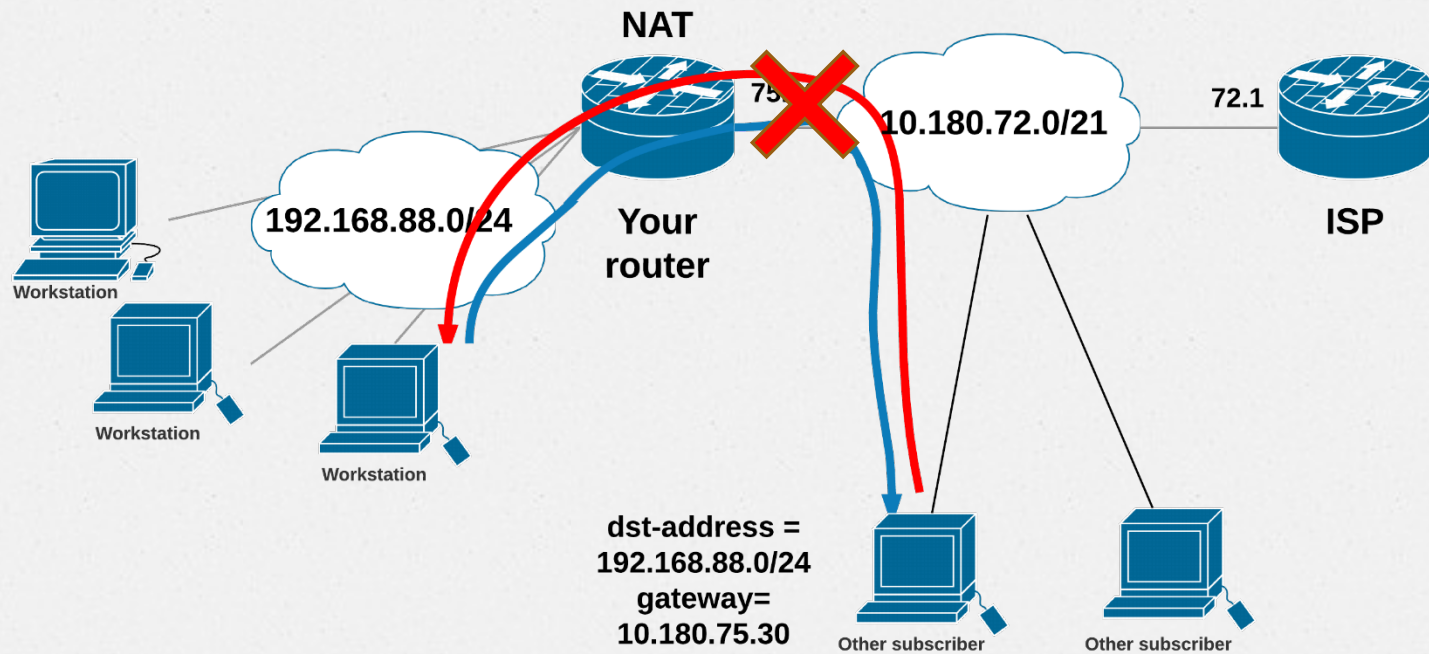
Типичная ситуация:



Защищена ли домашняя сеть
от несанкционированного
доступа?

Нет!

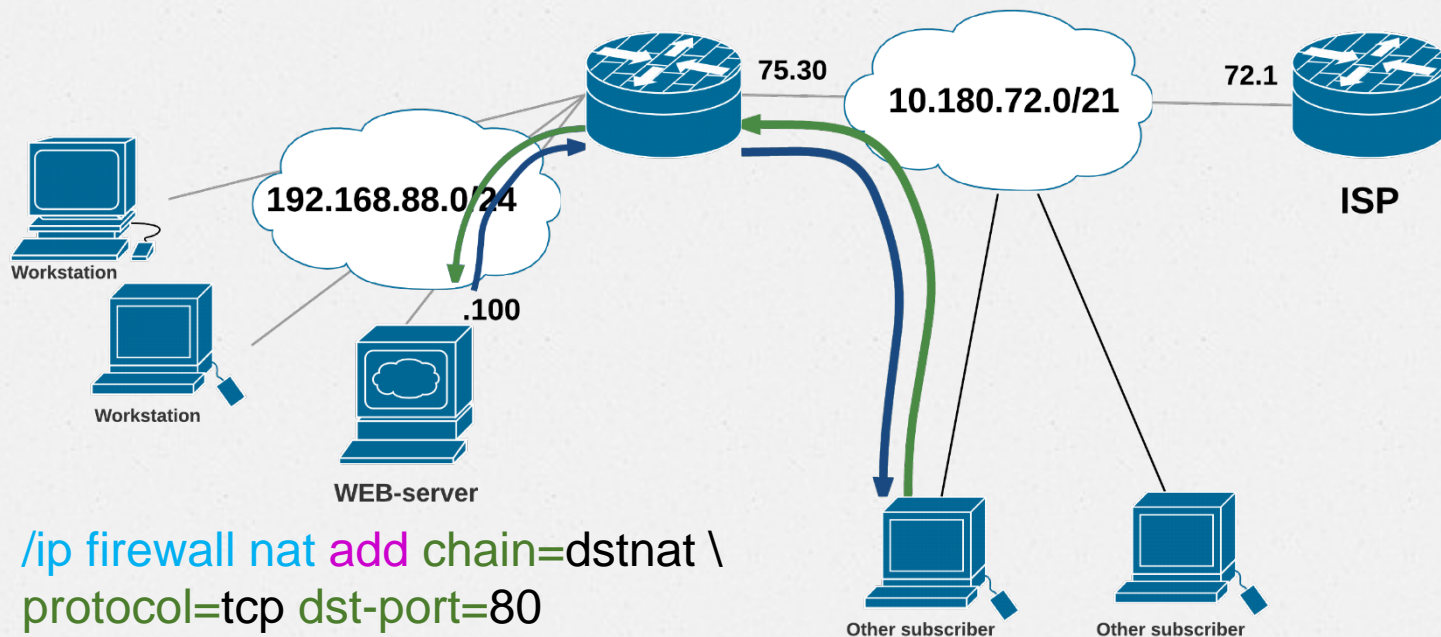
Маршрут в подсеть за NAT



```
add action=drop chain=forward comment=\  
"defconf: drop all from WAN not DSTNATED" connection-nat-state=!dstnat \  
connection-state=new in-interface=ether1
```

Проброс портов

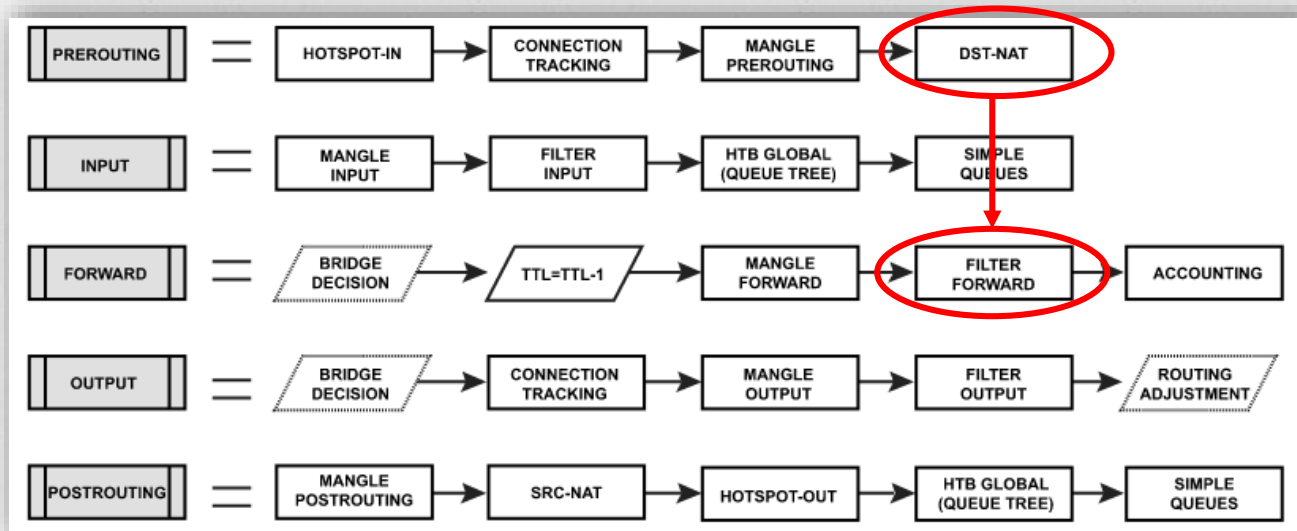
in-interface: ether1
tcp:80 dst-nat
to 192.168.88.100



```
/ip firewall nat add chain=dstnat \  
protocol=tcp dst-port=80  
action=dst-nat  
to-address=192.168.88.100
```

Трафик: input или forward?

Packet Flow Diagram v6



Задача:

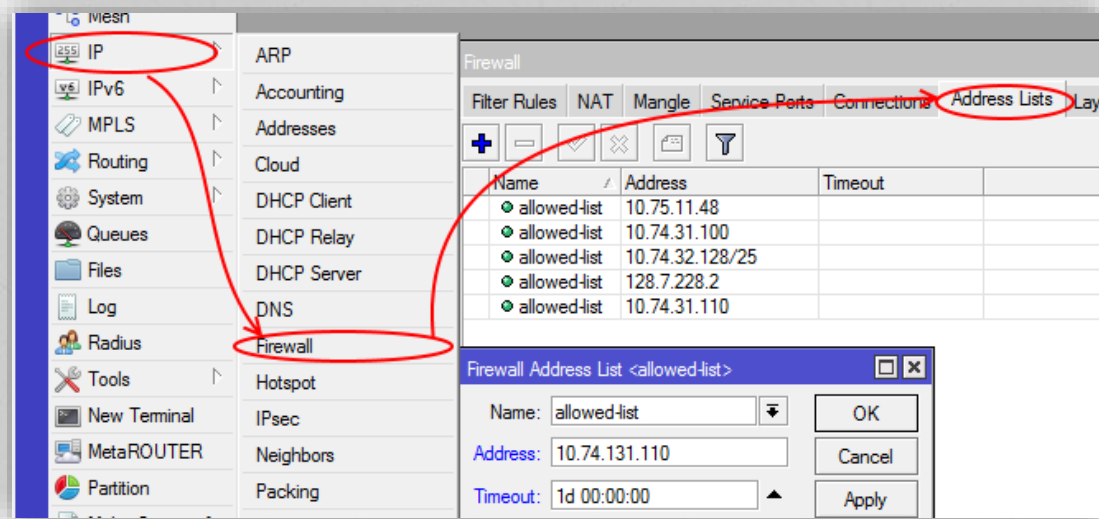
разрешить 5 IP-адресам доступ на этот веб-сервер.

Решение:

Сделаем ~~5 правил~~ одно правило со списком адресов

Адрес-листы: *must use!*

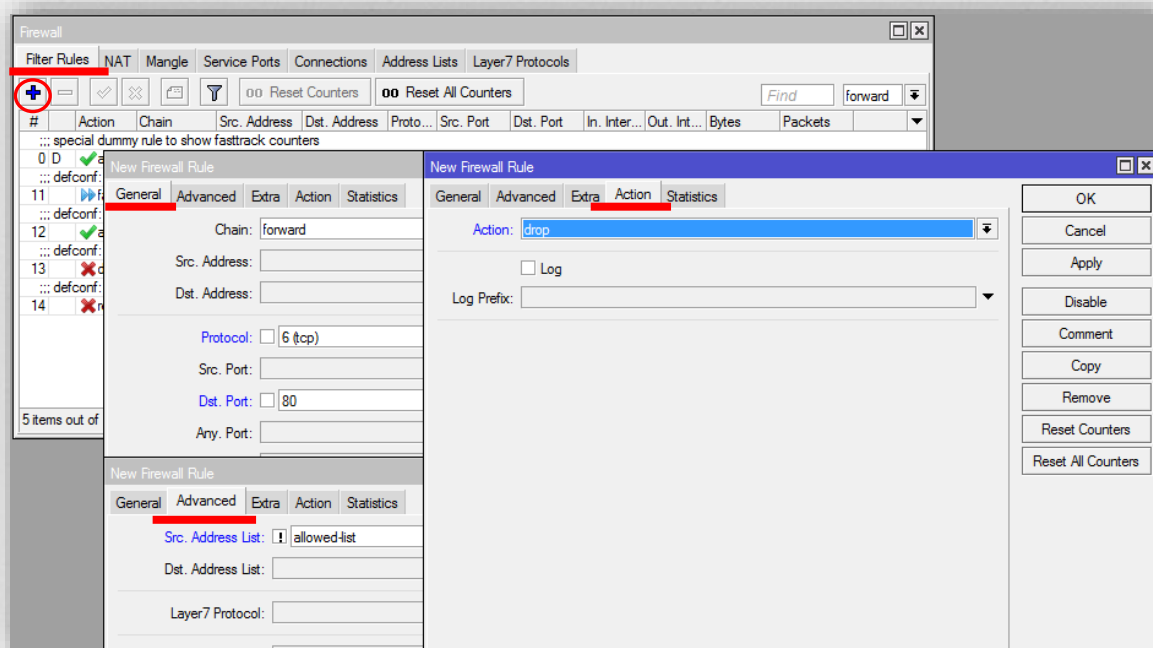
- o Легко управляются
- o Сокращают количество правил в firewall
- o Можно создавать динамические записи



```
/ip firewall address-list add address=10.75.11.48 list=allowed-list
```


Решение задачи

Теперь, когда есть список разрешённых хостов, добавляем правило firewall.



```
/ip firewall filter add chain=forward connection-state=new \  
src-address-list=!allowed-list protocol=tcp dst-port=80 \  
action=drop comment="drop not-in-list to webserver"
```

Защита от перебора паролей

/ip firewall filter

```
add chain=input protocol=tcp dst-port=22 src-address-list=ssh_blacklist action=drop \  
comment="drop ssh brute forcers" disabled=no
```

```
add chain=input protocol=tcp dst-port=22 connection-state=new \  
src-address-list=ssh_stage3 action=add-src-to-address-list address-list=ssh_blacklist \  
address-list-timeout=10d disabled=no
```

```
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_stage3 \  
address-list-timeout=1m disabled=no
```


```
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 disabled=no
```

```
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 disabled=no
```

```
add chain=input protocol=tcp dst-port=22 action=accept disabled=no
```

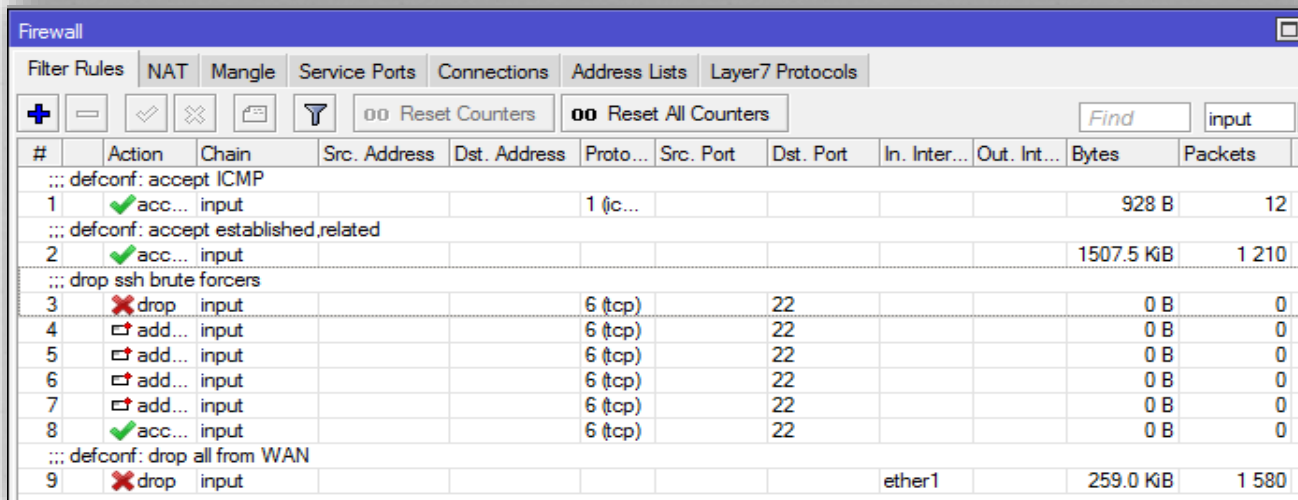
http://wiki.mikrotik.com/wiki/Bruteforce_login_prevention

Защита от перебора паролей



Firewall configuration window showing Filter Rules. The table below lists the rules:

#	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...					928 B	12
::: defconf: accept established,related											
2	✓ acc...	input								1507.5 KiB	1 210
::: defconf: drop all from WAN											
3	✗ drop	input						ether1		258.2 KiB	1 575
::: drop ssh brute forcers											
9	✗ drop	input			6 (tcp)		22			0 B	0
10	➡ add...	input			6 (tcp)		22			0 B	0
11	➡ add...	input			6 (tcp)		22			0 B	0
12	➡ add...	input			6 (tcp)		22			0 B	0
13	➡ add...	input			6 (tcp)		22			0 B	0
14	✓ acc...	input			6 (tcp)		22			0 B	0



Firewall configuration window showing Filter Rules after reordering. The table below lists the rules:

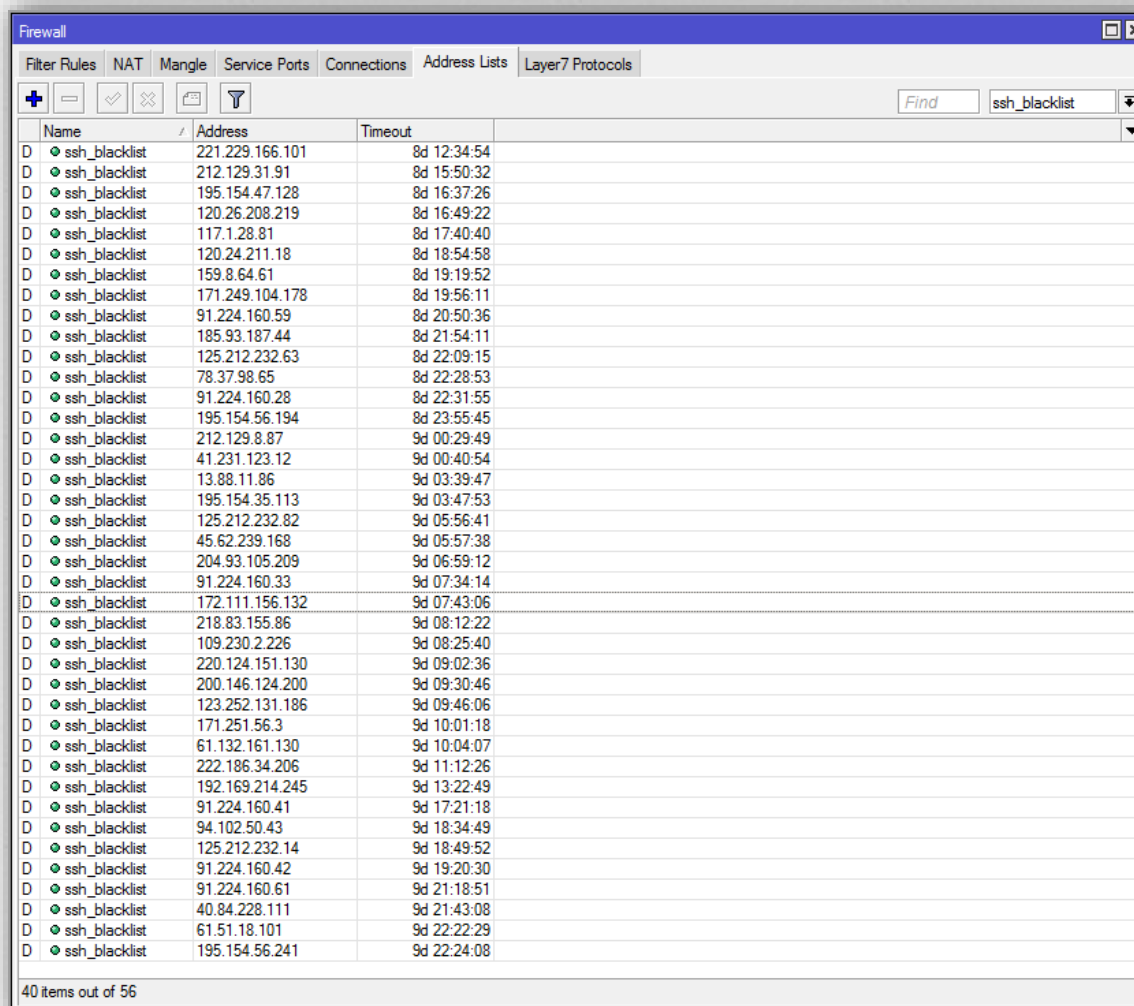
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
::: defconf: accept ICMP											
1	✓ acc...	input			1 (ic...					928 B	12
::: defconf: accept established,related											
2	✓ acc...	input								1507.5 KiB	1 210
::: drop ssh brute forcers											
3	✗ drop	input			6 (tcp)		22			0 B	0
4	➡ add...	input			6 (tcp)		22			0 B	0
5	➡ add...	input			6 (tcp)		22			0 B	0
6	➡ add...	input			6 (tcp)		22			0 B	0
7	➡ add...	input			6 (tcp)		22			0 B	0
8	✓ acc...	input			6 (tcp)		22			0 B	0
::: defconf: drop all from WAN											
9	✗ drop	input						ether1		259.0 KiB	1 580

Работает ли это?

Uptime:

1d 12:02:21

40 адресов!



The screenshot shows the Mikrotik WinBox Firewall configuration interface, specifically the 'Address Lists' tab. The search filter is set to 'ssh_blacklist'. The table below lists 40 items, each with a name, address, and timeout.

Name	Address	Timeout
D ssh_blacklist	221.229.166.101	8d 12:34:54
D ssh_blacklist	212.129.31.91	8d 15:50:32
D ssh_blacklist	195.154.47.128	8d 16:37:26
D ssh_blacklist	120.26.208.219	8d 16:49:22
D ssh_blacklist	117.1.28.81	8d 17:40:40
D ssh_blacklist	120.24.211.18	8d 18:54:58
D ssh_blacklist	159.8.64.61	8d 19:19:52
D ssh_blacklist	171.249.104.178	8d 19:56:11
D ssh_blacklist	91.224.160.59	8d 20:50:36
D ssh_blacklist	185.93.187.44	8d 21:54:11
D ssh_blacklist	125.212.232.63	8d 22:09:15
D ssh_blacklist	78.37.98.65	8d 22:28:53
D ssh_blacklist	91.224.160.28	8d 22:31:55
D ssh_blacklist	195.154.56.194	8d 23:55:45
D ssh_blacklist	212.129.8.87	9d 00:29:49
D ssh_blacklist	41.231.123.12	9d 00:40:54
D ssh_blacklist	13.88.11.86	9d 03:39:47
D ssh_blacklist	195.154.35.113	9d 03:47:53
D ssh_blacklist	125.212.232.82	9d 05:56:41
D ssh_blacklist	45.62.239.168	9d 05:57:38
D ssh_blacklist	204.93.105.209	9d 06:59:12
D ssh_blacklist	91.224.160.33	9d 07:34:14
D ssh_blacklist	172.111.156.132	9d 07:43:06
D ssh_blacklist	218.83.155.86	9d 08:12:22
D ssh_blacklist	109.230.2.226	9d 08:25:40
D ssh_blacklist	220.124.151.130	9d 09:02:36
D ssh_blacklist	200.146.124.200	9d 09:30:46
D ssh_blacklist	123.252.131.186	9d 09:46:06
D ssh_blacklist	171.251.56.3	9d 10:01:18
D ssh_blacklist	61.132.161.130	9d 10:04:07
D ssh_blacklist	222.186.34.206	9d 11:12:26
D ssh_blacklist	192.169.214.245	9d 13:22:49
D ssh_blacklist	91.224.160.41	9d 17:21:18
D ssh_blacklist	94.102.50.43	9d 18:34:49
D ssh_blacklist	125.212.232.14	9d 18:49:52
D ssh_blacklist	91.224.160.42	9d 19:20:30
D ssh_blacklist	91.224.160.61	9d 21:18:51
D ssh_blacklist	40.84.228.111	9d 21:43:08
D ssh_blacklist	61.51.18.101	9d 22:22:29
D ssh_blacklist	195.154.56.241	9d 22:24:08

40 items out of 56

Блокировка сайтов в *firewall*

Пример: хотим заблокировать vk.com

- o 1 попытка (плохая):

```
/ip firewall filter add chain=forward protocol=tcp \  
src-address=192.168.88.0/24 dst-address=87.240.143.244 \  
action=drop
```

- o 2 попытка (чуть лучше):

```
/ip firewall filter add chain=forward protocol=tcp \  
src-address=192.168.88.0/24 content="vk.com" action=drop
```

- o 3 попытка (чуть лучше, чем 2я):

```
/ip firewall filter add chain=forward protocol=tcp \  
src-address=192.168.88.0/24 content="Host: vk.com" \  
action=drop
```

Недостаток этих примеров – **долгий таймаут**

Блокировка сайтов в *firewall*

Пример: хотим заблокировать vk.com (стр.2)

Action=drop ничего не сообщает отправителю.

Action=reject сбрасывает соединение и сообщает об этом отправителю.

o Попытка 4 (удачная):

```
/ip firewall filter add chain=forward protocol=tcp \  
src-address=192.168.88.0/24 content="vk.com" \  
action=reject reject-with=tcp-reset
```

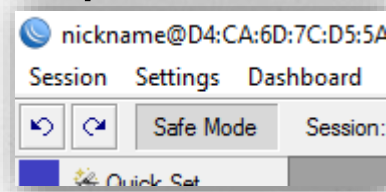
o Попытка 5 (похожа, тоже удачная):

```
/ip firewall filter add chain=forward protocol=tcp \  
src-address=192.168.88.0/24 content="Host: vk.com" \  
action=reject reject-with=tcp-reset
```

Как не потерять Mikrotik

Удалённая работа с Mikrotik'ом сопряжена с риском дисконнекта в следствие некорректных настроек. 2 способа избежать этого:

1. **Safe mode:** после дисконнекта откатывает роутер в состояние до нажатия кнопки. После выполнения настроек отжимаем кнопку обратно.



2. **COM-port:** непосредственный доступ к роутеру. Скорость порта 115200, чётность – нет, бит – 8, стоп-бит 1, контроля потока нет. Доступ есть всегда*.

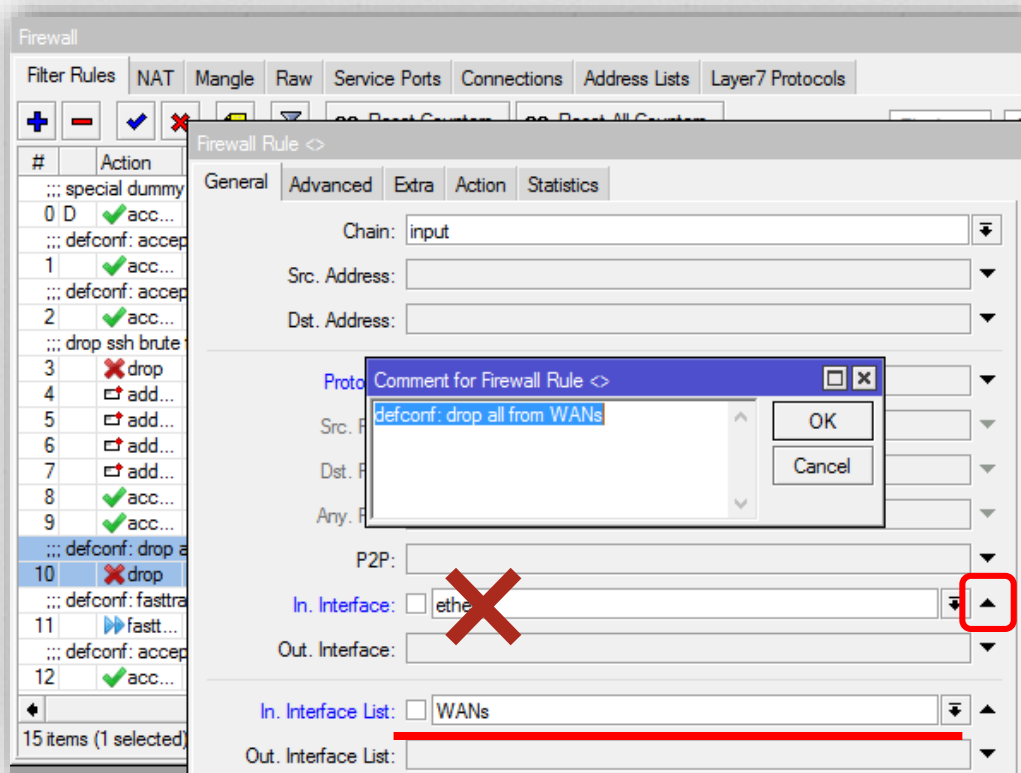
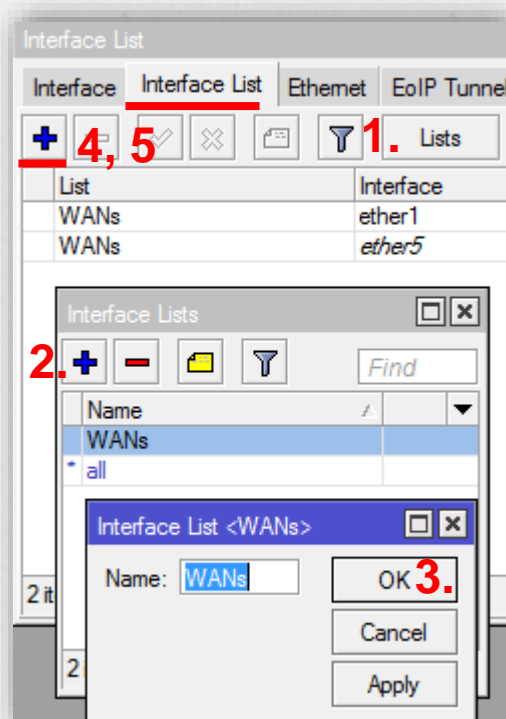
Что мы увидим в ближайшее время?

What's new in 6.36rc20 (2016-May-30 05:56):

- o *) firewall - added "/interface list" menu which allows to create list of interfaces which can be used as in/out-interface-list matcher in firewall;
- o *) firewall - allow to add domain name to address-lists (dynamic entries for resolved addresses will be added to specified list);

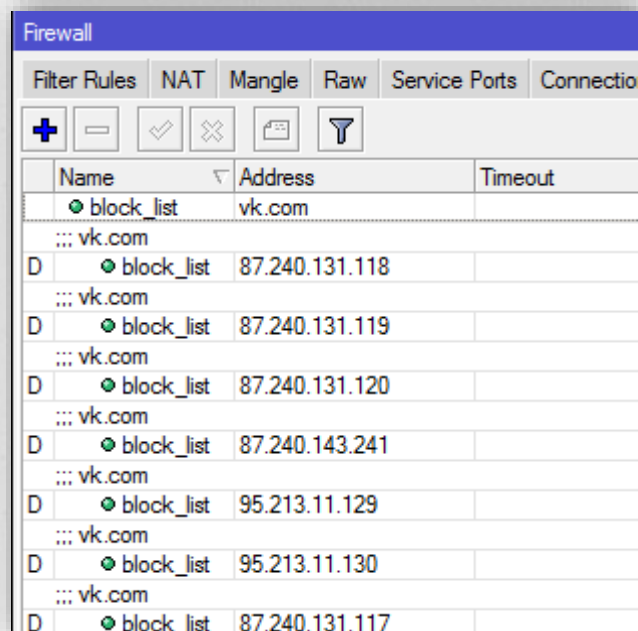
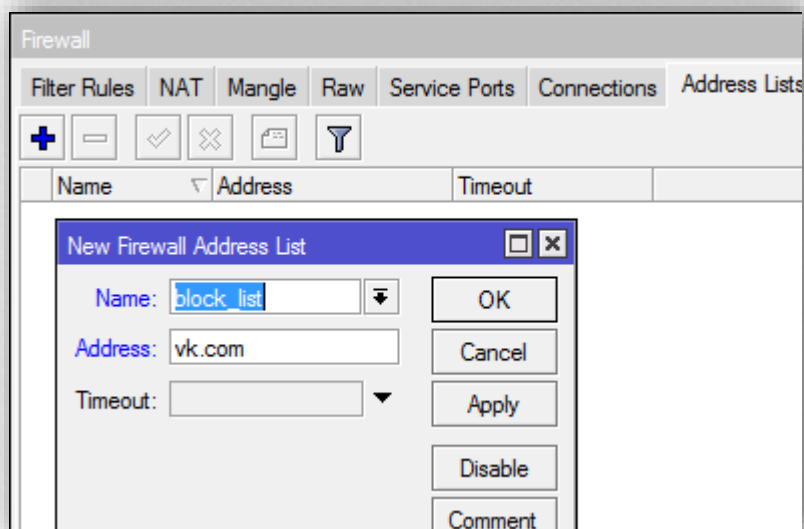
Список интерфейсов

- Одно правило будет работать для нескольких интерфейсов => нужно меньше правил!



Домены в списке адресов

- Если с доменом ассоциировано много ip-адресов – нужно вносить их все в список, чтобы управлять ими в фаерволе. Теперь можно добавлять домены:



Рассматриваемые вопросы

- Первоначальные настройки безопасности
- Принципы работы фаервола на примере конфигурации по умолчанию
- o Как облегчить жизнь самому себе? (Полезные советы и Best Practice)
- o Командная строка – это просто

Best practice *или упрости себе жизнь*

Часто простые вещи делают нашу жизнь проще, когда мы их используем. Несколько советов, которые найдены самыми разными способами: услышаны, придуманы, прочитаны.



Wi-Fi: в рамках закона

В каждой стране существует определённый законом порядок регистрации и использования передающей радиочастотной аппаратуры. Различные частоты и мощности передатчика, не подлежащие регистрации. Чтобы не идти в разрез с законом, выставляйте разрешённые параметры.



Wi-Fi: в рамках закона

Точки беспроводного радиодоступа ... подлежат регистрации в органах Роскомнадзора.

Исключение составляют:

- o Устройства ... беспроводной передачи данных **внутри закрытых помещений** в полосе **2400-2483,5 МГц** с максимальной ... излучаемой мощностью передатчика не более **100 мВт...**
- o Устройства ... беспроводной передачи данных **вне закрытых помещений** в полосе 2400 - 2483,5 МГц только при высоте установки ... **не более 10 м** от поверхности земли.

<https://35.rkn.gov.ru/directions/p1401/p1407/>

Wi-Fi: в рамках закона

- o Built-in wireless details <для **RB951G-2HnD**>

<band><power_per_chain><protocol><number_of_chains>

band

- o **2** - 2.4Ghz

power per chain

- o **H** - "High" - 23-24dBm at 6Mbps 802.11a; 24-27dBm at 6Mbps 802.11g

protocol

- o **n** - for cards with 802.11n support

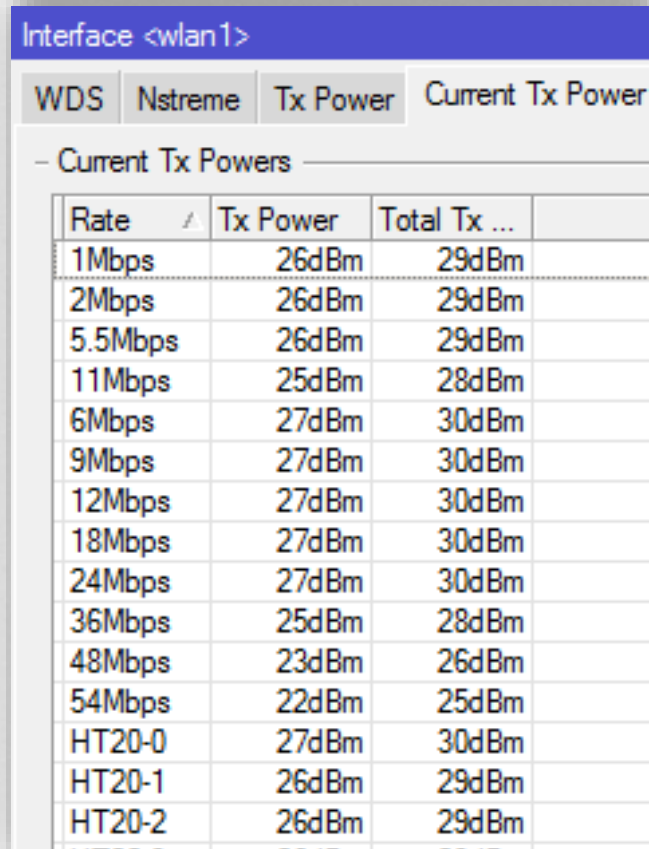
number_of_chains

- o **D** - dual chain

http://wiki.mikrotik.com/wiki/Manual:Product_Naming

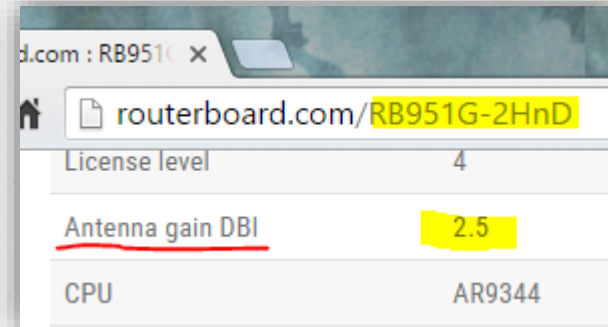
Wi-Fi: в рамках закона

По умолчанию:



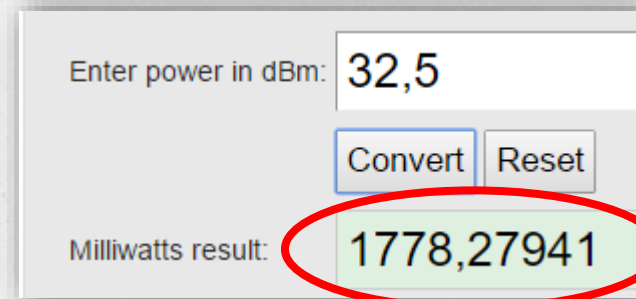
Rate	Tx Power	Total Tx ...
1Mbps	26dBm	29dBm
2Mbps	26dBm	29dBm
5.5Mbps	26dBm	29dBm
11Mbps	25dBm	28dBm
6Mbps	27dBm	30dBm
9Mbps	27dBm	30dBm
12Mbps	27dBm	30dBm
18Mbps	27dBm	30dBm
24Mbps	27dBm	30dBm
36Mbps	25dBm	28dBm
48Mbps	23dBm	26dBm
54Mbps	22dBm	25dBm
HT20-0	27dBm	30dBm
HT20-1	26dBm	29dBm
HT20-2	26dBm	29dBm

Коэф. усиления:



License level	4
<u>Antenna gain DBI</u>	2.5
CPU	AR9344

Общая мощность
равна $\text{dBm} + \text{dBi} =$
 $32,5 \text{ dBm} =$



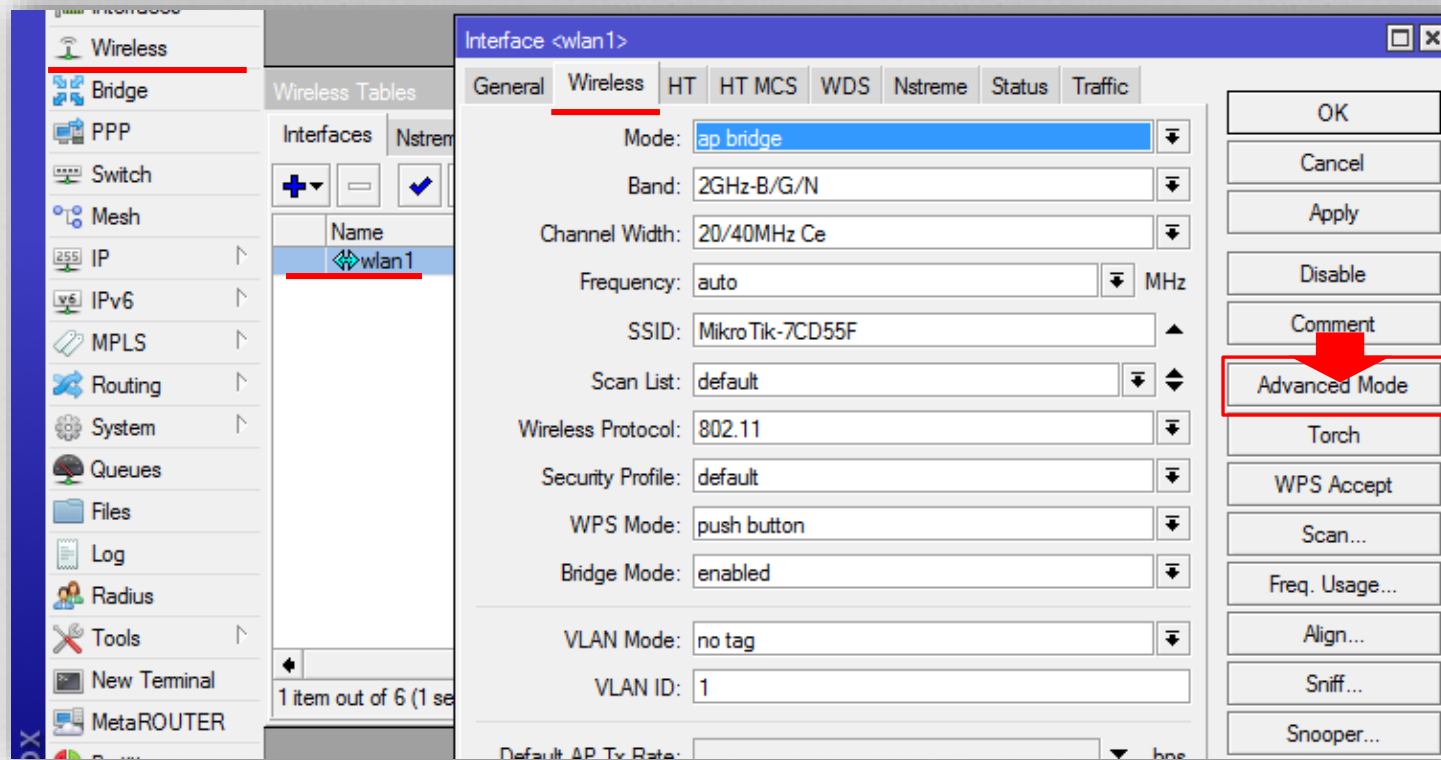
Enter power in dBm: 32,5

Convert Reset

Milliwatts result: 1778,27941



Wi-Fi: в рамках закона



Wi-Fi: в рамках закона

Interface <wlan1>

General Wireless Data Rates Advanced HT HT MCS WDS ...

Mode: ap bridge

Band: 2GHz-only-N

Channel Width: 20/40MHz Ce

Frequency: auto MHz

SSID: 951G

Radio Name: Tester

Scan List: default

Wireless Protocol: 802.11

Security Profile: mywifipass

WPS Mode: push button

Frequency Mode: regulatory-domain

Country: russia

Antenna Gain: 2 dBi

DFS Mode: none

WMM Support: disabled

Bridge Mode: enabled

VLAN Mode: no tag

VLAN ID: 1

OK
Cancel
Apply
Disable
Comment
Simple Mode
Torch
WPS Accept
Scan...
Freq. Usage...
Align...
Sniff...
Snooper...
Reset Configuration

Interface <wlan1>

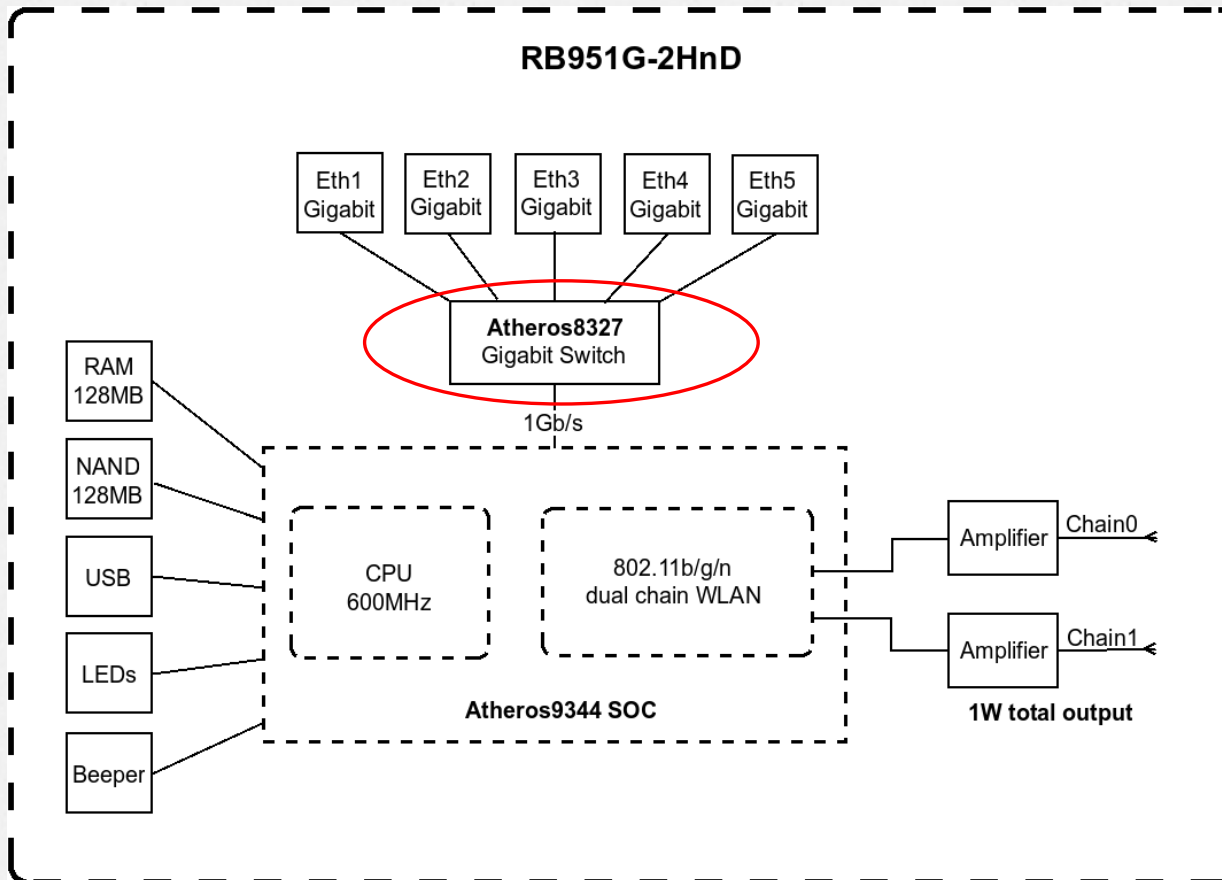
WDS Nstreme Tx Power Current Tx Power

- Current Tx Powers -

Rate	Tx Power	Total Tx ...
1Mbps	15dBm	18dBm
2Mbps	15dBm	18dBm
5.5Mbps	15dBm	18dBm
11Mbps	15dBm	18dBm
6Mbps	15dBm	18dBm
9Mbps	15dBm	18dBm
12Mbps	15dBm	18dBm
18Mbps	15dBm	18dBm
24Mbps	15dBm	18dBm
36Mbps	15dBm	18dBm
48Mbps	15dBm	18dBm
54Mbps	15dBm	18dBm
HT20-0	15dBm	18dBm
HT20-1	15dBm	18dBm
HT20-2	15dBm	18dBm
HT20-3	15dBm	18dBm

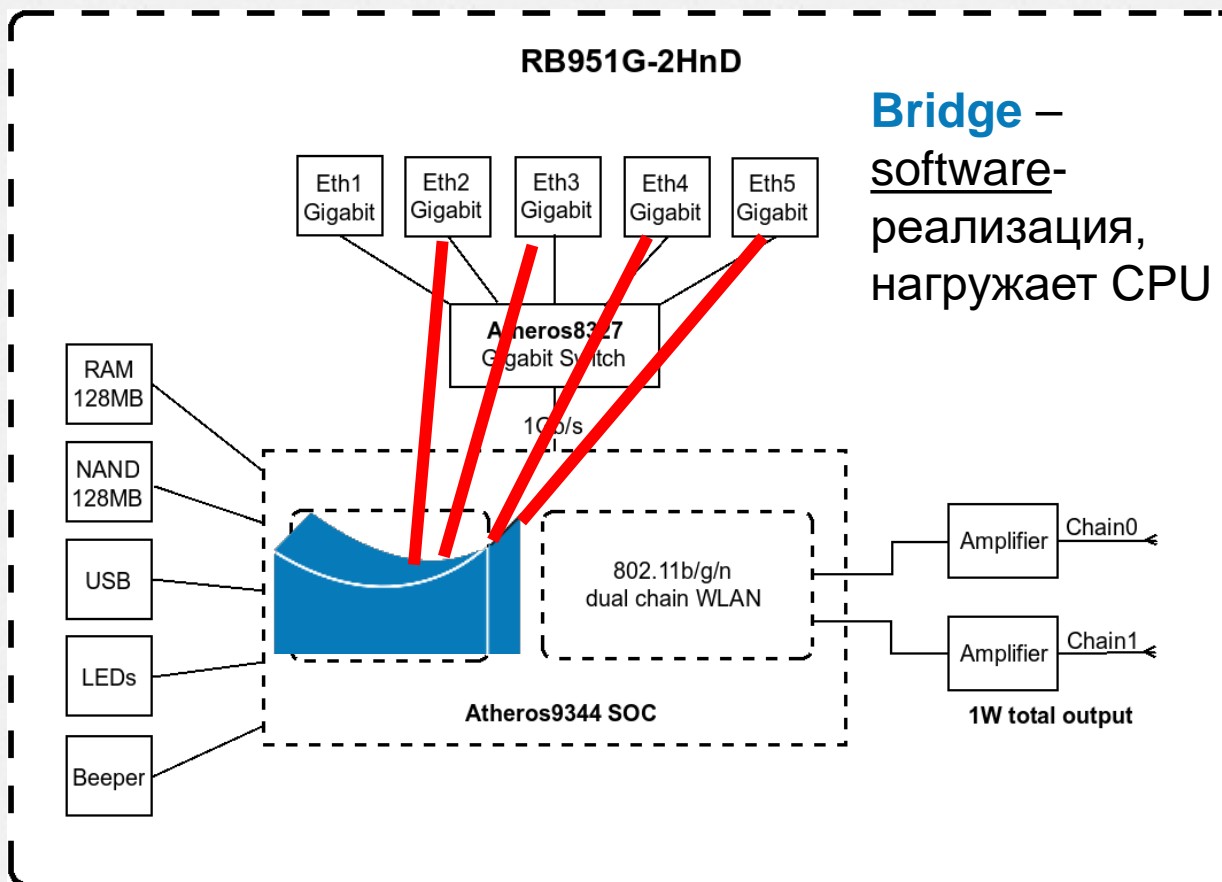
20dBm=100mW =)

Best Practice. Bridge vs Switch



Блок-диаграмма взята с routerboard.com

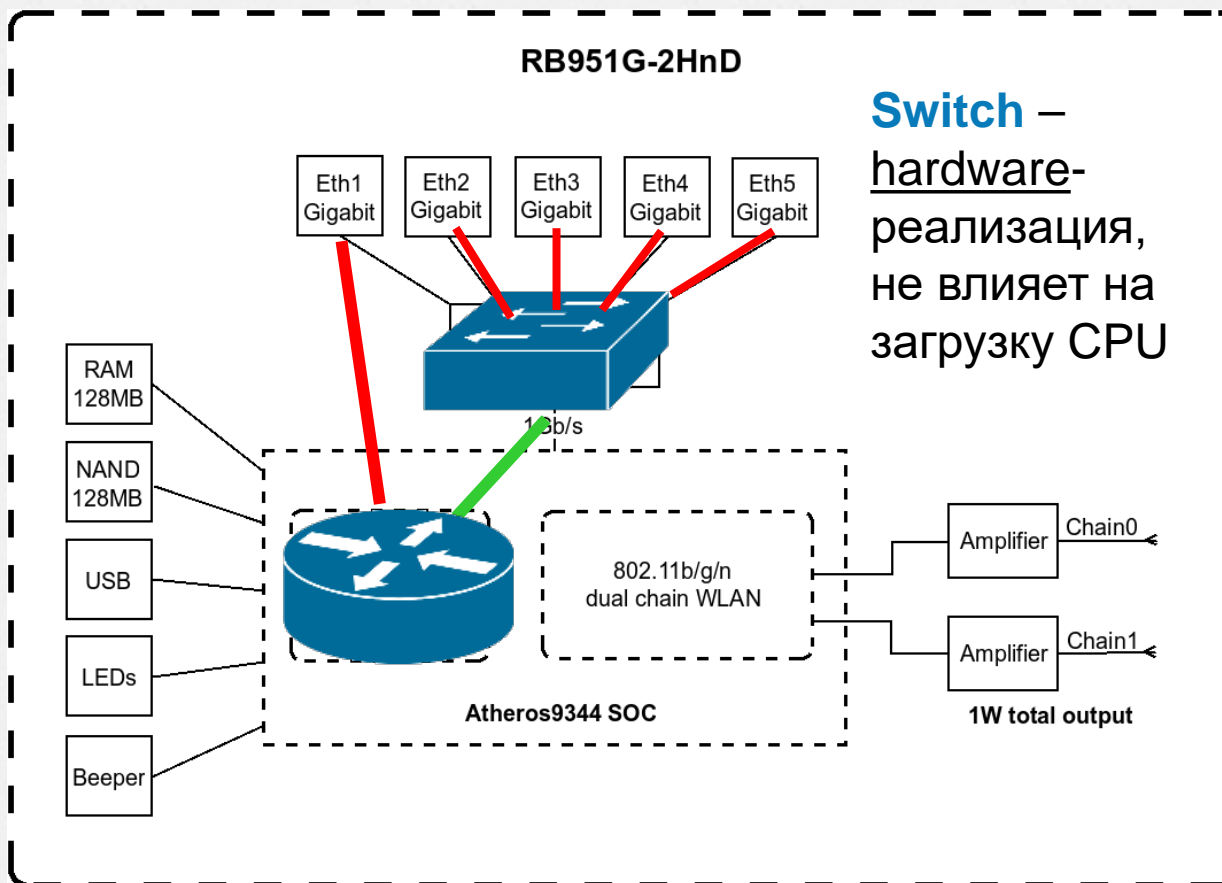
Best Practice. Bridge vs Switch



Bridge –
software-
реализация,
нагружает CPU

Блок-диаграмма взята с routerboard.com

Best Practice. Bridge vs Switch



Блок-диаграмма взята с routerboard.com

Best Practice. Bridge vs Switch

- Switch-чип включается указанием Master-порта в настройках интерфейса.
- На одном чипе может быть только один мастер-порт

```
[nickname@Test router] > interface ethernet print
Flags: X - disabled, R - running, S - slave
#   NAME                MTU MAC-ADDRESS      ARP      MASTER-PORT
0 R   ;;; internet
    ether1              1500 D4:CA:6D:7C:D5:5A enabled  none
1   ether2              1500 D4:CA:6D:7C:D5:5B enabled  none
2   ether3              1500 D4:CA:6D:7C:D5:5C enabled  none
3   ether4              1500 D4:CA:6D:7C:D5:5D enabled  none
4   ether5              1500 D4:CA:6D:7C:D5:5E enabled  none
[nickname@Test router] > interface ethernet set 2,3,4 master-port=ether2
[nickname@Test router] > interface ethernet print
Flags: X - disabled, R - running, S - slave
#   NAME                MTU MAC-ADDRESS      ARP      MASTER-PORT
0 R   ;;; internet
    ether1              1500 D4:CA:6D:7C:D5:5A enabled  none
1   ether2              1500 D4:CA:6D:7C:D5:5B enabled  none
2 S ether3              1500 D4:CA:6D:7C:D5:5C enabled  ether2
3 S ether4              1500 D4:CA:6D:7C:D5:5D enabled  ether2
4 S ether5              1500 D4:CA:6D:7C:D5:5E enabled  ether2
[nickname@Test router] > █
```

Best Practice. Bridge vs Switch

Настройка в Winbox:

The screenshot displays the Mikrotik Winbox interface configuration for a bridge. At the top, the 'Interface List' table shows the following data:

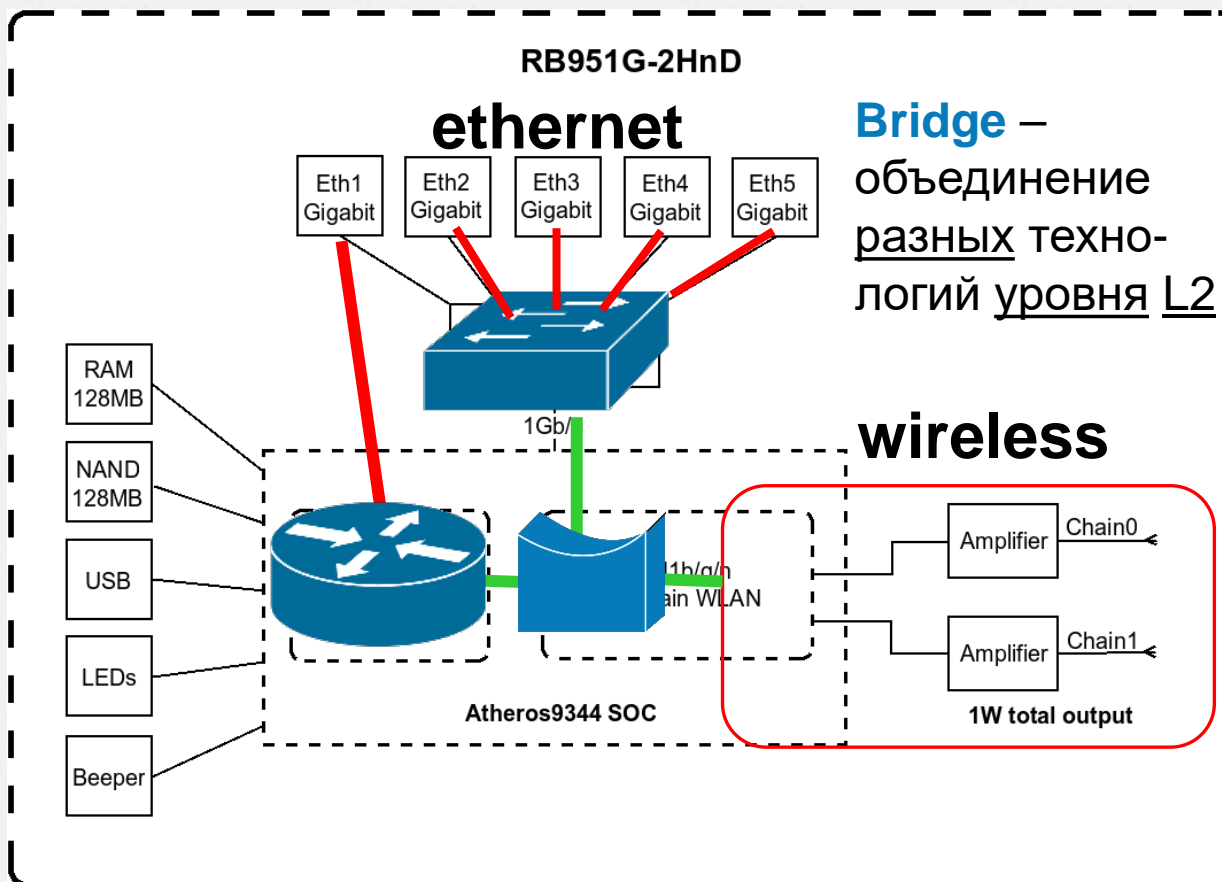
	Name	Type	MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx
R	ether1	Ethernet	1500	1598	101.5 kbps	7.3 kbps	10	9	
S	ether2	Ethernet	1500	1598	0 bps	0 bps	0	0	
S	ether3	Ethernet	1500	1598	0 bps	0 bps	0	0	
S	ether4	Ethernet	1500	1598	0 bps	0 bps	0	0	
S	ether5	Ethernet	1500	1598	0 bps	0 bps	0	0	

Below the table, three configuration windows are open for interfaces ether3, ether4, and ether5. Each window shows the 'General' tab with the following settings:

- Name: ether3, ether4, ether5
- Type: Ethernet
- MTU: 1500
- L2 MTU: 1598
- Max L2 MTU: 4074
- MAC Address: D4:CA:6D:..., D4:CA:..., D4:CA:6D:7C:D5:5E
- ARP: enabled
- Master Port: ether2 (circled in red)
- Bandwidth (Rx/Tx): unlimited

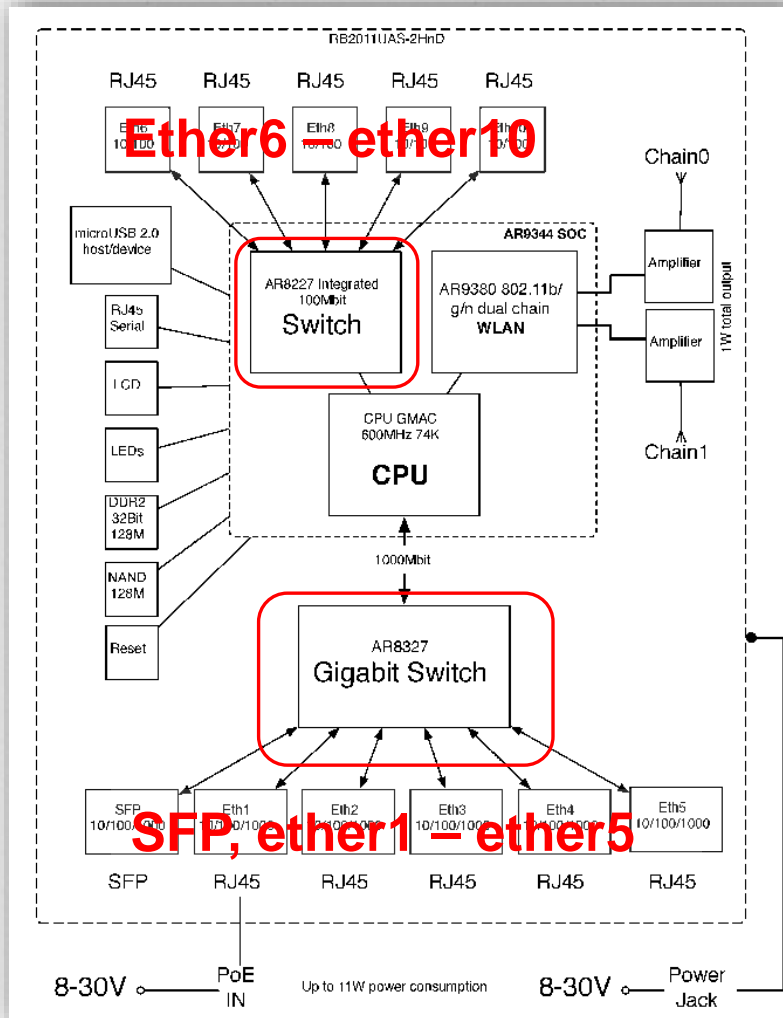
The 'Interface <ether5>' window also shows a 'Tx Stats' tab and a 'Tx Packet (p/s)' field set to 0.

Best Practice. Bridge vs Switch



Блок-диаграмма взята с routerboard.com

Best Practice. Bridge vs Switch

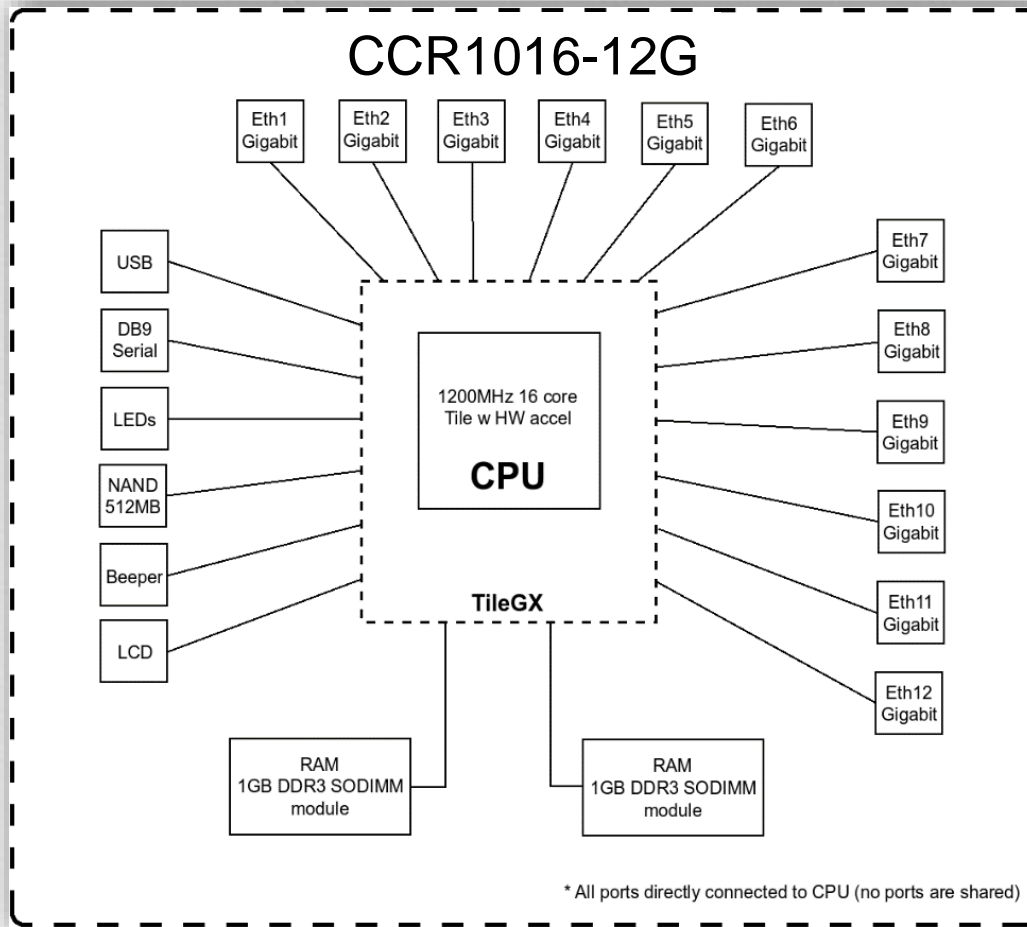


RB2011 series
2 свитч-чипа –
два мастер-порта.

Default configuration:
6: Master-port
7,8,9,10: Slaves of 6
2,3,4,5,6: Bridged

Optimal configuration:
6: Master-port
7,8,9,10: Slaves of 6
2: Master-port
3,4,5: Slaves of 2
2,6: Bridged

Best Practice. Bridge vs Switch



Выбирайте модель
ПОД СВОИ НУЖДЫ
ВНИМАТЕЛЬНО. Не
во всех есть
switch-chip.

Имена интерфейсов или комментарии?

Interface List

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



	Name	Type
S	NAS	Ethernet
S	accesspoint	Wireless (Atheros ...
S	gostevayato4ka	Virtual AP
R	gostevoymost	Bridge
R	internet	Ethernet
R	rabo4ayaset	VLAN
R	iptv	Bridge
RS	komp2	Ethernet
RS	gostNet	VLAN
R	offisyNaMarksa	L2TP Client
R	rezerv	GRE Tunnel
S	servak	Ethernet
	wifi-to4ka	Ethernet

13 items (1 selected)

Terminal

```
[nickname@MikroTik] > interface print
Flags: D - dynamic, X - disabled, R - running, S - s
#    NAME    TYPE
0   S  NAS      ether
1   R  internet ether
2   RS komp2   ether
3   S  servak   ether
4   wifi-to4ka ether
5   S  accesspoint wlan
6   S  gostevayato4ka wlan
7   RS gostNet  vlan
8   R  gostevoymost bridge
9   R  iptv      bridge
10  R  offisyNaMarksa l2tp-out
11  R  rabo4ayaset  vlan
12  R  rezerv     gre-tunne
```

```
[nickname@MikroTik] >
```

Имена интерфейсов или комментарии?

The screenshot displays two windows from the Mikrotik WinBox interface. The left window, titled "Interface List", shows a table of network interfaces. The right window, titled "New Firewall Rule", shows the configuration for a firewall rule.

Interface List

Interface	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRPP	Bonding	LTE
Name	Type							
::: IPTV								
R	bridge1							
::: guest bridge								
R	bridge2							
::: internet								
RS	ether1							
::: remoteWork								
R	vlan2							
::: komp2								
R	ether2							
::: guestnet								
RS	vlan15							
::: mailserv								
S	ether3							
::: NAS								
S	ether4							
::: STB								
S	ether5							
::: backup channel								
R	gre-tunnel1							
::: Offices on Marksa								
	l2tp-out1							
::: AP 2.4								
	wlan1							
::: guests AP								
S	wlan2							

13 items (1 selected)

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Chain: forward

Src. Address: []

Dst. Address: []

Protocol: []

Src. Port: []

Dst. Port: []

Any. Port: []

P2P: []

In. Interface: []

Out. Interface: ether1

Packet Mark: []

Connection Mark: []

Routing Mark: ether1

Routing Table: []

Connection Type: []

Connection State: []

Connection NAT State: []

Firewall

Filter Rules | NAT | Mangle | Service

#	Action	Chain	Src.
::: special dummy rule to show fasttra			
0	D	acc...	forward
::: defconf: accept ICMP			
1	✓	acc...	input
::: defconf: accept established, relate			
2	✓	acc...	input
::: drop ssh brute forcers			
3	✗	drop	input
4	⇨	add...	input
5	⇨	add...	input
6	⇨	add...	input
7	⇨	add...	input
8	✓	acc...	input
::: defconf: drop all from WAN			
9	✗	drop	input
::: drop not-in-list to webserver			
10	✗	drop	forward

15 items

Обычные и *inline*-комментарии

Используйте удобное вам отображение в каждом окне

The screenshot displays two windows from Mikrotik WinBox. The background window is the Firewall Filter Rules configuration page, showing a list of 56 rules. The foreground window is the DHCP Server Leases configuration page, showing a table of leases. A context menu is open over the table, with 'Inline Comments' selected.

Firewall Filter Rules Table:

#	Action	Chain
38	jump	forward
39	drop	forward
40	return	block-ddos
41	add...	block-ddos
42	add...	block-ddos
... drop ssh brute forcers		
43	drop	sshbrutefo...
44	add...	sshbrutefo...
45	add...	sshbrutefo...
46	add...	sshbrutefo...
47	add...	sshbrutefo...
48	acc...	sshbrutefo...
... drop ssh brute downstream		
49	drop	forward
... drop Winbox brute forces		
50	drop	winboxbrut...
51	add...	winboxbrut...
52	add...	winboxbrut...
53	add...	winboxbrut...
54	add...	winboxbrut...
55	acc...	winboxbrut...

DHCP Server Leases Table:

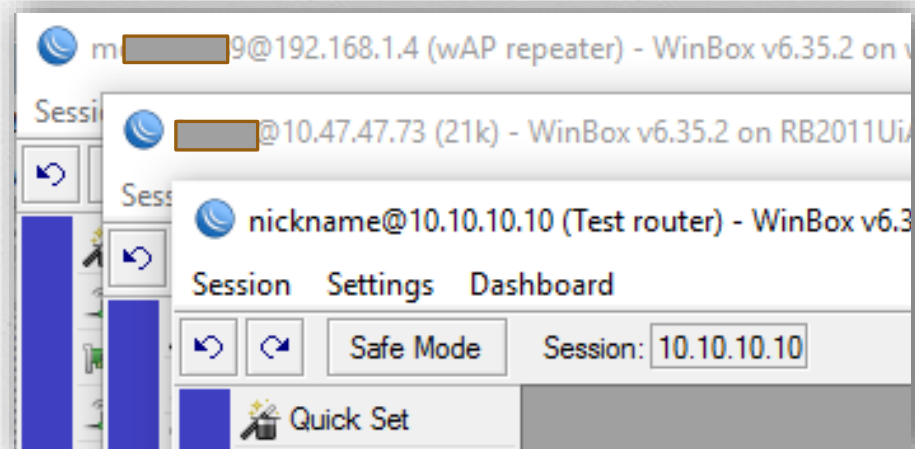
Address	MAC Address	Client ID	Server	Active Hos...	Expires After	Status	Comment
192.168.88.2	E4:8D:8C:EA:33:7C	1-e4-8d-8c-ea-33-7c	default	point1	2d 18:22:21	bound	Point 1
192.168.88.3	E4:8D:8C:D4:1...			point2	7d 13:35:12	bound	Point 2
192.168.88.4	E4:8D:8C:43:D...			point3	7d 13:35:07	bound	Point 3
192.168.88.5	E4:8D:8C:43:D...			point4	7d 13:35:06	bound	Point 4
192.168.88.6	E4:8D:8C:43:D...			point5	7d 13:35:31	bound	Point 5
192.168.88.7	0C:C4:7A:6B:68			ST_VE...	2d 18:19:49	bound	Server
192.168.88.8	98:EE:CB:25:56			in-ЦЪ	8d 10:30:03	bound	Reception
192.168.88.9	00:0A:83:02:2B					waiting	Online-controller S...
192.168.88.10	B8:E9:37:9A:03			osZP	9d 17:33:37	bound	sonos
192.168.88.11	B8:E9:37:00:9D			osZB	2d 18:19:48	bound	sonos
192.168.88.12	5C:AA:FD:44:CF			osZP	5d 16:20:47	bound	sonos
192.168.88.13	B8:97:5A:B4:D4			4s01	9d 10:17:04	bound	Terminal Bar
192.168.88.14	B8:AE:ED:9E:C...				9d 18:55:52	bound	Asterisk
192.168.88.15	00:0B:82:75:10				6d 19:26:35	bound	IP phone 210
192.168.88.20	D0:50:99:6A:6C			sir		waiting	Videoserver
192.168.88.21	90:18:7C:2C:5C			roid-3e...	8d 15:50:22	bound	
192.168.88.22	9C:4E:36:5D:43			SKTOP...	9d 19:35:09	bound	
192.168.88.24	2C:81:58:F8:D3			1078	9d 15:06:55	bound	

Identity – ваша страховка

Когда вы конфигурируете несколько роутеров, легко перепутать окно Winbox. Чтобы этого не случилось, присваивайте роутерам уникальные понятные имена:

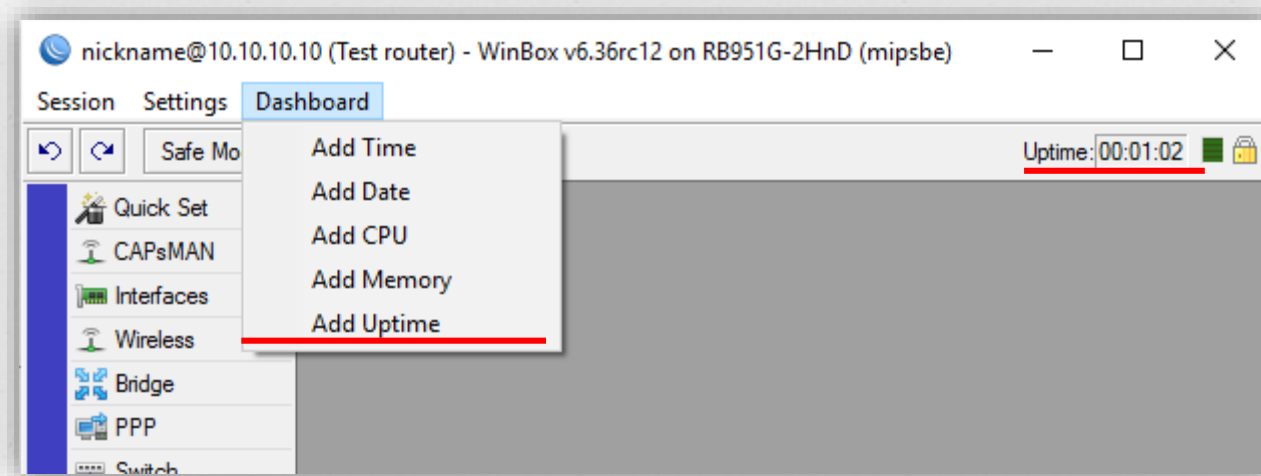
```
/system identity set name="Test router"
```

Либо в winbox
System-Identity



Маленькие полезности

Когда winbox теряет подключение к роутеру, мы узнаём об этом через ~20 сек. До этого он отображает пустые списки, например адреса, правила фаервола, интерфейсы. Чтобы всегда быть в курсе проблем с соединением – просто добавьте Uptime.



Маленькие полезности

Кнопка “Copy” часто незаслуженно забывается.

The screenshot shows the Mikrotik WinBox interface. On the left is the 'Firewall' sidebar with a list of filter rules. Rule 3, 'Drop UDP DNS from WAN', is selected. The main window is titled 'Firewall Rule <53>' and shows the configuration for this rule. The 'Chain' is set to 'input', the 'Protocol' is '17 (udp)', and the 'In. Interface' is 'ether1'. The 'Copy' button in the right-hand panel is highlighted with a red rectangle.

#	Action	Chain
0	D	forward
1	acc...	input
2	acc...	input
3	drop	input
4	drop	input
5	add...	input
6	add...	input
7	add...	input
8	add...	input
9	acc...	input
10	acc...	input

Firewall Rule <53> Configuration:

- Chain: input
- Src. Address: [empty]
- Dst. Address: [empty]
- Protocol: 17 (udp)
- Src. Port: [empty]
- Dst. Port: 53
- Any. Port: [empty]
- P2P: [empty]
- In. Interface: ether1
- Out. Interface: [empty]
- In. Interface List: [empty]
- Out. Interface List: [empty]

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters.

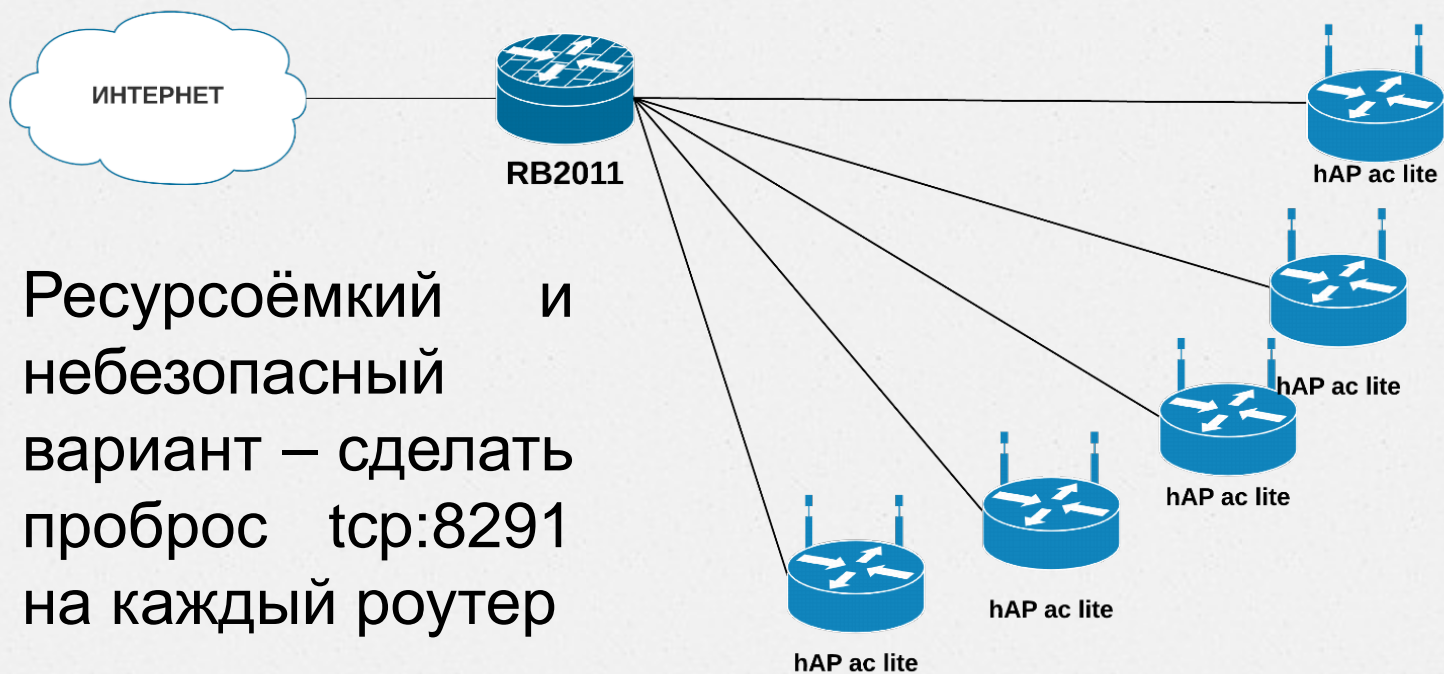
Маленькие полезности

Кнопка “**Copy**” упрощает настройку.

The screenshot displays the Mikrotik WinBox Firewall Rule configuration window for rule <53>. The 'General' tab is active, showing the rule is named 'Drop TCP DNS from WAN', has a chain of 'input', and is configured to drop TCP traffic on port 53 from the 'ether1' interface. A 'Comment for Firewall Rule <53>' dialog box is open, showing the text 'Drop TCP DNS from WAN'. The 'Copy' button is highlighted in the right-hand sidebar of the configuration window.

#	Action	Chain
0	special dummy rule	
1	defconf: accept ICM	input
2	defconf: accept esta	input
3	Drop UDP DNS from WAN	input
4	Drop TCP DNS from WAN	input
5	drop ssh brute force	input
6	add...	input
7	add...	input
8	add...	input
9	add...	input

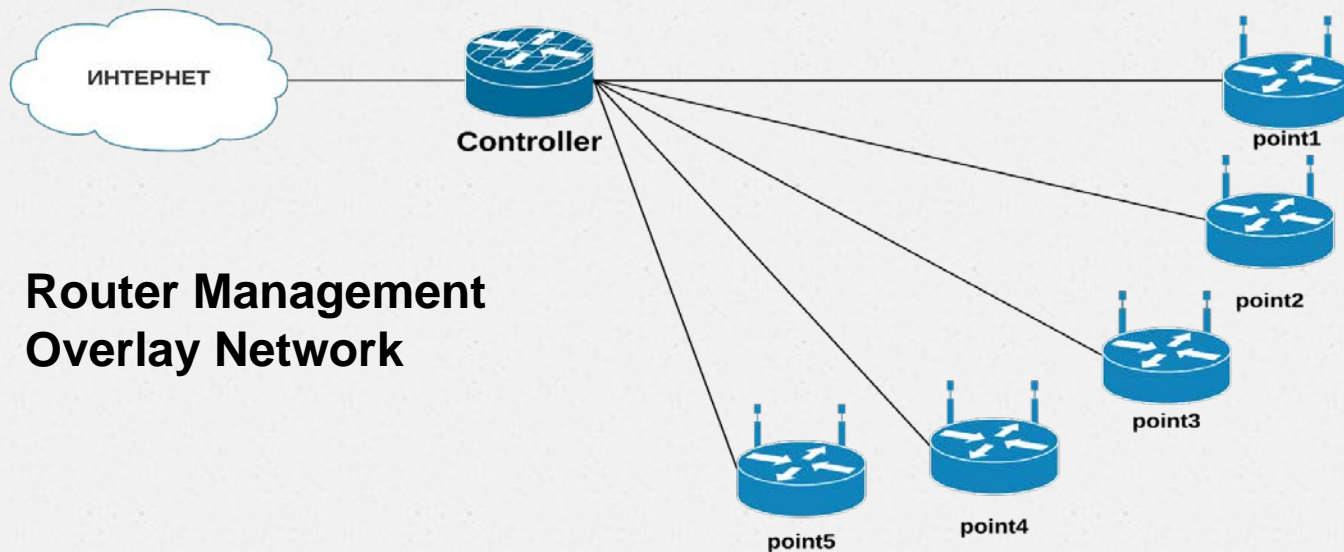
Задача: управление всеми роутерами из интернета



Ресурсоёмкий и небезопасный вариант – сделать проброс `tcp:8291` на каждый роутер

- Минусы:
- Для каждого роутера назначать и запоминать порт
- Все роутеры доступны из интернета

Решение: RoMON



Router Management Overlay Network

1. Включаем RoMON на всех роутерах и задаём секрет

```
/tool romon  
set enabled=yes secrets=SuperSecret
```

2. Подключаемся к основному роутеру через winbox кнопкой «Connect to RoMON»

Использование RoMON

- Подключаемся напрямую к роутерам
- Фаервол не мешает
- Кадры шифруются

WinBox v3.4 (Addresses)

File Tools

Connect To:

Login:

Password:

Session:

Note:

Group:

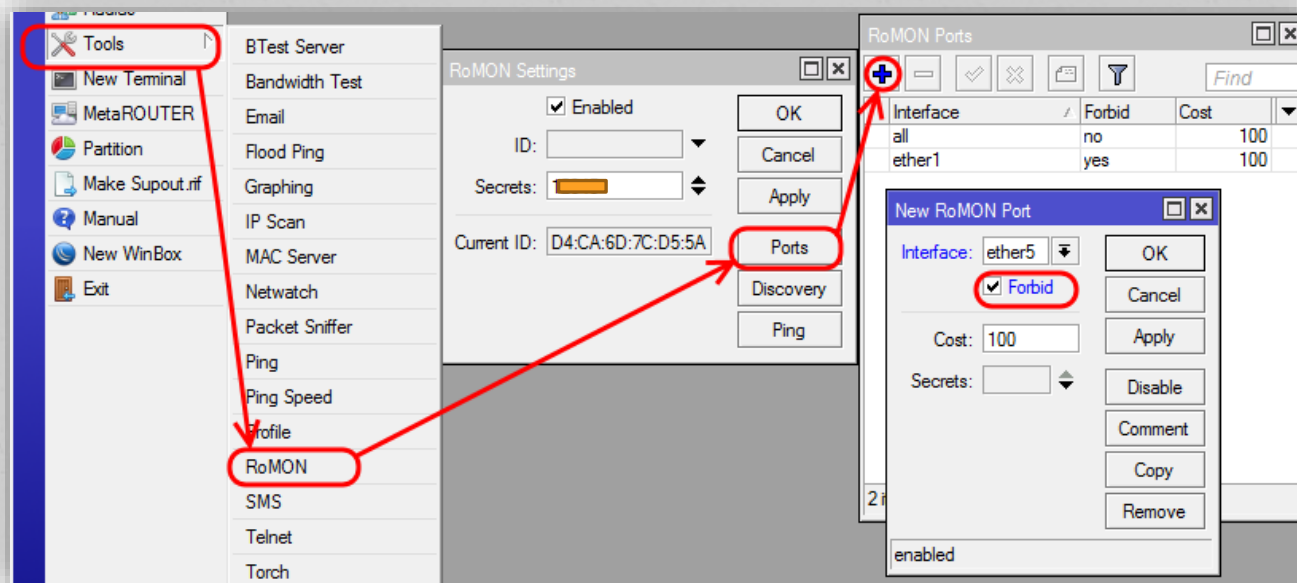
RoMON Agent:

Managed RoMON Neighbors

Address	Cost	Hops	Path	L2MTU	Identity	Version	Board
E4:8D:8C:EA:33:7C	200	1	E4:8D:8C:EA:33:7C	1500	point 1	6.35.2	RB952Ui-5ac2nD
E4:8D:8C:D4:17:A4	200	1	E4:8D:8C:D4:17:A4	1500	point2	6.35.2	RB952Ui-5ac2nD
E4:8D:8C:43:D7:B5	200	1	E4:8D:8C:43:D7:B5	1500	point3	6.35.2	RB952Ui-5ac2nD
E4:8D:8C:43:D8:17	200	1	E4:8D:8C:43:D8:17	1500	point4	6.35.2	RB952Ui-5ac2nD
E4:8D:8C:43:D7:0D	200	1	E4:8D:8C:43:D7:0D	1500	point5	6.35.2	RB952Ui-5ac2nD

RoMON работает независимо от конфигураций L2 и L3.

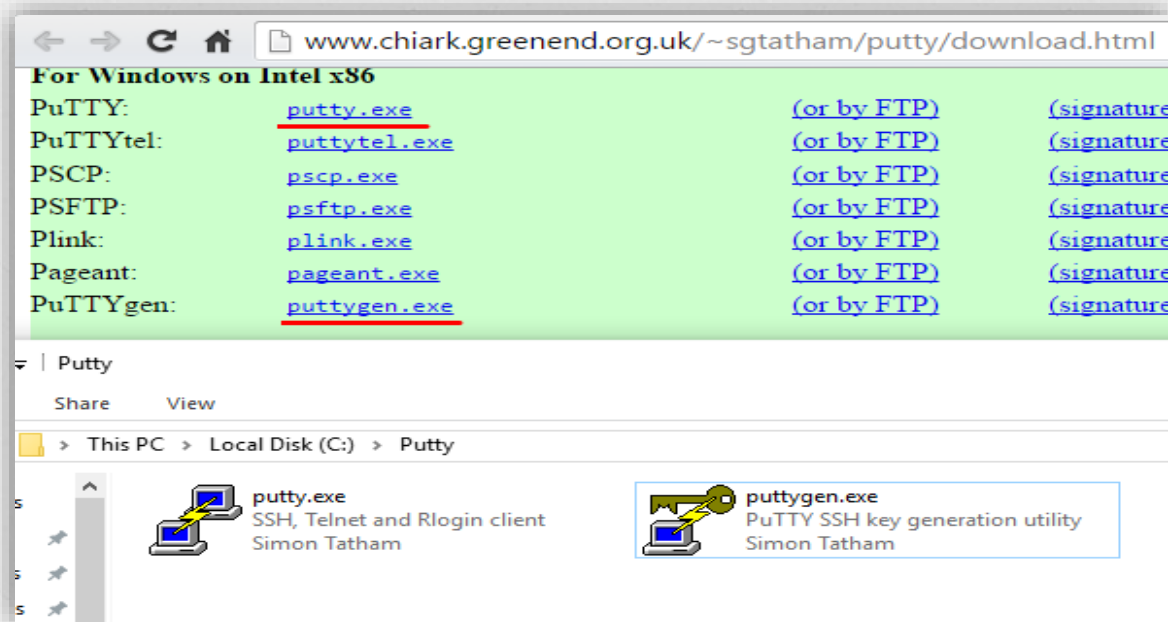
Защита от RoMON-подключений извне



```
/tool romon port add interface=ether1 forbid=yes \  
disabled=no
```

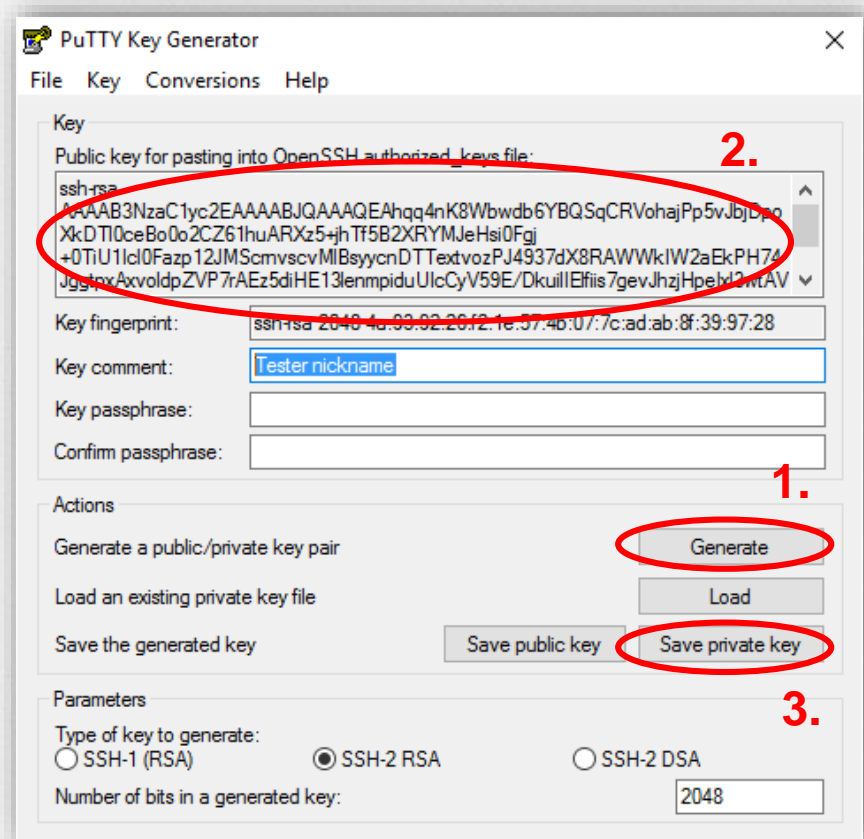
Доступ SSH по ключу

- Из публичного ключа нельзя сделать приватный
- Быстрый доступ после однократной настройки
- Ключ исключает возможность подбора пароля



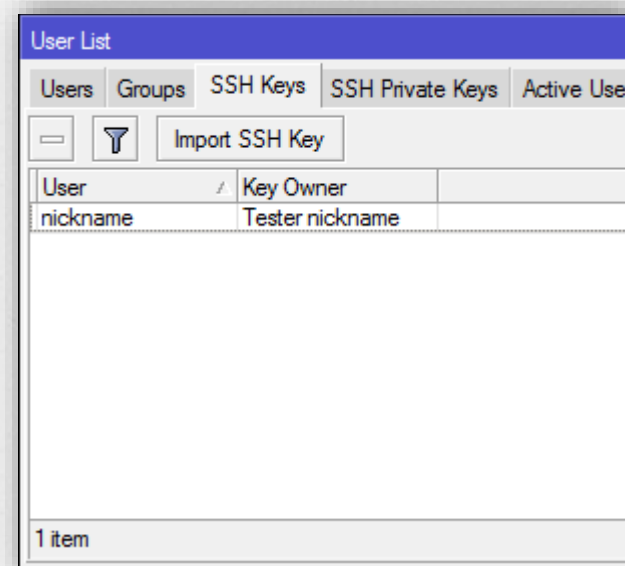
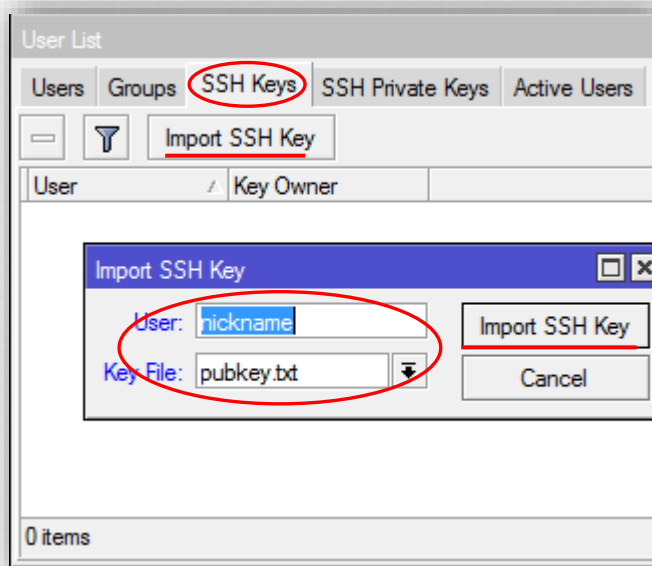
Доступ SSH по ключу

1. Генерируем RSA или DSA ключ длиной 2048 байт (Запускаем puttygen - Generate)
2. Копируем текст публичного ключа в файл и закидываем на роутер (pubkey.txt)
3. Сохраняем приватный ключ в файл .ppk



Доступ SSH по ключу

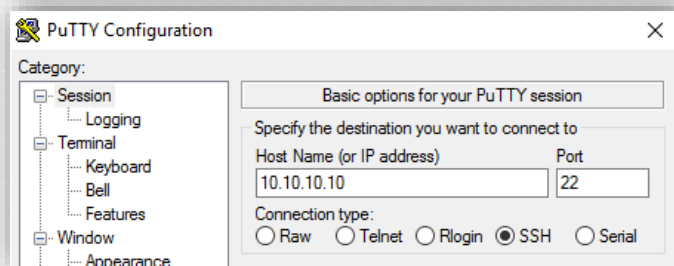
На роутере заходим в управление пользователями (*System-Users*) и импортируем ключ для конкретного пользователя:



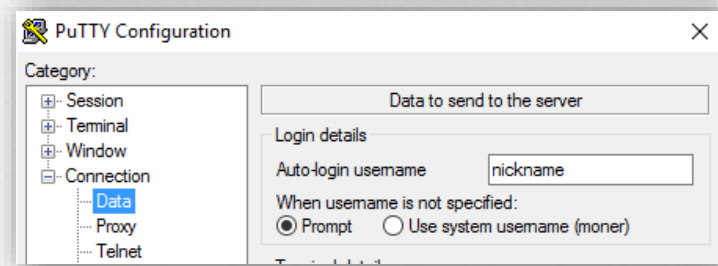
После импорта файл публичного ключа автоматически удаляется

Доступ SSH по ключу

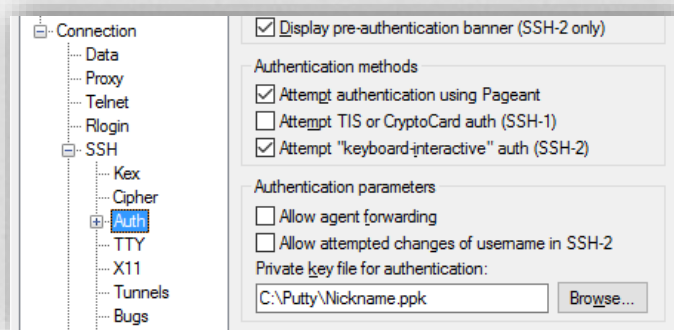
Настраиваем Putty:



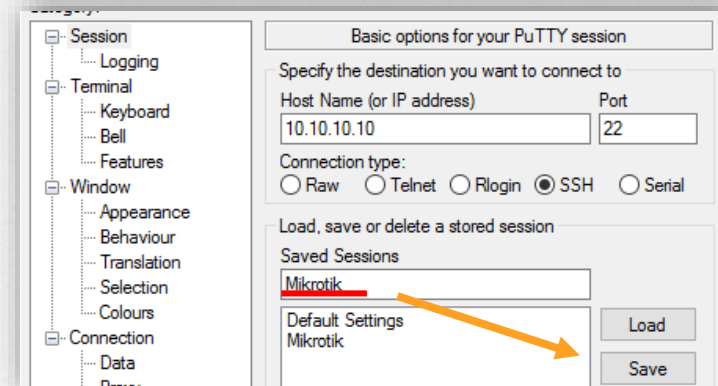
1. Указываем IP-адрес



2. Указываем имя пользователя



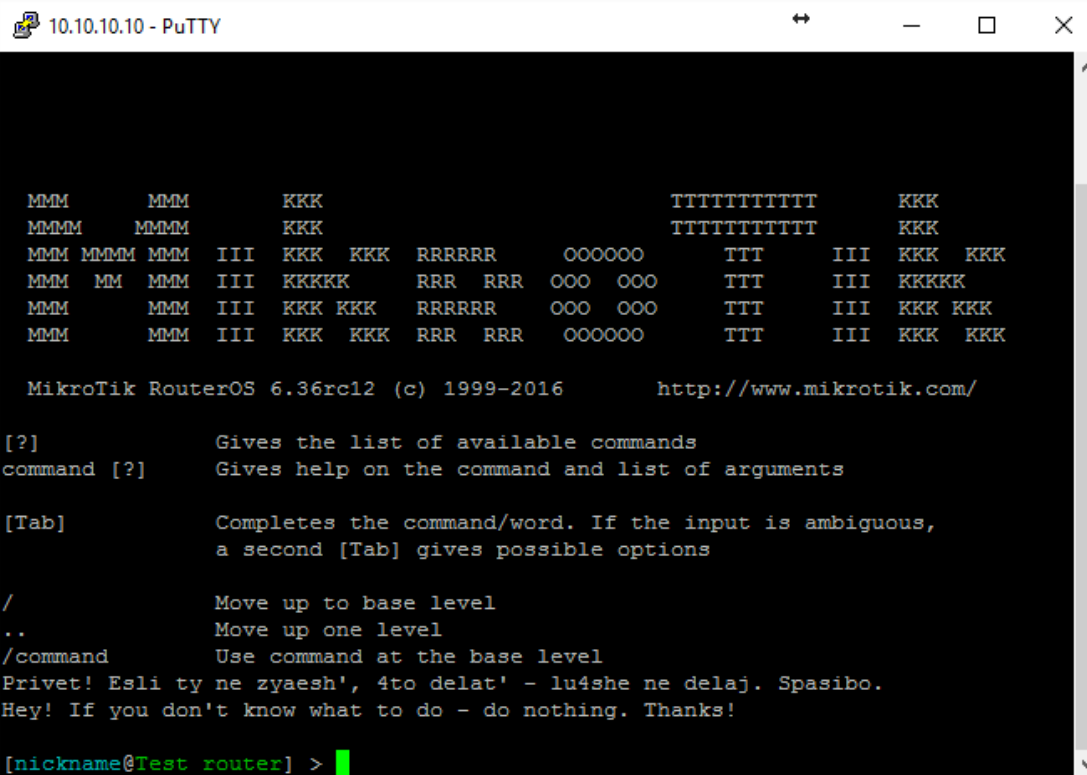
3. Указываем файл ключа



4. Сохраняем сессию

Доступ SSH по ключу

И, наконец, подключаемся кнопкой **Open**:



```
10.10.10.10 - PuTTY

MMM      MMM      KKK      TTTTTTTTTT      KKK
MMMMM    MMMM     KKK      TTTTTTTTTT      KKK
MMM MMMM MMM III  KKK  KKK  RRRRRR    OOOOOO    TTT   III  KKK  KKK
MMM MM  MMM III  KKKKK  RRR  RRR  OOO  OOO    TTT   III  KKKKK
MMM     MMM III  KKK  KKK  RRRRRR    OOO  OOO    TTT   III  KKK  KKK
MMM     MMM III  KKK  KKK  RRR  RRR    OOOOOO    TTT   III  KKK  KKK

MikroTik RouterOS 6.36rc12 (c) 1999-2016      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

/           Move up to base level
..         Move up one level
/command   Use command at the base level
Privet! Esli ty ne zyaesh', 4to delat' - lu4she ne delaj. Spasibo.
Hey! If you don't know what to do - do nothing. Thanks!

[nickname@Test router] > |
```

Рассматриваемые вопросы

- Первоначальные настройки безопасности
- Принципы работы фаервола на примере конфигурации по умолчанию
- Как облегчить жизнь самому себе? (Полезные советы и Best Practice)
- Командная строка – это просто

CLI – это просто!

Командная строка в RouterOS:

- o Помогает ускорить процесс настройки
- o Интуитивно понятна, синтаксис подсвечен
- o Разделы настройки практически полностью идентичны таковым в Winbox
- o Команды добиваются TAB-ом
- o Необходимые параметры запрашиваются, если отсутствуют во введённой команде.
- o Есть режимы Safe Mode (Ctrl+X) и HotLock Mode (Ctrl+V)

Включил *Safe Mode* – выключи *Safe Mode*!

- o Принцип *Safe Mode*: разорвалась сессия – откат на состояние до включения.

```
[nickname@Test router] > Ctrl+X
[Safe Mode taken]
[nickname@Test router] <SAFE> /ip firewall filter add disabled=no place-before=5
in-interface=ether5 chain=forward dst-address=12.12.12.12 protocol=tcp action=rej
ect reject-with=tcp-reset
[nickname@Test router] <SAFE> Ctrl+X
[Safe Mode released]
[Safe mode released by another user]
[nickname@Test router] > █
```

- o После настроек выключаем *Safe Mode*
- o Если потеряли роутер – откат через ~9 мин.
- o Best practice – периодически отключать *Safe Mode* и включать обратно, чтобы сохранить изменения.

<http://wiki.mikrotik.com/wiki/Manual:Console>

CLI – это просто!

Для быстрого освоения, настраивайте с помощью Winbox, затем в терминале смотрите, как это настроено:

- o Найдите нужный раздел в терминале
- o Чтобы увидеть, ЧТО настроено – **print**
- o Чтобы увидеть, КАК настроено – **export**
- o Просмотр возможных опций – **TAB** и ?

CLI – пример с маршрутами

The screenshot displays the Mikrotik WinBox interface. On the left, the 'IP' menu item is circled in red. Below it, the 'Routes' menu item is also circled in red. The main window shows the 'Route List' configuration page, which contains a table of routes. The table has columns for 'AS', 'Dst. Address', 'Gateway', 'Distance', 'Routing Mark', and 'Pref. Source'. Three routes are listed: AS (0.0.0.0/0), DAC (10.10.10.11), and DC (192.168.88.0/...). The 'AS' row is highlighted with a red line.

AS	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	10.10.10.11 reachable ether1	1		
DAC	10.10.10.11	ether1 reachable	0		10.10.10.10
DC	192.168.88.0/...	ether2 unreachable	255		192.168.88.1

Расположение в winbox: IP-Routes

CLI – пример с маршрутами

```
10.10.10.10 - PuTTY
[nickname@Test router] > TAB
caps-man      file      metarouter  queue      system     export     redo
certificate   interface mpls        radius     tool       import     setup
console       ip        partitions  routing    user       password   undo
disk          ipv6     port        snmp       beep       ping
driver        log      ppp         special-login blink      quit
[nickname@Test router] > ip TAB
accounting    dhcp-client firewall    packing    service    ssh         export
address       dhcp-relay hotspot     pool       settings   tftp
arp           dhcp-server ipsec      proxy      smb         traffic-flow
cloud         dns       neighbor   route      socks      upnp
[nickname@Test router] > ip route
[nickname@Test router] /ip route> print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
#      DST-ADDRESS      PREF-SRC      GATEWAY      DISTANCE
0 A S  0.0.0.0/0        10.10.10.11   1
1 ADC 10.10.10.11/32   10.10.10.10   ether1        0
2 DC  192.168.88.0/24  192.168.88.1  ether2        255
[nickname@Test router] /ip route> export
# may/21/2016 03:53:08 by RouterOS 6.36rc12
# software id = HAYH-5KVD
#
/ip route
add distance=1 gateway=10.10.10.11
[nickname@Test router] /ip route>
```


CLI – это просто!

- o Большинство разделов легко найти:
 - IP->Firewall->Filter Rules = `/ip firewall filter`
 - IP->Routes = `/ip route`
- o Встречаются небольшие отличия:
 - System->Users в Winbox, но `/user` в CLI
 - Wireless в Winbox, но `/interface wireless` в CLI
 - PPP->Interface в Winbox, но
`/interface ppp-client`, `/interface pptp-client`,
`/interface pppoe-client`, `/interface ovpn-client` и т. д.
- o Или просто наберите `/export` для просмотра полной конфигурации

Различия CLI и winbox

Winbox: **CLI:**

- o Tools-ping = /ping
- o Tools-Telnet = /system telnet (ssh)
- o Tools-Telnet = /tool mac-telnet
- o IP-SNMP = /snmp
- o Files-[Backup] = /system backup save
- o Files-[Restore] = /system backup load
- o System-Certificates = /certificate
- o System-Special login= /special-login
- o System-Disks = /disk

Рассмотренные вопросы

- Первоначальные настройки безопасности
- Принципы работы фаервола на примере конфигурации по умолчанию
- Как облегчить жизнь самому себе? (Полезные советы и Best Practice)
- Командная строка – это просто

*А напоследок
я скажу...*

RouterOS – дай волю фантазии!

The Dude:

The screenshot displays the 'The Dude' network management interface. The top-left pane shows a sidebar with a 'Contents' menu including Address Lists, Admins, Agents, Charts, and various network tools. The main area is divided into three sections:

- Map View:** A geographical map showing a network topology with nodes and links overlaid on a street map.
- Device List:** A table listing network devices with columns for Name, Version, Architecture, Board, Upgrade Status, and Packages. A context menu is open over the '64560' device, showing options like 'Device Settings', 'Show On Map', 'Tools', 'Settings', 'Upgrade', 'Force Upgrade', and 'Reconnect'.

Device	Group	Wireless Registration	Simple Queue	Architecture	Board	Upgrade Status	Packages
127n	ok			all	RB951U-2nD		
2ik	ok			all	RB2011UAS-2nD		
3b	ok			all	RB2011UAS-2nD		
64560	ok			all	RB2011UAS-2nD		
75b	ok			all	RB2011UAS-2nD		
81v	ok			all	RB2011LS		
BTesl	ok			all	RB951U-2nD		
OCPS	ok			all	CCP1009-80-15-15+		
Riveb	ok			all	RB2011UAS		
SxTlv	ok			all	RB2011UAS		
SxTlv	ok			all	6.35.2		
hAP C	ok			all	6.35c16		
wAP n	ok			all			
- Network Diagrams:** Two smaller diagrams on the right show detailed network topologies with nodes labeled with IP addresses and device names, connected by lines representing network links.

At the bottom left, status information is displayed: 'Client: α 21.3 kbps / tx 248 bps', 'Server: α 1.15 kbps / tx 5.62 kbps', and 'Connected'.

Ваши вопросы?

*Спасибо за
ваше внимание!*