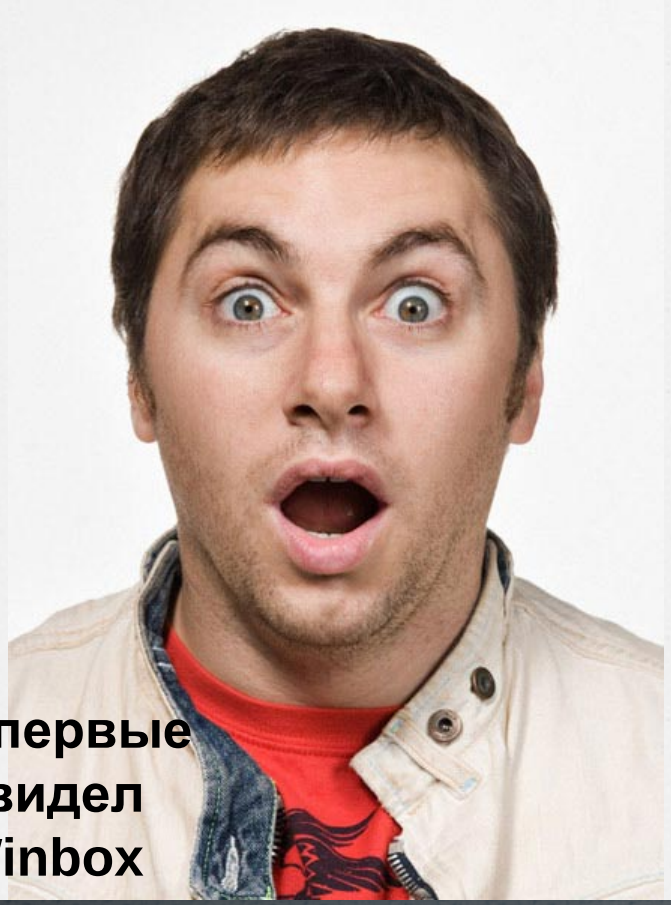
Начало работы
и рекомендации по настройке
на примерах из жизни.

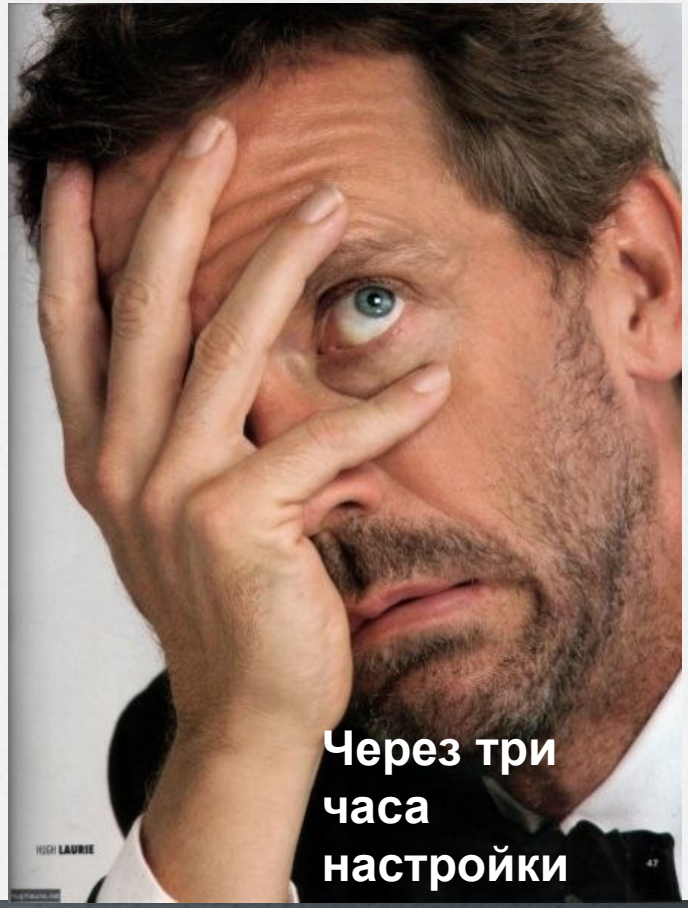
Давайте знакомиться:

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

Первое знакомство с Mikrotik

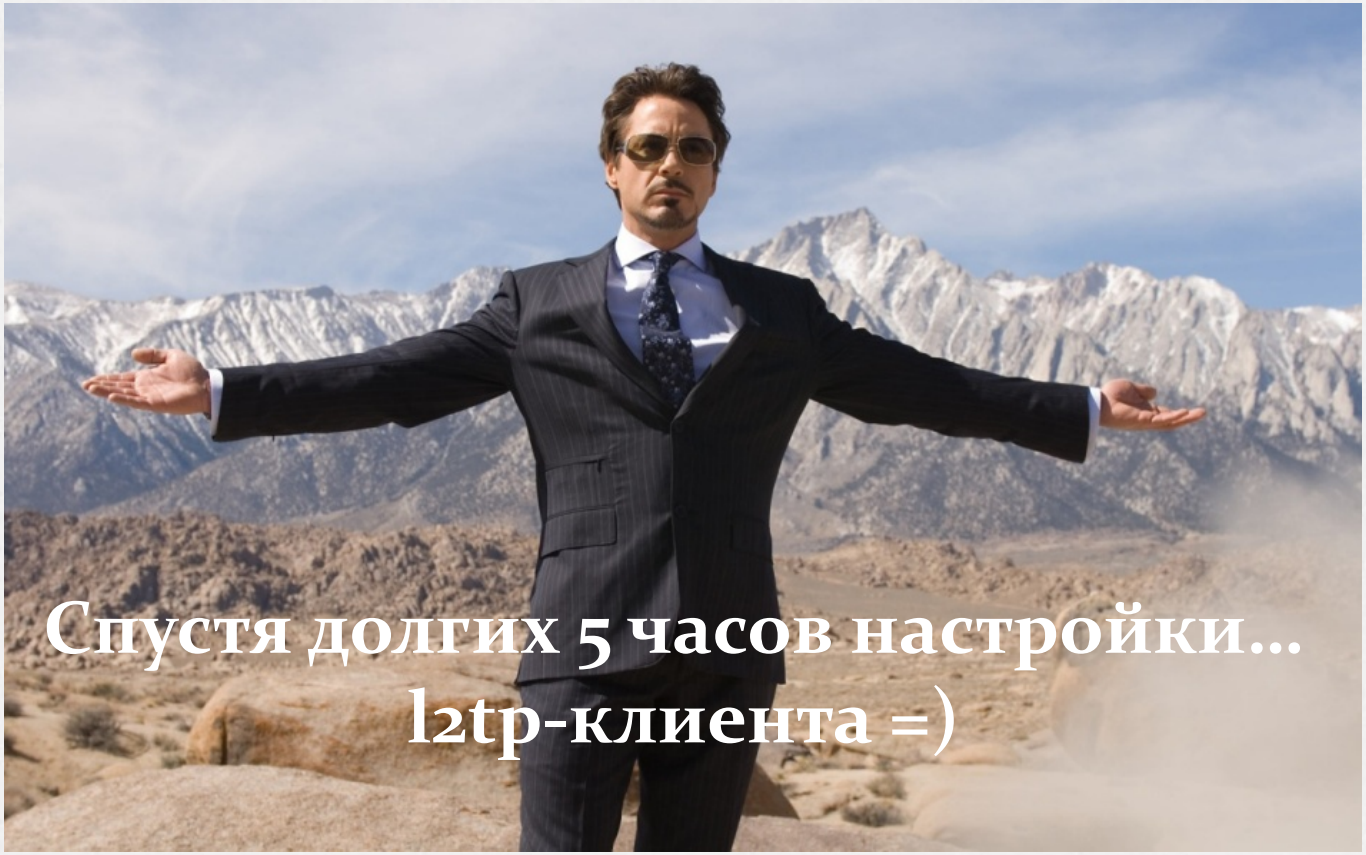


Впервые увидел Winbox



Через три часа настройки

Первое знакомство с Mikrotik



О чём пойдёт речь?

- 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

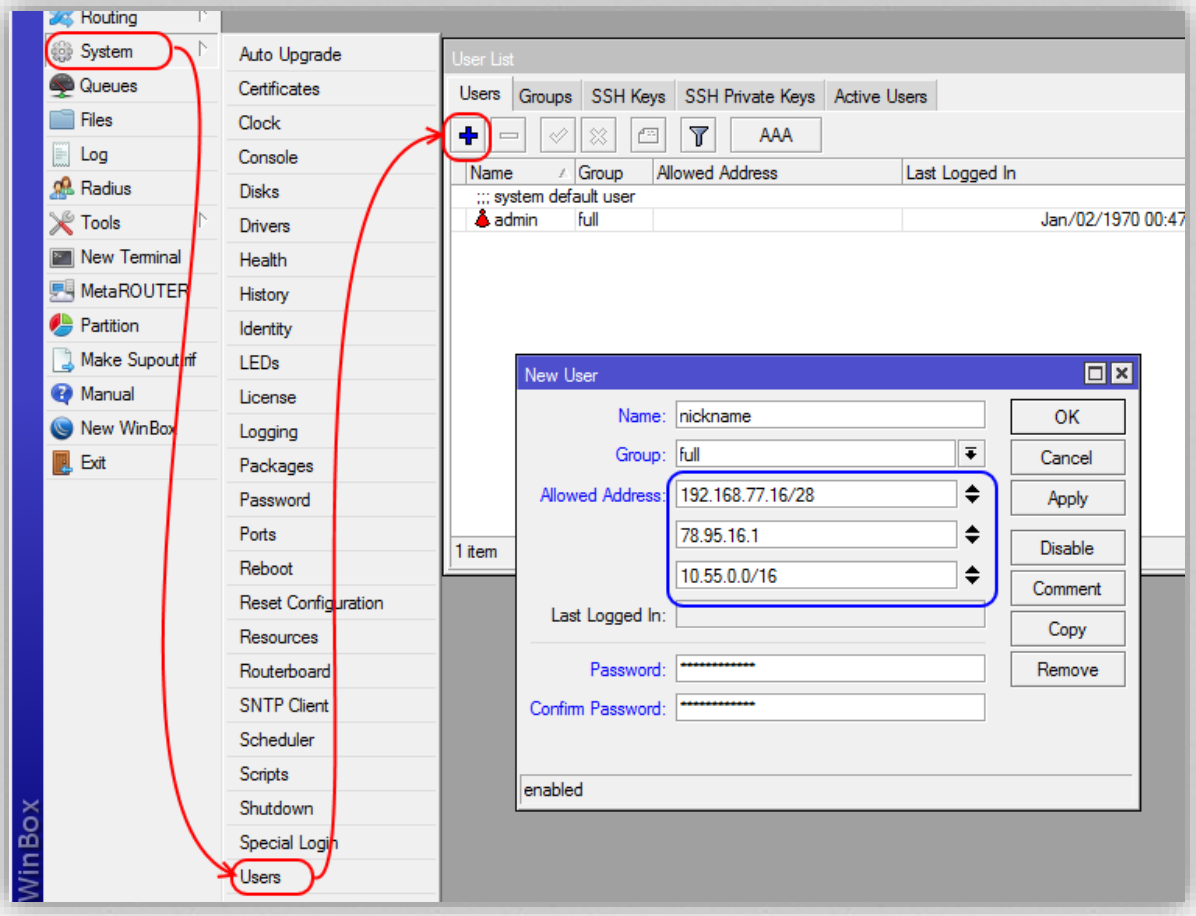
Безопасность в blank-конфигурации:

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



Создание пользователя

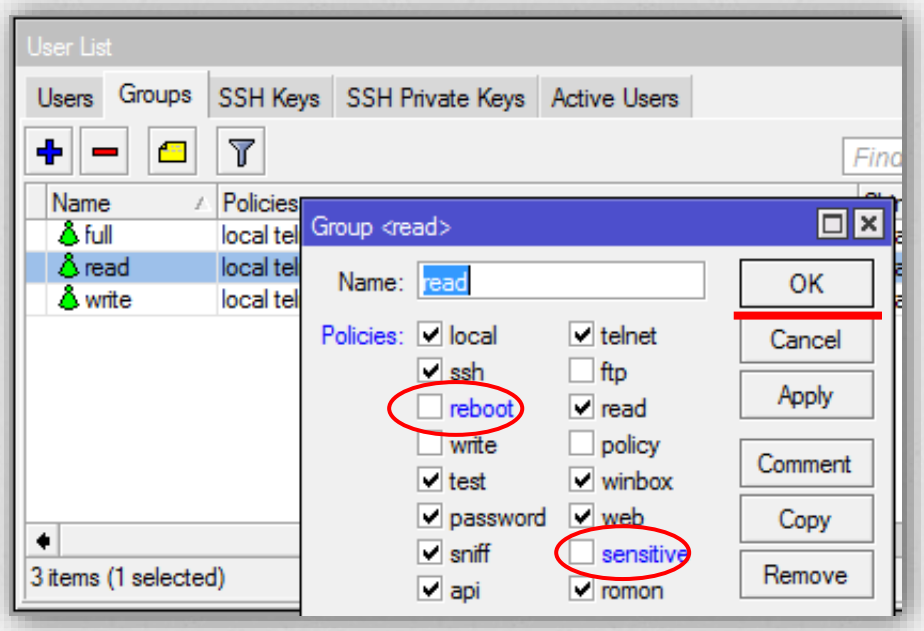
- /user add address=192.168.77.16/28, 78.95.16.1/32,10.55.0.0/16 group=full name=nickname password=MySuperP@$$
  Теперь пользователя **admin** можно отключать либо удалять.

- 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.

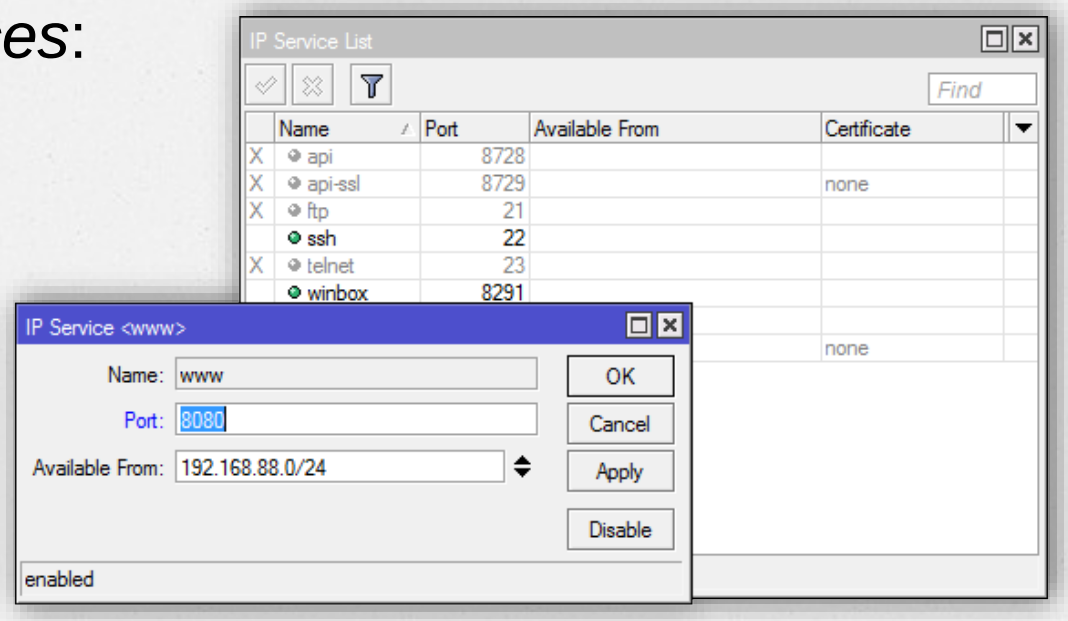
System – Users:



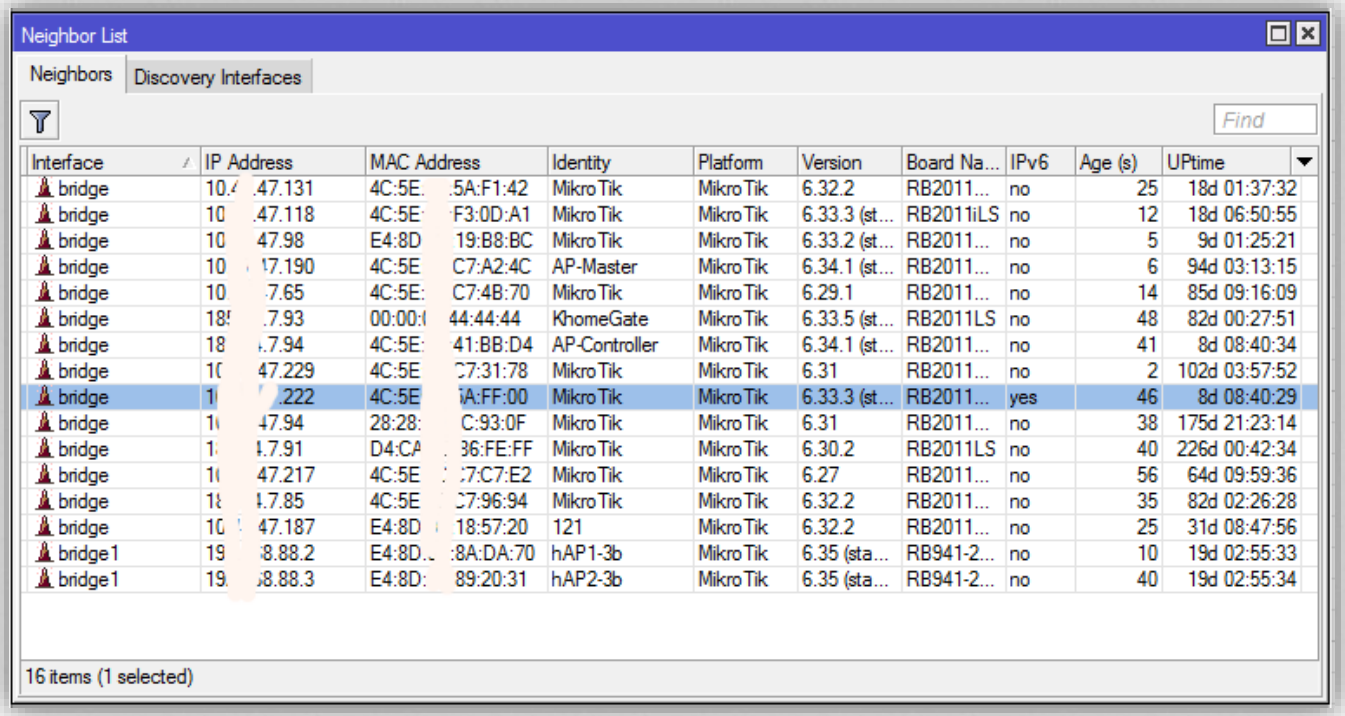
Сервисы:

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

IP-Services:



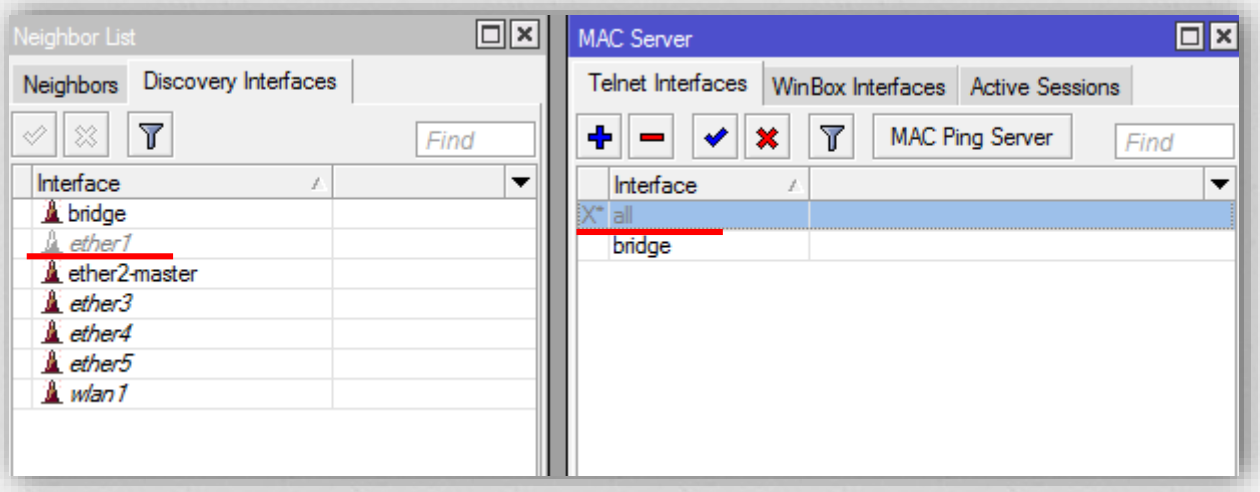
Пример с живой сети:



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

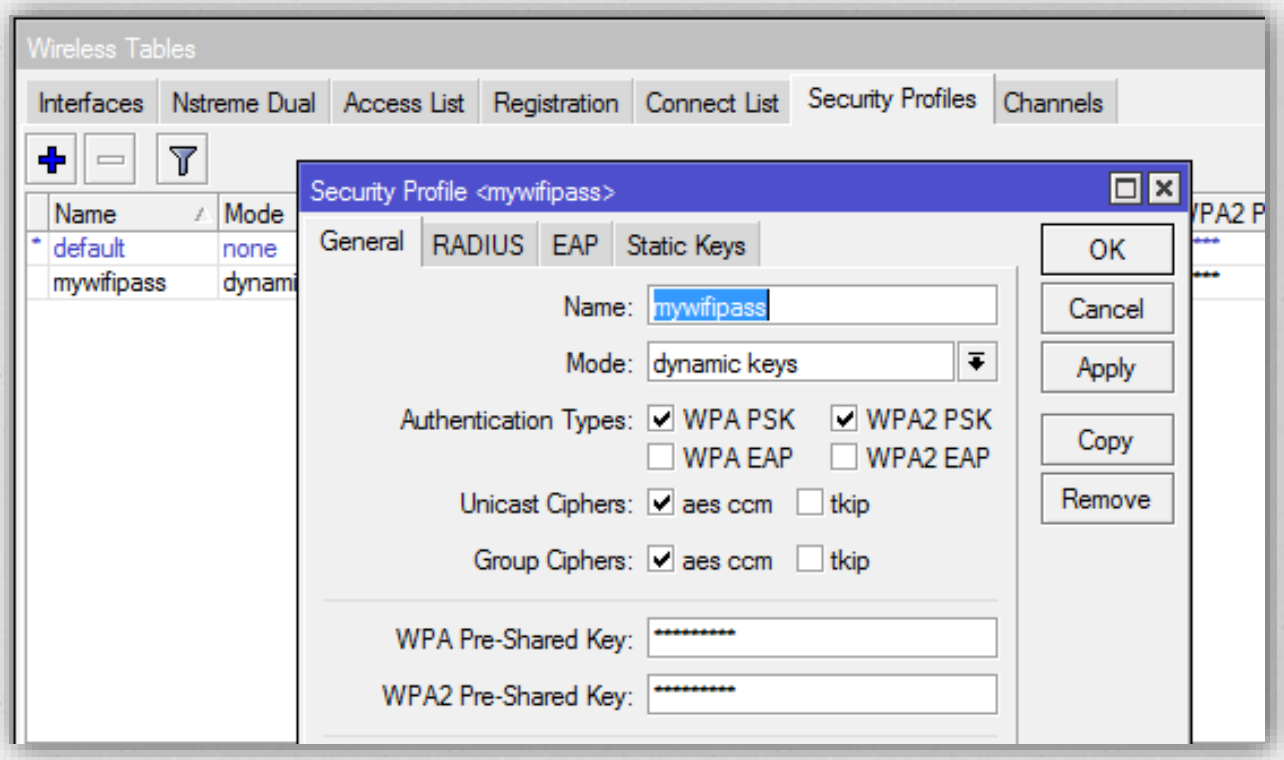
Чтобы не стать жертвой атаки:

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

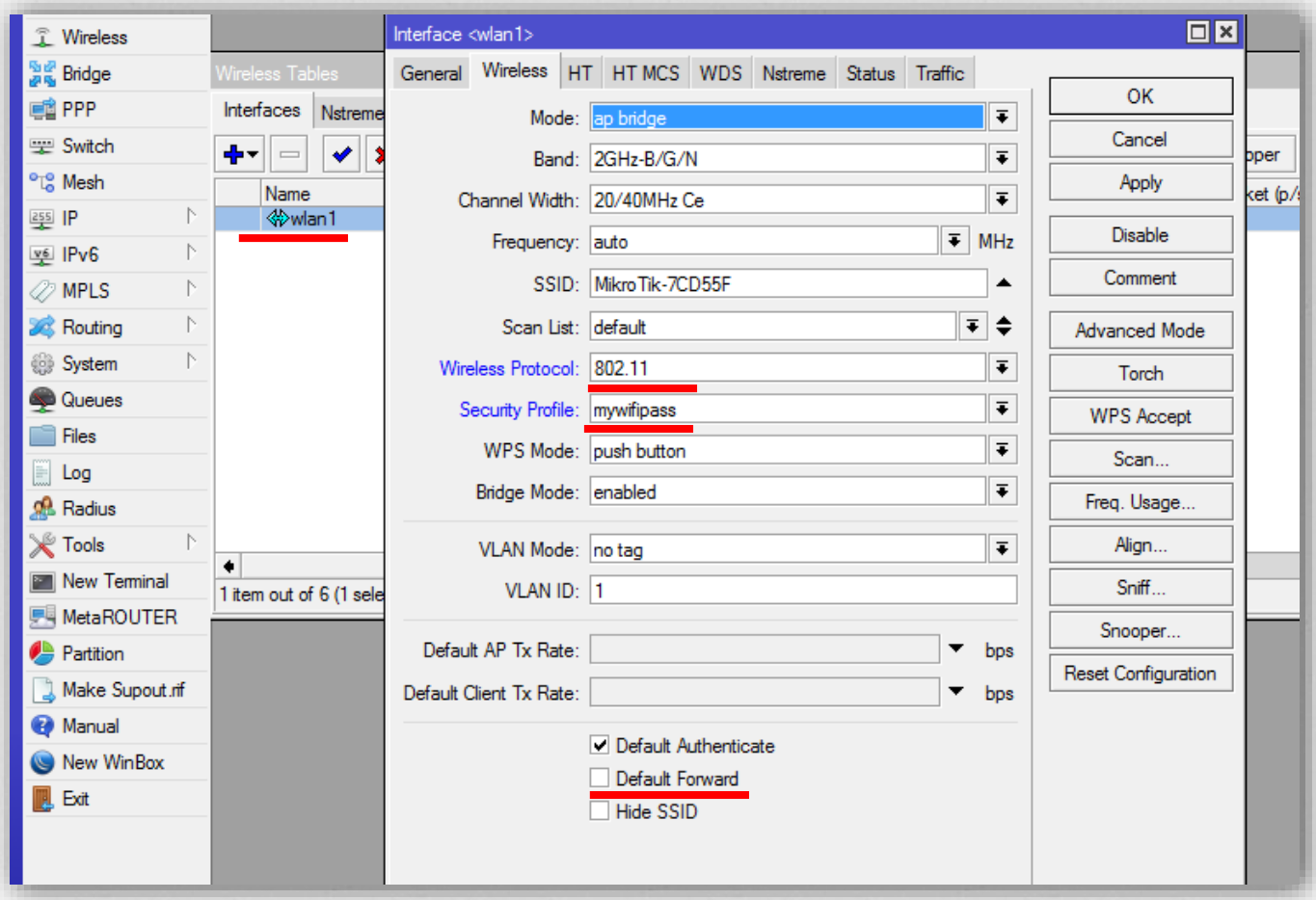


Защита Wi-Fi

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



Защита Wi-Fi


Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit
Wireless Tables
Interfaces
Nstreme
Name
wlan1
1 item out of 6 (1 sele
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
OK
Cancel
Apply
Disable
Comment
Advanced Mode
Torch
WPS Accept
Scan...
Freq. Usage...
Align...
Sniff...
Snooper...
Reset Configuration

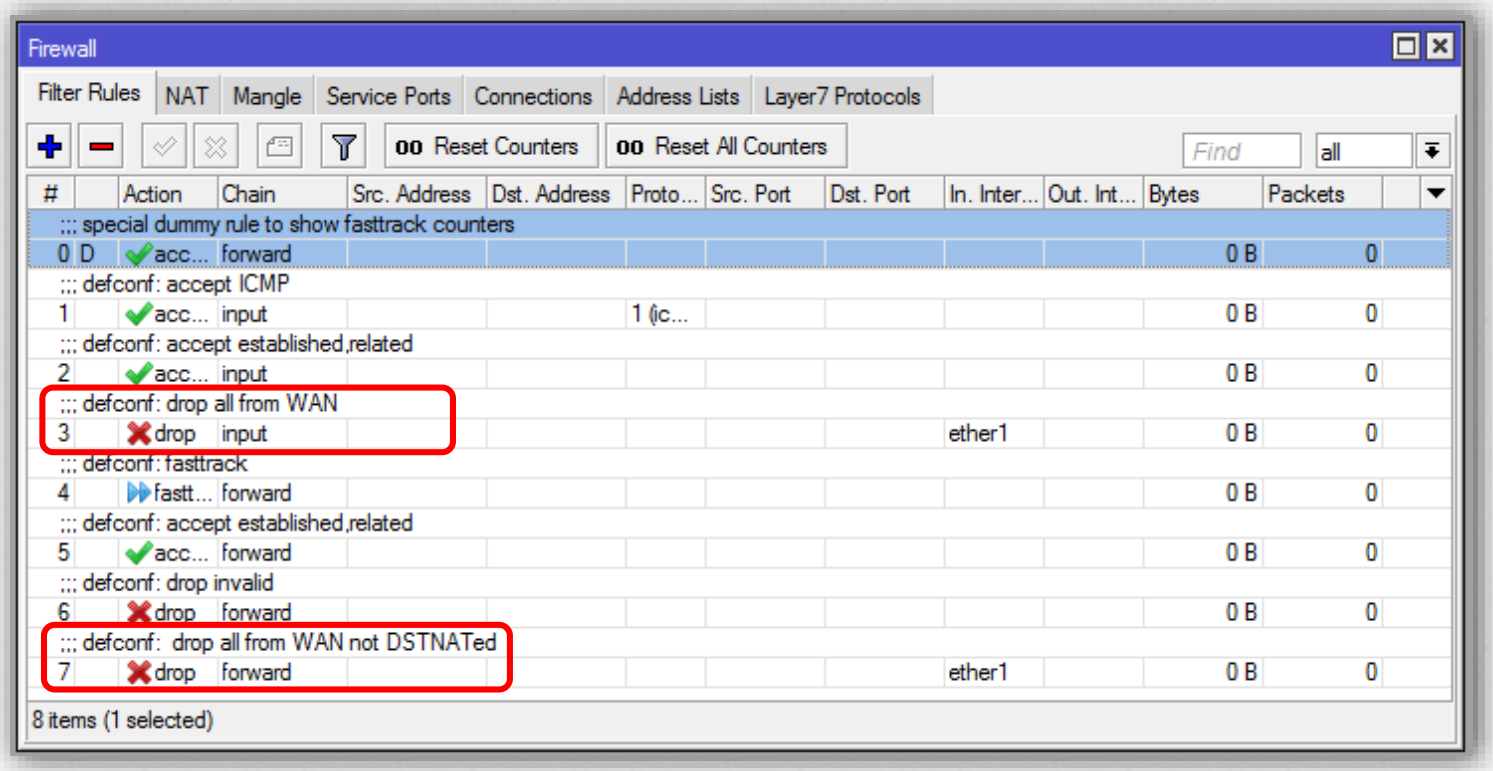
Рассматриваемые вопросы

- 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, сетево́й экра́н — это комплекс аппаратных и программных средств в компьютерной сети, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. ©Wikipedia

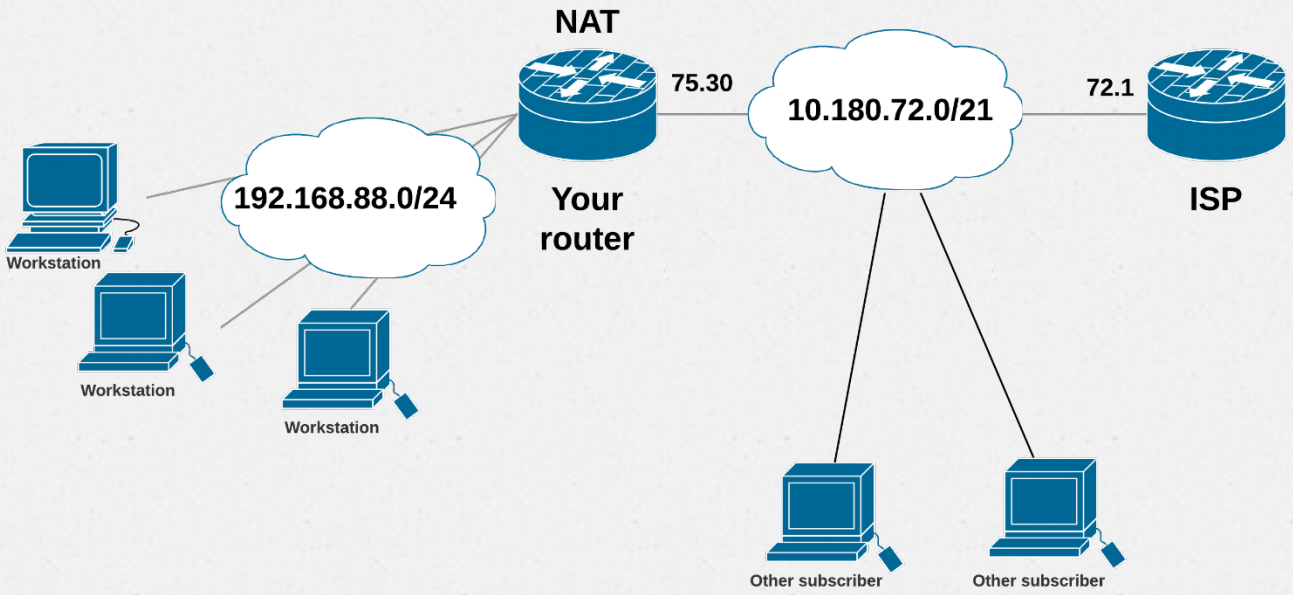
Firewall в конфигурации по умолчанию



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] >
```

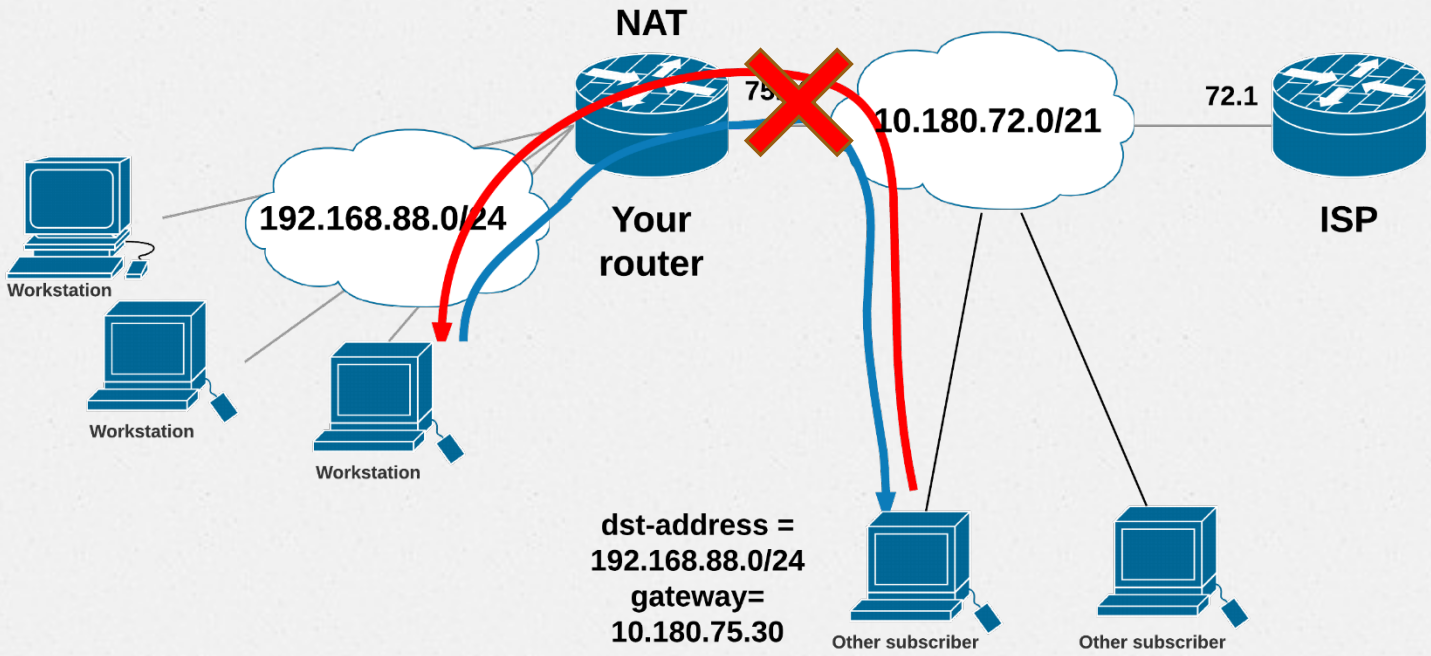
Типичная ситуация:



Защищена ли домашняя сеть от несанкционированного доступа?

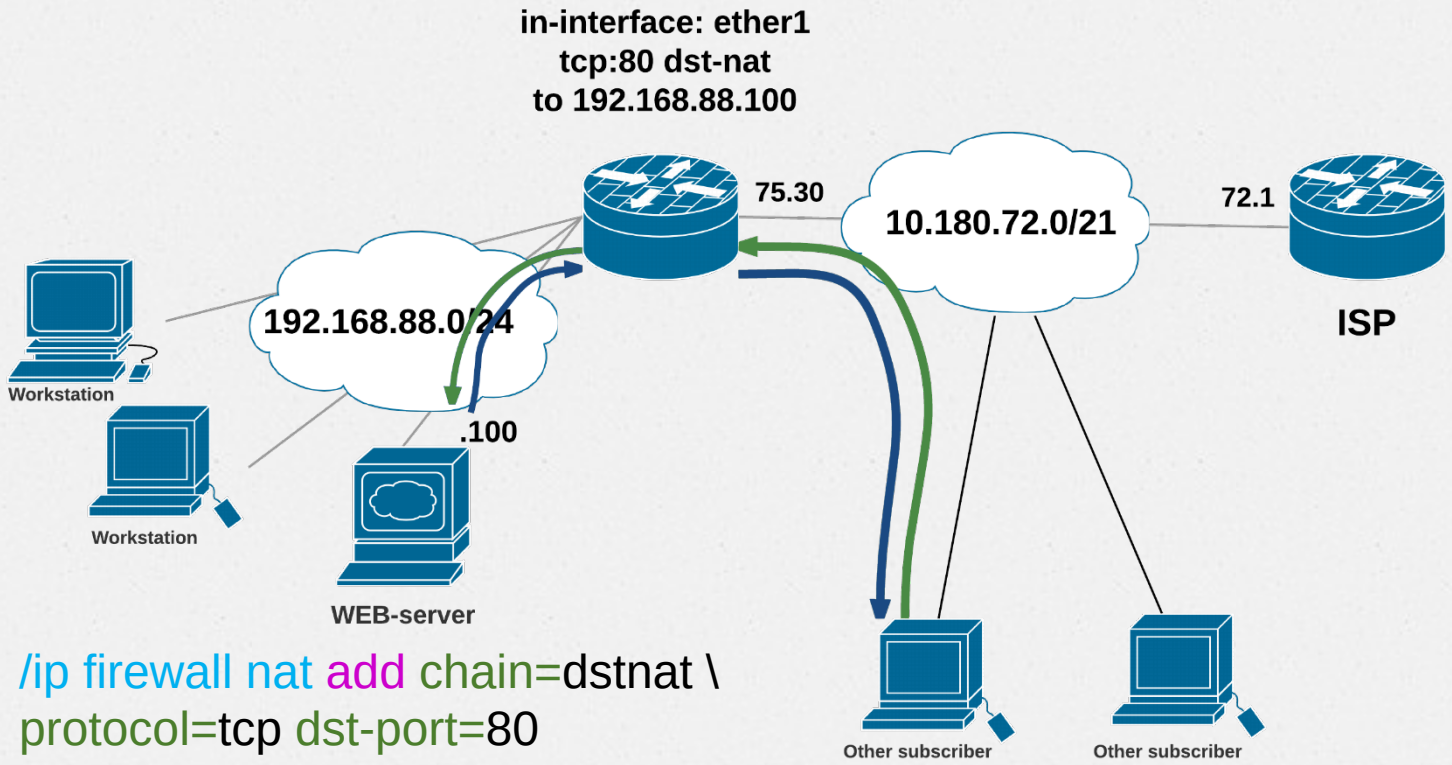
Нет!

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
```

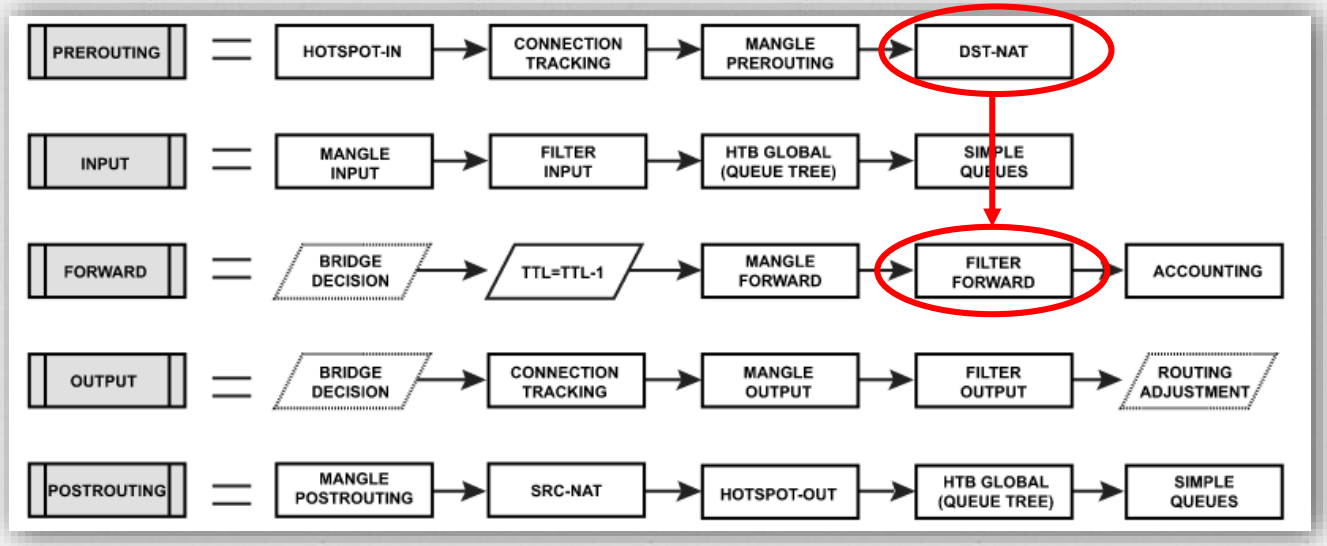
Проброс портов




```
/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



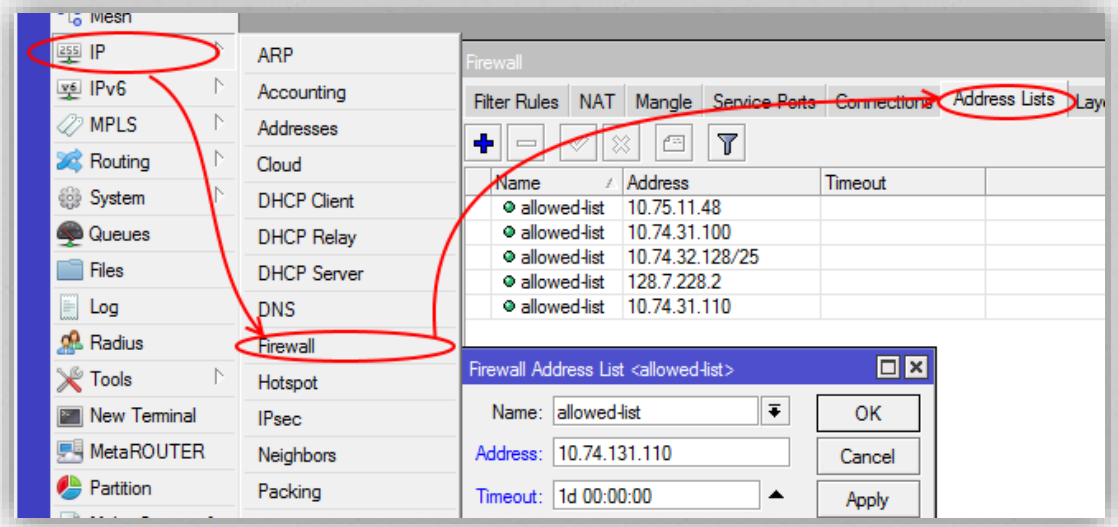
Задача:
разрешить 5 IP-адресам доступ на этот веб-сервер.

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

http://wiki.mikrotik.com/wiki/Manual:Packet_Flow_v6

Адрес-листы: must use!

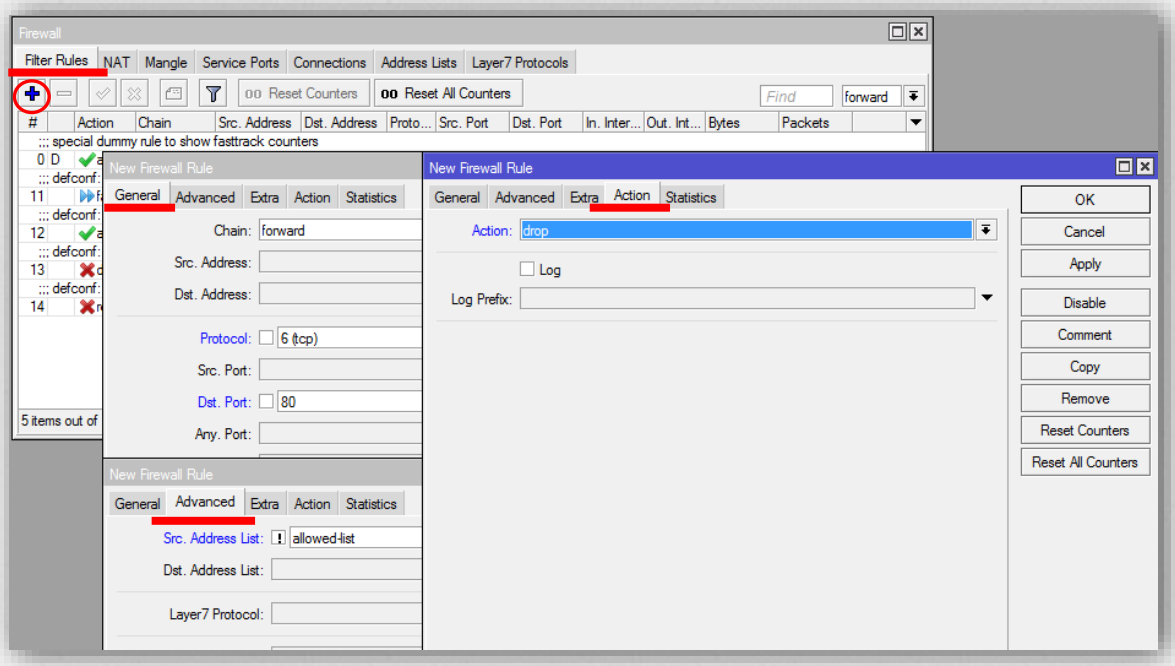
- Легко управляются
- Сокращают количество правил в firewall
- Можно создавать динамические записи



/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"
```

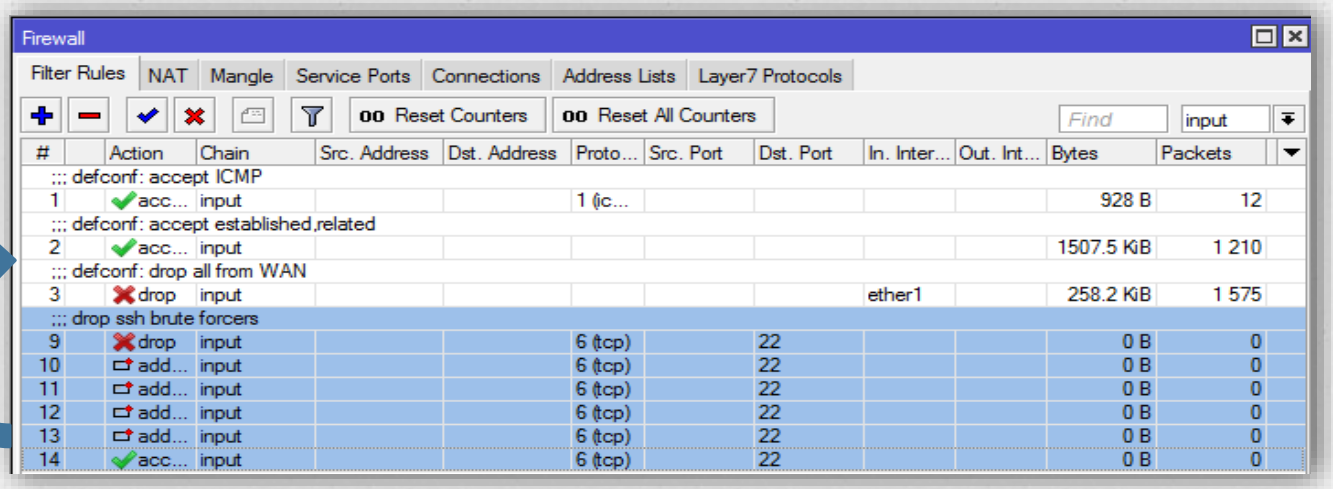
Защита от перебора паролей

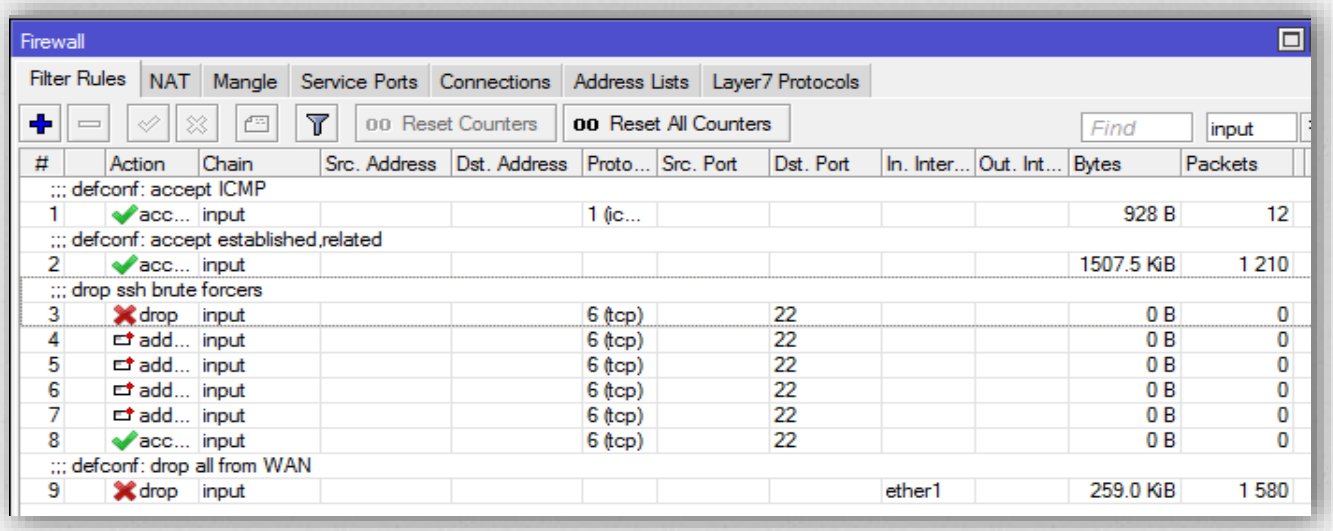
/ip firewall filter

```
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



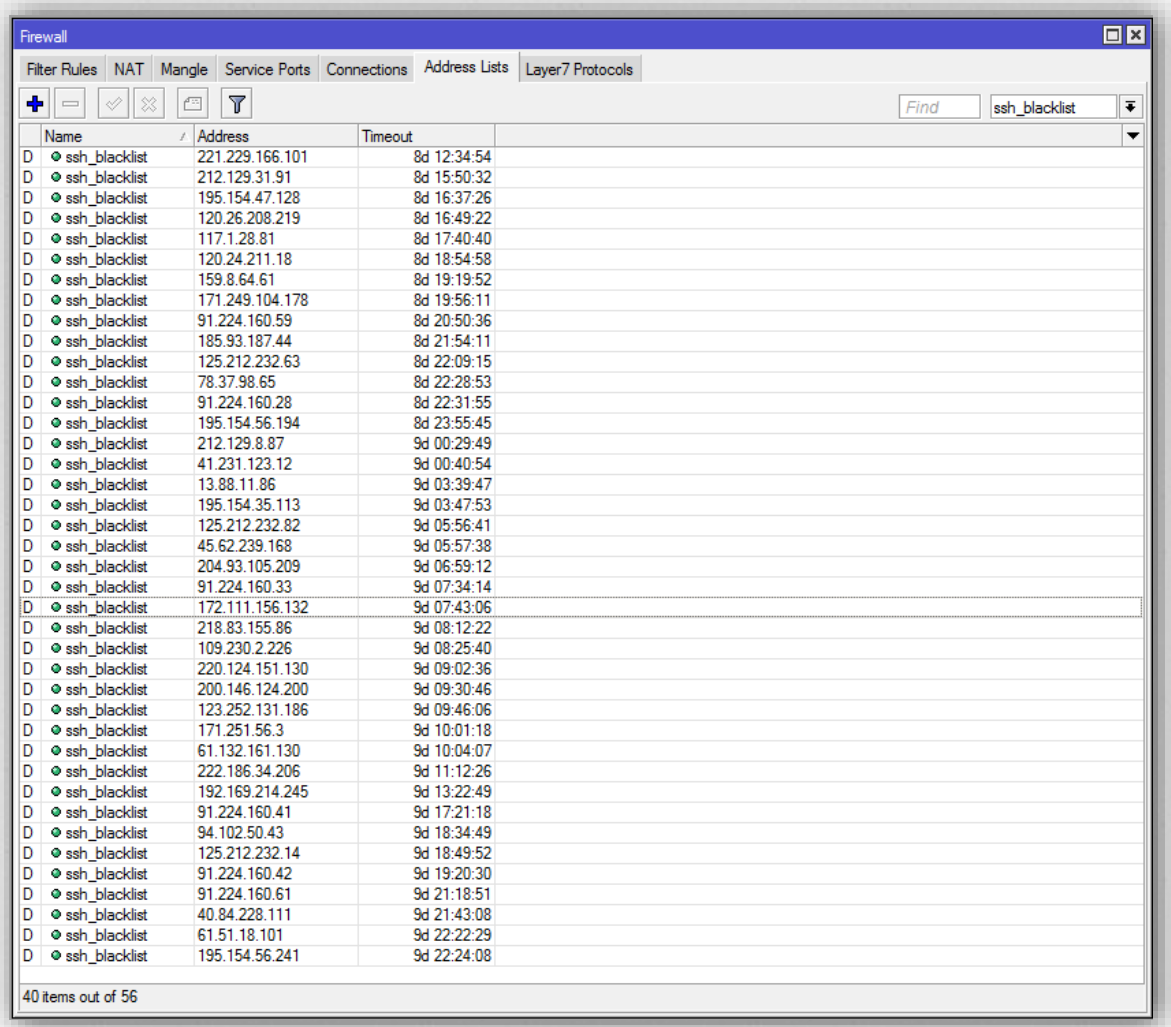


Работает ли это?

Uptime:

1d 12:02:21

40 адресов!



	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

Блокировка сайтов в firewall

Пример: хотим заблокировать vk.com

- 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
```

- 2 попытка (чуть лучше):

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

- 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.

- 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
```

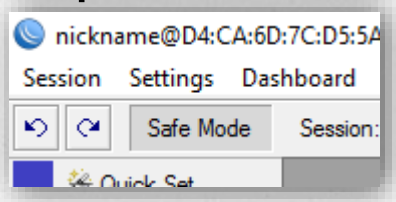
- Попытка 5 (похожа, тоже удачная):

```
/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*.

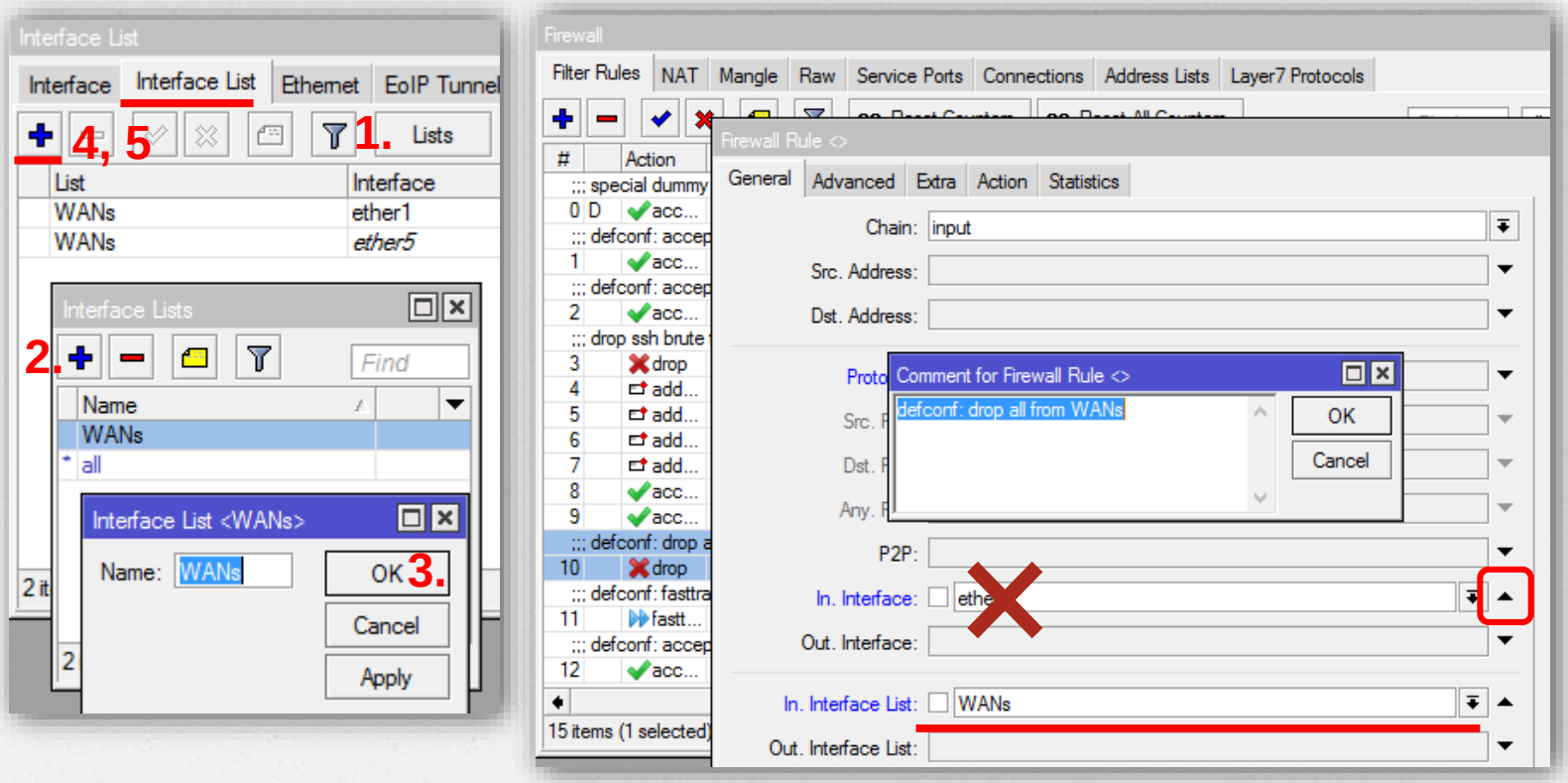
Что мы увидим в ближайшее время?

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

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

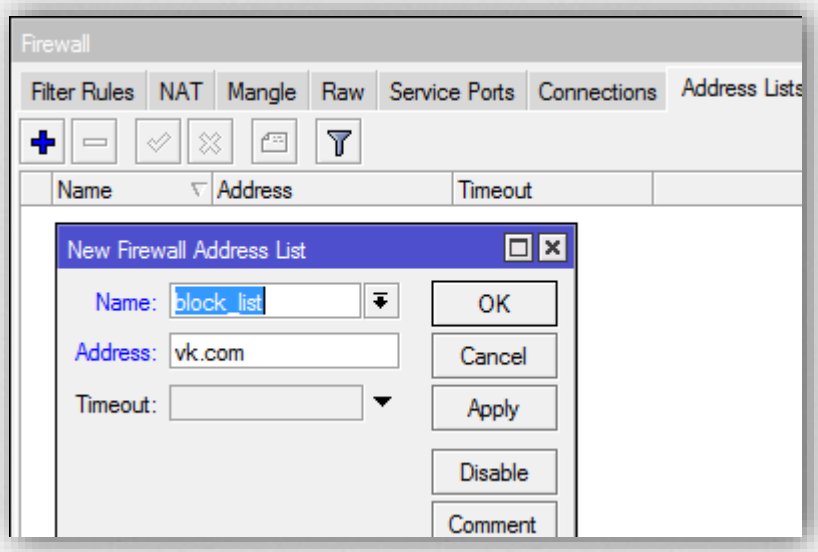
Список интерфейсов

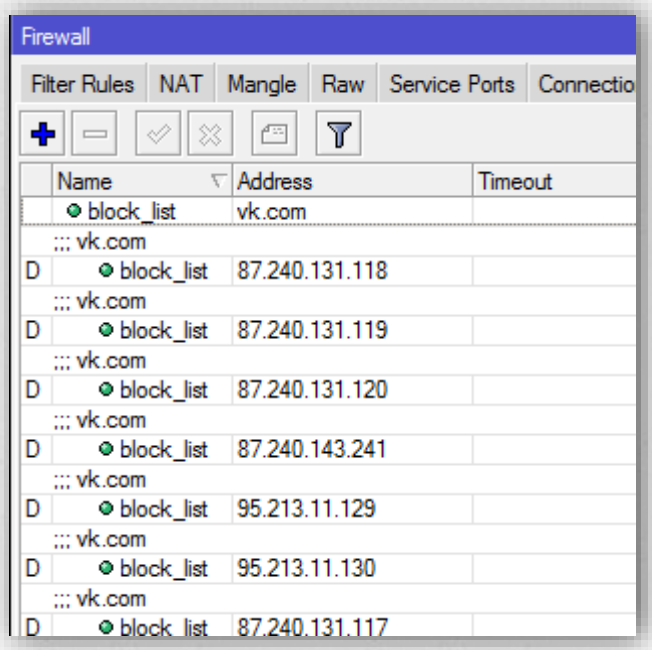
- Одно правило будет работать для нескольких интерфейсов => нужно меньше правил!



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
- Как облегчить жизнь самому себе? (Полезные советы и Best Practice)
- 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:

- Устройства … беспроводной передачи данных **внутри закрытых помещений** в полосе 2400-2483,5 МГц **с максимальной … излучаемой мощностью передатчика не более 100 мВт…**
- 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

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

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

band

- **2** - 2.4Ghz

power per chain

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

protocol

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

number_of_chains

- **D** - dual chain

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

Wi-Fi: в рамках закона

- По умолчанию:

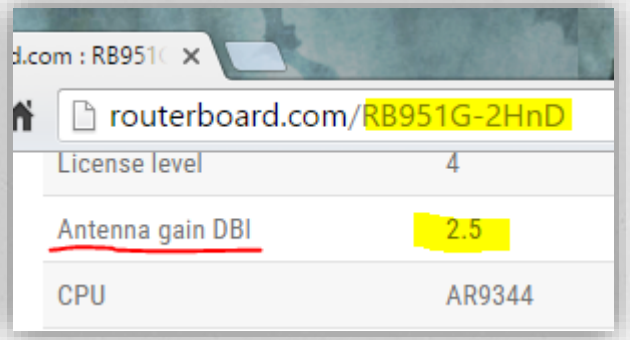
Interface <wlan1>

WDS | Nstreme | Tx Power | Current Tx Power

Current Tx Powers

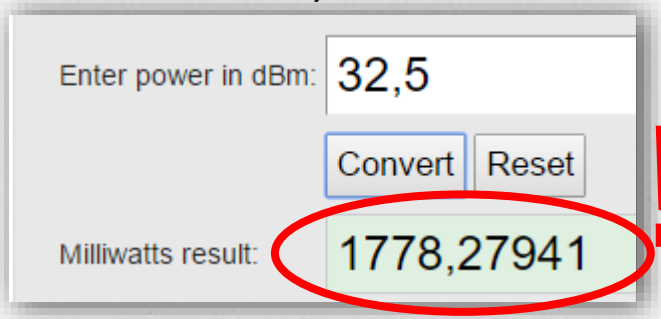
Rate	Tx Power	Total Tx ...
1Mbps	26dBm	29dBm
2Mbps	26dBm	29dBm
5.5Mbps	26dBm	29dBm
11Mbps	25dBm	28dBm
6Mbps	27dBm	30dBm
9Mbps	27dBm	30dBm
12Mbps	27dBm	30dBm
18Mbps	27dBm	30dBm
24Mbps	27dBm	30dBm
36Mbps	25dBm	28dBm
48Mbps	23dBm	26dBm
54Mbps	22dBm	25dBm
HT20-0	27dBm	30dBm
HT20-1	26dBm	29dBm
HT20-2	26dBm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

- Коэф. усиления:



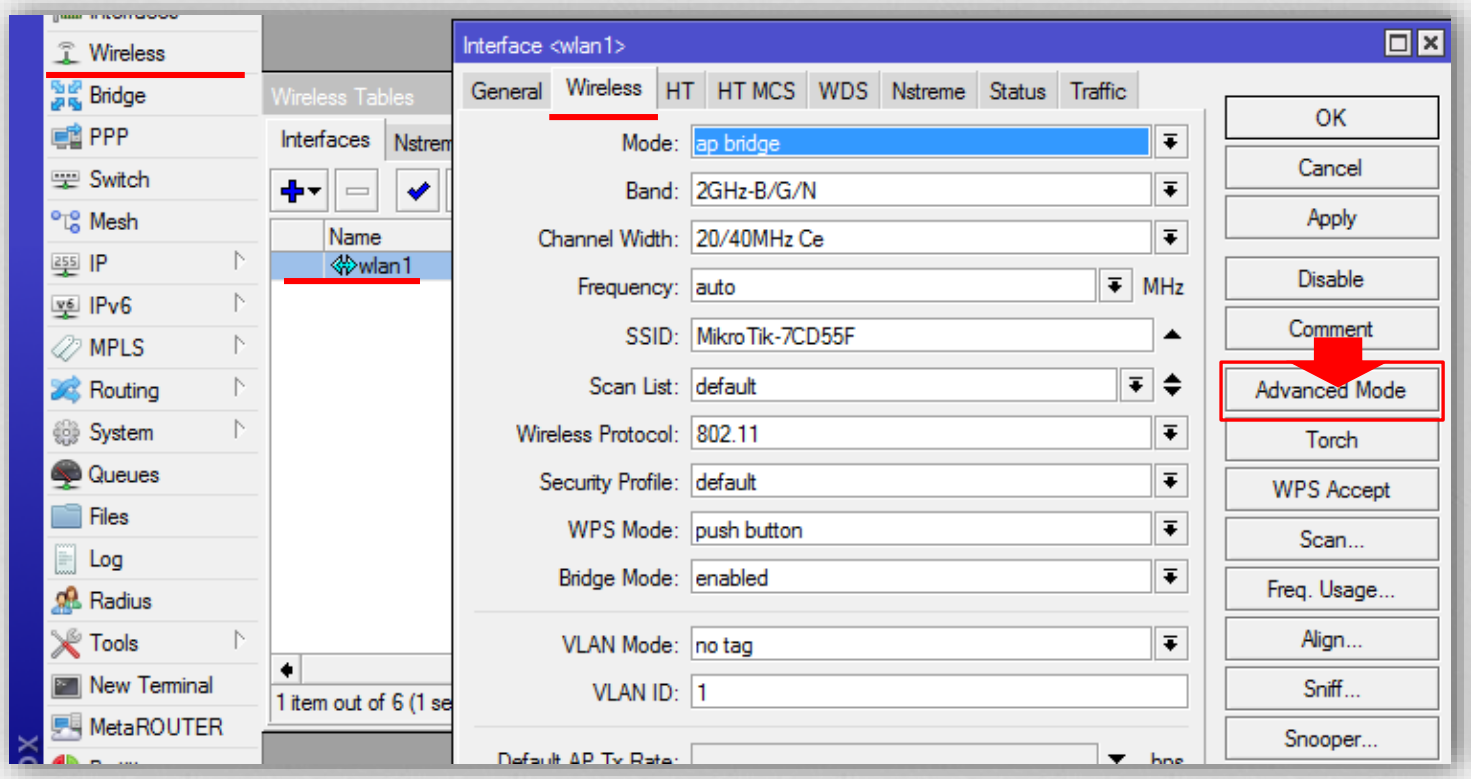
- Общая мощность равна dBm+dBi =

32,5 dBm =

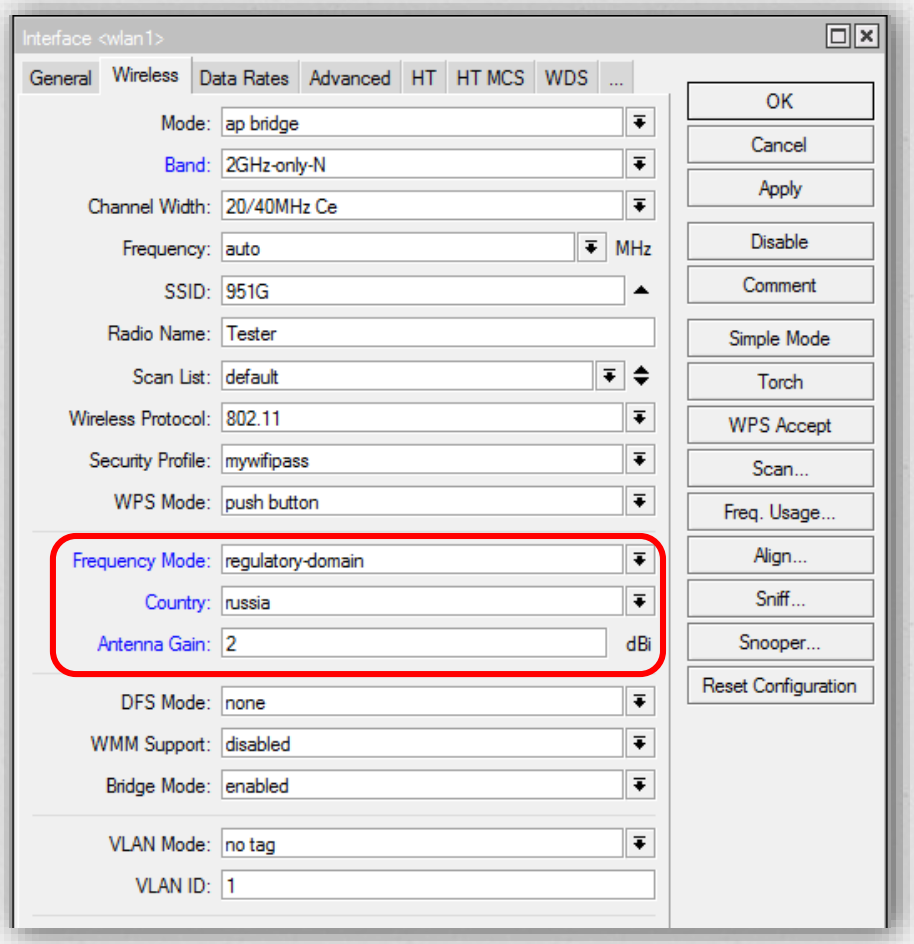


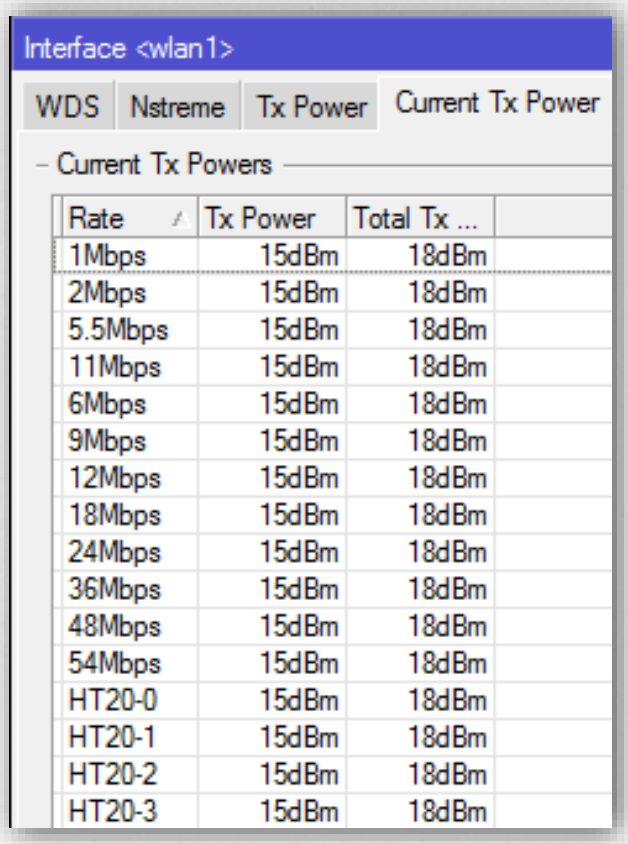
!!!

Wi-Fi: в рамках закона



Wi-Fi: в рамках закона

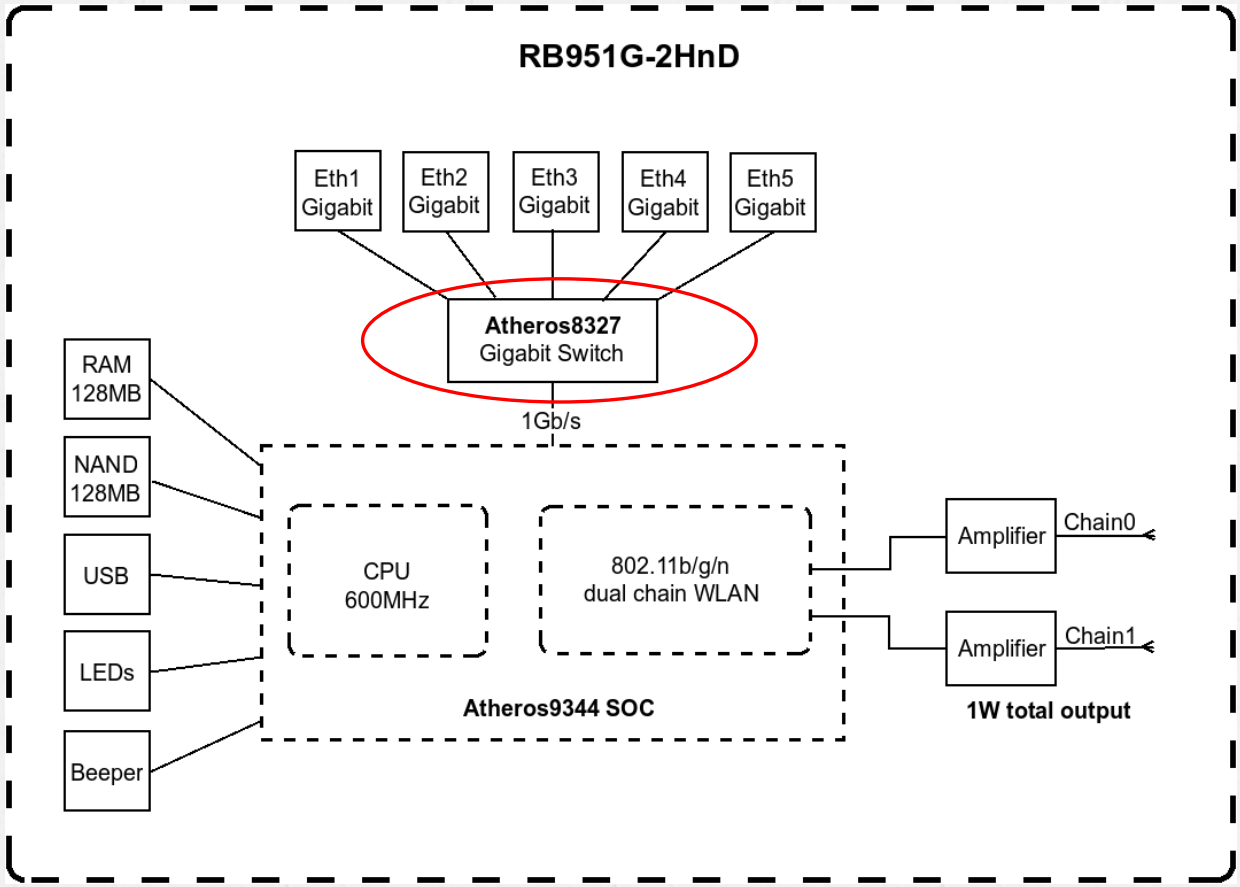




Rate	Tx Power	Total Tx ...
1Mbps	15dBm	18dBm
2Mbps	15dBm	18dBm
5.5Mbps	15dBm	18dBm
11Mbps	15dBm	18dBm
6Mbps	15dBm	18dBm
9Mbps	15dBm	18dBm
12Mbps	15dBm	18dBm
18Mbps	15dBm	18dBm
24Mbps	15dBm	18dBm
36Mbps	15dBm	18dBm
48Mbps	15dBm	18dBm
54Mbps	15dBm	18dBm
HT20-0	15dBm	18dBm
HT20-1	15dBm	18dBm
HT20-2	15dBm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

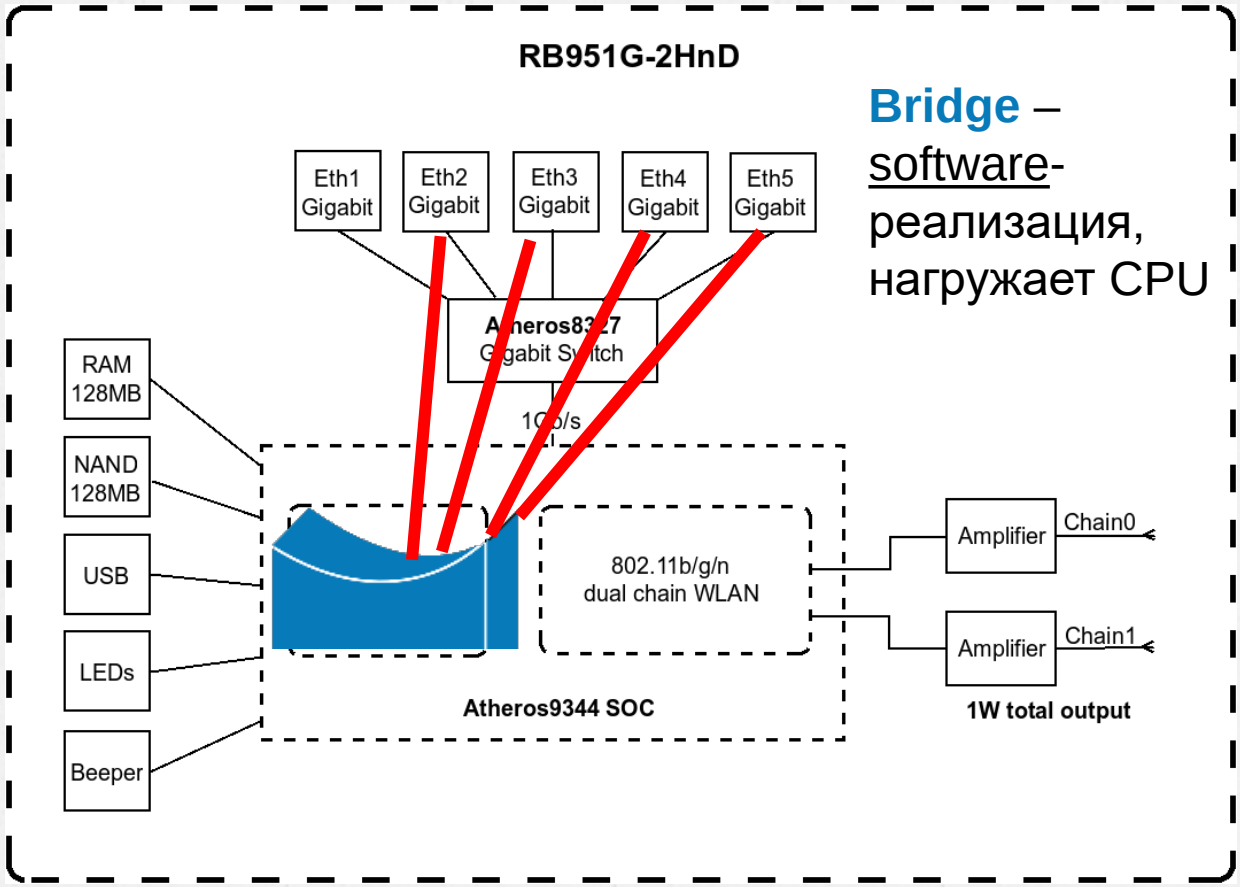
20dBm=100mW =)

Best Practice. Bridge vs Switch



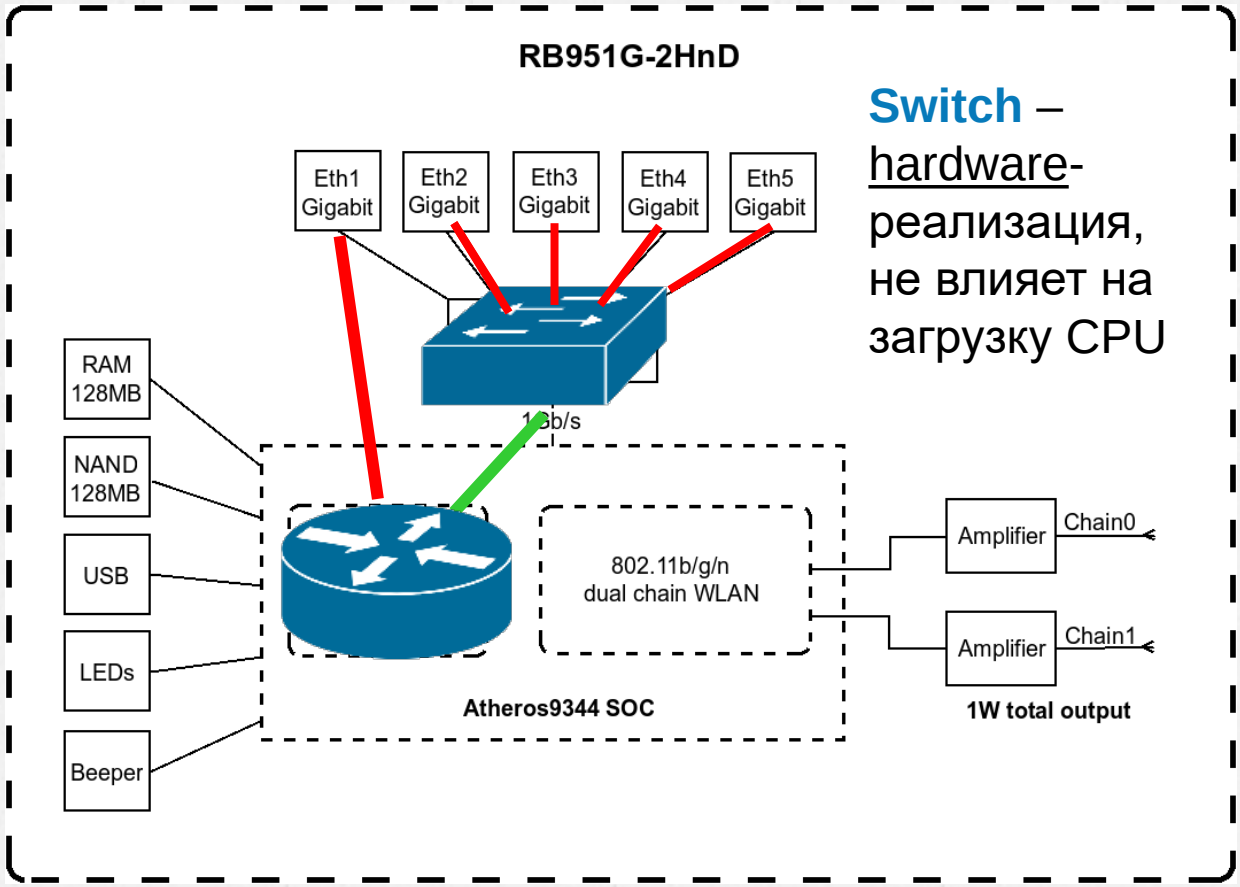
Блок-диаграмма взята с **routerboard.com**

Best Practice. Bridge vs Switch



Блок-диаграмма взята с **routerboard.com**

Best Practice. Bridge vs Switch



Switch – hardware-реализация, не влияет на загрузку CPU

Блок-диаграмма взята с **routerboard.com**

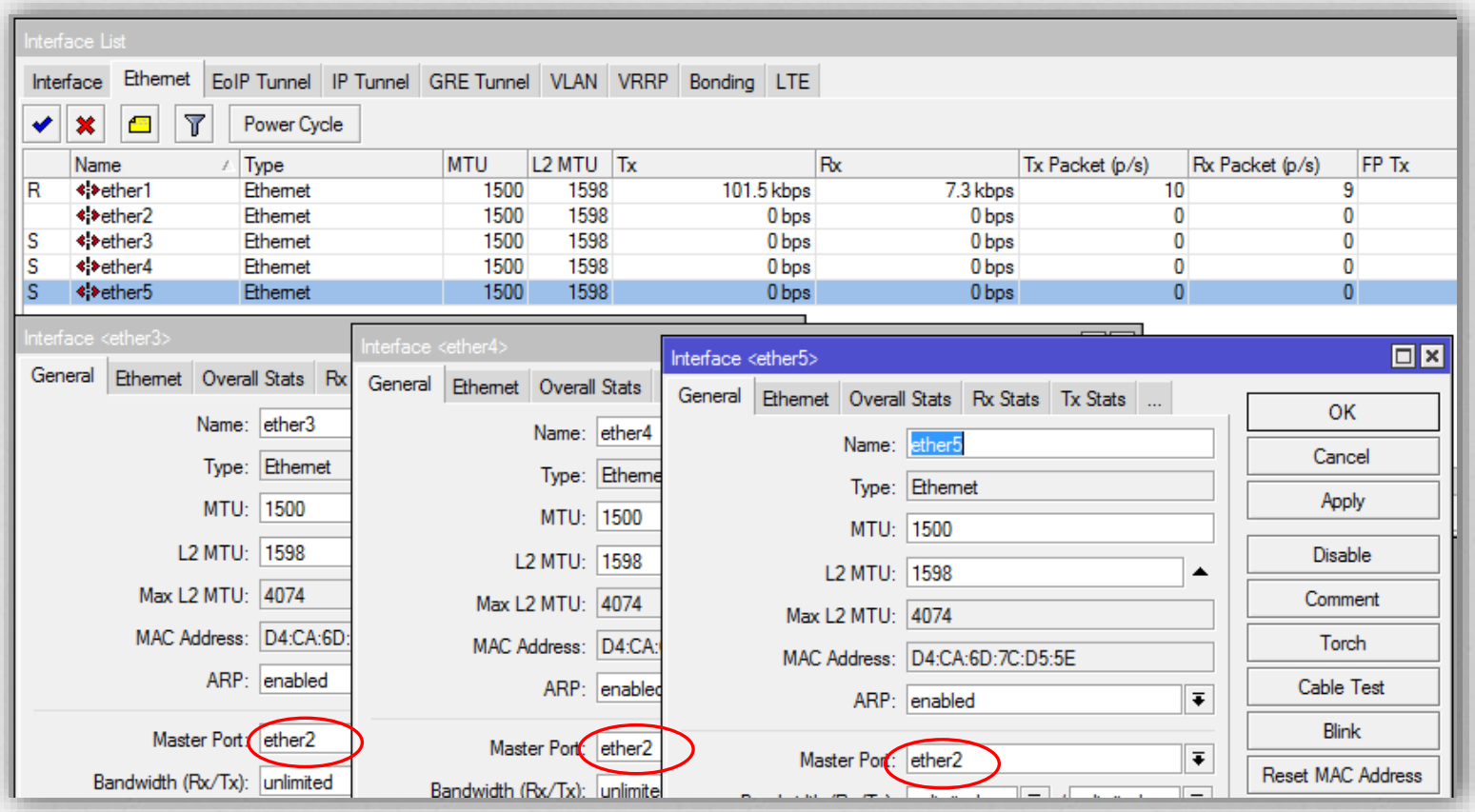
Best Practice. Bridge vs Switch

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

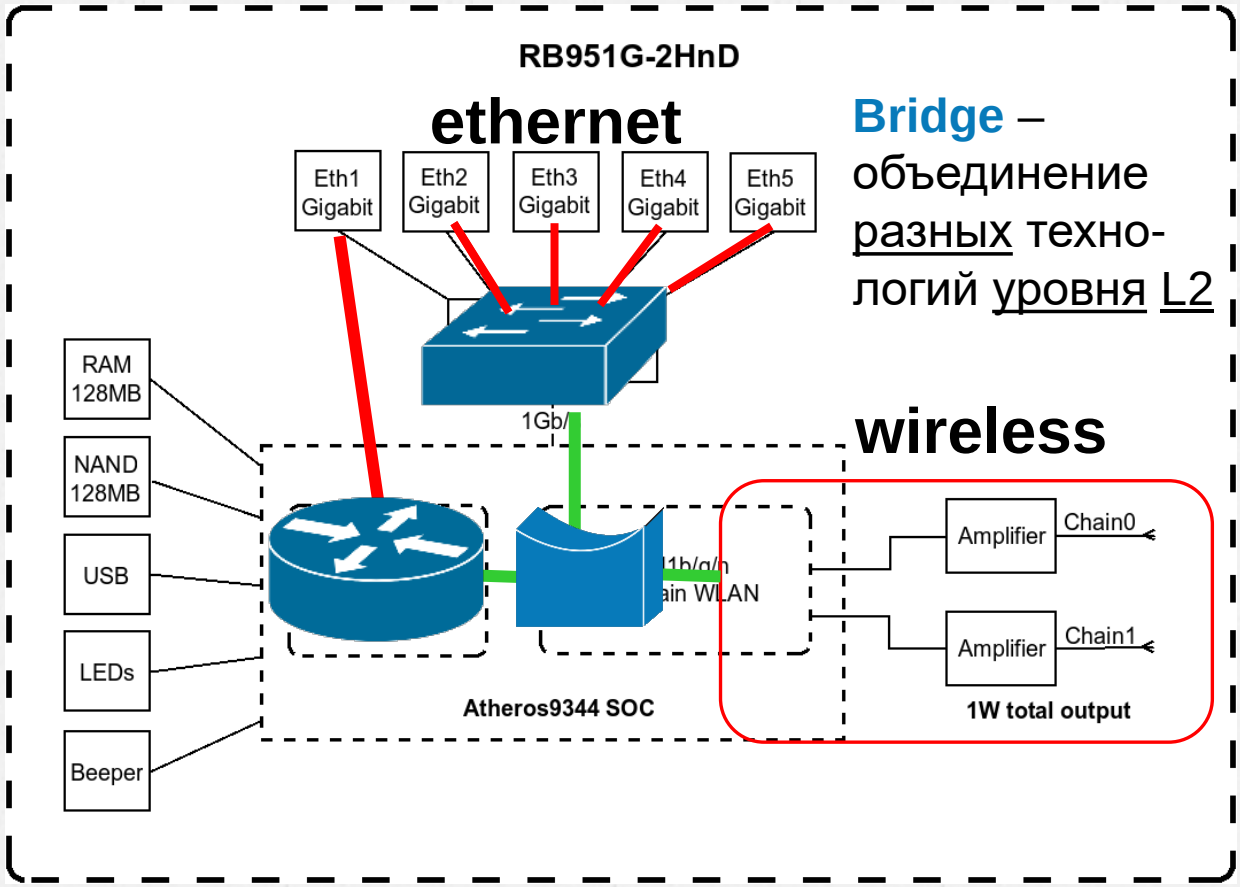
```
[nickname@Test router] > interface ethernet print
Flags: X - disabled, R - running, S - slave
 #    NAME                        MTU MAC-ADDRESS       ARP        MASTER-PORT
 0 R  ;;; internet
      ether1                     1500 D4:CA:6D:7C:D5:5A enabled    none
 1    ether2                     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:

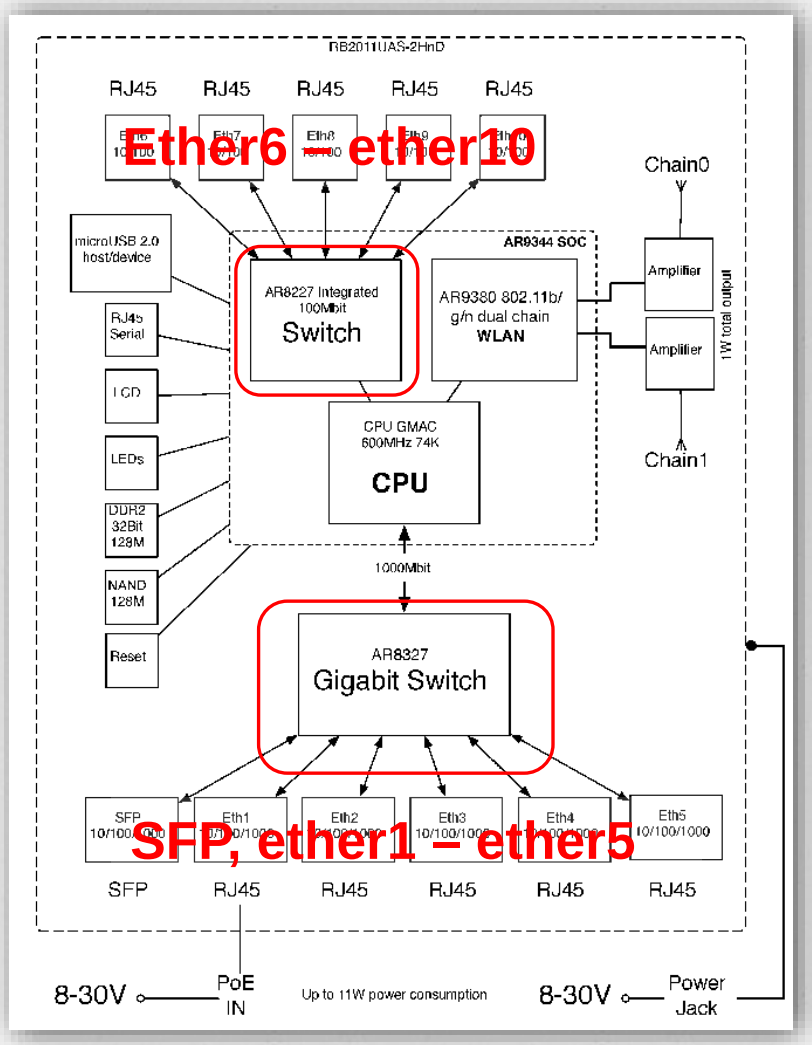


Best Practice. Bridge vs Switch



Блок-диаграмма взята с **routerboard.com**

Best Practice. Bridge vs Switch

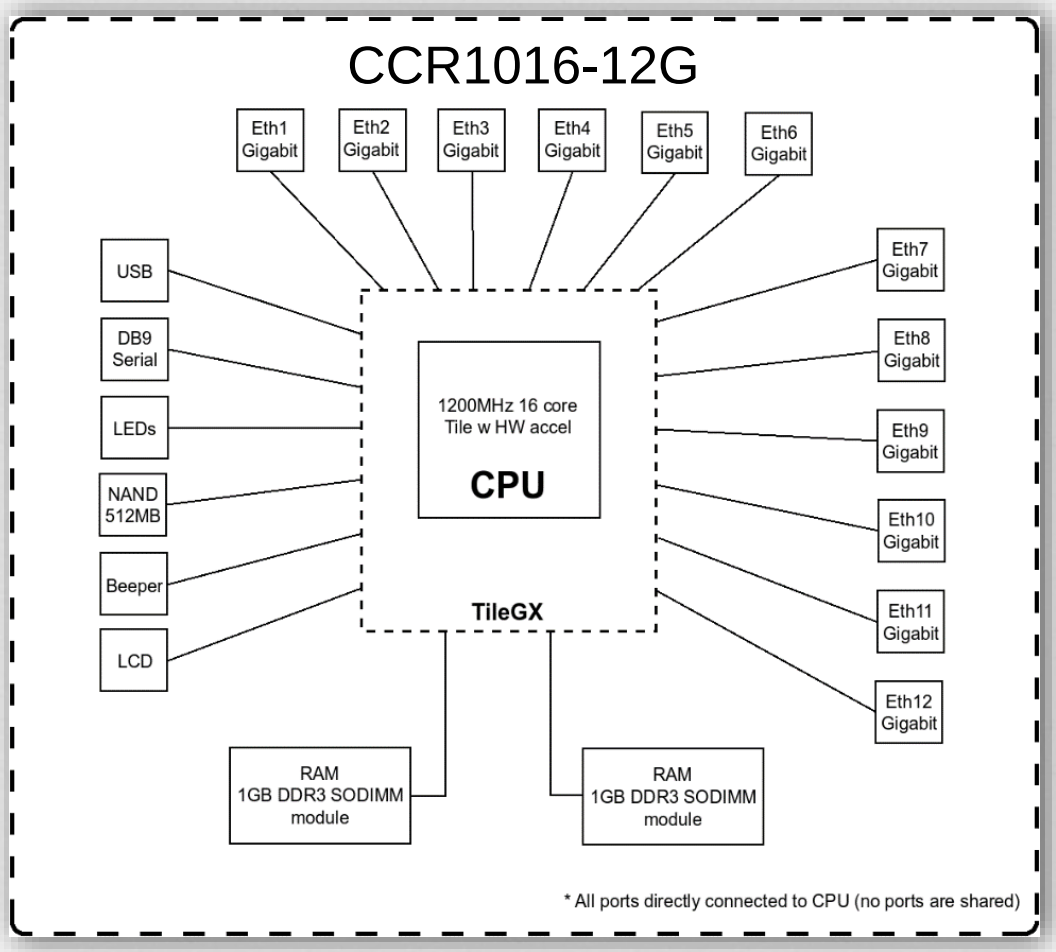


RB2011 series
2 свитч-чипа –
два мастер-порта.

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

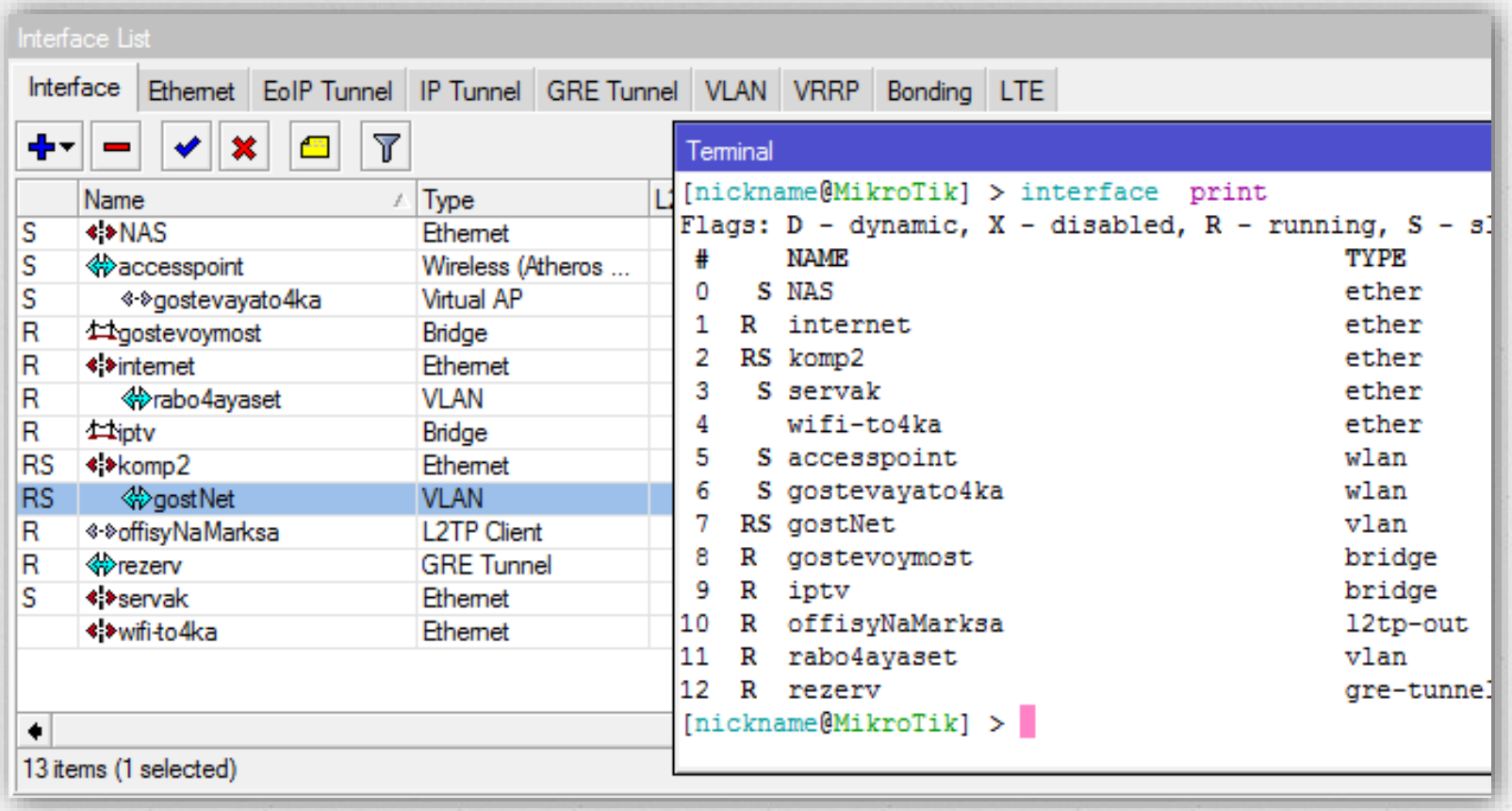
Optimal configuration:
6: Master-port
7,8,9,10: Slaves of 6
2: Master-port
3,4,5: Slaves of 2
2,6: Bridged

Best Practice. Bridge vs Switch

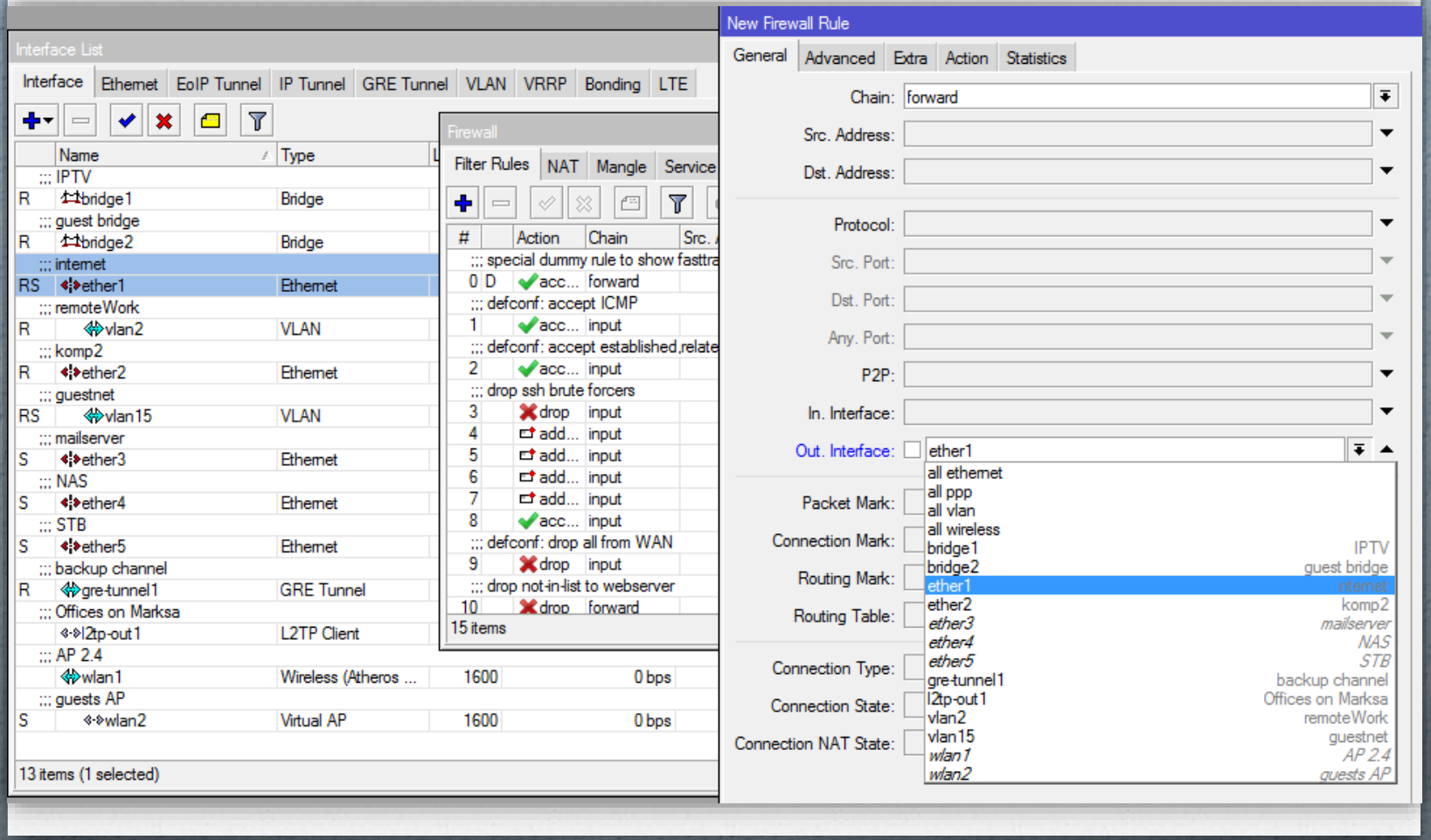


Выбирайте модель под свои нужды внимательно. Не во всех есть switch-chip.

Имена интерфейсов или комментарии?

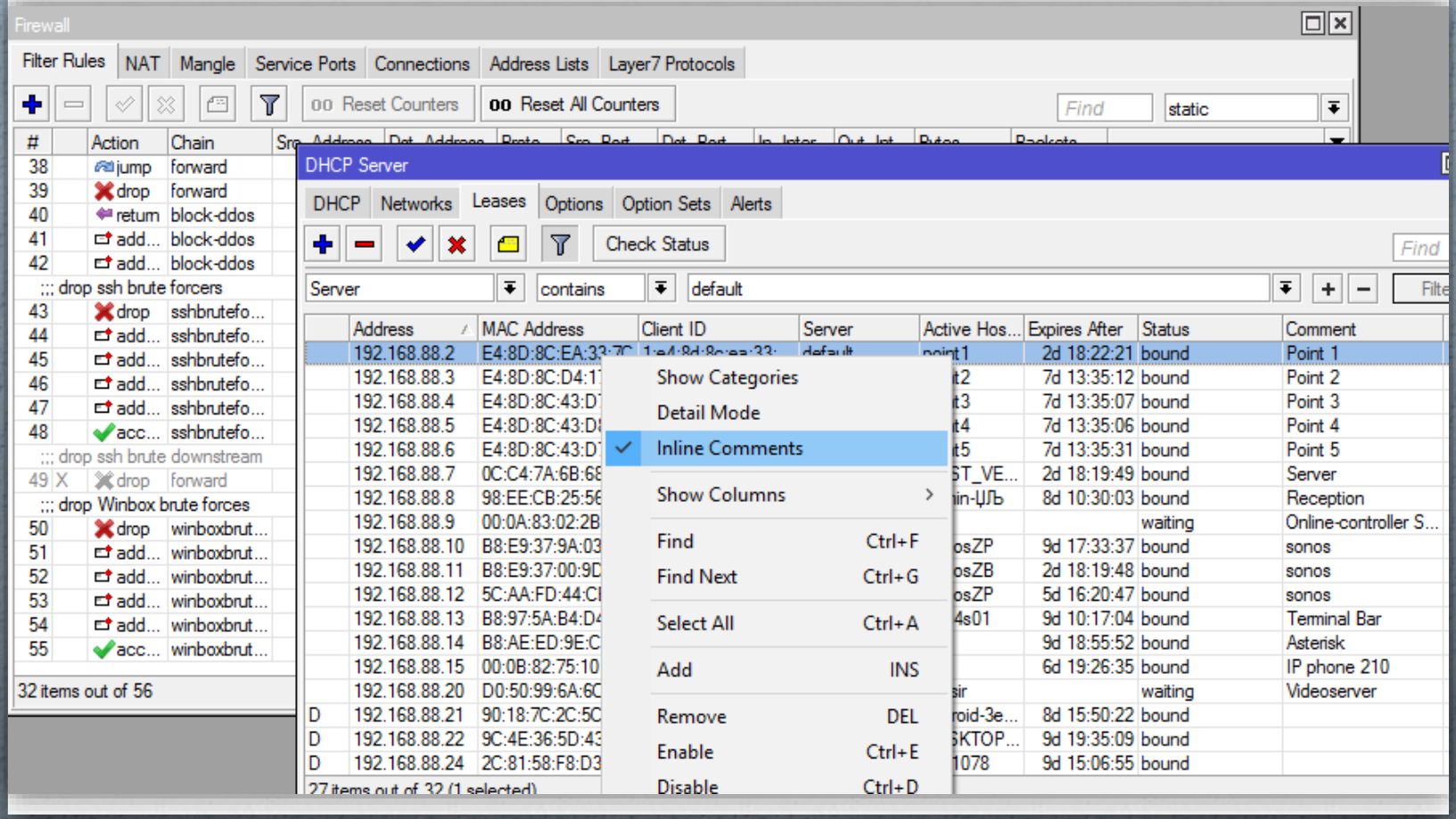


Имена интерфейсов или комментарии?



Обычные и inline-комментарии

Используйте удобное вам отображение в каждом окне



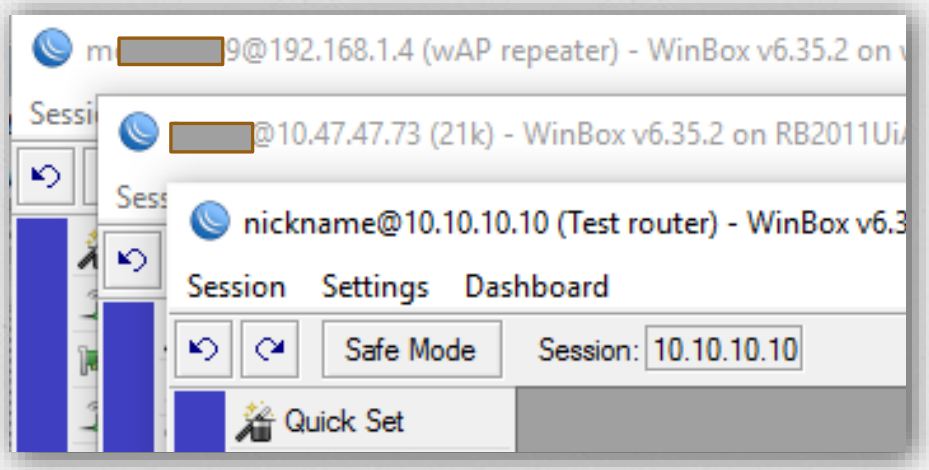
Identity – ваша страховка

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

/system identity set name=“Test router”

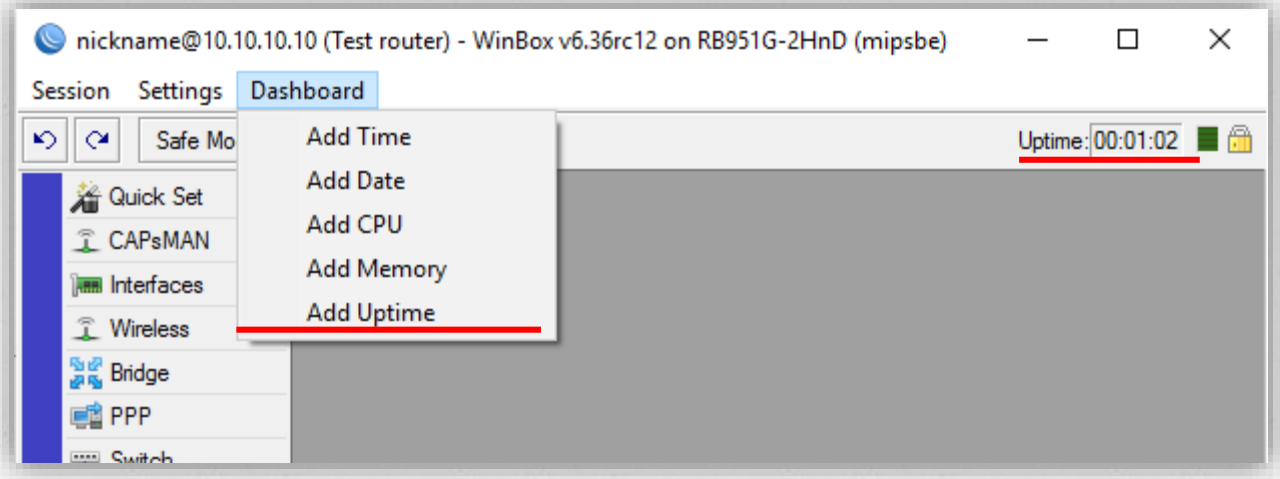
Либо в winbox

System-Identity



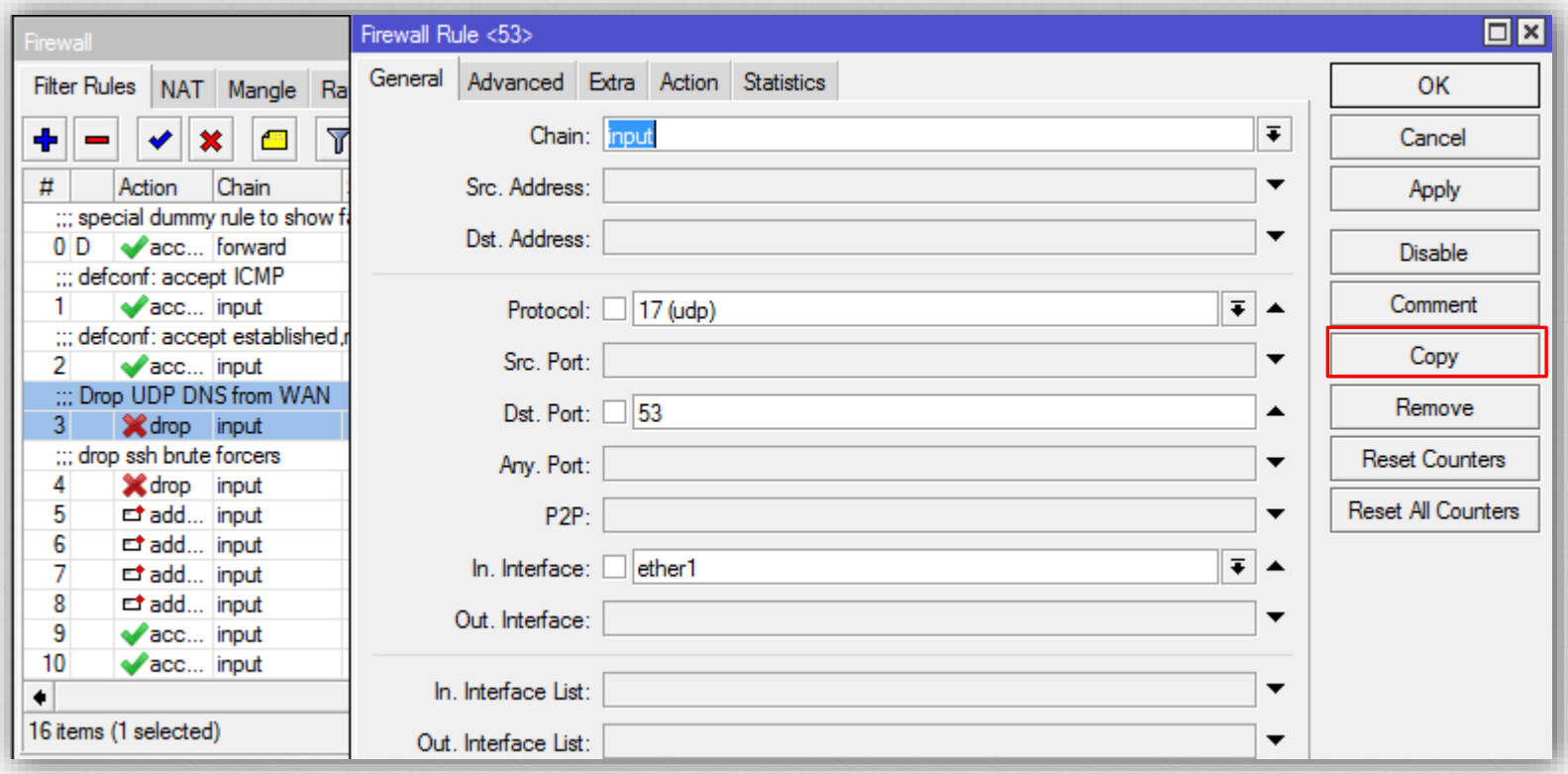
Маленькие полезности

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.



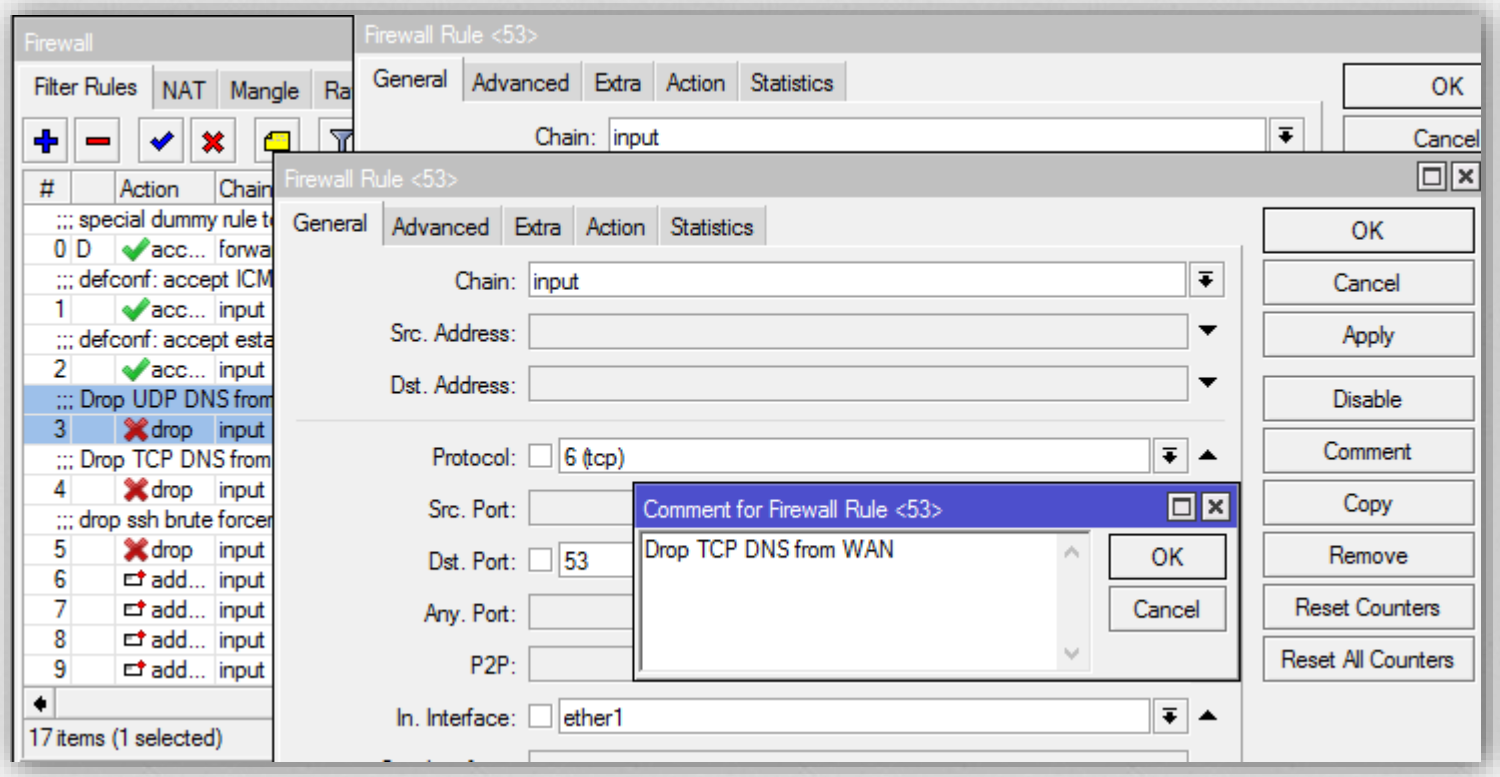
Маленькие полезности

Кнопка “**Copy**” часто незаслуженно забывается.

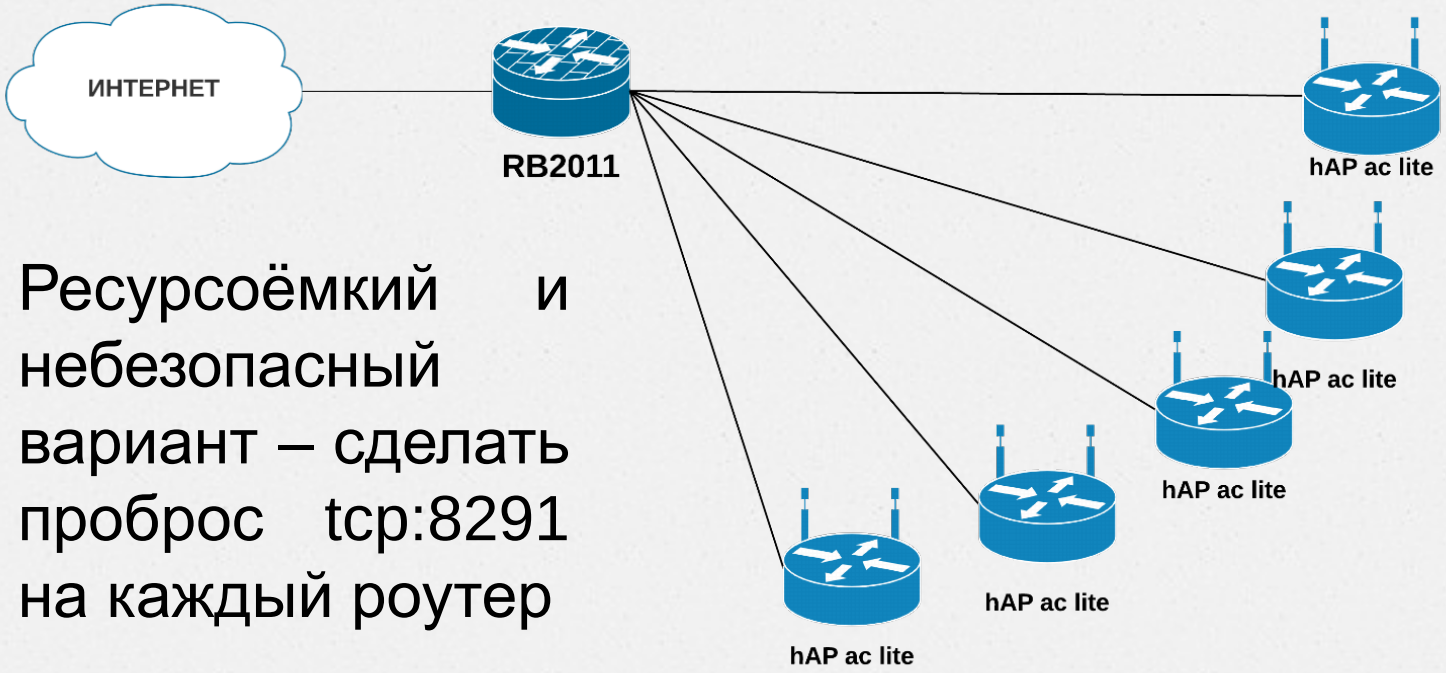


Маленькие полезности

Кнопка “**Copy**” упрощает настройку.



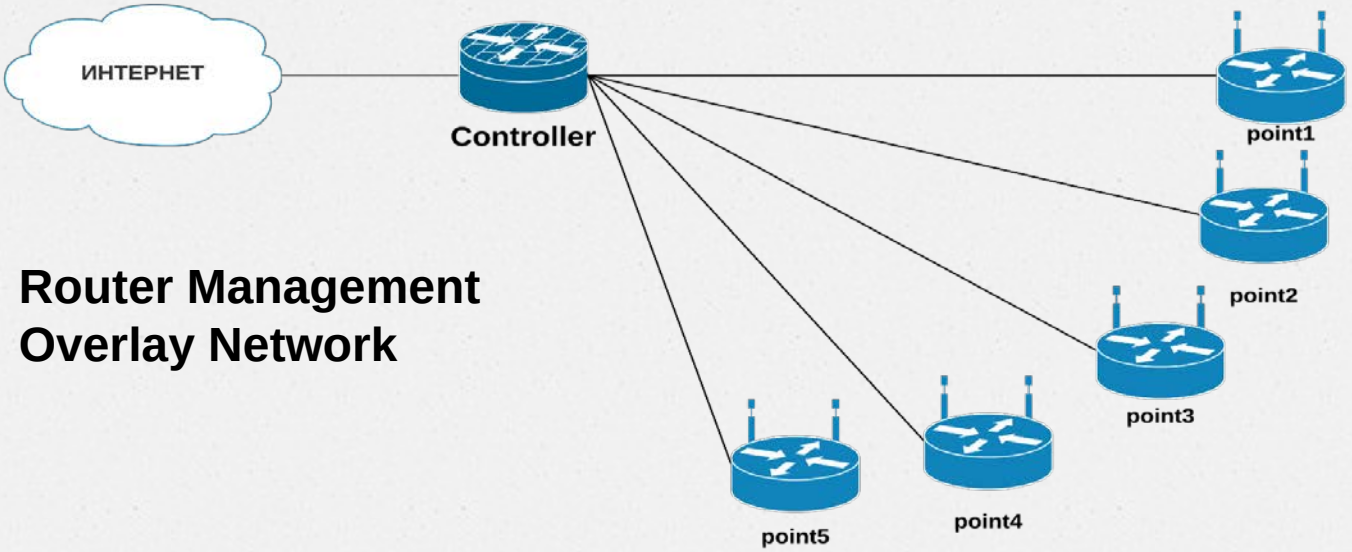
Задача: управление всеми роутерами из интернета



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

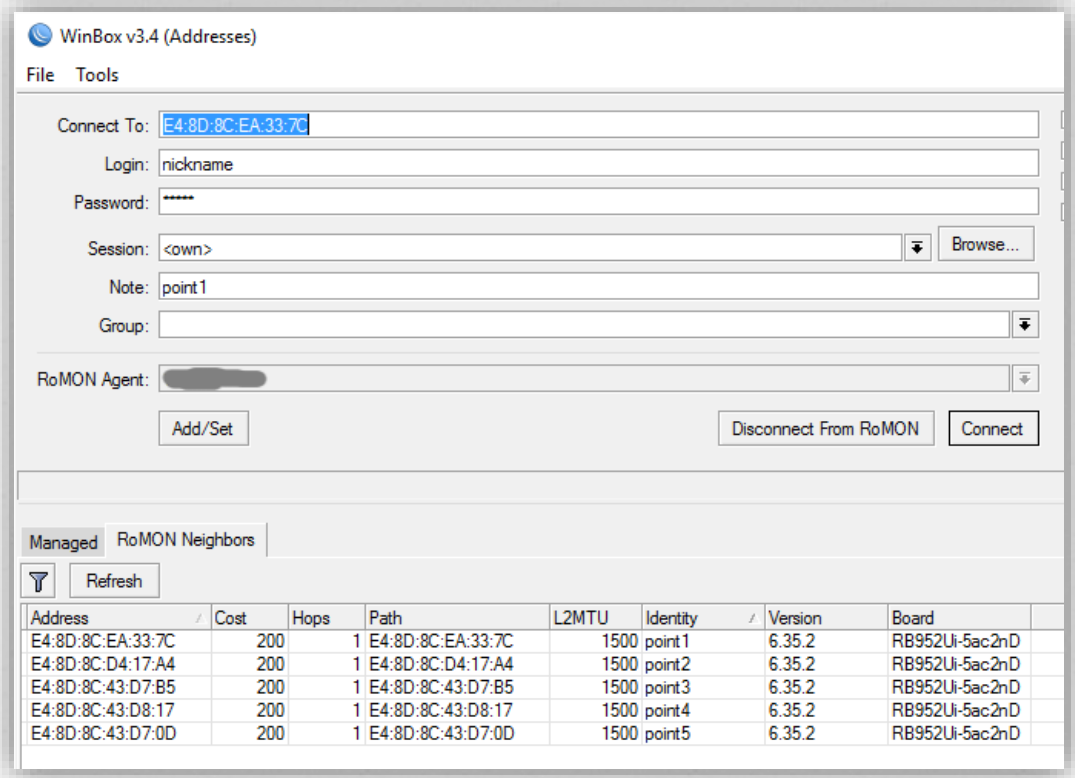
1. Включаем RoMON на всех роутерах и задаём секрет

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

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

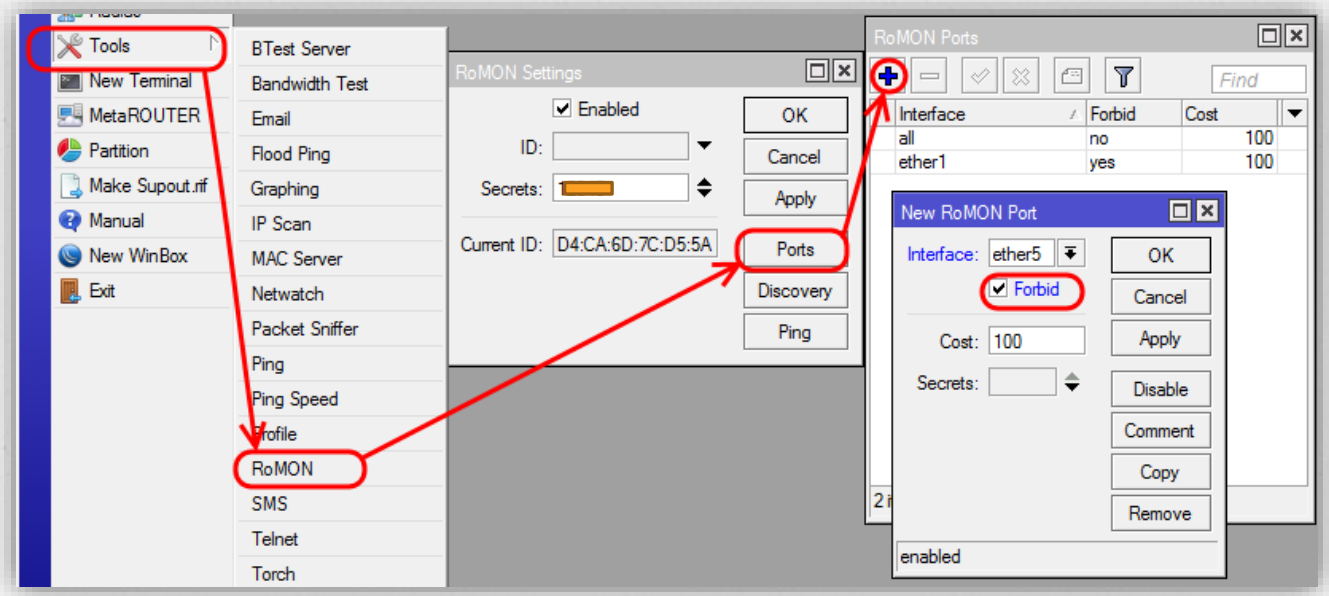
Использование RoMON

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



RoMON работает независимо от конфигураций L2 и L3.

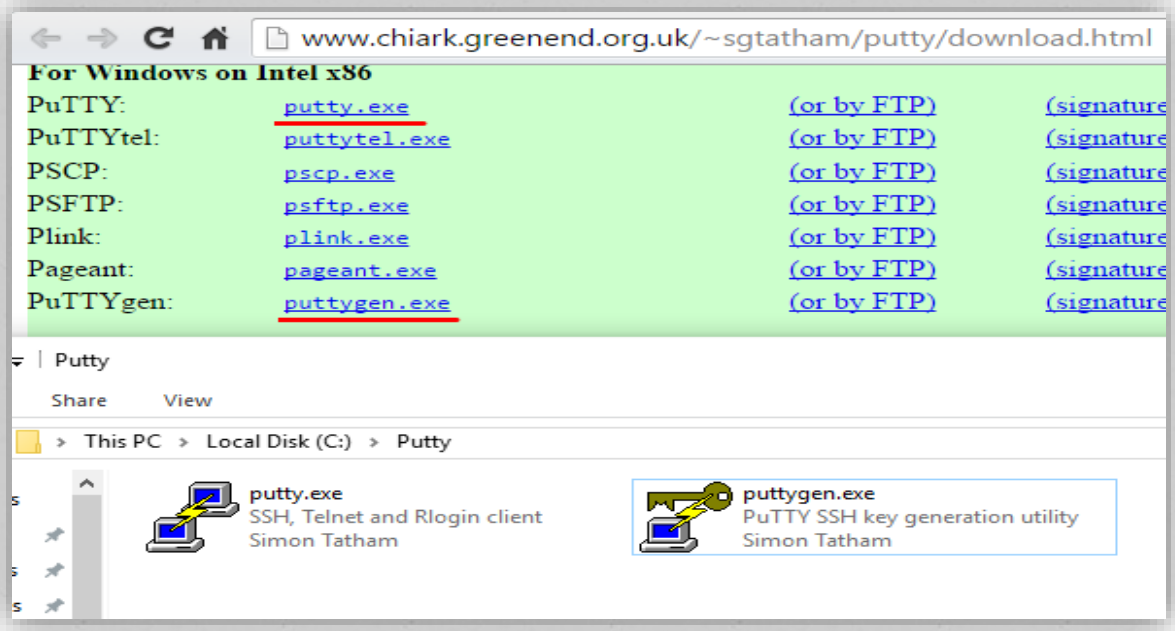
Защита от RoMON-подключений извне




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

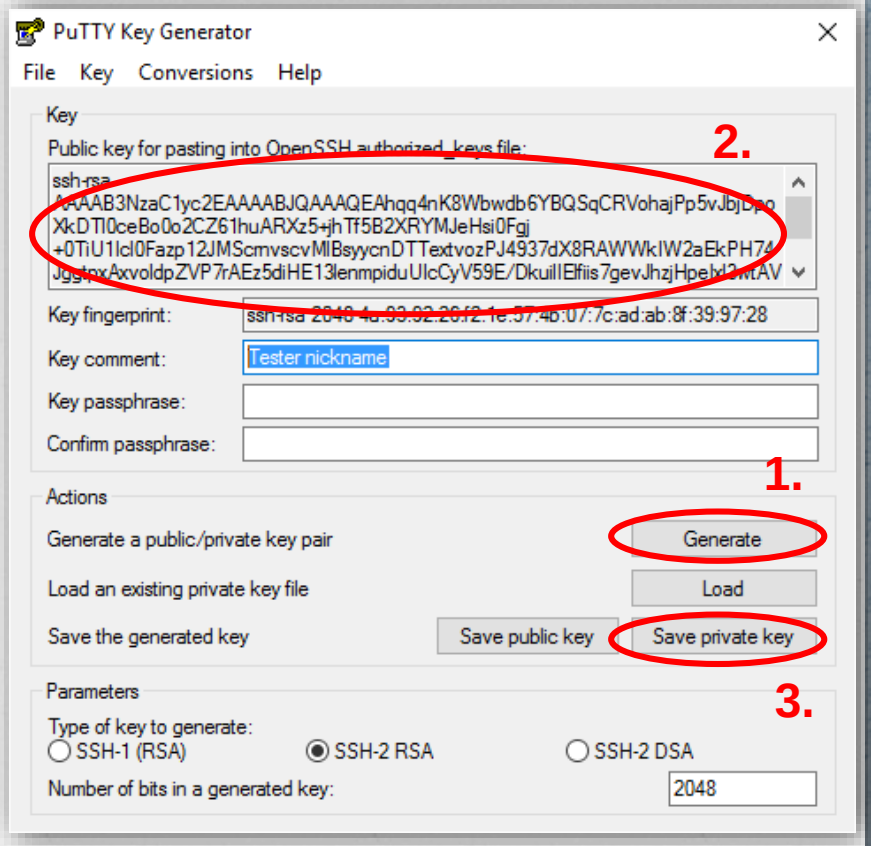
Доступ SSH по ключу

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



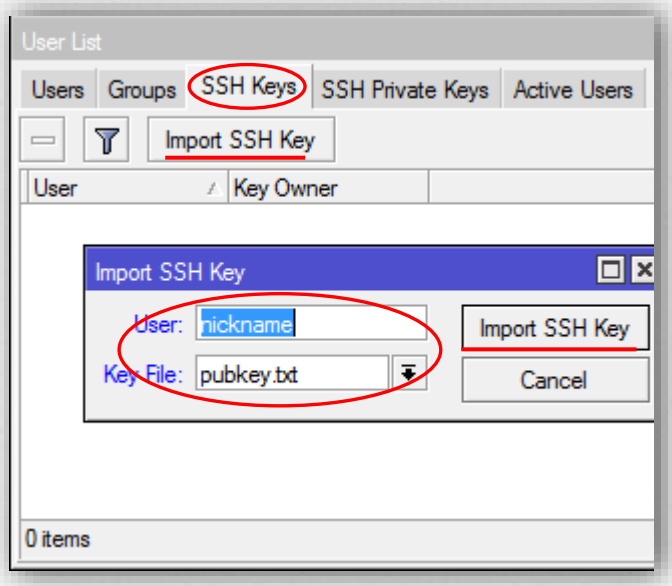
Доступ SSH по ключу

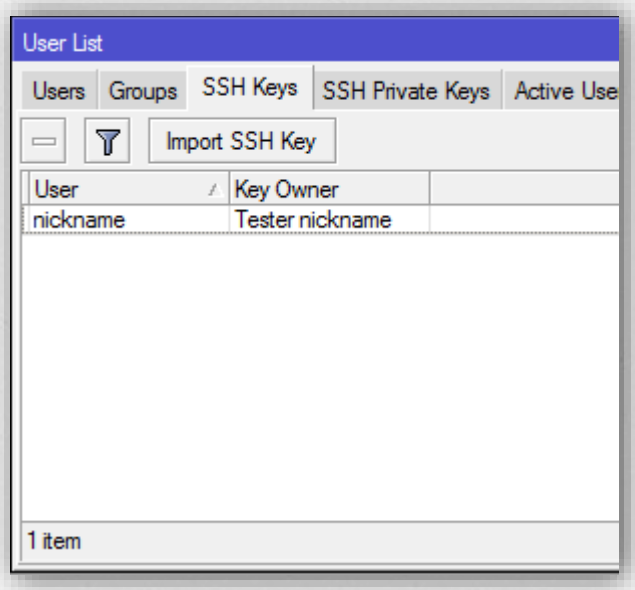
1. Генерируем RSA или DSA ключ длиной 2048 байт (Запускаем puttygen - Generate)
2. Копируем текст публичного ключа в файл и закидываем на роутер (pubkey.txt)
3. Сохраняем приватный ключ в файл .ppk



Доступ SSH по ключу

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

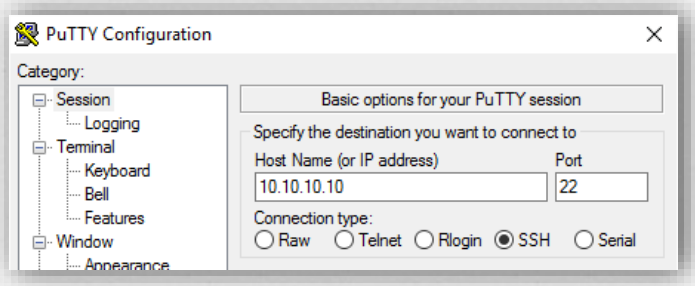




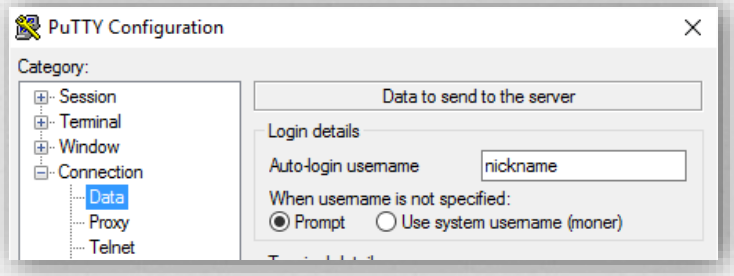
После импорта файл публичного ключа автоматически **удаляется**

Доступ SSH по ключу

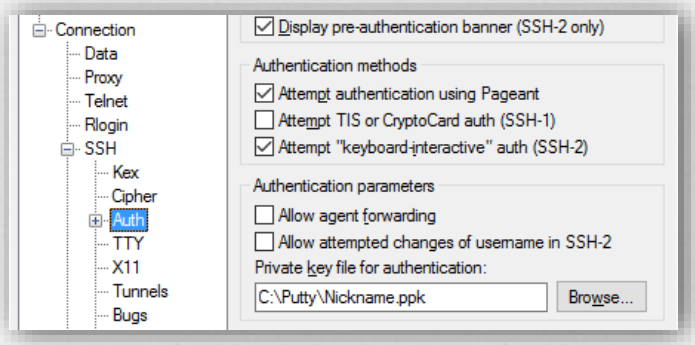
Настраиваем Putty:



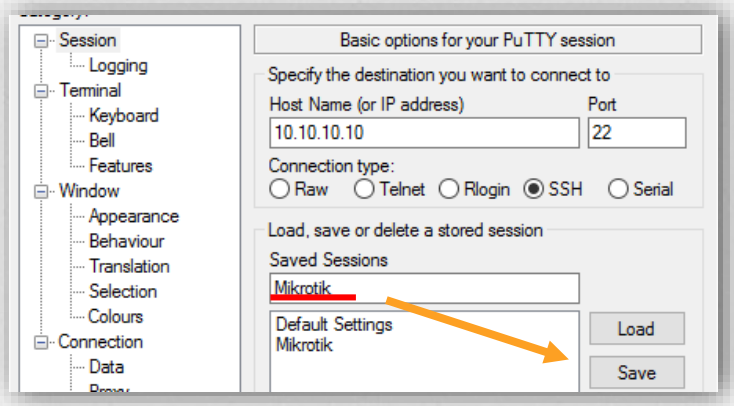
1. Указываем IP-адрес



2. Указываем имя пользователя



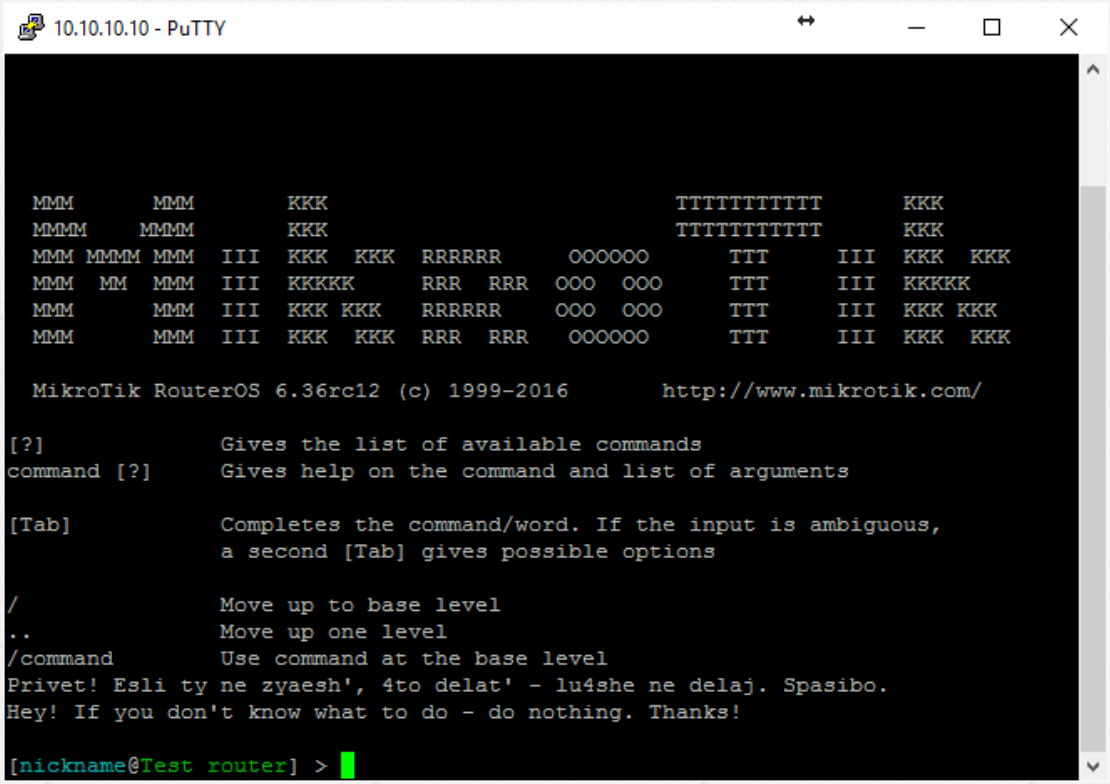
3. Указываем файл ключа



4. Сохраняем сессию

Доступ SSH по ключу

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



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:

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

Включил Safe Mode – выключи Safe Mode!

- 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] >
```

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

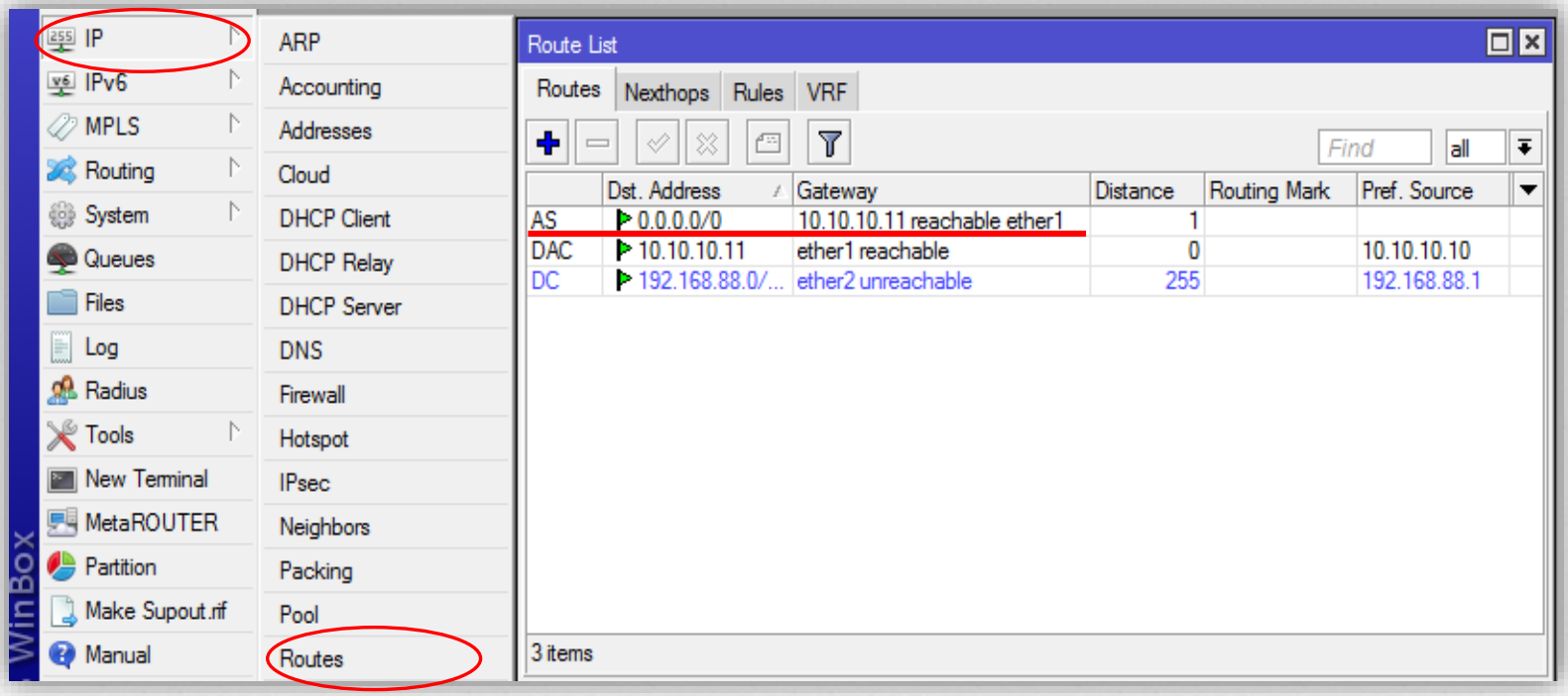
http://wiki.mikrotik.com/wiki/Manual:Console

CLI – это просто!

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

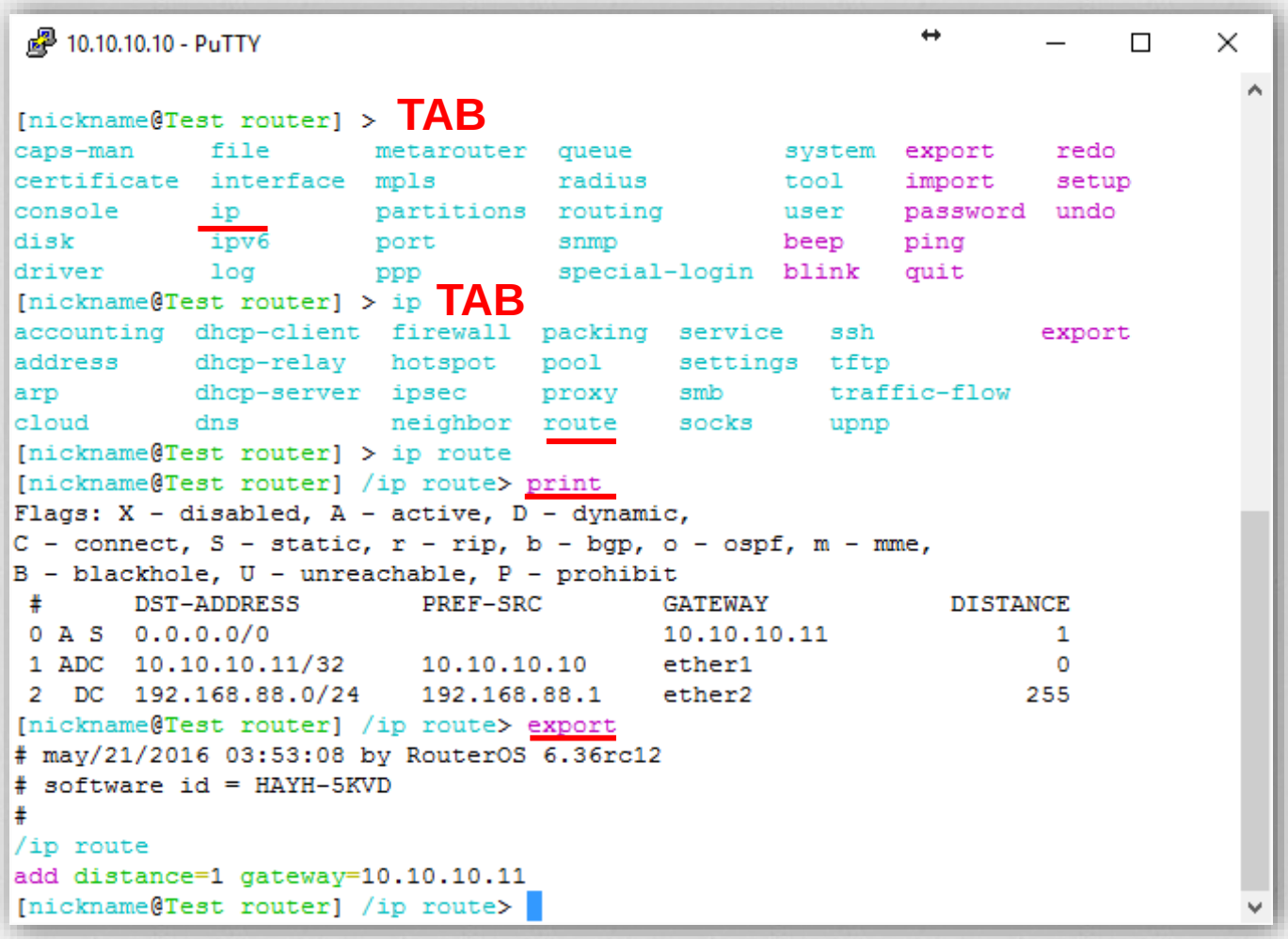
- Найдите нужный раздел в терминале
- Чтобы увидеть, ЧТО настроено – **print**
- Чтобы увидеть, КАК настроено – **export**
- Просмотр возможных опций – **TAB** и **?**

CLI – пример с маршрутами



Расположение в winbox: *IP-Routes*

CLI – пример с маршрутами



CLI – это просто!

- Большинство разделов легко найти:
  - IP->Firewall->Filter Rules = /ip firewall filter
  - IP->Routes = /ip route
- 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.
- Или просто наберите /export для просмотра полной конфигурации

Различия CLI и winbox

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

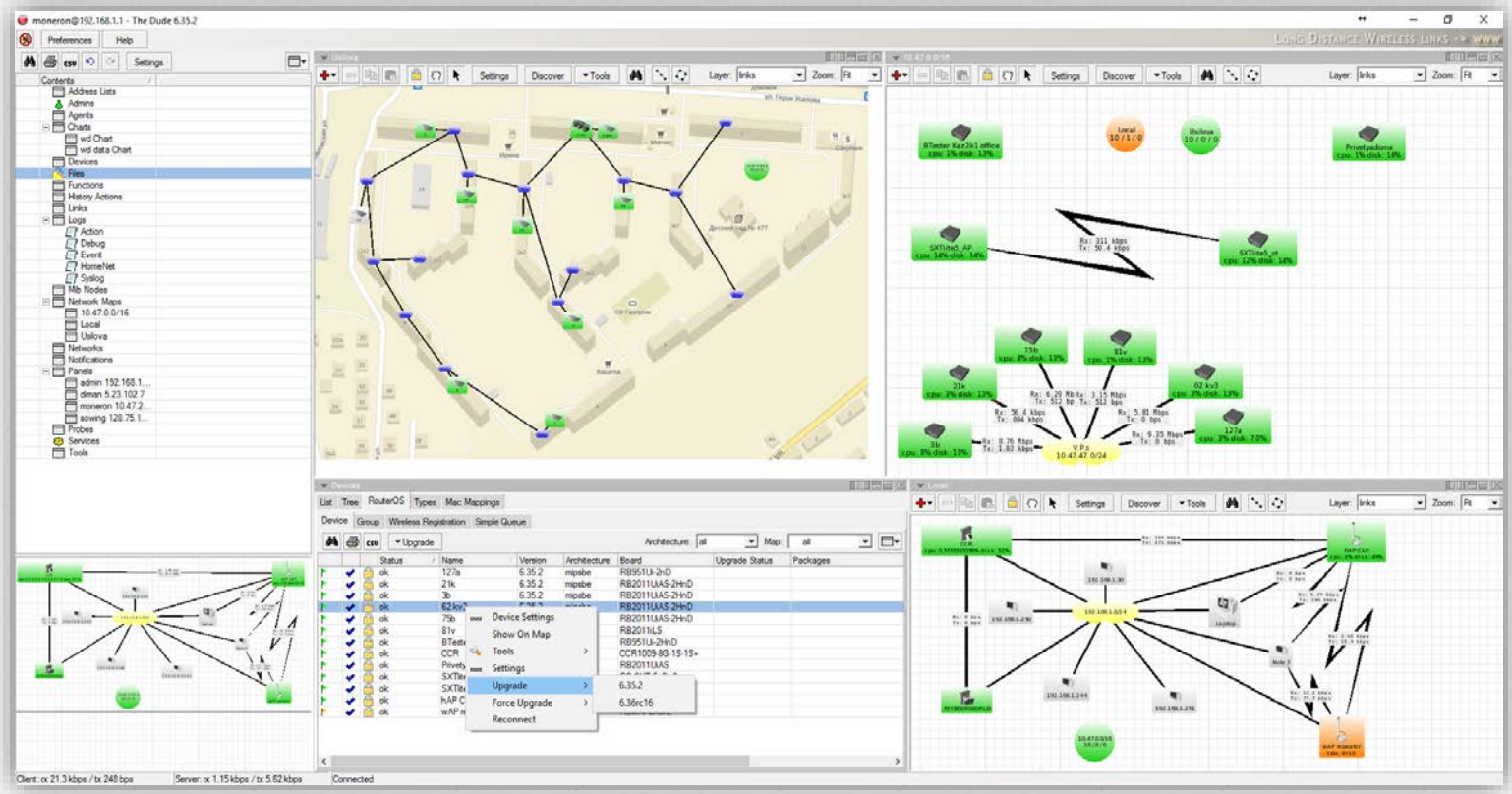
Рассмотренные вопросы

- 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

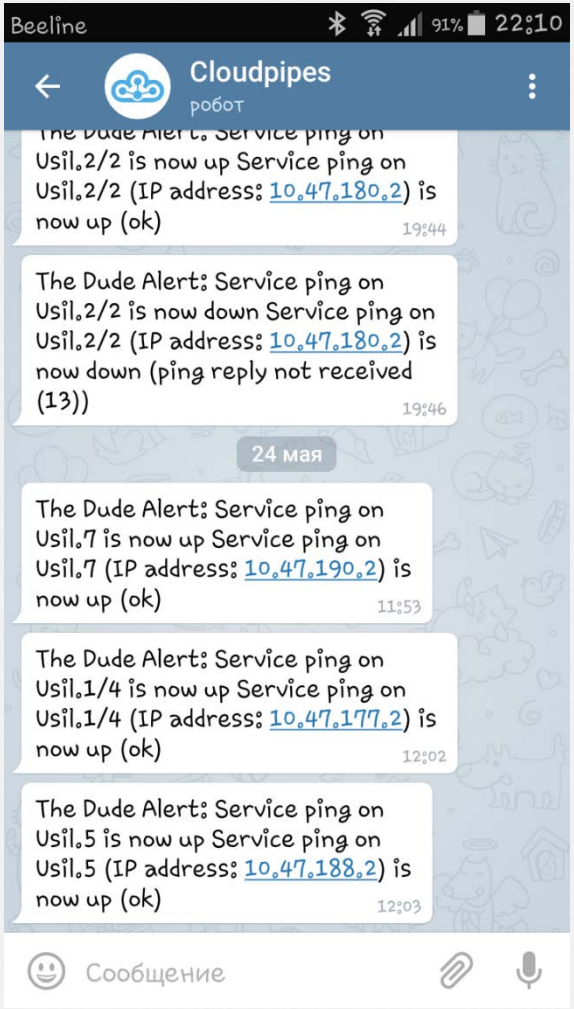
А напоследок
я скажу…

RouterOS – дай волю фантазии!

The Dude:



RouterOS – дай волю фантазии!



Ваши вопросы?

Спасибо за ваше внимание!