


Настройка роутера Микротик hAP Lite (RB941-2ND)

 mikrotiklab.ru/nastrojka/artga-hap-lite-rb941-2nd.html

January 27, 2021



Сегодня вашему вниманию представим настройку роутера Mikrotik hAP lite RB941-2nD. За полторы тысячи рублей вы получаете больше, чем роутер. Популярность его связана с ценой и функциональностью. У вас не будет какой-нибудь обрезанный RouterOS, все как положено, лицензия 4 уровня, можете крутить BGP, OSPF, MPLS без проблем (но мы надеемся вы этого не делаете на нем). Основные технические характеристики, следующие:

- Процессор архитектуры SMIPS — QCA9533, одно ядро 650 MHz;
- ОЗУ 32 Mb;
- Flash 16 Mb;
- Лицензия RouterOS 4 уровня;
- Порты 100 Mb/s в количестве 4 штук;
- WiFi чип на частоте 2,4 GHz;
- Кушает всего 3.5 W.

Маленький, скромный, но функциональный девайс, за хороший ценник, по функционалу ничем не отличается от своих старших братьев. Преимущественно падает выбор на эту модель, для не больших филиалов.

Если вы хотите построить CAPsMAN на базе данного устройства, то я вас огорчу, это не хорошая идея, т.к. антенны у него не изолированы. Доставит кучу хлопот. Для CAPsMAN стоит выбирать модели постарше.

Также вы можете воспользоваться статьёй про [настройку Микротика с нуля](#), она подойдёт для всех моделей роутеров, в том числе и для RB941-2ND

Содержание

1. [Сброс и обновление](#)
2. [Настройка WiFi](#)
3. [Настройка DNS и DHCP](#)
4. [Настройка NAT](#)
5. [Firewall](#)
6. [QoS](#)

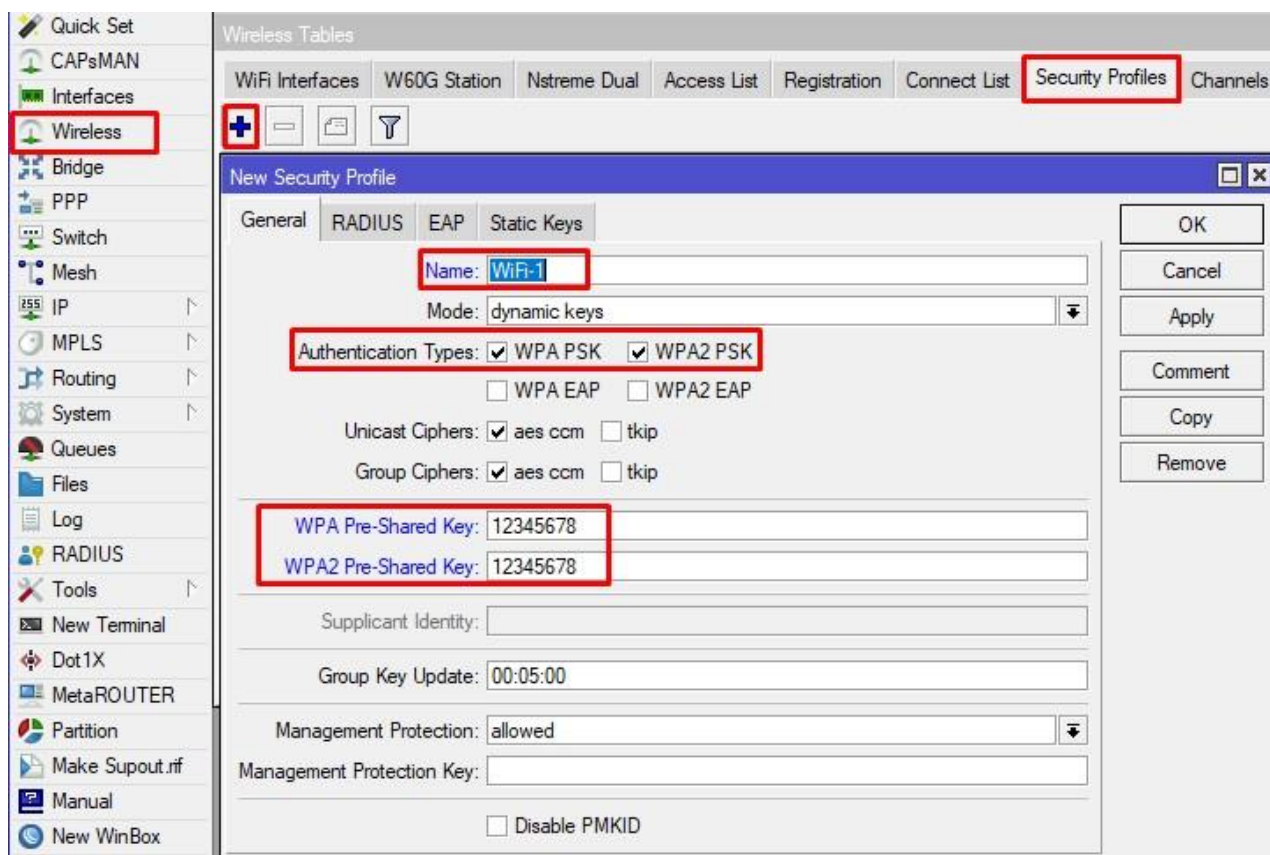
Сброс и обновление

Когда вы включите впервые девайс, по умолчанию в нем будет default config. Его достаточно для большинства случаев. Но мы пойдём другим путём и прошьём до актуальной версии 6.48 (Stable) через NetInstall. Об этом хорошо рассказано в [нашей статье тут](#).

На выходе вы должны получить blank (чистый) config, т.е. абсолютно чистый девайс.

Настройка WiFi

Правильная настройка беспроводной сети начинается с профиля безопасности. В ней мы задаём типы шифрования, алгоритмы, а также пароль. Открываем Wireless – Security Profiles, создаём новый профиль. Указываем имя, протоколы аутентификации, и сам пароль.



Рекомендуется не выбирать **tkip**, если вы используете **WPA PSK**.

Переходим в **Wireless**, двойным кликом открываем настройки адаптера **wlan1**, переключаем в расширенный режим кнопкой **Advanced Mode**. Открываем вкладку **wireless**. Это основное меню настройка адаптера. Указываем:

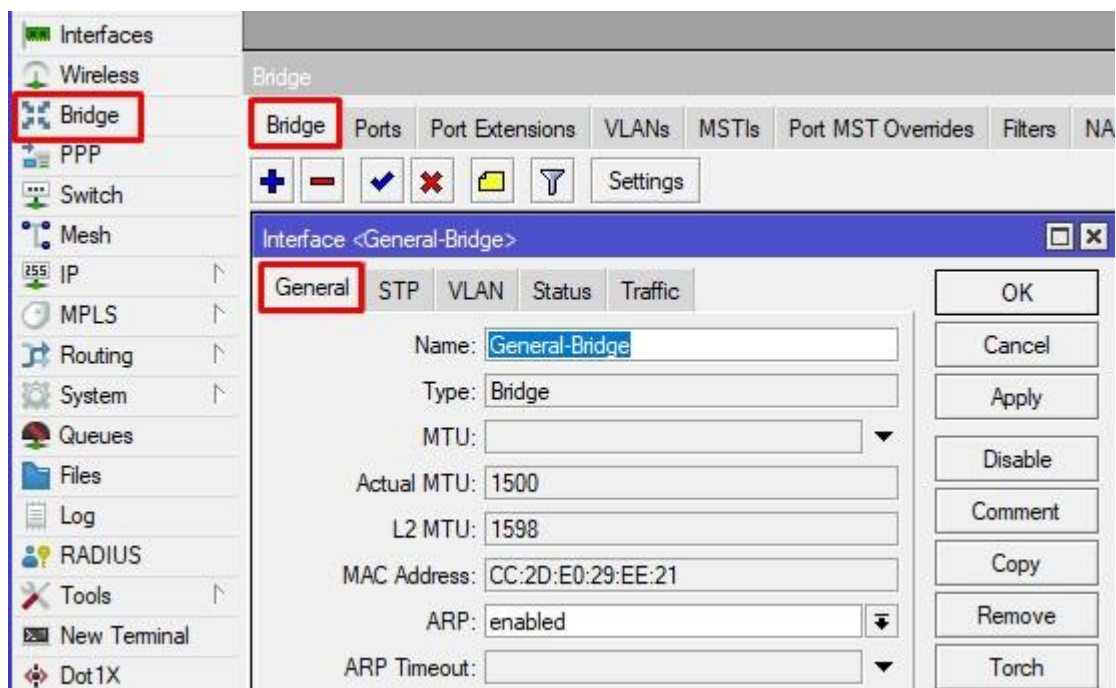
- Точка доступа в режиме **ap bridge** (как это было не странно, она у нас не в бридже, но все равно);
- Ширина канала **20MHz**;
- Частота (по желанию) **2462**;
- SSID **MikrotikLab**;
- WiFi Protocol **802.11**;
- Профиль безопасности **WiFi-1** (созданный ранее);
- Страна **ru** (или **us**).
- Убедитесь в наличии галочки **Default Authenticate** – без нее, клиенты не смогут подключаться к точке.

Применяем и включаем интерфейс (Enabled).

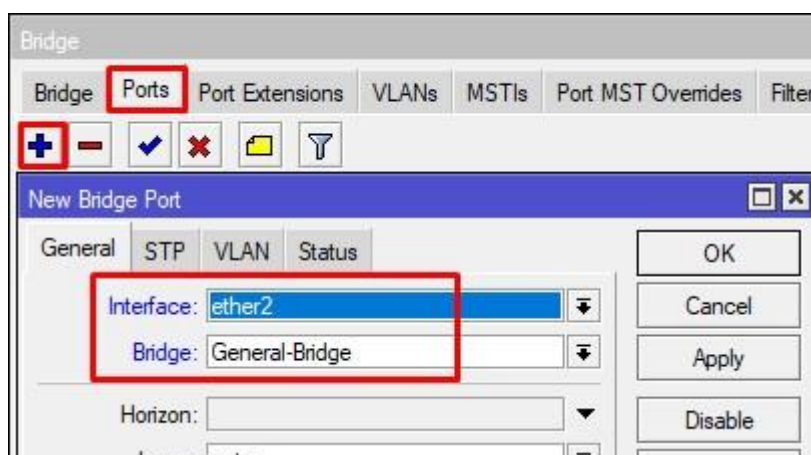
Наша команда рекомендует изучить [Наша команда рекомендует изучить углубленный курс по администрированию сетевых устройств MikroTik](#) В курсе много лабораторных работ по итогам которых вы получите обратную связь. После обучения вы получите диплом гос. образца РФ. Подробности и доступ к началу курса бесплатно [ТУТ](#).

Настройка DNS и DHCP

Задача, следующая: сделать 2 сегмента, 192.168.10.0/24 для портов 2-4. Подсеть 192.168.11.0/24 для WiFi и запретить между ними forwarding. Для проводных клиентов создаём bridge. Дадим ему корректное имя.



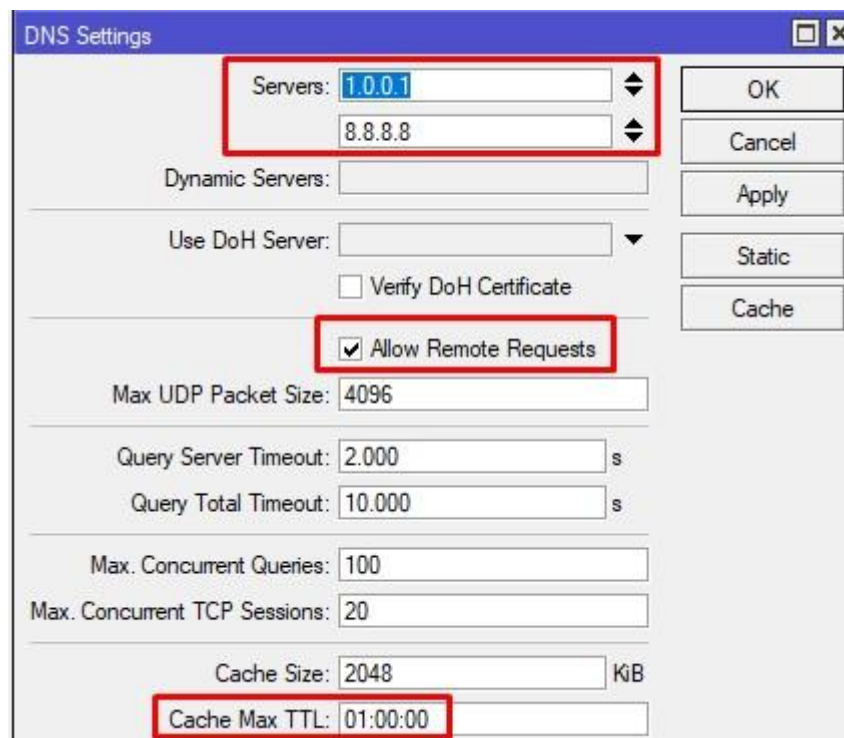
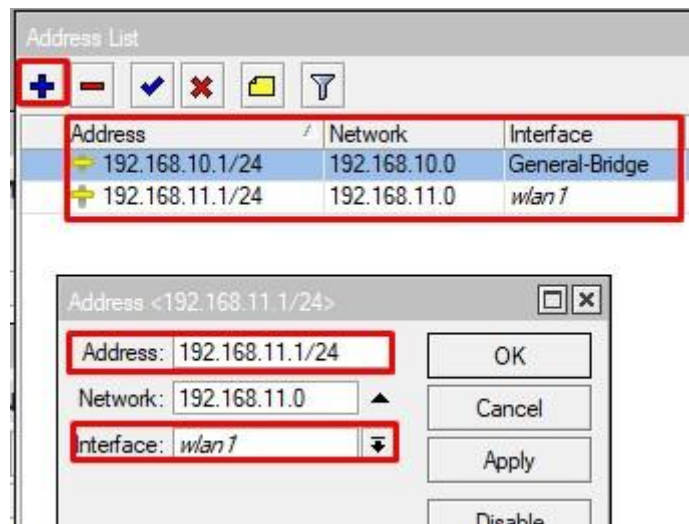
Далее добавим порты 2, 3, 4 в созданный бридж.



Зададим адреса через IP – Address.

Настроим разрешение имён. DNS серверами для нас будут 1.0.0.1 и 8.8.8.8.

Разрешим резолв на девайсе, а также изменим время жизни в кэше.

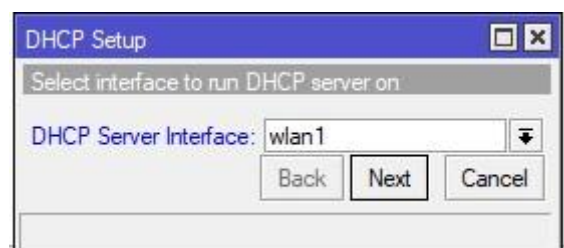


Настройка DHCP сервера. Воспользуемся мастером DHCP Setup. Выбираем интерфейс, на котором хотим его включить.

Девайс сразу поймёт, какой address space у сети на основе заданного адреса.

Шлюзом будет Mikrotik, здесь ничего не меняем.

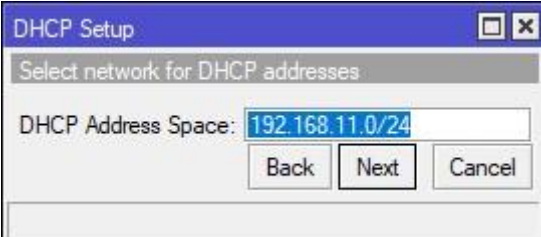
Далее предлагается ввести пул для раздачи. Я слегка изменил, и назначил раздачу с 192.168.11.10.



DNS сервером указываем IP роутера, в той сети, в которой он раздаёт адреса.

И, наконец, время аренды. Я предпочитаю изменять с 10 минут, на 1 день.

Теперь, проделываем аналогичные действия для проводных клиентов. Напомню, что следует задавать IP роутера, 192.168.10.1, шлюзом и DNS сервером.

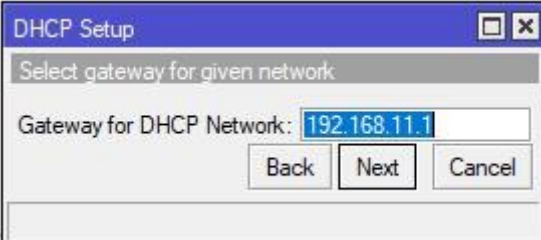


DHCP Setup

Select network for DHCP addresses

DHCP Address Space: 192.168.11.0/24

Back Next Cancel

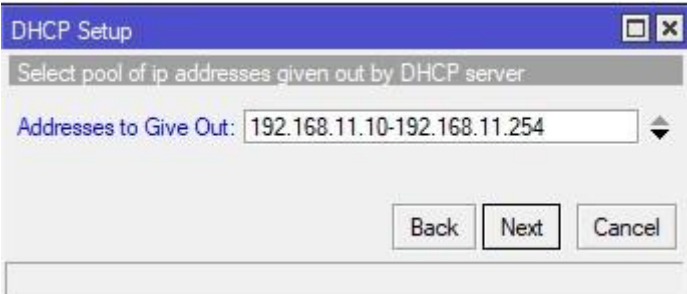


DHCP Setup

Select gateway for given network

Gateway for DHCP Network: 192.168.11.1

Back Next Cancel

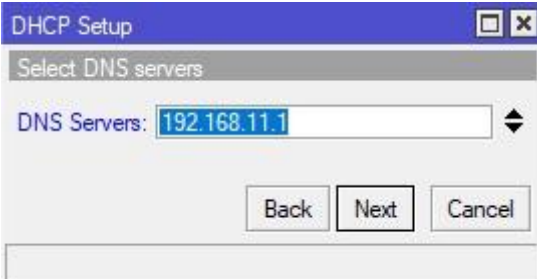


DHCP Setup

Select pool of ip addresses given out by DHCP server

Addresses to Give Out: 192.168.11.10-192.168.11.254

Back Next Cancel

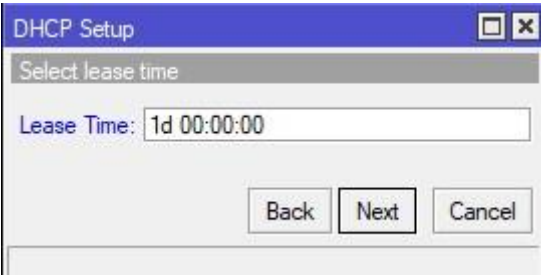


DHCP Setup

Select DNS servers

DNS Servers: 192.168.11.1

Back Next Cancel



DHCP Setup

Select lease time

Lease Time: 1d 00:00:00

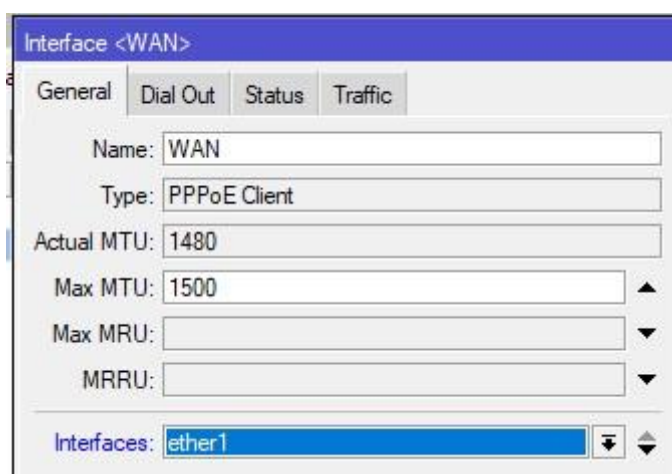
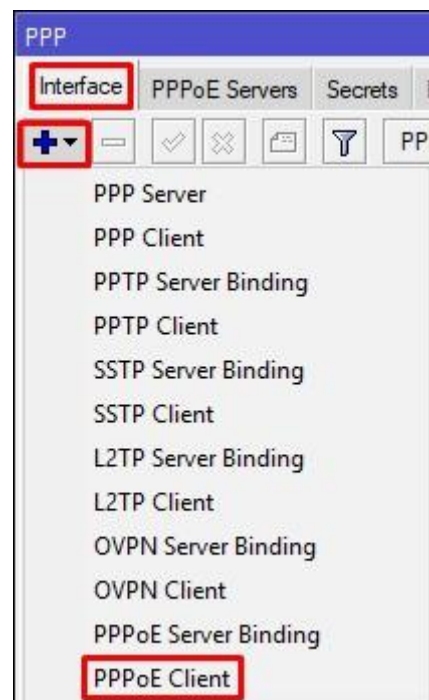
Back Next Cancel

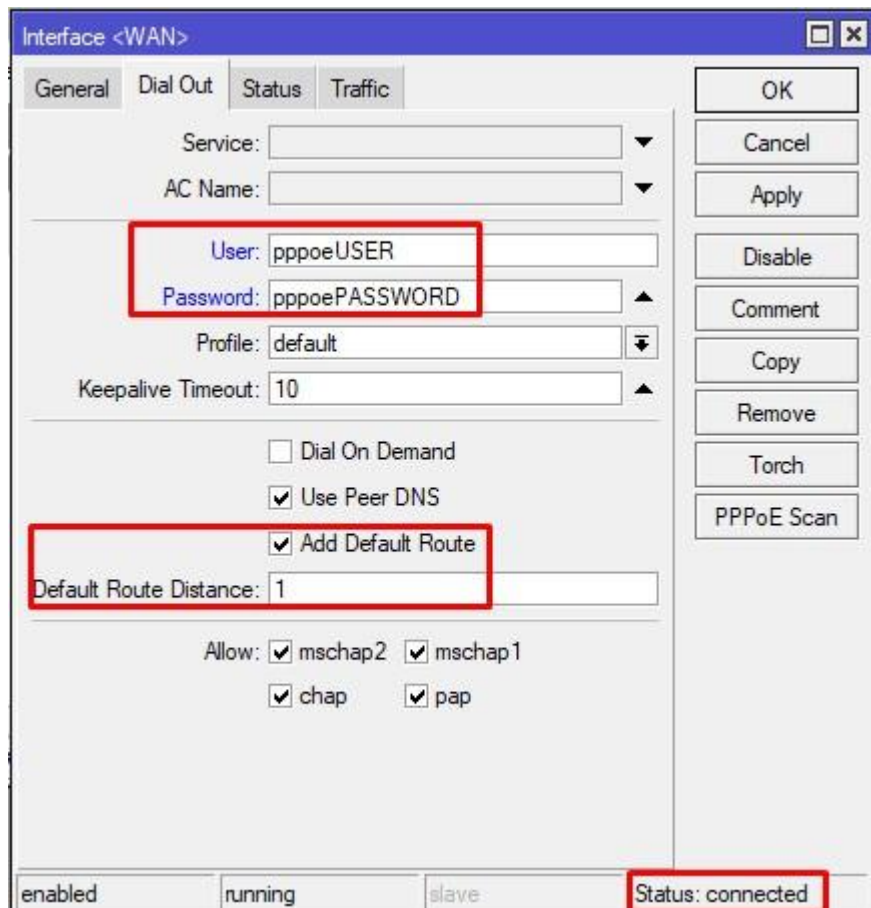
Настройка NAT

Но для начала настроим доступ в интернет, первый порт на mikrotik hap lite смотрит в провайдера, который подаёт доступ через PPPoE. В PPP – создадим PPPoE Client.

Зададим ему понятное для нас имя, и задаём интерфейс, который подключён в провайдера.

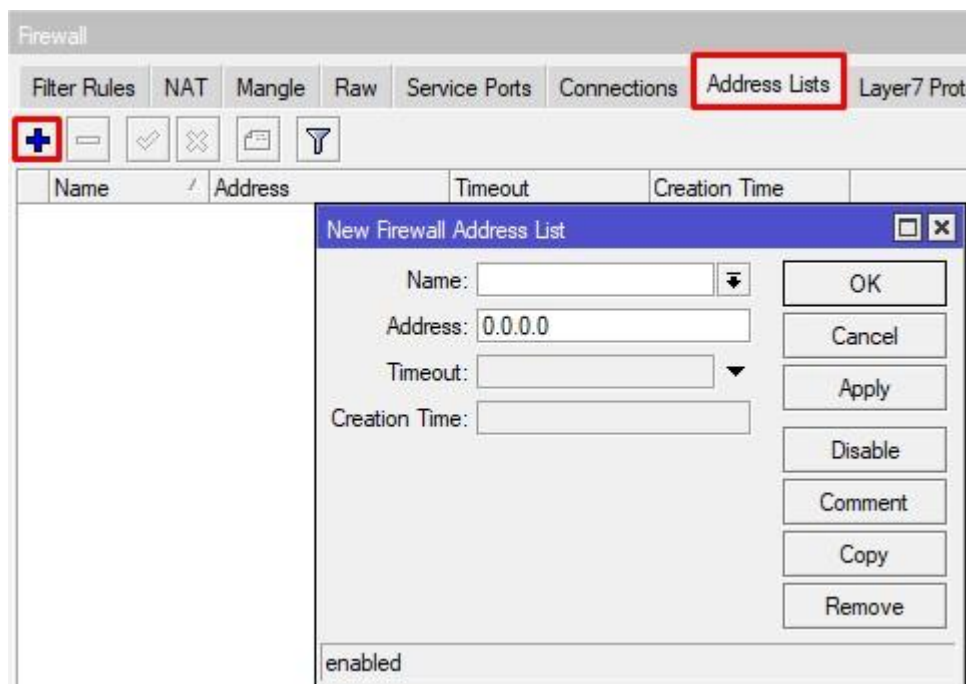
Пишем логин и пароль, и не забываем про галочку Add Default Route, если не хотите прописывать маршрут руками.



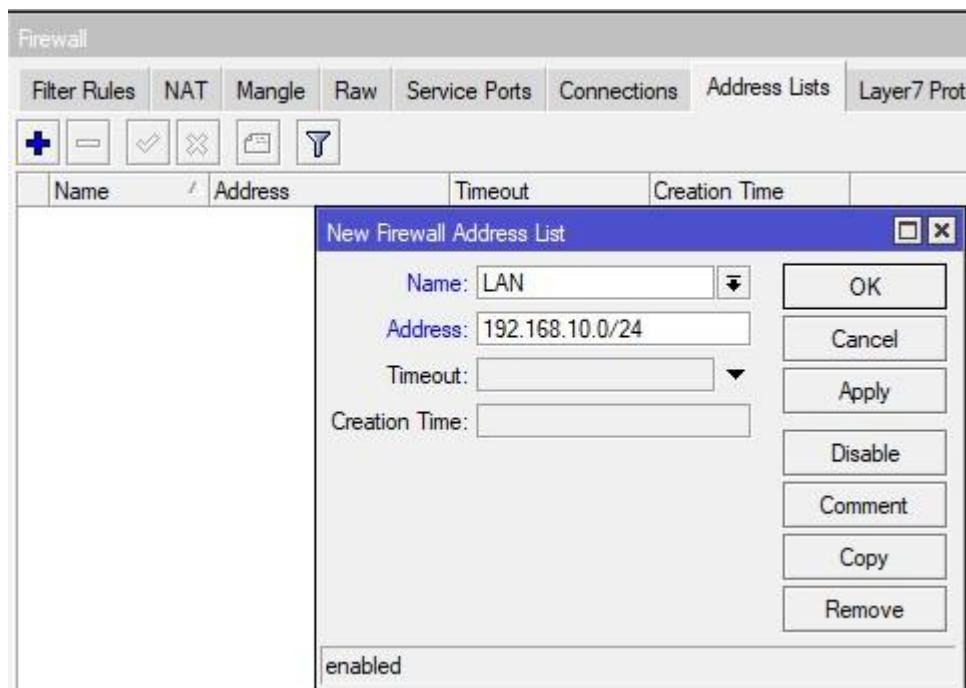


Статус Connected говорит, что все хорошо, двигаемся дальше.

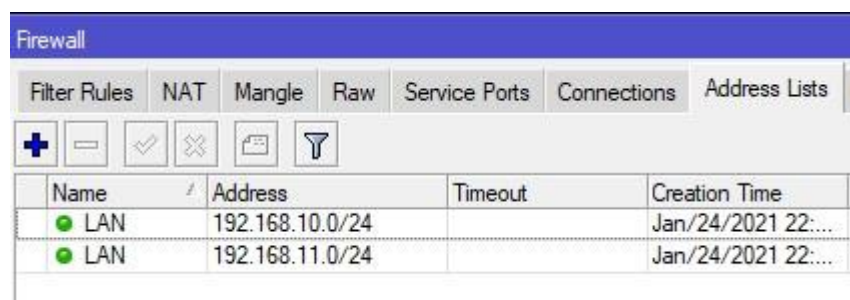
Для упрощения написания правила NAT, воспользуемся адрес листами. Находится в IP – Firewall – Address Lists.



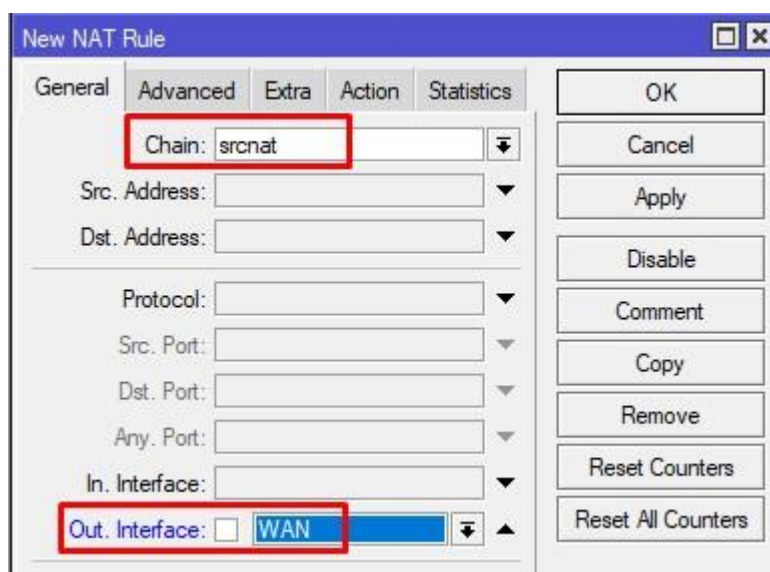
В строке Name – указываем имя листа, может быть любым. Главное, чтобы вам нравилось и было понятным. В Address, указываем наши подсети.



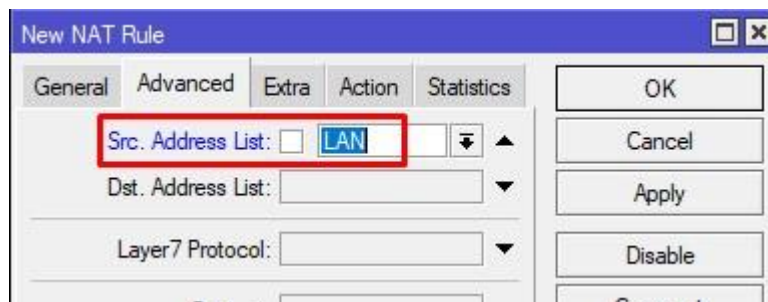
Применяем и создаём вторую запись. При создании второй записи, имя листа, можете выбрать из выпадающего списка. В итоге должна быть следующая картина.



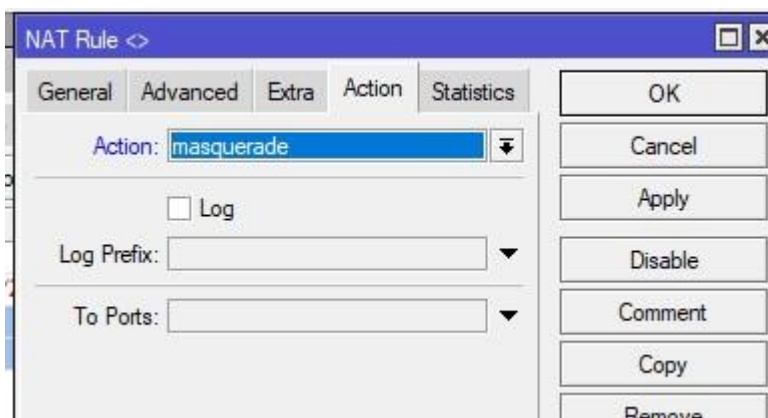
Переходим во вкладку NAT и создаём правило. Тут говорится, что мы хотим цепочку srcnat и выходной интерфейс будет WAN.



Переходим в Advanced, Src. Address List выбираем LAN.



На вкладке Action нас интересует masquerade. Применяем и если вы все сделали правильно, то проверяем что доступ в интернет появился у обеих сетей.



Firewall

Логика настройки и фильтрации трафика на маршрутизаторе MikroTik RB941-2ND не чем особым не отличается от старших моделей и будет следующая – разрешим подключение к Winbox, SSH откуда угодно. Web интерфейс будет доступен только с 192.168.10.0/24. Разрешим DNS только с локальных сетей, а все остальное запретим. Запретим пересылку между 192.168.10.0/24 и 192.168.11.0/24 используя ранее созданный адрес лист, тем самым обмен данными между WiFi и проводной сетями будет заблокирован. Разрешим new, established, related соединения.

Firewall																
Filter Rules																
NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols																
+ - ✓ ✗ 📁 🔍 ⚙️ ⚙️																
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes	Packets	
0	IN-SSH-Allow	input			6 (tcp)		22							0 B	0	
1	IN-Winbox-Allow	input			6 (tcp)		8291							0 B	0	
2	IN-DNS-from-LAN-Allow	input			17 (udp)		53					LAN		938 B	14	
3	IN-Web-from-LAN-Allow	input	192.168.10.0/24		6 (tcp)		80							0 B	0	
4	IN-EST-REL-Allow	input												100.7 KB	1 056	
5	IN-ALL-Drop	input												5.9 KB	88	
6	FRW-DROP-between-LAN	forward										LAN	LAN	0 B	0	
7	FRW-E&R&N-Allow	forward												44.5 KB	271	
8	FRW-Invalid-Drop	forward												0 B	0	

Будьте аккуратны с правилом 8, дропает инвалид пакеты. В стандартных сценариях обычно не мешает, но иногда его стоит отключать. Все вышеупомянутые правила можно загрузить через терминал:

```
/ip firewall filter

add action=accept chain=input comment=IN-SSH-Allow connection-state=new \
dst-port=22 protocol=tcp

add action=accept chain=input comment=IN-Winbox-Allow connection-state=new \
dst-port=8291 protocol=tcp

add action=accept chain=input comment=IN-DNS-from-LAN-Allow dst-port=53 \
protocol=udp src-address-list=LAN

add action=accept chain=input comment=IN-Web-from-LAN-Allow connection-
state=\
new dst-port=80 protocol=tcp src-address=192.168.10.0/24

add action=accept chain=input comment=IN-EST-REL-Allow connection-state=\
established,related

add action=drop chain=input comment=IN-ALL-Drop

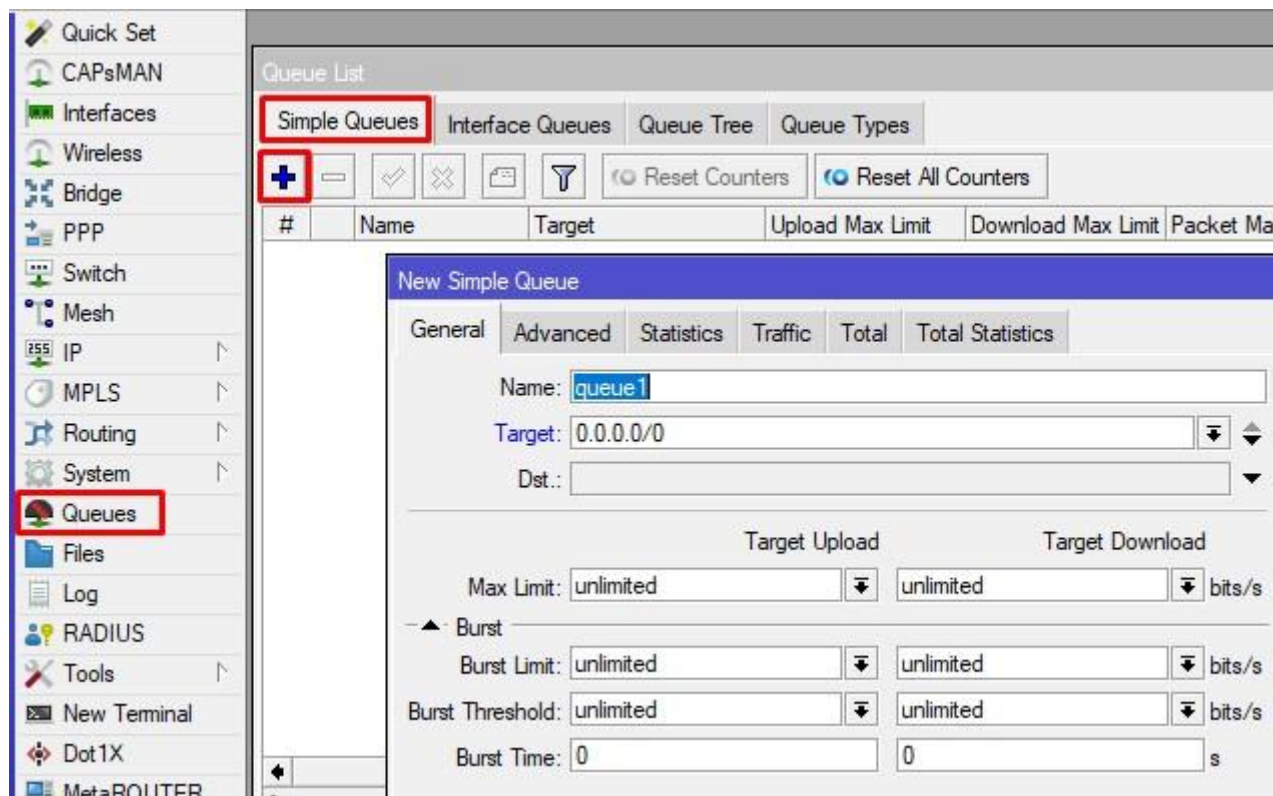
add action=drop chain=forward comment=FRW-DROP-between-LAN connection-
state=new \
dst-address-list=LAN src-address-list=LAN

add action=accept chain=forward comment=FRW-E&R&N-Allow connection-state=\
established,related,new

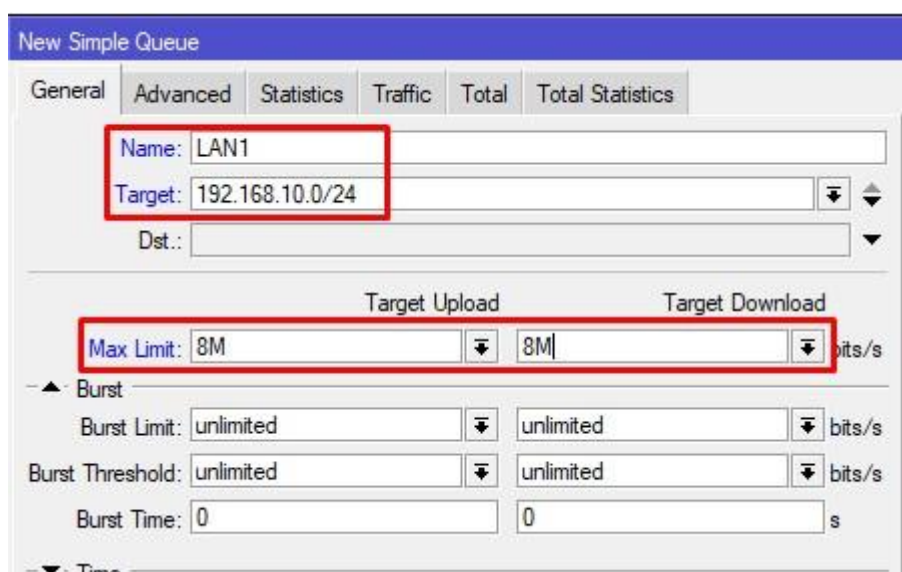
add action=drop chain=forward comment=FRW-Invalid-Drop connection-
state=invalid
```

QoS

В нашем сценарии провайдер выпускает в интернет на 10Мб/с. Нам нужно ограничить для проводных клиентов до 8 Мб/с, а беспроводных до 2 Мб/с. Я предлагаю не просто ограничить, а ещё поровну делить каждое соединение в случае максимальной нагрузки. Это достигается типом очереди PCQ. Переходим в Queues – Simple Queue и создаём новое правило.



Пишем имя правилу, в Target задаётся конкретный IP или диапазон адресов, для которых хотим применить правило. И конечно же сами значения скоростей в Target Upload и Target Download.



Переходим на вкладку Advanced и выбираем тип очереди rcq-upload-default для секции Upload, и rcq-download-default для секции Download.

New Simple Queue

General Advanced Statistics Traffic Total Total Statistics

Packet Marks:

Target Upload Target Download

Limit At: unlimited unlimited bits/s

Priority: 8 8

Bucket Size: 0.100 0.100 ratio

Queue Type: pcq-upload-default pcq-download-default

Parent: none

Продельываем аналогичные действия WiFi клиентов, указав соответствующую скорость в 2Мб/с и target.

Queue List

Simple Queues Interface Queues Queue Tree Queue Types

+ - ✓ ✗ 📁 📏 🔄 Reset Counters 🔄 Reset All Counters

#	Name	Target	Upload Max Limit	Download Max Limit
0	LAN1	192.168.10.0/24	8M	8M
1	LAN2	192.168.11.0/24	2M	2M

Из хорошего, данный алгоритм очередей может вас выпустить в интернет несмотря на то, что сосед качает торренты. Расплата за это будет серьезная утилизация CPU.

На этом мы закончим настройку маршрутизатора MikroTik RB941-2ND, удачных конфигураций!

Вы хорошо разбираетесь в Микротиках? Или впервые недавно столкнулись с этим оборудованием и не знаете, с какой стороны к нему подступиться? В обоих случаях вы найдете для себя полезную информацию в углубленном курсе «Администрирование сетевых устройств MikroTik». В курсе много практических лабораторных работ по результату выполнения которых вы получите обратную связь. После окончания обучения вы получите диплом гос. образца РФ. Подробности и доступ к началу курса бесплатно [тут](#).