

# Базовая настройка роутера MikroTik - Записки IT специалиста

---



interface31.ru/tech\_it/2018/11/bazovaya-nastroyka-routera-mikrotik.html

## Записки IT специалиста

---

Технический блог специалистов ООО "Интерфейс"

- [Главная](#)
- Базовая настройка роутера MikroTik

## Базовая настройка роутера MikroTik

---

За роутерами MikroTik давно закрепилась слава "сложных" в настройке. Это действительно так, если говорить о начинающих. После обычных роутеров, где производитель практически за руку ведет пользователя от настройки к настройке, RouterOS пугает обилием возможностей и отсутствием привычных интерфейсов. Но не стоит пугаться, если вы имеете начальные знания по устройству и работе сетей, то очень скоро вы будете чувствовать себя как рыба в воде, а настройки иных роутеров наоборот покажутся вам ограниченными. Сегодня мы начнем с базовой настройки, чтобы научить ваш MikroTik всему тому, что умеют обычные роутеры.

### Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на [углубленном курсе по администрированию MikroTik](#). Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.

В сети имеется достаточное количество инструкций по настройке роутеров этой марки, с разными подходами к этому процессу, поэтому мы не будем претендовать на истину в последней инстанции, а выразим наше видение этого вопроса. В первую очередь мы считаем, что возможности не должны опережать знания, поэтому не следует сразу браться за настройку сложных сетевых конфигураций. Лучше всего сначала разобраться в базовых настройках и только потом, по мере появления опыта переходить к более сложным схемам.

В свое время, когда вчерашний студент приходил на производство, ему говорили: "Забудь все чему тебя учили, и слушай сюда". Этот подход как никогда справедлив, если вы первый раз берете в руки MikroTik, забудьте о предыдущем опыте с другими роутерами и готовьтесь осваивать новые подходы.

Прежде всего абсолютно неважно какая именно модель роутера у вас в руках, главное, что внутри находится RouterOS, а значит вам подойдет любая инструкция по настройке, за небольшими поправками, связанными с аппаратными ограничениями (скажем, если в вашей модели отсутствует Wi-Fi, то часть инструкции посвященную настройке беспроводной сети вы можете просто пропустить).

Поэтому для подготовки материалов по Mikrotik мы будем использовать виртуальные машины с RouterOS, прибегая к реальному оборудованию только чтобы показать какие-то специфичные моменты.

## Подготовка к настройке

---

Первым делом, взяв в руки Mikrotik, следует обновить версию RouterOS до актуальной. Это следует сделать по нескольким причинам, в первую очередь в целях безопасности. Еще свежа история с широкой эксплуатацией уязвимости CVE-2018-14847, несмотря на то что производитель оперативно выпустил патч. Просто пользователи не спешили обновлять свои устройства, как говорится - пока гром не грянет...

Во-вторых, начиная с RouterOS 6.41 были изменены настройки коммутации и если вы хотите использовать актуальные инструкции, перед настройкой версию ОС следует обязательно обновить.

Для этого перейдем на сайт производителя в раздел [Downloads](#) и скачаем свежую версию **Winbox** - графической утилиты для настройки, а также свежую версию RouterOS. Представленные на странице пакеты отличаются только архитектурой вашего роутера, если вы ее не знаете, то рядом перечислены все подходящие модели роутеров. В каждом разделе представлено два пакета: **Main** и **Extra**, первый - это основная прошивка, то, что находится в вашем устройстве из коробки, второй - дополнительные пакеты, которые можно установить самостоятельно, они нам сейчас не нужны.

## Software

Downloads Changelogs Download archive RouterOS The Dude

## Upgrading RouterOS

If you are already running RouterOS, upgrading to the latest version can be done by clicking on "Check For Updates" in **QuickSet** or **System > Packages** menu in WebFig or WinBox.

See the [documentation](#) for more information about upgrading and release types.

To manage your router, use the web interface, or download the maintenance utilities. Winbox to connect to your device, Dude to monitor your network and Netinstall for recovery and re-installation.

WinBox

1

The Dude

Netinstall

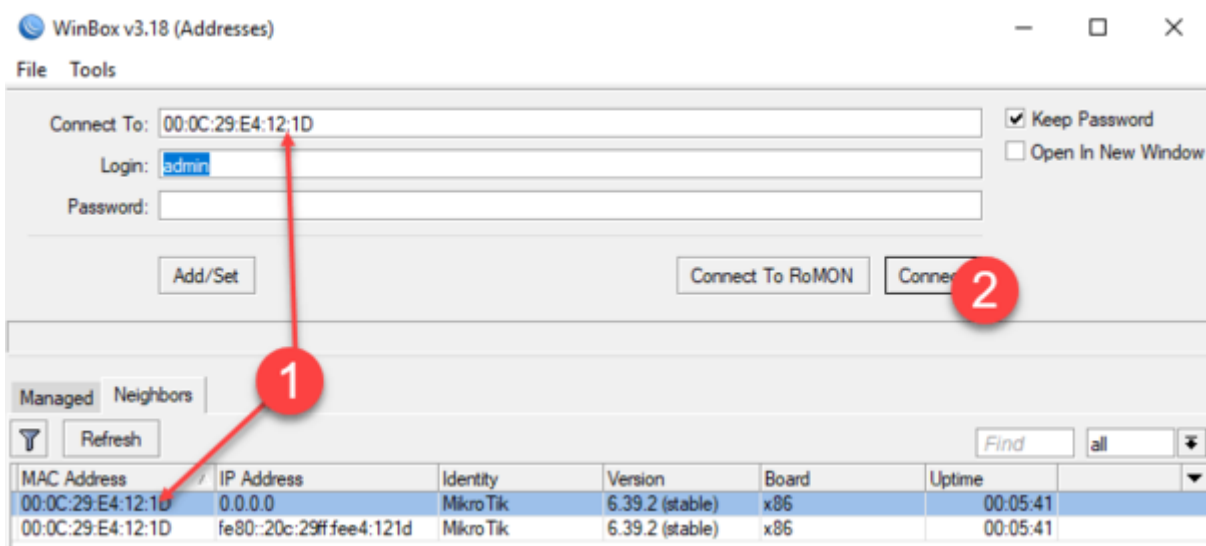


## RouterOS

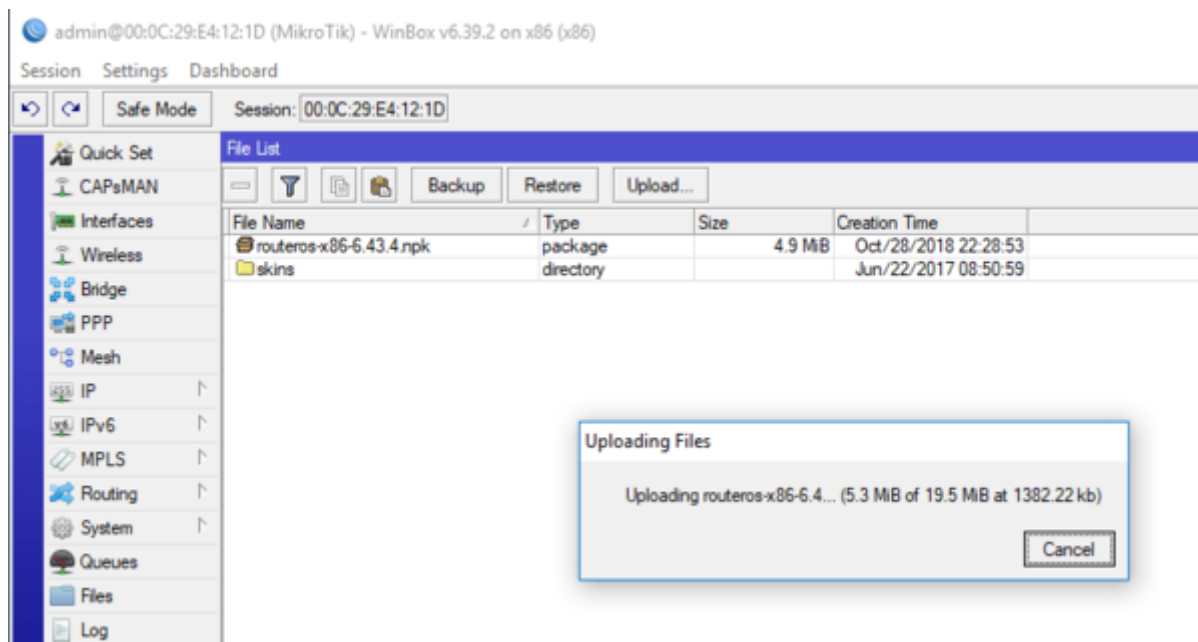


	6.42.9 (Long-term)	6.43.4 (Stable)	6.44beta20 (Testing)
<b>MIPSBE</b>	CRS1xx, CRS2xx, DISC, NAP, hAP ac, hAP ac lite, LDF, LHO, mANTBox, mAP, NetBox, NetMetal, PowerBox, QRT, RBxx, cAP, HEX Lite, RB4xx, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx		
Main package			
Extra packages			
<b>SMIPS</b>	hAP mini, hAP lite		
Main package			
Extra packages			

Теперь подключим патч-корд к любому порту роутера, кроме первого и запустим WinBox. По умолчанию в MikroTik включен MAC-сервер, что позволяет подключаться к устройству по MAC-адресу, не меняя настройки сетевого адаптера. Ваше устройство через некоторое время появится на закладке **Neighbors**, после чего щелкните мышью на поле MAC-адреса, который автоматически подставится в строку подключения, для входа используйте **admin** с пустым паролем.

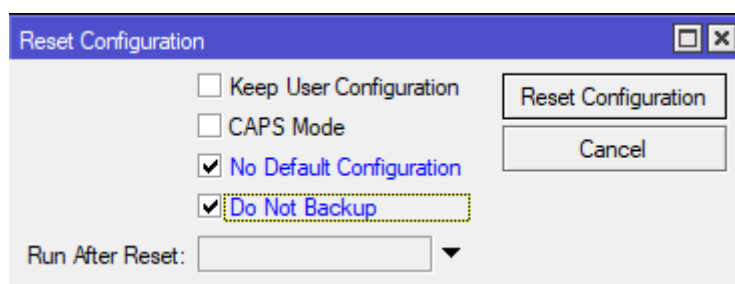
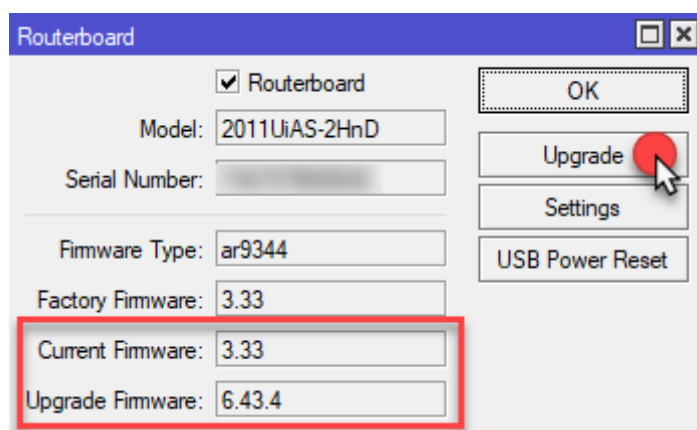


Для обновления перейдите в раздел **Files** и загрузите скачанный ранее пакет с RouterOS, это можно сделать как кнопкой **Upload**, так и простым перетаскиванием файла в окно. После чего просто перезагрузите устройство: **System - Reboot**.



Следующим шагом обновим загрузчик RouterBOOT, для этого перейдем **System - Routerboard** и сравним текущую версию с доступной прошивкой, для обновления нажмите **Upgrade** и еще раз перезагрузите устройство.

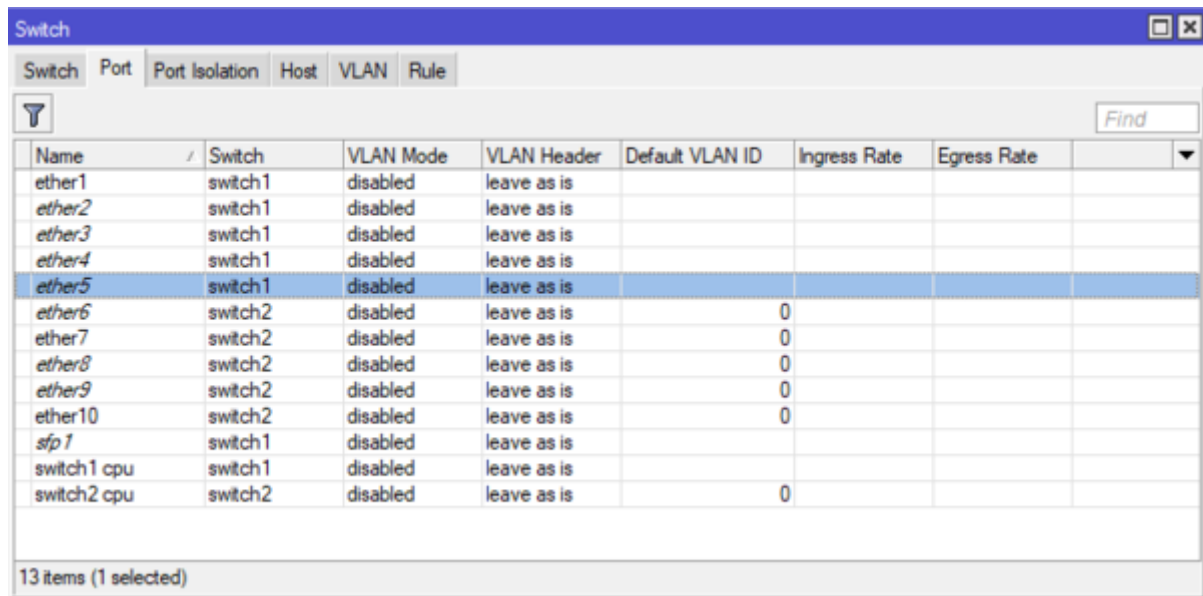
И, наконец, сбросим конфигурацию устройства. Хорошей практикой настройки Mikrotik является полный сброс настроек по умолчанию и настройка устройства с нуля, таким образом вы не только настроите свой роутер именно так, как нужно вам, но и будете уверены, что настройки не содержат никаких "сюрпризов", которые вы могли просто не заметить. Для этого выберем **System - Reset Configuration** и установим флаги No Default Configuration и Do Not Backup, после чего выполним сброс устройства, при этом роутер снова будет перезагружен.



## Настройка портов и коммутация

В старых версиях RouterOS было два варианта настройки коммутации: аппаратный, при помощи чипа коммутации (через мастер-порт) и программный (через мост), в современных версиях используется только один вариант - через мост, при этом чип коммутации будет задействован автоматически, при наличии такой возможности, т.е. коммутация будет по-прежнему выполняться на аппаратном уровне. Более подробно мы коснемся этого момента немного позже.

Открыв раздел **Switch** можно посмотреть какие чипы коммутации установлены в вашем роутере и какие порты они обслуживают:



Name	Switch	VLAN Mode	VLAN Header	Default VLAN ID	Ingress Rate	Egress Rate
ether1	switch1	disabled	leave as is			
ether2	switch1	disabled	leave as is			
ether3	switch1	disabled	leave as is			
ether4	switch1	disabled	leave as is			
ether5	switch1	disabled	leave as is			
ether6	switch2	disabled	leave as is	0		
ether7	switch2	disabled	leave as is	0		
ether8	switch2	disabled	leave as is	0		
ether9	switch2	disabled	leave as is	0		
ether10	switch2	disabled	leave as is	0		
sfp 1	switch1	disabled	leave as is			
switch1 cpu	switch1	disabled	leave as is			
switch2 cpu	switch2	disabled	leave as is	0		

Для примера показан RB2011, который имеет два чипа коммутации: первый обслуживает порты ether1-ether5 и sfp, второй ether6-ether10. Для портов, обслуживаемых одним чипом, доступна аппаратная коммутация, между портами обслуживаемыми разными чипами коммутация будет программной. Это следует учитывать при распределении портов, скажем если мы для файлового сервера выделим ether7, а для клиентов ether2-ether5, то получим повышенную нагрузку на устройство из-за программной коммутации.

Для новичков сообщим еще одну новость: в Mikrotik нет LAN и WAN портов, любой порт может быть настроен как вам нужно. Есть два внешних канала - настроим два WAN, нужно обслуживать две внутренних сети - не проблема, создадим две группы коммутации.

Далее в нашем примере мы будем использовать пятипортовый роутер и в качестве внешнего порта будем использовать здесь и далее последний порт. Остальные порты будут объединены в группу коммутации для локальной сети. Откроем **Interfaces - Interface** и добавим к портам ether1 и ether5 комментарии, указывающие на их назначение. Также можно переименовать сам порт, но мы предпочитаем оставлять им оригинальные названия, что позволяет быстро понимать к какому физическому порту относится та или иная запись.

admin@00:0C:29:E4:12:1D (MikroTik) - WinBox v6.43.4 on x86 (x86)

Session Settings Dashboard

Safe Mode Session: 00:0C:29:E4:12:1D

Quick Set CAPsMAN Interfaces Wireless Bridge PPP Mesh IP IPv6 MPLS Routing

### Interface List

Interface	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)
... LAN						
R ether1	Ethernet	1500		24.6 kbps	2.3 kbps	4
R ether2	Ethernet	1500		0 bps	0 bps	0
R ether3	Ethernet	1500		0 bps	0 bps	0
R ether4	Ethernet	1500		0 bps	0 bps	0
... WAN						
R ether5	Ethernet	1500		0 bps	1968 bps	0

Оставим пока настройку подключения к провайдеру и объединим локальные интерфейсы в группу коммутации, для этого нам нужно будет создать мост, переходим в раздел **Bridge** и создаем там сетевой мост **bridge1**, в комментариях также указываем его принадлежность к LAN.

Затем переходим на закладку **Bridge - Ports** и последовательно добавляем в мост интерфейсы локальной сети ether1-ether4, обратите внимание на активную по умолчанию опцию **Hardware Offload**, которая включает аппаратную коммутацию, если она доступна.

admin@00:0C:29:E4:12:1D (MikroTik) - WinBox v6.43.4 on x86 (x86)

Session Settings Dashboard

Safe Mode Session: 00:0C:29:E4:12:1D

Quick Set CAPsMAN Interfaces Wireless Bridge PPP Mesh IP IPv6 MPLS Routing

### Bridge

Bridge Ports VLANs MSTIs Port MST Overrides Filters NAT Hosts MDB

# Interface Bridge Horizon Trusted Priority (h) Path Cost Role

**New Bridge Port**

General STP VLAN Status

Interface: ether1

Bridge: bridge1

Horizon:

Learn: auto

☒ Unknown Unicast Flood

☒ Unknown Multicast Flood

☒ Broadcast Flood

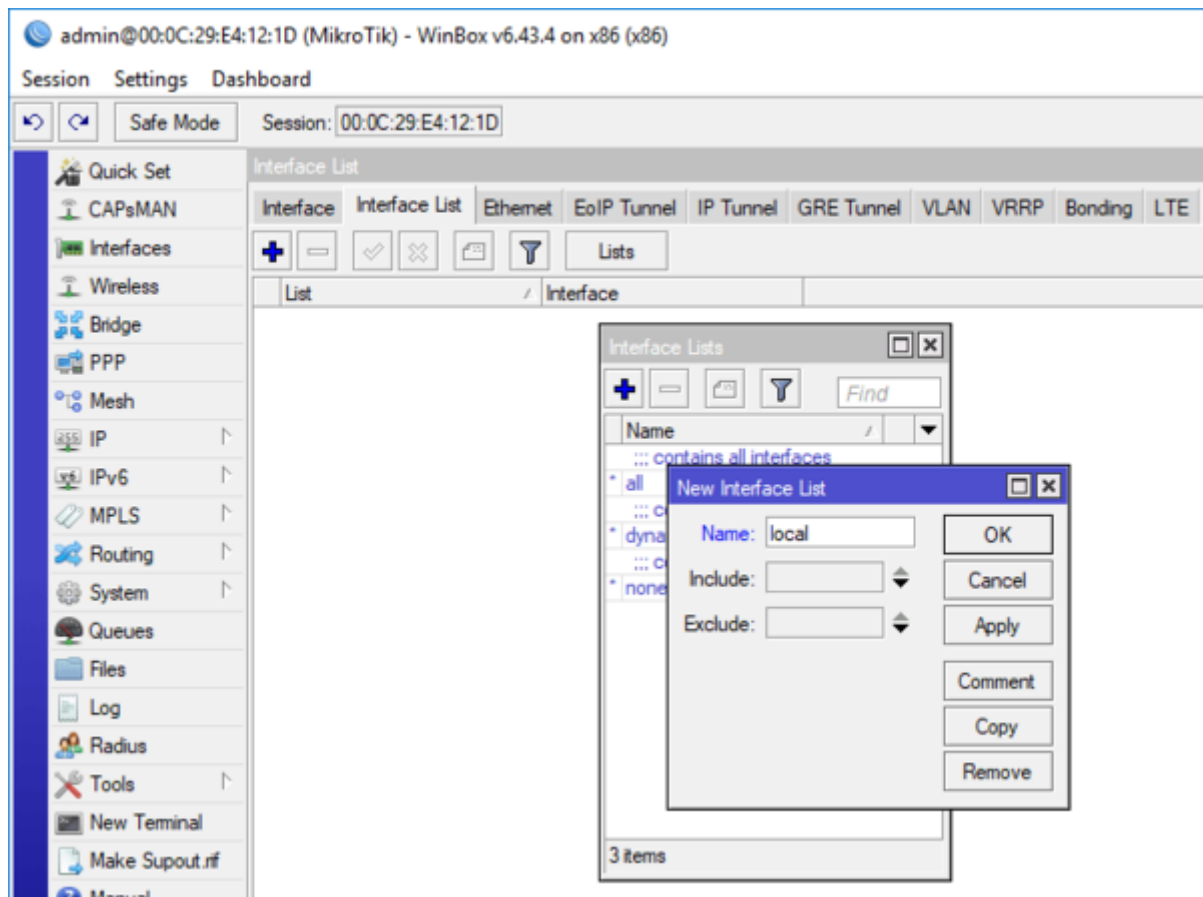
☐ Trusted

☒ Hardware Offload

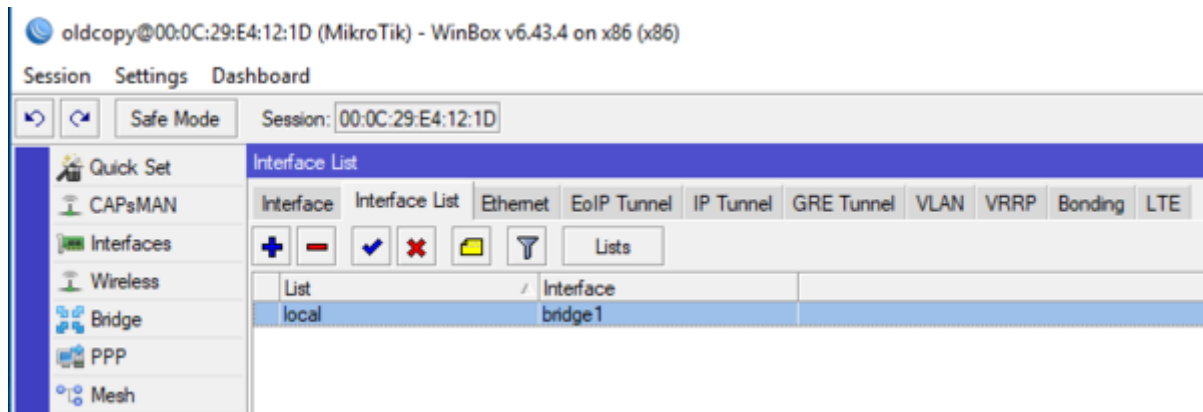
enabled inactive Hw. Offload



Итак, мост создан, порты добавлены, теперь перейдем в **Interfaces - Interface List** и создадим новый список, которому дадим название **local**:

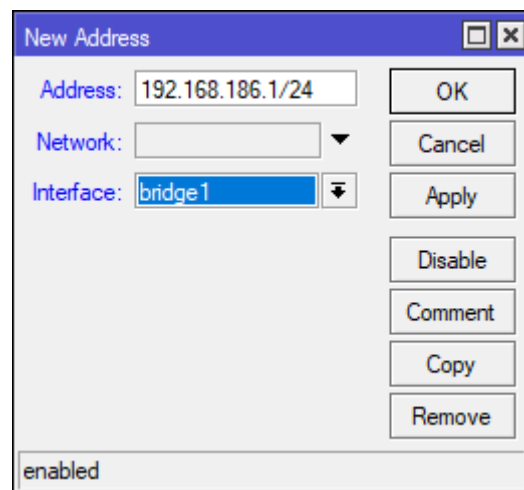


А затем добавим в этот список интерфейс нашего локального моста:



Осталось только присвоить нашему мосту локальный IP-адрес, для этого откроем **IP - Addresses** и добавим интерфейсу **bridge1** нужный адрес. Обратите внимание, что используется формат записи IP/маска, т.е. вы должны указать **192.168.186.1/255.255.255.0** или более короткий вариант **192.168.186.1/24**:

Теперь роутер будет пинговаться по указанному вами адресу и по нему можно будет подключиться к устройству. Для того, чтобы убедиться, что аппаратная коммутация работает перейдите в **Bridge - Ports**, символ **H** в строке порта указывает на то, что для обработки, передаваемой на уровне L2 информации, используется чип коммутации.



New Address






Address: 192.168.186.1/24

Network:

Interface: bridge1

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

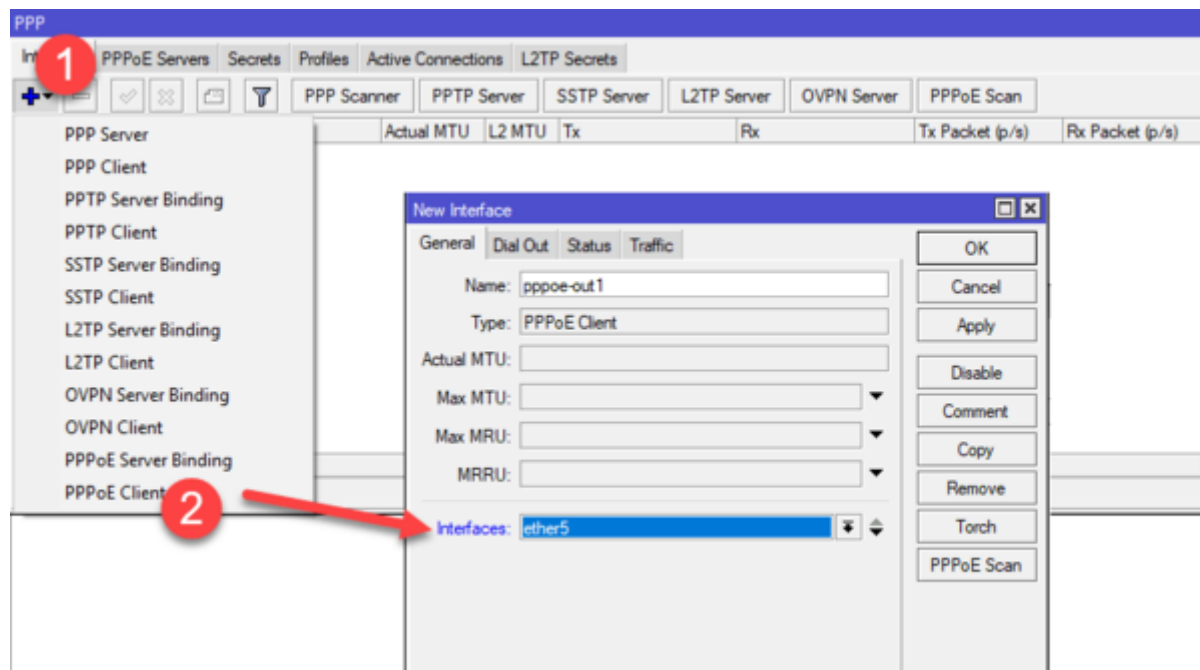
enabled

Bridge								
Bridge Ports VLANs MSTIs Port MST Overrides Filters NAT Hosts MDB								
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>...</div> <div>⌵</div> </div>								
#	Interface	Bridge	Horizon	Trusted	Priority (h	Path Cost	Role	
0	 wlan1	bridge1		no	80	10	designated port	
1	IH  ether1	bridge1		no	80	10	disabled port	
2	H  ether2	bridge1		no	80	10	designated port	
3	H  ether3	bridge1		no	80	10	designated port	
4	H  ether4	bridge1		no	80	10	designated port	

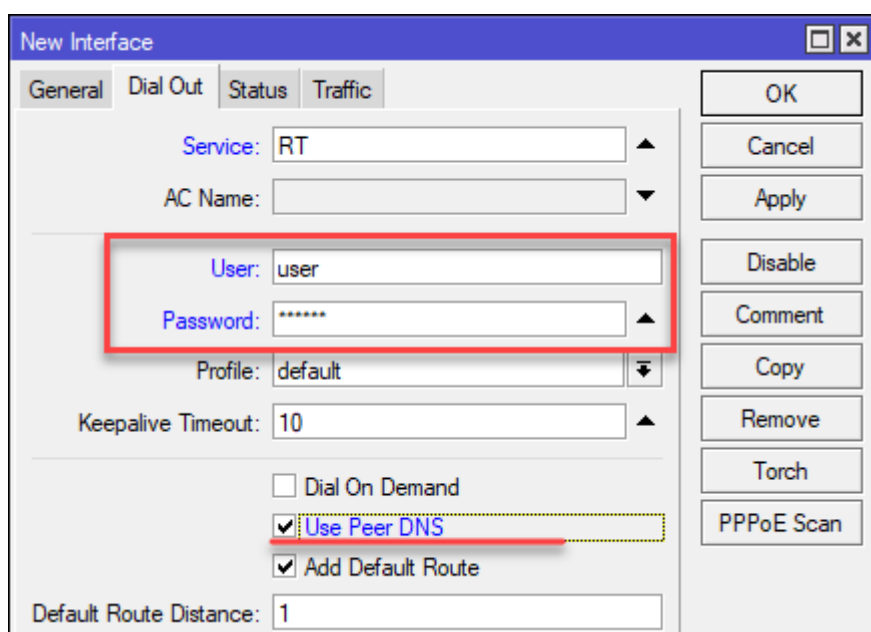
## Настройка подключения к интернет

В зависимости от вашего провайдера способ подключения к интернет может быть разным. Чаще всего встречается прямое подключение, когда провайдер раздает настройки по DHCP или PPPoE подключение (используется федеральным провайдером Ростелеком). Мы будем рассматривать далее прямое подключение, однако если у вас коммутируемый доступ (PPPoE или VPN), то вам потребуется перейти в раздел **PPP** и создать коммутируемое подключение типа **Client**, ниже показан пример для PPPoE Ростелеком. В качестве используемого интерфейса укажите внешний интерфейс ether5:





Затем на закладке **Dial Out** укажите данные для подключения к серверу провайдера и если вы хотите использовать его DNS-сервера установите флаг **Use Peer DNS**.

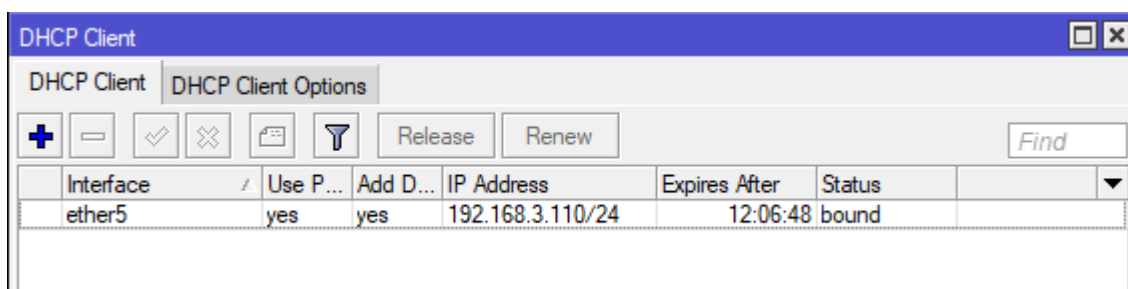
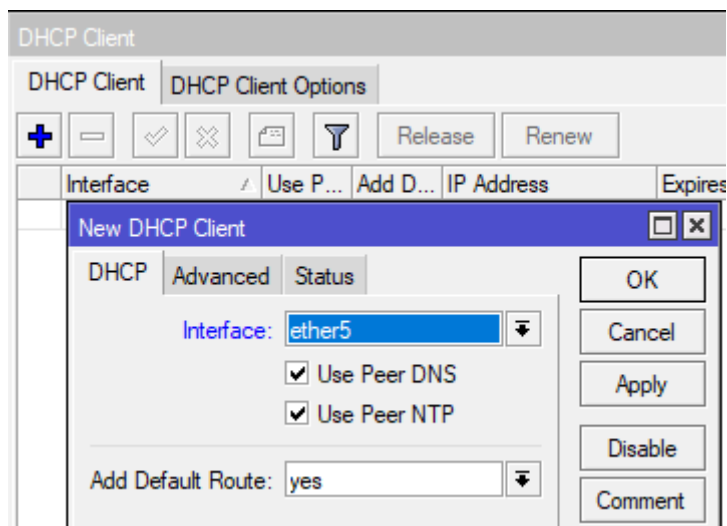


В дальнейшем, вместо внешнего интерфейса **ether5** вам потребуется указывать ваш коммутируемый интерфейс **pppoe-out1**.

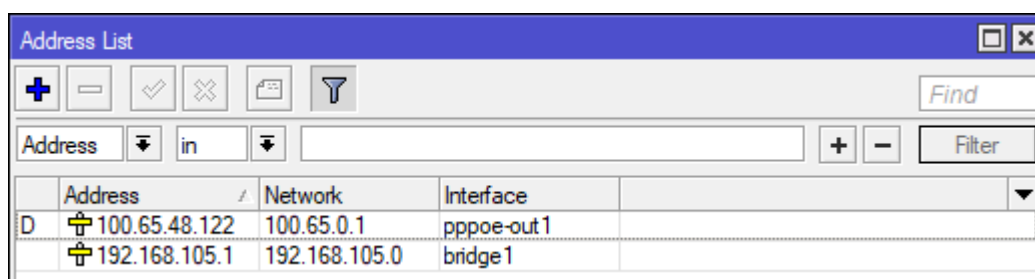
Более подробно про настройку VPN-подключений в Mikrotik вы можете прочитать в нашей статье [Настройка VPN-подключения в роутерах Mikrotik](#).

В зависимости от способа подключения вам может потребоваться настроить получение от провайдера внешнего IP-адреса, если у вас статический адрес, то переходим в **IP - Addresses** и добавляем еще один адрес, аналогично тому, как мы делали выше, но чаще всего провайдеры используют для присвоения адресов (даже статических) протокол DHCP. В этом случае переходим в **IP - DHCP Client** и добавляем нового клиента, в качестве интерфейса указываем внешний - **ether5**.

Здесь же можем убедиться, что IP-адрес от провайдера получен:

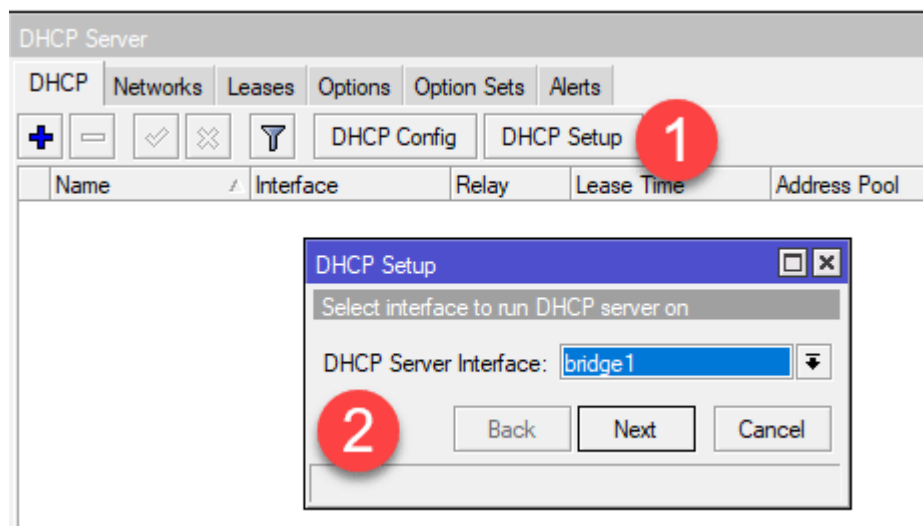


Для коммутируемых подключений DHCP-клиент настраивать не нужно, интерфейс получит адрес самостоятельно, чтобы убедиться в этом, еще раз откроем **IP - Addresses**, где должен появиться еще один адрес с индексом **D** (динамический) и принадлежащий коммутируемому подключению.



## Настройка сетевых служб (DHCP, DNS) и раздача интернета в локальную сеть

Одной из наиболее важных сетевых служб является DHCP, сегодня уже все привыкли, что достаточно просто подключиться к сети, неважно, проводом или через Wi-Fi, а все настройки будут произведены в автоматическом режиме. Поэтому мы тоже начнем с DHCP, для этого перейдем в **IP - DHCP Server** и запустим мастер настройки сервера **DHCP Setup**. Первым шагом потребуется указать рабочий интерфейс сервера - указываем сетевой мост bridge1, который мы настроили для локальной сети.



Затем укажем обслуживаемую сеть, которую мастер подставит автоматически, на основании адреса присвоенного интерфейсу моста:

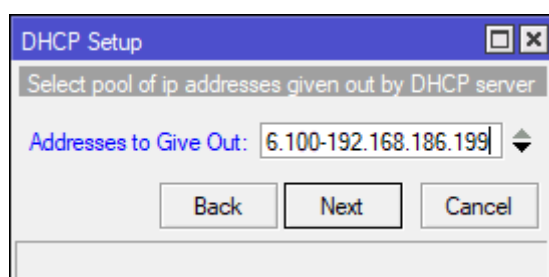
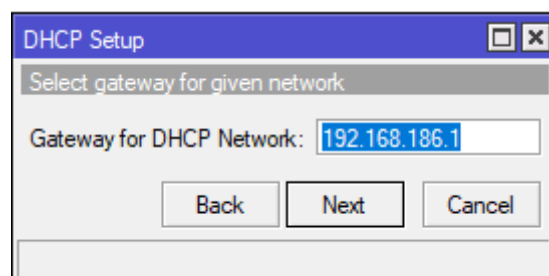
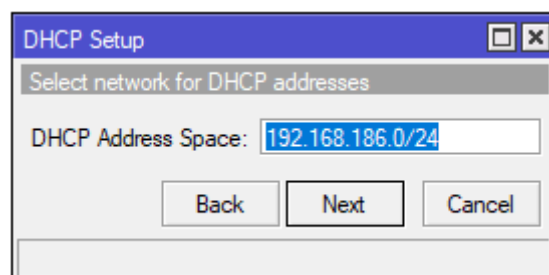
В качестве шлюза будет предложено использовать сам роутер, мастер по умолчанию подставит адрес, который мы присвоили устройству:

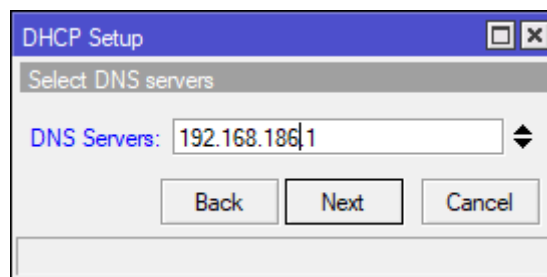
Потом будет предложено выделить диапазон адресов для выдачи клиентам, мастер предложит отдать весь доступный диапазон, но если дома еще можно так сделать, то в офисе однозначно нужно выделить статические диапазоны для серверов, сетевого оборудования, принтеров, камер и т.д. и т.п. Поэтому немного ограничим его аппетиты, мы выделили блок адресов 192.168.186.100-199, для дома или небольшого офиса этого вполне достаточно.

Ну и наконец укажем DNS-сервер, в его качестве также должен выступать роутер, иначе мы потеряем контроль над очень важной сетевой службой, поэтому указываем в этом окне адрес роутера.

Завершаем работу мастера и переходим на закладку **Leases**, здесь, по мере

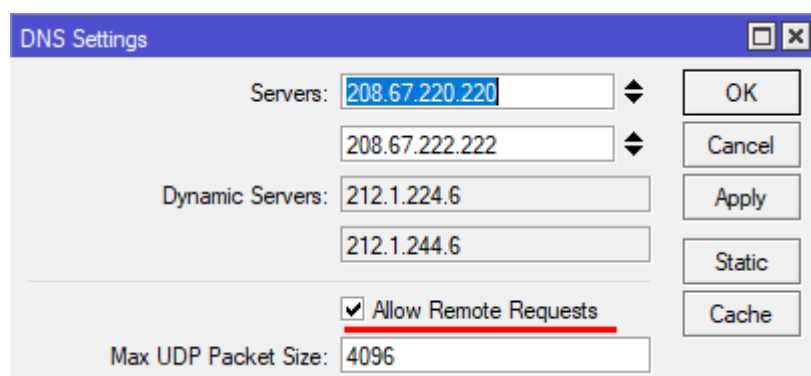
подключения, будут появляться клиенты, которым ваш роутер начнет выдавать адреса. Обратите внимание на "фирменную" особенность Mikrotik - он начинает выдавать адреса начиная с конца диапазона, т.е. от 199 до 100.





DHCP Server									
DHCP Networks Leases Options Option Sets Alerts									
<div> <div>+</div> <div>=</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> <div>Check Status</div> <div>Find</div> </div>									
	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Host Name	Expires After	
D	192.168.186.198	00:0C:29:B4:D0:05	1.0:c:29:b4:d0:5	dhcp1	192.168.186.	00:0C:29:B4:D0:05	DESKTOP-A4IHBVR	00:09:41 bou	
D	192.168.186.199	00:0C:29:B9:FF:2E		dhcp1	192.168.186.	00:0C:29:B9:FF:2E	andrey-mint	00:09:34 bou	

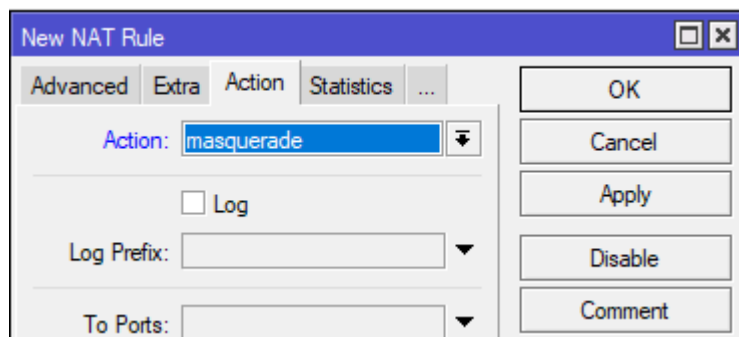
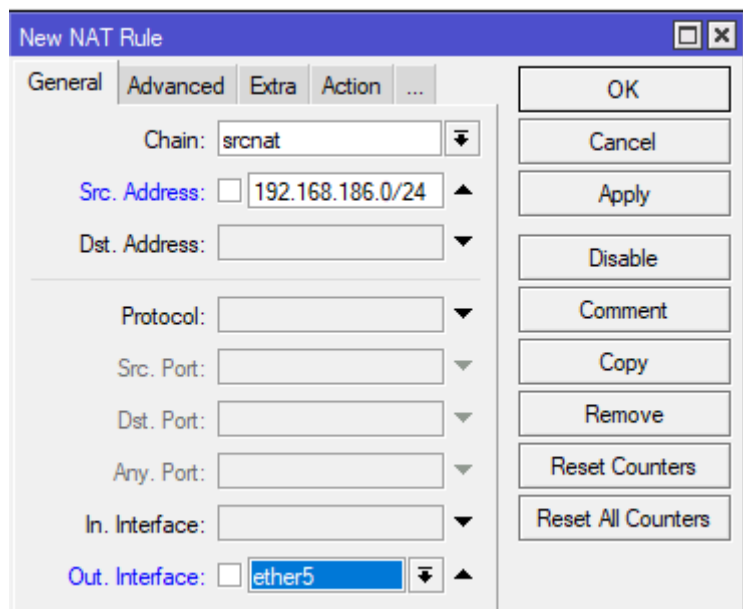
Следующим шагом настроим DNS-сервер, сделать это очень просто, открываем **IP - DNS** и добавляем в список вышестоящие DNS, это могут быть сервера провайдера или публичные службы, если вы получаете сетевые настройки от провайдера через DHCP, то его DNS-сервера уже будут указаны, они располагаются в разделе **Dynamic Servers** и не подлежат редактированию. Если вы добавите собственные сервера, то они будут иметь более высокий приоритет, в нашем случае указаны сервера OpenDNS.



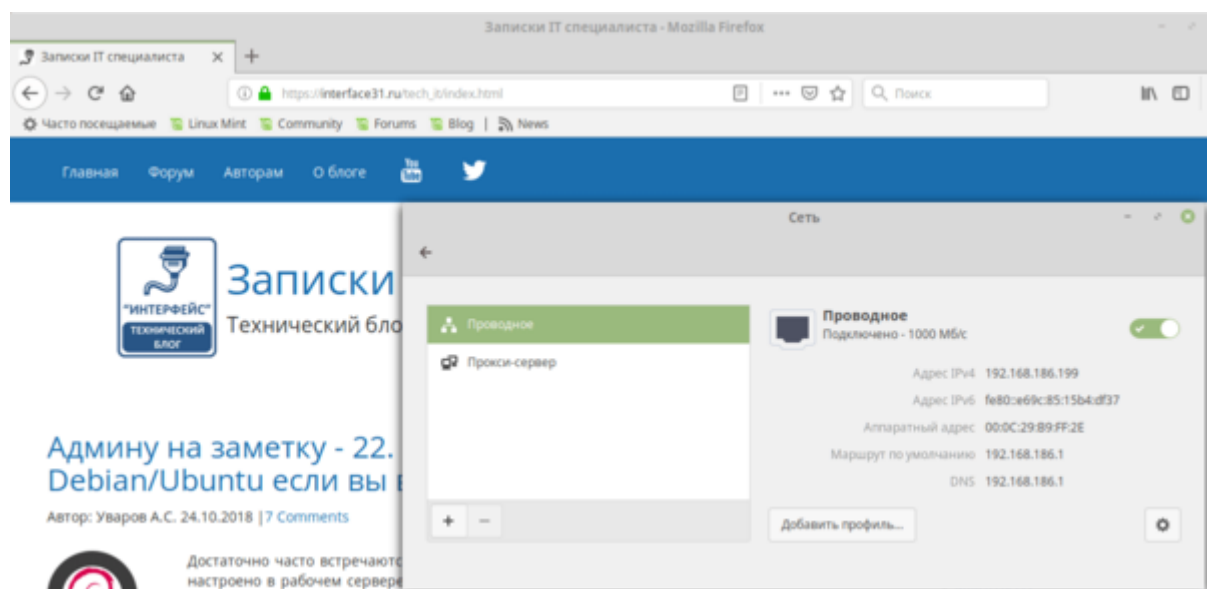
Для того, чтобы сервер мог обслуживать запросы клиентов локальной сети, не забудьте установить флаг **Allow Remote Requests**.

Базовые сетевые службы настроены, но доступа в интернет у клиентов пока нет, для этого осталось настроить службу трансляции адресов - NAT. Переходим в **IP - Firewall - NAT** и добавим новое правило, на закладке **General** в поле **Src. Address** укажем нашу локальную сеть 192.168.186.0/24, а в поле **Out. Interface** - внешний интерфейс, в нашем случае **ether5**. Если же вы используете коммутируемое подключение, то здесь следует указать его, например, **pppoe-out1**.

На закладке **Action** укажем действие - **masquerade**.

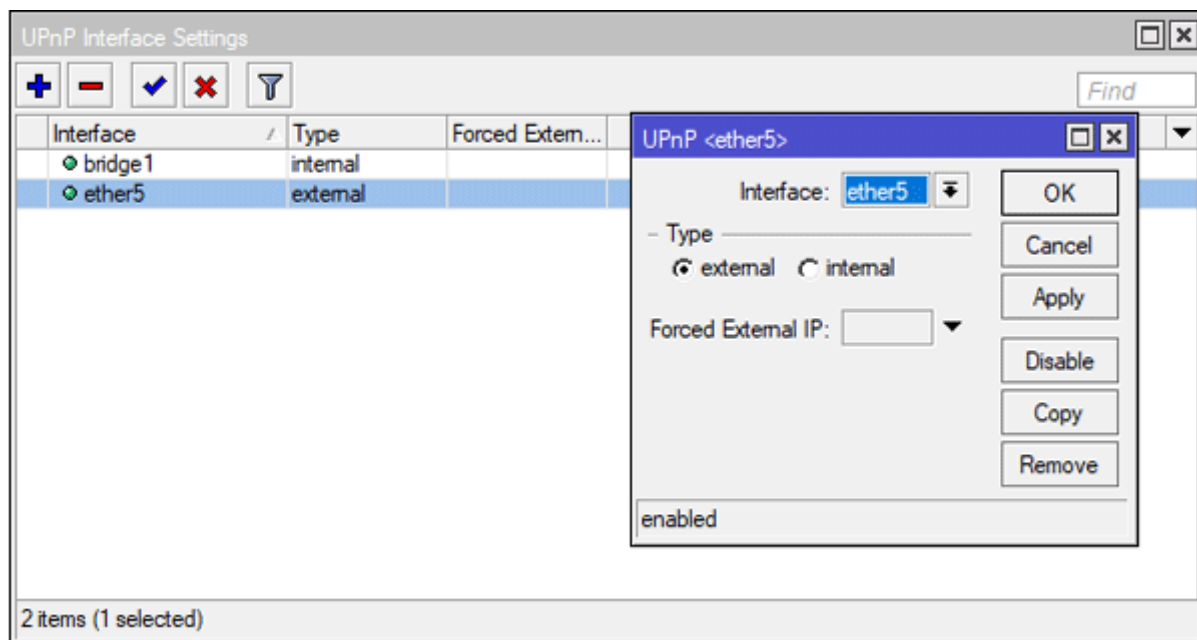
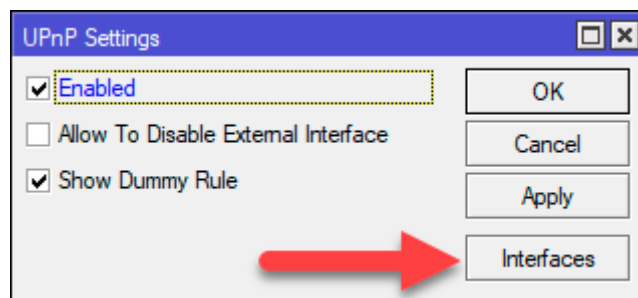


Теперь можем перейти на клиентский ПК и убедиться, что сетевые настройки получены и доступ в интернет есть.

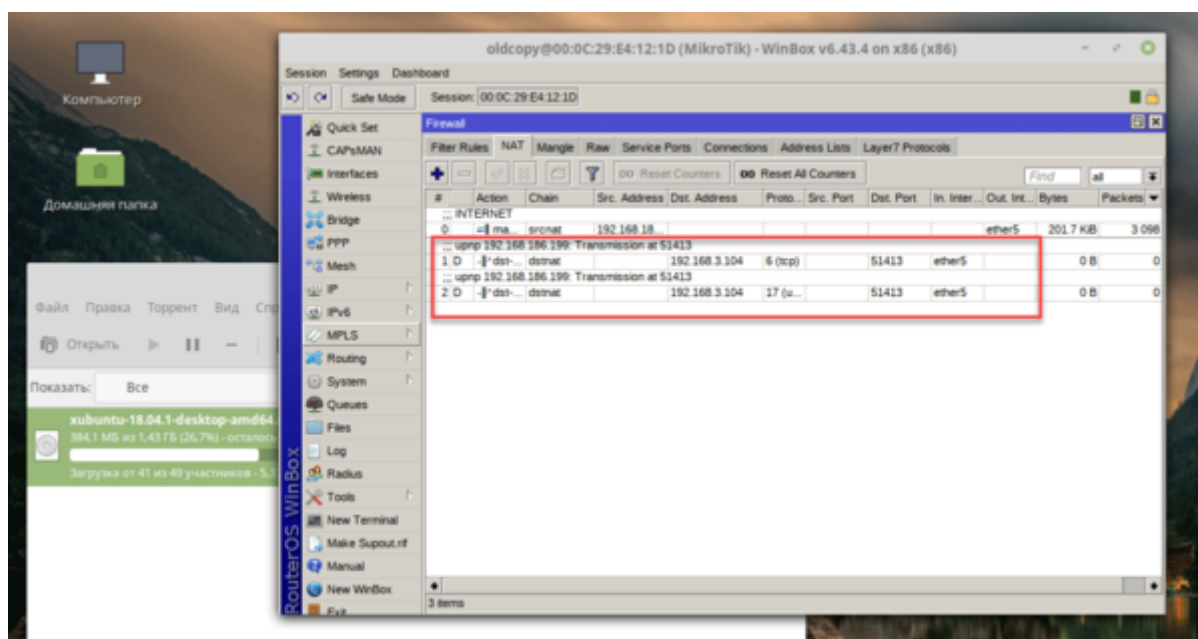


Если вы используете торренты или иной софт, требующий принимать входящие подключения, то следует также настроить службу UPnP, которая позволяет сетевому ПО автоматически осуществлять проброс нужных портов на роутере. Откроем **IP - UPnP**, включим службу и перейдем к настройке интерфейсов, нажав на кнопку **Interfaces**.

Теперь добавим два интерфейса: **bridge1** как внутренний и **ether5** как внешний, если вы используете коммутируемое подключение, то добавьте в список тот интерфейс, через который выходите в интернет, например, **pppoe-out1**.



Теперь если мы запустим на клиенте торрент, то в **IP - Firewall - NAT** созданные автоматически правила для проброса портов, если же закрыть торрент-клиент, то данные правила исчезнут. Это удобно и безопасно, а также позволяет полноценно использовать современные сетевые приложения.



## Настройка межсетевого экрана



Сетевой экран, он же фаерволл или брандмауэр (оба этих слова обозначают в английском и немецком языках противопожарную стену) является важнейшей частью роутера и было бы серьезной ошибкой выставить устройство в интернет не настроив брандмауэр. Поэтому перейдем в **IP - Firewall - Filter Rules** и приготовимся остаться тут надолго. Вообще-то гораздо быстрее и проще настроить межсетевой экран из командной строки, но так как наш материал рассчитан на начинающих, то мы будем это делать при помощи графического интерфейса Winbox.

Существует два основных состояния брандмауэра: **нормально открытый**, когда разрешено все, что не запрещено, и **нормально закрытый**, когда запрещено все, что не разрешено. Логично, что для внутренней сети следует использовать первую политику, а для внешней - вторую. По умолчанию все цепочки брандмауэра Mikrotik (а он построен на iptables) находятся в состоянии **ACCEPT**, т.е. разрешено.

Начнем с подключений к самому роутеру или цепочки **input**. В первую очередь добавим правило-пустышку разрешающее подключение к устройству из локальной сети. Почему "пустышку"? Потому что это и так разрешено, но данное правило будет нашей страховкой от случайного "выстрела в ногу", когда мы случайно запретим себе доступ к устройству. Правило-пустышка расположенное первым сработает раньше всех добавленных позже правил, в отличие от действия по умолчанию, которое сработает только тогда, если ни одно правило не подошло.

Итак, добавляем новое правило и указываем в нем **Chain** (цепочка) - **input**, **Src. Address** - **192.168.186.0/24** - диапазон вашей сети и **In. Interface** - **bridge1**, локальный интерфейс. Действия задаются на закладке **Action**, но так как **accept** (разрешить) уже установлено по умолчанию, то можно просто нажать OK.

The image shows a screenshot of the 'New Firewall Rule' window in Mikrotik Winbox. The window has a title bar with standard window controls. Below the title bar are tabs for 'General', 'Advanced', 'Extra', 'Action', and 'Statistics'. The 'General' tab is selected. In the 'Chain' dropdown, 'input' is selected. The 'Src. Address' field contains '192.168.186.0/24'. The 'In. Interface' dropdown shows 'bridge1'. The 'Action' tab is visible in the background, showing 'Accept' as the default action. On the right side of the window, there are several buttons: 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters'.

Также примите себе за правило давать для каждой записи детальные комментарии, чтобы впоследствии можно было быстро понять ее назначение. Особенно это касается правил, назначение которых неочевидно.

Следующим правилом разрешим входящие подключения на внешнем интерфейсе для уже установленных и связанных соединений, создаем новое правило: **Chain - input**, **In. Interface - ether5**, в **Connection State** устанавливаем флаг **established** и **related**, так как действие у нас снова **accept**, то просто сохраняем правило.

New Firewall Rule

General Advanced Extra Action Statistics

Chain: input

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface: ether5

Out. Interface:

Connection Type:

Connection State: ☐ invalid ☒ established ☒ related ☐ new ☐ untracked

Connection NAT State:

Затем запретим входящие пакеты в состоянии **invalid**, это пакеты которые не являются первыми и не принадлежат ни одному установленному соединению. Какого-либо смысла обрабатывать их нет, просто отбрасываем. Создаем правило **Chain - input**, **In. Interface - ether5**, в **Connection State** устанавливаем флаг **invalid** и переходим на закладку **Action** и ставим действие **drop**.

Firewall Rule <>

General Advanced Extra Action Statistics

Action: drop

☐ Log

Log Prefix:

Ниже располагаем разрешающие правила для различного типа входящего трафика. Обязательно разрешим роутеру принимать протокол ICMP: **Chain - input**, **Protocol - icmp**, **In. Interface - ether5**. ICMP - это не только пинги, но и гораздо более важные вещи, например, определение минимального MTU канала связи (PMTU).

The screenshot shows the 'New Firewall Rule' window with the following configuration:

- Chain: input
- Src. Address: (empty)
- Dst. Address: (empty)
- Protocol: ☐ icmp
- Src. Port: (empty)
- Dst. Port: (empty)
- Any. Port: (empty)
- In. Interface: ☐ ether5
- Out. Interface: (empty)

И самым последним создаем правило запрещающее все остальные подключения к роутеру: **Chain - input, In. Interface - ether5**, на закладке **Action** и ставим действие **drop**.

Если у вас коммутируемое подключение, то продублируйте правило для интерфейса, который смотрит в сеть провайдера, в большинстве случаев это избыточно, но вполне оправдано с точки зрения безопасности.

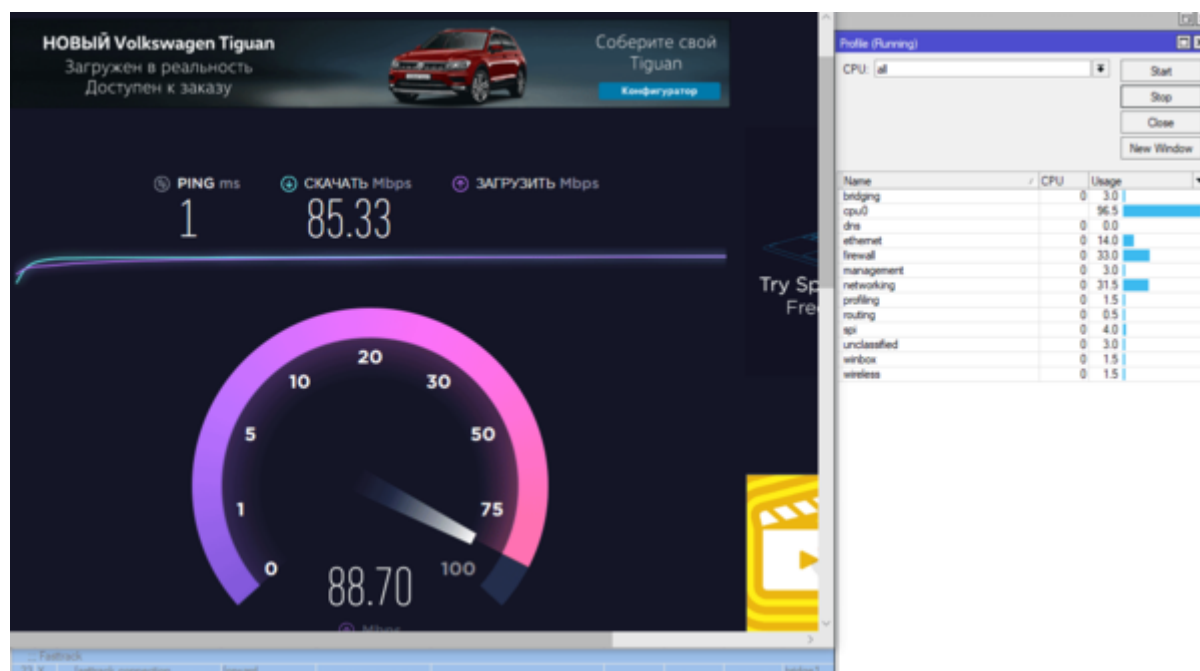
В последствии дополнительные разрешающие правила следует размещать **ниже** правила запрещающего invalid, но **выше** правила блокирующего все входящие подключения.

Данный набор правил является минимально необходимым и надежно закрывает ваше устройство от внешней сети, оно даже не будет отвечать на пинги, также невозможны внешние подключения. На наш взгляд выставлять управление устройством, особенно Winbox во внешнюю сеть - плохая идея, если же вам требуется удаленный доступ к роутеру, то следует использовать иные методы, например, через VPN.

При наличии базовых знаний по работе сетей работу с брандмауэром Mikrotik нельзя назвать сложной, особенно если вы работали с iptables (который здесь и находится "под капотом"), понимая откуда должен прийти пакет и куда попасть - создание новых правил не должно вызывать затруднений.

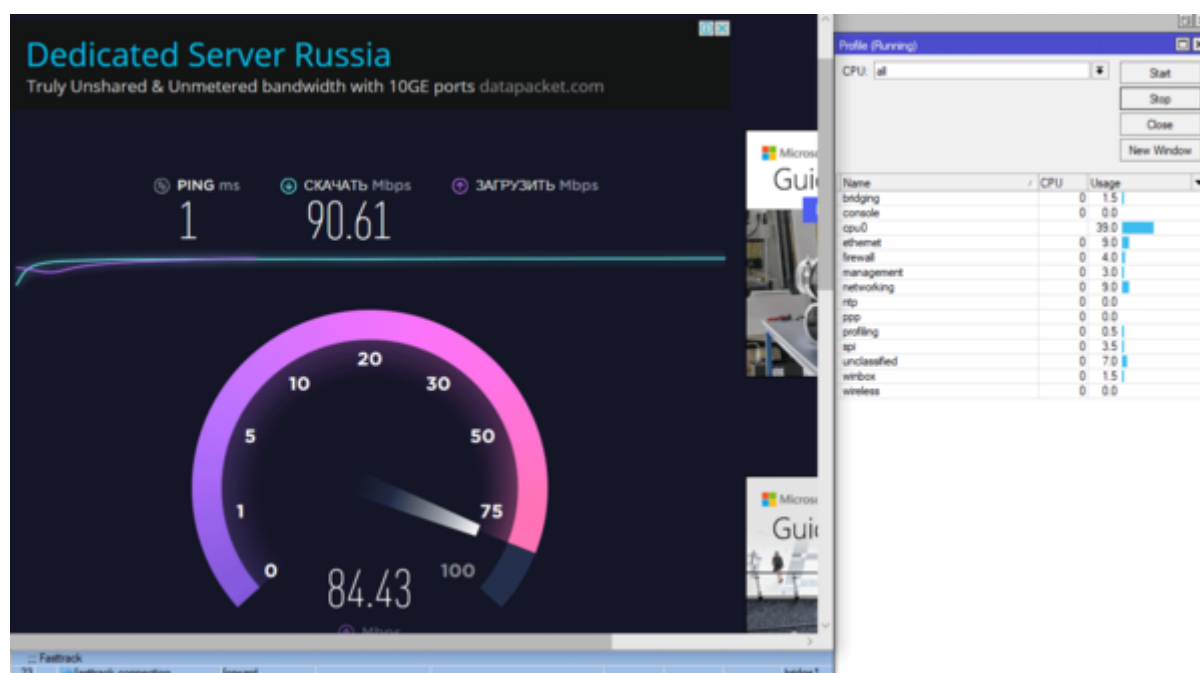
Закончим с собственными соединениями роутера и перейдем к транзитным, т.е. от клиентов локальной сети в интернет и обратно. За это отвечает цепочка **forward**, но прежде, чем переходить к правилам следует обратить внимание на еще одну фирменную технологию. Она называется **Fasttrack** и предусматривает упрощенную передачу пакетов, что позволяет значительно повысить производительность роутера. Однако это достигается ценой того, что к такому трафику не могут быть применены многие правила брандмауэра и иные сетевые технологии (подробнее можно прочитать на официальном сайте).

Так нужен ли Fasttrack? Смотрите сами, мы взяли RB2011 и прокачали через него при помощи Speedtest поток в 90 Мбит/с (при тарифе в 100 Мбит/с) сначала с отключенным Fasttrack:



Фактически мы уже положили роутер на лопатки, загрузив CPU на 100% при помощи только одного теста. В реальной жизни несколько активно использующих сеть клиентов сделают это даже на более узком канале. Говорить о какой-то сложной обработке трафика или каких-либо продвинутых сетевых функциях увы уже не приходится.

Включим Fasttrack и повторим тест:



Как видим, картина существенно изменилась, полная утилизация канала уже не вызывает предельной загрузки роутера и остается вполне достаточно ресурсов для реализации каких-то продвинутых сетевых конфигураций или создания сложных правил обработки трафика.

Поэтому первым делом добавим следующее правило: **Chain - forward, Connection State: established, related**, а на закладке Action установим действие **fasttrack connection**.

The image contains two screenshots of the Mikrotik WinBox 'New Firewall Rule' dialog. The top screenshot shows the 'General' tab with 'Chain' set to 'forward', 'Src. Address' and 'Dst. Address' empty, 'Connection Type' empty, and 'Connection State' with 'established' and 'related' checked. The bottom screenshot shows the 'Action' tab with 'Action' set to 'fasttrack connection', 'Log' unchecked, and 'Log Prefix' empty.

Таким образом мы пустим через Fasttrack все пакеты уже установленных транзитных соединений, и скажем честно, особой потребности как-то сложно обрабатывать такой трафик на роутере нет. Простую фильтрацию можно легко достичь предварительной обработкой и маркировкой пакетов, а на что-то более сложное у Mikrotik не хватит ресурсов, в этом случае есть смысл задуматься о полноценном роутере с прокси на базе Linux.

Остальной трафик из локальной сети в интернет мы никак не трогаем, потому что по умолчанию все и так разрешено, а любые дополнительные разрешающие правила окажутся пустышками, бесцельно расходующими вычислительные ресурсы роутера. Поэтому будем сразу закрываться от доступа из всемирной сети. Но прежде точно также разрешим уже установленные и связанные соединения: **Chain - forward, In. Interface - ether5, Out. Interface - bridge1**, ниже в **Connection State** устанавливаем флаги **established** и **related**, действие **accept**.

**New Firewall Rule**

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface: ☐

Out. Interface: ☐

Connection State: ☐ invalid ☒ established ☒ related ☐ new ☐ untracked

Connection NAT State:

Запретим пакеты в состоянии **invalid**: **Chain - forward**, **In. Interface - ether5**, **Connection State - invalid**, действие **drop**. Ниже, если необходимо, размещаем разрешающие правила, для доступа извне в локальную сеть.

Затем закрываемся от внешнего мира: **Chain - forward**, **In. Interface - ether5**, **Out. Interface - bridge1**, **Connection NAT State - ! dstnat**, действие **drop**. Общий принцип здесь такой же, как и в цепочке **input**, разрешаем установленные и связанные соединения, запрещаем **invalid**, потом идут собственные правила и запрет всего остального трафика. Единственный момент, в данном правиле мы поставили исключение для **dstnat**-трафика, т.е. для проброшенных наружу портов, если этого не сделать, то правила созданные UPnP будут работать некорректно. В итоге вы должны получить следующую конфигурацию брандмауэра:

Firewall														
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols														
+ [ ] [														

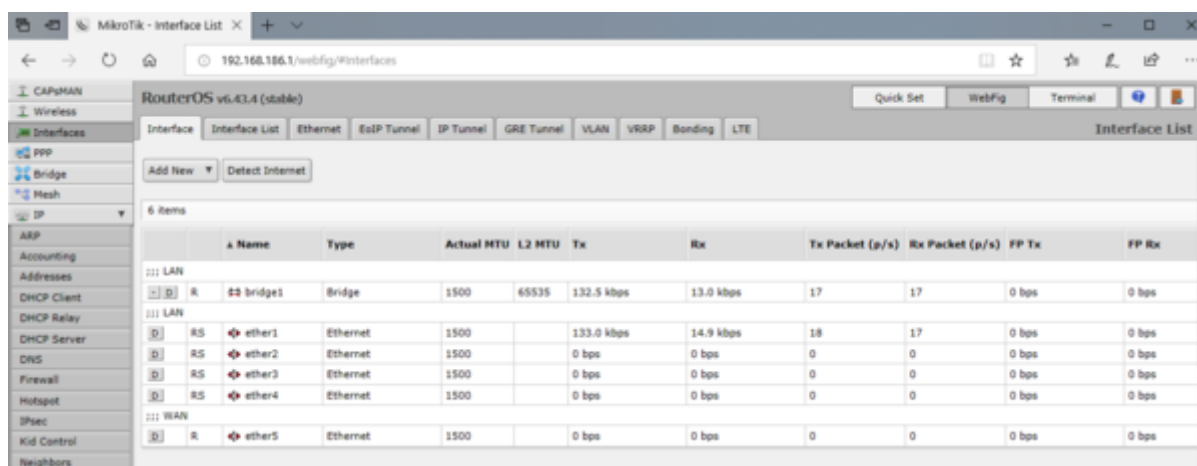


Это - минимально достаточная базовая конфигурация, которая обеспечивает необходимый уровень безопасности и на которую мы будем опираться в наших следующих материалах.

## Настройка безопасности роутера

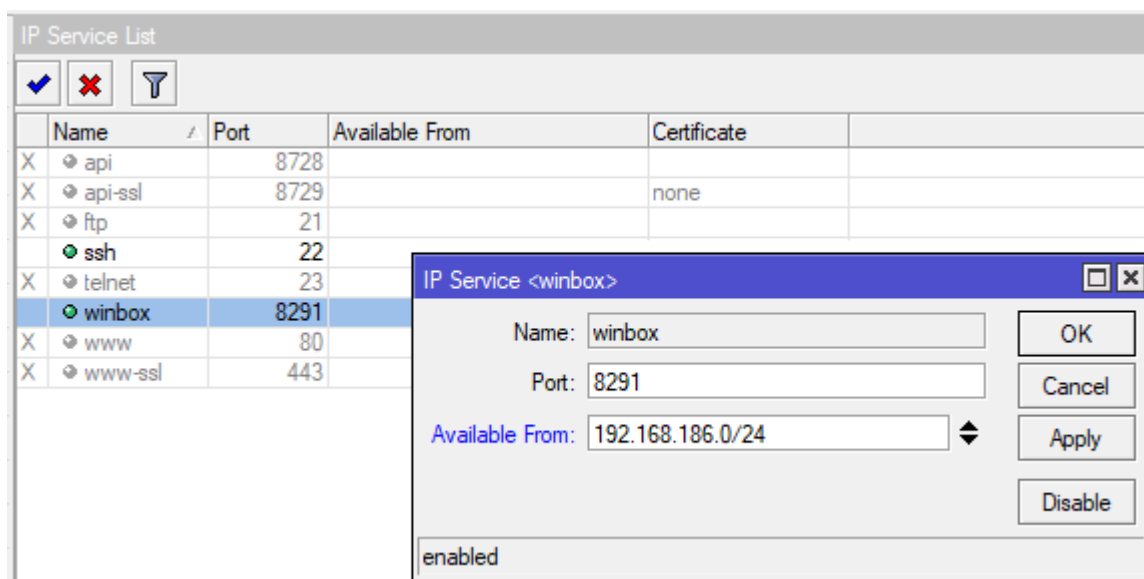
Основная настройка нашего роутера закончена, он уже может быть введен в эксплуатацию и обслуживать запросы клиентов локальной сети. А мы тем временем перейдем к дополнительным настройкам, которые существенно влияют на безопасность устройства.

Прежде всего перейдем в **IP - Services**, здесь перечислены включенные сетевые службы самого роутера, смело отключаем все неиспользуемые, включая и веб-интерфейс. Честно говоря, мы вообще не видим в нем смысла, так как по внешнему виду он полностью повторяет Winbox, но несколько менее удобен в использовании.



Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	PP Tx	PP Rx
bridge1	Bridge	1500	65535	132.5 kbps	13.0 kbps	17	17	0 bps	0 bps
ether1	Ethernet	1500		133.0 kbps	14.9 kbps	18	17	0 bps	0 bps
ether2	Ethernet	1500		0 bps	0 bps	0	0	0 bps	0 bps
ether3	Ethernet	1500		0 bps	0 bps	0	0	0 bps	0 bps
ether4	Ethernet	1500		0 bps	0 bps	0	0	0 bps	0 bps
ether5	Ethernet	1500		0 bps	0 bps	0	0	0 bps	0 bps

Обычно мы оставляем только Winbox и SSH, для Winbox не будет лишним задать диапазон допустимых адресов для подключения, ограничив их локальной сетью. При необходимости можно указать несколько сетей (сеть офиса и сеть филиала).



Name	Port	Available From	Certificate
api	8728		
api-ssl	8729		none
ftp	21		
ssh	22		
telnet	23		
winbox	8291	192.168.186.0/24	
www	80		
www-ssl	443		

IP Service <winbox>

Name: winbox

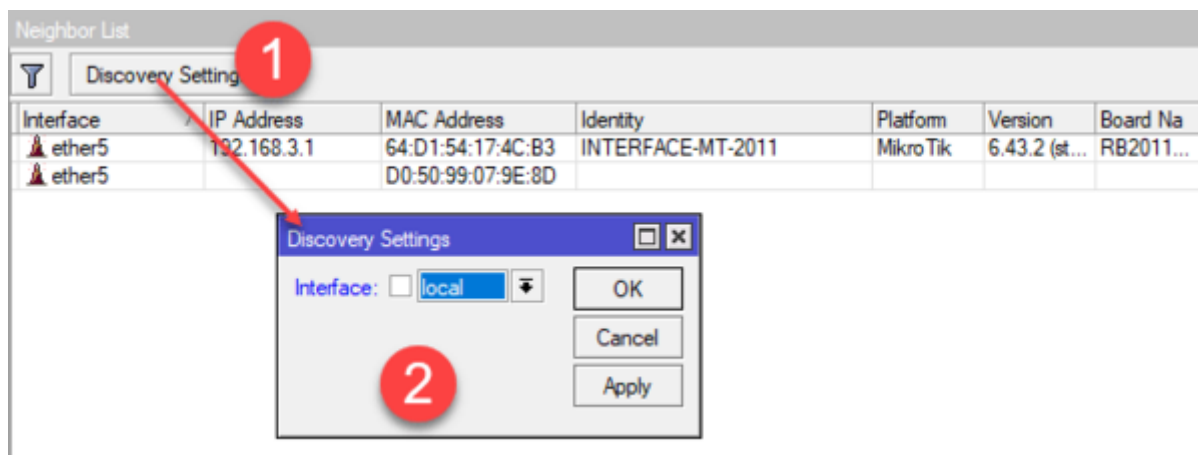
Port: 8291

Available From: 192.168.186.0/24

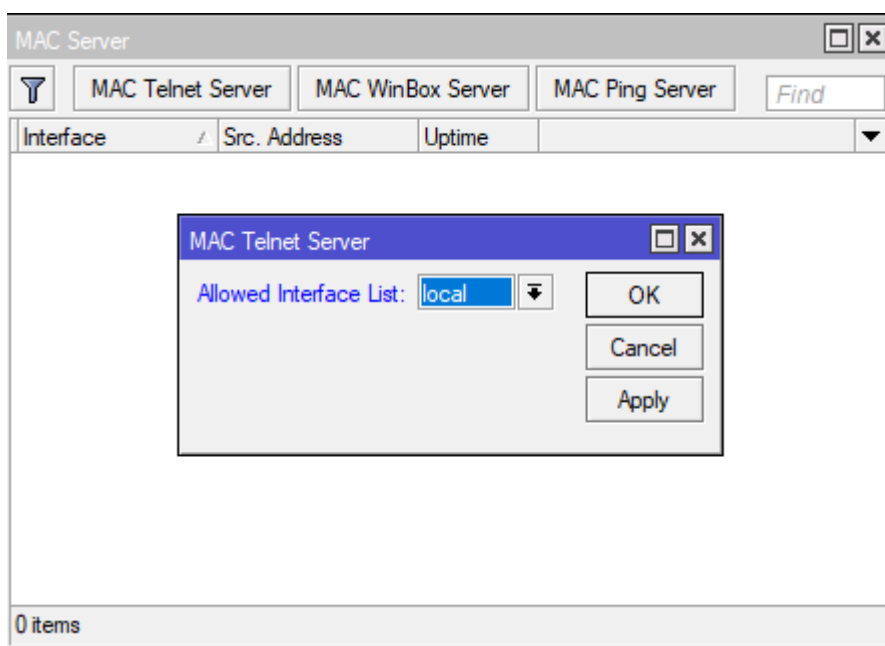
enabled

OK Cancel Apply Disable

Следующим шагом заходим в **IP - Neighbors**, данные настройки отвечают за автоматическое обнаружение устройств Mikrotik в сети, по вполне понятным причинам эту функцию следует ограничить только локальной сетью. Поэтому нажимаем **Discovery Settings** и в списке **Interface** выбираем созданный нами в самом начале список интерфейсов **local**.

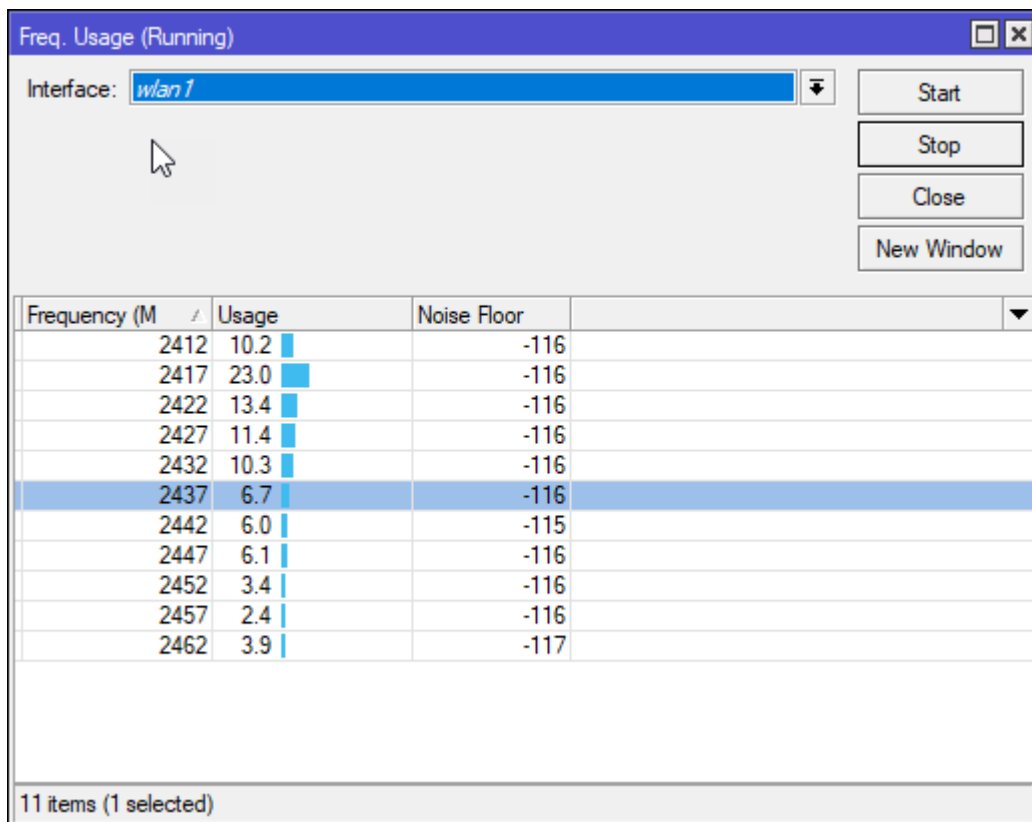


Обнаружение устройства и возможность подключения к нему по MAC-адресу - несомненно удобно, но также только в локальной сети. Открываем **Tools - MAC Server** и устанавливаем в **Allowed Interface List** список интерфейсов **local**.

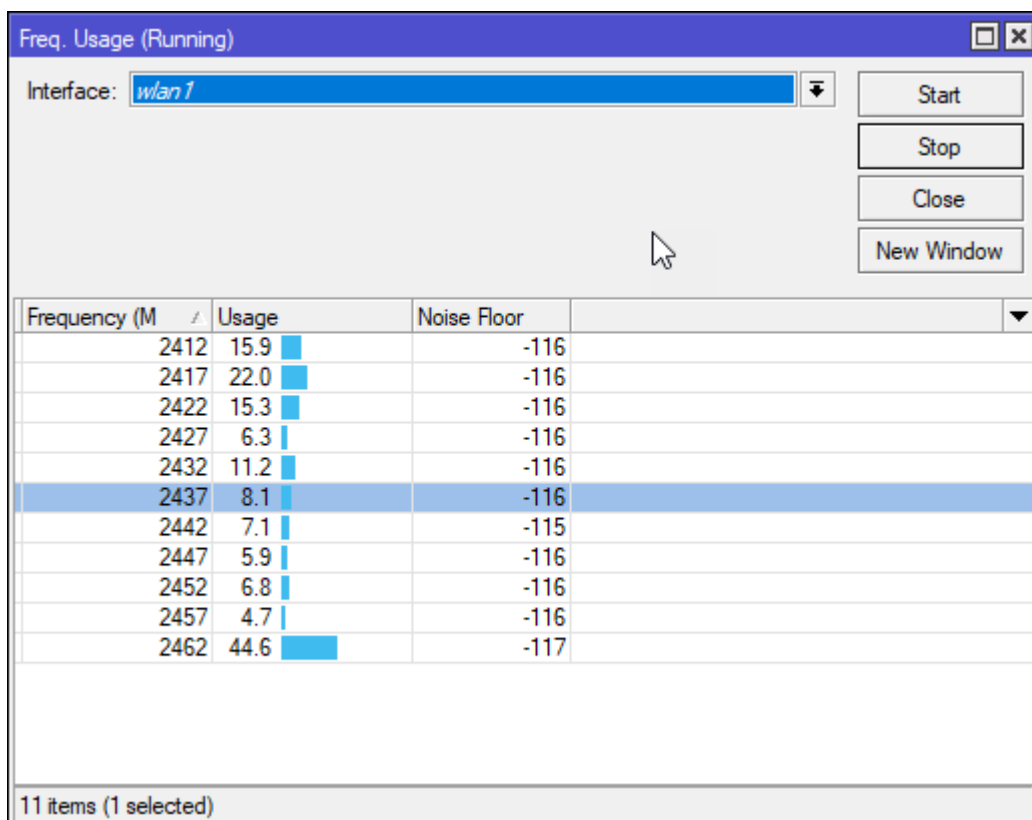


Ну и наконец сменим учетную запись по умолчанию. Перейдем в **System - Users** и создадим собственный аккаунт с полными правами, выйдем из Winbox и попробуем зайти с новыми учетными данными и только после этого, убедившись, что все работает правильно, можно выключить старую учетную запись.



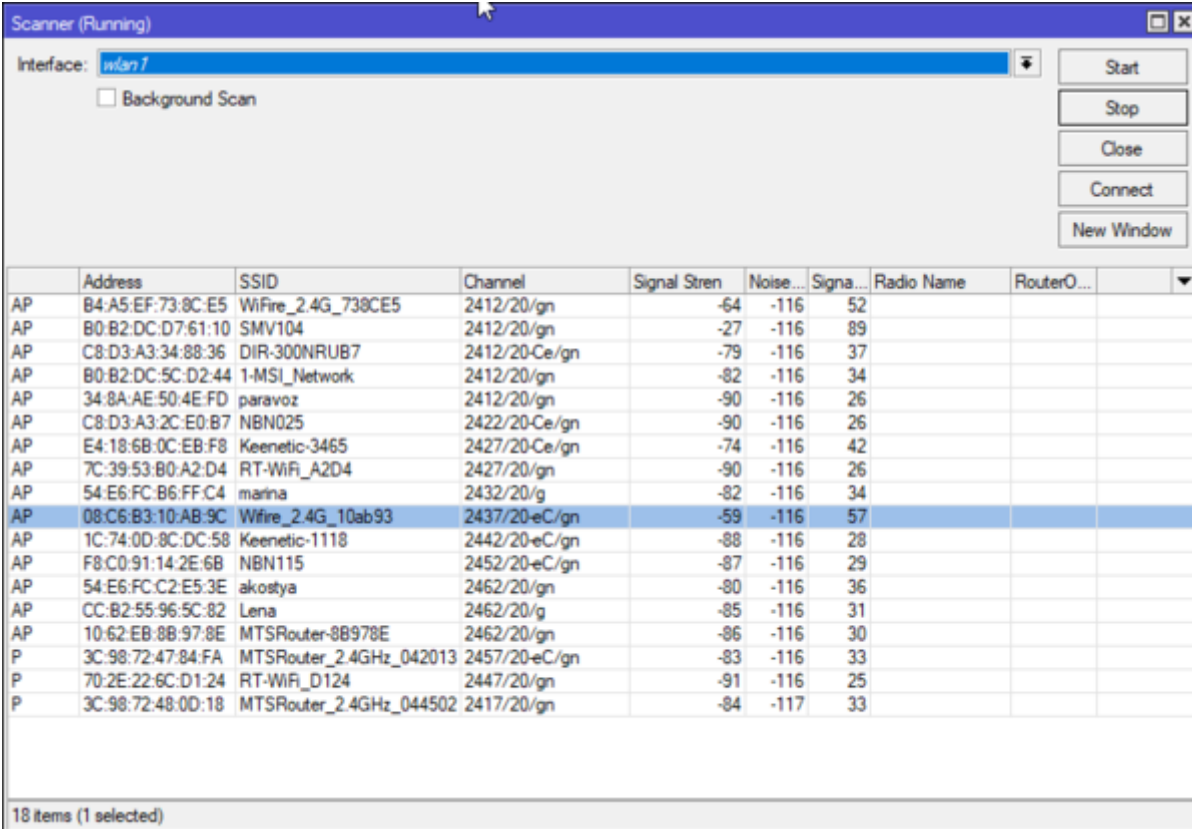


Однако не будем спешить и понаблюдаем немного подольше, как оказалось - не зря! На 11-ом канале время от времени отмечались сильные всплески непонятного характера, по которым можно было предположить наличие там не точки доступа, а какого-то иного источника излучения. Поэтому наиболее подходящим в этой ситуации можно назвать 6-й канал.



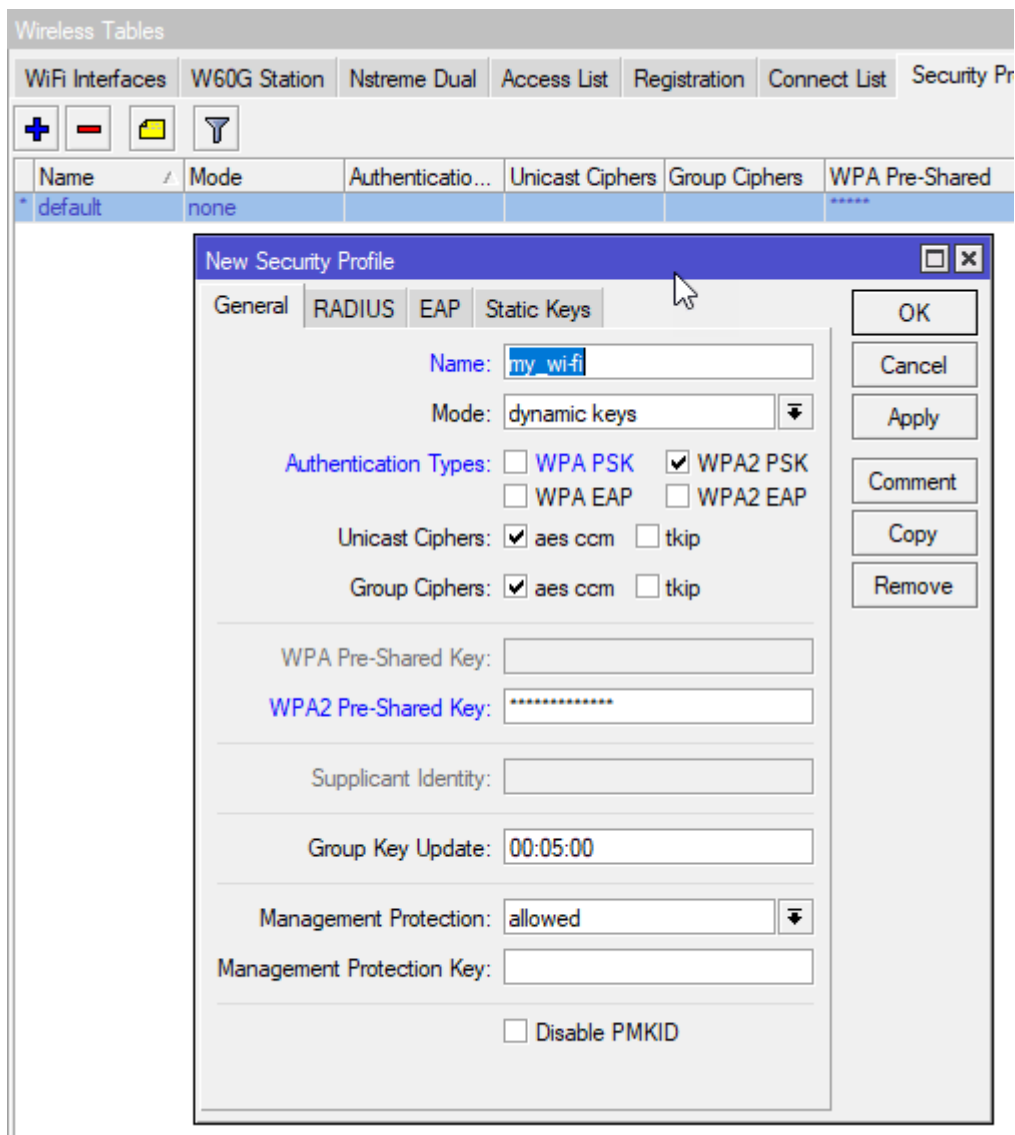
Закроем это окно и нажмем кнопку **Scanner**, который покажет нам все работающие в диапазоне точки доступа, при этом обращаем внимание на уровень сигнала. Сигнал в -35 dBm принимается за 100%, -95 dBm - 1%, шкала между этими значениями линейная, т.е. -65 dBm - 50%.

Как видим, на выбранном нами 6 канале есть только одна более-менее мощная точка с сигналом -59 dBm, что, впрочем, не сильно страшно, внутриканальные помехи достаточно легко преодолеваются на уровне протокола, что нельзя сказать о межканальных. С этим здесь достаточно неплохо, мощных источников на соседних каналах практически нет, чего не скажешь о начале диапазона, где есть очень мощная точка -27 dBm на первом канале (в реальности она стоит в 20 см от тестируемого нами роутера).



	Address	SSID	Channel	Signal Stren	Noise...	Signa...	Radio Name	RouterO...
AP	B4:A5:EF:73:8C:E5	WiFire_2.4G_738CE5	2412/20/gn	-64	-116	52		
AP	B0:B2:DC:D7:61:10	SMV104	2412/20/gn	-27	-116	89		
AP	C8:D3:A3:34:88:36	DIR-300NRUB7	2412/20-Ce/gn	-79	-116	37		
AP	B0:B2:DC:5C:D2:44	1-MSI_Network	2412/20/gn	-82	-116	34		
AP	34:8A:AE:50:4E:FD	paravoz	2412/20/gn	-90	-116	26		
AP	C8:D3:A3:2C:E0:B7	NBN025	2422/20-Ce/gn	-90	-116	26		
AP	E4:18:6B:0C:EB:F8	Keenetic-3465	2427/20-Ce/gn	-74	-116	42		
AP	7C:39:53:B0:A2:D4	RT-WiFi_A2D4	2427/20/gn	-90	-116	26		
AP	54:E6:FC:B6:FF:C4	marina	2432/20/g	-82	-116	34		
AP	08:C6:B3:10:AB:9C	WiFire_2.4G_10ab93	2437/20-eC/gn	-59	-116	57		
AP	1C:74:0D:8C:DC:58	Keenetic-1118	2442/20-eC/gn	-88	-116	28		
AP	F8:C0:91:14:2E:6B	NBN115	2452/20-eC/gn	-87	-116	29		
AP	54:E6:FC:C2:E5:3E	akostya	2462/20/gn	-80	-116	36		
AP	CC:B2:55:96:5C:82	Lena	2462/20/g	-85	-116	31		
AP	10:62:EB:8B:97:8E	MTSRouter-8B978E	2462/20/gn	-86	-116	30		
P	3C:98:72:47:84:FA	MTSRouter_2.4GHz_042013	2457/20-eC/gn	-83	-116	33		
P	70:2E:22:6C:D1:24	RT-WiFi_D124	2447/20/gn	-91	-116	25		
P	3C:98:72:48:0D:18	MTSRouter_2.4GHz_044502	2417/20/gn	-84	-117	33		

С каналом определились, теперь создадим профиль безопасности для нашей беспроводной сети в **Wireless - Security Profiles**. В нем оставляем только протокол **WPA2 PSK** и указываем ключ сети (пароль от Wi-Fi).



Теперь переходим в настройки интерфейса **wlan1** и на закладке **Wireless** последовательно меняем следующие опции: **Mode - ap bridge** - устанавливает режим точки доступа, **Band - 2GHz-only-N** - только n-режим, **Channel Width - 20 MHz** - одна из спорных настроек, устанавливает ширину канала, но в условиях реальной загруженности диапазона 2,4 ГГц в городских условиях мы считаем что стабильные 75 Мбит/с (при стандартной ширине канала в 20 МГц) лучше, чем 150 Мбит/с время от времени (при 40 МГц).

Далее указываем желаемый **SSID**, опцию **Wireless Protocol** устанавливаем, как **802.11**, в **Security Profile** указываем созданный нами ранее профиль и выключаем WPS: **WPS Mode - disabled**. На этом базовая настройка беспроводной сети закончена.



Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme Status Traffic

Mode: ap bridge

Band: 2GHz-only-N

Channel Width: 20MHz

Frequency: 2437 MHz

SSID: My-Wi-Fi

Scan List: default

Wireless Protocol: 802.11

Security Profile: my\_wi-fi

WPS Mode: disabled

Bridge Mode: enabled

Все что вам остается - это включить беспроводной интерфейс и добавить его в сетевой мост bridge1 вашей локальной сети.

Wireless Tables

WiFi Interfaces W60G Station Nstreme Dual Access List Registration Connect List Security Profiles Channels

+ - ✓ ✗ 📁 📏 CAP WPS Client Setup Repeater Scanner Freq. Usage Alignment

	Name	Type	Actual MTU	Tx	Rx	Tx Packet (p/s)
S	wlan1	Wireless (Atheros AR9...	1500	0 bps	0 bps	0 bps

Bridge

Bridge Ports VLANs MSTIs Port MST Overrides Filters NAT Hosts MDB

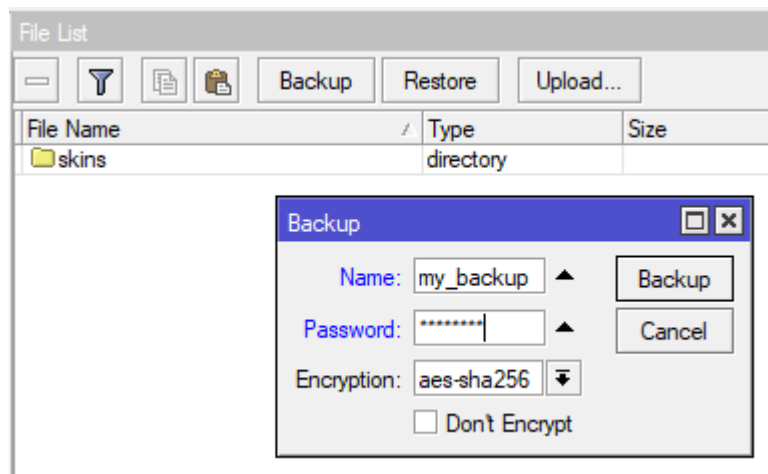
+ - ✓ ✗ 📁 📏

#	Interface	Bridge	Horizon	Trusted	Priority (h)	Path Cost	Role	Root Pat...
0	ether1	bridge1		no	80	10	disabled port	
1	ether2	bridge1		no	80	10	designated port	
2	ether3	bridge1		no	80	10	disabled port	
3	wlan1	bridge1		no	80	10	disabled port	

Более подробно о настройке беспроводных сетей вы можете прочитать в нашей статье: [Расширенная настройка Wi-Fi на роутерах Mikrotik. Режим точки доступа](#)

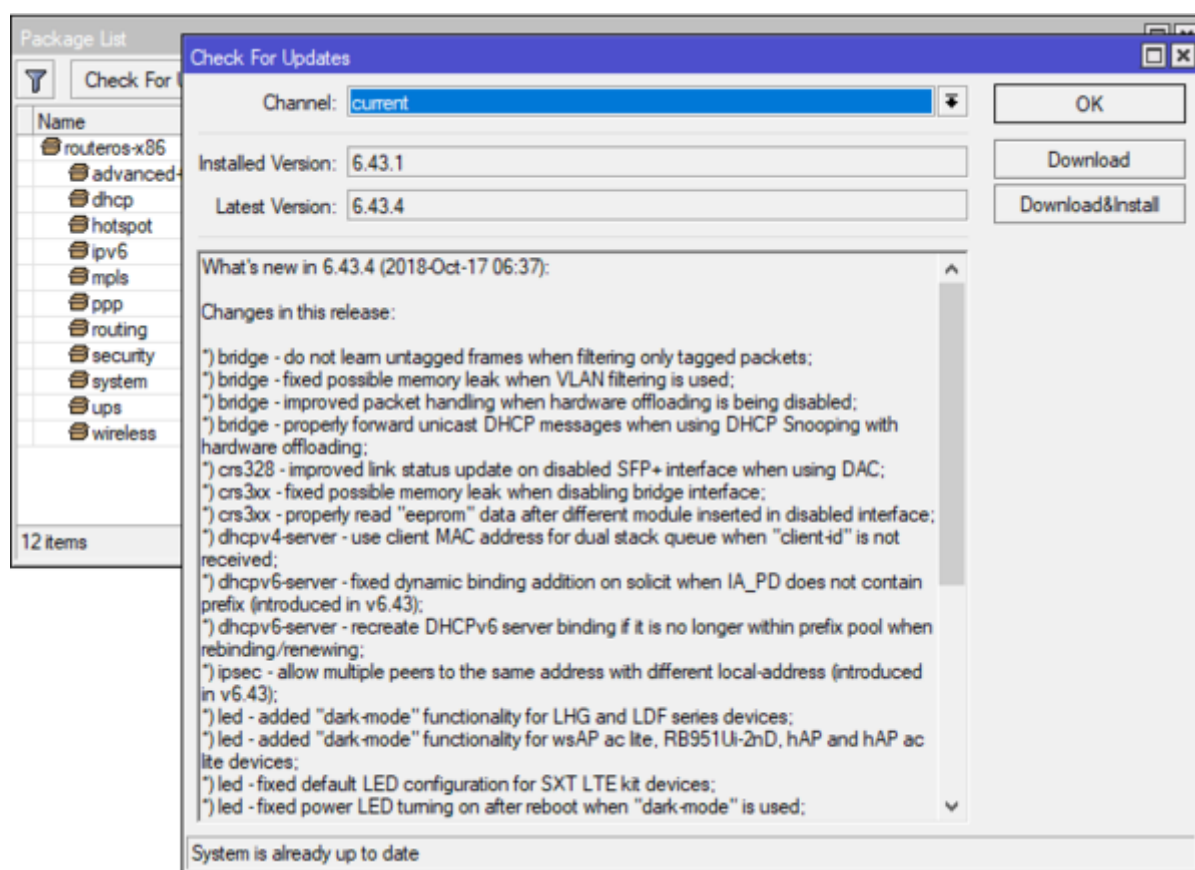
## Что нужно сделать после настройки

После того, как вы все настроили и убедились в работоспособности всех функций роутера следует сделать резервную копию настроек, это позволит в случае чего быстро развернуть готовую конфигурацию, что важно, если настройки вашего роутера сложнее чем базовые. Для этого перейдите в раздел **Files** и нажмите кнопку **Backup**, укажите имя резервной копии и пароль к файлу, после чего скачайте и сохраните резервную копию в надежном месте.



Мы рекомендуем создавать резервную копию после каждого изменения настроек роутера, это не займет много времени, но позволит существенно его сэкономить в нештатной ситуации.

Также важно постоянно поддерживать в актуальном состоянии ПО роутера, теперь, когда ваше устройство имеет доступ в интернет, обновить RouterOS становится очень просто. Перейдите в **System - Packages** и нажмите **Check For Updates**, если доступна новая версия RouterOS, то вам будет предложено скачать и установить ее.



Несмотря на то, что статья получилась весьма обширная, особых сложностей при настройке роутеров Mikrotik нет, если вы понимаете, что делаете, то с приобретением опыта настройка не будет занимать у вас много времени. В наших

последующих статьях мы также будем подразумевать, что читатель владеет базовой настройкой на уровне данной статьи и не будем возвращаться к описанным здесь вопросам.

---