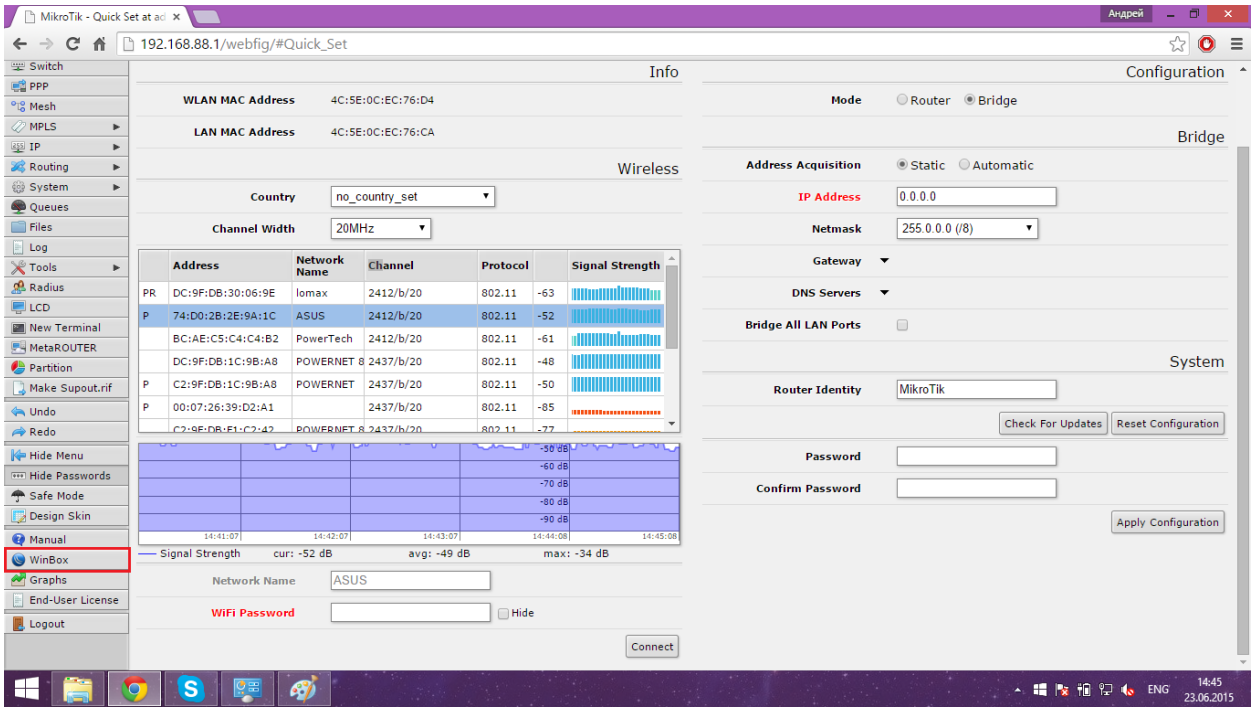
Инструкция по настройке маршрутизатора MikroTik на примере MikroTik RB2011UiAS-2HnD.

(Плотников А.В.)

Содержание

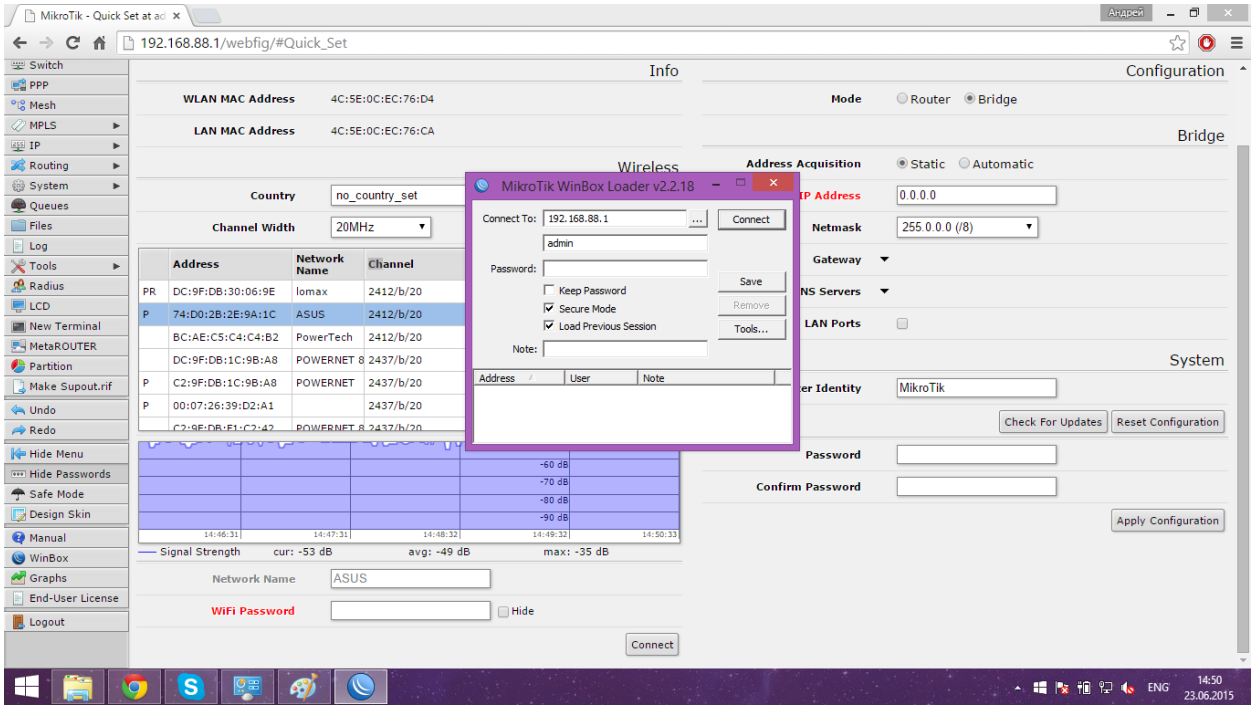
Сброс настроек и подключение через Winbox

Для начала необходимо зайти в настройки маршуритзатора. Для этого в строке браузера вводим адрес 192.168.88.1, откроется следующая страница (изображение 1).



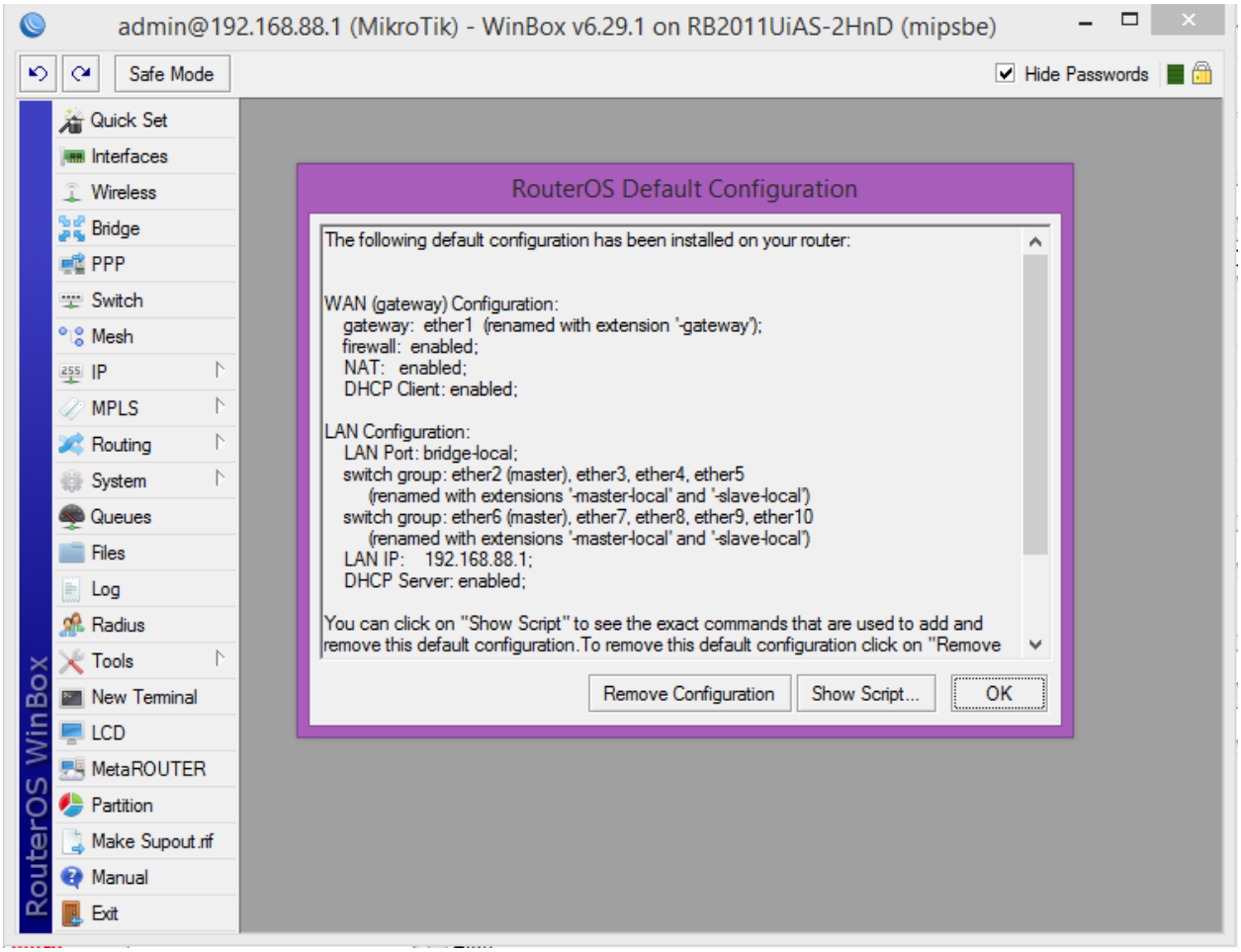
Изображение 1 – Внешний вид вэб-интерфейса.

Далее необходимо скачать с вэб-интерфейса приложение WinBox для подключения к маршрутизатору MikroTik (используется другой порт для подключения) и продолжить настройку.
Запускаем приложение WinBox, появится следующее окно, изображение 2.



Изображение 2 – Запуск программы WinBox.

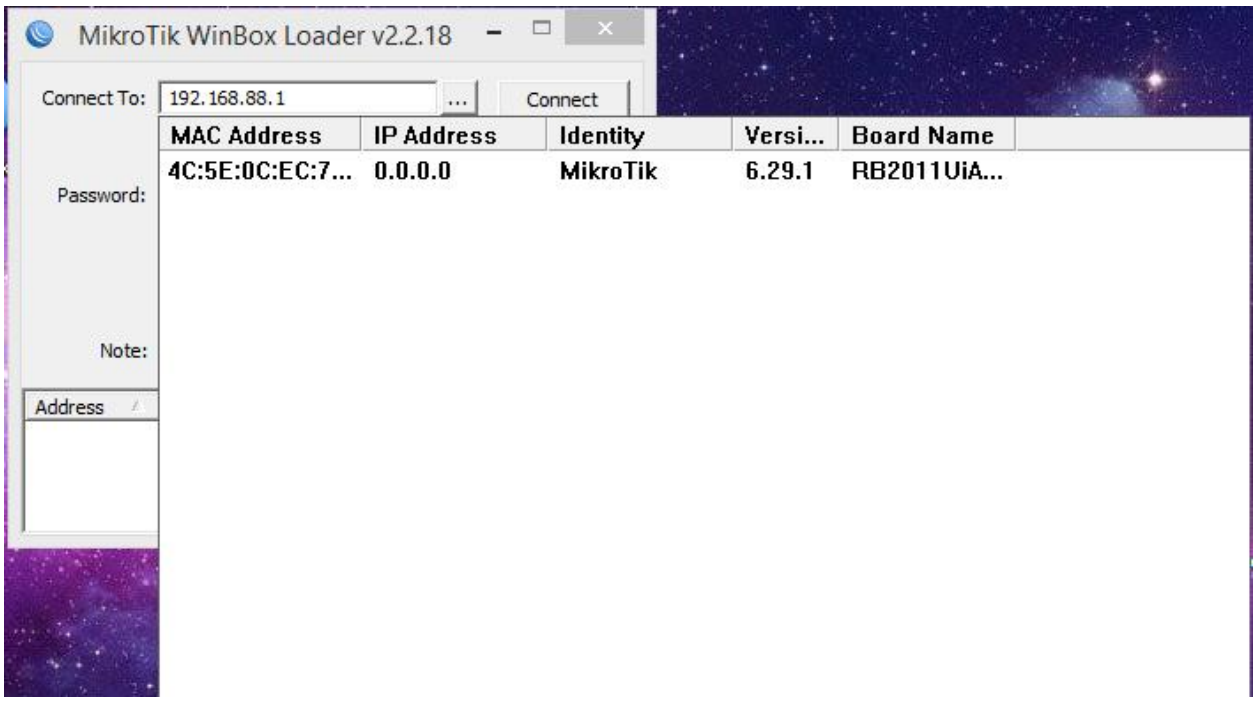
Вводим адрес 192.168.88.1, имя пользователя – «admin», пароль не вводим. Нажимаем кнопку «Connect», после чего откроется интерфейс программы с предложением сбросить настройки, изображение 3.



Изображение 3 – Информация о стандартной конфигурации.

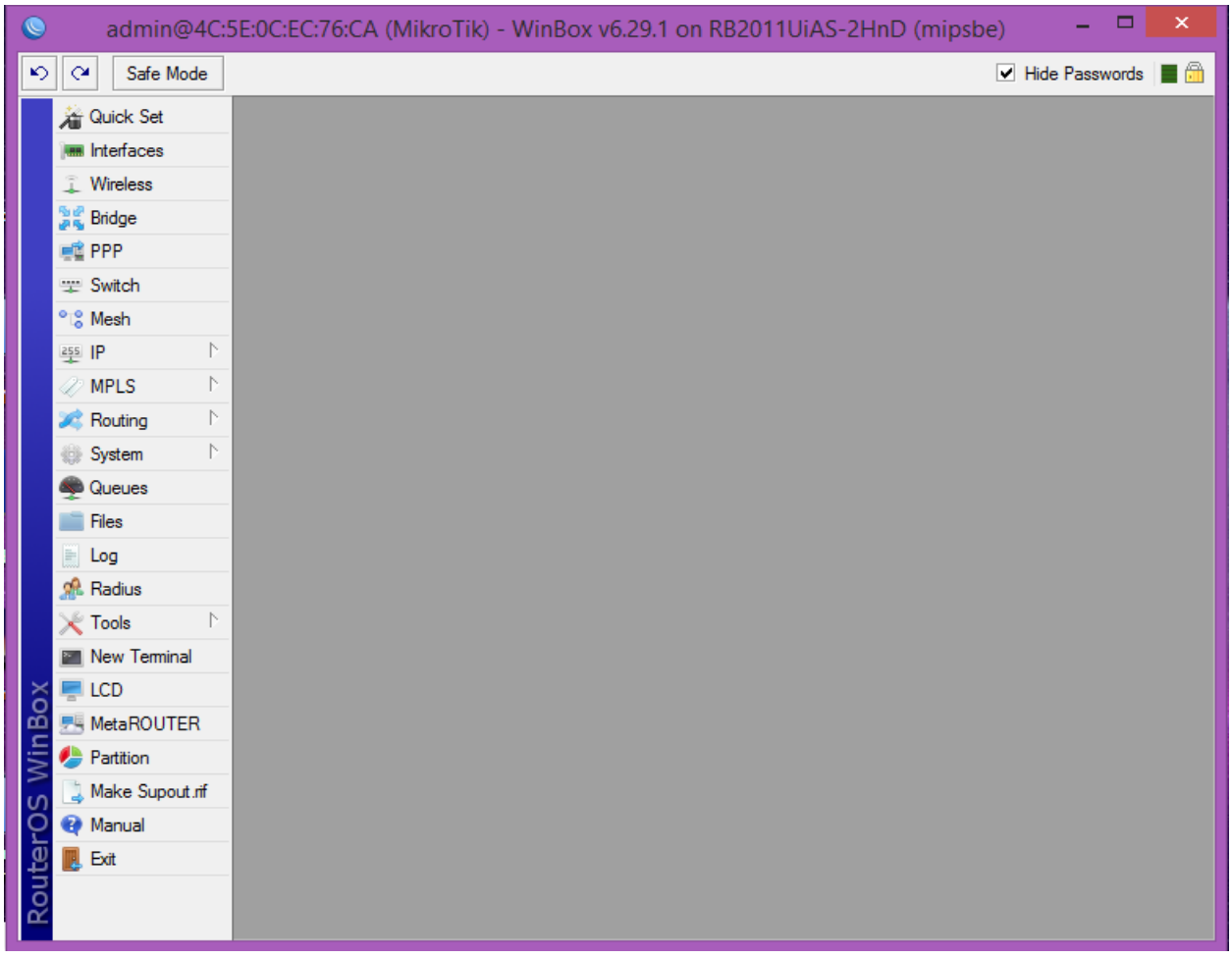
В появившемся окне с информацией о стандартной конфигурации необходимо нажать на кнопку «Remove Configuration», чтобы полностью сбросить настройки. После нажатия маршрутизатор перезагрузится, доступ через WinBox пропадет.

Подключаем кабель от компьютера в первый порт маршуризатора, запускаем WinBox снова и справа от поля «Connect To» нажимаем на кнопку «…». Появится строка с доступным устройством для подключения, изображение 4. Необходимо нажать на MAC-адрес устройства, после чего в поле «Connect To» появится MAC-адрес маршрутизатора. Логин также оставляем «admin», поле с паролем не заполняем. Нажимаем на «Connect».



Изображение 4 – Доступное устройство для подключения.

После этого снова откроется интерфейс программы WinBox, изображение 5.

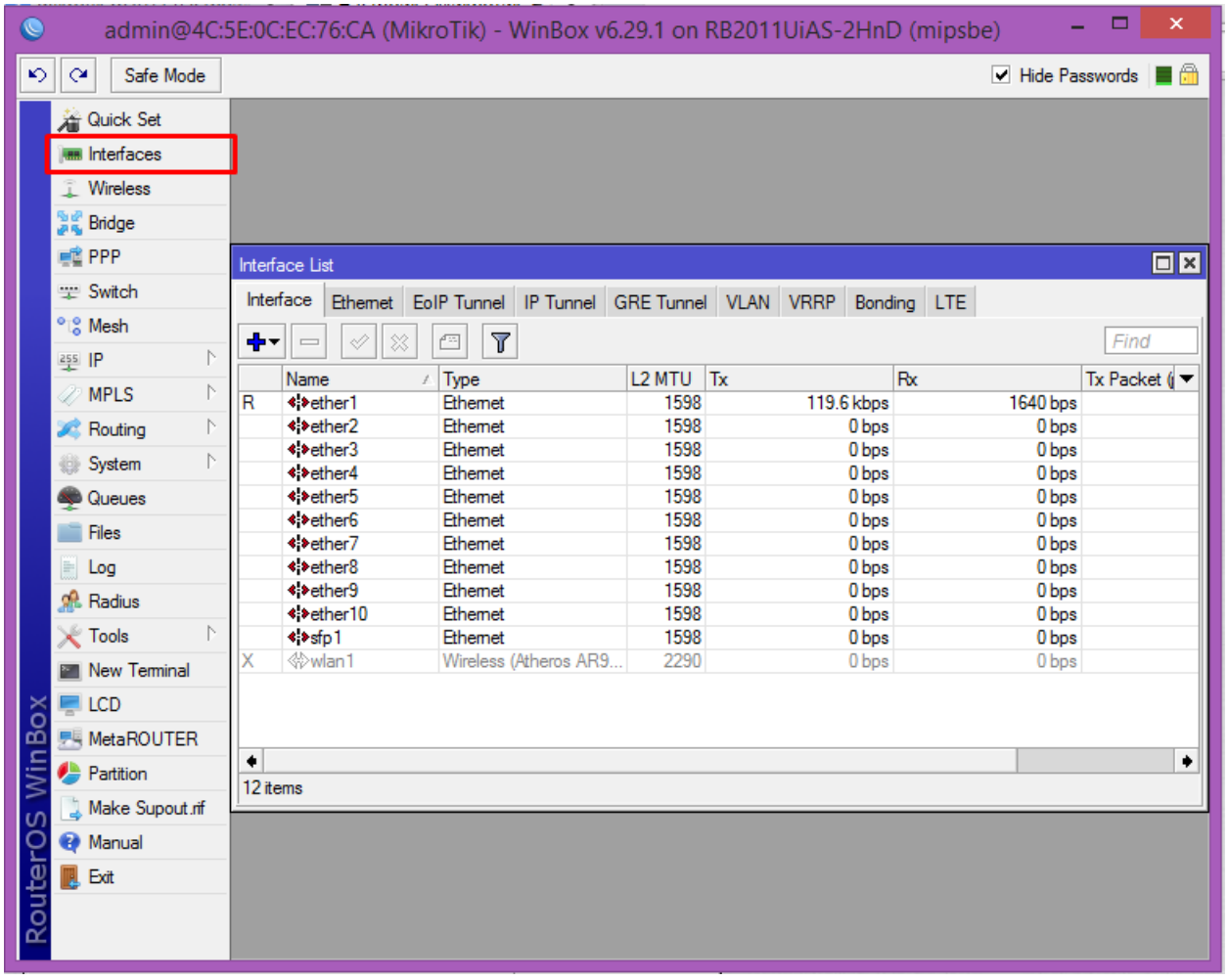


Изображение 5 – Интерфейс программы WinBox.

Настройка моста (Bridge)

Для начала необходимо объединить порты маршрутизатора. Данный маршрутизатор имеет два физически независимых коммутатора с пятью портами каждый. Первые пять портов имеют скорость подключения до 1 Гбит/сек, вторые – до 100 Мбит/сек. Для начала настроим первые пять портов, для которых будет своя локальная сеть 192.168.88.0/24, также сделаем 1 WAN-порт для подключения Интернет-кабеля.

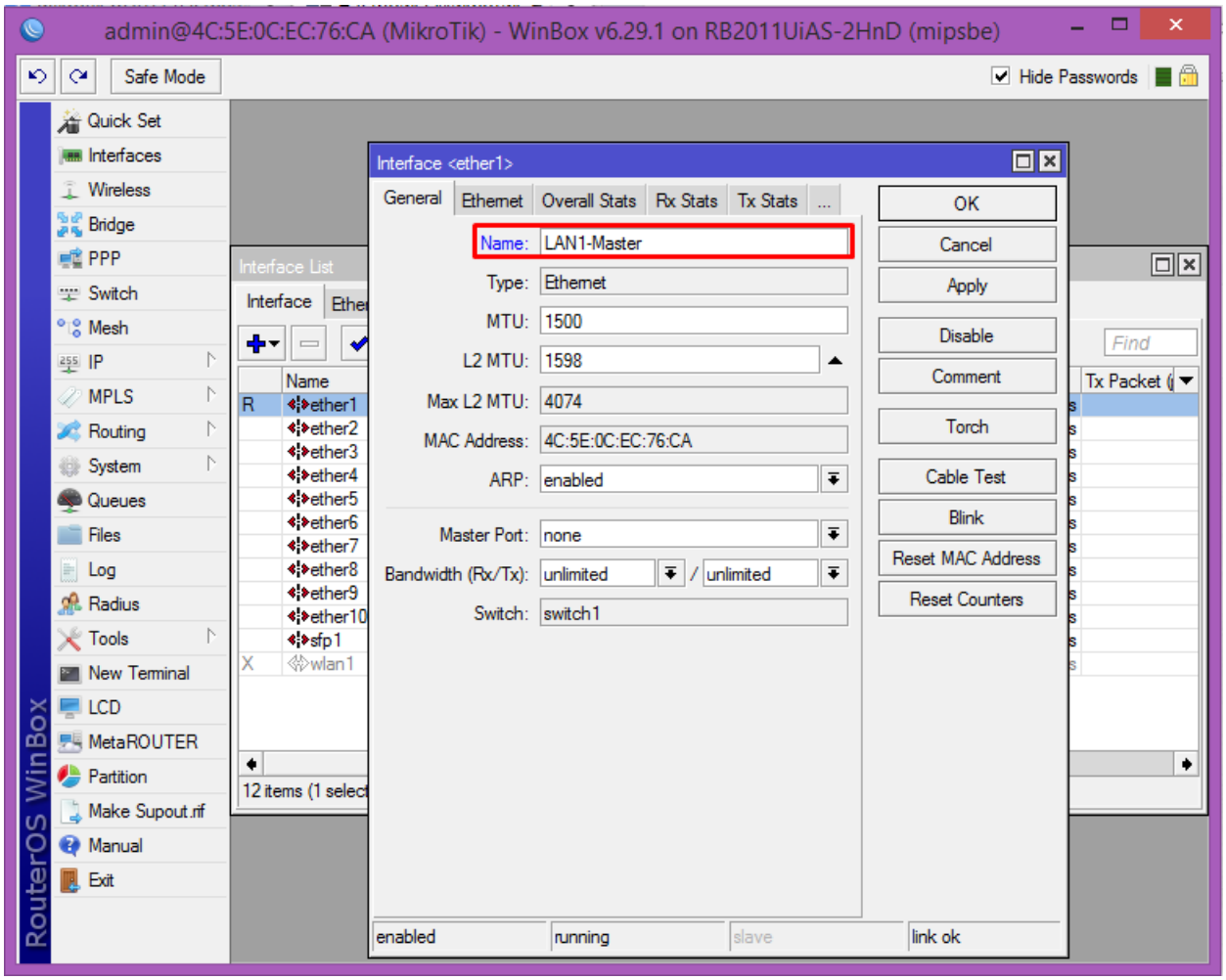
Для этого переходим в раздел «Interfaces», где появятся доступные порты для конфигурирования, изображение 6.



Изображение 6 – Конфигурирование портов.

Логика в настройки портов коммутатора следующая – один порт является мастером (Master-port), остальные порты являются подчиненными (Slave-port). Для нашей ситуации это будет выглядеть следующим образом. 1-й порт будет Master-port, порты 2-4 будут Slave-port, порт 5 будет WAN-порт.

Для настройки конфигурации порта во вкладке «Interface» дважды нажимаем на необходимый порт, изображение 7.



Изображение 7 – Настройка порта.

На изображении 7 представлена настройка 1-го порта, который является Master-port. Во вкладке «General» в поле «Name» указываем название порта. Для явного отображения информации назовем его «LAN1-Master». Остальные параметры оставляем без изменений, главное, чтобы в поле «Master Port» было выбрано «none». Для применения параметров нажимаем на «OK».

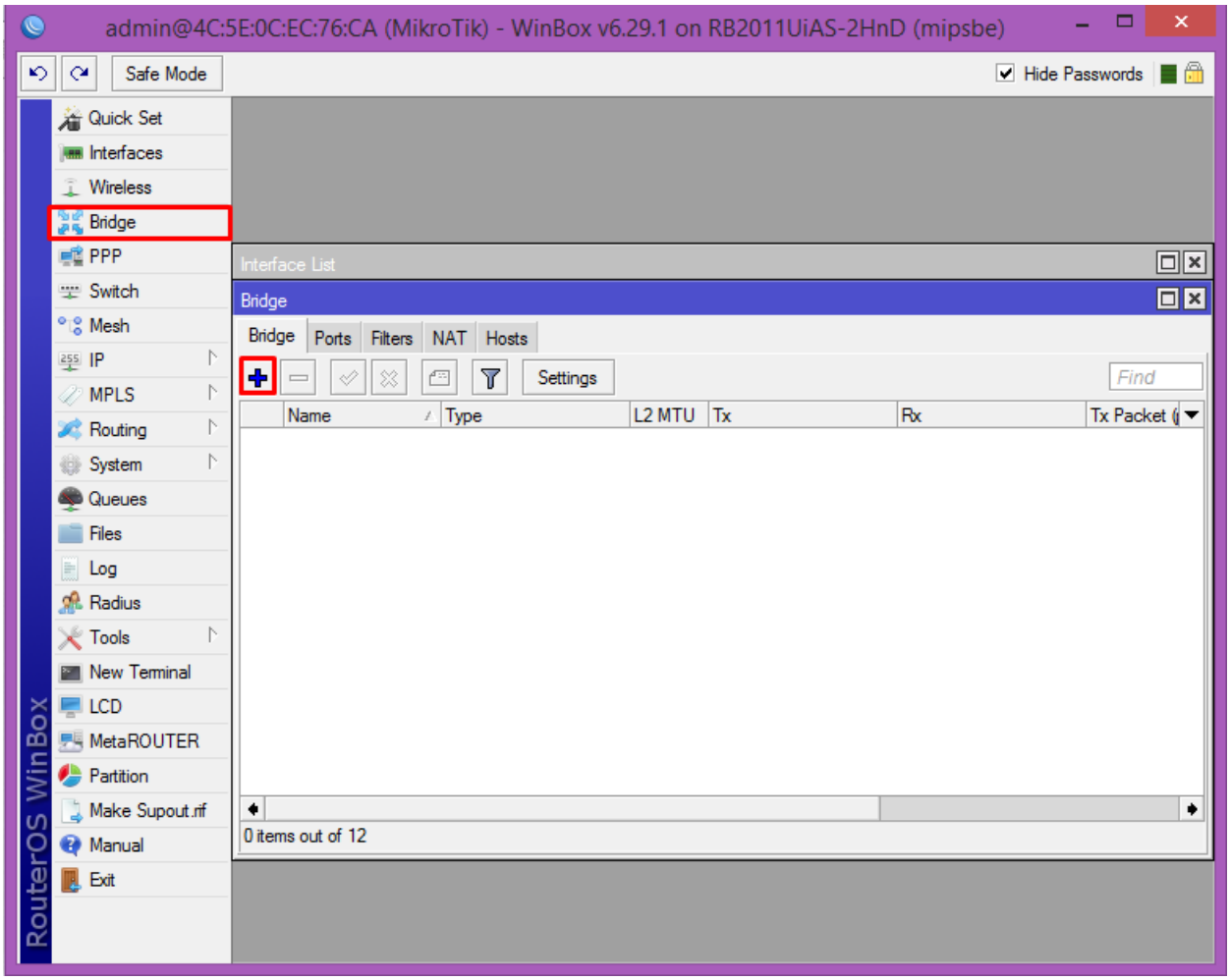
Для портов 2-4 проводим аналогичную настройку – в поле «Name» вводим соответственно «LAN(2-4)-Slave» и для каждого порта в поле «Master Port» выбираем «LAN1-Master». Для применения также нажимаем «OK».

Для порта 5 в поле «Name» вводим имя, к примеру, «WAN1» или «ETH-WAN1», в поле «Master Port» оставляем «none».

То есть получается так, что порты 2-4 стали подчиненными порту 1.

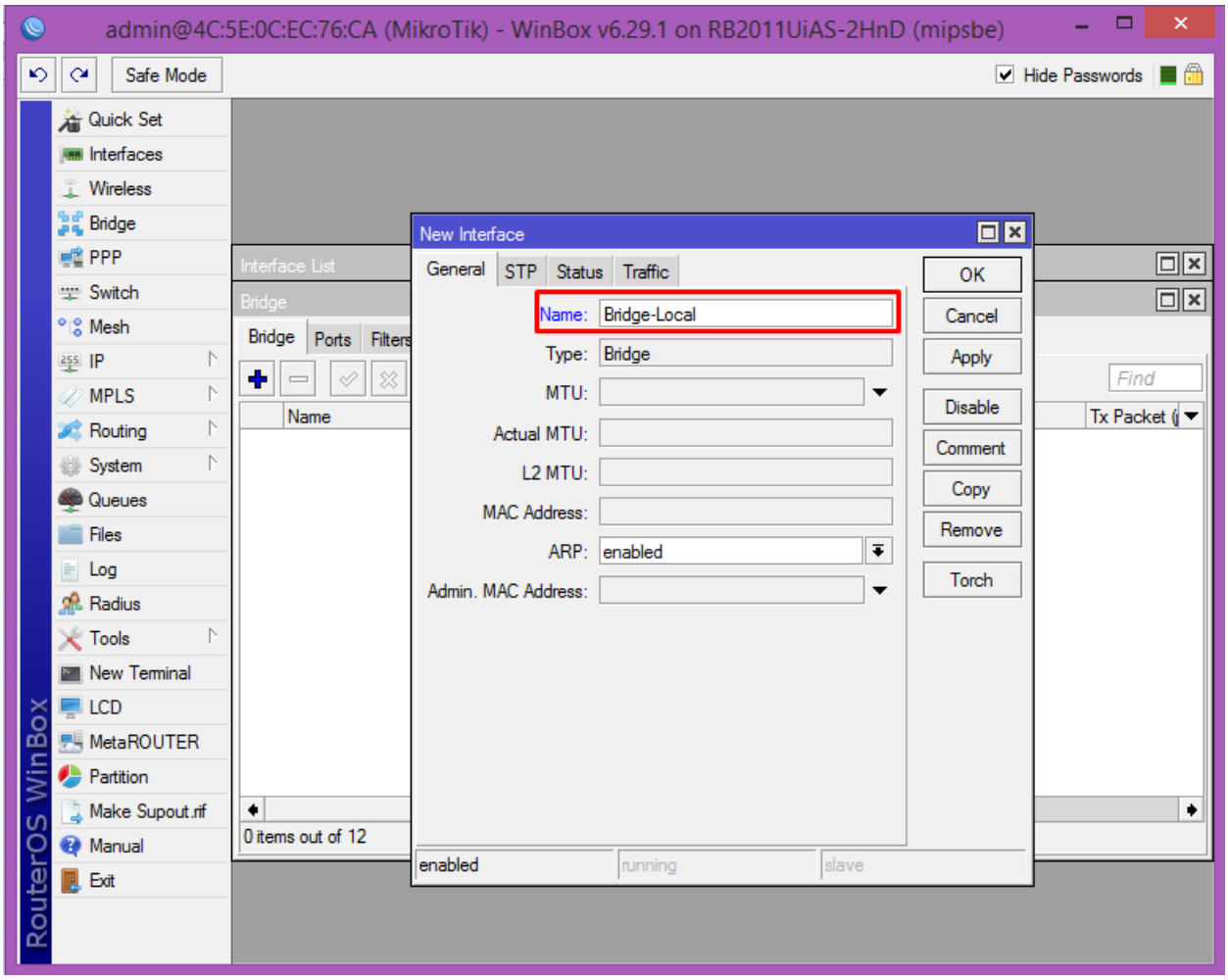
Далее необходимо объединить порты и беспроводную сеть в один мост (Bridge), чтобы можно было раздавать адреса.

Переходим в раздел «Bridge» и во вкладе «Bridge» нажимаем на кнопку «+», изображение 8.



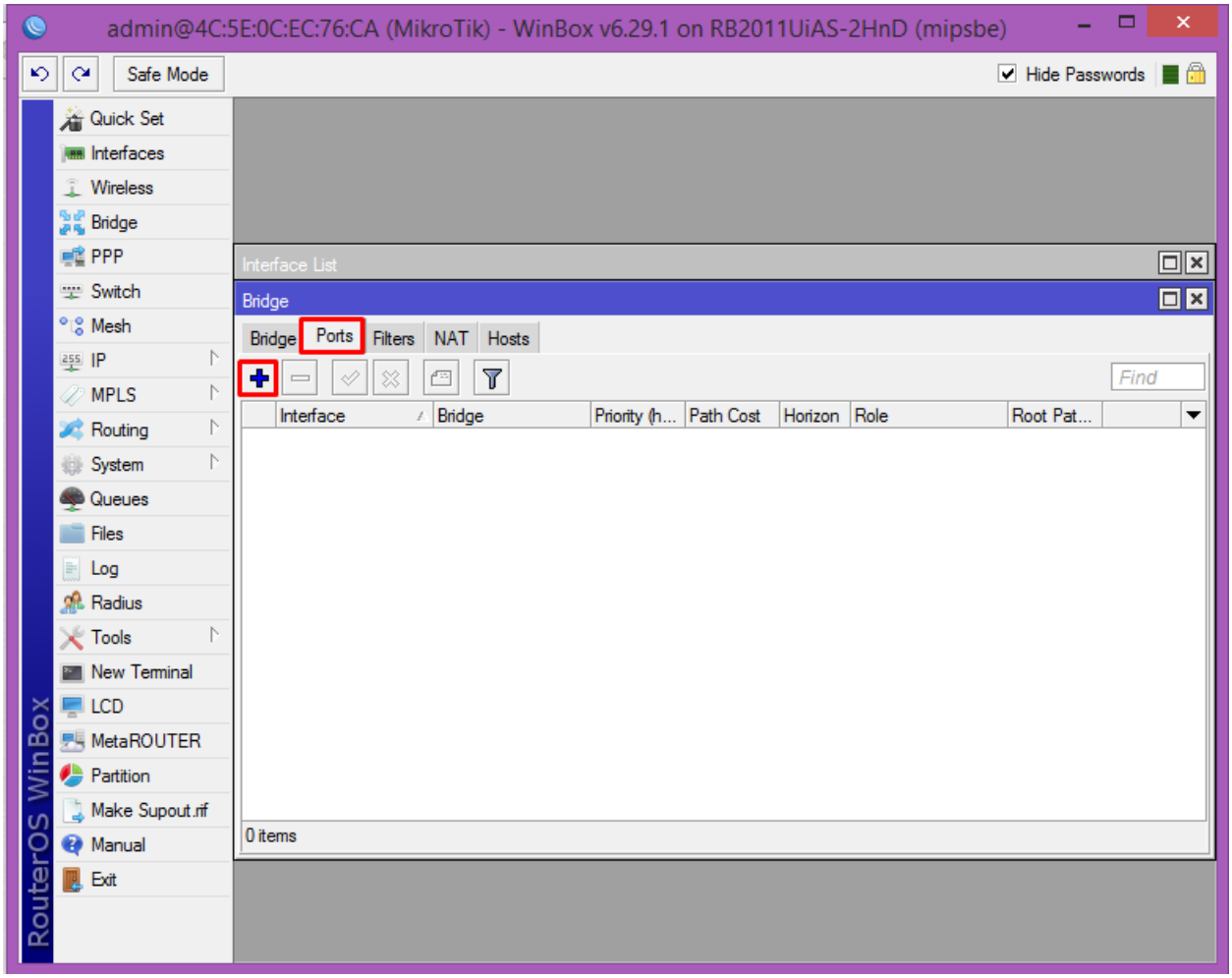
Изображение 8 – Конфигурирование моста (Bridge).

После этого откроется окно с созданием нового моста. Во вкладке «General» в поле «Name» вводим, к примеру, «Bridge-Local» и нажимаем на «OK», изображение 9.



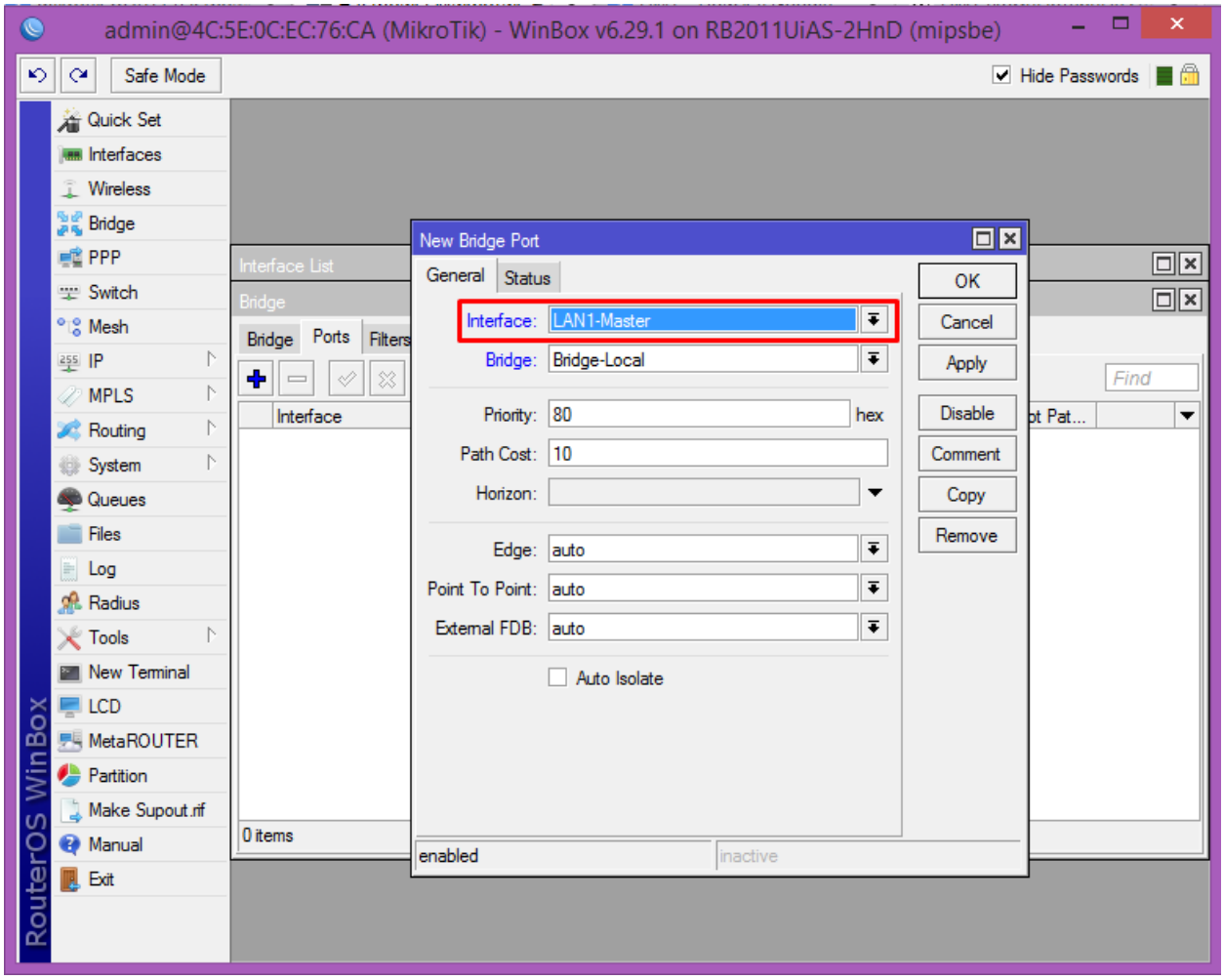
Изображение 9 – Создание нового моста.

Далее переходим во вкладку «Ports» и нажимаем на «+», изображение 10.



Изображение 10 – Добавление портов в мост.

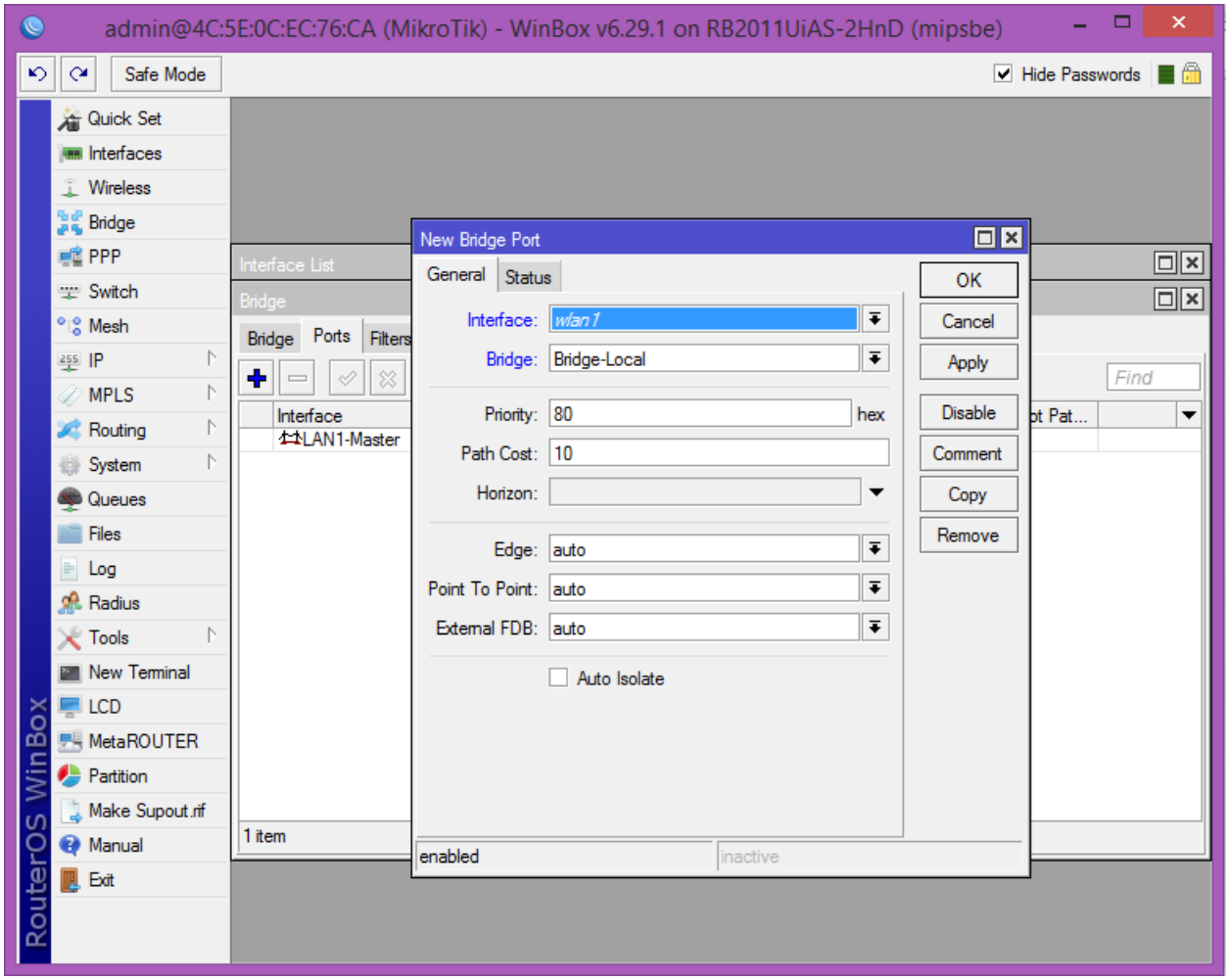
Откроется окно, где во вкладке «General» в поле «Interface» нужно выбрать необходимый порт и в поле «Bridge» необходимо выбрать мост, к которому этот порт будет принадлежать. Для нашей ситуации в поле «Interface» выбираем «LAN1-Master», в поле «Bridge» выбираем «Bridge-Local» и нажимаем на «OK», изображение 11.



Изображение 11 – Добавление Master-port в мост.

Дополнительно нам необходимо добавить беспроводную сеть «wlan1» в этот же мост. Порт 2-4 добавлять не нужно, так как они связаны с портом LAN1-Master, то есть по умолчанию принадлежат этому мосту.

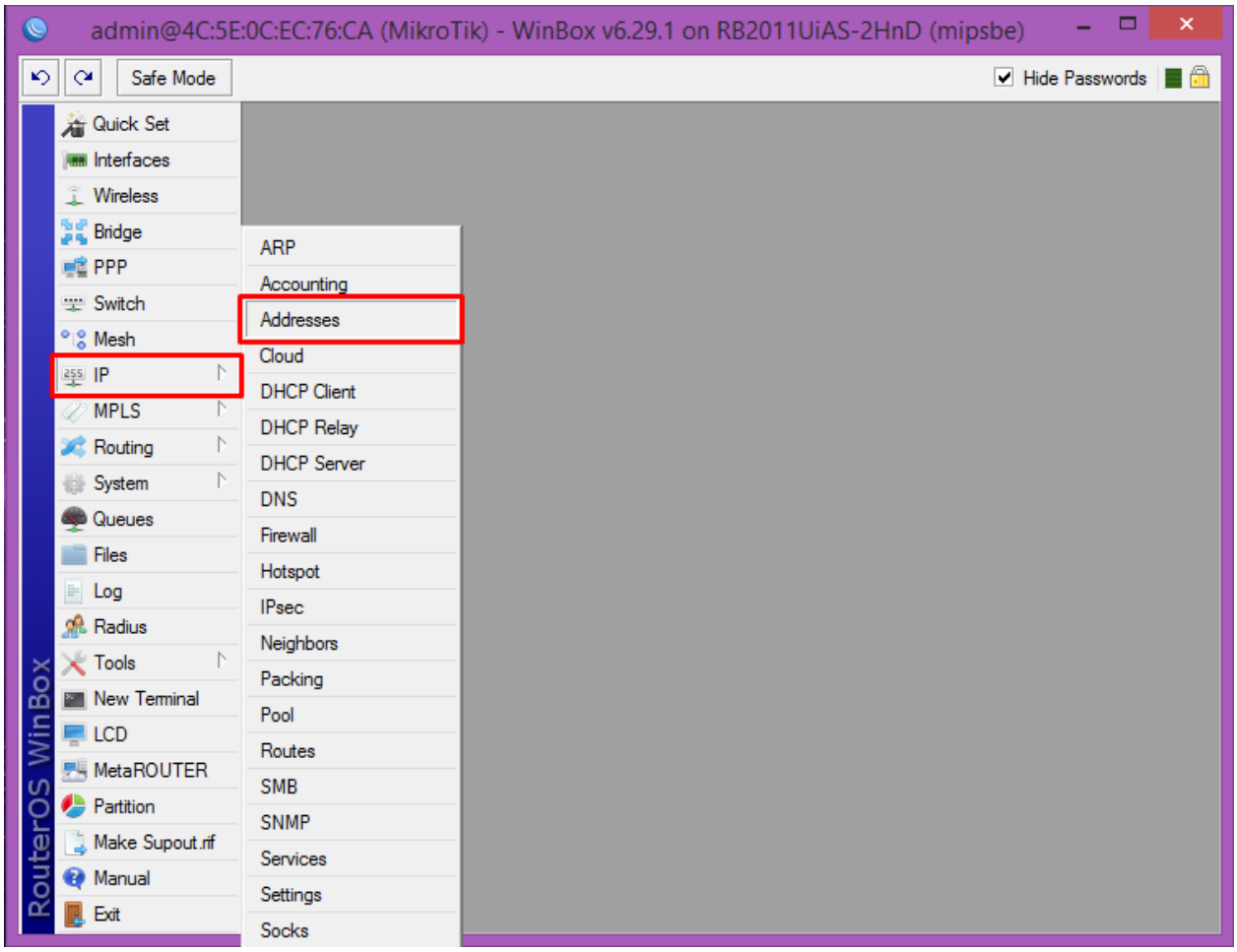
Во вкладке «Ports» снова нажимаем на «+». Теперь в поле «Interface» выбираем «wlan1», а в поле «Bridge» всё также выбираем «Bridge-Local», после нажимаем на «OK», изображение 12.



Изображение 12 – Добавление беспроводной сети (wlan1) в мост.

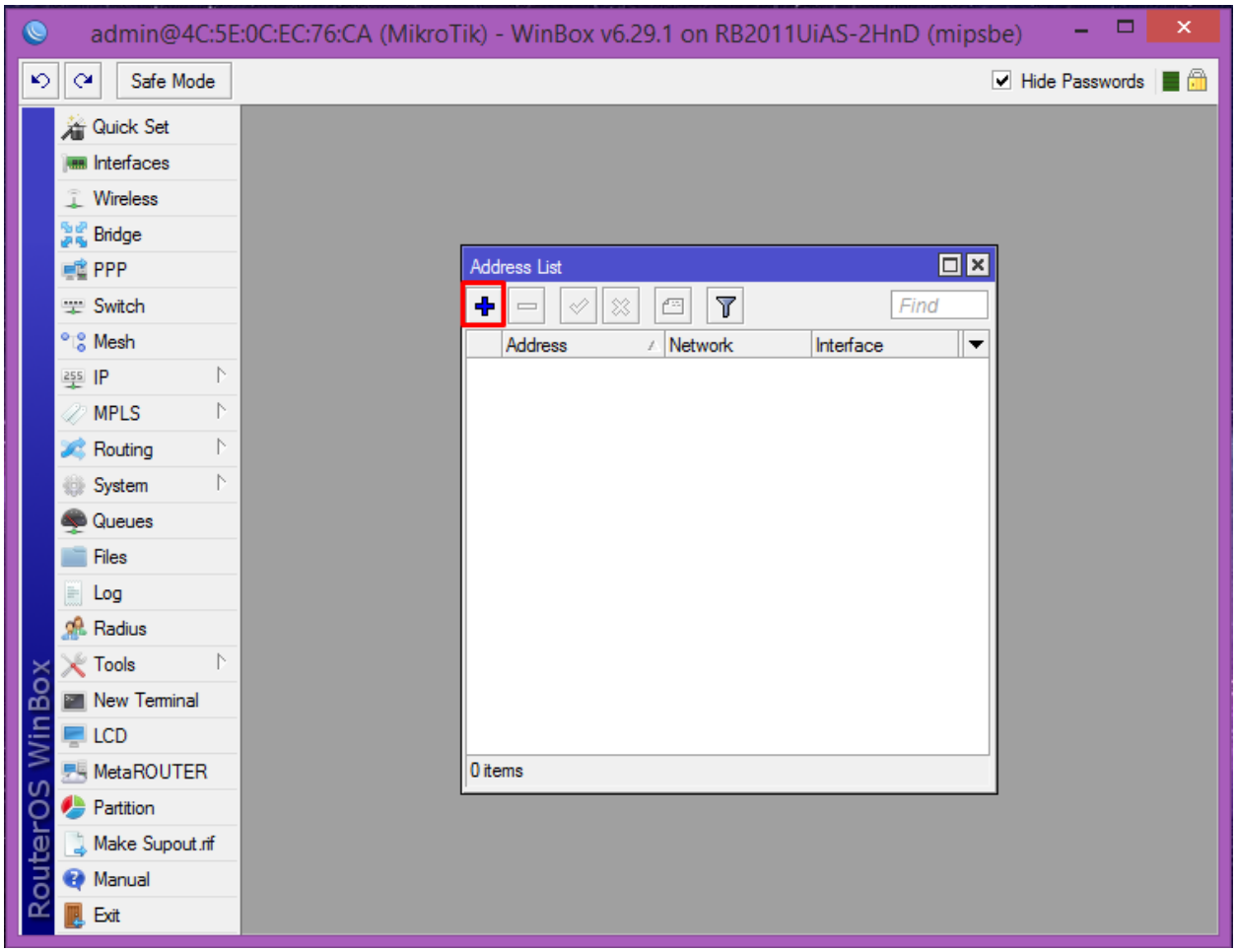
Создание IP-сети, настройка DHCP-клиента, -сервера, NAT.

Конфигурирование моста закончено, теперь необходимо настроить IP-сеть. Для этого переходим в раздел «IP» - «Addresses», изображение 13.



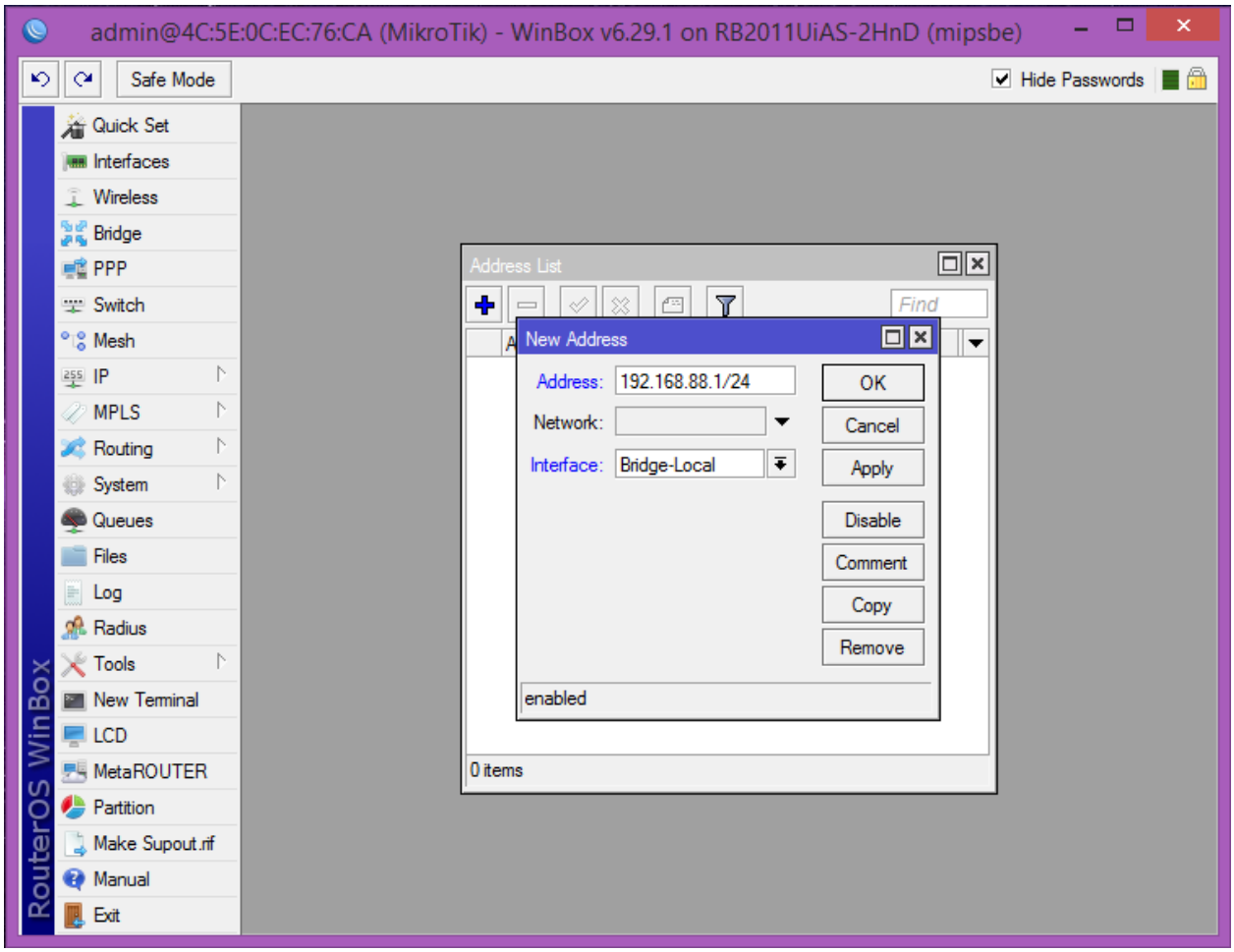
Изображение 13 – Настройки IP-сети.

Откроется окно, где необходимо нажать на «+», изображение 14.



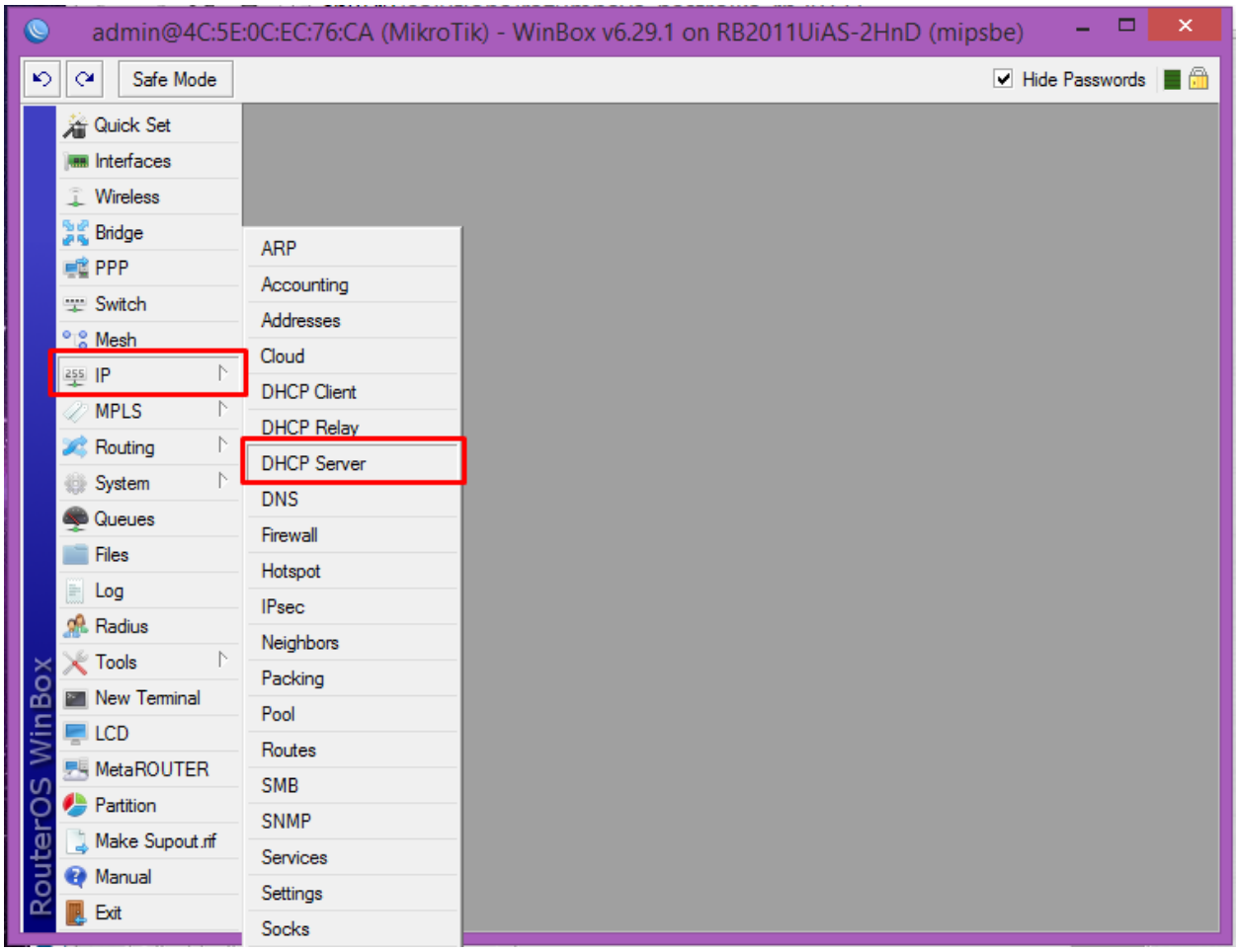
Изображение 14 – Добавление IP-сети.

В открывшемся окне, изображение 15, в поле «Address» пишем 192.168.88.1/24 и в поле «Bridge» выбираем наш выше сконфигурированный мост – «Bridge-Local». После этого нажимаем на «OK». То есть в данном мосту будут использоваться адреса 192.168.88.1 – 192.168.88.254.



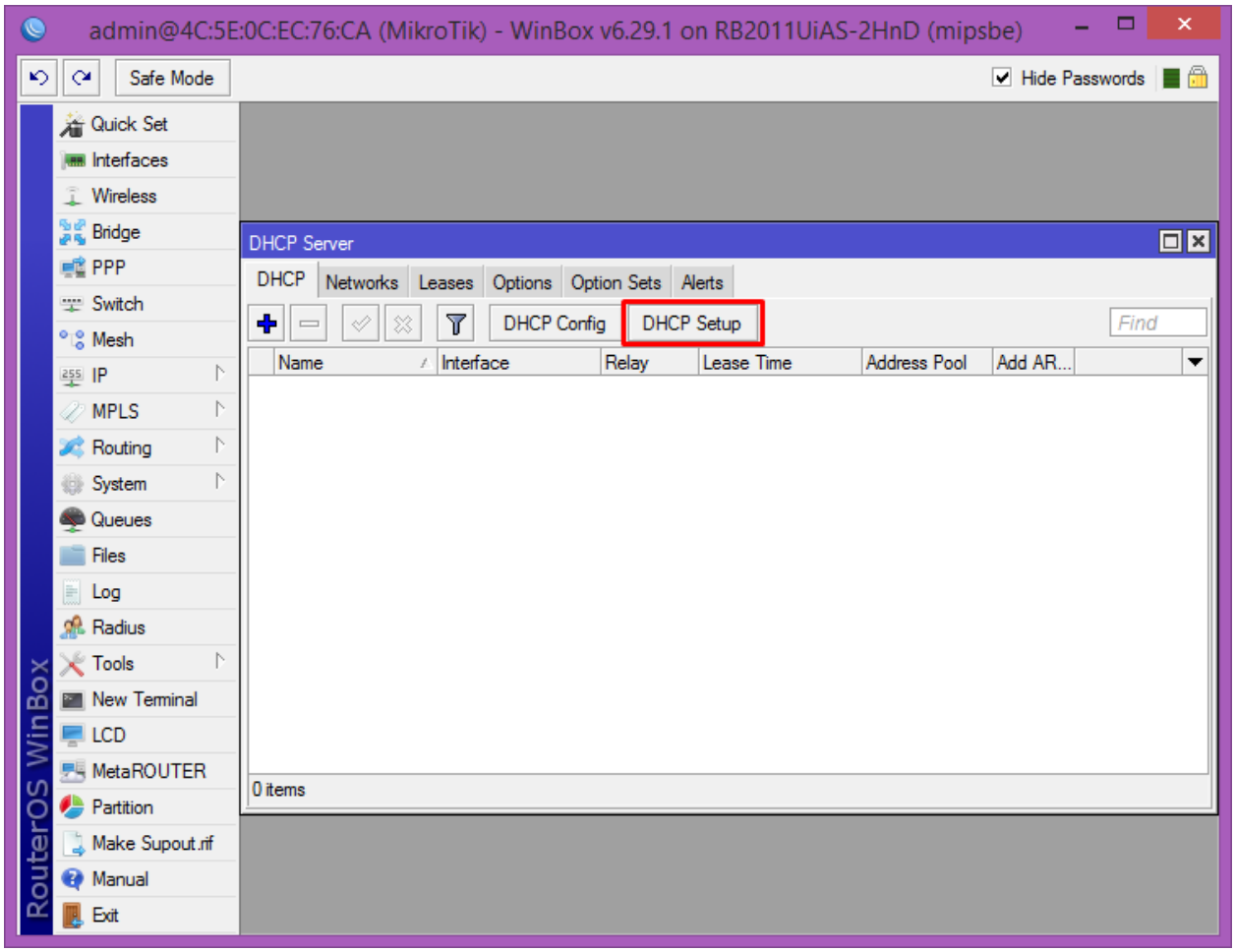
Изображение 15 – Добавление конкретной сети.

Далее проведем настройки DHCP-сервера, чтобы маршрутизатор мог автоматически раздавать адреса в наш мост. Для этого переходим в раздел «IP» – «DHCP Server», изображение 16.



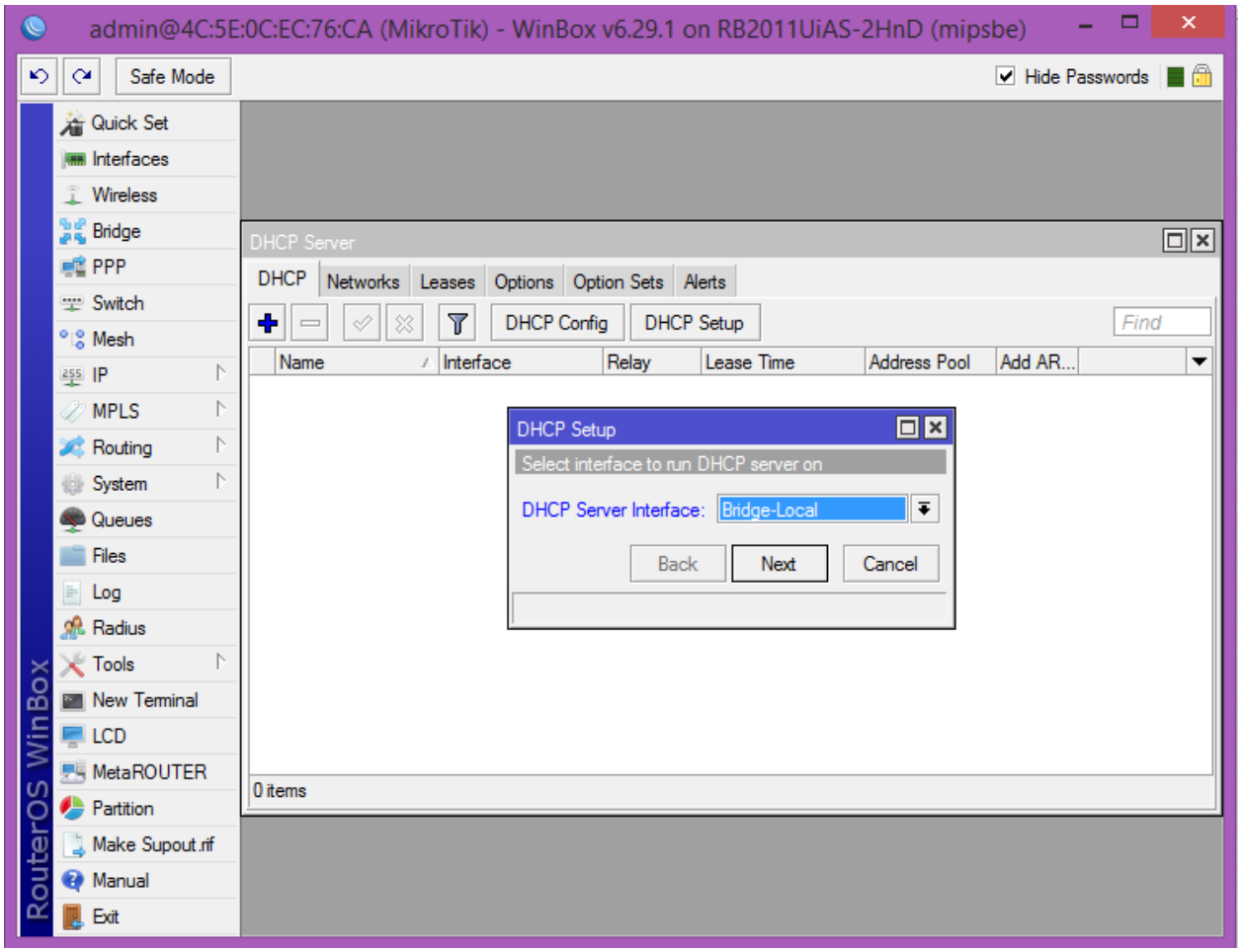
Изображение 16 – Переход в настройки DHCP-сервера.

Откроется окно, где во вкладке «DHCP» необходимо нажать на кнопку «DHCP Setup», изображение 17.



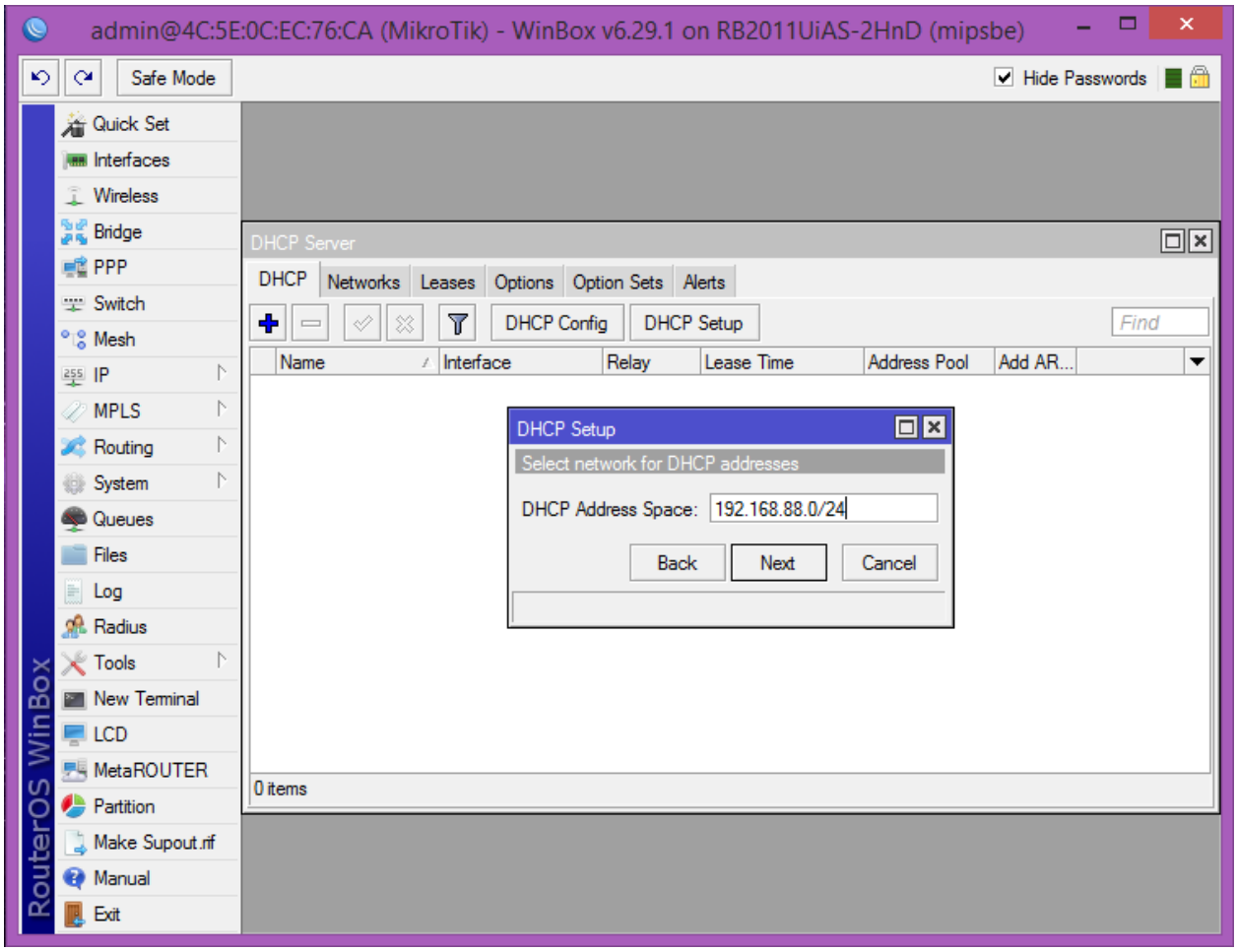
Изображение 17 – Настройки DHCP-серерва.

В открывшемся окне, изображение 18, выбираем интерфейс для DHCP-сервера «DHCP Server Interface». Данным интерфейсом будет являться наш сконфигурированный мост – «Bridge-Local». Нажимаем на кнопку «Next».



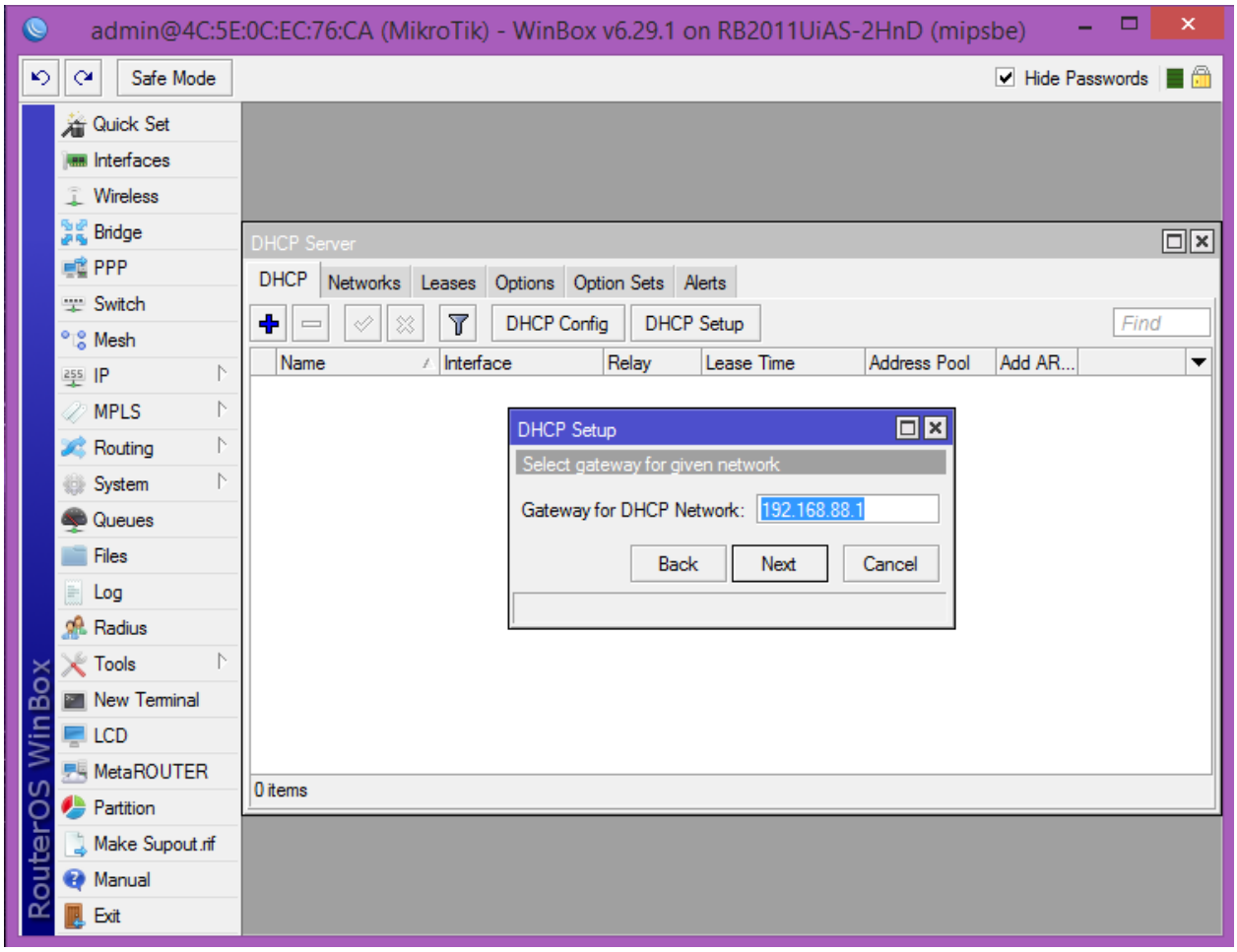
Изображение 18 – Интерфейс для DHCP-сервера.

Далее вводим адресное пространство «DHCP Address Space» для DHCP-сервера – 192.168.88.0/24, изображение 19.



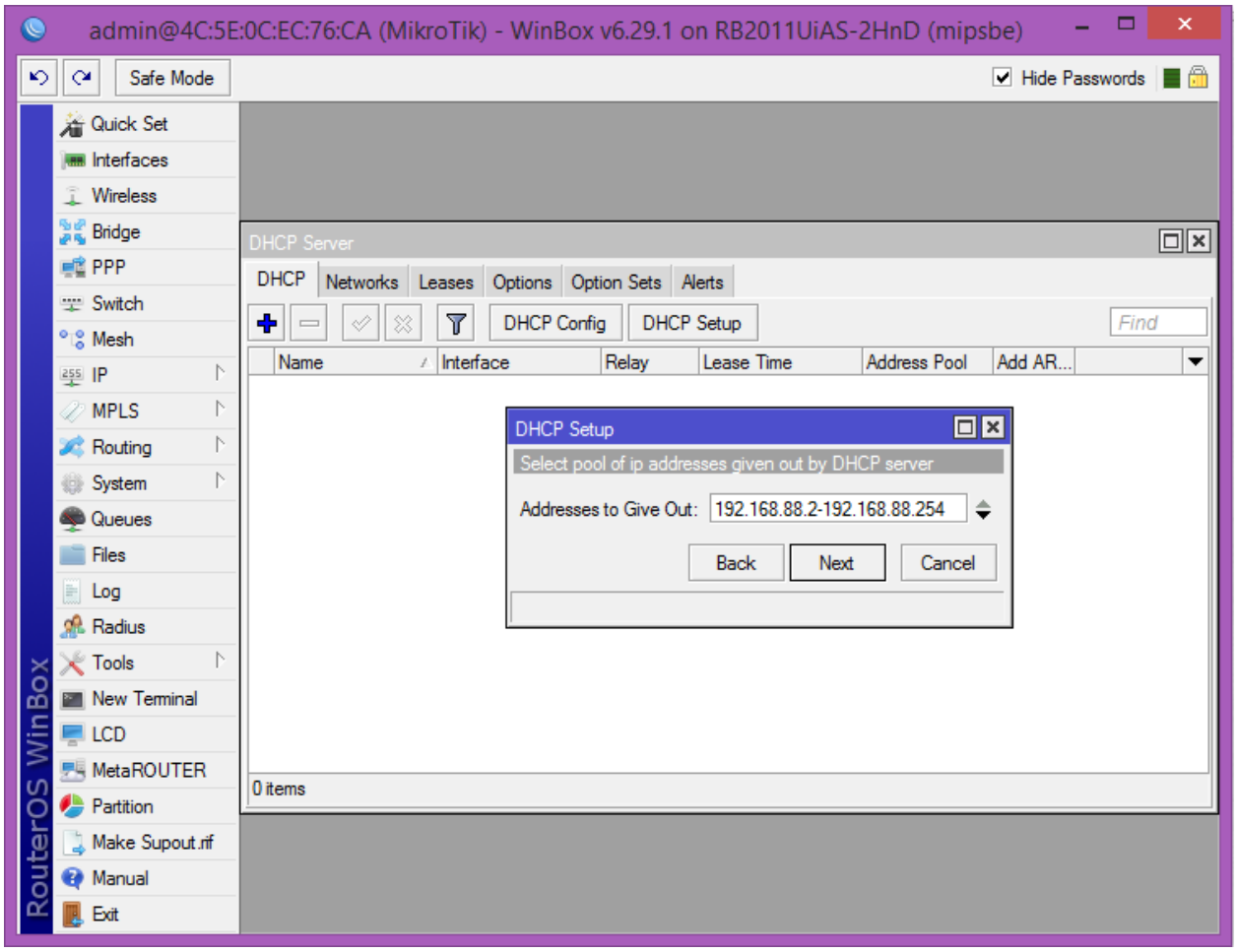
Изображение 19 – Адресное пространство для DHCP-сервера.

Далее вводим шлюз для нашей сети «Gateway for DHCP Network» – 192.168.88.1, изображение 20.



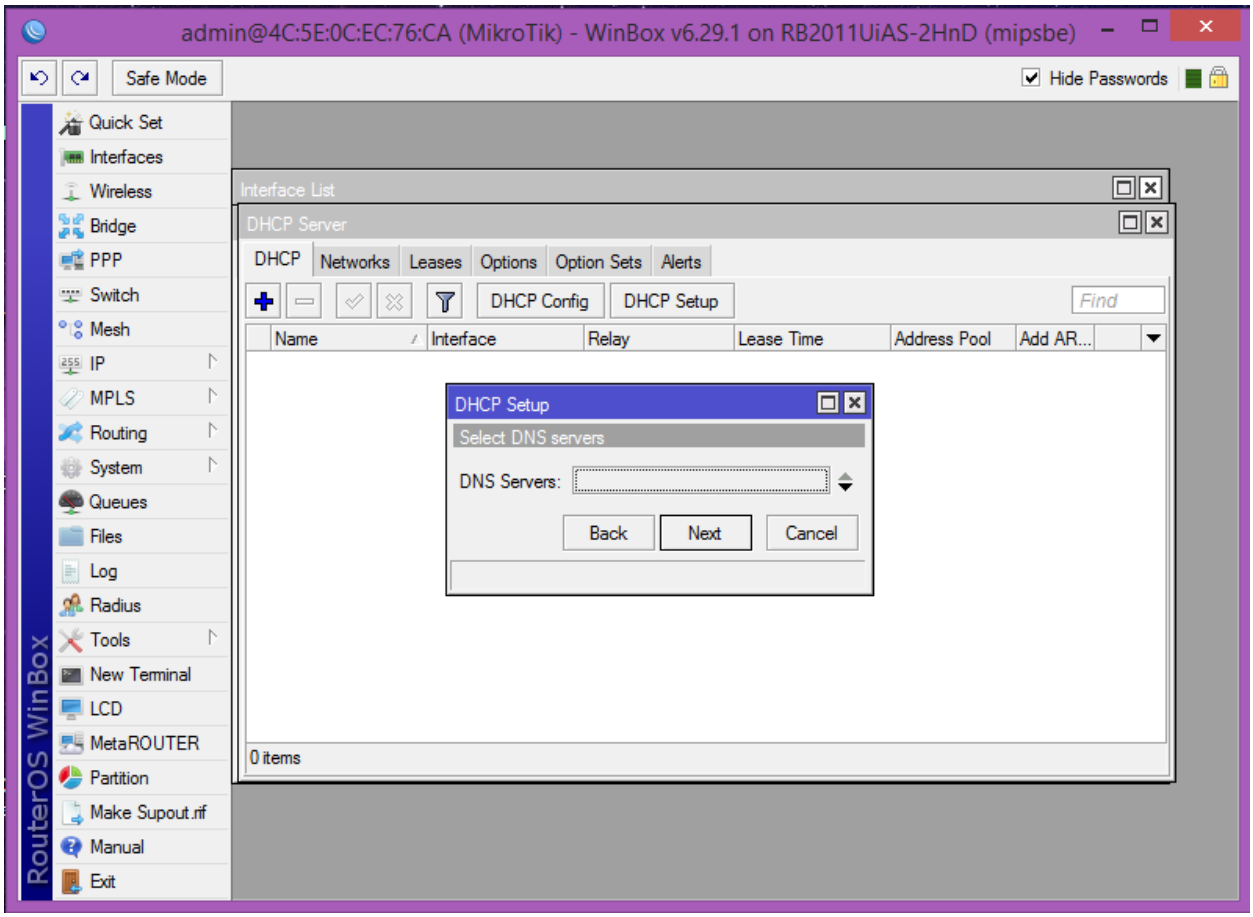
Изображение 20 – Шлюз для сети DHCP.

Далее выбираем диапазон адресов, которые будет раздавать DHCP-сервер «Addresses to Give Out» – 192.168.88.2-192.168.88.254, изображение 21.



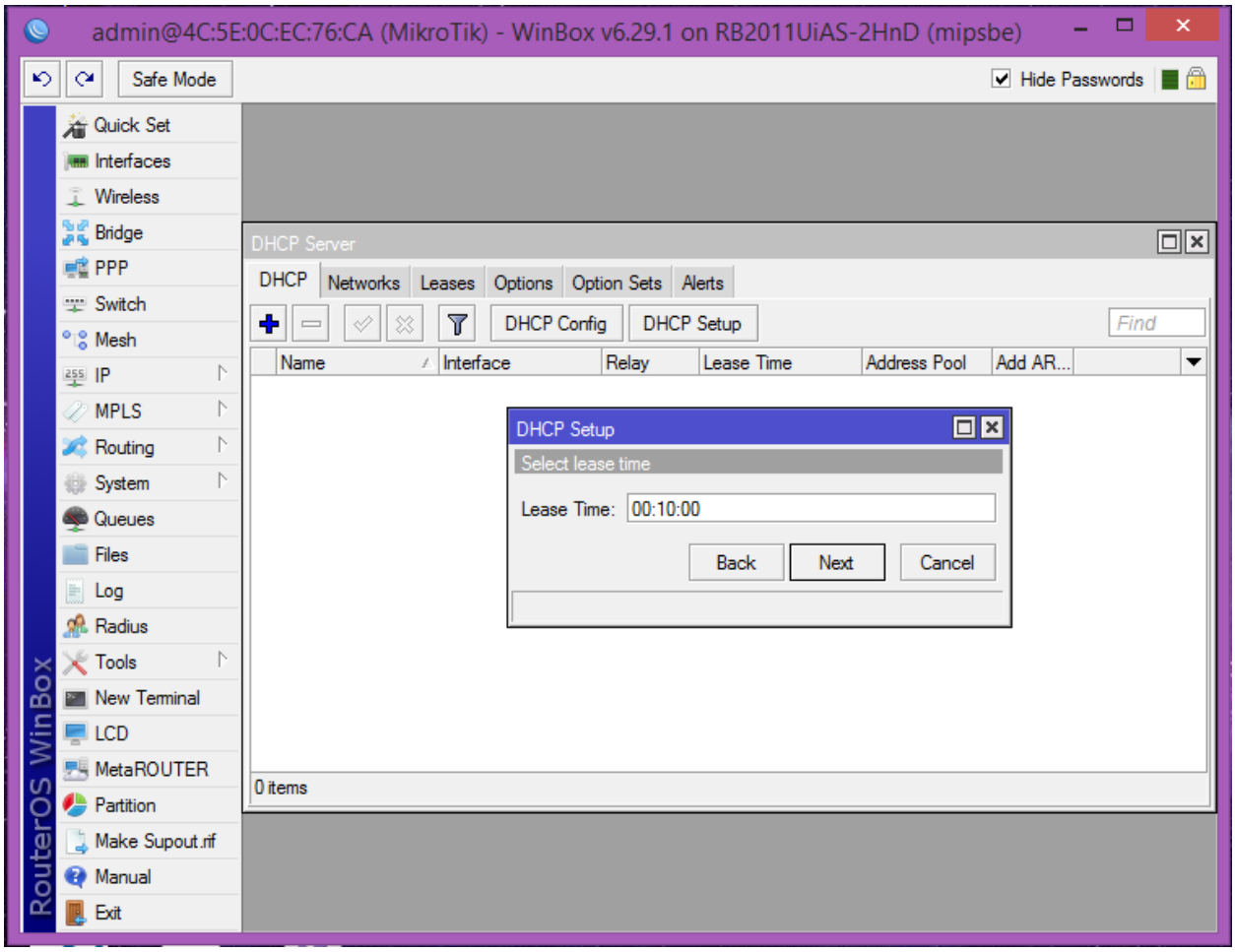
Изображение 21 – Диапазон раздаваемых адресов.

В следующем окне с настройкой DNS-серверов «DNS Servers», изображение 22, поле оставляем пустым, так как в дальнейшем мы настроем DNS Relay, чтобы получать адреса DNS-серверов в автоматическом режиме.



Изображение 22 – Настройки DNS-серверов.

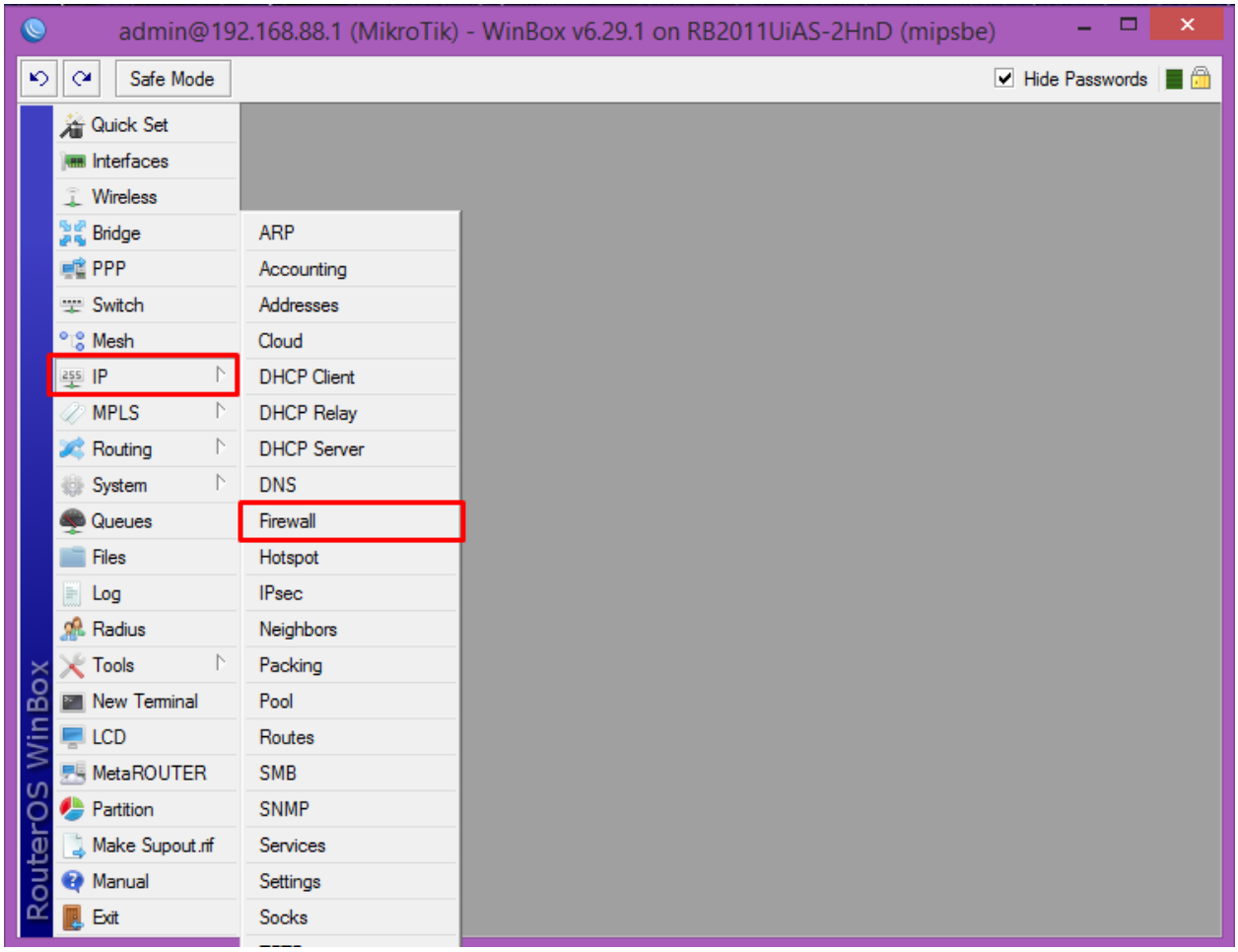
Далее необходимо настроить время аренды адреса «Lease Time», изображение 23. Можно выбрать, к примеру, 1 час – «01:00:00».



Изображение 23 – Настройки времени аренды адреса.

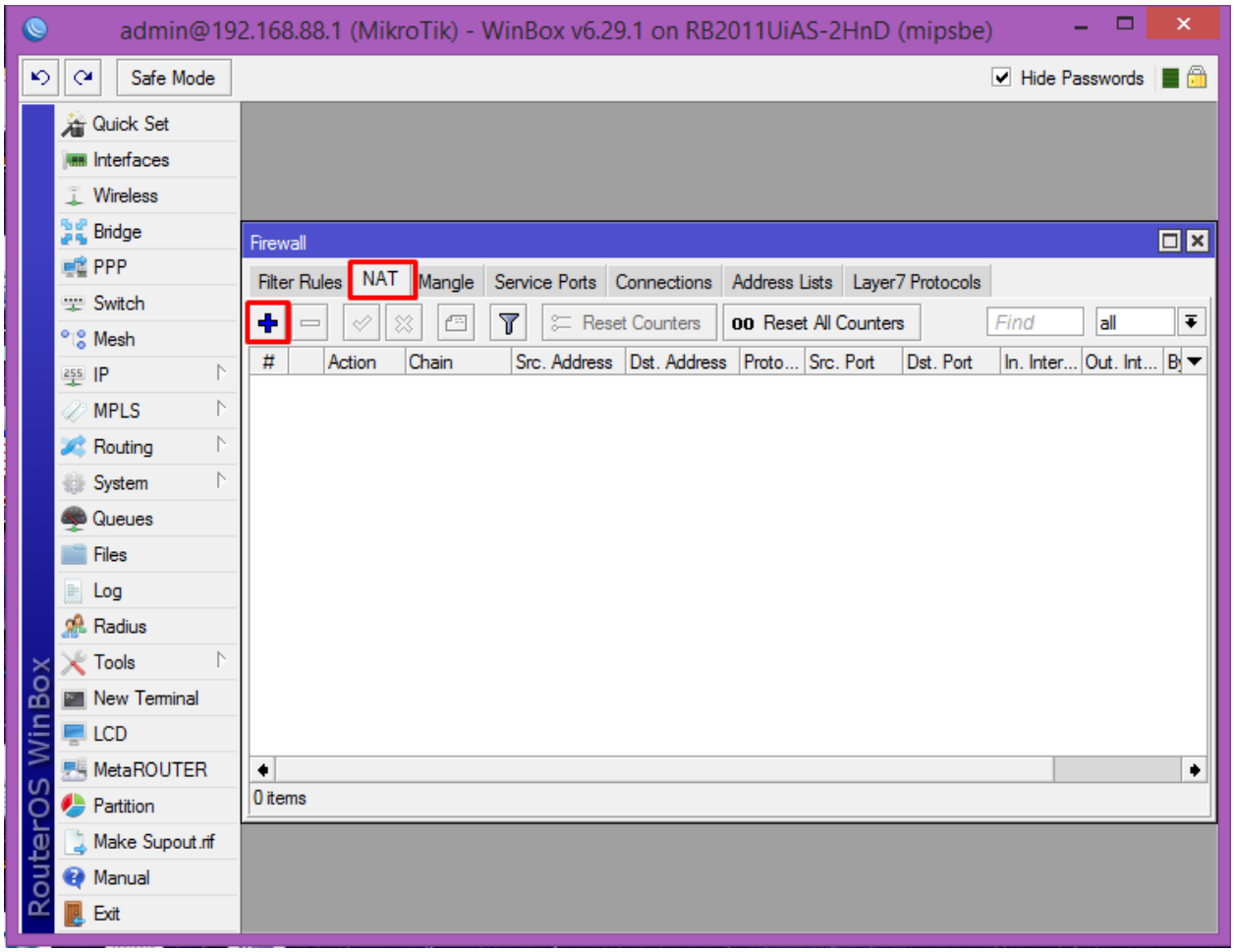
После этого мы сможем подключаться на маршрутизатор уже не по MAC-адресу, а по IP-адресу 192.168.88.1.

Теперь нам необходимо настроить NAT (Network Address Translation) для транслирования одного адреса, который мы будем получать от сети POWERNET, на адреса в нашей локальной сети 192.168.88.0/24. То есть будет использоваться перегруженный NAT.
Для этого переходим в раздел «IP» – «Firewall», изображение 24.



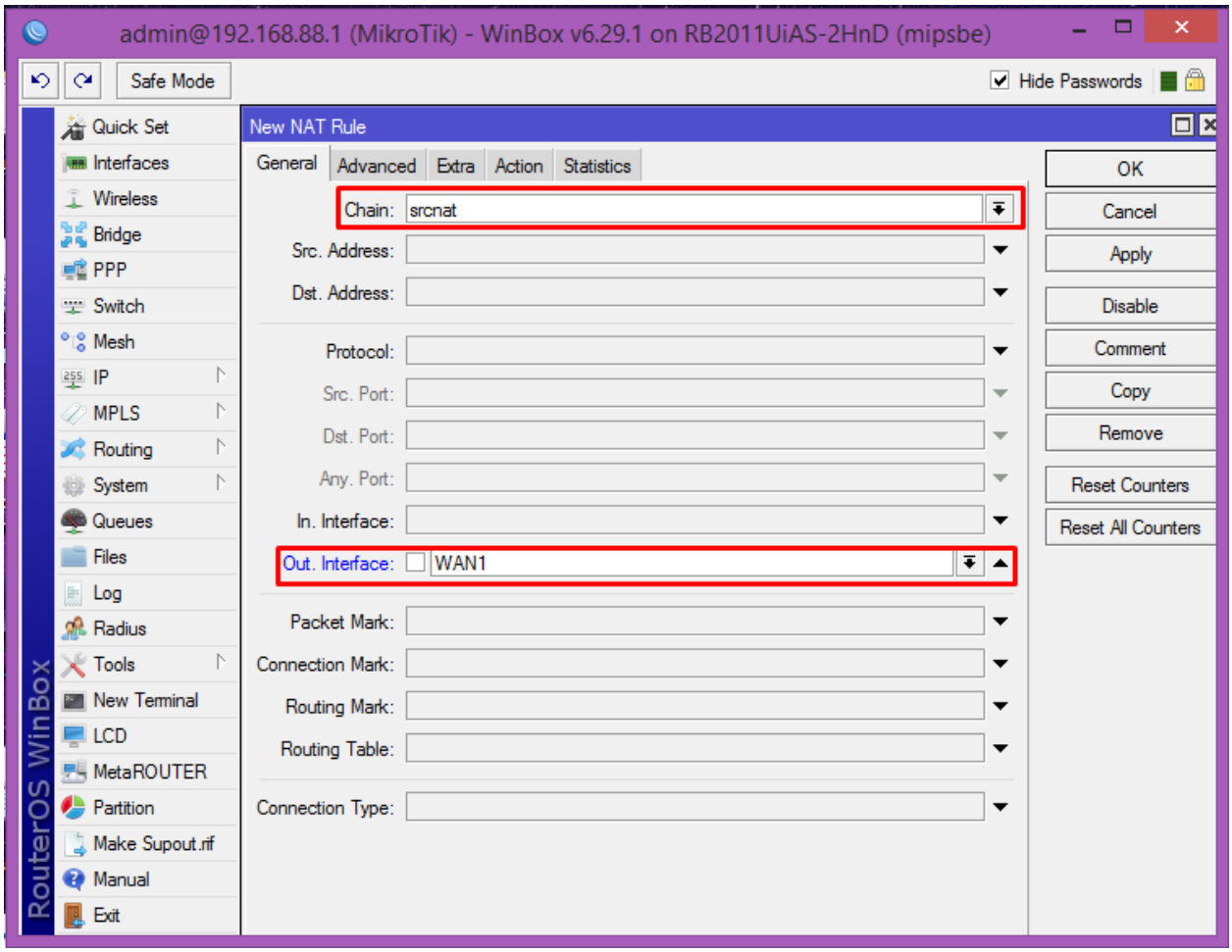
Изображение 24 – Переходит в раздел «Firewall» для настройки NAT.

В открывшемся окне, изображение 25, переходим во вкладку «NAT» и нажимаем на «+».



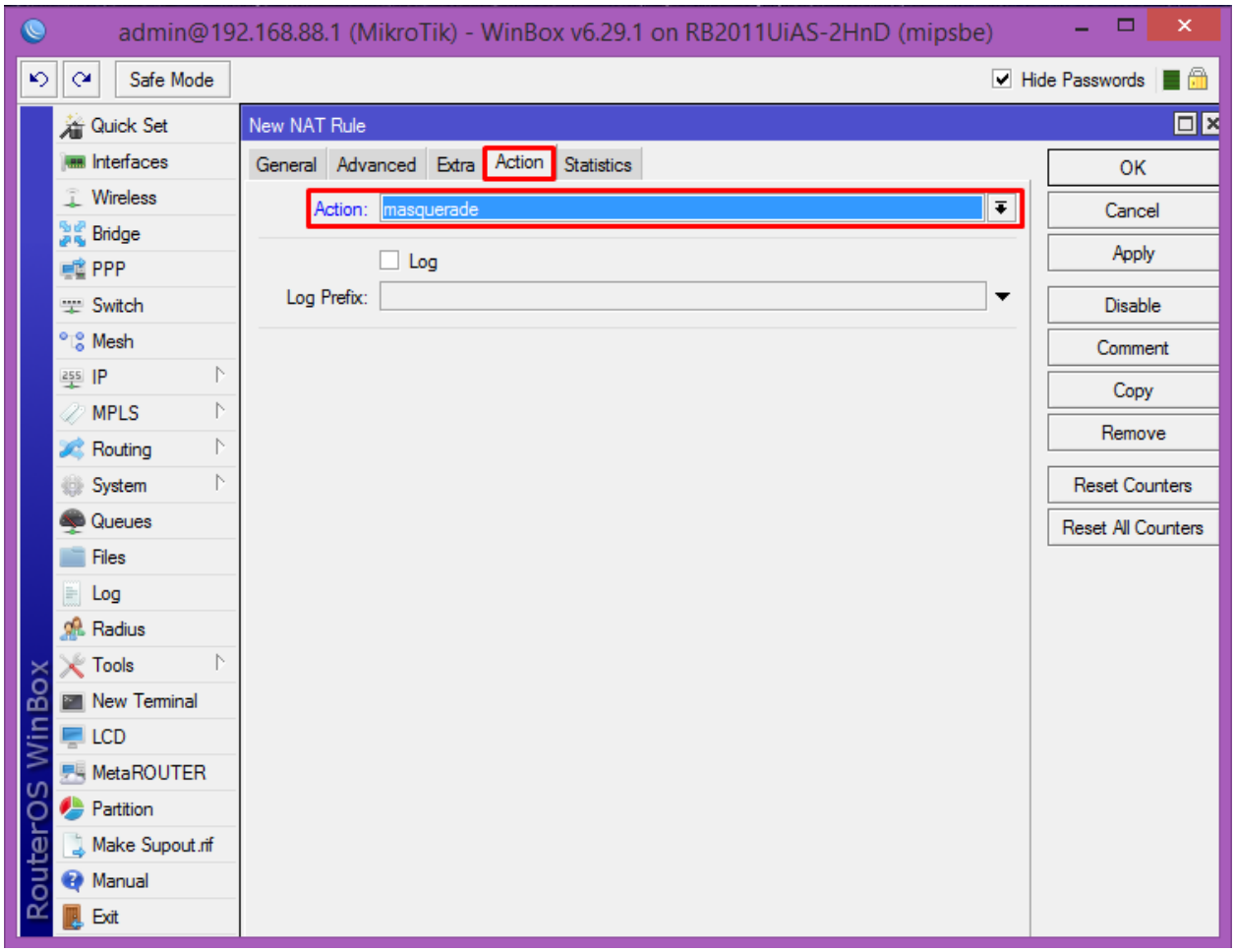
Изображение 25 – Добавление нового правила.

Откроется окно, изображение 26, где во вкладке «General» в поле «Chain» выбираем «srcnat», в поле «Out. Interface» выбираем наш WAN-порт.



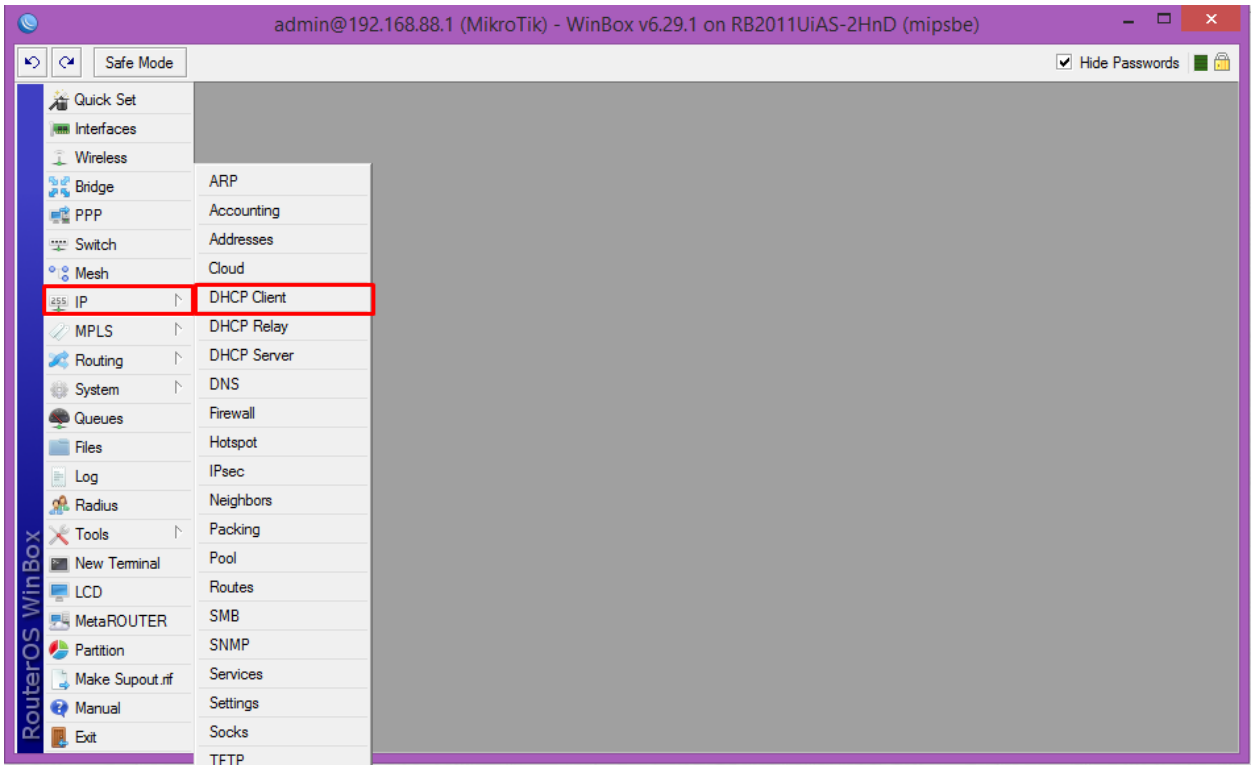
Изображение 26 – Настройка правила для NAT.

Далее переходим во вкладку «Action», изображение 27, и в поле «Action» выбираем «masquerade» – это и есть перегруженный NAT.



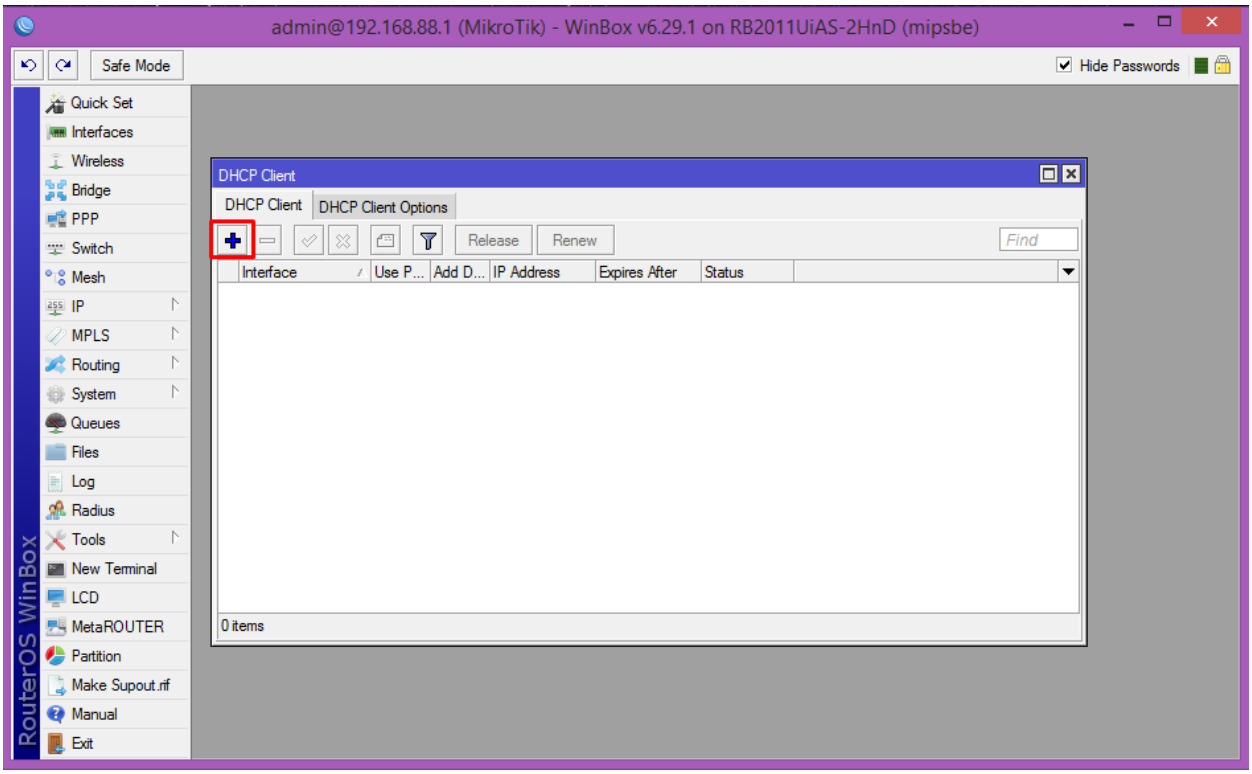
Изображение 27 – Настройка правила для NAT.

Необходимо настроить DHCP-клиент, чтобы наш маршрутизатор автоматически получал IP-адрес и необходимые настройки. Переходим в раздел «IP» – «DHCP Client», изображение 28.



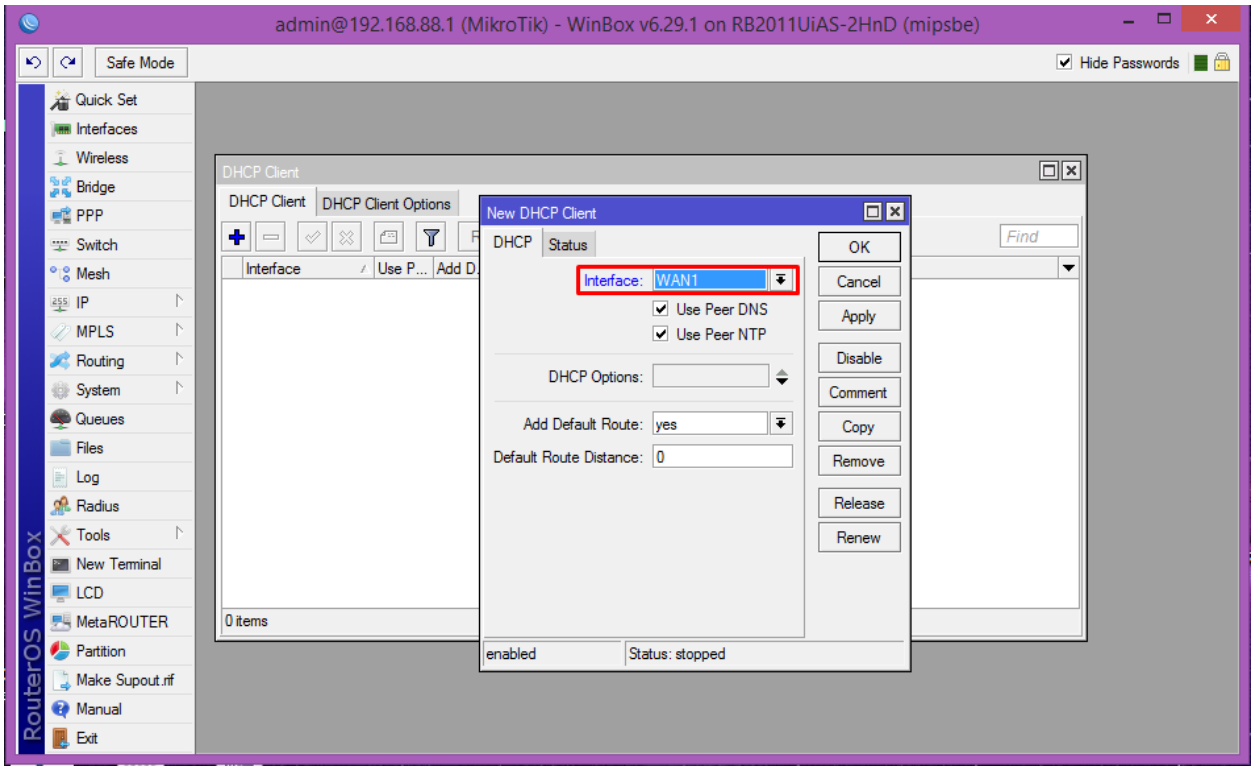
Изображение 28 – Переход в раздел DHCP Client.

В окне, изображение 29, во вкладке «DHCP Client» нажимаем «+».



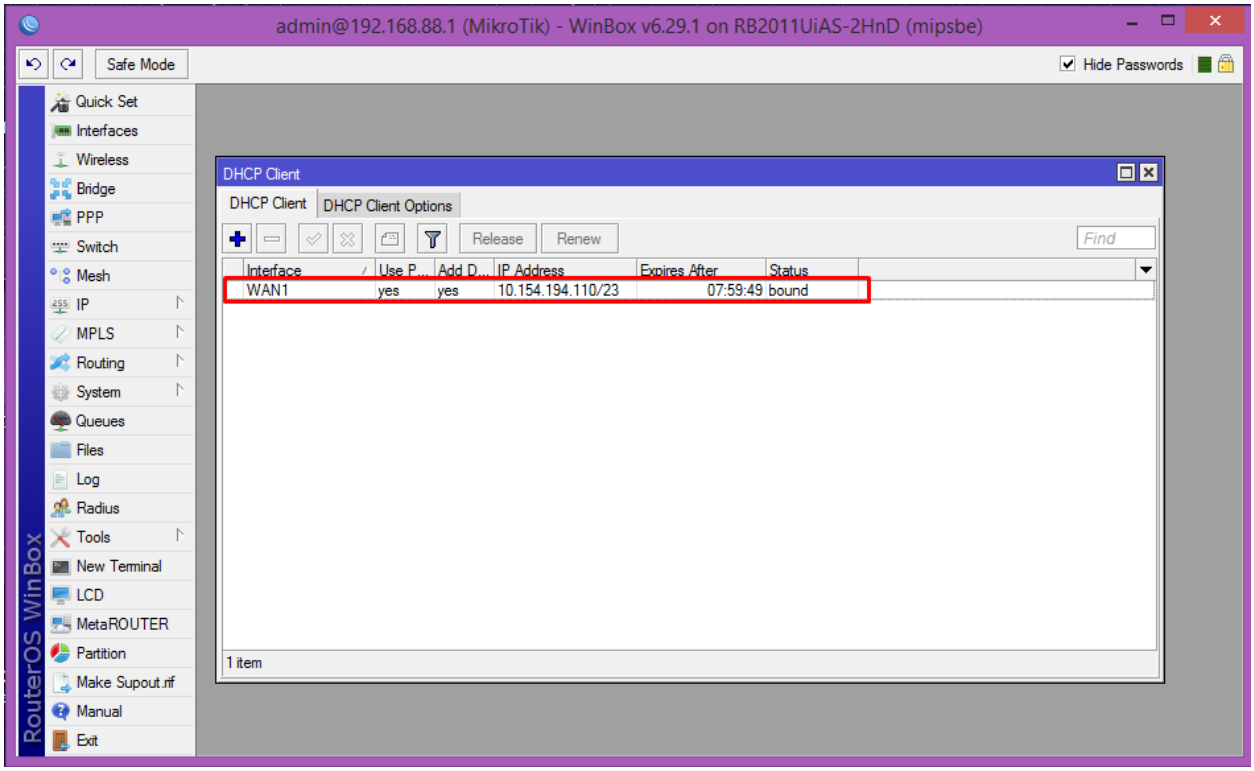
Изображение 29 – Добавления DHCP-клиента.

Откроется окно, изображение 30, где во вкладке «DHCP» необходимо выбрать интерфейс для DHCP-клиента, то есть в поле «Interface» выбираем наш WAN-порт. Остальные параметры оставляем, как на изображении.



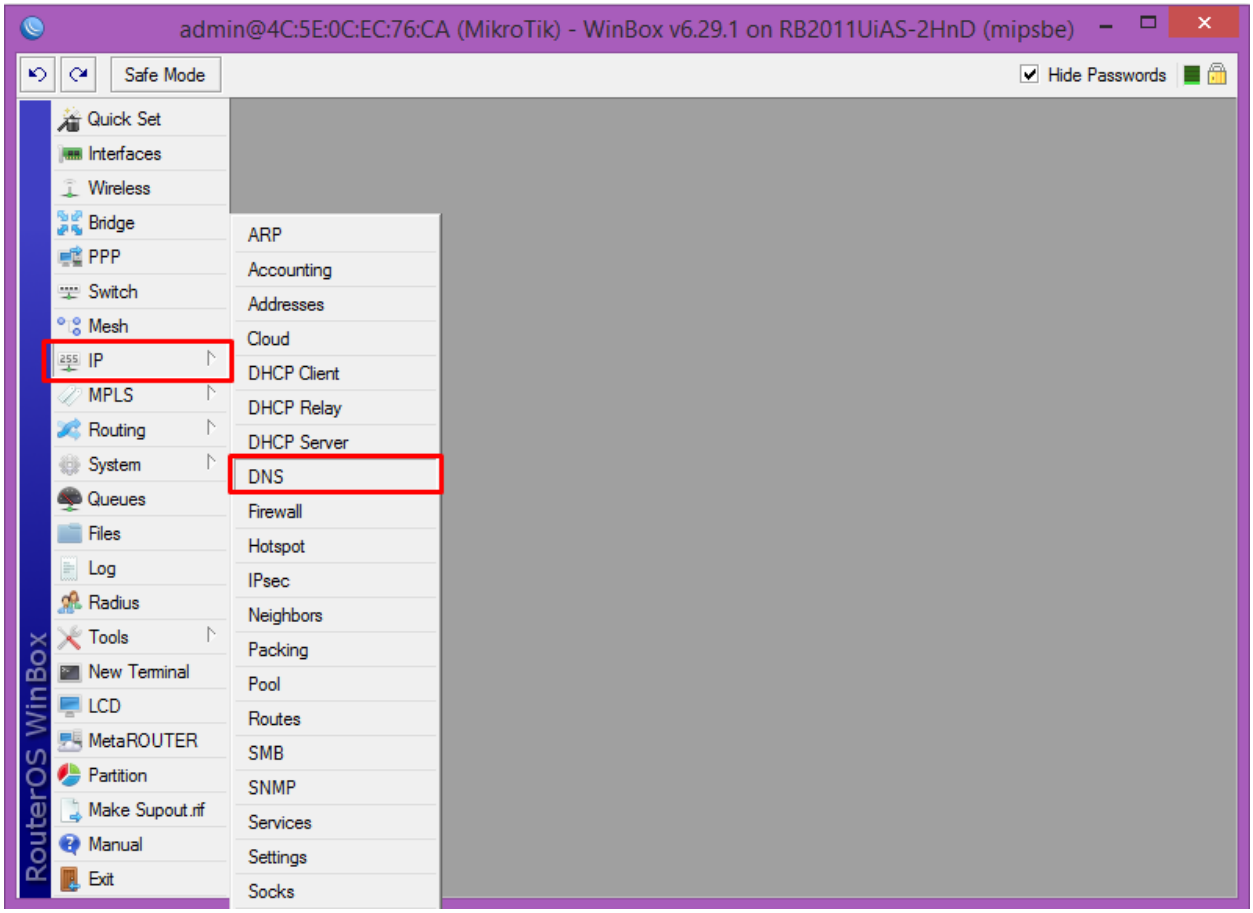
Изображение 30 – Выбор интерфейса для DHCP-клиента.

Подключаем кабель в WAN-порт (5-й порт) и проверяем, что наш интерфейс получил IP-адрес, изображение 31.



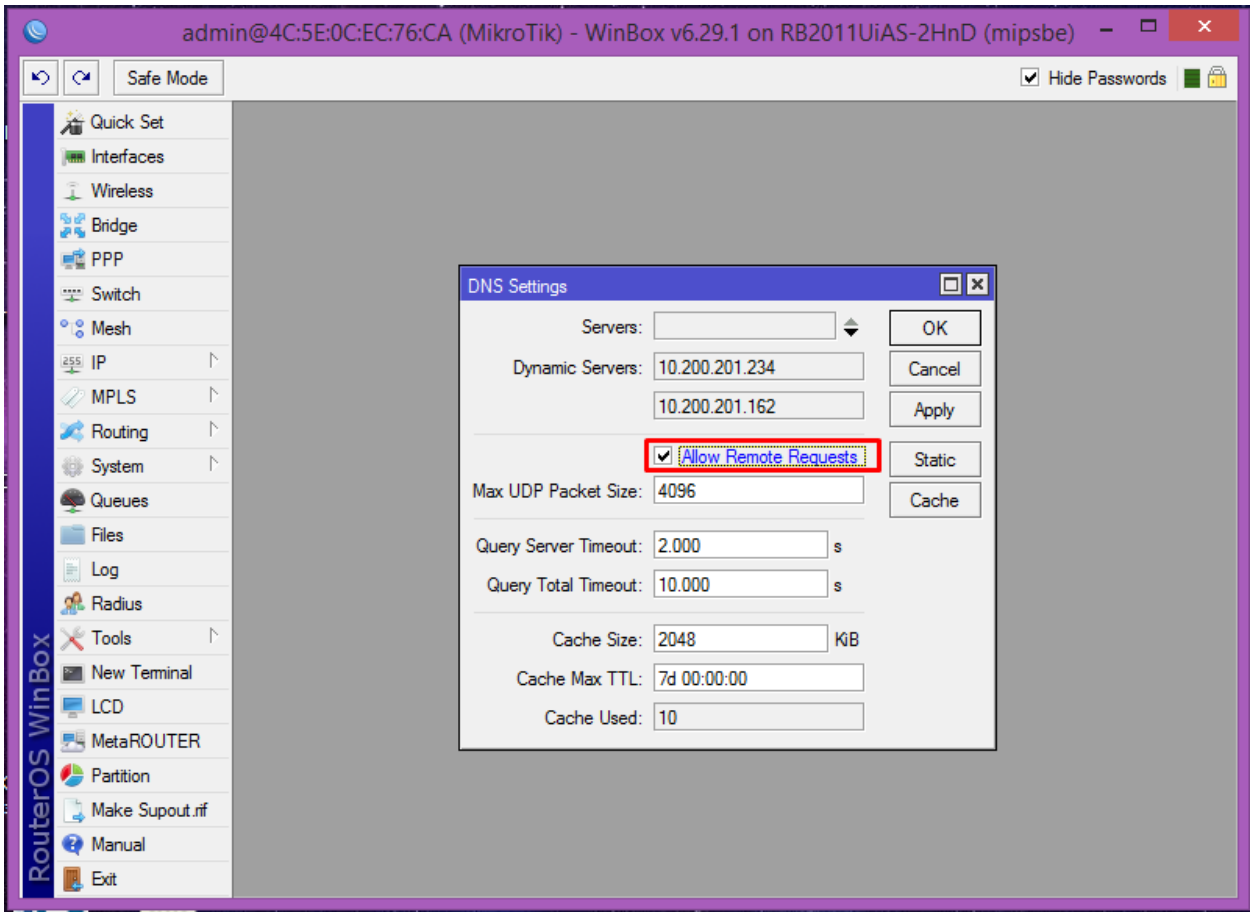
Изображение 31 – Проверка получения IP-адреса.

Теперь настроим DNS Relay, чтобы устройства автоматически получали адреса DNS-серверов. Для этого переходим в раздел «IP» – «DNS», изображение 32.



Изображение 32 – Переход в раздел с настройкой DNS.

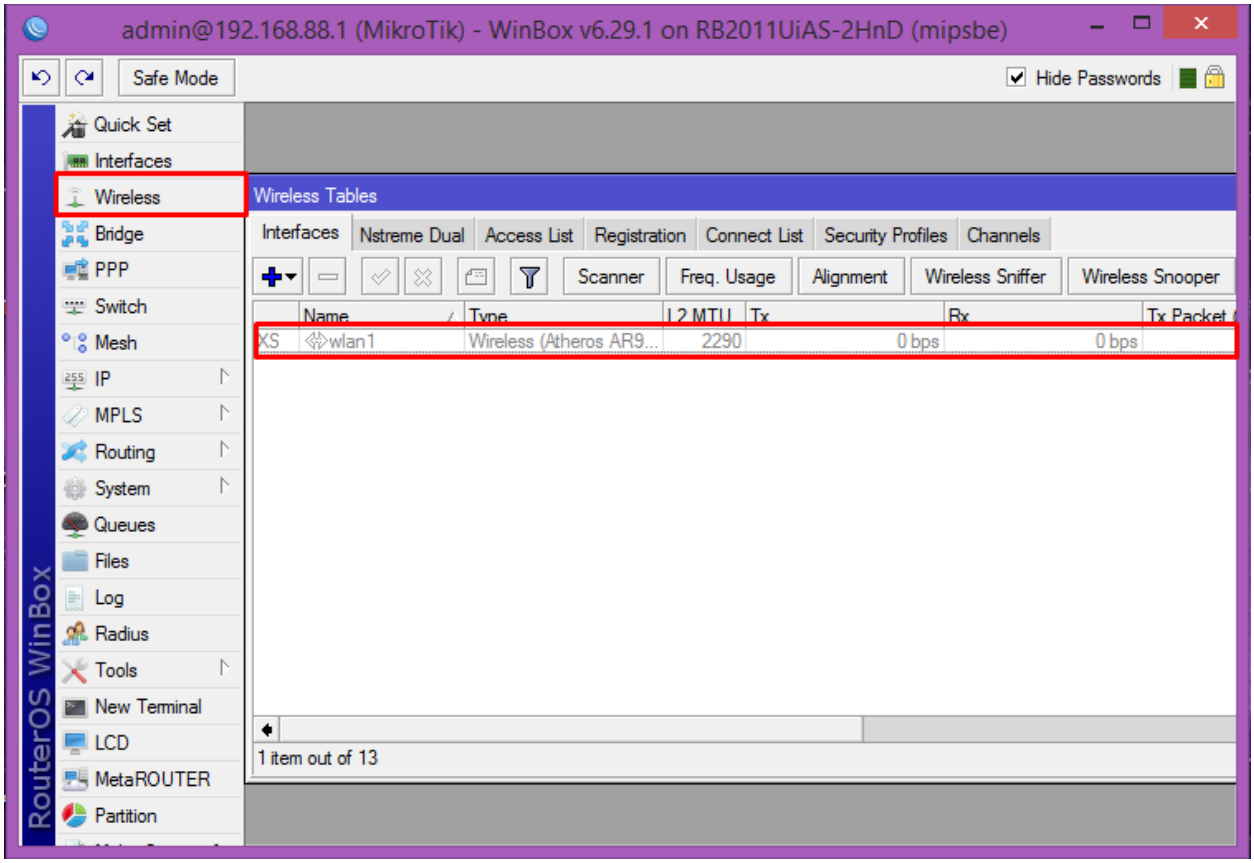
Здесь, изображение 33, необходимо установить галочку «Allow Remote Requests» для включения DNS Relay. Также можно посмотреть текущие адреса DNS-серверов.



Изображение 33 – Включение DNS Relay.

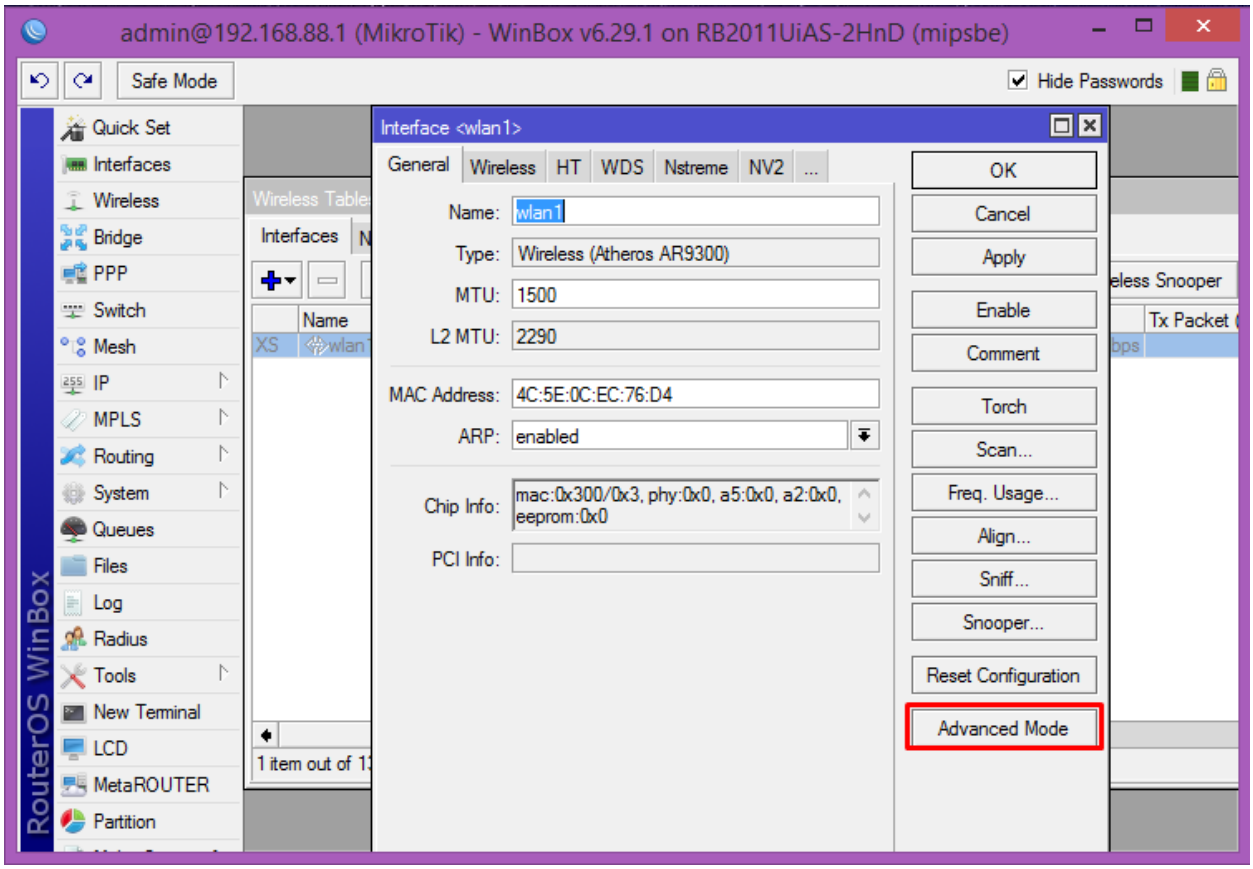
Настройка беспроводной сети

Перейдем к настройкам беспроводной сети. Открываем раздел «Wireless» и во вкладке «Interfaces» выбираем нашу беспроводную сеть «wlan1», изображение 34, после чего дважды нажимаем на неё для конфигурирования. После всех этих настроек должен заработать Интернет по кабелю через данный маршрутизатор.



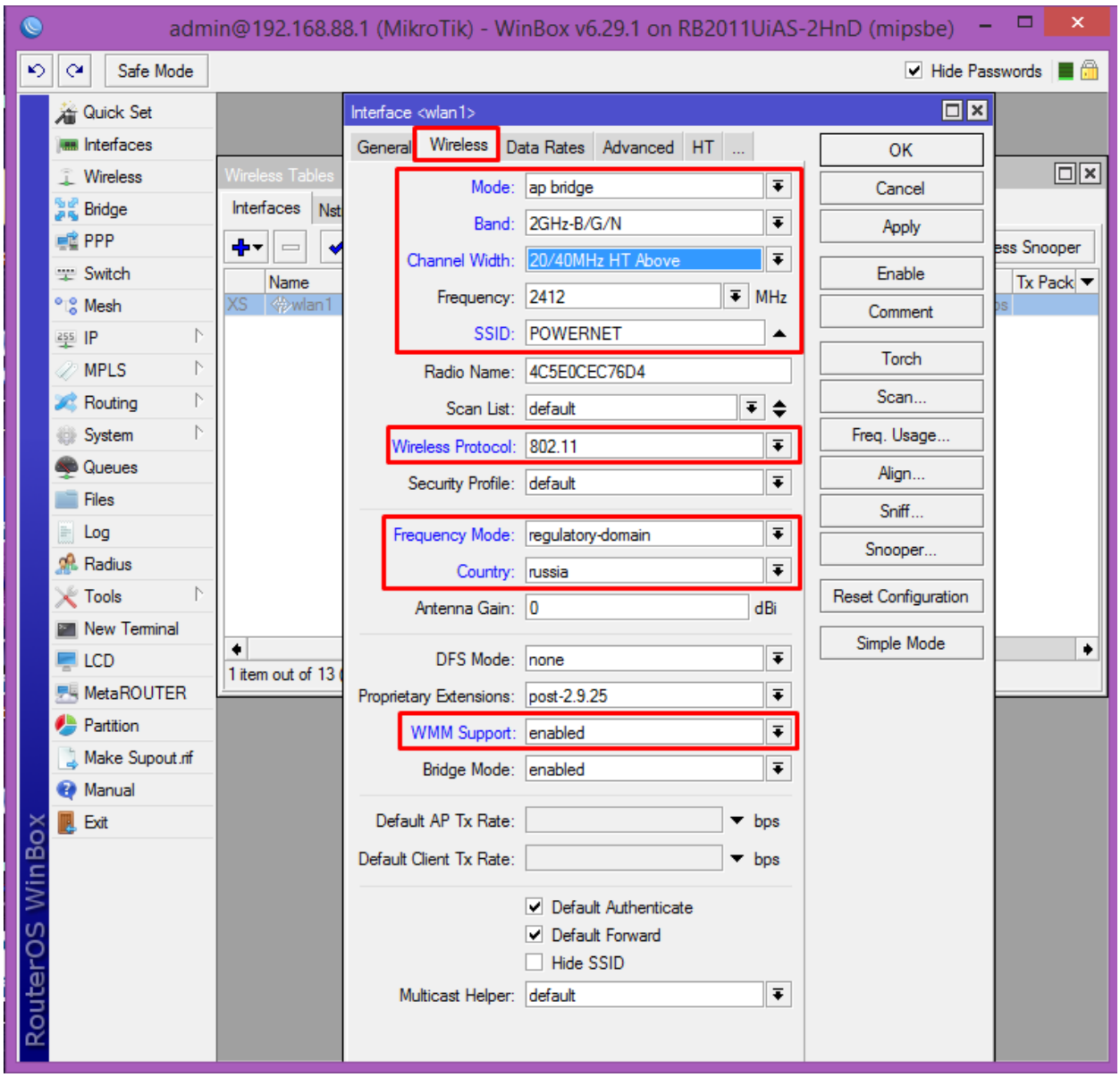
Изображение 34 – Переход к настройкам беспроводной сети.

Здесь мы можем задать имя для интерфейса беспроводной сети, изображение 35, но это имя не является именем беспроводной сети (SSID). Для перехода к расширенным настройкам нажимаем на кнопку «Advanced Mode».



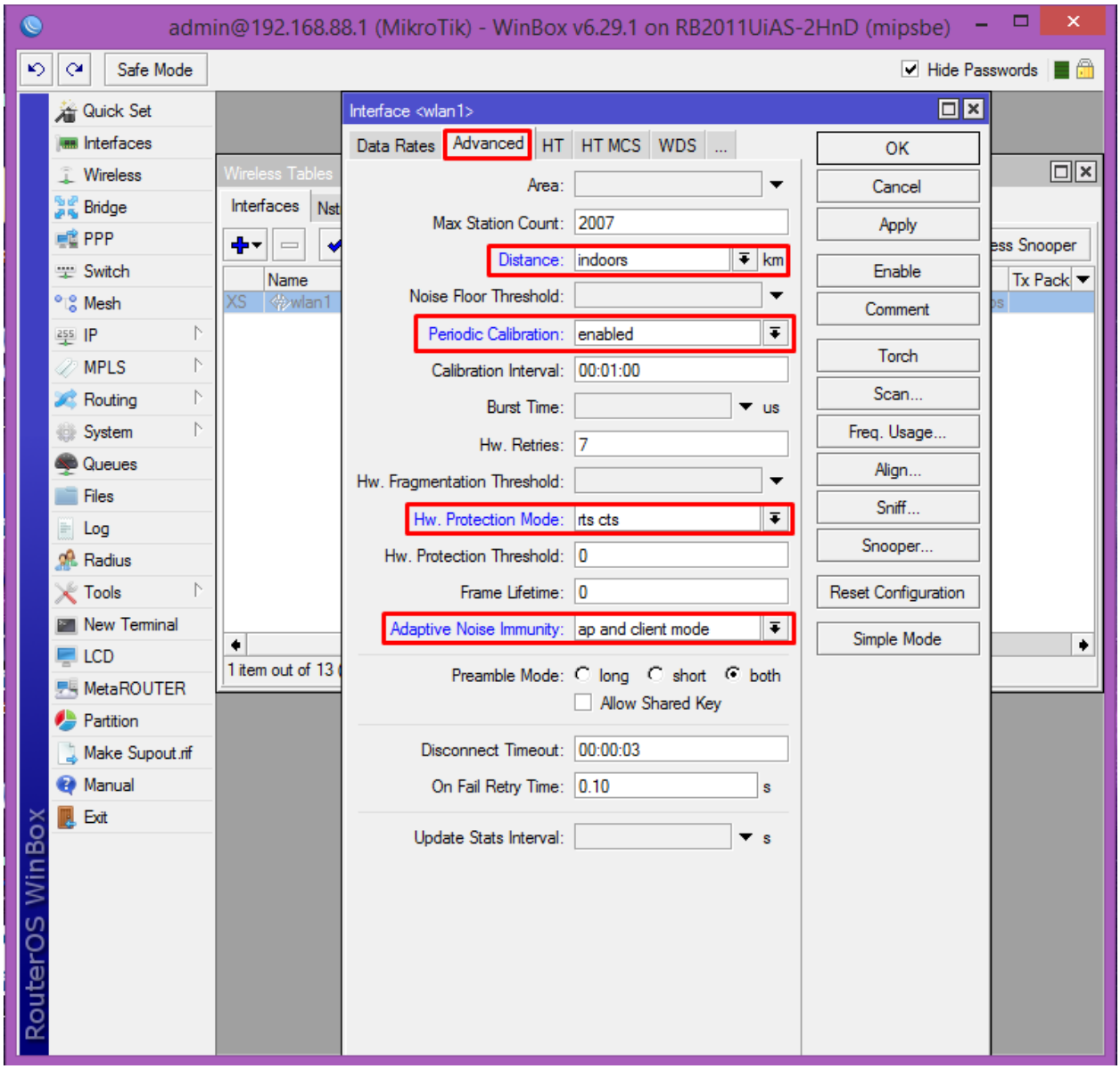
Изображение 35 – Переход к расширенным настройкам беспроводной сети.

В открывшемся окне, изображение 36, во вкладке «Wireless» необходимо произвести конфигурацию:
«Mode» – «ap bridge».
«Band» – «2GHz-B/G/N».
«Channel Width» – «20/40MHz HT Above».
«Frequency» – функция выбора канала, но здесь канал выбирается в виде частоты.
«SSID» – вводим название беспроводной сети.
«Wireless Protocol» – «802.11».
«Frequency Mode» – «regulatory-domain».
«Country» – «russia».
«WMM Support» – «enabled».



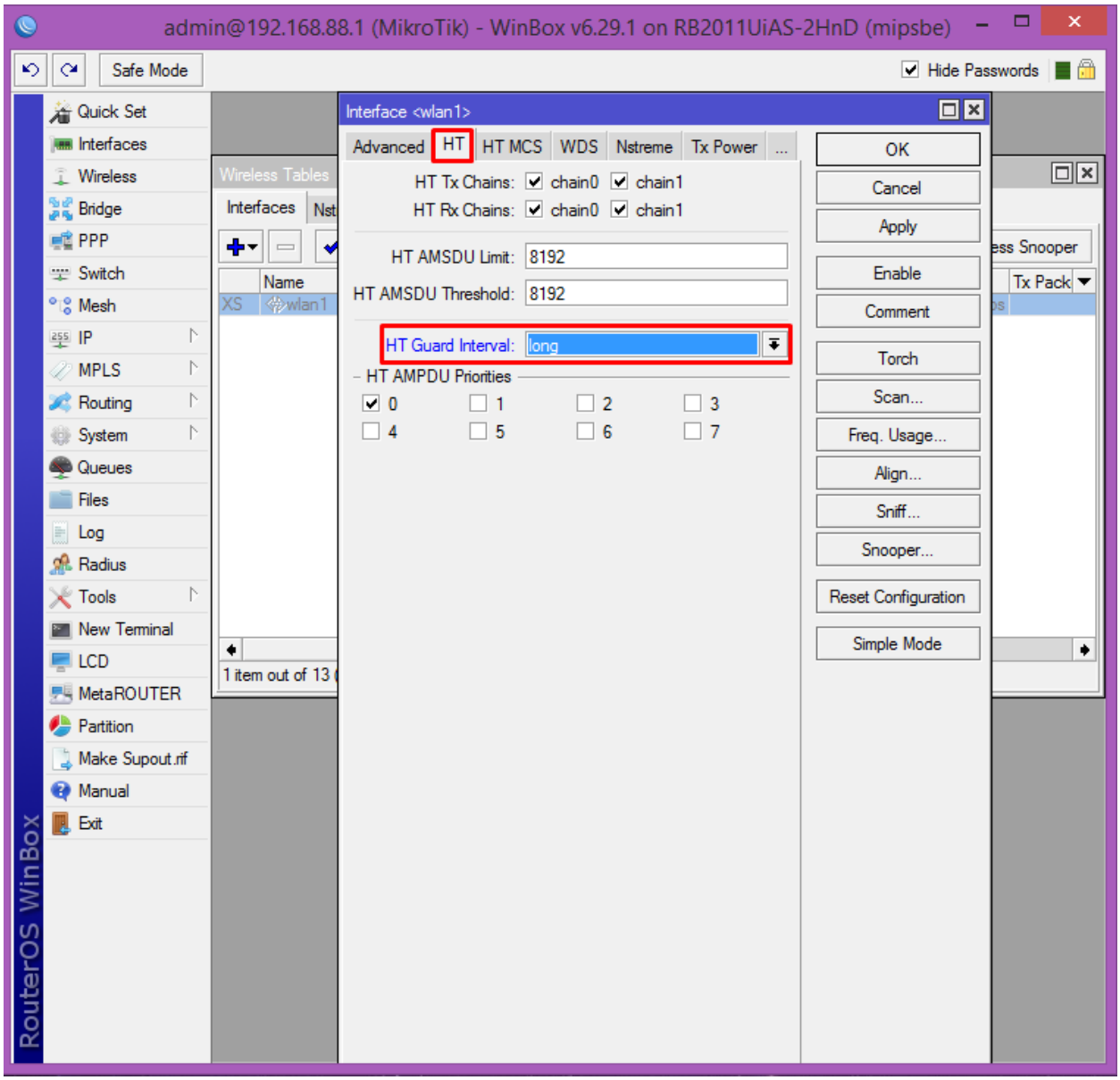
Изображение 36 – Расширенные настройки беспроводной сети.

Далее переходим во вкладку «Advanced», изображение 37, и настраиваем следующим образом:
«Distance» – «indoors».
«Periodic Calibration» – «enabled».
«Hw. Protection Mode» – «rts cts».
«Adaptive Noise Immunity» – «ap and client mode».



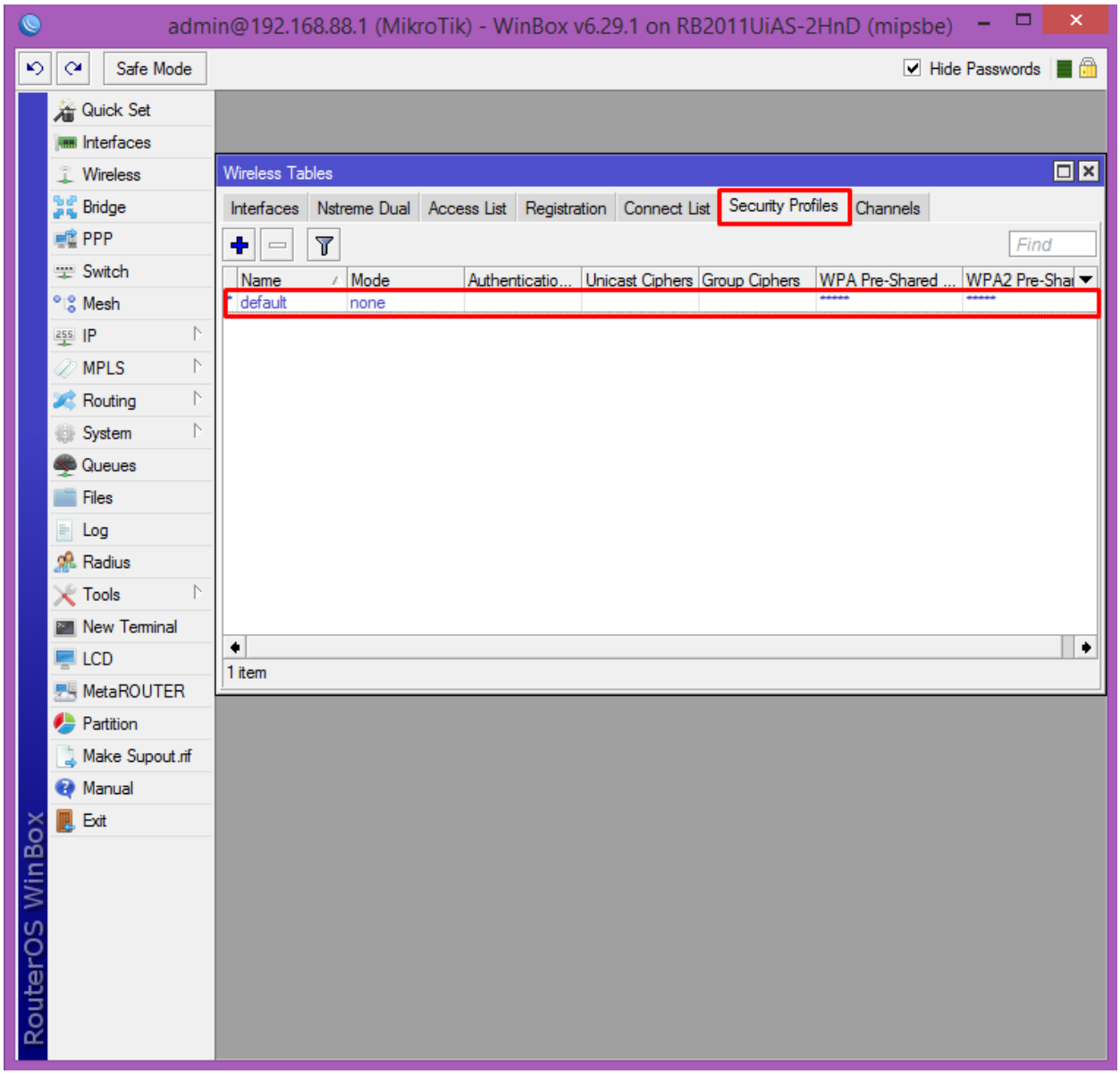
Изображение 37 – Расширенные настройки беспроводной сети.

Во вкладке «HT» в поле «HT Guard Interval» выставляем «long», изображение 38, и нажимаем «OK», чтобы применить параметры завершить расширенную настройку.



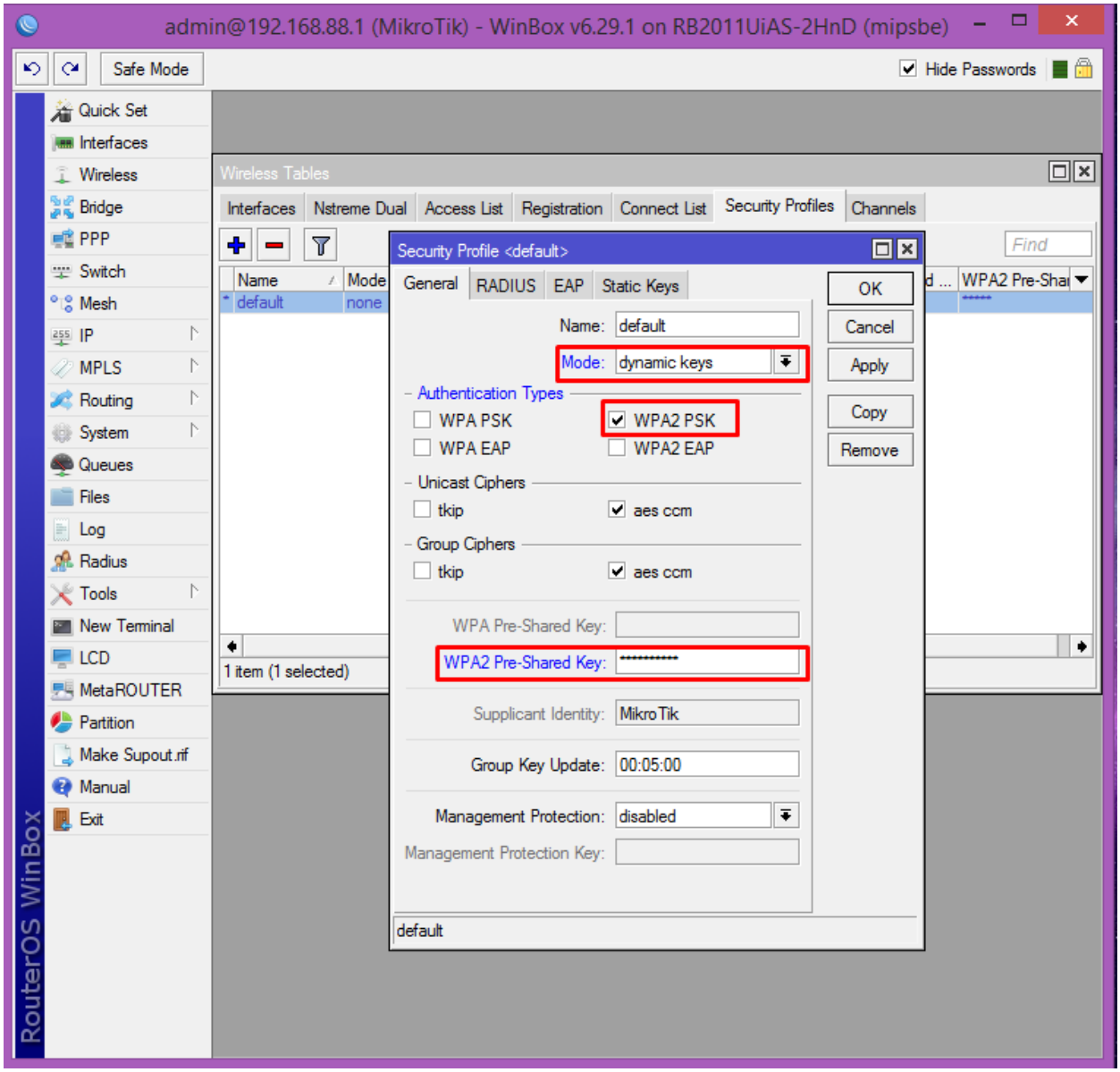
Изображение 38 – Расширенные настройки беспроводной сети.

Теперь проведем настройку защиты беспроводной сети. Переходим во вкладку «Security Profiles» и дважды нажимаем на существующий профиль, изображение 39.



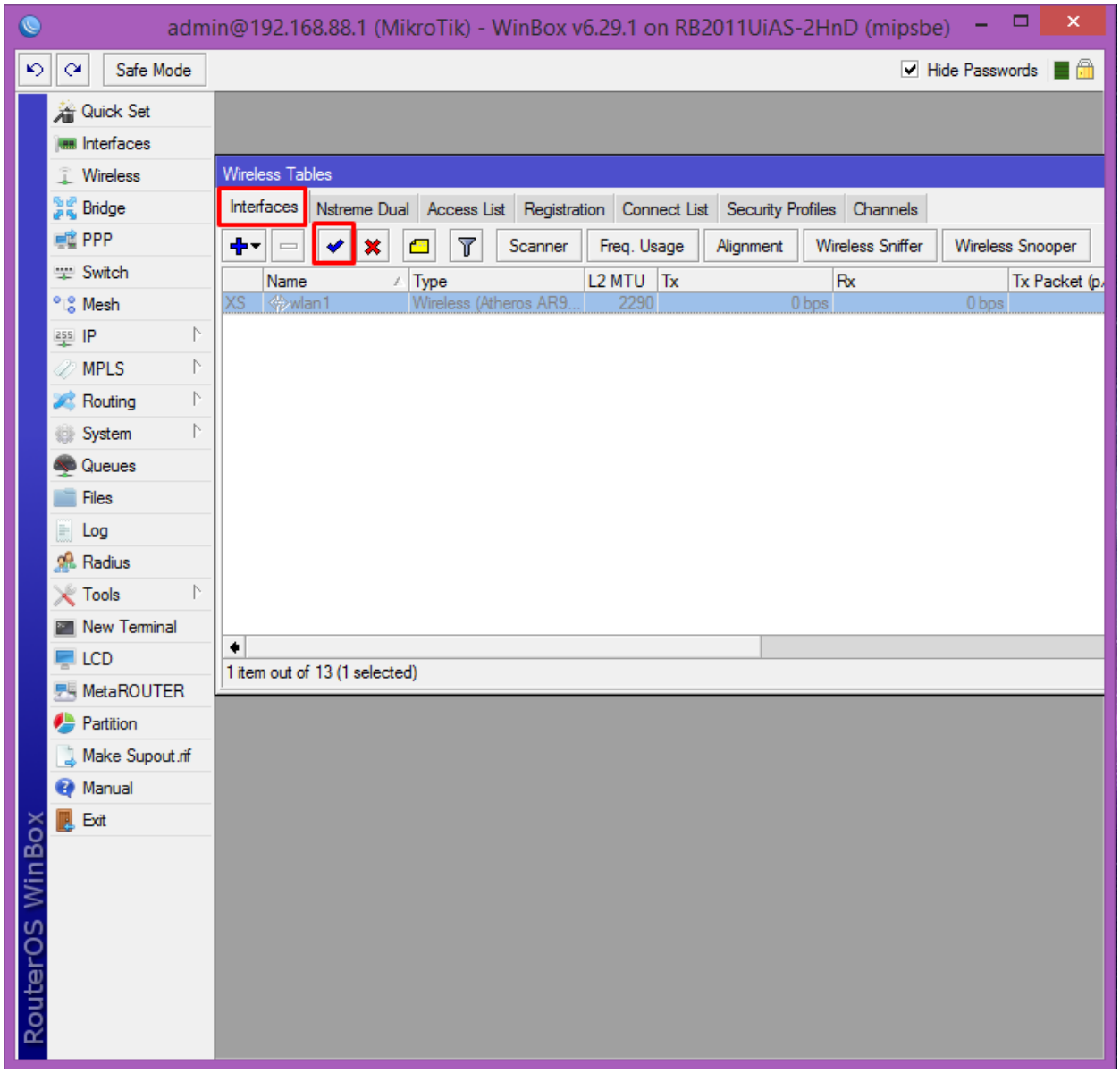
Изображение 39 – Переход к настройкам защиты беспроводной сети.

Откроется окно, изображение 40, где во вкладке «General» в поле «Mode» выставляем «dynamic keys», в «Authentication Types» выбираем нужным тип аутентификации, в нашем случае «WPA2 PSK», и в поле «WPA2 Pre-Shared Key» вводим пароль для подключения к беспроводной сети. Нажимаем «OK» для применения настроек.



Изображение 40 – Настройка защиты беспроводной сети.

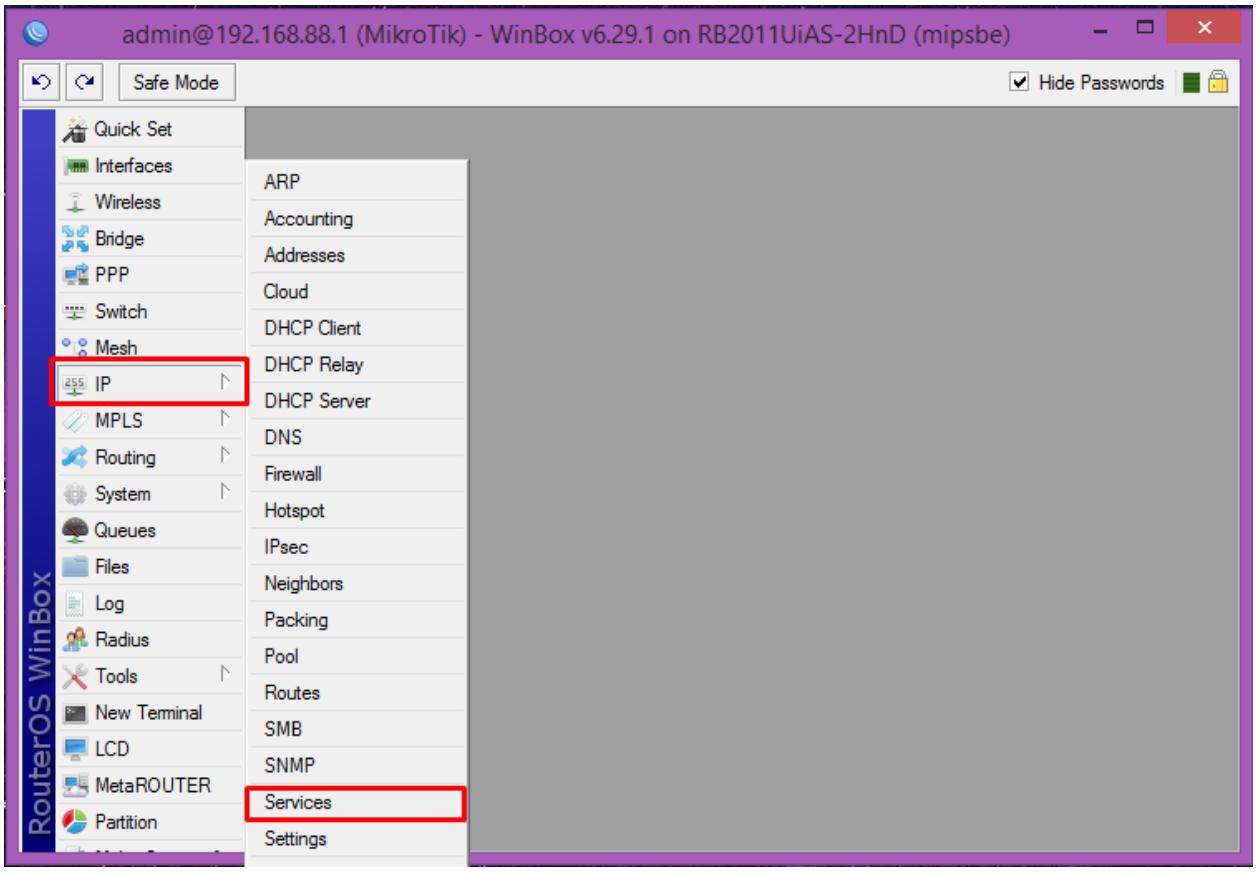
Теперь нам необходимо убедиться, что беспроводная сеть активна. Переходим во вкладку «Interfaces», и если сеть тусклая, значит она выключена, и необходимо её включить. Для этого нажимаем на кнопку с синей галочкой, изображение 41.



Изображение 41 – Включение беспроводной сети.

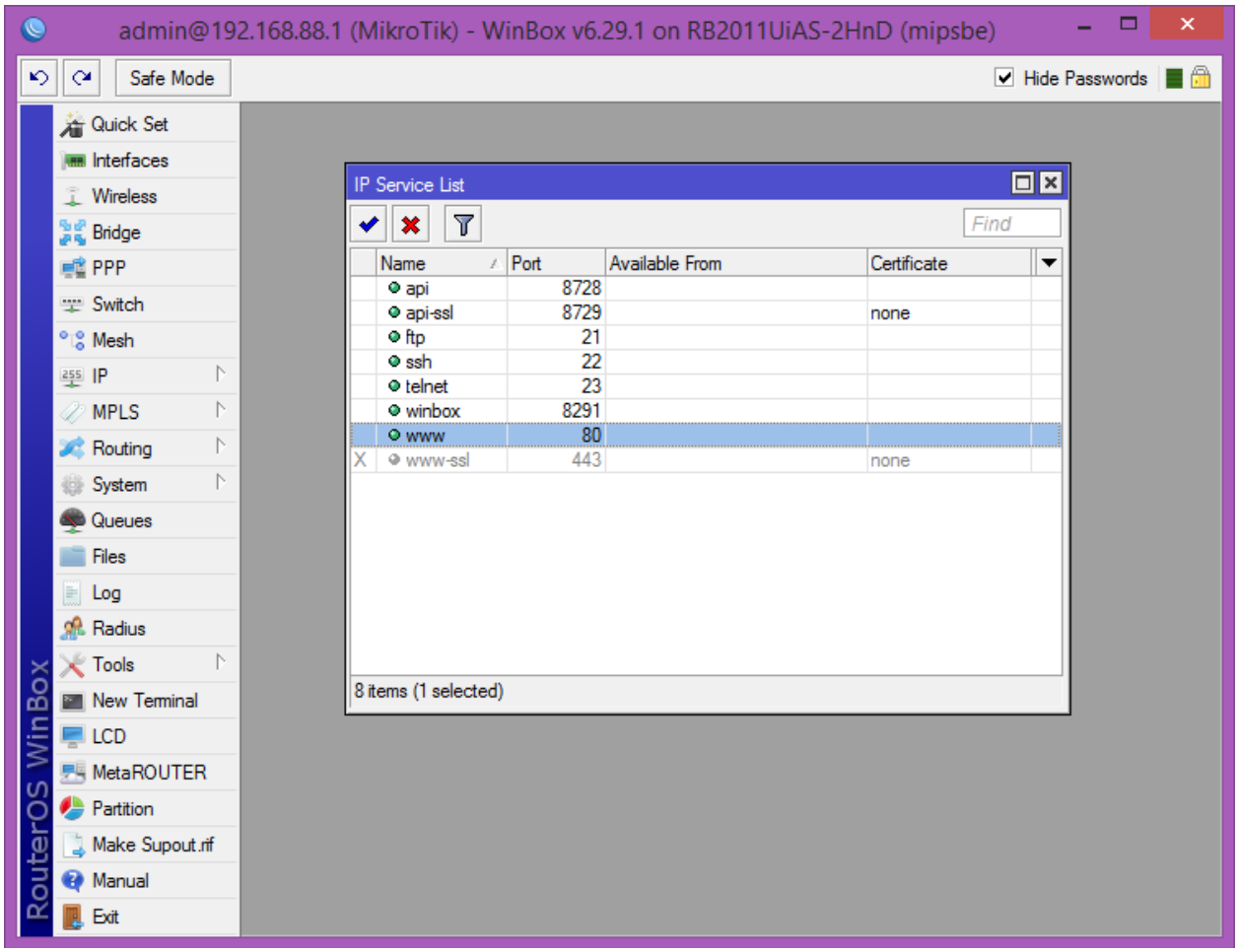
Настройка доступа

Теперь проведем настройку доступа к маршрутизатору. По умолчанию на маршрутизатор можно попасть из любой сети и любым способом (SSH, Telnet, WinBox). Сделаем так, чтобы доступ осуществлялся только из сети 192.168.88.0/24. Для этого переходим в раздел «IP» – «Services», изображение 42.



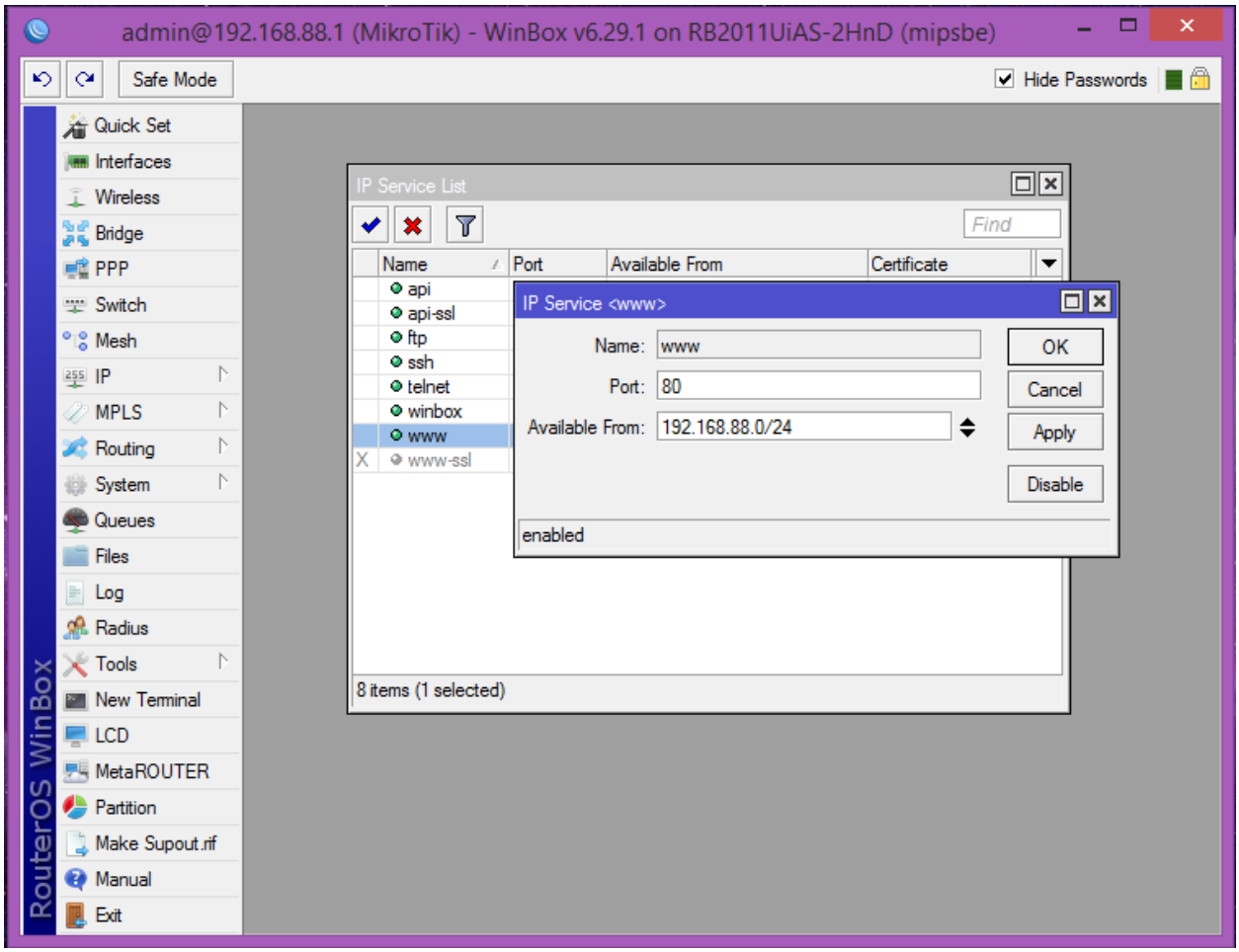
Изображение 42 – Переход к настройкам доступа.

Откроется окно, изображение 43, с настройками доступа. Доступ определенным способом можно отключить или включить, если выделить необходимый нам способ и нажать на синюю галочку или красный крестик соответственно.



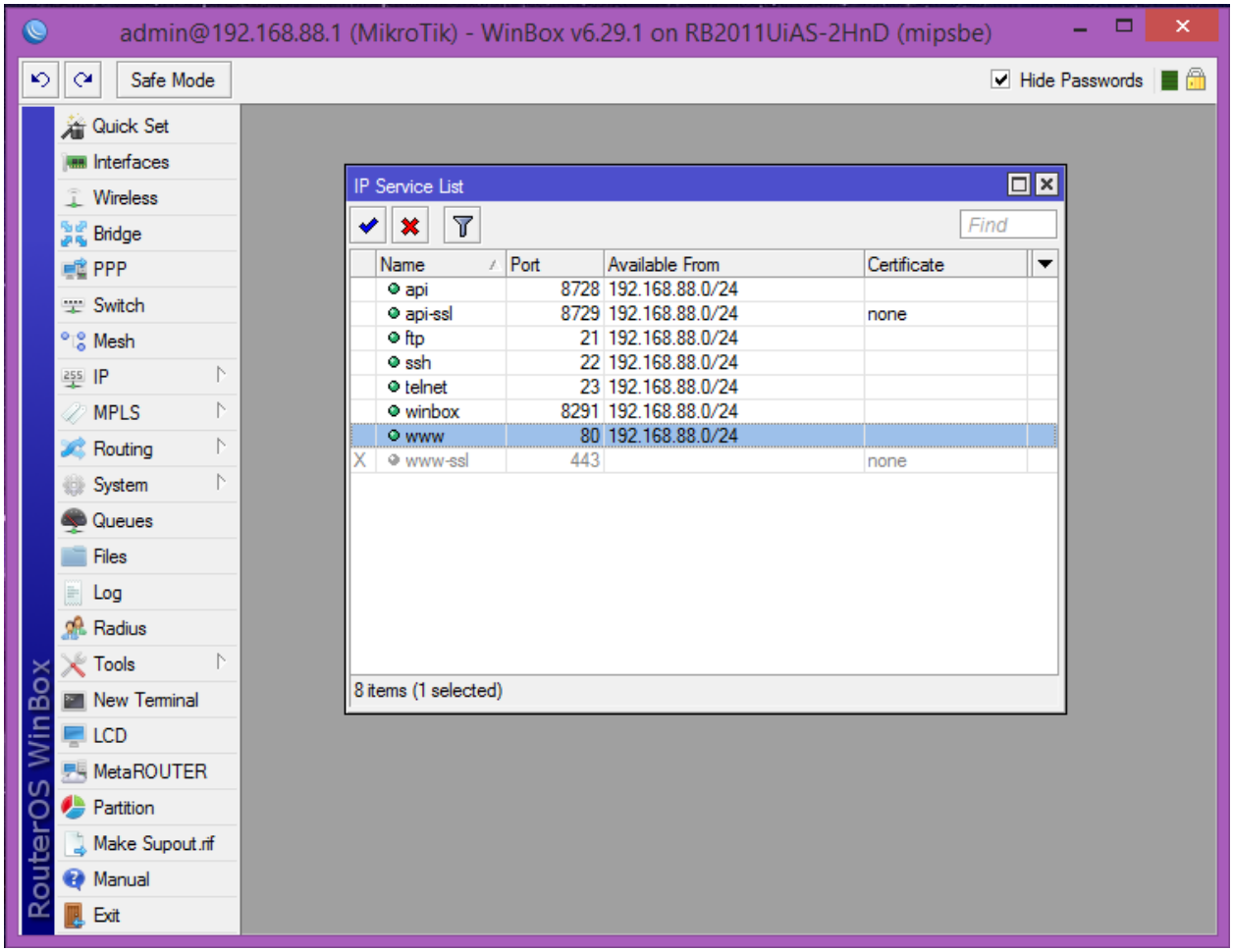
Изображение 43 – Список способов подключения к маршрутизатору.

Для изменения настроек какого-либо способа дважды нажимаем него. Откроется следующее окно, изображение 44, где для нашей ситуации в поле «Available Form» прописываем 192.168.88.0/24.



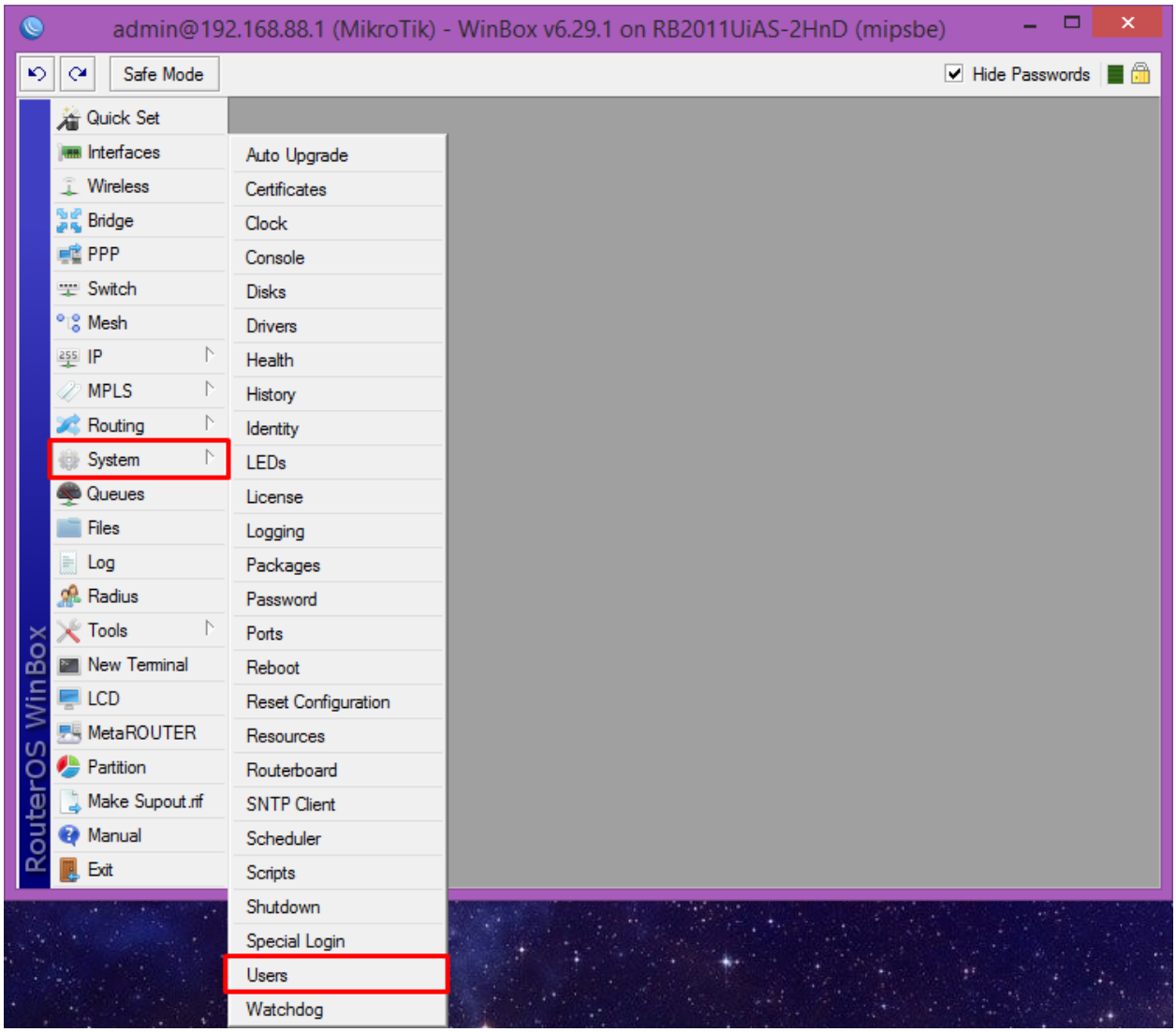
Изображение 44 – Конфигурирования доступа к маршрутизатору для определенного способа.

Данную настройку проводим для каждого способа, и в конечном итоге должно получиться следующее, изображение 45.



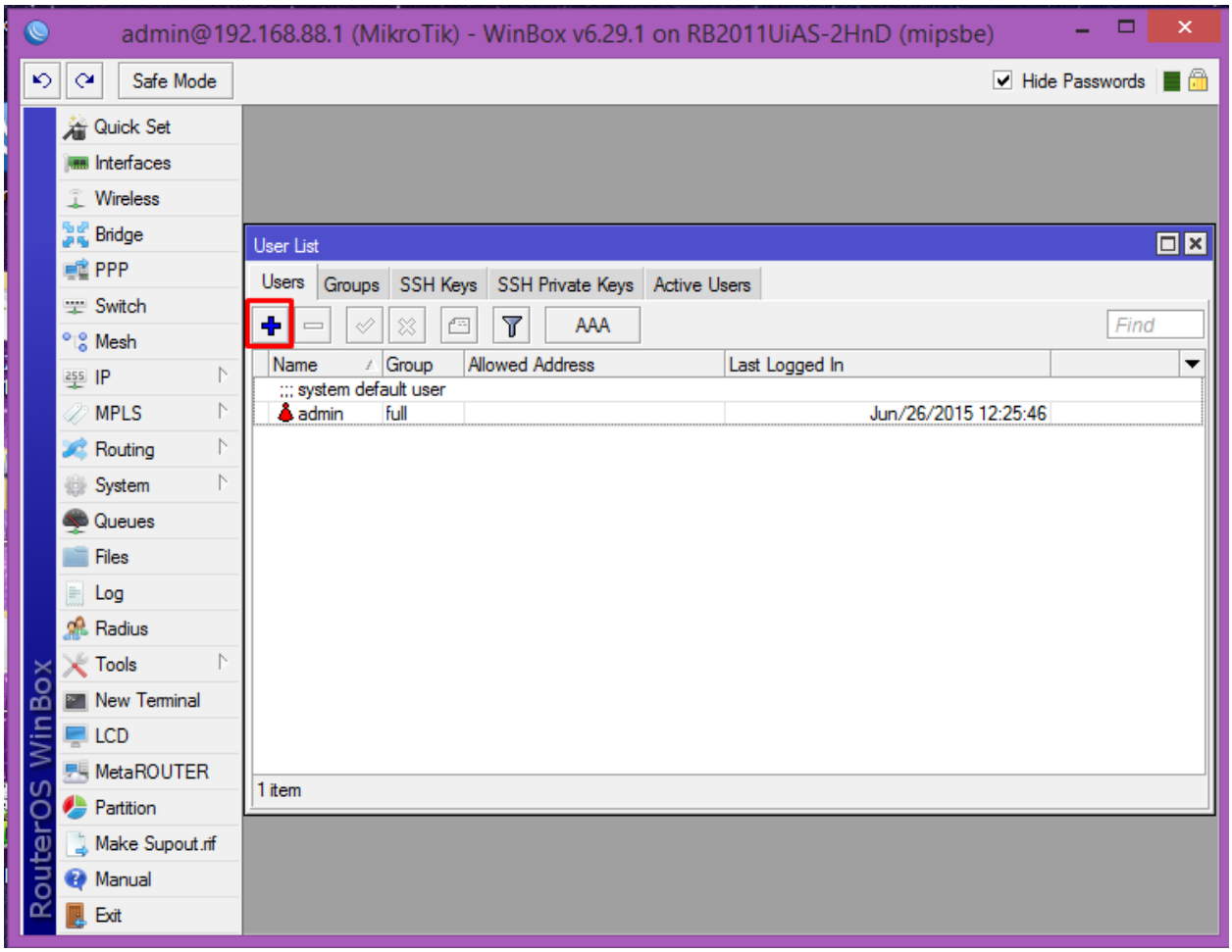
Изображение 45 – Вид после конфигурирования доступа к маршрутизатору.

Теперь перейдем к настройкам пользователей маршрутизатора. Открываем раздел «System» – «Users», изображение 46.



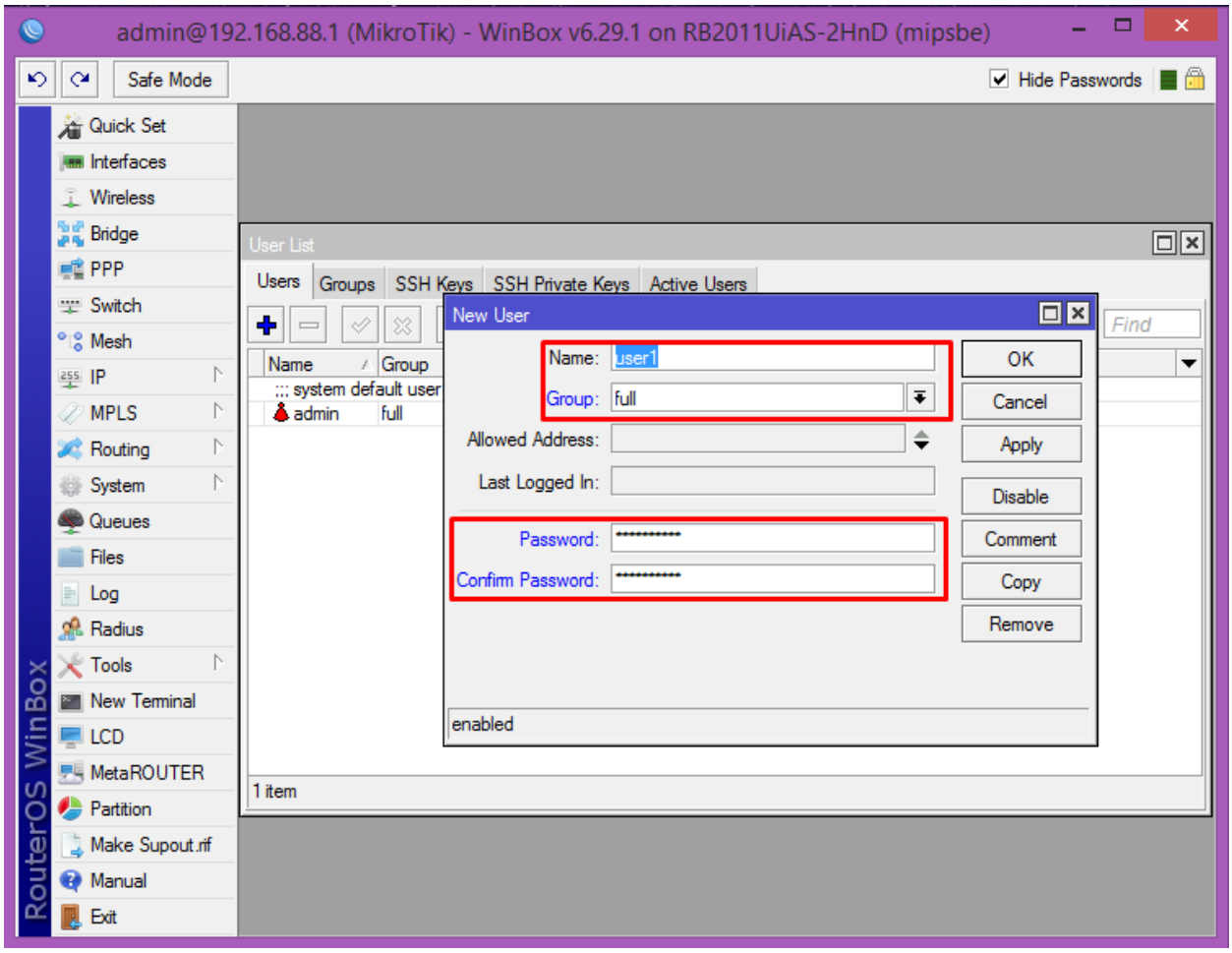
Изображение 46 – Переход к настройкам пользователей.

Откроется окно с имеющимися пользователями. Для создания нового пользователя во вкладке «Users» нажимаем на «+», изображение 47.



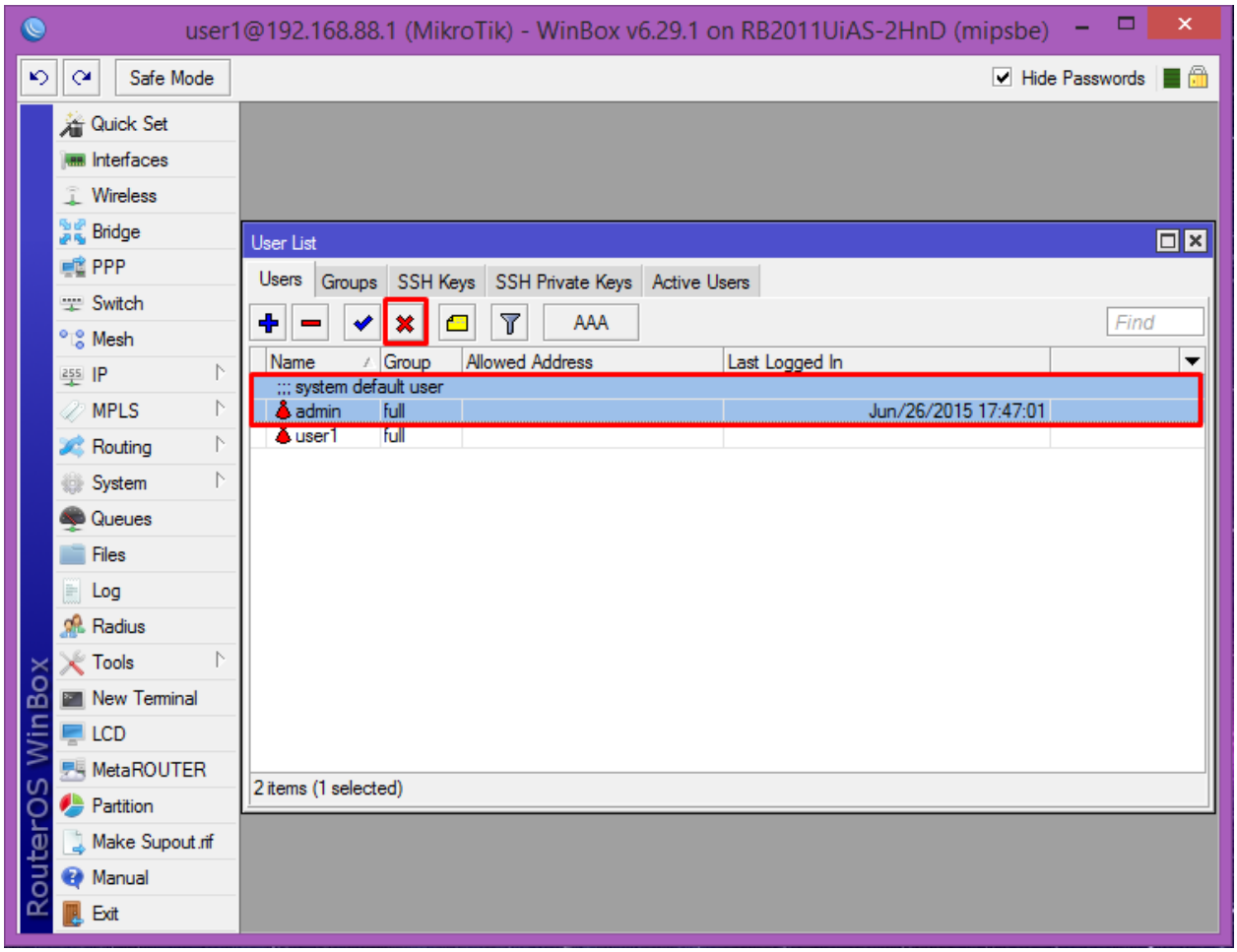
Изображение 47 – Создание нового пользователя.

В открывшемся окне, изображение 48, в поле «Name» вводим имя пользователя. В поле «Group» устанавливаем «full» для получения полного доступа. В полях «Password» и «Confirm Password» вводим пароль и подтверждение пароля. Нажимаем «OK» для применения настроек.



Изображение 48 – Настройка нового пользователя.

Использование какого-либо пользователя можно отключить или включить, путем нажатия на красный крестик и синюю галочку соответственно. Сделаем это на примере пользователя «admin», изображение 49.

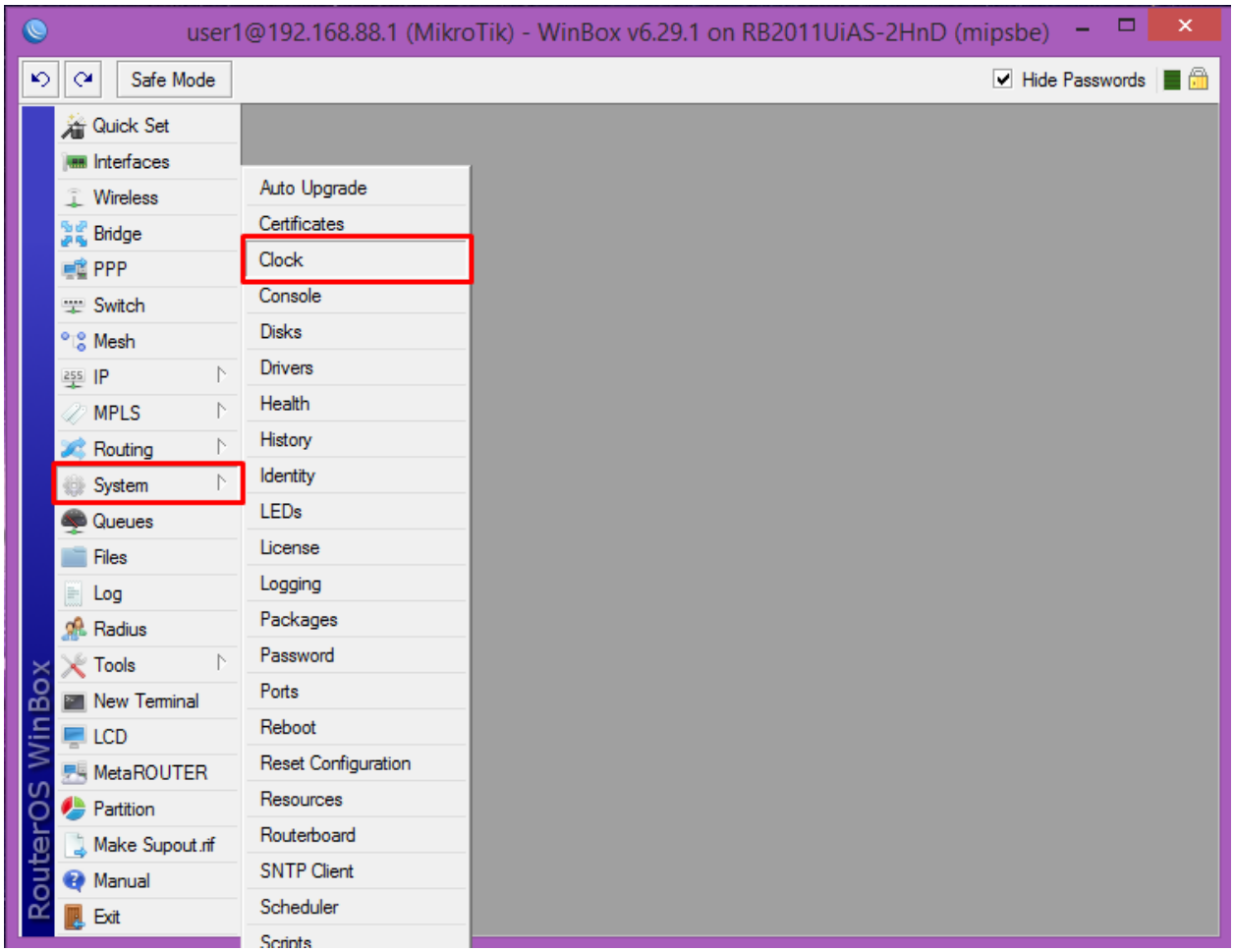


Изображение 49 – Отключение пользователя.

После этого пробуем подключаться к маршрутизатору с помощью созданного пользователя (в нашем случае user1).

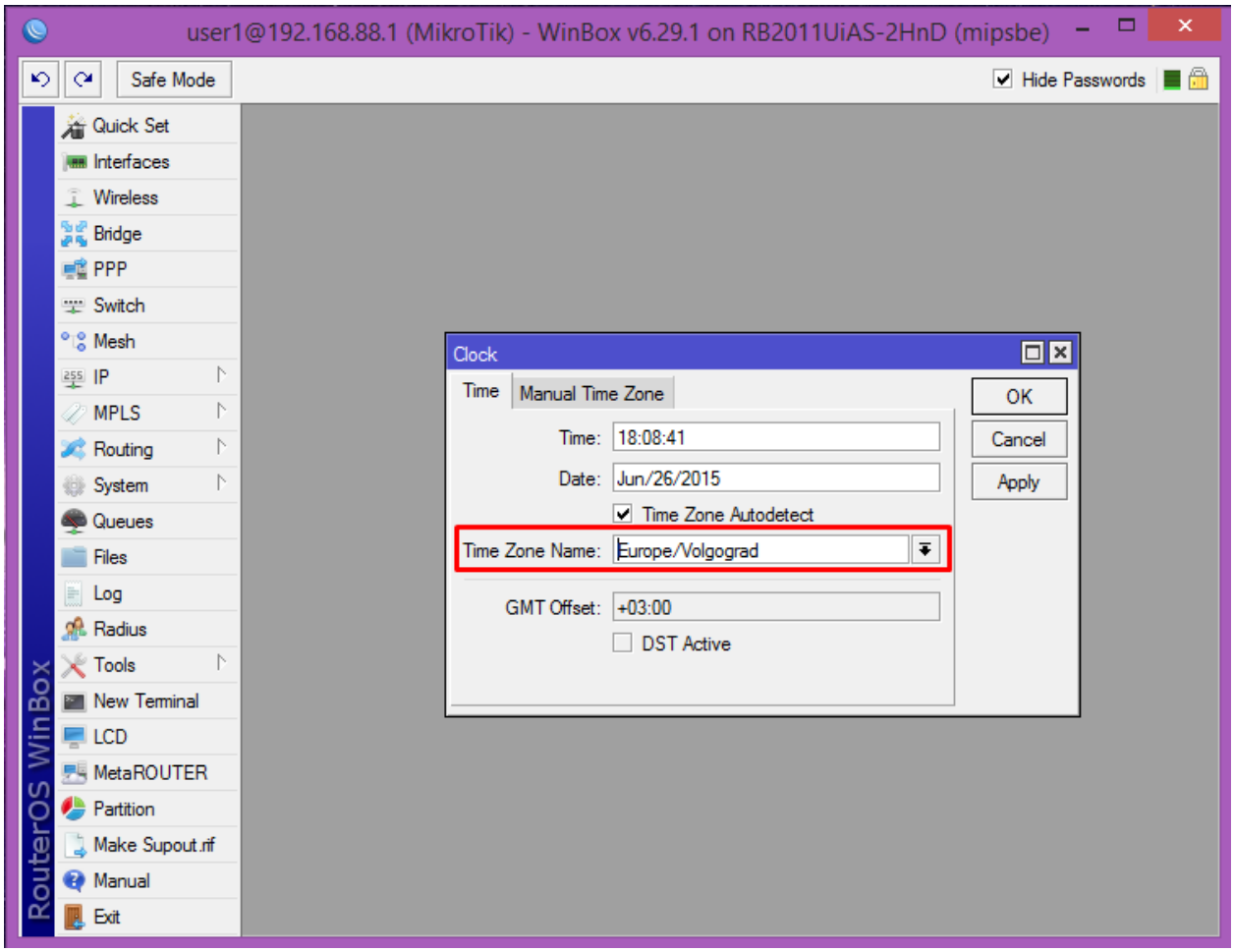
Настройка времени и NTP-клиента

Проведем настройку времени и SNTP-клиента. Переходим в раздел «System» – «Clock» для настройки времени, изображение 50.



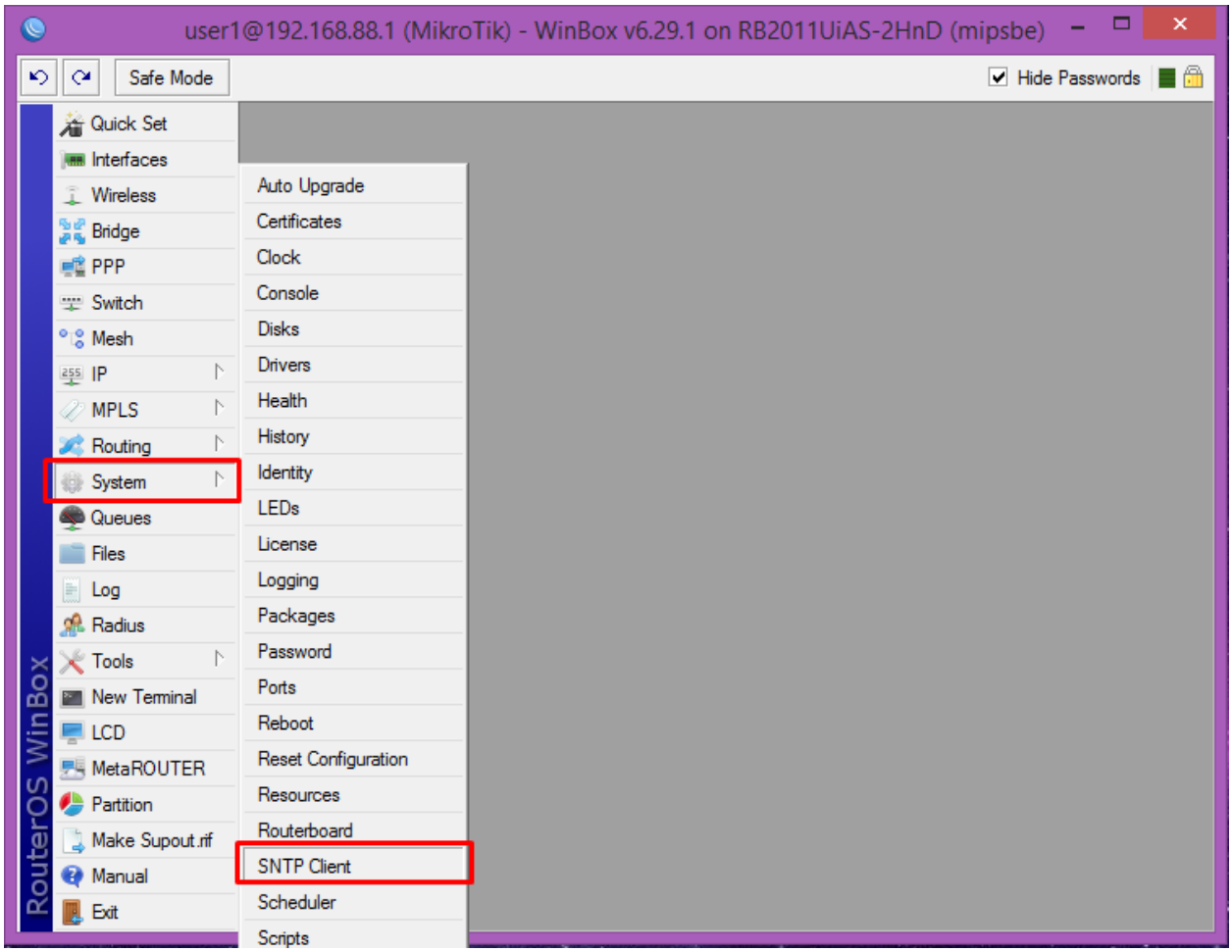
Изображение 50 – Переход к настройкам времени.

В открывшем окне, изображение 51, производим настройку времени, даты, а также выбираем временную зону «Time Zone Name». Для нашего случая временную зону выбираем «Europe/Volgograd». Нажимаем «OK» для применения настроек.



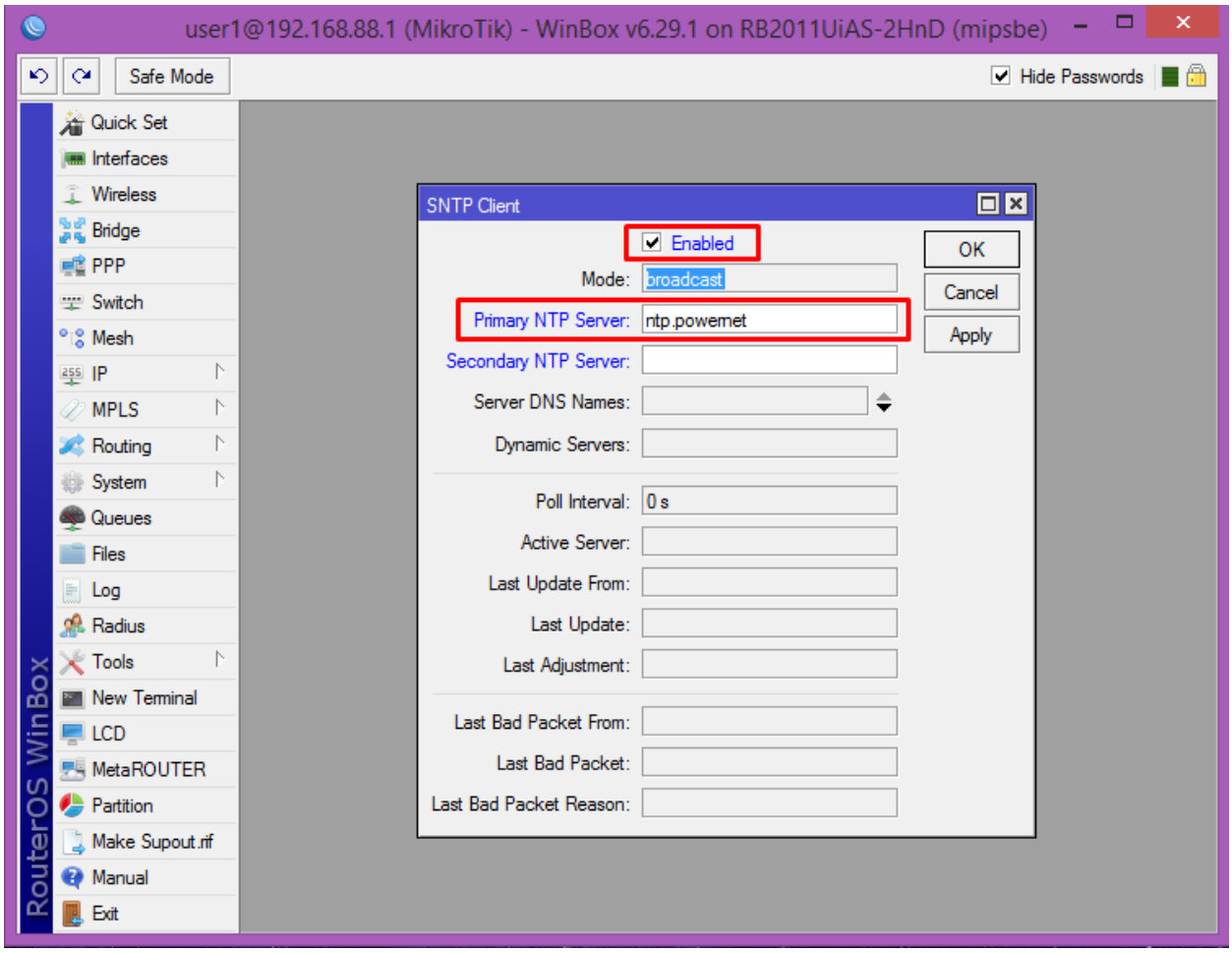
Изображение 51 – Настройка даты, времени и временной зоны.

Произведем настройку SNTP-клиента. Переходим в раздел «System» – «SNTP Client», изображение 52.



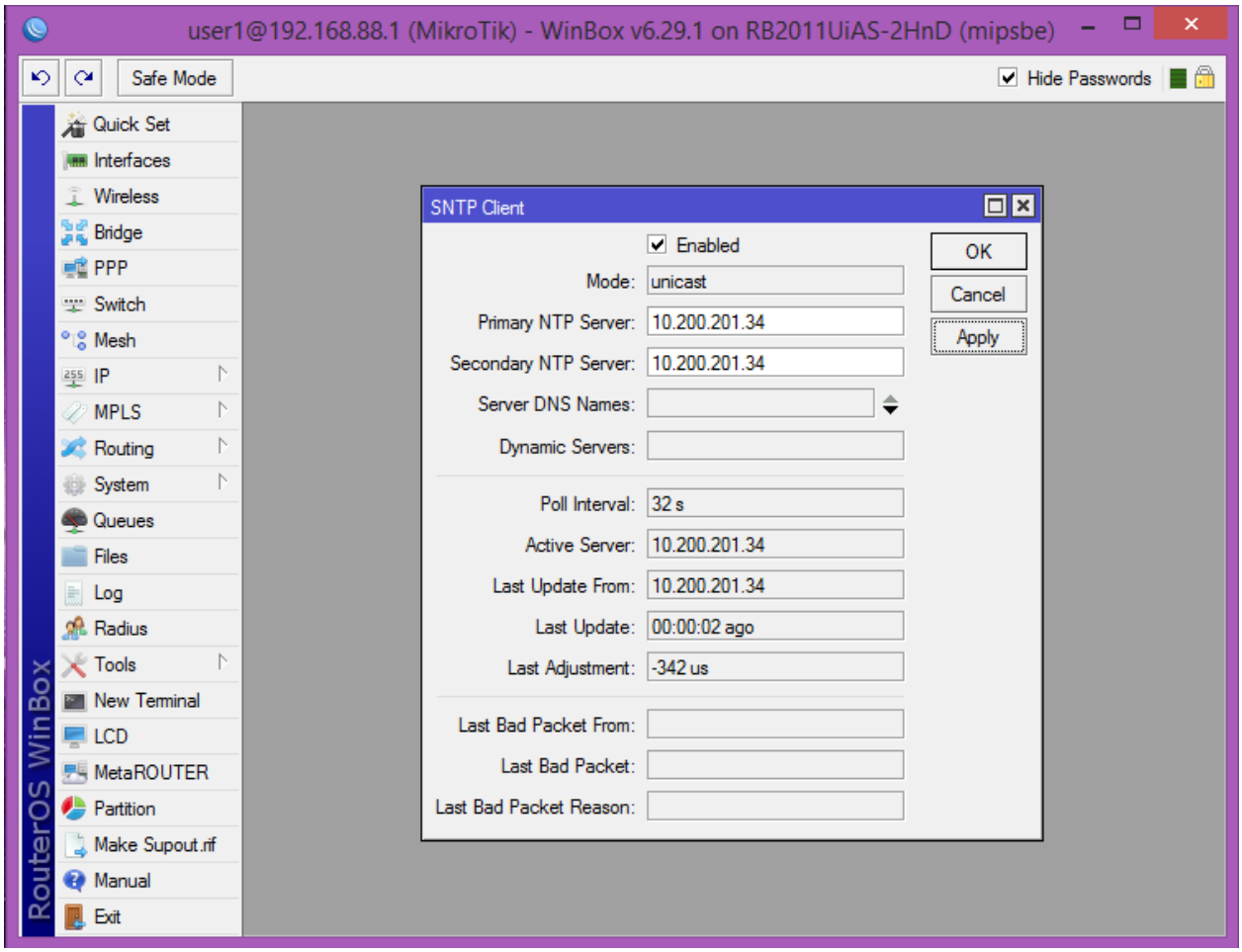
Изображение 52 – Переход к настройкам SNTP-клиента.

Здесь, изображение 53, выставляем галочку рядом с «Enabled» для включения SNTP-клиента и в полях «Primary NTP Server» и «Secondary NTP Server» вписываем «ntp.powernet». Нажимаем «OK» для применения параметров.



Изображение 53 – Настройка SNTP-клиента.

Проверяем, что подключение произошло успешно, изображение 54.

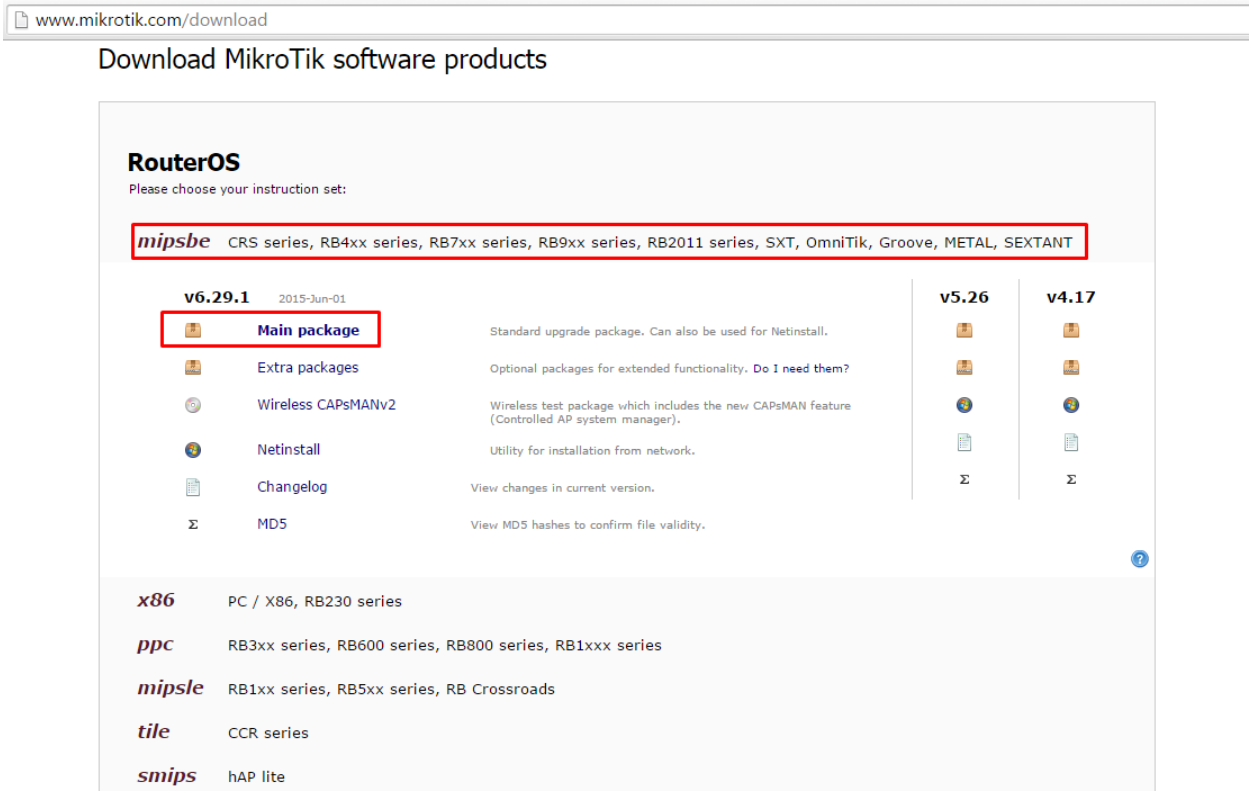


Изображение 54 – Успешное подключение к NTP-серверу.

Настройка IGMP Proxy

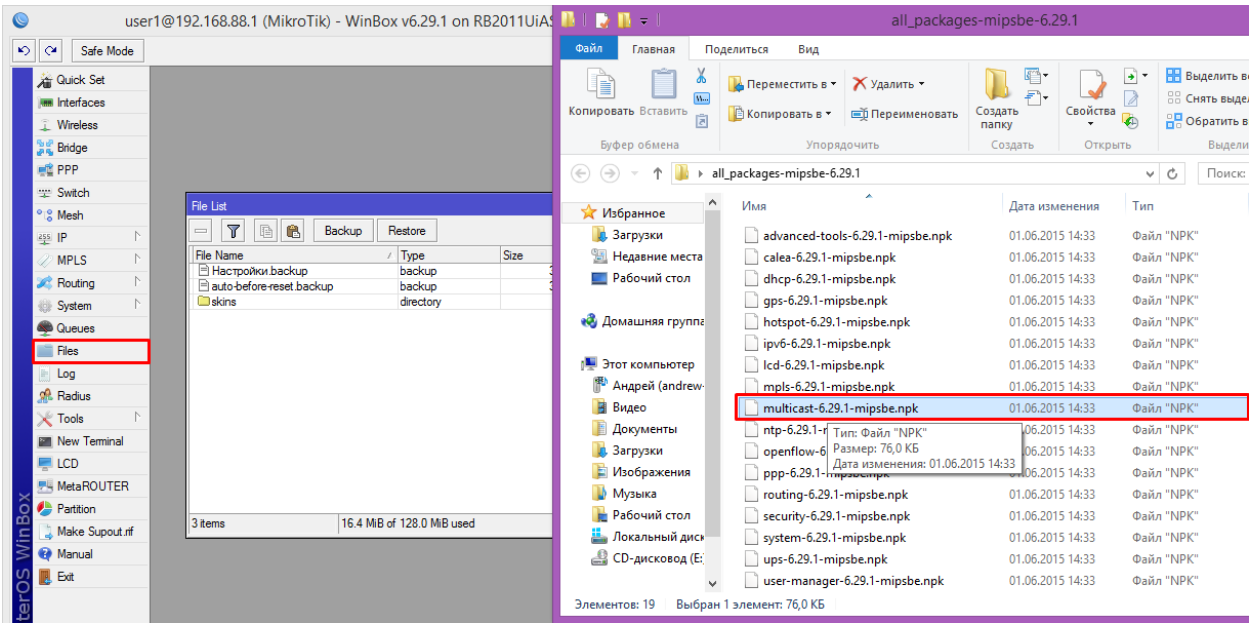
Перейдем к настройкам IGMP Proxy для данного маршрутизатора. По умолчанию на новых маршрутизаторах нет функции IGMP Proxy, то есть необходимо скачать пакет с данной функцией.

Для этого заходим на официальный сайт в раздел загрузок – http://www.mikrotik.com/download. Выбираем в списке необходимую модель маршрутизатора и версию программного обеспечения. Скачиваем «Main Package», изображение 55.



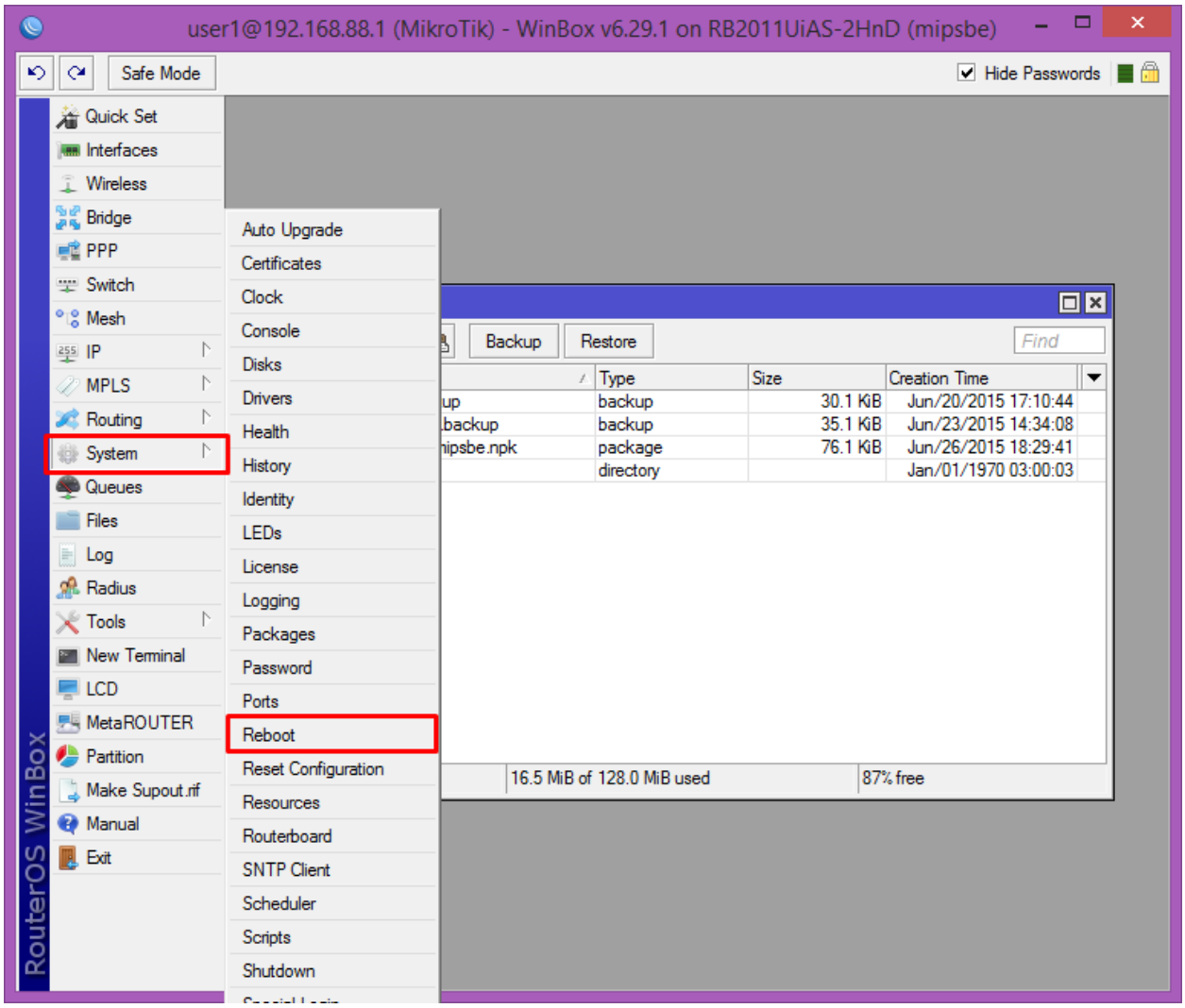
Изображение 55 – Скачивание дополнительных пакетов.

Распаковываем скачанный архив, открываем его и находим интересующий нас фай – «multicast-6.29.1-mipsbe.npk». На маршрутизаторе открываем раздел «Files» и перетаскиваем наш файл в открывшееся окно на маршрутизаторе, изображение 56.



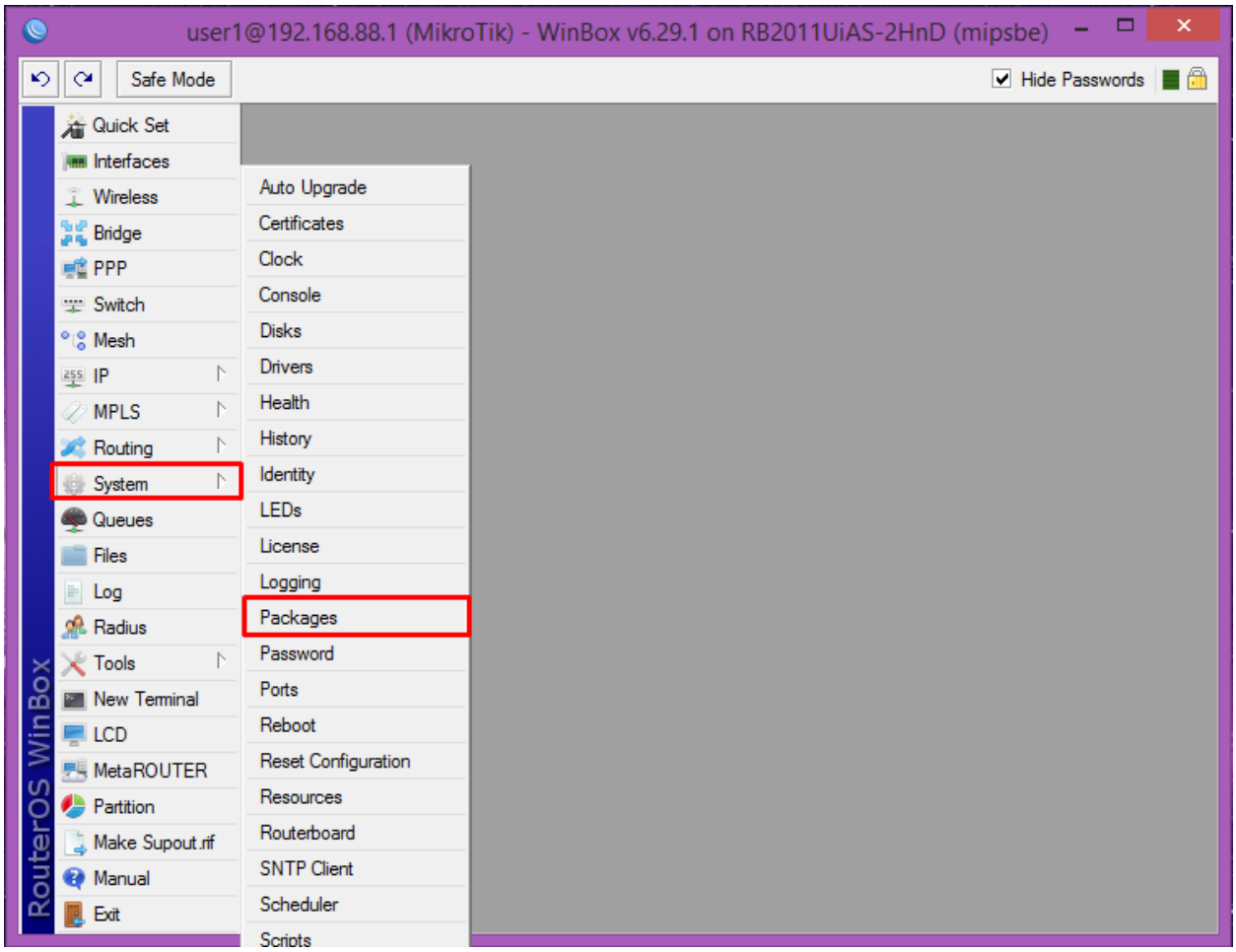
Изображение 56 – Добавления пакета IGMP Proxy на маршрутизатор.

После этого производим перезагрузку маршрутизатора для установки пакета. Для этого нажимаем на «System» – «Reboot», изображение 57.



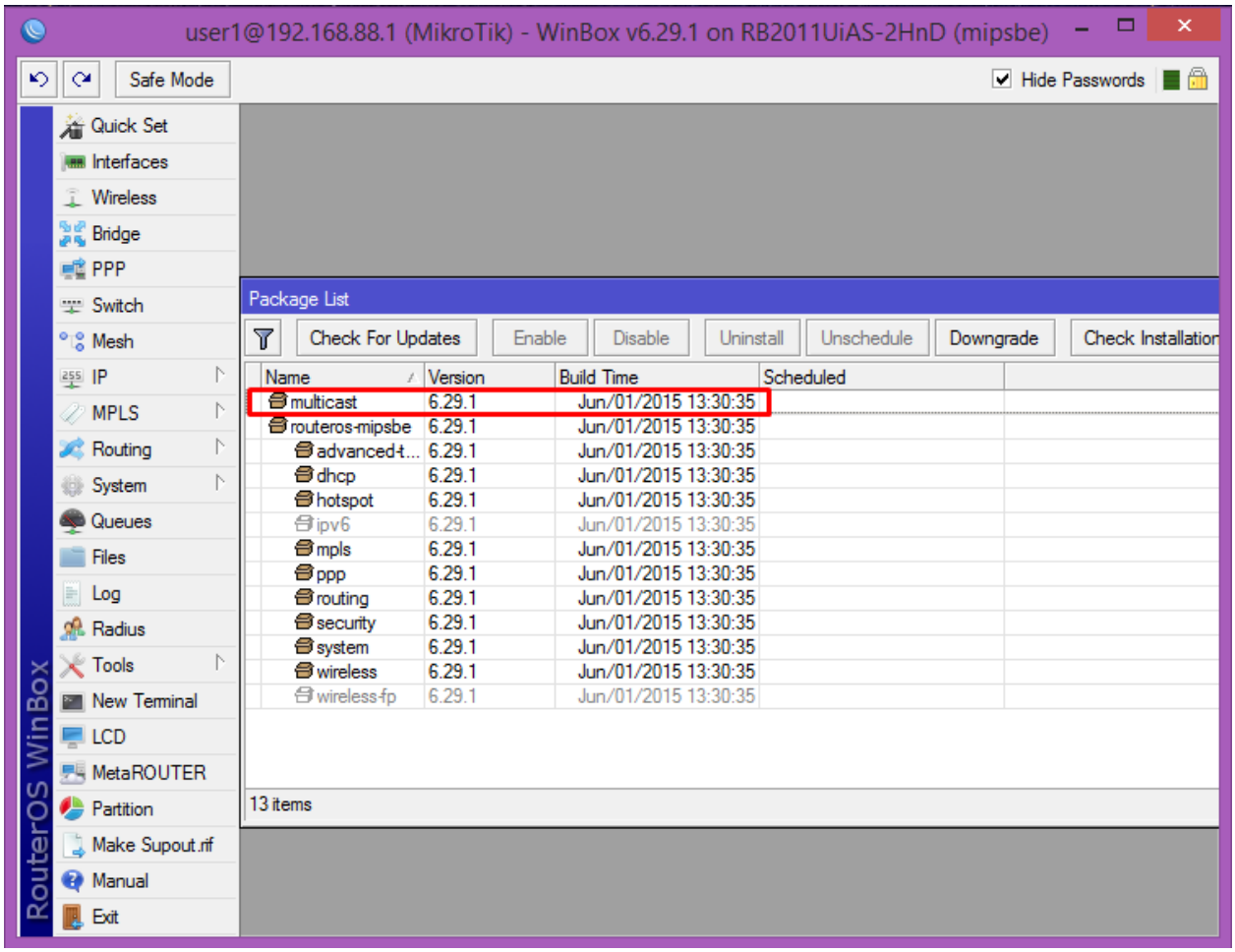
Изображение 57 – Перезагрузка маршрутизатора.

После перезагрузки маршрутизатора подключаемся к нему заново с помощью WinBox и проверяем, что наш пакет успешно установился. Для этого переходим в раздел «System» – «Packages», изображение 58.



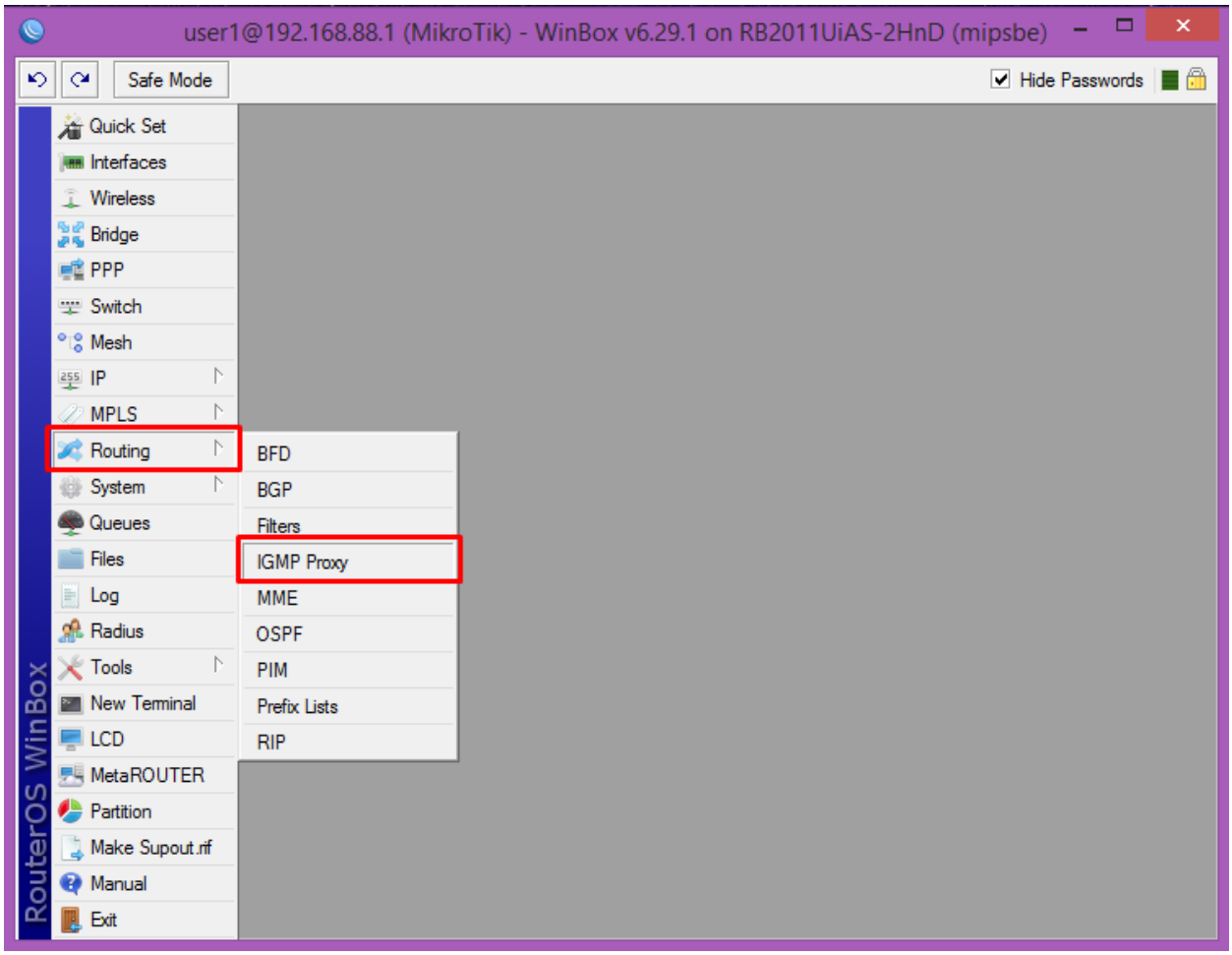
Изображение 58 – Переход к разделу установленных пакетов.

Здесь видим, что наш пакет успешно установился, изображение 59.



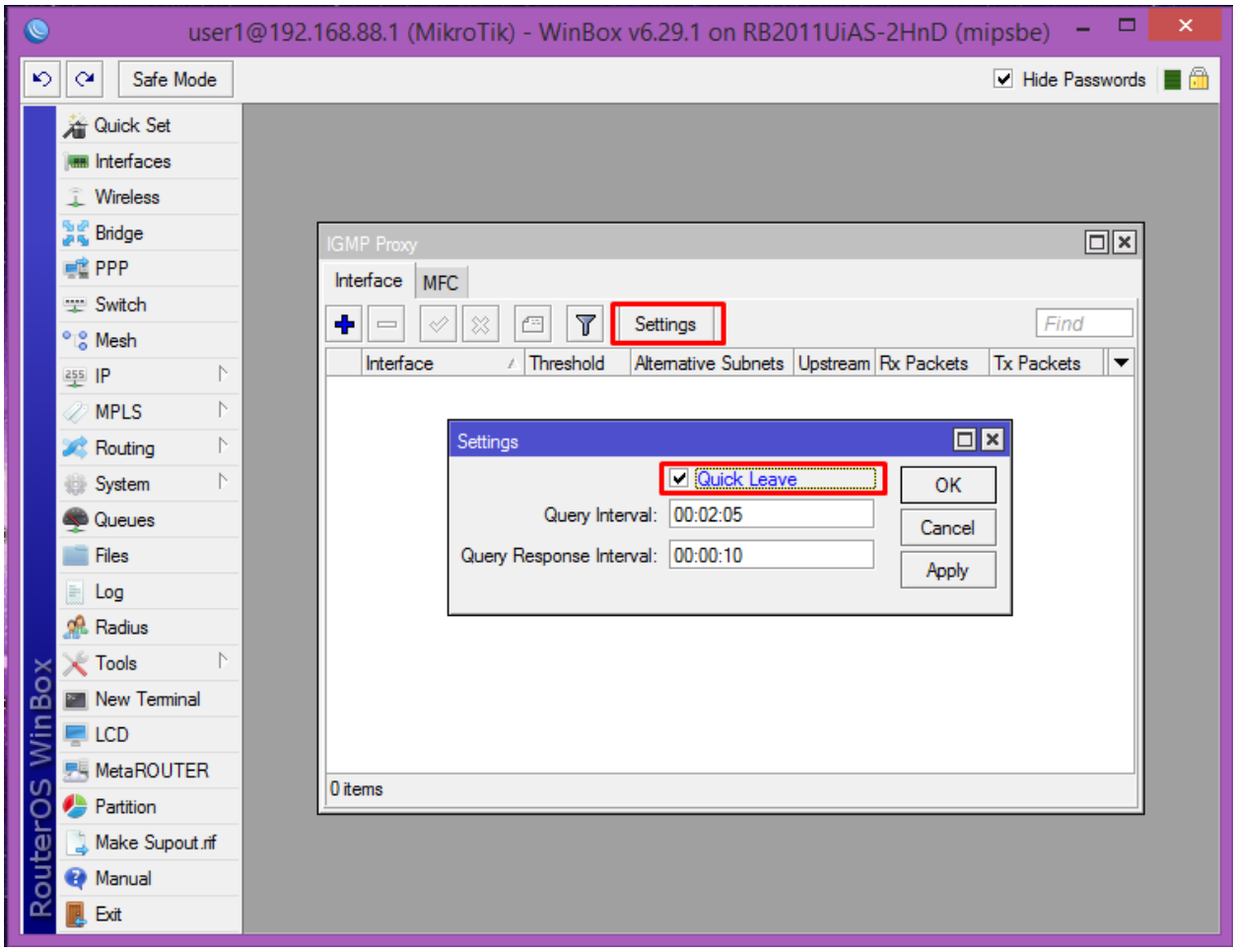
Изображение 59 – Установленный пакет.

Далее необходимо провести настройку IGMP Proxy. Для этого переходим в раздел «Routing» – «IGMP Proxy», изображение 60.



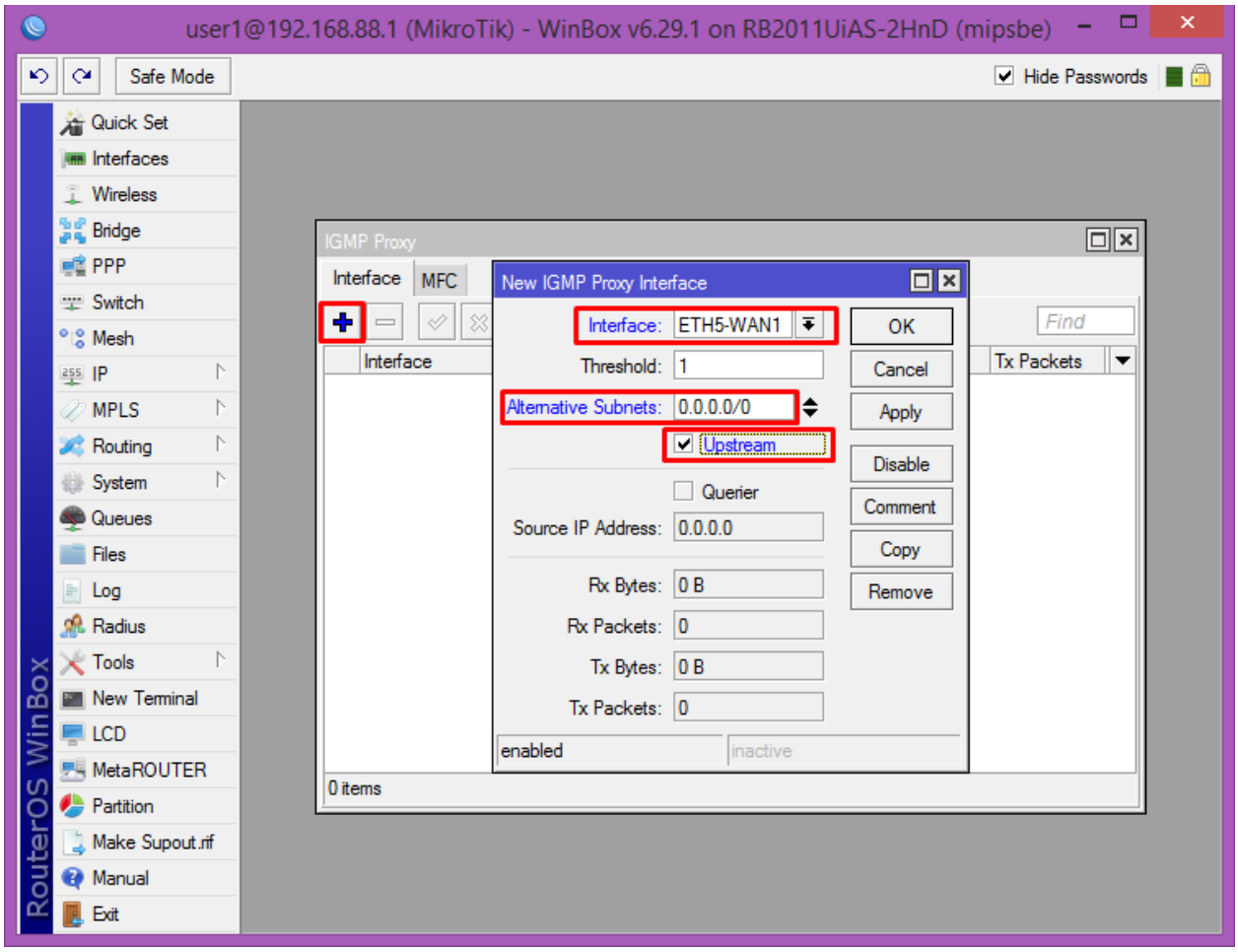
Изображение 60 – Переход к настройкам IGMP Proxy.

В открывшемся окне нажимаем на кнопку «Settings», ставим галочку рядом с «Quick Leave». Нажимаем на «OK» для сохранения настроек, изображение 61.



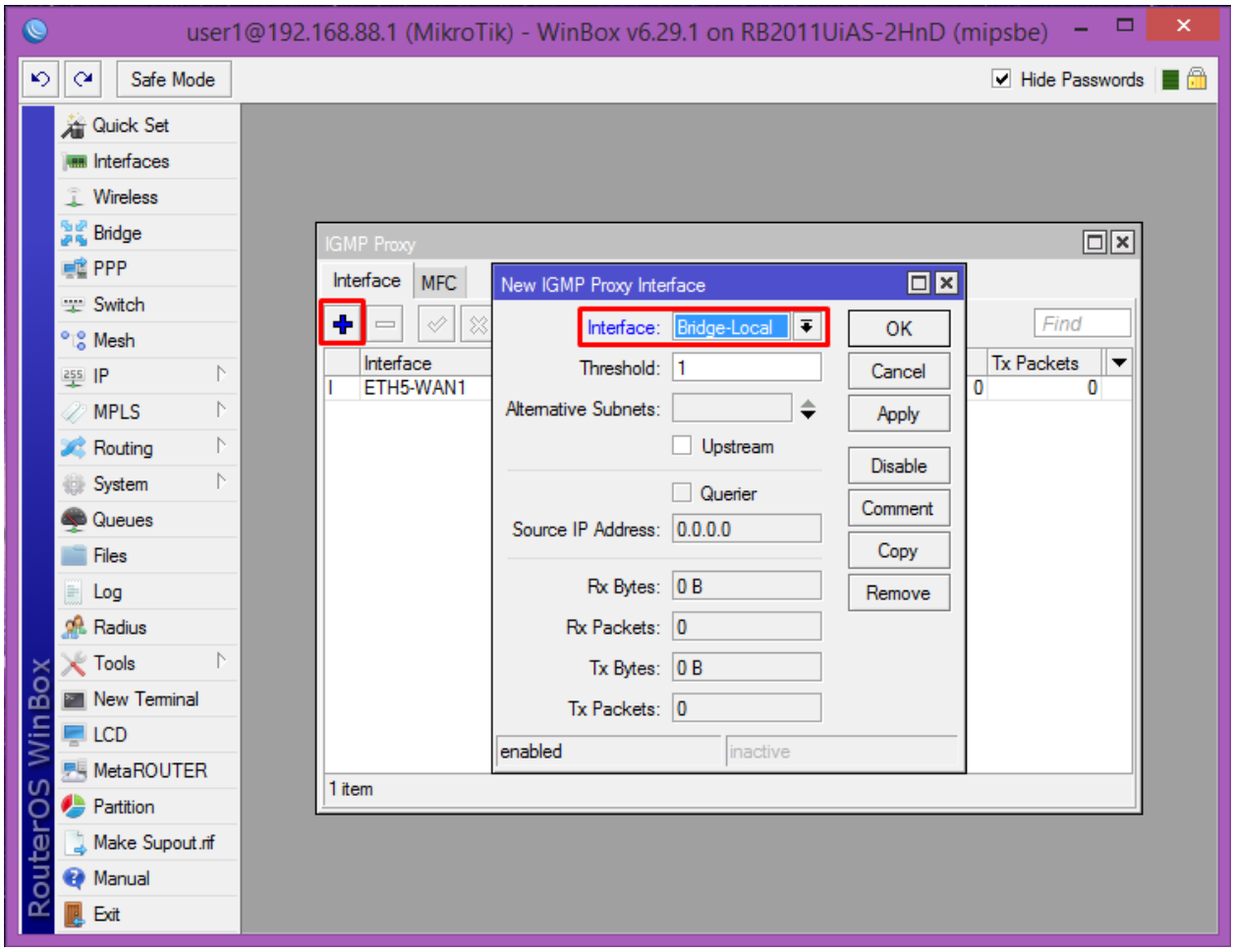
Изображение 61 – настройка функции Quick Leave.

Далее необходимо во вкладке «Interface» нажать на «+». «Interface» выбираем наш WAN-порт – «ETH5-WAN1», «Alternative Subnets» – 0.0.0.0/0 и ставим галочку рядом с «Upstream», изображение 62.



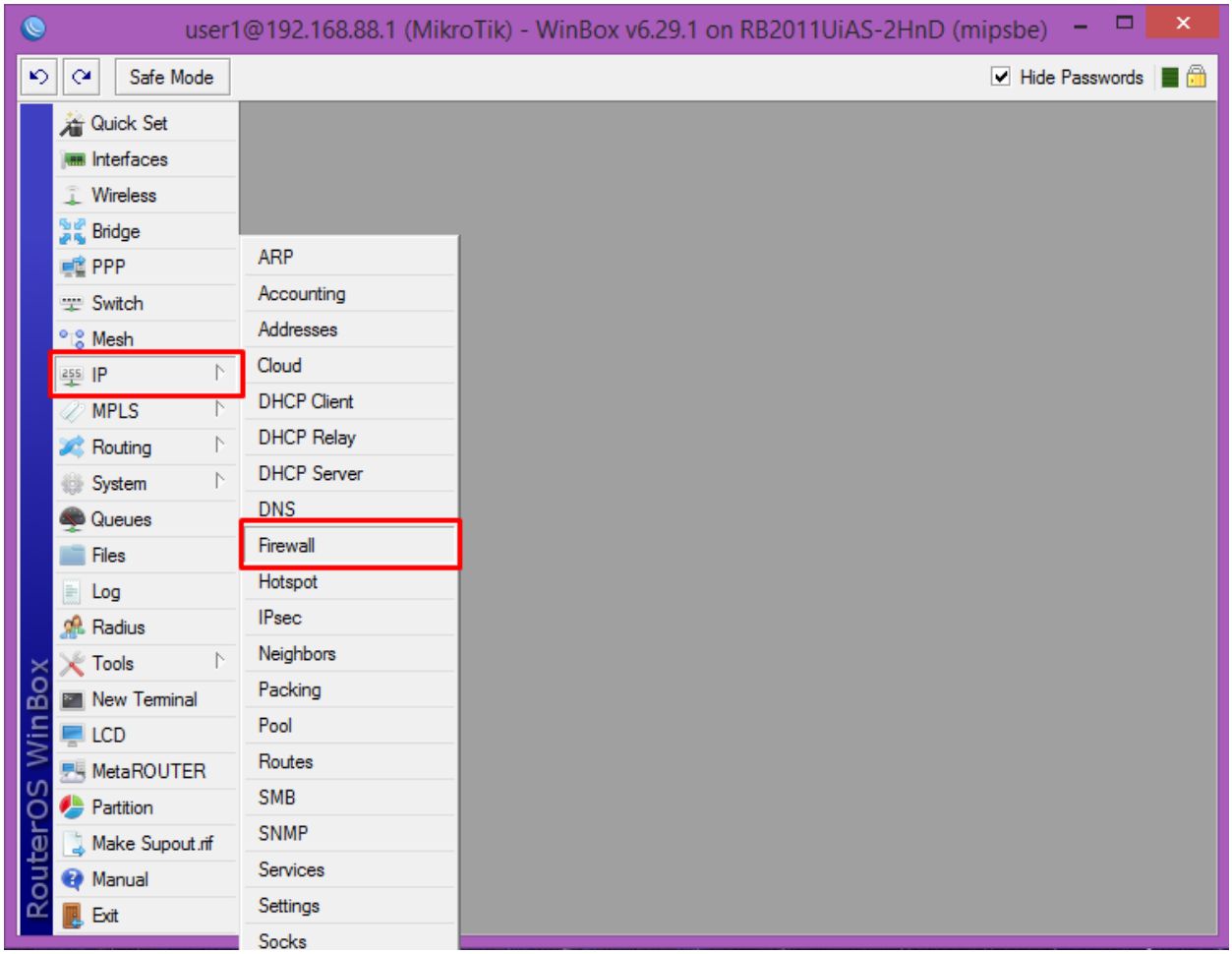
Изображение 62 – Настройка Upstream-интерфейса.

Нажимаем ещё раз на «+», «Interface» выбираем наш мост – «Bridge-Local», изображение 63.



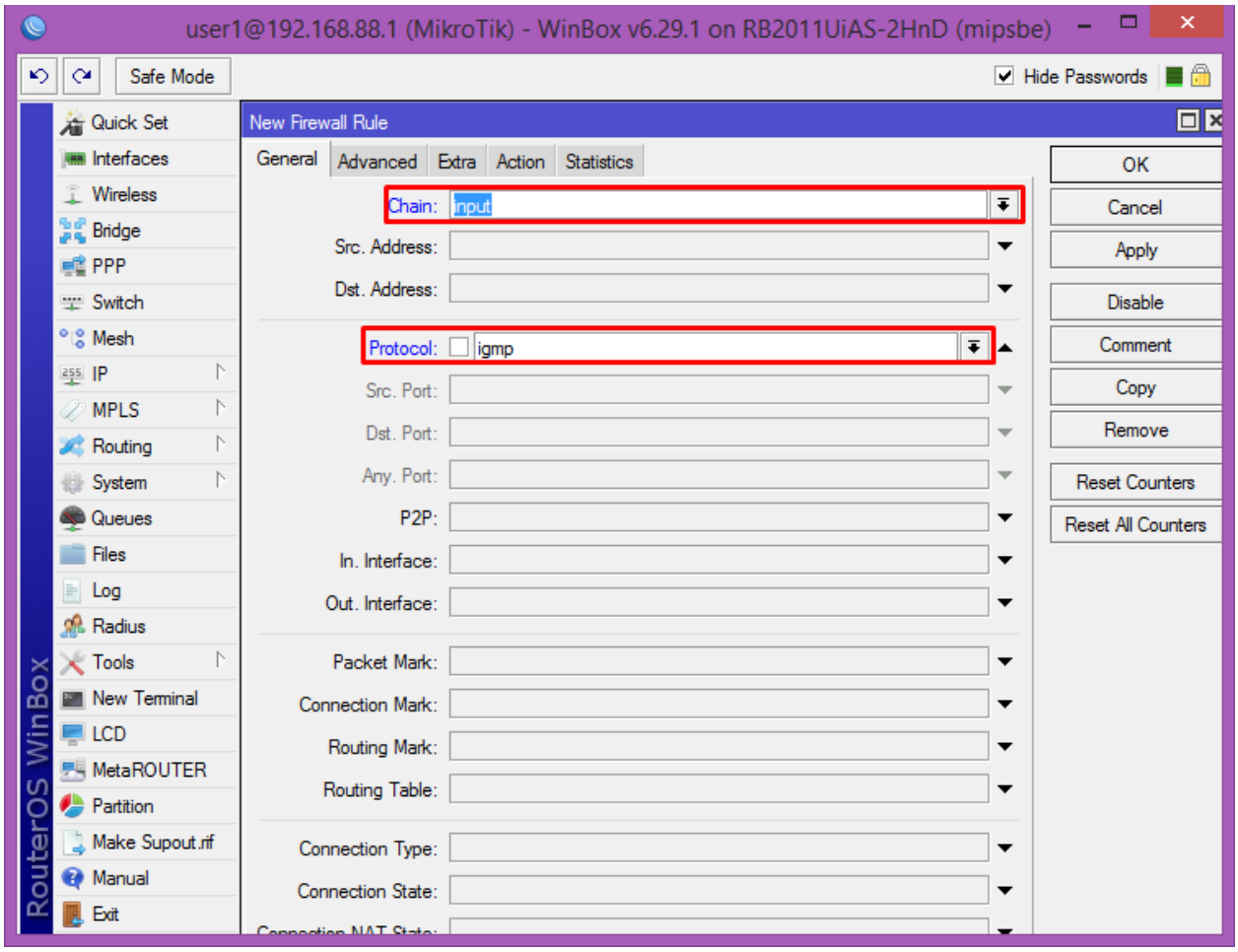
Изображение 63 – Настройка Downstream-интерфеса.

Далее перейдем к настройкам Firewall для разрешения IGMP-запросов. Переходим в раздел «IP» – «Firewall», изображения 64.

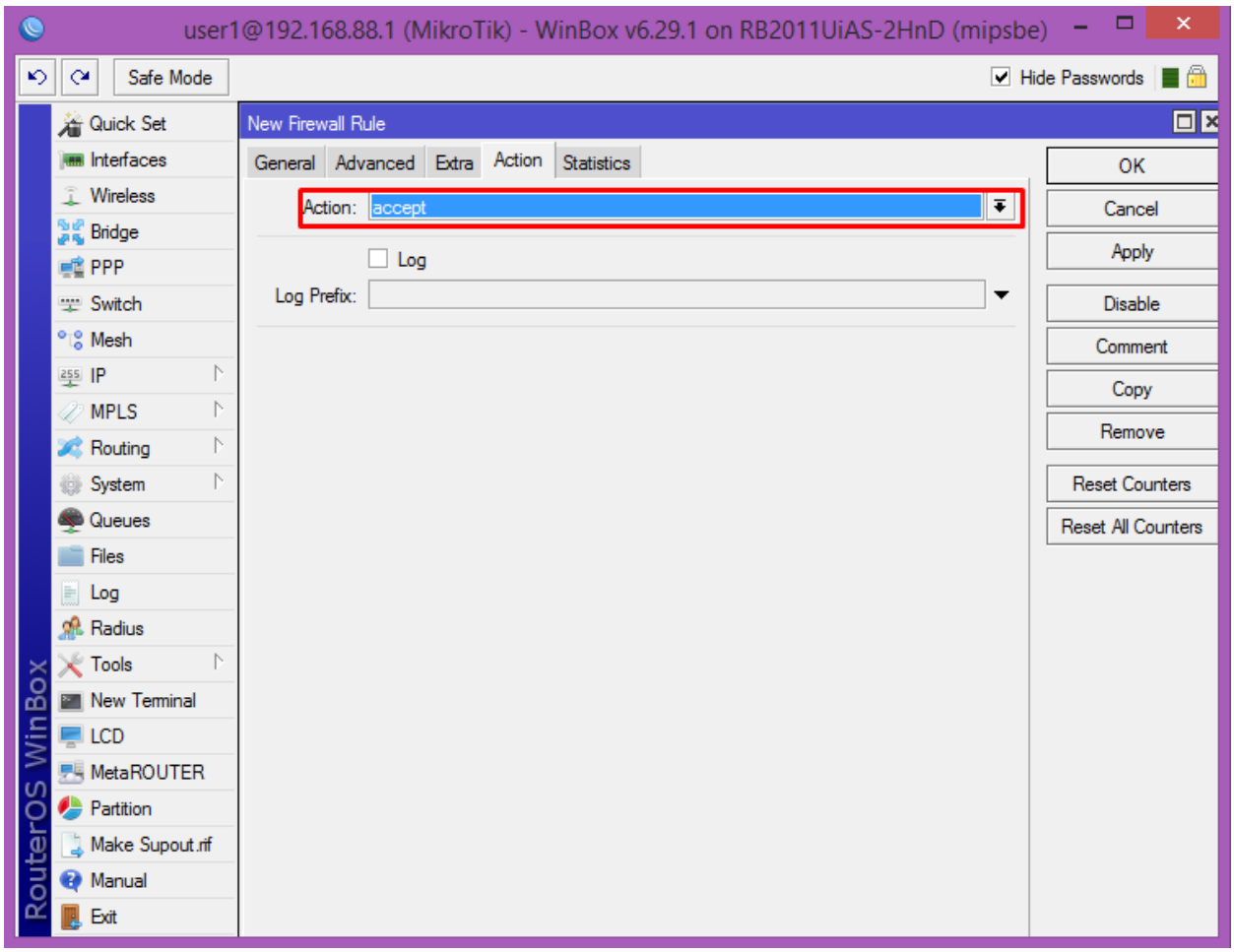


Изображение 64 – Переход к разделу Firewall.

Во вкладке «Filter Rules» нажимаем на «+». В открывшемся окне выбираем «Chain» – «input», «Protocol» – «igmp». Во вкладке «Action» в поле «Action» выставляем «accept», изображение 65 и 66.

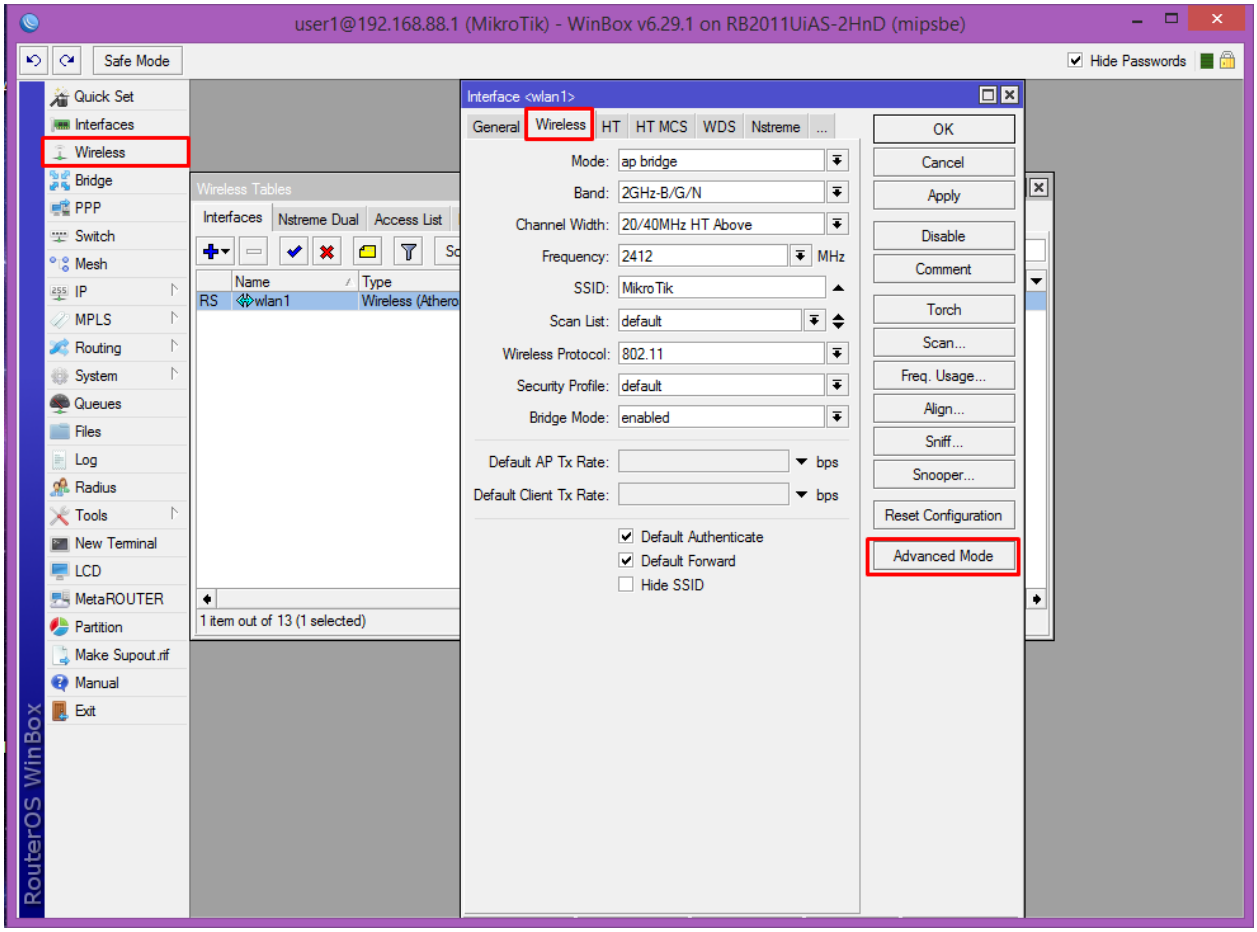


Изображение 65 – Настройка правила Firewall.

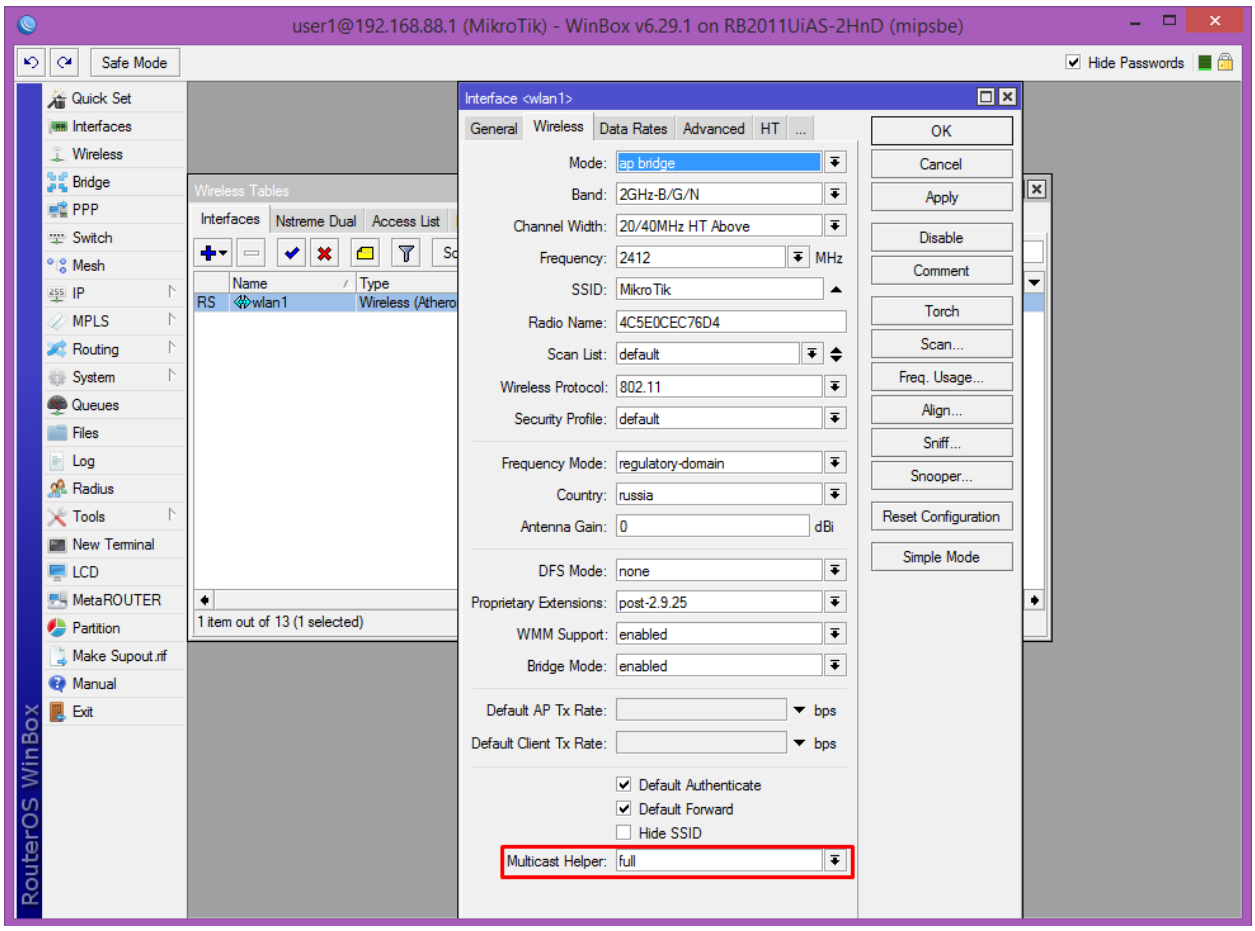


Изображение 66 – Настройка правила Firewall.

Для более качественной работы IPTV по беспроводной сети необходимо сделать следующее. Переходим в раздел «Wireless» и открываем наш интерфейс. Переходимо во вкладку «Wireless» и нажимаем на «Advance Mode». Далее в самом низу поле «Multicast Helper» выставляем в «full», изображение 67 и 68.



Изображение 67 – Настройка IPTV на беспроводной сети.

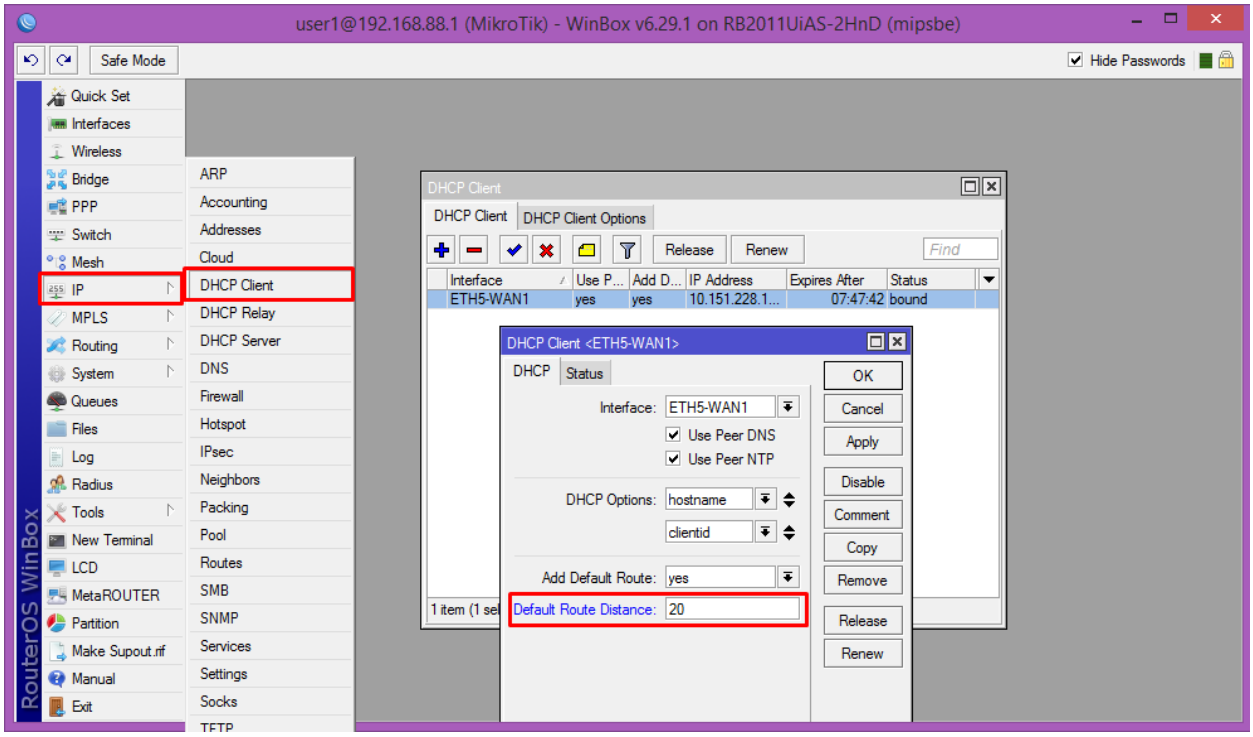


Изображение 68 – Настройка IPTV на беспроводной сети.

Настройка VPN-соединения

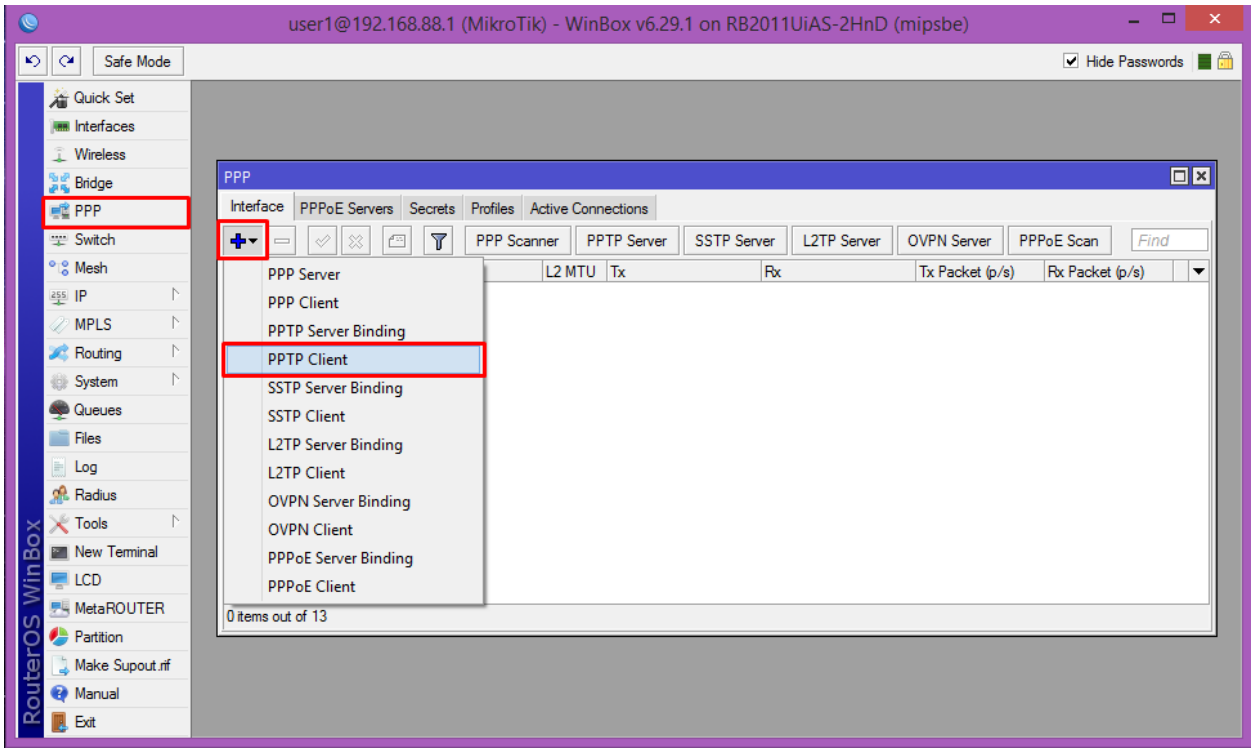
Перейдем к настройкам VPN-соединения. Здесь есть небольшая проблема в том, что маршрутизатор поддерживает только PPTP, а в сети POWERNET используется подключение типа PPTP Dual Access. Для этого необходимо будет произвести дополнительные настройки.

Для начала переходим в раздел «IP» – «DHCP Client», открываем наш WAN-интерфейс и в поле «Default Route Distance» выставляем значение, к примеру, «20». Это делается для того, чтобы наш маршрут при подключении по DHCP был запасной. То есть если VPN перестает работать, всё начинает работать по настройкам DHCP, если VPN поднимается, всё начинает работать через VPN, изображение 69.



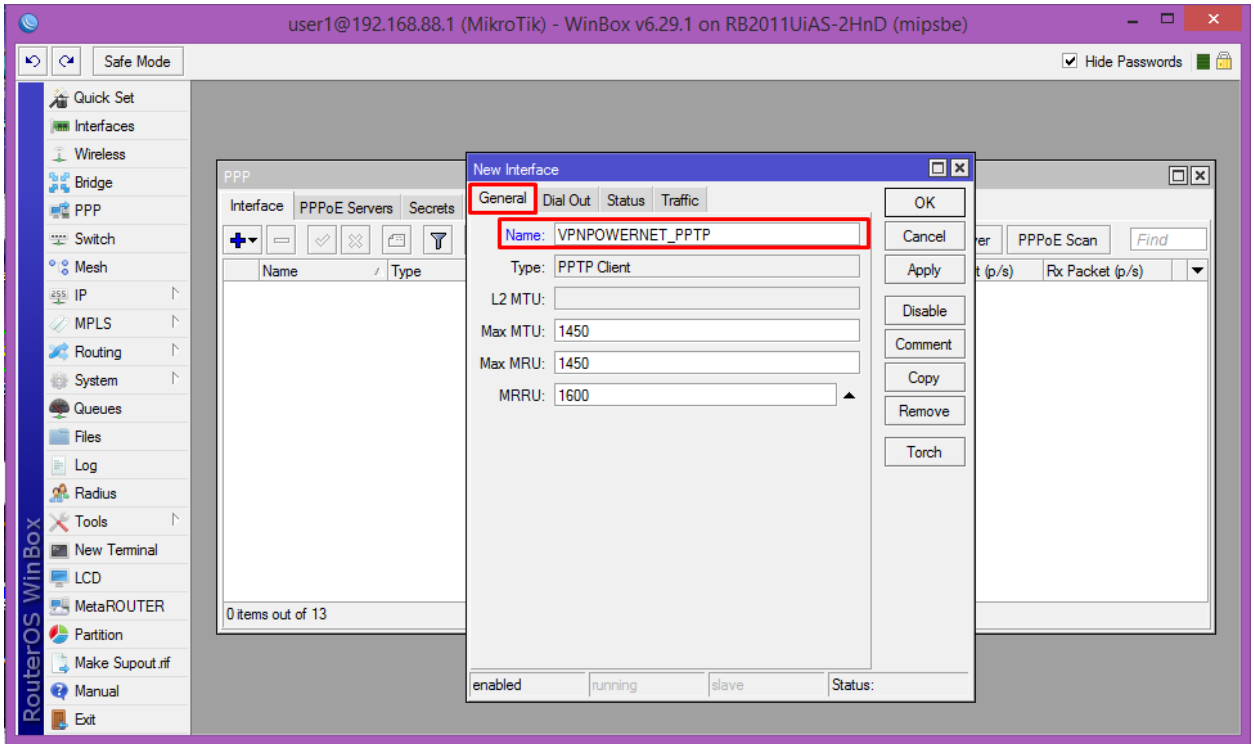
Изображение 69 – Настройка DHCP-клиента.

Далее переходим в раздел «PPP» и нажимаем на «+», выбираем «PPTP Client», изображение 70.

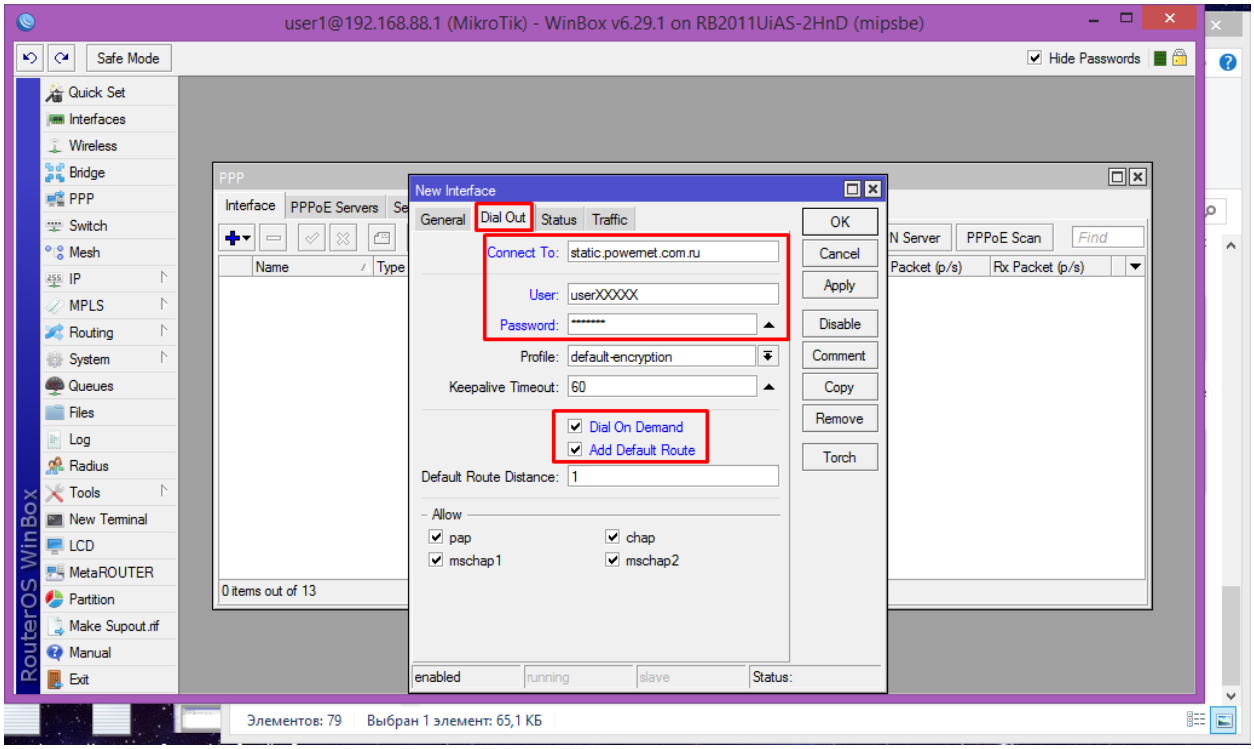


Изображение 70 – Создание PPTP-клиента.

Во вкладке «General» вводим имя нашего подключения, к примеру, «VPNPOWERNET_PPTP». Во вкладке «Dial Out» вводим данные для подключения. «Connect To» – «static.powernet.com.ru», «User» и «Password» – user-номер и пароль. Ставим галочки напротив «Dial On Demand» и «Add Default Route», «Default Route Distance» выбираем «1», изображение 71 и 72.

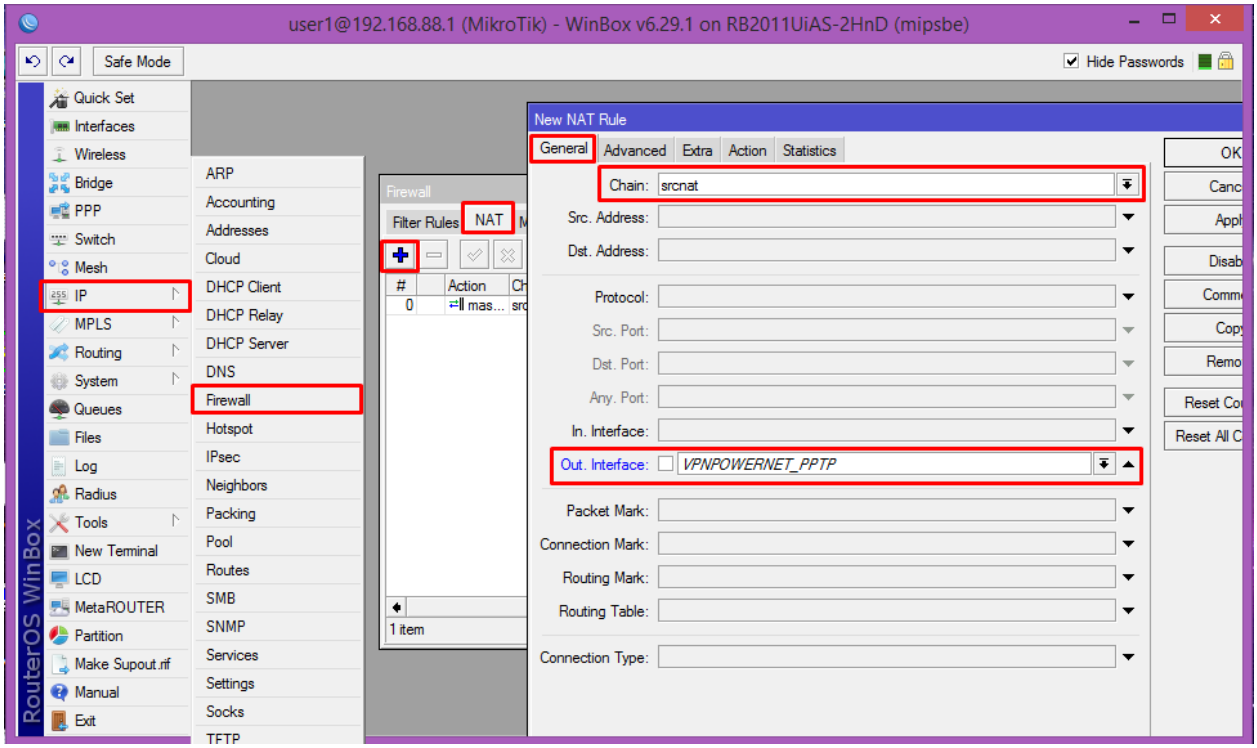


Изображение 71 – Настройка PPTP-клиента.



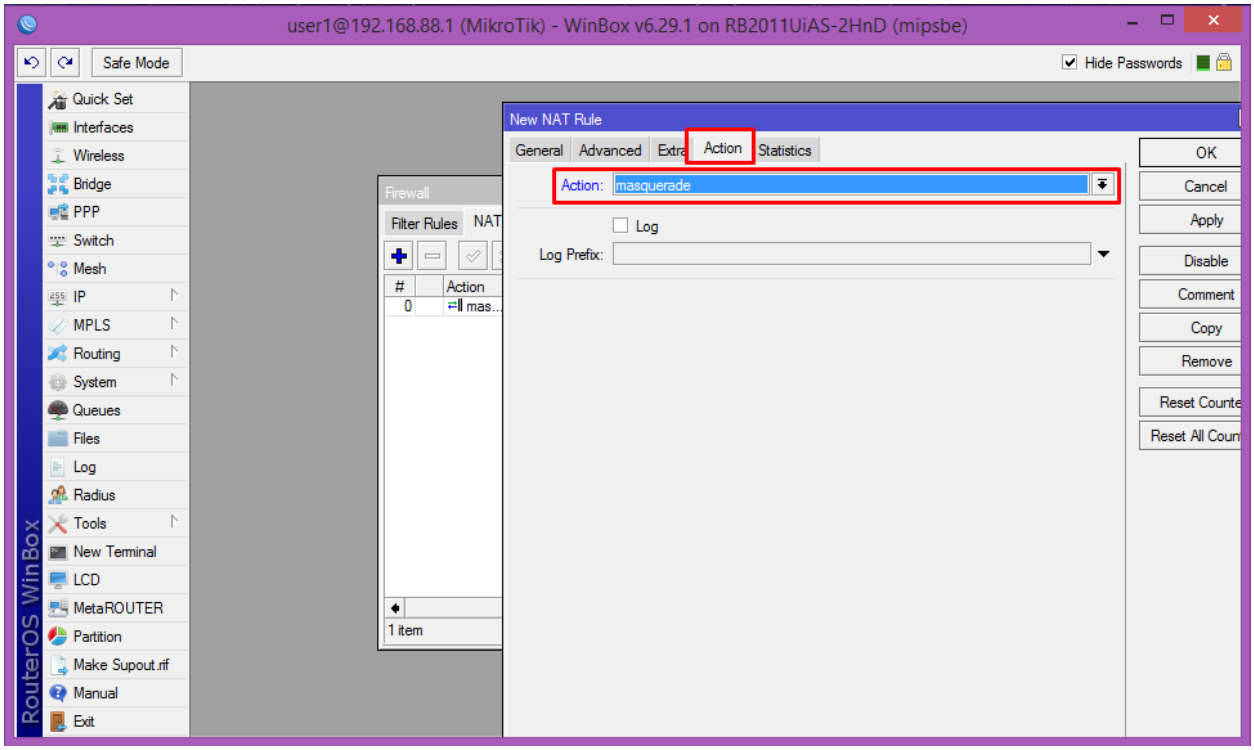
Изображение 72 – Настройка PPTP-клиента.

Далее переходим к настройкам NAT для нашего VPN-соединения. Переходимо в раздел «IP» – «Firewall», во вкладке «NAT» нажимаем на «+». Во вкладке «General» в поле «Chain» выбираем «srcnat», «Out Interface» выбираем наше VPN-соединение, в данном случае «VPNPOWERNET_PPTP», изображение 73.



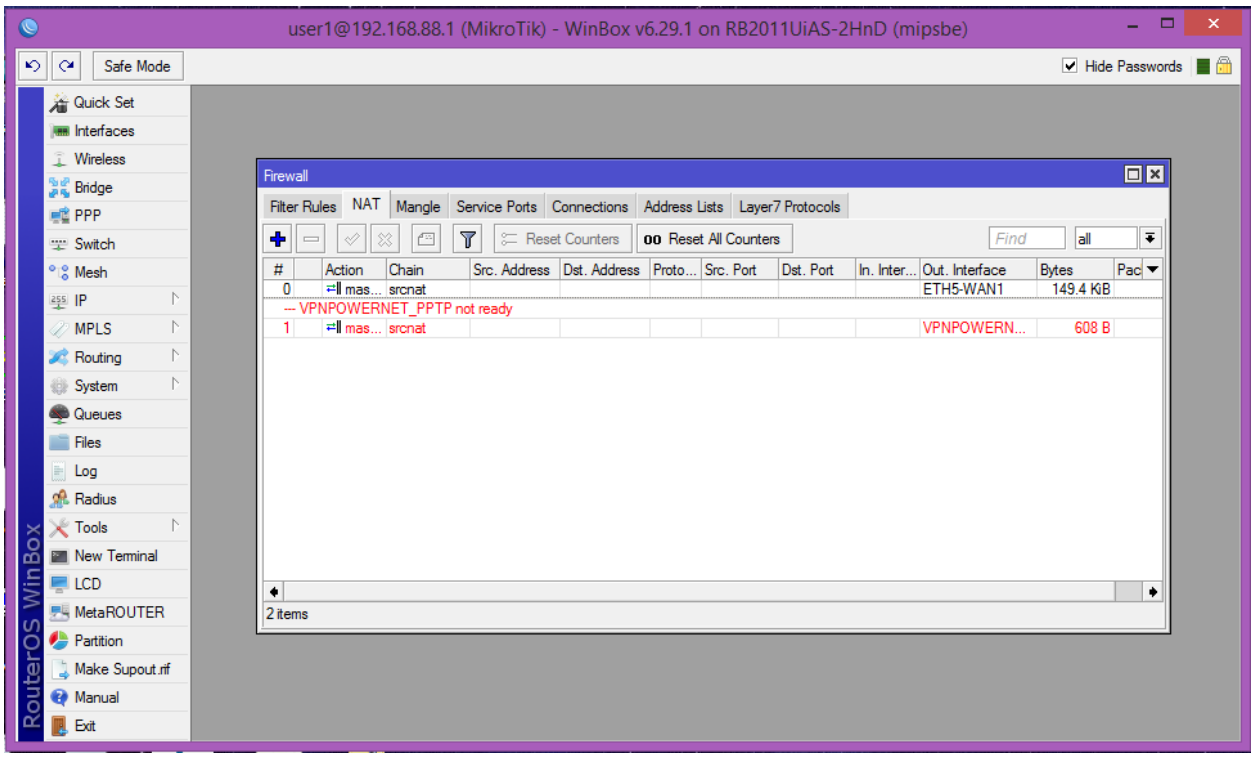
Изображение 73 – Настройка NAT для VPN-соединения.

Во вкладке «Action» в поле «Action» выбираем «masquerade», изображение 74.



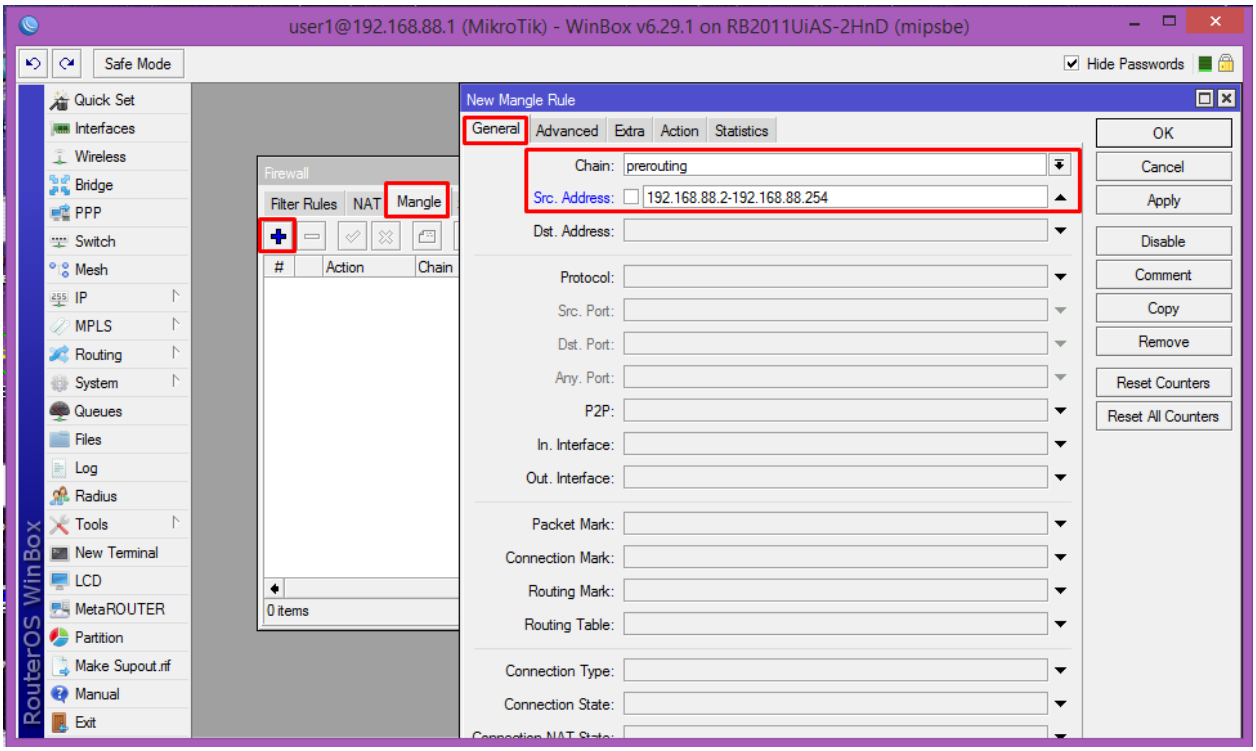
Изображение 74 – Настройка NAT для VPN-соединения.

После этого маршрутизатор выделит нашу настройку красным – это связано из-за того, что VPN-соединение ещё не до конца настроено, изображение 75.



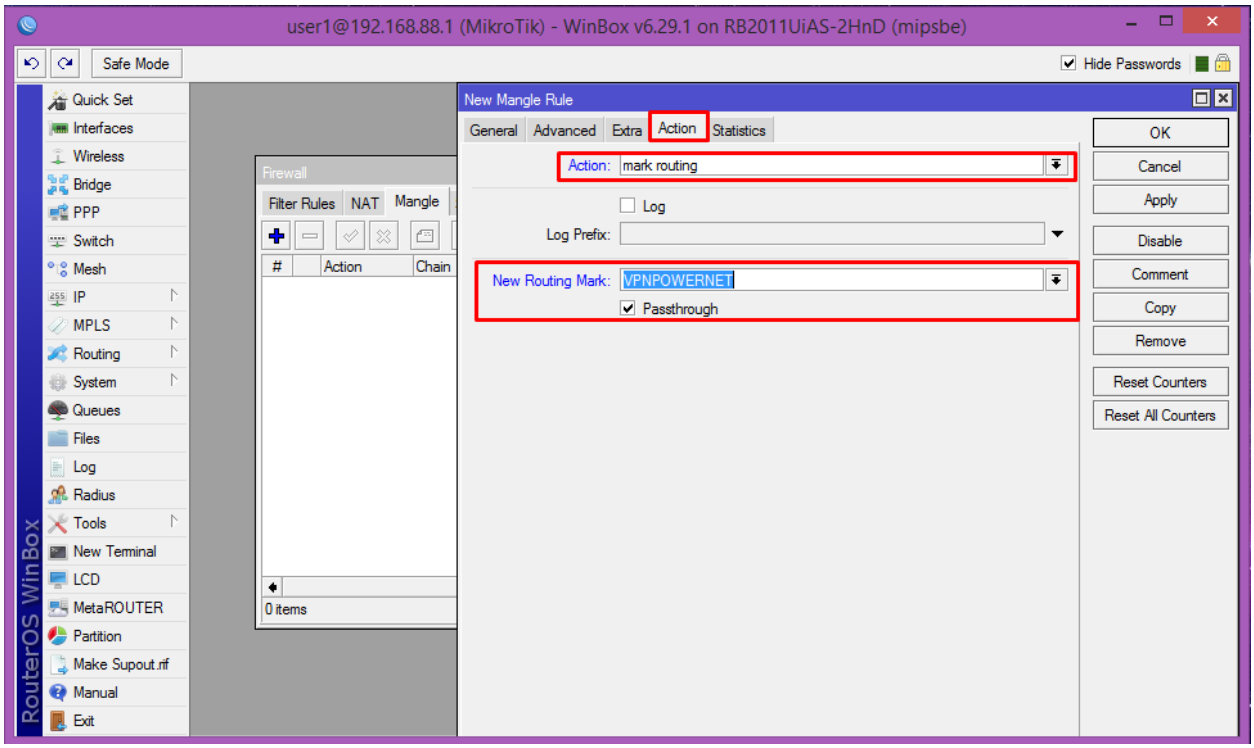
Изображение 75 – Отображение настройки NAT для VPN-соединения.

Далее необходимо создать маркировку трафика. В этом же разделе «Firewall» переходим во вкладку «Mangle» и нажимаем на «+». Во вкладке «General» в поле «Chain» выбираем «prerouting», «Src. Address» - «192.168.88.2-192.162.88.254», то есть пул наших адресов, изображение 76.



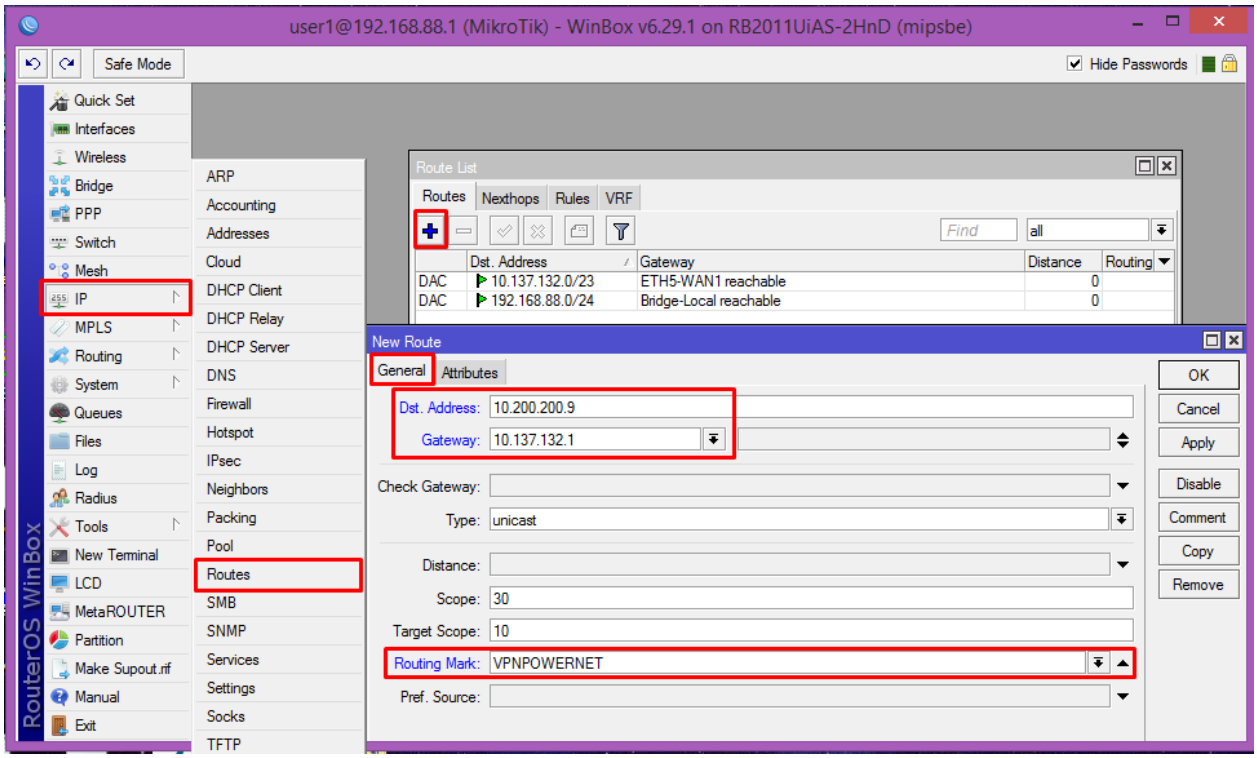
Изображение 76 – Настройка маркировки трафика.

Во вкладке «Action» в поле «Action» выбираем «mark routing», в поле «New Routing Mark» придумываем название, к примеру, «VPNPOWERNET», ставим галочку рядом с «Passthrough», изображение 77.



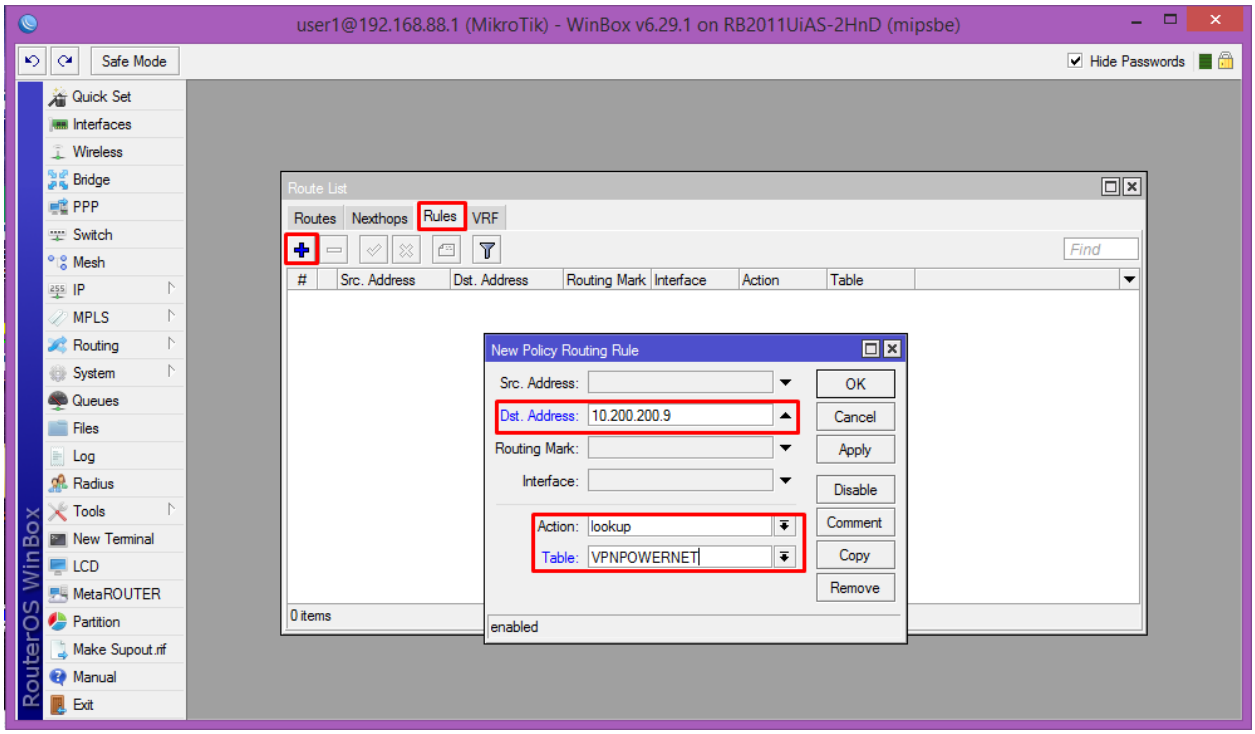
Изображение 77 – Настройка маркировки трафика.

Теперь необходимо создать статически маршрут до VPN-сервера. Переходим в раздел «IP» – «Routes», во вкладке «Routes» нажимаем на «+». В открывшемся окне во вкладке «General» в поле «Dst. Address» вписываем адрес VPN-сервера, с нашем случае – «10.200.200.9». В поле «Gateway» необходимо указать шлюз. В поле «Routing Mark» выбираем имя, которое мы придумали для маркировки трафика, то есть «VPNPOWERNET», изображение 78.



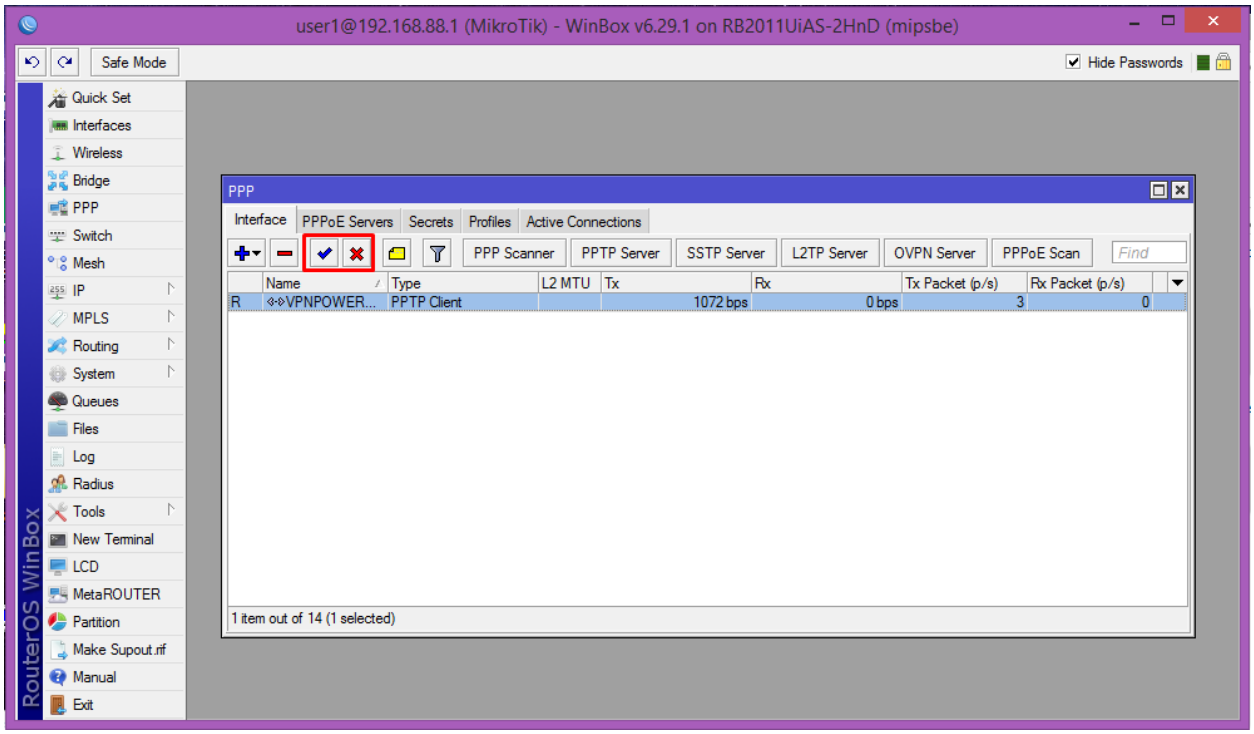
Изображение 78 – Добавление маршрута.

Дополнительно необходимо создать правило. Переходим во вкладку «Rules», нажимаем на «+». В открывшемся окне напротив «Dst. Address» указываем «10.200.200.9» (адрес VPN-сервера), «Action» выбираем «lookup», «Table» – «VPNPOWERNET» (имя для маркировки трафика), изображение 79.

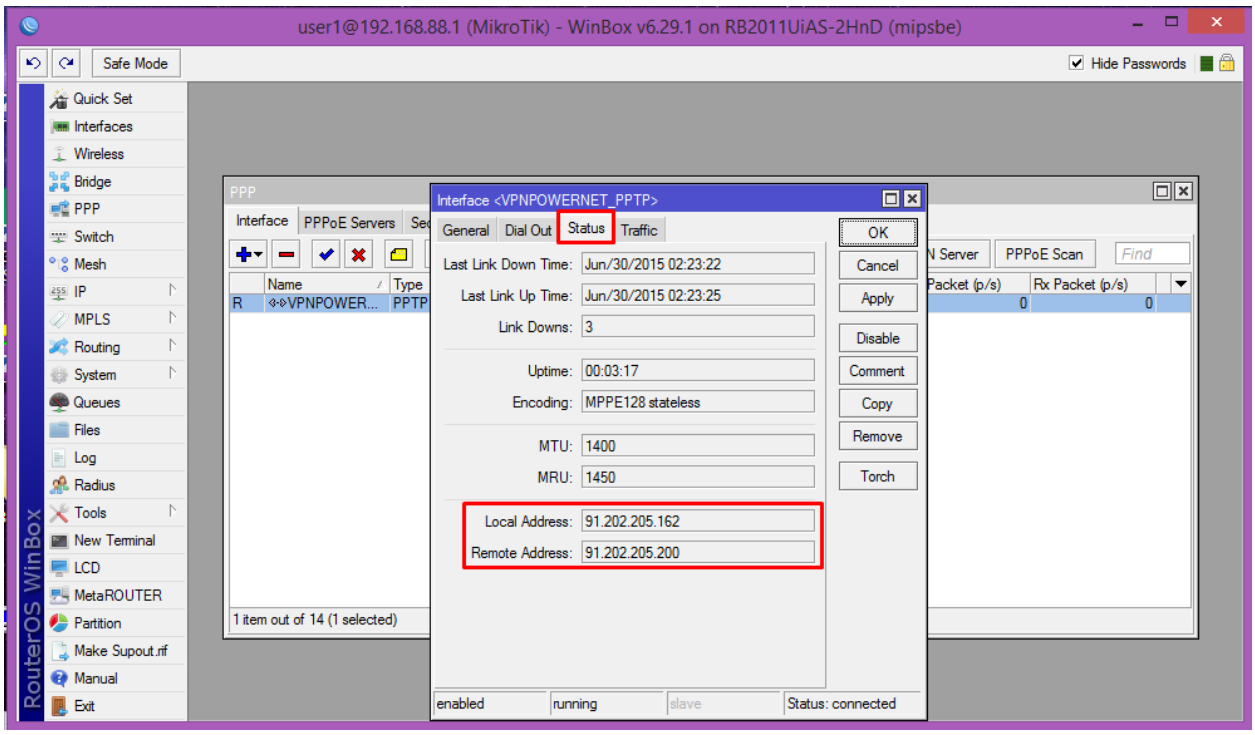


Изображение 79 – Настройка правила для маршрута.

Для проверки работоспособности переходим в раздел «PPP», с помощью значка «крест» можно временно отключить наше VPN-соединения. После отключения автоматически начинает работать Интернет с помощью настроек DHCP. Нажимаем на «галочку» – VPN-соединение включается. Нажимаем на него 2 раза и переходим во вкладку «Status». Здесь видим, что наше соединение успешно установилось, «Local Address» – наш внешний адрес в Интернете, «Remote Address» – внешний адрес VPN-сервера, изображения 80 и 81.



Изображение 80 – Проверка работоспособности VPN-соединения.



Изображение 81 – Проверка работоспособности VPN-соединения.

Может возникнуть проблема, что VPN-соединение работает, но некоторые страницы не открываются. Для этого необходимо в настройках PPTP-клиента, изображение 71, поменять значения «Max MTU» и «Max MRU», к примеру, выставить в «1400».