

?????????? ??????????? MikroTik RouterOS

?????????? ???????????

?????? ??????????

??? ??? ??????????????

- MikroTik роутер
- Компьютер с Ethernet-портом (желательно), но настройка через WiFi также возможна, если устройство имеет встроенную точку доступа WiFi
- Ethernet-кабель
- Интернет-соединение от вашего интернет-провайдера (ISP)
- 30-60 минут непрерывного времени

?????????? ??????????

Стандартная конфигурация: Предварительно загруженные настройки, которые могут не подходить под ваши нужды

Мост (Bridge): Виртуальный интерфейс, который соединяет несколько физических портов

ДНСР: Автоматическое присвоение IP-адресов устройствам

NAT: Трансляция сетевых адресов — позволяет нескольким устройствам использовать одно интернет-соединение

Брандмауэр: Правила безопасности, контролирующие сетевой трафик

?????????? ?????? ?????????????

В этом руководстве показаны оба метода: WinBox (графический) и CLI (текстовый).

Новички: Следуйте инструкциям WinBox

Продвинутые пользователи: Используйте команды CLI (представлены в блоках кода)

?????? ????????????? ????????

Это руководство поможет вам шаг за шагом настроить ваш MikroTik роутер:

- **Подключение:** Физическое подключение и доступ через WinBox
- **Оценка:** Работа с существующей или изменённой конфигурацией
- **Интернет:** Получение доступа в интернет
- **Локальная сеть:** Настройка IP-адресов и DHCP
- **NAT:** Позволяет устройствам использовать одно интернет-соединение
- **Безопасность:** Защита роутера и сети
- **Беспроводная сеть:** Настройка WiFi (если применимо)
- **Тестирование:** Проверка работоспособности

Каждый шаг строится на предыдущем. Выполняйте их по порядку для достижения наилучших результатов.

?????: ?????????? ??????????

После каждого крупного раздела делайте резервную копию вашей конфигурации:

CLI метод:

```
/export file=backup-step3
```

WinBox метод:

- Меню Файлы → Backup
- Назовите файл понятно (например, "after-internet-setup")
- Нажмите Backup

Если что-то пойдёт не так, вы сможете восстановить конфигурацию: Файлы → Выберите файл резервной копии → Restore...

????????????? ? ?????????

Большинство MikroTik роутеров поставляются с предустановленной конфигурацией, и вы можете использовать этот раздел для подключения к ним. Исключение — профессиональные устройства серии CCR, для них используйте следующий раздел.

??? 1: ?????????? ??????????????

- Подключите Ethernet-кабель от вашего компьютера к любому порту, кроме ether1 на роутере MikroTik
- Подключите интернет-кабель к порту ether1 (это будет ваш WAN/интернет-порт)
- Включите роутер и подождите минуту для полной загрузки

??? 2: ????????? WinBox

Если у вас нет WinBox:

- Перейдите на mikrotik.com/download

- Скачайте WinBox (подходит для Windows, macOS 12 или новее, Linux)
- Запустите winbox.exe (установка не требуется)

??? 3: ?????? ???????? ? ???????? ?????????????? ???????? (Neighbor Discovery)

- Откройте WinBox
- Нажмите кнопку "..." рядом с полем "Connect To:"
- Ваш роутер должен появиться во вкладке "Neighbors"
- Двойным щелчком выберите IP адрес роутера для подключения (если IP адрес 0.0.0.0 и подключение не работает, попробуйте дважды щелкнуть MAC-адрес)
- Имя пользователя: admin, пароль оставьте пустым или проверьте наклейку на устройстве

??? 4: ?????????? ?????????????? ???????????????

При первом подключении может появиться всплывающее окно о стандартной конфигурации:

- **Для начинающих:** Сохраните стандартную конфигурацию — она обеспечивает базовую безопасность и функциональность
- **Стандартная настройка включает:** Основные правила брандмауэра, DHCP сервер и защиту беспроводной сети
- **Вы можете ее безопасно настроить**, следуя этому руководству, не удаляя стандартных настроек

Удаление стандартной конфигурации уберет все правила безопасности. Делать это должны только опытные пользователи.

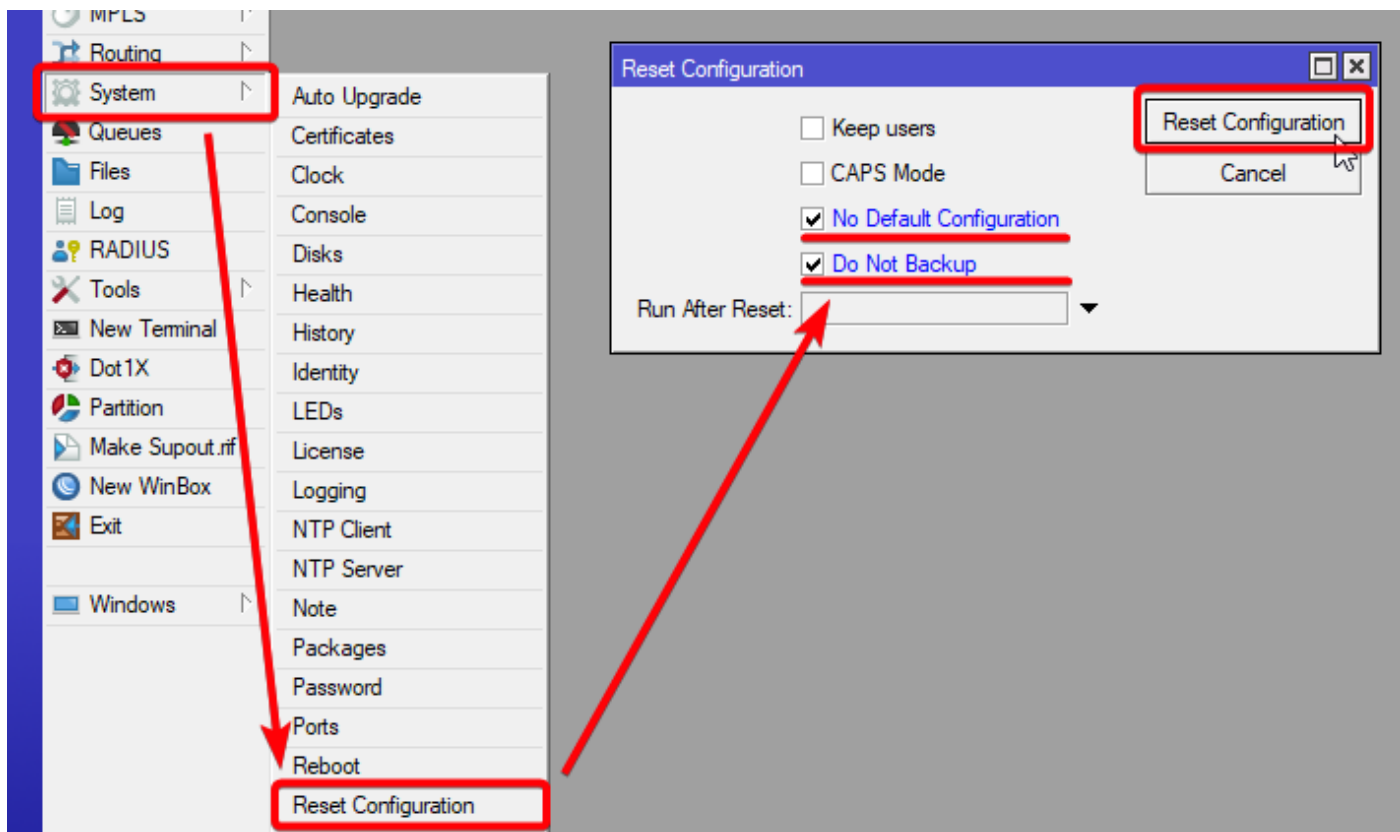
??????? ??? ?????????????? ???????????????? (??????? ??? ??????????????? ??????????????????)

Если роутер не имеет стандартной конфигурации, есть несколько вариантов. Мы выберем метод, который лучше всего подходит для наших требований. Подключите интернет-кабель к порту ether1 роутера и ПК к любому порту, кроме ether1. Запустите WinBox и найдите роутер через обнаружение соседей. Если роутер появится в списке, выберите его MAC-адрес и нажмите **Connect**.

Самый простой способ убедиться, что роутер чист, — выполнить в CLI команду:

```
/system reset-configuration no-defaults=yes skip-backup=yes
```

Или из WinBox:



????????? IP ????????

Поскольку MAC-соединение иногда бывает нестабильным, первым делом настройте роутер для IP-соединения:

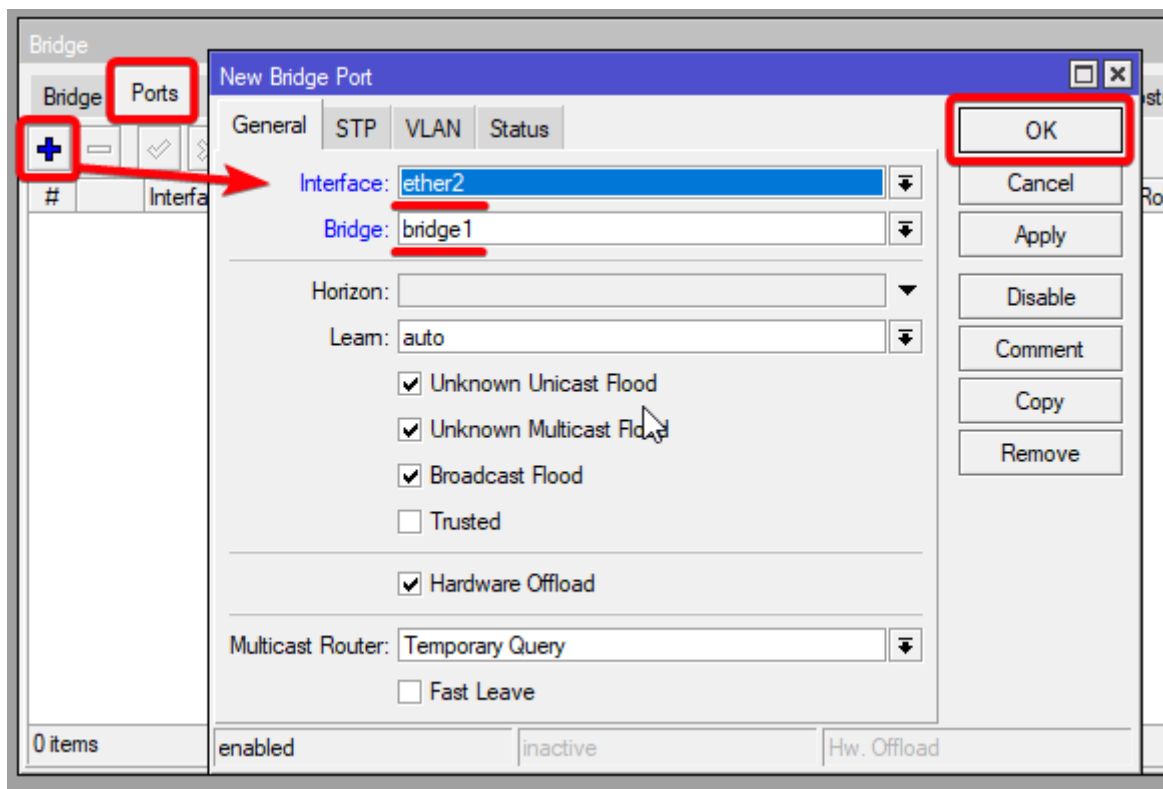
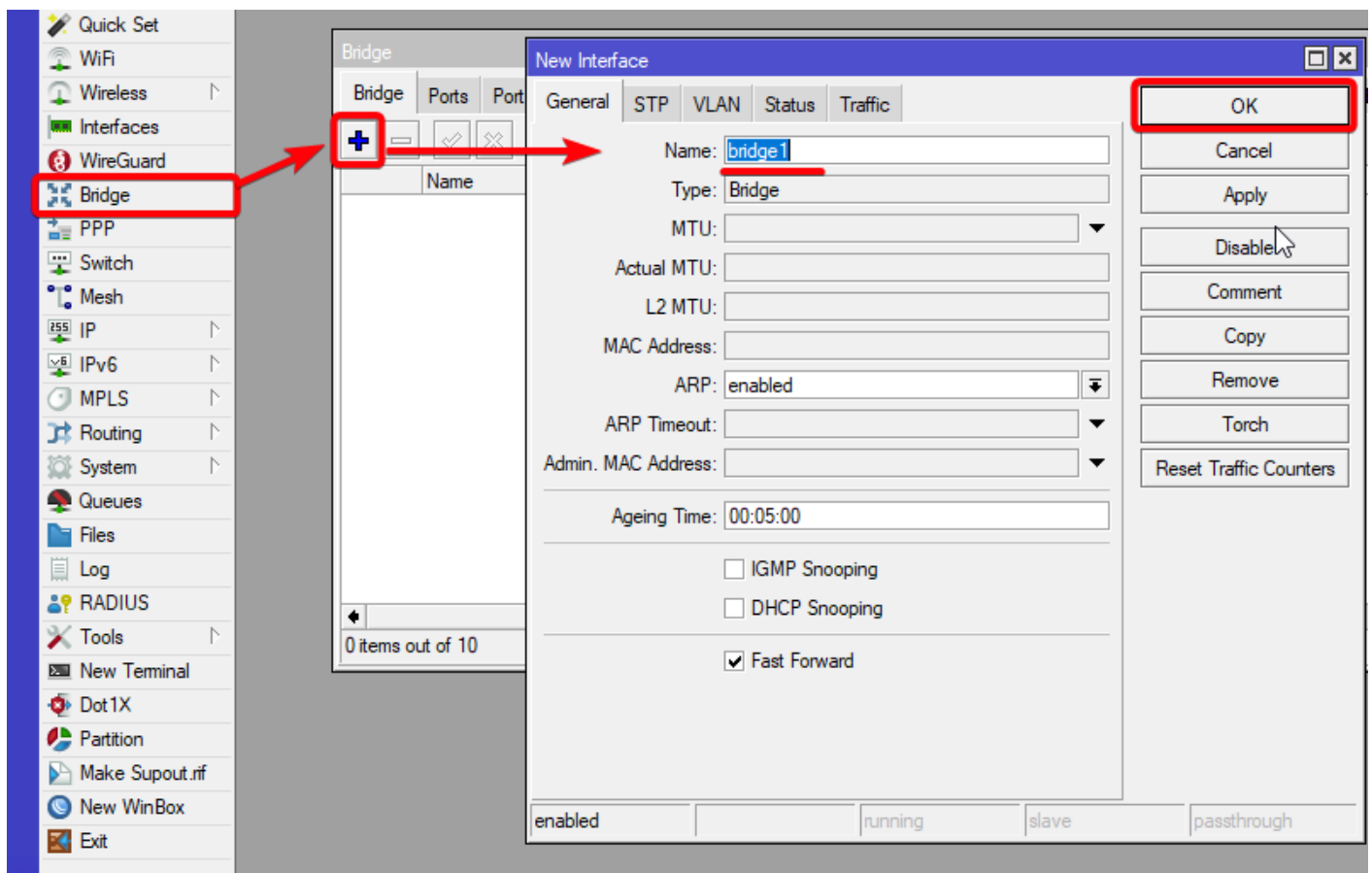
- Создайте мост (bridge) и добавьте к нему порты;
- Назначьте IP-адрес мостовому интерфейсу;
- Настройте DHCP сервер.

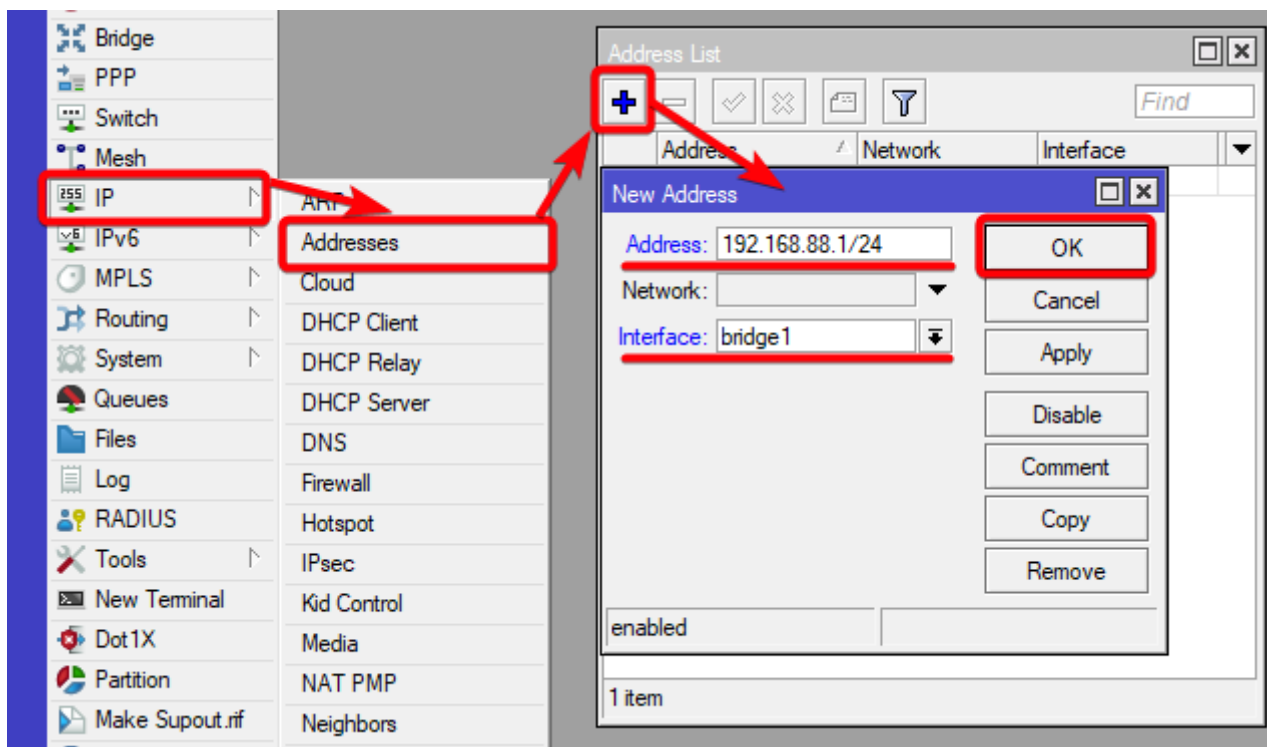
Настройка моста и IP-адреса — простая процедура:

```
/interface bridge add name=bridge1
/interface bridge port add interface=ether2 bridge=bridge1
/ip address add address=192.168.88.1/24 interface=bridge1
```

Если вы предпочитаете использовать WinBox/WebFig:

- Откройте окно **Bridge**, вкладка **Bridge** должна быть активна;
- Нажмите кнопку **+**, чтобы открыть диалог создания; введите имя моста или оставьте *bridge1*, нажмите **OK**;
- Перейдите на вкладку **Ports**, нажмите **+**; выберите интерфейс *ether2* и мост *bridge1*, затем **OK**;
- Закройте диалог моста;
- Перейдите в меню **IP → Addresses**;
Нажмите **+**, введите IP-адрес *192.168.88.1/24*, выберите интерфейс *bridge1*, нажмите **OK**.





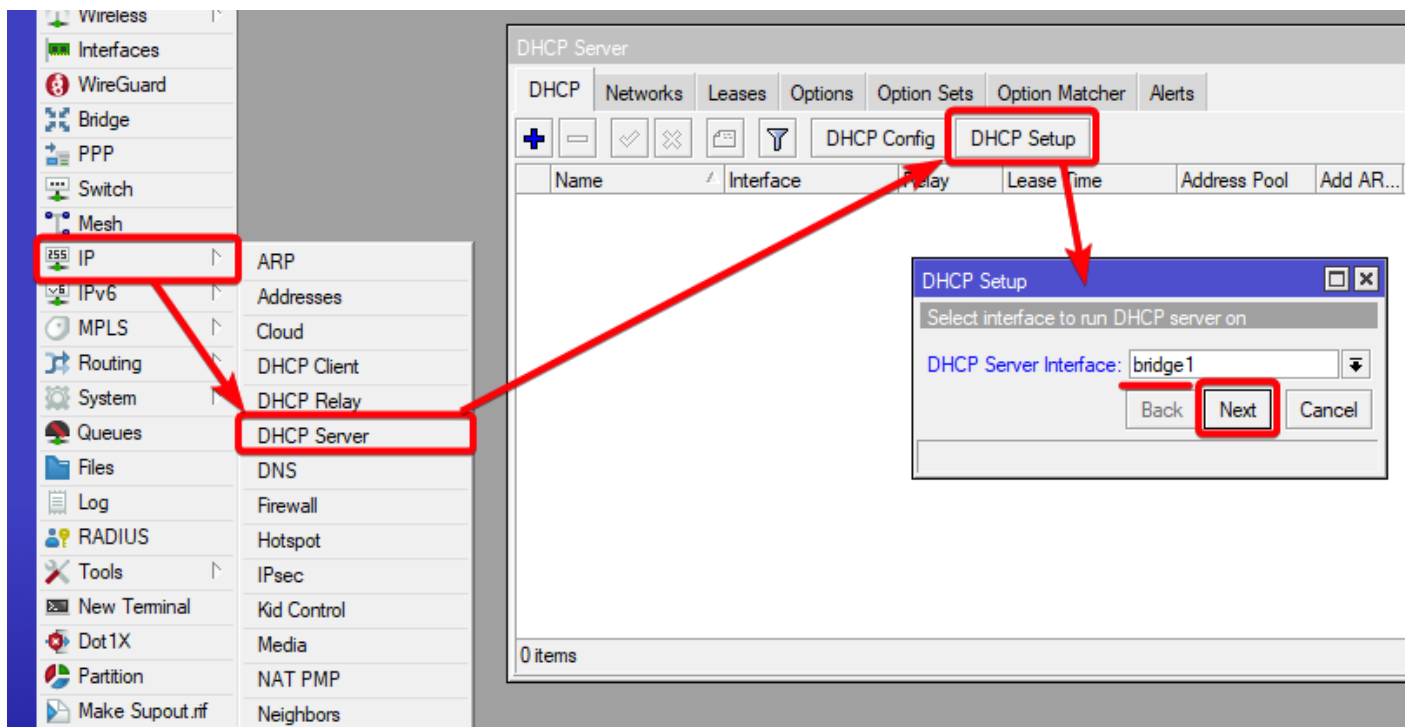
Далее перейдите к настройке DHCP сервера. Для простоты выполните команду `setup`:

```
[admin@MikroTik] > ip dhcp-server setup
Select interface to run DHCP server on dhcp server interface: bridge1
Select network for DHCP addresses dhcp address space: 192.168.88.0/24
Select gateway for given network gateway for dhcp network: 192.168.88.1
Select pool of ip addresses given out by DHCP server addresses to give out: 192.168.88.2-192.168.88.254
Select DNS servers dns servers: 192.168.88.1
Select lease time lease time: 1800
```

Обратите внимание: большинство параметров определяется автоматически, просто нажимайте Enter.

Инструмент настройки также доступен в WinBox/WebFig:

- Перейдите в окно **IP → DHCP Server**, убедитесь, что активна вкладка **DHCP**;
- Нажмите кнопку **DHCP Setup**;
- Выберите *bridge1* как интерфейс DHCP сервера, продолжите настройку по мастеру.



После этого, подключенный ПК должен получить динамический IP-адрес. Можно закрыть WinBox и переподключиться к роутеру по IP-адресу *192.168.88.1*.

????????? ?????????????? ? ???????????

Для выхода в Интернет необходимо определить, какой тип подключения вам нужен:

- **DHCP/Dynamic IP:** Большинство кабельных модемов, часть оптоволоконных подключений. Просто подключаете кабель и получаете интернет автоматически.
- **Static IP:** Для бизнес-подключений и некоторых домашних оптоволоконных подключений. Провайдер предоставляет фиксированный IP, шлюз и DNS.
- **PPPoE:** DSL и некоторые оптоволоконные провайдеры. Провайдер даёт логин и пароль для подключения.

Если не уверены, выбирайте DHCP — он подходит примерно для 80% домашних подключений.

????? A: DHCP (????? ??????????????????????)

Это самый простой и популярный способ настройки в домашних сетях. Добавьте DHCP-клиента на интерфейс, подключённый к интернету:

```
/ip dhcp-client add disabled=no interface=ether1
```

После добавления клиента вы должны увидеть назначенный IP-адрес и его статус bound:

```
[admin@MikroTik] > ip dhcp-client print
Columns: INTERFACE, USE-PEER-DNS, ADD-DEFAULT-ROUTE, STATUS, ADDRESS
```

```
# INTERFACE USE-PEER-DNS ADD-DEFAULT-ROUTE STATUS ADDRESS
0 ether1 yes yes bound 1.2.3.100/24
```

????? B: ????????????? IP

Если провайдер выдал фиксированные параметры, например:

- IP: 1.2.3.100/24
- Шлюз: 1.2.3.1
- DNS: 8.8.8.8

Настроить их в RouterOS вручную:

```
/ip address add address=1.2.3.100/24 interface=ether1
/ip route add gateway=1.2.3.1
/ip dns set servers=8.8.8.8
```

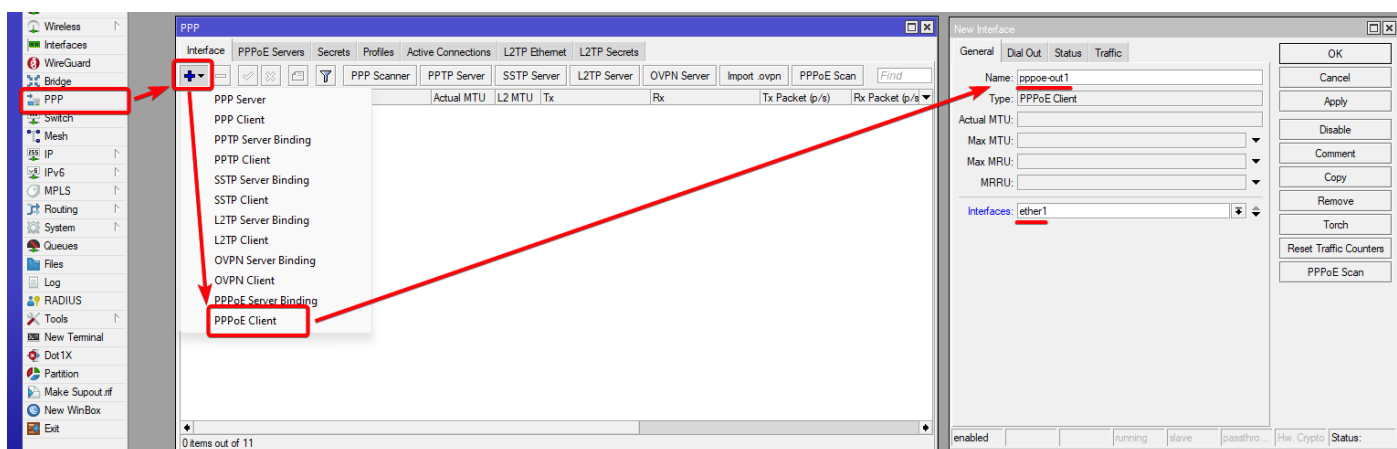
????? C: PPPoE ?????????????

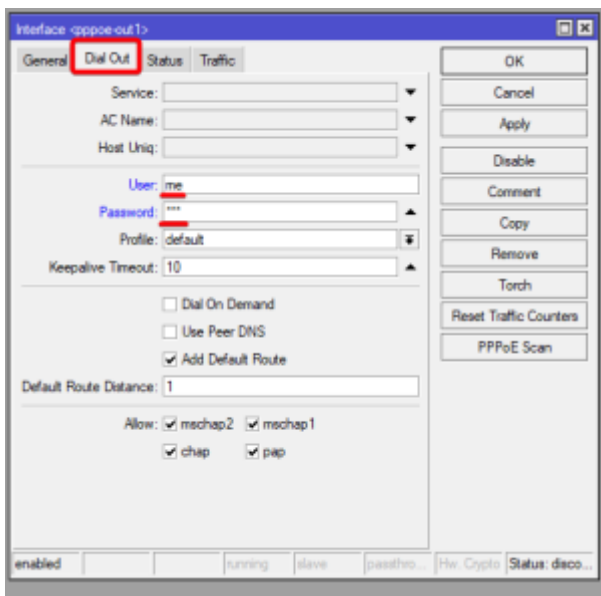
PPPoE обычно динамически назначает IP, DNS и маршрут. Провайдер даёт логин и пароль:

```
/interface pppoe-client add disabled=no interface=ether1 user=me password=123 \
add-default-route=yes use-peer-dns=yes
```

В WinBox/WebFig:

- В окне **PPP** выберите вкладку **Interfaces** и нажмите "+";
- Выберите **PPPoE Client**;
- Назначьте имя и интерфейс *ether1*;
- Перейдите на вкладку **Dial Out**, введите логин, пароль и другие параметры;
- Нажмите **OK** для сохранения.





Теперь WAN-интерфейс — *pppoe-out1*, а не *ether1*.

????????? ????????????

По окончании настроек вы сможете выходить в интернет с роутера. Проверьте IP-соединение с помощью ping:

```
[admin@MikroTik] > /ping 8.8.8.8
SEQ HOST SIZE TTL TIME STATUS
0 8.8.8.8 56 55 14ms399us
1 8.8.8.8 56 55 18ms534us
2 8.8.8.8 56 55 14ms384us
```

Также проверьте DNS-запрос:

```
[admin@MikroTik] > /ping google.com
SEQ HOST SIZE TTL TIME STATUS
0 142.250.74.14 56 55 14ms475us
1 142.250.74.14 56 55 14ms308us
2 142.250.74.14 56 55 14ms238us
```

При правильной настройке оба ping успешно проходят. В случае ошибки обратитесь к разделу устранения неполадок.

??????????? NAT

На данном этапе ПК ещё не может выходить в интернет, так как локальные адреса не маршрутизируются в интернет. Удалённые хосты не знают, как ответить на ваши локальные адреса.

Решение — изменить исходный адрес пакетов на публичный IP роутера, используя правило NAT:

```
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
```

Если публичный интерфейс — PPPoE, LTE или другой, то вместо *ether1* укажите соответствующий интерфейс.

Такой NAT защищает клиентов за роутером от прямого доступа из интернета.

??????? (Port Forwarding)

Для доступа к локальным клиентам из интернета по определённому порту (например, для RDP на IP 192.168.88.254), добавьте правило dstnat:

```
/ip firewall nat add chain=dstnat protocol=tcp port=3389 in-interface=ether1 \
action=dst-nat to-address=192.168.88.254
```

??????

Роутер теперь доступен извне, поэтому важно защитить его от взломов.

????????? (?????????)

1. ??????????

Без пароля любой может получить доступ к роутеру.

2. ?????????, ??? ????????? ????????? ?????????

Большинство домашних устройств имеют базовый брандмауэр. Не отключайте правила, добавляйте при необходимости.

3. ?????????? ? ?????????? ? ??????????

Это актуально для серии CCR, где firewall не настроен по умолчанию. Если нужен удалённый доступ, лучше использовать IPsec или Wireguard, а не открывать порты.

????????? ?????? ?????????

Рекомендуется создать надёжный пароль, содержащий:

- Не менее 12 символов;
- Цифры, символы, заглавные и строчные буквы;
- Исключить слова из словаря.

Команда для установки пароля пользователя:

```
/user set 0 password="!={Ba3N!40TyX+GvKBzjTLIUcx/, "
```

Или задать пароль для текущего пользователя:

```
/password  
old-password: *****  
new-password: *****  
confirm-new-password: *****
```

Учтите, что забытый пароль невозможно восстановить — придётся сбросить настройки или переустановить систему роутера!

Вы можете добавить новых пользователей с полными или ограниченными правами в меню

```
/user :
```

```
/user add name=myname password=mypassword group=full  
/user remove admin
```

Рекомендуется создать нового пользователя и отключить или удалить стандартного *admin*.

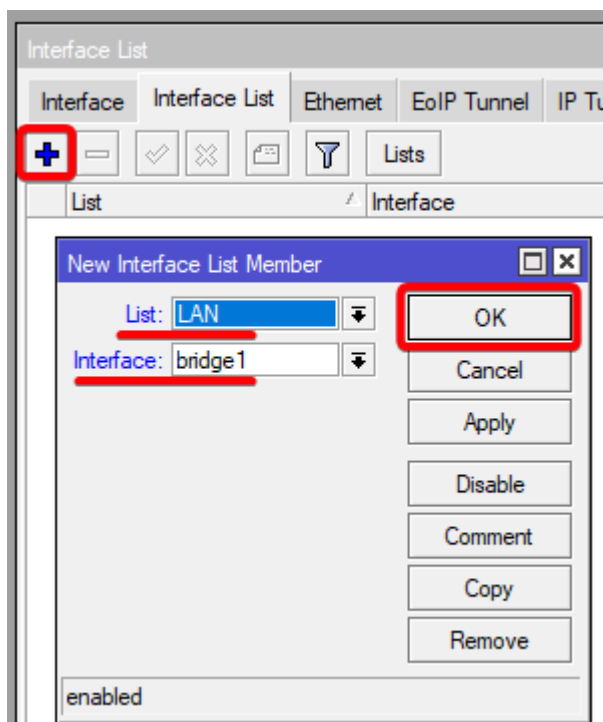
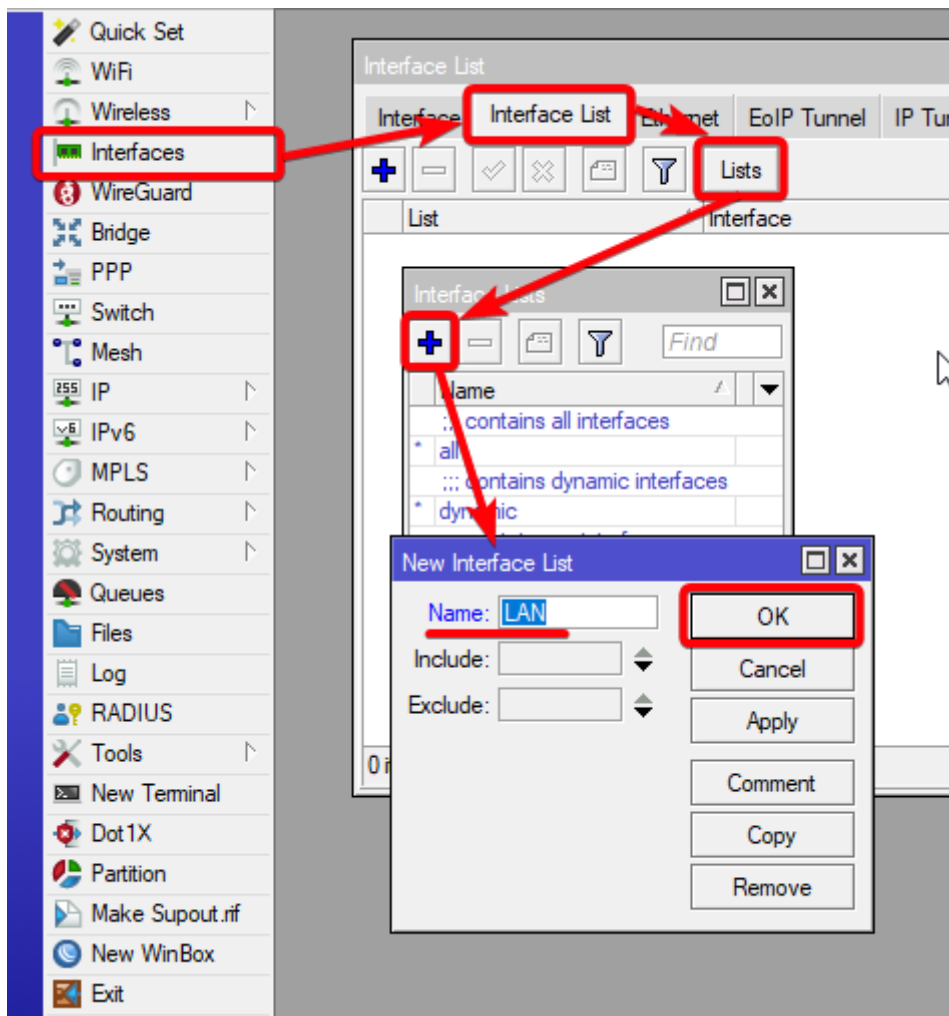
MAC ??????

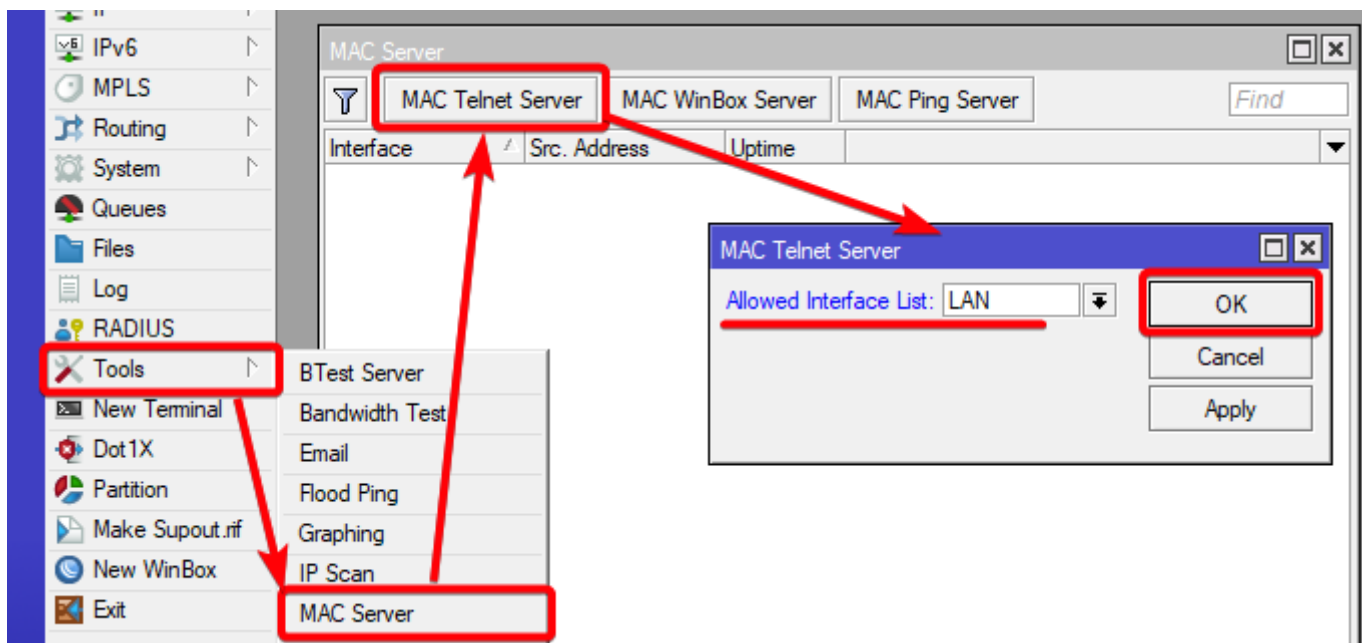
По умолчанию MAC сервер работает на **всех интерфейсах**. Чтобы ограничить MAC доступ с WAN, отключите default all и добавьте LAN интерфейс:

```
/interface list add name=LAN  
/interface list member add list=LAN interface=bridge1  
/tool mac-server set allowed-interface-list=LAN  
/tool mac-server mac-winbox set allowed-interface-list=LAN
```

Из WinBox/Webfig:

- Перейдите **Interfaces → Interface List → Lists**;
- Добавьте список с именем *LAN*;
- В секции Interface List добавьте в список *LAN* интерфейс *bridge1*;
- В меню **Tools → Mac Server** установите список *LAN* для MAC Telnet Server и MAC Winbox Server;
- Сохраните настройки.





???????????? (Neighbor Discovery)

Протокол MikroTik Neighbor Discovery показывает другие MikroTik роутеры в сети. Отключите его на публичных интерфейсах:

```
/ip neighbor discovery-settings set discover-interface-list=LAN
```

???????? IP ???????

Хотя firewall защищает роутер от внешних сетей, можно ограничить доступ по IP-адресам:

```
/user set 0 address=x.x.x.x/yy
```

где x.x.x.x/yy — ваш IP или подсеть для разрешения доступа.

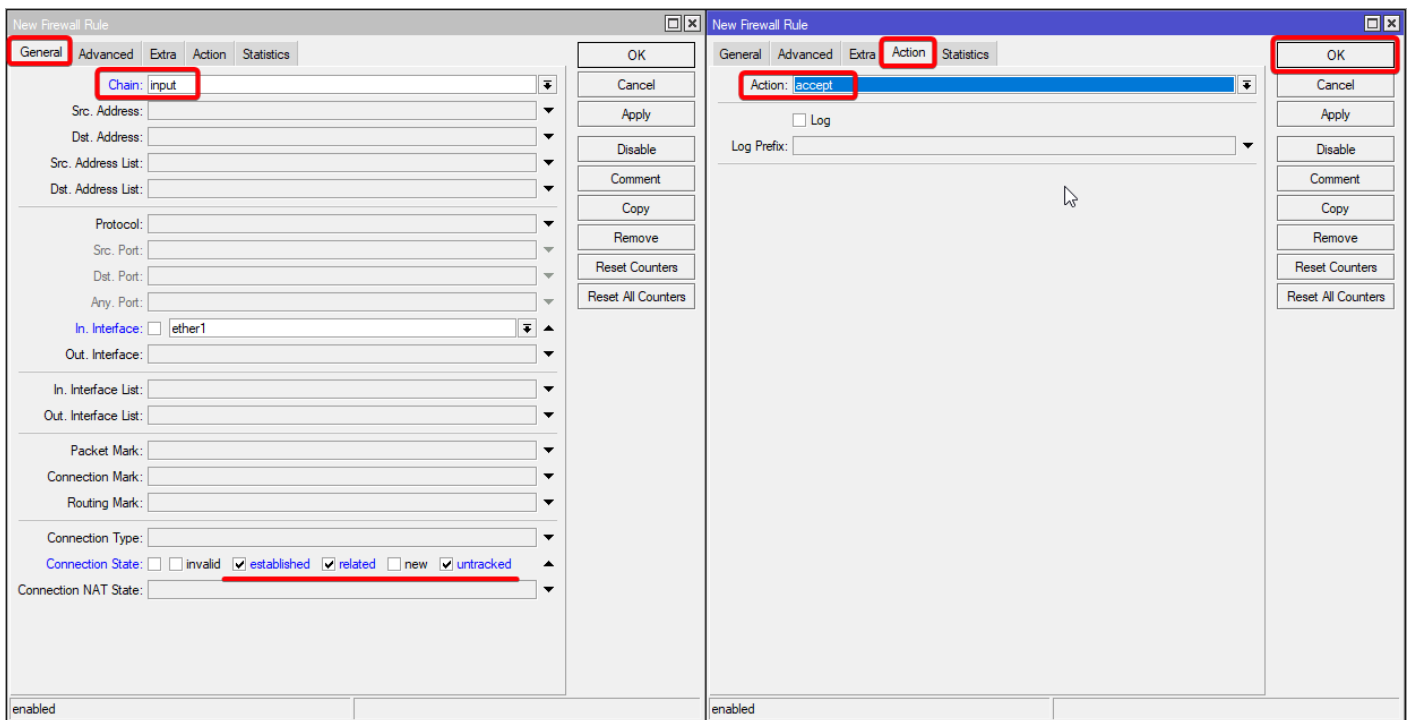
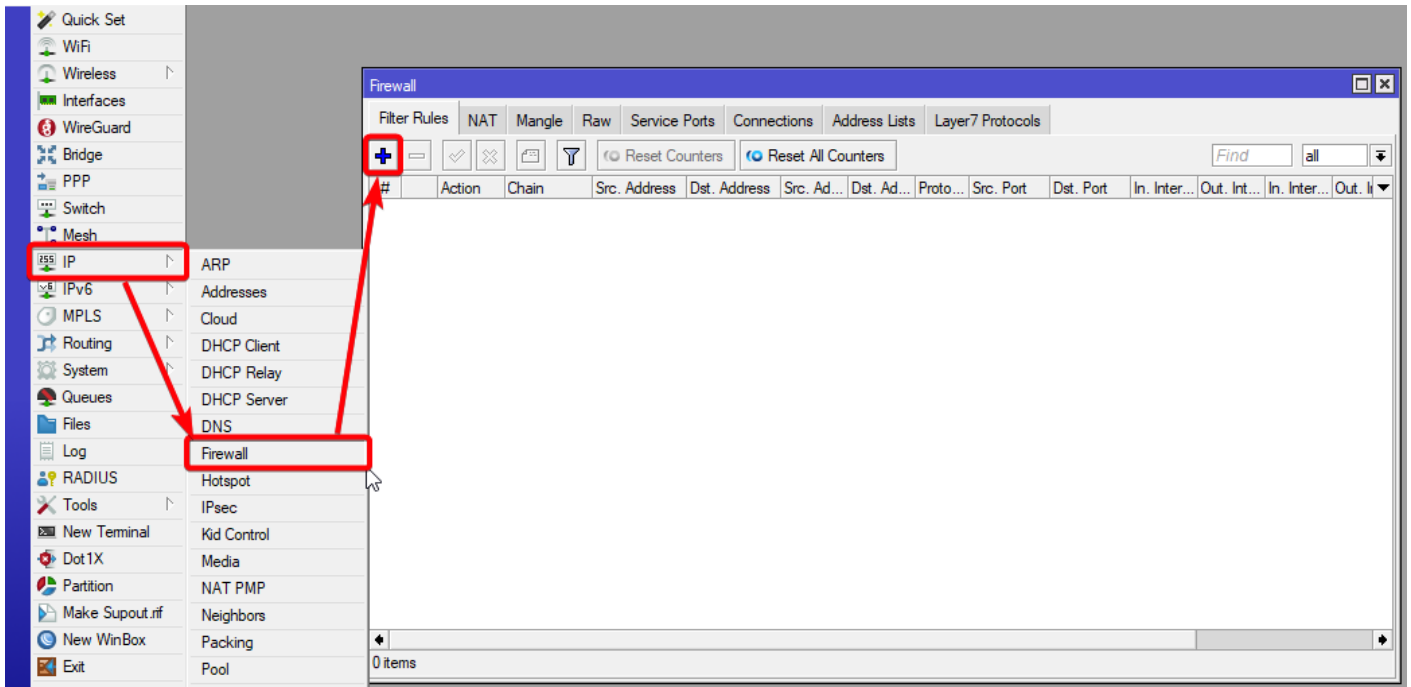
На публичном интерфейсе в firewall разрешите только ICMP (ping/traceroute), IP Winbox и ssh:

```
/ip firewall filter add chain=input action=accept connection-  
state=established,related,untracked comment="accept established,related,untracked"  
add chain=input action=drop connection-state=invalid comment="drop invalid"  
add chain=input in-interface=ether1 action=accept protocol=icmp comment="accept ICMP"  
add chain=input in-interface=ether1 action=accept protocol=tcp port=8291 comment="allow  
Winbox"  
add chain=input in-interface=ether1 action=accept protocol=tcp port=22 comment="allow SSH"  
add chain=input in-interface=ether1 action=drop comment="block everything else"
```

Если вместо ether1 используется PPPoE, LTE или другой интерфейс, замените в правилах *ether1* на соответствующий.

В WinBox/WebFig:

- Откройте IP → Firewall → Filter Rules;
- Добавьте правило с chain=input, выберите connection state с галочками для *established*, *related* и *untracked*;
- Выберите действие ассерт и сохраните.



Повторите, добавляя другие необходимые правила.

???????????????????? ???? ???? ?

Хотя firewall защищает роутер, вы можете отключить ненужные сервисы RouterOS:

```
/ip service disable telnet,ftp,www,api
```

Измените стандартные порты сервисов, чтобы снизить число случайных попыток входа по SSH:

```
/ip service set ssh port=2200
```

Каждый сервис можно ограничить по IP адресам:

```
/ip service set winbox address=192.168.88.0/24
```

?????? ????????

- Сервер пропускной способности для тестов между MikroTik роутерами следует отключать в продакшене:

```
/tool bandwidth-server set enabled=no
```

- Если не нужен DNS-кэш, его можно отключить:

```
/ip dns set allow-remote-requests=no
```

- Отключайте неиспользуемые интерфейсы для снижения риска несанкционированного доступа:

```
/interface set ether13 disabled=yes
```

(Где "ether13" - имя неиспользуемого интерфейса)

- Включите сильное шифрование SSH:

```
/ip ssh set strong-crypto=yes
```

- Проверьте отключение следующих сервисов (они по умолчанию отключены):

- MikroTik кэш-прокси: `/ip proxy set enabled=no`
- MikroTik socks-прокси: `/ip socks set enabled=no`
- MikroTik UPNP: `/ip upnp set enabled=no`
- MikroTik динамическое имя (IP Cloud): `/ip cloud set ddns-enabled=no update-time=no`

????????? ?????????????? ?????

Для удобства будет выполнена мостовая настройка беспроводной сети, чтобы проводные и беспроводные устройства находились в одной Ethernet-домене вещания.

Важно защитить беспроводную сеть, для начала создайте профиль безопасности:

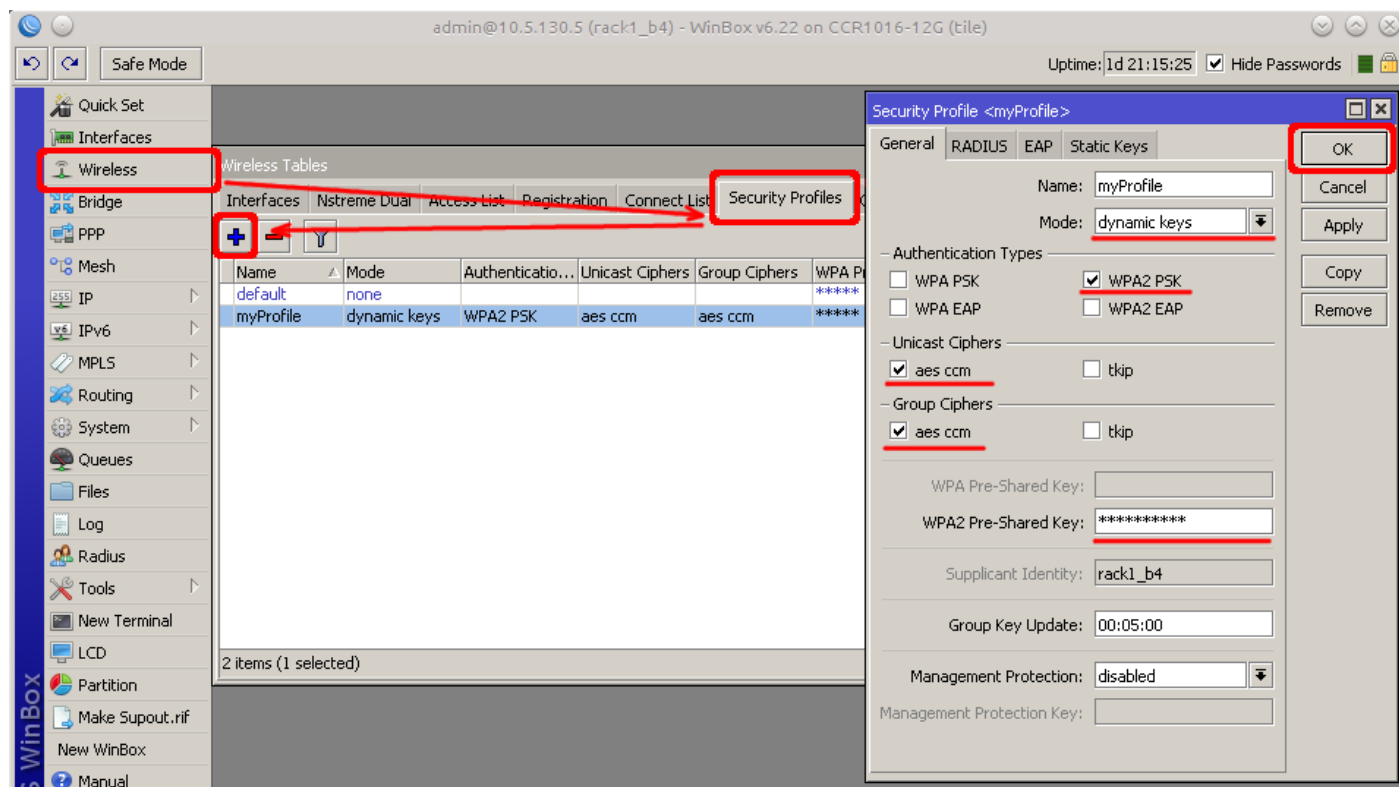
```

/interface wireless security-profiles add name=myProfile authentication-types=wpa2-psk
mode=dynamic-keys \
wpa2-pre-shared-key=1234567890

```

В Winbox/WebFig:

- Откройте окно **Wireless** и перейдите на вкладку **Security Profile**.



Если в сети есть старые устройства, не поддерживающие WPA2 (например, Windows XP), можно разрешить WPA протокол. Но WPA и WPA2 ключи должны быть разными.

Когда профиль безопасности готов, включите беспроводной интерфейс и задайте параметры:

```

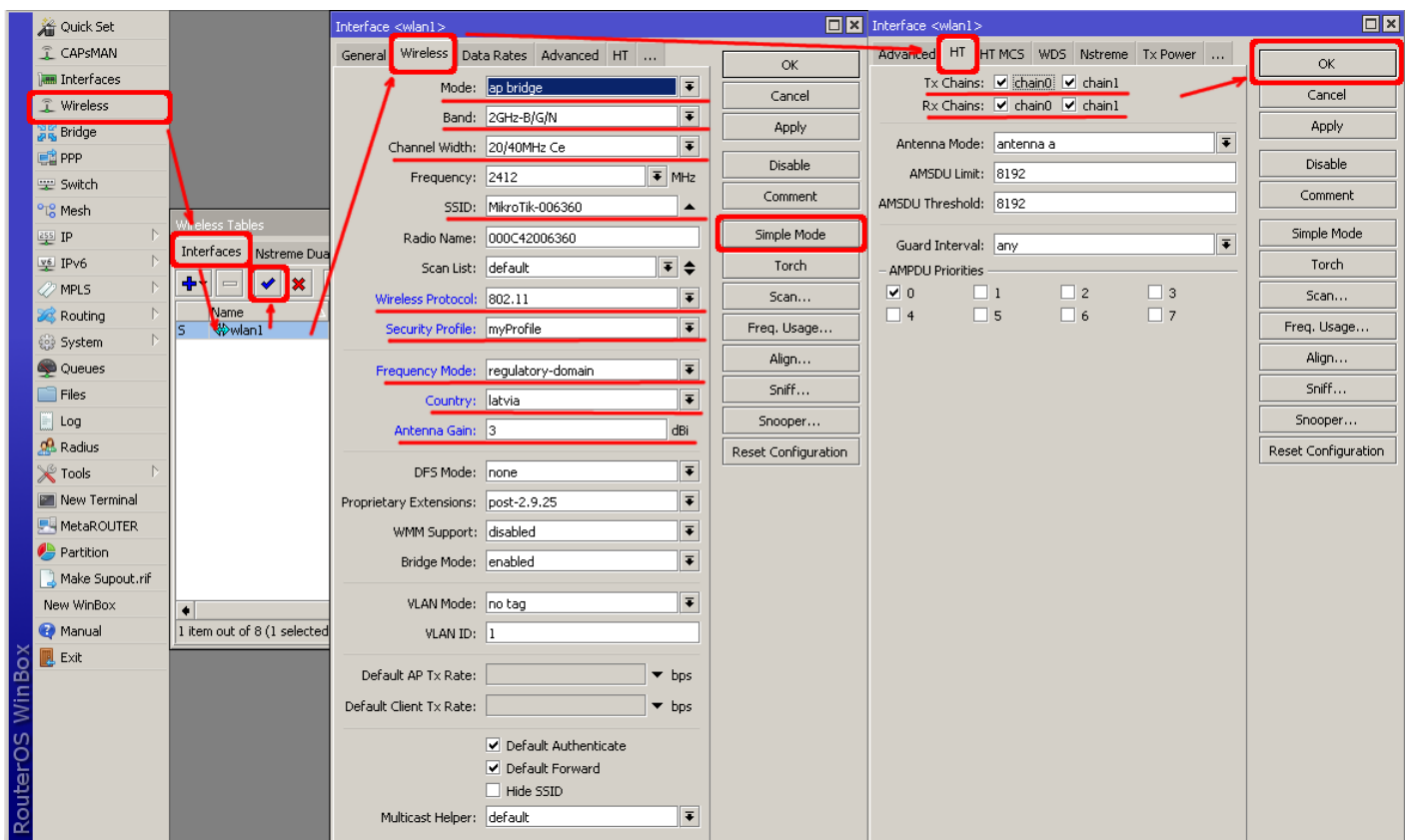
/interface wireless enable wlan1; set wlan1 band=2ghz-b/g/n channel-width=20/40mhz-Ce
distance=indoors \
mode=ap-bridge ssid=MikroTik-006360 wireless-protocol=802.11 \
security-profile=myProfile frequency-mode=regulatory-domain \
set country=latvia antenna-gain=3

```

В WinBox/WebFig:

- Откройте окно **Wireless**, выберите интерфейс wlan1 и нажмите кнопку *enable*;
- Дважды щёлкните интерфейс для открытия настроек;
- На вкладке **Wireless** нажмите кнопку *Advanced mode* справа для показа дополнительных параметров (переключит режим в *Simple mode* после нажатия);

- Выберите параметры как на скриншоте, кроме страны и SSID;
- На вкладке **HT** включите обе цепочки (~chains);
- Примените настройки кнопкой **OK**.



Последний шаг — добавить беспроводной интерфейс в локальный мост, иначе клиенты не получат IP:

```
/interface bridge port add interface=wlan1 bridge=bridge1
```

Теперь беспроводная сеть готова принимать клиентов, выдавать им IP и обеспечивать интернет-доступ.

?????? ????????

Добавим базовые правила защиты для клиентов локальной сети:

```
/ip firewall filter add chain=forward action=fasttrack-connection connection-
state=established,related \
comment="fast-track for established,related"
add chain=forward action=accept connection-state=established,related \
comment="accept established,related"
add chain=forward action=drop connection-state=invalid
add chain=forward action=drop connection-state=new connection-nat-state=!dstnat \
in-interface=ether1 comment="drop access to clients behind NAT from WAN"
```

Правила похожи на входящие (input): принимаются установленные/связанные и отбрасываются недействительные пакеты. Первая строка с fasttrack позволяет значительно уменьшить нагрузку на CPU.

Последнее правило блокирует новые соединения с WAN к LAN, если не используется dstnat. Это снижает риск атак на локальные хосты.

Подробности и расширенные примеры настройки брандмауэров поищите в статье о построении первого брандмауэра.

?????????? ?????????????? ???????

Иногда нужно запретить доступ к определённым сайтам (например, развлекательным, порнографическим) на работе. Для этого перенаправляют HTTP трафик на прокси и используют списки доступа для разрешения или блокировки сайтов.

Для начала добавим правило NAT, которое перенаправляет HTTP трафик на встроенный прокси на порту 8080:

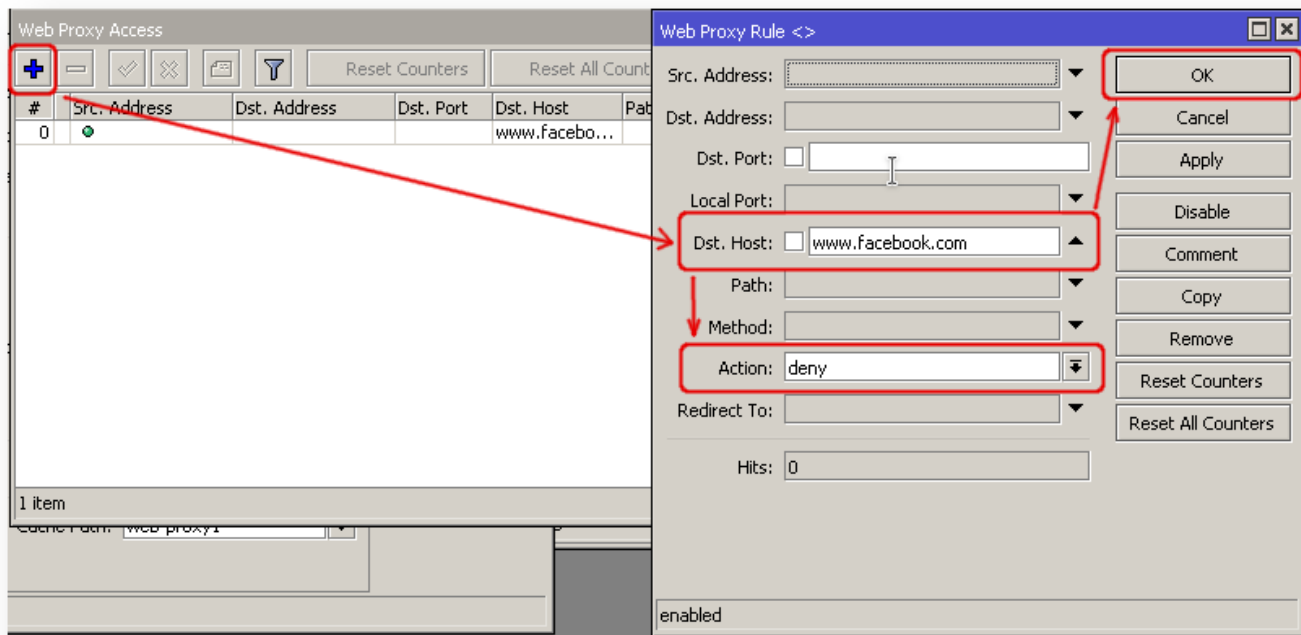
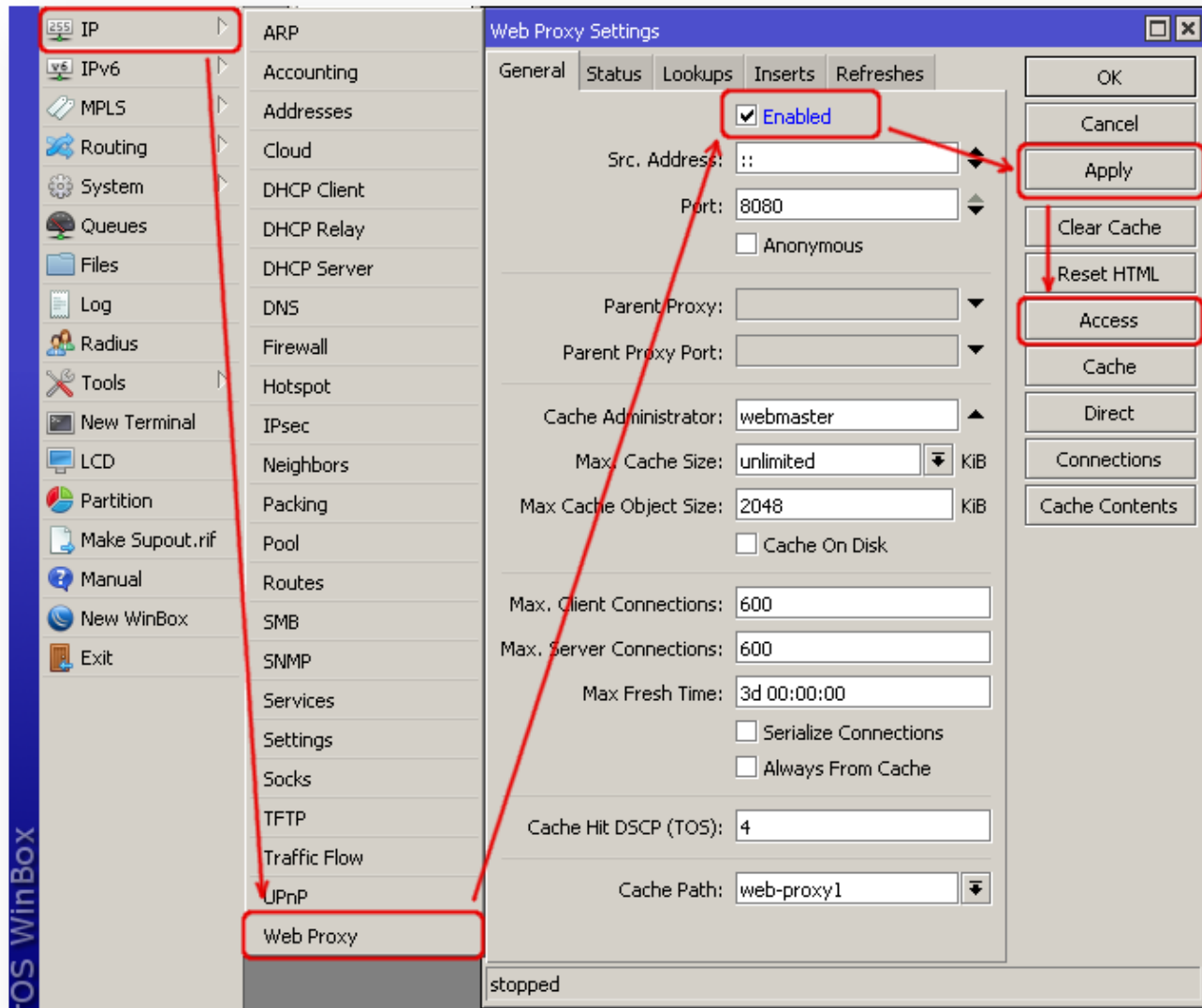
```
/ip firewall nat add chain=dst-nat protocol=tcp dst-port=80 src-address=192.168.88.0/24 \
action=redirect to-ports=8080
```

Включаем прокси и запрещаем некоторые сайты:

```
/ip proxy set enabled=yes
/ip proxy access add dst-host=www.facebook.com action=deny
/ip proxy access add dst-host=*.youtube.* action=deny
/ip proxy access add dst-host=:vimeo action=deny
```

Используя Winbox:

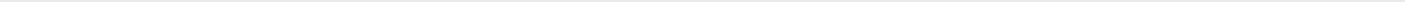
- Перейдите в IP → Web Proxy;
- Откроется окно настроек прокси, поставьте галочку "Enable" и нажмите "Apply";
- Нажмите кнопку "Access", добавьте новые правила с доменами сайтов и действием "deny";
- Повторите для других сайтов.



?????????? ??????????

RouterOS содержит встроенные инструменты для диагностики, например, ping, traceroute, torch, packet sniffer, bandwidth test.

Мы ранее использовали ping для проверки интернет-соединения.



Revision #8
Created 11 November 2025 08:17:13 by Admin
Updated 11 November 2025 10:57:26 by Admin