📡 MikroTik hAP ac³ - настраиваем Wi-Fi правильно и безопасно

Я купил себе новый роутер - **MikroTik hAP ac³** - и решил сделать с ним не «абы как, лишь бы работало», а **нормально и безопасно**, так, как это делается в осознанных сетях.

Цель простая и честная: настроить Wi-Fi **максимально грамотно с точки зрения безопасности**, без лишней магии, но с пониманием того, *что* мы делаем и *зачем*.

В этом гайде мы шаг за шагом:

- поднимем базовый Wi-Fi на **WPA3**
- аккуратно приведём MikroTik в состояние адекватной точки доступа
- подготовим его к работе через **RADIUS** (802.1X / EAP)
- разберём типичные ошибки и моменты, на которых чаще всего спотыкаются

Это не теория и не переписанный мануал.

Это **практика**, собранная по ходу реальной настройки нового устройства - так, как я бы делал это в своей сети.

А дальше - будет ещё интереснее: это лишь этап.
В следующих шагах сеть станет взрослее.

🔌 Шаг 1. Первое подключение и вход в MikroTik

Начинаем с самого простого - **физического подключения и первичного входа** в роутер.

Никакой магии, всё максимально приземлённо.

1️⃣ Подключаем кабели

- Берём кабель от провайдера и **подключаем его в порт ether1** - это будет WAN
- Компьютер для настройки подключаем **любым другим портом** (например, ether2)
- Включаем питание роутера и даём ему полностью загрузиться

На этом этапе **Wi-Fi можно вообще не трогать** - настраиваемся по проводу, так надёжнее.

2️⃣ Готовим компьютер для подключения

Так как роутер новый (или сброшен к заводским настройкам), подключаемся к нему напрямую.

На компьютере:

- открываем настройки сетевой карты
- вручную задаём **статический IP-адрес**

Параметры такие:

- **IP-адрес:** 192.168.88.2
- **Маска сети:** 255.255.255.0 (или /24)
- Шлюз и DNS можно оставить пустыми

Это временно - только для первичной настройки.

3️⃣ Подключаемся через Winbox

Для работы с MikroTik будем использовать **Winbox** - это самый удобный способ управления.

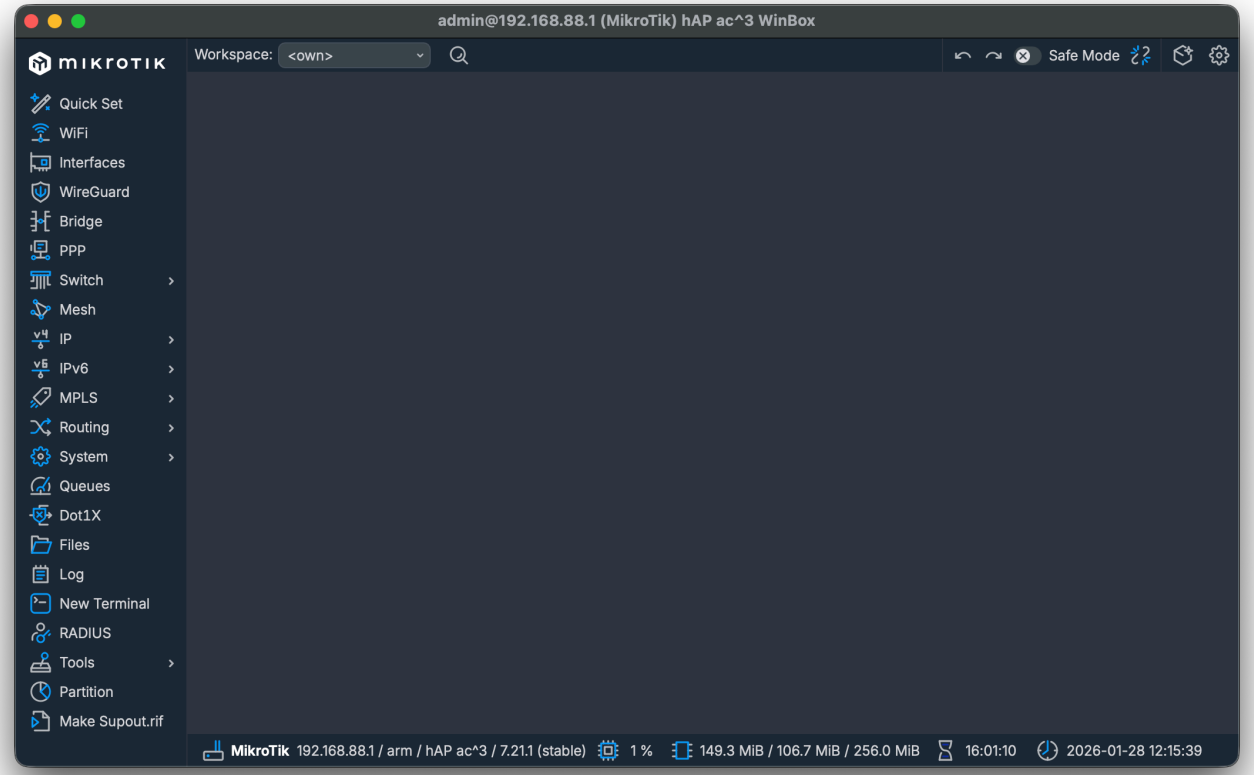
- Winbox скачиваем **с официального сайта MikroTik**
- Запускаем программу на компьютере
- В списке устройств (через MAC) или вручную указываем адрес роутера
- Подключаемся

Данные для входа по умолчанию:

- **Логин:** admin
- **Пароль:** пустой

После входа ты увидишь чистую, заводскую конфигурацию - с этого момента мы начинаем наводить порядок 😌

Вот здесь мы уже **полностью контролируем устройство** и можем двигаться дальше: приводить базовую конфигурацию в порядок и готовить почву под безопасный Wi-Fi.

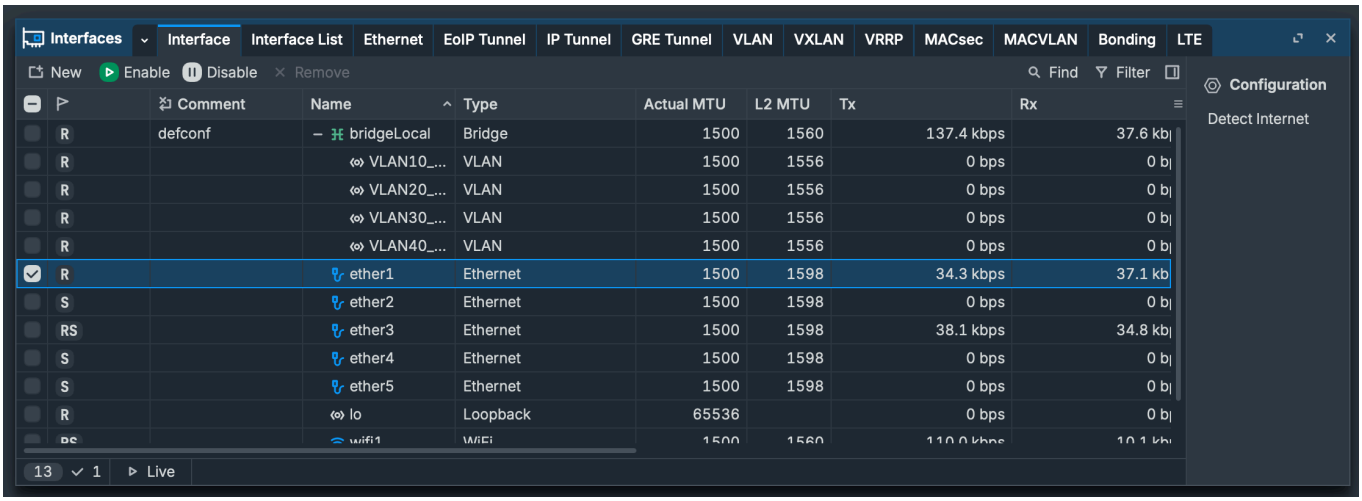


🌍 Шаг 2. Настройка WAN через Winbox (MikroTik)

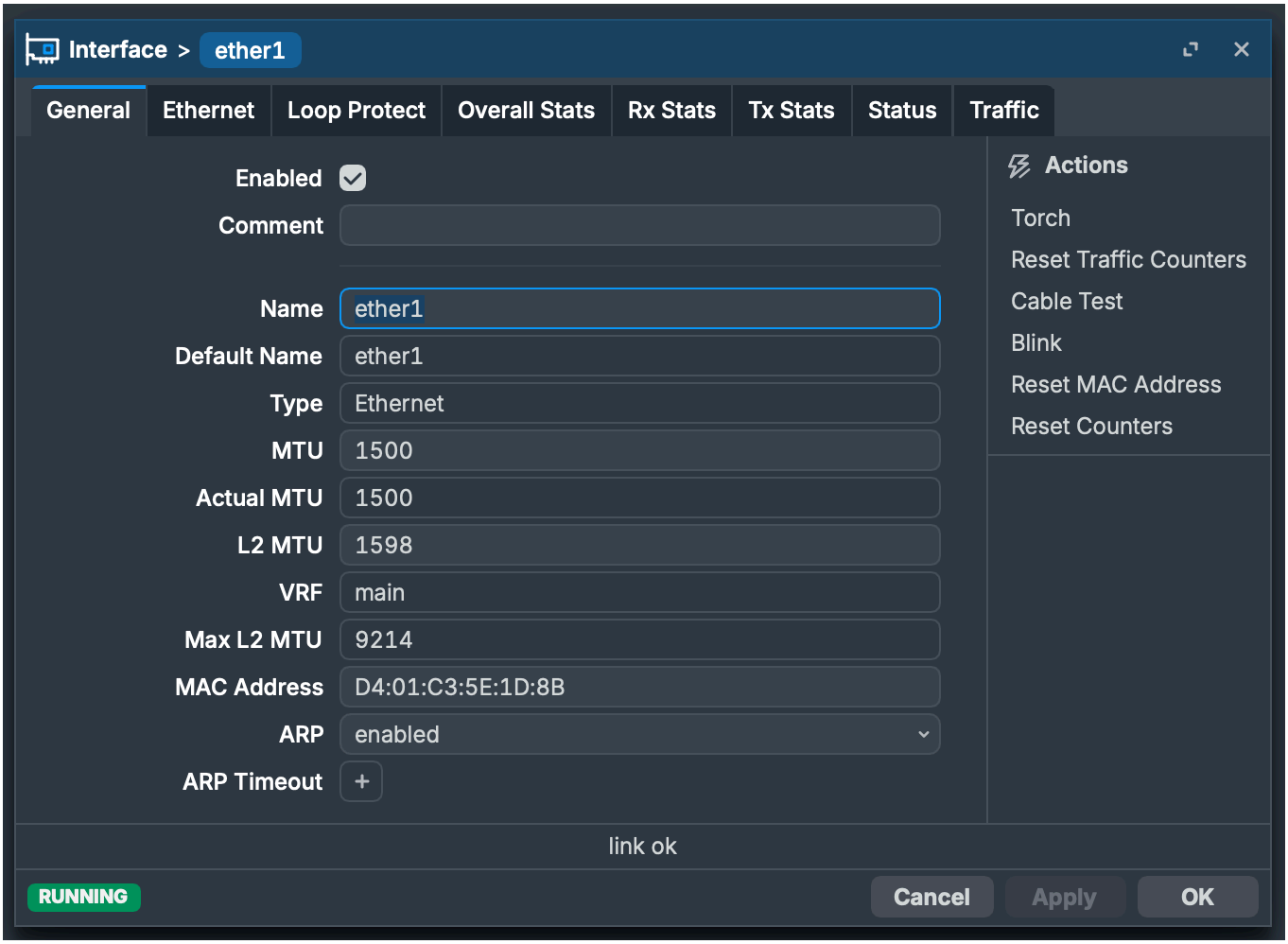
Мы уже подключились к роутеру через **Winbox** и видим его интерфейс.
Теперь настраиваем **WAN-подключение**, то есть интернет от провайдера.

> В нашем случае WAN - это порт **ether1**, в который подключён кабель провайдера.

2.1 Проверяем физическое состояние интерфейса



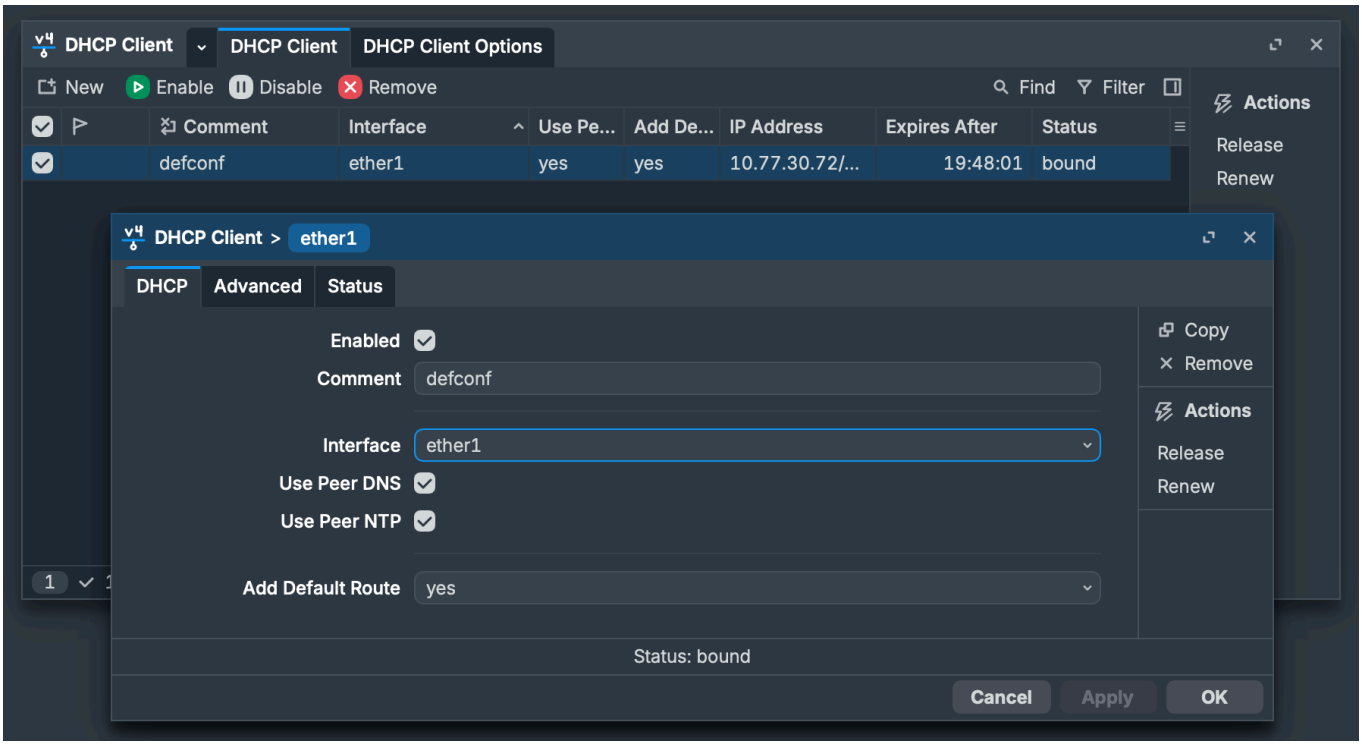
1. В Winbox переходим в меню
   Interfaces
2. В списке интерфейсов находим **ether1**
3. Обращаем внимание:
   - интерфейс **enabled** (нет красного крестика)
   - есть статус **R (running)** - это значит, что линк поднят



📌 *Если ether1 не running - сначала проверяем кабель и порт.*

2.2 Включаем DHCP Client на WAN

Так как в большинстве случаев провайдер выдаёт интернет по DHCP, настраиваем DHCP-клиент.



1. Переходим в меню
   IP → DHCP Client
2. Нажимаем **+ (Add New)**
3. В открывшемся окне указываем:
   - **Interface:** ether1
   - **Use Peer DNS:** ✅ включено
   - **Use Peer NTP:** ✅ включено
   - **Add Default Route:** ✅ включено

Остальные параметры **оставляем по умолчанию**.

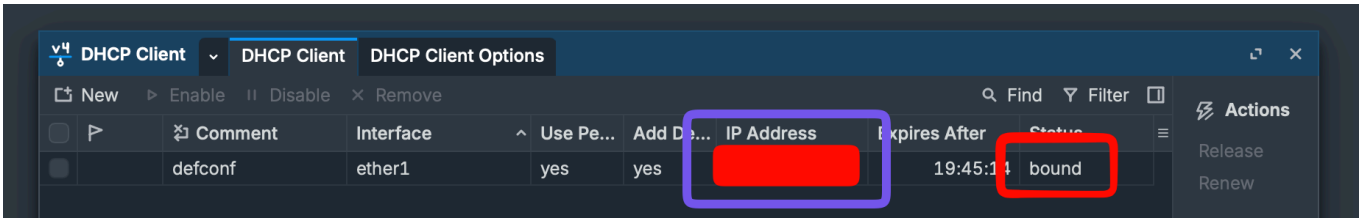
4. Нажимаем **OK**

📌 *После этого MikroTik должен автоматически получить IP-адрес от провайдера.*

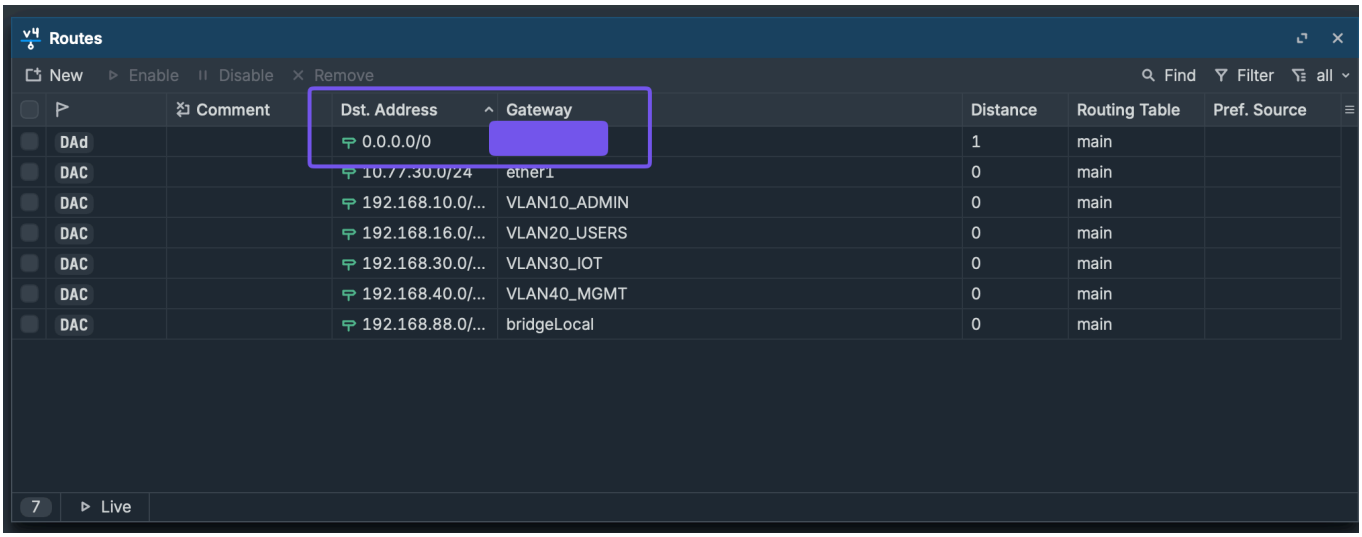
2.3 Проверяем, что интернет появился

Теперь важно убедиться, что роутер действительно получил доступ в интернет.

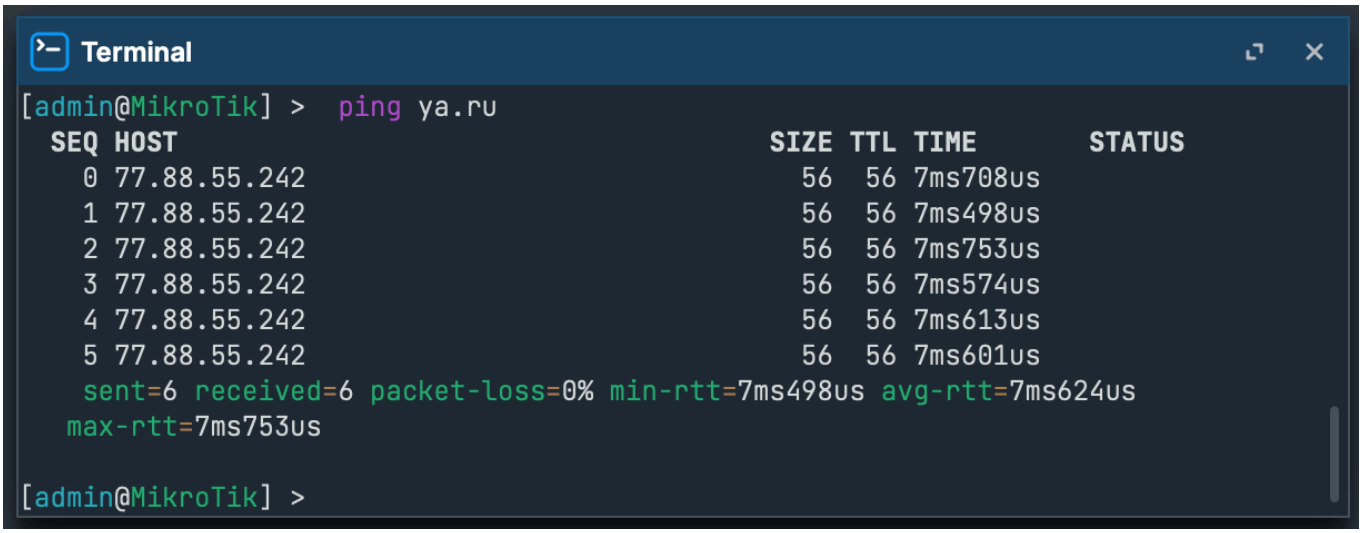
1. В том же разделе **IP → DHCP Client**:
   - статус должен быть **bound**
   - должен отображаться полученный IP-адрес



2. Переходим в
   IP → Routes
   - проверяем, что появился маршрут **0.0.0.0/0**
   - шлюз указывает на адрес провайдера



2. Для финальной проверки:
   - открываем **New Terminal**
   - пробуем выполнить ping любого внешнего IP



Если пинг проходит - значит:

> WAN настроен корректно, и роутер уже имеет доступ в интернет.

Важный момент

На этом этапе:

- ❌ Wi-Fi не настраиваем
- ❌ firewall не трогаем
- ❌ LAN пока не усложняем

Наша задача здесь одна - **убедиться, что WAN работает стабильно**.
Это основа для всех следующих шагов.

🏠 Шаг 3. Базовая настройка LAN (внутренняя сеть)

Теперь, когда WAN уже работает, настраиваем **LAN** - внутреннюю сеть, к которой будут подключаться устройства.

Пока без VLAN, без RADIUS и без усложнений. Наша задача - **чистая и понятная база**.

3.1 Проверяем и настраиваем Bridge

В MikroTik все LAN-порты обычно объединяются в **bridge** - это логика обычного коммутатора.

1. В Winbox переходим в меню
   Bridge
2. Во вкладке **Bridge**:
   - обычно уже есть bridge с именем bridge
   - если его нет - нажимаем **+** и создаём новый

Параметры:

- **Name:** bridge
- Остальное - по умолчанию

Нажимаем **OK**.

3.2 Добавляем LAN-порты в bridge

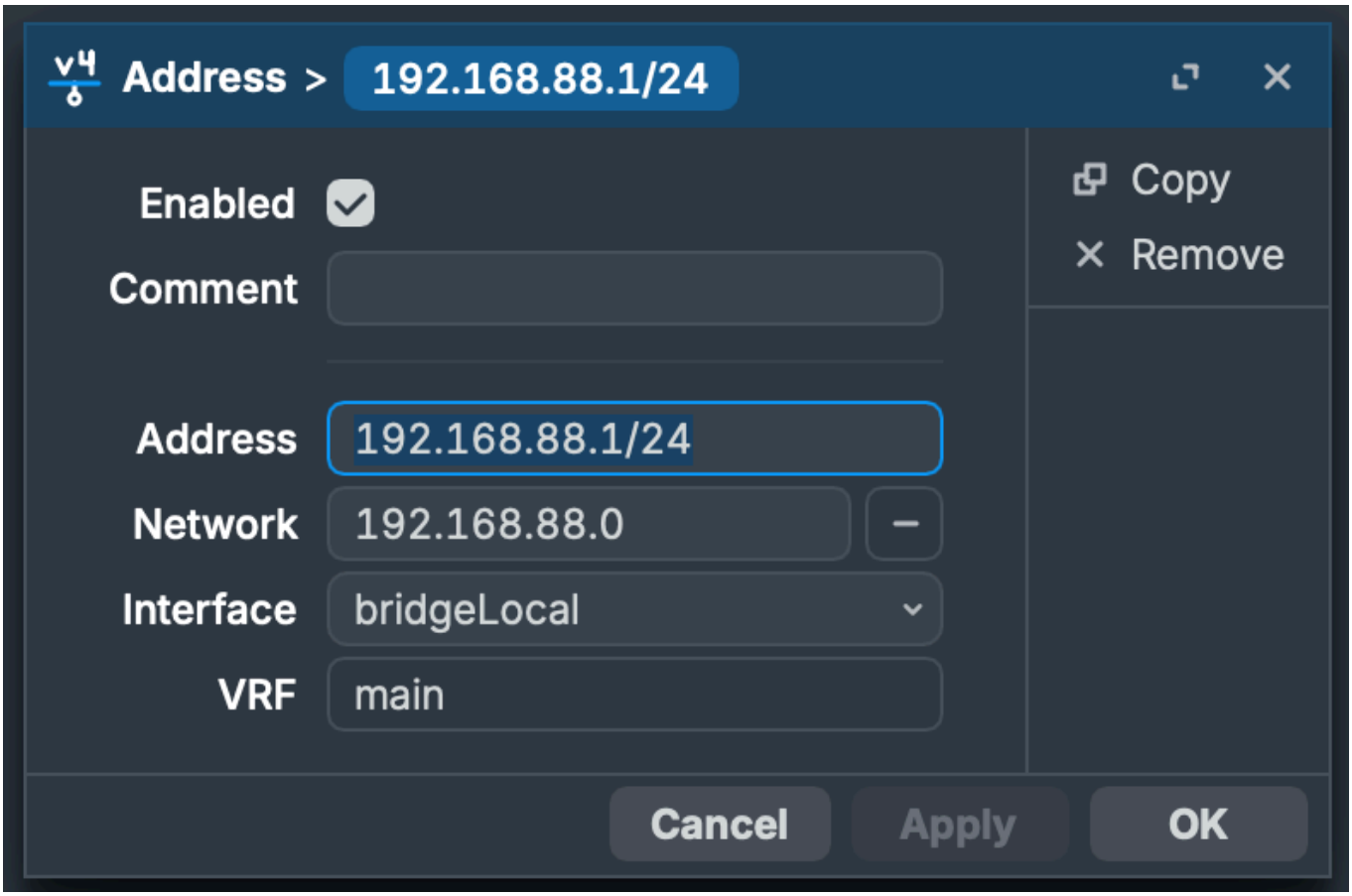
Теперь подключаем физические порты к bridge.

1. Переходим во вкладку
   Bridge → Ports
2. Добавляем порты:
   - нажимаем **+**
   - **Interface:** ether2
   - **Bridge:** bridge
   - **OK**
3. Повторяем для остальных LAN-портов:
   - ether3
   - ether4
   - ether5

📌 *Порт ether1 (WAN) **не добавляем** в bridge.*

3.3 Назначаем IP-адрес на bridge

Теперь задаём IP-адрес для внутренней сети.



1. Переходим в меню
   IP → Addresses
2. Нажимаем **+**
3. Указываем:
   - **Address:** 192.168.88.1/24
   - **Interface:** bridge
4. Нажимаем **OK**

Это будет:

- IP-адрес роутера в LAN
- шлюз по умолчанию для клиентов

3.4 Настраиваем DHCP-сервер для LAN

Чтобы устройства автоматически получали адреса, поднимаем DHCP.

1. Переходим в
   IP → DHCP Server
2. Нажимаем **DHCP Setup**
3. В мастере:
   - **DHCP Server Interface:** bridge
   - **DHCP Address Space:** 192.168.88.0/24
   - **Gateway:** 192.168.88.1
   - **Address Pool:** можно оставить предложенный
   - **DNS Servers:** можно оставить автоматически
4. Подтверждаем все шаги мастера

После завершения DHCP-сервер будет активен.

3.5 Проверяем работу LAN

Подключаем компьютер к любому LAN-порту:

- проверяем, что он получил IP-адрес автоматически
- пробуем открыть:
  - веб-интерфейс MikroTik
  - любой сайт в интернете

Если всё работает - значит:

> внутренняя сеть настроена корректно и готова к дальнейшим шагам.

Что важно на этом шаге

- ✓ простая и прозрачная LAN-схема

- ✓ всё завязано на bridge
- ✓ без лишних усложнений

Это та база, от которой мы будем дальше:

- строить Wi-Fi
- усиливать безопасность
- переходить к WPA3 и RADIUS

📦 Шаг 4.0. Установка пакета Wi-Fi

Перед настройкой современного и безопасного Wi-Fi важно понимать один момент:

> “ стандартный пакет **wireless** в RouterOS **ограничен**
> и **не позволяет корректно использовать WPA3**

Поэтому для дальнейшей настройки мы будем использовать **новый Wi-Fi стек MikroTik - wifi-qcom-ac**.

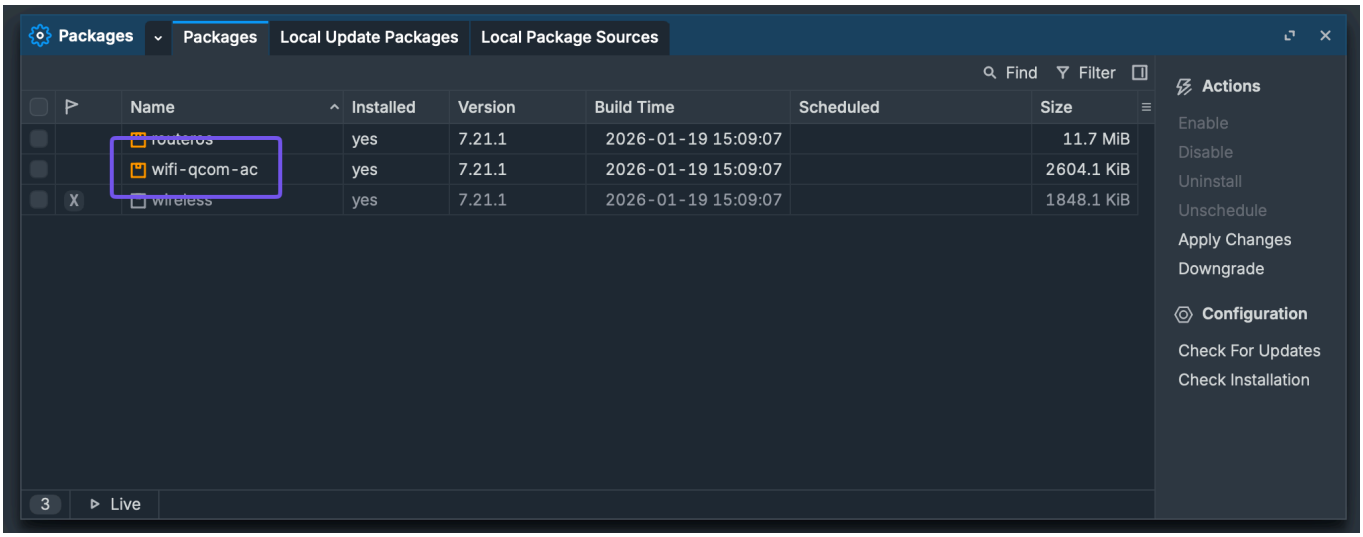
Что это и зачем

wifiwave2 - это новый беспроводной пакет MikroTik, который:

- поддерживает **WPA3**
- корректно работает с **802.11ac / ax**
- является актуальным и рекомендуемым вариантом

Если его не установить - дальше просто **нет смысла идти**.

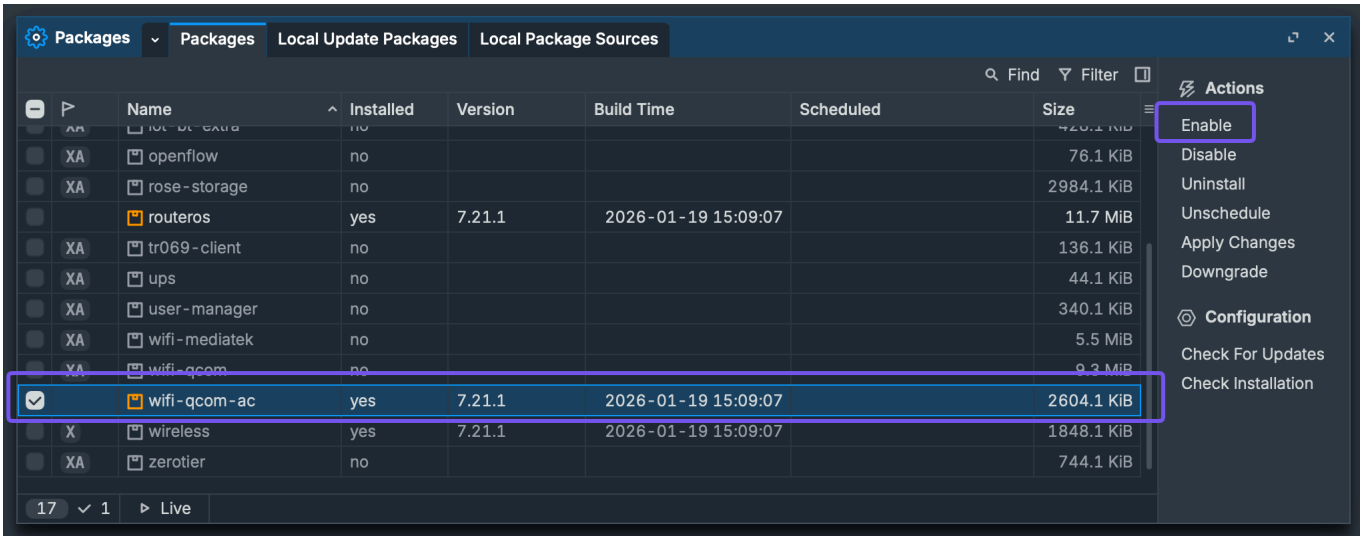
4.0.1 Проверяем текущие пакеты



1. В Winbox переходим в меню
   System → Packages
2. В списке пакетов:
   - ищем **wifi-qcom-ac**
   - если его **нет** - значит, он не установлен
   - если есть wireless - это нормально, мы его заменим логически

📌 *На этом этапе ничего не удаляем.*

4.0.2 Устанавливаем пакет



Вместо Enable у вас будет - Install

Теперь в меню Winbox:

- вместо старого **Wireless**
- появляется новый раздел **WiFi**

👉 Это означает, что роутер готов к современной настройке Wi-Fi.

Важный момент

С этого шага:

- ❌ **старый wireless больше не используем**
- ✅ **вся дальнейшая настройка Wi-Fi будет через WiFi**

Именно с этим пакетом мы дальше:

- настраиваем **WPA3**
- готовим почву под **RADIUS / 802.1X**

📶 Шаг 4. Настройка Wi-Fi через WiFi (PSK / WPA3)

После установки пакета **wifiwave2** вся дальнейшая работа с беспроводной сетью выполняется **через новый раздел WiFi**, а не через старый Wireless.

Наша цель на этом шаге -

👉 поднять **рабочий и безопасный Wi-Fi по PSK**, который станет базой для следующего перехода к RADIUS.

4.1 Проверяем Wi-Fi интерфейсы

1. В Winbox переходим в меню
   WiFi
2. Во вкладке **WiFi Interfaces** должны отображаться два интерфейса:
   - 2.4 ГГц

- 5 ГГц

Если интерфейсы **disabled** - включаем их (**Enable**).

4.2 Создаём профиль безопасности (Security)

Теперь настраиваем безопасность Wi-Fi.

1. Переходим в
   WiFi → Security
2. Нажимаем **+ (Add New)**
3. Указываем параметры:

- **Name:** wpa3-psk
- **Authentication Types:**
  - WPA2-PSK ✅
  - WPA3-PSK ✅
- **Encryption:**
  - CCMP (AES)
- **Passphrase:**
  - задаём сложный пароль (не короткий)

📌 *Оставляем WPA2 + WPA3 - это повышает совместимость со старыми устройствами.*

Нажимаем **OK**.

4.3 Создаём конфигурацию Wi-Fi (Configuration)

Теперь связываем SSID, безопасность и режим работы.

1. Переходим в
   WiFi → Configurations

2. Нажимаем **+**
3. Основные параметры:

- **Name:** wifi-main
- **SSID:** имя твоей Wi-Fi сети (Например - SUDO_MAKE_ME_A_SANDWICH 😂)
- **Country:** твоя страна
- **Mode:** ap
- **Security:** wpa3-psk
- **Disable PMKID:** ❌ (оставляем выключенным)

Нажимаем **OK**.

4.4 Привязываем Wi-Fi к bridge (Datapath)

1. В той же конфигурации открываем вкладку
   Datapath
2. Указываем:

- **Bridge:** bridge
- **Client Isolation:** ❌ (пока выключено)

📌 *Это позволяет Wi-Fi-клиентам попадать в LAN.*

4.5 Применяем конфигурацию к интерфейсам

1. Возвращаемся в
   WiFi → WiFi Interfaces
2. Для каждого интерфейса (2.4 и 5 ГГц):
   - открываем интерфейс
   - в поле **Configuration** выбираем wifi-main
   - нажимаем **OK**
     После этого:

- SSID становится видимым
- Wi-Fi начинает работать с заданной защитой

4.6 Проверяем подключение

Подключаемся с любого устройства:

- сеть видна
- пароль принимается
- устройство получает IP по DHCP
- есть доступ в интернет

Если всё это есть - значит:

> Wi-Fi по PSK настроен корректно и стабильно.

Важный смысл этого шага

Этот вариант - **осознанная база**, а не финал:

- ✓ современный Wi-Fi стек
- ✓ WPA3
- ✓ чистая интеграция с LAN

Дальше мы будем:

👉 усиливать безопасность
👉 отключать лишнее
👉 **переходить на RADIUS / 802.1X**

🔐 Шаг 6. Ужесточение безопасности MikroTik и Wi-Fi

На этом этапе считаем, что:

- WAN работает

- LAN стабилен
- Wi-Fi по **WPA3-PSK** уже проверен и используется

Теперь приводим всё в **более безопасное состояние**.

6.1 Защита доступа к самому MikroTik

Меняем пароль администратора

1. **System → Users**
2. Открываем пользователя admin
3. Задаём **сложный пароль**
4. OK

📌 *Пустой пароль - это только для первого входа. Дальше - никогда.*

Ограничиваем доступ к управлению

1. **IP → Services**
2. Обращаем внимание:
   - telnet ❌ disable
   - ftp ❌ disable
   - www ❌ disable
   - www-ssl - по желанию
   - ssh - только если нужен
   - winbox - оставить ✅

👉 В идеале:

- управление **только из LAN**
- никаких сервисов наружу

6.2 Базовая защита Wi-Fi

Переходим в **WiFi → Configurations**
Открываем нашу конфигурацию (wifi-main).

Проверяем и включаем:

- **WPS:** ❌ отключён
- **Management Protection:** ✅ включено (если доступно)
- **FT / Fast Transition:** ❌ (пока не нужен)
- **PMKID:** ❌ (если нет причины включать)

📌 *Чем меньше “умных” фич - тем меньше поверхность атаки.*

6.3 Ограничение управления Wi-Fi

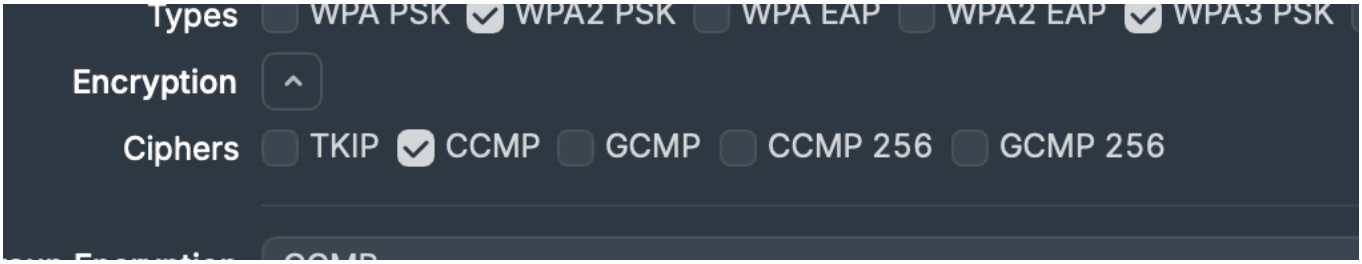
В **WiFi → Security**:

- используем **только CCMP (AES)**
- никаких TKIP
- никаких legacy-алгоритмов

Это особенно важно для WPA3 -

> “безопасность должна быть **реальной**, а не «на бумаге».

📝 Сноска: варианты шифрования Wi-Fi (Ciphers)



В настройках безопасности Wi-Fi можно выбрать разные алгоритмы шифрования. Кратко - **что это и что выбирать**

❌ TKIP

- Устаревший алгоритм (ещё со времён WPA)

- Считается **небезопасным**
- Сильно снижает уровень защиты

✅ CCMP (AES)

- Современный и **стабильный стандарт**
- Полностью поддерживается всеми устройствами
- Рекомендуется для:
  - WPA2-PSK
  - WPA3-PSK
  - WPA-Enterprise

👉 **Оптимальный выбор по умолчанию**

⚠️ GCMP

- Более новый алгоритм
- Используется в современных реализациях WPA3
- Может давать:
  - проблемы совместимости
  - нестабильность на старых клиентах

👉 **Можно использовать**, но только если все клиенты современные

⚠️ CCMP-256

- Усиленная версия CCMP
- Более высокая криптостойкость
- Требует поддержки со стороны клиентов

👉 **Избыточен для домашней и SOHO-сети**

⚠️ GCMP-256

- Максимальный уровень шифрования
- Используется в строгих корпоративных средах

- Часто вызывает проблемы совместимости

👉 **Только для специализированных сценариев**

✅ Рекомендация для этого гайда

Для стабильной, безопасной и совместимой сети:

> ❝ **Используем: CCMP (AES)**

> ❝ Без TKIP, без legacy-алгоритмов.

Это даёт:

- высокий уровень безопасности
- отличную совместимость
- предсказуемую работу сети

6.4 Клиенты и изоляция (опционально)

Если в сети будут:

- гости
- IoT
- непроверенные устройства

👉 можно включить **Client Isolation** в Datapath.

Пока:

- для основной сети ❌ выключено
- для гостевых - включим позже отдельным SSID

6.5 Общая логика этого шага

Мы сделали:

- ✓ закрыли лишние сервисы
- ✓ защитили управление
- ✓ убрали устаревшие протоколы
- ✓ минимизировали поверхность атаки

Это **базовый security hardening**, без фанатизма, но уже на уровне:

> «так не стыдно оставить в реальной сети»

Дальше - самое вкусное 😌

👉 **Шаг 7: переход на RADIUS / 802.1X**
👉 персональная аутентификация
👉 взрослая архитектура
\