Лабораторная работа

«Централизованное управление беспроводными точками доступа»

Разработал ведущий инженер
лаборатории телекоммуникационных и информационных систем
Института механики сплошных сред УрО РАН
Добрынин Никита Александрович
11.03.2026

Краткие теоретические сведения

Беспроводная точка доступа (Wireless access point) – устройство, которое выступает в роли центрального передатчика и приемника для беспроводных сигналов, обеспечивая связь между беспроводными устройствами, а также их подключение к проводному сегменту локальной сети.

Маршрутизатор (Router) — это устройство, передающее пакет в нужном направлении (через нужный интерфейс). В терминологии IETF маршрутизатор называют также шлюз (Gateway). По тексту пособия маршрутизатор называется роутером.

RouterOS - это автономная операционная система, основанная на ядре Linux. Она поддерживает работу аппаратных устройств MikroTik.

Winbox – утилита для настройки устройств MikroTik через графический интерфейс.

CAPsMAN (Controller Access Point system Manager) — встроенный программный компонент каждого маршрутизатора MikroTik.

CAPsMAN позволяет применять настройки беспроводной сети к нескольким устройствам MikroTik AP из центрального интерфейса конфигурации.

Если говорить конкретнее, то система управления точками доступа с контролем (CAPsMAN) позволяет централизовать управление беспроводной сетью и, при необходимости, обработку данных. При использовании функции CAPsMAN сеть будет состоять из нескольких «контролируемых точек доступа» (CAP), обеспечивающих беспроводное подключение, и «системного менеджера» (CAPsMAN), который управляет конфигурацией точек доступа, а также выполняет аутентификацию клиентов и, при необходимости, пересылку данных.

Лабораторная работа

Соберите топологию, указанную на рисунке 1. Соедините разъемы на патч-панели патчкордами согласно рисункам 2 и 3.

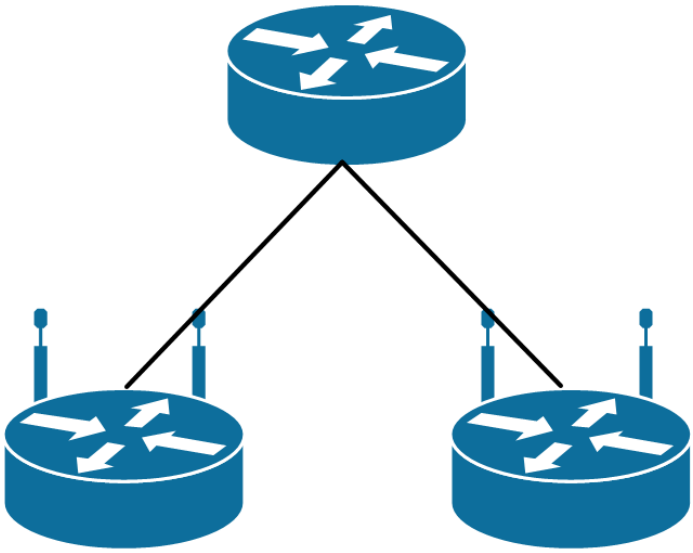


Рисунок 1 – Топология сети

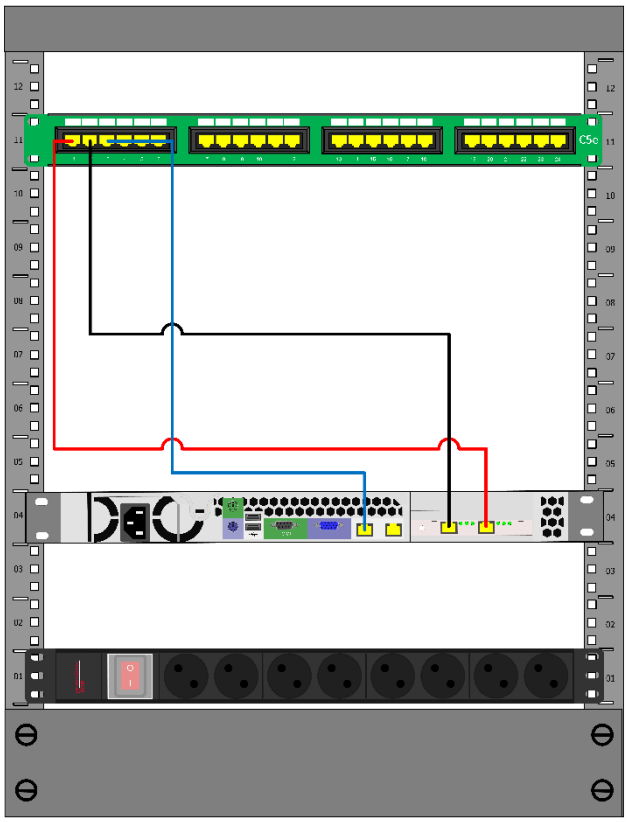


Рисунок 2 – Схема подключения телекоммуникационного шкафа

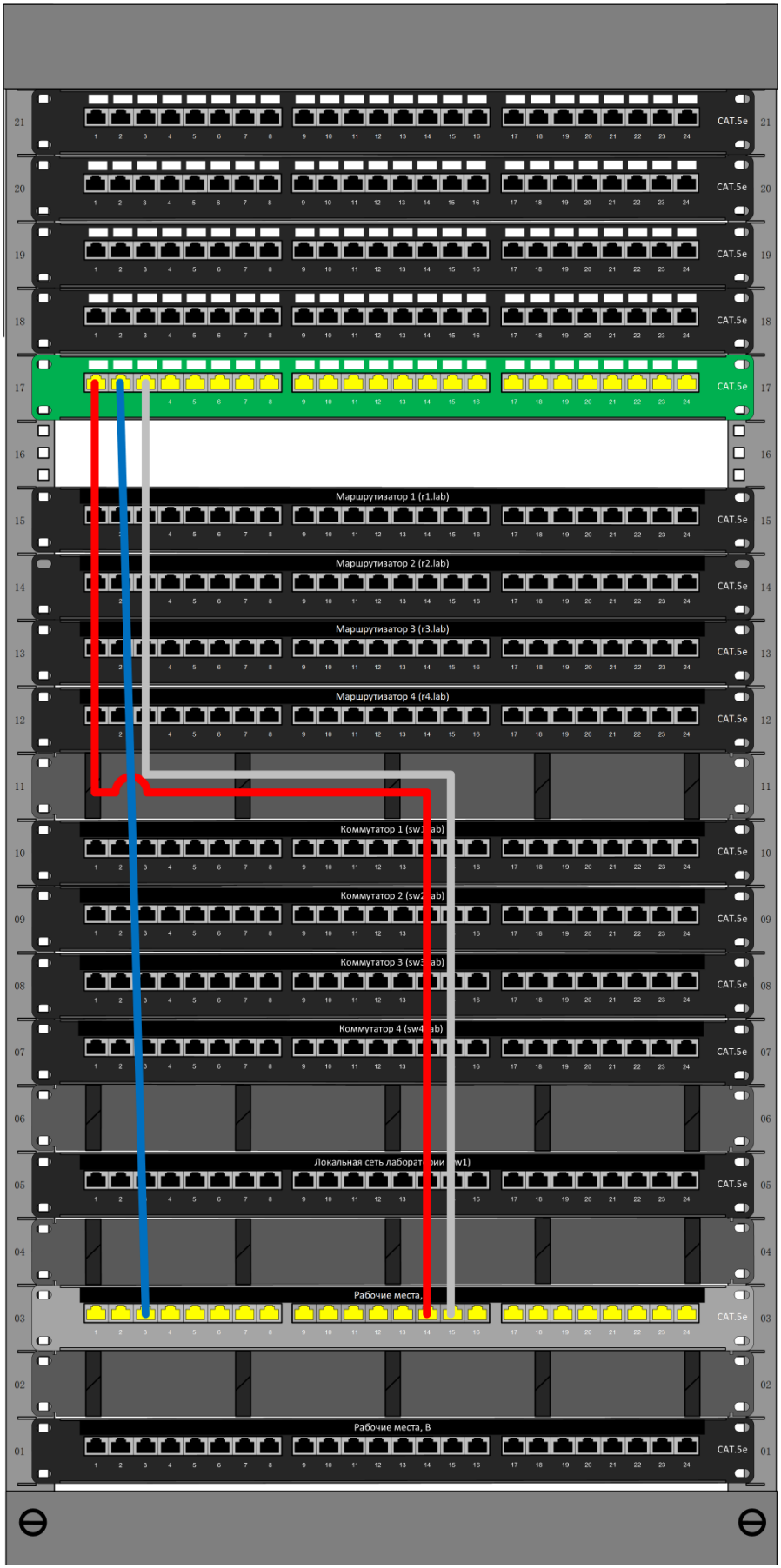


Рисунок 3 - Соединения на коммутационном поле

Для доступа к маршрутизатору используйте терминальный сервер с заранее предустановленной утилитой Winbox. Скачать Winbox можно со страницы загрузки. Рекомендованная версия Winbox v3.43 для RouterOS v7. С помощью Winbox проведите конфигурацию роутеров.

В Winbox для входа в маршрутизатор выберите вкладку Neighbors, в списке должны отображаться все устройства, доступные в локальном сегменте сети. Необходимо выбрать маршрутизатор MikroTik с MAC-адресом 00:1B:21:01:33:26, после чего поле **Connect** будет автоматически заполнено MAC-адресом устройства. Далее введите имя пользователя **admin**, поле пароля оставьте пустым (если пароль не был задан ранее) и нажмите кнопку **Connect**. После успешной аутентификации будет выполнен вход в систему управления маршрутизатором.

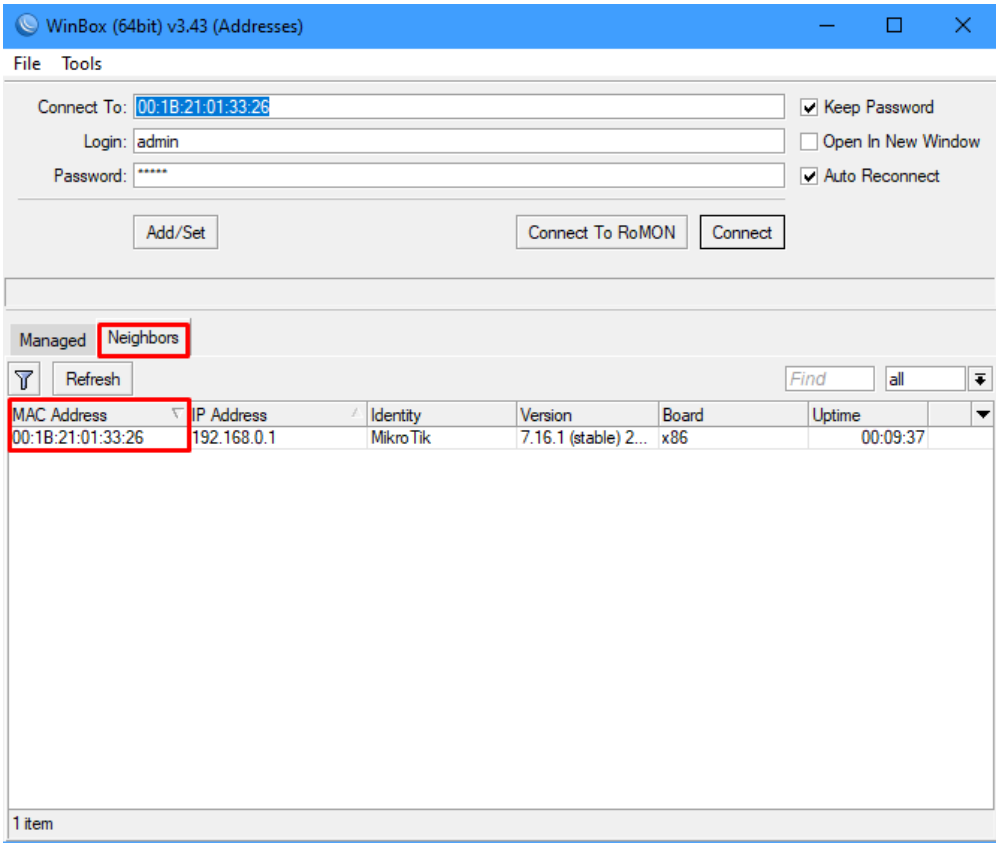


Рисунок 4 – Вход на маршрутизатор MikroTik

Приступим к начальной настройке маршрутизатора. Создадим интерфейс bridge1.

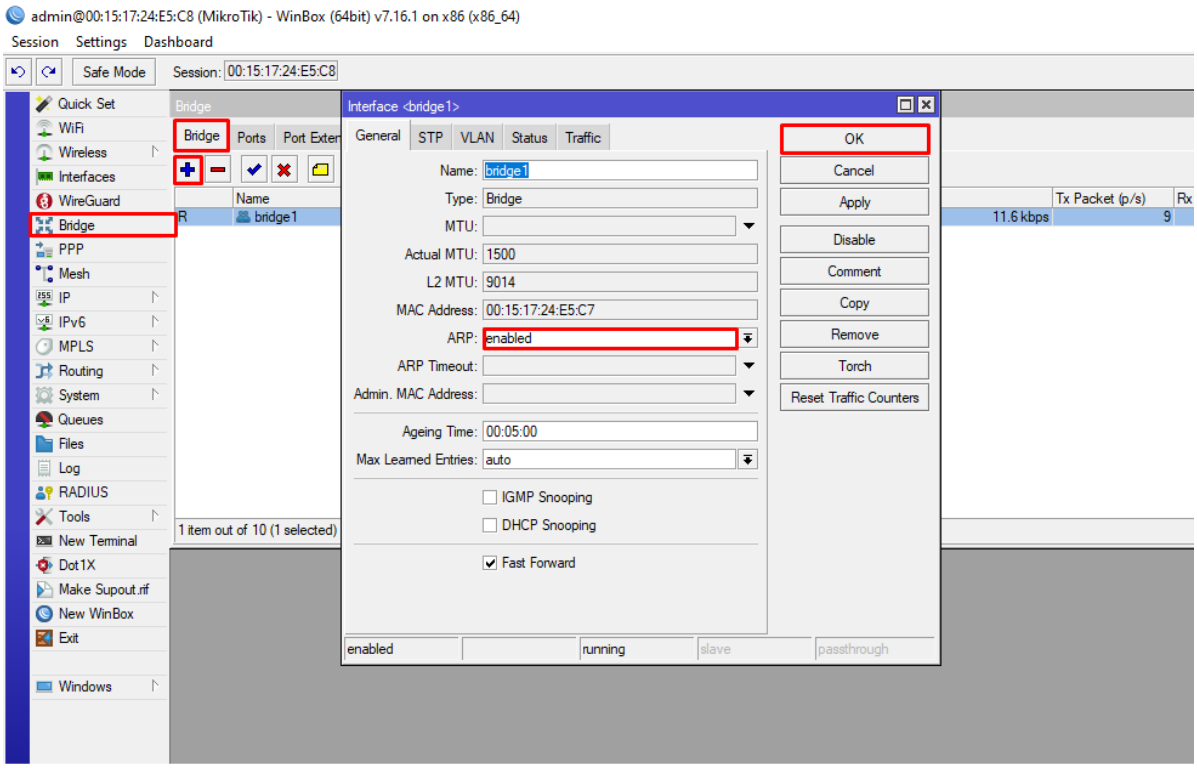


Рисунок 5 – Создание bridge интерфейса

Добавим в него все физические интерфейсы, для того чтобы все подключённые к маршрутизатору устройства находились в одном широковещательном домене.

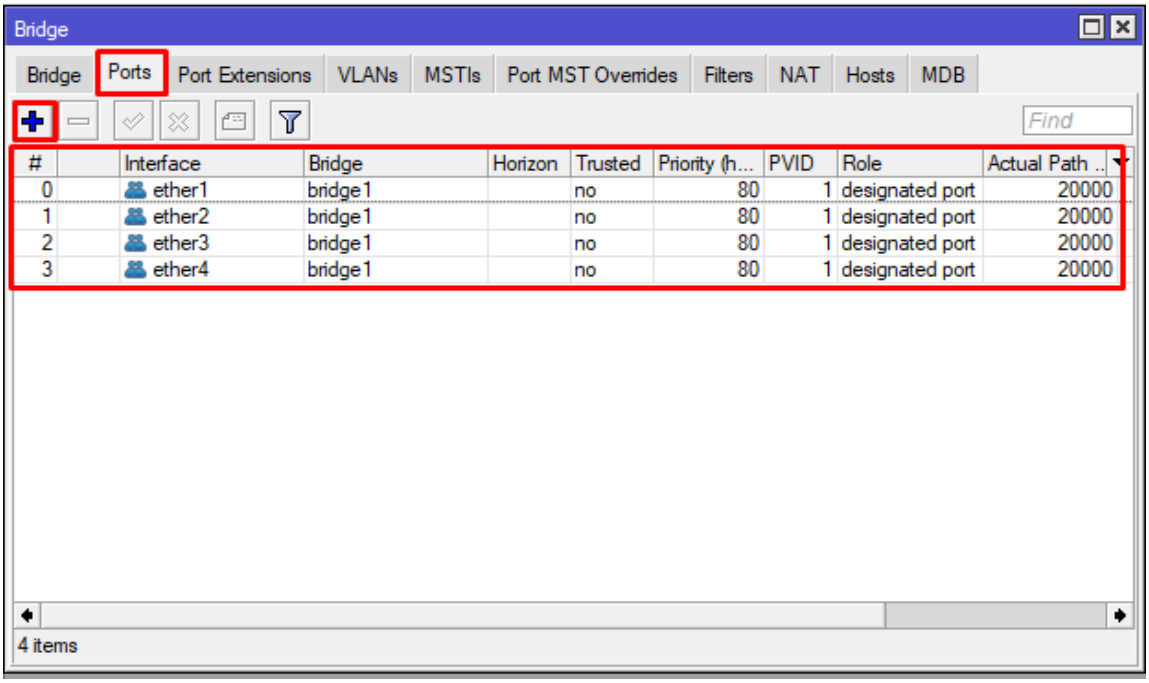


Рисунок 6 – Добавление интерфейсов в bridge

Назначим ip-адрес интерфейсу bridge1 (в дальнейшей адрес будет использоваться для DHCP-сервера).

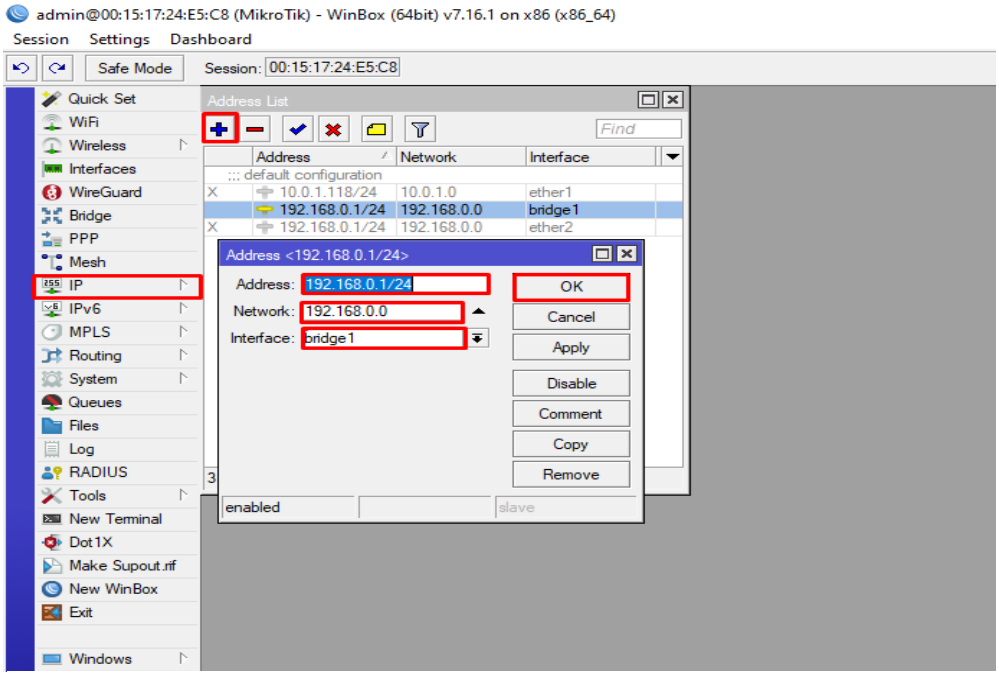


Рисунок 7 – Назначение ip-адреса интерфейсу bridge1

Настроим DHCP-сервер. Создадим пул IP-адресов (рисунок x). Созданный пул адресов будет использоваться DHCP-сервером для распределения IP-адресов в заданной подсети.

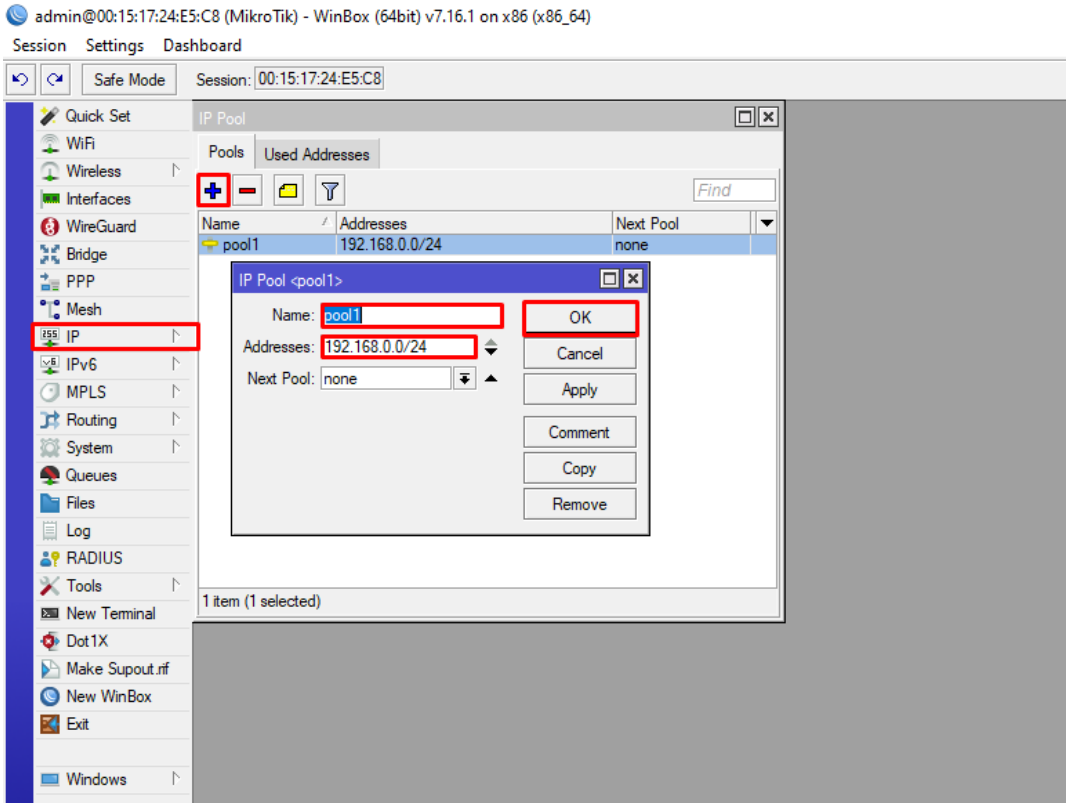


Рисунок 8 – Создание пула ip-адресов

Следующим шагом создадим DHCP-сервер.

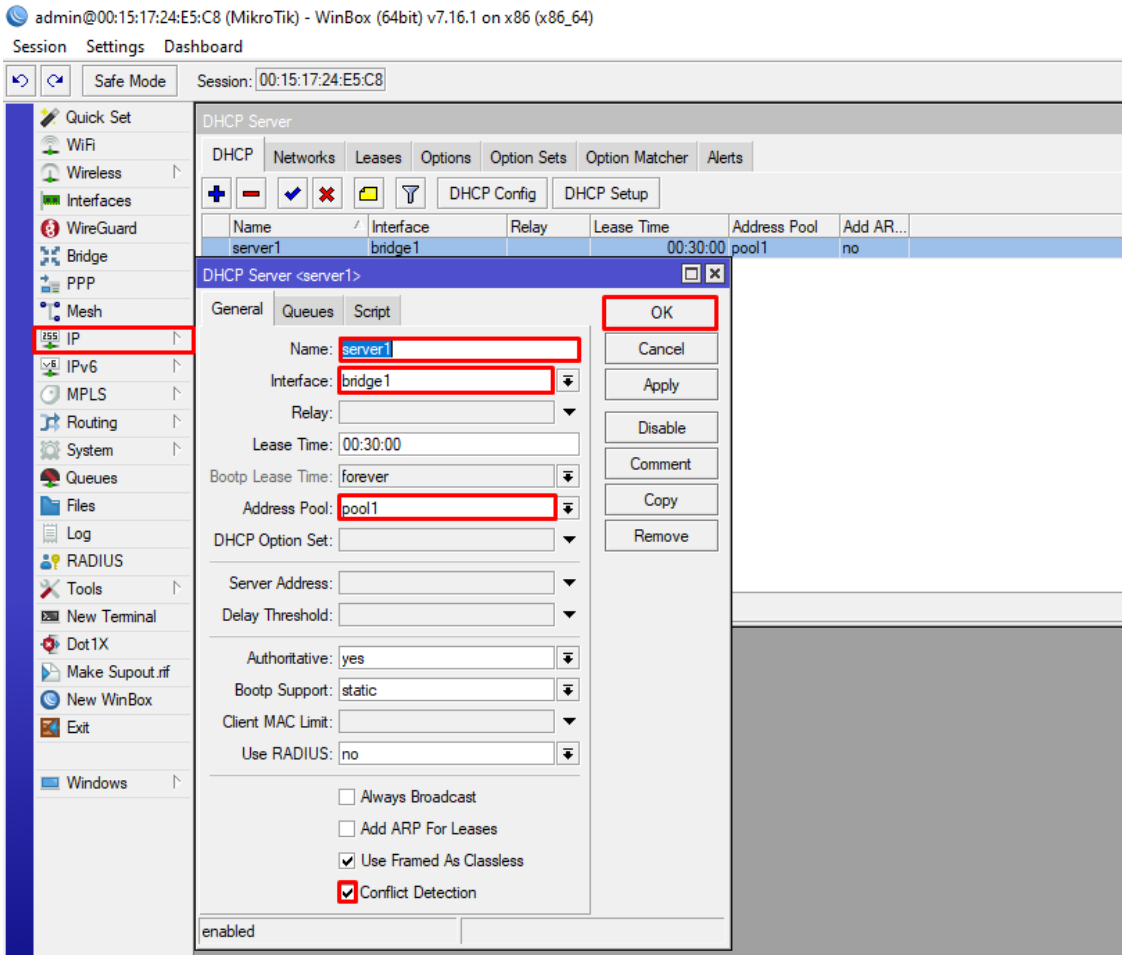


Рисунок 9 – Создание DHCP-сервера

Перейдем во вкладку **Networks**. В открывшемся окне указываем адрес сети и маску подсети. Значение сети должно соответствовать адресу подсети, для которой ранее был создан пул IP-адресов (**IP Pool**). Обязательно укажем ip-адрес контроллера в строке **CAPS Manager**, нужно это для того, чтобы точка доступа вместе с ip-адресом, получила от DHCP-сервера дополнительно адрес контролёра **CAPsMAN**.

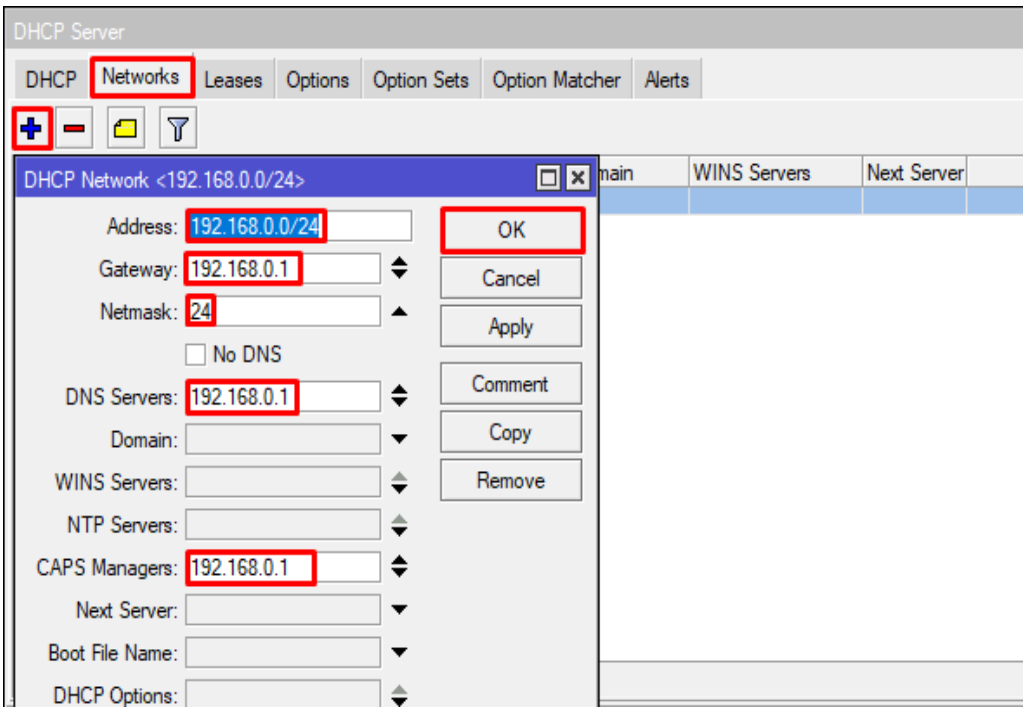


Рисунок 10 – настройка сети для DHCP-сервера

Настройка **CAPsMAN**

Перейдем в раздел WI-FI, откроем вкладку Channels (Рисунок x).

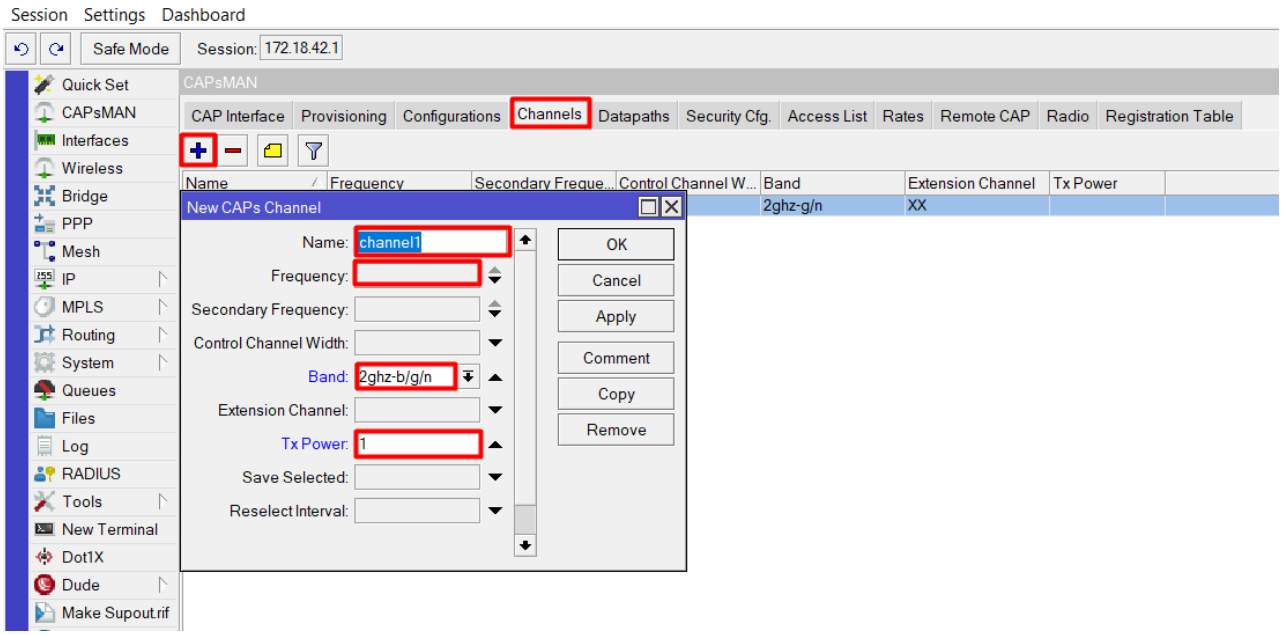


Рисунок 11 – Настройка канала WI-FI

Здесь заполним поля **Name**, **Band и Tx Power**, поле **Frequency** оставим без изменения. (Если не указать частоту, то она будет выбрана автоматически)

Для большей совместимости следует указать WI-FI стандарты (**Band**), на которых будет работать точка доступа. В поле мощность беспроводного передатчика (**Tx Power**) укажем 1. Значение **Tx Power** установлено в 1dBm для уменьшения радиуса покрытия каждой точки доступа. Чтобы в рамках лаборатории смоделировать перемещение Wi-Fi клиента между зонами покрытия разных точек доступа и наглядно увидеть процесс переключения. На рисунке 12 представлена примерная карта покрытия Wi-Fi лаборатории 128, построенная с учетом заданной мощности передатчика равной 1dBm.

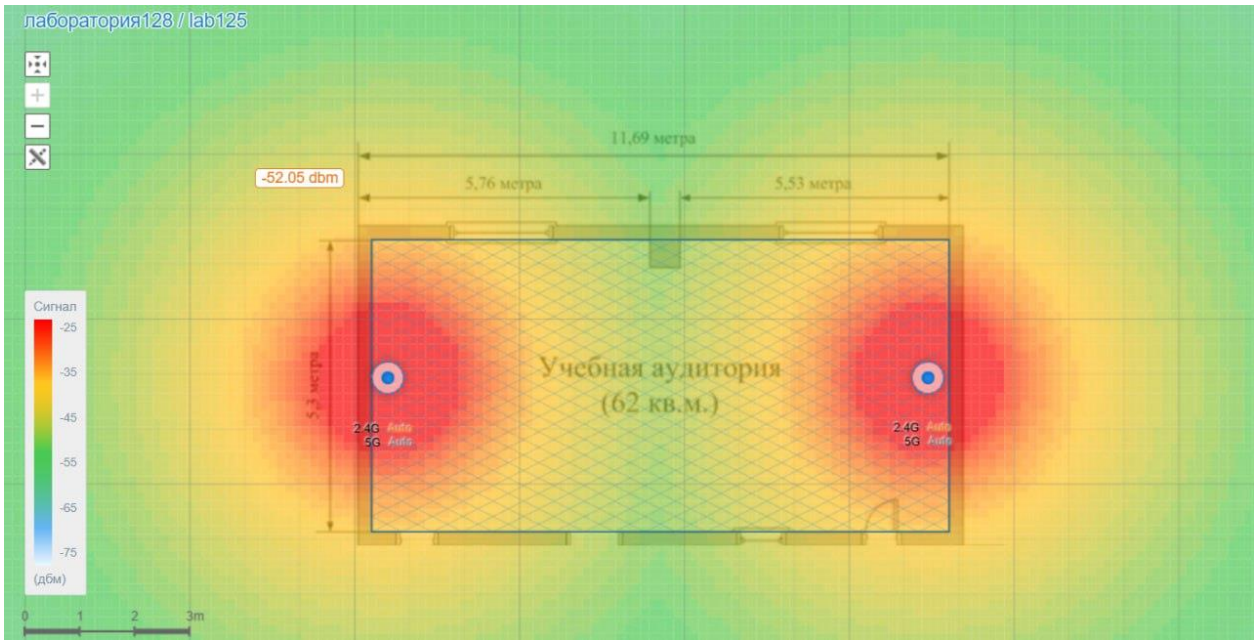


Рисунок 12 – Карта покрытия Wi-Fi лаборатории 128

Во вкладке **Security** укажем имя профиля, тип авторизации **Autentification Type WPA2-PSK** (по желанию можно указать больше, опять же для большей совместимости устройств). Алгоритм шифрования **Encryption** TKIP, а также **Passphrase** – пароль для аутентификации пользователей.

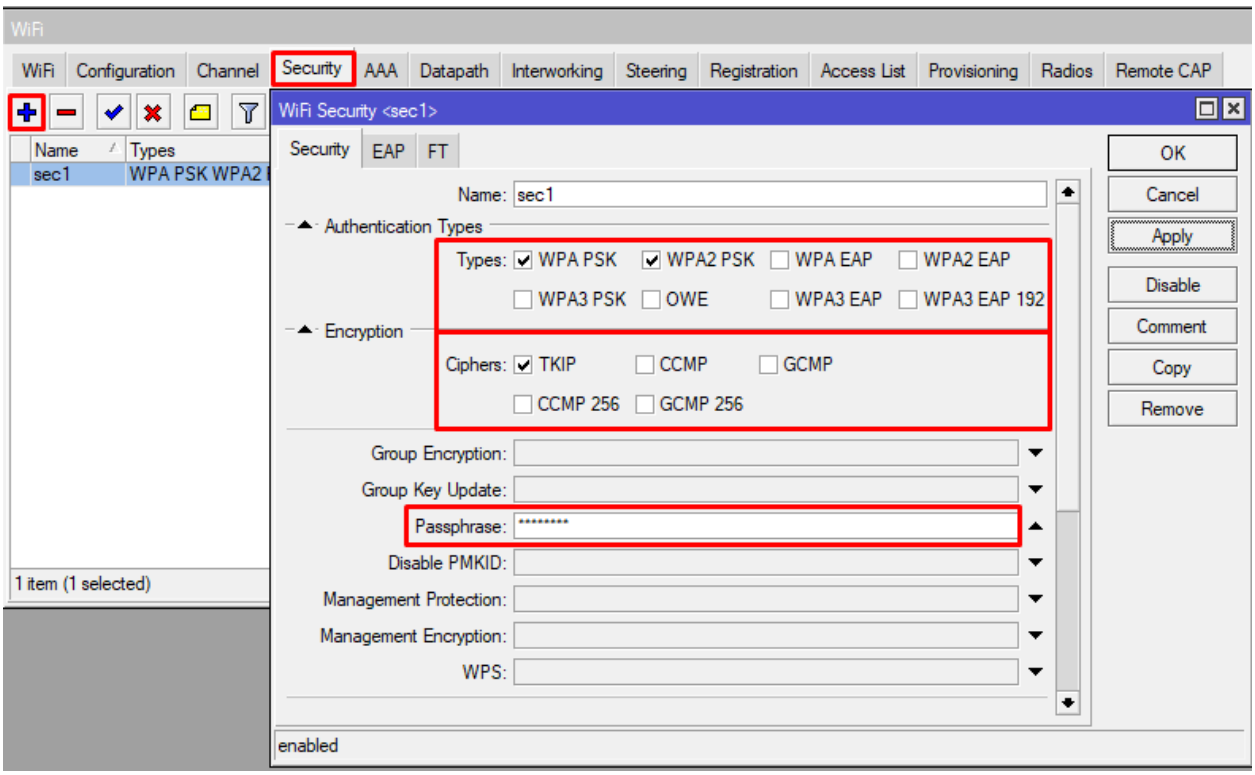


Рисунок 13 – Конфигурация параметров безопасности

Перейдем во вкладку **Datapaths.** Здесь нужно указать куда будет идти трафик от точек доступа. В поле Bridge выбираем ранее созданный мост **bridge1**.

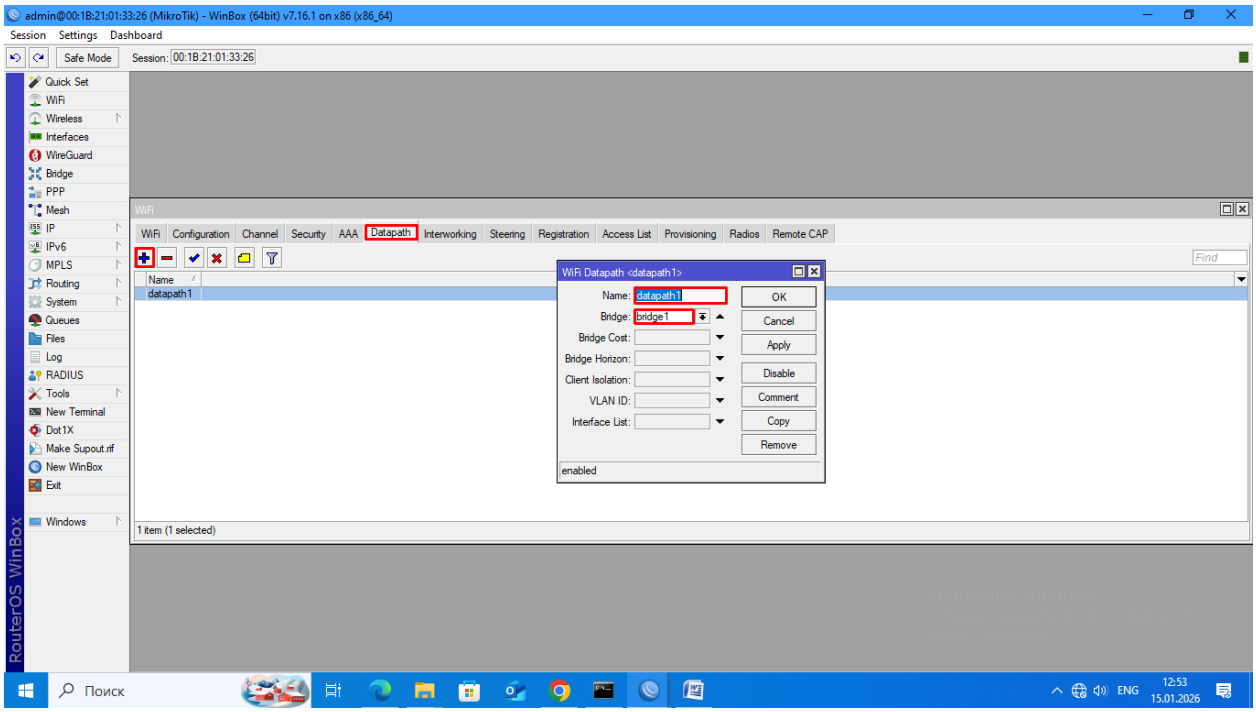


Рисунок 14 – Настройка Datapaths

Все вышеперечисленные настройки нужны для того, чтобы создать единую конфигурацию, которая будет распространяться на подключенные точки доступа.

Во вкладке **Configuration** зададим имя конфигурации**,** режим работы **(ap)** и имя беспроводной сети **(SSID).** В поле **Manager** выберем **local.** Этот режим означает, что устройство использует локальные настройки, прописанные непосредственно в ее конфигурации (на точках доступа в этом поле будет использоваться режим **capsman**, что означает что устройство ожидает получение конфигурации от контроллера, а не использует локальные настройки).

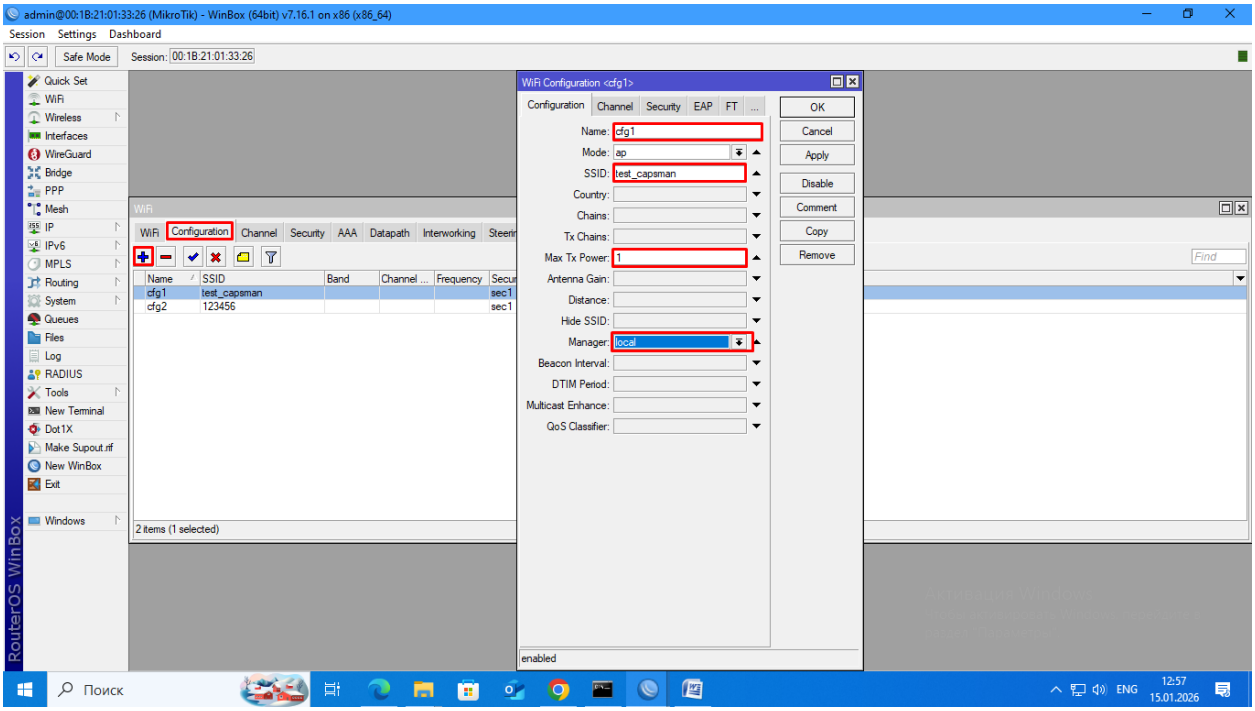


Рисунок 15 – Создание единой конфигурации точек доступа

Во вкладке Channel. Выберем ранее созданный канал. Во вкладках Security и Datapaths также выберем ранее созданные шаблоны.

Теперь необходимо настроить правило распространения конфигурации (**Provisioning**). Для этого во вкладке **Provisioning** создадим новое правило. Здесь указываем, какая конфигурация будет применяться к подключающимся точкам доступа и каким устройствам она будет распространяться.

В поле **Radio MAC** запишем **00:00:00:00:00:00**. Это означает, что правило не привязано к конкретной точке доступа (к конкретному MAC-адресу или группе MAC-адресов) и будет применяться ко всем устройствам, подключающимся к контроллеру. В **Action** выбираем create dynamic enabled, чтобы в контроллере CAPsMAN автоматически создавались интерфейсы подключаемых точек. В поле **Master Configuration** выберем созданную ранее конфигурацию.

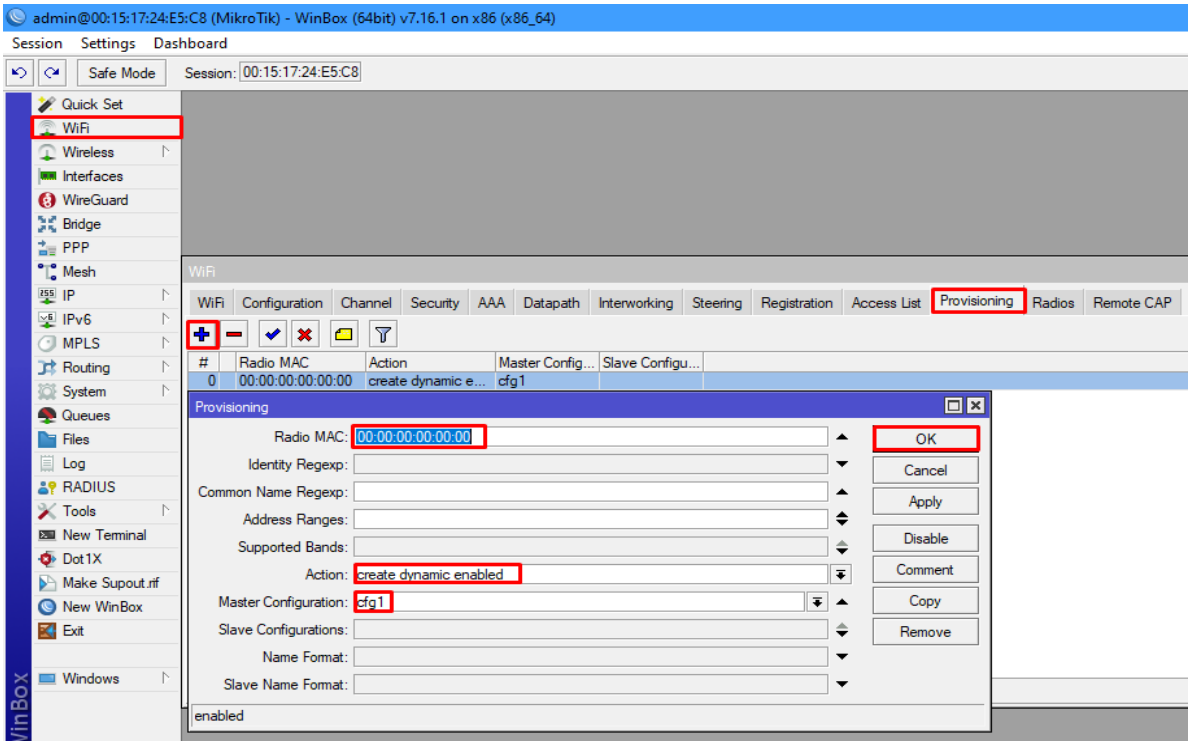
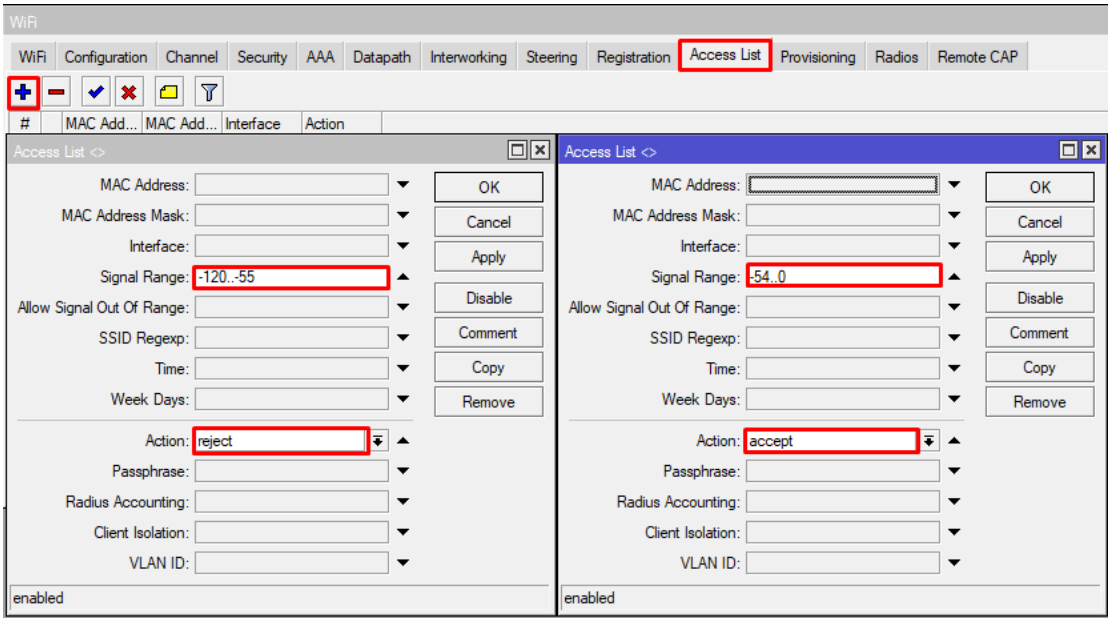


Рисунок 16 – Настройка правила распространения конфигурации

Ранее мы уменьшили мощность передатчика (**Tx Power** = 1dBm), чтобы ограничить радиус действия точек доступа в рамках лаборатории. Однако этого недостаточно — клиентское устройство может не переключаться на другую точку доступа даже при слабом сигнале, если настройки самого клиента не инициируют переключение.

Чтобы гарантировать переключение между точками, настроим **Access List** — правила, которые принудительно отключат клиента при падении уровня сигнала ниже



заданного порога. Во вкладке **Access List**, создадим два правила.

Чтобы активировать функцию контроллера беспроводной сети, во вкладке Remote CAP, нажимаем на CaPsMAN, ставим галочку Enabled и выбираем интерфейс bridge1

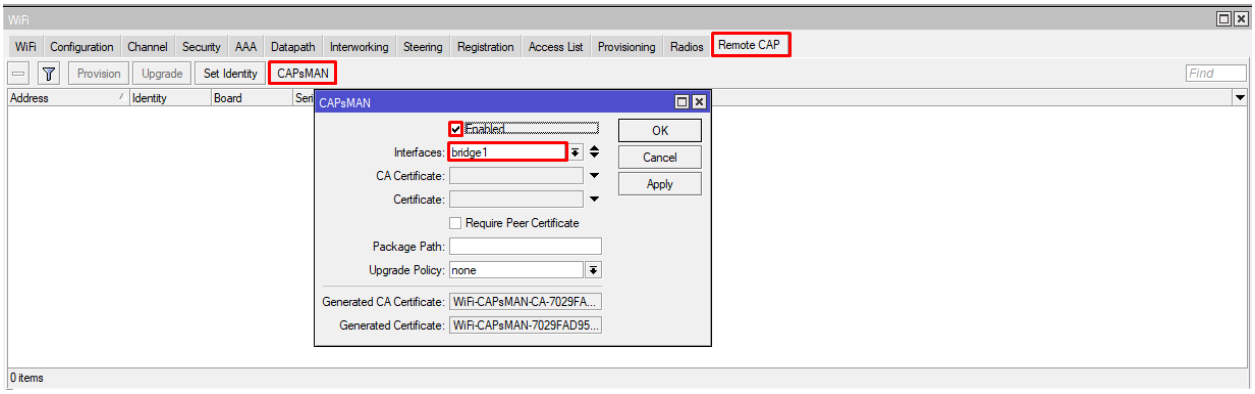


Рисунок 18 – Включение CAPSMAN

Рисунок 17 – Создание access list

Все корректно подключенные точки доступа должны отоораситься во вкладке Remote CAP.

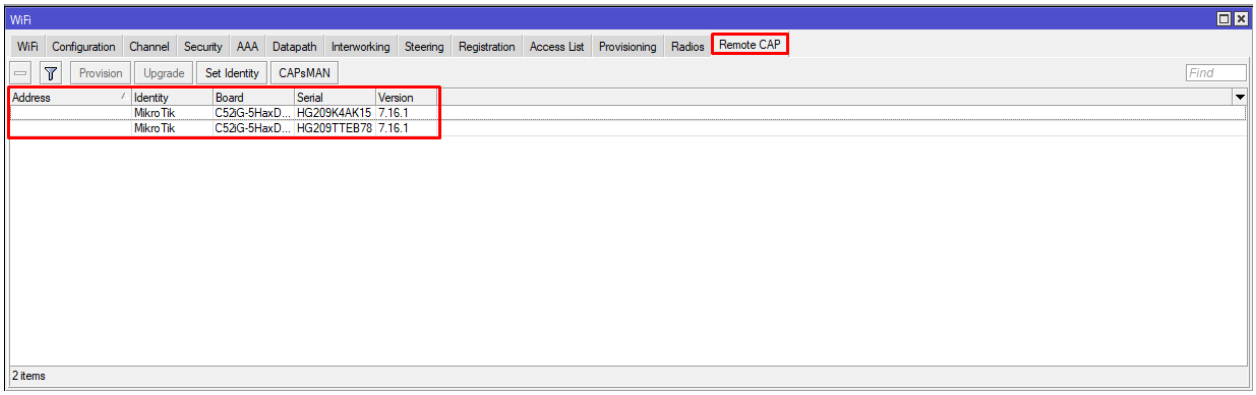


Рисунок 19 – Проверка подключения точек доступа к контроллеру

Для проверки работы подключитесь телефоном к созданной Wi-Fi сети. Во вкладке **Registration Table,** должны отображаться все подключенные устройства.

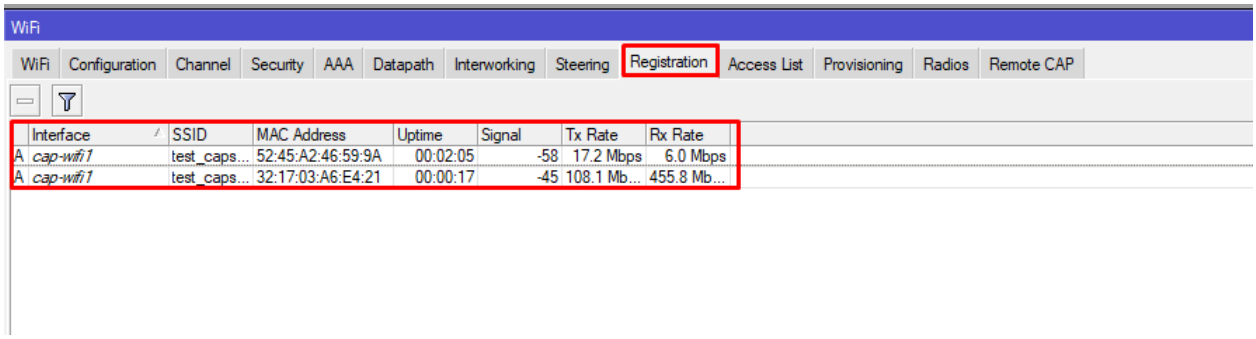


Рисунок 20 – Таблица подключенных устройств

Передвигайтесь от одной точке доступа к другой и вы увидите автоматическое переключение клиента между точками, о чем соответствует запись в логе представленном на рисунке 21.

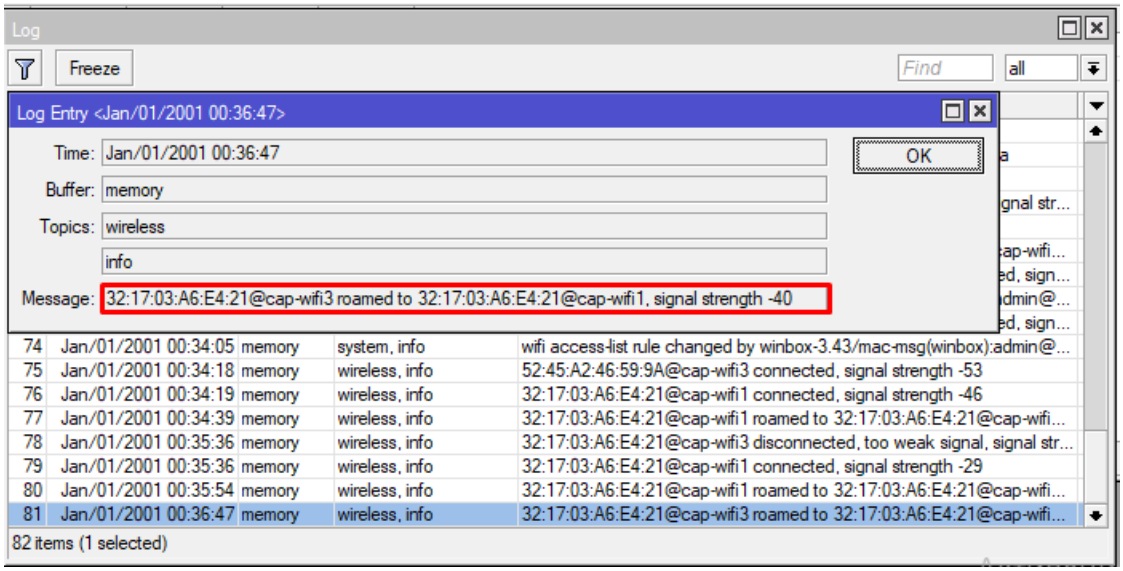


Рисунок 21 – Запись в логе о переключение клиента между точками доступа