

Начиная с версии 6.11 в Router OS появился функционал по **управлению точками доступа**. Теперь нет необходимости настраивать по отдельности каждую точку, достаточно настроить контроллер и подключать к нему управляемые точки доступа. В результате очень быстро и просто мы имеем **бесшовный wifi роуминг** на множество точек, позволяющих покрыть **единой сетью wifi** практически любой по площади объект.

Если у вас есть желание научиться работать с роутерами микротик и стать специалистом в этой области, рекомендую по программе, основанной на информации из официального курса **MikroTik Certified Network Associate**. Курс стоящий, все подробности читайте по ссылке.

Данная статья устарела. Есть свежий материал на тему настройки capsman v2 в mikrotik. Там более подробное описание и полезные примеры. Рассмотрены нововведения v2 и отличие от предыдущей версии.

Содержание:

- 1 Активируем функцию контроллера wifi на Mikrotik RouterBOARD 2011UiAS-2HnD-IN
- 2 Настраиваем CAPsMAN на wifi контроллере Mikrotik RouterBOARD 2011UiAS-2HnD-IN
- 3 Подключаем управляемые wifi точки доступа

Для примера возьмем трехэтажный коттедж с подвалом и расположим на каждом этаже по точке, решив таким образом проблему **единой wifi сети в коттедже**. В моем распоряжении оказались 4 новых точки доступа **RouterBOARD 2011UiAS-2HnD-IN**, с ними я и буду работать.

## Активируем функцию контроллера wifi на Mikrotik RouterBOARD 2011UiAS-2HnD-IN

Начнем настройку точек доступа. Первым делом после запуска роутера я удаляю конфигурацию по-умолчанию, сбрасываю настройки в дефолтные и объединяю все порты + wifi в bridge1. Подробнее о начальной настройке микротиков я рассказал отдельно, рекомендую ознакомиться.

Для активации функции контроллера необходимо установить обновление системы до последней, либо до любой, от 6.11 и выше. Чтобы обновить систему идем в раздел **System - Packages** и ждем Check For Updates. Роутер должен иметь доступ в интернет для обновления.



Видим доступные обновления и нажимаем Download & Upgrade. Роутер скачает прошивку, обновит ее и перезагрузится.



Теперь надо активировать пакет, содержащий необходимый нам функционал. По-умолчанию он отключен. Для включения идем опять в **System - Packages** и выбираем пакет **wireless-fp**, нажимаем enable. Пакет помечается как активный, но включится только после перезагрузки роутера.



Перезагружаем роутер. Пакет **wireless-fp** активируется, а **wireless** деактивируется. Теперь у нас появляется новый пункт настроек **CAPsMAN**:



В этом разделе осуществляются все настройки управляемых точек доступа. Принцип действия следующий. Вы создаете необходимые конфигурации wifi для точек доступа, потом в настройках беспроводных интерфейсов точек указываете, что настройки хранятся на контроллере. После подключения к контроллеру, точки получают ту или иную конфигурацию, при этом управление настроек с самих устройств становится невозможным. Конфигурации для разных точек могут быть разные.

Мы рассмотрим самый простой вариант: один контроллер и управляемые им точки доступа с единой конфигурацией. Настроив одну точку и сохранив ее конфигурацию, можно распространить настройку на сколь угодно много точек. Все они, по мере подключения, будут подключаться к контроллеру и применять необходимые настройки wifi.

Я расположил Mikrotik, который будет выполнять роль контроллера на одном этаже здания, управляемые точки установил на остальных. Задача получить полное покрытие всех этажей **единой сетью wifi**. При этом, находясь на одном из этажей, есть прием сигнала с обеих точек, с той которая на этом же

этаже уверенный мощный сигнал, с другого этажа очень слабый, на грани возможности использования. Подключенные к сети устройства должны автоматически переключаться на ту точку доступа, у которой увереннее сигнал. Забегая вперед скажу, что так и будет. Настроив все должным образом я получал переключение к разным точкам при перемещении с этажа на этаж. Итак, приступим к настройке.

## Настраиваем CAPsMAN на wifi контроллере Mikrotik RouterBOARD 2011UiAS-2HnD-IN

Для удобства, я назвал контроллер ar-master, а управляемые точки ar-1, ar-2, ar-3. Первым делом включаем на контроллере непосредственно функционал контроллера. Для этого заходим в **CAPsMAN**, нажимаем на **Manager** и ставим галочку Enable. Остальные пункты не трогаем.



Теперь здесь же открываем закладку **Channels** и создаем настройки канала:



Потом в **Datapaths** и создаем настройки:



Далее создаем настройки **Security Cfg.:**



Мы задали основные настройки. Теперь объединим их все в **единую конфигурацию**. Делается это в закладке **Configurations**. Создаем там новую конфигурацию. Указываем SSID нашей wifi сети. Для активации обеих антенн роутера отмечаем галками пункты HT Tx Chains и HT Rx Chains. На остальных трех вкладках указываем созданные нами ранее конфигурации. Остальные поля не трогаем, они будут заполнены автоматически на основе настроек.



После создания конфигурации, создаем правило ее распространения. У нас случай самый простой, единая конфигурация для всех точек. Идем во вкладку **Provisioning** и создаем правило. Поле **Radio MAC** оставляем по-умолчанию, в **Action** выбираем **create dynamic enabled**, в Master Configuration выбираем ранее созданную конфигурацию.



## Подключаем управляемые wifi точки доступа

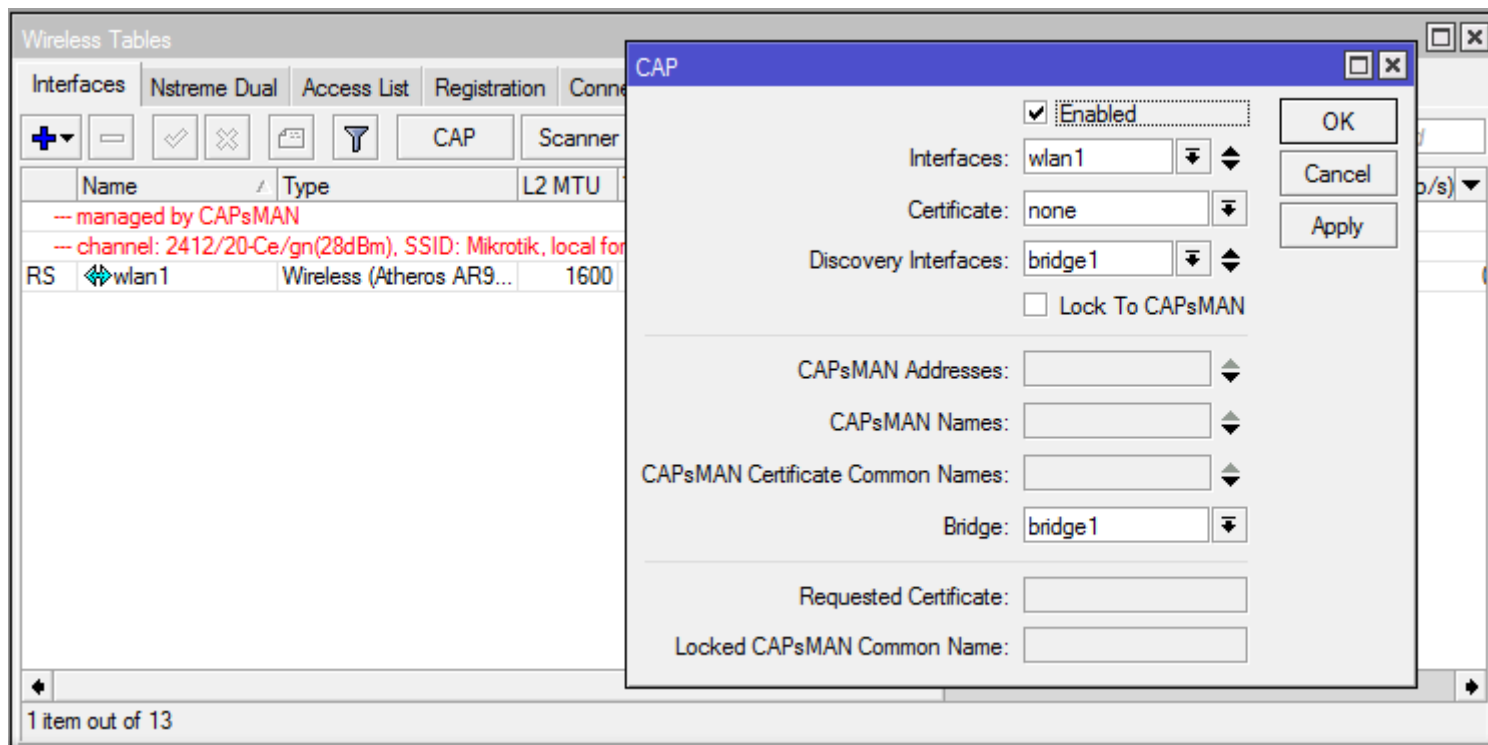
С настройками закончили. Теперь надо подключить точки доступа. ap-master выступает в качестве контроллера сети и одновременно с этим является управляемой точкой. Указываем его wifi интерфейсу брать настройки с контроллера. Для этого идем в раздел **Wireless**, нажимаем **CAP**, ставим галочку Enabled. В поле **CAPsMAN Addresses** вводим IP адрес контроллера, то есть адрес этой же точки. Обращаю внимание на то, что при подключении других точек, не являющихся одновременно контроллером, эти настройки будут немного другими. Указываем в поле **Bridge** Остальные поля не трогаем. Жмем ОК.



Wifi адаптер подключился к контроллеру и взял необходимые настройки. Об этом свидетельствуют две красные строчки, появившиеся после подключения.



**Wifi сеть с контроллером** создана, к ней можно подключиться и пользоваться. Подключим к ней теперь еще одну точку. Обновляем ее до последней версии, соединяем кабелем с контроллером, назначаем адрес, проверяем связь обоих роутеров друг с другом. Если все в порядке, то подключаем точку к контроллеру. Идем в раздел **Wireless**, жмем **CAP**. В поле **Discovery Interface** указываем bridge1. Как я уже писал раньше, у меня в бридж объединены все порты + wifi. В поле **Bridge** тоже указываем bridge1.



Точка доступа подключится к контроллеру, возьмет настройки и начнет раздавать wifi. Таким же образом настраиваем и подключаем остальные 2 точки. В итоге получаем такую картину:



У нас 4 виртуальных интерфейса, соответствующие каждому wifi адаптеру управляемых точек доступа. Здесь можно управлять настройками этих точек. К примеру, создать разные конфигурации и здесь их распределить между точками. Распределять можно и в автоматическом режиме, на основе MAC адресов. Делается это во вкладке **Provisioning**. На вкладке **Registration Table** отображается информация от подключенных к wifi устройствам, с указанием интерфейсов, к которым они подключены:



На вкладке **Radio** можно увидеть соответствие точек созданным виртуальным интерфейсам:



Собственно, на этом настройка закончена. После окончания я, вооружившись смартфоном с софтом по анализу wifi сетей, походил по зданию и убедился, что во всем здании функционирует единая wifi сеть и происходит автоматическое переключение от одной точки к другой при значительном ухудшении сигнала от предыдущей точки.

Помогла статья? Подписывайся на telegram канал автора

Анонсы всех статей, плюс много другой полезной и интересной информации, которая не попадает на сайт.

---

**Рекомендую полезные материалы по схожей тематике:**

## Онлайн курсы по Mikrotik

Если у вас есть желание научиться работать с роутерами микротик и стать специалистом в этой области, рекомендую пройти курсы по программе, основанной на информации из официального курса **MikroTik Certified Network Associate**. Помимо официальной программы, в курсах будут лабораторные работы, в которых вы на практике сможете проверить и закрепить полученные знания. Все подробности на сайте . Стоимость обучения весьма демократична, хорошая возможность получить новые знания в актуальной на сегодняшний день предметной области. Особенности курсов:

- Знания, ориентированные на практику;
- Реальные ситуации и задачи;
- Лучшее из международных программ.

- Используя функционал Mikrotik, выполняем блокировку социальных сетей.
- Защищаем локальную сеть с помощью простого фаервола на Mikrotike.
- Собираем логи микротик с помощью rsyslog.
- Настройка отказоустойчивого подключения интернет с помощью 2-х WAN каналов.