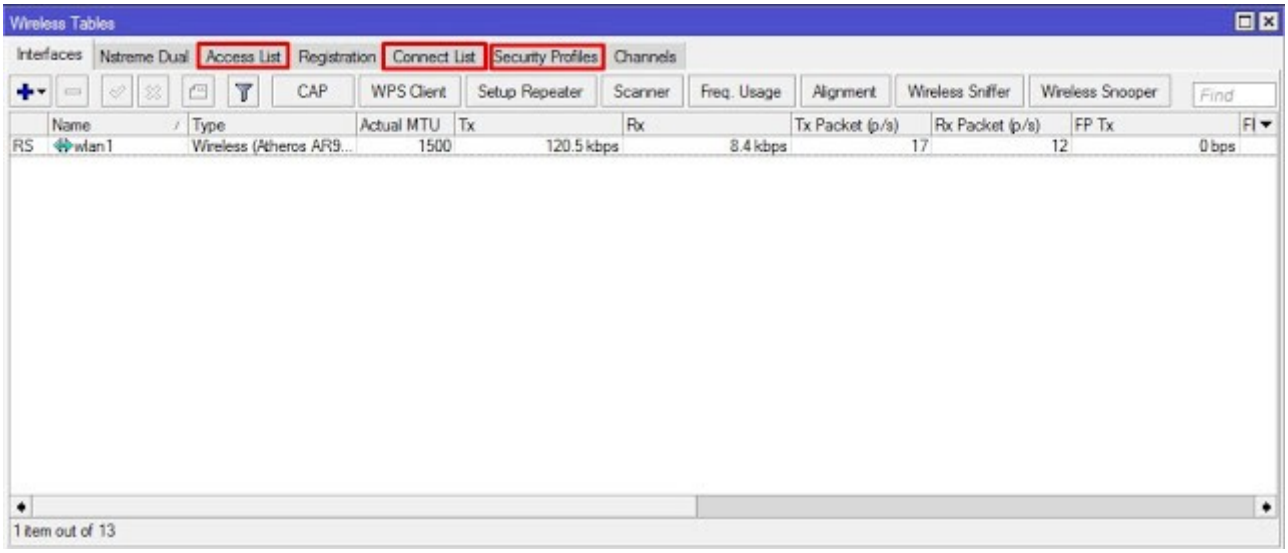
MikroTik / RouterOS
Настройки параметров WPA2

За защиту WiFi сети в Mikrotik отвечают три вкладки:

Access List (/interface wireless access-list), Connect List (/interface wireless connect-list), Security Profiles (/interface wireless security-profiles).



Access List - список правил, которые ограничивают соединения других устройств к вашей точке, а также служат для управления параметрами подключения. (режим ap mode).

Пример: вы хотите ограничить подключение к вашей точке доступа по MAC-адресам.

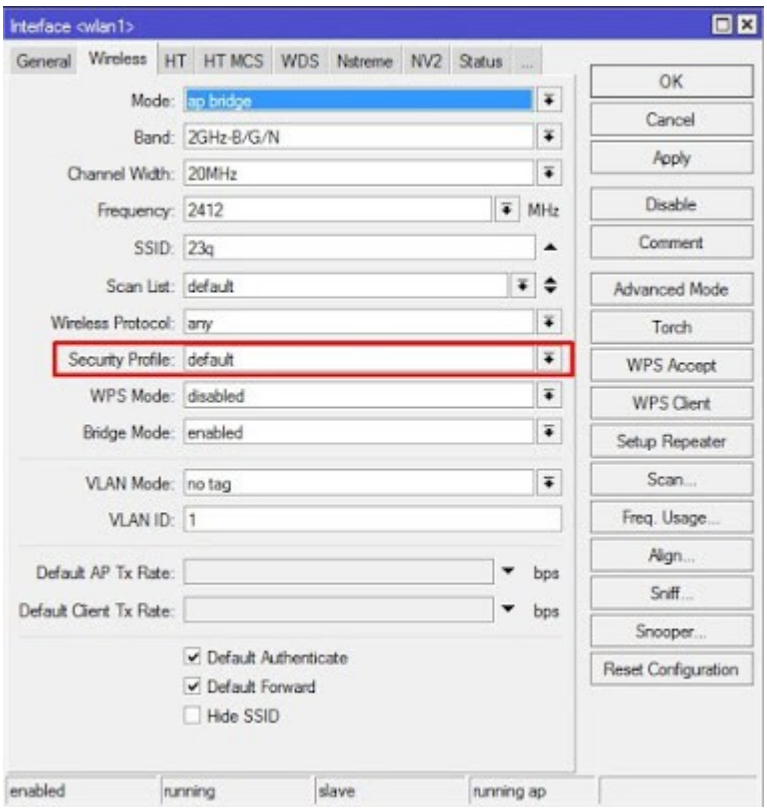
Connect List - список правил, которые ограничивают соединение вашего устройства к другим точкам доступа (режим station mode).

Пример: вы хотите автоматически подключать свою клиентскую станцию к точке доступа с максимальным уровнем сигнала (при наличии нескольких базовых станций).

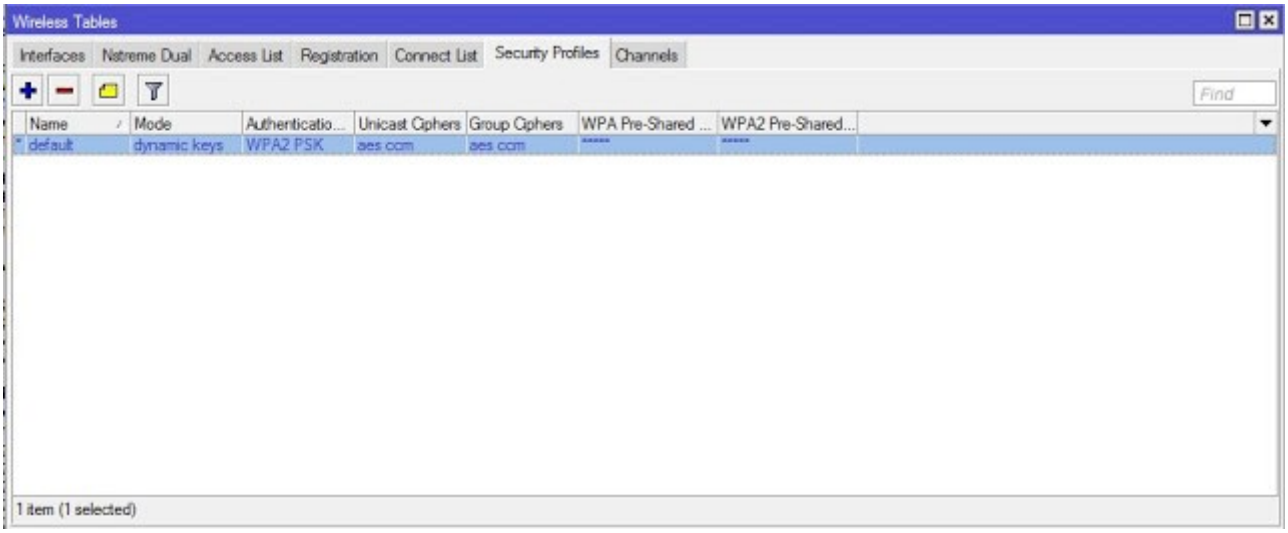
Security Profiles - настраиваются профили методов защиты и, непосредственно, ключи защиты беспроводной сети.

Security Profiles

Начнем с самого интересного - Security Profiles. Именно здесь мы настраиваем шифрование для наших беспроводных точек. Настройка будет осуществляться для домашней или офисной точки доступа. Профиль защиты выставляется непосредственно в свойства беспроводного интерфейса.

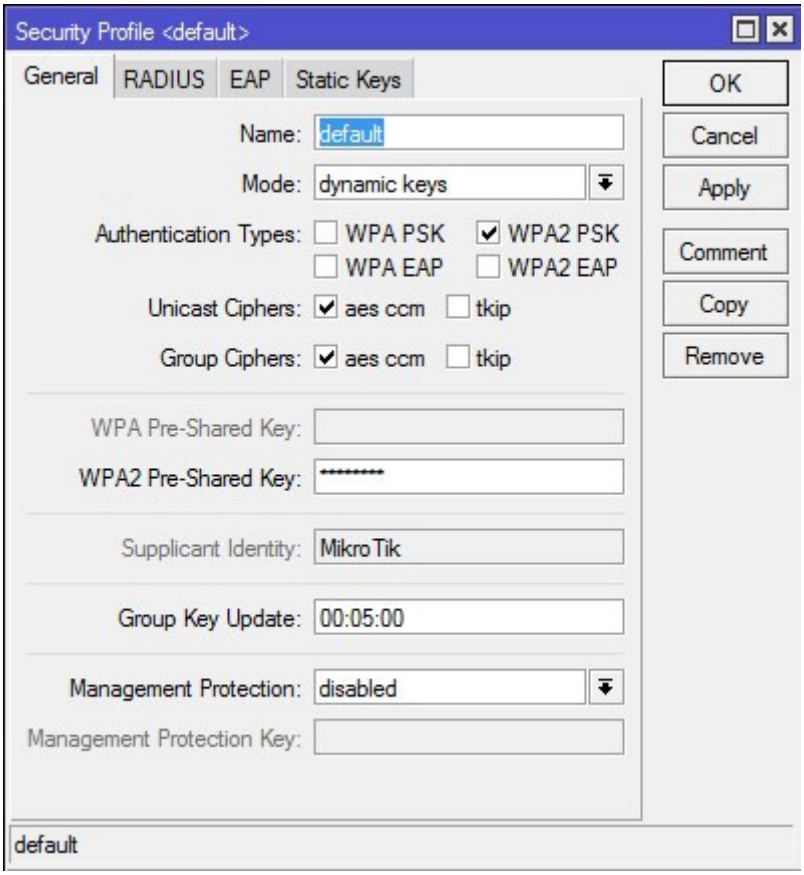


При переходе на вкладку /interface wireless security-profiles видим такую картину.



Вы можете добавить свой профиль, я всегда использую стандартный - че добру пропадать =).

Вкладка General.



Name - имя профиля.
Если используем стандартный профиль - оставляем по-умолчанию.

Mode - режим шифрования.

- none - шифрование не используется. Зашифрованные кадры не принимаются. Широко используется в системах гостевого доступа, вроде предоставления Интернета в кафе или гостинице. Для подключения нужно знать только имя беспроводной сети.
- static-keys-required - WEP-режим. Не принимать и не посылают незашифрованные кадры. Скомпроментированый протокол. Использовать нельзя, или в крайних случаях (для старых устройств). Основная статья - Настройка WEP-шифрования.
- static-keys-optional - WEP-режим. Поддержка шифрования и дешифрования, но также позволяют получать и отправлять незашифрованные кадры. Использовать нельзя, или в крайних случаях (для старых устройств). Основная статья - Настройка WEP-шифрования.
- dynamic-keys - WPA режим.

*Для защиты беспроводной сети **ВСЕГДА** используем режим dynamic-keys.*

Authentication Types - набор поддерживаемых типов аутентификации. Клиент сможет подключится к точке доступа только если поддерживает данный тип аутентификации. Предлагаемые варианты: WPA-PSK , WPA2-PSK , WPA-EAP и WPA2-EAP. Техническое отличие WPA от WPA2 состоит в технологии шифрования, в частности, в используемых протоколах. В WPA используется протокол TKIP, в WPA2 – протокол AES. На практике это означает, что более современный WPA2 обеспечивает более высокую степень защиты сети. К примеру, протокол TKIP позволяет создавать ключ аутентификации размером до 128 бит, AES – до 256 бит. Фактически WPA2 представляет собой улучшенный WPA; WPA2 использует протокол AES, WPA – протокол TKIP; WPA2 поддерживается всеми современными беспроводными устройствами; WPA2 может не поддерживаться устаревшими операционными системами.

Разница между WPA2-PSK и WPA2-EAP состоит в том, откуда берутся ключи шифрования, используемые в механике алгоритма AES. Для частных (домашних, мелких) применений используется статический ключ (пароль, кодовое слово, PSK (Pre-Shared Key)) минимальной длиной 8 символов, которое задается в настройках точки доступа, и у всех клиентов данной беспроводной сети одинаковым. Компрометация такого ключа (проболтались соседу, уволен сотрудник, украден ноутбук) требует немедленной смены пароля у всех оставшихся пользователей, что реалистично только в случае небольшого их числа. Для корпоративных применений, как следует из названия, используется динамический ключ, индивидуальный для каждого работающего клиента в данный момент. Этот ключ может периодический обновляться по ходу работы без разрыва соединения, и за его генерацию отвечает дополнительный компонент — сервер авторизации, и почти всегда это RADIUS-сервер.
RADIUS-сервер мы не используем, сотрудники у нас говорливые, но и пароли мы меняем часто, поэтому наш выбор WPA2-PSK. Оставляем галочку только на нем, все другие "небезопасные" протоколы - отключаем.

Unicast Ciphers - выбор типа шифрования. Клиенты смогут подключиться в вашей точке, если поддерживают данный тип шифрования. Поддерживаются два типа tkip и aes-ccm. AES - это современный и более безопасный алгоритм. Он совместим со стандартом 802.11n и обеспечивает высокую скорость передачи данных. TKIP является устаревшим. Он обладает более низким уровнем безопасности и поддерживает скорость передачи данных вплоть до 54 МБит/сек. Кроме того, стандарт алгоритма CCM требует использования новых временных ключей для каждой вновь создаваемой сессии, а это плюс к безопасности.
Используем только aes-ccm.

Group Ciphers - выбор типа шифрования. Ваша станция будет пытаться подключиться только к тем точкам доступа, которые поддерживаю данный тип шифрования. Описание ничем не отличается от предыдущего параметра.
Используем только aes-ccm.

WPA-Pre-Shared Key, WPA2 Pre-Shared Key - значение ключа. Для задания пароля используйте цифры, буквы верхнего **И** нижнего регистра, Специальные символы (%, *, @, #, $, ~). Не забывайте регулярно менять пароль (например раз в 15 дней). Mikrotik позволяется сделать это скриптом, у меня так меняется пароль на 10 офисах одновременно, если интересно - могу описать в отдельной статье.

Используем сложный пароль.

Supplicant Identity - EAP-идентификатор, который посылается клиентом в начале аутентификации EAP. Это значение используется в качестве значения для атрибута User-Name в сообщениях RADIUS.
WPA2-EAP не используем - значение игнорируем.

Group Key Update - время как часто обновлять ключ шифрования. Функция не работает в режиме station. Фактически изменять значение можно при непонятных отвалах устройств (например Android-смартфонов при уходе в ждущий режим).
Значение оставляем по-умолчанию - 5 минут.

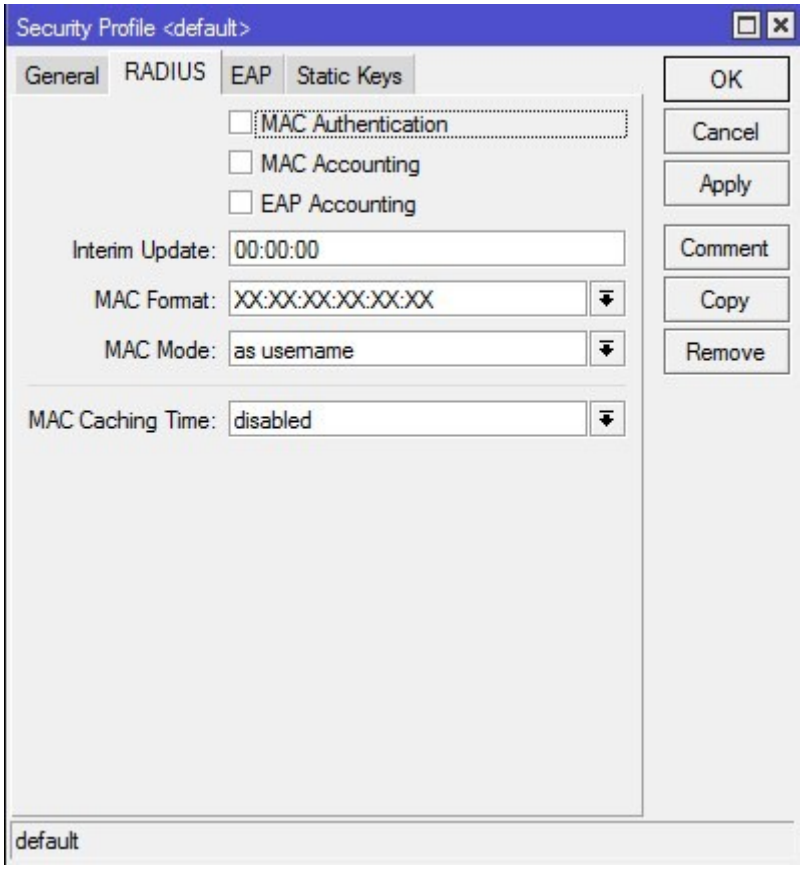
Managment Protection - защита от атак деаутентификации и клонирования MAC-адреса. Свой алгоритм защиты беспроводной сети от Mikrotik.

- disabled - защита управления отключена.
- allowed - разрешить использовать защиту, если это поддерживается удаленной стороной.
- required - требуется. Для базовой станции установить связь только с клиентами поддерживающими Managment Protection. Для клиентов - установить связь только с точками доступа поддерживающими Managment Protection.

Managment Protection не используем - оставляем disabled.

Managment Protection Key - ключ защиты Managment Protection.
Поле не активно, если не используется Managment Protection.

Вкладка RADIUS.



MAC Authentication - авторизация по mac-адресу. Эта настройка применяется к тем клиентам, которых нет в access-list. Сервер RADIUS будет использовать MAC-адрес клиента в качестве имени пользователя.
Галочку не ставим.

MAC Accounting - включить MAC-статистику.
Галочку не ставим.

EAP Accounting - включить EAP-статистику.
Галочку не ставим.

Interim Update - интервал времени через который точка доступа повторно запрашивает информацию об аккаунте с Radius сервера.
Параметр не изменяем.

MAC Format - формат в котором записываем MAC-адреса. Доступные форматы:

XX: XX: XX: XX: XX: XX
XXXX: XXXX: XXXX
XXXXXX: XXXXXX
XX-XX-XX-XX-XX-XX
XXXXXX-XXXXXX
XXXXXXXXXXXX
XX XX XX XX XX XX

Указывает как MAC-адрес клиента кодируется точкой доступа в атрибут User-Name RADIUS-сервера.

Параметр не изменяем.

MAC Mode - значения:

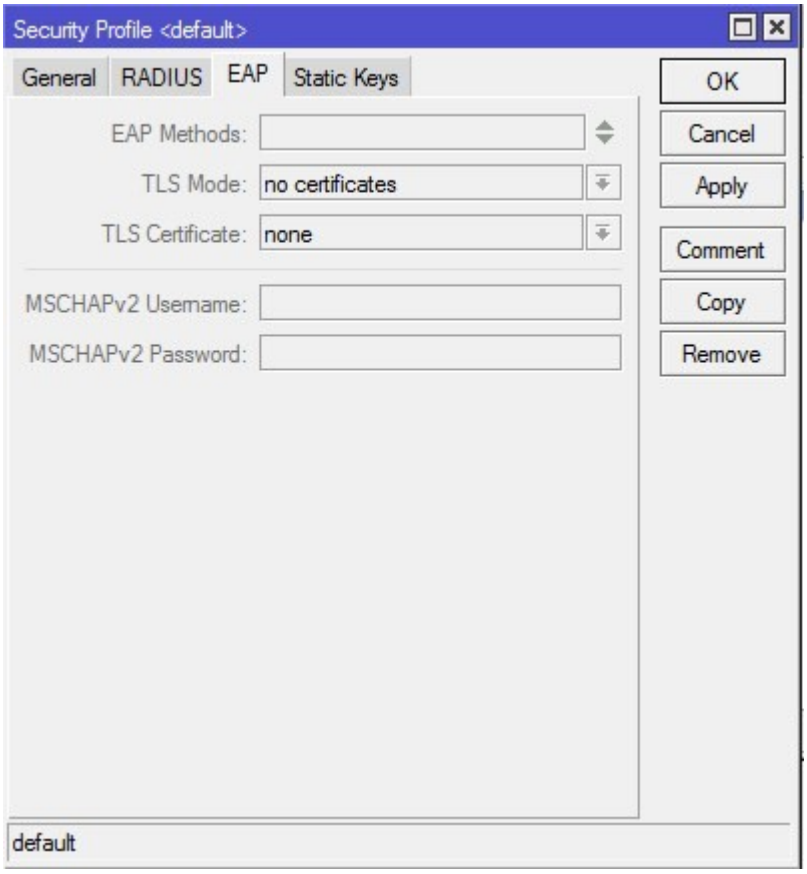
- as-username - использовать только имя при проверке подлинности в RADIUS-сервере.
- as-username-and-password - использовать имя и пароль при проверке подлинности в RADIUS-сервере (в качестве атрибута User-Name).

Параметр не изменяем.

MAC Caching Time - промежуток времени через который точка доступа будет кэшировать ответы аутентификации. Значение disabled отключает кэш, все ответы направляются напрямую в RADIUS-сервер.

Параметр не изменяем.

Вкладка EAP.



EAP Methods - метод EAP-аутентификации. Значения:

- eap-tls - использование встроенной аутентификации EAP TLS. Клиент и сервер поддерживают сертификаты.
- eap ttls mschapv2 - аутентификации EAP с именем пользователя и паролем.
- passthrough - точка доступа будет ретранслировать процесс аутентификации на сервер RADIUS.

TLS Mode - режим проверки TLS. Значения:

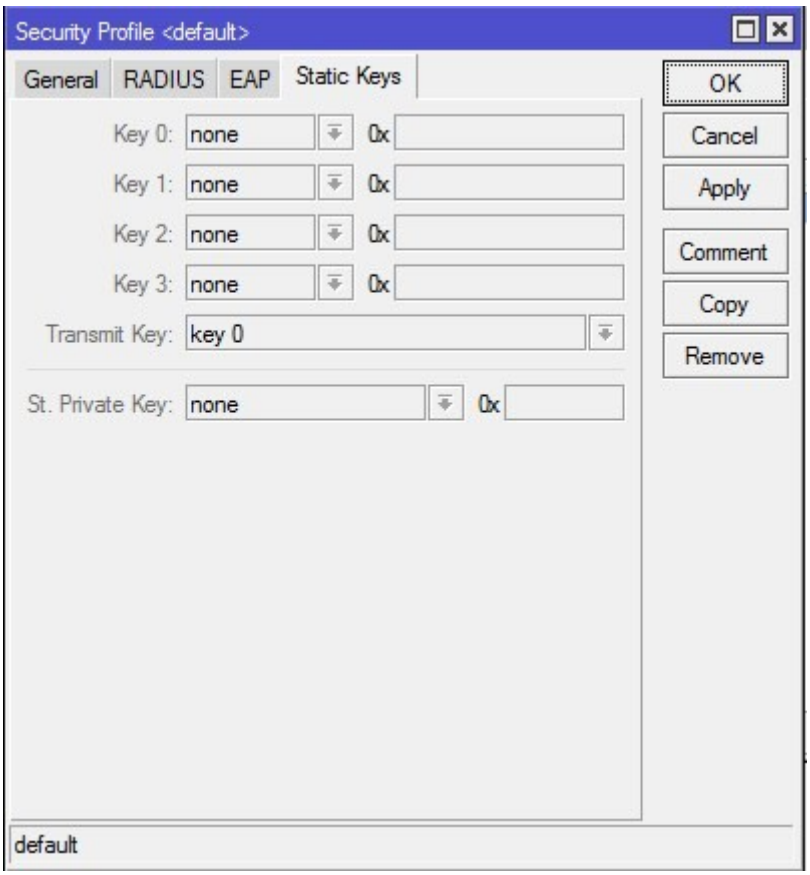
- verify certificate - проверять сертификат.
- dont verify certificate - не проверять сертификаты у клиента.
- no certificates - не использовать сертификат, использовать метод 2048 bit anonymous Diffie-Hellman key.
- verify certificate with crl - проверять сертификат по спискам CRL (список аннулированных сертификатов SSL).

TLS certificate - тут указываем непосредственно сертификат TLS.

MSCHAPv2 Username - имя пользователя для аутентификации eap ttls mschapv2.

MSCHAPv2 Password - пароль для аутентификации eap ttls mschapv2.

Вкладка Static Keys.



Данный раздел активен если используется "static keys optional" и "static-keys-required" на вкладке "General". Он используется для ввода ключей WEP-шифрования.

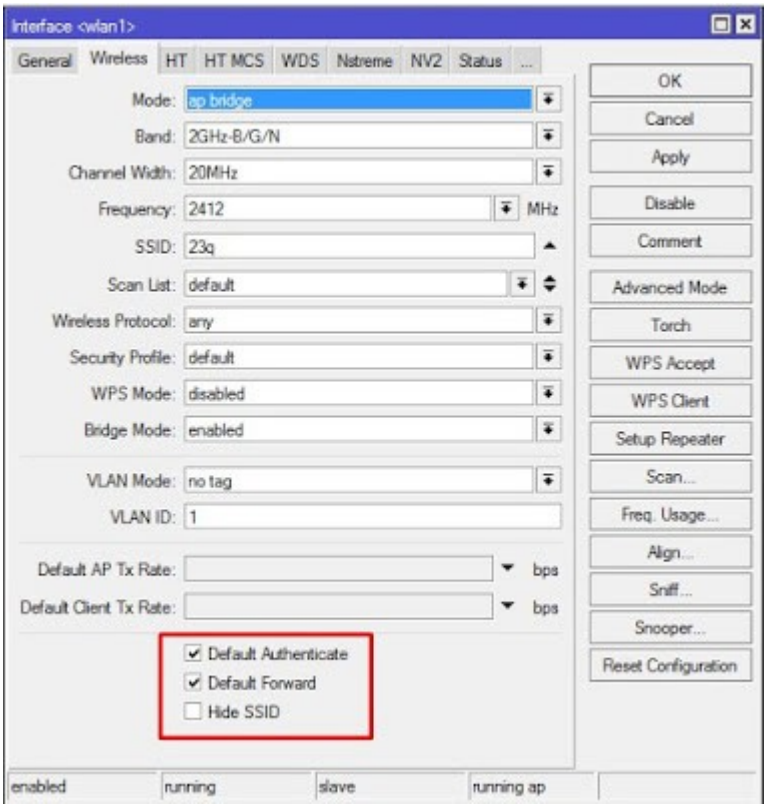
Key 0, Key-1, Key-2, Key-3 - шестнадцатеричное представление ключа. Длина ключа должна соответствовать выбранному алгоритму (40bit-wep, 104bit-wep, tkip или aes-ccm).

Transmit Key - точка доступа будет использовать указанный ключ для шифрования кадров для клиентов, также он будет использоваться для шифрования широковещательной и групповой передачи кадров.

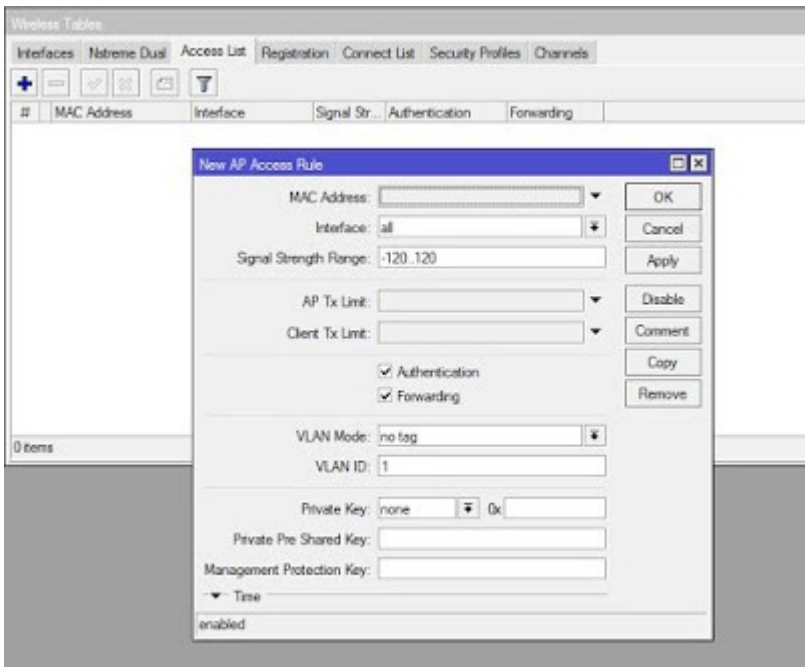
St. Private Key - только для использования в режиме "station". Точка доступа будет использовать соответствующий ключ выбранного алгоритма (в шестнадцатеричном представлении ключа).

Access List

Чтобы включить доступ по правилам Access List, на вкладке Interfaces необходимо открыть свойства беспроводного интерфейса, где на вкладке Wireless, убрать галочку с параметра Default Authenticate.



После снятия галки, переходим в Access List и создаем правило. Оно может быть для каждого клиента свое, или общее на всех.



MAC Address - MAC адрес устройства, которое будет подключатся к вашему роутеру. Если снять галочку Default Authenticate и выставить тут MAC адрес, то только это устройство сможет подключится к сети. Это и есть ограничение подключения по MAC-адресам в Mikrotik. Для того, что бы другое устройство смогло подключится к вашей точке, нужно внести его MAC в список правил.

Interface - интерфейс к которому будет производится подключение. Если указать "all" - правило будет применяться ко всем беспроводным интерфейсам вашего устройства.

Signal Strength Range - диапазон уровня сигнала, при котором возможно подключение. Настройка применяется в сетях с бесшовным роумингом между точками. Служит для того, что-бы ваше устройство не держалось за текущую точку доступа до критически слабого уровня сигнала, а перерегистрировалось на новую точку (при одинаковом SSID).
Обычно выставляют диапазон типа "-75..120" при наличии нескольких точек доступа в нормальной доступности.

AP Tx Limit - ограничить скорость передачи данных этому клиенту. Значение "0" - без ограничений.

Client Tx Limit - передать ограничение скорости клиента. Поддерживается только на RouterOS клиентах.

Authentication - возможность авторизации. Если убрать галочку, устройство с этим MAC адресом, не сможет подключиться к вашей сети.

Forwarding - возможность обмена информацией с другими участниками беспроводной сети. Если убрать галочку с этого пункта - пользователь этого устройства не будет иметь доступа к другим клиентам wifi-сети.

Обычно на публичных точка доступа - галочку снимают, для экономии трафика и безопасности.

VLAN-Mode - С помощью VLAN Tagging можно отделить трафик виртуальных беспроводных точек доступа от локальных клиентов (например, что-бы отделитель гостевую сеть от рабочей). Значения:

- no-tag - не использовать VLAN-тегирование на беспроводном интерфейсе;
- use-service-tag - использовать 802.1ad тегирование;
- use-tag - использовать 802.1q тегирование.

VLAN-ID - VLAN-идентификатор.
VLAN не используем, оставляем по-умолчанию - "1".

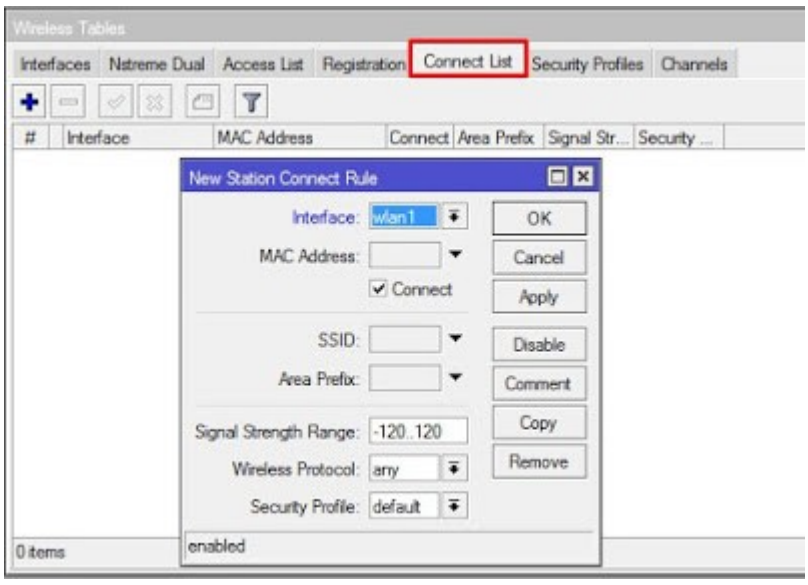
Private Key - возможность установки персонального ключа шифрования для устройства с данным MAC адресом. Только для режимов WEP.

Private Pre Shared Key - персональный ключ шифрования. Используется в режиме WPA PSK.

Managment Protection Key - ключ защиты Managment Protection. Managment Protection - защита от атак деаутентификации и клонирования MAC-адреса. Выставляется на вкладке "General" в Security Profiles.

Time - в этом разделе можно указать временной диапазон, в рамках которого будет возможно подключение этого устройства.

Connect List



Interface - правило в списке connect list может быть применимо только к одному беспроводному интерфейсу. Тут мы его выбираем.

MAC Address - указываем MAC AP к которой будем подключатся.

Connect - если галочка стоит, то подключатся к точке доступа, которая соответствует этому правило, если не стоит - не подключатся.

SSID - подключатся только к точкам доступа, которые имеют указанный SSID, если не активно - к любым SSID.

Area Prefix - правило действует для интерфейса с заданным префиксом. Area - позволяет создать группу и включить беспроводные устройства в нее, а затем использовать определенные правила для этой группы и всех входящих в нее устройств, вместо того, чтобы создавать отдельные правила для каждого устройства. Это значение заполняется в настройках точки доступа и может быть сопоставлено с правилами в connect-list.

Signal Strength Range - подключатся только к точкам доступа в пределах заданного диапазона уровня сигнала.

Wireless Protocol - протокол беспроводной связи. Значения:

- any - любой поддерживаемый (автовыбор);
- 802.11 - только стандартные протоколы 802.11abgn. Обычно используется для совместимости с оборудованием других производителей;
- nstreme - «фирменный» протокол Mikrotik, характеризующийся высокой скоростью потока данных в одну сторону (RX или TX);
- nv2 - "фирменный" протокол Mikrotik, характеризующийся высокой скоростью при работе в дуплексе или работе в режиме PtMP (точка-многоточка);

Security Profile - профиль безопасности, который соответствует защите точек доступа к которым идет подключение. Настраивается в Wireless Table — Security Profiles.

Общие рекомендации по безопасности WI-FI- сети:

1) используйте только WPA2-PSK с aes-ccm шифрованием.
2) отключите WPS.
3) для задания пароля используйте цифры, буквы верхнего и нижнего регистра, специальные символы.
4) регулярно меняйте пароль на точках.
5) если это возможно ограничите доступ по MAC-адресам в WiFi-сети.
6) снимите галочку Default Forward в настройках вашего интерфейса - запретите пересылку пакетом между wifi-клиентами.
7) скройте SSID вашей сети.
8) поменяйте MAC беспроводного интерфейса - для затруднения идентификации устройства.