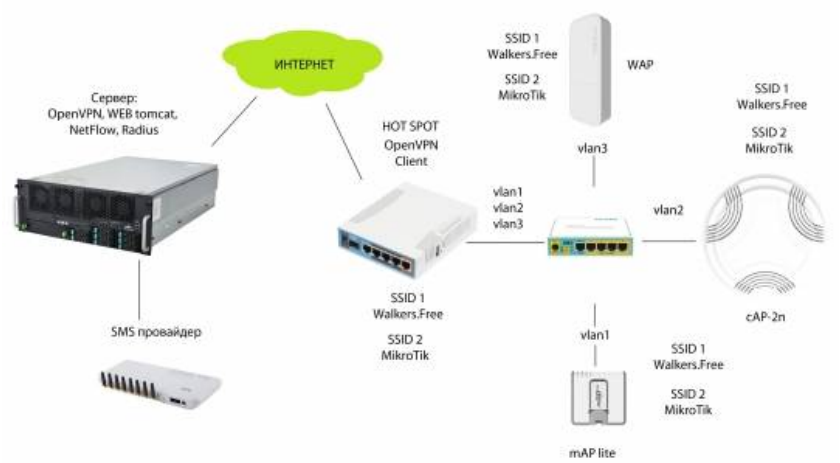
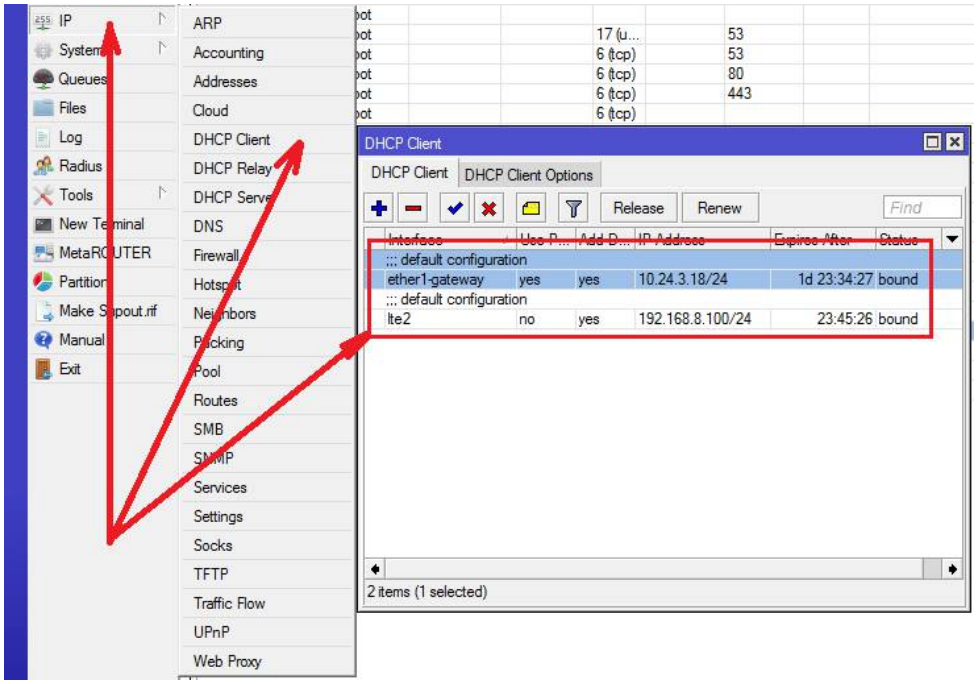
Настройка системы SMS авторизации iGoFree на MikroTik

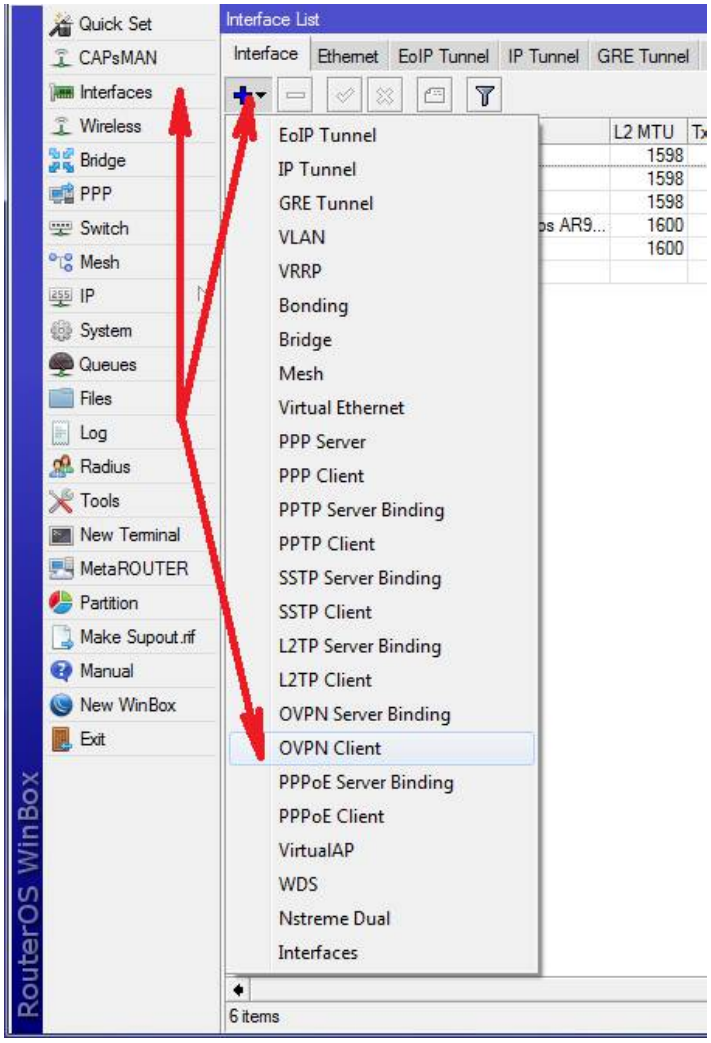


Данная статья содержит материалы со встречи пользователей MikroTik в Минске 3 июня 2016 года. Это выступление Кардаша Александра Владимировича на MUM Belarus 2016 о настройке системы SMS авторизации через сервис iGoFree на оборудовании MikroTik. Содержит типовую схему внедрения сервиса компании ООО "Уолкерс Системс" в сетевую инфраструктуру мест, где необходимо организовать публичный доступ к интернету через Wi-Fi сеть. Слайды с презентации Евгения Осипова можно скачать по этой ссылке.

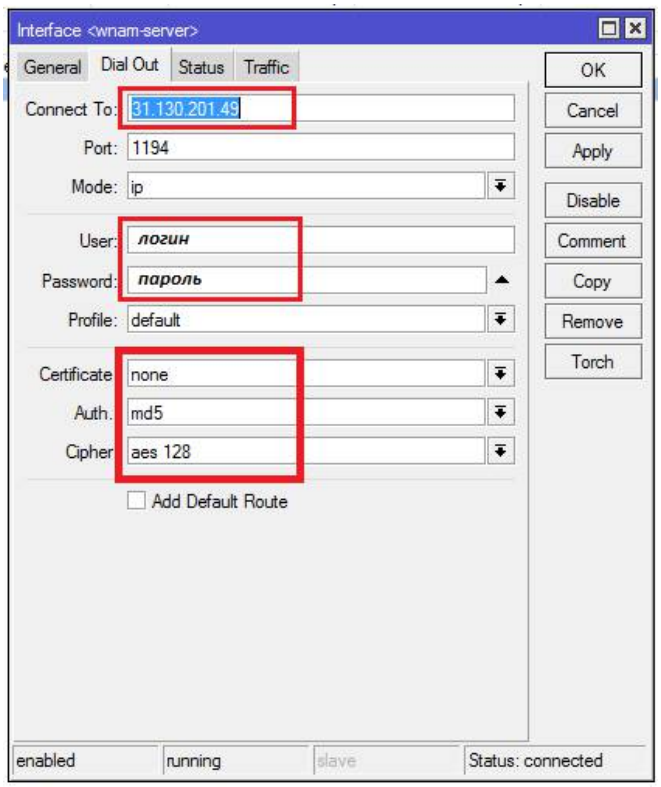
Настройка начинается с подключения маршрутизатора к интернету. В самом простом случае следует вставить Ethernet кабель от провайдера в первый порт MikroTik и роутер получает IP через **DHCP client**. Кроме того по умолчанию на первом порту сделан **scr-nat masqurade**. Если необходима постоянная достоступность интернета, можно настроить резервирование через 3G модем. С модемами Huawei поддерживающими Hi-Link нужно создать **DHCP client** на интерфейсе **lte2** указав в поле **Default Route Distance** (метрика или цена маршрута) значение большее чем на основном канале. Далее следует сделать в IP/Firewall/NAT правило **scr-nat** action **Masquarade** на интерфейс **lte2** созданный 3G модемом.



Настроим OpenVPN client на MikroTik. Для этого откроем окно с интерфейсами и плюсиком добавим новый интерфейс:

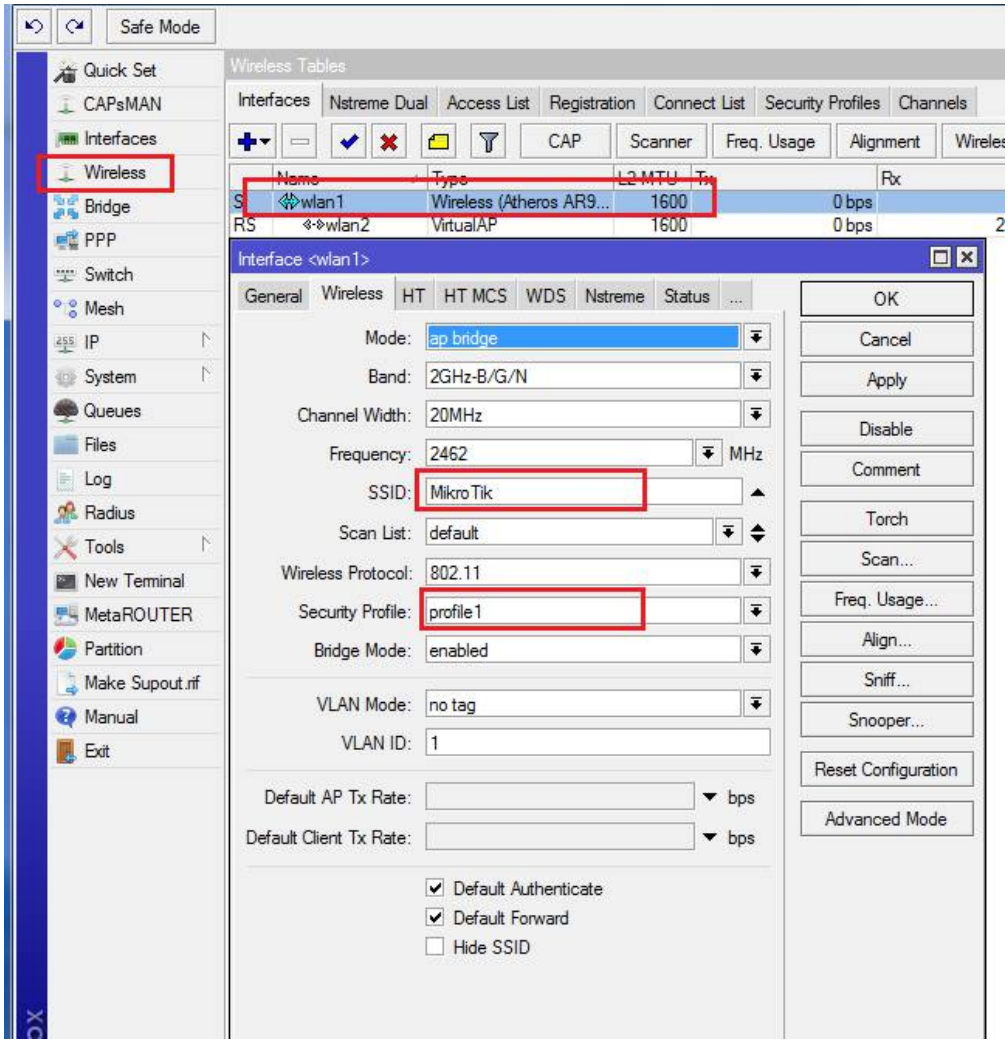


Введём IP адрес сервера OpenVPN и логин пароль для доступа к нему. Хэшкод MD5 и алгоритм шифрования AES с ключём 128 бит:

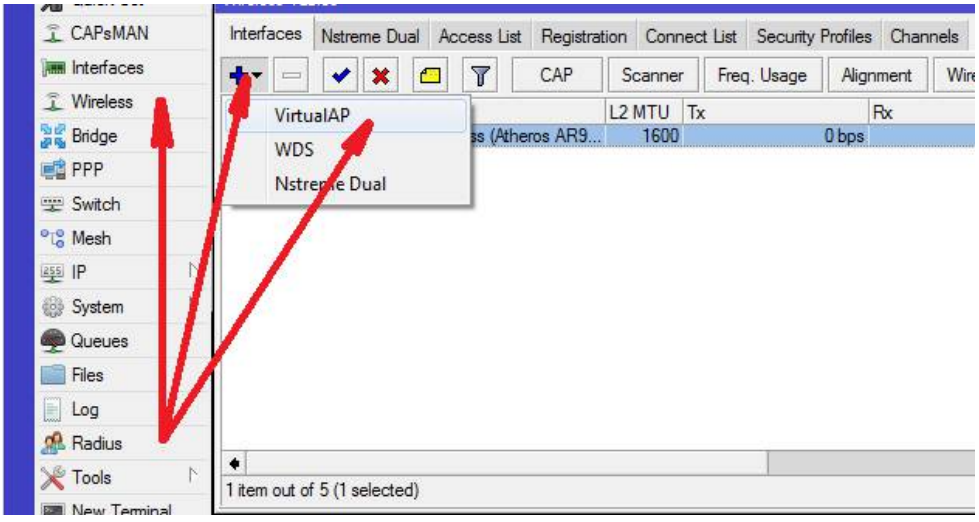


Настроим точку доступа **wlan1** вещающую Wi-Fi сеть персонала заведения в котором устанавливается система авторизации. Выбираем узкие каналы в 20 mHz которые позволяют достич максимальной дальности Wi-Fi сигнала. Связано это с тем, что энергия точки доступа распределяется на более узкую полосу, позволяя иметь в два раза большую силу сигнала на удалённых участках сети. Иначе сказать полезный сигнал Wi-Fi будет сильнее выделятся на уровне шумов. Кроме того на узких каналах можно разместить больше точек доступа разнеся их даже на 1, 5, 9, 13 канал максимально заполнив радиочастотный спектр полезным сигналом. Выбрав **Wireless Protocol 802.11** можно обеспечить максимальную совместимость с Wi-Fi устройствами клиентов заведения, ведь обычные

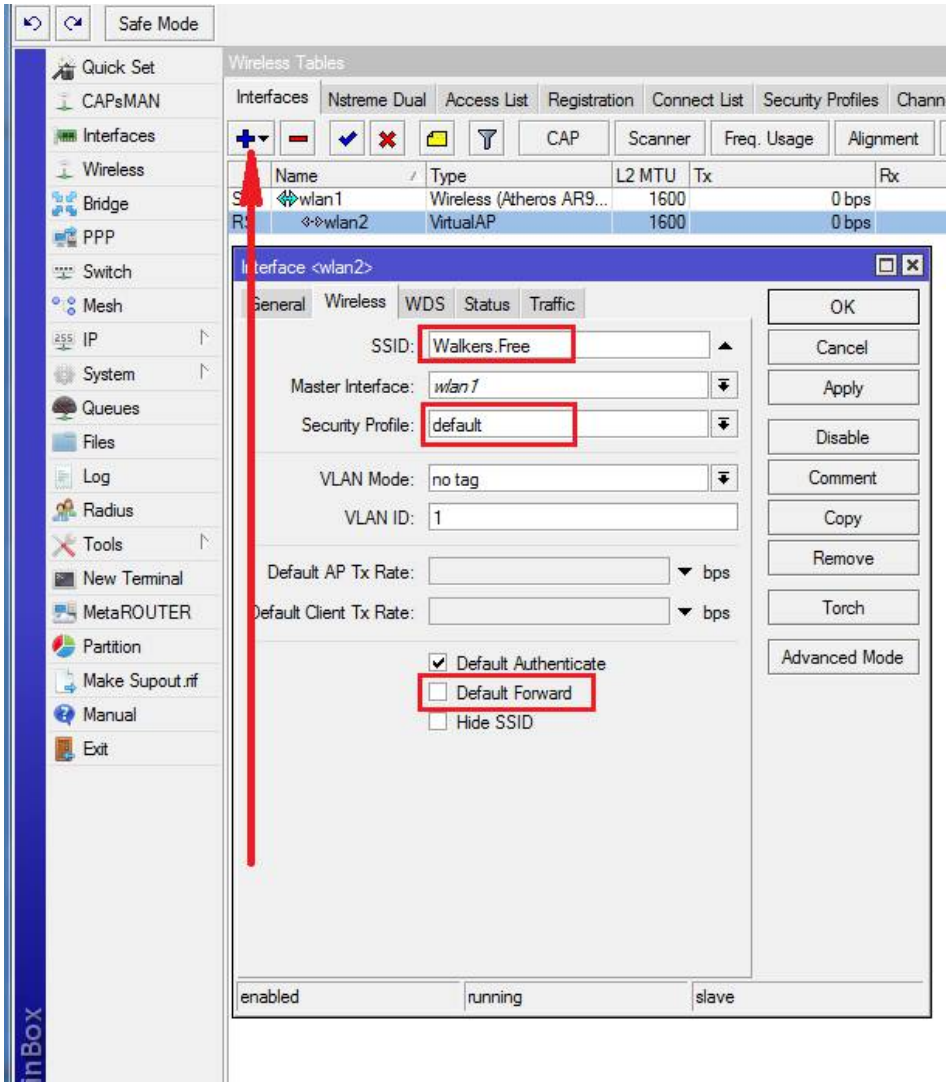
устройства не поддерживают проприетарных полинговых проколов MikroTik.



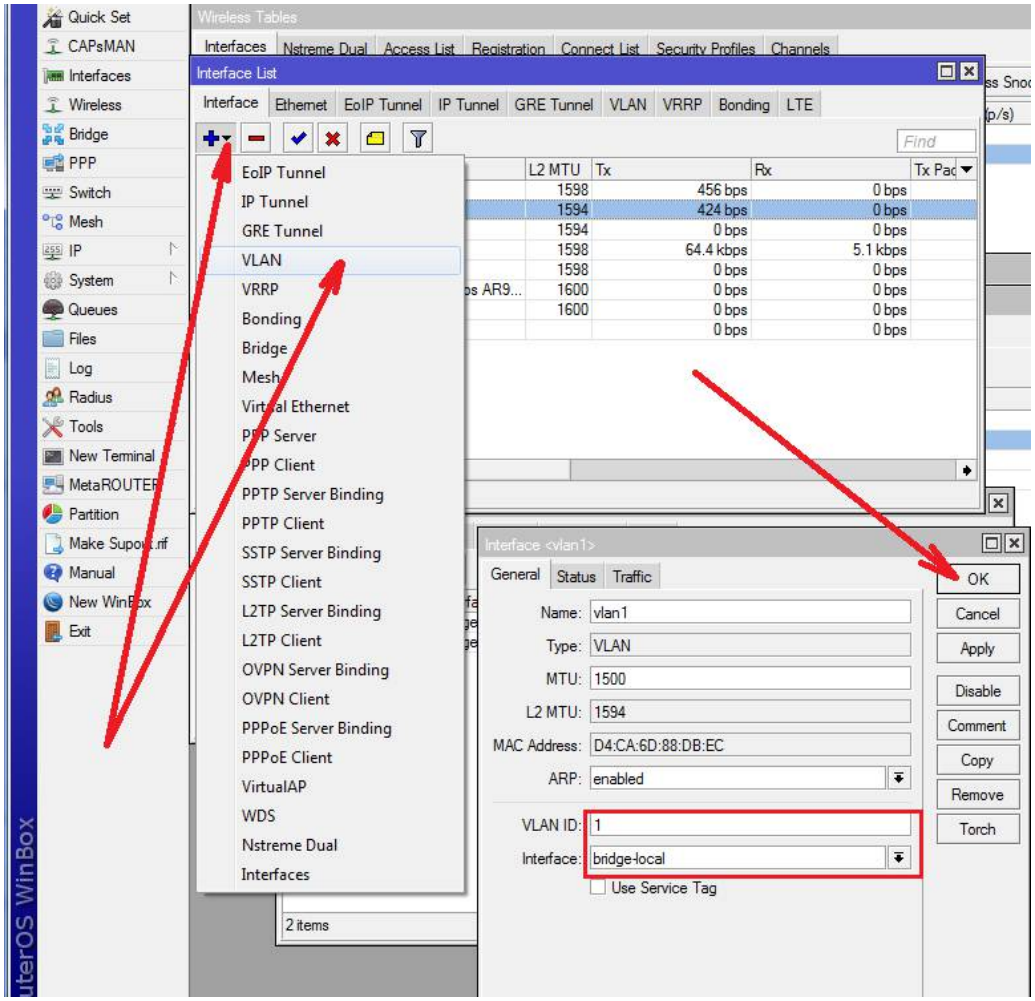
Создадим виртуальную точку доступа Wi-Fi в которой будет использоваться SMS авторизация:



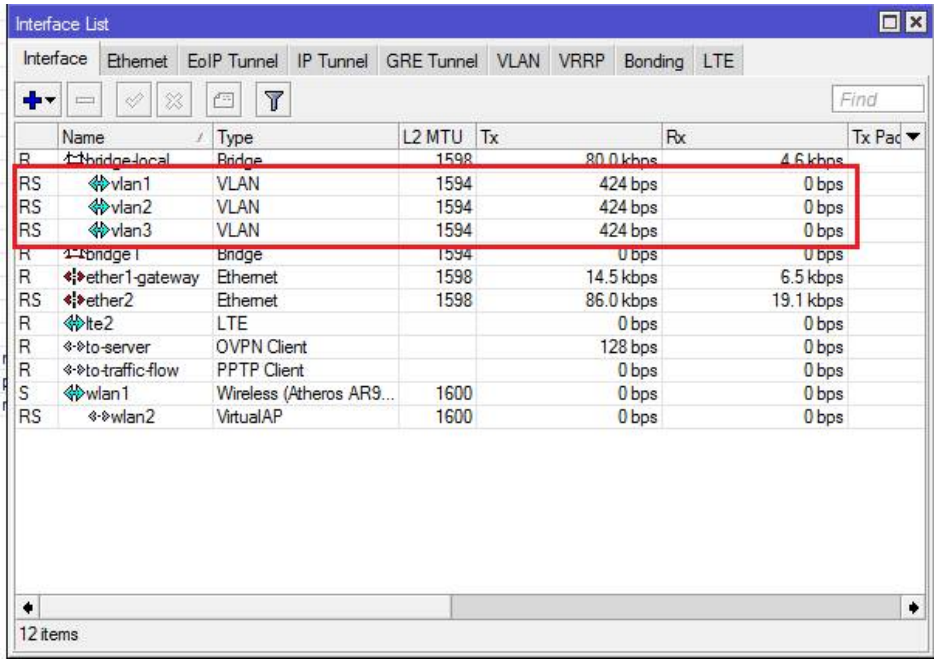
Индификатор сети **SSID** Walkers.Free профиль сети **default,** который не содержит пароля. Чтобы предотвратить ARP спуфинг клиентов друг другом (атака человек по середине позволяющая перехватывать трафик пользователя не использующего шифрования) снимаем галочку **Default Forward** и тем самым запрещаем передавать данные между клиентами подключенными к свободной Wi-Fi сети.



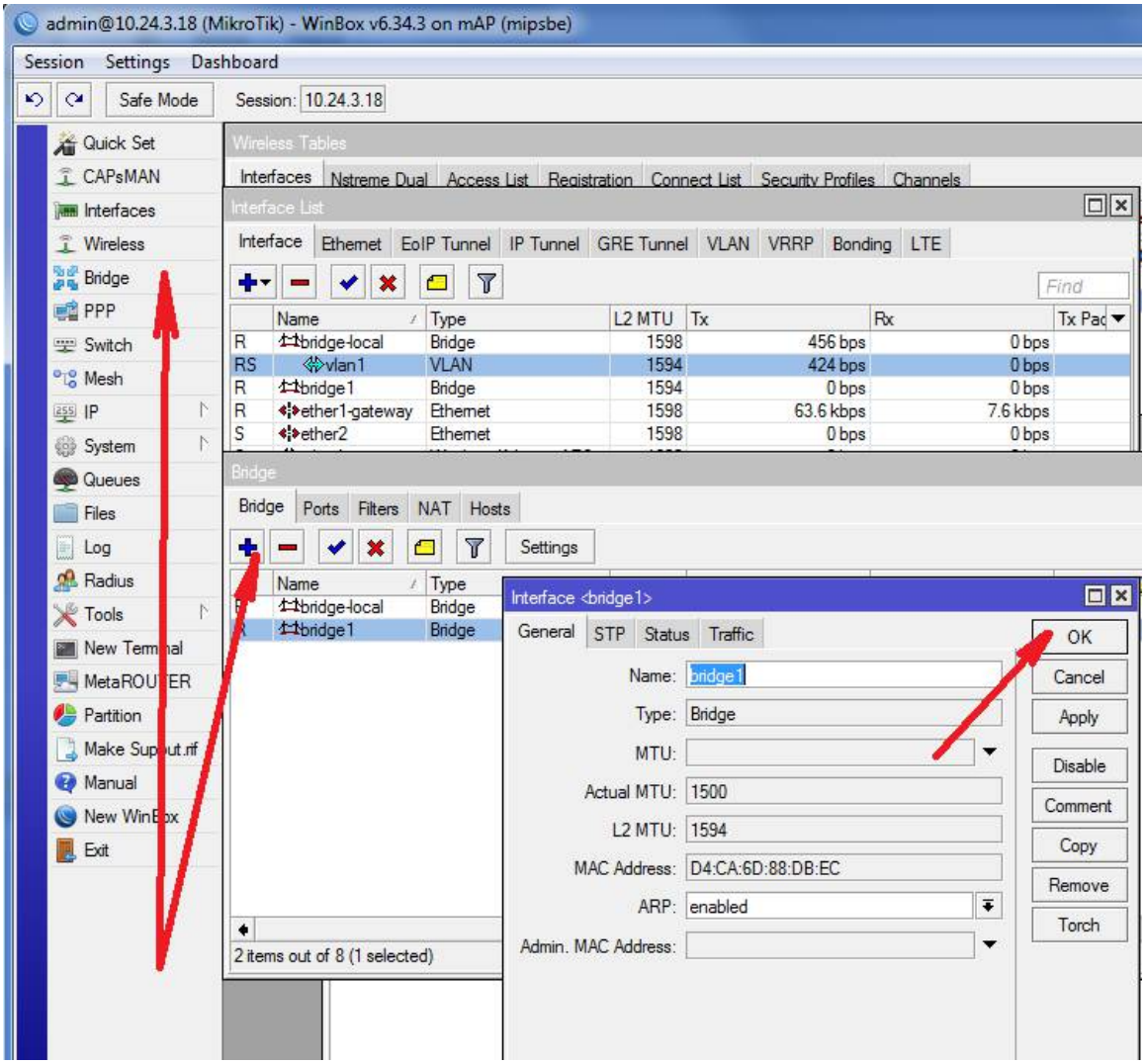
Мы хотим сделать одну сеть с индификатором Walkers.Free на четырёх точках доступа Wi-Fi позволяющую использовать SMS авторизацию. Проще всего это сделать с помощью технологии VLAN на основе меток. Кадры основной сети не будут иметь меток, а кадры дополнительной будут помечаться id 1, 2, 3. Создаём vlan1 с id 1 на интерфейсе **bridge-local**:



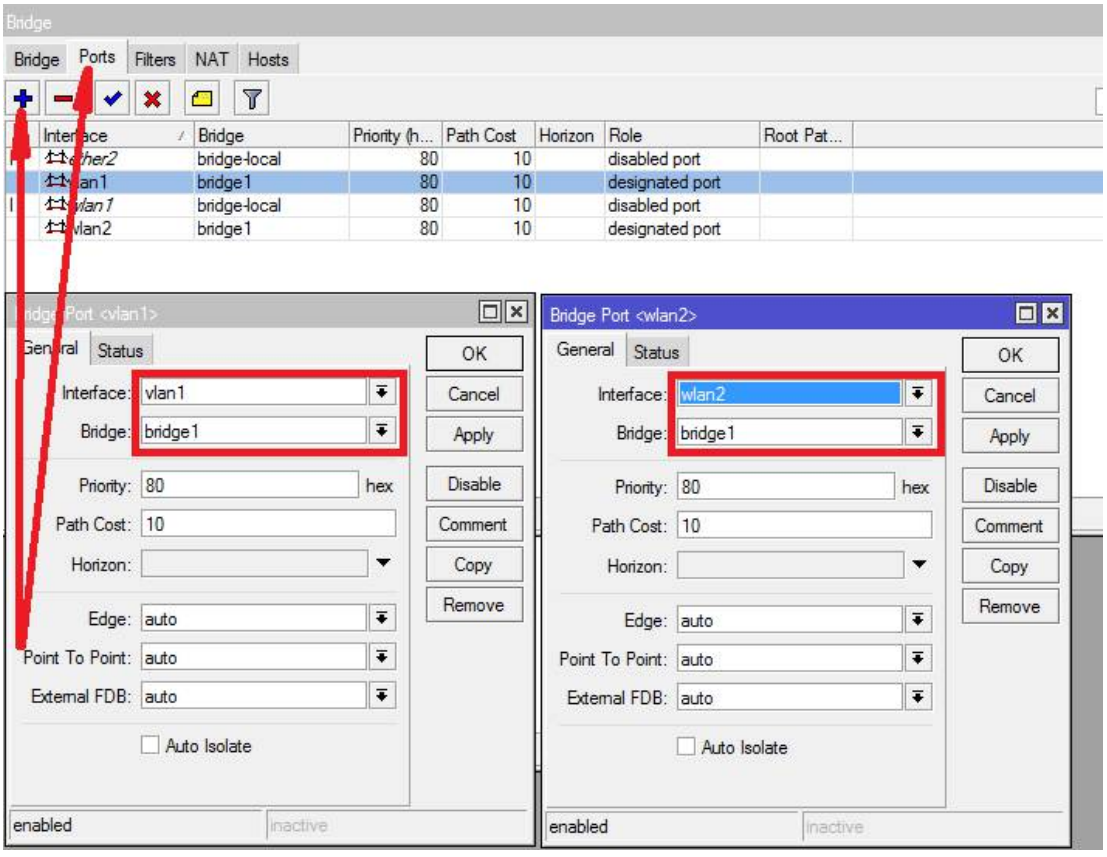
По анологии создаём **vlan2** с id 2 и **vlan3** с id 3:



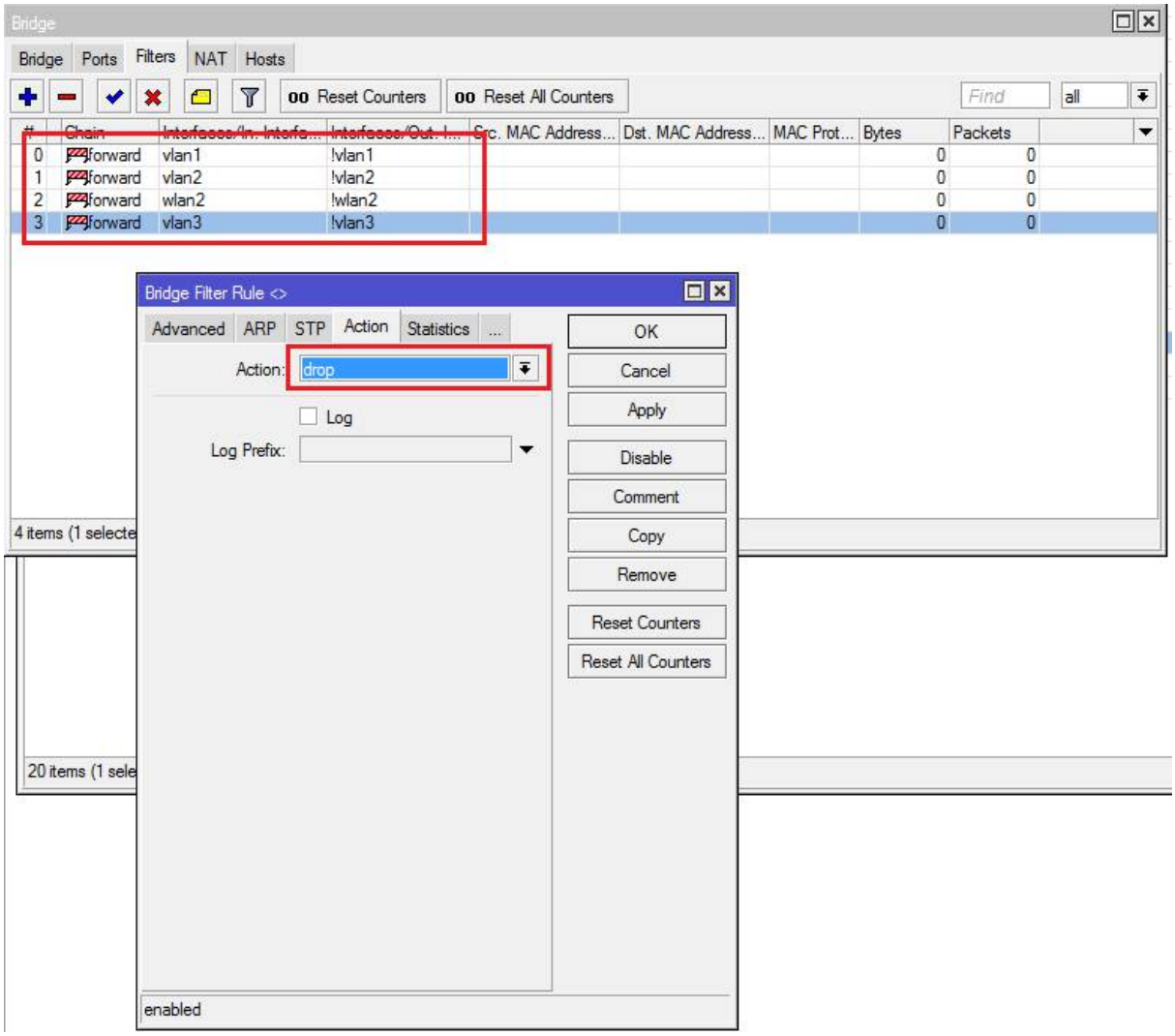
Создадим **bridge1** на котором будет работать хотспот:



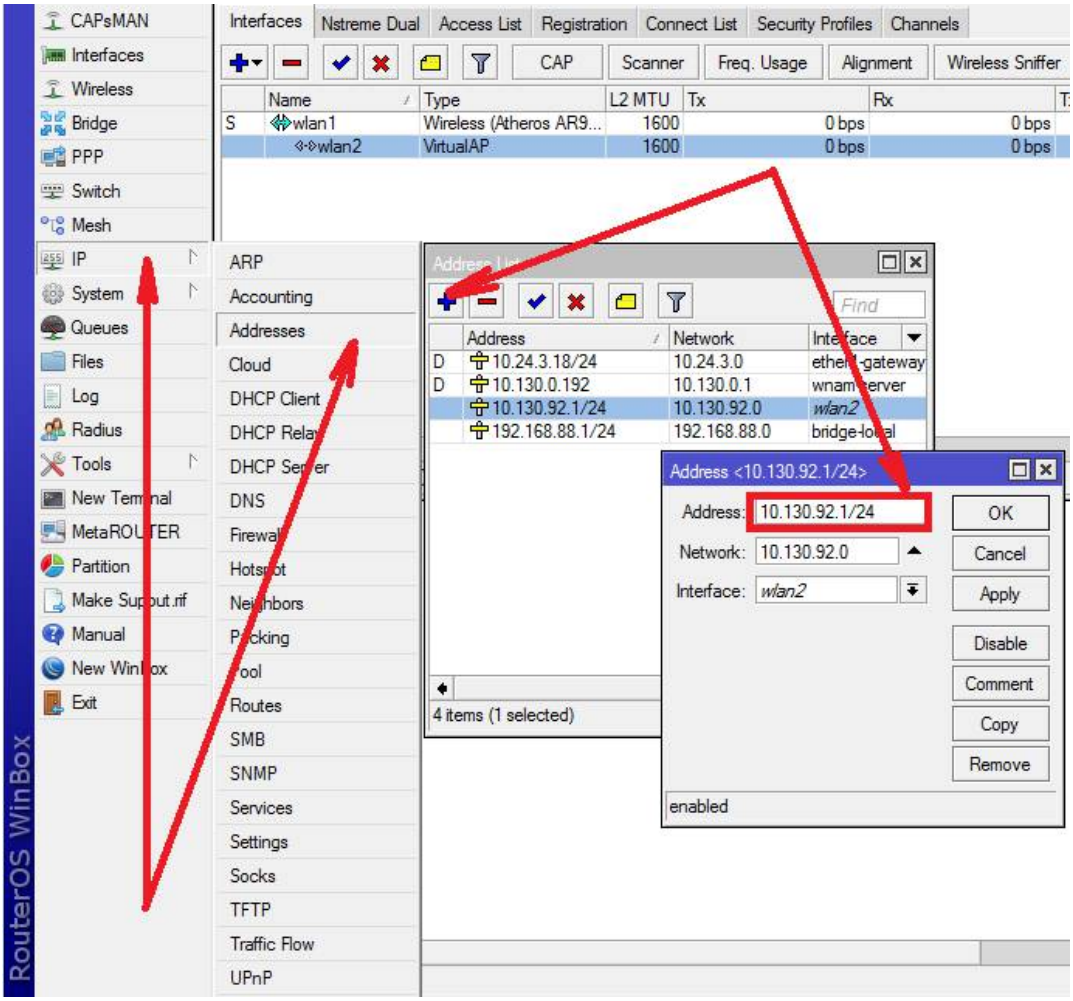
Добавим в **bridge1** **vlan1**, **vlan2**, **vlan3** и виртуальную точку доступа Wi-Fi **wlan2**:



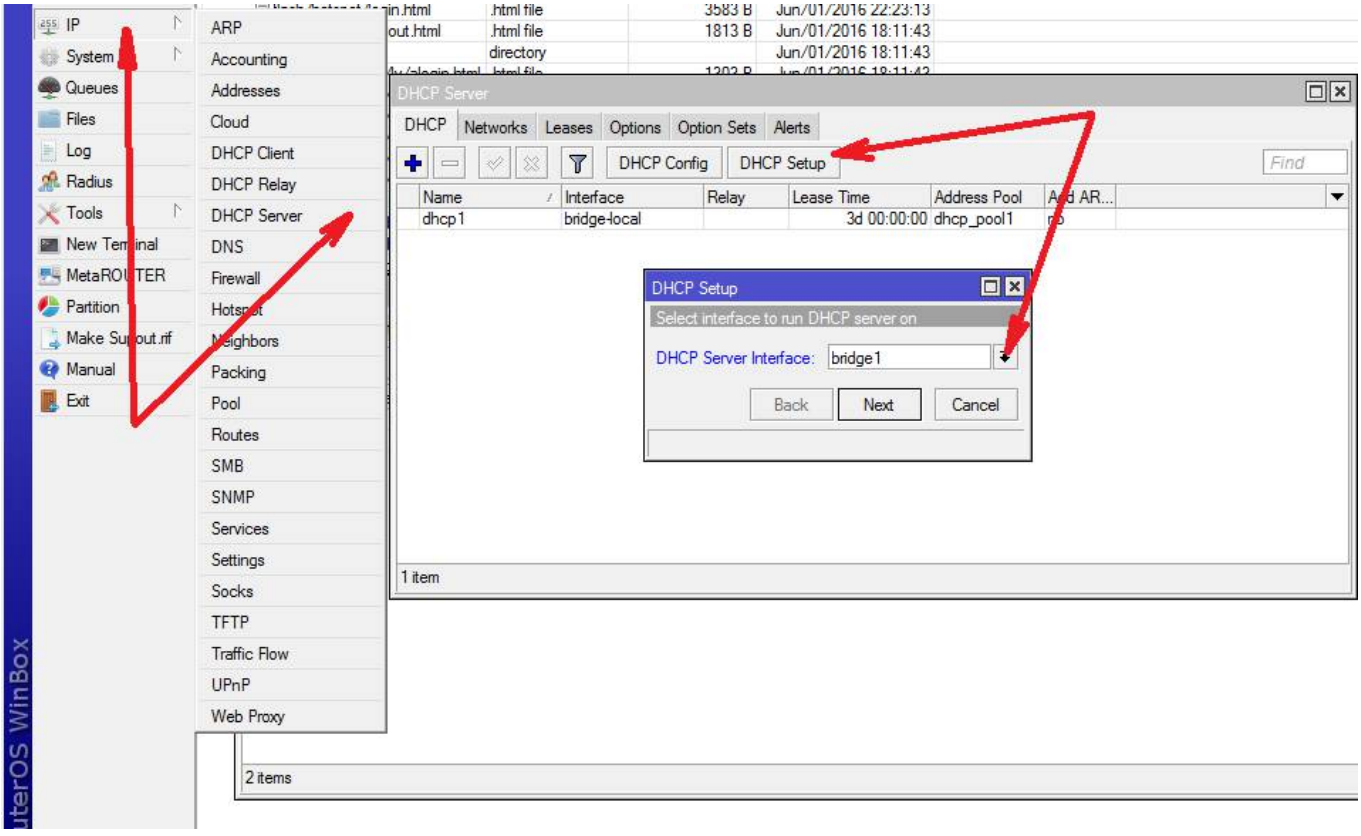
Зафильтруем на вкладке Filters трафик между **vlan1**, **vlan2**, **vlan3** и **wlan2**, чтобы клиенты подключённые к разным точкам доступа не могли передавать данные между собой:



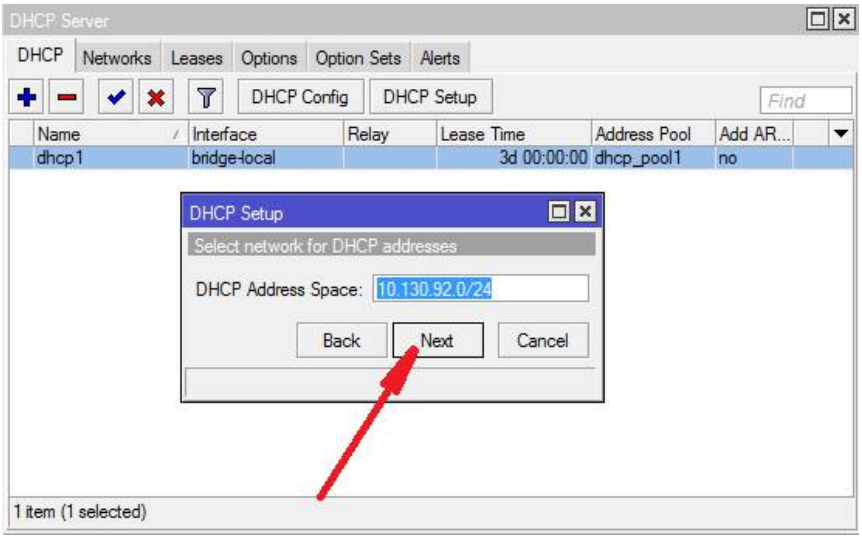
Пропишем IP адрес на интерфейсе на котором мы будем делать HotSpot. В нашем случае это bridge1 хотя можно прописать и на **wlan2**:



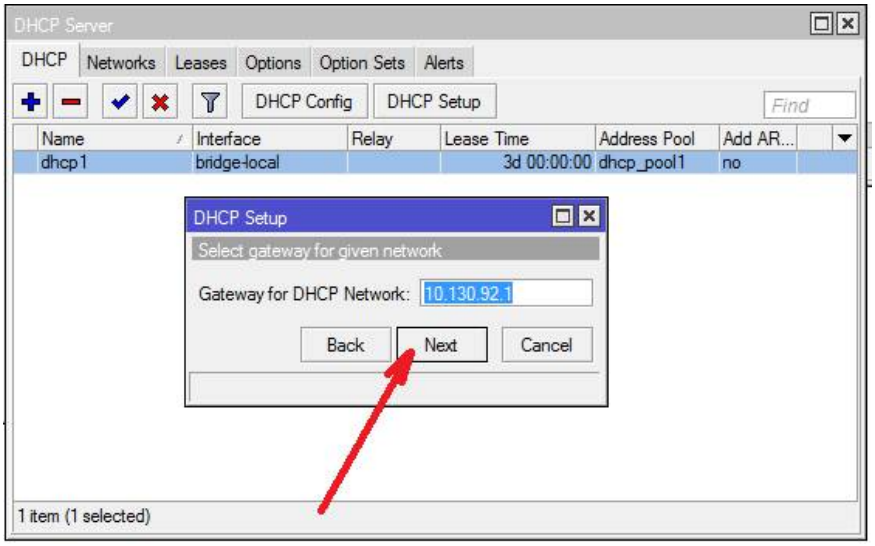
Настроим с помощью мастера DHCP сервер:



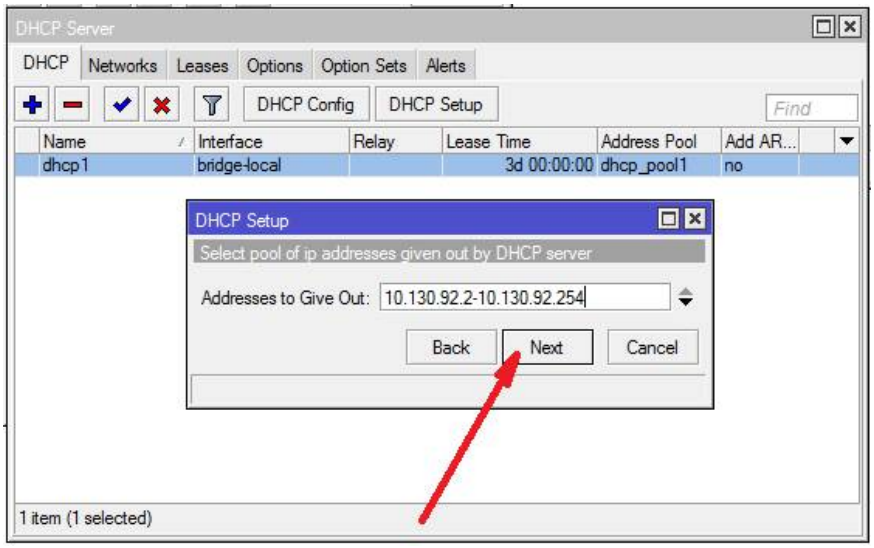
Согласимся с предложеной сетью 10.130.92.0/24:



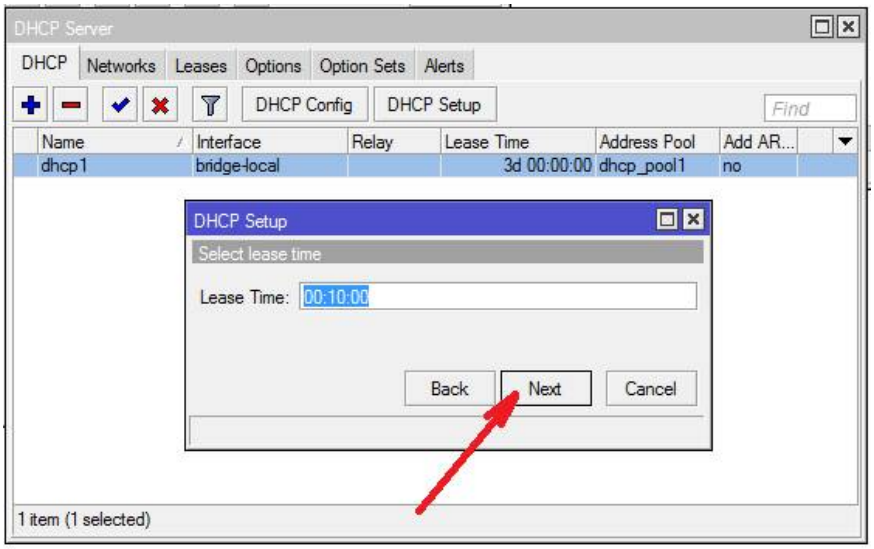
Согласимся с предложенным мастером шлюзом:



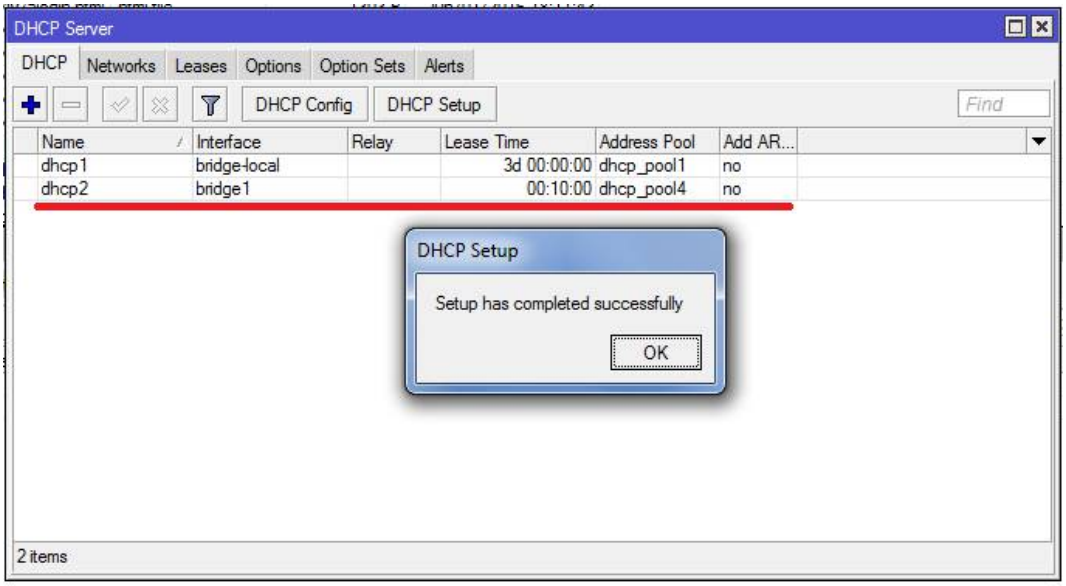
Ввиду того, что в свободной сети Walkers.Free не будет размещаться сетевое оборудование можно использовать весь пул свободных IP адресов кроме 10.130.92.1:



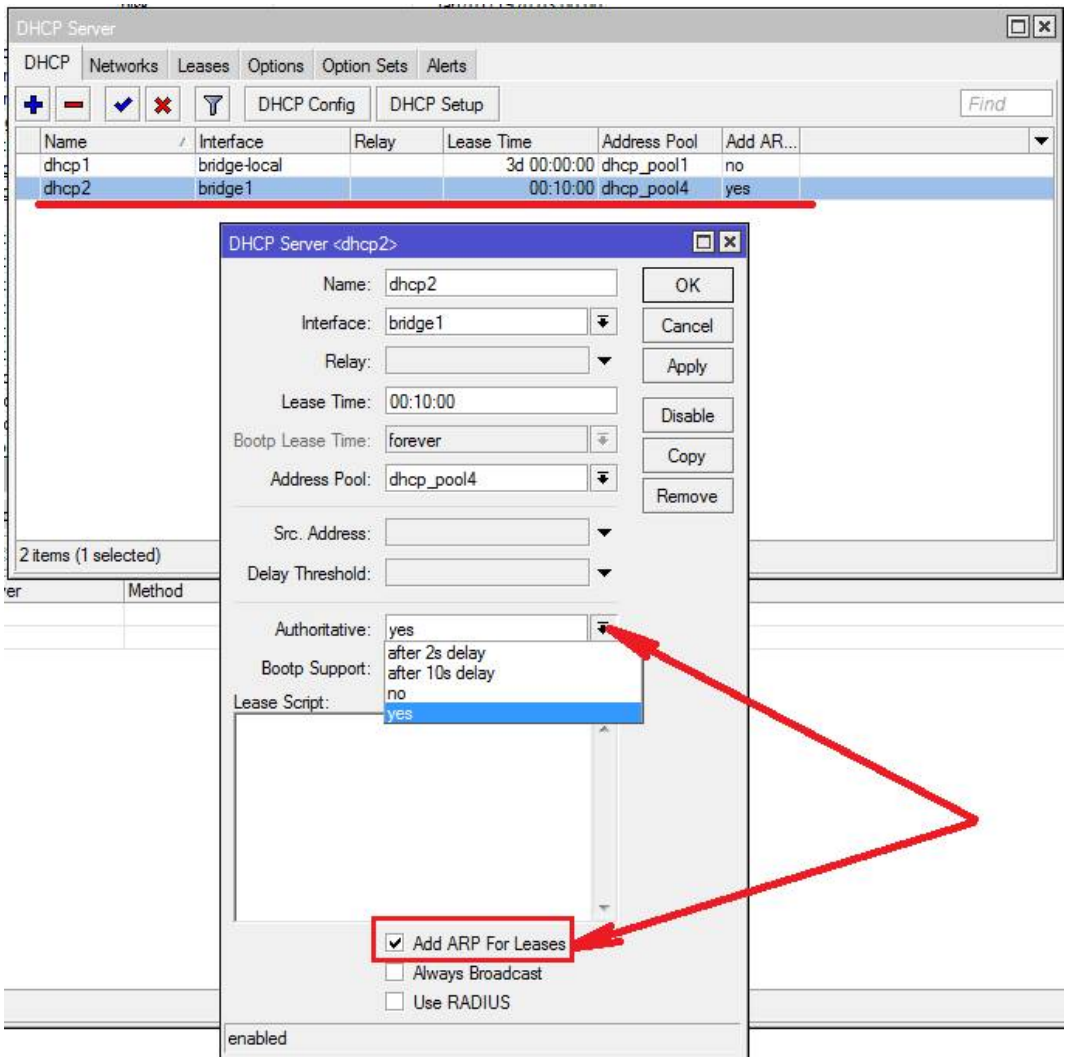
Время аренды IP адреса по умолчанию 10 минут, нажмём Next ничего не меняя:



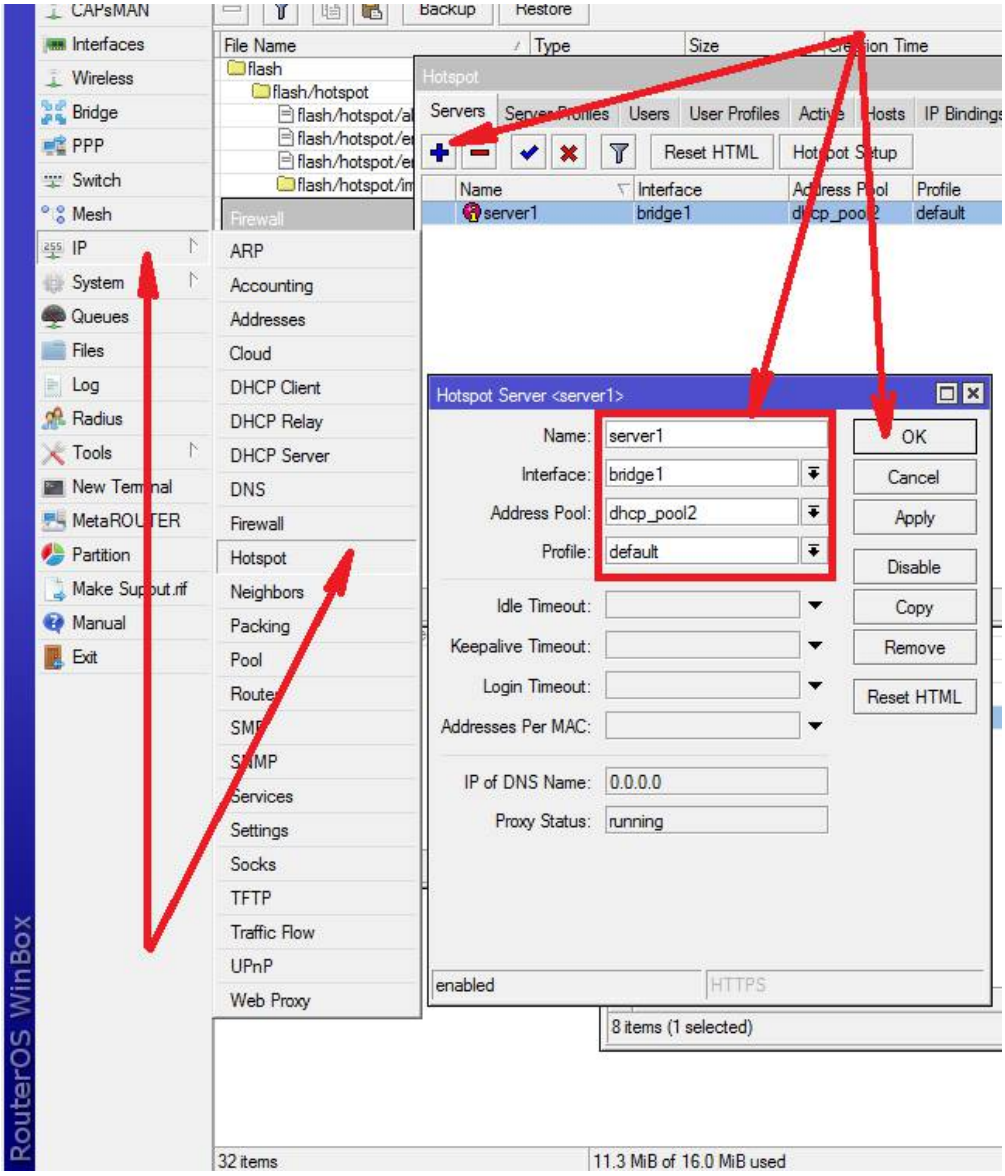
Если всё правильно сделано мы увидим сообщение, что DHCP успешно настроен:



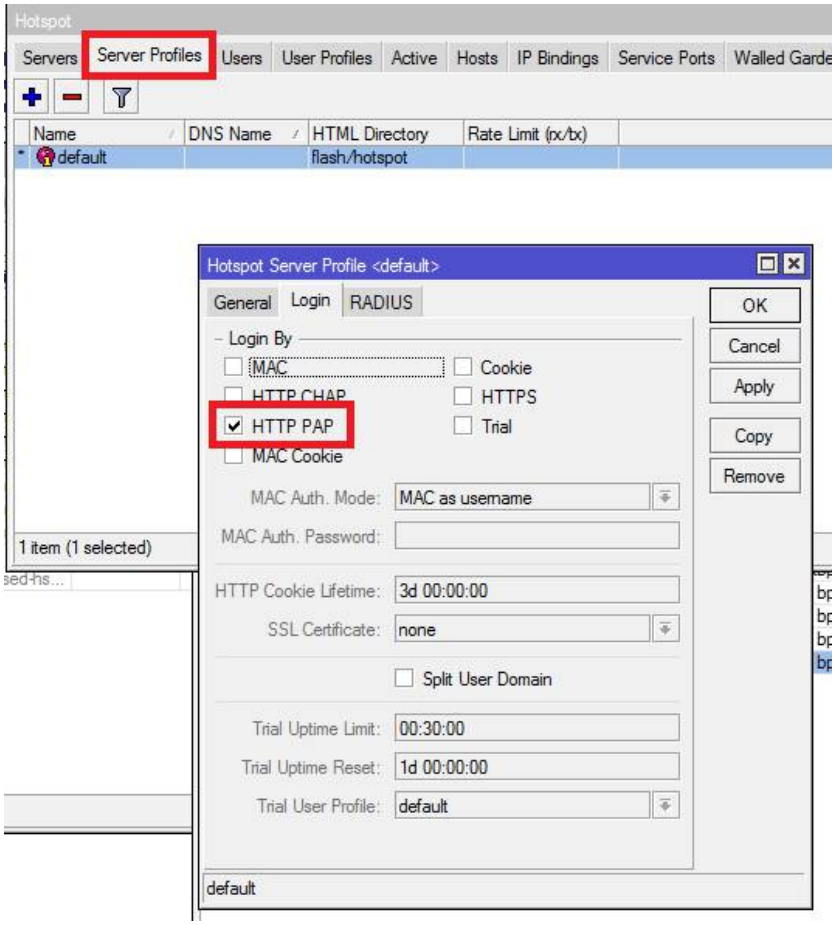
В сети персонала рекомендую выставить DHCP "authoritative" в Yes (DHCP авторитетный - Да), что заставит DHCP отвечать на запросы клиентов максимально быстро и отключить неавторитетные DHCP сервера в сети. Также выставить галочку "Add ARP for leases" для того чтобы в ARP таблицу автоматически добавлялись сопоставления IP с MAC.



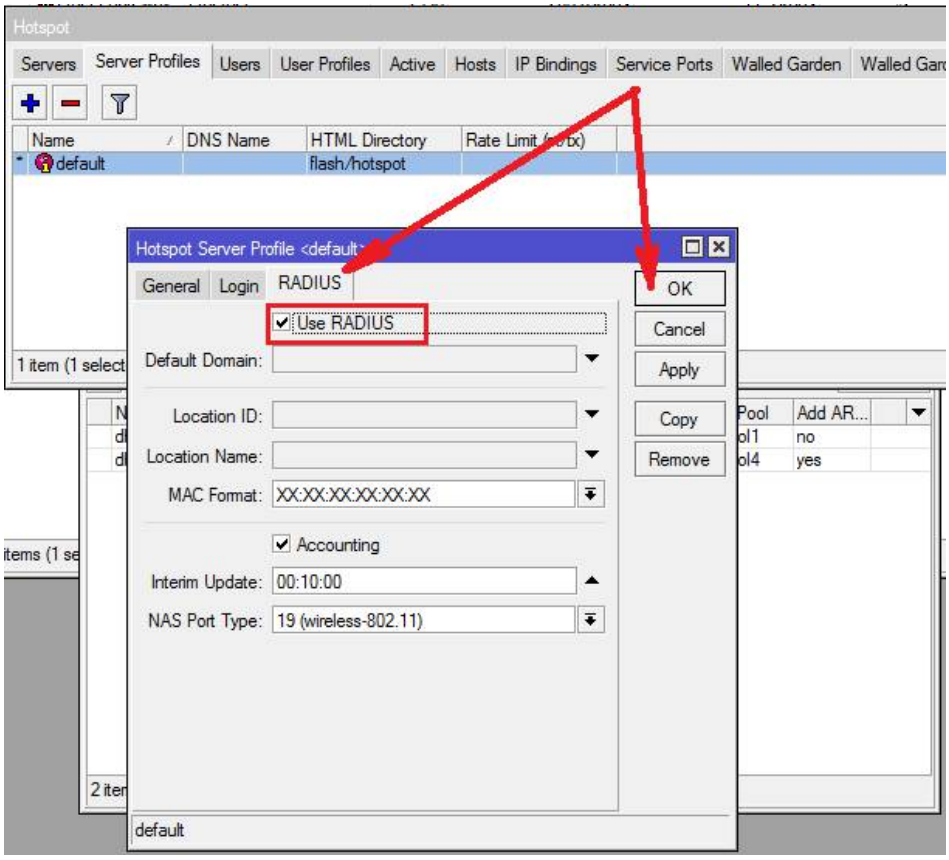
Настроим HotSpot. Если его нет в меню IP, значит необходимо зайти в System/Packages, включить его и программно перезагрузить маршрутизатор. Если он уже включён, открываем окно создания HotSpot и плюсиком создаём новый сервер: Выбираем интерфейс на котором будет работать HotSpot - **bridge1**; пул раздачи IP адресов ранее созданый с помощью мастера настройки DHCP и профиль **default**, который сейчас будем править:



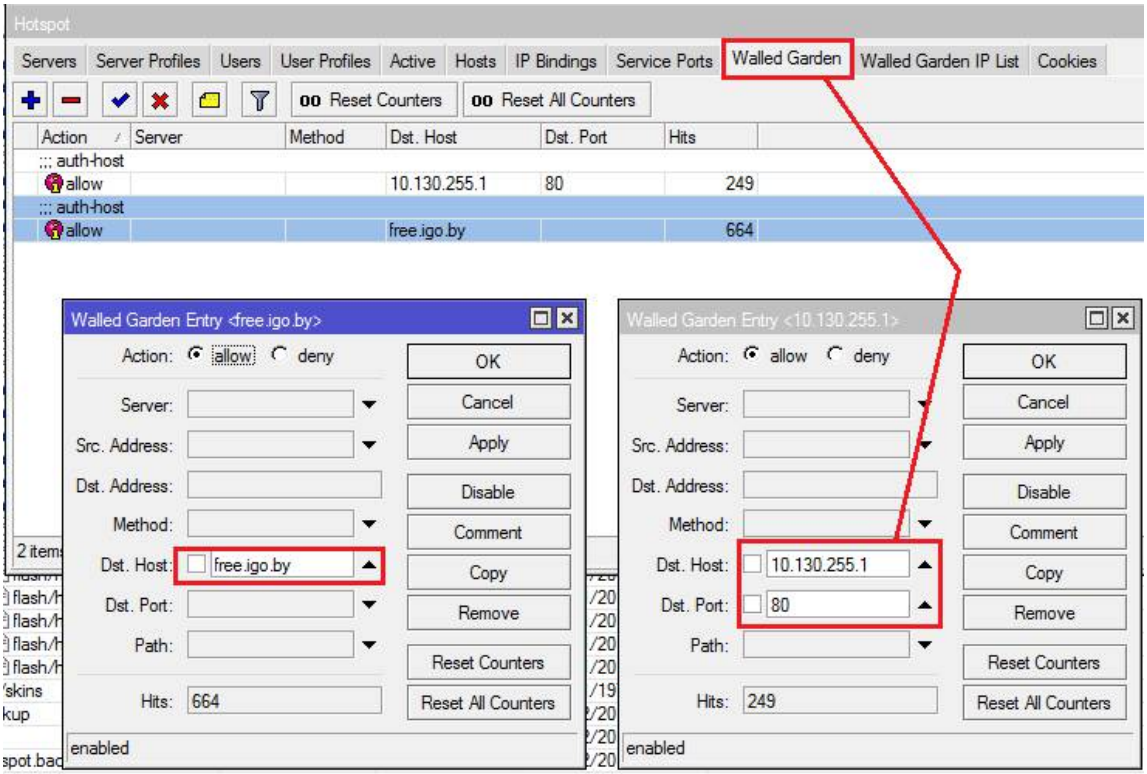
Поправим Server Profile **default**: Ставим галочку Login **HTTP PAP**. Данные для авторизации пользователя можно передавать открытым текстом по сети ввиду того, что ARP спуфинг не возможен.



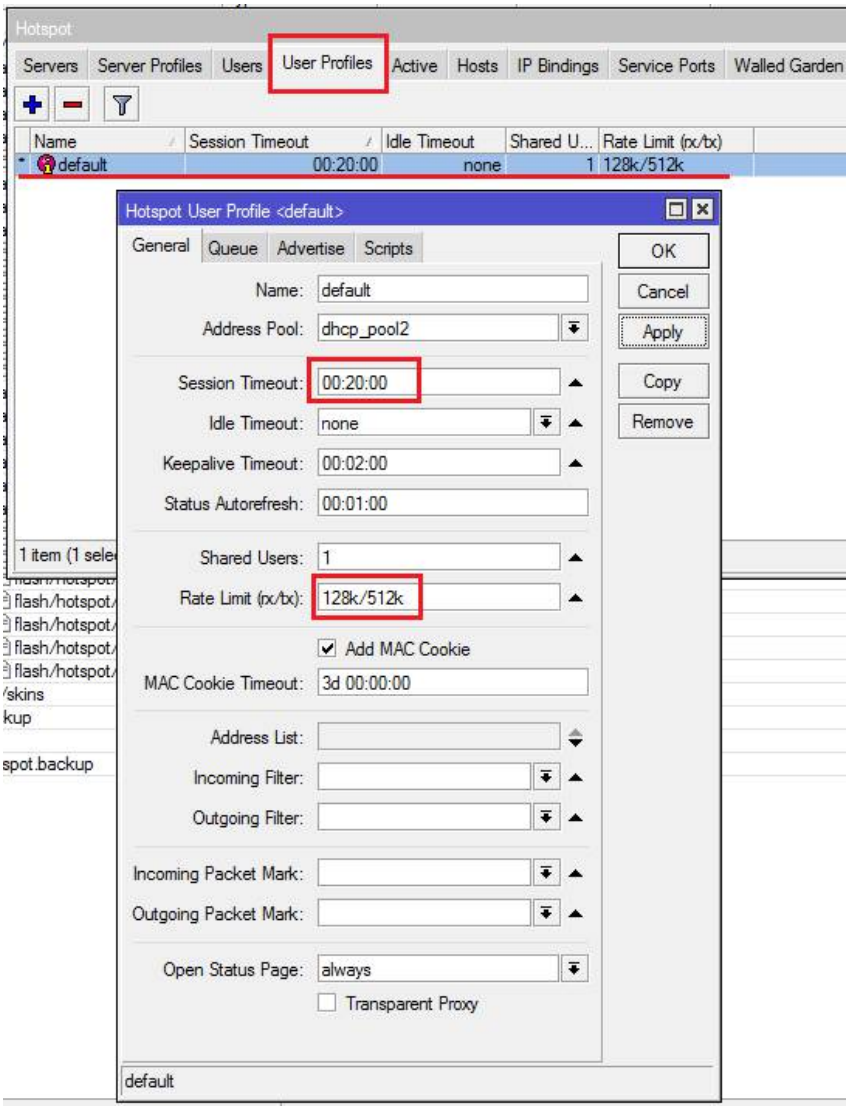
На вкладке **RADIUS** поставим галочку **Use RADIUS**, что означает что список пользователей (MAC адресов) будет храниться на радиус сервере ООО "Уолкерс Системс":



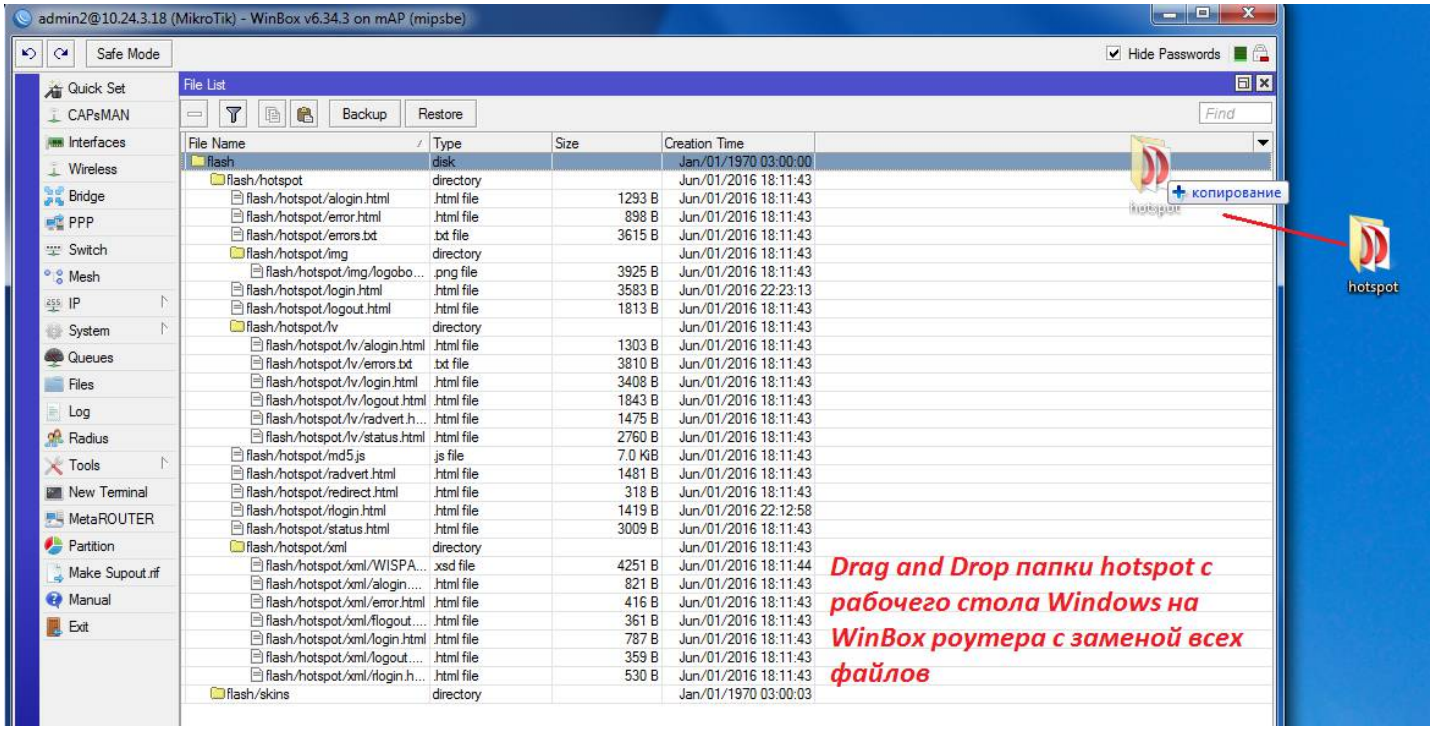
Добавим список хостов и IP адресов к которым разрешён доступ без авторизации на HotSpot, чтобы пользователи могли увидеть страничку авторизации:



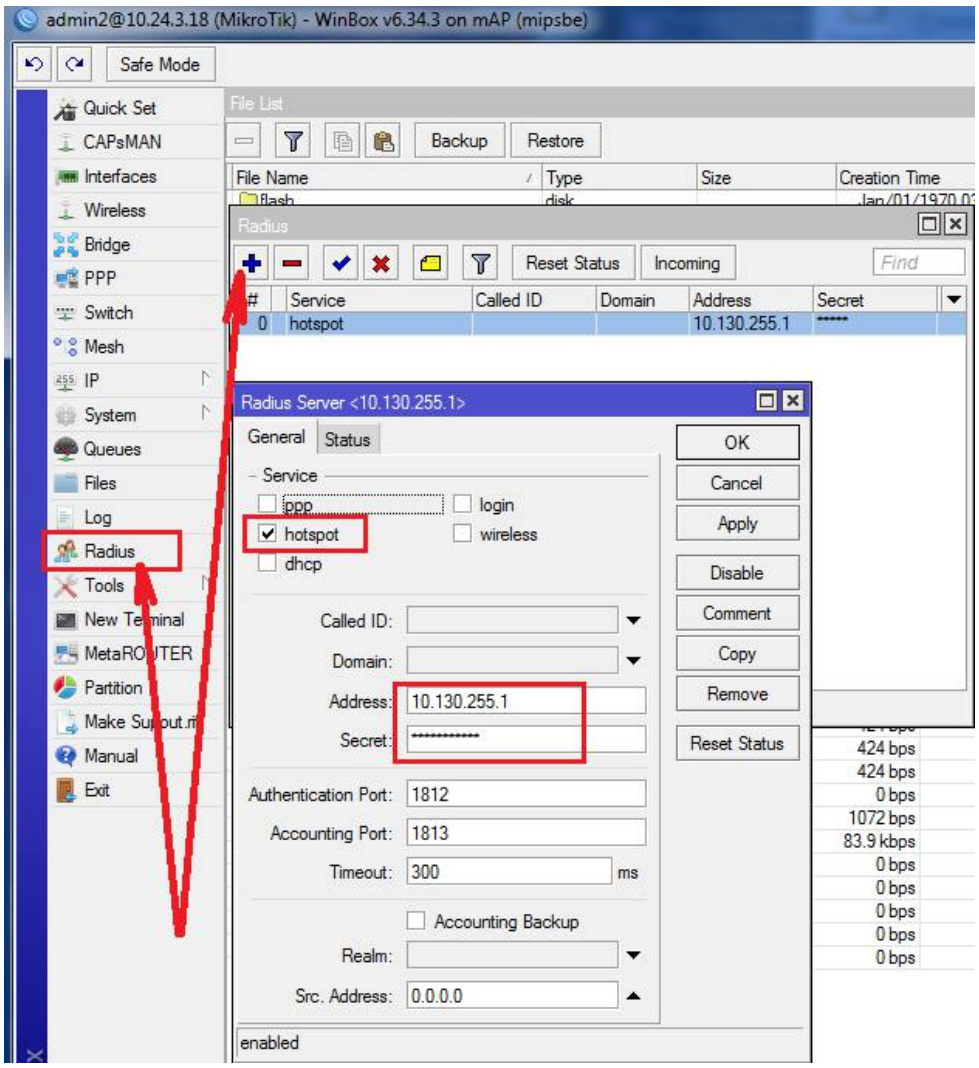
Дополнительно можно поправить **User Profiles** изменив период показа рекламы **Session Timeout.** Также можно дополнительно ограничить скорость пользователю, если в результате сбоя отказал основной канал связи с интернетом. Выставлено 128k исходящая скорость, 512k загрузка:



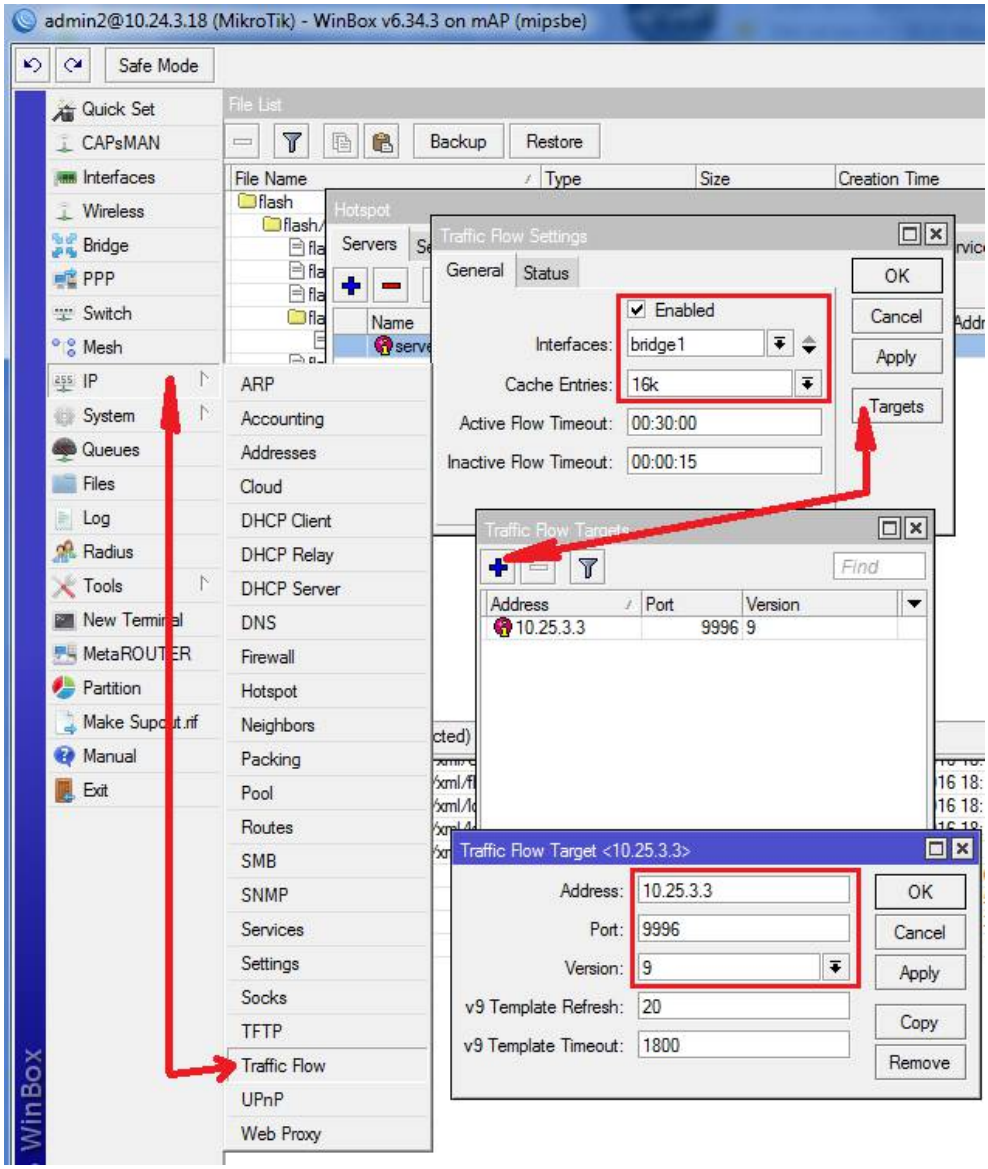
Что касается папки hotspot на самом роутере, то оно не годится нам и его следует заменить на то что мы предоставим: скачать



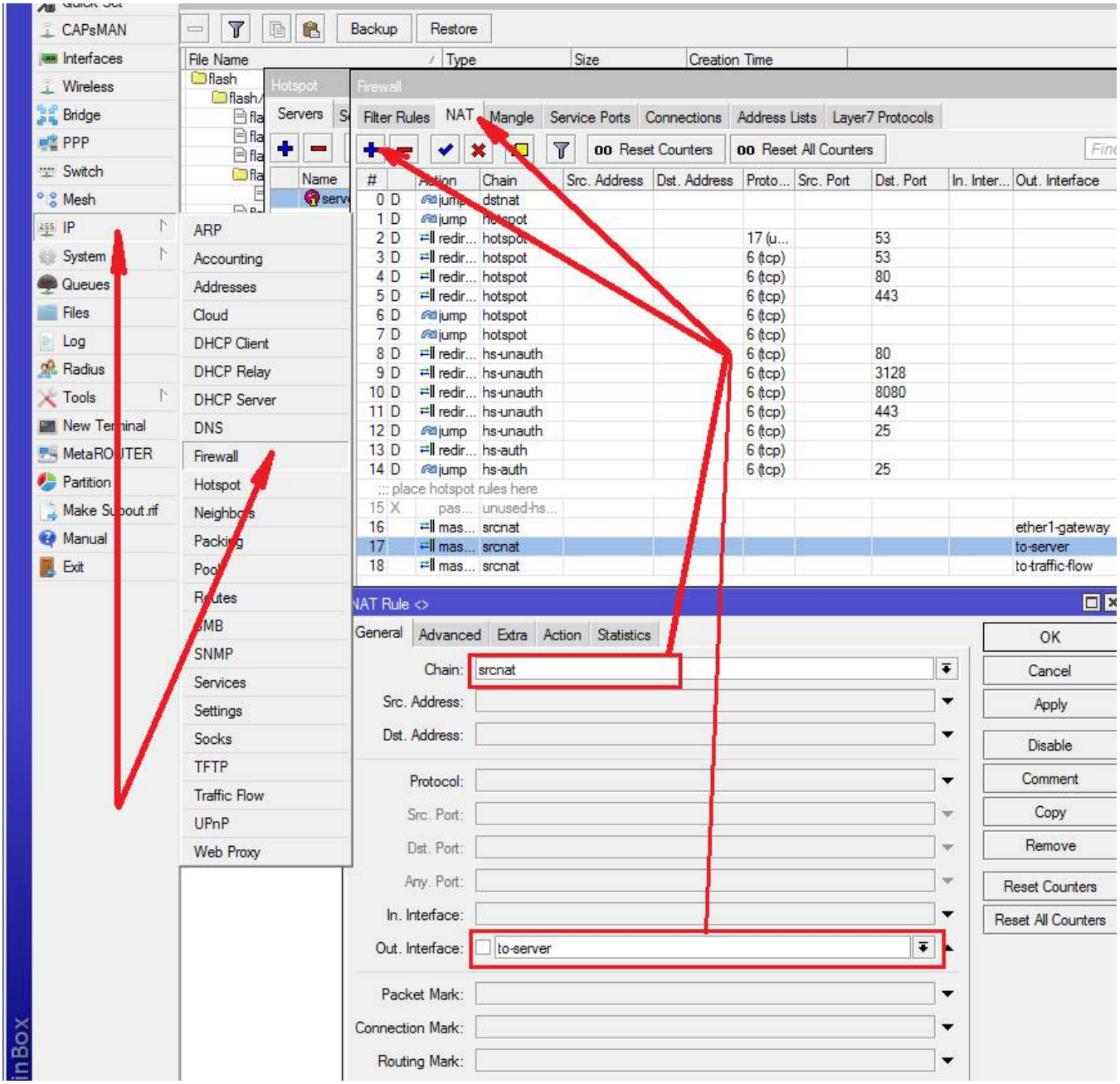
Номера телефонов и MAC адреса пользователей хранятся на FreeRadius сервере. Настроим подключение роутера к серверу. Укажем IP адрес его, сервис для которого он используется и пароль:



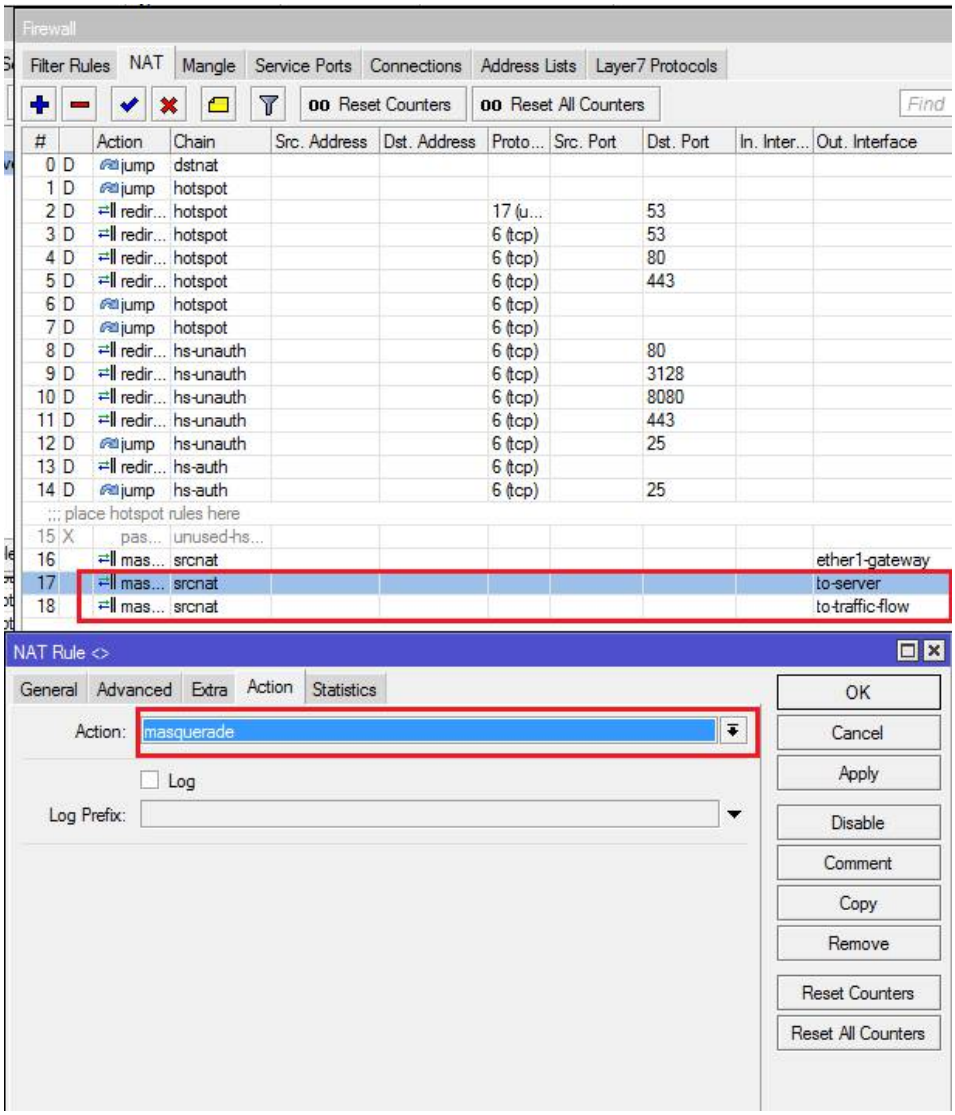
Сведения о трафике пользователей собираются на внешнем сервере (коллекторе) работающим с протоколом **netflow**. В данном примере показана работа по протоколу 9-ой версии. Включим сенсор netflow на роутере поставив галочку в поле **Enable.** Выберем интерфейс с которого нужно собирать статистику, для того чтобы в анализаторе не было дублированных данных выбираем только интерфейс на котором есть наши пользователи. Нажав кнопочку Terget добавляем IP адреса серверов (коллекторы **netflow**). Собирать данные можно на нескольких серверах. Данные которые можно увидеть в анализаторе будут содержать IP адрес, протокол и порт по которому происходит передача данных от пользователя и к нему. Также собираются сведения о количестве трафика и времени использования интернета.



Следует сделать также **scr-nat** с Action **masquarade** на интерфейс ведущий к серверам: FreeRADIUS, NetFlow коллектору:

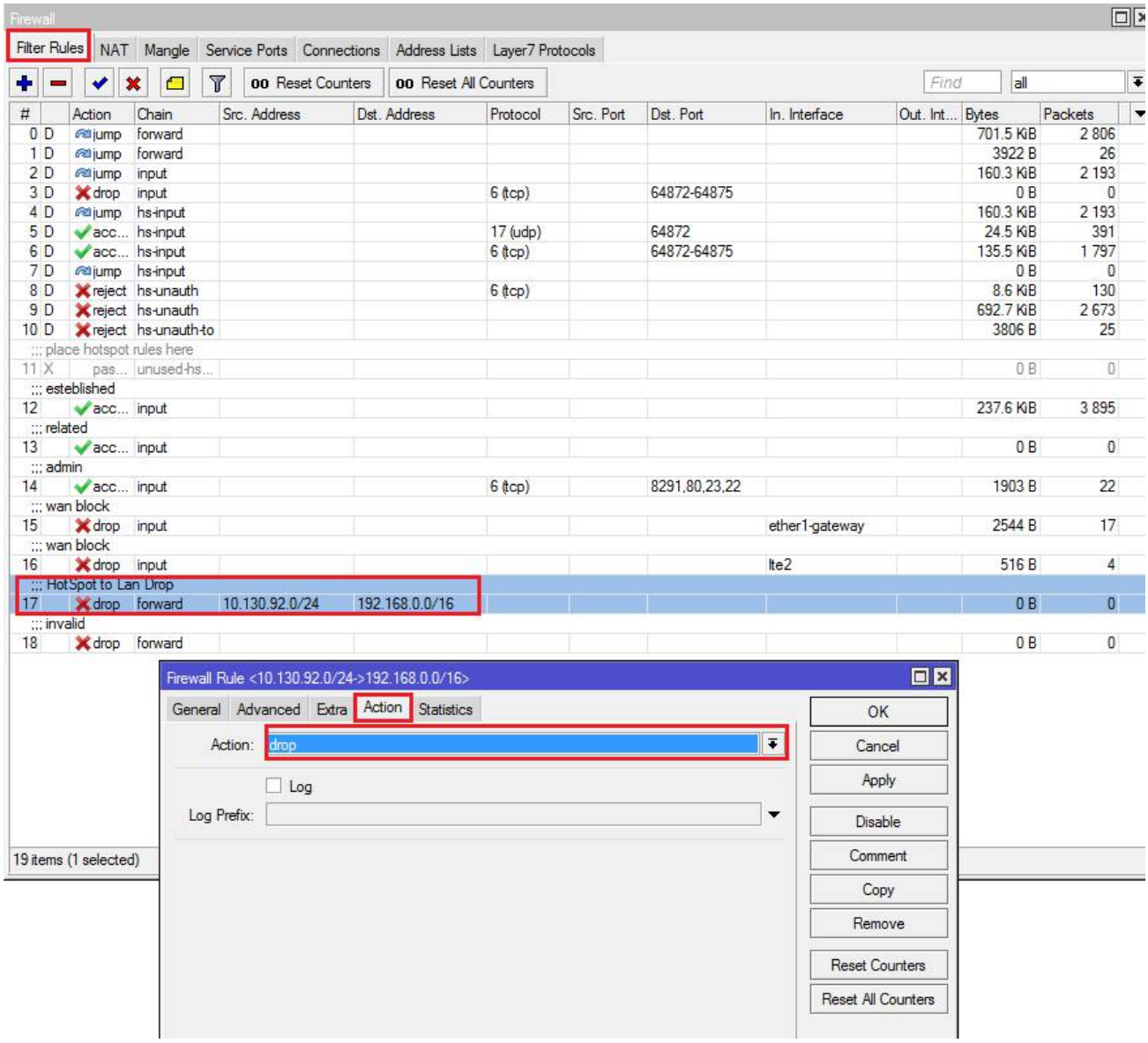


Можно также обратить внимание на правила с буквой D (от dynamic), автоматически добавленые HotSpot:

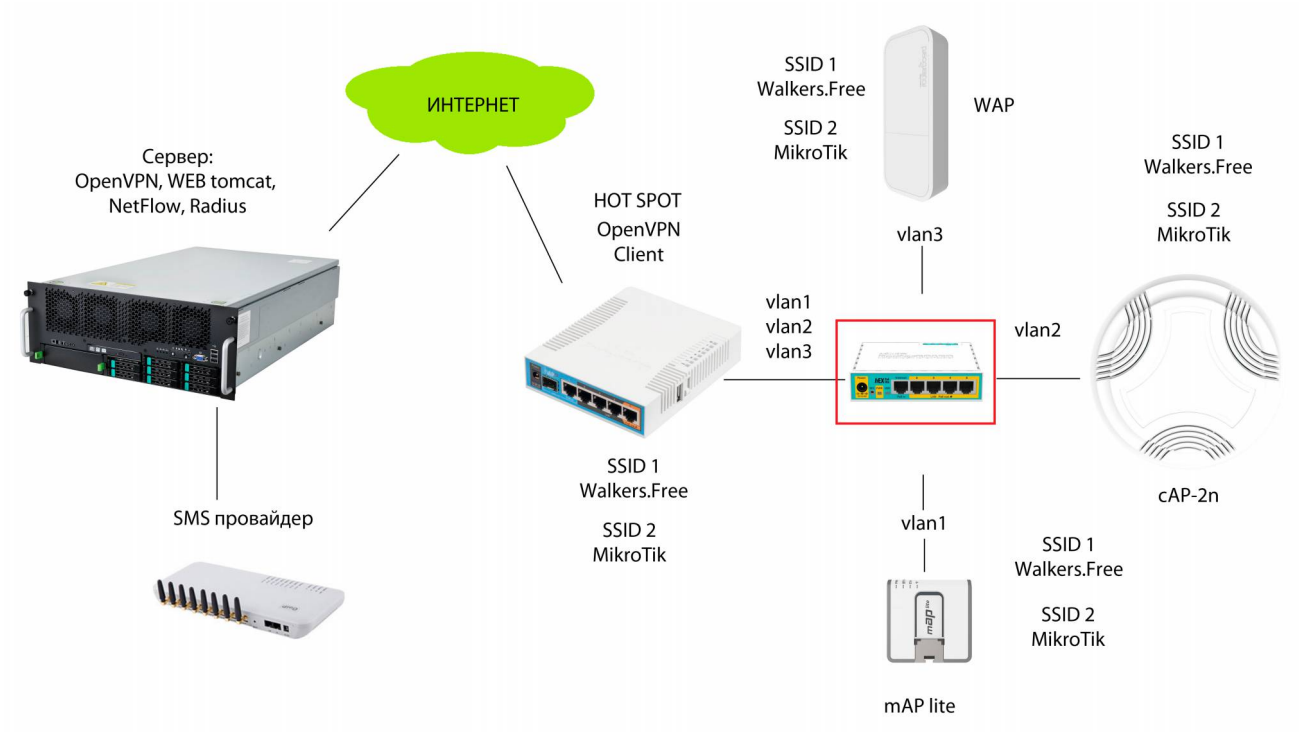


Настроим правила фильтрации трафика. Если на маршрутизаторе реальный (статический) IP адрес в интернете рекомендуем проверить наличие в цепочке input на внешнем интерфейсе разрешающих правил с**onnection state: established** и **related**. Если необходимо, можно разрешить ICMP, WEBBOX, WINBOX, SSH, Telnet. Остальной трафик к внешему интерфейсу лучше закрыть действием **drop**, что позволит уменьшить атаки на такие сервисы роутера как DNS и др..

Также следует в цепочке **forward** запретить доступ из сети с SMS авторизацией в сеть персонала и сетевого оборудования 10.130.92.0/24 –>> 192.168.0.0/16 действие**Drop**.

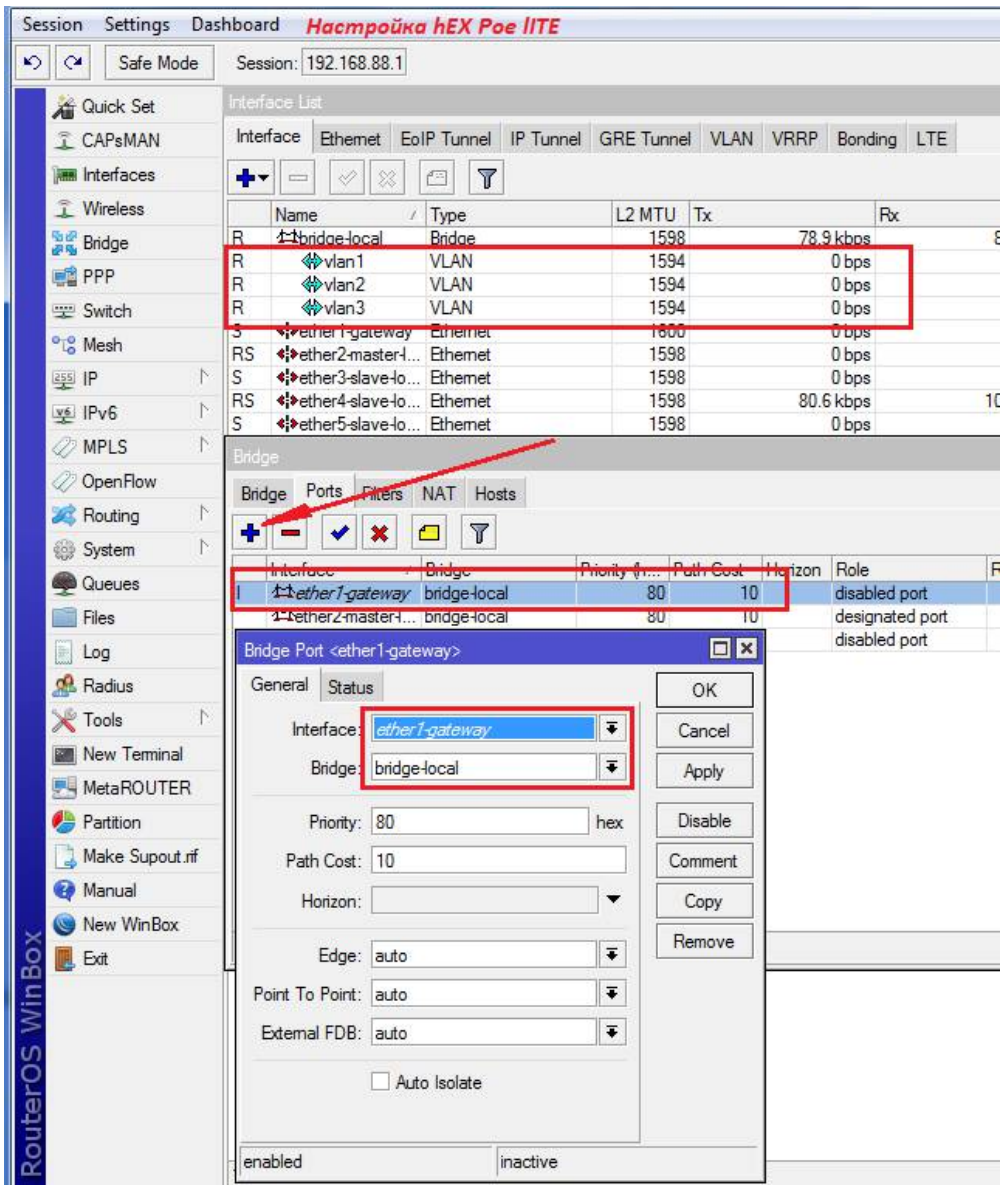


Настроим **hEX PoE lite** поддерживающий пассивный PoE и позволяющий строить недорогие сети в местах где невозможно запитать Wi-Fi точки доступа, кроме как по ethernet кабелю. На схеме он выделен красным:

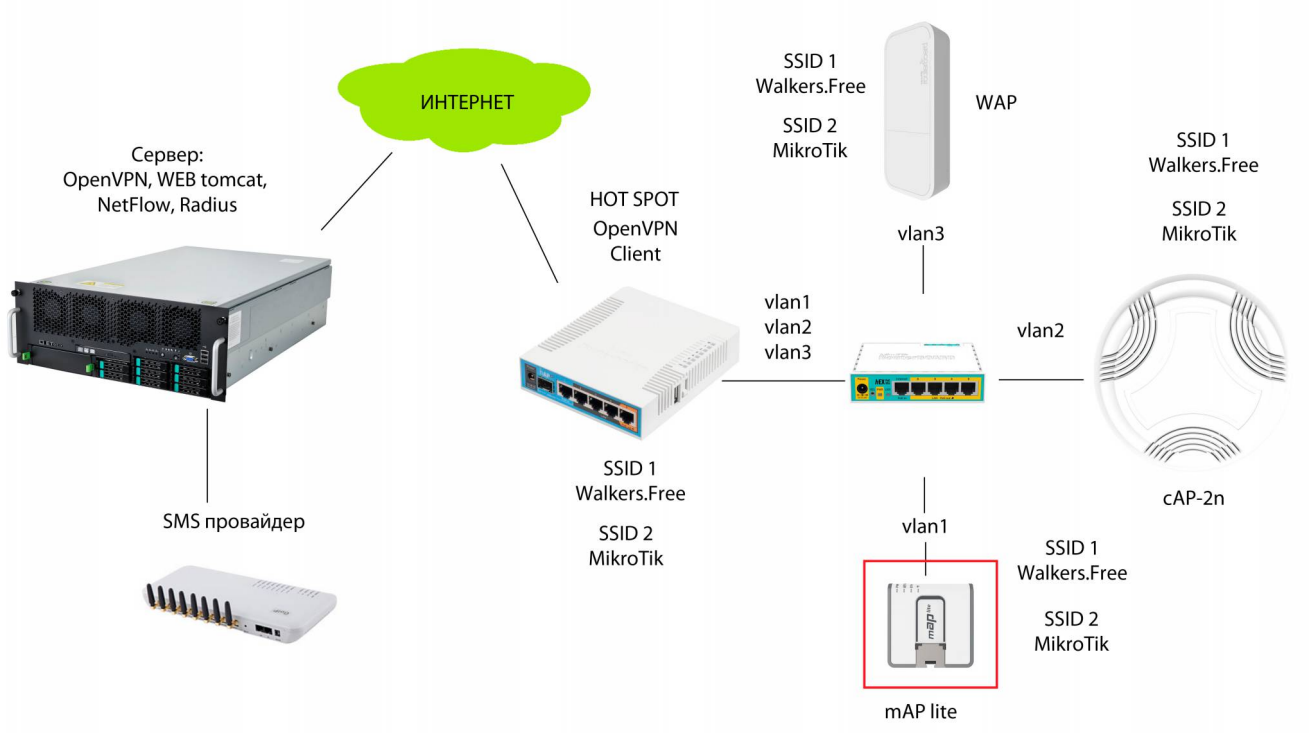


Используем его как свитч и поэтому добавим **ether1-gateway** и группу портов 2-5 в **local-bridge**. Вторым действием можно добавить vlan1, vlan2, vlan3 с метками

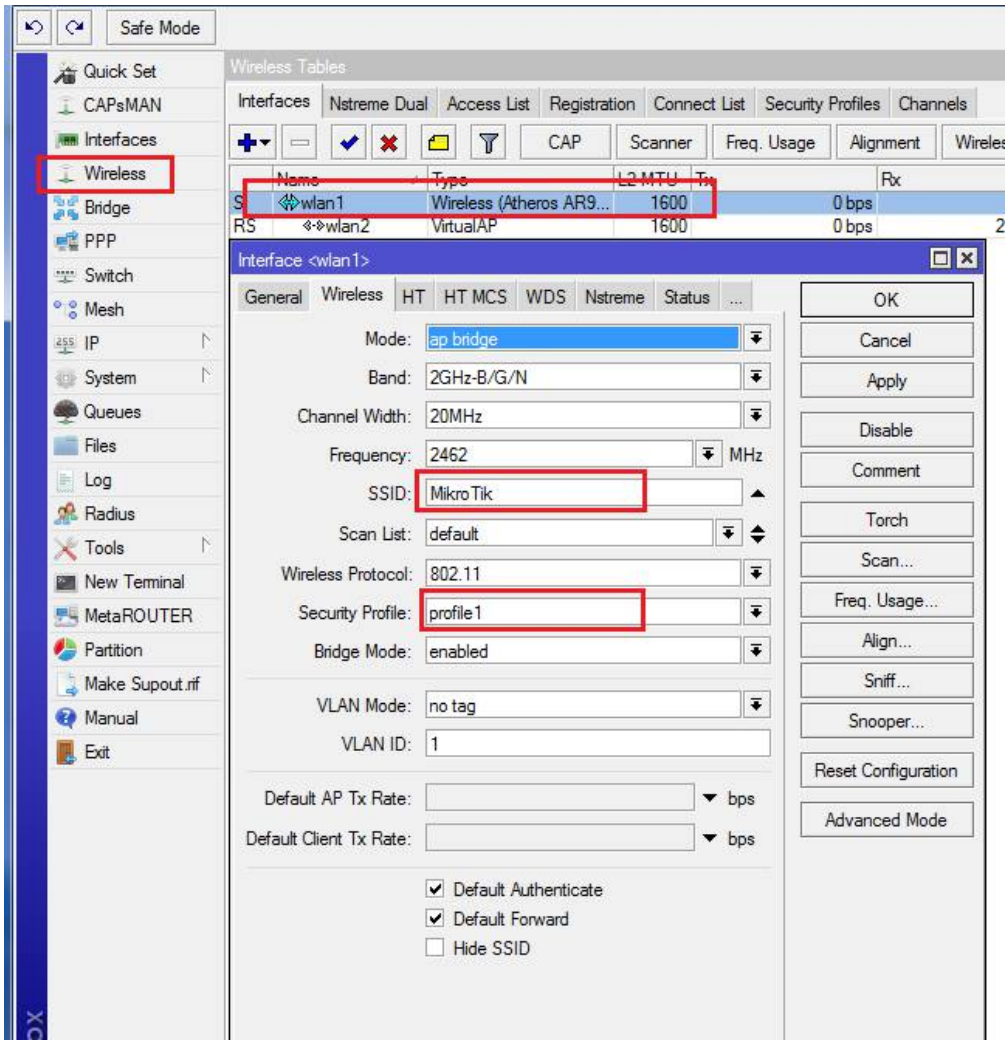
1, 2, 3 прикрепив их к этому бриджу. Дополнительно, если необходимо, можно удалить IP адресс 192.168.88.1/24 с маршрутизатора, выключить **DHCP** сервер, и навесить **DHCP-client** на **local-bridge:**



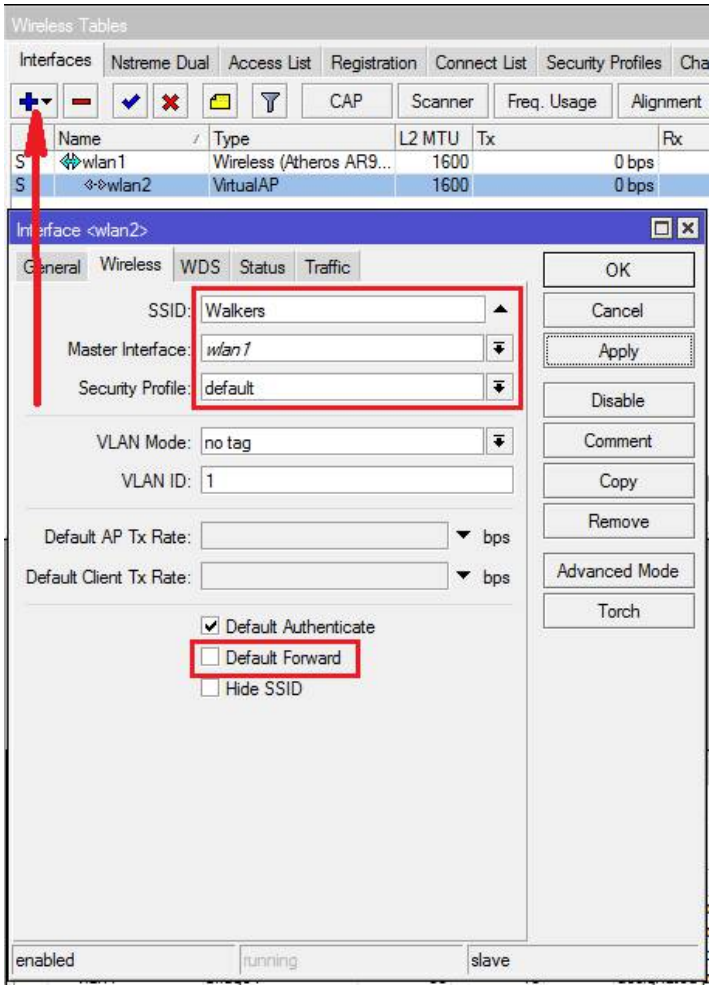
Далее настроим одну из конечных Wi-Fi точек доступа mAP lite:



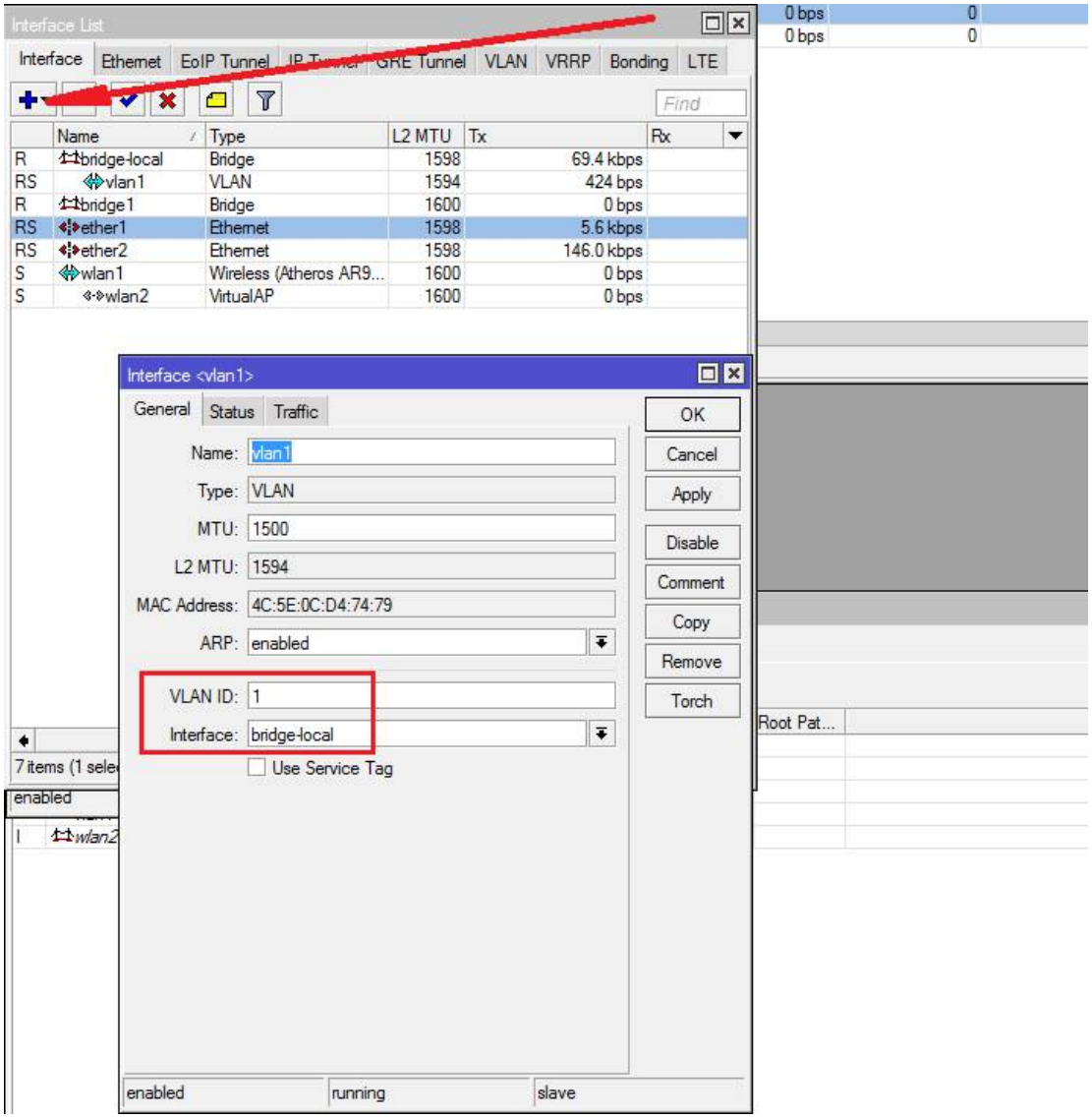
Настроим сеть персонала кафе на mAP lite выбрав предварительно созданый **profile1** где содержатся параметры шифрования и пароль доступа к сети:



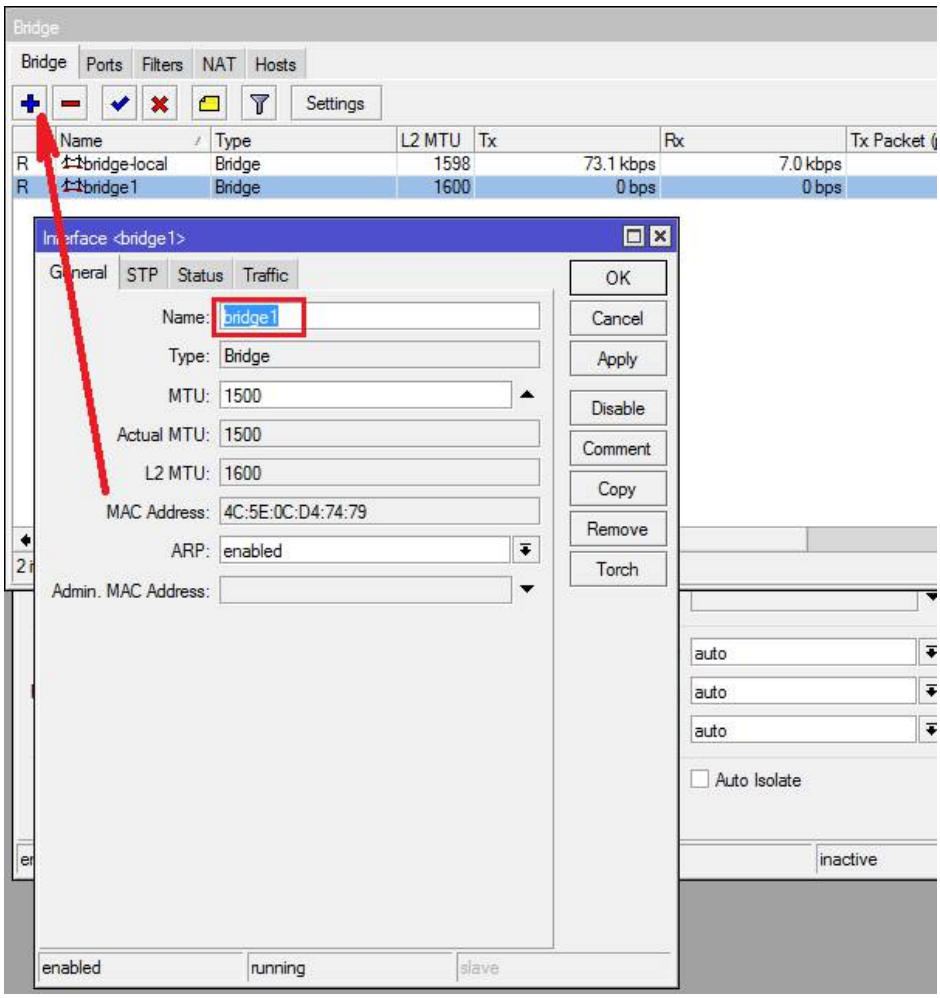
Создадим виртуальную точку доступа **vlan2** с SSID Walkers. Используем профиль **default** который не содержит пароля. Запрещаем forward клиентов данными между друг другом:



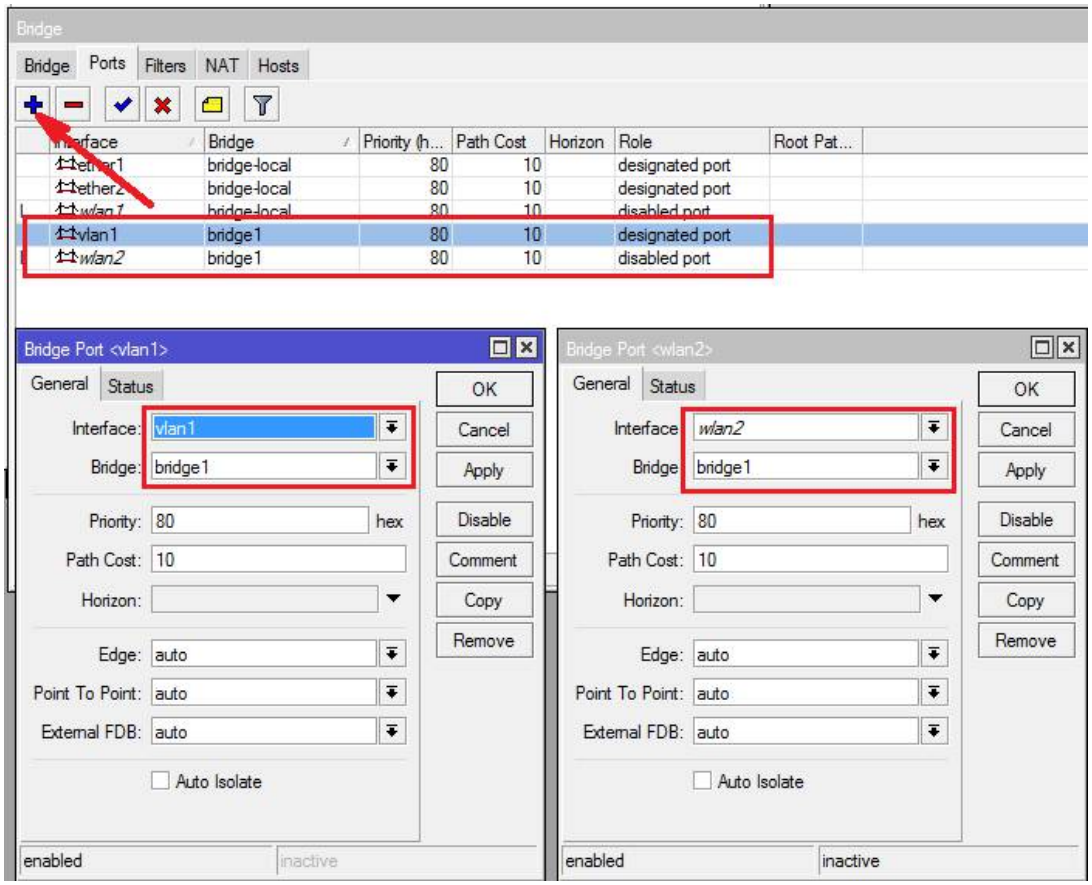
Вешаем **vlan1** с id 1 на **bridge-local**:



Создаём новый **bridge1** без настроек:



Добавляем виртуальный локальный интерфейс **vlan1** и виртуальный беспроводной интерфейс **wlan2** (SSID Walkers.Free) в **bridge1:**



Дополнительно по аналогии с hEX PoE lite можно удалить IP адрес 192.168.88.1/24, DHCP сервер, правила фильтрации.

Настройка закончена! Конфигурацию хотспота с SMS авторизацией для mAP-2n можно скачать по этойссылке. Логин: admin пароля нет.