

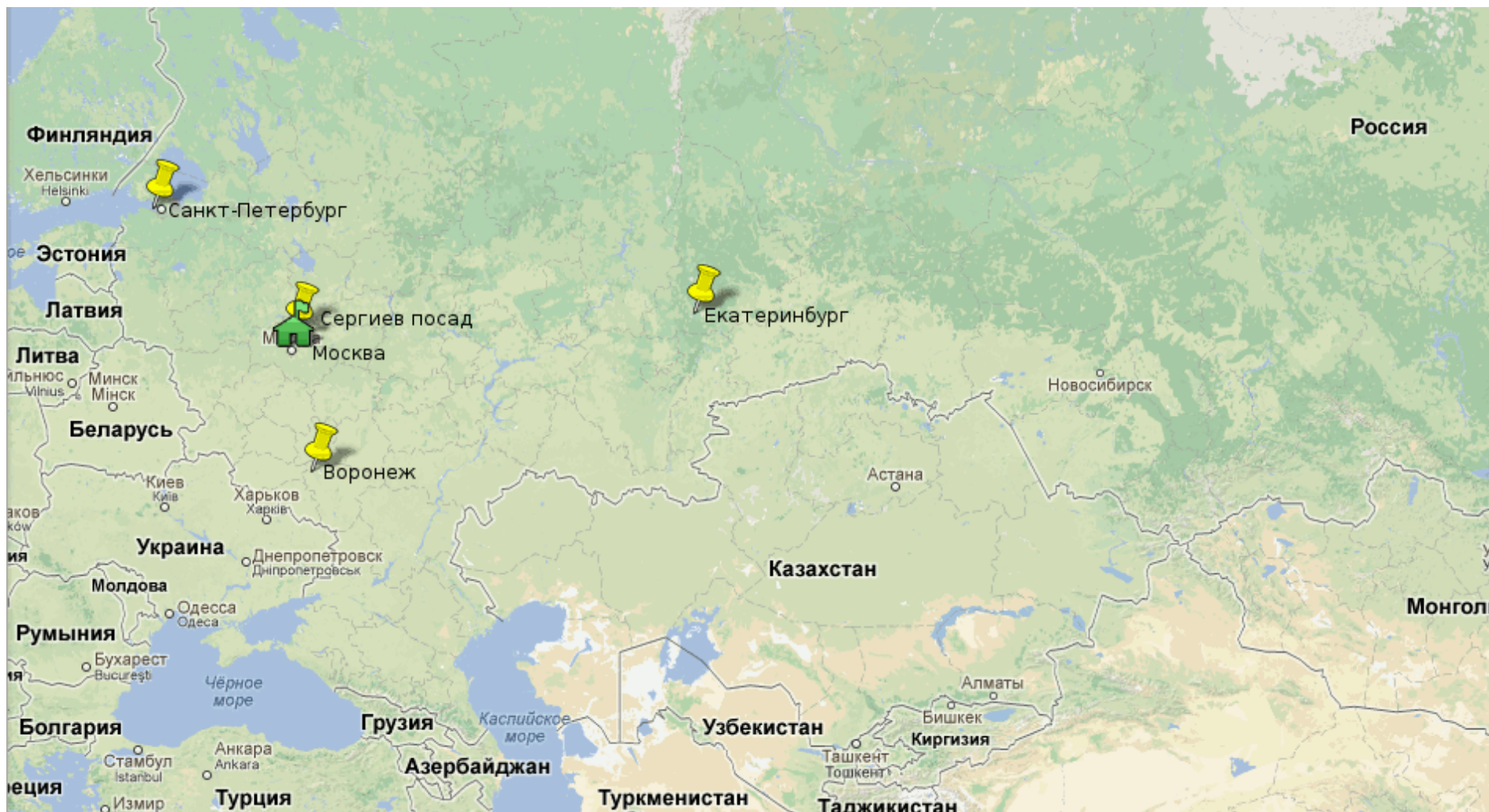
Предоставление доступа в Интернет по билетам

Москалёв Михаил
ООО «Роутерз»

Москва, 2013

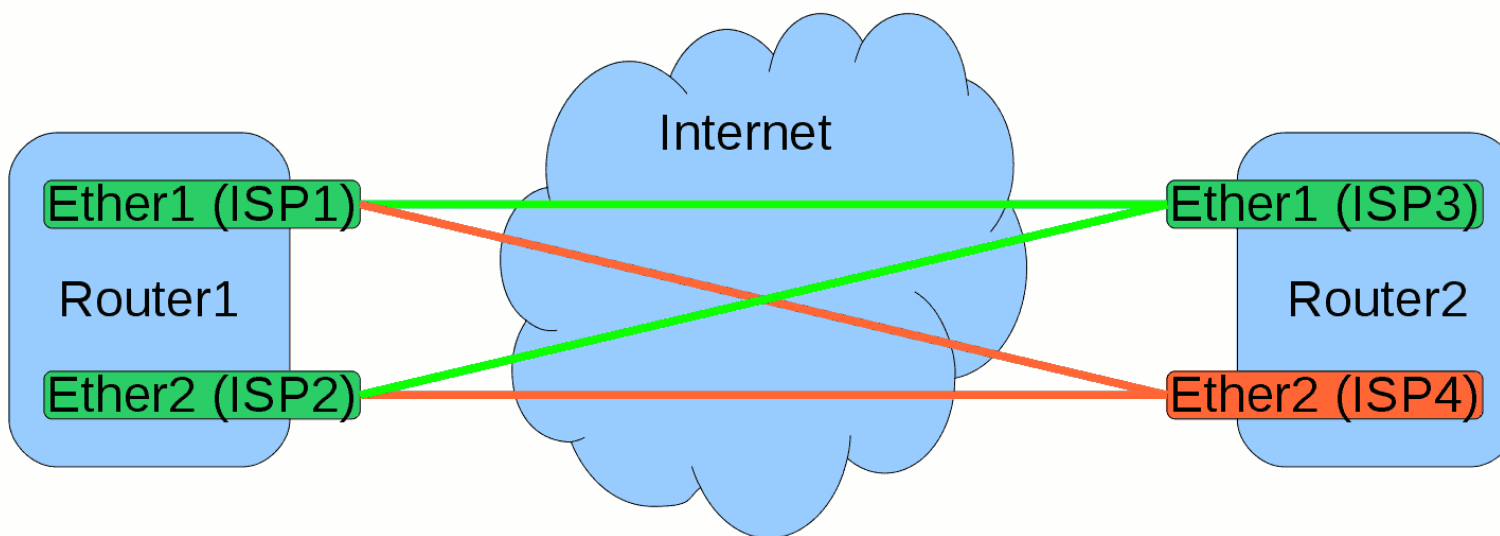


ООО «Роутерз» – учебный центр MikroTik в России и странах СНГ и дистрибьютор RouterBOARD.



RouterZ

Наша специализация — обучение и разработка решений на основе ПО и оборудования MikroTik.
Например: DualWAN VPN.



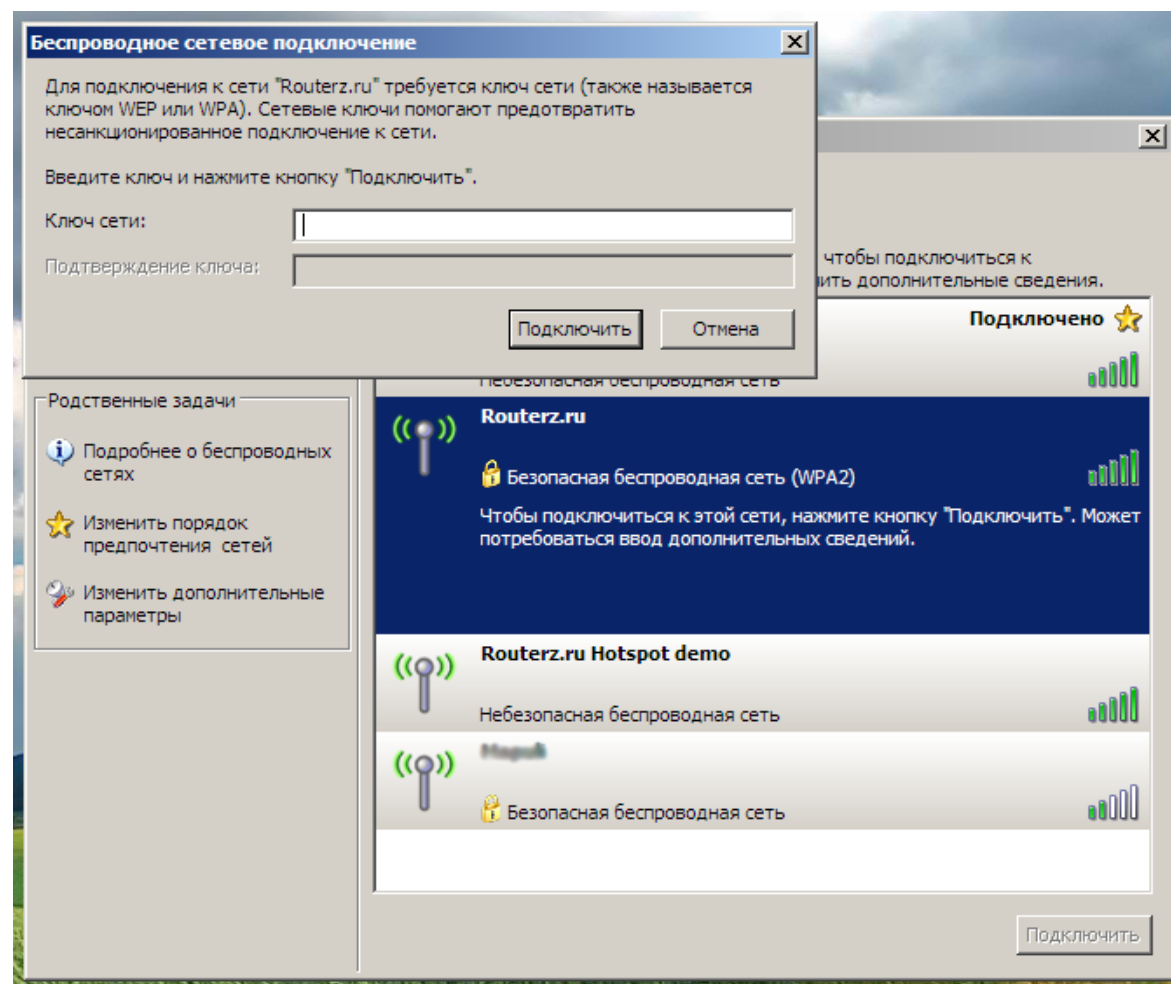
- Москалёв Михаил –
Технический директор ООО "Роутерз",
сертифицированный тренер Mikrotik
с 2011 года, сертификат # TR0125.

Пользователь оборудования MikroTik
с 2009 года.



Предоставление доступа в интернет в публичном месте

Точки доступа
в кафе, ресторанах,
гостиницах,
офисах и
на конференциях



Предоставление доступа в интернет в публичном месте

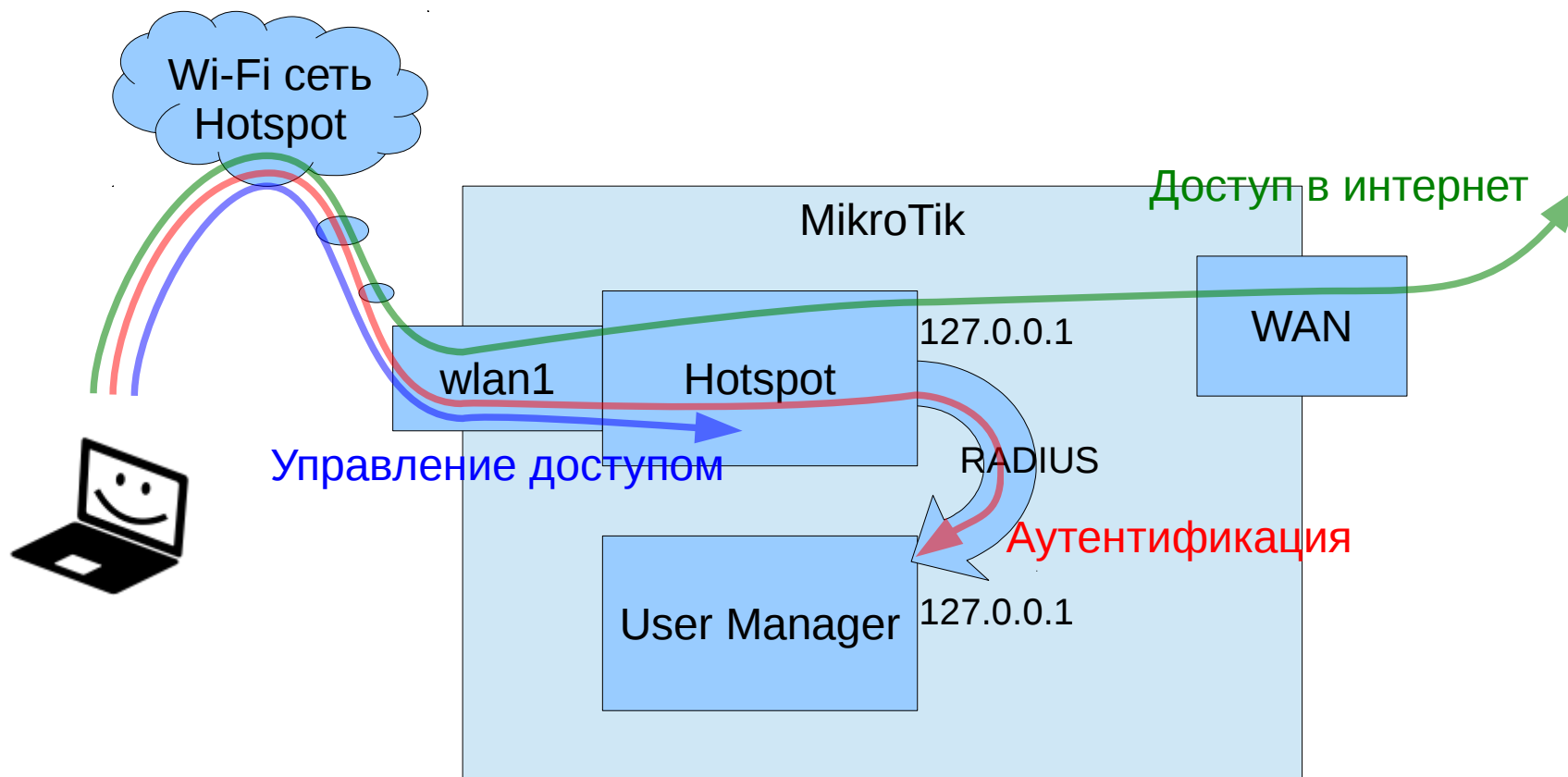
- Открытая точка доступа — полное отсутствие контроля.
- Доступ по PSK (ключу Wi-Fi), тоже не всегда удобно:
 - Нет аутентификации (все пользователи анонимны)
 - При смене PSK его нужно менять для всех пользователей

Предоставления доступа в интернет в публичном месте

Решение – интеграция следующих компонентов:

- открытая Wi-Fi сеть
- HotSpot (Captive portal) с RADIUS аутентификацией
- UserManager – RADIUS сервер и биллинг система работающая в RouterOS
- Wi-Fi принтер или предварительно сгенерированные в UserManager билеты

Схема создаваемой конфигурации



Демонстрация работы

Желающие могут ознакомиться с работой системы, получив предварительно напечатанные билеты или билеты на Wi-Fi с Wi-Fi принтера и подключиться к сети "Routerz.ru Hotspot demo"

Демонстрация работы

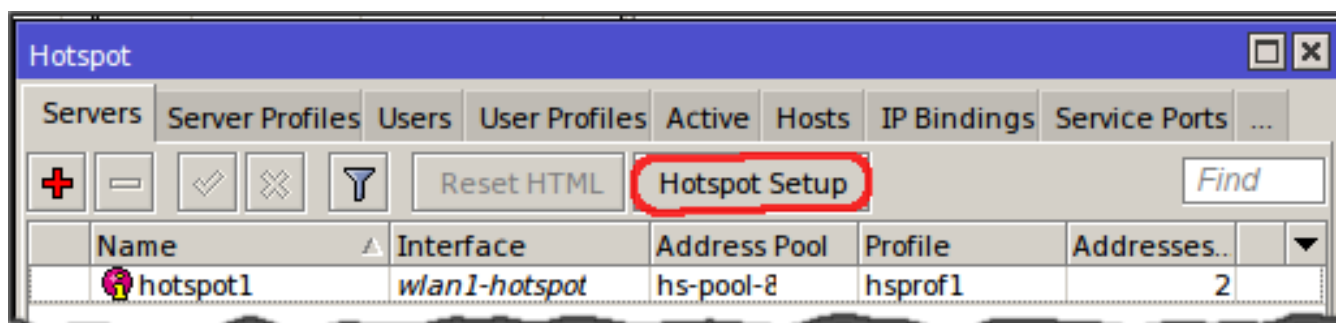
- Можно посмотреть на работу и конфигурацию Микротика, подключившись с помощью Winbox или браузера к адресу *192.168.88.1* логин *demo* без пароля
- Можно посмотреть на конфигурацию User Manager <http://192.168.88.1/userman> логин *demo* без пароля

Настройка HotSpot

- Требования к конфигурации маршрутизатора перед настройкой HotSpot:
 - IP-адрес на внешнем (WAN) интерфейсе
 - Статический IP-адрес на интерфейсе предназначенном для подключения пользователей HotSpot
 - Работающий DNS в Микротик

Настройка HotSpot

- Базовая настройка HotSpot выполняется мастером в `/ip hotspot setup` или аналогичной командой в winbox

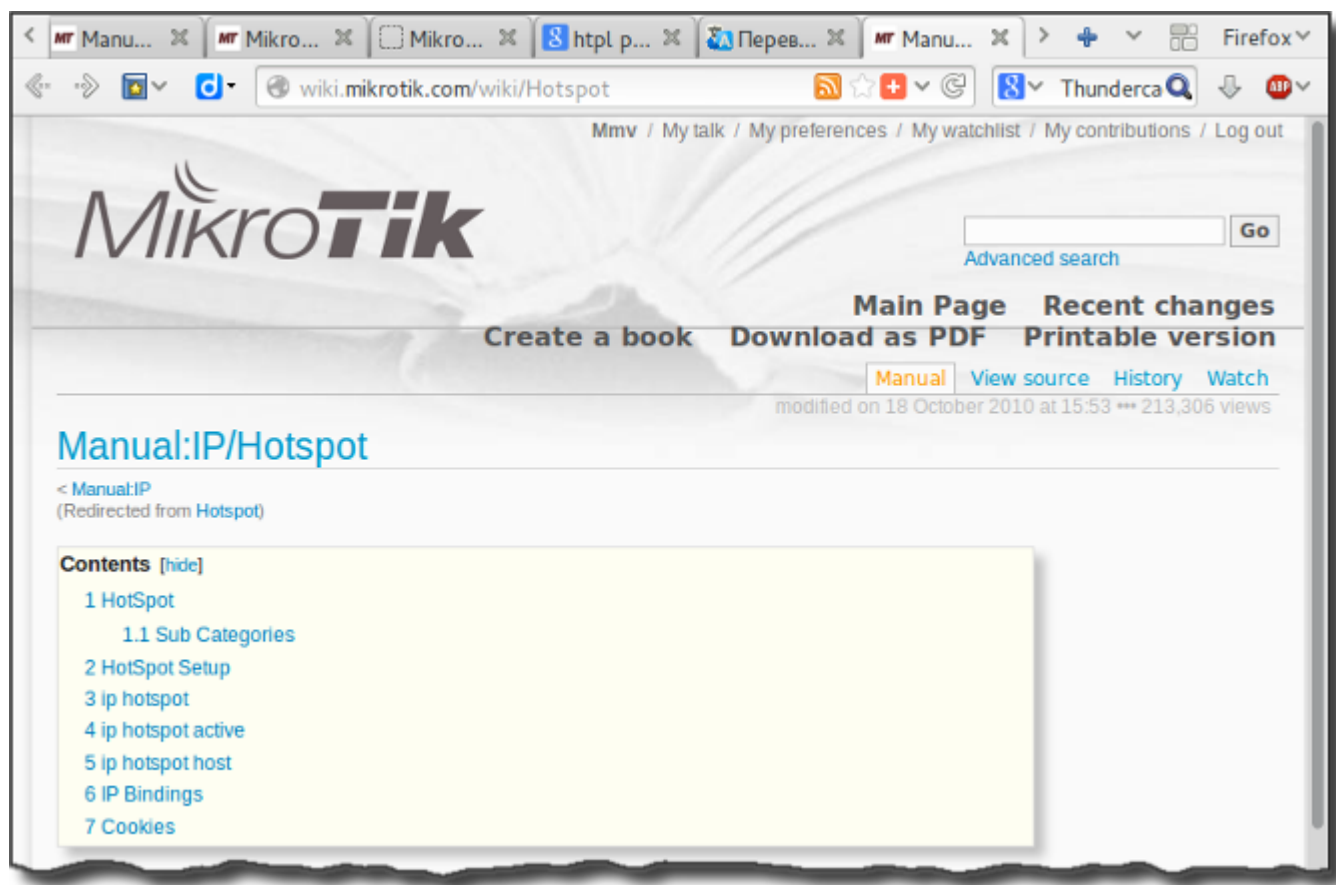


- Обратите внимание:
 - DNS имя хотспота должно быть FQDN, например, "hotspot.routerz.ru"
 - DHCP сервер для HotSpot будет создан автоматически, если его не было.

Настройка HotSpot

Более подробная информация о создании Hotspot можно посмотреть в Mikrotik Wiki

<http://wiki.mikrotik.com/wiki/Hotspot>



Настройка HotSpot

Поскольку Hotspot осуществляет идентификацию хостов по комбинации IP/MAC, для безопасности, важно обеспечить изоляцию клиентов Hotspot.

- *В данном примере достаточно отключить Default Forward для интерфейса точки доступа, на котором работает Hotspot*

Подробнее об изоляции клиентов в L2 сети можно прочитать в презентации

*<http://mum.mikrotik.com/presentations/PL10/maia.pdf>
(начиная со страницы 67)*

Установка User Manager

- User Manager – отдельный пакет обеспечивающий функциональность RADIUS сервера с веб-интерфейсом.
- Версия пакета должна совпадать с версией RouterOS

Скачать пакет и установить пакет (например user-manager-5.24-mipsbe.npk) с сайта <http://www.mikrotik.com/download> (All packages или Torrent)

Установка User Manager

RouterOS
Please choose your instruction set:

mipsbe RB400 series, RB700 series, RB900 series, RB2011 series, SXT, OmniTik, Groove, METAL

Version	Date	Upgrade package	All packages	Netinstall	Torrent	Changelog	MD5
v6.0	2013-May-20	Upgrade package	All packages	Netinstall	Torrent	Changelog	MD5
v5.25	2013-Apr-29	Upgrade package	All packages	Netinstall	Torrent	Changelog	MD5
v4.17	2011-Oct-17	Upgrade package	All packages	Netinstall	Torrent	Changelog	MD5

ALL All system downloads in one torrent file

Version	Date	Torrent	Changelog
v6.0	2013-May-20	Torrent	Changelog
v5.25	2013-Apr-29	Torrent	Changelog
v4.17	2011-Oct-17	Torrent	Changelog

Установка UserManager

Создать пользователя-администратора

```
/tool user-manager customer add \  
login="admin" password="PASS"  
permissions=owner
```

- Доступ к веб интерфейсу User Manager
http://external_ip/userman
с логином и паролем, которые мы создали
раньше

Файл русификации интерфейса User Manager можно скачать в Wiki
http://wiki.mikrotik.com/wiki/User_Manager/Languages

Интеграция UserManager и HotSpot

- В профиле HotSpot сервера нужно включить использование RADIUS

```
/ip hotspot profile set hsprof1 use-radius=yes
```

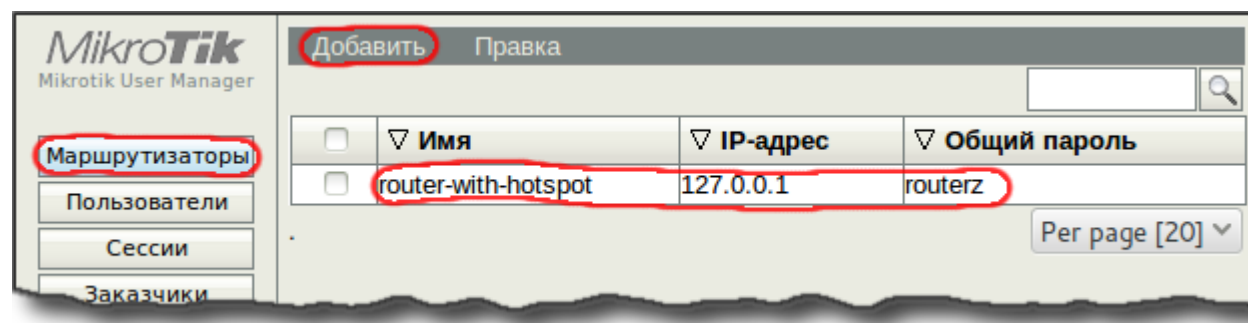
- В RouterOS нужно указать какой RADIUS сервер следует использовать:

```
/radius add service=hotspot address=127.0.0.1  
secret="routerz"
```

Подробнее о взаимодействии с RADIUS сервером можно прочитать в Wiki http://wiki.mikrotik.com/wiki/Manual:RADIUS_Client

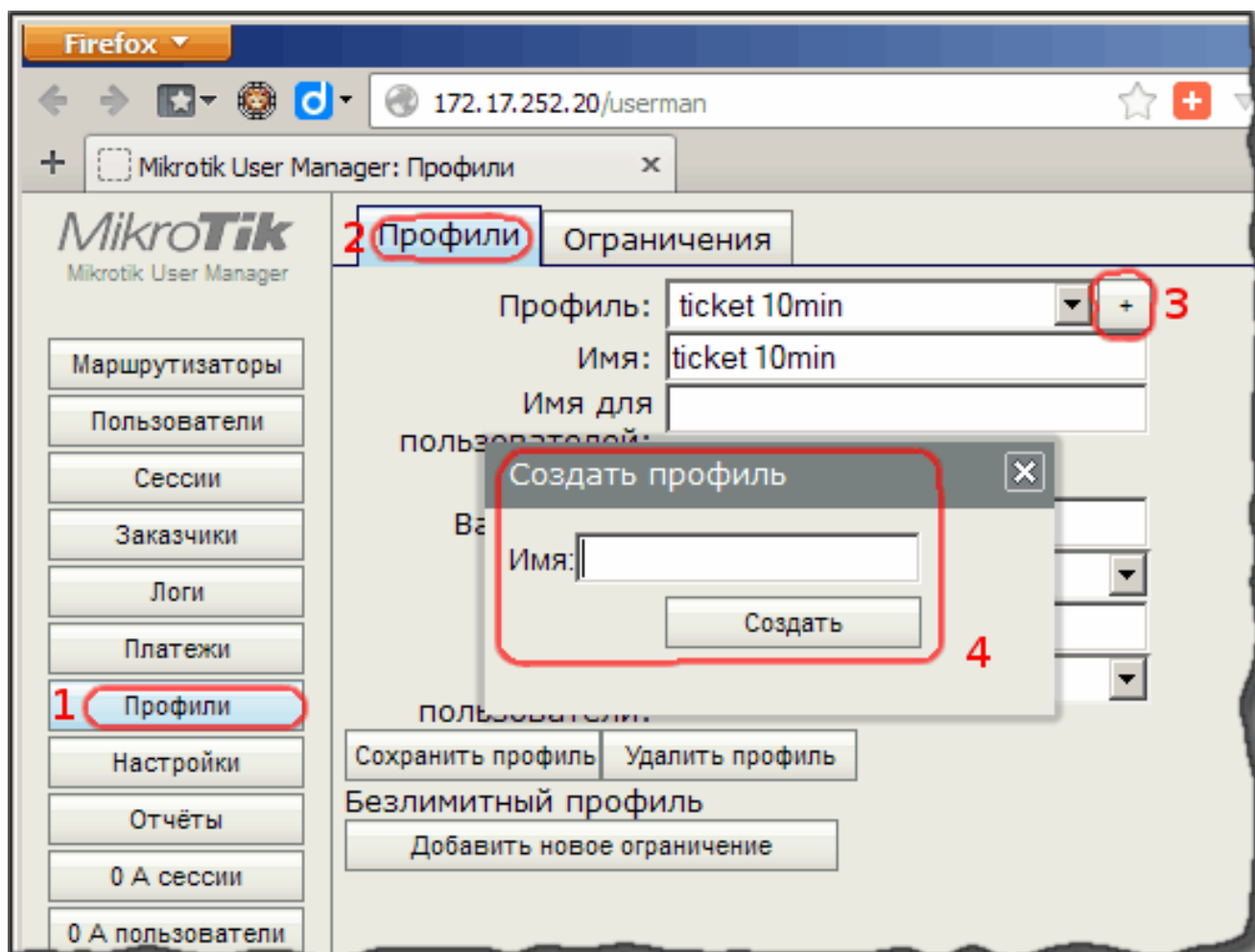
Интеграция UserManager и HotSpot

- В UserManager тоже нужно указать от какого маршрутизатора и с каким паролем следует принимать подключения:



Создание профиля пользователя в User Manager

По сути
профиль
пользователя
является
тарифным
планом



Задание ограничения в User Manager

Набор ограничений это то, чем один тариф отличается от другого

The screenshot shows the MikroTik User Manager web interface in a Firefox browser. The address bar shows the URL 172.17.252.20/userman. The interface has a sidebar with navigation buttons: Маршрутизаторы, Пользователи, Сессии, Заказчики, Логи, Платежи, Профили (highlighted), Настройки, Отчёты, 0 А сессии, 0 А пользователи, Расширенный поиск, Обслуживание, and Выход. The main content area has tabs for Профили and Ограничения (highlighted). Below the tabs are buttons for Добавить and Правка. A table lists existing limits with columns for a checkbox, Name (Имя), and Loaded (Загружено). The table contains three entries: 1h 1m/512k+burst, 1d 1m/512k+burst, and 10min 1m/512k+burst. A 'Детали ограничения' (Limit Details) dialog box is open, showing fields for Name (Имя: 30min), Owner (Владелец: admin), and Limits (Лимиты). The Limits section includes fields for Loaded (Загружено: 0B), Sent (Отправлено: 0B), Transmission (Передача: 0B), and Apptime (Аптайм: 30m). There are also sections for Speed Limits (Пределы скорости) and Restrictions (Ограничения). A 'Добавить' (Add) button is at the bottom right of the dialog box.

<input type="checkbox"/>	Имя	Загружено
<input type="checkbox"/>	1h 1m/512k+burst	
<input type="checkbox"/>	1d 1m/512k+burst	
<input type="checkbox"/>	10min 1m/512k+burst	

Детали ограничения
▲ Основной
Имя: 30min
Владелец: admin
▲ Лимиты
Загружено: 0B
Отправлено: 0B
Передача: 0B
Аптайм: 30m
▼ Пределы скорости
▼ Ограничения
Добавить

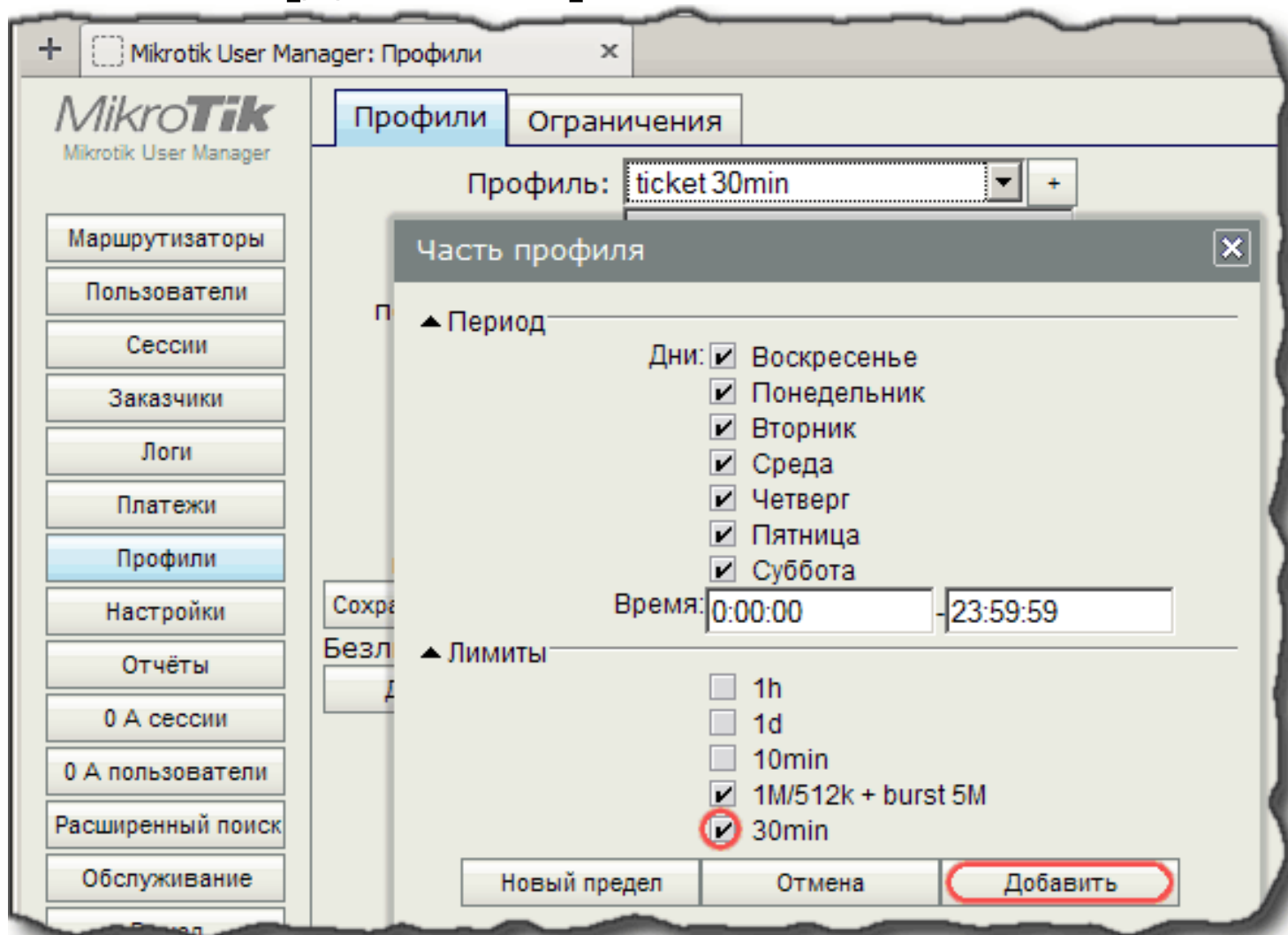
Назначение ограничений профилю в User Manager

Выбрать из выпадающего списка нужный профиль и нажать [Добавить новое ограничение]

The screenshot shows the Mikrotik User Manager web interface. The left sidebar contains a menu with the following items: Маршрутизаторы, Пользователи, Сессии, Заказчики, Логи, Платежи, Профили (highlighted), Настройки, Отчёты, and 0 А сессии. The main content area has two tabs: Профили and Ограничения. Under the Профили tab, the 'ticket 30min' profile is selected from a dropdown menu. Below the profile name, there are fields for 'Имя' (ticket 1h), 'Имя для пользователей' (ticket 1d), 'Владелец' (ticket 10min), 'Валидность' (empty), 'Запуски' (При первом входе), 'Цена' (0.00), and 'Общие пользователи' (not used). At the bottom of the main area, there are buttons for 'Сохранить профиль' and 'Удалить профиль', followed by the text 'Безлимитный профиль' and a button 'Добавить новое ограничение' which is highlighted with a red circle.

Назначение ограничений профилю в User Manager

Отметить галочками нужные ограничения (можно несколько) и нажать [Добавить]



User Manager - назначение ограничений профилю

В результате получаем профиль с установленными ограничениями

The screenshot shows the MikroTik User Manager web interface. On the left is a sidebar with navigation buttons: Маршрутизаторы, Пользователи, Сессии, Заказчики, Логи, Платежи, Профили (highlighted), Настройки, Отчёты, 0 А сессии, 0 А пользователи, and Расширенный поиск. The main area has two tabs: Профили and Ограничения. The Профили tab is active, showing a form for editing a profile named 'ticket 30min'. The form fields are: Профиль (dropdown), Имя (text), Имя для пользователей (text), Владелец (text: admin), Валидность (text), Запуски (dropdown: При первом входе), Цена (text: 0.00), and Общие пользователи (dropdown: not used). Below the form are buttons: Сохранить профиль and Удалить профиль. The Ограничения профиля section contains a table with two rows: one for 'Active' (checkbox) and one for 'Всегда' (checkbox). The 'Всегда' row has a value of '30m' for 'Предел аптайма' and a list of speed limits: '1M/512K 5M/5M 750K/480K 10s/20s 5 1M/512K'. At the bottom are buttons: Добавить новое ограничение and Удалить выбранные ограничения.

MikroTik
Mikrotik User Manager

Маршрутизаторы
Пользователи
Сессии
Заказчики
Логи
Платежи
Профили
Настройки
Отчёты
0 А сессии
0 А пользователи
Расширенный поиск

Профили Ограничения

Профиль: ticket 30min +

Имя: ticket 30min

Имя для пользователей:

Владелец: admin

Валидность:

Запуски: При первом входе

Цена: 0.00

Общие пользователи: not used

Сохранить профиль Удалить профиль

Ограничения профиля

<input type="checkbox"/> Active	Ограничения
<input type="checkbox"/> Всегда	Предел аптайма: 30m Пределы скорости: 1M/512K 5M/5M 750K/480K 10s/20s 5 1M/512K

Добавить новое ограничение Удалить выбранные ограничения

User Manager - пакетное создание билетов

Теперь с созданными профилями можно создавать пользователей и печатать билеты

Для массового создания пользователей нужно выбрать [Добавить] [Группа], указать количество пользователей, префикс и профиль.

The screenshot shows the MikroTik User Manager web interface. On the left is a sidebar with navigation buttons: Маршрутизаторы, Пользователи (highlighted), Сессии, Заказчики, Логи, Платежи, Профили, Настройки, Отчёты, 0 А сессии, 0 А пользователи, Расширенный поиск, Обслуживание, and Выход. The main area has a top bar with 'Добавить', 'Правка', and 'Генерировать' buttons. Below it are tabs for 'Один' and 'Группа' (highlighted). A table with columns 'Имя пользователя', 'Время окончания', and 'Общий' is partially visible. A 'Детали пользователя' dialog box is open, showing fields for 'Владелец' (admin), 'Количество пользователей' (20), 'Префикс имени пользователя' (1-10), 'Длина имени пользователя' (6), 'Пароль такой же, как логин' (unchecked), 'Длина пароля' (6), and 'Назначить профиль' (ticket 10min). The 'Add' button is at the bottom right of the dialog.

UserManager - пакетное создание билетов

Созданных пользователей можно экспортировать в CSV-файл

```
Login,Password,Uptime Limit,Used Uptime,Used Download,Used Upload
"1-10-25aqnd","btmubb","10m","","",""
"1-10-shcbzg","74xhfb","10m","","",""
"1-10-tt9s7g","552mxt","10m","","",""
"1-10-pbmeus","sh782g","10m","","",""
"1-10-5uz7ar","zxjy06","10m","","",""
```

Или распечатать в виде билетов, что будет показано далее.

UserManager - пакетное создание билетов

Шаблон создаваемых билетов (ваучеров) можно редактировать в настройках User Manager. В данном случае внесены некоторые изменения:

МикроТик
Mikrotik User Manager

Появление | Стил | **Шаблоны** | Язык | Платёжные шлюзы | Регистрация

Имя: Vouchers

Заголовок:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html
xmlns="http://www.w3.org/1999/xhtml"> <head> <title>Vouchers</title>
<style> @media print { .noprint { display: none; } .pagebreak
{ page-break-after: always; } } </style>
<meta charset="utf-8">
</head> <body>
```

Строка:

```
<table align="center" style="color: black; font-size: 11px;"> <tr
class="space1"><td colspan="3"></td></tr> <tr> <td>Prepaid
time:</td> <td><b>%u limitUptime%</b></td> <!-- <tr>
<td>Price:</td> <td><b>%u totalPrice%</b></td> </tr> --> <tr>
<td>Login:</td> <td><b>%u username%</b></td> </tr> <tr
class="space2"><td colspan="3"></td></tr> <tr> <td colspan="3">
После попытки открыть сайт, Вы должны использовать следующий логин и
пароль </td></tr> <tr height="5px"><td colspan="3"></td></tr>
<tr> <td>Имя:</td> <td><b>%u username%</b></td> <td>
style="padding-left: 20px">(Имя пользователя которое вы вводите на
странице HotSpot)</td></tr> <tr> <td>Пароль:</td> <td><font
face="courier new"><b>%u password%</b></font></td> <td>
style="padding-left: 20px">(password that you enter at the HotSpot login
page)</td></tr> <tr height="20px"><td colspan="3"></td></tr> <tr> <td
colspan="3" align="right"> Если Вам нужно продлить время
использования Интернет, обратитесь к менеджеру. </td></tr> </table>
```

Russian

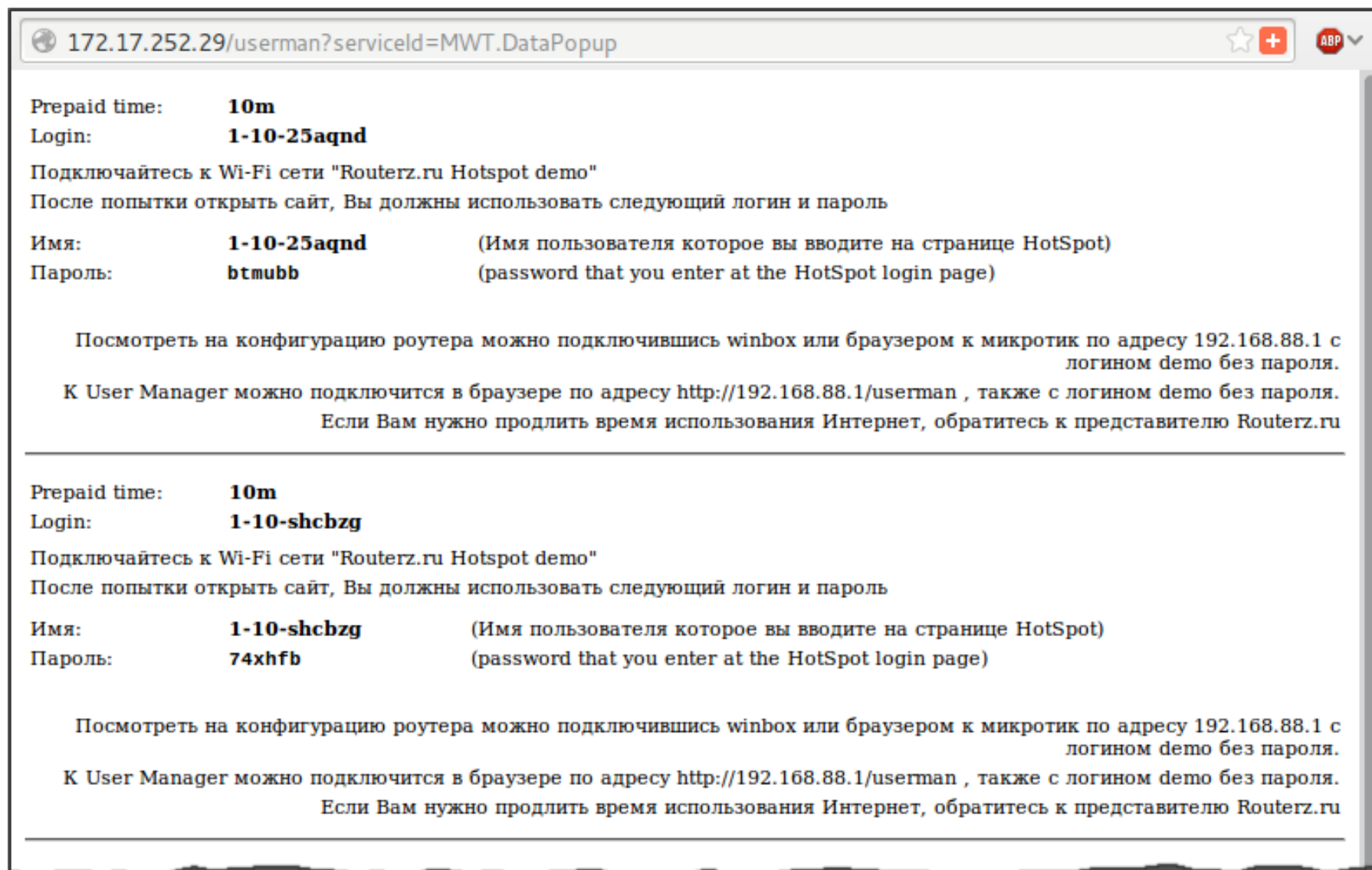
UserManager - пакетное создание билетов

- Удобно использовать префикс для поиска [1, 2] и выбор всех найденных пользователей [3], для последующего формирования билетов [4, 5]

The screenshot displays the MikroTik User Manager web interface. On the left is a sidebar with navigation links: Маршрутизаторы, Пользователи, Сессии, Заказчики, Логи, Платежи, Профили, Настройки, and Отчёты. The main area shows a table of users with columns: Имя пользователя, Имя окончания, Общий остаток времени, and Актуальный профиль. A 'Vouchers' dialog box is open in the center, with a 'Генерировать' button highlighted. Red annotations indicate the workflow: 1. Search prefix '1-'; 2. Search icon; 3. Select all users checkbox; 4. 'Vouchers' button; 5. 'Генерировать' button in the dialog.

Имя пользователя	Имя окончания	Общий остаток времени	Актуальный профиль
1-1h-xbhfnz	Неограничено	Неограничено	ticket 1h
1-1h-ka8rix	Неограничено	Неограничено	ticket 1h
1-1h-jzinbc	Неограничено	Неограничено	ticket 1h
1-1h-dxdvmv	Неограничено	Неограничено	ticket 1h
1-1h-daanwh	Неограничено	Неограничено	ticket 1h
1-1h-c2gxvh	Неограничено	Неограничено	ticket 1h
1-1h-ay6aek	Неограничено	Неограничено	ticket 1h
1-1h-a9a35k	Неограничено	Неограничено	ticket 1h
1-1h-8qn5fj	Неограничено	Неограничено	ticket 1h
1-1h-29rxms	Неограничено	Неограничено	ticket 1h

UserManager - Пакетное создание билетов



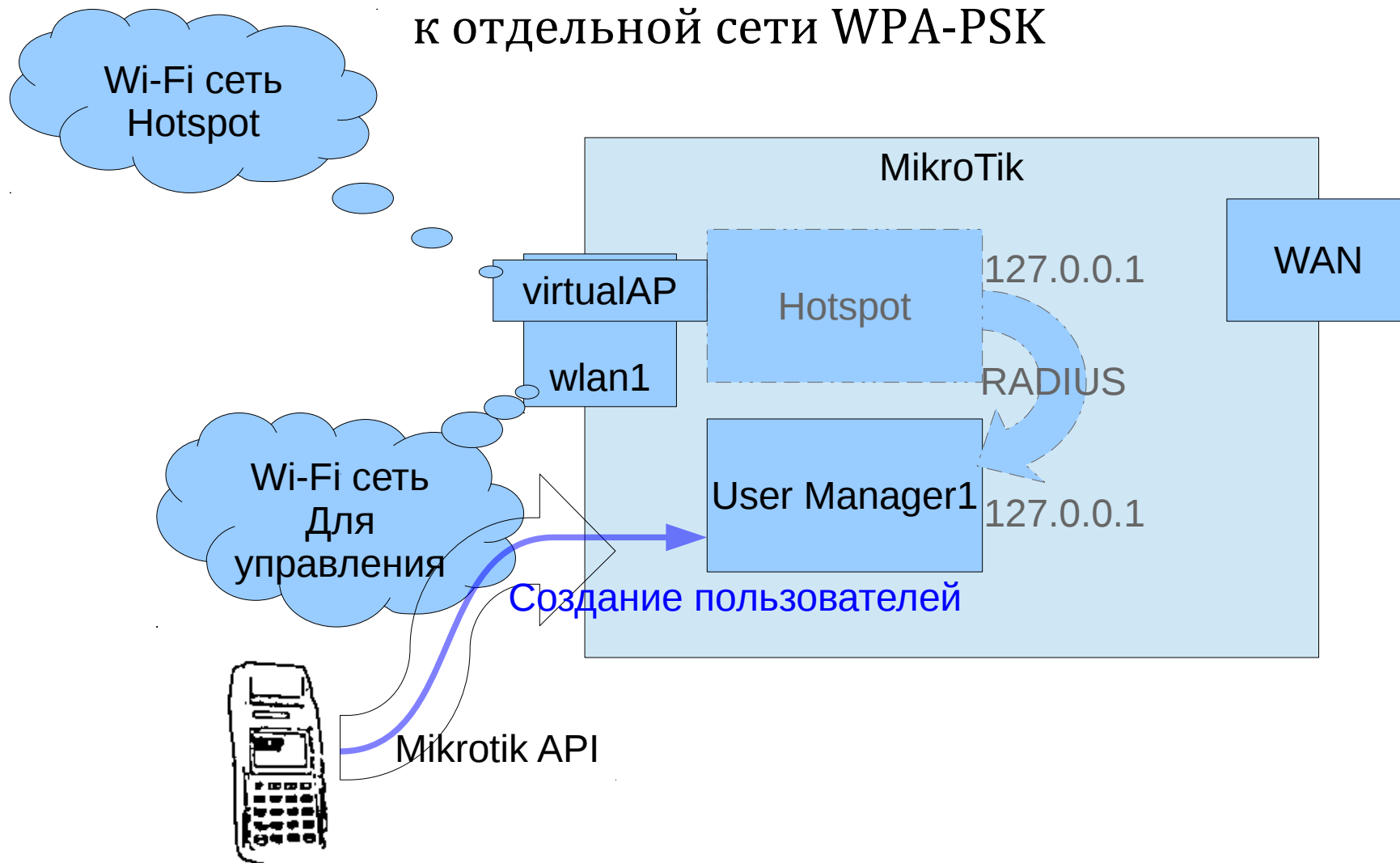
Подключение Wi-Fi принтера

- Wi-Fi принтер позволяет сразу создавать пользователя и печатать билет.
- Вначале нужно подключить принтер к Wi-Fi сети, либо к сети Hotspot задав IP-binding, либо к отдельной сети защищённой WPA-PSK.



Подключение Wi-Fi принтера

Схема создаваемой конфигурации
с подключением принтера
к отдельной сети WPA-PSK



Подключение Wi-Fi принтера

- В User Manager нужно создать пользователей с настроенными ограничениями, которые будут использоваться как шаблон при создании билетов.
 - Имена пользователей должны начинаться с **одного и того же префикса**, и у пользователей **должен быть установлен флаг *Отключено* (Disabled)**
- Имена этих пользователей будут использованы в Wi-Fi принтере как тарифные планы.

Подключение Wi-Fi принтера

- В Микротик на котором установлен User Manager нужно создать системного пользователя с правами read, write, api

```
/user group
```

```
add name=printer policy="read,write,api,  
local,!telnet,!ssh,!ftp,!reboot,!policy,!test,  
winbox,!password,!web,!sniff,!sensitive"
```

```
/user add disabled=no group=printer  
name=manager
```

- Включить сервис API

```
/ip service set api disabled=no
```

Подключение Wi-Fi принтера

Для настройки принтера нужно выполнить следующие шаги

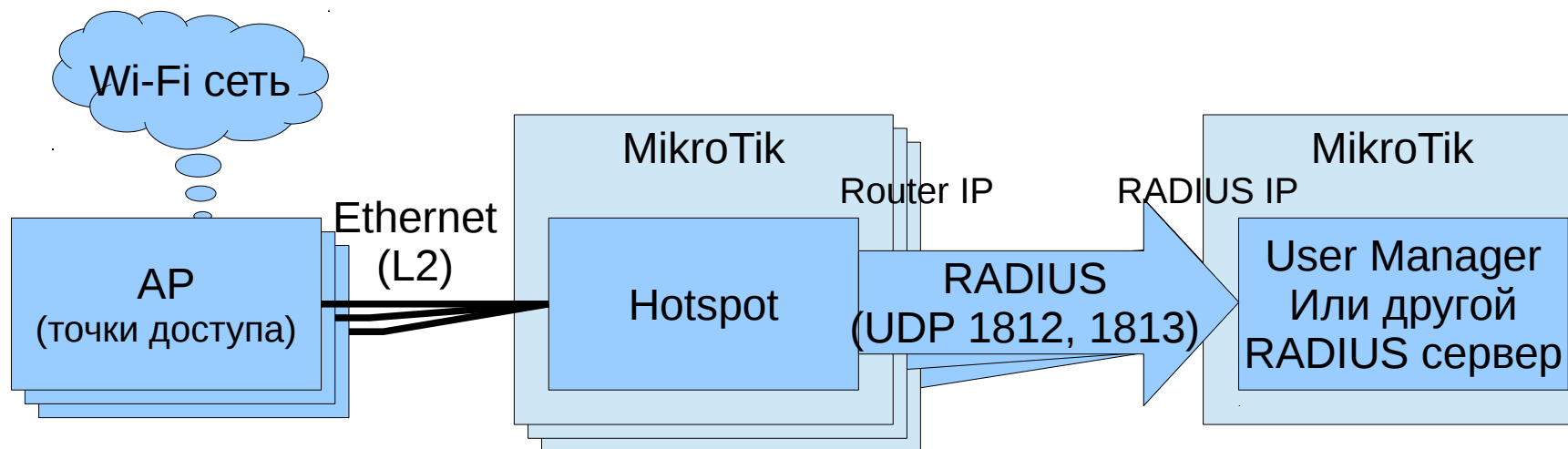
- Нажав [MENU] войти в конфигурационное меню.
- В "AP CONFIG" установить SSID и ключ защиты сети
- В "IP CONFIG", при необходимости, настроить параметры IP (по умолчанию используется DHCP)
- В "MT CONFIG" установить IP адрес, логин и пароль от Микротика на котором установлен User Manager. Там же можно протестировать связь с Микротик

Подключение Wi-Fi принтера

- В меню "TARIFF CONFIG" нужно задать
 - "Pattern" – префикс по которому опознаются пользователи-шаблоны
 - User – префикс который будет использоваться для создаваемых пользователей
- После выполнения этих настроек, в меню "Fetch Traif" следует получить список созданных в User Manager шаблонов

Что можно улучшить?

Возможное развитие архитектуры



- Поскольку связь Hotspot с RADIUS-сервером осуществляется по IP-протоколу, RADIUS-сервер может находиться в любом месте маршрутизируемой сети или связь с RADIUS-сервером может осуществляться через IP-туннель
- В качестве RADIUS-сервера может использоваться как User Manager так и другой RADIUS-сервер, например FreeRADIUS, xtradius или какой либо другой

Предоставление доступа в Интернет по билетам

Вопросы, комментарии, замечания?

Спасибо за внимание

<http://routerz.ru>

support@routerz.ru