Лучше один раз увидеть, чем сто раз услышать! Именно поэтому в интернете размещен специальный ТЕСТОВЫЙ сервер. В отличие от демо-сайта [1], на тестовом сервере установлен ПОЛНОЦЕННЫЙ сервер биллинга хотспота, а не только лишь один веб-интерфейс программы Easyhotspot. Иными словами, на тестовом сервере установлен и настроен полноценный сервер RADIUS со всеми необходимыми модулями, который может обслуживать внешние роутеры по «Варианту №3», показанному на странице [2]. Благодаря этому вы можете активировать Chillispot на вашем роутере, прошитом прошивкой от DD-WRT, и настроить его на взаимодействие с нашим сервером, на котором установлена программа Easyhotspot. Если же вы хотите провести тестирование с использованием роутеров Mikrotik, то вам понадобится инструкция [9] для активации и настройки хотспота. В результате, НА ТЕСТОВОМ СЕРВЕРЕ вы сможете непосредственно «в работе» проверить все возможности и функции программы.

1. Адрес тестового сервера и данные для входа в программу

Вход в программу Easyhotspot тестового сервера расположен по адресу:

http://91.204.72.65/easyhotspot/

Чтобы войти в программу как Администратор, введите в окне авторизации следующие данные:
Логин: **admin**
Пароль: **admin123**
Чтобы поработать в роли Кассира, вводить нужно такие данные:
Логин: **vcool**
Пароль: **vcool123**

ВНИМАНИЕ! Эти пароли предназначены ТОЛЬКО ДЛЯ ВХОДА В БИЛЛИНГ (в т. н. «черную админку»)!!! Вводить их впоследствии на странице авторизации хотспота (чтоб получить доступ в интернет) — БЕСПОЛЕЗНО, они там не сработают!!! О паролях для проверки авторизации в хотспоте — см. ниже!!!

Полную и подробную инструкцию по работе с программой Easyhotspot вы можете скачать по ссылке [3].

2. Список параметров и их необходимых значений

В приведенной ниже таблице указаны значения для параметров (настроек) программы Chillispot, которые нужно вписать в вашем оборудовании, для того, чтобы оно смогло подключиться к тестовому серверу с Easyhotspot.

Имя параметра, используемое в файле настроек (/etc/chilli.conf) программы Chillispot, установленной на компьютере с OS Linux	Имя параметра, используемое в настройках службы Chillispot, запущенной в роутере, работающем под управлением DD-WRT	Значение параметра
radiusserver1	Primary Radius Server IP/DNS	91.204.72.65
radiusserver2	Backup Radius Server IP/DNS	91.204.72.65
radiussecret	Shared Key	См. Примечание ниже!
radiusnasid	Radius NAS ID	См. Примечание ниже!
uamserver	Redirect URL	http://91.204.72.65/cgi-bin/hotspotlogin.cgi
uamsecret	UAM secret	your_uam_page_password

ПРИМЕЧАНИЯ:

- ***ВАЖНО! При копировании значений параметров из PDF-файла могут возникать ошибки — например, теряться дефисы, подчеркивания и т. д. и т. п.! Поэтому, если вы «копипейстите» параметры из PDF-файла непосредственно в поля меню настроек роутера — ВНИМАТЕЛЬНО ПЕРЕПРОВЕРЯЙТЕ, что в итоге туда вставилось!!! А то потом начинается: «я все настроил по пдф-нику, а оно не работает!!!»…***

- Пароль для связи с сервером RADIUS (подписанный как **radiussecret** или **Shared Key**) автоматически меняется самим тестовым сервером каждые четыре дня (1-го, 5-го, 9-го, 13-го и т. д. числа) около полуночи по киевскому времени (если точно, в 00:08 +2 GMT). Чтобы получить текущее значение пароля, пришлите запрос на адрес электронной почты [4]. Заказывая пароль, учтите график его смены, чтобы не оказалось, что вы, например, 12-го вечером пароль получили, а в полночь он сменился… И еще: новый пароль ГЕНЕРИРУЕТСЯ самим скриптом как произвольный набор (из 8...12 цифр) НЕПОСРЕДСТВЕННО в момент его смены! Заранее (до генерации) этот пароль не известен ни серверу, ни мне, ни самому богу или черту! Поэтому, прислать «новый» пароль я могу только после того, как сменился «старый»…
- Пароль, который я присылаю в письме в ответ на ваш запрос НЕ НАДО ВСТАВЛЯТЬ ВО ВСЕ ДЫРЫ КУДА НИ ПОПАДЯ! В том числе, НЕ НАДО пароль из письма вписывать в параметр **uamsecret** (или же **UAM secret**) — у него свое собственное значение, которое четко прописано в таблице выше! А присланный вам в письме пароль (число длинной от 8 до 12 цифр) — это именно пароль для связи с сервером RADIUS (который вписывается в параметр **radiussecret** или **Shared Key**)!
- **НЕ ВПИСЫВАЙТЕ НИЧЕГО** в поле Radius NAS ID (radiusnasid) на время тестов! Либо внимательно прочитайте инструкцию к программе [3] на предмет того, как ID хотспотов ограничивают доступ! И не удивляйтесь потом, что тестовые авторизации могут не получаться…
- Описание установки прошивки DD-WRT и настройки в нем Chillispot, на примере роутера D'link DIR-320 показаны в заметке в блоге [5].

3. Скриншот страницы настроек Chillispot на роутере, работающем под управлением DD-WRT:

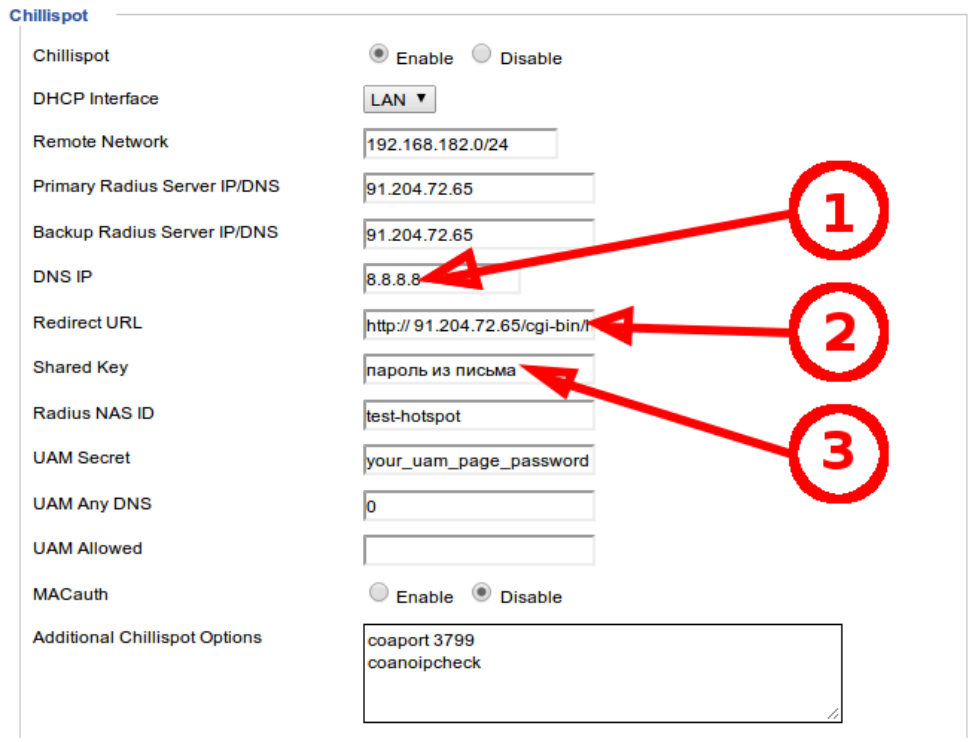

Рис. 1 — Скриншот настроек Chillispot

ПРИМЕЧАНИЯ:

1. Укажите в этом поле либо адрес сервера DNS, Вашего провайдера, либо адрес любого из т. н. «открытых серверов DNS», например, показанный на скриншоте адрес одного из серверов Google.
2. Укажите в этом поле адрес страницы авторизации (в одну строку, без пробелов и т. п., ОБЯЗАТЕЛЬНО ПРОВЕРЬТЕ, чтобы между **cgi** и **bin** СОХРАНИЛСЯ ДЕФИС!!!):
   `http://91.204.72.65/cgi-bin/hotspotlogin.cgi`
3. Укажите в этом поле пароль для связи с сервером RADIUS, который вы получили в письме с ответом на ваш запрос, отправленный на адрес электронной почты **[4]**.
4. После того, как вы вписали значения параметров в необходимые поля, сохраните настройки кнопкой «**Save**», расположенной в самом низу страницы, потом примените настройки кнопкой «**Apply Settings**»,

и напоследок, перезагрузите роутер (просто выключите его блок питания из розетки питающей сети, обождите немного и включите вновь).

5. В последних версиях прошивок DD-WRT параметры «**`coaport 3799`**» и «**`coanoipcheck`**», вписанные в поле «**Additional Chillispot Options**», могут приводить к неработоспособности Chillispot. В таких случаях, удалите указанные параметры, сохраните настройки и перезапустите роутер.
6. Чтобы попасть на страницу с настройками, показанными на рис. 1, вам нужно в меню прошивки роутера Выбрать пункт «**Services**» и затем подпункт «**Hotspot**»:

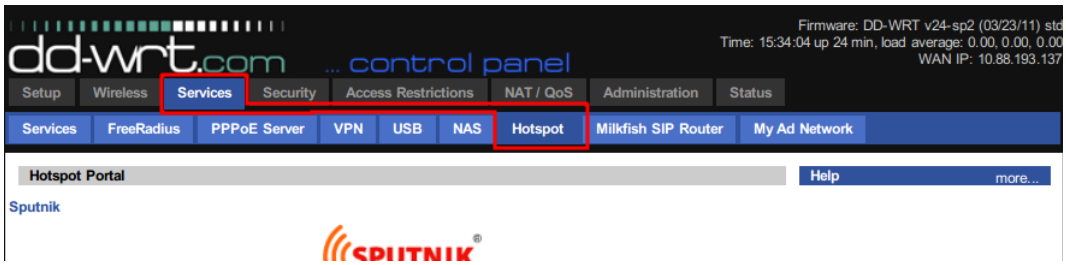

Рис. 2 — Расположение меню настроек Hotspot

4. Диагностика, возможные неполадки

После того, как вы активировали в роутере Chillispot, подключите к нему тестовый компьютер. Учтите, что на тестовом компьютере должен быть включен DHCP-клиент (в свойствах протокола TCP-IP должны быть активированы опции «*Получить адрес автоматически*» и «*Получить адрес сервера DNS автоматически*»)! Когда соединение будет установлено, проверьте — какие именно параметры протокола TCP-IP тестовый компьютер получил от роутера? **ПРАВИЛЬНЫЙ** результат — это когда «*собственный IP-адрес*» компьютеру будет присвоен из диапазона 192.168.182.2 — 192.168.182.254, «*адрес шлюза по умолчанию*» будет равен 192.168.182.1, а «*адрес сервера DNS*» — 8.8.8.8 (такие значения соответствуют тем настройками параметров, которые показаны на рис. 2). За выдаваемые компьютеру «*IP-адрес*» и «*адрес шлюза*» отвечает параметр «**Remote Network**» на рис. 1, а за «*адрес сервера DNS*» — параметр «**DNS IP**» на рис. 1.

Убедившись, что компьютер получил правильный адрес, откройте браузер и попробуйте перейти на какой-нибудь сайт. Вместо запрошенного сайта браузер должен отобразить страницу авторизации хотспота. В программе Easyhotspot на странице «постоянных» клиентов [6] или на странице ваучеров [7] вам нужно либо создать новый аккаунт (ваучер) для теста, либо взять данные уже существующего. Введите логин и пароль выбранного (созданного) аккаунта (ваучера) в соответствующие поля страницы авторизации и нажмите кнопку «**Войти**». Если все ОК, хотспот авторизует вас и вы перейдете на страницу, которую запрашивали изначально. Также, если на тестовом сервере будет активирован и настроен (а то иногда «добрые люди» в админке тарифы удаляют) гостевой режим, то на странице авторизации будет присутствовать кнопка «**Бесплатно**», и вы можете попробовать авторизоваться без пароля с помощью данной кнопки.

ВНИМАНИЕ! Выбирайте уже созданные («кем-то» и «когда-то») аккаунты в биллинге тестового сервера с осторожностью! Может оказаться так, что тот, кто их создал, вводил для проверки какие-то ограничения (например, «привязал» аккаунт к конкретному NASID, и в таком случае либо вы должны своему хотспоту выставить такой-же, или же авторизоваться не выйдет однозначно!!!)… Это же относится и к Тарифам, на основании которых вы будете выписывать тестовые ваучеры — Тарифам тоже можно внести самые разные ограничения, и вы потом будете сидеть и гадать - «А почему же никак не получается авторизоваться?»…

Если хотспот отказывается вас авторизовать, попробуйте повторить попытку. Если все попытки безуспешны, первым делом проверьте лог авторизации клиентов хотспота. Для этого в программе перейдите на страницу «**Клиентов, подключенных к интернету**» [8]. На ней нажмите кнопку «**Просмотреть протокол авторизации клиентов**». Вы должны увидеть список попыток авторизации.

В случае неудачных попыток авторизации (хотспот постоянно отказывает в авторизации) одной из причин может быть неверно указанный пароль сервера RADIUS — параметр «**Shared Key**», показанный на рис. 1.

ПРЯМЫМ СВИДЕТЕЛЬСТВОМ, ЧТО ВЫ ДОПУСТИЛИ ИМЕННО ЭТУ ОШИБКУ, ЯВЛЯЕТСЯ ТОТ ФАКТ, ЧТО В ЛОГЕ АВТОРИЗАЦИИ ВООБЩЕ НЕ БУДЕТ СТРОК О ПОПЫТКАХ ВАШЕЙ АВТОРИЗАЦИИ (сервер RADIUS просто отказывается обслуживать роутеры, обращающиеся к нему с неверным паролем)! Если же в логе видны ваши попытки (пусть даже и неудачные) — это однозначно свидетельствует, что **Shared Key** ВЫ ВВЕЛИ ПРАВИЛЬНО!

Другая возможная причина отказа в авторизации клиентов — неверно указанный вами пароль страницы авторизации (параметр «**UAM Secret**» на рис. 1). В таком случае, в строках протокола авторизации вы увидите, что вместо паролей, которые вы вводили на странице авторизации, показана какая-то «абракадабра» (зачастую еще и с непечатаемыми символами, типа такого `8L;%\256\005!\221\206\233\362H`), как показано на рис. 3 ниже (для наглядности обведено рамками красного цвета):

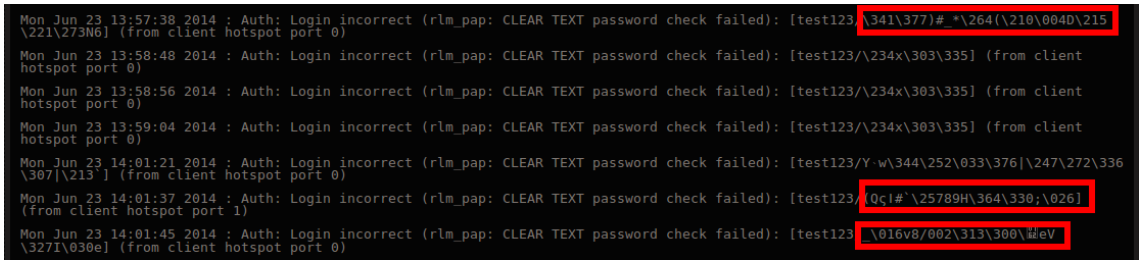

Рис. 3 — Примеры строк, в которых «абракадабра» вместо пароля

Также, причиной отказа могут быть и неверно указанные параметры выбранных (созданных) вами аккаунтов (ваучеров), ограничивающие доступ какими-то критериями (NASID, график обслуживания, дата окончания обслуживания, и т. д. и т.п.). Список возможных сообщений об ошибках приведен в разделе «*Просмотр данных об авторизации Клиентов (Кассир)*» инструкции «**Программа управления Wi-Fi хотспотом - Easyhotspot, Руководство по эксплуатации**», доступной по ссылке [**3**].

Ссылки:

1. Демо сайт программы Easyhotspot (***по этому адресу (в отличие от тестового сервера) размещен только веб-интерфейс программы Easyhotspot — ОН НЕ СМОЖЕТ УПРАВЛЯТЬ роутерами, не путайте его с тестовым сервером!!!***):
   http://wifi-hotspot.zp.ua/hotspot_demo/
2. Страница «Варианты построения сети хотспота»:
   http://dmitrykhn.homedns.org/hotspot-description/1-articles/47-networks
3. Файл «Программа управления Wi-Fi хотспотом - Easyhotspot, Руководство по эксплуатации»:
   http://dmitrykhn.homedns.org/hotspot_info/manual_ci3.pdf
4. Адрес электронной почты, куда нужно отсылать запрос для получения пароля:
   dmitrykhn@aol.com
5. Страница с описанием установки и настройки Chillispot на роутере с прошивкой DD-WRT:
   http://dmitrykhn.homedns.org/wp/2010/06/changing-firmware-for-dlink-dir-320/
6. Страница аккаунтов «постоянных» клиентов, обслуживаемых тестовым сервером:
   http://91.204.72.65/easyhotspot/index.php/postpaid
7. Страница ваучеров, обслуживаемых тестовым сервером:
   http://91.204.72.65/easyhotspot/index.php/voucher
8. Страница онлайн-клиентов (подключенных к интернету), обслуживаемым тестовым сервером:
   http://91.204.72.65/easyhotspot/index.php/onlineuser
9. Инструкция по настройке хотспота в роутерах Mikrotik:
   http://dmitrykhn.homedns.org/hotspot_info/minimal_Mikrotik_and_Easyhotspot.pdf