Защита беспроводных сетей: настройка PEAP на базе Freeradius v.2 и точки доступа DAP-1360

Microsoft Windows, начиная с XP SP1, при работе с беспроводными сетями, позволяет применять аутентификацию пользователей по протоколу EAP (Extensible Authentication Protocol). Это дает возможность проверять валидность пользователя не по единой парольной фразе, как в WPA/WPA2-PSK, а по логину/паролю (PEAP) и/или цифровому сертификату (EAP-TLS). Данный механизм значительно усиливает безопасность беспроводных сетей.

В данной статье рассмотрим детальную настройку PEAP. Для работы будем использовать:

- Беспроводной клиент – USB-адаптер DWA-140
- Точка доступа с поддержкой WPA-EAP – DAP-1360
- Сервер – операционная система CentOS ver. 5.7
- RADIUS-сервер – FreeRADIUS ver. 2.1.7

1. Установка и настройка FreeRADIUS

В операционной системе CentOS 5.7 это делается достаточно просто следующей командой (должны быть права администратора *root* или с помощью программы *sudo*)

 # yum –y install freeradius2

Базу пользователей можно хранить во внешних базах, например LDAP, MySQL, PostgreSQL, но в данном руководстве рассмотрим более простой вариант – хранение логинов/паролей пользователей в конфигурационном файле RADIUS.

Для автоматического запуска freeradius, при перезапуске операционной системы, дадим следующую команду

 # chkconfig radiusd on

Добавим в систему radius клиентов, т.е. точки доступа, которые будут работать по протоколу PEAP. Список клиентов находится в файле */etc/raddb/clients.conf* . Можно добавлять каждую точку в отдельности, со своим паролем или, как в примере, целой сетью

 # vi /etc/raddb/clients.conf

и в конец добавляем следующие строки

```
client 192.168.0.0/24 {
    secret          = testing123
    shortname       = private-network-1
}
```

где,

- *192.168.0.0/24* – сеть, в которой находятся точки доступа
- *secret* – парольная фраза, для авторизации точек на radius
- *shortname* – название сети

Рекомендуется так же сменить *secret* для секции *client localhost*

Настроим следующие конфигурационные файлы

/etc/raddb/modules/mschap

 # vi /etc/raddb/modules/mschap

Добавляем или изменяем на следующее

```
mschap {
        use_mppe = yes
        require_encryption = yes
        with_ntdomain_hack = yes
}
```

/etc/raddb/modules/realm

 # vi /etc/raddb/modules/realm

Добавляем или изменяем на следующее

```
realm ntdomain {
        format = prefix
        delimiter = "\\"
        ignore_default = no
        ignore_null = no
}
```

/etc/raddb/sites-available/default

 # vi /etc/raddb/sites-available/default

Добавляем или изменяем на следующее

```
authorize {
.........
#       suffix
        ntdomain
.........
}
```

/etc/raddb/proxy.conf

 # vi /etc/raddb/proxy.conf

Добавляем или изменяем на следующее

```
realm DEFAULT {
        type            = radius
        authhost        = LOCAL
        accthost        = LOCAL
}
```

/etc/raddb/eap.conf

 # vi /etc/raddb/eap.conf

Добавляем или изменяем на следующее

```
default_eap_type = tls peap
.....
peap {
            default_eap_type = mschapv2
}
```

/etc/raddb/modules/files

 # vi /etc/raddb/modules/files

Добавляем или изменяем на следующее

```
files {
        usersfile = ${confdir}/users
        compat = no
}
```

Логины и пароли пользователей прописываем в конце файла ***/etc/raddb/users***

 # vi /etc/raddb/users

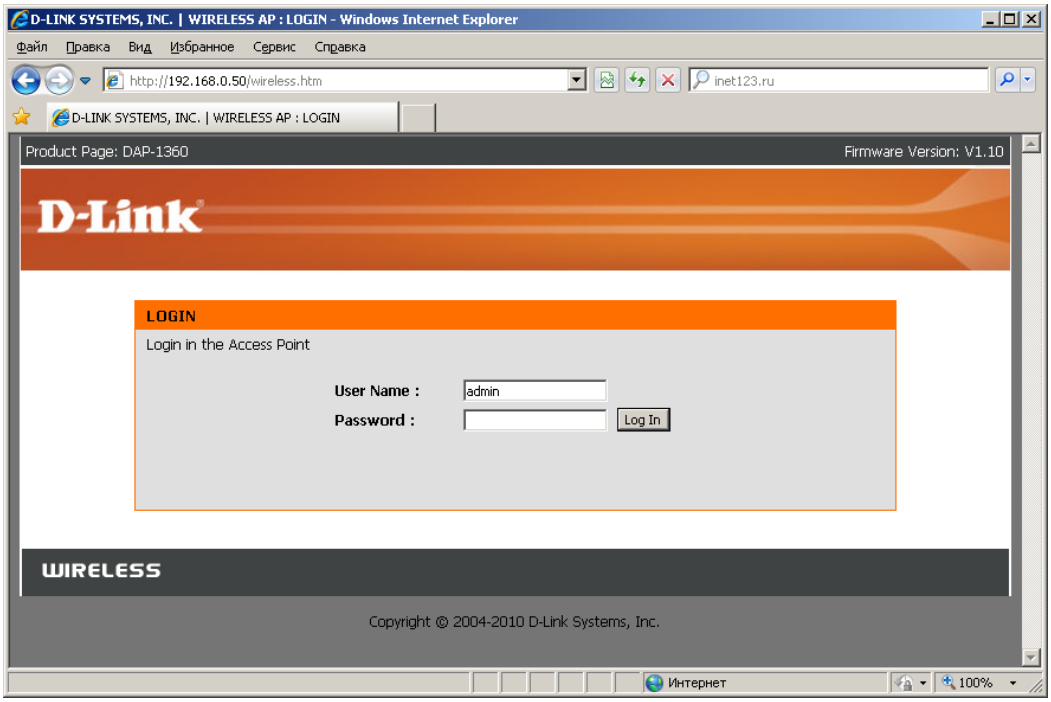
по следующему шаблону

```
username1    Cleartext-Password := "password1"
username2    Cleartext-Password := "password2"
username3    Cleartext-Password := "password3"
.....
```

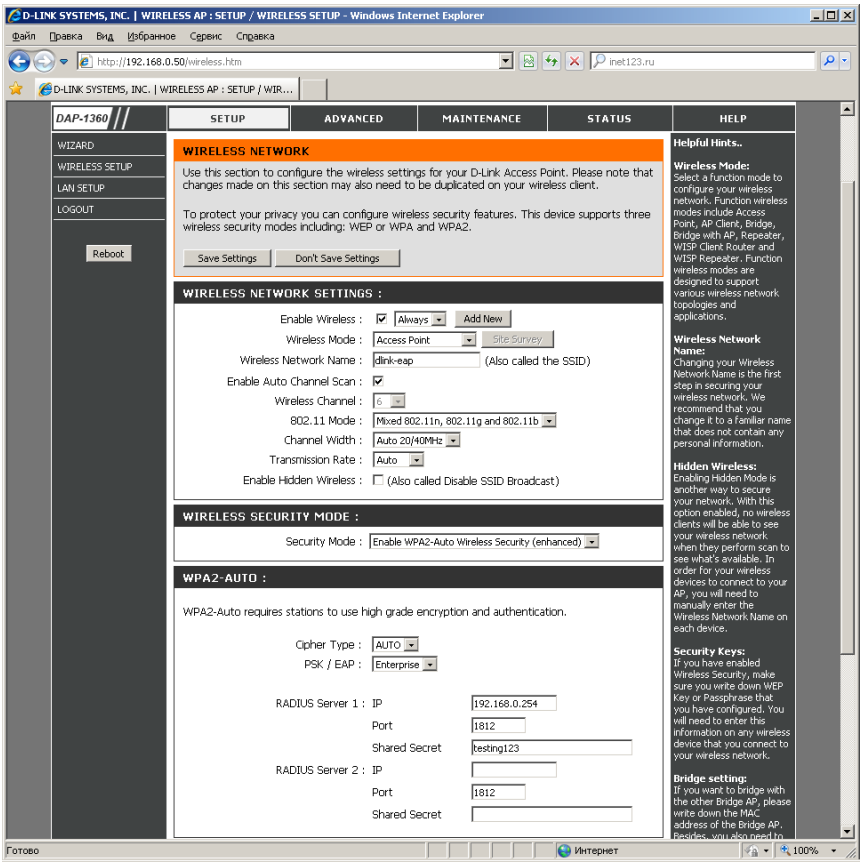
На этом настройка сервера закончена

2. **Настройка точки доступа DAP-1360**

Запускаем броузер, желательно Internet Explorer. В строке «Адрес» вводим ip-адрес точки доступа и нажимаем Enter. Все точки доступа D-Link по-умолчанию имеют ip-адрес 192.168.0.50



В поле User Name вводим «admin», поле Password оставляем пустым. Нажимаем кнопку LogIn.



Для включения PEAP в разделе «Wireless Security Mode» выбираем «Enable WPA2-Auto Wireless Security». В открывшемся ниже разделе «WPA2-Auto» прописываем следующее:

Cipher Type		AUTO
PSK / EAP		Enterprise
RADIUS Server 1 :	**IP**	192.168.0.254 (ip-адрес radius сервера)
	Port	1812 (значение по-умолчанию 1812)
	Shared Secret	testing123 (значение secret из файла /etc/raddb/clients.conf)

Значения для **RADIUS Server 2** оставляем без изменений. Нажимаем кнопку «Save Settings».

3. Запуск freeradius в отладочном режиме

Для проверки работоспособности freeradius можно запустить его в отладочном режиме. Для этого запускаем следующую команду

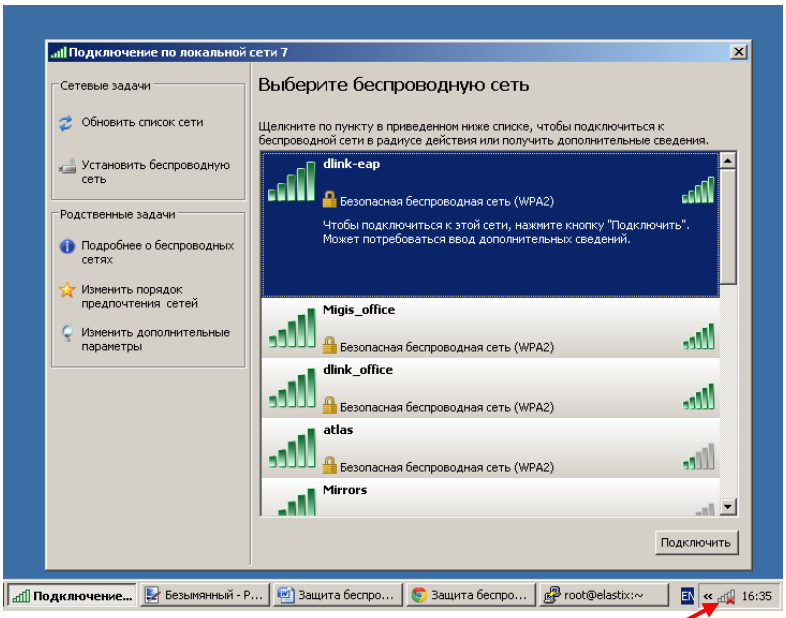
radius –fX

и видим примерно следующее

FreeRADIUS Version 2.1.7, for host i686-redhat-linux-gnu, built on Mar 31 2010 at 00:25:31
Copyright (C) 1999-2009 The FreeRADIUS server project and contributors.
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
You may redistribute copies of FreeRADIUS under the terms of the
GNU General Public License v2.
Starting - reading configuration files ...
including configuration file /etc/raddb/radiusd.conf
including configuration file /etc/raddb/proxy.conf
including configuration file /etc/raddb/clients.conf
including files in directory /etc/raddb/modules/
including configuration file /etc/raddb/modules/mschap
including configuration file /etc/raddb/modules/realm
including configuration file /etc/raddb/modules/smsotp
including configuration file /etc/raddb/modules/wimax
including configuration file /etc/raddb/modules/unix
……..
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on command file /var/run/radiusd/radiusd.sock
Listening on proxy address * port 1814
Ready to process requests.

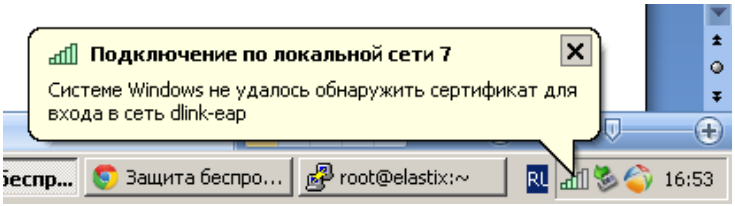
4. Настройка беспроводного клиента на Windows XP SP3

Для подключения к точке доступа с PEAP можно произвести настройку беспроводного адаптера вручную или полуавтоматически. Рассмотрим второй вариант.



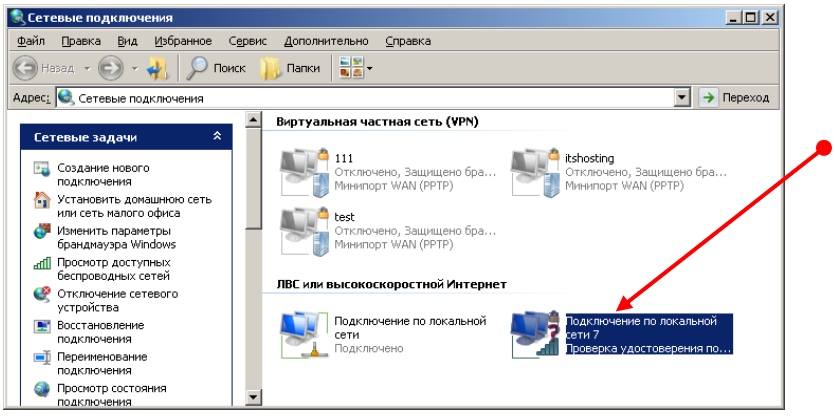
Нажимаем левой кнопкой мышки на «лестничку» в трее (правом нижнем углу). Откроется список беспроводных сетей. Если он будет пуст выберите меню «Обновить список сети». Выберите из списка точку доступа с вашим SSID и нажмите кнопку «Подключить».

Получите сообщение

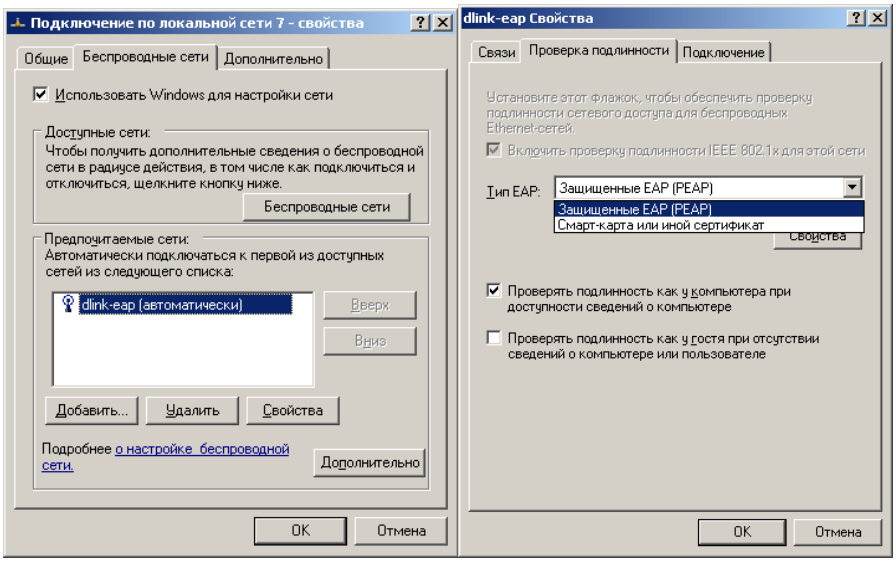


В окне отладки freeradius мы видим сообщение «entering group REJECT {...}», т.е. обращения к радиусу идут, но из-за отсутствия сертификата подключение невозможно.

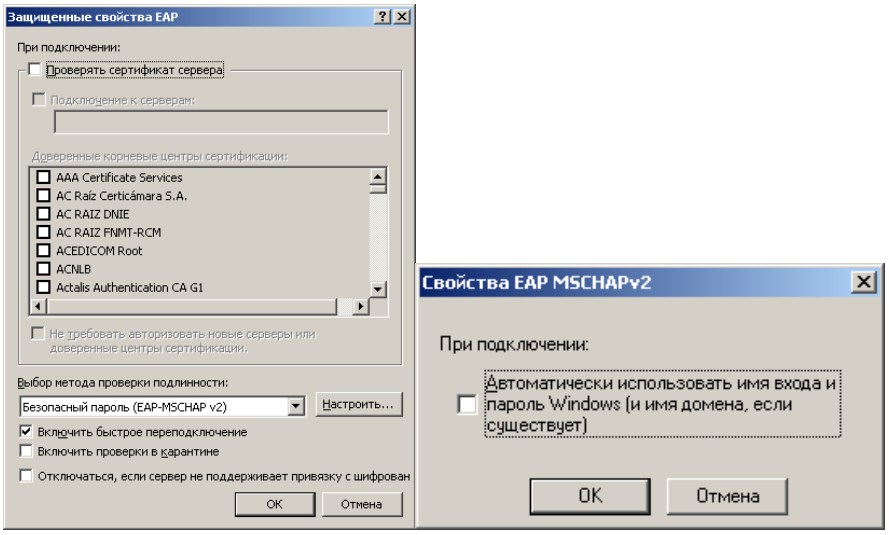
Переходим в настройку беспроводного адаптера. Пуск – Настройка – Панель управления – Сетевые подключения



Нажимаем на иконке беспроводного подключения правой кнопкой мышки и выбираем меню «Свойства – закладка Беспроводные сети»

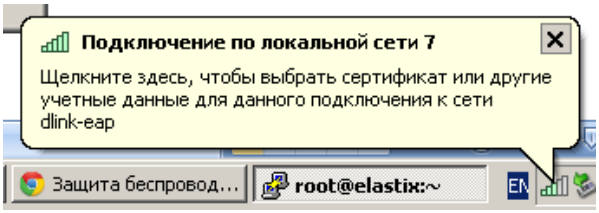


Выбираем в «Предпочитаемых сетях» в нашем случае SSID «dlink-eap» и нажимаем Свойства. Выбираем закладку «Проверка подлинности» и выбираем тип EAP «Защищенные EAP (PEAP)». Нажимаем «Свойства» под ним.



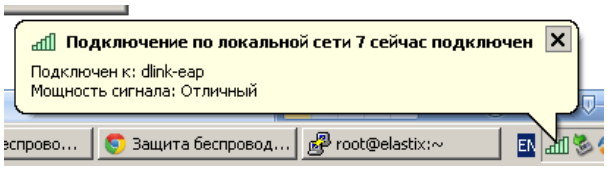
Убираем галочку «Проверять сертификат сервера». Метод проверки подлинности «EAP-MSCHAP v2». Нажимаем кнопку Настроить. Отключаем галочку «Автоматически использовать имя для входа и пароль Windows». Закрываем все 4 окошка нажатием кнопки «OK». На этом все, настройка завершена.

Через несколько секунд после последнего «OK» должно высветиться сообщение



Нажмите на нем левой кнопкой мышки. Откроется окно авторизации, наподобие этого

Введите Имя и Пароль одного из пользователей, прописанных в файле */etc/raddb/users* и нажмите «ОК». После проверки Логина и Пароля вы увидите сообщение



Windows запомнит логин/пароль и в дальнейшем будет подключаться автоматически, пока вы не смените логин/пароль для этого пользователя в */etc/raddb/users*

5. Запуск Freeradius в постоянную работу

Настройка завершена. Теперь можно запустить радиус в постоянную работу. Для этого перейдите в окно с радиусом, запущенным в режиме отладки, и нажмите Ctrl+C для завершения. После этого запустите демон radiusd для работы в штатном режиме

 # /etc/init.d/radiusd start

Starting RADIUS server: [OK]