Шифрования WiFi с помощью hostapd

Существуют два превосходных варианта микропрограммы с открытым кодом, DD-WRT и OpenWRT, которые заменяют микропрограмму пользовательских маршрутизаторов типа Linksys WRT54G (см. Ресурсы) и содержат `hostapd`. Обе они поддерживают обширную базу устройств. Я предпочитаю создавать свои собственные беспроводные точки доступа с помощью усеченных версий Linux на одноплатных компьютерах Soekris, PC Engines или MicroTik (см. Ресурсы). Эти компактные платы весьма надежны и обеспечивают полный контроль и гибкость.

Если вы хотите создать собственную беспроводную точку доступа, то наиболее важным компонентом является плата беспроводного интерфейса с встроенной поддержкой ядра Linux, а также поддержкой очень важного режима AP. Этот режим называется также режимом точки доступа, режимом ведущего устройства или инфраструктурным режимом. Он необходим для создания беспроводной точки доступа. Многие беспроводные сетевые интерфейсы не поддерживают режим AP и могут выступать только в роли клиентских устройств с минимальной функциональностью. Я предпочитаю использовать беспроводные интерфейсы Atheros, поскольку они обладают полным набором функций и хорошо поддерживаются как своими старыми драйверами Madwifi, так и более новыми драйверами mac80211.

Старайтесь не использовать в своей точке доступа ndiswrapper. Конечно, это отличный способ заставить беспроводной интерфейс работать, когда не остается ничего другого, но это всего лишь заплатка, скрывающая множество проблем. Старайтесь использовать хорошие беспроводные интерфейсы со встроенной поддержкой ядра.

В базе данных устройств Linux на Wireless.org можно найти поддерживаемые интерфейсы, а также массу информации о беспроводных драйверах и командах пространства пользователя (см. Ресурсы). The Linux Wireless project has done a great job ofВ рамках проекта Linux Wireless была проделана огромная работа по очистке и оптимизации беспроводного стека Linux.

На клиентской стороне все обстоит проще, так как почти любая совместимая с WiFi плата беспроводного интерфейса со встроенной поддержкой ядра может подключаться к точке доступа с криптостойким шифрованием WPA2. Клиенты Mac и Windows® тоже могут использовать вашу замечательную точку доступа на основе Linux.

Опробование плат беспроводного интерфейса

Как узнать, какие функции поддерживает ваша плата беспроводного интерфейса? Об этом расскажет команда `iw`. Найдите секцию "Supported interface modes" (поддерживаемые режимы интерфейса) и посмотрите, поддерживает ли ваша карта режим AP. Пример такой команды показан в листинге 1.

Листинг 1. Вывод команды iw

```
$ iw list

[...]

Supported interface modes:
*IBSS
*managed
*monitor
*AP
*AP/VLAN
```

В этом примере показана плата беспроводного интерфейса, поддерживающая режим AP и беспроводные виртуальные сети (VLAN). IBSS — это режим ad hoc. Режим monitor предназначен для анализа трафика в беспроводных сетях. Все платы беспроводного интерфейса поддерживают режим managed, в котором они играют роль клиента точки доступа.

Попробуйте выполнить команду `wlanconfig` для интерфейсов Atheros, использующих драйверы Madwifi. См. листинг 2.

Листинг 2. Пример команды wlanconfig

```
# wlanconfig ath0 list caps
ath0=7782e40f<WEP,TKIP,AES,AES_CCM,HOSTAP,TXPMGT,SHSLOT,SHPREAMBLE,TKIPMIC,WPA1,
WPA2,BURST
     ,WME>
```

Эта команда показывает наличие поддержки режима AP, а также шифрования WPA2 и криптостойкого шифра AES-CCMP.

Другим хорошим способом проверки беспроводного оборудования является чрезвычайно полезная команда `hwinfo`. Она имеет специальную опцию для беспроводных интерфейсов и дает много полезной информации, как показывает фрагмент вывода в листинге 3:

Листинг 3. Пример информации hwinfo для карты WIC

```
$ hwinfo --wlan
27: PCI 500.0: 0282 WLAN controller
Model: "Intel WLAN controller"
Driver: "iwlagn"
Driver Modules: "iwlagn"
WLAN encryption modes: WEP40
WEP104 TKIP CCMP
WLAN authentication modes: open sharedkey wpa-psk wpa-eap
Status: iwlagn is active
Driver Activation Cmd: "modprobe iwlagn"
```

Команда `hwinfo` называет драйвер, показывает, какое шифрование он поддерживает, сообщает имя устройства и многое другое. Кроме того, можно попробовать команду `lspci` для сетевых плат с интерфейсом PCI и команду `lsusb`— для интерфейсов USB. Эта плата сетевого интерфейса не может работать в качестве точки доступа, поскольку драйвер iwlagn не поддерживается в `hostapd`, и в любом случае она не поддерживает режим AP. (Этот интерфейс является частью малобюджетного чипа Centrino.)

Настройка hostapd

Установка зависит от используемого дистрибутива Linux, поэтому я предлагаю оставить ее в качестве домашнего задания. Сначала нужно настроить `hostapd` на точке доступа, а затем использовать wpa_supplicant на клиентском ПК для проверки обмена ключами.

Если в вашей точке доступа нет файла /etc/hostapd.conf, создайте его. Если ваша система уже создала этот файл, сделайте на всякий случай его резервную копию и создайте новый чистый файл. Пример в листинге 4 содержит все, что нам нужно для настройки WPA2-Personal:

Листинг 4. Пример файла /etc/hostapd.conf

```
interface=ath0
bridge=br0
driver=nl80211
ssid=alracnet
auth_algs=1
wpa=1
wpa_psk_file=/etc/hostapd-psk
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP TKIP
rsn_pairwise=CCMP
```

Возможно, вам придется заменить некоторые из этих параметров, такие как интерфейс, драйвер и ssid, своими собственными значениями. При перечислении нескольких опций разделяйте их пробелами, как показано в строке wpa_pairwise. Ниже приведены примечания к этому примеру.

- Интерфейсы Atheros всегда называются athx, а все другие интерфейсы — wlanx.
- Исключите строку bridge, если ваша точка доступа не содержит моста Ethernet.
- Если вы используете `hostapd` версии 0.6.8 или выше и сетевой интерфейс с поддержкой mac80211, то используется драйвер nl80211. Из старых драйверов поддерживаются только HostAP, madwifi и prism54. Версии `hostapd` ниже 0.6.8 поддерживают драйверы hostap, wired, madwifi, test, nl80211 и bsd.
- В качестве ssid можно использовать любое удобное вам значение или, например, имя точки доступа.
- auth_algs=1 позволяет использовать только алгоритмы аутентификации WPA2. Значение 2 означает WEP. Никогда не используйте шифрование WEP (Wired Equivalent Privacy), поскольку оно давно взломано. Значение 3 позволяет использовать оба алгоритма.
- wpa=2 позволяет использовать только WPA2. Значение 1 означает WPA1, а 3 позволяет и то, и другое.

- wpa_psk_file указывает на файл с общими ключами.
- wpa_key_mgmt указывает алгоритмы ключей шифрования, которые вы хотите разрешить. Вы можете выбрать WPA-PSK, WPA-EAP или оба варианта. PSK означает Pre-Shared Key (предварительно распространенные ключи). EAP означает Extensible Authentication Protocol — расширяемый протокол аутентификации, представляющий собой систему, поддерживающую множество разных методов аутентификации. Для вашей компактной конфигурации с предварительно распространенными ключами он не понадобится.
- wpa_pairwise и rsn_pairwise показывают, какие шифры можно использовать для шифрования данных; можно использовать CCMP, TKIP или оба. CCMP значительно устойчивей, чем TKIP, поэтому можно попробовать разрешить только CCMP. Клиенты Windows печально известны капризностью и проблемами при использовании стойких шифров, поэтому для них лучше разрешить TKIP.

Рекомендуется использовать только WPA2; шифрование WEP (Wired Equivalent Privacy) настолько слабо, что практически бесполезно, а WPA почти так же слабо, как и WEP. С 2006 г. поддержка WPA2 является обязательной в сертифицированных устройствах WiFi и присутствует во всех современных операционных системах, включая Windows XP SP3. Если даже вам придется заменить некоторые беспроводные интерфейсы, это все равно обойдется дешевле, чем восстановление системы после вторжения.

Затем создайте файл /etc/hostapd-psk, содержащий шаблон MAC-адреса и простой текстовый пароль длиной до 63 символов:

```
00:00:00:00:00:00 testpassword
```

Теперь перейдите на ПК с клиентом Linux и создайте простой конфигурационный файл wpa_supplicant.conf для wpa_supplicant примерно так, как показано в листинге 5.

Листинг 5. Пример файла wpa_supplicant.conf

```
ctrl_interface=/var/run/supplicant
network={
  ssid="alracnet"
  psk="testpassword"
  priority=5
}
```

Параметр ctrl_interface разрешает взаимодействовать в командной строке с wpa_supplicant. Укажите собственные ssid и текстовый пароль, заключив их в двойные кавычки. Чем выше приоритет (priority), тем быстрее выполняется соединение с точкой доступа. Теперь вернитесь к точке доступа и запустите `hostapd` в режиме отладки:

```
# hostapd -d /etc/hostapd.conf
```

При наличии ошибок конфигурации эта команда сообщит о них и прекратит работу. В противном случае она выведет на экран много строк текста. Нажмите CTRL+C, чтобы прервать вывод. После устранения ошибок вы можете настроить автоматический запуск этой команды, что мы потом и сделаем.

Затем остановите беспроводное соединение в клиенте, если оно работает, и запустите wpa_supplicant от имени root:

```
# wpa_supplicant -i wlan0 -D wext -c wpa_supplicant.conf -d
```

Параметр -i указывает на беспроводной интерфейс, -D wext означает стандартный драйвер wpa_supplicant, -c указывает на конфигурационный файл, а -d означает режим отладки. Вы увидите множество выведенных строк – как в точке доступа, так и в клиенте. Если обмен ключами пройдет успешно, он завершится быстро, и в клиенте вы увидите сообщения, подобные тем, что показаны в листинге 6.

Листинг 6. Пример сообщений от wpa_supplicant

```
EAPOL: SUPP_BE entering state IDLE
EAPOL authentication completed successfully
RTM_NEWLINK: operstate=1 ifi_flags=0x11043 ([UP][RUNNING][LOWER_UP])
RTM_NEWLINK, IFLA_IFNAME: Interface 'wlan0' added
```

Ура, заработало! Нажмите CTRL+C, чтобы прервать сеанс wpa_supplicant. Последним шагом будет создание индивидуальных ключей для пользователей. Сначала создайте их в точке доступа и затем скопируйте их в клиенты с помощью вашей любимой утилиты для настройки сети. Все графические конфигураторы действуют по сути одинаково: введите SSID, выберите аутентификацию WPA2-Personal и скопируйте ключ.

Добавление пользователей, более стойкие ключи

Осталось добавить последние штрихи. Простые текстовые пароли расточительно используют вычислительные ресурсы, поскольку их необходимо шифровать, поэтому в wpa_supplicant есть замечательная команда wpa_passphrase для генерации 256-битных ключей шифрования из простых текстовых паролей. Используйте ее, как показано в листинге 7, вместе с SSID:

Листинг 7. Создание пользователей с помощью wpa_passphrase

```
$ wpa_passphrase "alracnet" "greatbiglongpasswordbecauselongerisbetter"
network={
 ssid="alracnet"
 #psk="greatbiglongpasswordbecauselongerisbetter"
 psk=a8ed05e96eed9df63bdc4edc77b965770d802e5b4389641cda22d0ecbbdcc71c
}
```

Вернувшись в /etc/hostapd-psk, вы можете начать добавлять пользователей. Каждый зашифрованный предварительно распространенный ключ должен быть сопоставлен с MAC-адресом пользователя. Пример этого показан в листинге 8.

Листинг 8. Пример файла /etc/hostapd-psk

```
11:22:33:44:55:66
a8ed05e96eed9df63bdc4edc77b965770d802e5b4389641cda22d0ecbbdcc71c
22:33:44:55:66:77
eac8f79f06e167352c18c266ef56cc26982513dbb25ffa485923b07bed95757a
33:44:55:66:77:aa
550a613348ffe64698438a7e7bc319fc3f1f55f6f3facf43c15e11aaa954caf6
44:55:66:77:aa:bb
ad328e5f2b16bdd9b44987793ed7e09e6d7cca3131bc2417d99e48720b4de58c
```

Когда вы убедитесь, что все работает, вы, вероятно, захотите, чтобы `hostapd` запускался автоматически. Это можно сделать несколькими способами: создать сценарий автозапуска, чтобы он запускался во время начальной загрузки, или запускать демон при активизации интерфейса беспроводной сети. Существует так много способов реализации автозапуска в разных дистрибутивах Linux, что я тоже пропущу эту операцию и оставлю ее вам в качестве домашнего задания. Возможно, вы захотите использовать опцию -B, которая запускает эту команду в фоновом режиме, вместо опции –d, означающей отладку.

На этом мы закончим знакомство с прекрасным демоном `hostapd`. Более подробную информацию можно найти в Ресурсах.