

Wi-Fi роуминг в OpenBSD

Омелечко Дмитрий

2 августа 2008 г.

Содержание

1	Ведение	1
2	Схема на основе мостов	2
2.1	Недостатки схемы на основе мостов	2
2.1.1	Широковещательный шторм	2
2.1.2	Предел оборудования	3
3	Применение hostapd	3
3.1	Принцип работы	3
3.2	Конфигурация	4
3.2.1	hostapd.conf	4
3.2.2	ospfd.conf	4
3.2.3	hostname.wifi0	5
3.2.4	hostname.eth0	5
3.3	Запуск/Останов hostapd	5
3.4	Недостатки схемы с использованием hostapd	6
3.4.1	Децентрализованное хранилище данных абонентов	6
3.4.2	Отсутствие DHCP	6

1 Ведение

Сети Wi-Fi все чаще начинают напоминать обычные проводные сети. Тенденции, прослеживаемые на протяжении последних лет говорят о том, что в ближайшем будущем грани между ними практически не будет. Скоростные показатели беспроводных сетей уже приближаются к отметке 100Мбит/с и это далеко не предел. В связи с этим, в больших Wi-Fi сетях, возникают те же проблемы, с которыми сталкиваются администраторы в привычных сетях:

1. Контроль доступа клиентов. В беспроводных сетях добавляется проблема контроля перемещения клиентов между точками доступа, когда администратору необходимо обеспечить беспрепятственное перемещение клиента между точками.
2. Выделение приоритета определенным видам трафика. Например, VoIP.

3. Защита точек доступа от атак извне. Ненужно забывать о том, что это радиоканал и фактически, попытаться подключиться к ним может любой, в зоне покрытия.

Все удобства использования радиоканала, а главное из них отсутствие проводов и свобода перемещения в зоне покрытия, сводится на нет, в больших радиосетях без обеспечения роуминга. OpenBSD зарекомендовала себя как надежная и безопасная ОС. Особенно, ее любят применять на маршрутизаторах и фаерволах. То, что нужно, для защищенной точки доступа. Но что OpenBSD может предоставить для обеспечения роуминга в больших беспроводных сетях? Я надеюсь, что ответ на этот вопрос вы получите после этого доклада.

2 Схема на основе мостов

Наиболее распространенная схема в сетях Wi-Fi. Отличается простотой построения и неприхотливостью к оборудованию. Для того что бы построить беспроводную сеть на базе мостов понадобится:

1. DHCP сервер;
2. Несколько точек доступа настроенных в режиме моста.

Для того что бы настроить мост в OpenBSD достаточно ввести:

```
ifconfig bridge0 create
brconfig bridge0 add eth0 add wifi0
brconfig bridge0 up
```

Однако нет необходимости применять именно OpenBSD точки доступа для организации такой схемы, более того, как мы увидим дальше, этого делать в принципе не следует. Для конечной точки доступа, для этой схемы, может подойти любое оборудование, даже самое дешевое и различных вендоров, но не стоит обольщаться по этому поводу.

2.1 Недостатки схемы на основе мостов

2.1.1 Широковещательный шторм

В broadcast сетях, очень высока вероятность широковещательного шторма., после которого большинство точек доступа просто зависают. Многим администраторам ситуация до боли знакома. И всяческие ухищрения в виде ребуторов., установки сетевых фильтров (Wi-Fi оборудование очень чувствительно к качеству питания), урезание полосы пропускания на свитчах - являются лишь временными мерами, при этом, не решая задачи.

2.1.2 Предел оборудования

Если применять точки доступа на базе OpenBSD, или любого другого дистрибутива, в поставке которого есть фильтр пакетов, то есть возможность организовать защиту от широковещательного шторма в сети. При большой



Рис. 1: Схема на основе моста

концентрации подключенных абонентов, приходящихся на одну точку доступа, может возникнуть ситуация, когда один абонент может захватить всю полосу пропускания. Т.е. возникает необходимость в балансировке нагрузки и выделения трафика в очереди. Не стоит забывать о том, что режим моста очень прожорлив к ресурсам, особенно это касается прерываний (Interrupts). Даже один абонент может довести загрузку точки на 100% ее возможностей. А если мост построен на базе PC i386, то ограничение в 10000 . 11000 прерываний, сводит на нет вероятность их применения в подобных схемах.

3 Применение hostapd

Начиная с версии 3.8 OpenBSD имеет решение “из коробки” для построения больших беспроводных сетей - демон hostapd. hostapd предназначен для:

1. Защиты от Denial-of-Service И Man-in-the-Middle атак в Wi-Fi сетях.
2. Мониторинга беспроводной сети.
3. Работы с Inter Access Point Protocol (IAPP) ¹.

¹ IEEE 802.11f или IAPP был принят в 2003 году как рекомендация к расширению

3.1 Принцип работы

Опишем общие принципы работы демона.

1. Каждая точка доступа, это классический маршрутизатор.
2. На каждой точке доступа запущен `hostapd`.
3. Multicast с повышенным TTL используется для сообщения между всеми остальными точками.
4. `hostapd.conf`, конфигурационный файл `hostapd`. В нем же и хранятся списки клиентов (см. ниже).
5. Сообщения IAPP . ADD.notify используются для оповещения других точек доступа о том, добавлять или удалять записи клиентов.
6. Демон динамической маршрутизации (`ospfd`, `bgpd`) запущен на каждой точке доступа.
7. IP роутинг требует статической IP маршрутизации. Поэтому на точках доступа не должно быть запущенно серверов DHCP.

Для работы `hostapd` использует 2 интерфейса:

Wi-Fi интерфейс находится в режиме AP. На интерфейсе может не быть IP адресов. Необходимые адреса прописывает `hostapd`.

Второй интерфейс соединен с остальными участниками сети в одном broadcast домене или группе multicast. Обычно это проводной интерфейс.

Схематично, схема с использованием `hostapd` показана на Рис. 2

3.2 Конфигурация

3.2.1 `hostapd.conf`

Файл `hostapd.conf` поддерживает `includes`. Это может быть полезным при больших списках абонентов, когда необходимо четко отделить настройки.

```
#описание интерфейсов
```

```
wlan="wifi0"  
wired="eth0"
```

```
# таблица клиентов. mac клиента -> IP default route клиента!!!!  
# именно этот адрес будет прописывать hostapd на Wi-Fi интерфейсе точки доступа
```

```
table <clients> {  
00:13:ce:9a:98:7e -> 192.168.10.2/30,  
00:0c:f1:07:85:32 -> 192.168.10.6/30,
```

стандарта 802.11, которая описывает взаимодействие между беспроводными точками в режиме AP. В 2006 был заменен стандартом 802.11g.

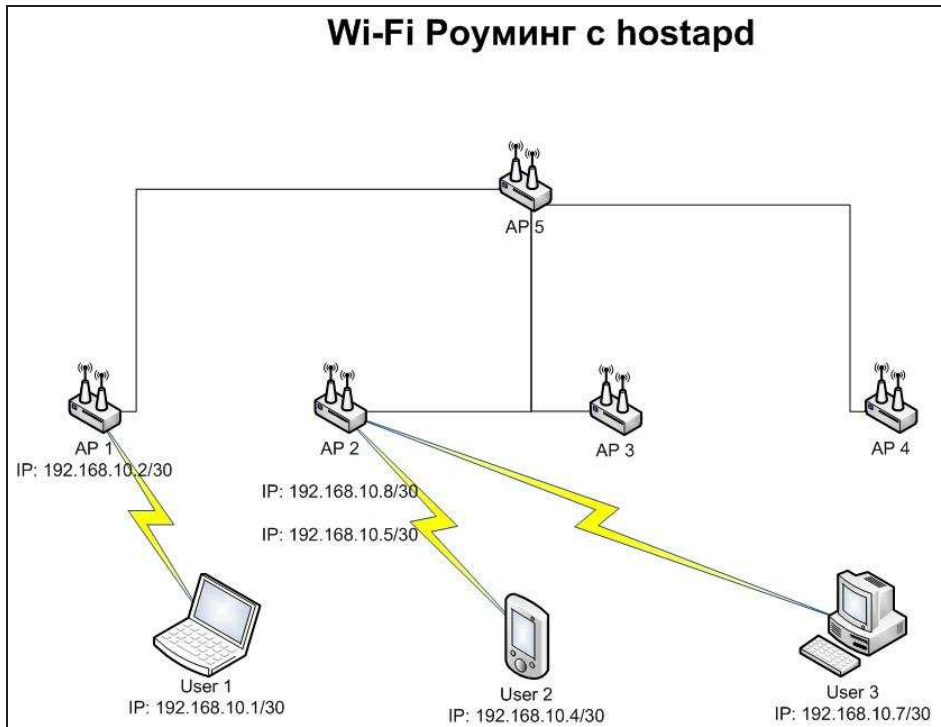


Рис. 2: Схема роуминга с hostapd

```
00:0c:f3:a7:85:32 -> 192.168.10.10/30
}
```

```
# global options
```

```
set hostap interface $wlan
set hostap mode radiotap
set iapp interface $wired
set iapp address roaming table <clients>
set iapp handle subtype address roaming
set iapp mode multicast ttl 2
```

3.2.2 ospfd.conf

```
password="bbos_secure"
auth-key $password
auth-type simple
```

```
fib-update yes
```

```
# должен быть уникальный для каждого маршрутизатора в сети
router-id 192.168.11.254
```

```
spf-delay 1
spf-holdtime 1
hello-interval 1
metric 1
router-dead-time 60

redistribute static
redistribute connected
redistribute default

area 0.0.0.0 {
    interface eth0
}
```

3.2.3 hostname.wifi0

Конфигурация Wi-Fi интерфейса

up

3.2.4 hostname.eth0

Конфигурация hostapd интерфейса. Он же используется и ospfd.

```
inet 192.168.11.254 255.255.255.0 NONE
```

3.3 Запуск/Останов hostapd

После настройки файлов конфигурации можно запускать демоны.

Для пробного запуска демона и отладки файлов конфигурации:

```
# /usr/sbin/ospfd -n -v -f /etc/ospfd.conf
# /usr/sbin/hostapd -d -v -f /etc/hostapd.conf
```

Если все хорошо, тогда прописываем в /etc/rc.conf.local

```
hostapd_flags=YES
ospfd_flags=YES
```

3.4 Недостатки схемы с использованием hostapd

Недостатки построения схем роуминга с использованием hostapd очевидны.

3.4.1 Децентрализованное хранилище данных абонентов

База данных пользователей, а именно соответствие пар .mac address . ip address, должна быть актуальная для каждой точки доступа. В hostapd не предусмотрено механизма централизованной синхронизации этих данных, и, следовательно, при появлении/удалении новой записи в базе данных, ее нужно вручную перенести на каждую точку. Это неудобно в больших сетях. Проблему можно решить написав скрипт синхронизации самостоятельно, но это уже не получается решением “из коробки”.

3.4.2 Отсутствие DHCP

Конечно же, этот досадный факт расстроит многих. Действительно, использование hostapd фактически запрещает использование DHCP. Я бы назвал это основной проблемой, даже не для администраторов, а, прежде всего, для пользователей сети. Ручная настройка соединения может отбить охоту использовать такую схему и сеть у конечного пользователя.

Список иллюстраций

1	Схема на основе моста	2
2	Схема роуминга с hostapd	4