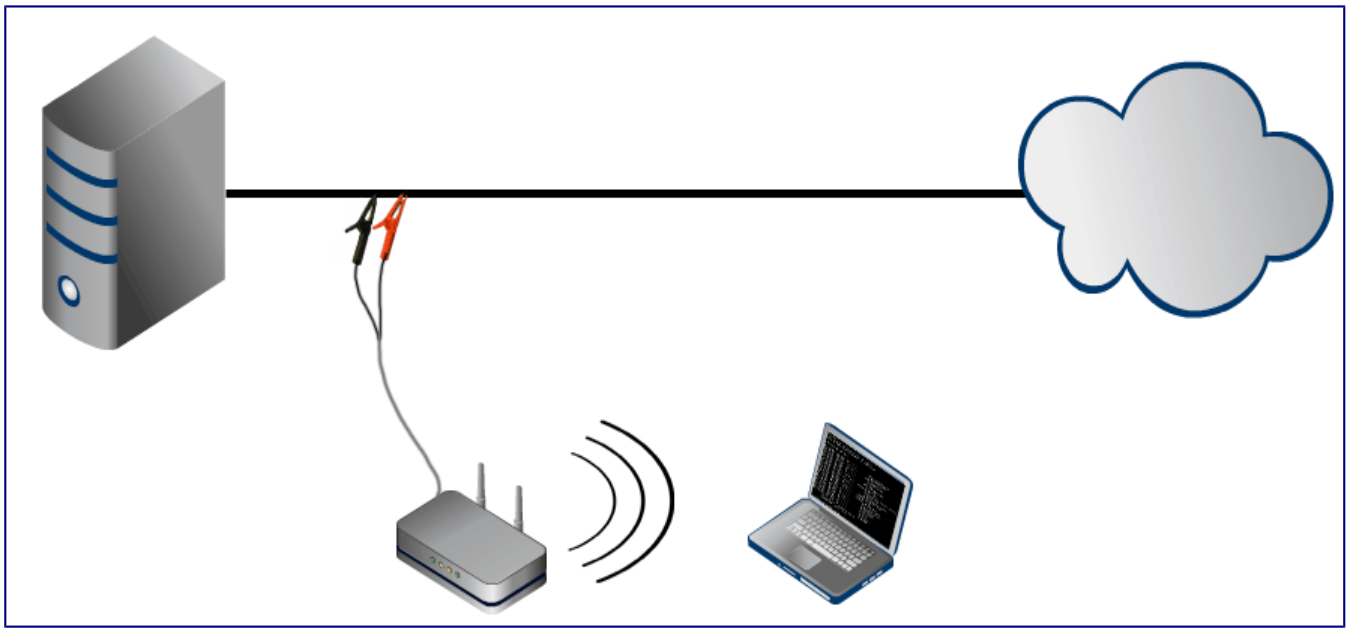
Мониторинг трафика автономный сниффер управляемый по Wi-Fi

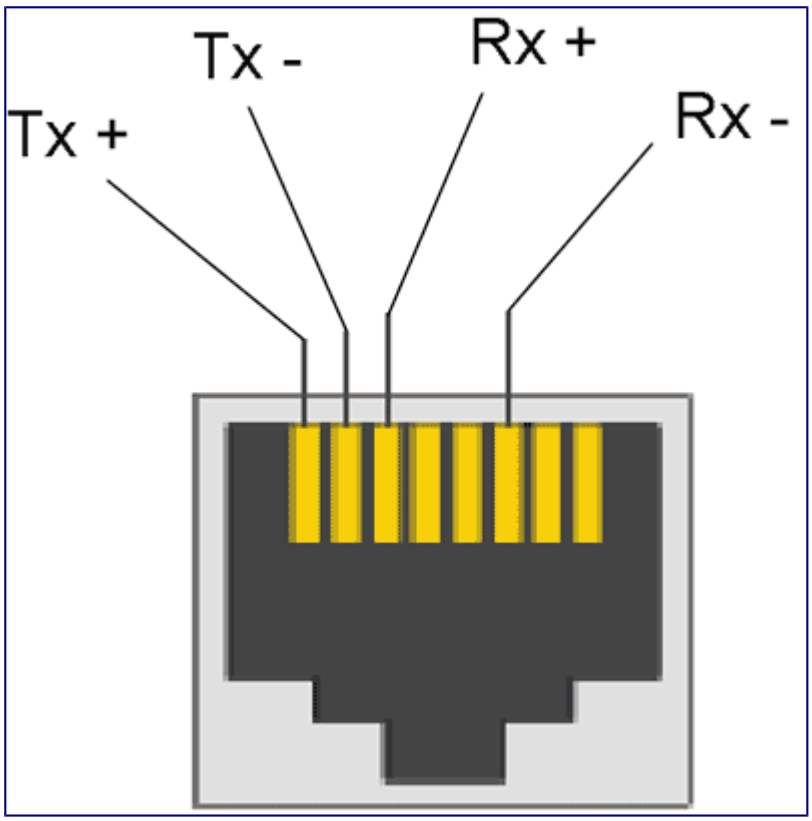
Трафик, проходящий по витой паре, может быть прослушан абсолютно незаметно для участников соединения. В этой истории будет рассказано как изготовить автономный сниффер управляемый по Wi-Fi с возможностью сохранения дампа на диск.



Теория

В сетях стандарта 10/100Base-T передача сигнала происходит по двум парам жил.
Tx — отправка
Rx — прием

Задача состоит в том, чтобы подключить прослушиваемую пару к принимающей паре сниффера.



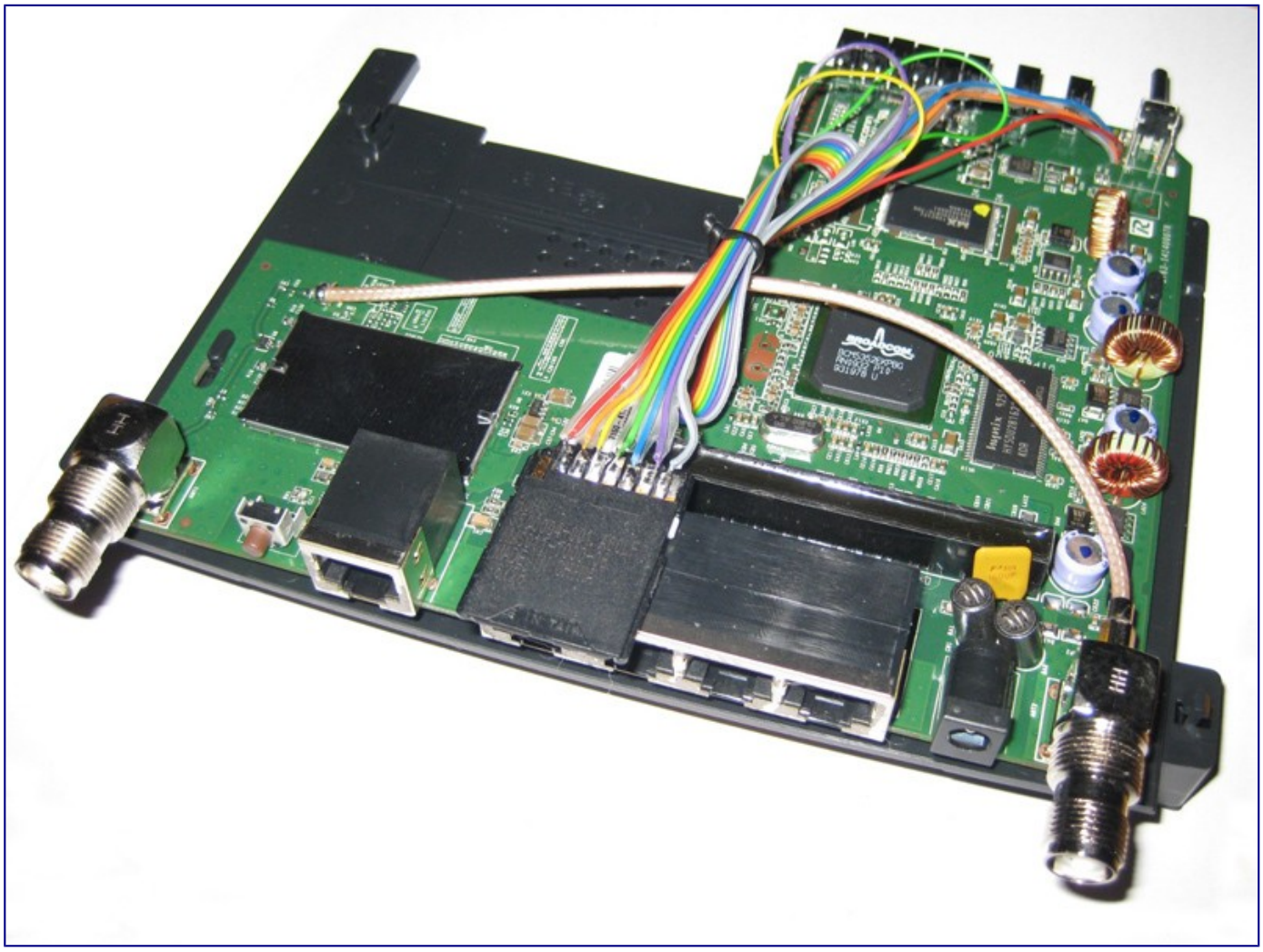
Практика

Подойдет любой роутер, на который можно установить прошивку DD-WRT (или OpenWRT) с возможностью подключения накопителя.

Список поддерживаемых моделей

Например, старый Linksys WRT-54GL.

В нем штатно нет возможности подключения флешек, но довольно просто можно впаять SD или MMC карту. Замечу только, что карту перед пайкой лучше отформатировать на компьютере в файловой системе *ext2*, а GPIO выставлять вручную как в этой инструкции. Я припаял контакты напрямую к карточке, но для сохранения возможности извлекать карту можно использовать гнездо от картридера или переходник microSD→SD.



Прошивка DD-WRT — это миниатюрный Linux. Который при наличии свободно места на диске легко превращается в полнофункциональную систему с менеджером пакетов.

На роутерах с объемом памяти мене 32 Мб (в моем случае 16 Мб), ядро урезано и процесс установки менеджера пакетов несколько отличается от такового в полных версиях прошивки с поддержкой jffs.

Далее подрозумевается, что роутер уже прошит (без поддержки jffs), карта памяти или USB-флешка уже установлена и смонитрованна в `/mmc`. Подключаемся с помощью `telnet`, логин `root`, пароль установленный на веб-морду.

Создаем папку:

```
mkdir /mmc/opt
```

Монтируем ее на карту(эту команду необходимо добавить в стартовый скрипт через веб-интерфейс):

```
mount -o bind /mmc/opt /opt
```

Запускаем установщик *ipkg-opt* (нужен интернет):

```
cd /mmc wget http://www.3iii.dk/linux/optware/optware-install-ddwrt.sh sh ./optware-install-ddwrt.sh
```

Установка займет несколько минут. Далее:

```
ipkg-opt install libuclibc++
```

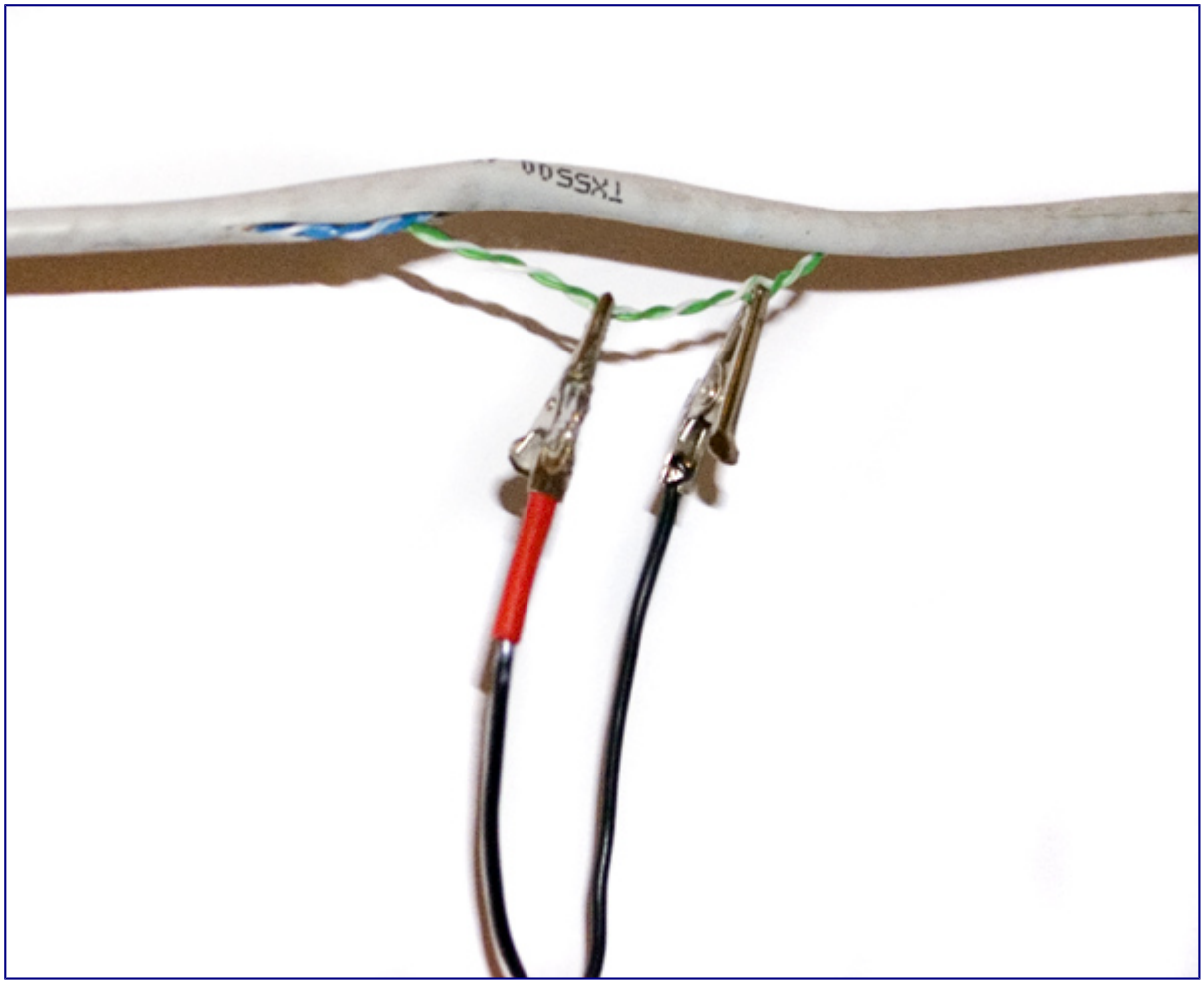
Теперь менджер пакетов готов к работе. Обновить список пакетов: `ipkg-opt update`. Вывести список доступных пакетов: `ipkg-opt list`. Для сбора трафика необходим tcpdump:

```
ipkg-opt install tcpdump
```

Слушающим портом будет WAN, в системе он *eth0*. Подсоединяем крокодильчики к интересующей паре (обычно **Tx** интересней) и запускаем дамп:

```
tcpdump -i eth0
```

В зависимости от схемы обжима, цвета пар могут быть разными. Определить нужную можно только экспериментально, по значению *destination* и *source*. Крокодильчики лучше припаять к многожильному гибкому кабелю, иначе хрупкие жилы будут отламываться.



Запуск *tcpdump* можно так же добавить в стартовый скрипт системы для автоматического запуска после перезагрузок. К роутеру можно подключаться по Wi-Fi и скачивать файлы например по sftp (нужно включить SSH в веб-интерфейсе).