Лабораторная работа Wireshark: 802.11

«Скажи мне, и я забуду. Покажи мне, и я запомню. Дай попробовать самому, и я пойму».
Китайская пословица

В данной лабораторной работе мы исследуем протокол беспроводных сетей 802.11. Перед началом этой лабораторной, вам, возможно, потребуется повторно прочесть раздел 6.3 книги. Кроме того, так как мы ознакомимся с технологией 802.11 чуть глубже, чем описано в книге, вы также можете обратиться к работе Пабло Бреннера (Pablo Brenner) (Breezecom Communications) A Technical Tutorial on the 802.11 Protocol, **sss-mag.com/pdf/802_11tut.pdf,** а также Understanding 802.11 Frame Types Джима Гейера (Jim Geier), **wi-fiplanet.com/tutorials/article.php/1447501**. И, конечно же, к «библии» технологии 802.11: к самому стандарту: ANSI/IEEE Std 802.11, 1999 Edition (R2003), **gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf**. В частности, возможно, при просмотре трассировочной таблицы беспроводного канала связи вы найдете полезной табл. 1 на стр. 36 стандарта.
До настоящего момента во всех лабораторных работах Wireshark мы захватывали только кадры, передаваемые по проводному Ethernet-подключению. В этой же работе, так как 802.11 — это протокол уровня беспроводного канала связи, мы будем захватывать кадры «из воздуха». К сожалению, драйверы многих устройств 802.11 NIC не имеют инструментов для захвата/копирования полученных кадров 802.11 для дальнейшего использования с программным обеспечением Wireshark (см. рис. 1 Лабораторной работы 1, на котором изображен механизм захвата кадра). Поэтому в данной работе мы предоставим вам для анализа трассировочную таблицу заранее захваченного кадра и предположим, что при ответе на вопросы к данной работе, вы будете пользоваться именно этой таблицей. Если вы можете захватывать кадры 802.11, используя имеющуюся у вас версию ПО Wireshark, вы можете использовать собственные трассировочные таблицы. Вдобавок, если вы на самом деле заинтересованы в возможности захвата кадров, вы можете приобрести небольшое USB-устройство *AirPcap*, **cacetech.com**, позволяющее захватывать кадры 802.11 и предоставляющее интегрированную поддержку ПО Wireshark.

Начало работы

Откройте папку wireshark-traces и выберите файл Wireshark_802_11.pcap. Предлагаемая таблица трассировки была собрана с помощью устройства AirPcap и программного обеспечения Wireshark, запущенного на компьютере, подключенного к домашней сети одного из авторов книги. Данная домашняя сеть состоит из комбинированного маршрутизатора/точки доступа 802.11g марки Linksys, двух подключенных по кабелю ПК и одного ПК-беспроводного хоста, подключенного к точке доступа/маршрутизатору. По счастливому стечению обстоятельств в домах по соседству от дома автора также есть несколько точек доступа. В файле трассировочной таблицы вы увидите кадры, захваченные на канале 6. Так как интересующий нас беспроводной хост и точка доступа не единственные устройства, использующие канал 6, мы также увидим большое количество не интересующих нас в рамках данной лабораторной работы кадров, например, сигнальные кадры, распространяемые по сети соседними ТД, также работающими на канале 6. В трассировочной таблице запечатлены следующие транзакции беспроводного хоста:

- На момент начала трассировки хост уже ассоциирован с точкой доступа *30 Munroe St.*
- В момент времени *t = 24,82* хост посылает запрос HTTP на адрес http://gaia.cs.umass.edu/wireshark-labs/alice.txt. IP-адрес сайта gaia.cs.umass.edu – 128.119.245.12.

- В *t=32,82* хост посылает запрос HTTP на адрес http://gaia.cs.umass.edu, чей адрес 128.119.240.19.
- В *t=49,58* хост отключается от ТД *30 Munroe St* и пытается подключиться к *linksys_ses_24086*. Данная точка доступа не является открытой, поэтому, хост не может к ней подключиться.
- В *t=63,0* хост прекращает попытки подключения к точке доступа *linksys_ses_24086* и заново ассоциируется с ТД *30 Munroe St.*

Используя файл трассировки, вы можете загрузить его в программу Wireshark и просмотреть трассировочную таблицу, выбрав пункт **Open** (Открыть) меню **File** (Файл) и дважды щелкнув левой кнопкой мыши по файлу *Wireshark_802_11.pcap*. Окно программы с открытым файлом трассировки должно выглядеть примерно так, как показано на рис. 1.

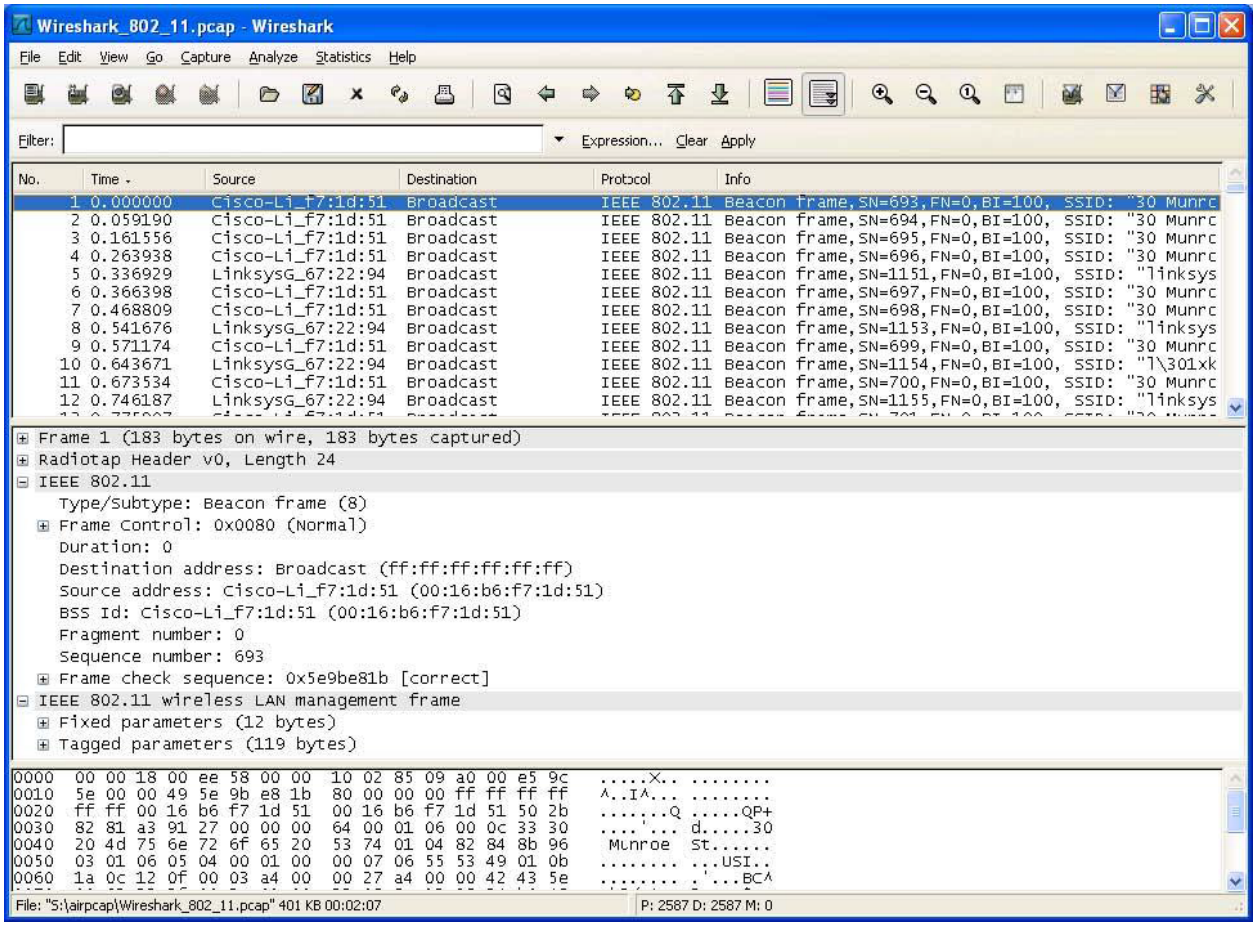

Рис. 1. Окно программы Wireshark после открытия файла *Wireshark_802_11.pcap*

Сигнальные кадры

Вспомним, что сигнальные кадры используются точками доступа 802.11 для распространения информации о своем существовании. Для ответа на некоторые из приведенных ниже вопросов вам потребуется просмотреть подробную информацию о кадре IEEE 802.11» и его подполях в центре окна программы Wireshark. Настоятельно рекомендуем вам всегда иметь под рукой распечатку результатов трассировки с пометками и комментариями, которые помогут вам с ответами[1]. Для того, чтобы распечатать информацию, относящуюся к конкретному пакету, выберите команду меню **File ⇒ Print** (Файл ⇒ Печать), установите переключатель в положение **Selected packet**

[1] Имеются в виду пометки и комментарии, которые можно нанести на бумажных копиях распечаток цветным карандашом, либо на электронных в виде выделения текста и добавления примечаний.

only (Только выбранный пакет), активируйте параметр **Packet summary line** (Заголовок списка пакетов) и включив таким образом минимально необходимый для ответа набор детальной информации о пакете, выведите результаты на печать.

1. Назовите идентификаторы SSID двух точек доступа, согласно таблице трассировки транслирующих наибольшее количество сигнальных кадров.
2. Какова величина временных интервалов между трансляциями сигнальных кадров точки доступа *linksys_ses_24086*? *30 Munroe St*? (*Подсказка*: значение длительности временного интервала содержится в самом сигнальном кадре).
3. Каков (в шестнадцатеричной нотации) исходящий MAC-адрес (адрес отправителя данных) сигнального кадра ТД *30 Munroe St*? Вспомните по рис. 6.13, что в кадре 802.11 используются три типа адреса: исходящий, адрес назначения и BSS. С детальным обсуждением структуры кадра 802.11 можно ознакомиться в разделе 7 стандартизирующего документа IEEE 802.11 (см. выше).
4. Каков (в шестнадцатеричной нотации) MAC-адрес назначения (адрес получателя данных) сигнального кадра ТД *30 Munroe St*?
5. Каков (в шестнадцатеричной нотации) MAC-адрес BSS сигнального кадра ТД *30 Munroe St*?
6. Сигнальные кадры точки доступа *30 Munroe St* сообщают, что данная точка доступа может поддерживать четыре скорости передачи данных и восемь дополнительных «расширенных поддерживаемых скоростей». Что это за скорости?

Передача данных

Так как на момент начала трассировки хост уже ассоциирован с точкой доступа, давайте сначала взглянем на передачу данных по ассоциированному каналу 802.11 прежде, чем мы рассмотрим подключение и отключение к/от ТД. Вспомним, что в приведенной таблице трассировки в момент времени *t=24.82* хост отправляет запрос HTTP на адрес http://gaia.cs.umass.edu/wireshark-labs/alice.txt. IP-адрес сайта gaia.cs.umass.edu 128.119.245.12. Затем, в *t=32,82* хост посылает запрос HTTP на адрес http://gaia.cs.umass.edu.

7. Найдите кадр 802.11, содержащий сегмент SYN TCP для первой сессии TCP (которая загружает файл *alice.txt*). Какие значения содержат три поля MAC-адреса в кадре 802.11? Который из MAC-адресов данного кадра соответствует беспроводному хосту (дайте MAC-адрес хоста в шестнадцатеричном представлении)? Точке доступа? Маршрутизатору первого транзитного участка? Каков IP-адрес беспроводного хоста, выполняющего отправку сегмента TCP? Каков IP-адрес назначения? Соответствует ли IP-адрес назначения хосту, точке доступа, маршрутизатору первого транзитного участка или какому-либо другому устройству, подключенному к сети? Объясните.
8. Найдите кадр 802.11, содержащий сегмент SYNACK для данной сессии TCP. Какие значения содержат три поля MAC-адреса в кадре 802.11? Который из MAC-адресов данного кадра соответствует беспроводному хосту? Точке доступа? Маршрутизатору первого транзитного участка? Соответствует ли указанный в кадре MAC-адрес отправителя IP-адресу устройства, отправившего сегмент TCP, инкапсулированный в данной дейтаграмме? (*Подсказка*: повторно изучите рис. 5.19 в книге, если вы не уверены, как следует отвечать на данный вопрос, либо на соответствующую часть предыдущего вопроса. Понимание этого момента крайне важно.)

Ассоциация и отключение

Вспомним из раздела 6.3.1 книги, что, прежде чем хост сможет выполнять отправку данных, он должен быть *ассоциирован* с какой-либо точкой доступа. В технологии 802.11 ассоциация производится с помощью кадра ASSOCIATE REQUEST, отправляемого

хостом точке доступа, при этом значение типа и подтипа кадра = 0 (см. рис. 6.13 в книге) и кадра ASSOCIATE RESPONSE, отправляемого точкой доступа хосту в ответ на полученный кадр запроса ассоциации, при этом значение типа кадра = 0, а подтипа — 1. Для детального объяснения каждого из полей кадра 802.11 см. стр. 34 (Раздел 7) спецификации 802.11 по адресу **gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf**.

9. Согласно таблице трассировки, какие два действия выполняет (в том смысле, какие кадры отправляет) хост сразу после отметки времени *t=49* для завершения установленной на момент начала трассировки ассоциации с точкой доступа *30 Munroe St*? (*Подсказка*: одно из действий находится на уровне IP, второе — на уровне 802.11). Прочитав спецификацию стандарта 802.11, ожидали ли вы увидеть на данном этапе какой-либо кадр, который отсутствует в данной таблице трассировки?
10. Изучите файл трассировки и найдите кадры AUTENTICATION, отправляемые хостом точке доступа и наоборот. Сколько кадров AUTENTICATION было отправлено беспроводным хостом точке доступа *linksys_ses_24086*, имеющей MAC-адрес Cisco_Li_f5:ba:bb, начиная примерно с временной отметки *t=49*?
11. Намеревается ли хост произвести аутентификацию по введенному ключу или желает, чтобы аутентификация была открытой?
12. Присутствует ли вы в трассировочной таблице ответ AUTENTICATION от ТД *linksys_ses_24086*?
13. Теперь давайте подумаем, что происходит как только хост прекращает попытки ассоциации с точкой доступа *linksys_ses_24086* и теперь пытается подключиться к ТД *30 Munroe St*. Найдите кадры AUTENTICATION отправленные хостом точке доступа и наоборот. В какой момент времени регистрируется кадр AUTENTICATION, отправленный хостом на ТД *30 Munroe St*, и в какой момент времени зарегистрирован ответ AUTENTICATION от этой ТД хосту? (Примечание, для отображения на экране только кадров AUTENTICATION, присутствующих в трассировочной таблице и относящихся к интересующему нас беспроводному хосту, вы можете воспользоваться следующим выражением фильтрации: wlan.fc.subtype == 1 and wlan.fc.type==0 and wlan.addr == IntelCor_d1:b6:4f).
14. Для ассоциации хоста с точкой доступа используется кадр запроса ассоциации (ASSOCIATE REQUEST), отправляемый хостом точке доступа и соответствующий ему кадр ответа на запрос об ассоциации (ASSOCIATE RESPONSE), направляемый точкой доступа хосту. В какой момент времени регистрируется кадр ASSOCIATE REQUEST, отправленный хостом на ТД *30 Munroe St*? Когда был отправлен соответствующий кадр ASSOCIATE REPLY? (Примечание, для отображения на экране только кадров ASSOCIATE REQUEST и ASSOCIATE RESPONSE, присутствующих в трассировочной таблице, вы можете воспользоваться следующим выражением фильтрации: wlan.fc.subtype < 2 and wlan.fc.type==0 and wlan.addr == IntelCor_d1:b6:4f).
15. Какие скорости передачи данных намеревается использовать хост? Точка доступа? Для ответа на эти вопросы вам потребуется рассмотреть поля параметров кадров управления беспроводной локальной сетью 802.11.

Прочие типы кадров

Приводимая нами таблица трассировки содержит несколько кадров PROBE REQUEST и PROBE RESPONSE.

16. Каковы адреса BSS ID MAC отправителя и получателя, указанные в этих кадрах? Какова цель отправки кадров двух вышеупомянутых типов? (Для ответа на последний вопрос вам потребуется углубиться в чтении рекомендуемых ранее в тексте лабораторной работы онлайн источников).