Universidad Rey Juan Carlos

PRÁCTICA PROTOCOLO 802.11

Traducido de Computer Networking: A Topdown Approach, 5th ed. v2.0 © 2009 J.F. Kurose, K.W. Ross.

NOTA: en el laboratorio, se emplearán únicamente las trazas ya capturadas y almacenadas en http://gaia.cs.umass.edu/wiresharklabs/wireshark-traces.zip. En concreto, para esta práctica se utilizará el fichero Wireshark_802_11.pcap, que podrás abrir desde Wireshark.

En esta práctica de laboratorio se trabajará con el protocolo 802.11. Las trazas que se emplean en esta práctica han sido capturadas "en el aire". Desafortunadamente la mayoría de los drivers para dispositivos inalámbricos 802.11 (particularmente bajo el sistema operativo Windows) no proporcionan el soporte necesario para capturar/copiar los paquetes 802.11 recibidos para ser utilizados en Wireshark.

1. Comenzando

Descarga el archivo comprimido http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip y extrae el archivo Wireshark_802_11.pcap. Esta traza ha sido capturada empleando AirPcap y Wireshark ejecutándose en un ordenador en la red doméstica, formada por un Access Point/Router Linksys 802.11g con dos ordenadores conectados por cable y uno de manera inalámbrica. Se dispone también, en las inmediaciones, de otros puntos de acceso en casas vecinas. En este archivo de traza se ven tramas capturadas en el canal 6. Debido a que el host y el AP en los que estamos interesados no son los únicos dispositivos que operan en este canal, se verán también muchas otras tramas que no son interesantes para esta práctica como, por ejemplo, tramas baliza publicitando un AP vecino que también opera en el canal 6. Las actividades del host inalámbrico reflejadas en las trazas del archivo son las siguientes:

- El host ya está asociado con el AP "*30 Munroe St*" cuando se empieza a capturar la traza.
- En el instante *t = 24.82* el host realiza una solicitud HTTP a http://gaia.cs.umass.edu/wireshark-labs/alice.txt. La dirección IP de gaia.cs.umass.edu es: 128.119.245.12.
- En el instante *t=32.82,* el host realiza una petición HTTP a http://www.cs.umass.edu, cuya dirección IP es 128.119.240.19.
- En el instante *t = 49.58,* el host se desconecta del AP *30 Munroe St* e intenta conectarse a *linksys_ses_24086*. Este no es un AP abierto por lo que el host es incapaz de conectarse
- En el instante *t=63.0* el host para de intentar asociarse con el AP *linksys_ses_24086* y se asocia nuevamente con el AP *30 Munroe St.*

Una vez descargada la traza, ésta puede ser cargada en Wireshark y vista en detalle. El resultado mostrado debería ser como el que aparece en la Figura 1.

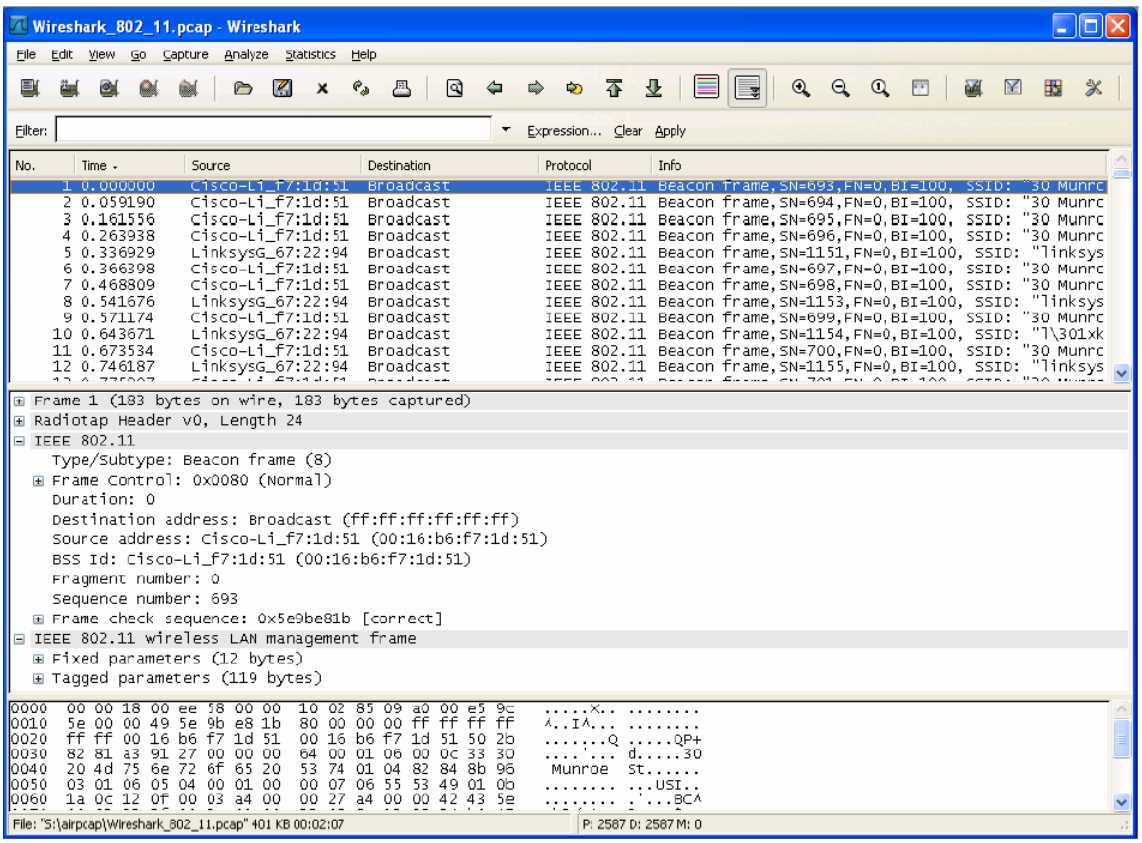

Figura 1: Aplicación Wireshark después de abrir el archivo Wireshark_802_11.pcap

2. Tramas baliza

Las tramas baliza son utilizadas en 802.11 por parte de los AP para publicitar su existencia. Para responder a algunas de las preguntas planteadas más abajo, deberás mirar a los detalles de las tramas IEEE 802.11 que aparecen en la ventana central de Wireshark.

1. ¿Cuáles son los SSID de los dos puntos de acceso responsables de la mayoría de las tramas baliza en esta traza?

2. ¿Cuáles son los intervalos de tiempo entre la transmisión de las tramas baliza del punto de acceso *linksys_ses_24086*? ¿y del punto de acceso *30 Munroe St*.? (Pista: este intervalo de tiempo está contenido en la propia trama baliza)

3. ¿Cuál es la dirección MAC origen (en notación hexadecimal) de la trama baliza enviada desde el AP *30 Munroe St*?

4. ¿Cuál es la dirección MAC destino (en notación hexadecimal) de la trama baliza enviada desde el AP *30 Munroe St*?

5. ¿Cuál es la dirección MAC (en notación hexadecimal) del identificador de la BSS en la trama baliza del AP *30Munroe St*?

6. Las tramas baliza del AP *30 Munroe St* publicitan que el AP puede soportar cuatro tasas de datos diferentes y que, adicionalmente existen ocho tasas extendidas más. ¿Cuáles son estas tasas?

3. Transferencia de información

Dado que la traza comienza con el host ya asociado con el AP, primeramente se observa una transferencia de datos sobre 802.11 antes que una asociación con el AP. Recuerda que en esta traza, en el instante *t = 24.82*, refleja que el host realiza una petición HTTP a http://gaia.cs.umass.edu/wireshark-labs/alice.txt. La dirección IP de gaia.cs.umass.edu es 128.119.245.12. Después, en el instante *t=32.82,* el host realiza una petición HTTP a http://www.cs.umass.edu.

7. Encuentra la trama 802.11 que contenga el segmento SYN TCP para esta sesión TCP (que descarga alice.txt). ¿Cuáles son los tres campos de dirección MAC en la trama 802.11? ¿Qué dirección MAC en esta trama se corresponde con el host inalámbrico? ¿y la del punto de acceso? ¿y la del router? ¿Cuál es la dirección IP del host inalámbrico que envía el segmento TCP? ¿Cuál es la dirección IP de destino? ¿Esta dirección se corresponde con el host, con el AP, con el router o con otro dispositivo unido a la red? Razona tu respuesta.

8. Encuentra una trama 802.11 que contenga el segmento SYN ACK para esta sesión TCP. ¿Cuáles son los tres campos de dirección MAC en la trama 802.11? ¿Cuál de las direcciones MAC en esta trama se corresponde con el host? ¿y con el AP? ¿y con el router? ¿La dirección MAC del emisor en la trama se corresponde con la dirección IP del dispositivo que envía el segmento TCP encapsulado en este datagrama?

4. Asociación

Recuérdese que un host debe asociarse con un AP antes de comenzar a enviar información. La asociación en 802.11 se realiza utilizando una trama de solicitud de asociación (ASSOCIATE REQUEST) enviada desde el host hasta el AP con el tipo y subtipo de trama igual a 0. La trama de respuesta de asociación (ASSOCIATE RESPONSE) es enviada por el AP al host con el tipo de trama 0 y el subtipo 1 en respuesta a una trama de tipo ASSOCIATE REQUEST.

9. ¿Qué dos acciones son realizadas (por ejemplo, tramas enviadas) por el host en la traza, justo después del instante *t=49* para finalizar la asociación con el AP *30 Munroe St* con el que estaba inicialmente enlazado al comienzo de esta práctica?

Mirando a la especificación de 802.11, ¿Existe otra trama que hubieras esperado ver pero que no has visto?.

10. Examina el archivo de la traza y busca tramas de autenticación enviados desde el host al AP y viceversa. ¿Cuántos mensajes de autenticación son enviados desde el host inalámbrico al AP *linksys_ses_24086* (con una dirección MAC de Cisco_Li_f5:ba:bb) comenzando alrededor del instante *t=49*?.

11. ¿Desea el host un proceso de autenticación? o por el contrario ¿desea que el acceso sea abierto?

12. ¿Puedes ver la respuesta de autenticación del AP *linksys_ses_24086* en la traza?

13. Considera lo que sucede a medida que el host intenta asociarse con el AP *linksys_ses_24086* y ahora intenta hacerlo con el AP *30 Munroe St*. Busca tramas de autenticación enviadas desde el host al AP y viceversa. ¿En qué instante hay una trama de autenticación del host hacia el AP *30 Munroe St.*? y ¿Cuándo hay una respuesta por parte del AP? (Puede utilizarse el filtro "wlan.fc.subtype == 11 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" para mostrar solo las tramas de autenticación en esta traza para el host inalámbrico.

14. Una petición de asociación del host al AP y su correspondiente trama de respuesta desde el AP al host son utilizadas por el host para asociarse con un AP. ¿En qué instante hay una solicitud de asociación del host hacia el AP *30 Munroe St?* ¿Cuándo se envía la correspondencia respuesta de aceptación?? (Pueden utilizar los filtros "wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor_d1:b6:4f" para mostrar solo las solicitudes de asociación y su respuesta.

15. ¿Cuáles son las tasas de transmisión aceptables para ser utilizadas? Para responder a esta pregunta necesitarás mirar los campos de la trama 802.11

5. Otros tipos de trama

Nuestra traza contiene un gran número de tramas PROBE REQUEST y PROBE RESPONSE.

16. ¿Cuál es la dirección MAC del BSS ID emisor y receptor? ¿Cuál es el propósito de estos dos tipos de tramas? (Para responder a estas preguntas puede que necesitas consultar referencias en Internet).