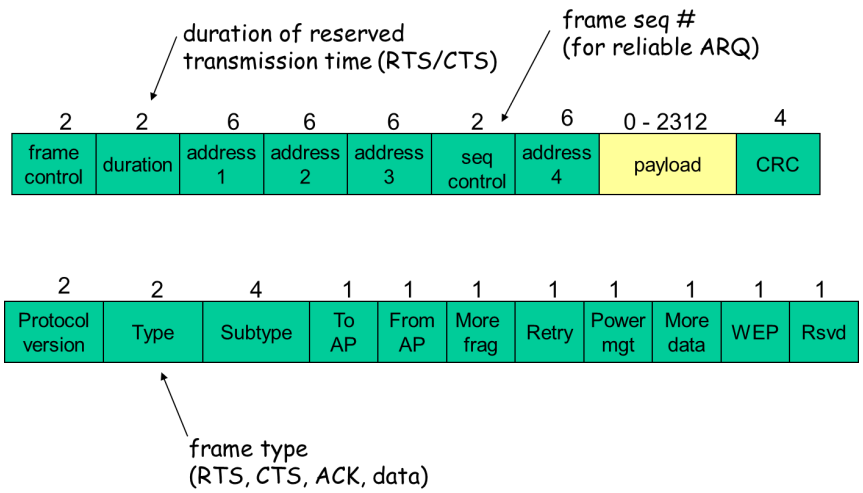
Análisis de redes WiFi - IEEE 802.11 con Wireshark

Todas las respuestas (a las cuestiones y ejercicios) se realizarán en base al contenido de los ficheros Wireshark_802_11, Wireshark_802_11LOCAL y Wireshark_802_11_RTS_CTS(.pcap)

Se aportarán capturas de pantalla, información sobre las tramas involucradas en las respuestas, y grafos de flujo, siempre que la respuesta lo requiera.

Primero, se recuerdan algunos conceptos teóricos del estándar 802.11 de IEEE. Además, dispones de las transparencias del Tema 2, en la que se tratan los temas en más detalle. Puedes consultar cualquier otra bibliografía que consideres de ayuda.

En 802.11 se transmiten tres tipos de tramas : Tramas de datos, de información y de control. Todas tienen la siguiente estructura



Asociación

En 802.11, una estación inalámbrica necesita asociarse a un AP antes de enviar o recibir datos del nivel de red. Cuando un administrador de red instala un AP, el administrador asigna un identificador SSID (Service Set Identifier) al punto de acceso y un número de canal.

802.11 opera en el rango de frecuencias de 2,4 GHz a 2,485GHz. Esta banda de 85 MHz se definen canales parcialmente solapados (dos canales no están separados si y sólo si están separados por 4 o más canales). El estándar 802.11 hace que un AP envíe periódicamente tramas *beacon*[1] que incluyen el SSID del AP y su dirección MAC. Las estaciones escanean los canales a la búsqueda de estas tramas para poder seleccionar una y establecer una asociación.

[1] baliza

Contesta las siguientes cuestiones y ejercicios con las capturas de ficheros Wireshark_802_11 y Wireshark_802_11LOCAL. Un filtro especialmente útil para visualizar los distintos tipos de tramas 802.11 en Wireshark es: wlan.fc.type == 0xAA y wlan.fc.type_subtype= = 0xAABB (donde AA es el tipo y BB el subtipo de trama en hexadecimal).

Cuestión 1. (Localiza las tramas Beacon) *¿Cuántas APs están en la cobertura de la estación desde la que se realizó la captura? ¿Cuales son sus identificadores? ¿Cada cuanto tiempo envían una trama de Beacon? ¿Qué tipo de trama es? (valor de campo tipo)*

Ejercicio 1. *Muestra la estructura y contenido de los campos de una trama Beacon (de ambos ficheros)*

Al proceso de escaneado de canales y escucha de tramas beacon se le denomina escaneado pasivo (*passive scanning)*. Las estaciones también pueden realizar un escaneado activo (*active scanning*), mediante la difusión de una trama *probe*[2] que reciben todas las APs en el rango de la estación inalámbrica. Las APs responden a la trama de petición probe con una trama de respuesta probe.

Cuestión 2. *¿En la captura, hay alguna estación que realice un escaneo activo? ¿Hay APs que respondan? ¿Qué tipos de tramas son? (Consulta e indica el valor de campo tipo)*

Ejercicio 2. *Localiza en la captura alguna trama de petición activo y la respuesta correspondiente. Muestra la estructura y contenido de ambas tramas*

Una vez elegida, la estación envía una trama de *petición de asociación* al AP, y el AP responde con una *respuesta de asociación.* La trama de petición de asociación (*association request*) permite a una interfaz de red (NIC) comenzar el proceso de asociación a un punto de acceso, al cual habilita para reservar recursos y sincronizarse con el NIC. Esta trama transporta información acerca del NIC y el SSID de la red a la que se quiere asociar. Una vez que el AP recibe una petición de asociación, el AP considera asociarse con el NIC y (si acepta) reserve espacio en memoria y establece un identificador de asociación (association ID) para el NIC.

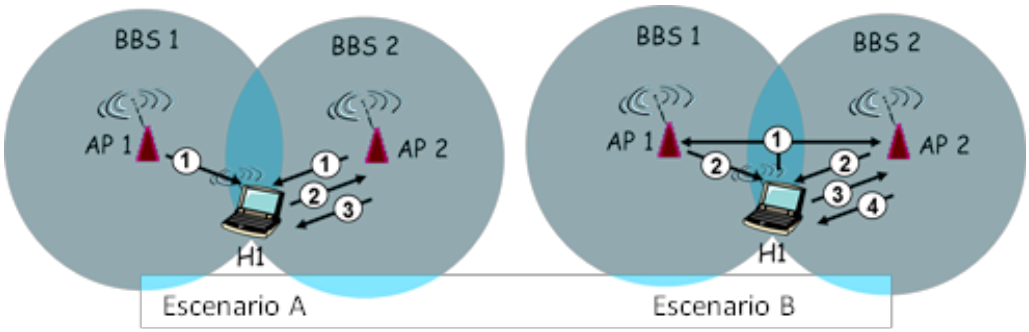
La trama de respuesta de asociación (Association response) es enviada por el AP conteniendo la notificación de asociación o rechazo al NIC que solicitó la asociación. Si el AP acepta, la trama de respuesta incluye información acerca de la asociación. Si la asociación tiene éxito el NIC podrá utilizar el AP para comunicarse con otros NIC de la red y sistemas accesibles a través del sistema de distribución al que se encuentra conectado el AP

Cuestión 3. *Localiza en la captura alguna petición de asociación. ¿Qué información incluye? Localiza en la captura alguna respuesta de asociación ¿Qué información incluye? ¿Qué tipos de tramas con? (valor de campo tipo)*

[2] sonda

Ejercicio 3. *Localiza en la captura alguna trama de petición de asociación y la respuesta correspondiente. Muestra la estructura y contenido de ambas tramas*

Cuestión 4 *¿Cual de estos dos escenarios correspondería con un escaneado pasivo y con uno activo? ¿Por qué?*



Transmisión de Datos

Una trama de datos en 802.11 consiste en un campo de control de trama, campos de dirección, cuerpo de la trama y campo de secuencia de comprobación de trama. La trama de control tiene la misma estructura que el resto de tramas 802.11. El subcampo ***Type*** en el campo de control distingue a una trama de datos de otros tipos. Además las tramas deben ser confirmadas con ACKs

Cuestión 5. *¿Cuántas tramas de datos diferentes observas en la captura? ¿Qué estaciones participan de esta comunicación? ¿Hay comunicación directa entre estaciones o siempre interviene un punto de acceso?*

Ejercicio 4 *Localiza en la captura alguna trama de datos y la confirmación correspondiente. Muestra la estructura y contenido de ambas tramas.*

Ejercicio 5. *Localiza en la captura alguna trama de datos NULL Muestra la estructura y contenido de esta trama. ¿Qué la diferencia de las tramas de datos normales? ¿Para qué sirve?*

Direccionamiento

Las tramas de datos pueden ser enviadas a una estación en particular o a múltiples estaciones a través de multicasting. Las tramas de datos viajan directamente de un cliente ad hoc a otro. En WLANs con infraestructura (con AP), las tramas de datos no viajan directamente entre estaciones. En su lugar, las estaciones envían la trama de datos a un punto de acceso y el punto de acceso envía el contenido de la trama de datos original en otra trama de datos a la estación receptora. Para más detalles acerca del uso de los cuatro campos de direccionamiento en las tramas IEEE 802.11 consulta las transparencias (Mecanismo de Direccionamiento).

Entre la captura del fichero Wireshark_802_11.pcap, alrededor del t=24.81, el host realiza una petición HTTP a http://gaia.cs.umass.edu/wireshark-lbs/alice.txt. (La dirección IP de gaia.cs.umass.edu es 128.119.245.12). Después, en t=32.82 (aprox.), el host hace una petición HTTP a http://www.cs.umass.edu

Cuestión 6. *Encuentra la trama que contenga el segmento TCP SYN de la primera sesión TCP (que descarga alice.txt). Muestra su contenido.*

6.a *¿Cuáles son las tres direcciones MAC de esta trama? ¿Cuál es la dirección MAC correspondiente al host inalámbrico desde el que se hace la petición? (representación hexadecimal) ¿Cuál la del punto de acceso? ¿y la del (primer) router?*

6.b *¿Cuáles es la dirección IP del host inalámbrico que envía este segmento? ¿y la dirección IP destino? ¿con que se corresponde esta dirección IP destino? (host, punto de acceso, router, o cualquier otro dispositivo de la red). Razona tu respuesta*

Colisiones

Para evitar colisiones, el protocolo 802.11 hace uso de las tramas RTS y CTS, que además resuelven el problema de la estación oculta.

Sobre la captura de los ficheros Wireshark_802_11.pcap y Wireshark_802_11_RTS_CTS.pcap

Cuestión 7 . Localiza las tramas RTS y CTS capturadas en el fichero Wireshar_802_11.pcap. ¿Es posible que sólo haya tramas RTS o CTS? ¿Por qué?

Cuestión 8 . Localiza las tramas RTS y CTS capturadas en el fichero Wireshar_802_11_RTS_CTS.pcap. ¿Qué información contiene estas tramas? ¿Para qué sirve el valor NAV?