Práctica 8: Análisis de tráfico WIFI

1. Video

https://media.upv.es/#/portal/video/c702b81a-35f9-469f-89e1-d1852b93ac83

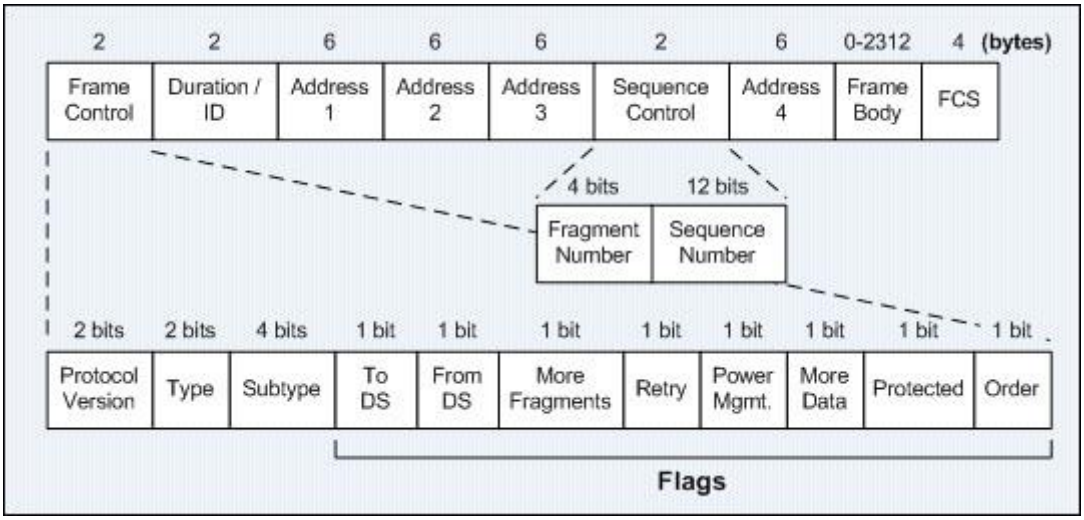
2. Introducción

Las redes de datos inalámbricas prácticamente se han convertido en algo imprescindible en nuestra vida cotidiana. Tras su introducción masiva en los ordenadores portátiles, ahora hacemos uso de ellas en todo tipo de dispositivos móviles (teléfonos, tabletas, etc.). El motivo de su gran aceptación es claro: permiten una flexibilidad que las redes cableadas no tienen. Además, al no necesitar conectores físicos también se permite la fabricación de dispositivos más compactos y manejables. Sin embargo, el hecho de no proteger la señal que transporta los datos en el medio de transmisión, como ocurre en las redes cableadas, provoca que las prestaciones de las redes inalámbricas sean, en general, inferiores a las de las redes cableadas. No obstante, la mayor flexibilidad que aportan suele compensar esta pérdida de prestaciones en la mayoría de los casos.

En esta práctica vamos a realizar un primer estudio de las redes de datos inalámbricas que siguen el estándar IEEE 802.11. Nótese que estas redes son mucho más complejas que las redes cableadas como Ethernet. Por ello, en esta práctica vamos a realizar un estudio sencillo sin entrar en muchos de los detalles de funcionamiento de las redes IEEE 802.11. También vamos a incluir en este estudio cuestiones relacionadas con la red cableada a la que se conecta el punto de acceso de una red inalámbrica dada.

3. Formato de las tramas 802.11

El formato general de las tramas 802.11 se presenta en la siguiente figura, donde también se muestran los formatos de dos de los campos de la cabecera de las tramas: el campo de control y el de secuencia.



A modo de breve introducción, el significado de cada uno de los campos de la trama 802.11 es el siguiente:

- **Frame control**: este campo incluye diversos subcampos y flags necesarios para el correcto funcionamiento del protocolo. El significado de estos subcampos y flags se describirá un poco más abajo.
- **Duration/ID**: Este campo tiene diversos significados dependiendo del valor de los bits 15 y 14 (bits MSB). De forma resumida, este campo puede indicar, o bien el número de microsegundos que el medio de trasmisión va a estar ocupado con la transmisión de la trama en curso, o bien cuestiones relacionadas con el ahorro de energía del dispositivo inalámbrico (en concreto, que se transmitan las tramas almacenadas en el punto de acceso mientras el dispositivo inalámbrico estaba en modo de bajo consumo).
- **Direcciones 1, 2, 3 y 4**: Estos campos de 48 bits contienen las direcciones MAC involucradas con la trama en curso. A modo de regla general, y para las tramas de datos unicamente, el campo "dirección 1" contiene la dirección MAC del dispositivo que debe recibir la trama que se está transmitiendo. El campo "dirección 2" contiene la dirección MAC del dispositivo que ha transmitido la señal inalámbrica.

  Nótese que puede ocurrir que la MAC contenida en el campo "dirección 1" no sea el destino final de la trama (por ejemplo, el destino final de la trama no es un dispositivo inalámbrico sino una tarjeta de red en la parte cableada, más allá del punto de acceso). Asimismo, puede darse el caso de que la MAC contenida en el campo "dirección 2" no sea el origen inicial de los datos contenidos en la trama 802.11 (es decir, el origen de los datos sería una tarjeta de red en la parte cableada, por ejemplo). Por este motivo, hace falta un tercer campo ("dirección 3") que indique dicha información. El campo "dirección 3" contiene el origen real de los datos (ya sea en la parte cableada o en la parte inalámbrica) o el destino final de los datos (en la parte cableada o en la parte inalámbrica). Para poder interpretar correctamente la información contenida en el campo "dirección 3" habrá que hacer uso de los flags "To DS" y "From DS" contenidos en el campo "Frame control".

  Finalmente, el campo "dirección 4" se usa para la comunicación entre puntos de acceso y queda por tanto fuera de este estudio inicial de las redes IEEE802.11.

- **Sequence Control**: Este campo se usa para tareas de reensamblado de mensajes del nivel superior que se enviaron fragmentados y también para detectar la recepción de tramas duplicadas. Para ello tiene dos subcampos:
    - **Fragment number**: Cuando un mensaje del nivel superior se fragmenta, este subcampo indica el número de fragmento (el primer fragmento tiene el número 0 y a partir de ahí se usan números consecutivos).
    - **Sequence number**: Este subcampo se usa a modo de identificador, de forma que dos tramas diferentes tienen valores diferentes en este subcampo. Si una trama debe retransmitirse (porque no se ha recibido el ACK correspondiente, por ejemplo), entonces la trama retransmitida mantiene el mismo número de secuencia. De esta forma, el receptor puede saber si los datos recibidos son nuevos o si ya se recibieron. Nótese que cuando una trama se fragmenta, todos los fragmentos tienen el mismo número de secuencia.
- **Frame body**: este campo contiene los datos enviados en la trama. La longitud máxima de este campo son 2304 bytes (2312 incluyendo los datos WEP).
- **FCS (Frame Check Sequence)**: Es el código CRC que permite saber si la trama se ha recibido sin errores de transmisión.

Respecto al campo “frame control”, los diferentes subcampos y flags que contiene son los siguientes:

- **Protocol version**: indica qué versión exacta del protocolo 802.11 está contenida en el resto de la trama. Actualmente solo hay una versión de 802.11 y se le asigna el valor 0. En el futuro quizá haya nuevas versiones.
- **Type** y **subtype**: Indica qué tipo de trama es la trama en curso, así como el subtipo.

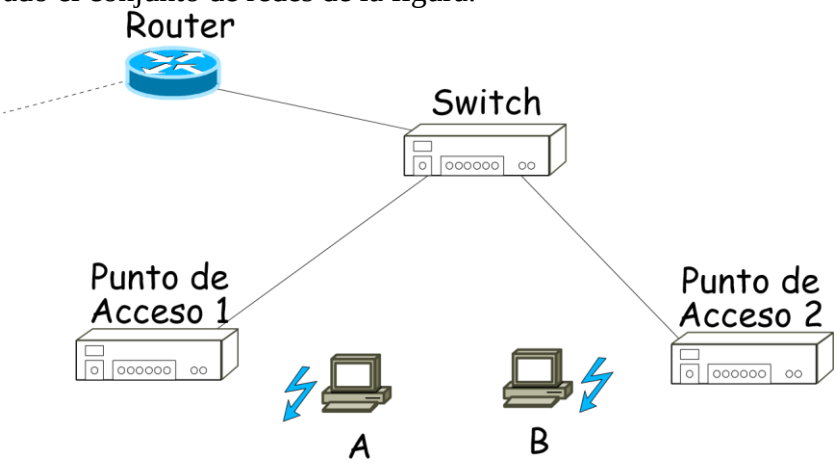
  Los tipos de trama son:
  - Management (type = 00)
  - Control (type = 01)
  - Data (type = 10)

  Cada tipo de trama contiene diversos subtipos. Por ejemplo, dentro del tipo “management” encontramos, entre otros, los subtipos
  - *Association request (0000)*
  - *Association response (0000)*
  - *Probe request (0100)*
  - *Probe response (0101)*
  - *Beacon* (1000)

  Dentro del tipo “control” están, entre otros, los subtipos:
  - *RTS (1011)*
  - *CTS (1100)*
  - *Acknowlegment (1101)*
- **ToDS** y **FromDS**: Estos flags se usan principalmente para indicar si la trama en curso viene del punto de acceso (“DS” significa “Distribution System”, que hace referencia a la red cableada), o si va al punto de acceso.
  - ToDS = 1 y FromDS = 0: la trama se origina en la parte inalámbrica y va destinada hacia el punto de acceso
  - ToDS = 0 y FromDS = 1: la trama se transmite desde el punto de acceso y va destinada a una estación inalámbrica
  - Las otras dos combinaciones de estos flags también se usan y tienen su propio significado, pero no los vamos a revisar en esta práctica.
- **More fragments**: Este flag se usa de forma similar al bit “more fragments” de la cabecera del datagrama IP. En este sentido, cuando un mensaje proveniente de la capa superior ha sido fragmentado en varias tramas, todos los fragmentos menos el último llevan este flag a uno.
- **Retry**: Este bit se pone a uno cuando se está retransmitiendo una trama previamente transmitida. Así se ayuda al receptor a eliminar tramas duplicadas.
- **Power management**: Cuando una estación transmite una trama, si pone este bit a uno indica que tras finalizar la transmisión en curso se pondrá en modo de ahorro de energía (y por tanto no recibirá tramas, las cuales tendrán que ser temporalmente almacenadas por el punto de acceso).

- **More data**: Como el punto de acceso tiene que almacenar tramas destinadas a dispositivos que se han puesto en modo de bajo consumo, este bit es usado por el punto de acceso para indicar si tiene tramas almacenadas pendientes de envío.
- **Protected (WEP)**: Cuando una trama está cifrada, este bit se pone a uno
- **Order**: Si se requiere que las tramas se transmitan en el orden en que se han generado (o recibido en el punto de acceso), este bit se pone a uno. Nótese que el uso de transmisión en orden requiere usar recursos adicionales tanto en el transmisor como en el receptor.

Ejercicio 1. Dado el conjunto de redes de la figura:



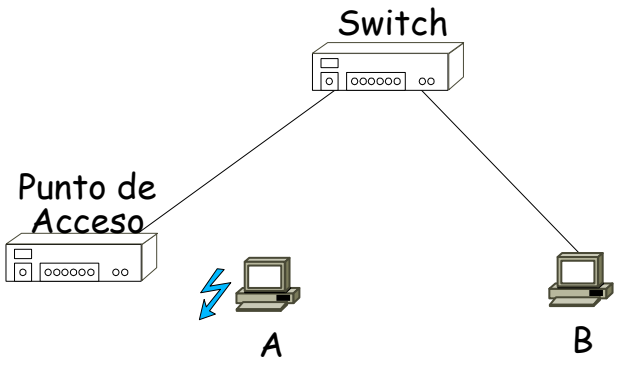
Todas las redes cumplen el estándar IEEE 802.3 o IEEE 802.11. El conmutador (*switch*) conoce la ubicación de todas las máquinas tras un periodo de funcionamiento. El *router* está correctamente configurado. La estación A está asociada al punto de acceso 1, mientras que la estación B está asociada al punto de acceso 2. Las cachés ARP de todos los sistemas están vacías, a excepción de las del router, que contiene todas las direcciones físicas necesarias.

Indica, completando una tabla como la siguiente (usa tantas filas como necesites), la secuencia de tramas que se generarán en el envío de un mensaje ICMP de tipo 8 desde el ordenador A al ordenador B (solamente el envío; no hay que describir las tramas que se generarían en la respuesta). Para las direcciones físicas utiliza los valores simbólicos A, B, PA1, PA2, etc. Para las direcciones IP utiliza los valores simbólicos IP A, IP B, IP R, etc.

Tipo de trama IEEE	Dir. destino/ Dir. 1	Dir. origen/ Dir. 2	Dir. 3	Dir IP origen relacionada (si la hay)	Dir IP destino relacionada (si la hay)	Papel que desempeña la trama	Máquinas (nodos) cuya tarjeta de red recibe copia de la trama

4. Análisis de tráfico. Escenario 1

Para comenzar nuestro estudio del tráfico generado por estaciones inalámbricas, vamos a usar el escenario mostrado en la figura:



En este escenario tenemos dos ordenadores. El ordenador A está asociado al punto de acceso, mientras que el ordenador B tiene una conexión de red cableada. Por otra parte, en lugar de realizar nosotros las capturas de paquetes con el programa wireshark, vamos a usar unas capturas previamente realizadas y que están contenidas en los ficheros **wifi2cable_1** y **wifi2cable_2**. Estos ficheros se encuentran en poliformaT. El motivo para utilizar unas capturas realizadas previamente es que no resulta sencillo capturar tráfico inalámbrico. Para poder llevar a cabo dichas capturas (y ver los campos asociados a IEEE802.11) es necesario que la tarjeta de red inalámbrica pueda operar en modo monitor. Por otra parte, en el laboratorio de redes hay mucho tráfico inalámbrico, lo cual podría complicar sobremanera el análisis de las capturas. Por ello, las capturas que vamos a estudiar se han realizado en un entorno con muy poco tráfico.

Por otra parte, el tráfico a analizar se ha generado ejecutando la orden "**ping -c 1 dir_IP_B**" en el ordenador A, y se ha capturado ejecutando el programa wireshark tanto en el ordenador A como en el ordenador B (de ahí que haya dos ficheros de captura).

Ejercicio 2. Abre desde el wireshark el fichero **wifi2cable_1** y responde a las siguientes cuestiones.

1. De acuerdo con el formato de las tramas que muestra wireshark, ¿se trata de las tramas capturadas en el segmento de red cableado o en el segmento inalámbrico?
2. ¿Cuál es la dirección IP del ordenador A? ¿Cuál es la dirección IP del ordenador B?
3. ¿Por qué se generan las dos primeras tramas de la captura?
4. ¿Cuáles son las direcciones físicas que aparecen en las tramas de la captura? ¿A quiénes corresponden dichas direcciones físicas?
5. ¿Cuál es la longitud de los datagramas enviados? ¿Ha hecho falta fragmentar dichos datagramas debido a un MTU demasiado pequeño? ¿Cuál es la longitud de los datos contenidos en el mensaje ICMP?

Ejercicio 3. Tras analizar en el ejercicio anterior parte del tráfico generado por la orden "**ping -c 1 dir_IP_B**", en este ejercicio vamos a analizar el resto del tráfico generado. Para ello, abre la captura **wifi2cable_2** (en esta captura se han eliminado todas las tramas que no son consecuencia directa de la orden ping, con el fin de facilitar el análisis del tráfico. La captura completa se puede encontrar en el fichero **wifi2cable_2_completa**).

1. De acuerdo con la información contenida en dicha captura, ¿se trata de las tramas capturadas en el segmento de red cableado o en el segmento inalámbrico?
2. ¿Puedes ver el contenido de los mensajes ARP e ICMP que has visto en la captura anterior? ¿Cuál crees que es la razón por la que no puedes ver el contenido de dichos mensajes?
3. Intenta localizar en esta captura las tramas generadas al ejecutar la orden ping y que complementan el tráfico analizado en el ejercicio anterior.

El motivo por el cual en la captura del ejercicio 3 no se muestran los datos contenidos en las tramas capturadas es porque dichos datos van cifrados de acuerdo con el protocolo WPA-PSK. Para poder ver los mensajes ARP e ICMP que viajan en las tramas de la captura sería necesario disponer de la clave asociada al punto de acceso. Esta clave es del estilo de las que habitualmente se introducen por pantalla cuando nos asociamos desde Windows o Linux a un punto de acceso. En nuestro caso, y dado que el ordenador desde el que se ha hecho la captura ya disponía de dicha clave, basta con ir al menú "Edit"-->"Preferences" y buscar en la ventana que aparece el protocolo "IEEE802.11". En las opciones que nos permite modificar, buscaremos la que dice "**Ignore the protection bit**" y seleccionaremos "**Yes – with IV**". A partir de ese momento podemos acceder al contenido de las tramas de la captura.

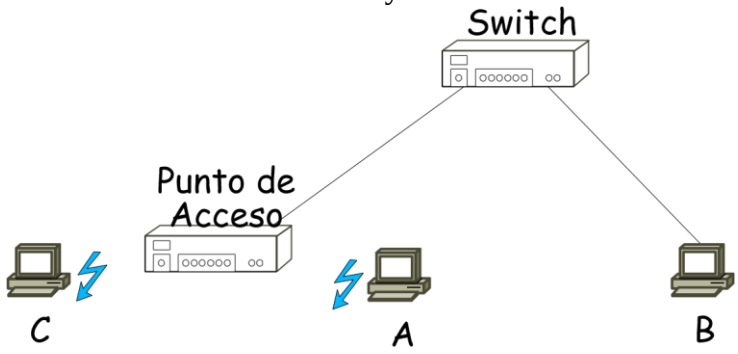
Ejercicio 4. Tras modificar las opciones de cifrado de acuerdo con la descripción anterior, responde a las siguientes cuestiones:

1. Localiza las tramas asociadas al protocolo ARP. ¿Cuántas tramas hay? ¿Hay el mismo número de tramas ARP que en la captura anterior? ¿Por qué?
2. ¿Cuál es la dirección física del punto de acceso? ¿Se trata de la dirección física en la parte cableada o en la parte inalámbrica? ¿Aparecía dicha dirección física en la captura anterior? ¿Por qué?
3. Céntrate en las dos primeras tramas ARP que se envían (tramas 1 y 2 en la captura). Aparentemente son iguales. ¿Qué diferencias observas entre ellas?
4. Analiza los bits "From DS" y "To DS" de ambas tramas. ¿Qué conclusiones extraes? ¿Estas conclusiones son coherentes con las diferencias que has observado en el punto anterior?
5. Busca en la captura la respuesta ARP. ¿Coinciden las direcciones MAC con las de la captura anterior? ¿Son diferentes? ¿Por qué?
6. Centrémonos ahora en la petición y respuesta del ping. ¿Cuáles son las direcciones MAC que intervienen en ambas tramas? Esas direcciones, ¿son coherentes con las direcciones MAC de la captura anterior?
7. ¿Cuáles son las direcciones IP que aparecen en esta captura? ¿Son las mismas que las que aparecían en la captura anterior? ¿Cuál es la dirección IP del punto del acceso?

8. Fíjate en los números de secuencia de las diferentes tramas que se generan como consecuencia de la orden ping (compara la respuesta del ARP y la respuesta del ping). ¿Son consecutivos?
9. De acuerdo con la captura que estás analizando, ¿se han fragmentado los mensajes ICMP? ¿Y los mensajes ARP?

5. Análisis de tráfico. Escenario 2

Vamos a continuar nuestro estudio de las redes inalámbricas introduciendo un ordenador adicional en el escenario de captura. Ahora vamos a tener el escenario de la figura siguiente, donde se ha introducido la estación inalámbrica C, que está asociada al mismo punto de acceso que el ordenador A del escenario anterior. Los ordenadores A y C no se ven entre ellos.



De forma similar al análisis anterior, en este caso vamos a analizar el tráfico generado por la orden "**ping -c 1 dir_IP_C**", que se ejecuta, de nuevo, en el ordenador A. Para capturar dicho tráfico se ha ejecutado el programa wireshark tanto en el ordenador B como en el ordenador A (de nuevo tenemos dos ficheros de captura: **wifi2wifi_1** y **wifi2wifi_2** (en esta ocasión no se han limpiado los ficheros de captura)).

Ejercicio 5. Abre con el programa wireshark el fichero de captura **wifi2wifi_1** y contesta a las siguientes preguntas:

1. ¿Qué contiene este fichero de captura? ¿Es correcto que contenga la(s) trama(s) que aparecen en la pantalla? ¿Falta alguna trama?
2. Comprueba las direcciones MAC y las direcciones IP que aparecen en el fichero. ¿A quién corresponden estas direcciones? ¿Son las mismas que en el escenario anterior?
3. A partir de la información contenida en esta captura, ¿puedes conocer las direcciones MAC y/o IP de los ordenadores incluidos en el escenario de la figura?

Ejercicio 6. Abre con el programa wireshark el fichero de captura **wifi2wifi_2** y contesta a las siguientes preguntas:

1. ¿En cuántas tramas aparece la dirección MAC del ordenador A? ¿Qué papel desempeñan dichas tramas?
2. Respecto a la primera trama que contiene la dirección MAC del ordenador A como origen de la trama, ¿qué papel desempeña dicha trama? ¿qué información se busca con

dicha trama? ¿Cuáles son las direcciones MAC involucradas en esa primera trama? ¿A quiénes perteneces esas direcciones MAC?

3. Volviendo sobre la trama anterior, ¿qué direcciones IP aparecen? ¿a quiénes pertenecen dichas direcciones IP?
4. La trama anterior parece que esté repetida en la captura. Analiza el por qué de esta duplicidad.
5. Localiza la trama que se genera como contestación a la trama anterior. ¿Quién transmite dicha trama? ¿Quién es el creador original de dicha trama? ¿Aparece en la captura la trama original transmitida por el creador inicial de dicha trama? ¿Por qué?
6. De acuerdo a la trama anterior, ¿cuál es el valor de la información buscada en la primera trama que envía el ordenador A?
7. Vuelve sobre las tramas analizadas y comprueba los bits "ToDS" y "FromDS" de las mismas. ¿El valor de dichos bits para cada una de las tramas es el esperado?
8. Busca las tramas que contienen el echo request y el echo reply que se transmiten como consecuencia de la orden "ping -c 1 dir_IP_C". ¿Cual es la dirección MAC que transmite cada una de esas tramas? ¿Y la dirección MAC del creador del mensaje inicial contenido en las tramas? ¿Qué direcciones destino se utilizan? Observa que tanto la dirección MAC del punto de acceso como las de la fuente y destino de las tramas aparecen en la cabecera de la trama en distinto orden dependiendo de que actúen como dirección 1, 2 o 3 (puedes mirar el apartado 3 de la práctica para revisar el formato de las tramas). ¿Quién debe quedarse copia de cada una de las tramas? ¿Serán retransmitidas dichas tramas?
9. Analiza el campo número de secuencia de las tramas siguientes: beacon, ARP y ping. ¿Encuentras alguna relación entre los números de secuencia que usa el punto de acceso?
10. Teniendo en cuenta que las estaciones A y C no se ven entre ellas, pero que ambas ven al punto de acceso, ¿falta alguna trama relacionada con la orden ping en la captura?