Práctica 1

Utilizar Wireshark para capturar y analizar tramas de Ethernet II y Wifi.

Conocimientos previos

□ Funcionamiento básico de las arquitecturas en capas, especialmente TCP/IP (tema 1).
□ Funcionamiento básico del encapsulamiento (tema 1).
□ Medidas de rendimiento en redes (tema 1).
□ Funcionalidad principal de la capa de enlace y su ámbito (tema 2).
□ Trama Ethernet: campos y características (tema 2).
□ Direcciones MAC: propiedades y tipos de direcciones (tema 2).
□ Protocolo CSMA/CA (tema 2)
□ Trama Wifi: campos y características (tema 2)

Información básica

Cuando los protocolos de capa superior se comunican entre sí, los datos fluyen hacia abajo en las capas TCP/IP y se encapsulan en la trama de la Capa 2. La composición de la trama y el tipo de tramas depende del tipo de acceso al medio. Por ejemplo, si el acceso al medio es Ethernet, la encapsulación de la trama de la Capa 2 será Ethernet II. Cuando se aprende sobre los conceptos de la Capa 2, es útil analizar la información del encabezado de la trama. Este encabezado se examinará en esta práctica de laboratorio. Las tramas de Ethernet II pueden admitir diversos protocolos de la capa superior, como IP, ARP...

En otros casos, el acceso al medio es más complejo debido a las propias características del mismo y requiere de mecanismos más elaborados como en el caso de la Wifi donde se usa CSMA/CA y requiere de tramas especiales (RTS, CTS, ACK…) para validar que la comunicación se realiza sin problema. En esta práctica analizaremos las tramas intercambiadas y su formato para afianzar y entender mejor su funcionamiento.

Escenario 1

Se utiliza Wireshark para capturar y analizar los campos de encabezado de tramas de Ethernet II. El análisis se realizará sobre el tráfico de red generado por el comando **`ping`** de Windows y el navegador web.

Paso 1: Configurar Wireshark para las capturas de tramas.

Prepare Wireshark para las capturas. Abra el programa como administrador si es posible. Para comenzar la captura de paquetes, seleccione en el menú **Captura > Opciones,** y luego haga clic en el botón "**Inicio**" (y en el botón *Detalles* si desea información adicional sobre la interfaz) de la tarjeta de red. Nota: **desactiva el modo promiscuo**, para capturar sólo el tráfico entrante o saliente hacia/desde tu ordenador (debería estar desactivado por defecto, compruébalo abriendo el botón Opciones de la ventana Interfaces). Con estas acciones se inicia la captura de paquetes.

Paso 2: Generar tráfico a www.informatica.uma.es y capturar la sesión en un fichero p1.pcapng.

Abra una ventana terminal de Windows (clic en **Inicio > Ejecutar**, escriba **`cmd`**). Para preparar el sistema y obtener el comportamiento esperado escriba el siguiente comando:

```
ipconfig /flushdns
```

Si tenéis acceso como administrador, también es conveniente:

```
arp –d
netsh interface ip delete arpcache
```

En la ventana de comandos ejecute un **`ping`** entre su ordenador y **www.informatica.uma.es**.

```
ping –n 1 www.informatica.uma.es
```

Posteriormente, abra el modo incógnito del navegador y acceda a la página de nuestro centro (**http://www.informatica.uma.es**[1]). La sesión comienza con el protocolo ARP haciendo consultas para la dirección MAC del *gateway*, seguida de una consulta DNS. Finalmente, el comando **`ping`** emite solicitudes de eco y el navegador

[1] No se olvide de poner el http://

pedirá (y recibirá) la página web. Cuando el comando haya finalizado la ejecución, detenga las capturas de Wireshark. Guarde la captura como **p1.pcapng**.

¿Qué ocurrirá?

i) En primer lugar, el protocolo ARP comenzará a solicitar la dirección MAC de la pasarela.

ii) A continuación, se envía una petición al servidor DNS.

iii) Más tarde, el comando ping envía peticiones de eco y espera las respuestas de eco.

iv) Por último, el navegador enviará una petición para obtener la página inicial del sitio web que se descargará inmediatamente.

Paso 3: Analizar la captura de Wireshark.

La ventana de la lista de tramas de Wireshark debe comenzar con una solicitud y respuesta ARP para la dirección MAC del *gateway*. Luego, se realiza una solicitud DNS para la dirección IP de **www.informatica.uma.es**. Finalmente, se ejecuta el comando **`ping`** (paquetes ICMP) y las peticiones del navegador (paquetes HTTP). Filtre la captura para que sólo parezcan las tramas pertenecientes a los protocolos ARP, DNS, ICMP y HTTP.

Ejercicio 1. Elija un mensaje `ICMP`, y localice en la cabecera Ethernet II[2] la siguiente información:

Número de la trama analizada:
Información de la dirección MAC de su computadora:
Dirección MAC (en hexadecimal):
Fabricante de NIC (en hexadecimal): nombre:
Número de serie de NIC (en hexadecimal):

Información de la dirección MAC de *gateway/router*:
Dirección MAC (en hexadecimal):
Fabricante de NIC (en hexadecimal): nombre:
Número de serie de NIC (en hexadecimal):

Ejercicio 2. Indique qué filtro debe añadir para que se muestren las tramas donde no se utilice su dirección MAC (ni como origen ni como destino). ¿Cuántas tramas recibe? ¿Por qué recibe esas tramas? (Para responder esta pregunta, observe las características de las direcciones MAC destino de esas tramas)

Ejercicio 3. Dibuje la torre de protocolos (tal como se ha visto en clase, es decir, en la parte inferior los protocolos de más bajo nivel) de un paquete ARP, uno ICMP, uno DNS y uno HTTP[3]. Indique el número de la trama usado en cada caso.

Ejercicio 4. Observe el valor del campo **tipo** de la cabecera Ethernet II para cada uno de los mensajes anteriores. Rellene la tabla y responda a las preguntas: ¿Qué significa este campo? ¿Por qué en tramas diferentes es igual?

	Tipo en la cabecera Ethernet II (valor en hexadecimal y en texto)
ARP	
HTTP	
ICMP	
DNS	

Ejercicio 5. En Wireshark observe **la diferencia entre el tiempo** de la primera petición ICMP (`Echo (ping) request`) y su respuesta (`Echo (ping) reply`). Indique los números de las tramas consultadas. ¿Cuánto tiempo es? ¿A qué concepto visto en la parte de teoría equivale dicho tiempo?

Ejercicio 6. Según la teoría vista en clase, las tramas Ethernet deben tener un **tamaño mínimo** de 64 bytes. Wireshark no muestra el campo FCS (ya que es tratado automáticamente por la tarjeta de red), por lo que la trama mostrada en

[2] Recuerde que el significado de los campos de "destination" y "source" cambia dependiendo si es un envío (en ICMP sería un mensaje tipo `Request`) o recepción (en ICMP sería un mensaje tipo `Reply`).

[3] Como protocolo Wireshark debe mostrar `http` y no `TLSvX`

Wireshark tendrá un tamaño de 60 bytes o más. Busque una trama con tamaño 60 (filtro: `frame.len == 60`), ¿cuántas tramas tienen esta característica? ¿Qué mecanismo se utiliza para completar el tamaño si los datos transmitidos son más pequeños de 46 bytes)?

Escenario 2

En el anterior escenario se analizó el tráfico cuando como capa de enlace se utilizaba Ethernet (802.3) y en este caso se utilizará Wifi (802.11). Como capturar tráfico de la tarjeta de red wifi es más complejo, en este caso, se proporciona en el campus virtual una traza con tráfico wifi (**p1-wifi.pcapng**) para analizarlo.

Paso 4: Analizando tráfico wifi

En el caso del tráfico wifi, Wireshark ofrece la siguiente información para cada trama:

- **Frame X:** Resumen de la traza (información generada por Wireshark, realmente no aparece en la trama)
- **Radiotap Header:** Cabecera de la capa física
- **802.11 radio information:** información generada por Wireshark a partir de la cabecera previa
- **IEEE 802.11:** Cabecera Wifi (dependiendo del tipo puede contener a continuación otra información adicional que Wireshark muestra como otra capa IEEE 802.11)
- **Data:** Información que viaja en la trama (dependiendo del tipo de trama puede que no aparezca).

En los siguientes ejercicios nos centraremos en la cabecera wifi (las cabeceras identificadas como IEEE 802.11 por Wireshark).

Ejercicio 7. Las tramas Beacon son utilizadas por wifi para anunciar los datos de la wifi para que los dispositivos puedan conectarse. Elija una trama Beacon (por ejemplo la trama 1) y responda las siguientes preguntas:

- Número de trama elegido:
- ¿Qué tipo de trama (gestión, control o datos) es? ¿En qué campo se puede ver?
- ¿Cuál es el destino de la trama? ¿Por qué va a esa?
- Observe el BSS ID, ¿sabría decidir cómo se calcula el ID usado en cada BSS?
- ¿Cuál es el SSID de la red wifi?
- Analizando la información de la capa física, indica en qué canal transmite y si usa las frecuencias de 2.4 GHz o las de 5 GHz

En las tramas 15946 a 15949 (puede ser el filtro: `frame.number >= 15946 && frame.number <= 15949`) se observa la comunicación entre dos estaciones (STA) que llamaremos Proxim y Netgear (por el fabricante de su NIC) a través de un punto de acceso (AP) que llamaremos Cisco (por el mismo motivo).

Ejercicio 8. Sobre las tramas CTS y RTS:

- ¿Qué tipo de trama (gestión, control o datos) es?
- ¿Cómo se sabe si la trama es CTS o RTS?
- ¿Cuánto vale el NAV en estas tramas?
- ¿Por qué la trama CTS ocupa 6 bytes menos que la RTS?

Ejercicio 9. Sobre las tramas de Datos (QoS Data) y su ACK (Block ACK):

- ¿Qué tipo de trama (gestión, control o datos) es cada una?
- Observe los campos de control “A DS” (To DS) y “De DS” (From DS), ¿está Proxim, Netgear y Cisco en la misma red wifi (BSS)?
- ¿Explica lo anterior por qué no se observan en la traza los RTS/CTS asociados con Netgear?
- ¿Cuál es la estación (STA) origen de la trama de datos? ¿y la estación final? ¿viaja la trama directamente entre ambas estaciones o pasa por algún nodo intermedio?
- ¿Por qué Proxim confirma la trama a Cisco y no a Netgear?
- ¿Se indica de alguna forma que la comunicación se ha acabado?

Anexo I: Explicación de los campos de encabezado en una trama de Ethernet II.

El formato de una trama de Ethernet II se muestra en la Figura 1.

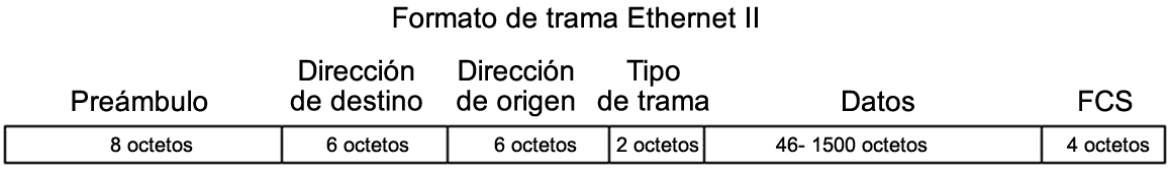


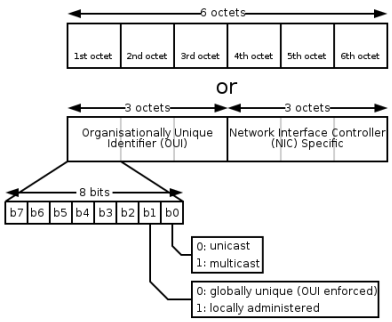
Figura 1. Formato de la trama de Ethernet II

La información que proporciona Wireshark acerca de esta trama es la siguiente:

Campo	Valor (ejemplo)	Descripción
Preámbulo	No se muestra en la captura.	Este campo contiene bits de sincronización, procesados por el hardware de NIC.
Dirección de destino	`ff:ff:ff:ff:ff:ff`	Direcciones de la Capa 2 para la trama. Cada dirección tiene una longitud de 48 bits, o 6 bytes, expresado como 12 dígitos hexadecimales, `0-9, A-F`. Un formato común es `12:34:56:78:9A:BC`. Véase abajo para más detalles.
Dirección de origen	`00:16:76:ac:a7:6a`	
Tipo de trama	`0x0806`	Para las tramas de Ethernet II, estos campos contienen un valor hexadecimal que se utiliza para indicar el tipo de protocolo de capa superior en el campo de datos. Existen muchos protocolos de capa superior admitidos por Ethernet II. Dos tipos comunes de trama son: Valor Descripción `0x0800` Protocolo IPv4 `0x0806` Address resolution protocol (ARP)
Datos	Datos ARP	Contiene el protocolo del nivel superior encapsulado. El campo de datos está entre 46 y 1500 bytes.
FCS	No se muestra en la captura.	Secuencia de verificación de trama, utilizada por la NIC para identificar errores durante la transmisión. El valor lo computa la máquina de envío, abarcando las direcciones de trama, campos de datos y tipo. El receptor lo verifica.

Anexo II: Direcciones MAC

Las direcciones MAC son 6 bytes (12 valores hexadecimales) que identifica (dirección de capa 2) a un equipo o grupo de equipos:



- Los primeros seis números hexadecimales (3 bytes) indican el fabricante de la tarjeta de interfaz de red (NIC). `https://macvendors.com/` permite obtener el fabricante a partir del código.
- Los últimos seis dígitos hexadecimales (3 bytes) representan el número de serie de NIC.
- Los dos últimos bits del primer byte son especiales.
- El último bit vale 0 si es una dirección *unicast* (dirección de un equipo concreto), mientras que es 1 si es una dirección *multicast* (dirección que se refiere a un grupo de equipos). En concreto, si la dirección está formada todo por 1 (`ff:ff:ff:ff:ff:ff`) se denomina dirección de *broadcast* (o difusión) y se refiere que quiere enviar a todos los equipos accesibles.
- El penúltimo bit es 0 si la dirección MAC es global o 1 si está localmente administrada.

Anexo III: Explicación de los campos de encabezado en una trama de Wifi.

El formato de una trama de Wifi se muestra en la Figura 2.

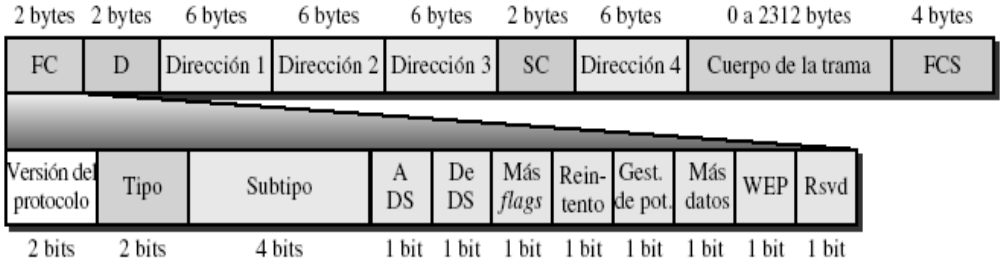


Figura 2. Formato de la trama de Wifi

La información que proporciona Wireshark acerca de esta trama es la siguiente:

Campo	**Descripción**
Frame Control (FC)	Información para gestionar la trama (versión, tipo…). Entre los campos incluye entre otros qué versión usa (0 para la actual), el tipo y subtipo que permiten identificar qué trama concreta estamos enviando (Beacon, CTS, RTS, Datos…), el "A DS" y "De DS" que indican si el origen o destino final están fuera de nuestro BSS o si hay más datos.
D	NAV o ID (para las tramas de control). Este tiempo se mide en microsegundos.
Direcciones	Direcciones MAC (atendiendo al tipo de tramas, puede omitir algunas). La primera trama siempre es el destino de la trama dentro del BSS y el segundo cuál es origen de la trama en nuestro BSS, mientras que el significado de la dirección tercera o cuarta depende de los bits "A DS" y "De DS" y el tipo/subtipo de trama
Sequence Control (SC)	Número de secuencia para el control de flujo/error.
FCS	Secuencia de verificación de trama, utilizada por la NIC para identificar errores durante la transmisión. No se captura por Wireshark ya que lo verifica directamente la tarjeta de red wifi.