## Práctica 1

**Apellidos:** Alcausa Luque

**Nombre:** Juan Carlos

**Titulación:** Grado de Ingeniería Informática + Matemáticas

**Grupo:** D

**PC de la práctica:** 510

**NOTA: Tiene más información en el enunciado de la práctica (especialmente en los anexos, con información sobre las cabeceras de las tramas Ethernet II y Wifi y sobre las direcciones MAC)**

**Ejercicios sobre la traza capturada en clase (p1.pcapng):**

**Ejercicio 1. Elija un mensaje icmp, y localice en la cabecera Ethernet II**[[1]](#footnote-1)la siguiente información:

Número de la trama analizada: 3002

Información de la dirección MAC de su computadora:

Dirección MAC (en hexadecimal): 7c:57:58:3a:e8:7b

Fabricante de NIC (en hexadecimal): 7c:57:58 nombre: HP

Número de serie de NIC (en hexadecimal): 3a:e8:7b

Información de la dirección MAC de *gateway/router*:

Dirección MAC (en hexadecimal): c4:b3:6a:0a:2e:75

Fabricante de NIC (en hexadecimal): c4:b3:6a nombre: Cisco

Número de serie de NIC (en hexadecimal): 0a:2e:75

**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? 6711
* ¿Por qué recibe esas tramas? (Para responder esta pregunta, observe las características de las direcciones MAC destino de esas tramas): Los paquetes que usan direcciones Broadcast se envían a todos los dispositivos

**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) **y las cabeceras trama enviada/recibida** (en la parte izquierda las cabeceras que se envía/reciben primero) de un paquete ARP, uno ICMP, uno DNS y uno HTTP[[2]](#footnote-2). Indique el número de la trama usado en cada caso.

* Protocolo ARP. Trama: 2913

Torre:

|  |
| --- |
| ARP |
| Ethernet II |
|  |
|  |

Cabeceras en la trama:

|  |  |  |  |
| --- | --- | --- | --- |
| ARP | Ethernet II |  |  |

* Protocolo ICMP. Trama: 3002

Torre:

|  |
| --- |
| ICMP |
| IPv4 |
| Ehernet II |
|  |

Cabeceras en la trama:

|  |  |  |  |
| --- | --- | --- | --- |
| ICMP | IPv4 | Ethernet II |  |

* Protocolo DNS. Trama: 505

Torre:

|  |
| --- |
| DNS |
| UDP |
| IPv4 |
| Ethernet II |

Cabeceras en la trama:

|  |  |  |  |
| --- | --- | --- | --- |
| DNS | UDP | IPv4 | Ethernet II |

* Protocolo HTTP. Trama: 1264

Torre:

|  |
| --- |
| HTTP |
| TCP |
| IPv4 |
| Ethernet II |

Cabeceras en la trama:

|  |  |  |  |
| --- | --- | --- | --- |
| HTTP | TCP | IPv4 | Ethernet II |

**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:

|  |  |
| --- | --- |
|  | Tipo en la cabecera Ethernet II (valor en hexadecimal y en texto) |
| ARP | ARP 0806 |
| HTTP | IPv4 0800 |
| ICMP | IPv4 0800 |
| DNS | IPv4 0800 |

* ¿Qué significa este campo? El protocolo que se usa en el nivel superior
* ¿Por qué en tramas diferentes es igual? Porque todos esos protocolos utilizan el mismo protocolo en el nivel superior en su torre de protocolos

**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.

* Tramas consultadas: 3002 y 3003
* ¿Cuánto tiempo es? 65,469611-65,469216= 0,00039499999
* ¿A qué concepto visto en la parte de teoría equivale dicho tiempo? Se refiere al rtt (tiempo que tarda en ir y volver un paquete

**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 Wireshark tendrá un tamaño de 60 bytes o más. Busque una trama con tamaño 60 (filtro: frame.len == 60),

* ¿cuántas tramas tienen esta característica? 3508
* ¿Qué mecanismo se utiliza para completar el tamaño si los datos transmitidos son más pequeños de 46 bytes (mínima cantidad de datos que hay que enviar en Ethernet)? Relleno / padding

**Pregunta extra/opcional (no entran en el parcial):** Observe que hay tramas con tamaño menor a 60 bytes (filtro: frame.len < 60), ¿por qué es eso posible? (Pista: analice cuáles son las direcciones MAC de origen). Puede que haya colisiones y al detectarse se detenga el envío de manera que no llegue a completarse.

**Ejercicios sobre la traza facilitada en el campus virtual (p1-wifi.pcapng):**

*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 y responda las siguientes preguntas:

* Número de trama elegido: 7
* ¿Qué tipo de trama (gestión, control o datos) es? ¿En qué campo se puede ver? Dentro del campo FC, el tercer y cuarto bit nos lo indican. En este caso es tipo 0 (Gestión) (Se pueden ver los tipos en la diapo. 80 del T2)
* ¿Cuál es el destino de la trama? ¿Por qué va a esa? Como A DS=0 y De DS=0, la dirección de destino es la primera de las dos que aparecen en nuestra cabecera
* Observe el BSS ID, ¿sabría decidir cómo se calcula el ID usado en cada BSS? 2c:f8:9b:dd:06:a0
* ¿Cuál es el SSID de la red wifi? HowIWiFi (Dentro de Wireless Management)
* 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: 2,4 GHz (En Radio Information)

*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? Control
* ¿Cómo se sabe si la trama es CTS o RTS? Porque lo pone en info (request-to-send/Clear-to-send)
* ¿Cuánto vale el NAV en estas tramas? 178 microsegundos (El campo justo después del FC)
* ¿Por qué la trama CTS ocupa 6 bytes menos que la RTS? RTS incluye 2 bytes con la duración del NAV??

**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? Las QoS son de datos y las ACK de control
* 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)? Las QoS tiene A DS=0 y De DS=1. NetGear y Proxim no están en la misma BSS ya que al enviar un QoS NetGear a Proxim tiene De DS=1. Cisco y Proxim están en la misma BSS ya que en una RTS (146) tiene ambas flags a 0.
* ¿Explica lo anterior por qué no se observan en la traza los RTS/CTS asociados con Netgear? Sí, ya que los RTS/CTS los envían al AP únicamente, no llega a retransmitirse por WiFi
* ¿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? La trama de origen es Netgear y la destino Proxim. Como están en BSS distintos pasan por el AP y por un sistema de distribución.
* ¿Por qué Proxim confirma la trama a Cisco y no a Netgear? Porque Cisco es el que le transmite la trama a Proxim (aunque originalmente venga de Netgear, el último nodo que se la transmite es Cisco)
* ¿Se indica de alguna forma que la comunicación se ha acabado? Creo que no

1. 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). [↑](#footnote-ref-1)
2. Como protocolo Wireshark debe mostrar http y no TLSvX [↑](#footnote-ref-2)