• Práctica 1

Apellidos: Ponce Arrocha
Nombre: Santiago

Titulación: Grado de Ingeniería Informática
Grupo: A

PC de la práctica: PC Personal

Ejercicio 1. Elija un mensaje `icmp`, y localice en la cabecera Ethernet II la siguiente información:

Número de la trama analizada: 52491
Información de la dirección MAC de su computadora:
Dirección MAC (en hexadecimal): 04:d9:f5:84:48:90
Fabricante de NIC (en hexadecimal): 04:d9:f5 nombre: ASUSTekC
Número de serie de NIC (en hexadecimal): 84:48:90

Información de la dirección MAC de *gateway/router*:
Dirección MAC (en hexadecimal): 48:8d:36:d1:08:9b
Fabricante de NIC (en hexadecimal): 48:8d:36 nombre: Arcadyan
Número de serie de NIC (en hexadecimal): d1:08:9b

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).

eth.src ne 04:d9:f5:84:48:90 && eth.dst ne 04:d9:f5:84:48:90

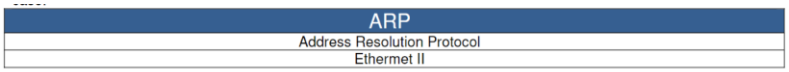
o

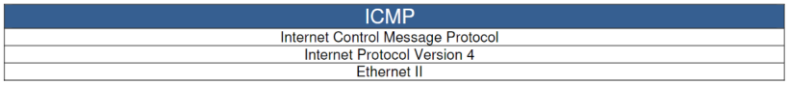
eth.src != 04:d9:f5:84:48:90 && eth.dst != 04:d9:f5:84:48:90

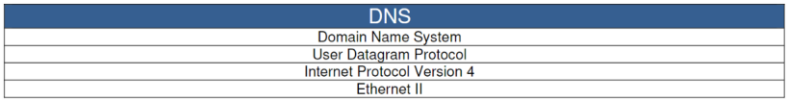
- ¿Cuántas tramas recibe?
  210 de 104693

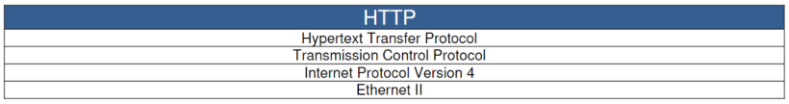
- ¿Por qué recibe esas tramas? (Para responder esta pregunta, observe las características de las direcciones MAC destino de esas tramas)
  Porque son tramas (de difusión) de tipo destino broadcast (ff:ff:ff:ff:ff:ff) o IPv4mcast (01:00:5e:7f:ff:fa)

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. Indique el número de la trama usado en cada caso.









- Torre ARP. Trama: 11907
- Torre ICMP. Trama: 52491
- Torre DNS. Trama: 94519
- Torre HTTP. Trama: 62188

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?

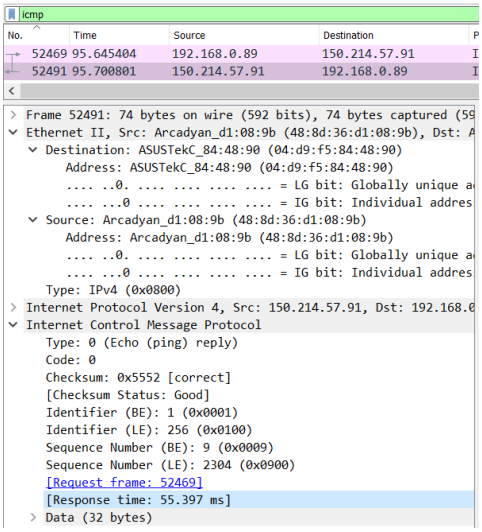
  Se encarga de permitir que un dispositivo conectado a una red pueda obtener una ruta MAC de otro equipo que está conectado a esa misma red, es decir, se encarga de «localizar» donde están los demás dispositivos cableados o inalámbricos en la red, preguntando por la dirección MAC de cada uno de ellos enviando un paquete a la dirección de broadcast que es FF:FF:FF:FF:FF:FF.

- ¿Por qué en tramas diferentes es igual?

  ARP / IPv4 son protocolos de resolución de direcciones. Puede haber distintas tramas que lo transmitan.

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: 52469 - 52491
- ¿Cuánto tiempo es?



- ¿A qué concepto visto en la parte de teoría equivale dicho tiempo?

  RTT (Round Trip Time) : tiempo que tarda un paquete de datos en ir y volver a su emisor habiendo pasado por su destino.

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?
  573

- ¿Qué mecanismo se utiliza para completar el tamaño si los datos transmitidos son más pequeños de 46 bytes)?
  Padding

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: 1
- ¿Qué tipo de trama (gestión, control o datos) es? ¿En qué campo se puede ver?
  Tipo 0 (gestión). Se puede ver en el campo de “Frame Control Field”.

- ¿Cuál es el destino de la trama? ¿Por qué va a esa?
  Broadcast, una conexión multipunto en redes IP que permite llegar de forma automática a todos los usuarios de una red sin la necesidad de conocer las respectivas direcciones de destino.

- Observe el BSS ID, ¿sabría decidir cómo se calcula el ID usado en cada BSS?
  Se calcula en base a la dirección MAC de la fuente.

- ¿Cuál es el SSID de la red wifi?
  “HowIWifi”
- 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
  802.11 radio information (frequency), que está a 2.4 GHz

Ejercicio 8. Sobre las tramas CTS y RTS:

- ¿Qué tipo de trama (gestión, control o datos) es?
  CTS: Control
  RTS: Control

- ¿Cómo se sabe si la trama es CTS o RTS?
  Se puede observar aquí.

```
IEEE 802.11 Request-to-send, Flags: ........C
    Type/Subtype: Request-to-send (0x001b)
  Frame Control Field: 0xb400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1011 .... = Subtype: 11
    Flags: 0x00
```

- ¿Cuánto vale el NAV en estas tramas?
  RTS: 178 microsegundos
  CTS: 120 microsegundos

- ¿Por qué la trama CTS ocupa 6 bytes menos que la RTS?
  Porque CTS no tiene fuente.

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?
  QoS: Datos (data frame – 2)
  ACK: Control (control frame – 1)

- 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)?
  NetGear no se encuentra en la misma red, mientras que los otros dos sí.

- ¿Explica lo anterior por qué no se observan en la traza los RTS/CTS asociados con Netgear?
  Si, como netgear esta es una red diferente, no podemos captar las tramas de control, mientras que Cisco y Proxim entre ellos se pueden escuchar, puesto que se encuentran en la misma red.

- ¿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?
  STA: NetGear / estación final: Proxim / pasa por el nodo Cisco

- ¿Por qué Proxim confirma la trama a Cisco y no a Netgear?
  Porque Cisco es el nodo dentro de toda la red que puede recibir las tramas de fuera (de NetGear). Por tanto, una vez Cisco recibe la trama de NetGear, Cisco se la envía a Proxim y una vez le llega, confirma la recepción a Cisco.

- ¿Se indica de alguna forma que la comunicación se ha acabado?
  Por la trama “block ack”, que confirma la recepción de la trama por parte de Proxim.