PRÁCTICA 1

ESCENARIO 1 (p1.pcapng)

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

Número de la trama analizada: 4467

Información de la dirección MAC de su computadora:

Dirección MAC (en hexadecimal): 64:5d:86:51:7c:fa
Fabricante de NIC (en hexadecimal): 64:5d:86 nombre: IntelCor
Número de serie de NIC (en hexadecimal): 51:7c:fa

Información de la dirección MAC de gateway/router:

Dirección MAC (en hexadecimal): 60:8d:26:fd:9b:a8
Fabricante de NIC (en hexadecimal): 60:8d:26 nombre: Arcadyan
Número de serie de NIC (en hexadecimal): fd:9b:a8

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 == 64:5d:86:51:7c:fa) && !(eth.dst == 64:5d:86:51:7c:fa)
eth.src ne 64:5d:86:51:7c:fa and eth.dst ne 64:5d:86:51:7c:fa

- ¿Cuántas tramas recibe? 1021 de 38376
- ¿Por qué recibe esas tramas? (Para responder esta pregunta, observe las características de las direcciones MAC destino de esas tramas) Porque son tramas de tipo destino broadcast (ff:ff:ff:ff:ff:ff) y tipo IPv4mcast_01 (01:00:5e:00:00:fb)

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: 4354

Address Resolution Protocol(ARP)
Ethernet II

- Torre ICMP. Trama: 4467

Internet Control Message Protocol(ICMP)
Internet Protocol Version 4
Ethernet II

- Torre DNS. Trama: 734

Domain Name System(DNS)
User Datagram Protocol

Internet Protocol Version 4
Ethernet II

- Torre HTTP. Trama: 5009

Hypertext Transfer Protocol(HTTP)
Transmission Control Protocol
Internet Protocol Version 4
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: Type: ARP (0x0806)
HTTP: Type: IPv4 (0x0800)
ICMP: Type: IPv4 (0x0800)
DNS: Type: IPv4 (0x0800)

- ¿Qué significa este campo? El campo type significa el tipo del protocolo por el que se transmiten los datos.
- ¿Por qué en tramas diferentes es igual? En tramas diferentes es igual ya que aunque el tipo de datos a transmitir es diferente, estos se transmiten de la misma manera.

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: 4467 y 4468
- ¿Cuánto tiempo es? 73.993211-73.932203 = 0,061008
- ¿A qué concepto visto en la parte de teoría equivale dicho tiempo? Este tiempo se asocia al Round Trip Time (RTT) ya que el tiempo de request es el tiempo de ida del mensaje hacia el receptor (yo envío) y el de reply (yo recibo) el tiempo de respuesta de este.

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? 551 de 38376

- ¿Qué mecanismo se utiliza para completar el tamaño si los datos transmitidos son más pequeños de 46 bytes? El mecanismo que utilizan para rellenar este campo es el Padding el cual lo rellenan con ceros hasta llegar al mínimo

ESCENARIO 2 (p1-wifi.pcapng)

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? Type: Management frame (trama de gestión)

¿En qué campo se puede ver? IEEE 802.11 Beacon frame→ Frame Control Field → ....00.. = Type : Management frame (0)

- ¿Cuál es el destino de la trama? ¿Por qué va a esa? El destino es Broadcast, ya que como es una trama de gestión esta se pasa como general (broadcast o mk) y para que todo el que esté conectado a la wifi pueda recibir dicho paquete.
- Observe el BSS ID, ¿sabría decidir cómo se calcula el ID usado en cada BSS? Se calcula mirando el Transmitter address, que normalmente se corresponde con la MAC del source.
- ¿Cuál es el SSID de la red wifi? Tag: SSID parameter set: "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. Channel: 1 Frequency: 2412MHz = 2.4GHz

Ejercicio 8. Sobre las tramas CTS y RTS:

- ¿Qué tipo de trama (gestión, control o datos) es? Ambas son Type: Control frame
- ¿Cómo se sabe si la trama es CTS o RTS? Mirando en IEEE 802.11 tendremos Request-to-send (RTS) o en otros casos aparecerá Clear-to-send (CTS)
- ¿Cuánto vale el NAV en estas tramas? RTS → Duration: 178 microseconds
CTS →Duration: 120 microseconds
- ¿Por qué la trama CTS ocupa 6 bytes menos que la RTS? Porque esta no contiene el Transmitter address ya que el CTS al ser la confirmación de que puede recibir el receptor no necesita tener este campo para saber el MAC de a quien le envía.

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 Data es una trama de datos. Block ACK es una trama 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)? QoS Data → (To DS: 0 From DS: 1)
ACK → (To DS: 0 From DS: 0)
Cisco y Proxim están en la misma red ya que tienen el mismo valor en la DS, mientras que Netgear no.
- ¿Explica lo anterior por qué no se observan en la traza los RTS/CTS asociados con Netgear? No se observan las trazas RTS y CTS de Netgear ya que solo estamos observando lo que está pasando en el BSS dónde están Proxim y Cisco y como Netgear está en otro BSS pues no podemos observar dichas trazas.
- ¿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 estación origen es Netgear ya que es la source, la final es proxim y la intermedia que sería el punto de acceso es Cisco que es el transmitter address.

- ¿Por qué Proxim confirma la trama a Cisco y no a Netgear? Porque Proxim y Cisco se encuentran en el mismo BSS y Netgear se encuentran en en un BSS distinto al de Proxim, por lo que este no puede confirmar nada a Netgear.
- ¿Se indica de alguna forma que la comunicación se ha acabado? Por la duración de la NAV , que tendría una duración de 0 o despreciable, lo cual nos indica que la transmisión se ha realizado con éxito.