## Práctica 2

**Apellidos:** Alcausa Luque

**Nombre:** Juan Carlos

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

**Grupo: D**

**PC de la práctica:** portátil

**Lea el enunciado de la práctica para saber cómo generar el tráfico de cada ejercicio.**

**Ejercicio 1.** Observe la cabecera IP de los diferentes datagramas:

* ¿Qué protocolo se indica en el campo “protocolo” en la cabecera de los datagramas que transportan mensajes DNS, ICMP, DHCP y HTTP?

|  |  |  |  |
| --- | --- | --- | --- |
| Protocolo | Valor Campo protocolo  (texto) | Valor Campo protocolo (HEX) | Número de trama |
| ICMP | ICMP | 01 | 17121 |
| HTTP | TCP | 06 | 15944 |
| DNS | UDP | 11 | 15935 |
| DHCP | UDP | 11 | 4 |

* ¿Qué indica este campo? El protocolo del nivel inmediatamente superior a IP al que debe entregar el paquete
* ¿Por qué este campo tiene el mismo valor si el protocolo de aplicación es diferente? Porque indica el protocolo a nivel de transporte (puede ser igual para distintos protocolos a nivel de aplicación)

Ejercicio 2. Seleccione una petición de ICMP de su equipo (el mensaje *Echo Request*) y complete la siguiente tabla indicando la dirección IP destino (en la cabecera IP) y la dirección MAC destino (en la cabecera Ethernet). Repita el proceso con una petición DNS (en la *Info* pone *Stardard Query 0x…*).

|  |  |  |
| --- | --- | --- |
|  | ICMP | DNS |
| Dirección IP destino (cab IP) | 150.214.57.91 | 150.214.40.12 |
| Dirección MAC destino (cab Ethernet) | 00:ee:ab:4f:2e:6e | 00:ee:ab:4f:2e:6e |
| Número de trama | 17121 | 17043 |

* ¿Por qué las direcciones MAC destino son iguales pero las direcciones IP destino no? Porque la dirección MAC va variando en cada salto, puede que en ese momento ambos paquetes sean entregados a un mismo router por ejemplo para después ser enviado por caminos distintos hasta alcanzar cada uno su destino, pero la dirección IP indica el destino final del paquete.

**Ejercicio 3.** Responda las siguientes preguntas:

Para poder encontrar los fragmentos tenemos que buscar el identificador que nos sale en Ip y aplicarlo como filtro. En nuestro caso el MTU es de 1500 por lo que el de 1300 no debe fragmentarse y el de 3200 fragmentarse en 3.

(ping -l 1300 -n 1 www.informatica.uma.es)

* ¿Cuál es el tipo de mensaje ICMP y su código (tanto para las peticiones como las respuestas)? Request tiene código 8 y Reply código 0 (Se ve dentro de la cabecera ICMP)

Para el resto de preguntas y rellena la tabla considere solo las peticiones (request)

* ¿Qué filtro podría poner para que sólo aparezcan los fragmentos relacionados con un datagrama concreto? Un filtro con el identificador del datagrama: ip.id == 0x384f para el primero de 1300 (no se fragmenta) y ip.id == 0x3850 para el segundo de 3400 que se fragmenta en tres fragmentos
* Completa la siguiente tabla, indicando los flags que tiene activo cada fragmento, su identificador y su desplazamiento (para cada tamaño escribe un valor por cada fragmento, separados por comas (,) cuando hay varios fragmentos) Los desplazamientos tienen 13 bits y se aparecen en binario en Wireshark, interpretado en decimal a la derecha (NO mirar los numeritos resaltados en azul a la derecha ya que esos incluyen más datos además del offset)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tamaño | Número de tramas | Identificadores | Flags | Desplazamientos |
| 1300 | 4 | 0x384f | 000 | 0 |
| 3400 | 191,192,193 | 0x3850 | 001, 001, 000 | 0, 1480, 2960 |

**Ejercicio 4.** Realice dos pings a **www.informatica.uma.es** con tamaños MAX y MAX+1 y el bit DF activo (MAX es el tamaño máximo calculado). Añada una captura de pantalla del terminal.

* ¿Cuál es el valor máximo? 1472
* ¿Por qué es ese tamaño? 1500 de MTU menos la cabecera que son 20 bytes serían 1480 pero he ido probando y el máximo que me deja enviar es 1472. Debe haber algún nodo intermedio con un MTU de 1492
* ¿En la traza de Wireshark aparece el primer ping? ¿Y el segundo? ¿Por qué? El primer ping sí que aparece pero el segundo no

**Ejercicio 5.** El uso de -r X cambia la cabecera en dos aspectos: añade el campo opciones de tamaño apropiado dependiente de X y por lo tanto cambia el campo HLEN.

* ¿Cómo aumenta el tamaño de HLEN según X? Si x=1 la cabecera aumenta a 28 bytes, si x=3 la cabecera aumenta a 36 y si x=9 la cabecera pasa a 60 bytes
* Si prueba otros valores X, verá que solo permite valores entre 1 y 9, ¿Por qué cree que solo permite esos valores y no mayores? Porque tenemos un tamaño máximo para la cabecera de un datagrama IP de 60 bytes
* Finalmente observe que además de la opción IP “Record Route” se incorpora la opción “End of Options List” para indicar que ya no hay más opciones, ¿por qué es necesaria añadir esta opción y no nos vale solo con el HLEN? Es necesario añadirlo si el final de las opciones no coincide con el final de la cabecera (la cabecera debe tener un tamaño fijo expresado en palabras de 4 bytes)

**Ejercicio 6.** Localiza y observa un paquete de respuesta y presta atención al campo TTL.

* ¿Cuánto vale? 128 en la salida (no hay respuesta)
* Compárelo con el TTL del mensaje de petición. ¿Quién establece cada valor?

**Ejercicio 7.** Haga un ping a **www.informatica.uma.es** usando un TTL creciente, empezando por 1 y deteniéndose cuando se empiece a recibir una respuesta del servidor. Observe en Wireshark el intercambio de paquetes que se produce.

* Número de trama analizada: filtrar con icmp
* ¿Qué mensaje ICMP se recibe cuando los paquetes no llegan (tipo, código y significado tiene dicho mensaje)? Time to live exceeded in transit, de tipo 11con código 0
* ¿Qué incluye dicho mensaje ICMP como información adicional? Información sobre el request que se ha hecho, incluyendo parte de la cabecera de IPv4 que llevaba el ping original.

**Ejercicio 8.** Responda a las siguientes preguntas:

* Indique el número de las tramas utilizadas para responder estas preguntas
* ¿Qué tipo de paquetes (protocolo de más alto nivel) usa **tracert** para hacer su función? ICMP
* Además de los mensajes propios para obtener el camino, **tracert** puede provocar que se realicen otros envíos auxiliares para conseguir información o mostrar de forma más amistosa la información, ¿qué otros mensajes pueden ser necesarios? Aparecen mensajes ARP cerca
* ¿Qué estrategia usa **tracert** para averiguar qué máquina hay en cada salto del paquete? va enviando distintos mensajes con un TTL creciente hasta llegar al destino