* **Práctica 2**

**Apellidos:** Ruiz Pareja

**Nombre:** José

**Titulación:** Grado de XXXX

**Grupo:** X

**PC de la práctica:** 012

**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(1) | 1 | 2334 |
| HTTP | TCP(6) | 6 | 247 |
| DNS | UDP(17) | 11 | 2332 |
| DHCP | UDP(17) | 11 | 2845 |



* ¿Qué indica este campo?

El protocolo que va a ser usado en la capa superior

* ¿Por qué este campo tiene el mismo valor si el protocolo de aplicación es diferente?

Porque todo los mensajes son mandados desde el mismo dispositivo, sin embargo dependiendo del tipo de mensaje que sea utilizara un protocolo u otro.

**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 | 150.214.40.11 |
| Dirección MAC destino (cab Ethernet) | c4:b3:6a:0a:2e:75 | c4:b3:6a:0a:2e:75 |
| Número de trama | 2334 | 2332 |



* ¿Por qué las direcciones MAC destino son iguales pero las direcciones IP destino no?

La direccion MAC se refiere a la direccion fisica, es decir, al siguiente nodo que tiene que ir para realizar el envio. El siguiente nodo es el mismo, mientras que la direccion IP varia al enviar a dispositivos distintos.

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

* ¿Cuál es el tipo de mensaje ICMP y su código (tanto para las peticiones como las respuestas)?





Para el resto de preguntas y rellena la tabla considere solo las peticiones.

* ¿Qué filtro podría poner para que sólo aparezcan los fragmentos relacionados con un datagrama concreto?

frame.number ==

* 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).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tamaño | Número de tramas | Identificadores | Flags | Desplazamientos |
| 1300 | 1 | 61885 | 000 | 0 |
| 3400 | 3 | 24949 | 001  001  000 | 0  1480  2960 |

**Ejercicio 4.** Realice dos pings a [**www.informatica.uma.es**](http://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? 1473
* ¿Por qué es ese tamaño?

Porque es el tamaño maximo que puede ocupar un paquete sin fragmentar la red

* ¿En la traza de Wireshark aparece el primer ping? ¿Y el segundo? ¿Por qué?

En la traza del wireshark aparece el ping de 1464, mientras que el de 1465 no, pues

es mayor que el valor de la MTU y no se puede enviar el paquete en la red.

**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?

Se añadiran tantas opciones como X indique(tam 4)

**(HLEN +rx+1)\*4 = tamaño cabecera**

* 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?

Para un X mayor a 9 se pasa de 60 que es el tope

* 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?

En el HLEN no se indica en ningun sitio donde acaban las opciones de cabecera, ahi que se necesite esta opción.

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



* ¿Cuánto vale?

63

* Compárelo con el TTL del mensaje de petición. ¿Quién establece cada valor?

128, no lo se

**Ejercicio 7.** Haga un ping a [**www.informatica.uma.es**](http://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

1785

* ¿Qué mensaje ICMP se recibe cuando los paquetes no llegan (tipo, código y significado tiene dicho mensaje)?

Tipo 11(Time-to-live exceeded), codigo 0(Time to live exceeded in transit), que el TTL es muy pequeño

* ¿Qué incluye dicho mensaje ICMP como información adicional?

Devuelve el TTL inicial y una copia del mensaje que se estaba enviando

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



* Indique el número de las tramas utilizadas para responder estas preguntas

689 y 690

* ¿Qué tipo de paquetes (protocolo de más alto nivel) usa **tracert** para hacer su función?

ICMP(1)

* 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?

DNS

* ¿Qué estrategia usa **tracert** para averiguar qué máquina hay en cada salto del paquete?

Envía paquetes cuyo tiempo de vida va aumentando progresivamente, hasta que llegue

un punto en el que alcanza el máximo o llega a su destino. Cuando al mensaje se le agota

dicho TTL, el nodo en el que ha “muerto” se encarga de comunicar que el tiempo de vida

del mensaje ha expirado. Así, se registran los nodos por los que ha pasado el mensaje y

se conoce el camino que el paquete debe seguir.