PRÁCTICA 2

TAREA 1: Encapsulamiento en IP (p2e1-2.pcapng)

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? Rellene la tabla con dicha información. ¿Qué indica este campo? ¿Por qué este campo tiene el mismo valor si el protocolo de aplicación es diferente?

Protocolo	Valor Campo protocolo (texto)	Valor Campo protocolo (HEX)	Número de trama
ICMP	Protocol: ICMP (1)	01	626
HTTP	Protocol: TCP (6)	06	595
DNS	Protocol: UDP (17)	11	458
DHCP	Protocol: UDP (17)	11	13750

En tramas diferentes es igual ya que aunque el tipo de datos a transmitir es diferente, estos se transmiten de la misma manera.

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 Standard query 0x…). ¿Por qué las direcciones MAC destino son iguales pero las direcciones IP destino no?

	ICMP	DNS
Dirección IP destino (cabecera IP)	150.214.57.91	150.214.40.11
Dirección MAC destino (cabecera Ethernet)	c4:b3:6a:0a:2e:75	c4:b3:6a:0a:2e:75
Número de trama	626	458

La dirección MAC es la dirección física del dispositivo y por eso no cambia, mientras que la dirección IP cambia dependiendo del protocolo, por eso es distinta.

TAREA 2: Fragmentación en IP (p2e3.pcapng, p2e4.pcapng.)

Ejercicio 3. ¿Cuál es el tipo de mensaje ICMP y su código (tanto para las peticiones como las respuestas)? Para las peticiones son de Type 8 con código 0. Para las respuestas son de Type 0 con código 0.
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?
Ip.id==identificador

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	Numero de trama	Identificadores	Flags	Desplazamiento
1300	542	0xce2f (52783)	0x00	0
3400	35117	0xce36 (52790)	0x0	2960

Ejercicio 4. Calcule el tamaño máximo de datos (MAX) que puede llevar un ping en la red del laboratorio. 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). ¿Cuál es el valor máximo? ¿Por qué es ese tamaño? Guarde la traza como p2e4.pcapng.

Para calcular ese número tenemos que coger el valor máximo de la MTU que es 1500 bytes y le tenemos que restar 20 bytes de la cabecera del protocolo IP y 8 bytes de la cabecera de ICMP: 1500-20-8 = 1472

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

El primero sí aparece puesto que al hacer ping fue enviado y correctamente recibido.
En cambio, el segundo no porque si observamos la terminal, aparece que se pierde el paquete ya que no se puede fragmentar y no puede mandar todos sus bytes.

TAREA 3: Cabecera en IP (p2e5-6.pcapng)

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 prueba otros valores X, verá que solo permite valores entre 1 y 9, ¿Por qué cree que solo permite esos valores y no mayores?

-r 1 Total Length: 68 -r 3 Total Length: 76 -r 9 Total Length: 100

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?

End of Option List (Fin de lista de opciones). Indica el final de la lista de opciones. Se utiliza al final en la última opción, no al final de cada opción individualmente. Sólo se debe utilizar esta opción si, de otra forma, el final de las opciones no va a coincidir con el final de la cabecera IP. El fin de lista de opciones se utiliza si las opciones exceden la longitud del datagrama.

Ejercicio 6. Localiza y observa un paquete de respuesta y presta atención al campo TTL. ¿Cuánto vale? Compárelo con el TTL del mensaje de petición. ¿Quién establece cada valor?

Trama: 569
Valor TTL (Time To Live): 51
Trama: 567
Valor TTL (Time To Live): 128
Cada registro DNS de tu dominio establece el TTL.

TAREA 4: Mensajes de error ICMP

Ejercicio 7. Haga varios pings a www.informatica.uma.es usando un TTL creciente, empezando por 1 y deteniéndose cuando se empiece a recibir una respuesta correcta del servidor. Pruebe con los siguientes valores (pare cuando responda de forma adecuada): 1, 2, 3,… Observe en Wireshark el intercambio de paquetes que se produce. ¿Qué mensaje ICMP se recibe cuando los paquetes no llegan (tipo, código y significado tiene dicho mensaje)?

Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)

¿Qué incluye dicho mensaje ICMP como información adicional (dentro del campo de datos)? Time to Live: 1

TAREA 5: Comando tracert

Ejercicio 8. ¿Qué tipo de paquetes (protocolo de más alto nivel) usa tracert para hacer su función? Los de tipo 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? Podría ser necesario algunos de tipo DNS, ya que traduce las direcciones IP a las URL que les corresponde.

¿Qué estrategia usa tracert para averiguar qué máquina hay en cada salto del paquete?
Según las diferentes tablas de encaminamiento de router a router se envían ICMP hasta que llega al destino determinado. Las tramas en negro devuelven la IP de los nodos

intercambiados y las tramas DNS las IPs dedestino de los nodos intermedios, así es como se ve todos los pasos que hace.