1. **Introducción.**

En esta tarea vamos a analizar el comportamiento del protocolo ICMP en mayor detalle. Para ello, estudiaremos una traza de los segmentos ICMP enviados y recibidos al ejecutar varios programas distintos. El objetivo es familiarizarse con los principales campos de la cabecera de los paquetes ICMP, así como con algunos de los tipos de paquetes ICMP que se utilizan de forma más frecuente.

Durante todo el desarrollo de la tarea emplearemos Wireshark con el filtro “icmp” activado.

2. **Paquetes *echo request* y *echo reply*.**

En primer lugar, analizaremos los paquetes generados mediante el programa *ping*. Se trata de un programa muy sencillo que permite verificar si un determinado host está conectado a la red. Mediante este programa, el host origen envía un paquete *echo request* al host destino y éste responde a su vez mediante otro paquete *echo reply* tan pronto como le sea posible. Los dos paquetes intercambiados son ICMP.

Utilizando el programa *ping* (en Windows o en Linux), envía 1 paquete a un host destino cualquiera y captura tanto las solicitudes como las respuestas mediante el programa *Wireshark*.

a) ¿Cuál es la dirección IP de tu host? ¿Cuál es la dirección IP del host destino?

b) ¿Por qué los paquetes ICMP no tienen ni puerto de origen ni de destino?

c) Examina una de las solicitudes de *ping* enviadas por tu host. ¿Cuáles son los valores del campo *type* y del campo *code*?

d) A continuación, examina una de las respuestas recibidas por tu host. ¿Cuáles son los valores del campo *type* y del campo *code*? ¿Cuál parece ser el uso de los campos *identifier* y *sequence* en vista de ambos mensajes de solicitud y respuesta?

3. **Paquetes relacionados con el rechazo de conexiones.**

El protocolo ICMP se utiliza también para llevar a cabo la notificación de que no ha sido posible entregar un mensaje al destinatario. Por ejemplo, en el caso en el que se haya establecido una regla de cortafuegos que impida el tráfico de un determinado protocolo, el equipo que actúa de cortafuegos (o que tiene instalado un programa de este tipo) puede decidir notificar al host emisor que dicho tráfico no está permitido. Para capturar este tipo de paquetes ICMP usaremos la orden *nc* para intentar establecer conexiones con puertos que generen esa respuesta, en este caso usando el protocolo UDP.

Desde la línea de comandos de Ubuntu debes ejecutar los tres comandos que os ponemos a continuación y en ese orden. **Os aconsejamos que las ejecutéis desde una máquina de la facultad, o en su defecto, desde EVA**, ya que debido a las diferentes configuraciones de los routers de vuestros domicilios, los de vuestros proveedores de Internet y los de las redes destino, **podría ser que las órdenes no tuvieran la respuesta esperada**, por ejemplo, quedándose bloqueadas y no apareciera respuesta en la captura. En el caso de que tuvierais dificultades para trabajar desde EVA

o la facultad, y se os diera el problema, os hemos adjuntado una captura en formato .pcap donde podréis encontrar ejemplos de respuestas ICMP y podéis usarla para responder a las cuestiones. Las órdenes son las siguientes:

```
$ echo "CADENA1" | nc -4 -u 155.54.1.1 666

$ echo "CADENA2" | nc -4 -t ditec.um.es 666

$ echo "CADENA3" | nc -4 -u localhost 666
```

Captura todo el tráfico ICMP que se genera mediante el programa *Wireshark*, y contesta para cada caso:

e) ¿Cuál es la dirección IP de tu host? ¿Cuál es la dirección IP del host destino?

f) ¿Qué protocolo de transporte se está utilizando para intentar establecer la conexión con el host destino en cada caso?

g) Examina el paquete ICMP devuelto por el host destino. ¿Cuáles son los valores del campo *type* y del campo *code*?

h) ¿Qué otra información contiene ese paquete ICMP? ¿A qué corresponde dicha información?

4. **Paquetes relacionados con el tiempo de vida**

La orden `traceroute` hace un uso ingenioso de los mensajes *ICMP* a la hora de averiguar los *routers* por los que ha ido pasando un paquete en su camino hacia el destino: va enviando paquetes en los que, partiendo de un TTL=1, sucesivamente se incrementa dicho campo para ir provocando una respuesta *Time-to-live exceeded* desde los correspondientes *routers* que se van atravesando camino de dicho destino, dando cada vez un salto más a través de los *routers* mencionados.

Usa la orden `traceroute -N 1 -q 1 cualquiermaquina.dominio.com` [1] para capturar el tráfico ICMP generado como respuesta y responde a las siguientes preguntas:

i) ¿Cuál es la dirección IP del router que responde?

j) ¿Qué protocolo se está utilizando para mandar mensajes al host destino?

k) Examina el paquete ICMP devuelto por el router. ¿Cuáles son los valores del campo *type* y del campo *code*?

l) ¿Qué otra información contiene ese paquete ICMP? ¿A qué corresponde dicha información?

1 El nombre de la máquina es el que queráis, por ejemplo, las webs de diarios como El Mundo (www.elmundo.es) o El País (www.elpais.com) suelen funcionar bien.