PL3: Wireshark ICMP y DHCP en IPv4

Nombres: Carlos Javier Hellín Asensio y Marcel Andrei Voicui **Puesto:** 7 y 8 **Grupo:** GII Tarde

OBJETIVOS.

El objetivo de esta práctica es comprender el funcionamiento de los protocolos ICMP y DHCP. Para ello emplearemos el analizador de protocolos Wireshark, ya conocido por los alumnos, junto con algunas órdenes que ayudaran a comprender el funcionamiento de ambos protocolos.

EJERCICIO 1, ICMP

Ejecute Wireshark (`$sudo wireshark`) y configúrelo para capturar tráfico en el interfaz de red de área local. Puede determinar cuál es su interfaz de red ejecutando la orden `ifconfig` y comprobando qué interfaz tiene la dirección IP de la etiqueta[1] puesta en la torre del PC. Envíe un comando `ping` a un PC situado en su misma red de área local. Elija, en este caso, el PC físicamente más próximo a su puesto de laboratorio[1] y haga un ping a dicho equipo.

```
$ ping x.x.x.x
```

Cuando se complete la ejecución de la orden, detenga Wireshark, filtre el tráfico ICMP (filtro ICMP) que tenga como origen o destino su equipo y localice las tramas que corresponden a los mensajes ICMP generados por el `ping`. Responda a las siguientes cuestiones:

1.1. ¿Cuáles son las direcciones IP origen y destino de las tramas ICMP que observa?

El origen es nuestro PC, en este caso 10.0.12.7, y el destino el 10.0.12.8

1.2. Identifique los distintos tipos de mensajes ICMP que se producen con su tipo y código.

Los dos distintos tipos de mensajes ICMP que se producen son:

Tipo 8 y código 0 que su descripción es echo request (petición de echo)

Tipo 0 y código 0 que su descripción es echo reply (respuesta de echo)

1.3. ¿Qué otros campos interesantes aparecen en este paquete ICMP? ¿Cuál es la utilidad de estos campos?

Tenemos los timestamp, que nos indican la fecha y hora de envío del paquete y nos sirve para conocer el tiempo necesitado para enviar el paquete. El checksum, que nos informa si el paquete ha llegado sin errores. Una identificación y números de secuencia que son usados por el cliente para ser asociados a cada Echo request y a cada Echo reply.

[1] Observe que cada PC tiene una etiqueta con la dirección IP que tiene asignada.

Aumente el tamaño del mensaje que emplea el `ping` del apartado anterior hasta 2000 bytes (en Linux hay que usar la opción –s, ping –s 2000 x.x.x.x)

1.4. ¿Cuántos paquetes IP recibe como respuesta por cada mensaje ICMP original?

Se reciben dos paquetes IP por cada mensaje ICMP a causa de la fragmentación.

1.5. ¿Cuál es el tamaño de cada uno?

El primer paquete es de protocolo IPv4 y envía 1480 bytes de datos, añadiéndole 20 de la cabecera IP y otros 14 de la cabecera ethernet, sumando en total 1514 bytes. El segundo paquete es ICMP, contiene los 520 bytes restantes, junto a los 8 bytes de datos del protocolo ICMP, los 20 bytes de la cabecera IP y los 14 de la cabecera ethernet, sumando en total 562.

1.6. ¿Puede explicar qué está ocurriendo?

El MTU de la red es 1500 por lo que debe fragmentar el mensaje ICMP.

EJERCICIO 2

Realizamos ahora un ping a una dirección web siguiendo las mismas instrucciones de captura que en el ejercicio anterior:

```
$ ping www.rediris.es
```

Responda a las siguientes preguntas:

2.1. ¿Cuáles son las direcciones IP origen y destino del tráfico ICMP?, ¿son direcciones IP públicas o privadas?

Nuestra dirección 10.0.12.7 es el origen y el destino es la web con dirección 120.206.13.20. La dirección 10.0.12.7 es privada ya que pertenece al rango de IP privadas de clase A (10.0.0.0 a 10.255.255.255) de la LAN del laboratorio y la dirección 120.206.13.20 es pública porque pertenece al rango de las IP públicas de clase A (1.0.0.0 a 126.255.255.255) del servidor www.rediris.es

2.2. ¿Llevan estos paquetes ICMP puerto origen/destino?

No llevan puerto origen/destino ya que ICMP se trata de un protocol de la capa de red y no de la capa transporte (como TCP y UDP)

EJERCICIO 3, TRACEROUTE

Vuelva a arrancar una captura con Wireshark mientras ejecuta:

```
$ traceroute –n www.google.es
```

Detenga Wireshark y filtre para obtener los mensajes ICMP (filtro ICMP || UDP) deseados de forma similar a como lo hizo en el ejercicio 1. Responda a las siguientes preguntas:

3.1. Identifique los mensajes que genera su PC. ¿Cuál es valor del campo TTL de los datagramas que genera su PC?

Los paquetes que genera nuestro PC siendo la IP fuente (en este caso el de 10.0.12.7) son datagramas UDP, y su valor del campo TTL es 1 que va incrementando de uno en uno porque según vaya alcanzando los distintos destinos, esos routers va decrementando los TTL. Al llegar al destino, dejará de enviar más datagramas y el TTL terminará con valor 13, indicando que se han atravesado 12 routers para llegar al destino www.google.es

3.2. ¿Cuáles son los valores de tipo y código de los mensajes seis primeros ICMP que se reciben? ¿Qué error se está produciendo?

El tipo es 11 y el código 0. Esto nos indica que el error es *Time-to-live exceeded in transit* (TTL expirado), es decir, que el TTL ha llegado a cero en uno de los routers intermediarios.

3.3. ¿Qué datos contienen dichos mensajes? ¿Guardan relación con los mensajes enviados?

En la sección de datos del datagrama ICMP se rellena con los primeros 32 bits del código ASCII empezando por el valor hexadecimal 40, que corresponde al '@', terminando en 5F, que corresponde a '_'. Se escogen estos datos en lugar de enviar datos aleatorios.

Sí, guardan relación, ya que nuestro equipo (el origen) envía datagramas con esos datos y los routers intermediarios nos responden con los mismos.

3.4. ¿Cuál es el tipo y código de los mensajes ICMP recibidos del ordenador destino? ¿Qué error se está produciendo?

Tipo 3 y código 3, que indica el error *destino inalcanzable,* y más concretamente (por el código 3), *puerto destino inalcanzable*.

EJERCICIO 4, DHCP

Arranque Wireshark y configúrelo para capturar tráfico en el interfaz de red de área local. Vamos a forzar al PC del laboratorio a que vuelva a adquirir su dirección mediante DHCP. Para ello proceda como se indica a continuación:

`$ sudo /sbin/dhclient -r` (con esto eliminaremos la configuración de red asignada al interfaz de red)

`$ sudo /sbin/dhclient [interfaz_de_red]` (para obtener una nueva configuración de red)

Cuando el comando se complete, detenga Wireshark, filtre el tráfico DHCP (filtro BOOTP) que tenga como origen o destino su equipo y responda a las siguientes cuestiones.

4.1. ¿Cuál es el servidor DHCP que está enviando una dirección IP para su equipo?

El servidor DHCP es 10.0.8.46 ya que el mensaje DHCP Offer que envía la dirección IP para el equipo lo hace el servidor DHCP.

4.2. ¿Cuál es la secuencia de mensajes DHCP que observa desde que se solicita una nueva dirección IP para su equipo hasta que éste la consigue?

La secuencia de mensajes DHCP son:

Desde el equipo al servidor DHCP se envía el mensaje DHCP Discover para saber quién es el servidor DHCP.

El servidor manda DHCP Offer, ofreciendo la nueva dirección IP.

El cliente manda DHCP Request, aceptando la oferta del servidor DHCP.

El servidor manda DHCP ACK, confirmando el DHCP Request.

4.3. ¿Cuál es la configuración de red IP completa, en concreto, dirección IP, máscara, router, servidor DNS que le asignan a su equipo?

Mirando en el mensaje DHCP Offer se sabe que:

Dirección IP es 10.0.12.7

Máscara: 255.255.248.0

Router: 10.0.8.2

Servidores DNS: 10.0.11.33 y 192.168.153.140