GP6-PL3: Wireshark ICMP y DHCP en IPv4

**Nombres: Álvaro Camacho y Ainara García Puesto: 5 Grupo: 1**

# 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. Esta práctica se hará en los PCs del laboratorio con Windows, aunque si el profesor lo estima conveniente se puede hacer en Linux.

# **EJERCICIO 1, ICMP**

Ejecute Wireshark, capturar tráfico en el interfaz de red de área local que será la primera que aparezca en con una gráfica pequeña de tráfico. Intentar capturar tráfico durante el menor tiempo posible (para analizar el tráfico con más rapidez).

Abra un terminal, buscando *terminal* o *cmd*. Envíe un ping a un equipo situado en su misma red de área local, en caso de usar Windows el Firewall bloquea la respuesta al ping, pero hay otros equipos que contestan:

* *10.0.8.2*
* *10.0.11.34*
* *10.0.8.46*

LINUX

$sudo wireshark

Abra un segundo terminal. Envíe un ping a un PC físicamente más próximo a su puesto de laboratorio[[1]](#footnote-1) y haga un ping a dicho equipo.

$ ping 10.x.x.x

Tras 2 o 3 pings parar el comando con Ctrl+C, detenga Wireshark (para evitar capturar mucho tráfico basura, se recomienda estar capturando durante el menor tiempo posible), 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.

Se recuerda que en la parte central del Wireshark hay desplegables (picando en el símbolo “>”) con información de los protocolos que componen un mensaje, empezando por nivel físico que no usaremos, ni tampoco ahora Ethernet, sobre IP (Internet Protocol) y por último en el ejemplo ICMP

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

Responda a las siguientes cuestiones:

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

Origen Destino

10.0.12.5 10.0.8.2

10.0.12.5 10.0.11.34

10.0.12.5 10.0.8.46

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza baja

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

10.0.8.2🡪10.0.12.5 type 0 code 0 reply

10.0.12.5🡪10.0.8.2 type 8 code 0 request

10.0.11.34🡪10.0.12.5 type 0 code 0 reply

10.0.12.5🡪10.0.11.34 type 8 code 0 request

10.0.8.46🡪10.0.12.5 type 0 code 0 reply

10.0.12.5🡪10.0.8.46 type 8 code 0 request

Aumente el tamaño del mensaje que emplea el ping del apartado anterior hasta 2000 bytes y capture con wireshark el tráfico que se genera.

ping -l 2000 10.0.x.y

LINUX

Imagen que contiene Diagrama

Descripción generada automáticamente

Tras 2 o 3 pings parar el comando con Ctrl+C, detenga Wireshark. Antes de contestar analice la MTU del interfaz **Ethernet** de donde ha capturado el tráfico con alguno de estos comandos

netsh interface ipv4 show subinterfaces

LINUX

ifconfig interface-name

Para analizar las tramas se recomienda quitar el filtro ICMP

1.3. ¿Cuántos paquetes IP se mandan por cada mensaje ICMP original? En Wireshark se recomienda leer detenidamente el campo “Info”, desplegar y analizar las pestañas de “Internet Protocol” e “Internet Message Control Protocol”

Se envían 2 fragmentos.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

1.4. ¿Cuál es el tamaño de cada uno?

El primer fragmento 1480 y el segundo 528.

1.5. ¿Puede explicar qué está ocurriendo?

Como el ping que hemos hecho, hemos puesto que transporte 2000 bytes, pero como la MTU es de 1500 entonces habría que fragmentarlo en 2 paquetes ip, uno de 1480 bytes (el máximo de datos ya que 20 son de cabecera) y el resto de datos 528 que serían los restantes para llegar a 2000 con el segundo paquete.

# **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 del tráfico ICMP? ¿Nuestra dirección IP?, ¿son direcciones IP públicas o privadas?

**Origen Destino**

10.0.12.5 130.206.13.20

Privada Publica

Se recuerda la torre de protocolos que usa PING y ICMP

Diagrama

Descripción generada automáticamente

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

No llevan puerto porque los mensajes de error y control de red, como ping o traceroute se envían con ICMP

# **EJERCICIO 3, TRACEROUTE**

RECORDATORIO FUNCIONAMIENTO TRACEROUTE

El programa traceroute averigua la secuencia de rutas seguida a un destino. Para ello manda primero mensajes con TTL=1 que al llegar al primer router, decrementa su valor y como es 0 tira el mensaje y genera una notificación ICMP que incluye también dicho mensaje.



De esta manera se averigua el primer router.

Se repite el proceso con TTL=2 y en este caso será el segundo router quien lleve el TTL a 0 y se averigüe su identificación.



El proceso se repite hasta llegar al destino.

Vuelva a arrancar una captura con Wireshark mientras ejecuta:

tracert -n www.google.es

LINUX



Nota, el “-n” evita traducir IP de los routes a sus nombres simbólicos. Al finalizar detener Wireshark, del resultado del comando copiar la dirección IP de [www.google.es](http://www.google.es) (se ve al ejecutar el comando, supongamos que es la 216.58.209.67). Filtrar los mensajes con ICMP o UDP, si aparecen muchos mensajes se puede añadir la IP anterior de Google,

icmp || udp && ip.addr == 216.58.209.67

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

Nota: el TTL normal vale 64, cuando tiene un valor muy bajo, puede salir con una línea roja en el Wireshark (Linux/Mac)

El TTL va aumentando según se van enviando los paquetes para mostrar el número de saltos de la ruta.

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

Type 11 code 0 el tipo de error es time to live exceded in transit.

Es el mismo en los 6 mensajes.

Una captura de pantalla de una computadora

Descripción generada automáticamente

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

No contienen datos.

No.

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

Type 8 code 0

El error que se produce es: no response found!

# **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:

ipconfig /release

LINUX



Con el comando anterior eliminaremos la configuración de red asignada al interfaz de red. Para obtener una nueva configuración de red del servidor DHCP, ejecute: ipconfig /renew

Si tarda mas de 10 segundos en devolver el indicador del sistema operativo, dar un Ctrl-C.

LINUX $ sudo /sbin/dhclient

Cuando el comando se complete, detenga Wireshark, filtre el tráfico DHCP (filtro **dhcp**) 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?

10.0.8.46

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?

1. Enviamos un mensaje a la red de difusión para encontrar al servidor. DHCP Discover

2.El servidor nos envía también a la red de difusión una oferta de dirección IP. DHCP Offer.

3.Nosotros enviamos a la red de difusión una solicitud de dirección IP. DHCP Request.

4. Por último, el servidor envía un mensaje de confirmación (ACK) de que se ha asignado la nueva dirección.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

4.3. ¿Cuál es la configuración de red IP completa, en concreto, dirección IP, máscara, router, servidores DNS (varios por fiabilidad) que le asignan a su equipo?

La dirección IP que nos asignan es 10.0.12.1, la máscara es 255.255.248.0, el Router 10.0.8.1 y los servidores DNS 10.0.11.34, 192.168.153.140 y 192.168.153.141.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. Observe que cada PC tiene una etiqueta con la dirección IP que tiene asignada. [↑](#footnote-ref-1)