Analizadores de red: Wireshark

Un ordenador que vaya a funcionar en red necesita una dirección para que la red pueda dirigir hacia él los datos que le envían el resto de ordenadores, es la dirección IP. Para ver la dirección IP de su ordenador (S.O. Linux) puede usar el comando **ifconfig**.

```
$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:11:2F:72:2B:9E
          inet addr:10.1.1.51  Bcast:10.1.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:241448 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84926 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:43488888 (41.4 Mb)  TX bytes:18249053 (17.4 Mb)
          Interrupt:10 Base address:0xd800

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3489 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3489 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2786870 (2.6 Mb)  TX bytes:2786870 (2.6 Mb)
```

Puede observar que su ordenador tiene dos interfaces:

- eth0 es una conexión a una red de área local Ethernet y es la verdadera conexión de red de ese ordenador.

- lo es un interfaz ficticio llamado interfaz de *loopback*, todo lo que se envía por ese interfaz se vuelve a recibir en el ordenador. Es típico de los sistemas UNIX tener este interfaz y vale para enviarse datos a sí mismo incluso cuando el ordenador no está conectado a la red. En los sistemas UNIX muchas partes del sistema operativo funcionan como servicios de red, de ahí que el interfaz de *loopback* sea muy útil. Pero de momento no se preocupe por él.

Pruebe el comando **ping.** El comando ping es una utilidad que le permite comprobar si existe conectividad de red entre dos máquinas. Con ayuda de ping podremos determinar si el nivel de red funciona adecuadamente, así como los niveles de enlace y físico sobre los que descansa. Para ello la máquina que lanza el comando ping envía paquetes del protocolo ICMP que el sistema operativo de la máquina destino está obligada a responder al origen. El comando ping recibe estos paquetes y nos los muestra indicándonos también el tiempo que tardan en ir y volver (Round Trip Time, RTT) y contando los que se pierden. Mire la dirección IP que tiene su vecino de mesa y haga ping a su propio ordenador y al del vecino.

$ ping direccion_IP_de_mi_vecino

$ ping mi_direccion_IP

Observe la diferencia de tiempos. ¿Cómo hace ping para saber que los paquetes se pierden?

Utilizando Wireshark

Por ahora, en nuestras pantallas, las distintas áreas que hemos comentado anteriormente aparecen en blanco. Capturemos los primeros paquetes y veamos qué sucede.

- Desde otro terminal terminal: $ ping direccion_IP_de_mi_vecino
- Para comenzar la captura desplegamos en wireshark el menú Capture, seleccionamos la opción Interfaces, aparecerán todos los interfaces disponibles, e iniciamos(Start) la captura en el interfaz eth0. Wireshark ya está capturando todas las tramas que traspasan nuestro interfaz de red.
- Observe que mientras wireshark captura, le muestra que está reconociendo paquetes de diversos protocolos. Cuando tenga algún paquete ICMP, los generados por el comando ping, detenga la captura y busque en estos paquetes ICMP qué dirección origen y destino llevan.
- Puede indicarle al programa wireshark que filtre el tráfico capturado, de forma que sólo muestre por pantalla los paquetes ICMP. Para ello en la casilla de texto junto al botón Filter escriba icmp y pulse intro. Del mismo modo puede introducir este mismo filtro en la ventana de programación de la captura de forma que sólo capture los paquetes que cumplan el filtro.
- Para finalizar la captura seleccione del menú Capture la opción Stop, o pulse el botón correspondiente en la barra de iconos.

Analicen, a continuación, las tramas capturadas ayudándose para ello de las siguientes cuestiones.

⇒ **Para la trama Ethernet que contiene el mensaje "echo request":**

1. ¿Cuál es la dirección Ethernet de 48-bit del interfaz de red de tu ordenador?

2. ¿Cuál es la dirección Ethernet destino dentro de la trama Ethernet? ¿A qué dispositivo pertenece dicha dirección?

3. ¿Cuál es el valor hexadecimal del campo Tipo de Trama (Frame Type)?

4. ¿Qué tamaño tiene el campo de datos de esta trama Ethernet?

⇒ **Y para la trama Ethernet que contiene el mensaje de respuesta "echo reply":**

1. ¿Cuál es la dirección Ethernet origen dentro de la trama Ethernet? ¿A qué dispositivo pertenece dicha dirección?

2. ¿Cuál es la dirección destino dentro de la trama Ethernet? ¿A qué dispositivo pertenece dicha dirección?

3. ¿Cuál es el valor hexadecimal del campo Tipo de Trama (Frame Type)?

4. ¿Qué tamaño tiene el campo de datos de esta trama Ethernet?

Muestre al profesor de prácticas el valor del campo, dentro de la cabecera IP, que ha permitido saber al analizador que el contenido del paquete IP era un paquete ICMP.