

	Práctica de análisis de tráfico IP e ICMP¹ S06	
Redes y Servicios de Comunicaciones		2016-2017

1.- Introducción y Objetivos

El análisis de tráfico es una herramienta de gran valor para comprender el funcionamiento de los protocolos de comunicación. Este análisis de protocolos permite observar la secuencia de mensajes intercambiados, así como profundizar en los detalles de cómo operan los protocolos.

El objetivo de esta práctica es manejar un analizador de tráfico que nos permita obtener datos acerca del tráfico que circula por la red del Laboratorio. Mediante el análisis de tráfico podemos cerciorarnos del correcto funcionamiento de la red, así como escrutar cómo actúa la pila de protocolos TCP/IP en un entorno real.

En particular, en esta práctica se estudiarán varios aspectos del protocolo ICMP: los paquetes ICMP generados por los programas ping y traceroute así como el formato y contenido de los mensajes ICMP.

2.- Normas de la práctica

Lea atentamente el enunciado hasta el final antes de la sesión. La práctica se realizará en grupos de 2 personas.

Para poder realizar la práctica es necesario disponer de una cuenta de usuario en los laboratorios docentes del Departamento de Ingeniería Telemática. La práctica se realizará utilizando el sistema operativo Linux.

Para realizar la práctica se hará uso del programa de captura y análisis de tráfico wireshark.

 *Las partes del enunciado entre estos símbolos plantean cuestiones que se van proponiendo a lo largo de la sesión. Cada grupo de prácticas debe contestar a estas cuestiones por escrito y entregarlas al final de la sesión de laboratorio al profesor de la asignatura.* 

Duración estimada en laboratorio: 2 horas

3.- Trabajo previo al comienzo de la sesión de laboratorio

Repase en el libro de la asignatura el funcionamiento de los comandos traceroute y ping (secciones 1.4.3 y 4.4.3) y conteste de forma individual el entregable que deberá presentar al profesor al inicio de la sesión.

Repase el funcionamiento del programa wireshark. Para el uso del programa, puede consultar las páginas de manual del sistema o la documentación en línea (Wireshark Documentation), disponible en <http://www.wireshark.org/docs/>. También se recomienda leer atentamente, antes de realizar la práctica, la guía de configuración de wireshark disponible conjuntamente con esta práctica.

**CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70**

**ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70**

Cartagena99

4.- Descripción de la práctica

1. ICMP y ping

En primer lugar analizaremos los paquetes ICMP generados por el comando ping. El programa ping es un programa muy simple que permite verificar si un host tiene conectividad IP (con otro host) o no. El programa ping en la máquina origen envía un paquete dirigido a la dirección IP de la máquina destino; si el destino está funcionando envía de vuelta un paquete hacia la máquina origen. Los paquetes intercambiados son paquetes ICMP.

- a. Arranque el wireshark y active la captura de tráfico.
- b. Haga un ping a la máquina "www.it.uc3m.es" con el parámetro "-c 5" (averigüe utilizando el comando man para que sirve el parámetro "-c").
- c. Cuando el acabe de ejecutarse el comando ping detenga la captura de paquetes en wireshark.
- d. Analice la salida del comando ping y conteste a los siguientes puntos (d.1-d.4):
 - d.1. ¿Cuántos paquetes ping envió su máquina?
 - d.2. ¿Cuál es la dirección IP de www.it.uc3m.es?
 - d.3. La salida de la ejecución del ping muestra, por cada mensaje ICMP enviado, un valor de *time* y un valor de *ttl*. Explique qué son esos valores y razone cómo puede calcularlos el ping.
 - d.4. Utilice de nuevo el comando ping pero esta vez con la máquina feem.it (máquina ubicada en Italia). Compare los resultados en los valores de *time* y en el *ttl* con los obtenidos en el apartado d.3. Razone a qué se deben las diferencias.

A continuación vamos a analizar el tráfico que ha generado el comando ping con la máquina www.it.uc3m.es y que usted habrá capturado con wireshark.

- e. Utilizando un filtro de visualización (por ejemplo por protocolo ICMP y direcciones IP), localice los paquetes ICMP que ha generado el ping a www.it.uc3m.es del apartado b. ¿Qué filtro ha utilizado?
- f. Despliegue en wireshark la información sobre el primer paquete enviado por su máquina. Wireshark ofrece dos visiones del contenido del paquete, una decodificada y otra con el contenido en hexadecimal. En la decodificada se ofrece la información dividida por cabecera, con lo que es fácil ir a la cabecera concreta que quiera analizar. En nuestro caso veremos cabeceras Ethernet, IP, e ICMP. Despliegue la información de la cabecera IP y vea los distintos campos. Por ejemplo, el campo de protocolo tiene valor 01 lo que significa que hay un mensaje ICMP en el campo de datos del datagrama IP. Si pulsa en un campo cualquiera verá que se resalta dicho campo en la secuencia hexadecimal que representa la trama en la otra ventana. Los campos entre corchetes no son datos incluidos en el paquete sino información adicional que wireshark ha podido deducir a partir del paquete capturado. Por ejemplo, en el Echo request se incluye un [Response In:] que indica el número de paquete en la captura wireshark en la que se puede encontrar el Echo reply correspondiente (si no aparece es que wireshark no ha podido determinarlo o que el paquete no se ha capturado). Y en el Echo reply hay un [Response to] en el que se indica el número de paquete en la captura wireshark en la que encontrar el Echo request correspondiente.

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70

Cartagena99

- i. Examine el resto de los Echo Request enviados por su máquina, podrá ver que el identificador es el mismo para todos, mientras que el número de secuencia va incrementandose. ¿A qué se debe eso?, ¿cómo se imagina que utiliza estos campos el comando ping?
- j. Ahora examine los correspondientes paquetes Echo Reply. ¿Cuál es el tipo y código para estos paquetes?, ¿qué otros campos tiene el paquete ICMP?, ¿cuántos bytes tienen los campos checksum, número de secuencia e identificador?

2. ICMP y traceroute

A continuación analizaremos los paquetes generados por el comando `traceroute`. Si recuerda el programa `traceroute` puede usarse para descubrir el camino que siguen los paquetes desde un origen a un destino.

El programa `traceroute` se implementa por defecto de forma diferente en Unix/Linux y en Windows. En esta práctica utilizaremos el parámetro “-I” del comando `traceroute` de Linux (lo que requiere permisos de administrador), con lo que funcionará igual que el `tracert` (comando equivalente) de Windows. El funcionamiento consiste en que la fuente envía una serie de paquetes ICMP de tipo Echo Request (como los que utiliza la utilidad `ping`) a la máquina destino: una primera serie de paquetes con `TTL=1`, una segunda serie de paquetes con `TTL=2`, etc. Recuerde que cuando un encaminador reenvía un paquete IP decrementa en uno el valor del campo `TTL` de dicho paquete. Cuando un paquete llega a un encaminador (que no es el destino del paquete) con `TTL=1`, el encaminador descarta el paquete y envía un paquete de error ICMP de vuelta hacia la fuente.

- k. Arranque `wireshark` y active la captura de tráfico.
- l. Ejecute el comando `traceroute` a la máquina `uw.edu.pl` con el parámetro “-I” y lanzándolo como superusuario (`sudo traceroute`).
- m. Cuando acabe la ejecución del comando, detenga la captura de paquetes.
- n. Analice la salida del comando `traceroute`. Observará que para cada valor de `TTL` la máquina origen (su máquina) ha enviado tres paquetes. Y la salida del comando muestra el `RTT` para cada uno de estos paquetes, así como la dirección IP y en algunos casos el nombre del encaminador que devolvió el paquete ICMP `TTL-exceeded`. Ahora conteste a los siguientes puntos:
- n.1. ¿Por cuántos encaminadores atraviesan sus paquetes hasta llegar a la máquina `uw.edu.pl`?
- n.2. ¿Cuál es la dirección IP del servidor `uw.edu.pl`?
- n.3. Si observa las medidas de `RTT` que ha obtenido con el comando `traceroute`, hay enlaces cuyo retardo es significativamente superior al resto de enlaces. Mirando los nombres de los encaminadores² que están en los extremos de esos enlaces, ¿puede imaginarse cuál es la localización física de dichos encaminadores? Compare localizaciones con incrementos en el `RTT` entre saltos.

A continuación vamos a analizar el tráfico que ha generado el comando `traceroute` y que usted habrá capturado con el `wireshark`. Mantenga en una ventana la salida del comando `traceroute`.

- o. Utilizando un filtro de visualización, localice entre los paquetes capturados, los paquetes que ha generado el `traceroute` ejecutado.
- p. Con relación al primer paquete IP que ha generado su máquina (debido al `traceroute`). ¿Qué

**CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70**

**ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70**

Cartagena99



- r. Examine los últimos paquetes ICMP recibidos por su máquina. ¿Qué diferencias hay entre estos paquetes y el resto de los paquetes ICMP previos recibidos?, ¿por qué son diferentes?



Bibliografía

- Páginas de manual de GNU/Linux
- RFC 792. ICMP: INTERNET CONTROL MESSAGE PROTOCOL. J. Postel, 1981.
- Linux Networking HOWTO, Disponible en: <http://www.tldp.org/HOWTO/Net-HOWTO/>. [Fecha de consulta: noviembre 2016].



Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70