**Práctica 4(VIII): ICMP/IP**[[1]](#footnote-0)

**Descripción**

En esta práctica se va a introducir al alumno en los protocolos IP e ICMP. Para ello se van a usar dos herramientas, muy usadas para la verificación y prueba de conectividad en un entorno de red local, como son ping y traceroute.

**Objetivos**

Utilidad Ping y Traceroute

Mensajes ICMP que se generan por el comando Ping

Mensajes ICMP generados por el programa Traceroute

Formato y contenido de un mensaje ICMP

Campos del datagrama IP

Fragmentación IP

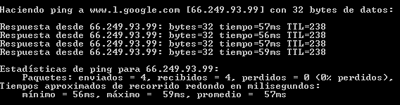
**Información**

**Comando PING**

Ping es una utilidad de administración de red que se utiliza para probar la posibilidad de conexión de un dispositivo en una red IP. Esta utilidad también mide el tiempo de ida y vuelta para los mensajes que se envían desde el host de origen hasta una PC de destino. Para ello se almacena el instante de tiempo en el que se envía el paquete y cuando llega la respuesta al valor almacenado se le resta del tiempo actual. El funcionamiento de la orden **ping** se basa en el uso de mensajes ICMP de tipo 0 (*Echo reply*) y 8 (*Echo request*).

Uso: **ping** *ip\_destino/nombre\_destino*

Ejemplo respuesta al ejecutar “**ping www.google.es**”:



Para cada respuesta, la fuente calcula el tiempo de ida y vuelta (RTT) y el valor del TTL. Al final se calcula el tiempo máximo, mínimo y promedio de RTT.

Otras utilidades de **ping** son:

* Averiguar si un destino está operativo, conectado a la red y sus protocolos TCP/IP en funcionamiento.
* Conocer la fiabilidad de la ruta entre origen y destino (calculando el porcentaje de paquetes que obtienen respuesta).

Los resultados que se obtienen mediante el comando **ping** son, a veces, difíciles de interpretar. El usuario obtiene poca información de por qué el tiempo de ida y vuelta es mayor en unos destinos que en otros. Incluso cuando no hay respuesta al ping, no es posible conocer cuál es el problema: la máquina referenciada está fuera de servicio, no existe una ruta desde el origen al destino o la saturación de la red es tan alta que no se obtiene respuesta del destino en un tiempo razonable. También, en ocasiones por motivos de seguridad y para evitar dar información sobre los ordenadores conectados a la red, los administradores de las redes filtran los mensajes de ping en los cortafuegos o desactivan el servicio en los propios ordenadores. A pesar de lo dicho, es una de las herramientas que más utilizan los administradores y usuarios de equipos conectados en red.

**Comando TRACERT (traceroute en Linux)**

La utilidad traceroute es una herramienta de diagnóstico de red para mostrar la ruta y medir las demoras en el tránsito de los paquetes que viajan por una red IP.

Traceroute se lleva a cabo de diferentes maneras en Unix/Linux y en Windows. En Unix / Linux, la fuente envía una serie de paquetes UDP al destino usando un número de puerto de destino poco probable; en Windows, la fuente envía una serie de paquetes ICMP al destino. Para ambos sistemas operativos, el programa envía el primer paquete con TTL = 1, el segundo paquete con TTL = 2, y así sucesivamente. Recordemos que un router disminuirá valor TTL de un paquete. Cuando un paquete llega a un router con TTL = 1, el router envía un paquete de error ICMP de vuelta a la fuente.

Uso: **tracert** *ip\_destino/nombre\_destino*

Sólo muestra la ruta de ida. El comando “**ping –r *nºsaltos***” muestra una ruta de ida y vuelta.

**Tareas**

**Parte 1. ICMP y Ping**

Vamos a comenzar nuestra aventura ICMP mediante la captura de los paquetes generados por el comando Ping.

Haz lo siguiente:

* Abre la aplicación de símbolo del sistema de Windows.
* Pon en marcha el analizador de paquetes de Wireshark y comienza la captura de paquetes.
* Ejecuta el comando “ping -n 10 [www.cam.ac.uk](http://www.cam.ac.uk)”. El argumento “-n 10” indica que se deben enviar 10 mensajes ping.
* Detén la captura de paquetes Wireshark luego que el comando Ping termine.

Observa los paquetes capturados por Wireshark, después de escribir “ICMP” en la ventana de visualización de filtro. Ten en cuenta que la lista de paquetes muestra 20 paquetes: las 10 consultas de ping enviados por tu PC y las 10 respuestas recibidas de ping. También ten en cuenta que la dirección IP del PC en el laboratorio es una dirección privada (detrás de un NAT) estilo 192.168/12; la dirección IP del destino es la del servidor web de la universidad de Cambridge. Ahora vamos a hacer un zoom sobre el primer paquete (enviado por el cliente).

El primer mensaje de solicitud eco ICMP enviado por tu PC y expande la cabecera IP en la ventana de detalles del paquete. Imprime el contenido del paquete con *File-> Print,* elige *Select packet only*, y *Packet summary line,* y selecciona la información de detalle necesaria para responder a las cuestiones.

Ahora responde a las siguientes cuestiones:

.

1. Dentro del encabezado del paquete IP, ¿cuál es el valor en el campo de protocolo de la capa superior? ¿Qué significa? ICMP. Se ha usado ICMP en la capa de red.
2. ¿Cuál es la dirección IP de tu PC? ¿Cuál es la dirección IP del destino? 172.19.31.138, dst: 128.232.132.8
3. ¿Por qué un paquete ICMP no tiene origen y puerto de destino? Porque omite la información de la capa de transporte y aplicación.
4. Examinar uno de los paquetes de solicitud de ping enviados por tu PC. ¿Cuáles son los números del tipo y código paquete ICMP? ¿Qué otro campo tiene este paquete ICMP? ¿Cuántos bytes son los campos de suma de comprobación y el identificador de número de secuencia? Tipo 8, código 0. Tiene otros 3 campos, checksum, identificador y número de secuencia. Checksum: 2Bytes, Secuencia: 2Bytes.
5. Examinar el paquete de respuesta de ping correspondiente. ¿Cuáles son los números de tipo y código del paquete ICMP? ¿Qué otro campo tiene este paquete ICMP? ¿Cuántos bytes son los campos de suma de comprobación y el identificador de número de secuencia? Tipo 0 y código 0. Los mismos que el de pregunta. 2Bytes cada uno.
6. ¿Cuántos bytes hay en el encabezado IP? ¿Cuántos bytes hay en la carga útil del datagrama IP? Encabezado: 20 bytes. 74 Bytes totales - 20 = 54 Bytes.
7. ¿Se ha fragmentado este datagrama IP? Explica cómo sabes si el datagrama se ha fragmentado o no? No se ha fragmentado porque el campo Fragment Offset está a 0.

**Parte 2. ICMP y Traceroute**

Ahora vamos a continuar nuestra aventura ICMP mediante la captura de los paquetes generados por el programa de Traceroute.

Haz lo siguiente:

• Abre la aplicación de símbolo del sistema de Windows.

• Inicia una captura con Wireshark.

• Ejecuta el comando “tracert [www.cam.ac.uk](http://www.cam.ac.uk)”.

• Detén la captura de paquetes Wireshark luego que el comando Tracert termine.

Traceroute muestra el RTT para cada uno de los paquetes de sonda, así como la dirección IP (y posiblemente el nombre) del router que devuelve el mensaje TTL superado ICMP.

Observa la captura Wireshark y filtra por “icmp”. Imprime de nuevo la información necesaria para responder a las cuestiones.

Ahora responde a las siguientes cuestiones:

1. Examina el paquete de eco ICMP en tu pantalla. ¿Se diferencia de los paquetes ICMP ping, compáralo con lo observado en la parte 2? En caso afirmativo, ¿cómo? El tamaño del paquete es mayor, de 76 Bytes a 106Bytes.
2. Examina el paquete de error ICMP. ¿Tiene más campos que el paquete echo ICMP de la Parte 1? ¿Que está incluido en estos campos? Tiene 2 menos que los otros pero a cambio incluye el campo unused.
3. Examina los últimos tres paquetes recibidos ¿Cómo son estos paquetes diferentes de los paquetes ICMP de error? ¿Por qué son diferentes? Porque se llegó al destino y tienen al igual que en la parte 1 los campos identifier y sequence number. Ya no son paquetes de mensaje de error o de que están por el camino.
4. Dentro de las mediciones tracert (en la ventana de comandos), ¿existe un vínculo cuyo retraso es significativamente más que otros? ¿Sobre la base de los nombres del router, se puede adivinar la ubicación de los dos routers en el extremo de este enlace? El paquete 14 tarda más que el resto. Podemos ver que la conexion pasa por 4 redes a mayores de la uvigo donde empieza.

A continuación, elimina el filtro “icmp” y ordena los paquetes rastreados según la dirección de origen de IP haciendo clic en el encabezado de la columna *Source*; debería aparecer una pequeña flecha apuntando hacia abajo junto a la palabra *Source*. (Si la flecha apunta hacia arriba, haga clic nuevamente). Selecciona el primer mensaje de solicitud de eco ICMP enviado por tu computadora y expande la parte del Protocolo de Internet en la ventana "detalles del encabezado del paquete seleccionado". En la ventana "listado de paquetes capturados", deberías ver todos los mensajes ICMP posteriores (tal vez con paquetes intercalados adicionales enviados por otros protocolos que se ejecutan en su computadora) debajo de este primer ICMP. Use la flecha hacia abajo para moverse a través de los mensajes ICMP enviados por su computadora.

1. ¿Qué campos en el datagrama IP siempre cambian de un datagrama a otro dentro de esta serie de mensajes ICMP enviados por su computadora? El identificador y el checksum
2. ¿Qué campos se mantienen constantes? ¿Cuál de los campos debe permanecer constante? ¿Qué campos deben cambiar? ¿Por qué? El resto. El identificador y por ello el checksum
3. Describa el patrón que ve en los valores en el campo Identificación del datagrama IP Son todos 1600 y algo y cada uno es menor que el anterior.

Ahora (con los paquetes aún ordenados por dirección de origen) encuentra la serie de respuestas “ICMP TTL Excedeed” enviadas a tu computador por el enrutador (primer salto) más cercano.

1. ¿Cuál es el valor en el campo Identificación y el campo TTL? 18186, ttl: 1
2. ¿Estos valores permanecen sin cambios para todas las respuestas superadas por ICMP TTL enviadas a su computadora por el enrutador (primer salto) más cercano? ¿Por qué?No, el ttl se mantiene pero el ID va cambiando.

**Parte 3. IP y Fragmentación**

No podemos observar la fragmentación que se produce en los routers pero podemos utilizar un pequeño truco para generar fragmentación en la propia interfaz del computador. Para ello, vamos a suponer que la tarjeta Ethernet del computador que limita la longitud del paquete IP máximo a 1500 bytes (40 bytes de datos de encabezado TCP / IP y 1460 bytes de carga útil de protocolo de capa superior). Este valor de 1500 bytes es la longitud máxima estándar permitida por Ethernet. Puedes conocer la MTU de tu interfaz con el comando: “netsh interface ip show interface”.

Haz lo siguiente:

* Inicia una nueva captura de Wireshark
* Desde una ventana de comandos ejecuta la orden siguiente: C:\> ping –n 1 –l 2000 direcciónIP\_de vuestro\_gateway

Con ello estamos forzando a nuestro computador al envío de un mensaje de más de 2000 bytes al destino especificado. Como estamos conectados a una red Ethernet cuya MTU es de 1500 bytes, el envío solicitado exigirá la fragmentación del mensaje en dos paquetes IP.

* Detén la captura de paquetes Wireshark luego que ping termine.

Identifica los paquetes que ha generado el ping. Utiliza un filtro de display para mostrar solamente los paquetes IP e ICMP (Wireshark en la fragmentación de un paquete ICMP solo etiqueta como ICMP el último fragmento) y responde a las siguientes cuestiones:

1. Encuentra el primer mensaje de solicitud de eco ICMP que envió tu computador. ¿Se ha fragmentado ese mensaje en más de un datagrama IP? Si, el Fragment Offset es distinto de 0 (vale 1480).
2. Imprime el primer fragmento del datagrama IP fragmentado. ¿Qué información en el encabezado IP indica que el datagrama ha sido fragmentado? ¿Qué información en el encabezado de IP indica si este es el primer fragmento versus un último fragmento? ¿Cuál es el tamaño de este datagrama IP? El flag More Fragments está encendido. Su fragment offset está a 0, indicando que es el 1º.1500 - 20 bytes = 1480.
3. Imprime el segundo fragmento del datagrama IP fragmentado. ¿Qué información en el encabezado IP indica que este no es el primer fragmento de datagrama? ¿Hay más fragmentos? ¿Cómo lo puedes saber? El offset distinto de 0 deja saber que es la contiuacion de otro fragmento y como More Fragments está a 0 no hay más.
4. ¿Qué campos cambian en el encabezado IP entre el primer y el segundo fragmento? Total length , los flags (More Fragments), y el fragment offset.

1. Adaptado de: Wireshark Labs v7.0 J.F. Kurose, K.W. Ross. [↑](#footnote-ref-0)