PRÁCTICA 2

Protocolo de Mensajes de Control de Internet (ICMP)

REDES (9359)

ING. TÉCNICA EN INFORMÁTICA DE SISTEMAS

CURSO 2009/2010

Pablo Gil Vázquez (Pablo.Gil@ua.es)
Grupo de Innovación Educativa en Automática

Universitat d'Alacant
Universidad de Alicante

2.1. Introducción

El objetivo de la práctica 2 de la asignatura Redes es profundizar en el funcionamiento del protocolo de mensajes de control y error ICMP.

El alumno adquirirá conocimientos acerca de los diferentes mensajes ICMP y su utilidad a la hora de controlar una red de ordenadores. En la realización de la práctica se abordarán distintas situaciones de error en el funcionamiento de una red de datagramas basada en el protocolo IP y se evaluará de forma práctica los tiempos de respuesta de la red.

2.2. Protocolo ICMP

2.2.1 Descripción del protocolo

ICMP (*Internet Control Message Protocol*, Protocolo de Mensajes de Control de Internet) es considerado como parte de la capa de red IP. ICMP es un protocolo empleado por los routers (encaminadores) y por los hosts (clientes, servidores, etc) para comunicar la información de control o de error de la red.

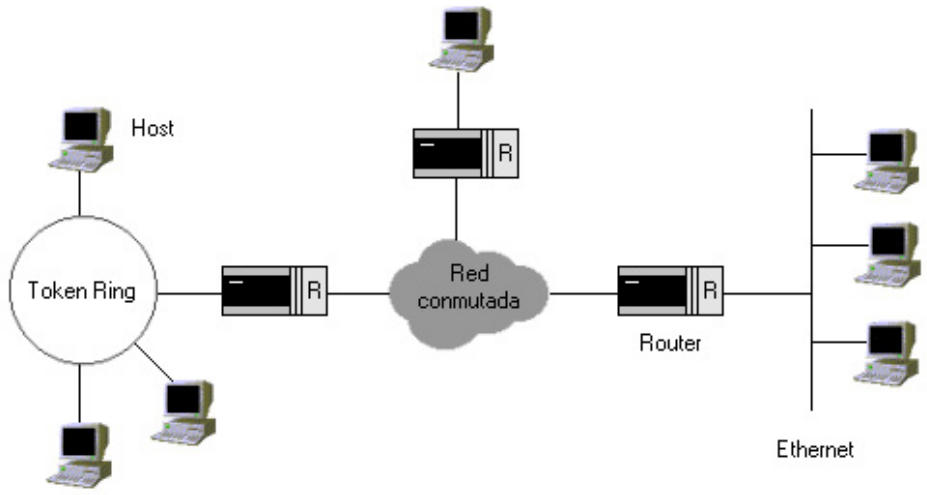

Figura 1. Red de datos compuesta por Routers y Hosts.

Además de los fallos en las líneas de comunicación, IP tiene fallos en la entrega de datagramas cuando la máquina destino está desconectada, cuando el tiempo de vida se acaba o cuando existe congestión en los encaminadores. El protocolo IP no puede controlar estas situaciones y los diseñadores de TCP/IP crearon ICMP como mecanismo de informe de errores y/o situaciones anómalas en la red. Una consideración a tener en cuenta es que ICMP informa de errores, pero no los corrige.

Los mensajes ICMP requieren dos niveles de encapsulación. ICMP es transmitido en el interior de datagramas IP, estructuras que viajan en la trama de cada red física:

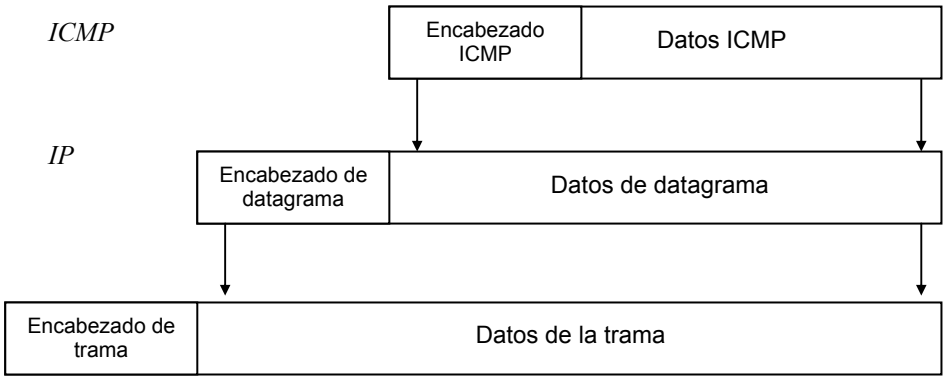

Figura 2. Encapsulación de protocolo ICMP.

2.2.2. Formato de los mensajes ICMP

Aunque cada mensaje ICMP tiene su propio formato, todos comienzan con los mismos tres campos; un campo **TYPE** (tipo) de mensaje, de 8 bits, que identifica el mensaje; un campo **CODE** (código) de 8 bits, que aporta más información sobre el tipo de mensaje, y un campo de verificación **SVT**, de 16 bits. Los siguientes 32 bits después del campo SVT tienen un propósito que varía y depende tipo y código del paquete ICMP considerado.

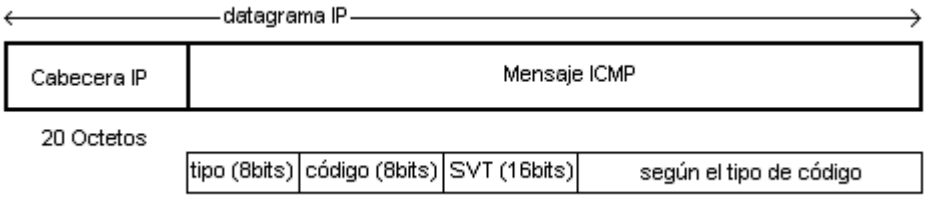

Figura 3. Esquema general de mensaje ICMP.

A continuación se describen los distintos **tipos** de mensajes ICMP (tabla 1):

Mensaje ICMP	Tipo
Respuesta de Eco.	0
Destino inaccesible.	3
Disminución de origen.	4
Redirección.	5
Solicitud de Eco.	8
Tiempo excedido para un datagrama.	11
Problema de parámetros de un datagrama.	12
Solicitud de timestamp.	13

Mensaje ICMP	Tipo
Respuesta de timestamp.	14
Solicitud de información.	15
Respuesta de información.	16
Solicitud de máscara de dirección.	17
Respuesta de máscara de dirección.	18

Tabla 1. Tipos de mensajes ICMP.

Un error ICMP enviado contiene siempre la cabecera IP y los 8 primeros octetos de datos del datagrama que lo provocó. Ello permite al módulo ICMP asociar el mensaje recibido a un protocolo particular (TCP o UDP en función del campo 'protocolo' de la cabecera IP) y a un proceso de usuario determinado (mediante los números de puerto de TCP o UDP).

Las situaciones expuestas a continuación **no** generan mensajes de error ICMP:

- Un mensaje de error ICMP. Un mensaje de error ICMP puede, a pesar de todo, ser generado como respuesta a una solicitud ICMP.
- Un datagrama destinado a una dirección IP de 'broadcast'.
- Un datagrama enviado como 'broadcast' de la capa de enlace.
- Un datagrama fragmentado que no sea el primero de la secuencia.
- Un fragmento recibido fuera de secuencia.
- Un datagrama cuya dirección fuente no está asociada a una única máquina. Esto significa que la dirección fuente no puede valer 0, ni ser el bucle local, ni una dirección broadcast.

En las siguientes secciones se describen los mensajes ICMP más destacados.

2.3. Mensajes echo y echo reply

Existe en los sistemas Unix, Linux, Windows 9X, NT, 2000 o XP un programa de aplicación denominado **ping** que presenta una serie de posibilidades que lo convierten en una herramienta muy valiosa a la hora de depurar y localizar errores. Formalmente 'ping' proporciona una prueba de accesibilidad y estado de un destino.

'Ping' se basa en el protocolo ICMP, o protocolo de control de transmisión. A diferencia del resto de aplicaciones TCP/IP, no utiliza ninguno de los protocolos de transporte TCP o UDP. Se apoya directamente sobre IP. Este aspecto debe tenerse en cuenta, dado que la recepción de una respuesta al comando ping indica que la máquina remota está activa a nivel IP, pero no asegura que el funcionamiento de su capa TCP o UDP sea el correcto.

'Ping' utiliza un mensaje de petición de echo (tipo 8) para enviar un datagrama a su destinatario y espera el retorno de un mensaje 'echo reply' (tipo 0) del destinatario. De este modo, es capaz de evaluar tiempos de respuesta promedios. Dispone de varias opciones, entre las que cabe destacar la posibilidad de modificar el tamaño del paquete enviado, el registro de ruta, y el control del número de paquetes enviados. Por ejemplo:

C:\> ping -l 200 172.20.43.231

provocaría la emisión hacia el router CISCO 1601 de 4 paquetes, cada uno de ellos con 200 bytes de datos a los que habría que sumar 20 bytes de la cabecera IP y 8 de la ICMP:

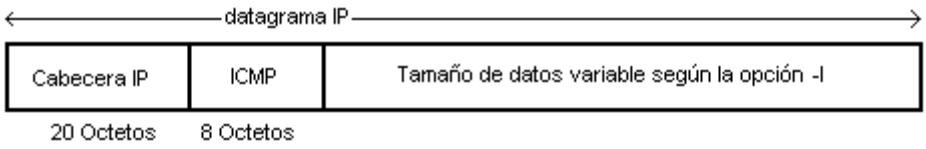

Figura 4. Mensaje ping.

La respuesta que Ping proporcionada en pantalla corresponde a una serie de líneas donde se indica el tiempo de respuesta del echo ICMP y el número de secuencia. Después de ejecutar el comando, queda reflejado el número de paquetes perdidos, los tiempos mínimos, máximos y medios de respuesta (ida y vuelta). Nos permitirá conocer la tasa de error de un enlace así como la velocidad real de transmisión de forma experimental.

Algunas opciones del comando ping para sistemas operativos MS Windows y Linux se reflejan en la tabla 2:

ping [opciones] <ipaddr>

MS Windows	Linux	Descripción
-n <x>.	**-c <x>**.	Envía <x> paquetes ICMP.
-l <y>.	**-s <y>**.	Envía paquetes de longitud <y>.
-i <z>.	**-t <z>**.	Limita la vida del paquete (TTL) a <z>.
-f .	**-D**.	Activa el bit Don't fragment.

Tabla 2. Opciones del comando *ping* para MS Windows y Linux.

siendo **<ipaddr>** la dirección IP de destino.

El formato de los mensajes ICMP de solicitud de Eco y respuesta de Eco es el siguiente:

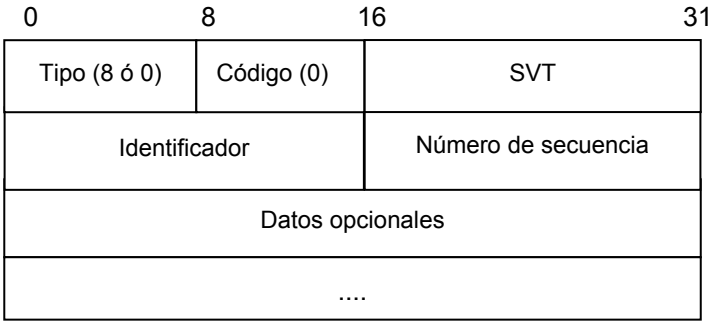

Figura 5. Formato de mensaje ICMP echo request y echo reply.

El campo indicado como **datos opcionales** es un campo de longitud variable que contiene los datos que regresarán al emisor. Una respuesta de 'echo' siempre devuelve exactamente los mismos datos presentes en la solicitud. Los campos **identificador** y **número de secuencia** son utilizados por la máquina de usuario para responder a las solicitudes.

2.4. Mensaje destination unreachable

El mensaje **Destination Unreachable** (tipo 3) se produce cuando un paquete IP no consigue alcanzar su destino por algún motivo. Dependiendo del valor del campo código en el mensaje ICMP se indica un motivo diferente:

Valor de Código	Significado
0	Red de destino inaccesible.
1	Host de destino inaccesible.
2	Protocolo de destino inaccesible.
3	Puerto de destino inaccesible.
4	Se necesita fragmentación y DF activo.
5	Fallo en la ruta origen.
6	Red de destino desconocida.
7	Host de destino desconocida.
8	Host de origen aislado.
9	Comunicación con la Red de destino prohibida administrativamente.
10	Comunicación con el Host de destino prohibida administrativamente.
11	Red de destino inaccesible por el tipo de servicio.
12	Host de destino inaccesible por el tipo de servicio.

Tabla 3. Códigos de mensajes ICMP para tipo 3.

De todos estos códigos destacan:

- **Código 1**. Host Unreachable (3/1). Un router informa que no ha podido enviar el paquete a la máquina de destino.

- **Código 3**. Port Unreachable (3/3). El puerto de destino del paquete IP en la máquina de destino no tiene asociado ningún proceso que lo atienda.

- **Código 4**. Fragmentation Needed and Don't Fragment was Set (3/4). Un router entre las máquinas origen y destino precisa realizar la fragmentación del datagrama IP y no se ha llevado a cabo porque el bit don't fragment de la cabecera IP está activo.

El resto de los mensajes se explican por sí mismos. El formato de este tipo de mensajes se detalla a continuación:

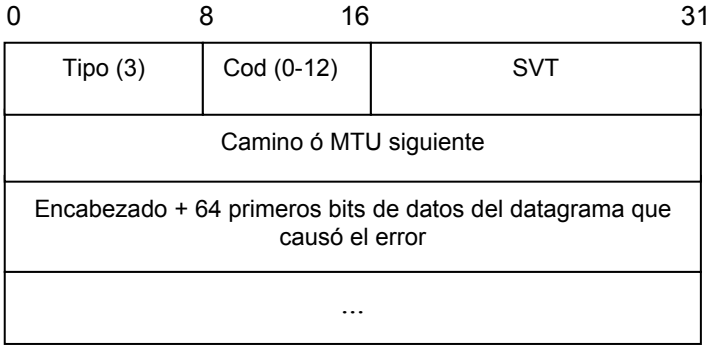

Figura 6. Formato de mensaje ICMP tipo 3.

2.5. Mensaje redirect

El mensaje **Redirect** (tipo 5) es enviado por un router hacia el emisor de un datagrama IP si el encaminador detecta que el emisor emplea una ruta no óptima. Según el router, este datagrama debería haber sido transmitido a un router diferente. En la figura 7 se muestra el esquema de la situación 'redirect' en una red.

Cada mensaje de redireccionamiento contiene un campo de 32 bits llamado **dirección de internet del encaminador** que contiene la IP de salida correcta para la máquina emisora.

A continuación, se explica el funcionamiento del redirect. Se pretende enviar información desde un PC1 a un PC2. Siguiendo el esquema de la figura 7, veamos paso a paso qué ocurre:

1. Suponemos que el PC 1 envía el datagrama IP que tiene como destino el PC 2 al router 1. La decisión de encaminamiento es coherente puesto que el router 1 está definido como puerta de enlace por defecto en esta máquina.
2. El router 1 percibe que la interfaz de salida para el mensaje es la misma por la que se recibió el datagrama procedente del PC 1. Emite el mensaje al PC 2 como si procediera del PC 1, es decir, la dirección IP origen del mensaje es la del PC 1.

3. A su vez, el router 1 emite un error de redirección ICMP hacia el PC 1, informándole que actualice su tabla de encaminamiento y que envíe directamente los próximos datagramas con ese mismo destino al router 2 sin pasar por el router 1.
4. Por último, el destino final (PC 2) responde a través del router 2 al emisor del mensaje original.

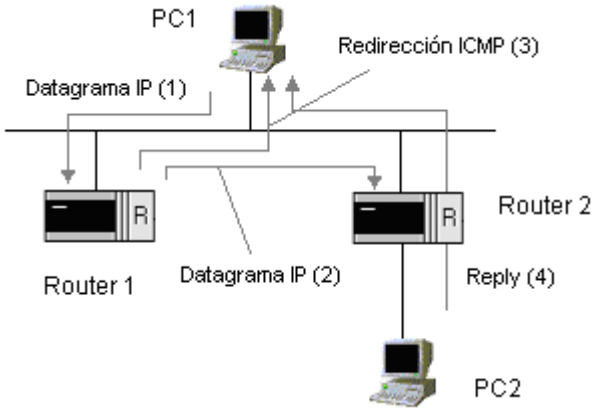

Figura 7. Error de redirección. Situación desencadenada.

Valor de Código	Significado
0	Redireccionar datagramas para la red (obsoleto).
1	Redireccionar datagramas para el Host.
2	Redireccionar datagramas para el tipo de servicio
3	Redireccionar datagramas para el tipo de servicio

Tabla 4. Códigos de mensaje para tipo 5.

El formato del mensaje ICMP es el siguiente:

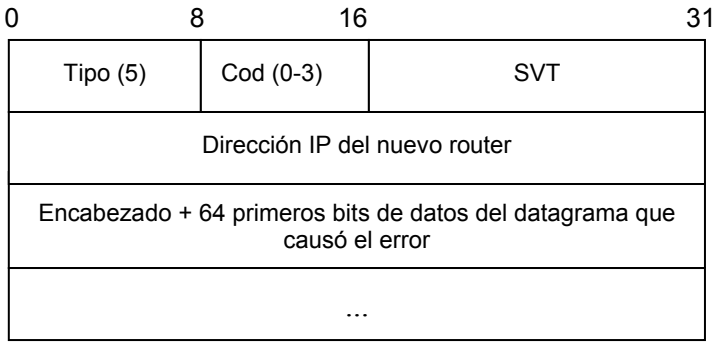

Figura 8. Formato de mensaje ICMP de redirección (tipo 5).

2.6. Mensaje time exceeded

El mensaje **Time Exceeded** (tipo 11) genéricamente indica que el tiempo máximo de tránsito para un datagrama en la red se ha sobrepasado, de esta forma es fácil detectar la presencia en la red de rutas circulares o excesivamente largas.

Dependiendo del código del mensaje éste se emplea en dos situaciones diferentes:

- **Código 0**. Time to Live exceeded in Transit. Este mensaje ICMP es enviado al origen por un router cuando el valor del campo TTL (Tme to live) en la cabecera IP de un datagrama toma el valor 0.
- **Código 1**. Time to Live exceeded in Reassembly. Este mensaje ICMP es enviado por un router o la máquina de destino de un datagrama cuando en el reensamblado de los fragmentos del mismo alguno de los fragmentos no se recibe antes de un tiempo determinado.

Un ciclo de encaminamiento puede consistir en dos encaminadores, cada uno encaminando al otro un datagrama con el mismo destino, o puede consistir en muchos encaminadores haciendo lo mismo, formando un bucle en el enrutamiento. Si un datagrama entrara en un ciclo de encaminamiento (debido a una mala gestión de las tablas de encaminamiento de los routers) recorrería indefinidamente y de manera circular todos los routers. Sin embargo, gracias al empleo del TTL, llega un momento en el que el tiempo de vida del mensaje es cero y el datagrama es eliminado. Esta situación debe ser comunicada al emisor del mensaje.

El reensamblado de fragmentos se refiere a la tarea de unir todos los fragmentos de un datagrama. Cuando llega el primer fragmento de un datagrama, el host que lo recibe activa un temporizador y considera como error que dicho temporizador expire antes de que lleguen a ser reensamblados todos los fragmentos del datagrama.

El formato del mensaje ICMP de tiempo excedido es el siguiente:

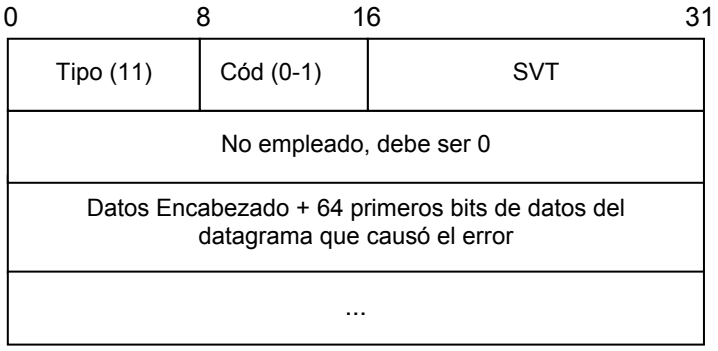

Figura 9. Formato de mensaje ICMP de tiempo excedido. Un encaminador envía este mensaje cuando se descarta un datagrama por TTL=0. Una máquina destino también emplea este formato de ICMP para avisar al origen de la imposibilidad de reensamblar datagramas.

Una aplicación muy interesante del mensaje *time exceeded* (tipo 11, código 0) es la posibilidad de conocer todos los routers por los que circula un datagrama hasta que llega a su destino. Si se realiza un 'ping' a una máquina destino con un tiempo de vida muy reducido es evidente que el datagrama morirá en el camino y el

router enviará el correspondiente informe de error. La técnica para conocer todos los routers por los que viaja un paquete IP es ir incrementando, uno a uno y desde cero, el TTL del paquete que se envía en el comando 'ping'. Aplicaciones sencillas como 'tracert' de Windows se basan en este mensaje de error para conocer las rutas de los mensajes. En la siguiente tabla se presenta el significado de las opciones del programa 'tracert'.

tracert [opciones] <destino>

MS Windows	Descripción
-d.	No convierte direcciones en nombre de hosts.
-h <salt_m>.	Máxima cantidad de saltos en la búsqueda del host.
-j <list_host>.	Encaminamiento a través de la lista de hosts.
-w <tiempo>.	Cantidad de milisegundos entre intentos.

Tabla 5. Opciones del comando *tracert* para MS Windows.

2.7. Mensaje source quench

Debido a que IP funciona sin conexión, un router no puede reservar memoria o recursos de comunicación antes de recibir datagramas. Como resultado, los encaminadores se pueden saturar con el tráfico, condición conocida como congestionamiento.

El congestionamiento puede surgir por dos razones diferentes:

- Envío de datagramas de LAN a WAN, el congestionamiento ocurrirá en el router que conecta la LAN con la WAN ya que los datagramas llegan más rápido de lo que se pueden enviar.
- Si muchas computadoras necesitan enviar datagramas al mismo tiempo a través de un mismo encaminador, éste se puede congestionar.

Cuando los datagramas llegan a los routers se almacenan temporalmente en una cola de espera. Cuando alguna de estas colas de entrada de paquetes del router se satura, éste emite mensajes ICMP **Source Quench** (disminución de tasa al origen), para informar del congestionamiento a la fuente original, y eliminar así los paquetes en exceso que le llegan. De esta manera, el mecanismo de control de flujo utilizado por IP se limita a enviar mensajes Source Quench al equipo fuente para indicarle que reduzca su caudal de salida.

En general, los encaminadores envían un mensaje de disminución de tasa al origen por cada datagrama que descartan. Cuando estos mensajes se reciben en la máquina origen se disminuye la velocidad de envío progresivamente hasta que dejan de recibirse informes de este error ICMP.

El formato del mensaje tipo 4 (source quench) es el siguiente:

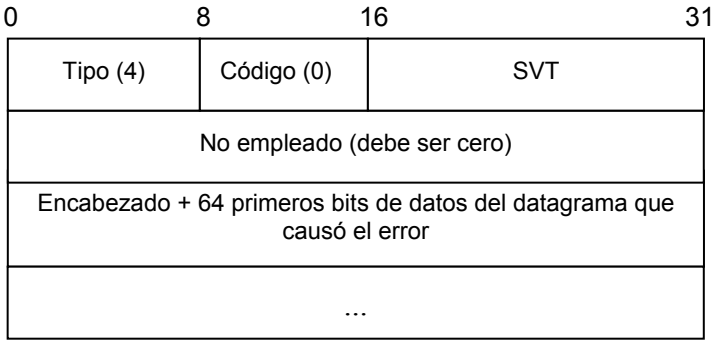

Figura 10. Formato de mensaje ICMP de Source Quench, también denominado disminución al origen. Un router congestionado envía este tipo de mensaje cada vez que descarta un datagrama.

2.8. Mensaje timestamp

Aunque las máquinas en una red se pueden comunicar, por lo general operan de forma independiente, manteniendo su propia noción de la hora actual. Los relojes que varían demasiado pueden confundir a los usuarios de software de sistemas distribuidos. El formato del mensaje timestamp se presenta a continuación:

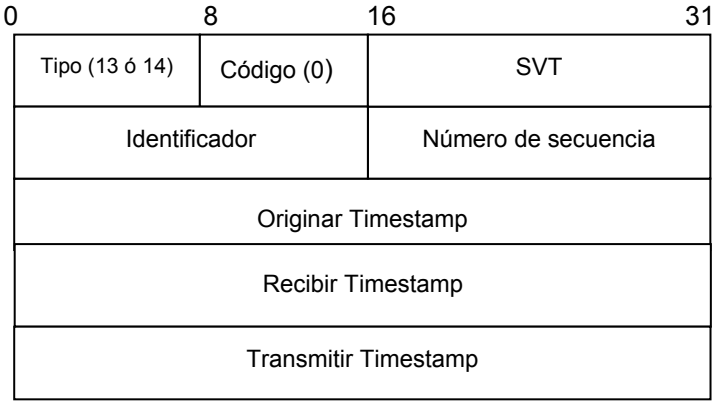

Figura 11. Formato de mensaje ICMP de solicitud de timestamp o de respuesta de timestamp.

TCP/IP incorpora una técnica sencilla para sincronizar relojes a través de mensajes ICMP. Una máquina solicitante envía un mensaje ICMP (tipo 13) de solicitud de timestamp (marca de hora) a otra, requiriéndole que informe de su valor actual de hora. La máquina receptora de dicha solicitud envía una respuesta de timestamp (tipo 14) a quién la solicitó

Al igual que en otro tipo de mensajes ICMP, los campos **identificador** y **número de secuencia** los utiliza la fuente para asociar las solicitudes con las respuestas. Los campos restantes especifican la hora, en milisegundos desde la medianoche, en tiempo del meridiano de Greenwich. El campo **originar timestamp** es llenado por la fuente original justo antes de transmitir el paquete. El campo **recibir timestamp** se llena inmediatamente en el destino al recibir una solicitud y el campo **transmitir timestamp** posee valor justo antes de transmitir la respuesta desde el destino.

Los Hosts o máquina de usuario utilizan estos tipos de mensajes ICMP (13 y 14) para computar estimaciones del tiempo de retraso entre ellos y sincronizar sus relojes. Además, debido a que la repuesta ICMP (tipo 14) incluye el campo **originar timestamp**, una máquina puede computar el tiempo total requerido para que una solicitud viaje hasta un destino, se transforme en una respuesta y regrese.

2.9. Ejercicios

Cuestión 1. Ping

Iniciar el programa monitor de red capturando los paquetes IP con origen o destino la máquina del alumno. A continuación ejecutar el comando:

C:\>ping –n 1 172.20.43.231

Detener la captura en el monitor de red y visualizar los paquetes capturados. En base a los paquetes capturados determinar:

a. ¿Qué tipos de mensajes ICMP aparecen?

b. Justificar la procedencia de cada dirección MAC e IP.

c. Justificar la longitud de los paquetes.

Cuestión 2. Fragmentación

Empleando el programa monitor de red de la misma forma que en la situación anterior, ejecutar:

C:\>ping –n 1 –l 2000 172.20.43.231

a. Describir el número de fragmentos correspondientes a cada datagrama IP.

b. Determinar el MTU de la máquina del alumno y de la máquina 10.3.2.0.

Cuestión 3. Destination Unreachable

Dentro del mensaje ICMP Destination Unreachable se analizará el de código 4: Fragmentation Needed and Don't Fragment was Set (3/4). En primer lugar iniciar el monitor de red de la misma forma que en las cuestiones anteriores. Ejecutar el comando:

C:\>route delete 10.3.7.0

Con el comando **route** se modifican las tablas de encaminamiento de una máquina, donde se indican a que interfaces han de ser dirigidos los paquetes IP. Con la opción **delete** eliminamos un camino o ruta a la dirección especificada. A continuación ejecutar el comando ping:

C:\>ping -n 1 –l 1000 -f 10.3.7.0

En base a los paquetes capturados, indicar:

- **a.** Identificar las direcciones IP/MAC de los paquetes involucrados.
- **b.** ¿Quién envía el mensaje ICMP Fragmentation Needed and Don't Fragment was Set (3/4)?

Se determinará ahora el tipo de mensaje Destination Unreachable cuando se ejecuta el siguiente comando:

C:\>ping -n 1 -l 2000 172.20.41.244

Indicar:

- **a.** ¿Cuál es el router que envía el mensaje ICMP de error? Justifica la respuesta.
- **b.** ¿Cuál es el código de error recibido?

Cuestión 4. Redirect

Iniciar el monitor de red con los filtros adecuados para capturar los paquetes involucrados en la situación de Redirect. A continuación ejecutar los comandos:

C:\>route delete 10.4.2.1
C:\>ping -n 1 10.4.2.1

En base a los paquetes capturados contestar a las siguientes preguntas:

- **a.** ¿Cuántos paquetes están involucrados? Ten en cuenta que debido al dispositivo Switch tu Pc no puede capturar el datagrama IP redirigido.
- **b.** Dibujar gráficamente el origen y destino de cada trama.
- **c.** ¿Quién envía el mensaje ICMP Redirect?
- **d.** ¿Qué datos complementarios transporta ese mensaje de Redirect?
- **e.** ¿Qué piensas que ocurre con los campos TTL y el Checksum del datagrama IP que se envió originalmente? ¿Y con los del paquete redirigido?

Ejecuta ahora los comandos:

C:\>route delete 10.4.2.2
C:\>ping -n 1 10.4.2.2

- **f.** ¿Qué camino siguen los paquetes de IDA y los de VUELTA?
- **g.** Dibujar gráficamente el origen y destino de cada trama.
- **h.** ¿Quién envía el mensaje ICMP Redirect?

Ejecuta los comandos:

C:\>ping -n 1 172.20.41.241
C:\>ping –n 1 172.20.41.242

i. Comprueba si hay redirección en algún caso.

Cuestión 5. Time Exceeded

Dentro del mensaje ICMP Time Exceeded se analizará el de código 0: Time to Live exceeded in Transit (11/0). En primer lugar iniciar el monitor de red para capturar paquetes IP relacionados con la máquina del alumno y ejecutar el comando:

C:\> ping –i 1 –n 1 10.3.7.0

Detener la captura y determinar:

¿Quién envía el mensaje ICMP Time to Live exceeded in Transit?

Iniciar de nuevo la captura y ejecutar a continuación el comando:

C:\> ping –i 2 –n 1 10.3.7.0

Detener la captura y determinar:

a. ¿Quién envía el mensaje ICMP TTL exceeded?

b. ¿Justificar la diferencia con el caso anterior?

c. ¿Cuántos saltos se necesitan para alcanzar la máquina destino 10.3.7.0 desde tu PC?

Cuestión 6. Fragment Reassembly Time Exceeded

Iniciar el programa monitor de red capturando los paquetes IP con origen o destino la máquina del alumno. A continuación abrir varias ventanas MS-DOS (de éste modo aumentaremos el tráfico generado) y en cada una de ellas ejecutar el comando:

C:\>ping -n 500 -l 20000 10.3.7.0

Detener la captura y determinar:

a. ¿De que equipo proceden los mensajes ICMP Fragment Reassembly Time Exceeded?

b. ¿Por qué proceden de ese equipo y no de otro?

c. En el mensaje ICMP aparecen unas direcciones fuente MAC e IP. ¿Pertenecen ambas al mismo equipo?