Instituto Politécnico Nacional
ESCOM
"Escuela Superior de Cómputo"

Aplicaciones Para Comunicaciones En Red

Tarea 7

Profesora: Bautista Rosales Sandra Ivette

Grupo: 3CV13

Nombre: Santiago Pérez Carlos Augusto

El Protocolo de control de mensajes de Internet (ICMP)

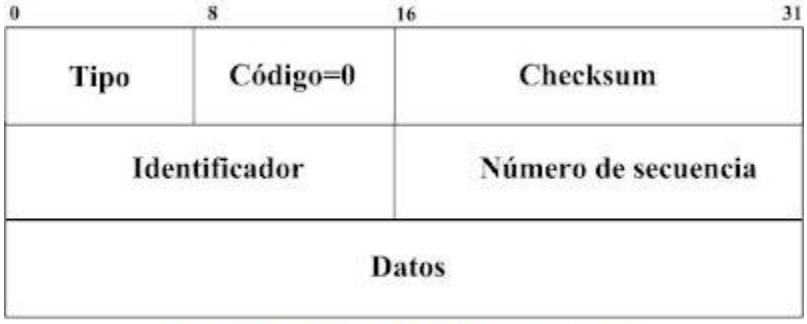
Es un protocolo en la capa de red que utilizan los dispositivos de red para diagnosticar problemas de comunicación en la red. El ICMP se utiliza principalmente para determinar si los datos llegan o no a su destino a su debido tiempo. El protocolo ICMP se suele utilizar en dispositivos de red, como los enrutadores. El ICMP es crucial para informar de errores y realizar pruebas, pero también puede utilizarse en ataques de denegación de servicio distribuido (DDoS).

El objetivo principal del ICMP es informar sobre errores. Cuando dos dispositivos se conectan a través de Internet, el ICMP genera errores para compartirlos con el dispositivo emisor en caso de que alguno de los datos no haya llegado a su destino previsto. Por ejemplo, si un paquete de datos es demasiado grande para un enrutador, este descartará el paquete y enviará un mensaje ICMP de vuelta a la fuente original de los datos.

Tipos de mensajes ICMP y breve descripción

Mensajes ICMP Echo (8) y Echo Reply (0)

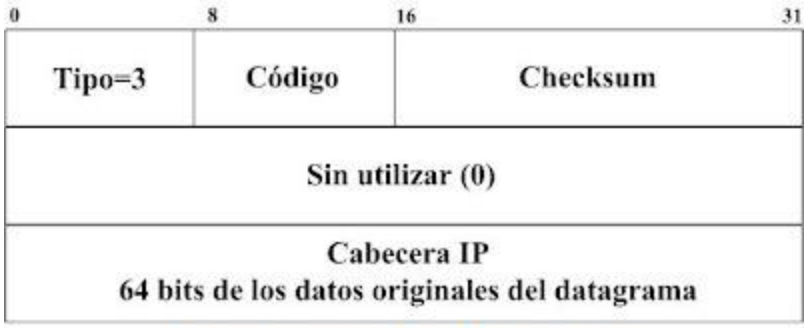
Los mensajes de echo son utilizados para detectar si otro equipo está activo en la red. Es utilizado por el comando Ping. El host que envía el mensaje de petición (request) inicializa los campos identifier, sequence number a valores escogidos por él, así como el contenido de los datos (data). El host receptor de la petición cambia el tipo de mensaje a Echo Reply y devuelve el datagrama al emisor con los mismos valores en los campos identifier, sequence number y contenido que recibió, es decir realiza un 'eco' del mensaje recibido.



Mensaje ICMP Destination Unreachable (3)

Si este mensaje es recibido desde un router intermedio nos indicará que el router considera la dirección IP destino como inalcanzable.

Si el mensaje es recibido desde el equipo destino nos indicará que el protocolo especificado en campo protocol number del datagrama original no está activo o que el puerto especificado no está activo.



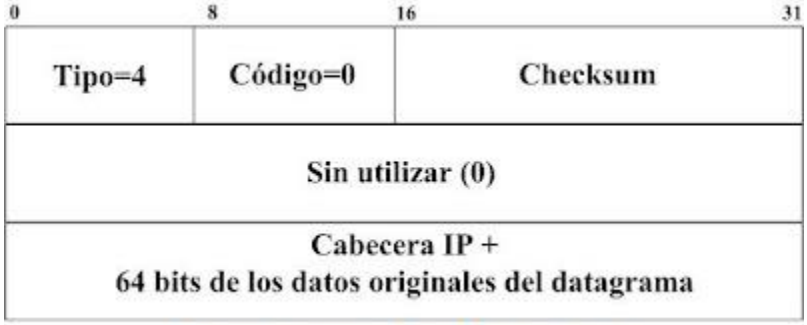
El campo código de la cabecera ICMP puede contener uno de los siguientes valores:

Código	Valor
0	Net unreachable
1	Host unreachable
2	Protocol unreachable
3	Port unreachable
4	Fragmentation needed and don't fragment bit was set
5	Source route failed
6	Destination network unknown
7	Destination host unknown
8	Source host isolated
9	Destination network is administratively prohibited
10	Destination host is administratively prohibited
11	Destination network unreacheable for type of service
12	Destination host unreacheable for type of service
13	Communication Administratively prohibited
14	Host precedence violation
15	Precedence cutoff in effect

Mensaje ICMP Source Quench (4)

Si el mensaje es recibido desde un router intermedio nos indicará que el router no tiene capacidad en los buffers para encolar el datagrama.

Si el mensaje es recibido desde el equipo destino nos indicará que los datagramas entrantes llegan demasiado deprisa para ser procesados. El campo código de la cabecera ICMP siempre será 0.



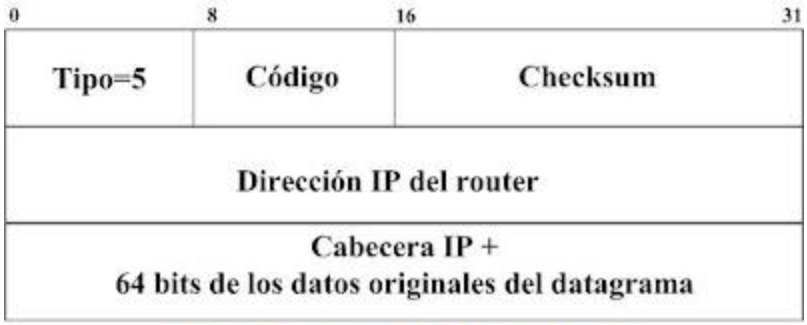
Mensaje ICMP Redirect (5)

El ICMP redirect es un mecanismo que permite a los router transmitir información de routing a los hosts. Este mensaje informa a un host para que actualice su información de routing.

Si el mensaje es recibido desde un router intermedio nos indicará que el host debe enviar futuros mensajes a un router alternativo cuya dirección IP es especificada en el mensaje ICMP. Este router alternativo deberá estar en la misma subred que el host que envía el datagrama y el router que lo devuelve.
Este mensaje no será enviado si el datagrama IP contiene información de routing.

El campo código de la cabecera ICMP puede contener, especificando la razón para la redirección, los valores siguientes:

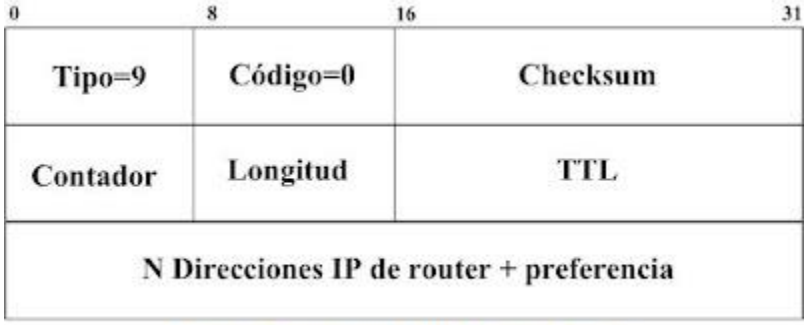
- 0. Error de red
- 1. Error de host
- 2. Error de tipo de servicio (TOS) y red
- 3. Error de tipo de servicio (TOS) y host



Mensaje ICMP Router Advertisement (9) and Router Solicitation (10)

Los mensajes de ICMP 9 y 10, de tipo Router discovery son opcionales y se encuentran descritos en la RFC 1256.
Periódicamente cada router envía mediante multicast mensajes router advertisement (RA) por cada una de sus interfaces anunciando la dirección IP de esta. Los host descubren la dirección IP de sus routers adyacentes simplemente escuchando estos mensajes. Un host, cuando se conecta a una subred, también puede enviar un mensaje multicast de router solicitation (RS) para recibir un anuncio inmediato, en vez de tener que esperar al próximo anuncio periódico. Si no recibe respuesta, retransmitirá el mensaje un número limitado de veces, tras la cuales desistirá de su solicitud.

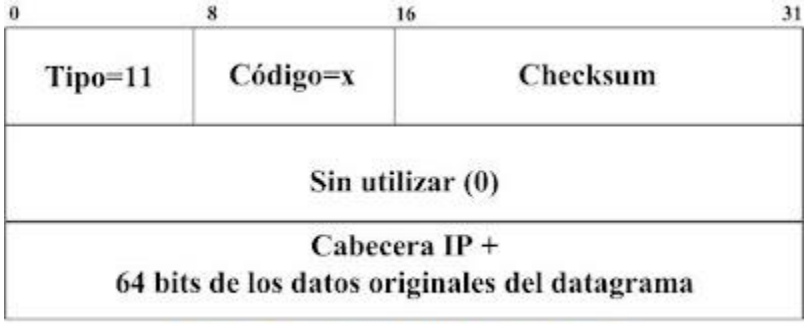
Estos mensajes para descubrir routers no constituyen un protocolo de routing. Únicamente permiten al host descubrir los routers existentes en su subred, pero no cuál de ellos es el mejor para alcanzar un destino concreto. Si un host elige uno de los routers que no es el mejor para alcanzar el destino, deberá recibir un mensaje ICMP de redirección indicándole el mejor.



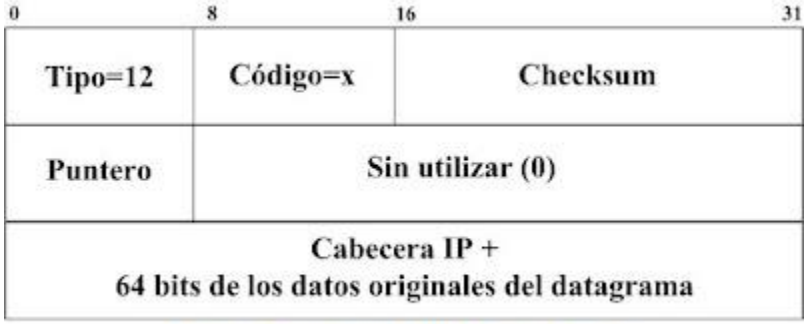
Mensaje ICMP Time exceeded (11)
Si este mensaje es recibido desde un router intermedio, nos indicará que el campo TTL de un datagrama IP ha expirado.

Si el mensaje lo recibimos desde el host destino, nos indicará que el timer TTL ha expirado durante el re-ensamblaje de un datagrama IP fragmentado (esperando a un fragmento del datagrama).

Estos mensajes son utilizados por el comando traceroute para identificar routers en el camino entre dos hosts.



Mensaje ICMP Parameter Problem (12)
Este tipo de mensaje indica que se ha encontrado un problema durante el procesamiento de los parámetros de la cabecera IP. Este mensaje es generado en respuesta a cualquier error no cubierto específicamente por otro mensaje ICMP. No es generado en respuesta a un datagrama destinado a una dirección multicast.

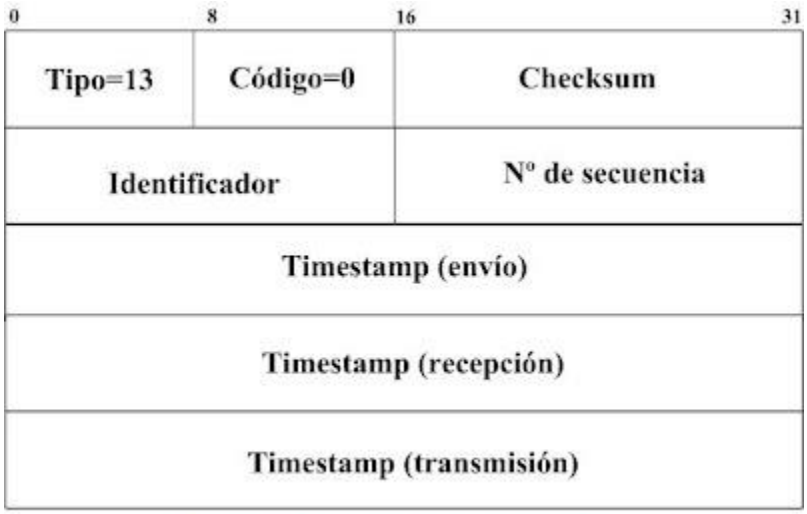


Mensajes ICMP Timestamp Request (13) and Timestamp Reply (14)

Estos dos mensajes son para debugging y medidas de rendimiento.

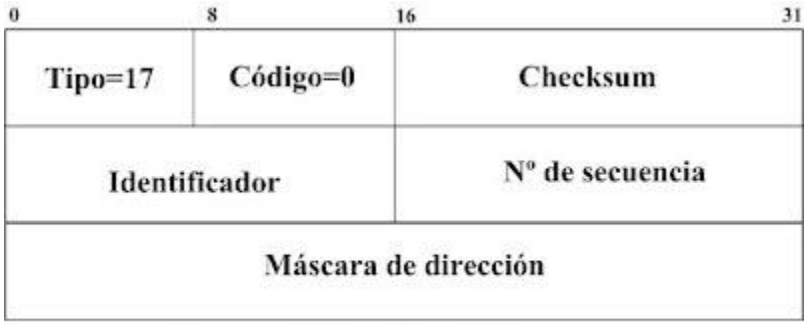
El emisor del mensaje inicializa el identificador (identifier) y el número de secuencia (sequence number; utilizado si se envían varias solicitudes), marca el timestamp y envía el datagrama al receptor. El host receptor rellena los timestamp de recepción (momento en que lo recibe) y transmisión (momento en que lo envía), cambia el tipo de mensaje a timestamp reply y se lo devuelve al emisor. Los campos identificador y número de secuencia deben volver al emisor sin alterar.

El datagrama tiene dos timestamps si hay una diferencia de tiempo perceptible entre los tiempos de recepción y transmisión. En la práctica, la mayoría de las implementaciones realizan ambos (recepción y transmisión) en una operación. Esto marca los dos tiempos con el mismo valor. Los timestamps son el número en milisegundos transcurrido desde la medianoche (UT).



Mensajes ICMP Address Mask Request (17) and Address Mask Reply (18)

El mensaje de solicitud de máscara es utilizado por un equipo para determinar la máscara de subred utilizada en la red donde está conectado. La mayoría de los equipos están configurados con su máscara, sin embargo, algunos equipos sin disco pueden obtener está información de un servidor. El equipo utiliza RARP (Reverse Address Resolution Protocol) para obtener su dirección IP. Para obtener la máscara de subred lanza una petición de máscara con el campo máscara a 0. Cualquier equipo que haya sido configurado para enviar respuestas de máscara de dirección rellena el campo de máscara de subred y devuelve el paquete al solicitante.



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.

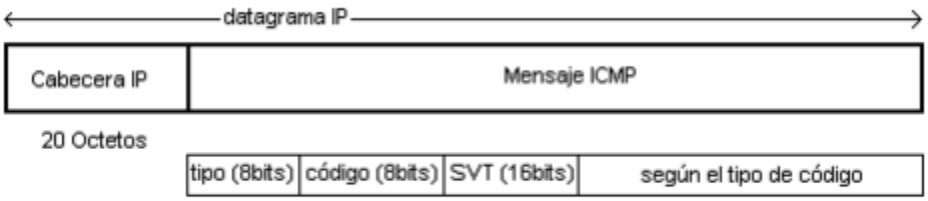


Figura 3. Esquema general de mensaje ICMP.

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.