ICMP

Internet Control Message Protocol

Protocolo de mensajería de control de internet

# Objetivo

Según [IBM](https://www.ibm.com/docs/es/aix/7.2?topic=protocols-internet-control-message-protocol):

**ICMP** es una parte necesaria de cada implementación de **IP**.

**ICMP** maneja los mensajes de error y control para **IP**. Permite a las pasarelas y los sistemas principales enviar informes de problemas a la terminal que envía un paquete.

**ICMP** realiza lo siguiente:

* Prueba si un destino está activo y es alcanzable
* Informa de los problemas de parámetros en una cabecera de datagrama
* Realiza la sincronización de reloj y las estimaciones de tiempo de tránsito
* Obtiene direcciones de Internet y máscaras de subred

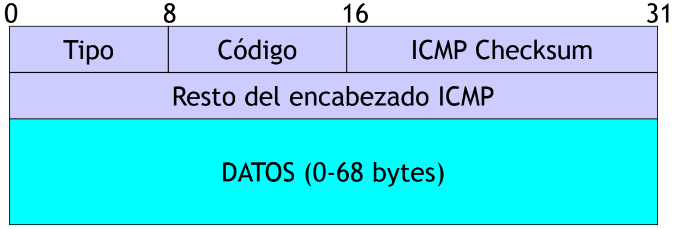
Para intercambiar datos de estado o mensajes de error, los nodos recurren al Internet Control Message Protocol (ICMP) en las redes TCP/IP. Concretamente, los servidores de aplicaciones y las puertas de acceso como los routers, usan esta implementación del protocolo IP para devolver mensajes sobre problemas con datagramas al remitente del paquete.

ICMP es un protocolo autónomo aun cuando los diferentes mensajes están incluidos en paquetes IP tradicionales. Para tal fin, el protocolo de Internet trata a la implementación opcional como un protocolo de capas superiores. Los diversos servicios de red que se suelen utilizar hoy en día, como traceroute o ping, se basan en el protocolo ICMP.

# Que hace ICMP

* Comunica errores a nivel de red.
* Informa acerca de eventos inesperados.
* Informa acerca de la red, en respuesta a consultas.
* Solo informa el error, no especifica qué acción correctiva tomar.

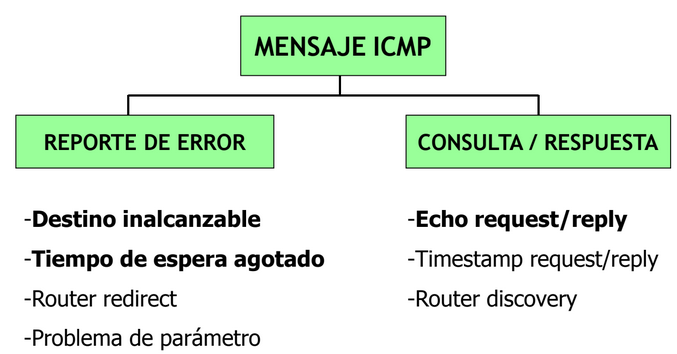
# Datagrama ICMP

****

* **Tipo (1 byte):** tipo de mensaje de error que se está generando.
* **Código (1 byte):** Código del mensaje de error.
* **ICMP Checksum (2 bytes):** Cubre todo el datagrama, garantiza la exactitud del mensaje.
* **Datos (0 a 68 bytes):** Generalmente contiene
  + Encabezado IP del datagrama que causó el error.
  + Primeros 8 bytes de datos de este datagrama.
  + Información necesaria para identificar la raíz del error.

Por ejemplo, un mensaje ICMP del tipo 3 indica que no se ha alcanzado el objetivo del paquete de datos, mientras que el código de este dato precisa y ofrece información acerca de si la red de destino (0), el host deseado (1) o el puerto esperado (3) no ha respondido a la solicitud.

# Tipos de mensaje ICMP más utilizados



## Destino inalcanzable

Ante la imposibilidad de conmutar/entregar un datagrama el router envía un mensaje ICMP antes de descartarlo.

Motivos:

* Network unreachable (0): Significa que el router no sabe cómo llegar a la red. Esto nunca sucede si tengo la default route 0.0.0.0 configurada.
* Host unreachable (1): cuando el router de la red destinataria envía un ARP request y nadie contesta.
* Protocol (TCP/UDP) not enabled.
* Port not bound to a service (3): Puerto no vinculado a ningún servicio, respuesta cuando se trata de pegar a un puerto (ej 8080) y no hay ningún servicio corriendo en él.
* Fragmentation needed, but DF flag set.
* Source route failed.

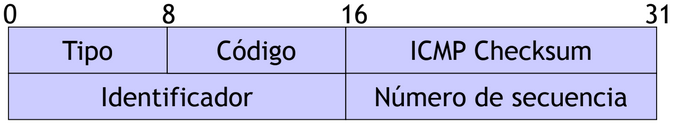
## Tiempo de espera agotado

Motivos:

* El router detecta que el campo TTL debe decrementarse a 0.
* El host destino ha desistido a la espera de un fragmento.

## Echo Request / Reply

Permite conocer si la interfaz destino es alcanzable y está funcionando.

* **Echo request:** Envía un identificador y un número de secuencia para contrastar request y replies.
* **Echo reply:** La respuesta no es obligatoria. Debe responder incluyendo los datos recibidos en el request.

Qué usa estos requests:

* PING: Si se envía un **ping utiliza un echo request y echo reply.**
* Traceroute: me permite identificar si el ruteo es correcto (ver no llegó, o si llego y no me respondió, etc). Se suele utilizar luego de un ping fallido.