

ICMP

Internet Control Message Protocol (**Protocolo de mensajería de control de internet**).

Surge para **intentar resolver algunas incertidumbres de IP originadas por no estar orientado a la conexión**.

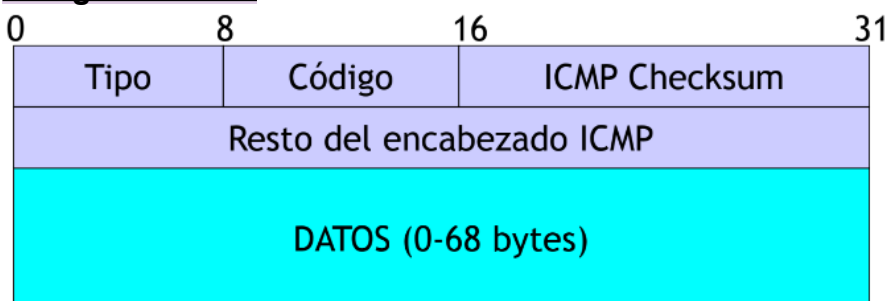
Para **intercambiar datos de estado o mensajes de error**, los nodos recurren al Internet Control Message Protocol (ICMP) en las redes TCP/IP. Concretamente, los servidores de aplicaciones y las puertas de acceso como los **routers**, **utilizan esta implementación del protocolo IP para devolver mensajes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

Por definición, 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 que acción correctiva tomar**.

Datagrama ICMP



Tipo: Informa que **tipo de mensaje de error** se esta generando.

Código: Código del mensaje de error.

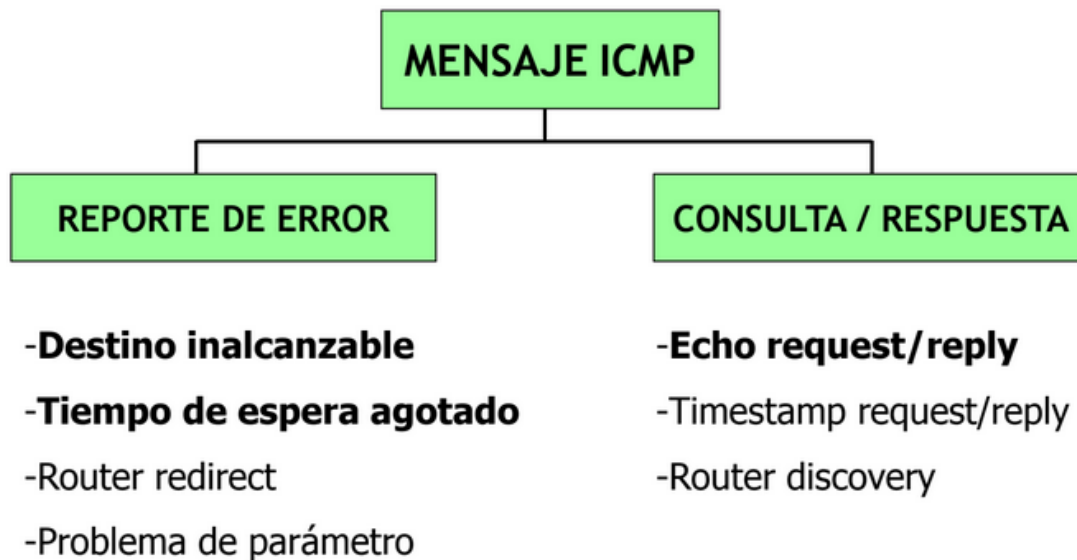
Por ejemplo, un mensaje ICMP del tipo 3 indica que no se ha alcanzado el objetivo del paquete de datos, mientras que el código de este dato precisa y ofrece información acerca de si la red de destino (0), el host deseado (1) o el puerto esperado (3) no ha respondido a la solicitud.

ICMP Checksum: Cubre todo el datagrama, garantiza la exactitud del mensaje.

Datos: Generalmente contiene

- **Encabezado IP del datagrama** que causo el error.
- **Primeros 8 bytes de datos** de este datagrama.
- Información necesaria para **identificar la raíz del error**.

Tipos de mensaje ICMP mas utilizados



Destino inalcanzable

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

Motivos:

- **Network unreachable:** esto nunca sucede si tengo el router default 0.0.0.0 seteado, significa que el **router no sabe como llegar a la red**.
- **Host unreachable:** sucede 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:** Puerto no vinculado a ningún servicio, respuesta cuando **se trata de pegar a un puerto (ej 8080) y no hay ningún servicio corriendo en el**.
- **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

Utilizado **para 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.

0	8	16	31
Tipo	Código	ICMP Checksum	
Identificador		Número de secuencia	

Si se envía un **ping** utiliza un **echo request** y **echo reply**.

Traceroute: me permite identificar si el ruteo es correcto (ver no llego, o si llego y no me respondió, etc). Se suele utilizar luego de un ping fallido.