Tema 1.1

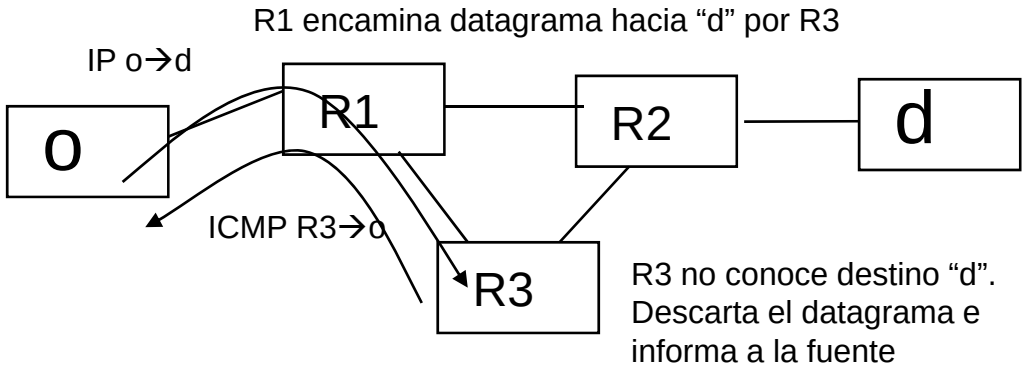
ICMP
(Internet Control Message Protocol)

Transmisión de mensajes de control en redes IP

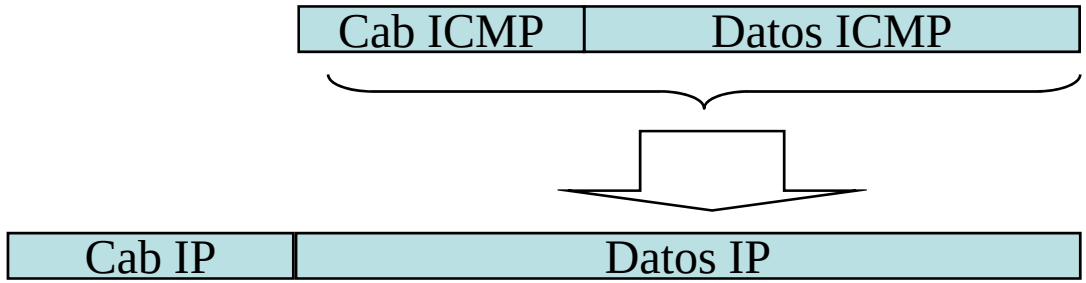
Índice

Introducción

- Las redes IP no aseguran al origen la llegada de datagramas al destino. Pueden producirse pérdidas de datagramas en el camino.
- ICMP es parte obligatoria de la implementación IP.
- Objetivos ICMP:
  - Que la fuente de un datagrama pueda ser informada de un error en la transmisión del mismo. El generador del mensaje ICMP es el dispositivo que ha detectado el error.
  - Cualquier máquina o router puede enviar un mensaje ICMP a otra máquina/router, informándole de distintas situaciones.
- Habitualmente, la fuente al ser informada de un problema, no puede hacer nada para solucionarlo. Ejemplo: Informar de problemas de encaminamiento de un datagrama.



Formato de mensaje ICMP (I)



- Cabecera ICMP
  - 1 byte de campo tipo (TYPE) --> identifica el mensaje
  - 1 byte de campo código (CODE) --> más información del tipo de mensaje
  - 2 bytes de campo CHECKSUM (calculado solo sobre cabecera + datos ICMP)
- Datos ICMP --> Mensajes que informan de errores incluyen (Cabecera IP + 8 primeros bytes de datos del datagrama que causó el problema)
  - Objetivo: Dar más información a la fuente para que pueda entender el problema

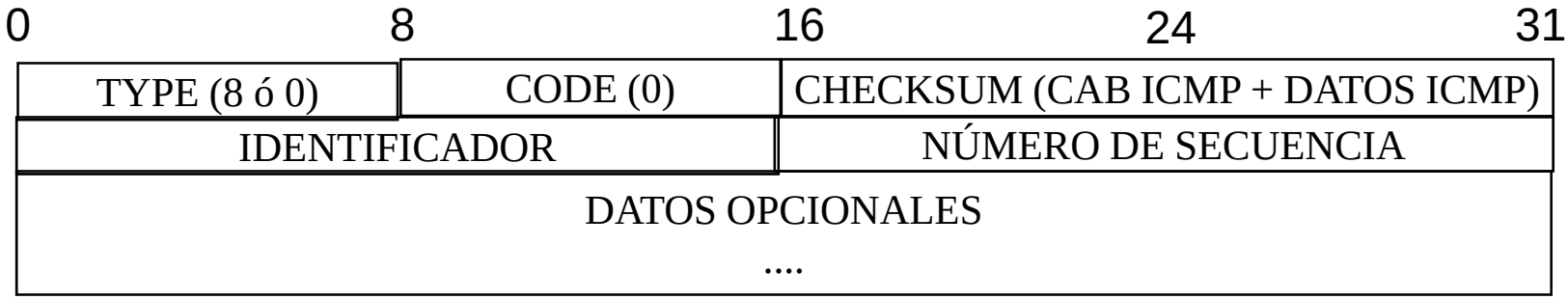
Formato de mensaje ICMP (II)

Campo Tipo	Tipo de mensaje ICMP
0	Mensaje Echo Reply *(ping)*
3	Destino inalcanzable
4	Disminución de origen
5	Redireccionar (cambiar una ruta)
8	Mensaje Echo Request *(ping)*
11	Tiempo excedido para un datagrama
12	Problema de parámetros en un datagrama
13	Solicitud de *timestamp*
14	Respuesta de *timestamp*
15	Solicitud de información (obsoleto)
16	Respuesta de información (obsoleto)
17	Solicitud de máscara de red
18	Respuesta a solicitud de máscara de red

Solicitud de eco *(ping)* (I)

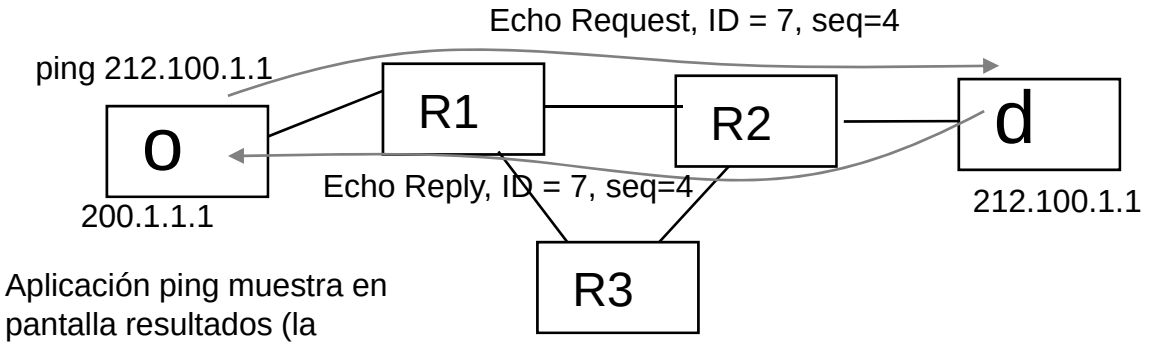
- *Ping:* herramienta de depuración de redes.
  - Solicitud: A genera mensaje ICMP *echo request* con destino dirección IP B. La solicitud contiene un área de datos opcionales.
  - Respuesta: Si B recibe el mensaje, genera un mensaje ICMP *echo reply* de respuesta, con destino A. La respuesta contiene una copia de los datos de la solicitud, en caso de estar incluidos.
- *Ping* correcto =>
  - Software IP de origen y destino correctos.
  - Existe ruta configurada en routers intermedios.
- *Ping* incorrecto =>
  - No se produce lo anterior,
  - O todo es correcto, pero el destino está configurado para no responder a los *echo request*.
- Versiones sofisticadas de herramienta *ping*:
  - proporcionan estadísticas (retardo y pérdidas)
  - permiten especificar TTL de datagrama que se envía
  - permiten especificar tamaño datos opcionales, y latencia entre consultas "eco"

Solicitud de eco *(ping)* (II)



- Formato:
  - Campo *datos opcionales*: tamaño variable.
  - Los campos *identificador* y *número de secuencia* son utilizados por el iniciador del *ping* para poder asociar respuestas *ping a* consultas *ping.*

Solicitud de eco *(ping)* (III)



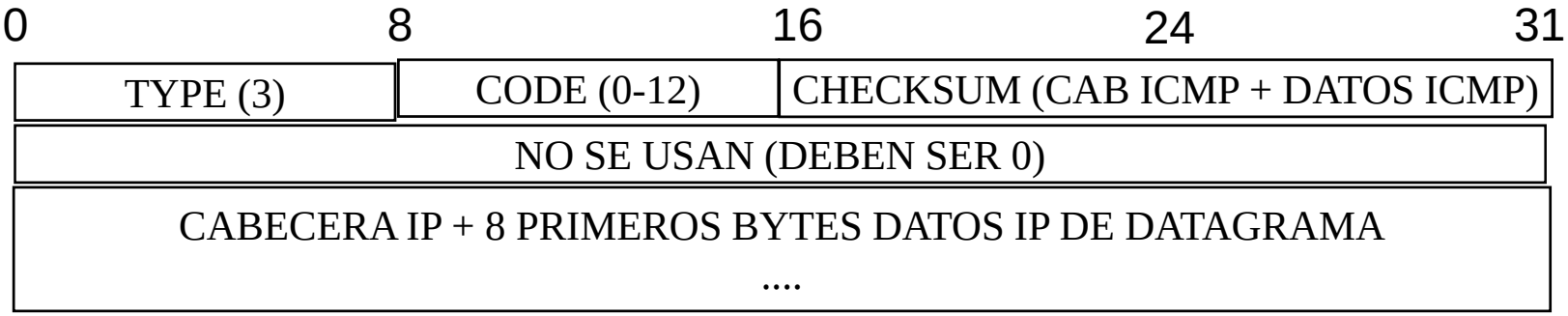
Software ICMP recibe *echo request*. Si no está bloqueada esta opción, genera *echo reply*.

Aplicación ping muestra en pantalla resultados (la forma depende de la aplicación)

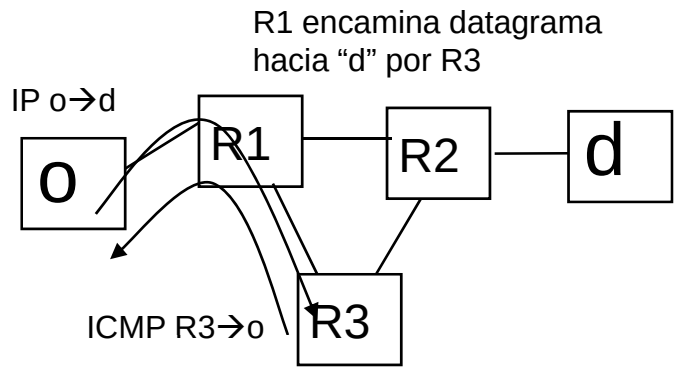
```
~ > ping 192.168.5.1
PING 192.168.5.1 (192.168.5.1): 56 data bytes
64 bytes from 192.168.5.1: icmp_seq=0 ttl=128 time=0.550 ms
64 bytes from 192.168.5.1: icmp_seq=1 ttl=128 time=0.248 ms
64 bytes from 192.168.5.1: icmp_seq=2 ttl=128 time=0.253 ms
64 bytes from 192.168.5.1: icmp_seq=3 ttl=128 time=0.244 ms
64 bytes from 192.168.5.1: icmp_seq=4 ttl=128 time=0.249 ms
64 bytes from 192.168.5.1: icmp_seq=5 ttl=128 time=0.241 ms
--- 192.168.5.1 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.241/0.297/0.550 ms
~ >
```

Destino inalcanzable (I)

- Cuando un router recibe un datagrama que no es para él, y no es capaz de encaminar (no encaja en ninguna entrada de la tabla de encaminamiento, que no tiene encaminamiento por defecto) => genera mensaje ICMP a IP origen de datagrama



- Campo CODE: Identifica tipo de problema que provoca mensaje. Ejemplos:
  - Host / red destino inaccesible
  - Necesidad de fragmentación, y bit *not-fragment* activado
  - Encaminamiento de fuente con errores
  - …

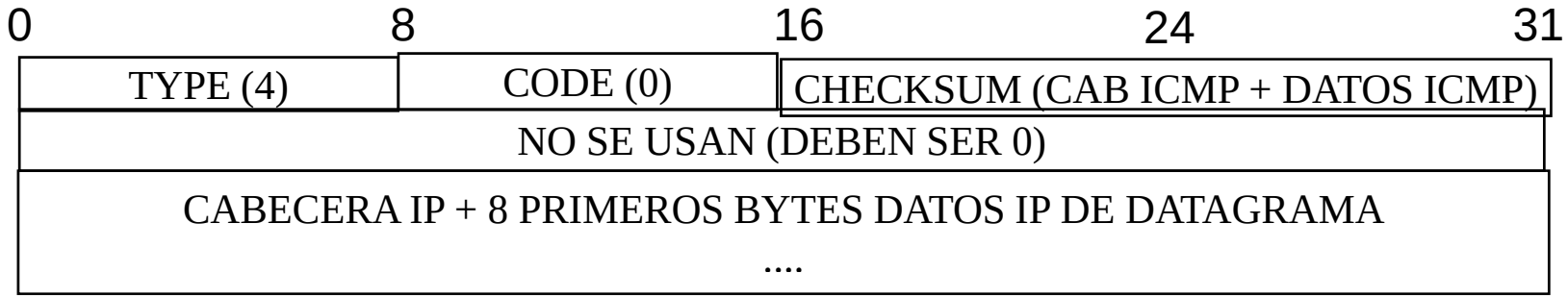


Destino inalcanzable (II)

Campo Code	Tipo de mensaje ICMP
0	Red inacesible
1	Anfitrión inaccesible
2	Protocolo inaccesible
3	Puerto inaccesible
4	Se necesita fragmentación y bit DF=1
5	Falla en la ruta origen
6	Red de destino desconocida
7	Anfitrión de destino desconocido
8	Anfitrión de origen aislado
9	Comunicación con red destino administrativamente prohibida
10	Comunicación con anfitrión destino adm. prohibida
11	Red inaccesible por el tipo de servicio
12	Anfitrión inaccesible por el tipo de servicio

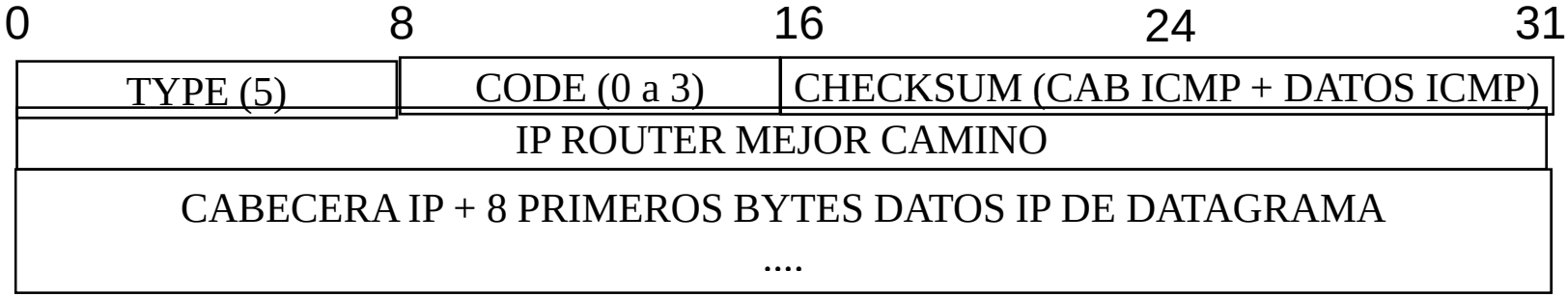
Disminución de fuente

- Memorias del router se congestionan --> debe comenzar a descartar datagramas.
- En general:
  - para cada datagrama descartado, genera mensaje de *disminución de fuente*, dirigido a la fuente que generó ese datagrama.
  - las fuentes que reciben estos datagramas actúan (no hay mensaje de respuesta), disminuyendo el tráfico que generan, hasta que dejen de recibir mensajes
- Otros comportamientos más sofisticados:
  - Routers detectan fuente que más genera y únicamente envían mensajes de disminución a ellas.
  - Routers monitorizan estado de sus colas de paquetes. Antes de que suceda congestión (y se deban descartar datagramas), envían mensajes de disminución preventivos.



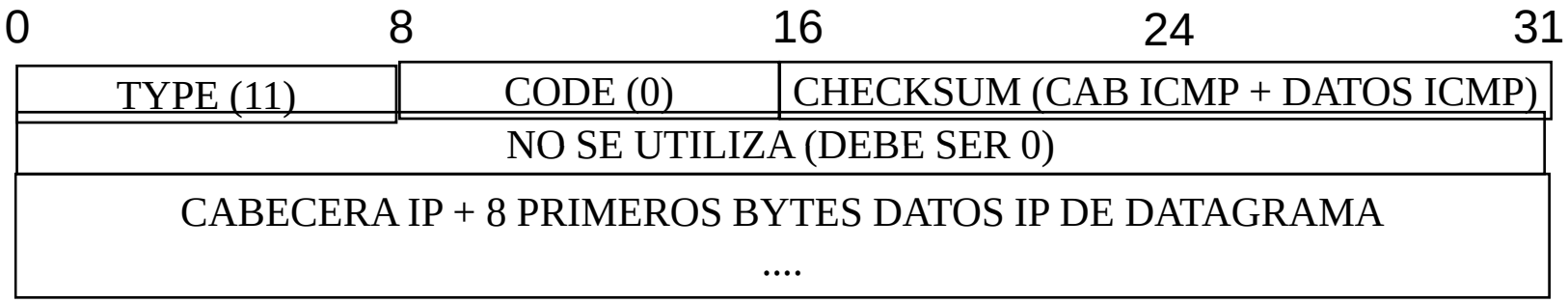
Solicitud de cambio de ruta (desde router)

- Sea una red de PCs con varios posibles gateways. Algunos destinos se alcanzan más rápidamente por un gateway que por el otro.
- La tabla de encaminamiento de los PCs debe distinguir destinos encaminados a través de un gateway y a través del otro.
- Mecanismo para simplificar gestión de PCs:
  - las tablas de encaminamiento de los PCs se mantienen sencillas: regla sencilla para elegir entre los gateways.
  - Estos “routers de 1º salto”, se configuran para que si reciben un datagrama cuyo destino se alcanza más rápidamente por otro router de 1º salto, se lo indiquen así al origen (mensaje ICMP *source route failed*, con código *redirect*).

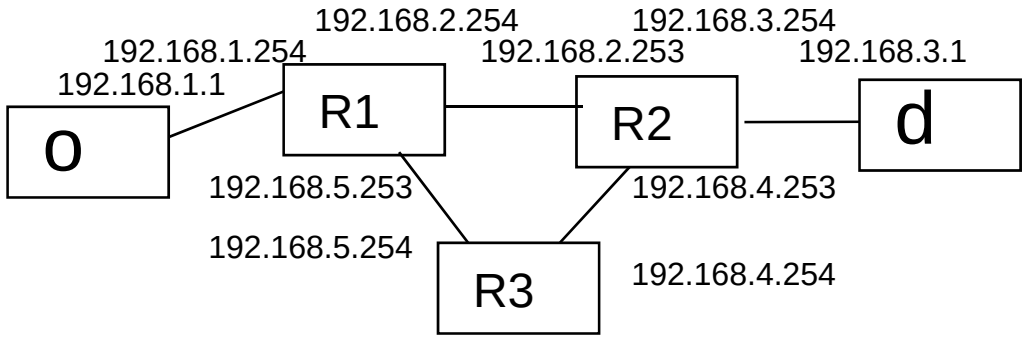


TTL Excedido

- Al recibir un datagrama, el router decrementa el valor del campo TTL, y luego lo observa. En caso de ser igual a 0, descarta el datagrama (no lo encamina).
- En este momento, el router genera un mensaje ICMP hacia el origen, indicando este suceso.



Herramienta *traceroute* (I)



- Desde 192.168.1.1 → traceroute 192.168.3.1
  - Mensaje echo request a 192.168.3.1 (TTL=1)
    - 192.168.1.254 genera ICMP.TTL excedido destinado a 192.168.1.1
    - 192.168.1.1 reconoce el echo request que se ha descartado a través de ID/Seq
    - 192.168.1.1 sabe que 192.168.1.254 está a 1 salto
  - Mensaje echo request a 192.168.3.1 (TTL=2)
    - 192.168.2.253 genera ICMP.TTL excedido destinado a 192.168.1.1
    - 192.168.1.1 reconoce el echo request que se ha descartado a través de ID/Seq
    - 192.168.1.1 sabe que 192.168.2.253 está a 2 saltos
  - Mensaje echo request a 192.168.3.1 (TTL=3)
    - 192.168.3.1 genera ICMP.echo reply destinado a 192.168.1.1
    - 192.168.1.1 reconoce el echo request original, a través de ID/Seq
    - 192.168.1.1 sabe que 192.168.3.1 está a 3 saltos

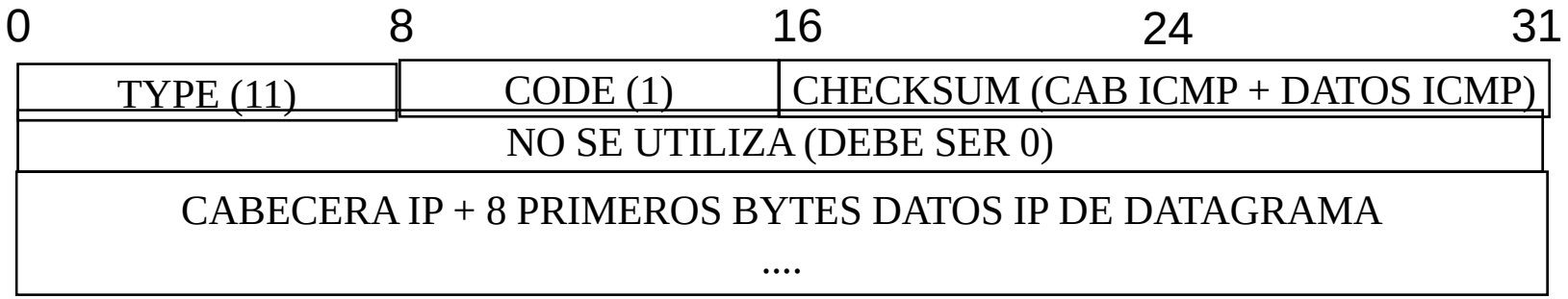
Herramienta *traceroute* (II)

```
C:\Documents and Settings\root>tracert -d www.rediris.es

Traza a la dirección sun.rediris.es [130.206.1.2]
sobre un máximo de 30 saltos:

  1    <1 ms    <1 ms    <1 ms  212.128.45.253
  2     1 ms     1 ms    <1 ms  212.128.20.152
  3     1 ms    <1 ms    <1 ms  172.16.1.1
  4     *        *        *     Tiempo de espera agotado para esta solicitud.
  5     4 ms     4 ms     4 ms  130.206.208.5
  6    15 ms    15 ms    14 ms  130.206.240.69
  7    26 ms    26 ms    25 ms  130.206.240.17
  8    26 ms    26 ms    26 ms  130.206.220.66
  9    26 ms    25 ms    26 ms  130.206.1.2

Traza completa.

C:\Documents and Settings\root>
```

- Distintos echo request pueden ir encaminados por rutas distintas. La aplicación *traceroute* puede detectar e informar de esta diversidad de rutas.
- Algunos routers pueden estar configurados para no generar mensajes TTL-exceeded: En la lista aparecen como saltos intermedios desconocidos.

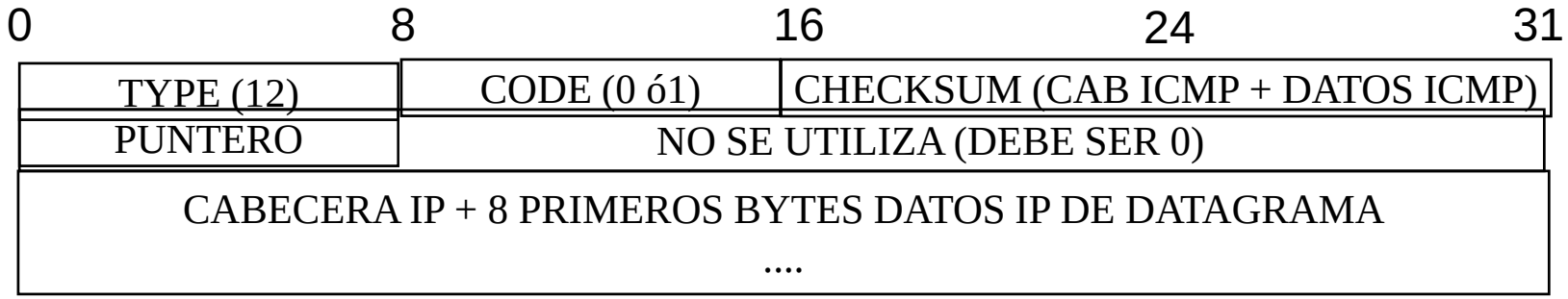
Tiempo fragmentación excedido

- El router recibe un datagrama destinado a él, que es un fragmento. Comienza el contador de fragmentación. Si este contador se agota => error de tiempo excedido de fragmentación



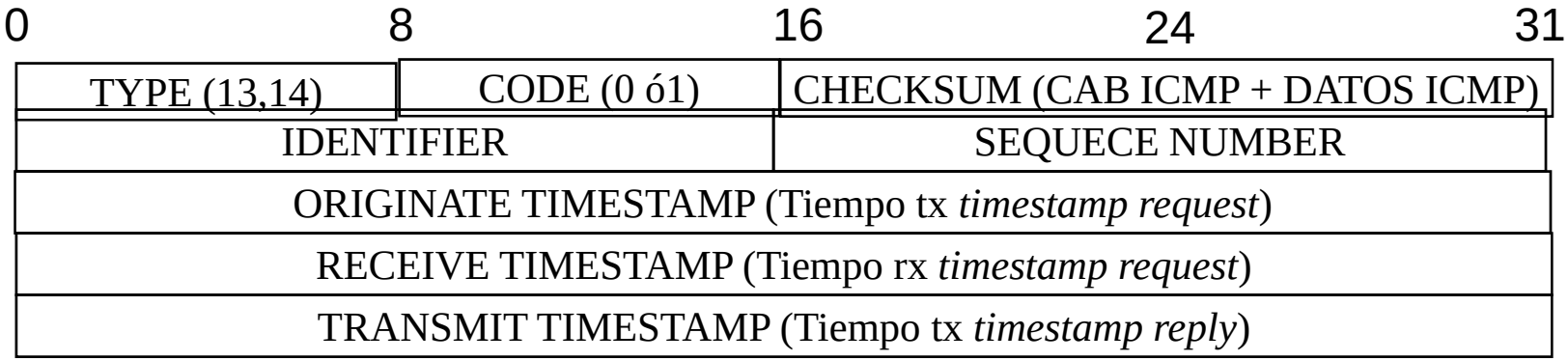
Otros errores

- Si el router detecta otros errores, no contemplados anteriormente (típicamente, error de formato en el campo de opciones del datagrama), se envía un mensaje de error genérico.
- El campo PUNTERO apunta a la posición en el datagrama original donde se ha producido el error al procesar el datagrama.



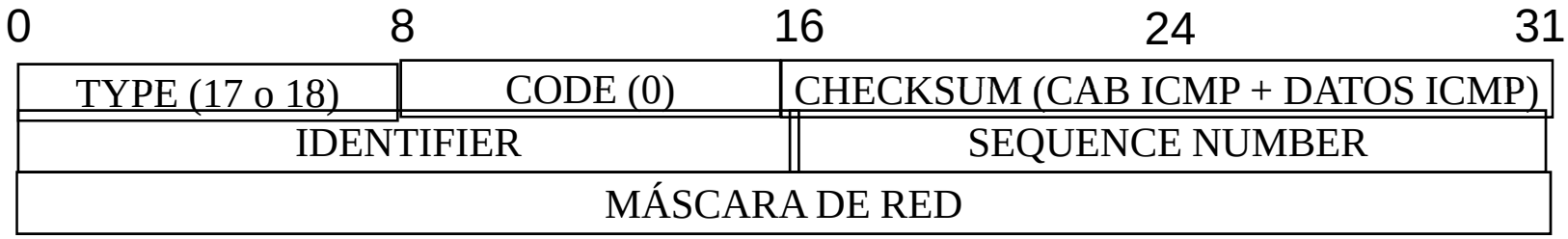
Sincronización de relojes

- Máquinas dentro de un sistema distribuido: existe necesidad de sincronización de relojes.
- Una máquina puede enviar una petición de sello temporal *(timestamp request)* a otra. La máquina responde con el mensaje *timestamp reply* completando los campos del mensaje.
- En general, se necesitan muchos mensajes de este tipo + tratamiento estadístico para poder estimar retardo entre dos routers



Obtención de máscara de subred

- En un entorno de direccionamiento de subred, una máquina debe conocer la máscara de red de su dirección IP propia, para cada interfaz.
- Una máquina que en el arranque no conozca su máscara de red, puede mandar un mensaje *address mask request* (campo *type* 17) a un router en su red física, o por broadcast.
- La respuesta es enviada por el router en un mensaje *address mask reply* (campo *type* 18).



Bibliografía recomendada

- Douglas E. Comer, “Internetworking with TCP/IP Vol. 1: Principles, Protocols, and Architecture. 5th Edition”, Prentice Hall 2006.
  - Capítulo 8: “Internet Protocol: Error and Control Messages (ICMP)”.
- RFC 792 (ICMP, Internet Control Message Protocol)