

Índice hora 2

Hora 1

1 Introducción

2 ARP

3 Asignación automática de direcciones IP

3.1 RARP

3.2 BOOTP/DHCP

Hora 2

4 ICMP

4.1 Cabecera ICMP básica

4.2 Tipos de mensajes ICMP

4.3 Mensajes ICMP de error

Hora 3

4.4 Mensajes ICMP petición/respuesta

5 IGMP

6 Evolucionando IP: IPv6

Objetivos

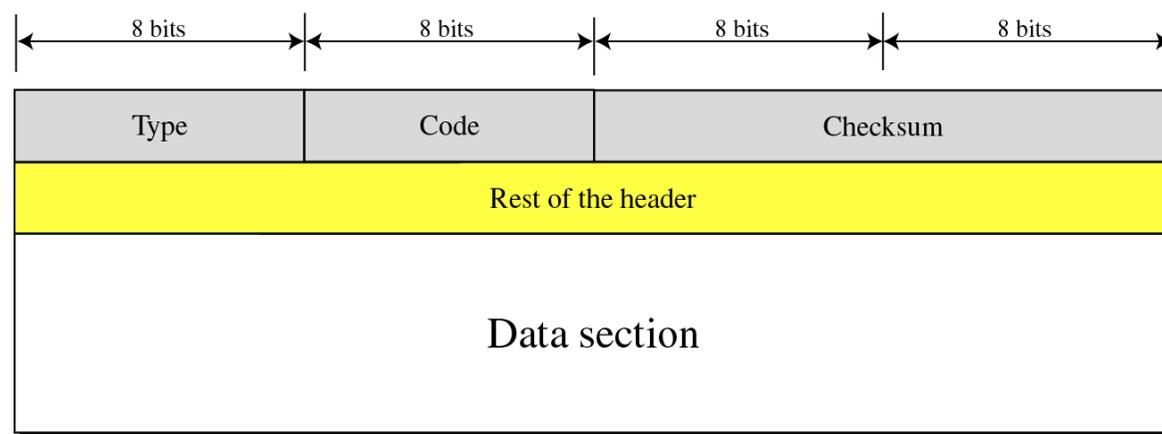
- Entender la necesidad de protocolos que acompañen a IP para:
 - Notificar errores
 - Diagnosticar el estado de la red
- Revisar los eventos relacionados con errores a nivel IP que implican una notificación hacia el origen del paquete que ocasionó el error

4 ICMP

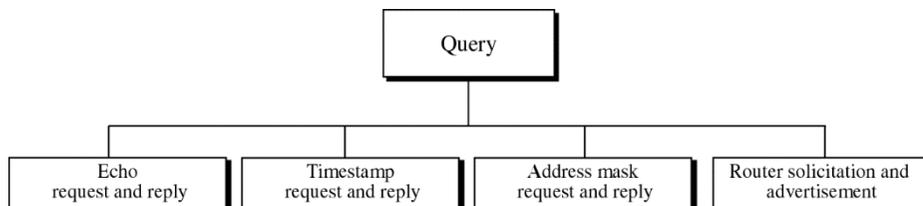
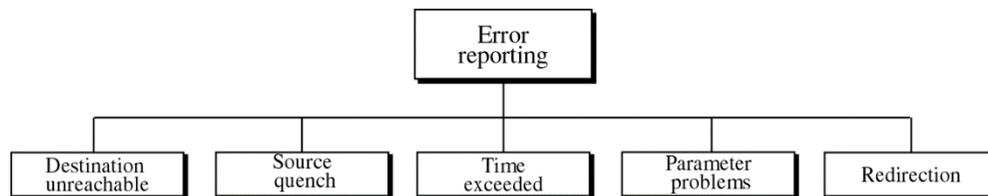
- Internet Control Message Protocol.
- ICMP compensa las deficiencias de IP en cuanto a:
 - Falta de control de errores.
 - Falta de mecanismos de diagnóstico.
- ICMP es un protocolo que hace funciones de nivel de red pero se encapsula dentro de datagramas IP (Protocol=1 de la cabecera IP).
- Tipos de mensajes ICMP:
 - De error: informa sobre un problema en un router o en una máquina.
 - De petición: útiles para conseguir información específica de un router o una máquina. Se producen por pares petición-respuesta.

4.1 Cabecera ICMP básica

- Type (8bits): tipo de mensaje ICMP.
- Code (8bits): código propio a cada tipo de mensaje ICMP.
- Checksum (16bits): se calcula sobre la cabecera + datos ICMP aplicando el mismo algoritmo de checksum que la cabecera IP.
- Rest of the header (32 bits): campos de cabecera propios para cada tipo de mensaje.
- Data section: tamaño variable con datos propios según tipo.



4.2 Tipos de mensajes ICMP

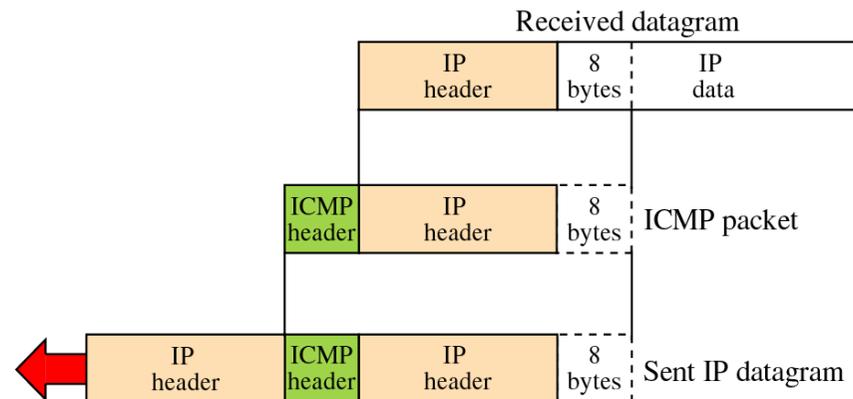


Type	Name	References
0	Echo Reply	RFC 792
1	Unassigned	
2	Unassigned	
3	Destination Unreachable	RFC 792
4	Source Quench	RFC 792
5	Redirect	RFC 792
6	Alternate Host Address	JBP
7	Unassigned	
8	Echo	RFC 792
9	Router Advertisement	RFC 1256
10	Router Solicitation	RFC 1256
11	Time Exceeded	RFC 792
12	Parameter Problem	RFC 792
13	Timestamp	RFC 792
14	Timestamp Reply	RFC 792
15	Information Request	RFC 792
16	Information Reply	RFC 792
17	Address Mask Request	RFC 950
18	Address Mask Reply	RFC 950

4.3 Mensajes ICMP de error

- Reporta errores (no los corrige, será labor ésta de niveles superiores).
- Siempre se envían al emisor original del paquete que ocasionó el error, porque se tiene su dirección IP como IP origen del paquete original.
- Todos los mensajes de error ICMP incluyen en el campo *data section* la cabecera IP del datagrama original seguido de los 8 primeros bytes de datos del datagrama original.

Los 8 bytes se eligen porque para TCP/UDP incluyen la información de puertos y número de secuencia (sólo TCP), para que así el origen pueda informar a niveles superiores.



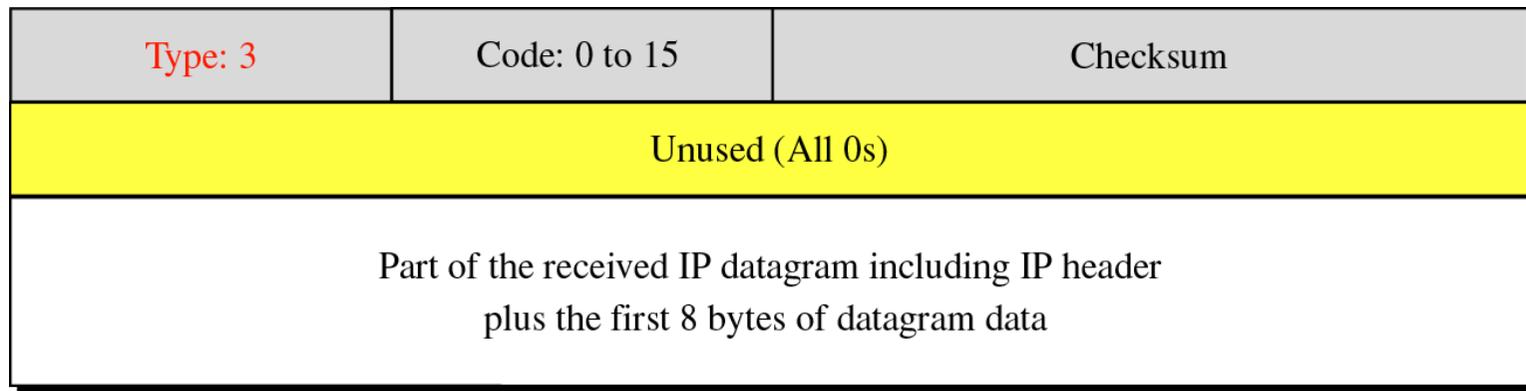
Mensajes ICMP de error

- Para evitar tormentas ICMP de error, nunca se generan en respuesta a:
 - Otro ICMP de error.
 - Un fragmento IP que no sea el primero.
 - Un datagrama destinado a una dirección IP de broadcast o multicast.
 - Un datagrama cuya dirección IP origen no haga referencia a una única máquina: loopback, broadcast, multicast y 0.0.0.0.

- En estos casos el paquete deberá ser descartado silenciosamente y el evento debería quedar registrado (log).

4.3.1 ICMP error: Destino inalcanzable

- Cuando un router no puede encaminar un datagrama o una máquina destino no puede entregarlo a niveles superiores, el datagrama se tira y el router o máquina manda un mensaje de vuelta de este tipo.
- Type=3
- Code=0...16 (\Rightarrow)
- Rest of Header=0 (sin uso)



ICMP error: Destino inalcanzable

Code	Definition
0	Net Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation Needed and Don't Fragment was Set
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Communication with Destination Network is Administratively Prohibited
10	Communication with Destination Host is Administratively Prohibited
11	Destination Network Unreachable for Type of Service
12	Destination Host Unreachable for Type of Service
13	Communication Administratively Prohibited
14	Host Precedence Violation
15	Precedence Cutoff in Effect

ICMP error: Destino inalcanzable

- 0: Net Unreachable
 - Lo manda un router cuando conoce la red destino pero esa red o un enlace intermedio no está activo en ese momento.
- 1: Host Unreachable
 - Lo manda un router cuando conoce la red destino pero la máquina no está activa.
- 2: Protocol Unreachable
 - Lo manda una máquina (o el router si es el destinatario final) indicando que el protocolo indicado en el paquete no se puede procesar (no soportado o no activo).
- 3: Port Unreachable
 - Lo manda una máquina (o el router si es el destinatario final) indicando que el proceso o aplicación al que se refiere el paquete no se puede alcanzar en ese destino.

ICMP error: Destino inalcanzable

- 4: Fragmentation Needed and Don't Fragment was Set
 - Lo manda un router para indicar que no ha podido enviar el paquete porque el bit Don't Fragment de la cabecera IP está activo y era necesario fragmentar el paquete para poderse reenviar.
 - En Rest of Header incluye la MTU para la que necesitaba fragmentar
- 5: Source Route Failed
 - Lo manda un router para indicar que no puede utilizar el encaminamiento fuente estricto o débil de la cabecera IP.
- 6: Destination Network Unknown
 - Obsoleto. Se utiliza el de código 7 en su lugar.
- 7: Destination Host Unknown
 - Lo manda un router para indicar que no conoce la red destino ni cómo acceder a ella.
- 8: Source Host Isolated
 - Obsoleto. Anteriormente se utilizaba para indicar que la máquina destino se encontraba aislada y no era posible reenviarle paquetes.

ICMP error: Destino inalcanzable

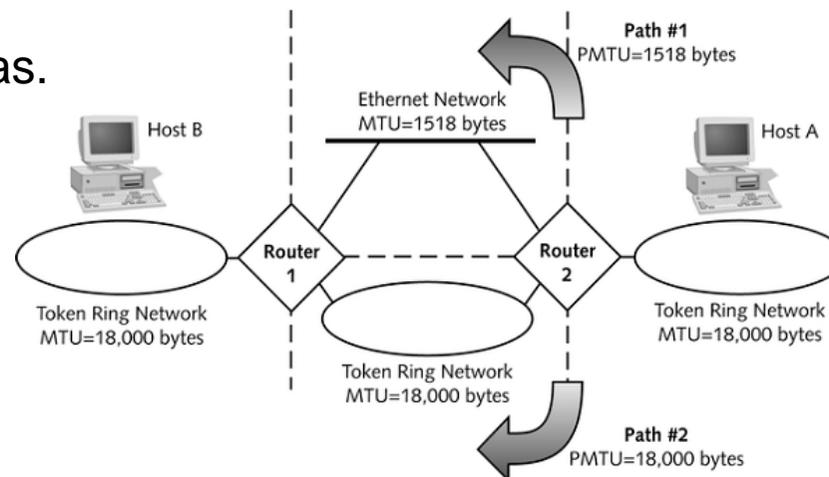
- 9: Communication with Destination Network is Administratively Prohibited
 - Lo manda un router para indicar que fue configurado para bloquear el acceso a la red destino deseada.
- 10: Communication with Destination Host is Administratively Prohibited
 - Lo manda un router para indicar que fue configurado para bloquear el acceso a la máquina destino deseada.
- 11: Destination Network Unreachable for Type of Service
 - Lo manda un router para indicar que no dispone del Tipo de Servicio declarado en la cabecera IP del paquete para acceder a esa red.
- 12: Destination Host Unreachable for Type of Service
 - Lo manda un router para indicar que no dispone del Tipo de Servicio declarado en la cabecera IP del paquete para acceder a esa máquina.

ICMP error: Destino inalcanzable

- 13: Communication Administratively Prohibited [RFC1812]
 - Lo manda un router para indicar al origen que no puede reenviar el paquete porque lo prohíben las reglas de filtrado de paquetes.
- 14: Host Precedence Violation [RFC1812]
 - Lo manda un router para indicar que no puede reenviar el paquete porque el campo prioridad de la cabecera IP no está permitido para ese origen, destino, protocolo o puerto.
- 15: Precedence cutoff in effect [RFC1812]
 - Lo manda un router para indicar que el paquete no tiene el mínimo valor de prioridad de la cabecera IP requerido por el administrador para obtener servicio (situaciones transitorias de congestión).

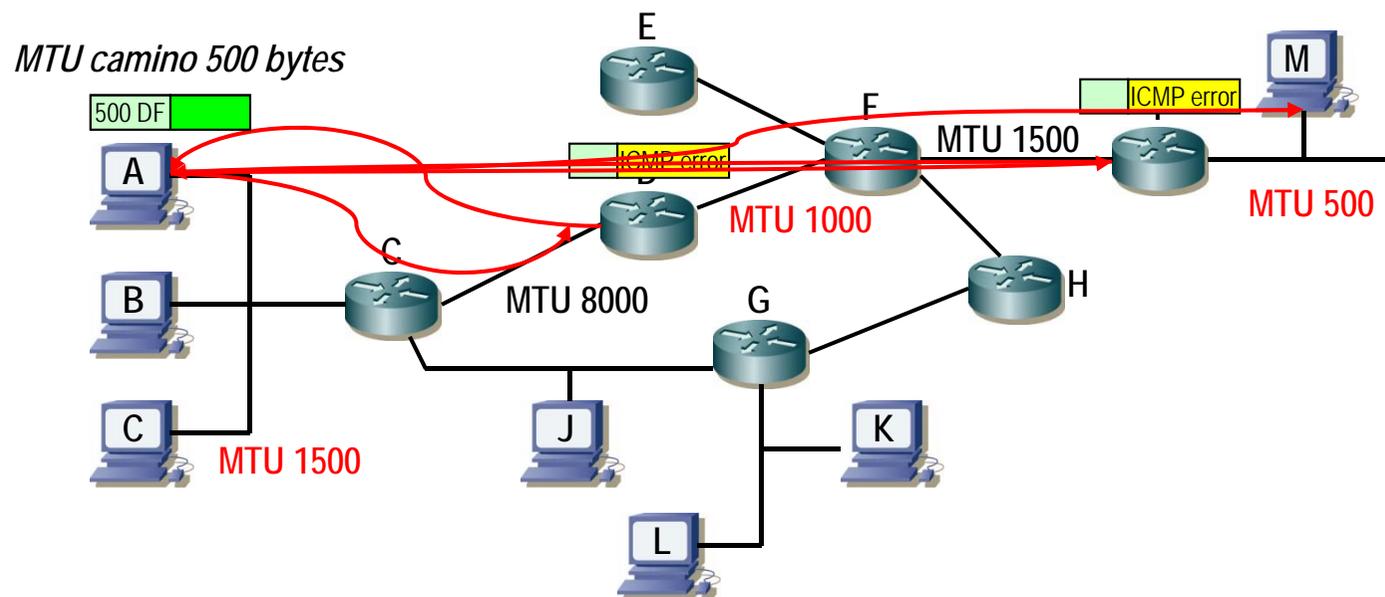
ICMP error: Destino inalcanzable

- Ejemplo de aplicación: **Descubrimiento de la MTU del camino**
 - Se mandan los paquetes con el bit Don't Fragment de la cabecera IP activo, empezando con tamaño marcado por la MTU de la red origen.
 - Si en algún salto intermedio la MTU es más pequeña, se retornará un paquete ICMP de error de destino inalcanzable de código 4.
 - El origen podrá entonces reducir el tamaño del paquete (teniendo en cuenta los valores de MTUs típicos) hasta encontrar un tamaño de paquete que no reciba el ICMP de error de destino inalcanzable de código 4.
 - Problema: variabilidad de rutas.



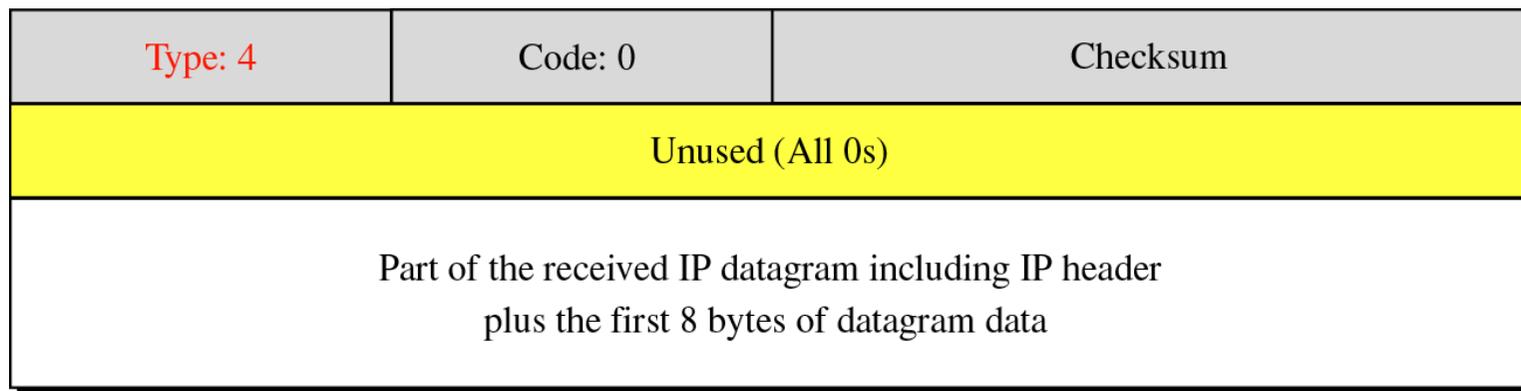
ICMP error: Destino inalcanzable

- Ejemplo de aplicación: *Descubrimiento de la MTU del camino*



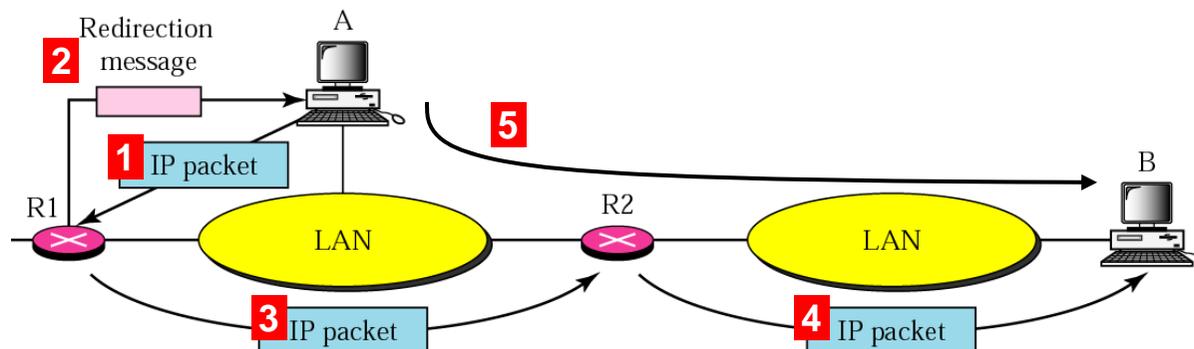
4.3.2 ICMP error: Source-quench

- Indica que un router intermedio o el destino no disponen de suficiente espacio en cola (buffers) en situaciones de congestión y que por tanto ha sido necesario tirar el paquete.
- Efecto de ralentización en el emisor.
- Type=4
- Code=0
- Rest of Header=0 (sin uso)



4.3.3 ICMP error: Redirección

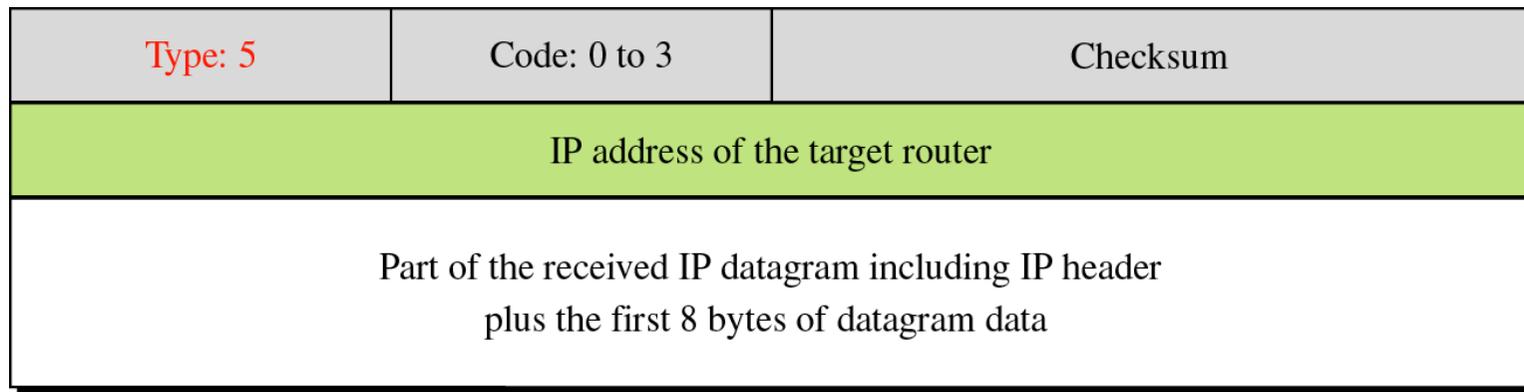
- Normalmente una máquina sólo tiene configurado un router que es el de por defecto. Si la máquina manda un paquete a través de ese router pero el camino es erróneo para alcanzar el destino **1**, ese router por defecto mandará un ICMP de redirección al origen informándole de la IP del router de salida correcto **2**.
- Ese primer paquete se reenvía correctamente al destino aunque se mande el ICMP de redirección **3 4**: el origen estará enterado para la siguiente vez.
- Para siguientes paquetes, el origen los enviará a través del nuevo router de salida **5**.



A quiere enviar a B y tiene como router por defecto R1 que no es el correcto para ese destino.

ICMP error: Redirección

- Type=5
- Code:
 - 0: redirección a ruta específica para la red.
 - 1: redirección a ruta específica para la máquina.
 - 3: redirección a ruta específica para la red y el TOS.
 - 4: redirección a ruta específica para la máquina y el TOS.
- Rest of Header: dirección IP del router al que se redirige.



4.3.4 ICMP error: Tiempo excedido

- Type=11
- Code:
 - 0: el TTL del datagrama ha llegado a 0 y se ha descartado.
 - 1: no han llegado al destino todos los fragmentos en el límite de tiempo y se han descartado todos los que había. Debe haber recibido el 1^{er} fragmento para tener los datos que adjunta el ICMP (cabecera IP + 8bytes de datos).
- Rest of Header: 0 (sin uso)
- La aplicación *traceroute* hace uso de este mensaje (code 0).

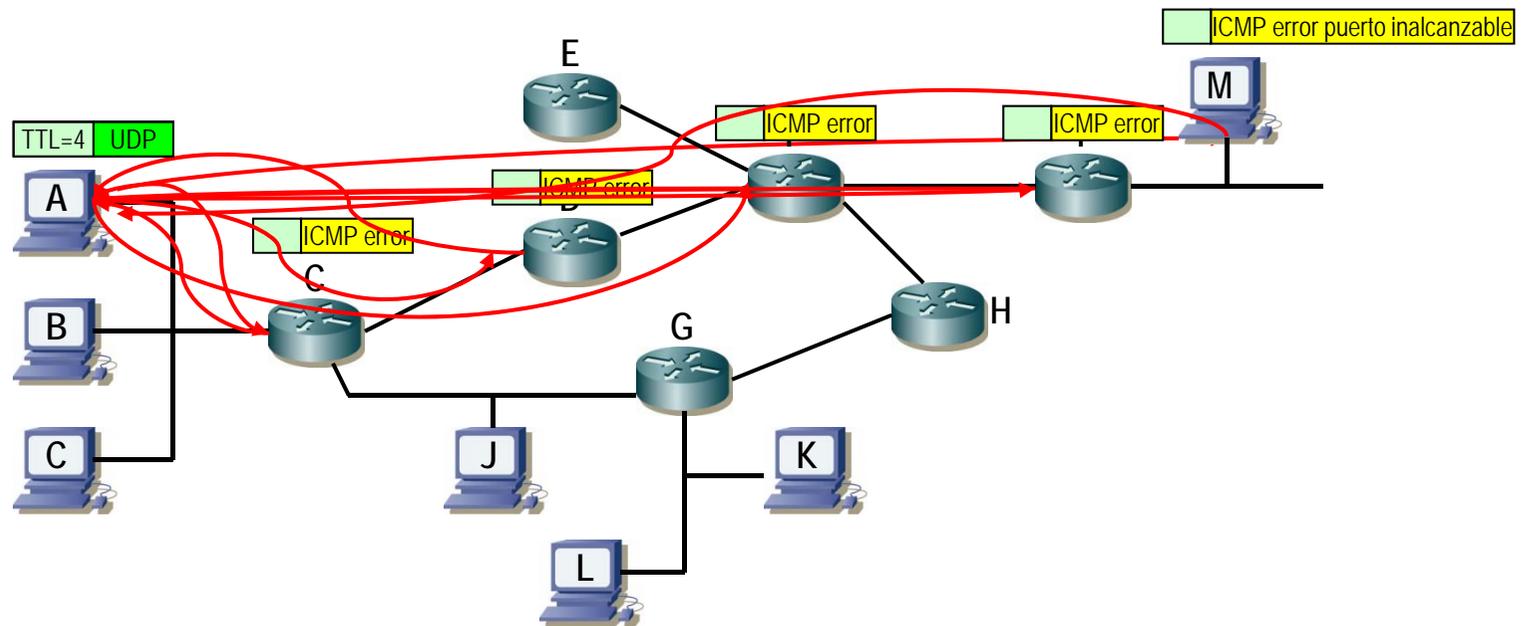
Type: 11	Code: 0 or 1	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

ICMP error: Tiempo excedido

- Ejemplo de aplicación: **Traceroute**, aplicación que permite determinar una posible ruta entre dos máquinas.
 - La ruta se mide salto a salto con series de paquetes cuyo campo TTL de la cabecera IP va creciendo 1,2,3,...
 - 3 intentos por cada valor de TTL.
 - El paquete es UDP con un puerto destino aleatorio por encima del 30000.
 - Windows (tracert) utiliza ICMP echo request en lugar de UDP.
 - Los nodos correspondientes a los saltos intermedios responderán con un ICMP de error de “tiempo excedido” al agotarse el TTL.
 - El nodo destino responderá con un ICMP de error de “puerto inalcanzable”.
- A tener en cuenta:
 - Las rutas pueden variar.
 - Las rutas pueden no ser simétricas.

ICMP error: Tiempo excedido

- Ejemplo de aplicación: *Traceroute*



A ⇒ C ⇒ D ⇒ F ⇒ I ⇒ M

ICMP error: Tiempo excedido

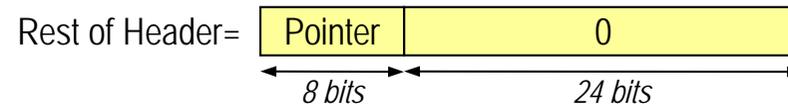
- Ejemplo de aplicación: **Traceroute** fry.tlm.unavarra.es → www.berkeley.edu

```

1 130.206.158.129 (130.206.158.129) 0.437 ms 0.828 ms 1.042 ms
2 130.206.158.49 (130.206.158.49) 0.244 ms 0.221 ms 0.275 ms
3 130.206.158.6 (130.206.158.6) 0.983 ms 0.971 ms 0.945 ms
4 130.206.158.1 (130.206.158.1) 1.021 ms 0.929 ms 0.881 ms
5 XE4-3-0-53.UNAVARRA.unizar.rt1.ara.red.rediris.es (130.206.195.1) 18.623 ms 18.612 ms 18.591 ms
6 130.206.245.5 (130.206.245.5) 161.563 ms * 130.206.245.5 (130.206.245.5) 23.485 ms
7 130.206.245.2 (130.206.245.2) 19.425 ms 23.895 ms 18.976 ms
8 rediris.rt1.mad.es.geant.net (62.40.124.53) 23.857 ms 23.846 ms 23.840 ms
9 as2.rt1.gen.ch.geant2.net (62.40.112.25) 50.750 ms 45.568 ms 45.541 ms
10 so-4-0-0.rt1.fra.de.geant2.net (62.40.112.161) 53.446 ms 53.814 ms 53.787 ms
11 abilene-wash-gw.rt1.fra.de.geant.net (62.40.125.18) 141.136 ms 145.429 ms 145.427 ms
12 ae-8.10.rtr.atla.net.internet2.edu (64.57.28.6) 158.488 ms 158.475 ms 154.446 ms
13 xe-1-0-0.0.rtr.hous.net.internet2.edu (64.57.28.112) 214.081 ms 214.054 ms 214.061 ms
14 * ge-6-1-0.0.rtr.losa.net.internet2.edu (64.57.28.96) 650.822 ms *
15 hpr-lax-hpr--i2-newnet.cenic.net (137.164.26.133) 224.745 ms 225.119 ms 225.178 ms
16 svl-hpr2--lax-hpr2-10g.cenic.net (137.164.25.38) 217.214 ms 221.543 ms 221.516 ms
17 hpr-ucb--svl-hpr2.cenic.net (137.164.27.130) 235.264 ms 231.276 ms 231.223 ms
18 t1-3.inr-201-sut.Berkeley.EDU (128.32.0.65) 223.396 ms 227.380 ms 227.376 ms
19 t5-4.inr-211-srb.Berkeley.EDU (128.32.255.41) 228.232 ms 227.899 ms 223.448 ms
  
```

4.3.5 ICMP error: Problema de parámetros

- Type=12
- Code:
 - 0: hay un error o ambigüedad en un campo de la cabecera IP. El puntero del campo Rest of Header apunta al byte con el problema.
 - 1: falta una parte requerida de una opción de la cabecera IP.
- Rest of Header: Pointer (8bits) + 24 bits no usados.



Type: 12	Code: 0 or 1	Checksum
Pointer	Unused (All 0s)	
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

Resumen

- ICMP de error
 - Se genera ante un paquete IP que genera una situación de error
 - Lo genera el elemento de red que detecta el error (un router habitualmente)
 - Con destino la dirección IP de la máquina emisora del paquete IP original
 - Contiene copia de la cabecera IP y 8 primeros bytes de datos sobre IP del paquete IP original
- Destacan
 - Destino inalcanzable
 - Redirección
 - Tiempo excedido: por TTL o timeout de reensamblado
- La máquina que recibe el ICMP error actuará a nivel IP o en función de niveles superiores que se implementen por encima de IP en esa comunicación, dependiendo del tipo de error

Referencias

- [Forouzan]
 - Capítulo 9 “ICMPv4”, secciones 9.1-9.3 “Introduction”, “Messages”, “Debugging tools”
- [Stevens]
 - Capítulo 6 “ICMP: Internet Control Message Protocol”
 - Capítulo 8 “Traceroute Program”
 - Capítulo 9 “IP Routing”, secciones 9.3-9.6