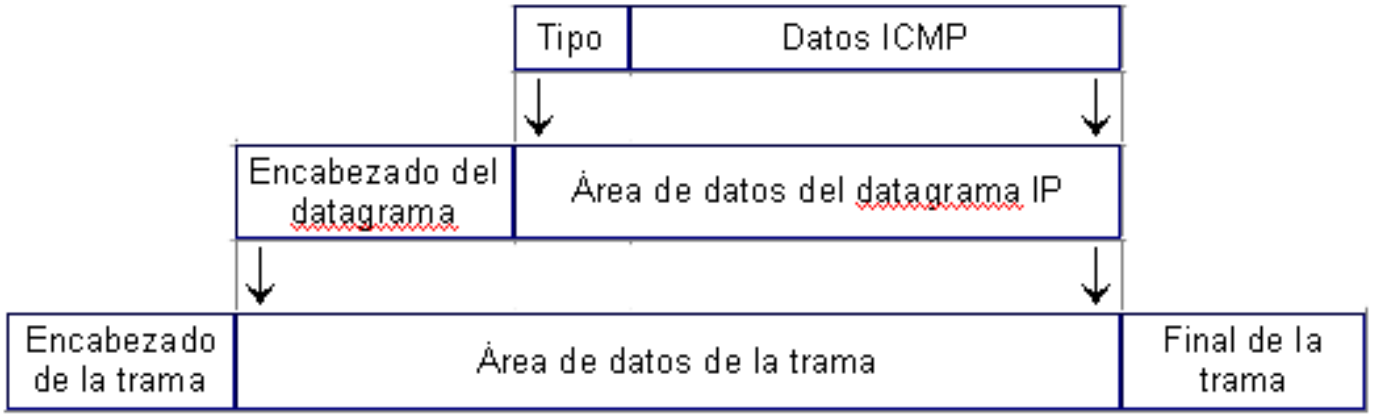
Protocolo ICMP

ICMP (*Internet Control Message Protocol*)

- El protocolo IP no es fiable y los datagramas pueden perderse o llegar defectuosos a su destino.
- Una función ICMP es informar al origen si se ha producido algún error durante la entrega de su mensaje.
- Pero no sólo se encarga de notificar los errores, sino que también transporta distintos mensajes de control.
- Este como otros protocolos esta descripto en un RFC (rfc 792)

ICMP (*Internet Control Message Protocol*)

- ICMP únicamente informa de incidencias en la red, no toma acciones.



Mensaje ICMP

- En la cabecera Ip tiene el campo Protocolo en 1 (Indicando que lo que contiene es un protocolo ICMP)

Mensaje ICMP campo TIPO

Tipo	Tipo de mensaje ICMP
0	Respuesta de eco (*Echo Reply*)
3	Destino inaccesible (*Destination Unreachable*)
4	Disminución del tráfico desde el origen (*Source Quench*)
5	Redireccionar (cambio de ruta) (*Redirect*)
8	Solicitud de eco (*Echo*)
11	Tiempo excedido para un datagrama (*Time Exceeded*)
12	Problema de Parámetros (*Parameter Problem*)
13	Solicitud de marca de tiempo (*Timestamp*)
14	Respuesta de marca de tiempo (*Timestamp Reply*)
15	Solicitud de información (obsoleto) (*Information Request*)
16	Respuesta de información (obsoleto) (*Information Reply*)
17	Solicitud de máscara (*Addressmask*)
18	Respuesta de máscara (*Addressmask Reply*)

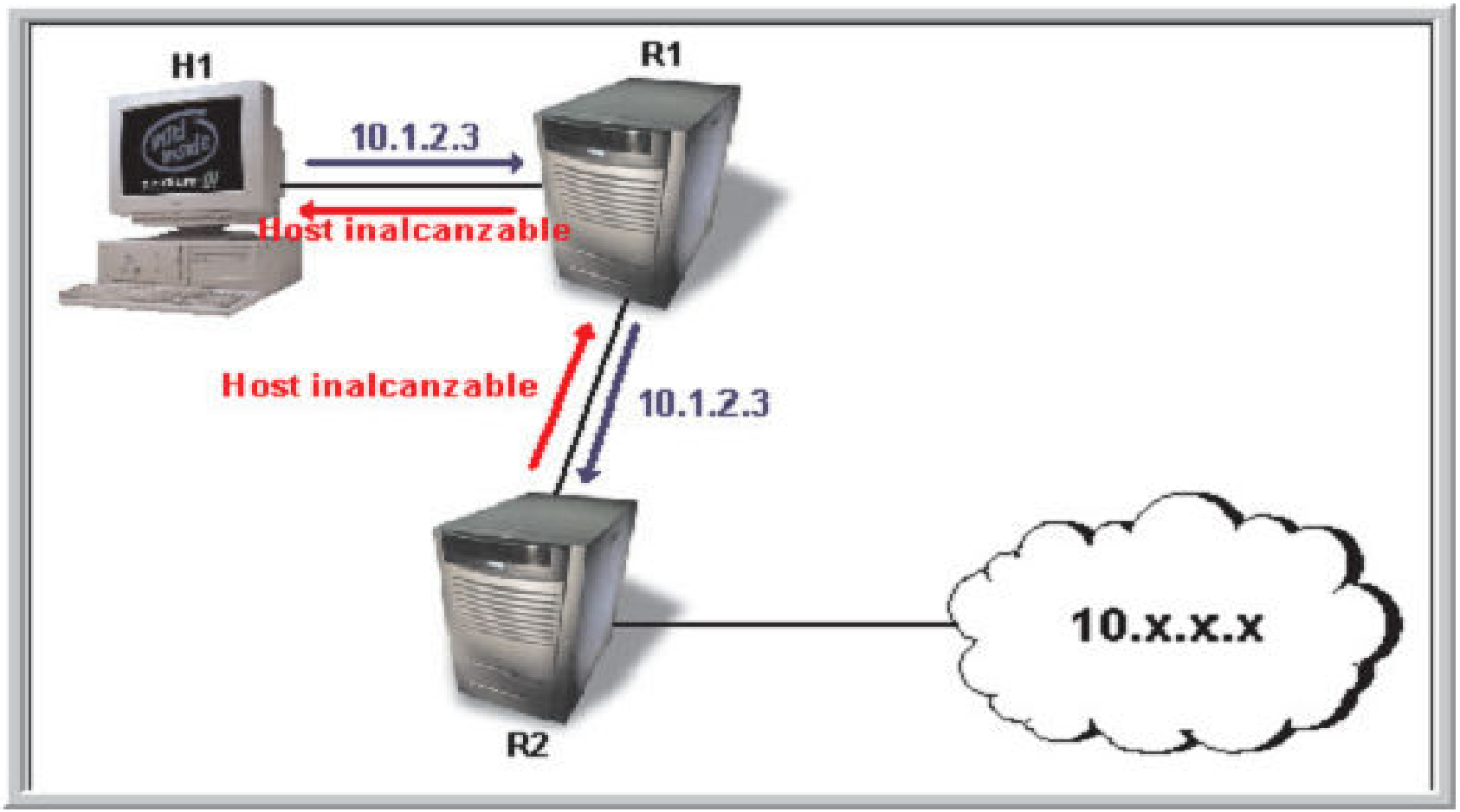
Mensaje ICMP campo Codigo

- El valor y el significado de este campo depende del tipo de ICMP

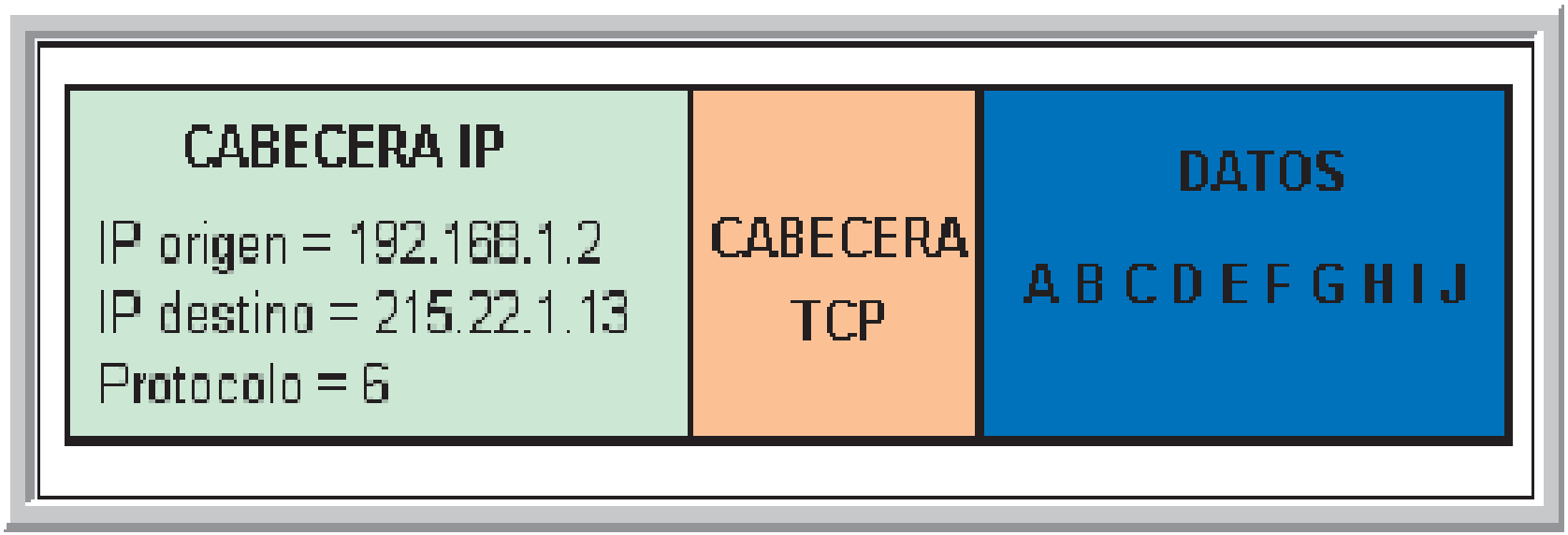
Ej: Destino Inalcanzable el campo código precisa la razón del error

Code	Descripción
0	Red inalcanzable.
1	Host inalcanzable.
2	Protocolo inalcanzable.
3	Puerto inalcanzable.
4	Paquete demasiado grande, y no puede ser fragmentado.
5	Error del router de origen.
6	Error desconocido en la red de destino.
7	Error desconocido en el host de destino.
8	Host de origen aislado (este mensaje está obsoleto).
9	Acceso no autorizado a la red de destino.
10	Acceso no autorizado al host de destino.
11	La red es inalcanzable para el tipo de servicio especificado.
12	El host es inalcanzable para el tipo de servicio especificado.
13	Comunicación no autorizada.
14	Violación de las reglas de precedencia de hosts.
15	Corte de precedencia.

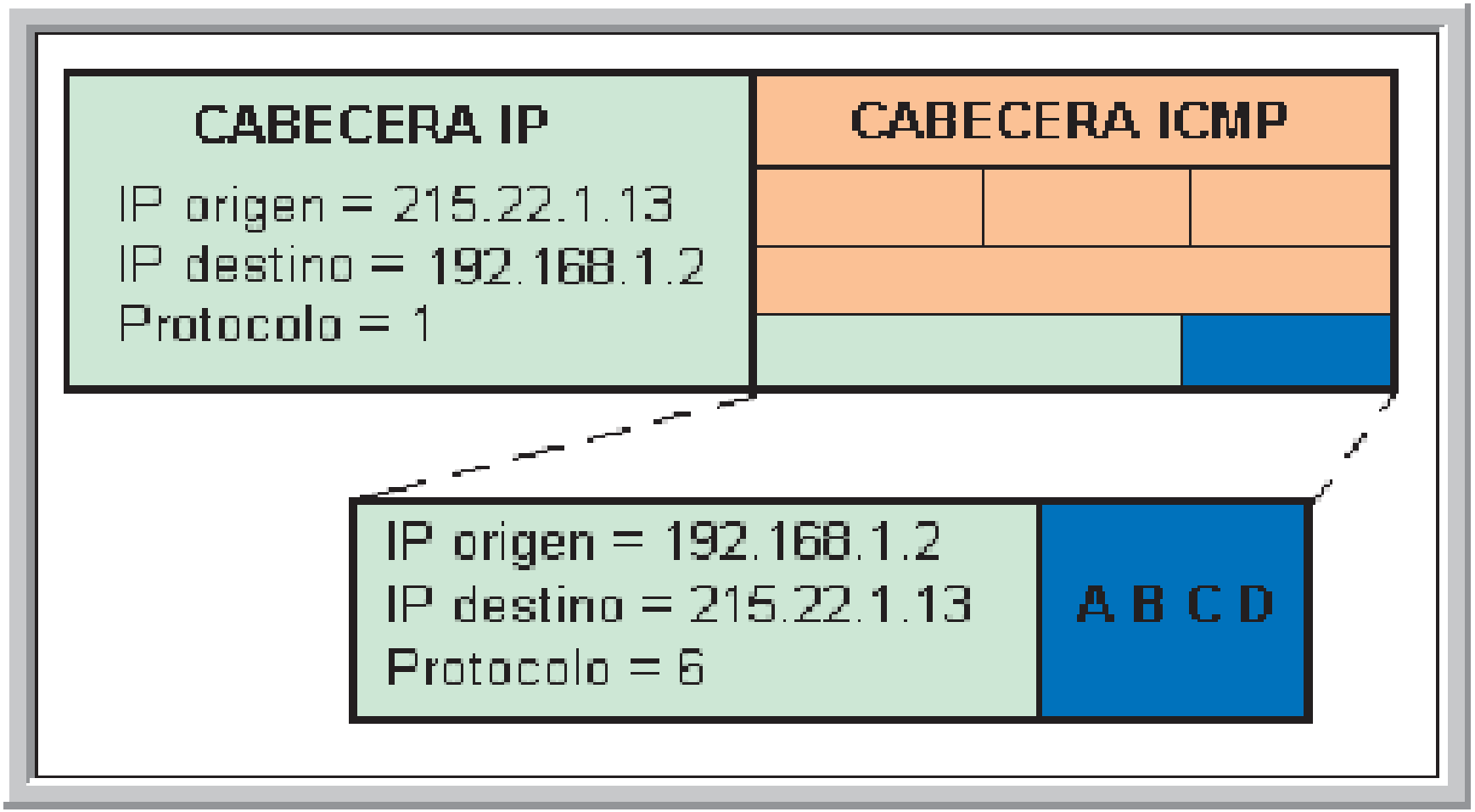
Quien envia mensajes ICMP



Envio de datos



Respuesta ICMP



Principales mensajes de ICMP

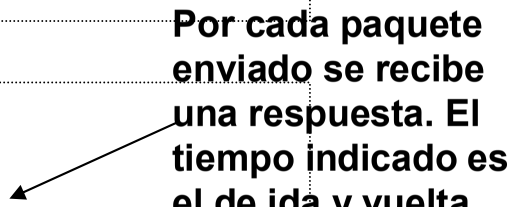
Mensaje	**Explicación**
Destination Unreachable (Destino inaccesible)	Red, host, protocolo o puerto (nivel de transporte) inaccesible o desconocido Datagrama con bit DF puesto no cabe en la MTU
Source quench (apagar la fuente)	Ejerce control de flujo sobre el emisor en casos de congestión. No se utiliza.
Echo request y Echo reply	Sirve para comprobar la comunicación (comando ping).
Time exceeded (Tiempo excedido)	Datagrama descartado por agotamiento del TTL (usado en comando traceroute)
Redirect (Cambio de ruta)	El router nos sugiere un camino más óptimo

Comando PING

ICMP ECHO REQUEST y ECHO REPLY

```
Iluso_$ ping -s www.uv.es 64 4
PING video.ci.uv.es: 64 bytes packets
64 bytes from 147.156.1.46: icmp_seq=0. time=1. ms
64 bytes from 147.156.1.46: icmp_seq=1. time=1. ms
64 bytes from 147.156.1.46: icmp_seq=2. time=1. ms
64 bytes from 147.156.1.46: icmp_seq=3. time=1. ms
---video.ci.uv.es PING Statistics ----
4 packets transmitted, 4 packets receivded, 0% packet loss
Round-trip (ms) min/avg/max = 1/1/1
```

```
Iluso_$ ping -s www.cmu.edu 64 4
PING server.andrew.cmu.edu: 64 bytes packets
64 bytes from 128.2.72.5: icmp_seq=0. time=287. ms
64 bytes from 128.2.72.5: icmp_seq=1. time=290. ms
64 bytes from 128.2.72.5: icmp_seq=2. time=285. ms
64 bytes from 128.2.72.5: icmp_seq=3. time=277. ms
---server.andrew.cmu.edu PING Statistics ----
4 packets transmitted, 4 packets receivded, 0% packet loss
Round-trip (ms) min/avg/max = 277/285/290
```



Traceroute

- La orden **TRACERT** (**traceroute** en entornos Unix) hace una traza a un determinado host. TRACERT funciona enviando mensajes ICMP de solicitud de eco con distintos TTL; traceroute, en cambio, envía mensajes UDP. Si la comunicación extremo a extremo no es posible, la traza nos indicará en qué punto se ha producido la incidencia.

Traceroute ¿Cómo funciona?

- Para poder realizar el trazado de tiempo del emisor a cada punto intermedio, esta aplicación hace uso del campo TTL. Para el primer router TTL vale 1, al llegar al equipo y descontarle 1, este pasa a valer 0 y es descartado enviando una respuesta de tiempo excedido. (Esta respuesta contendrá el IP del Router R1 que lo genero)

Traceroute ¿Cómo funciona?

- Ahora la aplicación envia otro mensaje con TTL=2, este pasara por R1 que

  al salir de este TTL valdra 1 y al pasar por R2 valdra 0, enviandose otra respuesta de tiempo excedido. (Que contendrá el IP del Router R2 que lo genero)

Traceroute ¿Cómo funciona?

- El próximo envío de la aplicación el TTL=3, este pasara por R1 que al salir de este TTL valdrá 2 y al pasar por R2 TTL=1, llegando al equipo de destino enviándose una respuesta de eco. (De este modo Traceroute sabe que llego a destino)

Comando Traceroute

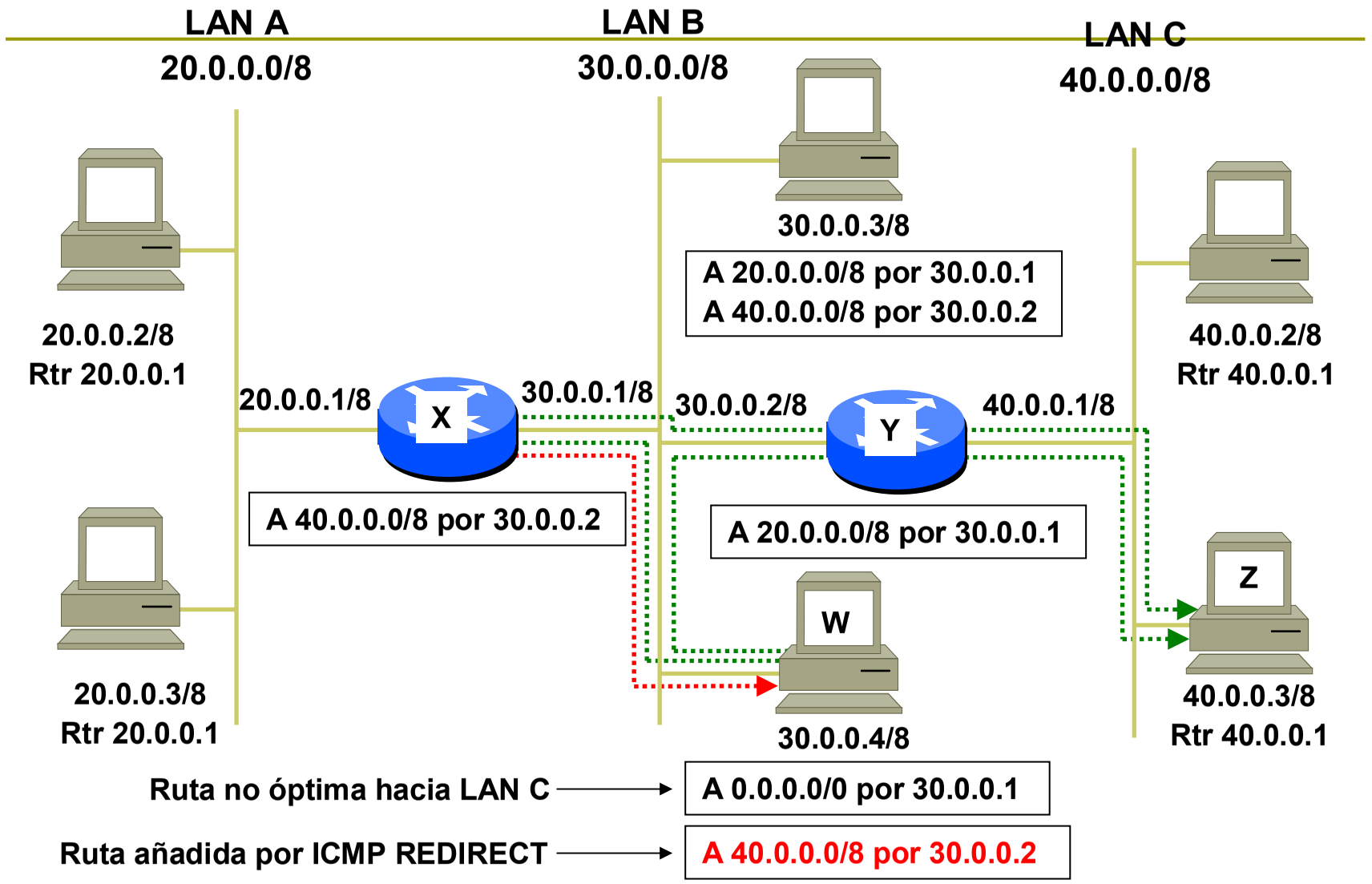
ICMP TIME EXCEEDED

```
Iluso_$ traceroute www.uniovi.es
traceroute to dana.vicest.uniovi.es (156.35.34.1), 30 hops max,
                                                    40 byte packets
 1  cisco.ci.uv.es (147.156.1.11)  3 ms  3 ms  2 ms
 2  A1-0-2.EB-Valencia1.red.rediris.es (130.206.211.181)  2 ms  2 ms  2 ms
 3  A1-0-2.EB-Madrid1.red.rediris.es (130.206.224.5)  8 ms  7 ms  7 ms
 4  A3-0-1.EB-Oviedo1.red.rediris.es (130.206.224.34)  22 ms  17 ms  17 ms
 5  rcpd02.net.uniovi.es (156.35.11.205)  16 ms  17 ms  16 ms
 6  156.35.12.253 (156.35.12.253)  20 ms  19 ms  19 ms
 7  rest34.cpd.uniovi.es (156.35.234.201)  24 ms  26 ms  26 ms
 8  dana.vicest.uniovi.es (156.35.34.1)  28 ms  28 ms  28 ms
Iluso_$
```

Valor del TTL utilizado en los paquetes

Enviados 24 paquetes en total

Uso del comando ICMP REDIRECT



Efecto de ICMP REDIRECT sobre el host 203.1.1.4 anterior

```
> route -n
Routing tables
Destination      Gateway       Flags   Refcnt      Use   Interface

127.0.0.1        127.0.0.1     UH      6         62806   lo0
Default           30.0.0.1     UG      62      2999087   le0
 30.0.0.0         30.0.0.4     U       33      1406799   le0


(recibido mensaje ICMP REDIRECT)

> route -n
Routing tables
Destination      Gateway       Flags   Refcnt      Use   Interface

127.0.0.1        127.0.0.1     UH      6         62806   lo0
Default           30.0.0.1     UG      62      2999385   le0
 30.0.0.0         30.0.0.4     U       33      1406927   le0
 40.0.0.0         30.0.0.2     UGD     1           357   le0

Flags: U: ruta operativa (Up)
       G: Ruta gateway (router)
       H: Ruta host
       D: ruta dinámica
```

Otro ejemplo de uso de ICMP REDIRECT

1. X quiere mandar un paquete a Y. Como está en otra red y X no tiene ruta para llegar a ella manda el paquete a su router por defecto, Z.
2. El router envía el datagrama a su destino, pero además envía un ICMP REDIRECT a X indicándole que Y está en su misma LAN, por lo que puede hablar directamente. Como consecuencia X incorpora en su tabla de rutas una entrada para indicar que la red B está accesible directamente (por eth0)