Práctica 4: El protocolo ICMP

1. Sesión L4

Lectura previa: Kurose 4.4.3 subapartado “Protocolo de mensajes de control ICMP” (pags. 343-345)

Trabajo previo antes de la sesión de laboratorio: Ejercicio 1 (realización).

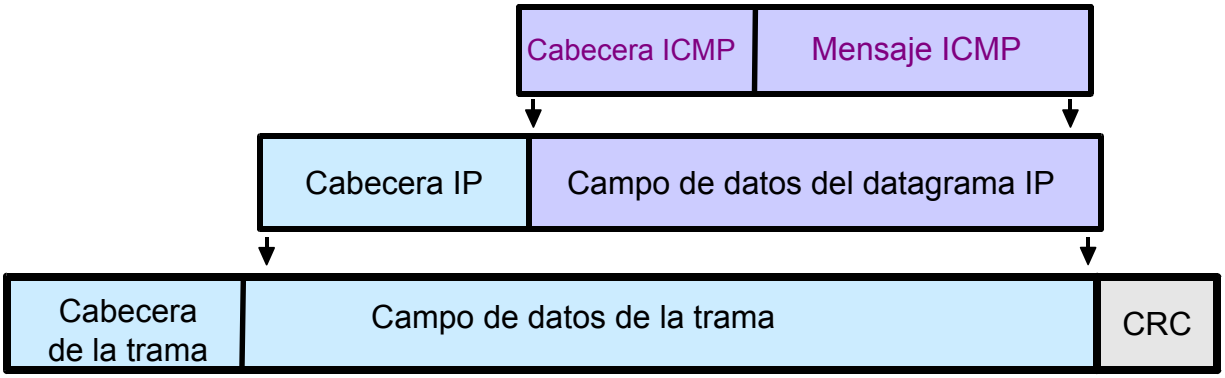
2. Introducción a ICMP

En esta práctica vamos a estudiar el protocolo ICMP (*Internet Control Message Protocol*) y algunas órdenes derivadas de él.

En Internet no disponemos de mecanismos hardware para comprobar la conectividad. Además, el protocolo IP no proporciona herramientas para la detección de fallos y problemas. Así es que se diseñó el protocolo ICMP para permitir a los hosts y routers enviar mensajes de control a otros hosts y routers. Está definido en el RFC 792.

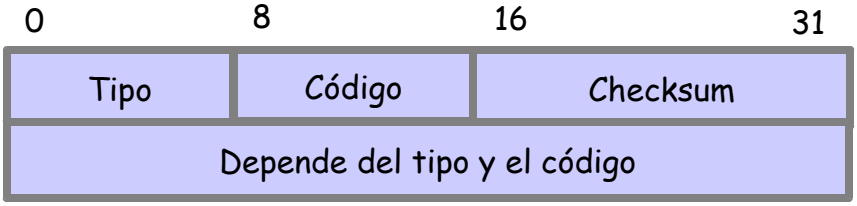
ICMP nos permite saber, por ejemplo, por qué no se ha entregado un datagrama (no hay ruta, el destino no responde, se ha agotado su tiempo de vida, etc.). Informa de errores sólo al origen del datagrama. Además, no se encarga de corregir el problema, sólo de avisar.

Como los mensajes ICMP pueden generarse en el exterior de la red IP donde se generó el datagrama original necesitan viajar en el campo de datos de un datagrama IP, pero ICMP no se considera un protocolo de nivel superior a IP, sino de nivel de red.



Cada mensaje ICMP tiene su propio formato, pero todos comienzan con los mismos campos:

- Tipo (8 bits): Identifica el tipo de mensaje
- Código (8 bits): Más información sobre el tipo de mensaje
- *Checksum* (16 bits): Utiliza el mismo algoritmo que IP.



El tipo de mensaje determina su significado y su formato. Hay 15 tipos distintos. Entre los principales tenemos:

- Tipo = 0. Respuesta de eco.
- Tipo = 3. Destino inalcanzable.
- Tipo = 8. Petición de eco.
- Tipo = 11. Tiempo de vida excedido en datagrama (TTL=0).

Los mensajes de error contienen la cabecera IP y los ocho primeros bytes de datos del datagrama original. Hay que señalar que esa información contine las direcciones IP fuente y destino, así como los puertos fuente y destino del datagrama que ha causado el error.

Para evitar problemas en la red, en particular *broadcast storms,* nunca se generan mensajes de error en respuesta a:

- Un mensaje de error ICMP.
- Un datagrama destinado a una dirección IP de difusión.
- Un fragmento que no sea el primero.
- Un datagrama cuya dirección origen no defina una conexión de red única (es decir, que la dirección origen no puede ser cero, la dirección de *loopback*, direcciones de difusión).

Mensajes ICMP de eco

La respuesta a una petición de eco devuelve los mismos datos que se recibieron en la petición. Estos mensajes se utilizan para construir la herramienta *ping*, empleada por administradores y usuarios para detectar problemas en la red.

Permite :

- Comprobar si un destino está activo y si existe una ruta hasta él.
- Medir el tiempo de “ida y vuelta”.
- Estimar la fiabilidad de la ruta.
- Puede ser utilizado tanto por hosts como por routers.

Mensajes ICMP de tiempo excedido

Este tipo de mensajes pueden ser enviados por routers y por hosts:

- Routers: cuando descartan un datagrama al llegar a cero su tiempo de vida.
- Hosts: al vencer un temporizador mientras esperan todos los fragmentos de un datagrama.

El campo código explica cuál de los dos sucesos ha ocurrido.

En estos mensajes se apoya la orden *traceroute*, que se estudiará después.

Mensajes de destino inalcanzable

Son enviados por un router o un host cuando no puede enviar o entregar un datagrama IP.

Se envían al emisor inicial del datagrama.

El campo código contiene un entero con información adicional. Los más importantes son:

- Código = 0. Red inalcanzable.
- Código = 1. Host inalcanzable.
- Código = 2. Protocolo inalcanzable.
- Código = 3. Puerto inalcanzable. Se genera usualmente cuando se recibe un datagrama UDP destinado a un puerto UDP que está cerrado en el destino.
- Código = 4. Se requiere fragmentación pero bit DF activado.
- Código = 6. Red destino desconocida.
- Código = 7. Host destino desconocido.

Ejercicio 1:

El computador B ha recibido los siguientes datagramas cuyo origen era el computador A. Los únicos puertos **TCP** abiertos en B al recibir los datagramas IP eran el 22 y el 30.000.

Nº	Identificador	MF	OFFSET	Long. Total	Protocolo	Tipo (si ICMP)/ Puerto si UDP o TCP
1	1340	1	185	1500	ICMP	8
2	1341	0	0	877	UDP	8.000
3	1342	1	0	1500	TCP	22
4	1340	0	370	78	ICMP	8
5	1342	1	185	1500	TCP	22

nada, porque (40) icmp es de nivel de red, (41) el puerto 8000 esta cerrado, (42) todavia no han llegado todos los fragmentos.

- ¿Qué datos recibirá el nivel de transporte? Justifica la respuesta.
- ¿Se generarán mensajes ICMP? Justifica la respuesta. En caso afirmativo indica qué datagrama(s) lo(s) genera(n).

Si, (1340) contestacion del icmp tipo 0, (1341) error de host inalcanzable tipo 3, falta el ultimo fragmento, si llega no contestara (1342)

3. Análisis de la cabecera IP

Enciende el ordenador e inicia sesión en la partición de Ubuntu con tu usuario y contraseña de upvnet.

Ejercicio 2:

Inicia el analizador de protocolos *wireshark* (desde el botón de la barra superior). La contraseña que solicita es la de tu usuario de upvnet. Captura los paquetes IP que se generan al cargar en el navegador la página www.uv.es, y filtra el resto del tráfico. Recuerda que los protocolos de aplicación se filtran indicando el puerto del servidor. No olvides comprobar que la interfaz de captura es la adecuada (debe coincidir con la que tiene asociada la dirección IP pública). Detén la captura, analiza los primeros 4 paquetes IP generados, y responde a las siguientes cuestiones:

	Identificador	***TTL***	***Dirección IP fte.***	***Dir. IP destino***
Paquete 1	0x2ch0	64	158.42.180.7	147.156.200.249

Paquete 2	0x3e75	57	147.156.200.249	156.42.180.7
Paquete 3	0x2cb4	64	158.42.180.7	147.156.200.249
Paquete 4	0x25e4	64	158.42.180.7	147.156.200.249

No, cada ordenador tiene un TTL, el inicial del servidor seria 64,

Con respecto al campo TTL (*Time To Live*) de la cabecera IP de los paquetes capturados, ¿tiene siempre el mismo valor? En general, todos los paquetes que envía un ordenador, ¿tienen siempre el mismo TTL inicial?¿Cuál sería el valor inicial del TTL en el paquete 2 (el primero que ha enviado el servidor)?

Observa cómo varia el campo identificador en el cliente y en servidor. Describe lo que observas. Anota el valor del campo protocolo. En este caso, ¿a qué protocolo se refiere? TCP

4. La orden ping

Mediante la orden ***ping*** (que se ejecuta desde un terminal) se obtiene una estimación del tiempo de ida y vuelta de un paquete (RTT), desde la estación origen a una estación destino que se especifica. Para ello se almacena el instante de tiempo en el que se envía el paquete y cuando llega la respuesta al valor almacenado se le resta del tiempo actual. El funcionamiento de la orden ***ping*** se basa en el uso de mensajes ICMP de tipo 0 (*Echo reply*) y 8 (*Echo request*).

Otras utilidades de la orden ***ping*** son:

- Averiguar si un destino está operativo, conectado a la red y sus protocolos TCP/IP en funcionamiento.
- Conocer la fiabilidad de la ruta entre origen y destino (calculando el porcentaje de paquetes que obtienen respuesta).

Ejemplo:

```
user@rdc14:~$ ping www.uji.es
PING www.uji.es (84.124.83.62) 56(84) bytes of data.
64 bates from 84.124.83.62.static.user.ono.com (84.124.83.62): icmp_seq=1 ttl=112 time=22.1 ms
64 bytes from 84.124.83.62.static.user.ono.com (84.124.83.62): icmp_seq=2 ttl=112 time=21.6 ms
64 bytes from 84.124.83.62.static.user.ono.com (84.124.83.62): icmp_seq=3 ttl=112 time=21.6 ms
64 bytes from 84.124.83.62.static.user.ono.com (84.124.83.62): icmp_seq=4 ttl=112 time=22.0 ms
    ^C
    --- www.uji.es ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 21.646/21.872/22.139/0.217 ms
```

La orden ***ping*** admite un serie de opciones, algunas de las más útiles se muestran a continuación. Para ver una información más completa puede consultarse el man de la orden.

```
ping [-b][-c count] [-s packetsize] [-t TTL] destino

   Opciones:

     -b            Permite hacer broadcast a una dirección de difusión
     -c cantidad   Cantidad de solicitudes de eco a enviar.
     -s tamaño     Número de bytes de datos.
     -t TTL        Tiempo de vida.

   Para interrumpir la ejecución del programa ping: hay que presionar Ctrl-C.
```

Ejercicio 3:

Haz un *ping- c 3* a las direcciones siguientes: zoltar.redes.upv.es (servidor dentro del Laboratorio de Redes), www.upv.es (servidor web de la UPV), www.rediris.es (servidor web de RedIris situado en Madrid), **www.uq.edu.au** (servidor web de la Universidad de Queensland en Australia), www.berkeley.edu (servidor web de la Universidad de California en Berkeley). La opción **-c 3** configura la orden ***ping*** para que realice únicamente tres intentos. Anota los resultados en la tabla siguiente:

	Tiempo de ida y vuelta (ms)		
	Mínimo	**Máximo**	**Medio**
www.upv.es	0.182	0.275	0.227
www.rediris.es	7.452	10.120	8.476
www.uq.edu.au	369.857	370.341	370.077
www.berkeley.edu	195.226	195.475	195.314

Los resultados que se obtienen mediante la orden ***ping*** son, a veces, difíciles de interpretar. El usuario obtiene poca información de por qué el tiempo de ida y vuelta es mayor en unos destinos que en otros. Incluso cuando no hay respuesta al *ping*, no es posible conocer cuál es el problema: el destino solicitado está fuera de servicio, no existe una ruta desde el origen al destino o la saturación de la red es tan alta que no se obtiene respuesta del destino en un tiempo razonable. También, en ocasiones por motivos de seguridad y para evitar dar información sobre los ordenadores conectados a la red, los administradores de las redes filtran los mensajes de *ping* en los cortafuegos o desactivan el servicio en los propios ordenadores. A pesar de lo dicho, es una de las herramientas que más utilizan los administradores y usuarios de equipos conectados en red.

Ejercicio 4:

Antes de iniciar la captura lee el ejercicio hasta llegar a las cuestiones.

Aplica un filtro de captura (no de visualización) que capture únicamente los paquetes ICMP generados tras la ejecución de la orden `ping -c 3 zoltar.redes.upv.es`. Ejecuta la orden dos veces.

Detén la captura cuando terminen los seis intentos y observa cuántos mensajes ICMP se producen, prestando especial atención a los campos **tipo**, **código**, y **bytes de datos**. Observa la diferencia entre los mensajes ICMP de petición y de respuesta de eco. Asimismo, analiza las cabeceras IP de cada

uno de ellos, y en concreto los campos **longitud de la cabecera**, **longitud total** y **bytes de datos**. Compara el valor del campo protocolo con el que observaste en el ejercicio 1.

Respecto a los mensajes ICMP:
¿Por qué los mensajes ICMP no llevan números de puerto fuente y destino?¿Para qué se utiliza el **número de secuencia**? ¿y el campo **identificador**? No lleva puerto porque es a nivel de red no llega a nivel de aplicacion

el numero de secuencia relaciona la peticion echo con su respuesta.
el identificador relaciona todos los echos de un mismo ping.

5. La orden traceroute

La orden ***traceroute*** **(**que se ejecuta desde un terminal) permite conocer el camino (secuencia de routers) que debe atravesar un paquete para llegar desde la estación origen a la estación destino. El funcionamiento se basa en gestionar adecuadamente un parámetro de la cabecera de los datagramas IP (el campo TTL: tiempo de vida) y en la información que aportan los mensajes ICMP que generan los routers cuando les llega un datagrama cuyo tiempo de vida se ha agotado.

Por cada nuevo router atravesado por el datagrama se dice que hay un *salto* en la ruta. Podemos decir, que el programa ***traceroute*** calcula y describe el número de saltos de una ruta.

Generalmente, el campo TTL tiene 8 bits que el emisor inicializa a algún valor. El valor recomendado actualmente en el RFC de números asignados (RFC 1700) es de 64. Cada router que atraviesa el datagrama debe reducir el TTL en una unidad. Cuando un router recibe un datagrama IP con TTL igual a uno y decrementa este valor obtiene un cero. Consecuentemente, el router descarta el datagrama y envía un mensaje ICMP de tipo 11 (*tiempo excedido)* al origen que generó el datagrama. La clave para el funcionamiento del programa ***traceroute*** es que este mensaje ICMP contiene la dirección IP del router que lo ha enviado.

En el caso del *traceroute*, el primer datagrama IP se envía al ordenador destino con TTL igual a 1. Si el destino no está en la misma red que el host origen, el primer router con el que se encuentre este datagrama decrementará el TTL y al obtener un cero lo descartará, enviando un mensaje ICMP de "tiempo excedido" (*Time exceed*) al origen. Así se identifica el primer router en el camino. A continuación se envía un datagrama con TTL igual a 2 para encontrar la dirección del segundo router, y así sucesivamente.

Cuando el datagrama alcance un valor de TTL suficiente para llegar a su destino, necesitaremos que el destino envíe un mensaje que nos permita detener el proceso. Para ello ***traceroute*** utiliza dos opciones distintas:

- Enviar mensajes ICMP de eco (es la que se usa en Microsoft Windows). La respuesta al alcanzar el destino será un mensaje de respuesta de eco.
- Enviar mensajes UDP a un puerto arbitrariamente grande (en principio es el 33434) y muy probablemente cerrado (es la opción que se usa en Linux/Unix). El sistema responderá con un mensaje ICMP de puerto inalcanzable si el puerto está cerrado en el destino, pero si estuviera abierto no se recibiría respuesta y no se detectaría que ya se ha alcanzado el destino.

Por defecto, para averiguar cada nuevo salto se envían tres datagramas y para cada uno de ellos se

calcula el valor del tiempo de ida y vuelta. Si en un tiempo máximo (configurable) no hay respuesta se indica en la salida mediante un asterisco.

Algunas puntualizaciones:

- No hay ninguna garantía de que la ruta que se ha utilizado una vez vaya a ser utilizada la siguiente.
- No hay ninguna garantía de que el camino seguido por el paquete de vuelta sea el mismo que ha seguido el paquete de ida. Esto implica que a partir del tiempo de ida y vuelta que ofrece ***traceroute*** puede no ser directo estimar el tiempo de ida o de vuelta por separado (si el tiempo que tarda el paquete en ir desde el origen hasta el *router* es de 1 segundo y el tiempo que tarda el paquete de vuelta es de 3 segundos, el valor que nos proporcionará ***traceroute*** será de 4 segundos).
- La dirección IP que se devuelve en el mensaje ICMP es la dirección de la interfaz entrante del router (aquélla por la que se recibió el paquete).

Ejercicio 5:

Ejecuta la orden ***traceroute*** para los siguientes destinos y anota el número de saltos.

	Saltos
www.upv.es	4
www.ua.es	6
www.usc.edu	24

Observa que si se alcanza el destino, la última línea mostrada corresponde a dicho destino (en nuestro caso un servidor web) y no a un router.

Analiza cuáles pueden ser las causas de la respuesta obtenida al ejecutar la orden *traceroute* www.ua.es. Que el puerto de echo este cerrado para que no se pueda averiguar la estructura de la red

En el *traceroute* a www.usc.edu, aparecen diferencias importantes en el retardo de los enlaces que se observa, ¿cuál crees que es el motivo? El retardo es mayor porque los servidores destino estan mas lejos

Ejercicio 6:

Desde el navegador accede a la página **http://www.traceroute.org/#USA**. En esta página puedes seleccionar diversos sitios web desde los que puedes lanzar un traceroute a un destino cualquiera. Selecciona el sitio de la University of Southern of California (**www.usc.edu**), y solicita un *traceroute* a tu ordenador de prácticas. Compara el resultado con el del ejercicio anterior. ¿Se sigue el mismo recorrido desde la UPV a www.usc.edu y viceversa? Observarás que algunos routers tienen nombres similares en los dos casos pero con direcciones IP distintas, ¿a qué crees que es debido? Es debido a que no se utilizan las mismas rutas de ida que de vuelta.

No sigue el mismo recorrido. A que se pasa por los mismos routers pero se entra por interficies diferentes.

Ejercicio 7:

Captura los paquetes IP derivados de la ejecución de la orden `traceroute -n www.upv.es`. Para capturar también los paquetes enviados por tu ordenador tendrás que modificar el filtro para incluya paquetes udp. Puedes emplear el filtro de captura "icmp or (host 158.42.180.X)", donde la X representa el valor en decimal del último octeto de la dirección IP de tu ordenador.
Enumera cuántos tipos distintos de paquetes se han obtenido y cuál es su función. Observa que las respuestas a los paquetes enviados pueden recibirse desordenadas, ya que vienen de distintos dispositivos. Puedes asociar fácilmente las respuestas con los datagramas enviados analizando el contenido de los paquetes ICMP recibidos. En particular, contienen el puerto destino del datagrama UDP que provocó el error. Primero envia los paquetes DNS para averiguar la ip del destino, despues utiliza el protocolo UDP para enviar peticiones a puertos cerrados del destino, y los paquetes ICMP son las contestaciones de error de que los puertos estavan cerrados y que el TTL se ha agotado.

UDP:

ICMP:

¿Qué información contiene el campo de código en los mensajes ICMP que has capturado?
Observa que los paquetes ICMP de error contienen muchos más campos que los paquetes ICMP de eco. Indica cuáles son esos campos, qué contienen y por qué se envían.
son las cabeceras opcionales ademas de que lleva parte del datagrama que ha generado el error