Arquitectura de Redes y Servicios

Práctica Tema 8: Uso de ICMP para PING

Jesús Cámara y Diego R. Llanos
Dpto. de Informática, Universidad de Valladolid

27 de noviembre de 2023

Índice

1. El Protocolo ICMP

El protocolo ICMP (*Internet Control Message Protocol*) se utiliza para realizar diagnósticos sobre el funcionamiento de la red y de los equipos conectados a ella, así como para enviar mensajes de error cuando una petición no ha podido completarse con éxito. Las principales características de este protocolo se pueden consultar en el documento que contiene las diapositivas que se han explicado en clase de teoría.

Este documento, en cambio, describe cómo utilizar datagramas ICMP para detectar si una máquina conectada a la red es alcanzable. Para ello, se hará uso de la herramienta `ping`, cuyo funcionamiento se basa en el envío y recepción de mensajes ICMP de tipo Echo Request y Echo Reply entre origen y destino, respectivamente. Si el destino no es alcanzable, devolverá un mensaje ICMP tipo Error.

2. Uso de ICMP para PING

Se hará uso del protocolo ICMP para implementar una versión propia del servicio `ping`. Este servicio utiliza un datagrama con el formato que muestra la Figura 1. El significado de cada campo es el siguiente:

- Cabecera:
  - *Type* (1 byte): tipo de mensaje (8 en Request, 0 en Reply)
  - *Code* (1 byte): código del mensaje (0 tanto en Request como Reply)
  - *Checksum* (2 bytes): suma de comprobación de integridad del datagrama. Hay que inicializarlo a cero y, posteriormente, almacenar el valor calculado cuando se haya construido el datagrama.

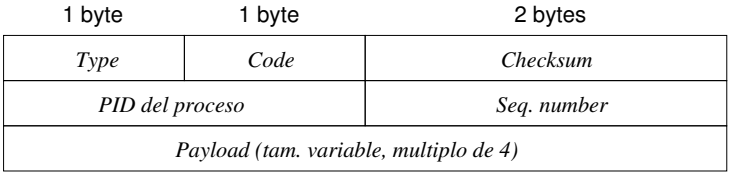

Figura 1: Formato del datagrama ICMP para realizar un *ping*.

- *PID* (2 bytes): identifica al proceso que realiza el `ping`. Contiene el resultado de invocar a `getpid(2)`
- *Sequence* (2 bytes): número de secuencia. Inicializarlo a 0.
- *Payload* (64 bytes): inicializarlo con una cadena arbitraria.

Si el servicio `ping` se ejecuta correctamente, la máquina a la que se le ha enviado el mensaje ICMP de solicitud (Echo Request) responderá con un datagrama IP que contendrá, tras la cabecera IP, el mensaje ICMP de respuesta (Echo Reply). En caso de error, los campos *Type* y *Code* del datagrama indicarán el tipo de error. La Tabla 1 muestra el listado completo de posibles errores junto con su descripción.

Type	Code	Description
3 : Destination Unreachable	0	Net Unreachable.
	1	Host Unreachable.
	2	Protocol Unreachable.
	3	Port Unreachable.
	4	Fragmentation Needed.
	5	Source Route Failed.
	6	Destination Network Unknown.
	7	Destination Host Unknown.
	8	Source Host Isolated.
	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.
5 : Redirect	1	Redirect for Destination Host.
	3	Redirect for Destination Host Based on Type-of-Service.
11 : Time Exceeded	0	Time-to-Live Exceeded in Transit.
	1	Fragment Reassembly Time Exceeded.
12 : Parameter Problem	0	Pointer indicates the error.
	1	Missing a Required Option.
	2	Bad Length.

Cuadro 1: Tipos de error devueltos por ICMP.

3. Práctica a Realizar

La práctica consiste en desarrollar un cliente llamado `miping` que haga uso de datagramas ICMP para reproducir el comportamiento del servicio `ping`. El código se implementará en el fichero miping-apellidos.c utilizando el lenguaje C y se ejecutará desde la terminal de comandos tal como se muestra a continuación:

```
./miping direccion_ip [-v]
```

Donde:

- `direccion_ip`: dirección IPv4 de la máquina a la que se hace ping.
- `-v` (opcional): permite informar de los pasos realizados (cada uno irá precedido por: `->`). Además, el programa deberá mostrar el valor del campo TTL de la cabecera IP del datagrama ICMP recibido.

Ejemplos:

```
 $> ./miping 10.0.25.250 -v
 -> Generando cabecera ICMP...
 -> Type: 8
 -> Code: 0
 -> PID : 1000
 -> Sequence Number: 0
 -> Cadena a enviar: Este es el payload.
 -> Checksum: 0x73df.
 -> Tamaño total del datagrama: 72.
 Mensaje ICMP enviado al host : 10.0.25.250

 Respuesta recibida desde : 10.0.25.250
 -> Tamaño de la respuesta: 92.
 -> Cadena recibida: Este es el payload.
 -> PID: 1000
 -> TTL: 56
 Respuesta correcta (Type 0, Code 0)

$> ./miping 10.0.25.250
Mensaje ICMP enviado al host : 10.0.25.250
Respuesta recibida desde : 10.0.25.250
Respuesta correcta (Type 0, Code 0)
```

Al recibir el datagrama de respuesta hay que indicar si la petición se ha procesado correctamente o, por el contrario, se ha producido algún error. En este último caso, se mostrará un mensaje describiendo el tipo de error. Por ejemplo, si se intenta acceder a una dirección IP protegida por un firewall, el mensaje de respuesta será:

```
Destination Unreachable: Communication Administratively Prohibited (Type 3, Code 13)
```

Para simplificar el desarrollo del código, se ha dejado en el Campus Virtual el fichero ip-icmp-ping.h, que contiene las estructuras de datos (cabecera IP, cabecera ICMP, datagrama ICMP) que son necesarias para implementar la funcionalidad del servicio `ping`. Para hacer uso de este fichero, simplemente hay que copiarlo al directorio donde se encuentre miping-apellidos.c y, a continuación, añadir al comienzo de este: `#include "ip-icmp-ping.h"`

Consideraciones:

- Al crear el socket, hay que indicar la familia `AF_INET`, el tipo `SOCK_RAW` y el protocolo `IPPROTO_ICMP`.
- Tras construir el datagrama ICMP, hay que usar la función `sendto(2)` para enviarlo al destino. Esta función se encarga, a su vez, de añadir la cabecera IP. Sin embargo, al recibir la respuesta con `recvfrom(2)`, **no** se suprime la cabecera IP. Por tanto, el buffer de recepción contendrá los 20 bytes de la cabecera IP y, a continuación, el datagrama ICMP. Esto permitirá indagar en la cabecera IP para extraer el valor del campo TTL (evita que datagrama ICMP viaje indefinidamente por la red)
- El servicio `ping` no funciona correctamente si la petición se envía a la dirección IP local. Si se hace, la capa de transporte devolverá el propio mensaje ICMP sin procesar, pero no la respuesta esperada.

4. Criterios de Evaluación y Condiciones de Entrega

1. La práctica debe realizarse en la máquina virtual asignada en Matrix.
2. El fichero de código fuente debe comenzar con un comentario con el siguiente formato:

   ```
   // Practica Tema 8: Apellido1 Apellido2, Nombre
   ```

3. El código desarrollado debe incluir comentarios que permitan comprobar que el alumno comprende perfectamente el significado de cada línea de código. De lo contrario, se penalizará con dos puntos la calificación obtenida.
4. El cliente debe compilar sin mostrar advertencias (*warnings*) ni errores. De lo contrario, se penalizará con tres puntos la calificación obtenida.
5. Esta práctica representa un 25 % en la calificación de las prácticas de la asignatura.
6. Cuando esté finalizada, se subirá a la tarea habilitada en el Campus Virtual el fichero de código fuente (sin comprimir) con el siguiente nombre: miping-apellidos.c. Un fallo en las condiciones de entrega supondrá un punto menos en la calificación.
7. Se utilizará un sistema automático de detección de copias. En caso de copia, los alumnos involucrados figurarán como suspensos en la convocatoria ordinaria, debiendo enviar todas las prácticas por correo electrónico al profesor para poder presentarse a la convocatoria extraordinaria. En esta situación, todas las prácticas se corregirán sobre 7.
8. Fecha de Entrega: **20 de diciembre de 2023 a las 23:55**.
9. No se admitirán entregas fuera de plazo.