

Observe la diferencia de tiempos. ¿Cómo hace ping para saber que los paquetes se pierden?

```
raul@raul:~$ ping localhost ($ ping mi_direccion_IP)
PING localhost(localhost (::1)) 56 data bytes
64 bytes from localhost (::1): icmp_seq=1 ttl=64 time=0.044 ms
64 bytes from localhost (::1): icmp_seq=2 ttl=64 time=0.075 ms
64 bytes from localhost (::1): icmp_seq=3 ttl=64 time=0.031 ms

raul@raul:~$ ping 192.168.1.1 ($ ping direccion_IP_de_mi_vecino)
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.529 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.316 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.343 ms
```

ping detecta los paquetes que se pierden, si el equipo destinatario no responde.

Analicen, a continuación, las tramas capturadas ayudándose para ello de las siguientes cuestiones.**Para la trama Ethernet que contiene el mensaje "echo request":**

¿Cuál es la dirección Ethernet de 48-bit del interfaz de red de tu ordenador?

Source: (96-48-fb-c3-51-c5)

¿Cuál es la dirección Ethernet destino dentro de la trama Ethernet? ¿A qué dispositivo pertenece dicha dirección?

Destination: (74:d4:35:2e:05:5c)

Pertenece al equipo destino (compañero de clase).

¿Cuál es el valor hexadecimal del campo Tipo de Trama (Frame Type)?

Type: IPv4 (0x0800)

¿Qué tamaño tiene el campo de datos de esta trama Ethernet?

2 octetos (16 bits)

Y para la trama Ethernet que contiene el mensaje de respuesta "echo reply":

¿Cuál es la dirección Ethernet origen dentro de la trama Ethernet? ¿A qué dispositivo pertenece dicha dirección?

Source: (74:d4:35:2e:05:5c)

Pertenece al equipo origen (compañero de clase).

¿Cuál es la dirección destino dentro de la trama Ethernet? ¿A qué dispositivo pertenece dicha dirección?

Destination: (96-48-fb-c3-51-c5)

Pertenece al equipo destino (mi equipo).

¿Cuál es el valor hexadecimal del campo Tipo de Trama (Frame Type)?

Type: IPv4 (0x0800)

¿Qué tamaño tiene el campo de datos de esta trama Ethernet?

2 octetos (16 bits)

Muestre al profesor de prácticas el valor del campo, dentro de la cabecera IP, que ha permitido saber al analizador que el contenido del paquete IP era un paquete ICMP.

```
Internet Protocol Version 4, Src: 172.16.8.138, Dst: 172.16.8.204
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xcf3a (53050)
  > Flags: 0x4000, Don't fragment
    Time to live: 64
  Protocol: ICMP (1)
  Header checksum: 0x01f8 [validation disabled]
  [Header checksum status: Unverified]

0010  00 54 cf 3a 40 00 40 01 01 f8 ac 10 08 8a ac 10  .T.:@.@. ....
0020  08 cc 08 00 04 6a 6a 03 00 01 71 0f 7b 5f 00 00  .jj. .q.{_..
0030  00 00 de 4f 00 00 00 00 00 00 10 11 12 13 14 15  .0.....
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..... !"#$$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060  36 37 67
```

Protocol (ip.proto), 1 byte