Problemas de Redes de Computadores.
Grado en Ingeniería Informática
Conjunto de problemas 3

Los siguientes paquetes han sido capturados, seguidos y en ese orden, en un sniffer. Se muestran las tramas capturadas a nivel Ethernet

```
0000   1A 00 00 33 33 33 1A 00  00 77 77 77 08 00 45 00   ...333...www..E.
0010   00 28 00 2A 00 00 40 06  65 92 C0 A8 01 07 50 50   .(.*..@.e.....PP
0020   03 15 3B 6D 00 6E 00 00  00 2A 00 00 00 00 50 02   ..;m.n...*....P.
0030   20 00 3E C9 00 00                                   .>...
```

```
0000   1A 00 00 33 33 33 1A 00  00 55 55 55 08 00 45 00   ...333...UUU..E.
0010   00 28 00 2A 00 00 33 06  5E E3 C0 A8 01 05 64 01   .(.*..3.^.....d.
0020   03 15 00 0A 00 50 00 00  00 64 00 00 00 00 50 02   .....P...d....P.
0030   20 00 66 61 00 00                                   .fa..
```

```
0000   1A 00 00 33 33 33 1A 00  00 55 55 55 08 00 45 00   ...333...UUU..E.
0010   00 38 00 2A 00 00 33 11  9F D8 C0 A8 01 05 25 04   .8.*..3.......%.
0020   01 02 00 0A 00 50 00 24  55 EE 6C 73 64 51 32 79   .....P.$U.lsdQ2y
0030   33 49 78 4D 79 73 58 63  36 31 53 68 4B 65 79 4E   3IxMysXc61ShKeyN
0040   6D 31 44 43 41 3D                                 m1DCA=
```

```
0000   1A 00 00 77 77 77 1A 00  00 33 33 33 08 00 45 00   ...www...333..E.
0010   00 28 8A 5E 00 00 36 06  E5 5D C0 A8 01 07 50 50   .(.^..6..]....PP
0020   03 15 00 6E 3B 6D 00 75  4E 07 00 00 00 2B 50 12   ...n;m.uN....+P.
0030   20 00 F0 3B 00 00                                   ..;..
```

```
0000   1A 00 00 55 55 55 1A 00  00 33 33 33 08 00 45 00   ...UUU...333..E.
0010   00 28 79 FF 00 00 30 06  E8 0D 64 01 03 15 C0 A8   .(y...0...d.....
0020   01 05 00 50 00 0A 00 00  00 00 00 00 00 00 50 04   ...P..........P.
0030   20 00 66 C3 00 00                                   .f...
```

```
0000   1A 00 00 33 33 33 1A 00  00 77 77 77 08 00 45 00   ...333...www..E.
0010   00 28 00 2B 00 00 40 06  65 91 C0 A8 01 07 50 50   .(.+..@.e.....PP
0020   03 15 3B 6D 00 6E 00 00  00 2B 00 75 4E 08 50 10   ..;m.n...+.uN.P.
0030   20 00 F0 3C 00 00                                   ..<..
```

Pregunta 3.1: ¿Qué protocolos de cada nivel hay presentes en cada paquete?

Pregunta 3.2: Indique razonadamente que aplicación ha generado los paquetes anteriores

Pregunta 3.3: A la vista de los paquetes anteriores explique que equipos (ordenadores y routers) puede identificar en dicha red privada y que direcciones conoce de dichos equipos.

Pregunta 3.4: Indique razonadamente para cada paquetes de los anteriores si el que pertenece a la red privada es el cliente o el servidor

Pregunta 3.5: Indique razonadamente si los paquetes anteriores pertenecen a la misma o a distintas conexiones TCP

Pregunta 3.6: ¿A cuantas conexiones TCP diferentes pertenecen los paquetes anteriores?

Pregunta 3.7: ¿Cuantas establecimientos completos de conexiones TCP diferentes se pueden ver en los paquetes anteriores?

Los siguientes paquetes han sido capturados, seguidos y en ese orden, en un sniffer. Se muestran las tramas capturadas a nivel Ethernet

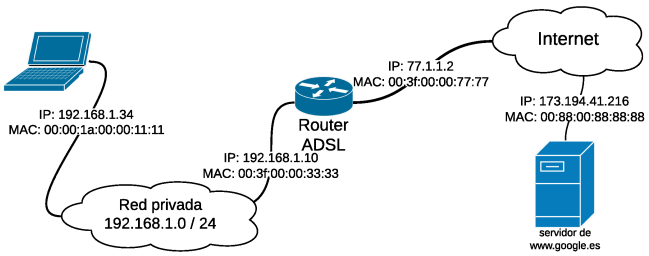
```
0000   1A 00 00 33 33 33 1A 00  00 77 77 77 08 00 45 00   ...333...www..E.
0010   00 28 00 2A 00 00 33 06  FA 8E 53 01 03 0C 35 01   .(.*..3...S...5.
0020   02 0A 4E 20 00 19 00 00  00 2A 00 00 00 00 50 02   ..N .....*....P.
0030   20 00 B4 67 00 00                                  ..g..

0000   1A 00 00 33 33 33 1A 00  00 77 77 77 08 00 45 00   ...333...www..E.
0010   00 28 00 2A 00 00 33 06  CD 66 82 14 01 21 35 01   .(.*..3..f...!5.
0020   02 0A 4E 20 00 19 00 00  00 2A 00 00 00 00 50 02   ..N .....*....P.
0030   20 00 87 3F 00 00                                  ..?..

0000   1A 00 00 33 33 33 1A 00  00 77 77 77 08 00 45 00   ...333...www..E.
0010   00 28 00 2A 00 00 33 06  37 37 17 64 02 01 35 01   .(.*..3.77.d..5.
0020   02 0A 4E 20 00 19 00 00  00 2A 00 00 00 00 50 02   ..N .....*....P.
0030   20 00 F1 0F 00 00                                  .....

0000   1A 00 00 77 77 77 1A 00  00 33 33 33 08 00 45 00   ...www...333..E.
0010   00 28 8A 5E 00 00 3F 06  64 5A 35 01 02 0A 53 01   .(.^..?.dZ5...S.
0020   03 0C 4E 20 00 19 00 75  4E 07 00 00 00 2B 50 12   ..N ...uN....+P.
0030   20 00 65 DA 00 00                                  .e...

0000   1A 00 00 33 33 33 1A 00  00 77 77 77 08 00 45 00   ...333...www..E.
0010   00 28 00 2A 00 00 33 06  EA 97 64 01 02 03 35 01   .(.*..3...d...5.
0020   02 0A 4E 20 00 19 00 00  00 2A 00 00 00 00 50 02   ..N .....*....P.
0030   20 00 A4 70 00 00                                  ..p..
```

Pregunta 3.8: ¿Qué protocolos de cada nivel hay presentes en cada paquete?

Pregunta 3.9: ¿A que aplicación pertenecen? ¿Han sido enviados por el cliente o por el servidor?

Pregunta 3.10: ¿Cuales son los orígenes y destinos de cada paquete? A nivel de enlace y a nivel de red.

Pregunta 3.11: ¿Pertenecen a la misma o a distintas conexiónes? ¿Cuantas y cuales conexiones puede identificar?

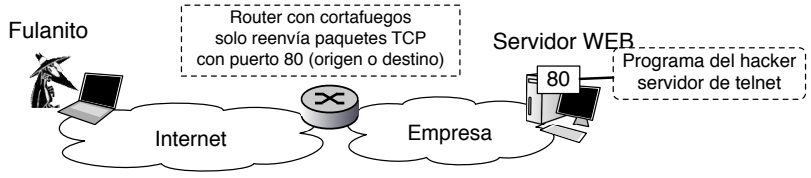


Pregunta 3.12: Un usuario residencial tiene una red como la de la figura. En un momento dado hace un ping a `www.google.com`. Obteniendo el siguiente resultado

```
$ ping www.google.es
PING www.google.es (173.194.41.216): 56 data bytes
64 bytes from 173.194.41.216: icmp_seq=0 ttl=55 time=31.228 ms
```

Seguidamente el usuario introduce en el navegador la dirección http://www.google.es

Explique los primeros 5 paquetes que se verán en la red de área local 192.168.1.0/24 tras pulsar el ENTER para que el navegador pida la pagina. Indicando que protocolos transportarán y cuales serán sus direcciones origen y destino, tanto MAC como IP y los puertos origen y destino si procede.



Pregunta 3.13: Dada la siguiente trama de nivel de enlace Ethernet II (en la que se ha eliminado el preambulo y CRC) capturado en una red local de un abonado ADSL.

```
Posicion  Datos                                                 ASCII
00000028  00 a0 c5 9d 52 00 00 0c  93 45 2d 74 08 00 45 10  |....R....E-t..E.|
00000038  00 3c 44 39 40 00 40 06  0d ac c0 a8 01 0c 82 ce  |.<D9@.@.........|
00000048  a4 44 e9 36 00 17 95 9e  d2 87 00 00 00 00 a0 02  |.D.6............|
00000058  ff ff e8 f5 00 00 02 04  05 b4 01 03 03 00 01 01  |................|
00000068  08 0a 7e f5 cb 7f 00 00  00 00                    |..~.......|
```

Indique cual de las siguientes afirmaciones son ciertas.
a) Es un paquete TCP
b) Es un paquete UDP
c) Es un paquete IP
e) Es un paquete ARP
f) Es un paquete ICMP

Pregunta 3.14: Sobre el paquete de la pregunta anterior capturado en una red local de un abonado ADSL. Indique cuales de las siguientes afirmaciones son ciertas
a) El paquete transporta datos de nivel de aplicacion
b) El cliente es la dirección IP de rango privado
c) El paquete ha sido generado por una petición Web
d) El paquete ha sido generado por una consulta de correo por POP o IMAP
e) El paquete ha sido generado por una sesión de Telnet
f) Ninguna de las dos direcciones IP es de rango privado
g) La dirección IP del router indica que el fabricante del router es Cisco

Pregunta 3.15: Dada la siguiente trama de nivel de enlace Ethernet II (en la que se ha eliminado el preambulo y CRC) capturado en una red local de un abonado ADSL.

```
0x0000:  0014 5122 7276 00a0 c59d 52db 0800 4500  ..Q"rv....R...E.
0x0010:  0073 8213 4000 ff11 74f3 c0a8 01fe c0a8  .s..@...t.......
0x0020:  0124 0035 c543 005f c270 94d7 8180 0001  .$.5.C._.p......
0x0030:  0000 0001 0000 0477 6562 3105 736b 7970  .......web1.skyp
0x0040:  6503 636f 6d00 001c 0001 c011 0006 0001  e.com...........
0x0050:  0000 0258 002b 036e 7331 0573 6b79 7065  ...X.+.ns1.skype
0x0060:  036e 6574 0005 7768 6565 6cc0 30a9 510e  .net..wheel.0.Q.
0x0070:  5400 00a8 c000 000e 1000 1baf 8000 000e  T...............
0x0080:  104b 5396 f2                             .KS..
```

Indique cual de las siguientes afirmaciones son ciertas.
a) Es un paquete TCP
b) Es un paquete UDP
c) Es un paquete IP
e) Es un paquete ARP
f) Es un paquete ICMP

Pregunta 3.16: Sobre el paquete de la pregunta anterior capturado en una red local de un abonado ADSL. Indique cuales de las siguientes afirmaciones son ciertas

a) El paquete transporta datos de nivel de aplicacion

b) El cliente es la dirección IP de rango privado

c) El paquete corresponde a una conexión TCP hacia la dirección de rango privado

d) El paquete corresponde a una conexión TCP hacia la dirección de rango público

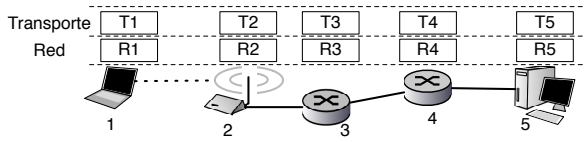
e) El paquete lo ha enviado un servidor del servicio _____

f) Ninguna de las dos direcciones IP es de rango privado

g) El paquete lo ha enviado un cliente del servicio _____

Problema 3.17: Se muestra a continuación un paquete TCP entregado por la tarjeta ethernet al sistema operativo. La tarjeta entrega la trama ethernet eliminando el campo de preámbulo y el CRC. Identifique las direcciones MAC, IP y puertos origen y destino. ¿Cual será el campo ACK del paquete que confirme la recepción de este paquete mostrado?

```
08 00 20 96  00 71 00 50  E4 66 3B 0B  08 00 45 00  .. ..q.P.f;...E.
00 45 46 6C  40 00 40 06  A7 DC 82 CE  A0 61 82 CE  .EFl@.@......a..
A6 6C C5 77  00 6E 09 71  CC 3C 5D 1F  F5 8D 80 18  .l.w.n.q.<].....
82 18 34 B3  00 00 01 01  08 0A 6E C6  0F E5 0C 96  ..4.......n.....
51 29 55 53  45 52 20 6D  69 6B 65 6C  2E 69 7A 61  Q)USER mikel.iza
6C 0D 0A                                          l..
```



Pregunta 3.18: En el escenario de la figura, utilizo un programa de correo en el ordenador 1 para leer mi correo almacenado en el servidor POP en el ordenador 5. ¿Qué niveles de transporte de los mostrados en la figura procesan un paquete que incluye mi nombre de usuario y mi contraseña?

a) Sólo T1 que es el que construye los paquetes

b) Sólo los extremos de la comunicación T1 y T5

c) Todos: T1, T2, T3, T4, T5

d) Todos menos T2 ya que no es un router y no transporta los paquetes

Problema 3.19: En una conexión TCP para una transferencia de ficheros entre los hosts H1 y H2 (ver figura), al transmitir un paquete entre R2 y R3 y debido a interferencias en el cable se cambian algunos bits en los datos transportados por TCP por lo que R3 los recibe cambiados. ¿Qué nivel de protocolos y en qué equipo descartará el paquete?

Problema 3.20: El siguiente paquete TCP ha sido capturado en el ordenador de dirección IP 130.206.169.177. Indique

a) si es un paquete enviado o recibido.

b) que tipo de paquete TCP es y en que estado se encuentran los niveles TCP origen y destino en el instante en que se ha capturado este paquete.

c) cual será el número de secuencia y de ACK del paquete que enviará el destino como respuesta a esta paquete.

d) que bytes corresponden a opciones de la cabecera IP, a opciones de la cabecera TCP y a datos transportados por el paquete. No hace falta decir que significan las opciones sólo donde están en el paquete.

```
00000000  45 00 00 34 46 54 40 00  40 06 9b 4c 82 ce a9 b1  |E..4FT@.@..L....|
00000010  82 ce a9 d5 e4 14 00 19  5a 53 1f 21 f6 ad 93 f9  |........ZS.!....|
00000020  80 11 ff ff 59 4a 00 00  01 01 08 0a 31 c6 2d 56  |....YJ......1.-V|
00000030  59 ca 95 39                                       |Y..9|
```

Pregunta 3.21: Fulanito el hacker consigue infiltrarse en el servidor Web de una empresa detrás de un cortafuegos que sólo deja pasar los paquetes que tienen puerto origen 80 o puerto destino 80. Para dejarse una puerta abierta, instala un servidor de telnet que escucha en el puerto 80 de ese ordenador. Pero cuando intenta conectarse a su servidor de telnet no le funciona... ¿Por qué no funciona?

a) Porque telnet sólo puede funcionar en el puerto 23 como manda el RFC-854

b) Porque los usuarios remotos no sabrán que el servidor está en el puerto 80

c) Porque no se puede tener dos aplicaciones TCP escuchando en el puerto 80

d) Porque telnet usa UDP y el cortafuegos sólo deja pasar los paquetes con el puerto 80 TCP

Problema 3.22: El siguiente paquete capturado en la universidad es un paquete UDP

```
0x0000:  4500 003c 4f9a 0000 4011 0000 82ce a9b1  E..<O...@.......
0x0010:  82ce a66e c5c7 0035 0028 55f6 14f1 0100  ...n...5.(U.....
0x0020:  0001 0000 0000 0000 0377 7777 0667 6f6f  .........www.goo
0x0030:  676c 6503 636f 6d00 0001 0001            gle.com.....
```

¿A qué protocolo de nivel de aplicación pertenece? ¿Es una pregunta o una respuesta?

Problema 3.23: El siguiente paquete capturado en la universidad es un paquete UDP

```
0x0000:  4500 0138 0000 4000 3f11 e4f8 82ce a66e  E..8..@.?......n
0x0010:  82ce a9b1 0035 c5c7 0124 7ce0 14f1 8180  .....5...$|.....
0x0020:  0001 0007 0004 0004 0377 7777 0667 6f6f  .........www.goo
0x0030:  676c 6503 636f 6d00 0001 0001 c00c 0005  gle.com.........
0x0040:  0001 0003 5b28 0008 0377 7777 016c c010  ....[(...www.l..
0x0050:  c02c 0001 0001 0000 0110 0004 d155 e563  .,...........U.c
0x0060:  c02c 0001 0001 0000 0110 0004 d155 e567  .,...........U.g
0x0070:  c02c 0001 0001 0000 0110 0004 d155 e568  .,...........U.h
0x0080:  c02c 0001 0001 0000 0110 0004 d155 e569  .,...........U.i
0x0090:  c02c 0001 0001 0000 0110 0004 d155 e56a  .,...........U.j
0x00a0:  c02c 0001 0001 0000 0110 0004 d155 e593  .,...........U..
0x00b0:  c010 0002 0001 0000 a53d 0006 036e 7334  .........=...ns4
0x00c0:  c010 c010 0002 0001 0000 a53d 0006 036e  ...........=...n
0x00d0:  7331 c010 c010 0002 0001 0000 a53d 0006  s1...........=..
0x00e0:  036e 7332 c010 c010 0002 0001 0000 a53d  .ns2...........=
0x00f0:  0006 036e 7333 c010 c0b2 0001 0001 0000  ...ns3..........
0x0100:  ad7b 0004 d8ef 200a c0c4 0001 0001 0000  .{..............
0x0110:  ad7b 0004 d8ef 220a c0d6 0001 0001 0000  .{....".........
0x0120:  ad7b 0004 d8ef 240a c0a0 0001 0001 0000  .{....$.........
0x0130:  ad7b 0004 d8ef 260a                      .{....&.
```

¿A qué protocolo de nivel de aplicación pertenece? ¿Es una pregunta o una respuesta?

Problema 3.24: El siguiente paquete capturado en la universidad es un paquete TCP

```
0x0000:  4500 003c 0000 4000 3e06 ed8b 82ce 9fe2
0x0010:  82ce a9b1 024b ec0c d673 c9f2 b025 1c8a
0x0020:  a012 16a0 26c7 0000 0204 05b4 0402 080a
0x0030:  94c5 2654 40b6 6421 0103 0300
```

Indique cuales de los siguientes son correctos

a) Es un paquete de cliente a servidor

b) Es un paquete de servidor a cliente

c) El paquete transporta datos de aplicacion

d) Es un paquete de datos

e) Es un paquete de ACK

f) Es un paquete de establecimiento de conexión

e) Es un paquete de cierre de conexion

¿Cual debería ser el valor del campo ACK del paquete que confirme la recepción de este paquete mostrado?

Problema 3.25: Los siguientes paquetes pertenecen a una misma conexión TCP

```
0x0000:  4510 0045 115d 4000 4006 0000 82ce a9b1  E..E.]@.@.......
0x0010:  82ce 9fe5 ec3a 006e a62c d997 5692 4a8f  .....:.n.,..V.J.
0x0020:  8018 ffff 4f6b 0000 0101 080a 40b6 8a50  ....Ok......@..P
0x0030:  d025 e50f 5553 4552 206d 696b 656c 2e69  .%..USER.mikel.i
0x0040:  7a61 6c0d 0a                             zal..
```

```
0x0000:  4500 0034 af72 4000 3e06 3e1e 82ce 9fe5  E..4.r@.>.>.....
0x0010:  82ce a9b1 006e ec3a 5692 4a8f a62c d9a8  .....n.:V.J..,..
0x0020:  8010 05a8 83b0 0000 0101 080a d025 f564  .............%.d
0x0030:  40b6 8a50                                @..P
```

```
0x0000:  4500 004c af74 4000 3e06 3e04 82ce 9fe5  E..L.t@.>.>.....
0x0010:  82ce a9b1 006e ec3a 5692 4a8f a62c d9a8  .....n.:V.J..,..
0x0020:  8018 05a8 808d 0000 0101 080a d025 f564  .............%.d
0x0030:  40b6 8a50 2b4f 4b20 5061 7373 776f 7264  @..P+OK.Password
0x0040:  2072 6571 7569 7265 642e 0d0a            .required...
```

```
0x0000:  4510 0034 5136 4000 4006 0000 82ce a9b1  E..4Q6@.@.......
0x0010:  82ce 9fe5 ec3a 006e a62c d9a8 5692 4aa7  .....:.n.,..V.J.
0x0020:  8010 ffff 4f5a 0000 0101 080a 40b6 8a50  ....OZ......@..P
0x0030:  d025 f564                                .%.d
```

```
0x0000:  4510 0045 9a0d 4000 4006 0000 82ce a9b1  E..E..@.@.......
0x0010:  82ce 9fe5 ec3a 006e a62c d9a8 5692 4aa7  .....:.n.,..V.J.
0x0020:  8018 ffff 4f6b 0000 0101 080a 40b6 8ab6  ....Ok......@...
0x0030:  d025 f564 5041 5353 2061 7361 6265 7263  .%.dPASS.asaberc
0x0040:  7561 6c0d 0a                             ual..
```

Indique cuales transportan datos y cuales son simplemente ACKs.

¿Cual es el siguiente numero de secuencia y ACK que esperaría encontrar en el siguiente paquete de servidor a cliente?

Identifique los datos del protocolo de nivel de aplicación del tercer paquete.

Problema 3.26: La siguiente traza ha sido capturada en la red de la universidad

```
 1 0.963491 IP 130.206.168.45.60905 > 193.252.23.108.110: S 2357731200:2357731200(0) win 65535
 2 0.964072 IP 193.252.23.108.110 > 130.206.168.45.60905: S 1061601894:1061601894(0) ack 2357731201 win 5792
 3 0.964129 IP 130.206.168.45.60905 > 193.252.23.108.110: . ack 1061601895 win 65535
 4 1.111168 IP 193.252.23.108.110 > 130.206.168.45.60905: P 1061601895:1061601927(32) ack 2357731201 win 5792
 5 1.111753 IP 130.206.168.45.60905 > 193.252.23.108.110: P 2357731201:2357731218(17) ack 1061601927 win 65535
 6 1.112349 IP 193.252.23.108.110 > 130.206.168.45.60905: . ack 2357731218 win 5792
 7 1.200422 IP 193.252.23.108.110 > 130.206.168.45.60905: P 1061601927:1061601956(29) ack 2357731218 win 5792
 8 1.200834 IP 130.206.168.45.60905 > 193.252.23.108.110: P 2357731218:2357731232(14) ack 1061601956 win 65535
 9 1.201287 IP 193.252.23.108.110 > 130.206.168.45.60905: . ack 2357731232 win 5792
10 1.711614 IP 193.252.23.108.110 > 130.206.168.45.60905: P 1061601956:1061601991(35) ack 2357731232 win 5792
11 1.712040 IP 130.206.168.45.60905 > 193.252.23.108.110: P 2357731232:2357731238(6) ack 1061601991 win 65535
12 1.712630 IP 193.252.23.108.110 > 130.206.168.45.60905: . ack 2357731238 win 5792
13 1.861177 IP 193.252.23.108.110 > 130.206.168.45.60905: P 1061601991:1061602000(9) ack 2357731238 win 5792
14 1.861596 IP 130.206.168.45.60905 > 193.252.23.108.110: P 2357731238:2357731244(6) ack 1061602000 win 65535
15 1.862059 IP 193.252.23.108.110 > 130.206.168.45.60905: . ack 2357731244 win 5792
16 2.064350 IP 193.252.23.108.110 > 130.206.168.45.60905: P 1061602000:1061602005(5) ack 2357731244 win 5792
17 2.065276 IP 130.206.168.45.60905 > 193.252.23.108.110: F 2357731244:2357731244(0) ack 1061602005 win 65535
18 2.065890 IP 193.252.23.108.110 > 130.206.168.45.60905: . ack 2357731245 win 5792
19 2.065894 IP 193.252.23.108.110 > 130.206.168.45.60905: F 1061602005:1061602005(0) ack 2357731245 win 5792
20 2.065957 IP 130.206.168.45.60905 > 193.252.23.108.110: . ack 1061602006 win 65535
```

a) Indique a qué aplicación pertenece y qué acción del usuario ha causado esos paquetes

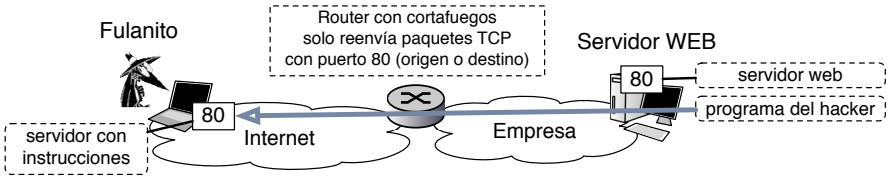
b) Indique cual es el cliente y cual el servidor en esta acción (con sus direcciones IP)

c) Haga una tabla para el cliente y otra para el servidor, indicando en qué estado de conexión estaba TCP al principio y en que estado ha quedado después de enviar o recibir cada paquete mostrado.

Problema 3.27: ¿Cuáles de estas funciones provoca el envío de algún paquete a la red?

`socket()` `connect()` `recvfrom()` `sendto()` `bind()` `listen()` `accept()`

Problema 3.28: ¿Como se detecta desde un programa que los datos entregados a un socket TCP pueden haber sufrido errores y no ser correctos?



Pregunta 3.29: Fulanito el hacker consigue infiltrarse en el servidor Web de una empresa detrás de un cortafuegos que sólo deja pasar los paquetes que tienen puerto origen 80 o puerto destino 80. Para dejarse una puerta abierta, instala un programa que cada cierto tiempo establece una conexión con el puerto 80 de un servidor externo controlado por él y se descarga instrucciones por HTTP ¿Qué problema tiene esto?

a) Que HTTP no puede funcionar en el puerto 80 porque el puerto está reservado para la web

b) No tiene ningún problema y debería funcionar

c) Que no se puede tener una conexión TCP al puerto 80 y a la vez escuchar conexiones en el puerto 80

d) Que HTTP usa UDP y el cortafuegos sólo deja pasar los paquetes con el puerto 80 TCP