

Problema 1

Suponga que un emisor TCP está enviando ventanas de 65.536 bytes sobre un canal de 100 Mbps. El tiempo de ida y vuelta es de 20 ms. ¿Cuál será el máximo rendimiento (throughput) alcanzable?, en los siguientes casos:

1. MSS= 64 Kbytes (65.536 bytes).
2. MSS= 1 Kbyte.
3. En el inicio de la conexión el otro extremo no ha incluido en el segmento de SYN ningún valor de RMSS y la MTU de la subred a la que está conectado dicho emisor TCP es de 1500 bytes.

Suponga que no se utilizan ACKs retardados y desprecie el tamaño de las distintas cabeceras.

Problema 2

Sean dos máquinas conectadas por un enlace full-duplex de 10 Mbps de capacidad, que establecen una conexión TCP para hacer la copia de seguridad de un archivo desde el cliente al servidor. Se sabe que:

- Ambos extremos indicaron en el establecimiento de la conexión un MSS de 2048 bytes
- Durante toda la conexión ambos extremos anuncian una ventana de 8192 bytes,
- Suponga que cada máquina envía inmediatamente un asentimiento por cada segmento recibido
- En condiciones normales el cliente se encarga tanto del establecimiento como del cierre de la conexión TCP
- El protocolo de aplicación que siguen para hacer la copia de seguridad ha sido diseñado específicamente con tal fin y consiste en el siguiente intercambio de mensajes:

```
Cliente -> Servidor: PUT <nombre del archivo>
Servidor -> Cliente: LISTO
Cliente -> Servidor: <<contenido del archivo>>
Servidor -> Cliente: RECIBIDO
```

1. Muestre en un diagrama temporal, que incluya la evolución de la ventana_efectiva, los segmentos intercambiados para la realización del proceso completo de la copia de seguridad del archivo incremental-lunes.tgz de tamaño $N=6 \cdot \text{MSS}$ bytes. Detalle el contenido de cada uno de los segmentos incluidos en el diagrama temporal utilizando una tabla como la mostrada al final de la página.
2. Muestre en un diagrama temporal, que incluya la evolución de la ventana_efectiva, los segmentos intercambiados en la realización del proceso completo de la copia de seguridad del archivo incremental-martes.tgz de tamaño $N=12 \cdot \text{MSS}$ bytes. Detalle el contenido de cada uno de los segmentos incluidos en el diagrama temporal utilizando una tabla como la mostrada al final de la página.

- Suponga que se pierde el segmento que lleva el comando inicial (PUT), ¿cómo detectará el emisor que debe retransmitir el segmento? Razone como afectará este hecho en el tiempo total consumido para transmitir el fichero.
- Suponga que transmitiendo el archivo incremental-martes.tgz se pierde el segmento de datos número 5, de todos los enviados en el sentido cliente.servidor ¿cómo presumiblemente detectará el emisor que debe retransmitir el segmento?

Tabla a incluir en apartado 1. y 2.:

| Nº segmento | Máquina genera segmento | Flags | Número de secuencia | Número de confirmación (próximo byte a recibir) | Datos (primer byte:último byte) |
|-------------|-------------------------|-------|---------------------|---|---------------------------------|
| | | | | | |

Problema 3

Comentar, paquete por paquete, la siguiente traza, indicando los diferentes mecanismos de TCP que aparecen reflejados en ella y explicando los diferentes valores de los campos ACK y WIN. ¿A qué protocolo de nivel de aplicación corresponden los datos que se están enviando en esta traza?

```

1 17:39:50.281054 host1.uc3m.es.1124 > host2.uvigo.es.80 S 2184508503:2184508503(0) win 32120
2 17:39:50.319074 host2.uvigo.es.80 > host1.uc3m.es.1120 R 1282387970:1282387970(0) win 0
3 17:39:50.333423 host2.uvigo.es.80 > host1.uc3m.es.1124 S 3613415056:3613415056(0) ack 2184508504 win 10136
4 17:39:50.333456 host1.uc3m.es.1124 > host2.uvigo.es.80 . 1:1(0) ack 1 win 32120
5 17:39:50.333784 host1.uc3m.es.1124 > host2.uvigo.es.80 P 1:298(297) ack 1 win 32120
6 17:39:50.368997 host2.uvigo.es.80 > host1.uc3m.es.1124 . 1:1(0) ack 298 win 9839
7 17:39:50.388233 host2.uvigo.es.80 > host1.uc3m.es.1124 . 1:1449(1448) ack 298 win 10136
8 17:39:50.388274 host1.uc3m.es.1124 > host2.uvigo.es.80 . 298:298 (0) ack 1449 win 31856
9 17:39:50.391457 host2.uvigo.es.80 > host1.uc3m.es.1124 P 1449:2897(1448) ack 298 win 10136
10 17:39:50.400969 host1.uc3m.es.1124 > host2.uvigo.es.80 . 298:298(0) ack 2897 win 30408
11 17:39:50.430218 host2.uvigo.es.80 > host1.uc3m.es.1124 . 2897:4345(1448) ack 298 win 10136
12 17:39:50.431713 host2.uvigo.es.80 > host1.uc3m.es.1124 P 4345:5793(1448) ack 298 win 10136
13 17:39:50.431751 host1.uc3m.es.1124 > host2.uvigo.es.80 . 298:298(0) ack 5793 win 31856
14 17:39:50.444519 host2.uvigo.es.80 > host1.uc3m.es.1124 . 5793:7241(1448) ack 298 win 10136
15 17:39:50.447505 host2.uvigo.es.80 > host1.uc3m.es.1124 P 7241:8689(1448) ack 298 win 10136
16 17:39:50.447558 host1.uc3m.es.1124 > host2.uvigo.es.80 . 298:298(0) ack 8689 win 31856
17 17:39:50.474946 host2.uvigo.es.80 > host1.uc3m.es.1124 . 8689:10137(1448) ack 298 win 10136
18 17:39:50.490932 host2.uvigo.es.80 > host1.uc3m.es.1124 . 13033:14481(1448) ack 298 win 10136
19 17:39:50.491002 host1.uc3m.es.1124 > host2.uvigo.es.80 . 298:298(0) ack 10137 win 31856
20 17:39:50.493419 host1.uc3m.es.1124 > host2.uvigo.es.80 . 298:298(0) ack 10137 win 31856
21 17:39:50.548361 host2.uvigo.es.80 > host1.uc3m.es.1124 . 17377:18825(1448) ack 298 win 10136
22 17:39:50.548436 host1.uc3m.es.1124 > host2.uvigo.es.80 . 298:298(0) ack 10137 win 31856
23 17:39:50.550510 host2.uvigo.es.80 > host1.uc3m.es.1124 P 18825:20273(1448) ack 298 win 10136
24 17:39:50.550541 host1.uc3m.es.1124 > host2.uvigo.es.80 . 298:298(0) ack 10137 win 31856
25 17:39:50.609269 host2.uvigo.es.80 > host1.uc3m.es.1124 . 10137:11585(1448) ack 298 win 10136
26 17:39:50.609341 host1.uc3m.es.1124 > host2.uvigo.es.80 . 298:298(0) ack 11585 win 30408
27 17:39:50.612922 host2.uvigo.es.80 > host1.uc3m.es.1124 . 11585:13033(1448) ack 298 win 10136

```

Problema 4

Realizamos una consulta DNS usando el programa dig, y obtenemos la siguiente respuesta:

```

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35947
;; flags: qr rd ra aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; QUESTION SECTION:
;dominioaptel.com. IN MX

;; ANSWER SECTION:
dominioaptel.com. 86400 IN MX 10 mx1.dominioaptel.com.

;; AUTHORITY SECTION:
dominioaptel.com. 86400 IN NS ns1.amenworld.com.
dominioaptel.com. 86400 IN NS ns2.amenworld.com.

```

```
;; ADDITIONAL SECTION:
mx1.dominioaptel.com. 86400 IN A      62.193.216.30
ns1.amenworld.com.    47645  IN      A      62.193.206.145
ns2.amenworld.com.    47645  IN      A      212.43.229.73

;; Query time: 2 msec
;; SERVER: 163.117.144.129#53(163.117.144.129)
```

Responda a las siguientes preguntas, justificando sus contestaciones:

1. ¿Para qué sirve el campo id (identificador) de la cabecera?
2. El servidor que nos está enviando esta respuesta, ¿ha obtenido esa información de su cache?
3. ¿Hemos obtenido una respuesta recursiva o iterativa?
4. ¿Qué pretendemos averiguar con esta consulta?
5. Calcule cuántos bytes ocupa el campo de petición que se está enviando en la consulta DNS.

Problema 5

A la vista de la siguiente consulta DNS: `monitor01:~> dig -t SOA lab.it.uc3m.es.`

```
;; <<>> DiG 9.2.4 <<>> -t SOA lab.it.uc3m.es.
;; global options: printcmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 7321
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 5

;; QUESTION SECTION:
lab.it.uc3m.es.                IN      SOA

;; ANSWER SECTION:
lab.it.uc3m.es.                62720  IN      SOA      lm000.lab.it.uc3m.es. sysadmin.lab.it.uc3m.es. 2005111663 300 3600 604800 60

;; AUTHORITY SECTION:
lab.it.uc3m.es.                60     IN      NS       lmserv.lab.it.uc3m.es.
lab.it.uc3m.es.                60     IN      NS       itserv.lab.it.uc3m.es.
lab.it.uc3m.es.                60     IN      NS       lm000.lab.it.uc3m.es.
lab.it.uc3m.es.                60     IN      NS       tamtam.it.uc3m.es.
lab.it.uc3m.es.                60     IN      NS       vortex.uc3m.es.

;; ADDITIONAL SECTION:
lmserv.lab.it.uc3m.es.         60     IN      A        163.117.144.67
itserv.lab.it.uc3m.es.         60     IN      A        163.117.144.68
lm000.lab.it.uc3m.es.          60     IN      A        163.117.144.129
tamtam.it.uc3m.es.             120    IN      A        163.117.139.31
vortex.uc3m.es.                149030 IN      A        163.117.131.31

;; Query time: 1 msec
;; SERVER: 163.117.144.68#53(163.117.144.68)
;; WHEN: Sun Feb 12 19:58:01 2006
;; MSG SIZE rcvd: 231
```

Responda a las siguientes preguntas (si para alguna de ellas considera que no tiene datos suficientes, diga qué otras consultas DNS necesitaría hacer para poder contestar):

1. Diga el nombre del servidor primario del dominio `lab.it.uc3m.es.`
2. Diga qué es `sysadmin.lab.it.uc3m.es.`
3. Diga qué máquina o máquinas actúan como servidoras de correo del dominio `lab.it.uc3m.es.`
4. Diga si esta respuesta ha venido de un servidor autorizado o de una cache, y cómo lo ha averiguado.
5. Diga cómo haría para obtener el nombre de domino de la máquina con dirección IP 163.117.144.128.
6. Diga cómo haría para obtener todos los registros de recurso de la zona `lab.it.uc3m.es.`

Problema 6

Conteste de forma razonada a las siguientes preguntas:

1. Diga qué consultas DNS realizaría para averiguar el servidor DNS primario y los secundarios del dominio google.com
2. Imagine que detecta un error en el dominio de DNS de google.com y que desea enviar un correo electrónico al administrador de este dominio para notificárselo. ¿Cómo averiguaría su dirección de correo?
3. Una vez que supiera su dirección de correo, ¿cómo averiguaría la dirección IP del servidor de correo al que enviar el mensaje por SMTP?

Problema 7

En un aula informática, todos los puestos tienen configurado como servidor SMTP por defecto al propio ordenador (localhost), y como servidor DNS por defecto a dns.lab.it.uc3m.es. Un alumno envía un correo electrónico desde uno de los puestos, pc05.lab.it.uc3m.es, a un amigo cuya dirección de e-mail es amigo@depto.empresa.ar.

Suponga que:

- El dominio depto.empresa.ar tiene un servidor DNS primario, dns1.depto.empresa.ar, y un secundario, dns2.depto.empresa.ar.
- El servidor dns1.depto.empresa.ar está caído en este momento.
- dns.lab.it.uc3m.es es el único servidor DNS de los consultados que soporta recursividad.
- Las caches de DNS de todos los ordenadores consultados están vacías de información relevante.

Se pide:

1. Describa todos los paquetes DNS que se intercambian (indicando qué irá en el campos más relevantes) desde que el alumno pulsa al botón “enviar” de su programa de correo electrónico hasta que el MTA de pc05.it.uc3m.es obtiene la IP de la máquina a la que enviar el correo.

Se observa el tráfico DNS en la red del aula informática y se recogen las siguientes estadísticas:

- El TTL de los registros de recurso observados en la red sigue una distribución uniforme entre 0 y 24 horas.
- La probabilidad de que el registro de recurso haya sido ya consultado en la red en los últimos t segundos sigue una función de distribución exponencial de media 12 horas:

$$F(x) = 1 - e^{-t/12 \text{ horas}}$$

Se pide:

2. Suponiendo que la caché del servidor dns.lab.it.uc3m.es es suficientemente grande, calcule la probabilidad de que el servidor nos devuelva un registro de recurso no autorizado directamente de su caché.

Problema 8

Un alumno, desde una máquina del laboratorio, quiere enviar un correo electrónico a un amigo cuya dirección de correo es `amigo@etsit.upm.es`.

Cuando pulsa en el botón “enviar” de su lector de correo, su máquina hace una consulta DNS al servidor DNS por defecto (`dns.it.uc3m.es`) y obtiene la siguiente respuesta, que mostramos con el mismo formato que usa el programa `dig` (alguna información la hemos enmascarado con `XXX`):

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58250
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
etsit.upm.es.                IN      MX

;; AUTHORITY SECTION:
etsit.upm.es.                83921   IN      NS      dir.etsit.upm.es.
etsit.upm.es.                83921   IN      NS      galileo.ccupm.upm.es.

;; ADDITIONAL SECTION:
dir.etsit.upm.es.           83921   IN      A       138.100.17.10
galileo.ccupm.upm.es.       79303   IN      A       138.100.4.4

;; Query time: 3 msec
;; SERVER: 163.117.139.120#53(dns.it.uc3m.es)
;; MSG SIZE rcvd: XXX
```

1. Explique por qué el campo de respuestas (ANSWER) está vacío, qué representa la información en la “AUTHORITY SECTION” y de dónde la ha obtenido el servidor (`dns.it.uc3m.es`).
2. Calcule el tamaño (en bytes) del mensaje DNS anterior.

En vista de la respuesta DNS anterior, el lector de correo hace una nueva consulta DNS a un servidor distinto, y recibe la siguiente respuesta:

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9795
;; flags: qr aa ra; QUERY: 1, ANSWER: 3, AUTHORITY: 2, ADDITIONAL: 5

;; QUESTION SECTION:
etsit.upm.es.                IN      MX

;; ANSWER SECTION:
etsit.upm.es.                172800  IN      MX      30 XXX
etsit.upm.es.                172800  IN      MX      20 XXX
etsit.upm.es.                172800  IN      MX      10 XXX

;; AUTHORITY SECTION:
etsit.upm.es.                172800  IN      NS      galileo.ccupm.upm.es.
etsit.upm.es.                172800  IN      NS      dir.etsit.upm.es.

;; ADDITIONAL SECTION:
smtp.etsit.upm.es.           172800  IN      A       138.100.17.3
relay.upm.es.                2162    IN      A       138.100.4.8
relay2.upm.es.               2162    IN      A       138.100.4.44
galileo.ccupm.upm.es.       2124    IN      A       138.100.4.4
dir.etsit.upm.es.           172800  IN      A       138.100.17.10

;; Query time: 14 msec
;; SERVER: XXX.XXX.XXX.XXX#53
;; MSG SIZE rcvd: 222
```

3. ¿De qué servidor DNS se está obteniendo esta respuesta? Justifique su respuesta.

Se observa a continuación que la máquina del alumno establece una conexión TCP con el puerto 25 de la máquina 138.100.17.3. Recibe por esta conexión un segmento de datos con la siguiente información en ASCII: “421 XXX<CR><LF>”, y se cierra la conexión. A continuación se observa el establecimiento de una nueva conexión TCP con el puerto 25 de la máquina 138.100.4.8.

4. Razone qué valor contenían los tres registros de recurso de la sección de respuestas (ANSWER SECTION) del mensaje DNS anterior.

El alumno observa el valor de TTL del registro de recurso de tipo A galileo.ccupm.upm.es en los dos mensajes DNS anteriores. Extrañado, decide hacer una consulta al servidor primario de ese dominio.

5. ¿Qué consulta hará el alumno a su servidor DNS por defecto para averiguar cuál es el servidor primario de ese dominio?

En la respuesta que obtiene del primario a la consulta de de tipo A de galileo.ccupm.upm.es, obtiene el siguiente resultado:

```
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 24004
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; QUESTION SECTION:
galileo.ccupm.upm.es.      IN      A

;; ANSWER SECTION:
galileo.ccupm.upm.es.    86400   IN      A      138.100.4.4

;; AUTHORITY SECTION:
ccupm.upm.es.           86400   IN      NS     einstein.ccupm.upm.es.
ccupm.upm.es.           86400   IN      NS     galileo.ccupm.upm.es.

;; ADDITIONAL SECTION:
einstein.ccupm.upm.es.  86400   IN      A      138.100.4.8

;; Query time: 5 msec
;; SERVER: XXX.XXX.XXX.XXX#53
;; MSG SIZE rcvd: 107
```

6. Explique a qué se debe la discrepancia en el valor de TTL del registro de recurso de tipo A correspondiente a galileo.ccupm.upm.es en los tres mensajes DNS de este problema.

Problema 9

Se obtiene con tcpdump la siguiente captura de tráfico en el laboratorio:

```
13:15:09.369533 IP monitor01.lab.it.uc3m.es.1023 > monitor02.lab.it.uc3m.es.513: S
802775060:802775060(0) win 5840 <mss 1460,sackOK,timestamp 6363432 0,nop,wscale 2>
 0x0000: 4500 003c 793c 4000 4006 58b1 a375 90f1  E..<y<@.X.u..
 0x0010: a375 90f2 03ff 0201 2fd9 6014 0000 0000  .u...../.'.....
 0x0020: a002 16d0 18f0 0000 0204 05b4 0402 080a  .....
 0x0030: 0061 1928 0000 0000 0103 0302  .a.(.....

13:15:09.369675 IP monitor02.lab.it.uc3m.es.513 > monitor01.lab.it.uc3m.es.1023: S
795344791:795344791(0) ack 802775061 win 5792 <mss 1460,sackOK,timestamp 6363771 6363432,nop,wscale 2>
 0x0000: 4500 003c 0000 4000 4006 d1ed a375 90f2  E..<..@.@.....
 0x0010: a375 90f1 0201 03ff 2f67 ff97 2fd9 6015  .u...../g../.'.
 0x0020: a012 16a0 cf33 0000 0204 05b4 0402 080a  .....3.....
 0x0030: 0061 1a7b 0061 1928 0103 0302  .a.{.a.(....
```

```

13:15:09.369712 IP monitor01.lab.it.uc3m.es.1023 > monitor02.lab.it.uc3m.es.513: . ack 1 win 1460
<nop,nop,timestamp 6363433 6363771>
0x0000: 4500 0034 793e 4000 4006 58b7 a375 90f1 E..4y>@.X.u..
0x0010: a375 90f2 03ff 0201 2fd9 6015 2f67 ff98 .u...../.'./g..
0x0020: 8010 05b4 0ee6 0000 0101 080a 0061 1929 .....a.)
0x0030: 0061 1a7b .a.{

13:15:09.370269 IP monitor01.lab.it.uc3m.es.1023 > monitor02.lab.it.uc3m.es.513: P 1:2(1) ack 1 win 1460
<nop,nop,timestamp 6363433 6363771>
0x0000: 4500 0035 7940 4000 4006 58b4 a375 90f1 E..5y@.X.u..
0x0010: a375 90f2 03ff 0201 2fd9 6015 2f67 ff98 .u...../.'./g..
0x0020: 8018 05b4 0edd 0000 0101 080a 0061 1929 .....a.)
0x0030: 0061 1a7b 00 .a.{

13:15:09.370597 IP monitor02.lab.it.uc3m.es.513 > monitor01.lab.it.uc3m.es.1023: . ack 2 win 1448
<nop,nop,timestamp 6363771 6363433>
0x0000: 4500 0034 e5e3 4000 4006 ec11 a375 90f2 E..4..@.u..
0x0010: a375 90f1 0201 03ff 2f67 ff98 2fd9 6016 .u...../g../'
0x0020: 8010 05a8 0ef1 0000 0101 080a 0061 1a7b .....a.{
0x0030: 0061 1929 .a.)

13:15:09.370777 IP monitor01.lab.it.uc3m.es.1023 > monitor02.lab.it.uc3m.es.513: P 2:28(26) ack 1 win 1460
<nop,nop,timestamp 6363433 6363771>
0x0000: 4500 004e 7942 4000 4006 5899 a375 90f1 E..NyB@.X.u..
0x0010: a375 90f2 03ff 0201 2fd9 6016 2f67 ff98 .u...../.'./g..
0x0020: 8018 05b4 c0d8 0000 0101 080a 0061 1929 .....a.)
0x0030: 0061 1a7b 6c61 6273 6364 006c 6162 7363 .a.{labscd.labsc
0x0040: 6400 7874 6572 6d2f 3338 3430 3000 d.xterm/38400.

13:15:09.370950 IP monitor02.lab.it.uc3m.es.513 > monitor01.lab.it.uc3m.es.1023: . ack 28 win 1448
<nop,nop,timestamp 6363771 6363433>
0x0000: 4500 0034 e5e5 4000 4006 ec0f a375 90f2 E..4..@.u..
0x0010: a375 90f1 0201 03ff 2f67 ff98 2fd9 6030 .u...../g../'0
0x0020: 8010 05a8 0ed7 0000 0101 080a 0061 1a7b .....a.{
0x0030: 0061 1929 .a.)

```

Responda a las siguientes preguntas:

1. ¿A qué protocolo corresponde esta traza? ¿Cómo lo ha averiguado?
2. ¿Con qué opciones habrá tenido que llamar a tcpdump para que sólo capture el tráfico mostrado en la traza, y no cualquier otro tráfico que haya en la red?
3. ¿Qué datos está enviando el cliente al servidor en la parte de traza que se muestra, y qué significan?
4. ¿Es el comportamiento que está observando en esta traza conforme al comportamiento teórico que vimos del protocolo en clase?
5. Según el protocolo, ¿cuál cree que será el siguiente paquete que veremos en esta traza?

Problema 10

En la siguiente negociación de opciones de TELNET, en la que hemos numerado cada línea para poder referenciarla posteriormente y en la que cierta información la hemos ocultado con ***:

```

01 telnet> open sdf.lonestar.org
02 Trying 192.94.73.1...
03 Connected to SDF.LONESTAR.ORG.
04 Escape character is '^]'.
05 SENT IAC DO SUPPRESS GO AHEAD
06 RCVD IAC *** SUPPRESS GO AHEAD
07 SENT IAC DO ECHO
08 RCVD IAC *** ECHO
09 SENT IAC WILL NAWS
10 RCVD IAC *** NAWS
11 SENT IAC SB NAWS 0 80 (80) 0 24 (24) IAC SE
12 SENT IAC WILL TSPEED
13 RCVD IAC DO TSPEED

```

```
14 RCVD IAC SB TSPEED SEND IAC SE
15 SENT IAC WILL LINEMODE
16 RCVD IAC *** LINEMODE
17 SENT IAC *** STATUS
18 RCVD IAC WILL STATUS
19 SENT IAC WONT ENVIRON
20 RCVD IAC *** ENVIRON
21 login:
```

Sabiendo que tras esta negociación el modo de operación queda en modo una línea cada vez (también denominado “kludge line mode”), diga qué iría en las marcas *** de las líneas 06, 08, 10, 16, 17 y 20.

Problema 11

Suponga que desde el ordenador maquina1 hacemos telnet a maquina2.

1. ¿Cuál es el modo de operación por defecto? Indique qué secuencia de comandos y respuestas se intercambian ambas máquinas para cambiar el modo de operación a un carácter cada vez. ¿Cómo se envían estos comandos y respuestas? ¿cuántos bytes ocuparía cada uno?
2. Nos hemos autenticado correctamente (login y password) y aparece el “prompt” de máquina2. Tecleamos “ftp maquina1” (todavía no pulsamos el retorno de carro). Indique cuántos paquetes se han enviado por la red.
3. Damos al retorno de carro nos aparece en pantalla:

```
Connected to maquina1.
220 maquina1 FTP server ready.
Name:
```

Indique cuántas conexiones tenemos abiertas entre maquina1 y maquina2, de qué tipo (TCP, UDP) y entre qué puertos.

4. Tecleo mi login, alumno, y me aparece este mensaje por pantalla:

```
331 Password required for alumno.
Password:
```

Indique cuántas paquetes se han intercambiado y qué contenía cada uno.

Problema 12

A continuación le presentamos dos capturas de tráfico pertenecientes a dos protocolos, que contienen errores (comandos o respuestas que no son legales en el protocolo). Diga qué errores encuentra y explique cómo serían si fueran correctos.

1. Captura telnet. Mostramos la salida de la aplicación telnet en el cliente con la opción de que muestre la negociación de opciones:

```
lm011:~> telnet
telnet> toggle options
Will show option processing.
telnet> open lm011.lab.it.uc3m.es
```

```

Trying 163.117.144.140...
Connected to lm011.lab.it.uc3m.es.
Escape character is '^]'.
SENT WILL SUPPRESS GO AHEAD
SENT WILL TERMINAL TYPE
SENT WILL NAWs
SENT WILL TSPEED
SENT WILL LFLOW
SENT WILL LINEMODE
SENT WILL NEW-ENVIRON
SENT DO STATUS
RCVD DO TERMINAL TYPE
RCVD DO TSPEED
RCVD DO XDISPLOC
SENT WONT XDISPLOC
RCVD DO NEW-ENVIRON
RCVD DO SUPPRESS GO AHEAD
RCVD DONT NAWs
SENT IAC SB NAWs 0 158 (158) 0 75 (75)
RCVD DO LFLOW
RCVD DONT LINEMODE
RCVD WILL STATUS
RCVD IAC SB TERMINAL-SPEED SEND
RCVD IAC SB ENVIRON SEND
SENT IAC SB ENVIRON IS
RCVD IAC SB TERMINAL-TYPE SEND
RCVD DONT ECHO
SENT WILL ECHO
Debian GNU/Linux 3.0 lm011.lab.it.uc3m.es
lm011.lab.it.uc3m.es login:

```

2. Captura rlogin. Sólo mostramos el contenido de los segmentos TCP que contienen información en la parte de datos. ”
 0representa al byte 0x00:

Segmento de datos de cliente a servidor con el siguiente contenido:
 \0

Segmento de datos de cliente a servidor con el siguiente contenido:
 labscd\0cgr\0xterm/38400\0

Segmento de datos de servidor a cliente con el siguiente contenido:
 \0

Segmento de datos de servidor a cliente con el siguiente contenido:
 Password:

Segmento de datos de cliente a servidor con el siguiente contenido:
 h

Segmento de datos de cliente a servidor con el siguiente contenido:
 o

Segmento de datos de cliente a servidor con el siguiente contenido:
 l

Segmento de datos de cliente a servidor con el siguiente contenido:
 a

Segmento de datos de cliente a servidor con el siguiente contenido:
 \n

Segmento de datos de servidor a cliente con el siguiente contenido:

\r\n

Problema 13

El método de entrega de la práctica obligatoria de la asignatura de Redes de Ordenadores II, consiste en dejar los ficheros fuente de la práctica empaquetados en un fichero `.zip`, con el nombre `<numero_grupo>_rotella.zip`, en el servidor ftp de la máquina `monitor03.lab.it.uc3m.es`. El alumno con número de grupo 1 va a realizar su entrega, `1_rotella.zip`, para ello dispone del login `grupo1` y password `rotella` para acceder al servidor FTP. La máquina desde la que se conecta el alumno es `monitor02.lab.it.uc3m.es`. Los profesores además han dejado disponible en el mismo servidor FTP el fichero `info_correccion.txt` en el que se proporciona información sobre la corrección de la práctica.

A continuación se muestra los segmentos TCP que se han capturado entre la máquina desde la que se conecta el alumno `monitor02.lab.it.uc3m.es` y el servidor ftp.

```
[1] monitor02.33837 > monitor03.ftp : S 3215980333:3215980333(0) win 5840 <mss 1460>
[2] monitor03.ftp > monitor02.33837: S 3597905054:3597905054(0) ack 3215980334 win 5792
    <mss 1460>
[3] monitor02.33837 > monitor03.ftp: . ack 1 win 5840
[4] monitor03.ftp > monitor02.33837: P 1:100(99) ack 1 win 5792
    DATOS:X20 monitor03.lab.it.uc3m.es FTP server (Version wu-2.6.2(1) Sun Apr 17 09:42:13
    UTC 2005) ready.\r\n
[5] monitor02.33837 > monitor03.ftp: . ack 100 win 5840
[6] monitor02.33837 > monitor03.ftp: P 1:14(13) ack 100 win 5840
    DATOS:XXXX grupo1\r\n
[7] monitor03.ftp > monitor02.33837: P 100:135(35) ack 14 win 5792
    DATOS:X31 Password required for grupo1.\r\n
[8] monitor02.33837 > monitor03.ftp: . ack 135 win 5840
[9] monitor02.33837 > monitor03.ftp: P 14:28(14) ack 135 win 5840
    DATOS:XXXX rotella\r\n
[10] monitor03.ftp > monitor02.33837: . ack 28 win 5792
[11] monitor03.ftp > monitor02.33837: P 135:163(28) ack 28 win 5792
    DATOS:230 User grupo1 logged in.\r\n
[12] monitor02.33837 > monitor03.ftp: . ack 163 win 5840
[13] monitor02.33837 > monitor03.ftp: P 28:34(6) ack 163 win 5840
    DATOS:SYST\r\n
[14] monitor03.ftp > monitor02.33837: . ack 34 win 5792
[15] monitor03.ftp > monitor02.33837: P 163:182(19) ack 34 win 5792
    DATOS:215 UNIX Type: L8\r\n
[16] monitor02.33837 > monitor03.ftp: . ack 182 win 5840
[17] monitor02.33837 > monitor03.ftp: P 34:42(8) ack 182 win 5840
    DATOS:TYPE I\r\n
[18] monitor03.ftp > monitor02.33837: P 182:202(20) ack 42 win 5792
    DATOS:200 Type set to I.\r\n
[19] monitor02.33837 > monitor03.ftp: . ack 202 win 5840
[20] monitor02.33837 > monitor03.ftp: P 42:71(29) ack 202 win 5840
    DATOS:XXXX XXX,XXX,XXX,XXX,132,49\r\n
```

```

[21] monitor03.ftp > monitor02.33837: P 202:232(30) ack 71 win 5792
    DATOS:200 XXXX command successful.\r\n

[22] monitor02.33837 > monitor03.ftp: P 71:91(20) ack 232 win 5840
    DATOS:STOR 1_rotella.zip\r\n

[23] XXXXXXXXXXXX > XXXXXXXXXXXX: S 3607453489:3607453489(0) win 5840 <mss 1460>

[24] XXXXXXXXXXXX > XXXXXXXXXXXX: S 3233078713:3233078713(0) ack 3607453490 win 5792 <mss 1460>

[25] XXXXXXXXXXXX > XXXXXXXXXXXX: . ack 1 win 5840

[26] monitor03.ftp > monitor02.33837: P 232:292(60) ack 91 win 5792
    DATOS:X50 Opening BINARY mode data connection for 1_rotella.zip.\r\n

[27] monitor02.33841 > monitor03.ftp-data: . 1:1449(1448) ack 1 win 5792
    DATOS: <...CONTENIDO FICHERO...>

[28] monitor03.ftp-data > monitor02.33841: . ack 1449 win 8688

[29] monitor02.33841 > monitor03.ftp-data: . 1449:2897(1448) ack 1 win 5792
    DATOS: <...CONTENIDO FICHERO...>

[30] monitor02.33841 > monitor03.ftp-data: P 2897:4345(1448) ack 1 win 5792
    DATOS: <...CONTENIDO FICHERO...>

[31] monitor03.ftp-data > monitor02.33841: . ack XXXX win 11584

[32] monitor02.33841 > monitor03.ftp-data: . 4345:5793(1448) ack 1 win 5792
    DATOS: <...CONTENIDO FICHERO...>

[33] monitor02.33841 > monitor03.ftp-data: . 5793:7241(1448) ack 1 win 5792
    DATOS: <...CONTENIDO FICHERO...>

[34] monitor02.33841 > monitor03.ftp-data: P 7241:8689 (1448) ack 1 win 5792
    DATOS: <...CONTENIDO FICHERO...>

[35] monitor03.ftp-data > monitor02.33841: . ack 5793 win 11584

[36] monitor03.ftp-data > monitor02.33841: . ack 7241 win 11584

[37] monitor03.ftp-data > monitor02.33841: . ack 8689 win 11584

[38] monitor02.33841 > monitor03.ftp-data: . XXXX:10137(1448) ack 1 win 5792
    DATOS: <...CONTENIDO FICHERO...>

[39] monitor02.33841 > monitor03.ftp-data: FP 10137:10139(1448) ack 1 win 5792
    DATOS: <...CONTENIDO FICHERO...>

[40] monitor03.ftp-data > monitor02.33841: . ack XXXXX win 11584

[41] monitor03.ftp-data > monitor02.33841: F 1:1(0) ack 10140

[42] monitor02.33841 > monitor03.ftp-data: . ack X win 5792

[43] monitor02.33837 > monitor03.ftp: . ack 292 win 5840

[44] monitor03.ftp > monitor02.33837: P 292:316(24) ack 91 win 5792
    DATOS:226 Transfer complete.\r\n

[45] monitor02.33837 > monitor03.ftp: . ack 316 win 5840

[46] monitor02.33837 > monitor03.ftp: P 91:99(8) ack 316 win 5840
    DATOS:TYPE A\r\n

[47] monitor03.ftp > monitor02.33837: P 316:336(20) ack 99 win 5792
    DATOS:200 Type set to A.\r\n

[48] monitor02.33837 > monitor03.ftp: . ack 336 win 5840

[49] monitor02.33837 > monitor03.ftp: P 99:105(6) ack 336 win 5840
    DATOS:XXXX\r\n

```

```

[50] monitor03.ftp > monitor02.33837: P 336:386(50) ack 105 win 5792
    DATOS:227 Entering ----- Mode (XXX,XXX,XXX,XXX,7,90)\r\n
[51] monitor02.33837 > monitor03.ftp: . ack 386 win 5840
[52] XXXXXXXXXXXXXXXX > XXXXXXXXXXXXXXXX: S 3252436659:3252436659(0) win 5840 <mss 1460>
[53] XXXXXXXXXXXXXXXX > XXXXXXXXXXXXXXXX: S 3633555841:3633555841(0) ack 3252436660 win 5792 <mss 1460>
[54] XXXXXXXXXXXXXXXX > XXXXXXXXXXXXXXXX: . ack 1 win 5840
[55] monitor02.33837 > monitor03.ftp: P 105:131(26) ack 386 win 5840
    DATOS:XXXX info_correccion.txt\r\n
[56] monitor03.ftp > monitor02.33837: P 386:463(77) ack 131 win 5792
    DATOS:150 Opening ASCII mode data connection for info_correccion.txt (___ bytes)\r\n
[57] monitor03.1882 > monitor02.33842: P 1:165(164) ack 1 win 5792
    DATOS: <CONTENIDO FICHERO>
[58] monitor02.33842 > monitor03.1882: . ack XXX win 6432
[59] monitor03.1882 > monitor02.33842: X 165:165(0) ack 1 win 5792
[60] monitor02.33837 > monitor03.ftp: . ack 463 win 5840
[61] monitor02.33842 > monitor03.1882: . ack XXX win 6432
[62] monitor02.33842 > monitor03.1882: F 1:1(0) ack XXX win 6432
[63] monitor03.1882 > monitor02.33842: . ack 2 win 5792
[64] monitor03.ftp > monitor02.33837: P 463:487(24) ack 131 win 5792
    DATOS:226 Transfer complete.\r\n
[65] monitor02.33837 > monitor03.ftp: . ack 487 win 5840
[66] monitor02.33837 > monitor03.ftp: P 131:137(6) ack 487 win 5840
    DATOS:QUIT\r\n
[67] monitor03.ftp > monitor02.33837: P 487:536(49) ack 137 win 5792
    DATOS:221-You have transferred ____ bytes in 2 files.\r\n
[68] monitor03.ftp > monitor02.33837: FP 536:687(151) ack 137 win 5792
    DATOS:221XTotal traffic for this session was ____ bytes in 2 transfers.\r\n
    221XThank you for using the FTP service on monitor03.lab.it.uc3m.es.\r\n
    221XGoodbye.\r\n
[69] monitor02.33837 > monitor03.ftp: . ack 688 win 5840
[70] monitor02.33837 > monitor03.ftp: F 137:137(0) ack 688 win 5840

```

1. En la traza aparecen algunos caracteres ocultos con una X indique cuál es el valor de estos caracteres.
 NOTA: La dirección IP de monitor03.lab.it.uc3m.es es 163.117.144.140 y la de monitor02.lab.it.uc3m.es es 163.117.144.242.
2. Observando las trazas, responda de forma razonada a las siguientes preguntas:
 - a) ¿Qué valor numérico se corresponde con el puerto indicado como ftp y cuál con ftp-data?
 - b) ¿En qué modo se ha transferido el fichero 1_rotella.zip y el fichero info_correccion.txt? ¿Cuál es el tamaño, en número de bytes, de ambos ficheros?
 - c) ¿Cuántas conexiones TCP se han establecido? ¿Se han finalizado todas correctamente?
 - d) ¿Considera que se implementa correctamente el algoritmo slow-start de TCP en todas las conexiones?

Problema 14

Se abre una sesión FTP en modo debug (opción -d) y se visualiza lo siguiente:

```
~> ftp -d 163.117.144.130
220 lm001.lab.it.uc3m.es FTP server
---> USER aptel
331
---> PASS XXXX
530
---> USER aptel
331
---> PASS XXXX
230
---> CWD rcs
550
---> CWD rsc
250
---> MKD rsc-hijo
257
---> TYPE XXX
200
---> PORT 163,117,139,120,7,94
200
---> RETR ejemplo.txt
150
226 Transfer complete. 134 bytes received in 0.0015 seconds (85 Kbytes/s)
---> TYPE XXX
200
---> PORT 163,117,139,120,7,97
200
---> RETR ejemplo.txt
150
226 Transfer complete. 156 bytes received in 0.0017 seconds (88 Kbytes/s)
---> PORT 163,117,139,120,7,99
200
---> STOR ejemplo1.txt
150
226
---> PORT 163,117,139,120,7,52
200
---> LIST ejemplo1.txt
150
-rw-r--r--  1 aptel  aptel                20 May 29 15:21 ejemplo1.txt ***
226
---> PORT 163,117,139,120,7,54
200
---> LIST ejemplo2.txt
150
226
---> QUIT
221
```

Averigüe los datos pedidos a continuación, razonando sus respuestas, y en aquellos casos en los que el enunciado no aporte la información suficiente para poder contestar, simplemente indique "información insuficiente":

1. La primera vez que se transfirió el fichero ejemplo.txt ¿se hizo en modo ascii o binario?

2. ¿Cuántos bytes tiene el fichero ejemplo.txt? ¿cuántas líneas?
3. ¿Cuántas conexiones TCP que se han establecido? Indique el puerto origen y destino de cada conexión.
4. Comente la visualización de la línea marcada con ***, entre las respuestas con códigos 150 y 226, e identifique la conexión por la que se han recibido.
5. Número de ficheros enviados (de cliente a servidor) y recibidos (de servidor a cliente).

Problema 15

En la siguiente sesión FTP, en la que hemos numerado cada línea para poder referenciarla posteriormente y en la que cierta información la hemos ocultado con ***:

```

01 220 monitor01.lab.it.uc3m.es FTP server
02 ---> USER labscd
03 331 Password required for labscd.
04 ---> PASS XXXX
05 230 User labscd logged in.
06 ---> SYST
07 215 UNIX Type: L8
08 ---> TYPE ***
09 200 Type set to ***.
10 ---> *** 163,117,139,250,228,198
11 200 ***
12 ---> RETR notas_reuniones.txt
13 150 Opening **** mode data connection for notas_reuniones.txt.
14 226 Transfer complete. 4077 bytes sent.
15 ---> TYPE ***
16 200 Type set to ***.
17 ---> ***
18 227 *** (163,117,144,241,230,68)
19 ---> STOR notas_reuniones.txt
20 150 Opening **** mode data connection for notas_reuniones.txt.
21 226 Transfer complete. 4213 bytes sent.
22 ---> QUIT
24 221-Total traffic for this session was 8805 bytes in 2 transfers.
25 221-Thank you for using the FTP service on monitor01.lab.it.uc3m.es.
26 221 Goodbye.
```

Diga:

- IP del cliente y servidor.
- Sentido y puertos de las conexiones TCP que se utilizan.
- Comandos de las líneas 08, 10, 15 y 17.
- Número de líneas del fichero.

Problema 16

En una sesión FTP entre dos máquinas, se intercambian los siguientes comandos y respuestas:

```

220
---> USER fulano
331
---> PASS XXXX
230
---> PORT 163,117,144,203,6,66
200
---> LIST
150
226
---> TYPE I
200
---> PORT 163,117,144,203,6,67
200
---> RETR prueba
150
226
---> PORT 163,117,144,203,6,68
200
---> RETR prueba1
550
---> TYPE A
200
---> PORT 163,117,144,203,6,69
200
---> RETR prueba2
150
226
---> QUIT
221

```

Teniendo en cuenta el intercambio anterior, averigüe los datos pedidos a continuación y en aquellos casos en los que el enunciado no aporte la información suficiente para poder contestar, simplemente indique “información insuficiente”:

1. Dirección IP del cliente FTP.
2. Dirección IP del servidor FTP.
3. Número de conexiones TCP que se han establecido.
4. Puerto origen y destino de cada conexión TCP.
5. Número de ficheros enviados (de cliente a servidor).
6. Número de ficheros recibidos (de servidor a cliente).

Problema 17

Se abre una sesión FTP en modo debug, lo cual permite visualizar los comandos y respuestas intercambiados, y se visualiza lo siguiente:

```

ftp -d 163.117.144.130 (ftp activando el modo debug)
220 lm001.lab.it.uc3m.es FTP server
---> USER labro
331
---> PASS XXXX
530
---> USER labro
331
---> PASS XXXX

```

```

230
---> CWD rcs
550
---> CWD rsc
250
---> MKD rsc-hijo
257
---> TYPE XXX
200
---> PORT 163,117,139,120,7,94
200
---> RETR ejemplo.txt
150
226 Transfer complete. 134 bytes received in 0.0015 seconds (85
Kbytes/s)
---> TYPE XXX
200
---> PORT 163,117,139,120,7,97
200
---> RETR ejemplo.txt
150
226 Transfer complete. 156 bytes received in 0.0017 seconds (88
Kbytes/s)
---> PORT 163,117,139,120,7,99
200
---> STOR ejemplo1.txt
150
226
---> PORT 163,117,139,120,7,52
200
---> LIST ejemplo1.txt
150
-rw-r--r--  1 labro  ptb           20 May 29 15:21 ejemplo1.txt ***
226
---> PORT 163,117,139,120,7,54
200
---> LIST ejemplo2.txt
150
226
---> QUIT
221

```

Teniendo en cuenta el intercambio anterior, averigüe los datos pedidos a continuación y en aquellos casos en los que el enunciado no aporte la información suficiente para poder contestar, simplemente indique “información insuficiente”:

1. Comandos ha tecleado el usuario?.
2. La primera vez que se transfirió el fichero ejemplo.txt, ¿se hizo en modo ascii o imagen?
3. ¿Cuántos octetos tiene el fichero ejemplo.txt? y ¿cuántas líneas?
4. Número de conexiones FTP que se han establecido.
5. Puerto origen y destino de cada conexión
6. Comente la visualización de la línea marcada con ***, entre las respuestas con códigos 150 y 226, e identifique la conexión por la que se han recibido.
7. Número de ficheros distintos enviados (de cliente a servidor)
8. Número de ficheros distintos recibidos (de servidor a cliente)

Problema 18

En un aula informática de la universidad, un alumno está conectado al ordenador puesto1.lab.uc3m.es con el login “jose”. Realiza las siguientes acciones:

- Ejecuta el comando de UNIX “rlogin -l pepe puesto2.lab.uc3m.es”. Esto hace un RLOGIN como usuario “pepe” a la máquina puesto2.
- Cuando se ha conectado a puesto2, ejecuta “ftp puesto3.lab.uc3m.es”, que hace que puesto2 se conecte por FTP a la máquina puesto3.
- Cuando el servidor FTP de puesto3 solicita un nombre de usuario, el alumno introduce “jose” y como clave “mipassword”.
- Una vez conectado con éxito por FTP, descarga el fichero “importante.txt”.
- Cierra el FTP.
- Cierra el RLOGIN.

Suponiendo que los tres ordenadores no conocen previamente la dirección IP de los otros, pero sí la del servidor DNS, diga qué paquetes se han enviado y recibido por la red en este proceso, detallando dirección origen y destino, TCP o UDP, números de puerto y todo lo que pueda de su contenido. Puede ignorar los paquetes de establecimiento y cierre de conexión TCP, así como los asentimientos de TCP.

Problema 19

Dada la sesión FTP que aparece a continuación:

1. Determine el valor de los siguientes parámetros (es posible que no tenga datos suficientes para determinar alguno de ellos; si es así, indíquelo).
 - Dirección IP del cliente FTP.
 - Dirección IP del servidor FTP.
 - Puerto origen y destino de cada una de las conexiones TCP que se han abierto.
 - Número de líneas del fichero `examen`.
2. Sabiendo que cada vez que se demanda interacción del usuario (introducir login, password, etc), éste tarda $T_{usuario}$ segundos en responder, que el retardo de propagación entre el cliente y servidor FTP es de T_{prop} segundos y que la velocidad de transmisión de la red es suficientemente rápida como para poderse despreciar el tiempo de transmisión de los paquetes, estime cuánto tiempo habrá tardado en realizarse esta sesión (desde la primera línea hasta la última).

```
~>ftp -d ftp
Connected to ftp.it.uc3m.es.
220 ftp.it.uc3m.es FTP server (Version wu-2.6.2(1) Wed Mar 3 22:51:51 UTC 2004) ready.
Name (ftp:rroo): rroo
--> USER rroo
331 Password required for rroo.
Password:
--> PASS XXXX
230 User rroo logged in.
ftp> ls examen
--> PORT 163,117,139,250,172,52
200 PORT command successful.
--> LIST examen
150 Opening ASCII mode data connection for /bin/ls.
-rw-r--r--  1 rroo   prof          57 Sep 18 09:43 examen
226 Transfer complete.
ftp> passive
```

```

Passive mode on.
ftp> get examen
----> TYPE I
200 Type set to I.
----> PASV
227 Entering Passive Mode (163,117,139,105,235,68)
----> RETR examen
150 Opening BINARY mode data connection for examen (57 bytes).
226 Transfer complete.
57 bytes received in 0.00 secs (47.6 kB/s)
ftp> bye
----> QUIT
221-You have transferred 57 bytes in 1 files.
221-Total traffic for this session was 681 bytes in 2 transfers.
221-Thank you for using the FTP service on ftp.it.uc3m.es.
221 Goodbye.

```

Problema 20

Un alumno se conecta desde el PC de su casa, con dirección IP 10.20.30.40, al servidor ftp de la universidad, con dirección IP 163.117.136.249 y hace lo siguiente:

- Se autentica.
- Hace un listado para ver todos los ficheros que tiene en su cuenta.
- Se descarga del servidor el fichero practica.c.
- Se despide y cierra el ftp.

Teniendo en cuenta que el alumno tiene configurado su cliente FTP para funcionar en modo pasivo, ya que si no tendría problemas con el firewall de su ISP, se pide:

1. Detalle al máximo posible todos los paquetes ha enviado y recibido el PC del alumno en este proceso: dirección origen y destino, TCP o UDP, números de puerto y detalle todo lo que pueda su contenido. En concreto, dé todo el detalle posible sobre los comandos y respuestas FTP.

Suponga ahora que se conecta a un servidor TFTP con dirección 163.117.136.249 y se descarga el fichero practica2.c de 2048 bytes.

3. Detalle al máximo posible todos los paquetes ha enviado y recibido el PC del alumno en este proceso: dirección origen y destino, TCP ó UDP, números de puerto y detalle todo lo que pueda su contenido.

Problema 21

Se envía un mensaje de correo MIME, que contiene:

- Una página HTML de 8 KBytes, con tres imágenes, dos GIF y un JPEG de 10, 30 y 25 KBytes respectivamente. En la página HTML no hay ningún carácter de la mitad alta de la tabla ASCII.
- Una versión alternativa en texto de la misma página HTML, para lectores de correo que no soporten HTML. Este texto está en castellano, tiene una longitud de 5 KBytes y un 10 % de caracteres que no son us-ascii (ñ, Á, á, ÿ, vocales acentuadas, etc.)
- Un fichero asociado (“attachment”), que deben recibir tanto los lectores que soporten HTML como los que no, que consiste en un fichero comprimido con “zip”, de 200 Kbytes.

Se pide:

1. Indique el valor de las principales cabeceras RFC 822 y MIME
2. Calcule qué tamaño tendría aproximadamente el mensaje, suponiendo que las cabeceras ocupan 500 bytes en total.

Problema 22

Enviamos un correo electrónico a un amigo, con copia a otro amigo, con un texto y una fotografía JPG. El destinatario del correo lee el mensaje con un UA IMAP.

A continuación mostramos el tráfico capturado correspondiente a las sesiones SMTP e IMAP, con las líneas numeradas para poderlas referenciar fácilmente. Además, en estas capturas, C: indica un comando enviado por el cliente, y S: una respuesta del servidor. Tenga en cuenta que en estas capturas intencionadamente se ha introducido erratas.

Se le pide que identifique qué erratas hay en estas capturas de tráfico, indicando número de línea y cómo sería de forma correcta.

Tráfico capturado en el envío SMTP:

```
1 C: HELO it003.lab.it.uc3m.es
2 S: 250 alumnos.uc3m.es
3 C: MAIL FROM:<yo@lab.it.uc3m.es>
4 S: 250 OK
5 C: RCPT TO:<amigo.mio@alumnos.uc3m.es>
6 S: 250 OK
7 C: RCPT CC:<otro.amigo@alumnos.uc3m.es>
8 S: 250 OK
9 C: DATA
10 S: 354 Start mail input
11 C: Date: 8 Sep 06 16:05:23
12 C: From: Examen < yo@lab.it.uc3m.es >
13 C: Subject: =?ISO-8859-1?Q? =B7qu=E9 foto!?=
14 C: To: <amigo.mio@alumnos.uc3m.es>
15 C: Cc: <otro.amigo@alumnos.uc3m.es>
16 C: Content-Type: multipart/mixed;
17 C:     boundary=unique-boundary-1
18 C:
19 C: --unique-boundary-1
20 C: Content-Type: text/plain; charset=ISO-8859-1
21 C: Content-Transfer-Encoding: quoted-printable
22 C:
23 C: Mira qu=E9 foto de mis vacaciones.
24 C:
25 C:   Yo
26 C:
27 C: --unique-boundary-2
28 C: Content-Type: image/jpeg
29 C: Content-Transfer-Encoding: base64
30 C:
31 C: (varias líneas aquí con la fotografía)
32 C:
33 C: .
34 S: 250 OK
35 C: QUIT
36 S: 221 alumnos.uc3m.es
```

Tráfico capturado de la lectura IMAP:

```
37 S: * OK IMAP4rev1 Service Ready
38 C: a001 USER amigo.mio stel
39 S: * 18 EXISTS
40 S: * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
41 S: * 2 RECENT
42 S: * OK [UNSEEN 17]
43 S: * OK [UIDVALIDITY 3857529045] UIDs valid
44 S: a001 OK USER completed
45 C: a002 RETR 17 body[text]
46 S: * 12 RETR (BODY[TEXT] {342}
47 S: (aquí el texto del mensaje)
48 S:
49 S: )
50 S: a003 OK RETR completed
51 C: a004 QUIT
52 S: * BYE IMAP4rev1 server terminating connection
53 S: a004 OK QUIT completed
```

Problema 23

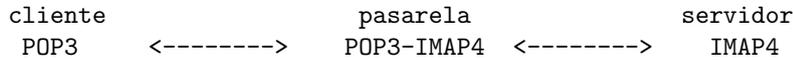
1. Escriba las principales cabeceras que tendría un correo electrónico MIME compuesto por un texto en inglés de 1 Kbytes, una fotografía JPG de 45 KBytes y un vídeo MPEG de 500 KBytes, codificado de manera que el lector de correo muestre siempre el texto y, dependiendo de su capacidad, la fotografía o el vídeo.
2. ¿Cuánto ocuparía aproximadamente el correo electrónico?
3. Se envía el correo con el protocolo SMTP. La captura de tráfico se muestra a continuación (S representa lo que manda el servidor, C lo que manda el cliente):

```
S: 220
C: HELO stockholm.ibm.com
S: 250
C: MAIL FROM:<abc@stockholm.ibm.com>
S: 250
C: RCPT TO:<xyz@delta.aus.edu>
S: 250
C: RCPT TO:<opq@delta.aus.edu>
S: 550
C: RCPT TO:<rst@delta.aus.edu>
S: 250
C: DATA
C: 354 Start mail input, end with <CRLF>.<CRLF>
C: Date: 23 Jan 89 18:05:23
C: From: Alex B. Carver <abc@stockholm.ibm.com>
C: Subject: Important meeting
C: To: <def@delta.aus.edu>
C: To: <opq@delta.aus.edu>
C: cc: <rst@delta.aus.edu>
C:
C: Blah blah blah
C: etc.....
C: .
S: 250 OK
C: QUIT
S: 221 delta.aus.edu Service closing transmission channel
```

¿Quién recibe realmente el mensaje?

Problema 24

Se tiene una pasarela POP3-IMAP4 que permite leer el correo almacenado en un servidor IMAP4 usando un cliente de correo POP3. La pasarela no es más que un programa que actúa como un servidor POP3 para un cliente de correo POP3 y como un cliente IMAP4 para un servidor de correo IMAP4.



Más concretamente el funcionamiento es como sigue:

1. El cliente de correo POP3 se conecta a la pasarela como si ésta fuera un servidor POP3.
2. El cliente POP3 no manda como nombre de usuario POP3 directamente el de la cuenta IMAP, sino que debe usar uno construido del siguiente modo:
`CuentaIMAP@nombre.srv.imap%NombreBuzónIMAP`
3. Si el nombre de usuario POP3 está construido de esta manera, la pasarela le dará una respuesta POP3 positiva.
4. A continuación el cliente POP3 mandará la contraseña, que será la misma que tenga el usuario CuentaIMAP en el servidor IMAP.
5. La pasarela se conectará entonces al servidor IMAP nombre.srv.imap (necesitará previamente hacer una consulta DNS para resolver la dirección IP) y seleccionará el buzón indicado (NombreBuzónIMAP).
6. La pasarela mandará una respuesta POP3 al cliente de correo indicando si la operación se ha hecho con éxito o no.
7. A partir de este momento, la pasarela recibirá comandos POP3 del cliente de correo, mandará el/los comandos IMAP4 que estime oportunos al servidor IMAP, recibirá la/s respuesta/s del servidor IMAP y construirá la respuesta POP3 que corresponda.

Se pide:

1. Indique los paquetes que envía y recibe la pasarela en los pasos 1 al 6, detallando de cada uno de ellos su dirección IP origen, IP destino, protocolo de transporte (TCP o UDP), puertos origen y destino, flags relevantes y datos que contendría. Puede ignorar los paquetes que simplemente contengan asentimientos de TCP. Suponga que no hay ningún error (el usuario y el buzón existen y el password es correcto).
2. Suponga que el usuario del cliente de correo POP3 lee el mensaje 3, lo borra y sale de la aplicación. ¿Qué comandos y respuestas POP3 se intercambiaría con la pasarela para hacer estas acciones? (suponga que el mensaje existía, no hay por tanto ningún error).
3. ¿Qué comandos IMAP mandaría la pasarela al servidor IMAP para poder generar las respuestas POP3 del apartado b?
4. ¿Podría el cliente POP3 manipular (leer mensajes, borrar mensajes) de buzones distintos del buzón por defecto?
5. Cite algunas funcionalidades IMAP que no pueden hacerse accesibles al cliente POP a través de la pasarela. Diga por qué.

Problema 25

Un alumno de la universidad Carlos III de Madrid, con dirección de correo `alumno@uc3m.es` quiere enviar un correo a un amigo suyo que trabaja en google, siendo su dirección de correo `amigo@google.com`. Nuestro alumno redacta el correo desde un UA instalado en su máquina `pc.uc3m.es`, este UA tiene preconfigurado como servidor SMTP la máquina `smtp.uc3m.es`. El servidor DNS por defecto es `vorteX.uc3m.es`.

Mostramos a continuación el contenido de algunos de los paquetes (no todos) que viajan por la red. Utilizamos para representar los mensajes DNS un formato similar a la salida del programa `dig`.

Un mensaje de respuesta DNS:

```
; <<>> DiG 8.3 <<>>
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 4
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 4
;; QUERY SECTION:
;;      XXXX, type = XXXX, class = IN

;; ANSWER SECTION:
XXXX      23h21m52s IN XXXX  163.117.136.121
XXXX      23h21m52s IN XXXX  163.117.136.122
XXXX      23h21m52s IN XXXX  163.117.136.123

;; AUTHORITY SECTION:
[...]

;; ADDITIONAL SECTION:
[...]
```

Varios paquetes intercambiados entre `pc.uc3m.es` (C) y la máquina con dirección IP `163.117.136.121` (S), con el siguiente contenido:

```
S: 220 ...
C: HELO XXXX
S: 250 ...
C: MAIL FROM: XXXX
S: 250 OK
C: RCPT TO: XXXX
S: 250 OK
C: DATA
S: 354 Start mail input, end with <CRLF>.<CRLF>
C: Date: 23 Jun 2005 18:05:23
C: From: Alumno <alumno@uc3m.es>
C: Subject: Examen
C: To: <amigo@google.com>
C:
C: Blah blah blah
C: etc.....
C: .
S: 250 OK
C: QUIT
S: 221 ...
```

Otro mensaje de respuesta DNS con el siguiente contenido:

```
; <<>> DiG 8.3 <<>>
;; res options: init recurs defnam dnsrch
;; got answer:
```

```

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 4, ADDITIONAL: 8
;; QUERY SECTION:
;;      XXXX, type = XXXX, class = IN

;; ANSWER SECTION:
google.com.      1H IN MX      XXXX smtp1.google.com.
google.com.      1H IN MX      2 smtp2.google.com.

;; AUTHORITY SECTION:
google.com.      3d4h13m5s IN NS  ns1.google.com.

;; ADDITIONAL SECTION:
smtp1.google.com. 10M IN A      216.239.57.25
smtp2.google.com. 10M IN A      64.233.167.25
ns1.google.com.  23h19m16s IN A 216.239.32.10

```

Y varios paquetes intercambiados entre smtp.uc3m.es (C) y la máquina con dirección IP 216.239.57.25 (S), con el siguiente contenido:

```

S: 220 ...
C: HELO XXXX
S: 250 ...
C: MAIL FROM: XXXX
S: 250 OK
C: RCPT TO: XXXX
S: 250 OK
C: DATA
S: 354 Start mail input, end with <CRLF>.<CRLF>
C: Date: 23 Jun 2005 18:05:23
C: From: Alumno <alumno@uc3m.es>
C: Subject: Examen
C: To: <amigo@google.com>
C: XXXXX: XXXXXXXXXXXXX
C:
C: Blah blah blah
C: etc.....
C: .
S: 250 OK
C: QUIT
S: 221 ...

```

1. Diga la máquina origen y destino, protocolo de transporte, puertos y el valor de los campos ocultos con XXXX de los diferentes paquetes.

Problema 26

Un alumno con dirección de correo alumno@gmail.com envía un correo electrónico en formato MIME al profesor de la asignatura RROOII profesor@uc3m.es. El mensaje está formado por un texto en castellano de 1280 bytes y un fichero adjunto (attachment) en formato postscript de tamaño 5 Kbytes.

El alumno utiliza como servidor de correo saliente smtp.gmail.com y el profesor utiliza como servidor de correo entrante la máquina pop3.uc3m.es.

1. Indique el valor de las principales cabeceras RFC822 y MIME que tendrá el mensaje de correo recibido por el profesor. Considerando que el tamaño total de las cabeceras son 1024 bytes y que el texto en castellano tiene un 10% de caracteres que no son NVT ASCII. ¿Cuál es tamaño que tendría este mensaje?

El profesor se conecta desde su máquina de trabajo `pc.uc3m.es` a su servidor de correo `pop3.uc3m.es` para leer su correo. Ambas máquinas están conectadas a un red FastEthernet (100Mbit/s) y el tiempo de propagación entre ellas es de 10 ms. El MSS empleado en la conexión TCP será de 2048 bytes y la ventana anunciada por ambos extremos es de 10240 bytes. Considere que cuando se descarga un mensaje de correo, el servidor POP3 envía en el mismo segmento TCP la respuesta al comando y los datos que quepan del mensaje. Suponga que en la conexión TCP no se usan ACKs retardados.

2. Indique los paquetes que se intercambian las máquinas `pc.uc3m.es` y `pop3.uc3m.es` para que el profesor pueda leer el correo que le ha enviado el alumno. Por cada paquete detalle, dirección IP origen y destino, puerto origen y destino, protocolo de transporte, flags y datos contenidos.
3. ¿Cuál es el tiempo transcurrido desde que se establece la conexión hasta que se recibe el último segmento de datos?

Suponga que se hubiera producido un problema esporádico en la red, que provocase que se perdiera el segundo segmento que contiene datos del mensaje de correo.

4. Indique los paquetes que se intercambiarían las máquinas `pc.uc3m.es` y `pop3.uc3m.es` en este caso, e indique como evoluciona la ventana de congestión y la ventana efectiva (no es necesario que calcule el RTO, considere que es suficientemente mayor que RTT).

Problema 27

Juan envía a dos amigos, Andrés y Óscar, el siguiente correo electrónico (mostramos las líneas numeradas para podernos referir a ellas en las preguntas).

```

001 Date: Wed, 25 Jan 2006 19:08:01 +0100
002 From: Juan Perez <estudiante@gmail.com>
003 To: Andres Miranzo Gomez <amigo@uc3m.es>
004 Cc: Oscar Turegano Rodriguez <otro@uc3m.es>
005 Subject: =?ISO-8859-1?Q?te_env=EDo_el_fichero_del_que_hablamos?=
006 Content-Type: multipart/mixed;
007
008 --_Part_1
009 Content-Type: multipart/alternative;
010
011 --_Part_2
012 Content-Type: text/plain; charset=ISO-8859-1
013 Content-Transfer-Encoding: quoted-printable
014
015 Hola:
016
017 Te env=EDo adjunto el fichero del que hablamos, =BFte acuerdas? Cuando lo l=
018 eas
019 me dices qu=E9 opinas.
020
021 Saludos,
022
023 Juan
024
025 --_Part_2
026 Content-Type: text/html
027
028 <html><body>
029 <div>Hola:</div>
030 <div>&nbsp;</div>
031 <div>Te env&iacute;o adjunto el fichero del que hablamos, &iquest;te
032 acuerdas?&nbsp;<div>&nbsp;</div>
033 <div>&nbsp;</div>
034 <div>Saludos,</div>
035 <div>&nbsp;</div>
036 <div>&nbsp;<div>&nbsp;</div> Juan</div>
037 </body></html>
038

```

```

039  --_Part_1
040  Content-Type: application/pdf; name=importante.pdf
041  Content-Transfer-Encoding: base64
042
043  [aquí van 220 líneas de 76 caracteres cada una (terminadas con un \r\n al final)
    más la siguiente línea final]
263  aXplZpj4=

```

La siguiente traza de tráfico se capturó en la máquina desde la que Juan envió el correo electrónico a sus amigos. Las líneas marcadas con C: corresponden a comandos enviados por su agente de usuario (UA), y las marcadas con S: a respuestas del servidor. Mostramos las líneas numeradas para podernos referir a ellas en las preguntas, y con cierta información oculta con XXXXXXXXXXXX.

```

001  S: 220 XXXXXXXXXXXX
002  C: EHLO XXXXXXXXXXXX
003  S: 500 Command unrecognized
004  C: RSET
005  S: 250 Reset state
006  C: HELO XXXXXXXXXXXX
007  S: 250
008  C: XXXXXXXXXXXX
009  S: 250 OK
010  C: XXXXXXXXXXXX
011  S: 250 OK
012  C: XXXXXXXXXXXX
013  S: 250 OK
014  C: DATA
015  S: 354 Start mail input, end with <CRLF>.<CRLF>
016  C: Date: Wed, 25 Jan 2006 19:08:01 +0100
    From: Juan Perez <estudiante@gmail.com>
    [... resto del mail aquí ...]
    .
017  S: 250 OK
018  C: QUIT
019  S: 221 Service closing transmission channel

```

Uno de los amigos, Andrés, lee el correo con un UA que usa el protocolo IMAP para acceder al buzón de correo. Capturamos el tráfico de la sesión IMAP y obtenemos la siguiente traza de comandos que envía el cliente (líneas marcadas con C:) y respuestas del servidor (líneas marcadas con S:):

```

C: A00000 LOGIN amigo gominola
S: * OK shem.uc3m.es IMAP4rev1 v12.264 server ready
A00000 OK LOGIN completed
C: A00001 LIST "" *
S: * LIST (\NoInferiors) "/" INBOX
    * LIST (\NoSelect) "/" mail
    * LIST (\NoInferiors \UnMarked) "/" mail/saved-messages
    * LIST (\NoInferiors \UnMarked) "/" mail/sent-mail
A00001 OK LIST completed
C: A00002 SELECT INBOX
S: * 37 EXISTS
    * 6 RECENT
    * OK [UNSEEN 32]
    * OK [UIDVALIDITY 1066827933] UID validity status
    * OK [UIDNEXT 15489] Predicted next UID
    * FLAGS ($MDNSent \Answered \Flagged \Deleted \Draft \Seen)
    * OK [PERMANENTFLAGS ($MDNSent \* \Answered \Flagged \Deleted \Draft \Seen)] Permanent flags
A00002 OK [READ-WRITE] SELECT completed
C: A00003 SEARCH FROM "Juan"
S: * SEARCH 34
A00003 OK SEARCH completed
C: A00004 FETCH 34 FLAGS
S: * 34 FETCH (FLAGS (\Recent))
A00004 OK FETCH completed
C: A00005 FETCH 34 RFC822.HEADER
S: * 34 FETCH (RFC822.HEADER {1778}
    Received: from smtp02.uc3m.es (smtp02.uc3m.es [163.117.136.122])
        by shem.uc3m.es (Postfix) with ESMTP id B3C20E8B4
        for <amigo@uc3m.es>; Wed, 25 Jan 2006 19:08:09 +0100 (CET)

```

```

Received: from wproxy.gmail.com (wproxy.gmail.com [64.233.184.193])
        by smtp02.uc3m.es (Postfix) with ESMTP id 77CB484FFF
        for <amigo@uc3m.es>; Wed, 25 Jan 2006 19:08:06 +0100 (CET)
Received: from 10.65.20.1 by wproxy.gmail.com with SMTP id i5so215244wra
        for <amigo@uc3m.es>; Wed, 25 Jan 2006 10:08:05 -0800 (PST)
Received: from 10.65.193.9 by 10.65.20.1 with SMTP id x1mr419567qbi;
        Wed, 25 Jan 2006 10:08:01 -0800 (PST)
Message-ID: <ab08ddbd0601251008o32da8dbs5804f67bda0613c1@mail.gmail.com>
Date: Wed, 25 Jan 2006 19:08:01 +0100
From: Juan Perez <estudiante@gmail.com>
To: Andres Miranzo Gomez <amigo@uc3m.es>
Cc: Oscar Turegano Rodriguez <otro@uc3m.es>
Subject: =?ISO-8859-1?Q?te_env=EDo_el_fichero_del_que_hablamos?=
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="_Part_1"

```

```

)
A00005 OK FETCH completed
C: A00006 FETCH 34 FULL
S: * 34 FETCH ... (no mostramos los detalles de esta respuesta)
[... ]
A00006 OK FETCH completed
C: A00007 STORE 34 +FLAGS (\Deleted)
S: * 34 FETCH (FLAGS (\Seen \Deleted))
A00007 OK STORE completed
C: A00008 LOGOUT
S: * BYE shem.uc3m.es IMAP4rev1 server terminating connection
A00008 OK LOGOUT completed

```

A la vista del mensaje de correo y de las dos trazas de tráfico capturado, responda a las siguientes preguntas:

1. Revise el mensaje de correo electrónico y diga qué cosas le falta para ser un mensaje de correo bien formado según las especificaciones de Internet, indicando número de línea y elemento que falta.
2. En la herramienta de captura de tráfico que hemos utilizado para obtener las dos trazas (por ejemplo, ethereal o tcpdump), ¿qué protocolo de transporte y qué número de puerto habremos tenido que indicar en cada una para capturar únicamente el tráfico de los protocolos que se muestran?
3. Diga a la vista de la trazas, por qué UAs y MTAs ha pasado el mensaje desde que lo envió Juan hasta que lo leyó Andrés, y qué protocolo se ha usado en cada salto.
4. Diga lo que iría en las zonas marcadas con XXXXXXXXXXXX en las líneas 1, 2, 6, 8, 10 y 12 de la primera traza.
5. Diga exáctamente cuál es el tamaño en bytes del fichero **importante.pdf** original (sin codificar) que está enviando como adjunto Juan.
6. Suponga que unos minutos después, Andrés vuelve a conectarse para comprobar si tiene correo nuevo en su buzón, pero no le ha llegado nada nuevo desde la conexión anterior. Detalle qué respuesta obtendrá su UA en esta nueva sesión IMAP cuando envíe el comando **B00002 SELECT INBOX**.

Problema 28

A continuación se presenta una versión ligeramente modificada de una traza, capturada mediante la herramienta Ethereal, que muestra los datos intercambiados en la interfaz del cliente como resultado del envío de un breve correo electrónico. Las líneas marcadas con C: se corresponden con los comandos enviados por el Agente de Usuario (AU) y las líneas marcadas con S: con las respuestas del servidor de correo.

Responda ahora a las preguntas que aparecen tras la traza. Note que algunas cadenas de caracteres de la traza han sido reemplazadas por las cadenas de caracteres WWW, XXX, YYY y ZZZ (el número de caracteres de reemplazo utilizado no es significativo)

```

S: 220 Lmserv.lab.it.uc3m.es ESMTP Sendmail 8.13.4/8.13.4/Debian-3sarge1;
Wed, 2 Aug 2006 15:57:27 +0200;
(No UCE/UBE) logging access from: lm002.lab.it.uc3m.es(OK)-root@lm002.lab.it.uc3m.es [163.117.144.131]
C: EHLO lm002.lab.it.uc3m.es
S: 250-Lmserv.lab.it.uc3m.es Hello root@lm002.lab.it.uc3m.es [163.117.144.131], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-EXPN
250-VERB
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH DIGEST-MD5 CRAM-MD5
250-DELIVERY
250 HELP
C: WWW:<guest2@smtp.lab.it.uc3m.es> SIZE=655
S: 250 2.1.0 <guest2@smtp.lab.it.uc3m.es>... Sender ok
C: XXX:<NoughtAboutOught@hotmail.com>
S: 250 2.1.5 <NoughtAboutOught@hotmail.com>... Recipient ok
C: YYY
S: 354 Enter mail, end with "." on a line by itself
C: Received: from lm002.lab.it.uc3m.es (guest2@localhost [127.0.0.1])
.by lm002.lab.it.uc3m.es (8.13.4/8.13.4/Debian-3) with ESMTP id k72DvRhP007390
.for <NoughtAboutOught@hotmail.com>; Wed, 2 Aug 2006 15:57:27 +0200
Received: (from guest2@localhost)
.by lm002.lab.it.uc3m.es (8.13.4/8.13.4/Submit) id k72DvRCU007389
.for NoughtAboutOught@hotmail.com; Wed, 2 Aug 2006 15:57:27 +0200
Date: Wed, 2 Aug 2006 15:57:27 +0200
From: GUEST <guest2@smtp.lab.it.uc3m.es>
Message-Id: <200608021357.k72DvRCU007389@lm002.lab.it.uc3m.es>
To: NoughtAboutOught@hotmail.com
Subject: what's up doc?

```

Dear Doc,

What, indeed, is up?

Yours

freddy the frog

```

.
S: 250 2.0.0 k72DvRGj005307 Message accepted for delivery
C: ZZZ
S: 221 2.0.0 Lmserv.lab.it.uc3m.es closing connection

```

1. ¿Cuáles son los comandos SMTP que han sido reemplazados por WWW, XXX, YYY y ZZZ?
2. Detalle el intercambio de mensajes que tendría lugar si el servidor de correo no comprendiera el comando EHLO, explicando su respuesta.
3. ¿Cuál es el significado de la respuesta multi-línea al comando EHLO?

Considere ahora una versión ligeramente modificada de la traza subyacente de los segmentos TCP intercambiados y responda a las respuestas que aparecen tras ella. Los números de mensaje aparecen en la columna situada más a la izquierda. El tiempo es el transcurrido desde el comienzo de la captura. Los números de secuencia TCP proporcionados son números de secuencia relativos. El campo **Len** de la columna **Info** de un mensaje TCP indica la longitud de datos en octetos.

| No. | Time | Source | Destination | Protocol | Info |
|-----|----------|-----------------|-----------------|----------|---|
| 1 | 0.000000 | 163.117.144.131 | 163.117.144.129 | TCP | 49874 > smtp [SYN] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460 |
| 2 | 0.000141 | 163.117.144.129 | 163.117.144.131 | TCP | smtp > 49874 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 |
| 3 | 0.000225 | 163.117.144.131 | 163.117.144.129 | TCP | 49874 > smtp [ACK] Seq=1 Ack=1 Win=5840 Len=0 |
| 4 | 0.010906 | 163.117.144.129 | 163.117.144.131 | TCP | smtp > 49874 [PSH, ACK] Seq=1 Ack=1 Win=5888 Len=207 |
| 5 | 0.010949 | 163.117.144.131 | 163.117.144.129 | TCP | 49874 > smtp [ACK] Seq=1 Ack=208 Win=6912 Len=0 |
| 6 | 0.011400 | 163.117.144.131 | 163.117.144.129 | TCP | 49874 > smtp [PSH, ACK] Seq=1 Ack=208 Win=6912 Len=27 |
| 7 | 0.012604 | 163.117.144.129 | 163.117.144.131 | TCP | smtp > 49874 [ACK] Seq=208 Ack=28 Win=5888 Len=0 |
| 8 | 0.012806 | 163.117.144.129 | 163.117.144.131 | TCP | smtp > 49874 [PSH, ACK] Seq=208 Ack=28 Win=5888 Len=257 |
| 9 | 0.013211 | 163.117.144.131 | 163.117.144.129 | TCP | 49874 > smtp [PSH, ACK] Seq=28 Ack=465 Win=7984 Len=49 |
| 10 | 0.024017 | 163.117.144.129 | 163.117.144.131 | TCP | smtp > 49874 [PSH, ACK] Seq=465 Ack=77 Win=5888 Len=53 |
| 11 | 0.024385 | 163.117.144.131 | 163.117.144.129 | TCP | 49874 > smtp [PSH, ACK] Seq=77 Ack=518 Win=7984 Len=46 |
| 12 | 0.030744 | 163.117.144.129 | 163.117.144.131 | TCP | smtp > 49874 [PSH, ACK] Seq=518 Ack=123 Win=5888 Len=108 |
| 13 | 0.031951 | 163.117.144.131 | 163.117.144.129 | TCP | 49874 > smtp [PSH, ACK] Seq=123 Ack=626 Win=7984 Len=664 |
| 14 | 0.070012 | 163.117.144.129 | 163.117.144.131 | TCP | smtp > 49874 [ACK] Seq=626 Ack=787 Win=7168 Len=0 |
| 15 | 0.070096 | 163.117.144.131 | 163.117.144.129 | TCP | 49874 > smtp [PSH, ACK] Seq=787 Ack=626 Win=7984 Len=3 |
| 16 | 0.071303 | 163.117.144.129 | 163.117.144.131 | TCP | smtp > 49874 [ACK] Seq=626 Ack=790 Win=7168 Len=0 |
| 17 | 0.104420 | 163.117.144.129 | 163.117.144.131 | TCP | smtp > 49874 [PSH, ACK] Seq=626 Ack=790 Win=7168 Len=56 |
| 18 | 0.142667 | 163.117.144.131 | 163.117.144.129 | TCP | 49874 > smtp [ACK] Seq=790 Ack=682 Win=7984 Len=0 |

```

19 0.163947 163.117.144.131 163.117.144.129 TCP 49874 > smtp [PSH, ACK] Seq=790 Ack=682 Win=7984 Len=6
20 0.165256 163.117.144.129 163.117.144.131 TCP smtp > 49874 [PSH, ACK] Seq=682 Ack=796 Win=7168 Len=52
21 0.165346 163.117.144.129 163.117.144.131 TCP smtp > 49874 [FIN, ACK] Seq=734 Ack=796 Win=7168 Len=0
22 0.165525 163.117.144.131 163.117.144.129 TCP 49874 > smtp [FIN, ACK] Seq=796 Ack=735 Win=7984 Len=0
23 0.165661 163.117.144.129 163.117.144.131 TCP smtp > 49874 [ACK] Seq=735 Ack=797 Win=7168 Len=0

```

1. ¿Cuál es el número del puerto destino del mensaje 1 (representado como smtp)?
2. ¿Cuál es el número del mensaje que contiene el segmento TCP que a su vez contiene al comando EHLO? Justifique su respuesta.
3. ¿Puede SMTP utilizar UDP como protocolo de transporte en lugar de TCP?

A continuación se presenta una versión ligeramente modificada de una traza, capturada mediante la herramienta Ethereal, que muestra los datos intercambiados a través de la interfaz del cliente cuando un usuario guest2 consulta su Inbox con una típica herramienta de correo que utiliza el protocolo POP3 configurada con opciones tales que se mantengan copias de los correos en el servidor. Las líneas marcadas con C: se corresponden con los comandos enviados por el cliente y las líneas marcadas con S: con las respuestas del servidor de correo.

Responda ahora a las preguntas que aparecen tras la traza. Note que algunas cadenas de caracteres de la traza han sido reemplazadas por ***, AAA, VVV, WWW, XXX, YYY y ZZZ (el número de caracteres de reemplazo usado no es significativo).

```

S: +OK Cubic Circle's v1.31 1998/05/13 POP3 ready <0667000072bbfe44@monitor01>;
C: CAPA
S: AAA Invalid command, try one of: USER name, PASS string, APOP name digest, QUIT
C: USER guest2
S: +OK guest2 selected
C: PASS ***
S: +OK Congratulations!
C: VVV
S: +OK 5 8501
C: WWW
S: +OK 5 messages (8501 octets)
1 2201
2 1592
3 2049
4 1350
5 1309
.
C: UIDL
S: +OK But remember to DELETE messages REGULARLY
1 65e23c4a8a080000
2 b762df9d29060000
3 6214c904f2070000
4 85ed0cb737050000
5 1ff6f7e70e050000
.
C: XXX 3
S: +OK 2049 octets
aquí el contenido del mensaje 3 terminado con <CR><LF>.<CR><LF>
C: XXX 4
+OK 1350 octets
aquí el contenido del mensaje 4 terminado con <CR><LF>.<CR><LF>
C: XXX 5
+OK 1309 octets
aquí el contenido del mensaje 5 terminado con <CR><LF>.<CR><LF>
C: ZZZ
S: +OK Was it as good for you, as it was for me?

```

El usuario borra entonces un mensaje y cierto tiempo después averigua de nuevo si ha llegado nuevos mensajes a su Inbox exactamente del mismo modo que cuando se capturó la traza anterior; se captura entonces la siguiente traza:

```

S: +OK Cubic Circle's v1.31 1998/05/13 POP3 ready <0a6700008fbbfe44@monitor01>
C: CAPA
S: AAA Invalid command, try one of: USER name, PASS string, APOP name digest, QUIT
C: USER guest2
S: +OK guest2 selected
C: PASS ***
S: +OK Congratulations!
C: VVV
S: +OK 5 8501

```

```

C: WWW
S: +OK 5 messages (8501 octets)
  1 2201
  2 1592
  3 2049
  4 1350
  5 1309
.
C: UIDL
S: +OK But remember to DELETE messages REGULARLY
  1 65e23c4a8a080000
  2 b762df9d29060000
  3 6214c904f2070000
  4 85ed0cb737050000
  5 1ff6f7e70e050000
.
C: YYY 4
S: +OK Message 4 deleted
C: ZZZ
S: +OK Was it as good for you, as it was for me?

```

1. ¿Cuál es el valor de la cadena de caracteres de la respuesta reemplazada por AAA y el del comando reemplazado por ZZZ?
2. ¿Cuál es el valor de los comandos reemplazados por VVV, WWW, XXX y YYY?
3. ¿Qué hace el comando UIDL y por qué interesa utilizarlo?
4. ¿La contraseña de guest2 (reemplazada aquí por ***) se ha enviado encriptada?
5. La primera vez que guest2 consultó su Inbox, ¿utilizó flags de mensaje el Agente de Usuario para saber que los mensajes 3, 4 y 5 son nuevos y necesitan descargarse mientras que los mensajes 1 y 2 no lo son (y la segunda vez para saber que no hay nuevos mensajes)?
6. Asumiendo que guest2 no realiza ninguna operación más con los mensajes de su Inbox y que no llegan nuevos mensjes, proporcione en detalle los comandos y respuestas que se capturarían cuando guest2 comprobase de nuevo su Inbox.

Problema 29

1. Un fichero codificado en base 64 tiene un tamaño de 1665 bytes. ¿Cuál es el tamaño del fichero sin codificar?
2. Escriba las cabeceras MIME que tendría un mensaje de correo electrónico en el que se enviase un texto en castellano sin formateo (plano) y en HTML (los lectores de correo sólo deberán presentar una de las dos versiones), junto con un fichero binario, codificado tanto en base64 como en quoted-printable (nuevamente el lector deberá presentar sólo una de las dos versiones).
3. En una red hay 20 ordenadores que usan un proxy para acceder al web. El proxy almacena las páginas en su caché durante 24 horas, y después las borra. Si cada ordenador visita una media de 30 páginas por hora, sólo el 20 % de estas visitas corresponde a páginas ya visitadas durante las últimas 24 horas, y cada página tiene un tamaño medio de 8 KBytes, calcule el tamaño de la caché de páginas que se necesita tener el proxy.

Problema 30

A continuación se presenta una versión ligeramente editada de una traza capturada mediante la herramienta Ethereal, donde se muestran los paquetes intercambiados a través de la interfaz del cliente, como resultado de introducir el URL www.guardian.co.uk en un navegador. Los números de mensaje aparecen en la columna situada más a la izquierda. El tiempo es el transcurrido desde el comienzo de la captura. Los números de secuencia TCP proporcionados son números de secuencia relativos. El campo Len de la columna Info indica la longitud de los datos en bytes del mensaje TCP.

Responda ahora a las preguntas que aparecen después de la traza.

| No. | Time | Source | Destination | Protocol | Info |
|-----|----------|-----------------|-----------------|----------|---|
| ... | | | | | |
| 25 | 4.152514 | 163.117.144.131 | 163.117.144.129 | DNS | Standard query A www.guardian.co.uk |
| 26 | 4.181479 | 163.117.144.129 | 163.117.144.131 | DNS | Standard query response A 212.187.153.30 |
| 27 | 4.181939 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [SYN] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460 |
| 28 | 4.210621 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460 |
| 29 | 4.210725 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=1 Ack=1 Win=5840 Len=0 |
| 30 | 4.211077 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=602 |
| 31 | 4.238831 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=1 Ack=603 Win=24616 Len=0 |
| 32 | 4.251292 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=1 Ack=603 Win=24616 Len=1448 |
| 33 | 4.251331 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=1449 Win=8736 Len=0 |
| 34 | 4.251495 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [PSH, ACK] Seq=1449 Ack=603 Win=24616 Len=1448 |
| 35 | 4.251510 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=2897 Win=11632 Len=0 |
| 36 | 4.251795 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [PSH, ACK] Seq=2897 Ack=603 Win=24616 Len=1448 |
| 37 | 4.251813 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=4345 Win=14528 Len=0 |
| 38 | 4.279960 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=4345 Ack=603 Win=24616 Len=1448 |
| 39 | 4.280025 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=5793 Win=17424 Len=0 |
| 40 | 4.280128 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [PSH, ACK] Seq=5793 Ack=603 Win=24616 Len=1448 |
| 41 | 4.280143 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=7241 Win=20320 Len=0 |
| 42 | 4.280857 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=7241 Ack=603 Win=24616 Len=1448 |
| 43 | 4.280921 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=8689 Win=23216 Len=0 |
| 44 | 4.280937 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=10137 Ack=603 Win=24616 Len=91 |
| | | | | | [TCP Previous segment lost] |
| 45 | 4.280965 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=8689 Win=23216 Len=0 |
| | | | | | [TCP Dup ACK 43#1] |
| 46 | 4.281039 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [PSH, ACK] Seq=8689 Ack=603 Win=24616 Len=1448 |
| | | | | | [TCP Retransmission] |
| 47 | 4.281054 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=10228 Win=26112 Len=0 |
| ... | | | | | |
| 122 | 4.340250 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=40829 Ack=603 Win=24616 Len=1448 |
| 123 | 4.340263 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=51244 Len=0 |
| 124 | 4.340377 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [PSH, ACK] Seq=43725 Ack=603 Win=24616 Len=1448 |
| | | | | | [TCP Previous segment lost] |
| 125 | 4.340394 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=51244 Len=0 |
| | | | | | [TCP Dup ACK 123#1] |
| 126 | 4.342254 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=45173 Ack=603 Win=24616 Len=1448 |
| 127 | 4.342326 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| | | | | | [TCP Window Update] |
| 128 | 4.342436 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [PSH, ACK] Seq=46621 Ack=603 Win=24616 Len=1448 |
| 129 | 4.342451 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| | | | | | [TCP Dup ACK 123#3] |
| 130 | 4.342847 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=48069 Ack=603 Win=24616 Len=1448 |
| 131 | 4.342898 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| | | | | | [TCP Dup ACK 123#4] |
| 132 | 4.343041 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [PSH, ACK] Seq=49517 Ack=603 Win=24616 Len=1448 |
| 133 | 4.343056 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| | | | | | [TCP Dup ACK 123#5] |
| 134 | 4.343142 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [PSH, ACK] Seq=50965 Ack=603 Win=24616 Len=923 |
| 135 | 4.343155 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| | | | | | [TCP Dup ACK 123#6] |
| 136 | 4.350339 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=51888 Ack=603 Win=24616 Len=1448 |
| 137 | 4.350408 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| | | | | | [TCP Dup ACK 123#7] |
| 138 | 4.350902 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [PSH, ACK] Seq=53336 Ack=603 Win=24616 Len=1448 |
| 139 | 4.350956 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| | | | | | [TCP Dup ACK 123#8] |
| 140 | 4.368094 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=54784 Ack=603 Win=24616 Len=1448 |
| 141 | 4.368171 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| | | | | | [TCP Dup ACK 123#9] |
| 142 | 4.368275 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=56232 Ack=603 Win=24616 Len=1448 |
| 143 | 4.368289 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| | | | | | [TCP Dup ACK 123#10] |
| 144 | 4.368404 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=57680 Ack=603 Win=24616 Len=1448 |
| 145 | 4.368420 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| | | | | | [TCP Dup ACK 123#11] |
| 146 | 4.368530 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=59128 Ack=603 Win=24616 Len=1448 |
| 147 | 4.368544 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| | | | | | [TCP Dup ACK 123#12] |
| 148 | 4.368662 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=60576 Ack=603 Win=24616 Len=1448 |
| 149 | 4.368679 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| | | | | | [TCP Dup ACK 123#13] |
| 150 | 4.368800 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=62024 Ack=603 Win=24616 Len=1448 |
| 151 | 4.368816 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| | | | | | [TCP Dup ACK 123#14] |
| 152 | 4.368829 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=64920 Ack=603 Win=24616 Len=143 |
| | | | | | [TCP Previous segment lost] |
| 153 | 4.368856 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| | | | | | [TCP Dup ACK 123#15] |
| 154 | 4.368929 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=63472 Ack=603 Win=24616 Len=1448 |
| | | | | | [TCP Retransmission] |
| 155 | 4.368947 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| | | | | | [TCP Dup ACK 123#16] |
| 156 | 4.369060 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=65063 Ack=603 Win=24616 Len=1448 |
| 157 | 4.369077 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| | | | | | [TCP Dup ACK 123#17] |

| | | | | | |
|-------|---------------------------|-----------------|-----------------|-----|---|
| 158 | 4.369178 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=66511 Ack=603 Win=24616 Len=1448 |
| 159 | 4.369194 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| [TCP | Dup ACK 123#18] | | | | |
| 160 | 4.369314 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=67959 Ack=603 Win=24616 Len=1448 |
| 161 | 4.369328 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| [TCP | Dup ACK 123#19] | | | | |
| 162 | 4.369434 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=69407 Ack=603 Win=24616 Len=1448 |
| 163 | 4.369448 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| [TCP | Dup ACK 123#20] | | | | |
| 164 | 4.369563 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=70855 Ack=603 Win=24616 Len=1448 |
| 165 | 4.369578 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| [TCP | Dup ACK 123#21] | | | | |
| 166 | 4.369615 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [PSH, ACK] Seq=72303 Ack=603 Win=24616 Len=762 |
| 167 | 4.369627 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=42277 Win=62980 Len=0 |
| [TCP | Dup ACK 123#22] | | | | |
| 168 | 4.371667 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=73065 Ack=603 Win=24616 Len=0 |
| [TCP | Dup ACK 31#1] | | | | |
| 169 | 4.371710 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=73065 Ack=603 Win=24616 Len=0 |
| [TCP | Dup ACK 31#2] | | | | |
| 170 | 4.372444 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [PSH, ACK] Seq=42277 Ack=603 Win=24616 Len=1448 |
| [TCP | Retransmission] | | | | |
| 171 | 4.372506 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [ACK] Seq=603 Ack=73065 Win=38028 Len=0 |
| ... | | | | | |
| 204 | 4.454893 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [FIN, ACK] Seq=93071 Ack=603 Win=24616 Len=0 |
| 205 | 4.456253 | 163.117.144.131 | 212.187.153.30 | TCP | 46070 > www [FIN, ACK] Seq=603 Ack=93072 Win=64088 Len=0 |
| 206 | 4.483923 | 212.187.153.30 | 163.117.144.131 | TCP | www > 46070 [ACK] Seq=93072 Ack=604 Win=24616 Len=0 |
| ... | | | | | |
| 209 | 4.531295 | 163.117.144.131 | 163.117.144.129 | DNS | Standard query A hits.gureport.co.uk |
| 210 | 4.531548 | 163.117.144.129 | 163.117.144.131 | DNS | Standard query response |
| CNAME | ehg-gureport1p.hitbox.com | A 64.154.82.26 | | | |
| 211 | 4.531951 | 163.117.144.131 | 64.154.82.26 | TCP | 48238 > www [SYN] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460 |
| ... | | | | | |
| 218 | 4.618860 | 163.117.144.131 | 163.117.144.129 | DNS | Standard query A ads.guardian.co.uk |
| 219 | 4.647918 | 163.117.144.129 | 163.117.144.131 | DNS | Standard query response A 212.187.153.37 |
| 220 | 4.648531 | 163.117.144.131 | 212.187.153.37 | TCP | 37579 > www [SYN] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460 |
| 221 | 4.648618 | 163.117.144.131 | 212.187.153.37 | TCP | 37580 > www [SYN] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460 |
| 222 | 4.676876 | 212.187.153.37 | 163.117.144.131 | TCP | www > 37579 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460 |
| 223 | 4.676985 | 163.117.144.131 | 212.187.153.37 | TCP | 37579 > www [ACK] Seq=1 Ack=1 Win=5840 Len=0 |
| 224 | 4.677016 | 212.187.153.37 | 163.117.144.131 | TCP | www > 37580 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460 |
| 225 | 4.677033 | 163.117.144.131 | 212.187.153.37 | TCP | 37580 > www [ACK] Seq=1 Ack=1 Win=5840 Len=0 |
| 226 | 4.677553 | 163.117.144.131 | 212.187.153.37 | TCP | 37580 > www [ACK] Seq=1 Ack=1 Win=5840 Len=730 |
| 227 | 4.677578 | 163.117.144.131 | 212.187.153.37 | TCP | 37580 > www [PSH, ACK] Seq=731 Ack=1 Win=5840 Len=58 |
| 228 | 4.677611 | 163.117.144.131 | 212.187.153.37 | TCP | 37579 > www [ACK] Seq=1 Ack=1 Win=5840 Len=730 |
| 229 | 4.677626 | 163.117.144.131 | 212.187.153.37 | TCP | 37579 > www [PSH, ACK] Seq=731 Ack=1 Win=5840 Len=62 |
| ... | | | | | |
| 231 | 4.705520 | 212.187.153.37 | 163.117.144.131 | TCP | www > 37580 [ACK] Seq=1 Ack=1 Win=24616 Len=0 |
| [TCP | Window Update] | | | | |
| 232 | 4.705593 | 212.187.153.37 | 163.117.144.131 | TCP | www > 37579 [ACK] Seq=1 Ack=1 Win=24616 Len=0 |
| [TCP | Window Update] | | | | |
| 233 | 4.705608 | 212.187.153.37 | 163.117.144.131 | TCP | www > 37579 [ACK] Seq=1 Ack=793 Win=24616 Len=0 |
| 234 | 4.705628 | 212.187.153.37 | 163.117.144.131 | TCP | www > 37580 [ACK] Seq=1 Ack=789 Win=24616 Len=0 |
| ... | | | | | |
| 240 | 4.725694 | 163.117.144.131 | 163.117.144.129 | DNS | Standard query A image.guardian.co.uk |
| 241 | 4.728690 | 212.187.153.37 | 163.117.144.131 | TCP | www > 37579 [FIN, ACK] Seq=1303 Ack=793 Win=24616 Len=0 |
| [TCP | Previous segment lost] | | | | |
| 242 | 4.728763 | 163.117.144.131 | 212.187.153.37 | TCP | 37579 > www [ACK] Seq=793 Ack=1 Win=5840 Len=0 |
| [TCP | Dup ACK 223#1] | | | | |
| 243 | 4.729385 | 212.187.153.37 | 163.117.144.131 | TCP | www > 37579 [PSH, ACK] Seq=1 Ack=793 Win=24616 Len=1302 |
| [TCP | Retransmission] | | | | |
| 244 | 4.729448 | 163.117.144.131 | 212.187.153.37 | TCP | 37579 > www [ACK] Seq=793 Ack=1304 Win=8736 Len=0 |
| 245 | 4.730260 | 163.117.144.131 | 212.187.153.37 | TCP | 37579 > www [FIN, ACK] Seq=793 Ack=1304 Win=8736 Len=0 |
| 246 | 4.733418 | 212.187.153.37 | 163.117.144.131 | TCP | www > 37580 [ACK] Seq=1 Ack=789 Win=24616 Len=1448 |
| 247 | 4.733483 | 163.117.144.131 | 212.187.153.37 | TCP | 37580 > www [ACK] Seq=789 Ack=1449 Win=8736 Len=0 |
| ... | | | | | |
| 252 | 4.735783 | 64.154.82.26 | 163.117.144.131 | TCP | www > 48238 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460 |
| 253 | 4.735885 | 163.117.144.131 | 64.154.82.26 | TCP | 48238 > www [ACK] Seq=1 Ack=1 Win=5840 Len=0 |
| 254 | 4.736239 | 163.117.144.131 | 64.154.82.26 | TCP | 48238 > www [ACK] Seq=1 Ack=1 Win=5840 Len=730 |
| 255 | 4.736265 | 163.117.144.131 | 64.154.82.26 | TCP | 48238 > www [PSH, ACK] Seq=731 Ack=1 Win=5840 Len=680 |
| 256 | 4.757888 | 212.187.153.37 | 163.117.144.131 | TCP | www > 37579 [ACK] Seq=1304 Ack=794 Win=24616 Len=0 |
| ... | | | | | |
| 259 | 4.761840 | 163.117.144.129 | 163.117.144.131 | DNS | Standard query response A 212.187.153.32 |
| 260 | 4.762433 | 163.117.144.131 | 212.187.153.32 | TCP | 43126 > www [SYN] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460 |
| 261 | 4.762472 | 212.187.153.37 | 163.117.144.131 | TCP | www > 37580 [FIN, PSH, ACK] Seq=4345 Ack=789 Win=24616 Len=42 |
| 262 | 4.762591 | 163.117.144.131 | 212.187.153.32 | TCP | 43127 > www [SYN] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460 |
| 263 | 4.762865 | 163.117.144.131 | 212.187.153.32 | TCP | 37580 > www [FIN, ACK] Seq=789 Ack=4388 Win=14528 Len=0 |
| 264 | 4.790325 | 212.187.153.32 | 163.117.144.131 | TCP | www > 43126 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460 |
| 265 | 4.790440 | 163.117.144.131 | 212.187.153.32 | TCP | 43126 > www [ACK] Seq=1 Ack=1 Win=5840 Len=0 |
| 266 | 4.790473 | 212.187.153.32 | 163.117.144.131 | TCP | www > 43127 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460 |

```

267 4.790490 163.117.144.131 212.187.153.32 TCP 43127 > www [ACK] Seq=1 Ack=1 Win=5840 Len=0
268 4.790908 163.117.144.131 212.187.153.32 TCP 43126 > www [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=713
269 4.790946 163.117.144.131 212.187.153.32 TCP 43127 > www [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=698
270 4.791146 212.187.153.37 163.117.144.131 TCP www > 37580 [ACK] Seq=4388 Ack=790 Win=24616 Len=0
...

```

■ Apartado 1:

1. ¿Por qué la solicitud de una dirección en un navegador tiene como resultado una petición DNS?
2. ¿En qué difieren los mensajes de petición DNS de los mensajes de respuesta DNS?
3. ¿Qué protocolo de transporte cree que usan los mensajes DNS de esta traza? Justifique su respuesta.
4. En caso de que se emitan varias peticiones DNS y se obtengan varias respuestas DNS, ha de establecerse la correspondencia entre preguntas y respuestas. ¿Qué mecanismo se usa para establecer esta correspondencia y en qué lugar de los mensajes DNS aparece la información necesaria?
5. ¿Cuál es el número de puerto del destino en del mensaje 27 (representado como www)?
6. Los datos del segmento TCP contenido en el mensaje número 30 es una petición HTTP 1.1 emitida por el navegador. ¿Cuál es su sintaxis?
7. Los datos del segmento TCP contenido en el mensaje número 32 es una respuesta HTTP 1.1 que indica que la petición previa HTTP se realizó con éxito. ¿Cuál es su sintaxis?
8. ¿Cuál es el propósito del segmento contenido en el mensaje número 127?
9. ¿Cuál es el significado de la respuesta DNS del mensaje 210?
10. Cuando el cliente recibió el mensaje 241 con el segmento de petición de terminación, ¿había recibido previamente el cliente algún segmento que contuviera datos del servidor?

■ Apartado 2:

1. Asumiendo que no se utiliza ningún sistema de compresión, ¿cuánto espacio ocupa la sección de petición de la petición DNS del mensaje número 25?
2. Proporcione la siguiente información sobre cada conexión TCP abierta a `ads.guardian.co.uk`:
 - el número del puerto efímero del cliente
 - los mensajes que contienen los segmentos que comprende el handshake (proporcione los números de mensaje)
 - los mensajes que contienen los segmentos que comprende la terminación de conexión (proporcione los números de mensaje).

■ Apartado 3:

1. Considere los paquetes 44, 45 y 46. Asumiendo que el mensaje 46 en efecto contenía la retransmisión de un paquete perdido emitido inmediatamente después del paquete del mensaje número 42 (en lugar de tratarse de una llegada en desorden mal etiquetada por la herramienta Ethereal) ¿podría haber sido generado como resultado de la recepción por parte del servidor 212.187.153.30 del ack duplicado contenido en el mensaje 45? Justifique su respuesta.
2. Asumiendo de nuevo que el mensaje 46 en efecto contenía la retransmisión de un paquete perdido emitido inmediatamente después del paquete del mensaje número 42 (en lugar de tratarse de una llegada en desorden mal etiquetada por la herramienta Ethereal), qué cota superior podemos establecer para el valor de RTO del servidor en el momento de la pérdida del paquete; debe asumir que se ha utilizado el algoritmo slow start (e ignorar si el valor de la cota superior es realista o no).
3. Asumiendo que el servidor repara en la pérdida del paquete indicada en los ack duplicados enviados por el cliente entre los mensajes 125 y 169 por medio de un temporizador, ¿qué comportamiento cabe esperar del servidor cuando repara en la pérdida de este paquete?
4. Otra vez, con respecto a la pérdida del paquete indicada en los acks duplicados enviados por el cliente entre los mensajes 125 y 169, en estas circunstancias el servidor puede realizar fast retransmit; ¿qué significa esto?

Problema 31

El siguiente problema trata sobre la búsqueda en red y posterior descarga de un fichero llamado “ficheroascii.txt”, desde la máquina 192.168.1.2, a través de una aplicación que realiza los siguientes pasos:

1. En el primer paso, la aplicación obtiene las direcciones de máquinas que están activas en red en ese momento, y que podrían contener el fichero. Para ello, realiza varias peticiones HTTP sobre un servidor central (82.144.26.188), que siempre está activo y que conoce las direcciones de máquinas activas.
2. En el segundo paso, la aplicación realiza una búsqueda del fichero “ficheroascii.txt” sobre las máquinas encontradas en el punto 1. Este paso no forma parte de este examen.
3. En el tercer paso, la aplicación finalmente descarga el fichero “ficheroascii.txt”.

A continuación, se muestra una traza capturada con la herramienta Wireshark correspondiente al primer paso, donde la aplicación realiza varias peticiones HTTP a un servidor para saber qué máquinas están activas en la red en ese momento y que podrían alojar el fichero pedido:

| No. | Tiempo | Origen | Destino | Protocolo | Información |
|-----|----------|---------------|---------------|-----------|--|
| 1 | 0.000000 | 192.168.1.2 | 82.144.26.188 | TCP | 2137 > http [SYN] Seq=0 Len=0 MSS=1460 |
| 2 | 0.090848 | 82.144.26.188 | 192.168.1.2 | TCP | http > 2137 [SYN,ACK] Seq=0 Ack=1 Win=5808 Len=0 MSS=1452 |
| 3 | 0.090948 | 192.168.1.2 | 82.144.26.188 | TCP | 2137 > http [ACK] Seq=1 Ack=1 Win=17424 Len=0 |
| 4 | 0.091198 | 192.168.1.2 | 82.144.26.188 | TCP | 2137 > http [ACK] Seq=1 Ack=1 Win=17424 Len=114 |
| | | DATOS: | | | GET http://82.144.26.188/cgi-bin/gcache.cgi?hostfile=1 HTTP/1.1\r\n User-Agent: R0tella v0.1\r\n Host: 82.144.26.188\r\n \r\n |
| 5 | 0.200737 | 82.144.26.188 | 192.168.1.2 | TCP | http > 2137 [ACK] Seq=1 Ack=115 Win=5808 Len=0 |
| 6 | 1.211909 | 82.144.26.188 | 192.168.1.2 | TCP | http > 2137 [ACK] Seq=1 Ack=115 Win=5808 Len=418 |
| | | DATOS: | | | HTTP/1.1 200 OK\r\n Date: Wed, 27 Dec 2006 18:58:55 GMT\r\n Server: Apache/2.0.54 (Debian GNU/Linux)\r\n Pragma: no-cache\r\n Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n Transfer-Encoding: chunked\r\n Content-Type: text/plain\r\n \r\n 26\r\n 82.144.26.210:6346\r\n 82.144.26.214:6346\r\n \r\n 0\r\n \r\n |
| 8 | 1.212249 | 192.168.1.2 | 82.144.26.188 | TCP | 2137 > http [ACK] Seq=115 Ack=419 Win=17006 Len=0 |
| 9 | 1.234729 | 192.168.1.2 | 82.144.26.188 | TCP | 2137 > http [ACK] Seq=115 Ack=419 Win=17006 Len=142 |
| | | DATOS: | | | GET http://82.144.26.188/cgi-bin/gcache.cgi?ip=192.168.1.2:6346 HTTP/1.1\r\n User-Agent: R0tella v0.1\r\n Host: 82.144.26.188\r\n Connection: close\r\n \r\n |
| 10 | 1.352637 | 82.144.26.188 | 192.168.1.2 | TCP | http > 2137 [ACK] Seq=419 Ack=257 Win=6432 Len=0 |
| 11 | 1.360073 | 192.168.1.2 | 82.144.26.188 | TCP | 2137 > http [FIN, ACK] Seq=257 Ack=419 Win=17006 Len=0 |
| | | [.....] | | | |
| 16 | 1.483868 | 82.144.26.188 | 192.168.1.2 | TCP | http > 2137 [ACK] Seq=419 Ack=258 Win=6432 Len=0 |
| | | [.....] | | | |
| 27 | 2.484045 | 82.144.26.188 | 192.168.1.2 | TCP | http > 2137 [ACK] Seq=419 Ack=258 Win=6432 Len=402 |
| | | DATOS: | | | HTTP/1.1 200 OK\r\n Date: Wed, 27 Dec 2006 18:58:56 GMT\r\n Server: Apache/2.0.54 (Debian GNU/Linux)\r\n Pragma: no-cache\r\n Cache-Control: no-store, no-cache\r\n Connection: close\r\n Transfer-Encoding: chunked\r\n Content-Type: text/plain\r\n \r\n 4\r\n |

```

                OK!\n
                \r\n
                O\r\n
                \r\n
28 2.484101 192.168.1.2      82.144.26.188  TCP      2137 > http [RST] Seq=258 Ack=821 Win=0 Len=0
29 2.484141 82.144.26.188  192.168.1.2   TCP      http > 2137 [FIN,ACK] Seq=821 Ack=258 Win=6432 Len=0
30 2.484189 192.168.1.2      82.144.26.188  TCP      2137 > http [RST] Seq=258 Len=0

```

Según la traza anterior, responde a las siguientes cuestiones:

- 1.1. ¿Cuántas conexiones TCP se han abierto, y entre qué máquinas y puertos?.
- 1.2. Indique los segmentos que contienen el inicio y el final de las conexiones TCP. Indique si ambas (inicio y fin) se han realizado correctamente
- 1.3. En el segmento 4, indique si la petición contiene alguna cabecera HTTP incorrecta o que falte.
- 1.4. En el segmento 6, indique si la respuesta contiene alguna cabecera HTTP incorrecta o que falte.
- 1.5. En el segmento 9, indique el significado de la cabecera “Connection: close”. En el segmento 27, indique el significado de la cabecera “Cache-control: no-store, no-cache”.
- 1.6. Asumiendo que la cabecera “Connection: close” se añada también en los segmentos 4 y 6 y asumiendo que todos los errores los apartados 1.2, 1.3 y 1.4 se han corregido (si los hubiera), indique si la traza anterior sigue siendo válida.

NOTA: los campos Len de la traza anterior no contienen ningún error.

El segundo paso consiste en, una vez encontradas las máquinas disponibles en red en ese momento (en nuestro caso, se trata de las máquinas 82.144.26.214 y de 82.144.26.210, véanse datos del segmento 6), realizar una búsqueda del fichero “ficheroascii.txt”. Este segundo paso no forma parte de este examen, y se debe asumir que el fichero “ficheroascii.txt” se ha encontrado en la máquina 82.144.26.214.

El tercer paso consiste en que, una vez encontrado el fichero “ficheroascii.txt” en la máquina 82.144.26.214, la aplicación realiza una descarga que se muestra a continuación capturada en forma de traza:

```

No. Tiempo  Origen          Destino          Protocolo  Información
1 0.000000 192.168.1.2     82.144.26.214  TCP      2488 > http [SYN] Seq=0 Len=0 MSS=1460
2 0.153173 82.144.26.214  192.168.1.2   TCP      http > 2488 [SYN,ACK] Seq=0 Ack=1 Win=5808 Len=0 MSS=1452
3 0.153331 192.168.1.2     82.144.26.214  TCP      2488 > http [ACK] Seq=1 Ack=1 Win=17424 Len=0
4 0.153639 192.168.1.2     82.144.26.214  TCP      2488 > http [ACK] Seq=1 Ack=1 Win=17424 Len=373
  DATOS:      GET /camino/ficheroascii.txt HTTP/1.1\r\n
             [Resto de cabeceras http irrelevantes para la resolución del problema]
5 0.248862 82.144.26.214  192.168.1.2   TCP      http > 2488 [ACK] Seq=1 Ack=374 Win=6432 Len=0
6 0.249675 82.144.26.214  192.168.1.2   TCP      http > 2488 [ACK] Seq=1 Ack=374 Win=6432 Len=1452
  DATOS:      [Cabeceras de respuesta http (ocupan 425 bytes) + Contenido de ‘ficheroascii.txt’]
7 0.251060 192.168.1.2     82.144.26.214  TCP      2488 > http [ACK] Seq=374 Ack=1453 Win=17424 Len=0
8 0.251175 82.144.26.214  192.168.1.2   TCP      http > 2488 [ACK] Seq=1453 Ack=374 Win=6432 Len=1452
  DATOS:      [Contenido de ‘ficheroascii.txt’]
9 0.440406 82.144.26.214  192.168.1.2   TCP      http > 2488 [ACK] Seq=2905 Ack=374 Win=6432 Len=1452
  DATOS:      [Contenido de ‘ficheroascii.txt’]
10 0.440546 192.168.1.2     82.144.26.214  TCP      2488 > http [ACK] Seq=374 Ack=4357 Win=17424 Len=0
11 0.440763 82.144.26.214  192.168.1.2   TCP      http > 2488 [ACK] Seq=4357 Ack=374 Win=6432 Len=1452
  DATOS:      [Contenido de ‘ficheroascii.txt’]
12 0.441220 82.144.26.214  192.168.1.2   TCP      http > 2488 [ACK] Seq=5809 Ack=374 Win=6432 Len=1452
  DATOS:      [Contenido de ‘ficheroascii.txt’]
13 0.441332 192.168.1.2     82.144.26.214  TCP      2488 > http [ACK] Seq=374 Ack=7261 Win=17424 Len=0
14 0.518408 82.144.26.214  192.168.1.2   TCP      http > 2488 [ACK] Seq=7261 Ack=374 Win=6432 Len=1452
  DATOS:      [Contenido de ‘ficheroascii.txt’]

```

```

15 0.518589 192.168.1.2 82.144.26.214 TCP 2488 > http [ACK] Seq=374 Ack=8713 Win=17424 Len=0
16 0.523138 82.144.26.214 192.168.1.2 TCP http > 2488 [ACK] Seq=8713 Ack=374 Win=6432 Len=1452
   DATOS: [Contenido de 'ficheroascii.txt']

17 0.524939 82.144.26.214 192.168.1.2 TCP http > 2488 [ACK] Seq=10165 Ack=374 Win=6432 Len=1452
   DATOS: [Contenido de 'ficheroascii.txt']

18 0.525059 192.168.1.2 82.144.26.214 TCP 2488 > http [ACK] Seq=374 Ack=11617 Win=17424 Len=0
19 0.525208 82.144.26.214 192.168.1.2 TCP http > 2488 [ACK] Seq=11617 Ack=374 Win=6432 Len=163
   DATOS: [Contenido de 'ficheroascii.txt']

20 0.722034 192.168.1.2 82.144.26.214 TCP 2488 > http [ACK] Seq=374 Ack=11780 Win=17261 Len=0

```

Según la traza anterior, responda a las siguientes cuestiones:

- 2.1. Indique el tamaño del fichero descargado.
- 2.2. Indique los diferentes mecanismos de TCP que aparecen en la traza anterior, y los diferentes valores de los campos ACK y WIN.
- 2.3. Si el segmento 11 se perdiera, construya una tabla con la evolución de la traza a partir del segmento 12 usando el algoritmo de Fast Retransmit/Fast Recovery hasta la retransmisión del segmento perdido. La tabla tendrá el mismo formato que la traza, con los siguientes campos: No. Origen Destino Protocolo Información(Puertos Flags Seg Ack Win Len)

Problema 32

En la siguiente sesión HTTP, en la que hemos numerado cada línea para poder referenciarla posteriormente y en la que cierta información la hemos ocultado con ***:

```

01 ~>telnet www.google.com 80
02 Trying 209.85.137.147...
03 Connected to mg-in-f147.google.com.
04 Escape character is '^]'.
05 GET / HTTP/1.1
06 ****: *****
07
08 HTTP/1.1 302 Found
09 *****: http://www.google.es/
10 Cache-Control: private
11 Set-Cookie: PREF=ID=79a8f699
12 Content-Type: text/html
13 Server: gws
14 *****: 218
15 *****: *****
16
17 <HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8">
18 <TITLE>302 Moved</TITLE></HEAD><BODY>
19 <H1>302 Moved</H1>
20 The document has moved
21 <A HREF="http://www.google.es/">here</A>.
22 </BODY></HTML>

```

Diga las cabeceras que hemos ocultado en las líneas 06, 09, 14 y 15.

Problema 33

Suponga que un usuario está navegando por web y en un determinado instante pincha en un hipervínculo para obtener una página web. Sea RTTs el Round Trip Time entre el cliente y el servidor

web.

- CASO 1: La página www a recuperar contiene exactamente un objeto de tamaño muy pequeño (pequeño texto en html) y por lo tanto el tiempo de transmisión del objeto es igual a 0
- CASO 2: La página www a recuperar contiene dos objetos de tamaño muy pequeño (pequeño texto en html junto con un pequeño gif) y por lo tanto el tiempo de transmisión de ambos objetos es igual a 0.

De acuerdo con lo anterior conteste a lo siguiente:

1. Suponiendo que se utiliza el protocolo HTTP 1.0 y que no se ésta utilizando ningún mecanismo de seguridad ¿Cuánto tiempo como mínimo pasará, desde que el usuario pincha el hipervínculo hasta que se recibe la página en el cliente? Calcule este tiempo tanto para el caso 1 como para el caso2.
2. Suponiendo que se utiliza el protocolo HTTP 1.0 y que el servidor tiene protegida la página con el mecanismo de autenticación básico ¿Cuánto tiempo como mínimo pasará, desde que el usuario pincha el hipervínculo hasta que se recibe la página en el cliente? Calcule este tiempo tanto para el caso 1 como para el caso2.
3. Suponiendo que se utiliza el protocolo HTTP 1.1 y que no se ésta utilizando ningún mecanismo de seguridad ¿Cuánto tiempo como mínimo pasará, desde que el usuario pincha el hipervínculo hasta que se recibe la página en el cliente? Calcule este tiempo tanto para el caso 1 como para el caso2.

Problema 34

Una empresa dispone de una red corporativa consistente en una LAN de alta velocidad (una gigabit ethernet) y tiene contratado a un ISP (proveedor de Internet) un acceso a Internet, esencialmente para permitir el acceso a www. La conexión consiste en un router corporativo conectado a un router del ISP mediante un enlace de acceso de 1,5 Mbps.

Se toman estadísticas y se observa que:

- El tamaño medio de un objeto http es de 100 Kbit (suponga 1K=1000)
- Tasa media de peticiones www que tienen como destino servidores de fuera de la red corporativa es de 15 peticiones/seg
- De estas peticiones el 25 % corresponde a objetos accedidos desde la corporación en las últimas 24 horas, mientras que el 30 % son peticiones que se hacen una única vez y no se repiten nunca.
- El tiempo medio desde que un paquete con una petición http sale del router del ISP hasta que el paquete IP con la respuesta correspondiente llega a dicho router es de 2 sg.
- El retardo medio que sufre un paquete en atravesar el enlace de acceso (incluidos ambos routers) varía según el porcentaje de carga del enlace según se muestra en la tabla, y es el mismo en ambos sentidos.

| % carga | retardo medio |
|---------|---------------|
| 15 | 10 ms. |
| 30 | 50 ms. |
| 50 | 100 ms. |
| 75 | 1 sg. |
| 90 | 20 sg. |
| 100 | 1 min. |

Despreciando la longitud de las cabeceras de todos los niveles y suponiendo que, los navegadores www no tienen cache, y que tanto las peticiones como las respuestas http caben en un único paquete IP, se pide:

1. ¿Cuál será el tiempo medio de respuesta percibido por el usuario para recuperar un objeto http?.
2. Con el fin de mejorar el tiempo de respuesta deciden evaluar diferentes alternativas:
 - a) Sustituir la línea que une ambos routers por una de 10 Mbps. ¿Cuál sería en este caso el tiempo medio de respuesta percibido por el usuario?
 - b) Dejar la línea a 1,5 Mbps pero instalar un proxy web en la red corporativa. Según datos proporcionados por la empresa que vende los proxies, si la memoria cache es de 2 Gbytes se podrán almacenar en la cache todas las páginas accedidas desde la corporación en las últimas 24 horas; el tiempo medio de respuesta que percibirá el usuario si el objeto solicitado está en la cache será de 20 ms. ¿Cuál sería en este caso el tiempo medio de respuesta percibido por el usuario?
3. ¿Cuál deberá ser el tamaño de la memoria cache para lograr que el tiempo medio de respuesta percibido por el usuario se reduzca a 0,5 segundos?

Problema 35

Un ISP (Proveedor de Internet) regional tiene contratado con un ISP nacional la transmisión de 1000 Gbytes por mes (30 días) a un coste de 15.000 pts/Gbyte. El mencionado ISP da servicios de Internet a sus clientes, que esencialmente utilizan el web.

Se toman estadísticas y se observa que:

- Prácticamente el 100 % de las consultas www van dirigidas a servidores accesibles a través del ISP nacional.
- Del tráfico que se recibe del ISP nacional, el 10 % corresponde a cabeceras de los distintos protocolos involucrados (PPP, IP, TCP y HTTP) y el 90 % a datos (es decir, páginas HTML, imágenes, etc).
- Cada cliente recibe una media de 60 respuestas HTTP por día.
- La longitud media de los datos contenidos en una respuesta es de 8000 Bytes.
- De estas respuestas, el 20 % corresponde a páginas ya visitadas por algún cliente del ISP regional en el último día, mientras que el 30 % son peticiones que se hacen una única vez y no se repiten nunca.

Se pide:

1. ¿Cuántos clientes como máximo puede tener el ISP regional? Suponga que los navegadores no tienen caché. (solución: 62.500 clientes)
2. Si se instala en el ISP regional un proxy que almacene las páginas consultadas en el último día ¿cuántos clientes como máximo puede tener contratados? (solución: 78.125 clientes)
3. ¿Cuánta memoria caché necesitaría el proxy del apartado anterior? (solución: 30 Gbytes)
4. Comente las ventajas e inconvenientes, de cara al usuario y al ISP regional, de disponer o no de un proxy caché, así como, de utilizar caching explícito frente a caching transparente.

Problema 36

Una empresa ofrece un servicio de acceso web para leer correos internos desde fuera de la empresa. Jacinto está de viaje en Australia cuando su jefe le llama para que compruebe su correo. El correo número 1 que ha recibido contiene información confidencial, enviado por error, y que debe de borrar.

Suponiendo que:

- pop3.empresa.com es el servido POP3 de la empresa de Jacinto y pccmail.empresa.com es la máquina con el servido HTTP y la aplicación web.
 - Las máquinas pop3.empresa.com y pccmail.empresa.com son máquinas distintas
 - La aplicación web de acceso al correo:
 - Se ejecuta en pccmail.empresa.com y se accede vía el servidor HTTP de la misma máquina.
 - Da un interfaz gráfico de usuario para acceder y modificar correos, que también muestra el resultado de la aplicación en el cliente.
 - Tiene una ventana de inicio que pide login y password de la cuenta de correo del usuario antes de comenzar la sesión.
 - Se comunica con el servidor POP3 interpretando los comandos del usuario y convirtiéndolos a comandos POP3.
 - Mantiene la conexión al servidor de POP3 que está en la máquina pop3.empresa.com (a los 5 minutos la conexión se cierra si no hay peticiones).
 - Almacena un cookie para cada sesión de usuario que contiene el login, el password y la dirección IP del cliente.
1. Dibuje un diagrama que muestre los mensajes y comandos que se intercambian las cuatro máquinas: el PC de Jacinto, el servidor DNS del ISP de Jacinto, pccmail.empresa.com e pop3.empresa.com. NOTA: Recuerde que Jacinto sigue los siguientes pasos: arranca su navegador, se conecta a la aplicación web de correo, se conecta al buzón, borra el correo número 1 y sale.
 2. Hoy no es el día de Jacinto. Su jefe le llama de nuevo y le tiene discutiendo durante 10 minutos, durante los cuales Jacinto no puede teclear nada en su ordenador, y además la llamada ocurrió justo el momento en el que iba a pulsar el botón de borrado de la página HTML. ¿Qué supone usted que ocurrirá cuando Jacinto pulse el botón de borrado después de la llamada de su jefe?

Problema 37

Después de haber obtenido dos documentos de 12KBytes del servidor HTTP/1.1 de su red, un usuario solicita un tercer documento, también de 12KBytes, en la misma conexión HTTP. Justamente después de que la petición salga de su máquina, el cable de su interfaz ethernet (que está defectuoso) se desconecta. La desconexión dura el tiempo necesario para que se pierda el primer segmento de la respuesta. La conexión se restablece inmediatamente y el cable no vuelve a fallar.

Sabiendo que las cabeceras de respuesta de HTTP/1.1 ocupan 608 Bytes y que el servidor utiliza el algoritmo *fast recovery/fast retransmit*. Responda a las siguientes cuestiones:

1. ¿Cuánto habría tardado en llegar el tercer documento en caso de que no hubiera fallado el cable?
2. Justifique su respuesta anterior con un diagrama temporizado.
3. ¿Qué parámetros de TCP se ven afectados por el fallo del cable? ¿Qué valores toman en ese momento?
4. Después de que el servidor sabe que el cliente ha recibido correctamente el tercer documento, ¿cuál es el tamaño máximo de documento (en Bytes) que podría mandar el servidor sin recibir ningún asentimiento del cliente? Justifique su respuesta con un diagrama temporizado, indicando los valores que toman los parámetros indicados en el apartado anterior.

Problema 38

Considere la siguiente descarga FTP del fichero examen.txt. Las líneas están numeradas para poderlas referenciar más fácilmente después. Observe también el comando ejecutado al final (líneas 25 y 26). Alguna información se ha ocultado con los caracteres **** (el número de * no es significativo).

```

1 ~>ftp -d it003.lab.it.uc3m.es
2 Connected to it003.lab.it.uc3m.es.
3 220 it003 FTP server (Version wu-2.4(1)) ready.
4 Name: aptel
5 ---> USER aptel
6 331 Password required for aptel.
7 Password:
8 ---> PASS XXXX
9 230 User aptel logged in.
10 ---> SYST
11 215 UNIX Type: L8
12 Remote system type is UNIX.
13 ftp> get examen.txt
14 ---> TYPE I
15 200 Type set to I.
16 ---> ****
17 ****
18 ---> RETR examen.txt
19 150 Opening BINARY mode data connection for examen.txt(**** bytes).
20 226 Transfer complete.
21 1008 bytes received in 0.028 seconds (38 Kbytes/s)
22 ftp> bye
23 ---> QUIT
24 221 Goodbye.
25 ~>wc -l examen.txt
26 35 lista

```

Sabiendo que:

- La dirección IP del cliente es 163.117.139.130.
- La dirección IP de it003.lab.it.uc3m.es es 163.117.144.203.
- La conexión de control tiene como puerto origen el 1028.
- La conexión de datos tiene IP origen 163.117.144.203, y puerto destino 1036.
- Cliente y servidor están conectados a la misma red de área local Ethernet.

Responda a las siguientes preguntas:

1. Escriba el comando y la respuesta que irían en las líneas 16 y 17. Calcule aproximadamente cuántos paquetes IP se habrán intercambiado el cliente y el servidor en esta sesión FTP.
2. Suponga que el fichero lo descargamos mediante TFTP en modo netascii. Diga cuantos paquetes IP se intercambiarían en total el cliente y el servidor para hacer esta descarga, detallando qué contendría cada uno.
3. Suponga que el fichero está disponible también por HTTP en la URL <http://it003.lab.it.uc3m.es/aptel/examen.txt>. Detalle la petición y la respuesta HTTP, únicamente con las cabeceras obligatorias, suponiendo que se usa la versión 1.1 del protocolo, y calcule aproximadamente cuántos paquetes IP se intercambiarían en total el cliente y el servidor para hacer esta descarga. Explique las suposiciones que asuma.

Problema 39

Una máquina A va a descargarse un fichero de 10 KBytes de otra máquina B a través de Internet. Se sabe que:

- El retardo de propagación ida y vuelta entre ambas máquinas es $RTT = 200ms$.
- El retardo de transmisión de los paquetes es despreciable.
- El tiempo de proceso de las máquinas también es despreciable.
- Caso de usarse TCP, el MSS de la conexión es 1460 Bytes y cada segmento se asiente inmediatamente.
- No se pierde ningún paquete.

Diga qué paquetes se intercambiarán entre las máquinas A y B, (detallando el contenido de cada uno y el instante en que se transmite), y el tiempo total que tardará A en recibir el fichero de B para cada uno de los casos siguientes:

1. Se usa el protocolo **FTP**. (1 punto)
2. Se usa el protocolo **TFTP**. (1 punto)
3. Se usa el protocolo **HTTP**. (1 punto)

Si hace alguna suposición, indíquela.

Problema 40

Un servidor obtiene datos de distintos sensores de temperatura. Los sensores envían la hora de la muestra (16 Bytes) y la temperatura (8 Bytes) cada dos segundos. Los sensores de temperatura están dispersos por todo el mundo y envían sus datos al servidor utilizando el protocolo HTTP/1.1.

1. Indique en un diagrama temporizado como se realiza el envío de datos de un sensor al servidor.
2. Si el único factor limitante en el servidor es su conexión a 10Mbps con su router, ¿a cuántos sensores podría atender el servidor? Suponga que de los 10Mbps, obtiene 8Mbps a nivel IP.
3. ¿A cuántos podría atender si el envío de datos se hiciera por UDP?

Problema 41

A continuación le presentamos una capturas de tráfico perteneciente a HTTP, que contienen errores (comandos o respuestas que no son legales en el protocolo). Diga qué errores encuentra y explique cómo serían si fueran correctos.

1. Captura HTTP (sólo mostramos el contenido de los segmentos TCP que contienen información en la parte de datos):

Segmento de datos de cliente a servidor con el siguiente contenido:

```
GET / HTTP/1.1\r\n
Server: Mozilla/5.0 /X11; U; Linux i686; en-US; rv:1.0.0)\r\n
Accept: text/xml,text/html\r\n
Connection: open\r\n
Cookie: PREF=ID=48d260254400577e:TM=979053311\r\n
\r\n
```

Segmento de datos de servidor a cliente con el siguiente contenido:

```

HTTP/1.1 200 Found\r\n
Location: http://www.google.es/\r\n
Set-Cookie: PREF=ID=48d260254400577e:TM=979053311\r\n
Content-Type: text/html\r\n
User-Agent: GWS/2.1\r\n
Transfer-Encoding: chunked\r\n
Content-Length: 151\r\n
Cache-Control: private\r\n
Date: Fri, 17 Jun 2005 08:25:04 GMT\r\n
Connection: close\r\n
<HTML><HEAD><TITLE>302 Moved</TITLE></HEAD><BODY>\r\n
<H1>302 Moved</H1>\r\n
The document has moved\r\n
<A HREF="http://www.google.es/">here</A>.\r\n
</BODY></HTML>\r\n

```

Problema 42

Un alumno usa el programa telnet para abrir una sesión al puerto 80 de un servidor situado en la máquina `monitor01.lab.it.uc3m.es`, cuya dirección IP es `163.117.144.241`. Para ello, ejecuta el siguiente comando:

```
~> telnet monitor01.lab.it.uc3m.es 80
```

La primera acción del cliente telnet será resolver el dominio anterior:

1. Indique los paquetes enviados y recibidos (dir origen:puerto, dir destino:puerto, protocolo transporte, flags y datos) que usará el cliente telnet para la resolución del dominio `monitor01.lab.it.uc3m.es`.
2. Calcule el tamaño, en bytes, de cada paquete enviado/recibido del punto anterior.
3. En el caso de que, antes de ejecutar el comando del principio, se usara telnet para abrir una sesión al puerto por defecto del servidor DNS, indique si se pueden escribir peticiones (desde el teclado) como si fuera un cliente DNS y ver las respuestas del servidor. Razone su respuesta.

Una vez resuelto el dominio anterior, el usuario teclea la siguiente secuencia desde su sesión telnet:

```

GET examen.txt HTTP/1.1\r\n
Host: monitor01.lab.it.uc3m.es\r\n
\r\n

```

Sabiendo que cliente y servidor están conectados a la misma red de área local Ethernet, y que en el servidor existe un fichero llamado `examen.txt` de tamaño $4 \cdot \text{MSS}$, responda a las siguientes cuestiones:

4. Indique la respuesta HTTP recibida, únicamente con las cabeceras obligatorias.
5. Indique cuantas conexiones se han abierto, entre qué máquinas y qué protocolos se han usado.
6. Sabiendo que se pierde el segundo segmento que contiene la respuesta HTTP y que la ventana anunciada por ambos extremos es de $4 \cdot \text{MSS}$, indique la evolución de los siguientes parámetros en el servidor, desde el inicio hasta el final de la conexión: ventana anunciada, ventana de congestión, umbral, modo (slow start ó congestion avoidance). Detalle su respuesta con una tabla incluyendo los 4 parámetros anteriores.

NOTA: considere $RTO \gg RTT$.