

# Examen Parcial II de Sistemas Telemáticos para Medios Audiovisuales

GSyC, Universidad Rey Juan Carlos

22 de diciembre de 2017

---

## HTTP

---

1. Analiza la captura `/opt/stma/http-1.cap`. El contenido de la respuesta HTTP proviene de un proxy caché. Indica cuánto tiempo falta para que caduque el contenido que viaja en la respuesta HTTP del mensaje 6:  
  - (A) No se puede saber.
  - (B) 100 segundos.
  - (C) 32 segundos
  - (D) 68 segundos.
2. Analiza la captura `/opt/stma/http-1.cap`. Indica cuál de las siguientes afirmaciones es correcta:  
  - (A) El proxy caché antes de enviar la respuesta HTTP al cliente ha necesitado revalidar el recurso `index.html` y se sabe que éste había cambiado en el servidor.
  - (B) El proxy caché antes de enviar la respuesta HTTP al cliente ha necesitado revalidar el recurso `index.html` y se sabe que éste no había cambiado en el servidor.
  - (C) El proxy caché antes de enviar la respuesta HTTP al cliente no ha necesitado revalidar el recurso `index.html` con el servidor.
  - (D) El proxy caché antes de enviar la respuesta HTTP al cliente ha necesitado pedirselo al servidor, pues no lo tenía almacenado en su caché.
3. Un cliente HTTP envía la siguiente petición a un servidor HTTP:

```
GET /page_1.html HTTP/1.1
Host: www.server_one.com
```

Se sabe que la página pedida contiene 3 imágenes, 1 que está en el mismo servidor, y 2 que están en el servidor `www.server_two.com`, con quien el cliente se comunicará usando HTTP/1.0.

A partir del momento en el que el cliente termine de recibir el recurso `/page_1.html`, indica cuántas **nuevas conexiones TCP** abrirá dicho cliente:

- (A) 1.
- (B) 2.
- (C) 3.
- (D) El resto de afirmaciones son falsas.

4. Analiza la captura /opt/stma/http-2.cap. El día **22 de diciembre de 2017** el mismo cliente abre una conexión TCP con el servidor pc3.emp2.net y envía únicamente la Cookie: global\_id=5678. Indica qué petición puede haber realizado el cliente:
- (A) GET /compras/lista.html HTTP/1.0
- (B) GET /tienda/compras/lista.html HTTP/1.0
- (C) GET /tienda/compras/navidad/lista.html HTTP/1.0
- (D) No es posible que sólo haya enviado esa cookie.
5. Analiza la captura /opt/stma/http-2.cap. Indica cuál de las siguientes afirmaciones es correcta:
- (A) El cliente está enviando los datos del formulario form4.html usando el método GET.
- (B) Para que el cliente envíe los datos del formulario form4.html usando el método GET sería necesario cambiar el recurso form4.html en el servidor.
- (C) Para que el cliente envíe los datos del formulario form4.html usando el método GET sería necesario cambiar el recurso form4.html en el cliente.
- (D) El resto de las respuestas son falsas.
6. Observa la siguiente figura:

Cabeceras	Cookies	Parámetros	Respuesta	Tiempos
<b>URL solicitada:</b> http://www.madrid.org/cs/StaticFiles/ComunidadMadrid/css/home.css <b>Método de la petición:</b> GET <b>Dirección remota:</b> 209.84.3.254:80 <b>Código de estado:</b> ▲ 304 Not Modified ⓘ <a href="#">Editar y volver a enviar</a> Cabeceras sin procesar <b>Versión:</b> HTTP/1.1				
▼ Filtrar cabeceras				
▼ Cabeceras de la respuesta (235 B)				
ⓘ Cache-Control: max-age=3600 ⓘ Connection: keep-alive ⓘ Date: Thu, 21 Dec 2017 20:18:41 GMT ⓘ ETag: W/"1258-1352891649000" ⓘ Expires: Thu, 21 Dec 2017 21:18:41 GMT ⓘ Last-Modified: Wed, 14 Nov 2012 11:14:09 GMT				
▼ Cabeceras de la petición (595 B)				
ⓘ Accept: text/css,*/*;q=0.1 ⓘ Accept-Encoding: gzip, deflate ⓘ Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3 ⓘ Cache-Control: max-age=0 ⓘ Connection: keep-alive ⓘ Cookie: _pk_id.1.dd0f=09019fae24d55e3d...1513887448; _pk_ses.1.dd0f=* ⓘ Host: www.madrid.org				

Indica cuál de las siguientes afirmaciones es correcta:

- (A) La petición se ha podido realizar con las líneas de cabecera que se muestran en la figura.
- (B) Es necesario que la petición haya incluido la siguiente línea de cabecera:  
If-None-Match: W/"1258-1352891649000"
- (C) Es necesario que la petición haya incluido la siguiente línea de cabecera:  
If-Modified-Since: Thu, 21 Dec 2017 21:18:41 GMT
- (D) Es necesario que la petición haya incluido la siguiente línea de cabecera:  
If-Modified-Since: Thu, 21 Dec 2017 20:18:41 GMT

**ATENCIÓN:**

- Si ya has usado NetGUI con otro diagrama de red, cierra NetGUI y ejecuta `clean-netgui.sh` antes de volver a lanzar NetGUI.
- Arranca NetGUI, en el menú “Archivo” elige la opción “Abrir” y escribe como nombre de archivo `/opt/stma/cs`
- Se cargará el escenario mostrado en la figura 1.
- Arranca cada una de las máquinas del escenario, de una en una.
- Si en algún momento quieres volver a tener el escenario en su estado inicial, cierra NetGUI, ejecuta `clean-netgui.sh` y ejecuta después `/opt/stma/cs/reset-lab`

---

En el escenario no se ha configurado ninguna disciplina de colas ni de entrada ni de salida. Si realizas alguna configuración para alguna de las siguientes preguntas, recuerda borrar dicha configuración antes de pasar a otra pregunta.

---

7. Partiendo de la situación inicial, en `r1` y `r2` hay 2 scripts para la configuración de disciplina de cola de entrada: `r1-ingress.sh` y `r2-ingress.sh`, respectivamente. Estudia el contenido de dichos *scripts*. Si se ejecutan dichos *scripts* y se realiza el envío simultáneo utilizando `iperf` en `pc1`, `pc2` y `pc5` de 1Mbit de tráfico UDP desde cada una de estas máquinas a `pc3`, indica cuánto tráfico recibiría `pc3`:
- (A) 3 Mbits aproximadamente durante 10 segundos, 1 Mbit de `pc1`, 1Mbit de `pc2` y 1Mbit de `pc5`.
  - (B) 2 Mbits aproximadamente durante 10 segundos, 1 Mbit de `pc1` y 1Mbit de `pc2`.
  - (C) 2.5 Mbits aproximadamente durante 10 segundos, 1 Mbit de `pc1`, 500kbit de `pc2` y 1Mbit de `pc5`.
  - (D) 1.5 Mbits aproximadamente durante 10 segundos, 1 Mbit de `pc1` y 500kbit de `pc2`.

8. Partiendo de la situación inicial del escenario se ha configurado en r3(eth2) una disciplina de cola que limita el tráfico a 700kbps y da mayor prioridad al tráfico de pc1, después al de pc2 y por último al de pc5.

Se comienza el envío simultáneo de tráfico hacia pc4 con las siguientes características:

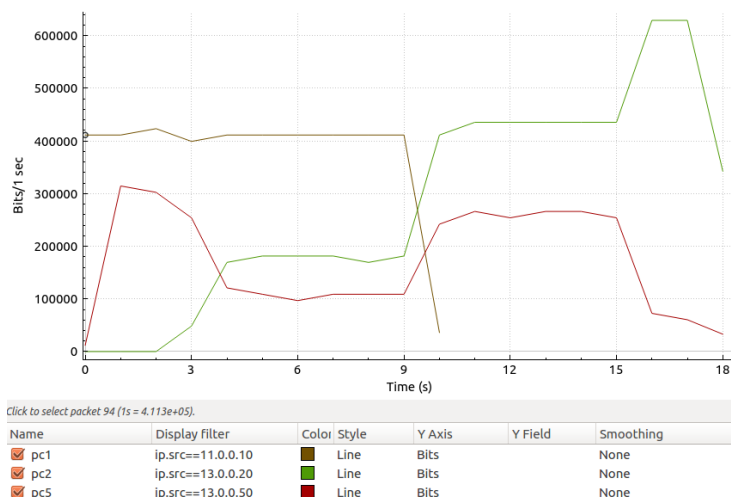
- 400kbps desde pc1
- 300kbps desde pc5

Después de que hayan pasado entre 3 ó 4 segundos aproximadamente desde que comenzó este envío de tráfico se inicia el envío de 500kbps desde pc2 a pc4. Indica cuál de las siguientes gráficas se corresponde con el tráfico descrito.

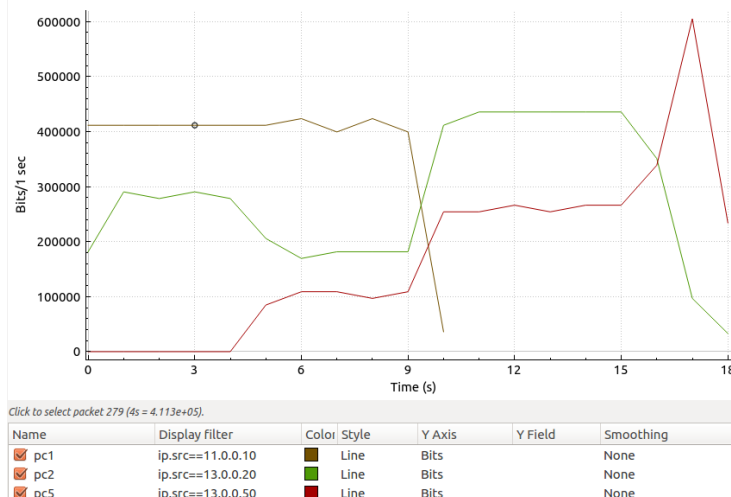
(A) Gráfica



(B) Gráfica



(C) Gráfica



(D) Ninguna de las gráficas se corresponde con el tráfico descrito.

9. Partiendo de la situación inicial del escenario se realiza una configuración de disciplina de cola HTB en la interfaz `eth2` de `r3`. Utilizando `iperf` se envía tráfico durante 10 segundos con diferentes anchos de banda. Se ha capturado dicho tráfico en la interfaz `r3(eth2)` y se encuentra almacenado en el fichero `/opt/stma/cs.cap`.

Suponiendo que no se ha descartado tráfico, indica cuál de las siguientes afirmaciones es correcta:

- (A)
  - En `pc1` se ha arrancado `iperf` para que envíe a 500kbps aproximadamente
  - En `pc2` se ha arrancado `iperf` para que envíe a 200kbps aproximadamente
  - En `pc5` se ha arrancado `iperf` para que envíe a 300kbps aproximadamente
- (B)
  - En `pc1` se ha arrancado `iperf` para que envíe a 800kbps aproximadamente
  - En `pc2` se ha arrancado `iperf` para que envíe a 200kbps aproximadamente
  - En `pc5` se ha arrancado `iperf` para que envíe a 500kbps aproximadamente
- (C)
  - En `pc1` se ha arrancado `iperf` para que envíe a 600kbps aproximadamente
  - En `pc2` se ha arrancado `iperf` para que envíe a 200kbps aproximadamente
  - En `pc5` se ha arrancado `iperf` para que envíe a 1Mbps aproximadamente
- (D)
  - En `pc1` se ha arrancado `iperf` para que envíe a 1Mbps aproximadamente
  - En `pc2` se ha arrancado `iperf` para que envíe a 200kbps aproximadamente
  - En `pc5` se ha arrancado `iperf` para que envíe a 1Mbps aproximadamente

10. Partiendo de la situación inicial del escenario se realiza una configuración de disciplina de cola de salida TBF para limitar el tráfico a 500kbit en la interfaz `r3(eth2)`. Se utilizan los valores `burst=10k` y `latencia=10ms` para la configuración de la misma.

Si se envía tráfico a 1Mbit simultáneamente durante 10 segundos desde `pc1`, `pc2` y `pc5` a la subred `15.0.0.0/24` utilizando `iperf`, indica cuál de las siguientes afirmaciones es correcta:

- (A) La tasa máxima de tráfico que alcanzará dicha subred es 500kbit de cada fuente.
- (B) La tasa máxima de tráfico que alcanzará dicha subred es 500kbit en total.
- (C) No se puede conocer cuál será la tasa máxima de tráfico que alcanzará dicha subred.
- (D) No es posible utilizar TBF cuando existen varias fuentes de tráfico como en este caso: `pc1`, `pc2` y `pc5`.

11. Partiendo de la situación inicial del escenario se desea marcar los paquetes por su dirección IP origen, tal y como se muestra en esta figura:

```
▶ Frame 17: 1512 bytes on wire (12096 bits), 1512 bytes captured (12096 bits)
▶ Ethernet II, Src: 52:9d:bb:35:42:01 (52:9d:bb:35:42:01), Dst: f2:b1:bd:ff:60:97 (f2:b1:bd:ff:60:97)
▼ Internet Protocol Version 4, Src: 11.0.0.10, Dst: 15.0.0.30
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
    ▶ Differentiated Services Field: 0x68 (DSCP: AF31, ECN: Not-ECT)
        Total Length: 1498
        Identification: 0x3bb4 (15284)
    ▶ Flags: 0x02 (Don't Fragment)
        Fragment offset: 0
        Time to live: 63
        Protocol: UDP (17)
    ▶ Header checksum: 0xdfcf [validation disabled]
        Source: 11.0.0.10
        Destination: 15.0.0.30
```

Partiendo de la siguiente configuración en r3:

```
tc qdisc add dev eth1 handle ffff: ingress

tc filter add dev eth1 parent ffff: protocol ip prio 1 \
    u32 match ip src 11.0.0.10/32 \
    police rate 500kbit burst 10k drop flowid :10

tc qdisc add dev eth0 handle ffff: ingress

tc filter add dev eth0 parent ffff: protocol ip prio 2 \
    u32 match ip src 13.0.0.20/32 \
    police rate 500kbit burst 10k drop flowid :20

tc qdisc add dev eth2 handle 1:0 root dsmark indices 8

tc class change dev eth2 classid 1:1 dsmark mask 0x3 value 0x68
tc class change dev eth2 classid 1:2 dsmark mask 0x3 value 0x88
```

Indica cuál debería ser el filtro definido para poder obtener el paquete marcado de la figura:

- (A) `tc filter add dev eth2 parent 1:0 protocol ip prio 1 handle 10 tcindex classid 1:1`
- (B) `tc filter add dev eth2 parent 1:0 protocol ip prio 1 handle 1 tcindex classid 1:1`
- (C) `tc filter add dev eth2 parent 1:0 protocol ip prio 1 handle 20 tcindex classid 1:1`
- (D) `tc filter add dev eth2 parent 1:0 protocol ip prio 1 handle 0x68 tcindex classid 1:2`

12. En un router que **no aparece en la figura** se tiene definida la siguiente configuración:

```
tc qdisc add dev eth1 root handle 1:0 dsmark indices 8 set_tc_index
tc filter add dev eth1 parent 1:0 protocol ip prio 1 tcindex mask 0xfc shift 2

tc qdisc add dev eth1 parent 1:0 handle 2:0 htb

tc class add dev eth1 parent 2:0 classid 2:1 htb rate 1Mbit

tc class add dev eth1 parent 2:1 classid 2:10 htb rate 800kbit ceil 1Mbit

tc filter add dev eth1 parent 2:0 protocol ip prio 1 handle 0x0a tcindex classid 2:10
```

Indica qué crees que ocurriría si en la configuración anterior no estuviera la línea:

```
tc filter add dev eth1 parent 1:0 protocol ip prio 1 tcindex mask 0xfc shift 2
```

- (A) La configuración funcionaría igualmente sin esa línea, para cualquier tráfico que viniera marcado con AF11.
- (B) La configuración no funcionaría igual ya que ese filtro desplaza todos los bits del campo DiffServ para eliminar ese campo y poder reutilizarlo con el valor que deseemos.
- (C) La configuración no funcionaría igual ya que ese filtro permite marcar los paquetes en su campo DiffServ con el valor 0xfc.
- (D) La configuración no funcionaría igual ya que el campo DiffServ estaría incluyendo los bits ECN y dependería de sus valores.

13. Al acceder a la página web **www.eloferton.es** desde el navegador, el servidor envía un certificado de su clave pública. Dicho certificado está emitido por la CA **Symantec**. Se sabe que dicha CA **NO es una CA raíz**.

Indica cuál de las siguientes afirmaciones es correcta:

- (A) Para comprobar la validez de dicho certificado el navegador necesita disponer de la clave pública de la CA **Symantec**.
- (B) Para comprobar la validez de dicho certificado el navegador **NO** necesita la clave pública de la CA **Symantec**, pues le basta con utilizar la clave pública de alguna de las CA Raíz, instaladas en su navegador.
- (C) Al estar dicho certificado emitido por una CA que **NO** es CA Raíz, será imposible para el navegador comprobar la validez del mismo.
- (D) El resto de afirmaciones son falsas.

14. Alicia y Roberto usan criptografía de clave pública para intercambiar mensajes, y conocen la función hash criptográfica  $H()$ .

Alicia y Roberto no han tenido oportunidad de intercambiarse en persona sus respectivas claves públicas, ni disponen de ningún certificado en las mismas.

Roberto recibe el siguiente mensaje:  $[M_1, K_A^+, K_A^-(H(M_1))]$ , siendo  $M_1$  el texto: "Soy Alicia. Te adjunto mi clave pública".

Indica cuál de las siguientes afirmaciones es correcta.

- (A) Dado que el mensaje incluye tanto  $K_A^+$  como una firma digital usando  $K_A^-$ , Roberto puede comprobar que el mensaje  $M_1$  procede realmente de Alicia.
- (B) Si Roberto envía el mensaje  $[K_A^+(M_2)]$ , sólo podrá extraer  $M_2$  el remitente del mensaje original  $M_1$ .
- (C) Si Roberto envía el mensaje  $[K_A^+(M_2)]$ , y como respuesta recibe el mensaje  $[M_2, K_A^-(H(M_2))]$ , es seguro que el mensaje original  $M_1$  procedía realmente de Alicia.
- (D) El resto de afirmaciones son falsas.

15. Alicia, Bárbara y Carlos usan criptografía de clave pública para intercambiar mensajes. Se sabe que:

- Alicia y Carlos se han intercambiado sus claves públicas de forma segura.
- Alicia y Bárbara se han intercambiado sus claves públicas de forma segura.

Carlos necesita la clave pública de Bárbara pero no la tiene.

Indica cuál de los siguientes mensajes permite que Alicia envíe la clave pública de Bárbara a Carlos, de forma que Carlos pueda obtenerla estando seguro de que se trata realmente de la clave pública de Bárbara.

- (A)  $[K_B^+, K_A^+(H(K_B^+))]$
- (B)  $[K_A^-(K_B^+)]$
- (C)  $[K_B^+, K_C^+(H(K_B^+))]$
- (D)  $[K_C^+(K_B^+), K_C^+(H(K_B^+))]$



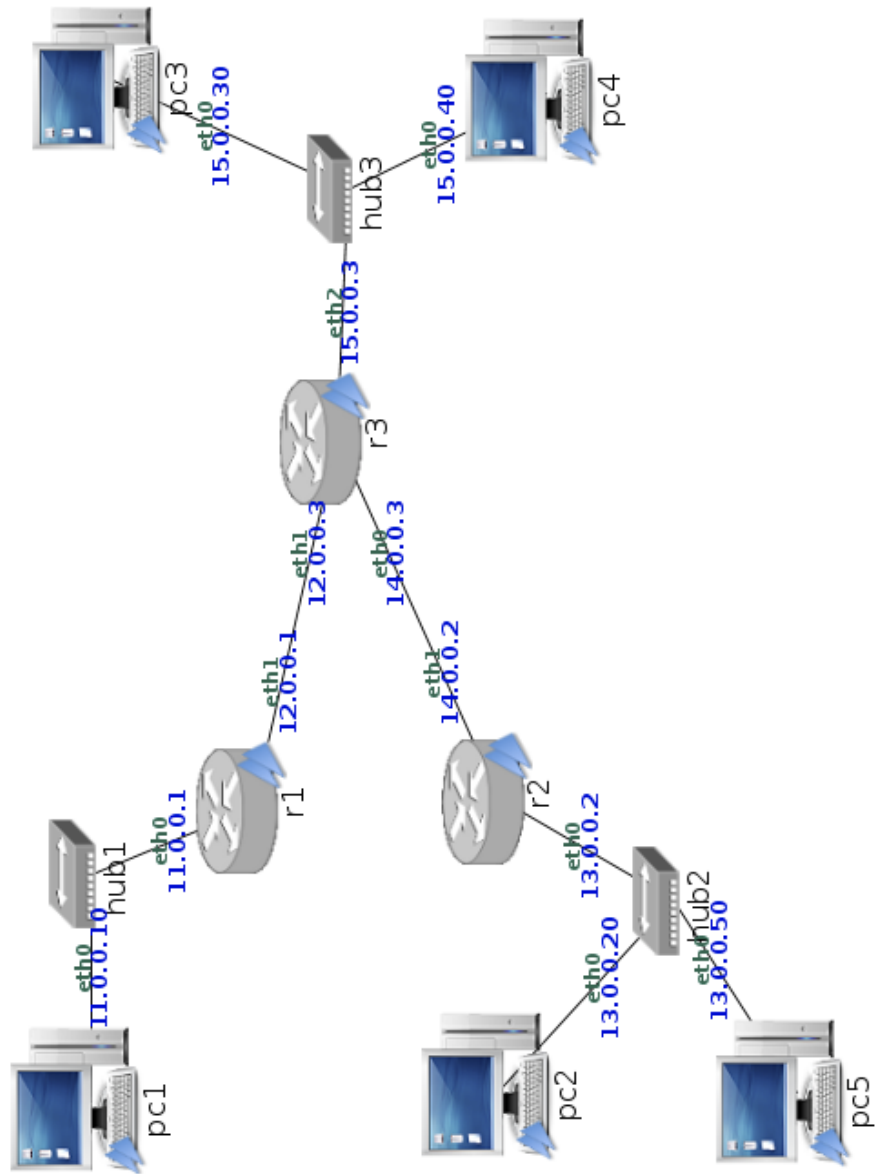


Figura 1: Calidad de servicio