

Examen Parcial II de Sistemas Telemáticos para Medios Audiovisuales

GSyC, Universidad Rey Juan Carlos

14 de junio de 2018

HTTP

1. Analiza la captura `/opt/stma/http-1.cap`. Indica cuál de las siguientes afirmaciones es correcta con respecto al momento en que se ha realizado la captura de tráfico:
 - (A) La máquina 11.0.0.1 solicita por primera vez el recurso `/index.html` a la máquina 14.0.0.100.
 - (B) La máquina 11.0.0.1 tenía almacenado previamente el recurso `/index.html` pero ha caducado en la siguiente fecha: 11 Jun 2018 a las 8:51:26 GMT, por eso vuelve a solicitarlo y la máquina 14.0.0.100 se lo envía.
 - (C) La máquina 11.0.0.1 tenía almacenado previamente el recurso `/index.html` pero ha caducado, por eso vuelve a solicitarlo. La máquina 14.0.0.100 vuelve a enviarle el recurso, aunque éste no había cambiado.
 - (D) La máquina 11.0.0.1 tenía almacenado previamente el recurso `/index.html` pero ha caducado, por eso vuelve a solicitarlo. La máquina 14.0.0.100 vuelve a enviarle el recurso porque sabe que el contenido del recurso ha cambiado con respecto a la versión que tiene 11.0.0.1.
2. Analiza la captura `/opt/stma/http-2.cap`. Indica cuál de las siguientes afirmaciones es correcta:
 - (A) La máquina 11.0.0.1 NO puede almacenar el recurso obtenido.
 - (B) La máquina 11.0.0.1 puede almacenar el recurso obtenido con una caducidad de 200 segundos.
 - (C) La máquina 11.0.0.1 puede almacenar el recurso obtenido con un período de validez de 200 segundos pero siempre habrá de revalidar su contenido, independientemente de su caducidad.
 - (D) No se puede saber si la máquina 11.0.0.1 puede almacenar el recurso obtenido.
3. Un cliente HTTP envía una petición del recurso `index.html` a un servidor HTTP, servidor1. Se sabe que la página pedida contiene 3 imágenes: una imagen está en el mismo servidor (servidor1) y 2 imágenes están en otro servidor (servidor2). Además, se sabe que desde que el cliente solicitó la página al servidor1 ha necesitado abrir un total de 3 conexiones TCP para poder mostrar la página completa.

Indica cuál de las siguientes afirmaciones es correcta:

 - (A) Es seguro que el cliente se comunica con servidor1 con conexiones persistentes y con el servidor2 con conexiones persistentes.
 - (B) Es seguro que el cliente se comunica con un servidor con conexiones persistentes y con el otro con conexiones NO persistentes.
 - (C) Es imposible que la descarga se haya completado con 3 conexiones TCP.
 - (D) Es seguro que el cliente se comunica con servidor1 con conexiones NO persistentes y con el servidor2 con conexiones NO persistentes.

4. Un cliente realiza la petición `GET /tienda/deportes/baloncesto/index.html HTTP/1.0` y envía las siguientes cookies:
- `Cookie: session-id=12345, token-id=abcde`
- Suponiendo que no ha caducado ninguna de esas cookies, indica qué cookies enviaría el mismo cliente si realizara al mismo servidor la siguiente petición `GET /tienda/deportes/baloncesto/canasta-mini/index.html HTTP/1.0`
- (A) Con la información mostrada no se puede decir nada de las cookies que se enviarían en la nueva petición.
- (B) Es posible que se envíen menos cookies que en la petición inicial.
- (C) Se enviarán exactamente las mismas cookies, ni más ni menos.
- (D) Se enviarán al menos las mismas cookies que en la petición inicial, y es posible que se envíe alguna cookie más.
5. Analiza la captura `/opt/stma/http-3.cap`. Transcurridos 100 segundos después de haber realizado dicha captura de tráfico si el usuario de la máquina 12.0.0.100 escribe en el navegador la URL `http://pc2.emp2.net/index.html`, indica cuál de las siguientes afirmaciones es correcta:
- (A) El navegador de la máquina 12.0.0.100 obtiene dicho contenido de la caché del navegador.
- (B) El proxy instalado en 12.0.0.1 obtiene dicho contenido de la caché del proxy y se lo proporciona al navegador de la máquina 12.0.0.100.
- (C) El servidor HTTP instalado en `pc2.emp2.net` proporciona el contenido al proxy HTTP instalado en 12.0.0.1 y el proxy se lo proporciona al navegador de la máquina 12.0.0.100.
- (D) El resto de las respuestas son falsas.
6. Analiza la captura `/opt/stma/http-3.cap`. Indica cuál de las siguientes afirmaciones es correcta:
- (A) La respuesta HTTP proviene de un proxy en el que el recurso lleva almacenado en la caché 200 segundos desde que se obtuvo o revalidó por última vez.
- (B) La respuesta HTTP proviene de un proxy en el que el recurso tendrá validez durante 200 segundos.
- (C) La respuesta HTTP proviene de un proxy. El recurso estaba caducado en el proxy, pero debido a que el proxy no ha podido contactar en este momento con el servidor para realizar la revalidación, le devuelve dicha respuesta caducada al cliente.
- (D) No se puede saber si la respuesta HTTP proviene de un proxy.

7. En r1 se realiza la siguiente configuración:

```
#!/bin/sh

tc qdisc add dev eth0 handle ffff: ingress

tc filter add dev eth0 parent ffff: protocol ip prio 1 \
    u32 match ip src 11.0.0.10/32 \
    police rate 1.2Mbit burst 10k drop flowid :1
```

Y, además, en r2 se realiza la siguiente configuración:

```
#!/bin/sh

tc qdisc add dev eth0 handle ffff: ingress

tc filter add dev eth0 parent ffff: protocol ip prio 1 \
    u32 match ip src 13.0.0.20/32 \
    police rate 500kbit burst 10k drop flowid :1
```

Se realiza el envío simultáneo utilizando `iperf` en pc1, pc2 y pc5 de 1Mbit de tráfico UDP desde cada una de estas máquinas a pc4, indica cuánto tráfico recibiría pc4:

- (A) 3 Mbps aproximadamente durante 10 segundos, 1 Mbps de pc1, 1Mbps de pc2 y 1Mbps de pc5.
- (B) 2 Mbps aproximadamente durante 10 segundos, 1 Mbps de pc1 y 1Mbps de pc2.
- (C) 1.7 Mbps aproximadamente durante 10 segundos, 1.2 Mbps de pc1 y 500kbps de pc2.
- (D) 2.7 Mbps aproximadamente durante 10 segundos, 1.2 Mbps de pc1, 500kbps de pc2 y 1Mbps de pc5.

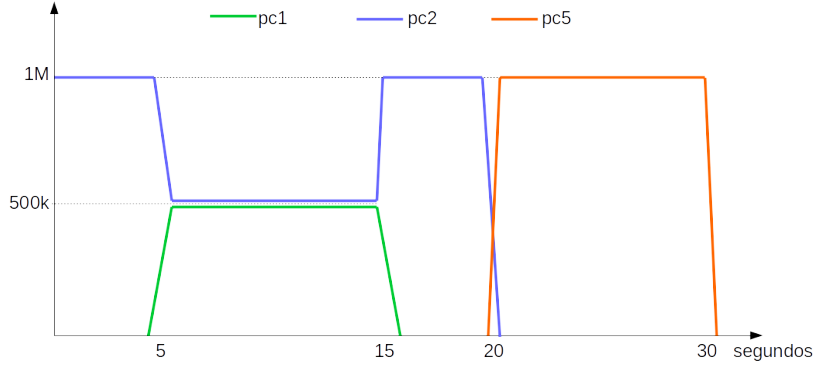
8. Partiendo de la situación inicial del escenario se ha configurado en r3(eth2) una disciplina de cola que limita el tráfico a 1Mbps y da mayor prioridad al tráfico de pc1, después al de pc2 y por último al de pc5.

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

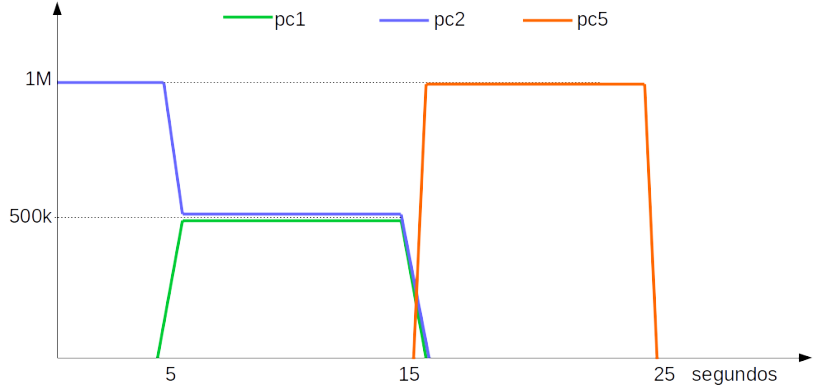
- 1Mbps desde pc2 durante 10 segundos.
- 1Mbps desde pc5 durante 10 segundos.

Después de que hayan pasado 5 segundos aproximadamente desde que comenzó este envío de tráfico se inicia el envío de 500kbps desde pc1 a pc4. Indica cuál de las siguientes gráficas se corresponde con el tráfico descrito.

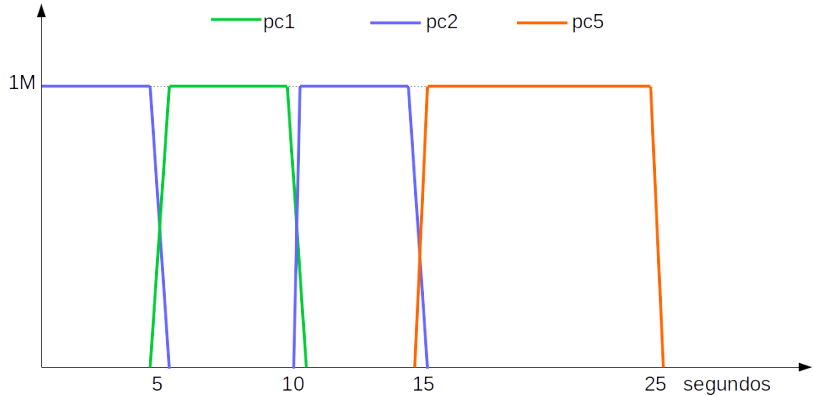
(A) Gráfica



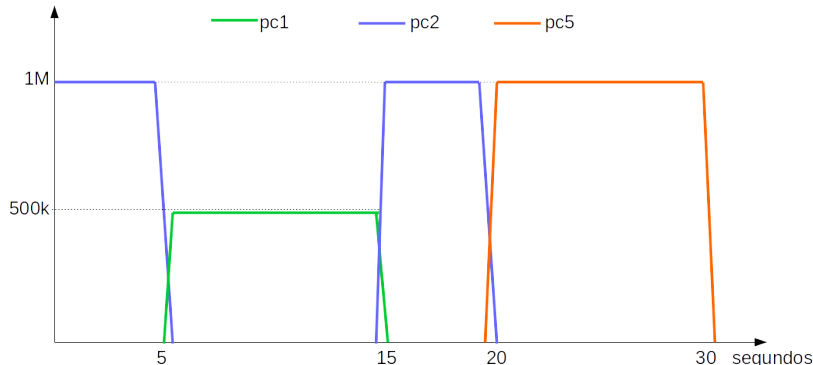
(B) Gráfica



(C) Gráfica



(D) Gráfica



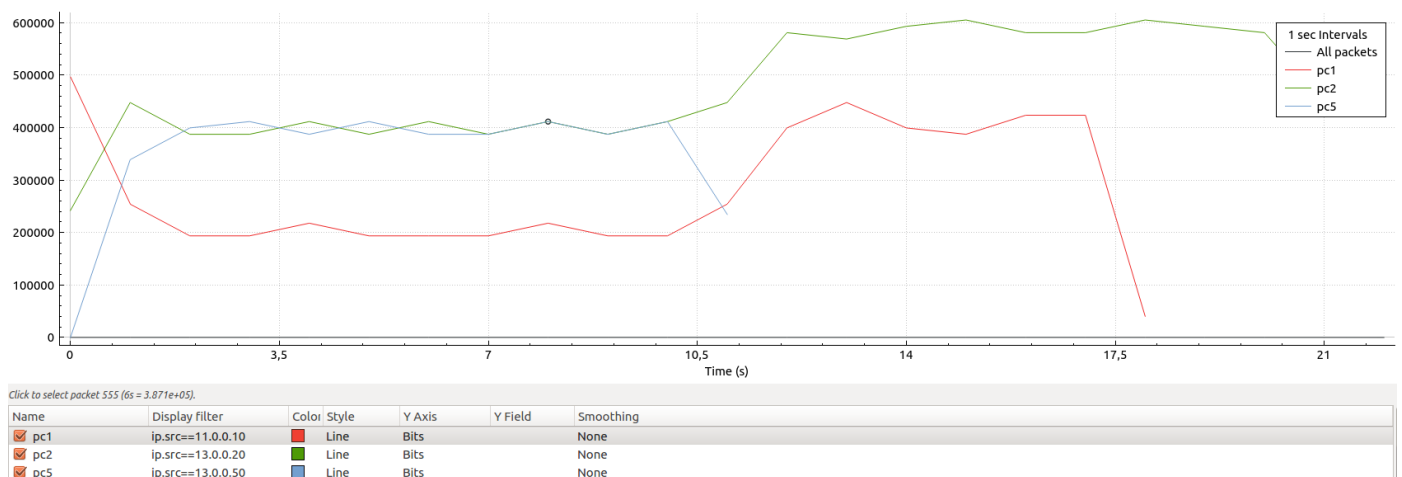
9. Partiendo de la situación inicial del escenario se realiza una configuración de disciplina de cola HTB en la interfaz **eth2** de **r3**. Utilizando **iperf** se envía tráfico durante 10 segundos con diferentes anchos de banda. Se ha capturado dicho tráfico en la interfaz **r3(eth2)** y se encuentra 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 400kbps aproximadamente
 ■ En **pc2** se ha arrancado **iperf** para que envíe a 1.2Mbps aproximadamente
 ■ En **pc5** se ha arrancado **iperf** para que envíe a 1Mbps aproximadamente
- (B) ■ En **pc1** se ha arrancado **iperf** para que envíe a 400kbps aproximadamente
 ■ En **pc2** se ha arrancado **iperf** para que envíe a 600kbps aproximadamente
 ■ En **pc5** se ha arrancado **iperf** para que envíe a 1Mbps aproximadamente
- (C) ■ En **pc1** se ha arrancado **iperf** para que envíe a 400kbps aproximadamente
 ■ En **pc2** se ha arrancado **iperf** para que envíe a 600kbps aproximadamente
 ■ En **pc5** se ha arrancado **iperf** para que envíe a 1.5Mbps aproximadamente
- (D) ■ En **pc1** se ha arrancado **iperf** para que envíe a 1Mbps aproximadamente
 ■ En **pc2** se ha arrancado **iperf** para que envíe a 1.2Mbps 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 HTB para limitar el tráfico total a 1Mbps en la interfaz **r3(eth2)**.

Se envía simultáneamente tráfico desde **pc1**, **pc2** y **pc5** durante 10 segundos y se obtiene la siguiente gráfica en **r3(eth2)**:



Sabiendo que está definida HTB con limitación de tráfico 1Mbps y están definidos los filtros que clasifican el tráfico de la siguiente forma: tráfico de **pc1** a la clase 1:2, tráfico de **pc2** a la clase 1:3 y tráfico de **pc5** a la clase 1:4, indica qué clases habrá sido necesario definir para obtener la gráfica anterior:

- (A) `tc class add dev eth2 parent 1:1 classid 1:2 htb rate 200kbit ceil 1Mbit`
`tc class add dev eth2 parent 1:1 classid 1:3 htb rate 400kbit ceil 600kbit`
`tc class add dev eth2 parent 1:1 classid 1:4 htb rate 400kbit ceil 1Mbit`
- (B) `tc class add dev eth2 parent 1:1 classid 1:2 htb rate 200kbit ceil 1Mbit`
`tc class add dev eth2 parent 1:1 classid 1:3 htb rate 400kbit ceil 400kbit`
`tc class add dev eth2 parent 1:1 classid 1:4 htb rate 400kbit ceil 1Mbit`
- (C) `tc class add dev eth2 parent 1:1 classid 1:2 htb rate 200kbit ceil 200kbit`
`tc class add dev eth2 parent 1:1 classid 1:3 htb rate 400kbit ceil 1Mbit`
`tc class add dev eth2 parent 1:1 classid 1:4 htb rate 400kbit ceil 1Mbit`
- (D) `tc class add dev eth2 parent 1:1 classid 1:2 htb rate 200kbit ceil 200kbit`
`tc class add dev eth2 parent 1:1 classid 1:3 htb rate 400kbit ceil 600kbit`
`tc class add dev eth2 parent 1:1 classid 1:4 htb rate 400kbit ceil 1Mbit`

11. Se ejecuta la siguiente configuración en r3:

```
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 100kbit burst 10k drop flowid :10

tc filter add dev eth0 parent ffff: protocol ip prio 2 \
  u32 match ip src 13.0.0.50/32 \
  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

tc filter add dev eth2 parent 1:0 protocol ip prio 1 handle 10 tcindex classid 1:1
tc filter add dev eth2 parent 1:0 protocol ip prio 1 handle 20 tcindex classid 1:2
```

Indica cuál de las siguientes afirmaciones es correcta:

- (A) Se permite 100kbps de pc2 que quedan marcados como AF31 y 500kbps de pc5 que quedan marcados como AF41.
- (B) Se permite 500kbps de pc2 que quedan marcados como AF31 y 100kbps de pc5 que quedan marcados como AF41.
- (C) Se permite 100kbps de pc2 que quedan marcados como AF41 y 500kbps de pc5 que quedan marcados como AF31.
- (D) Se permite 500kbps de pc2 que quedan marcados como AF41 y 100kbps de pc5 que quedan marcados como AF31.

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 400kbit ceil 800kbit
tc class add dev eth1 parent 2:1 classid 2:20 htb rate 800kbit ceil 1Mbit
```

Indica qué configuración adicional crees necesaria realizar para que los paquetes que vengan marcados con AF31 tengan garantizado un tráfico de 800kbps.

- (A) `tc filter add dev eth1 parent 2:0 protocol ip prio 1 handle 0x1a tcindex classid 2:10`
- (B) `tc filter add dev eth1 parent 2:0 protocol ip prio 1 handle 0x1a tcindex classid 2:20`
- (C) `tc filter add dev eth1 parent 2:0 protocol ip prio 1 handle 0x68 tcindex classid 2:10`
- (D) `tc filter add dev eth1 parent 2:0 protocol ip prio 1 handle 0x68 tcindex classid 2:20`

13. Al acceder a la página web **www.eliferton.es** desde el navegador, el servidor envía un certificado de su clave pública. Dicho certificado está emitido por la CA **Symantec**.

Indica cuál de las siguientes afirmaciones es correcta:

- (A) Se necesita utilizar la clave privada de **www.eliferton.es** para comprobar la validez de dicho certificado.
- (B) La CA **Symantec** ha necesitado utilizar su clave privada para generar el certificado de **www.eliferton.es**.
- (C) La CA **Symantec** ha necesitado utilizar su clave pública para generar el certificado de **www.eliferton.es**.
- (D) Se necesita utilizar la clave pública de **www.eliferton.es** para comprobar la validez de dicho certificado.

14. Alicia y Bárbara usan criptografía de clave pública y han intercambiado sus claves públicas de forma segura.

Alicia quiere utilizar criptografía de clave simétrica para intercambiar mensajes a Bárbara, para ello, Alicia eligirá una clave simétrica K_{AB} que enviará a Bárbara.

Indica cuál de los siguientes procedimientos le permite a Bárbara conocer la clave simétrica, de forma que puedan intercambiar mensajes de forma confidencial y que Bárbara pueda estar segura de que es Alicia quien le ha enviado K_{AB} :

- (A) $A \rightarrow B: \text{mensaje} = K_B^+(K_{AB})$
- (B) $A \rightarrow B: \text{mensaje} = K_A^-(K_{AB})$
- (C) $A \rightarrow B: \text{mensaje} = \{K_{AB}, K_A^-(H(K_{AB}))\}$
- (D) $A \rightarrow B: \text{mensaje} = \{K_B^+(K_{AB}), K_A^-(H(K_{AB}))\}$

15. Alicia y Bárbara usan criptografía de clave pública para enviarse mensajes, pero nunca se han visto en persona para intercambiarse sus claves públicas, K_A^+ y K_B^+ , y dichas claves no tienen ningún certificado.

Se sabe que Trudón, cuya clave pública es K_T^+ quiere engañar a Bárbara, aprovechándose de que Bárbara confía en Trudón y no piensa que le vaya a engañar.

Indica cuál de las siguientes afirmaciones es correcta:

- (A) Trudón le da (en persona) a Bárbara K_T^+ diciéndole que es la clave pública de Alicia. Esto le permitirá a Trudón leer los mensajes confidenciales que Bárbara envíe a Alicia.
- (B) Trudón le da (en persona) a Bárbara K_T^+ diciéndole que es la clave pública de Alicia. Esto le permitirá a Trudón enviar mensajes a Alicia que a ella le parecerá que son de Bárbara.
- (C) Trudón le da (en persona) a Bárbara K_A^+ diciéndole que es su propia clave pública (la de Trudón). Esto le permitirá a Trudón leer los mensajes confidenciales que Bárbara envíe a Alicia.
- (D) El resto de afirmaciones son falsas.

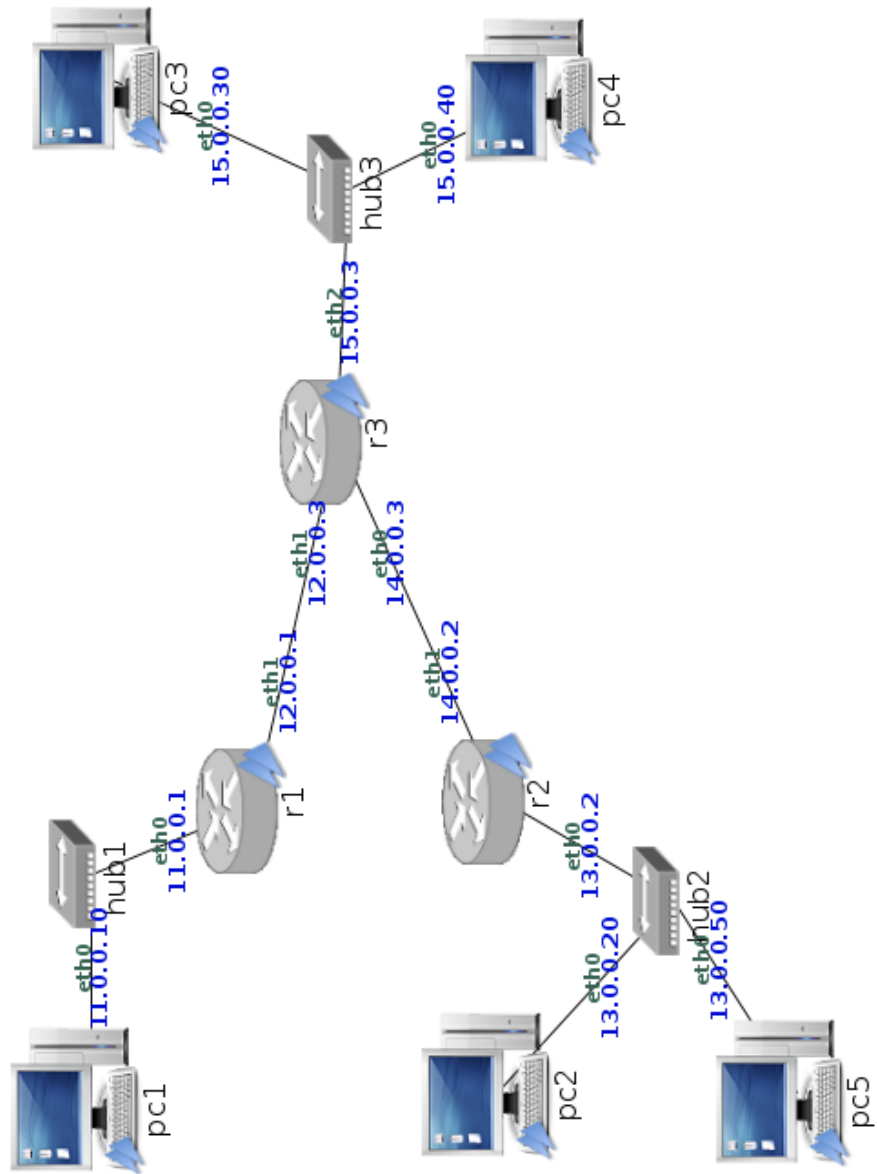


Figura 1: Calidad de servicio