Examen Parcial II de Sistemas Telemáticos para Medios Audiovisuales

GSyC, Universidad Rey Juan Carlos

17 de junio de 2016

CALIDAD DE SERVICIO y DiffServ

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.

---

1. Partiendo de la situación inicial del escenario se configura en `r3(eth2)` HTB con limitación de 1Mbit repartido de la siguiente forma:

   - rate=300 kbps para el tráfico de `pc1` con ceil=500kbps.
   - rate=400 kbps para el tráfico de `pc2` con ceil=1Mbps.
   - rate=300 kbps para le tráfico de `pc5` con ceil=1Mbps.

   Se inicia el envío simultáneo de tráfico UDP con `iperf` durante 10s con las siguientes características:

   - desde `pc1` dirigido a `pc3` a 300kbps
   - desde `pc2` dirigido a `pc4` a 1Mbps
   - desde `pc5` dirigido a `pc4` a 100kbps

   Indica cuál de las siguientes afirmaciones sería correcta:

   (A) `pc3` recibirá 300kbps durante los 10s que dura la transmisión y después de esos 10 segundos aproximadamente, no recibirá más tráfico. `pc4` recibirá 700kbit durante los 10s que dura la transmisión y después de esos 10 segundos aproximadamente, no recibirá más tráfico.

   (B) `pc3` recibirá 500kbps durante los 10s que dura la transmisión y después de esos 10 segundos aproximadamente, no recibirá más tráfico. `pc4` recibirá 500kbit durante los 10s que dura la transmisión y después de esos 10s aproximadamente, no recibirá más tráfico.

   (C) `pc3` recibirá 300kbit durante los 10s que dura la transmisión y después de esos 10 segundos aproximadamente, no recibirá más tráfico. `pc4` recibirá 700kbit durante los 10s que dura la transmisión. Después de esos 10s `pc4` seguirá recibiendo tráfico durante aproximadamente 4 segundos más, este tráfico estaba encolado en `r3` procedente de `pc2`.

   (D) `pc3` recibirá 300kbps durante los 10s que dura la transmisión y después de esos 10 segundos aproximadamente, no recibirá más tráfico. `pc4` recibirá 700kbit durante los 10s que dura la transmisión. Después de esos 10s `pc4` seguirá recibiendo tráfico durante aproximadamente 4 segundos más, este tráfico estaba encolado en `r3` procedente de `pc2` y `pc5` que se reparten entre ellos el ancho de banda sobrante.

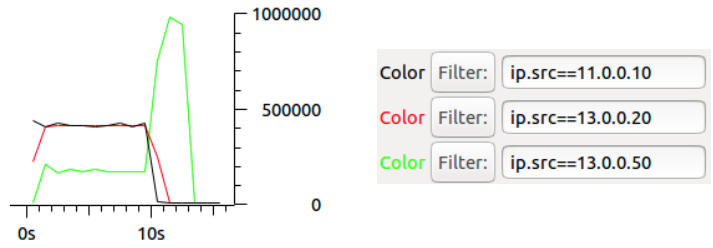
2. Partiendo de la situación inicial del escenario se configuran en `r3(eth2)` unas disciplinas de cola de salida que limiten el tráfico de salida a 800kbps, con latencia=50s, y que den prioridad al tráfico según su dirección IP origen (de más prioridad a menos prioridad): tráfico de `pc1` (más prioritario), tráfico de `pc2` (prioridad intermedia) y tráfico de `pc5` (tráfico menos prioritario).

   Desde `pc1`, `pc2` y `pc5` se realiza el envío simultáneo de tráfico UDP utilizando `iperf` durante 10s con las siguientes características:

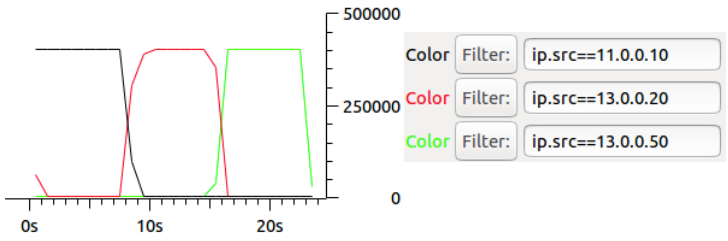
   - `pc1` envía a `pc3` a 400kbps.
   - `pc2` envía a `pc4` a 400kbps.
   - `pc5` envía a `pc4` a 400kbps.

   Indica cuál de las siguientes gráficas de tráfico sería posible que se capturara en la interfaz `r3(eth2)` (el tráfico se muestra en bits por segundo):

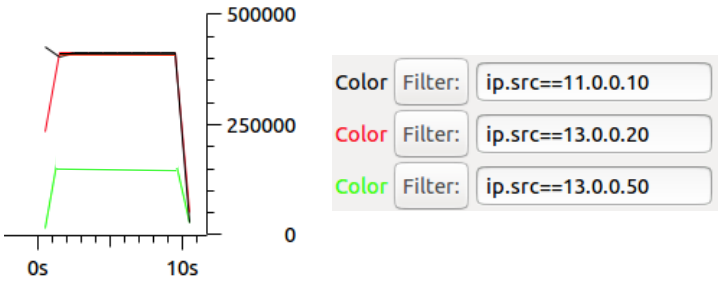
   (A) Gráfica 1.



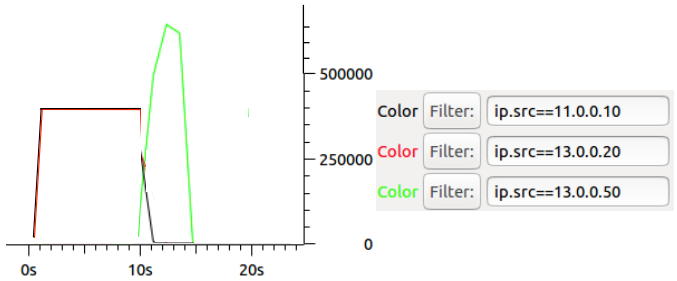
   (B) Gráfica 2.



   (C) Gráfica 3.



   (D) Gráfica 4.



3. Supón que se configura la siguiente disciplina de cola en r2:

```
tc qdisc add dev eth0 handle ffff: ingress

tc filter add dev eth0 parent ffff:
    protocol ip prio 4 u32 \
    match ip src 13.0.0.20/32 \
    police rate 100kbit burst 10k drop flowid :1

tc filter add dev eth0 parent ffff:
    protocol ip prio 5 u32 \
    match ip src 13.0.0.50/32 \
    police rate 400kbit burst 10k drop flowid :2
```

En r2 se recibe tráfico de pc2 y pc5 sin marcas DiffServ. Se desea que el tráfico de pc2 y pc5 llegue marcado a r3 con los siguientes valores DiffServ: el tráfico de pc2 con marca AF11 y el tráfico de pc5 con marca AF21. Indica cuál de las siguientes configuraciones lo permite:

(A) En r2:

```
tc qdisc add dev eth1 handle 1:0 root dsmark indices 8

tc class change dev eth1 classid 1:1 dsmark mask 0x3 value 0x28
tc class change dev eth1 classid 1:2 dsmark mask 0x3 value 0x48

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

(B) En r2:

```
tc qdisc add dev eth1 root handle 1:0 htb

tc class add dev eth1 parent 1:0 classid 1:1 htb rate 1Mbit
tc class add dev eth1 parent 1:1 classid 1:20 htb rate 100kbit ceil 1Mbit
tc class add dev eth1 parent 1:1 classid 1:30 htb rate 400kbit ceil 1Mbit

tc filter add dev eth1 parent 1:0 protocol ip prio 1 handle 0x0a tcindex classid 1:20
tc filter add dev eth1 parent 1:0 protocol ip prio 1 handle 0x12 tcindex classid 1:30
```

(C) En r2:

```
tc qdisc add dev eth1 handle 1:0 root dsmark indices 8

tc class change dev eth1 classid 1:20 dsmark mask 0x3 value 0x28
tc class change dev eth1 classid 1:30 dsmark mask 0x3 value 0x48

tc filter add dev eth1 parent 1:0 protocol ip prio 1 handle 0x0a tcindex classid 1:20
tc filter add dev eth1 parent 1:0 protocol ip prio 1 handle 0x12 tcindex classid 1:30
```

(D) El resto de las opciones no lo permiten.

4. Las cookies almacenadas por un cliente HTTP **en el día de hoy, 17-Jun-2016**, son las siguientes:

```
Cookie: Nif=123456789A
        Domain=www.server_one.com
        Path=/
        Expires=Tue Dec 31 23:12:40 2030

Cookie: Edad=23
        Domain=www.server_one.com
        Path=/dir_1/dir_2
        Expires=Tue Dec 31 23:12:40 2030

Cookie: Nombre=Luis
        Domain=www.server_two.com
        Path=/dir_1
        Expires=Tue Dec 30 23:12:40 2030

Cookie: DNI=0123456789A
        Domain=www.server_two.com
        Path=/
        Expires=Tue Dec 30 23:12:40 2030
```

A continuación dicho cliente hace una petición HTTP y como consecuencia envía únicamente la cookie: `Nif`.
Indica cuál de las siguientes afirmaciones es correcta:

(A) El cliente ha podido hacer la siguiente petición:

```
GET /dir_1/dir_3/dir_2/page_1.html HTTP/1.1
Host: www.server_one.com
```

(B) El cliente ha podido hacer la siguiente petición:

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

(C) El cliente ha podido hacer la siguiente petición:

```
GET /dir_1/dir_2/page_1.html HTTP/1.1
Host: www.server_one.com
```

(D) El resto de afirmaciones son falsas.

5. Un cliente HTTP envía la siguiente petición a un servidor HTTP:

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

Se sabe que la página pedida contiene 6 imágenes, 3 que están en el mismo servidor `www.server_one.com`, y otras 3 que están en el servidor `www.server_two.com`. Con este otro servidor el cliente se comunicará también usando HTTP/1.1 e incluirá también la cabecera `Connection: Close`.

Sabiendo que el cliente abre conexiones HTTP tan pronto como puede, indica cuál de las siguientes respuestas representa mejor el tiempo aproximado de carga de dicha página completa (el fichero html y las 6 imágenes):

(A) 6 RTT más el tiempo de transmisión de todos los recursos.

(B) 5 RTT más el tiempo de transmisión de todos los recursos.

(C) 4 RTT más el tiempo de transmisión de todos los recursos.

(D) 3 RTT más el tiempo de transmisión de todos los recursos.

6. Un cliente HTTP envía a las 08:00h GMT del día de hoy, 17-Jun-2016, la siguiente petición a un servidor final (no proxy) HTTP.

```
GET /dir_1/page_1.html HTTP/1.1
Host: www.server_one.com
```

Dicha petición no incluye ninguna cabecera opcional.

El servidor envía al cliente una respuesta cuyo comienzo es:

```
HTTP/1.1 200 Ok
Date: Tue, 17 Jun 2016 00:00:03 GMT
Last-Modified: Wed, 28 May 2014 18:41:28 GMT
Expires: Tue, 17 Jun 2016 12:00:00 GMT
Content-Type: text/html
Content-Length: 1202

...
```

Dicha página web no incluye recursos adicionales.

Se sabe que el cliente HTTP que hizo la petición tiene configurada una caché de contenidos suficientemente grande.

A las 09:00h GMT del día de hoy, 17-Jun-2016, un usuario utilizando dicho cliente introduce en la barra de dirección la siguiente URL:

```
http://www.server_one.com/dir_1/page_1.html
```

Indica cuál de las siguientes afirmaciones es correcta:

(A) El cliente no envía ninguna petición al servidor, mostrando al usuario directamente la página obtenida de su caché.

(B) El cliente envía la siguiente petición al servidor:

```
GET /dir_1/page_1.html HTTP/1.1
Host: www.server_one.com
If-modified-Since: Fri, 17 Jun 2016 08:00:03 GMT
```

(C) El cliente envía la siguiente petición al servidor:

```
GET /dir_1/page_1.html HTTP/1.1
Host: www.server_one.com
If-modified-Since: Wed, 28 May 2014 18:41:28 GMT
```

(D) El cliente envía la siguiente petición al servidor:

```
GET /dir_1/page_1.html HTTP/1.1
Host: www.server_one.com
If-modified-Since: Fri, 18 Jun 2016 09:00:00 GMT
```

CLAVES

Álex y Bárbara desean intercambiar mensajes de forma segura a través de una red. Para ello:

- Álex (utilizando criptografía de clave pública) genera en su ordenador una pareja de claves: K_A^+, K_A^-
- Bárbara (utilizando criptografía de clave pública) genera en su ordenador una pareja de claves: K_B^+, K_B^-
- Álex y Bárbara conocen una misma función Hash $H()$ que les permite calcular resúmenes criptográficos de mensajes.
- Álex y Bárbara tienen un enemigo común llamado Trudon

---

7. Un día en el que Álex y Bárbara se ven en persona:

   - Álex le da a Bárbara su K_A^+
   - Bárbara le da a Álex su K_B^+

   Días después, Bárbara recibe un mensaje, aparentemente enviado por Alex con el siguiente contenido:
   $\boxed{K_A^-(texto, K_B^+(H(texto))}$

   Indica cuál de las siguientes afirmaciones es correcta:

   (A) Trudon podría haber enviado ese mensaje.

   (B) Aunque Trudon no haya enviado ese mensaje, Trudon podría leerlo.

   (C) Aunque Trudon no haya enviado ese mensaje, Trudon podría alterar el texto sin que Bárbara se diera cuenta.

   (D) Aunque es seguro que Álex ha enviado ese mensaje, Bárbara no puede comprobarlo, ni tampoco puede leer el texto del mismo.

8. Álex y Bárbara nunca se han visto en persona, pero desean intercambiar mensajes seguros. Para ello, Álex y Bárbara intercambian la siguiente secuencia de mensajes a través de la red:

   - Bárbara recibe un mensaje aparentemente de Álex:
     `mensaje1 =` $\boxed{\text{“Soy Álex y ésta es mi clave pública: } K1\text{”}}$
   - Álex recibe un mensaje aparentemente de Bárbara:
     `mensaje2 =` $\boxed{\text{“Hola, Álex, soy Bárbara, gracias por tu clave pública, ésta es mi clave pública: } K2\text{”}}$
   - Bárbara recibe un mensaje aparentemente de Álex:
     `mensaje3 =` $\boxed{texto,\ K3(H(texto))}$

   (NOTA: se usa para las claves la notación $K1$, $K2$, $K3$, en vez de K_A^+, K_B^+, K_A^-, pues el objetivo de la pregunta es saber si estas claves son lo que parecen ser).

   Bárbara realiza la operación Hash del texto recibido en el tercer mensaje $H(texto)$ y obtiene el mismo resultado que al realizar la operación $K1(K3(H(texto)))$: $H(texto) = K1(K3(H(texto)))$

   Indica cuál de las siguientes afirmaciones es correcta:

   (A) Bárbara puede estar segura de que Álex ha escrito el `mensaje3` que ella ha recibido, pues $K1$ aplicada al resumen cifrado del texto ha dado el mismo resultado que al calcular el resumen al texto sin cifrar:
   $H(texto) = K1(K3(H(texto)))$

   (B) Bárbara puede estar segura de que Trudon no habrá podido leer el `mensaje3` que ella ha recibido.

   (C) Álex puede estar seguro de que el `mensaje2` que ha recibido procede de Bárbara, y no de Trudon.

   (D) Si Álex y Bárbara no se han visto en persona, necesitarían confiar ambos en una tercera persona con la que se hubieran visto en persona para que distribuyera las claves públicas.

9. Supón que, en un descuido de Álex, Trudon obtiene su clave privada K_A^-. Indica cuál de las siguientes afirmaciones es FALSA:

   (A) Trudon podría mandar mensajes a Bárbara como si procedieran de Álex, sin que Bárbara pudiera darse cuenta.

   (B) Trudon podría alterar el contenido de un mensaje enviado por Álex a Bárbara sin que Bárbara pudiera darse cuenta.

   (C) Trudon podría conocer el contenido de un mensaje cifrado enviado por Álex para Bárbara sin que Bárbara pudiera darse cuenta.

   (D) Trudon podría firmar digitalmente un mensaje en nombre de Álex sin que Bárbara pudiera darse cuenta.

IPTABLES

En la figura 2 se muestra la conexión de dos pequeñas empresas a Internet a través de un proveedor de servicios de Internet (ISP). Estas entidades quedan representadas en la figura de la siguiente forma:

- Empresa1: tiene las siguientes máquinas `e1-pc1` y `e1-pc2`, que pertenecen a una subred privada, `e1-pc3` y `e1-pc4`, que pertenecen a una zona DMZ, y el *router firewall* `e1-fw`.
- Empresa2: tiene las siguientes máquinas `e2-pc1`, `e2-pc2` que pertenecen a una subred privada y el *router firewall* `e2-fw`.
- ISP: tiene un único *router* `isp-r1`.
- Internet: tiene las siguientes máquinas `i-pc1`, `i-pc2` y los siguientes *routers* `i-r1` y `i-r2`.

Se supone que las máquinas `e1-fw` y `e2-fw` están funcionando como *firewalls* a los que se les ha configurado únicamente las siguientes reglas:

- Borrado de todas las reglas y reinicio de contadores
- Establecimiento de políticas por defecto para las cadenas de entrada y reenvío (`INPUT` y `FORWARD`) configuradas para **descartar** paquetes.
- Establecimiento de política por defecto para la cadena de salida (`OUPUT`) configurada para **aceptar** paquetes.

---

10. Partiendo de la configuración inicial, se establece en `e1-fw` el siguiente conjunto ordenado de reglas adicionales:

```
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to-source 20.0.1.1
iptables -t filter -A FORWARD -i eth2 -o eth0 -p udp -j DROP
iptables -t filter -A FORWARD -i eth2 -o eth0 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -p udp -j ACCEPT
```

Indica cuál de las siguientes afirmaciones es correcta:

(A) Cualquiera de los `pcs` de la Empresa1 puede ejecutar un cliente que puede comunicarse con cualquier servidor TCP o UDP en cualquier máquina de Internet.

(B) Cualquier máquina de Internet puede ejecutar un cliente TCP capaz de comunicarse con un servidor TCP en `e1-pc1`.

(C) Cualquier máquina de Internet puede ejecutar un `ping` para comprobar si está encendido `e1-fw`.

(D) El resto de afirmaciones son falsas.

11. Partiendo de la configuración inicial, se desea que `e2-fw` permita cumplir simultáneamente las siguientes reglas:

   a) Cualquier máquina de Internet puede acceder a un servidor UDP escuchando en el puerto 1000 de `e2-pc1`.

   b) Desde `e2-fw` se puede ejecutar un `ping` para comprobar si está encendida cualquier máquina de Internet.

   Indica cuál de los siguientes conjuntos de reglas se tienen que añadir en `e2-fw` para poder cumplir, simultáneamente:

(A)
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p udp --dport 1000 -j DNAT --to-destination 10.0.0.10:1000
iptables -t filter -A FORWARD -i eth0 -p udp --dport 1000 -j ACCEPT
iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -d 20.0.2.1 -p icmp -j ACCEPT
```

(B)
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p udp --dport 1000 -j DNAT --to-destination 10.0.0.10:1000
iptables -t filter -A FORWARD -i eth0 -d 10.0.0.10 -p udp --dport 1000 -j ACCEPT
iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A INPUT -i eth0 -p icmp -j ACCEPT
```

(C)
```
iptables -t nat -A POSTROUTING -i eth0 -d 20.0.2.1 -p udp --dport 1000 -j DNAT --to-destination 10.0.0.10:1000
iptables -t filter -A FORWARD -i eth0 -p udp --dport 1000 -j ACCEPT
iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A INPUT -i eth0 -p icmp -j ACCEPT
```

(D)
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p udp --dport 1000 -j DNAT --to-destination 10.0.0.10:1000
iptables -t filter -A FORWARD -i eth0 -d 20.0.2.1 -p udp --dport 1000 -j ACCEPT
iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A INPUT -i eth0 -p icmp -j ACCEPT
iptables -t filter -A OUTPUT -o eth0 -p icmp -j ACCEPT
```

12. Partiendo de la situación inicial,en un momento dado se ejectutan en e1-fw y e2-fw las siguientes órdenes, respectivamente:

```
e1-fw:~# cat /proc/net/ip_conntrack
tcp      6 431990 ESTABLISHED src=20.0.2.1 dst=20.0.0.40 sport=46162 dport=11000 packets=4 bytes=231 \
         src=20.0.0.40 dst=20.0.2.1 sport=11000 dport=46162 packets=3 bytes=164 [ASSURED] mark=0 use=1

e2-fw:~# cat /proc/net/ip_conntrack
tcp      6 431967 ESTABLISHED src=10.0.0.10 dst=20.0.0.40 sport=46162 dport=11000 packets=4 bytes=231 \
         src=20.0.0.40 dst=20.0.2.1 sport=11000 dport=46162 packets=3 bytes=164 [ASSURED] mark=0 use=1
```

Partiendo de la configuración inicial, indica cuál de los siguientes conjuntos de reglas se han tenido que añadir en e1-fw y e2-fw para que dichas comunicaciones hayan podido tener lugar:

(A) En e1-fw:

```
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --dport 11000 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -o eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Y en e2-fw:

```
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to-source 20.0.2.1
iptables -t filter -A FORWARD -o eth0 -p tcp -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

(B) En e1-fw:

```
iptables -t nat -A PREROUTING -d 20.0.1.1 -p tcp --dport 11000 -j DNAT --to-destination 20.0.0.40:11000
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --dport 11000 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -o eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Y en e2-fw:

```
iptables -t filter -A FORWARD -o eth0 -p tcp -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

(C) En e1-fw:

```
iptables -t nat -A PREROUTING -d 20.0.1.1 -p tcp --dport 11000 -j DNAT --to-destination 20.0.0.40:11000
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --dport 11000 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -o eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Y en e2-fw:

```
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to-source 20.0.2.1
iptables -t filter -A FORWARD -o eth0 -p tcp -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

(D) En e1-fw:

```
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --dport 11000 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -o eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Y en e2-fw:

```
iptables -t filter -A OUTPUT -o eth0 -p tcp -j ACCEPT
iptables -t filter -A INPUT -i eth0 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

IPv6

13. Carga el fichero de captura `/opt/stma/ipv6-1.cap` e indica cuál de las siguientes afirmaciones es correcta:

(A) El mensaje ha sido generado por un router para detectar si su dirección fe80::214:22ff:feaa:aa77 está duplicada en alguna otra máquina de la subred donde se envía.

(B) El mensaje ha sido generado por un router para responder a un mensaje ICMPv6 Echo Request.

(C) El mensaje ha sido generado por un router para anunciar el prefijo de red 2001:db8:300:300::/64 a todas las máquinas de la subred donde se envía.

(D) El mensaje ha sido generado por un router para responder a un mensaje *Neighbor Solicitation* y contiene la dirección Ethernet solicitada del router, 00:14:22:aa:aa:77 .

14. Carga el fichero de captura `/opt/stma/ipv6-2.cap` e indica cuál de las siguientes afirmaciones es correcta con respecto al mensaje de respuesta que provocará el mensaje que se observa en la captura:

(A) Un mensaje `Neighbor Advertisement` con direcciones IPv6:
`IP Origen= ff02::1:ffaa:aa11`
`IP Destino= 2001:db8:100:100:214:22ff:feaa:aa44`

(B) Un mensaje `Neighbor Advertisement` con direcciones IPv6:
`IP Origen= 2001:db8:100:100:214:22ff:feaa:aa11`
`IP Destino= 2001:db8:100:100:214:22ff:feaa:aa44`

(C) Un mensaje `Neighbor Advertisement` con direcciones IPv6:
`IP Origen= ::`
`IP Destino= 2001:db8:100:100:214:22ff:feaa:aa44`

(D) Ese mensaje mostrado en la captura no provoca ninguna respuesta. Es un mensaje que envía periódicamente un router para informar al resto de nodos de la subred de su dirección Ethernet 00:14:22:aa:aa:44.

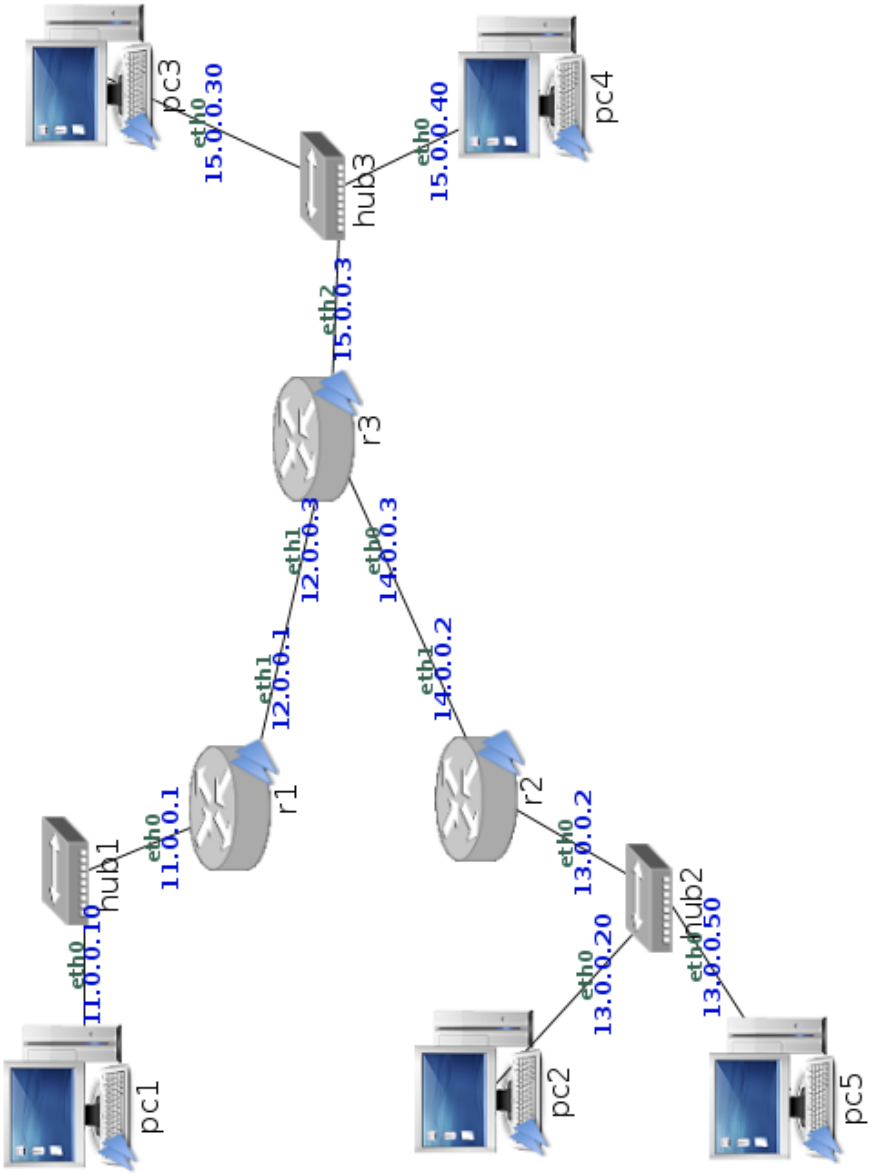


Figura 1: Calidad de servicio

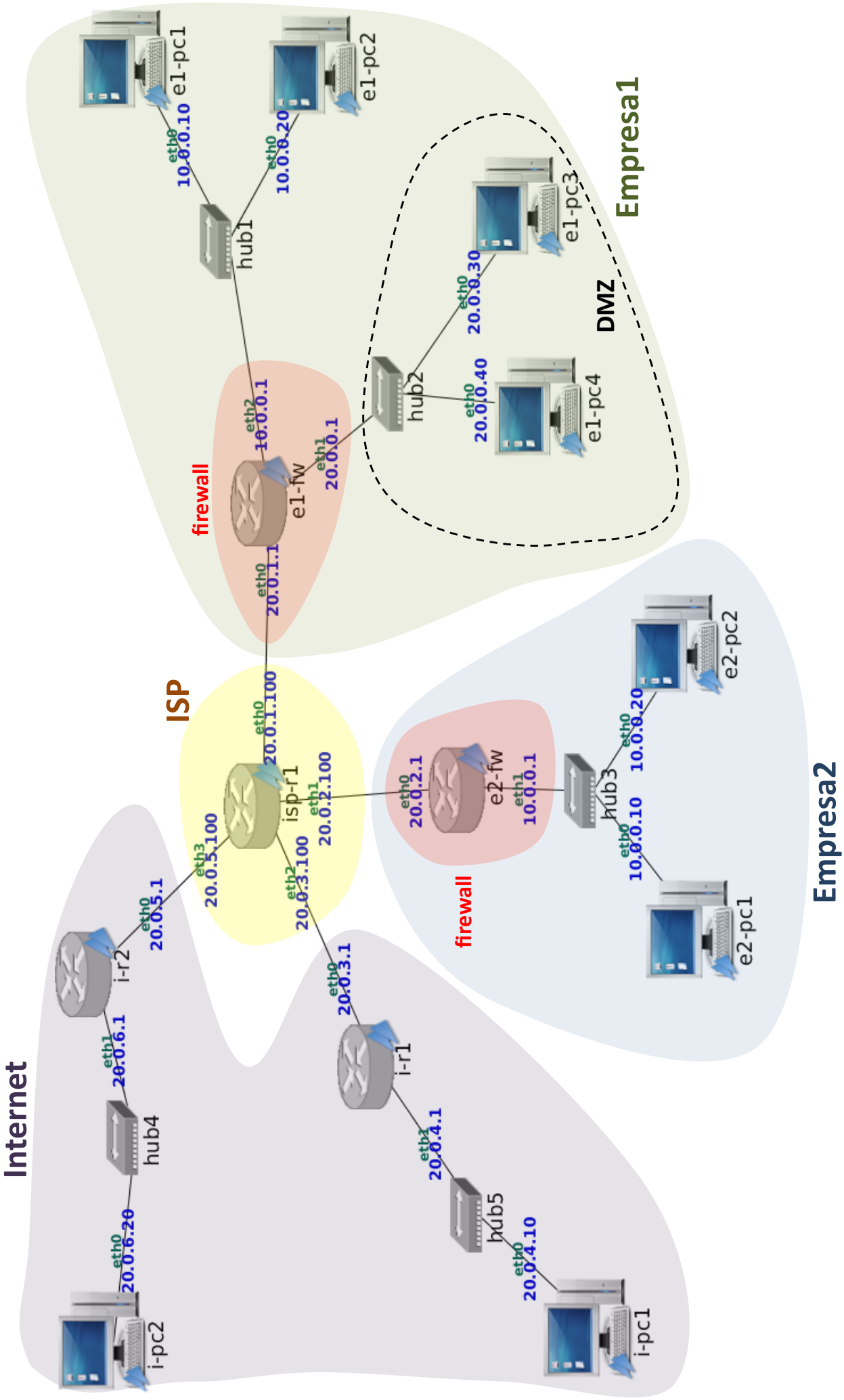


Figura 2: Seguridad