Examen Parcial II de Sistemas Telemáticos para Medios Audiovisuales

GSyC, Universidad Rey Juan Carlos

22 de diciembre de 2015

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 1Mbps

   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 700kbit 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 3 segundos más, este tráfico estaba encolado en `r3` procedente de `pc2` y `pc5`.

   (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 13 segundos más, este tráfico estaba encolado en `r3` procedente de `pc2` y `pc5`.

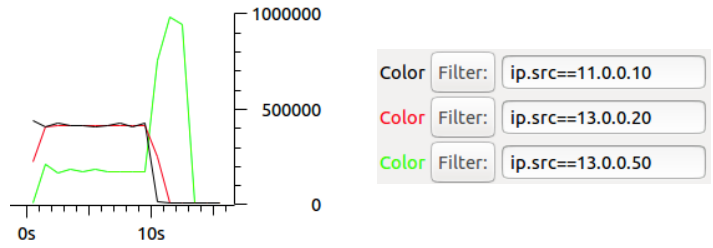
2. Partiendo de la situación inicial del escenario se configuran en `r3(eth2)` unas disciplinas de cola de salida que limiten el tráfico de salida a 1Mbit, con latencia=50s, y que den prioridad al tráfico según su dirección IP origen (de más prioridad a menos prioridad): tráfico de `pc1` (más prioritario), 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:

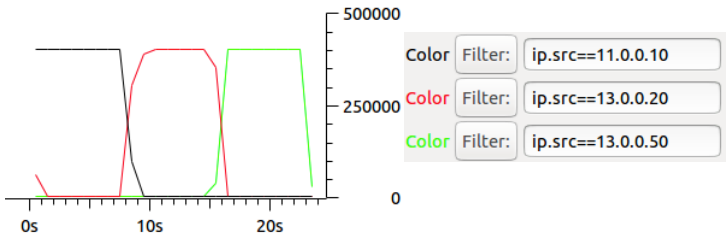
   - `pc1` envía a `pc3` a 400kbps.
   - `pc2` envía a `pc4` a 400kbps.
   - `pc5` envía a `pc4` a 400kbps.

   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):

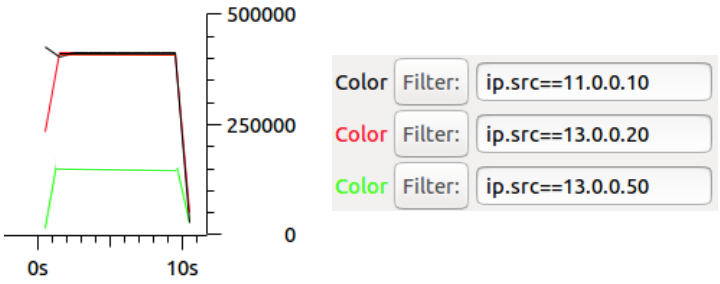
   (A) Gráfica 1.



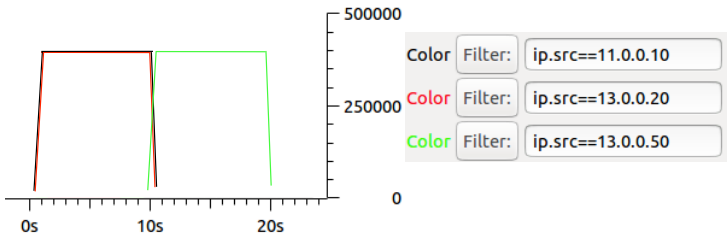
   (B) Gráfica 2.



   (C) Gráfica 3.



   (D) Gráfica 4.



3. Se sabe que `r1` y `r2` han realizado marcas en el campo DSCP de la cabecera IP de los paquetes con valores AF11 y AF21. En `r3` se desea limitar el tráfico de salida a 1Mbit garantizando las siguientes tasas de salida:

   - 400kbps para los paquetes que vengan marcados con AF11, pudiendo usar hasta un máximo de 1Mbps.
   - 600kbps para los paquetes que vengan marcados con AF21, pudiendo usar hasta un máximo de 1Mbps.

   Indica, cuál de las siguientes opciones permite garantizar esta configuración:

   (A)
   ```
   tc qdisc add dev eth2 handle 1:0 root dsmark indices 8

   tc class add dev eth2 classid 1:1 dsmark mask 0x3 value 0x28
   tc class add dev eth2 classid 1:2 dsmark mask 0x3 value 0x48

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

   (B)
   ```
   tc qdisc add dev eth2 root handle 1:0 htb

   tc class add dev eth2 parent 1:0 classid 1:1 htb rate 1Mbit
   tc class add dev eth2 parent 1:1 classid 1:20 htb rate 400kbit ceil 1Mbit
   tc class add dev eth2 parent 1:1 classid 1:30 htb rate 600kbit ceil 1Mbit

   tc filter add dev eth2 parent 1:0 protocol ip prio 1 handle 0x0a tcindex flowid 1:30
   tc filter add dev eth2 parent 1:0 protocol ip prio 1 handle 0x12 tcindex flowid 1:30
   ```

   (C)
   ```
   tc qdisc add dev eth2  handle 1:0 root dsmark indices 8 set_tc_index
   tc filter add dev eth2 parent 1:0 protocol ip prio 1 tcindex mask 0xfc shift 2

   tc qdisc add dev eth2 parent 1:0  handle 2:0 htb

   tc class add dev eth2 parent 2:0 classid 2:1 htb rate 1Mbit
   tc class add dev eth2 parent 2:1 classid 2:20 htb rate 400kbit ceil 1Mbit
   tc class add dev eth2 parent 2:1 classid 2:30 htb rate 600kbit ceil 1Mbit

   tc filter add dev eth2 parent 2:0 protocol ip prio 1 handle 0x0a tcindex flowid 2:20
   tc filter add dev eth2 parent 2:0 protocol ip prio 1 handle 0x12 tcindex flowid 2:30
   ```

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

HTTP

4. Las cookies almacenadas por un cliente HTTP **en el día de hoy, 22-Dic-2015**, son las siguientes:

```
Cookie: Nif=123456789A
        Domain=www.server_one.com
        Path=/
        Expires=Tue Nov 30 23:12:40 2015

Cookie: Edad=23
        Domain=www.server_two.com
        Path=/
        Expires=Tue Dec 31 23:12:40 2015

Cookie: Nombre=Luis
        Domain=www.server_two.com
        Path=/dir_1
        Expires=Tue Nov 30 23:12:40 2015
```

A continuación dicho cliente hace la siguiente petición HTTP:

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

Indica cuál de las siguientes afirmaciones es correcta:

(A) El cliente envíará las siguientes cabeceras:

```
If Modidified-Since: Tue Nov 30 23:12:40 2015
Cookie: Nif=123456789A
```

(B) El cliente enviará la siguiente cabecera:

```
Cookie: Nif=123456789A
```

(C) El cliente enviará la siguiente cabecera:

```
Cookie: Edad=23
```

(D) El cliente no enviará ninguna cabecera `Cookie`

5. 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 6 imágenes, 2 que están en el mismo servidor `www.server_one.com`, otras 2 que están el servidor `www.server_two.com`, y otras 2 que están en el servidor `www.server_three.com`. Con los otros dos servidores el cliente se comunicará también usando HTTP/1.1 sin incluir ninguna cabecera `Connection`.

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) 10 RTT más el tipo de transmisión de todos los recursos.

(B) 6 RTT más el tipo de transmisión de todos los recursos.

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

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

6. Un cliente HTTP envía a las 0:00h GMT del día de hoy, 22-Dic-2015, 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, 22 Dic 2015 00:00:03 gmailT
Last-Modified: Wed, 28 May 2014 18:41:28 GMT
Expires: Tue, 22 Dic 2015 04:00:00 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 9:00h GMT del día de hoy, 22-Dic-2015, 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: Tue, 22 Dic 2015 00:00:03 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: Tue, 22 Dic 2015 04:00:00 GMT
```

SEGURIDAD

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 amigo común llamado César
- Álex y Bárbara tienen un enemigo común llmado 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^+
   - Trudon aprovecha una distracción de ambos para, sin que Álex y Bárbara se den cuenta, hacerse con sus claves públicas: K_A^+ y K_B^+

   Días después, Trudon intercepta un mensaje enviado por Álex a Bárbara con el siguiente contenido: $\boxed{texto, K_A^-(H(texto))}$

   Indica cuál de las siguientes afirmaciones es correcta:

   (A) Trudon puede estar seguro que el mensaje proviene de Álex.
   (B) Trudon puede estar seguro de que el mensaje es para Bárbara.
   (C) Trudon puede modificar el texto del mensaje que envía Álex sin que Bárbara se dé cuenta.
   (D) Trudon puede, sin tocar el texto del mensaje, hacer creer a Bárbara que el mensaje proviene en realidad de César.

8. Álex y Bárbara, después de generar sus claves, pero antes de poder verse en persona, desean intercambiar mensajes de forma que ambos puedan estar seguros que los mensajes que envía el otro provienen realmente de él.

   Indica cuál de las siguientes afirmaciones es correcta:

   (A)
   - Álex se dirige a la Autoridad Certificadora CA1, y consigue un certificado de su clave pública, $K_{CA1}^-(K_A^+)$, y allí consigue de forma segura la clave pública de CA1: K_{CA1}^+
   - Bárbara se dirige a la Autoridad Certificadora CA2, y consigue un certificado de su clave pública, $K_{CA2}^-(K_B^+)$, y allí consigue de forma segura la clave pública de CA2: K_{CA2}^+
   - Álex envía a Bárbara: $K_{CA1}^-(K_A^+)$
   - Álex envía a Bárbara $\boxed{texto, K_A^-(H(texto))}$, y Bárbara puede estar segura de que ese mensaje proviene a Álex.

   (B)
   - Álex genera al azar una clave de sesión simétrica: K_S
   - Álex envía a Bárbara: $K_B^+(K_S)$
   - Álex envía a Bárbara $\boxed{texto, K_A^-(K_S(H(texto)))}$, y Bárbara puede estar segura de que ese mensaje proviene a Álex.

   (C)
   - Álex genera al azar una clave de sesión simétrica: K_S
   - Álex envía a Bárbara: $K_A^-(K_S)$
   - Álex envía a Bárbara $\boxed{K_S(texto, K_A^-(H(texto)))}$, y Bárbara puede estar segura de que ese mensaje proviene a Álex.

   (D) El resto de afirmaciones son falsas

9. Álex y Bárbara, antes siquiera de concerse entre ellos, tienen como amigo común a César, que también tiene una pareja de claves: K_C^+, K_C^-. Además:

   - Álex y César han coindidido en persona, por lo que ambos tiene la clave pública del otro
   - Bárbara y César han coindicido en persona, por lo que ambos tiene la clave pública del otro.

   Antes de que Álex y Bárbara se vean en persona, desean intercambiarse mensajes de forma segura pese a que Trudon pudiera interceptarlos. Se les ocurre el siguiente procedimiento:

   - Cuando Álex quiere enviar un mensaje a Bárbara, le envía a César lo siguiente: $\boxed{K_C^+(texto, H(texto))}$
   - César descifra el mensaje, y envía a Bárbara lo siguiente: $\boxed{K_B^+(texto, H(texto))}$

   Tanto Álex como Bárbara están seguros de que César no hará nada para engañarlos, pero temen que algunos de los mensajes sean interceptados y/o modificados por Trudon.

   Indica cuál de las siguientes afirmaciones es correcta:

   (A) Este procedimiento permite a Bárbara estar segura de que el mensaje que recibe contiene el mensaje original de Álex.

   (B) Este procedimiento permite a Álex estar seguro de que Trudon no podrá conocer el texto de su mensaje.

   (C) Este procedimiento permite a César estar seguro de que el mensaje que recibe contiene el mensaje original de Álex.

   (D) El resto de afirmaciones son falsas.

IPTABLES

ATENCIÓN:

- **Si ya has usado NetGUI con otro diagrama de red, cierra NetGUI y ejecuta** `clean-netgui.sh` **antes de volver a lanzar NetGUI.**
- **En NetGUI, en el menú "Archivo" elige la opción "Abrir" y carga el nombre de archivo** `/opt/stma/seg`**.**
- **Se cargará el escenario mostrado en la figura 2.**
- **NO ARRANQUES NINGUNA MÁQUINA. Es importante que las arranques en el orden indicado.**
- **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/seg/reset-lab`**.**

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`.

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

- Políticas por defecto para las cadenas de entrada y reenvío (`INPUT` y `FORWARD`) configuradas para **descartar** paquetes.
- Política por defecto para la cadena de salida (`OUPUT`) configurada para **aceptar** paquetes.

Al arrancar el *router* `e1-fw` ha ejecutado el *script* `/bin/fw1.sh` y al arrancar el *router* `e2-fw` ha ejecutado el *script* `/bin/fw2.sh`. Estos *scripts* aplican las reglas descritas previamente.

---

10. Se desea conseguir en la Empresa1 una configuración que cumpla, simultáneamente:

    a) `e1-pc3` debe puede comunicarse con cualquier servidor TCP instalado en cualquier máquina de Internet

    b) `e1-pc3` NO debe puede comunicarse con ningún servidor UDP instalado en cualquier máquina de Internet

    c) `e1-pc4` sólo debe poder comunicarse con servidores HTTP (servidores de TCP en el puerto 80) de Internet, no debe poder comunicarse con ningún otro tipo de servidor TCP ni UDP de Internet.

    d) Ninguna máquina de Internet debe poder comunicarse con ningún servidor TCP ni UDP de la Empresa1.

    Partiendo de la configuración inicial, indica cuál de los siguientes conjuntos de reglas en `e1-fw` lo permite:

    (A)
    ```
    iptables -t filter -A FORWARD -s 20.0.0.30 -p tcp -j ACCEPT
    iptables -t filter -A FORWARD -s 20.0.0.30 -p udp -j DROP
    iptables -t filter -A FORWARD -s 20.0.0.40 -p tcp --dport 80 -j ACCEPT
    iptables -t filter -A FORWARD -i eth0 -p tcp -j DROP
    iptables -t filter -A FORWARD -i eth0 -p udp -j DROP
    iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
    ```

    (B)
    ```
    iptables -t filter -A FORWARD -s 20.0.0.30 -p tcp -j ACCEPT
    iptables -t filter -A FORWARD -s 20.0.0.40 -p tcp --dport 80 -j ACCEPT
    iptables -t filter -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
    ```

    (C)
    ```
    iptables -t filter -A FORWARD -s 20.0.0.30 -p tcp -j ACCEPT
    iptables -t filter -A FORWARD -s 20.0.0.40 -p tcp --dport 80 -j ACCEPT
    iptables -t filter -A FORWARD -i eth0 -p tcp -j DROP
    iptables -t filter -A FORWARD -i eth0 -p udp -j DROP
    ```

    (D)
    ```
    iptables -t filter -A FORWARD -s 20.0.0.30 -p tcp -j ACCEPT
    iptables -t filter -A FORWARD -s 20.0.0.30 -p udp -j DROP
    iptables -t filter -A FORWARD -s 20.0.0.40 -p tcp --dport 80 -j ACCEPT
    iptables -t filter -A FORWARD -i eth0 -j DROP
    iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
    ```

11. Partiendo de la situación inicial, se ha realizado una configuración adicional en `e1-fw` para permitir las siguientes comunicaciones:

```
e1-fw:~# cat /proc/net/ip_conntrack
udp      17 178 src=20.0.4.10 dst=20.0.0.40 sport=8000 dport=7000 packets=2 bytes=70 \
         src=20.0.0.40 dst=20.0.4.10 sport=7000 dport=8000 packets=2 bytes=69 [ASSURED] mark=0 use=1
udp      17 159 src=20.0.6.20 dst=20.0.0.30 sport=7000 dport=8000 packets=5 bytes=169 \
         src=20.0.0.30 dst=20.0.6.20 sport=8000 dport=7000 packets=3 bytes=105 [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` para que dichas comunicaciones hayan podido tener lugar:

(A)
```
iptables -t filter -A FORWARD -i eth0 -d 20.0.0.30  -p udp --sport 7000 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -s 20.0.4.10 -p udp --dport 7000 -j ACCEPT
iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

(B)
```
iptables -t filter -A INPUT -i eth0 -p udp --dport 8000 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -s 20.0.4.10 -p udp --dport 7000 -j ACCEPT
iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

(C)
```
iptables -t filter -A FORWARD -o eth0 -d 20.0.0.30  -p udp --dport 8000 -j ACCEPT
iptables -t filter -A FORWARD -o eth0 -s 20.0.4.10 -p udp --sport 7000 -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

(D) No hay ninguna configuración de `iptables` capaz de permitir dichas comunicaciones en un *firewall*, es necesario desactivar por completo el *firewall* de `e1-fw` para que dichas comunicaciones hayan podido tener lugar.

12. En la máquina `e1-pc1` se arranca un servidor TCP esperando recibir mensajes en el puerto 9000.

Partiendo de la configuración inicial, indica cuál de los siguientes conjuntos de reglas en `e1-fw` permite que un cliente TCP en cualquier máquina de Internet se comunique con dicho servidor:

(A)
```
iptables -t filter -A FORWARD -i eth0 -d 10.0.0.10 -p tcp --dport 9000 -j ACCEPT
iptables -t filter -A FORWARD -i eth2 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t nat -A PREROUTING -i eth0 -d 20.0.1.1 -p tcp --dport 9000 -j DNAT --to-destination 10.0.0.10
```

(B)
```
iptables -t filter -A FORWARD -i eth0 -d 20.0.1.1 -p tcp --dport 9000 -j ACCEPT
iptables -t filter -A FORWARD -i eth2 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

(C)
```
iptables -t filter -A FORWARD -i eth0 -d 20.0.1.1 -p tcp --dport 9000 -j ACCEPT
iptables -t filter -A FORWARD -i eth2 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t nat -A PREROUTING -i eth0 -d 20.0.1.1 -p tcp --dport 9000 -j DNAT --to-destination 10.0.0.10
```

(D)
```
iptables -t nat -A PREROUTING -i eth0 -o eth2 -d 20.0.1.1 -p tcp --dport 9000 -j DNAT --to-destination 10.0.0.10
iptables -t filter -A FORWARD -i eth2 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

13. Analiza el contenido de la captura `ipv6-1.cap`. Indica qué ocurrirá justo después de capturar esos paquetes:

    (A) La máquina 2001:db8:300:300:214:22ff:feaa:aa77 fragmentará el paquete 1 debido a que el paquete número 1 es demasiado grande para ser transmitido por el nivel de enlace de un router intermedio.

    (B) No se producirá ningún paquete más relacionado con la comunicación que se muestra en el fichero de captura.

    (C) La máquina 2001:db8:300:300:214:22ff:feaa:aa88 fragmentará el paquete 1 debido a que el paquete número 1 es demasiado grande para ser transmitido por el nivel de enlace de un router intermedio.

    (D) La máquina 2001:db8:100:100:214:22ff:feaa:aa11 enviará la respuesta ICMPv6 Echo Reply a 2001:db8:300:300:214:22ff:feaa:aa88 en varios paquetes IP resultado de realizar fragmentación tal y como indica el paquete número 2.

14. Se ha realizado la captura `ipv6-2.cap` en una determinada subred. Indica qué ocurrirá en una máquina cuya dirección Ethernet es 00:14:22:aa:aa:dd cuando reciba dicho paquete:

    (A) La máquina configurará la dirección IPv6 fe80::214:22ff:feaa:aadd/64.

    (B) La máquina configurará la dirección IPv6 2001:db8:500:500:214:22ff:feaa:aadd/64.

    (C) La máquina configurará una dirección IPv6 global, pero es necesaria más información para saber exactamente cuál será dicha dirección IPv6.

    (D) La máquina no realizará ninguna configuración pues ese paquete no va dirigido a ella.

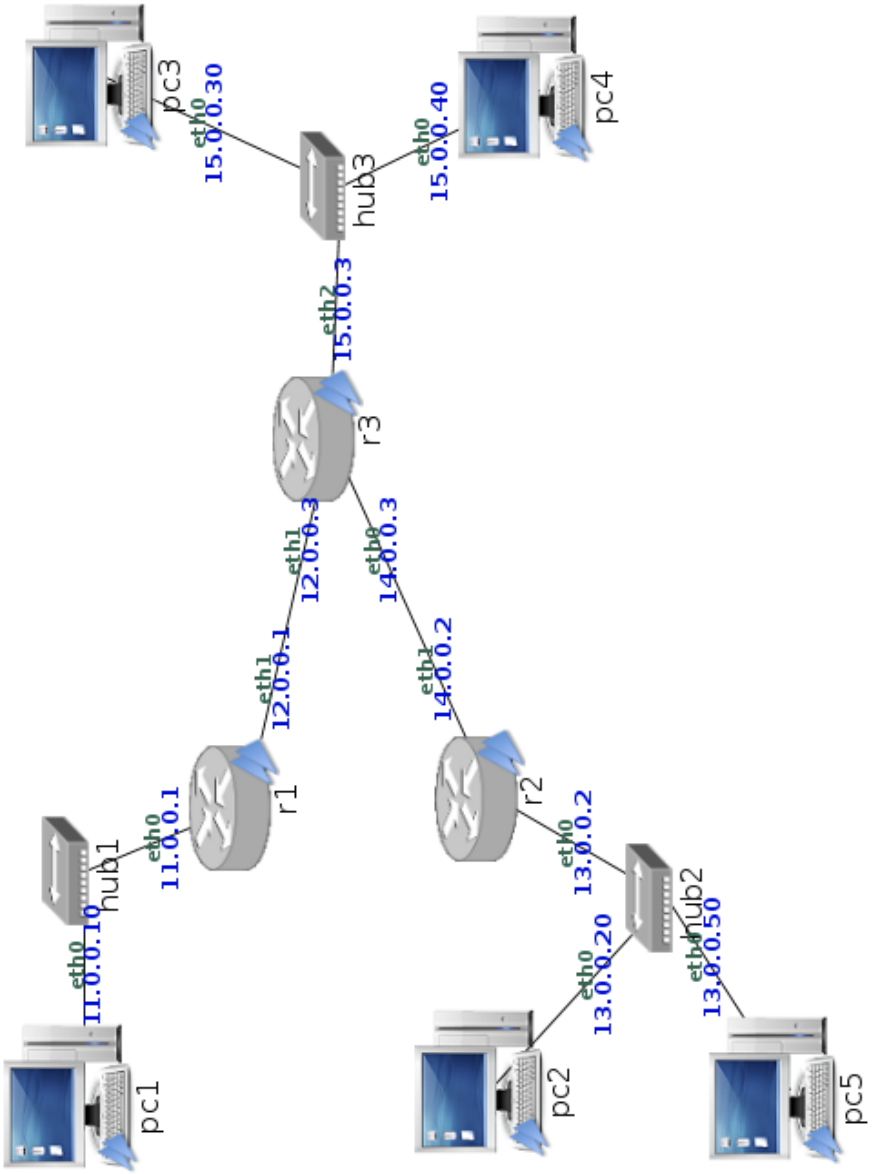


Figura 1: Calidad de servicio

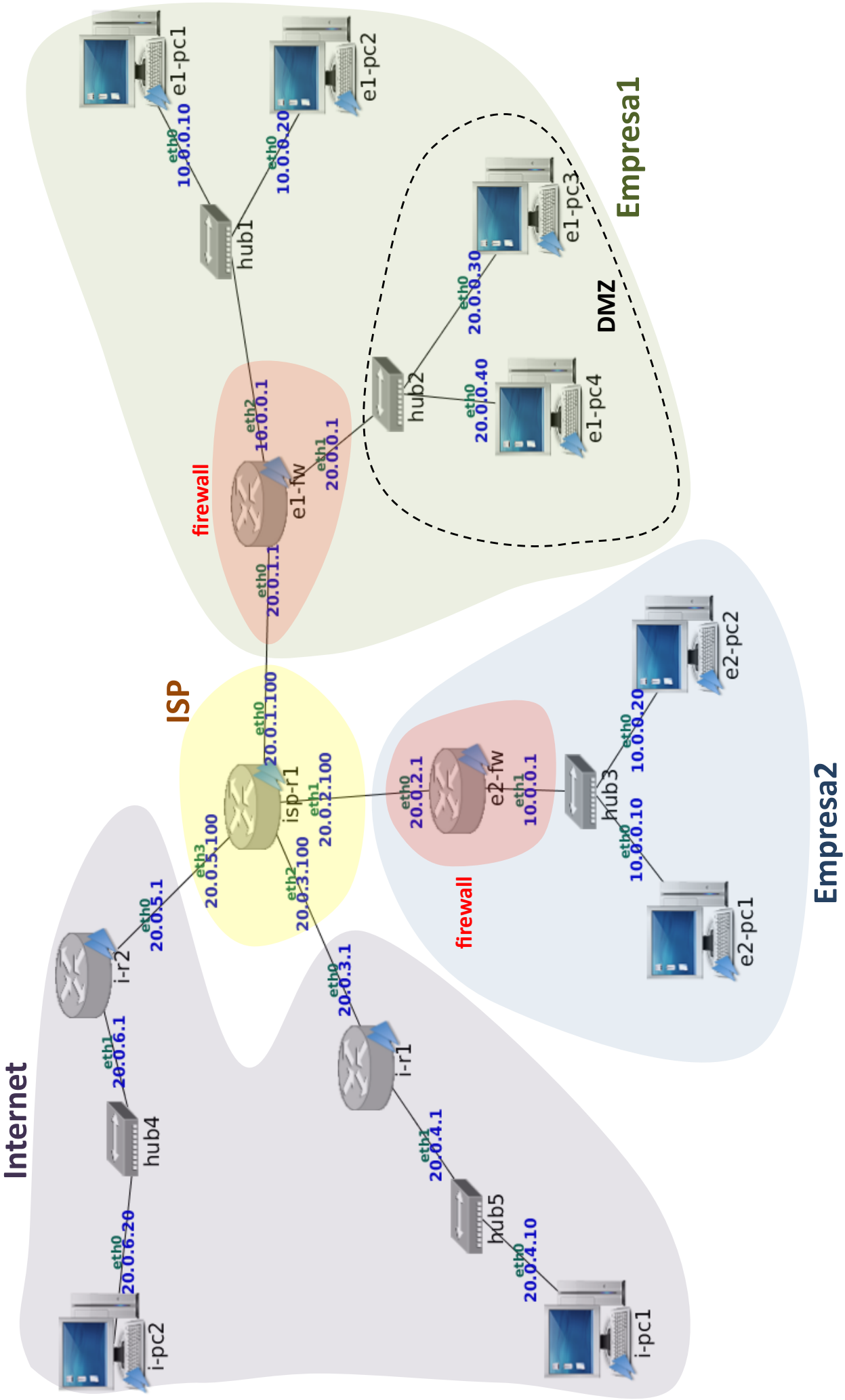


Figura 2: Seguridad