**Material docente en abierto de la Universidad Rey Juan Carlos**

# Proyectos de prácticas y Pruebas de evaluación

Asignatura: Sistemas Telemáticos

2º Grado en Ingeniería Telemática
2º Grado en Tecnologías de la Telecomunicación
2º Grado en Sistemas de Telecomunicación

Material disponible en BURJC Digital: https://burjcdigital.urjc.es

Curso 2023-24

Eva M. Castro Barbero (eva.castro@urjc.es)
José Centeno González (jose.centeno@urjc.es)
Pedro de las Heras Quirós (pedro.delasheras@urjc.es)

Universidad Rey Juan Carlos

# Contenido

Sistemas Telemáticos

# Práctica 1 (1ª parte): Dispositivos de Interconexión

GSyC
Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación

Diciembre de 2023

Antes de comenzar a realizar la práctica, deberás acceder a la **carpeta con tu nombre y apellidos que los profesores hemos compartido a través de OneDrive** y crear un nuevo documento de Word llamado: memoria-p1.docx

Usarás este documento para ir escribiendo en el mismo el trabajo que vayas realizando en esta práctica. Como es un documento compartido con los profesores, nosotros podremos ir revisando de forma gradual tu trabajo. Es obligatorio ir escribiendo los resultados de vuestra práctica según la vayáis realizando en este documento. Por favor, **no uséis ningún otro documento de forma temporal para ir escribiendo vuestros resultados**.

**Las capturas de tráfico** que vayáis realizando por favor, **no las subáis a esta carpeta compartida**. La carpeta sólo contendrá las memorias de las prácticas que realicéis durante el curso. Al terminar la práctica te indicaremos como entregar tanto la memoria como las capturas de tráfico que hayas realizado.

Para esta práctica, cada alumno tendrá escenarios diferentes en cada apartado. En particular, las direcciones IP de las máquinas tendrán asignado en el segundo byte un valor X distinto. Podrás ver qué valor X tienes asignado cuando cargues el escenario en NetGUI y observes la configuración.

Descarga tus escenarios del siguiente enlace donde deberás introducir tu número de DNI (8 dígitos) con la letra correspondiente:

`https://mobiquo.gsyc.es/practicas/st/p1.html`

## 1. Funcionamiento de hubs y switch

En el fichero `lab-hub-switch.tgz` está definida una red como la de la figura 1. Descomprime el fichero (con `tar -xvzf lab-hub-switch.tgz`), arranca NetGUI y abre el escenario.

**No arranques aún s1**.

Arranca el resto de las máquinas de una en una.

Deja por ahora sin arrancar el *switch* `s1`. Cada uno de los *hubs* estará aislado de los demás. Por lo tanto sólo habrá conectividad entre los ordenadores que están conectados al mismo *hub*. Las tramas Ethernet no pueden salir del *hub* en el que aparecen.

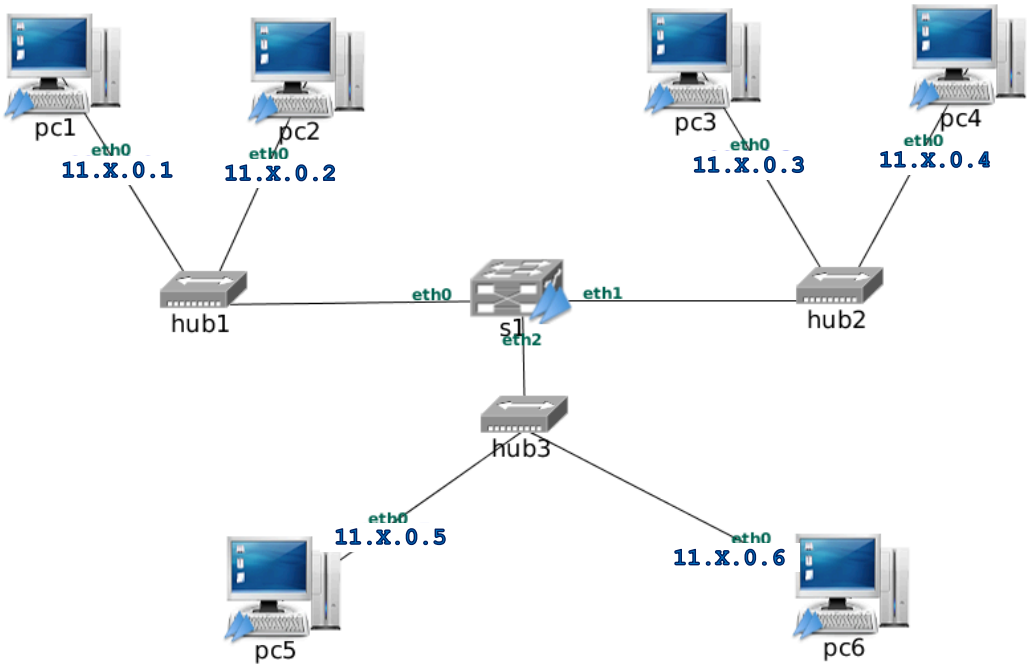



Figura 1: Escenario de hubs y switch

## 1.1. Comunicación entre máquinas con s1 apagado

NOTA: Las capturas a realizar en este apartado no es necesario redirigirlas a un fichero para estudiarlas con `wireshark`. Basta con ver la salida de `tpcdump` directamente en el terminal de cada máquina virtual, escribiendo: `tcpdump -i eth0`.

1. Piensa en qué paquetes se capturarán en `pc2`, `pc3` y en `pc5` si se hace un `ping` desde `pc1` a `pc2`.
2. Lanza `tcpdump` en `pc2`, `pc3` en `pc5`. A continuación ejecuta la siguiente orden en `pc1` para hacer un `ping` a `pc2`[1]:

   ```
   pc1:~# ping -c 3 11.X.0.2
   ```

   (`-c 3` hace que el `ping` sólo envíe 3 paquetes ICMP)

   Observa el tráfico capturado en `pc2`, `pc3` y `pc5` y comprueba si ha ocurrido lo que pensabas. Copia en la memoria lo que muestra `tcpdump` en cada una de las máquinas.
3. Comprueba que no existe conectividad (es decir, que no puede hacerse `ping`) entre máquinas que estén en diferentes *hubs*.

## 1.2. Comunicación entre máquinas con s1 arrancado

1. Arranca el *switch* `s1`.
2. Piensa en qué paquetes se capturarán ahora en `pc2`, `pc3` y en `pc5` repitiendo el mismo `ping`
3. Comprueba la caché de ARP en `pc1`. Si aún está en ella la dirección Ethernet de `pc2` borra esa entrada de la caché de ARP.
4. Lanza `tcpdump` en `pc2` (guarda la captura en un fichero `hub-switch-01.cap`), `pc3` (guarda la captura en un fichero `hub-switch-02.cap`) y en `pc5` (guarda la captura en un fichero `hub-switch-03.cap`). A continuación vuelve a hacer en `pc1` el `ping` a `pc2`:

   ```
   pc1:~# ping -c 3 11.X.0.2
   ```

[1] Fíjate en el valor que tienes asignado en tu escenario a X para ejecutar correctamente el comando

Interrumpe las capturas y observa el tráfico capturado en `pc2`, `pc3` y `pc5` y comprueba si ha ocurrido lo que pensabas.

5. Responde a estas preguntas:
   - ¿Por qué llega a `pc3` y a `pc5` la solicitud de ARP enviada por `pc1`?
   - ¿Por qué NO llega a `pc3` y a `pc5` la respuesta de ARP enviada por `pc2`?
   - ¿Por qué NO llega a `pc3` y a `pc5` el *ICMP echo request* enviado por `pc1`?
   - ¿Por qué NO llega a `pc3` y a `pc5` el *ICMP echo reply* enviado por `pc2`?
6. Comprueba las direcciones Ethernet que tiene cada interfaz de cada máquina de la figura (usando `ifconfig`), y apúntalas en la memoria.
7. Mira la tabla de direcciones aprendidas por el *switch* `s1` utilizando la orden `brctl showmacs s1`. Puedes utilizarla junto con la orden `watch` para observar periódicamente los cambios en las direcciones aprendidas:

   ```
   s1:~# watch brctl showmacs s1
   ```

   (`watch` repite cada 2 segundos la ejecución de la orden que se le pasa como parámetro)

   Identifica las máquinas a las que pertenece cada dirección Ethernet y explica su presencia en la tabla de direcciones aprendidas de `s1`.

   Tras 300 segundos comprobarás que el *switch* olvida las direcciones aprendidas (mira cómo va creciendo el valor de la columna *ageing timer*, contador de envejecimiento, en la salida de la orden). Comprueba también cómo el *ageing timer* de una dirección Ethernet se reinicializa cada vez que el *switch* ve una nueva trama con esa dirección Ethernet.
8. Lanza `tcpdump` en `pc2` (guarda la captura en un fichero `hub-switch-04.cap`), en `pc3` (guarda la captura en un fichero `hub-switch-05.cap`) y en `pc5` (guarda la captura en un fichero `hub-switch-06.cap`). A continuación ejecuta en `pc1` el `ping` a `pc6`:

   ```
   pc1:~# ping -c 3 11.X.0.6
   ```

   Interrumpe las capturas y observa el tráfico capturado en `pc2`, `pc3` y `pc5` y comprueba si ha ocurrido lo que pensabas.
9. Responde a estas preguntas:
   - ¿Por qué NO llegan a `pc3` y a `pc4` los mensajes *ICMP echo request* e *ICMP echo reply*?
   - ¿Por qué SÍ llegan a `pc2` y a `pc5` todos los mensajes enviados por `pc1` y `pc6`?
   - ¿Crees que si cambiamos todos los hubs de la figura por switches, los mensajes capturados anteriormente serían los mismos?
10. Comprueba que ahora sí existe conectividad entre todas las máquinas de la figura utilizando la orden `ping`.

## 2. Redes conectadas a través de switch y router

En el fichero `lab-switch-router.tgz` está definida una red como la que aparece en la figura 2. Descomprime el fichero, lanza NetGUI y abre el escenario. Arranca todas las máquinas: pcs, routers y switches.

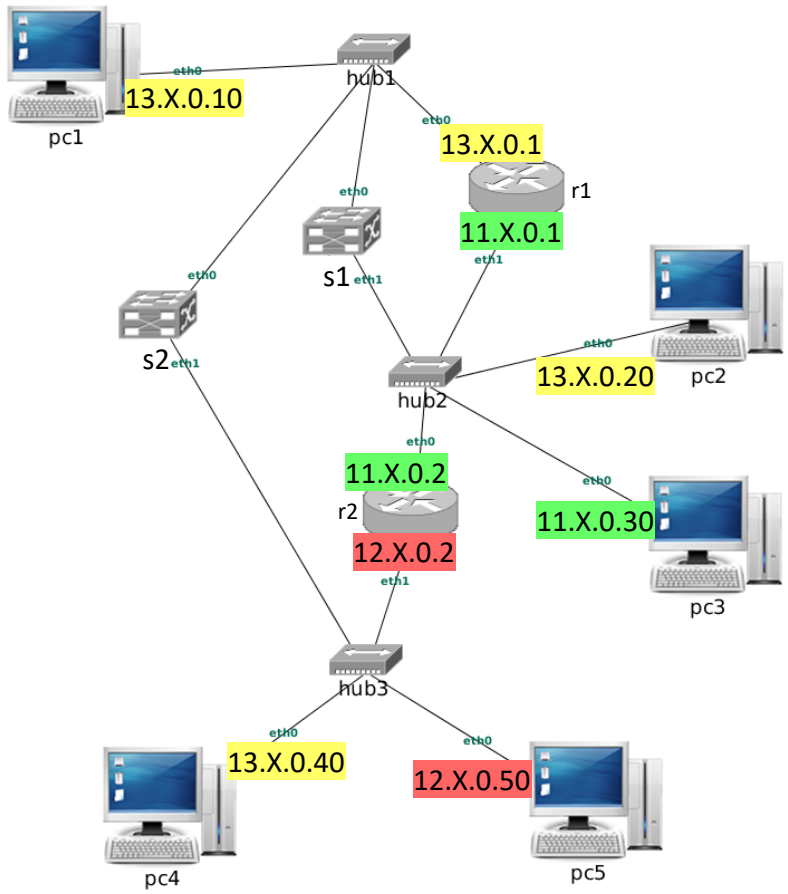



Figura 2: Escenario de redes conectadas por *switches* y *routers*

### 2.1. Comunicación entre pc2 y pc4

Con las cachés de ARP vacías y las tablas de direcciones aprendidas de los switches vacías se desea realizar un `ping` de `pc2` a `pc4`:

1. Observa la configuración que hay en el escenario para que `pc2` y `pc4` puedan intercambiar tráfico. ¿Cuál de los siguientes caminos crees que seguirán los mensajes ICMP echo request desde `pc2` a `pc4`?

   - `pc2` → `s1` → `s2` → `pc4`
   - `pc2` → `r1` → `s2` → `pc4`
   - `pc2` → `r2` → `pc4`

   Justifica la respuesta.

2. Indica cuántas solicitudes y respuestas de ARP serían necesarias para que dicho ping funcionase. Explica en qué pcs/routers/switches y su interfaz `eth` concreta se podrían capturar:

   - solicitud/es de ARP.
   - respuesta/s de ARP.

3. Para ver todo el tráfico generado deberás lanzar un `tcpdump` por cada `hub` de la figura. Justifica la respuesta.

4. Lanza `tcpdump` en las máquinas `pc1` (`switch-router-01.cap`), `pc3` (`switch-router-02.cap`) y `pc5` (`switch-router-03.cap`) para ayudarte a comprobar tus suposiciones [2].

5. Indica qué direcciones Ethernet habrán aprendido `s1` y `s2` después de ejecutar el `ping` y explica qué mensajes han generado dicho aprendizaje. Compruébalo.

6. ¿Crees que habrá llegado alguno de los mensajes ICMP echo request a `pc1`, `pc3` o `pc5`? Justifica la respuesta.

## 2.2. Comunicación entre pc1 y pc3

Con las cachés de ARP vacías y las tablas de direcciones aprendidas de los switches vacías se desea realizar un `ping` de `pc1` a `pc3`:

1. Observa la configuración que hay en el escenario para que `pc1` y `pc3` puedan intercambiar tráfico. ¿Cuál de los siguientes caminos crees que seguirán los mensajes ICMP echo request desde `pc1` a `pc3`?

   - `pc1` → `r1` → `pc3`
   - `pc1` → `s1` → `pc3`
   - `pc1` → `s2` → `r2` → `pc3`

   Justifica la respuesta.

2. Indica cuántas solicitudes y respuestas de ARP serían necesarias para que dicho ping funcionase. Explica en qué pcs/routers/switches y su interfaz `eth` concreta se podrían capturar:

   - solicitud/es de ARP.
   - respuesta/s de ARP.

3. Lanza `tcpdump` en las máquinas `r1(eth0)` (`switch-router-04.cap`), `pc2` (`switch-router-05.cap`) y `pc5` (`switch-router-06.cap`) para ayudarte a comprobar tus suposiciones.

4. Indica qué direcciones Ethernet habrán aprendido `s1` y `s2` después de ejecutar el `ping` y explica qué mensajes han generado dicho aprendizaje. Compruébalo.

5. ¿Crees que habrá llegado alguno de los mensajes ICMP echo request a `pc2`, `pc4` o `pc5`? Justifica la respuesta.

## 2.3. Comunicación entre pc2 y pc5

Con las cachés de ARP vacías y las tablas de direcciones aprendidas de los switches vacías se desea realizar un `ping` de `pc2` a `pc5`:

1. Observa la configuración que hay en el escenario para que `pc2` y `pc5` puedan intercambiar tráfico. ¿Cuál de los siguientes caminos crees que seguirán los mensajes ICMP echo request desde `pc2` a `pc5`?

   - `pc2` → `r2` → `pc5`
   - `pc2` → `r1` → `s2` → `pc5`
   - `pc2` → `r2` → `s1` → `s2` → `pc5`
   - `pc2` → `r2` → `r1` → `s2` → `pc5`
   - `pc2` → `s1` → `r1` → `r2` → `pc5`

   Justifica la respuesta.

2. Indica cuántas solicitudes y respuestas de ARP serían necesarias para que dicho ping funcionase. Explica en qué pcs/routers/switches y su interfaz `eth` concreta se podrían capturar:

   - solicitud/es de ARP.
   - respuesta/s de ARP.

[2] Recuerda que esta prueba necesita que las tablas de direcciones aprendidas y las cachés de ARP estén vacías. Para borrar las tablas de direcciones aprendidas de un switch puedes desactivar y activar el switch ejecutando, por ejemplo, el comando 'ifconfig s1 down' y a continuación ejecutar 'ifconfig s1 up'. Puedes comprobar cómo la tabla de direcciones aprendidas está vacía. Las cachés de ARP de las máquinas se comprueban ejecutando 'arp -a' y se pueden borrar cada una de sus entradas ejecutando 'arp -d direcciónIP'

3. Lanza `tcpdump` en las máquinas `pc1` (`switch-router-07.cap`), `pc3` (`switch-router-08.cap`) y `pc4` (`switch-router-09.cap`) para ayudarte a comprobar tus suposiciones.

4. Indica qué direcciones Ethernet habrán aprendido `s1` y `s2` después de ejecutar el `ping` y explica qué mensajes han generado dicho aprendizaje. Compruébalo.

5. ¿Crees que habrá llegado alguno de los mensajes ICMP echo request a `pc1`, `pc3` o `pc4`? Justifica la respuesta.

# 3. Proxy ARP

En el fichero `lab-proxyARP.tgz` está definida una red como la que aparece en la figura 3. Descomprime el fichero, lanza NetGUI y abre el escenario. Arranca las máquinas de una en una.

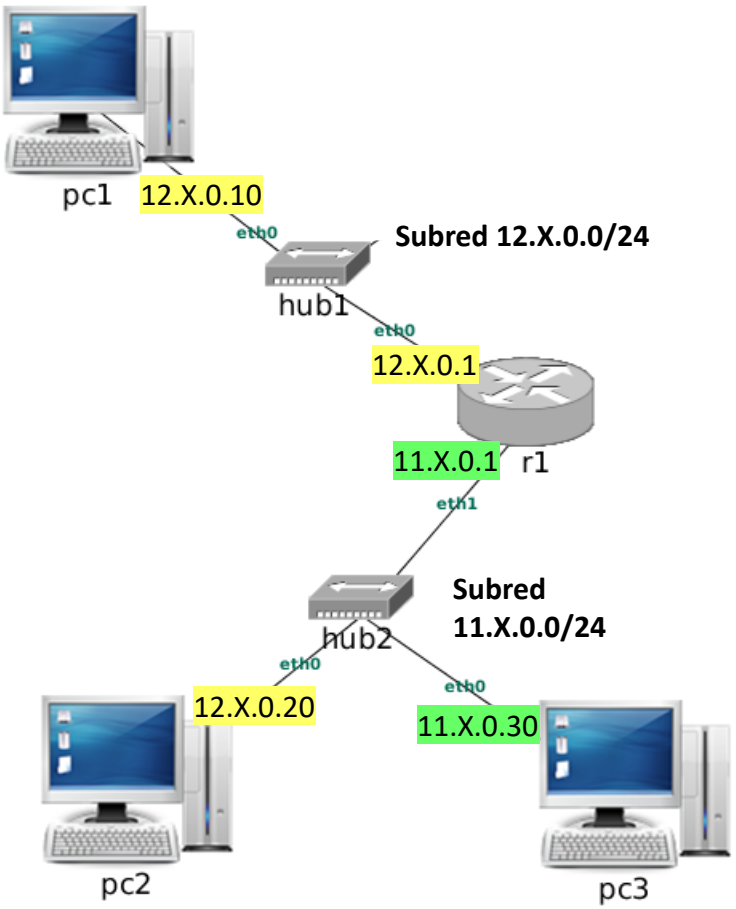



Figura 3: Escenario de Proxy ARP

Características del escenario:

- Los pcs y el router `r1` están configurados con las direcciones IP que se muestran en la figura.
- En el fichero `/etc/hosts` de cada pc están los nombres y direcciones IP de `pc1`, `pc2` y `pc3`, por lo que puedes referirte a ellos por su nombre además de por su IP en las órdenes que utilices.

1. Activa proxy ARP en la configuración del router `r1` para que las máquinas `pc1` y `pc2` tengan conectividad IP entre ellas en ambos sentidos. Explica qué modificaciones han sido necesarias y por qué.

2. Con las cachés de ARP vacías, realiza una captura en la interfaz `r1(eth0)` (`proxyARP-01.cap`) y en `pc3` (`proxyARP-02.cap`) y ejecuta un `ping` desde `pc1` a la dirección IP de `r1(eth0)`, enviando sólo 3 paquetes, y después un `ping` desde `pc1` a `pc2`, enviando sólo 3 paquetes. Interrumpe la captura y explicalas solicitudes de ARP que ves en el tráfico capturado en ambos ficheros.

3. A partir de la captura y de las direcciones IP de `r1`, ¿cómo puedes saber que `r1` está realizando proxy ARP?

4. Si se ha borrado la caché de ARP de `pc1` vuelve a ejecutar los 2 `ping` anteriores y consulta la caché de ARP de `pc1`, indica qué observas, explicando a qué máquina/s pertenece la información almacenada.

# 4. IP aliasing

En el fichero `lab-ipAliasing.tgz` está definida una red como la que aparece en la figura 4. Descomprime el fichero, lanza NetGUI y abre el escenario. Arranca las máquinas de una en una.

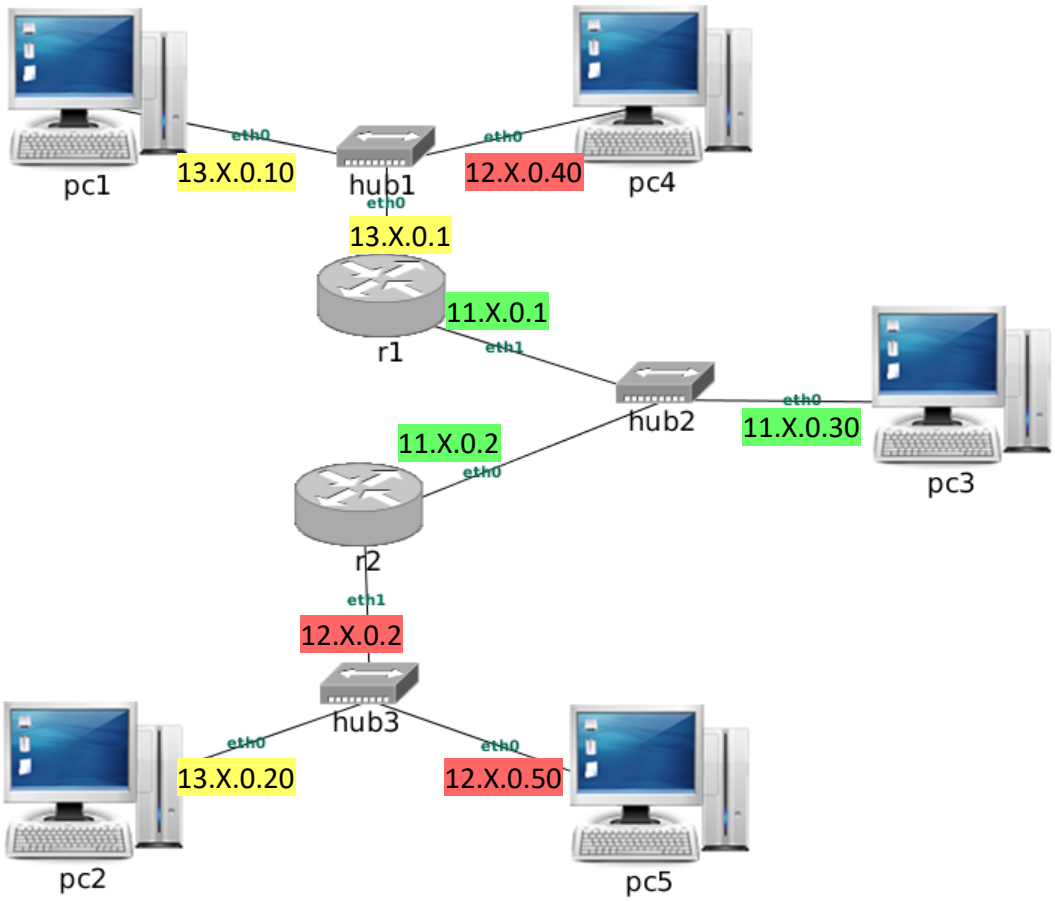



Figura 4: Escenario de IP Aliasing

Características del escenario:

- En el fichero `/etc/hosts` de cada pc están los nombres y direcciones IP de `pc1`, `pc2`, `pc3`, `pc4` y `pc5`, por lo que puedes referirte a ellos por su nombre además de por su IP en las órdenes que utilices.
- `pc1`, `pc3` y `pc5` tienen conectividad IP entre ellos. `pc2` y `pc4` no tienen conectividad IP, ya que no están conectados a sus respectivas subredes.

1. Asigna **direcciones IP adicionales** en los routers mediante *IP aliasing*, y configura las tablas de encaminamiento que sean necesarias para que `pc2` pueda hacer `ping` a `pc3`, ten en cuenta que desde `r2` se debería poder alcanzar también a `pc1` [3]. Indica por qué has configurado esas direcciones IP adicionales y en qué interfaces.

[3] Nótese que cuando añades una dirección por IP aliasing a una tabla de encaminamiento se añade automáticamente una entrada para la subred a la que pertenece, entrada que a veces es necesario borrar para que no haya en la misma tabla dos rutas diferentes a la misma subred.

2. Realiza una captura en `r2(eth1)` (`ipAliasing-01.cap`) y ejecuta un `ping` desde `pc2` a `pc3` enviando 3 paquetes y después ejecuta un `ping` desde `pc5` a la dirección IP de `r2(eth1)`. Interrumpe la captura y explica las solicitudes de ARP que observas.

3. ¿Se puede saber sólo mirando el fichero de captura que en `r2` no se ha configurado proxy ARP?

4. Con la configuración que has realizado previamente ¿pueden comunicarse `pc1` y `pc5`? ¿Por qué? Si tu respuesta es negativa, modifica la configuración para que `pc5` y `pc1` puedan intercambiar tráfico.

5. Utiliza de nuevo *IP aliasing* para que `pc4` pueda hacer `ping` a `pc1`, ten en cuenta que desde `r1` se debería poder alcanzar también a `pc5`.

6. Realiza una captura en `r1(eth0)` (`ipAliasing-02.cap`) para ver qué paquetes se intercambian cuando `pc4` hace `ping` a `pc1`. Explica los resultados en la memoria.

Sistemas Telemáticos

# Práctica 1 (2ª parte): Dispositivos de Interconexión

GSyC
Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación

Diciembre de 2023

Para escribir las respuestas de la segunda parte del enunciado, por favor, utiliza el mismo documento que creaste en la primera parte.

**Las capturas de tráfico** que vayáis realizando por favor, **no las subáis a la carpeta compartida**. La carpeta sólo contendrá las memorias de las prácticas que realicéis durante el curso. Al terminar la práctica te indicaremos como entregar tanto la memoria como las capturas de tráfico que hayas realizado.

Para esta práctica, cada alumno tendrá escenarios diferentes en cada apartado. En particular, las direcciones IP de las máquinas tendrán asignado en el segundo byte un valor X distinto. Podrás ver qué valor X tienes asignado cuando cargues el escenario en NetGUI y observes la configuración.

Descarga tus escenarios del siguiente enlace donde deberás introducir tu número de DNI (8 dígitos) con la letra correspondiente:

`https://mobiquo.gsyc.es/practicas/st/p1.html`

## 5. VLANs

En el fichero `lab-vlan.tgz` está definida la topología de una red como la de la figura 1 en la que aún no se han configurado las VLANs. Descomprime el fichero, arranca NetGUI y abre el escenario. Arranca las máquinas de una en una.

Los dispositivos de interconexión `s1`, `s2` y `s3` están configurados para que funcionen como *switches* Ethernet.

1. Explica qué máquinas se pueden comunicar entre ellas.

   Compruébalo realizando `ping`.

2. Suponiendo que la caché de ARP de pc1 está vacía, indica dónde se puede capturar un solicitud de ARP que la máquina `pc1` envía preguntando por la dirección Ethernet de la máquina `pc2`.

   Compruébalo realizando capturas. Para este caso puedes utilizar `tcpdump -i <interfaz> -s 0` sin necesidad de guardar la captura en un fichero, de esta forma verás el resultado mostrado en pantalla. (Comprueba antes que en la caché de ARP de `pc1` no se encuentra la dirección Ethernet de `pc2`; si estuviera, bórrala).

### 5.1. Configuración de VLAN100

Para facilitar la configuración de las VLANs en cada switch se propone que esta configuración quede almacenada en un fichero de script. Un script es un fichero que contiene comandos que se ejecutarán en el intérprete de comandos, tal y como si los tecleáramos en el terminal.

La configuración de la VLAN100 está escrita en los ficheros `vlan-s1.sh`, `vlan-s2.sh` y `vlan-s3.sh`, que se encuentran en `s1`, `s2` y `s3` respectivamente.

1. Estudia estos scripts para entender qué hace cada uno de ellos. Observa que la primera línea `#!/bin/bash` indica el intérprete que va a ejecutar este script, en este caso `bash`. El resto de líneas en el fichero que

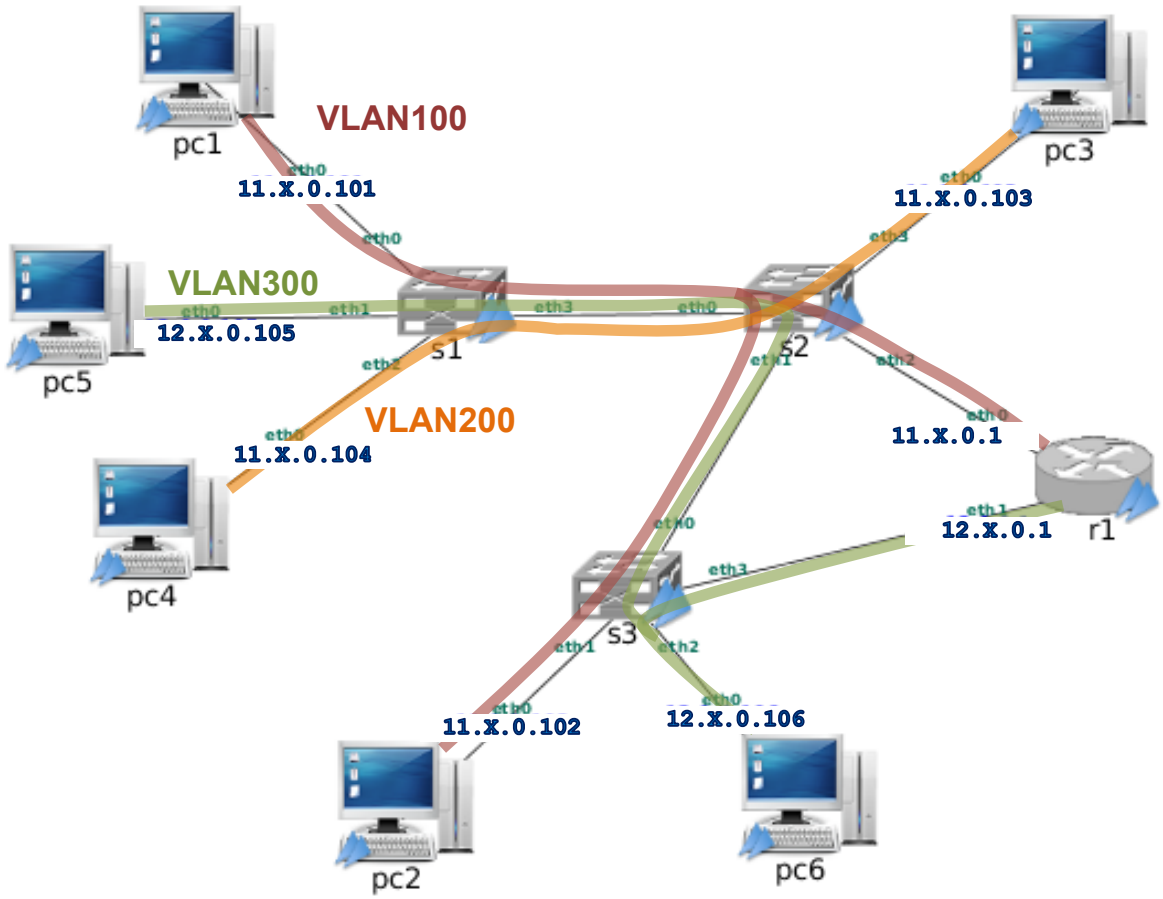



Figura 1: Escenario de VLANs

comienzan por `#` son comentarios. Cada uno de los comandos que se desean ejecutar se escriben en líneas diferentes [1].

2. Ejecuta los scripts para aplicar la configuración. Debes ejecutar cada uno de esos scritps en su switch, por ejemplo en `s1`:

   ```
   s1:~# ./vlan-s1.sh
   ```

   Puedes comprobar la configuración que tiene en un *switch* escribiendo `brctl show`.

3. Haz un dibujo de cada switch que muestre las interfaces que intervienen en la VLAN100, indicando si estas interfaces llevan o no etiqueta VLAN.

4. Indica qué máquinas se pueden comunicar entre ellas.

5. Suponiendo que la caché de ARP de `pc1` está vacía, indica dónde se puede capturar un solicitud de ARP que la máquina `pc1` envía preguntando por la dirección Ethernet de la máquina `pc2`.

   Compruébalo realizando las capturas que creas necesarias, sin necesidad de guardar en fichero el tráfico capturado. (Comprueba antes que en la caché de ARP de `pc1` no se encuentra la dirección Ethernet de `pc2`, si estuviera, bórrala).

[1] Los comandos que se han escrito para desactivar y borrar el switch terminan con '2 > /dev/null' que significa que si se produce algún error al ejecutar el comando, ese error no se muestra. Esto es necesario porque si ejecutamos sucesivas veces este script, la primera vez que se ejecutó, se desactivó y eliminó el switch y en las sucesivas veces que se ejecute dicho script el switch no existirá y se mostraría un error al desactivarlo y eliminarlo.

6. Indica qué ocurre cuando se hace un `ping` desde `pc1` a `pc2`, teniendo en cuenta que ambas máquinas se encuentran en la misma subred. Compruébalo realizando las capturas necesarias, sin necesidad de guardar en un fichero el tráfico capturado.

7. Asegúrate de que la caché de ARP de `pc1` está vacía, bórrala si es necesario. Arranca `tcpdump` en las siguientes interfaces: `pc1(eth0)` (`vlan-01.cap`), `s1(eth3)` (`vlan-02.cap`), `s2(eth2)` (`vlan-03.cap`), `s3(eth0)` (`vlan-04.cap`) y `pc2(eth0)` (`vlan-05.cap`), guardando esta vez el tráfico capturado en un fichero. Realiza un `ping` desde `pc1` a `pc2`.

8. Interrumpe las capturas. Observa las direcciones Ethernet aprendidas por `s1`, `s2` y `s3`.

9. Analiza las 5 capturas, indica en qué capturas se observa la etiqueta de VLAN en el tráfico y qué identificador de VLAN contiene.

   *a*) ¿Qué *switch* introduce dicha etiqueta?

   *b*) ¿Qué *switch* elimina dicha etiqueta?

   *c*) ¿`pc1` y `pc2` tienen alguna forma de saber si están usando una VLAN para comunicarse?

   *d*) ¿Por qué sólo se ve una trama Ethernet en la captura realizada en la interfaz `s2(eth2)`?

   *e*) ¿En qué se diferencia la solicitud de ARP que se captura en `pc1(eth0)` de la misma solicitud que se captura en `s1(eth3)`?

   *f*) ¿En qué se diferencia el mensaje ICMP Echo request que se captura en `pc1(eth0)` del mismo mensaje que se captura en `s1(eth3)`?

10. Indica qué ocurre cuando se hace un `ping` desde `pc1` a `pc4`, teniendo en cuenta que ambas máquinas se encuentran en la misma subred y conectadas al mismo *switch*. Compruébalo realizando una captura en `pc1(eth0)` (`vlan-06.cap`) y otra en `s1(eth3)` (`vlan-07.cap`). Explica los resultados.

## 5.2. Configuración de VLAN200

Configura la VLAN200 en los *switches* que creas necesarios. Para ello edita los ficheros de configuración proporcionados en el apartado anterior y añade la configuración de VLAN 200.

Antes de ejecutar la nueva configuración es necesario borrar la anterior, para ello, reinicia los switches `s1` y `s2`, y a continuación ejecuta sus scripts modificados.

Puedes comprobar la configuración que tiene cada *switch* escribiendo `brctl show`.

1. Haz un dibujo de cada switch que muestre las interfaces que intervienen en la VLAN200, indicando si estas interfaces llevan o no etiqueta VLAN.

2. Indica qué máquinas se pueden comunicar entre ellas con la configuración de VLAN200.

3. Asegúrate de que la caché de ARP de `pc4` está vacía, bórrala si es necesario. Arranca `tcpdump` en las siguientes interfaces: `pc4(eth0)` (`vlan-08.cap`), `s1(eth3)` (`vlan-09.cap`), `pc3(eth0)` (`vlan-10.cap`) y `pc1(eth0)` (`vlan-11.cap`) guardando esta vez el tráfico capturado en un fichero. Realiza un `ping` desde `pc4` a `pc3`.

4. Interrumpe las capturas y observa las direcciones Ethernet aprendiadas por los switches `s1`, `s2` y `s3`. Explica el resultado.

5. Analiza las 4 capturas, indica en qué capturas se observa la etiqueta de VLAN en el tráfico y qué identificador de VLAN contiene.

6. Indica qué ocurre ahora cuando se hace un ping desde `pc1` a `pc4`, teniendo en cuenta que ambas máquinas se encuentran en la misma subred, conectadas al mismo *switch* y las interfaces de dicho *switch* tienen configurada una VLAN. Compruébalo realizando una captura en `pc1` (`vlan-12.cap`) y otra en `pc4` (`vlan-13.cap`). Explica el resultado.

## 5.3. Configuración de VLAN300

En este apartado se analiza el comportamiento de 2 VLANs que están conectadas a través de un router. Esta configuración se proporciona en unos scripts que ya se encuentran en el escenario: `vlan100y300-s1.sh`, `vlan100y300-s2.sh` y `vlan100y300-s3.sh`, en `s1`, `s2` y `s3` respectivamente.

Antes de ejecutar la nueva configuración es necesario borrar la anterior, para ello, reinicia todos los switches y a continuación ejecuta cada uno de los scripts anteriores.

Puedes comprobar la configuración que tiene en un *switch* escribiendo `brctl show`.

1. Haz un dibujo de cada switch que muestre las interfaces que intervienen en la VLAN300, indicando si estas interfaces llevan o no etiqueta VLAN.

2. Realiza un ping desde `pc6` a `pc1`. ¿Qué crees que está ocurriendo?

3. Realiza un ping desde `pc6` a `pc5`. ¿Qué crees que está ocurriendo?

4. Suponiendo que la caché de ARP de `pc6` está vacía, al realizar un `ping` de `pc6` a `pc1`, ¿qué solicitudes de ARP hay y en qué interfaces aparecen? ¿Cuáles de ellas tendrán etiqueta VLAN e indica qué etiqueta?

   Compruébalo realizando las capturas que creas necesarias, sin necesidad de guardar en fichero el tráfico capturado. (Comprueba antes que las cachés de ARP de `pc6` y de `r1` están vacías, bórralas si es necesario).

5. Asegúrate de que las cachés de ARP de `pc6` y `r1` están vacías, bórralas si es necesario. Arranca `tcpdump` en las siguientes interfaces: `pc6(eth0)` (`vlan-14.cap`), `s3(eth1)` (`vlan-15.cap`), `r1(eth0)` (`vlan-16.cap`), `s2(eth0)` (`vlan-17.cap`) y `pc1(eth0)` (`vlan-18.cap`), guardando esta vez el tráfico capturado en un fichero. Realiza un `ping` desde `pc6` a `pc1`.

   Supón en qué interfaces aparecerá el tráfico etiquetado y su identificador de VLAN. Comprueba tus suposiciones analizando las capturas, indica en qué capturas se observa la etiqueta de VLAN en el tráfico y qué identificador de VLAN contiene.

Sistemas Telemáticos

# Práctica 1 (3ª parte): Dispositivos de Interconexión

GSyC
Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación

Diciembre de 2023

Para escribir las respuestas de la tercera parte del enunciado, por favor, utiliza el mismo documento que creaste en la primera parte.

**Las capturas de tráfico** que vayáis realizando por favor, **no las subáis a la carpeta compartida**. La carpeta sólo contendrá las memorias de las prácticas que realicéis durante el curso. Al final de este enunciado encontrarás las indicaciones de cómo entregar esta práctica.

Para esta práctica, cada alumno tendrá escenarios diferentes en cada apartado. En particular, las direcciones IP de las máquinas tendrán asignado en el segundo byte un valor X distinto. Podrás ver qué valor X tienes asignado cuando cargues el escenario en NetGUI y observes la configuración.

Descarga tus escenarios del siguiente enlace donde deberás introducir tu número de DNI (8 dígitos) con la letra correspondiente:

`https://mobiquo.gsyc.es/practicas/st/p1.html`

## 6. Spanning Tree Protocol (STP)

En el fichero `lab-STP.tgz` está definida una red como la que aparece en la figura 1. Descomprime el fichero, lanza NetGUI y abre el escenario. Arranca las máquinas de una en una.

Los *switches* están conectados físicamente formando un bucle pero tienen activado el protocolo STP.

1. Consulta en la información de cada switch cuál es su identificador. Deduce a partir de este identificador la prioridad configurada en cada switch.
2. Sin consultar la información de STP en cada switch calcula:
   *a*) El switch raíz.
   *b*) Para cada switch indica cuál es su puerto raíz.
   *c*) Para cada tramo de medio compartido (LAN), calcula cuál es switch designado (DS) y su puerto designado (DP).
   *d*) Deduce cuáles son los puertos bloquedados.
   *e*) Realiza un dibujo con el árbol de expansión que tendrán configurados los switches.
3. Comprueba tus suposiciones consultando la información STP en cada switch.
4. Arranca un `tcpdump` para capturar el tráfico en `s4(eth2)` almacenando la captura en el fichero `stp-01.cap`. Déjala al menos durante 10 segundos e interrumpe la captura. Antes de abrir la captura ¿qué mensajes crees que encontrarás y quién es el switch que los ha generado?
5. Comprueba tus suposiciones y anota la información más relevante que encuentres en los mensajes:
   *a*) Idendificador del switch raíz
   *b*) Coste al switch raíz

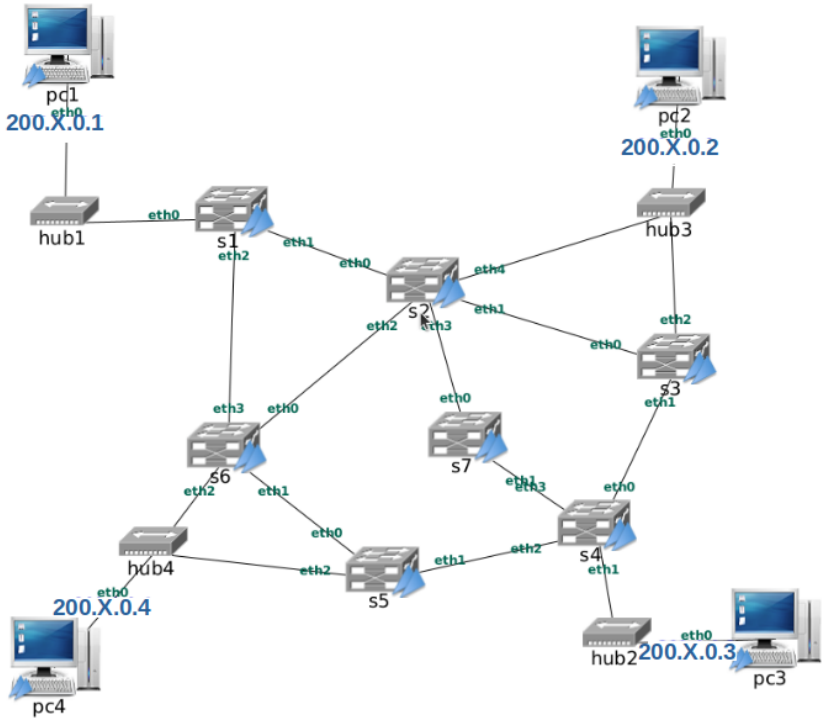



Figura 1: Escenario de STP

*c*) Identificador del switch que envía el mensaje

*d*) Número de puerto que está usando el switch que envía el mensaje

6. Si ejecutáramos un `ping` desde `pc1` a `pc3`, explica por dónde le llegarían los mensajes ICMP Echo Request a `s4`.

7. ¿Y los mensajes ICMP Echo Reply por donde los recibiría `s1`?

8. Inicia una captura en la interfaz de `s4` que has calculado en el apartado anterior. Arranca un `ping -c 1` en `pc1` dirigido a `pc3` almacenando el contenido en `stp-02.cap`. Interrumpe la captura. Para cada uno de los mensajes capturados indica cuál será el camino que han seguido esos mensajes a través de los switches del escenario y cuál de esos mensajes ha provocado el aprendizaje de una dirección Ethernet en los switches de la figura.

9. Apaga el switch `s3` y espera al menos 2 minutos a que se haya reconfigurado el nuevo árbol de expansión. Sin consultar la información de STP en cada switch indica:

   *a*) Para cada switch indica cuál es su puerto raíz.

   *b*) Para cada tramo de medio compartido (LAN), calcula cuál es sw itch designado (DS) y su puerto designado (DP).

   *c*) Deduce cuáles son los puertos bloquedados.

   *d*) Realiza un dibujo con el nuevo árbol de expansión que tendrán confi gurados los switches.

10. Comprueba tus suposiciones consultando la información STP en cada switch.

11. Si ejecutáramos un `ping` desde `pc1` a `pc3`, explica por dónde le llegarían los mensajes ICMP Echo Request a `s4`.

12. ¿Y los mensajes ICMP Echo Reply por donde los recibiría `s1`?

13. Inicia una captura en la interfaz de `s4` que has calculado en el apartado anterior. Arranca un `ping -c 1` en `pc1` dirigido a `pc3` almacenando el contenido en `stp-03.cap`. Interrumpe la captura. Para cada uno de los mensajes capturados indica cuál es el camino que han seguido esos mensajes a través de los switches del escenario y cuál de esos mensajes ha provocado el aprendizaje de una dirección Ethernet en los switches de la figura.

# 7. Entrega de la práctica

Sube al enlace que encontrarás en `aulavirtual` antes de que termine el plazo de entrega, los siguientes ficheros:

- Memoria en formato pdf donde se explique razonadamente la resolución de cada uno de los apartados de este enunciado. Para ello, exporta a pdf la memoria que has escrito en la carpeta de OneDrive.
- Fichero de nombre `p1.zip` o `p1.tgz` resultado de comprimir **una carpeta de nombre p1** que contenga en su interior todos los ficheros de captura de tráfico:
  - De `hub-switch-01.cap` a `hub-switch-06.cap`.
  - De `switch-router-01.cap` a `switch-router-09.cap`.
  - `proxyARP-01.cap` y `proxyARP-02.cap`.
  - `ipAlising-01.cap` e `ipAlising-02.cap`.
  - De `vlan-01.cap` a `vlan-18.cap`.
  - De `stp-01.cap` a `stp-03.cap`.

  Puedes crear el fichero de esta forma: primero crea una carpeta de nombre `p1` y mete dentro de esa carpeta todas los ficheros de captura. Desde el navegador de archivos pulsa con el botón derecho del ratón sobre el nombre de la carpeta y selecciona `'Comprimir'`, nombre del archivador `'p1'` y extensión `'.zip'`.

# Sistemas Telemáticos
# Práctica 2: Protocolos de Encaminamiento: OSPF

Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación

Diciembre de 2023

**Resumen**

En esta práctica, cada alumno tendrá escenarios diferentes en cada apartado. En particular, las direcciones IP de las máquinas tendrán asignado en el segundo byte un valor X distinto. Podrás ver qué valor X tienes asignado cuando cargues el escenario en NetGUI y observes la configuración.

Antes de comenzar a realizar la práctica, por favor, descarga tus escenarios del siguiente enlace donde deberás introducir tu número de DNI (8 dígitos) con la letra correspondiente:

`https://mobiquo.gsyc.urjc.es/practicas/st/p2.html`

Para la realización de estos ejercicios se utilizará el paquete de software *quagga* que permite estudiar el funcionamiento del protocolo OSPF. En la documentación adicional se explica cómo se configura el software *quagga* en Linux.

## 1. OSPF: todos los routers en la misma área

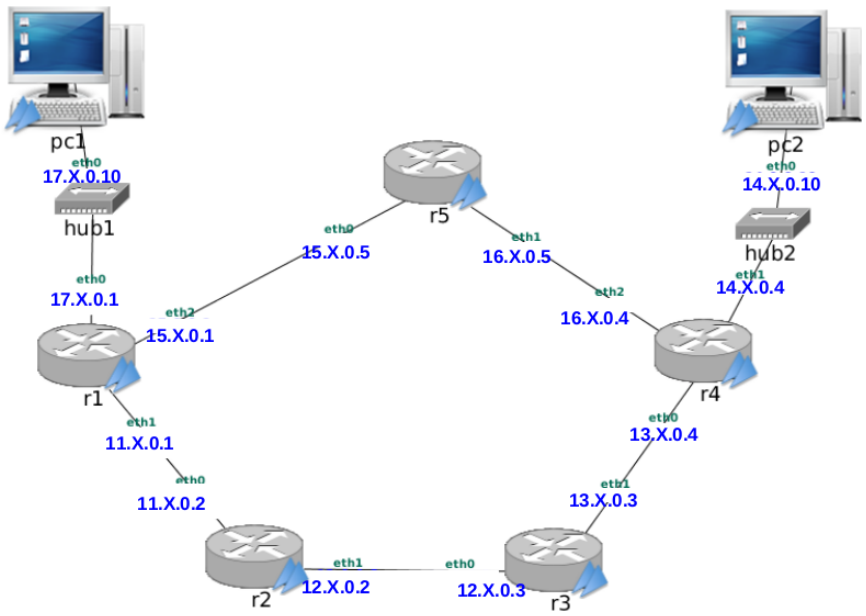



Figura 1: Diagrama de red para el protocolo OSPF

1. En el fichero `lab-OSPF.tgz` está definida una red como la que se muestra en la figura 1. Descomprime el fichero de configuración del escenario `lab-OSPF.tgz`. Al arrancar NetGUI debes abrir el escenario definido en el directorio `lab-OSPF`.

2. Arranca todas las máquinas de una en una. Las máquinas `pc1` y `pc2` tienen rutas por defecto a `r1` y `r4` respectivamente. Los *routers* no tienen configurada ninguna ruta, salvo la de las subredes a las que están directamente conectados. Compruébalo con la orden `route`.

   Los routers no tienen ningún de ellos arrancado `quagga` ni configurado OSPF. En los siguientes apartados se configurará OSPF en cada *router* de **forma incremental** dentro de la misma área (en el área 0) para que las tablas de encaminamiento permitan alcanzar cualquier punto de la red.

## 1.1. Activación de `r1`

Para observar los mensajes que envíe `r1` cuando se active OSPF, arranca `tcpdump` en `pc1` (`ospf-01.cap`), en `r2(eth0)` (`ospf-02.cap`) y en `r5(eth0)` (`ospf-03.cap`) utilizando la opción `-s 0` para que capture los paquetes completos y guardando la captura en un fichero con la opción `-w`.

A continuación configura OSPF en el encaminador `r1` en el área 0 para que su identificador de *router* sea la mayor de sus direcciones IP y para que exporte las rutas hacia las tres redes a las que está conectado. Ten en cuenta que en su interfaz `eth0` no habrá ningún otro router OSPF conectado y por ello configuraremos esa interfaz como **pasiva**. Para realizar la configuración edita con `mcedit` los ficheros `daemons` y `ospfd.conf` en `r1`, y después arranca *quagga*. Espera un minuto aproximadamente e interrumpe las capturas.

Analiza el comportamiento de `r1` estudiando las capturas con *wireshark* y consultando el estado de OSPF a través de su interfaz VTY y de la orden `route`:

1. Comprueba que en la captura realizada por `pc1` no se observan mensajes OSPF ya que has configurado esa interfaz pasiva.

2. Observa los mensajes `HELLO` que se envían al arrancar *quagga* en `r1` y analízalos utilizando Wireshark.

   *a*) ¿Cada cuánto tiempo se envían dichos mensajes? Observa si coincide con el valor del campo `Hello Interval` de los mensajes.

   *b*) Comprueba que el campo `Area ID` se corresponde con el identificador de área que has configurado en el fichero `ospfd.conf`.

   *c*) Comprueba que el identificador del *router* se corresponde con el que has configurado en el fichero mirando el campo `Source OSPF Router` de la cabecera obligatoria de OSPF en los mensajes `HELLO`.

   Comprueba que este identificador es el mismo para los mensajes enviados por las interfaces `eth1` y `eth2` de `r1`, aunque los mensajes se envíen con dirección IP origen diferente (cada mensaje llevará como dirección IP origen la de la interfaz de red de `r1` por la que se envíe).

   *d*) Observa el valor de los campos `DR` y `BDR` en los primeros mensajes `HELLO`. ¿Qué ocurre con dichos campos transcurridos 40 segundos después del primer mensaje `HELLO`? ¿Por qué?

3. ¿Se observan en las capturas mensajes `DB Description` o `LS Update`? ¿Por qué?

4. ¿Debería haber aprendido alguna ruta `r1`? Compruébalo consultando la tabla de encaminamiento mediante la orden `route`.

5. Consulta la información de OSPF relativa a la tabla de encaminamiento utilizando la interfaz VTY en `r1` con `show ip ospf route`.

6. Consulta la información de los vecinos que ha conocido `r1` a través de los mensajes `HELLO` recibidos mediante `show ip ospf neighbor`.

7. Consulta la información de la base de datos de *Router Link States* de `r1` con `show ip ospf database router`.

8. Consulta la información de la base de datos de *Network Link States* de `r1` con `show ip ospf database network`

## 1.2. Activación de `r2`

Para observar los mensajes que envíe `r2` cuando se active OSPF, y los que envíe `r1` a consecuencia de la activación de `r2`, arranca `tcpdump` en `r1(eth1)` (`ospf-04.cap`), en `r3(eth0)` (`ospf-05.cap`) y en `r5(eth0)` (`ospf-06.cap`) utilizando la opción `-s 0` para que capture los paquetes completos y guardando la captura en un fichero con la opción `-w`.

A continuación configura OSPF en el encaminador `r2` en el área 0 para que su identificador de *router* sea la mayor de sus direcciones IP y para que exporte las rutas hacia las dos redes a las que está conectado. Para ello edita los ficheros `daemons` y `ospfd.conf` en `r2`, y después arranca *quagga*.

Espera dos minutos aproximadamente e interrumpe las capturas.

Analiza el comportamiento de `r2` y `r1` estudiando las capturas con *wireshark* y consultando el estado de OSPF a través de las interfaces VTY y de la orden `route` en cada encaminador:

1. Observa la captura realizada en `r1` y responde a las siguientes cuestiones:

   *a*) Observa que aparecen mensajes `DB_DESCRIPTION` cuando `r1` detecta la presencia de `r2` y viceversa. ¿Cuál es su propósito? ¿Qué IP de destino llevan esos mensajes?

   *b*) Observa los mensajes `LS Request` que envían `r1` y `r2`. ¿Qué `LSA` pide cada uno al otro? ¿Qué IP de destino llevan estos mensajes?

   *c*) Observa el primer mensaje `LS Update` que envía `r1`. Comprueba que se corresponde con el `LS Request` enviado por `r2`. Comprueba cómo se corresponde su contenido con lo almacenado en la base de datos de `r1` analizada en el apartado anterior. Observa sus campos para ver si este mensaje incluye la información de que `r1` ha descubierto a `r2` como vecino. ¿Crees que la información contenida en este mensaje deberá cambiar próximamente? ¿Por qué?

   Observa el campo `LS Age` del anuncio que viaja en el mensaje, y explica su valor.

   *d*) Observa el primer mensaje `LS Update` que envía `r2`. Comprueba que se corresponde con el `LS Request` enviado por `r1`. Observa sus campos para ver si este mensaje incluye la información de que `r2` ha descubierto a `r1` como vecino. ¿Crees que la información contenida en este mensaje deberá cambiar próximamente? ¿Por qué?

   Observa el campo `LS Age` del anuncio que viaja en el mensaje, y explica su valor.

*e*) Observa el segundo y tercer mensajes `LS Update` que envía `r1`. ¿Responden a algún `LS Request` previo? ¿Por qué se envían? ¿Qué información contienen?

Observa el campo `LS Age` de los anuncios que viajan en los mensajes, y explica su valor.

*f*) Observa el segundo mensaje `LS Update` que envía `r2`. ¿Responde a algún `LS Request` previo? ¿Por qué se envía? ¿Qué información contiene?

Observa el campo `LS Age` del anuncio que viaja en el mensaje, y explica su valor.

*g*) ¿Por qué razón `r2` no envía ningún mensaje `Network-LSA`?

*h*) Observa los mensajes `LS Acknowledge`. Mira su contenido para comprobar a qué `LSA`s asienten.

*i*) Pasados 40 segundos del arranque de `r2`, ¿qué ocurre con los campos `DR` y `BDR` de los mensajes `HELLO` que intercambian?

2. Observa la captura realizada en `r5` y en `r3`. Explica por qué solo hay mensajes `HELLO`.

3. ¿Deberían haber aprendido alguna ruta `r2` y `r1`? Compruébalo consultando la tabla de encaminamiento en ambos encaminadores mediante la orden `route`.

4. Consulta la información de OSPF relativa a la tabla de encaminamiento utilizando la interfaz VTY en cada encaminador con `show ip ospf route`. Comprueba la métrica de cada ruta y a través de qué *router* se alcanza.

5. Consulta la información de los vecinos que ha conocido cada encaminador a través de los mensajes `HELLO` mediante `show ip ospf neighbor`. Analiza la información que muestra este comando en `r1` donde ya hay elegidos DR y BDR para la subred 11.X.0.0/24.

6. Consulta en cada encaminador la información de las bases de datos de *Router Link States* y de *Network Link States* mediante `show ip ospf database router` y `show ip ospf database network` respectivamente.

   Comprueba que la información mostrada coincide con el contenido de los últimos `LS Update` enviados por los encaminadores.

7. Apunta el número de secuencia de los mensajes `Router-LSA` y `Network-LSA` que ha generado `r1`, los campos `LS Age` y su contenido (recuerda que se encuentran almacenados en la base de datos de `r1` y `r2`). En un apartado posterior se hará referencia a esta información.

8. Consulta un resumen de las bases de datos en cada encaminador con `show ip ospf database`.

## 1.3. Activación de `r3` y `r4`

Para observar los mensajes que envíen `r3` y `r4` cuando activen OSPF, y los que envíe `r2` a consecuencia de la activación de `r3` y `r4`, arranca `tcpdump` en `r1(eth1)` (`ospf-07.cap`), en `r2(eth1)` (`ospf-08.cap`) y en `r3(eth1)` (`ospf-09.cap`) utilizando la opción `-s 0` para que capture los paquetes completos y guardando la captura en un fichero con la opción `-w`.

Configura OSPF en `r3` y en `r4` (ambos en el área 0), y **arranca quagga a la vez en ambos**. Analiza el comportamiento de los encaminadores estudiando las capturas con *wireshark* y consultando el estado de OSPF a través de las interfaces VTY y de la orden `route` en cada encaminador:

1. Trata de suponer los valores de `DR` y `BDR` en las subredes `12.X.0.0/24` y `13.X.0.0/24`. Comprueba si tus suposiciones son ciertas. Comprueba en los mensajes `HELLO` de la captura en `r3` cómo se ha producido la elección de `DR` y `BDR` al arrancar `r3` y `r4` a la vez.

2. En la captura en `r3` observa el intercambio de mensajes `LS Update` que se produce mientras arrancan `r3` y `r4`.

3. En la captura en `r2` observa el intercambio de mensajes `LS Update` que se produce mientras arrancan `r3` y `r4`.

   Observa también en dicha captura los mensajes `LS Update` que `r3` envía por inundación de los recibidos por él de `r4`. Indica cómo puedes saber si un `LS Update` lo ha originado el encaminador que lo envía o está siendo propagado por inundación (pista: mira el campo `Source OSPF Router` y el campo `Advertising router`).

4. Antes de examinar la captura en `r1` trata de suponer qué tipos de mensaje aparecerán en ella. Comprueba tus suposiciones.

5. Trata de suponer qué modificaciones se habrán realizado en las tablas de encaminamiento de cada *router*. Observa las tablas de encaminamiento utilizando la interfaz VTY con el proceso `ospfd` para verificar tus suposiciones.

6. Consulta la información de los vecinos que ha conocido cada encaminador a través de los mensajes `HELLO` mediante la interfaz VTY. Analiza el resultado del comando `show ip ospf netghbor` donde puedes ver si un vecino es el DR y el BDR de cada una de las subredes a las que está conectado un router.

7. Consulta en cada encaminador la información de las bases de datos de *Router Link States* y de *Network Link States*.

   Comprueba que la información mostrada coincide con el contenido de los últimos `LS Update` enviados por los encaminadores.

8. Por activar `r3` y `r4` la información de los mensajes Network-LSA y Router-LSA que generó `r1` (que se encuentran almacenados en todas las bases de datos) no debería haber cambiado (salvo LS Age). Compruébalo con la información que apuntaste en el apartado 1.2 (7). Fíjate en el campo número de secuencia y responde a estas preguntas:

   - Si es el mismo que tenías apuntado, fíjate en el campo LS Age e indica cuándo crees que cambiará el número de secuencia y por qué. Espera ese tiempo para comprobarlo.
   - Si es diferente, fíjate en el campo LS Age e indica cuándo ha cambiado y por qué.

9. Consulta el resumen de las bases de datos en cada encaminador.

## 1.4. Reconfiguración de rutas: Activación y desactivación de `r5`

1. Tras haber arrancado OSPF en los encaminadores `r1, r2, r3` y `r4`, `pc1` y `pc2` deberían tener conectividad IP. Compruébalo con las órdenes `ping` y `traceroute`.

   Interrumpe *quagga* en los encaminadores `r1`, `r2`, `r3` y `r4`. Comprueba que ya no funciona un `ping` de `pc1` a `pc2`. Deja lanzado el `ping` de `pc1` a `pc2`, y rearranca *quagga* en `r1`, `r2`, `r3`, `r4`, fijándote en los segundos (aproximadamente) que pasan desde que está arrancado *quagga* en todos los encaminadores hasta que el `ping` empieza a funcionar. Apunta este valor de tiempo.

2. Indica en la tabla de encaminamiento de `r1` que se muestra con la orden `route`. Fíjate en la métrica para la red `14.X.0.0/24`.

3. Para que la ruta seguida por los datagramas IP que envía `pc1` a `pc2` vayan por la ruta `pc1 => r1 => r5 => r4 => pc2` , y que los que envía `pc2` a `pc1` vayan por la ruta `pc2 => r4 => r5 => r1 => pc1` tendrás que configurar y activar *quagga* en `r5`.

   Para observar los mensajes que se envíen cuando se active OSPF en `r5`, arranca `tcpdump` en `r1(eth2)` (`ospf-10.cap`), y en `r2(eth1)` (`ospf-11.cap`), utilizando la opción `-s 0` para que capture los paquetes completos y guardando la captura en un fichero con la opción `-w`.

   Configura y arranca OSPF en `r5`. Mirando la tabla de encaminamiento de `r1`, observa y apunta el número de segundos que aproximadamente tarda en aprender `r1` la nueva ruta.

   Comprueba que se está utilizando dicha ruta a través de la orden `traceroute` desde `pc1` a `pc2`. Apunta las rutas y sus métricas en las tablas de encaminamiento de cada encaminador.

   Para las capturas y ábrelas en *wireshark* para estudiar su contenido. Responde a las siguientes cuestiones:

   - ¿Qué diferencias observas entre las 2 capturas respecto al tipo de mensajes capturados? ¿Por qué crees que aparecen o no según que tipo de mensajes en cada una de las dos capturas
   - Localiza en la captura realizada en r1 todos los LSAs distintos que hay contenidos en mensajes *LS Update*, y apunta en la memoria su campos *LS Type*, *Link State ID* y *Advertising Router*.
   - Localiza en la captura realizada en r2 todos los LSAs que hay contenidos en mensajes *LS Update*, y apunta en la memoria su campos *LS Type*, *Link State ID* y *Advertising Router*. ¿Por qué aparecen en esta captura concretamente estos LSAs y no otros?

   Comprueba cómo ha mejorado la métrica para la red 14.X.0.0/24 desde el *router* `r1`. ¿Qué valor tiene ahora?

   Deja corriendo en `pc1` un `ping` hacia `pc2`.

4. A continuación interrumpe la ejecución de *quagga* en el encaminador `r5` utilizando la orden `/etc/init.d/quagga stop`. Podrás observar con la orden `route` que ahora `r5` no conoce rutas aprendidas por OSPF. Apunta la tabla de `r5`. Tampoco exporta información de vecinos hacia otros encaminadores.

5. Observarás que el `ping` de `pc1` a `pc2` deja de funcionar durante un buen rato (fíjate en el número de secuencia `icmp_seq`, éste aumenta con cada paquete enviado cada segundo).

   Observa durante este período, en el que no está funcionando `r5`, la tabla de encaminamiento de `r1` y `r4`. Apunta el contenido.

   Observa también durante este periodo la lista de vecinos conocidos por `r1` y por `r4` (utilizando la interfaz VTY con el proceso `ospfd`). Observa la evolución de la columna `Dead Time` de las distintas entradas. ¿Qué entradas no reinician la cuenta desde los 40 segundos? ¿Por qué?

6. Espera hasta que vuelva a funcionar el `ping` (fíjate en el número `icmp_seq`). Observa y apunta el número de segundos que aproximadamente está sin funcionar el `ping` debido a que aún no se ha olvidado la ruta a través de `r5`.

   Comprueba que finalmente `r5` ha desaparecido de entre los vecinos conocidos por `r1` y `r4`.

7. Comprueba ahora las entradas de las tablas de encaminamiento de `r1` y de `r4`.

   Interrumpe el `ping` y comprueba la ruta que están siguiendo los mensajes intercambiados entre `pc1` y `pc2` con `traceroute`.

8. Por último, vuelve a arrancar de nuevo *quagga* en `r5`. Observa cómo cambian las tablas de encaminamiento en `r1` y `r4` y apenas se interrumpe el `ping`.

   Comprueba de nuevo cuál es ahora la ruta que están siguiendo los mensajes intercambiados entre `pc1` y `pc2` con `traceroute`. Observa y apunta el número de segundos que aproximadamente tarda en aprenderse de nuevo la ruta a través de `r5`, mirando continuamente la tabla de encaminamiento de `r1`. Mira también los números de secuencia de los `icmps` del `ping`, y fíjate si alguno se pierde mientras se cambia de la ruta antigua a la ruta nueva.

## 2. OSPF: red con varias áreas

En el fichero `lab-OSPF-Areas.tgz` está definida una red como la que se muestra en la figura 2. Descomprime el fichero de configuración del escenario `lab-OSPF-Areas.tgz`. Al arrancar NetGUI debes abrir el escenario definido en el directorio `lab-OSPF-Areas`.

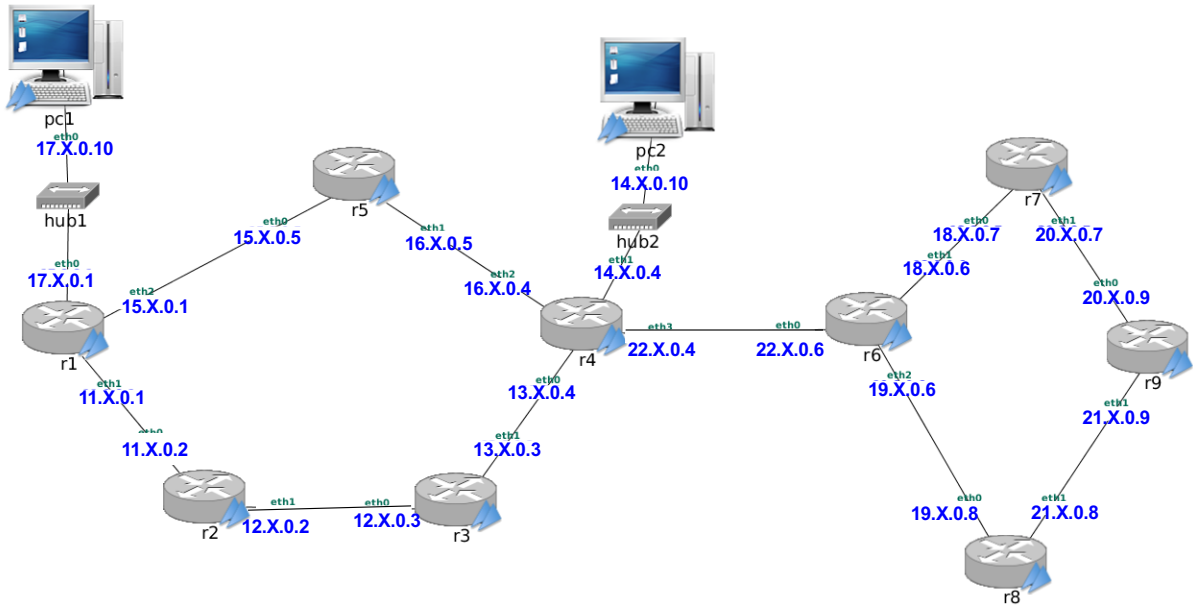



Figura 2: Diagrama de red con todos los *routers* en el área 0

- Arranca todas las máquinas de una en una. Las máquinas `pc1` y `pc2` tienen rutas por defecto a `r1` y `r4` respectivamente. Los *routers* tienen configurado OSPF, **estando todos ellos en el área 0**.
- Arranca *quagga* en todos los *routers*, y espera aproximadamente un minuto.

1. Con la orden `route` comprueba las tablas de encaminamiento en `r1`, `r4`, `r6` y `r9` e incluye su contenido en la memoria. Deberían tener ruta a todas las redes de la figura. Comprueba el coste de cada ruta.

2. Comprueba en esos mismos *routers*, a través de su interfaz VTY, los mensajes LSU *Router-LSA* y *Network-LSA* presentes en sus bases de datos. Toma nota de qué mensajes hay exactamente:

- Para Router LSA: toma nota del campo Link State ID que representa el router descrito en ese mensaje.
- Para Network LSA: toma nota del campo Link State ID que representa la subred descrita en ese mensaje.

- Apaga *quagga* en todos los *routers*. Configura ahora todos ellos de forma que se establezcan las áreas que se muestran en la figura 3. Para ello, edita sus ficheros `/etc/quagga/ospfd.conf` y cambia el área al que pertenece cada interfaz de cada router en las líneas `network`.

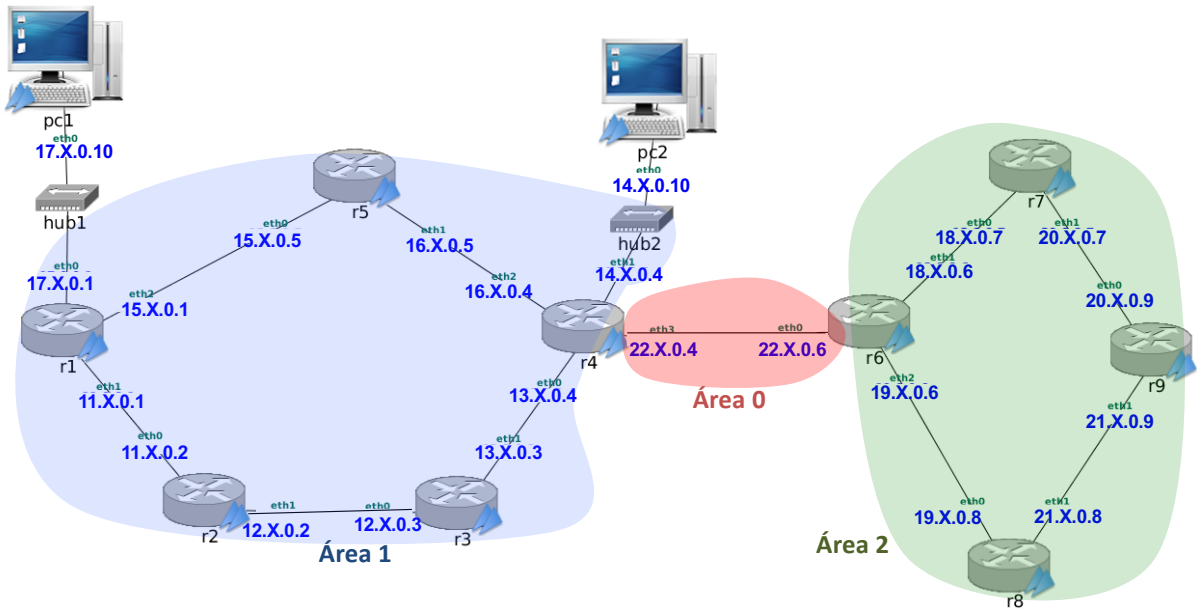



Figura 3: Diagrama de red con varias áreas

- Reinicia *quagga* en todos los *routers* **excepto `r4` y `r6`**, y espera aproximadamente un minuto.

3. Mira las bases de datos de `r1` y `r5`. ¿Hay algún mensaje LSU *Summary-LSA* en ellas? ¿Por qué?

- Para observar los mensajes que envíen `r4` y `r6` cuando activen OSPF, arranca `tcpdump` en `r3(eth1)` (`ospfAreas-01.cap`), `r4(eth3)` (`ospfAreas-02.cap`) y `r7(eth0)` (`ospfAreas-03.cap`).
- Arranca ahora *quagga* en `r4` y `r6`, y espera aproximadamente un minuto. Interrumpe las capturas.

4. Localiza en la captura los mensajes `LS Update` que envía `r4` a `r3` que permiten a `r3` añadir una ruta para cada una de las siguientes redes:
   - `18.X.0.0/24`
   - `19.X.0.0/24`
   - `20.X.0.0/24`
   - `21.X.0.0/24`

   Contesta a las siguientes preguntas:

   *a*) ¿De qué tipo de LSAs se trata?

*b*) ¿Qué router es el que está anunciando esos LSAs (`Advertising Router`)? ¿Por qué no es `r6` si las subredes son del área 2?

*c*) Para cada uno de esos LSAs, indica cuál es su métrica y por qué.

*d*) Busca en la tabla de encaminamiento OSPF de `r3` y relaciona el valor de la métrica del mensaje con el coste que tiene aprendido en la tabla de encaminamiento.

5. Con lo que has aprendido del apartado anterior, trata de suponer cómo serían los mensajes que `r6` le envía a `r7` para informar de las siguientes subredes:

   - `11.X.0.0/24`
   - `12.X.0.0/24`
   - `13.X.0.0/24`
   - `14.X.0.0/24`
   - `15.X.0.0/24`
   - `16.X.0.0/24`
   - `17.X.0.0/24`

   *a*) Para cada uno de los anuncios anteriores supón qué tipo de LSA, qué valor viaja en el campo `Advertising router`, cuál es el valor de métrica anunciado. Localiza en la captura los mensajes `LS Update` que envía `r6` a `r7` para confirmar tu suposición.

   *b*) Supón qué habrá añadido `r7` en su tabla de encaminamiento OSPF y comprueba tus suposiciones consultando la tabla en `r7`.

6. Localiza en las tres capturas qué tipo de LSA contiene el anuncio de la existencia de la red `22.X.0.0/24` e indica su tipo y el contenido de los campos `Advertising Router` y `metric`:

   - cuando `r3` la aprende de `r4`
   - cuando `r6` la aprende de `r4`
   - cuando `r7` la aprende de `r6`

7. Localiza en las tres capturas qué tipo de LSA contiene el anuncio de la existencia de la red `14.X.0.0/24` e indica su tipo y el contenido de los campos `Advertising Router` y `metric`:

   - cuando `r3` la aprende de `r4`
   - cuando `r6` la aprende de `r4`
   - cuando `r7` la aprende de `r6`

8. Comprueba las tablas de encaminamiento en `r1`, `r4`, `r6` y `r9`. Indica el coste de cada ruta. Compara los resultados con los obtenidos en la pregunta 1.

9. Indica en esos mismos *routers*, a través de su interfaz VTY, los mensajes LSU *Router-LSA*, los *Network-LSA* y los *Summary-LSA* presentes en sus bases de datos. Compara con los resultados obtenidos en la pregunta 2.

10. Explica gracias a qué mensaje/s `r1` ha conocido las siguientes subredes y qué router ha generado dicho/s mensaje/s:

    - 12.X.0.0/24
    - 22.X.0.0/24
    - 21.X.0.0/24

# 3. Entrega de la práctica

Sube al enlace que encontrarás en `aulavirtual` antes de que termine el plazo de entrega, dos ficheros:

- Memoria de la práctica en formato PDF
- Un fichero de nombre `p2.zip` o `p2.tgz` que incluya todas las capturas:
  - De `ospf-01.cap` a `ospf-11.cap`.
  - De `ospfAreas-01.cap` a `ospfAreas-03.cap`.

  Crea el fichero con las capturas de esta forma: primero crea una carpeta `p2` y mete dentro de esa carpeta todas los ficheros de captura. Desde el navegador de archivos pulsa con el botón derecho del ratón sobre el nombre de la carpeta y selecciona `'Comprimir'`, nombre del archivador `'p2'` y extensión `'.zip'`.

# Sistemas Telemáticos
# Práctica 3: Protocolos de Encaminamiento: BGP

Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación
(GSyC)

Diciembre de 2023

Antes de comenzar a realizar la práctica, deberás acceder a la **carpeta con tu nombre y apellidos que los profesores hemos compartido a través de OneDrive** y crear un nuevo documento de Word llamado: memoria-p3.docx

Usarás este documento para ir escribiendo en el mismo el trabajo que vayas realizando en esta práctica. Como es un documento compartido con los profesores, nosotros podremos ir revisando de forma gradual tu trabajo. Es obligatorio ir escribiendo los resultados de vuestra práctica según la vayáis realizando en este documento. Por favor, **no uséis ningún otro documento de forma temporal para ir escribiendo vuestros resultados**.

**Las capturas de tráfico** que vayáis realizando por favor, **no las subáis a esta carpeta compartida**. La carpeta sólo contendrá las memorias de las prácticas que realicéis durante el curso. Al terminar la práctica te indicaremos como entregar tanto la memoria como las capturas de tráfico que hayas realizado.

Para esta práctica, cada alumno tendrá escenarios diferentes en cada apartado. En particular, las direcciones IP de las máquinas tendrán asignado en el segundo byte un valor X distinto. Podrás ver qué valor X tienes asignado cuando cargues el escenario en NetGUI y observes la configuración.

Antes de comenzar a realizar la práctica, por favor, descarga tus escenarios del siguiente enlace donde deberás introducir tu número de DNI (8 dígitos) con la letra correspondiente:

`https://mobiquo.gsyc.urjc.es/practicas/st/p3.html`

## 1. Escenario de red utilizando OSPF y BGP

En el fichero `lab-BGP.tgz` se encuentran los ficheros de configuración para crear un escenario de red como el que se muestra en la figura 1. En esta figura hay tres AS (Sistemas Autónomos): AS10, AS20 y AS30. Se ha configurado OSPF dentro de AS20 y AS30 y se desea configurar BGP para conectar los 3 sistemas autónomos. En AS10 no se utilizará ningún protocolo de encaminamiento interior ya que sólo hay una red interna.

Se realizará la configuración por pasos. Supondremos para la configuración de BGP que AS10 y AS20 mantienen una relación de tránsito y que AS10 y AS30 mantienen una relación de tránsito, siendo en ambos casos AS10 el proveedor.

## 1.1. Configuración de los pcs y *routers* de AS20

1. Descomprime el fichero de configuración del escenario `lab-BGP.tgz`. Al arrancar NetGUI debes abrir el escenario definido en el directorio `lab-BGP`.

2. Arranca de una en una sólo las máquinas de AS20.

3. Las máquinas tienen configurada una dirección IP en cada una de sus interfaces de red. Los pcs además tienen configurada una ruta por defecto al único *router* al que están directamente conectados.

4. Los *routers* de AS20 (`as20-r1`, `as20-r2` y `as20-r3`) tienen configurado el protocolo OSPF para que intercambien información de encaminamiento dentro de AS20 (consulta los ficheros `daemons` y `ospfd.conf` de estos *routers*). Arranca `quagga` en todos los *routers* de AS20.

5. Consulta las tablas de encaminamiento utilizando la interfaz VTY con los procesos `ospfd` de cada *router* y mediante el comando `route`.

6. Comprueba utilizando `ping` que todos los pcs y *routers* tienen conectividad dentro de AS20.

7. Modifica la configuración de `quagga` en `as20-r1` para que utilice además de OSPF el protocolo BGP. Define como vecino suyo a `as10-r1`. Utiliza la redistribución de las subredes directamente conectadas (`redistribute connected`). No uses aún la redistribución de rutas entre OSPF y BGP. Inicia una captura en la interfaz `as20-r1(eth0)` y guarda su contenido en un fichero (`bgp-01.cap`). Reinicia `quagga` en `as20-r1`.

8. ¿Debería haber aprendido alguna ruta `as20-r1` por BGP? Compruébalo consultando la tabla de encaminamiento mediante el comando `route` y conectándote a la interfaz VTY del proceso `bgpd` para ver la tabla de encaminamiento BGP.

9. ¿Deberían haber aprendido alguna ruta `as20-r2` y `as20-r3`?

10. Después de al menos 3 minutos, interrumpe la captura e indica qué mensajes observas. Justifica tu respuesta.

## 1.2. Configuración del pc y *router* de AS10

1. Arranca `as10-pc1` y `as10-r1`. La máquina `as10-pc1` tiene configurada una dirección IP y una ruta por defecto al *router* al que está directamente conectado. El *router* `as10-r1` tiene configuradas direcciones IP, una en cada interfaz, pero no tiene configurada ninguna ruta adicional a las de las subredes a las que está directamente conectado.

2. Configura `quagga` en `as10-r1` para que utilice el protocolo BGP. Define como vecinos suyos a `as20-r1` y a `as30-r1`. Incluye la configuración en la memoria.

3. Captura el tráfico con `tcpdump` en `as20-r1(eth0)` y guarda la captura en un fichero (`bgp-02.cap`). Arranca `quagga` en `as10-r1`. Espera un minuto e interrumpe la captura.

4. Analiza la captura `bgp-02.cap` realizada:

   - Observa que el tráfico de BGP va dentro de una conexión TCP.
   - Localiza los mensajes `OPEN` que intercambian los *routers* vecinos. Observa en ambos mensajes `OPEN` los siguientes campos:
     - `My AS`

- Identificador del *router* BGP
- `Hold time`
- En los parámetros opcionales, el campo `Capability` que contiene la información del número de sistema autónomo usando 4 bytes (32 bits).

- Localiza los mensajes `KEEPALIVE` que intercambian los *routers*. Además de la cabecera obligatoria de BGP (`Marker`, `Length` y `Type`) ¿qué otra información viaja en este tipo de mensajes?
- Localiza los mensajes `UPDATE` que intercambian los *routers*. Observa en ambos mensajes `UPDATE` los siguientes campos:
  - Rutas eliminadas
  - Rutas anunciadas
  - Atributos, en particular el valor de `NEXT_HOP` y `AS_PATH`.
  - El atributo `ORIGIN` tiene como valor `INCOMPLETE` porque esas subredes se anuncian debido a la redistribución de subredes y no a través de líneas `network`. Elimina en el fichero `bgpd.conf` de `as10-r1` la línea:

    ```
    redistribute connected
    ```

    y añade las siguientes líneas (modificando el valor de X):

    ```
    network 11.X.1.0/24
    network 20.X.1.0/24
    network 20.X.2.0/24
    ```

    Interrumpe `quagga` en `as10-r1`, inicia una captura de tráfico en `as20-r1(eth0)` dirigiendo su contenido a un fichero (`bgp-03.cap`) y arranca `quagga` en `as10-r1` de nuevo. Pasado 2 minutos aproximadamente interrumpe la captura. Indica el contenido del atributo `ORIGIN` en el mensaje UPDATE que genera `as10-r1` para dichas subredes. Puedes observar como el valor de este atributo (i=IGP, e=EGP, ?=incomplete) también se observa en la tabla BGP, en la columna `Path`, junto al ASN que originó el anuncio. Copia el contenido de esta tabla en la memoria.

5. Consulta la tabla de encaminamiento utilizando la interfaz VTY con el proceso `bgpd` y con el comando `route` en los *routers* `as10-r1` y `as20-r1`. Incluye sus contenidos en la memoria y explica las diferencias.

6. Prueba a hacer un `ping` desde `as10-pc1` hacia `as20-pc2` y comprueba que no funciona. ¿Por qué? (Explica la tabla de encaminamiento que tiene `as10-r1`).

7. Modifica la configuración del fichero `bgpd.conf` de `as20-r1` para que se redistribuyan las rutas aprendidas por OSPF de AS20 a otros ASs utilizando BGP. Incluye la modificación en la memoria. Inicia una captura en `as20-r1(eth0)` y guarda su contenido en un fichero (`bgp-04.cap`). Reinicia `quagga` en `as20-r1`. Comprueba que ahora `as10-r1` tiene rutas a todas las redes de AS20. En la tabla BGP de `as10-r1` fíjate en el atributo `ORIGIN` para las subredes de AS20.

8. Interrumpe la captura y explica los anuncios de las redes internas de AS20 que ves en el tráfico capturado.

9. Prueba a hacer un `ping` desde `as10-pc1` hacia `as20-pc2` y comprueba que todavía no funciona. ¿Por qué? (Explica la tabla de encaminamiento que tiene `as20-r2`).

10. Modifica la configuración del fichero `ospfd.conf` de `as20-r1` para que se redistribuyan las rutas aprendidas por BGP a los *routers* de AS20 mediante OSPF. Incluye la modificación en la memoria. Reinicia `quagga` en `as20-r1`. Comprueba que `as20-r2` tiene ruta a la red de AS10.

11. Comprueba que ahora sí funciona el `ping` entre `as10-pc1` y `as20-pc2`.

## 1.3. Configuración de los pcs y *routers* de AS30

Arranca todas las máquinas de AS30 de una en una. Los *routers* tienen configurada una dirección IP por cada una de sus interfaces. Los pcs tienen configurada una dirección IP y una ruta por defecto al *router* al que están directamente conectados.

Los *routers* de AS30 (`as30-r1`, `as30-r2` y `as30-r3`) tienen configurado el protocolo OSPF para que intercambien información de encaminamiento dentro de AS30.

1. Consulta los ficheros `daemons` y `ospfd.conf` de los *routers* de AS30.

2. Arranca `quagga` en todos los *routers* de AS30. Consulta las tablas de encaminamiento utilizando la interfaz VTY con los procesos `ospfd` de cada *router* y mediante el comando `route`.

3. Comprueba utilizando `ping` que todos los pcs y *routers* tienen conectividad dentro de AS30.

4. Modifica la configuración de `quagga` en `as30-r1` para que utilice además el protocolo BGP. Define como vecino suyo a `as10-r1`. No uses aún la redistribución de rutas entre OSPF y BGP. Incluye la configuración en la memoria.

5. Captura el tráfico con `tcpdump` en `as10-r1(eth2)`, con la opción `-s` para capturar paquetes enteros y `-w` para guardar la captura en un fichero (`bgp-05.cap`). Reinicia `quagga` en `as30-r1`. Espera un minuto e interrumpe la captura.

6. Analiza la captura realizada:

   *a*) Observa que el tráfico de BGP va dentro de una conexión TCP.

   *b*) Localiza los mensajes `OPEN` que intercambian los *routers* vecinos. Observa en ambos mensajes `OPEN` los siguientes campos:

   - `My AS`
   - Identificador del *router* BGP
   - `Hold time`
   - En los parámetros opcionales, el campo `Capability` que contiene la información del número de sistema autónomo usando 4 bytes (32 bits).

   *c*) Localiza los mensajes `KEEPALIVE` que intercambian los *routers*. Comprueba que son similares a los que ya observaste en el apartado anterior

   *d*) Trata de suponer qué rutas le anunciará `as10-r1` a `as30-r1` en sus mensajes `UPDATE`. ¿Qué `AS_PATH` crees que traerán esas rutas? Como los atributos de un mensaje `UPDATE` son comunes a todas las rutas anunciadas, ¿podrá anunciar `as10-r1` todas las subredes que conoce en un solo mensaje `UPDATE`?

   *e*) Trata de suponer qué rutas le anunciará `as30-r1` a `as10-r1` en sus mensajes `UPDATE`.

   *f*) Localiza en la captura los mensajes `UPDATE` que intercambian los *routers* y confirma si tus suposiciones son ciertas. Observa el valor de los atributos `NEXT_HOP` y `AS_PATH`.

7. ¿Debería haber aprendido alguna ruta `as30-r1`? Compruébalo consultando la tabla de encaminamiento mediante el mandato `route`.

8. El resto de *routers* de AS30 ¿deberían haber aprendido alguna otra ruta? Compruébalo.

9. Prueba a hacer un `ping` desde `as10-pc1` hacia `as30-pc3` y comprueba que no funciona. ¿Por qué? (Explica la tabla de encaminamiento de `as10-r1`).

10. Modifica la configuración del fichero `bgpd.conf` de `as30-r1` para que se redistribuyan las rutas aprendidas por OSPF de AS30 a otros ASs utilizando BGP. Incluye la modificación en la memoria. Reinicia `quagga` en `as30-r1`. Comprueba que ahora `as10-r1` tiene rutas a todas las redes de AS30. En la tabla BGP de `as10-r1` fíjate en el atributo `ORIGIN` para las subredes de AS30.

11. Prueba a hacer un `ping` desde `as10-pc1` hacia `as30-pc3` y comprueba que todavía no funciona. ¿Por qué? (Explica la tabla de encaminamiento de `as30-r3`).

12. Modifica la configuración del fichero `ospfd.conf` de `as30-r1` para que se redistribuyan las rutas aprendidas por BGP a los *routers* de AS30 mediante OSPF. Incluye la modificación en la memoria. Reinicia `quagga` en `as30-r1`. Comprueba que ahora `as30-r3` tiene ruta a la red de AS10.

13. Comprueba que ahora sí funciona el `ping` entre `as10-pc1` y `as30-pc3` y realiza una captura de tráfico en `as10-pc1` guardando su contenido en el fichero `bgp-06.cap`.

14. Comprueba que hay conectividad entre todos los pcs de la figura.

## 2. Agregación de rutas

La configuración de BGP realizada en el apartado anterior provoca que las subredes del sistema autónomo AS20 se almacenen de forma independiente, ocupando cada una de ellas una entrada diferente en las tablas de encaminamiento de los *routers* de AS10 y AS30. De forma equivalente, cada una de las subredes de AS30 ocupan entradas diferentes en las tablas de encaminamiento de los *routers* de AS10 y AS20.

Utilizando CIDR pueden agruparse estas entradas para que los anuncios por BGP que emiten AS20 y AS30 optimicen el número de entradas en las tablas de encaminamiento en los *routers* externos a dichos sistemas autónomos.

1. Interrumpe la ejecución de `quagga` en `as20-r1` y `as30-r1`. Configura BGP en AS20 para que se optimice el número de entradas en las tablas de encaminamiento de los *routers* de AS10 y AS30. Ten en cuenta que al realizar la agregación de rutas, dicha agregación sólo puede referirse a subredes que pertenezcan a AS20. Incluye la modificación en la memoria.

2. Configura BGP en AS30 para que se optimice el número de entradas en las tablas de encaminamiento de los *routers* de AS10 y AS20. Ten en cuenta que al realizar la agregación de rutas, dicha agregación sólo puede referirse a subredes que pertenezcan a AS30. Incluye la modificación en la memoria.

3. Captura el tráfico con `tcpdump` en `as10-r1(eth2)`, con la opción `-s` para capturar paquetes enteros y `-w` para guardar la captura en un fichero `bgp-07.cap`.

4. Inicia `quagga` en `as20-r1` y `as30-r1`, espera a que todos los routers se hayan intercambiado la información de encaminamiento e interrumpe la captura. Analiza la captura realizada:

   - Trata de suponer cómo serán los nuevos mensajes `UPDATE` que intercambien los *routers* anunciando las redes de AS20 y AS30. Localízalos en la captura y confirma si tus suposiciones son ciertas.
   - Fíjate en el atributo `ORIGIN` para estas subredes en los mensajes `UPDATE` y en la tabla BGP de `as10-r1`, su valor es diferente después de realizar la agregación.

5. Consulta las tablas de encaminamiento de los *routers* de AS20 y AS30 mediante el comando `route`, para ver cómo se han agregado las rutas hacia el sistema autónomo externo. Explica el resultado.

6. Consulta la tabla BGP en `as20-r1`, observarás como las subredes de AS20 con el prefijo agregado aparecen como ruta preferida y serán las que se anuncian a otros vecinos BGP. Además, las subredes que se anunciaban previamente de forma independiente y ahora se anuncian dentro del prefijo agregado también aparecen pero marcadas con una `s` que indica que se suprimen. Consulta esta misma información en la tabla BGP de `as30-r1` para las subredes de AS30 que agrega este router. Explica los resultados.

# 3. Modificación del escenario: Políticas de exportación de rutas

AS20 y AS30 se dan cuenta de que intercambian mucho tráfico entre ellos y deciden conectar directamente `as20-r1` y `as30-r1` definiendo una relación entre iguales entre los mismos.

- Interrumpe *quagga* en `as20-r1` y `as30-r1`.
- Interrumpe la ejecución de los *routers* `as20-r1` y `as30-r1`, apagando cada uno de ellos desde la interfaz gráfica de NetGUI. Dibuja un enlace directo entre ambos *routers* y arráncalos de nuevo, uno después de otro.
- Asigna la dirección 20.X.3.20 a la nueva interfaz de `as20-r1` y la dirección 20.X.3.30 a la nueva interfaz de `as30-r1`, ambas direcciones de la red 20.X.3.0/24.
- No apliques por ahora ninguna política de exportación de rutas. Modifica la configuración de BGP de `as20-r1` y `as30-r1` para añadir en cada uno al otro como nuevo vecino. Por defecto si no se configuran políticas de exportación, se anuncian todas las rutas seleccionadas como preferidas.
- Arranca `quagga` en `as20-r1` y `as30-r1`.

Incluye en la memoria las respuestas a los siguientes apartados.

1. Realiza una captura de la interfaz gráfica de NetGUI donde se vea la nueva conexión y las direcciones IP asignadas. Incluyen esa imagen en la memoria.

2. Comprueba mediante `route` en `as20-r1` la ruta hacia las redes de AS30, y en `as30-r1` la ruta hacia las redes de AS20. Utilizando la interfaz VTY en ambos *routers* observa cómo cada uno tiene dos rutas alternativas para el sistema autónomo vecino, y ha elegido una de ellas. ¿Cuál? ¿Por qué? Ten en cuenta que `LOCAL_PREF` no se ha modificado y por tanto valdrá para todas las interfaces su valor por defecto, 100.

3. Observa la tabla BGP de `as20-r1` e indica cuántas rutas alternativas existen para las subredes 20.X.1.0/24, 20.X.2.0/24 y 20.X.3.0/24. Indica cómo `as20-r1` ha aprendido estas rutas alternativas y cuál se ha seleccionado como preferida.

4. ¿Qué ruta crees que seguirán los paquetes intercambiados entre `as20-pc3` y `as30-pc2`? Compruébalo.

5. ¿Qué ruta crees que seguirán los paquetes enviados desde `as30-pc3` con destino `as10-pc1`? Compruébalo utilizando `traceroute`. Utilizando la interfaz VTY en `as30-r1` comprueba cómo tiene dos rutas alternativas para la red `11.X.1.0/24`. Observa cuál es la elegida y por qué.

6. Apaga la interfaz `eth0` de `as30-r1` con `ifconfig eth0 down`. Espera unos 3 minutos. ¿Qué habrá pasado ahora con la ruta que seguirán los paquetes enviados desde `as30-pc3` con destino `as10-pc1`? Compruébalo utilizando `traceroute`. Utilizando la interfaz VTY en `as30-r1` comprueba que ahora sólo tiene una ruta para la red `11.X.1.0/24`. Dada las relaciones entre AS10, AS20 y AS30 indica si esta situación perjudica a alguno de los AS y por qué.

7. Teniendo en cuenta las relaciones entre AS10, AS20 y AS30:

   *a*) ¿Qué rutas debería exportar AS20 a AS30, y qué rutas no debería exportarle?

   *b*) ¿Qué rutas debería exportar AS30 a AS20, y qué rutas no debería exportarle?

8. Teniendo en cuenta las rutas que deben exportarse y las que no, vuelve a configurar BGP en `as20-r1` y `as30-r1` para que se anuncien y se exporten sólo las rutas que a cada AS le interesa. Incluye las modificaciones en la memoria.

9. Vuelve a levantar la interfaz `eth0` de `as30-r1` con `ifconfig eth0 up`. Inicia una captura de tráfico en la interfaz que une `as20-r1` y `as30-r1` y guarda el contenido en el fichero `bgp-08.cap`. Reinicia `quagga` en los 3 *routers* BGP: `as10-r1`, `as20-r1` y `as30-r1`.

10. Comprueba ahora las tablas de encaminamiento en `as20-r1` y `as30-r1`, tanto con `route` como con la interfaz VTY. Explica el contenido.

11. Interrumpe la captura y explica el contenido de los mensajes UPDATE que intercambian `as20-r1` y `as30-r1`. ¿Cuáles crees que son las diferencias de los mensajes UPDATE intercambiados en el apartado 3 y ahora?

12. ¿Qué ruta crees que seguirán ahora los paquetes intercambiados entre `as20-pc3` y `as30-pc2`? Compruébalo.

13. ¿Qué ruta crees que seguirán ahora los paquetes enviados desde `as30-pc3` con destino `as10-pc1`? Compruébalo utilizando `traceroute`. Utilizando la interfaz VTY en `as30-r1` comprueba qué rutas tiene disponibles hacia la red `11.X.1.0/24`.

14. Apaga la interfaz `eth0` de `as30-r1` con `ifconfig eth0 down`. ¿Qué habrá pasado ahora con la ruta que seguirán los paquetes enviados desde `as30-pc3` con destino `as10-pc1`? Compruébalo utilizando `traceroute`. Utilizando la interfaz VTY en `as30-r1` comprueba qué rutas hay ahora para la red `11.X.1.0/24`.

# 4. Políticas de exportación y orden de preferencia en la selección de rutas

En el fichero `lab-BGP2.tgz` se encuentran los ficheros de configuración para crear un escenario de red como el que se muestra en la figura 2. En esta figura hay 6 AS (Sistemas Autónomos): AS10, AS20, AS30, AS40, AS50 y AS60. Se ha configurado OSPF dentro de AS20, OSPF dentro de AS30 y BGP en todos ellos para intercambiar la información de encaminamiento. Se desea que:

- AS30 y AS10 tengan una relación de tránsito, donde AS30 sea el proveedor y AS10 el cliente.
- AS30 y AS40 tengan una relación de tránsito, donde AS30 sea el proveedor y AS40 el cliente.
- AS40 y AS50 tengan una relación de tránsito, donde AS40 sea el proveedor y AS50 el cliente.
- AS40 y AS60 tengan una relación de tránsito, donde AS40 sea el proveedor y AS60 el cliente.
- AS10 y AS20 tengan una relación de tránsito, donde AS10 sea el proveedor y AS20 el cliente.
- AS20 y AS60 tengan una relación de tránsito, donde AS20 sea el proveedor y AS60 el cliente.
- AS10 y AS40 tengan una relación entre iguales.
- AS20 y AS50 tengan una relación entre iguales.

Arranca todas las máquinas de una en una. Por defecto, al arrancar las máquinas se arranca `quagga`. En el escenario se ha configurado OSPF y BGP. Sin embargo, no se han configurado las políticas de exportación ni el atributo LOCAL PREF de BGP.

1. Piensa en qué *routers* debería existir una lista de exportación de rutas e indica qué rutas deberían estar en dicha lista y a qué *router/s* se le exportaría. Interrumpe `quagga` en los *routers* en los que necesites cambiar la configuración y realiza dicha configuración. Inicia nuevamente `quagga` en dichos *routers*.
2. Comprueba en tu nueva configuración las siguientes reglas consultando cada una de las tablas BGP de los routers de la figura:
   - Un AS no anuncia a su proveedor las subredes aprendidas de otro AS proveedor o de un AS con relación entre iguales.
   - Un AS no anuncia a un AS con relación entre iguales las subredes aprendidas de un AS proveedor o de otro AS con relación entre iguales.
3. Fíjate en la tabla BGP de `as50-r1`. ¿Cuántas rutas hay en la tabla BGP para alcanzar AS60?
4. Interrumpe `quagga` en `as20-r1`. Fíjate en la tabla BGP de `as50-r1`. ¿Cuántas rutas hay ahora en la tabla BGP para alcanzar AS60?
5. ¿Cuál es la ruta que aparece en la tabla de encaminamiento de `as50-r1` para alcanzar AS60?
6. Inicia `quagga` en `as20-r1`. Espera 2 minutos aproximadamente para que `as50-r1` y `as20-r1` hayan intercambiado la información de encaminamiento BGP. ¿Cuántas rutas hay en la tabla BGP para alcanzar AS60?
7. ¿Cuál es la ruta que aparece en la tabla de encaminamiento de `as50-r1` para alcanzar AS60?

8. ¿Es consistente esta ruta con las relaciones entre ASs definidas previamente?

9. Piensa en los atributos LOCAL PREF que configurarías en `as50-r1` y realiza dicha configuración en el escenario. Incluye la configuración en la memoria. Reinicia `quagga` en `as50-r1`.

10. Interrumpe `quagga` nuevamente en `as20-r1`. Fíjate en la tabla BGP de `as50-r1`. ¿Cuántas rutas hay en la tabla BGP para alcanzar AS60?

11. Inicia `quagga` en `as20-r1`. Espera 2 minutos aproximadamente para que `as50-r1` y `as20-r1` hayan intercambiado la información de encaminamiento BGP. ¿Cuántas rutas hay en la tabla BGP para alcanzar AS60?

12. ¿Cuál es la ruta que aparece en la tabla de encaminamiento de `as50-r1` para alcanzar AS60? Ahora debería ser consistente con las relaciones entre ASs definidas previamente.

13. Modifica la configuración de `as10-r1` para definir el parámetro `LOCAL_PREF` acorde a las relaciones que tiene con sus ASs vecinos. Incluye las modificaciones en la memoria.

14. Comprueba que después de realizar la configuración, `as10-r1` tiene como ruta preferida para alcanzar las subredes internas de AS60 a través de `as20-r1` (sin la configuración de `LOCAL_PREF`, en este caso la selección de ruta dependería del orden de arranque de los routers).

# 5. Rutas eliminadas

Con todas las máquinas arrancadas, después de realizar la configuración del apartado anterior, piensa qué anuncios BGP con las subredes internas de AS60 se enviarían si apagaras `as60-r1` y responde a las siguientes preguntas:

1. ¿A qué otros routers enviaría `as20-r1` un mensaje BGP con rutas eliminadas? ¿Por qué?

2. ¿A qué otros routers enviaría `as40-r1` un mensaje BGP con rutas eliminadas? ¿Por qué?

3. ¿A qué otros routers enviaría `as10-r1` un mensaje BGP con rutas eliminadas? ¿Por qué?

4. ¿A qué otros routers enviaría `as50-r1` un mensaje BGP con rutas eliminadas? ¿Por qué?

5. Inicia las siguientes capturas:

   - En `as20-r1(eth2)` guardando el contenido en `bgp-09.cap`.
   - En `as20-r1(eth3)` guardando el contenido en `bgp-10.cap`.
   - En `as40-r1(eth0)` guardando el contenido en `bgp-11.cap`.
   - En `as40-r1(eth1)` guardando el contenido en `bgp-12.cap`.
   - En `as40-r1(eth2)` guardando el contenido en `bgp-13.cap`.
   - En `as30-r1(eth3)` guardando el contenido en `bgp-14.cap`.

   Interrumpe la ejecución de `quagga` en `as60-r1`. Espera a que los routers intercambien toda la información de encaminamiento (al menos 2 minutos). Explica los mensajes UPDATE que encuentras en las capturas anteriores y que contengan información de las subredes de AS60 (16.X.0.0/24), indica qué router lo envía y por qué.

# 6. Ruta por defecto

1. Cambia la configuración de `as40-r1` de forma que AS40 anuncie a AS50 una ruta por defecto. No elimines aún los anuncios de las subredes individuales.

2. Reinicia `quagga` en `as40-r1` y observa la tabla de encaminamiento y la tabla BGP de `as50-r1`. Comprueba que en ambas tablas hay una ruta por defecto, pero siguen estando las rutas individuales. Las rutas a las subredes individuales, al ser más específicas serán las utilizadas, sin llegar a usarse nunca la ruta por defecto.

3. Cambia la configuración en `as40-r1` para evitar que siga anunciando a AS50 las subredes individuales.

4. Reinicia `quagga` en `as40-r1` y comprueba que la tabla de encaminamiento y la tabla BGP de `as50-r1` ahora sólo tienen la ruta por defecto.

# 7. Entrega de la práctica

Sube al enlace que encontrarás en `aulavirtual` antes de que termine el plazo de entrega, los siguientes ficheros:

- Memoria en formato pdf donde se explique razonadamente la resolución de cada uno de los apartados de este enunciado. Para ello, exporta a pdf la memoria que has escrito en la carpeta de OneDrive.

- Fichero de nombre `p3.zip` o `p3.tgz` resultado de comprimir **una carpeta de nombre p3** que contenga en su interior todos los ficheros de captura de tráfico: de `bgp-01.cap` a `bgp-14.cap`.

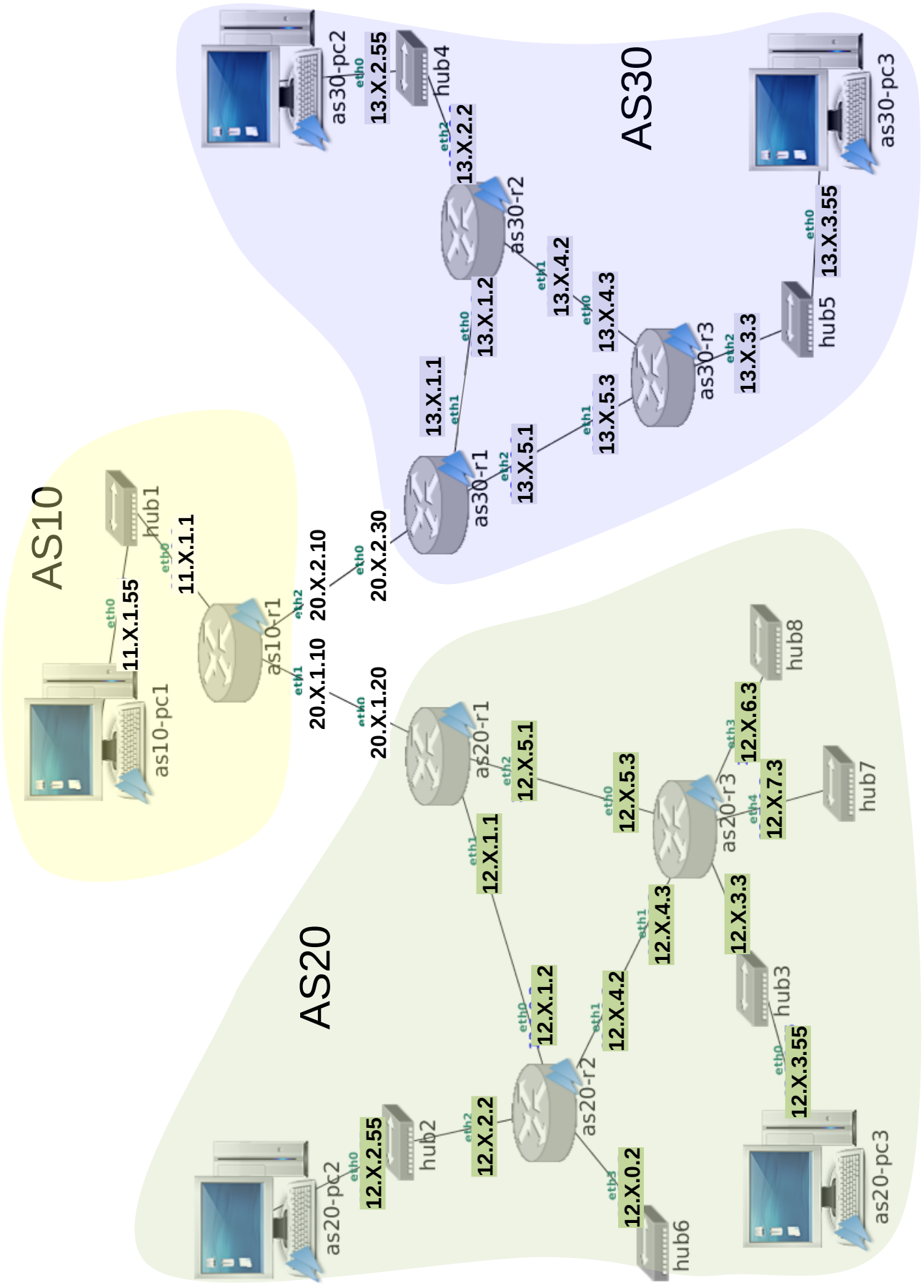



Figura 1: Escenario de red para los ejercicios de BGP

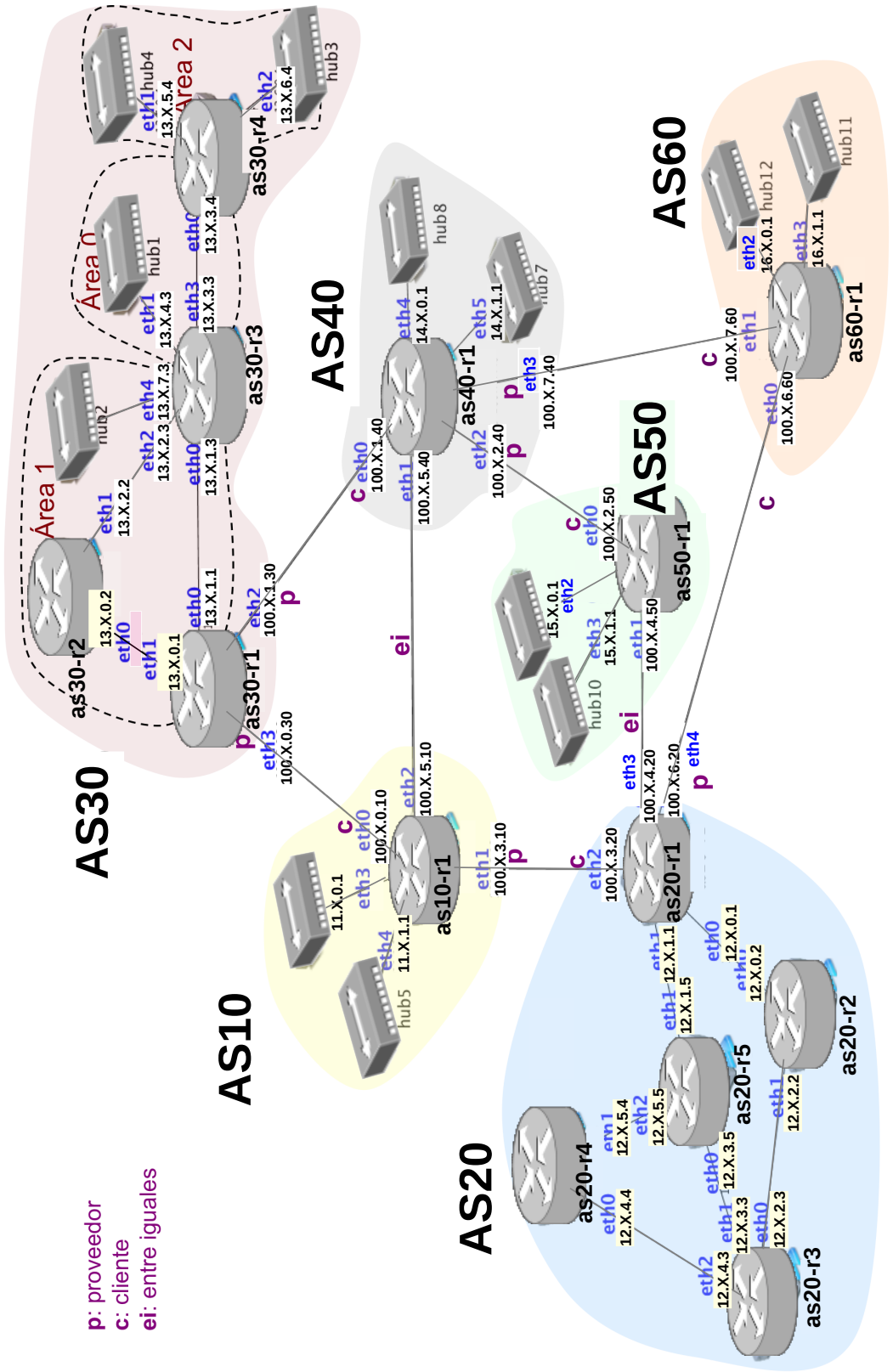



Figura 2: Escenario para listas de exportación y local pref en BGP

# Sistemas Telemáticos
# Práctica 4: Control de Congestión en TCP

GSyC
Departamento de Teoría de la Señal y Comunicaciones y Sistemas Telemáticos y Computación
URJC

Diciembre de 2023

## 1. Estados de una conexión TCP

En este apartado se observan los estados por los que va pasando un extremo de una conexión TCP.
Descomprime el escenario `estadosTCP-lab.tgz` y arranca las máquinas.

### 1.1. Establecimiento de la conexión

Una aplicación que funciona como servidor TCP comienza su ejecución aceptando conexiones de clientes. Hasta que haya alguna conexión de algún cliente la aplicación servidor TCP se encontrará en estado `LISTEN` y cambiará de estado en el momento en que el cliente se conecte.

Ve realizando los siguientes pasos, y responde en su momento a las preguntas que se indican:

1. Ejecuta `tcpdump` en `r1` en su interfaz `eth0`, no es necesario que guardes la captura en un fichero, especifica que sólo capture el tráfico TCP de la siguiente forma:

   ```
   tcpdump -i eth0 tcp
   ```

   Ensancha la ventana de `r1` todo lo que puedas para ver cada segmento capturado en una línea. Para interpretar la salida de `tcpdump` utiliza la información de la documentación adjunta ("Herramientas para el análisis de conexiones").

2. Arranca una aplicación servidor TCP que espere conexiones en el puerto 7777 en `pc2` utilizando la herramienta *netcat*, de la siguiente forma[1]:

   ```
   nc -l -p 7777 &
   ```

3. Para ver en qué estado se encuentran las conexiones TCP que tiene abiertas una máquina utilizaremos el comando `netstat -nat`. Para ejectuar repetidamente un comando utilizaremos el comando `watch`. Así, para comprobar el estado de la conexión TCP en el lado del servidor ejecuta en `pc2`:

   ```
   watch -n 0.5 netstat -nat
   ```

   La opción `-n` de `watch` permite especificar cada cuanto tiempo se repite la ejecución del comando que sigue a continuación; en este caso, cada 0.5 segundos.

4. Coloca en la pantalla las ventanas de los terminales de `pc1` y `pc2` para que puedas visualizarlas simultáneamente.

5. Explica en qué estado se encuentra la conexión en el servidor antes de arrancar el cliente.

6. Lanza en `pc1` una aplicación cliente TCP que se conecte al servidor de `pc2`:

   ```
   nc 12.0.0.2 7777
   ```

[1] La herramienta *netcat* (`nc`) permite lanzar de forma simple clientes o servidores de TCP o UDP, y se estudió en la asignatura de Arquitectura de Redes de Ordenadores.

7. Explica qué estados atraviesa el servidor hasta que el cliente se encuentra conectado [2].

8. Observa en el tráfico capturado en `r1` como se han intercambiado los 3 segmentos del establecimiento de la conexión.

9. Explica el valor de la ventana anunciada por el servidor.

10. Interrumpe la ejecución del comando `watch` en `pc2` con `Ctrl+C` y trae a primer plano de ejecución el comando `nc` en `pc2` ejecutando `fg`.

## 1.2. Intercambio de datos

Desde el cliente en `pc1` podemos escribir tantos datos como queramos por la entrada estándar para enviar a `pc2`. Vamos a comprobar que los datos que envía `pc1` a `pc2` se quedan almacenados en el buffer de recepción (*in*) de la conexión en el lado del servidor en `pc2` hasta que la aplicación servidor los lea.

Ve realizando los siguientes pasos, y responde en su momento a las preguntas que se indican:

1. Si has interrumpido la ejecución de `tcpdump` en `r1` en su interfaz `eth0`, vuelve a lanzarlo.

2. Detén la ejecución de `nc` en el lado servidor con `Ctrl+z`. Esto provocará que la ejecución del proceso servidor quede suspendida (pero no finalizada), y por tanto no realizará llamadas al sistema: en particular no leerá la información que reciba de TCP, que se irá acumulando en el buffer de recepción (*in*) de la conexión TCP.

3. Ejecuta en el lado servidor de nuevo el comando `netstat` de la siguiente forma:

```
watch -n 0.5 netstat -nat
```

4. En el proceso `nc` del cliente en `pc1` introduce una cadena de caracteres larga por la entrada estándar (por ejemplo pulsa un rato la tecla de alguna letra hasta que aparezcan 2 líneas enteras de esa letra por pantalla y después pulsa la tecla `Enter`). Esta cadena de caracteres se recibirá en la implementación de TCP en el lado servidor, pero la aplicación no leerá estos datos porque se encuentra detenida.

5. Fíjate en cómo los datos se han quedado almacenados en el *buffer* de recepción (*in*) del lado servidor (aparece etiquetado como `Recv-Q`).

   Explica el valor de `Recv-Q` teniendo en cuenta que has pulsado más caracteres para enviar en el cliente.

   Explica los segmentos enviados por el cliente que muestra la captura de tráfico de `r1`.

6. Interrumpe con `Ctrl+c` la ejecución de `netstat` en el lado servidor. Trae a primer plano la ejecución de `nc` en `pc2` (`fg`) y la ejecución de la aplicación servidor continuará. Observa cómo la aplicación servidor lee los datos del *buffer* de recepción (*in*) de la conexión y los muestra en la pantalla.

## 1.3. Finalización de la conexión

Ve realizando los siguientes pasos, y responde en su momento a las preguntas que se indican:

1. Si has interrumpido la ejecución de `tcpdump` en `r1` en su interfaz `eth0`, vuelve a lanzarlo.

2. Interrumpe la ejecución del cliente en `pc1` con `Ctrl+c`. La aplicación cliente mandará un segmento con el flag FIN activado.

3. El servidor `nc` está programado para terminar si el cliente le manda un segmento con el flag FIN activado, por este motivo, la aplicación `nc` en `pc2` finaliza la conexión mandando su segmento FIN+ACK. Cuando el servidor recibe el último ACK de `pc1` da por terminada la comunicación y finaliza su ejecución.

4. En `pc1` aunque la aplicación ha terminado, los recursos de la conexión TCP tardan un tiempo en liberarse y si ejecutas en `pc1`:

```
watch -n 0.5 netstat -nat
```

[2] Hemos añadido retardos a la interfaz de red de pc1 para que puedas visualizar esta transición entre estados ya que el cambio de estado normalmente se produce muy rápido y se aprecia fácilmente.

observarás que la conexión TCP tarda un tiempo en liberarse y fíjate en el estado en el que se encuentra.

Explica por qué se mantiene tanto tiempo en este estado.

5. En `pc2` la aplicación ha terminado y se han liberado inmediatamente los recursos de la conexión TCP. Si ejecutas en `pc2`:

```
watch -n 0.5 netstat -nat
```

observarás que ya no hay conexiones TCP abiertas en `pc2`.

Explica por qué ya no aparecen conexiones TCP en `pc2`.

## 2. Slow Start en el inicio de la conexión

En este apartado se observa el comportamiento del mecanismo de TCP arranque lento (*Slow Start*).

Carga en *Wireshark* la captura `slow-start.cap`. Ordena los paquetes por la columna `Time`. Selecciona el primer segmento que envía el cliente al servidor, y a continuación muestra en *Wireshark* el diagrama de la conexión mediante el menú: *Statistics→TCP Stream Graph→Time-Sequence Graph (tcptrace)*

Observa la gráfica de la captura, y cada uno de los segmentos. Trata de entender cómo afecta *Slow Start* el envío de nuevos segmentos desde que comienza la conexión.

Responde a las siguientes preguntas:

1. Indica el valor del *flightsize* en los siguientes instantes: 1'5s, 2'5s, 3'5s, 4'5s, 5s, 6s.
2. ¿En esta captura hay algún momento en que sea menor la ventana de control de flujo que la ventana de control de congestión?
3. ¿Por qué se envían inicialmente 3 segmentos con datos?
4. ¿Cuántos segmentos con nuevos datos se podrían enviar en el instante 3'5s?
5. ¿Cuántos segmentos con nuevos datos se podrían enviar en el instante 4'5s?

## 3. Control de Congestión tras Timeout

En este apartado se observa el comportamiento del mecanismo de control de congestión de TCP tras un *timeout*.

Carga en *Wireshark* la captura `ss-timeout.cap`. Ordena los paquetes por la columna `Time`.
Si en la columna "Protocol"ves en algunos paquetes el valor "Gryphon", desactiva el análisis de dicho protocolo en el menú: *Analize→Enabled Protocols*.
Selecciona el primer segmento que envía el cliente al servidor, y a continuación muestra en *Wireshark* el diagrama de la conexión mediante el menú: *Statistics→TCP Stream Graph→Time-Sequence Graph (tcptrace)*

1. Observa la captura y analiza cómo afecta *Slow Start* al envío de nuevos segmentos al inicio de la conexión. Entre el instante 3s y 3'5s se envían 6 segmentos. ¿Podrían haberse enviado más segmentos en ese instante? Razona la respuesta.
2. Localiza la retransmisión que se produce alrededor del instante 7'5s. Estudia el comportamiento de TCP tras el *timeout*. Analiza tanto la gráfica como cada uno de los segmentos. Responde a las siguientes preguntas:
   *a*) ¿Qué número de secuencia tiene el segmento retransmitido?
   *b*) ¿Qué valor se calcula para el umbral *ssthres*?
   *c*) ¿Qué tamaño tiene la ventana de congestión en el instante 8s?
   *d*) ¿Por qué se envían 2 segmentos alrededor del instante 9s?
   *e*) ¿Podría enviarse algún segmento más en el instante 9s? ¿Por qué?
   *f*) ¿En qué modo de control de congestión se haya la conexión en el instante 5s? ¿Por qué?
   *g*) ¿En qué modo de control de congestión se haya la conexión en el instante 10'5s? ¿Por qué?
3. ¿En qué modo de control de congestión termina la conexión?
4. ¿Qué valor aproximado tiene la ventana de congestión al final de la conexión?

# 4. Fast Retransmit / Fast Recovery

En este apartado se observa el comportamiento de TCP tras la recepción de 3 ACKs duplicados. Carga en wireshark la captura `fr-fr.cap` y ordena los paquetes de la captura según la columna `Time`.

Para identificar si una retransmisión es debida a *Fast Retransmit* comprueba las siguientes condiciones:

- Anteriormente a la retransmisión hay al menos 4 ACKs (1 + 3 duplicados) con el mismo número de ACK anteriores a la retransmisión de ese número de secuencia (condición necesaria).
- Se envían segmentos con nuevos datos después de la retransmisión y antes de recibir el ACK de lo retransmitido (condición suficiente).

*Wireshark* interpreta los segmentos TCP de las capturas e identifica si una retransmisión es debida a *Timeout* o *Fast Retransmit*. Sin embargo, a veces la captura no está bien ordenada según el eje temporal y las interpretaciones que hace *Wireshark* no son correctas. Por este motivo para saber por qué se produce una retransmisión es necesario analizar despacio los paquetes presentes en la captura.

Observando la captura, responde a las siguientes preguntas:

1. ¿Cuántas retransmisiones debidas a *timeout* se observan en la traza? Identifica en qué instante se producen.
2. ¿Cuántas retransmisiones debidas a *Fast Retransmit* se observan en la traza? Identifica en qué instante se producen.
3. Observa la primera ocasión en la que se produce *Fast Retransmit*. ¿En qué modo de control de congestión se entra tras efectuarse dicha retransmisión?
4. Poco después de producirse esa primera retransmisión debida a *Fast Retransmit* se envían nuevos segmentos de datos antes de recibir ningún ACK. ¿Cuántos nuevos segmentos de datos se envían? ¿Por qué se pueden enviar en ese instante? ¿Se podría enviar alguno más en ese periodo hasta que llegue el ACK del paquete retransmitido?
5. Observa en qué momento llega el primer ACK nuevo. ¿En qué modo de control de congestión se entra tras recibirse dicho ACK nuevo? Indica cuántos paquetes se envían en ese momento, y explica la razón de este número. Observa la evolución de la ventana de congestión desde este momento hasta la siguiente retransmisión.
6. Observa la segunda ocasión en la que se produce *Fast Retransmit*. Es en el paquete 114, aunque Wireshark no lo identifica correctamente. Estudia la evolución del control de congestión tras esta retransmisión.
7. Observa las otras 2 retransmisiones, que teambién son *Fast Retransmit*. Para cada una de ellas, estudia la evolución del control de congestión después de dicha retransmisión.

# 5. Control de Congestión y sondas de ventana

En este apartado se observa la interacción entre los mecanismos de control de flujo y de control de congestión de TCP.

Carga en wireshark la captura `sondas.cap`.

Observa la captura y comprueba el comportamiento de la ventana anunciada a partir del segmento 43. Responde a las siguientes preguntas:

1. Localiza en la traza los anuncios de ventana de tamaño 0 enviados por el servidor al cliente. ¿Qué segmentos son los que transportan estos anuncios?
2. Observa las sondas de ventana que envía el cliente en ese periodo. ¿Qué segmentos son los que transportan las sondas de ventana?
3. Estudia el comportamiento de TCP entre los segmentos 43 y 87. Responde a las siguientes preguntas:
   *a*) Indica cuál es el número de byte más alto que puede enviarse tras recibirse los siguientes segmentos: 41, 43, 51, 79.x
   *b*) ¿Cuántos bytes nuevos pueden enviarse tras recibirse el segmento 80?
   *c*) ¿Cuántos bytes de datos transportan los segmentos con sondas de ventana?

*d*) Tras haberse cerrado la ventana, ¿en qué segmento vuelve a abrirse? ¿Cuál es el tamaño de la nueva ventana anunciada?

*e*) Tras recibirse el segmento 84, ¿qué limita al emisor, la ventana de control de flujo o la de congestión?

4. Indica en qué modo de control de congestión se encuentra la conexión TCP en los siguientes puntos:

   *a*) Antes del segmento 43.

   *b*) Entre el segmento 43 y 87

   *c*) Después del segmento 87

5. Indica en qué momentos de la conexión es la ventana de control de flujo la que limita al emisor, y en cuáles es la ventana de control de congestión.

# 6. ACKs selectivos (SACK)

En este apartado se observa el comportamiento de SACKs en TCP, en la implementación *New Reno*.

Carga en *Wireshark* la captura `sack.cap`. Es muy importante que ordenes los segmentos según la columna `Time`, ya que Wireshark los tiene ordenados según el número de segmento.

Podrás encontrar los segmentos que contienen asentimientos selectivos (SACK) en la captura si en la caja `Filter` de Wireshark escribes `tcp.options.sack` y pulsas `<Intro>`. Además, en versiones antiguas de wireshark (versiones anteriores a la 2.0.0, como las que existían en distribuciones Linux basadas en Ubuntu 14.04 o anteriores), en la gráfica *tcptrace* se identifican fácilment la información de los asentimientos selectivos mediante trazos azules. En futuras versiones de wireshark (versiones posteriores a la 2.3.0) se identificarán también estos segmentos en la gráfica mediante trazos rojos.

NOTA: En distribuciones Ubuntu o Linux Mint recientes, si ejecutas `wireshark-gtk` en vez de `wireshark` (tras instalar el paquete con `sudo apt-get install wireshark-gtk`), podrás acceder a las gráficas *tcptrace* antiguas en vez de a las modernas.

Responde de forma razonada a las siguientes preguntas:

1. Dado que SACK es una opción que pueden usar ciertas implementaciones de TCP, indica cómo indica un extremo de la conexión que acepta asentimientos selectivos del otro extremo. ¿En qué segmentos de la conexión ocurre ese acuerdo? ¿Qué número de opción de TCP se utiliza?
2. Indica cuál es el primer segmento de la captura donde se muestran asentimientos selectivos. ¿En qué lugar del segmento va esta información? ¿Qué número de opción se utiliza? ¿Qué números de secuencia se están asintiendo y qué números de secuencia se asienten selectivente? ¿Qué números de segmento son los que se están asintiendo, y cuáles se asienten selectívamente?
3. Explica si el segmento 78 es una retransmisión por timeout o es una retransmisión rápida.
4. Explica en qué modo de control de congestión está la máquina 11.0.0.10 justo después de haber enviado el segmento 78. Indica el valor de `threshold` en ese instante.
5. Justo antes de enviar el segmento 83, ¿qué segmentos puede suponer la máquina 11.0.0.10 que le faltan a 13.0.0.10?
6. Si 11.0.0.10 sabe que a 13.0.0.10 le faltan varios segmentos, ¿por qué justo después de enviar el segmento 83 no retransmite todos los que sabe que le faltan?
7. Explica si el segmento 262 es una retransmisión por timeout o es una retransmisión rápida.
8. Explica en qué modo de control de congestión está la máquina 11.0.0.10 justo después de haber enviado el segmento 262. Indica el valor de `threshold` en ese instante.
9. Al recibir el segmento 257, ¿qué segmento/s puede suponer la máquina 11.0.0.10 que le falta/n a 13.0.0.10?
10. A recibir el segmento 259, ¿qué segmento/s puede suponer la máquina 11.0.0.10 que le falta/n a 13.0.0.10?
11. Fíjate en la diferencias que hay entre el segmento 257 y 259. ¿Qué crees que ha provocado que la máquina 13.0.0.10 haya enviado ese asentimiento?
12. A recibir el segmento 277, ¿qué segmento/s puede suponer la máquina 11.0.0.10 que le falta/n a 13.0.0.10?
13. Al recibir el segmento 669, ¿qué segmento/s puede suponer la máquina 11.0.0.10 que le falta/n a 13.0.0.10?
14. Explica si el segmento 747 es una retransmisión por timeout o es una retransmisión rápida.
15. ¿Por qué hay 2 retransmisiones juntas (segmentos 747 y 749)?

## 7. Entrega de la práctica

Sube al enlace que encontrarás en `aulavirtual` antes de que termine el plazo de entrega, un único fichero `p4.pdf` con la memoria de la práctica **en formato PDF**.

# Sistemas Telemáticos
# Práctica 5: HTTP

GSyC
Departamento de Teoría de la Señal y Comunicaciones
y Sistemas Telemáticos y Computación

Diciembre de 2023

Cuando un mensaje HTTP ocupa más de un segmento TCP, Wireshark muestra el siguiente mensaje por cada uno de los segmentos TCP que son parte de dicho mensaje HTTP:

`[TCP segment of a reassembled PDU]`

Cuando Wireshark interpreta que se ha recibido todo el mensaje HTTP, como resultado de haber recibido previamente un conjunto de segmentos `TCP segment of a reassembled PDU`, Wireshark concatena todos estos segmentos para mostrar el mensaje HTTP completo.

Por ejemplo, en la figura 1 se puede ver como en el segmento 8 se muestra todo el mensaje HTTP que en realidad viajaba en 3 segmentos TCP: segmento 4, 6 y 8.

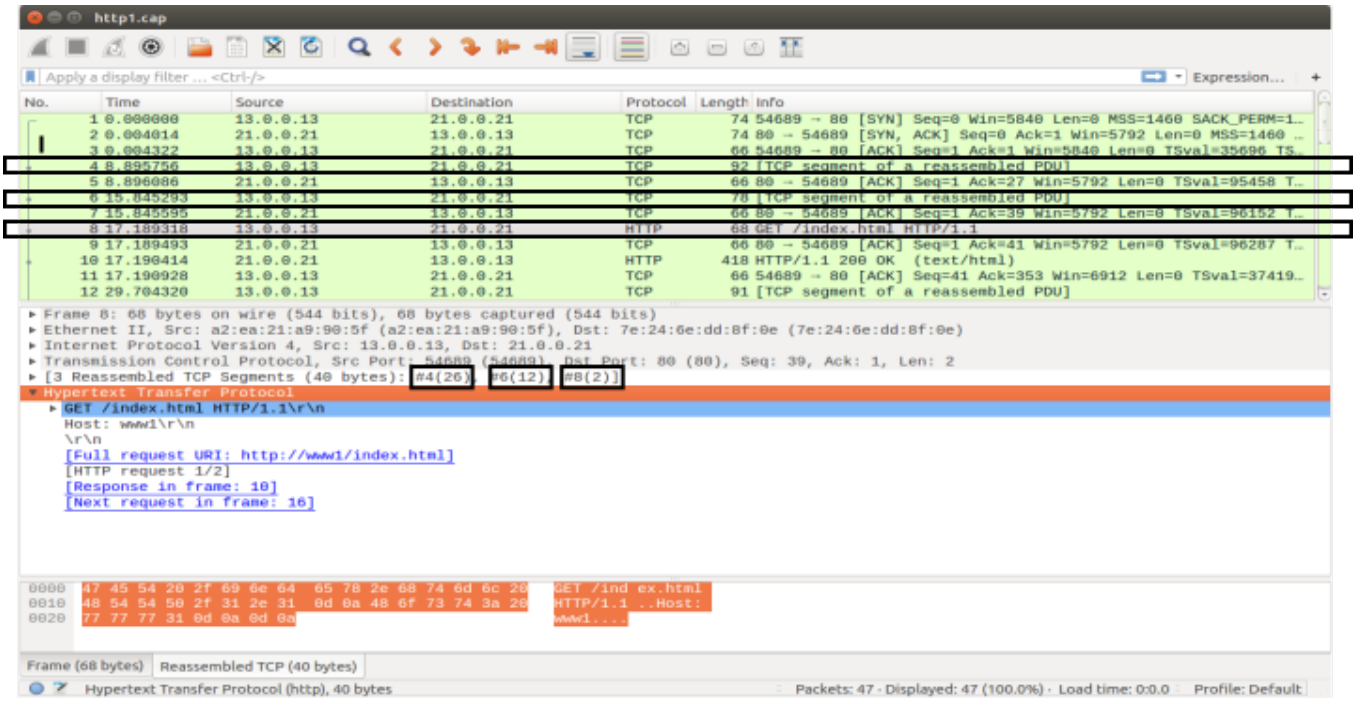



Figura 1: Mensaje HTTP compuesto de varios segmentos.

# 1. Comunicación cliente-servidor HTTP

Abre la captura `http1.cap` y responde a las siguientes preguntas:

1. Indica qué dirección IP es la de la máquina cliente HTTP y cuál la del servidor.
2. Indica qué versión HTTP están utilizando cliente/servidor
3. Indica el número de conexiones que se ven en el fichero de captura, y si los recursos del mismo servidor se transfieren todos por la misma conexión TCP o se usa conexión TCP diferente para cada uno.
4. ¿Cuántas peticiones GET observas desde el cliente?
5. ¿Cuántas URLs crees que ha escrito el usuario en el navegador para obtener dicha captura? ¿Cuál/es? ¿Por qué?
6. Fíjate en el contenido de la página `index.html` que se ha descargado el cliente. ¿Qué crees que ocurrirá cuando el navegador se haya descargado `index.html`?

Abre la captura `http2.cap` y responde a las siguientes preguntas:

7. Indica qué versión HTTP están utilizando cliente/servidor
8. Indica el número de conexiones que se ven en el fichero de captura, y si los recursos del mismo servidor se transfieren todos por la misma conexión TCP o se usa conexión TCP diferente para cada uno.

# 2. Diferentes tipos de respuestas de un servidor

Arranca el navegador Firefox. Abre una pestaña nueva y selecciona en el menú de la aplicación → Más herramientas → Herramientas para el desarrollador. La página se habrá dividido en 2 partes. La parte superior es la que muestra normalmente el navegador, la parte inferior contiene información de los mensajes HTTP intercambiados entre cliente y servidor. Selecciona la pestaña 'Red' y 'HTML', véase figura 2.


Figura 2: Herramientas para el desarrollador.

Esta vista del navegador te permitirá cargar una URL y observar todos los mensajes HTTP que se están intercambiando al cargar una página.

Selecciona la pestaña 'Todos', para ver todos los recursos descargados al solicitar una página y explica lo que ocurre al cargar las siguientes URLs:

1. Dentro de esa pestaña carga la página `http://www.google.es/prueba`. Selecciona dentro de las herramientas del desarrollador la petición GET y la pestaña Cabeceras, véase figura 3.

   Fíjate en el campo 'Estado' que indica el tipo de respuesta recibida y explica su contenido.

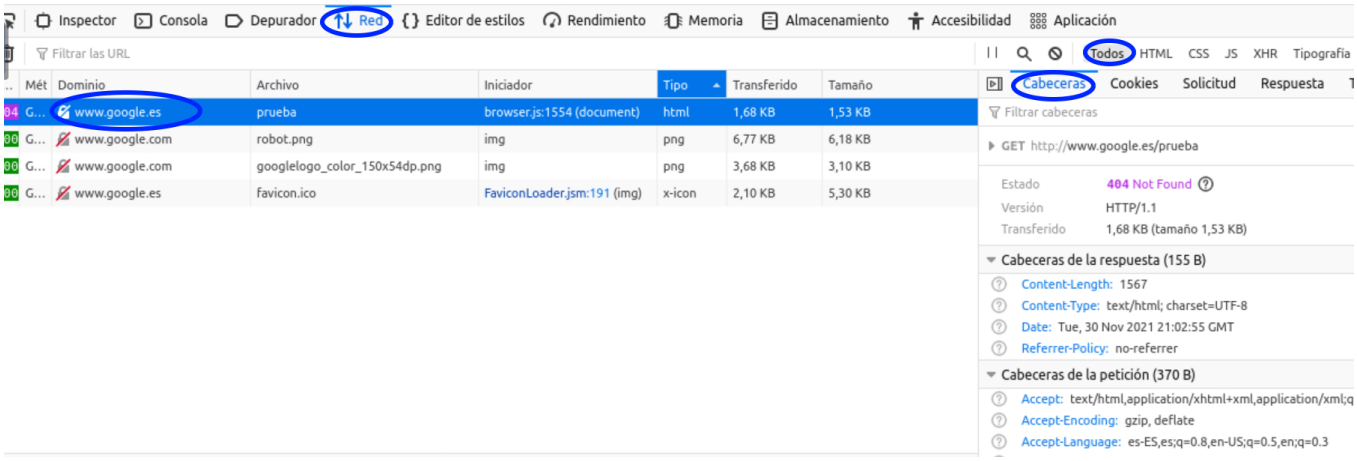



Figura 3: Cabeceras HTTP.

2. En esa misma pestaña carga la página `http://www.wikipedia.com`. Explíca qué ocurre en la primera petición GET y a partir de las líneas de cabecera que ves en la respuesta, explica la segunda petición GET. Fíjate en el lado de la derecha en el "Estado", pulsa en el deslizador "Sin procesar" para ver las cabeceras de la petición y de la respuesta tal y como han sido transmitidas.

# 3. Formularios en HTTP

Abre la captura `http3.cap` y responde a las siguientes preguntas:

1. Indica el número de conexiones entre cliente y servidor que aparecen en la captura.
2. Busca en la captura el segmento donde el servidor le envía al cliente un formulario. Indica los nombres de los campos del formulario que rellenará el usuario.
3. Indica si es el cliente o el servidor el que decide cómo debe enviar el cliente los datos del formulario (GET/POST) . ¿Qué método están usando en este caso? ¿Cómo lo sabes?
4. Busca en la captura el segmento donde el cliente le envía los datos del formulario al servidor y comprueba que se está realizando con el método GET
5. Fíjate cómo se llama el programa del servidor que va a recibir esos datos.
6. ¿Dónde viajan los datos que el cliente le envía al servidor? ¿Cuáles son esos datos?
7. Indica qué cabecera es la que representa el tipo de contenido del mensaje que el cliente envía al servidor con los datos del formulario.

Abre la captura `http4.cap` y responde a las siguientes preguntas:

9. Busca en la captura el segmento donde el servidor le envía al cliente un formulario. Indica los nombres de los campos del formulario que rellenará el usuario.
10. Indica si es el cliente o el servidor el que decide cómo debe enviar el cliente los datos del formulario (GET/POST) . ¿Qué método están usando en este caso? ¿Cómo lo sabes?

11. Busca en la captura el segmento donde el cliente le envía los datos del formulario al servidor y comprueba que se está realizando con el método POST.

12. Fíjate cómo se llama el programa del servidor que va a recibir esos datos.

13. Indica qué cabecera es la que representa el tipo de contenido que el cliente envía al servidor y cuál es su valor.

14. Indica en qué parte del mensaje van los datos del formulario que el cliente le envía al servidor.

15. Explica si en este caso es necesario la cabecera `Content-Length` en el mensaje HTTP que el cliente envía al servidor con los datos del formulario. ¿Por qué?

16. Observa si el servidor le manda alguna respuesta cuando recibe los datos del formulario del cliente. En caso afirmativo localiza el número de segmento y observa en las cabeceras HTTP: tipo de contenido, longitud y cuerpo del mensaje

# 4. Cookies

## 4.1. Almacén de cookies en el navegador Firefox

Para ver las Cookies en el navegador Firefox, selecciona la opción de menú de la aplicación: Editar → Ajustes. En la zona de la izquierda selecciona la pestaña "Privacidad y seguridad". Dentro de la sección "Cookies y datos del sitio" pulsa en "Administrar Datos". Podrás consultar la lista de sitios de los que tienes cookies almacenadas actualmente. Mira si tienes cookies del sitio web del Ayuntamiento de Fuenlabrada `ayto-fuenlabrada.es` (si las tienes, elimina sólo esas cookies).

NOTA: En las últimas versiones de Firefox sólo puede saberse si para un sitio hay almacenadas cookies, pero no los datos de las cookies almacenadas.

Abre una pestaña nueva y selecciona en el menú de la aplicación → Más herramientas → Herramientas para el desarrollador. Selecciona la pestaña 'Red' y 'HTML', igual que se muestra en la figura 2.

Dentro de esa pestaña carga la página `http://www.ayto-fuenlabrada.es/`. Selecciona dentro de las herramientas del desarrollador la petición GET y la pestaña Cabeceras, véase la figura 4.

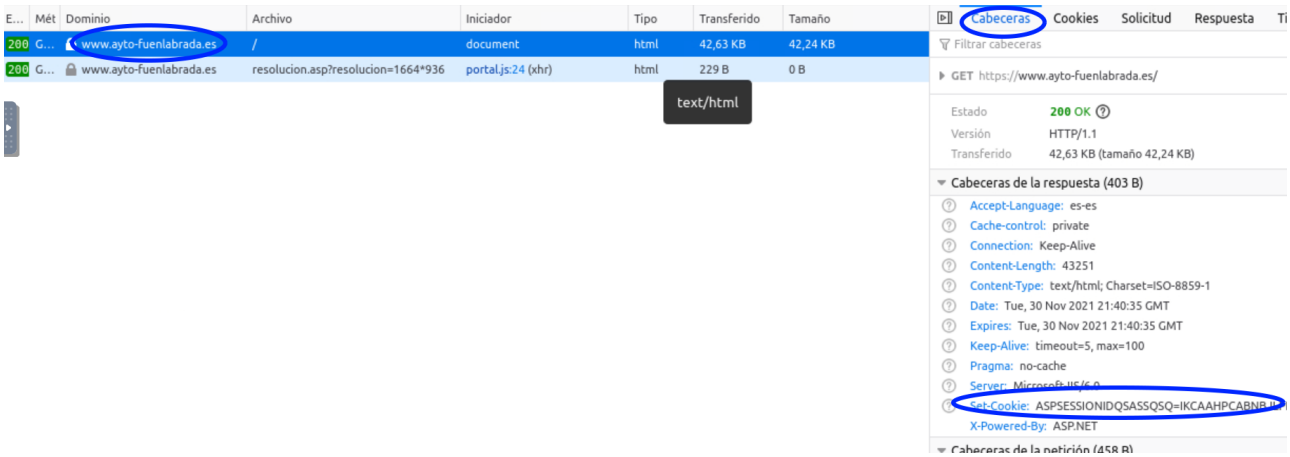



Figura 4: Cookies

1. Fíjate en la línea de cabecera que el servidor le envía al cliente con el contenido de las cookies.

2. Pulsa sobre la pestaña “Cookies” para poder ver de forma más clara el contenido de las cookies. Copia los campos importantes. Fíjate que no hay fecha de expiración, eso quiere decir que la Cookie se eliminará cuando se cierre el navegador.

3. Selecciona ahora la herramienta de desarrollador “Almacenamiento” y en el panel de la izquierda despliega “Cookies” para ver las cookies obtenidas al descargar esta página, véase la figura 5.

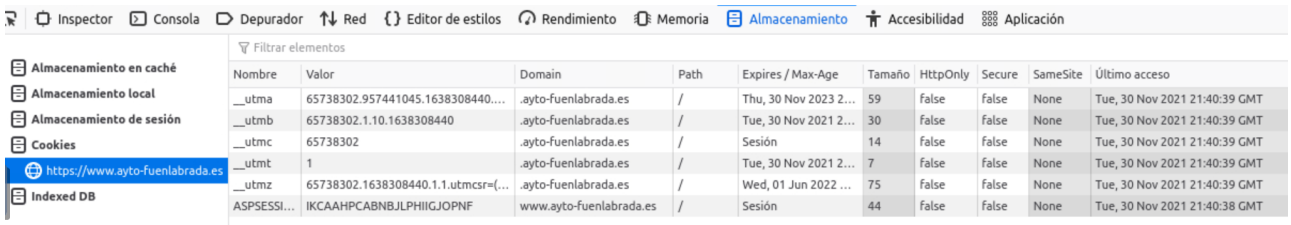



Figura 5: Almacenamiento de Cookies

Señala qué cookies has obtenido para el sitio `ayto-fuenlabrada.es`. Todas las cookies que en este caso comienzan por `__` son debidas a que el sitio web usa Google Analytics, es decir, al descargar la página del Ayuntamiento de Fuenlabrada se ha descargado también una biblioteca en javascript que ha creado estas cookies para este sitio web dentro de nuestro navegador. Estas cookies permiten medir la interacción de los usuarios con el sitio web. No te fijes en esas cookies de Google Analytics.

4. Vuelve a la herramienta de desarrollador “Red” y pulsa sobre la segunda petición GET que aparece, y observa las cookies que se envían. Usa también la pestaña Cookies para poder ver mejor los valores que se envían.

   NOTA: Sólo pueden conocerse los detalles de las cookies que se obtienen del sitio concreto observado con las herramientas del desarrollador[1].

## 4.2. Envío de Cookies en mensajes HTTP

Abre la captura `http5.cap` y responde a las siguientes preguntas:

1. Indica qué cookies envía el servidor al cliente:
2. Indica qué cookies enviará el cliente al servidor cuando acceda a la página con la URL: `http://elcortebritanico/tienda/index.html`
3. ¿Y si el cliente accediera en el año 2025 a dicha URL?
4. ¿Y si el cliente accediera en el año 2035 a dicha URL?

Abre la captura `http6.cap` y responde a las siguientes preguntas:

5. Indica qué cookies el cliente está enviando al servidor.
6. ¿Por qué crees que le envía dichas cookies?

[1]Si quieres consultar todos los datos de todas las cookies almacenadas en el navegador prueba a instalarte la extensión ”Cookie Quick Manager”de Firefox:
https://addons.mozilla.org/es/firefox/addon/cookie-quick-manager/

7. Escribe un ejemplo de la posibles cabeceras que le habrá enviado dicho servidor al cliente previamente.

8. A partir de la información de la captura ¿crees que si el cliente accede a otra página con la URL: `http://www2/dir1/dir2/index.html` enviaría esas cookies, más o menos?

9. A partir de la información de la captura ¿crees que si el cliente accede a otra página con la URL: `http://www2/index.html` enviaría esas cookies, más o menos?

10. A partir de la información de la captura ¿crees que si el cliente accede a otra página con la URL: `http://www/index.html` enviaría esas cookies, más o menos?

# 5. Comunicación a través de un Proxy HTTP

Abre la captura `http7.cap` y responde a las siguientes preguntas:

1. Indica qué dirección IP es el cliente, el proxy y el servidor final.

2. ¿Qué diferencia la petición HTTP que realiza el cliente de la petición que realiza el proxy?

3. Identifica el nombre de la máquina donde se encuentra el servidor HTTP.

4. ¿Se puede saber de la petición que realiza el proxy que dicho proxy tiene almacenada en su caché esa página?

Abre la captura `http8.cap` y responde a las siguientes preguntas:

5. Indica el número de conexiones entre cliente y servidor que aparecen en la captura.

6. Explica qué es lo que se está descargando el cliente del servidor HTTP y cuantos objetos se descarga.

7. Observa en las cabeceras HTTP el tipo de contenido de cada uno de los objetos.

8. ¿Podrías saber si los paquetes capturados se corresponde a la comunicación entre un cliente y un proxy HTTP, entre un cliente y servidor final HTTP o entre un proxy y el servidor final HTTP? ¿Por qué?

9. Sabiendo que la comunicación se ha realizado a través de un proxy HTTP, mira las cabeceras HTTP que envía dicho proxy para ver si en ellas existe alguna que muestre cuál es su nombre.

Abre la captura `http9.cap` y responde a las siguientes preguntas:

10. ¿Podrías saber si los paquetes capturados se corresponde a la comunicación entre un cliente y un proxy HTTP, entre un cliente y servidor final HTTP o entre un proxy y el servidor final HTTP? ¿Por qué?

# 6. Cachés en HTTP

## 6.1. Caché en un proxy HTTP

Estudia las capturas `http10.cap` y `http11.cap`, teniendo en cuenta que las direcciones 11.0.0.1 y 12.0.0.1 corresponden a la misma máquina. Responde a las siguientes preguntas:

1. Indica cuáles son las direcciones IP del cliente, proxy y servidor web. ¿Cómo lo sabes?
2. Explica qué es lo que ocurre en estas capturas.
3. Localiza los campos relevantes con respecto al tratamiento de caché que incluye en las líneas de cabecera el servidor. ¿Qué significan?
4. Explica qué ocurre en la segunda consulta que realiza el cliente.
5. Viendo los paquetes 14 y 16 de la captura `http10.cap` indica cómo se puede saber que el contenido proviene de una caché.
6. ¿Crees que el cliente tiene caché?

# 7. Entrega de la práctica

Sube al enlace que encontrarás en `aulavirtual` antes de que termine el plazo de entrega, un único fichero `p5.pdf` con la memoria de la práctica **en formato PDF**.

# Sistemas Telemáticos
# Práctica 6a: Claves

Departamento de Teoría de la Señal y Comunicaciones
y Sistemas Telemáticos y Computación
(GSyC)

Diciembre de 2023

Antes de comenzar a realizar la práctica, deberás acceder a la **carpeta con tu nombre y apellidos que los profesores hemos compartido a través de OneDrive** y crear un nuevo documento de Word llamado: memoria-p5.docx

Usarás este documento para ir escribiendo en el mismo el trabajo que vayas realizando en esta práctica. Como es un documento compartido con los profesores, nosotros podremos ir revisando de forma gradual tu trabajo. Es obligatorio ir escribiendo los resultados de vuestra práctica según la vayáis realizando en este documento. Por favor, **no uséis ningún otro documento de forma temporal para ir escribiendo vuestros resultados**.

## 1. Ejercicio 1

Se ha diseñado un sistema de comunicación que pretende que los usuarios puedan intercambiar información de manera anónima. El objetivo es dificultar que alguien que intercepte uno de los mensajes pueda conocer qué nodo envió originalmente el mensaje, ni cuál es el destinatario final del mismo, ni cuál es el contenido del mensaje.

Para conseguir este objetivo el mensaje se va enviando a través de una serie de nodos, elegidos por el nodo origen de la comunicación.

El nodo origen de una comunicación tiene que indicar en el mensaje que envía dos tipos de información:

- La secuencia de nodos que tiene que seguir el mensaje que envía
- El Contenido del Mensaje, que incluye la dirección del nodo que envía originalmente el mensaje, y el texto del mensaje.

Cuando un nodo recibe un mensaje, tiene que enviárselo al primero de los nodos especificados en la secuencia de nodos que viene en el mensaje, eliminando la primera entrada de la secuencia de nodos antes de enviar el mensaje.

**Ejemplo** con 5 ordenadores, $X, B, C, D, Z$, con direcciones IP $IP_X, IP_B, IP_C, IP_D, IP_Z$ respectivamente:

Supongamos que $X$ quiere enviar el texto $mensajeParaZ$ a $Z$ a través de la ruta $X \Rightarrow B \Rightarrow C \Rightarrow D \Rightarrow Z$, y que $X$ conoce $K_B^+, K_C^+, K_D^+, K_Z^+$.

1º) $X$ le envía a $B$ un datagrama IP en cuyo campo de datos va la siguiente información:
   - Secuencia de nodos: $\boxed{K_B^+(IP_C) \mid K_C^+(IP_D) \mid K_D^+(IP_Z) \mid K_Z^+(IP_Z)}$
   - Contenido del Mensaje: $\boxed{K_Z^+(IP_X, mensajeParaZ)}$

2º) $B$ descifra el primer componente de la secuencia de nodos recibida, y aprende que el siguiente salto es $C$. $B$ le envía entonces a $C$ un datagrama IP con la siguiente información en su campo de datos:
   - Secuencia de nodos: $\boxed{K_C^+(IP_D) \mid K_D^+(IP_Z) \mid K_Z^+(IP_Z)}$
   - Contenido del Mensaje: $\boxed{K_Z^+(IP_X, mensajeParaZ)}$

3º) $C$ descifra el primer componente de la secuencia de nodos recibida, y aprende que el siguiente salto es $D$. $C$ le envía a $D$:
   - Secuencia de nodos: $\boxed{K_D^+(IP_Z) \mid K_Z^+(IP_Z)}$
   - Contenido del Mensaje: $\boxed{K_Z^+(IP_X, mensajeParaZ)}$

4º) $D$ descifra el primer componente de la secuencia de nodos recibida, y aprende que el siguiente salto es $Z$. $D$ le envía a $Z$:

- Secuencia de nodos: $\boxed{K_Z^+(IP_Z)}$
- Contenido del Mensaje: $\boxed{K_Z^+(IP_X, mensajeParaZ)}$

5º) $Z$ descifra el primer y único componente de la secuencia de nodos recibida, y aprende que él es el nodo destinatario. Entonces $Z$ descifra el Contenido del Mensaje, sabiendo así que el mensaje lo ha enviado originalmente $IP_X$, y que el mensaje que le quería transmitir a $Z$ era $mensajeParaZ$.

## Preguntas

1. Explica si el nodo receptor del mensaje $Z$ puede o no descifrar el mensaje para acceder a su contenido.
2. Explica si el nodo receptor del mensaje $Z$ estar seguro de la confidencialidad del mensaje, es decir, de que ningún otro nodo ha podido descifrarlo.
3. Explica si el nodo receptor del mensaje $Z$ puede autenticar al nodo emisor del mensaje $X$.
4. Explica si el nodo receptor del mensaje $Z$ puede estar seguro de la integridad del mensaje, es decir, que ningún otro nodo ha podido alterar el contenido del mensaje.
5. Explica si un nodo cualquiera que intercepte un mensaje destinado al nodo $Z$ puede conocer el texto del $mensajeParaZ$.
6. Explica si un nodo cualquiera que intercepte un mensaje destinado al nodo $Z$ puede conocer el destino final del mensaje.
7. Explica si un nodo cualquiera que intercepte un mensaje destinado al nodo $Z$ puede conocer el nodo que creó el mensaje.

# 2. Ejercicio 2

En una sistema existen las siguientes autoridades de certificación CA1 y CA2, ambas autoridades de certificación han incluido sus propios certificados autofirmados en las aplicaciones de comunicaciones que se usan dentro de este sistema.

Alicia tiene un certificado de su clave pública firmado por CA1 y Roberto tiene un certificado de su clave pública firmado por CA2.

Cuando Alicia se quiere comunicar con Roberto elige una clave simétrica de sesión para la comunicación que quiere establecer, $K_s$. Ésta es la clave que usará para convertir sus mensajes en confidenciales.

## Preguntas

1. Indica cómo crees que debería enviarle la clave $K_s$ de Alicia a Roberto.
2. Alicia no tiene la clave pública de Roberto ni Roberto la de Alicia. Indica cómo podría conseguir Alicia la $K_R^+$, sin quedar físicamente para intercambiarse las claves, y como puede Alicia estar segura de que esta clave se corresponde con la de Roberto.
3. Con este sistema, ¿puede estar Alicia segura de que los mensajes que envía a Roberto son confidenciales y de que en realidad se está comunicando con Roberto? En caso negativo, explica cómo conseguirías estas propiedades en los mensajes enviados desde Alicia a Roberto.
4. Con este sistema, ¿puede estar Roberto seguro de que los mensajes son confidenciales y provienen de Alicia? En caso negativo, explica cómo conseguirías estas propiedades en los mensajes enviados desde Alicia a Roberto.
5. El certificado de la clave públicad de Roberto ha caducado y ya no es válido. Roberto decide cambiar de autoridad de certificación y consigue un certificado de su clave pública emitido por la autoridad de certificación CA3. Esta autoridad de certificación CA3 no ha incluido su certificado autofirmado en las aplicaciones de comunicaciones del sistema, pero CA3 tiene un certificado de la clave pública de CA3 firmado por CA2. Indica si ahora Alicia podría enviar a Roberto mensajes confidenciales y auténticos y explica cómo lo haría.

## 3. Ejercicio 3

Abre el navegador Firefox y a través del menú selecciona la opción: Editar → Preferencias → Privacidad y Seguridad → Seguridad → Certificados → Ver Certificados.

En la pestaña "Autoridades" verás los certificados de las autoridades de certificación de primer nivel. Cualquier certificado que venga firmado por las autoridades de certificación que se encuentran en esta pestaña podrá ser verificado ya que se poseen de forma fiable las claves públicas de estas autoridades de certificación que permiten comprobar las firmas.

1. Escribe en la URL del navegador la siguiente dirección: `www.amazon.es`, una vez que se haya cargado la página verás junto a la URL un candado verde, pulsa sobre él y luego sobre la flecha derecha al lado de "Conexión segura" ("Mostrar detalles de la conexión"). Indica cuál es la autoridad de certificación que ha verificado esta conexión segura.

2. En esa ventana de detalles de la conexión, pulsa sobre el botón "Más información" y luego en "Ver Certificado" y en la pestaña "Detalles". Indica cuál es la jerarquía de certificados que se está utilizando para verificar a Amazon. Selecciona empezando por www.amazon.es el campo "Emisor" y ve comprobando quiénes han sido las entidades que han generado los certificados que aparecen en la jerarquía. Comprueba la cadena de todos los certificados. Señala qué certificados de la jerarquía están autofirmados.

3. Vuelve a visitar la información de certificados de las Preferencias (Editar → Preferencias → Privacidad y Seguridad → ... → Ver Certificados). Observarás que las dos entidades que aparecen en la jerarquía de certificados de Amazon tienen instalado su certificado. Una de ellas muestra su certificado como `Builtin object token`, es decir, se trata de un certificado autofirmado de una autoridad de certificación raíz que venía instalado con la aplicación Firefox. El otro certificado se muestra como `Disp. software de seguridad`, por lo que no es un certificado autofirmado y la entidad que lo ha firmado es una autoridad de certificación raíz. Indica cuál de ellos es `Builtin object token` y cuál es `Disp. software de seguridad`.

## 4. Entrega de la práctica

Sube al enlace que encontrarás en `aulavirtual` antes de que termine el plazo de entrega:

- Memoria en **formato pdf** donde se explique razonadamente la resolución de cada uno de los apartados de este enunciado. Para ello, exporta a pdf la memoria que has escrito en la carpeta de OneDrive.

# Sistemas Telemáticos para Medios Audiovisuales
# Práctica 6b: Cortafuegos *(firewalls)*

GSyC
Departamento de Teoría de la Señal y Comunicaciones y Sistemas Telemáticos y Computación
URJC

Diciembre de 2023

Antes de comenzar, descarga tu escenario del siguiente enlace donde deberás introducir tu número de DNI (8 dígitos) con la letra correspondiente:

`https://mobiquo.gsyc.urjc.es/practicas/stma/p6.html`

En la figura 1 se representa un conjunto de subredes y máquinas (`pc1`, `pc2`, `pc4`, `pc5`, `r1`, `r2` y `firewall`) que pertenecen a una determinada empresa y su conexión a Internet a través de la máquina `firewall`. La empresa tiene definidas un conjunto de subredes de ámbito privado:

- 10.X.0.0/24: `r1(eth1)`, `pc1`, `pc2`
- 10.X.1.0/24: `firewall(eth0)`, `r1(eth0)`, `r2(eth0)`
- 10.X.2.0/24: `r2(eth1)`, `pc3`

Adicionalmente, la empresa tiene las máquinas `pc4` y `pc5` que se encuentran en una subred pública: 100.X.0.0/24. Estas máquinas proporcionan servicios básicos de la empresa: servidor de HTTP y servidor de fecha y hora. A este tipo configuración, donde la empresa tiene una o varias subredes públicas para ofrecer servicios a Internet se le denomina zona desmilitarizada o DMZ (DeMilitarized Zone).

Todas las máquinas de la empresa se conectan a Internet a través de la máquina `firewall` y la subred 100.X.1.0/24.

En este escenario, se considera que Internet está formado por las siguientes máquinas: `r3`, `r4`, `r5`, `pc6` y `pc7` que se encuentran conectadas a las siguientes subredes públicas:

- 100.X.1.0/24: `r3(eth0)`
- 100.X.2.0/24: `r3(eth1)`, `r5(eth2)`
- 100.X.3.0/24: `r3(eth2)`, `r4(eth2)`
- 100.X.4.0/24: `r4(eth1)`, `r5(eth0)`
- 100.X.5.0/24: `r4(eth0)`, `pc6`
- 100.X.6.0/24: `r5(eth1)`, `pc7`

Arranca de una en una todas las máquinas de la figura.

# 1. Introducción

A continuación se proporcionan algunos consejos para facilitar la realización de la práctica.

## 1.1. Edición y ejecución de *scripts*

En esta práctica se configurará la máquina `firewall` para que actúe como traductor de direcciones y como cortafuegos. Habrá que definir varias reglas utilizando `iptables`. Por este motivo, es recomendable guardar dichas reglas en un fichero *script de shell*.

Para hacer un *script de shell* crea un fichero de texto de nombre, por ejemplo, `fw.sh`, editándolo con `nano` o `mcedit`.

La primera línea del fichero debe ser `#!/bin/sh` y las siguientes líneas serán la definición de las reglas para `iptables` tal y como se escribirían en el terminal:

```
#!/bin/sh

# Esto es un comentario

iptables -t nat -F
iptables -t nat -Z
iptables ...
...
...
```

Una vez creado el *script* debes darle permisos de ejecución con la orden:

```
chmod 755 fw.sh
```

A partir de ahora ya podrás ejecutarlo, escribiendo:

```
./fw.sh
```

Considera la posibilidad de editar y guardar el script en el sistema de ficheros de la máquina real, ejecutándolo desde dentro de la máquina virtual. Así, si tu script `fw.sh` está almacenado directamente en tu HOME de la máquina real, podrías editarlo en ella con un editor gráfico (por ejemplo, `gedit`) y luego ejecutarlo en la máquina `firewall` escribiendo dentro de esa máquina virtual:

```
/hosthome/fw.sh
```

## 1.2. Comprobación de la configuración del *firewall*

Durante la práctica frecuentemente tendrás que ir comprobando que el *firewall* está correctamente configurado, es decir:

- deja pasar el tráfico que debe dejar pasar
- impide el paso del tráfico que debe impedir
- realiza la traducción de direcciones IP necesaria para que no aparezcan en Internet paquetes con direcciones privadas

Para ello deberás emplear la herramienta *netcat* (`nc`) (ya utilizada en otras prácticas con anterioridad) que permite arrancar aplicaciones TCP y UDP en modo cliente o servidor.

El enunciado de la práctica te irá indicando cuándo y en qué máquinas debes lanzar un cliente o un servidor TCP o UDP para ir probando la configuración del *firewall*. Consulta la documentación adjunta para recordar la sintaxis de *netcat*.

# 2. Traducción de direcciones y puertos en el *firewall*: tabla `nat`

## 2.1. Clientes en la red privada, servidores externos

Configura un *script* `fw1.sh` en el *firewall* para que:

- se borren las reglas que hubiera configuradas previamente en la tabla `nat`
- se reinicien los contadores de la tabla `nat`
- se realice la traducción de direcciones para el tráfico saliente de las redes privadas (SNAT) y su correspondiente tráfico de respuesta.

Incluye el script en la memoria.

### 2.1.1. Pruebas con TCP

Ejecuta el *script* `fw1.sh` de 2.1.

1. Captura el tráfico en `r3-eth0` (iptables-01.cap) y en `firewall-eth0` (iptables-02.cap) para ver los paquetes dentro de la red de la Empresa y por Internet. Arranca las siguientes aplicaciones:

   - `nc` como servidor TCP en `pc6`, puerto 7777
   - `nc` como cliente TCP en `pc1`

   Sin escribir nada ni en el cliente ni en el servidor, consulta la información de `ip_conntrack` del `firewall` cada medio segundo. Para hacerlo automáticamente, en vez de repetir el comando utiliza `watch` de la siguiente forma:

   ```
   firewall:~# watch -n 0.5 cat /proc/net/ip_conntrack
   ```

   Explica el número de paquetes que se han observado en cada sentido, razonando la respuesta, indicando de qué paquetes se trata (recuerda que estamos ante una conexión TCP).

2. Introduce una palabra en la entrada estándar de `pc1`, pulsa `<Enter>` y observa los cambios en `ip_conntrack`. Explica a qué se deben.

3. Realiza un Ctrl+C en el terminal de `pc1` para interrumpir la ejecución de `nc`. Observa los cambios en `ip_conntrack` y explica a qué se deben.

4. Interrumpe las capturas, y estúdialas. En particular, identifica los mismos paquetes en las 2 capturas, y observa cómo cambian las direcciones IP de los mismos paquetes según viajen dentro de la EMPRESA o por INTERNET. Explica el resultado.

5. Consulta la lista de reglas en el `firewall` con:

   ```
   firewall:~# iptables -t nat -L -v -n
   ```

   Obseva qué regla(s) están cumpliendo los paquetes y cuántas veces se cumple(n).

6. Vuelve a repetir la misma prueba anterior (sin necesidad de realizar las capturas de tráfico): lanza servidor y cliente, intercambia tráfico, y termina la conexión. Vuelve a mirar qué regla(s) se están cumpliendo y cuántas veces se cumple(n).

### 2.1.2. Pruebas con UDP

Ejecuta el *script* `fw1.sh` de 2.1 para que se reinicien los contadores de paquetes de iptables, compruébalo consultando la lista de reglas del firewall.

1. Captura el tráfico en `r3-eth0` (iptables-03.cap) y en `firewall-eth0` (iptables-04.cap) para ver los paquetes dentro de la red de la Empresa y por Internet. Arranca las siguientes aplicaciones:

   - `nc` como servidor UDP en `pc6`, puerto 7777
   - `nc` como cliente UDP en `pc2`

   Realiza las siguientes pruebas:

   *a*) Sin escribir nada ni en el cliente ni en el servidor, consulta la información de `ip_conntrack` del `firewall` cada medio segundo. Recuerda que el tráfico es ahora UDP y no hay conexiones propiamente dichas. Explica el resultado.

   *b*) Escribe 5 líneas en el terminal de `pc2` para que se las envíe a `pc6`. Explica el número de paquetes enviados en la información que muestra `ip_conntrack`.

   *c*) Escribe una línea en `pc6` para que se la envíe a `pc2`. Explica nuevamente el número de paquetes en `ip_conntrack`.

   *d*) Observa el poco tiempo que se mantiene la "asociación" entre cliente y servidor en `ip_contrack`. Indica cuánto ha sido.

   *e*) Interrumpe la captura y las ejecuciones de `nc`, explica la captura y cómo ésta se relaciona con la información que has visto en `ip_conntrack`.

2. Consulta la lista de reglas en el `firewall`, e indica cuáles se están cumpliendo y cuántas veces se cumplen.

3. Interrumpe la ejecución de cliente y servidor e inicia una nueva comunicación entre un nuevo cliente y un servidor UDP e intercambia tráfico entre ellos para ver cómo evolucionan las cuentas en la lista de reglas. Explica qué reglas se están cumpliendo ahora y cuántas veces se cumplen.

4. Captura de nuevo el tráfico en `r3-eth0` (iptables-05.cap) y en `firewall-eth0` (iptables-06.cap) para ver los paquetes dentro de la red de la Empresa y por Internet cuando tienes varios clientes desde un mismo puerto origen conectándose a un mismo servidor, para ello inicia:

   - `nc` como servidor UDP en `pc7`, puerto 7777
   - `nc` como cliente UDP en `pc1`, puerto 6666
   - `nc` como cliente UDP en `pc2`, puerto 6666

   Ahora, envía una línea desde `pc1` y después una línea desde `pc2`. Ten en cuenta que `nc` no funciona como las aplicaciones servidoras que pueden atender a varios clientes a la vez. La aplicación `nc` no está preparada para que un servidor se pueda comunicar a la vez con dos clientes, por ello el envío desde `pc2` provocará que `pc7` envíe un ICMP de error a `pc2`. Pero para lo que queremos comprobar este error no es importante, sólo queremos analizar lo que ocurre en el `firewall` con la traducción de direcciones IP y puertos.

   Interrumpe las capturas y analízalas fijándote en las direcciones IP **y puertos** que se utilizan en la red de la EMPRESA y en INTERNET.

### 2.1.3. Pruebas con ICMP

Ejecuta el *script* `fw1.sh` de 2.1 para que se reinicien los contadores de paquetes de iptables.

1. Ejecuta el siguiente comando en `pc1` (recuerda sustituir la X por el número que te corresponde):

   ```
   pc1:~# ping -c 2 100.X.5.60
   ```

2. Consulta la información de `ip_conntrack` del `firewall`. Verás que no aparece nada. Recuerda que esto se debe a que las "conexiones" que se consideran para los paquetes ICMP es una diferente entre cada *echo request* y su correspondiente *echo reply*, asociación que se "olvida" justo después del *echo reply*.

3. Consulta la lista de reglas en el `firewall`, y mira cuáles se están cumpliendo y cuántas veces.

## 2.2. Servidores en la red privada, clientes externos

Aunque en una red como la que aparece en la figura, lo habitual es colocar los servidores accesibles desde el exterior en la zona DMZ, para ver cómo funciona DNAT, vamos a permitir que haya servidores accesibles desde el exterior en la red privada interna.

### 2.2.1. Apertura de puertos TCP

1. Captura el tráfico en `r3-eth0` (`iptables-07.cap`) y en `firewall-eth0` (`iptables-08.cap`) para ver los paquetes dentro de la red de la Empresa y por Internet.

2. Realiza un nuevo *script* `fw2.sh` en el *firewall* para que:

   - se borren las reglas que hubiera configuradas previamente en la tabla `nat`
   - se reinicien los contadores de la tabla `nat`
   - el tráfico de entrada al firewall destinado al puerto TCP 80 sea redirigido a `pc3`, puerto 80.

   Incluye el script en la memoria. Ejecuta dicho script y arranca las siguientes aplicaciones:

   - `nc` como servidor TCP en `pc3`, puerto 80
   - `nc` como cliente TCP en `pc6`, de forma que su tráfico lo reciba el servidor de `pc3` (NOTA: presta especial atención a los parámetros con los que debes lanzar este cliente). Indica en la memoria el comando que has usado para lanzar el cliente y explica por qué lo has hecho así.

3. Monitorizando la salida de `ip_contrack` realiza lo siguiente:

   - Envía una línea desde `pc6`.
   - Realiza un Ctrl+C en el terminal de `pc6` para interrumpir la ejecución de `nc`.

4. Interrumpe las capturas. Explica los siguientes resultados:

   *a*) El resultado observado en `ip_conntrack` y la traducción de direcciones IP y puertos realizada.

   *b*) La lista de reglas en el `firewall`, indica cuáles se están cumpliendo y cuántas veces.

### 2.2.2. Apertura de puertos UDP

1. Captura el tráfico en `r3-eth0` (`iptables-09.cap`) y en `firewall-eth0` (`iptables-10.cap`) para ver los paquetes dentro de la red de la Empresa y por Internet.

2. Modifica el *script* `fw2.sh` para que, adicionalmente:

   - el tráfico de entrada al firewall destinado al puerto UDP 5001 sea redirigido a `pc1`, puerto 5001
   - El tráfico de entrada al firewall destinado al puerto UDP 5002 sea redirigido a `pc2`, puerto 5001

   Incluye el script en la memoria. Ejecuta el script que acabas de modificar y arranca las aplicaciones:

   - `nc` como servidor UDP en `pc1`, puerto 5001
   - `nc` como servidor UDP en `pc2`, puerto 5001
   - `nc` como cliente UDP en `pc6`, de forma que su tráfico lo reciba el servidor de `pc1`. Indica el comando que has utilizado para lanzar el cliente y explica por qué.
   - `nc` como cliente UDP en `pc7`, de forma que su tráfico lo reciba el servidor de `pc2`. Indica el comando que has utilizado para lanzar el cliente y explica por qué.

3. Monitorizando la salida de `ip_contrack`, envía una línea desde `pc6` y otra línea desde `pc7`.

4. Interrumpe las capturas. Explica los siguientes resultados:

   *a*) El resultado observado en `ip_conntrack` y la traducción de direcciones IP y puertos realizada.

   *b*) Consulta la lista de reglas en el `firewall` e indica cuáles se están cumpliendo y cuántas veces.

## 3. Filtrado de tráfico en el *firewall*: tabla `filter`

Crea un *script* `fw3.sh` en el `firewall` partiendo de la configuración de traducción de direcciones realizada en `fw1.sh` (clientes en la red privada, servidores externos) al que se le añada la siguiente configuración (todas en el mismo *script*). Descripción de las **especificaciones**:

1. Reiniciar la tabla `filter`: borrar su contenido y reiniciar sus contadores.

2. Fijar las políticas por defecto de las cadenas de la tabla `filter`, haciendo que por defecto se descarte todo el tráfico en el `firewall` excepto los paquetes que cree el propio `firewall` (configuración habitual en un *firewall*).

3. Permitir el tráfico de entrada dirigido a las aplicaciones que se están ejecutando en el propio `firewall` únicamente si este tráfico tiene su origen en las subredes privadas de la empresa.

4. Permitir todo el tráfico saliente desde las subredes privadas hacia Internet y el tráfico de respuesta al saliente.

   Ten en cuenta que como has partido del *script* `fw1.sh`, en dicho *script* ya tenías las reglas de la tabla `nat` para la traducción de la dirección IP de origen de los paquetes que reenvía el `firewall` y los paquetes del tráfico entrante de respuesta a éste.

5. Permitir desde Internet únicamente el tráfico entrante nuevo hacia la zona DMZ según las siguientes reglas:

   - acceso a un servidor *echo* existente en `pc4` (UDP, puerto 7). El servidor de *echo* es un servidor que al enviarle una cadena de caracteres, devuelve la misma cadena que se le ha enviado. Para comprobar el acceso a este servidor utiliza `nc` como cliente desde otra máquina.
   - acceso a un servidor *daytime* existente en `pc5` (UDP, puerto 13). El servidor *daytime* es un servidor que al enviarle algo, devuelve la fecha y hora de la máquina donde está instalado. Para comprobar el acceso a este servidor utiliza `nc` como cliente desde otra máquina.

6. Permitir únicamente la comunicación entre la red privada y la zona DMZ de la siguiente forma:

   - acceso desde `pc1` a un servidor de *echo* (TCP, puerto 7) existente en `pc4`.

7. Desde la zona DMZ no se debe perimitir iniciar ninguna comunicación con la red privada ni con el propio `firewall`.

Incluye el script en la memoria.

En el escenario se encuentra lanzado en `pc4` un servidor TCP en el puerto 7. Prueba a lanzar un cliente con `nc` desde `pc1` para que se conecte con este servidor. Consulta la lista de reglas en el `firewall` e indica cuáles se están cumpliendo y cuántas veces se cumplen. Es importante que observes que las reglas de la tabla `filter`, si se cumple la condición, se aplican con cada paquete que atraviesa el `firewall` y este comportamiento es diferente a lo que ocurría con las reglas de la tabla `nat`.

## 3.1. OPCIONAL: Pruebas de la configuración del firewall

A continuación se dan algunas pautas para poder probar cada una de las especificaciones de `fw3.sh`. Para cada prueba, asegúrate de relanzar el *script* para que se reinicien los contadores, y comprueba qué reglas son las que se han aceptado para aceptar o rechazar el tráfico. Cada una de las siguientes especificaciones se corresponden con los puntos descritos en el apartado 2.

**Especificación 3**

1. Si se arranca una aplicación servidor (TCP o UDP) en la máquina `firewall` sólo podrá aceptar tráfico de un cliente que envíe mensajes desde una de las máquinas de las subredes privadas.

2. No podrá aceptar tráfico desde aplicaciones cliente lanzadas en otras subredes diferentes.

**Especificación 4**

1. Si se arranca una aplicación servidor (TCP o UDP) en una de las máquinas de Internet y se arranca una aplicación cliente para que se comunique con ese servidor en una de las máquinas de las subredes internas, el tráfico debe poder enviarse del cliente al servidor y del servidor al cliente, observando que el tráfico que sale del firewall con destino a la máquina de Internet no tiene como dirección IP origen la dirección de la máquina que pertenece a la subred privada, sino que lleva la dirección 100.X.1.100.

2. Si se arranca una aplicación cliente en `pc4` o `pc5` para comunicarse con el servidor que se haya arrancado en una de las máquinas de Internet, el `firewall` no debería permitir reenviar ese tráfico hacia Internet.

**Especificación 5**

1. Si se arranca un cliente `nc` desde una máquina de Internet se debe poder acceder al servidor de *echo* de `pc4`.

2. Si se prueba lo mismo lanzando el cliente desde `pc3`, no debería poder comunicarse.

3. Si se arranca un cliente `nc` desde una máquina de Internet se debería poder obtener la hora de `pc5`. Pulsa `<INTRO>` en el terminal de `nc` y debería obtenerse la hora que le envía `pc5`.

4. No se debe permitir otro tipo de tráfico desde Internet a DMZ. Si se arranca una aplicación servidor (TCP o UDP) en una de las máquinas de DMZ y se arranca una aplicación cliente para que se comunique con ese servidor en una de las máquinas de Internet, el tráfico no debería poder enviarse del cliente al servidor.

**Especificación 6**

1. Desde `pc1` se debería poder lanzar un cliente `nc` capaz de conectarse con al servidor TCP de *echo* de `pc4`.

2. Si se prueba lo mismo arrancando `nc` desde `pc2` o `pc3` no debería conectarse.

3. No se debe permitir otro tipo de tráfico desde `pc1`, `pc2` o `pc3` con `pc4` o `pc5`. Si se arranca una aplicación servidor (TCP o UDP) en una de esas máquinas y se arranca una aplicación cliente en una de las otras, el tráfico no debería poder enviarse del cliente al servidor.

**Especificación 7**

1. Si se arranca una aplicación servidor (TCP o UDP) en una de las máquinas de las subredes privadas y se arranca una aplicación cliente para que se comunique con ese servidor en una de las máquinas de DMZ, el tráfico no debería poder enviarse del cliente al servidor ni del servidor al cliente.

2. Si se arranca una aplicación servidor (TCP o UDP) en el `firewall` y se arranca una aplicación cliente para que se comunique con ese servidor en una de las máquinas de DMZ, el tráfico no debería poder enviarse del cliente al servidor.

## Entrega de la práctica

Sube al enlace que encontrarás en `aulavirtual` antes de que termine el plazo de entrega, los siguientes ficheros:

- Memoria en formato pdf donde se explique razonadamente la resolución de cada uno de los apartados de este enunciado.

- Fichero de nombre `p6.zip` o `p6.tgz` resultado de comprimir **una carpeta de nombre p6** que contenga en su interior todos los ficheros de captura de tráfico: desde `iptables-01.cap` a `iptables-10.cap`

  Puedes crear el fichero de esta forma: primero crea una carpeta de nombre `p6` y mete dentro de esa carpeta todas los ficheros de captura. Desde el navegador de archivos pulsa con el botón derecho del ratón sobre el nombre de la carpeta y selecciona `'Comprimir'`, nombre del archivador `'p6'` y extensión `'.zip'`.

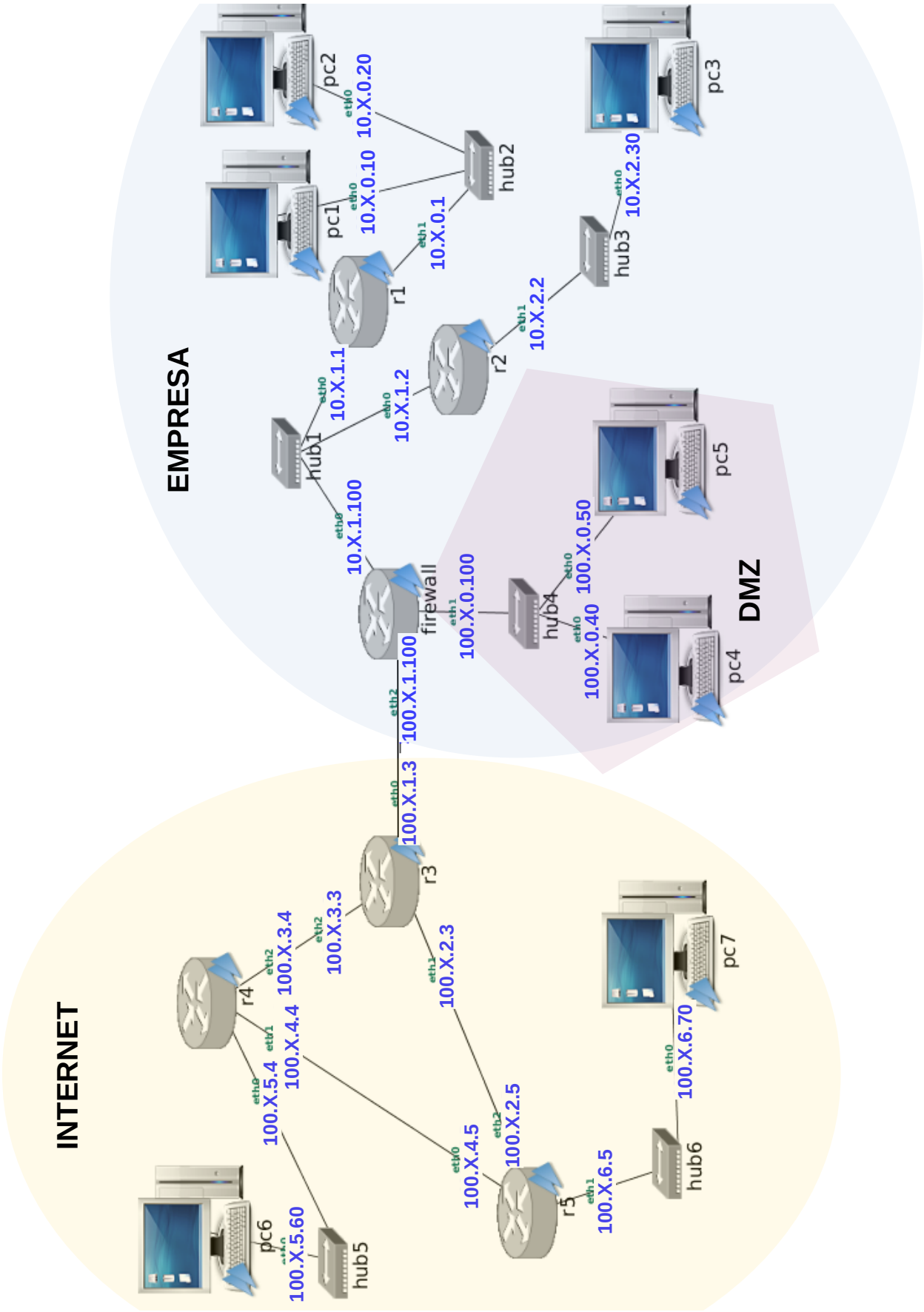



Figura 1: Escenario de red para los ejercicios de configuración de firewall

# Examen Parcial I de Sistemas Telemáticos
# Dispositivos de Interconexión, OSPF y BGP

GSyC
Departamento de Teoría de la Señal y Comunicaciones y Sistemas Telemáticos y Computación
Universidad Rey Juan Carlos

19 de marzo de 2019

## DISPOSITIVOS DE INTERCONEXIÓN

**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/st/disp`**.**
- **Se cargará el escenario mostrado en la figura 1.**
- **Si en algún momento quieres volver a tener el escenario en su estado inicial, cierra NetGUI, ejecuta** `clean-netgui.sh` **y ejecuta después** `/opt/st/disp/reset-lab`**.**

---

En la figura 1 se muestra el escenario que has cargado en NetGUI. Ten en cuenta que:

- Las máquinas `s1`, `s2`, `s3` y `s4` están configuradas como *switches*.
- Las máquinas `r1`, `r2` y `r3` están configuradas como *routers*.

**Arranca todas la máquinas de la figura**.

---

1. Partiendo de la configuración inicial del escenario, en un momento determinado, se sabe que las cachés de ARP de todas las máquinas del escenario tienen aprendidas la asociación entre direcciones IP y direcciones Ethernet de todas las máquinas que pertenecen a su misma subred y que los switches tienen aprendidas todas las posibles direcciones Ethernet de todas las máquinas del escenario. En estas condciones desde `pc10` se ejecuta un `ping` a 11.0.0.2.

   Indica cuál de las siguientes afirmaciones es correcta con respecto al tráfico capturado en la interfaz `s1(eth1)` durante la ejecución del `ping`:

   **(A)** No se capturará ningún mensaje.

   **(B)** Sólo se capturará la solicitud de ARP de `pc10` solicitando la dirección Ethernet de 11.0.0.2 ya que este mensaje va dirigido al Broadcast Ethernet.

   **(C)** Sólo se capturará la solicitud de ARP de `pc10` solicitando la dirección Ethernet de 11.0.0.2 y el mensaje ICMP Echo Request que envíe `pc10`.

   **(D)** Sólo se capturará el mensaje ICMP Echo Request que envíe `pc10`.

2. Partiendo de la configuración inical del escenario, supón que se realiza una configuración de proxy ARP y rutas en `r2` que permita que `pc60` pueda realizar un `ping` a `pc40`. Indica el contenido de la caché de ARP en `pc60` justo después de realizar el `ping`.

**(A)**
```
pc60:~# arp -a
? (14.0.0.2) at 00:07:E9:00:02:03 [ether] on eth0
```

**(B)**
```
pc60:~# arp -a
? (14.0.0.40) at 00:07:E9:00:02:03 [ether] on eth0
```

**(C)**
```
pc60:~# arp -a
? (14.0.0.40) at 00:07:E9:00:40:00 [ether] on eth0
```

**(D)** El resto de afirmaciones son falsas.

3. Partiendo de la configuración inicial del escenario,se ha eliminado el comportamiento por defecto de los switches y se ha realizado la siguiente configuración de VLANs:

   - VLAN100: se encuentran sólo las máquinas/routers de la subred 11.0.0.0/24.
   - VLAN200: se encuentran sólo las máquinas/routers de la subred 12.0.0.0/24.

   Se realiza un `ping` de `pc10` a `pc20`. Indica qué mensajes se capturarían en la interfaz `s2(eth3)`:

   **(A)** Únicamente la solicitud de ARP que realiza `r1` para preguntar por la dirección Ethernet de 12.0.0.20.

   **(B)** Únicamente los siguientes mensajes:
   - Solicitud de ARP que realiza `pc10` para preguntar por la dirección Ethernet de 11.0.0.1.
   - Solicitud de ARP que realiza `r1` para preguntar por la dirección Ethernet de 12.0.0.20.

   **(C)** Únicamente los siguientes mensajes:
   - Solicitud de ARP que realiza `pc10` para preguntar por la dirección Ethernet de 11.0.0.1.
   - La respuesta de ARP de 11.0.0.1 hacia `pc10`
   - El mensaje ICMP echo Request de `pc10`
   - El mensaje ICMP echo Reply que reenvía `r1` hacia `pc10`.

   **(D)** Los siguientes mensajes:
   - Solicitud de ARP que realiza `pc10` para preguntar por la dirección Ethernet de 11.0.0.1.
   - La respuesta de ARP de 11.0.0.1 hacia `pc10`
   - Solicitud de ARP que realiza `r1` para preguntar por la dirección Ethernet de 12.0.0.20.
   - El mensaje ICMP echo Request de `pc10`
   - El mensaje ICMP echo Reply que reenvía `r1` hacia `pc10`.

4. Partiendo de la configuración inicial del escenario, se ha eliminado el comportamiento por defecto de los switches y se ha realizado una configuración de VLAN. A continuación se muestra la configuración realizada (no se muestra el identificador de bridge porque no es relevante).
   En `s1`:

```
s1:~# brctl show
bridge name     bridge id       STP enabled     interfaces
vs200               ---             no            eth0.200
                                                  eth1.200
                                                  eth3
```

   En `s2`:

```
s2:~# brctl show
bridge name     bridge id       STP enabled     interfaces
vs200               ---             no            eth1.200
                                                  eth2.200
                                                  eth3.200
```

   En `s3`:

```
s3:~# brctl show
bridge name     bridge id       STP enabled     interfaces
vs200               ---             no            eth0.200
                                                  eth3.200
```

   En `s4`:

```
s4:~# brctl show
bridge name     bridge id       STP enabled     interfaces
vs200               ---             no            eth0.200
                                                  eth1.200
                                                  eth2
```

   Indica cuál de las siguientes afirmaciones es correcta.

   **(A)** La configuración mostrada permite que `pc20` y `pc30` puedan comunicarse.

   **(B)** La configuración mostrada permite que `pc20` y `pc50` puedan comunicarse.

   **(C)** La configuración mostrada permite que `pc30` y `pc40` puedan comunicarse.

   **(D)** La configuración mostrada permite que `pc20` y `r2(eth0)` puedan comunicarse.

## ENCAMINAMIENTO: OSPF

**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 escribe como nombre de archivo `/opt/st/ospf`**
- **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/st/ospf/reset-lab`**

---

La red de la figura tiene configurado OSPF como protocolo de encaminamiento interior. Se han definido 4 áreas OSPF:

- Área 0: `r1`, `r2` y `r3`.
- Área 1: `r1`, `r4`, `r5` y `r6`.
- Área 2: `r2` y `r7`.
- Área 3: `r3`, `r8`, `r9` y `r10`.

Arranca todos los *routers* de la figura **excepto r2 y r10**.

Espera unos segundos para que los *routers* se hayan intercambiado la información de encaminamiento usando OSPF y hayan configurado sus tablas de encaminamiento.

**Arranca ahora r2. No arranques r10**

Espera unos segundos para que los *routers* se hayan intercambiado la información de encaminamiento usando OSPF y hayan configurado sus tablas de encaminamiento.

---

5. Partiendo de la situación inicial (todos los *routers* están arrancados salvo `r10` y ya han configurado sus tablas de encaminamiento), indica cuál de las siguientes afirmaciones es correcta:

   **(A)** `r2`, por ser un router del área 0 o *backbone*, tiene en sus bases de datos OSPF información de las 5 direcciones IP que tiene configuradas `r1`: 11.0.0.1, 11.1.0.1, 11.3.0.1, 11.4.0.1 y 11.5.0.1.

   **(B)** `r8` tiene en sus bases de datos OSPF información de las 2 direcciones IP que tiene configuradas `r2`: 11.1.0.2 y 11.2.0.2.

   **(C)** `r4` NO tiene en sus bases de datos OSPF ninguna información de las direcciones IP que tiene configuradas `r2`.

   **(D)** `r1` NO tiene en sus bases de datos OSPF ninguna información de la dirección IP 11.7.0.4 porque esta interfaz es stub y no se ha generado ningún Network-LSA que informe de la existencia de los routers conectados a esa subred.

6. Partiendo de la situación inicial (todos los *routers* están arrancados salvo `r10` y ya han configurado sus tablas de encaminamiento), indica qué anuncios LSA se modificarían en las bases de datos de los **routers del área 3 cuando se arranque r10** con respecto a los anuncios LSA que existían antes de arrancar este *router*:

   **(A)** Habría los siguientes cambios:
   - 1 nuevo anuncio Router-LSA generado por `r10`
   - 2 nuevos anuncios Network-LSA de las subredes 11.16.0.0/16 y 11.15.0.0/16
   - 2 modificaciones de los anuncios existentes: Router-LSA generado por `r9` y Router-LSA generado por `r8`.

   **(B)** Habría los siguientes cambios:
   - 1 nuevo anuncio Router-LSA generado por `r10`
   - 2 nuevos anunciosNetwork-LSA de las subredes 11.16.0.0/16 y 11.15.0.0/16
   - 2 modificaciones de los anuncios existentes: Router-LSA generado por `r9` y Router-LSA generado por `r8`.
   - 1 nuevo anuncio Summary-LSA de la subred 11.17.0.0/16

   **(C)** Únicamente habría los siguientes cambios:
   - 1 nuevo anuncio Router-LSA generado por `r10`
   - 2 nuevos anuncios Network-LSA de las subredes 11.16.0.0/16 y 11.15.0.0/16

   **(D)** Únicamente habría los siguientes cambios:
   - 1 nuevo anuncio Router-LSA generado por `r10`

7. Partiendo de la situación inicial (todos los *routers* están arrancados salvo `r10` y ya han configurado sus tablas de encaminamiento), imagina que hay un problema en el suministro eléctrico de `r2` y `r3` y ambos routers permanecen apagados durante 1 minuto y a continuación se inician simultáneamente. Indica cuál de las siguientes afirmaciones sería correcta:

   **(A)** El DR de la subred 11.2.0.0/16 cambiaría con respecto al que había antes del corte en el suministro eléctrico pero el DR de la subred 11.1.0.0/16 seguiría siendo el mismo.

   **(B)** El DR de la subred 11.1.0.0/16 cambiaría con respecto al que había antes del corte en el suministro eléctrico pero el DR de la subred 11.2.0.0/16 seguiría siendo el mismo.

   **(C)** Los DRs de las subredes 11.2.0.0/16 y 11.1.0.0/16 cambiarían con respecto a los que había antes del problema en el suministro eléctrico.

   **(D)** Los DRs de las subredes 11.2.0.0/16 y 11.1.0.0/16 seguirían siendo los mismos que antes del problema en el suministro eléctrico.

8. Partiendo de la situación inicial (todos los *routers* están arrancados salvo `r10` y ya han configurado sus tablas de encaminamiento), indica qué router/s de la figura habrá/n generado un mensaje Summary-LSA de la subred 11.13.0.0/16 con coste 30.

   **(A)** El resto de afirmaciones son falsas.

   **(B)** Únicamente `r3`.

   **(C)** Únicamente `r1`.

   **(D)** Únicamente `r1` y `r2`.

## ENCAMINAMIENTO: BGP

**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 escribe como nombre de archivo** `/opt/st/bgp`
- **Se cargará el escenario mostrado en la figura 3.**
- **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/st/bgp/reset-lab`

---

Los sistemas autónomos AS10, AS20, AS30, AS40, AS50, AS60, AS70, AS80 y AS90 están utilizando BGP como protocolo de encaminamiento exterior para intercambiar sus tablas de encaminamiento. Se han definido entre ellos las siguientes relaciones entre sistemas autónomos:

- AS10 y AS20 mantienen una relación de tránsito donde AS10 es el proveedor y AS20 es el cliente.
- AS10 y AS30 mantienen una relación de tránsito donde AS10 es el proveedor y AS30 es el cliente.
- AS20 y AS90 mantienen una relación de tránsito donde AS20 es el proveedor y AS90 es el cliente.
- AS20 y AS70 mantienen una relación de tránsito donde AS20 es el proveedor y AS70 es el cliente.
- AS30 y AS50 mantienen una relación de tránsito donde AS30 es el proveedor y AS50 es el cliente.
- AS30 y AS60 mantienen una relación de tránsito donde AS30 es el proveedor y AS60 es el cliente.
- AS40 y AS20 mantienen una relación de tránsito donde AS40 es el proveedor y AS20 es el cliente.
- AS50 y AS70 mantienen una relación de tránsito donde AS50 es el proveedor y AS70 es el cliente.
- AS70 y AS80 mantienen una relación de tránsito donde AS70 es el proveedor y AS80 es el cliente.
- AS10 y AS40 mantienen una relación entre iguales.
- AS50 y AS90 mantienen una relación entre iguales.
- AS60 y AS70 mantienen una relación entre iguales.

Arranca todos los *routers* de la figura **excepto** `as30-r1`. Espera un minuto a que los *routers* se intercambien la información de encaminamiento a través de BGP.

**Arranca ahora** `as30-r1`. Espera un minuto a que los *routers* se intercambien la información de encaminamiento a través de BGP.

9. Consulta en la configuración de BGP de `as30-r1` la agrupación de sus redes internas. Teniendo en cuenta que se desea anunciar sólo las redes actualmente presentes en el sistema autónomo, indica cuál de las siguientes afirmaciones es correcta:

   **(A)** La agrupación es correcta.

   **(B)** La agrupación NO es correcta. La agrupación correcta es: 13.9.0.0/16, 13.10.0.0/15, 13.12.0.0/15, 13.14.0.0/16.

   **(C)** La agrupación NO es correcta. La agrupación correcta es: 13.9.0.0/15, 13.10.0.0/14.

   **(D)** La agrupación NO es correcta, pero no hay ninguna forma de agrupar las redes de AS30 y es necesario anunciar por separado sus 6 redes internas.

10. Partiendo de la configuración inicial del escenario, y teniendo en cuenta las relaciones entre los sistemas autónomos de la figura, indica cuál de las siguientes afirmaciones es correcta:

**(A)** `as20-r1` anunciará a `as90-r1` las redes 14.0.0.0/15 tanto con `ASPATH={20,40}` como también con `ASPATH={20,10,40}`.

**(B)** `as20-r1` NO anunciará a `as90-r1` las redes 14.0.0.0/15 con NINGÚN `ASPATH`, pues son las redes de un proveedor suyo.

**(C)** `as20-r1` anunciará a `as90-r1` las redes 14.0.0.0/15 únicamente con `ASPATH={20,40}`.

**(D)** `as20-r1` anunciará a `as90-r1` las redes 14.0.0.0/15 únicamente con `ASPATH={20,10,40}`.

11. Consulta la configuración de BGP de `as70-r1`. Teniendo en cuenta las relaciones entre los sistemas autónomos de la figura, indica cuál de las siguientes afirmaciones es correcta:

**(A)** La configuración de `as70-r1` es correcta.

**(B)** La configuración de `as70-r1` es incorrecta, y como consecuencia de ello, `as70-r1` ha elegido alguna ruta incorrectamente.

**(C)** La configuración de `as70-r1` es incorrecta, y como consecuencia de ello, `as50-r1` ha elegido alguna ruta incorrectamente.

**(D)** La configuración de `as70-r1` es incorrecta, y como consecuencia de ello, `as80-r1` ha elegido alguna ruta incorrectamente.

12. Partiendo de la configuración inicial del escenario (arrancado `as30-r1` después de que el resto de *routers* estuviera ya arrancado y configurado), y teniendo en cuenta las relaciones entre los sistemas autónomos de la figura, observa el siguiente mensaje `UPDATE` (sólo se muestran algunos campos):

```
Border Gateway Protocol - UPDATE Message
    Marker: ffffffffffffffffffffffffffffffff
    Length: ...
    Type: UPDATE Message (2)
    Withdrawn Routes Length: 0
    Total Path Attribute Length: ...
Path attributes
    Path Attribute - ORIGIN: IGP
    Path Attribute - AS_PATH: 10 40 20 70 80
    Path Attribute - NEXT_HOP: 100.6.0.10
    ...
Network Layer Reachability Information (NLRI)
    18.0.0.0/15
```

Indica cuál de las siguientes afirmaciones es correcta:

**(A)** Ningún router de la figura puede haber generado este anuncio, pues el router que podría anunciarla prefiere otra ruta para alcanzar el destino.

**(B)** Ningún router de la figura puede haber generado este anuncio, pues este anuncio no respeta las reglas de exportación de rutas entre sistemas autónomos.

**(C)** El mensaje `UPDATE` es un anuncio correcto que será enviado por `as10-r1` a `as30-r1`, y la ruta anunciada SERÁ la preferida por `as30-r1` para alcanzar las redes de AS80.

**(D)** El mensaje `UPDATE` es un anuncio correcto que será enviado por `as10-r1` a `as30-r1`, pero la ruta anunciada NO SERÁ la preferida por `as30-r1` para alcanzar las redes de AS80.

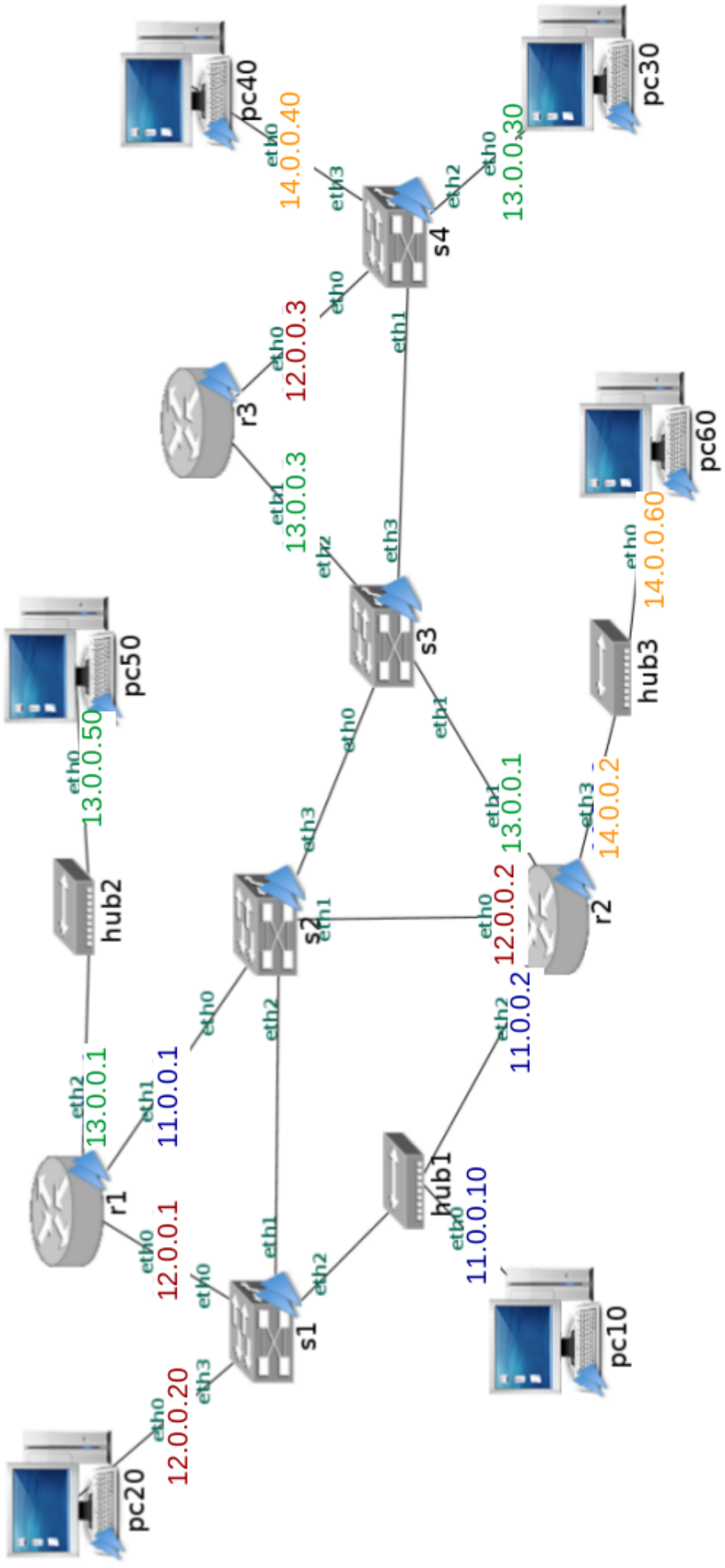



Figura 1: Dispositivos de Interconexión

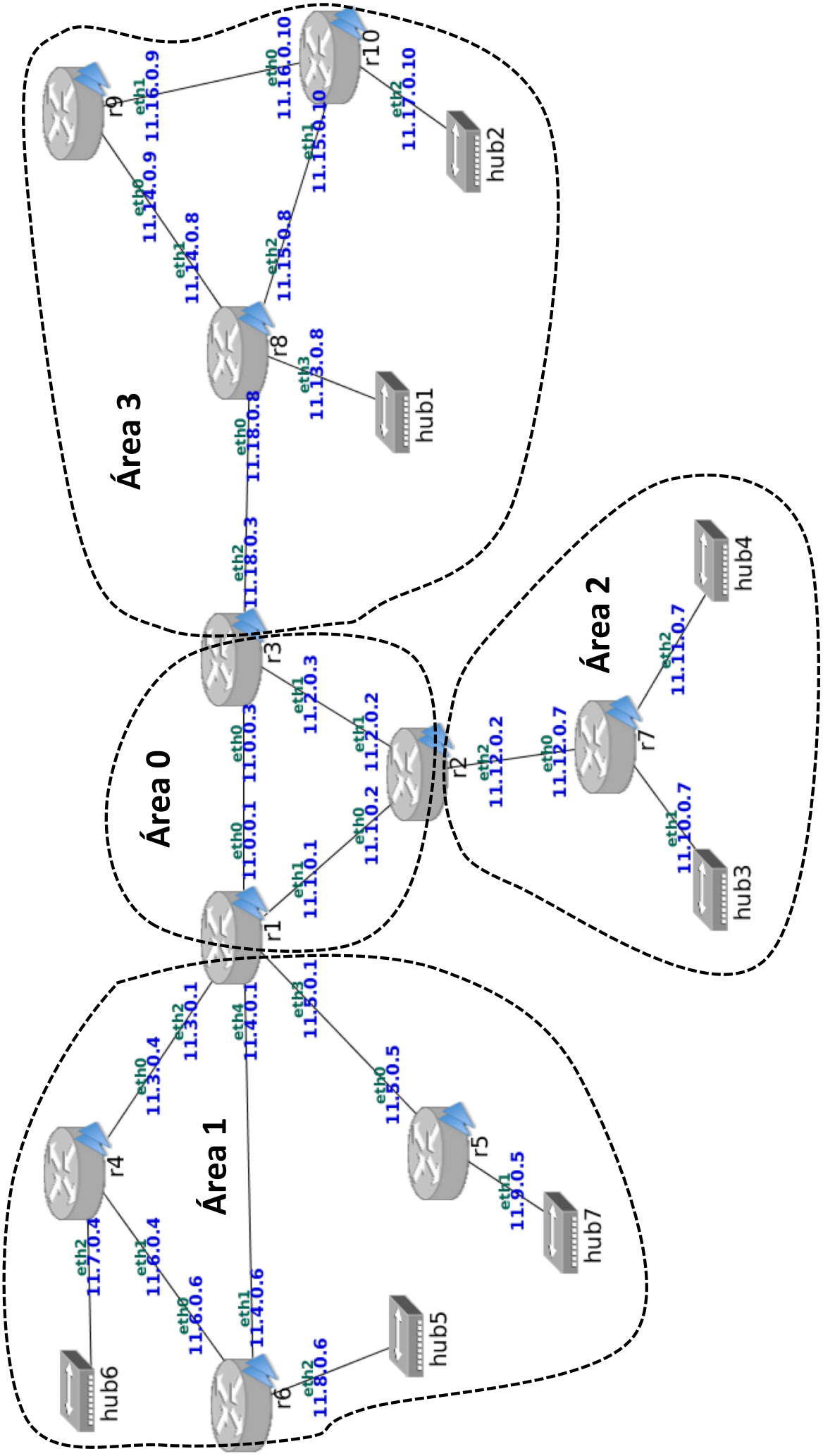



Figura 2: Encaminamiento OSPF

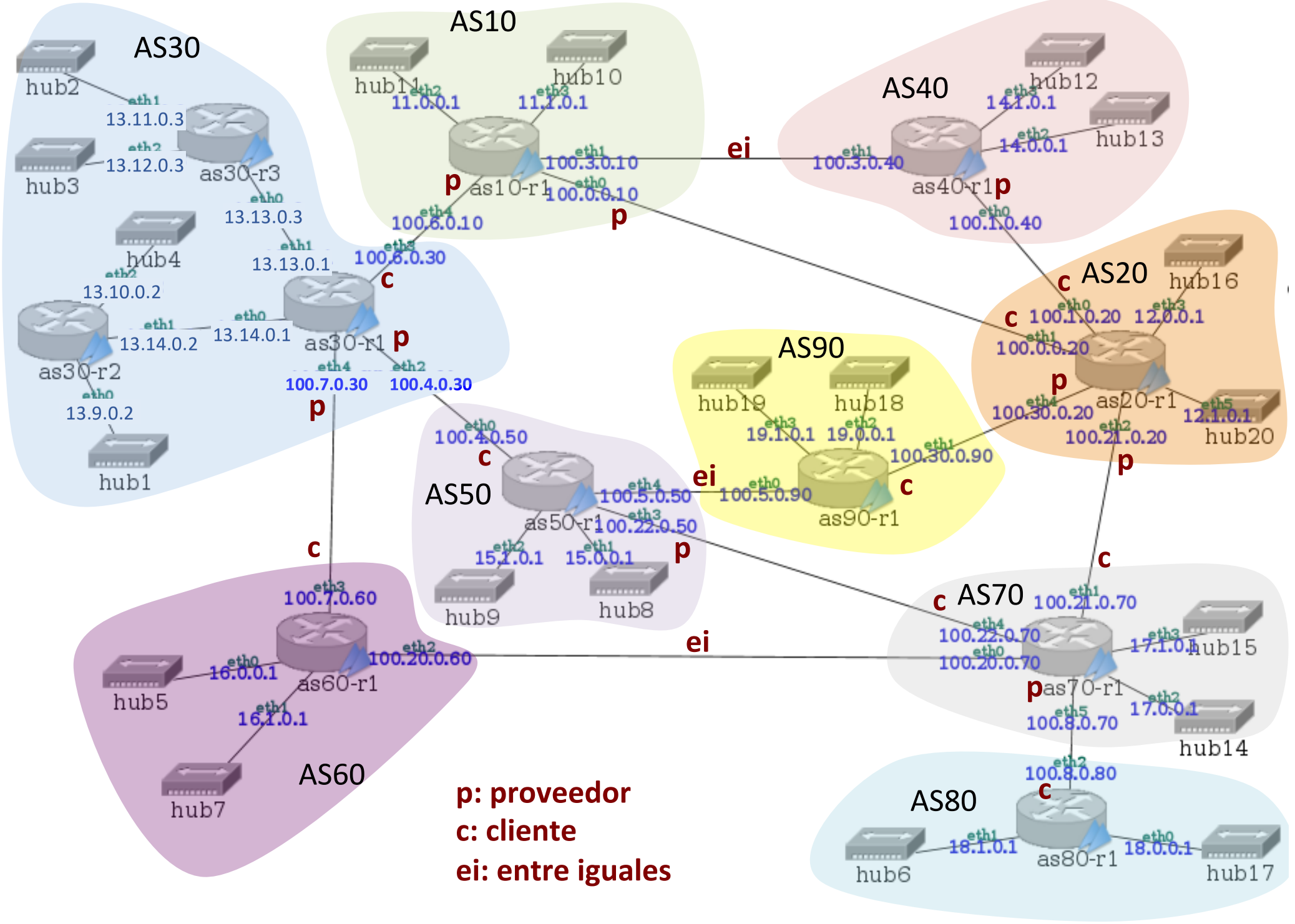



Figura 3: Encaminamiento BGP

Examen Parcial de Sistemas Telemáticos

# Parcial I: Dispositivos de Interconexión, OSPF y BGP

Grados de ITT, IT, IST, IST+ADE, ITT+IAA

GSyC
Departamento de Teoría de la Señal y Comunicaciones y Sistemas Telemáticos y Computación
Universidad Rey Juan Carlos

19 de marzo de 2019

| | |
|---|---|
| **Ordenador en el que estás sentado**: | |
| **Apellidos**: | |
| **Nombre**: | |
| **DNI**: | |
| **Titulación**: | |

| | A | B | C | D |
|---|---|---|---|---|
| **1** | X | | | |
| **2** | | X | | |
| **3** | X | | | |
| **4** | | | | |
| **5** | | | X | |
| **6** | X | | | |
| **7** | | | | X |
| **8** | | | | X |
| **9** | | X | | |
| **10** | | | | X |
| **11** | | | X | |
| **12** | X | | | |

**Instrucciones:** En cada pregunta debes seleccionar una única opción (A, B, C, D), marcándola con una ×.

**Ejemplo**:

Supongamos que consideras que la solución correcta para la pregunta 2 es la C. Deberías macarla así:

| | A | B | C | D |
|---|---|---|---|---|
| **1** | | | | |
| **2** | | | × | |
| **3** | | | | |

Si cambias de opinión y ahora crees que la solución correcta para la pregunta 2 es la D, debes redondear la marca incorrecta, y marcar la correcta:

| | A | B | C | D |
|---|---|---|---|---|
| **1** | | | | |
| **2** | | | ⊗ | × |
| **3** | | | | |

Si de nuevo rectificas y crees que la solución correcta para la pregunta 2 es la C, debes redondear la marca incorrecta y marcar la correcta:

| | A | B | C | D |
|---|---|---|---|---|
| **1** | | | | |
| **2** | | | ⊗ × | ⊗ |
| **3** | | | | |

En cualquier caso **asegúrate siempre de que como máximo hay una marca por pregunta**. Las preguntas en las que haya más de una marca se considerarán en blanco.

# Examen Parcial II de Sistemas Telemáticos

GSyC, Universidad Rey Juan Carlos

24 de junio de 2019

## TCP

Si al abrir alguna de las capturas de TCP en wireshark en el campo "Protocol" aparece algún paquete clasificado como perteneciente a un protocolo diferente de TCP (como por ejemplo, "RTPproxy" o "DCERPC"), ve a `Analyze -> Enabled Protocols` y desactiva dicho protocolo de la lista.

---

1. Carga en `wireshark` la captura `/opt/st/tcp1.cap` y **ordena los paquetes según la columna tiempo**.

   Indica cuál de las siguientes afirmaciones es correcta respecto a la situación del cliente inmediatamente después de transmitir el segmento 193 y antes de recibir ningún otro segmento de datos adicional.

   **(A)** El cliente se encuentra en modo de control de congestión *Slow Start*. No puede enviar ningún segmento con datos adicional.

   **(B)** El cliente se encuentra en modo de control de congestión *Slow Start*. Puede enviar 4 segmentos adicionales (de tamaño MSS).

   **(C)** El cliente se encuentra en modo de control de congestión *Congestion Avoidance*. NO puede enviar ningún segmento con datos adicional.

   **(D)** El cliente se encuentra en modo de control de congestión *Congestion Avoidance*. Puede enviar 1 segmento adicional (de tamaño MSS).

2. Carga en `wireshark` la captura `/opt/st/tcp1.cap` y **ordena los paquetes según la columna tiempo**.

   Indica cuál de las siguientes afirmaciones es correcta respecto al segmento 65:

   **(A)** El segmento 65 es una retransmisión por *Timeout*. Justo después de transmitirlo, la ventana de congestión tiene valor 1 MSS y está llena.

   **(B)** El segmento 65 es una retransmisión rápida (*Fast Retransmit*). Justo después de transmitirlo, la ventana de congestión tiene valor 14 MSS y se podrían transmitir 9 paquetes adicionales (de tamaño MSS).

   **(C)** El segmento 65 es una retransmisión rápida (*Fast Retransmit*). Justo después de transmitirlo, la ventana de congestión tiene valor 5 MSS y está llena.

   **(D)** El segmento 65 es una retransmisión por *Timeout*. Justo después de transmitirlo, la ventana de congestión tiene valor 3 MSS y se podrían transmitir 2 paquetes adicionales (de tamaño MSS).

3. Carga en `wireshark` la captura `/opt/st/tcp2.cap` y **ordena los paquetes según la columna tiempo**.

   Indica cuál de las siguientes afirmaciones es correcta respecto a la situación del cliente inmediatamente después de enviar el segmento 26 y antes de recibir ningún otro segmento de datos adicional.

   **(A)** El cliente se encuentra en modo de control de congestión *Fast Recovery*. NO puede enviar ningún segmento con datos adicional.

   **(B)** El cliente se encuentra en modo de control de congestión *Fast Recovery*. Puede enviar 1 segmento adicional (de tamaño MSS).

   **(C)** El cliente se encuentra en modo de control de congestión *Congestion Avoidance*. NO puede enviar ningún segmento con datos adicional.

   **(D)** El cliente se encuentra en modo de control de congestión *Congestion Avoidance*. Puede enviar 1 segmento adicional (de tamaño MSS).

4. Carga en `wireshark` la captura `/opt/st/tcp2.cap` y **ordena los paquetes según la columna tiempo**.

   Observa la retransmisión que se produce en el segmento 23. A partir de ese momento, señala con qué segmento se entra en *Congestion Avoidance* :

   **(A)** Con el segmento 33, por ser el asentimiento del segmento 29, último segmento enviado durante el *Fast Recovery*.

   **(B)** Con el segmento 30, por ser el asentimiento del segmento 23.

   **(C)** Con el segmento 28, por ser el último asentimiento repetido.

   **(D)** Con el segmento 26, por ser el primer segmento que se envía con datos nuevos.

5. Una máquina A está enviando datos a una máquia B a través de una conexión TCP. Se sabe que el MSS es de 1000 bytes. El último segmento de ACK que ha enviado B contiene los siguientes campos:

```
Transmission Control Protocol
    Source Port: 22222
    Destination Port: 11111
    Acknowledgement number: 1001
    Advertised Window: 10000
    Options:
         SACK: 3001-6001
```

A continuación, B recibe los dos segmentos siguientes:

```
Transmission Control Protocol
    Source Port: 11111
    Destination Port: 22222
    Sequence number: 7001
Data (1000 bytes)
```

```
Transmission Control Protocol
    Source Port: 11111
    Destination Port: 22222
    Sequence number: 1001
Data (1000 bytes)
```

Sabiendo que B aún no ha pasado ningún segmento recibido a la aplicación, indica cuál sería el contenido del siguiente mensaje de ACK que enviaría B tras recibir esos dos segmentos:

**(A)**
```
Transmission Control Protocol
    Source Port: 22222
    Destination Port: 11111
    Acknowledgement number: 1001
    Advertised Window: 10000
    Options:
         SACK: 1001-2001
         SACK: 3001-6001
         SACK: 7001-8001
```

**(B)**
```
Transmission Control Protocol
    Source Port: 22222
    Destination Port: 11111
    Acknowledgement number: 2001
    Advertised Window: 10000
    Options:
         SACK: 7001-8001
         SACK: 3001-6001
```

**(C)**
```
Transmission Control Protocol
    Source Port: 22222
    Destination Port: 11111
    Acknowledgement number: 2001
    Advertised Window: 9000
    Options:
         SACK: 7001-8001
         SACK: 3001-6001
```

**(D)**
```
Transmission Control Protocol
    Source Port: 22222
    Destination Port: 11111
    Acknowledgement number: 2001
    Advertised Window: 10000
    Options:
         SACK: 3001-8001
```

## HTTP

6. Analiza la captura `/opt/st/http-2.cap`.

   Transcurridos 20 minutos después de que dicha captura haya tenido lugar, desde un navegador en una máquina diferente a las que aparecen en la captura se envía la siguiente petición HTTP a la máquina 23.0.0.23:

   ```
   GET http://www1/ HTTP/1.1
   Host: www1
   ```

   Indica cuál de las siguientes afirmaciones es correcta con respecto a esta última petición:

   **(A)** La máquina 23.0.0.23 servirá el recurso pedido directamente desde su caché.

   **(B)** La máquina 23.0.0.23 deberá revalidar el recurso con el servidor `www1`.

   **(C)** La máquina 23.0.0.23 volverá a solicitar el recurso al servidor `www1`, y una vez recibido, se lo enviará al navegador.

   **(D)** La máquina 23.0.0.23 ignorará la petición del navegador.

7. Analiza la captura `/opt/st/http-1.cap`.

   En dicha captura el cliente pide a un *proxy-cache* un recurso principal y dos imágenes, y los 3 recursos residen originalmente en el servidor `www2`.

   Sabiendo que cuando recibe la petición de la captura el *proxy-cache* tiene los 3 recursos en su caché, ¿es seguro que los 3 recursos transmitidos en la captura son exactamente los mismos que los que en ese momento había en `www2`?

   **(A)** El recurso principal transmitido es seguro que es el mismo que el que había el servidor en el momento de la captura, pero las dos imágenes podrían ser diferentes.

   **(B)** Los 3 recursos transmitidos (el principal y las dos imágenes) es seguro que son los mismos que los que había en el servidor en el momento de la captura.

   **(C)** Los 3 recursos transmitidos (el principal y las dos imágenes) podrían ser distintos de los que había en el servidor en el momento de la captura.

   **(D)** Las dos imágenes transmitidas es seguro que son las mismas que las que había en el servidor en el momento de la captura, pero el recurso principal podría ser diferente.

8. Analiza la captura `/opt/st/http-3.cap`. Sabiendo que antes de realizarse esa captura el navegador del cliente no tenía ninguna *Cookie* almacenada, supón que tras realizar la captura el mismo navegador realiza la siguiente petición HTTP:

   ```
   GET / HTTP/1.1
   Host: www2
   ```

   Indica el valor de la cabecera `Cookie` enviará el navegador con esta nueva petición:

   **(A)** `Cookie: theme=basic; lang=en`

   **(B)** `Cookie: theme=basic; lang=en, id=2001`

   **(C)** `Cookie: theme=basic; lang=en, id=5001`

   **(D)** `Cookie: id=5001`

## CLAVES

9. 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 `Amazon CA 1`. Se sabe que dicha CA **NO es una CA raíz**. Se sabe que el navegador tiene instalados todos los certificados de las CA raíz.

   Indica cuál de las siguientes afirmaciones es correcta con respecto al certificado del servidor `www.eloferton.es`:

   **(A)** Para comprobar la validez de dicho certificado el navegador solicitará el certificado de `Amazon CA 1` y si este certificado estuviera firmado por una CA raíz permitirá comprobar la validez de la clave pública de `www.eloferton.es`.

   **(B)** Para comprobar la validez de dicho certificado el navegador NO necesitará la clave pública de la CA `Amazon CA 1` por ser una CA.

   **(C)** Para comprobar la validez de dicho certificado el navegador utilizará la clave pública de alguna de las CA raíz que están instaladas en el navegador.

   **(D)** Para comprobar la validez de dicho certificado el navegador solicitará el certificado de `Amazon CA 1` y este certificado, independientemente de la CA que lo haya emitido, permirá comprobar la validez de la clave pública de `www.eloferton.es`.

10. Suponiendo que se ha producido la siguiente comunicación y que tanto Álex como Bárbara tienen de forma fiable las claves públicas correspondientes:

    - Álex envía a Bárbara el siguiente mensaje: $\boxed{texto, K_A^-(H(texto))}$
    - Bárbara recibe el siguiente mensaje: $\boxed{texto2, K_A^-(H(texto))}$

    Indica cuál de las siguientes afirmaciones es correcta:

    **(A)** Bárbara no puede saber que el mensaje que ha recibido no es el mensaje original de Álex.

    **(B)** Bárbara puede saber que el mensaje que ha recibido no es el mensaje original de Álex porque el resultado de aplicar $K_A^+$ sobre el campo $K_A^-(H(texto))$ no coincide con el campo $texto2$ recibido.

    **(C)** Bárbara puede saber que el mensaje que ha recibido no es el mensaje original de Álex porque el resultado de aplicar $K_A^+$ sobre el campo $K_A^-(H(texto))$ no coincide con el resultado de aplicar la función $H(.)$ sobre el campo $texto2$ recibido.

    **(D)** Bárbara sabe que el mensaje que ha recibido sí es el mensaje original de Álex porque el mensaje viene firmado por Álex y Bárbara podrá usar su clave privada para verificar la firma.

En la figura 1 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:

- 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.

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.

---

11. Partiendo de la situación inicial, se desea permitir, simultáneamente:

    - Que las máquinas de Internet puedan intercambiar mensajes con un servidor TCP instalado en `e1-pc2` en el puerto 80
    - Que desde el *firewall* `e1-fw` se pueda hacer *ping* a todas las máquinas de la organización.

    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 nat -A PREROUTING -i eth0 -d 20.0.1.1  -p tcp --dport 80 -j DNAT --to-destination 10.0.0.20
    iptables -t filter -A FORWARD -i eth0 -d 10.0.0.20 -p tcp --dport 80 -j ACCEPT
    iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
    iptables -t filter -A OUTPUT -o eth1 -j ACCEPT
    iptables -t filter -A OUTPUT -o eth2 -j ACCEPT
    ```

    **(B)**
    ```
    iptables -t nat -A PREROUTING -i eth0 -d 20.0.1.1  -p tcp --dport 80 -j DNAT --to-destination 10.0.0.20
    iptables -t filter -A FORWARD -i eth0 -d 10.0.0.20 -p tcp --dport 80 -j ACCEPT
    iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
    iptables -t filter -A INPUT -i eth1 -j ACCEPT
    iptables -t filter -A INPUT -i eth2 -j ACCEPT
    ```

    **(C)**
    ```
    iptables -t nat -A PREROUTING -i eth0 -d 20.0.1.1  -p tcp --dport 80 -j DNAT --to-destination 10.0.0.20
    iptables -t filter -A INPUT -i eth1 -j ACCEPT
    iptables -t filter -A INPUT -i eth2 -j ACCEPT
    ```

    **(D)**
    ```
    iptables -t nat -A PREROUTING -i eth0 -d 20.0.1.1  -p tcp --dport 80 -j DNAT --to-destination 10.0.0.20
    iptables -t filter -A FORWARD -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
    iptables -t filter -A OUTPUT -i eth1 -j ACCEPT
    iptables -t filter -A OUTPUT -i eth2 -j ACCEPT
    ```

12. Partiendo de la configuración inicial descrita del escenario, se ha aplicado en `e1-fw` **exclusivamente** la siguiente configuración:

```
iptables -t filter -A FORWARD -i eth0 -o eth1 -j DROP
iptables -t filter -A FORWARD -d 20.0.0.30 -p tcp --dport 7000 -j ACCEPT
iptables -t filter -A FORWARD -i eth1 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Indica cuál de las siguientes afirmaciones es correcta:

**(A)** La configuración permite a cualquier máquina de Internet intercambiar mensajes con un servidor TCP instalado en `e1-pc3` en el puerto 7000.

**(B)** La configuración permite a un cliente TCP instalado en `e1-pc3` en el puerto 7000 comunicarse con servidores lanzados en cualquier máquina de Internet en cualquier puerto.

**(C)** La configuración permite a un cliente TCP instalado en `e1-pc3` en cualquier puerto comunicarse con servidores lanzados en cualquier máquina de Internet en el puerto 7000.

**(D)** El resto de afirmaciones son falsas.

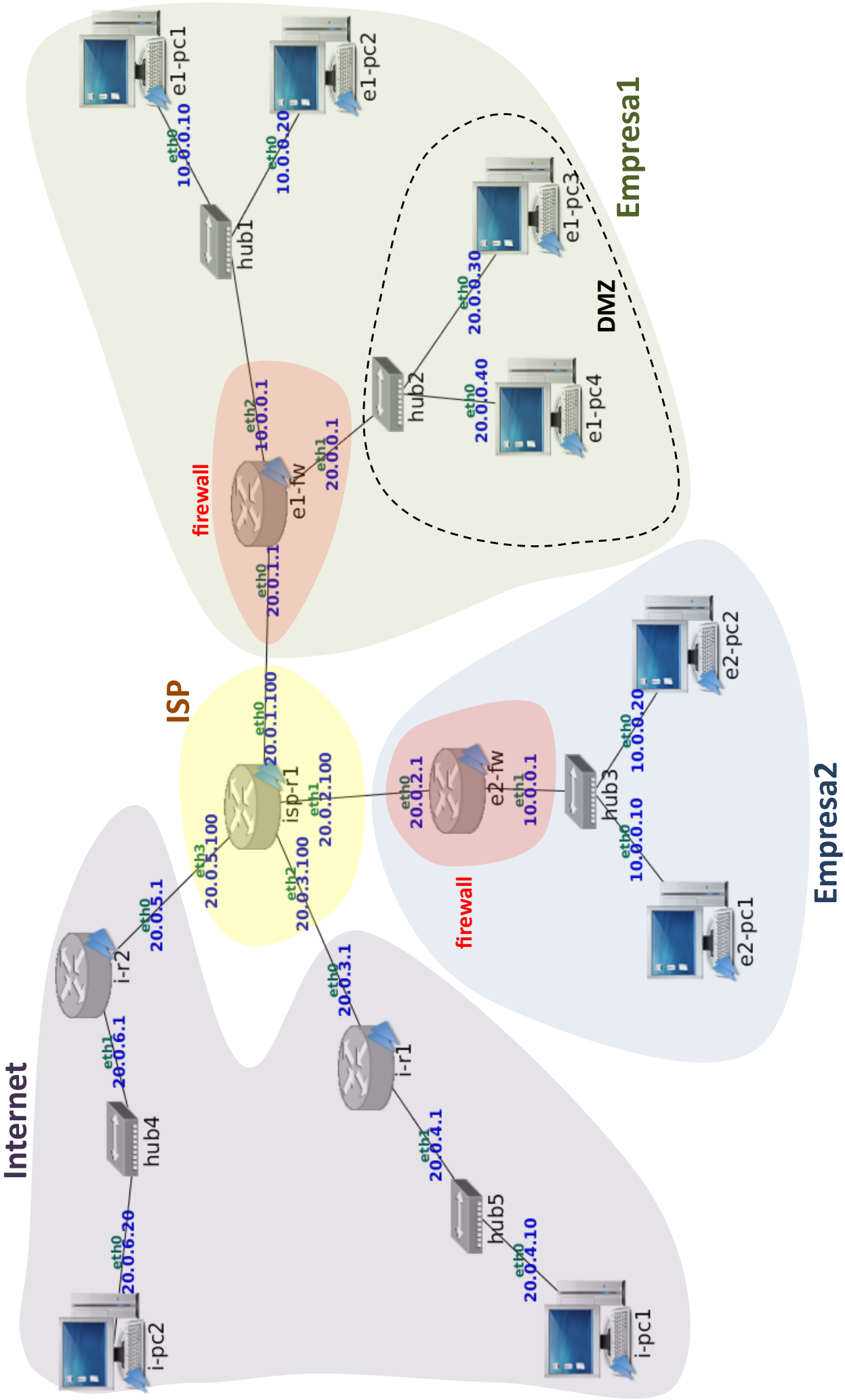



Figura 1: iptables

Examen Final de Sistemas Telemáticos

# Parcial II: Control de Congestión en TCP, HTTP, Seguridad

Grados de ITT, IT, IST, IST+ADE, ITT+IAA

GSyC
Departamento de Teoría de la Señal y Comunicaciones y Sistemas Telemáticos y Computación
Universidad Rey Juan Carlos

24 de junio de 2019

| | |
|---|---|
| **Ordenador en el que estás sentado**: | |
| **Apellidos**: | |
| **Nombre**: | |
| **DNI**: | |
| **Titulación**: | |

| | A | B | C | D |
|---|---|---|---|---|
| **1** | | | | X |
| **2** | X | | | |
| **3** | X | | | |
| **4** | | X | | |
| **5** | | | X | |
| **6** | | | X | |
| **7** | X | | | |
| **8** | | | | X |
| **9** | X | | | |
| **10** | | | X | |
| **11** | | X | | |
| **12** | | | | X |

**Instrucciones:** En cada pregunta debes seleccionar una única opción (A, B, C, D), marcándola con una ×.

**Ejemplo**:

Supongamos que consideras que la solución correcta para la pregunta 2 es la C. Deberías macarla así:

| | A | B | C | D |
|---|---|---|---|---|
| **1** | | | | |
| **2** | | | × | |
| **3** | | | | |

Si cambias de opinión y ahora crees que la solución correcta para la pregunta 2 es la D, debes redondear la marca incorrecta, y marcar la correcta:

| | A | B | C | D |
|---|---|---|---|---|
| **1** | | | | |
| **2** | | | ⊗ | × |
| **3** | | | | |

Si de nuevo rectificas y crees que la solución correcta para la pregunta 2 es la C, debes redondear la marca incorrecta y marcar la correcta:

| | A | B | C | D |
|---|---|---|---|---|
| **1** | | | | |
| **2** | | | ⊗ × | ⊗ |
| **3** | | | | |

En cualquier caso **asegúrate siempre de que como máximo hay una marca por pregunta**. Las preguntas en las que haya más de una marca se considerarán en blanco.

# GRADO EN INGENIERIA EN SISTEMAS DE TELECOMUNICACION (FUENLABRADA)

## 2040 - SISTEMAS TELEMATICOS - MAÑANA A - 2Q



**Pregunta 1**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS.

Dada la situación inicial del escenario, y estando la tabla de direcciones aprendidas de los *switches* vacía, y las cachés de ARP de todas las máquinas también vacías, se realiza un *ping* entre `pc20` y `pc50`. Indica cuál de las siguientes afirmaciones es correcta respecto a cuántas de las 3 direcciones Ethernet de las interfaces de `r1` habrá aprendido `s2` al terminar el *ping*:

a. Habrá aprendido las 3 direcciones Ethernet de las 3 interfaces de `r1`.

b. Habrá aprendido exclusivamente 2 direcciones Ethernet de 2 interfaces de `r1`.

c. No habrá aprendido ninguna dirección Ethernet de ninguna de las interfaces de `r1`.

d. Habrá aprendido exclusivamente 1 dirección Ethernet de 1 interfaz de `r1`.

**Pregunta 2**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS.

Dada la situación inicial del escenario, se rompe el enlace entre 's1' y 's2'. Para que `pc10` pueda hacer un *ping* a `pc30`, se configura adecuadamente *Proxy-ARP* en `r1` y se ajusta su tabla de encaminamiento. Una vez que el *ping* esté de nuevo funcionando, cuál de las siguientes asociaciones estará en la caché de ARP de la máquina `pc10`:

a. 11.0.0.1 está asociada a `r1-eth0`.

b. 11.0.0.30 está asociada a `r1-eth0`.

c. 11.0.0.30 está asociada a `pc30-eth0`.

d. Ninguna de las otras 3 asociaciones estará en la caché de ARP de `pc10`.

**Pregunta 3**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS.

Dada la situación inicial del escenario, **se APAGAN `r1` y `r2`**. Se añade a `r3-eth1` por *IP aliasing* la dirección 11.0.0.1. Se modifica la tabla de encaminamiento de `r3` hasta que sea la siguiente (sólo se muestran las columnas más relevantes):

```
Destination     Gateway         Iface
13.0.0.0        *               eth0
14.0.0.0        *               eth1
12.0.0.0        *               eth2
11.0.0.0        *               eth1
```

Señala cuál de las siguientes afirmaciones es correcta:

a. Es necesario eliminar una ruta a la tabla de encaminamiento de `r3` para permitir a `pc40` y `pc10` intercambiar datagramas IP.

b. Es necesario añadir una ruta a la tabla de encaminamiento de `r3` para permitir a `pc40` y `pc10` intercambiar datagramas IP.

c. Es necesario añadir una dirección IP adicional por *IP aliasing* a `r3` para permitir a `pc40` y `pc10` intercambiar datagramas IP.

d. Esta configuración de `r3` permitirá a `pc40` y `pc10` intercambiar datagramas IP.

**Pregunta 4**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS.

Partiendo de las situación inicial del escenario, se configuran VLANs para que todas las interfaces con IPs de la subred 11.0.0.0/24 puedan comunicarse entre sí (VLAN100), y que todas las interfaces con IPs de la subred 12.0.0.0/24 puedan comunicarse entre sí (VLAN200). Una vez hecha la configuación, `r1` envía una solicitud de ARP por su `eth0` preguntando por la IP 12.0.0.20. Indica cuál de las siguientes afirmaciones es correcta respecto a `s2`:

a. Recibirá dicha solicitud de ARP por `eth0` SIN etiqueta de VLAN, y la reenviará exclusivamente por `eth5` SIN etiqueta de VLAN.

b. Recibirá dicha solicitud de ARP por `eth0` SIN etiqueta de VLAN, y la reenviará por el resto de sus interfaces SIN etiqueta de VLAN.

c. Recibirá dicha solicitud de ARP por `eth0` CON etiqueta de VLAN200, y la reenviará exclusivamente por `eth5` CON etiqueta de VLAN200.

d. No recibirá dicha solicitud de ARP.

**Pregunta 5**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF. Suponiendo que se desconoce el orden de arranque de los routers, en un instante dado se consulta la tabla de vecinos en un router del escenario, obteniéndose:

```
Neighbor ID     Prio      State            Dead Time     Address        Interface
13.6.0.7          1       Full/Backup        36.00s      13.4.0.7     eth0:13.4.0.8
13.7.0.10         1       Full/DR             4.00s      13.5.0.10    eth1:13.5.0.8
```

Si el router del cuál estamos viendo la información no recibe ningún mensaje de OSPF durante los 4 segundos siguientes, indica cuál de las siguientes afirmaciones es correcta con respecto a ese router del cuál estamos viendo la información:

a. El router se convertiría en DR de la subred 13.5.0.0/16

b. El router se convertiría en DR de la subred 13.6.0.0/16

c. El router se convertiría en DR de la subred 13.7.0.0/16

d. El router no modificaría su situación sobre ser DR o BDR de las subredes a las que está conectado.

**Pregunta 6**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF. Desconociendo el orden en que han arrancado los routers, se ha capturado en el escenario el mensaje que aparece en la siguiente captura de tráfico. Señala cuál de las siguientes afirmaciones es correcta:

a. En el momento de crearse el mensaje de la captura, el router `r7` estaba apagado.

b. El resto de afirmaciones son falsas.

c. Es imposible capturar este mensaje en este escenario.

d. Todos los routers del área 3 han arrancado a la vez (es decir, en un intervalo de 40 segundos)

**Pregunta 7**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF. Supondremos que han arrancado todos los routers a la vez y ha pasado al menos 1 minuto. Después, uno de los routers de la red se ha apagado, y ha estado 1 minuto apagado. Posteriormente, ese router apagado ha vuelto a arrancar, y mientras tanto se ha realizado la siguiente captura de tráfico. Señala cuál de los siguientes routers es que estaba apagado y arrancó mientras se efectuaba la captura:

a. `r7`.

b. `r8`.

c. El router NO puede ser ni `r3`, ni `r7`, ni `r8`.

d. `r3`.

**Pregunta 8**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF. Suponiendo que todos los routers han arrancado a la vez, indica cuál de las siguientes afirmaciones es correcta:

a. `r3` **crea** un Summary-LSA de la red 13.4.0.0/16 con coste 40.

b. `r3` **crea** un Summary-LSA de la red 13.4.0.0/16 con coste 20.

c. `r3` **recibe** un Summary-LSA de la red 13.4.0.0/16 con coste 10.

d. `r3` **recibe** un Summary-LSA de la red 13.4.0.0/16 con coste 40.

**Pregunta 9**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP.

Estudia la configuración de exportación de rutas en `as30-r1`.

Indica cuál de las siguientes afirmaciones sería correcta:

a. La configuración de exportación de rutas en `as30-r1` es correcta.

b. La exportación de rutas hacia AS10 es incorrecta, el resto de exportaciones son correctas.

c. La exportación de rutas hacia AS40 es incorrecta, el resto de exportaciones son correctas.

d. La exportación de rutas hacia AS10 y AS70 son incorrectas, la otra exportación es correcta.

**Pregunta 10**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP.

Estudia la configuración de `LOCAL_PREF` en `as10-r1`.

Indica cuál de las siguientes afirmaciones sería correcta:

a. La configuración de `LOCAL_PREF` es correcta en `as10-r1`.

b. La configuración de `LOCAL_PREF` es incorrecta en `as10-r1`: Se corregiría poniendo un valor de 350 a `confLocalPrefAS20`.

c. La configuración de `LOCAL_PREF` es incorrecta en `as10-r1`: Se corregiría poniendo un valor de 350 a `confLocalPrefAS30`.

d. La configuración de `LOCAL_PREF` es incorrecta en `as10-r1`: Se corregiría poniendo un valor de 150 a `confLocalPrefAS40`.

**Pregunta 11**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP.

Supón que se modifica la configuración del escenario de forma que las reglas de exportación y los valores de `LOCAL_PREF` funcionen correctamente según las relaciones entre sistemas autónomos que se muestran en la figura.

Una vez que todos los routers intercambien la información para configurar sus tablas, se interrumpe el enlace entre AS10 y AS30. Indica cuál de las siguientes afirmaciones es correcta:

a. as30-r1 no enviaría ningún mensaje UPDATE de eliminación de las rutas de las subredes internas de AS10.

b. as30-r1 enviaría únicamente a AS50 un mensaje UPDATE de eliminación de las rutas de las subredes internas de AS10.

c. as30-r1 enviaría a AS40, AS50 y AS70 un mensaje UPDATE de eliminación de las rutas de las subredes internas de AS10.

d. as30-r1 enviaría únicamente a AS40 y AS50 un mensaje UPDATE de eliminación de las rutas de las subredes internas de AS10.

**Pregunta 12**

Sin responder aún

Puntúa como 1,00

Un sistema autónomo tiene asignadas las siguientes subredes: 100.80.0.0/12, 100.96.0.0/12 y 100.112.0.0/12. Indica cuál de las siguientes afirmaciones sería correcta:

a. El sistema autónomo podría realizar la siguiente agrupación 100.80.0.0/12 y 100.96.0.0/11.

b. El sistema autónomo podría realizar la siguiente agrupación: 100.80.0.0/11 y 100.112.0.0/12.

c. El sistema autónomo podría realizar la siguiente agrupación: 100.80.0.0/12 y 100.96.0.0/13.

d. El sistema autónomo no podría realizar ninguna agrupación con esas subredes.

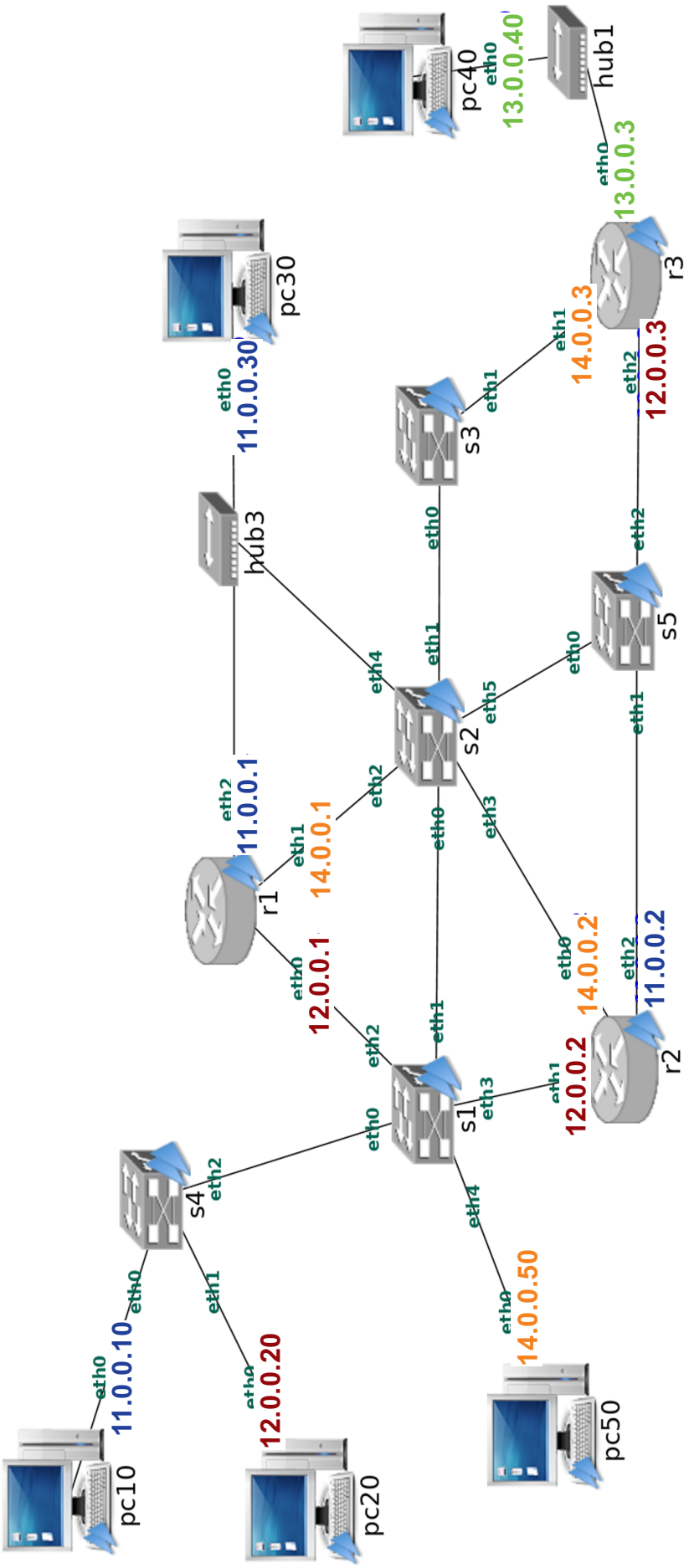



Figura 1: Dispositivos de Interconexión

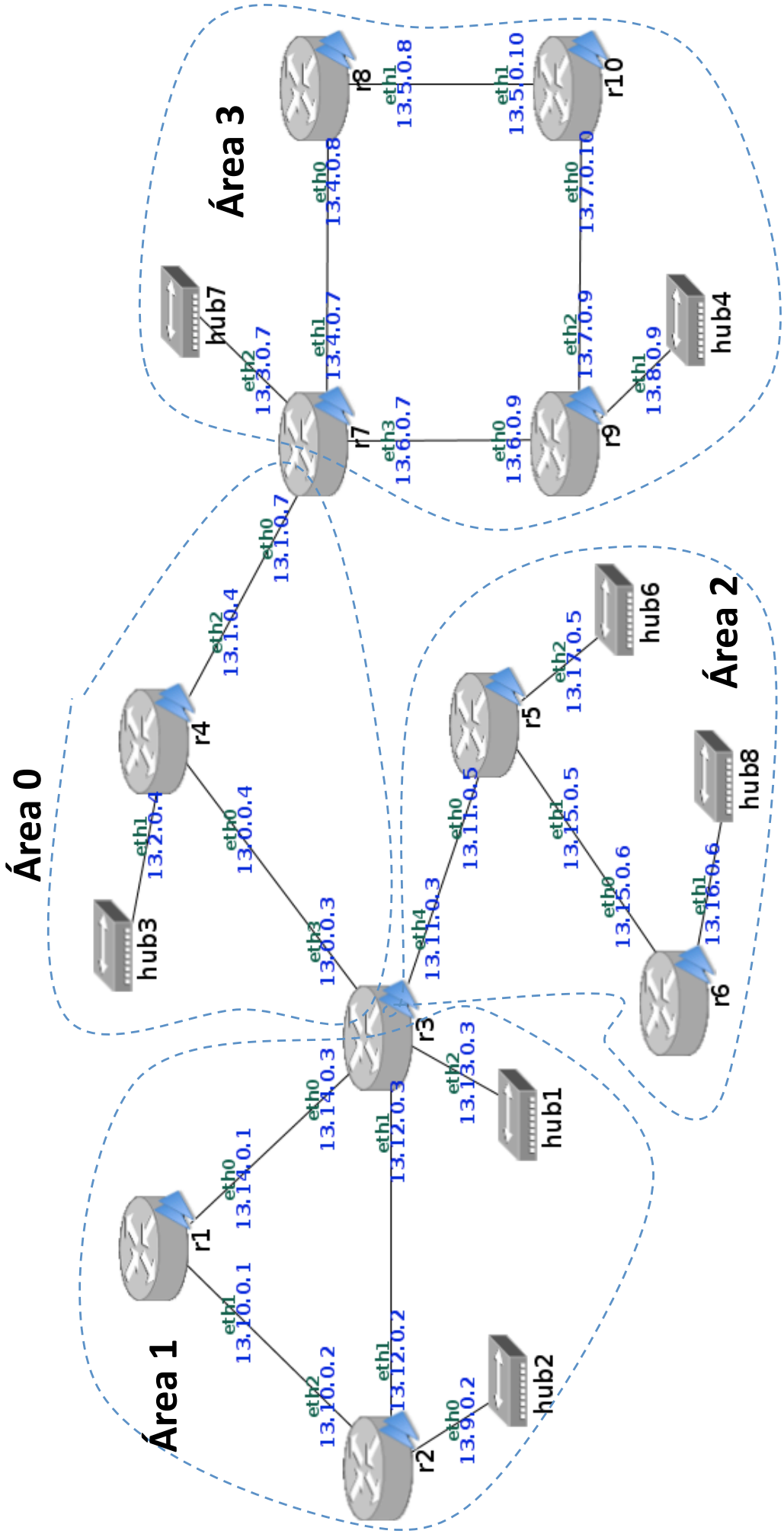



Figura 2: Encaminamiento OSPF

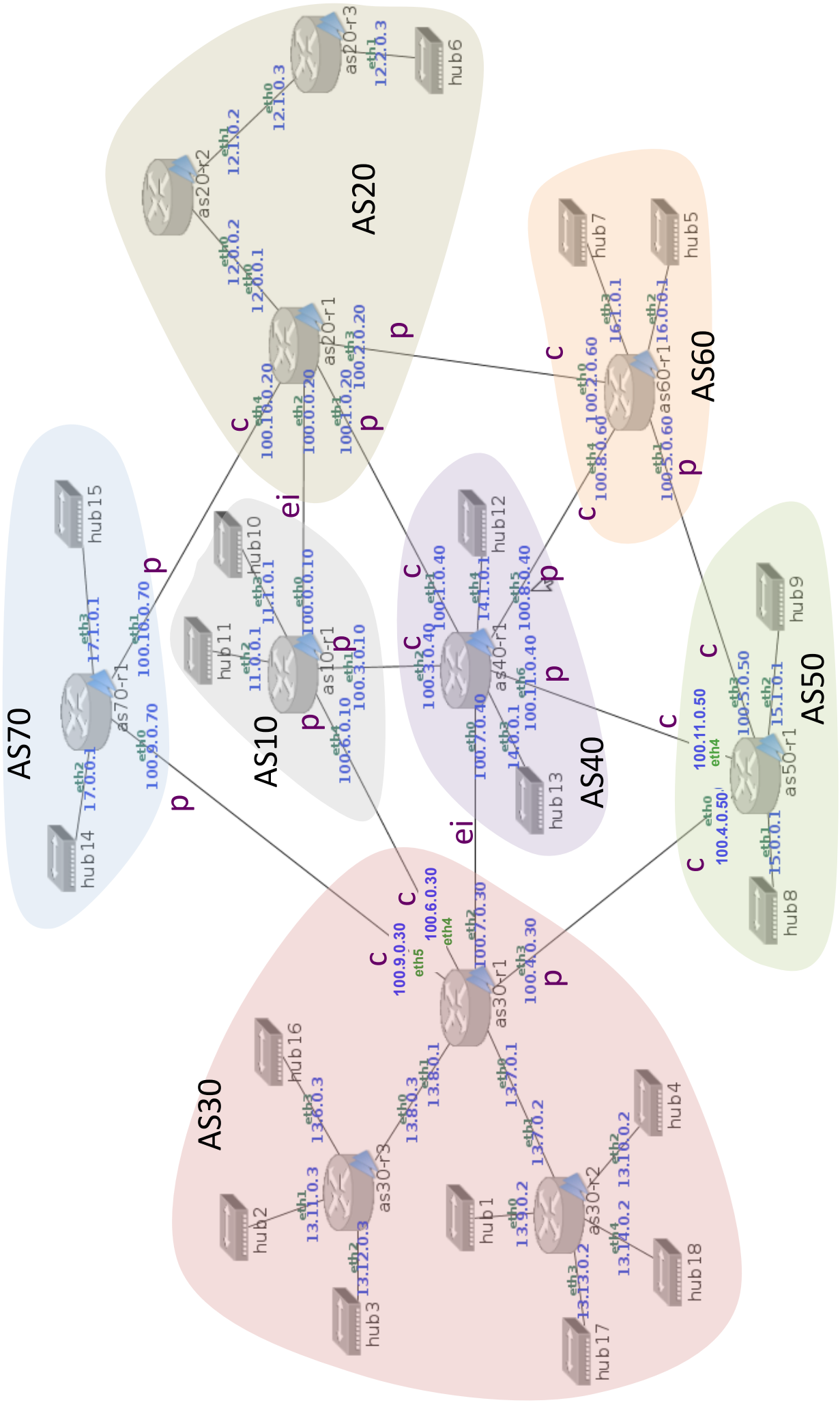



Figura 3: Encaminamiento BGP

# GRADO EN INGENIERIA EN SISTEMAS DE TELECOMUNICACION (FUENLABRADA)

## 2040 - SISTEMAS TELEMATICOS - MAÑANA A - 2Q



**Pregunta 1**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS.

Dada la situación inicial del escenario, y estando la tabla de direcciones aprendidas de los *switches* vacía, y las cachés de ARP de todas las máquinas también vacías, se realiza un *ping* entre `pc20` y `pc50`. Indica cuál de las siguientes afirmaciones es correcta respecto a cuántas de las 3 direcciones Ethernet de las interfaces de `r1` habrá aprendido `s2` al terminar el *ping*:

- a. Habrá aprendido las 3 direcciones Ethernet de las 3 interfaces de `r1`.
- b. Habrá aprendido exclusivamente 2 direcciones Ethernet de 2 interfaces de `r1`.
- c. No habrá aprendido ninguna dirección Ethernet de ninguna de las interfaces de `r1`.
- d. Habrá aprendido exclusivamente 1 dirección Ethernet de 1 interfaz de `r1`.

✖ Quitar mi elección

**Pregunta 2**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS.

Dada la situación inicial del escenario, se rompe el enlace entre 's1' y 's2'. Para que `pc10` pueda hacer un *ping* a `pc30`, se configura adecuadamente *Proxy-ARP* en `r1` y se ajusta su tabla de encaminamiento. Una vez que el *ping* esté de nuevo funcionando, cuál de las siguientes asociaciones estará en la caché de ARP de la máquina `pc10`:

- a. 11.0.0.1 está asociada a `r1-eth0`.
- b. 11.0.0.30 está asociada a `r1-eth0`.
- c. 11.0.0.30 está asociada a `pc30-eth0`.
- d. Ninguna de las otras 3 asociaciones estará en la caché de ARP de `pc10`.

✖ Quitar mi elección

**Pregunta 3**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS.

Dada la situación inicial del escenario, **se APAGAN** `r1` **y** `r2`. Se añade a `r3-eth1` por *IP aliasing* la dirección 11.0.0.1. Se modifica la tabla de encaminamiento de `r3` hasta que sea la siguiente (sólo se muestran las columnas más relevantes):

```
Destination     Gateway         Iface
13.0.0.0        *               eth0
14.0.0.0        *               eth1
12.0.0.0        *               eth2
11.0.0.0        *               eth1
```

Señala cuál de las siguientes afirmaciones es correcta:

- a. Es necesario eliminar una ruta a la tabla de encaminamiento de `r3` para permitir a `pc40` y `pc10` intercambiar datagramas IP.
- b. Es necesario añadir una ruta a la tabla de encaminamiento de `r3` para permitir a `pc40` y `pc10` intercambiar datagramas IP.
- c. Es necesario añadir una dirección IP adicional por *IP aliasing* a `r3` para permitir a `pc40` y `pc10` intercambiar datagramas IP.
- d. Esta configuración de `r3` permitirá a `pc40` y `pc10` intercambiar datagramas IP.

✖ Quitar mi elección

**Pregunta 4**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS.

Partiendo de las situación inicial del escenario, se configuran VLANs para que todas las interfaces con IPs de la subred 11.0.0.0/24 puedan comunicarse entre sí (VLAN100), y que todas las interfaces con IPs de la subred 12.0.0.0/24 puedan comunicarse entre sí (VLAN200). Una vez hecha la configuación, `r1` envía una solicitud de ARP por su `eth0` preguntando por la IP 12.0.0.20. Indica cuál de las siguientes afirmaciones es correcta respecto a `s2`:

- a. Recibirá dicha solicitud de ARP por `eth0` SIN etiqueta de VLAN, y la reenviará exclusivamente por `eth5` SIN etiqueta de VLAN.
- b. Recibirá dicha solicitud de ARP por `eth0` SIN etiqueta de VLAN, y la reenviará por el resto de sus interfaces SIN etiqueta de VLAN.
- c. Recibirá dicha solicitud de ARP por `eth0` CON etiqueta de VLAN200, y la reenviará exclusivamente por `eth5` CON etiqueta de VLAN200.
- d. No recibirá dicha solicitud de ARP.

✖ Quitar mi elección

**Pregunta 5**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF. Suponiendo que se desconoce el orden de arranque de los routers, en un instante dado se consulta la tabla de vecinos en un router del escenario, obteniéndose:

```
Neighbor ID     Prio       State           Dead Time     Address         Interface
13.6.0.7           1       Full/Backup        36.00s     13.4.0.7      eth0:13.4.0.8
13.7.0.10          1       Full/DR             4.00s     13.5.0.10     eth1:13.5.0.8
```

Si el router del cuál estamos viendo la información no recibe ningún mensaje de OSPF durante los 4 segundos siguientes, indica cuál de las siguientes afirmaciones es correcta con respecto a ese router del cuál estamos viendo la información:

- a. El router se convertiría en DR de la subred 13.5.0.0/16
- b. El router se convertiría en DR de la subred 13.6.0.0/16
- c. El router se convertiría en DR de la subred 13.7.0.0/16
- d. El router no modificaría su situación sobre ser DR o BDR de las subredes a las que está conectado.

✖ Quitar mi elección

**Pregunta 6**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF. Desconociendo el orden en que han arrancado los routers, se ha capturado en el escenario el mensaje que aparece en la siguiente captura de tráfico. Señala cuál de las siguientes afirmaciones es correcta:

- a. En el momento de crearse el mensaje de la captura, el router `r7` estaba apagado.
- b. El resto de afirmaciones son falsas.
- c. Es imposible capturar este mensaje en este escenario.
- d. Todos los routers del área 3 han arrancado a la vez (es decir, en un intervalo de 40 segundos)

✖ Quitar mi elección

**Pregunta 7**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF. Supondremos que han arrancado todos los routers a la vez y ha pasado al menos 1 minuto. Después, uno de los routers de la red se ha apagado, y ha estado 1 minuto apagado. Posteriormente, ese router apagado ha vuelto a arrancar, y mientras tanto se ha realizado la siguiente captura de tráfico. Señala cuál de los siguientes routers es que estaba apagado y arrancó mientras se efectuaba la captura:

- a. `r7`.
- b. `r8`.
- c. El router NO puede ser ni `r3`, ni `r7`, ni `r8`.
- d. `r3`.

✖ Quitar mi elección

**Pregunta 8**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF. Suponiendo que todos los routers han arrancado a la vez, indica cuál de las siguientes afirmaciones es correcta:

a. `r3` **crea** un Summary-LSA de la red 13.4.0.0/16 con coste 40.

b. `r3` **crea** un Summary-LSA de la red 13.4.0.0/16 con coste 20.

c. `r3` **recibe** un Summary-LSA de la red 13.4.0.0/16 con coste 10.

d. `r3` **recibe** un Summary-LSA de la red 13.4.0.0/16 con coste 40.

✖ Quitar mi elección

**Pregunta 9**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP.

Estudia la configuración de exportación de rutas en `as30-r1`.

Indica cuál de las siguientes afirmaciones sería correcta:

a. La configuración de exportación de rutas en `as30-r1` es correcta.

b. La exportación de rutas hacia AS10 es incorrecta, el resto de exportaciones son correctas.

c. La exportación de rutas hacia AS40 es incorrecta, el resto de exportaciones son correctas.

d. La exportación de rutas hacia AS10 y AS70 son incorrectas, la otra exportación es correcta.

✖ Quitar mi elección

**Pregunta 10**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP.

Estudia la configuración de `LOCAL_PREF` en `as10-r1`.

Indica cuál de las siguientes afirmaciones sería correcta:

a. La configuración de `LOCAL_PREF` es correcta en `as10-r1`.

b. La configuración de `LOCAL_PREF` es incorrecta en `as10-r1`: Se corregiría poniendo un valor de 350 a `confLocalPrefAS20`.

c. La configuración de `LOCAL_PREF` es incorrecta en `as10-r1`: Se corregiría poniendo un valor de 350 a `confLocalPrefAS30`.

d. La configuración de `LOCAL_PREF` es incorrecta en `as10-r1`: Se corregiría poniendo un valor de 150 a `confLocalPrefAS40`.

✖ Quitar mi elección

**Pregunta 11**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP.

Supón que se modifica la configuración del escenario de forma que las reglas de exportación y los valores de `LOCAL_PREF` funcionen correctamente según las relaciones entre sistemas autónomos que se muestran en la figura.

Una vez que todos los routers intercambien la información para configurar sus tablas, se interrumpe el enlace entre AS10 y AS30. Indica cuál de las siguientes afirmaciones es correcta:

a. as30-r1 no enviaría ningún mensaje UPDATE de eliminación de las rutas de las subredes internas de AS10.

b. as30-r1 enviaría únicamente a AS50 un mensaje UPDATE de eliminación de las rutas de las subredes internas de AS10.

c. as30-r1 enviaría a AS40, AS50 y AS70 un mensaje UPDATE de eliminación de las rutas de las subredes internas de AS10.

d. as30-r1 enviaría únicamente a AS40 y AS50 un mensaje UPDATE de eliminación de las rutas de las subredes internas de AS10.

✖ Quitar mi elección

Pregunta 12

Sin responder aún

Puntúa como 1,00

Un sistema autónomo tiene asignadas las siguientes subredes: 100.80.0.0/12, 100.96.0.0/12 y 100.112.0.0/12. Indica cuál de las siguientes afirmaciones sería correcta:

- a. El sistema autónomo podría realizar la siguiente agrupación 100.80.0.0/12 y 100.96.0.0/11.
- b. El sistema autónomo podría realizar la siguiente agrupación: 100.80.0.0/11 y 100.112.0.0/12.
- c. El sistema autónomo podría realizar la siguiente agrupación: 100.80.0.0/12 y 100.96.0.0/13.
- d. El sistema autónomo no podría realizar ninguna agrupación con esas subredes.

✖ Quitar mi elección

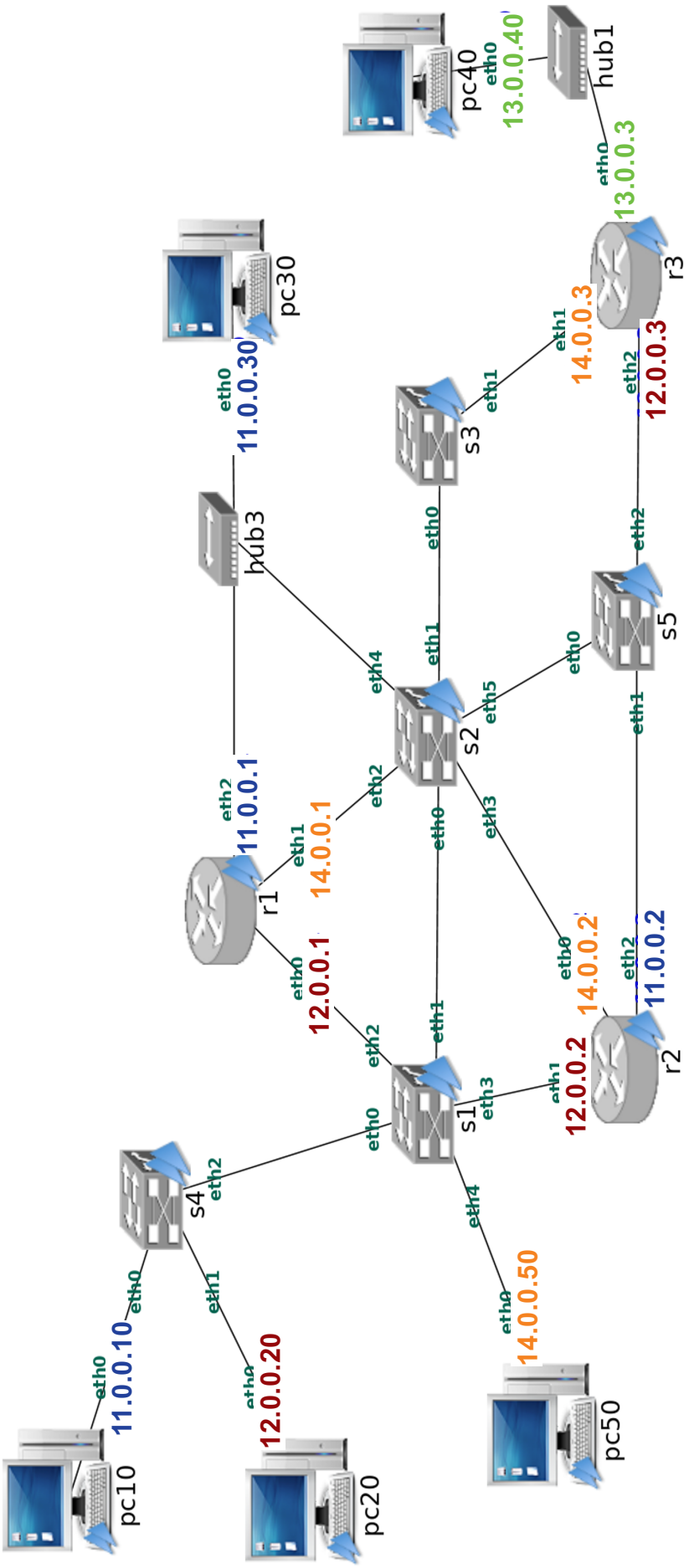



Figura 1: Dispositivos de Interconexión

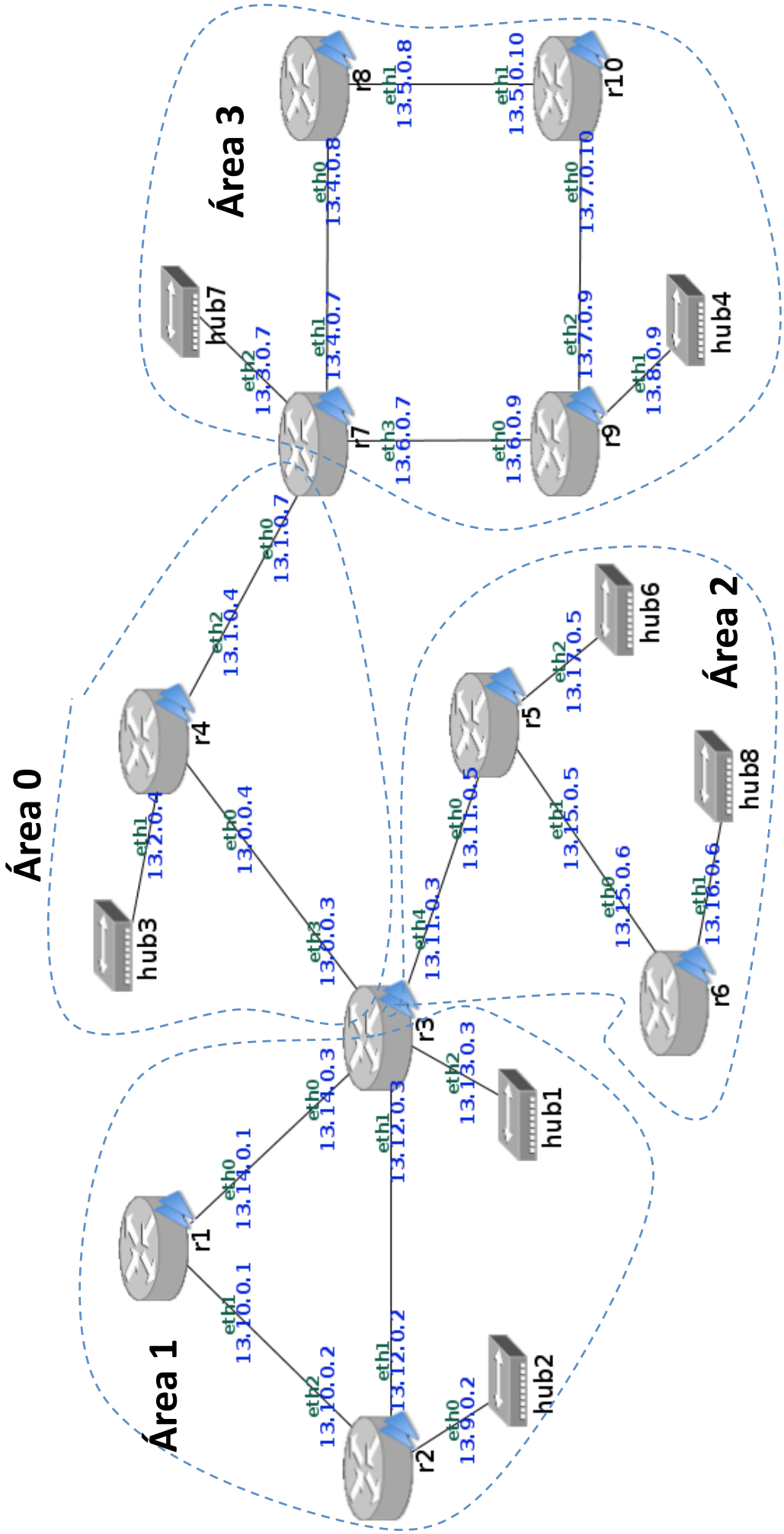



Figura 2: Encaminamiento OSPF

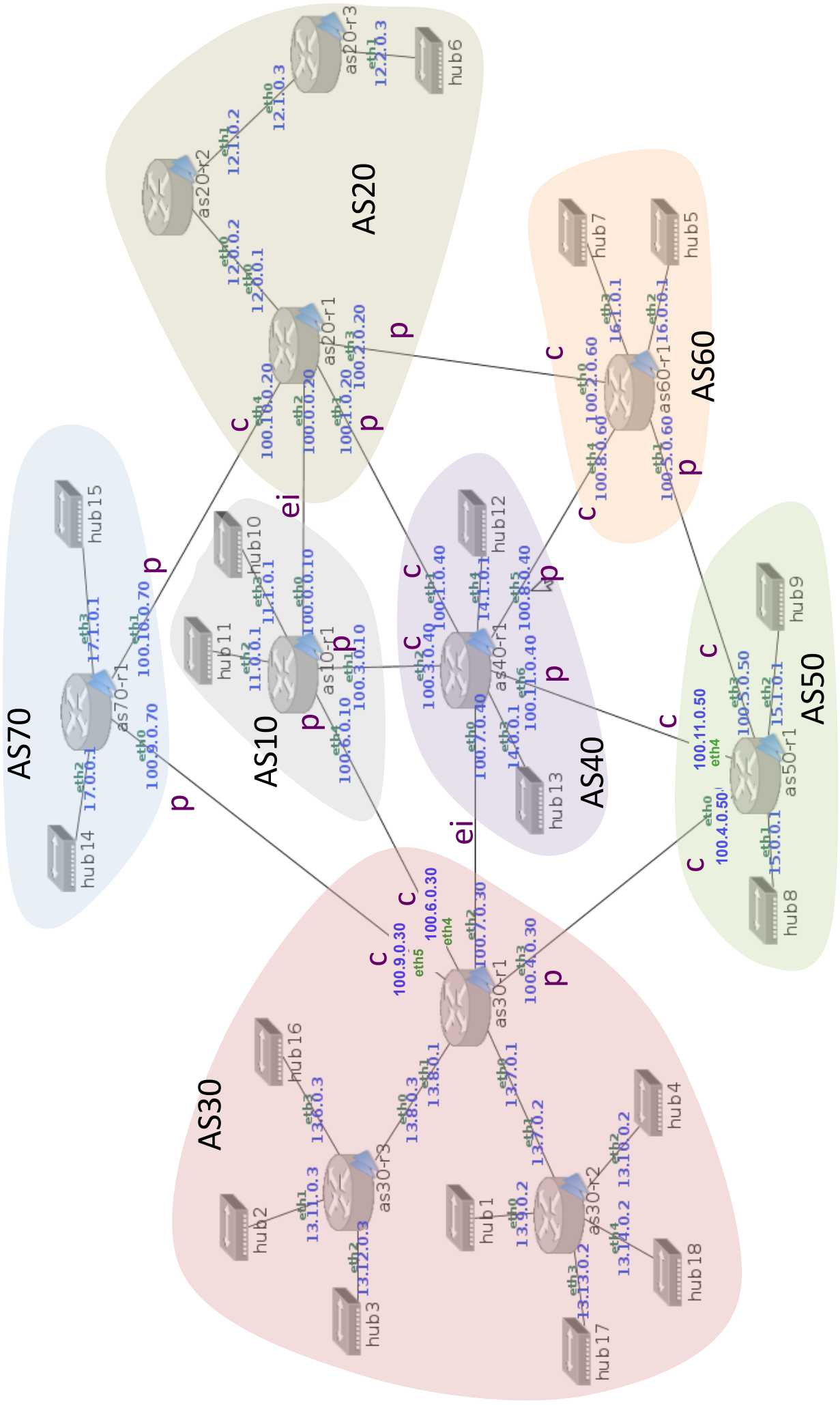



Figura 3: Encaminamiento BGP

# GRADO EN INGENIERIA EN SISTEMAS DE TELECOMUNICACION (FUENLABRADA)

## 2040 - SISTEMAS TELEMATICOS - MAÑANA A - 2Q



Pregunta **1**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF, con todos los routers arrancados a la vez y habiendo pasado al menos 1 minuto.

Después, uno de los routers de la red se ha apagado, y ha estado 1 minuto apagado. Posteriormente, ese router apagado ha vuelto a arrancar, y mientras tanto se ha realizado la siguiente captura de tráfico.

Señala cuál de los siguientes routers es el que estaba apagado y arrancó mientras se efectuaba la captura:

- a. r5.
- b. El router NO puede ser ni r3, ni r5, ni r7.
- c. r7.
- d. r1.

Pregunta **2**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF, con todos los routers arrancados a la vez.

Transcurrido al menos 1 minuto de que hayan arrancado todos los routers, uno de los routers del escenario se ha apagado y, transcurrido 1 minuto ha vuelto arrancar. 1 minuto después de que todos los routers vuelvan a estar arrancados de nuevo, se consulta la tabla de vecinos en un router del escenario, obteniéndose:

```
Neighbor ID     Prio       State           Dead Time     Address       Interface
13.14.0.1          1       Full/Backup        5.00s      13.10.0.1    eth2:13.10.0.2
13.14.0.3          1       Full/DR            4.00s      13.12.0.3    eth1:13.12.0.2
```

Indica cuál de las siguientes afirmaciones es correcta::

- a. El router apagado y vuelto a arrancar ha sido `r2`.
- b. El router apagado y vuelto a arrancar ha sido `r1`.
- c. De la tabla de vecinos mostrada no se puede deducir cuál es el router apagado y vuelto a arrancar.
- d. El router apagado y vuelto a arrancar ha sido `r3`.

Pregunta **3**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP.

Supón que se corrigen en el escenario la configuraciones incorrectas de exportación y de `LOCAL_PREF` según las relaciones entre sistemas autónomos que se muestran en la figura.

Una vez que todos los routers intercambien la información para configurar sus tablas, se interrumpe el enlace entre AS40 y AS60. Indica cuál de las siguientes afirmaciones es correcta:

a. `as40-r1` enviaría únicamente a AS10, AS20 y AS30 un mensaje UPDATE de eliminación de las rutas de las subredes internas de AS60.

b. `as40-r1` enviaría únicamente a AS30 y AS50 un mensaje UPDATE de eliminación de las rutas de las subredes internas de AS60.

c. `as40-r1` enviaría a AS10, AS20, AS30 y AS50 un mensaje UPDATE de eliminación de las rutas de las subredes internas de AS60.

d. `as40-r1` enviaría únicamente a AS50 un mensaje UPDATE de eliminación de las rutas de las subredes internas de AS60.

Pregunta **4**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP.

Estudia la configuración de `LOCAL_PREF` en `as30-r1`.

Indica cuál de las siguientes afirmaciones es correcta:

a. La configuración de `LOCAL_PREF` es incorrecta en `as30-r1`. Se corregiría eliminando la configuración de `LOCA_PREF` asociada a `confLocalPrefAS50`y manteniendo el resto de configuraciones de `LOCAL_PREF` en `as30-r1`.

b. La configuración de `LOCAL_PREF` es incorrecta en `as30-r1`. Se corregiría eliminando la configuración de `LOCA_PREF` asociada a `confLocalPrefAS40` y manteniendo el resto de configuraciones de `LOCAL_PREF` en `as30-r1`.

c. La configuración de `LOCAL_PREF` es incorrecta en `as30-r1`. Se corregiría eliminando la configuración de `LOCA_PREF` asociada a `confLocalPrefAS40` y a `confLocalPrefAS50`. Se mantendría el resto de configuraciones de `LOCAL_PREF` en `as30-r1`.

d. La configuración de `LOCAL_PREF` es correcta en `as30-r1`.

Pregunta **5**

Sin responder aún

Puntúa como 1,00

Un sistema autónomo tiene asignadas las siguientes subredes: 100.0.0.0/13, 100.8.0.0/13 y 100.240.0.0/13 y 100.248.0.0/13. Indica cuál de las siguientes afirmaciones sería correcta:

a. El sistema autónomo podría realizar la siguiente agrupación: 100.0.0.0/12, 100.240.0.0/13, 100.248.0.0/13.

b. El sistema autónomo podría realizar la siguiente agrupación: 100.0.0.0/11.

c. El sistema autónomo podría realizar la siguiente agrupación 100.0.0.0/12 y 100.240.0.0/12.

d. El sistema autónomo no podría realizar ninguna agrupación con esas subredes.

Pregunta **6**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF, con todos los routers arrancados a la vez y habiendo pasado al menos 1 minuto.

Indica qué información tendrá almacenada r1 en su BD de mensajes Router-LSA sobre el Router-LSA generado por r7:

a. Tendrá información de las 3 interfaces transit y 1 interfaz stub de `r7`.

b. Únicamente tendrá información de 2 interfaces transit y 1 interfaz stub de `r7`.

c. No tendrá información de ninguna de las interfaces de `r7`.

d. Únicamente tendrá información de 1 interfaz transit de `r7`.

Pregunta **7**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS.

Dada la situación inicial del escenario, en un momento dado se consulta la tabla de direcciones aprendidas de `s2`, cuyo contenido se puede ver a continuación (únicamente se han omitido las direcciones locales):

```
port no     mac addr       is local?      ageing timer
3           r1(eth1)          no             50
2           r3(eth1)          no             50
```

Indica cuál de las siguientes afirmaciones es correcta respecto a la tabla de direcciones aprendidas de `s2`:

- a. Se ha ejecutado un `ping` entre `pc40` y `pc30` hace menos de 1 minuto.
- b. Se ha ejecutado un `ping` entre `pc40` y 14.0.0.1 hace menos de 1 minuto.
- c. Se ha ejecutado un `ping` entre `pc40` y `pc50` hace menos de 1 minuto.
- d. Se ha ejecutado un `ping` entre `pc40` y 14.0.0.2 hace menos de 1 minuto.

Pregunta **8**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS.

Partiendo de las situación inicial del escenario, se configuran VLANs para que todas las interfaces con IPs de la subred 11.0.0.0/24 puedan comunicarse entre sí (VLAN100), que todas las interfaces con IPs de la subred 12.0.0.0/24 puedan comunicarse entre sí (VLAN200) y que todas las interfaces con IPs de la subred 14.0.0.0/24 puedan comunicarse entre sí (VLAN400). Una vez hecha la configuación, `r2` envía una solicitud de ARP por su `eth0` preguntando por la IP 14.0.0.50. Indica cuál de las siguientes afirmaciones es correcta respecto a `s2`:

- a. `s2` añadirá etiqueta VLAN400 a dicha solicitud ARP y la reenviará por las siguientes interfaces: `eth0` y `eth1`. Además, `s2` reenviará dicha solicitud ARP sin etiqueta VLAN a través de su interfaz `eth2`, `eth4` y `eth5`.
- b. `s2` añadirá etiqueta VLAN400 a dicha solicitud ARP y la reenviará únicamente por su interfaz `eth0`. El switch `s2` no reenviará nada por el resto de interfaces.
- c. `s2` añadirá etiqueta VLAN400 a dicha solicitud ARP y la reenviará por las siguientes interfaces: `eth0` y `eth1`. Además, `s2` reenviará dicha solicitud ARP sin etiqueta VLAN a través de su interfaz `eth2`. El switch `s2` no reenviará nada por el resto de interfaces.
- d. `s2` añadirá etiqueta VLAN400 a dicha solicitud ARP y la reenviará por las siguientes interfaces: `eth0`, `eth2` y `eth1`. El switch `s2` no reenviará nada por el resto de interfaces.

Pregunta **9**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS. Si se configura IP aliasing en `r3(eth2)` añadiendo la dirección IP 11.0.0.3 y sin realizar ninguna otra configuración adicional, indica cuál de las siguientes afirmaciones sería la correcta:

- a. Esta configuración permitirá a `r3` comunicarse directamente con todas las máquinas en la subred 11.0.0.0/24, sin necesidad de otro router.
- b. Esta configuración permitirá que `pc30` se comunique con `pc40` a través de `r3` sin necesidad de otro router.
- c. Esta configuración permitirá que `pc10` se comunique con `pc40` a través de `r3` sin necesidad de otro router.
- d. Esta configuración permitirá que `pc50` se comunique con `pc40` a través de `r3` sin necesidad de otro router.

Pregunta **10**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF, con todos los routers arrancados a la vez y habiendo pasado al menos 1 minuto.

Indica cuál de las siguientes afirmaciones es correcta:

a. En las bases de datos de LSAs de `r2` hay 13 Summary-LSAs diferentes.

b. En las bases de datos de LSAs de `r2` hay 9 Summary-LSAs diferentes.

c. En las bases de datos de LSAs de `r2` hay 4 Summary-LSAs diferentes.

d. En las bases de datos de LSAs de `r2` hay 18 Summary-LSAs diferentes.

Pregunta **11**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS.

Dada la situación inicial del escenario, se rompe el enlace entre 's1' y 's2'. Para que `pc50` pueda hacer un *ping* a `14.0.0.3`, se va a configurar *Proxy-ARP* en `r2`.
Indica cuál de las siguientes afirmaciones es correcta:

a. Es necesario y suficiente:
- activar proxy-ARP en `r2(eth1)` para que `r2` responda por la solicitud de ARP que pregunta por 14.0.0.3
- configurar una ruta en `r2` que permita alcanzar 14.0.0.3 a través de la interfaz `r2(eth0)`
- activar proxy-ARP en `r2(eth0)` para que `r2` responda por la solicitud de ARP que pregunta por 14.0.0.50

b. Es necesario y suficiente:
- activar proxy-ARP en `r2(eth1)` para que `r2` responda por la solicitud de ARP que pregunta por 14.0.0.3
- activar proxy-ARP en `r2(eth0)` para que `r2` responda por la solicitud de ARP que pregunta por 14.0.0.50

c. Es necesario y suficiente:
- activar proxy-ARP en `r2(eth1)` para que `r2` responda por la solicitud de ARP que pregunta por 14.0.0.3
- configurar una ruta en `r2` que permita alcanzar 14.0.0.50 a través de la interfaz `r2(eth1)`
- activar proxy-ARP en `r2(eth0)` para que `r2` responda por la solicitud de ARP que pregunta por 14.0.0.50

d. Es necesario y suficiente:
- activar proxy-ARP en `r2(eth1)` para que r2 responda por la solicitud de ARP que pregunta por 14.0.0.3
- configurar una ruta en `r2` que permita alcanzar 14.0.0.3 a través de la interfaz `r2(eth0)`
- activar proxy-ARP en `r2(eth0)` para que r2 responda por la solicitud de ARP que pregunta por 14.0.0.50 y
- configurar una ruta en `r2` que permita alcanzar 14.0.0.50 a través de la interfaz `r2(eth1)`

Pregunta **12**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP.

Estudia la configuración de exportación de rutas en `as10-r1`.

Indica cuál de las siguientes afirmaciones es correcta:

a. La exportación de rutas hacia AS20 es incorrecta, el resto de exportaciones son correctas.

b. La configuración de exportación de rutas en `as10-r1` es correcta.

c. Todas las exportaciones en `as10-r1` son incorrectas ya que no hay ninguna lista de exportación definida.

d. Las exportaciones de rutas hacia AS40 y AS30 son incorrectas, la otra exportación es correcta.

# GRADO EN INGENIERIA EN SISTEMAS DE TELECOMUNICACION (FUENLABRADA)

## 2040 - SISTEMAS TELEMATICOS - MAÑANA A - 2Q



Pregunta **1**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF, con todos los routers arrancados a la vez y habiendo pasado al menos 1 minuto.

Despúes, uno de los routers de la red se ha apagado, y ha estado 1 minuto apagado. Posteriormente, ese router apagado ha vuelto a arrancar, y mientras tanto se ha realizado la siguiente captura de tráfico.

Señala cuál de los siguientes routers es el que estaba apagado y arrancó mientras se efectuaba la captura:

- a. r5.
- b. El router NO puede ser ni r3, ni r5, ni r7.
- c. r7.
- d. r1.

Quitar mi elección

Pregunta **2**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF, con todos los routers arrancados a la vez.

Transcurrido al menos 1 minuto de que hayan arrancado todos los routers, uno de los routers del escenario se ha apagado y, transcurrido 1 minuto ha vuelto arrancar. 1 minuto después de que todos los routers vuelvan a estar arrancados de nuevo, se consulta la tabla de vecinos en un router del escenario, obteniéndose:

```
Neighbor ID     Prio      State           Dead Time     Address       Interface
13.14.0.1         1       Full/Backup        5.00s      13.10.0.1    eth2:13.10.0.2
13.14.0.3         1       Full/DR            4.00s      13.12.0.3    eth1:13.12.0.2
```

Indica cuál de las siguientes afirmaciones es correcta::

- a. El router apagado y vuelto a arrancar ha sido `r2`.
- b. El router apagado y vuelto a arrancar ha sido `r1`.
- c. De la tabla de vecinos mostrada no se puede deducir cuál es el router apagado y vuelto a arrancar.
- d. El router apagado y vuelto a arrancar ha sido `r3`.

Quitar mi elección

Pregunta **3**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP.

Supón que se corrigen en el escenario la configuraciones incorrectas de exportación y de `LOCAL_PREF` según las relaciones entre sistemas autónomos que se muestran en la figura.

Una vez que todos los routers intercambien la información para configurar sus tablas, se interrumpe el enlace entre AS40 y AS60. Indica cuál de las siguientes afirmaciones es correcta:

a. `as40-r1` enviaría únicamente a AS10, AS20 y AS30 un mensaje UPDATE de eliminación de las rutas de las subredes internas de AS60.

b. `as40-r1` enviaría únicamente a AS30 y AS50 un mensaje UPDATE de eliminación de las rutas de las subredes internas de AS60.

c. `as40-r1` enviaría a AS10, AS20, AS30 y AS50 un mensaje UPDATE de eliminación de las rutas de las subredes internas de AS60.

d. `as40-r1` enviaría únicamente a AS50 un mensaje UPDATE de eliminación de las rutas de las subredes internas de AS60.

Quitar mi elección

Pregunta **4**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP.

Estudia la configuración de `LOCAL_PREF` en `as30-r1`.

Indica cuál de las siguientes afirmaciones es correcta:

a. La configuración de `LOCAL_PREF` es incorrecta en `as30-r1`. Se corregiría eliminando la configuración de `LOCA_PREF` asociada a `confLocalPrefAS50`y manteniendo el resto de configuraciones de `LOCAL_PREF` en `as30-r1`.

b. La configuración de `LOCAL_PREF` es incorrecta en `as30-r1`. Se corregiría eliminando la configuración de `LOCA_PREF` asociada a `confLocalPrefAS40` y manteniendo el resto de configuraciones de `LOCAL_PREF` en `as30-r1`.

c. La configuración de `LOCAL_PREF` es incorrecta en `as30-r1`. Se corregiría eliminando la configuración de `LOCA_PREF` asociada a `confLocalPrefAS40` y a `confLocalPrefAS50`. Se mantendría el resto de configuraciones de `LOCAL_PREF` en `as30-r1`.

d. La configuración de `LOCAL_PREF` es correcta en `as30-r1`.

Quitar mi elección

Pregunta **5**

Sin responder aún

Puntúa como 1,00

Un sistema autónomo tiene asignadas las siguientes subredes: 100.0.0.0/13, 100.8.0.0/13 y 100.240.0.0/13 y 100.248.0.0/13. Indica cuál de las siguientes afirmaciones sería correcta:

a. El sistema autónomo podría realizar la siguiente agrupación: 100.0.0.0/12, 100.240.0.0/13, 100.248.0.0/13.

b. El sistema autónomo podría realizar la siguiente agrupación: 100.0.0.0/11.

c. El sistema autónomo podría realizar la siguiente agrupación 100.0.0.0/12 y 100.240.0.0/12.

d. El sistema autónomo no podría realizar ninguna agrupación con esas subredes.

Quitar mi elección

Pregunta **6**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF, con todos los routers arrancados a la vez y habiendo pasado al menos 1 minuto.

Indica qué información tendrá almacenada r1 en su BD de mensajes Router-LSA sobre el Router-LSA generado por r7:

a. Tendrá información de las 3 interfaces transit y 1 interfaz stub de `r7`.

b. Únicamente tendrá información de 2 interfaces transit y 1 interfaz stub de `r7`.

c. No tendrá información de ninguna de las interfaces de `r7`.

d. Únicamente tendrá información de 1 interfaz transit de `r7`.

Quitar mi elección

Pregunta **7**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS.

Dada la situación inicial del escenario, en un momento dado se consulta la tabla de direcciones aprendidas de `s2`, cuyo contenido se puede ver a continuación (únicamente se han omitido las direcciones locales):

```
port no     mac addr       is local?      ageing timer
3           r1(eth1)          no             50
2           r3(eth1)          no             50
```

Indica cuál de las siguientes afirmaciones es correcta respecto a la tabla de direcciones aprendidas de `s2`:

a. Se ha ejecutado un `ping` entre `pc40` y `pc30` hace menos de 1 minuto.

b. Se ha ejecutado un `ping` entre `pc40` y 14.0.0.1 hace menos de 1 minuto.

c. Se ha ejecutado un `ping` entre `pc40` y `pc50` hace menos de 1 minuto.

d. Se ha ejecutado un `ping` entre `pc40` y 14.0.0.2 hace menos de 1 minuto.

Quitar mi elección

Pregunta **8**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS.

Partiendo de las situación inicial del escenario, se configuran VLANs para que todas las interfaces con IPs de la subred 11.0.0.0/24 puedan comunicarse entre sí (VLAN100), que todas las interfaces con IPs de la subred 12.0.0.0/24 puedan comunicarse entre sí (VLAN200) y que todas las interfaces con IPs de la subred 14.0.0.0/24 puedan comunicarse entre sí (VLAN400). Una vez hecha la configuación, `r2` envía una solicitud de ARP por su `eth0` preguntando por la IP 14.0.0.50. Indica cuál de las siguientes afirmaciones es correcta respecto a `s2`:

a. `s2` añadirá etiqueta VLAN400 a dicha solicitud ARP y la reenviará por las siguientes interfaces: `eth0` y `eth1`. Además, `s2` reenviará dicha solicitud ARP sin etiqueta VLAN a través de su interfaz `eth2`, `eth4` y `eth5`.

b. `s2` añadirá etiqueta VLAN400 a dicha solicitud ARP y la reenviará únicamente por su interfaz `eth0`. El switch `s2` no reenviará nada por el resto de interfaces.

c. `s2` añadirá etiqueta VLAN400 a dicha solicitud ARP y la reenviará por las siguientes interfaces: `eth0` y `eth1`. Además, `s2` reenviará dicha solicitud ARP sin etiqueta VLAN a través de su interfaz `eth2`. El switch `s2` no reenviará nada por el resto de interfaces.

d. `s2` añadirá etiqueta VLAN400 a dicha solicitud ARP y la reenviará por las siguientes interfaces: `eth0`, `eth2` y `eth1`. El switch `s2` no reenviará nada por el resto de interfaces.

Quitar mi elección

Pregunta **9**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS. Si se configura IP aliasing en `r3(eth2)` añadiendo la dirección IP 11.0.0.3 y sin realizar ninguna otra configuración adicional, indica cuál de las siguientes afirmaciones sería la correcta:

- a. Esta configuración permitirá a `r3` comunicarse directamente con todas las máquinas en la subred 11.0.0.0/24, sin necesidad de otro router.
- b. Esta configuración permitirá que `pc30` se comunique con `pc40` a través de `r3` sin necesidad de otro router.
- c. Esta configuración permitirá que `pc10` se comunique con `pc40` a través de `r3` sin necesidad de otro router.
- d. Esta configuración permitirá que `pc50` se comunique con `pc40` a través de `r3` sin necesidad de otro router.

Quitar mi elección

Pregunta **10**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF, con todos los routers arrancados a la vez y habiendo pasado al menos 1 minuto.

Indica cuál de las siguientes afirmaciones es correcta:

- a. En las bases de datos de LSAs de `r2` hay 13 Summary-LSAs diferentes.
- b. En las bases de datos de LSAs de `r2` hay 9 Summary-LSAs diferentes.
- c. En las bases de datos de LSAs de `r2` hay 4 Summary-LSAs diferentes.
- d. En las bases de datos de LSAs de `r2` hay 18 Summary-LSAs diferentes.

Quitar mi elección

Pregunta **11**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS.

Dada la situación inicial del escenario, se rompe el enlace entre 's1' y 's2'. Para que `pc50` pueda hacer un *ping* a `14.0.0.3`, se va a configurar *Proxy-ARP* en `r2`.
Indica cuál de las siguientes afirmaciones es correcta:

- a. Es necesario y suficiente:
  - activar proxy-ARP en `r2(eth1)` para que `r2` responda por la solicitud de ARP que pregunta por 14.0.0.3
  - configurar una ruta en `r2` que permita alcanzar 14.0.0.3 a través de la interfaz `r2(eth0)`
  - activar proxy-ARP en `r2(eth0)` para que `r2` responda por la solicitud de ARP que pregunta por 14.0.0.50
- b. Es necesario y suficiente:
  - activar proxy-ARP en `r2(eth1)` para que `r2` responda por la solicitud de ARP que pregunta por 14.0.0.3
  - activar proxy-ARP en `r2(eth0)` para que `r2` responda por la solicitud de ARP que pregunta por 14.0.0.50
- c. Es necesario y suficiente:
  - activar proxy-ARP en `r2(eth1)` para que `r2` responda por la solicitud de ARP que pregunta por 14.0.0.3
  - configurar una ruta en `r2` que permita alcanzar 14.0.0.50 a través de la interfaz `r2(eth1)`
  - activar proxy-ARP en `r2(eth0)` para que `r2` responda por la solicitud de ARP que pregunta por 14.0.0.50
- d. Es necesario y suficiente:
  - activar proxy-ARP en `r2(eth1)` para que r2 responda por la solicitud de ARP que pregunta por 14.0.0.3
  - configurar una ruta en `r2` que permita alcanzar 14.0.0.3 a través de la interfaz `r2(eth0)`
  - activar proxy-ARP en `r2(eth0)` para que r2 responda por la solicitud de ARP que pregunta por 14.0.0.50 y
  - configurar una ruta en `r2` que permita alcanzar 14.0.0.50 a través de la interfaz `r2(eth1)`

Quitar mi elección

Pregunta **12**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP.

Estudia la configuración de exportación de rutas en `as10-r1`.

Indica cuál de las siguientes afirmaciones es correcta:

a. La exportación de rutas hacia AS20 es incorrecta, el resto de exportaciones son correctas.

b. La configuración de exportación de rutas en `as10-r1` es correcta.

c. Todas las exportaciones en `as10-r1` son incorrectas ya que no hay ninguna lista de exportación definida.

d. Las exportaciones de rutas hacia AS40 y AS30 son incorrectas, la otra exportación es correcta.

Anote las respuestas introducidas en esta página en los últimos minutos, y trate de volver a conectarse.

Una vez que la conexión se haya restablecido, sus respuestas deben ser guardados y este mensaje desaparecerá.

Comenzar una nueva previsualización

# GRADO EN INGENIERIA EN SISTEMAS DE TELECOMUNICACION (FUENLABRADA)

## 2040 - SISTEMAS TELEMATICOS - MAÑANA A - 2Q



Pregunta **1**

Sin responder aún

Puntúa como 1,00

Un servidor HTTP envía el siguiente formulario en un mensaje HTTP:

```
<FORM action="http://pc3.emp3.net/p3.pl" method=POST>
<P>
Asignatura: <INPUT type="text" name="asignatura"><BR>
Curso: <INPUT type="text" name="curso"><BR>
<INPUT type="submit" value="Enviar"><INPUT type="reset">
</P>
</FORM>
```

Si el usuario rellena las cajas del formulario con los siguientes datos: asignatura="redes de ordenadores" y curso=2, indica cuál será la línea inicial del mensaje del cliente para enviar dichos datos al servidor:

a. `POST /p3.pl HTTP/1.1`

b. `POST http://pc3.emp3.net HTTP/1.1`

c. `POST http://pc3.emp3.net/asignatura=redes+de+ordenadores&curso=2 HTTP/1.1`

d. `POST /p3.pl/asignatura=redes+de+ordenadores&curso=2 HTTP/1.1`

Pregunta **2**

Sin responder aún

Puntúa como 1,00

Indica cuál de las siguientes afirmaciones es correcta:

a. Un certificado está firmado digitalmente con la clave privada del dueño del certificado.

b. Un certificado está firmado digitalmente con la clave pública de una CA.

c. Un certificado está firmado digitalmente con la clave pública del dueño del certificado.

d. El resto de las afirmaciones son falsas.

Pregunta **3**

Sin responder aún

Puntúa como 1,00

Un conjunto de amigos $A, B, C, D, E$ utilizan criptografía de clave pública/privada para intercambiar mensajes. Cada uno de los amigos ha conseguido de forma segura las claves públicas del resto. Entre ellos se han puesto de acuerdo para utilizar la función *hash* H.

Cada vez que quiere entrar un amigo Z nuevo en el grupo, tienen que comunicarle de forma segura las claves públicas de todos los miembros del grupo $K_i^+$, donde $i = A, B, C, D, E$, y los miembros del grupo deben obtener de forma segura la clave pública de Z, $K_Z^+$. Para ello, Z quedará personalmente con uno de los miembros del grupo, $i$, y se intercambiarán las claves que necesitan. De esta forma Z ya poseerá las claves públicas de todos los miembros del grupo, $i$ poseerá la clave pública de Z $K_Z^+$, y sólo quedará que $i$ le comunique de forma segura al resto de miembros del grupo esa clave. Se supone que todos los miembros confían en $i$ y en que éste no va a enviarles una $K_Z^+$ falsa.

Indica cuál de los siguientes mensajes enviados por $i$ a otro miembro del grupo $j$ es un mecanismo seguro para que $i$ le pueda pasar a $j$ la clave $K_Z^+$:

- a. `mensaje`$= K_i^+(nombre = Z, clave = K_Z^+)$ ; `firma`$= K_j^+(H(mensaje))$
- b. `mensaje`$= (nombre = Z, clave = K_Z^+)$ ; `firma`$= K_i^-(H(mensaje))$
- c. `mensaje`$= K_i^+(nombre = Z, clave = K_Z^+)$
- d. `mensaje`$= K_j^+(nombre = Z, clave = K_Z^+)$

Pregunta **4**

Sin responder aún

Puntúa como 1,00

Un navegador recibe un recurso del cuál sólo se muestra un conjunto de líneas de cabecera del mensaje HTTP de respuesta que lo contiene:

```
HTTP/1.1 200 OK
Date: Mon, 18 May 2020 17:00:00 GMT
Server: Apache/2.2.9 (Debian)
Last-Modified: Thu, 21 Dec 2017 17:06:47 GMT
ETag: "411d-67-560dcb9a197c0"
Content-Length: 103
Cache-Control: private, max-age=300, must-revalidate
Via: 1.0 r1:8080
Content-Type: text/html
```

Indica cuál de las siguientes afirmaciones es correcta:

- a. El navegador puede almacenar ese recurso durante 300 segundos, pero es obligatorio realizar revalidación antes de mostrar ese recurso desde la caché incluso durante ese período.
- b. Ninguna de las otras respuestas es correcta.
- c. El navegador no puede almacenar ese recurso.
- d. El navegador puede almacenar ese recurso durante 300 segundos y mostrar ese recurso desde la caché durante este tiempo sin necesidad de revalidarlo.

Pregunta **5**

Sin responder aún

Puntúa como 1,00

La captura de tráfico muestra parte de una comunicación HTTP. Se sabe que antes de realizar dicha captura, el cliente no tenía almacenada ninguna cookie. El mismo cliente solicita la siguiente petición el día de **hoy**:

```
GET /bio/fruta/temporada/kiwi.jpg HTTP/1.1
Host: www1
```

Indica cuál de las siguientes afirmaciones es correcta con respecto a todas las cookies que enviará el cliente con dicha petición:

- a. `country=spain; tokenid=45678; frame=clear;.`
- b. `country=spain`.
- c. El resto de afirmaciones son incorrectas.
- d. `country=spain; tokenid=45678`.

Pregunta **6**

Sin responder aún

Puntúa como 1,00

Carga en `wireshark` esta captura y ordena los paquetes por la columna de tiempo.

NOTA 1: Ten en cuenta que `wireshark` a veces se equivoca al marcar todos los ACK duplicados, o al marcar si una retransmisión es rápida o no.

NOTA 2: Al calcular un valor de umbral redondea hacia abajo

IMPORTANTE: En Wireshark asegúrate de tener desactivado el protocolo DCERPC en *Analyze -> Enabled Protocols*.

Justo después de enviar el paquete 22, y antes de recibir ningún otro segmento del receptor, indica cuál de las siguientes afirmaciones es correcta:

- a. El emisor está en modo *Fast Recovery* y NO puede enviar ningún segmento de datos adicional.
- b. El emisor está en modo *Fast Recovery* y puede enviar 1 segmento de datos adicional (de tamaño MSS).
- c. El emisor está en modo *Congestion Avoidance* y NO puede enviar ningún segmento de datos adicional.
- d. El emisor está en modo *Congestion Avoidance* y puede enviar 1 segmento de datos adicional (de tamaño MSS).

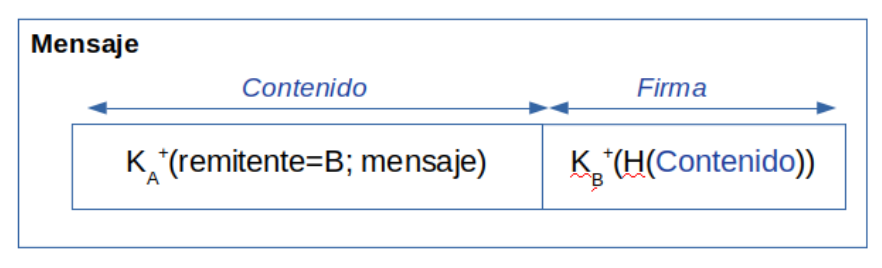
Pregunta **7**

Sin responder aún

Puntúa como 1,00

Un conjunto de amigos $A, B, C, D, E$ utilizan criptografía de clave pública/privada para intercambiar mensajes. Cada uno de los amigos ha conseguido de forma segura las claves públicas del resto de los amigos. Entre ellos se han puesto de acuerdo para utilizar la función *hash* H.

Uno de los amigos, $A$, recibe el siguiente mensaje:




Indica cuál de las siguientes afirmaciones es correcta:

- a. El contenido del mensaje no es confidencial y $A$ puede estar seguro de que B es el remitente del mensaje.
- b. El contenido del mensaje es confidencial y $A$ puede estar seguro de que B es el remitente del mensaje.
- c. El contenido del mensaje no es confidencial y $A$ no puede estar seguro de que B es el remitente del mensaje.
- d. El contenido del mensaje es confidencial y $A$ no puede estar seguro de que B es el remitente del mensaje.

Pregunta **8**

Sin responder aún

Puntúa como 1,00

Carga en `wireshark` esta captura y ordena los paquetes por la columna de tiempo.

NOTA: Ten en cuenta que `wireshark` a veces se equivoca al marcar todos los ACK duplicados, o al marcar si una retransmisión es rápida o no.

Fíjate en el paquete 37 e indica cuál de las afirmaciones es correcta:

- a. Antes de recibir el paquete 37, la máquina 100.0.5.100 se encontraba en Congestion Avoidance y continúa en ese mismo modo de control de congestión una vez recibido.
- b. Antes de recibir el paquete 37, la máquina 100.0.5.100 se encontraba en Slow Start y continúa en ese mismo modo de control de congestión una vez recibido.
- c. Antes de recibir el paquete 37, la máquina 100.0.5.100 se encontraba en Fast Recovery y continúa en ese mismo modo de control de congestión una vez recibido.
- d. Antes de recibir el paquete 37, la máquina 100.0.5.100 se encontraba en Fast Recovery, después de recibirlo pasa a Congestion Avoidance.

Pregunta **9**

Sin responder aún

Puntúa como 1,00

Un emisor está enviando datos a través de una conexión TCP. Se sabe que el MSS de la conexión es de 1000 bytes.

En un instante dado, el último ack recibido por el emisor tiene el número de ACK=3001, y el emisor transmite los segmentos con número de secuencia: 3001, 4001, 5001, 6001, 7001, 8001, 9001, 10001.

Poco después recibe 5 segmentos con los siguientes valores:

```
Acknowledgement number: 4001
Advertised Window: 10000
Options: No
```

```
Acknowledgement number: 5001
Advertised Window: 10000
Options: No
```

```
Acknowledgement number: 5001
Advertised Window: 10000
Options:
SACK: 6001-7001
```

```
Acknowledgement number: 5001
Advertised Window: 10000
Options:
SACK: 6001-7001
SACK: 8001-9001
```

```
Acknowledgement number: 5001
Advertised Window: 10000
Options:
SACK: 6001-7001
SACK: 8001-10001
```

Justo después de recibir estos paquetes, y teniendo en cuenta que el plazo de retransmisión de los paquetes en vuelo aún no se ha cumplido, indica cuál de los siguientes paquetes puede transmitirse:

- a. Únicamente el paquete con número de secuencia 5001.
- b. Los paquetes con números de secuencia 5001 y 7001.
- c. Los paquetes con números de secuencia 5001, 7001 y 10001.
- d. No se puede retransmitir ningún paquete, sólo se pueden enviar segmentos con datos nuevos.

Pregunta **10**

Sin responder aún

Puntúa como 1,00

Carga en `wireshark` esta captura y ordena los paquetes por la columna de tiempo.

NOTA 1: Ten en cuenta que `wireshark` a veces se equivoca al marcar todos los ACK duplicados, o al marcar si una retransmisión es rápida o no.

NOTA 2: Al calcular un valor de umbral redondea hacia abajo

IMPORTANTE: En Wireshark asegúrate de tener desactivado el protocolo DCERPC en *Analyze* `->` *Enabled Protocols*.

Justo después de enviar el paquete 124, y antes de recibir ningún otro segmento del servidor, indica cuántos segmentos de tamaño MSS con datos nuevos podría enviar el cliente:

- a. Podría enviar 5.
- b. Sólo podría enviar 1.
- c. Podría enviar 2 como máximo.
- d. Ninguno.

Pregunta **11**

Sin responder aún

Puntúa como 1,00

Carga en `wireshark` esta captura y ordena los paquetes por la columna de tiempo.

Supón que la implementación de TCP del emisor actualiza el valor de `cwnd` tras la recepción de cada ACK.

Justo después de enviar el paquete 28, y antes de enviar/recibir ningún otro segmento, indica cuál es el **valor de la ventana EFECTIVA** (en número de segmentos de tamaño MSS):

- a. 14.
- b. 2.
- c. 5.
- d. 7.

Pregunta **12**

Sin responder aún

Puntúa como 1,00

Una aplicación HTTP envía el siguiente mensaje:

```
GET /index.html HTTP/1.1
If-None-Match: "zx234598uty""
Host: pc3.emp3.com
Via: 1.0 r3:8080
```

Indica cuál de las siguientes afirmaciones es correcta:

- a. La aplicación es un proxy HTTP que está solicitando por primera vez el recurso `index.html` al servidor.
- b. La aplicación es un proxy HTTP y no se puede saber si está solicitando por primera vez el recurso `index.html` o lo está revalidando.
- c. La aplicación es un cliente HTTP y no se puede saber si está solicitando por primera vez el recurso `index.html` o lo está revalidando.
- d. La aplicación es un proxy HTTP que está revalidando el recurso `index.html` almacenado en su caché.

# GRADO EN INGENIERIA EN SISTEMAS DE TELECOMUNICACION (FUENLABRADA)

## 2040 - SISTEMAS TELEMATICOS - MAÑANA A - 2Q



Pregunta **1**

Sin responder aún

Puntúa como 1,00

Un servidor HTTP envía el siguiente formulario en un mensaje HTTP:

```
<FORM action="http://pc3.emp3.net/p3.pl" method=POST>
<P>
Asignatura: <INPUT type="text" name="asignatura"><BR>
Curso: <INPUT type="text" name="curso"><BR>
<INPUT type="submit" value="Enviar"><INPUT type="reset">
</P>
</FORM>
```

Si el usuario rellena las cajas del formulario con los siguientes datos: asignatura="redes de ordenadores" y curso=2, indica cuál será la línea inicial del mensaje del cliente para enviar dichos datos al servidor:

- a. `POST /p3.pl HTTP/1.1`
- b. `POST http://pc3.emp3.net HTTP/1.1`
- c. `POST http://pc3.emp3.net/asignatura=redes+de+ordenadores&curso=2 HTTP/1.1`
- d. `POST /p3.pl/asignatura=redes+de+ordenadores&curso=2 HTTP/1.1`

Quitar mi elección

Pregunta **2**

Sin responder aún

Puntúa como 1,00

Indica cuál de las siguientes afirmaciones es correcta:

- a. Un certificado está firmado digitalmente con la clave privada del dueño del certificado.
- b. Un certificado está firmado digitalmente con la clave pública de una CA.
- c. Un certificado está firmado digitalmente con la clave pública del dueño del certificado.
- d. El resto de las afirmaciones son falsas.

Quitar mi elección

Pregunta **3**

Sin responder aún

Puntúa como 1,00

Un conjunto de amigos $A, B, C, D, E$ utilizan criptografía de clave pública/privada para intercambiar mensajes. Cada uno de los amigos ha conseguido de forma segura las claves públicas del resto. Entre ellos se han puesto de acuerdo para utilizar la función *hash* H.

Cada vez que quiere entrar un amigo Z nuevo en el grupo, tienen que comunicarle de forma segura las claves públicas de todos los miembros del grupo $K_i^+$, donde $i = A, B, C, D, E$, y los miembros del grupo deben obtener de forma segura la clave pública de Z, $K_Z^+$. Para ello, Z quedará personalmente con uno de los miembros del grupo, $i$, y se intercambiarán las claves que necesitan. De esta forma Z ya poseerá las claves públicas de todos los miembros del grupo, $i$ poseerá la clave pública de Z $K_Z^+$, y sólo quedará que $i$ le comunique de forma segura al resto de miembros del grupo esa clave. Se supone que todos los miembros confían en $i$ y en que éste no va a enviarles una $K_Z^+$ falsa.

Indica cuál de los siguentes mensajes enviados por $i$ a otro miembro del grupo $j$ es un mecanismo seguro para que $i$ le pueda pasar a $j$ la clave $K_Z^+$:

a. `mensaje`= $K_i^+(nombre = Z, clave = K_Z^+)$ ; `firma`= $K_j^+(H(mensaje))$

b. `mensaje`= $(nombre = Z, clave = K_Z^+)$ ; `firma`= $K_i^-(H(mensaje))$

c. `mensaje`= $K_i^+(nombre = Z, clave = K_Z^+)$

d. `mensaje`= $K_j^+(nombre = Z, clave = K_Z^+)$

Quitar mi elección

Pregunta **4**

Sin responder aún

Puntúa como 1,00

Un navegador recibe un recurso del cuál sólo se muestra un conjunto de líneas de cabecera del mensaje HTTP de respuesta que lo contiene:

```
HTTP/1.1 200 OK
Date: Mon, 18 May 2020 17:00:00 GMT
Server: Apache/2.2.9 (Debian)
Last-Modified: Thu, 21 Dec 2017 17:06:47 GMT
ETag: "411d-67-560dcb9a197c0"
Content-Length: 103
Cache-Control: private, max-age=300, must-revalidate
Via: 1.0 r1:8080
Content-Type: text/html
```

Indica cuál de las siguientes afirmaciones es correcta:

a. El navegador puede almacenar ese recurso durante 300 segundos, pero es obligatorio realizar revalidación antes de mostrar ese recurso desde la caché incluso durante ese período.

b. Ninguna de las otras respuestas es correcta.

c. El navegador no puede almacenar ese recurso.

d. El navegador puede almacenar ese recurso durante 300 segundos y mostrar ese recurso desde la caché durante este tiempo sin necesidad de revalidarlo.

Quitar mi elección

Pregunta **5**

Sin responder aún

Puntúa como 1,00

La captura de tráfico muestra parte de una comunicación HTTP. Se sabe que antes de realizar dicha captura, el cliente no tenía almacenada ninguna cookie. El mismo cliente solicita la siguiente petición el día de **hoy**:

```
GET /bio/fruta/temporada/kiwi.jpg HTTP/1.1
Host: www1
```

Indica cuál de las siguientes afirmaciones es correcta con respecto a todas las cookies que enviará el cliente con dicha petición:

- a. `country=spain; tokenid=45678; frame=clear;`.
- b. `country=spain`.
- c. El resto de afirmaciones son incorrectas.
- d. `country=spain; tokenid=45678`.

Quitar mi elección

Pregunta **6**

Sin responder aún

Puntúa como 1,00

Carga en `wireshark` esta captura y ordena los paquetes por la columna de tiempo.

NOTA 1: Ten en cuenta que `wireshark` a veces se equivoca al marcar todos los ACK duplicados, o al marcar si una retransmisión es rápida o no.

NOTA 2: Al calcular un valor de umbral redondea hacia abajo

IMPORTANTE: En Wireshark asegúrate de tener desactivado el protocolo DCERPC en *Analyze -> Enabled Protocols*.

Justo después de enviar el paquete 22, y antes de recibir ningún otro segmento del receptor, indica cuál de las siguientes afirmaciones es correcta:

- a. El emisor está en modo *Fast Recovery* y NO puede enviar ningún segmento de datos adicional.
- b. El emisor está en modo *Fast Recovery* y puede enviar 1 segmento de datos adicional (de tamaño MSS).
- c. El emisor está en modo *Congestion Avoidance* y NO puede enviar ningún segmento de datos adicional.
- d. El emisor está en modo *Congestion Avoidance* y puede enviar 1 segmento de datos adicional (de tamaño MSS).

Quitar mi elección

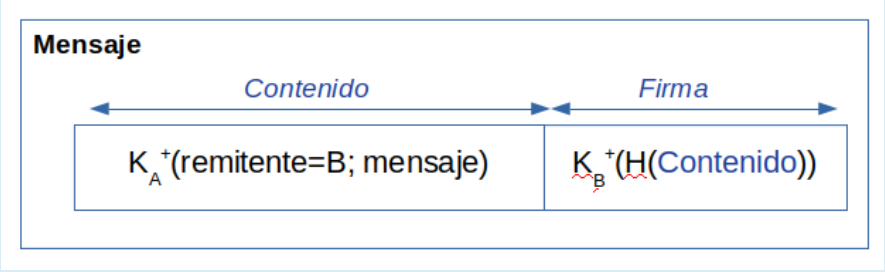
Pregunta **7**

Sin responder aún

Puntúa como 1,00

Un conjunto de amigos $A, B, C, D, E$ utilizan criptografía de clave pública/privada para intercambiar mensajes. Cada uno de los amigos ha conseguido de forma segura las claves públicas del resto de los amigos. Entre ellos se han puesto de acuerdo para utilizar la función *hash* H.

Uno de los amigos, $A$, recibe el siguiente mensaje:




Indica cuál de las siguientes afirmaciones es correcta:

- a. El contenido del mensaje no es confidencial y $A$ puede estar seguro de que B es el remitente del mensaje.
- b. El contenido del mensaje es confidencial y $A$ puede estar seguro de que B es el remitente del mensaje.
- c. El contenido del mensaje no es confidencial y $A$ no puede estar seguro de que B es el remitente del mensaje.
- d. El contenido del mensaje es confidencial y $A$ no puede estar seguro de que B es el remitente del mensaje.

Quitar mi elección

Pregunta **8**

Sin responder aún

Puntúa como 1,00

Carga en `wireshark` esta captura y ordena los paquetes por la columna de tiempo.

NOTA: Ten en cuenta que `wireshark` a veces se equivoca al marcar todos los ACK duplicados, o al marcar si una retransmisión es rápida o no.

Fíjate en el paquete 37 e indica cuál de las afirmaciones es correcta:

a. Antes de recibir el paquete 37, la máquina 100.0.5.100 se encontraba en Congestion Avoidance y continúa en ese mismo modo de control de congestión una vez recibido.

b. Antes de recibir el paquete 37, la máquina 100.0.5.100 se encontraba en Slow Start y continúa en ese mismo modo de control de congestión una vez recibido.

c. Antes de recibir el paquete 37, la máquina 100.0.5.100 se encontraba en Fast Recovery y continúa en ese mismo modo de control de congestión una vez recibido.

d. Antes de recibir el paquete 37, la máquina 100.0.5.100 se encontraba en Fast Recovery, después de recibirlo pasa a Congestion Avoidance.

Quitar mi elección

Pregunta **9**

Sin responder aún

Puntúa como 1,00

Un emisor está enviando datos a través de una conexión TCP. Se sabe que el MSS de la conexión es de 1000 bytes.

En un instante dado, el último ack recibido por el emisor tiene el número de ACK=3001, y el emisor transmite los segmentos con número de secuencia: 3001, 4001, 5001, 6001, 7001, 8001, 9001, 10001.

Poco después recibe 5 segmentos con los siguientes valores:

```
Acknowledgement number: 4001
Advertised Window: 10000
Options: No
```

```
Acknowledgement number: 5001
Advertised Window: 10000
Options: No
```

```
Acknowledgement number: 5001
Advertised Window: 10000
Options:
SACK: 6001-7001
```

```
Acknowledgement number: 5001
Advertised Window: 10000
Options:
SACK: 6001-7001
SACK: 8001-9001
```

```
Acknowledgement number: 5001
Advertised Window: 10000
Options:
SACK: 6001-7001
SACK: 8001-10001
```

Justo después de recibir estos paquetes, y teniendo en cuenta que el plazo de retransmisión de los paquetes en vuelo aún no se ha cumplido, indica cuál de los siguientes paquetes puede transmitirse:

a. Únicamente el paquete con número de secuencia 5001.

b. Los paquetes con números de secuencia 5001 y 7001.

c. Los paquetes con números de secuencia 5001, 7001 y 10001.

d. No se puede retransmitir ningún paquete, sólo se pueden enviar segmentos con datos nuevos.

Quitar mi elección

Pregunta **10**

Sin responder aún

Puntúa como 1,00

Carga en `wireshark` esta captura y ordena los paquetes por la columna de tiempo.

NOTA 1: Ten en cuenta que `wireshark` a veces se equivoca al marcar todos los ACK duplicados, o al marcar si una retransmisión es rápida o no.

NOTA 2: Al calcular un valor de umbral redondea hacia abajo

IMPORTANTE: En Wireshark asegúrate de tener desactivado el protocolo DCERPC en *Analyze* -> *Enabled Protocols*.

Justo después de enviar el paquete 124, y antes de recibir ningún otro segmento del servidor, indica cuántos segmentos de tamaño MSS con datos nuevos podría enviar el cliente:

- a. Podría enviar 5.
- b. Sólo podría enviar 1.
- c. Podría enviar 2 como máximo.
- d. Ninguno.

Quitar mi elección

Pregunta **11**

Sin responder aún

Puntúa como 1,00

Carga en `wireshark` esta captura y ordena los paquetes por la columna de tiempo.

Supón que la implementación de TCP del emisor actualiza el valor de `cwnd` tras la recepción de cada ACK.

Justo después de enviar el paquete 28, y antes de enviar/recibir ningún otro segmento, indica cuál es el **valor de la ventana EFECTIVA** (en número de segmentos de tamaño MSS):

- a. 14.
- b. 2.
- c. 5.
- d. 7.

Quitar mi elección

Pregunta **12**

Sin responder aún

Puntúa como 1,00

Una aplicación HTTP envía el siguiente mensaje:

```
GET /index.html HTTP/1.1
If-None-Match: "zx234598uty""
Host: pc3.emp3.com
Via: 1.0 r3:8080
```

Indica cuál de las siguientes afirmaciones es correcta:

- a. La aplicación es un proxy HTTP que está solicitando por primera vez el recurso `index.html` al servidor.
- b. La aplicación es un proxy HTTP y no se puede saber si está solicitando por primera vez el recurso `index.html` o lo está revalidando.
- c. La aplicación es un cliente HTTP y no se puede saber si está solicitando por primera vez el recurso `index.html` o lo está revalidando.
- d. La aplicación es un proxy HTTP que está revalidando el recurso `index.html` almacenado en su caché.

# Sistemas Telemáticos - Marzo-2023 - Parcial1

Tiempo restante 1:29:31

**Pregunta 1**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS: `/opt/st/disp`

Partiendo de la configuración inicial del escenario, **arranca exclusivamente los *switches* `s2`, `s3` y `s5`**. Indica qué configuración adicional es necesaria para que `pc2` y `pc7` puedan intercambiar datagramas IP:

a. Basta con realizar los siguientes cambios:
- Activar *Proxy ARP* en `r1-eth0` y en `r1-eth2`
- Ejecutar en `r1`: `route add -net 12.0.0.0 netmask 255.255.255.0 dev eth2`

b. Basta con realizar los siguientes cambios:
- Activar *Proxy ARP* en `r1-eth0` y en `r1-eth2`

c. Basta con realizar los siguientes cambios:
- Activar *Proxy ARP* en `r1-eth0` y en `r1-eth2`
- Ejecutar en `r1`: `route add -host 12.0.0.107 dev eth2`
- Ejecutar en `r1`: `route add -host 12.0.0.102 dev eth0`

d. Basta con realizar los siguientes cambios:
- Activar *Proxy ARP* en `r1-eth0` y en `r1-eth2`
- Ejecutar en `r1`: `route add -net 12.0.0.0 netmask 255.255.255.0 dev eth0`

**Pregunta 2**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS: `/opt/st/disp`

Partiendo de la configuración inicial del escenario, **arranca exclusivamente los *switches* `s1`, `s3`, `s4` y `s5`,Y SE DESACTIVA STP EN ELLOS**. Pasado al menos 1 minuto, y suponiendo vacías todas las cachés de ARP de las máquinas y todas las tablas de direcciones aprendidas de los *switches*, en `pc1` se ejecuta la siguiente orden:

```
pc1:~# ping -c 1 13.0.0.103
```

Cuando termine por completo la ejecución de dicha orden, indica qué interfaces de *switches* habrán aprendido la dirección Ethernet de `pc3`:

a. Sólo `s4-eth0`, `s5-eth2`.

b. Sólo `s4-eth0`, `s3-eth2`.

c. Sólo `s4-eth0`, `s5-eth2`, `s3-eth2`.

d. Sólo `s4-eth0`.

**Pregunta 3**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS: `/opt/st/disp`

Los switches del escenario tienen configurado STP. Partiendo de la configuración inicial del escenario, **arranca todos los pcs, switches y r1 en el escenario** y espera al menos 2 minutos hasta que los switches hayan configurado el árbol de expansión. Suponiendo que todas las cachés de ARP están vacías y las tablas de direcciones aprendidas en todos los switches también están vacías, desde la máquina `pc6` se desea ejecutar un ping a `pc1`. Indica cuál de las siguientes afirmaciones es correcta con respecto a la solicitud de ARP que envía `pc6` preguntando por la dirección Ethernet de `pc1`:

a. `pc1` recibe 2 veces esta solicitud de ARP. La primera vez a través de `pc6` -> `s5` -> `s4` -> `s3`-> `pc1`. La segunda vez a través de `pc6`-> `s5` -> `s1` -> `s2` -> `s3` -> `pc1`.

b. `pc1` recibe 1 vez esta solicitud de ARP a través de `pc6`-> `s5` -> `s1` -> `s2` -> `s3` -> `pc1`.

c. `pc1` recibe 1 vez esta solicitud de ARP a través de `pc6` -> `s5` -> `s4` -> `s3`-> `pc1`.

d. `pc1` recibe 3 veces esta solicitud de ARP. La primera vez a través de `pc6` -> `s5` -> `s4` -> `s3`-> `pc1`. La segunda vez a través de `pc6`-> `s5` -> `s1` -> `s2` -> `s3` -> `pc1`. La tercera vez a través de `pc6` -> `s5` -> `r1` -> `s3`-> `pc1`.

Pregunta **4**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de DISPOSITIVOS: `/opt/st/disp`

Los switches del escenario tienen configurado STP. Partiendo de la configuración inicial del escenario, arranca todas las máquinas **exceptuando s3 y pc1**. Espera al menos 2 minutos hasta que los switches hayan configurado el árbol de expansión. Supongamos que se configuran 3 VLANs: VLAN100 para las máquinas de la subred 11.0.0.0/24 (exceptuando `pc1`), VLAN200 para las máquinas de la subred 12.0.0.0/24 y VLAN300 para las máquinas de la subred 13.0.0.0/24. Suponiendo que todas las cachés de ARP están vacías y las tablas de direcciones aprendidas en todos los switches también están vacías, desde la máquina `pc2` se ejecuta un `ping -c 1` hacia `pc3`. Indica cuántos mensajes se capturarán en `pc7` durante la ejecución de dicho ping:

- a. Ninguno.
- b. 1.
- c. 2.
- d. Más de 2.

Pregunta **5**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF `/opt/st/ospf`. Supongamos que se desconoce el orden de arranque de los routers dentro de NetGUI, en un momento determinado se consulta una tabla de vecinos en un router:

```
Neighbor ID     Prio       State           Dead Time         Address         Interface
13.8.0.10          1       Full/Backup         7.00s       13.7.0.10       eth1:13.7.0.9
13.21.0.7          1       Full/DR             4.12s        13.6.0.7       eth0:13.6.0.9
```

Dada la información que se observa en dicha tabla, indica cuál será el valor de campo `Link State ID` del *Network LSA* de la red 13.7.0.0/16:

- a. 13.7.0.0
- b. 13.8.0.10
- c. 13.7.0.9
- d. 13.7.0.10

Pregunta **6**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF `/opt/st/ospf` y con todos los routers habiendo arrancado a la vez y habiendo pasado al menos 1 minuto.

Indica cuál de las siguientes afirmaciones es correcta:

- a. Hay 3 *Router LSA* diferentes de `r3`. Todos los routers del Área 0 tienen almacenados estos 3 anuncios *Router LSA*.
- b. Hay sólo 1 *Router LSA* de `r3`. Todos los routers de las áreas 0, 1 y 2 tienen almacenado este anuncio *Router LSA*, con los mismos campos del anuncio (salvo el campo *Age*). Los routers del Área 3 no tienen almacenado este anuncio.
- c. Hay 3 *Router LSA* diferentes de `r3`. El router `r3` es el único router del escenario que tiene almacenados los 3 *Router LSA*.
- d. Hay sólo 1 *Router LSA* de `r3`. Todos los routers del escenario tienen almacenado este anuncio *Router LSA*, con los mismos campos del anuncio (salvo el campo *Age*).

Pregunta **7**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF `/opt/st/ospf` y con todos los routers habiendo arrancado a la vez y habiendo pasado al menos 1 minuto.

Después, uno de los routers de la red se ha apagado, y ha estado 1 minuto apagado. Posteriormente, ese router apagado ha vuelto a arrancar, y mientras tanto se ha realizado la siguiente captura de tráfico. Señala cuál de los siguientes routers es que estaba apagado y arrancó mientras se efectuaba la captura:

- a. r5.
- b. r10.
- c. r6.
- d. r8.

**Pregunta 8**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF `/opt/st/ospf` y con todos los routers habiendo arrancado a la vez y habiendo pasado al menos 1 minuto.

Indica cuál es valor de campo `Metric` del *Summary LSA* de la red 13.8.0.0/16 en la base de datos de LSAs de `r6`:

- a. 50
- b. 30
- c. 60
- d. 40

**Pregunta 9**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP: `/opt/st/bgp`

Fíjate en las rutas para las subredes 17.0.0.0/15 que hay en la tabla BGP de `as30-r1`.

Indica cuál de las siguientes afirmaciones es correcta:

- a. Hay un error en la configuración de `as10-r1` que provoca que en la tabla BGP de `as30-r1` haya una ruta equivocada a las subredes 17.0.0.0/15.
- b. Hay un error en la configuración de `as60-r1` que provoca que en la tabla BGP de `as30-r1` haya una ruta equivocada a las subredes 17.0.0.0/15.
- c. Hay un error en la configuración de `as50-r1` que provoca que en la tabla BGP de `as30-r1` falte una ruta a las subredes 17.0.0.0/15 con NEXT_HOP=100.4.0.50.
- d. Hay un error en la configuración de `as20-r1` que provoca que en la tabla BGP de `as30-r1` haya una ruta equivocada a las subredes 17.0.0.0/15.

**Pregunta 10**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP: `/opt/st/bgp`

Partiendo de la configuración inicial, con todos los routers arrancados y habiendo dejado pasar un par de minutos para que intercambien las rutas, estudia la configuración BGP de `as20-r1`.

Si se cambia el valor de LOCAL_PREF con AS70 a 180 en la configuración de `as20-r1`, indica qué crees que ocurriría en la tabla de encaminamiento de `as20-r1` con las entradas a las subredes 17.0.0.0/15 y 18.0.0.0/15:

- a. `as20-r1` modificaría su tabla de encaminamiento para las subredes 18.0.0.0/15 pero no para las subredes 17.0.0.0/15.
- b. `as20-r1` modificaría su tabla de encaminamiento para las subredes 17.0.0.0/15 pero no para las subredes 18.0.0.0/15.
- c. `as20-r1` no modificaría su tabla de encaminamiento ni para las subredes 17.0.0.0/15, ni para las subredes 18.0.0.0/15.
- d. `as20-r1` modificaría su tabla de encaminamiento para las subredes 17.0.0.0/15 y 18.0.0.0/15.

**Pregunta 11**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP: `/opt/st/bgp`

Partiendo de la configuración inicial, con todos los routers arrancados y habiendo dejado pasar un par de minutos para que intercambien las rutas, supón que se interrumpe el enlace entre AS50 y AS90. Indica cuál de las siguientes afirmaciones sería correcta:

- a. Ninguna de las otras opciones sería correcta.
- b. `as50-r1` enviaría sólo a su vecino `as60-r1` un mensaje UPDATE de eliminación de rutas de las subredes 17.0.0.0/15, 18.0.0.0/15, 19.0.0.0/15.
- c. `as50-r1` enviaría sólo a su vecino `as30-r1` un mensaje UPDATE de eliminación de rutas de las subredes 17.0.0.0/15, 18.0.0.0/15, 19.0.0.0/15.
- d. `as50-r1` enviaría sólo a sus dos vecinos `as30-r1` y `as60-r1` un mensaje UPDATE de eliminación de rutas de las subredes 17.0.0.0/15, 18.0.0.0/15, 19.0.0.0/15.

Pregunta **12**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP: `/opt/st/bgp`

Partiendo de la configuración inicial, con todos los routers arrancados y habiendo dejado pasar un par de minutos para que intercambien las rutas, fíjate en las entradas de las subredes 13.X.Y.Z que hay en la tabla BGP de `as10-r1` e indica cuál de las siguientes afirmaciones es correcta:

a. Falta la configuración de redistribución de rutas de OSPF a través de BGP en el router `as30-r1`.

b. Falta la configuración de redistribución de rutas de BGP a través de OSPF en el router `as30-r1`.

c. Las listas de exportación definidas en `as30-r1` son incorrectas.

d. La configuración de LOCAL_PREF en `as10-r1` es incorrecta.

# Examen Parcial I
# Sistemas Telemáticos

GSyC – Universidad Rey Juan Carlos

Marzo de 2023

**Respuestas:**

| | **A** | **B** | **C** | **D** |
|---|---|---|---|---|
| **1** | | | **X** | |
| **2** | **X** | | | |
| **3** | | **X** | | |
| **4** | | **X** | | |
| **5** | | | **X** | |
| **6** | | | **X** | |
| **7** | | **X** | | |
| **8** | **X** | | | |
| **9** | | **X** | | |
| **10** | | | | **X** |
| **11** | | **X** | | |
| **12** | **X** | | | |

# Parcial 1 - Mayo 2023

**Pregunta 1**
Sin responder aún
Puntúa como 1,00

Partiendo de la configuración inicial del escenario de DISPOSITIVOS, supongamos que **x4 ha dejado de funcionar**. Se desea que `pc1` y `pc5` puedan intercambiar tráfico. Indica cuál de las siguientes configuraciones permitiría dicha comunicación:

a. Únicamente añadir una ruta en `pc1` para alcanzar `pc5` a través de 12.0.0.1 como siguiente salto.
b. Configurar la dirección IP 11.0.0.3 en `r2(eth0)` usando IP aliasing y añadir una ruta de máquina en `pc1` para llegar a `pc5` a través de 11.0.0.3.
c. Únicamente configurar la dirección IP 11.0.0.3 en `r2(eth0)` usando IP aliasing.
d. Únicamente configurar la dirección IP 11.0.0.3 en `r1(eth1)` usando IP aliasing.

**Pregunta 2**
Sin responder aún
Puntúa como 1,00

Partiendo de la configuración inicial del escenario de DISPOSITIVOS, en `pc2` se ejecuta la siguiente orden:

```
pc2:~# ping -c 1 13.0.0.106
```

Cuando termine por completo la ejecución de dicha orden, indica qué interfaces de *switches* habrán aprendido la dirección Ethernet de `r2(eth0)`:

a. Sólo `x4-eth1` y `x2-eth1`.
b. Sólo `x4-eth1`.
c. Sólo `x3-eth1`, `x4-eth1` y `x2-eth1`.
d. Sólo `x3-eth1`, `x4-eth1`, `x2-eth1` y `x1-eth1`.

**Pregunta 3**
Sin responder aún
Puntúa como 1,00

Supongamos que en el escenario de DISPOSITIVOS se conecta un nuevo switch *x5* con 2 interfaces: x5(eth0) se conecta al hub2 y x5(eth1) se conecta al hub1. Supongamos, además, que se activa STP en los switches, configurando las siguientes prioridades:

- x1 con prioridad 0x0001
- x2 con prioridad 0x0002
- x3 con prioridad 0x0003
- x4 con prioridad 0x0004
- x5 con prioridad 0x0005.

Después de que se haya calculado el árbol de STP, la máquina `pc2` envía una solicitud de ARP dirigida al broadcast Ethernet solicitando la dirección Ethernet de `pc5`, indica cómo llega esa solicitud de ARP al **hub2**:

a. Esa solicitud no alcanzará el hub2.
b. Únicamente la reenviaría el switch `x3` a través de su interfaz `eth0`.
c. Únicamente la ha reenviado el switch `x5` a través de su interfaz `eth0`.
d. La han reenviado tanto el switch `x3` a través de su interfaz `eth0` como el switch `x5` a través de su interfaz `eth0`.

**Pregunta 4**

Sin responder aún

Puntúa como 1,00

En un switch que no está en la figura de DISPOSITIVOS al que llamaremos **s10**, ejecutamos el siguiente comando para obtener información de su configuración:

```
s10:~# brctl show
bridge name bridge id       STP enabled interfaces
vs200       8000.0007e904aa00   no      eth0
                                        eth1.200
                                        eth2.200
vs300       8000.0007e904aa01   no      eth1.300
                                        eth2.300
                                        eth3
```

Indica en cuál de sus interfaces se ha podido obtener la siguiente captura de tráfico:

a. Únicamente en `eth0` y `eth3`.

b. En ninguna de sus interfaces.

c. Únicamente en `eth1` y `eth2`.

d. En cualquiera de sus interfaces.

**Pregunta 5**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF `/opt/st/ospf`. Supongamos que se desconoce el orden de arranque de los routers dentro de NetGUI, y en un momento determinado se consulta la tabla de vecinos en un router:

```
Neighbor ID     Prio       State           Dead Time   Address         Interface
13.19.0.3          1       Full/DR         35.143s     13.12.0.3       eth0:13.12.0.2
13.14.0.1          1       Full/Backup     33.096s     13.10.0.1       eth1:13.10.0.2
```

Dada la información que se observa en dicha tabla, indica cuál será el valor de campo `Advertising Router` del *Network LSA* de la red 13.10.0.0/16:

a. 13.14.0.1

b. 13.12.0.2

c. 13.10.0.2

d. 13.10.0.1

**Pregunta 6**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF `/opt/st/ospf`, con todos los routers habiendo arrancado a la vez y habiendo pasado al menos 1 minuto.

Indica cuál de las siguientes afirmaciones es correcta:

a. El resto de afirmaciones son falsas.

b. En las bases de datos de `r3` aparece 1 *Router LSA* de `r7` en el que se indica que `r7` está conectado a 2 redes *transit*.

c. En las bases de datos de `r3` aparece 1 *Router LSA* de `r7` en el que se indica que `r7` está conectado a 4 redes *transit* y 1 red *stub*.

d. En las bases de datos de `r3` aparecen 2 *Router LSA* de `r7`, en uno se indica que `r7` está conectado a 2 redes *transit*, y en otro se indica que `r7` está conectado a 2 redes *transit* y una red *stub*.

**Pregunta 7**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF `/opt/st/ospf` y con todos los routers habiendo arrancado a la vez y habiendo pasado al menos 1 minuto.

Después, uno de los routers de la red se ha apagado, y ha estado 1 minuto apagado. Posteriormente, ese router apagado ha vuelto a arrancar, y mientras tanto se ha realizado la siguiente captura de tráfico. Señala cuál de los siguientes routers es que estaba apagado y arrancó mientras se efectuaba la captura:

a. r3.

b. r2.

c. r1.

d. r4.

**Pregunta 8**

Sin responder aún

Puntúa como 1,00

En el escenario `/opt/st/ospf` de NetGUI, en un momento determinado se observa el siguiente LSA en las bases de datos de un router:

```
LS age: 116
Options: 0x2  : *|-|-|-|-|-|E|*
LS Flags: 0x6
LS Type: summary-LSA
Link State ID: 13.5.0.0 (summary Network Number)
Advertising Router: 13.21.0.7
LS Seq Number: 80000003
Checksum: 0x669b
Length: 28
Network Mask: /16
        TOS: 0  Metric: 30
```

Indica cuál de las siguientes afirmaciones es correcta:

- a. Este LSA aparecerá en las bases de datos de los routers del área 1, con todos los routers encendidos.
- b. Este LSA aparecerá en las bases de datos de los routers del área 1, y muestra que `r8` está apagado.
- c. Este LSA aparecerá en las bases de datos de los routers del área 0, con todos los routers encendidos.
- d. Este LSA aparecerá en las bases de datos de los routers del área 0, y muestra que `r8` está apagado.

**Pregunta 9**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP: `/opt/st/bgp`

Partiendo de la configuración inicial, con todos los routers arrancados y habiendo dejado pasar un par de minutos para que intercambien las rutas, fíjate en las rutas para las subredes 14.0.0.0/15 que hay en la tabla BGP de `as10-r1`.

Indica cuál de las siguientes afirmaciones es correcta:

- a. Hay un error en la configuración de `as10-r1` que provoca que en la tabla BGP de `as10-r1` haya una ruta equivocada a las subredes 14.0.0.0/15.
- b. Las rutas para las subredes 14.0.0.0/15 en la tabla BGP de `as10-r1` son correctas.
- c. Hay un error en la configuración de `as20-r1` que provoca que en la tabla BGP de `as10-r1` haya una ruta equivocada a las subredes 14.0.0.0/15.
- d. Hay un error en la configuración de `as40-r1` que provoca que en la tabla BGP de `as10-r1` haya una ruta equivocada a las subredes 14.0.0.0/15.

**Pregunta 10**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP: `/opt/st/bgp`

Partiendo de la configuración inicial, con todos los routers arrancados y habiendo dejado pasar un par de minutos para que intercambien las rutas, estudia la configuración BGP de `as90-r1`.

Los valores de LOCAL_PREF configurados provocan que:

- a. `as90-r1` ha elegido erróneamente la ruta preferida sólo al destino 15.0.0.0/15.
- b. `as90-r1` ha elegido erróneamente la ruta preferida sólo a los destinos 15.0.0.0/15, 16.0.0.0/15 y 17.0.0.0/15.
- c. `as90-r1` ha elegido erróneamente la ruta preferida sólo a los destinos 15.0.0.0/15 y 16.0.0.0/15.
- d. `as90-r1` ha elegido erróneamente la ruta preferida sólo al destino 16.0.0.0/15.

**Pregunta 11**

Sin responder aún

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP: `/opt/st/bgp`

Partiendo de la configuración inicial, con todos los routers arrancados y habiendo dejado pasar un par de minutos para que intercambien las rutas, supón que se interrumpe el enlace entre AS50 y AS60. Indica cuál de las siguientes afirmaciones sería correcta:

- a. `as60-r1` enviaría sólo a su vecino `as30-r1` un mensaje UPDATE de eliminación de rutas de las subredes 15.0.0.0/15.
- b. `as60-r1` enviaría a sus dos vecinos `as30-r1` y `as70-r1` un mensaje UPDATE de eliminación de rutas de las subredes 15.0.0.0/15.
- c. `as60-r1` no enviaría ningún mensaje UPDATE de eliminación de rutas de las subredes 15.0.0.0/15.
- d. `as60-r1` enviaría sólo a su vecino `as70-r1` un mensaje UPDATE de eliminación de rutas de las subredes 15.0.0.0/15.

**Pregunta 12**

Sin responder aún

Puntúa como 1,00

En un router BGP `as111-r1` que NO se encuentra en el escenario de BGP, se observa la siguiente configuración en su fichero bgpd.conf:

```
aggregate-address 120.8.0.0/14
aggregate-address 120.12.0.0/14
```

Indica cuál de las siguientes afirmaciones permite la agrupación de las subredes de dicho AS de la forma más eficiente:

a. La agrupación de dichas subredes debería realizarse de la siguiente forma:

```
aggregate-address 120.8.0.0/12
```

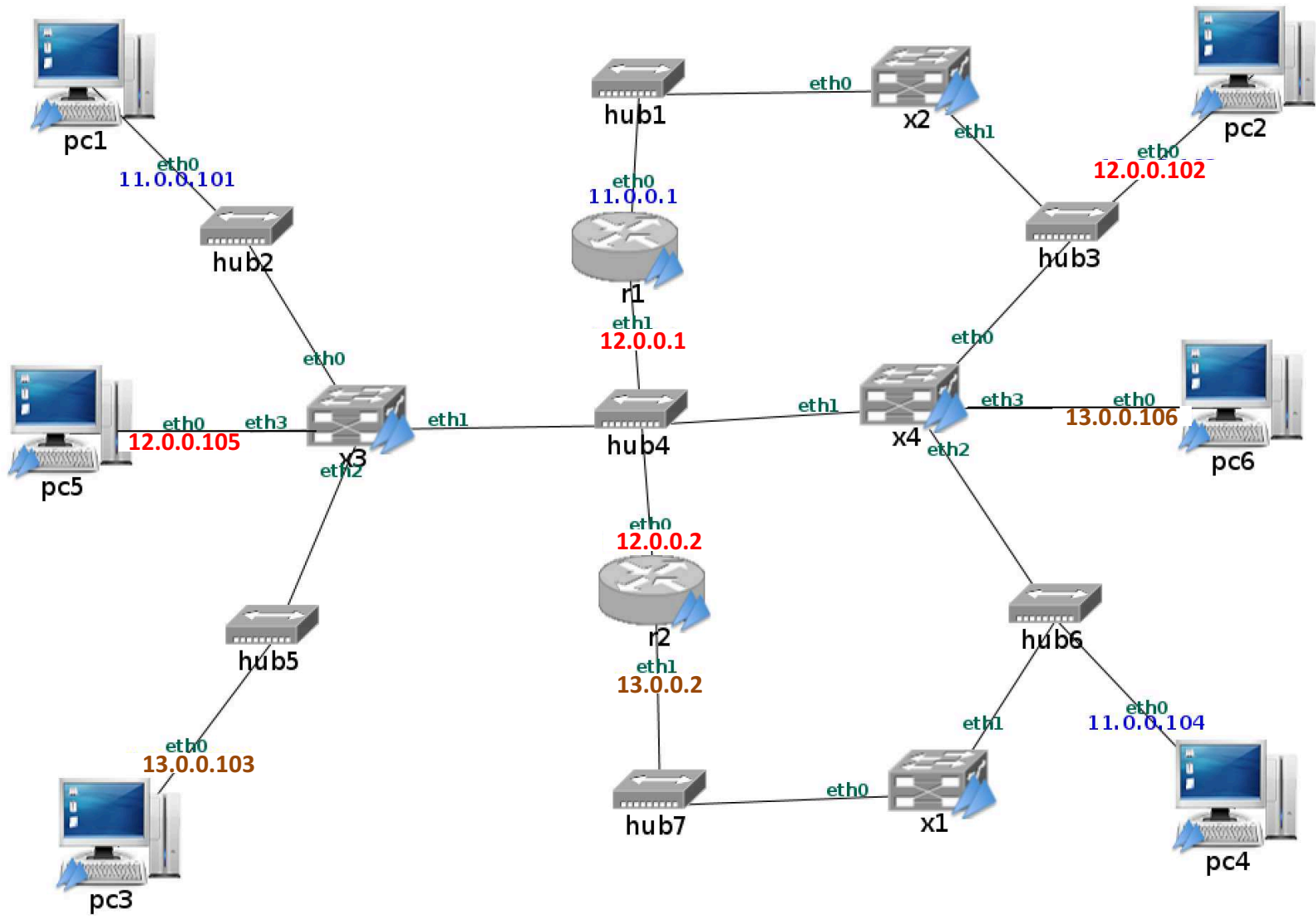
b. La agrupación de dichas subredes debería realizarse de la siguiente forma:

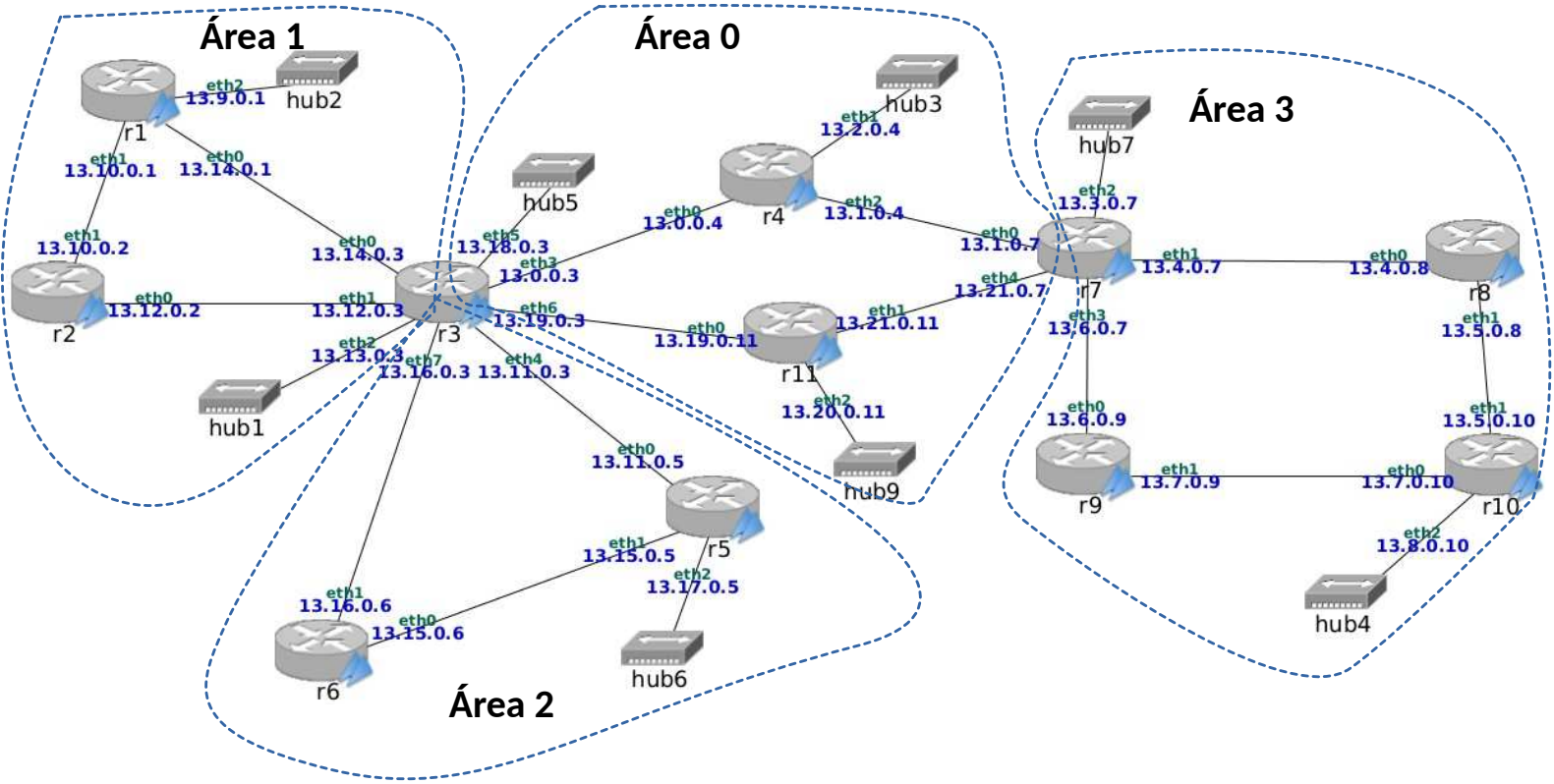
```
aggregate-address 120.8.0.0/13
```

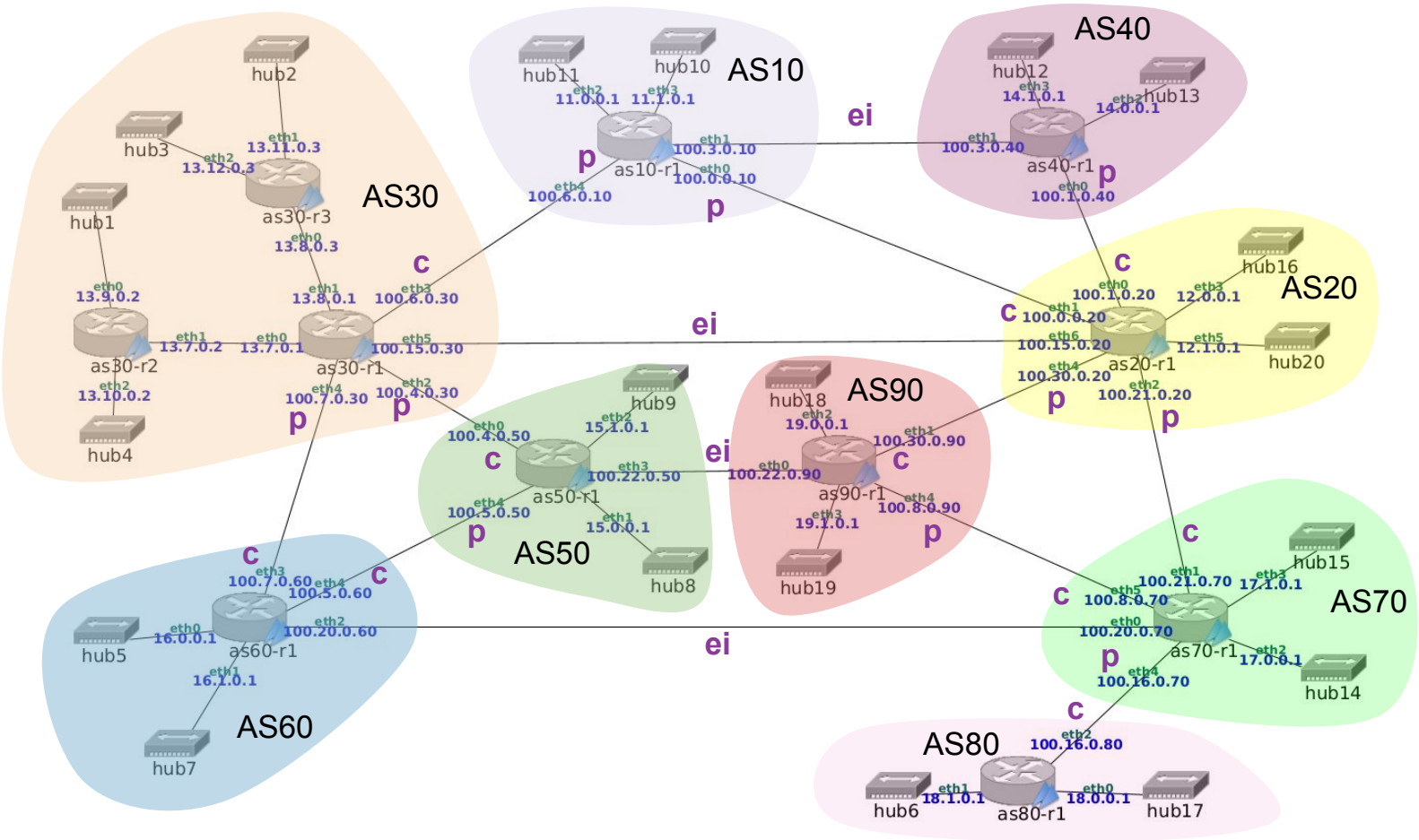
c. La agrupación de dichas subredes debería realizarse de la siguiente forma:

```
aggregate-address 120.0.0.0/12
```

d. La agrupación es correcta, no hay ninguna otra forma de agrupar esas subredes de forma más eficiente.


pc1
eth0
11.0.0.101
hub2
eth0
hub1
eth0
x2
eth1
pc2
eth0
12.0.0.102
hub3
eth0
11.0.0.1
r1
eth1
12.0.0.1
eth0
x3
eth1
hub4
eth1
x4
eth3
eth0
13.0.0.106
pc6
pc5
eth0
12.0.0.105
eth3
eth2
eth2
eth0
12.0.0.2
r2
hub5
hub6
eth1
13.0.0.2
eth1
eth0
11.0.0.104
eth0
13.0.0.103
hub7
eth0
x1
pc4
pc3


Área 1
Área 0
Área 3
Área 2
r1
r2
r3
r4
r5
r6
r7
r8
r9
r10
r11
hub1
hub2
hub3
hub4
hub5
hub6
hub7
hub9
eth2 13.9.0.1
eth1 13.10.0.1
eth0 13.14.0.1
eth1 13.10.0.2
eth0 13.12.0.2
eth0 13.14.0.3
eth1 13.12.0.3
eth2 13.13.0.3
eth7 13.16.0.3
eth4 13.11.0.3
eth5 13.18.0.3
eth3 13.0.0.3
eth6 13.19.0.3
eth1 13.2.0.4
eth0 13.0.0.4
eth2 13.1.0.4
eth0 13.1.0.7
eth2 13.3.0.7
eth4 13.21.0.7
eth1 13.21.0.11
eth0 13.19.0.11
eth2 13.20.0.11
eth1 13.4.0.7
eth0 13.4.0.8
eth3 13.6.0.7
eth1 13.5.0.8
eth0 13.6.0.9
eth1 13.7.0.9
eth0 13.7.0.10
eth1 13.5.0.10
eth2 13.8.0.10
eth0 13.11.0.5
eth1 13.15.0.5
eth2 13.17.0.5
eth1 13.16.0.6
eth0 13.15.0.6


AS10
AS20
AS30
AS40
AS50
AS60
AS70
AS80
AS90
hub1
hub2
hub3
hub4
hub5
hub6
hub7
hub8
hub9
hub10
hub11
hub12
hub13
hub14
hub15
hub16
hub17
hub18
hub19
hub20
as10-r1
as20-r1
as30-r1
as30-r2
as30-r3
as40-r1
as50-r1
as60-r1
as70-r1
as80-r1
as90-r1
ei
p
c

# GRADO EN INGENIERIA EN SISTEMAS DE TELECOMUNICACION (FUENLABRADA)

## 2040 - SISTEMAS TELEMATICOS - MAÑANA A - 2Q

**Pregunta 1**
Sin contestar
Puntúa como 1,00

Partiendo de la configuración inicial del escenario de DISPOSITIVOS, supongamos que **x4 ha dejado de funcionar**. Se desea que `pc1` y `pc5` puedan intercambiar tráfico. Indica cuál de las siguientes configuraciones permitiría dicha comunicación:

a. Únicamente añadir una ruta en `pc1` para alcanzar `pc5` a través de 12.0.0.1 como siguiente salto.

b. Configurar la dirección IP 11.0.0.3 en `r2(eth0)` usando IP aliasing y añadir una ruta de máquina en `pc1` para llegar a `pc5` a través de 11.0.0.3.

c. Únicamente configurar la dirección IP 11.0.0.3 en `r2(eth0)` usando IP aliasing.

d. Únicamente configurar la dirección IP 11.0.0.3 en `r1(eth1)` usando IP aliasing.

La respuesta correcta es: Configurar la dirección IP 11.0.0.3 en `r2(eth0)` usando IP aliasing y añadir una ruta de máquina en `pc1` para llegar a `pc5` a través de 11.0.0.3.

**Pregunta 2**
Sin contestar
Puntúa como 1,00

Partiendo de la configuración inicial del escenario de DISPOSITIVOS, en `pc2` se ejecuta la siguiente orden:

```
pc2:~# ping -c 1 13.0.0.106
```

Cuando termine por completo la ejecución de dicha orden, indica qué interfaces de *switches* habrán aprendido la dirección Ethernet de `r2(eth0)`:

a. Sólo `x4-eth1` y `x2-eth1`.

b. Sólo `x4-eth1`.

c. Sólo `x3-eth1`, `x4-eth1` y `x2-eth1`.

d. Sólo `x3-eth1`, `x4-eth1`, `x2-eth1` y `x1-eth1`.

La respuesta correcta es: Sólo `x3-eth1`, `x4-eth1` y `x2-eth1`.

**Pregunta 3**
Sin contestar
Puntúa como 1,00

Supongamos que en el escenario de DISPOSITIVOS se conecta un nuevo switch *x5* con 2 interfaces: x5(eth0) se conecta al hub2 y x5(eth1) se conecta al hub1. Supongamos, además, que se activa STP en los switches, configurando las siguientes prioridades:

- x1 con prioridad 0x0001
- x2 con prioridad 0x0002
- x3 con prioridad 0x0003
- x4 con prioridad 0x0004
- x5 con prioridad 0x0005.

Después de que se haya calculado el árbol de STP, la máquina `pc2` envía una solicitud de ARP dirigida al broadcast Ethernet solicitando la dirección Ethernet de `pc5`, indica cómo llega esa solicitud de ARP al **hub2**:

a. Esa solicitud no alcanzará el hub2.

b. Únicamente la reenviaría el switch `x3` a través de su interfaz `eth0`.

c. Únicamente la ha reenviado el switch `x5` a través de su interfaz `eth0`.

d. La han reenviado tanto el switch `x3` a través de su interfaz `eth0` como el switch `x5` a través de su interfaz `eth0`.

La respuesta correcta es: Únicamente la reenviaría el switch `x3` a través de su interfaz `eth0`.

**Pregunta 4**
Sin contestar
Puntúa como 1,00

En un switch que no está en la figura de DISPOSITIVOS al que llamaremos **s10**, ejecutamos el siguiente comando para obtener información de su configuración:

```
s10:~# brctl show
bridge name bridge id       STP enabled interfaces
vs200       8000.0007e904aa00   no      eth0
                                        eth1.200
                                        eth2.200
vs300       8000.0007e904aa01   no      eth1.300
                                        eth2.300
                                        eth3
```

Indica en cuál de sus interfaces se ha podido obtener la siguiente captura de tráfico:

a. Únicamente en `eth0` y `eth3`.

b. En ninguna de sus interfaces.

c. Únicamente en `eth1` y `eth2`.

d. En cualquiera de sus interfaces.

La respuesta correcta es: Únicamente en `eth1` y `eth2`.

**Pregunta 5**

Sin contestar

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF `/opt/st/ospf`. Supongamos que se desconoce el orden de arranque de los routers dentro de NetGUI, y en un momento determinado se consulta la tabla de vecinos en un router:

```
Neighbor ID     Prio       State           Dead Time     Address         Interface
13.19.0.3          1       Full/DR         35.143s       13.12.0.3       eth0:13.12.0.2
13.14.0.1          1       Full/Backup     33.096s       13.10.0.1       eth1:13.10.0.2
```

Dada la información que se observa en dicha tabla, indica cuál será el valor de campo `Advertising Router` del *Network LSA* de la red 13.10.0.0/16:

a. 13.14.0.1

b. 13.12.0.2

c. 13.10.0.2

d. 13.10.0.1

La respuesta correcta es: 13.12.0.2

**Pregunta 6**

Sin contestar

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF `/opt/st/ospf`, con todos los routers habiendo arrancado a la vez y habiendo pasado al menos 1 minuto.

Indica cuál de las siguientes afirmaciones es correcta:

a. El resto de afirmaciones son falsas.

b. En las bases de datos de `r3` aparece 1 *Router LSA* de `r7` en el que se indica que `r7` está conectado a 2 redes *transit*.

c. En las bases de datos de `r3` aparece 1 *Router LSA* de `r7` en el que se indica que `r7` está conectado a 4 redes *transit* y 1 red *stub*.

d. En las bases de datos de `r3` aparecen 2 *Router LSA* de `r7`, en uno se indica que `r7` está conectado a 2 redes *transit*, y en otro se indica que `r7` está conectado a 2 redes *transit* y una red *stub*.

La respuesta correcta es: En las bases de datos de `r3` aparece 1 *Router LSA* de `r7` en el que se indica que `r7` está conectado a 2 redes *transit*.

**Pregunta 7**

Sin contestar

Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de OSPF `/opt/st/ospf` y con todos los routers habiendo arrancado a la vez y habiendo pasado al menos 1 minuto.

Despúes, uno de los routers de la red se ha apagado, y ha estado 1 minuto apagado. Posteriormente, ese router apagado ha vuelto a arrancar, y mientras tanto se ha realizado la siguiente captura de tráfico. Señala cuál de los siguientes routers es que estaba apagado y arrancó mientras se efectuaba la captura:

a. r3.

b. r2.

c. r1.

d. r4.

La respuesta correcta es: r1.

**Pregunta 8**

Sin contestar

Puntúa como 1,00

En el escenario `/opt/st/ospf` de NetGUI, en un momento determinado se observa el siguiente LSA en las bases de datos de un router:

```
LS age: 116
Options: 0x2  : *|-|-|-|-|-|E|*
LS Flags: 0x6
LS Type: summary-LSA
Link State ID: 13.5.0.0 (summary Network Number)
Advertising Router: 13.21.0.7
LS Seq Number: 80000003
Checksum: 0x669b
```

```
Length: 28
Network Mask: /16
        TOS: 0  Metric: 30
```

Indica cuál de las siguientes afirmaciones es correcta:

- a. Este LSA aparecerá en las bases de datos de los routers del área 1, con todos los routers encendidos.
- b. Este LSA aparecerá en las bases de datos de los routers del área 1, y muestra que `r8` está apagado.
- c. Este LSA aparecerá en las bases de datos de los routers del área 0, con todos los routers encendidos.
- d. Este LSA aparecerá en las bases de datos de los routers del área 0, y muestra que `r8` está apagado.

La respuesta correcta es: Este LSA aparecerá en las bases de datos de los routers del área 0, y muestra que `r8` está apagado.

**Pregunta 9**
Sin contestar
Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP: `/opt/st/bgp`

Partiendo de la configuración inicial, con todos los routers arrancados y habiendo dejado pasar un par de minutos para que intercambien las rutas, fíjate en las rutas para las subredes 14.0.0.0/15 que hay en la tabla BGP de `as10-r1`.

Indica cuál de las siguientes afirmaciones es correcta:

- a. Hay un error en la configuración de `as10-r1` que provoca que en la tabla BGP de `as10-r1` haya una ruta equivocada a las subredes 14.0.0.0/15.
- b. Las rutas para las subredes 14.0.0.0/15 en la tabla BGP de `as10-r1` son correctas.
- c. Hay un error en la configuración de `as20-r1` que provoca que en la tabla BGP de `as10-r1` haya una ruta equivocada a las subredes 14.0.0.0/15.
- d. Hay un error en la configuración de `as40-r1` que provoca que en la tabla BGP de `as10-r1` haya una ruta equivocada a las subredes 14.0.0.0/15.

La respuesta correcta es: Hay un error en la configuración de `as20-r1` que provoca que en la tabla BGP de `as10-r1` haya una ruta equivocada a las subredes 14.0.0.0/15.

**Pregunta 10**
Sin contestar
Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP: `/opt/st/bgp`

Partiendo de la configuración inicial, con todos los routers arrancados y habiendo dejado pasar un par de minutos para que intercambien las rutas, estudia la configuración BGP de `as90-r1`.

Los valores de LOCAL_PREF configurados provocan que:

- a. `as90-r1` ha elegido erróneamente la ruta preferida sólo al destino 15.0.0.0/15.
- b. `as90-r1` ha elegido erróneamente la ruta preferida sólo a los destinos 15.0.0.0/15, 16.0.0.0/15 y 17.0.0.0/15.
- c. `as90-r1` ha elegido erróneamente la ruta preferida sólo a los destinos 15.0.0.0/15 y 16.0.0.0/15.
- d. `as90-r1` ha elegido erróneamente la ruta preferida sólo al destino 16.0.0.0/15.

La respuesta correcta es: `as90-r1` ha elegido erróneamente la ruta preferida sólo a los destinos 15.0.0.0/15 y 16.0.0.0/15.

**Pregunta 11**
Sin contestar
Puntúa como 1,00

Asegúrate de tener abierto en NetGUI el escenario de BGP: `/opt/st/bgp`

Partiendo de la configuración inicial, con todos los routers arrancados y habiendo dejado pasar un par de minutos para que intercambien las rutas, supón que se interrumpe el enlace entre AS50 y AS60. Indica cuál de las siguientes afirmaciones sería correcta:

- a. `as60-r1` enviaría sólo a su vecino `as30-r1` un mensaje UPDATE de eliminación de rutas de las subredes 15.0.0.0/15.
- b. `as60-r1` enviaría a sus dos vecinos `as30-r1` y `as70-r1` un mensaje UPDATE de eliminación de rutas de las subredes 15.0.0.0/15.
- c. `as60-r1` no enviaría ningún mensaje UPDATE de eliminación de rutas de las subredes 15.0.0.0/15.
- d. `as60-r1` enviaría sólo a su vecino `as70-r1` un mensaje UPDATE de eliminación de rutas de las subredes 15.0.0.0/15.

La respuesta correcta es: `as60-r1` no enviaría ningún mensaje UPDATE de eliminación de rutas de las subredes 15.0.0.0/15.

**Pregunta 12**
En un router BGP `as111-r1` que NO se encuentra en el escenario de BGP, se observa la siguiente configuración en su fichero

Pregunta 12

Sin contestar

Puntúa como 1,00

En un router BGP `as11-r1` que NO se encuentra en el escenario de BGP, se observa la siguiente configuración en su fichero bgpd.conf:

```
aggregate-address 120.8.0.0/14
aggregate-address 120.12.0.0/14
```

Indica cuál de las siguientes afirmaciones permite la agrupación de las subredes de dicho AS de la forma más eficiente:

a. La agrupación de dichas subredes debería realizarse de la siguiente forma:

```
aggregate-address 120.8.0.0/12
```

b. La agrupación de dichas subredes debería realizarse de la siguiente forma:

```
aggregate-address 120.8.0.0/13
```

c. La agrupación de dichas subredes debería realizarse de la siguiente forma:

```
aggregate-address 120.0.0.0/12
```

d. La agrupación es correcta, no hay ninguna otra forma de agrupar esas subredes de forma más eficiente.

La respuesta correcta es: La agrupación de dichas subredes debería realizarse de la siguiente forma:

```
aggregate-address 120.8.0.0/13
```

# Parcial 2 - Mayo 2023

Pregunta 1
Sin responder aún
Puntúa como 1,00

Carga en `wireshark` esta captura y ordena los paquetes por la columna de tiempo.

NOTA 1: Ten en cuenta que `wireshark` a veces se equivoca al marcar todos los ACK duplicados, o al marcar si una retransmisión es rápida o no.

NOTA 2: Al calcular un valor de umbral redondea hacia abajo.

Justo después de que el cliente envíe el paquete 252, y antes de enviar o recibir ningún otro segmento, indica como máximo cuántos paquetes de tamaño MSS podría enviar el cliente:

- a. 4 paquetes.
- b. No podría enviar ningún paquete.
- c. 8 paquetes.
- d. 2 paquetes.

Pregunta 2
Sin responder aún
Puntúa como 1,00

Carga en `wireshark` esta captura y ordena los paquetes por la columna de tiempo.

NOTA 1: Ten en cuenta que `wireshark` a veces se equivoca al marcar todos los ACK duplicados, o al marcar si una retransmisión es rápida o no.

NOTA 2: Al calcular un valor de umbral redondea hacia abajo.

IMPORTANTE: En Wireshark asegúrate de tener desactivado el protocolo DCERPC en *Analyze -> Enabled Protocols*.

Observa el paquete 158. Indica cuál de las siguientes afirmaciones es correcta:

- a. A partir del paquete 158 el emisor está en modo *Fast Recovery*, modo que termina al recibir el paquete 163.
- b. A partir del paquete 158 el emisor está en modo *Fast Recovery*, modo que termina al recibir el paquete 161.
- c. A partir del paquete 158 el emisor está en modo *Fast Recovery*, modo que termina al recibir el paquete 162.
- d. A partir del paquete 158 el emisor está en modo *Slow Start*, modo que termina al enviar el paquete 160.

Pregunta 3
Sin responder aún
Puntúa como 1,00

Carga en `wireshark` esta captura y ordena los paquetes por la columna de tiempo.

NOTA: Ten en cuenta que `wireshark` a veces se equivoca al marcar todos los ACK duplicados, o al marcar si una retransmisión es rápida o no.

Justo después de que la máquina 11.0.0.11 reciba el paquete 196, y antes de enviar/recibir ningún otro segmento, indica cuál es el **valor de la ventana de congestión** (en número de segmentos de tamaño MSS):

- a. 11 MSS.
- b. 17 MSS.
- c. 6 MSS.
- d. 9 MSS.

**Pregunta 4**

Sin responder aún

Puntúa como 1,00

Carga en `wireshark` esta captura y ordena los paquetes por la columna de tiempo.

Indica cuál de las siguientes afirmaciones es correcta respecto a los estados durante el cierre de la conexión :

- a. El cliente tras enviar el paquete 248 se encuentra en estado `CLOSE_WAIT`.
- b. El cliente tras enviar el paquete 255 se encuentra en estado `FIN_WAIT_2`.
- c. El servidor tras enviar el paquete 253 se encuentra en estado `CLOSE_WAIT`.
- d. El servidor tras enviar el paquete 254 se encuentra en estado `CLOSE_WAIT`.

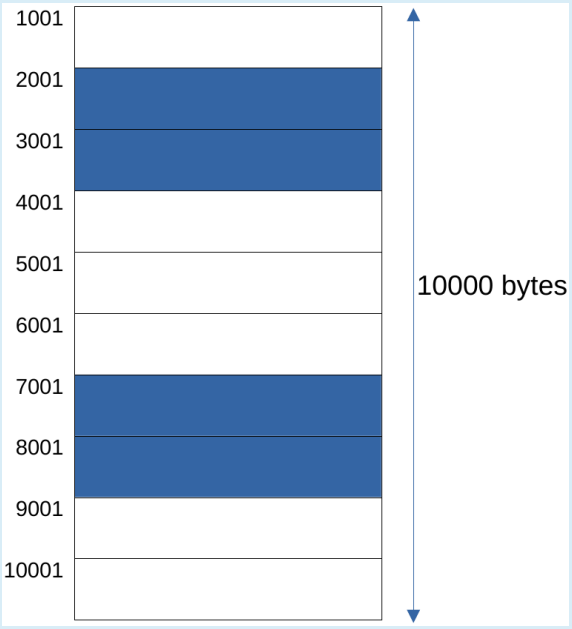
**Pregunta 5**

Sin responder aún

Puntúa como 1,00

En una conexión TCP, se sabe que el MSS de la conexión es de 1000 bytes.

En un instante dado, el receptor tiene su buffer 'in' tal y como se muestra en la siguiente figura, donde cada rectángulo azul se corresponde con un segmento con datos recibidos y el número que se muestra en el lado izquierdo es el número de secuencia de cada segmento:




A continuación el receptor recibe el segmento con número de secuencia 1001. Suponiendo que no pasa ningún byte a la aplicación receptora, indica cuáles son los campos relevantes del ACK que envíe el receptor:

- a.
```
Acknowledgement number: 4001
Advertised Window: 7000
Options:
SACK: 1001-4001
SACK: 7001-9001
```
- b. El resto de respuestas son incorrectas.
- c.
```
Acknowledgement number: 1001
Advertised Window: 10000
Options:
SACK: 1001-4001
SACK: 7001-9001
```
- d.
```
Acknowledgement number: 4001
Advertised Window: 7000
Options:
SACK: 7001-9001
```

**Pregunta 6**

Sin responder aún

Puntúa como 1,00

La captura de tráfico muestra parte de una comunicación HTTP. Indica cuál de los siguientes opciones representa un conjunto de *cookies* válido que podría haber tenido almacenado el cliente que se ejecutaba la máquina 13.0.0.13 **antes de que dicha captura se realizara**:

a.
- `id1=11111 Path=/ Domain=www1`.
- `id2=22222 Path=/ Domain=www1`.
- No se puede saber nada sobre el Path de las cookies `id3` e `id4`.

b.
- `id1=11111 Path=/electronica Domain=www1`.
- `id2=22222 Path=/electronica Domain=www1`.
- `id3=33333 Path=/electronica Domain=www1`.
- `id4=44444 Path=/electronica Domain=www1`.

c.
- `id1=11111 Path=/ Domain=www1`.
- `id2=22222 Path=/ Domain=www1`.
- `id3=33333 Path=/electronica Domain=www1`.
- `id4=44444 Path=/musica Domain=www1`.

d.
- `id1=11111 Path=/electronica Domain=www1`.
- `id2=22222 Path=/electronica Domain=www1`.
- No se puede saber nada sobre el Path de las cookies `id3` e `id4`.

**Pregunta 7**

Sin responder aún

Puntúa como 1,00

Ante la siguiente petición de un cliente:

```
GET http://pc1.emp1.net/index.html HTTP/1.1
Host: pc1.emp1.net
```

Un proxy le envía un mensaje de respuesta del cuál sólo se muestra un conjunto de líneas de cabecera del mensaje HTTP:

```
HTTP/1.1 200 OK
Date: Mon, 18 May 2020 17:00:00 GMT
Server: Apache/2.2.9 (Debian)
Last-Modified: Thu, 21 Dec 2017 17:06:47 GMT
ETag: "411d-67-560dcb9a197c0"
Content-Length: 103
Cache-Control: public, max-age=100
Age: 90
Via: 1.0 r1:8080
Content-type: text/html
```

Indica cuál de las siguientes afirmaciones es correcta:

a. El proxy-caché necesitará revalidar ese recurso siempre que se lo soliciten de nuevo porque debe ofrecer la versión más actualizada de ese recurso.

b. Si el proxy-caché recibiera una petición de ese mismo recurso pasados 20 segundos desde que se generó la respuesta mostrada en el enunciado, el proxy-caché necesariamente debería revalidar ese recurso con el servidor.

c. El proxy-caché no necesitará revalidar nunca ese recurso cuando se lo soliciten de nuevo porque no aparece la opción `must-revalidate`.

d. Si el proxy-caché recibiera una petición de ese mismo recurso pasados 5 segundos desde que se generó la respuesta mostrada en el enunciado, el proxy-caché necesariamente debería revalidar ese recurso con el servidor.

**Pregunta 8**

Sin responder aún

Puntúa como 1,00

Un proxy envía el siguiente mensaje:

```
GET /index.html HTTP/1.1
If-None-Match: "hydf87qw""
Host: pc6.emp6.com
Via: 1.0 r6:8080
```

Y el servidor responde:

```
HTTP/1.1 304 Not Modified
Server: Apache/2.2.9 (Debian)
Date: Mon, 18 May 2020 09:00:00 GMT
Cache-Control: public, max-age=300
ETag: "hydf87qw"
```

Indica cuál de las siguientes afirmaciones es correcta:

- a. El servidor no ha podido enviar esa respuesta.
- b. El proxy no ha podido enviar esa petición.
- c. El servidor ha enviado esa respuesta porque el recurso index.html no ha cambiado en el servidor.
- d. El servidor ha enviado esa respuesta con una nueva versión del recurso index.html que ha cambiado en el servidor.

**Pregunta 9**

Sin responder aún

Puntúa como 1,00

Un conjunto de 5 personas $A, B, C, D, E$ quieren utilizar criptografía de clave pública/privada para intercambiar mensajes de forma segura. Cada persona ha generado una pareja de claves $K_I^+$ y $K_I^-$. Las 5 personas se conocían previamente, pero desde que han generando sus claves no se han visto en persona, por lo que no se han podido intercambiar sus claves públicas de forma segura (aunque pueden acceder a dichas claves públicas, no están seguros de que sean de quien aparentan ser).

Unos días después de que las 5 personas generaron sus claves, A y B coinciden en persona. Indica cuál de las siguientes afirmaciones es **FALSA** respecto a lo que A pueda hacer al coincidir con B en persona:

- a. Si A acepta la clave que le ofrece B como $K_B^+$, A podrá estar seguro de que cualquier mensaje que posteriormente envíe cifrado con esa clave sólo podrá ser leído por B.
- b. Si A le pasa a B $K_A^+$ diciéndole que es la clave pública de C, A podrá beneficiarse maliciosamente de ello en el futuro.
- c. Si A le pasa a B $K_A^-$, A podrá ser gravemente perjudicado en el futuro si B actua maliciosamente.
- d. Si A le pasa a B $K_C^+$ diciéndole que es su clave pública (es decir, diciéndole que es $K_A^+$), A podrá beneficiarse maliciosamente de ello en el futuro.

**Pregunta 10**

Sin responder aún

Puntúa como 1,00

Un conjunto de 6 amigos $A, B, C, D, E$ utilizan criptografía de clave pública/privada para intercambiar mensajes. Cada uno de los amigos ha conseguido de forma segura las claves públicas del resto de los amigos. Entre ellos se han puesto de acuerdo para utilizar la función *hash* H.

Una sexta persona, Trudón, intercepta el siguiente mensaje enviado por A para B:

$$\texttt{mensaje} = K_B^+(m1); K_A^-(H(m1))$$

Indica cuál de las siguientes afirmaciones es correcta:

- a. Trudón NO puede cambiar $m1$ por un nuevo mensaje $m2$ sin que el destinario previsto $B$ lo note.
- b. Trudón puede cambiar el destinatario del mensaje a otro, por ejemplo a $C$ en lugar de $B$, manteniendo $m1$ y dejando el mensaje de forma que $C$ pueda comprobar que el mensaje proviene de $A$.
- c. Trudón puede comprobar que el mensaje proviene de $A$ y no ha sido alterado desde que él lo envió.
- d. Trudón puede conocer el contenido del mensaje $m1$, pero no puede modificarlo sin que el destinario previsto $B$ lo note.

**Pregunta 11**

Sin responder aún

Puntúa como 1,00

En la figura correspodiente a un escenario de seguridad 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, los *routers* `e1-fw` y `e2-fw` han ejecutado un *script* que aplica estas reglas.

---

Se hacen cambios en la configuración de `e2-fw` de forma que se puedan comunicar los siguientes cliente y servidor:

- En `e2-pc1` se ha ejecutado: `nc -l -p 11000`
- En `i-pc1` se ha ejecutado: `nc -p 22000 20.0.2.1 100`

Para que esta comunicación haya sido posible, indica qué cambios respecto a la configuración inicial han sido necesarios en `e2-fw` :

a.
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp --dport 100 -j DNAT --to-destination
10.0.0.10:11000
iptables -t filter -A FORWARD -p tcp --dport 11000 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

b.
```
iptables -t filter -A FORWARD -p tcp -d 10.0.0.10 --dport 100 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

c.
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp --dport 11000 -j DNAT --to-destination
10.0.0.10:11000
iptables -t filter -A FORWARD -p tcp -d 10.0.0.10 --dport 11000 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

d.
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp --dport 100 -j DNAT --to-destination
10.0.0.10
iptables -t filter -A FORWARD -p tcp -d 10.0.0.10 --dport 100 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

**Pregunta 12**

Sin responder aún

Puntúa como 1,00

En la figura correspodiente a un escenario de seguridad 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, los *routers* `e1-fw` y `e2-fw` han ejecutado un *script* que aplica estas reglas.

---

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

- Desde cualquier máquina de Internet se puede acceder a un servidor web (puerto 80 de TCP) lanzado en `e2-pc2`.
- Desde `e2-pc1` o `e2-pc2` NO se puede acceder a ningún servidor TCP o UDP que se lance en cualquier máquina de Internet.
- Desde cualquier máquina de Internet NO se puede acceder a ningún otro servidor TCP o UDP lanzado en `e2-pc1` o `e2-pc2`.

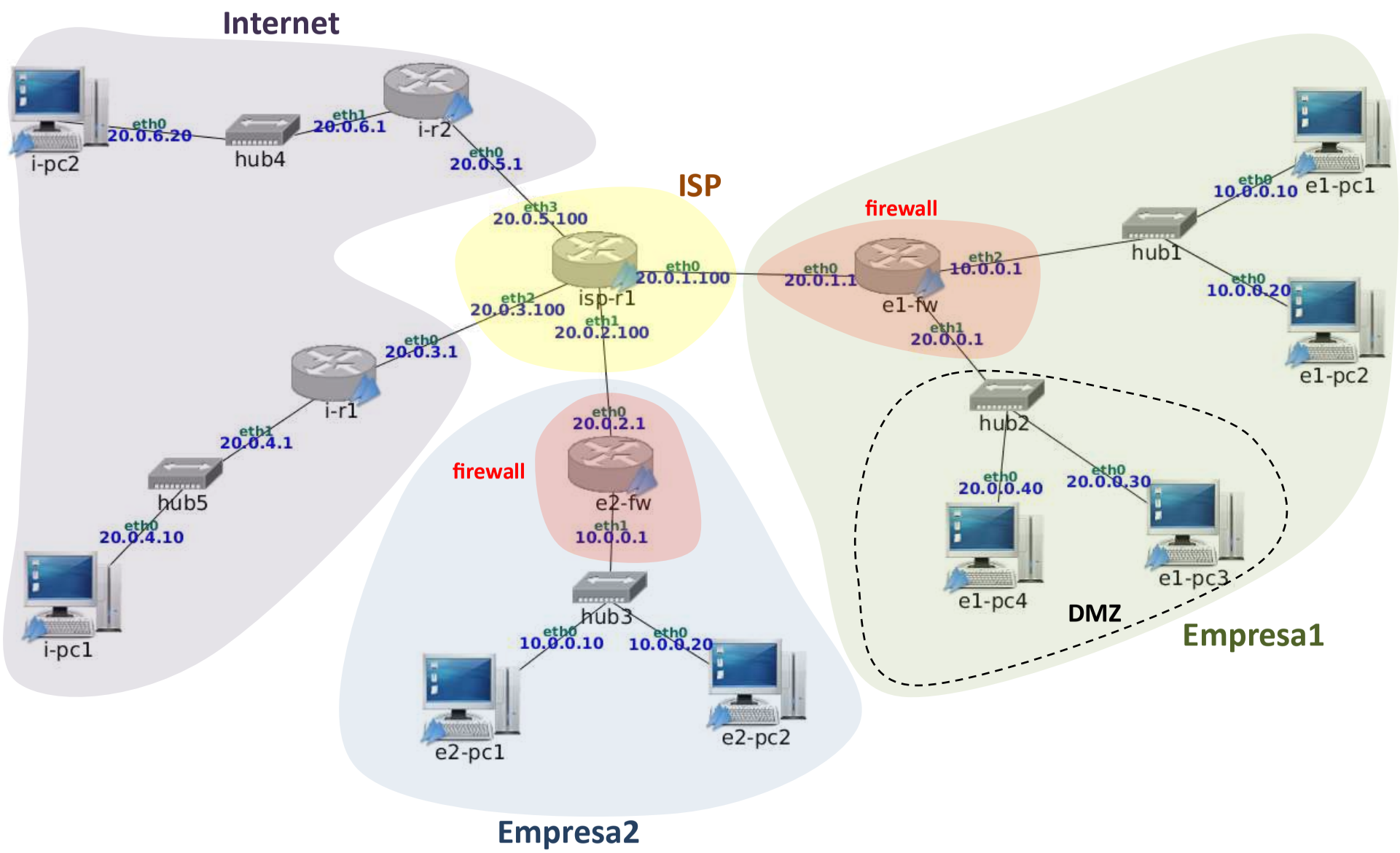
Partiendo de la configuración inicial, indica cuál de los siguientes conjuntos de reglas en `e2-fw` permite dicha configuración:

a.
```
iptables -t filter -A FORWARD -p tcp -d 10.0.0.20 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -i eth1 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp -j DNAT --to-destination 10.0.0.20
```

b.
```
iptables -t filter -A FORWARD -p tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp --dport 80 -j DNAT --to-destination
10.0.0.10:80
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp --dport 8080 -j DNAT --to-destination
10.0.0.20:80
```

c.
```
iptables -t filter -A FORWARD -p tcp -i eth0 -o eth1 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -i eth1 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp -j DNAT --to-destination 10.0.0.20
```

d.
```
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -i eth1 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp -j DNAT --to-destination 10.0.0.20
```


Internet
i-pc2
eth0
20.0.6.20
hub4
eth1
20.0.6.1
i-r2
eth0
20.0.5.1
ISP
eth3
20.0.5.100
isp-r1
eth0
20.0.1.100
eth2
20.0.3.100
eth1
20.0.2.100
eth0
20.0.3.1
i-r1
eth1
20.0.4.1
hub5
eth0
20.0.4.10
i-pc1
firewall
eth0
20.0.2.1
e2-fw
eth1
10.0.0.1
hub3
eth0
10.0.0.10
eth0
10.0.0.20
e2-pc1
e2-pc2
Empresa2
firewall
eth0
20.0.1.1
e1-fw
eth2
10.0.0.1
eth1
20.0.0.1
hub1
eth0
10.0.0.10
e1-pc1
eth0
10.0.0.20
e1-pc2
hub2
eth0
20.0.0.40
eth0
20.0.0.30
e1-pc4
e1-pc3
DMZ
Empresa1

# GRADO EN INGENIERIA EN SISTEMAS DE TELECOMUNICACION (FUENLABRADA)

## 2040 - SISTEMAS TELEMATICOS - MAÑANA A - 2Q

**Pregunta 1**

Sin contestar

Puntúa como 1,00

Carga en `wireshark` esta captura y ordena los paquetes por la columna de tiempo.

NOTA 1: Ten en cuenta que `wireshark` a veces se equivoca al marcar todos los ACK duplicados, o al marcar si una retransmisión es rápida o no.

NOTA 2: Al calcular un valor de umbral redondea hacia abajo.

Justo después de que el cliente envíe el paquete 252, y antes de enviar o recibir ningún otro segmento, indica como máximo cuántos paquetes de tamaño MSS podría enviar el cliente:

- a. 4 paquetes.
- b. No podría enviar ningún paquete.
- c. 8 paquetes.
- d. 2 paquetes.

La respuesta correcta es: 2 paquetes.

**Pregunta 2**

Sin contestar

Puntúa como 1,00

Carga en `wireshark` esta captura y ordena los paquetes por la columna de tiempo.

NOTA 1: Ten en cuenta que `wireshark` a veces se equivoca al marcar todos los ACK duplicados, o al marcar si una retransmisión es rápida o no.

NOTA 2: Al calcular un valor de umbral redondea hacia abajo.

IMPORTANTE: En Wireshark asegúrate de tener desactivado el protocolo DCERPC en *Analyze* -> *Enabled Protocols*.

Observa el paquete 158. Indica cuál de las siguientes afirmaciones es correcta:

- a. A partir del paquete 158 el emisor está en modo *Fast Recovery*, modo que termina al recibir el paquete 163.
- b. A partir del paquete 158 el emisor está en modo *Fast Recovery*, modo que termina al recibir el paquete 161.
- c. A partir del paquete 158 el emisor está en modo *Fast Recovery*, modo que termina al recibir el paquete 162.
- d. A partir del paquete 158 el emisor está en modo *Slow Start*, modo que termina al enviar el paquete 160.

La respuesta correcta es: A partir del paquete 158 el emisor está en modo *Fast Recovery*, modo que termina al recibir el paquete 161.

**Pregunta 3**

Sin contestar

Puntúa como 1,00

Carga en `wireshark` esta captura y ordena los paquetes por la columna de tiempo.

NOTA: Ten en cuenta que `wireshark` a veces se equivoca al marcar todos los ACK duplicados, o al marcar si una retransmisión es rápida o no.

Justo después de que la máquina 11.0.0.11 reciba el paquete 196, y antes de enviar/recibir ningún otro segmento, indica cuál es el **valor de la ventana de congestión** (en número de segmentos de tamaño MSS):

- a. 11 MSS.
- b. 17 MSS.
- c. 6 MSS.
- d. 9 MSS.

La respuesta correcta es: 6 MSS.

**Pregunta 4**

Sin contestar

Puntúa como 1,00

Carga en `wireshark` esta captura y ordena los paquetes por la columna de tiempo.

Indica cuál de las siguientes afirmaciones es correcta respecto a los estados durante el cierre de la conexión :

- a. El cliente tras enviar el paquete 248 se encuentra en estado `CLOSE_WAIT`.
- b. El cliente tras enviar el paquete 255 se encuentra en estado `FIN_WAIT_2`.
- c. El servidor tras enviar el paquete 253 se encuentra en estado `CLOSE_WAIT`.
- d. El servidor tras enviar el paquete 254 se encuentra en estado `CLOSE_WAIT`.

La respuesta correcta es: El servidor tras enviar el paquete 253 se encuentra en estado `CLOSE_WAIT`.

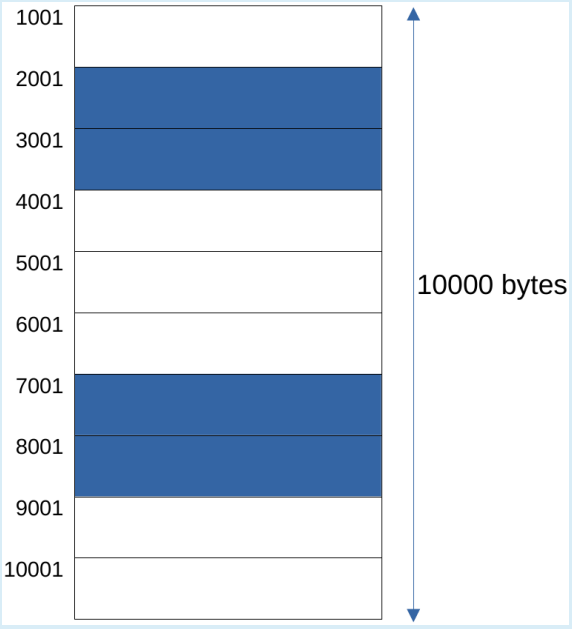
**Pregunta 5**

Sin contestar

Puntúa como 1,00

En una conexión TCP, se sabe que el MSS de la conexión es de 1000 bytes.

En un instante dado, el receptor tiene su buffer 'in' tal y como se muestra en la siguiente figura, donde cada rectángulo azul se corresponde con un segmento con datos recibidos y el número que se muestra en el lado izquierdo es el número de secuencia de cada segmento:




A continuación el receptor recibe el segmento con número de secuencia 1001. Suponiendo que no pasa ningún byte a la aplicación receptora, indica cuáles son los campos relevantes del ACK que envíe el receptor:

a.
```
Acknowledgement number: 4001
Advertised Window: 7000
Options:
SACK: 1001-4001
SACK: 7001-9001
```

b. El resto de respuestas son incorrectas.

c.
```
Acknowledgement number: 1001
Advertised Window: 10000
Options:
SACK: 1001-4001
SACK: 7001-9001
```

d.
```
Acknowledgement number: 4001
Advertised Window: 7000
Options:
SACK: 7001-9001
```

La respuesta correcta es:
```
Acknowledgement number: 4001
Advertised Window: 7000
Options:
SACK: 7001-9001
```

**Pregunta 6**

Sin contestar

Puntúa como 1,00

La captura de tráfico muestra parte de una comunicación HTTP. Indica cuál de los siguientes opciones representa un conjunto de *cookies* válido que podría haber tenido almacenado el cliente que se ejecutaba la máquina 13.0.0.13 **antes de que dicha captura se realizara**:

a.
- `id1=11111 Path=/ Domain=www1.`
- `id2=22222 Path=/ Domain=www1.`
- No se puede saber nada sobre el Path de las cookies `id3` e `id4`.

b.
- `id1=11111 Path=/electronica Domain=www1.`
- `id2=22222 Path=/electronica Domain=www1.`
- `id3=33333 Path=/electronica Domain=www1.`
- `id4=44444 Path=/electronica Domain=www1.`

c.
- `id1=11111 Path=/ Domain=www1.`
- `id2=22222 Path=/ Domain=www1.`
- `id3=33333 Path=/electronica Domain=www1.`
- `id4=44444 Path=/musica Domain=www1.`

d.
- `id1=11111 Path=/electronica Domain=www1`.
- `id2=22222 Path=/electronica Domain=www1`.
- No se puede saber nada sobre el Path de las cookies `id3` e `id4`.

La respuesta correcta es:
- `id1=11111 Path=/ Domain=www1`.
- `id2=22222 Path=/ Domain=www1`.
- `id3=33333 Path=/electronica Domain=www1`.
- `id4=44444 Path=/musica Domain=www1`.

**Pregunta 7**
Sin contestar
Puntúa como 1,00

Ante la siguiente petición de un cliente:

```
GET http://pc1.emp1.net/index.html HTTP/1.1
Host: pc1.emp1.net
```

Un proxy le envía un mensaje de respuesta del cuál sólo se muestra un conjunto de líneas de cabecera del mensaje HTTP:

```
HTTP/1.1 200 OK
Date: Mon, 18 May 2020 17:00:00 GMT
Server: Apache/2.2.9 (Debian)
Last-Modified: Thu, 21 Dec 2017 17:06:47 GMT
ETag: "411d-67-560dcb9a197c0"
Content-Length: 103
Cache-Control: public, max-age=100
Age: 90
Via: 1.0 r1:8080
Content-type: text/html
```

Indica cuál de las siguientes afirmaciones es correcta:

a. El proxy-caché necesitará revalidar ese recurso siempre que se lo soliciten de nuevo porque debe ofrecer la versión más actualizada de ese recurso.

b. Si el proxy-caché recibiera una petición de ese mismo recurso pasados 20 segundos desde que se generó la respuesta mostrada en el enunciado, el proxy-caché necesariamente debería revalidar ese recurso con el servidor.

c. El proxy-caché no necesitará revalidar nunca ese recurso cuando se lo soliciten de nuevo porque no aparece la opción `must-revalidate`.

d. Si el proxy-caché recibiera una petición de ese mismo recurso pasados 5 segundos desde que se generó la respuesta mostrada en el enunciado, el proxy-caché necesariamente debería revalidar ese recurso con el servidor.

La respuesta correcta es: Si el proxy-caché recibiera una petición de ese mismo recurso pasados 20 segundos desde que se generó la respuesta mostrada en el enunciado, el proxy-caché necesariamente debería revalidar ese recurso con el servidor.

**Pregunta 8**
Sin contestar
Puntúa como 1,00

Un proxy envía el siguiente mensaje:

```
GET /index.html HTTP/1.1
If-None-Match: "hydf87qw""
Host: pc6.emp6.com
Via: 1.0 r6:8080
```

Y el servidor responde:

```
HTTP/1.1 304 Not Modified
Server: Apache/2.2.9 (Debian)
Date: Mon, 18 May 2020 09:00:00 GMT
Cache-Control: public, max-age=300
ETag: "hydf87qw"
```

Indica cuál de las siguientes afirmaciones es correcta:

a. El servidor no ha podido enviar esa respuesta.

b. El proxy no ha podido enviar esa petición.

c. El servidor ha enviado esa respuesta porque el recurso index.html no ha cambiado en el servidor.

d. El servidor ha enviado esa respuesta con una nueva versión del recurso index.html que ha cambiado en el servidor.

La respuesta correcta es: El servidor ha enviado esa respuesta porque el recurso index.html no ha cambiado en el servidor.

**Pregunta 9**
Sin contestar

Un conjunto de 5 personas $A, B, C, D, E$ quieren utilizar criptografía de clave pública/privada para intercambiar mensajes de forma segura. Cada persona ha generado una pareja de claves $K_I^+$ y $K_I^-$. Las 5 personas se conocían previamente, pero

Puntúa como 1,00

desde que han generando sus claves no se han visto en persona, por lo que no se han podido intercambiar sus claves públicas de forma segura (aunque pueden acceder a dichas claves públicas, no están seguros de que sean de quien aparentan ser).

Unos días después de que las 5 personas generaron sus claves, A y B coinciden en persona. Indica cuál de las siguientes afirmaciones es **FALSA** respecto a lo que A pueda hacer al coincidir con B en persona:

a. Si A acepta la clave que le ofrece B como $K_B^+$, A podrá estar seguro de que cualquier mensaje que posteriormente envíe cifrado con esa clave sólo podrá ser leído por B.

b. Si A le pasa a B $K_A^+$ diciéndole que es la clave pública de C, A podrá beneficiarse maliciosamente de ello en el futuro.

c. Si A le pasa a B $K_A^-$, A podrá ser gravemente perjudicado en el futuro si B actua maliciosamente.

d. Si A le pasa a B $K_C^+$ diciéndole que es su clave pública (es decir, diciéndole que es $K_A^+$), A podrá beneficiarse maliciosamente de ello en el futuro.

La respuesta correcta es: Si A le pasa a B $K_C^+$ diciéndole que es su clave pública (es decir, diciéndole que es $K_A^+$), A podrá beneficiarse maliciosamente de ello en el futuro.

**Pregunta 10**

Sin contestar

Puntúa como 1,00

Un conjunto de 6 amigos $A, B, C, D, E$ utilizan criptografía de clave pública/privada para intercambiar mensajes. Cada uno de los amigos ha conseguido de forma segura las claves públicas del resto de los amigos. Entre ellos se han puesto de acuerdo para utilizar la función *hash* H.

Una sexta persona, Trudón, intercepta el siguiente mensaje enviado por A para B:

`mensaje`$= K_B^+(m1); K_A^-(H(m1))$

Indica cuál de las siguientes afirmaciones es correcta:

a. Trudón NO puede cambiar $m1$ por un nuevo mensaje $m2$ sin que el destinario previsto $B$ lo note.

b. Trudón puede cambiar el destinatario del mensaje a otro, por ejemplo a $C$ en lugar de $B$, manteniendo $m1$ y dejando el mensaje de forma que $C$ pueda comprobar que el mensaje proviene de $A$.

c. Trudón puede comprobar que el mensaje proviene de $A$ y no ha sido alterado desde que él lo envió.

d. Trudón puede conocer el contenido del mensaje $m1$, pero no puede modificarlo sin que el destinario previsto $B$ lo note.

La respuesta correcta es: Trudón NO puede cambiar $m1$ por un nuevo mensaje $m2$ sin que el destinario previsto $B$ lo note.

**Pregunta 11**

Sin contestar

Puntúa como 1,00

En la figura correspodiente a un escenario de seguridad 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, los *routers* `e1-fw` y `e2-fw` han ejecutado un *script* que aplica estas reglas.

---

Se hacen cambios en la configuración de `e2-fw` de forma que se puedan comunicar los siguientes cliente y servidor:

- En `e2-pc1` se ha ejecutado: `nc -l -p 11000`
- En `i-pc1` se ha ejecutado: `nc -p 22000 20.0.2.1 100`

Para que esta comunicación haya sido posible, indica qué cambios respecto a la configuración inicial han sido necesarios en `e2-fw` :

a.
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp --dport 100 -j DNAT --to-destination
10.0.0.10:11000
iptables -t filter -A FORWARD -p tcp --dport 11000 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

b.
```
iptables -t filter -A FORWARD -p tcp -d 10.0.0.10 --dport 100 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

c.
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp --dport 11000 -j DNAT --to-destination
10.0.0.10:11000
iptables -t filter -A FORWARD -p tcp -d 10.0.0.10 --dport 11000 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

d.
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp --dport 100 -j DNAT --to-destination
10.0.0.10
iptables -t filter -A FORWARD -p tcp -d 10.0.0.10 --dport 100 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

La respuesta correcta es:
```
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp --dport 100 -j DNAT --to-destination 10.0.0.10:11000
iptables -t filter -A FORWARD -p tcp --dport 11000 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Pregunta 12

Sin contestar

Puntúa como 1,00

En la figura correspodiente a un escenario de seguridad 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, los *routers* `e1-fw` y `e2-fw` han ejecutado un *script* que aplica estas reglas.

---

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

- Desde cualquier máquina de Internet se puede acceder a un servidor web (puerto 80 de TCP) lanzado en `e2-pc2`.
- Desde `e2-pc1` o `e2-pc2` NO se puede acceder a ningún servidor TCP o UDP que se lance en cualquier máquina de Internet.
- Desde cualquier máquina de Internet NO se puede acceder a ningún otro servidor TCP o UDP lanzado en `e2-pc1` o `e2-pc2`.

Partiendo de la configuración inicial, indica cuál de los siguientes conjuntos de reglas en `e2-fw` permite dicha configuración:

a.
```
iptables -t filter -A FORWARD -p tcp -d 10.0.0.20 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -i eth1 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp -j DNAT --to-destination 10.0.0.20
```

b.
```
iptables -t filter -A FORWARD -p tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp --dport 80 -j DNAT --to-destination
10.0.0.10:80
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp --dport 8080 -j DNAT --to-destination
10.0.0.20:80
```

c.
```
iptables -t filter -A FORWARD -p tcp -i eth0 -o eth1 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -i eth1 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp -j DNAT --to-destination 10.0.0.20
```

d.
```
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -i eth1 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp -j DNAT --to-destination 10.0.0.20
```

La respuesta correcta es:
```
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --dport 80 -j ACCEPT
iptables -t filter -A FORWARD -p tcp -i eth1 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t nat -A PREROUTING -i eth0 -d 20.0.2.1 -p tcp -j DNAT --to-destination 10.0.0.20
```