Sistemas Telem´aticos para Medios Audiovisuales Pra´ctica 1: Dispositivos de Interconexio´n

### GSyC

Departamento de Teor´ıa de la Sen˜al y Comunicaciones y Sistemas Telem´aticos y Computaci´on

Octubre de 2020

Para esta pr´actica, cada alumno tendr´a escenarios diferentes en cada apartado. En particular, las direcciones IP de las m´aquinas tendr´an asignado en el segundo byte un valor X distinto. Podr´as ver qu´e valor X tienes asignado cuando cargues el escenario en NetGUI y observes la configuraci´on.

Antes de comenzar a realizar la pr´actica, por favor, descarga tus escenarios del siguiente enlace donde deber´as introducir tu nu´mero de DNI (8 d´ıgitos) con la letra correspondiente:

<http://mobiquo.gsyc.es/practicas/stma/p1.html>

# Funcionamiento de hubs y switch

En el fichero lab-hub-switch.tgz est´a 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 au´n s1**.

Arranca el resto de las m´aquinas de una en una.

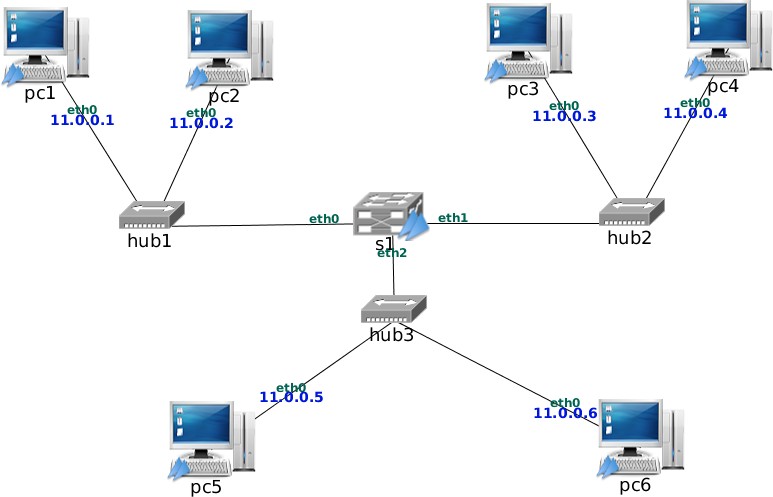


Figura 1: Escenario de hubs y switch

Deja por ahora sin arrancar el *switch* s1. Cada uno de los *hubs* estar´a aislado de los dem´as. Por lo tanto s´olo habr´a conectividad entre los ordenadores que est´an conectados al mismo *hub*. Las tramas Ethernet no pueden salir del *hub* en el que aparecen.

## Comunicacio´n entre m´aquinas 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 m´aquina virtual, escribiendo: tcpdump -i eth0.

1. Piensa en qu´e paquetes se capturar´an en pc2, pc3 y en pc5 si se hace un ping desde pc1 a pc2.
2. Lanza tcpdump en pc2, pc3 en pc5. A continuaci´on ejecuta la siguiente orden en pc1 para hacer un ping a

pc21:

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

(-c 3 hace que el ping s´olo env´ıe 3 paquetes ICMP)

Observa el tr´afico 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 m´aquinas.

1. Comprueba que no existe conectividad (es decir, que no puede hacerse ping) entre m´aquinas que est´en en diferentes *hubs*.

## Comunicacio´n entre m´aquinas con s1 arrancado

1. Arranca el *switch* s1.
2. Piensa en qu´e paquetes se capturar´an ahora en pc2, pc3 y en pc5 repitiendo el mismo ping
3. Comprueba la cach´e de ARP en pc1. Si au´n est´a en ella la direcci´on Ethernet de pc2 borra esa entrada de la cach´e 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 continuaci´on vuelve a hacer en pc1 el ping a pc2:

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

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

1. Responde a estas preguntas:

¿Por qu´e llega a pc3 y a pc5 la solicitud de ARP enviada por pc1?

¿Por qu´e NO llega a pc3 y a pc5 la respuesta de ARP enviada por pc2?

¿Por qu´e NO llega a pc3 y a pc5 el *ICMP echo request* enviado por pc1?

¿Por qu´e NO llega a pc3 y a pc5 el *ICMP echo reply* enviado por pc2?

1. Comprueba las direcciones Ethernet que tiene cada interfaz de cada m´aquina de la figura (usando ifconfig), y apu´ntalas en la memoria.
2. 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 peri´odicamente los cambios en las direcciones aprendidas:

s1:~# watch brctl showmacs s1

(watch repite cada 2 segundos la ejecuci´on de la orden que se le pasa como par´ametro)

Identifica las m´aquinas a las que pertenece cada direcci´on Ethernet y explica su presencia en la tabla de direcciones aprendidas de s1.

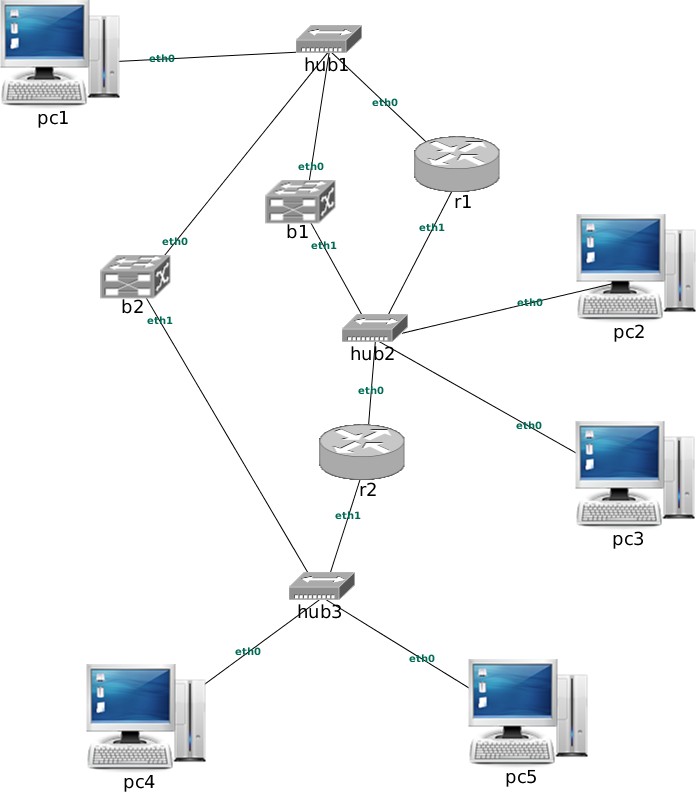
Tras 300 segundos comprobar´as que el *switch* olvida las direcciones aprendidas (mira c´omo va creciendo el valor de la columna *ageing timer*, contador de envejecimiento, en la salida de la orden). Comprueba tambi´en c´omo el *ageing timer* de una direcci´on Ethernet se reinicializa cada vez que el *switch* ve una nueva trama con esa direcci´on Ethernet.

1. Comprueba que ahora s´ı existe conectividad entre todas las m´aquinas de la figura utilizando la orden ping.

1F´ıjate en el valor que tienes asignado en tu escenario a X para ejecutar correctamente el comando

# Redes conectadas a trav´es de switch y router

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



13.X.0.10

13.X.0.1

r1

11.X.0.1

s1

s2

13.X.0.20

11.X.0.2

r2

12.X.0.2

11.X.0.30

13.X.0.40

12.X.0.50

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

## Comunicacio´n entre pc2 y pc4

Con las cach´es de ARP vac´ıas y las tablas de direcciones aprendidas de los switches vac´ıas se desea realizar un ping de pc2 a pc4:

* + 1. Observa la configuraci´on que hay en el escenario para que pc2 y pc4 puedan intercambiar tr´afico. ¿Cu´al de los siguientes caminos crees que seguir´an los mensajes ICMP echo request desde pc2 a pc4?

pc2 *→* s1 *→* s2 *→* pc4 pc2 *→* r1 *→* s2 *→* pc4 pc2 *→* r2 *→* pc4

Justifica la respuesta.

* + 1. Indica cu´antas solicitudes y respuestas de ARP ser´ıan necesarias para que dicho ping funcionase. Explica en qu´e pcs/routers/switches y su interfaz eth concreta se podr´ıan capturar:

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

* + 1. Para ver todo el tr´afico generado deber´as lanzar un tcpdump por cada hub de la figura. Justifica la respuesta.
    2. Lanza tcpdump en las m´aquinas pc1 (switch-router-01.cap), pc3 (switch-router-02.cap) y pc5

(switch-router-03.cap) para ayudarte a comprobar tus suposiciones 2.

* + 1. Indica qu´e direcciones Ethernet habr´an aprendido s1 y s2 despu´es de ejecutar el ping y explica qu´e mensajes han generado dicho aprendizaje. Compru´ebalo.
    2. ¿Crees que habr´a llegado alguno de los mensajes ICMP echo request a pc1, pc3 o pc5? Justifica la respuesta.

## Comunicacio´n entre pc1 y pc3

Con las cach´es de ARP vac´ıas y las tablas de direcciones aprendidas de los switches vac´ıas se desea realizar un ping de pc1 a pc3:

* + 1. Observa la configuraci´on que hay en el escenario para que pc1 y pc3 puedan intercambiar tr´afico. ¿Cu´al de los siguientes caminos crees que seguir´an los mensajes ICMP echo request desde pc1 a pc3?

pc1 *→* r1 *→* pc3 pc1 *→* s1 *→* pc3

pc1 *→* s2 *→* r2 *→* pc3

Justifica la respuesta.

* + 1. Indica cu´antas solicitudes y respuestas de ARP ser´ıan necesarias para que dicho ping funcionase. Explica en qu´e pcs/routers/switches y su interfaz eth concreta se podr´ıan capturar:

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

* + 1. Lanza tcpdump en las m´aquinas r1(eth0) (switch-router-04.cap), pc2 (switch-router-05.cap) y pc5

(switch-router-06.cap) para ayudarte a comprobar tus suposiciones.

* + 1. Indica qu´e direcciones Ethernet habr´an aprendido s1 y s2 despu´es de ejecutar el ping y explica qu´e mensajes han generado dicho aprendizaje. Compru´ebalo.
    2. ¿Crees que habr´a llegado alguno de los mensajes ICMP echo request a pc2, pc4 o pc5? Justifica la respuesta.

## Comunicacio´n entre pc2 y pc5

Con las cach´es de ARP vac´ıas y las tablas de direcciones aprendidas de los switches vac´ıas se desea realizar un ping de pc2 a pc5:

* + 1. Observa la configuraci´on que hay en el escenario para que pc2 y pc5 puedan intercambiar tr´afico. ¿Cu´al de los siguientes caminos crees que seguir´an 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.

* + 1. Indica cu´antas solicitudes y respuestas de ARP ser´ıan necesarias para que dicho ping funcionase. Explica en qu´e pcs/routers/switches y su interfaz eth concreta se podr´ıan capturar:

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

2Recuerda que esta prueba necesita que las tablas de direcciones aprendidas y las cach´es de ARP est´en vac´ıas. 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 continuaci´on ejecutar ’ifconfig s1 up’. Puedes comprobar c´omo la tabla de direcciones aprendidas est´a vac´ıa. Las cach´es de ARP de las ma´quinas se comprueban ejecutando ’arp -a’ y se pueden borrar cada una de sus entradas ejecutando ’arp -d direcci´onIP’

* + 1. Lanza tcpdump en las m´aquinas pc1 (switch-router-07.cap), pc3 (switch-router-08.cap) y pc4

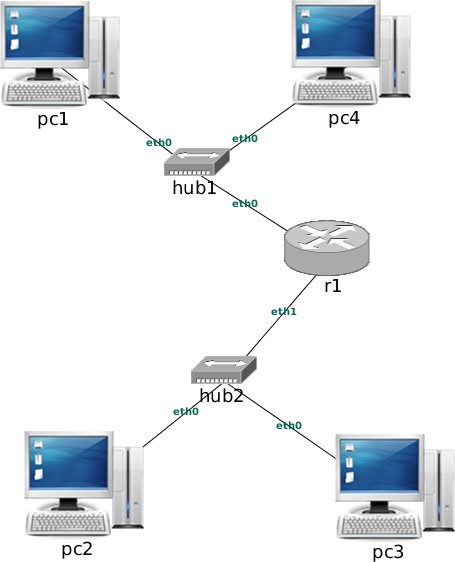
(switch-router-09.cap) para ayudarte a comprobar tus suposiciones.

* + 1. Indica qu´e direcciones Ethernet habr´an aprendido s1 y s2 despu´es de ejecutar el ping y explica qu´e mensajes han generado dicho aprendizaje. Compru´ebalo.
    2. ¿Crees que habr´a llegado alguno de los mensajes ICMP echo request a pc1, pc3 o pc4? Justifica la respuesta.

# Proxy ARP

En el fichero lab-proxyARP.tgz est´a definida una red como la que aparece en la figura 3. Descomprime el fichero, lanza NetGUI y abre el escenario. Arranca las m´aquinas de una en una.

11.0.0.3



12.X.0.10

**Subred 12.X.0.0/24**

12.X.0.1

11.X.0.1

**Subred 11.X.0.0/24**

12.X.0.20

11.X.0.30

Figura 3: Escenario de Proxy ARP

Caracter´ısticas del escenario:

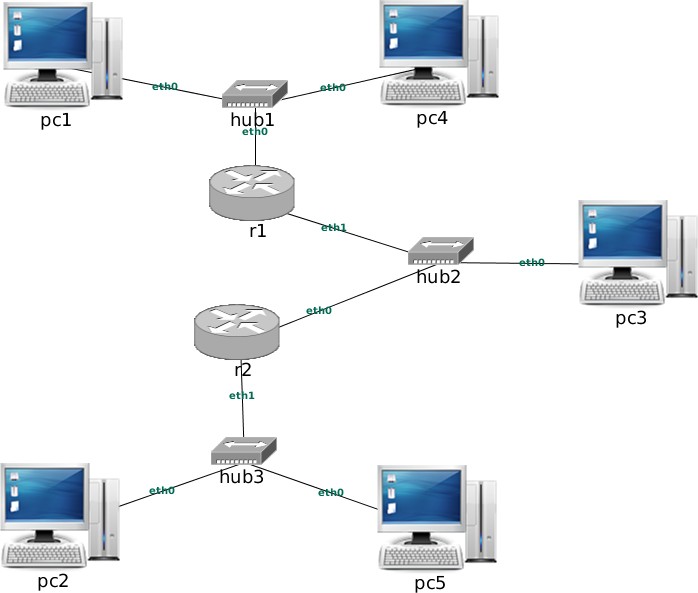
Los pcs y el router r1 est´an configurados con las direcciones IP que se muestran en la figura.

En el fichero /etc/hosts de cada pc est´an los nombres y direcciones IP de pc1, pc2 y pc3, por lo que puedes referirte a ellos por su nombre adem´as de por su IP en las ´ordenes que utilices.

* 1. Activa proxy ARP en la configuraci´on del router r1 para que las m´aquinas pc1 y pc2 tengan conectividad IP entre ellas en ambos sentidos. Explica qu´e modificaciones han sido necesarias y por qu´e.
  2. Con las cach´es de ARP vac´ıas, 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 direcci´on IP de r1(eth0), enviando s´olo 3 paquetes, y despu´es un ping desde pc1 a pc2, enviando s´olo 3 paquetes. Interrumpe la captura y explicalas solicitudes de ARP que ves en el tr´afico capturado en ambos ficheros.
  3. A partir de la captura y de las direcciones IP de r1, ¿c´omo puedes saber que r1 est´a realizando proxy ARP?
  4. Si se ha borrado la cach´e de ARP de pc1 vuelve a ejecutar los 2 ping anteriores y consulta la cach´e de ARP de pc1, indica qu´e observas, explicando a qu´e m´aquina/s pertenece la informaci´on almacenada.

# IP aliasing

En el fichero lab-ipAliasing.tgz est´a definida una red como la que aparece en la figura 4. Descomprime el fichero, lanza NetGUI y abre el escenario. Arranca las m´aquinas de una en una.



13.X.0.10

12.X.0.40

11.X.0.2

11.X.0.30

12.X.0.2

13.X.0.20

12.X.0.50

11.X.0.1

13.X.0.1

Figura 4: Escenario de IP Aliasing

Caracter´ısticas del escenario:

En el fichero /etc/hosts de cada pc est´an los nombres y direcciones IP de pc1, pc2, pc3, pc4 y pc5, por lo que puedes referirte a ellos por su nombre adem´as de por su IP en las ´ordenes que utilices.

pc1, pc3 y pc5 tienen conectividad IP entre ellos. pc2 y pc4 no tienen conectividad IP, ya que no est´an conectados a sus respectivas subredes.

* 1. Asigna **direcciones IP adicionales** en los routers mediante *IP aliasing*, y configura las tablas de encami- namiento que sean necesarias para que pc2 pueda hacer ping a pc3, ten en cuenta que desde r2 se deber´ıa poder alcanzar tambi´en a pc1 3. Indica por qu´e has configurado esas direcciones IP adicionales y en qu´e

interfaces.

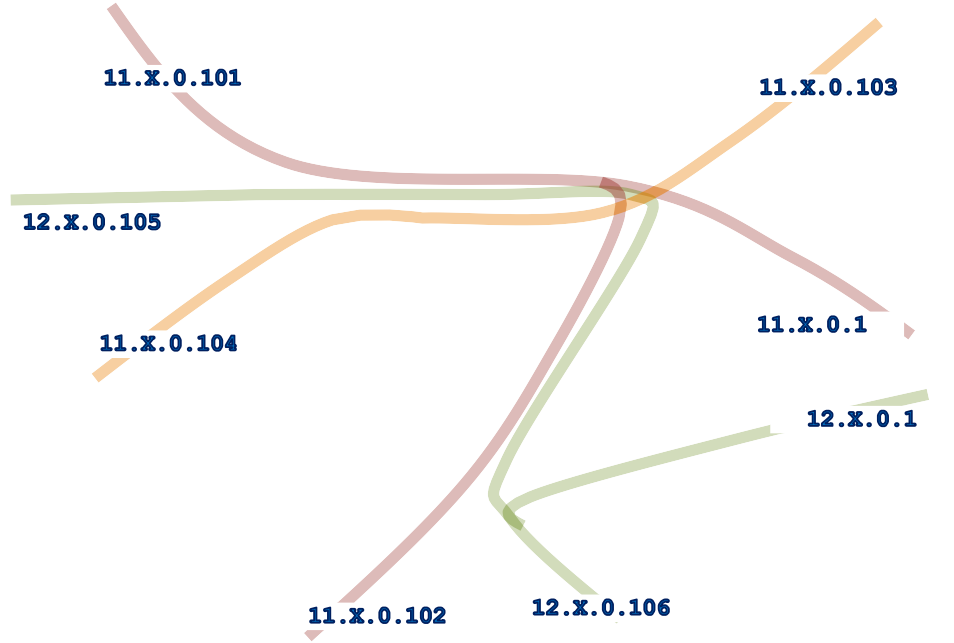
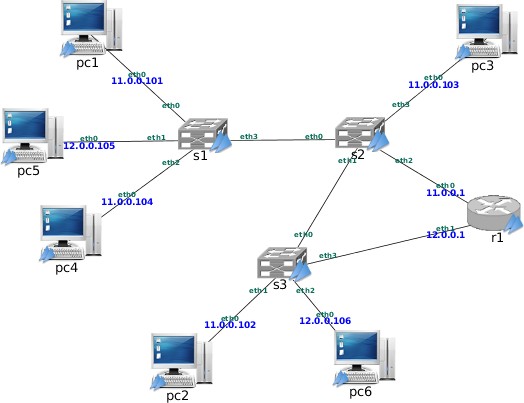
3N´otese que cuando an˜ades una direcci´on por IP aliasing a una tabla de encaminamiento se an˜ade autom´aticamente una entrada para la subred a la que pertenece, entrada que a veces es necesario borrar para que no haya en la misma tabla dos rutas diferentes a la misma subred.

* 1. Realiza una captura en r2(eth1) (ipAliasing-01.cap) y ejecuta un ping desde pc2 a pc3 enviando 3 paquetes y despu´es ejecuta un ping desde pc5 a la direcci´on IP de r2(eth1). Interrumpe la captura y explica las solicitudes de ARP que observas.
  2. ¿Se puede saber s´olo mirando el fichero de captura que en r2 no se ha configurado proxy ARP?
  3. Con la configuraci´on que has realizado previamente ¿pueden comunicarse pc1 y pc5? ¿Por qu´e? Si tu respuesta es negativa, modifica la configuraci´on para que pc5 y pc1 puedan intercambiar tr´afico.
  4. Utiliza de nuevo *IP aliasing* para que pc4 pueda hacer ping a pc1, ten en cuenta que desde r1 se deber´ıa poder alcanzar tambi´en a pc5.
  5. Realiza una captura en r1(eth0) (ipAliasing-02.cap) para ver qu´e paquetes se intercambian cuando pc4

hace ping a pc1. Explica los resultados en la memoria.

# VLANs

En el fichero lab-vlan.tgz est´a definida la topolog´ıa de una red como la de la figura 5 en la que au´n no se han configurado las VLANs. Descomprime el fichero, arranca NetGUI y abre el escenario. Arranca las m´aquinas de una en una.



**VLAN100**

**VLAN300**

**VLAN200**

Figura 5: Escenario de VLANs

Los dispositivos de interconexi´on s1, s2 y s3 est´an configurados para que funcionen como *switches* Ethernet.

* 1. Explica qu´e m´aquinas se pueden comunicar entre ellas. Compru´ebalo realizando ping.
  2. Suponiendo que la cach´e de ARP de pc1 est´a vac´ıa, indica d´onde se puede capturar un solicitud de ARP que la m´aquina pc1 env´ıa preguntando por la direcci´on Ethernet de la m´aquina pc2.

Compru´ebalo realizando capturas. Para este caso puedes utilizar tcpdump -i <interfaz> -s 0 sin necesi- dad de guardar la captura en un fichero, de esta forma ver´as el resultado mostrado en pantalla. (Comprueba antes que en la cach´e de ARP de pc1 no se encuentra la direcci´on Ethernet de pc2; si estuviera, b´orrala).

## Configuraci´on de VLAN100

Para facilitar la configuraci´on de las VLANs en cada switch se propone que esta configuraci´on quede almace- nada en un fichero de script. Un script es un fichero que contiene comandos que se ejecutar´an en el int´erprete de comandos, tal y como si los tecle´aramos en el terminal.

La configuraci´on de la VLAN100 est´a 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 qu´e hace cada uno de ellos. Observa que la primera l´ınea #!/bin/bash indica el int´erprete que va a ejecutar este script, en este caso bash. El resto de l´ıneas en el fichero que comienzan por # son comentarios. Cada uno de los comandos que se desean ejecutar se escriben en l´ıneas diferentes 4.
    2. Ejecuta los scripts para aplicar la configuraci´on. Debes ejecutar cada uno de esos scritps en su switch, por ejemplo en s1:

s1:~# ./vlan-s1.sh

Puedes comprobar la configuraci´on que tiene en un *switch* escribiendo brctl show.

* + 1. Haz un dibujo de cada switch que muestre las interfaces que intervienen en la VLAN100, indicando si estas interfaces llevan o no etiqueta VLAN.
    2. Indica qu´e m´aquinas se pueden comunicar entre ellas.
    3. Suponiendo que la cach´e de ARP de pc1 est´a vac´ıa, indica d´onde se puede capturar un solicitud de ARP que la m´aquina pc1 env´ıa preguntando por la direcci´on Ethernet de la m´aquina pc2.

Compru´ebalo realizando las capturas que creas necesarias, sin necesidad de guardar en fichero el tr´afico capturado. (Comprueba antes que en la cach´e de ARP de pc1 no se encuentra la direcci´on Ethernet de pc2, si estuviera, b´orrala).

* + 1. Indica qu´e ocurre cuando se hace un ping desde pc1 a pc2, teniendo en cuenta que ambas m´aquinas se encuentran en la misma subred. Compru´ebalo realizando las capturas necesarias, sin necesidad de guardar en un fichero el tr´afico capturado.
    2. Asegu´rate de que la cach´e de ARP de pc1 est´a vac´ıa, b´orrala si es necesario. Arranca tcpdump en las siguien- tes 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 tr´afico capturado en un fichero. Realiza un ping desde pc1 a pc2.
    3. Interrumpe las capturas. Observa las direcciones Ethernet aprendidas por s1, s2 y s3.
    4. Analiza las 5 capturas, indica en qu´e capturas se observa la etiqueta de VLAN en el tr´afico y qu´e identificador de VLAN contiene.
       1. ¿Qu´e *switch* introduce dicha etiqueta?
       2. ¿Qu´e *switch* elimina dicha etiqueta?
       3. ¿pc1 y pc2 tienen alguna forma de saber si est´an usando una VLAN para comunicarse?
       4. ) ¿Por qu´e s´olo se ve una trama Ethernet en la captura realizada en la interfaz s2(eth2)?

4Los comandos que se han escrito para desactivar y borrar el switch terminan con ’2 *>* /dev/null’ que significa que si se produce algu´n 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 ejecut´o, se desactiv´o y elimin´o el switch y en las sucesivas veces que se ejecute dicho script el switch no existir´a y se mostrar´ıa un error al desactivarlo y eliminarlo.

* + - 1. ¿En qu´e se diferencia la solicitud de ARP que se captura en pc1(eth0) de la misma solicitud que se captura en s1(eth3)?

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

* + 1. Indica qu´e ocurre cuando se hace un ping desde pc1 a pc4, teniendo en cuenta que ambas m´aquinas se encuentran en la misma subred y conectadas al mismo *switch*. Compru´ebalo realizando una captura en pc1(eth0) (vlan-06.cap) y otra en s1(eth3) (vlan-07.cap). Explica los resultados.

## Configuraci´on de VLAN200

Configura la VLAN200 en los *switches* que creas necesarios. Para ello edita los ficheros de configuraci´on proporcionados en el apartado anterior y an˜ade la configuraci´on de VLAN 200.

Antes de ejecutar la nueva configuraci´on es necesario borrar la anterior, para ello, reinicia los switches s1 y

s2, y a continuaci´on ejecuta sus scripts modificados.

Puedes comprobar la configuraci´on 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 qu´e m´aquinas se pueden comunicar entre ellas con la configuraci´on de VLAN200.
    3. Asegu´rate de que la cach´e de ARP de pc4 est´a vac´ıa, b´orrala 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 tr´afico 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 qu´e capturas se observa la etiqueta de VLAN en el tr´afico y qu´e identificador de VLAN contiene.
    6. Indica qu´e ocurre ahora cuando se hace un ping desde pc1 a pc4, teniendo en cuenta que ambas m´aquinas se encuentran en la misma subred, conectadas al mismo *switch* y las interfaces de dicho *switch* tienen configu- rada una VLAN. Compru´ebalo realizando una captura en pc1 (vlan-12.cap) y otra en pc4 (vlan-13.cap). Explica el resultado.

## Configuraci´on de VLAN300

En este apartado se analiza el comportamiento de 2 VLANs que est´an conectadas a trav´es de un router. Esta configuraci´on 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 configuraci´on es necesario borrar la anterior, para ello, reinicia todos los switches y a continuaci´on ejecuta cada uno de los scripts anteriores.

Puedes comprobar la configuraci´on 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. ¿Qu´e crees que est´a ocurriendo?
    3. Realiza un ping desde pc6 a pc5. ¿Qu´e crees que est´a ocurriendo?
    4. Suponiendo que la cach´e de ARP de pc6 est´a vac´ıa, al realizar un ping de pc6 a pc1, ¿qu´e solicitudes de ARP hay y en qu´e interfaces aparecen? ¿Cu´ales de ellas tendr´an etiqueta VLAN e indica qu´e etiqueta?

Compru´ebalo realizando las capturas que creas necesarias, sin necesidad de guardar en fichero el tr´afico capturado. (Comprueba antes que las cach´es de ARP de pc6 y de r1 est´an vac´ıas, b´orralas si es necesario).

* + 1. Asegu´rate de que las cach´es de ARP de pc6 y r1 est´an vac´ıas, b´orralas 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 tr´afico capturado en un fichero. Realiza un ping desde pc6 a pc1.

Sup´on en qu´e interfaces aparecer´a el tr´afico etiquetado y su identificador de VLAN. Comprueba tus supo- siciones analizando las capturas, indica en qu´e capturas se observa la etiqueta de VLAN en el tr´afico y qu´e identificador de VLAN contiene.

# Entrega de la pr´actica

Para entregar la pr´actica sube al enlace que encontrar´as en aulavirtual antes de que termine el plazo de entrega, un u´nico fichero p1.tgz con el siguiente contenido:

Memoria

Ficheros de captura:

ˆ De hub-switch-01.cap a hub-switch-03.cap.

ˆ De switch-router-01.cap a switch-router-09.cap.

ˆ proxyARP-01.cap y proxyARP-02.cap.

ˆ ipAlising-01.cap e ipAlising-02.cap.

ˆ De vlan-01.cap a vlan-18.cap.