

Sistemas Telemáticos

Práctica 1: Dispositivos de Interconexión

GSyC

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

Enero de 2018

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 -xvzpf lab-hub-switch.tgz`), arranca NetGUI y abre el escenario.

No arranques aún s1.

Arranca el resto de las máquinas de una en una.

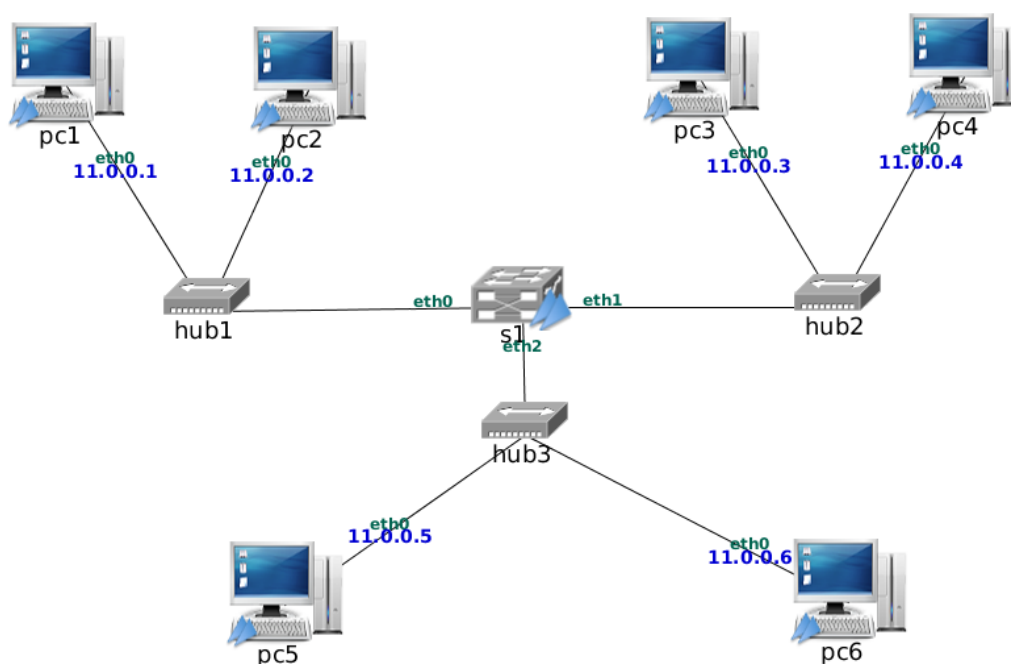


Figura 1: Escenario de hubs y switch

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.

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 `tcpdump` directamente en el terminal de cada máquina virtual, escribiendo: `tcpdump -i eth0`.

1.1. Comunicación entre máquinas con s1 apagado

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 y en pc5. A continuación ejecuta la siguiente orden en pc1 para hacer un ping a pc2:

```
pc1:~# ping -c 3 11.0.0.2
```

(-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.

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, pc3 y en pc5. A continuación vuelve a hacer en pc1 el ping a pc2:

```
pc1:~# ping -c 3 11.0.0.2
```

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.
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. 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 los pcs y los *routers* de uno en uno.

No arranques aún los *switches* s1 y s2.

Para todos los apartados de esta sección no se utilizará IP aliasing.

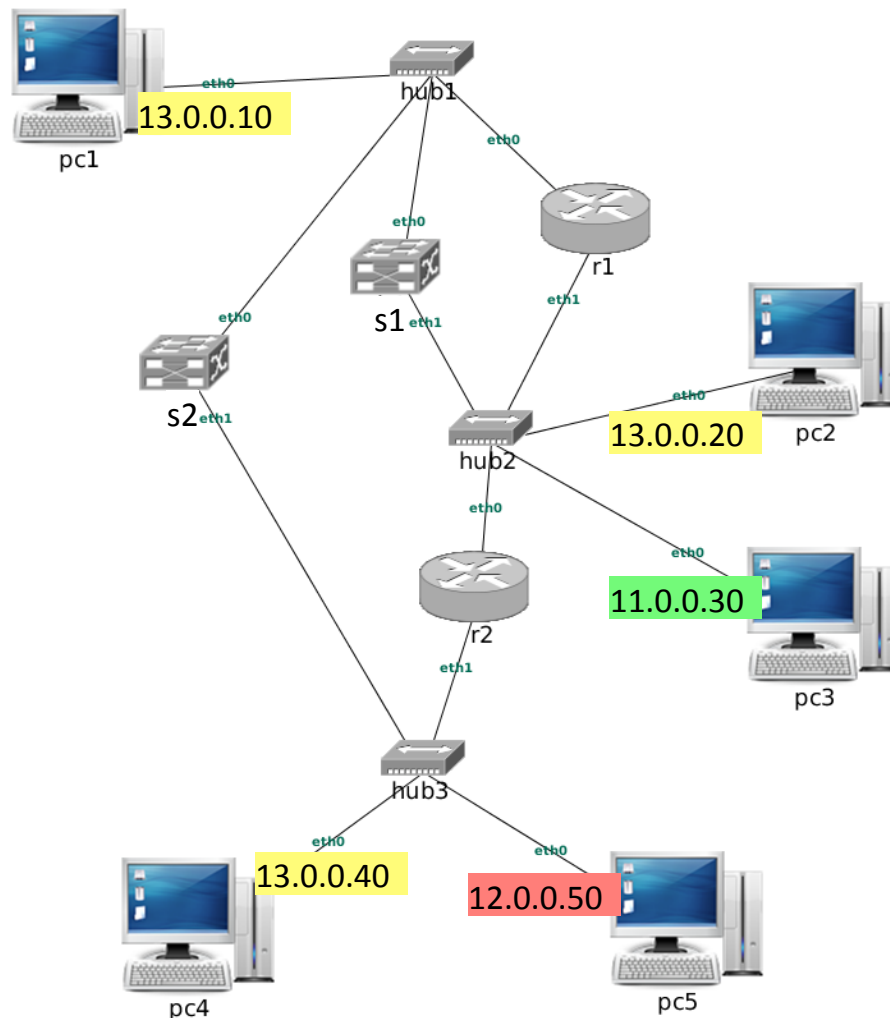


Figura 2: Escenario de redes conectadas por *switches* y *routers*

Características del escenario:

- Hay dos *routers* r1 y r2. No tienen configuradas direcciones IP y será necesario configurarlas cuando se indique explícitamente más adelante.
- Hay dos *switches* s1 y s2.
- Los pcs sólo tienen configurada la ruta de la red a la que pertenece su dirección IP.
- 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.

2.1. Comunicación entre pc1 y pc2

Arranca **s1**, pero todavía no arranques **s2**. No configures aún las direcciones IP de **r1** ni **r2**.

1. Piensa si en estas condiciones funcionará un **ping** de **pc1** a **pc2**. Compruébalo realizando el **ping**. Lanza **tcpdump** en las máquinas que necesites para ayudarte a ver por dónde se transmiten las tramas.
2. Piensa qué direcciones Ethernet habrá aprendido **s1** después de ejecutar el **ping** y compruébalo.
3. ¿Crees que habrá llegado alguno de las tramas/paquetes que han resultado de la comunicación anterior a **pc3**, **pc4** o **pc5**? Para comprobarlo, deberás iniciar el *switch* para que su tabla de direcciones aprendidas esté vacía ¹

2.2. Comunicación entre pc1 y pc3

1. Partiendo de la configuración realizada en el apartado anterior, piensa si en estas condiciones funcionará un **ping** de **pc1** a **pc3**. Compruébalo realizando el **ping**. Lanza **tcpdump** en las máquinas que necesites para ayudarte a ver por dónde se transmiten las tramas.
2. Piensa qué configuración adicional deberías hacer en el escenario para que dicho *ping* funcionara. ¿Bastaría con arrancar **s2**? ¿Tendrías que configurar las direcciones IP de **r1**? ¿Necesitarías también modificar algunas tablas de encaminamiento?
3. Sin arrancar **s2**, realiza las mínimas configuraciones que consideres necesarias en el escenario para que funcione el **ping** de **pc1** a **pc3**.
4. Si la tabla de direcciones aprendidas de **s1** está vacía y todas las cachés de ARP de las máquinas están vacías, piensa qué paquetes serán capturados en **pc3** cuando se realice el **ping** entre **pc1** y **pc3**. Compruébalo realizando una captura de tráfico.
5. Explica que direcciones aprende **s1** y en qué interfaces. Compruébalo.

2.3. Comunicación entre pc2 y pc4

1. Una vez realizados los cambios del apartado anterior, piensa si en esas condiciones funcionará un **ping** de **p2** a **pc4**. Compruébalo realizando el **ping**. Lanza **tcpdump** en las máquinas que necesites para ayudarte a ver por dónde se transmiten las tramas.
2. Piensa qué configuración adicional deberías hacer en el escenario para que dicho *ping* funcionara. ¿Bastaría con arrancar **s2**? ¿Tendrías que configurar las direcciones IP de **r2**? ¿Necesitarías también modificar algunas tablas de encaminamiento?
3. Arranca **s2**. Si las tablas de direcciones aprendidas de **s1** y **s2** están vacías y todas las cachés de ARP de las máquinas están vacías, piensa qué paquetes serán capturados en **pc4** cuando se realice el **ping** entre **pc1** y **pc2**. Compruébalo realizando una captura de tráfico.
4. Explica qué direcciones aprende **s2** y en qué interfaces después de realizar el **ping** entre **pc1** y **pc2**. Compruébalo.
5. Si las tablas de direcciones aprendidas de **s1** y **s2** están vacías y todas las cachés de ARP de las máquinas están vacías, piensa qué paquetes serán capturados en **pc1** cuando se realice el **ping** entre **pc2** y **pc4**. Compruébalo realizando una captura de tráfico.
6. Explica qué direcciones aprenden **s1** y **s2** y en qué interfaces después de realizar el **ping** entre **pc2** y **pc4**. Compruébalo.

¹Para reiniciar el switch puedes desactivar y activar el switch ejecutando el comando 'ifconfig s1 down' y a continuación ejecutar 'ifconfig s1 up'. Puedes comprobar cómo la tabla de direcciones aprendidas está vacía.

2.4. Comunicación entre pc5 y pc2

1. Partiendo de la configuración realizada en el apartado anterior, piensa si en estas condiciones funcionará un **ping** de pc5 a pc2. Compruébalo realizando el **ping**.
2. Piensa qué configuración adicional deberías hacer en el escenario para que dicho **ping** funcionara. ¿Tendrías que configurar las direcciones IP de r2? ¿Necesitarías también modificar algunas tablas de encaminamiento?
3. Realiza las mínimas configuraciones que consideres necesarias en el escenario para que funcione el **ping** de pc5 a pc2.
4. Si la tabla de direcciones aprendidas de s1 y s2 están vacías y todas las cachés de ARP de las máquinas están vacías, piensa qué paquetes serán capturados en pc3 cuando se realice el **ping** desde pc5 a pc2. Compruébalo realizando una captura de tráfico.
5. Explica qué direcciones aprenden s1 y s2, indicando en qué interfaces, una vez realizado el **ping** desde pc5 a pc2. Compruébalo.
6. Fíjate como pc2 recibe una solicitud de ARP que envía pc5, ¿por qué pc2 no responde?

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.

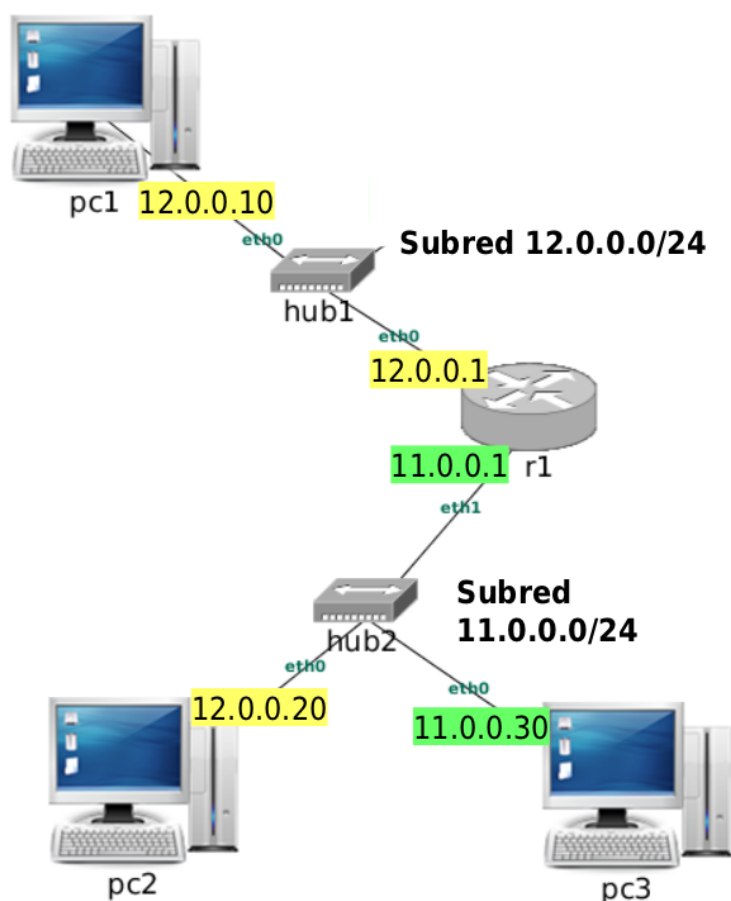


Figura 3: Escenario de Proxy ARP

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)` guardando su contenido en un fichero y ejecuta un ping desde `pc1` a `12.0.0.1`, enviando sólo 3 paquetes, y después un ping desde `pc1` a `pc2`, enviando sólo 3 paquetes. Interrumpe la captura y fíjate en las solicitudes de ARP que ves en el tráfico capturado. A partir de la captura y de las direcciones IP de `r1`: ¿cómo puedes saber que `r1` está realizando proxy ARP?
 3. Si se ha borrado la caché de ARP de `pc1` vuelve a ejecutar los 2 pings anteriores y consulta la caché de ARP de `pc1`, indica qué observas.

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.

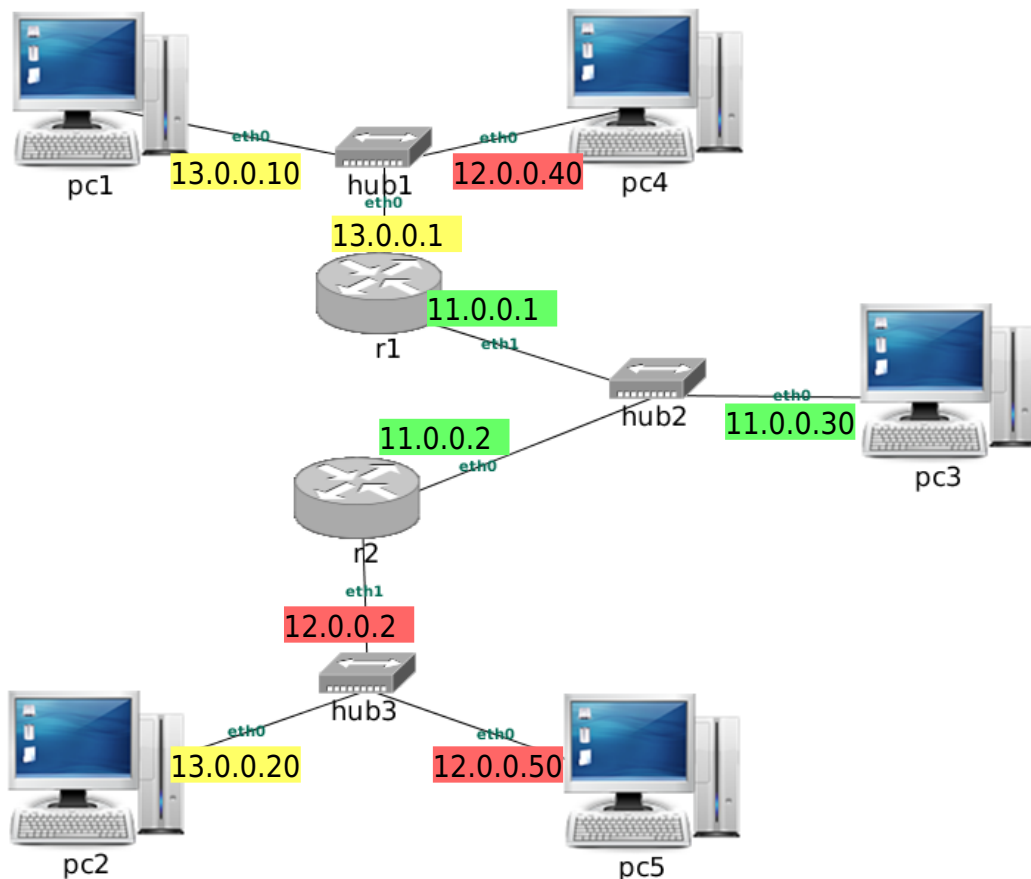


Figura 4: Escenario de IP Aliasing

Características del escenario:

- Los pcs y los routers `r1` y `r2` 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`, `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. 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) guardando su contenido en un fichero y ejecuta un ping desde pc2 a pc3 enviando 3 paquetes y después ejecuta un ping desde pc5 a 12.0.0.2. Interrumpe la captura y observa las solicitudes de ARP. ¿Se puede saber sólo mirando el fichero de captura que en r2 no se ha configurado proxy ARP?
 3. 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.
 4. 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.
 5. Realiza una captura en r1(eth0) (sin necesidad de guardarlo en un fichero) para ver qué paquetes se intercambian cuando pc4 hace ping a pc1.

5. VLANs

En el fichero lab-vlan.tgz está definida una red como la de la figura 5. Descomprime el fichero, arranca NetGUI y abre el escenario. Arranca las máquinas de una en una.

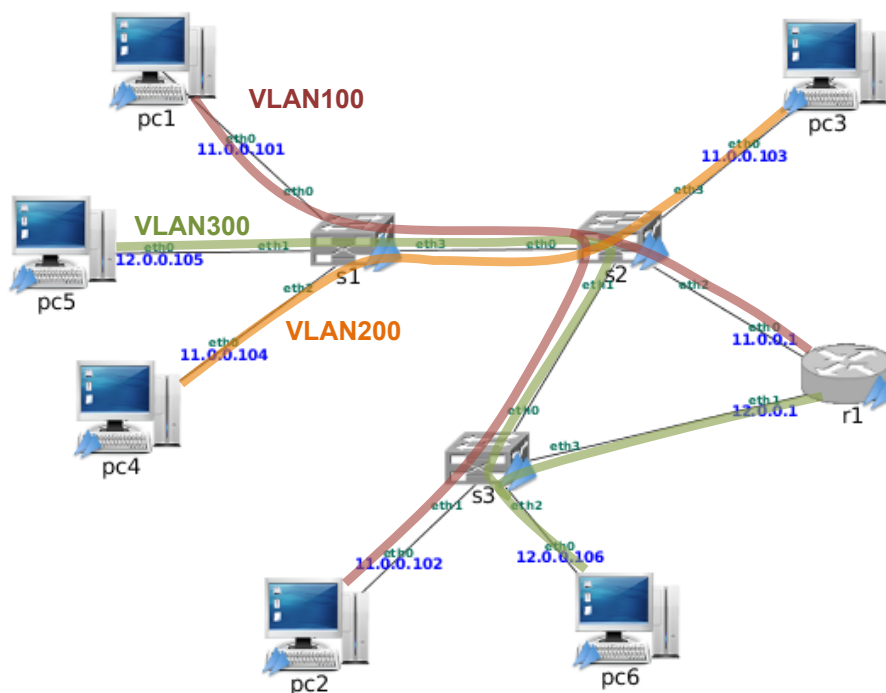


Figura 5: Escenario de VLANs

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

1. Indica 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).

Como los switches están configurados por defecto para trabajar en forma normal, sin VLANs, es necesario desactivarlos para aplicar la configuración de las VLANs que necesites. Para ello ejecuta lo siguiente en cada uno de ellos.

En `s1`:

```
s1:~# ifconfig s1 down
s1:~# brctl delbr s1
```

En `s2`:

```
s2:~# ifconfig s2 down
s2:~# brctl delbr s2
```

En `s3`:

```
s3:~# ifconfig s3 down
s3:~# brctl delbr s3
```

5.1. Configuración de VLAN100

Configura la VLAN100 en los *switches* que creas necesarios. Puedes comprobar la configuración que tiene en un *switch* escribiendo `brctl show`.

1. Indica qué máquinas se pueden comunicar entre ellas.
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 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).
3. 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.
4. Asegúrate de que la caché de ARP de `pc1` está vacía, bórrala si es necesario. Arranca `tcpdump` en las siguientes interfaces: `pc1(eth0)`, `s1(eth3)`, `s3(eth0)` y `pc2(eth0)`, guardando esta vez el tráfico capturado en un fichero. Realiza un `ping` desde `pc1` a `pc2`.
Analiza las 4 capturas, indica en qué capturas se observa la etiqueta de VLAN en el tráfico y qué identificador de VLAN contiene.
5. ¿Qué *switch* introduce dicha etiqueta?
6. ¿Qué *switch* elimina dicha etiqueta?
7. ¿`pc1` y `pc2` tienen alguna forma de saber si están usando una VLAN para comunicarse?
8. 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 las capturas necesarias, sin necesidad de guardar en un fichero el tráfico capturado.

5.2. Configuración de VLAN200

Configura la VLAN200 en los *switches* que creas necesarios. Puedes comprobar la configuración que tiene en un *switch* escribiendo `brctl show`.

1. Indica qué máquinas se pueden comunicar entre ellas con la configuración de VLAN200.
2. Suponiendo que la caché de ARP de **pc4** está vacía, indica dónde se puede capturar un solicitud de ARP que la máquina **pc4** envía preguntando por la dirección Ethernet de la máquina **pc3**.

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 **pc4** no se encuentra la dirección Ethernet de **pc3**, si estuviera, bórrala).

3. Indica qué ocurre ahora cuando se hace un **ping** desde **pc4** a **pc3**, 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.
4. Asegúrate de que la caché de ARP de **pc4** está vacía, bórrala si es necesario. Arranca `tcpdump` en las siguientes interfaces: **pc4(eth0)**, **s1(eth3)** y **pc3(eth0)**, guardando esta vez el tráfico capturado en un fichero. Realiza un **ping** desde **pc4** a **pc3**.

Analiza las 3 capturas, indica en qué capturas se observa la etiqueta de VLAN en el tráfico y qué identificador de VLAN contiene.

5. 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 las capturas necesarias, sin necesidad de guardar en un fichero el tráfico capturado.
6. Después de realizar un **ping** desde **pc3** a **pc4** indica qué switches aprenden direcciones Ethernet y por qué.

5.3. Configuración de VLAN300

Configura la VLAN300 en los *switches* que creas necesarios. Puedes comprobar la configuración que tiene en un *switch* escribiendo `brctl show`.

1. Indica qué máquinas se pueden comunicar entre ellas con la configuración de VLAN300.
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?

Compruébalo realizando las capturas que creas necesarias, sin necesidad de guardar en fichero el tráfico capturado. (Comprueba antes que en 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)**, **s3(eth1)**, **r1(eth0)**, **s2(eth0)** y **pc1(eth0)**, 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.