Práctica 4: Funciones del Switch

José Antonio Martín Martínez
Miguel Ángel Martínez Sánchez
Jorge San Emeterio Villalaín

1 Explicación de la maqueta con el Switch

Cuestión 1: Planteamiento teórico en grupo

a) Dibujamos la maqueta con el número de puerto de los switches asociados a cada equipo, además de la interfaz de cada PC. En la Figure 1 se muestra la topología física de la maqueta especificada en la que se indica el código de cada tarjeta Ethernet usada y el nº de puerto usado en el cableado.

Figure 1: Topología física.

Le asociammos ahora a cada equipo una dirección IP

IP equipos		
Equipo	IP	Interfaz
PCA	192.168.0.2	eth0
PCB0	192.168.1.1	eth0
PCB1	192.168.0.1	eth1
PC0	192.168.0.3	eth0
PC1	192.168.1.2	eth0
PC2	192.168.1.3	eth0

b) En la Figure 2 se representa la topología lógica. En ella se representan los switches en forma de bus, ya que solo operan a nivel dos. El enlace que interconecta los dos switches lo indicamos en azul con lineas discontinuas.
Los niveles OSI que se representan son el nivel físico y el nivel de enlace ya que los switches no son capaces de trabajar a un nivel superior.

Figure 2: Topología lógica.

d) Escribimos la tabla FDB de cada Switch

Tabla FDB S1	
MAC	Puerto
MA	1
MB0	4
MC0	4
MB1	2
MC1	3
MC2	4

Tabla FDB S2	
MAC	Puerto
MA	1
MB1	1
MB0	2
MC0	3
MC2	4

e) Para este caso solo existe un único dominio broadcast en el que pertenecen todos los puertos e interfaces de los equipos.

Cuestión 2: Monta y cablea la maqueta.
Usamos el comando *ethtool* < *interfaz* > y comprobamos la velocidad y el modo. Para este caso todas las tarjetas tienen velocidad de 100Mbps y el modo es Full-Duplex.
En la tarjeta se enciende una luz verde para indicar que se conecta el cable.

La luz SDP del switch indica la velocidad, si el LED es amarillo indica que la velocidad es de 100M y el LED verde 1000M. La luz IDX indica el modo, en este caso Full-Duplex. Los niveles que comprobamos con estas cuestiones son los nieveles 1, físico, y nivel 2, enlace.

Cuestión 3: Configuración IP
Configuramos las tarjetas de las maquinas virtuales PC0, PC1 y PC2 desde su consola:
PC0:ifconfig eth0 192.168.0.3 netmask 255.255.255.0 up
PC1:ifconfig eth0 192.168.1.2 netmask 255.255.255.0 up
PC2:ifconfig eth0 192.168.1.3 netmask 255.255.255.0 up

Configuramos ahora las de PCB y PCA
PCB:ifconfig eth0 192.168.0.1 netmask 255.255.255.0 up
PCB:ifconfig eth1 192.168.1.1 netmask 255.255.255.0 up
PCA:ifconfig eth0 192.168.0.2 netmask 255.255.255.0 up

a) Tecleamos route -n en cada uno de los equipos y vemos su tabla de encaminamiento. PC0, PCB(eth0) y PCA tienen una entrada para la red 192.168.0.0 y PC1, PC2 y PCB(eth1) tienen una entrada para la red 192.168.1.1. Por tanto, su tabla de encaminamiento es correcta con la configuración existente.

b) Obtenemos la dirección MAC de cada una de las tarjetas Ethernet.

Dirección MAC		
Equipo	MAC	Interfaz
PCA	00:0f:fe:0c:db:52	eth0
PCB	00:0f:fe:4c:d1:c6	eth0
PCB	00:4f:4e:04:02:fb	eth1
PC0	08:00:27:de:a4:d0	eth0
PC1	08:00:27:fo:f9:d6	eth0
PC2	08:00:27:a7:39:65	eth0

PC tiene 3 interfaces como hemos dibujado en el esquema aunque, a efectos prácticos, en las 3 máquinas virtuales aparece eth0.

c) Ejecutamos el comando: ping -c 4 ip_host
Los ping entre los equipos de la misma red tienen éxito, por tanto se ha configurado correctamente el cableado de la red.

d) Ejecutamos el comando arp -d en cada equipo y borramos la tabla ARP.

Cuestión 4: Análisis de la función de aprendizaje

Paso 1. Desde PC0 haz un ping a PCA con un solo paquete icmp.
Para realizar el ping ejecutamos `ping -c 1 192.168.0.2` desde la terminal de PC0.
Las tablas de PC1 y PC2 están vacías mientras que las del resto de quipos son las siguientes.

ARP PC0		
Equipo	MAC	Interfaz
PCA	00:0f:fe:0c:db:52	eth0

ARP PCA		
Equipo	MAC	Interfaz
PC0	08:00:27:de:a4:d0	eth0

ARP PCB0		
Equipo	MAC	Interfaz
PC0	08:00:27:de:a4:d0	eth0

Se llevan a cabo un ARP multicast(request) y un ARP unicast(reply) para aprender las direcciones MAC. En la captura aparecen dos paquetes ICMP, uno request (de PC0 a PCA) y otro reply (de PCA a PC0).
El primer ARP request, enviado por PC0, es recibido por las dos interfaces eth0 y eth1 del PCB, en cambio las tramas ICMP y el arp reply no llegan en ningún momento al equipo mencionado ya que los switches han aprendido y han reencaminado el tráfico correctamente.

Paso 2. Desenchufa un breve instante los dos switches y vuelve a enchufarlo.
Tras reiniciar el switch comprobamos que las tablas arp indicadas en el Paso 1 siguen igual . Una vez comprobadas volvemos a realizar el ping.

a) En la Figure 3 mostramos un cronograma temporal en el que indicamos el emisor, receptor y los dos switches indicando el puerto por el que reciben y envian cada uno de ellos.

Figure 3: Topología lógica.

b) Una primera entrada se realizará en el switch 2 tras asociar la mac de PC0 con su puerto 3. El switch S1, tras recibir la trama que le envía S1, asocia el puerto de recepción, puerto 1, también con la mac de PC0.
Cuando PCA contesta al ping, S1 asocia la mac de PCA al puerto de recepción, es decir, al puerto 2. Lo mismo hace S2, que asocia la mac de PCA al puerto 1 tras recibir la trama que le envia S1.
Finalmente, recopilando los datos nos quedan las dos tablas siguientes:

Tabla FDB Switch 1	
MAC	Puerto Asociado
MPC0	1
MPCA	2

Tabla FDB Switch 2	
MAC	Puerto Asociado
MPC0	3
MPCA	1

Cuestión 5. Dominio broadcast de un switch no gestionable

a) No se llega a enviar ningún paquete ICMP. El tipo de tráfico que se genera es ARP request para preguntar la mac del equipo que no existe.

b) No se llega a enviar ningún paquete ICMP. En este caso no se genera ningún tipo de tráfico porque intentamos enviar tráfico a redes distintas y no tenemos puerta de enlace.

c) Las tramas broadcast que se han enviado llegan a la interfaz eth0 de PCA y a todas las interfaces de PCB. En este escenario las tramas broadcast de las dos redes lógicas están mezcladas ya que estamos trabajando como si los switches fueran no gestionables dónde todos sus puertos pertenecen al mismo dominio broadcast al no haber asociado estos a VLANs distintas.

d) Cuando el switch recibe una trama broadcast primero consulta su tabla FDB. Si la mac origen no existe en la tabla la añade y en el caso de que ya exista la actualiza. El siguiente paso, como estamos trabajando en modo no gestionable en los switches, envía la trama broadcast recibida por todos los puertos menos por el que la ha recibido.

Cuestión 6: Comprobación y análisis de la función de reenvío de tramas en otros contextos.

a) - Nivel de red: El mensaje tiene tanto la IP origen como la destino y por ello puede formar el paquete.
- Nivel de enlace: Se posee la MAC origen pero no la destino. Se envía un ARP request con dirección destino broadcast para conocer la MAC de la interfaz objetivo. EL ARP request llega a todos los miembros del dominio de broadcast. Sin embargo, como la interfaz no existe nunca se devuelve un ARP reply.

b) $IP\begin{cases} \text{Ori:} & 192.168.0.2 \\ \text{Dest:} & 192.168.100 \end{cases}$ $MAC\begin{cases} \text{Ori:} & 00{:}0f{:}fe{:}0c{:}db{:}52 \\ \text{Dest:} & 0f{:}0f{:}0f{:}0f{:}0f{:}0f \end{cases}$

- La trama es recibida por todas las interfaces del dominio broadcast.
- Cuando un switch no conoce el puerto por el que llega a una dirección MAC, reenvía la trama por todos sus puertos. Se cumple el principio de funcionamiento.

c) El firewall de Windows impide que llegue el mensaje ICMP al PCA. No funciona el ping.

Cuestión 7: Proceso de aprendizaje IP-MAC en un PC

Paso 1. Desde PCA haz ping a PC0

Tabla ARP PCA		
IP	MAC	interfaz
192.168.0.3	08:00:27:31:cc:de	eth0

En la transmisión del mensaje hay un mensaje ARP para conocer la MAC de 192.168.0.3 y hay otro para responder a PC0 sobre la MAC de PCA.

Tabla ARP PC0		
IP	MAC	interfaz
192.168.0.2	00:0f:fe:0c:db:60	eth0

Los ARP son los mismos que en el anterior pero invertidos. Los demás elementos no intervienen en la transmisión.

Paso 2. Desde PC1 haz ping a PC2
PCA y PCB no intervienen en la transmisión del mensaje.

Tabla ARP PC1		
IP	MAC	interfaz
192.168.1.3	08:00:27:a7:39:65	eth0

PC2		
IP	MAC	interfaz
192.168.1.1	08:00:27:f0:f9:d6	eth0

a) Se envia un ARP request broadcast al dominio buscando la direccion MAC de la IP destino. Al llegar a la interfaz que tiene asignada la IP, esta devuelve un mensaje ARP reply al origen y actualiza su tabla ARP con el mensaje recibido. El PC 1 recibe el reply y actualiza la tabla ARP.

b) El mensaje ARP request tiene los siguientes campos:

```
MAC origen: 00:0f:fe:0c:db:60
MAC destino: ff:ff:ff:ff:ff:ff
Campo Type: ARP (0x0800)
-o-
OpCode: request (1)
Sender MAC: 00:0f:fe:0c:db:60
Sender IP: 192.168.0.2
Target MAC: 00:00:00:00:00:00
Target IP: 192.168.0.3
```

c) El mensaje ARP reply está formado por:

```
MAC origen: 00:0f:fe:0c:db:60
MAC destino: 08:00:27:31:cc:de
Campo Type: ARP (0x0806)
-o-
OpCode: reply (2)
Sender MAC: 00:0f:fe:0c:db:60
Sender IP: 192.168.0.2
Target MAC: 08:00:27:31:cc:de
Target IP: 192.168.0.3
```

d) ARP request: los datos del emisor se corresponden con los del PC origen. En los datos del objetivo, conocemos la IP pero desconocemos la MAC. Esto nos lleva a enviar un mensaje ARP para poder terminar de encapsular el mensaje.
ARP reply: Los datos del emisor están otra vez formados por los del origen del mensaje. En este caso, hemos aprendido mediante el ARP request que nos llegó anteriormente la MAC e IP del dispositivo que está preguntando. De esta manera podemos encapsular el mensaje.

e) Se generan dos mensajes ARP request. En el primero, PCA pregunta cual es la MAC de 192.168.0.1. Para esto genera un mensaje con dirección broadcast. En el segundo, PCA vuelve a pedir la MAC de PCB, aunque conozca de antemano los datos, debido a que su tabla va a caducar.

Cuestión 8: Profundizando en el tipo de mensajes ARP

a) Desde PCB ejecutamos `arping -c 2 192.168.0.2`

b) Desde PCB ejecuta `arping -c 2 192.168.0.1`

c) Desde PCB ejecuta `arping -c 2 -U 192.168.0.1`

d) Desde PCB ejecuta `arping -c 2 -A 192.168.0.1`

e) Desde PCB ejecuta `arping -c 2 -D 192.168.0.1`

f) Desde PCB ejecuta `arping -c 2 -D 192.168.1.1`

h) El comando arping es un comando peligroso debido a que podemos ocultar la IP origen tras la IP 0.0.0.0. Cuando un PC se encuentra con esta IP en el campo destino la interpreta como que cualquier PC es un destino válido. De esta manera se manda un ARP a todos los dispositivos de la red y provoca que todos ellos respondan. Un ordenador situado en escucha puede utilizar este comando tanto para aprender como es la red como para sobresaturarla a base de mensajes innecesarios.

i) Con el comando -U se envían los ARP con la IP origen correspondiente con lo que el dispositivo se da cuenta de que se pregunta a sí mismo. Sin embargo, con el comando -D ocultamos la IP tras 0.0.0.0. El dispositivo ya desconoce quien le ha preguntado y por ello responde a toda la red.