

Dispositivos de red

Switches

Walter Lozano
Alejandro Rodríguez Costello

August 27, 2024

1. Dispositivos activos

En el escenario de la figura 1, provisto por la cátedra, la PC11 y la PC21 quieren realizar una impresión usando Printer1 y Printer2 respectivamente. Aun introduciendo un pequeño retraso entre el comienzo de cada comunicación de 1 ms, se producirán un serie de colisiones. Compruébelo¹.

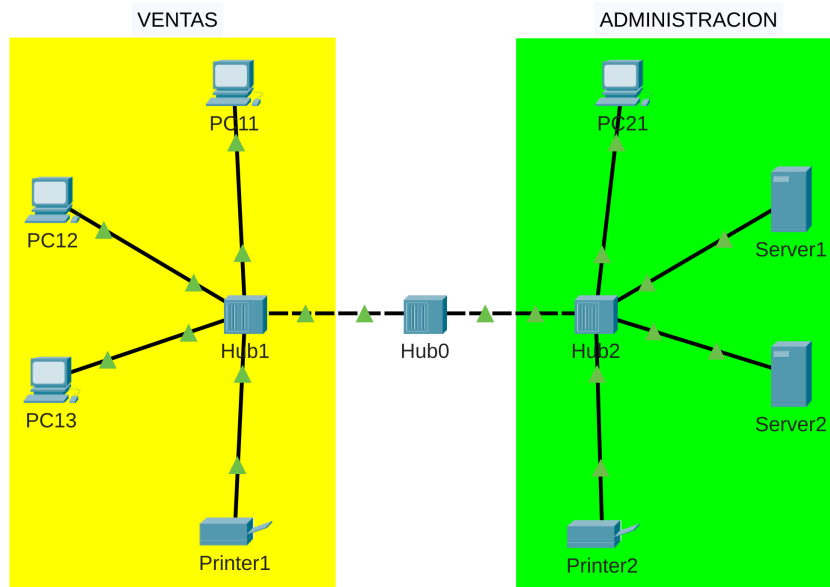


Figura 1: Escenario con múltiples hubs

Ahora vamos a cambiar de escenario, utilizando uno provisto por la cátedra², reemplazando el Hub0 por un dispositivo activo llamado switch. El mismo no realiza un envío de todos los PDU por sus ports de salida siempre y cuando haya realizado el correspondiente aprendizaje (*switch learning*). Realizando un envío previo de los PDU en modo *Realtime* y luego repitiendo la operación en modo *Simulation* podemos observar que la comunicación se lleva a cabo sin problemas (figura 2). Además observamos que los PDU de un color no se propagan fuera del dominio de colisión. ¿Que puede deducir?

Probemos ver que ocurre con una colisión por ejemplo en VENTAS. Para ello repetimos la experiencia solicitando la transmisión de un PDU desde la PC12 a PC13 con 1 ms de atraso. ¿Cómo se comporta el switch? Podemos observar que en esta configuración se mantienen dos dominios de colisión separados. Ahora modifica el escenario de forma tal que todos los dispositivos

¹Utilice procedimientos similares a labs anteriores.

²El Switch0 está configurado para evitar problemas en los experimentos.

estén conectados al Switch0 respetando la tabla 1 como se observa en la figura 3³. Luego realiza experimentos similares y llega a una conclusión.

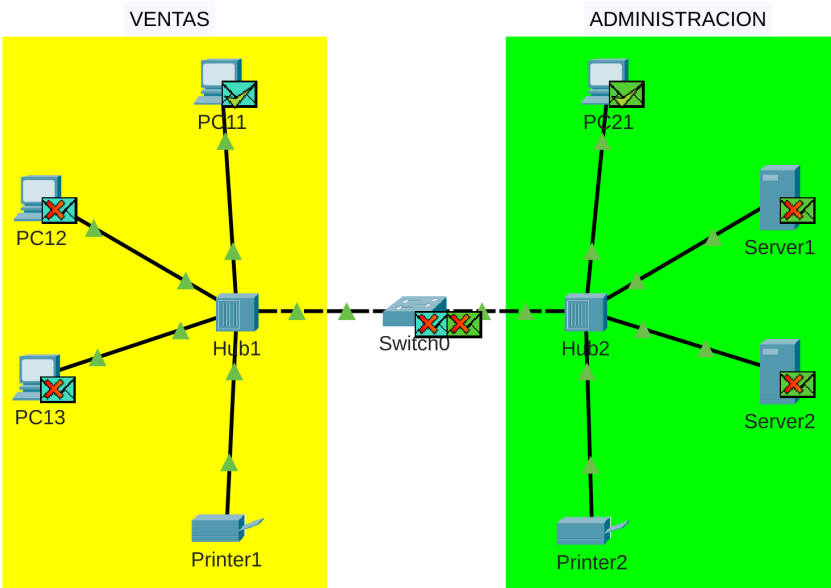


Figura 2: Escenario con un switch y dos hubs

Name	Switch port	Name	Switch port
PC11	Fa1	PC21	Hub1 Fa5
PC12	Fa2	Server1	Hub1 Fa6
PC13	Fa3	Server2	Hub1 Fa7
Printer1	Fa4	Printer2	Hub1 Fa8

Cuadro 1: Asignaciones de dirección y conexionado de los hosts

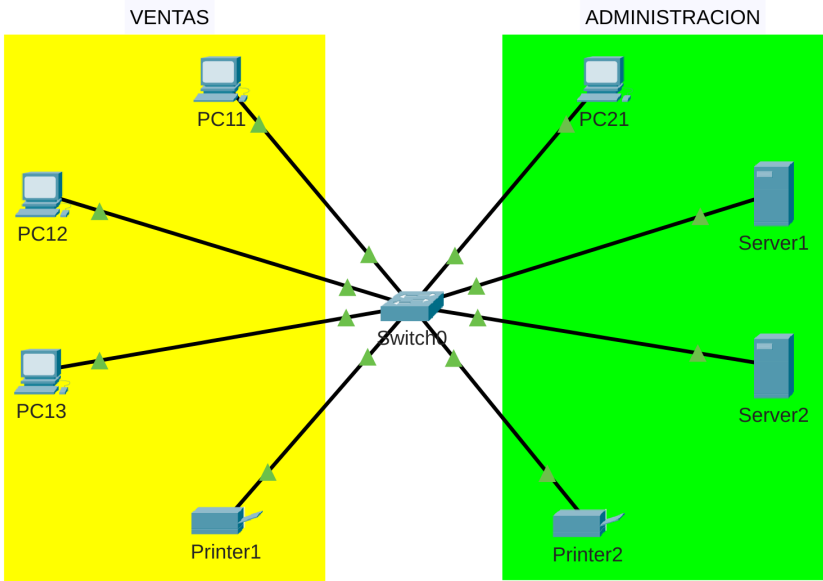


Figura 3: Escenario con un switch

³Es importante que las modificaciones se realicen usando el escenario previo y lo guardes.

2. El protocolo ARP

Vamos a profundizar en el protocolo ARP. Tome nota de todas las direcciones MAC de los hosts (PCs, Printers y Servers) del escenario anterior, seleccionando en la pestaña *Config*, la interface FastEthernet0 y en las propiedades de la misma el valor en *MAC Address*. La misma tiene aproximadamente la forma 0004.9AED.E15B de 48 bits, donde cada subconjunto de bits tiene un significado específico que puede explorarse en la referencia dada. Elabore una tabla con las mismas.

Ahora carga el escenario nuevamente y pasa a modo simulación. Aunque no es mandatorio para esta práctica aprovechamos la oportunidad para mencionar que en el panel *Simulation Panel* se puede utilizar el filtrado de paquetes que puede ser de utilidad en prácticas más complejas⁴. Para ello pulsamos el botón *Edit filters* y en la ventana emergente IPv4⁵ seleccionamos los protocolos de interés, solamente ARP en nuestro caso.

En dicho modo realizamos un `ping -n 1 192.168.1.12` a PC12 desde la consola de PC11 enviando un solo PDU (*ICMP Echo Request*), asegurándonos que su cache ARP está vacía previamente. Para que la operación se complete debes darle play y detenerla cuando se halla completado. En la ventana *Event List* debes ver los eventos que se muestran en la figura 4.


Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC11	ARP
	0.001	PC11	Switch0	ARP
	0.002	Switch0	PC12	ARP
	0.002	Switch0	PC13	ARP
	0.002	Switch0	Printer1	ARP
	0.002	Switch0	PC21	ARP
	0.002	Switch0	Server1	ARP
	0.002	Switch0	Server2	ARP
	0.002	Switch0	Printer2	ARP
	0.003	PC12	Switch0	ARP
	0.004	Switch0	PC11	ARP

Figura 4: Intercambio de mensajes ARP

¿Cómo logra PC11 comunicarse con PC12? Es obvio de que PC11 debería conocer la dirección MAC de PC12 para poder realizar la comunicación. De hecho la lógica indica que cada máquina debería tener o construir una tabla similar a la elaborada antes manualmente. Pero ¿cómo?

Para la obtención de dicha tabla se utiliza una difusión (*broadcast*) en la red, conocida como difusión Ethernet. La dirección MAC de una difusión es FFFF.FFFF.FFFF y todas las máquinas de la LAN deben atender dichos mensajes. En dicha difusión un PDU Ethernet transporta en su *payload* una solicitud de ARP Request. A este fenómeno se lo conoce como **encapsulamiento**. Para ver la trama Ethernet y el paquete ARP, podemos usar seleccionar el segundo evento que describe al PDU en el dispositivo Switch0 que llega desde la PC11, como vemos en la figura 5.

Solo se observan dos *layers* del modelo OSI, el nivel físico y el de enlace, que es donde pertenecen los protocolos en estudio. Del layer 2 podemos ver el origen y destino del PDU Ethernet y del layer 1 podemos deducir el comportamiento del switch físicamente y responder ¿que papel juegan los switches en las difusiones?

El análisis en detalle del PDU puede realizarse al observar la información en *PDU Details* (figura 6).

⁴Al seleccionar **Show None** podemos filtrar todos.

⁵Hay otras opciones que no estamos explorando como IPv6 o Misc que no son de interés para esta práctica.

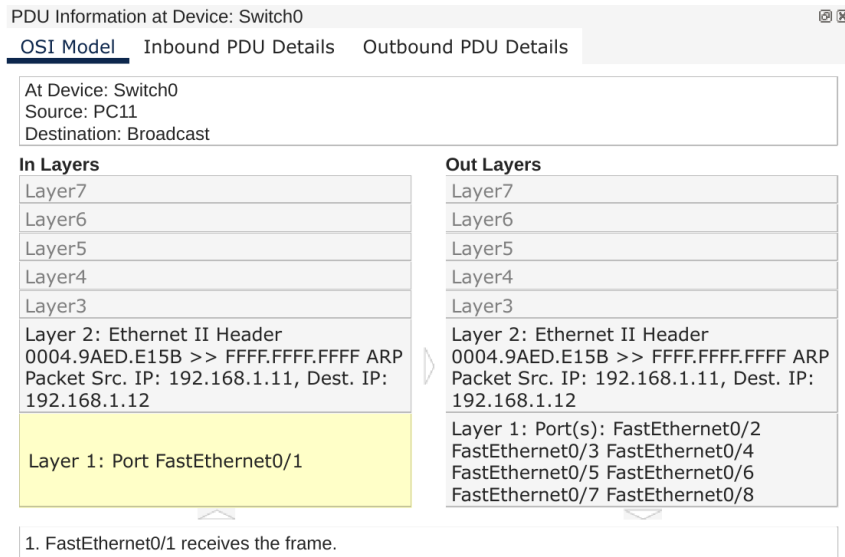


Figura 5: PDU Info OSI level

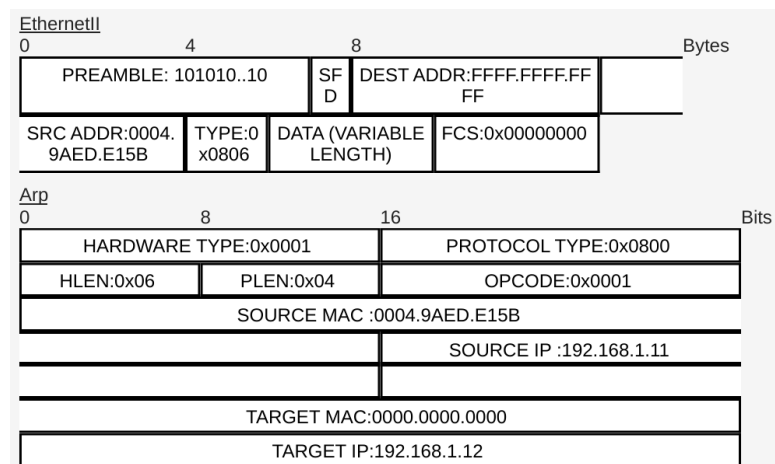


Figura 6: PDU Detail

A nivel Ethernet:

Destination Address: FFFF.FFFF.FFFF (broadcast)

Source Address: 0004.9AED.E15B (PC11)

Type: 0x0806 (ARP)

A nivel ARP:

Hardware Type: FFFF.FFFF.FFFF (broadcast)

Protocol Type: 0004.9AED.E15B (PC11)

Hardware Length: 0x06 bytes (MAC)

Protocol Length: 0x04 bytes (IP)

Opcode: 0x0001 (Request)

Source MAC: 0004.9AED.E15B (PC11)

Source IP: 192.168.1.11 (PC11)

Target MAC: 0000.0000.0000 (unknown)

Target IP: 192.168.1.12 (PC12)

De la anterior información podemos entender que ARP solicita mediante un broadcast a todos los hosts de la LAN que le informen cuál es la MAC del la IP que solicita en el campo **Target IP** mediante un mensaje **Request** (*Opcode 0x1*). En contraposición la PC12 enviará un mensaje **Replay** (*Opcode 0x2*) en modo unicast, que puede comprobarse analizando el penúltimo PDU.

Debido a serias limitaciones de Packet Tracer no podemos ensayar entradas estáticas en la cache ARP (*ARP Static Entry*) de las PCs. Sin embargo todos los sistemas operativos modernos disponen de esta característica.

Investigue cuales son los comandos de Linux y Windows para colocar entradas estáticas en la cache ARP ¿cuáles son las ventajas y las desventajas? Discuta el tema en clase y elabore un caso de uso práctico aunque sea a nivel conceptual.

3. Switch learning

A traves de las diferentes simulaciones llevadas a cabo en esta práctica es evidente que el switch sufre alguna transformación interna adquiriendo conocimiento de la red a medida que fluyen los paquetes ARP (*learning*). Esto se almacena en una tabla llamada **FIB**. Luego mediante esta tabla el switch toma decisiones de reenvío inteligente mejorando la performance de la red (*forwarding*). Aunque todos los switches aprenden las MAC que pasan por sus interfaces y elaboran tablas internas para hacer el forwarding, no todos los switches permiten ver o interactuar con estas tablas. Para ello se requiere tener acceso a la consola del switch, característica en general propias de los switch administrables.

Debido a que el switch utilizado en estas simulaciones dispone de esta característica, aprovechamos para ver como acceder a la misma. Esto puede realizarse de dos maneras: mediante el uso de la opción CLI *Command Line Interface* de las propiedades del switch, que es una característica del simulador Packet Tracer, o colocando un cable de consola entre la una máquina, en este caso, PC11 y el Switch0 y luego acceder al CLI mediante la aplicación *Terminal* con parámetros default. Esta última es la opción que utilizaremos en esta práctica, para tener una experiencia más real, pero luego utilizaremos normalmente la primera.

A partir de allí tendremos acceso a **Cisco IOS**, que es uno de los sistemas operativo de red de Cisco para sus equipos. En el modo **User EXEC** podemos poner el siguiente comando para observar el contenido de la tabla de direcciones MAC del switch:

```
Switch0>show mac address-table
```

La misma puede estar vacía, pero basta con ejecutar un **ping** entre algunas PCs, por ejemplo PC11 y PC12 para ver una salida como la que se exhibe a continuación:

```
Switch0>show mac address-table
```

```
Mac Address Table
```

Vlan	Mac Address	Type	Ports
----	-----	-----	-----
1	0004.9aed.e15b	DYNAMIC	Fa0/1
1	000d.bd96.b915	DYNAMIC	Fa0/2

Realice algunas otras experiencias para ver como se llena la tabla.

Cambiando al modo **Priviledge EXEC** con el comando **enable** puede entrar al modo configuración (*Global Configuration*) del switch con el comando **configure terminal** y configurar entradas estáticas a esta tabla con el comando:

```
Switch0(config)#mac address-table static <mac addr> vlan 1 interface <ifname>
```

Realice algunas pruebas y discuta en clase su aplicación.