Trabajo Práctico 3 - Redes de las Computadoras I

Valentino Privitera

19 de septiembre de 2024

1. Introducción

En este documento se realizará la practica de laboratorio número tres de la asignatura Redes de las Computadoras I. En esta ocasión vamos a comparar el comportamiento de una red LAN con un dispositivo Hub y un dispositivo Switch de por medio.

1.1. Conexiones a través de Hubs

La primer parte de este práctico de laboratorio consiste en enviar un PDU simple desde una computadora hacia una impresora en una sección de la empresa, y hacer lo mismo para otra sección de la misma empresa. Ambas secciones están unidas mediante un Hub satélite, y cada uno de estos esta centralizado a otro Hub también. Entramos en modo simulación, seleccionamos un PDU para la PC11 y su Printer1 y uno para la PC21 y su Printer2; en la pestaña *edit* agregamos un delay de 1 milisegundo (0.001 seg.) para el envío en cada computadora para intentar evitar problemas. Aun introduciendo un pequeño retraso entre el comienzo de cada comunicación, vemos que se producen una serie de colisiones dado que todo se encuentra en el mismo dominio.

El Hub al ser un repetidor eléctrico, se dedica a reenviar el PDU a todos los dispositivos de la red, independientemente de si son el destino del paquete o no; realiza esta acción hasta que da con el verdadero destinatario, lo que implica que este tipo de dispositivos no es tan eficiente debido al tiempo de envío, el excesivo uso de banda de la red y la limitada eficiencia a la hora de enviar paquetes en redes LAN.

1.2. Conexiones de Hub a través de Switch

Ahora vamos a cambiar de escenario, utilizando uno provisto por la cátedra, reemplazando el Hub por un dispositivo activo llamado Switch. Un **Switch** o conmutador es un dispositivo de red que conecta múltiples dispositivos dentro

de una red LAN y filtra y envía datos solo a los dispositivos de destino correspondientes, lo que mejora la eficiencia de la red en comparación con un hub. El Switch dispone de un número de puertos determinados en los que podemos conectar cableado de red tipo Ethernet y es a través de cada uno de estos que envía los paquetes. Además, se caracteriza porque admite comunicación Full Dúplex (enviar y recibir datos al mismo tiempo).

Después de realizar el envío de PDU, siguiendo los pasos del primer experimento, podemos apreciar como a la hora de enviar los paquetes, el Switch no permite que pasen los paquetes de un dominio de colisión al otro; de hecho, separa dominios de colisión. Podemos observar que la comunicación se lleva a cabo sin problemas. Además observamos que los PDU de un color no se propagan fuera del dominio de colisión, lo que verifica el hecho de que distingue cada dominio de colisión por color (osea dominios de Hubs).

Por ultimo, probamos a enviar un PDU desde la PC12 a la PC13 en el mismo dominio de colisión, con un atraso de 1ms también en cada equipo; efectivamente el Hub vuelve a reenviar a todos los dispositivos del dominio el mismo paquete, y PC13 lo recibe, devuelve la solicitud y el Hub vuelve a enviarlo a todos a la vez que llega la respuesta a PC12; lo bueno de todo esto es que el Switch no dejo pasar el paquete a la otra sección de la empresa, lo que evito que se cargue el trafico de red.

1.3. Conexión Estrella con un Switch

En la próxima experiencia, vamos a proceder a desconectar todos los dispositivos que antes teníamos divididos en secciones por un Hub, y vamos a conectar cada uno de ellos (computadoras, printers y servers) al Switch central, mediante un cable Copper Straight Through (no punteado). Se recomienda eliminar los Hub directamente y conectar cada dispositivo por individual (ir conectando por FastEthernet0 al puerto FastEthernet0/N del Switch, donde N es 1, 2, 3..).

Como mencionamos antes, un switch elimina el problema de las colisiones al crear un dominio de colisión separado por cada puerto que posee. Así se introduce el concepto de **puerto de colisión**, lo que significa que cada dispositivo conectado a un puerto del Switch tiene su propio dominio de colisión, por lo que dos dispositivos conectados a diferentes puertos pueden transmitir datos simultáneamente sin que se produzcan colisiones.

Una vez organizado el escenario, tendremos **ocho puertos de colisión**; procedemos a guardar la practica y la volvemos a abrir para evitar problemas. Pondremos Packet Tracer en modo simulación y procederemos a enviar los PDU nuevamente, pero esta vez con todos los dispositivos conectados al Switch, formando una estrella. Para nuestra sorpresa, el envío se realizo exitosamente, sin colisiones, y de manera precisa y rápida, asegurándose que el paquete solo se dirija a destino, y no a todos los dispositivos en la red.

2. Protocolo ARP

El protocolo **ARP** (Address Resolution Protocol) es un protocolo de red utilizado para mapear o traducir una dirección IP (que es una dirección lógica) en una dirección MAC (que es una dirección física o de hardware) dentro de una red local LAN. Este protocolo corresponde a las IPv4, las nuevas versiones IPv6 ya no lo admiten, sin embargo para nuestras practicas funciona perfecto.

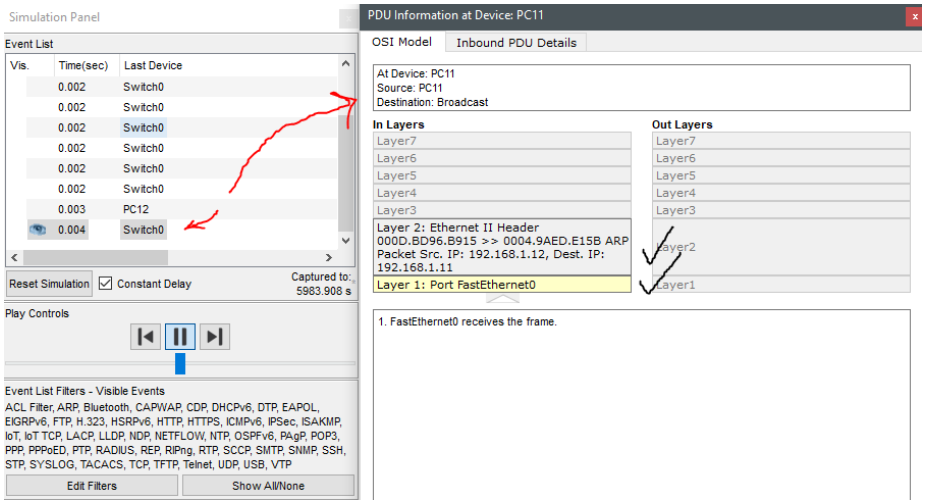
Gracias a este protocolo, los dispositivos pueden conocer la MAC de los demás dispositivos vecinos en la red LAN, solamente mediante el envío de paquetes. Mencionamos de paso que en el *Simulation Panel* se puede utilizar el filtrado de paquetes que puede ser de utilidad en practicas mas complejas. Para ello pulsamos el botón *Edit filters* y en la ventana emergente IPv4 seleccionamos los protocolos de interés; en nuestro caso, solo ARP.

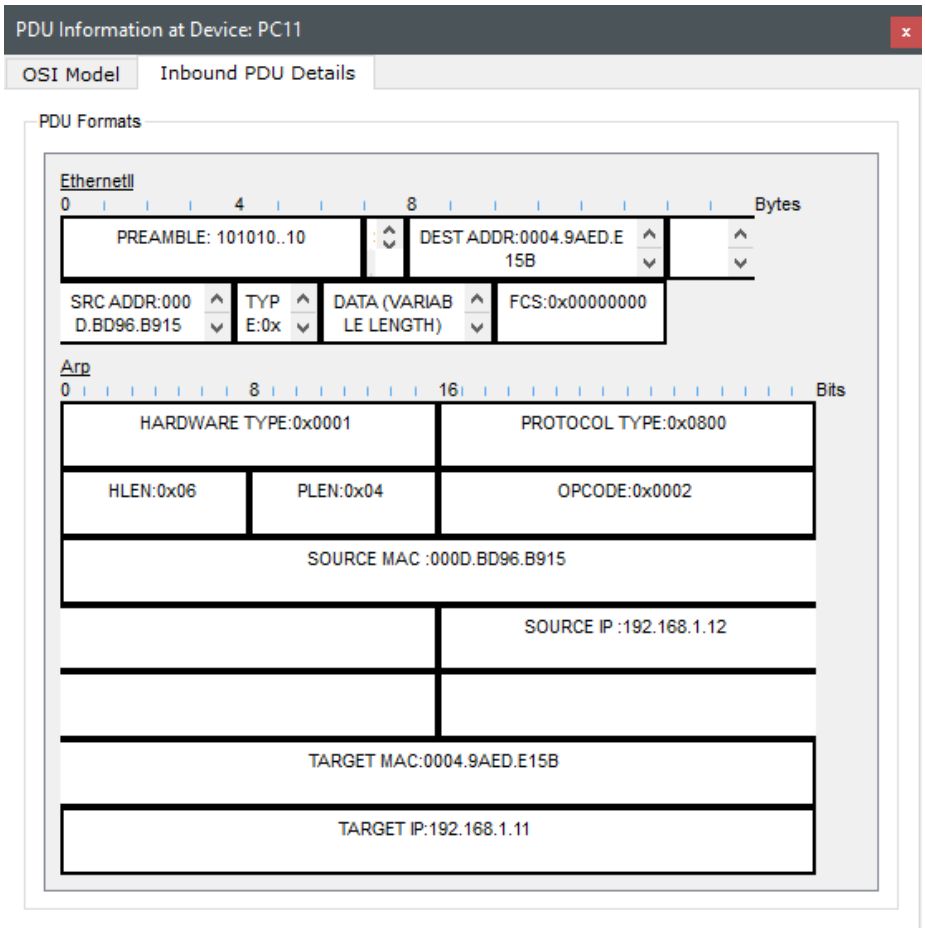
Vamos a proceder a realizar el envío de un paquete entre dos computadoras para comprobar esto. Nos ponemos en modo simulación, y en dicho modo realizamos un comando *ping -n 1 192.168.1.12* desde la consola de PC11 a PC12, enviando un solo PDU, asegurándonos que su cache ARP esta vacıa previamente.

Una vez realizado el envío por consola, vamos a darle al botón Play del modo Simulation para ver como, sin haber hecho ningún envío previamente, el Switch por primera y única vez, reenvía el paquete a **todos** los dispositivos de la red local, sin importar si son los destinatarios o no; esto quiere decir que, mientras no haya conocido la MAC de sus vecinos, todavía no sabe como filtrar el envío. Sin embargo, una vez conoce a todos los dispositivos, el envío se hace efectivo y preciso, solo a su destinatario, sin congestionar la red. Además, ahora en la memoria cache del Switch, este posee una tabla con las MAC de todos sus dispositivos vecinos:

Dispositivos	MAC
PC11	0004.9AED.E15B
PC12	000D.BD96.B915
PC13	0010.114D.79D9
PC21	0001.96DA.9132
Printer1	0001.6394.A11E
Printer2	00D0.FFED.0B5A
Server1	00E0.F9A9.3157
Server2	0000.0C11.2106

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 maquinas 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**:


Simulation Panel
Event List
Vis.
Time(sec)
Last Device
0.002 Switch0
0.002 Switch0
0.002 Switch0
0.002 Switch0
0.002 Switch0
0.002 Switch0
0.003 PC12
0.004 Switch0
Reset Simulation
Constant Delay
Captured to:
5983.908 s
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, Bluetooth, CAPWAP, CDP, DHCPv6, DTP, EAPOL, EIGRPv6, FTP, H.323, HSRPv6, HTTP, HTTPS, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
PDU Information at Device: PC11
OSI Model
Inbound PDU Details
At Device: PC11
Source: PC11
Destination: Broadcast
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header 000D.BD96.B915 >> 0004.9AED.E15B ARP Packet Src. IP: 192.168.1.12, Dest. IP: 192.168.1.11
Layer2
Layer 1: Port FastEthernet0
Layer1
1. FastEthernet0 receives the frame.


PDU Information at Device: PC11
OSI Model
Inbound PDU Details
PDU Formats
EthernetII
0
4
8
Bytes
PREAMBLE: 101010..10
DEST ADDR:0004.9AED.E15B
SRC ADDR:000D.BD96.B915
TYPE:0x
DATA (VARIABLE LENGTH)
FCS:0x00000000
Arp
0
8
16
Bits
HARDWARE TYPE:0x0001
PROTOCOL TYPE:0x0800
HLEN:0x06
PLEN:0x04
OPCODE:0x0002
SOURCE MAC :000D.BD96.B915
SOURCE IP :192.168.1.12
TARGET MAC:0004.9AED.E15B
TARGET IP:192.168.1.11

Lo que sucede a nivel técnico es que ARP solicita mediante un broadcast a todos los hosts (dispositivos) de la LAN que le informen cual es la MAC de 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. Este proceso que realiza el Switch se conoce como **Dominio de Difusión**, y solo hay uno por Switch.

- **Pequeño detalle**: en las fotos podemos ver que el HARDWARE TYPE es 0x0001, sin embargo esto esta mal; el profesor quiso indicar que era Ethernet el tipo de hardware, y este es 0x001. Además, los **inlayer** indican por donde entro el paquete, y los **outlayer** hacia donde va dirigido.

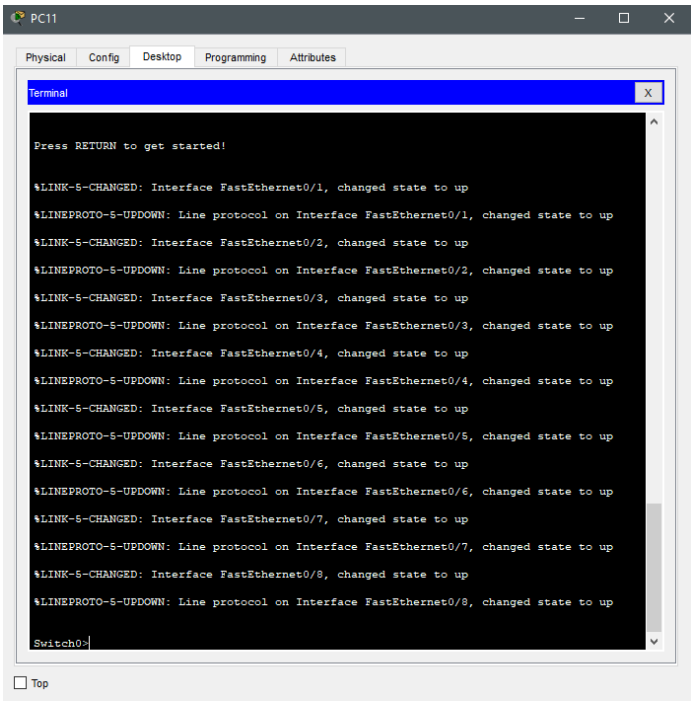
3. Switch learning

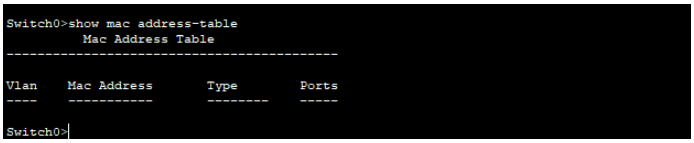
A través de las diferentes simulaciones llevadas a cabo en esta practica es evidente que el Switch sufre alguna transformación interna adquiriendo conocimiento de la red a medida que fluyen los paquetes ARP (learning). Esto se almacena en una tabla llamada FIB. Luego mediante esta tabla el switch toma decisiones de reenvıo inteligente mejorando la performance de la red (forwarding).

La tabla **FIB** (Forwarding Information Base), también conocida como tabla de reenvío o tabla de encaminamiento, es una estructura de datos utilizada por Routers y Switches para tomar decisiones rápidas sobre cómo reenviar los paquetes de datos a través de una red. Es una tabla dinámica que asigna direcciones MAC a puertos y esta diseñada específicamente para ser utilizada durante el proceso de reenvío de paquetes. Almacena la información necesaria para reenviar los paquetes lo más rápidamente posible.

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, caracterıstica en general propias de los **Switch administrables**.

El Switch utilizado en laboratorio es administrable y permite esta característica; este puede configurarse de dos maneras: mediante el uso de la opción **CLI (Command Line Interface)** de las propiedades del Switch (consola blanca dentro del Switch); o colocando un cable de consola (cable azul) entre el Host (como PC11) y el Switch0, haciendo que la PC maneje la configuración del Switch desde la aplicación *PC11 - Desktop - Terminal*, accediendo con los en parámetros default.





Vamos a empezar la experiencia seleccionando el cable Console (azul) y conectando la PC11 al Switch0; a partir de allı tendremos acceso a **Cisco IOS**, que es uno de los sistemas operativos de redes Cisco para sus equipos. Desde la PC11, 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 vacıa, pero basta con ejecutar un ping entre algunas PCs, por ejemplo PC11 y PC12 para ver como la tabla se empieza a llenar con las MAC addresses de las PC que pasaron por sus puertos, e incluso indica por que numero de puerto pasó cada MAC (PC11 por Fa0/1 o PC12 por Fa0/2 por ejemplo).

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>
```