PRÁCTICA 4

Planificación y Administración de Redes. Switch, Hub.

César Pérez Molaguero

Contenido

TABLA DE ILUSTRACIONES

Planificación y Administración de Redes. *Switch, HUB.*

Curso: 2018-19

Administración de Sistemas Informáticos en Red

EJERCICIOS

EJERCICIO 1

Pide un HUB a tu profesor y envía a un compañero un fichero de tamaño considerable. Calcula la velocidad de transmisión y compárala con la velocidad de transmisión real. Realiza el mismo proceso con un SWITCH que tu profesor te proporcione y compara los resultados. ¿Qué conclusiones extraes?

Primero crearemos una carpeta compartida, donde vamos a enviar un fichero, en este caso una ISO de Ubuntu Server que ocupa 1.86GB.

- Velocidad real de transmisión en un HUB.

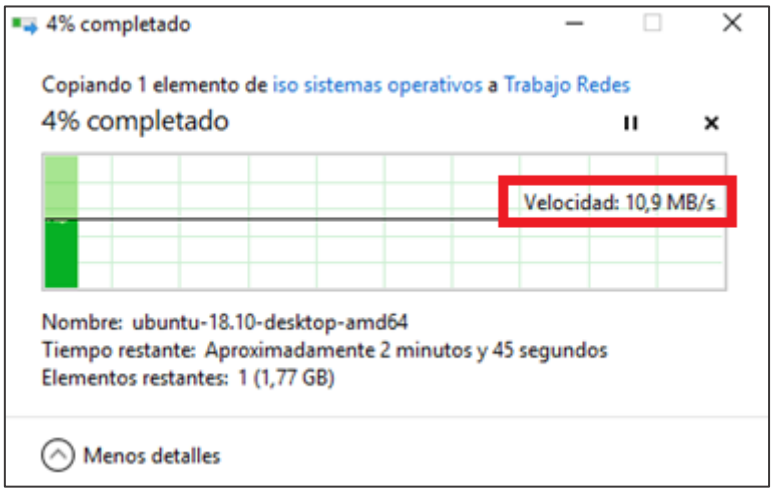

Ilustración 1. Velocidad real de transmisión(HUB)

- Velocidad teórica de transmisión en un HUB es de 10/100 Mbps, porque es Ethernet.

- Velocidad real de transmisión en un SWITCH:

  Un fichero de 2818MB ha tardado unos 35 segundos en llegar de una máquina a otra por lo que la velocidad media es de 80.5Mbps.

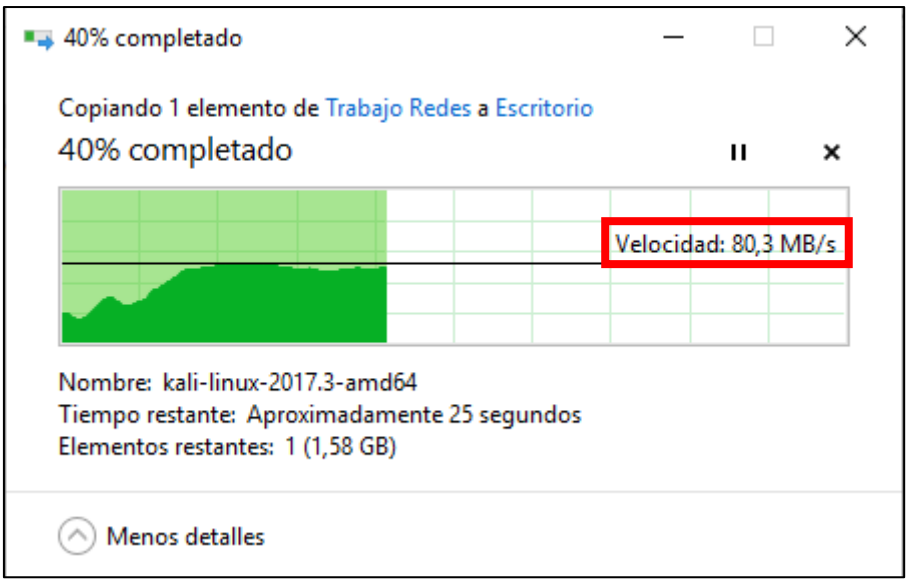

Ilustración 2. Velocidad real de transmisión en un SWITCH

- Velocidad teórica de transmisión en un SWITCH es de 10/100 Mbps y puede llegar hasta 1000 Mbps mediante un adaptador, porque es Fast-Ethernet.

La conclusión que sacamos es que la velocidad del Switch es considerablemente más alta que la del HUB, la velocidad real del Switch asciende a unos 80 Mbps mientras que el HUB se quedaba en 10 Mbps.

EJERCICIO 2

Comprueba que realmente es cierto que el HUB envía toda la información por todas sus bocas excepto por aquella por donde le llega. Utiliza el HUB proporcionado por tu profesor para realizar las pruebas necesarias que ratifiquen la afirmación anterior, documentado y explicando las pruebas que has realizado.

La prueba que hemos realizado es un ping desde la máquina con la dirección ip 169.254.216.108 a la 169.254.223.222 y hemos analizado con un analizador de tráfico de red , en este caso Wireshark, desde la máquina con la tercera IP (169.254.147.222) y como se ve en la imagen hemos podido ver esos paquetes de tipo ICMP.

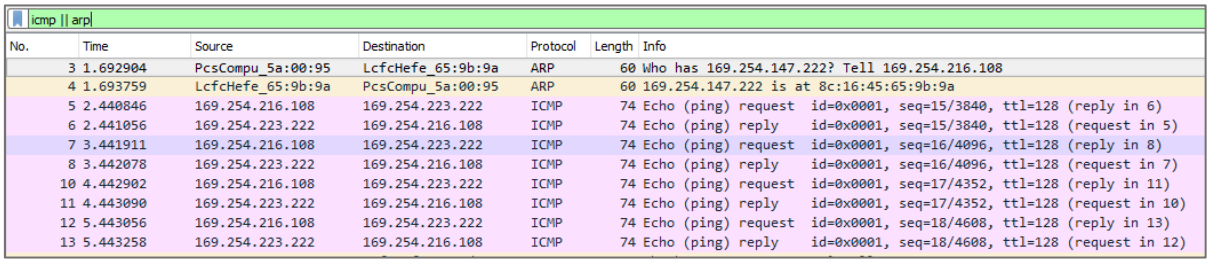

Ilustración 3. Prueba, HUB envía información a todas sus bocas.

EJERCICIO 3

Una herramienta para hacer que un SWITCH tenga el mismo comportamiento que un HUB es desbordar la tabla CAM del SW. Para ello existen herramientas que generan tramas de manera aleatoria para conseguir desbordar la tabla CAM del SW. Una herramienta muy conocida para ello es macof: https://kalilinuxtutorials.com/macof/

Se pide:

-Explica con tus palabras que es lo que realiza esta herramienta.

Esta herramienta lo que hace es generar tramas de manera aleatoria con direcciones IP y MAC totalmente aleatorias para así desbordar la tabla CAM del Switch y de esta manera hacer que este funcione como un HUB.

-Documenta todos los parámetros de esta herramienta y explica para qué vale cada uno de ellos.

```
macof [-i interface] [-s src] [-d dst] [-e tha] [-x sport] [-y dport] [-n times]
```

Simplemente con poner macof este empezará a generar tramas, pero además podemos aplicarle una serie de parámetros:

-i interface: Podemos especificar la interfaz que queremos atacar.
-s src: Especificar la dirección IP de origen.
-d dst: Especificar la dirección IP de destino.
-e tha: Especificar la dirección hardware de destino.
-x sport: Puerto TCP de origen.
-y dport: Puerto TCP de destino.
-n times: Número de tramas que genera.

-Explica con tus palabras la diferencia entre "inundación simple" e "inundación diferida" y pon un ejemplo de las mismas.

La inundación simple consiste en generar tramas de manera aleatoria para desbordar la tabla CAM del Switch, así el Switch empezará a funcionar como un HUB y veremos todo el tráfico de red. La inundación dirigida es un proceso similar en el dirigimos el ataque hacia la interfaz de red que queramos.

-Comenta alguna contramedida para evitar la inundación de la tabla CAM de un SW.

- Seguridad del puerto : limita el número de direcciones MAC que se conectan a un solo puerto en el Switch.
- Filtrado de MAC : limita el número de direcciones MAC en cierta medida.
- Implementación de 802.1X : permite las reglas de filtrado de paquetes emitidas por un servidor AAA centralizado basado en el aprendizaje dinámico de los clientes.

-Realiza un ataque con macof a un SW proporcionado por tu profesor y averigua si el SW para a comportarse como un HUB.

Para realizar este ataque hemos montado el siguiente entorno:

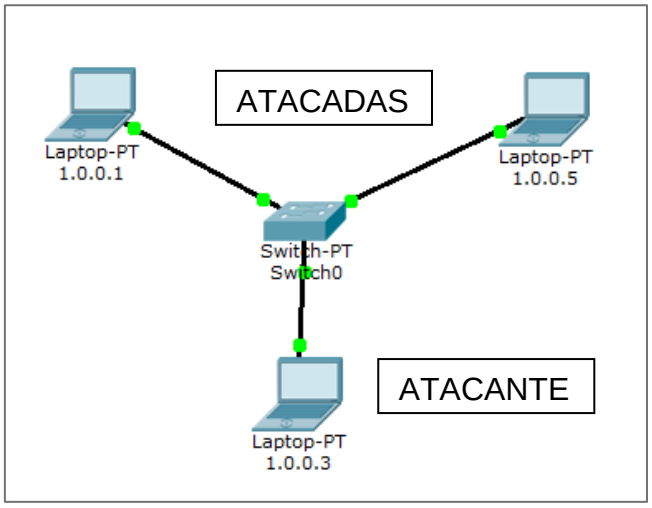

Ilustración 4. Diagrama de red

IMPORTANTE: Primero debemos lanzar macof antes de que las máquinas que van a ser atacadas se conecten al SW, de esta manera conseguiremos que la tabla CAM del SW se desborde y a la hora de que las máquinas que van a ser atacadas se conecten al SW este no podrá cachear sus direcciones MAC, porque si lanzamos el ataque con las máquinas conectadas sus direcciones MAC serán cacheadas por el SW y el ataque fracasará.

Una vez lanzado macof conectaremos las máquinas al SW y haremos continuos pings entre las dos máquinas mediante el comando ping direccionIP -t.

Después desde la máquina atacante abriremos Wireshark y aplicaremos el filtro ICMP, de esta manera veremos los paquetes que se están mandando las dos máquinas atacadas.