SWITCH, HUB.

Gonzalo Tudela Chavero

Práctica 4

ÍNDICE DE CONTENIDOS

EJERCICIO 1 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? 1

Pruebas Ejercicio 1: 3

a. Transferencia HALF-DUPLEX: 4

b. Transferencia FULL-DUPLEX: 5

EJERCICIO 2 8

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. 8

EJERCICIO 3 9

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/ 9

a. Explica con tus palabras que es lo que realiza esta herramienta 9

b. Documenta todos los parámetros de esta herramienta y explica para qué vale cada uno de ellos. 9

c. Explica con tus palabras la diferencia entre “inundación simple” e “inundación diferida” y pon un ejemplo de estas. 9

d. Comenta alguna contramedida para evitar la inundación de la tabla CAM de un SW. 10

e. Realiza un ataque con macof a un SW proporcionado por tu profesor y averigua si el SW pasa a comportarse como un HUB. 10

ÍNDICE DE FIGURAS

Figura 1. Switch Dlink DES-1005D versión hardware L2. 1
Figura 2 . Cable Cat.5E amarillo. 2
Figura 3. Cable Cat.5E gris. 2
Figura 4. Equipos utilizados para las pruebas. 3
Figura 5. T480 copiando una ISO localizada en TJ66 a su disco local. 4
Figura 6. Velocidad mostrada en prueba Full-Duplex, T480 5
Figura 7. Velocidad mostrada en prueba Full-Duplex, TJ66. 5

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?

Material para las pruebas con SWITCH:

Para la realización de las pruebas con SWITCH he utilizado los siguientes componentes:

Switch Dlink modelo DES-1005D, pulsar aquí para ver lista completa de las características.

Figura 1. Switch Dlink DES-1005D versión hardware L2.

Características mas interesantes para el ámbito de esta práctica:

- Cinco puertos 10/100Mbps Fast Ethernet.
- Funcionamiento Full/half-duplex para velocidades Ethernet/Fast Ethernet.
- Velocidad Ethernet: 10/20Mbps para half o full dúplex respectivamente.

- Velocidad Fast Ethernet: 100/200 Mbps para half o full dúplex respectivamente.
- Tabla CAM de 2k (2000) entradas.

2 cables UTP cat.5e (enhanced) capaces de hasta 1Gbps.

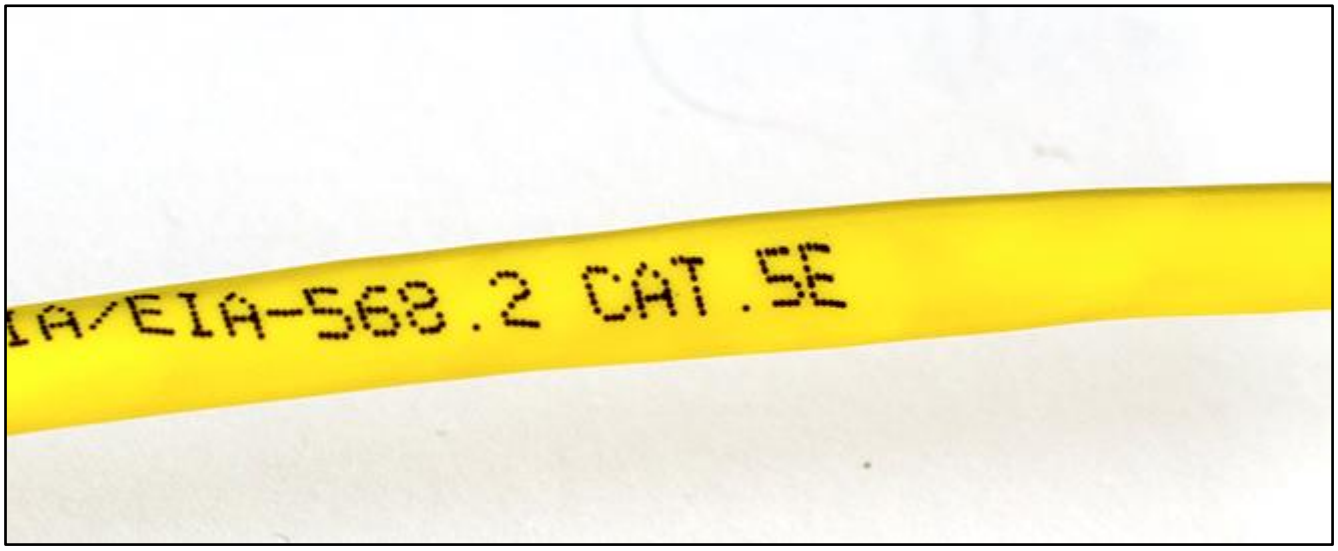

Figura 2 . Cable Cat.5E amarillo.

Figura 3. Cable Cat.5E gris.

2 portátiles con capacidad suficiente para no suponer cuello de botella durante las transferencias.

Figura 4. Equipos utilizados para las pruebas.

El equipo de color blanco es llamado en las pruebas TJ66 por su nombre de modelo EasyNote TJ66, a su vez el equipo de color negro es llamado en las pruebas T480 por su nombre de modelo ThinkPad T480.

Pruebas con SWITCH:

El Switch tiene una velocidad máxima teórica 100Mbps (conexiones Fast Ethernet), en esta prueba estamos utilizando equipos con bocas Gigabit ethernet y cables cat.5Enhanced, por lo que el medio y las tarjetas son capaces de hasta 1Gigabit/s, así que el Switch deberá funcionar a pleno rendimiento iluminando los testigos de las bocas como Fast Ethernet (verde) y ofreciendo una velocidad teórica half-duplex de 100Mbit por segundo o Full-dúplex de 200Mbit por segundo.

a. Transferencia HALF-DUPLEX:

Para realizar esta prueba utilizando el T480 traemos un archivo ISO de 4Gb a una carpeta local y se observa la velocidad durante la copia.

- Velocidad máxima teórica: 100 megabit/s o 12,5 megabytes/s.
- Velocidad media mostrada durante la copia: 11,4 megabytes/s o 91,2 megabits/s.

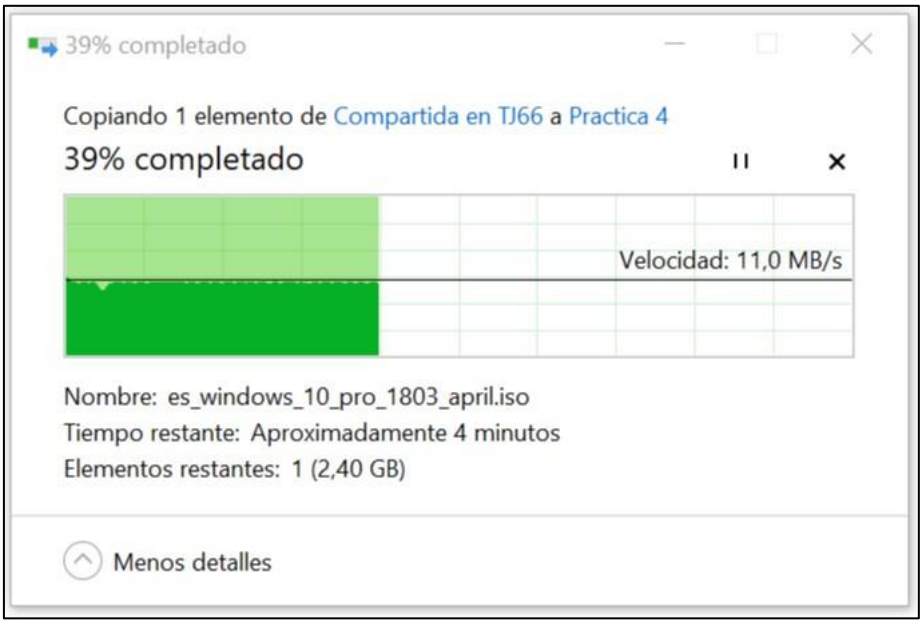

Figura 5. T480 accede a TJ66 y copia a su disco local.

b. Transferencia FULL-DUPLEX:

Para esta prueba se realizan las solicitudes desde ambas maquinas recogiendo una ISO en las carpetas compartidas y copiándola al escritorio local, resultando en 2 máquinas solicitando comunicación simultánea a través de la red en direcciones opuestas, lo que crea tráfico full dúplex.

- Velocidad máxima teórica: 200 megabits/s o 25 Megabytes/s.
- Velocidad media mostrada durante la copia: 187,2 megabits/s o 23,4 megabytes/s

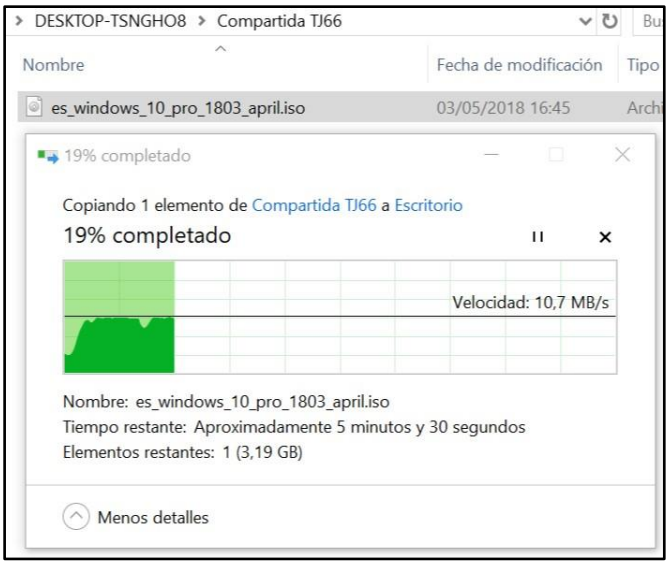

Figura 6. T480 lee datos de TJ66 y copia a su disco local.

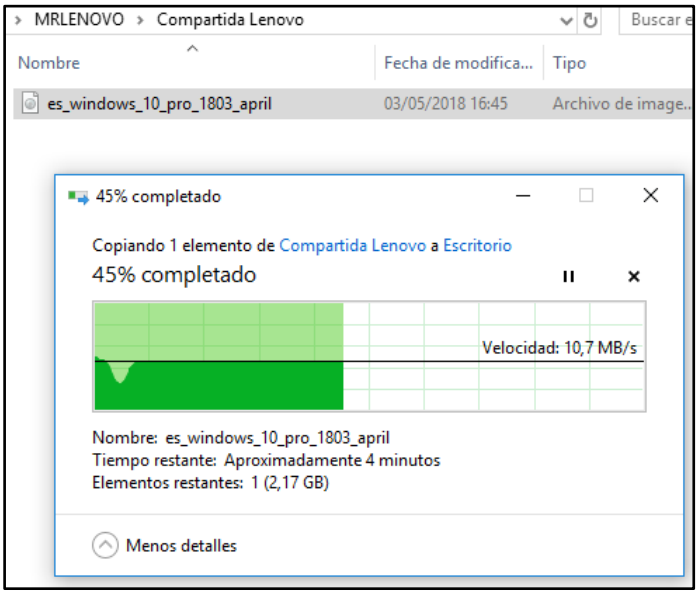

Figura 7. TJ66 lee datos de T480 y copia a su disco local.

Pruebas con HUB (grupo en clase):

a. Transferencia HALF-DUPLEX:

La prueba con HUB se realizo escribiendo datos en la carpeta compartida de otro equipo conectado al mismo, pudiéndose observar la velocidad alcanzada en la siguiente figura.

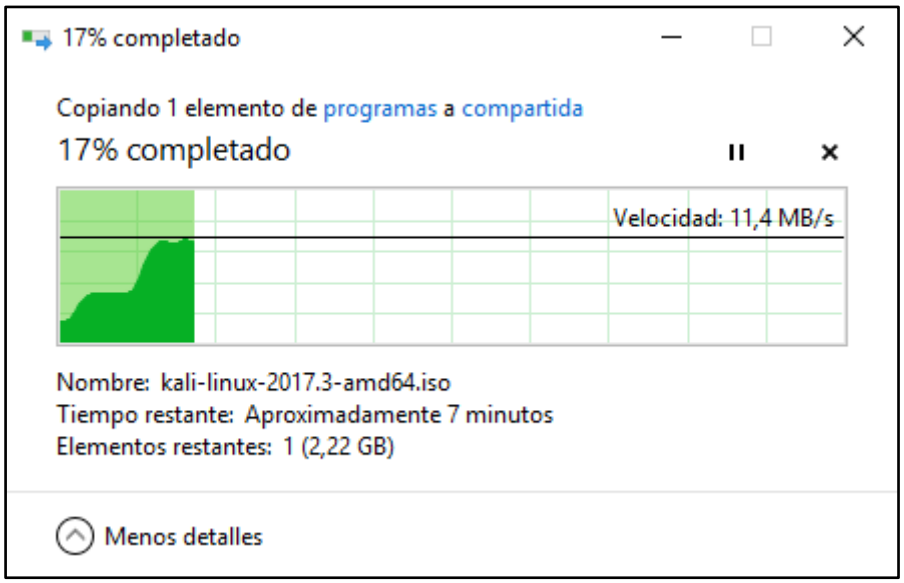

Figura 8. Enviando datos a través de un HUB 10/100.

La velocidad media alcanzada fueron 11,4 Megabytes por segundo o 91,2 Megabits por segundo lo que coincide exactamente con las pruebas realizadas por mí con el Switch.

Conclusiones sobre la comparativa HUB y SWITCH:

Para el HUB no se realizaron pruebas de transferencias Full-Duplex, por lo que no se ha podido realizar una comparativa en ambos casos (full y half) para el Switch y Hub, sin embargo, la velocidad de transferencia en comunicaciones half-dúplex es exactamente la misma, por lo que puedo concluir que:

- La velocidad teórica no es alcanzada en ninguno de los casos, existe un déficit de aproximadamente 1Megabyte/s según lo indicado por el fabricante, tanto para el HUB como el SWITCH.
- Las transmisiones full-dúplex se consiguen cuando las solicitudes de transmisión provienen de máquinas distintas y los datos han de pasar por el Switch.

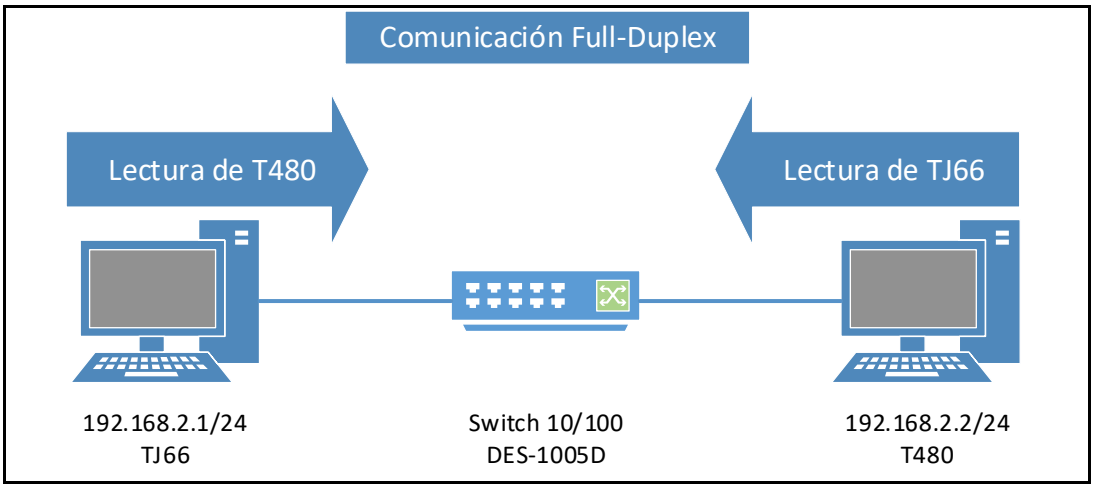

Figura 9. Esquema Full-Duplex.

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.

Ya que no dispongo de un HUB para realizar esta comprobación describiré los pasos necesarios a seguir para comprobar que este dispositivo envía por todas las bocas los paquetes que le llegan, actuando a modo concentrador.

Se debe establecer una red de como mínimo 3 equipos para realizar la comprobación fácilmente, o en su defecto 2 equipos con uno de ellos haciendo funcionar una maquina virtual que actuará de tercer equipo.

Para mayor brevedad en la explicación supondremos que son 3 equipos físicos diferentes:

Dados 3 equipos A, B y C que están en la misma red, por ejemplo (192.168.2.0/24) y siendo sus direcciones IP 192.168.2.1, 192.168.2.2 y 192.168.2.3 respectivamente, se deberá:

1. Establecer conexión entre 2 de ellos, por ejemplo, A y B mediante el envío de paquetes ICMP utilizando el comando siguiente desde una ventana CMD en del equipo A, `ping 192.168.2.2 -t`, lo que permitirá que los paquetes se envíen constantemente hasta que se presione la combinación de teclas `Control+C`.
2. Mientras el equipo A y B están generando tráfico a través del HUB, el equipo C deberá ejecutar Wireshark para escuchar el trafico que hay en la red, si se prefiere, estableciendo un filtro ICMP para ver este tipo de paquetes únicamente.

Si lo anterior está siendo realizado utilizando un HUB para conectar estos equipos el equipo C mostrará en Wireshark solicitudes ICMP enviadas desde el equipo A con destino equipo B.

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/

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

Esta herramienta genera paquetes aleatorios para sobrepasar la capacidad de la tabla CAM del Switch con la esperanza de que este no tenga ningún método de protección ante este evento y pase a actuar como un HUB para salvaguardar la comunicación enviando todos los paquetes por todas las bocas, permitiendo que un atacante pueda escuchar todos los paquetes son transmitidos a través del Switch.

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

- Parámetro -i: Este parámetro determina la interfaz de red por la que se enviaran los paquetes.
- Parámetro -s: Sirve para especificar la dirección IP origen del paquete.
- Parámetro -d: Sirve para especificar la dirección IP destino del paquete.
- Parámetro -e: Sirve para especificar la dirección de hardware del objetivo.
- Parámetro -x: Sirve para especificar el puerto de origen TCP del paquete.
- Parámetro -y: Sirve para especificar el puesto de destino TCP del paquete.
- Parámetro -n: Sirve para especificar el numero de paquetes a enviar.

c. Explica con tus palabras la diferencia entre “inundación simple” e “inundación diferida” y pon un ejemplo de estas.

Entiendo 3 tipos de Inundación mediante la herramienta `macof`:

- Inundación simple: Utilizando el comando sin ningún origen o destino especificado en los parámetros -d o -s.
- Inundación dirigida: Utilizando el comando definiendo un origen o destino ya sea con el parámetro -d o -s.
- Inundación diferida: Algunos switch pueden requerir que el envió de los paquetes sea a intervalos por lo que deberíamos utilizar `macof` de la siguiente forma, `# while [1] ; do macof -d 192.168.1.1 -n 100000 ; sleep 50 ; done`

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

Establecer un límite de direcciones MAC que pueden estar relacionadas con una boca de red.

Establecer una lista de direcciones MAC que están autorizadas en el Switch.

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

Configuración del entorno de pruebas:

Configuro 3 máquinas conectadas al Switch con sendas carpetas compartidas para poder mover archivos entre ellas.

- TJ66 tiene asignada la IP 192.168.2.1
- T480 tiene asignada la IP 192.168.2.3
- VM Kali Linux en T480 tiene asignada la IP 192.168.2.6
- QX9600 tiene asignada la IP 192.168.2.2

Prueba 1:

La máquina de escritorio QX9600 está realizando peticiones ICMP tipo 8 a la máquina virtual Kali.

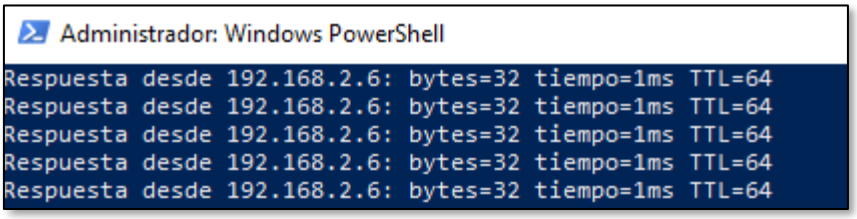

Figura 10. QX9600 (192.168.2.2) enviando ICMP tipo 8 a la VM Kali (192.168.2.6).

TJ66 tiene lanzado un Wireshark a la escucha en el puerto ethernet, el filtro ICMP ha sido establecido.

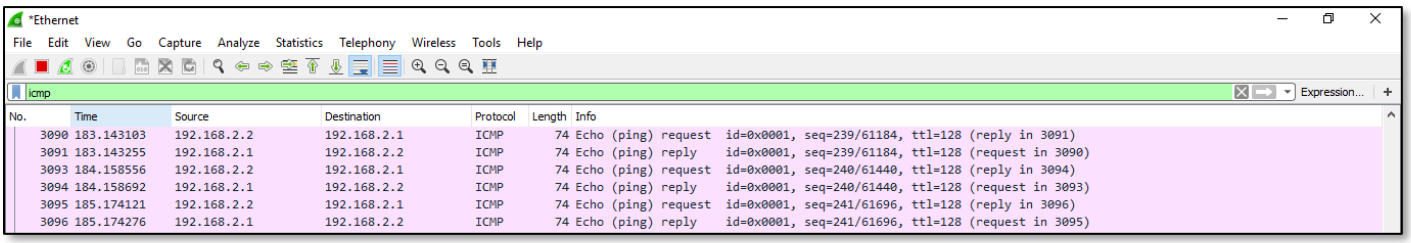

Figura 11. Wireshark en TJ66 (192.168.2.1) escuchando ICMP.

Desde la máquina virtual Kali (192.168.2.6) ejecuto `macof` con el siguiente comando:

```
Macof -s 192.168.2.7 -d 192.168.2.9 -i eth0 -n 30000
```

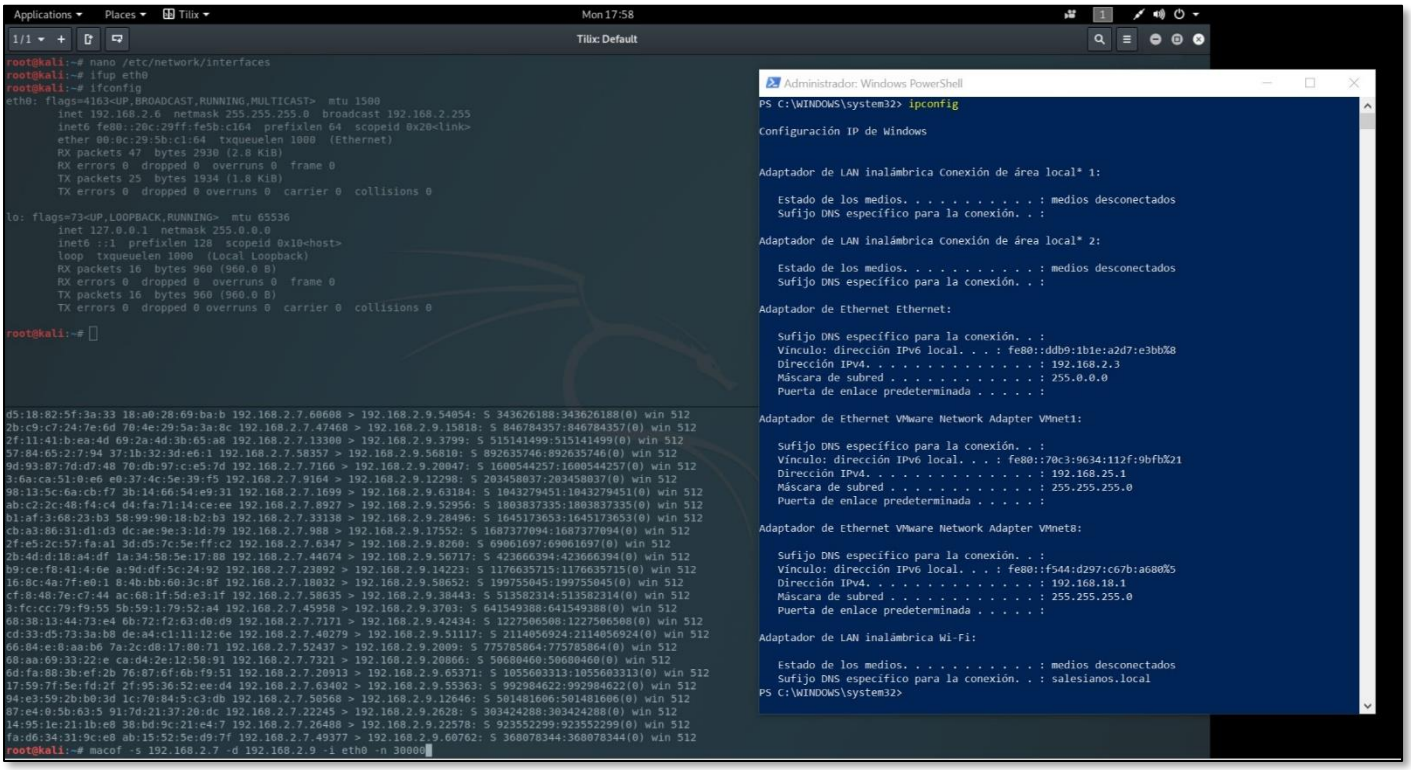

Figura 12. Maquina Kali 192.168.2.6 ejecutando `macof`, la IP del host 192.168.2.3 se muestra en la ventana Powershell.

Los parámetros indican a `macof` que genere 30.000 paquetes cuya IP de origen sea 192.168.2.7 y destino 192.168.2.9 (siendo sus MAC aleatorias) a través de la interfaz eth0.

Resultados:

Wireshark en TJ66 (192.168.2.1) recibe una solicitud ICMP tipo 8 (request) cuyo destino era 192.168.2.6 por lo que en ese momento el Switch ha enviado las peticiones ICMP (8) de la maquina QX9600 (192.168.2.2) a todas las bocas de conexión.

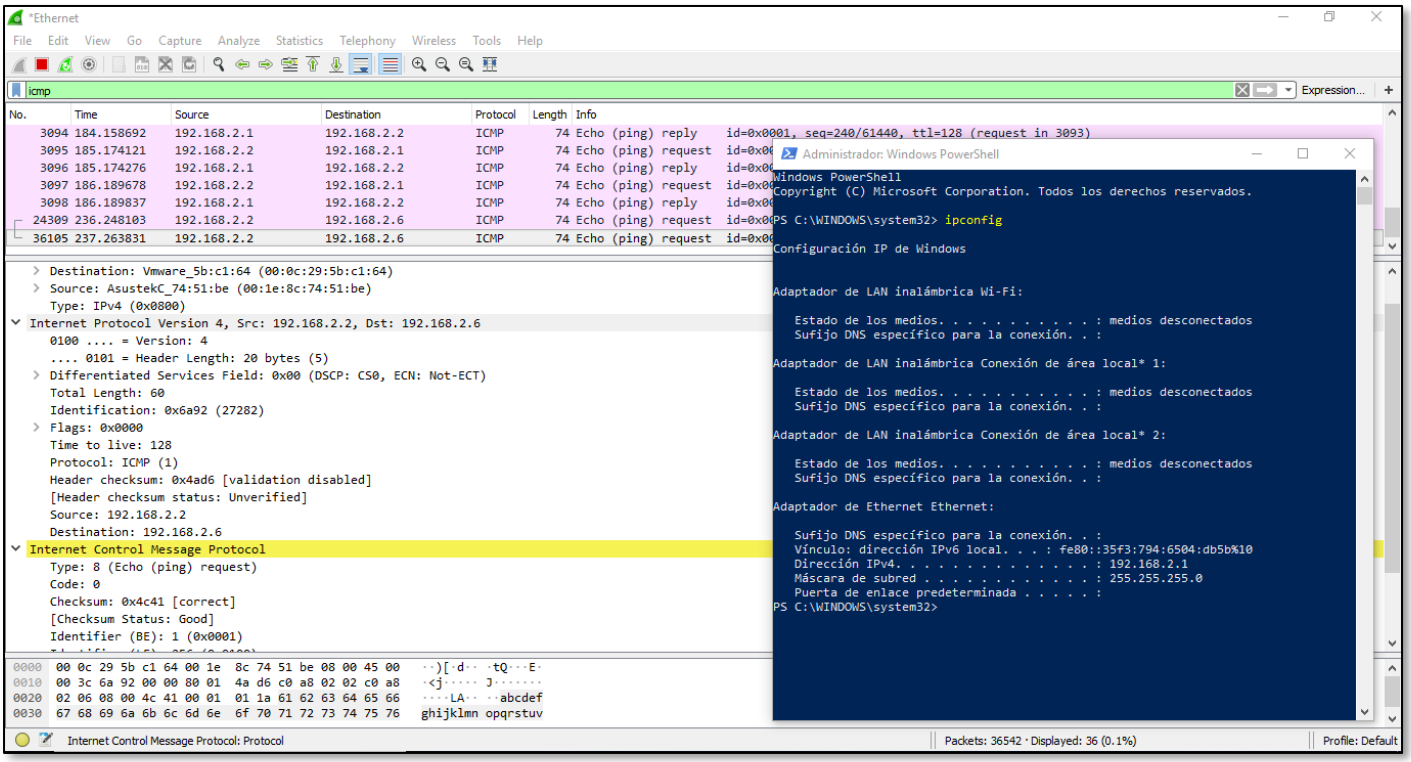

Figura 13. Wireshark en (192.168.2.1) recibe un paquete ICMP destinado a (192.168.2.6)

VIDEO EXPLICATIVO

El video ha sido creado grabando cada escritorio de la maquina involucrada y posteriormente montando las partes en un solo video para alojarlo en Youtube, puede accederse a él haciendo click en el siguiente enlace.

https://youtu.be/u9MSPz8qpog

Observaciones:

Ya que la prueba sobre el ataque con `macof` al Switch fue grabada en una fecha distinta de la prueba escrita una de las maquinas (QX9600) no pudo ser utilizada y fue sustituida por otra (4770K) esto no afecta al resultado, pero si cambian los nombres y las IP asignadas pudiéndose comprobar la nueva relación de nombres e IP en la siguiente lista:

TJ66 – 192.168.2.1/24

T480 – 192.168.2.2/24

4770K – 192.168.2.3/24

4770K (máquina virtual Kali) – 192.168.2.4/24

Conclusiones:

Tras esta nueva prueba se pueden extraer las siguientes conclusiones:

- El SWITCH no elimina de su tabla CAM entradas que tienen abiertas una comunicación ya que para el éxito del ataque fue necesario saturar la tabla CAM del Switch únicamente con la maquina atacante conectada al mismo, para posteriormente conectar los 2 equipos que iban a realizar la comunicación, en este caso envío de paquetes ICMP.
- Este SWITCH elimina las entradas en su tabla CAM con relativa rapidez, ya que tan pronto como cesa la inundación los paquetes ICMP entre las maquinas TJ66 y T480 dejan de recibirse en el Wireshark de 4770K.
- Un SWITCH para hogar como el utilizado es perfectamente capaz de soportar un spam como el que produce `macof` y seguir funcionando correctamente sin apenas afectar al trafico ya existente manteniendo tasas de transferencias perfectamente aceptables.
- Este tipo de ataques son limitados y hoy en día los dispositivos tienen suficiente capacidad y medidas que pueden evitar este abuso en un SWITCH.
- Cuando el SWITCH está saturado, las tablas ARP de los equipos conectados al mismo se llenan de direcciones basura y en algunos casos no es posible eliminarla con el comando `arp -d *` y se hace necesario el comando `netsh interface ip delete arpcache`.
- Los HUB son dispositivos que han desaparecido casi en su totalidad, es muy difícil adquirir uno puesto que han sido sustituidos por los SWITCH.
- Las tasas de transferencias se ven mermadas entre otras causas porque los paquetes en si mismos no son solamente datos que el usuario desea transferir, también transportan información inherente a la comunicación (corrección de errores, destino, origen…etc.).
- La configuración de las interfaces de red y el entorno es mucho más clara y concisa en el entorno Kali Linux que en Windows 10, se investigaron comandos para cambio de ip en Powershell y son bastante mas extensos y complejos que en Kali, por ejemplo:

```
New-NetIPAddress -InterfaceAlias 'Ethernet' -IPv4Address '192.168.2.3' -
PrefixLength 24
```