Universidad Autónoma Metropolitana

Unidad Azcapotzalco

Práctica 2: Captura y análisis de tráfico en una LAN

ASIGNATURA

Diseño y Administración de Redes de Computadoras

PRESENTA

Luis Ángel Cruz Díaz - 2183038433
Diego Alexis Moreno Valero - 2243900185

PROFESOR

José Alfredo Estrada Soto

11 de noviembre de 2024

1. Introducción

2. Objetivos

- Emplear la herramienta **Wireshark** para realizar capturas y análisis de tráfico en una LAN.
- Analizar el comportamiento de los mandatos **ping** en una comunicación vía red.

3. Marco Teórico

Ejemplo de cita (Buffett, 1984).

4. Desarrollo del Trabajo

Para esta práctica se requiere del uso de dos PC's (las denominaremos como PC1 y PC2), ambos equipos conectados por enlace directo y con IP's estáticas.

4.1. Tarea 1.

Paso 1. Realice una tabla que contenga el nombre de cada equipo, su IP y su MAC.

Para comenzar, en la PC1 se inició con el sistema operativo **Windows** y se realizó el cambio de la dirección IP a `192.168.0.14` con la puerta de enlace `192.168.0.1`. Como se muestra en la Figura 1.

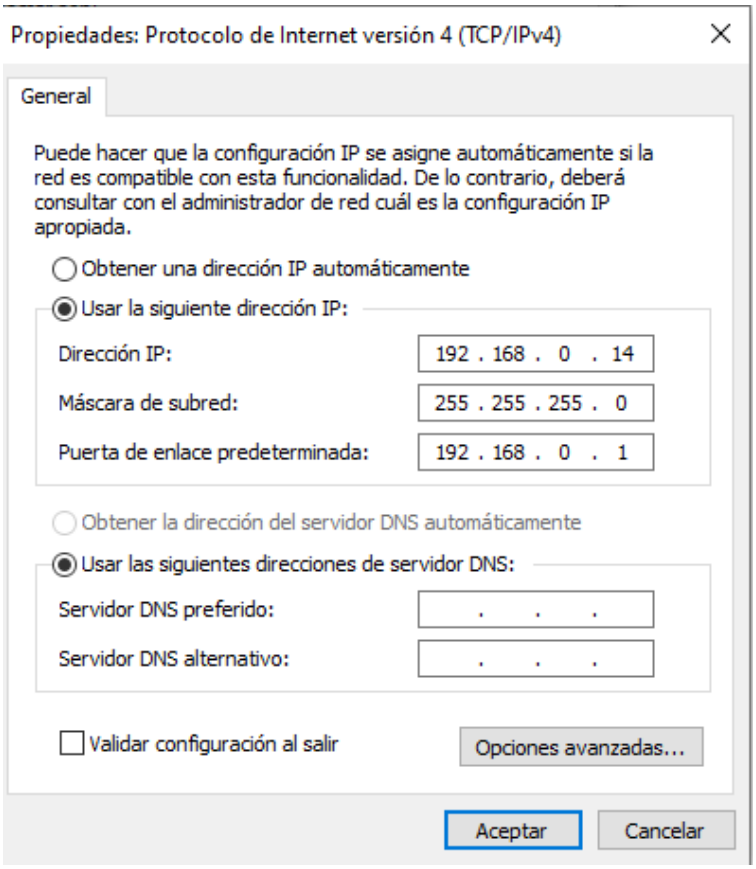

Figura 1: Configuración de la Dirección IP en Windows

Para obtener la dirección MAC de un equipo en Windows abrimos la terminal y ejecutamos el comando `ipconfig -all` y se mostrará la dirección MAC como se muestra en la Figura 2. La dirección MAC que se obtuvo de la PC1 fue `64:00:6A:44:B6:0A`.

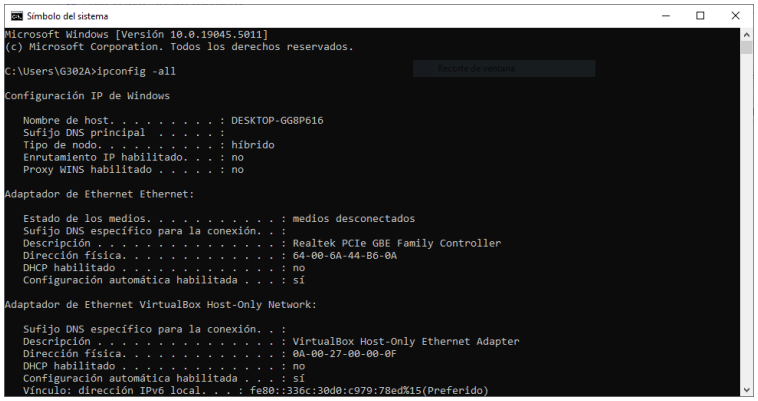

Figura 2: Obtención de la Dirección MAC en Windows

En la PC2 se inició con el sistema operativo **Linux** y se realizó el cambio de la dirección IP a `192.168.0.13` con la puerta de enlace `192.168.0.1`. Como se muestra en la Figura 3.

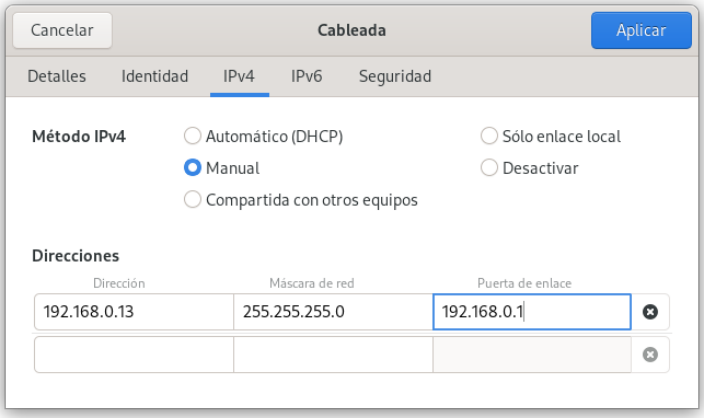

Figura 3: Configuración de la Dirección IP en Linux

Para obtener la dirección MAC en la PC2 con Linux nos dirigimos a configuración de red y seleccionamos la interfaz de red deseada, en este caso **Ethernet** y se mostrará la dirección MAC como se muestra en la Figura 4. La dirección MAC que se obtuvo de la PC2 fue `64:00:6A:44:A5:DF`.

Figura 4: Obtención de la Dirección MAC en Linux

Los datos obtenidos de ambas PC's se muestran en el Cuadro 1.

Integrante	Equipo	IP	MAC
Diego Alexis Moreno Valero	PC1	192.168.0.14	64:00:6A:44:B6:0A
Luis Ángel Cruz Díaz	PC2	192.168.0.13	64:00:6A:44:A5:DF

Cuadro 1: Tabla de Equipos

4.2. Tarea 2.

Paso 1. Tabla ARP.

a. **Borre el contenido de la tabla ARP.**
Para borrar la tabla ARP de la PC1, debemos abrir la terminal de Windows y ejecutamos el comando `arp -d` como se muestra en la Figura 5. No se muestra la ejecución del comando ya que no se obtiene una respuesta del sistema.

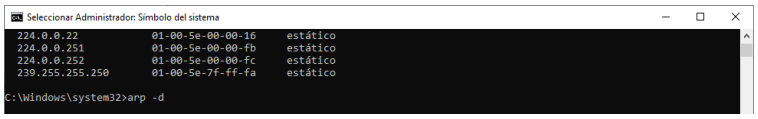

Figura 5: Borrar Tabla ARP

b. **Muestre el contenido de la tabla ARP.**
Para mostrar la tabla ARP de la PC1, debemos abrir la terminal de Windows y ejecutamos el comando `arp -a` como se muestra en la Figura 6.

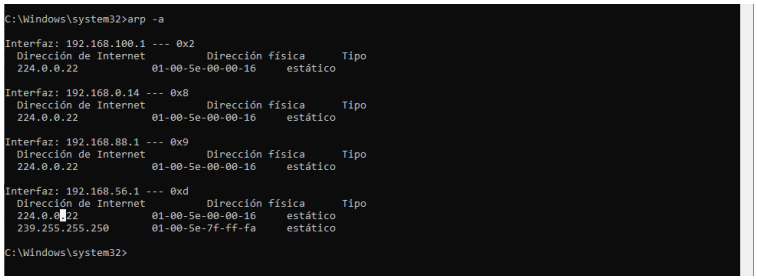

Figura 6: Tabla ARP

c. **¿Qué comandos y qué parametros se empleó en los puntos (a) y (b)?**

I) En el punto (a) se empleó el comando `arp` con el parámetro `-d` para borrar la tabla ARP.

II) En el punto (b) se empleó el comando `arp` con el parámetro `-a` para mostrar la tabla ARP.

d. **Explique con detalle el contenido de la tabla.**
Podemos observar en la Figura 6 que la tabla ARP contiene la dirección IP y la dirección MAC de los equipos que han sido contactados recientemente por la PC1.

4.3. Tarea 3.

Paso 1. Arranquen en la PC1 **Wireshark** para capturar el tráfico en su interfaz ethernet empleando los filtros adeacuados (ARP).

Paso 2. Realice el ping de la PC2 a la PC1.

a. ¿Cuál es el comando y los parámetros empleados?
Una vez terminado el ping, interrumpan la captural del Wireshark y guarde la captura en un archivo (utilicen como nombre del archivo captura1.cap) Compruebe el estado de las cachés del ARP en la PC.

b. Consulte la tabla ARP y analice si hubo cambios con los valores obtenidos en el paso 1 de la tarea 2; explique el contenido de la tabla.

Paso 3. Configure los filtros para capturar toda la información que se genere. Envíe el ping de la PC2 a la PC1 y al finalizar guarde el archivo como captura2.cap.

4.4. Tarea 4.

Paso 1. Con Wireshark cargue cada archivo capturado y explique los resultados obtenidos.

5. Conclusiones

Referencias

Buffett, W. E. (1984). *The Superinvestors of Graham-and-Doddsville*. Consultado el 30 de junio de 2019, desde https://www.gsb.columbia.edu/sites/valueinvesting/files/files/Buffett1984.pdf