



Universidad
Autónoma
Metropolitana 
Casa abierta al tiempo **Azcapotzalco**

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

12 de noviembre de 2024

1. Introducción

En las redes de comunicación, la capacidad de capturar y analizar son cosas esenciales para la comprender el comportamiento de los dispositivos y optimizar la comunicación en una red local (LAN). El monitorear y evaluar el tráfico de red puede servirnos al momento de la detección de los problemas de conectividad, diagnosticar algunos fallos en la configuración de los dispositivos que están conectados a la red, de forma que podemos asegurar un flujo eficiente y seguro de los datos.

Para esta práctica, utilizaremos una herramienta llamada **Wireshark** ampliamente usada en el análisis de tráfico en el campo de redes. Wireshark permite capturar y examinar los datos intercambiados entre dos computadores conectados por una (LAN). A través de las capturas, se va a buscar comprender como funcionan los protocolos **ARP** e **ICMP** y como estos protocolos nos facilitan la resolución de direcciones y la comunicación entre dispositivos conectados a la red.

El propósito de esta práctica es el análisis y familiarización con el uso de herramientas como la de Wireshark, para la interpretación de los protocolos ARP y analizar los efectos del comando ping entre dispositivos LAN. Adicionalmente, se busca observar los cambios en la caché ARP tras el intercambio de paquetes y comprender el flujo de tráfico unicast y multicast, así como el intercambio en las estructuras de la red.

Además de la captura y el análisis de tráfico, es importante entender cómo se comunican los distintos protocolos que conforman la comunicación en redes locales, de manera que interactúen entre sí para garantizar una conectividad eficiente. Tanto el protocolo ARP como el ICMP juegan un papel importante para la resolución de las direcciones así como para la gestión de errores y el diagnostico de problemas de conectividad, como se observa con el uso del comando ping

A lo largo de este informe, se detallarán los pasos seguidos para la configuración y la captura del tráfico, así mismo, los resultados obtenidos y la interpretación de estos. Este proceso nos permitirá habilidades fundamentales en el análisis del tráfico en la red y en la resolución de problemas que sean comunes en este tipo de redes locales.

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. 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.

3.1. 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.

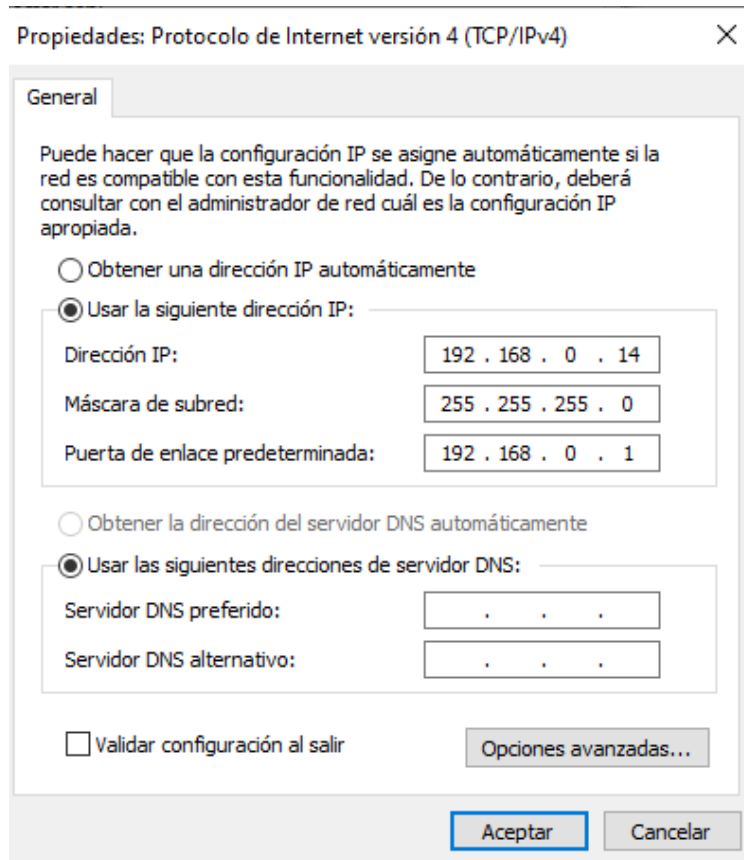


Figura 1: Configuración de la Dirección IP en Windows

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.

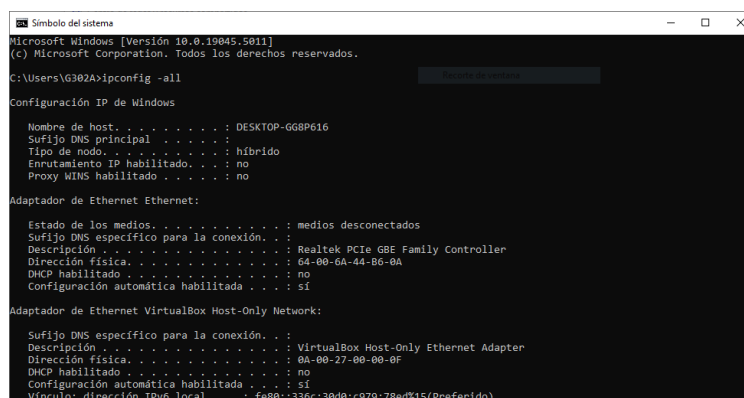


Figura 2: Obtención de la Dirección MAC en Windows

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.

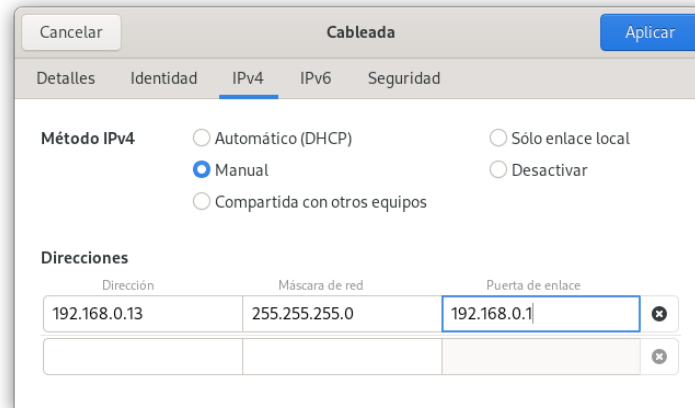


Figura 3: Configuración de la Dirección IP en Linux

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.

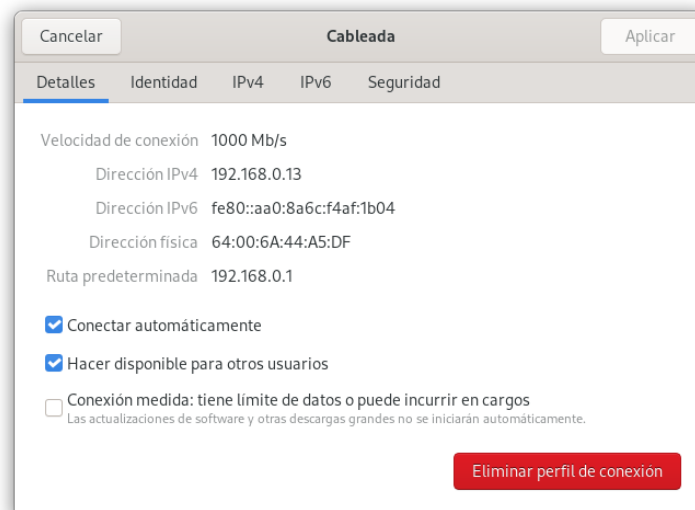


Figura 4: Obtención de la Dirección MAC en Linux

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

3.2. 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.

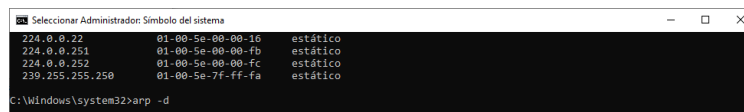


Figura 5: Borrar Tabla ARP

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.

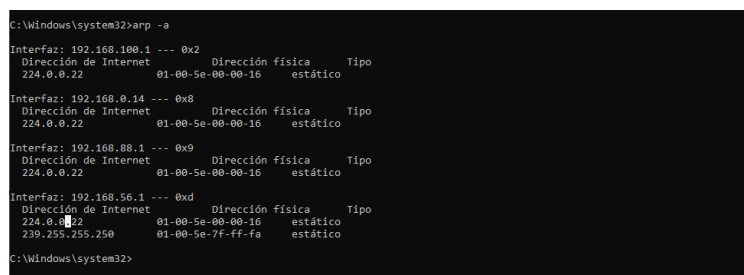


Figura 6: Contenido de la tabla ARP

c. ¿Qué comandos y qué parámetros 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. La tabla ARP muestra las direcciones IP y las direcciones físicas (MAC) que están asignadas en el sistema. En esta tabla, se observan varias interfaces (192.168.100.1, 192.168.0.14, 192.168.88.1 y 192.168.56.1),

lo cual indica que el dispositivo cuenta con múltiples conexiones de red o adaptadores.

Las direcciones IP presentadas corresponden a los dispositivos en la red con los cuales el dispositivo local ha interactuado o se ha comunicado recientemente. Todas las entradas de la tabla ARP son de tipo **estático**, lo que significa que estas asociaciones entre direcciones IP y MAC fueron configuradas manualmente o están asignadas de forma permanente, en lugar de ser asignadas dinámicamente por el sistema operativo.

Asimismo, en esta tabla se incluyen direcciones IP de tipo multicast (como 224.0.0.22 y 239.255.255.250), las cuales están asociadas a direcciones MAC específicas. Esto permite que determinados servicios o protocolos de red funcionen correctamente.

3.3. Tarea 3.

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

Para iniciar la captura de tráfico en la PC1, se abrió Wireshark y se seleccionó la interfaz de red Ethernet, se aplicó el filtro `arp` para capturar únicamente los paquetes ARP como se muestra en la Figura 7.

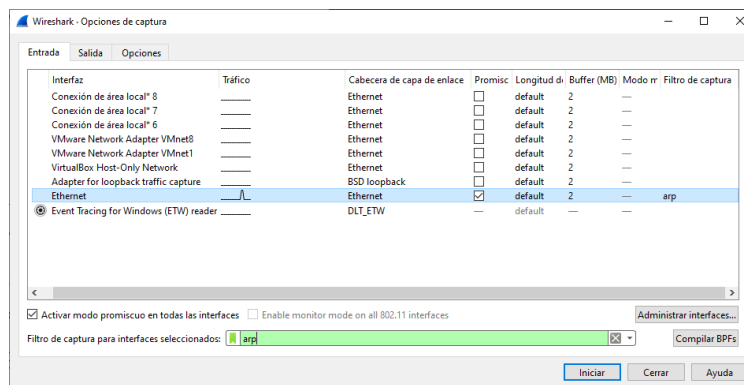
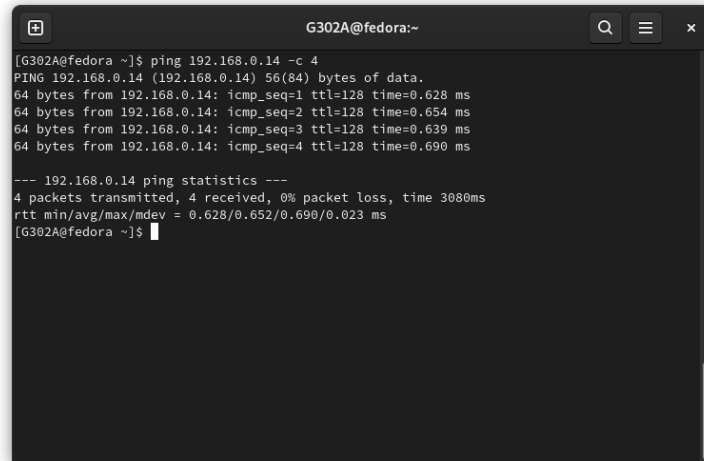


Figura 7: Wireshark

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

Para realizar el ping de la PC2 a la PC1, se abrió la terminal de Linux y se ejecutó el comando `ping -c 4` seguido de la dirección IP de la PC1, como se muestra en la Figura 8.

A terminal window titled 'G302A@fedora:~' showing the output of a ping command. The command is 'ping 192.168.0.14 -c 4'. The output shows four successful ping requests, each with a 64-byte payload, TTL of 128, and response times ranging from 0.628 ms to 0.690 ms. Below the individual responses, a summary line states: '--- 192.168.0.14 ping statistics ---', followed by '4 packets transmitted, 4 received, 0% packet loss, time 3080ms' and 'rtt min/avg/max/mdev = 0.628/0.652/0.690/0.023 ms'.

```
[G302A@fedora ~]$ ping 192.168.0.14 -c 4
PING 192.168.0.14 (192.168.0.14) 56(84) bytes of data:
64 bytes from 192.168.0.14: icmp_seq=1 ttl=128 time=0.628 ms
64 bytes from 192.168.0.14: icmp_seq=2 ttl=128 time=0.654 ms
64 bytes from 192.168.0.14: icmp_seq=3 ttl=128 time=0.639 ms
64 bytes from 192.168.0.14: icmp_seq=4 ttl=128 time=0.690 ms

--- 192.168.0.14 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3080ms
rtt min/avg/max/mdev = 0.628/0.652/0.690/0.023 ms
[G302A@fedora ~]$
```

Figura 8: Ping de la PC2 a la PC1

a. ¿Cuál es el comando y los parámetros empleados?

Se empleó el comando `ping` con el parámetro `-c 4` para enviar 4 paquetes de ping a la PC1.

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.

Al consultar la tabla ARP con el comando `arp -a` en la PC2, se observa que se han añadido nuevas entradas a la tabla ARP, las cuales corresponden a la dirección IP y MAC de la PC1. Esto se puede ver en la Figura 9. Esto se debe a que la PC2 ha enviado paquetes ARP a la PC1 para obtener su dirección MAC y poder establecer la comunicación entre ambos dispositivos.

A terminal window titled 'G302A@fedora:~' showing the output of the 'arp -a' command. The output displays the ARP table, including a new entry for IP address 192.168.0.14 with MAC address 64:00:6a:44:b6:0a, identified as an ether interface on enp3s0.

```
[G302A@fedora ~]$ arp -a
? (192.168.0.14) at 64:00:6a:44:b6:0a [ether] on enp3s0
[G302A@fedora ~]$
```

Figura 9: Tabla ARP en la PC2

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`.

Se eliminó el filtro arp y se configuró Wireshark para capturar todo el tráfico en la red. Se realizó el ping de la PC2 a la PC1 y se guardó la captura con el nombre `captura2.cap`.

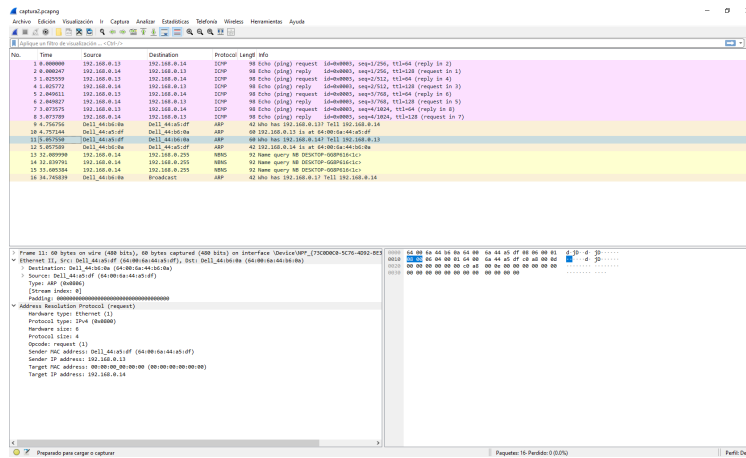


Figura 10: Captura de Tráfico en Wireshark

3.4. Tarea 4.

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

- los campos Ethernet y ARP (petición y respuesta; archivo: captura)

En la imagen se puede observar cómo los campos Ethernet contienen las Direcciones MAC de los dispositivos de origen, además de los dispositivos de destino. En este caso el dispositivo de origen tiene la dirección MAC **64:00:6a:44:b6:0a** y el destino suele ser **Broadcast** ya que por el método ARP suele enviar la información a todos los dispositivos.

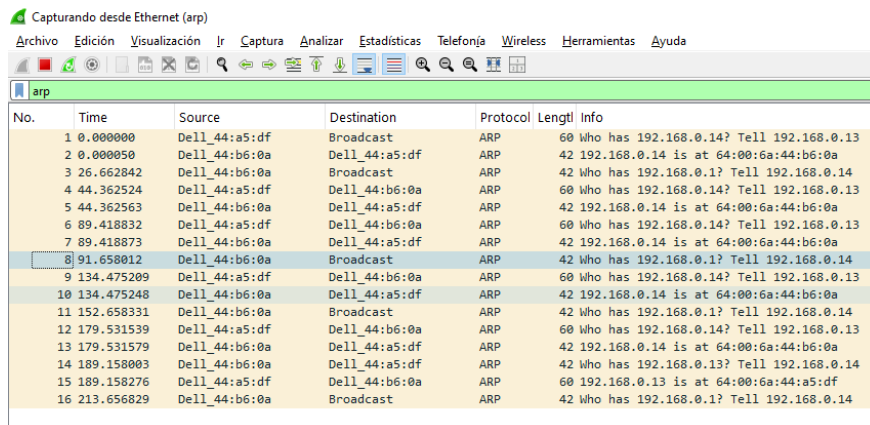


Figura 11: Captura del ARP en Wireshark

Se puede observar en la imagen que el metodo ARP tiene la solicitud: "Who has

192.168.0.14? Tell 192.168.0.13 lo cual indica que el dispositivo **192.168.0.13** esta buscando a la direccion MAC del dispositivo **192.168.0.14**.

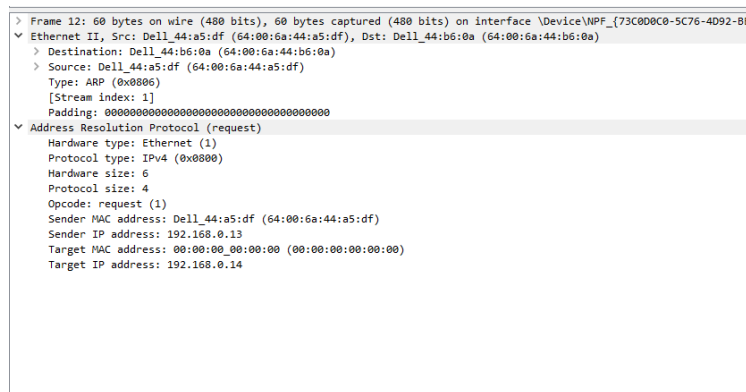


Figura 12: Captura de las tramas de la peticion ARP

b. ICMP(peticion y respuesta; archivos: captura2)

En la captura podemos observar como los paquetes tienen el protocolo ICMP para la comunicación de los dispositivos mediante el ping estas solicitudes y respuestas se envían entre las IP 192.168.0.13 y 192.168.0.14. Cada solicitud y respuesta tiene un identificador (id) y un número de secuencia (seq), que nos ayuda a rastrear el orden de los paquetes.

También se indica el TTL (Time to Live), que es el número de saltos que el paquete puede realizar antes de ser descartado. En las solicitudes, el TTL es 128, mientras que en las respuestas es 64.

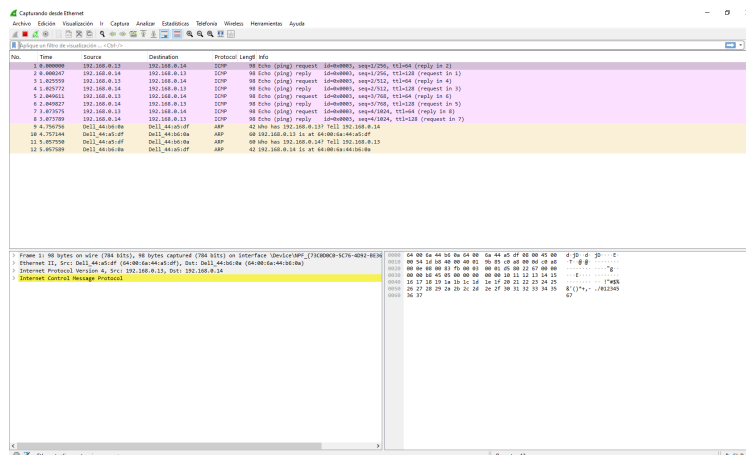


Figura 13: Captura del ICMP en Wireshark

Para ello, muestren gráficamente en el reporte los resultados de Wireshark resaltando la información correspondiente a los campos de las tramas.

4. Conclusiones

- Luis Ángel Cruz Díaz - 2183038433
- Diego Alexis Moreno Valero - 2243900185
- En esta práctica se logró comprender el funcionamiento de los protocolos ARP e ICMP y su importancia en las redes locales. A través del uso de Wireshark, se capturaron datos importantes, como el análisis del tráfico de paquetes generados por estos protocolos, lo que nos permitió visualizar de manera más detallada las tramas Ethernet y las peticiones/respuestas generadas durante el intercambio de mensajes.