Universidad Nacional Autónoma de México

Facultad de Ciencias

Redes de Computadoras

Práctica 1

Protocolo ARP y direcciones de capa de enlace.

Profesor: Paulo Contreras Flores

Ayudante Lab: José Daniel Campuzano Barajas

Objetivo

• El alumno aprenderá a identificar direcciones lógicas y físicas de una interfaz de red.

• Conocerá el funcionamiento del protocolo ARP mediante el uso de la herramienta Wireshark.

Introducción

En las redes bajo los estándares IEEE802.3 y IEEE802.11, la forma de identificar físicamente a los dispositivos de red es a través de la llamada dirección MAC (Media Access Control address).

También se le conoce como dirección física (physical address), dirección de hardware (hadware address), dirección LAN (Local Área Network address).

Está compuesta por 48 bits los cuales se representa en seis grupos de dos dígitos hexadecimales.

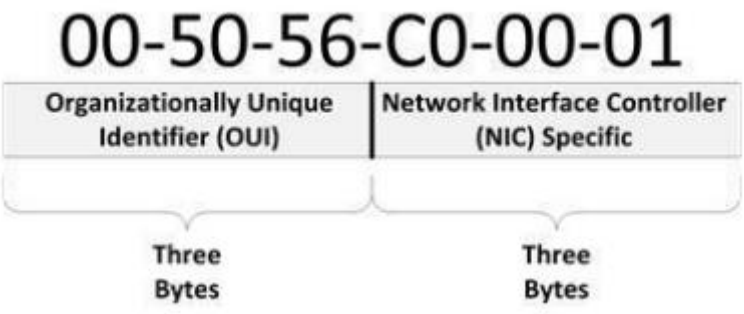

Figura 1. Composición de la dirección MAC.

Prerequisitos.

Software de virtualización VMware o VirtualBox.

Sistema operativo GNU/Linux o Windows instalado en VMware.

Utilerías estándar del sistema operativo elegido

Wireshark

Desarrollo

1. Configuración de la infraestructura virtual.

1.1. Configurar la tarjeta de red de la máquina virtual ingresando en el menú *VM -> Settings -> Network Adapter*

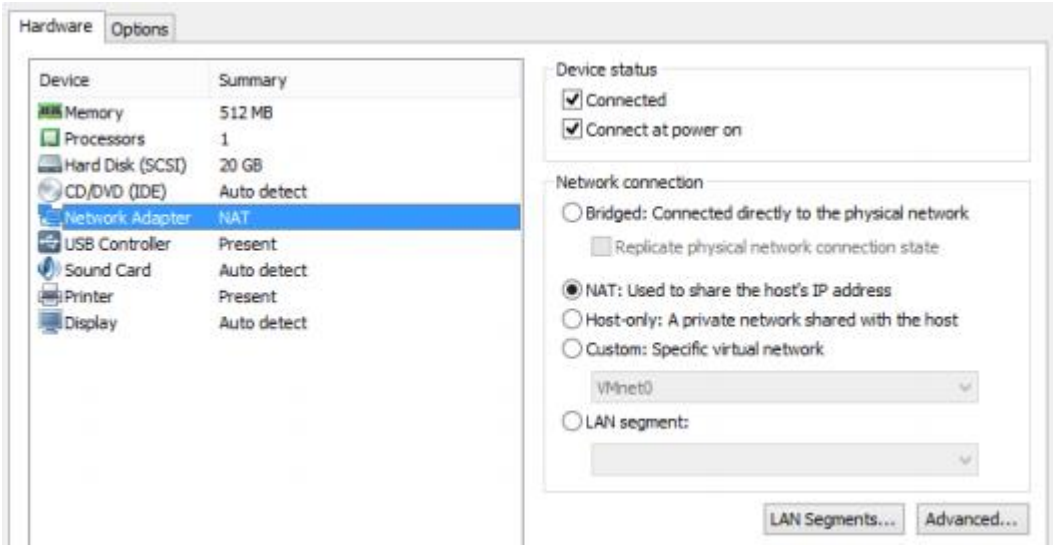

Figura 2. Menú de configuración de máquina virtual

Verificar que las opciones de la sección Device status: Connected y Connected at power on estén marcadas.

En la sección Network Connection la opción marcada debe ser NAT.

1.2. Encender la máquina virtual y ejecutar el comando ip addr en una terminal.

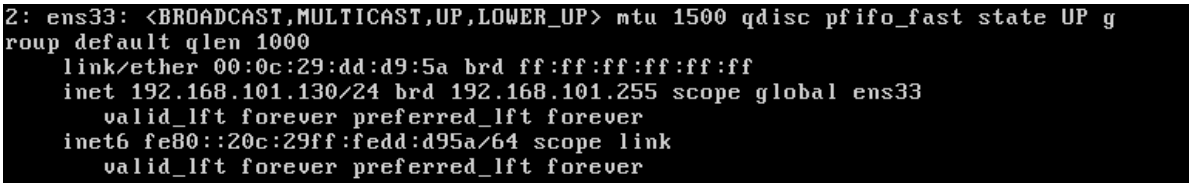

Figura 3. Configuración del adaptador de red eth0, ejemplo en SO Ubuntu.

Anotar a continuación la dirección física y lógica asignada a la tarjeta de red eth0.

Dirección física: _____

Dirección lógica: _____

Ejemplo:

Dirección física: 00:0C:29:DD:D9:5A

Dirección lógica: 192.168.101.130

1.3. Realizar el mismo procedimiento en el equipo físico. Para el caso concreto de Windows el comando es ipconfig /all el resultado se muestra en la imagen a continuación:

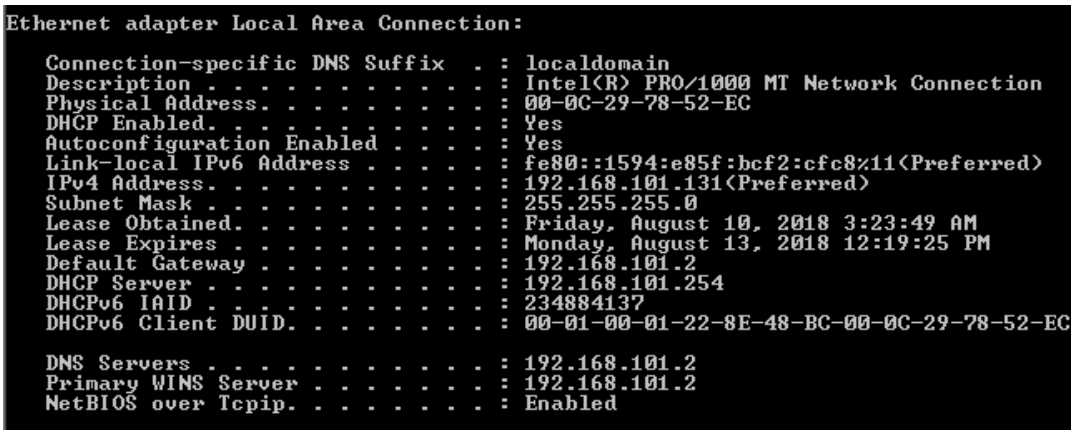

Figura 4. Configuración del adaptador de red en Windows.

Anotar a continuación la dirección física y lógica asignada a la tarjeta de red VMnet8.

Dirección física: _____

Dirección lógica: _____

Ejemplo:

Dirección física: 00:0C:29:78:52:EC

Dirección lógica: 192.168.101.130

2. Revisión del funcionamiento del protocolo ARP utilizando Wireshark.

2.1. Abrir la herramienta Wireshark. La interfaz a monitorizar dependerá del sistema operativo donde se ejecuta Wireshark, se puede seleccionar la interfaz directamente desde la pantalla inicial de Wireshark

presionando dos veces sobre el nombre del adaptador de red a monitorizar.

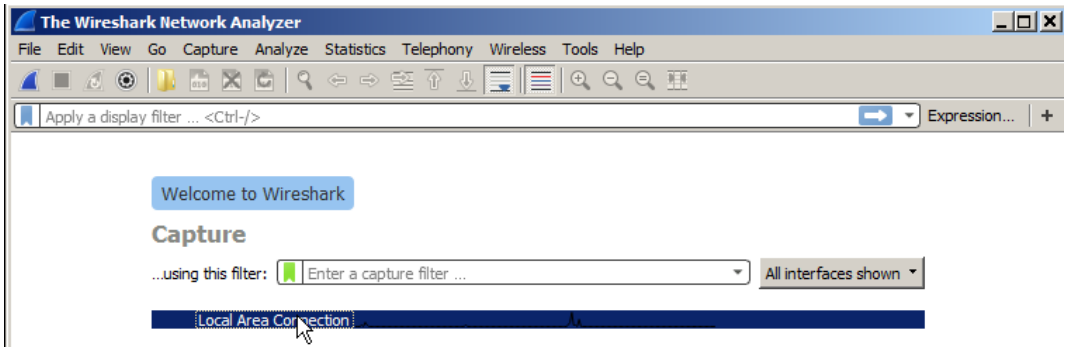

Figura 5. Interface de inicio de Wireshark.

2.2. Se mostrará la interface de captura de paquetes; continuar con la captura de paquetes mientras se realizan las siguientes acciones.

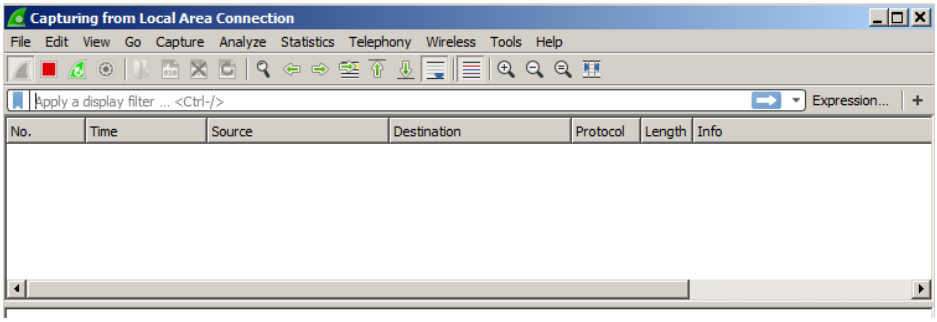

Figura 6. Interface de captura de paquetes de Wireshark.

2.3. Abrir una terminal de línea de comandos en Windows con permisos de administrador y ejecutar el siguiente comando:

```
C:\Users\Administrator>arp -d *
```

2.4. Utilizar la herramienta ping para comprobar conectividad entre el equipo físico y el equipo virtual.

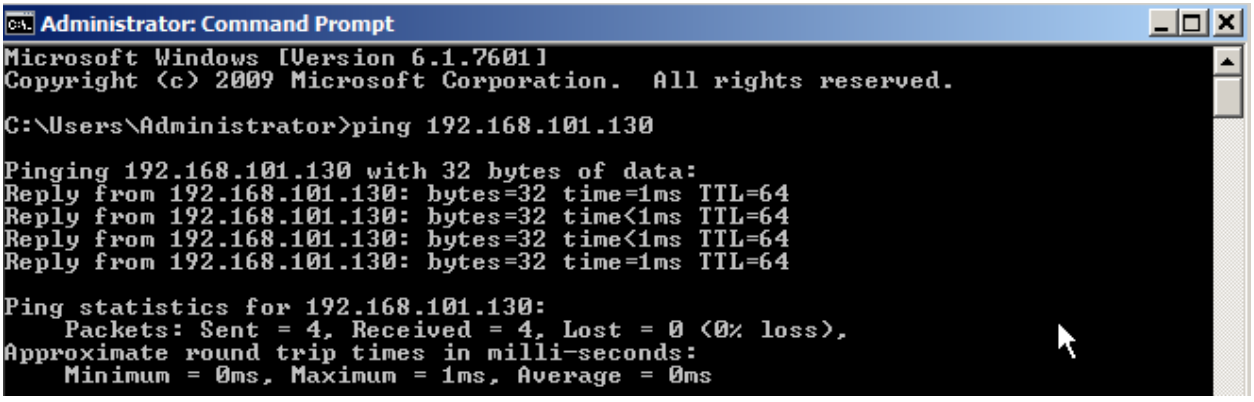

Figura 7. Uso de ping desde el equipo Windows hacia la dirección IP del equipo GNU/Linux.

2.5. Verificar dentro de Wireshark los paquetes correspondientes al protocolo ARP.

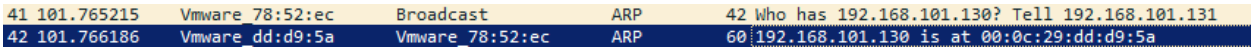

Figura 8. Paquetes ARP consultando la dirección del equipo GNU/Linux.

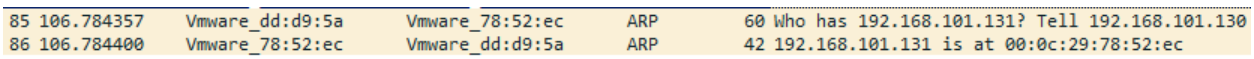

Figura 9. Paquetes ARP consultando la dirección del equipo Windows.

Cuestionario

1. ¿Cuál es la diferencia a nivel de bits entre una dirección física y una lógica?

2. ¿Por qué existen dos consultas ARP?

3. Describe que significa la salida del comando ***arp -a*** en el sistema operativo Windows.

4. Investigar y describir de manera breve en que consiste un ataque de ARP spoofing.

5. Investigar el fabricante del adaptador de red físico del equipo personal.

Notas adicionales

• El reporte se entrega de manera individual.

• Registrar en el reporte los pasos que sean considerados necesarios para explicar cómo se realizó la práctica, incluir capturas de pantalla que justifiquen los resultados obtenidos.

• Incluir las respuestas del Cuestionario en el reporte.

• Adjuntar el archivo PCAP (*.pcapng) de Wireshark.

• Se pueden agregar posibles errores, complicaciones, opiniones, críticas de la práctica o del laboratorio, o cualquier comentario relativo a la práctica.

• Subir los archivos relacionados con la práctica al classroom o entregar el reporte impreso en papel al inicio del laboratorio.

• Fecha de entrega martes 27 de agosto de 2018 antes de las 23:59 hrs.