



**UNIVERSIDAD DE LAS FUERZAS ARMADAS**

**ESPE**

**Laboratorio 1**

**Redes de Computadores**

**INTEGRANTES**

BONILLA JAIRO

MORALES ANTHONY

TOSCANO ALEJANDRO

**NRC**

23292

**DOCENTE**

MILTON ARGUELLO

**FECHA DE ENTREGA:**

20 de mayo del 2025

**TEMA**

Tramas Ethernet - Direcciones MAC.

*QUITO - ECUADOR*

*2025*

## Contenidos

OBJETIVOS .....	4
Objetivo general:.....	4
Objetivos específicos .....	4
ANTECEDENTES .....	4
Trama Ethernet: .....	4
• Dirección MAC de destino y origen: .....	4
• Tipo de protocolo:.....	4
• Datos: .....	4
• CRC (Cyclic Redundancy Check): .....	5
Protocolo ARP (Address Resolution Protocol): .....	5
• Función de ARP:.....	5
• Solicitud y Respuesta ARP:.....	5
• Solicitud ARP (ARP Request):.....	5
• Respuesta ARP (ARP Reply): .....	5
• Tiempo de vida de la información ARP: .....	6
Intercambio de información en ARP. ....	6
1. Código del Request y Response:.....	6
2. Identificación del Paquete de Petición y Respuesta:.....	6
PROCEDIMIENTO.....	7
1. Configuración de dirección IP y máscara de subred:.....	7
2. Comando ARP para obtener la tabla ARP:.....	9
3. Prueba de conectividad entre dispositivos mediante ping: .....	9
4. Captura de tráfico de red con Wireshark: .....	9
ANÁLISIS .....	15

Paquete ARP Request: .....	15
Paquete ARP Request Analizado:.....	15
Paquete ARP Response:.....	15
Paquete ARP Response Analizado: .....	16
Conclusiones .....	17
Recomendaciones .....	17
Bibliografías.....	17

### **Tabla de Ilustraciones**

Ilustración 1. Firewall de Windows Defender .....	7
Ilustración 2. Configuración de dirección IP estática. ....	8
Ilustración 3. Configuración de dirección IP estática. ....	8
Ilustración 4. Consola de comandos con el código <b>arp -a</b> . ....	9
Ilustración 5. <b>ping 10.10.10.7</b> .....	9
Ilustración 6. Captura de paquetes en Wireshark.....	10
Ilustración 7. ARP request. ....	10
Ilustración 8. ARP reply. ....	11
Ilustración 9. Tabla ARP.....	11
Ilustración 10. Activación del Hotspot. ....	12
Ilustración 11. Tabla ARP.....	13
Ilustración 12. Ilustración 6. Captura de paquetes en Wireshark II.....	13
Ilustración 13. Captura del protocolo ARP request. ....	14
Ilustración 14. Captura del protocolo ARP reply.....	14
Ilustración 15. Tabla ARP.....	15

## OBJETIVOS

### Objetivo general:

- Reconocer intercambio de datos en nivel de capa 2 mediante el protocolo ARP.

### Objetivos específicos:

- Reconocimiento de protocolo ARP.
- Establecer redes punto a punto.
- Reconocimiento de comandos de línea de consola para estados de red.
- Reconocimiento de la herramienta Wireshak para tráfico de datos.

## ANTECEDENTES

### Trama Ethernet:

La trama Ethernet es la unidad básica de transmisión en redes Ethernet, ampliamente utilizada en redes de área local (LAN). Una trama Ethernet tiene una estructura estandarizada que se compone de varios campos esenciales, tales como las direcciones MAC de origen y destino, el tipo de protocolo, los datos y la verificación de integridad mediante el campo de verificación de redundancia cíclica (CRC).

- ***Dirección MAC de destino y origen:***

Cada dispositivo en una red Ethernet está identificado por una dirección única de 48 bits, conocida como la Dirección de Control de Acceso de Medios (MAC). La dirección MAC de destino indica a qué dispositivo se enviará el paquete de datos, mientras que la dirección MAC de origen identifica al dispositivo que envió la trama.

- ***Tipo de protocolo:***

Este campo se utiliza para indicar qué tipo de protocolo de red está encapsulado dentro de la trama Ethernet, como IPv4 o IPv6, por ejemplo.

- ***Datos:***

Este es el campo que transporta la carga útil o datos reales que el paquete lleva de un dispositivo a otro.

- ***CRC (Cyclic Redundancy Check):***

El CRC es un valor utilizado para verificar la integridad de los datos en la trama. Permite al receptor de la trama verificar si los datos han llegado sin errores, garantizando la fiabilidad en la transmisión.

### **Protocolo ARP (Address Resolution Protocol):**

ARP es un protocolo de red de la capa de enlace de datos que se utiliza para resolver direcciones IP a direcciones MAC en una red local. Cuando un dispositivo necesita enviar datos a otro en la misma red local, debe conocer la dirección MAC del destinatario. Si el dispositivo solo tiene la dirección IP, utiliza ARP para obtener la dirección MAC correspondiente.

- ***Función de ARP:***

ARP permite que un dispositivo que posee una dirección IP pueda obtener la dirección MAC de otro dispositivo en la misma red. Este proceso es crucial para el funcionamiento de redes Ethernet, ya que las direcciones IP son utilizadas a nivel de la capa de red (capa 3), mientras que las direcciones MAC se utilizan a nivel de la capa de enlace de datos (capa 2).

- ***Solicitud y Respuesta ARP:***

ARP funciona mediante dos tipos principales de mensajes.

- ***Solicitud ARP (ARP Request):***

El dispositivo que desea conocer la dirección MAC de otro dispositivo envía un mensaje ARP Request. Este mensaje incluye la dirección IP del dispositivo destino, y se envía a todos los dispositivos en la red local.

- ***Respuesta ARP (ARP Reply):***

El dispositivo con la dirección IP solicitada responde con un mensaje ARP Reply que contiene su dirección MAC. Este mensaje es enviado directamente al dispositivo que realizó la solicitud.

- ***Tiempo de vida de la información ARP:***

Una vez que un dispositivo ha recibido la respuesta ARP, guarda la dirección MAC en su tabla ARP local por un período determinado. Este período varía dependiendo de la configuración de la red, y al expirar, el dispositivo debe realizar una nueva solicitud ARP si necesita comunicarse nuevamente con el dispositivo cuya dirección MAC ha caducado.

### **Intercambio de información en ARP.**

El intercambio de información ARP es un proceso fundamental para la resolución de direcciones dentro de una red local. Este proceso se puede observar mediante la ejecución de comandos como ***arp - a***, que muestra la tabla ARP local, donde se almacenan las asociaciones entre direcciones IP y direcciones MAC. En una red Ethernet, la falta de resolución de una dirección MAC puede generar problemas de comunicación entre dispositivos, ya que los paquetes no pueden ser enviados sin conocer la dirección física del destinatario.

#### ***1. Código del Request y Response:***

- **Request ARP:** Un paquete ARP Request se envía como una difusión (broadcast) en la red. El código de este paquete es de tipo 0x0806 para identificar que se trata de un mensaje ARP en un entorno Ethernet.
- **Response ARP:** El paquete ARP Reply contiene la dirección MAC del dispositivo solicitado y es enviado como una transmisión unicast directamente al dispositivo que realizó la solicitud.

#### **2. Identificación del Paquete de Petición y Respuesta:**

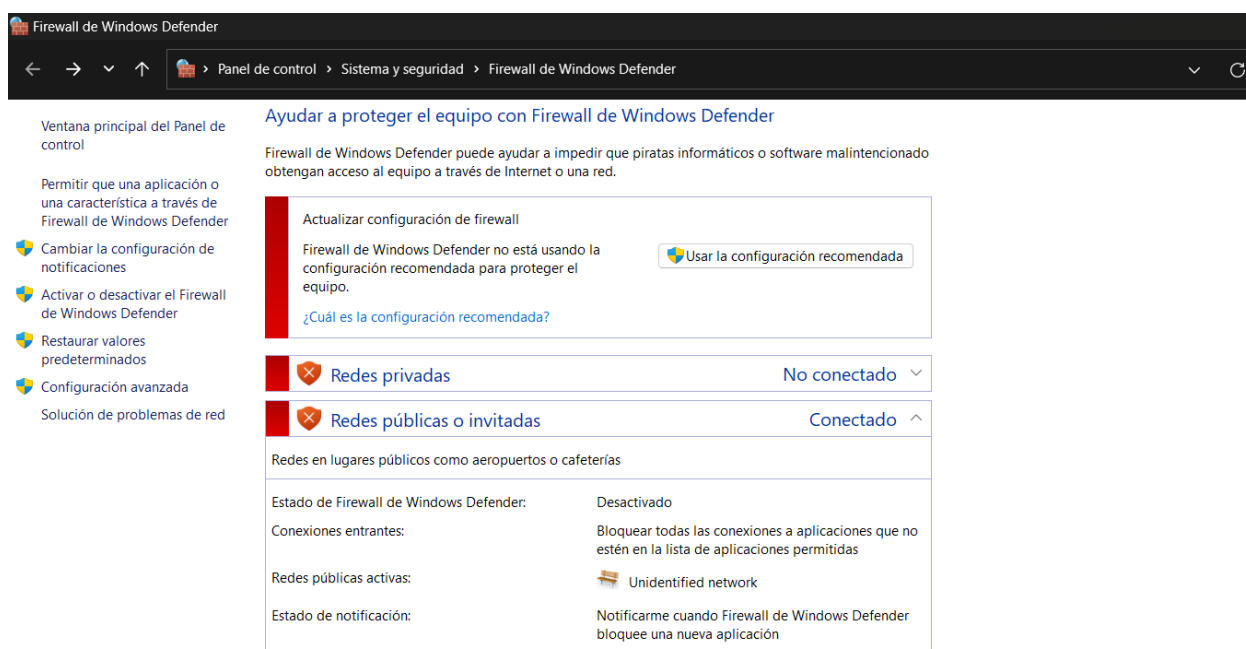
Los paquetes ARP se pueden diferenciar visualmente mediante herramientas como Wireshark, que muestran los campos de origen y destino. La diferencia principal entre un paquete ARP Request y un paquete ARP Reply es que el primero se envía a toda la red, mientras que el segundo se envía directamente al solicitante. La herramienta Wireshark permite analizar estos paquetes de forma detallada, mostrando las direcciones IP y MAC involucradas, así como el tipo de acción (solicitud o respuesta).

## PROCEDIMIENTO

Se llevaron a cabo dos métodos de conexión con el objetivo de analizar el funcionamiento del protocolo ARP en la capa 2 del modelo OSI. En ambos casos, se utilizó la herramienta **Wireshark** para capturar y analizar el tráfico de red, y la consola de comandos para ejecutar instrucciones como **arp - a**, **arp - d \***.

### ESCENARIO 1: CONEXIÓN DIRECTA MEDIANTE CABLE ETHERNET

1. *Se desactivó temporalmente el firewall de los equipos para permitir la comunicación sin restricciones.*

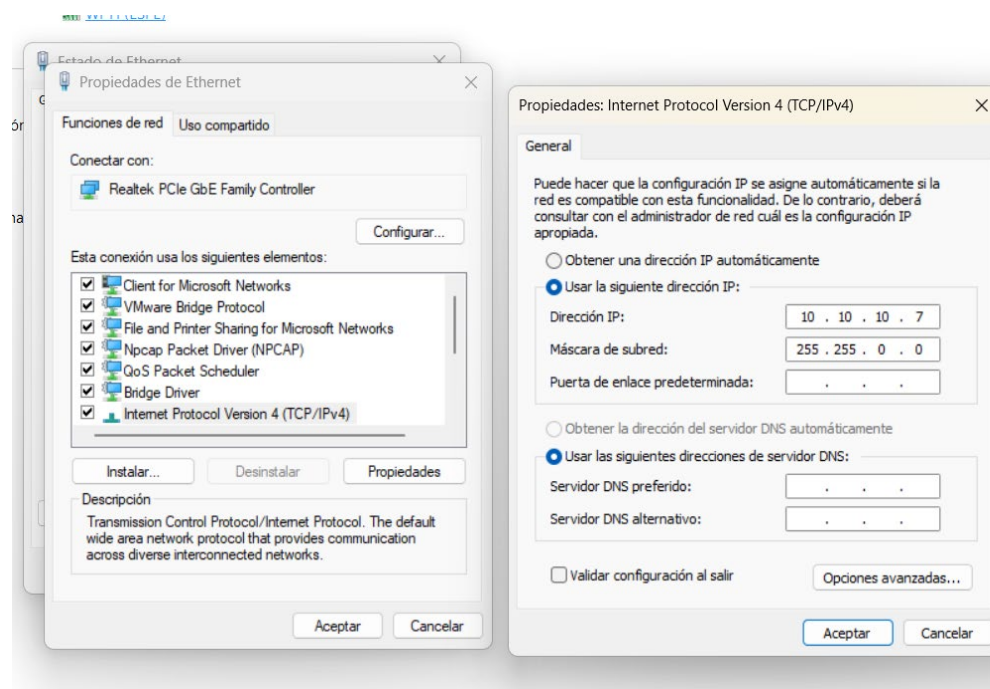


*Ilustración 1. Firewall de Windows Defender*

2. *Configuración de dirección IP y máscara de subred:*

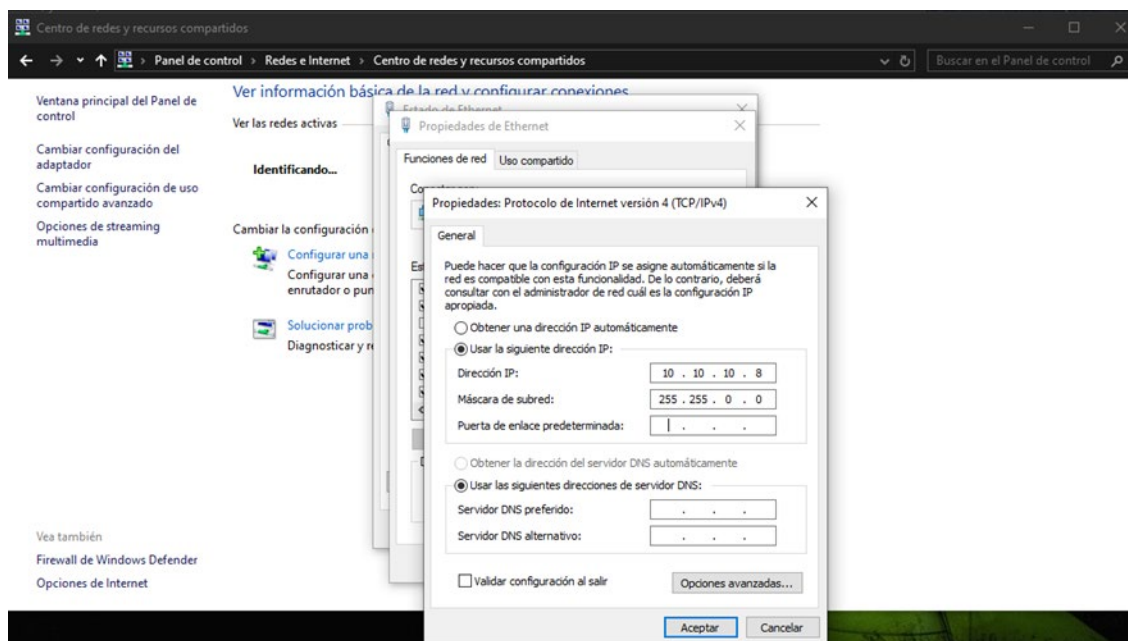
Se configuró direcciones IP estáticas en los computadores ingresando a las propiedades de red “**Protocolo de internet versión 4 (TCP/IPv4)**”.

**Equipo 1.** IP: 10.10.10.7 y Máscara de subred: 255.255.0.0



*Ilustración 2. Configuración de dirección IP estática.*

**Equipo 2.** IP: 10.10.10.8 y Máscara de subred: 255.255.0.0



*Ilustración 3. Configuración de dirección IP estática.*



### 3. Comando ARP para obtener la tabla ARP:

Se ejecutó la consola de comandos en modo **administrador** y se ejecutó el comando **arp -a** para verificar las direcciones IP y las correspondientes direcciones MAC en la tabla ARP.

```
C:\WINDOWS\system32>arp -a

Interfaz: 10.10.10.8 --- 0xf
Dirección de Internet      Dirección física      Tipo
224.0.0.22                01-00-5e-00-00-16    estático
239.255.255.253          01-00-5e-7f-ff-fd    estático

C:\WINDOWS\system32>
```

*Ilustración 4. Consola de comandos con el código arp -a.*

### 4. Prueba de conectividad entre dispositivos mediante ping:

Se ejecuto el comando **ping** a la dirección IP **10.10.10.7**, confirmando la conectividad entre los dispositivos. Y generando tráfico de red.

```
C:\WINDOWS\system32>ping 10.10.10.7

Haciendo ping a 10.10.10.7 con 32 bytes de datos:
Respuesta desde 10.10.10.7: bytes=32 tiempo=1ms TTL=128
Respuesta desde 10.10.10.7: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.10.10.7: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.10.10.7: bytes=32 tiempo=1ms TTL=128

Estadísticas de ping para 10.10.10.7:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\WINDOWS\system32>
```

*Ilustración 5. ping 10.10.10.7*

### 5. Captura de tráfico de red con Wireshark:

Se capturaron los paquetes ARP en la red usando Wireshark. Los paquetes de solicitud y respuesta ARP fueron visualizados para identificar las direcciones IP y MAC asociadas.

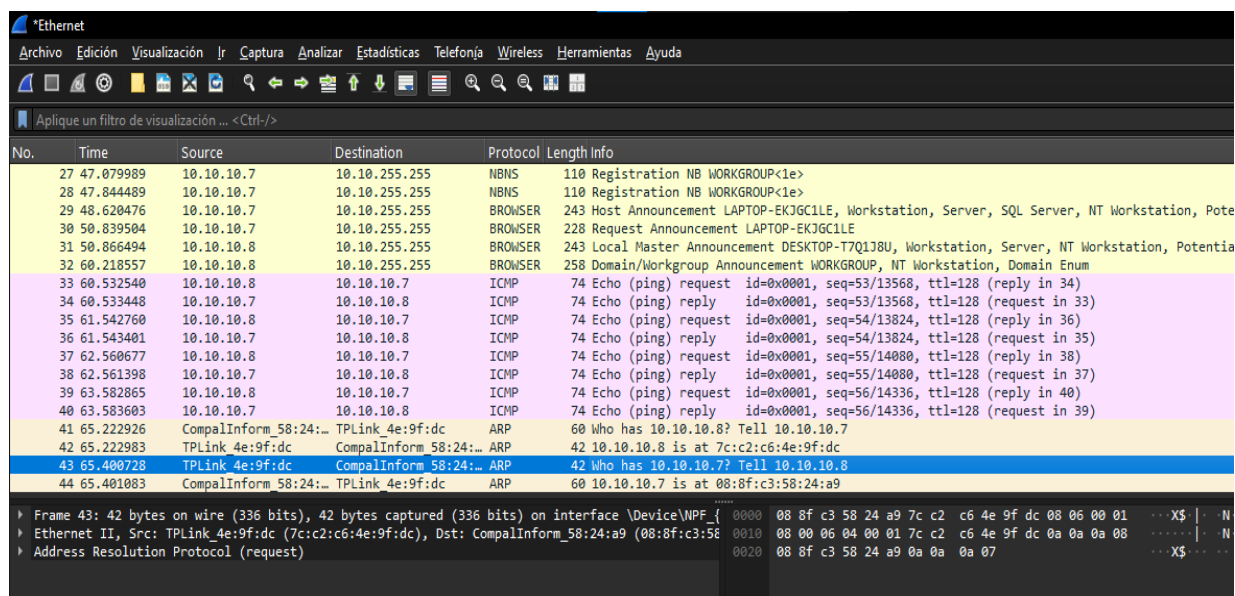


Ilustración 6. Captura de paquetes en Wireshark.

- **ARP request:** El equipo solicita la dirección MAC asociada a la IP 10.10.10.7.

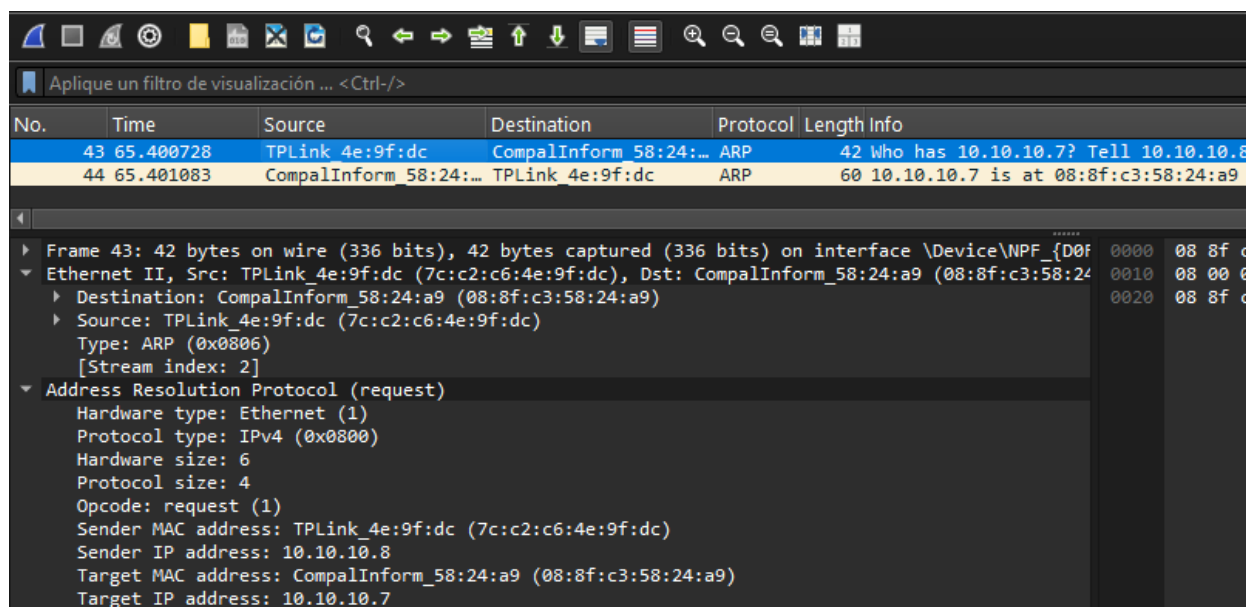
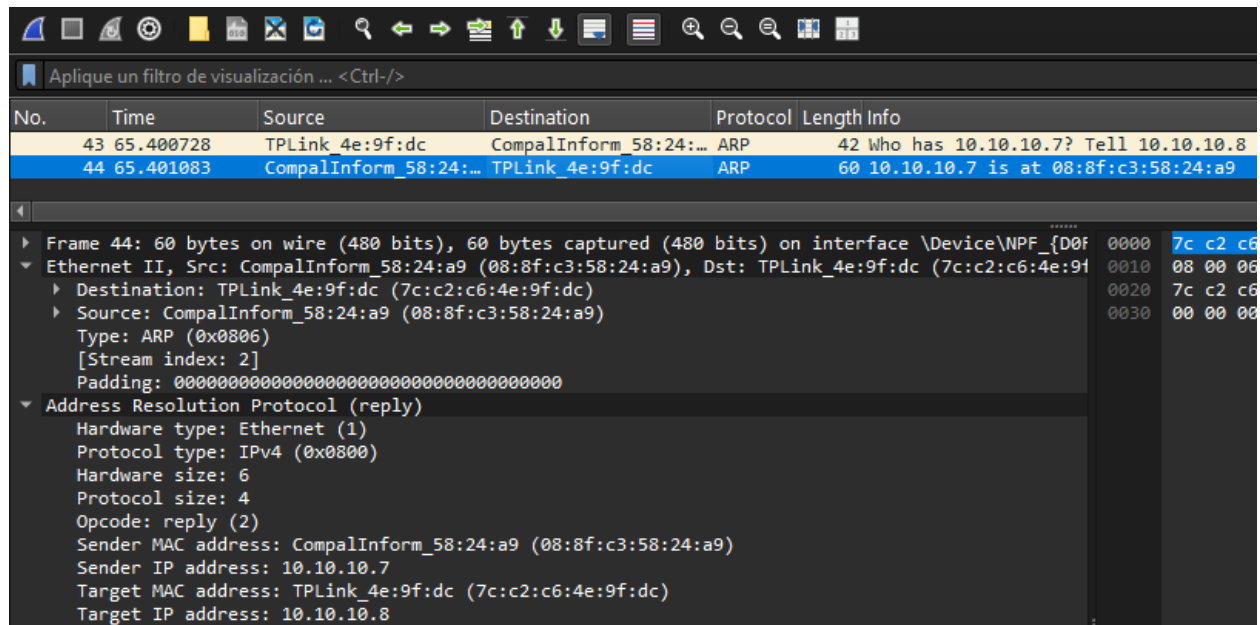


Ilustración 7. ARP request.

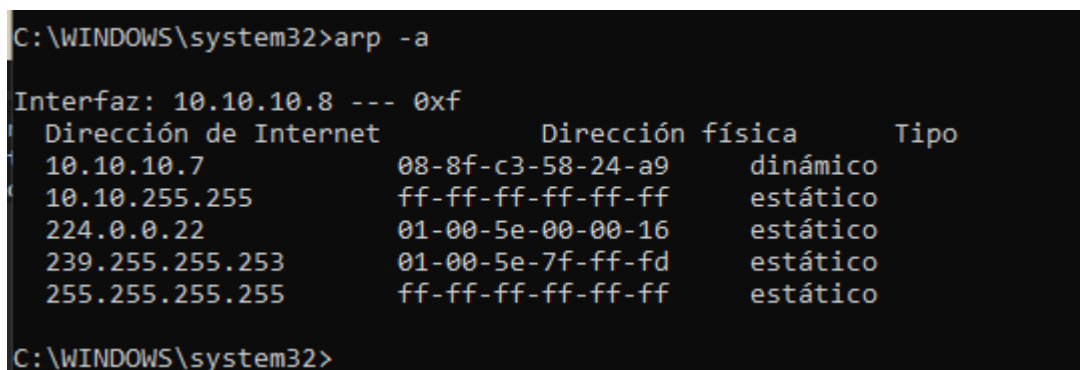
- **ARP reply:** El equipo destino responde con su dirección MAC correspondiente.



*Ilustración 8. ARP reply.*

## 6. Comando ARP para obtener la nueva tabla ARP

Finalmente, se ejecutó nuevamente el comando **arp -a**, esta vez observando que la IP del equipo remoto (**10.10.10.7**) ya aparece en la tabla ARP, junto con su dirección MAC física.

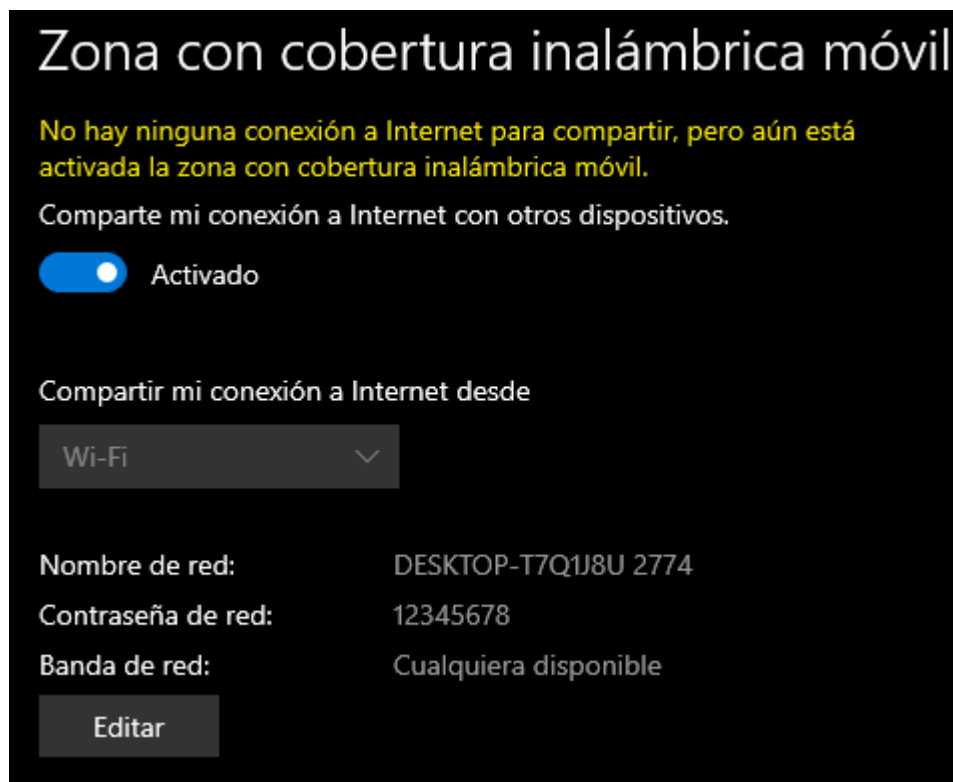


*Ilustración 9. Tabla ARP.*

## ESCENARIO 2: CONEXIÓN MEDIANTE RED HOTSPOT (ZONA PORTÁTIL)

### 1. *Activación del hotspot y conexión del segundo equipo:*

En el **Equipo 1**, se desconectó de la red wifi y se activó la opción de **Zona con cobertura inalámbrica móvil** desde la configuración de red. Posteriormente, en el **Equipo 2**, se buscó la red Wi-Fi generada por el hotspot del Equipo 1 y se realizó la conexión correctamente.



*Ilustración 10. Activación del Hotspot.*

### 2. *Limpieza de la tabla ARP:*

Se accedió a la consola de comandos del **Equipo 1** en modo administrador y se ejecutó el comando **arp -d \*** para eliminar todas las entradas previas de la tabla ARP. A continuación, se utilizó **arp -a** para verificar que no existieran direcciones IP almacenadas.

```
C:\WINDOWS\system32>arp -d *

C:\WINDOWS\system32>arp -a

Interfaz: 192.168.137.1 --- 0xc
Dirección de Internet      Dirección física      Tipo
224.0.0.22                01-00-5e-00-00-16    estático
239.255.255.250           01-00-5e-7f-ff-fa    estático

C:\WINDOWS\system32>
```

Ilustración 11. Tabla ARP

### 3. Generación de tráfico de red (ping):

Se ejecuto el comando **ping** a la dirección IP **192.168.137.68**, confirmando la conectividad entre los dispositivos. Y generando tráfico de red. Esto generó paquetes ICMP y automáticamente una solicitud ARP si la dirección MAC no estaba almacenada.

### 4. Captura de tráfico con Wireshark:

En el **Equipo 1**, se abrió **Wireshark**, seleccionando la interfaz de red correspondiente al adaptador de red local inalámbrica. Se comenzó la captura de paquetes.

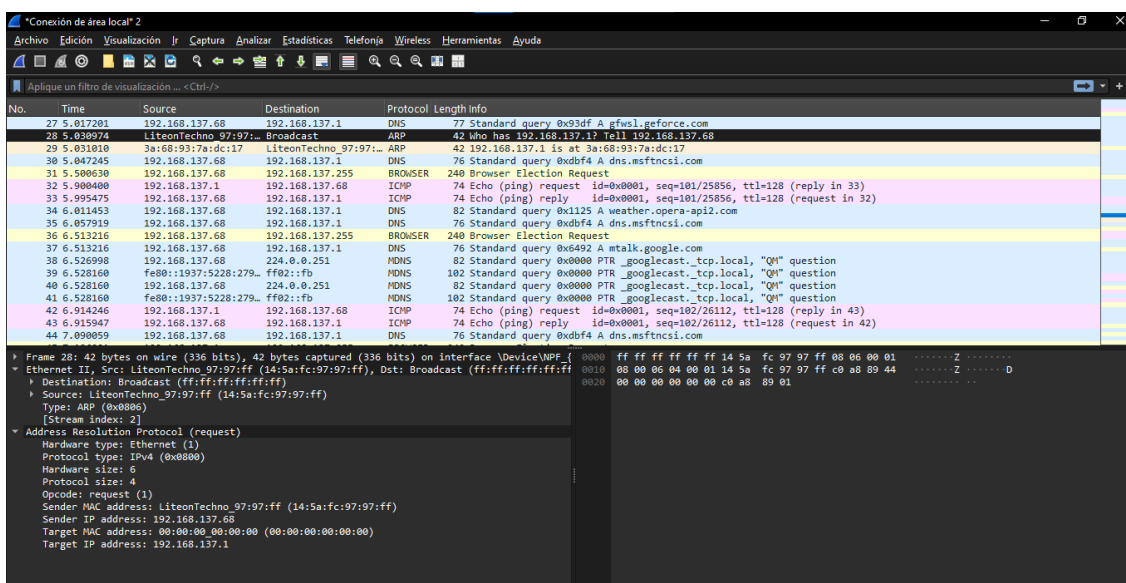
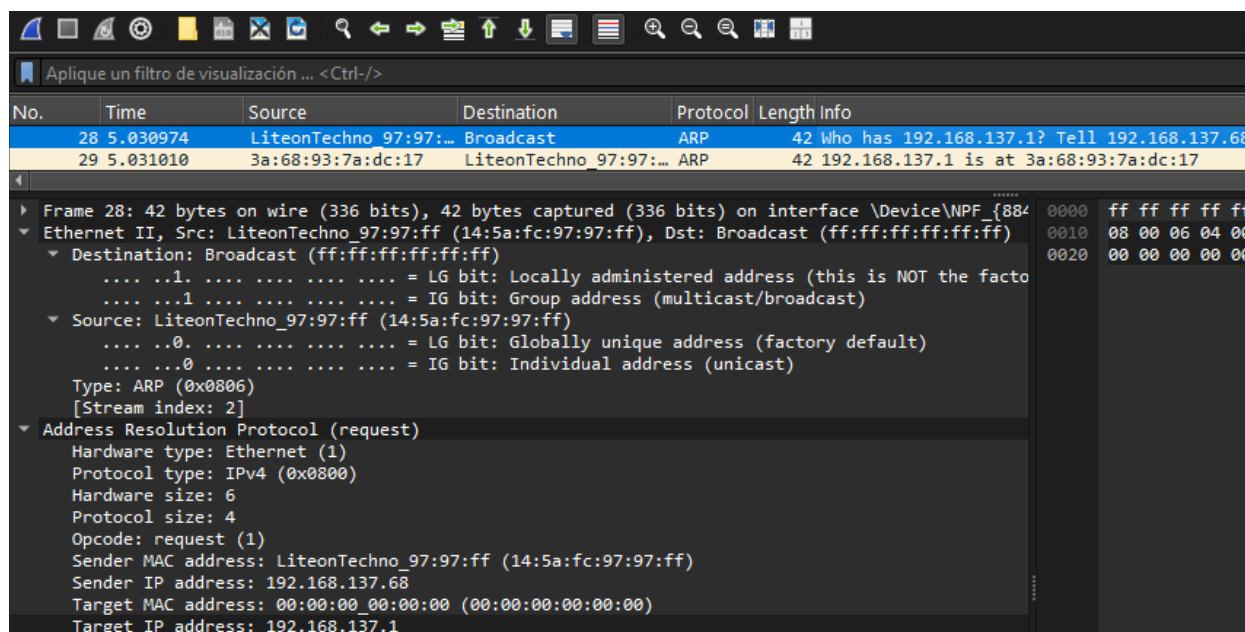


Ilustración 12. Ilustración 6. Captura de paquetes en Wireshark II.

- ARP request:



Wireshark interface showing an ARP request capture. The packet list shows two packets: packet 28 (ARP request) and packet 29 (ARP reply). Packet 28 is selected, showing its details in the packet pane. The details pane shows the Ethernet II header (Source: LiteonTechno\_97:97:ff, Destination: Broadcast), the ARP header (Type: ARP (0x0806)), and the Address Resolution Protocol (request) section. The ARP section shows the hardware type (Ethernet), protocol type (IPv4), hardware size (6), protocol size (4), opcode (request), sender MAC address (LiteonTechno\_97:97:ff), sender IP address (192.168.137.68), target MAC address (00:00:00\_00:00:00), and target IP address (192.168.137.1).

No.	Time	Source	Destination	Protocol	Length	Info
28	5.030974	LiteonTechno_97:97:ff	Broadcast	ARP	42	Who has 192.168.137.1? Tell 192.168.137.68
29	5.031010	3a:68:93:7a:dc:17	LiteonTechno_97:97:ff	ARP	42	192.168.137.1 is at 3a:68:93:7a:dc:17

Frame 28: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF\_{884...}

Ethernet II, Src: LiteonTechno\_97:97:ff (14:5a:fc:97:97:ff), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  - ...1. .... = LG bit: Locally administered address (this is NOT the factory default)
  - ...1. .... = IG bit: Group address (multicast/broadcast)
- Source: LiteonTechno\_97:97:ff (14:5a:fc:97:97:ff)
  - ...0. .... = LG bit: Globally unique address (factory default)
  - ...0. .... = IG bit: Individual address (unicast)

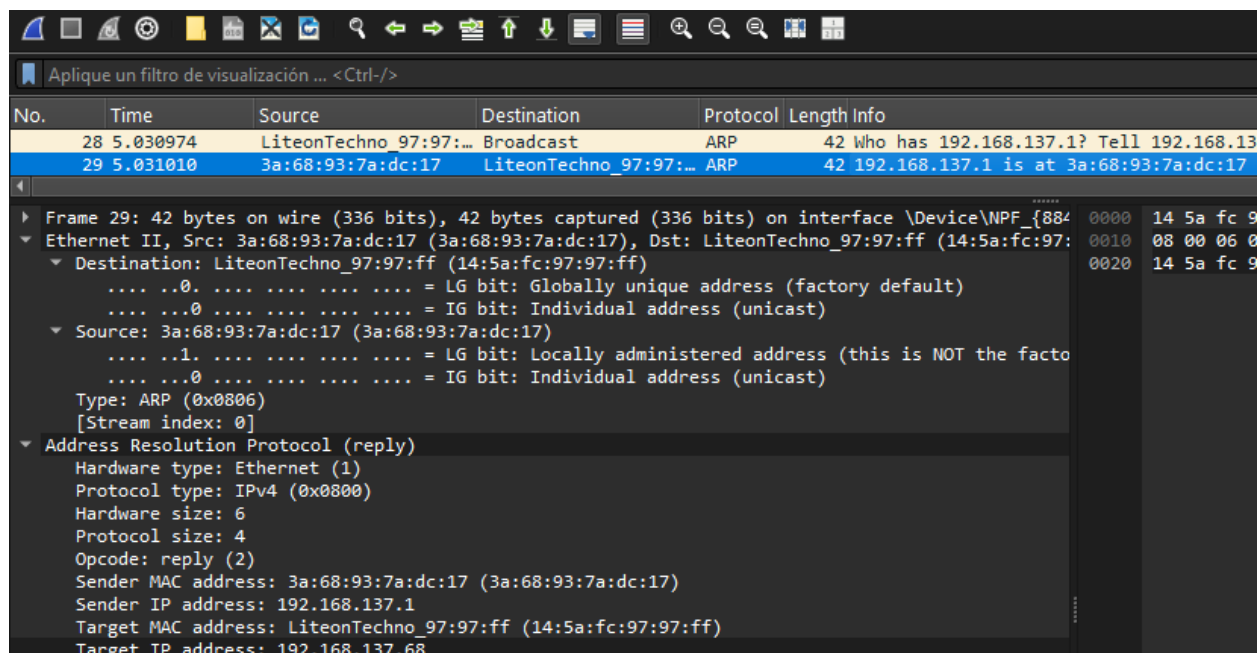
Type: ARP (0x0806)  
[Stream index: 2]

Address Resolution Protocol (request)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: LiteonTechno\_97:97:ff (14:5a:fc:97:97:ff)
- Sender IP address: 192.168.137.68
- Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00)
- Target IP address: 192.168.137.1

Ilustración 13. Captura del protocolo ARP request.

- ARP reply:



Wireshark interface showing an ARP reply packet capture. The packet list shows two packets: packet 28 (ARP request) and packet 29 (ARP reply). Packet 29 is selected, showing its details in the packet pane. The details pane shows the Ethernet II header (Source: 3a:68:93:7a:dc:17, Destination: LiteonTechno\_97:97:ff), the ARP header (Type: ARP (0x0806)), and the Address Resolution Protocol (reply) section. The ARP section shows the hardware type (Ethernet), protocol type (IPv4), hardware size (6), protocol size (4), opcode (reply), sender MAC address (3a:68:93:7a:dc:17), sender IP address (192.168.137.1), target MAC address (LiteonTechno\_97:97:ff), and target IP address (192.168.137.68).

No.	Time	Source	Destination	Protocol	Length	Info
28	5.030974	LiteonTechno_97:97:ff	Broadcast	ARP	42	Who has 192.168.137.1? Tell 192.168.137.68
29	5.031010	3a:68:93:7a:dc:17	LiteonTechno_97:97:ff	ARP	42	192.168.137.1 is at 3a:68:93:7a:dc:17

Frame 29: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF\_{884...}

Ethernet II, Src: 3a:68:93:7a:dc:17 (3a:68:93:7a:dc:17), Dst: LiteonTechno\_97:97:ff (14:5a:fc:97:97:ff)

- Destination: LiteonTechno\_97:97:ff (14:5a:fc:97:97:ff)
  - ...0. .... = LG bit: Globally unique address (factory default)
  - ...0. .... = IG bit: Individual address (unicast)
- Source: 3a:68:93:7a:dc:17 (3a:68:93:7a:dc:17)
  - ...1. .... = LG bit: Locally administered address (this is NOT the factory default)
  - ...0. .... = IG bit: Individual address (unicast)

Type: ARP (0x0806)  
[Stream index: 0]

Address Resolution Protocol (reply)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: reply (2)
- Sender MAC address: 3a:68:93:7a:dc:17 (3a:68:93:7a:dc:17)
- Sender IP address: 192.168.137.1
- Target MAC address: LiteonTechno\_97:97:ff (14:5a:fc:97:97:ff)
- Target IP address: 192.168.137.68

Ilustración 14. Captura del protocolo ARP reply.

### 5. Verificación de la tabla ARP:

Se volvió a ejecutar **arp -a** en el **Equipo 1**, y se pudo comprobar que la IP 192.168.137.68 ya estaba registrada en la tabla ARP, asociada a la dirección física 14-5a-fc-97-97-ff. Esta entrada fue clasificada como de tipo **estática**.

```

C:\WINDOWS\system32>arp -a

Interfaz: 192.168.137.1 --- 0xc
Dirección de Internet      Dirección física      Tipo
192.168.137.68             14-5a-fc-97-97-ff    estático
192.168.137.255            ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático

C:\WINDOWS\system32>

```

*Ilustración 15. Tabla ARP*

## ANÁLISIS

En el análisis de la tabla ARP, se observó la asociación de las direcciones IP con las direcciones MAC correspondientes. Se identificaron los siguientes paquetes en la captura de Wireshark:

### Paquete ARP Request:

El dispositivo con dirección IP 10.10.10.8 solicitó la dirección MAC correspondiente a 10.10.10.7, como se observa en la Ilustración 4.

### Paquete ARP Request Analizado:

- Dirección MAC de origen: 00:1A:2B:3C:4D:5E (Dispositivo A)
- Dirección IP de destino: 192.168.1.2 (Dispositivo B)

### Paquete ARP Response:

El dispositivo con IP 10.10.10.7 respondió con su dirección MAC, permitiendo que 10.10.10.8 actualizara su tabla ARP. Ilustración 9.

Tabla con las direcciones IP y MAC de ambos dispositivos capturados en el tráfico de ARP:

Dirección IP	Dirección MAC	Paquete ARP
192.168.1.1	00:1A:2B:3C:4D:5E	Request
192.168.1.2	00:1F:2E:3D:4C:5B	Response

***Paquete ARP Response Analizado:***

- Dirección MAC de origen: 00:1F:2E:3D:4C:5B (Dispositivo B)
- Dirección IP de origen: 192.168.1.2

**Escenario 2**

**Paquete ARP Request:**

El dispositivo con dirección IP 192.168.137.1 solicitó la dirección MAC correspondiente a 192.168.137.68 para poder enviarle paquetes. Ilustración 13.

**Paquete ARP Request Analizado:**

- Dirección MAC de origen: 3a:68:93:7a:dc:17
- Dirección IP de origen: 192.168.137.1
- Dirección MAC de destino: ff:ff:ff:ff:ff:ff (*difusión/broadcast*)
- Dirección IP de destino: 192.168.137.68

**Paquete ARP Response:**

El dispositivo con IP **192.168.137.68** respondió con su dirección MAC (**14:5a:fc:97:97:ff**), permitiendo que el dispositivo **192.168.137.1** actualizara su tabla ARP con esta información y pudiera continuar con la comunicación. Ilustración 14.

**Paquete ARP Response Analizado:**

- Dirección MAC de origen: 14:5a:fc:97:97:ff
- Dirección IP de origen: 192.168.137.68
- Dirección MAC de destino: 3a:68:93:7a:dc:17
- Dirección IP de destino: 192.168.137.1



Tabla con las direcciones IP y MAC de ambos dispositivos capturados en el tráfico de ARP:

Dirección IP	Dirección MAC	Tipo de Paquete
192.168.137.1	3a:68:93:7a:dc:17	Request
192.168.137.68	14:5a:fc:97:97:ff	Response

### Conclusiones

El intercambio de información ARP permite la correcta resolución de direcciones IP a direcciones MAC, fundamental para el funcionamiento de redes locales. Wireshark demostró ser una herramienta eficaz para la captura y análisis del tráfico de red, permitiendo una visualización clara de las solicitudes y respuestas ARP.

### Recomendaciones

- Se recomienda asegurar que todos los dispositivos en la red estén correctamente configurados con direcciones IP y MAC correspondientes para evitar problemas de conectividad.
- Utilizar Wireshark regularmente para monitorear el tráfico de red y detectar posibles problemas en el intercambio de datos.
- Mantener la tabla ARP actualizada para asegurar que las solicitudes y respuestas ARP se gestionen de manera eficiente.

### Bibliografías

Castro González, S. V., & Salvador Antón, M. C. (2011). CAPTURADOR DE PAQUETES IMPLEMENTADO EN HARDWARE. Guayaquil: ESCUELA SUPERIOR POLITECNICA DEL LITORAL. Obtenido de <https://www.dspace.espol.edu.ec/bitstream/123456789/45350/1/T-83494%20CASTRO-SALVADOR.pdf>

Tannenbaum, A. S., & Wetherall, D. J. (2011). *Redes de computadoras* (5ª ed.). Pearson Educación.

Tannenbaum, A. S., & Wetherall, D. J. (2011). *Redes de computadoras* (5ª ed.). Pearson Educación.

Wright, J. (2019). *Wireshark Network Analysis* (2ª ed.). Packt Publishing.

Kurose, J., & Ross, K. (2017). *Redes de computadoras y sistemas distribuidos* (6ª ed.). Pearson Educación.

Stallings, W. (2017). *Redes y sistemas distribuidos* (8ª ed.). Pearson.

Forouzan, B. A. (2007). *Data Communications and Networking* (4th ed.). McGraw-Hill Education.

Tanenbaum, A. S. (2003). *Computer Networks* (4th ed.). Prentice Hall.

Comer, D. E. (2018). *Computer Networks and Internets* (6th ed.). Pearson Education.