

**2025**

**TRABAJO DE LABORATORIO Nº 5**

**(Versión para desarrollo No Presencial)**

**Análisis de tramas y paquetes en redes Ethernet**

**ACTIVIDAD DE FORMACIÓN PRÁCTICA**

1. Formación experimental (laboratorio).

**OBJETIVOS**

1. Comprender el funcionamiento de los protocolos IEEE 802.3, IEEE 802.11, IEEE 802.1D, IEEE 802.1Q, ARP, IP e ICMP, en un entorno de red LAN Ethernet con acceso a Internet, mediante la observación de tramas capturadas con software de análisis.
2. Analizar el tráfico en una LAN, entre un host Tx y otro Rx, para identificar procesos de encapsulamiento y de comunicación par-par.
3. Verificar el funcionamiento de cada protocolo específico y su relación con los servicios que la capa OSI, en la que funciona cada protocolo, le proporciona a una capa superior.
4. Comprender el proceso de fragmentación y reensamble de paquetes IP, así como la incidencia de la MTU de la red en dicho proceso.

**CONOCIMIENTOS PREVIOS**

1. Redes LAN Ethernet/IEEE 802.3 – Formato de tramas y paquetes. Funcionamiento del proceso de encapsulamiento.
2. Protocolos de:
  - a. Capa de Enlace:
    - [Ethernet](#): IEEE 802.3 Ethernet
    - [IEEE 802.11](#): IEEE 802.11 wireless LANs
    - [STP](#): IEEE 802.1D Spanning Tree Protocol
    - [VLAN](#): IEEE 802.1Q Virtual Bridged Local Area Networks
  - b. Capa de Red:
    - [ARP](#): Address Resolution Protocol (ARP)
    - [IP](#): Internet Protocol (version 4)
    - [IPv6](#): Internet Protocol (version 6)
    - [ICMP](#): Internet Control Message Protocol (version 4)

Se deben conocer los formatos de las PDUs y el funcionamiento de cada protocolo, comprendiendo los campos que intervienen en cada servicio que se brinda a la capa superior.

3. Instalación y configuración del Analizador de Tramas **Wireshark, última versión.**
4. Empleo hábil de las funcionalidades del software a utilizar.
5. **EJERCICIOS RESUELTOS DE LAS GUÍAS DE EJERCICIOS DE ESCRITORIO (GEE):**

<b>2.2.1. – 2.2.2</b>	<b>Análisis</b>
<b>2.3.15. / 2.3.18.</b>	<b>Análisis</b>



UTN - FRBA

Departamento de Sistemas

**MATERIA:** Redes de Información

**NIVEL:** Cuarto

2.4.8.	Análisis
5.4.16.1 a 5.4.16.3. – 5.4.17.1. – 5.4.17.2.	Análisis
5.5.1. a 5.5.6.	Análisis
5.6.1. a 5.6.5.	Análisis
5.11.1. a 5.11.5.	Análisis

### **MATERIAL NECESARIO**

1. PC con acceso a la LAN/WLAN basada en switch / WiFi con acceso a Internet, con Analizador de Tramas **Wireshark, última versión.**

### **DESCRIPCION**

Este trabajo será desarrollado por cada alumno en una PC con acceso a LAN/WLAN Ethernet y evaluado **individualmente.**

#### **1. Caso de Estudio**

Tráfico real circulante en la red y / o generado por el alumno.

#### **2. Requerimientos para el alumno (Objetivos Técnicos)**

- a. Examinar y utilizar las funciones de análisis del software de análisis de protocolos.
- b. Comprender el funcionamiento de los siguientes protocolos mediante la verificación experimental del modelo y proceso descrito en la teoría y en las RFCs respectivas.
- c. Resguardar los archivos de capturas, para futuras actividades de laboratorio.
- d. Responder el cuestionario escrito al finalizar las tareas.

#### **3. Tareas**

Realice las siguientes tareas en el intérprete de comandos (ejecute **cmd** en Windows):

```

C:\> Símbolo del sistema
Microsoft Windows [Versión 10.0.17134.1]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Users\Usuario2024.>

```

#### **a. Análisis de la LAN / WLAN donde está su estación de trabajo**

- 1) Obtenga los datos de su Host en su entorno de LAN/WLAN con el comando **ipconfig /all** y **analice** / registre los datos obtenidos:

a) ¿Cuántas interfaces de red identifica? ¿cuáles son virtuales? ¿cuál es la interfaz real que se empleará en la red LAN y cuál en la WLAN?

b) Datos de su equipo:

Nombre del Host	
Dirección IP del Host	
Máscara de Subred del Host	
Puerta de enlace predeterminada	



<b>Dirección de Broadcast IP de la red</b>	
<b>Servidor DHCP de la Red WiFi</b>	
<b>Dirección MAC de la Placa de Red WiFi</b>	
<b>Servidor/es DNS reconocidos</b>	

- 2) Obtenga las direcciones IP conocidas por su Host en el entorno de la misma red IP para utilizarlas en el laboratorio, mediante el comando **arp - a**:

C:\>WINDOWS>arp -a

- 3) Si tiene el celular, tablet, notebook o PC conectados en la misma LAN / WLAN identifique cuáles direcciones IP y MAC corresponden a cada uno.

HOST	IP	MAC
PC		
Celular		
Notebook		
Access Point (Gateway)		

- 4) Confirme los datos con los que fueron obtenidos mediante el comando **ipconfig /all**
- 5) Verifique la correspondencia de alguna dirección IP, entre las versiones 4 y 6. Utilice una calculadora disponible en Internet (<https://www.whatsmydns.net/ipv4-to-ipv6>).
- a) Compare las diferentes formas de las notaciones IPv6.
- b) Comprenda sus usos.
- 6) ¿De qué clase es la dirección IP del Host utilizado?
- 7) ¿Cuál es su máscara de red? ¿Es una máscara por defecto o natural?
- 8) ¿La red tiene subredes?
- 9) ¿La dirección de red es pública o privada? ¿Qué otras direcciones de red de esta misma clase están reservadas? ¿para qué?
- 10) ¿Cuántos hosts puede haber en la red como máximo?
- 11) ¿Cuál es el estándar IEEE que se emplea en esta red? ¿Qué método de Control de Acceso utiliza, CSMA/CD o CSMA/CA?
- 12) ¿Es una red que detecta colisiones? En caso afirmativo, ¿Cuántos dominios de colisión tiene?
- 13) ¿Es una red que previene colisiones? En caso afirmativo, ¿Qué problemas resuelve CSMA/CA que no resuelve CSMA/CD?
- 14) ¿Es una red que utiliza broadcast de direcciones MAC? En caso afirmativo, ¿Cuántos dominios de broadcast tiene? ¿Qué protocolos en entorno LAN/WLAN utilizan broadcast de capa 2 para funcionar?
- 15) En una LAN ¿cómo se puede segmentar un dominio de colisión?
- 16) En una LAN ¿cómo se puede segmentar un dominio de broadcast?



- 17) ¿Esta red emplea direccionamiento IP estático o dinámico? ¿Qué protocolo se utiliza para asignación dinámica de direcciones IP y cuántas PDU se intercambian entre el cliente y el servidor?
- 18) Identifique direcciones IP públicas conocidas por su Host.

**b. Análisis de una trama Ethernet**

Inicie una captura con el Analizador y haga PING al Gateway (puerta de enlace) o a otro host de su misma LAN/WLAN (puede ser su móvil u otro dispositivo conectado a su LAN/WLAN). Detenga la captura. Responda las siguientes preguntas, analizando una trama en particular:

- 1) ¿Cuáles son los campos de la trama? ¿Qué valores tiene cada campo y cuál es su significado?
- 2) ¿Qué tamaño tiene el encabezado de la trama y cuáles son sus campos?
- 3) ¿Qué tamaño tiene la cola de su trama? ¿Qué campo sirve para detectar errores y cuál es su valor?
- 4) ¿Cuántos bytes corresponden a los datos? ¿Este campo es de tamaño fijo o variable? En este nivel ¿el campo de datos tiene una longitud mínima, máxima o no está especificado por su estándar?
- 5) Revisando nuevamente la trama Ethernet ¿qué campos se corresponden con los especificados en IEEE 802.2 y cuáles a IEEE 802.3?
- 6) ¿Qué protocolos de nivel 3 (TCP/IP) se encapsularon en las tramas?
- 7) ¿Qué protocolos de nivel 4 y 5 (TCP/IP) se encapsularon en la trama?

**c. Estudio comparativo de tramas típicas de LAN Ethernet**

Agregue a la captura de tramas [Ethernet](https://wiki.wireshark.org/): IEEE 802.3 ó 802.11, las capturas en su red o ejemplos del sitio <https://wiki.wireshark.org/> que se correspondan con:

- [IEEE 802.11](#): IEEE 802.11 wireless LANs
- [STP](#): IEEE 802.1D Spanning Tree Protocol
- [VLAN](#): IEEE 802.1Q Virtual Bridged Local Area Networks

Realice un estudio comparativo de los 4 tipos de tramas, identificando las funciones particulares de la capa de enlace, qué campos intervienen en cada caso, los procesos que intervienen en el Tx y en el Rx, señalando similitudes y diferencias.

**d. Análisis del tráfico ARP**

Realice las siguientes tareas en el intérprete de comandos (cuando sea necesario ejecute el comando con permisos de *Administrador*) y capture una o más tramas auxiliándose con el analizador de protocolos:

- 1) Observe el estado de la memoria caché de ARP en su PC.  
`C:\>WINDOWS>arp -a`
- 2) Borre la memoria caché de ARP en su PC.  
`C:\>WINDOWS>arp -d <dirección IP>`
- 3) Inicie una captura con el Analizador y haga PING a otra PC, host o dispositivo de la misma LAN/WLAN o al Gateway de su red. Detenga la captura.

Responda:



- a) ¿En qué nivel del modelo OSI funciona el protocolo ARP?
  - b) ¿Cuántas PDU intervienen en la resolución ARP?
  - c) Describa la secuencia de tramas involucradas, justificando todas las direcciones MAC e IP que aparecen.
  - d) ¿Cuál es el estado actual de la memoria caché de ARP?
  - e) Volver a ejecutar el comando Ping a la misma máquina y observar la secuencia de tramas ARP. ¿Aparecen las mismas tramas ARP? ¿Por qué?
  - f) ¿Qué formato tiene una PDU ARP?
- 4) Abra una página en Internet que no haya abierto desde que encendió la PC. Capture el tráfico involucrado.
- a) Responda las mismas preguntas que en el ejercicio anterior.
  - b) ¿Los Hosts que intervienen en esta captura son los mismos que en el caso anterior?

**c) ¿Cómo se llama a este mecanismo de ARP?**

**e. Análisis del tráfico IP e ICMP**

Realice las siguientes tareas en el intérprete de comandos y registre lo obtenido, auxiliándose con el analizador de protocolos:

Responda las siguientes preguntas para cada caso:

- 1) Al hacer Ping a la dirección IP de su PC.
- 2) Al hacer Ping a otra PC, host o Gateway de la LAN o WLAN.
- 3) Al hacer Ping a la dirección IP de un sitio de Internet no disponible en caché (por ej: a una web de otro país no visitada habitualmente).

Preguntas	Caso 1)	Caso 2)	Caso 3)
a) ¿Se ejecutó la aplicación Ping?			
b) ¿Salen paquetes hacia la red? ¿Cuántos?			
c) ¿Qué tamaño tiene cada paquete?			
d) ¿Cuántos bytes corresponden a cada protocolo?			
e) ¿Cuántos bytes corresponden a los datos transmitidos?			

- 4) Al hacer Ping ¿cuántas capas del Modelo OSI y qué protocolos intervienen? ¿Qué tipos y códigos de mensaje ICMP se observaron en los casos analizados?



UTN - FRBA

Departamento de Sistemas

**MATERIA:** Redes de Información

**NIVEL:** Cuarto

**f. Análisis del MTU de la red**

Ejecute la aplicación COMMAND o en Programas el icono MS-DOS e inicie una nueva captura con el analizador de protocolos. Utilice para el tamaño de paquetes el parámetro -l de la aplicación Ping.

Realice las siguientes tareas en el intérprete de comandos y registre lo obtenido:

**1) Ping a una PC o terminal con tamaño de paquete de 200 bytes.**

(C:\>WINDOWS>ping -l 200 <dirección IP>)

**2) Ídem con 1499 bytes.**

**3) Ídem con 2000 bytes**

Responda las siguientes preguntas para cada ítem:

- a) ¿En qué caso se fragmentaron los paquetes? ¿A cuántos bytes se produjo la fragmentación?
- b) ¿Qué campos de que protocolos intervienen en la fragmentación?
- c) ¿Qué tamaño tiene cada paquete?
- d) ¿Cuántos bytes corresponden a cada protocolo?
- e) ¿Cuántos bytes corresponden a los datos transmitidos?
- f) ¿Qué valor de tamaño de paquete tiene el umbral de fragmentación?  
¿es constante o variable?

**4) Calcule un valor umbral de Bytes, que deben ser configurados como parámetro en la aplicación Ping, para que el datagrama IP se fragmente en 15 paquetes. Verifíquelo en la PC.**

**TIEMPO ASIGNADO:** 120 minutos