Imagen que contiene Icono

Descripción generada automáticamenteDibujo en blanco y negro

Descripción generada automáticamente con confianza bajaINSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE COMPUTO

Laboratorio de redes de computadoras

PRACTICA 6

CAPTURA Y ANÁLISIS DE PAQUETES CON WIRESHARK

NOMBRE DEL ALUMNO: GARCÍA QUIROZ GUSTAVO IVAN

GRUPO: 5CV4

**NOMBRE DEL PROFESOR:** ALCARAZ TORRES JUAN JESUS

16/12/2023

Índice

[Objetivos: 3](#_Toc153463688)

[Requerimientos: 3](#_Toc153463689)

[Marco teórico 4](#_Toc153463690)

[Wireshark 4](#_Toc153463691)

[Desarrollo: 6](#_Toc153463692)

[Uso de Wireshark para examinar las tramas de Ethernet 6](#_Toc153463693)

[Analizar las tramas y paquetes de las siguientes direcciones: 8](#_Toc153463694)

[Encabezado IP (Capa de red) 8](#_Toc153463695)

[Trama Ethernet 2 (Capa de Enlace de Datos) 8](#_Toc153463696)

[Encabezado TCP (capa de Transporte) 8](#_Toc153463697)

[Encabezado UDP (capa de Transporte) 8](#_Toc153463698)

[Conclusión 13](#_Toc153463699)

[Bibliografía 14](#_Toc153463700)

## Objetivos:

* Aprender a utilizar Wireshark para capturar y analizar paquetes de red.
* Identificar los diferentes tipos de paquetes de red y sus campos.
* Analizar el tráfico de red para identificar problemas de rendimiento y seguridad.
* Identificar los protocolos de red utilizados en la comunicación entre dispositivos.
* Identificar los dispositivos de red que están generando tráfico en la red.

## Requerimientos:

* 1 Computadora Personal.
* Software para simulación de redes.

# Marco teórico

Cuando dos aplicaciones se comunican a través de la red, éstas generan PDU’s con datos de aplicación que es necesario encapsular dentro de otros PDU’s de capas inferiores y poder dar así un buen tratamiento a los datos enviados. Dos de las principales capas son la capa de red (Internet) y la capa de Transporte, en las cuales se manejan datos sensibles, tales como las direcciones lógicas de los dispositivos de red que contienen dichas aplicaciones y los identificadores de estas aplicaciones (# de puerto).

## Wireshark

Wireshark es una herramienta muy conocida dentro de los analizadores de protocolos (*sniffers*) que permite leer la información contenida dentro de los distintos PDU’s de un paquete que viaja por la red. A continuación mostraremos un ejemplo de una trama (Capa 2) capturada con Wireshark.

Observe la siguiente trama capturada con la herramienta wireshark :

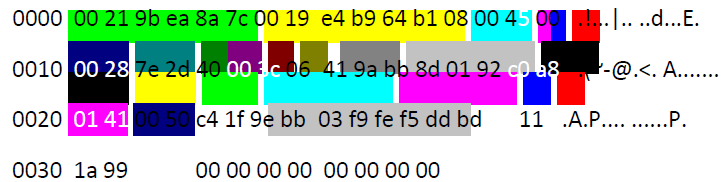


Imagen trama capturada con la herramienta wireshark

Ésta trama puede ser desencapsulada de la siguiente manera:

* Trama Ethernet2 (Capa de Enlace de Datos)

1. MAC Destino: 00:21:9b:ea:8a:7c

O MAC Origen: 00:19:e4:b9:64:b1

o Tipo de trama: IP(0x800)

* 1. Trailer: 000000000000
* Paquete IP (Capa de Red)

o Versión: 4

o Longitud encabezado: 5 (palabras de 32 bits=20 bytes) o TOS: 0

o Longitud total del paquete: 40 palabras de 32 bits(0028)=160 bytes

o Identificador: 32301(0x7e2d)

o Banderas: No fragmentar (0x04)

o Offset: 0(0x00)

o TTL: 60 (0x3c)

o Protocolo: TCP (0x06) //RFC 1340

o Checksum: 0x419a

o IP Origen: 187.141.1.146 (bb8d0192)

o IP destino: 192.168.1.65 (c0a80141)

* Segmento TCP (capa de Transporte)
  1. Puerto Origen: 80 (0x0050) //http RFC 1340
  2. Puerto Destino: 50207 (0xc41f)
  3. Número de secuencia: 2663056377 (0x9ebb03f9)
  4. Número de acuse: 4277525949 (0xfef5ddbd)
  5. Longitud de encabezado: 20 bytes (0x05)

o Banderas: 0x11 (ACK + FIN)

Texto

Descripción generada automáticamente con confianza media

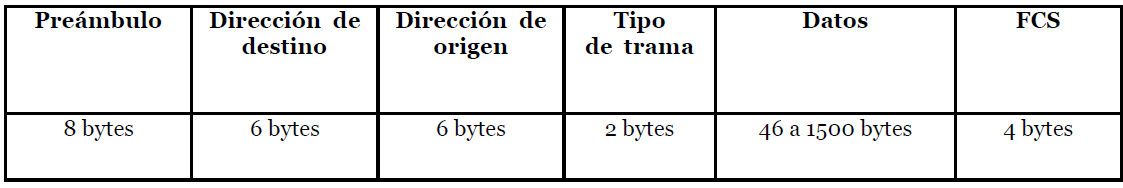
1. Tamaño ventana: 6809 (0x1a99)

o Checksum: 0xd259

# Desarrollo:

# Uso de Wireshark para examinar las tramas de Ethernet

**Paso 1: Revisar las descripciones y las longitudes de los campos de encabezado de Ethernet II**



**Paso 2: Examinar el contenido de encabezado de Ethernet II de una solicitud de ARP**

En la tabla siguiente, se toma la primera trama de la captura de Wireshark y se muestran los datos de los campos de encabezado de Ethernet II.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | **Campo** |  |  |  | **Valor** |  |  |  |  | **Descripción** |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Preámbulo | | |  | No se muestra en la | | |  | Este campo contiene bits de sincronización, procesados por | | | |
|  |  |  |  |  | captura. | | |  | el hardware de NIC. | | | |
|  |  | | |  |  | | |  |  | | | |
|  | Dirección de destino | | |  | Broadcast | | |  | Direcciones de la Capa 2 para la trama. Cada dirección tiene | | | |
|  |  |  |  |  | (ff:ff:ff:ff:ff:ff) | | |  | una longitud de 48 bits, o seis octetos, expresada como 12 | | | |
|  |  |  |  |  |  |  |  |  | dígitos hexadecimales, 0-9, A-F. Un formato común | | | |
|  | Dirección de origen | | |  | Dell\_24:2a:60 | | |  |
|  |  |  | es 12:34:56:78:9A:BC. | | | |
|  |  |  |  |  | (5c:26:0a:24:2a:60) | | |  |
|  |  |  |  |  |  | Los primeros seis números hexadecimales indican el | | | |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | fabricante de la tarjeta de interfaz de red (NIC); los seis | | | |
|  |  |  |  |  |  |  |  |  | últimos números hexadecimales corresponden al número de | | | |
|  |  |  |  |  |  |  |  |  | serie de la NIC. | | | |
|  |  |  |  |  |  |  |  |  | La dirección de destino puede ser un broadcast, que contiene | | | |
|  |  |  |  |  |  |  |  |  | todos unos, o un unicast. La dirección de origen es siempre | | | |
|  |  |  |  |  |  |  |  |  | unicast. |  |  |  |
|  | Tipo de trama | | |  | 0x0806 | | |  | Para las tramas de Ethernet II, estos campos contienen un | | | |
|  |  |  |  |  |  |  |  |  | valor hexadecimal que se utiliza para indicar el tipo de | | | |
|  |  |  |  |  |  |  |  |  | protocolo de capa superior en el campo de datos. Existen | | | |
|  |  |  |  |  |  |  |  |  | muchos protocolos de capa superior que admite Ethernet II. | | | |
|  |  |  |  |  |  |  |  |  | Dos tipos comunes de trama son: | | | |
|  |  |  |  |  |  |  |  |  | Valor | Descripción | | |
|  |  |  |  |  |  |  |  |  | 0x0800 | Protocolo IPv4 | | |
|  |  |  |  |  |  |  |  |  | 0x0806 Protocolo de resolución de direcciones (ARP) | | | |
|  | Datos | | |  | ARP | | |  | Contiene el protocolo de nivel superior encapsulado. El | | | |
|  |  |  |  |  |  |  |  |  | campo de datos está entre 46 y 1,500 bytes. | | | |
|  |  | | |  |  | | |  |  | | | |
|  | FCS | | |  | No se muestra en la | | |  | Secuencia de verificación de trama, utilizada por la NIC para | | | |
|  |  |  |  |  | captura. | | |  | identificar errores durante la transmisión. El valor lo | | | |
|  |  |  |  |  |  |  |  |  | computa la máquina de envío, abarcando las direcciones de | | | |
|  |  |  |  |  |  |  |  |  | trama, campos de datos y tipo. El receptor lo verifica | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

# Analizar las tramas y paquetes de las siguientes direcciones:

Capture por lo menos 10 paquetes utilizando Wireshark y para cada uno de ellos rellene los siguientes encabezados

### Encabezado IP (Capa de red)

Un conjunto de letras negras en un fondo blanco

Descripción generada automáticamente con confianza media

### Trama Ethernet 2 (Capa de Enlace de Datos)

Texto, Carta

Descripción generada automáticamente

### Encabezado TCP (capa de Transporte)

Imagen que contiene Diagrama

Descripción generada automáticamente

### Encabezado UDP (capa de Transporte)

Tabla

Descripción generada automáticamente

1. Análisis de una **IP** de una **máquina de laboratorio**

|  |  |  |  |
| --- | --- | --- | --- |
| 4 | 32 bits | IPv4 | 60 |
| 0x42bd (17085) | | 0X00 | 0 |
| 128 | ICMP | 0xe586 | |
| 8.40.1.23 | | | |
| 8.40.1.12 | | | |
| - | | - | |

¿Cuál es la MAC destino?

40-5B-D8-30-F8-A1

¿Cuál es la IP destino?

8.40.1.12

c) En el campo Protocol ¿Cuál es el valor del campo?

ICMP

1. Análisis de una **IP** de la pagina [**www.escom.ipn.mx**](http://www.escom.ipn.mx)

|  |  |  |  |
| --- | --- | --- | --- |
| 4 | IHL | IPv4 | 60 |
| 0x86c4(34500) | | 0X02 | 0 |
| 128 | TCP | 0x0000 | |
| 187.189.146.143 | | | |
| 186.96.42.179 | | | |
| - | | - | |

d) ¿Cuál es la MAC destino?

40-5B-D8-30-F8-A1

e) ¿Cuál es la IP destino?

186.96.42.179

f) En el campo Protocol ¿Cuál es el valor del campo?

TCP

1. Análisis de una **IP** de la pagina [**www.saes.escom.ipn.mx**](http://www.saes.escom.ipn.mx)

|  |  |  |  |
| --- | --- | --- | --- |
| 4 | 20 bits | IPv4 | 60 |
| 0x86c4(34500) | | 0X00 | 0 |
| 128 | ICMP | 0x00000 | |
| 187.189.146.143 | | | |
| 148.204.56.240 | | | |
| - | | - | |

g) ¿Cuál es la MAC destino?

40-5B-D8-30-F8-A1

h) ¿Cuál es la IP destino?

148.204.56.240

i) En el campo Protocol ¿Cuál es el valor del campo?

ICMP

1. Análisis de una **IP 148.204.56.254**

|  |  |  |  |
| --- | --- | --- | --- |
| 4 | 20 bits | IPv4 | 20 |
| 0x86c4(34500) | | 0X00 | 0 |
| 128 | ICMP | 0x4D52 | |
| 187.189.146.143 | | | |
| 148.204.56.254 | | | |
| - | | - | |

j) ¿Cuál es la MAC destino?

40-5B-D8-30-F8-A1

k) ¿Cuál es la IP destino?

148.204.56.240

l) En el campo Protocol ¿Cuál es el valor del campo?

ICMP

1. Análisis de una **IP 148.204.61.254**

|  |  |  |  |
| --- | --- | --- | --- |
| 4 | 20 bits | IPv4 | 60 |
| 0x86c4(34500) | | 0X00 | 0 |
| 128 | ICMP | 0x1566 | |
| 187.189.146.143 | | | |
| 148.204.61.254 | | | |
| - | | - | |

m) ¿Cuál es la MAC destino?

40-5B-D8-30-F8-A1

n) ¿Cuál es la IP destino?

148.204.61.254

o) En el campo Protocol ¿Cuál es el valor del campo?

ICMP

1. Análisis de una de la pagina [**www.ipn.mx**](http://www.ipn.mx)**[www.ipn.mx](http://www.ipn.mx)**

|  |  |  |  |
| --- | --- | --- | --- |
| 4 | IHL | IPv4 | 20 |
| 0x86c4(34500) | | 0X00 | 0 |
| 128 | ICMP | 0x4D52 | |
| 187.189.146.143 | | | |
| 104.214.26.43 | | | |
| - | | - | |

p) ¿Cuál es la MAC destino?

40-5B-D8-30-F8-A1

q) ¿Cuál es la IP destino?

104.214.26.43

r) En el campo Protocol ¿Cuál es el valor del campo?

ICMP

1. Análisis de una de la pagina [**www.google.com.mx**](http://www.google.com.mx)

|  |  |  |  |
| --- | --- | --- | --- |
| 4 | 20 bytes | IPv4 | 60 |
| 0x86c4(34500) | | 0X00 | 0 |
| 128 | ICMP | 0x00000 | |
| 187.189.146.143 | | | |
| 142.250.69.36 | | | |
| - | | - | |

s) ¿Cuál es la MAC destino?

40-5B-D8-30-F8-A1

t) ¿Cuál es la IP destino?

142.250.69.36

u) En el campo Protocol ¿Cuál es el valor del campo?

ICMP

1. Análisis de una de la pagina [**www.facebook.com**](http://www.facebook.com)

|  |  |  |  |
| --- | --- | --- | --- |
| 4 | 20 bytes | IPv4 | 60 |
| 0x86c4(34500) | | 0X00 | 0 |
| 128 | ICMP | 0x4a6c | |
| 187.189.146.143 | | | |
| 8.40.1.27 | | | |
| - | | - | |

v) ¿Cuál es la MAC destino?

40-5B-D8-30-F8-A1

w) ¿Cuál es la IP destino?

8.40.1.27

x) En el campo Protocol ¿Cuál es el valor del campo?

ICMP

1. Análisis de una de la pagina [**www.epicgames.com**](http://www.epicgames.com)

|  |  |  |  |
| --- | --- | --- | --- |
| 4 | 20 bytes | IPv4 | 60 |
| 0x86c4(34500) | | 0X00 | 0 |
| 128 | ICMP | 0x00000 | |
| 187.189.146.143 | | | |
| 54.156.160.50 | | | |
| - | | - | |

y) ¿Cuál es la MAC destino?

40-5B-D8-30-F8-A1

z) ¿Cuál es la IP destino?

54.156.160.50

aa) En el campo Protocol ¿Cuál es el valor del campo?

ICMP

1. Análisis de una **IP 148.204.1.2**

|  |  |  |  |
| --- | --- | --- | --- |
| 4 | 20 bytes | IPv4 | 60 |
| 0x86c4(34500) | | 0X00 | 0 |
| 128 | ICMP | 0x00000 | |
| 187.189.146.143 | | | |
| 54.156.160.50 | | | |
| - | | - | |

* 1. ¿Cuál es la MAC destino?
  2. ¿Cuál es la IP destino?
  3. En el campo Protocol ¿Cuál es el valor del campo?

1. Capturar una trama ARP (mandar un ping a la **IP** ping **148.204.56.255**) y rellenar los campos

|  |  |  |  |
| --- | --- | --- | --- |
| 4 | 20 bytes | IPv4 | 60 |
| 0x86c4(34500) | | 0X00 | 0 |
| 128 | ICMP | 0x00000 | |
| 187.189.146.143 | | | |
| 54.156.160.50 | | | |
| - | | - | |

Texto

Descripción generada automáticamente Forma, Rectángulo

Descripción generada automáticamente

**Reflexión**

11. ¿Por qué Wireshark muestra la dirección MAC vigente de los hosts locales, pero no la

dirección MAC vigente de los hosts remotos?

Porque la dirección MAC es una de capa 2, ósea que no trasciende al dominio de colisión, por lo

que todo paquete dirigido a algún host queda fuera de este dominio.

12. ¿Cuál es la importancia del análisis de una red con el programa Wireshark?

Para poder analizar las tramas y paquetes en una red, así como saber que datos son importantes

como los protocolos que están usando.

## Conclusión

La configuración de enrutamiento estático y conmutación multicapa en un entorno de red es fundamental para lograr un rendimiento óptimo y una segmentación eficiente del tráfico. La implementación de VLANs y la asignación de puertos a estas VLANs permiten crear segmentos de red virtuales que pueden comunicarse entre sí mediante un switch-multicapa que también funciona como router.

La configuración de enrutamiento estático proporciona rutas predefinidas entre diferentes redes, lo que es esencial para la comunicación entre VLANs y subredes. Esto mejora la eficiencia del tráfico y permite una administración más controlada de la red.

La conmutación multicapa, que combina las funciones de un switch y un router en un solo dispositivo, es crucial para minimizar la latencia y mejorar el rendimiento de la red. Permite que las VLANs se comuniquen entre sí dentro del mismo dispositivo, evitando la necesidad de enviar todo el tráfico a través de un router externo.

En resumen, la configuración de enrutamiento estático y conmutación multicapa en una red proporciona flexibilidad, eficiencia y un mejor control del tráfico, contribuyendo a un entorno de red más seguro y eficaz. La correcta implementación de estas configuraciones es esencial para optimizar el rendimiento y la seguridad de la red.

## Bibliografía

Walton, A. (2020, junio 8). *Configuración Básica del Router*. CCNA desde Cero. https://ccnadesdecero.es/configuracion-basica-router/