INSTITUTO 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

18/12/2023

Índice

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 :

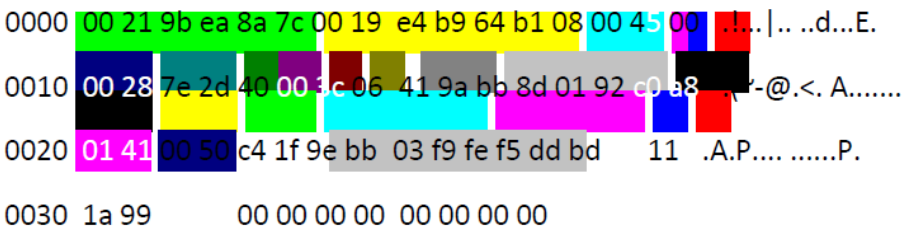


Imagen 1 trama capturada con la herramienta wireshark

Ésta trama puede ser desencapsulada de la siguiente manera:

- Trama Ethernet2 (Capa de Enlace de Datos)
  - MAC Destino: 00:21:9b:ea:8a:7c
  - MAC Origen: 00:19:e4:b9:64:b1
  - Tipo de trama: IP(0x800)
  - Trailer: 000000000000
- Paquete IP (Capa de Red)
- Versión: 4
- Longitud encabezado: 5 (palabras de 32 bits=20 bytes) ○ TOS: 0
- Longitud total del paquete: 40 palabras de 32 bits(0028)=160 bytes
- Identificador: 32301(0x7e2d)
- Banderas: No fragmentar (0x04)
- Offset: 0(0x00)
- TTL: 60 (0x3c)
- Protocolo: TCP (0x06) //RFC 1340
- Checksum: 0x419a

- IP Origen: 187.141.1.146 (bb8d0192)
- IP destino: 192.168.1.65 (c0a80141)

- Segmento TCP (capa de Transporte)

  - Puerto Origen: 80 (0x0050) //http RFC 1340
  - Puerto Destino: 50207 (0xc41f)
  - Número de secuencia: 2663056377 (0x9ebb03f9)
  - Número de acuse: 4277525949 (0xfef5ddbd)
  - Longitud de encabezado: 20 bytes (0x05)
  - Banderas: 0x11 (ACK + FIN)
    - 0_____: Reducción de ventana por congestión
    - _0_____: ECN-Echo (Notificación explícita de congestión)
    - __0_____: Urgente
    - ___1____: ACK
    - ____0___: PUSH
    - _____0 : RESET
    - ______0_: SYN
    - _____1: FIN
  - Tamaño ventana: 6809 (0x1a99)
  - 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

Preámbulo	Dirección de destino	Dirección de origen	Tipo de trama	Datos	FCS
8 bytes	6 bytes	6 bytes	2 bytes	46 a 1500 bytes	4 bytes

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

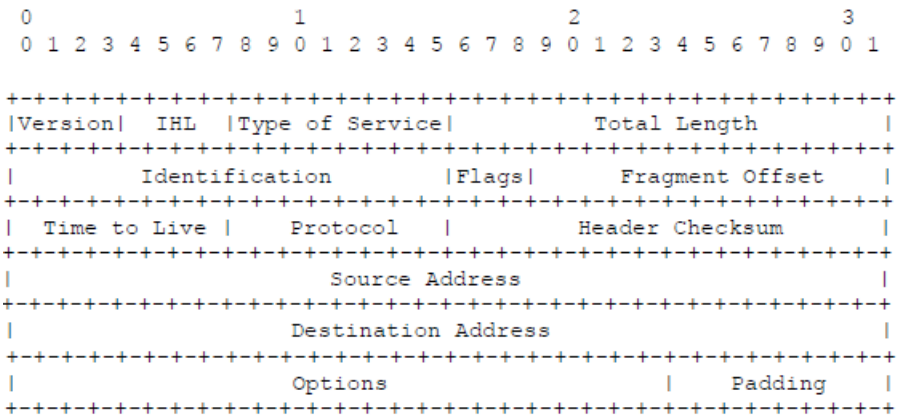
En la tabla siguiente, se toma la primera trama de la captura de Wireshark y se muestran los datos de los campos de encabezado de Ethernet II.

Campo	Valor	Descripción
Preámbulo	No se muestra en la captura.	Este campo contiene bits de sincronización, procesados por el hardware de NIC.
Dirección de destino	Broadcast (ff:ff:ff:ff:ff:ff)	Direcciones de la Capa 2 para la trama. Cada dirección tiene una longitud de 48 bits, o seis octetos, expresada como 12 dígitos hexadecimales, `0-9, A-F`. Un formato común es `12:34:56:78:9A:BC`. 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.
Dirección de origen	Dell_24:2a:60 (5c:26:0a:24:2a:60)	
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 captura.	Secuencia de verificación de trama, utilizada por la NIC para 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

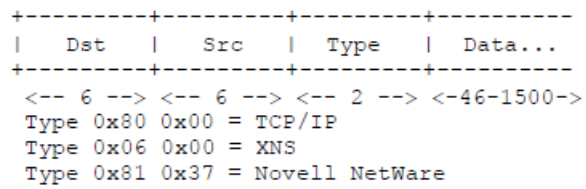
Analizar las tramas y paquetes de las siguientes direcciones:

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

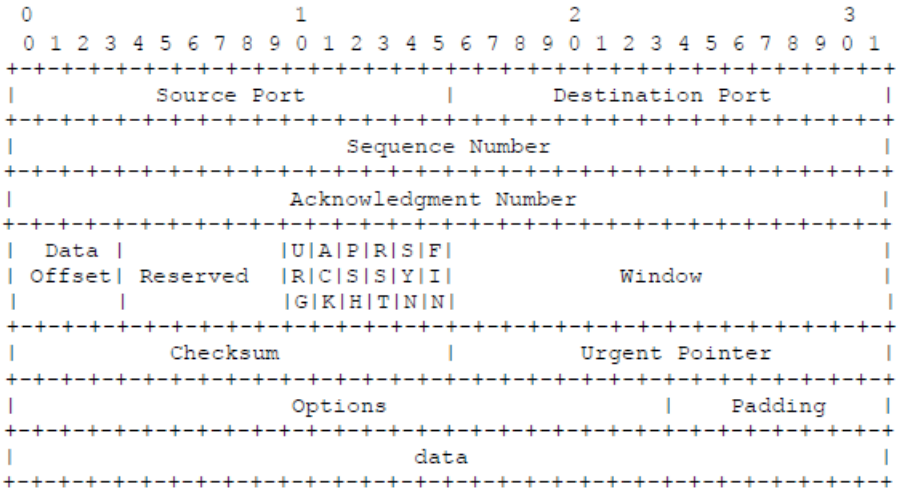
Encabezado IP (Capa de red)



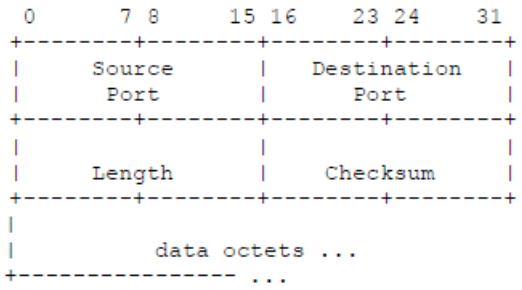
Trama Ethernet 2 (Capa de Enlace de Datos)



Encabezado TCP (capa de Transporte)



Encabezado UDP (capa de Transporte)



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

2. Análisis de una **IP** de la pagina **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

3. Análisis de una **IP** de la pagina **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

4. 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

5. 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

6. Análisis de una de la pagina **www.ipn.mx**

4	20 bytes	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

7. Análisis de una de la pagina **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

8. Análisis de una de la pagina **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

9. Análisis de una de la pagina **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

10. Análisis de una **IP 148.204.1.2**

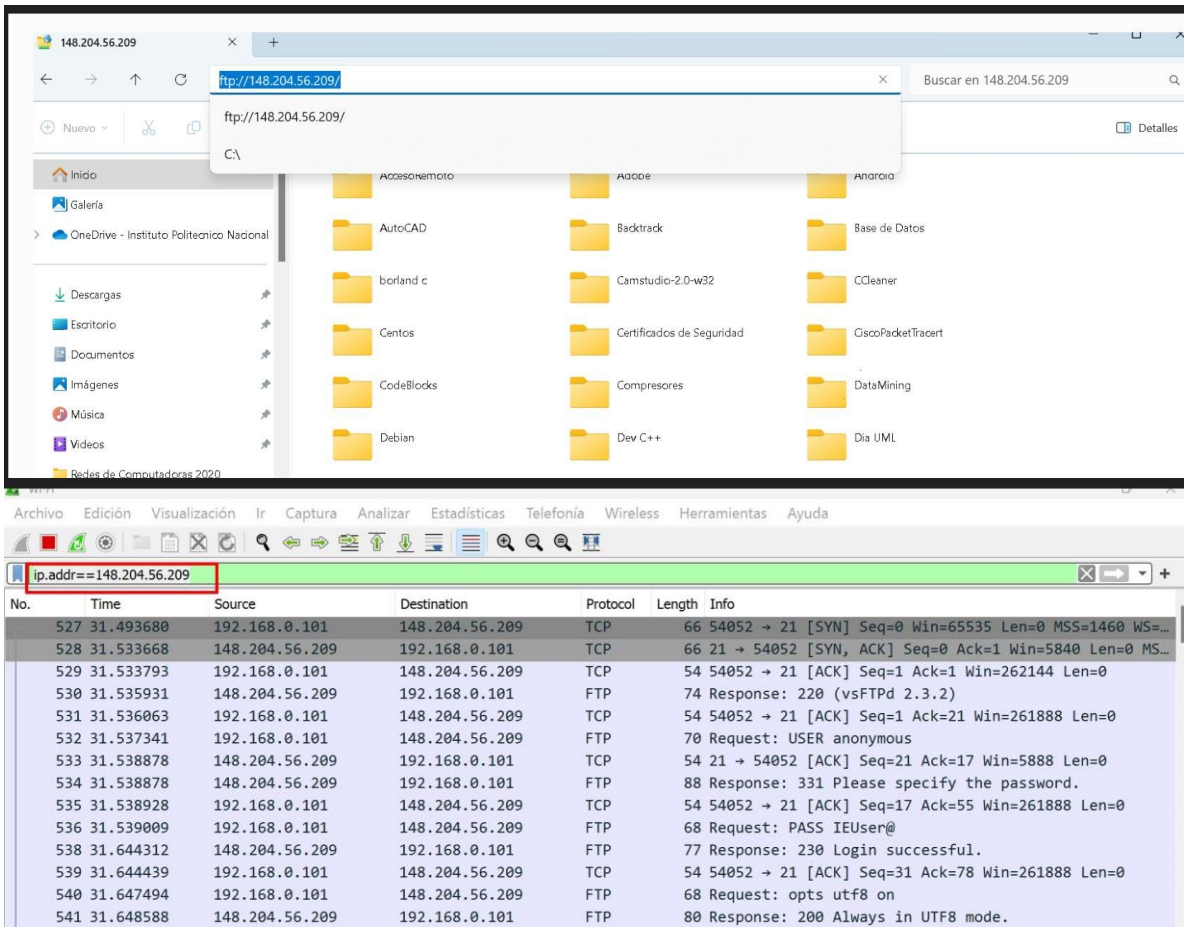
4	20 bytes	IPv4	60
0x86c4(34500)		0X00	0
128	ICMP	0x00000	
187.189.146.143			
148.204.1.2			
-		-	

bb) ¿Cuál es la MAC destino?
40-5B-D8-30-F8-A1
cc) ¿Cuál es la IP destino?
148.204.1.2
dd) En el campo Protocol ¿Cuál es el valor del campo?
ICMP

11. 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			
148.204.56.255			
-		-	

12. Incluir el filtro ip.addr==148.204.56.209 en el análisis de Wireshark. Posteriormente para que les capture abren explorador de archivos y colocan la dirección ftp://148.204.56.209 y realizan su análisis de su captura



El filtro ip.addr==148.204.56.209 en Wireshark se utiliza para limitar la visualización de paquetes a aquellos que involucran la dirección IP específica 148.204.56.209, ya sea como dirección de origen o destino. Esto es útil cuando se desea enfocar el análisis en la comunicación con un host específico.Al abrir el explorador de archivos y acceder a la dirección ftp://148.204.56.209, estás realizando una conexión FTP a ese servidor.

Durante esta actividad, Wireshark capturará los paquetes relacionados con la transferencia de archivos a través de FTP y mostrará información detallada sobre estos en su interfaz.

4	20 bytes	IPv4	60
0x86c4(34500)		0X00	0
128	ICMP	0x00000	
187.189.146.143			
148.204.56.209			
-		-	

Reflexión

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

Wireshark muestra las direcciones MAC locales porque captura el tráfico en la interfaz de red de tu dispositivo, donde puede ver y analizar los paquetes que entran y salen. Sin embargo, para los hosts remotos, solo puede ver la dirección MAC del router o dispositivo intermedio más cercano,

ya que los paquetes enviados a través de la red pública generalmente tienen la dirección MAC del enrutador como destino.

Las direcciones MAC locales se utilizan para la comunicación en la red local, mientras que las direcciones MAC remotas se vuelven más evidentes cuando los paquetes atraviesan varios dispositivos de red en su ruta hacia el destino final.

12. ¿Cuál es la importancia del análisis de una red con el programa Wireshark?
El análisis de una red con Wireshark es importante por varias razones:

Diagnóstico de Problemas:
Permite identificar y solucionar problemas de red, como cuellos de botella, errores de configuración o mal funcionamiento de dispositivos.

Seguridad de la Red:
Facilita la detección de actividades maliciosas, como intrusiones o ataques, al analizar el tráfico en busca de patrones sospechosos.

Optimización del Rendimiento:
Ayuda a optimizar el rendimiento de la red al identificar el tráfico innecesario, la congestión y otros factores que pueden afectar la eficiencia.

Monitoreo del Tráfico:
Permite monitorear el tráfico en tiempo real, lo que es esencial para comprender el comportamiento de la red y tomar decisiones informadas sobre su gestión.

Resolución de Problemas de Aplicaciones:
Facilita la identificación de problemas relacionados con aplicaciones al analizar cómo se comunican a través de la red y detectar posibles fallos o retrasos.

Cumplimiento de Políticas de Seguridad:
Ayuda a garantizar que la red cumpla con las políticas de seguridad establecidas al identificar cualquier actividad que pueda violar estas políticas.

Conclusión

Wireshark, como herramienta de captura y análisis de tráfico IP, despliega una relevancia fundamental en el ámbito de la gestión de redes al ofrecer una panorámica detallada de la comunicación entre dispositivos. Esta herramienta, al permitir la inspección minuciosa de datos como direcciones IP de origen y destino, direcciones MAC, paquetes IPv4, entre otros, se convierte en un pilar esencial para diversos aspectos de la administración de redes.

En primer lugar, la capacidad de Wireshark para diagnosticar problemas en la red es insustituible. Al analizar paquetes capturados, los administradores pueden identificar cuellos de botella, errores de configuración y mal funcionamiento de dispositivos. La información detallada sobre direcciones IP y MAC permite rastrear el flujo de datos y determinar rápidamente la fuente de problemas potenciales, agilizando así el proceso de resolución.

La seguridad de la red también se ve fortalecida mediante el uso de Wireshark. Al examinar el tráfico en busca de patrones sospechosos, los administradores pueden detectar actividades maliciosas, intrusiones o intentos de ataque. La capacidad de Wireshark para proporcionar información detallada sobre cada paquete facilita la identificación de comportamientos anómalos, permitiendo respuestas rápidas y eficaces para proteger la integridad de la red.

El monitoreo del tráfico en tiempo real es una característica distintiva de Wireshark. Al visualizar la actividad de la red en tiempo real, los administradores pueden comprender mejor el comportamiento dinámico de los dispositivos y las aplicaciones. La información detallada sobre direcciones IP y MAC permite una supervisión efectiva, lo que resulta esencial para anticipar y abordar problemas antes de que afecten significativamente el rendimiento de la red.

Por último, Wireshark contribuye al cumplimiento de políticas de seguridad al permitir la identificación de cualquier actividad que pueda violar estas políticas. El análisis detallado de paquetes posibilita la supervisión efectiva para asegurar que la red opere de acuerdo con las normativas establecidas.

En conclusión, Wireshark emerge como una herramienta integral que proporciona una visión profunda y detallada del tráfico de red. Al destacar información clave como direcciones IP y MAC, la herramienta permite a los administradores de red abordar problemas, mejorar la seguridad, optimizar el rendimiento y garantizar el cumplimiento de políticas. En última instancia, Wireshark se erige como un aliado inestimable en la tarea de mantener la integridad y eficacia de las infraestructuras de red.

Bibliografía

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