Instrucciones

Parte 1: Examinar los campos de encabezado de una trama de Ethernet II

I En la parte 1, examinará los campos de encabezado y el contenido de una trama de Ethernet II. Se utilizará una captura de Wireshark para examinar el contenido de esos campos.

En este ejemplo, la dirección IP del host de esta PC es 192.168.1.147 y la puerta de enlace predeterminada tiene una dirección IP de 192.168.1.1.

C:\> ipconfig /all (comando ejecutado en host local)

Dirección IPv4. . . . . : 192.168.8.100

Máscara de subred . . . . . : 255.255.255.0

Puerta de enlace predeterminada . . . . . : 192.168.8.1

Paso 3: Examinar las tramas de Ethernet en una captura de Wireshark

Las imágenes de la captura de Wireshark a continuación muestran los paquetes generados por un ping emitido desde un host de PC a su puerta de enlace predeterminada. Se le aplicó un filtro a Wireshark para ver solamente el protocolo de resolución de direcciones (ARP) y el protocolo de mensajes de control de Internet (ICMP). ARP significa protocolo de resolución de direcciones. ARP es un protocolo de comunicación que se utiliza para determinar la dirección MAC asociada a la dirección IP. La sesión comienza con una consulta ARP para obtener la dirección MAC del router de la puerta de enlace seguida de cuatro solicitudes y respuestas de ping.

¿Qué característica significativa tiene el contenido del campo de dirección de destino?

Que no va dirigido a un host en concreto si no a todos a través del broadcast

¿Por qué envía la PC un ARP de difusión antes de enviar la primera solicitud de ping?

Porque no conoce la mac del host al que tiene que hacer el ping

¿Cuál es la dirección MAC del origen en la primera trama?

50:cf:c8

¿Cuál es el ID de proveedor (OUI) de la NIC de origen en la respuesta ARP?

30:46:9a

¿Qué porción de la dirección MAC corresponde al OUI?

Los primeros 6 números hexadecimales

¿Cuál es el número de serie de la NIC del origen?

50:fc:c8

Paso 1: Determinar la dirección IP del gateway predeterminado de la PC

Abra una ventana del símbolo del sistema y emita el comando **ipconfig.**

¿Cuál es la dirección IP del gateway predeterminado de la PC?

Dirección IPv4. . . . . : 192.168.8.100

Máscara de subred . . . . . : 255.255.255.0

Puerta de enlace predeterminada . . . . . : 192.168.8.1

Paso 2: Comenzar a capturar el tráfico de la NIC de la PC

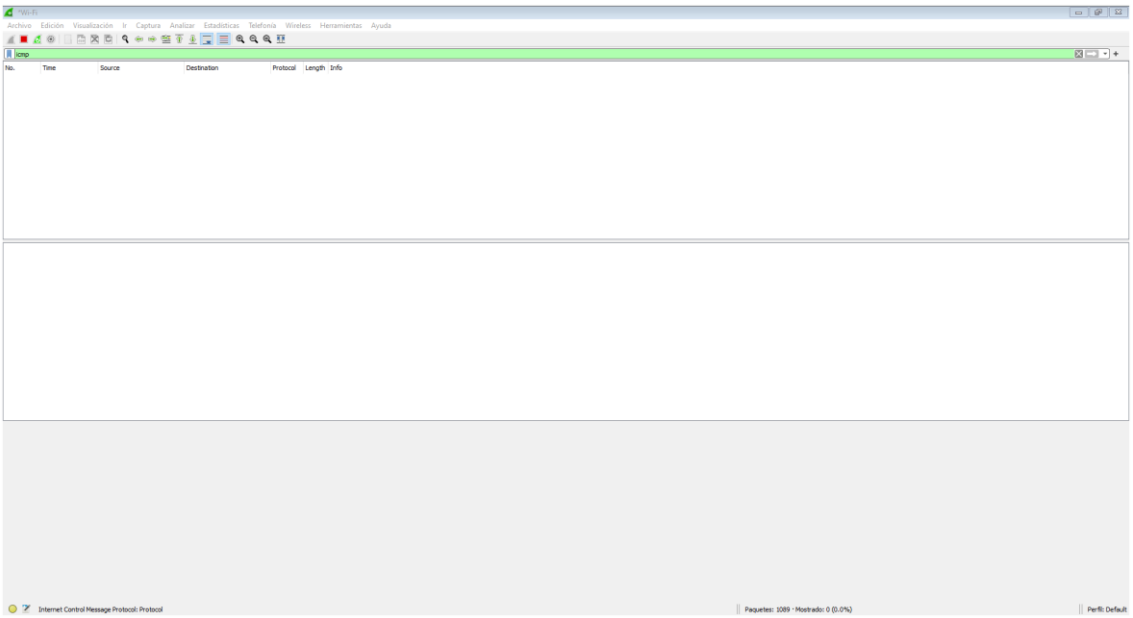
a. Abrir Wireshark para iniciar la captura de datos.

b. Observe el tráfico que aparece en la ventana Packet List (Lista de paquetes).

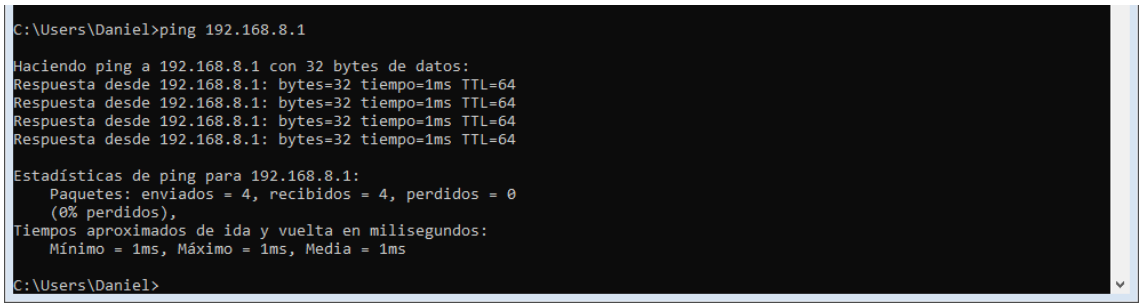
Paso 3: Filtrar Wireshark para que solamente se muestre el tráfico ICMP

Puede usar el filtro de Wireshark para bloquear la visibilidad del tráfico no deseado. El filtro no bloquea la captura de datos no deseados; solo filtra lo que desea mostrar en la pantalla. Por el momento, solo se debe visualizar el tráfico ICMP.

En el cuadro Filter (Filtro) de Wireshark, escriba icmp. Si escribió el filtro correctamente, el cuadro debe volverse de color verde. Si el cuadro está de color verde, haga clic en Apply (Aplicar) (la flecha hacia la derecha) para que se aplique el filtro.



Paso 4: En la ventana del símbolo del sistema, hacer un ping al gateway predeterminado de la PC



¿Cuál es la dirección MAC de la NIC de la PC.

54:8d:**:**

¿Cuál es la dirección MAC del gateway predeterminado?

E0:24:81

d. Puede hacer clic en el signo mayor que (>) al comienzo de la segunda línea para obtener más información sobre la trama de Ethernet II. Pregunta:

¿Qué tipo de trama se muestra?

Destination, source, type

e. En las últimas dos líneas de la parte central, se proporciona información sobre el campo de datos de la trama. Observe que los datos contienen información sobre las direcciones IPv4 de origen y de destino.

¿Cuál es la dirección IP de origen?

192.168.8.100

¿Cuál es la dirección IP de destino?

192.168.8.1

F Puede hacer clic en cualquier línea de la parte central para resaltar esa parte de la trama (hexadecimal y ASCII) en el panel Packet Bytes (Bytes del paquete) de la parte inferior. Haga clic en la línea Internet Control Message Protocol (Protocolo de mensajes de control de Internet) de la parte central y examine lo que se resalta en el panel Packet Bytes (Bytes de paquete).

¿Qué texto muestran los últimos dos octetos resaltados?

g. Haga clic en la siguiente trama de la parte superior y examine una trama de respuesta de eco. Observe que las direcciones MAC de origen y de destino se invirtieron porque esta trama se envió desde el router del gateway predeterminado como respuesta al primer ping.

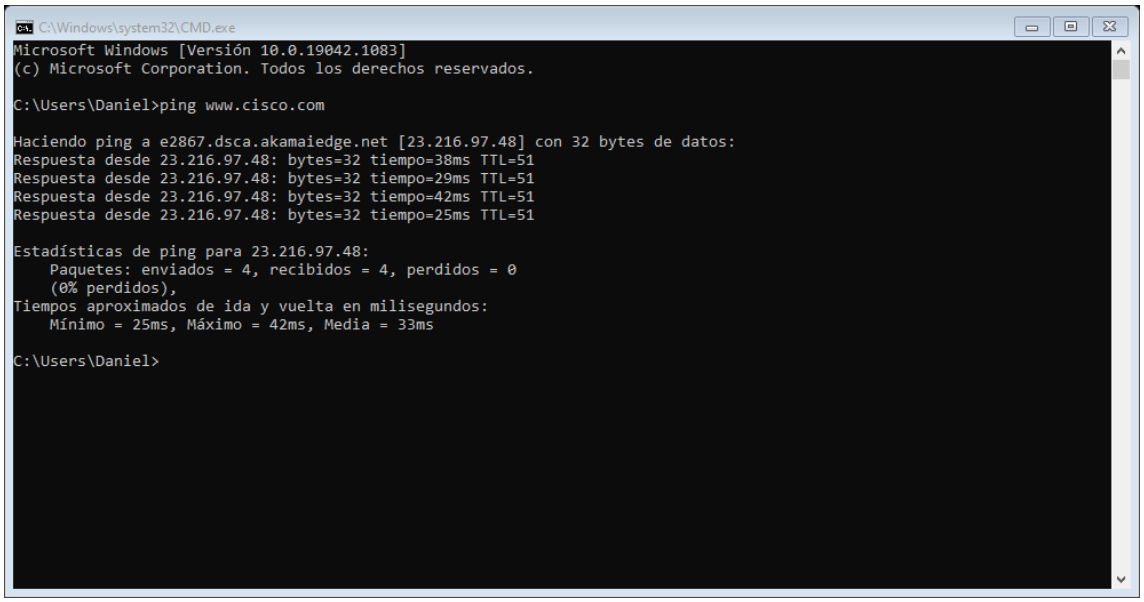
Qué dispositivo y qué dirección MAC se muestran como dirección de destino?

Intel core 54:8d:** IP: 192.168.8.100

Paso 7: Capturar paquetes para un host remoto.

a. Haga clic en el ícono Start Capture (Iniciar captura) para iniciar una nueva captura de Wireshark. Se muestra una ventana emergente que le pregunta si desea guardar los anteriores paquetes capturados en un archivo

b. En la ventana del símbolo del sistema, hacer ping a www.cisco.com



c. Dejar de capturar paquetes.

d. Examinar los nuevos datos del panel de la lista de paquetes de Wireshark.

En la primera trama de solicitud de eco (ping), ¿cuáles son las direcciones MAC de origen y de destino?

Fuente intelcor15:0d:**

Destino: guaweite2f:7f:**

¿Cuáles son las direcciones IP de origen y de destino que contiene el campo de datos de la trama?

Fuente:192.168.8.0

Destino: 23.216.97.48

Compare estas direcciones con las direcciones que recibió en el paso 6. La única dirección que cambió es la dirección IP de destino. ¿Por qué cambió la dirección IP de destino mientras que la dirección MAC permaneció igual?

las mac no cambian dado que la solicitud aunque sea a otra ip, sigue realizándose desde el mismo cliente y la mac de los clientes no cambian ni la del pc y la del ruter

Pregunta de reflexión En Wireshark, no se muestra el campo de preámbulo de un encabezado de trama.

¿Qué contiene el preámbulo?

El preámbulo contiene los delimitadores de trama de inicio