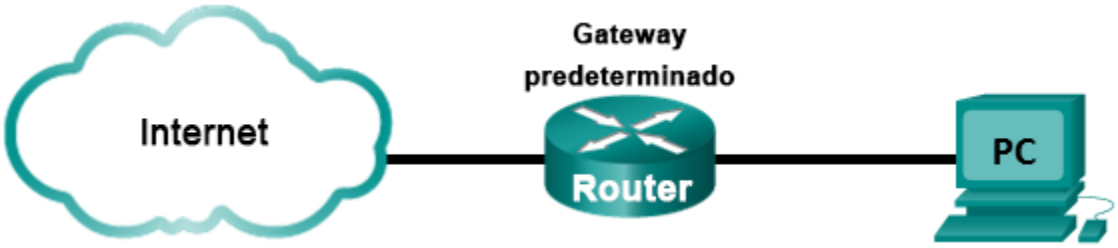
Práctica de laboratorio: Uso de Wireshark para examinar tramas de Ethernet (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología



Objetivos

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

Parte 2: Utilizar Wireshark para capturar y analizar tramas de Ethernet

Información básica/Situación

Cuando los protocolos de la capa superior se comunican entre sí, los datos fluyen hacia abajo en las capas de interconexión de sistema abierto (OSI) y se encapsulan en la trama de la capa 2. La composición de la trama depende del tipo de acceso al medio. Por ejemplo, si los protocolos de capa superior son TCP e IP, y el acceso al medio es Ethernet, la encapsulación de la trama de la capa 2 será Ethernet II. Esto es típico de un entorno LAN.

Cuando se aprende sobre los conceptos de la capa 2, es útil analizar la información del encabezado de la trama. En la primera parte de esta práctica de laboratorio, revisará los campos incluidos en una trama de Ethernet II. En la parte 2, utilizará Wireshark para capturar y analizar los campos de encabezado de la trama de Ethernet II para el tráfico local y remoto.

Nota para el instructor: para esta práctica de laboratorio, se supone que el estudiante utiliza una PC con acceso a Internet. También se supone que Wireshark se instaló previamente en la PC. Las capturas de pantalla de esta práctica de laboratorio se tomaron de Wireshark v1.8.3 para Windows 7 (64 bits).

Recursos necesarios

- 1 PC (Windows 7, Vista o XP con acceso a Internet y Wireshark instalado)

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

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 estos campos.

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 la configuración de red de la PC

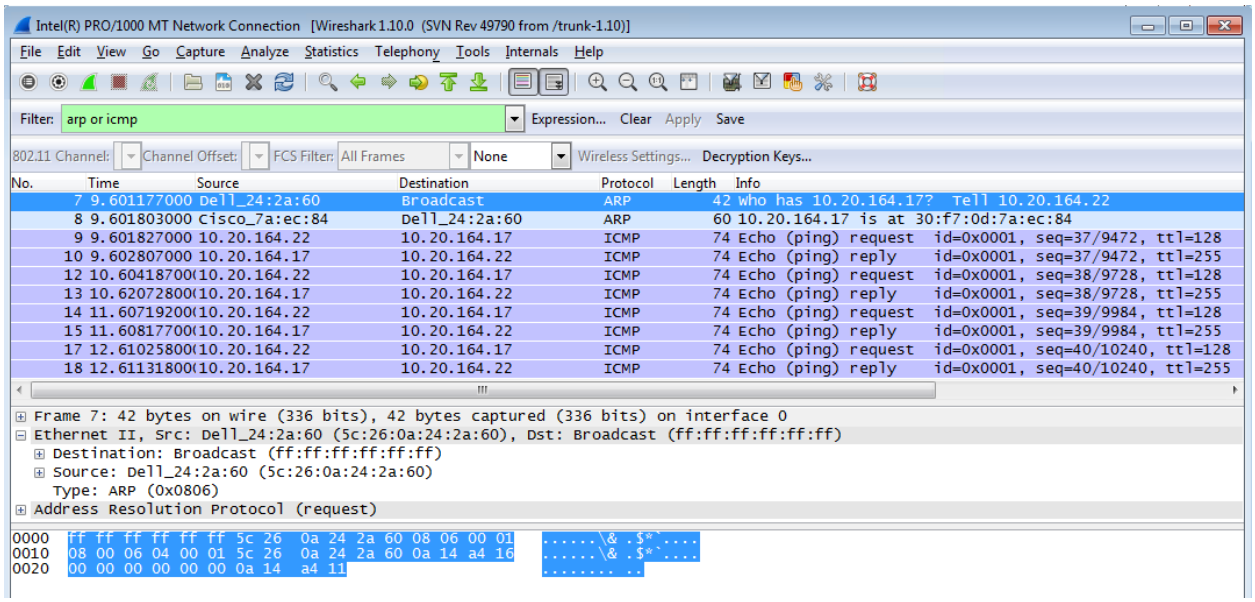
La dirección IP del host de esta PC es 10.20.164.22 y la dirección IP del gateway predeterminado es 10.20.164.17.

```
Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . : cisco.com
   Vínculo: dirección IPv6 local. . . . . : fe80::b875:731b:3c7b:c0b1
   Dirección IPv4. . . . . . . . . . . . . : 10.20.164.22
   Máscara de subred . . . . . . . . . . . : 255.255.255.240
   Puerta de enlace predeterminada . . . . . : 10.20.164.17
```

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

En la siguiente captura de Wireshark, se muestran los paquetes que generó un ping que se emitió desde un host de la PC hasta su gateway predeterminado. Se aplicó un filtro a Wireshark para ver los protocolos ARP e ICMP únicamente. La sesión comienza con una consulta de ARP para la dirección MAC del router del gateway, seguida de cuatro solicitudes y respuestas de ping.



Paso 4: 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.

¿Qué es importante acerca del contenido del campo de la dirección de destino?

_____

_____

Todos los hosts de la LAN recibirán esta trama de broadcast. El host con la dirección IP 10.20.164.17 (gateway predeterminado) enviará una respuesta unicast al origen (host de la PC). Esta respuesta contiene la dirección MAC de la NIC del gateway predeterminado.

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

_____

_____

_____

Antes de que la PC pueda enviar una solicitud de ping a un host, necesita determinar la dirección MAC de destino para poder armar el encabezado de la trama para esa solicitud de ping. El broadcast de ARP se utiliza para solicitar la dirección MAC del host con la dirección IP incluida en el ARP.

¿Cuál es la dirección MAC del origen en la primera trama? _____ 5c:26:0a:24:2a:60

¿Cuál es la ID de proveedor (OUI) de la NIC de origen? _____ Dell

¿Qué parte de la dirección MAC es la OUI?

_____

Los primeros tres octetos de la dirección MAC indican la OUI.

¿Cuál es el número de serie de la NIC de origen? _____ 24:2a:60

Parte 2: Utilizar Wireshark para capturar y analizar tramas de Ethernet

En la parte 2, utilizará Wireshark para capturar tramas de Ethernet locales y remotas. Luego examinará la información incluida en los campos de encabezado de la trama.

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

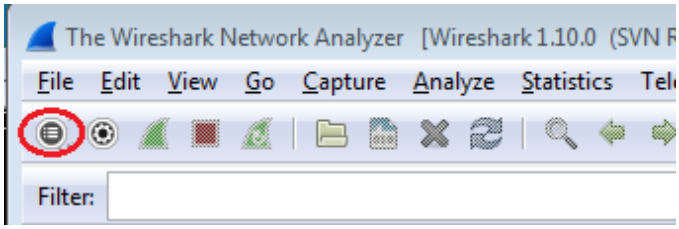
Abra una ventana del símbolo del sistema y emita el comando **ipconfig**.

¿Cuál es la dirección IP del gateway predeterminado de la PC? _____ Las respuestas varían.

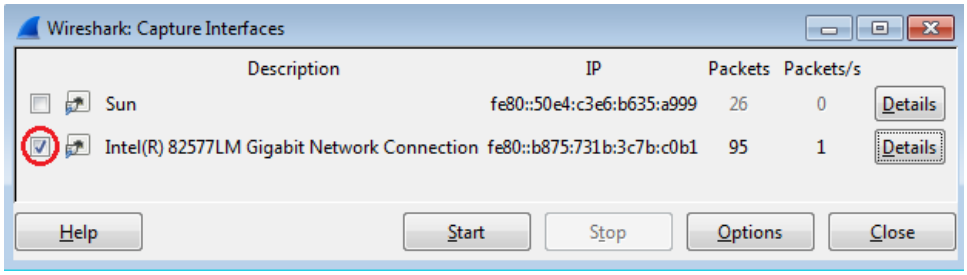
Paso 2: Iniciar la captura de tráfico en la NIC de la PC

a. Abra Wireshark.

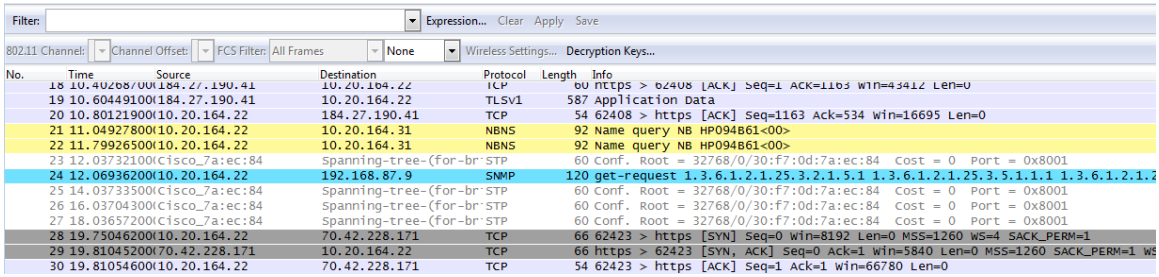
b. En la barra de herramientas de Wireshark Network Analyzer, haga clic en el ícono **Interface List** (Lista de interfaces).



c. En la ventana Wireshark: Capture Interfaces (Wireshark: capturar interfaces), seleccione la interfaz para iniciar la captura de tráfico haciendo clic en la casilla de verificación apropiada, y luego haga clic en **Start** (Comenzar). Si no está seguro de qué interfaz activar, haga clic en **Details** (Detalles) para obtener más información sobre cada interfaz enumerada.



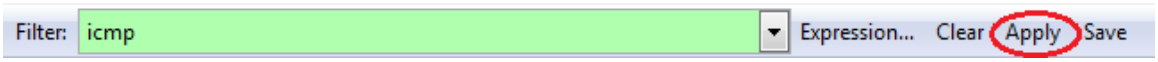
d. Observe el tráfico que aparece en la ventana Packet List (Lista de paquetes).



Paso 3: Filtrar Wireshark para mostrar solamente el tráfico de ICMP

Puede utilizar 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 se muestra en la pantalla. Por ahora, solo se debe ver el tráfico de ICMP.

En el cuadro **Filter** (Filtrar) de Wireshark, escriba **icmp**. Si escribió el filtro correctamente, el cuadro se volverá verde. Si el cuadro está de color verde, haga clic en **Apply** (Aplicar) para aplicar el filtro.

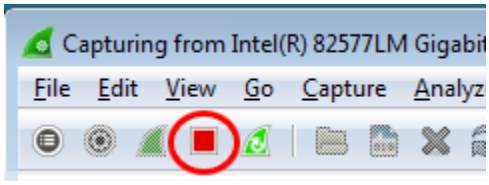


Paso 4: En la ventana del símbolo del sistema, haga ping al gateway predeterminado de la PC

En esta ventana, utilice la dirección IP que registró en el paso 1 para hacer ping al gateway predeterminado.

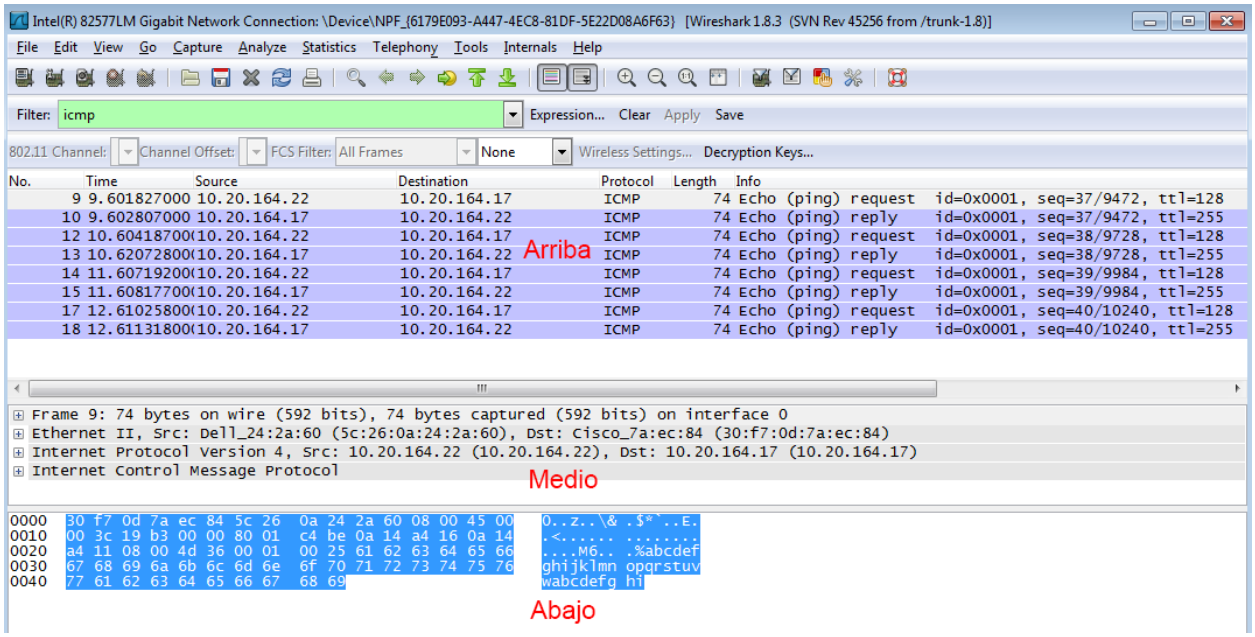
Paso 5: Detener la captura de tráfico en la NIC

Haga clic en el ícono **Stop Capture** (Detener captura) para detener la captura de tráfico.



Paso 6: Examinar la primera solicitud de eco (ping) en Wireshark

La ventana principal de Wireshark está dividida en tres secciones: el panel de la lista de paquetes (Arriba), el panel de detalles del paquete (Medio) y el panel de bytes del paquete (Abojo). Si seleccionó la interfaz correcta para la captura de paquetes en el paso 3, Wireshark mostrará la información ICMP en el panel de la lista de paquetes de Wireshark, como se muestra en el ejemplo siguiente.



a. En el panel de la lista de paquetes (sección superior), haga clic en la primera trama que se indica. Debería ver **Echo (ping) request** (Solicitud de eco [ping]) debajo del encabezado **Info** (Información). Esta acción debería resaltar la línea en color azul.

b. Examine la primera línea del panel de detalles del paquete (sección media). En esta línea, se muestra la longitud de la trama; 74 bytes en este ejemplo.

c. En la segunda línea del panel de detalles del paquete, se muestra que es una trama de Ethernet II. También se muestran las direcciones MAC de origen y destino.

¿Cuál es la dirección MAC de la NIC de la PC? _____ 5c:26:0a:24:2a:60 en el ejemplo.

¿Cuál es la dirección MAC del gateway predeterminado? _____ 30:f7:0d:7a:ec:84 en el ejemplo.

d. Puede hacer clic en el signo más (+) que se encuentra al comienzo de la segunda línea para obtener más información sobre la trama de Ethernet II. Observe que el signo más cambia al signo menos (-).

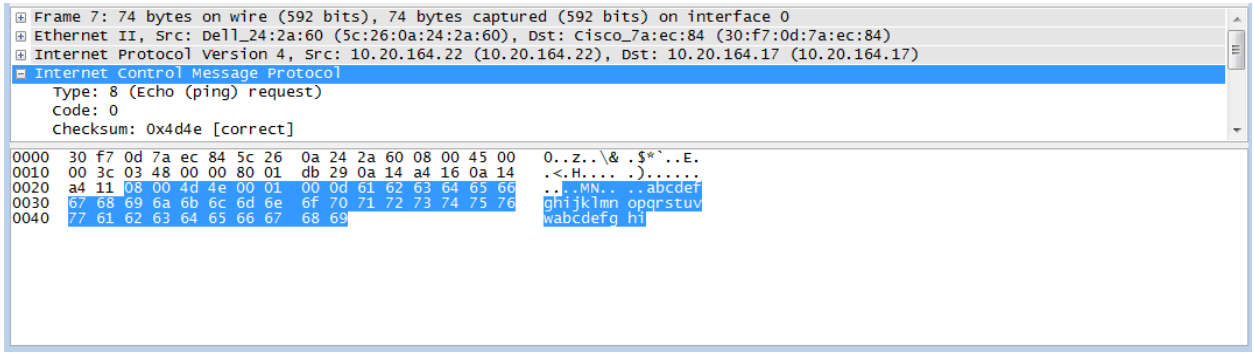
¿Qué tipo de trama se muestra? _____ 0x0800 o un tipo de trama IPv4.

e. Las dos últimas líneas que se muestran en la sección media proporcionan información sobre el campo de datos de la trama. Observe que los datos contienen la información de la dirección IPv4 de origen y destino.

¿Cuál es la dirección IP de origen? _____10.20.164.22 en el ejemplo.

¿Cuál es la dirección IP de destino? _____10.20.164.17 en el ejemplo.

f. Puede hacer clic en cualquier línea de la sección media para resaltar esa parte de la trama (hexadecimal y ASCII) en el panel de bytes del paquete (sección inferior). Haga clic en la línea **Internet Control Message Protocol** (Protocolo de mensajes de control de Internet) en la sección media y examine qué está resaltado en el panel de bytes del paquete.



¿Qué indican los dos últimos octetos resaltados? _____ hi

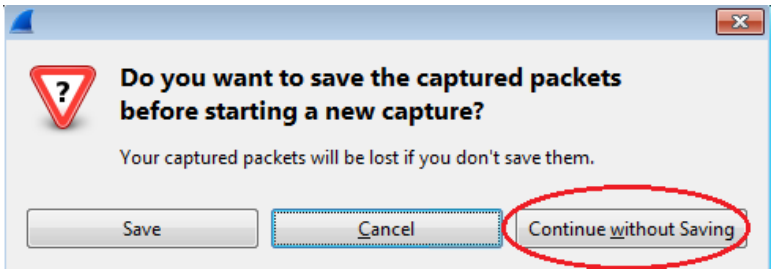
g. Haga clic en la trama siguiente de la sección superior y examine una trama de respuesta de eco. Observe que las direcciones MAC de origen y destino se invirtieron, porque esta trama se envió desde el router del gateway predeterminado como una respuesta al primer ping.

¿Qué dirección de dispositivo y dirección MAC se muestran como la dirección de destino?

_____ La PC del host, 5c:26:0a:24:2a:60 en el ejemplo.

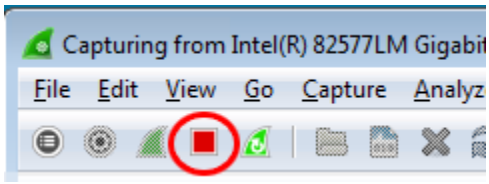
Paso 7: Reiniciar la captura de paquetes en Wireshark

Haga clic en el ícono **Start Capture** (Iniciar captura) para iniciar una nueva captura de Wireshark. Aparece una ventana emergente en la que se le pregunta si desea guardar los paquetes capturados anteriormente en un archivo antes de iniciar una nueva captura. Haga clic en **Continue without Saving** (Continuar sin guardar).



Paso 8: En la ventana del símbolo del sistema, hacer ping a www.cisco.com

Paso 9: Detener la captura de paquetes



Paso 10: Examinar los datos nuevos en el 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 destino?

Origen: _____ Debería ser la dirección MAC de la PC.

Destino: _____ Debería ser la dirección MAC del gateway predeterminado.

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

Origen: _____ Sigue siendo la dirección IP de la PC.

Destino: _____ Es la dirección del servidor en www.cisco.com.

Compare estas direcciones con las direcciones que recibió en el paso 7. La única dirección que cambió es la dirección IP de destino. ¿Por qué la dirección IP de destino cambió y la dirección MAC de destino siguió siendo la misma?

_____

_____

_____

_____

Las tramas de la capa 2 nunca dejan la LAN. Cuando se emite un ping a un host remoto, el origen utiliza la dirección MAC del gateway predeterminado para el destino de la trama. El gateway predeterminado recibe el paquete, quita de este la información de la trama de la capa 2 y, a continuación, crea un nuevo encabezado de trama con una dirección MAC de siguiente salto. Este proceso continúa de router a router hasta que el paquete llega a la dirección IP de destino.

Reflexión

Wireshark no muestra el campo de preámbulo de un encabezado de trama. ¿Qué contiene el preámbulo?

_____

_____

El campo de preámbulo contiene siete octetos de secuencias 1010 alternas y un octeto que indica el comienzo de la trama, 10101011.