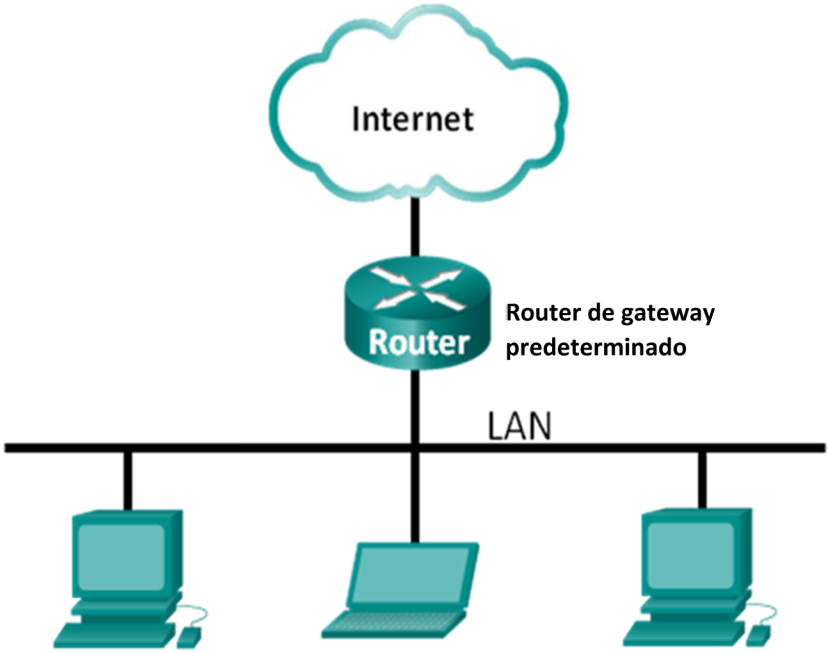
Práctica de laboratorio: Uso de Wireshark para ver el tráfico de la red

Topología



Objetivos

Parte 1: Capturar y analizar datos ICMP locales en Wireshark

Parte 2: Capturar y analizar datos ICMP remotos en Wireshark

Información básica/situación

Wireshark es un analizador de protocolos de software o una aplicación “husmeador de paquetes” que se utiliza para el diagnóstico de problemas de red, verificación, desarrollo de protocolo y software y educación. Mientras el flujo de datos va y viene en la red, el husmeador “captura” cada unidad de datos del protocolo (PDU) y puede decodificar y analizar su contenido de acuerdo a la RFC correcta u otras especificaciones.

Es una herramienta útil para cualquiera que trabaje con redes y se puede utilizar en la mayoría de las prácticas de laboratorio en los cursos de CCNA para el análisis de datos y la solución de problemas. En esta práctica de laboratorio, usará Wireshark para capturar direcciones IP del paquete de datos ICMP y direcciones MAC de la trama de Ethernet.

Recursos necesarios

- 1 PC (Windows 7, 8 o 10 con acceso a Internet)
- Se utilizarán PC adicionales en una red de área local (LAN) para responder a las solicitudes de ping.

Parte 1: Captura y análisis de datos ICMP locales en Wireshark

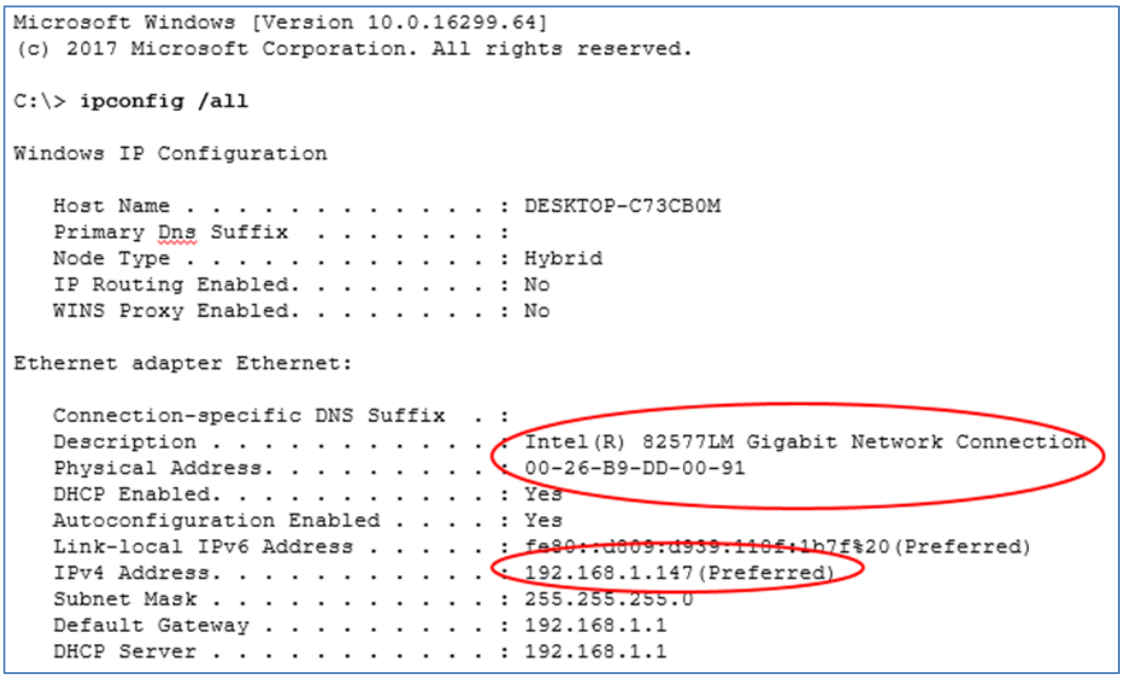
En la parte 1 de esta práctica de laboratorio, hará ping a otra PC en la LAN y capturará solicitudes y respuestas ICMP en Wireshark. También verá dentro de las tramas capturadas para obtener información específica. Este análisis debe ayudar a aclarar de qué manera se utilizan los encabezados de paquetes para transmitir datos al destino.

Paso 1: Recuperar las direcciones de interfaz de la PC

Para esta práctica de laboratorio, deberá recuperar la dirección IP de la PC y la dirección física de la tarjeta de interfaz de red (NIC), que también se conoce como “dirección MAC”.

a. Abra una ventana de comandos, escriba **ipconfig /all** y luego presione Enter (Introducir).

b. Registre la dirección IP de la interfaz de su PC, su descripción y su dirección MAC (física).



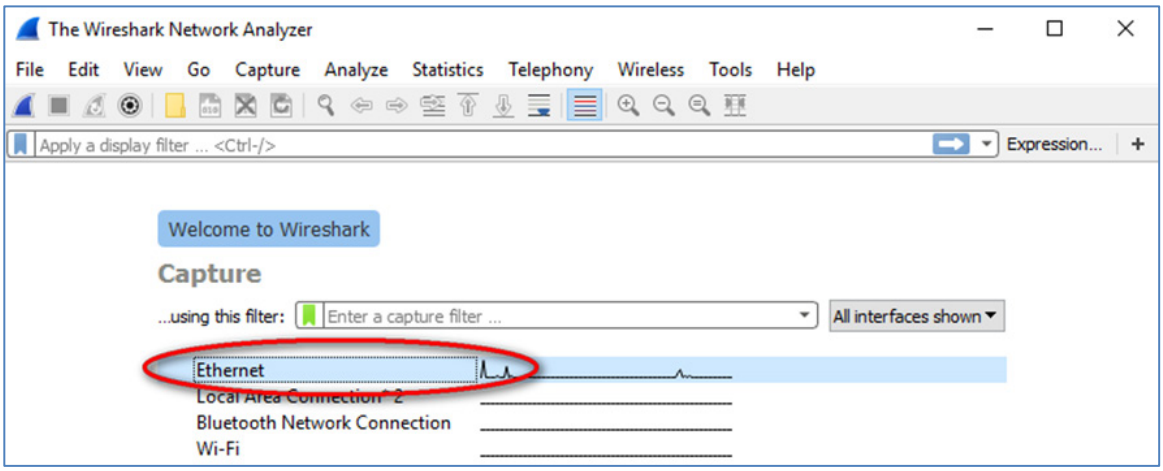
```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-C73CB0M
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-26-B9-DD-00-91
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
```

c. Solicite a un miembro o a los miembros del equipo la dirección IP de su PC y proporcióneles la suya. En esta instancia, no proporcione su dirección MAC.

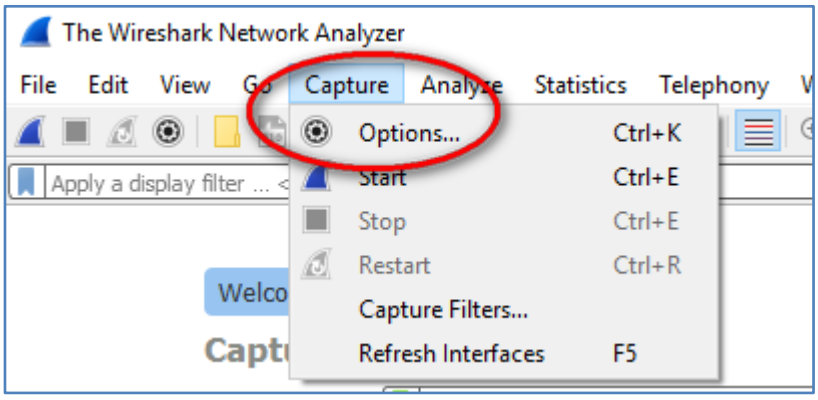
Paso 2: Iniciar Wireshark y comenzar a capturar datos

a. En la PC, haga clic en el botón **Inicio** de Windows para ver Wireshark como uno de los programas en el menú emergente. Haga doble clic en **Wireshark**.

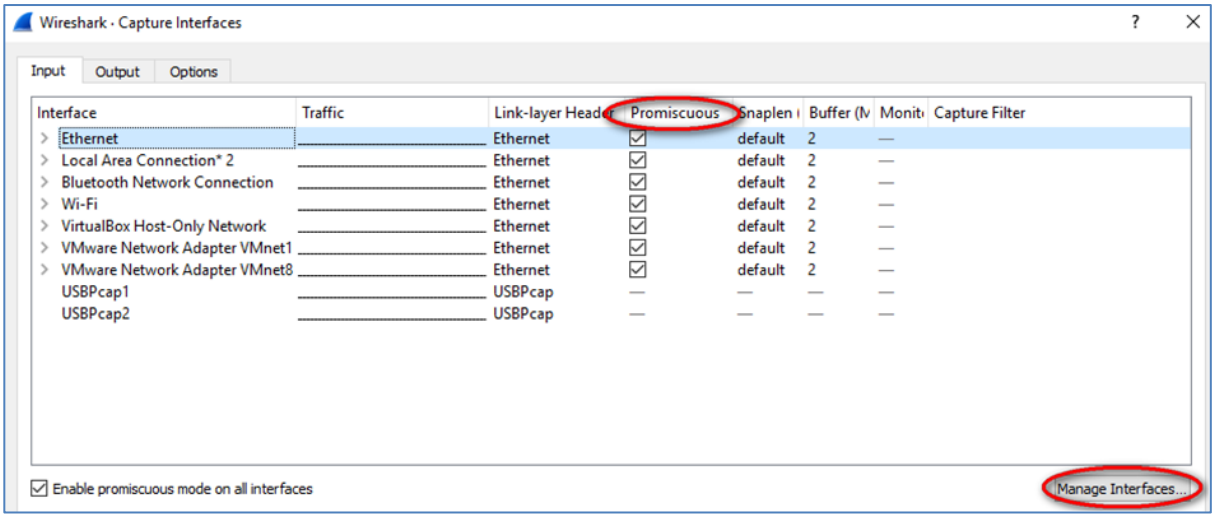
b. Después de que se inicie Wireshark, haga clic en la interfaz de captura que se utilizará. Dado que utilizamos la conexión Ethernet por cable en la PC, asegúrese de que la opción Ethernet esté en la parte superior de la lista.



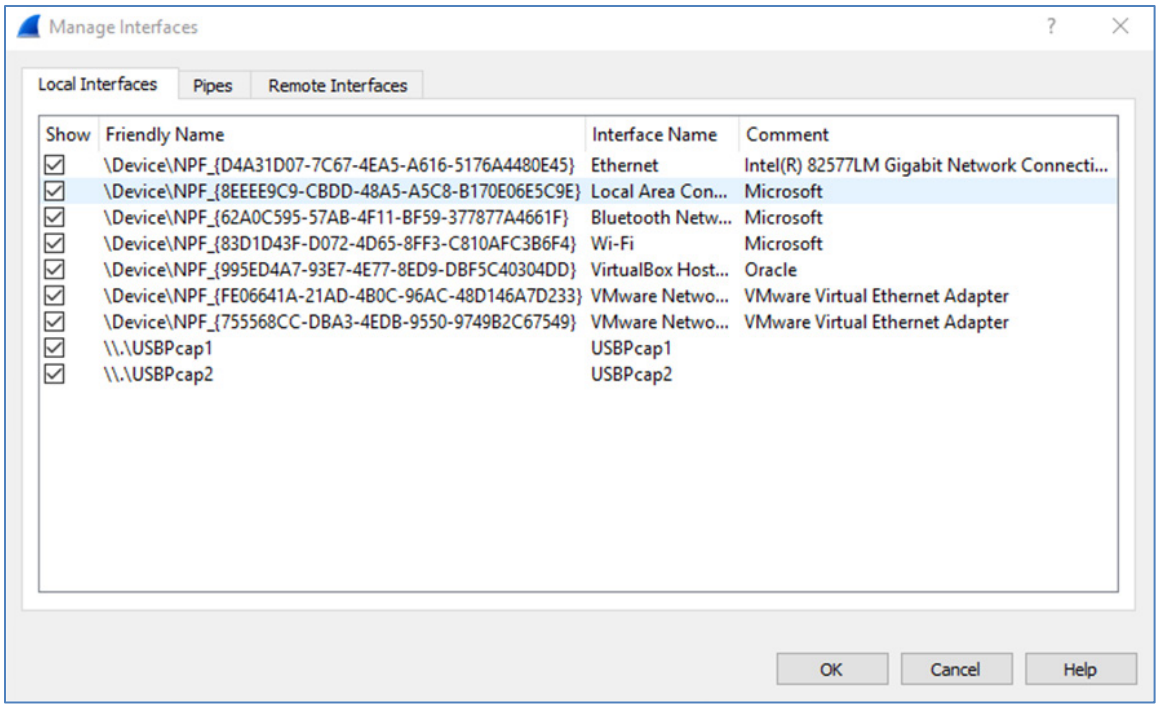
Para administrar la interfaz de captura, haga clic en **Capture** (Captura) y **Options** (Opciones):



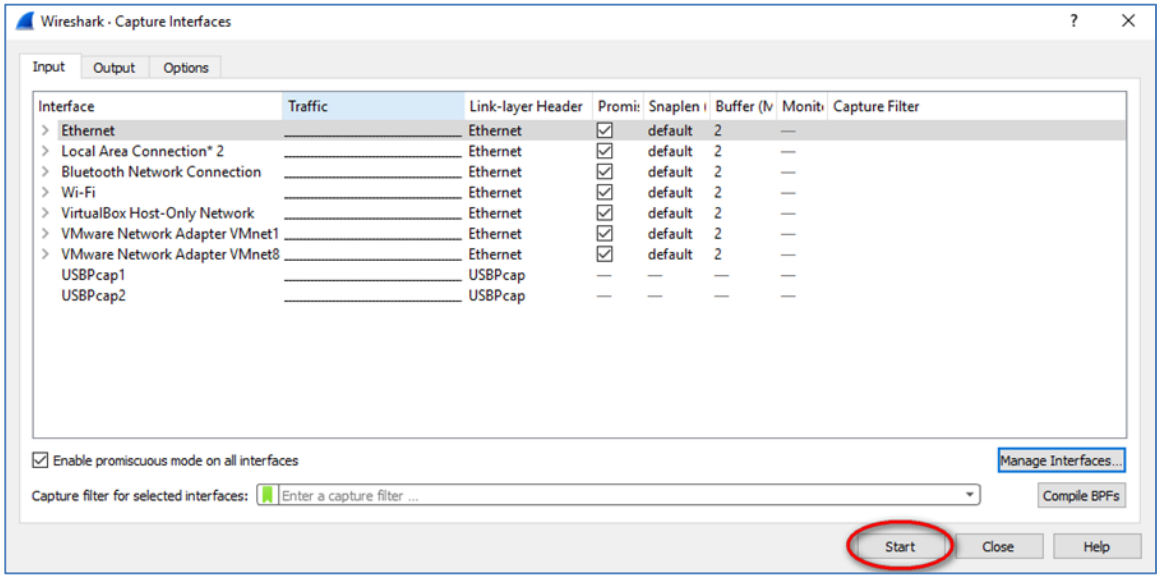
c. Se mostrará una lista de interfaces. Asegúrese de que la interfaz de captura esté marcada en **Promiscuous** (Promiscuo).



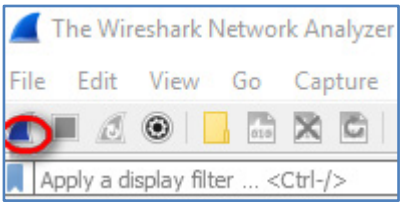
Nota: También se pueden administrar las interfaces en la PC; para ello, haga clic en **Manage Interfaces** (Administrar interfaces). Verifique que la descripción coincida con lo que observó en el paso 1b. Después de verificar la interfaz correcta, cierre la ventana **Manage Interfaces** (Administrar interfaces).



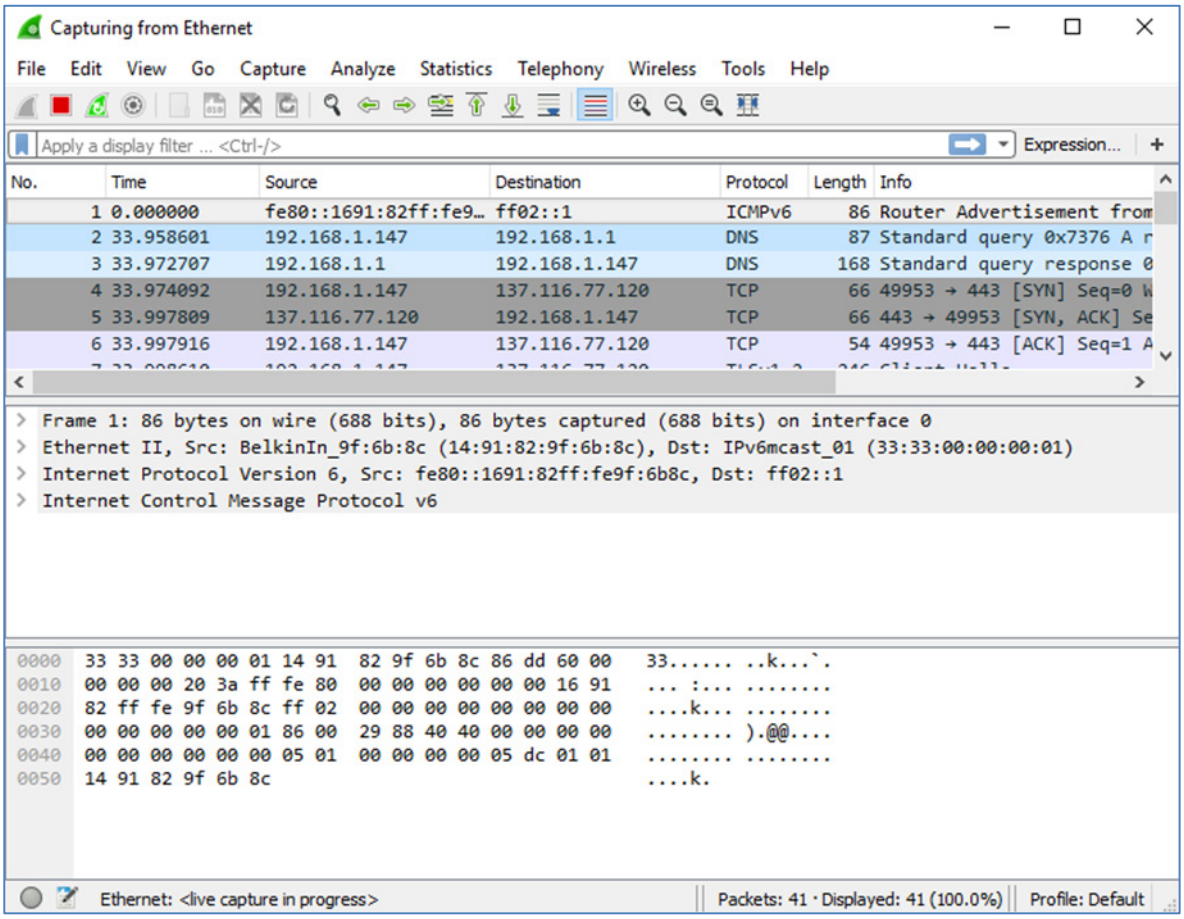
d. Después de activar la interfaz correcta, haga clic en **Start** (Comenzar) para comenzar la captura de datos.



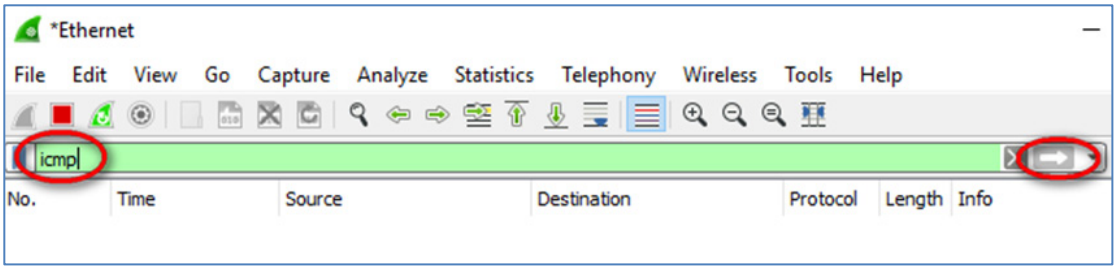
Nota: Para iniciar la captura de datos, también puede hacer clic en el ícono de **Wireshark** en la interfaz principal.



La información comienza a desplazar hacia abajo la sección superior de Wireshark. Las líneas de datos aparecen en diferentes colores según el protocolo.



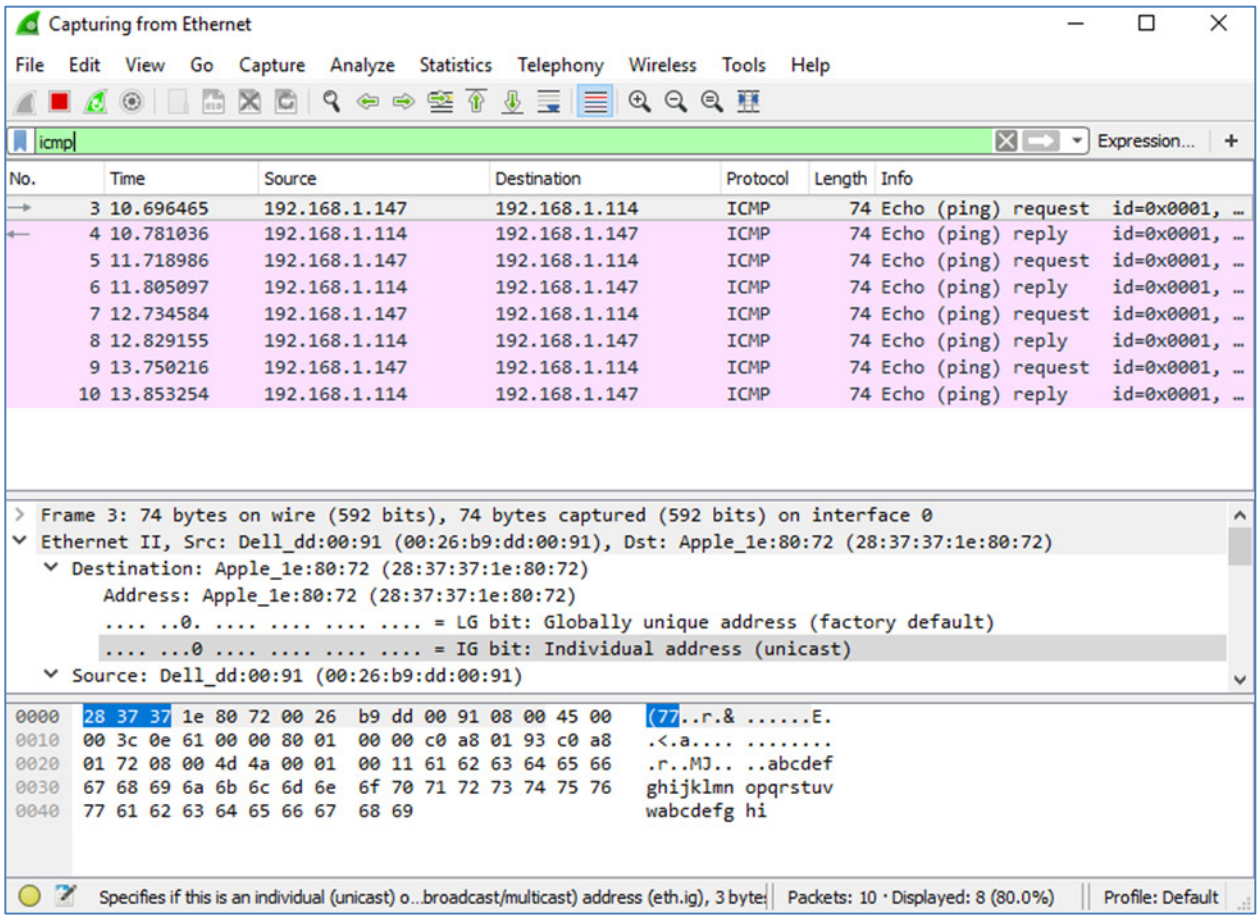
e. Es posible desplazarse muy rápidamente por esta información según la comunicación que tiene lugar entre la PC y la LAN. Se puede aplicar un filtro para facilitar la vista y el trabajo con los datos que captura Wireshark. Para esta práctica de laboratorio, solo nos interesa mostrar las PDU de ICMP (ping). Escriba **icmp** en el cuadro **Filter** (Filtro) que se encuentra en la parte superior de Wireshark y presione **Enter** (Introducir) o haga clic en el botón **Apply** (Aplicar) (signo de flecha) para ver solamente PDU de ICMP (ping).



f. Este filtro hace que desaparezcan todos los datos de la ventana superior, pero se sigue capturando el tráfico en la interfaz. Abra la ventana del símbolo del sistema que abrió antes y haga ping a la dirección IP que recibió del miembro del equipo.

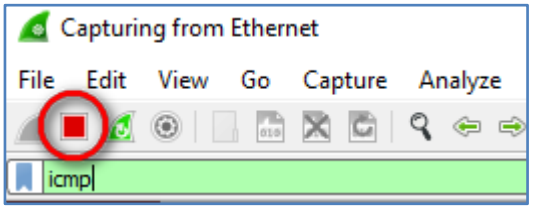
```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\> ping 192.168.1.114

Pinging 192.168.1.114 with 32 bytes of data:
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```


Comenzará a ver que aparecen datos en la ventana superior de Wireshark nuevamente.



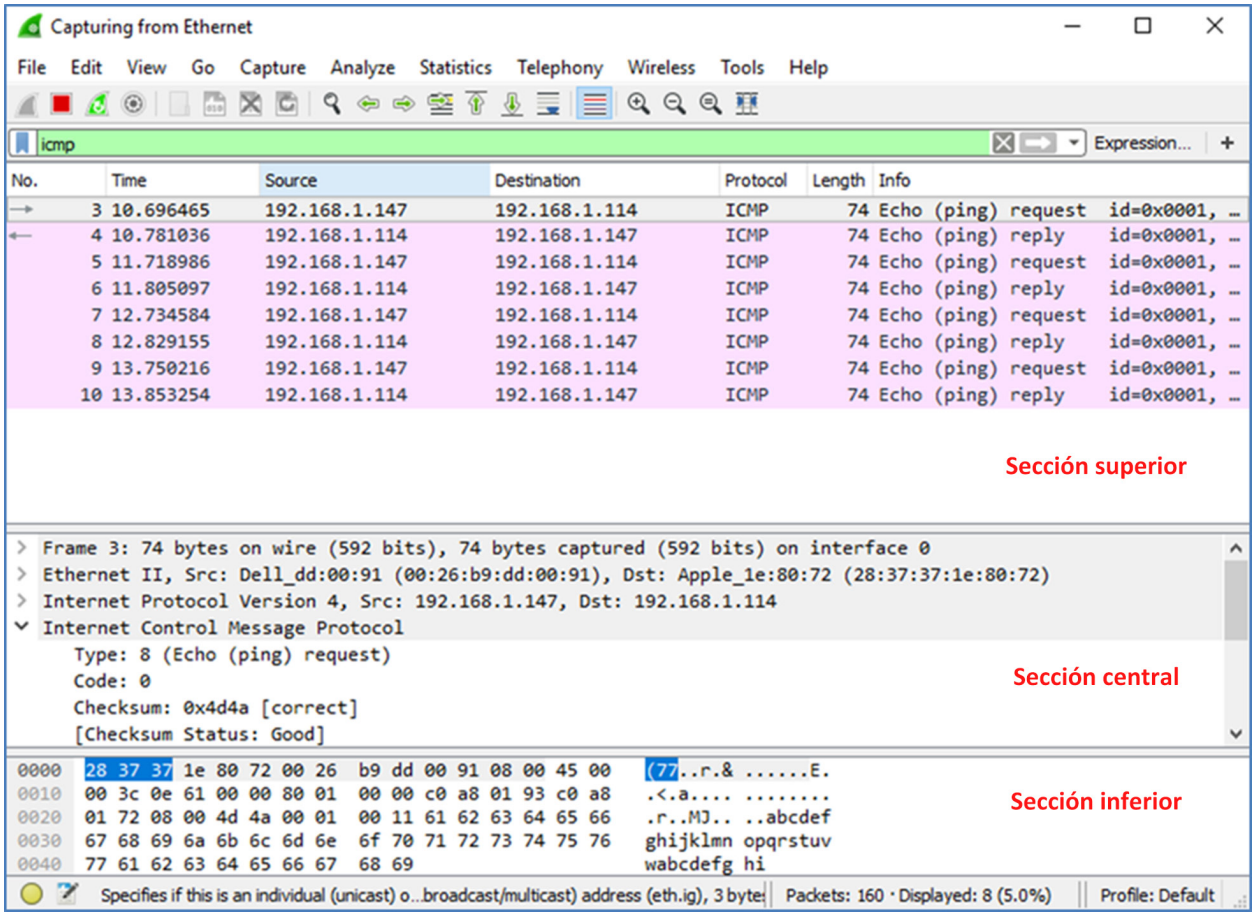
Nota: Si la PC del miembro de su equipo no responde a sus pings, es posible que el firewall de la PC del miembro del equipo bloquee estas solicitudes. Consulte Appendix A: Allowing ICMP Traffic Through a Firewall para obtener información sobre cómo permitir el tráfico ICMP a través del firewall con Windows 7.

g. Detenga la captura de datos haciendo clic en el ícono **Stop Capture** (Detener captura).

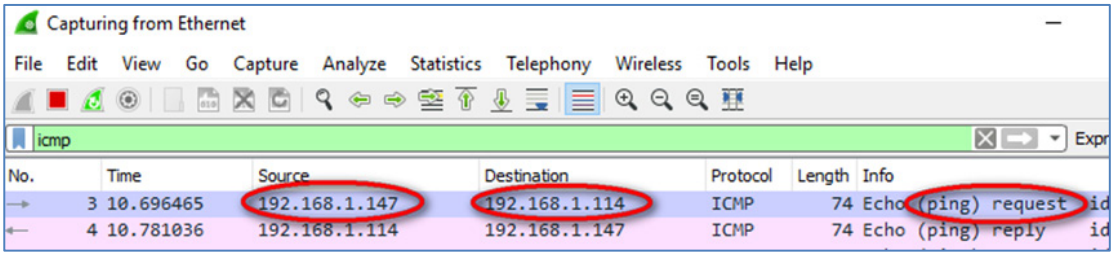


Paso 3: Examine los datos capturados

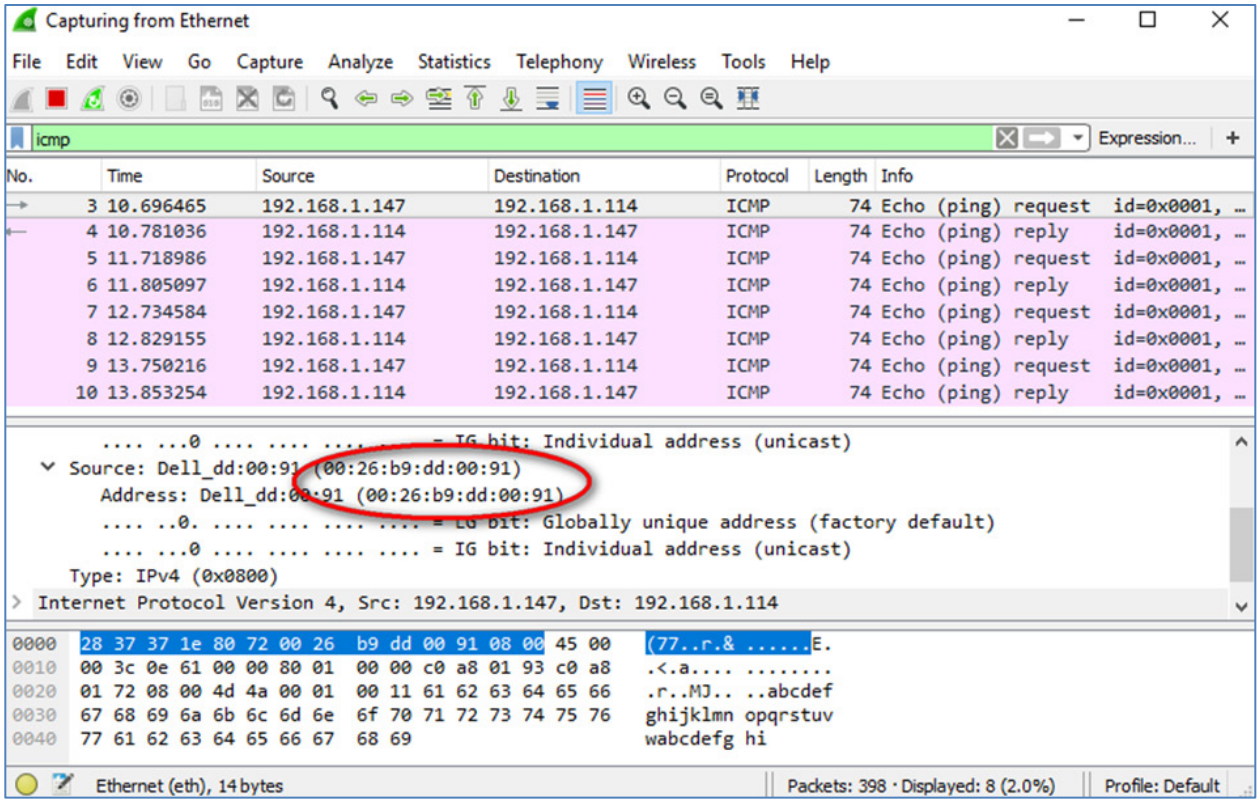
En el paso 3, examine los datos que se generaron mediante las solicitudes de ping de la PC del miembro del equipo. Los datos de Wireshark se muestran en tres secciones: 1) la sección superior muestra la lista de tramas de PDU capturadas con un resumen de la información de paquetes IP enumerada, 2) la sección media indica información de la PDU para la trama seleccionada en la parte superior de la pantalla y separa una trama de PDU capturada por las capas de protocolo, y 3) la sección inferior muestra los datos sin procesar de cada capa. Los datos sin procesar se muestran en formatos hexadecimal y decimal.



a. Haga clic en las primeras tramas de PDU de la solicitud de ICMP en la sección superior de Wireshark. Observe que la columna **Source** (Origen) contiene la dirección IP de su PC y la columna **Destination** (Destino) contiene la dirección IP de la PC del compañero de equipo a la que hizo ping.



b. Con esta trama de PDU aún seleccionada en la sección superior, navegue hasta la sección media. Haga clic en el signo más que está a la izquierda de la fila de Ethernet II para ver las direcciones MAC de origen y destino.



¿La dirección MAC de origen coincide con la interfaz de la PC (que se muestra en el paso 1.b)?

¿La dirección MAC de destino en Wireshark coincide con la dirección MAC del compañero de equipo?

¿De qué manera su PC obtiene la dirección MAC de la PC a la que hizo ping?

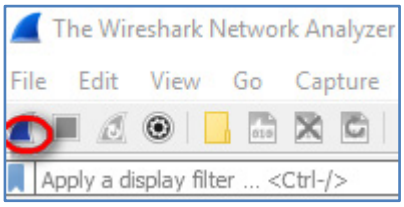
Nota: En el ejemplo anterior de una solicitud de ICMP capturada, los datos ICMP se encapsulan dentro de una PDU del paquete IPv4 (encabezado de IPv4), que luego se encapsula en una PDU de trama de Ethernet II (encabezado de Ethernet II) para la transmisión en la LAN.

Parte 2: Captura y análisis de datos ICMP remotos en Wireshark

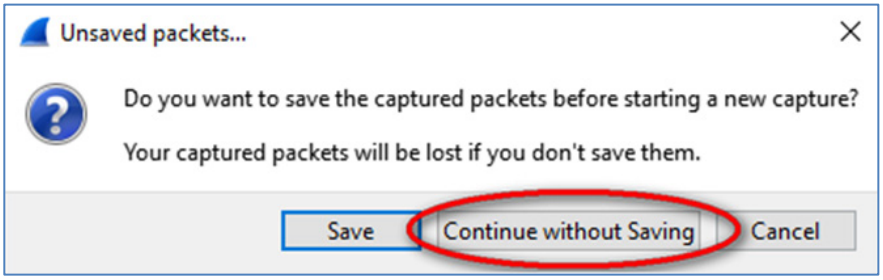
En la parte 2, hará ping a los hosts remotos (hosts que no están en la LAN) y examinará los datos generados a partir de esos pings. Luego, determinará las diferencias entre estos datos y los datos examinados en la parte 1.

Paso 1: Comience a capturar datos en la interfaz

a. Vuelva a iniciar la captura de datos.



b. Se abre una ventana que le solicita guardar los datos capturados anteriormente antes de comenzar otra captura. No es necesario guardar esos datos. Haga clic en **Continue without Saving** (Continuar sin guardar).



c. Con la captura activa, haga ping a los URL de los tres sitios web siguientes:

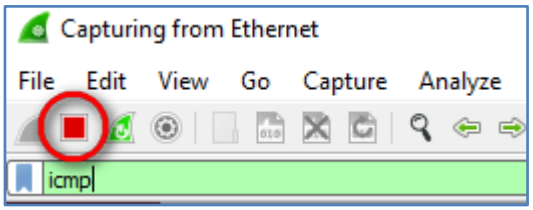
1) www.yahoo.com
2) www.cisco.com

3) www.google.com

```
C:\> ping www.yahoo.com

Pinging atsv2-fp.wg1.b.yahoo.com [98.139.180.180] with 32 bytes of data:
Reply from 98.139.180.180: bytes=32 time=43ms TTL=53
Reply from 98.139.180.180: bytes=32 time=60ms TTL=53
Reply from 98.139.180.180: bytes=32 time=43ms TTL=53
Reply from 98.139.180.180: bytes=32 time=42ms TTL=53

Ping statistics for 98.139.180.180:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 60ms, Average = 47ms

C:\> ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [23.13.155.188] with 32 bytes of data:
Reply from 23.13.155.188: bytes=32 time=20ms TTL=56
Reply from 23.13.155.188: bytes=32 time=21ms TTL=56
Reply from 23.13.155.188: bytes=32 time=19ms TTL=56
Reply from 23.13.155.188: bytes=32 time=19ms TTL=56

Ping statistics for 23.13.155.188:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 21ms, Average = 19ms

C:\> ping www.google.com

Pinging www.google.com [216.58.194.100] with 32 bytes of data:
Reply from 216.58.194.100: bytes=32 time=56ms TTL=54
Reply from 216.58.194.100: bytes=32 time=56ms TTL=54
Reply from 216.58.194.100: bytes=32 time=55ms TTL=54
Reply from 216.58.194.100: bytes=32 time=57ms TTL=54

Ping statistics for 216.58.194.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 55ms, Maximum = 57ms, Average = 56ms

C:\>
```

Nota: Al hacer ping a los URL que se indican, observe que el servidor de nombres de dominio (DNS) traduce el URL a una dirección IP. Observe la dirección IP recibida para cada URL.

d. Puede detener la captura de datos haciendo clic en el ícono **Stop Capture** (Detener captura).



Paso 2: Inspeccione y analice los datos de los hosts remotos

a. Revise los datos capturados en Wireshark y examine las direcciones IP y MAC de las tres ubicaciones a las que hizo ping. Indique las direcciones IP y MAC de destino para las tres ubicaciones en el espacio proporcionado.

1.ª ubicación: IP: 98 . 138 . 253 . 109 MAC: 34 : 64 : a9 : 51 : a0 : 00

2.ª ubicación: IP: 23 . 14 . 16 . 170 MAC: 34 : 64 : a9 : 51 : a0 : 00

3.ª ubicación: IP: 64 . 233 . 177 . 104 MAC: 34 : 64 : a9 : 51 : a0 : 00

b. ¿Qué es importante sobre esta información?

MAC

c. ¿En qué se diferencia esta información de la información de ping local que recibió en la parte 1?

En una red LAN es mucho mas rapida.

Reflexión

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

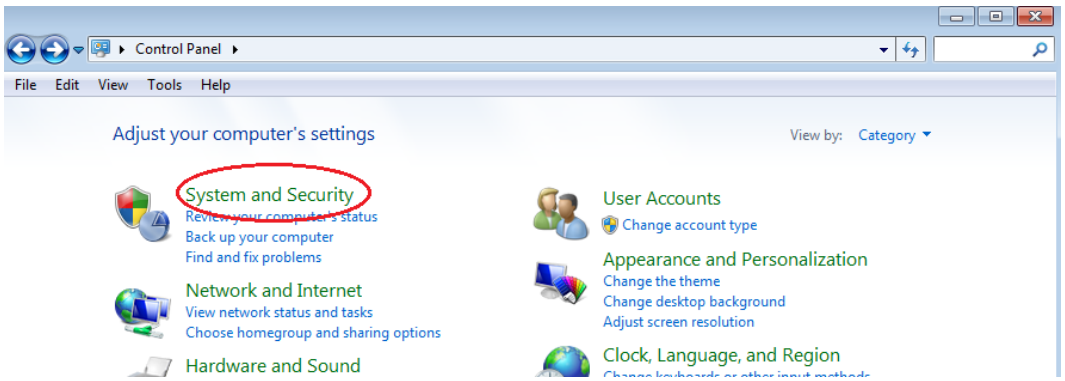
Por que el dominio de la difusión es hasta el router y el router no deja pasar y le que devuelve es su MAC

Apéndice A: Permitir el tráfico ICMP a través de un firewall

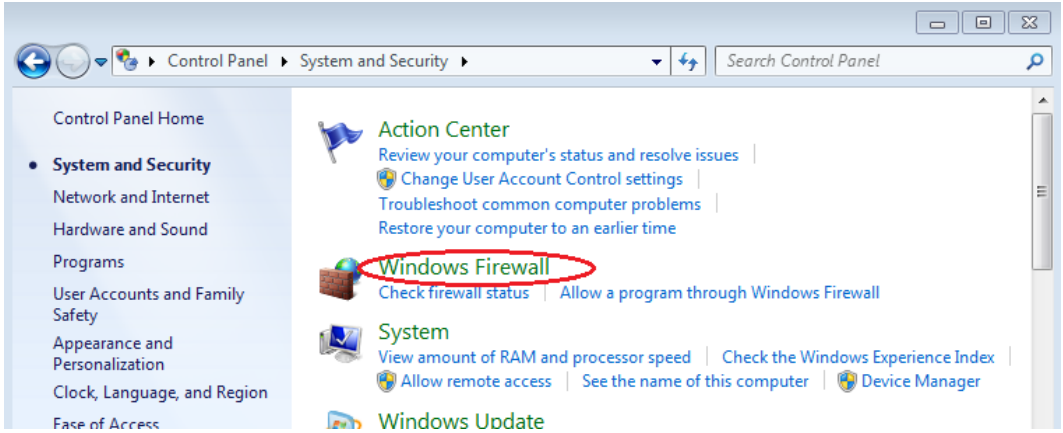
Si los miembros del equipo no pueden hacer ping a su PC, es posible que el firewall esté bloqueando esas solicitudes. En este apéndice, se describe cómo crear una regla en el firewall para permitir las solicitudes de ping. También se describe cómo deshabilitar la nueva regla ICMP después de haber completado la práctica de laboratorio.

Paso 1: Crear una nueva regla de entrada que permita el tráfico ICMP a través del firewall

a. En el **Control Panel** (Panel de control), haga clic en la opción **System and Security** (Sistema y seguridad).

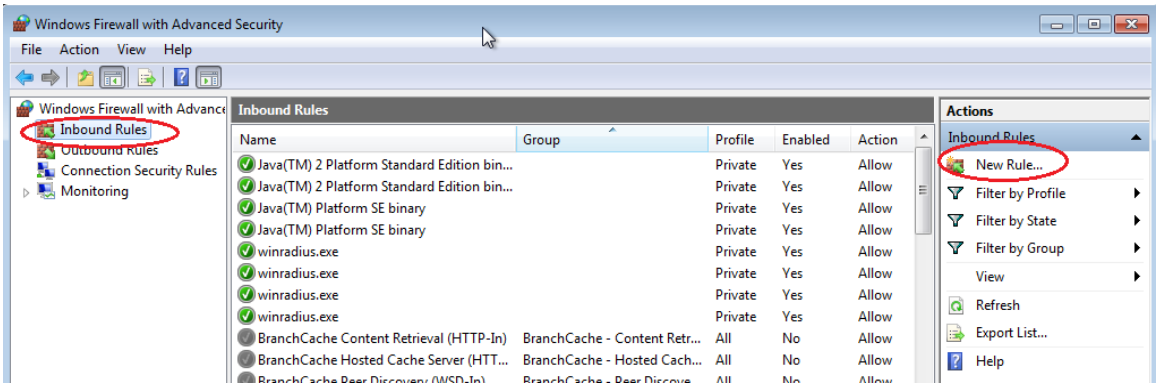


b. En la ventana **System and Security** (Sistema y seguridad), haga clic en **Windows Firewall** (Firewall de Windows).

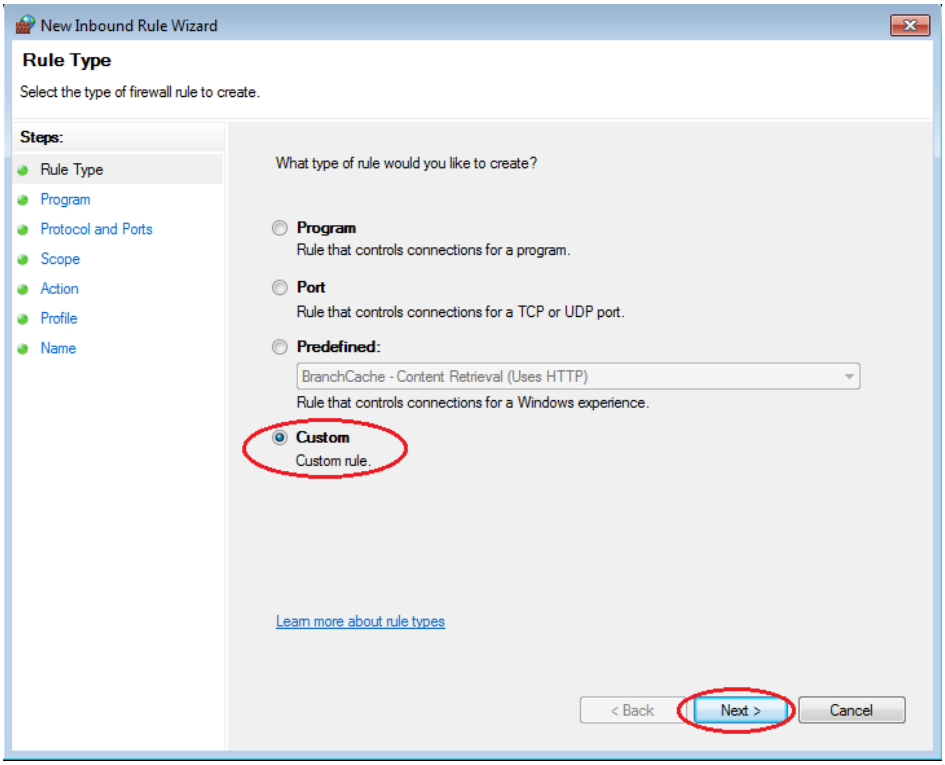


c. En el panel izquierdo de la ventana **Windows Firewall** (Firewall de Windows), haga clic en **Advanced settings** (Configuración avanzada).

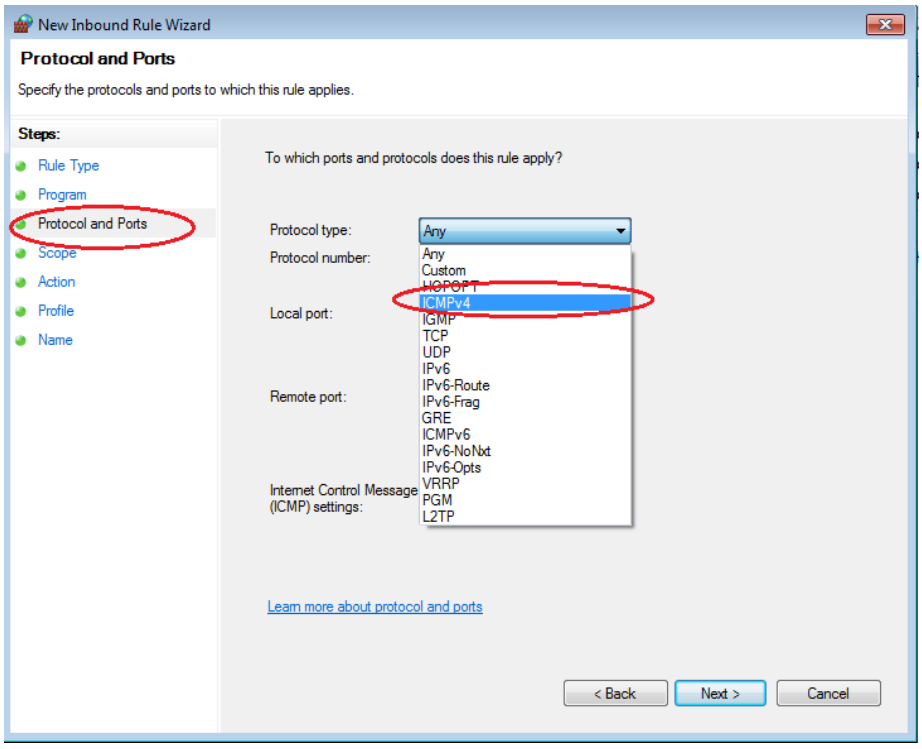
d. En la ventana **Advanced Security** (Seguridad avanzada), seleccione la opción **Inbound Rules** (Reglas de entrada) en la barra lateral izquierda y, a continuación, haga clic en **New Rule…** (Nueva regla...) en la barra lateral derecha.



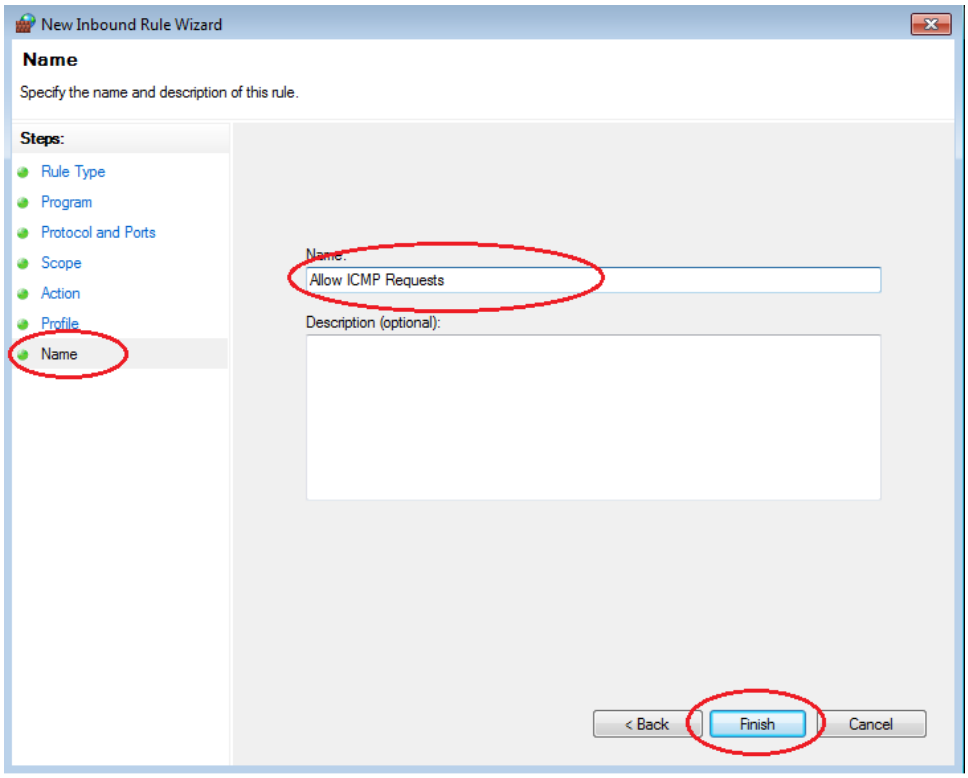
e. Se inicia el asistente **New Inbound Rule** (Nueva regla de entrada). En la pantalla **Rule Type** (Tipo de regla), haga clic en el botón de opción **Custom** (Personalizada) y, a continuación, en **Next** (Siguiente).



f. En el panel izquierdo, haga clic en la opción **Protocol and Ports** (Protocolo y puertos) y, en el menú desplegable **Protocol Type** (Tipo de protocolo), seleccione **ICMPv4**; luego, haga clic en **Next** (Siguiente).



g. En el panel izquierdo, haga clic en la opción **Name** (Nombre), y, en el campo **Name** (Nombre), escriba **Allow ICMP Requests** (Permitir solicitudes ICMP). Haga clic en **Finalizar**.

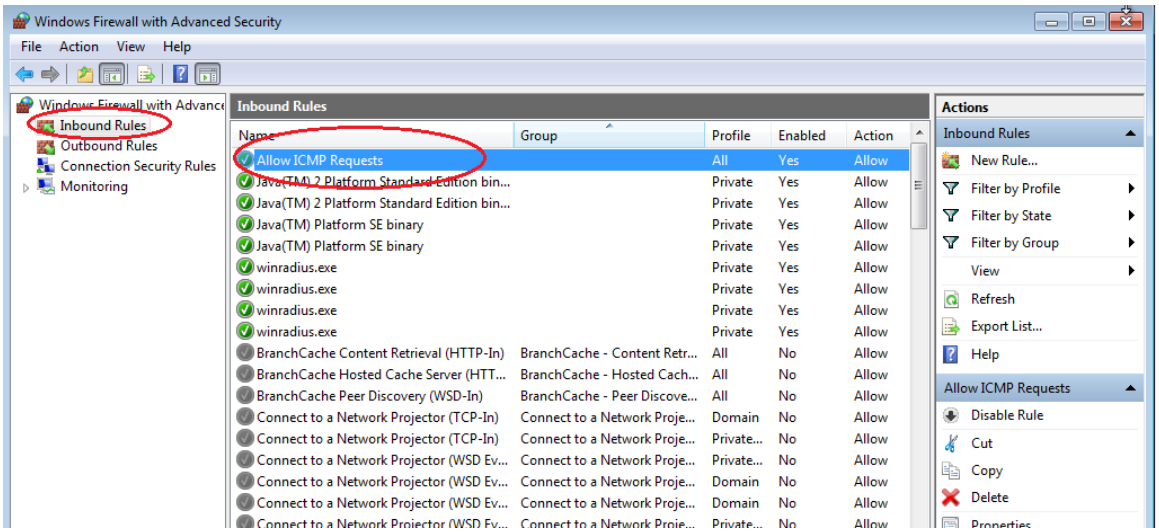


Esta nueva regla debe permitir que los miembros del equipo reciban respuestas de ping de su PC.

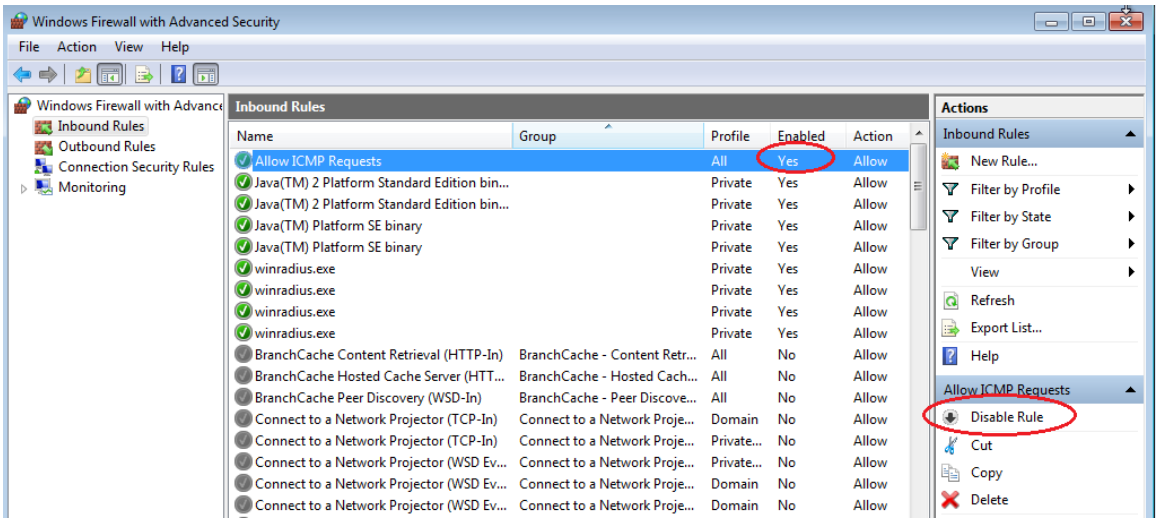
Paso 2: Deshabilitar o eliminar la nueva regla ICMP

Una vez completada la práctica de laboratorio, es posible que desee deshabilitar o incluso eliminar la nueva regla que creó en el paso 1. La opción **Deshabilitar regla** le permite volver a habilitar la regla en una fecha posterior. Al eliminar la regla, esta se elimina permanentemente de la lista de reglas de entrada.

a. En el panel izquierdo de la ventana **Advanced Security** (Seguridad avanzada), haga clic en **Inbound Rules** (Reglas de entrada) y, a continuación, ubique la regla que creó en el paso 1.



b. Para deshabilitar la regla, haga clic en la opción **Desable Rule** (Deshabilitar regla). Al seleccionar esta opción, verá que esta cambia a **Enable Rule** (Habilitar regla). Puede alternar entre **Disable Rule** (Deshabilitar regla) y **Enable Rule** (Habilitar regla); el estado de la regla también se muestra en la columna **Enabled** (Habilitada) de la lista **Inbound Rules** (Reglas de entrada).



c. Para eliminar permanentemente la regla ICMP, haga clic en **Delete** (Eliminar). Si elige esta opción, deberá volver a crear la regla para permitir las respuestas de ICMP.