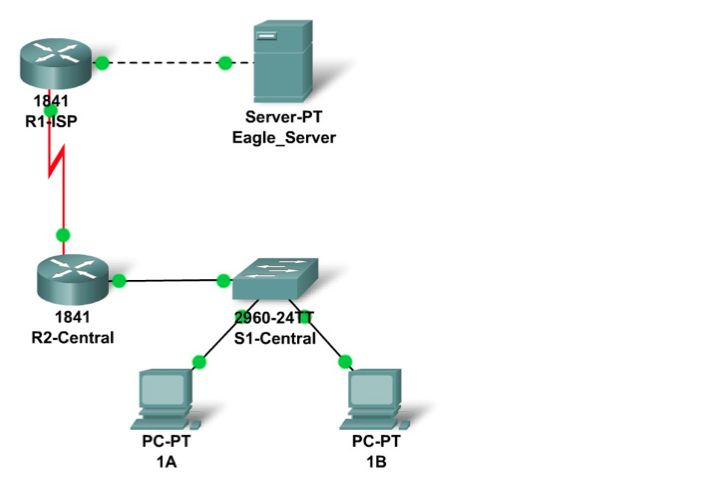
Uy7



**Práctica de laboratorio: Uso de Wireshark para observar el tráfico de la red**

Diagrama de topología



**Objetivos**

**Tarea 1: Descargar e instalar Wireshark (Optativo)**

**Tarea 2: Capturar y analizar datos ICMP locales en Wireshark**

* Capturar datos del tráfico de ping a los hosts locales.
* Ubicar la información de la dirección MAC y de la dirección IPv4 en las PDU capturadas.

**Tarea 3: Capturar y analizar datos ICMP remotos en Wireshark**

* + - Captura datos del tráfico de ping a los hosts remotos.
    - Ubicar la información de la dirección MAC y de la dirección IPv4 en las PDU capturadas.
    - Explicar por qué las direcciones MAC para los hosts remotos son diferentes de las direcciones MAC para los hosts locales.

Información básica/Situación

Wireshark es un analizador de protocolos de software o una aplicación “husmeador de paquetes” que se utiliza para el diagnóstico de fallos de red, verificación, desarrollo de protocolos y software, y educación. Mientras los flujos de datos van y vienen por la red, este programa “captura” cada unidad de datos de protocolo (PDU) y puede decodificar y analizar su contenido de acuerdo con la RFC correcta u otras especificaciones.

Wireshark es una herramienta útil para cualquier persona que trabaje con redes y se puede utilizar con la mayoría de las prácticas de laboratorio para tareas de análisis de datos y resolución de problemas. Esta práctica de laboratorio proporciona instrucciones para descargar e instalar Wireshark, aunque es posible que ya esté instalado. 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 con acceso a la red del laboratorio.

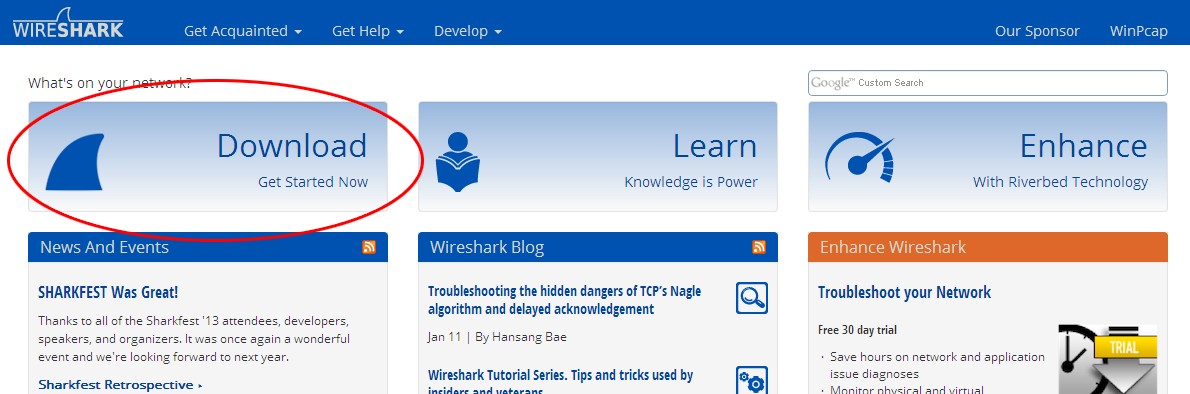
Tarea 1: Descargar e instalar Wireshark (optativo)

Wireshark se convirtió en el programa detector de paquetes estándar del sector que utilizan los ingenieros de redes. Este software de código abierto está disponible para muchos sistemas operativos diferentes, incluidos Windows, MAC y Linux. En la parte 1 de esta práctica de laboratorio, descargará e instalará el programa de software Wireshark en el PC.

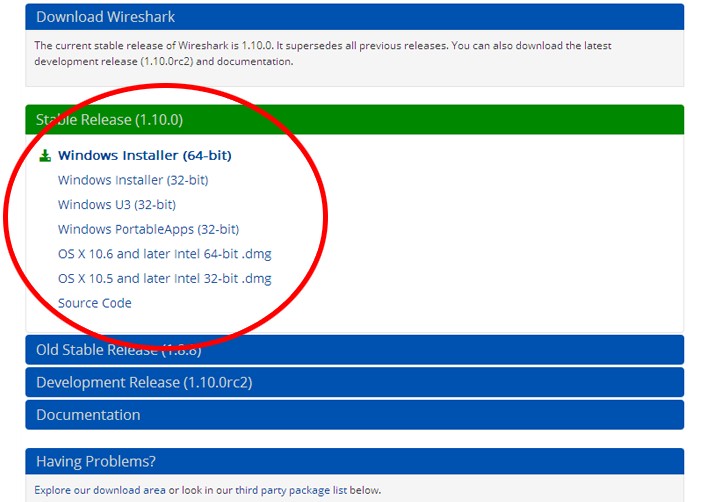
**Nota:** si Wireshark ya está instalado en el PC, puede saltear la Tarea 1 e ir directamente a la Tarea 2. Si Wireshark no está instalado en el PC consulte con el profesor.

Paso 1: Descargar Wireshark

1. Wireshark se puede descargar de [www.wireshark.org.](http://www.wireshark.org/)
2. Haga clic en **Download Wireshark** (Descargar Wireshark).



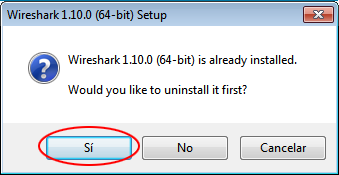
1. Elija la versión de software que necesita según la arquitectura y el sistema operativo del PC. Por ejemplo, si tiene un PC de 64 bits con Windows, seleccione **Windows Installer (64-bit)** (Instalador de Windows [64 bits]).



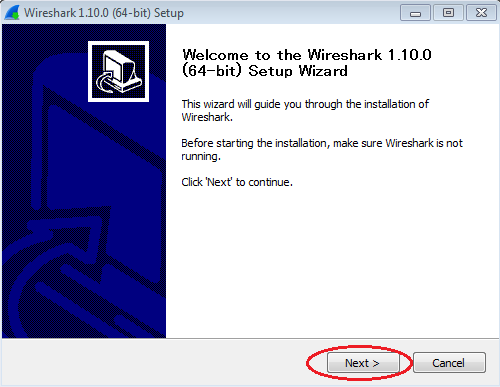
Después de realizar la selección, comienza la descarga. La ubicación del archivo descargado depende del explorador y del sistema operativo que utiliza. Para usuarios de Windows, la ubicación predeterminada es la carpeta **Descargas**.

Paso 2: Instalar Wireshark

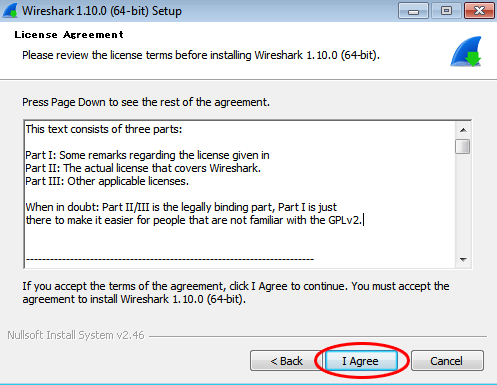
1. El archivo descargado se denomina **Wireshark-win64-x.x.x.exe**, en el que **x** representa el número de versión. Haga doble clic en el archivo para iniciar el proceso de instalación.
2. Responda los mensajes de seguridad que aparezcan en la pantalla. Si ya tiene una copia de Wireshark en el PC, se le solicitará desinstalar la versión anterior antes de instalar la versión nueva. Se recomienda eliminar la versión anterior de Wireshark antes de instalar otra versión. Haga clic en **Sí** para desinstalar la versión anterior de Wireshark.



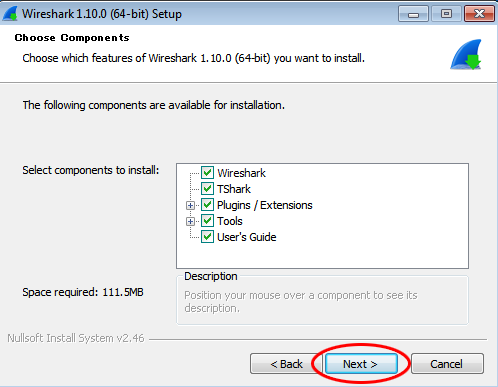
1. Si es la primera vez que instala Wireshark, o si lo hace después de haber completado el proceso de desinstalación, navegue hasta el asistente para instalación de Wireshark. Haga clic en **Next** (Siguiente).



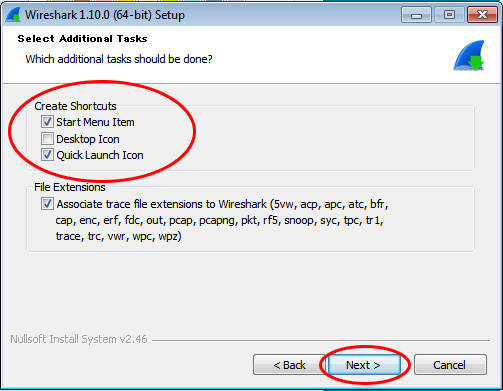
1. Continúe avanzando por el proceso de instalación. Cuando aparezca la ventana License Agreement (Contrato de licencia), haga clic en **I agree** (Acepto).



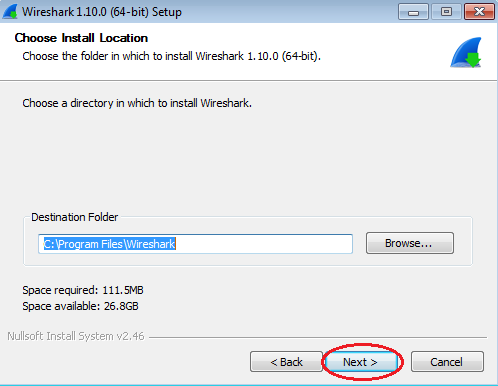
1. Guarde la configuración predeterminada en la ventana Choose Components (Elegir componentes) y haga clic en **Next** (Siguiente).



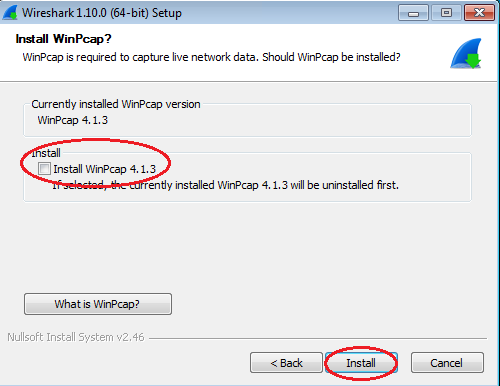
1. Elija las opciones de método abreviado que desee y, a continuación, haga clic en **Next** (Siguiente).



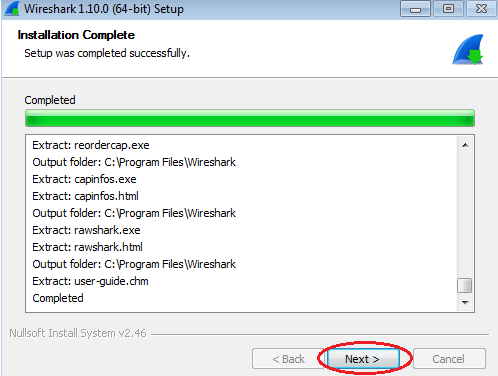
1. Puede cambiar la ubicación de instalación de Wireshark, pero, a menos que tenga un espacio en disco limitado, se recomienda mantener la ubicación predeterminada.



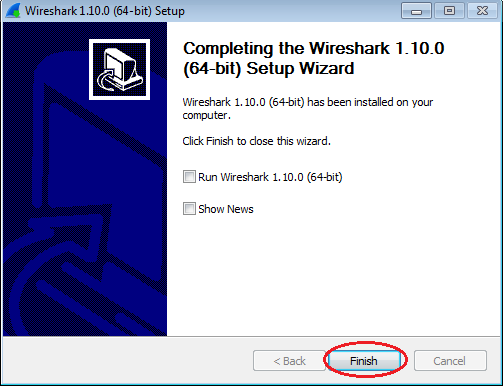
1. Para capturar datos de la red activa, WinPcap debe estar instalado en el PC. Si WinPcap ya está instalado en el PC, la casilla de verificación Install (Instalar) estará desactivada. Si la versión instalada de WinPcap es anterior a la versión que incluye Wireshark, se recomienda que permita que la versión más reciente se instale haciendo clic en la casilla de verificación **Install WinPcap x.x.x** (Instalar WinPcap [número de versión]).
2. Finalice el asistente de instalación de WinPcap si instala WinPcap.



1. Wireshark comienza a instalar los archivos, y aparece una ventana independiente con el estado de la instalación. Haga clic en **Next** (Siguiente) cuando la instalación esté completa.



1. Haga clic en **Finish** (Finalizar) para completar el proceso de instalación de Wireshark.



Tarea 2: Capturar y analizar datos ICMP locales en Wireshark

En esta tarea hará ping a otro PC en la LAN (red de laboratorio) y capturará solicitudes y respuestas ICMP en Wireshark. También observará el interior 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 y comprender mejor el proceso de comunicación en red.

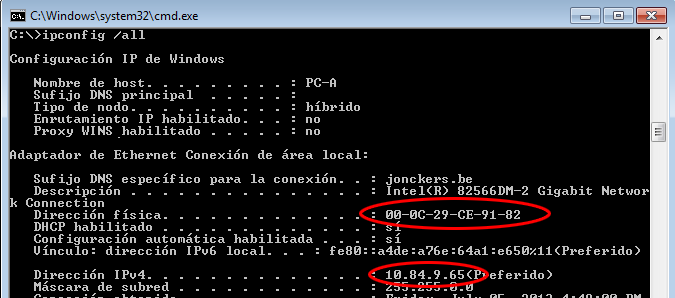
Paso 1: Conectarse a la red del laboratorio

En primer lugar, conecte el PC de su puesto de trabajo a la red de laboratorio tal y como aprendió en durante la primera práctica. Siga todos los pasos y asegúrese de disponer de una conectividad correcta con el servidor **Eagle-server**.

Paso 2: Recuperar las direcciones de interfaz del PC

Para esta práctica de laboratorio, deberá recuperar la dirección IPv4 del PC y la dirección física de la tarjeta de interfaz de red (NIC) tipo Ethernet, que también se conoce como “dirección MAC”.

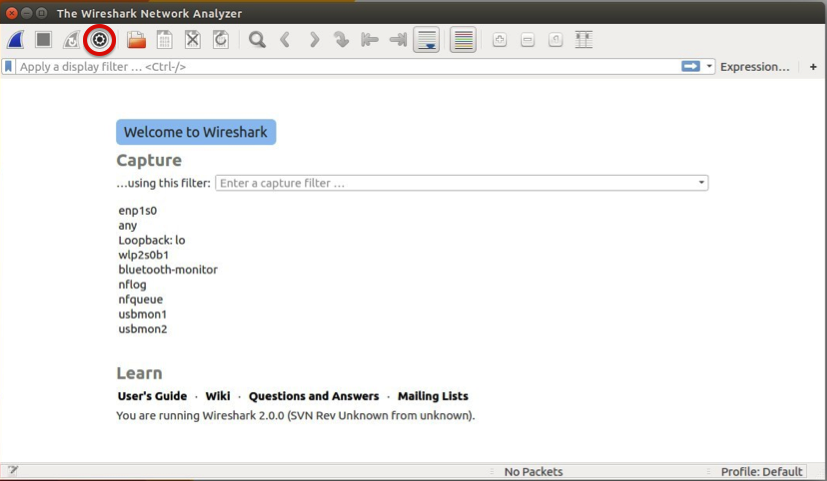
1. Abra una ventana de comandos **CMD**, escriba **ipconfig /all** y luego presione Entrar.
2. Observe la dirección IPv4 y la dirección MAC (física) de la interfaz del PC.



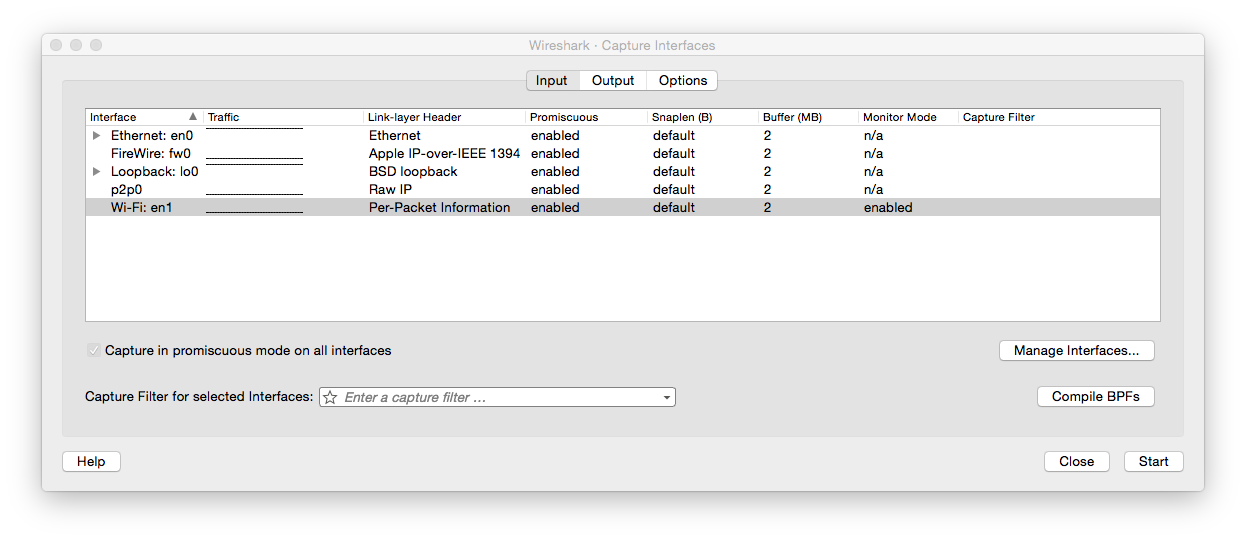
1. Solicite a un compañero o compañera la **dirección IPv4** de su PC y proporciónele a su vez la suya. ¡¡¡NO proporcione su dirección MAC!!!

Paso 3: Iniciar Wireshark y comenzar a capturar datos

1. En el 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**.
2. Una vez que se inicia Wireshark, haga clic en el icono **Capture options** (aparece en la barra de herramientas):



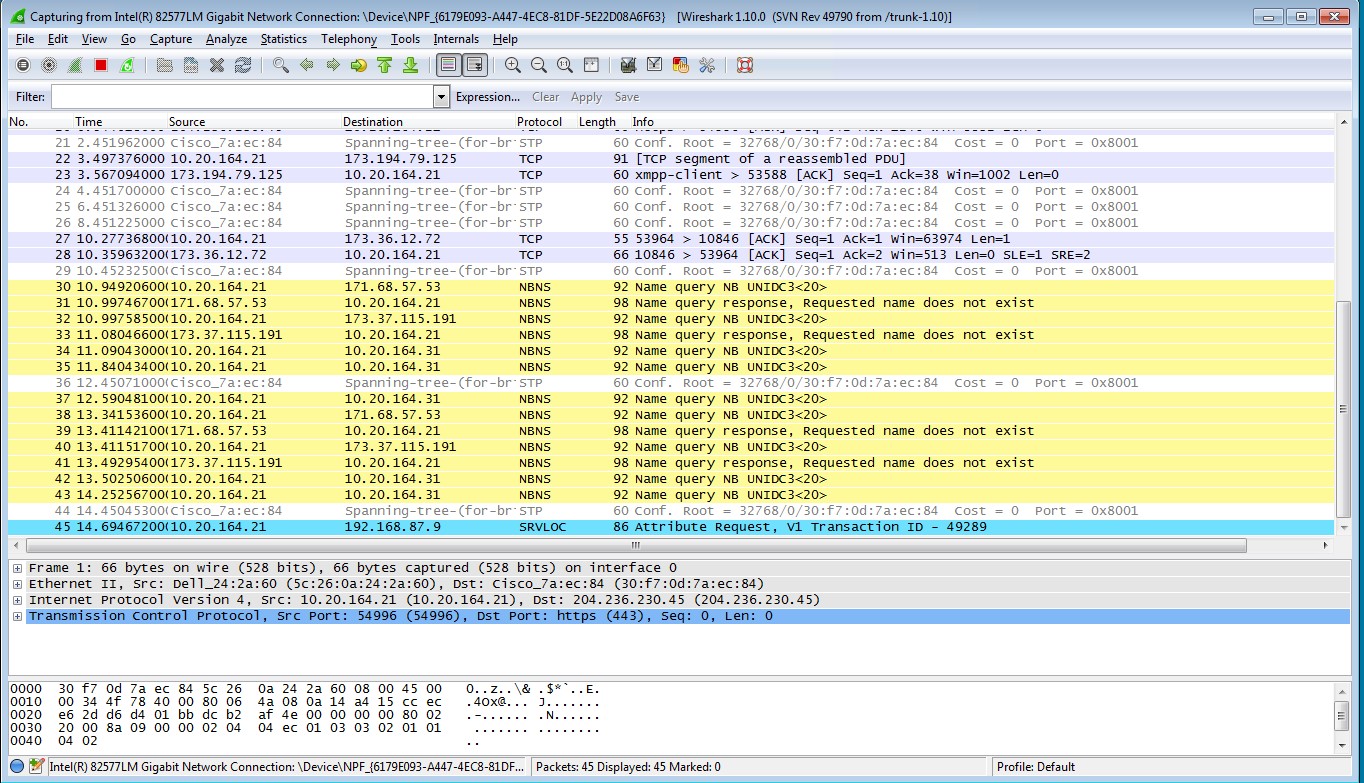
1. En la ventana Wireshark **Capture Interfaces**, observe que aparece la interfaz **Laboratorio**, que será la que utilizará para realizar las capturas de datos:



**Nota:** compruebe que tiene habilitado el modo promiscúo en esta ventana, marcando la opción **Enable promiscuous mode on all interfaces**.

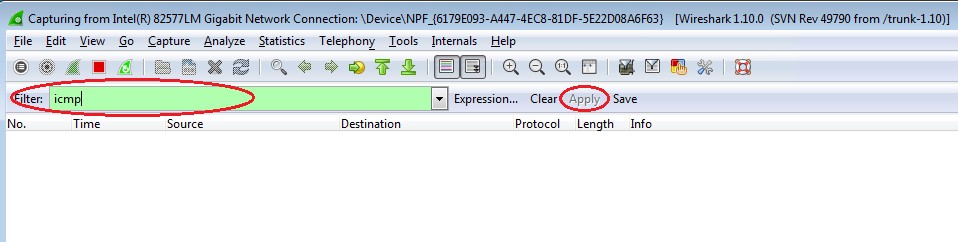
1. Después seleccione la interfaz **Laboratorio**, haga clic en **Start** (Comenzar) para comenzar la captura de datos.

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

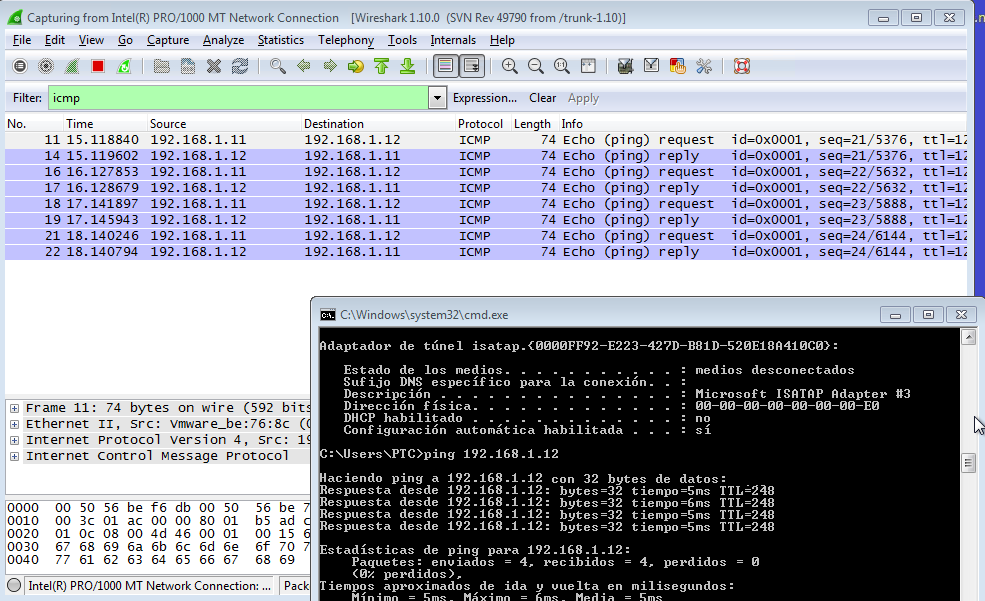


1. Es posible desplazarse muy rápidamente por esta información según la comunicación que tiene lugar entre el PC y la LAN. Se puede aplicar un filtro para facilitar la vista y el trabajo con los datos que captura Wireshark. Para esta práctica de laboratorio, sólo nos interesa mostrar las PDU de ICMP (ping). Escriba **icmp** en el cuadro **Filter** (Filtro) que se encuentra en la parte superior de Wireshark y presione Entrar

o haga clic en el botón **Apply** (Aplicar) para ver solamente PDU de ICMP (ping).

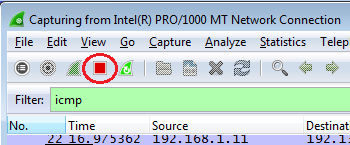


1. Este filtro hace que desaparezcan todos los datos de la ventana superior, pero se sigue capturando el tráfico en la interfaz. Abra la ventana del símbolo del sistema que abrió antes y haga ping a la dirección IPV4 que recibió del otro estudiante. Comenzará a ver que aparecen datos en la ventana superior de Wireshark nuevamente.



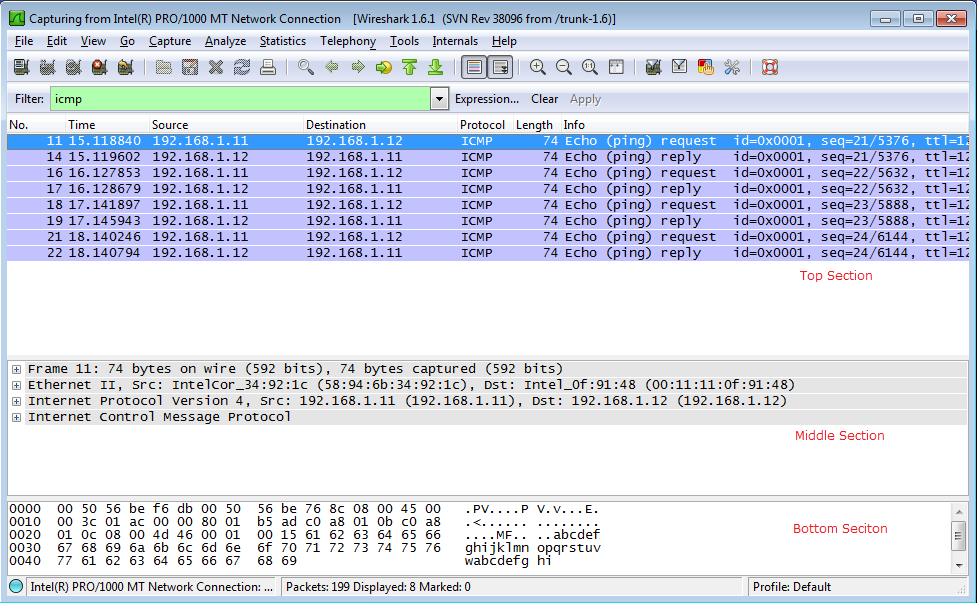
**Nota:** si el PC del compañero/a no responde a sus pings, es posible que se deba a que el firewall de ese equipo está bloqueando estas solicitudes. Puede, o bien deshabilitar el servicio Firewall o permitir el tráfico ICMP. Consulte [Apéndice A: Permitir el tráfico ICMP a través de un](#_bookmark0) [firewall](#_bookmark0) para obtener información sobre cómo permitir el tráfico ICMP a través del firewall con Windows.

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

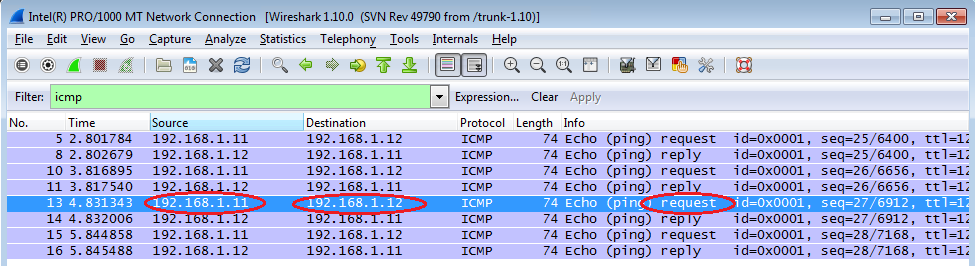


Paso 4: Examinar los datos capturados

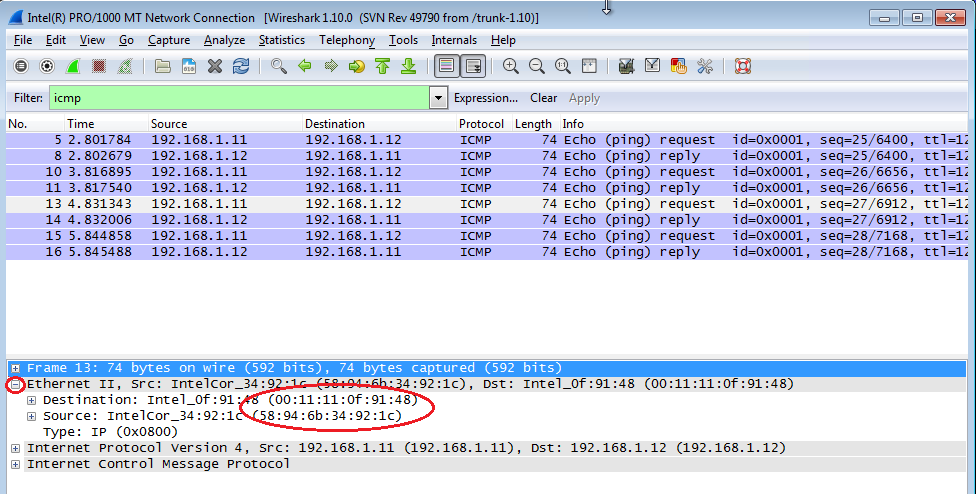
En el paso 3, examine los datos que se generaron mediante las solicitudes de ping del PC del miembro del equipo. Los datos de Wireshark se muestran en tres secciones: 1) la sección superior muestra la lista de tramas de PDU capturadas con un resumen de la información de paquetes IP enumerada, 2) la sección 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.



1. Haga clic en una **trama** **de solicitud de eco ICMP/Echo (ping) request** en la sección superior de la ventana de Wireshark. Observe que la columna **Source (Origen)** contiene la dirección IPV4 de su PC y la columna **Destination (Destino)** contiene la dirección IPV4 del PC del compañero o compañera a la que hizo ping.



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



**¿La dirección MAC origen coincide con la interfaz de su PC? \_\_\_Sí\_\_\_\_\_**

**¿La dirección MAC destino en Wireshark coincide con la dirección MAC del equipo del compañero o compañera? \_\_\_\_Sí\_\_\_\_**

\_\_\_

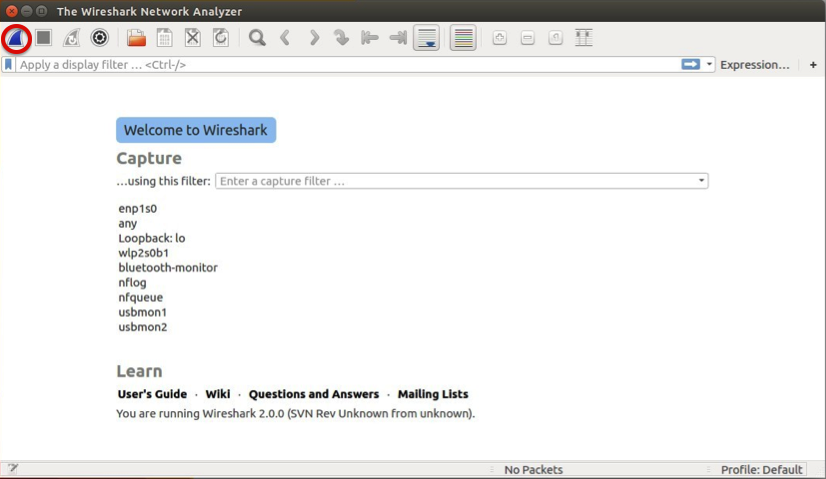
**Nota:** para el ejemplo anterior, los datos ICMP se encapsulan dentro de una **PDU paquete IPv4**, que luego se encapsula en una **PDU trama Ethernet II** para su transmisión en la LAN.

Tarea 3: Capturar y analizar datos ICMP remotos en Wireshark

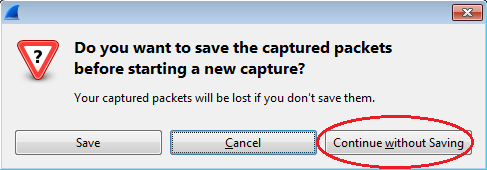
En esta tarea, hará ping a un host remoto (host que no está en la LAN) y examinará los datos generados a partir de esos pings. Luego, determinará las diferencias entre estos datos y los datos examinados en la tarea anterior.

Paso 1: Comenzar a capturar datos en la interfaz

1. Haga clic en el ícono **Start capturing packets** para volver a comenzar una nueva captura con la misma interfaz.



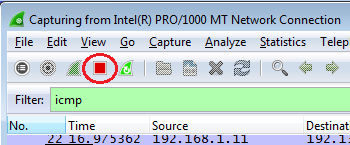
1. Se abre una ventana que le solicita guardar los datos capturados anteriormente antes de comenzar otra captura. No es necesario guardar esos datos. Haga clic en **Continue without Saving** (Continuar sin guardar).



1. Con la captura activa, haga ping a la siguiente URL del servidor **eagle-server.example.com** y capture los paquetes ICMP intercambiados.

**Nota:** al hacer ping a la dirección Web anterior (URL), observe que el servidor de nombres de dominio (DNS) traduce el URL a una dirección IPv4 (192.168.254.254).

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



Paso 2: Inspeccionar y analizar los datos de los hosts remotos

1. Revise los datos capturados en Wireshark y examine las **direcciones IP y MAC destino** de la primera **trama de solicitud de eco ICMP/Echo (ping) request**. Indique las mismas en el espacio proporcionado:

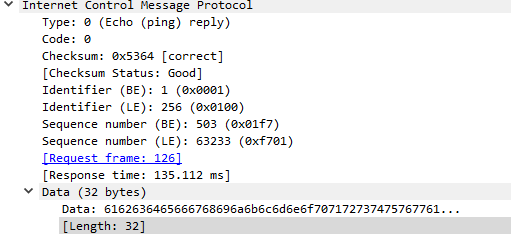
IP: 192.168.254.254

MAC: 00: 30:19:59:d1: a0

1. **¿A qué dispositivo (ver diagrama de topología) corresponde la dirección MAC destino de la trama enviada?** \_\_\_\_\_R2-Central Es el siguiente dispositivo de red que hay.
2. **¿A qué dispositivo (ver diagrama de topología) corresponde la dirección MAC origen de la trama enviada?** \_\_\_\_\_\_ mi ordenador\_\_\_\_\_\_\_\_\_\_\_\_\_
3. **¿En qué se diferencia esta información de la información de ping local que obtuvo en la tarea 2?**

**Se diferencian en el tiempo medio en el que viaja el paquete.**

1. **¿Cuál es el contenido enviado dentro del paquete de solicitud de petición de eco ICMP?**



**Reflexión**

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

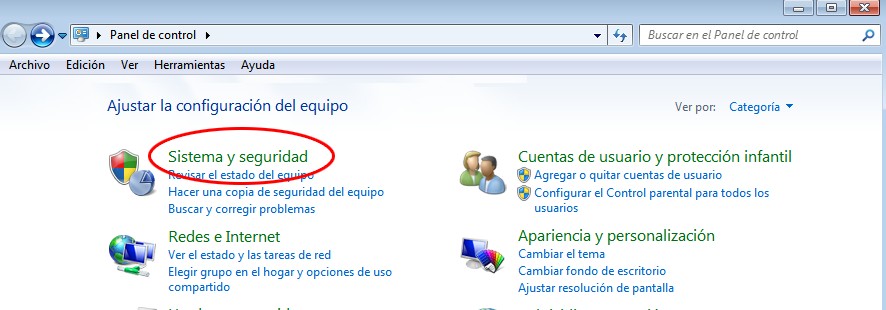
Porque la dirección mac cambia en cada paso, por tanto no aparece la mac del de los host remotos, si no del dispositivo siguiente.

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

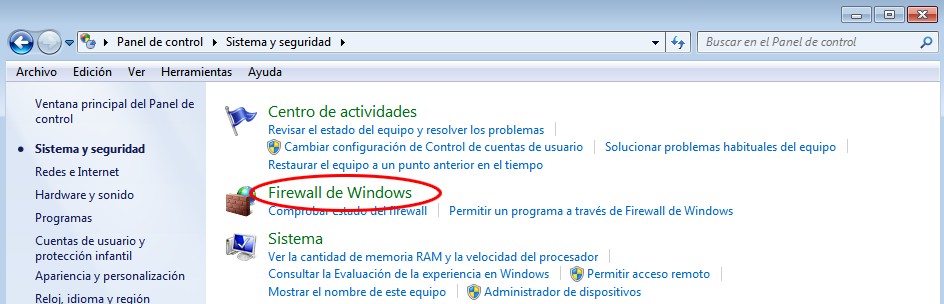
Si los miembros del equipo no pueden hacer ping a su PC, es posible que el firewall esté bloqueando esas solicitudes. En este apéndice, se describe cómo crear una regla en el firewall para permitir las solicitudes de ping. También se describe cómo deshabilitar la nueva regla ICMP después de haber completado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

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

1. En el panel de control, haga clic en la opción **Sistema y seguridad**.



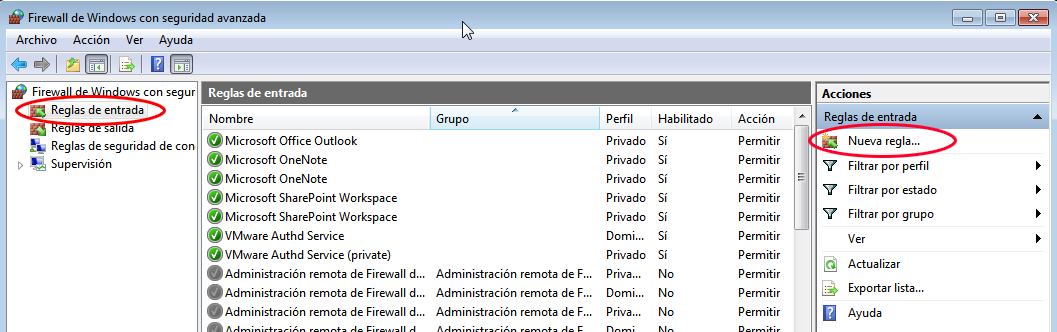
1. En la ventana Sistema y seguridad, haga clic en **Firewall de Windows**.



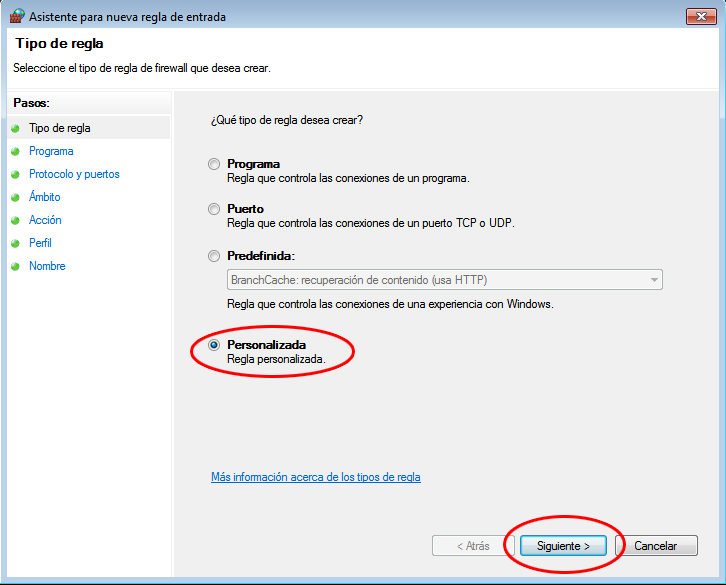
1. En el panel izquierdo de la ventana Firewall de Windows, haga clic en **Configuración avanzada**.



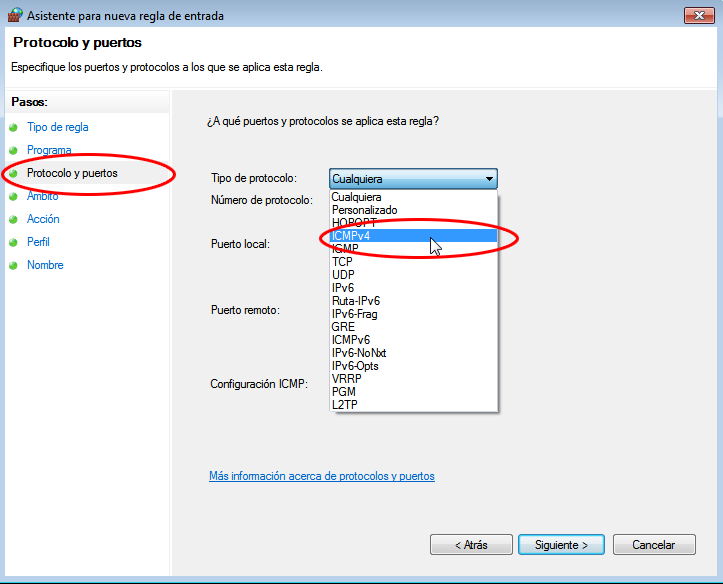
1. En la ventana Seguridad avanzada, seleccione la opción **Reglas de entrada** en la barra lateral izquierda y, a continuación, haga clic **Nueva regla** en la barra lateral derecha.



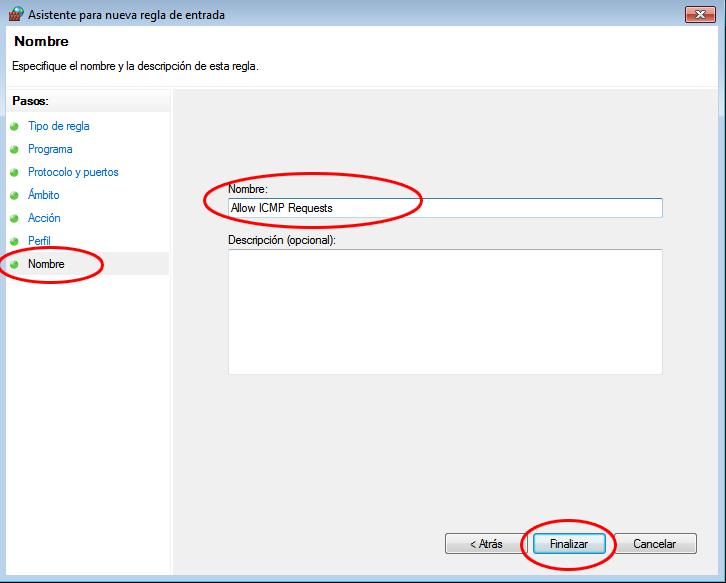
1. Se inicia el Asistente para nueva regla de entrada. En la pantalla Tipo de regla, haga clic en el botón de opción **Personalizada** y, a continuación, en **Siguiente.**



1. En el panel izquierdo, haga clic en la opción **Protocolo y puertos**, y en el menú desplegable Tipo de protocolo, seleccione **ICMPv4**; a continuación, haga clic en **Siguiente**.



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

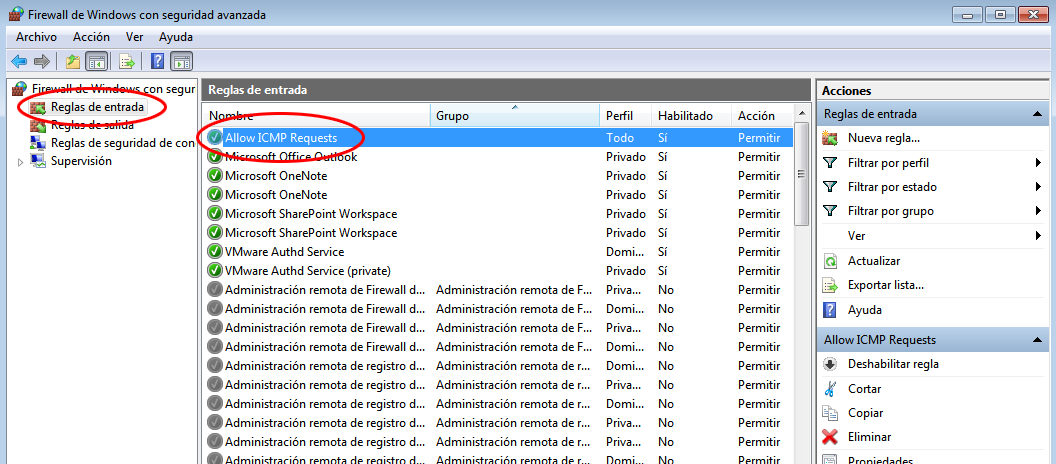


Esta nueva regla debe permitir que los miembros del equipo reciban respuestas de ping de su PC.

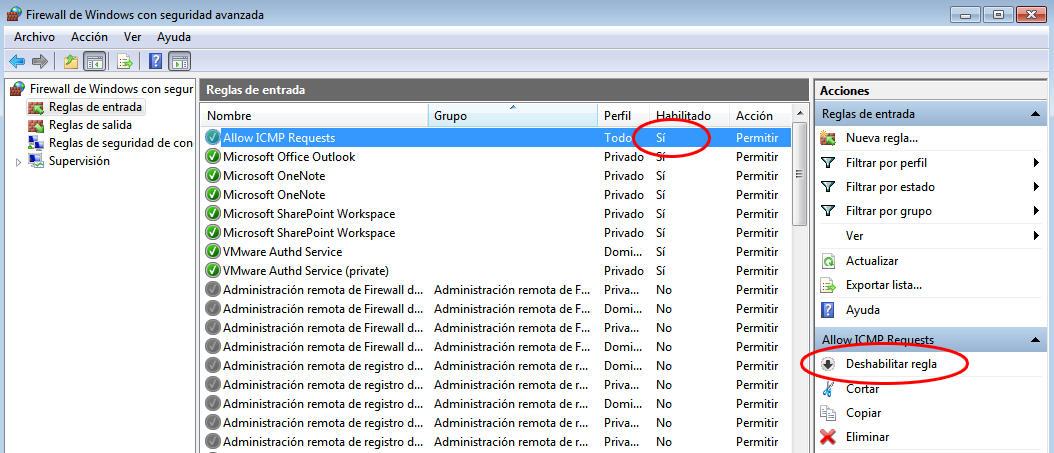
Paso 2: Deshabilitar o eliminar la nueva regla ICMP

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** 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.

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



1. Para deshabilitar la regla, haga clic en la opción **Deshabilitar regla**. Al seleccionar esta opción, verá que esta cambia a **Habilitar regla**. Puede alternar entre deshabilitar y habilitar la regla; el estado de la regla también se muestra en la columna Habilitada de la lista Reglas de entrada.



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

