Facultad de Ingeniería

Ingeniería en Informática y Sistemas

Redes I

# Laboratorio 3: Uso de Wireshark para ver el tráfico de la red

**Serie I : inicialización y recarga de un Switch**

**Topología:**

Imagen de la pantalla de un computador

Descripción generada automáticamente con confianza baja

**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 con 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 Redes 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 laptop por persona (Windows 10, 11, Mac)
* 1 switch Cisco 2960 por pareja de laboratorio

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.

* 1. Configurar direcciones IP y consultar mac-address de las tarjetas de red

Para esta práctica de laboratorio, deberá configurar una dirección IP en la tarjeta de red Ethernet de cada computadora personal.

En Windows, para configurar la dirección IP deberá seguir los siguientes pasos:

Abrir la opción de “Ejecutar” con la secuencia de comandos Windows + R

Ejecutar la instrucción “ncpa.cpl”

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

En la interfaz Ethernet dar clic derecho >> propiedades >> Protocolo de Internet versión 4

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Para 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 Intro.

b. Observe la dirección IP y la dirección MAC (física) de la interfaz de la PC.

Texto

Descripción generada automáticamente

Paso 2: Inicie Wireshark y comience a capturar datos.

* + 1. 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**.
    2. Luego de que se inicia Wireshark, dar doble clic en la interfaz Ethernet del listado de interfaces.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

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

Imagen que contiene Tabla

Descripción generada automáticamente

* + 1. 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 Filtro que se encuentra en la parte superior de Wireshark y presione Intro o haga clic en el botón Apply (Aplicar) para ver solamente PDU de ICMP (ping).

Una captura de pantalla de una red social

Descripción generada automáticamente

* + 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 IP que recibió del miembro del equipo. Comenzará a ver que aparecen datos en la ventana superior de Wireshark nuevamente.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente con confianza media

Nota: Si la PC del miembro del equipo no responde a sus pings, es posible que se deba a que el firewall de la PC está bloqueando 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 10.

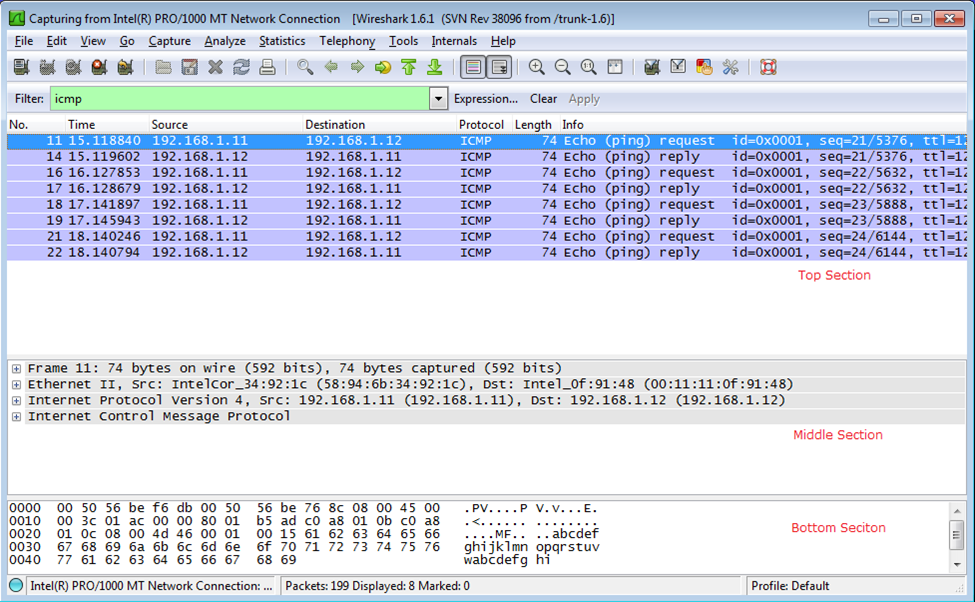
* + 1. Detenga la captura de datos haciendo clic en el ícono Stop Capture (Detener captura).

Una captura de pantalla de una red social

Descripción generada automáticamente

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.



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

Interfaz de usuario gráfica, Aplicación, Tabla

Descripción generada automáticamente

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.

Interfaz de usuario gráfica, Aplicación, Tabla

Descripción generada automáticamente

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

¿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?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Requerido:** adjunte captura de pantalla del monitor de tráfico de Wireshark.

**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.

1. 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.

* + 1. Comience una nueva captura en Wireshark de la interfaz Ethernet
    2. Con la captura activa, haga ping a los URL de los tres sitios web siguientes:
       1. [www.facebook.com](http://www.facebook.com)
       2. [www.cisco.com](http://www.cisco.com)
       3. [www.dell.com](http://www.dell.com)

Texto

Descripción generada automáticamente

**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.

* + 1. Detenga la captura de datos en Wireshark luego de realizar los tres ping.
  1. Inspeccione y analice los datos de los hosts remotos.
     1. 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: \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_ MAC: \_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_

2.a ubicación: IP: \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_ MAC: \_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_

3.a ubicación: IP: \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_ MAC: \_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_

* + 1. ¿Qué es importante sobre esta información?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Requerido:** adjunte captura de pantalla del monitor de tráfico de Wireshark.

1. Reflexión

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_