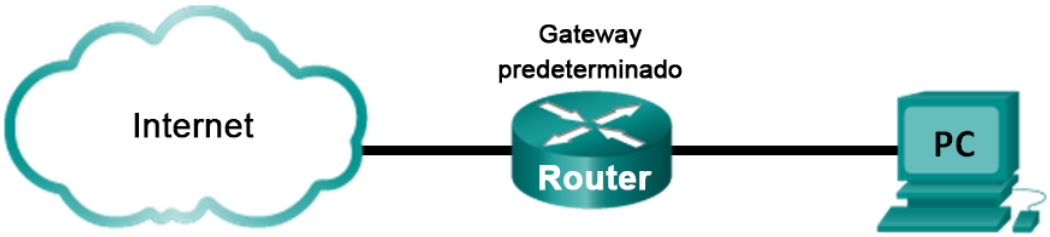
Práctica de laboratorio: Uso de Wireshark para examinar una captura de UDP y DNS

Topología



Objetivos

Parte 1: Registrar la información de configuración IP de una PC

Parte 2: Utilizar Wireshark para capturar consultas y respuestas DNS

Parte 3: Analizar los paquetes DNS o UDP capturados

Información básica/Situación

Si alguna vez usó Internet, usó el Sistema de nombres de dominios (DNS). El DNS es una red distribuida de servidores que traduce nombres de dominio fáciles de usar, como www.google.com, en una dirección IP. Cuando escribe el URL de un sitio Web en el explorador, la PC realiza una consulta DNS a la dirección IP del servidor DNS. La consulta del servidor DNS de la PC y la respuesta del servidor DNS utilizan el protocolo de datagramas de usuario (UDP) como el protocolo de la capa de transporte. UDP opera sin conexión y no requiere una configuración de sesión como TCP. Las consultas y respuestas DNS son muy pequeñas y no requieren la sobrecarga de TCP.

En esta práctica de laboratorio, se comunicará con un servidor DNS enviando una consulta DNS mediante el protocolo de transporte UDP. Utilizará Wireshark para examinar los intercambios de consultas y respuestas DNS con el servidor de nombres.

Nota: esta práctica de laboratorio no se puede realizar utilizando Netlab. Para la realización de esta práctica de laboratorio, se da por sentado que tiene acceso a Internet.

Recursos necesarios

1 PC (Windows 7, Vista o XP con acceso al símbolo del sistema, acceso a Internet y Wireshark instalado)

Parte 1: Registrar la información de configuración IP de la PC

En la parte 1, utilizará el comando **ipconfig /all** en la PC local para buscar y registrar las direcciones MAC e IP de la tarjeta de interfaz de red (NIC) de la PC, la dirección IP del gateway predeterminado especificado y la dirección IP del servidor DNS especificada para la PC. Registre esta información en la tabla proporcionada. La información se utilizará en las partes siguientes de esta práctica de laboratorio con análisis de paquetes.

Dirección IP	
Dirección MAC	
Dirección IP de la puerta de enlace predeterminada	
Dirección IP del servidor DNS	

Parte 2: Utilizar Wireshark para capturar consultas y respuestas DNS

En la parte 2, configurará Wireshark para capturar paquetes de consultas y respuestas DNS para demostrar el uso del protocolo de transporte UDP mientras se comunica con un servidor DNS.

a. Haga clic en el botón **Inicio** de Windows y navegue hasta el programa Wireshark.

   Nota: si Wireshark aún no está instalado, se puede descargar de http://www.wireshark.org/download.html.

b. Seleccione una interfaz para que Wireshark capture paquetes. Utilice **Interface List** (Lista de interfaces) para elegir la interfaz asociada a las direcciones IP y de control de acceso al medio (MAC) registradas de la PC en la parte 1.

c. Después de seleccionar la interfaz deseada, haga clic en **Start** (Comenzar) para capturar los paquetes.

d. Abra un explorador Web y escriba **www.google.com**. Presione Entrar para continuar.

e. Haga clic en **Stop** (Detener) para detener la captura de Wireshark cuando vea la página de inicio de Google.

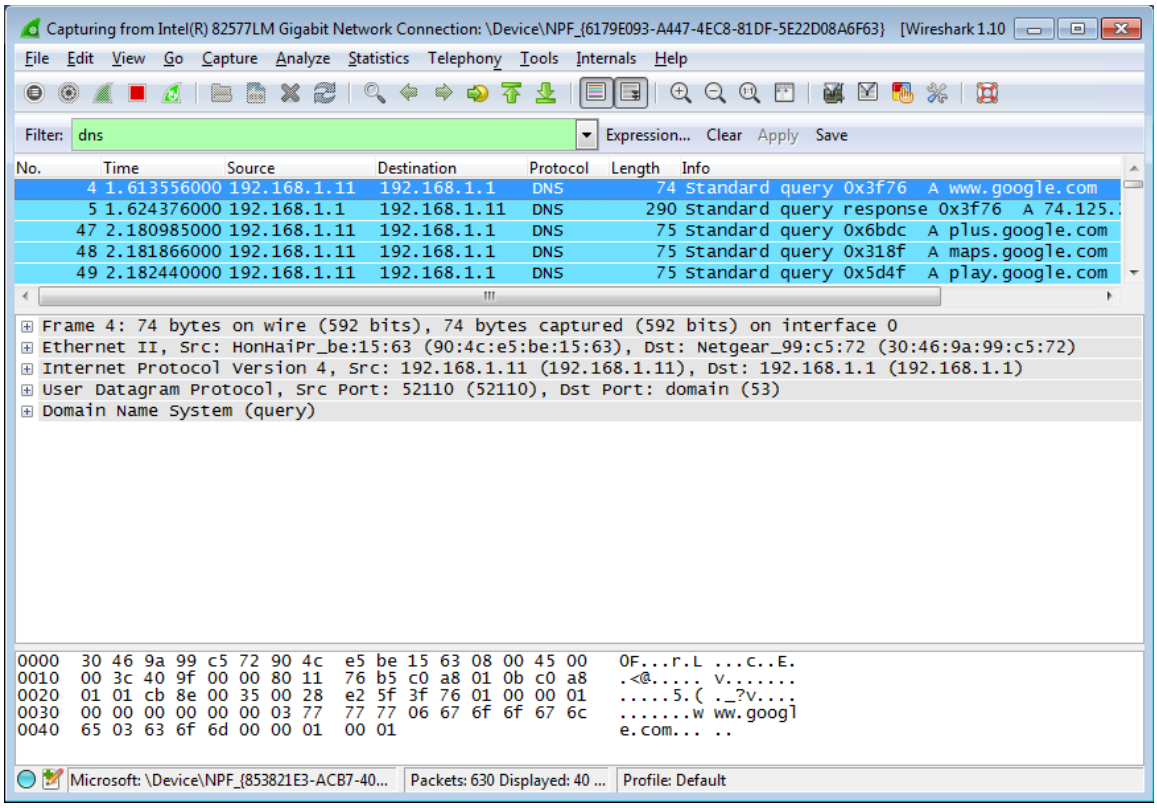
Parte 3: Analizar los paquetes DNS o UDP capturados

En la parte 3, examinará los paquetes UDP que se generaron al comunicarse con un servidor DNS para las direcciones IP para www.google.com.

Paso 1: Filtrar paquetes DNS

a. En la ventana principal de Wireshark, escriba **dns** en el área de entrada de la barra de herramientas **Filter** (Filtrar). Haga clic en **Apply** (Aplicar) o presione Entrar.

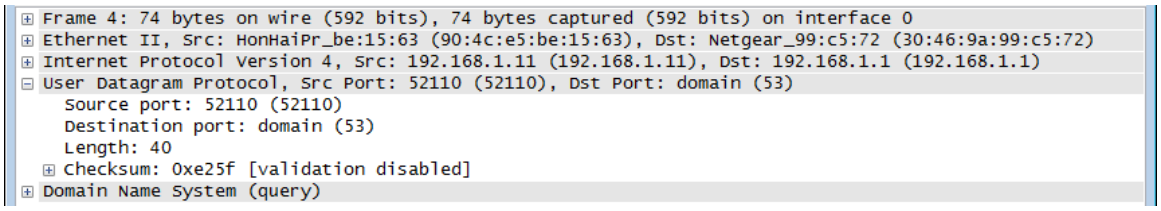
   Nota: si no ve resultados después de aplicar el filtro DNS, cierre el explorador Web y, en la ventana del símbolo del sistema, escriba **ipconfig /flushdns** para eliminar todos los resultados anteriores del DNS. Reinicie la captura de Wireshark y repita las instrucciones de la parte 2b a la parte 2e. Si el problema no se resuelve, en la ventana del símbolo del sistema, puede escribir **nslookup www.google.com** como alternativa para el explorador Web.



b. En el panel de la lista de paquetes (sección superior) de la ventana principal, ubique el paquete que incluye “standard query” (consulta estándar) y “A www.google.com”. Vea la trama 4, por ejemplo.

Paso 2: Examinar el segmento UDP mediante una consulta DNS

Examine UDP mediante una consulta DNS para www.google.com según lo capturado por Wireshark. En este ejemplo, está seleccionada la trama 4 de la captura de Wireshark en la lista de paquetes para su análisis. Los protocolos en esta consulta se muestran en el panel de detalles del paquete (sección media) de la ventana principal. Las entradas del protocolo están resaltadas en gris.



a. En el panel de detalles del paquete, la trama 4 tenía 74 bytes de datos en el cable, tal como se muestra en la primera línea. Esta es la cantidad de bytes para enviar una consulta DNS a un servidor de nombres que solicita direcciones IP de www.google.com.

b. En la línea Ethernet II, se muestran las direcciones MAC de origen y destino. La dirección MAC de origen proviene de la PC local, ya que esta originó la consulta DNS. La dirección MAC de destino proviene del gateway predeterminado, dado que esta es la última parada antes de que la consulta abandone la red local.

¿La dirección MAC de origen es la misma que la que se registró en la parte 1 para la PC local?

c. En la línea Internet Protocol Version 4 (Protocolo de Internet versión 4), la captura de Wireshark de paquetes IP indica que la dirección IP de origen de esta consulta DNS es 192.168.1.11 y la dirección IP de destino es 192.168.1.1. En este ejemplo, la dirección de destino es el gateway predeterminado. El router es el gateway predeterminado en esta red.

¿Puede emparejar las direcciones IP y MAC para los dispositivos de origen y destino?

Dispositivo	Dirección IP	Dirección MAC
PC local		
Gateway predeterminado		

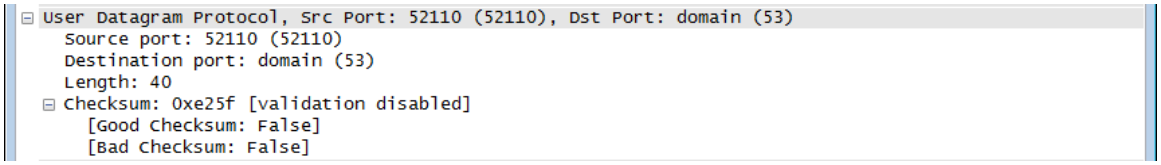
El paquete y el encabezado IP encapsulan el segmento UDP. El segmento UDP contiene la consulta DNS como los datos.

d. Un encabezado UDP solo tiene cuatro campos: source port (puerto de origen), destination port (puerto de destino), length (longitud) y checksum. Cada campo en el encabezado UDP es de solo 16 bits, como se ilustra a continuación.

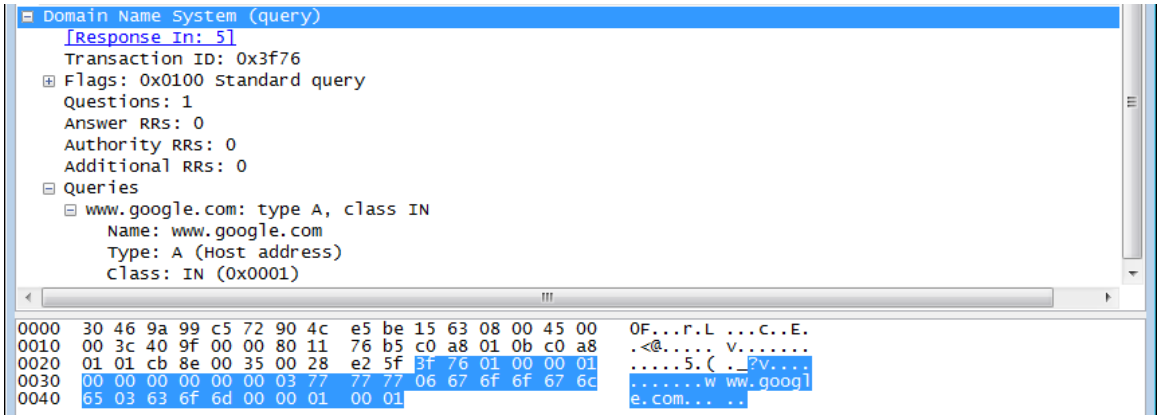
SEGMENTO UDP

0	16	31
PUERTO DE ORIGEN UDP	PUERTO DE DESTINO UDP	
LONGITUD DE MENSAJE UDP	CHECKSUM DE UDP	
DATOS		
DATOS...		

Amplíe el protocolo de datagramas de usuario en el panel de detalles del paquete haciendo clic en el signo más (+). Observe que hay solo cuatro campos. El número de puerto de origen en este ejemplo es 52110. La PC local generó el puerto de origen aleatoriamente utilizando los números de puerto que no están reservados. El puerto de destino es 53. El puerto 53 es un puerto conocido reservado para ser utilizado con DNS. En el puerto 53, los servidores DNS escuchan las consultas DNS de los clientes.



En este ejemplo, la longitud de este segmento UDP es de 40 bytes. De los 40 bytes, 8 bytes se utilizan como encabezado. Los otros 32 bytes los utilizan los datos de la consulta DNS. Estos 32 bytes están resaltados en la ilustración siguiente en el panel de bytes del paquete (sección inferior) de la ventana principal de Wireshark.



El valor de checksum se usa para determinar la integridad del paquete después de haber atravesado Internet.

El encabezado UDP tiene una sobrecarga baja, porque UDP no tiene campos asociados con el protocolo de enlace de tres vías en TCP. Cualquier problema de confiabilidad de transferencia de datos que ocurra debe solucionarse en la capa de aplicación.

Registre los resultados de Wireshark en la tabla siguiente:

Tamaño de trama	
Dirección MAC de origen	
Dirección MAC de destino	
Dirección IP de origen	
Dirección IP de destino	
Puerto de origen	
Puerto de destino	

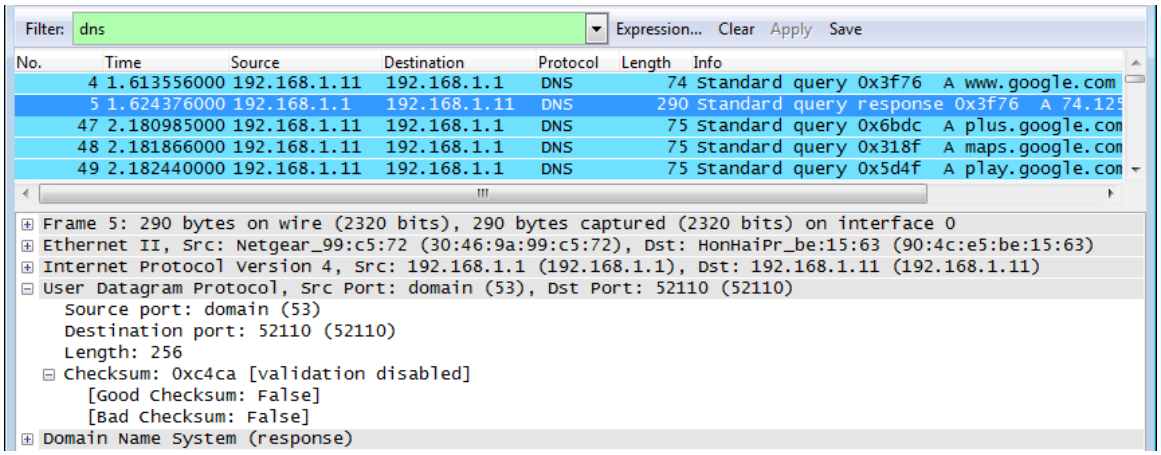
¿La dirección IP de origen es la misma que la dirección IP de la PC local registrada en la parte 1?

¿La dirección IP de destino es la misma que el gateway predeterminado que se registró en la parte 1?

Paso 3: Examinar el UDP usando la respuesta DNS

En este paso, examinará el paquete de respuesta DNS y verificará que este también utilice UDP.

a. En este ejemplo, la trama 5 es el paquete de respuesta DNS correspondiente. Observe que la cantidad de bytes en el cable es 290 bytes. Es un paquete más grande con respecto al paquete de consulta DNS.



b. En la trama Ethernet II para la respuesta DNS, ¿de qué dispositivo proviene la dirección MAC de origen y de qué dispositivo proviene la dirección MAC de destino?

c. Observe las direcciones IP de origen y destino en el paquete IP. ¿Cuál es la dirección IP de destino? ¿Cuál es la dirección IP de origen?

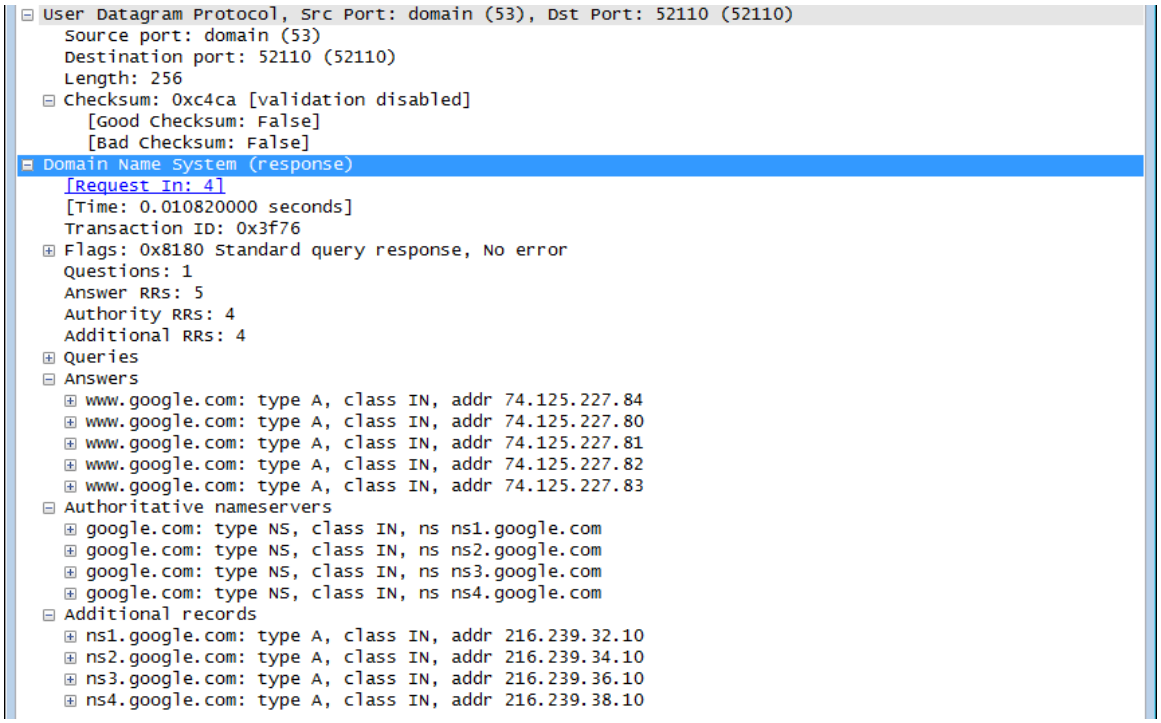
Dirección IP de destino: Dirección IP de origen:

¿Qué ocurrió con los roles de origen y destino para el host local y el gateway predeterminado?

d. En el segmento UDP, el rol de los números de puerto también se invirtió. El número de puerto de destino es 52110. El número de puerto 52110 es el mismo puerto que el que generó la PC local cuando se envió la consulta DNS al servidor DNS. La PC local escucha una respuesta DNS en este puerto.

El número de puerto de origen es 53. El servidor DNS escucha una consulta DNS en el puerto 53 y luego envía una respuesta DNS con un número de puerto de origen 53 de vuelta a quien originó la consulta DNS.

Cuando la respuesta DNS esté expandida, observe las direcciones IP resueltas para www.google.com en la sección **Answers** (Respuestas).



Reflexión

¿Cuáles son los beneficios de utilizar UDP en lugar de TCP como protocolo de transporte para DNS?