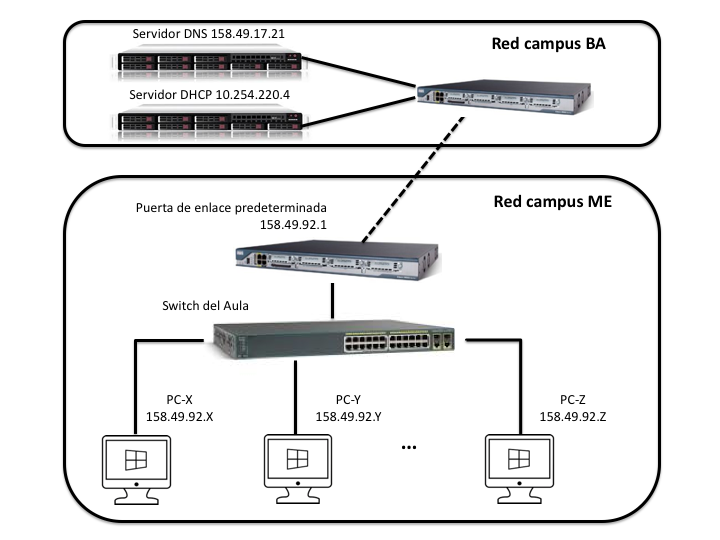
**AL04-2. Investigación de protocolos de capa de Aplicación con Wireshark: DNS**

Diagrama de topología

****

**Objetivos**

**Tarea 1: Propiedades de red del PC**

**Tarea 2: Capturar y analizar consultas/respuestas DNS**

**Información básica**

Si alguna vez usaste Internet, también usaste 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,](http://www.google.com/) en una dirección IP. También recibe este nombre el **protocolo de comunicación de la capa de Aplicación** encargado de regular el funcionamiento de este servicio (RFC 1034/1035). Cuando escribes la dirección (URL) de un sitio Web en el navegador, el PC habitualmente realiza una consulta DNS a la dirección IP del servidor DNS preferido configurada en los parámetros de red. La consulta al servidor DNS desde el PC y la respuesta del servidor DNS utilizan el protocolo de datagramas de usuario (**UDP**) como protocolo de la **capa de Transporte**. Las consultas y respuestas DNS son de tamaño muy pequeño comparadas con las peticiones/respuestas enviadas por otros protocolos de la capa de Aplicación como HTTP o FTP y no requieren una transferencia confiable.

Recursos necesarios

1 PC con Wireshark conectado a Internet.

**Tarea 1: Propiedades de red del PC**

Asegúrate que la configuración de las **propiedades de red del adaptador Ethernet** conectado a la red del campus (**Internet**) para el **Protocolo de Internet IPv4** tiene marcadas las opciones **Obtener una dirección IP automáticamente** y **Obtener la dirección del servidor DNS automáticamente**. En caso contrario, cámbialas por las opciones anteriores. Recopila la información de la tabla mediante el comando **ipconfig /all** en el Símbolo del sistema (**CMD**) para ese adaptador.

|  |  |
| --- | --- |
| **Dirección IP** | 158.49.92.132 |
| **Dirección MAC** | FC-AA-14-07-89-E2 |
| **Dirección IP de la puerta de enlace predeterminada** | 158.49.92.1 |
| **Direcciones IP de los servidores DNS locales** | 158.49.17.21  158.49.113.21 |

Para verificar tu conexión a Internet, haz una prueba de conectividad con el comando **PING** a la dirección IP de la **puerta de enlace** **predeterminada** y después, si es correcto, a la dirección de un host externo como **www.cisco.com**.

Tarea 2: Capturar y analizar consultas/respuestas DNS

**Paso 1. Capturar paquetes correspondientes a las consultas/respuestas DNS**

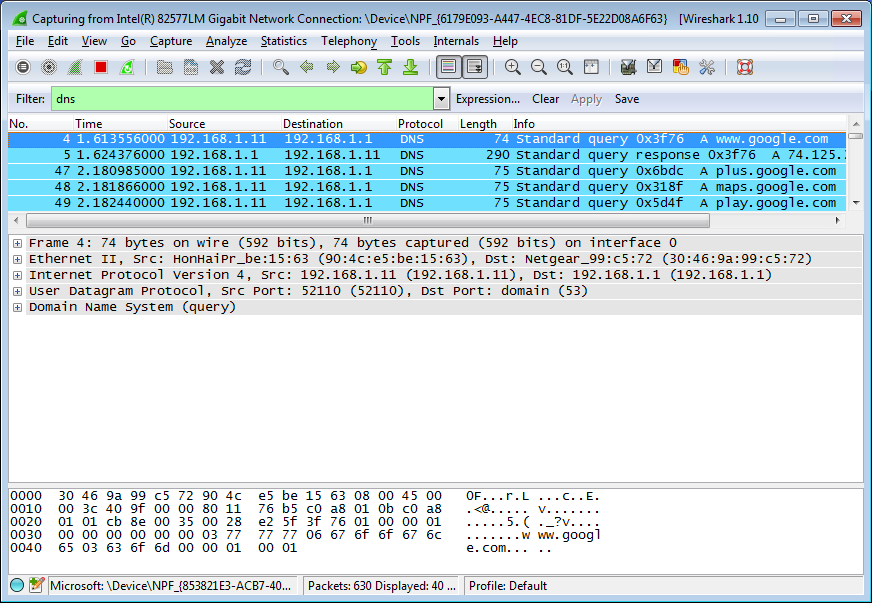
En la tarea 2 utilizarás Wireshark para la captura de paquetes de consultas (**query**) y respuestas (**response**) **DNS**, observarás el proceso de encapsulamiento e investigarás encabezados correspondientes a las PDUs en cada capa.

1. Primero, para forzar el envío de solicitudes DNS al servidor asignado, vacía la caché DNS del PC. En Windows usar el comando **ipconfig /flushdns**.
2. Abre el navegador Web. Vacía la caché web del navegador o utiliza una **ventana de incógnito o privada.**
3. Haz clic en el botón **Inicio** de Windows y abre el programa Wireshark.
4. Después de seleccionar la interfaz deseada, haz doble clic sobre el identificador de la misma o clic en **Start** para comenzar la captura de los paquetes.
5. Para localizar más rápido las tramas relacionadas con la consulta DNS, introduce el filtro de visualización **ip.addr==dirección\_IP\_de\_tu\_PC&&dns.qry.name==gaia.cs.umass.edu** en el área de entrada de la barra de herramientas **Filter** (Filtrar) para una búsqueda más precisa.
6. Vuelve al navegador Web y escribe la dirección Web **http://gaia.cs.umass.edu.** Presiona Entrar para continuar.
7. Haz clic en **Stop** (Detener) para detener la captura de Wireshark cuando vea la página de inicio del servidor.
8. Guarda la captura como **AL04-2.pcapng.**

Paso 2. Analizar los datos capturados

Observa las tramas número 4 y 5 del ejemplo en la Figura 1. En el panel de **Lista de paquetes** (sección superior) de la ventana principal aparece como seleccionada la **trama número 4** que incluye una **consulta estándar DNS (standard query)** para un **registro de recurso tipo A** correspondiente al nombre de dominio [**www.google.com**](http://www.google.com/)**.** Localiza estas mismas tramas para la consulta/respuesta DNS que has capturado en el laboratorio para el nombre de dominio **gaia.cs.umass.edu**.

**Nota:** si no ves resultados, cierra el navegador Web y en la ventana del símbolo del sistema escribe **ipconfig /flushdns** para eliminar todos los resultados anteriores del DNS. Reinicia la captura de Wireshark y repita las instrucciones de la Tarea 2, paso 1. Si el problema no se resuelve, ve a la ventana del símbolo del sistema y prueba a escribir **nslookup gaia.cs.umass.edu** como alternativa al navegador Web.



**Figura 1**. Ejemplo de captura de consulta estándar DNS

Selecciona el **mensaje de consulta DNS realizada** y responde a las siguientes preguntas:

1. En el panel **Detalles del paquete**, **la trama 4** correspondiente a la consulta DNS del ejemplo tenía **74 bytes** **de datos en el cable (on wire),** tal como se muestra en la línea **Frame**. Esta es la cantidad de bytes totales que se envían a la red al enviar la consulta DNS al servidor DNS local para el nombre [www.google.com.](http://www.google.com/) ¿Cuánta información total se envía en el caso de la consulta DNS realizada para **gaia.cs.umass.edu**?

Se envían 74 bits on wire (616 bits).

1. En la línea **Ethernet II,** se muestran las direcciones MAC de origen y destino. La dirección MAC de origen proviene del PC local ya que es el origen la consulta DNS. ¿A qué dispositivo según el diagrama de topología corresponde la dirección MAC destino? ¿La dirección MAC origen es la misma que la registrada en la tabla durante la tarea 1 para el PC local?

MAC destino: 00:11:88:05:61:15

1. En la línea **Internet Protocol Version 4**, la captura de Wireshark 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. Por tanto, en este ejemplo la dirección de destino es el propio gateway predeterminado. En entornos domésticos es habitual que el CPE sea el encargado de reenviar las consulta DNS (Relay DNS) a los servidores indicados por el ISP en la configuración del propio CPE. ¿Crees qué ocurre lo mismo en la captura que tú has realizado? Explícalo.

No, ya que

1. ¿Puedes emparejar las direcciones IP y MAC para los dispositivos de origen y destino a partir de la información de la consulta DNS capturada con Wireshark?

|  |  |  |
| --- | --- | --- |
| **Dispositivo** | **Dirección IP** | **Dirección MAC** |
| **PC local** | 158.49.92.132 | FC-AA-14-07-89-E2 |
| **Gateway predeterminado** |  |  |
| **Servidor DNS** | 128.119.245.12 |  |

1. Observa la PDU de capa de Transporte para la consulta DNS y el mensaje de respuesta. ¿Son enviados a través de UDP o TCP?

UDP

1. En la captura de Wireshark, expande la línea **User Datagram Protocol** en el panel **Detalles del paquete** haciendo clic en el signo más (+). Observa que hay sólo cuatro campos. El número de puerto origen (**source port**), que en el ejemplo de la Figura 1 es **52110**, el PC origen lo genera aleatoriamente utilizando los números de puerto que no están reservados. El puerto destino (**destination port**) será el puerto **53** que es un **puerto conocido** reservado para ser utilizado por los clientes para enviar las consultas DNS. En el puerto 53 los servidores DNS escuchan las consultas DNS de los clientes. ¿Cuál es el número de puerto origen? ¿Cuál es el número de puerto destino? ¿Coinciden total o parcialmente con la Figura 1? Explícalo.

Puerto de origen: 532313

Puerto destino: 53

Coinciden parcialmente, en el puerto del destino, ya que es el puerto que utiliza el servidor DNS.

1. Examina la línea **Domain Name System (query)** ¿Qué “tipo” de consulta DNS es? ¿El mensaje de consulta contiene alguna “respuesta” (buscar campo **Answer RRs**)?

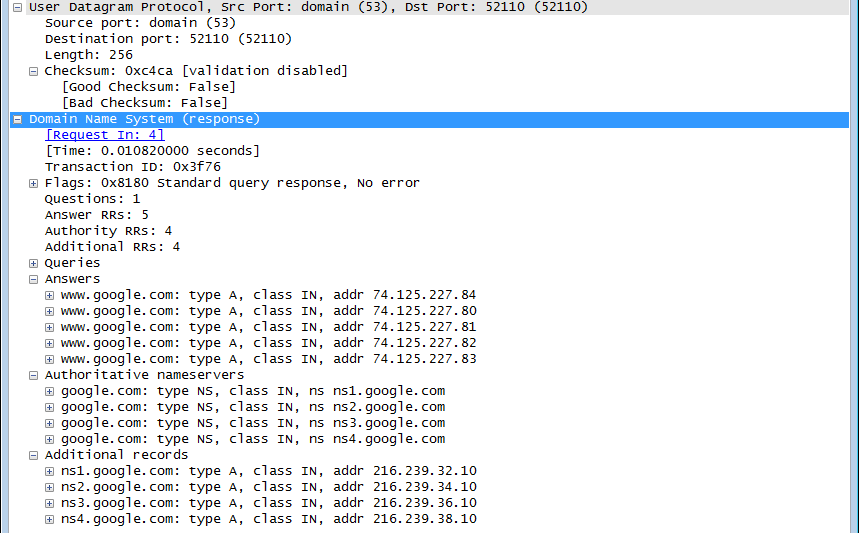
Es de tipo A.

No contiene respuesta, ya que Anwer RRs = 0

Selecciona el **mensaje de respuesta DNS correspondiente** y responde a la siguiente pregunta:

1. Examina la línea **Domain Name System (response)**. La Figura 2 muestra la sección **Answers** de la respuesta DNS del ejemplo mostrado en la Figura 1, con un total de 5 direcciones IP resueltas por el servidor DNS local para el nombre de dominio [www.google.com](http://www.google.com/). En la captura de Wireshark realizada observa las direcciones IP resueltas para **gaia.cs.umass.edu** en la sección **Answers.** ¿Cuántas direcciones aparecen (buscar campo **Answer RRs**)? Incluye un listado con esas direcciones.

Aparacecen sólo una dirección, ya que



**Figura 2**. Ejemplo del campo Answers de una respuesta DNS