**Práctica 2 (II): DNS[[1]](#footnote-0)**

**Descripción**

El Sistema de Nombres de Dominio (DNS) traduce los nombres de host a direcciones IP, cumpliendo un papel crítico en la infraestructura de Internet. En esta práctica, vamos a echar un vistazo más de cerca en el lado del cliente de DNS. Recordemos que el papel del cliente DNS es relativamente sencillo, un cliente envía una consulta a su servidor DNS local y recibe una respuesta. Sin embargo, muchas cosas pueden suceder “tras bambalinas”, invisibles a los clientes DNS, como que los servidores DNS jerárquicos se comunican entre sí para resolver, ya sea de forma recursiva o iterativa, una consulta DNS del cliente. Desde el punto de vista del cliente DNS, sin embargo, el protocolo es muy simple una consulta está formulado para el servidor DNS local y se recibe una respuesta de ese servidor.

**Objetivos**

Explorar el protocolo DNS:

* Uso de nslookup
* Uso ipconfig para la gestión de información
* Seguimiento con Wireshark

**Tareas**

**Parte 1. NSLOOKUP**

La herramienta nslookup, está disponible en la mayoría de los sistemas Linux/Unix y Windows. Para ejecutarlo en Windows, abre el símbolo del sistema y ejecute nslookup en la línea de comandos. Esta es la operación más básica, la herramienta nslookup permite al host que lo ejecuta consultar cualquier servidor DNS especificado para un registro DNS. El servidor DNS consultado puede ser un servidor DNS de la raíz, un servidor de dominio de nivel superior, un servidor DNS autoritativo, o un servidor de DNS intermedio. Para realizar esta tarea, nslookup envía una consulta DNS al servidor DNS especificado, recibe una respuesta DNS de ese mismo servidor DNS y muestra el resultado.

La captura de la Figura 1 muestra los resultados de tres comandos nslookup independientes (que se muestra en el símbolo del sistema de Windows). En este ejemplo, la máquina cliente se encuentra en el campus de la Universidad Politécnica de Brooklyn, donde el servidor DNS local por defecto es dns-prime.poly.edu. Cuando se ejecuta nslookup, si no se especifica ningún servidor DNS, nslookup envía la consulta al servidor DNS por defecto, que en este caso es dns-prime.poly.edu.

Considere el primer comando: **nslookup www.mit.edu**

En otras palabras, este comando está diciendo “por favor me envía la dirección IP para de www.mit.edu”. Como se muestra en la pantalla, la respuesta de este comando proporciona dos tipos de información:

1. El nombre y la dirección IP del servidor DNS que proporciona la respuesta
2. La respuesta en sí, que es el nombre de host y la dirección IP de www.mit.edu. Aunque la respuesta vino desde el servidor DNS local de la Universidad Politécnica, es muy posible que este servidor DNS local se contactará de forma iterativa a varios servidores DNS para obtener la respuesta.



Figura 1. Comando nslookup con www.mit.edu

Consideremos ahora el segundo comando: **nslookup -type=NS mit.edu**

En este ejemplo, hemos proporcionado la opción “-type=NS” y el dominio “mit.edu”. Esto hace que nslookup envie una consulta a un registro de tipo=NS para el servidor DNS local por defecto. Es decir, la consulta está diciendo: “Por favor, envíenme los nombres del host del DNS autorizado para mit.edu”. (Si no se utiliza la opción de tipo, nslookup utiliza el valor predeterminado, que es para consultar registros de tipo A). La respuesta, que se muestra en la Figura 1, indica primero el servidor DNS que está proporcionando la respuesta (que es el servidor DNS local por defecto) junto con tres servidores de nombres del MIT. Cada uno de estos servidores es un servidor DNS con autoridad para los anfitriones en el campus del MIT. Sin embargo, nslookup también indica que la respuesta es “no autorizada”, lo que significa que esta respuesta vino de la memoria caché de algún servidor en lugar de un servidor DNS con autoridad MIT. Por último, la respuesta también incluye las direcciones IP de los servidores DNS autorizados en el MIT. (A pesar de que la consulta de tipo NS generada por nslookup no pide explícitamente las direcciones IP, el servidor DNS local las devolvió “gratis” y nslookup muestra el resultado.)

Ahora, finalmente, considerar el tercer comando: **nslookup www.aiit.or.kr bitsy.mit.edu**

En este ejemplo, indicamos que queremos la consulta sea enviada al servidor DNS bitsy.mit.edu en lugar de al servidor DNS por defecto (dnsprime.poly.edu). Por lo tanto, la operación de consulta y respuesta tiene lugar directamente entre nuestro anfitrión y la consulta bitsy.mit.edu. En este ejemplo, el servidor DNS bitsy.mit.edu proporciona la dirección IP del anfitrión www.aiit.or.kr, que es un servidor web en el Instituto Avanzado de Tecnología de la Información (en Corea).

Una vez vistos estos ejemplos, realiza las siguientes tareas y responde a las cuestiones planteadas

1. Ejecuta nslookup para obtener la dirección de IP del servidor web de la Universidad de Vigo ([www.uvigo.es](http://www.uvigo.es)). ¿Cuál es la dirección IP de ese servidor? ¿Y la del servidor DNS?

Ip servidor: 193.146.32.200

Ip DNS: 1.1.1.1

1. Ejecuta nslookup para determinar los servidores DNS autorizados para la Universidad de Vigo

uvigo.es nameserver = chico.rediris.es

uvigo.es nameserver = sun.rediris.es

uvigo.es nameserver = dns2.uvigo.es

uvigo.es nameserver = dns.uvigo.es

1. Ejecuta nslookup de modo que uno de los servidores DNS autorizados obtenidos en la pregunta (2) es consultado por la dirección IP de faitic.uvigo.es. ¿Cuál es su dirección IP?

193.146.32.203

**Parte 2. IPCONFIG**

Además de los usos que se vieron para ipconfig en la Práctica 1(I), también es muy útil para la gestión de la información DNS almacenada en la caché del host.

Para ver los registros almacenados en caché: **ipconfig /displaydns**

Para borrar la caché: **ipconfig /flushdns**

**Parte 3. Seguimiento de DNS con Wireshark**

Ahora que estas familiarizado con nslookup y ipconfig, estás listo para trabajar algo un poco más avanzado. Primero vamos a capturar los paquetes DNS que se generan por la actividad ordinaria navegar en la web.

1. Utilizar ipconfig para vaciar la caché DNS.
2. Abre tu navegador y vacía la caché del navegador.
3. Abre Wireshark y escribe el siguiente filtro de display “ip.addr == la IP de tu PC”(la puedes obtener con ipconfig). Este filtro elimina todos los paquetes que no se originan ni están destinados a tu PC.
4. Inicia la captura de paquetes de Wireshark.
5. Con tu navegador, visita la página Web: http://www.ietf.org
6. Detén la captura de paquetes.
7. Responde las siguientes preguntas:
8. Busca la consulta DNS y la respuesta DNS. ¿Son enviados a través de UDP o TCP?

A través de UDP.

1. ¿Cuál es el puerto del destino para el mensaje de consulta DNS? ¿Cuál es el puerto de origen de la respuesta DNS?

53 y 53.

1. ¿A qué dirección IP se envía el mensaje de consulta DNS? Utiliza ipconfig para determinar la dirección IP de tu servidor DNS local. ¿Son estas dos direcciones IP las mismas?

1.1.1.1 Son la misma.

1. Examina el mensaje de consulta DNS. ¿Qué “tipo” de consulta DNS es? ¿El mensaje de consulta contiene “respuestas”?

Es de tipo A. No hay respuestas.

1. Examina el mensaje de respuesta DNS. ¿Cuántas “respuestas” se producen? ¿Qué contiene cada una de estas respuestas?

3 respuestas. La primera respuesta contiene la traducción del alias de la dirección especificada y las 2 siguientes son 2 direcciones IP asociadas a esta.

1. Considera el siguiente paquete TCP SYN enviado por tu PC. ¿La dirección IP de destino del paquete SYN corresponde a cualquiera de las direcciones IP proporcionadas en el mensaje de respuesta DNS?

Si, se corresponde a una de las 2 que recibió.

1. Adaptado de: Wireshark Labs v7.0 J.F. Kurose, K.W. Ross. [↑](#footnote-ref-0)