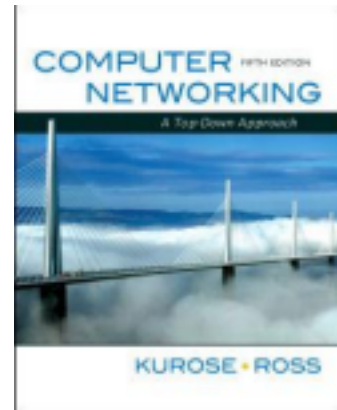


# Telemática Laboratorios

## Wireshark Lab: DNS



*Computer Networking:  
A Top-down Approach, 5º ed.*

Como se describe en la Sección 2.5 del libro de texto, el sistema de nombres de dominio (DNS) traduce nombres de nodo a direcciones IP, cumpliendo un papel importantísimo en la infraestructura de Internet. En esta práctica, vamos a ver más de cerca a la parte cliente de DNS. Recordemos que el papel del cliente en el DNS es relativamente simple - un cliente envía una consulta al servidor DNS local y recibe una respuesta. Como se muestra en las figuras 2.21 y 2.22 en el libro de texto, hay muchas cosas invisibles para los clientes DNS, ya que los servidores DNS jerárquicos se comunican entre sí de forma recursiva o iterativa para resolver las consultas DNS del cliente. Desde el punto de vista del cliente DNS, sin embargo, el protocolo es muy simple - una consulta se formula para el servidor DNS local y se recibe una respuesta de ese servidor.

Antes de comenzar con esta práctica de laboratorio, deberías revisar DNS mediante la lectura de la sección 2.5 del texto. En particular, debes revisar el material en servidores locales DNS, caché DNS, los registros DNS y los mensajes y el campo TYPE en el registro DNS.

### 1. NSLOOKUP

En esta práctica, vamos usar la herramienta nslookup, que está disponible en la mayoría de las plataformas Linux y Microsoft. Para ejecutar nslookup en Windows, abre la ventana de comandos y ejecuta **nslookup** en la línea de comandos.

La herramienta nslookup permite consultar a cualquier servidor DNS especificado sobre un registro DNS. El servidor DNS consultado puede ser un servidor DNS raíz, un servidor DNS de primer nivel de dominio, un servidor DNS autorizado, o un servidor DNS intermedio (consulta el libro de texto para las definiciones de estos términos). Para conseguirlo nslookup envía una consulta DNS al servidor DNS especificado, recibe una respuesta DNS de ese mismo servidor DNS, y visualiza el resultado.

```

C:\>
C:\>
C:\>nslookup www.mit.edu
Server: 250.Red-80-58-61.staticIP.rima-tde.net
Address: 88.58.61.250

Respuesta no autoritativa:
Nombre: www.mit.edu
Address: 18.7.22.169

C:\>nslookup -type=NS mit.edu
Server: 250.Red-80-58-61.staticIP.rima-tde.net
Address: 88.58.61.250

Respuesta no autoritativa:
mit.edu nameserver = bitoy.mit.edu
mit.edu nameserver = stroub.mit.edu
mit.edu nameserver = w20ns.mit.edu

bitoy.mit.edu internet address = 18.72.0.3

C:\>nslookup www.schub.ac.kr bitoy.mit.edu
Server: BITOY.MIT.EDU
Address: 18.72.0.3

Respuesta no autoritativa:
Nombre: www.schub.ac.kr
Address: 211.115.210.05

C:\>

```

La imagen anterior muestra los resultados de tres comandos de nslookup independientes. En este ejemplo, el equipo cliente se conecta con FTTH a la red de Telefónica, donde el servidor DNS local por defecto es 250.Red-80-58-61.staticIP.rima-tde.net.

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 el indicado anteriormente.

Analicemos el primer comando :

### ***nslookup www.mit.edu***

En palabras, este comando está diciendo "Por favor, envíenme la dirección IP para el host www.mit.edu.". Como se muestra en la captura de pantalla, la respuesta de este comando proporciona dos tipos de información:

- ( 1 ) el nombre y la dirección IP del el servidor DNS que nos da la respuesta
- ( 2 ) la respuesta en sí, que es el nombre de host y la dirección IP de www.mit.edu.

Aunque la respuesta llegó desde el servidor DNS local de Telefónica, es muy posible que este servidor DNS local contactó iterativa varios otros servidores DNS para obtener la respuesta, como se describe en la Sección 2.5 del

libro de texto.

Consideremos ahora el segundo comando:

***nslookup -type=NS mit.edu***

En este ejemplo, hemos utilizado la opción "-type = NS" y el dominio "mit.edu".

Esto hace que nslookup envíe una consulta sobre un registro de tipo NS al servidor DNS local predeterminado. En palabras, la consulta está diciendo: "Por favor, envíenme los nombres de host del DNS autorizado para mit.edu." (Cuando no se utiliza la opción -type , nslookup utiliza el valor predeterminado , que es para consultar los registros de tipo A , véase Sección 2.5.3 en el texto ).

La respuesta, que se muestra en la imagen anterior, en primer lugar indica que el servidor DNS que está proporcionando la respuesta (que es el servidor DNS local predeterminado) junto con tres servidores de nombres del MIT. Cada uno de estos servidores es de hecho un servidor DNS autorizado para los nodos del campus del MIT.

Sin embargo, nslookup también indica que la respuesta es "no autorizada", lo que significa que esta respuesta vino de la caché de algún servidor y no de un servidor DNS autoritativo 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 pidió explícitamente las direcciones IP, el servidor DNS local devuelve estos "adicionalmente" y nslookup muestra el resultado. Sin embargo no podemos prever con exactitud la información adicional que cada servidor DNS va a incluir en la respuesta)

Finalmente, vamos a analizar el tercer comando :

***nslookup www.schuh.ac.kr bitsy.mit.edu***

En este ejemplo, indicamos que queremos que la consulta sea enviada al servidor DNS bitsy.mit.edu en lugar de al servidor DNS por defecto ( 250.Red-80-58-61.staticIP.rima-tde.net ) . Por lo tanto, la operación de consulta y respuesta tiene lugar directamente entre nuestro nodo y bitsy.mit.edu. En este ejemplo, el servidor DNS bitsy.mit.edu proporciona la dirección IP de la www.schuh.ac.kr anfitrión, que es un servidor web en el Soon Chun Hyang University Hospital de Seúl ( Corea ) .

Ahora que hemos analizado un par de ejemplos ilustrativos, vamos a ver la sintaxis general de los comandos de nslookup.

La sintaxis es:

`nslookup <-option1> <-opcion2> host-to -find <dns -server>`

En general, nslookup se puede ejecutar con cero, uno, dos o más opciones. Y como hemos visto en los ejemplos anteriores, el servidor DNS es opcional y, si no se suministra, la consulta se envía al servidor DNS local predeterminado.

La lista de opciones disponibles para nslookup es:

[no] debug - información de depuración visualizada

[no] d2 – visualizar información de depuración completa

[no] recurse - pedir una respuesta recursiva a la consulta

root = NAME - definir como servidor raíz a NAME

retry = X - definir el número de reintentos como X

type = X - definir el tipo de pregunta (es decir, A, AAAA, ANY, CNAME , MX , NS , PTR , SOA , SRV )

class = X - definir la clase de pregunta (es decir , IN (Internet) , NINGUNA )

Ahora que hemos tenido una visión general de nslookup, es el momento para probar por ti mismo la funcionalidad de nslookup. Esta vez las respuestas pueden obtenerse no sólo de la captura sino también de los resultados que proporciona nslookup :

- Ejecute nslookup para obtener la dirección IP del servidor web de Telefónica.
- Ejecute nslookup para determinar los siguientes servidores DNS autorizados (Spotify , Lauro.org )
- Ejecute nslookup para determinar los servidores de correo para los buzones de outlook.es  
(<number>@outlook.es)

No necesitarás subir la captura sino anotar las respuestas proporcionadas por nslookup.

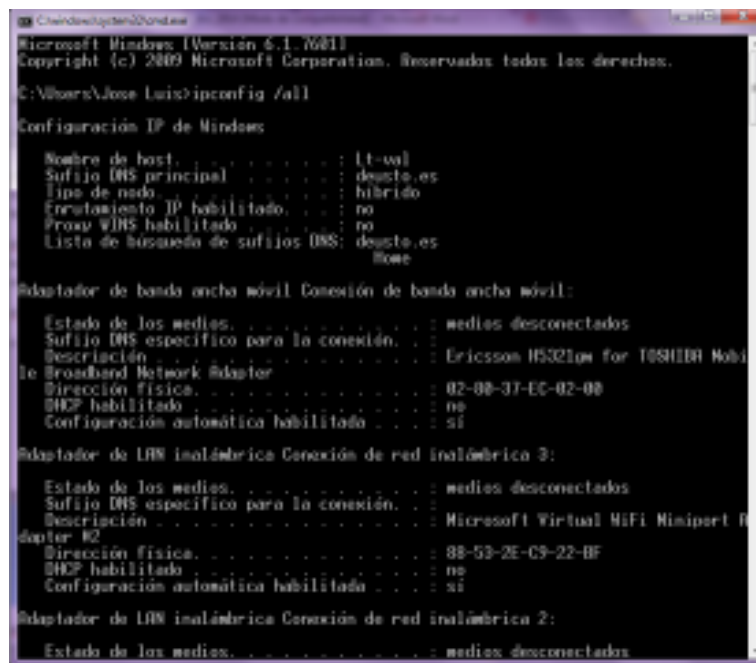
## 2. ipconfig

ipconfig (para Windows) y ifconfig (Unix) son unas de las pequeñas utilidades más útiles de los sistemas operativos sobre todo en materia de depuración de redes de comunicaciones. Sólo describiremos ipconfig, aunque el ifconfig de Linux es muy similar.

ipconfig se puede utilizar para mostrar información de configuración de TCP/IP, incluyendo la dirección IP y máscara, las direcciones de los servidores DNS, el tipo de adaptador de red, etc. Por ejemplo, si quieres ver toda esta información sobre la configuración de tu nodo, introduce:

```
ipconfig /all
```

en el símbolo del sistema , como se muestra en la siguiente captura de pantalla.



```
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Jose Luis>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : lt-wal
Sufijo DNS principal . . . . : deusta.es
Tipo de nodo . . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . : no
Lista de búsqueda de sufijos DNS: deusta.es
                                     none

Adaptador de banda ancha móvil Conexión de banda ancha móvil:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Ericsson H5321m for TOSHIBA Mob
Te Broadband Network Adapter
Dirección física. . . . . : 02-00-37-EC-02-00
DHCP habilitado . . . . . : no
Configuración automática habilitado . . . : sí

Adaptador de LAN inalámbrica Conexión de red inalámbrica 3:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Microsoft Virtual WiFi Miniport R
dapter #2
Dirección física. . . . . : 88-53-2E-C9-22-BF
DHCP habilitado . . . . . : no
Configuración automática habilitado . . . : sí

Adaptador de LAN inalámbrica Conexión de red inalámbrica 2:

Estado de los medios. . . . . : medios desconectados
```

ipconfig es también muy útil para la gestión de la información de DNS almacenada en su servidor. En la sección 2.5 se describe que un host puede almacenar en caché los registros DNS que obtuvo recientemente. Para ver estos registros en caché, después del indicador C: \> proporcionar el siguiente comando:

```
ipconfig /displaydns
```

Cada entrada muestra el tiempo restante de vida (TTL) medido en segundos. Para borrar la caché puedes introducir

```
ipconfig /flushdns
```

### 3. Análisis de DNS with Wireshark

Ahora que estamos familiarizados con nslookup e ipconfig estamos preparados para comenzar a analizar el protocolo utilizado en consultas y respuestas. En primer lugar vamos a capturar los paquetes DNS que se generan por la actividad de navegación Web ordinaria.

- Utiliza ipconfig para vaciar la caché de DNS en tu nodo.
- Abre el navegador y vacía la caché del navegador. (En Internet Explorer, ve al menú Herramientas, selecciona Opciones de Internet y, en la ficha General , seleccione Eliminar archivos. En Firefox, ve al menú Opciones, selecciona Avanzado y en el menú de red selecciona Limpiar Ahora la caché Web).
- Abre Wireshark y escribe "ip.addr==tu\_dirección\_IP" en el filtro. Con este filtro eliminas en la captura todos los paquetes que no se originan ni están destinadas a su nodo.
- Inicia la captura de paquetes en Wireshark .
- Con el navegador, visita la página Web: <http://www.ietf.org>
- Detén la captura de paquetes .

#### (CAPTURA 2)

Sobre la captura tendrás que resolver preguntas como las siguientes (a modo de ejemplo):

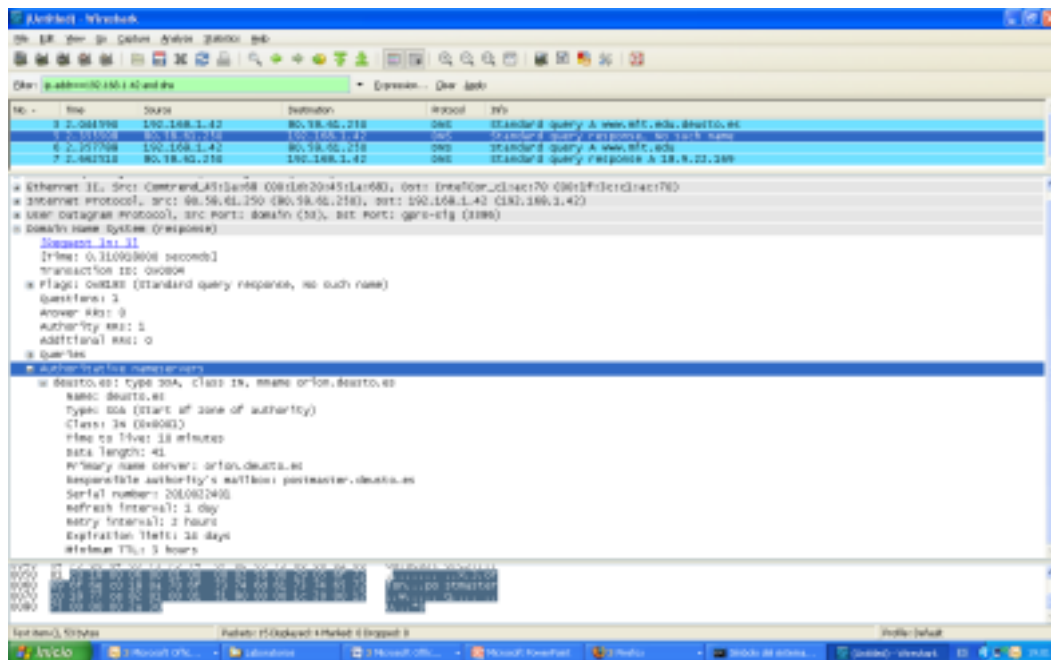
1. Busque la consulta DNS y mensajes de respuesta. ¿Se envían a través de UDP o TCP? **UDP**
2. ¿Cuál es el puerto de destino del mensaje de la consulta de DNS? ¿Cuál es el puerto de origen del mensaje de respuesta de DNS? **DNS #53 UDP**
3. ¿En qué dirección IP se envía el mensaje de consulta DNS? Utiliza ipconfig para averiguar la dirección IP de tu servidor DNS local. ¿Coinciden las dos direcciones IP? **Se mira con ipconfig: DNS 130.206.100.10**
4. Examina el mensaje de respuesta de DNS. ¿Cuántas "respuestas" se ofrecen? ¿Qué significa el contenido de cada una de estas respuestas? **una respuesta**
5. Considera el paquete TCP SYN enviado por tu nodo inmediatamente a continuación de la consulta. ¿La dirección IP de destino del paquete SYN corresponde con alguna de las direcciones IP proporcionadas en el mensaje de respuesta de DNS (podrías explicarlo)?
- 6 . Esta página web contiene imágenes. Antes de recuperar cada imagen, ¿envía el nodo nuevas consultas DNS? ¿por qué? **Porque son todas contra el mismo sentido, y como tenemos cacheado el destino, no es necesario hacer otra consulta DNS.**

Ahora vamos a jugar con nslookup .

- Iniciar de nuevo la captura de paquetes en Wireshark.
- Hacer una consulta a nslookup sobre [www.mit.edu](http://www.mit.edu)
- Detener la captura de paquetes.

### (CAPTURA 3)

Obtendrás una traza como la siguiente:



Vemos en la imagen de arriba que nslookup en realidad envió dos consultas de DNS y recibió dos respuestas DNS (lo que dependerá de la configuración de nslookup en tu nodo). Es posible que tú también hayas capturado varias preguntas, en ese caso, ignora la primera serie de consultas/respuestas y centrate en la última consulta y mensajes de respuesta (la que corresponde a la pregunta que deseabas realizar ([www.mit.edu](http://www.mit.edu))).

Intenta contestar a preguntas como la siguiente:

7. Examina el mensaje de consulta DNS. ¿Qué "Tipo" de consulta DNS es? [SOA](#)
8. Examina el mensaje de respuesta DNS. ¿Qué contenido hay en el campo respuestas y autoridades?

Ahora repite el experimento anterior, pero cambia el comando nslookup por el siguiente:

Nslookup -type=NS mit.edu

#### **(CAPTURA 4)**

Conteste las siguientes preguntas:

9. Examina el mensaje de respuesta de DNS. ¿Qué servidores de nombre proporciona el mensaje de respuesta?
10. ¿En este mensaje de respuesta se proporcionan también las direcciones IP de los servidores de nombres del MIT? [te da 2 de ellas \( son 3\) Esta se encuentra en el additional RRs](#)

Ahora repite la prueba pero con el comando:

```
nslookup www.aiit.or.kr bitsy.mit.edu
```

#### **( CAPTURA 5 )**

Intenta contestar a preguntas como las siguientes:

11. ¿A qué dirección IP se envía el mensaje de consulta DNS? ¿Es la dirección IP de tu servidor DNS local por defecto? Si no fuera así, ¿a quién corresponde la dirección IP?
12. Examina el mensaje de respuesta de DNS. ¿Cuántas " autoridades " se informan? ¿Qué significa el contenido de cada una de estas respuestas?



## 4. Vamos a seguir experimentando con nslookup

### ( CAPTURA 6 )

1. Comienza la captura con Wireshark (pon el filtro de “dns” si quieres).
2. Desde línea de comandos ejecuta los siguientes comando y chequea los resultados:

```
nslookup www.deusto.es.
```

```
nslookup -type=NS deusto.es.
```

```
nslookup -type=MX opendeusto.es.
```

```
nslookup -type=NS com.
```

```
nslookup -type=NS google.com.
```

```
nslookup www.google.com.
```

```
nslookup -type=PTR 130.206.100.2
```

```
nslookup -type=NS .
```

3. Detén la captura de paquetes.
4. Analiza e interpreta los resultados.