

Tarea N° 2

“Dime y lo olvido, enséñame y lo recuerdo, involúcrame y lo aprendo.” Proverbio Chino.

En esta tarea se experimentará con los servicios ofrecidos por DNS (capa aplicación) y UDP (capa transporte). La función y razón de ser del Sistema de Dominios de Nombres (Domain Name System, DNS) es traducir nombres de máquinas a sus IPs.

Para la experimentación con DNS usted usará el utilitario nslookup. Éste está disponible en Linux/Unix y Windows. Nslookup es un programa que permite consultar a un servidor DNS. Esta función es normalmente hecha por las aplicaciones antes de establecer conexiones a máquinas para las cuales conoce su nombre pero no su IP. La consulta hecha por nslookup puede ser dirigida a un servidor DNS raíz, DNS de nivel superior, DNS autoritario, o DNS intermedio.

NSLOOKUP

El formato general de nslookup es:

```
nslookup [-option] [name | -] [server]
```

En esta tarea usaremos el modo no interactivo de este utilitario. Ejemplos:

a) nslookup www.elo.utfsm.cl

Consulta al DNS local por la IP del servidor web del Depto. de Electrónica.

b) nslookup www.elo.utfsm.cl bitsy.mit.edu

Consulta al DNS bitsy.mit.edu por la IP del servidor web del Depto. de Electrónica.

c) nslookup -type=NS elo.utfsm.cl

Consulta al servidor local por el o los servidores DNS autoritarios para el nombre elo.utfsm.cl.

ipconfig (Windows) ifconfig (Linux/Unix)

Este utilitario entrega información sobre la configuración de las capas inferiores de red de su computador; por ejemplo, dirección IP, direcciones de servidores DNS locales, y tipo de interfaz de red. Ejemplo de uso (use ipconfig en esta tarea. Con ifconfig se puede lograr sólo algunos resultados, más comandos son precisos en Linux/Unix):

```
ipconfig /all /* para mostrar información de todas las interfaces de red */
```

```
ipconfig /displaydns /* para información almacenada en cache DNS local  
incluyendo tiempos de expiración */
```

```
ipconfig /flushdns /* para limpiar el cache */
```

1. Escriba brevemente qué es cada uno de los siguientes tipos de DNS: servidor DNS raíz, DNS de nivel superior, DNS autoritario, DNS intermedio, y servidor DNS local.
2. i) Determine el servidor DNS autoritario para www.kaist.edu. ii) Consulte a ese servidor DNS por la IP de www.google.cl. *Nota: por correo se pidió reportar resultado de ii) y luego repetir usando www.kaist.edu en lugar de www.google.cl.*
3. Para las siguientes preguntas, siga los siguientes pasos:
 - Use ipconfig para vaciar el cache del DNS de su computador.
 - Limpie el cache de su browser.
 - Usando Wireshark ingrese `ip.addr == your_IP_address` en la ventana del filtro.

- Con Wireshark capture los paquetes al bajar la página <http://www.ietf.org>

a) ¿Qué protocolo de capa transporte usa los paquetes DNS?

b) ¿A qué dirección IP van dirigidos las consultas DNS? ¿Qué dirección tiene su servidor DNS local? ¿Coinciden?

4. Repita la pregunta (3) 2, pero esta vez realizando la captura con Wireshark. Muestre el mensaje DNS de consulta y el mensaje de respuesta para los casos i) e ii).

User Datagram Protocol (UDP): Este protocolo de transporte es simple comparado con TCP (más adelante). Prácticamente replica el modelo de servicio de la capa de red (Internet Protocol, IP), agregando números de puertos para identificar a las aplicaciones de cada extremo y un mecanismo para reconocer errores en su contenido (checksum). Se pide usar Wireshark para validar experimentalmente algunas de sus características.

Cuando sea posible, al responder una pregunta incluya la versión impresa de el (los) paquete(s) de la captura que usted usó para responder. Para imprimir un paquete, use la opción File → Print, seleccione “packet only”, seleccione “Packet summary”, y seleccione la cantidad mínima de detalles del paquete que usted requiera para responder.

Ejecute Wireshark y corra alguna aplicación que use protocolo de transporte UDP. Para variar respecto a la primera parte de la tarea, si lo desea puede probar corriendo Skype y generando una llamada al número de prueba (Test call).

5. Seleccione un paquete.
- a) A partir de éste determine cuántos campos hay en el encabezado UDP. Nombre cada uno de esos campos e indique sus tamaños.
- b) ¿Qué representa el campo “Length”? Verifique su respuesta con el paquete capturado.
- c) ¿Cuál es el máximo número de bytes que pueden ser incluidos como datos de la capa superior en un paquete UDP?
- d) ¿Cuál es el número de protocolo usado en la capa IP para saber que el paquete es UDP y no TCP? (para esto usted deberá mirar el encabezado IP. Cabe notar que así como los protocolos de transporte llevan un número de puerto para denotar el socket - aplicación- destino del paquete, la capa IP también tiene un campo para indicar el protocolo de transporte al cual entregar los datos que IP transporta. Es así de simple...).
6. Examine un par de paquetes UDP que correspondan, por ejemplo, a un requerimiento y su respuesta; es decir paquetes en sentidos desde y hacia su computador. Determine la relación entre los números de puertos origen y destino de estos dos paquetes.
7. Busque por “UDP” (o “UDP checksum”) en Google e indique los campos sobre los cuales se calcula el checksum de UDP.