# 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). El objetivo del Sistema de Dominios de Nombres (Domain Name System, DNS) es traducir nombres de máquinas a sus IPs.

Para experimentar con DNS usted usará el utilitario nslookup. Éste está disponible en Linux/Unix y Windows. Nslookup es un programa que permite hacer consultas 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 intermedio, o DNS autoritativo.

Antes de realizar las actividades indicadas y obtener sus respuestas, piense sobre qué puede usted anticipar del resultado esperado.

**NSLOOKUP**

El formato general de nslookup es:

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

Nota: [ ...algo...] significa que ese "...algo.." es opcional. Una barra vertical "|" significa *poner una* de las dos opciones que acompañan la barra vertical.

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. Al omitir el campo dns-server, se entiende como consultar al DNS local.

b) nslookup www.elo.utfsm.cl mateo.elo.utfsm.cl

Consulta al DNS mateo.elo.utfsm.cl por la IP del servidor web del Depto. de Electrónica.

c) nslookup –type=NS berkeley.edu

Consulta al servidor local por el o los servidores DNS autoritativos (indicado por type=NS) para el nombre de dominio berkeley.edu.

**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. Ejemplos de usos (use ipconfig de Windows en esta tarea. Con ifconfig se puede lograr solo 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 de su máquina
incluyendo tiempos de expiración */

ipconfig /flushdns /* para limpiar el cache de la máquina donde se ejecuta */

1. Escriba brevemente qué es cada uno de los siguientes tipos de DNS: servidor DNS raíz, DNS de nivel superior, DNS autoritativo, DNS intermedio, y servidor DNS local.
2. Ejecutando nslookup en aragorn y usando el comando script para registrar sus acciones:

   i) Determine los servidores DNS autoritativos (o autoritarios) para usm.cl

ii) Para el primero de ellos consulte por la IP de ~~www.kaist.kr~~ www.kaist.edu. Muestre capturas de la ventana donde usted hace estas consultas DNS.

iii) Repita la consulta previa pero esta vez consulte al servidor ~~ns3.dnszi.com~~ ns.kaist.ac.kr.

3. Para las preguntas a continuación 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 dirigidas las consultas DNS? ¿Qué dirección tiene su servidor DNS local? ¿Coinciden?

4. Repita la pregunta 2, pero esta vez desde su computador (no aragorn) y realizando la captura con Wireshark. Muestre el mensaje DNS de consulta y el mensaje de respuesta para los casos i) e iii).

**User Datagram Protocol (UDP)**: Este protocolo de transporte es simple comparado con TCP (más adelante). UDP 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 sus datagramas (checksum). Se pide usar Wireshark para validar experimentalmente algunas de sus características.

Cuando se indique, 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, usted puede usar la aplicación Python vista en clases para pasar un línea de texto a mayúscula, o si lo desea puede probar corriendo Skype y generando una llamada al número de prueba (Test call).

5. Seleccione un paquete UDP de la captura previa:

   a) A partir de éste determine cuántos campos hay en el encabezado UDP. Nombre cada uno de esos campos e indique el tamaño en byte para cada campo del encabezado. Acompañe versión impresa del paquete.

   b) ¿Qué representa el campo “Length”? Verifique la consistencia de su contenido para el paquete capturado. Acompañe versión impresa del paquete.

   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 u otro? Acompañe versión impresa del encabezado IP donde se muestra ese número. (Para esto usted deberá mirar el encabezado IP. Cabe notar que así como los protocolos de transporte llevan un número de puerto para denotar la 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.)

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. Acompañe versión impresa de ambos paquetes.

7. Voluntaria, extra créditos: 5 puntos adicionales, éstos sirven para compensar descuentos en esta tarea. La nota de esta tarea igualmente se satura en 100%.

   Busque por “UDP” (o “UDP checksum”) en Google e identifique los campos sobre los cuales se calcula el checksum de UDP. Calcule a mano el valor del checksum y verifique su correspondencia con el de un paquete. Acompañe versión impresa de ese paquete.

8. (Voluntaria, extra crédito: 5 puntos adicionales. Ídem caso anterior, en total su grupo puede obtener 10 puntos adicionales)

   a) Envíese un correo con la imagen happyFace4.jpg adjunta a un correo. La imagen la puede obtener desde:

   http://alumnos.elo.utfsm.cl/~agustin.gonzalez/happyFace4.jpg
   Luego use la opción que su lector de correo le proporcione para acceder a la versión fuente del correo en texto ASCII de 7 bits (message source o similar según el lector de correo).

   b) Marque y copie la sección del correo donde debería estar la imagen, guarde la codificación de 7 bits de la imagen en un archivo con extensión .txt (por ejemplo, happyFace7bits.txt)

   c) En aragorn, o en algún computador con linux, use el comando base64 para convertir el texto de 7 bits en datos binarios que usted guardará en archivo newHappyFace.jpg. Con un visualizador de imágenes, verifique que usted ha recuperado su imagen original.

   Qué entregar en tarea:

   i) Indique el tamaño del archivo happyFace7bits.txt. Muestre las 5 líneas previas al inicio de la imagen incrustada en el correo y las dos líneas iniciales de la imagen (total 7 líneas, donde las dos finales son el inicio de la imagen).

   ii) Muestre la línea donde usted ejecuta el comando base64 pedido en c). Indique el tamaño del archivo newHappyFace.jpg resultante.