



Universidad de Buenos Aires  
Facultad de Ingeniería

Guía de Ejercicios  
U2 - Nivel de Aplicación  
del Modelo TCP/IP

TB067 – Redes de Comunicaciones

1. Para una sesión de comunicación entre un par de procesos, ¿qué proceso es el cliente y cuál es el servidor?
2. Luego de leer “2.1.1 Arquitecturas de las aplicaciones de red” en Computer Networking (Kurose), responder si para una aplicación de intercambio de archivos P2P, ¿está de acuerdo con la afirmación: “No existe la noción de los lados cliente y servidor de una sesión de comunicación”? ¿Por qué o por qué no?
3. ¿Qué es un “socket”?
4. Mencione una aplicación que requiera que no haya pérdida de datos y que también sea extremadamente sensible al tiempo.
5. ¿Cuáles son algunas diferencias entre TCP y UDP?
6. ¿Por qué TCP y UDP no tienen mecanismos de cifrado?
7. ¿Por qué HTTP, SMTP e IMAP se ejecutan sobre TCP en lugar de UDP?  
SMTP (protocolo simple de transferencia de correo) es un protocolo para un servidor de salida de correo, encargado de enviar los correos, distribuirlos, y entregarlos a su destino. IMAP (Protocolo de acceso a mensajes de Internet) es un protocolo para servidores de correo de entrada, se encargan de almacenar y organizar los correos, una vez recibidos.
8. ¿Cuál es la diferencia entre una conexión HTTP persistente y una conexión no persistente?
9. Describa cómo el almacenamiento en caché web puede reducir el retraso en la recepción de un objeto solicitado. ¿El almacenamiento en caché web reducirá la demora para todos los objetos solicitados por un usuario o solo para algunos de los objetos? ¿Por qué? ¿En qué casos un almacenamiento en caché web no mejora el tiempo de respuesta?
10. La siguiente cadena de caracteres ASCII ha sido capturada por Wireshark cuando el navegador enviaba un mensaje GET HTTP (es decir, este es el contenido real de un mensaje GET HTTP). Los caracteres <cr><lf> representan el retorno de carro y el salto de línea (es decir, la cadena de caracteres en cursiva <cr> del texto que sigue a este párrafo representa el carácter de retorno de carro contenido en dicho punto de la cabecera HTTP). Responda a las siguientes cuestiones, indicando en qué parte del siguiente mensaje GET HTTP se encuentra la respuesta.

```
GET /cs453/index.html HTTP/1.1<cr><lf>Host: gai
a.cs.umass.edu<cr><lf>User-Agent: Mozilla/5.0 (
Windows;U; Windows NT 5.1; en-US; rv:1.7.2) Gec
ko/20040804 Netscape/7.2 (ax) <cr><lf>Accept:ex
t/xml, application/xml, application/xhtml+xml, text
/html;q=0.9, text/plain;q=0.8,image/png,*/*;q=0.5
<cr><lf>Accept-Language: en-us,en;q=0.5<cr><lf>Accept-
```

```
Encoding: zip,deflate<cr><lf>Accept-Charset: ISO
-8859-1,utf-8;q=0.7,*;q=0.7<cr><lf>Keep-Alive: 300<cr>
<lf>Connection:keep-alive<cr><lf><cr><lf>
```

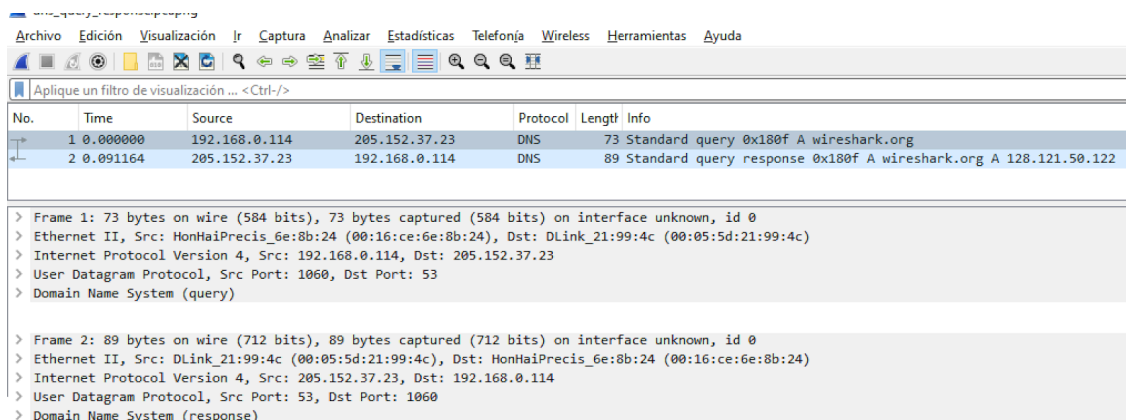
- a. ¿Cuál es el URL del documento solicitado por el navegador?
  - b. ¿Qué versión de HTTP se está ejecutando en el navegador?
  - c. ¿Qué tipo de conexión solicita el navegador, persistente o no persistente?
  - d. ¿Cuál es la dirección IP del host en el que se está ejecutando el navegador?
  - e. ¿Qué tipo de navegador inicia este mensaje? ¿Por qué es necesario indicar el tipo de navegador en un mensaje de solicitud HTTP?
11. El siguiente texto muestra la respuesta devuelta por el servidor al mensaje de solicitud GET HTTP del problema anterior. Responda a las siguientes cuestiones, indicando en qué parte del siguiente mensaje se encuentran las respuestas.

```
HTTP/1.1 200 OK<cr><lf>Date: Tue, 07 Mar 2008
12:39:45GMT<cr><lf>Server: Apache/2.0.52 (Fedora)
<cr><lf>Last-Modified: Sat, 10 Dec2005 18:27:46 GMT<cr><lf>ETag:
"526c3-f22-a88a4c80"<cr><lf>Accept-
Ranges: bytes<cr><lf>Content-Length: 3874<cr><lf>
Keep-Alive: timeout=max=100<cr><lf>Connection:
Keep-Alive<cr><lf>Content-Type: text/html; charset=
ISO-8859-1<cr><lf><cr><lf><!doctype html public "-
//w3c//dtd html 4.0transitional//en"><lf><html><lf> <head><lf>
<meta http-equiv="Content-Type"
content="text/html; charset=iso-8859-1"><lf> <meta
name="GENERATOR" content="Mozilla/4.79 [en] (Windows NT
5.0; U) Netscape]"><lf> <title>CMPSCI 453 / 591 /
NTU-ST550ASpring 2005 homepage</title><lf></head><lf>
<aquí continúa el texto del documento (no mostrado)>
```

- a. ¿Ha podido el servidor encontrar el documento? ¿En qué momento se suministró la respuesta con el documento?
  - b. ¿Cuándo fue modificado por última vez el documento?
  - c. ¿Cuántos bytes contiene el documento devuelto?
  - d. ¿Cuáles son los primeros cinco bytes del documento que se está devolviendo?
  - e. ¿Ha acordado el servidor emplear una conexión persistente?
12. Haga Telnet a un servidor web y envíe un mensaje de solicitud multilínea. Incluya en el mensaje de solicitud la línea de encabezado If-modified-since: para forzar un mensaje de respuesta con el código de estado 304 No modificado.

13. La LAN de una universidad tiene una velocidad de transmisión de 100 Mbps. Para acceder a Internet tiene un enlace de acceso cuya velocidad de transmisión es de 10 Mbps. La velocidad media de paquetes es de 20 solicitudes / seg. Si cada paquete es de 1Mbit, se pide:
- La velocidad media de los bits en bits/seg.
  - La intensidad de tráfico en la LAN.
  - La intensidad de tráfico en el enlace de acceso.
  - ¿Cómo son las intensidades de tráfico calculadas comparadas con 1? ¿Qué significa esa comparación en términos de retardos?
  - Proponga dos soluciones posibles para bajar la intensidad de tráfico en el enlace de acceso..
  - Suponga que la universidad instala una caché y que la tasa de acierto es de 0,45. ¿Qué porcentaje de solicitudes serán satisfechas casi de inmediato? ¿Qué porcentaje de solicitudes serán satisfechas por los servidores de origen?
14. Un cliente HTTP desea recuperar un documento web que se encuentra en un URL dado. Inicialmente, la dirección IP del servidor HTTP es desconocida. ¿Qué protocolos de la capa de aplicación y de la capa de transporte además de HTTP son necesarios en este escenario?
15. Mencione 3 motivos por los cuales un servidor de DNS no puede ser centralizado.
16. Dada la jerarquía de servidores DNS (Servidores DNS raíz, Servidores de dominio de nivel superior y servidores autoritativos) se pide:
- ¿Qué direcciones IP proporcionan cada uno?
  - Cuando un host realiza una consulta DNS, ¿a qué tipo de servidor de DNS, que actúa como proxy llega?
  - Llamamos R al Servidor DNS raíz, T al Servidor TLD, A al servidor autoritativo, L al servidor local y H al host que realiza la consulta. Suponíamos que el servidor TLD conoce el servidor DNS autoritativo correspondiente al nombre de host. Indique el trayecto del mensaje de consulta desde que el host lo inicia hasta que obtiene la dirección IP del host consultado mediante la letra correspondiente, un guión, la letra siguiente y así sucesivamente..
  - ¿Cuántos mensajes DNS se necesitan enviar para obtener la dirección correspondiente a un nombre de host si no se encuentra en el proxy del servidor local y servidor TLD conoce el servidor DNS autoritativo correspondiente al nombre del host consultado?
17. ¿Cuál es la diferencia entre consultas de DNS iterativas y consultas recursivas?
18. Dado que la correspondencia entre el nombre de un host y su dirección IP puede cambiar, ¿cuál es el comportamiento de un servidor de DNS respecto de la información almacenada en su caché DNS para prevenir esto?

19. Un cliente se conecta a una aplicación de home banking basada en la web mediante protocolo HTTP, el cual no tiene memoria del estado de la conexión. Una vez que inició sesión, ¿cómo identifica el servidor al cliente?
20. Supongamos que estás realizando un análisis de tráfico de red y te encuentras con la siguiente captura de dos paquetes DNS relacionados con la resolución de nombres de dominio para "wireshark.org".



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.114	205.152.37.23	DNS	73	Standard query 0x180f A wireshark.org
2	0.091164	205.152.37.23	192.168.0.114	DNS	89	Standard query response 0x180f A wireshark.org A 128.121.50.122

> Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface unknown, id 0  
 > Ethernet II, Src: HonHaiPrecis\_6e:8b:24 (00:16:ce:6e:8b:24), Dst: DLink\_21:99:4c (00:05:5d:21:99:4c)  
 > Internet Protocol Version 4, Src: 192.168.0.114, Dst: 205.152.37.23  
 > User Datagram Protocol, Src Port: 1060, Dst Port: 53  
 > Domain Name System (query)

> Frame 2: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface unknown, id 0  
 > Ethernet II, Src: DLink\_21:99:4c (00:05:5d:21:99:4c), Dst: HonHaiPrecis\_6e:8b:24 (00:16:ce:6e:8b:24)  
 > Internet Protocol Version 4, Src: 205.152.37.23, Dst: 192.168.0.114  
 > User Datagram Protocol, Src Port: 53, Dst Port: 1060  
 > Domain Name System (response)

- ¿Qué tipo de consulta DNS se envía en el primer paquete y quién la realiza?
  - ¿Cuál es la dirección IP del servidor DNS al que se envía la consulta DNS en el primer paquete?
  - ¿Qué tipo de respuesta se recibe en el segundo paquete y cuál es la dirección IP asociada al nombre de dominio "wireshark.org"?
  - ¿Cuáles son las direcciones MAC de origen y destino en ambos paquetes Ethernet?
  - ¿Puedes explicar por qué el puerto de origen y destino cambia entre la consulta DNS en el primer paquete y la respuesta DNS en el segundo paquete?
21. Descargar, analizar mediante Wireshark y contestar las preguntas sobre la transmisión de datos HTTP relacionada con la descarga de un archivo de imagen desde un servidor web a partir de la captura de paquetes de HTTP.cap del siguiente enlace:
- <https://packetlife.net/captures/category/web/>
- ¿Qué recurso se está solicitando en el primer paquete HTTP y quién realiza la solicitud?
  - ¿Cuál es el código de estado de la respuesta del servidor en el segundo paquete y qué significa este código?
  - ¿Qué tipo de archivo se está transfiriendo según la información proporcionada en la captura?

- d. ¿Cuál es el tamaño del contenido (en bytes) de la imagen que se está transfiriendo según la respuesta del servidor?
- e. ¿Cuál es la longitud de la respuesta HTTP (en bytes) en el segundo paquete?
- f. ¿Cuál es la fecha y hora en que se envió la respuesta del servidor al cliente según los datos proporcionados en la captura?
22. Enviar un mensaje de consulta DNS directamente desde el host en el que está trabajando al servidor google.com.ar mediante nslookup.
- a. ¿Qué información devuelve este comando?
- b. ¿Cuál es la dirección IP del servidor web de google.com.ar?
- c. ¿Cuál es la dirección IP del servidor DNS que proporcionó la respuesta al comando nslookup?
- d. La respuesta de este comando proporciona dos datos, ¿Que representa cada uno?
- e. Existen tres clases de servidores DNS: los servidores DNS raíz, los servidores DNS de dominio de nivel superior (TLD, Top-Level Domain) y los servidores DNS autoritativos, organizados en una jerarquía:

- Los servidores de nombres raíz proporcionan las direcciones IP de los servidores TLD.
- Los servidores TLD proporcionan las direcciones IP para los servidores DNS autoritativos.
- Los servidores autoritativos contienen las direcciones IP y sus nombres correspondientes de cada página web.

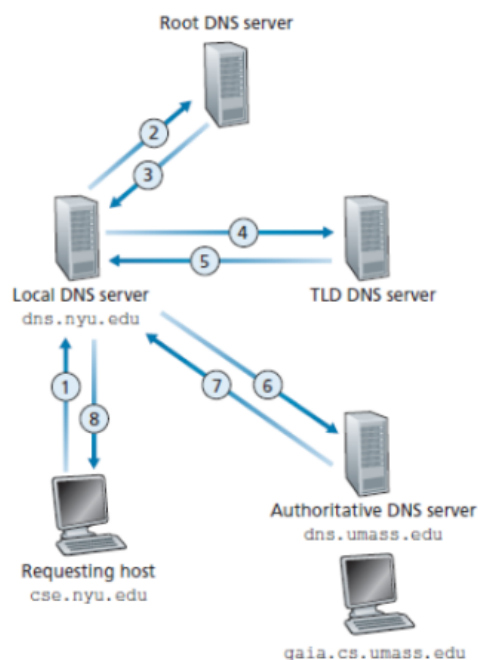


Figure 2.19 + Interaction of the various DNS servers

¿Qué servidor, según el esquema de la figura anterior, devuelve esta información?

23. Para el comando nslookup -type=NS fi.uba.ar se pide:
- a. ¿Qué información devuelve el comando?
- b. ¿La respuesta al comando nslookup provino de un servidor autorizado o no autorizado?
- c. ¿Qué significa "Respuesta no autoritativa" en la respuesta?

- d. ¿De qué tipo es el archivo de recursos que contiene la información devuelta?
- e. ¿Por qué hay dos tipos diferentes de direcciones IP?

24. ¿Qué respuesta aparece en la pantalla con el comando `nslookup 157.92.1.1`?

25. DNS usa UDP en vez de TCP. Si se pierde un paquete DNS, no hay recuperación automática. ¿Provoca esto un problema y, de ser así, cómo se resuelve?

26. Suponga que en `UDPCliente.py`, después de crear el socket, añadimos esta línea:  
`clientSocket.bind(("", 5432))`

- a. ¿Será necesario modificar el programa `UDPServidor.py`?
- b. ¿Cuáles son los números de puerto para los sockets en `UDPCliente` y `UDPServidor` luego del cambio?
- c. ¿Cuáles eran antes de realizar este cambio?

27. Análisis de captura de paquetes del protocolo DNS.

a. Mediante el comando `ipconfig /all` obtener:

Dirección IPv4 e IPv6 la placa de red o de WiFi según corresponda:

Dirección MAC:

Dirección IP de la puerta de enlace predeterminada:

Direcciones IP del servidor DNS:

b. En Wireshark, en Interface List (captura-opciones-entrada) elija la asociada a la IP y MAC registrada en a.

Guardar la captura en un archivo llamado `ejercicio30.pcap` (captura-opciones-salida)

c. Comience a capturar paquetes.

d. Ir a `www.google.com` en un navegador.

e. Al ver la página de Google detenga la captura de paquetes.

f. Filtre paquetes DNS

Si no se ve ninguno, cerrar el navegador web y enviar el comando `ipconfig /flushdns`.

Repetir los pasos desde b.

Si no se ven paquetes DNS, enviar el comando `nslookup www.google.com` en vez de usar el navegador.

g. Busque un paquete `standard query (A)` `google.com` y complete la tabla:

Número de trama:

Cantidad de bytes capturados:

Dirección MAC de origen:

Dirección MAC registrada en a):

Dirección MAC de destino:

Dirección IP de origen:

Dirección IP registrada en a):

Dirección IP de destino:

Dirección IP de la puerta de enlace predeterminada registrada en a) :

Puerto de origen:  
Puerto de destino:

h. Expanda los campos de detalle del análisis de Wireshark

Longitud del segmento UDP del datagrama de usuario:

Cantidad de bytes del encabezado de la consulta DNS:

Cantidad de bytes de datos (UDP payload) de la consulta DNS (marcarlo con el cursor y observar esos bytes):

Utilidad del checksum:

i: Busque el paquete de standard query response (A)

Número de trama:

Cantidad de bytes capturados:

Indicar si la cantidad de bytes capturados es mayor o menor que en standard query:

Indicar si la dirección MAC de origen es la del cliente o la del servidor:

Indicar si la dirección MAC de destino es la del cliente o la del servidor:

Dirección IP de origen:

Dirección IP de destino:

El origen (MAC, IP y puerto) y el destino (MAC, IP y puerto) coinciden con los de standard query o se invirtieron?:

j: ¿Por qué se usa el protocolo de transporte UDP y no TCP en consultas DNS?