Práctica 5 - Capa de Aplicación

Revisión 2.3

1. ¿Cuáles son las funciones de la capa de aplicación? Compare funcionalidades entre modelo OSI y TCP/IP.
2. ¿Qué es un User-Agent? Nombre algunos que conozca e indique qué protocolo de aplicación soportan?

DNS

3. ¿Cuál es el objetivo del protocolo DNS? ¿Cómo funciona? ¿Es posible que Internet funcione sin este servicio?
4. ¿Qué protocolo de la capa de transporte utiliza? ¿Qué puertos?
5. ¿Qué es un root-server? ¿Qué son los TLD? Diferencias entre gTLD y ccTLD? Indique 3 ejemplos de c/u. Cómo se acceden y que tipo de consultas se les hacen.
6. ¿Qué es el *resolver*? ¿Cómo se configura en Linux y en Windows? ¿Qué tipos de resolvers hay?
7. ¿Cuándo una respuesta es autoritativa?
8. Explique las diferencias entre una consulta iterativa y una recursiva
9. Indique un posible orden de los nombres de servidores consultados desde la raíz para resolver el nombre www.info.unlp.edu.ar
10. Describa la relación de los servidores primario/secundario, determine cuales son los servidores de DNS autoritativos de los dominios .com , .ar , .yahoo.com , edu.ar e indique cuál es el primario.

11. Explique para que se usan cada uno de los siguientes tipos de registros de DNS:
    - SOA
    - A
    - AAAA
    - CNAME
    - PTR
    - NS
    - MX

12. En una caché DNS, ¿qué problemas conllevaría cambiar la dirección IP de, por ejemplo, el nombre de servidor de mail? ¿Cómo podría ser minimizado?

13. Mediante algunos de los comandos de DNS (dig, nslookup o host), contestar las

siguientes preguntas:

a) ¿Cuántos servidores raíces (ROOT-Servers) hay? Indique las direcciones IP del servidor “B” y “J”.

b) ¿Cuántos servidores de correo aceptan mails en gmail.com? ¿Qué tipo de consulta es enviada para obtener la respuesta?

c) ¿Cuál es el servidor SMTP principal de gmail.com? ¿En base a qué información se puede determinar esto? ¿Utiliza IPv6 Gmail ?

d) Realice esta misma consulta contra hotmail.com. Nota alguna diferencia en las respuestas

e) ¿Cuántos servidores de nombre existen para google.com? ¿Siempre se obtiene la misma respuesta?

f) ¿Cuál es el nombre asociado a la dirección IP 163.10.0.145? ¿Qué tipo de consulta DNS es enviada para obtener la respuesta?

14. De acuerdo a lo obtenido en la siguiente salida , responder:

```
; <<>> DiG 9.8.5-P1 <<>> mx unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61675
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 0

;; QUESTION SECTION:
;unlp.edu.ar.            IN    MX

;; ANSWER SECTION:
unlp.edu.ar.            19124  IN    MX    20 anubis.unlp.edu.ar.
unlp.edu.ar.            19124  IN    MX    10 unlp.unlp.edu.ar.

;; AUTHORITY SECTION:
unlp.edu.ar.            86399  IN    NS    unlp.unlp.edu.ar.
unlp.edu.ar.            86399  IN    NS    anubis.unlp.edu.ar.
unlp.edu.ar.            86399  IN    NS    ns1.riu.edu.ar.

;; Query time: 6 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Thu Sep 19 10:45:55 ART 2013
;; MSG SIZE rcvd: 123
```

a) ¿Cuántos servidores de correo hay disponibles? ¿Cuál es el servidor primario?
b) ¿Es autoritativa la respuesta? Justifique
c) Si quisiese que la respuesta fuese autoritativa, ¿a qué servidor debería realizarle la consulta?
d) ¿ La consulta fue realizada de forma recursiva? ¿ La respuesta lo consideró ?

15. **OPCIONAL:** Responda y justifique los siguientes ejercicios.

a. En la VM, utilice el comando dig para obtener la dirección IP del host www.redes.unlp.edu.ar y responda:

I. ¿La solicitud fue recursiva? ¿Y la respuesta? ¿Cómo lo sabe?

Ii. ¿Puede indicar si se trata de una respuesta autoritativa?

iii. ¿Cuál es la dirección IP del resolver utilizado? ¿Cómo lo sabe?

b. ¿Cuáles son los servidores de correo del dominio redes.unlp.edu.ar? ¿Por qué hay más de uno y qué significan los números que aparecen entre MX y el nombre? Si se quiere enviar un correo destinado a redes.unlp.edu.ar, ¿a qué servidor se le entregará? ¿En qué situación se le entregará al otro?

c. ¿Cuáles son los servidores de DNS del dominio redes.unlp.edu.ar?

d. Repita la consulta anterior cuatro veces más. ¿Qué observa? ¿Puede explicar a qué se debe?

E. Observe la información que obtuvo al consultar por los servidores de DNS del dominio. En base a la salida, ¿es posible indicar cuál de ellos es el primario?

F. Consulte por el registro SOA del dominio y responda.

I. ¿Puede ahora determinar cuál es el servidor de DNS primario?

Ii. ¿Cuál es el número de serie, qué convención sigue y en qué casos es importante actualizarlo?

Iii. ¿Qué valor tiene el segundo campo del registro? Investigue para qué se usa y cómo se interpreta el valor.

Iv. ¿Qué valor tiene el TTL de caché negativa y qué significa?

g. Indique qué valor tiene el registro TXT para el nombre saludo.redes.unlp.edu.ar. Investigue para qué es usado este registro.

h. Utilizando dig, solicite la transferencia de zona de redes.unlp.edu.ar, analice la salida y responda.

I. ¿Qué significan los números que aparecen antes de la palabra IN? ¿Cuál es su finalidad?

Ii. ¿Cuántos registros NS observa? Compare la respuesta con los servidores de DNS del dominio redes.unlp.edu.ar que dio anteriormente. ¿Puede explicar a qué se debe la diferencia y qué significa?

I. Consulte por el registro A de www.redes.unlp.edu.ar y luego por el registro A de www.practica.redes.unlp.edu.ar. Observe los TTL de ambos. Repita la operación y compare el valor de los TTL de cada uno respecto de la respuesta anterior. ¿Puede explicar qué está ocurriendo? (Pista: observar los flags será de ayuda).

J. Consulte por el registro A de www.practica2.redes.unlp.edu.ar. ¿Obtuvo alguna respuesta? Investigue sobre los códigos de respuesta de DNS. ¿Para qué son utilizados los mensajes NXDOMAIN y NOERROR?

16. **OPCIONAL:** Observando la captura: **`dns_capture_1.pcap`**, conteste:

a) ¿En la primer consulta qué nombre de dominio se está consultando? ¿Qué tipo de registro se solicita?

b) ¿Qué tipo de consulta se realiza: recursiva o iterativa?

c) ¿Qué consulta y obtiene el cliente en la segunda interacción?

d) ¿Qué consulta y obtiene el cliente en el último diálogo, la respuesta es autoritativa? Realizar la misma consulta a su resolver local, por ejemplo usando los comandos dig, nslookup o host, desde su dispositivo y comparar los flags enviados y obtenidos.

HTTP

17. ¿Qué protocolo de la capa de transporte utiliza? ¿Qué puertos?
18. ¿Cuáles son las principales diferencias entre HTTP 1.0 y HTTP 1.1?
19. ¿Qué cambios hace HTTP 2?
20. ¿Por qué HTTP es un protocolo sin estados (stateless)?
21. Si una página web contiene un archivo base HTML y 4 imágenes. ¿Cuántas conexiones TCP son necesarias en HTTP 1.0 para obtener toda la página? ¿Y en HTTP 1.1?
22. Explique las diferencias entre los métodos GET, POST y PUT.
23. De acuerdo a lo obtenido en la figura 2, responder:

```
user1@apolo:~$ telnet www.unlp.edu.ar 80
Trying 163.10.0.145...
Connected to www.unlp.edu.ar.
Escape character is '^]'.
HEAD / HTTP1.1

HTTP/1.1 200 OK
Server: Apache
X-Powered-By: PHP/5.3.3-7+squeeze14
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
Date: Sun, 17 Nov 2013 21:21:31 GMT
X-Varnish: 738122746 738122076
Age: 28
Via: 1.1 varnish
Connection: close
X-Cache: HIT
```

a) ¿Qué método de acceso a la página se está utilizando? ¿Para qué sirve este método?¿Cuál debería usar si quiero acceder a toda la página?
b) ¿Qué versión del protocolo HTTP se utilizó en la consulta? ¿Cuál es la respuesta?
c) ¿Es correcta la respuesta del servidor? ¿Por qué?

d) ¿Cuántas cabeceras hay en la respuesta?
e) ¿Qué servidor se está ejecutando?

25. Observando la captura:h **`http_capture_1.pcap`**, responder:

En la línea 4 de la captura:

a) ¿Qué versión de HTTP se utilizó?
b) ¿A qué servidor se le envía la solicitud? ¿Qué recurso se está solicitando?
c) ¿Qué lenguaje se acepta?
d) ¿Qué charset se aceptan? ¿Cuál se prefiere? ¿Por qué?
e) ¿Para qué se utiliza el header Connection: keep-alive?
f) ¿Qué User-agent se usó?

En la línea 6 de la captura:

a) ¿Es exitosa la respuesta? ¿Por qué?
b) ¿Qué servidor envía la respuesta? ¿Qué versión del protocolo se está utilizando para la misma?
c) ¿Para qué sirve el Header ETAG?
d) ¿La conexión es persistente? ¿Por qué?

En la línea 8 de la captura:

¿Para qué se utiliza la cabecera If-Modified-Since? ¿Qué respuesta se obtiene?
¿Qué funcionalidad tiene la cabecera Pragma: no-cache? ¿Se la sigue utilizando? ¿Qué cabecera la reemplaza?
¿Qué finalidad tiene la cabecera If-None-Match?

26. **OPCIONAL:** Ejecute el comando curl sin ningún parámetro adicional y acceda a www.redes.unlp.edu.ar. Luego responda:
a. ¿Cuántos requerimientos realizó y qué recibió? Pruebe redirigiendo la salida (>) del comando curl a un archivo con extensión html y abrirlo con un navegador.
b. ¿Cómo funcionan los atributos href de los tags link e img en html?
c. Para visualizar la página completa con imágenes como en un navegador, ¿alcanza con realizar un único requerimiento?
d. ¿Cuántos requerimientos serían necesarios para obtener una página que tiene dos CSS, dos Javascript y tres imágenes? Diferencie cómo funcionaría un navegador respecto al comando curl ejecutado previamente.

27. **OPCIONAL:** Ejecute a continuación los siguientes comandos:

```
curl -v -s www.redes.unlp.edu.ar > /dev/null
curl -I -v -s www.redes.unlp.edu.ar
```

a. ¿Qué diferencias nota entre cada uno?

b. ¿Qué ocurre si en el primer comando se quita la redirección a /dev/null? ¿Por qué no es necesaria en el segundo comando?
c. ¿Cuántas cabeceras viajaron en el requerimiento? ¿Y en la respuesta?

28. **OPCIONAL:** Utilizando curl, realice un requerimiento con el método HEAD al sitio www.redes.unlp.edu.ar e indique:
a. ¿Qué información brinda la primera línea de la respuesta?
b. ¿Cuántos encabezados muestra la respuesta?
c. ¿Qué servidor web está sirviendo la página?
d. ¿El acceso a la página solicitada fue exitoso o no?
e. ¿Cuándo fue la última vez que se modificó la página?
f. Solicite la página nuevamente con curl usando GET, pero esta vez indique que quiere obtenerla sólo si la misma fue modificada en una fecha posterior a la que efectivamente fue modificada. ¿Cómo lo hace? ¿Qué resultado obtuvo? ¿Puede explicar para qué sirve?

29. **OPCIONAL:** Utilizando curl, acceda al sitio www.redes.unlp.edu.ar/restringido/index.php y siga las instrucciones y las pistas que vaya recibiendo hasta obtener la respuesta final. Será de utilidad para resolver este ejercicio poder analizar tanto el contenido de cada página como los encabezados.

30. **OPCIONAL:** Utilizando la VM, realice las siguientes pruebas:
a. Ejecute el comando 'curl www.redes.unlp.edu.ar/extras/prueba-http-1-0.txt' y copie la salida completa (incluyendo los dos saltos de línea del final).
b. Desde la consola ejecute el comando telnet www.redes.unlp.edu.ar 80 y luego pegue el contenido que tiene almacenado en el portapapeles. ¿Qué ocurre luego de hacerlo?
c. Repita el proceso anterior, pero copiando la salida del recurso /extras/prueba-http-1-1.txt. Verifique que debería poder pegar varias veces el mismo contenido sin tener que ejecutar el comando telnet nuevamente.

31. **OPCIONAL**: En base a lo obtenido en el ejercicio anterior, responda:
a. ¿Qué está haciendo al ejecutar el comando telnet?
b. ¿Qué método HTTP utilizó? ¿Qué recurso solicitó?
c. ¿Qué diferencias notó entre los dos casos? ¿Puede explicar por qué?
d. ¿Cuál de los dos casos le parece más eficiente? Piense en el ejercicio donde analizó la cantidad de requerimientos necesarios para obtener una página con estilos, javascripts e imágenes. El caso elegido, ¿puede traer asociado algún problema?

32. **OPCIONAL:** En el siguiente ejercicio veremos la diferencia entre los métodos POST y GET. Para ello,
será necesario utilizar la VM y la herramienta Wireshark. Antes de iniciar considere:

- Capture los paquetes utilizando la interfaz con IP 172.28.0.1. (Menú "Capture -> Options". Luego seleccione la interfaz correspondiente y presione Start).

- Para que el analizador de red sólo nos muestre los mensajes del protocolo http introduciremos la cadena 'http' (sin las comillas) en la ventana de especificación de filtros de visualización (display-filter). Si no hiciéramos esto veríamos todo el tráfico que es capaz de capturar nuestra placa de red. De los paquetes que son capturados, aquel que esté seleccionado será mostrado en forma detallada en la sección que está justo debajo. Como sólo estamos interesados en http ocultaremos toda la información que no es relevante para esta práctica (Información de trama, Ethernet, IP y TCP). Desplegar la información correspondiente al protocolo HTTP bajo la leyenda "Hypertext Transfer Protocol".
- Para borrar la cache del navegador, deberá ir al menú "Herramientas->Borrar historial reciente". Alternativamente puede utilizar Ctrl+F5 en el navegador para forzar la petición HTTP evitando el uso de caché del navegador.
- En caso de querer ver de forma simplificada el contenido de una comunicación http, utilice el botón derecho sobre un paquete HTTP perteneciente al flujo capturado y seleccione la opción Follow TCP Stream.

a. Abra un navegador e ingrese a la URL: www.redes.unlp.edu.ar e ingrese al link en la sección "Capa de Aplicación" llamado "Métodos HTTP". En la página mostrada se visualizan dos nuevos links llamados: Método GET y Método POST. Ambos muestran un formulario como el siguiente:

b. Analice el código HTML
c. Utilizando el analizador de paquetes Wireshark capture los paquetes enviados y recibidos al presionar el botón Enviar.
d. ¿Qué diferencias detectó en los mensajes enviados por el cliente?
e. ¿Observó alguna diferencia en el browser si se utiliza un mensaje u otro?

33. Suponga un cliente HTTP 1.0 se conecta a un servidor HTTP 1.1 y realiza las siguientes peticiones: http://www.http11.com.ar/, http://www.http11.com.ar/index.html, http://www.http11.com.ar/home.html dentro de un una ventana de tiempo de 1 minuto.

a) ¿Cuántas conexiones TCP se utilizarían si ninguna de las páginas contiene referencias a otros objetos?
b) ¿Cuántas conexiones TCP se utilizarán si home.html tiene los TAGs HTML:
<IMG SRC="dd.jpg"> y <A HREF="otro.html">
c) ¿Qué sucedería si el cliente y el servidor soportaran ambos HTTP 1.1 ?
d) Responda la misma pregunta que la anterior suponiendo que entre la primera y la segunda petición la máquina donde ejecuta el cliente se reinicia. (Justifique todas sus respuestas).

26. Usando un navegador/browser active el modo debug indique que versiones de protocolos HTTP se ven accediendo a diferentes sites. Investigue las diferencias entre estas. Acceda al site de la UNLP o de la Facultad e investigue el header Cookie como es su uso.
.
27. **OPCIONAL:** Investigue la aplicación “curl”, utilicela para acceder al site de la Facultad con diferentes métodos: HEAD, GET, POST. Ver las respuestas si se accede con HTTP o con HTTPS. Agregar opción verbose (-v) para ver los detalles de los encabezados. Luego usar para acceder al site ***httpbin.org*** con HTTP y HTTPS. Vea que opciones ofrece el site de testing.

E-MAIL (SMTP, POP, IMAP)

34. ¿Qué protocolos se utilizan para el envío y la recepción de mails? ¿Qué protocolos de la capa de transporte utilizan y qué puertos?
35. ¿Cuáles son las diferencias entre SMTP y ESMTP?
36. ¿Cuáles son las diferencias entre POP e IMAP? ¿Cuál supone que utilizan gmail o hotmail?
37. **OPCIONAL:** Intente enviar un email utilizando los comandos SMTP vía un terminal virtual de telnet a su cuenta. Averigüe primero mediante comandos la resolución de registros de DNS y luego realice la conexión usando el comando telnet ***<<server-MX>>*** 25. Repita el procedimiento cambiando los encabezados, por ejemplo “From:”.
39.. ¿Para qué sirve la extensión MIME?
40. Contestar las siguientes preguntas observando el archivo: **`mail_1.pdf`**:
    a) ¿Para qué sirve la cabecera Return-Path?
    b) ¿Desde qué dirección IP se envió el mail?
    c) ¿Qué User-Agent se usó para enviar el mensaje?
    d) ¿Qué versión de MIME se está utilizando?
    e) ¿Qué tipo de información y codificación se envía en el mail?
    f) ¿Para qué se usa el campo boundary=“=1rn50g4mnglf”?
    g) ¿Cuántos attachments (adjuntos) se enviaron?

FTP

41. ¿Por qué FTP utiliza dos puertos?
42. ¿Cuáles son las diferencias entre FTP Activo y FTP Pasivo?
43. ¿FTP cifra las sesiones? ¿Qué se podría utilizar para lograr esta funcionalidad?

Nota: La práctica es muy extensa, por esto se han marcado ejercicios como OPCIONALES los cuales ayudarán a entender mejor el tema, pero su contenido no será evaluado.