

Práctica 2 - Capa de Aplicación

1. ¿Cuál es la función de la capa de aplicación?
2. Si dos procesos deben comunicarse:
 - a. ¿Cómo podrían comunicarse si están en diferentes máquinas?
 - b. ¿Y si están en la misma máquina qué alternativas existen?
3. Explique brevemente cómo es el modelo Cliente/Servidor. De un ejemplo de un sistema Cliente/Servidor en la "vida cotidiana" y un ejemplo de un sistema informático que siga el modelo Cliente/Servidor. ¿Conoce algún otro modelo de comunicación?
4. Describa la funcionalidad de la entidad genérica "Agente de usuario" o "User agent".

DNS

Requerimientos:

- Debe usar el Live CD de Lihuen GNU/Linux provisto. Ver URL de descarga en el sitio de la cátedra en <https://catedras.info.unlp.edu.ar/>
 - La forma recomendable de usar la ISO armando una maquina virtual con VirtualBox con:
 - Placa de red en modo NAT
 - Verifique que el CD de la máquina virtual reference el archivo ISO de Lihuen LiveCD.
- 5. Investigue y describa cómo funciona el DNS. ¿Cuál es su objetivo?
- 6. ¿Qué es un root server? ¿Qué es un *generic top-level domain (gtld)*?
- 7. ¿Qué es una respuesta del tipo authoritative?
- 8. ¿Qué diferencia una consulta DNS recursiva de una iterativa?
- 9. ¿Qué es el resolver?
- 10. Describa para que se usan los siguientes tipos de registros de DNS:

a. PTR	d. MX
b. A	e. SOA
c. NS	f. CNAME

11. Utilizando el Live CD, utilice alguno de los siguientes comandos: nslookup, host o dig, para obtener:
 - a. La dirección de Internet del host www.redes.unlp.edu.ar
 - b. La dirección de Internet o el hostname del servidor de DNS del dominio redes.unlp.edu.ar
 - c. La dirección de Internet o el hostname del servidor de correo del dominio redes.unlp.edu.ar
12. **Para realizar el siguiente ejercicio va a necesitar que el LiveCD tenga Internet. También puede realizarlo desde una PC que tenga los comandos y conexión a Internet.**
 Realice consultas de DNS para averiguar, ya sea con el comando dig, host o nslookup los siguientes datos:
 - a. La cantidad de servidores de mail que aceptan correo para el dominio gmail.com: ¿____?
 - b. El nombre del servidor de correo principal de gmail.com. ¿_____?
 - c. ¿En que ocasión los demás servidores de correo recibirían correos dirigidos al dominio gmail.com? ¿que sucede luego de que uno de estos servidores recibe un correo para un usuario del dominio, gmail.com en este caso?
 - d. La cantidad de servidores de DNS del dominio unlp.edu.ar: ¿____?
 - e. La dirección de Internet del host www.info.unlp.edu.ar
13. ¿Qué función cumple en Linux/Unix el archivo /etc/hosts o en Windows el archivo \WINDOWS\system32\drivers\etc\hosts?
14. Abra el programa **Wireshark (as root)** para comenzar a capturar el tráfico de red en la interfaz de

loopback **lo**. una vez abierto realice una consulta DNS con el comando dig para averiguar el registro MX de redes.unlp.edu.ar y luego otra para averiguar los registros NS correspondientes a el dominio redes.unlp.edu.ar. Analice la información proporcionada por dig y comparelo con la captura.

15. Dada la siguiente situación: “Una PC en una red determinada, con acceso a Internet, utiliza los servicios de DNS de un servidor de la red”. Analice:
- ¿Qué tipo de consultas (iterativas o recursivas) realiza la PC a su servidor de DNS?
 - ¿Qué tipo de consultas (iterativas o recursivas) realiza el servidor de DNS para resolver requerimientos de usuario como el anterior? ¿A quién le realiza estas consultas?

HTTP

16. Defina cada una de las siguientes entidades: Navegador, Servidor WEB, Página WEB, HTTP y URL. ¿Cómo participa cada uno de ellas en la comunicación cliente WEB – servidor WEB?

17. ¿Qué son y en qué se diferencian HTML y HTTP?

18. Utilizando el Live CD, abra un navegador (Iceweasel). Utilizando el analizador de paquetes **Wireshark (as root)** capture los paquetes HTTP enviados y recibidos teniendo en cuenta:

- **Nota 1:** capture los paquetes utilizando la interfaz de loopback **lo**. (Menú “**Capture -> Options**”. Luego seleccione la interfaz **lo** y presione **Start**)
- **Nota 2:** 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 ésto veríamos todo el tráfico de red que es capaz de capturar nuestra placa de red, **lo** en este caso. 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”
- **Nota 3:** 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 cache del navegador .
- **Nota 4:** 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**.

- Borrar la cache del navegador y luego, con la captura activada, visitar la URL: www.redes.unlp.edu.ar. Luego de un instante refresque la página utilizando F5 o el icono para recargar la misma.

- ¿Cuántos requerimientos realizó el navegador? Para cada par de requerimiento/respuesta responda:
 - ✓ ¿Qué versión de http emplea tu navegador?
 - ✓ ¿Qué versión de http ejecuta el servidor?
 - ✓ ¿Qué idiomas indica tu navegador al servidor que está dispuesto aceptar en la respuesta?
 - ✓ ¿Qué recurso solicitó?
 - ✓ ¿Cuándo fue modificado por última vez el recurso solicitado?
 - ✓ ¿Qué método utilizó: (GET/POST)?
 - ✓ ¿Cuántas cabeceras viajaron en el requerimiento?
 - ✓ ¿Cuál es el código de estado devuelto a tu navegador por el servidor en la respuesta? ¿Cuál es el significado de ese código de estado?
 - ✓ ¿Cuántas cabeceras viajaron en el respuesta?
 - ✓ ¿Por qué en uno de los requerimientos está presente el encabezado “If-Modified-Since”? (Relacionar con el código de la respuesta recibida).

- ✓ ¿Es posible extraer de la respuesta recibida la página que carga el navegador? Verifique en la captura los datos recibidos y compare con el código fuente de la página cargada.
19. Utilizando el Live CD, abra un navegador (Iceweasel) e ingrese a la URL: www.redes.unlp.edu.ar/
- a. Ingrese al link en la sección “Capa de Aplicación” llamado “Protocolos HTTP”. En la página mostrada se visualizan dos nuevos links llamados: Protocolo HTTP/1.1 y Protocolo HTTP/1.0. Antes de ingresar a estos links continúe con el siguiente punto.
 - b. Utilizando el analizador de paquetes Wireshark capture los paquetes enviados y recibidos al presionar sobre el link.
 - c. Explique la diferencia entre la versión HTTP 1.0 y la versión HTTP 1.1
20. Utilizando el Live CD, abra un navegador e ingrese a la URL: www.redes.unlp.edu.ar/
- a. 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:

Formulario de registro con los siguientes campos:

- Nombre:
- Apellido:
- Email:
- Sexo: Masculino: ☒ Femenino: ☐
- Contraseña:
- Recibir confirmaciones por email: ☐
- Botón Enviar:

- 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?
21. Investigue para qué puede ser utilizado el comando curl. Con el mismo, determine la versión del servidor web que sirve el sitio <https://www.google.com/>. ¿Qué parámetros del comando utilizó?
22. Relacione DNS con HTTP. ¿Se puede navegar si no hay servicio de DNS?

SMTP, POP e IMAP

23. ¿Qué protocolos se utilizan para el envío y la recepción de mails?
24. ¿Qué protocolos se utilizan para la recepción de mails? Enumere y explique características y diferencias entre las alternativas posibles.
25. Utilizando el Live CD, abra el cliente de correo (Icedove) y configure:
- a. Una cuenta de correo POP (Omitir advertencia por uso de conexión sin cifrado)
 - ✓ Cuenta de correo: alumnopop@redes.unlp.edu.ar
 - ✓ Nombre de usuario: **alumnopop**
 - ✓ Contraseña: **alumnopoppass**
 - ✓ Servidor de correo POP: **mail.redes.unlp.edu.ar**
 - ✓ Servidor de correo saliente (SMTP): **mail.redes.unlp.edu.ar**
 - b. Una cuenta de correo IMAP (Omitir advertencia por uso de conexión sin cifrado)
 - ✓ Cuenta de correo: alumnoimap@redes.unlp.edu.ar
 - ✓ Nombre de usuario: **alumnoimap**
 - ✓ Contraseña: **alumnoimappass**

- ✓ Servidor de correo IMAP: **mail.redes.unlp.edu.ar**

Nota: Luego de autoconfigurar automáticamente una cuenta pop o imap, el envío de mails se auto configura para realizarse vía SMTP con autenticación. Para poder enviar mails es necesario sacar la opción de autenticación en los servidores de correo saliente (Editar → Configuración de cuentas → configuración del servidor saliente → editar → destildar la opción “usar nombre y contraseña”)

- c. Envíe un email desde el cliente de una cuenta a la otra y luego chequee el correo de ambas cuentas.

Enviando mails (Analizando SMTP):

- d. Reitere el proceso de envío, esta vez capturando los paquetes de protocolo SMTP utilizando Wireshark. Analice el intercambio del protocolo entre el cliente y el servidor, identificando cada comando y su correspondiente respuesta, realice un gráfico que muestre este intercambio.
- e. Desde una terminal, utilice los comandos del protocolo SMTP observados en el punto anterior, para enviar un mail al servidor en forma manual.

- **Nota 1:** para conectarse al servidor deberá utilizar el comando:

telnet mail.redes.unlp.edu.ar 25

- **Nota 2:** Verifique que haya recibido el correo en la cuenta a la que haya enviado el correo desde la consola.

- f. Repita este procedimiento utilizando una cuenta diferente de mail para el campo **From:**, luego verifique que el correo recibido por el destinatario tenga la cuenta ficticia.

Recibiendo mails (Analizando POP e IMAP):

- g. Vuelva a enviar un correo a alumnopop@redes.unlp.edu.ar utilizando el cliente de correo configurado. Comience la captura con Wireshark y chequee la cuenta de correo de alumnopop para capturar tráfico del protocolo POP. Analice el intercambio del protocolo entre el cliente y el servidor, identificando cada comando y su correspondiente respuesta, realice un gráfico que muestre este intercambio.
- h. Vuelva a enviar un mensaje a alumnopop@redes.unlp.edu.ar y sin chequear los mensajes con el cliente, Comience la captura y desde una terminal, utilice los comandos del protocolo POP observados en el punto anterior para consultar los mails del usuario alumnopop. lea el contenido del primer mail desde la consola utilizando telnet.

- **Nota:** para conectarse al servidor deberá utilizar el comando:

telnet mail.redes.unlp.edu.ar 110

- i. Cierre el telnet y comience una nueva captura. Chequee nuevamente el mail con el cliente configurado. ¿Qué diferencia encuentra entre ambas capturas?
- j. Con el rol de administrador del sistema (root), ejecute el cliente de correos. Para esto, abra una consola de comandos y ejecute: **sudo icedove**

De esta forma, ud. iniciará el cliente de correo con el perfil del superusuario (diferente del usuario con el que configuró las cuentas antes mencionadas). Recuerde que la contraseña del usuario root es lihen.

Luego configure las cuentas pop e imap de los usuarios alumnopop y alumnoimap como se describió anteriormente pero desde el cliente de correos del usuario **root**

¿Qué diferencias observa entre el servicio ofrecido por POP vs el ofrecido por IMAP?

26. Relacione DNS con SMTP. Describa el proceso completo para el envío de un correo desde pepe@yahoo.com a jose@hotmail.com.

Ayuda: Tenga en cuenta al analizar dicho proceso, como hace el servidor de correo del usuario que manda el correo electrónico, para identificar el servidor de correo al que debería enviar el correo. El proceder de las comunicaciones tiene un parecido al ejercicio en el que se describe cómo viaja una carta postal desde el origen al destino.