Capa de Aplicación Redes y comunicaciones

**Práctica 2 - Capa de Aplicación**

1. ¿Cuál es la función de la capa de aplicación?

es la comunicacion entre 2o+ procesos en distintas terminales

La capa de aplicación da soporte a las aplicaciones de red; incluye los protocolos HTTP (Web), SMTP (email) y FTP (transferencias de archivos) entre otros.

**3. Si dos procesos deben comunicarse**

**a. En diferentes máquinas:** Utilizan intercambio de mensajes a través de la red. El proceso emisor crea y envía los mensajes, y el receptor los recibe y responde si es apropiado hacerlo. Los protocolos de la capa de aplicación definirán el formato y orden en que deben enviarse esos mensajes, y las acciones a tomar en consecuencia a la llegada de un mensaje.

**b. En la misma máquina:** Utilizan las facilidades de comunicación inter-proceso que soporte el SO huésped (uso de señales, memoria compartida...).

3. Explique brevemente cómo es el modelo Cliente/Servidor. Dé 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?

En la arquitectura Cliente-Servidor un host **cliente** se comunica con otro, **servidor**, enviando solicitudes. Los clientes se comunican sólo con el servidor -no entre ellos-, y posiblemente desde *IP dinámica* -al contrario del servidor, con *IP fija*-. Es común que un host actúe como cliente y servidor de un servicio, o que haya solicitudes y envío de información en ambas direcciones; en este caso, se denomina *cliente* al host que comienza la sesión. Ejemplo: Un servidor Web -i.e. Apache- y un browser -i.e. Mozilla Firefox-.

Otros modelos de comunicación son: P2P (Peer to Peer, los clientes se comunican entre ellos directamente y posiblemente con un servidor que administra las IP de los clientes conectados) y sistemas híbridos (un servidor coordina algunas tareas y administra las IP cliente, y los clientes se comunican entre ellos tras interactuar con el servidor).

4. Describa la funcionalidad de la entidad genérica “Agente de usuario” o “User agent”.

Un **user agent** es la interfaz entre el usuario final y una aplicación de red (por ejemplo, el browser en el caso de la WEB). Implementa la parte cliente de algunos protocolos de aplicación.

***DNS***

Requerimientos:

●f0 Debe usar el Live CD de Lihuen GNU/Linux provisto

5. Investigue y describa cómo funciona el DNS. ¿Cuál es su objetivo?

Un DNS es una *base de datos distribuida* implementada en una jerarquía de servidores de nombres, y un *protocolo de nivel de aplicación* que permite a los hosts y dichos servidores comunicarse para proveer el servicio de traducción entre la dirección mnemónica y la dirección IP.

Cuando una aplicación precisa traducir una dirección mnemónica a IP, el host invocará un mensaje hacia el cliente DNS con el nombre a traducir. El cliente envía un mensaje de petición a través de la red, y luego de un retardo recibe la dirección de IP enviada por el servidor DNS.

6. ¿Qué es un root server? ¿que es un generic top-level domain (gtld)?

Los servidores DNS se organizan en forma jerárquica. Un host hace su solicitud a un **servidor local de nombres** que, si no posee la traducción, se transforma en un cliente consultando a un **servidor raíz de nombres -root server-**. Si el root server conoce al **servidor autorizado de nombres** para el dominio que se intenta resolver, envía la solicitud terminando la cadena; si lo desconoce, consulta a servidores intermedios hasta que eventualmente alguno lo conozca. En cada paso, un servidor podría tener registrado el IP del dominio consultado o mantenerlo en cache por una consulta anterior, ofreciendo una respuesta directa.

Para un nombre de dominio, se denomina *Top Level Domain* (TLD) a la etiqueta más a la derecha, desde el último punto. Un **generic top-level domain** es una clasificación de los dominios de Internet, -un subconjunto de los TLD's- que actualmente incluye sólo las terminaciones: .com, .info, .net y .org. Otras clasificaciones mantienen por ejemplo códigos por país o administrados por distintas organizaciones.

7. ¿Que es una respuesta del tipo authoritative?

Una respuesta authoritative es aquella entregada por el servidor oficial para el nombre de dominio consultado -es decir, que ningún servidor local, raíz ni intermedio respondió con información de caché-.

8. ¿Qué diferencia una consulta DNS recursiva de una iterativa?

**- Consulta DNS Recursiva:** Un host realiza una consulta a un servidor, éste se encarga de obtener la resolución de IP y devuelve la respuesta al host.

**- Consulta DNS Iterativa:** Un name server realiza una consulta a un servidor; si este no tiene la respuesta le devuelve la IP del próximo servidor. El name server original se encarga de realizar nuevas solicitudes hasta obtener la respuesta.

Típicamente, un **local name server** realiza **consultas iterativas**, y el resto recursivas -ya que tienen mayor volúmen de consultas que el local name server-.

9. ¿Qué es el resolver? Se denomina **resolver** a la parte cliente del DNS, encargada de iniciar y secuenciar las consultas. Usualmente trabajan de modo iterativo, aunque algunos sólo se conectan a un name server único y trabajan con consultas recursivas.

10.Describa cada uno de los siguientes tipos de registros de DNS:

a. PTR A NS MX SOA CNAME

Los name servers mantienen **registros de recursos** (RR) con el mapeo hostname <=> IP, en una cuádrupla (name, value, type, TTL). Las respuestas a consultas incluyen uno o varios RR de distintos tipos. El campo TTL -Time To Live- indica cuánto tiempo mantener el RR en caché. Los distintos *tipos* son:

**• A.** El campo name es un **hostname**, value su **IP**. Es el único que traduce hostname<=>IP, y representa al *nombre canónico* (cualquier otro nombre para el hosts será un alias con RR tipo CNAME). Puede haber más de un registro tipo A con igual hostname y distintas IP en el caso de *servidores replicados* para realizar un *balance de carga*: la respuestas DNS incluirán la lista de asociaciones pero el servidor irá alternando las posiciones para distribuir los accesos de los clientes.

**• PTR (Pointer Record).** Exactamente al revés que un registro tipo A, indica en name el **IP** de un host y en value su **hostname**. Permten la resolución reversa.

**• NS (Name Server Record).** El campo name es un **hostname**, value el **hostname de un name server** a quien seguir consultando. Permite continuar las consultas hasta obtener la traducción definitiva.

**• MX (Mail eXchange Record).** El campo name es un **alias para un mail server**, value incluye un valor numérico que indica la **prioridad y el hostname del mail server**. Permite que los hosts del mail server tengan una dirección mas simple a través del alias. Si un programa desea enviar un correo a un host de ese dominio, debe intentar primero con el de menor valor de prioridad -prioridad más alta- y sólo si falla intentar con el resto.

**• CNAME (Canonical Name Record).** El campo name es un **alias para un hostname**, value el **nombre canónico** o real del mismo (por ejemplo, el uso de alias permite que un sitio sea accedido como www.sitio.com y como sitio.com -alias-).

Otro tipo de registro es:

**• SOA.** Por *Start of Authority*, indica que los registros siguientes de la base de datos (los RR se almacenan en archivos secuenciales, no en bases relacionales) corresponden a información autoritativa. Indica: nombre canónico del NS, usuario responsable -dirección de email con un punto en vez del arroba-, número de versión -serial- del archivo de configuración del NS, refresh o tiempo de espera de servidores secundarios para pedir el SOA al primario, expire o tiempo en segundos que tardarán los servidores secundarios en descartar los datos si no logran contactar al primario, y el mínimo valor TTL para los registros de recursos siguientes.

11.Utilizando el Live CD, utilice alguno de los siguientes comandos: nslookup, host o dig,

para obtener:

a. La IP del host www.redes.unlp.edu.ar 127.0.0.1

b. La IP o el hostname del servidor de nombres para el dominio redes.unlp.edu.ar 127.0.0.1

c. La IP o el hostname del servidor de correo para redes.unlp.edu.ar 127.0.0.1 or ns.redes.unlo.edu.ar

12.En base a lo aprendido, especifique que comando es necesario para obtener la siguiente informacion:

a. Dirección IP de www.google.com

1. Comando: host

2. Respuesta: 74.125.65.256

b. Servidor de mail para el dominio @google.com

1. Comando:

2. Respuesta:

c. Servidor de nombres para el dominio @google.com

1. Comando:

2. Respuesta:

13.¿Qué función cumple el archivo /etc/hosts (Linux/Unix) y el

\WINDOWS\system32\drivers\etc\hosts (Windows)?

a. Pruebe editar el archivo (en cualquier Windows/Linux) agregando la línea:

Capa de Aplicación Redes y comunicaciones

127.0.0.1 www.prueba.com

b. Luego pruebe ejecutar desde una consola de línea de comandos: ping

www.prueba.com

14. Abra el programa Wireshark para comenzar a capturar tráfico, una vez abierto realice

una consulta DNS por el registro MX de redes.unlp.edu.ar y luego otra preguntando por

los registros NS correspondiente a el dominio redes.unlp.edu.ar, utilice dig. Analice la

información proporcionada por dig y comparelo con la captura.

***HTTP***

Requerimientos:

●f0 Debe usar el Live CD de Lihuen GNU/Linux provisto

15.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?

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

17. Clasifique las siguientes aplicaciones WEB según sean clientes o servidores.

a. Microsoft Internet Explorer

b. MS Internet Information

Server

c. Safari

d. Tomcat

e. FireFox

f. Epiphany

g. Iceweasel

h. Apache

i. Konqueror

j. Opera

k. Chrome

18.Explique la diferencia entre la versión HTTP 1.0 y la versión HTTP 1.1

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.

○f0 Nota 1: capture los paquetes utilizando la interfaz de loopback lo.

○f0 Nota 2: si el analizador no captura paquetes, utilice Ctrl+F5 en el navegador

para forzar la petición HTTP evitando el uso de cache del navegador .

○f0 Nota 3: ya realizada la captura, la lectura de la captura de paquetes se

simplifica utilizando botón derecho sobre un paquete HTTP perteneciente al

flujo capturado y seleccionando la opción Follow TCP Stream.

c. ¿Qué diferencias observa de ambos protocolos?

20.Utilizando el Live CD, abra un navegador en 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:

Capa de Aplicación Redes y comunicaciones

b. Analice el código HTML

c. Utilizando el analizador de paquetes Wireshark capture los paquetes enviados y

recibidos al presionar el botón Enviar.

○f0 Nota 1: capture los paquetes utilizando la interfaz de loopback lo.

○f0 Nota 2: si el analizador no captura paquetes, utilice Ctrl+F5 en el navegador

para forzar la petición HTTP evitando el uso de cache del navegador

○f0 Nota 3: ya realizada la captura, la lectura de la misma se simplifica utilizando

botón derecho sobre un paquete HTTP perteneciente al flujo capturado y

seleccionando la opción Follow TCP Stream.

d. ¿Qué diferencias detectó en los mensajes enviados por el cliente? ¿Observó alguna

diferencia en el browser si se utiliza un mensaje u otro?

21. Relacione DNS con HTTP

***SMTP, POP e IMAP***

Requerimientos:

●f0 Debe usar el Live CD de Lihuen GNU/Linux provisto

22.¿Qué protocolos se utilizan para el envío y la recepción de mails. Enumere y explique

sus características.

23.Clasifique las siguientes aplicaciones de correo:

a. Microsoft Exchange

b. Microsoft Outlook

c. Postfix

d. Thunderbird

e. Qmail

f. Eudora

g. Courier

h. Cyrus

24.Utilizando el Live CD, abra el cliente de correo (Icedove) y configure:

a. Una cuenta de correo POP

1. Cuenta de correo: alumnopop@redes.unlp.edu.ar

2. Nombre de usuario: alumnopop

3. Contraseña: alumnopoppass

4. Servidor de correo POP: mail.redes.unlp.edu.ar

5. Servidor de correo saliente (SMTP): mail.redes.unlp.edu.ar

b. Una cuenta de correo IMAP

1. Cuenta de correo: alumnoimap@redes.unlp.edu.ar

2. Nombre de usuario: alumnoimap

3. Contraseña: alumnoimappass

Capa de Aplicación Redes y comunicaciones

4. Servidor de correo IMAP: mail.redes.unlp.edu.ar

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

grafico 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: para conectarse al servidor deberá utilizar el comando: telnet

mail.redes.unlp.edu.ar 25 .

Nota2: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

cuando pregunte por la password introduzca "lihuen"

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 lihuen.

Luego configure las cuentas pop e imap como se describió anteriormente

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

Requerimientos: Debe usar el Live CD de Lihuen GNU/Linux provisto

25. Relacione DNS con SMTP. Describa el proceso completo en el envio 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, identificar la dirección del servidor de

correos al que debería enviar el correo.

26.¿Cuál es el objetivo del protocolo FTP?

Capa de Aplicación Redes y comunicaciones

27.Explique los siguientes comandos FTP: open, user, ls, cd, prompt, mget, mput,

get, put, hash, bye, lcd y por último el uso del símbolo !.

28.Utilizando el Live CD conéctese al servidor ftp utilizando el comando ftp

ftp.redes.unlp.edu.ar utilizando los siguientes datos:

○f0 Nombre de usuario: lihuen

○f0 Password: lihuen

a. Transfiera un archivo cualquiera al servidor.

b. Transfiera un archivo desde el servidor a la máquina local

Ejercicios Evaluables:

1- Utilizando la herramienta dig o nslookup simule con consultas iterativas la consulta

recursiva por el nombre de dominio WWW.XXX.YYY.ZZZ Debe poder describir la rama del

árbol de servidores de DNS dentro del esquema de servidores que tuvo que consultar

para llegar a la respuesta del tipo authoritative para ese dominio.

Nota: El dominio será proporcionado por el ayudante que tenga asignado.

Nota2: va a necesitar que la maquina que utilice tenga acceso a internet.

2- Analizar la captura de tráfico llamada evaluable2.pcap que será suministrada por la

cátedra a través del sitio https://catedras.linti.unlp.edu.ar. La misma fué generada en un

servidor de correos. El alumno deberá poder responder:

●f0 ¿Quién es el usuario que revisa su casilla de correos?

●f0 ¿A quién le escribe un correo?

●f0 ¿A qué se debe la aparición de los distintos protocolos de capa de aplicación

hallados en la misma? Es necesario que explique porque aparecen en cada caso.

El alumno deberá explicar estas cuestiones al ayudante evaluador.