Practica 3 DNS

Ejercicio 1 ✅

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

El objetivo de DNS es traducir nombres de dominio en direcciones IP y viceversa. Es una base de datos distribuida implementada en una jerárquica de servidores de nombres y una aplicación de la capa de aplicación que permite la comunicación entre el host y el servidor de nombres para proporcionar el servicio de traducción.

Ejercicio 2 ✅

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

Un root server o servidor raíz es el punto de entrada en la jerarquía DNS, delegan las consultas a los TLDs, estos últimos se pueden clasificar en 3 grandes categorías una de estas categorías son los gTLD (Generic TLD), dominios con propositos específicos como por ejemplo .com, .org, .gov, etc

Ejercicio 3 ✅

¿Qué es una respuesta del tipo autoritativa?

Es un tipo de respuesta con la cual contestan aquellos servidores los cuales poseen un dominio especifico o zona de dominios, puede delegar subdominios a otros servidores

Ejercicio 4 ✅

¿Qué diferencia una consulta DNS recursiva de una iterativa?

Una respuesta recursiva obliga a un servidor DNS para responder a una solicitud con un error o con una respuesta de éxito, mientras que la consulta iterativa es una en el que se espera que el servidor DNS responda con la mejor información local que tiene y deja que el cliente o el siguiente servidor de la cadena realice la búsqueda adicional.

Ejercicio 5 ✅

¿Qué es el resolver?

El *resolver* es un componente del sistema DNS que se encarga de procesar las consultas de nombres de dominio realizadas por las aplicaciones. Puede ser un resolver local en el sistema del cliente o un resolver recursivo en un servidor DNS.

Este componente utiliza una **memoria caché** para guardar los resultados de las consultas DNS durante un período de tiempo determinado por el **TTL (Time To Live)** de cada respuesta. Además, también puede almacenar temporalmente los errores de resolución (como dominios inexistentes) en una **caché negativa**, lo que evita consultas repetidas para dominios inválidos.

Ejercicio 6 ✅

Describa para qué se utilizan los siguientes tipos de registros de DNS: A, MX, PTR, AAAA, SRV, NS, CNAME, SOA, TXT.

A, AAAA (Address Record)	Asocian un nombre de dominio con una dirección IP (IPv4 e IPv6).
PTR (Pointer Record)	Asocia una dirección IP con un nombre de dominio (resolución inversa).
CNAME (Canonical Name Record)	Alias que redirige un nombre de dominio a otro.
HINFO	Información del hardware.
TXT	Almacena información de texto (ej. SPF para correo).
MX (Mail Exchange)	Define los servidores de correo para un dominio.
NS (Name Server)	Especifica los servidores DNS responsables de un dominio. (autoritativos)
SOA (Start of Authority)	Define parámetros de control de una zona DNS.
SRV (Service Record)	Se utiliza para especificar la ubicación (host y puerto) de servicios específicos dentro de un dominio. Es muy útil para servicios como SIP, LDAP, XMPP, etc.
AXFR	Obtener toda la informacion

Ejercicio 7 ✅

En Internet, un dominio suele tener más de un servidor DNS, ¿por qué cree que esto es así?
Un dominio tiene más de un servidor DNS para
garantizar su disponibilidad, **resistir fallos**, **responder más rápido desde cualquier parte del mundo** y **soportar gran volumen de consultas**.

El servidor primario (master) gestiona las actualizaciones y cambios, mientras que los secundarios (slaves) replican esta información para ofrecer respaldo en caso de que falle o este inactivo

Ejercicio 8 ✅

Cuando un dominio cuenta con más de un servidor, uno de ellos es el primario (o maestro) y todos los demás son secundarios (o esclavos). ¿Cuál es la razón de que sea así?

Se define un servidor primario para **centralizar la edición y administración de los datos**, mientras que los servidores secundarios permiten **disponibilidad, redundancia y balanceo de carga** distribuyendo copias sincronizadas de la zona.

Ejercicio 9 ✅

Explique brevemente en qué consiste el mecanismo de transferencia de zona y cuál es
su finalidad.

La transferencia de zona DNS permite a los servidores secundarios obtener una copia actualizada de la BD DNS desde el servidor primario
Funcionamiento:
1. Solicitud: El servidor secundario, pode transferencia al primero
2. Autorización: El primer verifico que el secundario tenga permiso
3. Transferencia: Se envían los datos de la zona
4. Actualización: El secundario actualiza la BD

Ejercicio 10 ✅

Imagine que usted es el administrador del dominio de DNS de la UNLP (unlp.edu.ar). A
su vez, cada facultad de la UNLP cuenta con un administrador que gestiona su propio
dominio (por ejemplo, en el caso de la Facultad de Informática se trata de info.unlp.edu.ar).
Suponga que se crea una nueva facultad, Facultad de Redes, cuyo dominio será

redes.unlp.edu.ar, y el administrador le indica que quiere poder manejar su propio dominio.

¿Qué debe hacer usted para que el administrador de la Facultad de Redes pueda gestionar
el dominio de forma independiente? (Pista: investigue en qué consiste la delegación de
dominios). Indicar qué registros de DNS se deberían agregar.

Como administrador del dominio unlp.edu.ar debo delegar la responsabilidad de la resolución del domino
redes.unlp.edu.ar a el mismo. Delegar significa que el servidor DNS **autoritativo** para `unlp.edu.ar` **ya no resuelve directamente** las consultas sobre `redes.unlp.edu.ar`, sino que **redirige la resolución** a los servidores DNS que controle el administrador de la Facultad de Redes.
Tenés que agregar
registros NS (Name Server) en la zona de `unlp.edu.ar` para delegar `redes.unlp.edu.ar`.
Además, opcionalmente, se pueden agregar registros **A o AAAA** si el nombre de los servidores delegados no está en un dominio público (glue records).

Ejercicio 11 ✅

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? ¿Qué significa que lo sea?

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?

a. i La solicitud y la respuesta fueron recursivas, esto lo podemos saber gracias a las flags recursion desired y recursion available

   ii. Si, la respuesta es autoritativa ya que tiene los flags de authoritative answer, significa que la respuesta es el resultado de haber consultado

directamente al responsable por el dominio

iii. La dirección del servidor DNS utilizado es 178.28.0.29. En los detalles de la consulta hay un Header llamado SERVER: que nos permite saber la ip del servidor DNS utilizado para la consulta

b. Los servidores de correo son mail.redes.unlp.edu.ar y mail2.redes.unlp.edu.ar y su valor 10 y 5 indican la prioridad cuando mas chico el numero mas prioridad tiene.
Es una buena practica establecer dos correos con distinta prioridad con el fin de mantener la alta disponibilidad, balanceo de carga, mantenimiento y la seguridad.
Se podria entregar un mail al servidor de menor prioridad en caso de que el primero falle o este inactivo / no responda.

c. Los servidores DNS del dominio redes.unlp.edu.ar son ns-sv-a.redes.unlp.edu.ar y ns-sv-b.redes.unlp.edu.ar

d. Los campos que cambian son los Cookie e id, esto sucede ya que ante cada solicitud se genera nuevos identificadores para la transaccion y el numero de cookie cambia entre consultas especialmente si el cliente o el servidor DNS estan configurados para usar diferentes mecanismos de sesion, o si es necesario establecer un nuevo estado de sesion.

e. Los dos tienen las mismas probabilidades de ser primario pero podemos saberlo con certeza al consultar por el registro SOA, pero ambos servidores deberían tener la misma información

f. i. ns-sv-b.redes.unlp.edu.ar es el primario
ii. Dado que el numero de serie es el correspondiente al primer campo, es el 2020031700 y esta formado por la siguiente convencion: año, mes, dia, y numero de version
iii. El segundo campo corresponde al timer de actualizacion o refresh interval que indica el tiempo que debe esperar un servidor secundario antes de consultar nuevamente al servidor primario.
iv. El tercer campo corresponder al tiempo por el cual se van a guardar los errores o ttl negativa, si un dominio no existe (NXDOMAIN) la ttl negativa nos dice cuanto tiempo se va a guardar este error en el servidor antes de tener que volver a consultar

g. El registro TXT dice: “HOLA”, este registro nos permite almacenar informacion legible para humanos o por aplicaciones, aunque puede

contener cualquier tipo de texto, se utiliza principalmente para fines de verificacion, autenticacion y seguridad

h. i. Los numeros anteriores a la palabra IN es el TTL , este indica la cantidad de tiempo que debe pasar para que se vuelva a hacer todo el camino DNS para obtener la respuesta del dominio, es decir es el tiempo que tiene que pasar para que caduque
ii. Se pueden observar 4 servidores DNS, los primeros 2 corresponden al dominio
redes.unlp.edu.ar mientras que ns1.practica.redes.unlp.edu.ar y ns2.practica.redes.unlp.edu.ar son los servidores DNS del dominio practica.redes.unlp.edu.ar

i. Lo que sucede es que los requerimientos a practica.redes estan siendo servidos desde la cache del servidor DNS local por lo tanto el ttl se va reduciendo en cada consulta hasta que expira
Mientras que consultar por redes.unlp como se estan consultando directamente al autoritativo del dominio el TTL es fijo

j. NXDOMAIN → El dominio solicitado no existe
NOERROR → No hubo errores en la consulta

Ejercicio 12 ✅

Investigue los comandos nslookup y host. ¿Para qué sirven? Intente con ambos comandos obtener:
● Dirección IP de
www.redes.unlp.edu.ar.
● Servidores de correo del dominio
redes.unlp.edu.ar.
● Servidores de DNS del dominio
redes.unlp.edu.ar.

host -a www.redes.unlp.edu.ar / nslookup www.redes.unlp.edu.ar → IP = 172.
host -a redes.unlp.edu.ar / nslookup -query=mx redes.unlp.edu.ar + nslookup
mail.redes.unlp.edu.ar y mail2.redes.edu.ar
ns-sv-a.redes.unlp.edu.ar
ns-sv-b.redes.unlp.edu.ar

Ejercicio 13 ✅

¿Qué función cumple en Linux/Unix el archivo /etc/hosts o en Windows el archivo
\WINDOWS\system32\drivers\etc\hosts?
El archivo /etc/hosts se utiliza para mapear nombres de host a direcciones ip (sin dns) permite una configuracion personalizada para redirigir dominios a IP's especificos; se consulta antes que los servidores DNS y tambien permite bloquear el acceso a los sitios

Ejercicio 14 ✅

Abra el programa Wireshark para comenzar a capturar el tráfico de red en la interfaz con
IP 172.28.0.1. 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 al dominio
redes.unlp.edu.ar. Analice la información proporcionada por dig
y compárelo con la captura.

Ejercicio 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:
a. ¿Qué tipo de consultas (iterativas o recursivas) realiza la PC a su servidor de DNS?
b. ¿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?

a. La PC siempre va a solicitarle recursividad al servidor DNS, Incluso si la información está en la **caché del servidor DNS**, **la naturaleza de la consulta sigue siendo recursiva**, ya que el cliente no hace ningún paso adicional. Por su parte el servidor DNS puede tener habilitada esta característica o no, es decir, se puede solicitar recursión y no recibirla por parte del DNS server.
b. El servidor DNS tiene habilitada la recursividad y no tiene la información sobre el dominio consultado en su resolver local debe salir a realizar todas

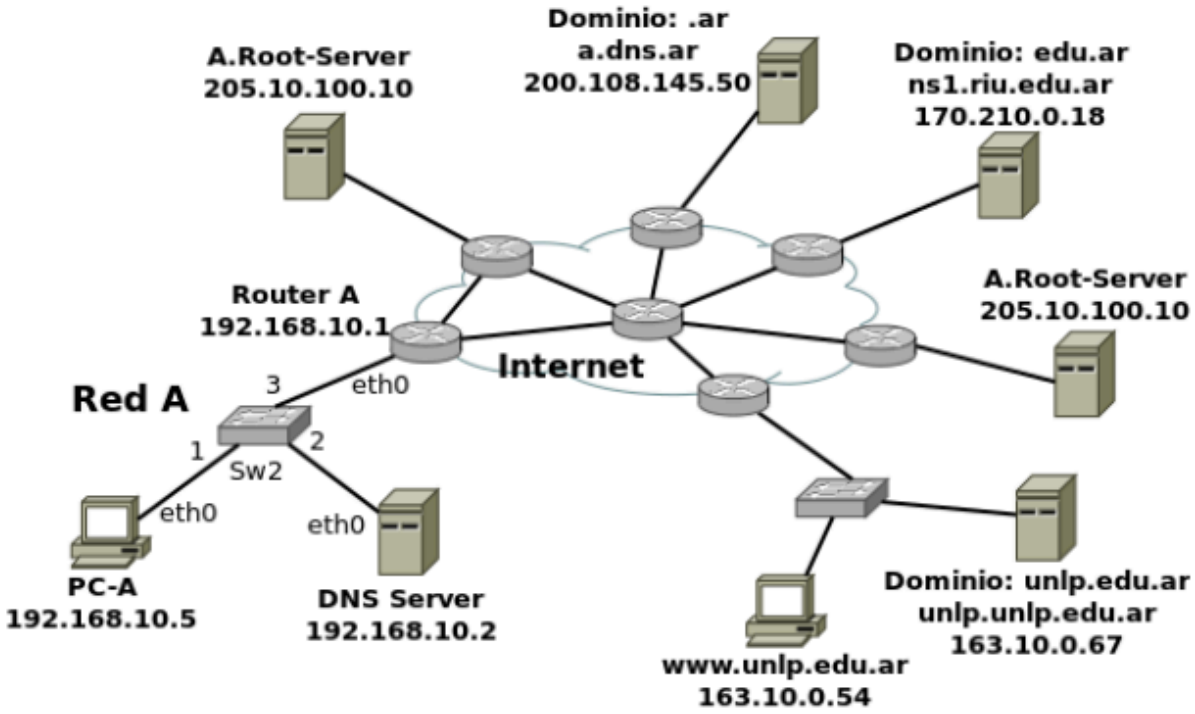
las consultas necesarias para obtener la información sobre un dominio, estas consultas son iterativas.
Una vez que da con el servidor autoritativo del dominio y construye la respuesta a la hora de devolverla al cliente se considera una respuesta recursiva.

Ejercicio 16 ✅

Relacione DNS con HTTP. ¿Se puede navegar si no hay servicio de DNS?

Si, se puede navegar pero se deberia conocer de antemano las IP donde se almacenan los sitios que debemos utilizar.

Ejercicio 17 ✅



a. Si la PC-A, que usa como servidor de DNS a "DNS Server", desea obtener la IP de www.unlp.edu.ar, cuáles serían, y en qué orden, los pasos que se ejecutarán para obtener la respuesta.

b. ¿Dónde es recursiva la consulta? ¿Y dónde iterativa?
a.

1 La PC necesita resolver el nombre de dominio www.unlp.edu.ar y envia el requerimiento al DNS Server
2 Si el DNS Server no posee la información sobre el dominio en su cache debe

consultar a los Root Si la informacion se encuentra en su cache este la devuelve al PC

3 El DNS Server consulta a algun root server sobre el dominio www.unlp.edu.ar, este le contesta con la información del servidor TLD .ar
4 El DNS Server consulta al TLD .ar por www.unlp.edu.ar y este le contesta con la dirección del servidor autoritativo para .edu.ar

5 El DNS Server consulta al TLD .edu.ar por www.unlp.edu.ar y este le contesta con la dirección del servidor autoritativo unlp.edu.ar
6 El servidor DNS consulta al **servidor autoritativo** para el dominio `unlp.edu.ar`, que es responsable de responder por todos los subdominios de `unlp.edu.ar` (incluido `www.unlp.edu.ar`). Este servidor autoritativo le responde con la dirección IP de `www.unlp.edu.ar`.

7 El DNS ya tiene la información sobre el dominio www.unlp.edu.ar, guarda el resultado en su cache y retorna recursivamente (si tiene habilitada esta funcion) con el PC.

b. La consulta es recursiva durante la comunicacion de solucion de un dominio de la PC al DNS Server y vice versa, cuando el DNS Server tiene la informacion y se la da al PC, despues el proceso de obtener la direccion ip del dominio y las consultas con los TLD o root servers se realizan de manera iterativa.

Ejercicio 18 ✅

¿A quién debería consultar para que la respuesta sobre www.google.com sea autoritativa?

Se debería consultar por el servidor DNS autoritativo de google mediante el mensaje NS
Para obtener una respuesta **autoritativa** sobre `www.google.com`, se debe consultar al **servidor DNS autoritativo del dominio** `google.com`, que se puede identificar consultando por el **registro NS** (Name Server) de `google.com`.

Ejercicio 19 ✅

¿Qué sucede si al servidor elegido en el paso anterior se lo consulta por www.info.unlp.edu.ar? ¿Y si la consulta es al servidor 8.8.8.8?

Si se consulta al **servidor DNS autoritativo de** `google.com` por el nombre `www.info.unlp.edu.ar`, **este no podrá resolver la consulta**, ya que **no es autoritativo para ese dominio**, ni está obligado a reenviar la consulta. Lo más probable es

que responda con un **error del tipo NXDOMAIN** (nombre no existente) o con una **respuesta vacía y no autoritativa**.

En cambio, si se consulta al servidor público **8.8.8.8** (Google Public DNS), **sí podría resolver** `www.info.unlp.edu.ar`, porque:

- Podría tener la respuesta en **su caché**.
- Si no la tiene, realizará **recursivamente** todas las consultas necesarias (a los root servers, TLDs, y servidores autoritativos intermedios) hasta obtener una **respuesta válida**.

Ejercicio 20

a. MX

   MX

   MX

   NS

   NS

   NS

   NS

   A

   AAAA

   A

   AAAA

b. No, para recibir una respuesta autoritativa deberiamos preguntarle a los servidores
   ss00.ejemplo.com, ss01.ejemplo.com, ss02.ejemplo.com, ss03.ejemplo.com

c. Si, las consultas y las respuesta fueron recursivas

d. Representan la prioridad de los servidores de mail, siendo el srv00.ejemplo.com el servidor con mas prioridad

Practica 2 HTTP