Práctica 3

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

   Existen dos formas de identificar a un host

   - Nombre de host ⇒ elegidas por las personas porque es más fácil de recordar, como *www.yahoo.com*
   - Direcciones IP ⇒ elegidas por los routers porque son de longitud fija y estructuradas jerárquicamente.

   El **DNS (Domain Name Service, sistemas de nombres de dominio),** es un protocolo de la capa de aplicación como HTTP, FTP, SMP, donde además es

   - Una BD distribuida implementada en una jerarquía de servidores de nombres
   - Una aplicación e la capa de aplicación que permite que se comuniquen los Host y los servidores de nombres para dar el servicio de traducción

   El objetivo del DNS es que debido a las diferentes formas de identificar un host, se encarga de traducir los nombres de Host a direcciones IP

   Mecanismo del DNS

   Es usado por otros protocolos de la capa de aplicación para traducir los nombres del host proporcionados por los usuarios a direcciones IP

   - Un navegador (cliente HTTP) que se ejecuta en algún host de usuario pide el url www.escuela.edu/index.html
   - Para que el host del usuario pueda enviar un mensaje HTTP de petición al servidor web www.escuela.edu, se debe obtener la dirección IP del servidor web
   - Para obtener la dirección IP, la máquina del usuario ejecuta el lado cliente del DNS
     - El navegador extrae el nombre de host “www.escuela.edu” de la url y lo pasa al lado cliente del DNS
   - El cliente DNS envía una consulta a un servidor DNS con el nombre del host

    - De esto se trata el mensaje DNS de petición
- El cliente recibe luego una rta con la dirección IP para el nombre de host enviado
    - Puede haber un retardo pero puede ser mínimo porque las direcciones IP suelen estar almacenadas en un servidor de nombres DNS cercano
- El navegador abre una conexión TCP con el proceso HTTP servidor localizado en la dirección IP localizada

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

   Los root servers son los encargados de proporcionar las direcciones IP de losTop Level Domains (la parte más alta de la jerarquía luego de la raíz) gTLD son una categoría TLD en DNS. Son dominios con propósitos particulares, de acuerdo a diferentes actividades politicas definidas por el ICANN (Unsponsored TLD) o definidas por otra organización (Sponsored TLD).
   Son los dominios que básicamente se utilizan para identificar categorías amplias y distintos tipos de sitios web. Algunos ejemplos de gTLDs incluyen .com, .org, .net y .info.

3. ¿Qué es una respuesta del tipo autoritativa?

   Una respuesta autoritativa es aquella dada por el servidor que tiene la autoridad sobre el nombre que se está consultando. Este responde directamente desde su base de datos de nombres, sin subdelegaciones ni cacheo de direcciones. Caso contrario, si se realiza esto último, se trata de una
   Respuesta NO Autoritativa

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

   (LIBRO)

   Una consulta DNS recursiva es cuando un Host o un servidor de nombres A hace una consulta a un servidor de nombres B y este último obtiene la correspondencia pedida en representación de A y luego reenvía la correspondencia a A. Una consulta iterativa es aquella cuando un servidor

de nombres A hace una consulta a B si el servidor B no dispone de la correspondencia, le envía a A una rta DNS con la dirección IP del siguiente servidor de nombres en la cadena, por ejemplo el servidor C; luego A envía una consulta directa a C

(CHAT GPT)

Consulta DNS Recursiva

- **Definición**: En una consulta DNS recursiva, el servidor de nombres que recibe la consulta (el servidor recursivo) actúa en nombre del cliente para resolver la consulta DNS. Esto significa que el servidor recursivo se encarga de hacer todas las consultas necesarias para obtener la respuesta final y luego devuelve esa respuesta al cliente original.
- **Proceso**:
    1. El cliente envía una consulta DNS a un servidor recursivo.
    2. Si el servidor recursivo no tiene la respuesta en su caché, hace consultas a otros servidores DNS (pueden ser servidores raíz, servidores de dominio superior, etc.) en nombre del cliente.
    3. Una vez que el servidor recursivo obtiene la respuesta, la envía de vuelta al cliente.
- **Ventaja**: El cliente no necesita realizar consultas adicionales; el servidor recursivo maneja todo el proceso.

Consulta DNS Iterativa

- **Definición**: En una consulta DNS iterativa, el servidor DNS que recibe la consulta (el servidor iterativo) proporciona al cliente la mejor información que tiene en ese momento, normalmente una referencia a otro servidor DNS que pueda tener la información requerida.
- **Proceso**:
    1. El cliente envía una consulta a un servidor DNS.
    2. Si el servidor DNS no tiene la respuesta, en lugar de buscar la respuesta completa, le proporciona al cliente la dirección IP de otro servidor DNS que probablemente tenga la respuesta.
    3. El cliente debe entonces enviar una nueva consulta al servidor recomendado y repetir el proceso hasta obtener la respuesta final.

- **Ventaja**: El servidor DNS no necesita realizar búsquedas adicionales en nombre del cliente; simplemente dirige al cliente al siguiente paso en el proceso de resolución.

Ejemplo

- **Recursiva**: Un cliente solicita la dirección IP de "example.com". El servidor recursivo hace todo el trabajo de resolver el nombre, haciendo consultas a otros servidores DNS si es necesario, y devuelve la dirección IP final al cliente.
- **Iterativa**: Un cliente solicita la dirección IP de "example.com". El servidor DNS responde con la dirección IP de un servidor de nombres de nivel superior, como un servidor de dominio de segundo nivel, y el cliente debe hacer la siguiente consulta a ese servidor.

En resumen, en una consulta recursiva el servidor maneja la resolución completa en nombre del cliente, mientras que en una consulta iterativa el servidor proporciona información que ayuda al cliente a continuar el proceso de resolución por sí mismo.

5. ¿Qué es el resolver?

   El resolver se encarga de realizar las consultas al servidor DNS, interpretar dichas consultar y devolverlas al programa que generó la consulta. Suele hacer sólo consultas recursivas.

6. Describa para qué se utilizan los siguientes tipos de registros de DNS:

   Los registros de DNS son para almacenar las correspondencias nombre de host/direccion IP. Cada mensaje de RTA DNS transporta 1 o + registros de recursos

   Registro de recurso ⇒ 4tupla (nombre, tipo, valor, ttl)

   TTL⇒ tiempo de vida del RR, determina el momento en el que debe borrarse de la caché

   Nombre y valor ⇒ dependen del Tipo

   a. A

      nombre⇒ nombre del host

      valor ⇒ dirección IP del host

Proporciona la correspondencia estándaar de nombres de host a direcciones IP

Ejemplo ⇛ (relay.bar.foo.com, 145.37.93.126, A)

b. MX

valor⇛ nombre canónico de un servidor de correo con el alias Nombre

Permiten que los nombres de servidores de correo tengan alias sencillos. Al usarlos, una compañia puede tener el mismo nombre de alias para su servidor de correo y para otro de sus servidores

- Para obtener el nombre canónico del servidor de correo, el cliente DNS consulta el MX, si quiere el de otro servidor, le consulta al CNAME

Ejemplo ⇛ (foo.com.mail.bar.foo.com, MX)

c. PTR

1. PTR (Pointer Record)

- **Uso**: El registro PTR se utiliza para realizar una búsqueda inversa de DNS, es decir, para resolver una dirección IP en un nombre de dominio.
- **Ejemplo de Uso**: Si tienes una dirección IP y quieres saber qué nombre de dominio está asociado a esa IP, se realiza una consulta PTR. Esto es comúnmente utilizado en la resolución inversa para verificar que la dirección IP asociada a un nombre de dominio es correcta.
- **Formato**: En la búsqueda inversa, el PTR record está asociado a un dominio en la zona de búsqueda inversa. Por ejemplo, una búsqueda inversa de la IP `192.0.2.1` puede devolver el nombre de dominio `example.com`.

  En el archivo de zona, esto podría verse así:

  ```
  1.2.0.192.in-addr.arpa. IN PTR example.com.
  ```

d. AAAA

- **Uso**: El registro AAAA se usa para mapear un nombre de dominio a una dirección IP de versión 6 (IPv6).
- **Ejemplo de Uso**: Si quieres que un nombre de dominio como `example.com` apunte a una dirección IPv6 específica, usarás un registro AAAA. Esto es esencial para las redes modernas que están adoptando IPv6.
- **Formato**: Un registro AAAA contiene una dirección IPv6 en formato hexadecimal. Por ejemplo, si `example.com` tiene una dirección IPv6 `2001:db8::1`, el registro AAAA sería:

```
example.com. IN AAAA 2001:db8::1
```

e. SRV

- **Uso**: El registro SRV se utiliza para especificar la ubicación de servicios específicos en una red. Esto incluye la dirección del servidor y el puerto en el que un servicio particular está disponible.
- **Ejemplo de Uso**: Se usa comúnmente para servicios como SIP (Session Initiation Protocol), LDAP (Lightweight Directory Access Protocol), y otros servicios que requieren un descubrimiento dinámico de servicios. Por ejemplo, si deseas que un cliente de chat encuentre el servidor de un servicio de mensajería, un registro SRV puede proporcionar la dirección y el puerto del servidor.
- **Formato**: Un registro SRV incluye el nombre del servicio, el protocolo, el peso, la prioridad, el puerto y el objetivo (la dirección del servidor). Un ejemplo de registro SRV podría ser:

```
_sip._tcp.example.com. IN SRV 10 5 5060 sipserver.
example.com.
```

  - `_sip._tcp` es el nombre del servicio y el protocolo (SIP sobre TCP).
  - `10` es la prioridad.

- `5` es el peso.
- `5060` es el puerto en el que el servicio está escuchando.
- `sipserver.example.com` es el objetivo, el nombre del servidor que proporciona el servicio.

f. NS

Nombre ⇒ dominio

Valor ⇒ nombre de Host de un servidor autorizado que sabe cómo obtener las direcciones IP de host en el dominio

g. CNAME

- **Uso**: El registro CNAME se utiliza para alias o nombres alternativos de un dominio. Permite que un nombre de dominio sea un alias de otro nombre de dominio, que es el nombre canónico. Los registros CNAME se usan para redirigir solicitudes de un nombre de dominio a otro, facilitando la gestión de nombres de dominio y proporcionando flexibilidad en la configuración.
- **Ejemplo de Uso**: Si tienes un nombre de dominio `www.example.com` y deseas que apunte a `example.com`, puedes usar un registro CNAME para redirigir `www.example.com` a `example.com`. Así, cualquier consulta para `www.example.com` será resuelta como si fuera `example.com`.
- **Formato**: En el archivo de zona, un registro CNAME se vería así:

  ```
  www.example.com. IN CNAME example.com.
  ```

  Esto indica que `www.example.com` es un alias de `example.com`, y cualquier solicitud para `www.example.com` se resolverá con la misma dirección que `example.com`.

h. SOA

Parte de la configuración

- **Uso**: El registro SOA proporciona información sobre la zona DNS, incluyendo el servidor de nombres principal, el correo electrónico del administrador, y varios parámetros importantes relacionados con la gestión de la zona, como los tiempos de actualización y la duración del caché.
- **Ejemplo de Uso**: El registro SOA es fundamental para la configuración de zonas en un servidor DNS. Incluye datos clave como la dirección de correo del administrador (donde el punto se sustituye por un @), el número de serie de la zona, y los tiempos de actualización.
- **Formato**: En el archivo de zona, un registro SOA se vería así:

```
@ IN SOA ns1.example.com. admin.example.com. (
     2024091501 ; Serial
     3600       ; Refresh (1 hour)
     1800       ; Retry (30 minutes)
     1209600    ; Expire (2 weeks)
     86400      ; Minimum TTL (1 day)
)
```

  - `ns1.example.com.`: El servidor de nombres principal para la zona.
  - `admin.example.com.`: El correo electrónico del administrador (donde `.` reemplaza el `@`).
  - `2024091501`: Número de serie de la zona, que debe incrementarse con cada cambio.
  - `3600`: Tiempo de refresco (en segundos) que indica con qué frecuencia los servidores secundarios deben actualizar la zona.
  - `1800`: Tiempo de reintento si un servidor secundario no puede actualizar la zona.
  - `1209600`: Tiempo de expiración, el tiempo que un servidor secundario puede usar los datos antes de considerar que la zona está desactualizada.
  - `86400`: Tiempo mínimo de vida (TTL) para los registros en la zona.

i. TXT

- **Uso**: El registro TXT permite almacenar información de texto arbitrario en un dominio. Estos registros se usan comúnmente para almacenar información de verificación y para propósitos como autenticación de correo electrónico (SPF, DKIM) y otros metadatos.
- **Ejemplo de Uso**: Los registros TXT son a menudo utilizados para especificar políticas de SPF (Sender Policy Framework), que ayudan a prevenir el envío de correos electrónicos fraudulentos desde dominios no autorizados. También se usan para la verificación de dominios en servicios web y para almacenar claves públicas para DKIM (DomainKeys Identified Mail).
- **Formato**: En el archivo de zona, un registro TXT se vería así:

```
example.com. IN TXT "v=spf1 include:_spf.example.com
~all"
```

Este ejemplo especifica un registro SPF para `example.com`, que indica qué servidores están autorizados para enviar correos electrónicos en nombre de este dominio. Otro ejemplo podría ser un registro TXT usado para verificación de dominios:

```
arduino
Copiar código
_acme-challenge.example.com. IN TXT "some_verificatio
n_token"
```

7. En Internet, un dominio suele tener más de un servidor DNS, ¿por qué cree que esto es
así?

   Para que se puede acceder lo más rápido posible (geográficamente hablando):
   mejora la velocidad de resolución al servir a usuarios más cercanos; para

que haya redundancia y disponibilidad: en caso de que un servidor falle se tiene otro como “backup”; para que haya distribución de carga: en caso de que sea un servidor muy consultado, se evita la sobrecarga en un solo servidor.

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?

   La razón de que un dominio tenga un servidor primario (o maestro) y uno o más servidores secundarios (o esclavos) se basa en la necesidad de garantizar la disponibilidad, la redundancia y la fiabilidad de los servicios DNS. A continuación, te explico cada uno de estos aspectos:

   ## 1. Disponibilidad y Redundancia

   - **Objetivo**: Asegurar que el servicio DNS esté siempre disponible, incluso si uno de los servidores falla o está inactivo.
   - **Cómo lo Logra**: Tener múltiples servidores DNS para un dominio (uno primario y varios secundarios) garantiza que si el servidor primario no está disponible debido a un problema técnico o mantenimiento, los servidores secundarios aún pueden resolver consultas DNS para ese dominio. Esto proporciona un mecanismo de respaldo y asegura que los usuarios puedan seguir accediendo a los servicios asociados con el dominio.

   ## 2. Carga Distribuida

   - **Objetivo**: Distribuir la carga de trabajo de las consultas DNS entre varios servidores para mejorar el rendimiento y reducir la sobrecarga en un solo servidor.
   - **Cómo lo Logra**: Los servidores secundarios ayudan a distribuir las consultas DNS entrantes. Los clientes DNS pueden consultar cualquier servidor DNS autoritativo para el dominio, ya sea el primario o los secundarios. Esto equilibra la carga y puede mejorar el tiempo de respuesta al permitir que las consultas se manejen por el servidor menos ocupado.

3. Actualización y Sincronización

- **Objetivo**: Mantener una base de datos DNS actualizada y consistente en todos los servidores autoritativos.
- **Cómo lo Logra**: El servidor primario es el único servidor que puede hacer cambios directos en la base de datos DNS (la zona). Los servidores secundarios obtienen estos datos del primario mediante un proceso de transferencia de zona (AXFR o IXFR). El servidor primario es responsable de propagar actualizaciones a los servidores secundarios para mantener la consistencia de los datos. Los servidores secundarios pueden ser configurados para solicitar actualizaciones periódicas al primario para asegurar que siempre tengan la versión más reciente de la base de datos DNS.

4. Gestión Centralizada

- **Objetivo**: Facilitar la gestión y configuración de los registros DNS.
- **Cómo lo Logra**: Con un servidor primario encargado de las actualizaciones, la administración de la zona DNS es centralizada. Los cambios y actualizaciones se realizan en el servidor primario y luego se distribuyen a los servidores secundarios, simplificando la administración y reduciendo la posibilidad de errores.

Proceso General:

1. **Servidor Primario (Maestro)**:
    - Es el servidor DNS donde se realizan las modificaciones y actualizaciones en los registros de zona.
    - Publica la información de la zona DNS y proporciona una copia de esa información a los servidores secundarios.
2. **Servidores Secundarios (Esclavos)**:
    - Reciben una copia de la zona DNS desde el servidor primario a través de una transferencia de zona.
    - Mantienen una copia actualizada de la zona y responden a las consultas DNS como servidores autoritativos para el dominio.
    - Se actualizan regularmente desde el servidor primario para garantizar que la información sea precisa y esté al día.

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

   La transferencia de zona es la copia de la base de datos de nombres de un servidor primario a uno secundario. Esto permite mantener la consistencia entre los servidores de una zona de dominio.

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.

Pasos para delegar el dominio redes.unlp.edu.ar:

1. **Asignar Servidores DNS para redes.unlp.edu.ar**:

   El administrador de la Facultad de Redes deberá contar con al menos dos servidores DNS (por redundancia) que gestionarán el subdominio `redes.unlp.edu.ar`.

   Estos servidores DNS son los que se encargarán de resolver las consultas relacionadas con el dominio `redes.unlp.edu.ar`.

2. **Crear los registros NS (Name Server) en el DNS de unlp.edu.ar**:

En la zona de DNS de `unlp.edu.ar`, debes agregar los registros de delegación que indiquen que las consultas para el subdominio `redes.unlp.edu.ar` serán resueltas por los servidores DNS gestionados por la Facultad de Redes. Esto se hace mediante la creación de registros **NS (Name Server)** que apunten a los servidores DNS de la Facultad de Redes.

Ejemplo de los registros NS a agregar en la zona de `unlp.edu.ar`:

```
redes.unlp.edu.ar.   IN  NS  ns1.redes.unlp.edu.ar.
redes.unlp.edu.ar.   IN  NS  ns2.redes.unlp.edu.ar.
```

3. **Crear los registros A o glue records si es necesario**:

   Si los servidores DNS de la Facultad de Redes están dentro del mismo dominio (es decir, `ns1.redes.unlp.edu.ar` y `ns2.redes.unlp.edu.ar`), debes proporcionar sus direcciones IP con registros **A** (o **glue records**), ya que al estar dentro del dominio que están gestionando, se debe evitar un bucle en la resolución.

   Ejemplo de los registros A (glue records):

   ```
   ns1.redes.unlp.edu.ar.  IN  A   192.168.1.1
   ns2.redes.unlp.edu.ar.  IN  A   192.168.1.2
   ```

4. **Configuración de los servidores DNS delegados**:

   Finalmente, el administrador de la Facultad de Redes deberá configurar sus servidores DNS (ns1.redes.unlp.edu.ar y ns2.redes.unlp.edu.ar) para gestionar las entradas DNS dentro del subdominio `redes.unlp.edu.ar`. Estos servidores deberán responder a consultas sobre los registros de ese subdominio (como registros A, MX, etc.).

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:

```
redes@debian:~$ dig www.redes.unlp.edu.ar

; <<>> DiG 9.16.27-Debian <<>> www.redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15789
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 2994578d6f7f5c590100000066e831b794c897458d1ae32f (good)
;; QUESTION SECTION:
;www.redes.unlp.edu.ar.         IN      A

;; ANSWER SECTION:
www.redes.unlp.edu.ar.  300     IN      A       172.28.0.50

;; Query time: 0 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Mon Sep 16 10:25:11 -03 2024
;; MSG SIZE  rcvd: 94
```

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

SOLICITUD RECURSIVA⇒ lo es porque están presentes las flags:

- rd ⇒ indica que la consultaa solicitó recursión
- ra ⇒ indica que el servidor DNS respondió indicando qu epuede manejar consultas recursivas

RESPUESTA RECURSIVA⇒ lo es porque está

- flag ra ⇒ significa que el servidor efectuó la resolución recursiva darme la rta
- respuesta con datos completos, obtengo el resultado final en ANSWER SECTION

ii. ¿Puede indicar si se trata de una respuesta autoritativa? ¿Qué significa que lo sea?

RESPUESTA AUTORITATIVA ⇒ lo es porque está presente la flag aa

Que sea autoritativa significa que provino directamente del servidor que tiene autoridad sobre el dominio consultado

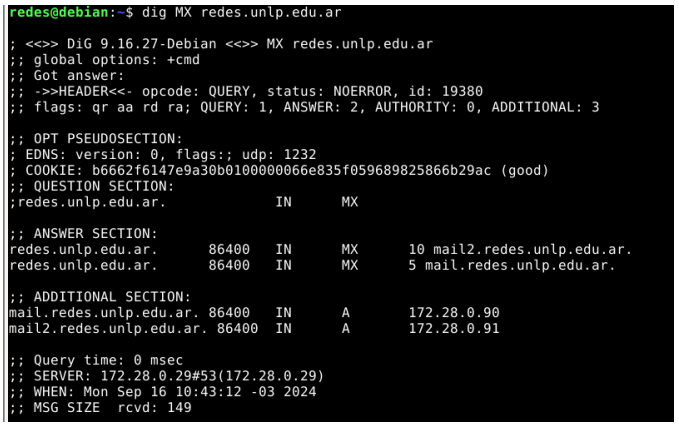
iii. ¿Cuál es la dirección IP del resolver utilizado? ¿Cómo lo sabe?

La dirección IP del resolver usado es

;; SERVER: 172.28.0.29#53(172.28.0.29)

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?



Servidores de correo

- mail2.redes.unlp.edu.ar
- mail.redes.unlp.edu.ar

Hay más de uno porque

- **Redundancia:** Tener múltiples servidores de correo mejora la redundancia y la disponibilidad del servicio. Si uno de los servidores falla, el correo se puede enrutar al otro.
- **Balance de carga:** Al asignar diferentes pesos a los servidores de correo, se puede distribuir la carga de correo entrante de manera más equitativa. En este caso, el servidor `mail2.redes.unlp.edu.ar.` recibirá aproximadamente el doble de correo que el servidor `mail.redes.unlp.edu.ar.`.
- **Diferentes funciones:** A veces, los servidores de correo se configuran para manejar diferentes tipos de correo o para diferentes grupos de usuarios.
- **Migración:** Durante una migración de servidores de correo, se pueden configurar múltiples servidores para una transición más suave.

Números entre MX y el nombre del servidor de correo ⇒ Significa el peso/prioridad, lo cual es la probabilidad de que el correo electrónico sea enrutado a ese servidor específico, cuanto mayor sea el número, mayor la probabilidad

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?

- Se le entregará al servidor mail2.redes.unlp.edu.ar porque su peso es 10.
- Se lo entregará al otro en el caso de que no esté disponible el primero, por carga de trabajo en el caso de que mail2 este muy cargado, por fallos transitorios o por configuración adicional que determine el servidor final.

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

Usando el comando

```
dig NS redes.unlp.edu.ar
```

Se obtienen los siguientes servidores que se encuentran a la derecha

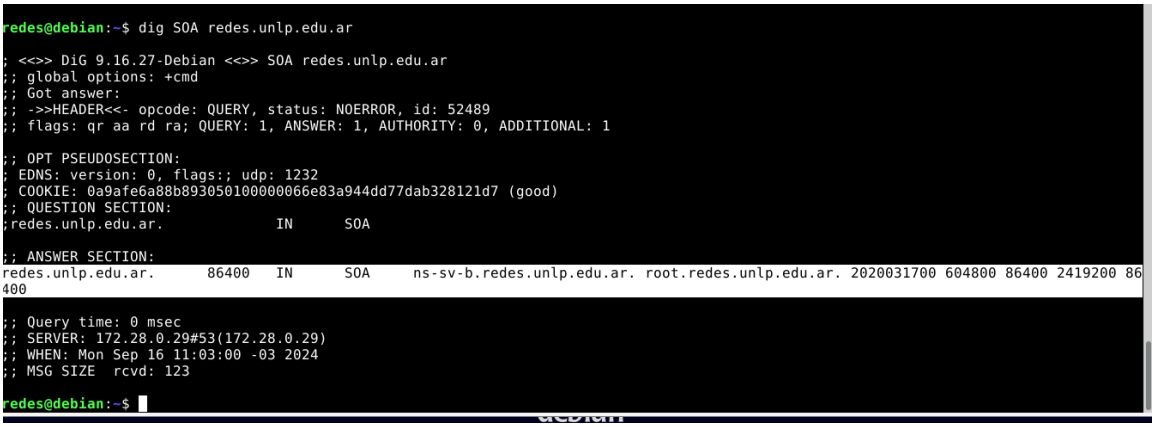
```
;; ANSWER SECTION:
redes.unlp.edu.ar.      86400   IN      NS      ns-sv-a.redes.unlp.edu.ar.
redes.unlp.edu.ar.      86400   IN      NS      ns-sv-b.redes.unlp.edu.ar.
```

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?

No, no es posible. Se puede indicar por el comando SOA

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



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

Si, el servidor primario es ns-nv-b.redes.unlp.edu.ar

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

```
redes.unlp.edu.ar.     86400  IN  SOA  ns-sv-b.redes.unlp.edu.ar.
root.redes.unlp.edu.ar. 2020031700 604800 86400 2419200 86400
```

El número de serie es `2020031700`. Este formato sigue la **convención de fecha y revisión**. Los primeros 8 dígitos (20200317) representan la fecha (17 de marzo de 2020) y los dos últimos dígitos (00) indican la revisión en ese día.

Casos en los que es importante actualizarlo:

- **Cuando se agregan nuevos registros:**
  - Al incorporar un nuevo registro (por ejemplo, un registro A para un nuevo servidor web), el número de serie debe incrementarse para notificar a los servidores DNS secundarios que deben actualizar su copia de la zona. De esta manera, los nuevos servicios estarán disponibles de inmediato.
- **Cuando se modifican registros existentes:**
  - Si se cambia el valor de un registro existente (por ejemplo, la dirección IP de un servidor), es necesario actualizar el número de serie. Esto garantiza que la información de los servidores DNS

secundarios esté siempre actualizada y refleje los cambios realizados.

- **Cuando se eliminan registros:**
  - Al eliminar un registro, el número de serie debe incrementarse para indicar a los servidores DNS secundarios que eliminen ese registro de sus copias locales.
- **Cuando se modifican los TTLs:**
  - Los TTLs (Time To Live) determinan cuánto tiempo los servidores DNS pueden almacenar una respuesta en caché antes de volver a consultar al servidor primario. Si se modifican los TTLs, es recomendable actualizar el número de serie para asegurar que los cambios se propaguen rápidamente.
- **Cuando se realizan cambios en la estructura de la zona:**
  - Si se realizan cambios en la estructura de la zona DNS, como agregar o eliminar subdominios, es necesario actualizar el número de serie.

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

- **Segundo campo (86400):** Este valor representa el **TTL (Time To Live)** del registro SOA. El TTL indica durante cuánto tiempo los servidores DNS pueden almacenar en caché la información del registro SOA antes de volver a consultarlo al servidor primario. En este caso, el TTL es de 86400 segundos, lo que equivale a 1 día.

¿Qué significa esto?

- Los servidores DNS que consulten la información de la zona `redes.unlp.edu.ar` pueden almacenar en caché el registro SOA durante un día completo antes de volver a solicitar una actualización al servidor primario.
- Si no hay cambios en la zona durante ese período, los servidores DNS secundarios pueden utilizar la información almacenada en caché, lo que mejora la velocidad y eficiencia de la resolución de nombres.
- Si se realiza algún cambio en la zona, el servidor primario debe ser consultado nuevamente para obtener la nueva información y actualizar

el valor del número de serie en el registro SOA.

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.

```
redes@debian:~$ dig TXT saludo.redes.unlp.edu.ar

; <<>> DiG 9.16.27-Debian <<>> TXT saludo.redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47919
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 586b85695de1ee850100000066e8403ced93dca6e6f4b7c3 (good)
;; QUESTION SECTION:
;saludo.redes.unlp.edu.ar.      IN      TXT

;; ANSWER SECTION:
saludo.redes.unlp.edu.ar. 86400 IN      TXT     "HOLA"

;; Query time: 0 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Mon Sep 16 11:27:08 -03 2024
;; MSG SIZE  rcvd: 98
```

Tiene el valor “HOLA” . El registro TXT permite almacenar información de texto arbitrario en un dominio.

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

```
redes@debian:~$ dig AXFR redes.unlp.edu.ar

; <<>> DiG 9.16.27-Debian <<>> AXFR redes.unlp.edu.ar
;; global options: +cmd
redes.unlp.edu.ar.      86400   IN      SOA     ns-sv-b.redes.unlp.edu.ar. root.redes.unlp.edu.ar. 2020031700 604800 86400 2419200 86
400
redes.unlp.edu.ar.      86400   IN      NS      ns-sv-a.redes.unlp.edu.ar.
redes.unlp.edu.ar.      86400   IN      NS      ns-sv-b.redes.unlp.edu.ar.
redes.unlp.edu.ar.      86400   IN      MX      5 mail.redes.unlp.edu.ar.
redes.unlp.edu.ar.      86400   IN      MX      10 mail2.redes.unlp.edu.ar.
ftp.redes.unlp.edu.ar.  86400   IN      CNAME   www.redes.unlp.edu.ar.
mail.redes.unlp.edu.ar. 86400   IN      A       172.28.0.90
mail2.redes.unlp.edu.ar. 86400  IN      A       172.28.0.91
ns-sv-a.redes.unlp.edu.ar. 604800 IN    A       172.28.0.30
ns-sv-b.redes.unlp.edu.ar. 604800 IN    A       172.28.0.29
practica.redes.unlp.edu.ar. 86400 IN    NS      ns1.practica.redes.unlp.edu.ar.
practica.redes.unlp.edu.ar. 86400 IN    NS      ns2.practica.redes.unlp.edu.ar.
ns1.practica.redes.unlp.edu.ar. 86400 IN A      172.28.0.120
ns2.practica.redes.unlp.edu.ar. 86400 IN A      172.28.0.121
saludo.redes.unlp.edu.ar. 86400 IN      TXT     "HOLA"
www.redes.unlp.edu.ar.  300     IN      A       172.28.0.50
redes.unlp.edu.ar.      86400   IN      SOA     ns-sv-b.redes.unlp.edu.ar. root.redes.unlp.edu.ar. 2020031700 604800 86400 2419200 86
400
;; Query time: 7 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Mon Sep 16 11:36:51 -03 2024
;; XFR size: 17 records (messages 1, bytes 441)
```

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

Signifcan el TLL, cuya finalidad es determinar el momento en el que el recurso debe ser borrado de la caché

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?

Hay 4 registros NS. En cambio, cuando se obtuvieron los servidores de DNS del mismo dominio a través de dig NS redes.unlp.edu.ar solo se obtuvieron 2. Esa diferencia se debe a que con AXFR me da los servidores de los subdominios de redes.unlp.edu.ar, como lo es practica.redes.unlp.edu.ar.

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).

```
redes@debian:~$ dig A redes.unlp.edu.ar

; <<>> DiG 9.16.27-Debian <<>> A redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25326
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 586c68aa6bb6e0e50100000066e8450b688509422c9b67c6 (good)
;; QUESTION SECTION:
;redes.unlp.edu.ar.             IN      A

;; AUTHORITY SECTION:
redes.unlp.edu.ar.      86400   IN      SOA     ns-sv-b.redes.unlp.edu.ar. root.redes.unlp.edu.ar. 2020031700 604800 86400 2419200 864
00

;; Query time: 3 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Mon Sep 16 11:47:39 -03 2024
;; MSG SIZE  rcvd: 123
```

TLL ⇒ 86400

```
redes@debian:~$ dig A practica.redes.unlp.edu.ar

; <<>> DiG 9.16.27-Debian <<>> A practica.redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14999
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 2670a85f44bbb7190100000066e845011e91ba3edd914773 (good)
;; QUESTION SECTION:
;practica.redes.unlp.edu.ar.    IN      A

;; AUTHORITY SECTION:
practica.redes.unlp.edu.ar. 8588 IN     SOA     ns1.practicas.redes.unlp.edu.ar. admin.practicas.redes.unlp.edu.ar. 2020031904 60480
86400 2419200 604800

;; Query time: 3 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Mon Sep 16 11:47:29 -03 2024
;; MSG SIZE  rcvd: 156
```

TLL⇒ 8588

2da

```
redes@debian:~$ dig A redes.unlp.edu.ar

; <<>> DiG 9.16.27-Debian <<>> A redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28620
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a68fd39d99a656750100000066e845a1a6a9380da663e35d (good)
;; QUESTION SECTION:
;redes.unlp.edu.ar.             IN      A

;; AUTHORITY SECTION:
redes.unlp.edu.ar.      86400   IN      SOA     ns-sv-b.redes.unlp.edu.ar. root.redes.unlp.edu.ar. 2020031700 604800 86400 2419200 864
00

;; Query time: 0 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Mon Sep 16 11:50:09 -03 2024
;; MSG SIZE  rcvd: 123
```

Mismo TLL

```
redes@debian:~$ dig A practica.redes.unlp.edu.ar

; <<>> DiG 9.16.27-Debian <<>> A practica.redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13271
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 413b650f5622cb860100000066e84595d0ecb886a856b88f (good)
;; QUESTION SECTION:
;practica.redes.unlp.edu.ar.    IN      A

;; AUTHORITY SECTION:
practica.redes.unlp.edu.ar. 8440 IN     SOA     ns1.practicas.redes.unlp.edu.ar. admin.practicas.redes.unlp.edu.ar. 2020031904 604800
86400 2419200 604800

;; Query time: 0 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Mon Sep 16 11:49:57 -03 2024
;; MSG SIZE  rcvd: 156
```

TLL ⇒ 8440

¿Puede explicar qué está ocurriendo? (Pista: observar los flags será de ayuda).

El TLL de practica va disminuyendo, a diferencia de el TLL de redes en el que se mantiene. Esto es debido a que en practica no se encuentra la flag “aa”, lo que significa que la respuesta es no autoritativa y debe ir a buscar la información a otro servidor y almacenarla en su cache, a más bajo TLL significa que su caché se actualiza con frecuencia. En cambio en redes la flag “aa” se encuentra, lo que significa que no tiene que ir a buscar a otro lado la rta.

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?

```
redes@debian:~$ dig A www.practica2.redes.unlp.edu.ar

; <<>> DiG 9.16.27-Debian <<>> A www.practica2.redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 21189
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 139087b15887093a0100000066e848aed1bdef7f5235a1f5 (good)
;; QUESTION SECTION:
;www.practica2.redes.unlp.edu.ar. IN    A

;; AUTHORITY SECTION:
redes.unlp.edu.ar.      86400   IN      SOA     ns-sv-b.redes.unlp.edu.ar. root.redes.unlp.edu.ar. 2020031700 604800 86400 2419200
00

;; Query time: 0 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Mon Sep 16 12:03:10 -03 2024
;; MSG SIZE  rcvd: 154
```

Códigos de Respuesta No Erróneos

- **0 (NOERROR):** La consulta se ha realizado correctamente y se ha encontrado una respuesta.
- **2 (NXDOMAIN):** El dominio o el nombre de host no existe.
- **3 (NXRRSET):** No existe un conjunto de recursos del tipo solicitado.
- **5 (REFUSED):** El servidor se niega a procesar la consulta debido a una política de servidor.
- **6 (SERVFAIL):** Un error interno del servidor ha impedido procesar la consulta.
- **7 (NOTIMP):** El servidor no soporta la operación solicitada.
- **8 (REFUSED):** El servidor se niega a procesar la consulta debido a una política de servidor.

Códigos de Respuesta Relacionados con la Autoridad

- **15 (NOTAUTH):** La respuesta no es autoritativa, es decir, el servidor no es la autoridad final para la zona.
- **16 (NOTZONE):** El nombre de dominio no está dentro de la zona del servidor.

Códigos de Respuesta Relacionados con el Caching

- **11 (NXRRSET):** No existe un conjunto de recursos del tipo solicitado en la caché.

Me devolvió NXDOMAIN, lo que significa que no existe.

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.

Nslookup es un programa utilizado para saber si el DNS está resolviendo correctamente los nombres y las IPs. Se utiliza con el comando

```
nslookup
```

, que funciona tanto en Windows como en UNIX para obtener la dirección IP conociendo el nombre, y viceversa.

El comando

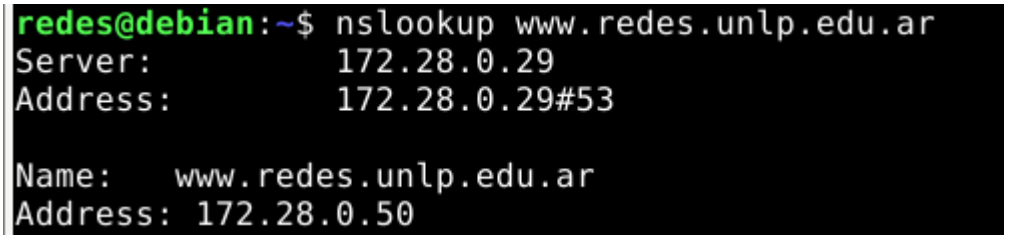
```
host
```

se usa para encontrar la dirección IP del dominio dado y también muestra el nombre de dominio para la IP dada.

● Dirección IP de www.redes.unlp.edu.ar.

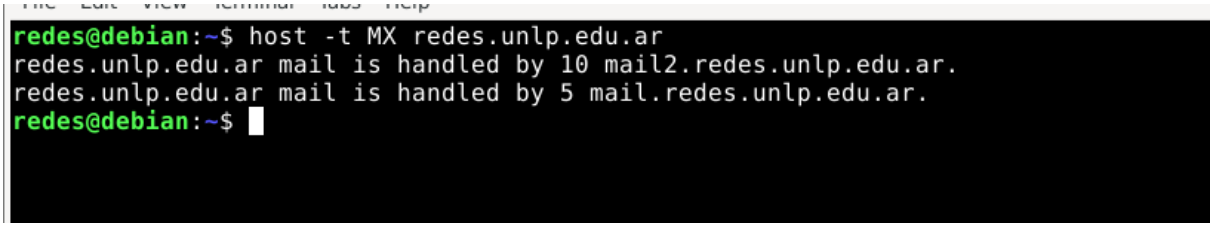
Host

Nslookup



● Servidores de correo del dominio redes.unlp.edu.ar.

Host



Nslookup

```
redes@debian:~$ nslookup -type=mx redes.unlp.edu.ar
Server:         172.28.0.29
Address:        172.28.0.29#53

redes.unlp.edu.ar       mail exchanger = 5 mail.redes.unlp.edu.ar.
redes.unlp.edu.ar       mail exchanger = 10 mail2.redes.unlp.edu.ar.
```

- Servidores de DNS del dominio redes.unlp.edu.ar.

Host

```
redes@debian:~$ host -t NS redes.unlp.edu.ar
redes.unlp.edu.ar name server ns-sv-b.redes.unlp.edu.ar.
redes.unlp.edu.ar name server ns-sv-a.redes.unlp.edu.ar.
```

Nslookup

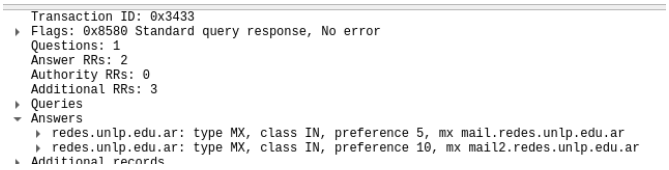
```
redes@debian:~$ nslookup -type=ns redes.unlp.edu.ar
Server:         172.28.0.29
Address:        172.28.0.29#53

redes.unlp.edu.ar       nameserver = ns-sv-a.redes.unlp.edu.ar.
redes.unlp.edu.ar       nameserver = ns-sv-b.redes.unlp.edu.ar.
```

13. ¿Qué función cumple en Linux/Unix el archivo /etc/hosts o en Windows el archivo \WINDOWS\system32\drivers\etc\hosts?

El archivo hosts de un ordenador se usa por el sistema operativo para guardar la correspondencia entre dominios de Internet y direcciones IP. Este es uno de los diferentes métodos que usa el sistema operativo para resolver nombres de dominio. Antiguamente, cuando no había servidores DNS que resolvieran los dominios, el archivo hosts era el único encargado de hacerlo.

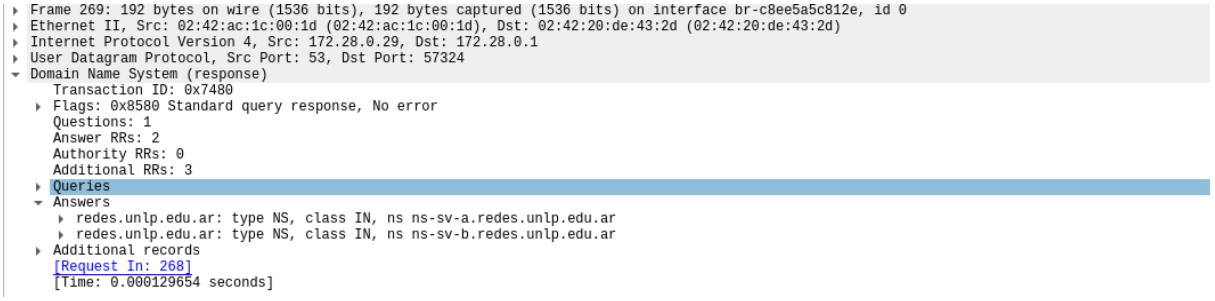
14. Abra el programa Wireshark para comenzar a capturar el tráfico de red en la interfaz con
IP 172.28.0.1. Una vez abierto realice una consulta DNS con el comando dig para averiguar
el registro MX de
redes.unlp.edu.ar y luego, otra para averiguar los registros NS correspondientes al dominio
redes.unlp.edu.ar. Analice la información proporcionada por dig
y compárelo con la captura.

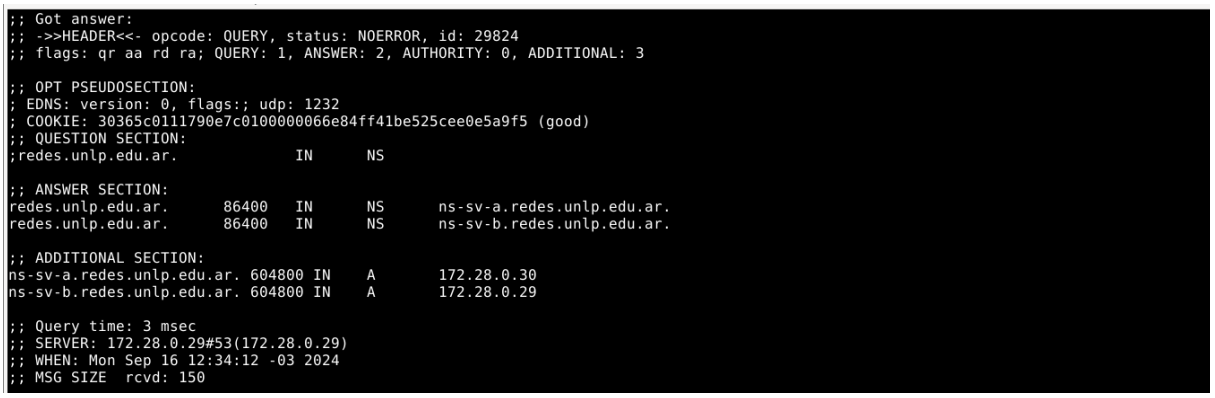
MX




```
; <<>> DiG 9.16.27-Debian <<>> MX redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13363
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 0ea8739e211aad1a0100000066e84f1539627850b0f4aba5 (good)
;; QUESTION SECTION:
;redes.unlp.edu.ar.             IN      MX

;; ANSWER SECTION:
redes.unlp.edu.ar.      86400   IN      MX      5 mail.redes.unlp.edu.ar.
redes.unlp.edu.ar.      86400   IN      MX      10 mail2.redes.unlp.edu.ar.

;; ADDITIONAL SECTION:
mail.redes.unlp.edu.ar. 86400   IN      A       172.28.0.90
mail2.redes.unlp.edu.ar. 86400  IN      A       172.28.0.91

;; Query time: 0 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Mon Sep 16 12:30:29 -03 2024
;; MSG SIZE  rcvd: 149
```

NS





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?

    Hace consultas recursivas al servidor DNS, el cual le va a responder al resolver con la rta esperada o un error. Si fueraiterativa, le responde de la mejor manera para que el cliente pueda seguir buscando

    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?

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

- **Solicitud de página:** Cuando escribes una URL (como https://www.google.com) en tu navegador, este primero consulta al

servidor DNS para obtener la dirección IP correspondiente a "google.com".

- **Conexión al servidor:** Una vez que el navegador tiene la dirección IP, establece una conexión HTTP con el servidor web en esa dirección.
- **Descarga de la página:** El navegador envía una solicitud HTTP al servidor, solicitando la página web. El servidor responde enviando la página web al navegador, que la muestra en la pantalla.

En resumen, el DNS es como una guía telefónica que nos ayuda a encontrar la dirección correcta en internet, mientras que el HTTP es el mensajero que se encarga de enviar y recibir la información entre tu computadora y el servidor web.

¿Se puede navegar si no hay servicio de DNS?

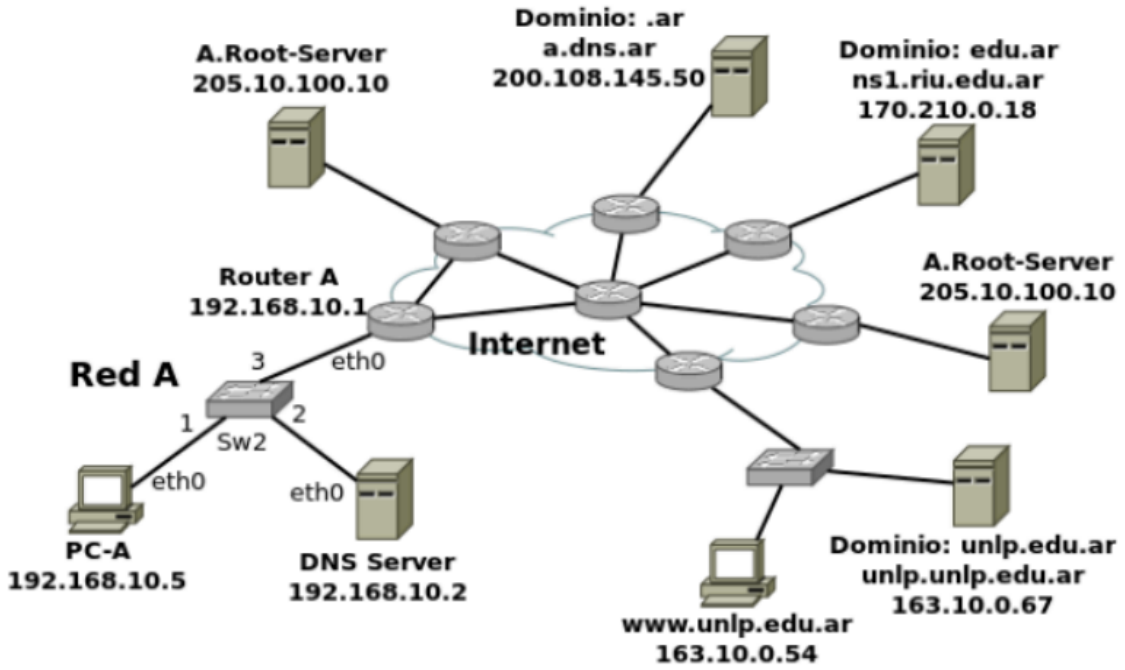
No, no es posible navegar por internet de forma normal si no hay servicio de DNS. Sin el DNS, no podríamos convertir los nombres de dominio que conocemos en las direcciones IP necesarias para acceder a los servidores web. Tendríamos que recordar y escribir las largas direcciones IP de cada sitio web que quisiéramos visitar, lo cual sería extremadamente engorroso y poco práctico.

Sin embargo, existen algunas excepciones:

- **Archivos locales:** Si tienes archivos almacenados en tu computadora o en una red local, puedes acceder a ellos utilizando su dirección IP local sin necesidad de DNS.
- **Aplicaciones que almacenan direcciones IP:** Algunas aplicaciones pueden almacenar las direcciones IP de los sitios web que visitas con frecuencia, lo que te permite acceder a ellos incluso si el servicio DNS está caído temporalmente.

En conclusión, el DNS es una parte esencial de la infraestructura de internet y juega un papel fundamental en la forma en que navegamos por la web.

17. Observar el siguiente gráfico y contestar: PREGUNTAR



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.

Pasos:

1. PC-A hace una consulta al DNS Server 192.168.10.2
2. DNS Server 192.168.10.2 hace una consulta a A Root-Server (siempre se arranca desde este)
3. PC-A hace una consulta a DNS Server `192.168.10.2` por el dominio www.unlp.edu.ar
4. DNS Server `192.168.10.2` hace una consulta a A.Root-Server (el que este más cerca)
5. A.Root-Server el responde a DNS Server `192.168.10.2` con los NS de `.ar` que es `a.dns.ar`
6. DNS Server `192.168.10.2` consulta a `a.dns.ar`
7. a.dns.ar le responde con el los NS de edu.ar
8. DNS Server `192.168.10.2` hace una consulta a ns1.riu.edu.ar
9. ns1.riu.edu.ar le responde con los NS de unlp.edu.ar

10. DNS Server `192.168.10.2` hace una consulta a unlp.edu.ar por los registros A
11. unlp.edu.ar le responde con los registros A de unlp.edu.ar (que incluye el de www)
12. DNS Server `192.168.10.2` le envia a PC-A el IP de www.unlp.edu.ar

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

De PC-A a DNS Server la consulta es recursiva, mientras que todas las consultas de DNS Server son iterativas.

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

Para que la respuesta sea autoritativa hay que hacer la consulta a un servidor autoritativo del dominio `www.google.com`, dicho servidor podemos obtenerlo consultando por los registros NS.

- Obtenemos el servidor:

```
redes@debian:~$ dig www.google.com NS

; <<>> DiG 9.16.27-Debian <<>> www.google.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36797
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 1cb18f85f0b385fb010000006314abc09fa659572bcf583a (good)
;; QUESTION SECTION:
;www.google.com.                        IN      NS

;; AUTHORITY SECTION:
google.com.             60      IN      SOA     ns1.google.com. dns-admin.google
.com. 471985200 900 900 1800 60
```

- Consultamos a ese servidor:

```
redes@debian:~$ dig @ns1.google.com. www.google.com

; <<>> DiG 9.16.27-Debian <<>> @ns1.google.com. www.google.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47679
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         300     IN      A       142.251.134.36
```

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 al servidor le consulto por `www.info.unlp.edu.ar` no obtengo respuesta ya que dicho servidor no tiene en sus registros el IP de la URL consultada.

```
redes@debian:~$ dig @ns1.google.com. www.info.unlp.edu.ar

; <<>> DiG 9.16.27-Debian <<>> @ns1.google.com. www.info.unlp.edu.ar
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 14354
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.info.unlp.edu.ar.          IN      A

;; Query time: 36 msec
;; SERVER: 216.239.32.10#53(216.239.32.10)
;; WHEN: Sun Sep 04 10:48:02 -03 2022
;; MSG SIZE  rcvd: 49
```

En cambio, si le consulto al servidor `8.8.8.8` si obtengo respuesta.

```
redes@debian:~$ dig @8.8.8.8 www.info.unlp.edu.ar

; <<>> DiG 9.16.27-Debian <<>> @8.8.8.8 www.info.unlp.edu.ar
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36812
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.info.unlp.edu.ar.          IN      A

;; ANSWER SECTION:
www.info.unlp.edu.ar.   300     IN      A       163.10.5.71

;; Query time: 80 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Sep 04 10:51:36 -03 2022
;; MSG SIZE  rcvd: 65
```

Ejercicio de parcial

20. En base a la siguiente salida de dig, conteste las consignas. Justifique en todos los
casos.

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 4
;; QUESTION SECTION:
;ejemplo.com.          IN      __

;; ANSWER SECTION:
ejemplo.com.          1634 IN      __      10      srv01.ejemplo.com.   (1)
ejemplo.com.          1634 IN      __      5       srv00.ejemplo.com.   (2)

 ;; AUTHORITY SECTION:
ejemplo.com.          92354 IN     __      ss00.ejemplo.com.
ejemplo.com.          92354 IN     __      ss02.ejemplo.com.
ejemplo.com.          92354 IN     __      ss01.ejemplo.com.
ejemplo.com.          92354 IN     __      ss03.ejemplo.com.

;; ADDITIONAL SECTION:
srv01.ejemplo.com.    272     IN     __      64.233.186.26
srv01.ejemplo.com.    240     IN     __      2800:3f0:4003:c00::1a
srv00.ejemplo.com.    272     IN     __      74.125.133.26
srv00.ejemplo.com.    240     IN     __      2a00:1450:400c:c07::1b
```

a. Complete las líneas donde aparece __ con el registro correcto.

;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 4
;; QUESTION SECTION:
;
ejemplo.com. IN MX
;; ANSWER SECTION:

ejemplo.com. 1634 IN MX 10 srv01.ejemplo.com. (1)

ejemplo.com. 1634 IN MX 5 srv00.ejemplo.com. (2)
;; AUTHORITY SECTION:

ejemplo.com. 92354 IN NS ss00.ejemplo.com.

ejemplo.com. 92354 IN NS ss02.ejemplo.com.

ejemplo.com. 92354 IN NS ss01.ejemplo.com.

ejemplo.com. 92354 IN NS ss03.ejemplo.com.
;; ADDITIONAL SECTION:

srv01.ejemplo.com. 272 IN A 64.233.186.26

srv01.ejemplo.com. 240 IN __ 2800:3f0:4003:c00::1a

srv00.ejemplo.com. 272 IN A 74.125.133.26

srv00.ejemplo.com. 240 IN A 2a00:1450:400c:c07::1b

b. ¿Es una respuesta autoritativa? En caso de no serlo, ¿a qué servidor le preguntaría
para obtener una respuesta autoritativa?

No, no es autoritativa porque en las flags no está “aa” que indica que es autoritativa. Le preguntaría a soa cual es el primario (que va a ser alguno que esté en authority

c. ¿La consulta fue recursiva? ¿Y la respuesta?

Si, ambas lo fueron ya que están las flags

rd ⇒ indica que la consulta solicitó recursión

ra ⇒ indica que el servidor DNS respondió indicando que puede manejar consultas recursivas

d. ¿Qué representan los valores 10 y 5 en las líneas (1) y (2).

Representa la prioridad de cada servidor de correo, a menr numero, mayor prioridad a la hora de entregarle un correo a algun de los servidores. En este caso, s más probable que se le entregue al de valor 5.