Práctica 3 - Redes y Comunicaciones

Ejercicios de la Práctica

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

- Es una base de datos distribuida implementada en una jerarquía de servidores DNS y un protocolo de la capa de aplicación que permite a los hosts consultar la base de datos distribuida.
    - Se ejecuta entre sistemas terminales que están en comunicación utilizando el paradigma Cliente/Servidor.
    - Se basa en un protocolo de transporte subyacente extremo a extremo para transferir los mensajes DNS entre los sistemas terminales en comunicación.
    - Usa una base de datos distribuida para mantener una gran cantidad de información, generar delegación y porque una base de datos de este estilo es más tolerante a fallos y más escalable. Tiene un modelo de acceso a la información altamente cacheable.

Tiene como **función principal** ser un servicio de directorio que traduce los nombres de host en direcciones IP. Por ejemplo, si un navegador que se ejecuta sobre un host de usuario solicita el URL "www.unaEscuela.edu/index.html" para que el host del usuario pueda enviar un mensaje de solicitud HTTP al servidor "www.unaEscuela.edu" el host del usuario debe obtener la dirección IP de "www.unaEscuela.edu". Esto ocurre de la siguiente manera:

1) La propia máquina cliente ejecuta el lado del cliente de la aplicación DNS.
2) El navegador extrae el nombre del host "www.unaEscuela.edu" de la URL y pasa ese nombre al lado del cliente de la aplicación DNS.
3) El cliente DNS envía una consulta que contiene el nombre del host a un servidor DNS.
4) El cliente DNS recibe una respuesta que incluye la dirección IP correspondiente al nombre del host.
5) Una vez que el navegador recibe la dirección IP del servidor DNS, puede iniciar una conexión TCP con el proceso servidor HTTP localizado en el puerto 80 en esa dirección IP.

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

- **Root Server/Servidor Raíz**
    - Servidores que proporcionan las direcciones IP de los servidores TLD. No deberían permitir recursivas. Existen unos 400 servidores de nombres raíz distribuidos por todo el mundo. Trece organizaciones diferentes se encargan de gestionarlos.
- **Generic top-level domain (gtld)**

- Son una categoría TLD en DNS, contienen dominios con propósitos particulares, de acuerdo a diferentes actividades. Estos son los más comunes y no están vinculados a ninguna ubicación geográfica específica. Ejemplos incluyen .com, .net, y .org. Se utilizan para una amplia variedad de propósitos y son ideales para sitios web globales.
  Pueden ser:
  - **Sponsored TLD´s**
    - Son dominios de nivel superior que tienen una organización patrocinadora específica que representa a una comunidad particular y establece las reglas y políticas para su uso. Estas comunidades pueden estar basadas en criterios étnicos, geográficos, profesionales, técnicos u otros conceptos temáticos.
  - **Unsponsored TLDs (uTLDs)**
    - Son dominios de nivel superior que no tienen una organización patrocinadora específica que establezca las reglas y políticas para su uso. En cambio, operan bajo políticas establecidas por la comunidad global de Internet a través del proceso de ICANN (Internet Corporation for Assigned Names and Numbers).

3. **¿Qué es una respuesta del tipo autoritativa?**

- Una **respuesta autoritativa** proviene directamente del servidor que es responsable del dominio que se está consultando. Esto significa que el servidor tiene información confiable y directa sobre el dominio en cuestión.

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

- En una **consulta recursiva**, el **servidor DNS** hace todo el trabajo de búsqueda, mientras que en una **consulta iterativa**, el **cliente DNS** sigue las referencias proporcionadas por los **servidores DNS** hasta encontrar la respuesta.

5. **¿Qué es el resolver?**

- Un **resolver DNS** es un componente crucial en la arquitectura DNS. Su función es recibir las consultas DNS de un cliente (como un navegador web o una aplicación) y gestionar el proceso para obtener la dirección IP correspondiente a un nombre de dominio. En términos generales, se encarga de todo el proceso de búsqueda de una dirección IP, interactuando con diferentes servidores DNS a lo largo del camino, desde los servidores raíz hasta los servidores autoritativos del dominio en cuestión. Se puede tener un **Stub/Dumb Resolver** que no realiza ninguna forma de caching y deja que el encargado de esto sea el Servidor Local o un resolver activo, llamado **Smart Resolver**, que funciona en cada equipo como si fuese un Servidor Local, realizando caching u ofreciendo funcionalidades extras. Este suele hacer consultas recursivas.

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

- El registro **A (Address Record)** es uno de los más comunes y asocia un nombre de dominio con una dirección IPv4. Cada vez que un usuario ingresa un dominio en su navegador, el servidor DNS busca el registro A para obtener la dirección IP del servidor donde está alojado el sitio web.

    b. **MX**

- El registro **MX (Mail Exchange Record)** indica los servidores de correo responsables de recibir correos electrónicos para el dominio. Define la prioridad y el servidor al cual deben ser enviados los correos electrónicos destinados a ese dominio.

    c. **PTR**

- El registro **PTR (Pointer Record)** es utilizado en las búsquedas DNS inversas, es decir, cuando se desea encontrar el nombre de dominio asociado a una dirección IP. Es común en sistemas de autenticación y correo para verificar el origen de los mensajes.

    d. **AAAA**

- El registro **AAAA (IPv6 Address Record)** es similar al registro A, pero para direcciones IPv6. Este registro asocia un nombre de dominio con una dirección IP versión 6 (IPv6), que es la nueva generación de direcciones IP.

    e. **SRV**

- El registro **SRV (Service Record)** es utilizado para definir la ubicación de servicios específicos dentro del dominio, como servidores de mensajería o VoIP. Indica el puerto y la prioridad para acceder al servicio.

    f. **NS**

- El registro **NS (Name Server Record)** indica los servidores DNS autoritativos para un dominio. Estos son los servidores que tienen la autoridad para responder consultas sobre el dominio en cuestión. A partir de esto, se puede lograr una delegación de sub-dominios. No hay prioridad, todos los servidores tienen la misma precedencia.

    g. **CNAME**

- El registro **CNAME (Canonical Name Record)** es utilizado para crear un alias de un dominio. Redirige un nombre de dominio a otro, lo que permite usar

diferentes nombres de dominio que apunten a la misma dirección IP. Hacen el mapeo del alias de un dominio su nombre canónico

h. SOA

- El registro **SOA (Start Of Authority Record)** contiene información administrativa sobre la zona DNS, como el servidor principal de la zona, el correo electrónico del administrador, el número de serie y los tiempos de actualización de los registros. Solo se admite un registro SOA por zona. Permite que servidores autoritarios de la misma zona se puedan sincronizar.

i. TXT

- El registro **TXT (Text Record)** permite asociar texto arbitrario a un dominio. Se utiliza para diversas finalidades, como verificar la propiedad del dominio o especificar políticas de seguridad (por ejemplo, en SPF o DKIM para proteger el correo electrónico).

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

- Un dominio suele tener múltiples servidores DNS para garantizar **redundancia** y **tolerancia a fallos**. Las razones principales son:
    - **Alta disponibilidad**
        - Si un servidor DNS falla o no está disponible, los otros servidores pueden seguir respondiendo a las consultas. Esto asegura que el dominio siga siendo **accesible** en **todo momento**, reduciendo el riesgo de **interrupciones**.
    - **Balanceo de carga**
        - Al tener más de un servidor DNS, la carga de consultas se puede distribuir entre varios servidores, lo que mejora el **rendimiento** y evita que un solo servidor se **sobrecargue**.
    - **Resiliencia ante ataques**
        - Múltiples servidores DNS hacen que un dominio sea más resistente a **ataques de denegación de servicio (DDoS)**, ya que es más difícil que todos los servidores queden fuera de servicio al mismo tiempo.
    - **Georredundancia**
        - Tener servidores DNS en distintas ubicaciones geográficas mejora el tiempo de respuesta para los usuarios en diferentes partes del mundo, ya que las consultas pueden ser atendidas por el **servidor más cercano**.

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 por la cual un dominio tiene un **servidor DNS primario (maestro)** y **servidores secundarios (esclavos)** es para permitir una **gestión centralizada y coherente** de la zona DNS, a la vez que se proporciona **redundancia y respaldo**.
    - **Servidor Primario (maestro)**
        - Servidor donde se realizan las actualizaciones y cambios en los registros DNS de un dominio. Este servidor tiene la autoridad y el control sobre la zona DNS. Cualquier modificación en los registros se realiza aquí.
    - **Servidores Secundarios (esclavos)**
        - Servidores que mantienen una copia de la información de la zona DNS, replicada desde el servidor primario. Su función principal es proporcionar **redundancia**. Si el servidor primario falla, los servidores secundarios pueden seguir respondiendo las consultas DNS para ese dominio.

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

- Los servidores secundarios se actualizan automáticamente a través de un proceso llamado **transferencia de zona**, que permite que los cambios en los registros del servidor primario se propaguen a los servidores secundarios de manera periódica, manteniendo 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.**

- Para que el administrador de la nueva Facultad de Redes pueda gestionar su dominio “redes.unlp.edu.ar” de forma independiente, es necesario realizar una **delegación de dominio** que implica que yo (administrador del dominio de la UNLP) le delegue la autoridad sobre el subdominio “redes.unlp.edu.ar” a los servidores DNS que gestiona el administrador de la Facultad de Redes. Yo, debería agregar los **registros NS (Name Server)** en la zona DNS de “unlp.edu.ar" que apunten a los servidores DNS de la Facultad de Redes generando de este modo la delegación de dominio, ya que se redirigen las consultas para el subdominio “redes.unlp.edu.ar” a los servidores DNS que gestionan ese subdominio. **Los registros NS deben incluir los nombres de los servidores DNS autoritativos de “redes.unlp.edu.ar”.**

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: 38146
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 1537643c7d5d20100100000066eab9d1f68b194f91dacec1 (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: Wed Sep 18 08:30:25 -03 2024
;; MSG SIZE  rcvd: 94
```

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

- La solicitud fue recursiva, esto lo podemos ver gracias al flag **rd (Recursion Desired)** que indica que el cliente le pidió al servidor que resolviera la consulta de manera recursiva. La respuesta también fue recursiva, esto lo podemos ver gracias al flag **ra (Recursion Available)** que indica que el servidor completó la consulta en nombre del cliente de manera recursiva. La sección relevante de la salida para saber esto es:
  - **; ; flags: qr aa rd ra;**

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

- La respuesta fue autoritativa, esto lo vemos gracias al flag **aa (Authoritative Answer).** Una respuesta autoritativa significa que el servidor que proporcionó la respuesta es directamente responsable del dominio “redes.unlp.edu.ar” y tiene la autoridad sobre los registros DNS de ese dominio.

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

- La dirección IP del resolver utilizado es **172.28.0.29**. Esto se ve en la línea que indica el servidor que procesó la consulta:

- ;; **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?

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

; <<>> DiG 9.16.27-Debian <<>> MX redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24164
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 6ddd9e5d37861b9b0100000066eabf361a5f919ca7053370 (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: Wed Sep 18 08:53:26 -03 2024
;; MSG SIZE  rcvd: 149
```

- Los servidores de correo (registros MX) para el dominio redes.unlp.edu.ar son:
  - **mail.redes.unlp.edu.ar con prioridad 5.**
  - **mail2.redes.unlp.edu.ar con prioridad 10.**

  Hay más de un servidor para garantizar **redundancia** y **tolerancia a fallos**. Si uno falla o está inactivo, el otro se puede encargar de la entrega del correo. **Los números entre MX y el nombre (5 y 10)** representan la prioridad de cada servidor de correo. Cuanto más bajo sea el número, mayor será la prioridad del servidor. En este caso, **mail.redes.unlp.edu.ar** con **prioridad 5** es el servidor principal, y **mail2.redes.unlp.edu.ar** con **prioridad 10** es el secundario.
  Si se quiere enviar un correo destinado a redes.unlp.edu.ar, será entregado primero al servidor con **mayor prioridad**, es decir, mail.redes.unlp.edu.ar. Si el servidor con mayor prioridad (mail.redes.unlp.edu.ar) no está disponible o no responde, el correo será entregado al siguiente servidor en la lista de prioridades, que en este caso es mail2.redes.unlp.edu.ar.

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

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

; <<>> DiG 9.16.27-Debian <<>> NS redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10922
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 6935887347bc03f00100000066eac17bdbc40475c8003c31 (good)
;; QUESTION SECTION:
;redes.unlp.edu.ar.             IN      NS

;; 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.

;; ADDITIONAL SECTION:
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

;; Query time: 4 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Wed Sep 18 09:03:07 -03 2024
;; MSG SIZE  rcvd: 150
```

- Los servidores de DNS del dominio redes.unlp.edu.ar son:
  - **ns-sv-a.redes.unlp.edu.ar** con dirección IP **172.28.0.30.**
  - **ns-sv-b.redes.unlp.edu.ar** con dirección IP **172.28.0.29.**

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

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

; <<>> DiG 9.16.27-Debian <<>> NS redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57832
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 1a406da9fa68909101000000066eac293e2f553227768c1a3 (good)
;; QUESTION SECTION:
;redes.unlp.edu.ar.             IN      NS

;; 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.

;; ADDITIONAL SECTION:
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

;; Query time: 0 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Wed Sep 18 09:07:47 -03 2024
;; MSG SIZE  rcvd: 150
```

Cuarta respuesta proporcionada

- **En comparación con la cuarta respuesta podemos ver:**
  - El ID de la consulta cambió.
  - El TTL de los registros NS y A se mantuvo igual.
  - Los tiempos de respuesta de Query Time cambiaron, que haya tardado 0 msec para la cuarta puede indicar que la respuesta estaba almacenada en la caché de DNS.
  - La Cookie en cada consulta es diferente.
  - El contenido de When también cambió.

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?

- La consulta **dig NS redes.unlp.edu.ar** no proporciona información sobre cuál es el servidor primario. Para saber esto deberíamos verificar el registro SOA del dominio con el comando:
  - **dig SOA redes.unlp.edu.ar**

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

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

; <<>> DiG 9.16.27-Debian <<>> SOA redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56262
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 857c88885d30801f0100000066eac63e2d2e2b4a73e1a029 (good)
;; QUESTION SECTION:
;redes.unlp.edu.ar.             IN      SOA

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

;; Query time: 0 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Wed Sep 18 09:23:26 -03 2024
;; MSG SIZE  rcvd: 123
```

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

- Si, ahora que consultamos por el registro SOA podemos determinar el servidor DNS primario que es:
  - **ns-sv-b.redes.unlp.edu.ar**

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

- **El número de serie es:**
  - 2020031700

  Convención
  - El número de serie en el registro SOA generalmente sigue un **formato basado en la fecha**, con una posible **secuencia adicional para versiones incrementales.** En este caso, el formato **YYYYMMDDnn** indica que el número de serie representa el **17 de marzo de 2020**, con **00 indicando la primera versión del día.**

  Importancia
  - **El número de serie se usa para mantener la sincronización entre el servidor primario y los servidores secundarios**. Cuando se actualiza la zona en el servidor primario, se **incrementa el número de serie**. Los servidores secundarios usan este número para saber si necesitan actualizar su copia de la zona. **Es crucial para la propagación correcta de los cambios en la configuración de DNS.**

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

- **El segundo campo del registro tiene el valor**
  - 86400

Representa el **intervalo de actualización (refresh interval) en segundos.** Este valor indica cada cuánto tiempo (en este caso, cada 7 días) un servidor secundario debe consultar al servidor primario para ver si hay cambios en la zona.

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

- **El valor de TTL de caché negativa es**
  - 86400

El **TTL (Time-To-Live) de caché negativa** es el tiempo durante el cual un servidor DNS debe considerar una respuesta negativa (por ejemplo, que un dominio no existe) como válida. En este caso, **86400 segundos (24 horas)** significa que si un servidor DNS no puede encontrar una respuesta para una consulta (como un dominio inexistente), almacenará esa respuesta negativa en caché durante 24 horas antes de intentar nuevamente. **Esto ayuda a reducir la carga en los servidores DNS y a evitar consultas repetitivas para nombres que no existen.**

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: 51657
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 4598c217d50418c20100000066eacd8c4206ea7da88daeb5 (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: Wed Sep 18 09:54:36 -03 2024
;; MSG SIZE  rcvd: 98
```

- **El valor que tiene el registro TXT para el nombre saludo.redes.unlp.edu.ar es**
  - "HOLA"

  Propósito General del registro TXT
  - Se utilizan para almacenar información de texto arbitraria asociada con un dominio.

  Usos Comunes
  - **Verificación de Dominio**
    - Se usan comúnmente para la verificación de dominio en servicios de correo electrónico y otros servicios en línea. Por ejemplo, se utilizan para verificar que el dominio pertenece a una entidad o para configurar políticas de seguridad.
  - **Configuración de Políticas de Seguridad**
    - Pueden almacenar configuraciones relacionadas con políticas de seguridad, como SPF (Sender Policy Framework) y DKIM (DomainKeys Identified Mail), que ayudan a prevenir el spoofing y el phishing en correos electrónicos.
  - **Información Adicional**
    - Pueden contener cualquier tipo de información textual que el administrador del dominio considere relevante.

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

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

; <<>> DiG 9.16.27-Debian <<>> redes.unlp.edu.ar AXFR
;; global options: +cmd
redes.unlp.edu.ar.      86400   IN      SOA     ns-sv-b.redes.unlp.edu.ar. root.redes.unlp.edu.ar. 2020
031700 604800 86400 2419200 86400
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. 2020
031700 604800 86400 2419200 86400
;; Query time: 0 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Wed Sep 18 10:05:05 -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?

- Los números que aparecen antes de la palabra IN son los **valores del TTL (Time-To-Live) para cada registro DNS**. El **TTL** es un valor en segundos que indica cuánto tiempo un registro debe ser almacenado en caché por los servidores DNS y los resolutores antes de ser descartado y volver a consultar el servidor autoritativo. Tienen **como Propósito** controlar la vida útil de la información en caché. Un **TTL más alto** significa que la información se mantendrá en caché por más tiempo, lo que puede **reducir la carga en los servidores DNS** y **mejorar el rendimiento**, pero también puede hacer que **los cambios en los registros tarden más en propagarse**. Un **TTL más bajo** puede resultar en una **propagación más rápida de los cambios**, pero puede **aumentar la carga en los servidores DNS.**

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?**

- **Esta vez se observan 4 registros NS**
  - ns-sv-a.redes.unlp.edu.ar
  - ns-sv-b.redes.unlp.edu.ar
  - ns1.practica.redes.unlp.edu.ar
  - ns2.practica.redes.unlp.edu.ar

  La **diferencia** se debe a que la **consulta de transferencia de zona (AXFR)** proporciona una vista completa de todos los registros DNS para el **dominio**, **incluyendo subdominios** como practica.redes.unlp.edu.ar, que también tiene sus propios servidores de nombres (NS). La **consulta NS inicial** solo muestra los servidores de nombres para el **dominio** redes.unlp.edu.ar y no incluye los registros de servidores de nombres para **subdominios**.

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 www.redes.unlp.edu.ar

; <<>> DiG 9.16.27-Debian <<>> A www.redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64298
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: f8f4c334c9bb5bcb0100000066ead308904df13458d58fdf (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: Wed Sep 18 10:18:00 -03 2024
;; MSG SIZE  rcvd: 94
```

dig del registro A de www.redes.unlp.edu.ar

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


; <<>> DiG 9.16.27-Debian <<>> A www.practica.redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41002
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 7d03310a16dfee400100000066ead318691e75d7b2b72fa5 (good)
;; QUESTION SECTION:
;www.practica.redes.unlp.edu.ar.        IN      A

;; ANSWER SECTION:
www.practica.redes.unlp.edu.ar. 60 IN   A       172.28.0.10

;; Query time: 980 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Wed Sep 18 10:18:16 -03 2024
;; MSG SIZE  rcvd: 103
```

dig del registro A de www.practica.redes.unlp.edu.ar

- Lo que ocurre es que al hacer el **dig del registro A de www.redes.unlp .edu.ar** su TTL se mantiene en 300 ya que estamos recibiendo una respuesta autoritativa del servidor DNS que está directamente encargado de esta zona. Al hacer el **dig del registro A de** www.practica.redes.unlp.edu.ar su TTL

empieza en 60 y va disminuyendo con cada consulta ya que estamos recibiendo una respuesta no autoritativa. El TTL de www.practica.redes.unlp.edu.ar disminuye porque está siendo caché por un servidor resolutor, y cada consulta subsiguiente muestra el valor actualizado del TTL, reflejando cuánto tiempo queda hasta que esta respuesta necesite ser refrescada desde un servidor autoritativo.

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: 53671
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 223cfb14c9c6bb790100000066ead57cc77f5037452928d4 (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 86400

;; Query time: 0 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Wed Sep 18 10:28:28 -03 2024
;; MSG SIZE  rcvd: 154
```

- La consulta realizada devolvió una respuesta con el código **NXDOMAIN**, lo que indica que el nombre de dominio no existe.
- **NXDOMAIN (Non-Existent Domain)**
  - Indica que el dominio solicitado no existe en el servidor DNS consultado. Esto puede significar que el nombre del dominio está mal escrito, o que el dominio no está configurado en los servidores DNS.
- **NOERROR**
  - Indica que la consulta fue procesada correctamente y que la respuesta fue obtenida sin errores. Esto significa que el dominio existe y que la respuesta incluye datos válidos para la consulta.

12. **Investigue los comandos nslookup y host. ¿Para qué sirven? Intente con ambos comandos obtener:**

- **nslookup (Name Server Lookup)**
  - Es una herramienta de línea de comandos utilizada para consultar registros DNS de un dominio. Puedes usarlo para resolver nombres de dominio a direcciones IP y viceversa, así como para consultar diferentes tipos de

registros DNS. Se puede usar en modo interactivo para realizar múltiples consultas sin salir del programa, o en modo no interactivo para consultas únicas.

- **host**
  - Es una herramienta más simple y directa que se utiliza para realizar consultas DNS y obtener información sobre dominios. Es generalmente más fácil de usar para consultas simples y no ofrece el modo interactivo que proporciona nslookup. Normalmente se utiliza para convertir nombres a direcciones IP y viceversa. Cuando no se le dan argumentos ni opciones, host imprime un breve resumen de sus argumentos y opciones de línea de comandos.

    - **Dirección IP de www.redes.unlp.edu.ar.**

```
redes@debian:~$ nslookup www.redes.unlp.edu.ar
Server:         172.28.0.29
Address:        172.28.0.29#53

Name:   www.redes.unlp.edu.ar
Address: 172.28.0.50

redes@debian:~$ host www.redes.unlp.edu.ar
www.redes.unlp.edu.ar has address 172.28.0.50
```

    - **Servidores de correo del dominio redes.unlp.edu.ar.**

```
redes@debian:~$ nslookup
> set 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.
```

Consulta con modo interactivo de nslookup

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

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

redes@debian:~$ host -t MX redes.unlp.edu.ar
redes.unlp.edu.ar mail is handled by 10 mail2.redes.unlp.edu.ar.
redes.unlp.edu.ar mail is handled by 5 mail.redes.unlp.edu.ar.
```

Consulta con el modo no interactivo de nslookup y usando host

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

```
redes@debian:~$ nslookup -query=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.

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

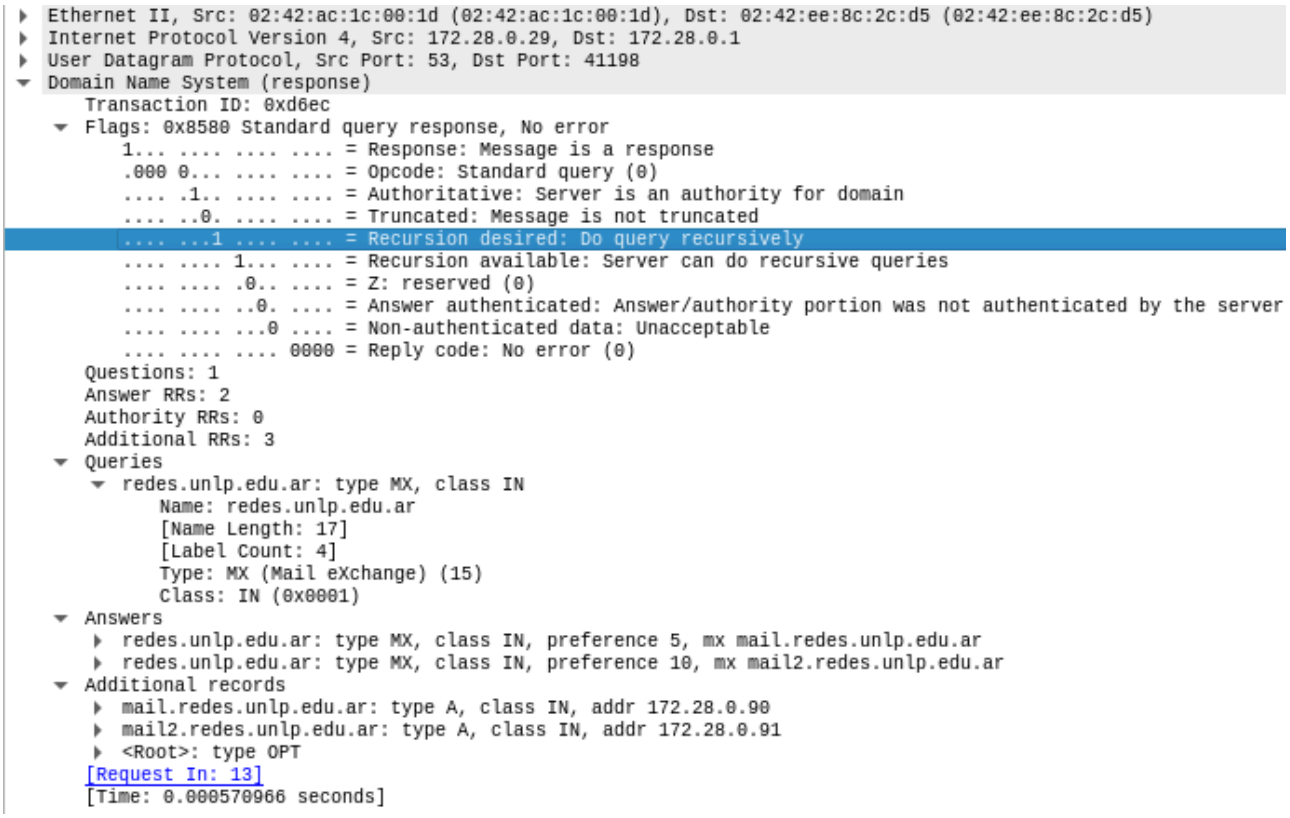
13. ¿Qué función cumple en Linux/Unix el archivo /etc/hosts o en Windows el archivo \WINDOWS\system32\drivers\etc\hosts?

- El archivo /etc/hosts en Linux/Unix y el archivo C:\WINDOWS\system32\drivers\etc\hosts en Windows son archivos de configuración importantes para la resolución de nombres de dominio en sus respectivos sistemas operativos. La función que cumplen es mapear nombres de host a direcciones IP locales sin la necesidad de consultar un servidor DNS externo.

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.

```
▸ Ethernet II, Src: 02:42:ee:8c:2c:d5 (02:42:ee:8c:2c:d5), Dst: 02:42:ac:1c:00:1d (02:42:ac:1c:00:1d)
▸ Internet Protocol Version 4, Src: 172.28.0.1, Dst: 172.28.0.29
▸ User Datagram Protocol, Src Port: 41198, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xd6ec
  ▾ Flags: 0x0120 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..1. .... = AD bit: Set
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▾ redes.unlp.edu.ar: type MX, class IN
        Name: redes.unlp.edu.ar
        [Name Length: 17]
        [Label Count: 4]
        Type: MX (Mail eXchange) (15)
        Class: IN (0x0001)
  ▾ Additional records
    ▸ <Root>: type OPT
    [Response In: 14]
```

Consulta de registro MX de redes.unlp.edu.ar



Respuesta proporcionada

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

; <<>> DiG 9.16.27-Debian <<>> MX redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55020
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 7ad97673515f24aa0100000066eade43871f45597da6beca (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: Wed Sep 18 11:05:55 -03 2024
;; MSG SIZE  rcvd: 149
```

Información proporcionada por dig

```
▸ Ethernet II, Src: 02:42:ee:8c:2c:d5 (02:42:ee:8c:2c:d5), Dst: 02:42:ac:1c:00:1d (02:42:ac:1c:00:1d)
▸ Internet Protocol Version 4, Src: 172.28.0.1, Dst: 172.28.0.29
▸ User Datagram Protocol, Src Port: 36767, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x9a6b
  ▾ Flags: 0x0120 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..1. .... = AD bit: Set
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▾ redes.unlp.edu.ar: type NS, class IN
        Name: redes.unlp.edu.ar
        [Name Length: 17]
        [Label Count: 4]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
  ▾ Additional records
    ▾ <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 4096
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      ▸ Z: 0x0000
        Data length: 12
      ▸ Option: COOKIE
```

Consulta de los registros NS de redes.unlp.edu.ar

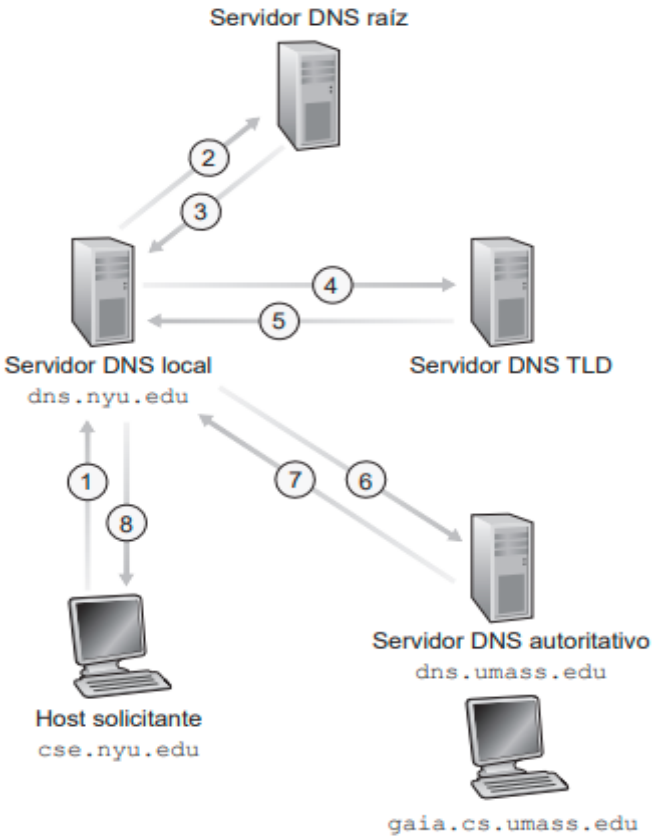
```
▸ Ethernet II, Src: 02:42:ac:1c:00:1d (02:42:ac:1c:00:1d), Dst: 02:42:ee:8c:2c:d5 (02:42:ee:8c:2c:d5)
▸ Internet Protocol Version 4, Src: 172.28.0.29, Dst: 172.28.0.1
▸ User Datagram Protocol, Src Port: 53, Dst Port: 36767
▾ Domain Name System (response)
    Transaction ID: 0x9a6b
  ▾ Flags: 0x8580 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .1.. .... .... = Authoritative: Server is an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 3
  ▾ Queries
    ▾ redes.unlp.edu.ar: type NS, class IN
        Name: redes.unlp.edu.ar
        [Name Length: 17]
        [Label Count: 4]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
  ▾ Answers
    ▸ redes.unlp.edu.ar: type NS, class IN, ns ns-sv-a.redes.unlp.edu.ar
    ▸ redes.unlp.edu.ar: type NS, class IN, ns ns-sv-b.redes.unlp.edu.ar
  ▾ Additional records
    ▸ ns-sv-a.redes.unlp.edu.ar: type A, class IN, addr 172.28.0.30
    ▸ ns-sv-b.redes.unlp.edu.ar: type A, class IN, addr 172.28.0.29
    ▸ <Root>: type OPT
```

Respuesta proporcionada

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

; <<>> DiG 9.16.27-Debian <<>> NS redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39531
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 34d57ffa91bd89d20100000066eae17e1a9a1cceea94b1aa (good)
;; QUESTION SECTION:
;redes.unlp.edu.ar.             IN      NS

;; 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.

;; ADDITIONAL SECTION:
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

;; Query time: 8 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Wed Sep 18 11:19:42 -03 2024
;; MSG SIZE  rcvd: 150
```

Información proporcionada por dig

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?**

- **La PC a su servidor de DNS local realiza consultas recursivas** ya que la PC no sabe cómo resolver el nombre de dominio por sí sola, por lo que confía en el servidor DNS para realizar todo el proceso de resolución. La PC solo espera la respuesta final del servidor 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?**

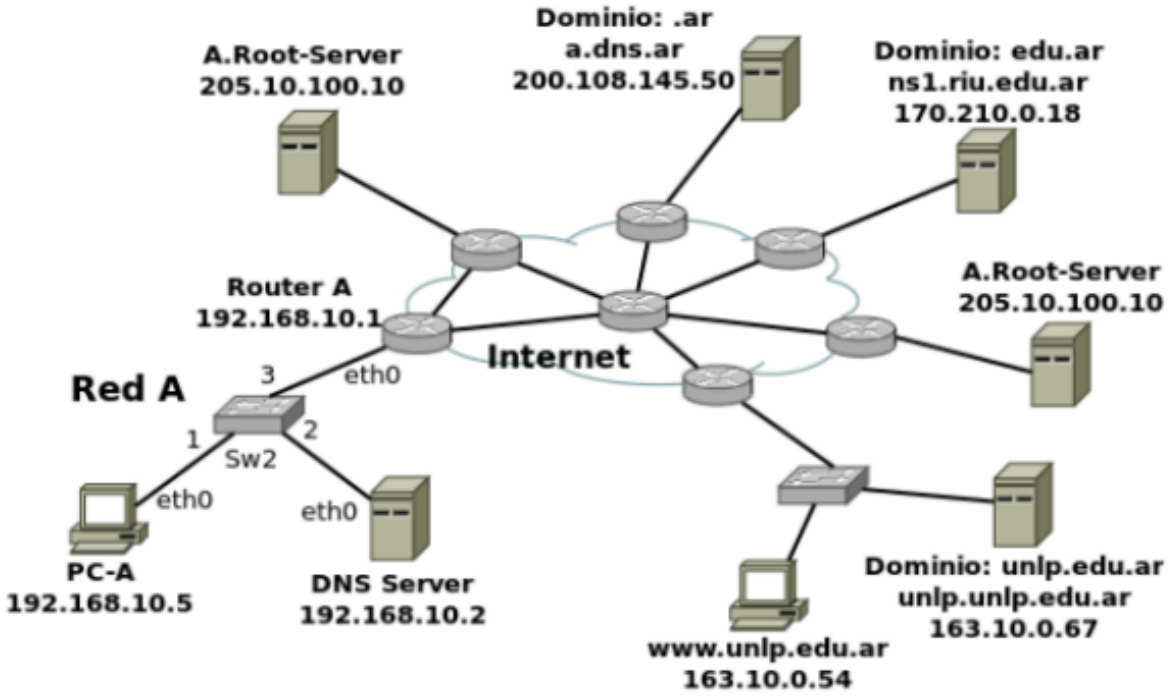
- **El servidor de DNS local** realiza **consultas iterativas** a otros servidores de DNS para resolver el requerimiento. En una consulta iterativa, el servidor de DNS pregunta a otros **servidores de DNS (raíz, TLD y autoritativos)** de manera secuencial hasta obtener la respuesta final.

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

- DNS es esencial para la navegación web moderna porque traduce nombres de dominio en direcciones IP que HTTP utiliza para realizar las solicitudes y transferencias de datos. Sin DNS, la navegación web se vuelve muy limitada, y

generalmente solo es posible si se utilizan direcciones IP directamente o métodos alternativos para la resolución de nombres.

17. Observar el siguiente gráfico y contestar:



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 con la IP 192.168.10.5** realiza una consulta recursiva a su servidor de DNS configurado que es **DNS Server con la IP 192.168.10.2.**
    2. **DNS Server** verifica en su caché si es que tiene la respuesta, si la tiene la devuelve a **PC-A**, sino empieza una consulta iterativa**.**
    3. **DNS Server** consulta iterativamente a un servidor raíz como por ejemplo **A.Root-Server con la IP 205.10.100.10.**
    4. **A.Root-Server** responde iterativamente con el NS y la dirección del servidor TLD para ".ar" que sería **a.dns.ar con la IP 200.108.145.50.**
    5. **DNS Server** consulta iterativamente al servidor TLD **a.dns.ar con la IP 200.108.145.50.**
    6. **a.dns.ar con la IP 200.108.145.50** responde iterativamente con el NS y la dirección del servidor TLD para "edu.ar" que sería **ns1.riu.edu.ar con la IP 170.210.0.18.**
    7. **DNS Server** consulta iterativamente al servidor TLD **ns1.riu.edu.ar con la IP 170.210.0.18.**

8. **ns1.riu.edu.ar con la IP 170.210.0.18** responde iterativamente con el NS y la dirección del servidor autoritativo para “unlp.edu.ar” que sería **unlp.unlp.edu.ar con la IP 163.10.0.67.**
9. **DNS Server** consulta iterativamente al servidor autoritativo **unlp.unlp.edu.ar con la IP 163.10.0.67.**
10. **unlp.unlp.edu.ar con la IP 163.10.0.67** responde iterativamente con la dirección IP de **www.unlp.edu.ar (163.10.0.54).**
11. **DNS Server** cacheara la respuesta y le responderá a la **PC-A** con la dirección IP de **www.unlp.edu.ar (163.10.0.54).**

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

- La consulta de **PC-A con DNS Server** es recursiva, después la que hace **DNS-Server con los demás servidores de la jerarquía** son iterativas.

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

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

; <<>> DiG 9.16.27-Debian <<>> NS google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26858
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: be7d01476432855801000000066eaf062f553616e95f966de (good)
;; QUESTION SECTION:
;google.com.                    IN      NS

;; ANSWER SECTION:
google.com.             158637  IN      NS      ns2.google.com.
google.com.             158637  IN      NS      ns3.google.com.
google.com.             158637  IN      NS      ns4.google.com.
google.com.             158637  IN      NS      ns1.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         345439  IN      A       216.239.32.10
ns2.google.com.         158636  IN      A       216.239.34.10
ns3.google.com.         158636  IN      A       216.239.36.10
ns4.google.com.         158636  IN      A       216.239.38.10
ns1.google.com.         345439  IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         158636  IN      AAAA    2001:4860:4802:34::a
ns3.google.com.         158636  IN      AAAA    2001:4860:4802:36::a
ns4.google.com.         158636  IN      AAAA    2001:4860:4802:38::a

;; Query time: 44 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Wed Sep 18 12:23:14 -03 2024
;; MSG SIZE  rcvd: 315
```

Hacemos una consulta de los registros NS del dominio google.com para saber cuáles son los servidores DNS autoritativos de ese dominio

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

; <<>> DiG 9.16.27-Debian <<>> google.com @ns1.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62348
;; 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:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             300     IN      A       142.251.134.78

;; Query time: 44 msec
;; SERVER: 216.239.32.10#53(216.239.32.10)
;; WHEN: Wed Sep 18 12:27:31 -03 2024
;; MSG SIZE  rcvd: 55
```

Usamos uno de los servidores DNS autoritativos y obtenemos la respuesta autoritativa

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?**

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

; <<>> DiG 9.16.27-Debian <<>> www.info.unlp.edu.ar @ns1.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 62820
;; 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: 48 msec
;; SERVER: 216.239.32.10#53(216.239.32.10)
;; WHEN: Wed Sep 18 12:30:55 -03 2024
;; MSG SIZE  rcvd: 49
```

- Al hacer la consulta recibimos el código de status **REFUSED**, esto significa que el servidor DNS al que se consultó rechazó la petición. Un servidor DNS puede rechazar una petición por varios motivos
    - **Restricciones de la Configuración del Servidor**

        - El servidor DNS puede estar configurado para rechazar ciertas consultas, especialmente si provienen de fuentes no autorizadas o desconocidas.
    - **Políticas de Seguridad**
        - Algunos servidores DNS tienen políticas de seguridad que limitan las consultas a ciertos tipos de registros o a clientes específicos.
    - **Problemas de Configuración**
        - Puede haber un problema en la configuración del servidor DNS que impide que responda a las consultas adecuadamente.
    - **Protección contra Ataques**
        - Los servidores DNS a veces están configurados para protegerse contra ciertos tipos de ataques, como ataques de amplificación DNS, y pueden rechazar consultas sospechosas.

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

; <<>> DiG 9.16.27-Debian <<>> www.info.unlp.edu.ar @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12912
;; 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.   161     IN      A       163.10.5.71

;; Query time: 28 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Sep 18 12:38:36 -03 2024
;; MSG SIZE  rcvd: 65
```

- La consulta al servidor **8.8.8.8** no genera error ya que este servidor es un **Open Name Server** que funciona como servidor local para cualquier cliente.

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 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 AAAA 2800:3f0:4003:c00::1a
srv00.ejemplo.com. 272 IN A 74.125.133.26
srv00.ejemplo.com. 240 IN AAAA 2a00:1450:400c:c07::1b

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

- Completado con rojo.

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

- No es una respuesta autoritativa ya que no está el **flag aa.** Le podría preguntar a cualquiera de estos servidores para obtener una respuesta autoritativa
    - **ss00.ejemplo.com.**
    - **ss01.ejemplo.com.**
    - **ss02.ejemplo.com.**
    - **ss03.ejemplo.com.**

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

- Sabemos que ambas consulta y respuesta fueron recursivas ya que están presentes los **flags rd y ra.**

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

- **Los valores 10 y 5** representan la prioridad de cada servidor de correo. Cuanto más bajo sea el número, mayor será la prioridad del servidor. En este caso, **srv00.ejemplo.com** con **prioridad 5** es el servidor principal, y **srv01.ejemplo.com** con **prioridad 10** es el secundario.