Práctica 3

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

   El servicio DNS (Domain Name System) funciona como un sistema distribuido de forma jerárquica, a través de dominios, sub-dominios y nombres finales, con un conjunto de servidores a lo largo del mundo. Cada servidor tiene la responsabilidad de parte dentro de la jerarquía de nombres.

   Su objetivo principal es el de traducir nombres de dominio a direcciones IP para lograr una abstracción de las direcciones de red utilizadas internamente por los protocolos, permitiendo así ubicar a un dispositivo por su nombre sin importar cuál es su dirección IP actual, haciendo que no sea necesario para las personas recordar la dirección IP.

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 los Top 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 dominoions. 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?**

   - En una consulta recursiva, el servidor DNS consultado se encarga de resolver toda la consulta en nombre del cliente, realizando consultas adicionales si es necesario y proporcionando una respuesta completa.
   - En una consulta iterativa, el servidor DNS consultado proporciona una respuesta parcial con información sobre dónde buscar más detalles, y el cliente debe seguir el proceso de consulta paso a paso para obtener la respuesta completa.

5. **¿Qué es el resolver?**

   El Resolver se lo podría considerar como un agente encargado de resolver los nombres a solicitud del cliente. 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 :** mapean un nombre de domino a una dirección IPv4. Pueden existir varios registros (A) con el mismo nombre

   b) **NS:** indican los servidores de nombre autoritativos para una sub-dominio. A partir de esto, se puede lograr una delegación de sub-dominios. No hay prioridad, todos los servidores tienen la misma precedencia.

   c) **MX:** indican para un nombre de dominio cuáles son los servidores de mail SMTP encargados de recibir los mensajes para ese dominio. El servidor de mail SMTP que envía el mensaje deberá consultar, vía el servicio de DNS, cuáles son los servidores SMTP receptores para el dominio dado. Se asignan prioridades para servidores del mismo dominio. Se puede también lograr un balance de cargas entre distintos servidores SMTP

   d) **CNAME:** mapean un nombre de domino a otros nombres. Hacen el mapeo del alias de un dominio su nombre canónico (vendría a ser el nombre original)

   e) **PTR:** mapean direcciones IP a nombres de dominio. Son el inverso de los registros (A). Trabajan en el dominio especial in-addr.arpa

   f) **SOA:** se utilizan para proporcionar información autoritaria sobre una zona de dominio, lo que incluye información sobre la administración y configuración de esa zona. Solo se admite un registro SOA por zona. Permite que servidores autoritarios de la misma zona se puedan sincronizar.

   g) **AAAA:** mapean un nombre de domino a una dirección IPv6.

   h) **TXT:** Son registros que mapean de un nombre de domino a información extra asociada con el equipo que tiene dicho nombre, por ejemplo pueden indicar finalidad, usuarios, etc. No son utilizados habitualmente. Se los puede ver en uso asociando una clave publica, utilizando por ejemplo IPSec con un esquema de Opportunistic Encryption

   i) **SRV:** se utilizan para asociar servicios o recursos a nombres de dominio.

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 los secundarios (o esclavos). ¿Cuál es la razón de que sea así?**

   La razón de que sea así es para simplificar la configuración de los servidores autoritarios, evitando configurar a cada servidor de un mismo dominio de forma independiente. En lugar de esto, se configura aquel que es primario y el resto de los servidores se sincronizan con este. Esto a su vez garantizar la consistencia de los datos DNS.

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)**

    Debo delegarle la administración del dominio. Para ello transfiero la autoridad del subdominio "redes.unlp.edu.ar" al administrador de la Facultad de Redes. Hay que configurar registros NS que apunten a los servidores DNS de la Facultad de Redes como servidores autoritarios para ese subdominio. Para hacerlo, el administrador de la Facultad de Redes debe proporcionarle los nombres y direcciones IP de los servidores DNS que desea utiliza

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:**

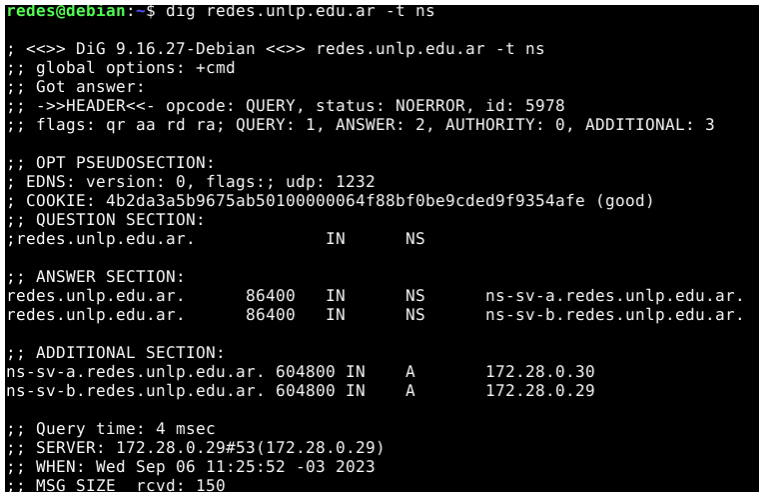
```
redes@debian:~$ dig www.redes.unlp.edu.ar

; <<>> DiG 9.16.27-Debian <<>> www.redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 800
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a19e18b7d8fc2c560100000064f9b2d9bd490db3a81d20ad (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: Thu Sep 07 08:24:09 -03 2023
;; MSG SIZE  rcvd: 94
```

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

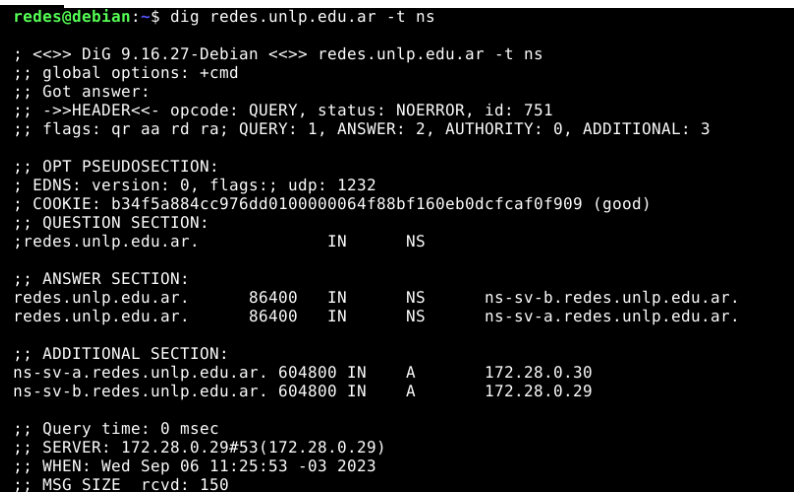
```
redes@debian:~$ dig redes.unlp.edu.ar -t ns

; <<>> DiG 9.16.27-Debian <<>> redes.unlp.edu.ar -t ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21858
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d0a90ff8989ab1580100000064f88bb4e370e41403fa85c0 (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 06 11:24:52 -03 2023
;; MSG SIZE  rcvd: 150
```

Son ns-sv-a.redes.unlp.edu.ar y ns-sv-b.redes.unlp.edu.ar

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



```
redes@debian:~$ dig redes.unlp.edu.ar -t ns

; <<>> DiG 9.16.27-Debian <<>> redes.unlp.edu.ar -t ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5978
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 4b2da3a5b9675ab50100000064f88bf0be9cded9f9354afe (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 06 11:25:52 -03 2023
;; MSG SIZE  rcvd: 150
```



```
redes@debian:~$ dig redes.unlp.edu.ar -t ns

; <<>> DiG 9.16.27-Debian <<>> redes.unlp.edu.ar -t ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 751
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b34f5a884cc976dd0100000064f88bf160eb0dcfcaf0f909 (good)
;; QUESTION SECTION:
;redes.unlp.edu.ar.             IN      NS

;; ANSWER SECTION:
redes.unlp.edu.ar.      86400   IN      NS      ns-sv-b.redes.unlp.edu.ar.
redes.unlp.edu.ar.      86400   IN      NS      ns-sv-a.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 06 11:25:53 -03 2023
;; MSG SIZE  rcvd: 150
```

Se puede observar:

- Cambia el ID de la consulta
- Cambia COOKIE
- El TTL del NS y de A es el mismo
- Cambia el valor de When
- También cambia el Query time

d. 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, para eso se debe hacer:
`dig redes.unlp.edu.ar -t soa`

e. Consulte por el registro SOA del dominio y responda

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

Si, se puede determinar

```
redes@debian:~$ dig redes.unlp.edu.ar -t soa

; <<>> DiG 9.16.27-Debian <<>> redes.unlp.edu.ar -t soa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35117
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 95b69675be4d86c00100000064f88d26f7ddc93d24f76648 (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.re
es.unlp.edu.ar. 2020031700 604800 86400 2419200 86400

;; Query time: 4 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Wed Sep 06 11:31:02 -03 2023
;; MSG SIZE  rcvd: 123
```

El root 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 numero de serie es “2020031700”.
Hay dos métodos comunes para actualizar el campo SERIAL del registro SOA de zona:

- El primer método es comenzar el número de serie en 1 y aumentarlo en cada cambio
- El segundo es el siguiente utilizando formato *YYYYMMDDSS* que permite saber en qué fecha se creó la actualización. Con cada cambio en un mismo día, el número de versión (SS) aumenta en una cifra. Al día siguiente cambia el número de serie y el número de versión vuelve a ponerse a 00.

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

El segundo campo tiene el valor “604800”.
Se trata del campo “Refresh” que indica cada cuanto tiempo los servidores secundarios deben refrescar desde el primario. La RFC-1912 recomienda entre 1200 a 43200 segundos.

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

Tiene el valor “86400”. Esto quiere decir que si se preguntó por un valor en donde el servidor autoritativo respondió que no lo tiene el cliente no volverá a preguntar por ese nombre de dominio durante 86400 segundos (24 horas) después de recibir la respuesta negativa del servidor autoritativo.

f. 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 saludos.redes.unlp.edu.ar -t TXT

; <<>> DiG 9.16.27-Debian <<>> saludos.redes.unlp.edu.ar -t TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 64961
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c223be9f78f52bd10100000064f8923e8c35cf6b4677dd18 (good)
;; QUESTION SECTION:
;saludos.redes.unlp.edu.ar.     IN      TXT

;; 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
```

Ninguno. Este registro es usado para mapear el nombre de domino a información extra asociada con el equipo que tiene dicho nombre

g. 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.
 2020031700 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.
 2020031700 604800 86400 2419200 86400
;; Query time: 0 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Wed Sep 06 12:13:54 -03 2023
;; XFR size: 17 records (messages 1, bytes 441)
```

Si el servidor DNS autoritativo para "redes.unlp.edu.ar" está configurado para permitir la transferencia de zona desde la dirección IP desde la cual se realiza la consulta, entonces se recibirán todos los registros DNS asociados con ese dominio. De lo contrario, se mostrará un mensaje de error indicando que la transferencia de zona no está permitida.

En este caso, se muestran los registros.

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

Es el TTL. Este indica cuánto tiempo debe almacenarse en caché una pieza de información antes de que deba considerarse obsoleta o caduca.

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?**

Observo cuatro registros NS debido a que se están obteniendo todos los registros del dominio "redes.unlp.edu.ar", que incluyen los registros que indican a donde delegar cuando se trata del subdominio “practica.redes.unlp.edu.ar” (se está delegando a los servidores "ns1.practica.redes.unlp.edu.ar." y "ns2.practica.redes.unlp.edu.ar.")

h. **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 www.redes.unlp.edu.ar A

; <<>> DiG 9.16.27-Debian <<>> www.redes.unlp.edu.ar A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9585
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b93c4df9f9fff8d50100000064f9b3b44b61029ea6c29fe0 (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: 4 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Thu Sep 07 08:27:48 -03 2023
;; MSG SIZE  rcvd: 94
```

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

; <<>> DiG 9.16.27-Debian <<>> www.practica.redes.unlp.edu.ar A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63322
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 1856079cfae6569c0100000064f9b3bf1e89be0d16c2533d (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: 1256 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Thu Sep 07 08:27:59 -03 2023
;; MSG SIZE  rcvd: 103
```

El TTL de practica.redes.unlp.edu.ar es menor que el de redes.unlp.edu.ar y ademes el de practica va disminuyendo a medida que se sigue consultando. Esto ocurre porque redes.unlp.edu.ar es el autoritativo (se puede ver en el flag aa) y practica.redes.unlp.edu.ar debe actualizar su información.

i. **Consulte por el registro A de www.practica2.redes.unlp.edu.ar. ¿Obtuvo alguna respuesta? Investigue sobre los codigos de respuesta de DNS. ¿Para qué son utilizados los mensajes NXDOMAIN y NOERROR?**

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

; <<>> DiG 9.16.27-Debian <<>> practica2.redes.unlp.edu.ar a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 45155
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: fada3d2aec8d4a590100000064f89cab919c6ad3438bf878 (good)
;; QUESTION SECTION:
;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: 4 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Wed Sep 06 12:37:15 -03 2023
;; MSG SIZE  rcvd: 133
```

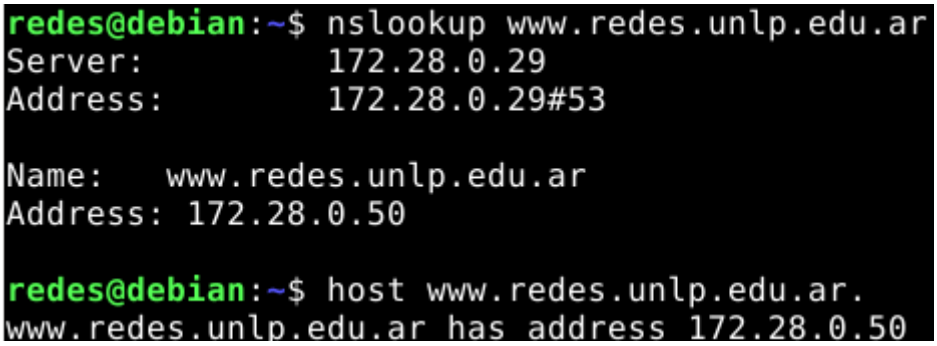
Se obtiene una respuesta con el estado “NXDOMAIN”.
El mensaje NXDOMAIN se utiliza para informar que no se pudo encontrar el nombre de dominio consultado, mientras que el mensaje NOERROR se utiliza para indicar que la resolución de nombres se realizó con éxito y se encontró una respuesta válida.

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

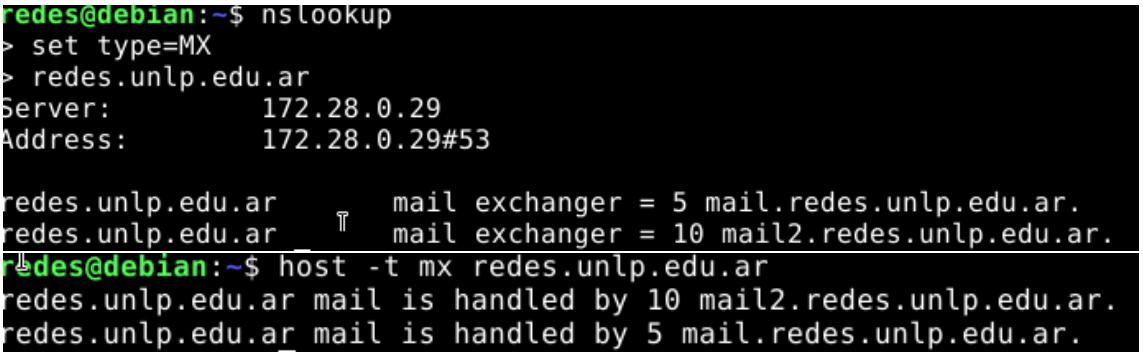
Nslookup es un programa utilizado para saber si el DNS está resolviendo correctamente los nombres y las IPs. Se utiliza con el comando nslookup, que funciona tanto en Windows como en UNIX para obtener la dirección IP conociendo el nombre, y viceversa

El comando host es una utilidad simple para realizar búsquedas de DNS. 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.

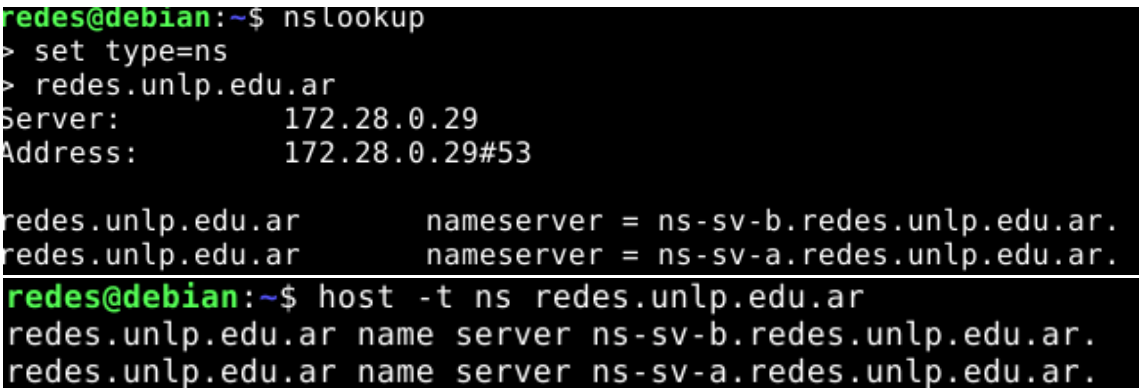
- **Dirección IP de www.redes.unlp.edu.ar.**



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



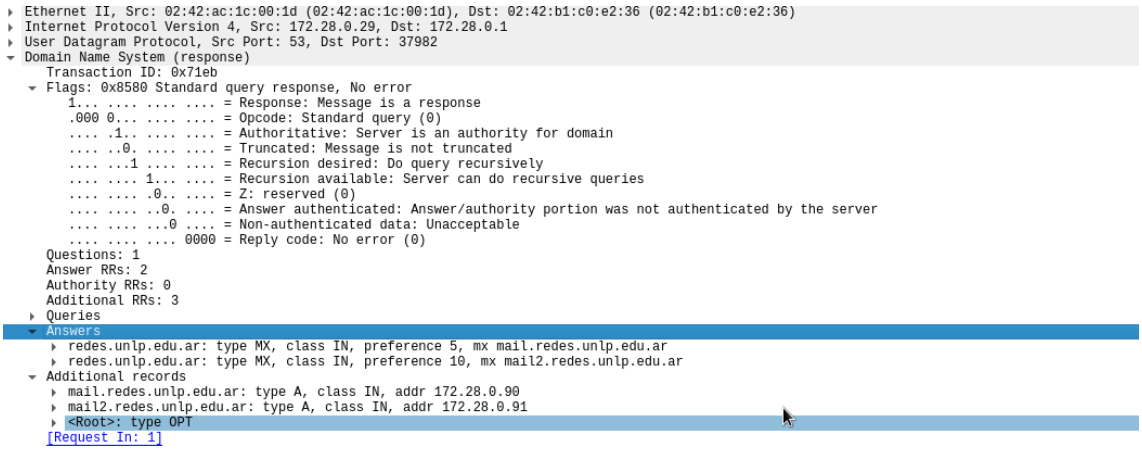
- **Servidores de DNS del dominio redes.unlp.edu.ar**



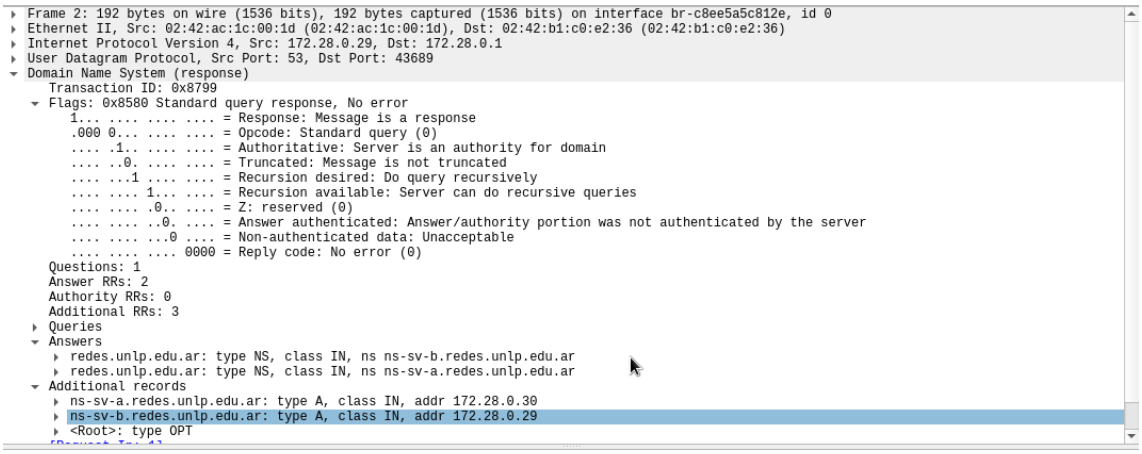
13. **¿Qué función cumple en Linux/Unix el archivo /etc/hosts o en Windows el archivo \WINDOWS\system32\drivers\etc\hosts?**

    La función que cumplen es mapear nombres de host a direcciones IP locales sin la necesidad de consultar un servidor DNS externo. Originalmente, se utilizaba principalmente para realizar la resolución de nombres de host a direcciones IP en una red antes de la existencia generalizada de servidores DNS

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.**




```
<<>> DiG 9.16.27-Debian <<>> redes.unlp.edu.ar -t mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29163
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a8e4afa2799ebaee0100000064f8a58919c9d6f6c75cce3d (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
```




```
; <<>> DiG 9.16.27-Debian <<>> redes.unlp.edu.ar -t ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34713
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 1b609dc159e6b4e00100000064f8a608f78d3da7f264fed8 (good)
;; QUESTION SECTION:
;redes.unlp.edu.ar.             IN      NS

;; ANSWER SECTION:
redes.unlp.edu.ar.      86400   IN      NS      ns-sv-b.redes.unlp.edu.ar.
redes.unlp.edu.ar.      86400   IN      NS      ns-sv-a.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 06 13:17:12 -03 2023
;; MSG SIZE  rcvd: 150
```

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?**

       Realiza consultas recursivas a su servidor DNS.

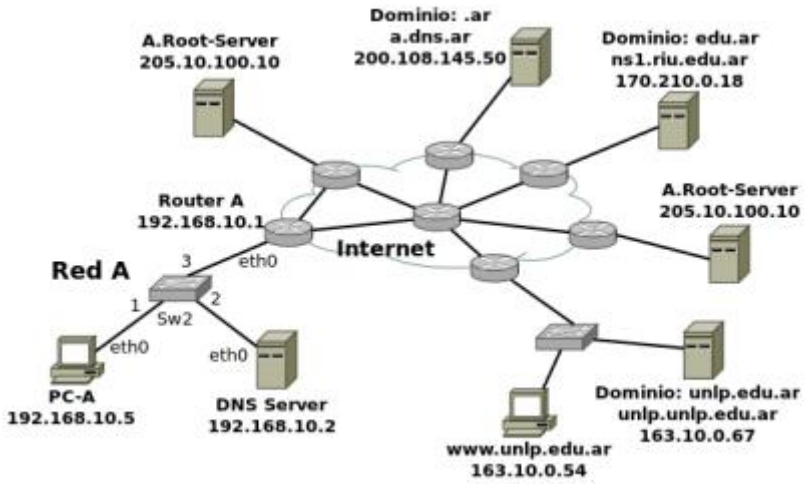
    b. **¿Qué tipo de consultas (iterativas o recursivas) realiza el servidor de DNS para resolver requerimientos de usuario como el anterior? ¿A quién le realiza estas consultas?**

       Realiza consultas iterativas para resolver requerimientos de un usuario. Realiza las consultas dentro de la jerarquía de nombres, comenzado por el servidor raíz, hasta llegar al servidor autoritativo para el dominio solicitado.

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

Se podría navegar pero se tornaría difícil y limitado puesto que para acceder a un sitio web se debería conocer la dirección IP.

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.

1. PC-A (192.168.10.5) consulta primero a su resolver privado sobre la IP del host www.unlp.edu.ar.
2. Si no puede obtener una respuesta (no esta cacheada) el resolver primario delega al DNS Server (192.168.10.2).
3. Si este no puede obtenerla de su cache entonces el DNS Server consultara de forma iterativa al A.Root-Server (205.10.100.10) más cercano.
3. Este le responderá (también de forma iterativa) con el NS (y el IP) de .ar, a.dns.ar (200.108.145.50).
4. DNS Server consultara (de forma iterativa) a a.dns.ar.
5. Este le responderá con los NS de .edu.ar, ns1.riu.edu.ar (170.210.0.18)
6. DNS Server consultara a ns1.riu.edu.ar
7. Este le responderá con el NS del servidor autoritativo del dominio unlp.edu.ar, unlp.unlp.edu.ar (163.10.0.67)
8. DNS Server consultará a unlp.unlp.edu.ar que le responderá con la IP de www.unlp.edu.ar (163.10.0.54)
9. El DNS Server cacheara la respuesta y le responderá al resolver de la PC-A con la IP de www.unlp.edu.ar (el resolver también la cacheara)

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

Con el resolver privado de PC-A y el DNS Server es recursiva. Entre DNS Server y los servidores de la jerarquía de nombres es iterativa.

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

Para saber eso se debe hacer

```
dig google.com ns
```

```
; <<>> DiG 9.16.27-Debian <<>> google.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21181
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 552f22da15d3f5610100000064f8abb1dd80bc04d4db5121 (good)
;; QUESTION SECTION:
;google.com.                    IN      NS

;; ANSWER SECTION:
google.com.             168872  IN      NS      ns1.google.com.
google.com.             168872  IN      NS      ns3.google.com.
google.com.             168872  IN      NS      ns2.google.com.
google.com.             168872  IN      NS      ns4.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         168872  IN      A       216.239.32.10
ns2.google.com.         345433  IN      A       216.239.34.10
ns3.google.com.         168872  IN      A       216.239.36.10
ns4.google.com.         168872  IN      A       216.239.38.10
ns1.google.com.         168872  IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         345433  IN      AAAA    2001:4860:4802:34::a
ns3.google.com.         168872  IN      AAAA    2001:4860:4802:36::a
ns4.google.com.         168872  IN      AAAA    2001:4860:4802:38::a
```

```
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: 30725
;; 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: 40 msec
;; SERVER: 216.239.32.10#53(216.239.32.10)
;; WHEN: Wed Sep 06 13:45:38 -03 2023
;; MSG SIZE  rcvd: 55
```

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 consulto al servidor elegido en el paso anterior:

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

; <<>> DiG 9.16.27-Debian <<>> info.unlp.edu.ar @ns1.google.com.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 52343
;; 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:
;info.unlp.edu.ar.              IN      A

;; Query time: 44 msec
;; SERVER: 216.239.32.10#53(216.239.32.10)
;; WHEN: Wed Sep 06 13:46:49 -03 2023
;; MSG SIZE  rcvd: 45
```

Se obtiene el status “Refused” este status quiere decir que el servidor DNS consultado ha denegado explícitamente la solicitud y no proporcionará la información solicitada, en este, porque no la tiene en sus registros la IP de www.info.unlp.edu.ar.

Si consulto a 8.8.8.8

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

; <<>> DiG 9.16.27-Debian <<>> info.unlp.edu.ar @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52329
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

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

;; Query time: 92 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Sep 06 13:48:29 -03 2023
;; MSG SIZE  rcvd: 61
```

Esto se debe a que 8.8.8.8 es un servidor local

Ejercicio de parcial

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

```
1 ;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4,
ADDITIONAL: 4
2
```

```
3 ;; QUESTION SECTION:
4 ;ejemplo.com. IN MX
5
6 ;; ANSWER SECTION:
7 ejemplo.com. 1634 IN MX 10 srv01.ejemplo.com.
8 ejemplo.com. 1634 IN MX 5 srv00.ejemplo.com.
9
10 ;; AUTHORITY SECTION:
11 ejemplo.com. 92354 IN MX ss00.ejemplo.com.
12 ejemplo.com. 92354 IN MX ss02.ejemplo.com.
13 ejemplo.com. 92354 IN MX ss01.ejemplo.com.
14 ejemplo.com. 92354 IN MX ss03.ejemplo.com.
15
16 ;; ADDITIONAL SECTION:
17 srv01.ejemplo.com. 272 IN A 64.233.186.26
18 srv01.ejemplo.com. 240 IN AAAA 2800:3f0:4003:c00::1a
19 rv00.ejemplo.com. 272 IN A 74.125.133.26
20 rv00.ejemplo.com. 240 IN AAAA 2a00:1450:400c:c07::1b
```

- **Complete las líneas donde aparece __ con el registro correcto.**
- **¿Es una respuesta autoritativa? En caso de no serlo, ¿a qué servidor le preguntaría para obtener una respuesta autoritativa?**

  No, no es una respuesta autoritativa puesto que no esta el flag aa. Para que sea una respuesta autoritativa podría preguntarle a ss00.ejemplo.com (uno de los servidores autoritativos ya que sale en authority section)

- **¿La consulta fue recursiva? ¿Y la respuesta?**

  La consulta fue recursiva, y eso se puede saber mediante el flag rd. La respuesta también fue recursiva y se puede saber mediante el flag ra

- **¿Qué representan los valores 10 y 5 en las líneas 7 y 8.**

  Representan la prioridad. Indican el orden en el que se deben entregar los correos electrónicos a los servidores de correo asociados al dominio ejemplo.com. Esto quiere decir que los correos electrónicos se entregarán primero al servidor con la prioridad más baja y si no está disponible, se intentará entregar al servidor con la siguiente prioridad más baja.