Práctica 3

1) El DNS (Domain Name System) es un sistema cuya función principal es traducir nombres de dominio legibles por humanos (como www.google.com) a direcciones IP (como 142.250.78.68), que son las que realmente utilizan los dispositivos para comunicarse en Internet.
    1. Tu navegador primero consulta al **sistema operativo** para ver si la dirección IP de `www.ejemplo.com` ya está en caché.
    2. El sistema operativo envía la consulta al **servidor DNS local** (también llamado **resolvedor recursivo**), que normalmente lo proporciona tu proveedor de Internet (ISP).
    3. Si el servidor local no tiene la respuesta en caché, sigue una serie de pasos jerárquicos:
        a. Consulta al servidor raíz (root DNS servers)
            - Existen 13 grupos de servidores raíz en el mundo.
            - El servidor raíz no sabe la IP de www.ejemplo.com, pero sabe a qué servidor TLD (.com) debe preguntarse.
        b. Consulta al servidor TLD (Top-Level Domain)
            - Por ejemplo, para www.ejemplo.com, el TLD sería .com.
            - El servidor TLD tampoco tiene la IP final, pero sabe a qué servidor autoritativo apuntar.
        c. Consulta al servidor autoritativo
            - Este sí tiene la IP exacta del dominio www.ejemplo.com.
            - El resolvedor local recibe la respuesta final con la IP.
    4. El resolvedor local devuelve la IP al sistema operativo, que la pasa al navegador.
    5. El navegador puede ahora **establecer la conexión** con el servidor web.
2) **Root Server:** Un Root Server (servidor raíz del DNS) es el punto más alto en la jerarquía del sistema DNS. Es el primer lugar al que se acude cuando se necesita resolver un nombre de dominio completo y no se tiene información en caché. Cuando el servidor DNS local (resolvedor) no conoce la IP de un dominio, realiza una consulta al root server. Este no conoce la IP final del dominio, pero sí sabe qué servidor TLD (Top-Level Domain) debe consultarse.
   Existen 13 conjuntos de root servers, identificados por letras: de la A a la M.
   Cada uno de estos servidores está replicado en muchos lugares del mundo usando una tecnología llamada **Anycast**, lo que permite que múltiples copias respondan a la misma IP.
   Generic Top Level Domain: Un gTLD (Generic Top-Level Domain) es un dominio de nivel superior genérico en el sistema DNS. Son las extensiones más conocidas de los dominios, como:
    - `.com` (comercial)
    - `.org` (organización)
    - `.net` (red)
    - `.edu` (educación)
    - `.gov` (gobierno)

3) Una respuesta autoritativa es una respuesta que proviene directamente del servidor DNS que tiene autoridad sobre el nombre de dominio consultado.
   Es decir, es la fuente oficial de información sobre ese dominio.
   Una respuesta es autoritativa cuando:
   - Proviene del servidor autoritativo (el que gestiona el dominio directamente).
   - La respuesta no viene de caché, ni de otro servidor que simplemente pasó la información.

4) Una **consulta recursiva** es cuando el cliente (por ejemplo, tu PC o tu navegador) pide una respuesta completa a un servidor DNS y espera que este haga todo el trabajo para obtener la IP final. La hace un cliente (PC, smartphone, navegador) al servidor DNS local. El servidor debe resolver completamente la consulta, incluso si eso implica consultar a otros servidores (raíz, TLD, autoritativo). El cliente no participa del proceso intermedio.
   Una **consulta iterativa** es cuando un servidor DNS pregunta a otro servidor y este no responde con la IP, sino que devuelve una referencia a otro servidor más cercano a la respuesta.Suele ocurrir entre servidores DNS (por ejemplo: local → raíz → TLD → autoritativo). Cada servidor responde con la mejor información que tiene, pero no hace la resolución completa por sí mismo. El servidor que inició la consulta va siguiendo las pistas.

5) **Resolver:** Un resolver es un software cliente del sistema DNS, encargado de iniciar las consultas DNS en nombre de aplicaciones como navegadores web, clientes de correo, etc. Normalmente está en tu computadora, teléfono o dispositivo cliente. Se comunica con un servidor DNS local (también llamado resolvedor recursivo).

6)
   a. **A:** A (Address), Asocia un nombre de dominio a una dirección IPv4. Es uno de los registros más comunes. Ej: www.ejemplo.com → 192.0.2.1
   b. **MX:** MX (Mail Exchange), Define los servidores de correo responsables de recibir emails para un dominio. Puede haber múltiples con diferentes prioridades. Ej: correo.ejemplo.com
   c. **PTR:** PTR (Pointer), Se usa para resolución inversa: traduce una IP a un nombre de dominio. Es lo contrario al registro A. Ej: 192.0.2.1 → www.ejemplo.com
   d. **AAAA:** AAAA, Similar al registro A, pero para direcciones IPv6. Ej: www.ejemplo.com → 2001:db8::1
   e. **SRV:** SRV (Service), Define servicios específicos disponibles en un dominio, como SIP o XMPP, con información sobre puerto y prioridad. Ej: _sip._tcp.ejemplo.com
   f. **NS:** NS (Name Server), Indica los servidores de nombres autoritativos para un dominio. Esencial para delegar autoridad de subdominios. Ej: ns1.ejemplo.com
   g. **CNAME:** CNAME (Canonical Name), Asocia un alias de nombre a un nombre canónico. Útil para redirigir múltiples nombres a un solo servidor. Ej: blog.ejemplo.com → www.ejemplo.com

h. **SOA:** SOA (Start of Authority), Proporciona información sobre la zona DNS, como el servidor principal, el correo del administrador, número de serie, etc. Ej: Es el primer registro de una zona.
i. **TXT:** TXT (Text), Permite incluir información arbitraria en texto, muy usado para configuraciones como SPF, verificación de dominios, etc. Ej: v=spf1 include:_spf.google.com ~all

7) Para garantizar disponibilidad, tolerancia a fallos, redundancia y rendimiento.
    a. Si un servidor DNS cae (por mantenimiento, ataque, o falla de red), otro servidor puede responder. Esto asegura que el dominio siga siendo accesible, incluso si hay problemas.
    b. Los servidores se ubican en diferentes lugares del mundo. Esto permite que las consultas se respondan desde el servidor más cercano o más rápido, reduciendo la latencia.
    c. DNS es uno de los primeros pasos de acceso a un sitio. Tener varios servidores ayuda a repartir la carga de consultas. Esto evita cuellos de botella y mejora el tiempo de respuesta.
    d. Con múltiples servidores, es posible repartir las consultas DNS entre ellos (round-robin o mediante cualquier cast). Esto evita sobrecargar un único servidor.
    e. El estándar de DNS (RFC 1034/1035) recomienda al menos dos servidores autoritativos por dominio. La mayoría de los registradores de dominios exigen esto como requisito mínimo técnico.

8) Para centralizar la gestión de los datos DNS en un solo lugar (el servidor primario) y permitir que los secundarios mantengan copias sincronizadas para redundancia, carga y disponibilidad.
    El servidor primario (master) es el único que tiene autoridad de escritura sobre la zona DNS.
    Los servidores secundarios (slaves) hacen copias automáticas del archivo de zona mediante un proceso llamado transferencia de zona (zone transfer). Cuando se hace un cambio en el primario, los secundarios se actualizan automáticamente usando el campo Serial del registro SOA (Start of Authority).

9) **Zone Transfer:** Es el mecanismo mediante el cual un servidor DNS secundario obtiene una copia actualizada del archivo de zona desde el servidor primario. Sincroniza los datos DNS entre el servidor primario (maestro) y los secundarios (esclavos), para que todos los servidores autoritativos tengan la misma información y respondan igual a las consultas.
    1. El servidor secundario consulta al primario y revisa el número de serie del registro SOA.
    2. Si el número ha cambiado, significa que el archivo de zona fue actualizado.
    3. Entonces, el secundario solicita una transferencia de zona para copiar el archivo completo o solo los cambios.

10) La **delegación de un subdominio** en DNS consiste en transferir la autoridad de un subdominio (en este caso, redes.unlp.edu.ar) a un conjunto de servidores DNS que serán responsables de resolver las consultas para ese subdominio. El administrador

de redes.unlp.edu.ar podrá gestionar su propio dominio sin necesidad de intervención en el dominio principal (unlp.edu.ar).
Pasos:

1. Crear los servidores DNS para el subdominio redes.unlp.edu.ar:
    - El administrador de la Facultad de Redes necesita configurar sus propios servidores DNS para que gestionen el subdominio. Supongamos que los servidores de la Facultad de Redes son:
        - ns1.redes.unlp.edu.ar
        - ns2.redes.unlp.edu.ar
2. Configurar los servidores DNS en el dominio principal (unlp.edu.ar):
    - Como administrador del dominio unlp.edu.ar, debes delegar el subdominio redes.unlp.edu.ar a esos servidores DNS.
    - Para hacerlo, deberás agregar registros NS en el dominio principal unlp.edu.ar.
3. Agregar los registros NS y A:
    - Registros NS en el dominio unlp.edu.ar que apunten a los servidores de nombres de la Facultad de Redes.
    - Registros A para asegurar que los servidores de nombres (ns1.redes.unlp.edu.ar y ns2.redes.unlp.edu.ar) sean accesibles (esto también podría implicar crear registros A para los servidores ns1 y ns2).

Ej:

```
; Delegación para la Facultad de Redes
redes.unlp.edu.ar.  IN  NS  ns1.redes.unlp.edu.ar.
redes.unlp.edu.ar.  IN  NS  ns2.redes.unlp.edu.ar.

; Asegúrate de que los servidores DNS sean accesibles
ns1.redes.unlp.edu.ar.  IN  A  192.168.1.1
ns2.redes.unlp.edu.ar.  IN  A  192.168.1.2
```

11)

a.

i) Tanto la solicitud como la respuesta fueron recursivas, lo indica los flags que se activaron rd(recursion desired) y ra(recursion available). Básicamente se solicita una respuesta recursiva y el servidor acepta otorgarla.

ii) Fue una respuesta autoritativa ya que se activó el flag aa(authoritative answer).La respuesta proviene de un servidor DNS que es autoritativo para el dominio consultado. Es decir, el servidor es dueño de la zona (tiene la información "oficial") y está respondiendo directamente desde su base de datos, no porque consultó a otros servidores.

iii) 172.28.0.29, lo se porque hay una línea que pone SERVER:

b. [dig MX redes.unlp.edu.ar] Los servidores de correo del dominio son: mail.redes.unlp.edu.ar y mail2.redes.unlp.edu.ar. Los números entre MX y el nombre del servidor indican la prioridad, 5 para el primero (mayor prioridad) y 10 para el segundo. En caso de mandar un mail a redes.unlp.edu.ar intentará

entregarse al de mayor prioridad y, en caso de no estar disponible, se entregará al segundo.

c. [dig NS redes.unlp.edu.ar] Los servidores DNS son: ns-sv-b.redes.unlp.edu.ar. y ns-sv-a.redes.unlp.edu.ar.

d. Cambia la variable COOKIE y el id en el HEADER. El id es un identificador único de la consulta DNS, generado por el cliente. Se usa para emparejar las respuestas con sus respectivas consultas, por lo tanto cada vez que se realice una consulta se genera un nuevo id. En el caso de la cookie, la misma tiene dos partes:
   Ej:
   - 59b12f66cf13b248 <- client cookie (8 bytes) Es un identificador pseudoaleatorio basado en tu dirección IP y posiblemente un timestamp o secreto local. (generada por el cliente)
   - 0100000067fd1b1d86ea846ba88584a5 <- server cookie (variable, aquí 16 bytes) Generada por el servidor DNS en base a tu client cookie y tu IP. Si se realizan más consultas al mismo servidor, y él recuerda tu cookie anterior, puede enviarte la misma server cookie.

e. No hay información sobre quién es primario.

f. [dig SOA redes.unlp.edu.ar]
   i) Sí, es ns-sv-b.redes.unlp.edu.ar. ya que solo aparece él.
   ii) El número de serie es 2020031700 -> YYYY MM DD NN. Conviene actualizarlo cuando el servidor reciba cambios sustanciales.
   iii) Sería el refresh tiempo para que el server secundario espere hasta volver de consultar al primario (refrescandose a sí mismos). 604800.
   iv) Time to live (TTL), de caché negativa simboliza el tiempo durante el cual el servidor guardará información sobre una consulta de un nombre que no existe para retornar el error.

g. [dig TXT saludo.redes.unlp.edu.ar] Dice “HOLA”

h. [dig AXFR redes.unlp.edu.ar]

```
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 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: 8 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Mon Apr 14 11:46:34 -03 2025
;; XFR size: 17 records (messages 1, bytes 441)
```

i. TTL, tiempo que debe almacenarse en caché una pieza de información antes de que este caducada.
ii. 4, ya que se incluyen los registros que indican a donde delegar cuando se trata el subdominio practica.redes.unlp.edu.ar (delegando a “ns*.practica.redes.unlp.edu.ar).

i. www.practica.redes.unlp.edu.ar. va bajando su TTL a medida que se consulta y es menor que el de www.redes.unlp.edu.ar, esto se debe a que www.redes.unlp.edu.ar tiene la flag aa (autoritativo) y el otro no.

j. Si, además viene con el mensaje NXDOMAIN.
   - **NXDOMAIN** (Non-Existent Domain): Este mensaje indica que el dominio solicitado no existe. Por ejemplo, si alguien intenta acceder a un sitio web que no tiene un registro DNS, el servidor DNS responderá con NXDOMAIN para informar que no hay coincidencias.
   - **NOERROR**: Este mensaje se utiliza cuando la consulta DNS se resuelve correctamente y se encuentra un registro correspondiente al dominio solicitado. Esto significa que el dominio existe y se devuelve la información pertinente, como la dirección IP asociada.

12) **nslookup (Name Server Lookup):** Herramienta de diagnóstico de red. Permite consultar servidores DNS manualmente para obtener registros de nombres de dominio. Interactivo o por línea de comando.
host: Comando más simple y directo. También consulta registros DNS, pero con una sintaxis más amigable para scripts y resultados más legibles.

```
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
```

```
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 = 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 5 mail.redes.unlp.edu.ar.
redes.unlp.edu.ar mail is handled by 10 mail2.redes.unlp.edu.ar.
```

```
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.

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) El archivo hosts tanto en Linux/Unix (/etc/hosts) como en Windows (C:\Windows\System32\drivers\etc\hosts) cumple la función de un mapeo local entre nombres de dominio y direcciones IP. Es una forma de resolver nombres sin consultar un servidor DNS.
    Cuando una aplicación (como un navegador o ping) necesita convertir un nombre de dominio (como redes.unlp.edu.ar) en una dirección IP, el sistema operativo sigue este orden:
    - Primero revisa el archivo hosts.
    - Si no encuentra el nombre ahí, recién consulta al servidor DNS configurado.

14) Respuesta de la Consulta NS:

```
▸ Frame 1: 100 bytes on wire (800 bits), 100 bytes captur
▸ Ethernet II, Src: 02:42:c0:47:e0:78 (02:42:c0:47:e0:78)
▸ Internet Protocol Version 4, Src: 172.28.0.1, Dst: 172.
▸ User Datagram Protocol, Src Port: 43315, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x22f9
  ▸ Flags: 0x0120 Standard query
    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
    [Response In: 2]
```

```
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: 8953
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 7b3fb55f36b3011f0100000067fd2696c791f6cb9a9fe6a9 (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: Mon Apr 14 12:15:34 -03 2025
;; MSG SIZE  rcvd: 150
```

Respuesta de la consulta MX:

```
▾ Domain Name System (response)
    Transaction ID: 0xc890
  ▸ Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 3
  ▾ 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)
  ▾ Answers
    ▾ redes.unlp.edu.ar: type MX, class IN, preference 10, mx mail2.redes.unlp.edu.ar
        Name: redes.unlp.edu.ar
        Type: MX (Mail eXchange) (15)
        Class: IN (0x0001)
        Time to live: 86400 (1 day)
        Data length: 10
        Preference: 10
        Mail Exchange: mail2.redes.unlp.edu.ar
    ▾ redes.unlp.edu.ar: type MX, class IN, preference 5, mx mail.redes.unlp.edu.ar
        Name: redes.unlp.edu.ar
        Type: MX (Mail eXchange) (15)
        Class: IN (0x0001)
        Time to live: 86400 (1 day)
        Data length: 9
        Preference: 5
        Mail Exchange: mail.redes.unlp.edu.ar
  ▾ Additional records
    ▸ mail.redes.unlp.edu.ar: type A, class IN, addr 172.28.0.90
    ▸ mail2.redes.unlp.edu.ar: type A, class IN, addr 172.28.0.91
    ▸ <Root>: type OPT
    [Request In: 378]
    [Time: 0.000269023 seconds]
```

```
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: 51344
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 88181f0b6fa687670100000067fd27cd84b76313e4cff1f9 (good)
;; QUESTION SECTION:
;redes.unlp.edu.ar.             IN      MX

;; ANSWER SECTION:
redes.unlp.edu.ar.      86400   IN      MX      10 mail2.redes.unlp.edu.ar.
redes.unlp.edu.ar.      86400   IN      MX      5 mail.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: 4 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Mon Apr 14 12:20:45 -03 2025
;; MSG SIZE  rcvd: 149

redes@debian:~$
```

15)

a. La **PC realiza consultas recursivas al servidor DNS** configurado.
   Entonces, la PC se desentiende del resto, y espera una única respuesta final con la dirección IP que corresponde al nombre solicitado.
b. El **servidor DNS realiza consultas iterativas a otros servidores DNS** para obtener la información paso a paso.
   Proceso:
   La PC consulta recursivamente al servidor DNS local por, por ejemplo, www.google.com.
   Si el servidor no tiene esa información en caché, empieza a hacer consultas iterativas así:
   - Pregunta a un root server: "¿Dónde encuentro información sobre .com?"
   - Luego al servidor de TLD .com: "¿Dónde está el DNS de google.com?"
   - Luego al DNS autoritativo de google.com: "¿Cuál es la IP de www.google.com?"

   Cada uno de estos pasos son consultas iterativas, donde el servidor recibe una referencia y luego decide a quién preguntar en el siguiente paso.

16) Cuando escribís en el navegador (por ejemplo): https://www.redes.unlp.edu.ar, estás usando HTTP(S), el protocolo de transferencia de hipertexto. Pero para que el navegador pueda conectarse con ese servidor web, necesita la dirección IP correspondiente a www.redes.unlp.edu.ar. El sistema operativo consulta al servidor DNS para resolver el nombre. Cuando obtiene la IP, se realiza la conexión HTTP(S).
Podés navegar solo si conocés la dirección IP exacta del servidor web.
Por ejemplo, si sabés que 163.10.20.45 corresponde a www.redes.unlp.edu.ar, podés escribir directamente:
   - http://163.10.20.45

Pero pueden haber problemas:
   - Muchos sitios no responden correctamente por IP directa, porque esperan que la cabecera Host: del navegador coincida con el dominio.
   - Sitios con HTTPS y certificados SSL van a fallar si no usás el dominio correcto, ya que el certificado no va a coincidir con la IP.

17)

a. Pasos:
   i) **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**.
   ii) **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. DNS Server consulta iterativamente a un servidor raíz como por ejemplo **A.Root-Server con la IP 205.10.100.10**.
   iii) **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**.
   iv) **DNS Server** consulta iterativamente al servidor TLD **a.dns.ar con la IP 200.108.145.50**.

v) **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**.

vi) **DNS Server** consulta iterativamente al servidor TLD **ns1.riu.edu.ar con la IP 170.210.0.18**.

vii) **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**.

viii) **DNS Server** consulta iterativamente al servidor autoritativo **unlp.unlp.edu.ar con la IP 163.10.0.67**.

ix) **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)**.

x) **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. 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) Consultamos por los servidores de google.com para saber cuales son autoritativos:

```
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: 32336
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ab2e8092df330a2a0100000067fd3b31926220c64fd4d2d4 (good)
;; QUESTION SECTION:
;google.com.                    IN      NS

;; ANSWER SECTION:
google.com.             11016   IN      NS      ns3.google.com.
google.com.             11016   IN      NS      ns1.google.com.
google.com.             11016   IN      NS      ns2.google.com.
google.com.             11016   IN      NS      ns4.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         11003   IN      A       216.239.32.10
ns2.google.com.         11003   IN      A       216.239.34.10
ns3.google.com.         11003   IN      A       216.239.36.10
ns4.google.com.         11003   IN      A       216.239.38.10
ns1.google.com.         11003   IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         11003   IN      AAAA    2001:4860:4802:34::a
ns3.google.com.         11003   IN      AAAA    2001:4860:4802:36::a
ns4.google.com.         11003   IN      AAAA    2001:4860:4802:38::a

;; Query time: 2421 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Mon Apr 14 13:43:29 -03 2025
;; MSG SIZE  rcvd: 315
```

Consultamos algunos de los servidores DNS autoritativos:

```
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: 34440
;; 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       142.251.133.238

;; Query time: 528 msec
;; SERVER: 216.239.32.10#53(216.239.32.10)
;; WHEN: Mon Apr 14 13:46:33 -03 2025
;; MSG SIZE  rcvd: 55
```

19) Si realizamos la consulta:

```
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: 44217
;; 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: 152 msec
;; SERVER: 216.239.32.10#53(216.239.32.10)
;; WHEN: Mon Apr 14 13:48:26 -03 2025
;; 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: 32763
;; 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: 196 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Apr 14 13:51:39 -03 2025
;; 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.

20)

a. ;; 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

b. No es autoritativa, podría preguntarle a:
   - **ss00.ejemplo.com.**
   - **ss02.ejemplo.com.**
   - **ss01.ejemplo.com.**
   - **ss03.ejemplo.com.**

c. Tanto la pregunta como la respuesta fueron recursivas.

d. 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.