**Capa de Aplicación - DNS Redes y comunicaciones - 2022**

**Práctica 3-Capa de Aplicación - DNS**

**5, 12, 14b(se contradecían)**

**El 11 es distinto**

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

Teoría:

Surge de la necesidad de utilizar nombres en lugar de direcciones IP como un mecanismo para mapear nombres de internet (nombres de dominio) a dir. IP.

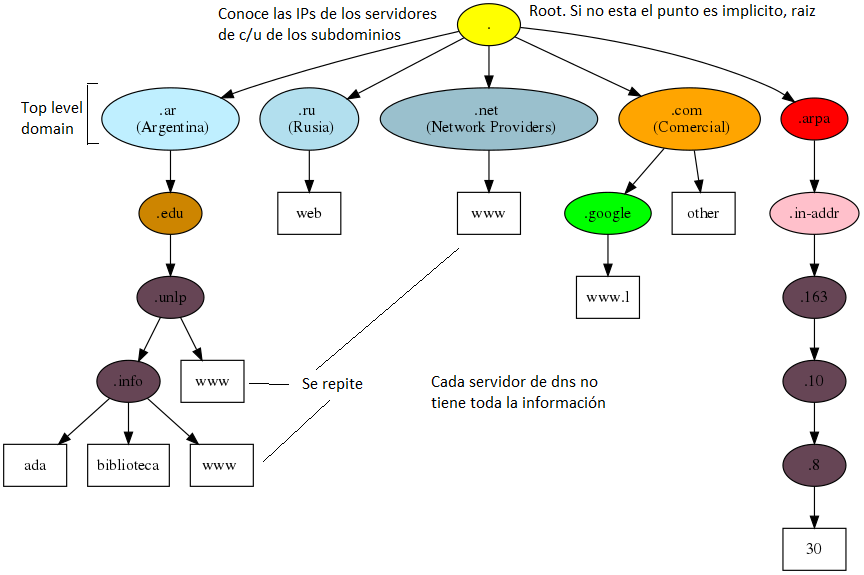
**Aspectos y Elementos de DNS**

* Espacio de nombres (sintaxis y zonas, dominios), para hacerlo escalable y delegable.
* Procedimiento de Delegación y Arquitectura. Servidores.
* Base de datos distribuida en servidores a lo largo de la red.
* Define las componentes y el protocolo para su comunicación (Que puertos usa).
* Procedimiento de búsqueda/resolución (Protocolos).

**Elementos de DNS, FQDN**

* Nombre de dominio FQDN (Fully Qualified Domain Name): lista de etiquetas (labels) separadas por puntos.
* Se leen desde el nodo/etiqueta de la izquierda hasta la raíz del árbol (el punto), estructura jerárquica con subnombres (niveles).
  + La sintaxis jerárquica refleja la delegación de autoridad.
  + No son case-sensitive, cada etiqueta Máximo 63 chars.
  + Máx etiquetas 127, nombre máx. 255 chars, acepta valores internacionales, UTF-8, Unicode.
* www, biblioteca, ada (No FQDN)
* www.info.unlp.edu.ar. , biblioteca.info.unlp.edu.ar. (FQDN)
* ada.info.unlp.edu.ar. (FQDN)
* www.info.unlp.edu.ar (Considerado FQDN) 🡪 Le falta el punto al final

Esquema de Nombres de DNS



El sistema es una estructura jerárquica según el nombre FQDN. El nombre . es la raíz, de ahí cuelgan TLDs como .ar y .org, de estos dominios como .edu.ar, y así sucesivamente. Este permite acceder a extremos remotos a partir de su nombre FQDN, sin conocer su dirección IP exacta

DNS (Domain Name System) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como internet o una red privada. Este sistema asocia información variada con nombre de dominio asociada a cada uno de los participantes. Su función más importante es “traducir” nombres a identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

Podría decirse que la segunda función más importante es la localización de servidores de correo electrónico de dominio.

La organización jerárquica del sistema DNS está reflejada en su base de datos, la cual también es distribuida y jerárquica.

Supongamos que la dirección IP de Google es 216.58.210.163. Es mucho más lógico que la gente pueda recordar un nombre de dominio (www.google.com), que su IP. Además, la dirección numérica podría cambiar, problema es también solucionado por DNS, para que el usuario pueda ignorar por completo el cambio.

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

Es un servidor de nombres DNS que tiene asignada a la zona Root (raíz del árbol de jerarquías). Delega las solicitudes a las TLDs.

Un **Generic Top-Level Domain (GTLD)** contiene dominios con propósitos particulares (.com para páginas comerciales, .org para organizaciones, etc)

DNS posee un gran número de servidores, organizados de forma jerárquica y distribuidos alrededor del mundo. Ninguno responde todas las solicitudes de todos los hosts de internet.

De los servidores, existen 3 clases:

● Servidores DNS raíz **(Root server)**: existen 13 (etiquetados de la A a la M), distribuidos por el mundo. Cada servidor es una agrupación (cluster) de servidores replicados (seguridad y fiabilidad).

* Punto de inicio (Bootstrap).
* 7 trabajan con redundancia y las réplicas están distribuidas geográficamente.
* El DNS local conoce la IP de alguno y puede pedir la de los demás y usarla a su gusto.
* Los servidores implementan el protocolo DNS definido en RFC.

● **Servidores de dominio de nivel superior (TLD**): responsables de los dominios de nivel superior. Hay 3 tipos:

1. **Generic TLD (gTLD)**: contienen dominios con propósitos particulares, de acuerdo a diferentes actividades, como son .com, .org, .net, .edu, .gov, etc.

2. **Country-Code TLD (ccTLD):** dominios de nivel superior correspondientes a países: uk, ar, cl.

3. **ARPA TLD:** usado por los protocolos. Resuelve direcciones a nombres.

● Servidores DNS **autoritativos:** cada zona tiene uno, el cual es la autoridad en la zona, ya que contiene todos los registros de recursos de la zona. Un servidor de nombres autoritativo se define con el registro de recurso NS y SOA. Para que el protocolo DNS sea tolerante a fallas, se recomienda dos o más servidores de nombres de dominio autoritarios por zona, donde al menos uno de ellos sea el master.

Un servidor **DNS autoritativo** es el autorizado a responder la IP para los nombres de dominio que tiene alojados localmente.

También existe el servidor DNS local, el cual actúa como proxy reenviando las consultas a la jerarquía de servidores DNS. Mantiene una caché con los nombres que resuelve, para que, ante futuras solicitudes por ciertos nombres de DNS, no deba salir a la red a buscar la dirección IP en cuestión.

Proxy: (representante) es un agente o sustituto autorizado para actuar en nombre de otra persona (máquina o entidad) o un documento autorizado a hacerlo.

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

Es una respuesta por parte del servidor autoritativo (“oficial”), para una consulta DNS sobre un nombre de dominio en el cual tiene autoridad. Cuando la respuesta es emitida por un servidor DNS local, y este no oficia de servidor autoritativo para ese dominio (es decir que lo obtiene de la caché), esta respuesta es NO-Autoritativa.

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

**Consulta recursiva**

Es emitida por el cliente y recibida por un servidor DNS, quien consulta a otros servidores para satisfacerla, y así recursivamente.

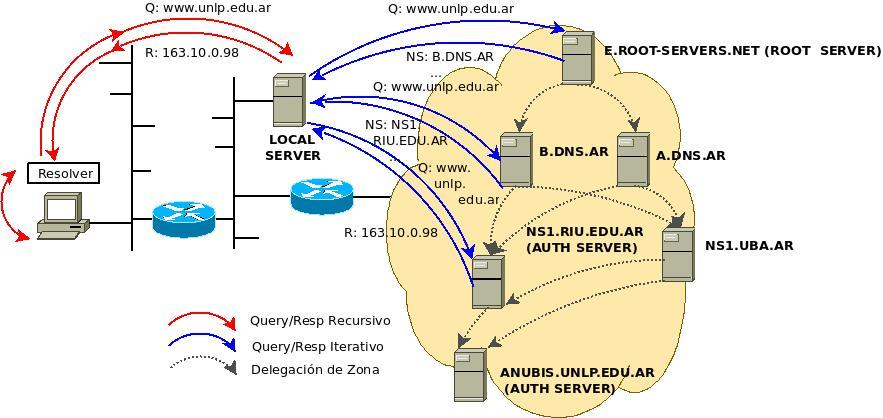
Obliga a un servidor DNS a responder a una solicitud con un error, o una respuesta de éxito. Ante este tipo de consulta, el servidor DNS debe ponerse en contacto con otros servidores DNS que necesita para resolver la solicitud. Cuando reciba una respuesta correcta de DNS (los otros servidores), a continuación, envía una respuesta al cliente.

Cuando un servidor DNS local no puede responder a una consulta con sus datos locales (archivos de zona local o caché), la consulta recursiva debe trasladarse a un servidor DNS raíz. A partir de este punto se genera una **consulta iterativa**. (si no está configurado con un reenviador).

**Consulta iterativa:**

Es emitida por el cliente y recibida por un servidor DNS, quien responde con otra dirección. Luego, el cliente consulta a esa dirección y obtiene otra respuesta, y así iterativamente

Se espera que el servidor DNS responda con la mejor información local que tiene, basado en lo que sabe el servidor DNS de los archivos de zona local o de la caché.



**5. ¿Qué es el resolver?**

El resolver es quien recibe la solicitud inicial del cliente, se comunica con los servidores DNS, y le responde con el resultado

El código (instrucciones de máquina) del cliente se agrupa en un módulo llamado Resolver.

Al “resolver” se lo podría considerar como un agente encargado de resolver los nombres a solicitud del cliente. El servidor raíz tiene que conocer la lista de servidores del dominio de primer nivel del nombre (o sabe que no existe). Si sabe más que eso responde lo más posible. Las respuestas son de dos tipos:

* lista de servidores de nombres que saben más que él (servidores del dominio o del sub-dominio),
* lista de direcciones IP que corresponden a la máquina buscada.

Además de los primarios y secundarios, los otros servidores pueden responder consultas sobre un dominio si ellos preguntaron hace poco y almacenaron la respuesta. Esta respuesta queda en un caché, y se marca como sin autoridad y se acompaña de la lista de servidores que saben más que él. El resolver elige si la acepta o no.

Nuestro resolver de DNS está definido en el servidor de DNS local.

RFC 1034: Los resolvers son programas que extraen información de los servidores de nombres en respuesta a las peticiones de los clientes. Los resolvers deben ser capaces de tener acceso a al menos un servidor de nombres y utilizar la información de ese servidor de nombres para responder a una consulta directamente, o resolver la consulta utilizando referencias a otros servidores de nombres.

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

**a. A (Address) b. MX c. PTR d. AAAA e. SRV – f. NS g. CNAME h. SOA i. TXT**

**Servicios y Registros de DNS**

Servidor de DNS almacena la información formando base de datos (DB) de RR (Resource Records).

No necesariamente es DB relacional.

El tipo de registro establece cómo se interpreta la información. Cada registro tiene diferente tipo de información:

* **Registros A, AAAA (Address):** nombre ! El valor del registro es una IP, o una IPv6 que es la dirección real del dominio.

Registros A (Address)

# less /etc/bind/db.cities.org

...

berlin.cities.org. IN A 172.20.1.100

brasilia.cities.org. IN A 172.20.1.5

paraguil-br0.cities.org. IN A 172.20.1.1

...

Registros AAAA (IPv6 Address)

# less /etc/bind/db.cities.org

...

berlin.cities.org. IN AAAA 2001:db8:1234:4567::100

brasilia.cities.org. IN AAAA 2001:db8:1234:4567::5

...

* **Registros MX (Mail Exchanger):** nombre-dom ! mail exchanger(s). Indica la lista de servidores para un dominio determinado. Ej: Gmail, yahoo, etc. Cada servidor tiene un numero asociado que indica prioridad (Mas chico, mas prioridad)

# less /etc/bind/db.cities.org

...

cities.org. IN MX 1 brasilia.cities.org.

cities.org. IN MX 10 berlin.cities.org.

...

# dig -t mx gmail.com

...

gmail.com IN MX **5** gmail-smtp-in.l.google.com. //Numero de prioridad

gmail.com IN MX 10 alt1.gmail-smtp-in.l.google.com.

gmail.com IN MX 10 alt2.gmail-smtp-in.l.google.com.

gmail.com IN MX 50 gsmtp147.google.com.

gmail.com IN MX 50 gsmtp183.google.com.

...

* **Registros PTR (Pointer**): IP ! nombre. Puntero en el árbol de esquemas de nombres. Mapear al contrario 🡪 De IP a nombres. ¿Cómo encontrarlo? Porque no se tiene el nombre para arrancar por los servidores raíz. Cuando alguien se conecta de una IP a un servidor, el servidor podría validar al cliente sabiendo que viene de una IP registrada en su registro de nombres o para no atender a algunos. Ej: Servidor de mail con spam deberían tener este recurso.

Estructura paralela que tiene la información en zonas según la IP

# less /etc/bind/db.172

...

1.1.20 IN PTR paraguil-br0.cities.org.

5.1.20 IN PTR brasilias.cities.org.

100.1.20 IN PTR berlin.cities.org.

...

5.1.19 IN PTR sucre.lat.org.

1.1.19 IN PTR paraguil-tap2.lat.org.

...

* **Registros CNAME (Canonical Name):** nombre ! nombre. Una dirección IP con varios nombres. Hay un nombre que redirige a otro nombre y ese es el que tiene dirección IP. Alias canónico. Permite asociar subdominios a un dominio ya existente.

# less /etc/bind/db.cities.org

...

ftp.cities.org. IN CNAME berlin.cities.org.

www.cities.org. IN CNAME berlin.cities.org.

...

* **Registros SRV:** “servicio”. Se utiliza para la definición de un servicio TPC en el que opera el dominio. Información necesaria para el servicio.
* **Registros NS (Name Server**): nombre-dom ! dns server(s). Indica los servidores de nombres para un dominio. Una zona puede tener uno o más. Mediante los registros dns se hace la delegación. Serv dns para algo (Ej: raíz, .com, etc). Esos deberían estar cargados en los servers. DNS para google, unlp, etc. Son autoritativos, puede haber 1ª y 2ª y eso se ve en el SOA.

# less /etc/bind/db.cities.org

...

; ## ZONA RAIZ

cities.org. IN NS berlin.cities.org.

cities.org. IN NS brasilia.cities.org.

; ## ZONA delegada

trees.cities.org. IN NS brasilia.cities.org.

trees.cities.org. IN NS berlin.cities.org.

trees.cities.org. IN NS oak.trees.cities.org.

; ## GLUE RECORD ##

oak.trees.cities.org. IN A 192.168.40.1

...

* **Registros SOA (Start Of Authority):** params. de dominio. Datos útiles para los servidores secundarios. Nombre del servidor donde se ejecutó, mail del administrador (Donde se reemplaza @ por .).

Uno por zona, definido por el primario, quien es el administrador de zona, quien es el primario.

$TTL 604800 ; ### TTL global para todos

cities.org. IN SOA berlin.cities.org.

root.berlin.cities.org. (

2008092901 ; ## Serial //*Año, mes, dia, nº de secuencia > Sirve para ver si es la misma versión que en el servidor primario.*

604800 ; ## Refresh //*Tiempo de refresco, cada cuanto se debe resincronizar. Si ya paso el refresh, esta desactualizado, asi que no funcinó. Por cuanto cachear una respuesta, es decir, preguntar por algo que se haya respondido que no exista(?*

*El tiempo (en segundos) que los servidores secundarios deben esperar antes de pedir a los servidores primarios el registro SOA para comprobar si se ha actualizado.*

86400 ; ## Retry. *El tiempo que debe esperar un servidor para volver a pedir una actualización a un servidor de nombres primario que no responde.*

2419200 ; ## Expiry. *Si un servidor secundario no recibe una respuesta del servidor primario durante este tiempo, debe dejar de responder a las consultas de la zona.*

604800 ) ; ## Neg Cache TTL

...

\*Lo verde se saco de internet

* **Registros TXT (Textual):** nombre ! info. Son informativos, definen políticas de mail, para, por ejemplo, evitar el spam. También permiten a los administradores insertar texto.

TTL y Registros TXT

? dig www.unlp.edu.ar | grep -A1 "ANSWER SECTION"

;; ANSWER SECTION:

www.unlp.edu.ar. 155 IN A 163.10.0.145

? dig -t mx gmail.com | grep -A1 "ANSWER SECTION"

;; ANSWER SECTION:

gmail.com. 3599 IN MX 20 alt2.gmail-smtp-in.l.google.com.

? dig -t txt gmail.com | grep -A1 "ANSWER SECTION"

;; ANSWER SECTION:

gmail.com. 299 IN TXT "v=spf1 redirect=\_spf.google.com"

? dig -t txt \_spf.google.com | grep -A1 "ANSWER SECTION"

;; ANSWER SECTION:

\_spf.google.com. 299 IN TXT

"v=spf1 include:\_netblocks.google.com

include:\_netblocks2.google.com

include:\_netblocks3.google.com ~all"

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

Porque ofrece una serie de ventajas:

* Permite que un único servidor no tenga que soportar toda la carga de los request en todo el mundo, lo que resultaría ineficiente.
* Posibilita que, en caso de que falle un servidor, otro responda.
* Proporciona seguridad para los datos, ya que hay copias idénticas (Redundancia), por si se pierde la información.
* Mejora en la estabilidad de la conexión entre el dominio y el resto de Internet

**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?**

Esto es una cuestión de implementación, no es visible para el cliente. Si ambos son autoritativos, es decir, son dueños del registro, los que imponen su valor, tienen que mantener coherencia entre ellos. Para esto en uno (El primario) se configura la información y el segundo, tercero, cuarto…n (Secundarios) la copian mediante una sincronización llamada **transferencia de zona**. Ambos siguen siendo igual de autoritativos. En el caso de que haya varios, pero todos se configuran “A mano”, todos serían primarios.

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

Cuando un servidor es primario y otro secundario se sincronizan mediante transferencia de zona. Esto consiste en que el secundario le pida a su servidor primario (Solo puede al suyo, no a otros primarios) que le mande toda la información que tiene. La finalidad es que los servidores compartan la información actualizada sin tener que ser modificada en todos directamente por el administrador, si no que se haga automáticamente.

**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).**

**Delegar un dominio:** acción de transferir la responsabilidad de la resolución de nombres bajo una denominación a un conjunto de servidores de nombres para lo mismo.

Para este caso tendría que delegar las solicitudes de acceso a redes.unlp.edu.ar a un servidor de DNS que el administrador de redes de la Facultad pueda manejar o tenga control sobre él.

**//dejarla porque la toman en parciales**

**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:**

*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: 50085

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

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

; COOKIE: 9fe19a49e66d8fe5010000006317c0bb9cf148b46a7d31b4 (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: Tue Sep 06 18:50:51 -03 2022

;; MSG SIZE rcvd: 94

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

El flag **rd** (recursion desired) nos indica que la solicitud fue recursiva.

El flag **ra** (recursion available) nos indica que el servidor puede responder recursivamente, por lo que la respuesta también lo fue.

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

El flag **aa** (authoritative answer) nos indica que la respuesta fue autoritativa. Significa que el servidor es autoritativo del dominio solicitado y sabe responder su dirección IP.

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

La IP del resolver usado (no necesariamente el configurado en la PC, ya que se puede seleccionar usar otro) es **172.28.0.29**, ya que es la especificada bajo la etiqueta SERVER:. Además, tiene el puerto **53** abierto, el cual es usado para brindar servicios DNS

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

*dig "redes.unlp.edu.ar" mx //o dig –t mx redes.unlp.edu.ar*

; <<>> DiG 9.16.27-Debian <<>> redes.unlp.edu.ar mx

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43684

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

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

; COOKIE: fb9aaba23a4d1b92010000006317c542f7d004f886826a0f (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: Tue Sep 06 19:10:10 -03 2022

;; MSG SIZE rcvd: 149

Los servidores son mail.redes.unlp.edu.ar y mail2.redes.unlp.edu.ar, bajo las IPs 172.28.0.90 y 172.28.0.91, respectivamente

**¿Por qué hay más de uno y qué significan los números que aparecen entre MX y el nombre?**

Hay más de uno para no sobrecargar al servidor y para que, si uno no funciona, se pueda intentar con los demás.

El número indica la prioridad de cada servidor. Cuanto más bajo el valor, ese servidor será contactado antes que los demás.

**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?**

Si el servidor mail.redes.unlp.edu.ar funciona, éste lo recibirá (Va primero porque tiene un 5, y el otro tiene un 10, por lo que tiene más prioridad). Sino, si el servidor mail2.redes.unlp.edu.ar funciona, éste lo recibirá. Sino, hay error de SMTP (si se obtiene una IP pero está caído) o de DNS (si no se encuentra el dominio).

**c. ¿Cuáles son los servidores de DNS del dominio redes.unlp.edu.ar? (no está en el tp)**

*dig "redes.unlp.edu.ar" ns o dig –t ns redes.unlp.edu.ar*

; <<>> DiG 9.16.27-Debian <<>> redes.unlp.edu.ar ns

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39444

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

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

; COOKIE: f4f5cc6dbe431285010000006317c8a4b92892b7ef7ff240 (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

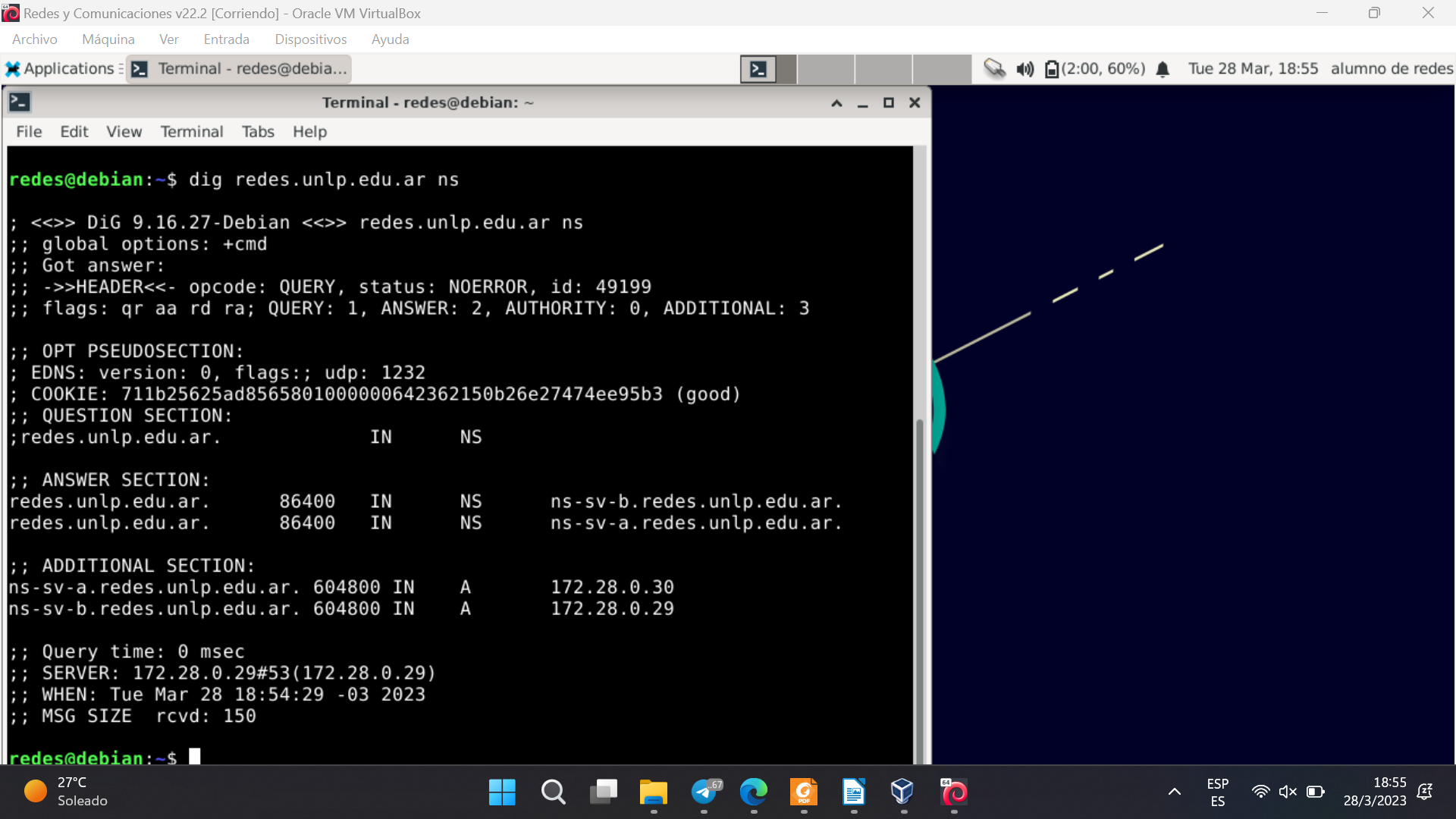
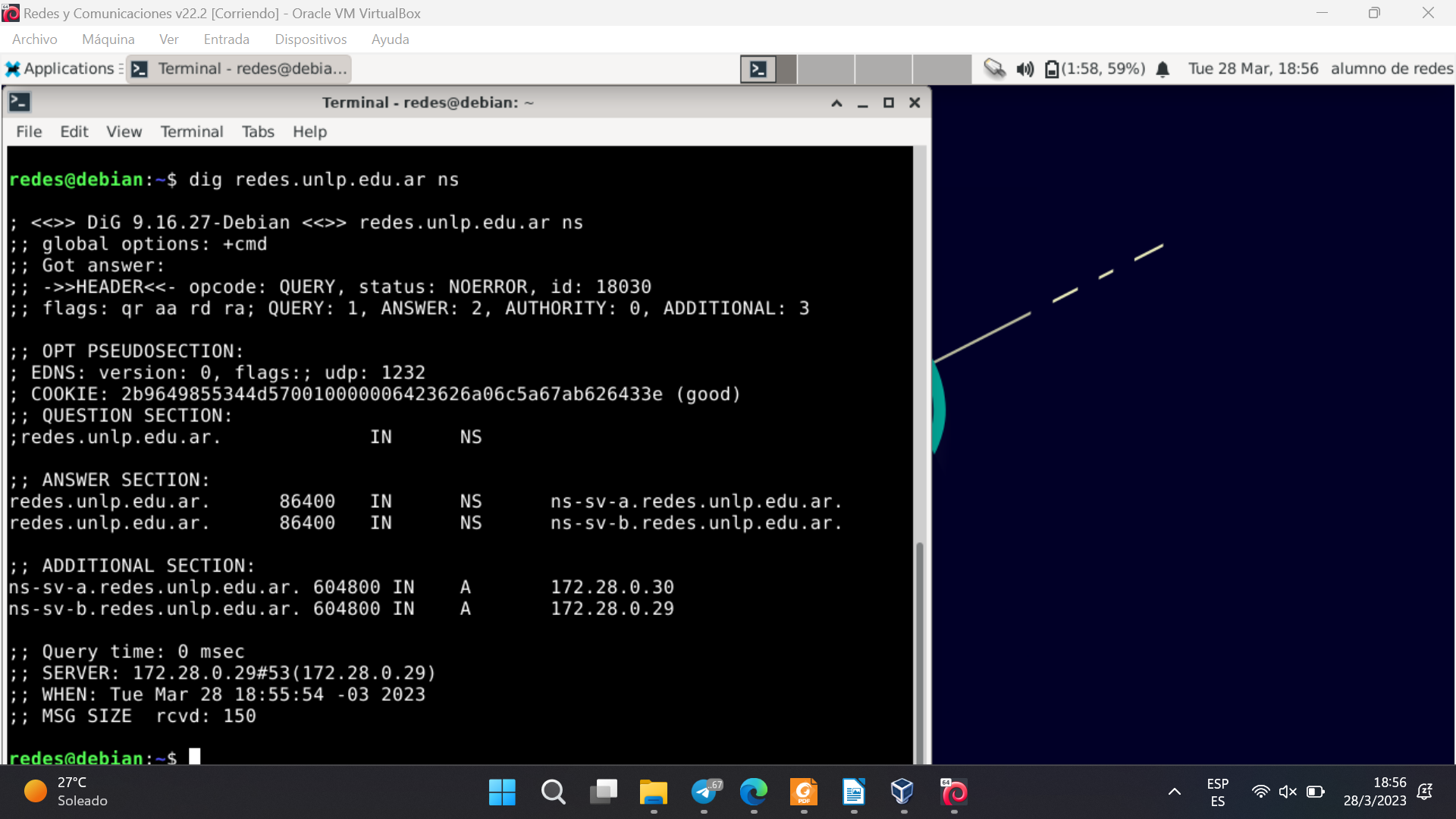
;; SERVER: 172.28.0.29#53(172.28.0.29)

;; WHEN: Tue Sep 06 19:24:36 -03 2022

;; MSG SIZE rcvd: 150

Los servidores DNS son **ns-sv-a.redes.unlp.edu.ar y ns-sv-b.redes.unlp.edu.ar**, bajo las IPs 172.28.0.30 y 172.28.0.29, respectivamente

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

****

Cada consulta tiene una ID distinta de las demás

En el protocolo Extended DNS (EDNS), se incluyen cookies DNS para aumentar la seguridad de las consultas

Por política Round Robin y balanceo de carga, el orden de la lista de servidores va variando. Suele accederse al primero de la lista

Cada consulta puede tardar diferente, aunque se haga a la misma dirección, por ejemplo, según la carga del servidor DNS en cada momento. O si una dirección ya fue cacheada, etc

Cada consulta fue realizada en un instante de tiempo distinto.

**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, no es posible.

**e. Consulte por el registro SOA del dominio y responda.**

*dig "redes.unlp.edu.ar" soa*

; <<>> DiG 9.16.27-Debian <<>> redes.unlp.edu.ar soa

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24826

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

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

; COOKIE: 4132e9cbe51cf5100100000063181922244fb3947da2da71 (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: 4 msec

;; SERVER: 172.28.0.29#53(172.28.0.29)

;; WHEN: Wed Sep 07 01:08:02 -03 2022

;; MSG SIZE rcvd: 123

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

Sí, 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?**

En la sección ANSWER SECTION, 7ma columna (3er campo del SOA) podemos encontrar el número de serie **2020031700**, que es por convención el momento de la última actualización 00 17/03/2020 - 2020 03 17 00. Los 2 últimos dígitos no es la hora sino el número de versión.

Sigue un formato estándar YYYYMMDDnn, donde:

|  |  |  |
| --- | --- | --- |
| **Parámetro** | **Significado** | **Cantidad de dígitos** |
| YYYY | Año | 4 |
| MM | Mes | 2 |
| DD | Día | 2 |
| nn | Cantidad de cambios en el día | 2 |

Es importante actualizarlo al editar el archivo hosts, para que los servidores secundarios vean que existe una versión nueva en el primario, y así mantener la sincronía

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

El valor del segundo campo es root.redes.unlp.edu.ar

Es el correo del administrador. El @ se sustituye por un . debido a que @ representa el dominio raíz de la zona, por lo que el mail correcto es **root@redes.unlp.edu.ar**

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

La caché negativa (séptimo campo) es el tiempo que pasó desde que un registro no está en la caché, el valor máximo es de **86.400** segundos, es decir, 24 hs.

Las entradas solicitadas al servidor podrán permanecer en la caché de los clientes, como máximo por esa cantidad de segundos (exclusivo). Pasado ese tiempo, deben solicitar los datos actualizados

**f. Indique qué valor tiene el registro TXT para el nombre saludo.redes.unlp.edu.ar. Investigue para qué**

**es usado este registro.**

*dig "saludo.redes.unlp.edu.ar" txt*

; <<>> DiG 9.16.27-Debian <<>> saludo.redes.unlp.edu.ar txt

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31036

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

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

; COOKIE: 1f6bf9d1c7ff53f00100000063182355a409e73b93aa416c (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 07 01:51:33 -03 2022

;; MSG SIZE rcvd: 98

El valor del registro es "**HOLA**"

Este registro fue diseñado para que el administrador de un dominio pueda asociarle notas de texto con el fin de documentar y dejar mensajes para los que vayan a usar el servidor. En la actualidad, también se lo usa para prevenir spam por email, y verificar la propiedad de los dominios

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

**¿Por qué un atacante querría realizar la transferencia de zona y recolección los registros de los servidores DNS?**

Sucede que a través de ellos se llega a recolectar información de una red corporativa, exponiendo sus direcciones IP internas, servidores y equipos. Para recolectar esta información debe usarse el parámetro “axfr” (a este tipo de ataque también se lo denomina AXFR) donde el comando queda de la siguiente manera:

dig @ns1.midominio.net axfr midominio.net

El parámetro “axfr” es quien permite la transferencia de zona de dicho DNS, ya que se usa para sincronizar y actualizar datos de la zona cuando se produjeron cambios. Si bien la transferencia puede hacerse vía “axfr”, también es posible hacerla de forma incremental, denominada entonces “ixfr” -cuando se ejecuta la solicitud se obtiene la transferencia de toda la zona como respuesta. Sin la debida configuración, esto le permite a un atacante replicar la base de datos DNS, obteniendo información sensible.

*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: 4 msec

;; SERVER: 172.28.0.29#53(172.28.0.29)

;; WHEN: Wed Sep 07 02:04:01 -03 2022

;; XFR size: 17 records (messages 1, bytes 441)

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

Representa la cantidad de segundos, que luego de transcurrir, el servidor secundario deberá descartar su valor y solicitar la versión actualizada al servidor primario

Sin ésta, los servidores secundarios no tendrían forma de saber si sus datos están actualizados, y cada cuánto volver a sincronizarla

**ii. ¿Cuántos registros NS observa? Compare la respuesta con los servidores de DNS del dominio redes.unlp.edu.ar que dio anteriormente. ¿Puede explicar a qué se debe la diferencia y qué significa?**

Hay 4 registros NS (En azul). Anteriormente (11c), hay 2 que son los 2 primeros que aparecen en este punto, se sumaron n1. practica.redes.unlp.edu.ar y n2. practica.redes.unlp.edu.ar

generalmente son 2, hay uno o más. Propios del dominio

rta autoritativa: es válida, está “certificada”

Esto se debe a que practica.redes.unlp.edu.ar es un sub-dominio de redes.unlp.edu.ar, por lo que el segundo servidor delega las solicitudes al primero. Los servidores autoritativos son 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.**

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: 21015

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

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

; COOKIE: ce93f61a6a80d2560100000063183554638e3b5e9ebe199c (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 07 03:08:20 -03 2022

;; MSG SIZE rcvd: 94

\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-

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: 58786

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

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

; COOKIE: bd24f6dcc11411b6010000006318358ddfd571b1e24bb45a (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: 484 msec

;; SERVER: 172.28.0.29#53(172.28.0.29)

;; WHEN: Wed Sep 07 03:09:17 -03 2022

;; MSG SIZE rcvd: 103

**Observe los TTL de ambos. Repita la operación y compare el valor de los TTL de cada uno respecto de la respuesta anterior.**

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: 40325

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

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

; COOKIE: dd2cd48fcd373ee2010000006318359131cbd86d81f2648b (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: Wed Sep 07 03:09:21 -03 2022

;; MSG SIZE rcvd: 94

\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-\*-

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: 64191

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1 *🡪 en este no esta el flag aa*

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

; COOKIE: efbef15b63a8f30201000000631835931c7229cf8669547a (good)

;; QUESTION SECTION:

;www.practica.redes.unlp.edu.ar. IN A

;; ANSWER SECTION:

www.practica.redes.unlp.edu.ar. **54** IN A 172.28.0.10

;; Query time: 0 msec

;; SERVER: 172.28.0.29#53(172.28.0.29)

;; WHEN: Wed Sep 07 03:09:23 -03 2022

;; MSG SIZE rcvd: 103

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

En el caso de www.redes.unlp.edu.ar, el contador de segundos es inicializado a **300** (valor configurado) y no se decrementa, porque la solicitud fue respondida por un servidor autoritario (flag **aa**)

En el caso de www.practica.redes.unlp.edu.ar, el contador de segundos es inicializado a 60 y decrementado al llegar a 0, donde el cliente descartará el registro por considerarlo viejo. El flag aa no está presente, por lo que la solicitud no fue respondida por un servidor autoritario

**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?**

No se obtuvo respuesta, pero sí el código de estado NXDOMAIN

Mensaje Se emite cuando…

NOERROR La solicitud fue completada satisfactoriamente. Se obtuvo una respuesta válida

NXDOMAIN La solicitud falló porque el dominio ingresado no existe

SERVFAIL La solicitud falló porque no se pudo obtener una respuesta

REFUSED La solicitud falló porque el servidor DNS rechazó procesarla, por sus políticas

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

* **Dirección IP de** [**www.redes.unlp.edu.ar**](http://www.redes.unlp.edu.ar/)
* **Servidores de correo del dominio redes.unlp.edu.ar**
* **Servidores de DNS del dominio redes.unlp.edu.ar.**

|  |  |  |
| --- | --- | --- |
|  | **nslookup** | **host** |
| **Para qué sirve?** | Hablarle a servidores DNS, de forma interactiva o usando comandos.  Encontrar la dirección IP de un equipo determinado o realizar una búsqueda DNS inversa (encontrar el nombre de dominio de una determinada dirección IP). | Hablarle a servidores DNS, usando comandos. Más moderno que nslookup |
| **Dir IP de www.redes.unlp.edu.ar** | nslookup "www.redes.unlp.edu.ar" | host "www.redes.unlp.edu.ar" |
| **Resultado** | Server: 172.28.0.29 Address: 172.28.0.29#53 Name: www.redes.unlp.edu.ar Address: 172.28.0.50 | www.redes.unlp.edu.ar has address 172.28.0.50 |
| **Servidores de correo de redes.unlp.edu.ar** | nslookup -querytype=mx "redes.unlp.edu.ar"  nslookup -type=x redes.unlp.edu.ar | host -t MX "redes.unlp.edu.ar" |
| **Resultado** | 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.  El segundo comando devuelve lo mismo. | 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. |
| **Servidores DNS de redes.unlp.edu.ar** | nslookup -querytype=ns "redes.unlp.edu.ar" | host -t NS "redes.unlp.edu.ar" |
| **Resultado** | Server: 172.28.0.29 Address: 172.28.0.29#53  redes.unlp.edu.ar nameserver = ns-sv-b.redes.unlp.edu.ar. redes.unlp.edu.ar nameserver = ns-sv-a.redes.unlp.edu.ar. | redes.unlp.edu.ar name server ns-sv-b.redes.unlp.edu.ar. redes.unlp.edu.ar name server ns-sv-a.redes.unlp.edu.ar. |

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

El archivo hosts de un ordenador es usado por el sistema operativo para guardar la correspondencia entre dominios de Internet y direcciones IP. Este es uno de los métodos que usa el sistema operativo para resolver nombres de dominios. Antiguamente cuando no había servidores DNS que resolvieran los dominios, el archivo hosts era el único encargado de hacerlo. En muchos sistemas operativos este método es usado preferentemente respecto a otros como el DNS. En la actualidad también es usado para bloquear contenidos de Internet como la publicidad web. El archivo hosts es un archivo de texto plano que puede ser editado por el administrador del equipo.

**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 ejecutado en 11.B. Respuesta en Wireshark:*

Domain Name System (response)

Transaction ID: 0x2573

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 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

Name: mail.redes.unlp.edu.ar

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 86400 (1 day)

Data length: 4

Address: 172.28.0.90

mail2.redes.unlp.edu.ar: type A, class IN, addr 172.28.0.91

Name: mail2.redes.unlp.edu.ar

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 86400 (1 day)

Data length: 4

Address: 172.28.0.91

<Root>: type OPT

Name: <Root>

Type: OPT (41)

UDP payload size: 1232

Higher bits in extended RCODE: 0x00

EDNS0 version: 0

Z: 0x0000

0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs

.000 0000 0000 0000 = Reserved: 0x0000

Data length: 28

Option: COOKIE

Option Code: COOKIE (10)

Option Length: 24

Option Data: 961e1d96d01c83bc01000000631aceaece89692f7a0c5f06

Client Cookie: 961e1d96d01c83bc

Server Cookie: 01000000631aceaece89692f7a0c5f06

=======================================

*dig ejecutado en 11.C. Respuesta en Wireshark:*

Domain Name System (response)

Transaction ID: 0xa6e6

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-b.redes.unlp.edu.ar

Name: redes.unlp.edu.ar

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 86400 (1 day)

Data length: 10

Name Server: ns-sv-b.redes.unlp.edu.ar

redes.unlp.edu.ar: type NS, class IN, ns ns-sv-a.redes.unlp.edu.ar

Name: redes.unlp.edu.ar

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 86400 (1 day)

Data length: 10

Name Server: ns-sv-a.redes.unlp.edu.ar

Additional records

ns-sv-a.redes.unlp.edu.ar: type A, class IN, addr 172.28.0.30

Name: ns-sv-a.redes.unlp.edu.ar

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 604800 (7 days)

Data length: 4

Address: 172.28.0.30

ns-sv-b.redes.unlp.edu.ar: type A, class IN, addr 172.28.0.29

Name: ns-sv-b.redes.unlp.edu.ar

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 604800 (7 days)

Data length: 4

Address: 172.28.0.29

<Root>: type OPT

Name: <Root>

Type: OPT (41)

UDP payload size: 1232

Higher bits in extended RCODE: 0x00

EDNS0 version: 0

Z: 0x0000

0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs

.000 0000 0000 0000 = Reserved: 0x0000

Data length: 28

Option: COOKIE

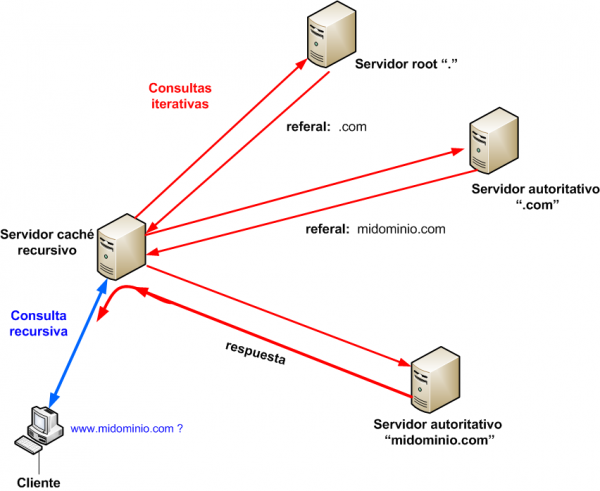
Option Code: COOKIE (10)

Option Length: 24

Option Data: e4346d75a32fdaf801000000631aceafde530a72eb01e9f1

Client Cookie: e4346d75a32fdaf8

Server Cookie: 01000000631aceafde530a72eb01e9f1

**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 realiza consultas recursivas al servidor DNS, por lo cual este le responderá al

resolver ya sea con la respuesta esperada o con un error.

**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 DNS realiza consultas iterativas a la jerarquía de servidores DNS, empezando por los servidores raíz, hasta obtener un resultado o error

El servidor DNS hará varias consultas iterativas a los servidores DNS de la jerarquía (Empezando por los raíz) y cada uno responderá con su propia información (respuesta autoritativa) la mejor respuesta posible acerca de a que servidor consultar hasta obtener un resultado o un error que devolver a la PC.

Cuando el Resolver encuentre la información, la cachea y se la da nuestra máquina.

Todo esto es considerando que el Resolver no cacheó dicho dominio.

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

HTTP permite trabajar con recursos compartidos (documentos, servicios, etc.) entre dos o más sistemas terminales (hosts). Para esto, los hosts deben ser identificables unívocamente, y así poder direccionar a un host y un recurso particular (URI). Dichos hosts se identifican en la red mediante una dirección IP.

El servicio DNS permite mapear (y consultar) direcciones IP con nombres nemotécnicos. HTTP permite referenciar recursos con nombres de dominio, como con direcciones IP. Pero lógicamente, navegar en internet se complicaría muchísimo sin servicio de DNS, ya que deberíamos:

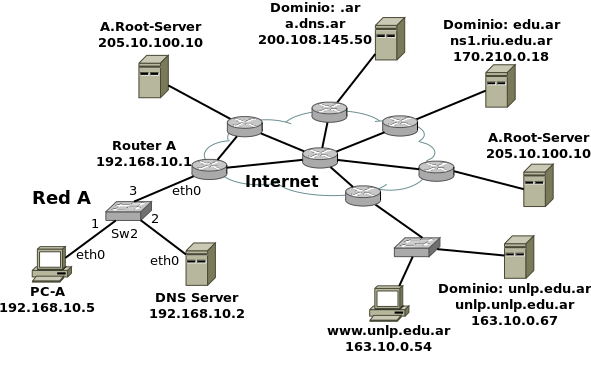
● Tener localmente el mapeo entre los nombres de host y las IPs (archivo host). O conocer previamente las IP de los hosts que deseamos acceder.

● Referenciar todos los recursos de internet mediante la IP.

● Mantener todas las IP estáticas (ya que sino los documentos y archivos dejarían de servir).

Por esto, sin servicio de DNS, Internet, tal cual lo conocemos, sería inviable.

**17. Observar el siguiente gráfico y contestar:**



Uno de esos es servidor unlp, el otro es el equipo de unlp(?

**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.**

● El resolver de PC-A realiza una consulta DNS recursiva al servidor DNS 192.168.10 por el dominio www.unlp.edu.ar.

● El DNS server 192.168.10.2 hace una consulta iterativa a a.root-server, el cual responderá con la dirección del TLD a.dns.ar (Va de atrás hacia adelante) el cual es el servidor dns autoritativo para el dominio ar.

● El DNS server hace una consulta iterativa a a.dns.ar, el cual responde con la dirección de ns1.riu.edu.ar (Lo que sigue desde la derecha) el cual es el servidor dns autoritativo para el dominio edu.ar.

● El DNS server hace una consulta iterativa a ns1.riu.edu.ar el cual responde con la dirección unlp.unlp.edu.ar el cual es el servidor autoritativo para el dominio unlp.edu.ar.

● El DNS server hace una consulta iterativa a unlp.unlp.edu.ar el cual es el servidor autoritativo de unlp.edu.ar y este le devuelve… la dirección ip de www.unlp.edu.ar(?

Vale aclarar que el DNS local consulta a cada uno por todo el nombre de dominio. A cada uno le pregunta por www.unlp.edu.ar, y cada cual va desglosando la dirección de derecha a izquierda, y responde como mejor sabe.

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

Es recursiva la consulta de PC-A al servidor DNS, pero podría haber más de una solicitud recursiva. Por ejemplo, en casas de familia, se puede hacer consulta recursiva a un módem, y otra recursiva al servidor local. También se podría hacer consultas iterativas directamente desde el cliente.

Son iterativas son las consultas del servidor DNS al resto de Internet

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

*dig "google.com" ns*

; <<>> DiG 9.16.27-Debian <<>> google.com ns

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15370

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

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

; COOKIE: 76e504c09033717101000000631aa84e94faac24e98481a1 (good)

;; QUESTION SECTION:

;google.com. IN NS

;; ANSWER SECTION:

google.com. 172405 IN NS **ns3.google.com.**

google.com. 172405 IN NS **ns4.google.com.**

google.com. 172405 IN NS **ns1.google.com.**

google.com. 172405 IN NS **ns2.google.com.**

;; ADDITIONAL SECTION:

ns1.google.com. 172405 IN A 216.239.32.10

ns2.google.com. 172405 IN A 216.239.34.10

ns3.google.com. 172405 IN A 216.239.36.10

ns4.google.com. 172405 IN A 216.239.38.10

ns1.google.com. 172405 IN AAAA 2001:4860:4802:32::a

ns2.google.com. 172405 IN AAAA 2001:4860:4802:34::a

ns3.google.com. 172405 IN AAAA 2001:4860:4802:36::a

ns4.google.com. 172405 IN AAAA 2001:4860:4802:38::a

;; Query time: 0 msec

;; SERVER: 172.28.0.29#53(172.28.0.29)

;; WHEN: Thu Sep 08 23:43:26 -03 2022

;; MSG SIZE rcvd: 315

Se debería consultar a los servidores DNS **ns1.google.com, ns2.google.com, ns3.google.com, o ns4.google.com**

Para que una consulta DNS a www.google.com sea autoritativa hay que hacerla a un nameserver del dominio www.google.com el cual lo podemos obtener consultando por los registros NS.

Un ejemplo para obtener una respuesta autoritativa sería: **dig @ns3.google.com www.google.com.**

Ante una solicitud, lo normal es que la respuesta no sea autoritativa directamente al cliente. Este primero se conecta con su servidor de DNS local, que hace consultas hasta conectarse con un servidor autoritativo, el cual responde la IP, el servidor local la almacena en su caché, y la entrega al cliente.

Por esto es que las consultas no son siempre autoritativas, ya que pasan por el servidor local y este mantiene en caché por un cierto tiempo.

Este tiempo (TTL), definido por el servidor autoritativo, se lo puede ver en el comando dig www.google.com. Por ende, ante modificaciones en las webs, los administradores suelen bajar el tiempo de caché, para que los clientes puedan ver los cambios rápidamente.

Puede suceder que el servidor local sepa responder (Por tener la información en cache o ser el autoritativo). En este caso, en la respuesta solo voy a ver el flag de request recursiva, sin embargo el servidor no salió a buscar la IP, y por ende “no es recursiva”. Una vez que obtengo la IP, hago una solicitud por HTTP con GET o POST, y utilizando la IP que conseguí gracias al servicio DNS.

**19. ¿Qué sucede si al servidor elegido en el paso anterior se lo consulta por www.info.unlp.edu.ar?**

*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: 24618

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

;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 512

;; QUESTION SECTION:

;www.info.unlp.edu.ar. IN A

;; Query time: 36 msec

;; SERVER: 216.239.32.10#53(216.239.32.10)

;; WHEN: Fri Sep 09 01:40:42 -03 2022

;; MSG SIZE rcvd: 49

Si se realiza una consulta DNS al servidor ns1/n2/n3.google.com. por el dominio www.info.unlp.edu.ar, no habrá respuesta útil debido a que este nameserver no tiene registros asociados a este dominio, si no que respondería con el código de estado **REFUSED**, ya que, por sus políticas configuradas, no procesará la solicitud.

**¿Y si la consulta es al servidor 8.8.8.8?**

*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: 5292

;; 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: 68 msec

;; SERVER: 8.8.8.8#53(8.8.8.8)

;; WHEN: Fri Sep 09 01:39:55 -03 2022

;; MSG SIZE rcvd: 65

El servidor DNS 8.8.8.8 responde con el código de estado **NOERROR**, ya que procesa la solicitud y encuentra el dominio www.info.unlp.edu.ar (con IP 163.10.5.71). Esta respuesta esperada se debe a que 8.8.8.8 referencia a el servicio Google Public DNS, el cual es un servicio de DNS gratuito.

**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.** //Va Mx por que solo ese tiene numero de prioridad,

**8 ejemplo.com. 1634 IN MX 5 srv00.ejemplo.com.** // en este caso, 10 y 5 (Es el mail)

**9**

**10 ;; AUTHORITY SECTION:**

**11 ejemplo.com. 92354 IN NS ss00.ejemplo.com.**

**12 ejemplo.com. 92354 IN NS ss02.ejemplo.com.**

**13 ejemplo.com. 92354 IN NS ss01.ejemplo.com.**

**14 ejemplo.com. 92354 IN NS ss03.ejemplo.com.**

**15**

**16 ;; ADDITIONAL SECTION:**

**17 srv01.ejemplo.com. 272 IN A 64.233.186.26** //A=address, A= ipv4, y AAAA= ipv6

**18 srv01.ejemplo.com. 240 IN AAAA 2800:3f0:4003:c00::1a**

**19 srv00.ejemplo.com. 272 IN A 74.125.133.26**

**20 srv00.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 es una respuesta autoritativa debido a que no está presente el flag **aa** que corresponde a "Authoritative Answer".

Para obtener una respuesta de este tipo preguntaría a **ss00.ejemplo.com, ss01.ejemplo.com, ss02.ejemplo.com, o ss03.ejemplo.com**

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

Ambas fueron recursivas. El flag **rd** (Recursion Desired) indica que la consulta lo fue y como el servidor soporta solicitudes recursivas, en la respuesta incluyó el flag **ra** (Recursion Available)

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

Esos números indican la prioridad de cada servidor. El sistema de DNS elegirá primeramente al servidor de menor número. Si hay dos o más registros con la misma preferencia se elegirá al azar cualquiera de estos**.**