Práctica 3 RyC

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

Abstrae encontrar IP 's con un sistema de nombres para búsqueda fácil.
Funcionamiento del DNS

1. Consulta Inicial: Cuando un usuario ingresa un nombre de dominio en su navegador, se envía una consulta DNS al servidor de nombres local (resolver DNS). Si el nombre ya está en caché, se devuelve la dirección IP correspondiente.
2. Consulta Recursiva: Si el nombre no está en caché, el resolver DNS realiza una consulta recursiva. Esto significa que el resolver se encargará de buscar la dirección IP en nombre del cliente, consultando otros servidores DNS si es necesario.
3. Consulta Iterativa: Si el resolver no puede encontrar la dirección IP, comenzará a realizar consultas iterativas. Primero, consultará un servidor raíz, que le proporcionará la dirección de un servidor de dominio de nivel superior (TLD) correspondiente al dominio consultado.
4. Delegación de Zonas: El servidor TLD, a su vez, proporcionará la dirección de un servidor de nombres autoritativo para el dominio específico. Este servidor es responsable de la información del dominio y puede devolver la dirección IP final.
5. Respuesta Final: Una vez que se obtiene la dirección IP del servidor autoritativo, esta se envía de vuelta al resolver, que la almacena en caché para futuras consultas y la devuelve al navegador del usuario.
6. Acceso al Recurso: Con la dirección IP en mano, el navegador puede ahora establecer una conexión con el servidor web correspondiente y solicitar el recurso deseado

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

Un **root server** es un servidor fundamental en la jerarquía del Sistema de Nombres de Dominio (DNS). Su función principal es proporcionar información sobre los Top-Level Domains (TLDs), que son las extensiones más altas en la jerarquía de nombres de dominio, como .com, .org, .net, entre otros.
Características de los Root Servers:

- Punto de Inicio: Los root servers son el punto de partida para la resolución de nombres en Internet. Cuando un resolver DNS no puede encontrar la dirección IP de un dominio, consulta primero a un root server.
- Distribución Global: Actualmente, existen 13 root servers, identificados por letras (A a M), que están distribuidos geográficamente y funcionan con redundancia para garantizar la disponibilidad y la resiliencia del sistema.
- Ruteo Anycast: Utilizan técnicas de ruteo Anycast, lo que significa que múltiples servidores pueden compartir la misma dirección IP, permitiendo que las consultas sean dirigidas al servidor más cercano en términos de red, mejorando así la velocidad de respuesta.

Generic Top-Level Domain (gTLD)
Un generic top-level domain (gTLD) es un tipo de dominio de nivel superior que no está asociado a un país específico y se utiliza para identificar categorías amplias de sitios web. Los gTLD son administrados por la Internet Corporation for Assigned Names and Numbers (ICANN) y pueden ser utilizados por cualquier persona o entidad que cumpla con los requisitos establecidos.
Ejemplos de gTLD:

- .com: Originalmente destinado a entidades comerciales, pero ahora es utilizado por una amplia variedad de sitios.
- .org: Generalmente utilizado por organizaciones sin fines de lucro.
- .net: Originalmente destinado a proveedores de servicios de red, pero ahora es utilizado por muchos tipos de sitios.
- .info: Utilizado para sitios que proporcionan información.

3. ¿Qué es una respuesta del tipo autoritativa?

Se refiere a aquella dada por un servidor que tiene la autoridad sobre el nombre consultado, sin hacer subdelegaciones ni caché.

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

Una **respuesta recursiva** es aquella donde el **servidor** se encarga de **resolver toda la consulta en nombre del cliente**, **preguntando a otros servidores** DNS hasta obtener la respuesta completa.
Una **respuesta iterativa** en cambio el **servidor retorna** una **respuesta parcial y donde deben buscarse más detalles**, para que el cliente siga el proceso de consulta.

5.¿Qué es el resolver?

Al Resolver se lo podría considerar como un **agente encargado de resolver los nombres a solicitud del cliente** (dentro de mi maquina), es decir la consulta de la envió a este y luego el decide como resolverlo.

- **Stub/Dumb Resolver**: **No hace caching** sino que **deja** a un **servidor local lo haga** o un **Resolver activo** (smart Resolver), que **funciona** en cada equipo **como** si fuese un **servidor local** (este suele hacer consultas recursivas).

6. Describa para que se utilizan los siguientes tipo s de DNS:

a. **A**: Este registro mapea un nombre de dominio a una dirección IPv4. Permite que los navegadores y otros clientes encuentren la dirección IP correspondiente a un nombre de dominio.

b. **MX**: Este registro indica cuáles son los servidores de correo SMTP responsables de recibir los mensajes para un dominio específico. Los registros MX pueden tener prioridades asignadas para determinar el orden en que se deben utilizar los servidores de correo.

c. **PTR**: Este registro realiza el mapeo inverso, asociando direcciones IP a nombres de dominio. Se utiliza principalmente para la resolución de nombres inversa, permitiendo que se identifique el nombre de dominio asociado a una dirección IP.

d. **AAAA**: Similar al registro A, pero este mapea un nombre de dominio a una dirección IPv6. Permite la resolución de nombres para direcciones en el nuevo protocolo IPv6.

e. **SRV**: Este registro se utiliza para especificar información sobre servicios disponibles en un dominio, incluyendo el puerto y el protocolo utilizado. Es útil

para aplicaciones que requieren información sobre servicios específicos, como VoIP o mensajería instantánea.

f. **NS**: Este registro indica los servidores de nombres autoritativos para un subdominio. Permite la delegación de subdominios y es esencial para la estructura jerárquica del DNS.

g. **CNAME**: Este registro mapea un nombre de dominio a otro nombre de dominio (alias). Permite que múltiples nombres de dominio apunten a un solo nombre canónico, facilitando la gestión de dominios.

h. **SOA**: Este registro proporciona información autoritativa sobre una zona de dominio, incluyendo detalles sobre la administración y configuración de esa zona. Contiene información como el número de serie, el tiempo de refresco y el tiempo de expiración.

i. **TXT**: Este registro permite almacenar texto libre asociado a un dominio. Se utiliza comúnmente para verificar la propiedad del dominio y para configuraciones de seguridad, como SPF (Sender Policy Framework) para la autenticación de correos electrónicos [T5], [T6].

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

Redundancia, si se cae uno no se cae todo el servicio.

8. Cuando un dominio cuenta con más de un servidor, uno de ellos es el primario (o maestro) y todos los demás son secundarios (o esclavos). ¿Cuál es la razón de que sea así?

Esto se hace así para simplificar la configuración y garantizar la consistencia, los secundarios toman la configuración del primario y se sincronizan con él, además permite redundancia y tolerancia de fallos.

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

La transferencia de zona se refiere al proceso mediante el cual el DNS copia las db de nombres de los DNS primarios a los secundarios. Fundamental para la consistencia y disponibilidad.

10. Imagine que usted es el administrador del dominio de DNS de la UNLP (unlp.edu.ar). A su vez, cada facultad de la UNLP cuenta con un administrador que gestiona su propio dominio (por ejemplo, en el caso de la Facultad de Informática se trata de info.unlp.edu.ar).

Suponga que se crea una nueva facultad, Facultad de Redes, cuyo dominio será redes.unlp.edu.ar, y el administrador le indica que quiere poder manejar su propio dominio.

¿Qué debe hacer usted para que el administrador de la Facultad de Redes pueda gestionar el dominio de forma independiente? (Pista: investigue en qué consiste la delegación de dominios). Indicar qué registros de DNS se deberían agregar.

Dea q flashaban los de redes facultad de redes????? menos egocéntricos imposible.
En este caso se debe asignar autoridad sobre un subdominio de nombres específico al administrador de la facultad para poder gestionar estos registros DNS.
Subsecuentemente se deberían configurar servidores de nombre para el subdominio, incluyendo al menos un servidor de nombres autoritativo para el subdominio.
Además habría que agregar registros NS (name server) en el dominio principal (unlp.edu.ar) para que apunten a los servidores de nombres de la facultad de redes.

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:

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

La respuesta es que ambas fueron recursivas porque hay 2 flags
rd -> recursion desired
ra -> recursion available

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

Si, ya que tiene la flag aa (authoritative answer), significa que la información fue dada por un servidor con la autoridad oficial para el dominio.

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

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

b. ¿Cuáles son los servidores de correo del dominio redes.unlp.edu.ar? ¿Por qué hay más de uno y qué significan los números que aparecen entre MX y el nombre? Si se quiere enviar un correo destinado a redes.unlp.edu.ar, ¿a qué servidor se le entregará? ¿En qué situación se le entregará al otro?

Usando dig MX redes.unlp.edu.ar sacamos que:
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 es la prioridad. Normalmente se entregaría primero al de menor número (mayor prioridad) sino al otro si no está disponible el primero.

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

Usando dig NS redes.unlp.edu.ar sabemos que son ns-sv-a.redes.unlp.edu.ar. y ns-sv-b.redes.unlp.edu.ar.

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

Cambia la variable COOKIE y la variable id en el header.

e. Observe la información que obtuvo al consultar por los servidores de DNS del dominio. En base a la salida, ¿es posible indicar cuál de ellos es el primario?

Como tal no hay información específica sobre quién es el primario.

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

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

Si, es ns-sv-b... ya que es literalmente el único que aparece.

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

El número de serie es 2020031700 -> YYYY MM DD NN (todo junto obviamente, NN es el número de revisiones del dia).
Conviene actualizarlo cuando el servidor reciba cambios sustanciales.

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

Sería el refresh tiempo para que el server secundario espere hasta volver de consultar al primario (refrescandose a sí mismos). 604800.

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

86400.
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. Indique qué valor tiene el registro TXT para el nombre saludo.redes.unlp.edu.ar. Investigue para qué es usado este registro.

Dice “HOLA”.

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

dig AXFR redes.unlp.edu.ar

```
redes@debian:~/Desktop$ 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: 0 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Sat Sep 21 23:31:16 -03 2024
;; XFR size: 17 records (messages 1, bytes 441)
```

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

TTL, tiempo que debe almacenarse en caché una pieza de información antes de que este caducada.

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?

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. 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).

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.

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

; <<>> DiG 9.16.27-Debian <<>> A www.practica.redes.unlp.edu.ar.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46224
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: e21f4c14a565cc710100000066ef82d29951a7800bbc1211 (good)
;; QUESTION SECTION:
;www.practica.redes.unlp.edu.ar.        IN      A

;; ANSWER SECTION:
www.practica.redes.unlp.edu.ar. 52 IN   A       172.28.0.10

;; Query time: 0 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Sat Sep 21 23:37:06 -03 2024
;; MSG SIZE  rcvd: 103
```

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

; <<>> DiG 9.16.27-Debian <<>> A www.redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5115
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 8a687f45e08fb5800100000066ef834332febe2bb753ea66 (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: Sat Sep 21 23:38:59 -03 2024
;; MSG SIZE  rcvd: 94
```

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

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.

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

; <<>> DiG 9.16.27-Debian <<>> A www.practica2.redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 14577
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 2cc4550161270a950100000066ef83712e5fa810720b8623 (good)
;; QUESTION SECTION:
;www.practica2.redes.unlp.edu.ar. IN    A

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

;; Query time: 0 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Sat Sep 21 23:39:45 -03 2024
;; MSG SIZE  rcvd: 154
```

12. Investigue los comandos nslookup y host. ¿Para qué sirven?

nslookup permite consultar DNS para obtener información de los dominios, host hace consultas DNS pero de forma sencilla.

Intente con ambos comandos obtener:

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

nslookup www.redes.unlp.edu.ar.
host www.redes.unlp.edu.ar.

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

nslookup -type=MX redes.unlp.edu.ar
host -t MX redes.unlp.edu.ar

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

nslookup -type=NS redes.unlp.edu.ar
host -t NS 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?

Mapea nombres de host a direcciones IP, para resolver nombres de dominio a direcciones IP sin consultar 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.

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?

Recursivas.

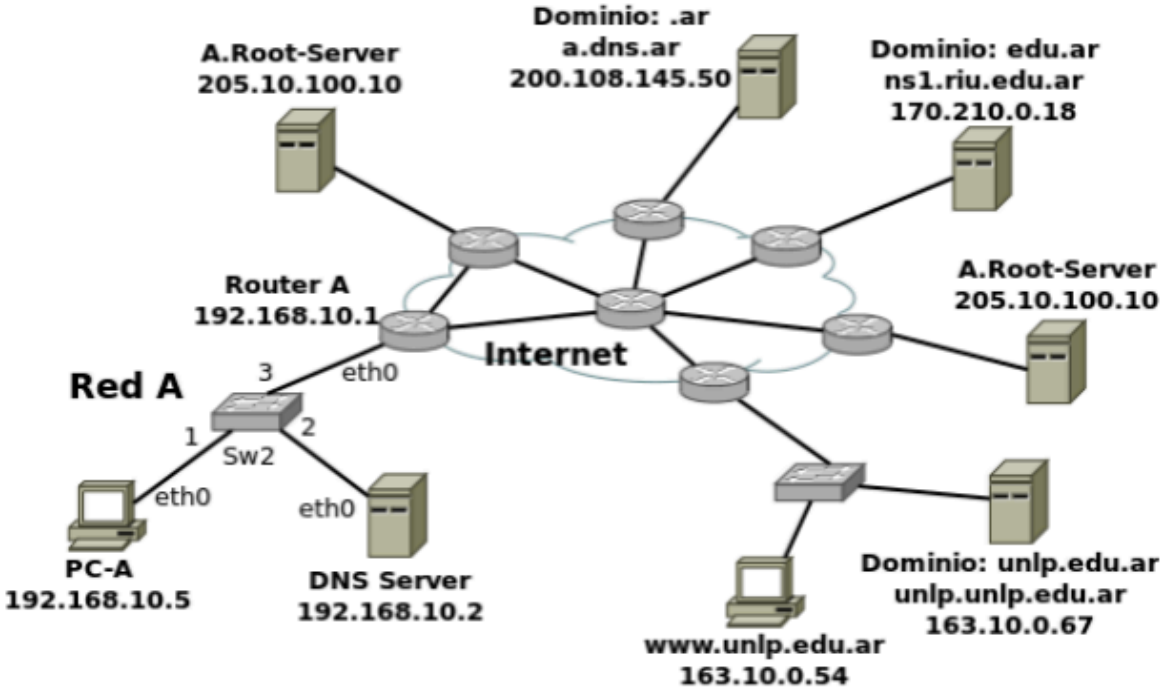
b. ¿Qué tipo de consultas (iterativas o recursivas) realiza el servidor de DNS para resolver requerimientos de usuario como el anterior? ¿A quién le realiza estas consultas?

Iterativas, va consultando dentro de la jerarquía de nombres comenzando 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 si uno sabe la dirección IP de la página a la que se quiere consultar, de otra forma se requiere DNS.

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. Primero debería fijarse si lo tiene en su lista de hosts locales del resolver privado.
2. Sino se lo delega al DNS server 192.168.10.2
3. Si no la puede obtener el DNS server consulta de forma iterativa al ROOT SERVER mas cercano, el root server le responderá de forma iterativa con el NS e IP de a.dns.ar
4. DNS server consulta a.dns.ar iterativamente y le respondera con el NS de .edu.ar y ns1.riu.edu.ar
5. DNS server consultara a ns1.riu.edu.ar que respondera con NS del servidor autoritativo del domino unlp.edu.ar, unlp.unlp.edu.ar
6. DNS server consultara a unlp.unlp.edu.ar q respondera con la IP buscada, y el DNS cachera la respuesta y le responderá al resolver de la PC-A con la IP (también es cacheada ahí).

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

Es recursiva en el resolver privado de PC-A y de DNS Server, iterativa entre las consultas entre DNS server y los servidores de la jerarquía de nombres.

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

El servidor autoritativo de google es ns1.google.com
Lo sabemos porque si usamos dig google.com @ns1.google.com tiene la flag aa.

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 server de google por www.info.unlp.edu.ar me deniega la petición, en cambio a 8.8.8.8 pasa normal porque es un servidor local.
Ejercicio de parcial

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

;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 4
;; QUESTION SECTION:
;ejemplo.com. IN __
;; ANSWER SECTION:
ejemplo.com. 1634 IN __ 10 srv01.ejemplo.com. (1)
ejemplo.com. 1634 IN __ 5 srv00.ejemplo.com. (2)
;; AUTHORITY SECTION:
ejemplo.com. 92354 IN __ ss00.ejemplo.com.
ejemplo.com. 92354 IN __ ss02.ejemplo.com.
ejemplo.com. 92354 IN __ ss01.ejemplo.com.
ejemplo.com. 92354 IN __ ss03.ejemplo.com.
;; ADDITIONAL SECTION:
srv01.ejemplo.com. 272 IN __ 64.233.186.26
srv01.ejemplo.com. 240 IN __ 2800:3f0:4003:c00::1a
srv00.ejemplo.com. 272 IN __ 74.125.133.26
srv00.ejemplo.com. 240 IN __ 2a00:1450:400c:c07::1b

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

;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 4
;; QUESTION SECTION:
;ejemplo.com. IN MX
;; ANSWER SECTION:
ejemplo.com. 1634 IN MX 10 srv01.ejemplo.com. (1)
ejemplo.com. 1634 IN MX 5 srv00.ejemplo.com. (2)
;; AUTHORITY SECTION:
ejemplo.com. 92354 IN NS ss00.ejemplo.com.
ejemplo.com. 92354 IN NS ss02.ejemplo.com.
ejemplo.com. 92354 IN NS ss01.ejemplo.com.
ejemplo.com. 92354 IN NS ss03.ejemplo.com.
;; ADDITIONAL SECTION:
srv01.ejemplo.com. 272 IN A 64.233.186.26
srv01.ejemplo.com. 240 IN 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

Las de abajo son IPS, así se sacan, las que tienen prio son si o si MX, como las 2 son MX la principal de la pregunta también lo es, NS porque siempre está eso en authority section.

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

No, no tiene la flag aa, para que lo sea habría que preguntarle a ss00.ejemplo.com.

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

Fue recursiva ambas por las flags rd, y ra.

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

Prioridad.