# Práctica 3 - DNS.

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

- El protocolo DNS sirve para mapear nombres de hosts a direcciones IP.
- En las redes, los dispositivos se identifican con direcciones IP (propias de la Capa de Red). Para nosotros es muy difícil, incómodo e impráctico referirnos a los hosts mediante direcciones IP, por lo cuál nos referimos a ellos a través de un nombre más sencillo y DNS se encarga de hacer esa traslación.

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

- Un root server es el servidor DNS que encabeza la jerarquía de servidores DNS. Es donde comienzan las consultas y se va descendiendo en función de lo que se esté consultando.
- Un generic top-level domain son un tipo de servidores subordinados del root server. Estos gtld son de propósito general y existen varios, por ejemplo: .com, .net., .org, etc.

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

- Que una respuesta sea del tipo autoritativa, significa que el servidor DNS que respondió a la consulta, es autoritativo para cierto dominio, tiene la información de dicha zona al día.

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

- En una consulta DNS recursiva, el servidor DNS recibe mi consulta y la resuelve por completo.
- En una consulta DNS iterativa, el servidor DNS me da una respuesta parcial, se deberían seguir haciendo consultas a otros servidores para obtener la respuesta deseada.

# 5. ¿Qué es el resolver?

- El resolver o servidor DNS local, es un servidor DNS el cuál resuelve todas nuestras consultas DNS (recursivas como iterativas), se comunica con otros servidores DNS vía Internet.
- Cada ISP ofrece su Resolver.

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

a. A
   - El registro A tiene la correspondencia entre un nombre de host y una dirección IP.

b. MX
   - Para un nombre de dominio, el registro MX tiene el nombre del servidor de correo canónico correspondiente a dicho nombre.

c. PTR
   - Para una dirección IP, el registro PTR establece la relación entre dicha dirección IP y el nombre de host canónico correspondiente.

d. AAAA
   - Similar al registro A. Para un nombre de host, el registro AAAA me brinda la dirección IPv6 de dicho nombre.

e. SRV
   - Usado para identificar servicios y ubicaciones de servidores para servicios específicos en un dominio. Básicamente, tiene información sobre un servicio que se ofrece a cierto dominio, junto con el o los servidores que brindan dicho servicio (dirección IP y puerto).

f. NS
   - El registro NS lo que hace es darme el nombre de host del servidor DNS autoritativo del dominio para un nombre de dominio.

g. CNAME
   - El registro CNAME establece la correspondencia entre los alias de un host y su nombre de dominio canónico.

h. SOA
   - Este registro sirve para configurar y sincronizar a los servidores DNS secundarios.

i. TXT
   - Este registro básicamente contiene información sobre el dominio y los servidores DNS.

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

- Esto suele darse para equilibrar la carga de consultas DNS al servidor autoritativo de dicha zona. Podríamos tener un servidor DNS autoritativo primario y otros secundarios, entre ellos se reparte la carga de trabajo.

## 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?

- El servidor primario es el que tiene la información al día del dominio (tiene autoridad sobre la zona). Los servidores secundarios copian esa información, pero puede llegar a pasar que en cierto momento esa información se vuelva obsoleta. Una consulta va a tener prioridad para el servidor principal, pero si las consultas son muchas probablemente se la asigne a un servidor secundario para equilibrar la carga de trabajo.

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

- El mecanismo de transferencia de zona complementa la idea de tener un servidor primario y varios secundarios.
- Básicamente, una transferencia de zona es una copia de la información del servidor primario a un servidor secundario (ya sea porque se actualiza o porque se crea uno nuevo). En esa transferencia de zona se establece el registro SOA para dicho servidor secundario.
- Es una operación costosa, por lo cuál se hace exclusivamente con TCP.

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).

- Lo que debería hacer como administrador, básicamente es tener los registros necesarios para que los servidores DNS autoritativos del dominio unlp.edu.ar deleguen las consultas del dominio redes.unlp.edu.ar a los servidores DNS de dicho dominio.
- Esto se puede hacer a través de registros NS, por ejemplo.
- Esto significa, que cuando mis servidores reciban consultas DNS del dominio redes.unlp.edu.ar, van a responder con el name server de los servidores autoritativos de ese dominio.

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:

- 172.28.0.50

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

- Los servidores DNS de redes.unlp.edu.ar son:
    - ns-sv-a.redes.unlp.edu.ar
    - ns-sv-b.redes.unlp.edu.ar

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

- Cada vez que hago la consulta, aparece un servidor primero y después otro.
- Esto sucede por Round-Robin, esto permite que la carga de trabajo se vaya dividiendo para ambos servidores.

## 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, ya que cuando se consultan los NS de un dominio, se obtiene una respuesta de aquellos servidores que son autoritativos para dicho dominio, más allá de si son primarios o secundarios.

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

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

- Si, ya que el registro SOA se usa para configurar a los servidores DNS secundarios. El servidor primario es el ns-sv-b.redes.unlp.edu.ar

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

- El número de serie: 2020031700
- La convención que sigue es: YYYYMMDDSS
  - YYYY → Año
  - MM → Mes
  - DD → Día
  - SS → Dígitos que representan la cantidad de cambios hechos en un día.
- Es importante actualizarlo cuando se realizan modificaciones en la zona.

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

- El 2do campo del registro es conocido como *refresh*.
- Sirve para indicar cada cuanto tiempo el servidor secundario le consultará al primario si hay cambios en la zona para actualizarse.
- El valor del *refresh* es de 604800, esto se interpreta como 604,800 segundos (7 días).

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

- El valor de TTL de caché negativa es de 86400

- Dicho valor significa el tiempo que el servidor mantendrá en caché una respuesta negativa a una consulta.

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

- “HOLA”

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

```
dig -t @ns-sv-a.redes.unlp.edu.ar redes.unlp.edu.ar AXFR
```

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

- Los números que aparecen antes de la palabra IN son los valores de TTL.
- Su función es indicar el tiempo que se deben mantener en la caché de los servidores.

### 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?

- Los registros NS que aparecen son 4 (antes habían sido 2)
- //CONSULTAR Esto podría ser porque redes.unlp.edu.ar tiene un sub-dominio llamado practica.redes.unlp.edu.ar, esos registros NS serían los servidores autoritativos para ese sub-dominio.

## h. Consulte por el registro A de www.redes.unlp.edu.ar y luego por el registro A de www.practica.redes.unlp.edu.ar. Observe los TTL de ambos. Repita la operación y compare el valor de los TTL de cada uno respecto de la respuesta anterior. ¿Puede explicar qué está ocurriendo? (Pista: observar los flags será de ayuda).

- //CONSULTAR
- En la consulta del registro A de www.redes.unlp.edu.ar, el TTL no se decrementa y el flag AA está activo. Significa que la consulta me la está dando un servidor autoritativo para esa zona.
- En cambio, en la consulta del registro A de www.practica.redes.unlp.edu.ar, el TTL se decrementa y el flag AA no está activo. Esto significa que el servidor que me está respondiendo no es autoritativo para dicha zona, puede ser porque ese servidor le consulta a otro servidor o porque tiene la respuesta en su caché.

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?

- Se obtuvo el registro SOA de redes.unlp.edu.ar
- Básicamente, el dominio practica2.redes.unlp.edu.ar no existe.
- Los mensajes NXDOMAIN y NOERROR sirven para describir el estado de la consulta DNS.
    - **NXDOMAIN:** Aparece cuando no se encuentra algún registro asociado a la zona consultada.
    - **NOERROR:** Aparece cuando la consulta DNS se realizó exitosamente.

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

- Dirección IP de www.redes.unlp.edu.ar.
    - nslookup: Me devolvió el nombre junto con la dirección IP (172.28.0.50)
    - Mismo caso para host, solo que nslookup también me devolvió otras direcciones IP
- Servidores de correo del dominio redes.unlp.edu.ar.
    - Con nslookup no me deja ver los servidores de correo, la consulta sería:
        - nslookup; set_type=MX; redes.unlp.edu.ar
    - Con host si puedo verlos, los servidores y la consulta son:
        - mail2.redes.unlp.edu.ar ; mail.redes.unlp.edu.ar
        - host -t MX redes.unlp.edu.ar
- Servidores de DNS del dominio redes.unlp.edu.ar.
    - Con nslookup no me deja ver los servidores DNS, la consulta sería:
        - nslookup; set_type=NS; redes.unlp.edu.ar
    - Con host si puedo verlos, los servidores DNS y la consulta son:
        - ns-sv-b.redes.unlp.edu.ar; ns-sv-a.redes.unlp.edu.ar
        - host -t NS redes.unlp.edu.ar

- El comando nslookup sirve para hacer consultas DNS, puede buscar información sobre un dominio (dirección IP, servidor de correo electrónico, etc.), puede resolver problemas de red, para verificar la actividad de un servidor DNS.
- El comando host sirve para obtener información sobre nombres de dominio, direcciones IP, parsearlos. También puede consultar por registros específicos, hacer el parseo inverso, diagnosticar problemas de DNS, verificar la configuración de un dominio y la disponibilidad de un servidor.

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

- //CONSULTAR
- Es un archivo de texto plano que se usa para asociar nombres de host con direcciones IP. En una solicitud, el SO busca en el archivo correspondiente para determinar si la dirección IP correspondiente a un nombre de host se encuentra en el archivo, si es ese el caso, el SO usa esa información para realizar la solicitud sin tener que consultar los servidores DNS externos, caso contrario consulta a los servidores para obtener la dirección IP

## 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.

- No tuve diferencias entre ambas cosas //CONSULTAR

## 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?

- //CONSULTAR
- Las respuestas que realiza una PC a su Resolver son recursivas.

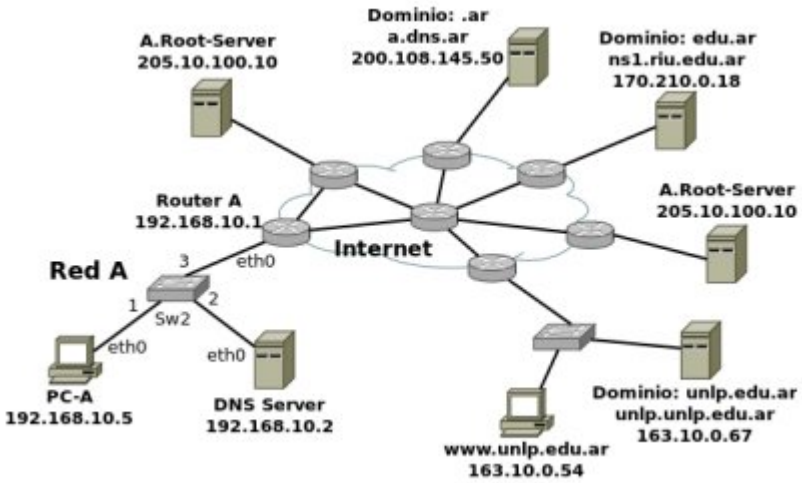
b. ¿Qué tipo de consultas (iterativas o recursivas) realiza el servidor de DNS para resolver requerimientos de usuario como el anterior? ¿A quién le realiza estas consultas?

- La PC le envía todas sus consultas al servidor DNS local.
- El servidor local (si no tiene las respuestas en caché) consulta a un servidor root.
- El servidor root no funciona para consultas iterativas, por lo cuál le brinda información del NS del dominio que está consultando.
- El servidor local le envía su consulta al servidor DNS obtenido. Si ese servidor DNS es autoritativo para el dominio consultado, podría obtener la información buscada, sino (si se trata de un sub-dominio):
    - Si el servidor DNS consultado acepta recursión, el hace todas las consultas y me retorna lo que consulto.
    - Sino, me da el NS del servidor DNS siguiente hasta encontrar la información solicitada.

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

- No, ya que sin DNS no podría obtener las direcciones IP de los hosts con los cuáles me quiero comunicar.
- Antes de hacer el requerimiento HTTP, se toma el nombre de host del receptor y se consulta su dirección IP. Una vez encontrada, se continua con HTTP.

# 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.

- PC-A solicita a DNS Server la dirección IP de www.unlp.edu.ar
- DNS Server (Si no tuviera la respuesta en caché) le consulta al A.root-server
- El A.Root-Server le devuelve al DNS server el registro NS del servidor autoritativo para el dominio .ar (a.dns.ar)
- DNS Server se comunica con a.dns.ar (asumo que las consultas son iterativas). a.dns.ar le brinda el nombre del servidor autoritativo para el sub-dominio edu.ar (edu.ar)
- DNS Server se comunica con ns1.riu.edu.ar, el cuál responde con el ns del sub-dominio unlp.edu.ar
- DNS Server se comunica con unlp.unlp.edu.ar y obtiene la dirección IP de www.unlp.edu.ar (163.10.0.54)

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

- La consulta es recursiva por parte de DNS Server a PC-A
- La consulta es iterativa de A.Root-Server a DNS Server.
- Después depende, yo asumí que las consultas de los otros servidores autoritativos de los dominios son iterativas (podrían no serlo, podrían ser en algunos).

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

- Si hago una consulta a www.google.com, la respuesta es un SOA, el cuál me da el nombre del servidor autoritativo para esa zona (ns1.google.com).
- Ahora con dig → dig @ns1.google.com www.google.com

## 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?

- No lo podría hacer, ya que ns1.google.com no es ni autoritativo para info.unlp.edu.ar ni es un Resolver que resuelva las consultas de los hosts.
- Para 8.8.8.8 si se podría hacer, ya que ese es un servidor (provisto por google) Resolver el cuál puede responder las consultas DNS de los hosts.

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

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

```
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 MX10 srv01.ejemplo.com.
8   ejemplo.com. 1634 IN MX 5 srv00.ejemplo.com.
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
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

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

- Como el flag aa no está activado, la respuesta no es autoritativa.
- En la sección de *Authority*, obtenemos los NS del dominio, podríamos consultarle a dichos servidores para tener una respuesta autoritativa.

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

- La consulta fue recursiva, lo podemos comprobar porque el flag rd (Recursion Desired) está activado.
- La respuesta también lo fue, porque el flag ra (Recursion Admited) está activado.

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

- Eso representa la prioridad que tienen los servidores de correo del dominio. Los servidores con menor número son los que más prioridad tienen (en este caso, el servidor srv00.ejemplo.com es el que más prioridad tiene).