**Práctica 3 - Capa de Aplicación**

**DNS (Domain Name Server)**

**Introducción**

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

El Sistema de Nombres de Dominio o DNS (por su sigla en inglés) permite asociar cada dirección IP - identificador numérico que posee cada dispositivo conectado a la red - con un nombre que sea más fácil de recordar: un nombre de dominio.

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

Los ROOT SERVER almacenan información sobre dónde encontrar los servidores de nombres de los dominios de nivel superior (TLD), como “.com”, “.net”, “.org”, y códigos de países como “.ar”.

Los “gTLD” o Dominios de Nivel Superior Genéricos, de tres o más letras (‘.com’, ‘.musica’, etc.)

1. ¿Qué es una respuesta del tipo autoritativa?

Una respuesta autoritativa es una respuesta que proviene directamente de un servidor DNS que tiene autoridad sobre el dominio consultado. Esto significa que el servidor posee la información oficial y original sobre el dominio solicitado, en lugar de obtenerla de la caché o de otros servidores intermedios.

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

Recursiva: El servidor DNS al que consultas (normalmente uno configurado por tu proveedor de internet) se encarga de obtener la respuesta completa para ti. Si no tiene la respuesta almacenada en caché, contactará con otros servidores en tu nombre.

Iterativa: En este caso, el servidor DNS responde con la mejor información que tiene, como la dirección de otro servidor DNS más cercano al dominio que buscas. Luego, el cliente es responsable de seguir consultando a esos servidores uno por uno hasta llegar al servidor autoritativo que puede resolver la consulta.

Ejemplo práctico:

Recursiva: Pides la dirección IP de “www.ejemplo.com”. El servidor DNS realiza todo el trabajo (consulta a un servidor raíz, luego al TLD y finalmente al autoritativo) y te da la respuesta final.

Iterativa: Pides lo mismo, pero el servidor inicial solo te dice “pregunta al servidor X” (por ejemplo, el servidor del TLD “.com”), y luego tú sigues preguntando hasta llegar al servidor autoritativo.

1. ¿Qué es el resolver?

Un resolver es el componente (normalmente parte del sistema operativo o del proveedor de internet) que toma las consultas de nombres de dominio y se encarga de obtener la IP correspondiente, haciendo consultas DNS recursivas si es necesario. Suele ser el primer paso en la cadena de resolución.

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

|  |  |
| --- | --- |
| a. A | f. NS |
| b. MX | g. CNAME |
| c. PTR | h. SOA |
| d. AAAA | i. TXT |

e. SRV

a. **A**: Asocia un nombre de dominio a una dirección IPv4.  
b. **MX**: Define los servidores de correo electrónico para el dominio.  
c. **PTR**: Asocia una dirección IP a un nombre de dominio (resolución inversa).  
d. **AAAA**: Igual que el registro A, pero para direcciones IPv6.  
e. **SRV**: Indica qué servicios están disponibles en un dominio y cómo acceder a ellos (usado por ejemplo en VoIP).  
f. **NS**: Especifica qué servidores de nombres (DNS) son responsables del dominio.  
g. **CNAME**: Alias para un dominio; redirige un nombre a otro.  
h. **SOA**: Contiene información sobre la zona del dominio, incluyendo el servidor primario, número de serie, y más.  
i. **TXT**: Almacena texto. Se usa comúnmente para verificaciones (como SPF, DKIM) y otros usos.

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

Para asegurar **redundancia y disponibilidad**. Si un servidor DNS falla, otros pueden responder, garantizando que el dominio siga siendo accesible.

1. 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?

El **servidor primario** es el que contiene la copia original y editable de los registros DNS. Los **secundarios** (o esclavos) replican esta información y la usan para responder consultas, mejorando rendimiento y disponibilidad.

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

Es el proceso por el cual un servidor DNS secundario copia la base de datos de zona desde el servidor primario. Sirve para mantener sincronizados los datos entre servidores.

1. 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.

Para delegar el control del dominio redes.unlp.edu.ar, hay que agregar **registros NS** apuntando a los servidores que administrará la Facultad de Redes.

Ejemplo:

redes.unlp.edu.ar. IN NS ns1.redes.unlp.edu.ar.

redes.unlp.edu.ar. IN NS ns2.redes.unlp.edu.ar.

1. Responda y justifique los siguientes ejercicios.
2. En la VM, utilice el comando dig para obtener la dirección IP del host www.redes.unlp.edu.ar y responda:

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

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

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44145

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

;; OPT PSEUDOSECTION:

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

; COOKIE: 071e2a554c5329730100000068000868265ab37f3e67a650 (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 Apr 16 16:43:36 -03 2025

;; MSG SIZE rcvd: 94

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

Si, la solicitud fue recursiva ya que en la flag se observa “rd” (recursión desired) y también fue recursiva la respuesta ya que se observa “ra” (recursión available).

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

Si, al aparecer el flag “aa” (authoritative answer) significa que es autoritativa.

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

La dirección IP del resolver es: “172.28.0.29” indicado por la anteúltima línea “SERVER”

1. ¿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?

;; ANSWER SECTION:

redes.unlp.edu.ar. 86400 IN MX 10 mail2.redes.unlp.edu.ar.

redes.unlp.edu.ar. 86400 IN MX 5 mail.redes.unlp.edu.ar.

Los servidores de correo del dominio “REDES.UNLP.EDU.AR” son:

* mail2.redes.unlp.edu.ar
* mail.redes.unlp.edu.ar

Los numeros (5, 10) son prioridad, mientras menor sea el numero, mayor prioridad.

El correo se intentara entregar primero a “mail.redes.unlp.edu.ar”, luego, si este servidor no responde, se intenta con “mail2.redes.unlp.edu.ar”

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

;; 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

Los servidores de DNS del dominio redes.unlp.edu.ar son:

* ns-sv-b.redes.unlp.edu.ar
* ns-sv-a.redes.unlp.edu.ar

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

Al repetir la consulta varias veces, el orden de los NS cambia. Esto se debe a que el protocolo DNS no garantiza un orden fijo en la respuesta. Esta rotación sirve para balancear la carga y mejorar la distribución de las consultas entre los servidores disponibles.

1. 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 es posible determinar cuál es el servidor DNS primario únicamente con la salida de los registros NS, ya que esta lista muestra todos los servidores autorizados sin indicar jerarquía.  
Para saber cuál es el servidor primario se debe consultar el registro SOA del dominio, el cual contiene explícitamente el nombre del servidor maestro.

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

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

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

El servidor DNS primario es: “ns-sv-b.redes.unlp.edu.ar”

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

El numero de serie es: “2020031700”

Este número sigue la convención **AAAAMMDDnn** (Año, Mes, Día, número de edición en el día).  
En este caso:

* **2020**: Año
* **03**: Marzo
* **17**: Día 17
* **00**: Primera versión del día

Se utiliza para que los servidores secundarios (slaves) sepan **cuándo deben actualizar sus datos**.  
Si el número cambia, significa que la zona fue modificada y deben sincronizarse.

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

El valor del segundo campo es: “604800”

Este valor representa el **Refresh**:  
**Cada cuánto tiempo (en segundos) el servidor secundario consulta al primario para ver si hay actualizaciones.**

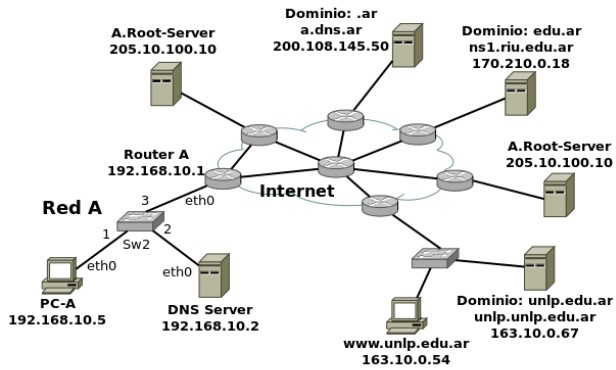
Eso significa que los servidores secundarios preguntan al primario **una vez por semana** si hubo cambios en la zona.

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

1. Indique qué valor tiene el registro TXT para el nombre saludo.redes.unlp.edu.ar. Investigue para qué es usado este registro.
2. Utilizando dig, solicite la transferencia de zona de redes.unlp.edu.ar, analice la salida y responda.
3. ¿Qué significan los números que aparecen antes de la palabra IN?

¿Cuál es su finalidad? 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?

1. 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).
2. 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?
3. Investigue los comandos nslookup y host. ¿Para qué sirven? Intente con ambos comandos obtener:
   * + - Dirección IP de www.redes.unlp.edu.ar.
       - Servidores de correo del dominio redes.unlp.edu.ar.
       - Servidores de DNS del dominio redes.unlp.edu.ar.
4. ¿Qué función cumple en Linux/Unix el archivo /etc/hosts o en Windows el archivo \WINDOWS\system32\drivers\etc\hosts?
5. 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.
6. 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:
   * 1. ¿Qué tipo de consultas (iterativas o recursivas) realiza la PC a su servidor de DNS?
     2. ¿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?
7. Relacione DNS con HTTP. ¿Se puede navegar si no hay servicio de DNS?
8. Observar el siguiente gráfico y contestar:



* + 1. Si la PC-A, que usa como servidor de DNS a "DNS Server", desea obtener la IP de [www.unlp.edu.ar](http://www.unlp.edu.ar/), cuáles serían, y en qué orden, los pasos que se ejecutarán para obtener la respuesta.
    2. ¿Dónde es recursiva la consulta? ¿Y dónde iterativa?

1. ¿A quién debería consultar para que la respuesta sobre www.google.com sea autoritativa?
2. ¿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?

**Ejercicio de parcial**

1. 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 ;; AUTHORITY SECTION: | \_\_ | 5 srv00.ejemplo.com. | (2) |
| 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 ;; ADDITIONAL SECTION: | \_\_ | ss03.ejemplo.com. |  |
| 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 |  |

* 1. Complete las líneas donde aparece \_\_ con el registro correcto.
  2. ¿Es una respuesta autoritativa? En caso de no serlo, ¿a qué servidor le preguntaría para obtener una respuesta autoritativa?
  3. ¿La consulta fue recursiva? ¿Y la respuesta?
  4. ¿Qué representan los valores 10 y 5 en las líneas (1) y (2).