# Práctica 3

Capa de Aplicación – DNS

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

El sistema de nombres de dominio (DNS, por sus siglas en inglés, 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 asignado a cada uno de los participantes. Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

Está compuesto por tres partes con funciones bien diferenciadas.

- Cliente DNS: está instalado en el cliente (es decir, nosotros) y realiza peticiones de resolución de nombres a los servidores DNS.
- Servidor DNS: son los que contestan las peticiones y resuelven los nombres mediante un sistema estructurado en árbol. Las direcciones DNS que ponemos en la configuración de la conexión, son las direcciones de los Servidores DNS.
- Zonas de autoridad: son servidores o grupos de ellos que tienen asignados resolver un conjunto de dominios determinado (como los .es o los .org).

El Sistema de Nombres de Dominio o DNS es un sistema de nomenclatura jerárquico que se ocupa de la administración del espacio de nombres de dominio (Domain Name Space). Su labor primordial consiste en resolver las peticiones de asignación de nombres.
Para ello, el sistema de nombres de dominio recurre a una red global de servidores DNS, que subdividen el espacio de nombres en zonas administradas de forma independiente las unas de las otras. Esto permite la gestión descentralizada de la información de los dominios.

Cada vez que un usuario registra un dominio, se crea una entrada WHOIS en el registro correspondiente y esta queda almacenada en el DNS como un “resource record”. La base de datos de un servidor DNS se convierte, así, en la compilación de todos los registros de la zona del espacio de nombres de dominio que gestiona.

Cuando se introduce la dirección de una página web (URL) en el campo de búsqueda del navegador, este realiza una petición al llamado resolver, un componente especial del sistema operativo cuya función consiste en almacenar en caché direcciones IP ya solicitadas anteriormente, y proporcionarlas cuando la aplicación cliente (navegador, programa de correo) la solicita. Si la

dirección IP solicitada no se encuentra en el caché del resolver, este redirige la petición al servidor DNS que corresponda, que, en general, se trata del servidor DNS del proveedor de Internet. Aquí se coteja la petición con la base de datos del DNS y, si está disponible, se envía la dirección IP correspondiente como respuesta (“forward lookup”). Esta permite al navegador del usuario dirigirse al servidor web deseado en Internet. Otra vía alternativa consiste en el camino inverso, es decir, en traducir la dirección IP en la dirección de dominio (“reverse lookup”).

Si un servidor DNS no puede responder a una petición con la información de que dispone en su base de datos, puede solicitar la información a otro servidor o reenviar la petición al servidor DNS que corresponda. Esta resolución se puede realizar de dos formas:

- Resolución recursiva: es la que se produce cuando el servidor DNS no puede responder por sí mismo a una petición y toma la información de otro servidor. El resolver transfiere la petición completa a su servidor DNS, que proporciona a su vez la respuesta al resolver con el nombre de dominio, si se ha resuelto.
- Resolución iterativa: cuando el servidor DNS no puede resolver la petición, envía como respuesta la dirección del siguiente servidor DNS de la jerarquía. El resolver tiene que enviar él mismo una nueva petición y repetir la maniobra hasta que se resuelve el nombre de dominio.

La administración centralizada de la información de los dominios en el DNS se caracteriza por un índice elevado de fiabilidad y flexibilidad. Si la dirección IP de un servidor cambia, el usuario no suele percibir nada, ya que la dirección IP actual para el dominio correspondiente se guarda en la base de datos.

---

Primero el ordenador revisa su propio caché de DNS en busca de la dirección IP (si ya has entrado antes a un sitio, la segunda siempre es más rápida porque queda almacenado en la memoria caché o temporal), si no la consigue se reenvía la petición al servidor de DNS local (este es usualmente el de tu ISP si nunca lo has cambiado).

Ahora los servidores DNS locales verifican su propia caché para buscar la dirección IP y comprobar si ya conocen la respuesta, y si no lo consiguen entonces reenvían la petición a los servidores raíz del dominio (esto es lo que se conoce como búsqueda recursiva), y estos responden con la información.

Luego el servidor DNS local reenvía la información que obtuvo de los servidores raíz con la dirección IP para el host, y almacena en caché la información para el futuro. La computadora del usuario hace lo mismo, y por último el navegador genera una petición HTTP al servidor WWW de unsitiowebcualquiera.com localizado en la dirección IP 001.000.000.111. El servidor WWW responde la petición y le envía la página web al usuario.

2. ¿Qué es un root server? ¿Qué es un generic top-level domain (gtld)?
Un servidor raíz (root server en inglés) es un servidor de nombres para la zona raíz del Sistema de nombres de dominio de Internet(DNS).1 Los servidores de nombres raíz son una parte fundamental

de Internet, ya que son el primer paso en la traducción (resolución) de los nombres de host legibles por humanos en direcciones IP que se utilizan en la comunicación entre los hosts de Internet.
Los Root Servers son los servidores DNS principales de todo el mundo, estos se encargan de resolver las peticiones DNS para los dominios de más alto nivel. Existen 13 Root Serverdistribuidos en varios puntos del planeta, principalmente en Estados Unidos.

Dada una consulta de cualquier dominio, el servidor raíz proporciona al menos el nombre y la dirección del servidor autorizado de la zona de más alto nivel para el dominio buscado. De manera que el servidor del dominio proporcionará una lista de los servidores autorizados para la zona de segundo nivel, hasta obtener una respuesta razonable.

Los gTLD son los dominios de primer nivel genéricos (Generic Top Level Domain). Entre ellos figuran los ".com", ".info", ".org" o ".net". En este tipo se incluyen los dominios patrocinados (sTLD ó sponsored Top Level Domain), que impulsan colectivos determinados. Como ejemplo de ellos se pueden citar los ".cat", ".museum" o ".aero".

Los gTLD deben tener un mínimo de tres caracteres y no están asociados a países. Su gestión corre a cargo de organismos internacionales como la Corporación de Internet para la Asignación de Nombres y Números (ICANN).

El segundo gran grupo de dominios son los ccTLD (country code Top Level Domain) o dominios de primer nivel de código de país, que actualmente rozan los 300.

3. ¿Qué es una respuesta del tipo autoritativa?
Una respuesta con autoridad viene de un servidor de nombres que se considera autorizado para el dominio, que es la devolución de un registro (uno de los servidores de nombres en la lista para el dominio que usted hizo una búsqueda).

Authoritative Answer significa que la respuesta DNS se ha producido desde el servidor DNS que tiene todo el archivo de información disponible para esa zona.

Non Authoritative Answer significa que la respuesta DNS se ha producido desde un servidor DNS que tiene en caché una copia de las consultas realizadas para esa zona, al servidor que tiene la Autoridad para responder (el que tiene el archivo de zona). Por esto veremos muy a menudo la respuesta desde servidores que son Non Authoritative.

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

Las resoluciones iterativas consisten en la respuesta completa que el servidor de nombres pueda dar. El servidor de nombres consulta sus datos locales (incluyendo su caché) buscando los datos solicitados. El servidor encargado de hacer la resolución realiza iterativamente preguntas a los diferentes DNS de la jerarquía asociada al nombre que se desea resolver, hasta descender en ella hasta la máquina que contiene la zona autoritativa para el nombre que se desea resolver.

En las resoluciones recursivas, el servidor no tiene la información en sus datos locales, por lo que busca y se pone en contacto con un servidor DNS raíz, y en caso de ser necesario repite el mismo proceso básico (consultar a un servidor remoto y seguir a la siguiente referencia) hasta que obtiene la mejor respuesta a la pregunta.

Cuando existe más de un servidor autoritario para una zona, BIND utiliza el menor valor en la métrica RTT (tiempo de ida y vuelta) para seleccionar el servidor. El RTT es una medida para determinar cuánto tarda un servidor en responder una consulta.

El proceso de resolución normal se da de la siguiente manera:

1.El servidor A recibe una consulta iterativa desde el cliente DNS.
2.El servidor A envía una consulta iterativa a B.
3.El servidor B refiere a A otro servidor de nombres, incluyendo a C.
4.El servidor A envía una consulta iterativa a C.
5.El servidor C refiere a A otro servidor de nombres, incluyendo a D.
6.El servidor A envía una consulta iterativa a D.
7.El servidor D responde.
8.El servidor A regresa la respuesta al resolver.
9.El servidor entrega la resolución al programa que solicitó la información.

---

Una consulta recursiva obliga a un servidor DNS para responder a una solicitud con un error o una respuesta de éxito. Los clientes DNS (resoluciones) normalmente realizan consultas recursivas. Con una consulta recursiva, 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 DNS
Cuando un servidor DNS procesa una consulta recursiva y la consulta no se puede resolver desde datos locales (archivos de zona local o caché de consultas anteriores), la consulta recursiva debe trasladarse a un servidor DNS raíz. Cada aplicación basada en estándares de DNS incluye un archivo de caché o sugerencias del servidor raíz que contiene entradas para los servidores DNS de raíz de los dominios de Internet.

Una consulta iterativa es uno en el que 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. Esta respuesta es también conocida como una remisión, si el servidor DNS no está autorizado para el nombre. Si un servidor DNS no tiene ninguna información local que puede responder la consulta, simplemente envía una respuesta negativa.

5. ¿Qué es el resolver?

Un resolver es una parte del sistema operativo que se encarga de realizar las consultas a un servidor DNS, interpretarlas y devolverlas al programa que ha efectuado la consulta. Los servidores DNS también pueden incorporar un resolver, que gestiona las consultas que un servidor DNS debe hacer. Un resolver siempre suele hacer consultas recursivas exclusivamente.

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

A = Dirección (address). Este registro se usa para traducir nombres de servidores de alojamiento a direcciones IPv4.

AAAA = Dirección (address). Este registro se usa en IPv6 para traducir nombres de hosts a direcciones IPv6.

CNAME = Nombre canónico (canonical Name). Se usa para crear nombres de servidores de alojamiento adicionales, o alias, para los servidores de alojamiento de un dominio. Es usado cuando se están corriendo múltiples servicios (como FTP y servidor web) en un servidor con una sola dirección IP. Cada servicio tiene su propia entrada de DNS (como `ftp.ejemplo.com.` y `www.ejemplo.com.`). Esto también es usado cuando corres múltiples servidores HTTP, con diferentes nombres, sobre el mismo host. Se escribe primero el alias y luego el nombre real. Ej. `Ejemplo1 IN CNAME ejemplo2`

NS = Servidor de nombres (name server). Define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información de dicho dominio. Cada dominio se puede asociar a una cantidad cualquiera de servidores de nombres.

MX = Intercambio de correo (mail exchange). Asocia un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio. Tiene un balanceo de carga y prioridad para el uso de uno o más servicios de correo.

PTR = Indicador (pointer). También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio. Se usa en el archivo de configuración de la zona DNS inversa.

SOA = Autoridad de la zona (start of authority). Proporciona información sobre el servidor DNS primario de la zona.

ANY = Toda la información de todos los tipos que exista. (No es un tipo de registro, sino un tipo de consulta)

TXT = Registro de texto. Originalmente para arbitrario humano-texto legible en un DNS registro.

SRV = Localizador de Servicios. Registro de ubicación de servicio generalizado, utilizado para protocolos más nuevos en vez de crear protocolo-registros concretos como MX.

7. En la VM, utilice el comando dig para obtener la dirección IP del host www.redes.unlp.edu.ar. Responda:

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

La consulta fue recursiva y autoritativa. Esto significa que el servidor DNS local al que le hicimos la consulta tenía registros con información del sitio www.redes.unlp.edu.ar y fue recursiva porque es nuestro servidor DNS local al que le delegamos la responsabilidad de hacer las consultas iterativas extras necesarias para poder traducir el host en una dirección IP.

En los flags de respuesta nos dice si la respuesta fue autoritativa o recursiva.

Flag aa: authoritative answer.

Flag ra: recursive available.

b. ¿Puede indicar si se trata de una respuesta autoritativa?

En la parte de la respuesta, hay que chequear la respuesta con el registro NS, ya que el registro de tipo NS almacena quien es el servidor que almacena el registro (A) con la correspondencia entre nombre de host y dirección IP.

c. ¿Cuál es la dirección IP del servidor de DNS al que le realizó la consulta? ¿Cómo lo sabe?

Se indica en los detalles de la consulta.
En la parte de SERVER aclara a que server nuestra computadora le hizo la solicitud recursiva, y si se quiere utilizar un server distinto se puede hacer añadiendo al final del comando @IP. Ejemplo: dig google.com. @216.221.235.12.

d. ¿Es posible obtener la misma información con el comando host? ¿Cómo?

Es posible obtener esta misma informción con el comando host, simplemente se añade el parametro -v (host -v www.redes.unlp.edu.ar) .

Dig nos presenta por consola la información dividida en secciones:

- **Got Answer.** En esta sección nos dan información acerca de la consulta realizada. Mención especial hay que hacer a la sección **flags**.
- **Flags:**
  - QR (Query/Response): Informa de que el mensaje es de respuesta.
  - RD (Recursion Desired): Informa de que queremos que en caso de no resolver la consulta en el servidor inicial seguirá realizando consultas recursivamente a otros.
  - RA (Recursion Allowed): Informa de que pedimos al servidor que consulte recursivamente a otros servidores de darse el caso de no ser capaz de resolver una consulta. El server puede aceptar o no.
  - AA: Informa de que es una respuesta autorizada.
  - TC (Truncated Response),Informa de que la respuesta se ha truncado por ser demasiado grande.
  - AD (Authentic Data): Informa de que los datos incluidos en la respuesta han sido verificados por el servidor que nos la ha devuelto.
  - CD (Checking Disabled): Informa de que una consulta con los datos sin verificar es valida.
- **Question Section.** En esta sección se nos muestra la consulta realizada. Consta de tres partes
  - El dominio consultado
  - Ámbito donde se realiza la consulta. Normalmente tiene el valor IN que representa a Internet.
  - Registros consultados. Estos registros pueden ser:
    - A: IPv4 de un dominio
    - ANY: Cualquier tipo de registro
    - AAAA: IPv6 de un dominio
    - CNAME: Alias de host
    - MX: Servidores de correo
    - NS: Servidores de nombres
    - TXT: Texto, se utiliza para configurar SPF
    - SOA: Servidor autorizado para el dominio
- **Answer Section.** En esta sección se nos muestra la respuesta a nuestra consulta. En el caso de que haya uno o varios alias especificados para nuestra consulta, dig seguira consultando a los alias hasta llegar al registro A.

•**Authority Section.** En esta sección se nos muestra información de los servidores de nombres autorizados para una determinada zona.

•**Additional Section.** Es en esta sección donde se nos mostrara las IP's de los servidores de nombres mostrados en la **Authority Section.**

•**Detalles de la consulta.**en esta sección se nos muestran datos sobre como se ha realizado la consulta:

•Tiempo en realizar la consulta

•Server y puerto al que se ha realizado la consulta

•Cuando se ha realizado la consulta

•Tamaño del mensaje recibido

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

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> www.redes.unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63083
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.redes.unlp.edu.ar.          IN      A

;; ANSWER SECTION:
www.redes.unlp.edu.ar.  604800  IN      A       172.28.0.50

;; AUTHORITY SECTION:
redes.unlp.edu.ar.604800  IN      NS      ns.redes.unlp.edu.ar.

;; ADDITIONAL SECTION:
ns.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 Mar 27 22:03:20 GMT 2018
;; MSG SIZE  rcvd: 99
```

8. Usando el comando dig, averigüe la dirección IP de www.google.com. Observe los números que aparecen antes de la palabra IN. Vuelva a ejecutar la misma consulta y observe nuevamente esos números. ¿Qué ocurrió? ¿Por qué? ¿Qué significado cree que tienen dichos números?El valor se decremento.
Ese valor es el tiempo que la respuestas va a ser almacenadas en cache, antes de tener que volver a pedirlas a los servidores autoritativos.

```
redes@redes:~$ dig www.google.com

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64409
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.         300     IN      A       172.217.30.164

;; AUTHORITY SECTION:
google.com.             172799 IN       NS      ns4.google.com.
google.com.             172799 IN       NS      ns2.google.com.
google.com.             172799 IN       NS      ns1.google.com.
google.com.             172799 IN       NS      ns3.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         172799 IN       A       216.239.32.10
ns1.google.com.         172799 IN       AAAA    2001:4860:4802:32::a
ns2.google.com.         172799 IN       A       216.239.34.10
ns2.google.com.         172799 IN       AAAA    2001:4860:4802:34::a
ns3.google.com.         172799 IN       A       216.239.36.10
ns3.google.com.         172799 IN       AAAA    2001:4860:4802:36::a
ns4.google.com.         172799 IN       A       216.239.38.10
ns4.google.com.         172799 IN       AAAA    2001:4860:4802:38::a

;; Query time: 405 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Tue Mar 27 22:04:12 GMT 2018
;; MSG SIZE  rcvd: 307

redes@redes:~$ dig www.google.com

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17103
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.         275     IN      A       172.217.30.164

;; AUTHORITY SECTION:
google.com.             172774 IN       NS      ns3.google.com.
google.com.             172774 IN       NS      ns1.google.com.
google.com.             172774 IN       NS      ns2.google.com.
```

```
google.com.             172774 IN       NS      ns4.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         172774 IN       A       216.239.32.10
ns1.google.com.         172774 IN       AAAA    2001:4860:4802:32::a
ns2.google.com.         172774 IN       A       216.239.34.10
ns2.google.com.         172774 IN       AAAA    2001:4860:4802:34::a
ns3.google.com.         172774 IN       A       216.239.36.10
ns3.google.com.         172774 IN       AAAA    2001:4860:4802:36::a
ns4.google.com.         172774 IN       A       216.239.38.10
ns4.google.com.         172774 IN       AAAA    2001:4860:4802:38::a

;; Query time: 1 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Tue Mar 27 22:04:37 GMT 2018
;; MSG SIZE  rcvd: 307
```

9. Observe nuevamente las respuestas del paso anterior, ¿el orden de los servidores en la respuesta es siempre el mismo? ¿Por qué piensa que sucede esto?

No es el mismo orden de los servidores, esto se hace para balancear la carga de pedidos a los distintos servidores, y no saturar a ninguno.

10. Utilizando el comando dig responda (debe tener conexión a Internet para realizar este ejercicio):
a. Cantidad de servidores que aceptan correos para el dominio gmail.com.

Hay 5 servidores que haceptan los mail de gmail.

b. Cuándo se envía un correo a una cuenta gmail.com, ¿cuál de los servidores recibirá el correo? Justifique.

gmail-smtp-in.l.google.com. es el encargado de recibir los mail, se indica en el valor que aparece antes del nombre, siendo el de menor numero el de mayor prioridadd.

c. ¿En qué ocasión los demás servidores de correo recibirían correos dirigidos al dominio gmail.com? ¿Qué sucede luego de que uno de estos servidores recibe algún correo para el mencionado dominio?

Si el servidor primario no puede recibir el mail, este se envia a alguno de los secundarios que este disponible, intentando según la prioridad. Cuando el servidor primario se vuelva a habilitar, los otros servidores les envian los mail que habian recibido.

d. Cantidad de servidores de DNS del dominio unlp.edu.ar.

dig -t ns info.unlp.edu.ar

anubis.unlp.edu.ar.
ns1.riu.edu.ar.
unlp.unlp.edu.ar.

e. Dirección IP del host www.info.unlp.edu.ar.

163.10.5.71

```
redes@redes:~$ dig -t mx gmail.com

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> -t mx gmail.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50407
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;gmail.com.                     IN      MX

;; ANSWER SECTION:
gmail.com.              3600    IN      MX      30 alt3.gmail-smtp-in.l.google.com.
gmail.com.              3600    IN      MX      20 alt2.gmail-smtp-in.l.google.com.
gmail.com.              3600    IN      MX      40 alt4.gmail-smtp-in.l.google.com.
gmail.com.              3600    IN      MX      5 gmail-smtp-in.l.google.com.
gmail.com.              3600    IN      MX      10 alt1.gmail-smtp-in.l.google.com.

;; AUTHORITY SECTION:
gmail.com.              172800  IN      NS      ns4.google.com.
gmail.com.              172800  IN      NS      ns2.google.com.
gmail.com.              172800  IN      NS      ns1.google.com.
gmail.com.              172800  IN      NS      ns3.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.                 172647  IN      A       216.239.32.10
ns1.google.com.                 172647  IN      AAAA    2001:4860:4802:32::a
ns2.google.com.                 172647  IN      A       216.239.34.10
ns2.google.com.                 172647  IN      AAAA    2001:4860:4802:34::a
ns3.google.com.                 172647  IN      A       216.239.36.10
ns3.google.com.                 172647  IN      AAAA    2001:4860:4802:36::a
ns4.google.com.                 172647  IN      A       216.239.38.10
ns4.google.com.                 172647  IN      AAAA    2001:4860:4802:38::a

;; Query time: 354 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Tue Mar 27 22:06:44 GMT 2018
;; MSG SIZE  rcvd: 409
```

11. Investigue los comando nslookup y host. ¿Para qué sirven? Intente con ambos comandos obtener:
Dirección IP de www.redes.unlp.edu.ar.

```
redes@redes:~$ nslookup www.redes.unlp.edu.ar
Server:         172.28.0.29
Address:        172.28.0.29#53
Name: www.redes.unlp.edu.ar
Address: 172.28.0.50
```

```
redes@redes:~$ host  www.redes.unlp.edu.ar.
www.redes.unlp.edu.ar has address 172.28.0.50
```

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

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

Acerca de nslookup
El comando nslookup se utiliza para consultar los servidores de nombres de Internet de forma interactiva para obtener información. nslookup , que significa "servidor de nombres de búsqueda", es una herramienta útil para encontrar información sobre un dominio con nombre.
De forma predeterminada, nslookup traducirá un nombre de dominio a una dirección IP (o viceversa). Por ejemplo, para averiguar cuál es la dirección IP de microsoft.com , puede ejecutar el comando:
nslookup microsoft.com

COMANDO host:
El comando host se usa para encontrar la dirección IP del dominio dado y también muestra el nombre de dominio para la IP dada.

a.

Host funciona de manera similar a dig, para averiguar los servidores de correo electrónico de un dominio, por ejemplo de google, se utiliza host -t mx google.com.
Para los servidores DNS funciona de manera análoga al dig.

```
redes@redes:~$ host www.redes.unlp.edu.ar
www.redes.unlp.edu.ar has address 172.28.0.50

redes@redes:~$ host -t MX www.redes.unlp.edu.ar
www.redes.unlp.edu.ar has no MX record

redes@redes:~$ host -t MX gmail.com
gmail.com mail is handled by 20 alt2.gmail-smtp-in.l.google.com.
gmail.com mail is handled by 30 alt3.gmail-smtp-in.l.google.com.
gmail.com mail is handled by 5 gmail-smtp-in.l.google.com.
gmail.com mail is handled by 10 alt1.gmail-smtp-in.l.google.com.
gmail.com mail is handled by 40 alt4.gmail-smtp-in.l.google.com.

*************************

redes@redes:~$ nslookup -type=mx gmail.com
Server:         172.28.0.29
Address:    172.28.0.29#53

Non-authoritative answer:
gmail.com   mail exchanger = 20 alt2.gmail-smtp-in.l.google.com.
gmail.com   mail exchanger = 5 gmail-smtp-in.l.google.com.
gmail.com   mail exchanger = 10 alt1.gmail-smtp-in.l.google.com.
gmail.com   mail exchanger = 30 alt3.gmail-smtp-in.l.google.com.
gmail.com   mail exchanger = 40 alt4.gmail-smtp-in.l.google.com.

Authoritative answers can be found from:
gmail.com   nameserver = ns2.google.com.
gmail.com   nameserver = ns3.google.com.
gmail.com   nameserver = ns1.google.com.
gmail.com   nameserver = ns4.google.com.
ns1.google.com    internet address = 216.239.32.10
ns1.google.com    has AAAA address 2001:4860:4802:32::a
ns2.google.com    internet address = 216.239.34.10
```

```
ns2.google.com    has AAAA address 2001:4860:4802:34::a
ns3.google.com    internet address = 216.239.36.10
ns3.google.com    has AAAA address 2001:4860:4802:36::a
ns4.google.com    internet address = 216.239.38.10
ns4.google.com    has AAAA address 2001:4860:4802:38::a
```

```
redes@redes:~$ nslookup -type=mx www.redes.unlp.edu.ar
Server:         172.28.0.29
Address:        172.28.0.29#53

*** Can't find www.redes.unlp.edu.ar: No answer
```

12. ¿Qué función cumple en Linux/Unix el archivo /etc/hosts o en Windows el archivo \WINDOWS\sys-tem32\drivers\etc\hosts?

El fichero /etc/hosts

Este fichero se utiliza para obtener una relación entre un nombre de máquina y una dirección IP: en cada línea de /etc/hosts se especifica una dirección IP y los nombres de máquina que le corresponden, de forma que un usuario no tenga que recordar direcciones sino nombres de hosts. Habitualmente se suelen incluir las direcciones, nombres y aliases de todos los equipos conectados a la red local, de forma que para comunicación dentro de la red no se tenga que recurrir a DNS a la hora de resolver un nombre de máquina. El formato de una línea de este fichero puede ser el siguiente:
158.42.2.1 pleione pleione.cc.upv.es pleione.upv.es
Esta línea indica que será equivalente utilizar la dirección 158.42.2.1, el nombre de máquina pleione, o los aliases pleione.cc.upv.es y pleione.upv.es cuando queramos comunicarnos con este servidor:

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 diferentes 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, pero dejó de utilizarse cuando Internet empezó a crecer en nombres de dominio, pasando a usar servidores de resolución de DNS. 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.1 Este archivo es tradicionalmente llamado "hosts" y su ubicación depende del sistema operativo.

13. 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.

14. 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?

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 computadora realiza una consulta recursiva al resolver ya que le indicara que va esperar una respuesta de la resolución a IP. Este resolver o servidor DNS local va a tener que hacer consultas iterativas a los otros servidores DNS (en caso que no tenga la información solicitada en la caché), comenzando por un root server y pasando por gTLDs o ccTLDs hasta llegar a un servidor autoritativo que contenga el registro con la dirección efectiva del host solicitado.

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

DNS y HTTP son protocolos que se ejecutan en la capa de aplicación. Aunque ambos son muy importantes para el funcionamiento de Internet, proveen funcionalidades distintas. HTTP es el protocolo utilizado para recuperar documentos (páginas web o de otro tipo) en servidores. DNS traduce nombres de dominio en direcciones IP. En el momento en que un usuario escribe el nombre de un sitio en el navegador, el usuario esperaria que la página cargue. Para poder cargar la página, primero debe recuperarse y para eso se utiliza el protocolo HTTP. Antes de que se pueda enviar un mensaje HTTP al sitio para recuperar la página, primero es necesario averiguar la dirección IP del sitio, y para eso se utilizaria el servicio de traducción de direccion de host a direccion IP que provee DNS.
Sería posible navegar en Internet sin servicio DNS, pero sería necesario conocer de antemano las direcciones IP de los sitios que se desean visitar. Para esto se podría hacer como antes, que se agregaban las correspondencias entre nombre de host y dirección IP de manera manual al archivo hosts del sistema, o utilizar de forma directa la dirección IP.

16. 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.
b. ¿Dónde es recursiva la consulta? ¿Y dónde iterativa?

Asumiendo que DNS Server es el servidor DNS resolver de PC-A, entonces primero PC-A le haría una consulta recursiva pidiendo la direccion IP de www.unlp.edu.ar a DNS Server. Luego, DNS Server haría las consultas iterativas que hagan falta para resolver la petición. La primera de ellas sería al root server que tenga configurado, posiblemente el A, puesto que queda a un router de distancia menos que el B.Con la dirección IP del servidor DNS con autoridad sobre el dominio .ar, y luego de realizarle una consulta a este último recibiría la dirección IP del servidor DNS con autoridad sobre unlp.edu.ar.

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

Debería consultarle al servidor DNS de google. Para eso haria dig -t ns google.com.ar y luego un dig www.google.com.ar @(Dirección IP de algun servidor DNS que devolvió el comando anterior).

redes@redes:~$ dig www.google.com

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40712

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

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.         300     IN      A       172.217.30.164

;; AUTHORITY SECTION:
google.com.             171121  IN      NS      ns2.google.com.
google.com.             171121  IN      NS      ns3.google.com.
google.com.             171121  IN      NS      ns4.google.com.
google.com.             171121  IN      NS      ns1.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         171121  IN      A       216.239.32.10
ns1.google.com.         171121  IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         171121  IN      A       216.239.34.10
ns2.google.com.         171121  IN      AAAA    2001:4860:4802:34::a
ns3.google.com.         171121  IN      A       216.239.36.10
ns3.google.com.         171121  IN      AAAA    2001:4860:4802:36::a
ns4.google.com.         171121  IN      A       216.239.38.10
ns4.google.com.         171121  IN      AAAA    2001:4860:4802:38::a

;; Query time: 30 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Tue Mar 27 22:32:10 GMT 2018
;; MSG SIZE  rcvd: 307
```

18. ¿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 respondería ya que no tendría habilitada la recursión. Si la consulta se hiciera al servidor 8.8.8.8 sería posible, puesto que es un servidor DNS público al que se le pueden hacer consultas recursivas.

redes@redes:~$ dig www.info.unlp.edu.ar @216.239.32.10

```
; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> www.info.unlp.edu.ar @216.239.32.10
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 54241
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.info.unlp.edu.ar.          IN      A

;; Query time: 26 msec
;; SERVER: 216.239.32.10#53(216.239.32.10)
;; WHEN: Tue Mar 27 22:33:10 GMT 2018
;; MSG SIZE  rcvd: 38
```

```
redes@redes:~$ dig www.google.com @216.239.32.10

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> www.google.com @216.239.32.10
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53424
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.         300     IN      A       172.217.30.164

;; Query time: 28 msec
;; SERVER: 216.239.32.10#53(216.239.32.10)
;; WHEN: Tue Mar 27 22:33:21 GMT 2018
;; MSG SIZE  rcvd: 48

redes@redes:~$ dig www.info.unlp.edu.ar @8.8.8.8

; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> www.info.unlp.edu.ar @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26768
;; 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.   299     IN      A       163.10.5.71

;; Query time: 56 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Mar 27 22:33:44 GMT 2018
;; MSG SIZE  rcvd: 65
```

## Ejercicio de parcial

19. 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.
8  ejemplo.com. 1634 IN MX        5 srv00.ejemplo.com.
9
10  ;; AUTHORITY SECTION: 11 ejemplo.com. 92354 IN __ 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 __ 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

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, no esta el flag aa.

¿La consulta fue recursiva? ¿Y la respuesta?
Ambas fueron recursivas, ya que los flags rd (Recursion Desired) y ra (Recursion Allowed) estan activados.

¿Qué representan los valores 10 y 5 en las líneas 7 y 8.
Los valores de prioridad para recibir mails.