DFS. Zonzamas
UT6. Actividad 2
DNS en Linux

- **Objetivo general:** Configuración de BIND como servidor de DNS de una red privada.

- **Duración prevista:** 3 horas

- **Software:**
  - Distribución Ubuntu Server LTS

- **Mínimos que se persiguen en la actividad:**
  - Enumeración y reflexión sobre la utilidad de la utilización de DNS, así como de la evolución histórica de la resolución de nombres en INTERNET desde el fichero `/etc/hosts` hasta BIND 9.
  - Realización práctica de los distintos pasos en la configuración de clientes y servidores de DNS con BIND.
  - Conocimiento de los tipos básicos de servidores DNS: **maestro, esclavo y sólo-caché**.
  - Configuración de los ficheros /etc/resolv.conf y **`/etc/nsswitch.conf`, `/etc/hosts`.**
  - Comprensión del mecanismo de resolución de nombres. Autoridad.
  - Distinción entre **zona**, **dominio**, **subdominios**, **servidor de nombres**, **agente de resolución**, **resolución inversa** y **FQDN**.
  - Conocimiento práctico de los principales tipos de registros de recursos: SOA, A, AAAA, MX, NS, CNAME y PTR.
  - Utilización práctica de las utilidades de verificación: **dig, nslookup, named-checkconf, namedcheckzone** y **host**
  - Diferenciación entre DNS y BIND.

- **Documentación:**
  - **Linux Network Administrator's Guide (nag2.pdf)**
  - Bind 9 Administrator Reference Manual (http://www.isc.org/products/BIND)
  - Tutorial y apuntes en curso LPIC 2 en wiki
  - Tutoriales enlazados en aula virtual

- **Teoría:**

  La resolución de nombres es el proceso en virtud del cual un cliente pregunta a un servidor cuál es la dirección IP que corresponde a un nombre dado.

En sentido amplio la resolución de nombres no sólo se refiere a la resolución de nombres de hosts como el ejemplo dibujado arriba sino a cualquier resolución de nombres como por ejemplo:

- Nombres de redes que se corresponden con direcciones de redes (/etc/networks)
- Nombres de puertos que se corresponden con números de puertos (/etc/services)
- Nombres de cuentas de usuario que se corresponden con su **uid** (/etc/passwd)

En este documento nos centraremos en la resolución de nombres de hosts y sus direcciones IP. Uno de los primeras sistemas de resolución de nombres de INTERNET es el del fichero **`/etc/hosts`**, de tal manera que **cada equipo** tiene un fichero **`/etc/hosts`** con la correspondencia entre nombres de host y su dirección IP.

Este sistema funcionaba bien teniendo en cuenta que en los albores de INTERNET existían pocos ordenadores, de tal manera que cada cierto tiempo se actualizaba el fichero `/etc/hosts` de cada equipo de tal manera que todos los ordenadores de INTERNET tuvieran el mismo contenido.

Cuando el número de ordenadores de INTERNET aumentó este sistema se volvió poco adecuado. Por ello se creo el sistema DNS (Domain Name System) que consiste en una base de datos **distribuida** y **jerarquizada** para la resolución de nombres de host.

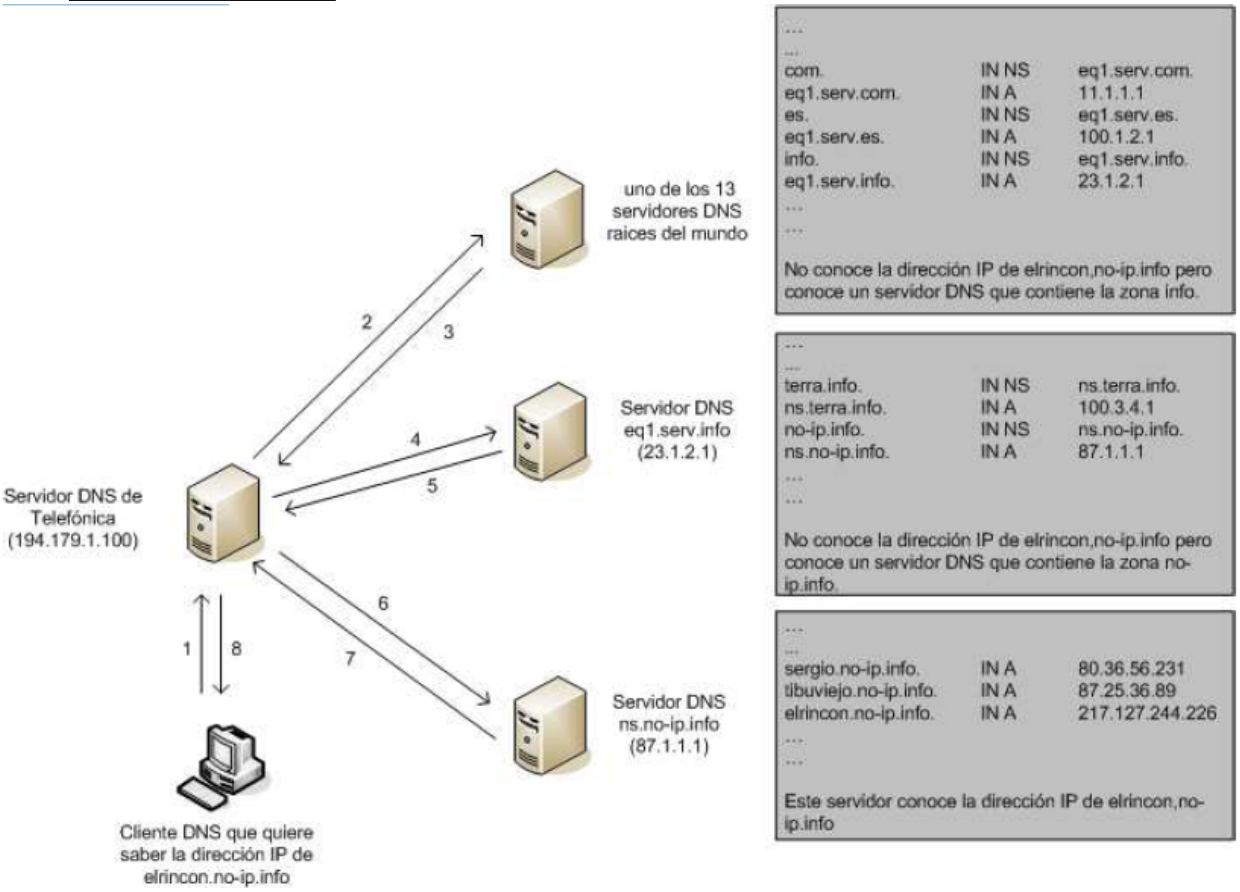
Es **distribuida** porque la base de datos está repartida en multitud de servidores DNS en INTERNET. Es **jerarquizada** porque tiene una estructura jerarquizada ya que existen servidores DNS a partir de los cuales se puede seguir una ruta para llegar al servidor DNS que contiene la dirección IP correspondiente al nombre de host que buscamos.

Un nombre FQDN (Fully qualified Domain Name) es un nombre de dominio totalmente cualificado. Por Ejemplo, elrinco.no-ip.info podría ser el nombre totalmente cualificado de un host (FQDN), mientras que se podría configurar un cliente DNS para que buscara nombres utilizando el **sufijo** no-ip.info, de tal manera que bastaría con decir que queremos ir al equipo **elrincon**.

Existen dos mecanismos para la resolución de nombres FQDN en una dirección IP:

- Recursiva
- Iterativa

Petición Iterativa:



El cliente DNS quiere saber la dirección IP del host elrincon.no-ip.info, y para ello sigue los siguientes pasos:

1. El cliente DNS le pregunta a su servidor DNS. Su servidor DNS es el que ha indicado el administrador al configurar el equipo. (fichero **/etc/resolv.conf** en el caso de Linux)

2. El servidor DNS 194.179.1.100 no sabe la dirección IP de elrincon.no-ip.info, así que le pregunta a alguno de los **13 servidores DNS raices** del mundo.

3. El servidor DNS raiz no sabe la dirección IP de elrincon.no-ip.info, pero conoce un servidor con IP 23.1.2.1que contiene la zona **info**. y se lo comunica al servidor DNS de telefónica.

4. El servidor de Telefónica le traslada la petición al servidor DNS con IP 23.1.2.1.

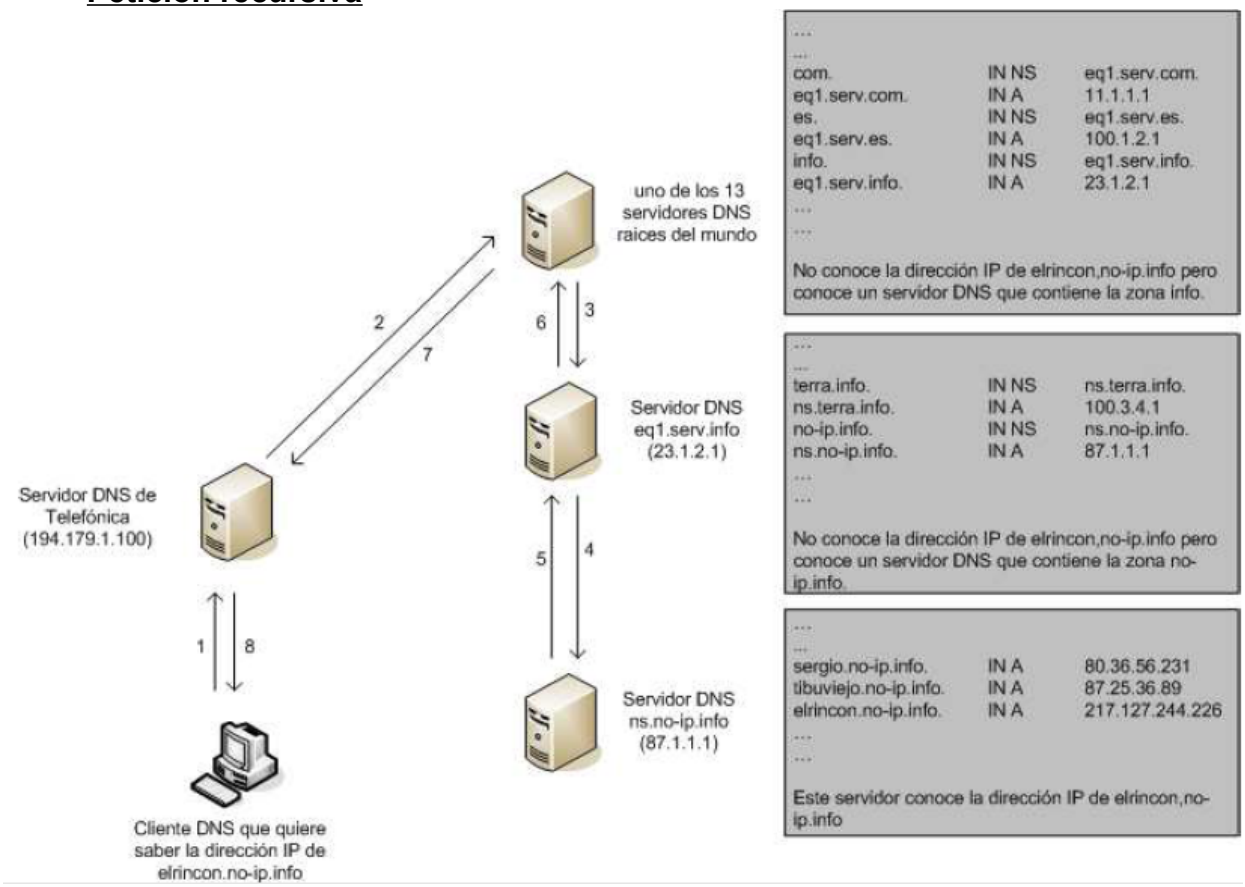
5. El servidor DNS con IP 23.1.2.1 tampoco conoce la dirección IP del host elrincon.no-ip.info pero conoce la dirección IP del servidor DNS que contiene la zona **no-ip.info**., y se la devuelve al servidor DNS de Telefónica.

6. El servidor DNS de Telefónica le pregunta a el servidor DNS con IP 87.1.1.1 por la dirección IP del host elrincon.no-ip.info

7. El servidor DNS ns.no-ip.info conoce la dirección IP de elrincon.no-ip.info y se la devuelve al servidor DNS de telefónica.

8. El servidor DNS de Telefónica devuelve por fin la dirección IP de **elrincon.no-ip.info** al cliente DNS que lo había solicitado.

<u>Petición recursiva</u>



En el caso de una petición recursiva el servidor DNS se encarga de resolver la petición completamente.

Obsérvese que las peticiones recursivas no son adecuadas puesto que recargan mucho los **13 servidores raíces** del mundo.

Obsérvese también que si los 13 servidores raíces DNS del mundo caen simultáneamente, la resolución de nombres no funcionaría completamente.

- Zona de resolución directa y zona de resolución inversa:
  Uno se puede imaginar un servidor DNS como las páginas amarillas. Las páginas amarillas están **ordenadas por nombre**, de tal manera que si uno busca por un nombre encuentra fácilmente el número de teléfono; sin embargo, sería difícil lo contrario, es decir, utilizar las páginas amarillas para encontrar el nombre de una persona a partir de su número de teléfono, a no ser que tuviéramos las mismas páginas amarillas ordenadas por número de teléfono en vez de por nombre.

  En el argot DNS una **zona** es como un libro de páginas amarillas, es decir, una zona contiene correspondencias entre direcciones IP y nombres DNS.

  Dependiendo de cómo esté **ordenada la información** de la zona tendremos zonas de **resolución directa** e **inversa**.

  Una zona de resolución directa sirve para que un **cliente** DNS le pregunte al servidor DNS cuál es la dirección IP de un nombre DNS de dicha zona. P.Ej: El cliente DNS pregunta por la IP de t0-01.rouco.com y el servidor DNS responde **192.168.10.51**

  Una zona de resolución inversa sirve para que un cliente DNS le pregunte al servidor DNS cuál es el nombre DNS correspondiente a una IP determinada. P.Ej: El cliente DNS pregunta por el nombre DNS de la IP 192.168.91.1 y el servidor DNS responde **t0-01.rouco.com**

- **Mecanismos de caché**

  Cada vez que un servidor de nombres envía una respuesta, lo hace adjuntando el tiempo de validez de la misma (TTL o “tiempo de vida“). Esto posibilita que el receptor, ante la necesidad de volver a resolver la misma consulta, pueda utilizar la información previamente obtenida en vez de realizar un nuevo requerimiento.

  Esta es la razón por la cual los cambios realizados en el DNS no se propagan instantáneamente a través del sistema. Dependiendo de la naturaleza de los mismos (y de la configuración de cada servidor), la propagación puede tardar desde algunos minutos hasta varios días.

- **Tipos de registro en un servidor de nombres**

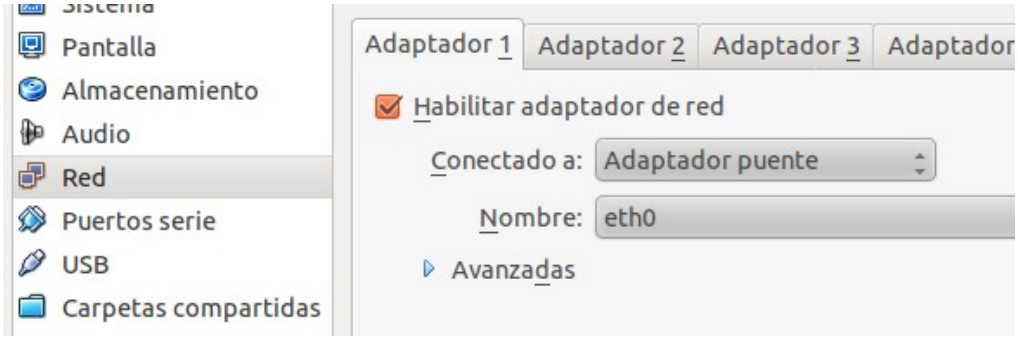
  Un servidor de nombres puede almacenar distinta información. Para ello, en cada zona de autoridad dispondrá de entradas de distinto tipo. Entre los más importantes se encuentran:

  - **A (Address)**: Este registro se utiliza para traducir nombres de hosts del dominio en cuestión a direcciones IP.
  - **CNAME (Canonical Name)**: El nombre canónico es un alias para un host determinado. (No define una dirección IP, sino un nuevo nombre.)
  - **NS (Name Server)**: Especifica el servidor (o servidores) de nombres para un dominio.

- **MX (Mail Exchange)**: Define el servidor encargado de recibir el correo electrónico para el dominio.
- **PTR (Pointer)**: Especifica un “registro inverso“, a la inversa del registro A, permitiendo la traducción de direcciones IP a nombres.
- **TXT (Text)**: Permite asociar información adicional a un dominio. Esto se utiliza para otros fines, como el almacenamiento de claves de cifrado, “DomainKeys” o “Sender Policy Framework“.

Pasos de la actividad

La actividad la realizaremos en la máquina virtual de ***Ubuntu Server****. Para que sea accesible desde la red local del aula directamente sin necesidad de abrir puertos vamos a modificar en VirtualBox la configuración de la primera tarjeta de red y la vamos a poner conectada a adaptador puente:*



Estudio de los ficheros de configuración más importantes en la resolución de nombres:

- ***Paso 1:*** *Ten en cuenta el significado de los siguientes ficheros*

Nombre del fichero	*Utilidad/Formato/Comentarios*	*¿Es clienteDNS o servidor DNS?*
/etc/hosts	*Fichero con la correspondencia entre IP y nombre correspondiente a esa IP. Método más primitivo de resolución de nombres de equipo (host).*	---
/etc/networks	*Fichero con la correspondencia entre IP de una red y nombre correspondiente a dicha red.*	---
/etc/services	*Fichero con la correspondencia entre número de puerto TCP ó UDP y nombre correspondiente a dicho puerto.*	---
/etc/resolv.conf	*Fichero de configuración del cliente DNS, es decir, es dónde indicamos la IP del servidor/es DNS a los que vamos a ir para saber cuál es la IP de un nombre DNS determinado.*	*Cliente**
/etc/network/interfaces	*Fichero de configuración de las interfaces de red*	---
/etc/sysctl.conf	*Fichero de configuración de parámetros del núcleo del sistema operativo como por ejemplo si está habilitado el enrutamiento (ip_forward)*	---
/etc/nsswitch.conf	*Fichero que le indica al sistema en qué orden se va a realizar la resolución de nombres. P.Ej: se puede configurar de tal manera que un cliente DNS primero mira en /etc/hosts para ver si ahí se encuentra la información de la IP de un nombre determinado, y luego si no se encuentra entonces vaya a un sevidor DNS a buscar dicha información.*	*Cliente**
/etc/named.conf	*Fichero de configuración principal de un servidor BIND, que es un software de servidor DNS que se usa mucho en linux. En este fichero se indica dónde se encuentran los ficheros con las zonas directas e inversas disponibles en el servidor DNS.*	*Servidor*
/etc/bind /named.hosts	*Nombre por defecto del fichero de configuración de una zona de resolución directa en BIND*	*Servidor*
/etc/bind /db.root	*Nombre por defecto del fichero de configuración en el que se indican los 13 servidores raices.*	*Servidor*
/etc/bind/db.local	*Nombre por defecto del Fichero de configuración de una zona correspondiente a la red 127.0.0.0 en BIND*	*Servidor*
/etc/bind/named.rev	*Nombre por defecto del fichero de configuración de una zona de resolución inversa en BIND*	*Servidor*

* Recuerda que un servidor o un cliente es un proceso que actúa como tal en un ordenador. Por lo tanto lo normal es que un ordenador que ejecute un programa servidor DNS también ejecute un programa cliente DNS.

Pasos a realizar en la configuración de un servidor DNS en Linux (Ordenador de adrian P.Ej):

Cada alumno configurará un servidor de DNS para el dominio `nombre.edu`, donde **nombre** es el nombre del alumno.

- **Paso 2**: Comprueba que tienes instalados los paquetes necesarios e instálalos en caso de que no lo estén:

```
$ sudo apt-get install bind9
```

- **Paso 3**: Si no es así, configura el fichero **/etc/network/interfaces** como ya has aprendido en actividades anteriores, para que los ordenadores en el aula tengan una dirección IP fija dentro de la red 172.16.0.0/16 y fuera del rango que asigna el servidor de DHCP de clase. Por ejemplo si tu ordenador es el número 2 de clase y la tarjeta de red enp0s3 entonces tu configuración sería:

```
auto lo
iface lo inet loopback

auto enp0s3
iface enp0s3 inet static
     address 172.16.110.2
     netmask 255.255.0.0
     gateway 172.16.0.1
     dns-nameservers 172.16.0.1
     dns-domain adrian.edu
```

Después de reiniciar la red asegúrate de tener conectividad con el resto de la red ejecutando

```
$ sudo ifdown enp0s3 && sudo ifup enp0s3
```

- **Paso 4**: Comprueba que tienes conectividad

```
$ ping 172.16.0.1
$ ping rediris.es
```

- **Paso 5:** Configuramos el servidor para que sólo sirva peticiones por IPv4. Para ello editamos el fichero **/etc/default/bind9** y lo modificamos añadiendo un -4 a la línea options. Quedará de la forma:

```
OPTIONS="-4 -u bind"
```

Ficheros de configuración de bind

Aparte del fichero en el que se especifican las opciones de arranque (**/etc/default/bind9**), el resto de los ficheros de configuración de Bind se encuentran en **/etc/bind**:

```
$ ls /etc/bind
db.0    db.empty  named.conf                named.conf.options
db.127  db.local  named.conf.default-zones  rndc.key
db.255  db.root   named.conf.local          zones.rfc1918
```

En el fichero **named.conf** se especifican los archivos en los que se configuran las zonas del servidor. En las distribuciones basadas en Debian (Ubuntu entre ellas) este fichero se sobreescribe al actualizar el paquete bind, por lo que las modificaciones al servidor la hacemos en **named.conf.local** que se incluye en named.conf.

```
$ cat /etc/bind/named.conf
// This is the primary configuration file for the BIND
DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz
for information on the
// structure of BIND configuration files in Debian,
*BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in
/etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

- **Paso 6**: Verificar zonas por defecto. Las zonas por defecto se especifican su ubicación en el fichero incluido **/etc/bind/named.conf.default-zones**:

```
$ cat /etc/bind/named.conf.default-zones
// prime the server with knowledge of the root servers
zone "." {
     type hint;
     file "/etc/bind/db.root";
};
zone "localhost" {
     type master;
     file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
     type master;
     file "/etc/bind/db.127";
};
```

Los archivos **db.** guardan la configuración de las diferentes zonas:

- La zona ".". Es la zona correspondiente a los 13 servidores raices. **/etc/bind/db.root** es el fichero que contiene la IP de dichos 13 servidores raices.
- La zona "localhost" es para la resolución directa del dispositivo virtual localhost cuya IP es 127.0.0.1 y la zona "127.in-addr-arpa" es para la resolución inversa de la misma

- **Paso 7. Definiendo nuestras zonas.** Añadimos al fichero **/etc/bind/named.conf.local** las siguientes líneas:

```
zone "adrian.edu" {
     type master;
     file "/etc/bind/db.adrian.edu";
};
zone "16.172.in-addr.arpa" {
     type master;
     file "/etc/bind/db.172.16";
};
```

Lo que acabamos de hacer es especificar las zonas de nuestro servidor. En este caso la zona de resolución directa e inversa de nuestro dominio. Para cada una de ellas especificamos el **type**, en este caso **master,** de la zona (de tipo maestro). Y el fichero en el que se almacena la base de datos de la misma.

- **Paso 8** : Ahora vamos a crear el fichero en el que se almacenan los registros de la zona de resolución directa “adrian.edu”. Para ello creamos el fichero **/etc/bind/db.adrian.edu**

  Observa que:

  - Este fichero se corresponde con la zona **“adrian.edu”** porque lo dice el fichero **/etc/bind/named.conf.local** que configuraste anteriormente.
  - El ordenador con el nombre adrian.edu tiene IP 172.16.110.2
  - El nombre **ns.adrian.edu** y adri**.adrian.edu** se refieren al mismo ordenador con la misma IP y son el propio servidor.
  - El ordenador **jimmy.adrian.edu.** termina en punto, por lo que indica que su nombre totalmente cualificado FQDN es jimmy.adrian.edu. Fíjate en que la línea correspondiente a **router** no termina en punto y por tanto su FQDN es router más el nombre de la zona que es adrian.edu, y que por tanto su FQDN es **router.adrian.edu**.
  - Para no empezar por un fichero vacio hacemos una copia de /etc/bind/db.local para que nos sirva de base

    ```
    $ sudo cp /etc/bind/db.local /etc/bind/db.adrian.edu
    ```

  - Lo modificamos para que quede de la forma

    ```
    $TTL 604800
    @ IN SOA adrian.edu. root.adrian.edu. (
        1         ; serial no
        604800    ; refresh
        86400     ; retry
        3600000   ; expire
        604800    ; Negative Cache TTL
    )
    @                   IN   NS        ns.adrian.edu.
    @                   IN   A         172.16.110.2
    ns                  IN   A         172.16.110.2
    router              IN   A         172.16.0.1
    moodle              IN   A         192.168.1.15
    jimmy.adrian.edu.   IN   A         172.16.110.3
    adri                     IN   CNAME     ns
    ```

    - @ ← Dominio con el que estamos trabajando
    - SOA ← registro Start Of Autorithy
    - adrian.edu. ← Dominio que gestiona
    - root.adrian.edu ← email del propietario del dominio (la @ se sustituye por ”.”)
    - El punto, “.” al final indica nombre de dominio completo. Si no acaba en punto se le añada el dominio completo.

- **Paso 9**: visualiza el fichero **`/etc/bind/db.root.`** Este fichero contiene la información de la zona raiz, es decir, de los 13 servidores raices.

```
. 3600000 IN NS A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000 IN A 198.41.0.4
. 3600000 IN NS B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000 IN A 128.9.0.107
```

- **Paso 10**: Configura el fichero de resolución inversa **/etc/bind/db.172.16** Copiamos un fichero para que nos sirva de base:

```
$ sudo cp /etc/bind/db.127 /etc/bind/db.172.16
```

Hacemos que quede de la forma

```
$TTL 604800
@ IN SOA ns.adrian.edu. root.adrian.edu. (
1 360000 3600 3600000 360000)
@               IN   NS   ns.
2.110           IN   PTR  ns.adrian.edu.
2.110           IN   PTR  adri.adrian.edu.
1.0             IN   PTR  router.adrian.edu.
3.110           IN   PTR  jimmy.adrian.edu.
```

Observa que los números de la dirección IP se escriben en orden inverso y que no llevan punto al final. Así, por ejemplo, cuando un registro es de la forma:

```
2.110                   IN   PTR adri.adrian.edu.
```

Es equivalente a:

```
2.110.16.172.in-addr.arpa.    IN   PTR  adri.adrian.edu
```

Ya que al no tener punto al final se le concatena el nombre de la zona que estamos definiendo.

- **Paso 11:** Comprueba la corrección de los ficheros de configuración ejecutando:

```
named-checkconf /etc/bind/named.conf
named-checkzone adrian.edu. /etc/bind/db.adrian.edu
named-checkzone 16.172.in-addr.arpa /etc/bind/db.172.16
```

Es una buena forma de asegurarnos de que no hemos cometido errores al escribir los archivos

- **Paso 12**: Reinicia el servicio named, correspondiente al servicio DNS que implementa el software BIND para que tome la configuración que acabamos de crear.

```
$ sudo service bind9 restart
```

Pasos para configurar como cliente de DNS del equipo servidor de DNS a si mismo :

- **Paso 13**: Configura ella red del servidor de forma que su servidor de DNS sea el mismo.

  Primero, echamos abajo la red:

```
$ sudo ifdown enp0s3
```

  Modificamos el fichero `/etc/network/interfaces` hacemos que las peticiones de DNS se las haga al nuevo servidor

```
...
     dns-domain adrian.edu
     dns-nameservers 127.0.0.1
...
```

  El atributo **domain** indica el nombre de dominio por defecto. Si no se especifica se asume el nombre de dominio obtenido a partir del primer punto del nombre local de la maquina. Si por ejemplo, la máquina se llama pc01.adrian.edu, se toma como nombre de dominio adrian.edu.

  Aplicamos la nueva configuración de la red:

```
$ sudo ifdown enp0s3
```

Paso para poder acceder de forma externa al servicio :

- **Paso 14**: Como el servidor está configurado para bloquear todo el tráfico entrante hemos crear una regla en el cortafuegos para permitirlo. Investiga y aplica utilizando ufw la regla necesaria para permitir el acceso entrante al servidor para las consultas de DNS.

Pasos para verificar que todo funciona correctamente:

- **Paso 15:** Comprueba lo siguiente.

Desde el servidor DNS:

```
ping 172.16.110.2
ping router
ping adri
ping 172.16.0.1
ping moodle
dig moodle.adrian.edu
dig adri.adrian.edu -t cname
dig router.adrian.edu
dig www.rediris.com
dig -x 172.16.0.1
dig -x 172.16.110.2
host moodle
host adrian
host adri
host www.rediris.com
```

Desde cualquier otro equipo de la red:

```
dig @172.16.110.2 router.adrian.edu
dig @172.16.110.2 router.adrian.edu
dig @172.16.110.2 -x 172.16.0.1
dig @172.16.110.2 -x 172.16.110.2
dig @172.16.110.2 rediris.es
dig @172.16.110.2 adri.adrian.edu -t cname
```

Pasos complementarios

- Configura el servidor de forma que sólo sirva peticiones provenientes del propio servidor y de otro equipo de la red. Cualquier otro equipo no debería obtener respuestas del servidor.
- Configura el servidor de forma que haga resoluciones inversas para la IP 192.168.1.15. O sea, que si ejecutamos:

```
dig -x 192.168.1.15
```

Obtengamos:

```
moodle.adrian.edu
```