

SRC. IES Haría

UT2. Actividad 2

DNS en Linux

- **Objetivo general:** Configuración de un servidor DNS maestro y los clientes en el aula.
- **Duración prevista:** 3 horas
- **Software:**
 - "BIND-9"
- **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/named.conf, /var/named/named.ca, /var/named/named.rev, /var/named/named.hosts, /var/named/named.local, /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, CNAME y PTR.
 - Utilización práctica de las utilidades de verificación: nslookup, named-checkconf, named-checkzone 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
- **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 primeros 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 inicios 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 creó el sistema DNS (Domain Name System) que consiste en una base de datos **distribuida** y **jerarquizada** para la resolución de nombres de host.

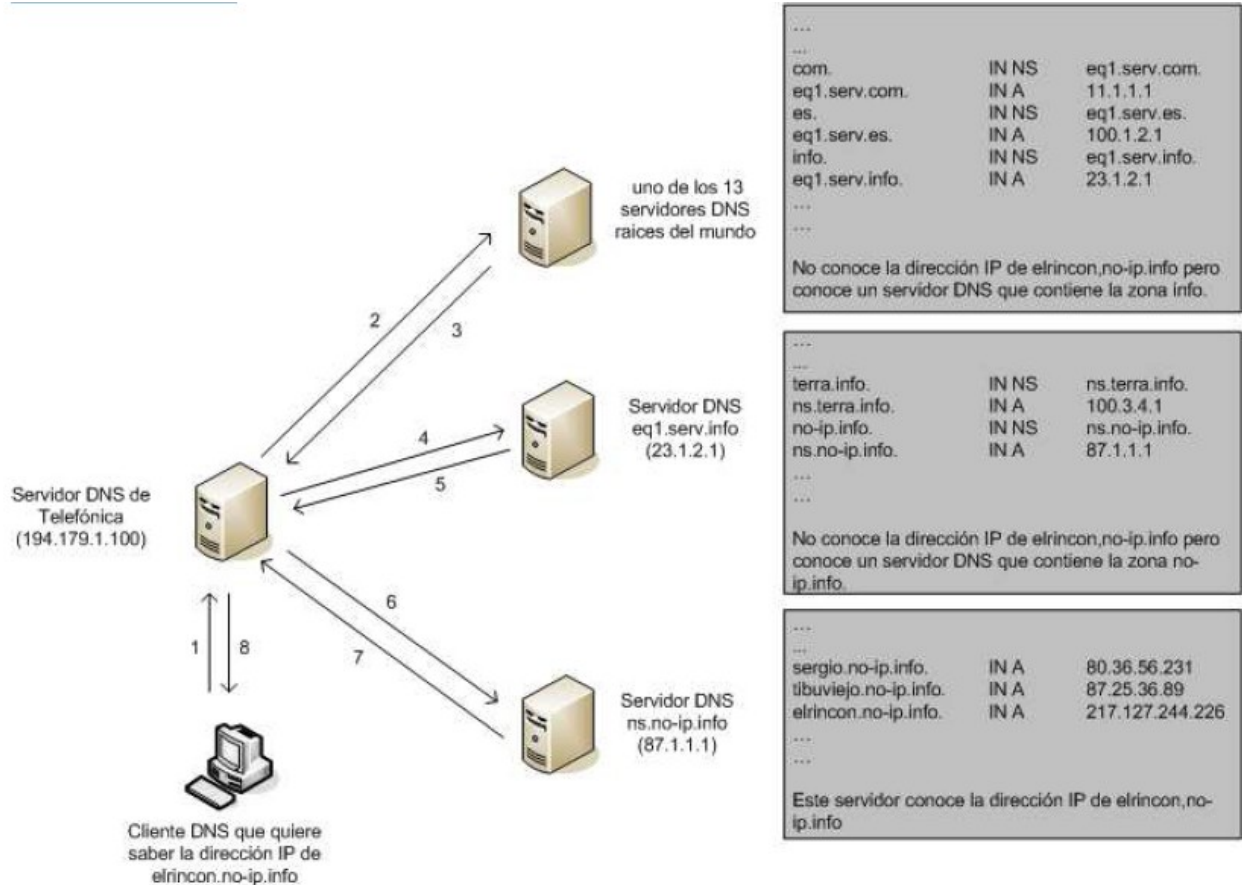
Es **distribuida** porque la base de datos está repartida en multitud de servidores DNS en INTERNET. Es **jerarquizada** porque tiene una estructura jerárquica ya que existen servidores DNS a partir de los cuales se puede seguir una ruta para llegar al servidor DNS que contiene la dirección IP correspondiente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

Un nombre FQDN (Fully qualified Domain Name) es un nombre de dominio totalmente cualificado. Por Ejemplo, **elrincon.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. (archivo **/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 raíces** del mundo.
3. El servidor DNS raíz no sabe la dirección IP de elrincon.no-ip.info, pero conoce un servidor con IP 23.1.2.1 que 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.

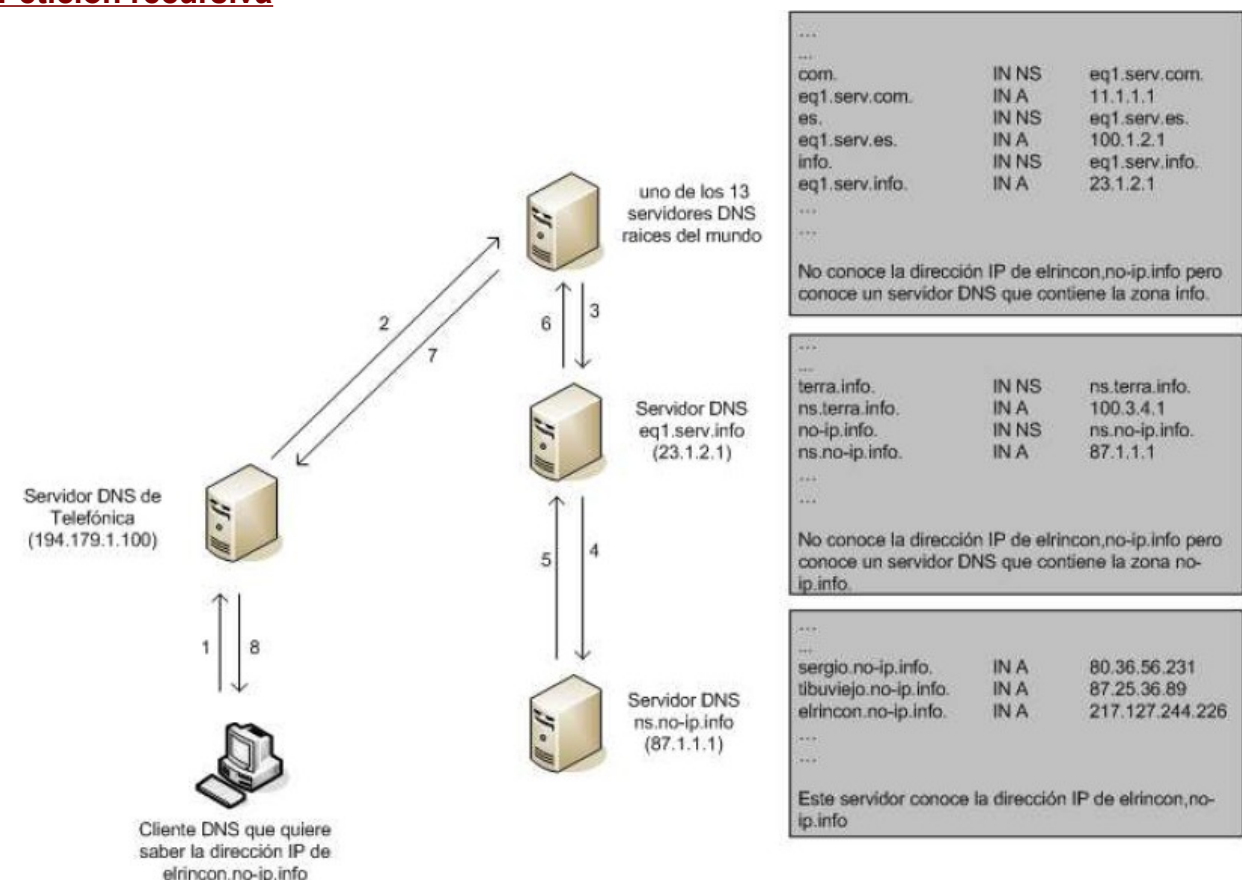
5. El servidor DNS con IP 23.1.2.1 tampoco conoce la dirección IP del host elrincon.no-ip.info pero conoce la dirección IP del servidor DNS que contiene la zona **no-ip.info.**, y se la devuelve al servidor DNS de Telefónica.

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.

Petición recursiva



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

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

Obsérva también que si los 13 servidores raices 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

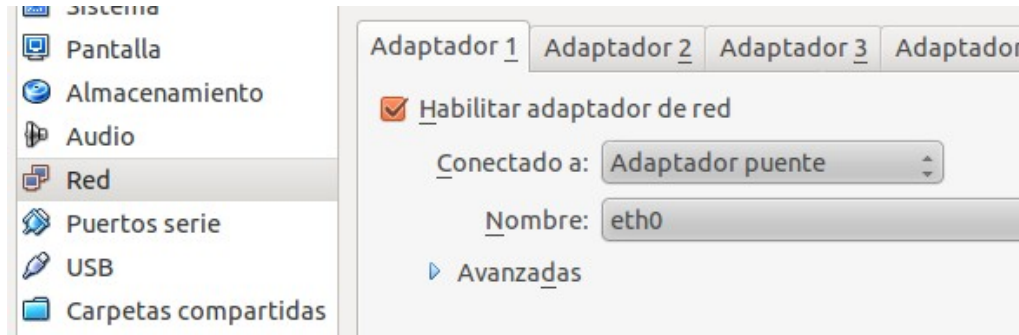
Un servidor de nombres puede almacenar distinta información. Para ello, en cada zona de autoridad dispondrá de entradas de distinto tipo. Entre los más importantes se encuentran:

- **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 cliente DNS 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 servidor 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 raíces.	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

Nota: 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):

- **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:** Configura el fichero **/etc/network/interfaces** y asigna una IP estática a la primera tarjeta de red de la máquina virtual que ahora mismo está configurada de forma dinámica. Si tu equipo es el 201 le pondremos la IP 192.168.1.201, entonces tu configuración sería:

```
iface eth0 inet static
    address 192.168.1.201
    netmask 255.255.255.0
    gateway 192.168.1.1
```

Después de reiniciar la red (sudo /etc/init.d/networking restart) asegúrate de tener conectividad con el resto de la red ejecutando ping 192.168.1.1

- **Paso 4:** Cambia el fichero **/etc/nsswitch.conf** de tal forma que la resolución de host se haga primero con dns y posteriormente con **/etc/hosts**, mientras que los nombres de las redes se obtenga del fichero **/etc/networks**.

```
hosts: dns files
networks: files
```

- **Paso 5:** Edita el fichero **/etc/resolv.conf** de tal forma que únicamente indique el nombre del dominio de la clase (comenta el resto de las líneas).

```
domain adrian.edu      <- Para el alumno adrian
nameserver 127.0.0.1
```

Nota: El paso 4 y 5 realmente corresponden a la configuración del cliente DNS del ordenador en el que estamos configurando el servidor DNS.

- **Paso 6:** 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 sobrescribe al actualizar el paquete bind, por lo que las modificaciones al servidor las 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";
```

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
- **Especifica** donde se encuentra la configuración de tu servidor. Para ello incluye en el fichero **/etc/bind/named.conf.local** las siguientes líneas:

```
zone "adrian.edu" {
    type master;
    file "/etc/bind/db.adrian.edu";
};
zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192.168.1";
};
```

- **Paso 8** : Configura 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 moodle.adrian.edu tiene IP 192.168.1.15
- El nombre **ns.adrian.edu** y **adri.adrian.edu** se refieren al mismo ordenador con la misma IP.
- 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 moodle no termina en punto y por tanto su FQDN es moodle más el nombre de la zona que es adrian.edu, y que por tanto su FQDN es moodle.adrian.edu.

```
$TTL 2d
@ IN SOA adrian.edu. root.adrian.edu. (
    1 ; serial no
    360000 ; refresh
    3600 ; retry
    3600000 ; expire
    3600 ; default ttl
)
@ IN NS ns.adrian.edu.
@ IN A 192.168.1.201
ns IN A 192.168.1.201
router IN A 192.168.1.1
moodle IN A 192.168.1.15
jimmy.adrian.edu. IN A 192.168.1.203
adri IN CNAME ns
```

- @ ← Dominio con el que estamos trabajando
 - SOA ← registro Start Of Authority
 - 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 añade el dominio completo.
- **Paso 9:** visualiza el fichero /etc/bind/db.root. Este fichero contiene la información de la zona raíz, es decir, de los 13 servidores raíces.

```
. 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 /etc/bind/db.192.168.1

```
@ IN SOA adrian.edu. root.adrian.edu. (
1 360000 3600 3600000 360000)
@      IN      NS      ns.adrian.edu.
201    IN      PTR     ns
201    IN      PTR     adri
1      IN      PTR     router.adrian.edu.
15     IN      PTR     moodle
203    IN      PTR     jimmy.adrian.edu.
```

- **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 localhost. /etc/bind/db.local
named-checkzone 1.168.172.in-addr.arpa /etc/bind/db.192.168.1
```

- **Paso 12:** Arranca el servicio named, correspondiente al servicio DNS que implementa el software BIND.

```
$ sudo /etc/init.d/bind9 restart
```

Pasos para configurar el cliente DNS de Linux (el equipo anfitrión):

- **Paso 13:** Cambia el fichero **/etc/nsswitch.conf** de tal forma que la resolución de host se haga primero con DNS y posteriormente con **/etc/hosts**.

```
hosts: dns files
```

- **Paso 14:** Edita el fichero **/etc/resolv.conf** de tal forma que únicamente indique el nombre del dominio de la clase (comenta el resto de las líneas).

```
domain adrian.edu
nameserver 192.168.1.201 (Si es que tu servidor DNS es
el de adrian)
```

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 máquina. Si por ejemplo, la máquina se llama pc01.adrian.edu, se toma como nombre de dominio adrian.edu.

Pasos para verificar que todo funciona correctamente:

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

Desde el servidor DNS:

```
ping 192.168.1.201
ping moodle
ping adri
ping 192.168.1.1
ping router
nslookup moodle
nslookup adrian
nslookup router
nslookup www.google.com
nslookup 192.168.1.1
host moodle
host adrian
host router
host www.google.com
```

Desde el cliente DNS:

```
ping 192.168.1.201
ping ns
ping adri
ping 192.168.1.1
ping router
nslookup ns
nslookup adrian
nslookup router
nslookup www.google.com
nslookup 192.168.1.1
host ns
host adrian
host router
host www.google.com
```

Cuando hayas terminado avisa al profesor para que te revise la práctica