Práctica 1.3. Domain Name System (DNS)

**Objetivos**

En esta práctica, emplearemos herramientas para explorar la estructura del servicio en Internet. Después, configuraremos un servicio de nombres basado en BIND9. El objetivo es estudiar tanto los pasos básicos de configuración del servicio, como la base de datos y el funcionamiento del protocolo.

**Contenidos**

[Cliente DNS](#_oaacscp23e1c)

[Servidor DNS](#_eofrh0ah6ijw)

[Preparación del entorno](#_14a3ftqman5y)

[Zona directa (*forward*)](#_w2ynjijgd1kw)

[Zona inversa (*reverse*)](#_sfcsed37y3uw)

# Cliente DNS

Usaremos clientes DNS, que serán de utilidad tanto para depurar el despliegue del servicio DNS en nuestra red local, como para estudiar la estructura de DNS en Internet. La principal herramienta para consultar servicios DNS es dig. En esta primera parte, **se usará la máquina física**. Como las consultas DNS a determinados servidores están bloqueadas en la red de la UCM, **se usará un interfaz web** como [www.digwebinterface.com](http://www.digwebinterface.com) (activando las opciones “Stats” y “Show command”) o [www.diggui.com](http://www.diggui.com).

***Ejercicio 1.***Ver el contenido del fichero de configuración del cliente DNS, /etc/resolv.conf. Consultar la página de manual de resolv.conf y buscar las opciones nameserver y search.

Nameserver: dirección ip del servidor de nombre

Search: lista de búsquedas del nombre de host

Domain example.org

Search example.org

**servidor de nombres** Dirección IP del servidor de nombres

Dirección de Internet de un servidor de nombres que el solucionador debe consultar, ya sea una dirección IPv4 (en notación de puntos) o una dirección IPv6 en notación de dos puntos (y posiblemente de puntos) según RFC 2373. Hasta MAXNS (actualmente 3, **consulte** < *resolv* [*. h*](https://linux.die.net/include/resolv.h) *>* ) se pueden enumerar servidores de nombres, uno por palabra clave. Si hay varios servidores, la biblioteca de resolución los consulta en el orden indicado. Si no hay entradas **de servidor de nombres** , el valor predeterminado es utilizar el servidor de nombres en la máquina local. (El algoritmo utilizado es probar un servidor de nombres, y si la consulta se agota, intente con la siguiente, hasta que se acaben los servidores de nombres, luego repita la prueba con todos los servidores de nombres hasta que se realice un número máximo de reintentos).

**search** Lista de búsqueda para la búsqueda de nombres de host.

La lista de búsqueda normalmente se determina a partir del nombre de dominio local; de forma predeterminada, contiene sólo el nombre de dominio local. Esto se puede cambiar enumerando la ruta de búsqueda del dominio deseado después de la palabra clave *de búsqueda* con espacios o tabulaciones que separe los nombres. Las consultas de resolución que tengan menos de *ndots* puntos (el valor predeterminado es 1) se intentarán utilizando cada componente de la ruta de búsqueda por turno hasta que se encuentre una coincidencia. Para entornos con múltiples subdominios, lea **las opciones ndots:** *n*a continuación para evitar ataques de intermediario y tráfico innecesario para los servidores DNS raíz. Tenga en cuenta que este proceso puede ser lento y generará mucho tráfico de red si los servidores de los dominios enumerados no son locales, y que las consultas expirarán si no hay ningún servidor disponible para uno de los dominios.

Actualmente, la lista de búsqueda está limitada a seis dominios con un total de 256 caracteres.

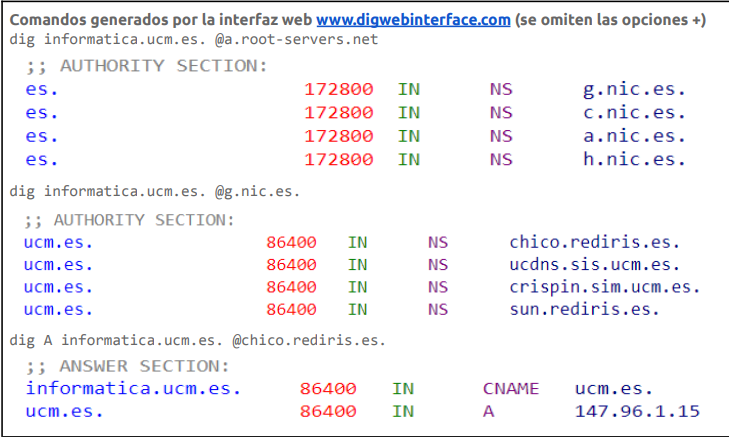
***Ejercicio 2****.* Partiendo del servidor raíz a.root-servers.net y usando las respuestas obtenidas, obtener la dirección IP de [informatica.ucm.es](http://informatica.ucm.es). Completar la siguiente tabla:

NS=NAME SERVER

Stat,show command y no recursive

| **Servidor** | **Nombre** | **TTL** | **Tipo** | **Datos** |
| --- | --- | --- | --- | --- |
| a.root-servers.net | es. | 72800 | ns | g.nic.es |
| g.nic.es | ucm.es. | 86400 | ns | chico.rediris.es. |
| chico.rediris.es. | Informatica.ucm.es. | 86400 | Cname | Ucm.es. |
| ucm.es. | 86400 | a | 147.96.1.15 |
|  |  |  |  |  |
| *NOTA: Añadir tantas filas como sea necesario* | | | | |

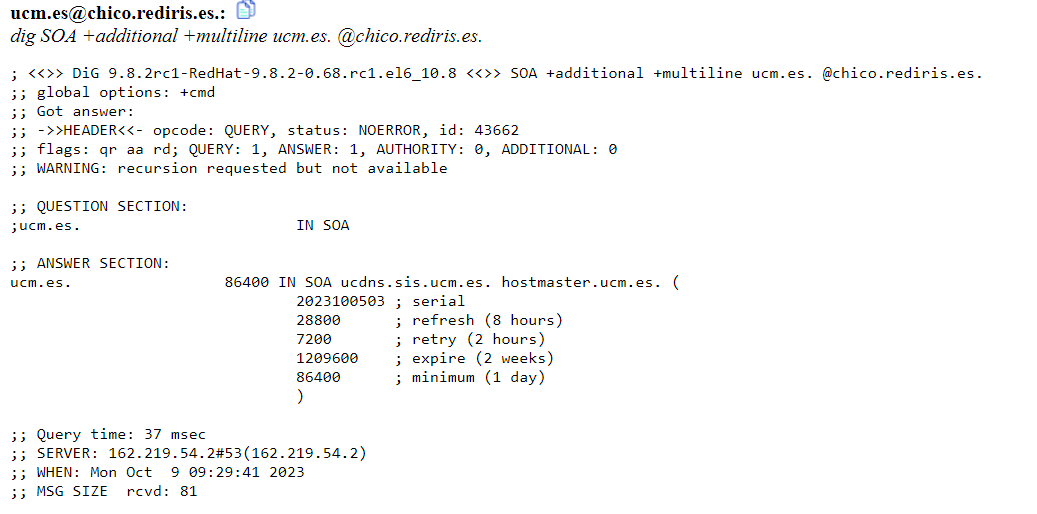
**Nota:** Si se usa la herramienta dig desde línea de comandos, la sintaxis es dig @<servidor> <nombre> <tipo>. Consultar la página de manual de dig y la [estructura del registro](https://docs.google.com/presentation/d/17AnDsSj5O7iUKep-RMJfS2Yi9vEKd4xjPCzN2cTveqY/#slide=id.g1204fc089_01) y la [base de datos DNS](https://docs.google.com/presentation/d/17AnDsSj5O7iUKep-RMJfS2Yi9vEKd4xjPCzN2cTveqY/#slide=id.g16fd59ec7_030).





***Ejercicio 3****.* Obtener el registro SOA de ucm.es. usando un servidor autoritativo de la zona. Identificar los campos relevantes del registro.

**SOA=Cuando el tipo de registro DNS es "SOA" (Start of Authority), significa que estás buscando información sobre la autoridad del dominio y otros parámetros relacionados con la administración de la zona DNS.**

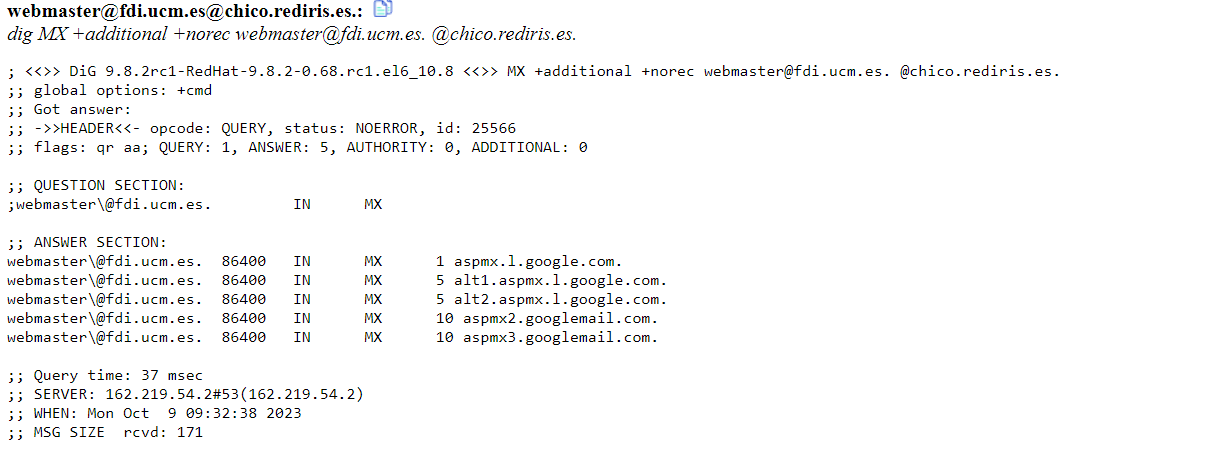


ucdns.sis.ucm.es: Es el servidor primario de la zona.

hostmaster.ucm.es: Es el email de contacto en notación user.host.

2022100701, 28800, 7200, 1209600, 86400: Número de serie y temporizadores.

***Ejercicio 4****.* Determinar qué servidor de correo debería usarse para enviar un mail a [webmaster@fdi.ucm.es](mailto:webmaster@fdi.ucm.es), usar un servidor autoritativo de la zona.



**mx=mail exchange**

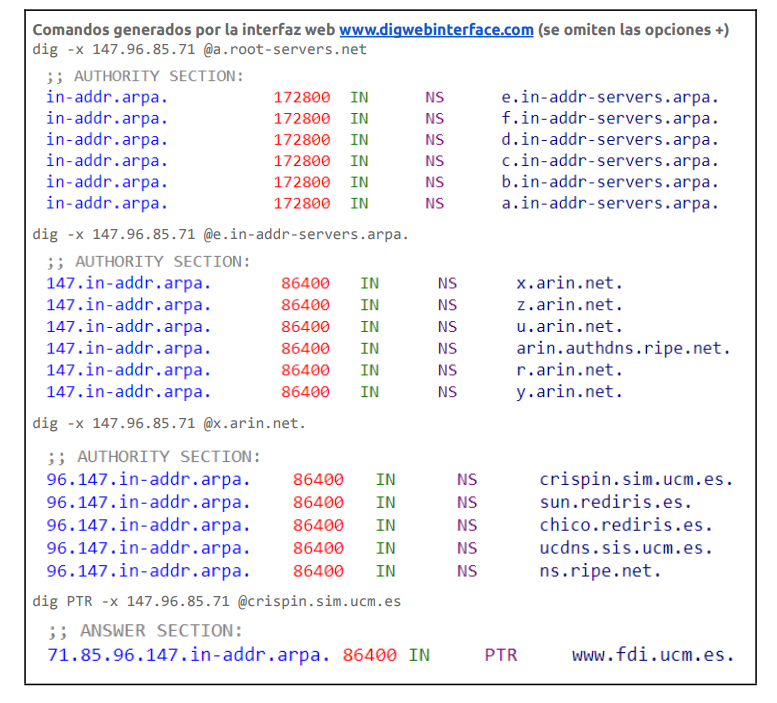
**Informacion relacionada con la configuracion de servidores de correo electrónico para un dominio**

***Ejercicio 5****.* Determinar el nombre de dominio para 147.96.85.71 partiendo del servidor raíz a.root-servers.net y usando las respuestas obtenidas. Completar la siguiente tabla:

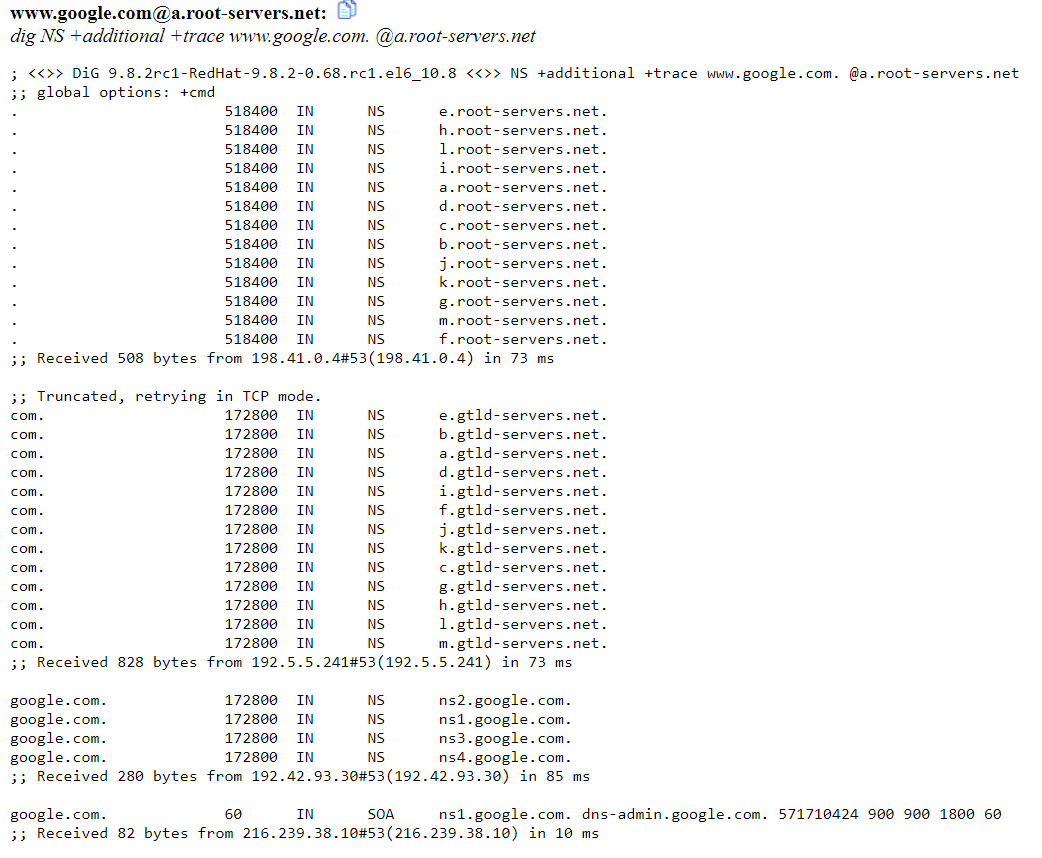
**HAY QUE PONER REVERSE**

| **Servidor** | **Nombre** | **TTL** | **Tipo** | **Datos** |
| --- | --- | --- | --- | --- |
| a.root-servers.net | in-addr.arpa. | 172800 | ns | e.in-addr-servers-arpa. |
| e.in-addr-servers-arpa. | 147.in-addr.arpa. | 86400 | ns | x.arin.net. |
| x.arin.net. | 96.147.in-addr.arpa. | 86400 | ns | crispin.sim.ucm.es |
| crispin.sim.ucm.es | 71.85.96.147.in-addr.arpa. | 86400 | ptr | www.fdi.ucm.es |
| *NOTA: Añadir tantas filas como sea necesario* | | | | |

**Nota:** La opción -x de dig facilita la búsqueda inversa cuando detecta una dirección IP como argumento, creando el dominio de búsqueda a partir de la dirección IP (esto es, invierte el orden de los bytes y añade .in-addr.arpa.) y estableciendo el tipo de registro por defecto a PTR. En el interfaz web, se activa seleccionando “Reverse” como tipo de registro.



***Ejercicio 6****.* Obtener la IP de www.google.com usando el servidor por defecto. Usar la opción +trace del comando dig (option “Trace” en el interfaz web) y observar las consultas realizadas.



# Servidor DNS

## Preparación del entorno

Para esta parte, configuraremos la topología de red que se muestra en la siguiente figura:



Como en prácticas anteriores, construiremos la topología con la herramienta vtopol y un fichero de topología adecuado. Configurar cada interfaz de red como se indica en la figura y comprobar la conectividad entre las máquinas.

## Zona directa (*forward*)

vm\_1server actuará como servidor de nombres del dominio labfdi.es. La mayoría de los registros se incluyen en la zona directa.

***Ejercicio 7****.* Configurar el servidor de nombres añadiendo una entrada zone para la zona directa en el fichero /etc/bind/named.conf. El tipo de servidor de la zona debe ser master y el fichero que define la zona, db.labfdi.es. Por ejemplo:

| zone "labfdi.es." {  type master;  file "/etc/bind/db.labfdi.es";  }; |
| --- |

Revisar la configuración por defecto y consultar la página de manual named.conf(5) para ver las opciones disponibles para el servidor y las zonas. En los servidores autoritativos debemos deshabilitar la recursión, simplemente añadir la opción recursion false; en el fichero named.conf.options. Una vez creado el fichero, ejecutar el comando named-checkconf para comprobar que la sintaxis es correcta.



***Ejercicio 8****.* Crear el fichero de la zona directa labfdi.es. en /etc/bind/db.labfdi.es con los registros especificados en la siguiente tabla. Especificar también la directiva $TTL.

| **Registro** | **Descripción** |
| --- | --- |
| Start of Authority (SOA) | Elegir libremente los valores de refresh, update, expiry y nx ttl. El servidor primario es ns.labfdi.es y el email de contacto es contact@labfdi.es. |
| Servidor de nombres (NS) | El servidor de nombres es ns.labfdi.es, como se especifica en el registro SOA |
| Servidor de correo (MX) | El servidor de correo es mail.labfdi.es |
| Direcciones (A y AAAA) | La dirección de ns.labfdi.es es 192.168.0.1 (vm\_1server), la de mail.labfdi.es es 192.168.0.250 y las de www.labfdi.es son 192.168.0.200 y fd00::1. |
| Nombre canónico (CNAME) | correo.labfdi.es es un *alias* de mail.labfdi.es |

**Nota:** No olvidar que los nombres FQDN terminan en el dominio raíz (“.”). El nombre de la zona puede especificarse con @ en el nombre del registro.

Una vez generado el fichero de zona, se debe comprobar su integridad con el comando named-checkzone <nombre\_zona> <fichero>. Finalmente, arrancar el servicio DNS con el comando systemctl start named.

Comprobar que el el servicio named ha arrancado correctamente con el comando systemctl status named y verificar que está escuchando en el puerto 53 UDP y TCP con el comando ss. ¿A qué direcciones se ha enlazado el socket?

**Sudo nano db.labfdi.es**

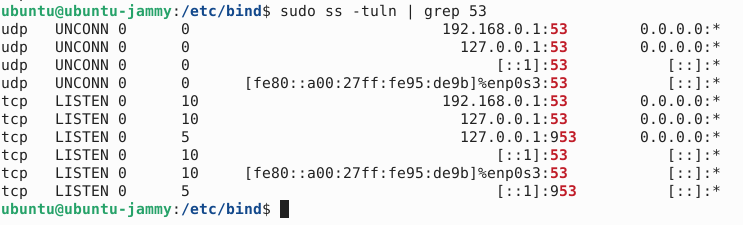
**Sudo named-checkzone labfdi.es db.labfdi.es**

**sudo systemctl restart named**

**systemctl status named**

**sudo ss -tuln | grep 53**

**Tuln es t de tcp,u de udp,l de lisyten n de mostrar numerico**

****

DENTRO DE LABFDI  
$TTL 86400 ; Tiempo de vida en caché (en segundos)

@ IN SOA ns.labfdi.es. contact.labfdi.es. (

2023100901 ; Número de serie (cambia cada vez que actualices)

3600 ; Refresh (cada 1 hora)

1800 ; Retry (cada 30 minutos)

604800 ; Expiry (1 semana)

86400 ) ; NX TTL (1 día)

; Registros de nombres de servidor

@ IN NS ns.labfdi.es.

; Registros de correo

@ IN MX 10 mail.labfdi.es.

; Direcciones IPv4 (A)

ns IN A 192.168.0.1

mail IN A 192.168.0.250

www IN A 192.168.0.200

; Direcciones IPv6 (AAAA)

www IN AAAA fd00::1

; Nombre canónico (CNAME)

correo IN CNAME mail.labfdi.es.

***Ejercicio 9****.* Configurar vm\_2client para que use vm\_1server como servidor de nombres. Para ello, crear o modificar el fichero /etc/resolv.conf con los valores apropiados para nameserver y search.

**# Configuración de resolución de nombres**

**nameserver 192.168.0.1 # Aquí debes especificar la dirección IP de vm\_1server**

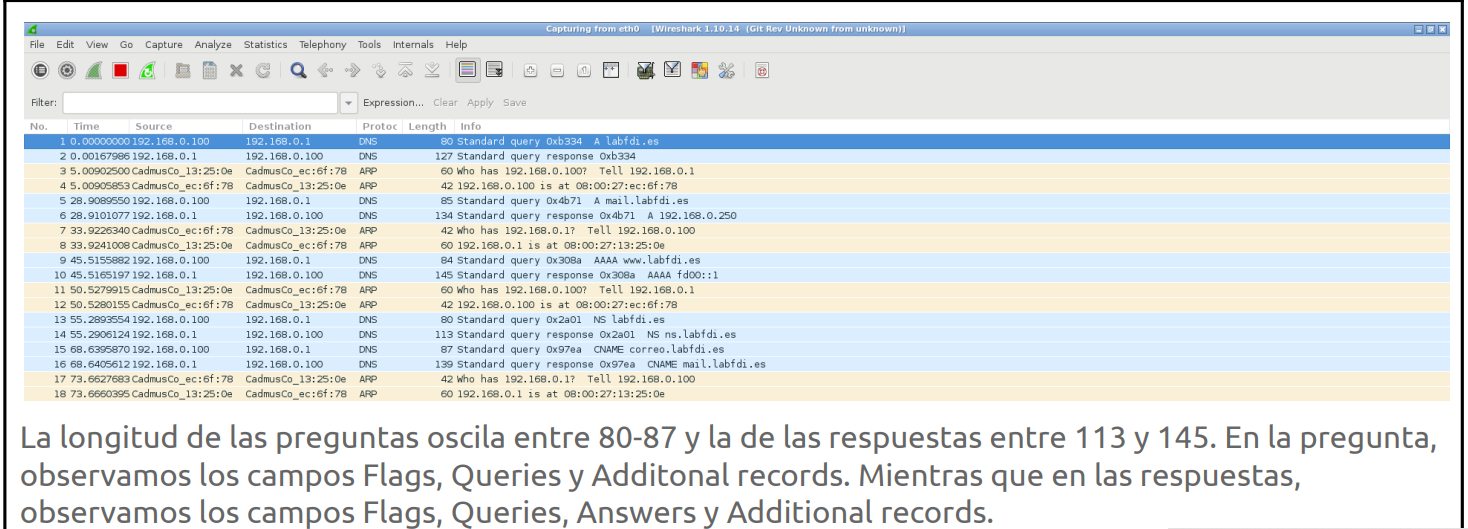
**search labfdi.es # Dominio de búsqueda (puedes especificar el dominio de tu red)**

***Ejercicio 10****.* Usar el comando dig en vm\_2client para obtener la información del dominio labfdi.es.



***Ejercicio 11****.* Realizar más consultas y, con la ayuda de wireshark:

* Comprobar el protocolo y puerto usado por el cliente y servidor DNS
* Estudiar el formato (campos incluidos y longitud) de los mensajes correspondientes a las preguntas y respuestas DNS.



## Zona inversa (reverse)

Además, el servidor incluirá una base de datos para la búsqueda inversa. La zona inversa contiene los registros PTR correspondientes a las direcciones IP.

***Ejercicio 12****.* Añadir otra entrada zone para la zona inversa 0.168.192.in-addr.arpa. en /etc/bind/named.conf. El tipo de servidor de la zona debe ser master y el fichero que define la zona, /etc/bind/db.0.168.192.

**zone "0.168.192.in-addr.arpa." {**

**type master;**

**file "db.0.168.192";**

**};**

**Fichero**

**;**

**; Zona inversa para la red 192.168.0.0/24**

**;**

**$TTL 86400**

**@ IN SOA ns.labfdi.es. contact.labfdi.es. (**

**2023100901 ; Número de serie (cambia cada vez que actualices)**

**3600 ; Refresh (cada 1 hora)**

**1800 ; Retry (cada 30 minutos)**

**604800 ; Expiry (1 semana)**

**86400 ) ; NX TTL (1 día)**

**; Delegar la zona a ns.labfdi.es**

**@ IN NS ns.labfdi.es.**

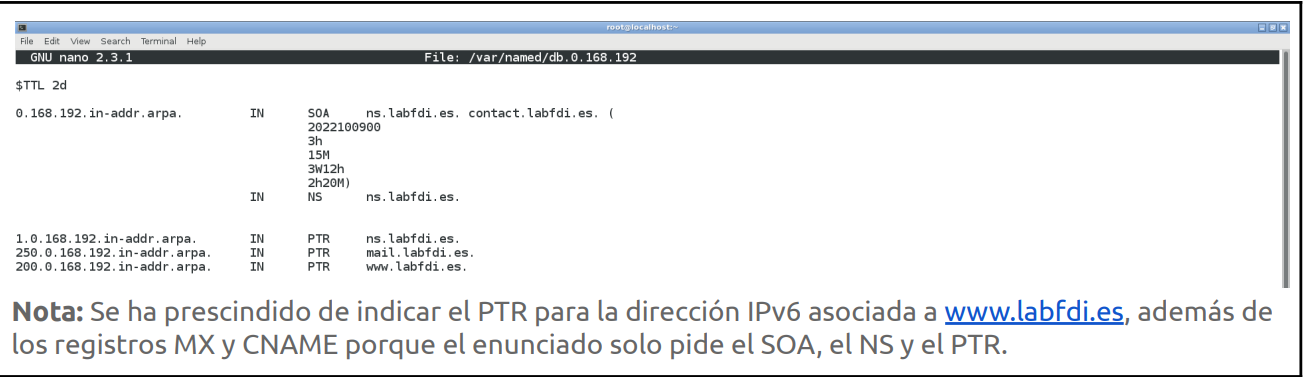
**; Definir registros PTR (resolución inversa)**

**1 IN PTR ns.labfdi.es. ; Resolución inversa para 192.168.0.1**

**250 IN PTR mail.labfdi.es. ; Resolución inversa para 192.168.0.250**

**200 IN PTR www.labfdi.es. ; Resolución inversa para 192.168.0.200**

***Ejercicio 13****.* Crear el fichero de la zona inversa en /etc/bind/db.0.168.192 con los registros SOA, NS y PTR. Esta zona usará el mismo servidor de nombres y parámetros de configuración en el registro SOA. Después, reiniciar el servicio DNS con el comando systemctl restart named (o bien, recargar la configuración con el comando systemctl reload named).



***Ejercicio 14****.* Comprobar el funcionamiento de la resolución inversa, obteniendo el nombre asociado a la dirección 192.168.0.250.

