Práctica 1.3. Domain Name System (DNS)

**Objetivos**

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

**Contenidos**

[Preparación del entorno para la práctica](#_14a3ftqman5y)

[Cliente DNS](#_spc65q2nbnj6)

[Servidor DNS](#_7gbx7pg7srk8)

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

[Zona inversa (*reverse*)](#_14xxb49cfigw)

# Preparación del entorno para la práctica

En la primera parte de la práctica (Cliente DNS), **usaremos el host físico del puesto del laboratorio**.

Para la segunda parte de la práctica (Servidor DNS), configuraremos la topología de red que se muestra en la Figura 1. Como en prácticas anteriores construiremos la topología con la herramienta vtopol y un archivo de topología adecuado. Antes de comenzar esa parte, configurar los interfaces de red como se indica en la figura y comprobar la conectividad entre las máquinas.

|  |
| --- |
|  |
| **Figura 1:** Topología y direccionamiento de las red usada en la práctica |

# Cliente DNS

En esta primera parte usaremos las herramientas 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. Las herramientas principales para consultar un servicio DNS son dig y host. Para esta primera parte **se usará el host físico del puesto del laboratorio**.

***Ejercicio 1.***El archivo de configuración del cliente DNS es /etc/resolv.conf. Consultar la página de manual (man resolv.conf) y estudiar el significado de las opciones nameserver y search. Ver el contenido del archivo en el host físico del laboratorio.

* El servicio resolver está formado por un cjto de rutinas de la biblioteca C que proporcionan acceso al DNS (Sistema de Nombres de Dominio) de internet.
* nameserver- Dirección IP de un servidor que pueden ser consultados para resolver. Se listan hasta un máximo de 3 servidores, uno por palabra clave. En caso de no haber entradas por defecto se utiliza el servidor de la máquina local.
* search- Lista de búsqueda de nombres de host. La lista de búsqueda está actualmente limitada a 6 dominios con un total de 256 caracteres.

***Ejercicio 2****.* Partiendo únicamente del servidor a.root-servers.net y de las respuestas obtenidas de cada servidor obtener la dirección IP de [informatica.ucm.es](http://informatica.ucm.es). Determinar el TTL de cada registro y completar la siguiente tabla:

IP ucm.es. (informática es CNAME (alias) de ucm.es.) → 147.96.1.15

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Servidor** | **Nombre del registro** | **TTL** | **Tipo** | **Datos** |
| a.root-servers.net | es. | 172800 | NS | g.nic.es. |
| g.nic.es | ucm.es. | 86400 | NS | sun.rederis.es. |
| sun.rederis.es | informatica.ucm.es | 86400 | CNAME | ucm.es. |
| ucm.es. | 86400 | A | 147.96.1.15 |

**Nota:** Usar el comando host -v <hostname o dominio> [servidor DNS], o el comando dig [@server] <hostname o dominio>. Más información en la página de manual de los comandos. Si las consultas DNS estuvieran bloqueadas, usar un interfaz web como [www.digwebinterface.com](http://www.digwebinterface.com).



***Ejercicio 3****.* Obtener la información del registro SOA para la zona ucm.es. usando un servidor autoritativo de la zona. Identificar los campos relevantes del registro. **Nota**: usar la opción -t en el comando host, o añadir el campo tipo en dig.

ucdns.sis.ucm.es. hostmaster.ucm.es. (  
 2017102301 ; serial  
 28800 ; refresh (8 hours)  
 7200 ; retry (2 hours)  
 1209600 ; expire (2 weeks)  
 86400 ; minimum (1 day)  
)

**SERIAL:** número de serie de zona, utilizado para las transferencias de zona.

**REFRESH:** intervalo de actualización, utilizado para las transferencias de zona.

**RETRY:** intervalo de reintento, utilizado para las transferencias de zona.

**EXPIRE:** intervalo de caducidad, utilizado para las transferencias de zona.

**MINIMUM:** solía ser el TTL mínimo, pero se utiliza hoy en día como TTL para las respuestas negativas.



***Ejercicio 4****.* Determinar qué servidor debería usarse para enviar un mail a [webmaster@fdi.ucm.es](mailto:webmaster@fdi.ucm.es), usar un servidor autoritativo de la zona.   
**webmaster\@fdi.ucm.es.** 86400 IN [MX](http://www.ietf.org/rfc/rfc1035.txt) 1 aspmx.l.google.com.

(El menor número indica mayor prioridad)



***Ejercicio 5****.* Determinar el nombre de dominio para 147.96.85.71. Al igual que en el ejercicio 2, usar únicamente el servidor a.in-addr-servers.arpa y las respuestas obtenidas a partir de éste. Completar la siguiente tabla:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Servidor** | **Nombre del registro** | **TTL** | **Tipo** | **Datos** |
| a.in-addr-servers.arpa. | 147.in-addr.arpa. | 86400 | NS | u.arin.net |
| u.arin.net | 96.147.in-addr.arpa. | 172800 | NS | crispin.sim.ucm.es. |
| crispin.sim.ucm.es. | 71.85.96.147.in-addr.arpa. | 86400 | PTR | www.fdi.ucm.es |

**NOTA:** El comando host 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. La opción -x del comando dig produce el mismo efecto.

***Ejercicio 6****.* Obtener la IP de [www.google.com](http://www.google.com) usando el servidor configurado en el sistema (según /etc/resolv.conf). Usar el comando dig con la opción +trace y observar las consultas realizadas.

IPV4 (tipo A)

www.google.com. 300 IN A 172.217.6.4

IPV6 (tipo AAAA)

www.google.com. 300 IN AAAA 2607:f8b0:4009:811::2004



# Servidor DNS

## Zona directa (*forward*)

La máquina VM1 actuará como servidor de nombres del dominio labfdi.es. La zona directa labfdi.es. debe incluir los registros descritos en la siguiente tabla:

|  |  |
| --- | --- |
| **Registro** | **Descripción** |
| Start of Authority (SOA) | Descripción de la zona. Se pueden elegir libremente los valores de refresh, update, expiry y ttl. El servidor primario de la zona es ns.labfdi.es. |
| Servidor de nombres (NS) | El servidor de nombres es ns.labfdi.es., como se especifica en el registro SOA |
| Dirección (A) de ns.labfdi.es. | La dirección de ns.labfdi.es. es 192.168.0.1 (VM1) |
| Direcciones (A y AAAA) del servidor web | Las direcciones de www.labfdi.es. son 192.168.0.200 y fd00::1 |
| Servidor de correo (MX) | El servidor de correo es mail.labfdi.es. |
| Dirección (A) del servidor de correo | La dirección de mail.labfdi.es.es 192.168.0.250 |
| Nombre canónico (CNAME) de servidor | El nombre canónico de servidor.labfdi.es. es mail.labfdi.es. |

**NOTA:** En la configuración del servicio, no olvidar que los nombres FQDN terminan en el dominio raíz (“.”).

***Ejercicio 1****.* Configurar el servidor de nombres. Los archivos se encuentran en el directorio /etc/bind. El archivo principal (named.conf) incluye la configuración de otros tres (named.conf.options, named.conf.local y named.conf.default\_zones):

* Comentar todas las entradas include del archivo /etc/bind/named.conf.
* Añadir una entrada zone para la zona directa. El tipo de servidor de la zona debe ser master y el archivo que define la zona, db.labfdi.es.

|  |
| --- |
| **Listado 1.** Ejemplo de definición de zona en /etc/bind/named.conf |
| zone “labfdi.es.” {  type master;  file “/etc/bind/db.labfdi.es”;  }; |

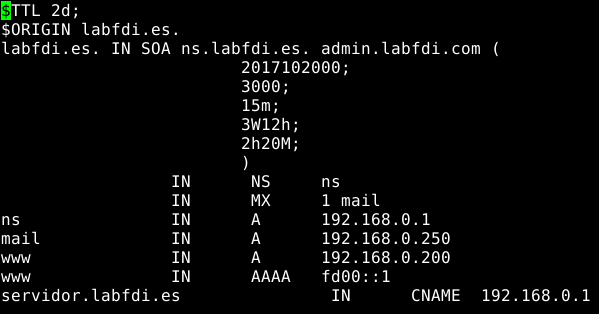
**NOTA:** Consultar la página de manual de named.conf para ver las opciones disponibles en la definición de la zona.

**NOTA:**  Una vez creado el archivo de configuración, se debe ejecutar el comando named-checkconf, para comprobar que la sintaxis es correcta.



***Ejercicio 2****.* Crear el archivo de la zona directa con los registros especificados en la tabla anterior (se puede usar como base alguno de los archivos db existentes). Especificar también el comando $TTL.

nano db.labfdi.es



**NOTA:** El nombre de la zona puede especificarse con @ en el campo nombre del registro.

**NOTA:** Una vez generado el archivo de zona, se debe comprobar su integridad con el comando named-checkzone <nombre\_zona> <archivo>.

named-checkzone labfdi.es. db.lab.fdi.es

***Ejercicio 3****.* Arrancar el servicio DNS con el comando service bind9 start.



***Ejercicio 4****.* Configurar la máquina virtual cliente para que use el nuevo servidor de nombres. Para ello, crear o modificar /etc/resolv.conf con los nuevos valores para nameserver y search. Probar la resolución de nombres para [www.labfdi.es](http://www.labfdi.es).

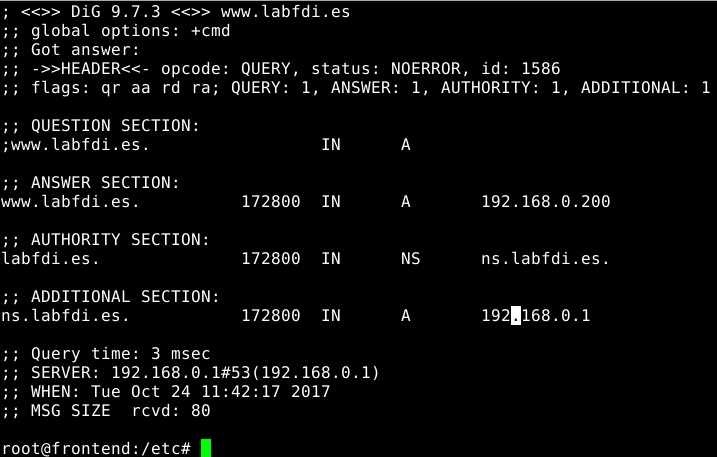
nameserver 192.168.0.1

search www.labfdi.es



***Ejercicio 5****.* Usar el comando dig o host para obtener la información del dominio labfdi.es ofrecida por el servidor.

dig www.labfdi.es





***Ejercicio 6****.* Repetir alguna de las consultas anteriores 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.

|  |  |
| --- | --- |
| Standard query: Cliente | Protocolo: UDP |
| * Src. Port: 58261 * Dest. Port: 53 |
| Flags:   * Recursion desired (1) |
| Standard query response: Servidor | Protocolo: UDP |
| * Src. Port: 53 * Dest. Port: 58261 |
| Flags:   * Response (1) * Authoritative (1) * Recursion desired (1) * Recursion available (1) |

## Zona inversa (*reverse*)

Además el servidor incluirá una base de datos para la búsqueda inversa. Para ello, definiremos la zona inversa 0.168.192.in-addr.arpa. con los registros PTR correspondientes a las direcciones IPv4. Esta zona usará el mismo servidor de nombres y parámetros de configuración en el registro SOA.

***Ejercicio 1****.* Añadir otra entrada zone para la zona inversa. El tipo de servidor de la zona debe ser master y el archivo que define la zona, db.0.168.192.

zone “0.168.192.in-addr.arpa.” {

type master;

file “/etc/bind/db.0.168.192”;

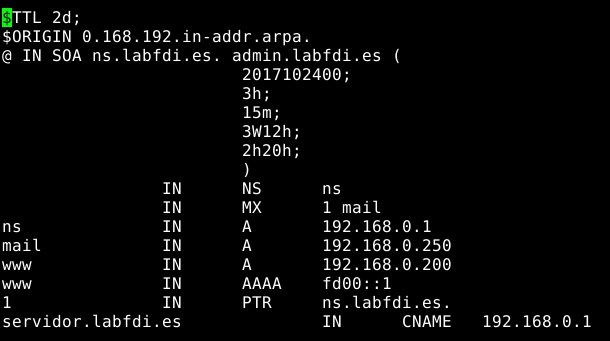
};

named-checkconf



***Ejercicio 2****.* Crear el archivo de la zona inversa con los registros SOA y PTR.

nano db.0.168.192



named-checkzone 0.168.192.in-addr.arpa. db.0.168.192

***Ejercicio 3****.* Reiniciar el servicio DNS con el comando service bind9 restart (o bien, recargar la configuración con el comando service bind9 reload).

VM1: service bind9 restart



***Ejercicio 4****.* Comprobar el funcionamiento de la resolución inversa, obtener el nombre asociado a 192.168.0.250.

dig -x 192.168.0.250

