

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. Previamente, emplearemos herramientas cliente DNS para explorar la estructura del servicio en Internet.

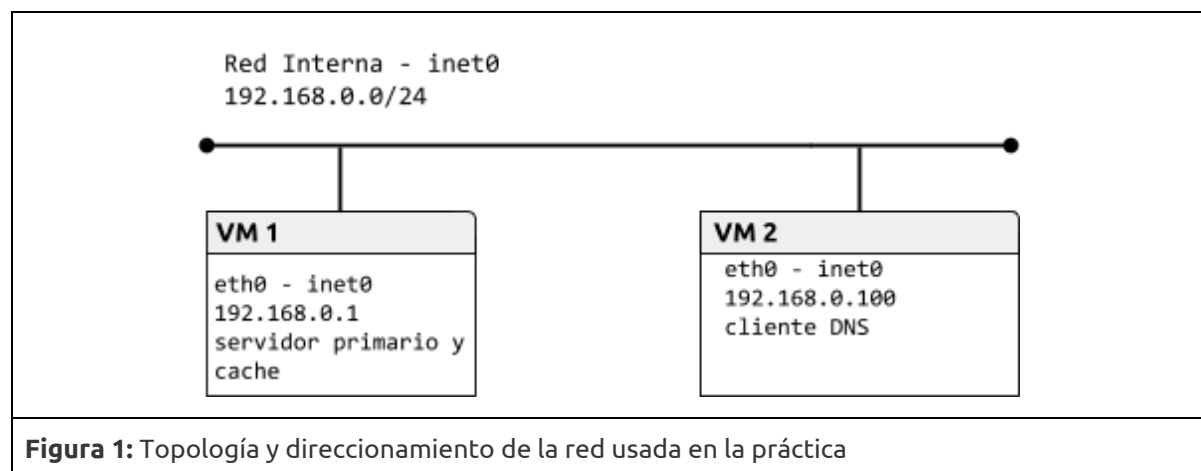
Contenidos

- Preparación del entorno para la práctica
- Cliente DNS
- Servidor DNS
 - Zona directa (*forward*)
 - Zona inversa (*reverse*)

Preparación del entorno para la práctica

En la primera parte de la práctica (Cliente DNS), **usaremos la máquina física 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 vtopo1 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.



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 la máquina física del puesto del laboratorio.** Si las consultas DNS a determinados servidores estuvieran bloqueadas, **usar un interfaz web** como www.digwebinterface.com (activando las opciones "Stats" y "Show command").

Ejercicio 1. El archivo de configuración del cliente DNS es `/etc/resolv.conf`. Consultar la página

de manual de resolv.conf y estudiar el significado de las opciones nameserver y search. Ver el contenido del archivo en la máquina física del laboratorio.

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

Servidor	Nombre	TTL	Tipo	Datos
a.root-servers.net				

NOTA: Usar el comando dig @<servidor> <nombre> <tipo>. Más información en la página de manual de dig.

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

Ejercicio 4. Determinar qué servidor debería usarse para enviar un mail a webmaster@fdi.ucm.es, usar un servidor autoritativo de la zona.

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

Servidor	Nombre	TTL	Tipo	Datos
a.root-servers.net				

NOTA: La opción -x de dig (en el interfaz web, se activa seleccionando “Reverse” como tipo de registro) 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.

Ejercicio 6. Obtener la IP de www.google.com usando el servidor por defecto. Usar el comando dig con la opción +trace y observar las consultas realizadas.

Servidor DNS

Zona directa (*forward*)

La máquina VM1 actuará como servidor de nombres del dominio labfdi.es. La mayoría de los registros se incluyen en la zona directa.

Ejercicio 1. Configurar el servidor de nombres añadiendo una entrada zone para la zona directa en el fichero /etc/named.conf. El tipo de servidor de la zona debe ser master y el archivo que define la zona, db.labfdi.es. Por ejemplo:

```
zone "labfdi.es." {  
    type master;  
    file "db.labfdi.es";  
};
```

Revisar la configuración por defecto y consultar la página de manual de named.conf para ver las opciones disponibles para el servidor y las zonas. Por ejemplo, la recursión debe estar deshabilitada en servidores autoritativos y las consultas pueden estar restringidas a solo ciertas máquinas.

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

Ejercicio 2. Crear el archivo de la zona directa labfdi.es. en /var/named/db.labfdi.es con los registros especificados en la siguiente tabla. Especificar también la directiva \$TTL.

Registro	Descripción
Start of Authority (SOA)	Descripción de la zona. Se pueden elegir libremente los valores de refresh, update, expiry y nx ttl. El servidor primario de la zona es ns.labfdi.es y el e-mail 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
Dirección (A) del servidor de nombres	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

Una vez generado el archivo de zona, se debe comprobar su integridad con el comando named-checkzone <nombre_zona> <archivo>.

NOTA: No olvidar que los nombres FQDN terminan en el dominio raíz (“.”). El nombre de la zona

puede especificarse con @ en el campo nombre del registro.

Ejercicio 3. Arrancar el servicio DNS con el comando `service named 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`.

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

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.

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

Ejercicio 2. Crear el archivo de la zona inversa en `/var/named/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.

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

Ejercicio 4. Comprobar el funcionamiento de la resolución inversa, obteniendo el nombre asociado a `192.168.0.250`.

