

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 BIND. El objetivo es estudiar tanto los pasos básicos de configuración del servicio, como la base de datos y el funcionamiento del protocolo.



Para cada ejercicio, se tienen que proporcionar los **comandos utilizados con sus correspondientes salidas**, las **capturas de pantalla de Wireshark realizadas**, y la **información requerida de manera específica**.

Activar el portapapeles bidireccional en las máquinas (menú Dispositivos) para copiar la salida de los comandos. Realizar capturas de pantalla con Virtualbox (menú Ver).

Las **credenciales de la máquina virtual** son: usuario `cursoresdes` y contraseña `cursoresdes`.

Contenidos

Cliente DNS

Servidor DNS

Preparación del entorno

Zona directa (*forward*)

Zona inversa (*reverse*)

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**. Si las consultas DNS a determinados servidores estuvieran bloqueadas, **se usará un interfaz web** como www.digwebinterface.com (activando las opciones "Stats" y "Show command") o 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`.

Ejercicio 2. Partiendo del servidor raíz `a.root-servers.net` y usando las respuestas obtenidas, obtener la dirección IP de informatica.ucm.es. Completar la siguiente tabla:

Servidor	Nombre	TTL	Tipo	Datos
a.root-servers.net.	es.	172800	NS	g.nic.es.
g.nic.es.	ucm.es.	86400	NS	sun.rediris.es.
sun.rediris.es.	informatica.ucm.es.	86400	CNAME	ucm.es.
ucm.es.		86400	A	147.96.1.15

Nota: Usar el comando `dig @<servidor> <nombre> <tipo>`. Consultar la página de manual de `dig` y la [estructura del registro](#) y la [base de datos DNS](#).

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

Copiar el comando utilizado e indicar los campos relevantes del registro.

- **dig @ucdns.sis.ucm.es ucm.es SOA**

```
ucm.es.      86400 IN SOA ucdns.sis.ucm.es. hostmaster.ucm.es. (
                                2020102801 ; serial
                                28800  ; refresh (8 hours)
                                7200   ; retry (2 hours)
                                1209600 ; expire (2 weeks)
                                86400  ; minimum (1 day)
                                )
```

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

Copiar el comando utilizado e indicar el servidor de correo.

- **dig @ucdns.sis.ucm.es. webmaster@fdi.ucm.es. NS**

```
ucm.es. 86400 IN SOA ucdns.sis.ucm.es. hostmaster.ucm.es. 2020102801 28800 7200 1209600
86400
```

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:

- **dig +nocmd -x 147.96.85.71 +additional @a.root-servers.net**

Servidor	Nombre	TTL	Tipo	Datos
a.root-servers.net	in-addr.arpa.	172800	NS	a.in-addr-servers.arpa.
.in-addr-servers.arpa.	147.in-addr.arpa.	86400	NS	z.arin.net.
z.arin.net.	96.147.in-addr.arpa.	172800	NS	ucdns.sis.ucm.es.
ucdns.sis.ucm.es.	71.85.96.147.in-addr.arpa.	86400	PTR	www.fdi.ucm.es.

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.

Copiar el comando utilizado y su salida.

- **dig +additional +trace www.google.com. @8.8.4.4**

```
;; global options: +cmd
```

```
.      87004 IN      NS      b.root-servers.net.
.      87004 IN      NS      c.root-servers.net.
.      87004 IN      NS      k.root-servers.net.
.      87004 IN      NS      j.root-servers.net.
.      87004 IN      NS      m.root-servers.net.
.      87004 IN      NS      d.root-servers.net.
.      87004 IN      NS      f.root-servers.net.
.      87004 IN      NS      h.root-servers.net.
.      87004 IN      NS      e.root-servers.net.
.      87004 IN      NS      l.root-servers.net.
.      87004 IN      NS      i.root-servers.net.
.      87004 IN      NS      g.root-servers.net.
.      87004 IN      NS      a.root-servers.net.
```

```
;; Received 228 bytes from 8.8.4.4#53(8.8.4.4) in 38 ms
```

```
com.    172800 IN      NS      b.gtld-servers.net.
com.    172800 IN      NS      m.gtld-servers.net.
com.    172800 IN      NS      c.gtld-servers.net.
com.    172800 IN      NS      d.gtld-servers.net.
com.    172800 IN      NS      a.gtld-servers.net.
com.    172800 IN      NS      j.gtld-servers.net.
com.    172800 IN      NS      l.gtld-servers.net.
com.    172800 IN      NS      f.gtld-servers.net.
com.    172800 IN      NS      g.gtld-servers.net.
com.    172800 IN      NS      k.gtld-servers.net.
com.    172800 IN      NS      h.gtld-servers.net.
com.    172800 IN      NS      e.gtld-servers.net.
com.    172800 IN      NS      i.gtld-servers.net.
```

```
;; Received 492 bytes from 192.36.148.17#53(192.36.148.17) in 56 ms
```

```
google.com. 172800 IN      NS      ns2.google.com.
google.com. 172800 IN      NS      ns1.google.com.
google.com. 172800 IN      NS      ns3.google.com.
google.com. 172800 IN      NS      ns4.google.com.
```

```
;; Received 280 bytes from 192.52.178.30#53(192.52.178.30) in 29 ms
```

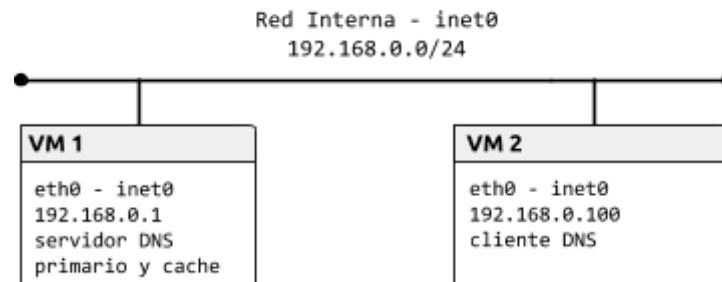
```
www.google.com.      300    IN      A      172.217.8.196
```

```
;; Received 48 bytes from 216.239.36.10#53(216.239.36.10) in 19 ms
```

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 vtopo1 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*)

La máquina VM1 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/named.conf. El tipo de servidor de la zona debe ser master y el fichero que define la zona, db.labfdi.es. Por ejemplo:

Recordar en **"vim"** para pasar al modo **edición: "i"**, para pasar al modo **comandos: "esc"**. Guardar **":w"**. Salir: **":q"**.

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

(Mi código)
zone "labfdi.es." {
    type master;
    file "db.labfdi.es";
};
```

Revisar la configuración por defecto y consultar vim la página de manual de named.conf para ver las opciones disponibles para el servidor y las zonas. La recursión debe estar deshabilitada en servidores autoritativos y no deben restringirse las consultas (directiva allow-query). 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 /var/named/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 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	correo.labfdi.es es un <i>alias</i> de mail.labfdi.es

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 `service named start`.

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.

Copiar el fichero de la zona directa.

\$TTL 2d

&ORIGIN labfdi.es. (Me da error si pongo esta línea ¿Por que?)

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

2003080800 ;serial number

3h ;refresh

15M ;update retry

3W12h ;expiry

2h20M ;nx

)

IN NS ns.labfdi.es.

IN MX 10 mail.labfdi.es.

ns IN A 192.168.0.1

mail IN A 192.168.0.250

www IN A 192.168.0.50

www IN AAAA fd00::1

servidor.labfdi.es. IN CNAME mail.labfdi.es.

Ejercicio 9. 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`.

Copiar el fichero de configuración del cliente.

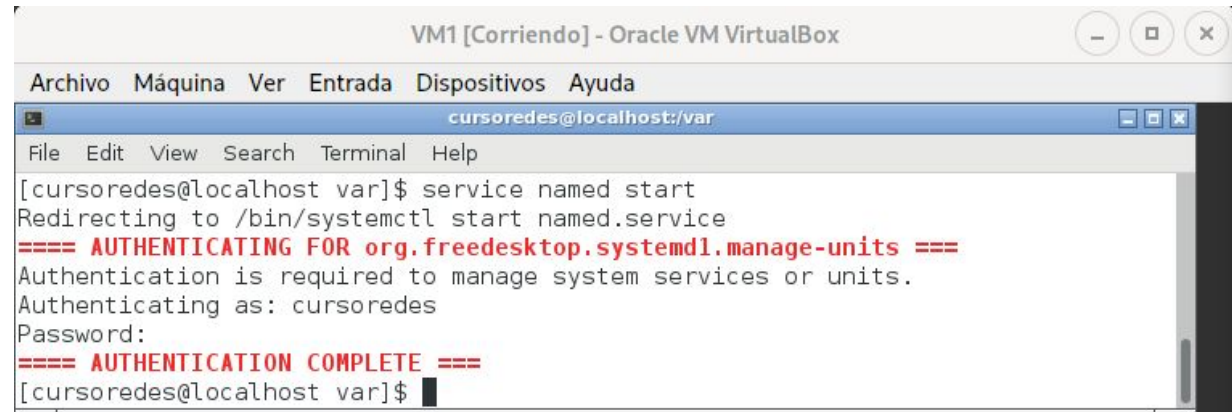
```
; generated by /usr/sbin/dhclient-script
search Home
```

```
nameserver 192.168.0.1
search ns.labfdi.es
domain ns.labfdi.es
```

Ejercicio 10. Usar el comando `dig` en el cliente para obtener la información del dominio `labfdi.es`.

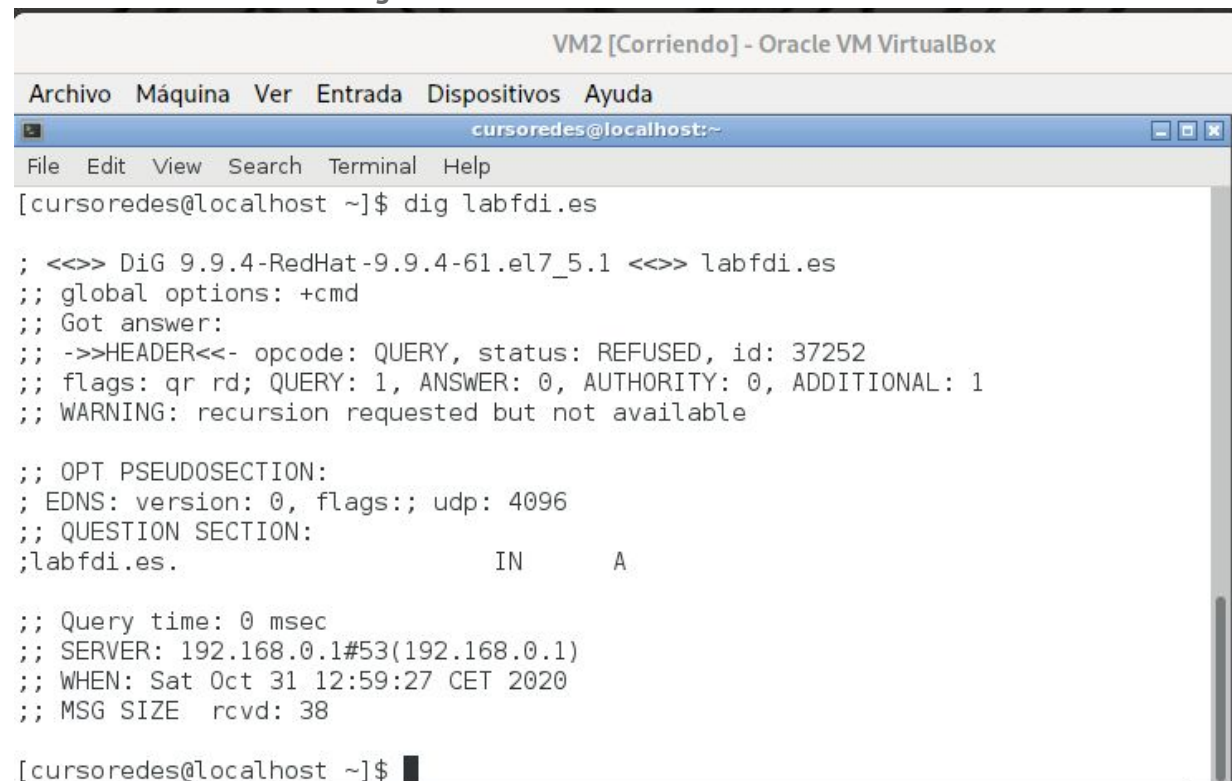
Copiar el comando utilizado y su salida.

En VM1 utilizar comando: “service named start”.



```
VM1 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
cursoredes@localhost:/var
File Edit View Search Terminal Help
[cursoredes@localhost var]$ service named start
Redirecting to /bin/systemctl start named.service
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to manage system services or units.
Authenticating as: cursoredes
Password:
==== AUTHENTICATION COMPLETE ====
[cursoredes@localhost var]$
```

En VM2 utilizar comando: “dig labfdi.es”.



```
VM2 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
cursoredes@localhost:~
File Edit View Search Terminal Help
[cursoredes@localhost ~]$ dig labfdi.es

; <>> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <>> labfdi.es
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: REFUSED, id: 37252
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;labfdi.es.                IN      A

;; Query time: 0 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Sat Oct 31 12:59:27 CET 2020
;; MSG SIZE rcvd: 38

[cursoredes@localhost ~]$
```

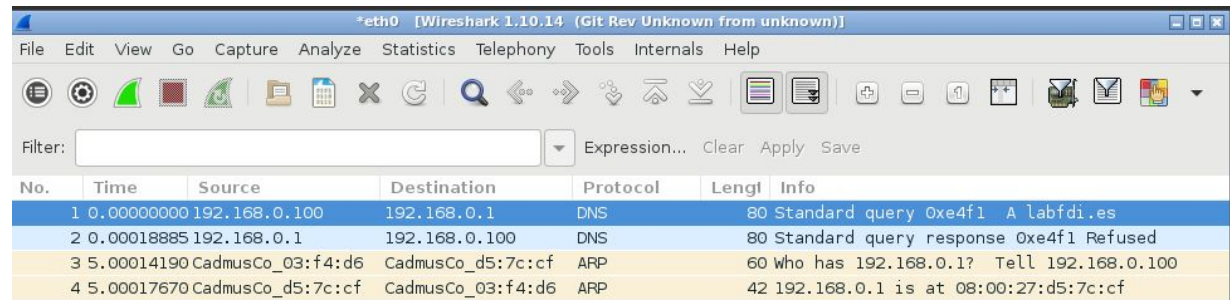
Ejercicio 11. Realizar más consultas y, con la ayuda de Wireshark:

- 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.

Copiar una captura de Wireshark con los mensajes DNS.

Desde VM2 aplicar comando “dig labfdi.es” y capturar con Wireshark por eth0 y ver protocolo DNS.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.0.100	192.168.0.1	DNS	80	Standard query 0xe4f1 A labfdi.es
2	0.00018885	192.168.0.1	192.168.0.100	DNS	80	Standard query response 0xe4f1 Refused
3	5.00014190	CadmusCo_03:f4:d6	CadmusCo_d5:7c:cf	ARP	60	Who has 192.168.0.1? Tell 192.168.0.100
4	5.00017670	CadmusCo_d5:7c:cf	CadmusCo_03:f4:d6	ARP	42	192.168.0.1 is at 08:00:27:d5:7c:cf

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/named.conf. El tipo de servidor de la zona debe ser master y el fichero que define la zona, db.0.168.192.

```

• sudo vim /var/named/db.labfdi.es

zone "0.168.192.in-addr.arpa." {
    type master;
    file "db.0.168.192";
};

```

Ejercicio 13. Crear el fichero 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. Después, reiniciar el servicio DNS con el comando `service named restart` (o bien, recargar la configuración con el comando `service named reload`).

Copiar el fichero de la zona inversa.

(Preguntar cómo configurar estos ficheros, este último me daba error)

- **sudo named-checkzone labfdi.es. /var/named/db.0.168.192**

zone labfdi.es/IN: NS 'ns.labfdi.es' has no address records (A or AAAA)
zone labfdi.es/IN: not loaded due to errors.

- **sudo vim /var/named/db.0.168.192**


```

$TTL 2d
0.168.192.in-addr.arpa. IN SOA ns.labfdi.es. contac@labfdi.es.(
    2003080800      ;serial number
    3h              ;refresh
    15M             ;update retry
    3W12h           ;expiry
    2h20M           ;nx ttl
)

@      IN NS    ns.labfdi.es.
@      IN PTR   ns.labfdi.es.
1      IN PTR   ns.labfdi.es.
50     IN PTR   labfdi.es.
250    IN PTR   mail.labfdi.es.

```

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

Copiar el comando utilizado y su salida.

```

[cursoredes@localhost var]$ service named start
Redirecting to /bin/systemctl start named.service
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to manage system services or units.
Authenticating as: cursoredes
Password:
==== AUTHENTICATION COMPLETE ====
[cursoredes@localhost var]$ dig 192.168.0.250

; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <<>> 192.168.0.250
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: SERVFAIL, id: 6624
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, udp: 4096
;; QUESTION SECTION:
;192.168.0.250.                IN      A

;; Query time: 9 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Sat Oct 31 13:44:38 CET 2020
;; MSG SIZE rcvd: 42

```