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.

Activar el **portapapeles bidireccional** (menú Dispositivos) en las máquinas virtuales.

Usar la opción de Virtualbox (menú Ver) para realizar **capturas de pantalla**.

La **contraseña** del usuario `cursoredes` es `cursoredes`.

Contenidos

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	a.nic.es.
a-nic.es	ucm.es.	86400	NS	crispin.sim.ucm.es.
crispin.sim.ucm.es	informatica.ucm.es.	86400	CNAME	ucm.es.
crispin.sim.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 @crispin.sim.ucm.es ucm.es. SOA

;; ANSWER SECTION:
ucm.es. 86400 IN SOA ucdns.sis.ucm.es. hostmaster.ucm.es. 2021100102 28800 7200 1209600 86400

Los campos más relevantes se encuentran en la parte de datos del registro:

1. Servidor de nombres primario de la zona
2. Email del administrador de la zona
3. Número serie de la zona (indica cuándo se actualizó la zona y cuántas veces en el día)
4. Segundos que deben pasar antes de que los servidores secundarios pregunten al maestro por los cambios en la zona.
5. Segundos que deben pasar antes de que los servidores secundarios vuelvan a preguntar al maestro si este no responde.
6. Segundos que deben pasar antes de que los servidores secundarios dejen de preguntar al maestro si sigue sin responder.
7. TTL.

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 @crispin.sim.ucm.es fdi.ucm.es. MX

;; ANSWER SECTION:
fdi.ucm.es. 86400 IN MX 5 alt1.aspmx.l.google.com.
fdi.ucm.es. 86400 IN MX 10 aspmx3.googlemail.com.
fdi.ucm.es. 86400 IN MX 10 aspmx2.googlemail.com.
fdi.ucm.es. 86400 IN MX 1 aspmx.l.google.com.
fdi.ucm.es. 86400 IN MX 5 alt2.aspmx.l.google.com.

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:

Servidor	Nombre	TTL	Tipo	Datos
`a.root-servers.net`	in-addr.arpa.	172800	NS	a.in-addr-servers.arpa.
a.in-addr-servers.arpa.	147.in-addr.arpa.	86400	NS	z.arin.net.
z.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: 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.

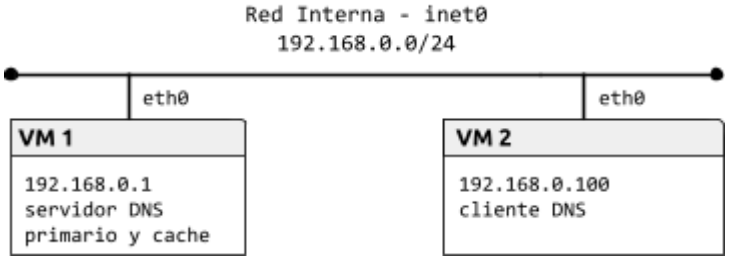
Copiar el comando utilizado y su salida.
dig A +additional +trace www.google.com. @8.8.4.4

```
; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8 <<>> A +additional +trace www.google.com.
@8.8.4.4
;; global options: +cmd
.                       33872   IN      NS      a.root-servers.net.
.                       33872   IN      NS      b.root-servers.net.
.                       33872   IN      NS      c.root-servers.net.
.                       33872   IN      NS      d.root-servers.net.
.                       33872   IN      NS      e.root-servers.net.
.                       33872   IN      NS      f.root-servers.net.
.                       33872   IN      NS      g.root-servers.net.
.                       33872   IN      NS      h.root-servers.net.
.                       33872   IN      NS      i.root-servers.net.
.                       33872   IN      NS      j.root-servers.net.
.                       33872   IN      NS      k.root-servers.net.
.                       33872   IN      NS      l.root-servers.net.
.                       33872   IN      NS      m.root-servers.net.
;; Received 228 bytes from 8.8.4.4#53(8.8.4.4) in 89 ms

com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      m.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      e.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
;; Received 495 bytes from 192.36.148.17#53(192.36.148.17) in 125 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 192.5.6.30#53(192.5.6.30) in 13 ms

www.google.com.         300     IN      A       142.250.191.132
;; Received 48 bytes from 216.239.34.10#53(216.239.34.10) in 11 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 `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*)

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:

```
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. La recursión debe estar deshabilitada en servidores autoritativos (opción `recursion`) y no deben restringirse las consultas (opción `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
Servidor de correo (MX)	El servidor de correo es `mail.labfdi.es`
Direcciones (A y AAAA) de los	La dirección de `ns.labfdi.es` es `192.168.0.1` (VM1). La

servidores	de `mail.labfdi.es` es `192.168.0.250`. Las de `www.labfdi.es` son `192.168.0.200` y `fd00::1`.
Nombre canónico (CNAME) de servidor	`correo.labfdi.es` es un *alias* 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 1d

labfdi.es. IN SOA ns.labfdi.es. contact.labfdi.es. (
            2021100400 ;
            86400 ; refresh = 24 horas segun RIPE 203
            7200 ; retry = 2 horas segun RIPE 203
            3600000 ; expire = 1000 horas segun RIPE 203
            3600 ; minimum = 1 hora segun RIPE 203
            )

           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
correo             IN CNAME mail.labfdi.es.
www        IN A  192.168.0.200
www        IN AAAA fd00::1
```

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.

```
[cursoredes@localhost ~]$ cat /etc/resolv.conf
search labfdi.es.
nameserver 192.168.0.1
```

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

Copiar los comandos utilizados y sus salidas.

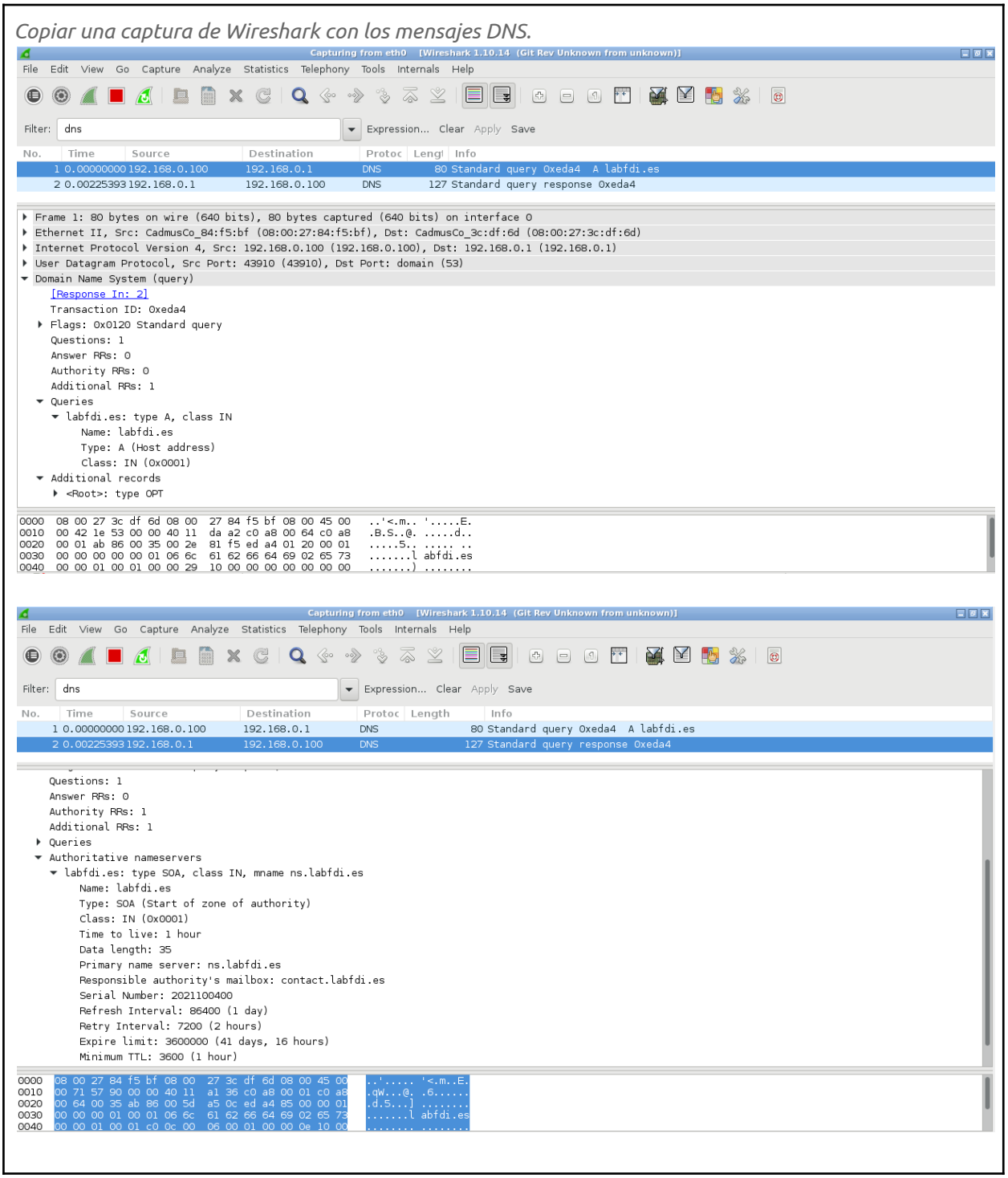
```
[cursoredes@localhost ~]$ dig labfdi.es.

; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <<>> labfdi.es.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35394
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

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

```
;; AUTHORITY SECTION:
labfdi.es.          3600    IN    SOA    ns.labfdi.es. contact.labfdi.es. 2021100400 86400 7200 3600000
3600

;; Query time: 3 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Sun Oct 03 16:14:25 CEST 2021
;; MSG SIZE  rcvd: 85

[cursoredes@localhost ~]$ dig www.labfdi.es. A

; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <<>> www.labfdi.es. A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27348
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
www.labfdi.es.          86400   IN      A       192.168.0.200

;; AUTHORITY SECTION:
labfdi.es.              86400   IN      NS      ns.labfdi.es.

;; ADDITIONAL SECTION:
ns.labfdi.es.           86400   IN      A       192.168.0.1

;; Query time: 3 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Sun Oct 03 16:19:28 CEST 2021
;; MSG SIZE  rcvd: 91
```

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.



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`.

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.

```
$TTL 1d

0.168.192.in-addr.arpa. IN SOA ns.labfdi.es. contact.labfdi.es. (
            2021100400 ;
            86400 ; refresh = 24 horas segun RIPE 203
            7200 ; retry = 2 horas segun RIPE 203
            3600000 ; expire = 1000 horas segun RIPE 203
            3600 ; minimum = 1 hora segun RIPE 203
            )
           IN NS ns.labfdi.es.

250.0.168.192.in-addr.arpa. PTR mail.labfdi.es.
100.0.168.192.in-addr.arpa. PTR www.labfdi.es.
1.0.168.192.in-addr.arpa.   PTR ns.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 ~]$ dig -x 192.168.0.250

; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <<>> -x 192.168.0.250
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40621
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;250.0.168.192.in-addr.arpa.    IN    PTR

;; ANSWER SECTION:
250.0.168.192.in-addr.arpa. 86400 IN    PTR    mail.labfdi.es.

;; AUTHORITY SECTION:
0.168.192.in-addr.arpa.    86400    IN    NS    ns.labfdi.es.

;; ADDITIONAL SECTION:
ns.labfdi.es.        86400    IN    A    192.168.0.1

;; Query time: 4 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Sun Oct 03 16:35:46 CEST 2021
;; MSG SIZE  rcvd: 116
```