

## 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

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](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.

**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:

Servidor	Nombre	TTL	Tipo	Datos
a.root-servers.net	es.	172800	NS	
g.nic.es	ucm.es.	86400	NS	
chico.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.

```

HOSTNAME: ucm.es.
TYPE: SOA
NAMESERVERS: chico.rediris.es

ucm.es.      86400 IN SOA ucdns.sis.ucm.es. hostmaster.ucm.es. (
                2021100401 ; 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](mailto:webmaster@fdi.ucm.es), usar un servidor autoritativo de la zona.

```

HOSTNAME: webmaster@fdi.ucm.es
TYPE: MX
NAMESERVERS: chico.rediris.es

webmaster\@fdi.ucm.es.      86400 IN      MX      5 alt1.aspmx.l.google.com.
webmaster\@fdi.ucm.es.      86400 IN      MX      10 ucsmtpt.ucm.es.
webmaster\@fdi.ucm.es.      86400 IN      MX      1 aspmx.l.google.com.
webmaster\@fdi.ucm.es.      86400 IN      MX      10 aspmx3.googlemail.com.
webmaster\@fdi.ucm.es.      86400 IN      MX      5 alt2.aspmx.l.google.com.
webmaster\@fdi.ucm.es.      86400 IN      MX      10 aspmx2.googlemail.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	<a href="#">in-addr.arpa.</a>	172800	NS	<a href="#">e.in-addr-servers.arpa.</a>
<a href="#">e.in-addr-servers.arpa.</a>	<a href="#">147.in-addr.arpa.</a>	86400	NS	<a href="#">x.arin.net.</a>
<a href="#">x.arin.net.</a>	<a href="#">96.147.in-addr.arpa.</a>	172800	NS	<a href="#">sun.rediris.es.</a>
<a href="#">sun.rediris.es.</a>	<a href="#">71.85.96.147.in-addr.arpa.</a>	86400	PTR	<a href="#">www.fdi.ucm.es.</a>

**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](http://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.

```

HOSTNAME: www.google.com
TYPE: A
NAMESERVERS: a.root-servers.net

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8 <<>> A +additional +trace www.google.com.
@a.root-servers.net
;; global options: +cmd
.                518400 IN      NS      e.root-servers.net.
.                518400 IN      NS      h.root-servers.net.
.                518400 IN      NS      l.root-servers.net.
.                518400 IN      NS      i.root-servers.net.
.                518400 IN      NS      a.root-servers.net.
.                518400 IN      NS      d.root-servers.net.
.                518400 IN      NS      c.root-servers.net.
.                518400 IN      NS      b.root-servers.net.
.                518400 IN      NS      j.root-servers.net.
.                518400 IN      NS      k.root-servers.net.
.                518400 IN      NS      g.root-servers.net.
.                518400 IN      NS      m.root-servers.net.
.                518400 IN      NS      f.root-servers.net.
;; Received 508 bytes from 198.41.0.4#53(198.41.0.4) in 58 ms

com.             172800 IN      NS      a.gtld-servers.net.
com.             172800 IN      NS      b.gtld-servers.net.
com.             172800 IN      NS      c.gtld-servers.net.
com.             172800 IN      NS      d.gtld-servers.net.
com.             172800 IN      NS      e.gtld-servers.net.
com.             172800 IN      NS      f.gtld-servers.net.
com.             172800 IN      NS      g.gtld-servers.net.
com.             172800 IN      NS      h.gtld-servers.net.
com.             172800 IN      NS      i.gtld-servers.net.
com.             172800 IN      NS      j.gtld-servers.net.
com.             172800 IN      NS      k.gtld-servers.net.
com.             172800 IN      NS      l.gtld-servers.net.
com.             172800 IN      NS      m.gtld-servers.net.
;; Received 508 bytes from 193.0.14.129#53(193.0.14.129) in 96 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 192.26.92.30#53(192.26.92.30) in 30 ms

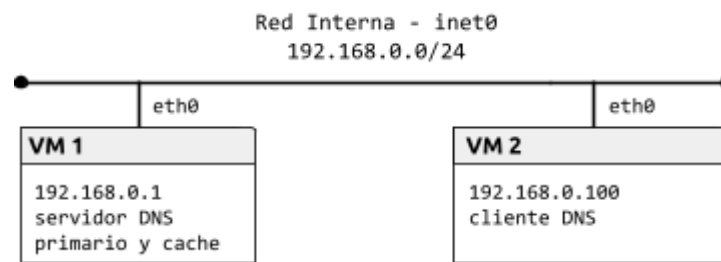
www.google.com.  300    IN      A      142.250.191.132
;; Received 48 bytes from 216.239.34.10#53(216.239.34.10) in 11 ms

```

## 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 servidores	La dirección de ns.labfdi.es es 192.168.0.1 (VM1). La 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 <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.

```
$TTL 2d ; TTL por defecto = 2 días o 172800 segundos
$ORIGIN labfdi.es.
;; REG SOA
labfdi.es.      IN  SOA ns.labfdi.es. contact.labfdi.es. (
                    2003080800 ; serial number (año,mes,día,secuencia)
                    3h         ; refresh = 3 horas
                    15M        ; update retry = 15 minutos
                    3W12h      ; expiry = 3 semanas + 12 horas
                    2h20M)     ; nx ttl = 2 horas + 20 minutos

;; REG NS
                IN  NS  ns.labfdi.es

;; MX
                IN  MX  10 mail ; equiv a mail.labfdi.es

;; A y AAAA
ns.labfdi.es.   IN  A   192.168.0.1
mail.labfdi.es. IN  A   192.168.0.250
www.labfdi.es.  IN  A   192.168.0.200
www.labfdi.es.  IN  AAAA fd00::1
correo.labfdi.es. IN CNAME mail.labfdi.es.
```

```
service named start
```

**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`.

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

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

```
dig www.labfdi.es
```

```

; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <<>> www.labfdi.es
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 46203
;; 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.                172800  IN      A      192.168.0.200

;; AUTHORITY SECTION:
labfdi.es.                    172800  IN      NS      ns.labfdi.es.

;; ADDITIONAL SECTION:
ns.labfdi.es.                 172800  IN      A      192.168.0.1

;; Query time: 0 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Sun Oct 10 17:16:26 CEST 2021
;; MSG SIZE rcvd: 81
dig labfdi.es.
[root@localhost cursoredes]# 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: 31906
;; 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.                    8400    IN      SOA     ns.labfdi.es. contact
.labfdi.es. 2003080800 10800 900 1857600 8400

;; Query time: 0 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Sun Oct 10 17:19:57 CEST 2021
;; MSG SIZE rcvd: 85

```

**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.

No.	Time	Source	Destination	Protoc	Lengl	Info
1	0.00000000	192.168.0.100	192.168.0.1	DNS	84	Standard query 0xfd37 A www.labfdi.es
2	0.00030938	192.168.0.1	192.168.0.100	DNS	133	Standard query response 0xfd37 A 192.168.0.200

▶	Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
▶	Ethernet II, Src: CadmusCo_95:20:9c (08:00:27:95:20:9c), Dst: CadmusCo_bc:a8:bd (08:00:27:bc:a8:bd)
▶	Internet Protocol Version 4, Src: 192.168.0.100 (192.168.0.100), Dst: 192.168.0.1 (192.168.0.1)
▶	User Datagram Protocol, Src Port: 59552 (59552), Dst Port: domain (53)
▼	Domain Name System (query)

[\[Response In: 2\]](#)

Transaction ID: 0xfd37

▼ Flags: 0x0120 Standard query

- 0... .. = Response: Message is a query
- .000 0... .. = Opcode: Standard query (0)
- .... ..0. .... = Truncated: Message is not truncated
- .... ..1. .... = Recursion desired: Do query recursively
- .... ..0.. .... = Z: reserved (0)
- .... ..1. .... = AD bit: Set
- .... ..0 .... = Non-authenticated data: Unacceptable

Questions: 1  
 Answer RRs: 0  
 Authority RRs: 0  
 Additional RRs: 1

- ▶ Queries
- ▶ Additional records

## 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).

```
zone "0.168.192.in-addr.arpa." {
    type master;
    file "/var/named/db.0.168.192";
};
```

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

```
dig 250.0.168.192.in-addr.arpa.

$TTL 2d ; TTL por defecto = 2 días o 172800 segundos
;; REG SOA
0.168.192.in-addr.arpa. IN SOA ns.labfdi.es. contact.labfdi.es. (
    2003080800 ; serial number (año,mes,día,secuencia)
    3h ; refresh = 3 horas
    15M ; update retry = 15 minutos
    3W12h ; expiry = 3 semanas + 12 horas
    2h20M) ; nx ttl = 2 horas + 20 minutos
```

```
;
@      IN  NS  ns.labfdi.es.
@      IN  PTR ns.labfdi.es.
1      IN  PTR ns.labfdi.es.
200    IN  PTR labfdi.es.
250    IN  PTR mail.labfdi.es.
```

*ns.labfdi.es*