

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 (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.	1728000	NS	
g.nic.es.	ucm.es.	86400	NS	
crispin.sim.ucm.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.

He utilizado el link de digweb y he puesto como host: ucm.es. ; tipo: SOA ; y servidor: crispin.sim.ucm.es.

La salida obtenida:

```
ucm.es.      86400 IN SOA ucdns.sis.ucm.es. hostmaster.ucm.es. (
                2021100601 ; serial
                28800  ; refresh (8 hours)
                7200   ; retry (2 hours)
                1209600 ; expire (2 weeks)
                86400  ; minimum (1 day) -> TTL
            )
```

Servidor primario de nombres de la zona:ucdns.sis.ucm.es.

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.

Al igual que en 3, he usado dicha página tal que host: webmaster@fdi.ucm.es. ; tipo: MX; y servidor: crispin.sim.ucm.es.

```
webmaster\@fdi.ucm.es.      86400 IN      MX      1 aspmx.l.google.com.
webmaster\@fdi.ucm.es.      86400 IN      MX      5 alt2.aspmx.l.google.com.
webmaster\@fdi.ucm.es.      86400 IN      MX      10 ucsmtip.ucm.es.
webmaster\@fdi.ucm.es.      86400 IN      MX      10 aspmx3.googlemail.com.
webmaster\@fdi.ucm.es.      86400 IN      MX      5 alt1.aspmx.l.google.com.
webmaster\@fdi.ucm.es.      86400 IN      MX      10 aspmx2.googlemail.com.
```

Como los números de la derecha de MX indican prioridad en orden decreciente, se tiene que el servidor de correo es: aspmx.l.google.com.

;; SERVER: 147.96.1.9#53(147.96.1.9)

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	
e.in-addr-servers.arpa.	147.in-addr.arpa.	86400	NS	
u.arin.net.	96.147.in-addr.arpa.	172800	NS	
sun.rediris.es.	71.85.96.147.in-addr.arpa.	86400	PTR	www.fdi.ucm.es. ESTE ES EL NOMBRE DEL DOMINIO

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.

De nuevo en la pagina usando la opción de nameserver a default.

```
dig +noadditional +noquestion +nocomments +nocmd +nostats +trace www.google.com. @8.8.4.4
```

```
.           63702 IN      NS       a.root-servers.net.
.           63702 IN      NS       b.root-servers.net.
.           63702 IN      NS       c.root-servers.net.
.           63702 IN      NS       d.root-servers.net.
.           63702 IN      NS       e.root-servers.net.
.           63702 IN      NS       f.root-servers.net.
.           63702 IN      NS       g.root-servers.net.
.           63702 IN      NS       h.root-servers.net.
.           63702 IN      NS       i.root-servers.net.
.           63702 IN      NS       j.root-servers.net.
.           63702 IN      NS       k.root-servers.net.
.           63702 IN      NS       l.root-servers.net.
.           63702 IN      NS       m.root-servers.net.
```

```
;; Received 228 bytes from 8.8.4.4#53(8.8.4.4) in 38 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 199.9.14.201#53(199.9.14.201) in 54 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 192.33.14.30#53(192.33.14.30) in 65 ms
```

```
www.google.com.      300 IN      A       142.250.191.132
```

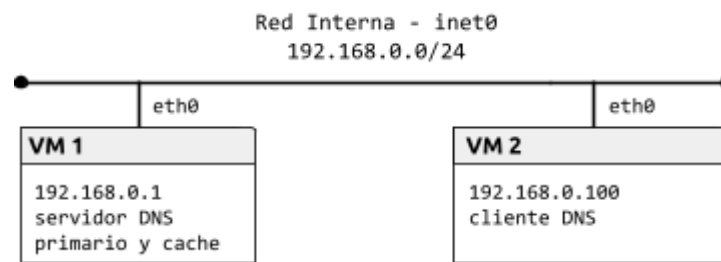
```
;; Received 48 bytes from 216.239.32.10#53(216.239.32.10) in 10 ms
```

La dirección ip de www.google.com es 142.250.191.132

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";
};
```

En options modificar:

```
allow-query {any;}
recursion no
```

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.

Copiar el fichero de la zona directa.

```
$TTL 172800
labfdi.es.      IN      SOA     ns.labfdi.es. contact.labfdi.es. (
                    2003080800 ; sn = serial number
                    172800    ; ref = refresh = 2d
                    900       ; ret = update retry = 15m
                    1209600   ; ex = expiry = 2w
                    3600      ; nx = nxdomain ttl = 1h
                )
               IN      NS      ns.labfdi.es.
ns.labfdi.es.  IN      A        192.168.0.1
www.labfdi.es. IN      A        192.168.0.200
www.labfdi.es. IN      AAAA     fd00::1
               IN      MX      10    mail.labfdi.es.
mail.labfdi.es. IN     A        192.168.0.250
correo.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 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 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: 16284
;; 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: 2 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Wed Oct 06 19:59:11 CEST 2021
;; MSG SIZE rcvd: 38
```

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	Length	Info
1	0.00000000	192.168.0.100	192.168.0.1	DNS	80	Standard query 0x7c96 A labfdi.es
2	0.00108458	192.168.0.1	192.168.0.100	DNS	80	Standard query response 0x7c96
3	5.00976263	CadmusCo_51:cf:f9	CadmusCo_5a:3f:05	ARP	42	Who has 192.168.0.1? Tell me
4	5.01060146	CadmusCo_5a:3f:05	CadmusCo_51:cf:f9	ARP	60	192.168.0.1 is at 08:00:27:5
5	18.3094958	192.168.0.100	192.168.0.1	DNS	84	Standard query 0xdf61 A www.labfdi.es
6	18.3104373	192.168.0.1	192.168.0.100	DNS	84	Standard query response 0xdf61
7	23.3225866	CadmusCo_5a:3f:05	CadmusCo_51:cf:f9	ARP	60	Who has 192.168.0.100? Tell me
8	23.3227332	CadmusCo_51:cf:f9	CadmusCo_5a:3f:05	ARP	42	192.168.0.100 is at 08:00:27:5

Los puertos son 53 en VM1 y 51071 en VM2

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`).

```
$TTL 172800
0.168.192.in-addr.arpa. IN      SOA  ns.labfdi.es. hostmaster.labfdi.es. (
    2003080800
    172800
    900
    1209600
```

```

        3600)
@      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.

```

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 250.0.168.192.in-addr.arpa.

; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <<>> 250.0.168.192.in-addr.arpa.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 39192
;; 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:
;250.0.168.192.in-addr.arpa.      IN      A

;; Query time: 1 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Wed Oct 06 20:30:24 CEST 2021
;; MSG SIZE rcvd: 55

```