

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	.	518400	NS	a.root-servers.net.
	es.	172800	NS	a.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.

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

`dig SOA +additional +multiline +trace ucm.es. @k.root-servers.net`

```
ucm.es.                86400 IN SOA ucdns.sis.ucm.es. hostmaster.ucm.es. (
                        2020102804 ; 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 MX +additional +trace webmaster@fdi.ucm.es. @k.root-servers.net`

```
webmaster\@fdi.ucm.es. 86400 IN MX 5 alt1.aspmx.l.google.com.
webmaster\@fdi.ucm.es. 86400 IN MX 10 aspmx3.googlemail.com.
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 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	.	518400	NS	a.root-servers.net.
	in-addr.arpa.	172800	NS	a.in-addr-servers.arpa.
	147.in-addr.arpa.	86400	NS	r.arin.net.
	96.147.in-addr.arpa.	172800	NS	chico.rediris.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. @a.root-servers.net

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.7 <<>> 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 55 ms

com.             172800 IN      NS      j.gtld-servers.net.
com.             172800 IN      NS      g.gtld-servers.net.
com.             172800 IN      NS      f.gtld-servers.net.
com.             172800 IN      NS      d.gtld-servers.net.
com.             172800 IN      NS      c.gtld-servers.net.
com.             172800 IN      NS      k.gtld-servers.net.
com.             172800 IN      NS      l.gtld-servers.net.
com.             172800 IN      NS      h.gtld-servers.net.
com.             172800 IN      NS      b.gtld-servers.net.
com.             172800 IN      NS      a.gtld-servers.net.
com.             172800 IN      NS      e.gtld-servers.net.
com.             172800 IN      NS      i.gtld-servers.net.
com.             172800 IN      NS      m.gtld-servers.net.
;; Received 492 bytes from 199.9.14.201#53(199.9.14.201) in 56 ms

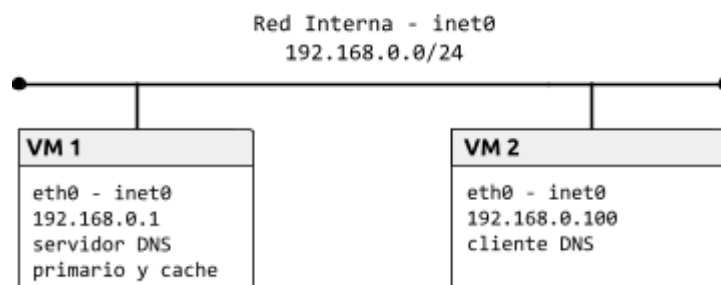
google.com.      172800 IN      NS      ns2.google.com.
google.com.      172800 IN      NS      ns1.google.com.
google.com.      172800 IN      NS      ns3.google.com.
google.com.      172800 IN      NS      ns4.google.com.
;; Received 280 bytes from 192.41.162.30#53(192.41.162.30) in 30 ms

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

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:

```
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
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`.

OJO QUE LOS NOMBRES TIENEN QUE SER IGUALES EN TODOS LOS SITIOS!!

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

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

IN NS ns.labfdi.es.
IN MX 10 mail.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
mail.labfdi.es. IN A 192.168.0.250
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 ns.labfdi.es.
domain 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.

Copiar el comando utilizado y su salida.

```
[root@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: 1073
;; 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

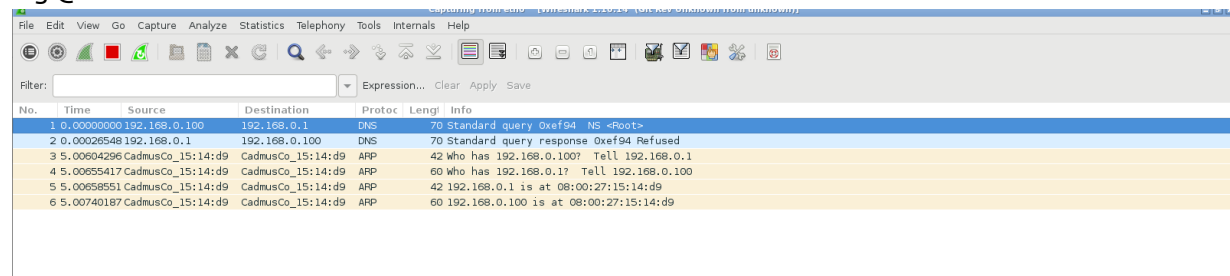
;; Query time: 1 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Thu Oct 29 11:48:13 CET 2020
;; MSG SIZE rcvd: 92
```

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.

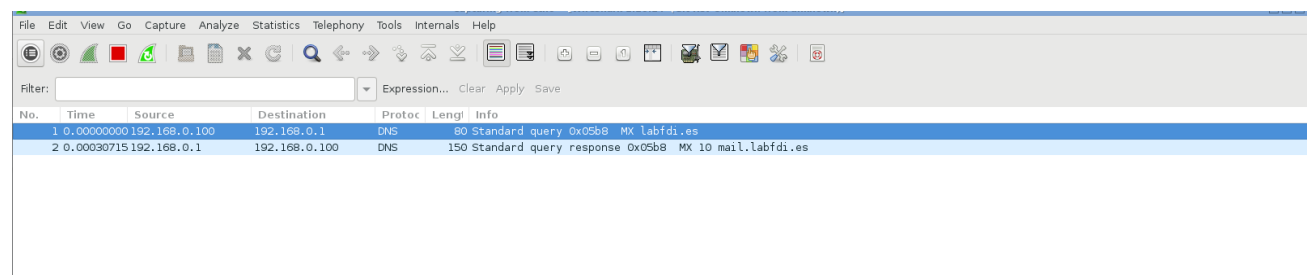
Dig @192.168.0.1



The image shows a Wireshark packet capture of a DNS query and response. The packet list shows a standard query for 'labfdi.es' from 192.168.0.1 to 192.168.0.1. The packet details pane shows the query structure, including the question section with 'labfdi.es. IN A'.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.0.100	192.168.0.1	DNS	70	Standard query 0x6f94 NS «Root»
2	0.00026548	192.168.0.1	192.168.0.100	DNS	70	Standard query response 0x6f94 Refused
3	5.00604296	CadmusCo_15:14:d9	CadmusCo_15:14:d9	APP	42	Who has 192.168.0.100? Tell 192.168.0.1
4	5.00695417	CadmusCo_15:14:d9	CadmusCo_15:14:d9	APP	60	Who has 192.168.0.1? Tell 192.168.0.100
5	5.00658551	CadmusCo_15:14:d9	CadmusCo_15:14:d9	APP	42	192.168.0.1 is at 08:00:27:15:14:d9
6	5.00740187	CadmusCo_15:14:d9	CadmusCo_15:14:d9	APP	60	192.168.0.100 is at 08:00:27:15:14:d9

Dig MX labfdi.es



The image shows a Wireshark packet capture of a DNS query and response for a mail exchange (MX) record. The packet list shows a standard query for 'MX labfdi.es' from 192.168.0.1 to 192.168.0.1. The packet details pane shows the query structure, including the question section with 'labfdi.es. IN MX'.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.0.100	192.168.0.1	DNS	80	Standard query 0x05b8 MX labfdi.es
2	0.00030715	192.168.0.1	192.168.0.100	DNS	150	Standard query response 0x05b8 MX 10 mail.labfdi.es

Dig SOA labfdi.es

3	59.7177250	192.168.0.100	192.168.0.1	DNS	80 Standard query 0x6507 SOA labfdi.es
4	59.7179171	192.168.0.1	192.168.0.100	DNS	164 Standard query response 0x6507 SOA ns.labfdi.es
5	64.7255868	CadmusCo_15:14:d9	CadmusCo_15:14:d9	ARP	42 Who has 192.168.0.100? Tell 192.168.0.1
6	64.7258926	CadmusCo_15:14:d9	CadmusCo_15:14:d9	ARP	60 Who has 192.168.0.1? Tell 192.168.0.100
7	64.7259108	CadmusCo_15:14:d9	CadmusCo_15:14:d9	ARP	42 192.168.0.1 is at 08:00:27:15:14:d9
8	64.7262369	CadmusCo_15:14:d9	CadmusCo_15:14:d9	ARP	60 192.168.0.100 is at 08:00:27:15:14:d9

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.

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

$TTL 2d;
0.168.192.in-addr.arpa. IN SOA ns.labfdi.es. contact@labfdi.es.(
    2003080800 ; serial number
    3h        ; refresh
    15M       ; update retry
    3W12h     ; expiry
    2h20M     ; nx ttl
)
@           IN   NS    ns.labfdi.es.
@           IN   MX    10 mail.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.

```
[root@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: NOERROR, id: 37062
;; 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:
```


;250.0.168.192.in-addr.arpa. IN A

:: AUTHORITY SECTION:

**0.168.192.in-addr.arpa. 8400 IN SOA ns.labfdi.es. contact\@labfdi.es. 2003080800
10800 900 1857600 8400**

:: Query time: 1 msec

:: SERVER: 192.168.0.1#53(192.168.0.1)

:: WHEN: Thu Oct 29 12:19:09 CET 2020

:: MSG SIZE rcvd: 118