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 `cursoredes` y contraseña `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`.

Hacemos **cat `/etc/resolv.conf`**
`El contenido del fichero es:`

```
; generated by /usr/sbin/dhclient-script
search Home
nameserver 192.168.0.1
```

Si miramos el manual: **man `resolv.conf`** `apreciamos para qué sirven las opciones:`

`nameserver:` `Dirección IPv4 o IPv6 de un servidor de nombres para resolver las consultas DNS. Si no hay ninguno se utiliza por defecto la dirección local. (El algoritmo es usarlos en orden en el que aparecen, pasando al siguiente si uno no nos responde).`

search: Lista de nombres de dominio que completarán nuestras consultas. (p.e si ponemos ponemos ucm.es, cuando hagamos ping fdi se hará un ping fdi.ucm.es). Se pueden poner hasta 6 nombres de dominio en esta lista.

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. (dir IPv4: 194.69.254.1)
a.nic.es.	ucm.es	86400	NS	crispin.sim.ucm.es. (dirIPv4: 147.96.1.9)
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.

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

El comando sería:
dig @crispin.sim.ucm.es. informatica.ucm.es. SOA

El registro es:
ucdns.sis.ucm.es. hostmaster.ucm.es. (
2020102301 ; serial
28800 ; refresh (8 hours)
7200 ; retry (2 hours)
1209600 ; expire (2 weeks)
86400 ; minimum (1 day)
)

El nombre de la zona es ucdns.sis.ucm.es.
El correo electrónico de contacto es: hostmaster@ucm.es.
El nº de serie (versión que tiene el servidor) es: 2020102301
Se refresca con el servidor primario cada 8 horas
Si hay algún fallo en zone transfer lo vuelve a intentar cada 2 horas
Deja de responder como servidor autoritativo en caso de que el primario no responda en 2 semanas
Pone un TTL para caché negativa de 1 día

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.

El comando sería:

dig @crispin.sim.ucm.es. `fdi.ucm.es`. MX
Obtenemos:

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

Como es más prioritario cuando más bajo sea el número de prioridad. Se usará el servidor que tiene prioridad 1, es decir, 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	e.in-addr-servers.arpa.
e.in-addr-servers.arpa.	147.in-addr.arpa.	86400	NS	r.arin.net.
r.arin.net.	96.147.in-addr.arpa.	172800	NS	chico.rediris.es.
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 + trace www.google.com. A

```
;; global options: +cmd
.                       86344   IN      NS      a.root-servers.net.
.                       86344   IN      NS      b.root-servers.net.
.                       86344   IN      NS      c.root-servers.net.
.                       86344   IN      NS      d.root-servers.net.
.                       86344   IN      NS      e.root-servers.net.
.                       86344   IN      NS      f.root-servers.net.
.                       86344   IN      NS      g.root-servers.net.
.                       86344   IN      NS      h.root-servers.net.
.                       86344   IN      NS      i.root-servers.net.
.                       86344   IN      NS      j.root-servers.net.
.                       86344   IN      NS      k.root-servers.net.
.                       86344   IN      NS      l.root-servers.net.
.                       86344   IN      NS      m.root-servers.net.
;; Received 228 bytes from 8.8.4.4#53(8.8.4.4) in 40 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 492 bytes from 198.97.190.53#53(198.97.190.53) in 105 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 192.48.79.30#53(192.48.79.30) in 28 ms

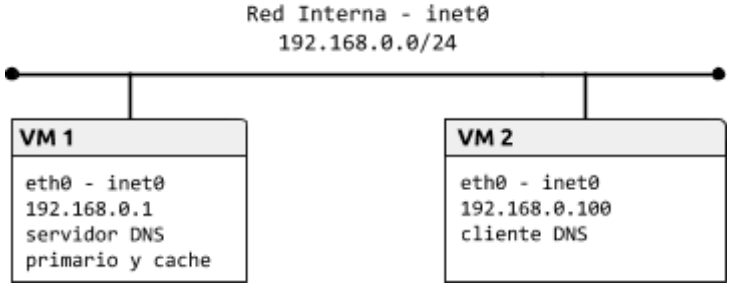
www.google.com. *300* *IN* *A* *172.217.4.68*
;; Received 48 bytes from 216.239.36.10#53(216.239.36.10) in 15 ms

La dir IPv4 de www.google.es. es 172.217.4.68

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:

```
Se ha puesto tras hacer nano /etc/named.conf
zone "labfdi.es." {
  type master;
  file "db.labfdi.es";
};
Ponemos allow-query { any; }; (MUY IMPORTANTE)

En recursión que ponía “recursion yes” se ha puesto “recursion no”.

Al hacer named-checkconf no obtenemos salida.
```

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 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 *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`. (service named reload para volver a cargarla)

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.

$ORIGIN 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
               IN MX 1 mail;
correo     IN CNAME mail
ns         IN A 192.168.0.1
www        IN A 192.168.0.200
mail       IN A 192.168.0.250
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.

; generated by /usr/sbin/dhclient-script
search labfdi.es
nameserver 192.168.0.1
```

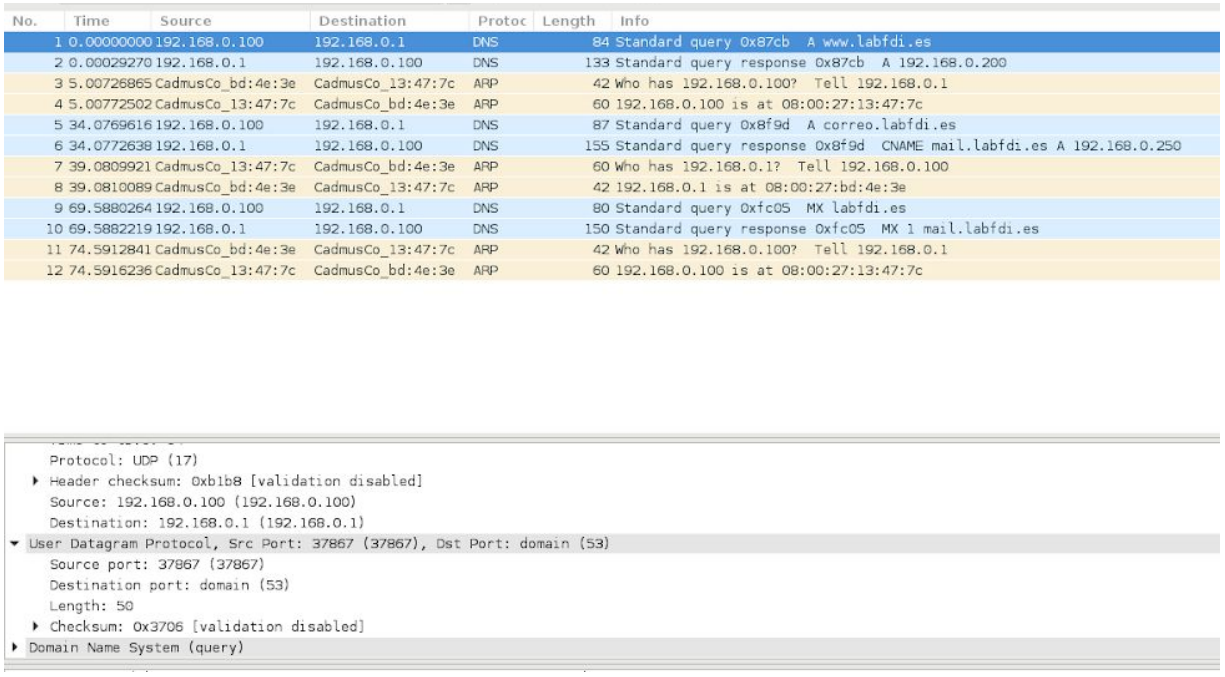
Ejercicio 10. Usar el comando `dig` en el cliente para obtener la información del dominio `labfdi.es`.

```
Copiar el comando utilizado y su salida.

Comando: dig labfdi.es.

Salida:

; <<>> 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: 28480
;; 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: Fri Oct 23 22:19:59 CEST 2020
;; 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.

Copiar una captura de Wireshark con los mensajes DNS.



No.	Time	Source	Destination	Protoc	Length	Info
1	0.00000000	192.168.0.100	192.168.0.1	DNS	84	Standard query 0x87cb A www.labfdi.es
2	0.00029270	192.168.0.1	192.168.0.100	DNS	133	Standard query response 0x87cb A 192.168.0.200
3	5.00726865	CadmusCo_bd:4e:3e	CadmusCo_13:47:7c	ARP	42	Who has 192.168.0.100? Tell 192.168.0.1
4	5.00772502	CadmusCo_13:47:7c	CadmusCo_bd:4e:3e	ARP	60	192.168.0.100 is at 08:00:27:13:47:7c
5	34.0769616	192.168.0.100	192.168.0.1	DNS	87	Standard query 0x8f9d A correo.labfdi.es
6	34.0772638	192.168.0.1	192.168.0.100	DNS	155	Standard query response 0x8f9d CNAME mail.labfdi.es A 192.168.0.250
7	39.0809921	CadmusCo_13:47:7c	CadmusCo_bd:4e:3e	ARP	60	Who has 192.168.0.1? Tell 192.168.0.100
8	39.0810089	CadmusCo_bd:4e:3e	CadmusCo_13:47:7c	ARP	42	192.168.0.1 is at 08:00:27:bd:4e:3e
9	69.5880264	192.168.0.100	192.168.0.1	DNS	80	Standard query 0xfc05 MX labfdi.es
10	69.5882219	192.168.0.1	192.168.0.100	DNS	150	Standard query response 0xfc05 MX 1 mail.labfdi.es
11	74.5912841	CadmusCo_bd:4e:3e	CadmusCo_13:47:7c	ARP	42	Who has 192.168.0.100? Tell 192.168.0.1
12	74.5916236	CadmusCo_13:47:7c	CadmusCo_bd:4e:3e	ARP	60	192.168.0.100 is at 08:00:27:13:47:7c


```
Protocol: UDP (17)
▸ Header checksum: 0xb1b8 [validation disabled]
Source: 192.168.0.100 (192.168.0.100)
Destination: 192.168.0.1 (192.168.0.1)
▾ User Datagram Protocol, Src Port: 37867 (37867), Dst Port: domain (53)
Source port: 37867 (37867)
Destination port: domain (53)
Length: 50
▸ Checksum: 0x3706 [validation disabled]
▸ Domain Name System (query)
```

Todos los mensajes son lo suficientemente pequeños como para que se hayan mandado usando el protocolo UDP. El servidor siempre está establecido en el puerto 53, y el cliente cambia en cada consulta, en el caso de la seleccionada en wireshark está en el puerto 37867.

Lo más interesante es que los mensajes de vuelta llevan desactivado el recursión avalaible, activado el AA de dominio autoritativo y en caso de responder con un RR de tipo NS en la sección adicional incluyen un RR de tipo A con su IP.

La longitud es mayor en las tramas de vuelta que en las de ida (lógico porque llevan más RR's)pero no llegan ni de lejos a 512 bytes como para usar TCP.

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`.

Añadimos:

```
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.

```
$TTL 2d;
@         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.
1        IN PTR ns.labfdi.es.
200      IN PTR www.labfdi.es.
250      IN PTR mail.labfdi.es.
ns.labfdi.es IN A 192.168.0.1
```

Metemos: named-checkzone 0.168.192.in-addr.arpa. /var/named/db.0.168.192

Y la salida es:

```
zone 0.168.192.in-addr.arpa/IN: loaded serial 2003080800
OK
```

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.

Comando: dig 250.0.168.192.in-addr.arpa. PTR

Salida:

```
; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <<>> 250.0.168.192.in-addr.arpa. PTR
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46848
;; 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. 172800 IN    PTR       mail.labfdi.es.

;; AUTHORITY SECTION:
0.168.192.in-addr.arpa.  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: Fri Oct 23 23:07:14 CEST 2020
;; MSG SIZE rcvd: 116

Efectivamente, en la sección de respuesta nos da el dominio mail.labfdi.es. que es el que tiene IP 192.1680.250.