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`.

En máquina base:
GNU nano 2.3.1 File: /etc/resolv.conf

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

nameserver Name server IP address
Internet address of a name server that the resolver should query, either an IPv4 address (in dot notation), or an IPv6 address in colon (and possibly dot) notation as per RFC 2373. Up to MAXNS (currently 3, see <resolv.h>) name servers may be listed, one per keyword. If there are multiple servers, the resolver library queries them in the order listed. If no name-server entries are present, the default is to use the name server on the local machine. (The algorithm used is to try a name server, and if the query times out, try the next, until out

of name servers, then repeat trying all the name servers until a maximum number of retries are made.)

search Search list for host-name lookup.
The search list is normally determined from the local domain name; by default, it contains only the local domain name. This may be changed by listing the desired domain search path following the search keyword with spaces or tabs separating the names. Resolver queries having fewer than ndots dots (default is 1) in them will be attempted using each component of the search path in turn until a match is found. For environments with multiple subdomains please read options ndots:n below to avoid man-in-the-middle attacks and unnecessary traffic for the root-dns-servers. Note that this process may be slow and will generate a lot of network traffic if the servers for the listed domains are not local, and that queries will time out if no server is available for one of the domains.

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.	172 800	NS	g.nic.es.
g.nic.es.	ucm.es.	864 00	NS	ucdns.sis.ucm.es.
ucdns.sis.ucm.es.	informatica.ucm.es	864 00	CNAME	ucm.es.
	ucm.es.	864 00	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.

En digweb: Hostname ucm.es. y nameserver ucdns.sis.ucm.es.. Typo SOA

```
; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8 <<>> SOA +additional +multiline ucm.es.
@ucdns.sis.ucm.es.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43136
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;ucm.es.                        IN SOA
```

```
;; ANSWER SECTION:
ucm.es.                 86400 IN SOA ucdns.sis.ucm.es. hostmaster.ucm.es. (
                                2022100304 ; serial
                                28800      ; refresh (8 hours)
                                7200       ; retry (2 hours)
                                1209600    ; expire (2 weeks)
                                86400      ; minimum (1 day)
                                )

;; Query time: 104 msec
;; SERVER: 147.96.2.4#53(147.96.2.4)
;; WHEN: Mon Oct  3 11:32:03 2022
;; MSG SIZE  rcvd: 81
```

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.

En digweb, hostname webmaster@fdi.ucm.es, nameserver ucdns.sis.ucm.es. Tipo MX

```
dig MX +additional webmaster@fdi.ucm.es. @ucdns.sis.ucm.es.
; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8 <<>> MX +additional webmaster@fdi.ucm.es.
@ucdns.sis.ucm.es.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2366
;; flags: qr aa rd; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;webmaster\@fdi.ucm.es.          IN      MX

;; ANSWER SECTION:
webmaster\@fdi.ucm.es.  86400   IN      MX      5 alt1.aspmx.l.google.com.
webmaster\@fdi.ucm.es.  86400   IN      MX      1 aspmx.l.google.com.
webmaster\@fdi.ucm.es.  86400   IN      MX      10 aspmx2.googlemail.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.
```

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.	172 800	NS	e.in-addr-servers.arpa.
e.in-addr-servers.arpa.	147.in-addr.arpa.	864 00	NS	y.arin.net.
y.arin.net.	96.147.in-addr.arpa.	864 00	NS	sun.rediris.es.

sun.rediris.es.	96.147.in-addr.arpa.	86400	NS	ucdns.sis.ucm.es.
ucdns.sis.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

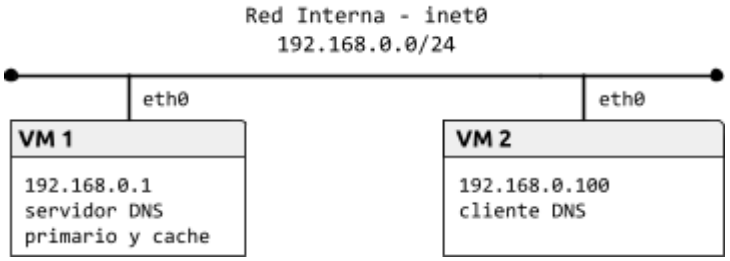
Ejercicio 6. Obtener la IP de `www.google.com` usando el servidor por defecto. Usar la opción `+trace` del comando `dig` (option "Trace" en el interfaz web) y observar las consultas realizadas.

En digweb: Hostname www.google.com, Nameserver default
www.google.com. 300 IN A 172.217.2.36

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` y 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.

```
$TTL 2d
$ORIGIN labfdi.es.
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          10 mail
correo        IN    CNAME   mail
ns            IN    A 192.168.0.1
www           IN    A 192.168.0.200
www           IN    AAAA    fd00::1
mail          IN    A 192.168.0.250



$sudo named-checkzone labfdi.es. /var/named/db.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`.

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

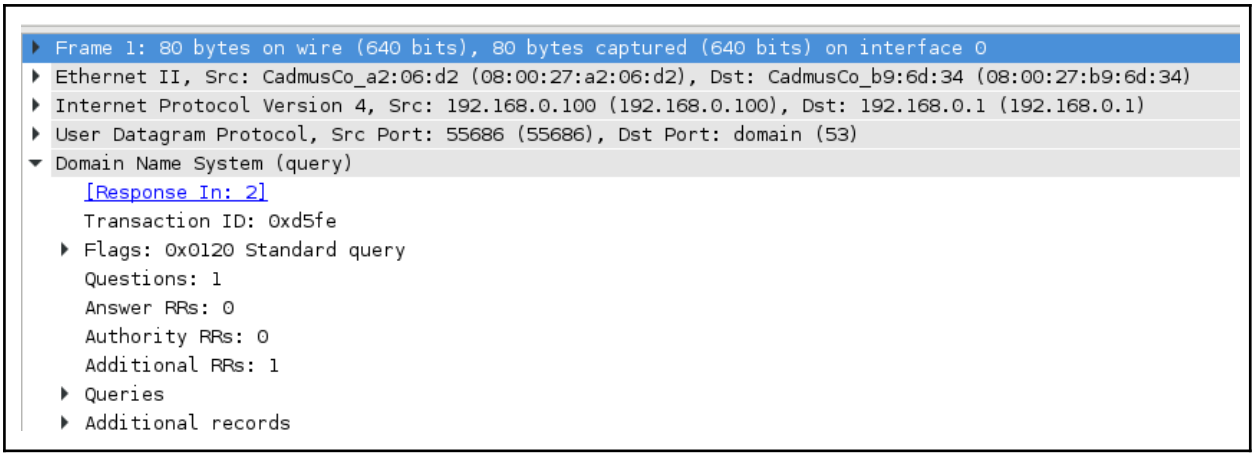
Ejercicio 10. Usar el comando `dig` en el cliente para obtener la información del dominio `labfdi.es`.

```
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: NOERROR, id: 39478
;; 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: Wed Oct 05 13:03:17 CEST 2022
;; 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	Lengt	Info
1	0.00000000	192.168.0.100	192.168.0.1	DNS	80	Standard query 0xd5fe A labfdi.es
2	0.00021465	192.168.0.1	192.168.0.100	DNS	127	Standard query response 0xd5fe
3	5.01368186	CadmusCo_b9:6d:34	CadmusCo_a2:06:d2	ARP	42	Who has 192.168.0.100? Tell 192.168.0.1
4	5.01471254	CadmusCo_a2:06:d2	CadmusCo_b9:6d:34	ARP	60	Who has 192.168.0.1? Tell 192.168.0.100
5	5.01474469	CadmusCo_b9:6d:34	CadmusCo_a2:06:d2	ARP	42	192.168.0.1 is at 08:00:27:b9:6d:34
6	5.01478847	CadmusCo_a2:06:d2	CadmusCo_b9:6d:34	ARP	60	192.168.0.100 is at 08:00:27:a2:06:d2



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 2d
0.168.192.in-addr.arpa.   IN      SOA    ns.labfdi.es.  contact.labfdi.es. (
                2003080805      ; 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.
```

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

```
[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: NOERROR, id: 26593
;; 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. 2003080805 10800 900
1857600 8400

;; Query time: 0 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Wed Oct 05 13:12:50 CEST 2022
;; MSG SIZE  rcvd: 111
```