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`.

```
usuario_vms@pto0709:~$ cat /etc/resolv.conf

nameserver 147.96.85.57
nameserver 147.96.85.61
nameserver 147.96.85.62

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 ad-
       dress 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 re-
       solver 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.
By default, the search list contains one entry, the local domain name. It is determined from the local hostname returned by gethostname(2); the local domain name is taken to be everything after the first '.'. Finally, if the hostname does not contain a '.', the root domain is assumed as the local domain name.

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	g.nic.es.
g.nic.es.	ucm.es.	86400	NS	crispin.sim.ucm.es.
crispin.sim.ucm.es.	informatica.ucm.es.	86400	CNAME	ucm.es.
crispin.sim.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.

dig SOA +additional +multiline ucm.es. @chico.rediris.es.

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

```
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`, usar un servidor autoritativo de la zona.

dig MX +additional webmaster@fdi.ucm.es. @chico.rediris.es.

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

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	x.arin.net.
x.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.

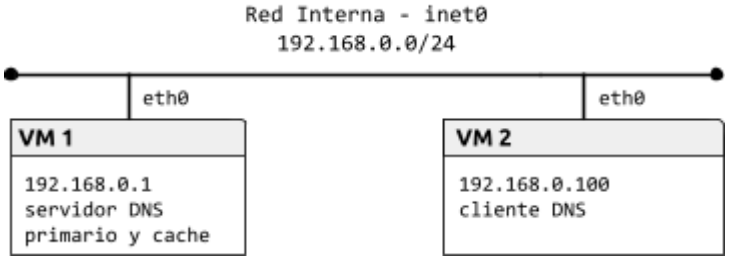
```
dig +noadditional +noquestion +nocomments +nocmd +nostats +trace www.google.com. @8.8.4.4
.                       42697   IN      NS      a.root-servers.net.
.                       42697   IN      NS      b.root-servers.net.
.                       42697   IN      NS      c.root-servers.net.
.                       42697   IN      NS      d.root-servers.net.
.                       42697   IN      NS      e.root-servers.net.
.                       42697   IN      NS      f.root-servers.net.
.                       42697   IN      NS      g.root-servers.net.
.                       42697   IN      NS      h.root-servers.net.
.                       42697   IN      NS      i.root-servers.net.
.                       42697   IN      NS      j.root-servers.net.
.                       42697   IN      NS      k.root-servers.net.
.                       42697   IN      NS      l.root-servers.net.
.                       42697   IN      NS      m.root-servers.net.
;; Received 228 bytes from 8.8.4.4#53(8.8.4.4) in 41 ms

;; Truncated, retrying in TCP mode.
com.                    172800 IN       NS      e.gtld-servers.net.
com.                    172800 IN       NS      b.gtld-servers.net.
com.                    172800 IN       NS      j.gtld-servers.net.
com.                    172800 IN       NS      m.gtld-servers.net.
com.                    172800 IN       NS      i.gtld-servers.net.
com.                    172800 IN       NS      f.gtld-servers.net.
com.                    172800 IN       NS      a.gtld-servers.net.
com.                    172800 IN       NS      g.gtld-servers.net.
com.                    172800 IN       NS      h.gtld-servers.net.
com.                    172800 IN       NS      l.gtld-servers.net.
com.                    172800 IN       NS      k.gtld-servers.net.
com.                    172800 IN       NS      c.gtld-servers.net.
com.                    172800 IN       NS      d.gtld-servers.net.
;; Received 828 bytes from 198.41.0.4#53(198.41.0.4) in 59 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 30 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
```

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:

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// See the BIND Administrator's Reference Manual (ARM) for details about the
// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html

options {
       listen-on port 53 { any; };
       listen-on-v6 port 53 { any; };
       directory     "/var/named";
       dump-file     "/var/named/data/cache_dump.db";
       statistics-file "/var/named/data/named_stats.txt";
       memstatistics-file "/var/named/data/named_mem_stats.txt";
       allow-query     { localhost; };

       /*
        - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
        - If you are building a RECURSIVE (caching) DNS server, you need to enable
```

```
         recursion.
        - If your recursive DNS server has a public IP address, you MUST enable
access
         control to limit queries to your legitimate users. Failing to do so will
         cause your server to become part of large scale DNS amplification
         attacks. Implementing BCP38 within your network would greatly
         reduce such attack surface
      */
      recursion yes;

      dnssec-enable yes;
      dnssec-validation yes;

      /* Path to ISC DLV key */
      bindkeys-file "/etc/named.iscdlv.key";

      managed-keys-directory "/var/named/dynamic";

      pid-file "/run/named/named.pid";
      session-keyfile "/run/named/session.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
      type hint;
      file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";


Fichero:
zone "labfdi.es" {
  type master;
  file "/var/named/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 *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 ; TTL por defecto = 2 días o 172800 segundos
labfdi.es.          IN SOA ns.labfdi.es. contact.labfdi.es. (
                    20211004   ; 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.

                    IN MX 10 mail.labfdi.es.

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.



[cursoredes@localhost ~]$ sudo named-checkzone labfdi.es /var/named/db.labfdi.es
zone labfdi.es/IN: loaded serial 20211004
OK
```

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`.

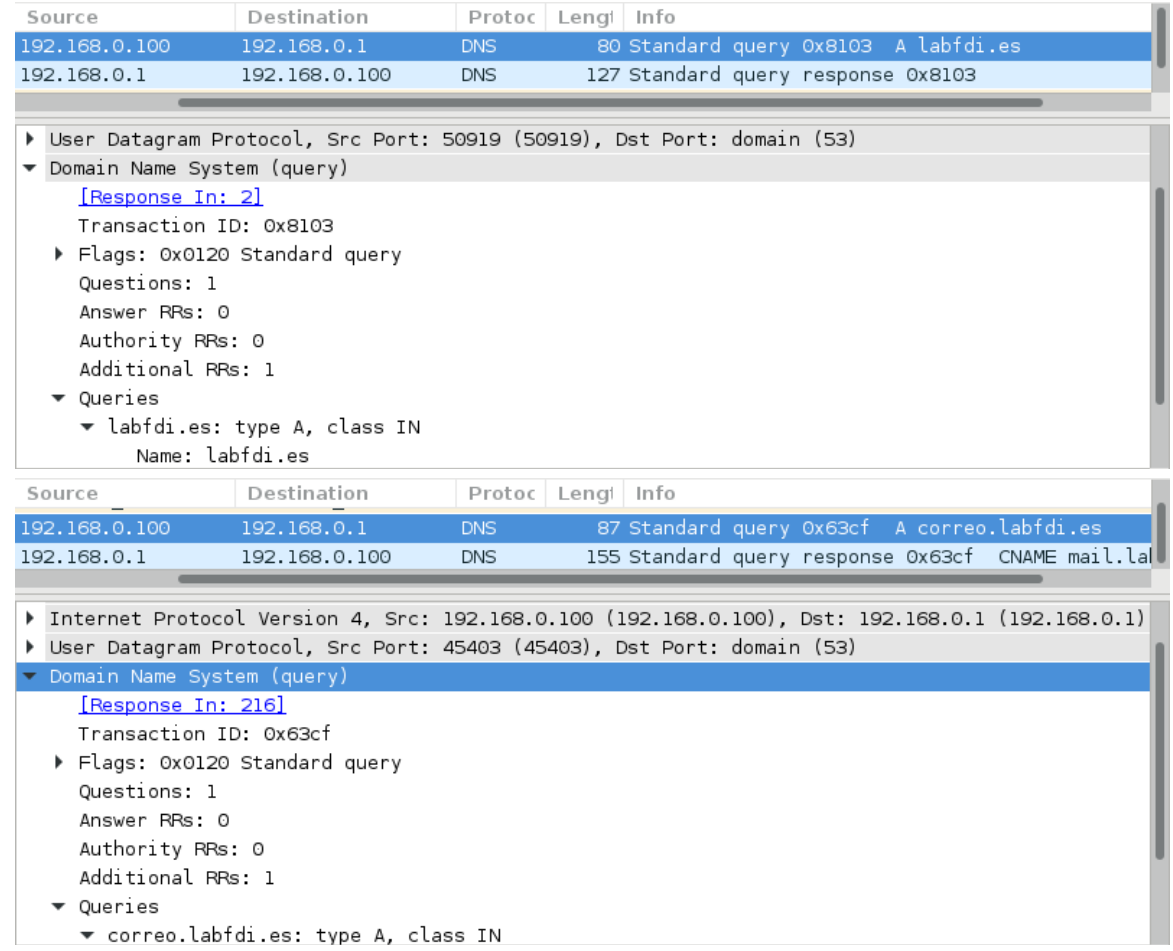
```
; generated by /usr/sbin/dhclient-script
search ns.labfdi.es
nameserver 192.168.0.1
```

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

```
[cursoredes@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: 13235
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;labfdi.es.                     IN      A

;; AUTHORITY SECTION:
labfdi.es.              3600    IN      SOA     ns.labfdi.es. contact.labfdi.es. 20211004 172800 900
1209600 3600

;; Query time: 0 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Sat Oct 09 17:11:02 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.



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`.

```
Fichero:
zone "labfdi.es" {
  type master;
  file "/var/named/db.labfdi.es";
};

zone "0.168.192.in-addr.arpa." {
  type master;
  file "/var/named/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 ; TTL por defecto = 2 días o 172800 segundos
0.168.192.in-addr.arpa.  IN SOA ns.labfdi.es contact.labfdi.es. (
                         20211005  ; 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.
                         IN PTR ns.labfdi.es.

1                        IN PTR   ns.labfdi.es.
250                      IN PTR   mail.labfdi.es.
200                      IN PTR   www.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: 29865
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; 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.  3600  IN  SOA  ns.labfdi.es.0.168.192.in-addr.arpa. contact.labfdi.es.
20211005 172800 900 1209600 3600

;; Query time: 1 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Sat Oct 09 17:25:07 CEST 2021
;; MSG SIZE  rcvd: 121
```