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 el fichero de configuración del cliente DNS se encuentra la siguiente información:

nameserver 147.96.85.57

nameserver 147.96.85.61

nameserver 147.96.85.62

En la página de manual de resolv.conf, encontramos las siguientes definiciones:
"The resolver is a set of routines in the C library that provide access to the Internet Domain Name System (DNS). The resolver configuration file contains information that is read by the resolver routines the first time they are invoked by a process."
`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."
`Search`: "Search list for host-name lookup. By default, the search list contains one entry, 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	chico.rediris.es
chico.rediris.es	informatica.ucm.es.	77512	CNAME	ucm.es.
	ucm.es.	77296	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.

Hemos accedido a la información desde www.digwebinterface.com. Con escribir en hostNames ucm.es. y elegir el tipo SOA, obtenemos esta salida:

```
ucm.es.   21567 IN SOA ucdns.sis.LAFns.INucm.es. hostmaster.ucm.es. (
                                2022100304 ; serial
                                28800      ; refresh (8 hours)
                                7200       ; retry (2 hours)
                                1209600    ; expire (2 weeks)
                                86400      ; minimum (1 day)
                                )
```

Nombre: ucm.es.
TTL: 21567
Servidor primario de nombres de la zona: ucdns.sis.ucm.es.
Email de contacto: hostmaster.ucm.es.
La información entre paréntesis son temporizadores (medidos en segundos): comprueba cambios cada 'refresh' segundos, en caso de fallo reintenta cada 'retry' segundos, sirve 'expire' segundos el dominio si no hay primario y establece TTL de las respuestas negativas a 'minimum' segundos

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.
Hemos accedido a la información desde www.digwebinterface.com. Escribimos webmaster@fdi.ucm.es, tipo MX y nameserver autoritativo. La salida es la siguiente:

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

El servidor de correo a usar debería ser aspmx.l.google.com, por ser el servidor con mayor prioridad (menor número).

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	86400	NS	sun.rediris.es.
sun.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.
Desde la página digwebinterface.com, hemos especificado el hostname www.google.com, type sin especificar, opción "trace" y nameserver por defecto.

La salida es la siguiente:

```
.                       70952   IN      NS      e.root-servers.net.
.                       70952   IN      NS      h.root-servers.net.
.                       70952   IN      NS      l.root-servers.net.
.                       70952   IN      NS      i.root-servers.net.
.                       70952   IN      NS      a.root-servers.net.
.                       70952   IN      NS      d.root-servers.net.
.                       70952   IN      NS      c.root-servers.net.
.                       70952   IN      NS      b.root-servers.net.
.                       70952   IN      NS      j.root-servers.net.
.                       70952   IN      NS      k.root-servers.net.
.                       70952   IN      NS      g.root-servers.net.
.                       70952   IN      NS      m.root-servers.net.
.                       70952   IN      NS      f.root-servers.net.
;; Received 228 bytes from 8.8.4.4#53(8.8.4.4) in 36 ms

com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
```

com. 172800 IN NS c.gtld-servers.net.
;; Received 495 bytes from 192.33.4.12#53(192.33.4.12) in 37 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

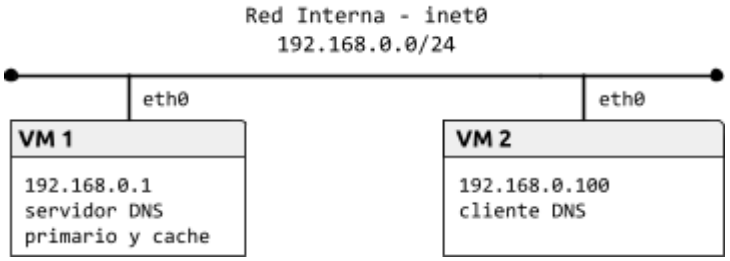
www.google.com. 300 IN A 172.217.2.36
;; Received 48 bytes from 216.239.34.10#53(216.239.34.10) in 11 ms

Por tanto, la dirección IP de www.google.com es 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:

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

Al ejecutar el comando `named-checkconf` *no salta ningún error.*

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.

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 10 mail

ns  IN A    192.168.0.1
mail IN A    192.168.0.250
www  IN A    192.168.0.200
www  IN AAAA fd00::1
correo 86400 IN CNAME mail

[VM1]
sudo named-checkzone labfdi.es. /var/named/db.labfdi.es
zone labfdi.es/IN: loaded serial 2003080800
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`.

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`.

No sabemos por qué, pero en el cliente no nos deja. Si usamos el comando desde el servidor, sale lo siguiente:
[VM1]

```
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: 14685
;; 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: Thu Oct 06 14:02:28 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.

Copiar una captura de Wireshark con los mensajes 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`.

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

[VM1]
sudo named-checkzone 0.168.192.in-addr.arpa. /var/named/db.0.168.192
zone 0.168.192.in-addr.arpa/IN: loaded serial 2003080800
OK

sudo service named restart
Redirecting to /bin/systemctl restart named.service

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:

[VM1]

dig 250.0.168.192.in-addr.arpa. PTR

; <<>> 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: 4085
;; 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: Thu Oct 06 14:01:24 CEST 2022
;; MSG SIZE rcvd: 116