Práctica 1.3. Domain Name System (DNS)

Objetivos

En esta práctica 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 funcionamiento del protocolo. Previamente, emplearemos herramientas cliente DNS para explorar la estructura del servicio en Internet.

Contenidos

Preparación del entorno para la práctica

En la primera parte de la práctica (Cliente DNS), **usaremos la máquina física del puesto del laboratorio**.

Para la segunda parte de la práctica (Servidor DNS), configuraremos la topología de red que se muestra en la Figura 1. Como en prácticas anteriores, construiremos la topología con la herramienta `vtopol` y un archivo de topología adecuado. Antes de comenzar esa parte, configurar los interfaces de red como se indica en la figura y comprobar la conectividad entre las máquinas.

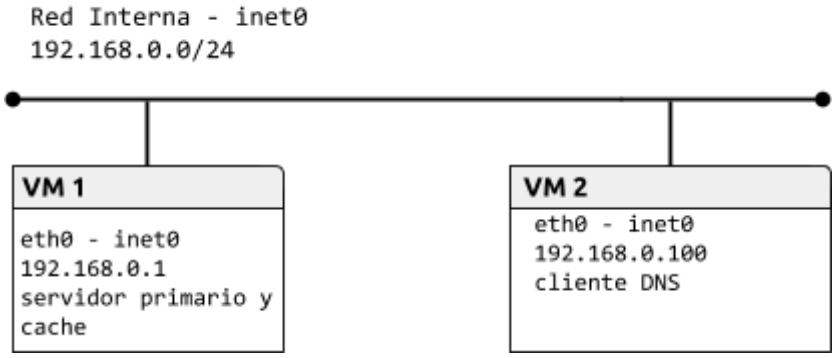

Figura 1: Topología y direccionamiento de la red usada en la práctica

Cliente DNS

En esta primera parte usaremos las herramientas 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. Las herramientas principales para consultar un servicio DNS son `dig` y `host`. Para esta primera parte **se usará la máquina física del puesto del laboratorio**. Si las consultas DNS a determinados servidores estuvieran bloqueadas, **usar un interfaz web** como www.digwebinterface.com (activando las opciones "Stats" y "Show command").

Configuración de las VMs:

VM1:

$sudo ip link set eth0 up
$sudo ip address add 192.168.0.1/24 dev eth0

VM2:

$sudo ip link set eth0 up
$sudo ip address add 192.168.0.100/24 dev eth0

Ejercicio 1. El archivo de configuración del cliente DNS es `/etc/resolv.conf`. Consultar la página de manual de `resolv.conf` y estudiar el significado de las opciones `nameserver` y `search`. Ver el contenido del archivo en la máquina física del laboratorio.

- Resolv.conf: conjunto de rutinas que proporcionan el acceso al DNS de internet.
- Nameserver: dirección ip de un servidor de DNS.
- Search: lista de búsqueda de nombres de host.

Ejercicio 2. Partiendo únicamente del servidor raíz `a.root-servers.net` y de las respuestas obtenidas de cada servidor obtener la dirección IP de `informatica.ucm.es`. Determinar el TTL de cada registro y completar la siguiente tabla:

Rellenado con: https://www.digwebinterface.com/

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.
	ucm.es.	86400	A	147.96.1.15

NOTA: Usar el comando `dig @<servidor> <nombre> <tipo>`. Más información en la página de manual de `dig`.

Tipos de registros:

- **SOA:** marca el comienzo de definicio´n de una zona.
- **NS**: especifica los servidores autoritativos para la zona e incluye los servidores de nombres de los subdominios delegados a otras organizaciones.
- **A:** El registro Address (A para IPv4 y AAAA para IPv6) es la base de DNS. Incluye la traducción directa (nombre → IP).
- **PTR:** El registros Pointer contiene la traducción inversa (IP → nombre)
- **MX**: es usado por los sistemas de correo para encaminar los mensajes eficientemente. Permite recibir de forma centralizada el correo de una organización.

Ejercicio 3. Obtener el registro SOA de `ucm.es.` usando un servidor autoritativo de la zona. Identificar los campos relevantes del registro.

Servidor autoritativo: crispin.sim.ucm.es.

```
ucm.es.                 86400 IN SOA ucdns.sis.ucm.es. hostmaster.ucm.es. (
                        2018122002 ; serial
                        28800      ; refresh (8 hours)
                        7200       ; retry (2 hours)
                        1209600    ; expire (2 weeks)
                        86400      ; minimum (1 day)
                        )
```

Ejercicio 4. Determinar qué servidor debería usarse para enviar un mail a webmaster@fdi.ucm.es, usar un servidor autoritativo de la zona.

Type: MX

```
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    10 ucsmtp.ucm.es.
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    5 alt2.aspmx.l.google.com.
```

Ejercicio 5. Determinar el nombre de dominio para `147.96.85.71`. Al igual que en el ejercicio 2, usar únicamente el servidor raíz `a.root-servers.net` y las respuestas obtenidas a partir de éste. Completar la siguiente tabla:

Servidor	Nombre	TTL	Tipo	Datos
a.root-servers.net	147.in-addr.arpa.	86400	NS	u.arin.net.
u.arin.net.	96.147.in-addr.arpa	172800	NS	ns.ripe.net.
ns.ripe.net.	71.85.96.147.in-addr.arpa.	86400	PTR	www.fdi.ucm.es.

NOTA: La opción `-x` de `dig` (en el interfaz web, se activa seleccionando “Reverse” como tipo de registro) 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.

Ejercicio 6. Obtener la IP de `www.google.com` usando el servidor por defecto. Usar el comando `dig` con la opción `+trace` y observar las consultas realizadas.

```
www.google.com.          300    IN     A      172.217.4.36
```

Servidor DNS

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 1. 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 archivo 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. Por ejemplo, la recursión debe estar deshabilitada en servidores autoritativos y las consultas pueden estar restringidas a solo ciertas máquinas.

Una vez creado el archivo de configuración, ejecutar el comando `named-checkconf` para comprobar que la sintaxis es correcta.

EN VM1:

$sudo nano /etc/named.conf
Comentar los “include”
$sudo name-checkconf

Ejercicio 2. Crear el archivo 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)	Descripción de la zona. Se pueden elegir libremente los valores de refresh, update, expiry y nx ttl. El servidor primario de la zona 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	El nombre canónico de `servidor.labfdi.es` es `mail.labfdi.es`

Una vez generado el archivo de zona, se debe comprobar su integridad con el comando `named-checkzone <nombre_zona> <archivo>`.

En VM1:

$sudo nano /var/named/db.labfdi.es

```
$TTL 2d

labfdi.es. IN     SOA     ns.labfdi.es     hostmaster.labfdi.es(

                          2003080800   ; Serial
                          3h           ; Refresh
                          14M          ; Retry
                          3W12h        ; Expire
                          2h20M        ; Negative Cacha TTL
       )

               IN     NS      ns.labfdi.es.
ns.lab.fdi.es.    IN     A       192.168.0.1
www.labfdi.es.  IN        A      192.168.0.200
www.labfdi.es.  IN        AAAA   fd00::1
             IN     MX     10     mail.labfdi.es.
mail.labfdi.es. IN        A      192.168.0.250
ser.labfdi.es.   IN       CNAME   mail.labfdi.es.
```

$sudo named-checkzone labfdi.es. /etc/bind/db.labfdi.es

NOTA: No olvidar que los nombres FQDN terminan en el dominio raíz (“`.`”). El nombre de la zona puede especificarse con `@` en el campo nombre del registro.

Ejercicio 3. Arrancar el servicio DNS con el comando `service named start.`

```
$sudo service named start
```

Ejercicio 4. 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`. Probar la resolución de nombres para `www.labfdi.es`.

En VM2:

$sudo nano /etc/resolv.conf
domain ns.labfdi.es
nameserver 192.168.0.1
search ns.labfdi.es

$sudo dig www.labfdi.es

Ejercicio 5. Usar el comando `dig` para obtener la información del dominio `labfdi.es` ofrecida por el servidor.

$sudo dig labfdi.es

Ejercicio 6. Repetir alguna de las consultas anteriores 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.

$sudo dig www.labfdi.es

DNS Standard query.

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 1. 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 archivo que define la zona, `db.0.168.192`.

En VM1:

$sudo nano /etc/named.conf

Añadir en el archivo:

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

```
$sudo named-checkconf /etc/named.conf
```

Ejercicio 2. Crear el archivo 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.

VM1:

```
$nano /var/named/db.0.168.192
```

```
----
$TTL   604800
0.168.192.in-addr.arpa. IN SOA ns.labfdi.es. hostmaster.labfdi.es. (
                          2           ; Serial
                          604800       ; Refresh
                          86400        ; Retry
                          2419200      ; Expire
```

```
                        604800       ; Negative Cache TTL
);
@                   IN     NS     ns.labfdi.es.
@                   IN     PTR    ns.labfdi.es.
1                   IN     PTR    ns.labfdi.es.
200                 IN     PTR    labfdi.es.
250                 IN     PTR    mail.labfdi.es.
```

`$named-checkzone 0.168.192.in-addr.arpa. /var/named/db.0.168.192`

Ejercicio 3. Reiniciar el servicio DNS con el comando `service named restart` (o bien, recargar la configuración con el comando `service named reload`).

$sudo service named restart

Ejercicio 4. Comprobar el funcionamiento de la resolución inversa, obteniendo el nombre asociado a `192.168.0.250`.

$sudo dig 250.0.168.192.in-addr.arpa