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 BIND9. El objetivo es estudiar tanto los pasos básicos de configuración del servicio, como la base de datos y el funcionamiento del protocolo.

Contenidos

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**. Como las consultas DNS a determinados servidores están bloqueadas en la red de la UCM, **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`.

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 añadiendo tantas filas como sea necesario:

Servidor	Nombre	TTL	Tipo	Datos
`a.root-servers.net`				

Nota: Si se usa la herramienta dig desde línea de comandos, la sintaxis es `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.

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.

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 añadiendo tantas filas como sea necesario:

Servidor	Nombre	TTL	Tipo	Datos
a.root-servers.net				

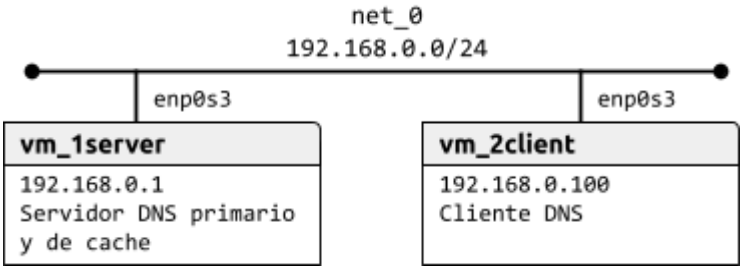
Nota: La opción `-x` de `dig` facilita la búsqueda inversa cuando detecta una dirección IP como argumento, creando el dominio de búsqueda a partir de la dirección IP (esto es, invierte el orden de los bytes y añade `.in-addr.arpa.`) y estableciendo el tipo de registro por defecto a PTR. En el interfaz 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` (opción "Trace" en el interfaz web) y observar las consultas realizadas.

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*)

vm_1server 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/bind/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 "/etc/bind/db.labfdi.es";
};
```

Revisar la configuración por defecto y consultar la página de manual `named.conf(5)` para ver las opciones disponibles para el servidor y las zonas. En los servidores autoritativos debemos deshabilitar la recursión, simplemente añadir la opción `recursion false;` en el fichero `named.conf.options`. 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 `/etc/bind/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 email 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)	La dirección de `ns.labfdi.es` es `192.168.0.1` (vm_1server), 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)	`correo.labfdi.es` es un *alias* de `mail.labfdi.es`

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.

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 `systemctl start named`.

Comprobar que el el servicio `named` ha arrancado correctamente con el comando `systemctl status named` y verificar que está escuchando en el puerto 53 UDP y TCP con el comando `ss`. ¿A qué direcciones se ha enlazado el socket?

Ejercicio 9. Configurar vm_2client para que use vm_1server como servidor de nombres. Para ello, crear o modificar el fichero `/etc/resolv.conf` con los valores apropiados para `nameserver` y `search`.

Ejercicio 10. Usar el comando `dig` en vm_2client para obtener la información del dominio `labfdi.es`.

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/bind/named.conf`. El tipo de servidor de la zona debe ser `master` y el fichero que define la zona, `/etc/bind/db.0.168.192`.

Ejercicio 13. Crear el fichero de la zona inversa en `/etc/bind/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 `systemctl restart named` (o bien, recargar la configuración con el comando `systemctl reload named`).

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