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.

|  |  |
| --- | --- |
|  | **Para cada ejercicio**, se tienen que proporcionar los **comandos utilizados con sus correspondientes salidas**, las **capturas de pantalla de Wireshark** **realizadas**, y la **información requerida de manera específica**.  **Activar el portapapeles bidireccional en las máquinas** (menú Dispositivos) para copiar la salida de los comandos. Realizar capturas de pantalla con Virtualbox (menú Ver).  Las **credenciales de la máquina virtual** son: usuario cursoredes y contraseña cursoredes. |

**Contenidos**

[Cliente DNS](#_oaacscp23e1c)

[Servidor DNS](#_eofrh0ah6ijw)

[Preparación del entorno](#_14a3ftqman5y)

[Zona directa (*forward*)](#_w2ynjijgd1kw)

[Zona inversa (*reverse*)](#_sfcsed37y3uw)

# 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](http://www.digwebinterface.com) (activando las opciones “Stats” y “Show command”) o [www.diggui.com](http://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](http://informatica.ucm.es). Completar la siguiente tabla:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Servidor** | **Nombre** | **TTL** | **Tipo** | **Datos** |
| a.root-servers.net | es. | 172800 | NS | f.nic.es |
| f.nic.es | ucm.es. | 86400 | NS | ucdns.sis.ucm.es |
| ucdns.sis.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>. Consultar la página de manual de dig y la [estructura del registro](https://docs.google.com/presentation/d/17AnDsSj5O7iUKep-RMJfS2Yi9vEKd4xjPCzN2cTveqY/#slide=id.g1204fc089_01) y la [base de datos DNS](https://docs.google.com/presentation/d/17AnDsSj5O7iUKep-RMJfS2Yi9vEKd4xjPCzN2cTveqY/#slide=id.g16fd59ec7_030).



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

|  |
| --- |
| *Copiar el comando utilizado e indicar los campos relevantes del registro.*  dig SOA +additional +multiline ucm.es. @ucdns.sis.ucm.es. |

***Ejercicio 4****.* Determinar qué servidor de correo debería usarse para enviar un mail a [webmaster@fdi.ucm.es](mailto:webmaster@fdi.ucm.es), usar un servidor autoritativo de la zona.

|  |
| --- |
| *Copiar el comando utilizado e indicar el servidor de correo.*  $ dig MX +additional webmaster@fdi.ucm.es. @ucdns.sis.ucm.es.    El servidor aspmx.l.google.com. ya que tiene nivel de prioridad 1 |

***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 | r.arin.net. |
| r.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 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.*  *$ dig A +additional +trace www.google.com. @8.8.4.4* |

# 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 y no deben restringirse las consultas (directiva 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 |
| 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 | 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.*  [cursoredes@localhost ~]$ service named start  Redirecting to /bin/systemctl start named.service  ==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===  Authentication is required to manage system services or units.  Authenticating as: cursoredes  Password:  ==== AUTHENTICATION COMPLETE ===  [cursoredes@localhost ~]$ sudo cat db.labfdi.es  $TTL 2d  labfdi.es. IN SOA ns.labfdi.es. contact@labfdi.es. (  2003004 ; Serial  3h ; Refresh  14M ; Retry  2W10h ; Expire  2h30M ; Negative Cacha TTL  )  IN NS ns.labfdi.es.  ns.labfdi.es. IN A 192.168.0.1  www.labfdi.es. IN A 192.168.0.200  www.labfdi.es. IN AAAA fd00::1  IN MX 10 mail.labfdi.es.  mail.labfdi.es. IN A 192.168.0.250  correo.labfdi.es. IN CNAME mail.labfdi.es.  [cursoredes@localhost ~]$ named-checkzone labfdi.es. db.labfdi.es  zone labfdi.es/IN: loaded serial 2003004  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.*  [cursoredes@localhost ~]$ sudo cat /etc/resolv.conf  ; 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.

|  |
| --- |
| *Copiar el comando utilizado y su salida.*  [cursoredes@localhost ~]$ dig www.labfdi.es.  ; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7\_5.1 <<>> www.labfdi.es.  ;; global options: +cmd  ;; Got answer:  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29375  ;; 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:  ;www.labfdi.es. IN A  ;; ANSWER SECTION:  www.labfdi.es. 172800 IN A 192.168.0.200  ;; AUTHORITY SECTION:  labfdi.es. 172800 IN NS ns.labfdi.es.  ;; ADDITIONAL SECTION:  ns.labfdi.es. 172800 IN A 192.168.0.1  ;; Query time: 2 msec  ;; SERVER: 192.168.0.1#53(192.168.0.1)  ;; WHEN: Tue Oct 27 18:21:35 CET 2020  ;; MSG SIZE rcvd: 91 |

***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.*  (Client)[cursoredes@localhost ~]$ cat gedit db.0.168.192  cat: gedit: No such file or directory  $TTL 2  0.168.192.in-addr.arpa. IN SOA ns.labfdi.es. contact@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. |

***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.*  [cursoredes@localhost ~]$ dig -x 192.168.0.250  ; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7\_5.1 <<>> -x 192.168.0.250  ;; global options: +cmd  ;; Got answer:  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31779  ;; 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. 2 IN PTR mail.labfdi.es.  ;; AUTHORITY SECTION:  0.168.192.in-addr.arpa. 2 IN NS ns.labfdi.es.  ;; ADDITIONAL SECTION:  ns.labfdi.es. 172800 IN A 192.168.0.1  ;; Query time: 1 msec  ;; SERVER: 192.168.0.1#53(192.168.0.1)  ;; WHEN: Tue Oct 27 18:18:39 CET 2020  ;; MSG SIZE rcvd: 116 |