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](#_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 | a.nic.es.  IPV4 -> 194.69.254.1 |
| a.nic.es. | ucm.es. | 86400 | NS | crispin.sim.ucm.es.  IPV4-> 147.96.1.9 |
| 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>. 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.*  *[cursoredes@localhost ~]$* ***dig @crispin.sim.ucm.es. informatica.ucm.es. SOA***  *Registro SOA:*  *ucdns.sis.ucm.es. hostmaster.ucm.es. (*  *2022100701 ; serial*  *28800 ; refresh (8 hours)*  *7200 ; retry (2 hours)*  *1209600 ; expire (2 weeks)*  *86400 ; minimum (1 day)*  *)*  *ucdns.sis.ucm.es -> nombre de la zona*  *hostmaster.ucm.es -> email de contacto en notación (user.host)*  *2022100701 -> número de serie (versión del servidor)*  *28800 -> el servidor primario se refresca cada 28800s (8 horas)*  *7200 -> los fallos en zone transfer se vuelven a reintentar cada 2 horas*  *1209600 -> Si el servidor primario no responde en 2 semanas deja de responder como servidor autoritativo*  *86400 -> TTL de las respuestas negativas (expresado en segundos)* |
| --- |

***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.*  *[cursoredes@localhost ~]$* ***dig @crispin.sim.ucm.es. fdi.ucm.es. MX***  *; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7\_5.1 <<>> @crispin.sim.ucm.es. fdi.ucm.es. MX*  *; (1 server found)*  *;; global options: +cmd*  *;; Got answer:*  *;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45741*  *;; flags: qr aa rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1*  *;; OPT PSEUDOSECTION:*  *; EDNS: version: 0, flags:; udp: 4096*  *;; QUESTION SECTION:*  *;fdi.ucm.es. IN MX*  *;; ANSWER SECTION:*  ***fdi.ucm.es. 86400 IN MX 10 aspmx2.googlemail.com.***  ***fdi.ucm.es. 86400 IN MX 5 alt2.aspmx.l.google.com.***  ***fdi.ucm.es. 86400 IN MX 10 aspmx3.googlemail.com.***  ***fdi.ucm.es. 86400 IN MX 5 alt1.aspmx.l.google.com.***  ***fdi.ucm.es. 86400 IN MX 1 aspmx.l.google.com.***  *Puesto que la prioridad más alta se indica con el número más bajo se utilizará el servidor que posee prioridad 1, que en este caso es* ***aspmx.l.google.com.*** |
| --- |

***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 | u.arin.net. |
| u.arin.net. | 96.147.in-addr.arpa | 86400 | 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.*   * *En la consola:*   *[cursoredes@localhost ~]$* ***dig +trace www.google.com. A***  *; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7\_5.1 <<>> +trace www.google.com. A*  *;; global options: +cmd*  *. 166660 IN NS a.root-servers.net.*  *. 166660 IN NS m.root-servers.net.*  *. 166660 IN NS c.root-servers.net.*  *. 166660 IN NS j.root-servers.net.*  *. 166660 IN NS b.root-servers.net.*  *. 166660 IN NS d.root-servers.net.*  *. 166660 IN NS h.root-servers.net.*  *. 166660 IN NS l.root-servers.net.*  *. 166660 IN NS i.root-servers.net.*  *. 166660 IN NS g.root-servers.net.*  *. 166660 IN NS k.root-servers.net.*  *. 166660 IN NS f.root-servers.net.*  *. 166660 IN NS e.root-servers.net.*  *. 517971 IN RRSIG NS 8 0 518400 20221023050000 20221010040000 18733 . sWa6UdyCR+Qx6Fzgfy6EZM8dGzcs/j/XB5H+z9ff24tTDlvdJOfOzGQP aHcljLuwav1gvTx+CehRwwAQEHi4Ksj5wYQwx3PtAiJhCMZTYnYiZ1MW NpnzOX2emj+f7RgK8d8jpqDaYfMwCAKK4i7RLahtzx1BhCCjVdNUyowV wKErU7F4SOw7k0D3HC4ojVYF7aJcbSN7qS0zpa4KcXz1igAXSTmAIQ5T i7sbKubSOVKzIWQ1Pp+bKgY+HoiesaU23PnTPPuT9cWGwDypGXh45NSQ zPg+Sl6lJTaj7FQaqXFT+o65iux7NvO3DpJrm4Gn7pk5e3uAVqH3/8wm UYM5Ow==*  *;; Received 525 bytes from 147.96.1.9#53(147.96.1.9) in 10655 ms*  *;; connection timed out; no servers could be reached*   * *En la interfaz web:*   *. 84315 IN NS i.root-servers.net.*  *. 84315 IN NS h.root-servers.net.*  *. 84315 IN NS e.root-servers.net.*  *. 84315 IN NS d.root-servers.net.*  *. 84315 IN NS b.root-servers.net.*  *. 84315 IN NS l.root-servers.net.*  *. 84315 IN NS f.root-servers.net.*  *. 84315 IN NS c.root-servers.net.*  *. 84315 IN NS a.root-servers.net.*  *. 84315 IN NS g.root-servers.net.*  *. 84315 IN NS k.root-servers.net.*  *. 84315 IN NS j.root-servers.net.*  *. 84315 IN NS m.root-servers.net.*  *;; Received 228 bytes from 8.8.4.4#53(8.8.4.4) in 86 ms*  *com. 172800 IN NS a.gtld-servers.net.*  *com. 172800 IN NS b.gtld-servers.net.*  *com. 172800 IN NS c.gtld-servers.net.*  *com. 172800 IN NS d.gtld-servers.net.*  *com. 172800 IN NS e.gtld-servers.net.*  *com. 172800 IN NS f.gtld-servers.net.*  *com. 172800 IN NS g.gtld-servers.net.*  *com. 172800 IN NS h.gtld-servers.net.*  *com. 172800 IN NS i.gtld-servers.net.*  *com. 172800 IN NS j.gtld-servers.net.*  *com. 172800 IN NS k.gtld-servers.net.*  *com. 172800 IN NS l.gtld-servers.net.*  *com. 172800 IN NS m.gtld-servers.net.*  *;; Received 508 bytes from 199.9.14.201#53(199.9.14.201) in 84 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 192.43.172.30#53(192.43.172.30) in 101 ms*  *www.google.com. 300 IN A 172.217.2.36*  *;; Received 48 bytes from 216.239.32.10#53(216.239.32.10) in 25 ms*  *Podemos observar que www.google .es. Tiene dirección IPV4 172.217.4.68* |
| --- |

# 

# 

# 

# 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; };  zone "labfdi.es." {  type master;  file "db.labfdi.es";  };  recursion no;  El comando named-checkconf no devuelve respuesta |
| --- |

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 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. (*  *2022101011;serial number*  *28800 ;refresh*  *7200 ;update retry*  *1209600 ;expiry*  *86400 ;nx ttl*  *)*  *IN NS ns*  *IN MX 1 mail;*  *correo IN CNAME mail*  *ns IN A 192.168.0.1*  *www IN A 192.168.0.200*  *mail IN A 192.168.0.250*  *www IN AAAA fd00::1*  *[root@localhost named]#* ***named-checkzone labfdi.es. db.labfdi.es***  *zone labfdi.es/IN: loaded serial 2022101011*  *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.

| *Copiar los comandos utilizados y sus salidas.*  *[root@localhost etc]#* ***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: 39082*  *;; 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. 8100 IN SOA ns.labfdi.es. contact.labfdi.es. 2022101011 7200 1200 648000 8100*  *;; Query time: 1 msec*  *;; SERVER: 192.168.0.1#53(192.168.0.1)*  *;; WHEN: Mon Oct 10 12:35:32 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.*    *El servidor se encuentra establecido en el puerto 53 a diferencia del cliente que es distinto en cada consulta y las tramas de ida son más pequeñas que las de vuelta.*  *Recursion avaliable está desactivado en los mensajes de vuelta a diferencia del AA de dominio autoritativo.*  *Las respuestas RR de tipo NS incluyen un RR de tipo A con la IP* |
| --- |

## 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.

| *Se nos pide añadir al archivo:*  *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 (*  *2022101011;serial number*  *28800 ;refresh*  *7200 ;update retry*  *1209600 ;expiry*  *86400 ;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* |
| --- |

***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.*  *[root@localhost etc]#* ***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: 46848*  *;; flags: qr 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: Tue Oct 11 12:47:39 CEST 2022*  *;; MSG SIZE rcvd: 55* |
| --- |