Redes de Computadoras
–
Prácticas

Juana López Redondo
María Laura Da Silva Hernández
Vicente González Ruiz
2 de junio de 2011

El servicio DNS

El DNS es una de las aplicaciones fundamentales de Internet, con una función primordial: la de traducir los nombres de los hosts a direcciones IP. El servicio de nombres de dominio es una gigantesca base de datos distribuida a nivel mundial que funciona sin pausa, está constantemente actualizándose y resuelve las consultas en tiempo real (¿qué más se puede pedir?).

El DNS se basa en la arquitectura cliente-servidor. En su consulta más frecuente, los clientes piden resoluciones de nombres de dominio y los servidores las contestan indicando sus direcciones IP. La comunicación entre ambos se realiza a través del UDP.

En esta sesión práctica vamos a aprender a instalar un servidor DNS y a hacer uso del mismo. Esto genera varias ventajas. La primera y la más interesante es que las consultas son resueltas utilizando un nodo local (en nuestra sub-red), con lo que el tiempo de acceso se minimiza cuando este nodo almacena en su caché una resolución previa. La segunda es que descargamos de trabajo al resto de servidores de la jerarquía, cosa que algunos administradores nos agradecerán. También aprenderemos a realizar consultas de diversa índole con el objetivo de aprender qué posibilidades ofrece el sistema DNS.

8.1. Los nombres de dominio

Un dominio es, básicamente hablando, una organización cualquiera dentro de Internet que desea ser referenciada mediante un *nombre de dominio*. Por ejemplo, la Universidad de Almería es una organización que posee una serie de computadoras llamadas de la forma "*.ual.es". "ual.es" es el nombre del dominio de la Universidad de Almería. En la práctica para mucha gente es demasiado largo decir "nombre de dominio" y generalmente se dice simplemente "dominio".

8.2. Dominios y subdominios

Es frecuente que un nombre de dominio conste de varios subdominios, normalmente separados por un punto. Por ejemplo, el dominio "ual.es" es en realidad un

subdominio del dominio "es".

Este hecho genera una **jerarquía de dominios** en la que cualquier nodo público de Internet puede ser localizado. Por ejemplo, el nodo filabres.ual.es es un host de la Universidad de Almería, que se trata de una universidad española.

8.3. La jerarquía de dominios

En cada dominio normalmente se instala un **servidor de nombres de dominio**, también llamado servidor DNS. Dicho servidor se encarga de mantener la base de datos de registros DNS para ese dominio. Por ejemplo, en la Universidad de Almería hay un servidor DNS que conoce todas las resoluciones de las direcciones IP para todos los hosts con nombres de la Universidad. En concreto, filabres.ual.es (150.214.156.2) es un servidor DNS del dominio ual.es. Otra forma de decir esto consiste en llamar a filabres.ual.es el servidor de nombres autorizado para el dominio ual.es.

8.4. El proceso de resolución

Normalmente, cuando un servidor DNS no conoce una resolución utiliza otro servidor DNS situado en un nivel superior en la jerarquía de dominios para intentar resolverla (o al menos, así debería ser). Esta política de **consultas recursivas** finalmente encuentra un servidor DNS que sí conoce la resolución. Entonces el registro DNS solicitado viaja desde dicho servidor DNS deshaciendo el camino hasta el servidor DNS al que inicialmente realizamos la consulta. En este proceso, cada servidor DNS actualiza su caché con esta información por un determinado periodo de tiempo.

Por ejemplo, cuando queremos acceder a www.nasa.gov desde un host de la Universidad de Almería, dicho host debería preguntar a filabres.ual.es[1]. Si filabres no almacena en su caché la resolución[2], podría[3] preguntar al siguiente servidor DNS en la jerarquía que podría ser un nodo del CICA (Centro Informático Científico de Andalucía). Si éste fallara, preguntaría a un servidor de RedIRIS (la red académica y de investigación nacional), y así sucesivamente hasta llegar a un servidor DNS raíz[4]. Si éste falla, entonces la consulta comienza a descender por la jerarquía de servidores DNS hasta llegar al responsable del dominio nasa.gov que necesariamente debe conocer la resolución.

Existe una versión diferente de este algoritmo recursivo que se realiza una **consulta iterativa**. La diferencia radica en que cuando un servidor DNS falla en lugar de hacer él la consulta le indica al cliente a qué otro servidor DNS puede preguntar. Este proceso, sin embargo, no actualiza las cachés de los servidores.

---

[1] En realidad puede consultar a qualquier otro que se deje consultar, pero lo más lógico es usar filabres porque es el servidor DNS más cercano.

[2] No olvidemos que filabres no es el servidor de nombres autorizado para el dominio nasa.gov. Bueno, en realidad, habría que decir que en filabres no corre el servidor DNS que es el autorizado para este dominio.

[3] Esto en realidad depende de cómo se ha configurado el servidor DNS en filabres.

[4] Los servidores de nombres raíz no están configurados para ser servidores de nombres autorizados para ningún dominio (excepto el domonio nulo, aquél que va destrás del top level domain).

8.5. Instalación de un servidor DNS

Para convertir un host con Linux en un servidor DNS basta con instalar el programa BIND (Berkeley Internet Name Domain) (http://www.isc.org/products/BIND):

Debian's distros:

```
root# apt-get install bind9 bind9-doc dnsutils
```

Red Hat's distros:

```
root# yum install bind bind-utils caching-nameserver system-config-bind
```

Gentoo's distros:

```
root# emerge bind bind-utils
```

8.6. Configuración del servidor DNS

El servidor puede configurarse para ofrecer servicio de tres formas diferentes:

1. **Como servidor de nombres autorizado del dominio X:** Si almacena los registros de resolución para los hosts del dominio X.
2. **Como servidor de nombres réplica:** Si mantiene una copia de los registros de otro servidor DNS.
3. **Como servidor sólo caché:** Cuando no almacena ningún registro, excepto los adquiridos en las consultas.

La primera configuración es la que utilizaría el administrador de una nueva red que desea que sus hosts tengan nombres de dominio asignados. En dicha configuración se generarían los registros de resolución para cada uno de estos hosts y se almacenarían en el servidor de nombres autorizado. Además, el servidor DNS del ISP debería tener en cuenta el servidor DNS instalado[5]. Por desgracia, esto último es imposible llevarlo a la práctica si no se adquiere legalmente un dominio y negociamos la delegación del dominio con el correspondiente ISP.

Aunque parezca que esta forma de configurar el DNS es demasiado burocrácica, en realidad hay razones de peso para hacerse así. Si este tema no estuviera suficientemente controlado, un usuario malicioso puede inventarse un dominio con el objetivo de introducir "ruido" en el DNS con la idea de desviar conexiones hacia un conjunto determinados de servidores (probablemente controlados por dicho usuario malicioso). Por estos motivos, en esta ocasión no vamos a instalar un servidor DNS autorizado. Sin

[5] Ya que ha dejado de ser el servidor de nombres autorizado para el dominio que sirve el servidor de nombres que estaríamos instalando.

embargo, bastaría con modificar el fichero de configuración correspondiente y construir los registros DNS utilizando alguna herramienta como system-config-bind de Red Hat Linux. La parte de la delegación del dominio es otro tema que ya no depende sólo de nosotros.

La segunda configuración sirve para aumentar la fiabilidad del DNS ya que permite replicar los registros de resolución. Así, si el servidor de nombres autorizado fallase, el otro pasaría a resolver las consultas. Por ejemplo, en la Universidad de Almería hay un servidor DNS autorizado para el dominio ual.es (filabres.ual.es, 150.214.156.2) y otro réplica (alboran.ual.es, 150.214.156.32). Instalar un servidor DNS réplica plantea los mismos problemas de seguridad que instalar uno autorizado y además, una replicación sin control constituye un buen ataque por denegación de servicio. Por estos motivos, desistiremos también de realizar dicha opción.

Finalmente, la tercera y última configuración, en la que instalamos un servidor DNS que funciona en realidad como un proxy DNS, sí que es posible en cualquier situación y tiene sentido si queremos reducir el tráfico a través del gateway de la red, descargar de trabajo a otros servidores DNS y minimizar el tiempo de resolución para las máquinas a las que servimos. Por suerte, esta configuración es la que por defecto se instala con BIND.

8.6.1. Configuración como servidor caché

Como hemos indicado anteriormente, en principio no es necesario hacer ninguna modificación en el fichero named.conf para conseguir que el servidor DNS funcione como un proxy DNS. Sin embargo, sí que vamos a hacer un pequeño cambio para que BIND utilice los servidores DNS más próximos cuando la caché falle.[6] Para hacer esto hay que modificar el fichero named.conf insertando el código:

```
forward first;
forwarders {
  150.214.156.2;
  150.214.156.32;
};
```

en su sección options. Veamos exactamente qué hacer en cada distribución:

Debian's: La instalación de bind crea el fichero /etc/bind/named.conf y otros dos ficheros asociados /etc/bind/named.conf.local y /etc/bind/named.conf.options. El código anterior debe insertarse en este último fichero.

Red Hat's: El fichero que configura el servidor es /etc/named.conf. Para configurarlo como un servidor DNS cache ejecutar:

```
root# system-config-bind # Salir sin hacer ninguna modificaci'on
```

[6] De lo contrario las resoluciones funcionan porque se consultan directamente a los servidores de nombres raíz con el consiguiente aumento de la latencia.

A continuación insertar el código anterior en el fichero.

Gentoo's: La instalación de BIND crea el fichero `/etc/bind/named.conf` para que funcione como un DNS caché. Simplemente insertaremos el código anterior en este fichero.

Finalmente hay que modificar el fichero `/etc/resolv.conf` indicando que ahora es `localhost` el servidor DNS. Si tuviéramos más hosts en nuestra red local, dicha modificación debería realizarse en todos ellos.

8.6.2. Configuración como servidor del dominio X

Aunque realmente no tendría sentido crear un determinado dominio si no se le indica al resto de servidores DNS que el servidor que vamos a configurar es el responsable de ese dominio, en esta sección vamos a ver qué pasos habría que realizar para llevarla a cabo.

Como ya sabemos, el fichero `named.conf` es leído por Bind cada vez que éste arranca. Dicho fichero, por defecto, debería incluir la carga del fichero `named.conf.local`. En este fichero se definen las *zonas* (dominios) locales creadas y mantenidas por el servidor de nombres que estamos configurando. En nuestro caso, supongamos que estamos declarando el dominio `dominio.X`. Así, `named.conf.local` debería tener el siguiente contenido:

```
zone "dominio.X" {
    type master;
    file "/etc/bind/db.dominio.X";
};
```

donde `/etc/bind/db.dominio.X` contiene, a modo de ejemplo:

```
;$TTL 604800
$TTL 9
@ IN SOA dominio.X. hostmaster.dominio.X. (
  2007110701  ; Serial yyyy/mm/dd/id
        10800  ; Refresh (3 hours)
         7200  ; Retry (2 hours)
      1296000  ; Expire (15 days)
       172800 ); Negative Cache TTL (2 days)
;
@ IN NS     ns0.dominio.X.
@ IN NS     ns1.dominio.X.
@ IN MX 10 mail.dominio.X.
@ IN TXT "Servidor"
@ IN HINFO "Servidor privado" "LAN interna"
;
@ IN A 101.102.103.103
* IN A 101.102.103.104
```

Este último fichero define los parámetros fundamentales del registro de resolución para el cual nuestro servidor de nombres es el autorizado. De arriba a abajo se declaran cosas como:

TTL 9 : Número máximo de saltos a realizar en una consulta DNS.

2007110701 : El instante de creación del dominio dominio.X (año, mes, día e identificador).

10800 : El tiempo de frescura (medido en segundos) del registro en un servidor de nombres caché. 3 horas.

7200 : Ante una falta del registro, un servidor de nombres no debería reclamarlo a otro servidor no antes de 2 horas.

1296000 : Los servidores de nombres borrarán este registro de sus cachés a los 15 días.

NS : Name Server.

MX : Mail eXchanger.

101.102.103.103 : Dirección IP del host que corre nuestro servidor de nombres.

8.7. Configuración del cliente

La única opción de configuración que permiten los clientes es la especificación del (o los) servidor(es) DNS. En Linux esta información está declarada en el fichero:

/etc/resolv.conf

quen es texto (ASCII) y puede ser editado como administrador.

8.8. Ejemplos de consultas

8.8.1. ¿Cuáles son mis servidores DNS?

A la hora de determinar el servidor DNS que estamos utilizando existen dos alternativas:

1. Acceder a esta información en los ficheros de configuración correspondientes. Por ejemplo, en Linux hay que leer el fichero

   /etc/resolv.conf

   Evidentemente, esta opción sólo funciona bajo Linux.

   En este fichero aparecen al menos la IP de un servidor DNS. Al primero de ellos se le llama servidor DNS primario y debería ser un servidor DNS próximo, por motivos de eficiencia. El resto de direcciones IP son los llamados servidores secundarios porque, en el caso de fallar el primerio, se haría uso de estos.

2. Utilizar programas para chequear el funcionamiento del DNS como pueden ser nslookup y dig. nslookup funciona tanto desde la línea de comandos como de forma interactiva. dig sólo lo hace desde la línea de comandos. Indicar además que el resultado de la consulta no depende del host, ni de que éste pertenezca al dominio por el que estamos preguntando. El resultado sólo depende del dominio por el que preguntamos. Veamos algunos ejemplos:

```
# Preguntamos a nuestro servidor DNS primario
#  el dominio "ual.es"
alumno$ dig ual.es

; <<>> DiG 9.2.4 <<>> ual.es
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65305
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;ual.es.                                IN      A

;; AUTHORITY SECTION:
ual.es.                 172800  IN      SOA     filabres.ual.es.\
postmaster.filabres.ual.es. 2006111502 16400 7200 2592000 172800

;; Query time: 0 msec
;; SERVER: 150.214.156.2#53(150.214.156.2)
;; WHEN: Thu Nov 30 10:26:33 2006
;; MSG SIZE  rcvd: 80
```

En esta consulta, entre mucha otra información dig indica que el servior DNS autorizado para el dominio ual.es es filabres.ual.es.

Ejercicio 9: Averigue el (o los) servidor(es) de nombres autorizado(s) para el dominio google.es.

8.8.2. ¿Cuál es la dirección IP del host ...?

En la siguiente consulta preguntamos a nuestro servidores DNS primario (o en su defecto, secundario) por la dirección IP del host www.google.es:

```
# Preguntamos a nuestro servidor DNS por la IP de "www.google.es"
alumno$ dig www.google.es

; <<>> DiG 9.2.4 <<>> www.google.es
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46300
```

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 6, ADDITIONAL: 6

;; QUESTION SECTION:
;www.google.es.                  IN      A

;; ANSWER SECTION:
www.google.es.          167616  IN      CNAME   www.google.com.
www.google.com.         425476  IN      CNAME   www.l.google.com.
www.l.google.com.       201     IN      A       209.85.129.104
www.l.google.com.       201     IN      A       209.85.129.99
www.l.google.com.       201     IN      A       209.85.129.147

;; AUTHORITY SECTION:
l.google.com.           81028   IN      NS      a.l.google.com.
l.google.com.           81028   IN      NS      b.l.google.com.
l.google.com.           81028   IN      NS      c.l.google.com.
l.google.com.           81028   IN      NS      d.l.google.com.
l.google.com.           81028   IN      NS      e.l.google.com.
l.google.com.           81028   IN      NS      g.l.google.com.

;; ADDITIONAL SECTION:
a.l.google.com.         23928   IN      A       216.239.53.9
b.l.google.com.         23928   IN      A       64.233.179.9
c.l.google.com.         14956   IN      A       64.233.161.9
d.l.google.com.         81028   IN      A       64.233.183.9
e.l.google.com.         14956   IN      A       66.102.11.9
g.l.google.com.         21711   IN      A       64.233.167.9

;; Query time: 12 msec
;; SERVER: 150.214.156.2#53(150.214.156.2)
;; WHEN: Thu Dec 21 10:39:27 2006
;; MSG SIZE  rcvd: 319
```

Esta respuesta es un poco complicada por dos motivos: (1) www.google.es y www.google.com son la misma máquina cuando hacemos la consulta a nuestro servidor de nombres y (2), el servidor Web está replicado tres veces en las direcciones IP 209.85.129.104, 209.85.129.147 y 209.85.129.99. Esto puede comprobarse si preguntamos por www.google.com:

```
# Preguntamos a nuestro servidor DNS por la IP de "www.google.com"
alumno$ dig www.google.com

; <<>> DiG 9.2.4 <<>> www.google.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20533
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 6, ADDITIONAL: 6
```

```
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         420014  IN      CNAME   www.l.google.com.
www.l.google.com.       207     IN      A       209.85.129.104
www.l.google.com.       207     IN      A       209.85.129.99
www.l.google.com.       207     IN      A       209.85.129.147

;; AUTHORITY SECTION:
l.google.com.           75566   IN      NS      a.l.google.com.
l.google.com.           75566   IN      NS      b.l.google.com.
l.google.com.           75566   IN      NS      c.l.google.com.
l.google.com.           75566   IN      NS      d.l.google.com.
l.google.com.           75566   IN      NS      e.l.google.com.
l.google.com.           75566   IN      NS      g.l.google.com.

;; ADDITIONAL SECTION:
a.l.google.com.         18466   IN      A       216.239.53.9
b.l.google.com.         18466   IN      A       64.233.179.9
c.l.google.com.         9494    IN      A       64.233.161.9
d.l.google.com.         75566   IN      A       64.233.183.9
e.l.google.com.         9494    IN      A       66.102.11.9
g.l.google.com.         16249   IN      A       64.233.167.9

;; Query time: 1 msec
;; SERVER: 150.214.156.2#53(150.214.156.2)
;; WHEN: Thu Dec 21 12:10:30 2006
;; MSG SIZE  rcvd: 292
```

Además, como puede verse www.google.com es un alias de www.l.google.com.

8.8.3. ¿Cuáles son los servidores de nombres del dominio ...?

```
# Preguntamos por el dominio "mit.edu"
alumno$ dig mit.edu
; <<>> DiG 9.2.4 <<>> mit.edu
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10644
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;mit.edu.                       IN      A
```

```
;; ANSWER SECTION:
mit.edu.                60      IN      A       18.7.22.69

;; AUTHORITY SECTION:
mit.edu.                14655   IN      NS      BITSY.mit.edu.
mit.edu.                14655   IN      NS      STRAWB.mit.edu.
mit.edu.                14655   IN      NS      W20NS.mit.edu.

;; ADDITIONAL SECTION:
BITSY.mit.edu.          14655   IN      A       18.72.0.3
STRAWB.mit.edu.         8735    IN      A       18.71.0.151
W20NS.mit.edu.          8735    IN      A       18.70.0.160

;; Query time: 158 msec
;; SERVER: 150.214.156.2#53(150.214.156.2)
;; WHEN: Thu Dec 21 12:20:46 2006
;; MSG SIZE  rcvd: 157
```

Podemos ver que existen tres servidores de nombres autorizados para el dominio "bit.edu".

> **Ejercicio 10:** Encuentre los servidores nombres autorizados de un dominio que conozca. ¿A qué servidor de nombres ha consultado?

8.8.4. ¿Cómo interrogamos a otro servidor DNS?

```
# Preguntamos al servidor DNS "bitsy.mit.edu" por el host "www.google.es"
alumno$ dig @bitsy.mit.edu www.google.es

; <<>> DiG 9.2.4 <<>> @bitsy.mit.edu www.google.es
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7735
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 7, ADDITIONAL: 7

;; QUESTION SECTION:
;www.google.es.                 IN      A

;; ANSWER SECTION:
www.google.es.          304614  IN      CNAME   www.google.com.
www.google.com.         557306  IN      CNAME   www.l.google.com.
www.l.google.com.       174     IN      A       64.233.161.104
www.l.google.com.       174     IN      A       64.233.161.99
www.l.google.com.       174     IN      A       64.233.161.147
```

```
;; AUTHORITY SECTION:
l.google.com.           72376   IN      NS      c.l.google.com.
l.google.com.           72376   IN      NS      f.l.google.com.
l.google.com.           72376   IN      NS      d.l.google.com.
l.google.com.           72376   IN      NS      b.l.google.com.
l.google.com.           72376   IN      NS      e.l.google.com.
l.google.com.           72376   IN      NS      g.l.google.com.
l.google.com.           72376   IN      NS      a.l.google.com.

;; ADDITIONAL SECTION:
c.l.google.com.         40415   IN      A       64.233.161.9
f.l.google.com.         72376   IN      A       72.14.235.9
d.l.google.com.         38903   IN      A       64.233.183.9
b.l.google.com.         38903   IN      A       64.233.179.9
e.l.google.com.         38903   IN      A       66.102.11.9
g.l.google.com.         44316   IN      A       64.233.167.9
a.l.google.com.         39459   IN      A       216.239.53.9

;; Query time: 231 msec
;; SERVER: 18.72.0.3#53(bitsy.mit.edu)
;; WHEN: Thu Dec 21 12:15:01 2006
;; MSG SIZE  rcvd: 351
```

Ahora preguntamos al servidor DNS "bitsy.mit.edu" por el host "www.google.com":

```
# Preguntamos al servidor DNS "bitsy.mit.edu" por el host "www.google.com"
alumno$ dig @bitsy.mit.edu www.google.com

; <<>> DiG 9.2.4 <<>> @bitsy.mit.edu www.google.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29537
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 7, ADDITIONAL: 7

;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         557281  IN      CNAME   www.l.google.com.
www.l.google.com.       149     IN      A       64.233.161.99
www.l.google.com.       149     IN      A       64.233.161.147
www.l.google.com.       149     IN      A       64.233.161.104

;; AUTHORITY SECTION:
```

```
l.google.com.          72351   IN      NS      c.l.google.com.
l.google.com.          72351   IN      NS      f.l.google.com.
l.google.com.          72351   IN      NS      d.l.google.com.
l.google.com.          72351   IN      NS      b.l.google.com.
l.google.com.          72351   IN      NS      e.l.google.com.
l.google.com.          72351   IN      NS      g.l.google.com.
l.google.com.          72351   IN      NS      a.l.google.com.

;; ADDITIONAL SECTION:
c.l.google.com.        40390   IN      A       64.233.161.9
f.l.google.com.        72351   IN      A       72.14.235.9
d.l.google.com.        38878   IN      A       64.233.183.9
b.l.google.com.        38878   IN      A       64.233.179.9
e.l.google.com.        38878   IN      A       66.102.11.9
g.l.google.com.        44291   IN      A       64.233.167.9
a.l.google.com.        39434   IN      A       216.239.53.9

;; Query time: 156 msec
;; SERVER: 18.72.0.3#53(bitsy.mit.edu)
;; WHEN: Thu Dec 21 12:15:25 2006
;; MSG SIZE  rcvd: 324
```

Como podemos ver, ambas respuestas son idénticas (como en el caso de preguntar a filabres), pero diferentes comparadas con las que devuelve nuestro servidor de nombres. Esto significa que, si nos conectamos a www.google.es desde el MIT, veremos la versión americana de google.

Finalmente, nótese que el servidor DNS no devuelve las direcciones IP de las réplicas del servidor Web siempre en el mismo orden. Esto se utiliza para distribuir la carga.

> **Ejercicio 11:** Encuentre los servidores nombres autorizados para el dominio "ual.es" interrogando al servidor DNS "bitsy.mit.edu" (o a otro que conozca). En esta consuta, ¿está usando el servidor DNS especificado en "/etc/resolv.conf"?

8.8.5. Averiguando la jerarquía de servidores DNS

Como hemos comentado anteriormente, cuando consultamos a un servidor DNS sobre una dirección para la cual él no es el servidor DNS autorizado lo más frecuente es que éste tenga que consultar a otro servidor DNS (consulta recursiva) o nos indique a qué otro servidor DNS podemos preguntar nosotros (consulta iterativa).

Activando el flag +trace de dig podemos conocer qué servidores DNS se han consultado. En el siguiente ejemplo preguntamos a bitsy.mit.edu por la dirección IP del host gogh.ace.ual.es:

```
alumno$ dig +trace @bitsy.mit.edu gogh.ace.ual.es
```

```
; <<>> DiG 9.2.4 <<>> +trace @bitsy.mit.edu gogh.ace.ual.es
;; global options:  printcmd
.                       488373  IN      NS      a.root-servers.net.
.                       488373  IN      NS      h.root-servers.net.
.                       488373  IN      NS      c.root-servers.net.
.                       488373  IN      NS      g.root-servers.net.
.                       488373  IN      NS      f.root-servers.net.
.                       488373  IN      NS      b.root-servers.net.
.                       488373  IN      NS      j.root-servers.net.
.                       488373  IN      NS      k.root-servers.net.
.                       488373  IN      NS      l.root-servers.net.
.                       488373  IN      NS      m.root-servers.net.
.                       488373  IN      NS      i.root-servers.net.
.                       488373  IN      NS      e.root-servers.net.
.                       488373  IN      NS      d.root-servers.net.
;; Received 436 bytes from 18.72.0.3#53(bitsy.mit.edu) in 158 ms

es.                     172800  IN      NS      NS3.NIC.FR.
es.                     172800  IN      NS      SUN.REDIRIS.es.
es.                     172800  IN      NS      SUNIC.SUNET.SE.
es.                     172800  IN      NS      NS.UU.NET.
es.                     172800  IN      NS      NS1.NIC.es.
es.                     172800  IN      NS      AUNIC.AUNIC.NET.
es.                     172800  IN      NS      NS1.CESCA.es.
es.                     172800  IN      NS      NS2.NIC.es.
;; Received 352 bytes from 198.41.0.4#53(a.root-servers.net) in 134 ms

ual.es.                 7200    IN      NS      chico.rediris.es.
ual.es.                 7200    IN      NS      alboran.ual.es.
ual.es.                 7200    IN      NS      filabres.ual.es.
ual.es.                 7200    IN      NS      sun.rediris.es.
ual.es.                 7200    IN      NS      dns1.cica.es.
ual.es.                 7200    IN      NS      dns2.cica.es.
;; Received 263 bytes from 192.134.0.49#53(NS3.NIC.FR) in 49 ms

ace.ual.es.             172800  IN      NS      filabres.ual.es.
ace.ual.es.             172800  IN      NS      alboran.ual.es.
;; Received 110 bytes from 130.206.1.3#53(chico.rediris.es) in 37 ms

gogh.ace.ual.es.        172800  IN      A       193.147.118.57
ace.ual.es.             172800  IN      NS      filabres.ual.es.
ace.ual.es.             172800  IN      NS      alboran.ual.es.
;; Received 126 bytes from 150.214.156.2#53(filabres.ual.es) in 0 ms
```

Como podemos ver, `bitsy.mit.edu` consulta (en la versión recursiva) al servi-

dor de nombres raíz a.root-servers.net, que consulta a NS3.NIC.FR, que consulta a chico.rediris.es, que consulta a filabres.ual.es.

> **Ejercicio 12:** Determine qué servidor(es) DNS de nivel más bajo tienen en común los servidores DNS de la Universidad de Almería y los de la Universidad de Córdoba.

8.8.6. Resolución inversa

Finalmente, también podemos interrogar al servidor DNS por el nombre de un host a partir de su direccion IP:

```
# Preguntamos al servidor DNS por el nombre del host que tiene la IP
# 193.147.118.57
alumno$ dig -x 193.147.118.57

; <<>> DiG 9.2.4 <<>> -x 193.147.118.57
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44233
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 6, ADDITIONAL: 7

;; QUESTION SECTION:
;57.118.147.193.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
57.118.147.193.in-addr.arpa. 172800 IN    PTR     gogh.ace.ual.es.

;; AUTHORITY SECTION:
118.147.193.in-addr.arpa. 172800 IN     NS      filabres.ual.es.
118.147.193.in-addr.arpa. 172800 IN     NS      alboran.ual.es.
118.147.193.in-addr.arpa. 172800 IN     NS      dns1.cica.es.
118.147.193.in-addr.arpa. 172800 IN     NS      dns2.cica.es.
118.147.193.in-addr.arpa. 172800 IN     NS      sun.rediris.es.
118.147.193.in-addr.arpa. 172800 IN     NS      chico.rediris.es.

;; ADDITIONAL SECTION:
filabres.ual.es.        172800  IN      A       150.214.156.2
alboran.ual.es.         172800  IN      A       150.214.156.32
dns1.cica.es.           163357  IN      A       150.214.5.83
dns2.cica.es.           3265    IN      A       150.214.4.35
sun.rediris.es.         15046   IN      A       130.206.1.2
chico.rediris.es.       15295   IN      A       130.206.1.3
dns2.cica.es.           127925  IN      AAAA    2001:720:c10:9::4

;; Query time: 1 msec
```

```
;; SERVER: 150.214.156.2#53(150.214.156.2)
;; WHEN: Thu Dec 21 13:19:57 2006
;; MSG SIZE rcvd: 332
```

Como podemos ver, el host es gogh.ace.ual.es.

8.9. Servidores DNS en la Web

Existen servidores Web que prestan servicio DNS. Ejemplos:

http://remote.12dt.com/
http://www.zoneedit.com/lookup.html

Utilice algunas de estas páginas Web para comprobar que el resultado coincide con el que devuelve dig para una determinada consulta.

8.10. ¡Cuidado con el DNS!

El DNS es uno de los servicios más críticos que existen en Internet. A continuación mostramos algunos de los riesgos más importantes a los que nos exponemos cuando utilizamos un servidor DNS inseguro (más información en BULMA (http://bulma.net/body.phtml?nIdNoticia=1334)).

1. Si definimos un dominio e instalamos un servidor DNS autorizado para el mismo, estamos obligados a ofrecer información sobre el dominio definido. Esto significa que cualquier usuario de Internet puede conocer qué máquinas y con qué direcciones IP existen en nuestro dominio.

2. Los servidores DNS que delegan dominios a otros servidores (es decir, que ya no son servidores autorizados para ese sub-dominio) están obligados a escuchar las modificaciones que en dichos dominios se producen (en caso contrario, el DNS no escalaría). Si no tenemos cuidado cuando configuramos nuestro servidor y no controlamos adecuadamente "la transferencia de dominio", un hacker puede instalar un servidor DNS y hacerlo pasar por el servidor DNS autorizado de ese dominio. Si esto ocurre, puede inyectar información falsa en el sistema DNS y hacer que cuando accedamos a un host en realidad entremos en otro. Imagine lo que sería acceder a nuestra cuenta bancaria a través del host del hacker, creyendo que estamos enviando los datos al servidor de nuestro banco cuando en realidad lo estamos haciendo a un host que controla el hacker.

8.11. DNS + DHCP

Cuando utilizamos el DHCP para gestionar redes públicas en las que las direcciones IP asignadas son dinámicas, podemos configurar el servidor DHCP para que avise al servidor DNS autorizado de ese dominio de los cambios que se vayan produciendo en las asignaciones de las direcciones.

Este sistema tiene una gran ventaja: se gestiona sólo. Sin embargo, no es muy recomendable su uso cuando vamos a instalar servicios importantes en los hosts del dominio. Supongamos que en uno de estos host tenemos un servidor Web que tiene miles de accesos diarios. En esta situación la dirección IP de este host está diseminada por las cachés de miles de servidores DNS de toda la Internet. Si dicho host recibe una nueva IP, muchas resoluciones serían incorrectas hasta que las cachés son actualizadas.

8.11 DNS + DHCP