Servidor de nombres DNS. DNSmasq

Alberto Molina Coballes <alberto.molina@hispalinux.es>
José Domingo Muñoz Rodríguez <josedom24@gmail.com>
IES Gonzalo Nazareno. Dos Hermanas (Sevilla)

24 de septiembre de 2006

Resumen

En este documento se describe la instalación y configuración del proxy-dns dnsmasq, para acelerar la resolución de nombres en una red local que accede a Internet. Esta documentación se elaboró para el curso *Máquinas virtuales para la puesta en marcha de un portal educativo* organizado por el CEP de Sevilla en Septiembre de 2006.

1. Introducción

Llegó la hora de las direcciones simbólicas. Las direcciones IP han campado a sus anchas y la verdad es que para nosotros son difíciles de recordar y propensas a errores. Donde esté un nombre simple y descriptivo como `thales.cica.es`, que se quiten todas las direcciones IP como su equivalente 172.26.0.2 ¿o quizás era 150.214.22.12? ¡Ah! no, es 150.214.5.10. Véis, nuestra capacidad simbólica es superior a nuestra capacidad de recordar números.

El sistema DNS es una base de datos distribuida. Presenta una jerarquía en la que su parte más alta es el "punto" o raíz y de él cuelgan los dominios de primer nivel (.com, .edu, .es, etc).

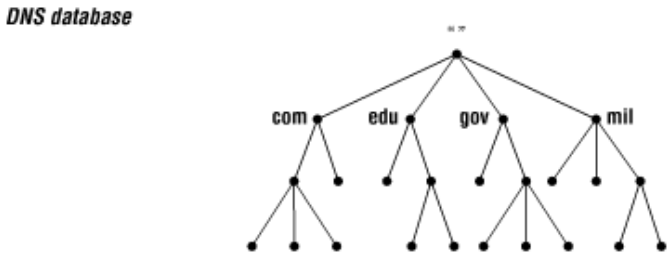

Figura 1:

Su lectura en el orden jerárquico se realiza de derecha a izquierda. Por ejemplo, para la máquina `thales.cica.es`, primero en la jerarquía se encuentra el dominio de primer nivel[1] (.es), luego va el subdominio o subdominios (en este caso, cica) y por último el nombre de la máquina (thales).

En la figura 2, podemos ver cómo sería la estructura jerárquica para la máquina `winnie.corp.hp.com`.

Los dominios genéricos de primer nivel son los .com, .edu, .org, ...más los correspondientes a los países (.es, .it, .uk, .pt, ...). En Noviembre de 2000, ICANN (*Internet Corporation for Assigned Names and Numbers* `www.icann.org`) anunció la aparición de 7 nuevos dominios de primer nivel: .biz, .info, .name, .pro, .aero, .coop y .museum.

Además de estar jerarquizada, esta estructura se encuentra delegada. Veamos qué significa esto aplicándolo a nuestra dirección `thales.cica.es`.

ICANN es una organización sin fines de lucro que opera a nivel internacional, responsable de asignar espacio de direcciones numéricas de protocolo de Internet (IP), identificadores de protocolo y de las funciones de gestión del sistema de nombres de dominio de primer nivel genéricos (gTLD) y de códigos de países (ccTLD).

El dominio de primer nivel .es se encuentra delegado por ICANN a España, más concretamente al Organismo Red.es[2]. A su vez, Red.es delega la administra-

[1] En inglés, *Top Level Domain*

[2] Anteriormente era Rediris la encargada, a través del ES-NIC.

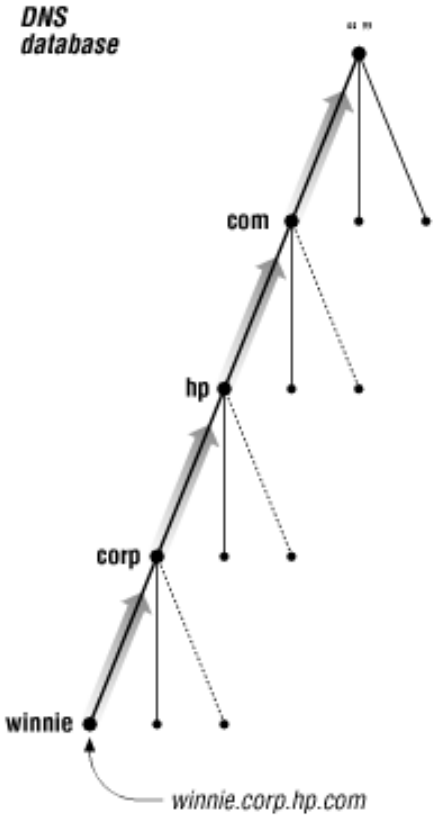

Figura 2:

ción del subdominio cica al Centro Informático Científico de Andalucía, que se convierte en responsable de todo lo que cuelgue de él, y así por ejemplo, puede darle nombre (y apellidos) a la máquina thales como `thales.cica.es`.

Este sistema hace que a pesar de la distribución y delegación de responsabilidades, todo funcione con la necesaria coordinación a nivel regional y mundial.

Para profundizar en el tema y conocer más sobre el dominio .es, podéis consultar en:
http://plugindoc.mozdev.org/linux.html

Al principio, con pocas máquinas en Internet, bastaba para mantener este sistema con unos ficheros de nombre `HOSTS.TXT o /etc/hosts`, en los que se encontraban los nombres de las máquinas uno a uno. A medida que el sistema fue creciendo, se hacía necesario el soporte de un sistema más potente, que es el basado en *Servidores de Nombres*.

2. ¿Qué necesito del DNS?

Ésta es una de las principales cuestiones a las que deberemos responder a la hora de configurar y gestionar nuestros sistemas.

La gran mayoría no necesitará montar y configurar un servidor de nombres,

pero sí se utilizan prácticamente en cada momento. Por ello, el comprender su funcionamiento y los recursos que ofrece es de gran ayuda.

Como vimos en la primera entrega, nuestra máquina Linux[3] necesita saber cómo resolver las direcciones simbólicas a numéricas. Ello se hacía mediante los ficheros `/etc/hosts`, `/etc/nsswitch.conf` y `/etc/resolv.conf`, o los correspondientes interfaces gráficos.

Debemos diferenciar la utilización que hacemos de los servidores de nombres del hecho de montar un servidor de nombres propio. Es algo así como la diferencia entre utilizar un procesador de textos para nuestro trabajo diario y el desarrollar un procesador de textos nosotros mismos.

3. Recursos del Servidor de Nombres

Para ver qué nos ofrece un servidor de nombres utilizaremos la herramienta `dig`[4]. En su forma más simple, le preguntamos como argumento con un nombre de host para conocer la dirección que le corresponde.

```
root@guadalinex:~# dig thales.cica.es

; <<>> DiG 9.2.4rc5 <<>> thales.cica.es
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49051
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;thales.cica.es.                        IN      A

;; ANSWER SECTION:
thales.cica.es.         172800  IN      A       150.214.5.10

;; AUTHORITY SECTION:
cica.es.                172800  IN      NS      chico.rediris.es.
cica.es.                172800  IN      NS      sun.rediris.es.
cica.es.                172800  IN      NS      dns1.cica.es.
cica.es.                172800  IN      NS      dns2.cica.es.

;; ADDITIONAL SECTION:
sun.rediris.es.         13337   IN      A       130.206.1.2
dns1.cica.es.           172800  IN      A       150.214.5.83
dns2.cica.es.           172800  IN      A       150.214.4.35
chico.rediris.es.       10872   IN      A       130.206.1.3

;; Query time: 80 msec
;; SERVER: 150.214.4.35#53(150.214.4.35)
;; WHEN: Sat Mar  5 18:54:39 2005
;; MSG SIZE  rcvd: 196
```

[3] Y las windows también.

[4] *Domain Information Groper*. Esta herramienta sustituye a otra anterior que se llama `nslookup`.

↬ Ésta es la salida del comando `dig`, bastante parlanchina, por cierto. La respuesta principal es la línea:

```
thales.cica.es. 172800 IN A 150.214.5.10
```

que nos dice que la máquina thales.cica.es tiene la dirección IP 150.214.5.10. Además, nos dice que es una dirección de tipo INternet (IN) y es un recurso de tipo A (Address). El valor 172800 es un valor de tiempo de vida (ttl) del servidor de nombres.

Además, dentro de su cortesía nos regala información adicional, como las líneas:

```
cica.es. 172800 IN NS sun.rediris.es.
```

que nos indican cuáles son los servidores de nombres "oficiales" para la zona cica.es, que son cuatro, con el tipo de recurso NS (Name Server), también nos ofrece sus direcciones:

```
sun.rediris.es. 13337 IN A 130.206.1.2
```

y añade el tiempo que ha tardado la consulta, a quién y cuándo. La siguiente línea

```
;; SERVER: 150.214.4.35\#53(150.214.4.35)
```

nos dice que la consulta ha sido realizada al servidor con dirección IP 150.214.4.35 por el puerto 53, que es el que utiliza el servicio DNS. Como curiosidad, comentar que las consultas a los servidores DNS pueden realizarse tanto por TCP como por UDP.

La instrucción `dig` nos será de gran ayuda para consultar a los servidores de nombres. Una llamada típica al comando `dig` es de la forma:

```
dig @servidor_de_nombres recurso tipo_del recurso
```

donde:

servidor_de_nombres es el servidor de nombres al que vamos a preguntar. En caso de que no lo especifiquemos, preguntará a los servidores de nombres que estén en el fichero `/etc/resolv.conf`

recurso es el nombre o dirección del que queremos consultar información.

tipo_del_recurso es el tipo del recurso que buscamos. Si no especificamos ninguno, buscará el tipo A por defecto.

Si el puerto del servicio de nombres (53 o domain) está cortado por nuestro proveedor de acceso o red interna, podemos utilizar un interfaz web en http://us.mirror.menandmice.com/cgibin/DoDig.

Un servidor de nombres nos ofrece varios tipos de recursos. Veremos a continuación los más importantes.

A (*Address*) Nos da la correspondencia de dirección simbólica a dirección IP

CNAME (*canonical name*) Nos especifica un alias o apodo para una dirección simbólica

MX (*mail exchanger*) Indica la máquina o las máquinas que recibirán el correo

NS (*name server*) Indica los servidores de nombres oficiales para el dominio

PTR (*pointer*) Nos da la resolución inversa de una dirección IP a una dirección simbólica

SOA (*start of authority*) Autoridad sobre el Dominio de nombres.

Exprimamos un poco más el comando `dig`. Le preguntaremos al servidor de nombres 150.214.5.83[5], que como vimos en el anterior comando, es un servidor de nombres oficial[6] para el dominio cica.es.

```
root@guadalinex:~/curso-linux# dig @150.214.4.35 ANY cica.es

; <<>> DiG 9.2.4rc5 <<>> @150.214.4.35 ANY cica.es
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51712
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 6

;; QUESTION SECTION:
;cica.es.                       IN      ANY

;; ANSWER SECTION:
cica.es.                172800  IN      SOA     dns1.cica.es. \
hostmaster.cica.es . 2005022401 86400 7200 2592000 172800
cica.es.                300     IN      MX      15 smtp2.cica.es.
cica.es.                300     IN      MX      10 smtp.cica.es.
cica.es.                172800  IN      NS      sun.rediris.es.
cica.es.                172800  IN      NS      dns1.cica.es.
cica.es.                172800  IN      NS      dns2.cica.es.
cica.es.                172800  IN      NS      chico.rediris.es.

;; ADDITIONAL SECTION:
smtp.cica.es.           172800  IN      A       150.214.5.84
smtp2.cica.es.          172800  IN      A       150.214.5.100
sun.rediris.es.         12959   IN      A       130.206.1.2
dns1.cica.es.           172800  IN      A       150.214.5.83
dns2.cica.es.           172800  IN      A       150.214.4.35
chico.rediris.es.       10494   IN      A       130.206.1.3

;; Query time: 129 msec
;; SERVER: 150.214.4.35#53(150.214.4.35)
;; WHEN: Sat Mar  5 19:00:57 2005
;; MSG SIZE  rcvd: 295
```

[5] Podríamos haber puesto `dns1.cica.es`

[6] El nombre en inglés es *authoritative*

Los registros A y NS ya nos son conocidos. También nos encontramos con registros MX, que a pesar de tener una gran importancia no son muy conocidos[7].

```
cica.es. 300 IN MX 15 smtp2.cica.es.
cica.es. 300 IN MX 10 smtp.cica.es.
```

¿Por qué dijimos que eran muy importantes?, pues sencillamente porque dirigen los correos electrónicos. ¿Quién hoy día si le quitan el correo electrónico se quedaría igual?. Pues estos registros dicen que para todas las direcciones de correo electrónico del dominio cica.es[8], como por ejemplo *jperez@cica.es*, deben dirigirse a los "intercambiadores de correo"[9]. Como es algo muy crítico, se suelen poner varios con una preferencia y en caso de fallo de alguno, los correos van al siguiente. En este caso irían preferentemente a `smtp.cica.es` y en caso de fallo de éste a `smtp2.cica.es`.

Preguntemos por un registro CNAME. El registro CNAME se suele utilizar como un alias o pseudónimo de otra u otras máquinas. ¿Qué utilidad puede tener ésto? Por ejemplo, los servicios de Internet suelen prestarse en direcciones estandarizadas. Si queremos ver el Boletín Oficial del Estado y no sabemos con certeza la dirección, una de las primeras que probaremos si tenemos cierta experiencia con internet será `www.boe.es`. Nuestra máquina con el servidor web, no tiene porqué llamarse www[10] y además nos permite cambiar rápidamente a otra máquina sin demasiados problemas en nuestra red. Veamos lo que hace el CICA.

```
root@guadalinex:~# dig CNAME www.cica.es

; <<>> DiG 9.2.4rc5 <<>> CNAME www.cica.es
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31238
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;www.cica.es.                   IN      CNAME

;; ANSWER SECTION:
www.cica.es.            3600    IN      CNAME   ataman.cica.es.

;; AUTHORITY SECTION:
cica.es.                172800  IN      NS      chico.rediris.es.
cica.es.                172800  IN      NS      sun.rediris.es.
cica.es.                172800  IN      NS      dns1.cica.es.
cica.es.                172800  IN      NS      dns2.cica.es.

;; ADDITIONAL SECTION:
sun.rediris.es.         12495   IN      A       130.206.1.2
dns1.cica.es.           172800  IN      A       150.214.5.83
dns2.cica.es.           172800  IN      A       150.214.4.35
chico.rediris.es.       10030   IN      A       130.206.1.3
```

[7] Bueno, tú ya sé que eres un experto y sí los conoces ;-)

[8] Y de sus subdominios en caso de que no tengan especificados los suyos propios.

[9] Que eso es *Mail eXchanger*, de donde viene MX.

[10] Sería un nombre bastante feo

```
;; Query time: 80 msec
;; SERVER: 150.214.4.35#53(150.214.4.35)
;; WHEN: Sat Mar  5 19:08:41 2005
;; MSG SIZE  rcvd: 198
```

La línea importante en esta consulta es la que nos dice que `www.cica.es` es un apodo (CNAME) de la máquina `ataman.cica.es`. Si esa máquina se cae, una posible solución es cambiar el registro CNAME de `www.cica.es` a `atamon.cica.es`, que es una máquina que tenemos preparada para ello. El resto de usuarios (de todo el mundo) seguirán apuntando sus navegadores a `www.cica.es` sin enterarse del problema.

El recurso PTR es un poco más complicado. Veamos. Para que el mismo sistema funcione tanto para pedir conversiones de direcciones simbólicas a direcciones IP, como al revés, de direcciones IP a direcciones simbólicas se crea el recurso PTR y un dominio especial de nombre `in-addr.arpa`.

Un comando sencillo para saber el nombre que le corresponde a una dirección IP es el comando host:

```
maquina:\# host 150.214.5.10
10.5.214.150.in-addr.arpa domain name pointer thales.cica.es.
```

Vemos que nos devuelve que la dirección IP 150.214.5.10 se corresponde con la dirección simbólica `thales.cica.es`, pero antes da una información un poco rara. Como en las direcciones simbólicas la jerarquía va de derecha a izquierda y en las direcciones IP de izquierda a derecha, se emplea un truco. Todas las direcciones IP se colocan bajo el `dominio in-addr.arpa` y se va poniendo cada uno de los bytes de la dirección IP de derecha a izquierda. Así 150.214.5.10 queda como `10.5.214.150.in-addr.arpa`. Veamos qué dice nuestro amigo `dig` sobre esto:

```
root@guadalinex:~/curso-linux# dig PTR 10.5.214.150.in-addr.arpa

; <<>> DiG 9.2.4rc5 <<>> PTR 10.5.214.150.in-addr.arpa
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17607
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

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

;; ANSWER SECTION:
10.5.214.150.in-addr.arpa. 3600 IN      PTR     thales.cica.es.

;; AUTHORITY SECTION:
5.214.150.in-addr.arpa. 3600    IN      NS      dns2.cica.es.
5.214.150.in-addr.arpa. 3600    IN      NS      dns1.cica.es.

;; ADDITIONAL SECTION:
dns1.cica.es.           172800  IN      A       150.214.5.83
dns2.cica.es.           172800  IN      A       150.214.4.35

;; Query time: 155 msec
```

```
;; SERVER: 150.214.4.35#53(150.214.4.35)
;; WHEN: Sat Mar  5 19:15:56 2005
;; MSG SIZE  rcvd: 141
```

Correcto. Nos dice que estamos hablando de `thales.cica.es` y es un registro de tipo PTR (*PoinTeR*).

4. Servidores de Nombres

Seguro que el DNS os ha deparado muchas sorpresas. Pues aún hay más. El hecho de configurar un Servidor de Nombres es una auténtica odisea.

El servidor de nombres por excelencia es el demonio `named`, que es parte del paquete BIND, preparado y coordinado por el *Internet Software Consortium*.

Un servidor de nombres puede estar configurado de alguna de estas formas:

master Es el "dueño" del dominio[11], en el que se hacen las modificaciones para ese dominio, responde las consultas que se le hagan y se encarga de propagarlo al resto.

slave Son servidores de nombres del dominio y así se encargan de resolver las preguntas que se les hagan. Pero cada cierto tiempo le preguntan al "master" del que dependen para actualizar su información.

caching-only Solamente constituyen un caché de datos para optimizar las respuestas [12]. Por ejemplo, podemos montar uno de este tipo en nuetro equipo u organización para que todos los puestos clientes le pregunten a él. Sirve para optimizar las respuestas y el uso de la línea de comunicaciones, pero además simplifica la política de seguridad. Para las peticiones de resolución DNS, los clientes no pueden atravesar el cortafuegos y sí esta única máquina.

forwarding Redirige las peticiones a otros servidores de nombres. Es poca la diferencia con el de caché.

5. DNSmasq

DNSmasq actúa como DNS forwarder, cacheando las peticiones DNS que se realizan y por tanto acelerando la resolución de nombres para una red local. Además, DNSmasq resuelve también las direcciones estáticas que estén definidas en su `/etc/hosts`, lo que permite tener de una manera sencilla el mismo servidor DNS para la resolución de nombres internos y externos.

Para instalar DNSmasq basta con hacer:

```
apt-get install dnsmasq
```

[11] Zona es el término empleado.

[12] En algunos sistemas (por ejemplo, fedora) se incluye una caché local mediante el demonio `nscd` (*name server cache daemon*)

A continuación, editamos el fichero `/etc/dnsmasq.conf` y modificamos las siguientes líneas:

- Descomentamos `strict-order` para que se realicen las peticiones DNS a los servidores que aparecen en el fichero `/etc/resolv.conf` en el orden en el aparecen.
- Descomentamos `address` y ponemos el dominio de que alojamos en nuestra red local:

  ```
  address=/dominio1.com/192.168.2.3
  ```

  para que la petición no tenga que salir a Internet.
- Incluimos las interfaces de red que deben aceptar peticiones DNS, por ejemplo:

  ```
  interface=eth2
  interface=eth3
  ```

- Incluímos las direcciones IP que aceptan peticiones DNS, por ejemplo:

  ```
  listen-address=192.168.2.2
  listen-address=127.0.0.1
  ```

En los clientes bastará con modificar los ficheros `/etc/resolv.conf`, incluyendo sólo la dirección de nuestro DNS local, por ejemplo:

```
nameserver 192.168.2.2
```