



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE EDUCACIÓN,  
POLÍTICA SOCIAL Y DEPORTE

SECRETARÍA DE ESTADO  
DE EDUCACIÓN Y FORMACIÓN  
DIRECCIÓN GENERAL DE  
FORMACIÓN PROFESIONAL

INSTITUTO SUPERIOR DE  
FORMACIÓN Y RECURSOS EN  
RED PARA EL PROFESORADO

# REDES DE ÁREA LOCAL: APLICACIONES Y SERVICIO EN LINUX

## Servidor DNS



Formación en **Red**

# Índice de contenido

Servidor DNS.....	1
Definición de Servidor DNS .....	2
Servidor DNS sencillo con dnsmasq.....	4
Instalación del servidor dnsmasq.....	4
Arranque y parada del servidor dnsmasq .....	5
Configuración básica de dnsmasq.....	5
Servidor DNS y servidor DHCP .....	7
Instalación del servidor DNS bind.....	8
Configuración del servidor DNS.....	8
Servidor DNS maestro .....	8
Servidor DNS esclavo.....	9
Servidor caché DNS .....	9
Archivos de configuración del DNS .....	10
Configuración como caché DNS.....	10
Configuración DNS maestro .....	11
Archivo de zona de búsqueda directa .....	11
Archivo de zona de búsqueda inversa .....	12
Configuración DNS esclavo .....	13
Arranque y parada manual del servidor DNS .....	15
Arranque automático del servidor DNS al iniciar el sistema. ....	15

## Definición de Servidor DNS

*El número de ordenadores en el centro educativo, cada vez es mayor. Aunque hayamos elegido un direccionamiento IP que relacione la asignación de direcciones con la ubicación física de los PCs, sería mucho más cómodo poder referirse a todos los PCs del centro utilizando nombres en lugar de direcciones IPs. Un servidor DNS en la red local, nos permitirá crear una asociación directa Nombre de PC <-> Dirección IP en nuestra red, que nos facilitará la identificación de nuestros equipos.*

En las redes TCP/IP, cada PC dispone de una dirección IP para poder comunicarse con el resto de PCs. Es equivalente a las redes de telefonía en las que cada teléfono dispone de un número de teléfono que le identifica y le permite comunicarse con el resto de teléfonos.

Trabajar con direcciones IP es incómodo para las personas, ya que requeriría conocer en todo momento las direcciones IP de los equipos a los que queremos conectarnos. En su lugar utilizamos **nombres** que son más fáciles de recordar y utilizar como por ejemplo **enebro.pntic.mec.es**, **www.google.es**, **www.mec.es**, etc...

Cada equipo y cada servidor conectado a Internet, dispone de una dirección IP y de un nombre perteneciente a un dominio. Internamente, la comunicación entre los PCs se realiza utilizando direcciones IP por eso es necesario algún sistema que permita, a partir de los nombres de los PCs, averiguar las direcciones IPs de los mismos. Ejemplo, cuando queremos acceder a la página web del MEC (Ministerio de Educación), en la barra de direcciones del navegador escribimos:

**<http://www.mec.es>**

nuestro PC tendrá que averiguar cual es la IP correspondiente a **www.mec.es** y una vez que ha averiguado que su IP es **195.53.123.85**, se conecta con el servidor para adquirir la página web principal y mostrarla al usuario. Si en el navegador escribimos:

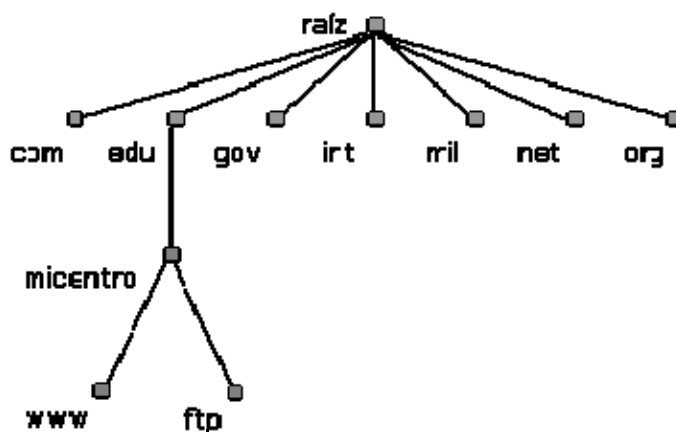
**http://193.147.0.29**

ahorraremos el paso de averiguar la IP y directamente nos mostrará la página web del MEC.

Un **servidor DNS** es un servidor que permite averiguar la IP de un PC a partir de su nombre. Para ello, el servidor DNS dispone de una base de datos en la cual se almacenan todas las direcciones IP y todos los nombres de los PCs pertenecientes a su dominio.

No existe una base de datos única donde se almacenan todas las IPs existentes en el mundo, sino que cada servidor almacena las IPs correspondientes a su dominio. Los servidores DNS están dispuestos jerárquicamente de forma que cuando nuestro servidor más inmediato no puede atender nuestra petición, éste la traslada al DNS superior.

En el proceso de resolución de un nombre, hay que tener en cuenta que los servidores DNS funcionan frecuentemente como clientes DNS, consultando a otros servidores para resolver completamente un nombre consultado.



En este curso configuraremos un servidor DNS local. Las entradas existentes en nuestro DNS no serán visibles en Internet solamente servirán a los equipos de nuestra red local. De esta forma, cuando un usuario de nuestra red intente acceder a un recurso local, podrá utilizar **nombres** en lugar de direcciones IP. Si el usuario desea acceder fuera de nuestra red local a algún recurso en Internet, el DNS local nunca podrá llevar a cabo dicha resolución y se la traslada al siguiente servidor DNS (que sí estará en Internet) en su jerarquía de servidores DNS, hasta que la petición sea satisfecha.

Con servidor DNS en nuestra red local, si hacemos un ping a un PC cuyo nombre es "equipo10" y cuya IP es 192.168.0.40; podemos lanzar el comando "ping" indistintamente contra dicha IP o contra el nombre del equipo en el dominio:

- ping 192.168.0.40
- ping equipo10.micentro.edu

en ambos casos obtendremos respuesta. Esto es muy útil cuando las estaciones de trabajo reciben su IP por DHCP ya que puede ocurrir que desconozcamos la IP que tiene cierto equipo pero sí conocer su nombre en el dominio, que será invariable.

Otro ejemplo donde el servidor DNS tomará protagonismo será cuando deseemos acceder a un servidor web instalado en nuestro servidor; si hemos denominado al sitio web como "www", podremos introducir en el DNS una entrada que identifique "www" como 192.168.0.220 (dirección IP de nuestro servidor web), de modo que cuando introduzcamos la URL "www.micentro.edu" accederemos a nuestro servidor web. Lo mismo sería aplicable al servidor ftp o cualquier otro servicio.

Antes de comenzar con los procesos de instalación y configuración de nuestro DNS, vamos a definir algunos términos que utilizaremos a lo largo de dicho proceso.

**Zona de Búsqueda Directa:** Las resoluciones de esta zona devuelven la dirección IP correspondiente al recurso solicitado. Realiza las resoluciones que esperan como respuesta la dirección IP de un determinado recurso.

**Zona de Búsqueda Inversa:** Las resoluciones de esta zona buscan un nombre de equipo en función de su dirección IP; una búsqueda inversa tiene forma de pregunta, del estilo "¿Cuál es el nombre DNS del equipo que utiliza la dirección IP 192.168.0.20?".

**Reenviador DNS:** Servidor DNS designado por otros servidores DNS internos para su uso en consultas para resolver nombres de dominio DNS externos o fuera del dominio local.

Linux dispone de varios paquetes de software que permiten poner en marcha un servidor DNS. En este capítulo hablaremos de dos de ellos: el paquete **dnsmasq** que es un sencillo servidor DNS ideal para redes pequeñas como las que podemos encontrar en los centros educativos y el paquete **bind** que es un completo servidor DNS utilizado por muchos servidores DNS en Internet.

## Servidor DNS sencillo con dnsmasq

*El paquete dnsmasq permite poner en marcha un servidor DNS de una forma muy sencilla. Simplemente instalando y arrancando el servicio dnsmasq, sin realizar ningún tipo de configuración adicional, nuestro PC se convertirá en un servidor caché DNS y además, resolverá los nombres que tengamos configurados en el archivo /etc/hosts de nuestro servidor. La resolución funcionará tanto en sentido directo como en sentido inverso, es decir, resolverá la IP dado un nombre de PC y el nombre del PC dada la IP. Adicionalmente, dnsmasq dispone de servidor DHCP y permite resolver los nombres de los PCs a los que les ha asignado dirección IP dinámica. A lo largo de esta sección veremos todas estas posibilidades que nos ofrece dnsmasq.*

## Instalación del servidor dnsmasq

Para instalar la última versión de dnsmasq, podemos hacerlo con apt-get desde una consola de root:

```
// Instalación del servidor dnsmasq
# apt-get install dnsmasq
```

De esta forma instalaríamos los programas necesarios para disponer de un sencillo servidor DNS. Tan solo será necesario configurarlo y ponerlo en marcha.

## Arranque y parada del servidor dnsmasq

El servicio dnsmasq, al igual que todos los servicios, dispone de scripts de arranque y parada en la carpeta /etc/init.d. Debemos ejecutarlos desde una consola de root.

```
// Arrancar o reiniciar el servidor dnsmasq
# /etc/init.d/dnsmasq restart

// Parar el servidor dnsmasq
# /etc/init.d/dnsmasq stop
```

Para un arranque automático del servicio al iniciar el servidor, debemos crear los enlaces simbólicos correspondientes tal y como se indica en el apartado [Arranque automático de servicios al iniciar el sistema](#).

## Configuración básica de dnsmasq

Para que dnsmasq pueda ser un servidor caché DNS, es necesario que nuestro servidor tenga en el archivo de /etc/resolv.conf configurado al menos un servidor DNS externo. Normalmente los servidores DNS externos nos los proporciona el operador de telecomunicaciones que nos da servicio de Internet. Por ejemplo, Telefónica tiene unos DNSs, Orange tiene otros, ONO tiene otros, Tele2 otros, etc... Aunque podemos utilizar los de cualquier operador, lo mejor es configurar los del nuestro, porque responderá más rápido.

Servidores DNS de Telefónica:

- **DNS primario 80.58.0.33**
- **DNS alternativo (por si falla el primario) 80.58.32.97**

Servidores DNS de Orange:

- **DNS primario 62.36.225.150**
- **DNS alternativo 62.37.228.20**

Para que nuestro servidor utilice los DNS externos, debemos añadirlos en /etc/resolv.conf. En el caso de Telefónica, deberemos añadir en /etc/resolv.conf las siguientes líneas:

```
// Ejemplo: Utilización de los DNS externos de Telefónica
// Añadir en /etc/resolv.conf del servidor
nameserver 80.58.0.33
nameserver 80.58.32.97
```

Una vez introducidos los DNS externos en /etc/resolv.conf, debemos comprobar si dichos DNS externos funcionan correctamente y responden a las peticiones. Para ello haremos una consulta al DNS mediante el comando nslookup. También podríamos utilizar el comando host o el comando dig:

```
// Probar DNS externo
// Ejecutar en una consola del servidor
```

```
$ nslookup www.unican.es
```

Si el DNS funciona, nos dirá cual es la IP del servidor de la Universidad de Cantabria, www.unican.es.

En este punto, ya tendremos en nuestro servidor un **servidor DNS caché** funcionando. Para probar su funcionamiento, configuraremos el archivo /etc/resolv.conf del resto de los PCs de nuestra red pero en lugar de indicar los DNS de Telefónica, indicaremos el nuestro. Si nuestro servidor tiene la IP 192.168.1.239, lo añadiremos en el archivo /etc/resolv.conf de cada PC

```
// Añadir en /etc/resolv.conf del PC cliente
nameserver 192.168.1.239
```

Al igual que hemos hecho anteriormente, podemos comprobar si nuestro servidor DNS funciona correctamente, haciendo una consulta mediante el comando nslookup:

```
// Probar nuestro servidor DNS
//Ir al PC cliente, abrir una consola de comandos y ejecutar:
$ nslookup www.unican.es
```

Si nuestro servidor DNS funciona, nos responderá con la IP del servidor de la Universidad de Cantabria.

Ahora que ya tenemos el servidor DNS caché funcionando, iremos más allá. El siguiente paso será editar el archivo /etc/hosts de nuestro servidor, para que nuestro DNS resuelva también los nombres y las IPs de nuestra red. Si los PCs de nuestra red disponen de IP fija y queremos que dnsmasq resuelva sus nombres e IPs, tan solo tenemos que añadir los nombres y las IPs en el archivo hosts del servidor y sería como disponer de un **DNS maestro** para nuestra red:

```
//Añadir en /etc/hosts del servidor las IPs y los nombres de nuestros PCs
//Se pueden añadir varios nombres en la misma línea. Separar con un tabulador
192.168.1.239      www.ieslapaloma.com      proxy      www
192.168.1.238      impresora
192.168.1.1        router
192.168.1.101     a1pc1      aula1pc1
192.168.1.102     a1pc2      aula1pc2
192.168.1.103     a1pc3      aula1pc3
192.168.1.104     a1pc4      aula1pc4
192.168.1.105     a1pc5      aula1pc5
192.168.1.106     a1pc6      aula1pc6
192.168.1.107     a1pc7      aula1pc7
192.168.1.108     a1pc8      aula1pc8
192.168.1.109     a1pc9      aula1pc9
192.168.1.110     a1pc10     aula1pc10
```

Si desde un PC de nuestra red hacemos una consulta al DNS preguntando por otro PC de nuestra red, dnsmasq resolverá en el servidor y devolverá la IP configurada en el archivo hosts del servidor:

```
// Probar nuestro servidor DNS con nombres de nuestra red
// Ejecutar en una consola del PC cliente
$ nslookup aula1pc1
```

Cada vez que modifiquemos el archivo `/etc/hosts` del servidor, deberemos ejecutar **`/etc/init.d/dnsmasq restart`** para reiniciar el servicio dnsmasq y recargue la información contenida en dicho archivo.

De esta manera, tan solo editando el archivo `/etc/hosts` del servidor, dispondremos de un sencillo servidor DNS para nuestra red lo que nos permitirá referirnos a nuestros PCs utilizando sus nombres que son mucho más fáciles de recordar que las direcciones IP.

## Servidor DNS y servidor DHCP

Cuando las IPs de los PCs de nuestra red son dinámicas, se nos presenta un problema para utilizar un servidor DNS ya que el mismo PC, hoy puede tener una IP y mañana puede tener otra IP diferente. Dicho problema se puede resolver de tres formas:

**Utilizando un servidor DNS dinámico:** Los PCs, al recibir la IP del servidor DHCP, informarán al servidor DNS dinámico de la IP que les ha sido asignada de forma dinámica y así poder asociar de forma correcta el nombre con la IP que tiene en un momento dado. El inconveniente de este método es que nos obliga a instalar en los PCs un servicio que informe al servidor DNS dinámico de los cambios de IP de cada PC. Es similar al sistema utilizado por los servidores DNS dinámicos de Internet como [www.no-ip.org](http://www.no-ip.org) o [www.dyndns.com](http://www.dyndns.com). Aquí no hablaremos de servidores DNS dinámicos porque las dos soluciones siguientes son más sencillas.

**Utilizando reservas de DHCP:** En el servidor DHCP existe la posibilidad de establecer una configuración concreta a un cliente concreto identificándolo por la dirección MAC de su tarjeta de red. Si configuramos tantas reservas de IPs como PCs hay en nuestra red, podríamos configurar a cada PC la IP que deseemos. Esto sería como tener IPs fijas en nuestra red, pero asignadas por DHCP. Esta idea no es para nada descabellada y nos permitiría controlar en todo momento la IP de cada PC.

**Utilizando el servidor DHCP de dnsmasq:** Dnsmasq, además de ofrecernos un servidor DNS, nos ofrece también un servidor DHCP fácilmente configurable que además resolverá los nombres de los PCs de nuestra red aún cuando sus IPs hayan sido configuradas por DHCP. Para configurar el servidor DHCP de dnsmasq debemos editar el archivo de configuración `/etc/dnsmasq.conf` y añadir una línea como esta: **`dhcp-range=ip-inicial,ip-final, tiempo de cesión`**. Ejemplo, si queremos que el DHCP utilice el rango desde 192.168.1.201 hasta 192.168.1.230 y que la cesión dure 24 horas, editaremos `/etc/dnsmasq.conf` y añadiremos la siguiente línea:

```
//Editar /etc/dnsmasq.conf para establecer el rango DHCP
//Añadir la siguiente línea:
dhcp-range=192.168.1.201,192.168.1.230,24h
```

Cuando los PCs clientes pidan una IP al servidor DHCP, normalmente el cliente suministrará su nombre de PC. Dicho nombre será utilizado por dnsmasq para asociarlo a la IP que le ha sido asignada al PC y así resolver correctamente cualquier consulta DNS.

A medida que el servidor DHCP va concediendo IPs a todos los PCs que se la solicitan, éste va almacenándolas en el archivo de concesiones **/var/lib/misc/dnsmasq.leases** donde guarda la fecha y la hora de la cesión en formato %s (ver man date para información sobre dicho formato) la MAC del cliente, la IP concedida al cliente y el nombre del PC cliente siempre y cuando el cliente haya enviado su nombre de PC.

```
//Archivo donde aparecen las IPs asignadas a cada PC
/var/lib/misc/dnsmasq.leases
```

Para que dnsmasq pueda conocer el nombre del cliente, éste deberá enviar su nombre cuando realiza la petición DHCP. En los clientes Linux, el nombre que envía el PC cliente, suele almacenarse en el parámetro send host-name del archivo de configuración del cliente dhcp: /etc/dhcp3/dhclient.conf. Ejemplo, si nuestro PC se llama aula1pc1, deberemos configurarlo en el cliente dhcp:

```
//Configurar en /etc/dhcp3/dhclient.conf el nombre que envía el cliente al servidor DHCP:
send host-name aula1pc1
```

Lo normal es que dicho nombre coincida con el nombre del PC almacenado en el archivo /etc/hostname.

## Instalación del servidor DNS bind

Si con las posibilidades que nos ofrece dnsmasq no son suficientes para nuestra red y necesitamos un servidor DNS más completo, podemos utilizar el paquete **bind9**. Para instalarlo, podemos hacerlo con apt-get desde una consola de root:

```
// Instalación del servidor DNS bind
# apt-get install bind9
```

De esta forma instalaríamos los programas necesarios para disponer de un completo servidor DNS con bind. Tan solo será necesario configurarlo y ponerlo en marcha.

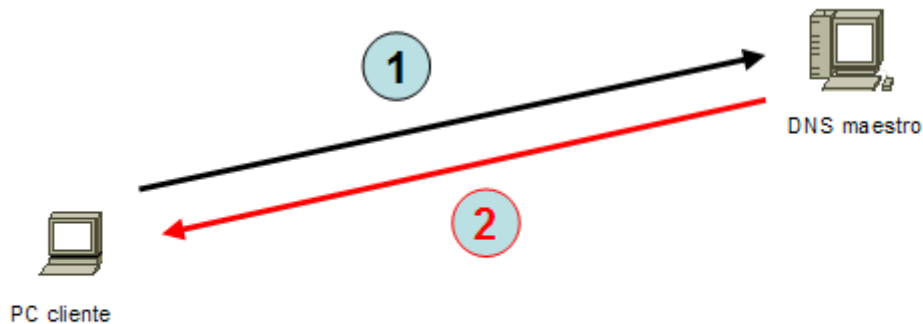
## Configuración del servidor DNS

El servidor DNS bind admite tres modos de funcionamiento

- Servidor DNS maestro
- Servidor DNS esclavo
- Servidor caché DNS

## Servidor DNS maestro

En este modo de funcionamiento, nuestro servidor se comporta como un auténtico servidor DNS para nuestra red local. Atenderá directamente a las peticiones de resolución de direcciones pertenecientes a la red local y reenviará a servidores DNS externos las peticiones del resto de direcciones de Internet.



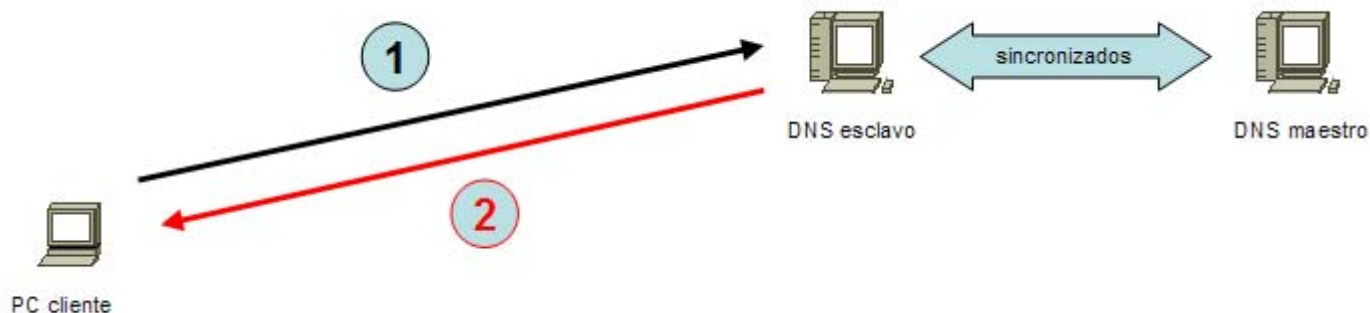
1 – Consulta DNS: ¿Cuál es la IP de aula5pc7.ieslapaloma.com?

2 – Respuesta DNS: La IP de aula5pc7.ieslapaloma.com es 192.168.0.107

### Consulta a un DNS maestro

## Servidor DNS esclavo

Un servidor esclavo actuará como un servidor espejo de un servidor DNS maestro. Permanecerá sincronizado con el maestro. Se utilizan para repartir las peticiones entre varios servidores aunque las modificaciones solo se realicen en el maestro. En redes locales salvo por razones de disponibilidad, es raro que exista la necesidad de tener dos servidores DNS ya que con uno será suficiente.



### Consulta a un DNS esclavo

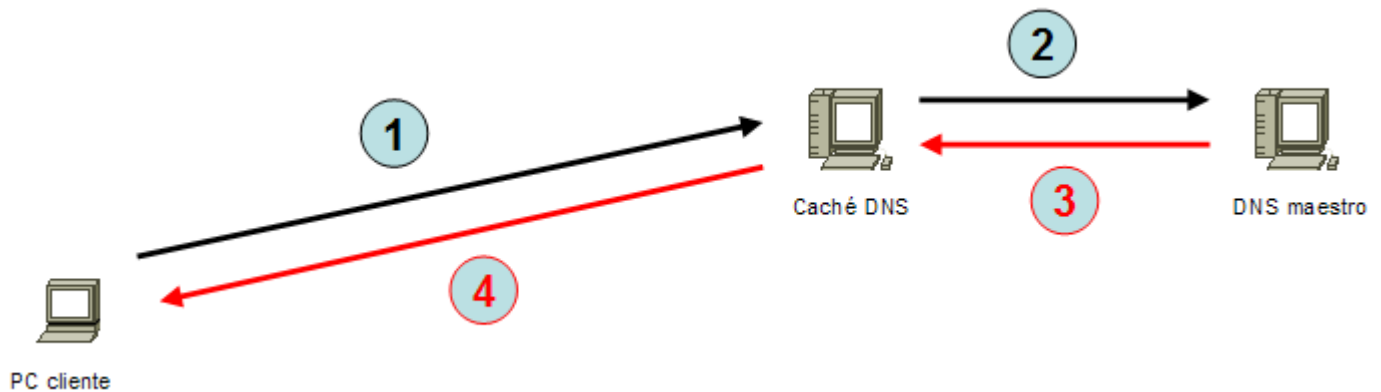
## Servidor caché DNS

En este modo de funcionamiento, nuestro servidor se comporta como si fuera un auténtico servidor DNS para nuestra red local aunque realmente no sea un servidor DNS propiamente dicho. Cuando recibe una petición de DNS por parte de un cliente de nuestra red, la trasladará a un DNS maestro que puede estar en nuestra red o fuera, almacenará en una memoria caché la respuesta y a la vez la comunicará a quien hizo la petición. Si un segundo cliente vuelve a realizar la misma petición, como nuestro servidor tiene la respuesta almacenada en su memoria caché, responderá inmediatamente sin tener que cursar la petición a ningún servidor DNS de Internet.

Disponer de un servidor caché DNS en nuestra red local aumenta la velocidad de la conexión a Internet pues cuando navegamos por diferentes lugares, continuamente se están realizando peticiones DNS. Si nuestro caché DNS almacena la gran mayoría de peticiones que se realizan desde la red local, las respuestas de los clientes se satisfarán

prácticamente de forma instantánea proporcionando al usuario una sensación de velocidad en la conexión.

Es un modo de funcionamiento de sencilla configuración ya que prácticamente lo único que hay que configurar son las direcciones IP de un DNS primario y de un DNS secundario. Muchos routers ADSL ofrecen ya este servicio de caché, tan solo hay que activarlo y configurar una o dos IPs de servidores DNS en Internet. En los PCs de nuestra red local podríamos poner como DNS primario la IP de nuestro router y como DNS secundario una IP de un DNS de Internet.



**Consulta a un cache DNS. En caso de fallo, se redirecciona hacia un DNS maestro**

## Archivos de configuración del DNS

El archivo de configuración del DNS es el archivo `/etc/bind/named.conf`, pero este hace referencia a otros cuantos archivos como por ejemplo:

Archivo	Descripción
<code>named.conf</code>	Archivo principal de configuración
<code>named.conf.options</code>	Opciones genéricas
<code>named.conf.local</code>	Especificación particular de este servidor DNS
<code>db.127</code>	Especificación dirección de retorno
<code>db.root</code>	DNSs de nivel superior
otros	<code>db.0, db.255, db.empty, db.local, rndc.conf, rndc.key, zones.rfc1918</code>

## Configuración como caché DNS

Por defecto, al instalar el paquete `bind` está preconfigurado como servidor caché DNS. Tan solo será necesario editar el archivo `/etc/bind/named.conf.options` y en la sección `forwarders` añadir las IPs de dos servidores DNS donde redirigir las peticiones DNS:

```
// Configuración como caché DNS
// Añadir IPs de los DNS de nuestro proveedor en /etc/bind/named.conf.options
options {
    forwarders {
        80.58.0.33; 80.58.32.97;
    };
};
```

## Configuración DNS maestro

Por razones de accesibilidad y organizativas, deseamos asignar un nombre a todos los equipos de nuestra red, para lo que instalaremos un servidor DNS privado con un **dominio ficticio**, por ejemplo 'ieslapaloma.com'. Todos los PCs de nuestra red pertenecerán a dicho dominio ficticio que funcionará solo en nuestra red interna, no en Internet. En tal caso el nombre completo de los PCs terminará con 'ieslapaloma.com', por ejemplo: aula5pc2.ieslapaloma.com. Lo ideal en una situación así es disponer de un servidor DNS que sea maestro de nuestro dominio, es decir, maestro del dominio interno 'ieslapaloma.com'.

Nuestro servidor DNS maestro para nuestro dominio ficticio interno 'ieslapaloma.com' será capaz de resolver peticiones internas de nombres de este dominio, tanto de forma directa como de forma inversa, es decir, si recibe una consulta acerca de quién es aula5pc7.ieslapaloma.com deberá devolver su IP, pongamos por ejemplo 192.168.0.107. Si la consulta es una consulta DNS inversa acerca de quién es 192.168.0.107, deberá responder aula5pc7.ieslapaloma.com. Por ello deberemos añadir en el archivo /etc/bind/named.conf.local la especificación de maestro para el dominio y para la resolución inversa, por ejemplo:

```
// Añadir en /etc/bind/named.conf.local
// Archivo para búsquedas directas
zone "ieslapaloma.com" {
    type master;
    file "/etc/bind/ieslapaloma.db";
};

// Archivo para búsquedas inversas
zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/192.rev";
};
```

Evidentemente será necesario crear los archivos ieslapaloma.db y 192.rev que especificarán la asociación entre nombres y direcciones IP de nuestra red en un sentido y en otro respectivamente.

### Archivo de zona de búsqueda directa

Supongamos que en nuestra red local tenemos un aula llamada aula5 con 12 PCs con IPs que van desde la 192.168.0.101 hasta 112 y cuyos nombres van desde aula5pc1 hasta aula5pc10, luego un servidor web (pc11) y un servidor de correo electrónico que además es servidor DNS (pc12). El archivo de configuración DNS de nuestro dominio podría ser así:

```
// Archivo /etc/bind/ieslapaloma.db
;
; BIND data file for ieslapaloma.com
;
@      IN      SOA     ieslapaloma.com. root.ieslapaloma.com. (
        1          ; Serial
        604800     ; Refresh
        86400      ; Retry
        2419200    ; Expire
        604800 )   ; Default TTL
```

```

      IN      NS      dns.ieslapaloma.com.
            IN      MX      10      mail.ieslapaloma.com.

aula5pc1 IN      A      192.168.0.101
aula5pc2 IN      A      192.168.0.102
aula5pc3 IN      A      192.168.0.103
aula5pc4 IN      A      192.168.0.104
aula5pc5 IN      A      192.168.0.105
aula5pc6 IN      A      192.168.0.106
aula5pc7 IN      A      192.168.0.107
aula5pc8 IN      A      192.168.0.108
aula5pc9 IN      A      192.168.0.109
aula5pc10      IN      A      192.168.0.110
www         IN      A      192.168.0.111
dns         IN      A      192.168.0.112
mail        IN      A      192.168.0.112

```

Las primeras líneas son unos parámetros relacionados con la actualización del DNS (número de serie y periodos de actuación). Las dos siguientes líneas indican quién es el servidor primario (NS = Name Server) y quien procesa el correo electrónico del dominio (MX = Mail eXchange). Las siguientes líneas especifican las IPs de los distintos PCs componentes del dominio (A = Address).

Si olvidamos algún punto y coma, dará errores y no funcionará correctamente. Para revisar los archivos disponemos de los comandos `named-checkconf` y `named-checkzone` que analizan que esté correcta la sintaxis de los mismos.

## Archivo de zona de búsqueda inversa

Para poder realizar consultas inversas (de IP a nombre) será necesario crear el siguiente archivo:

```

// Archivo /etc/bind/192.rev
;
; BIND reverse data file for 192.168.0.0
;
@      IN      SOA      ieslapaloma.com. root.ieslapaloma.com. (
        1          ; Serial
        604800     ; Refresh
        86400      ; Retry
        2419200    ; Expire
        604800 )    ; Default TTL

      IN      NS      dns.ieslapaloma.com.

101           IN      PTR      aula5pc1.ieslapaloma.com.
102           IN      PTR      aula5pc2.ieslapaloma.com.
103           IN      PTR      aula5pc3.ieslapaloma.com.
104           IN      PTR      aula5pc4.ieslapaloma.com.
105           IN      PTR      aula5pc5.ieslapaloma.com.
106           IN      PTR      aula5pc6.ieslapaloma.com.
107           IN      PTR      aula5pc7.ieslapaloma.com.
108           IN      PTR      aula5pc8.ieslapaloma.com.
109           IN      PTR      aula5pc9.ieslapaloma.com.
110           IN      PTR      aula5pc10.ieslapaloma.com.
111           IN      PTR      www.ieslapaloma.com.
112           IN      PTR      dns.ieslapaloma.com.
112           IN      PTR      mail.ieslapaloma.com.

```

Una vez configurado nuestro servidor DNS, debemos indicar a nuestro servidor Linux que el servidor DNS es él mismo, lo cual se especifica en el archivo `/etc/resolv.conf`.

```
// Indicamos que nosotros mismos somos servidores DNS
// y por defecto buscamos en nuestro dominio
// Editar /etc/resolv.conf del servidor DNS
nameserver 127.0.0.1
search ieslapaloma.com
```

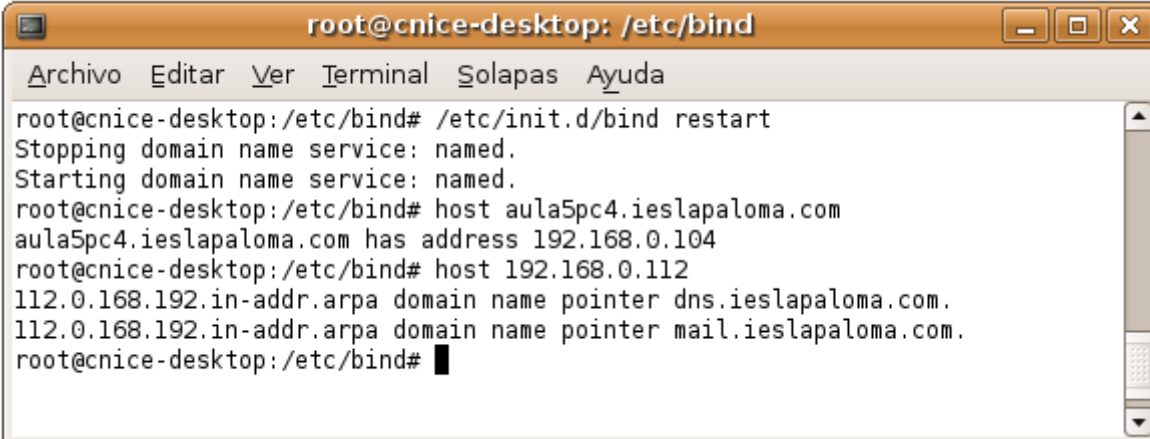
En el resto de PCs de la red, indicaremos que el servidor DNS es 192.168.0.112

```
// En el resto de PCs de la red indicamos quién es el DNS
// Editar /etc/resolv.conf del resto de PCs de la red
nameserver 192.168.0.112
```

Tan solo nos faltará poner en marcha nuestro servidor de nombres ejecutando en el servidor el script de inicio correspondiente:

```
// Arranque del servidor DNS
# /etc/init.d/bind9 restart
```

y, mediante el comando **host**, el comando **dig** o el comando **nslookup** hacer alguna consulta de prueba:



```
root@cnice-desktop: /etc/bind
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
root@cnice-desktop:/etc/bind# /etc/init.d/bind restart
Stopping domain name service: named.
Starting domain name service: named.
root@cnice-desktop:/etc/bind# host aula5pc4.ieslapaloma.com
aula5pc4.ieslapaloma.com has address 192.168.0.104
root@cnice-desktop:/etc/bind# host 192.168.0.112
112.0.168.192.in-addr.arpa domain name pointer dns.ieslapaloma.com.
112.0.168.192.in-addr.arpa domain name pointer mail.ieslapaloma.com.
root@cnice-desktop:/etc/bind# █
```

**DNS funcionando correctamente**

## Configuración DNS esclavo

Si deseamos configurar nuestro servidor DNS para que actúe como esclavo de un servidor DNS maestro, la configuración es mucho más sencilla que en el caso anterior ya que únicamente será necesario indicar en el DNS esclavo quién es el servidor DNS maestro, y en el DNS maestro, la IP del DNS esclavo.

Ejemplo, supongamos que el nombre del DNS maestro es `dns.ieslapaloma.com` (IP 192.168.0.112) y que el nombre del DNS esclavo es `dns2.ieslapaloma.com`. En el archivo `'ieslapaloma.db'` de zona de búsqueda directa añadiremos la línea del segundo dns justo debajo de donde está la del primero:

```
// Añadir línea en /etc/bind/ieslapaloma.db del maestro

....
      IN      NS      dns.ieslapaloma.com.
      IN      NS      dns2.ieslapaloma.com. // Nueva línea
....
```

de esta forma indicaremos que existen más servidores DNS para dicha zona. Lo mismo haremos en el archivo '192.rev' de la zona inversa:

```
// Añadir línea en /etc/bind/192.rev del maestro

....
      IN      NS      dns.ieslapaloma.com.
      IN      NS      dns2.ieslapaloma.com. // Nueva línea
....
```

En el archivo /etc/bind/named.conf.local del servidor DNS esclavo debemos indicar que se trata de un servidor esclavo y también debemos indicar quién es el maestro:

```
// Añadir en /etc/bind/named.conf.local del esclavo
zone "ieslapaloma.com" {
    type slave;
    file "/etc/bind/ieslapaloma.db";
    masters { 192.168.0.112; };
};

zone "0.168.192.in-addr.arpa" {
    type slave;
    file "/etc/bind/192.rev";
    masters { 192.168.0.112; };
};
```

En el archivo /etc/bind/named.conf.local del servidor DNS maestro podemos utilizar also-notify para mantener los DNS sincronizados. Con also-notify pasamos los cambios de zonas en el maestro al esclavo:

```
// Archivo /etc/bind/named.conf.local del maestro
zone "ieslapaloma.com" {
    type master;
    file "/etc/bind/ieslapaloma.db";
    also-notify {ip_del_esclavo;}
};

zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/192.rev";
    also-notify {ip_del_esclavo;}
};
```

De ésta forma dispondremos en la red de un servidor DNS esclavo que podrá satisfacer las peticiones DNS al igual que lo haría el maestro. Es interesante si el número de peticiones es muy elevado y se requiere distribuir la carga entre los dos servidores, o si

deseamos disponer de servicio DNS de alta disponibilidad de forma que aunque el servidor maestro deje de funcionar, el servidor esclavo podrá seguir ofreciendo el servicio.

Cada vez que hagamos un cambio en los archivos `/etc/bind/ieslapaloma.db` y `/etc/bind/192.rev` del maestro, debemos acordarnos de actualizar el parámetro serial (incrementar en una unidad) para que los dns dependientes del maestro sepan que ha cambiado y actualicen su información para mantenerse perfectamente sincronizados.

## Arranque y parada manual del servidor DNS

El servidor DNS, al igual que todos los servicios en Debian, dispone de un script de arranque y parada en la carpeta `/etc/init.d`.

```
// Arranque del servidor DNS
```

```
# /etc/init.d/bind9 start
```

```
// Parada del servidor DNS
```

```
# /etc/init.d/bind9 stop
```

```
// Reinicio del servidor DNS
```

```
# /etc/init.d/bind9 restart
```

## Arranque automático del servidor DNS al iniciar el sistema.

Para un arranque automático del servicio al iniciar el servidor, debemos crear los enlaces simbólicos correspondientes tal y como se indica en el apartado [Arranque automático de servicios al iniciar el sistema](#).