



# Ciclo Formativo: Desarrollo de Aplicaciones Web

## DESPLIEGUE DE APLICACIONES WEB

TEMA 3 – Servicio de nombres de dominio (DNS)

*Bind9* sobre Ubuntu 16

Marcos Alcañiz

## Contenido

1.	Servidores DNS.....	2
1.1.	Servidor DNS Maestro.....	4
1.2.	Servidor DNS Esclavo.....	4
1.3.	Servidor DNS Caché.....	5
2.	Instalación y configuración con Bind9.....	6
2.1.	Servidor DNS Maestro de traducción directa.....	7
2.2.	Servidor DNS Maestro de traducción inversa .....	10
2.3.	Servidor DNS Esclavo.....	12

## TEMA 3

# Servicio de nombres de dominio (DNS)

Instalaremos y configuraremos un servidor DNS (*Bind9*) en nuestro servidor virtual. A continuación, instalaremos en alguno de nuestros clientes virtuales otro servidor en modo esclavo.

### 1. Servidores DNS

Cuando desde un navegador escribimos la URL de una página web, obviamente nuestro PC no puede conocer las URL's de todas las páginas del mundo. Necesita que algún otro le traduzca cada URL por la dirección IP pública correspondiente.

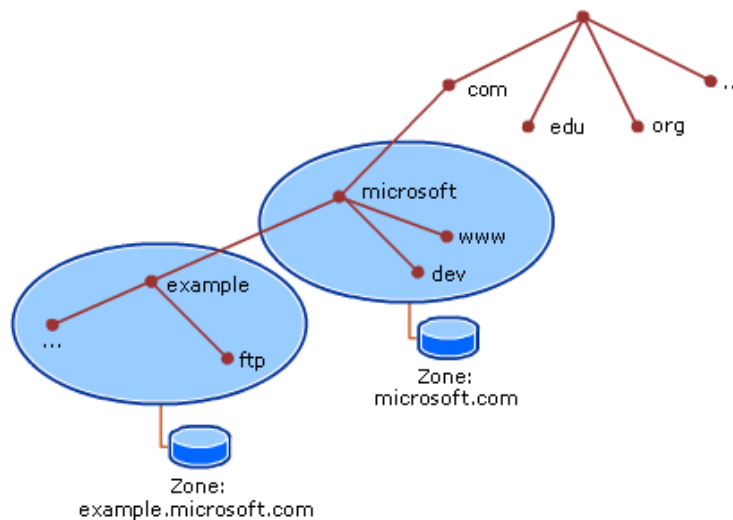
Existen servidores DNS públicos, como los de *Google* (8.8.8.8 y 8.8.4.4, con soporte para IPv6), los de *Level 3* (209.244.0.3 y 209.244.0.4), los de *OpenDNS* de CISCO (208.67.222.222 y 208.67.220.220)... y un largo etcétera. Por otra parte, nuestros proveedores de internet también suelen ofrecernos sus propios servidores DNS.

Y, por supuesto, nosotros mismos podemos instalar y configurar nuestros propios servidores DNS locales. Esto se usa en empresas generalmente para acceder a páginas web internas (*intranets*) y gestionar otros servicios locales.

**NOTA:** *Técnicamente un navegador debería ser capaz de mostrar páginas web sin ningún servidor DNS, siempre y cuando accedamos a las páginas web a través de sus direcciones IP, en vez de por sus URL. Sin embargo, en la práctica esto no suele ser cierto: resulta que a la hora de programar páginas y aplicaciones web, hoy en día todos los programadores utilizamos muy a menudo URL's y nombres de máquinas dentro de nuestros códigos.*

En las primeras versiones de servidores DNS, únicamente disponían de un listado de traducciones enorme donde se introducían todas las URL's con sus respectivas direcciones IP.

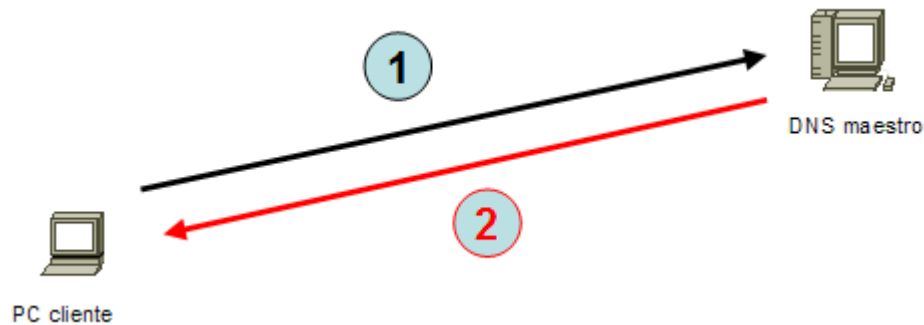
Sin embargo, hoy en día todos los servidores DNS nos dan la opción de organizar las líneas de traducciones en **zonas**. Esto nos permite mantener las traducciones repartidas por (típicamente) dominios y/o subdominios, pudiendo de esta manera personalizar la configuración de cada uno de estos dominios.



Un servidor DNS puede trabajar, en general, de tres formas diferentes: como servidor **maestro**, como servidor **esclavo** y como servidor **caché**.

### 1.1. Servidor DNS Maestro

Esta es la configuración por defecto de cualquier servidor DNS. Básicamente el servidor se ocupa personalmente de atender todas las peticiones de traducción.

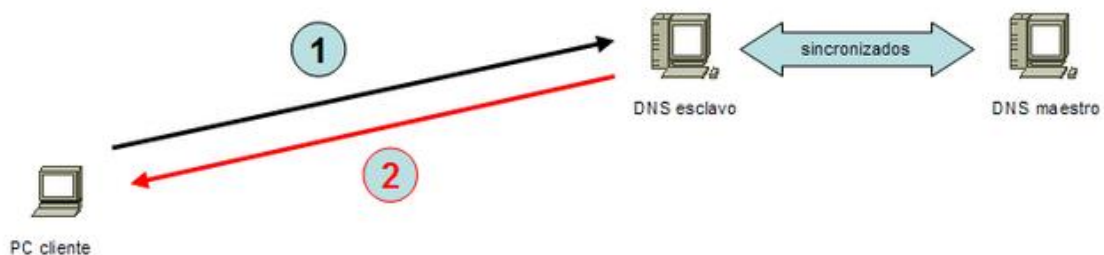


1. El cliente envía al servidor maestro la petición de traducción.
2. El servidor maestro responde con la traducción.

### 1.2. Servidor DNS Esclavo

Con esta configuración, el servidor se encuentra continuamente sincronizado con un servidor DNS maestro. Las peticiones de traducción que lleguen al esclavo, las atiende el esclavo. Las peticiones que lleguen al maestro, las atiende el maestro.

De esta manera, aligeramos el trabajo del servidor maestro. Además, si el servidor esclavo se encuentra físicamente más cerca de nuestra máquina (o incluso en la misma red local), puede aumentar considerablemente la carga de páginas web.



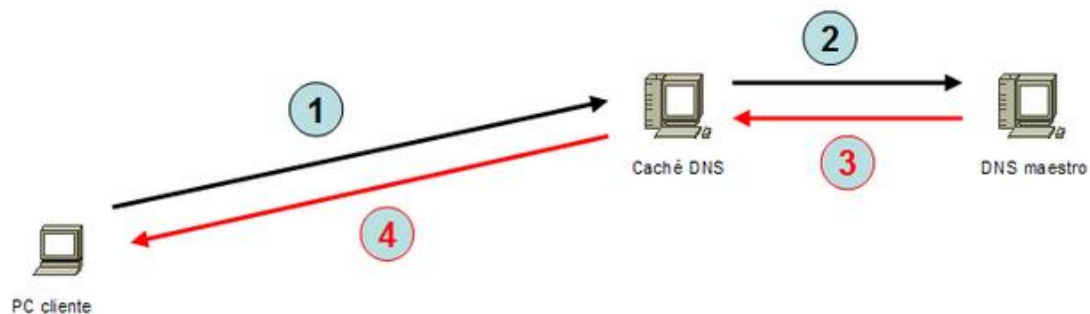
1. El cliente envía al servidor esclavo la petición de traducción.
  2. Es este servidor esclavo el que responde con la traducción.
- \* Cualquier modificación que se realice en los listados del servidor DNS maestro se extenderá a los listados del servidor DNS esclavo.

### 1.3. Servidor DNS Caché

Si configuramos un servidor como caché, éste atenderá las peticiones de traducción como si fuera un servidor DNS normal y corriente. Sin embargo, en realidad transmitirá todas las peticiones a un servidor DNS maestro. Eso sí: una vez haya transmitido una traducción, guardará esta en memoria, de modo que cuando vuelva a recibir otra petición de esa misma traducción, podrá realizarla él mismo sin necesidad de consultar al DNS maestro.

Básicamente podríamos decir que se trata de un DNS esclavo que sólo sincroniza las entradas de la lista de traducciones que se le solicitan.

Prácticamente todos los routers actuales proporcionados por los proveedores de internet vienen por defecto con esta configuración de DNS caché.



1. El cliente envía al servidor caché la petición de traducción.
  2. El servidor caché retransmite la petición al DNS maestro.
  3. El servidor maestro proporciona la traducción al DNS caché.
  4. Es el DNS caché quien finalmente responde al cliente. Además, ha guardado en memoria el resultado de la traducción.
- 
1. Otro cliente envía al servidor caché una petición de la traducción anterior.
  4. Ahora el servidor caché es capaz de resolver la traducción, por lo que responde al cliente sin tener que consultar al DNS maestro.

## 2. Instalación y configuración con Bind9

Utilizaremos la aplicación *Bind9* para instalar un servidor DNS en nuestro *Ubuntu Server* virtual. Podemos instalarlo directamente utilizando los repositorios:

```
~$ apt install bind9
```

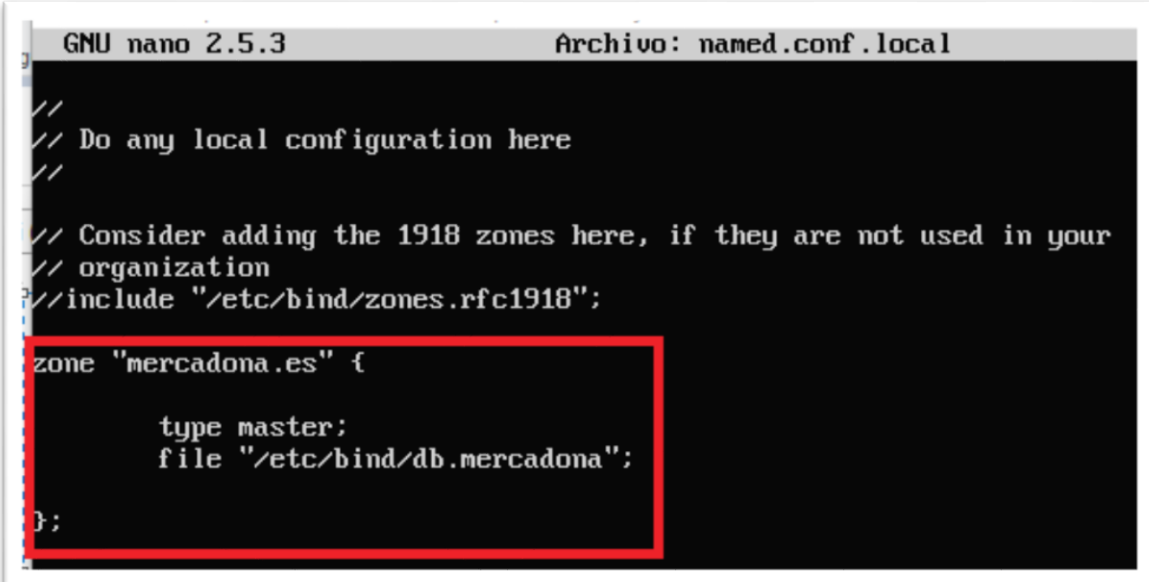
Una vez instalado, podemos acceder a sus archivos de configuración en el directorio */etc/bind*.

- ***named.conf.options***: Archivo de configuración global de *Bind9*.
- ***named.conf.local***: En este archivo declararemos y configuraremos las zonas que va a usar nuestro servidor DNS.
- ***named.conf.default-zones***: Declaradas y configuradas las zonas que ya vienen creadas por defecto.
- ***named.conf***: Este archivo reúne los tres anteriores (es el que realmente utiliza la aplicación).
- ***db.\****: Cada archivo con este nombre (aunque en realidad podemos ponerles el nombre que nos dé la gana) contendrá el listado de traducciones de una de las zonas declaradas en *named.conf.local*. Se recomienda que el nombre del archivo esté relacionado con el dominio o subdominio de la zona a la que pertenece.

**NOTA:** Podemos comprobar si nuestros archivos de configuración y de zonas tienen algún error de sintaxis con los comandos ***named-checkconf*** y ***named-checkzone*** respectivamente. Un error de sintaxis generará un error al intentar poner en marcha el servicio de *Bind9*.

## 2.1. Servidor DNS Maestro de traducción directa

En primer lugar, deberemos crear la zona que cubrirá el dominio de las traducciones que queremos añadir a nuestro servidor. Editamos el archivo ***named.conf.local***, indicándole el nombre del dominio o subdominio, la ruta del archivo donde se encontrará su listado de traducciones, y el tipo de servidor (master, esclavo o caché):



```
GNU nano 2.5.3 Archivo: named.conf.local

//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "mercadona.es" {
    type master;
    file "/etc/bind/db.mercadona";
};
```

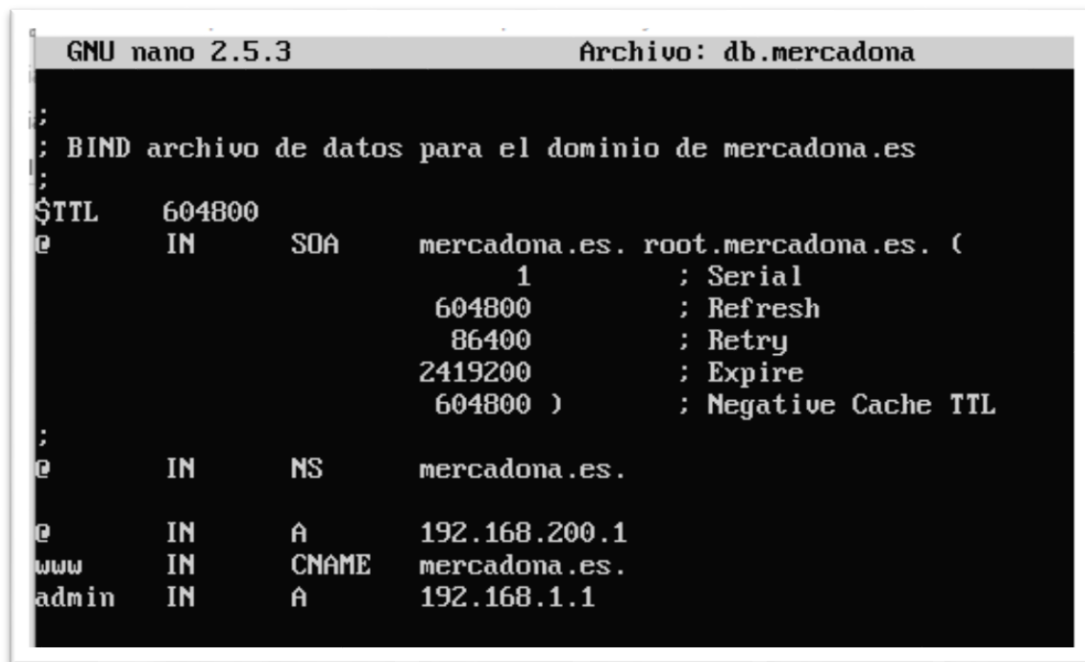
**NOTA:** Cada vez que modifiquemos alguna de las configuraciones, deberemos reiniciar el servidor DNS para que los cambios surtan efecto. Podemos reiniciarlo desde el comando ejecutable de Bind9, o directamente desde el propio servicio:

```
~$ /etc/init.d/bind9 restart
```

```
~$ service bind9 restart
```



A continuación deberemos crear el archivo **db.\***, y rellenarlo con el listado de traducciones que deseemos asignarle al dominio de esa zona. Aconsejo realizar una copia de un archivo de zona que ya exista, por ejemplo de *db.local*, cambiarle el nombre y reutilizarlo:



```
GNU nano 2.5.3 Archivo: db.mercadona
;
; BIND archivo de datos para el dominio de mercadona.es
;
$TTL      604800
@         IN      SOA      mercadona.es. root.mercadona.es. (
                        1          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
@         IN      NS       mercadona.es.
@         IN      A        192.168.200.1
www       IN      CNAME    mercadona.es.
admin     IN      A        192.168.1.1
```

El símbolo **arroba (@)** en estos archivos siempre hace referencia al nombre de dominio (en este caso, @ = [mercadona.es](mailto:root@mercadona.es)).

La primera línea **SOA (Start of Authority)** indica que se trata de un servidor maestro. Contiene el **nombre** del servidor (*mercadona.es*) y el **correo** del administrador (cambiando el primer punto por la *arroba*, siendo por tanto *root@mercadona.es*). Además, engloba varias opciones que afectan precisamente a su interacción con posibles servidores esclavos:

- **Serial:** Este número se utiliza simplemente para indicar que se ha modificado el listado de traducciones. Cada vez que cambiemos manualmente este número, el servidor informará a todos sus esclavos de las modificaciones (*¡Cuidado! Si no modificamos este serial, los esclavos no se enterarán de las modificaciones*). Por regla general suele ponerse la fecha de cada cambio en formato AAAAMMDD seguido de un contador.
- **Refresh:** Número de segundos tras los que se actualizarán automáticamente los servidores esclavos.
- **Retry:** Número de segundos que debe esperar un servidor esclavo tras un fallo de actualización.
- **Expire:** Número de segundos que tardarán en expirar las traducciones mantenidas por un servidor esclavo.
- **Negative Cache TTL:** Equivalente al anterior, pero para servidores caché.

A continuación, con **NS (Name Server)** indicamos los servidores de nombres principales de este dominio (en este caso, sólo hay uno y además es él mismo). También podemos indicar con **MX (Mail eXchange)** si tenemos algún servidor que se ocupe exclusivamente de procesar los correos electrónicos del dominio (no es el caso).

A partir de aquí, pasaríamos a listar todas las traducciones que queramos que resuelva nuestro servidor DNS para este dominio en cuestión.

Con **A (Address)** indicamos que es una traducción típica de URL a dirección IP. En este caso, hemos indicado que la URL [mercadona.es](http://mercadona.es) se debe traducir como `192.168.200.1`, y que la URL [admin.mercadona.es](http://admin.mercadona.es) se debe traducir como `192.168.1.1`.

Con **CNAME (Canonical Name)** indicamos que se trata de un alias que se asigna a otro nombre de dominio. En este caso, hemos indicado que la URL [www.mercadona.es](http://www.mercadona.es) en realidad se trata de la URL [mercadona.es](http://mercadona.es) (que a su vez posee su propia traducción a la IP `192.168.200.1`, como hemos indicado anteriormente).

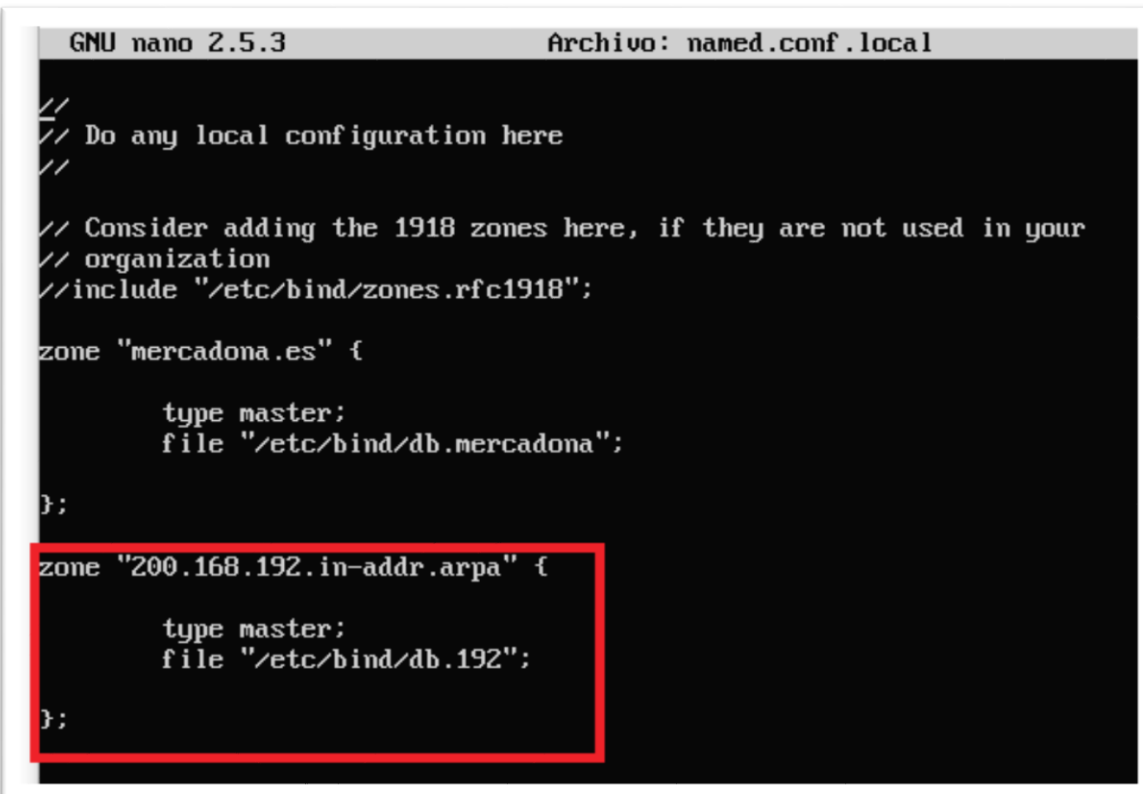
Existen otros tipos de entradas, pero estas dos son las más típicas y utilizadas. Consulta el manual de la aplicación para conocer todas las opciones que nos ofrece *Bind9*.

**NOTA:** Podemos comprobar si nuestro servidor DNS realmente funciona configurando cualquier otra máquina, poniéndole como DNS la dirección de nuestro servidor e intentando navegar en los dominios añadidos en sus listados de traducciones. También podemos usar los comandos **dig** (**-x** para las traducciones inversas), **host** o **nslookup**.

## 2.2. Servidor DNS Maestro de traducción inversa

Un servidor de traducción inversa es aquel que traduce direcciones IP a nombres de máquinas (y no al contrario, como hasta ahora). La configuración es básicamente la misma, con alguna pequeña excepción.

En primer lugar, deberemos crear en ***named.conf.local*** una nueva zona para las traducciones inversas para, por ejemplo, las IP's dentro de *192.168.200.0*:



```
GNU nano 2.5.3                Archivo: named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "mercadona.es" {
    type master;
    file "/etc/bind/db.mercadona";
};

zone "200.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
};
```

A continuación creamos el archivo **db.192** a partir de, por ejemplo, el archivo **db.127**:

```
; BIND fichero de traducciones inversas para el dominio mercadona.es
;
$TTL      604800
@         IN      SOA      mercadona.es. root.mercadona.es. (
                        1      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       mercadona.es.
1         IN      PTR      mercadona.es.
166       IN      PTR      inventor.mercadona.es
```

Ahora, con **PTR (PoinTer Record)** indicamos una traducción inversa típica de dirección IP a nombre de máquina. En este caso, hemos indicado que la IP 192.168.200.1 debe traducirse como [mercadona.es](http://mercadona.es), y que la IP 192.168.200.166 debe traducirse como [inventor.mercadona.es](http://inventor.mercadona.es) (hay que puntualizar que éste último nombre no tiene en realidad la traducción directa a esa IP... pero bueno, siempre podríamos volver al archivo de las traducciones directas y añadirlo).

**¡Cuidado!** Tanto en la declaración de las zonas inversas como en sus listados de traducciones, las direcciones IP's deben indicarse al revés.

Por ejemplo, si hubiéramos querido crear una zona para traducir todas las IP's que comiencen por "192", habríamos llamado a la zona "192.in-addr.arpa" y con una entrada de traducción tal que "50.100.168" nos estaríamos refiriendo realmente a la dirección "192.168.100.50".

### 2.3. Servidor DNS Esclavo

Para probar la configuración de un servidor DNS esclavo, instalamos *Bind9* en una tercera máquina y lo enlazaremos con nuestro servidor maestro anterior.

En primer lugar, al servidor maestro deberemos indicarle que permita transmitir su listado de producción al nuevo servidor esclavo. Y por otra parte, deberemos añadir al listado de las traducciones el nombre del nuevo DNS esclavo.

Por tanto, modificamos la **zona** correspondiente en el archivo ***named.conf.local*** del servidor maestro:

```
GNU nano 2.5.3 Archivo: named.conf.local

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "mercadona.es" {
    type master;
    file "/etc/bind/db.mercadona";
    also-notify {192.168.200.3:};
};
```

De esta manera, permitimos que nuestro servidor maestro se sincronice con el servidor esclavo *192.168.200.3*. Aquí podemos añadir tantos servidores esclavos como dispongamos.

Y a continuación, en el archivo de entradas de traducción correspondiente (***db.mercadona***) del servidor maestro añadiremos el nombre del nuevo servidor esclavo y su correspondiente traducción:

```
GNU nano 2.5.3 Archivo: db.mercadona

; BIND archivos de datos para el dominio de mercadona.es
$TTL      604800
@         IN      SOA      mercadona.es. root.es.mercadona. (
                        2      ; Serial
                        604800  ; Refresh
                        86400   ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;

@         IN      NS       mercadona.es
@         IN      NS       esclavo.mercadona.es.
@         IN      A        192.168.200.1
www       IN      CNAME    mercadona.es
admin     IN      A        192.168.1.1
esclavo   IN      A        192.168.200.3
```

Con esto, ya tendríamos el servidor DNS maestro preparado para sincronizarse con el servidor DNS esclavo.

Ahora es cuando deberíamos ir a la máquina `192.168.200.3` e instalar de nuevo `Bind9`. La configuración, sin embargo, va a ser mucho más sencilla que la del maestro: únicamente tendremos que crear una zona en **`named.conf.local`** con el nombre del dominio en cuestión, indicándole la dirección del servidor DNS maestro que queramos asignarle, y ya está:



```
GNU nano 2.5.3      Archivo: named.conf.local

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "mercadona.es" {
    type slave;
    file "/etc/bind/db.mercadona";
    masters {192.168.200.1;};
};
```

Indicamos a la zona que se trata de un **servidor esclavo (*slave*)**, la **ruta del archivo de traducciones del servidor maestro** (*¡Este archivo no debemos crearlo en el esclavo! Durante la sincronización con el maestro, Bind9 lo creará automáticamente*), y los **maestros** con los que debe sincronizarse.