Servicio DNS

IES Polígono Sur
Despliegue de Aplicaciones Web
CFGS DESARROLLO DE APLICACIONES WEB

El servicio DNS

En una **red TCP/IP**, las máquinas se identifican mediante su **dirección de red** o número IP.

Para las personas resulta más sencillo recordar un nombre que se asocia a una máquina concreta.

También es más fiable, ya que la dirección IP puede cambiar, pero no así el nombre.

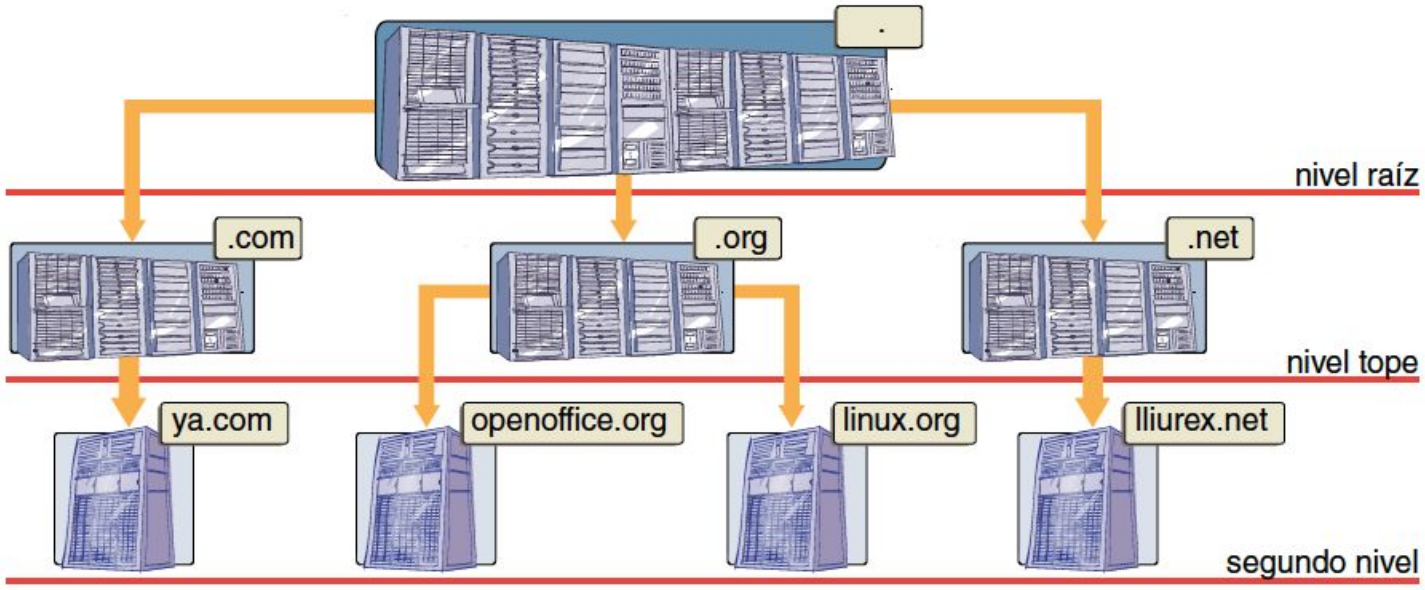
Es necesario un mecanismo que traduzca los nombres de las máquinas a direcciones IP.

El servicio DNS permite que esta tarea se lleve a cabo.

El servicio DNS

El servicio DNS se compone de una base de datos distribuida (integrada por varias máquinas conectadas en red) en la que se almacenan las asociaciones de nombres de dominios y direcciones IP.

Esta base de datos está clasificada por nombres de dominio, donde cada uno puede considerarse una rama en un árbol invertido llamado **espacio de nombres de dominio.**



El servicio DNS

El nivel superior o primer nivel **(TLD)** está formado por los dominios que descienden directamente del dominio raíz.

Los principales TLD genéricos son:

TLD	Descripción
com	Agrupa organizaciones comerciales. Ejemplos: google.com, yahoo.com, strands.com.
edu	Reúne organizaciones educativas universitarias. Ejemplos: eada.edu, ortegaygasset.edu, mit.edu.
net	Agrupa organizaciones dedicadas a Internet y a las telecomunicaciones. Ejemplos: rpmfind.net, listas.net, php.net.
org	Reúne organizaciones no comerciales. Ejemplos: linuxdoc.org, ubuntu.org, linux.org, insflug.org.
gov	Agrupa organizaciones gubernamentales de EEUU. Ejemplos: nasa.gov, nsf.gov, whitehouse.gov.
int	Se usa en organizaciones internacionales. Ejemplos: redcross.int, interpol.int, coe.int
name	Se emplea para nombres de personas.
mobi	Es propio de empresas de telefonía móvil o servicios para móvil.

Puede ocurrir que los dominios geográficos de primer nivel contengan a su vez alguno de los dominios genéricos. Estos dominios serían de segundo nivel (com.es, edu.au, org.uk, teso.org.es, etcétera.).

Delegación de dominios

DNS es una base de datos distribuida y permite su **administración descentralizada** mediante la **delegación de dominios**.

El dominio puede ser dividido en **subdominios** por el administrador y delegar el control de cada uno.

La autoridad que se hace cargo de la delegación debe asumir también la responsabilidad de mantener **actualizados** los registros de recursos de ese subdominio.

Pero delegación no significa independencia, sino **coordinación**. **La división de un dominio en subdominios no implica siempre una cesión de autoridad.**

Dominios y zonas

El servidor de nombres almacena información acerca de algunas partes o **zonas** del espacio de nombres de dominio.

Se dice que el servidor de nombres tiene **autoridad** sobre la zona.

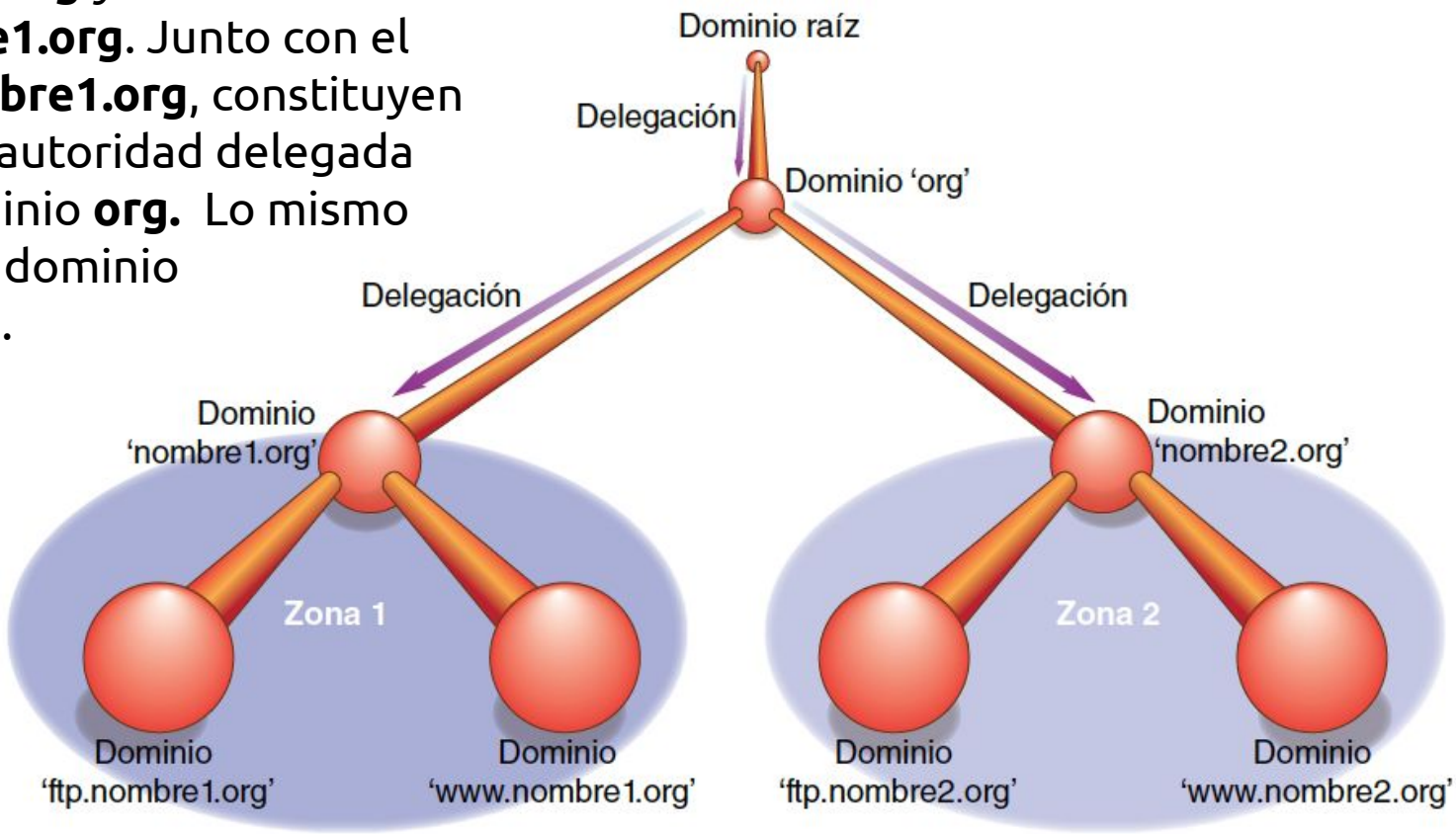
Por lo tanto, un servidor de nombres podrá tener autoridad sobre varias zonas.

La zona es un **archivo** que contiene determinados **registros** de la base de datos del espacio de nombres de dominio, que identifican a uno o más dominios.

La generación de zonas se hace mediante la **delegación de autoridad**.

Dominios y zonas

En la figura se observa que el dominio **nombre1.org** contiene a su vez los dominios **ftp.nombre1.org** y **www.nombre1.org**. Junto con el dominio **nombre1.org**, constituyen la **zona1** con autoridad delegada desde el dominio **org.** Lo mismo ocurre con el dominio **nombre2.org**.

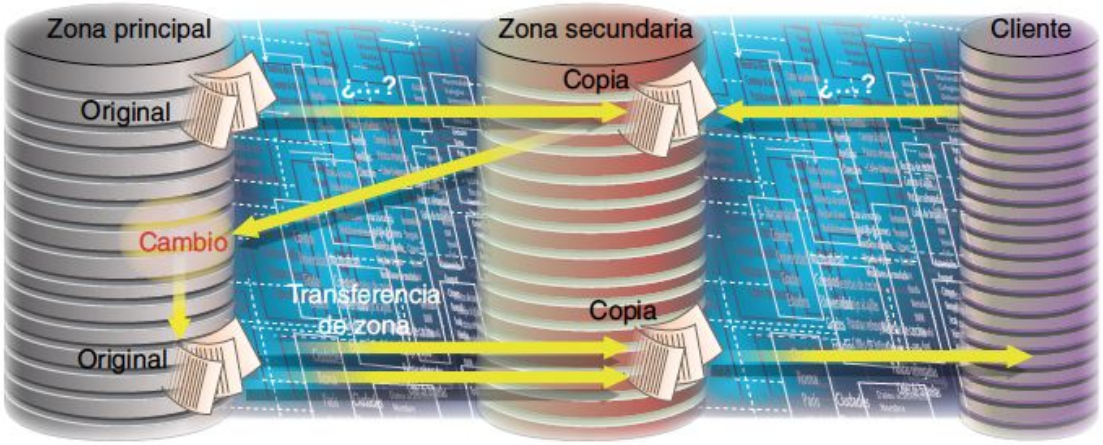


Dominios y zonas

Los servidores de nombres se pueden clasificar en los tipos siguientes:

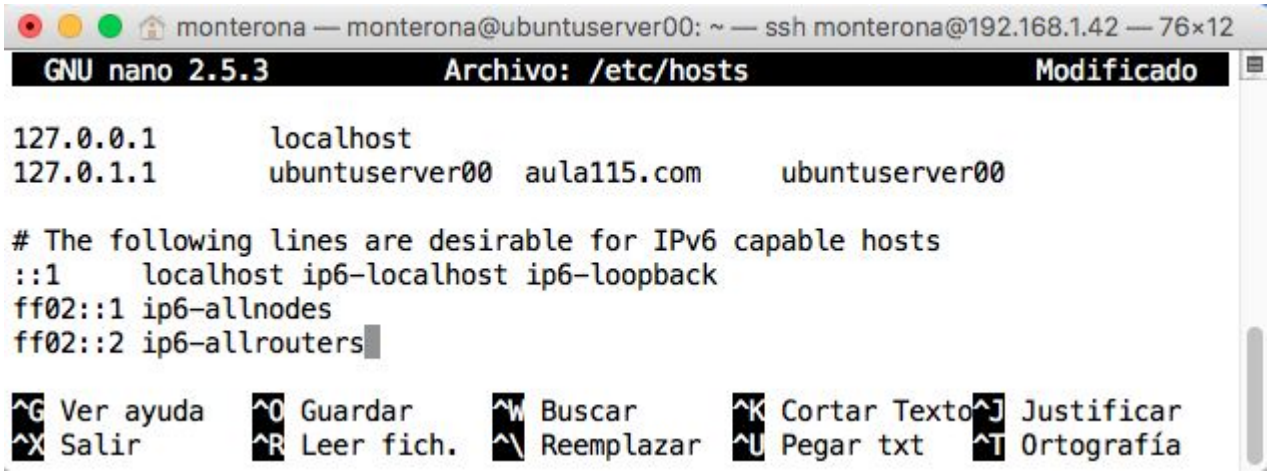
1. **Servidor primario (maestro):** en él se llevan a cabo todas las modificaciones sobre una zona.
2. **Servidor secundario (esclavo):** contiene una copia de solo lectura de los archivos de zona.
3. **Servidor caché:** No contiene ningún tipo de información acerca de la zona y se utiliza para acelerar las consultas.

La información de las zonas se obtiene a través de la red mediante la **transferencia de zona.**



Configuración cliente GNU/Linux

/etc/hosts

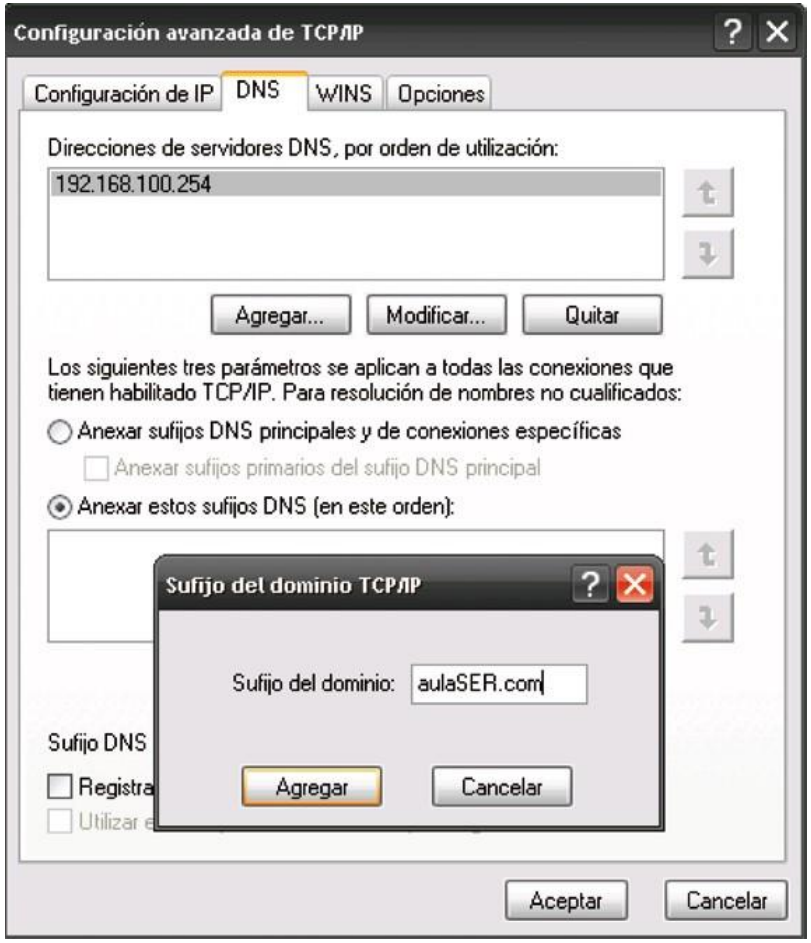


/etc/resolv.conf (implementar en interfaces)

/etc/hostname (Ej: $cat /etc/hostname -> ubuntuserver00

Configuración cliente Windows

En Windows se configura editando las propiedades de la conexión de área local:



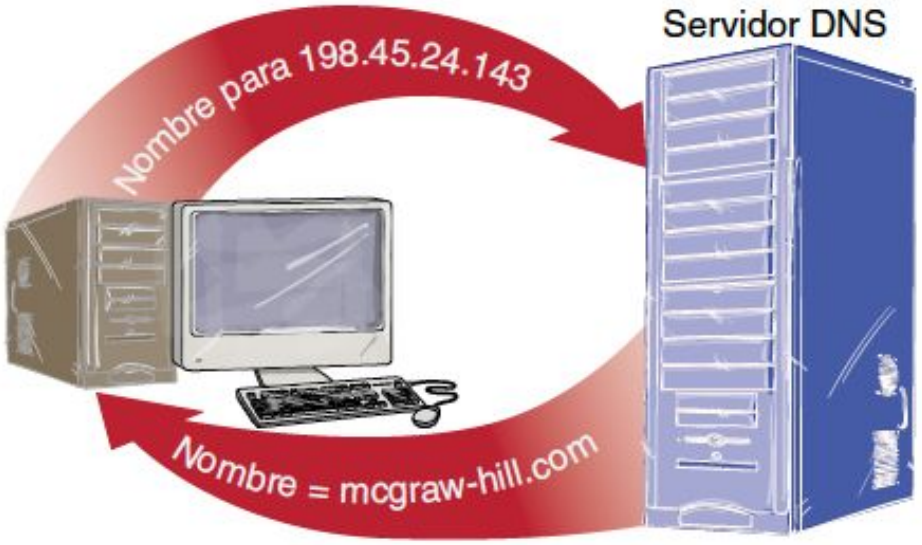
Principales tipos de registros de recursos

Nombre de recurso	Tipo de registro	Función
Inicio de autoridad	**SOA**	Identifica al servidor autoritario de una zona y sus parámetros de configuración.
Servidor de nombres	**NS**	Identifica servidores de nombres autorizados para una zona.
Dirección	**A**	Asocia un nombre de dominio FQDN con una dirección IP.
Puntero	**PTR**	Asigna una dirección IP a un nombre de dominio completamente cualificado. Para las búsquedas inversas.
Registro de correo	**MX**	Indica máquinas encargadas de la entrega y recepción de correo en el dominio.
Nombre canónico	**CNAME**	Permite asignar uno o más nombres a una máquina.
Text	**TXT**	Almacena cualquier información.
Servicio	**SRV**	Ubicación de los servidores para un servicio.

Resolución inversa

De la misma forma que los nombres de dominio se resuelven efectuando consultas para cada componente de **derecha a izquierda**, las direcciones IP siguen el mismo esquema.

Su dominio raíz se denomina **in-addr.arpa**.



Servidores de dominio: BIND

Existen varias aplicaciones de servicios para servidores de nombres de dominio. La más utilizada es **Bind** (www.isc.org/products/ BIND/), disponible bajo licencia BSD.

La ejecución de un servidor DNS (utilizando **Bind9**) en una máquina implica la ejecución en el sistema del proceso **named**, cuyo archivo de configuración es **`/etc/bind/named.conf`**.

Bind9 en GNU/Linux

Para realizar la instalación de Bind9 en GNU/Linux:

```
#apt install bind9 bind9-utils
```

En el directorio /etc/bind/ se encuentra named.conf y el resto de archivos de configuración.

El archivo named.conf no se suele modificar. Las zonas específicas del servidor DNS que se configuran se definen en /etc/bind/**named.conf.local** y se incluyen al final de este archivo con un ***include***.

Para lanzar el servicio debemos ejecutar la orden siguiente:

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

named.conf

La primera línea del archivo es una declaración ***include*** en la que se integra el archivo **named.conf.options**, donde se encuentran las opciones globales del servidor.

La última línea del archivo es otra declaración ***include***, del archivo **named.conf.local**, donde se definen las **zonas locales**.

Las principales sentencias de **named.conf.options**:

acl: define listas de direcciones IP para permitir o denegar el acceso al servidor de nombres.

options: controla las opciones de configuración del servidor y de otras sentencias. Sólo debe aparecer una vez en el archivo de configuración.

named.conf

Las principales **sentencias** del archivo named.conf son:

- **zone:** permite definir las zonas y describir sus configuraciones. Existen cuatro tipos:

1. **Zona maestra (master zone):** alberga la copia principal de los datos de la zona.
2. **Zona esclava (slave zone):** contiene datos que se obtienen como resultado de la duplicación de la información de una zona maestra.
3. **Zona oculta (hint zone):** cuando se hacen peticiones a una zona que no se conoce, ésta ofrece información relativa a los servidores de la raíz.
4. **Zona de reenvío (forward zone):** indica al servidor de nombres que redirija las peticiones de información sobre la zona hacia otros servidores.

- **include:** sentencia que se utiliza para incluir los archivos que contienen las opciones y las zonas locales.

```
include “/etc/bind/named.conf.local”;
```

named.conf

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 **named.conf**: Archivo principal de configuración

Archivo **named.conf.options**: Opciones genéricas

Archivo **named.conf.local**: Especificación particular de este servidor DNS

Archivo **db.127**: Especificación dirección de retorno

Archivo **db.root**: DNSs de nivel superior

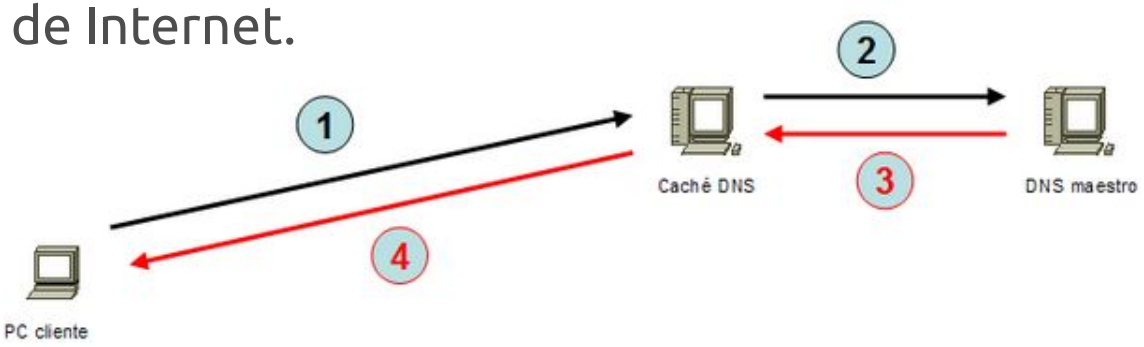
Otros archivos: db.0, db.255, db.empty, db.local, rndc.conf, rndc.key, zones.rfc1918

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.



Configurar servidor caché DNS

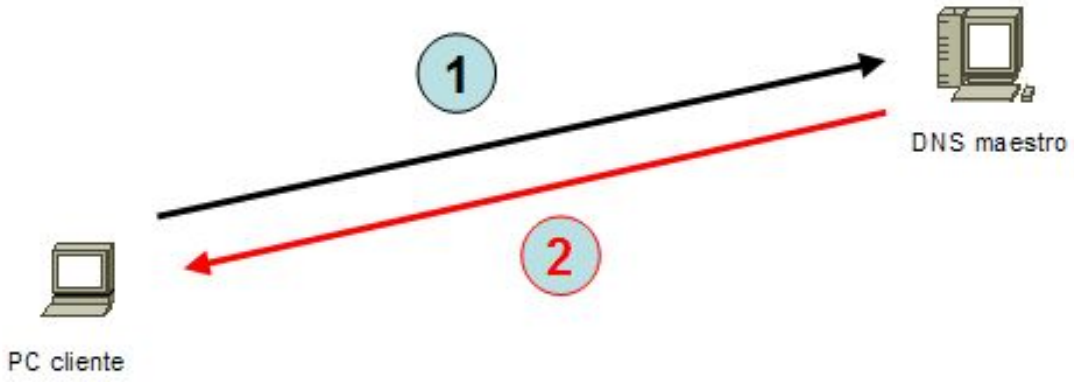
Por defecto, al instalar el paquete bind está preconfigurado como servidor caché DNS. Tan solo será necesario editar el archivo **/etc/bind/named.conf.options** y en la sección forwarders añadir las IPs de dos servidores DNS donde redirigir las peticiones DNS:

```
// 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;
};
};
```

Configurar 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.



Configurar servidor DNS maestro

Se debe 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 "iespoligonosur.org" {
type master;
file "/etc/bind/iespoligonosur.db";
};
// Archivo para búsquedas inversas
zone "XXX.168.192.in-addr.arpa" {
type master;
file "/etc/bind/192.rev";
};
```

Hay que crear los archivos **iespoligonosur.db** y **192.rev** que especificarán la asociación entre nombres y direcciones IP de nuestra red en un sentido y en otro respectivamente.

Configurar servidor DNS maestro

```
// Archivo /etc/bind/aula129.iespoligonosur.db
;
; BIND data file for aula129.iespoligonosur.org
;
@ IN SOA aula129.iespoligonosur.org. root.iespoligonosur.org. (
1 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Default TTL

IN NS dns.aula129.iespoligonosur.org.
IN MX 10 mail.aula129.iespoligonosur.org.

pc12 IN A 192.168.129.212
pc13 IN A 192.168.129.213
aula5pc3 IN A 192.168.XXX.103
aula5pc4 IN A 192.168.XXX.104
aula5pc5 IN A 192.168.XXX.105
aula5pc6 IN A 192.168.XXX.106
aula5pc7 IN A 192.168.XXX.107
www IN A 192.168.XXX.111
dns IN A 192.168.XXX.112
mail IN A 192.168.XXX.112
```

Configurar servidor DNS maestro

```
// Archivo /etc/bind/192.rev
;
; BIND reverse data file for 192.168.129.0
;
@ IN SOA aula129.iespoligonosur.org. root.iespoligonosur.org. (
1 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Default TTL

IN NS dns.aula129.iespoligonosur.org.

101 IN PTR equipo5.aula129.iespoligonosur.org.
102 IN PTR aula5pc2.iespoligonosur.org.
103 IN PTR aula5pc3.iespoligonosur.org.
104 IN PTR aula5pc4.iespoligonosur.org.
105 IN PTR aula5pc5.iespoligonosur.org.
106 IN PTR aula5pc6.iespoligonosur.org.
107 IN PTR aula5pc7.iespoligonosur.org.
108 IN PTR www.iespoligonosur.org.
109 IN PTR dns.aula129.iespoligonosur.org.
110 IN PTR mail.iespoligonosur.org.
```

Configurar servidor DNS maestro

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 iespoligonosur.org
```

En el resto de PCs de la red, indicaremos que el servidor DNS es, por ejemplo, la IP 192.168.0.112:

```
// En el resto de PCs de la red indicamos el servidor DNS
// Editar /etc/network/interfaces en los PCs de la red
dns-nameservers 192.168.0.112
```

checkconf y checkzone en Bind9

A partir de Bind9 se incluyen dos herramientas para chequear la sintaxis y semántica de los archivos que describen las zonas y el archivo named.conf. Son:

named-checkzone y **named-checkconf**

Una vez configurado el servicio DNS, si se quiere hacer una comprobación sintáctica del archivo de configuración named.conf, hay que ejecutar como administrador *(root):*

```
$sudo named-checkconf
```

La salida indica los errores que detecta. Si no genera salida, está todo correcto.

En el caso de los archivos de zona, hay que ejecutar:

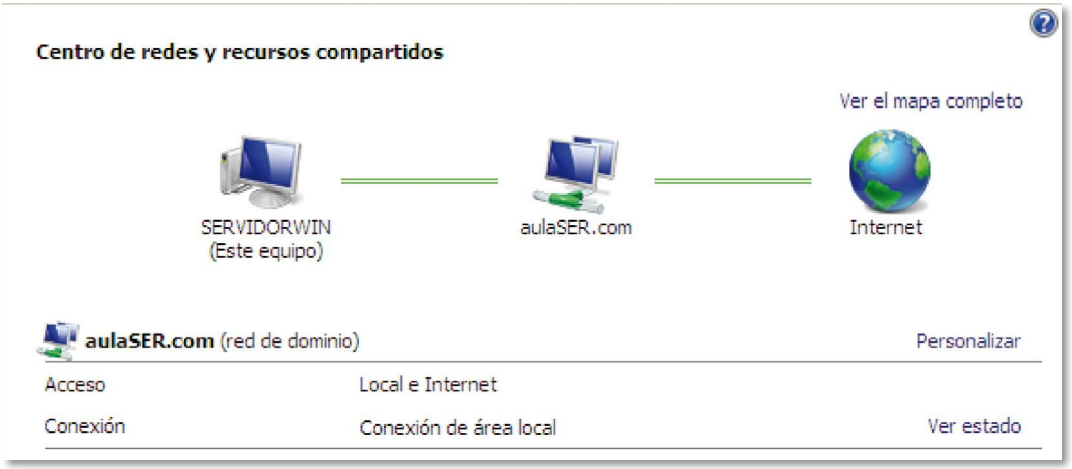
```
$sudo named-checkzone aulaSER.com /etc/bind/db.iespoligonosur.org
```

Servidor DNS en Windows Server 2008

En Windows 2008, el servicio DNS, integrado en Active Directory, realiza las siguientes funciones:

• Resolución de nombres, tanto directa como inversa, siguiendo el esquema de funcionamiento explicado al principio de la unidad.

• Integración de los nombres de dominio asignados por Active Directory y los nombres de dominio de DNS. Ambos siguen la misma estructura jerárquica de nombres, aunque representan dos espacios de nombres distintos, ya que almacenan distinta información. No obstante, las máquinas y dominios DNS son los mismos que los de Active Directory.



Servidor DNS en Windows Server 2008

Una vez instalado el servicio, deberemos supervisar los registros de dirección, así como otras configuraciones DNS. La zona de búsqueda directa tiene el nombre del dominio creado al instalar Active Directory.
A continuación, crearemos la zona de búsqueda inversa en el servidor DNS.
Para comprobar que el servidor DNS funciona, abriremos un navegador web y escribiremos su URL, por ejemplo: \\servidor.aulaSER.com
Entonces ejecutaremos la orden nslookup para ver si, desde el servidor, se resuelven los nombres.