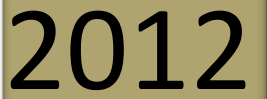




Abril



2012

Puesta en Marcha de un servidor DNS

Puesta en Marcha de un servidor DNS

Gabriel Fernández Díaz

David Morales Sáez

---

## Tabla de contenido

<b>1.- Introducción al DNS .....</b>	<b>3</b>
Funcionamiento .....	4
<b>2.- Configuración de dominios sin utilización de DNS .....</b>	<b>5</b>
/etc/hosts .....	5
/etc/host.conf .....	5
<b>3.- Configuración y puesta en marcha de los servidores DNS de su dominio...</b>	<b>6</b>
Servidor DNS Primario .....	6
DNS Secundario .....	8
Pruebas .....	9

## 1.- Introducción al DNS

Un DNS (Domain Name System) es un conjunto de protocolos y servicios (base de datos distribuida) que permiten a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas. Ésta es ciertamente la función más conocida de los protocolos DNS: la asignación de nombres a direcciones IP. Por ejemplo, si la dirección IP del sitio FTP de redes.es es 200.64.128.4, la mayoría de la gente llega a este equipo especificando redes.es y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

Inicialmente los DNS nacieron de la necesidad de recordar fácilmente los sitios visitados o a visitar y sustituir el antiguo sistema de identificación de "host" en internet que consistía en un gran archivo donde estaban almacenados los nombres y las direcciones **IP** de cada nodo de la red con el cual se podía establecer comunicación

Los servidores de nombres se dividen en cuatro tipos:

1. El servidor primario, que contiene toda la información acerca de un dominio.
2. El servidor secundario, que copia la base de datos del primer servidor.
3. El servidor de sólo caché, que construye una base de datos de DNS exclusivamente para las peticiones a la caché.
4. El servidor silencioso o , que actúa con un servidor normal de tipo primario, pero sin declararse.

La base de datos del DNS tiene una estructura jerárquica. En la cima de la jerarquía está el dominio raíz, etiquetado por el nulo. La información en este dominio reside en un número muy selecto de servidores raíz repartidos por toda Internet. Por debajo del dominio raíz están los dominios de primer nivel, que pueden ser tanto códigos de países como códigos de organizaciones o empresas. A continuación, y por debajo de los dominios de primer nivel, están los dominios de segundo nivel y luego los de tercer nivel, cuarto, etc ...

El nombre de un dominio no es más que un conjunto de etiquetas separadas por puntos que identifica un camino desde la raíz en orden inverso. Cada dominio puede ser administrado por una organización diferente, pudiendo contener hosts y subdominios. Cada organizador puede crear subdominios y repartir responsabilidad de cada uno de sus subdominios en organizaciones diferentes. Los datos asociados a los nombres de dominio se encuentran en los registros de recursos (RR), los cuales deben contar con cinco partes: nombre de dominio, tiempo de vida, tipo, clase y valor.

## Funcionamiento

DNS utiliza un modelo cliente/servidor en el cual los servidores DNS (servidores de nombres) contienen información acerca de la base de datos DNS y la ponen a disposición de los clientes. Cuando un servidor de DNS recibe una petición por parte de un cliente sobre un host que aún no tiene en su caché, lo que hace es preguntar a alguien que lo sepa. Este alguien es un servidor autoritario, un servidor responsable de mantener la información de DNS. Un servidor es autoritario si, cuando se le pregunta acerca de una dirección de su dominio, puede certificar con seguridad que el nombre existe.

Si el servidor contactado no contiene información para ese nombre de dominio pasa la información al servidor autoritario superior en la cadena, formando una serie de preguntas que siguen hasta que la información se encuentra. En la práctica, esto significa que la petición puede ser manejada por un cierto número de servidores y las peticiones suceden a lo largo de todo el día, todos los días en la cambiante Internet. El servidor que originalmente hizo la petición almacenará la información en su caché para satisfacer futuras peticiones sin necesidad de ir a un servidor autoritario. Esta información es configurada por el administrador del servidor DNS para que caduque después de un determinado período de tiempo, para evitar el problema de tener datos antiguos o no válidos.

La traducción en DNS no toma demasiado tiempo, pero se añade al tiempo que tarda nuestra petición en llegar al equipo remoto. Los servidores de nombres DNS resuelven los nombres interpretando la información de la red para encontrar una dirección IP específica. Por ejemplo, el proceso de resolución de [www.google.es](http://www.google.es) puede resumirse en los siguientes pasos:

1. El cliente pasa una pregunta a su servidor de nombres local.
2. El servidor local de nombres envía una solicitud iterativa a uno de los servidores raíz de DNS, pidiéndole que resuelva el nombre de dominio. El servidor raíz devuelve una referencia de los servidores de nombres encargados del dominio DNS es.
3. El servidor local de nombres envía una solicitud iterativa a uno de los servidores especificados en el paso anterior, el cual devuelve una referencia de los servidores de nombres encargados del dominio google.
4. El servidor local de nombres envía una solicitud iterativa a uno de los servidores especificados en el punto anterior.

El proceso anterior es el de una interrogación iterativa, pues los servidores DNS de alto nivel suelen responder de esta forma para que su carga de trabajo no sea elevada. En la interrogación recursiva es el propio servidor DNS el que interroga en busca de la resolución final, que es la que devuelve al cliente. Por su parte, la interrogación iterativa se lleva a cabo hasta que finalmente se responde al cliente con la resolución que éste solicita; hasta entonces recibe las direcciones IP de las máquinas con servidores DNS a las que debe interrogar para obtener la resolución que desee. En el ejemplo, el servidor de nombres del dominio google pasa la parte [www](http://www) del nombre DNS a su servidor local para que la resuelva y, una

vez hecho esto, la dirección empieza a devolverse sobre los servidores anteriores hasta llegar al cliente.

## 2.- Configuración de dominios sin utilización de DNS

Para la configuración de dominios sin utilizar DNS hemos de modificar el archivo `/etc/hosts` y el archivo `/etc/hosts.conf`.

### `/etc/hosts`

La resolución de nombres de dominio se puede realizar modificando el fichero `/etc/hosts`. El formato de cada línea en dicho fichero es:

```
[IP] [Hostname] [Alias]
```

En nuestro caso lo hemos modificado el archivo para apuntar a:

```
127.0.0.1  pasarela.red9.redes.dis.ulpgc.es  pasarela  localhost.localdomain
localhost
172.16.9.51 david.red9.redes.dis.ulpgc.es  david
172.16.9.1  pasarela.red9.redes.dis.ulpgc.es  pasarela  localhost.localdomain
localhost gabriel
```

Para comprobar que los resultados son correctos, hacemos un ping a los alias y los hosts:

```
[root@pasarela ~]# ping david
PING david.red9.redes.dis.ulpgc.es (172.16.9.51) 56(84) bytes of data.
64 bytes from david.red9.redes.dis.ulpgc.es (172.16.9.51) icmp_seq=1 ttl=64
time=0.168 ms
64 bytes from david.red9.redes.dis.ulpgc.es (172.16.9.51) icmp_seq=2 ttl=64
time=0.107 ms
64 bytes from david.red9.redes.dis.ulpgc.es (172.16.9.51) icmp_seq=3 ttl=64
time=0.126 ms
64 bytes from david.red9.redes.dis.ulpgc.es (172.16.9.51) icmp_seq=4 ttl=64
time=0.129 ms
^C
--- david.red9.redes.dis.ulpgc.es ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3606ms
rtt min/avg/max/mdev = 0.107/0.132/0.168/0.024 ms
```

### `/etc/hosts.conf`

En el fichero `/etc/hosts.conf` podemos configurar el orden en que se resuelven los nombres según los servicios usados. En nuestro caso, y generalmente por defecto, se usa primero el archivo hosts mencionado anteriormente y luego los servicios DNS estándar. El contenido del fichero de nuestro ordenador es:

```
order hosts,bind
```

### 3.- Configuración y puesta en marcha de los servidores DNS de su dominio

Los ficheros que hemos tenido que configurar se enumeran, muestran y explican a continuación. Para ello se tratará por separado la configuración realizada en el servidor primario (ubicado en el equipo Pasarela) y la del secundario (ubicado en el equipo PC, situado en la red interna).

#### Servidor DNS Primario

El DNS primario será el que responderá de forma autoritativa para su dominio y contendrá las bases de datos de forma permanente o persistent, es decir, en ficheros. Dichos ficheros requieren inicialmente la configuración del demonio named, que se hará en el fichero /etc/named.conf. Su contenido será la declaración de zonas. Seguidamente se muestra el fichero y a continuación se comenta cada una de las zonas declaradas y su funcionalidad.

```
/etc/named.conf

//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND
named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver
only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration
files.
//

acl red-david {    172.16.9.0/24; };

options {
    listen-on port 53 { 127.0.0.1; };
    directory    "/var/named";
    dump-file     "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file
"/var/named/data/named_mem_stats.txt";
    allow-query   { localhost; };
    recursion yes;
    allow-recursion { localhost; red-david; };

    allow-transfer {172.16.9.51;};

};

zone "." IN {
    type hint;
    file "named.ca";
};
```

```

zone "red9.redes.dis.ulpgc.es" IN {
    type master;
    // DNS primario
    file "db.red9";
};

zone "9.16.172.in-addr.arpa" IN {
    type master;
    // DNS inverso primario
    file "db.172.16.9";
};

include "/etc/named.rfc1912.zones";

```

En primer lugar, en las opciones de named, donde indicamos el lugar donde está el demonio instalado, el fichero de volcado y de estadísticas:

```

directory    "/var/named";
dump-file    "/var/named/data/cache_dump.db";
statistics-file "/var/named/data/named_stats.txt";

```

Habilitamos las respuestas recursivas y sólo permitimos la descarga a nuestros secundarios:

```

recursion yes;
allow-recursion { localhost; red-david; };

```

Después definimos las distintas zonas, como los servidores raíz:

```

zone "." IN {
    type hint;
    file "named.ca";
};

```

el DNS primario:

```

zone "red9.redes.dis.ulpgc.es" IN {
    type master;
    // DNS primario
    file "db.red9";
};

```

y la resolución inversa del DNS Primario:

```

zone "9.16.172.in-addr.arpa" IN {
    type master;
    // DNS inverso primario
    file "db.172.16.9";
};

```

Las zonas que se han definido están configuradas en los ficheros indicados, es decir, la zona red9.redes.dis.ulpgc.es está configurada en el fichero db.red9:

```
$TTL 4h
@ IN SOA pasarela.red9.redes.dis.ulpgc.es. root.red9.redes.dis.ulpgc.es. (
    2012041703 ; Serial formato: yyyymmddn donde n es un número cualquiera
    1d ; Refresh después de 1 día
    1m ; Reintentar después de 1 minuto
    1w ; Expirar después de una semana
    3h ; TTL(Time to Live) mínimo de tres horas
)

      IN      NS      pasarela
      IN      NS      david
pasarela IN      A      127.0.0.1
david    IN      A      172.16.9.51
gabriel  IN      CNAME  pasarela
```

donde definimos los parámetros de refresco, tiempo de vida, el DNS Primario, el DNS Secundario, las IP de ambos DNS y un alias para el DNS Primario. La zona 9.16.172.in-addr.arpa está configurada en el fichero db.172.16.9:

```
$TTL 86500
@ IN SOA pasarela.red9.redes.dis.ulpgc.es. root (
    2012041702 ; Serial formato: yyyymmddn donde n es un número cualquiera
    10800 ; Refresh después de tres horas
    3600 ; Reintentar después de una hora
    604800 ; Expirar después de una semana
    86400 ; TTL(Time to Live) mínimo de un día )

      IN      NS      pasarela.red9.redes.dis.ulpgc.es.
      IN      NS      david.red9.redes.dis.ulpgc.es.
1     IN      PTR     pasarela.red9.redes.dis.ulpgc.es.
51    IN      PTR     david.red9.redes.dis.ulpgc.es.
```

Finalmente, se ha modificado el archivo /etc/hosts, para indicar la dirección del servidor al que hemos de conectarnos.

```
domain redes.dis.ulpgc.es
search redes.dis.ulpgc.es red9.redes.dis.ulpgc.es
nameserver 127.0.0.1
```

## DNS Secundario

Para el servidro DNS secundario situado en nuestro dominio, en el equipo PC, es decir, el que está dentro de la red interna, con la IP 172.16.9.51, tendremos que



tener el demonio named instalado y configurado según el siguiente fichero named.conf:

```
/etc/named.conf

//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
    directory     "/var/named";
    dump-file      "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";

    allow-recursion { 172.16.9.1; 172.16.9.51; };
};

zone "." IN {
    type hint;
    file "named.ca";
};

zone "red9.redes.dis.ulpgc.es" IN {
    type slave;
    file "slaves/db.red9";
    masters { 172.16.9.1; };
};

zone "9.16.172.in-addr.arpa" IN {
    type slave;
    file "slave/db.172.16.9";
    masters { 172.16.9.1; };
};

};
```

donde, las definiciones de zonas han cambiando visiblemente, ya que se ha cambiado el tipo de zona (de tipo master a slave), lo que conlleva un cambio de lugar de los ficheros y se a añadido una nueva línea en cada uno donde se establece quién dispone de los ficheros (el maestro).

## Pruebas

Para comprobar el funcionamiento del DNS, se han hecho una serie de pruebas, buscando a ordenadores internos a la red y a ordenadores externos de la misma. Por ejemplo, si desde el ordenador secundario buscamos al primario con el nslookup:

```
> pasarela
```

obtenemos:

```
Server:      172.16.9.51
Address:     172.16.9.51#53

Name:        pasarela.red9.redes.dis.ulpgc.es
Address:     172.16.9.1
```

y, si buscamos a google:

```
> www.google.es
```

obtenemos:

```
Server:      172.16.9.51
Address:     172.16.9.51#53

Non-authoritative answer:
www.google.es canonical name = www-cctld.l.google.com
Name:        www-cctld.l.google.com
Address:     173.194.34.247
Name:        www-cctld.l.google.com
Address:     173.194.34.248
```

Una vez hechas estas pruebas, hemos hecho otras desde el ordenador principal:

```
> david
```

obtenemos:

```
Server:      127.0.0.1
Address:     127.0.0.1#53

Name:        david.red9.redes.dis.ulpgc.es
Address:     172.16.9.51
```

y, si buscamos a la nasa:

```
> www.nasa.gov
```

obtenemos:

```
Server:      127.0.0.1
Address:     127.0.0.1#53

Non-authoritative answer:
www.nasa.gov canonical name = www.nasa.gov.speedera.net.
www.nasa.gov.speedera.net canonical name =
www.nasa.gov.edgesuite.net.
www.nasa.gov.edgesuite.net canonical name = a1718.x.akamai.net.
```

Name: a1718.x.akamai.net  
Address: 130.206.192.33  
Name: a1718.x.akamai.net  
Address: 130.206.192.41