Domain Name Server

Daniel Pecos Martínez

dani@netpecos.org

Castellón, 1 de Diciembre 2003

INTRODUCCIÓN

En este documento se realiza una breve explicación sobre los conceptos básicos del DNS, poniendo como ejemplo una configuración sencilla del servidor de nombres GNU *bind*.

CONCEPTOS BÁSICOS

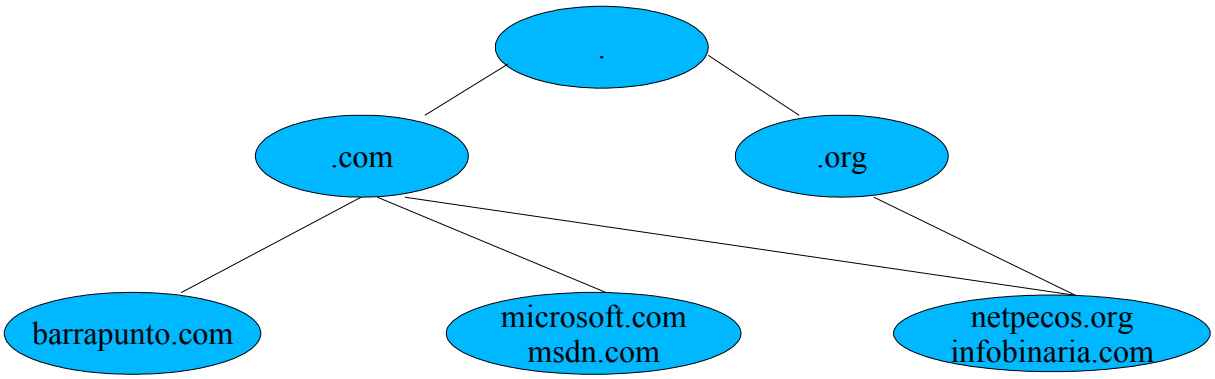
¿Qué es un DNS?

El Domain Name Server consiste en un sistema de traducción de nombres o dominios a direcciones IP y viceversa. Podría verse como una gigantesca base de datos distribuida por todo Internet, estructurada de forma jerárquica por medio de un árbol, el cual suele ser denominado como *espacio de nombres*.

Los dominios se clasifican en función de su nivel o profundidad dentro del árbol de la jerarquía DNS. De este modo existen dominios:

- Primer nivel, gestionados, bien por organizaciones específicas para ello, bien por organizaciones gubernamentales.
- Segundo nivel, gestionados por entes particulares.
- Tercer nivel.
- Etcétera.

Además se puede considerar un dominio de nivel 0 o raíz, del que cuelgan el resto de dominios de primer nivel (ver figura). Dicho dominio recibe el nombre de «.».



Jerarquía servidores de nombre.

Los dominios de primer nivel que se crearon cuando se diseñó el DNS, y que siguen siendo los de mayor importancia en Internet son:

Dominio	***Descripción***
edu	Instituciones educativas.
com	Organizaciones comerciales.
org	Organizaciones no comerciales.
net	Pasarelas y otras redes administrativas.
gov	Gobierno norteamericano.
mil	Ejército norteamericano.
uucp	Redes UUCP.

Así, los dominios que cuelguen de algunos de estos dominios de primer nivel, deberán estar destinados a las actividades a las que se destinan su dominio padre. Ésto no es cierto para los dominios .com, .org, .net, ya que hoy en día cualquiera puede adquirir un dominio que deriven de algunos de éstos, sin tener que demostrar que va a estar destinado a ninguna tarea en especial.

Además de los dominios de primer nivel ya comentados, existen dominios propios a cada país, que corresponden a las siglas con las que se denomina a cada uno de los países según la nomeclatura seguida por la ONU. Dichos dominios son gestionados según la política que cada país crea conveniente.

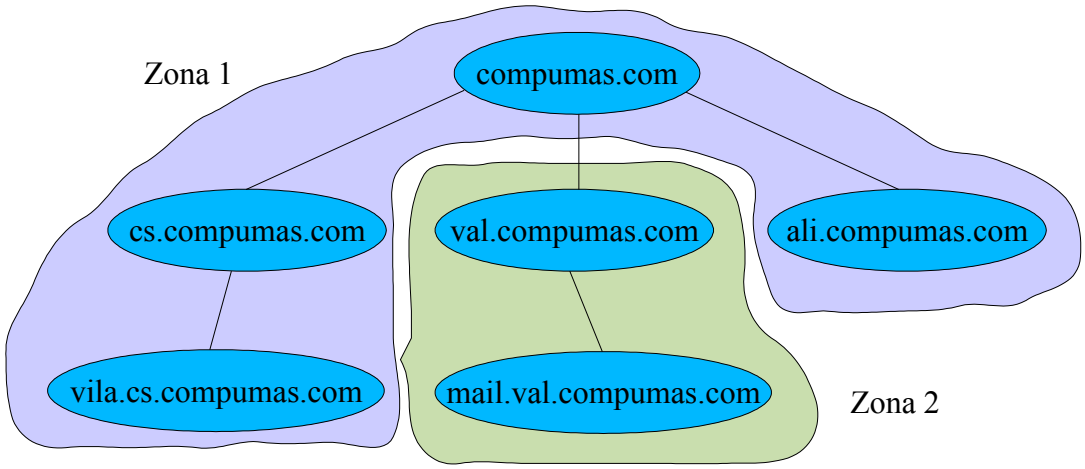
Delegación

Hemos comentado que los dominios de primer nivel destinados a los países son gestionados por estos a su voluntad. Ésto es posible porque éstos dominios están *delegados* en administradores propios al país, de forma que son éstos los que los gestionan. Dicha delegación de *autoridad* sobre un dominio se puede realizar a cualquier nivel del espacio de nombres, de manera que si se dispone un dominio de segundo nivel para una empresa, se podrían crear dominios de niveles inferiores según la estructura organizativa de la empresa, por poner un ejemplo.

Más concretamente, la delegación consiste en la cesión del control de una *zona* del espacio de nombre a

otro servidor DNS. Una zona es una porción del espacio de nombres, de forma que se posee autoridad desde el nodo raíz de dicha zona dentro del árbol jerárquico, pudiendo crear o eliminar nuevos subdominios a partir del nivel en el que se encuentre dicho nodo raíz.

La diferencia entre dominio y zona suele ser confusa en un principio. Se trata de dos conceptos relacionados en diferentes capas: dominio es un concepto del espacio de nombres, mientras que zona es la forma en la que se distribuye la autoridad sobre un determinado dominio. Así pues, un dominio contiene todas las máquinas que están dentro de dicho dominio, incluidos subdominios, mientras que una zona incluye solo las máquinas del dominio que cuelgan del subdominio sobre el que se posee la autoridad. Podría decirse que las zonas es la forma en la que se distribuye el control sobre el espacio de nombres, y, por lo tanto, que son una causa directa de la delegación de autoridad sobre el espacio de nombre.



División en zonas del espacio de nombres

Resolución directa y resolución inversa

Existen dos tipos de preguntas a las que responde un DNS: la resolución directa, que consiste en contestar la IP o IP's que corresponden a un determinado nombre de dominio, y la resolución inversa, que consiste en, dada una IP de Internet, qué nombre se le asocia. En el apartado de «Configuración de Bind» se verán algunos ejemplos y se explicará un poco más sobre esto conceptos.

Propagación entre servidores

El proceso de propagación en el DNS consiste en la difusión de los cambios producidos en dominios de los que se tiene autoridad. Este proceso suele tardar entre 28 y 72 horas (tiempo de *latencia*), aunque en teoría los cambios deberían ser visibles inmediatamente después de haberlos realizado. Este retraso se debe en la mayor parte a las caché que suelen usar los DNS.

Existen dos tipos de configuraciones para los servidores DNS: *recursivos* y *no recursivos*. Dependiendo de si el servidor intenta o no devolver el resultado exacto de la petición recibida, éste será recursivo o no recursivo, respectivamente. Cuando un servidor no es recursivo, lo que hace es devolvernos la dirección del servidor DNS que posee autoridad sobre el siguiente dominio de la petición que le hemos realizado, de forma que cada vez estamos más próximos al servidor autoritativo. Por tanto, el proceso de resolución de nombres con servidores no recursivos es un proceso iterativo y en el que el cliente participa activamente. Por contra, en el

caso de usar servidores recursivos el proceso, desde el punto de vista del cliente, es lineal y con una actuación pasiva. Normalmente no suelen configurarse servidores exclusivamente no recursivos (a excepción de los servidores raíz y de muy alto nivel en el espacio de nombres), sino que suelen actuar como recursivos para un determinado conjunto de nodos y como no recursivos para el resto.

Normalmente los servidores recursivos incorporan una tabla caché, de forma que si se les vuelve a preguntar por un dominio del cual han averiguado su IP y el *TTL* o *Tiempo de Vida* de la respuesta no ha vencido, no vuelven a realizar la búsqueda, sino que devuelven el resultado anterior. Cuando la resolución se lleva a cabo de esta forma, el servidor DNS que la realiza indica en la respuesta que no es *autoritativa*. Una respuesta se considera que es autoritativa cuando proviene del servidor que posee autoridad sobre el dominio en cuestión, siendo *no autoritativa* para el resto de casos.

Así pues, el problema de que la propagación entre servidores DNS tenga una latencia tan grande se debe a que debemos esperar a que el tiempo de vida de la entrada en caché del dominio venza en todos los servidores, de forma que llegará un momento en que será necesario volver a realizar la consulta al servidor que posee autoridad, de forma que éste nos responderá con la respuesta correcta, la cual, de nuevo será introducida en la tabla caché de los distintos servidores. El tiempo de expiración de la caché depende de las implementaciones del software DNS y de su configuración, aunque por lo normal se suele respetar el tiempo de vida indicado por la respuesta DNS del servidor.

CONFIGURACIÓN BIND

A continuación se comentará la configuración básica de un servidor de DNS. En concreto usaremos el software Berkeley Internet Name Domain o *bind* en su versión 8.4.1.0, ya que es uno de los servidores de DNS que goza de mayor difusión en Internet.

Para el ejemplo, supondremos la posesión del dominio compumas.com, para el cual se deberán añadir diferentes zonas para las distintas secciones de la empresa, algunas de las cuales estarán administradas por computadores propios a dichas secciones. Se deberán incluir nombres para los servidores de correo, web y ftp que posee la empresa. Se configurarán un servidor *maestro* y un *esclavo*.

La diferencia básica entre un servidor maestro y un servidor esclavo, es cuál de los dos recibe las modificaciones introducidas en las configuraciones de los dominios. Ésto es así porque el servidor configurado como esclavo realiza un *polling* sobre el servidor maestro para mantener sincronizadas las configuraciones de ambos. Dicha diferenciación no se realiza desde el punto de vista del DNS, puesto que ambos pueden realizar respuestas autoritativas a una petición, sino que se realiza a nivel de configuración del software. El propósito de esto es el balanceo de carga entre los diferentes servidores definidos para un dominio.

A continuación se da una configuración básica del servidor de nombres primario o maestro:

/etc/named.conf

```
options {
            directory “/var/lib/named”;
            allow recursion {
                        // direcciones de redes y/o ordenadores para las
                        // que se actuará como DNS recursivo
                        183.165.75.0/24;
                        183.165.72.8/32;
                  };

            allow transfer {
                        // dirección del servidor esclavo
                        150.165.43.176;
                  };
```

```
            forward first;
            forwarders   {
                              232.154.178.35;
                              157.246.33.2;
                        };
      };

// zona en la que se incluyen los servidores raíz (no debería ser modificado)
zone “.” {
      type hint;
      file “root.hint”;
      };

// zona para nuestro dominio (configurado como maestro)
zone “compumas.com” {
      type master;
      // fichero de configuración de subdominios
      file “zone/compumas.com”;
      };

// zona de resolución inversa
zone “75.165.183.in-addr.arpa” {
      type master;
      file “zone/183.165.75”;
      };
```

De esta forma, el servidor actúa como recursivo para una red y para una IP determinadas. Se permitirá el actuar como esclavo de este servidor a la IP configurada en el campo *allow transfer*. También podemos observar que las peticiones sobre las que no se tenga autoridad serán reenviadas (*forward*) a otros servidores DNS, que generalmente son los de tú ISP.

El fichero de configuración del dominio es el siguiente. En él se especifican el número de serie, tiempo de refresco, de reintento, de vencimiento y el mínimo TTL, así como la serie de subdominios que se hayan configurado.

/var/lib/named/zone/compumas.com

```
$TTL 1m
@      IN     SOA    ns.compumas.com. hostmaster.compumas.com. (
                           2003120101;  serial
                           8H;          refresh
                           2H;          retry
                           4W;          expire
                           1D;          minimum
                     );
       IN     NS     ns                        ; Dirección IP del servidor
       IN     MX     10 mail                   ; Servidor de mail principal
       IN     MX     20 mail.compumenos.com.   ; Servidor de mail de respaldo

ns     IN     A      127.0.0.1
mail   IN     A      183.165.75.7
www    IN     A      183.165.75.8
web    CNAME  www    // web es un alias para www
ftp    IN     A      183.165.75.9

cs             IN     A      167.154.8.2
vila.cs        IN     A      167.154.8.4
val            IN     NS     dns.val
dns.val        IN     A      88.76.43.58
ali            IN     A      25.43.67.3
```

Hemos definido cuatro subdominios para este dominio (ns, mail, www, ftp), y se han configurado dos servidores de correo, uno principal y otro de respaldo, de forma que el de respaldo no está bajo las mismas instalaciones que el primario, reduciendo drásticamente las posibilidades de que los dos servidores caigan durante un mismo espacio de tiempo.

En esta configuración también se han incluido los parámetros necesarios para representar una jerarquía semejante a la indicada en el gráfico del apartado anterior. Se puede observar que el dominio val.compumas.com ha sido delegado completamente excepto dns.val.compumas.com, ya que es necesario conocerlo para poder realizar la delegación.

De esta forma cedemos la gestión total del dominio val.compumas.com a otro servidor DNS, de manera que dicho servidor tendrá un fichero val.compumas.com que podría ser semejante al siguiente:

```
$TTL 1m

@       IN      SOA     dns.val.compumas.com. hostmaster.compumas.com. (
                                2003120101;  serial
                                8H;          refresh
                                2H;          retry
                                4W;          expire
                                1D;          minimum
                        );
        IN      NS      dns                     ; Dirección IP del servidor
        IN      MX      10 mail                 ; Servidor de mail principal
        IN      MX      20 mail.compumenos.com.   ; Servidor de mail de respaldo

dns     IN      A       88.76.43.58
mail    IN      A       88.76.43.100
www     IN      A       88.76.43.27
```

El fichero de configuración para la zona de resolución inversa es el que sigue. En él se definen los mismos parámetros que en el fichero anterior, salvo que en este caso no se configuran subdominios, sino que se asignan nombres a las IP de las que se tiene autoridad (ya que de no tenerla, la configuración no tendrá efecto alguno en Internet).

/var/lib/named/zone/183.165.75

```
$TTL 1m

@       IN      SOA     ns.compumas.com. hostmaster.compumas.com. (
                                2003120101;  serial
                                8H;          refresh
                                2H;          retry
                                4W;          expire
                                1D;          minimum
                        );
        IN      NS      ns                      ; Dirección IP del servidor
        IN      MX      10 mail                 ; Servidor de mail principal
        IN      MX      20 mail.compumenos.com.   ; Servidor de mail de respaldo

6       PTR     ns.compumas.com.
7       PTR     mail.compumas.com.
8       PTR     www.compumas.com.
9       PTR     ftp.compumas.com.
```

Una vez configurado el servidor maestro, solo queda configurar el servidor esclavo. Dicha configuración será semejante a la del maestro, salvo por el detalle de que este servidor no poseerá más información sobre

dominios configurados como esclavo que la que el servidor maestro le comunique.

/etc/named.conf

```
options {
        directory “/var/lib/named”;
        allow recursion {
                        // direcciones de redes y/o ordenadores para las
                        // que se actuará como DNS recursivo
                        183.165.75.0/24;
                        183.165.72.8/32;
                };

        allow transfer {
                        // dirección del servidor esclavo
                        150.165.43.176;
                };

        forward first;
        forwarders   {
                        232.154.178.35;
                        157.246.33.2;
                };
};

// zona en la que se incluyen los servidores raíz (no debería ser modificado)
zone “.” {
        type hint;
        file “root.hint”;
        };


// zona para nuestro dominio (configurado como esclavo)
zone “compumas.com” {
        type slave;
        // fichero de configuración de subdominios (será copiado del maestro)
        file “zone/compumas.com”;
        masters { 183.165.75.6; };
        };

// zona de resolución inversa
zone “75.165.183.in-addr.arpa” {
        type master;
        file “zone/183.165.75”;
        };
```

Como se puede observar, esta configuración es muy semejante a la del servidos maestro, con las únicas diferencias de que la zona “compumas.com” se ha declarado como servidor esclavo (definiendo, por tanto, cuál es el servidor maestro). La zona de resolución inversa la hemos mantenido como servidor maestro, debido a lo sencillo y bastante estático de su configuración.

De esta forma, el servidor consultará al servidor maestro por si ha habido modificaciones según los parámetros establecidos en el campo SOA. En caso de que haya habido, el servidor copiará el fichero de configuración del dominio, repitiendo el proceso descrito indefinidamente.

BIBLIOGRAFÍA

DNS and Bind

Autores: Paul Albitz & Cricket Liu
Editorial: O'Reilly

Guía de Administración de Redes con Linux

Autores: Olaf Kirch & Terry Dawson
WEB: http://lucas.hispalinux.es

DNS-HOWTO

Autor: Nicolai Langfeldt
WEB: http://tldp.org