

Coloquio DNS

Dominios

Para empezar a tratar el tema de DNS, primero debemos empezar por explicar lo que es un Dominio y como esta estructurada la red que es Internet.

Un Dominio, básicamente es una dirección. Como todas las casas tienen una dirección, pues las computadoras también la tienen. Esta dirección es lo que se conoce como dirección IP. Ya que la dirección IP se conforma de números, en una red suficientemente grande como Internet se hace un poco difícil recordar las direcciones, de ahí es que se le asignan los nombres de Dominio. Estos dominios son únicos y permiten agrupar un conjunto de equipos o dispositivos.

Los dominios se estructuran como árboles, donde la más alta jerarquía sería lo que se conoce como TLD (Top Level Domain). El TLD es la parte final de un dominio de Internet; esto es, las letras que siguen al punto final de cualquier nombre de dominio.

La Internet Assigned Numbers Authority (IANA) actualmente clasifica los dominios de nivel superior en tres tipos:

* Dominios de nivel superior geográfico (ccTLD): Usados por un país o un territorio dependiente. Tienen dos letras de largo.

Existen unos 243 ccTLDs, tienen una longitud de dos letras, y la mayoría corresponden al estándar de códigos de países ISO 3166-1 (las diferencias se explican más adelante). Cada país designa gestores para su ccTLD y establece las reglas para conceder dominios.

* Dominios de Internet genéricos (gTLD): Usado (al menos en teoría) por una clase particular de organizaciones (por ejemplo, com para organizaciones comerciales). Tiene tres o más letras de largo. La mayoría de los gTLDs están disponibles para el uso mundial, pero por razones históricas mil (militares) y gov (gubernamental) están restringidos para el uso por las respectivas autoridades estadounidenses. Los gTLDs se clasifican, a su vez, en los dominios de Internet patrocinados (sTLD), Ej..aero,.coop y .museum, y los dominios de Internet no patrocinados (uTLD), Ej..biz, .info, .name y .pro.

* Dominios de nivel superior de infraestructura: El dominio de nivel superior arpa es el único confirmado.

Finalmente, al principio del dominio está el nombre de la máquina o servidor web, así que por ejemplo: www ldc.usb.ve, se traduciría en que se busca conectarse al servidor web (www) perteneciente al dominio del ldc, a su vez perteneciente al dominio usb y todos ellos pertenecientes al .ve que sería el ccTLD correspondiente a Venezuela.

Cada Dominio puede tener hasta 127 subdivisiones y cada subdivisión no puede tener más de 63 caracteres. Cada subdominio está relacionado con un subdominio.

DNS (Domain Name System)

Antes, cuando las redes de computadoras eran bastante reducidas se contaba con un archivo llamado HOSTS que contenía todos los dominios de Internet conocidos, pero a raíz de la expansión de Internet, ya no resultaba práctico tener el archivo HOSTS, así que en 1983 se publicaron los RFCs para definirlo que hoy es DNS.

El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar distintos tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

Básicamente el DNS es como una guía telefónica, donde los teléfonos son las direcciones IP y los nombres serían los nombres de Dominio, donde nosotros buscamos un nombre de Dominio y nos devuelve su dirección IP o vice versa.

Entonces en la computadora del cliente, un programa cliente DNS genera peticiones para la resolución de nombres.

Pueden enviarse dos tipos de consultas DNS distintas, y que se distinguen por un bit que se llama RD (Recursion Desired, se solicita recursividad). Las consultas recursivas, cuando este bit está activado, las envían normalmente programas de usuario, usando rutinas en las bibliotecas del sistema, como por ejemplo `gethostbyname(3)`. Normalmente, éstas enviarán la consulta a otro servidor, cuya dirección hallarán consultando `/etc/resolv.conf` para saber qué servidor de nombres deben usar.

- Recursiva
- Iterativa

Una consulta recursiva le pide al servidor que haga lo que sea preciso para encontrar la respuesta, incluyendo la consulta recursiva a cualesquiera otros servidores que tenga que consultar para darnos la respuesta; de ahí su nombre. La respuesta a una consulta recursiva debiera ser la respuesta final a la pregunta, o una declaración firme de que la respuesta no se pudo hallar.

El proceso de resolución de nombres de manera recursiva sería la siguiente:

Cuando una aplicación (cliente) necesita resolver un FQHN (Fully Qualified Host Name) envía un requerimiento al servidor de nombres configurado en el sistema (normalmente, el provisto por el ISP). A partir de entonces se desencadena el proceso de resolución del nombre:

1. El servidor de nombres inicial consulta a uno de los servidores raíz (cuya dirección IP debe conocer previamente).
2. Este devuelve el nombre del servidor a quien se le ha delegado la sub-zona.
3. El servidor inicial interroga al nuevo servidor.
4. El proceso se repite nuevamente a partir del punto 2 si es que se trata de una sub-zona delegada.
5. Al obtener el nombre del servidor con autoridad sobre la zona en cuestión, el servidor inicial lo interroga.
6. El servidor resuelve el nombre correspondiente, si este existe.
7. El servidor inicial informa al cliente el nombre resuelto.

La manera iterativa sigue básicamente la forma recursiva, solo que el servidor consulta los datos locales, incluyendo su cache, y si hay más de un servidor autorizado para la zona, BIND devuelve el que tenga menor RTT (round-trip time), es decir el tiempo que tarda un servidor para responder a la consulta.

típicamente le envía un programa que actúa como resolutivo recursivo; dicho programa estaría a la escucha en una dirección que el cliente puede hallar en `/etc/resolv.conf`. Así pues, un cliente que quiera encontrar la dirección del nombre de una máquina, o el nombre de la máquina a partir una dirección, o que quiera hacer cualquier otra consulta al sistema DNS, buscaría la dirección del resolutivo recursivo apropiado en el `/etc/resolv.conf` local y enviaría su petición recursiva, con el bit RD activado. Esta funcionalidad se halla en `gethostbyname(3)` y `gethostbyaddr(3)`. El resolutivo recursivo comienza entonces el proceso de averiguar realmente la información solicitada por parte del usuario, usando una serie de consultas iterativas (con el bit RD sin activar). Estas consultas iterativas no le piden al servidor que localice las respuestas en nuestro lugar mediante peticiones sucesivas, sino que simplemente le piden al servidor que nos conteste a la pregunta, o que nos diga quién sabe la respuesta mejor que él.

Así pues, allí donde una consulta recursiva para un dominio en particular podría devolver su dirección IP, un una declaración firme de que no hay tal máquina, una consulta iterativa podría devolver las identidades de otros servidores de nombres para probarlos en la búsqueda de la respuesta.

Cada dominio necesita un servidor primario DNS, aunque un servidor DNS puede ser el primario de muchos dominios. El servidor DNS primario contiene unos pequeños archivos de texto, llamados archivos de zona, que constituyen la base de datos de direcciones IP y nombres de dominio. El siguiente podría ser el archivo de zona para un supuesto dominio misitio.com:

```
misitio.com. IN SOA ns1.saulo.net. postmaster.misitio.com. (
    2002080801 ; Numero de Serie, fecha de hoy + numero de serie de hoy
    28800      ; Tasa de refresco [8h]
    7200      ; Tasa de reintento [2h]
    604800    ; Caducidad para secundario [7d]
    86400)    ; Validez para clientes [1d]

; Servidores DNS

misitio.com.      IN NS  ns1.saulo.net.
misitio.com.      IN NS  ns2.saulo.net.

; Servidores de correo

misitio.com.      IN MX  10 correo1.misitio.com. ; Servidor de correo principal
misitio.com.      IN MX  20 correo2.misitio.com. ; Servidor de correo de reserva

; Direcciones IP de los hosts

ulises.misitio.com IN A   10.7.3.2 ; Dirección IP del servidor web
correo1.misitio.com IN A   10.7.3.3 ; Dirección IP del servidor de correo principal
correo2.misitio.com IN A   10.7.3.4 ; Dirección IP del servidor de correo de reserva

; Otros nombres para los mismos hosts (alias)
www.misitio.com   IN CNAME ulises.misitio.com
```

En este archivo vemos que la dirección IP del servidor web es 10.7.3.2 y su nombre real, ulises. El nombre www se ha escrito como un alias de ulises para que desde un navegador se pueda teclear www.misitio.com. Las www se han convertido en un convenio a la hora de designar los servidores web. Obsérvese que es en este archivo donde se determina si el sitio web se podrá invocar de la forma http://misitio.com o bien, de la forma http://www.misitio.com, de ambas o de cualquier otra que elijamos siempre y cuando termine en el nombre de dominio que hemos registrado

El servicio DNS está compuesto de un grupo de servidores que transmiten de un lado a otro <registros de recursos> (RRs). Hay muchos tipos de registros de recursos, y varios protocolos diferentes para solicitar dichos recursos. DNS se transmite tanto sobre TCP como sobre UDP, en el puerto 53. Las peticiones más corrientes son sobre UDP. TCP se usa cuando el total del conjunto de RRs de una réplica excede los 512 bytes, o para llevar a cabo "transferencias de zonas".

Como tipos de registros tenemos:

- A = Address – (Dirección) Este registro se usa para traducir nombres de hosts a direcciones IP.
- CNAME = Canonical Name – (Nombre Canónico) Se usa para crear nombres de hosts adicionales, o alias, para los hosts de un dominio. Es usado cuando se están corriendo múltiples servicios (como ftp y web server) en un servidor con una sola dirección ip. Cada servicio tiene su propia entrada de DNS (como ftp.ejemplo.com. y www.ejemplo.com.). Esto también es usado cuando corren múltiples servidores http, con diferentes nombres, sobre el mismo host.
- NS = Name Server – (Servidor de Nombres) Define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información de dicho dominio. Cada dominio se puede asociar a una cantidad cualquiera de servidores de nombres.

- MX = Mail Exchange – (Registro de Intercambio de Correo) Asocia un Dominio de nombre a una lista Servidores de intercambio de correo para ese Dominio.
- PTR = Pointer – (Indicador) También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio.
- SOA = Start of authority – (Autoridad de la zona) Proporciona información sobre la zona.
- HINFO = Host INFOrmation – (Información del sistema informático) Descripción del host, permite que la gente conozca el tipo de máquina y sistema operativo al que corresponde un dominio.
- TXT = TeXT - (Información textual) Permite a los dominios identificarse de modos arbitrarios.
- LOC = LOCalización - Permite indicar las coordenadas del dominio.
- WKS - Generalización del registro MX para indicar los servicios que ofrece el dominio. Obsoleto en favor de SRV.
- SRV = SeRVicios - Permite indicar los servicios que ofrece el dominio. RFC 2782
- SPF = Sender Policy Framework - Ayuda a combatir el Spam. En este record se especifica cual o cuales hosts están autorizados a enviar correo desde el dominio dado. El servidor que recibe consulta el SPF para comparar la IP desde la cual le llega, con los datos de

Tipos de DNS

BIND:

Prácticamente el único software utilizado en los servidores de nombres de Internet es bind ("Berkeley Internet Name Domain"), creado originalmente en la Universidad de California, y actualmente propiedad del Internet Systems Consortium.

Este programa, distribuido bajo una licencia libre, es utilizado en prácticamente todos los sistemas Unix del mundo. Esto ha sido considerado un problema de seguridad, al punto que se ha propuesto la migración de algunos root servers a otro sistema, ya que la aparición de algún problema de seguridad en bind podría implicar la caída de todo el DNS de Internet. Uso del DNS en una red local

BIND es el servidor de DNS más común, especialmente en sistemas Unix, en los cuales es un standard de facto.

Una nueva versión de BIND (BIND 9) fue escrita desde cero en parte para superar las dificultades arquitectónicas presentes anteriormente para auditar el código en las primeras versiones de BIND, y también para incorporar DNSSEC (DNS Security Extensions). BIND 9 incluye entre otras características importantes: TSIG, notificación DNS, nsupdate, IPv6, rndc flush, vistas, procesamiento en paralelo, y una arquitectura mejorada en cuanto a portabilidad. Es comúnmente usado en sistemas Linux.

PowerDNS:

PowerDNS es versátil y está escrito en C++ y licenciado debajo de GPL. Corre en la mayoría de sistemas Unix y en windows. PowerDNS cuenta con la posibilidad de actuar como los archivos de zona como los de BIND hasta bases de datos relacionales. Incluye un DNS recursor pero está separado del programa

MaraDNS:

MaraDNS es un security-aware DNS. Junto con BIND, NSD, djbdns, y PowerDNS, es uno de un pequeño número de servidores DNS con código de fuente pública. Al igual que BIND y djbdns, MaraDNS puede funcionar independientemente de que sea un servidor DNS con autoridad, como un cache DNS recursivo que utiliza la raíz de nombres del DNS, o como cache transportista que depende de los otros servidores DNS recursivos.

djbdns:

Este DNS simple y de implementación security-aware DNS, nació de los problemas que tenía BIND. Hasta el 2004 fue el segundo DNS más popular

pdnsd:

Es un servidor proxy DNS, es configurable con un config file, o usando el programa pdnsd-clt que viene con el paquete. A diferencia de BIND, pdnsd guarda en él cache en el disco y lo mantiene por largo plazo y no lo borra cuando arranca o termina el programa. Está diseñado para situaciones donde la conectividad es baja, como en casos con wifi hotspots o dialup. Está limitada la capacidad para ser el servidor autoritario de una zona DNS sin una red privada.

MyDNS:

Es servidor DNS de fuente abierta para sistemas UNIX. Los RR (Resource Records) están almacenados en una base de datos MySQL o PostgreSQL. Los cambios al servicio no deben ser reiniciados. Tiene una resolución a tiempo real como DynDNS. Desde la versión 1.1.0, ofrece la oportunidad de responder a peticiones recursivas. Si un dominio que el MyDNS no tiene información, la petición se puede configurar a otro servidor DNS.

SERVIDOR DNS BIND

- Cómo instalarlo?

Una vez bajado el programa se usa "sudo apt-get install bind9" o "sudo aptitude install bind9"

Después hay que modificar el archivo named.conf.local con "sudo vi /etc/bind/named.conf.local"

En ese archivo es donde se van a insertar las zonas, vamos a insertar lo siguiente:

```
zone "nuestrodominio" {
    type master;
    file "/etc/bind/zones/nuestrodominio.db";
};

# esta es la parte de definicion del reverse DNS. hay que reemplazar 0.168.192 por nuestra direccion
de red, pero al revés
zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/rev.0.168.192.in-addr.arpa";
};
```

Después hay que modificar las opciones del archivo named.conf.options con "sudo vi /etc/bind/named.conf.options" la parte de forwarders. forwarders es la dirección del DNS que se va a enviar la petición de resolver un dominio en caso que nuestro DNS no la contenga

por ejemplo:

```
forwarders {
    # reemplazamos esta dirección por el DNS de nuestro proveedor por ejemplo el de CANTv
    (200.44.32.123)
    123.123.123.123;
};
```

Ahora hay que agregar el archivo de zona, para esto hacemos lo siguiente

```
sudo mkdir /etc/bind/zones
sudo vi /etc/bind/zones/nuestrodominio.db
```

El archivo redefinición de zona es donde vamos a poner todas las direcciones, nombres de maquinas que nuestro DNS va a conocer como por ejemplo:

```
nuestrodominio.      IN      SOA      nuestroDNS.nuestrodominio. admin.nuestrodominio. (
```

```

2006081401
28800
3600
604800
38400
)

nuestrodominio.    IN    NS    nuestroDNS.nuestrodominio.
nuestrodominio.    IN    MX    10    nuestrosevidormail.nuestrodominio.

// Reemplazar las IPs por las de Ips de los servidores correspondientes.
www                IN    A    159.90.0.3
nuestroservidormail IN    A    159.90.0.2
nuestroDNS        IN    A    159.90.0.1

```

Ahora hay que crear el archivo de zona reverso

```
"sudo vi /etc/bind/zones/rev.0.168.192.in-addr.arpa"
```

y copiamos lo siguiente:

```

@ IN SOA nuestroDNS.nuestrodominio. admin.nuestrodominio. (
    2006081401;
    28800;
    604800;
    604800;
    86400
)

                IN    NS    nuestroDNS.nuestrodominio.
// el 1 se refiere al ultimo numero de la IP del DNS, es decir el nombre de la maquina, en este caso
por ejemplo el IP seria //algo como 159.90.10.1
1                IN    PTR    nuestrodominio

```

Ahora ya esta todo listo y hay que reiniciar el bind con "sudo /etc/init.d/bind9 restart"

para probarlo, primero hay que modificar el etc/resolv.conf, que contiene el servidor DNS al que se van a enviar las consultas.

```
"sudo vi /etc/resolv.conf"
```

y introducimos:

```

search nuestrodominio
nameserver 159.90.10.1 (cambiar 159.90.10.1 por la IP de nuestro DNS)

```

listo, podemos probar si funciona con

```
"dig nuestrodominio"
```

-Configuración del DNS

Ficheros

named.conf es el lugar donde le dice a BIND qué, dónde y cómo. Se trata del fichero de configuración principal de BIND.

```
// generated by named-bootconf.pl

options {
    directory "/var/named";
    /*
     * If there is a firewall between you and nameservers you want
     * directive below. Previous versions of BIND always asked
     * questions using port 53, but BIND 8.1 uses an unprivileged
     * port by default.
     */
    // query-source address * port 53;
};

//
// Boot file for name server
//
// type          domain          source          file
zone "." {
    type hint;
    file "named.root";
};

// Zone boot information and daemon options are kept in other files
// (autoincluded from boot.zones)
//
// Name server zone boot file
// See named(8) for syntax and further information
//
// type          domain          source          file
// (autoincluded from boot.options)
//
// Options for name server
// Use `bindconfig' to automatically configure this file
//
// type          domain          source          file
zone "localhost" {
    type master;
    file "named.local";
};

zone "127.in-addr.arpa" {
    type master;
    file "named.rev-local";
};

// Custom configurations below (will be preserved)
```

En el ejemplo anterior, "type" especifica si es un master o un esclavo de ese dominio. El tipo master quiere decir que su servidor DNS no pedirá a nadie más información sobre ese dominio. Otros sistemas pueden configurarse para realizar transferencias de zona ("zone-transfers") de ese dominio. La transferencia de zona básicamente significa pasar la información a otro servidor DNS y así ser utilizado para realizar búsquedas DNS. En cambio, si va a extraer la información de otro servidor, necesitará usar el tipo esclavo ("type slave").

"file" en el ejemplo de arriba especifica el nombre del fichero donde se guarda o se guardará la información. Estos ficheros se encuentran (o deberían encontrarse) por defecto en /var/named (a menos que cambie la sentencia "directory" en /etc/named.conf).

Archivos de zona

Los archivos de zona (o archivos de base de datos) son el corazón de su sistema BIND. Aquí está toda la información sobre qué nombre de host se asocia con qué dirección IP.

ejemplo de archivo de zona:

```
;
; BIND data file for sudominio.com
;
@      IN      SOA      sudominio.com. root.sudominio.com. (
                        1          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Default TTL

      IN NS      dns.sudominio.com.

      IN  MX      10      mail.sudominio.com.

www    IN  A      192.168.100.5
dns    IN  A      192.168.100.10
mail   IN  A      192.168.100.20
```

Las primeras 6 líneas son de configuración de la zona. Estas líneas dicen cuál es la zona (sudominio.com), quién es el responsable (root.sudominio.com, que es equivalente a root@sudominio.com) y alguna otra cosa más. Estas otras cosas incluyen un número de serie que nos dé una pista de cuándo se ha actualizado, cada cuánto actualizar la base de datos, cada cuánto reintentar una transferencia de zona, cuándo caduca la información de zona y un tiempo de vida por defecto. En el momento en que haga cambios a los ficheros de zona, debe incrementar el número de serie. Si no lo hace, puede haber problemas, sobre todo si es un servidor primario proporcionando información a sitios secundarios. La mayoría de esta información sólo se usa si tiene sistemas tanto maestros como esclavos.

Las dos líneas siguientes le dicen quién es el servidor DNS primario y quién debería coger el correo en este dominio. Puede tener múltiples líneas de cada uno de estos. Para añadir más servidores DNS tan solo hay que repetir exactamente lo que está listado, cambiando el servidor dns.sudominio.com por otro servidor DNS. Para añadir otro servidor de correo, haga lo mismo salvo que tiene un campo extra. El "10" en la línea MX establece la prioridad, los números bajos son los primeros. Esto quiere decir que, si tiene 2 líneas MX, una con 10 y la otra con 20, intentará enviar el correo a la lista MX con la prioridad 10 y si falla irá a la lista MX con la prioridad 20.

El resto del fichero de zona relaciona todas sus computadoras e IPs

Ficheros inversos

Los ficheros de búsqueda inversa son casi iguales a los ficheros de dominio, pero con algunos pequeños cambios. Aquí hay un ejemplo de un fichero de búsqueda inversa.

```
;
; BIND reverse data file for 192.168.100.0
;
@      IN      SOA      sudominio.com. root.sudominio.com. (
                        1          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Default TTL
;

      IN  NS      dns.sudominio.com.

5      IN  PTR     www.sudominio.com.
10     IN  PTR     dns.sudominio.com.
20     IN  PTR     mail.sudominio.com.
```

La primera sección de este fichero es exactamente la misma que la primera sección de los ficheros de zona de dominio. La sección de abajo es la diferente. Aquí estamos listando primero la última parte de la dirección IP y por tanto el nombre del puesto al final.

Aquí tiene que fijarse en dos detalles. Debe usar el nombre de dominio completamente cualificado y poner un punto al final de él. Estas 2 observaciones son importantes y el comportamiento será extraño de no hacerlo así.

-Crear un nuevo dominio

Para crear un nuevo dominio tenemos que crear dos nuevos archivos, correspondientes a la zona del nuevo dominio a la subred.

Por ejemplo usaremos el dominio ldc.com y la subred 159.90.10.x. Empecemos con el archivo del dominio ldc.com. Necesita crear un archivo llamado ldc.db en /etc/bind (Este archivo puede llamarse como quiera, pero lo hacemos así por el ejemplo). El archivo debería parecerse a algo como esto:

```
;  
; BIND data file for ldc.db  
; /etc/bind/ldc.db  
;  
@      IN      SOA      ldc.com. root.ldc.com. (  
                2008032001      ; Serial  
                604800      ; Refresh  
                86400      ; Retry  
                2419200      ; Expire  
                604800 )      ; Default TTL  
  
      IN      NS       dns.ldc.com.  
  
      IN      MX       10      mail.ldc.com.  
  
www      IN      A       159.90.10.1  
mail     IN      A       159.90.10.2  
dns      IN      A       159.90.10.3
```

Observe, en el ejemplo anterior, que usamos como serie 2008032001. La razón principal por la que lo hacemos es tener una pista de cuándo fue modificado por última vez el archivo. Nos dice que el archivo fue modificado por última vez el 20-03-2008 y que fue la primera vez en ese día. No hace falta que lo haga así, pero necesitará estar seguro de que aumenta la serie cada vez que lo modifica. (Especialmente si tiene Secundarios).

Ahora necesita crear su archivo de la subred 159.90.10.x. Cree un archivo llamado 159.90.10.db en /etc/bind. Se parecerá necesariamente a algo como lo siguiente:

```
;  
; BIND reverse data file for 159.90.10.0  
; /etc/bin/159.90.10.db  
;  
@      IN      SOA      ldc.com. root.ldc.com. (  
                2008032001      ; Serial  
                604800      ; Refresh  
                86400      ; Retry  
                2419200      ; Expire  
                604800 )      ; Default TTL  
  
      IN      NS       dns.ldc.com.  
  
1      IN      PTR      www.ldc.com.  
2      IN      PTR      mail.ldc.com.
```

```
3      IN      PTR      dns.ldc.com.
```

Ahora necesitamos añadir su nuevo dominio al archivo de configuración de BIND. Adelante, edite su archivo/etc/bind/named.conf y añada las siguientes líneas al final.

```
zone "ldc.com" {
    type master;
    file "ldc.db";
};

zone "10.90.159.in-addr.arpa" {
    type master;
    file "159.90.10.rev";
};
```

Guarde ese fichero y lo habrá hecho. Todo lo que tiene que hacer ahora es ejecutar /etc/init.d/bind reload y probarlo.

PROBLEMAS DEL DNS

El principal problema que presenta el DNS es que, al estar basado en UDP (protocolo de transporte que no garantiza la recepción de la información enviada), tanto las consultas como las respuestas pueden "perdersse" (por ejemplo, a causa de congestión en algún enlace de la red). Es común apreciar cómo, en el caso de servidores y redes no muy bien configuradas, la resolución de nombres se resiente sensiblemente ante cualquier anomalía (saturación de tráfico o del servidor de nombres local).

Otro inconveniente, que ya hemos hecho notar, es la lentitud de la propagación de las modificaciones en el sistema, producto de la propia arquitectura del mismo.