Domain Name Service

Georg Lehner

24 de Febrero del 2002

El servicio primario para el funcionamiento de INTERNET es el Domain Name Service. Este documento resume de forma breve su funcionamiento y da algunas referencias a otra información

1. Qué es DNS

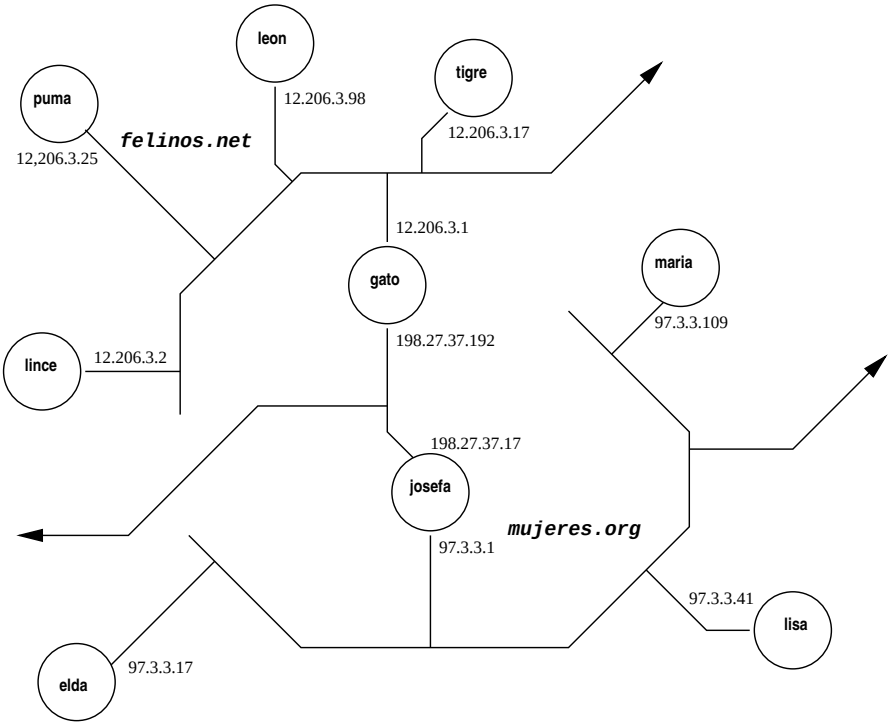
Cada computadora conectada a Internet tiene (al menos) un número de identificación asociado: su *número IP*. En todo Internet no se repite un número en diferentes computadoras.

Cada computadora tiene (generalmente) un nombre. Grupos de computadoras están organizados en *dominios* lo que permite que diferentes computadora tengan el mismo nombre, siempre y cuando se encuentran en diferentes dominios. El nombre calificado *(fully qualified domain name – fqdn)* de una computadora es la concatenación del nombre con el dominio, mediante un punto '.' de separación, ejemplo: puma.felinos.net = computadora puma, dominio felinos.net

Existe una base de datos distribuida en Internet, de la cual se puede obtener el número IP de una computadora de la cual se conoce el fqdn mediante un *query*; este tipo de query se llama *forward resolution* (resolución de nombre directo). Teniendo un número IP se puede obtener el fqdn de la computadora correspondiente mediante un *reverse query* (resolución inversa).

Es responsabilidad de la administración de un dominio proveer este servicio de resolución de nombres para las computadoras conectados. Esto involucra dos tareas: instalación de servidores de nombres y actualización constante de los registros de nombres en el dominio administrado.

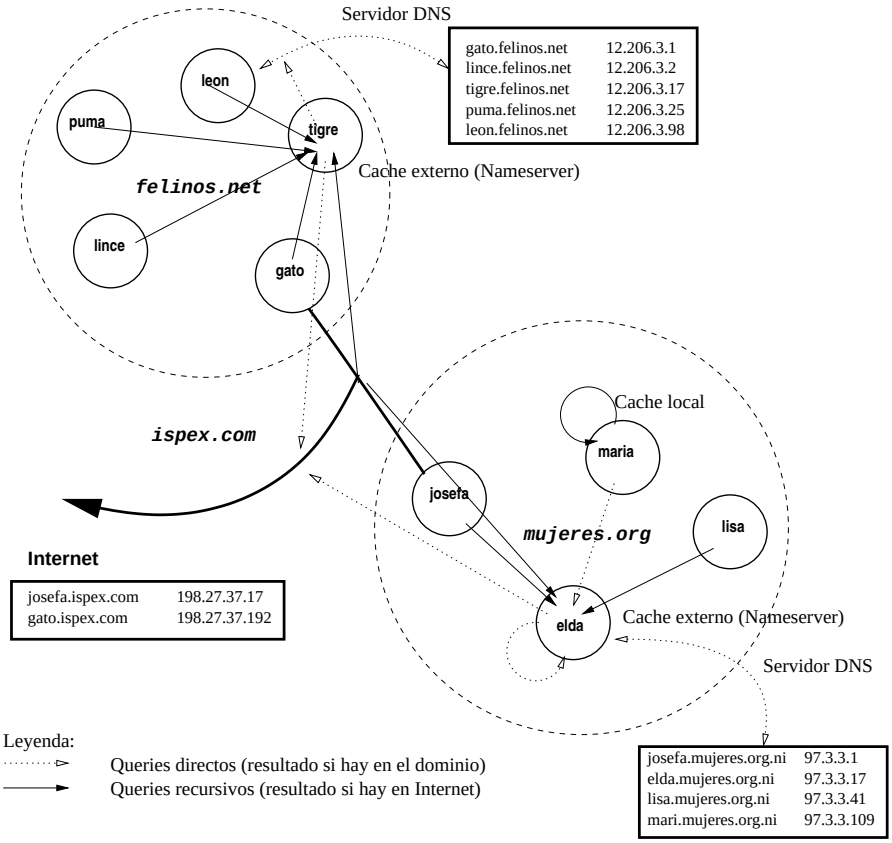
Una buena administración del DNS puede hacer más fiable y eficiente el funcionamiento del dominio. Muchas veces esto también involucra tareas de configuración de las computadoras clientes del dominio.

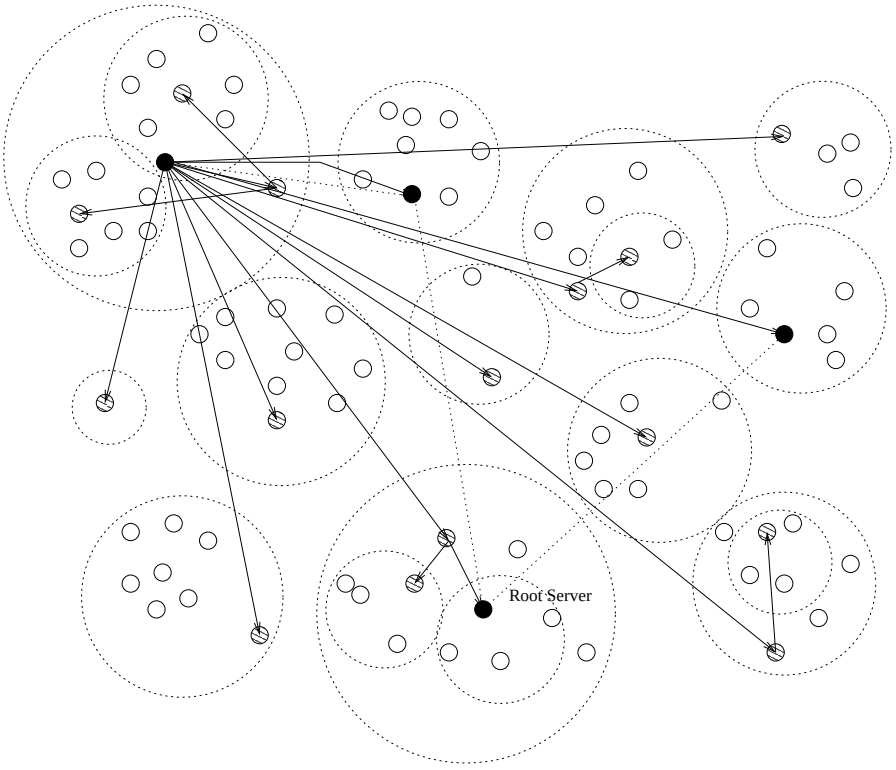


2. Una base de datos distribuida

En el dibujo 2 apreciamos la vista a dos dominios (ficticios) de Internet. Cada computadora tiene un nombre y un número IP asignado. Por más conveniencia, todas las computadoras en una red física utilizan números de un grupo común: 12.206.3.[0...255] corresponde al dominio felinos.net, 97.3.3.[0...255] a mujeres.org, y por ende 198.27.37.[0...255] a ispex.com. En la figura 2 observamos de forma esquemática la agrupación de la información sobre un dominio en una tabla, manejado por una computadora, el servidor DNS. En vez de crear una tabla completa de todos los números de todas las computadoras que podrían estar conectados a Internet y manejar esta tabla inmensa en todas las computadoras se manejan tablas de los "vecinos cercanos", que de todas formas se requieren más frecuentemente. Para obtener la información sobre computadoras remotas se establece un sistema de búsqueda jerárquica explicados más adelante.

El número de computadoras en un dominio puede ser grande, y con ello la frecuencia de consultas que se hacen al servidor de base de datos que maneja la tabla para el dominio. Esto puede causar un retraso significativo en el acceso a la red. Para aliviar esta situación, se maneja la información sobre nombres y números IP en uno o varios cachés. El caché realiza la búsqueda correspondiente a una consulta hecha por un cliente y entrega el resultado, pero a la vez guarda el resultado localmente en memoria o en el disco duro. Si se repite la misma consulta ya no se realiza una búsqueda en las tablas "oficiales", sino se entrega el resultado guardado. El problema de un caché es, que su información puede hacerse obsoleta: una computadora puede desaparecer, cambiar su nombre o su número


Servidor DNS
gato.felinos.net 12.206.3.1
lince.felinos.net 12.206.3.2
tigre.felinos.net 12.206.3.17
puma.felinos.net 12.206.3.25
leon.felinos.net 12.206.3.98
leon
puma
tigre
Cache externo (Nameserver)
felinos.net
lince
gato
ispex.com
Cache local
maria
josefa
mujeres.org
lisa
Internet
josefa.ispex.com 198.27.37.17
gato.ispex.com 198.27.37.192
elda
Cache externo (Nameserver)
Servidor DNS
Leyenda:
Queries directos (resultado si hay en el dominio)
Queries recursivos (resultado si hay en Internet)
josefa.mujeres.org.ni 97.3.3.1
elda.mujeres.org.ni 97.3.3.17
lisa.mujeres.org.ni 97.3.3.41
mari.mujeres.org.ni 97.3.3.109



IP. Por esto cada resultado grabado contiene un tiempo de expiración (TTL - Time To Live), después del cual está descartado de la memoria del caché, una subsiguiente consulta del dato resulta en una búsqueda en los Servidores DNS y por lo tanto (ojalá) en una respuesta auténtica. El programa caché puede ser instalado en todas las computadoras (óptimo), o puede instalarse solo en alguna(s), las cuales entonces sirven dentro de un dominio como la fuente de información DNS: son los servidores de nombre del dominio, o *nameserver*.

2.1. Jerarquía de la base de datos distribuida

Una serie de servidores root (por redundancia no es solo uno) manejan *delegaciones* de dominios, que son listas de cuales Servidores DNS manejan cual dominio. Estos Servidores pueden delegar a su vez la resolución de nombres de sub-dominios a Servidores DNS subordinados.

En la figura 2.1 solamente se muestra la delegación de un (1) servidor raíz (root server) en la parte izquierda arriba, todas las flechas sólidas que indican la delegación a los dominios primarios, tienen que duplicarse en cada uno de los servidores raíz (puntos negros conectados con una línea punteada). Se puede apreciar entonces, que el tiempo de respuesta del DNS se mejora, ya que cualquier consulta a los servidores root en promedio toma la vía de acceso media en la red global.

Regresando a la imagen 2 podemos ver dos vías que caracterizan el sistema DNS: La distribución jerárquica de los servidores DNS que garantiza (teóricamente) que todos los datos pueden ser encontrados, aunque recursivamente (líneas punteadas), y la jerarquía de búsqueda de los nameserver (cachés), que forman "ventanas restringidas" pero adaptables a la base de datos completa (líneas sólidas). Los cachés son cercanos a la computadora cliente, y pueden ascender de un caché al siguiente hacia "arriba". Si encuentran la respuesta en algún caché superior en el camino, no necesitan recurrir al servidor root.

3. Escenarios comunes

La práctica común en Internet es configuración minimista, deficiente y arcaica, por lo que muchos administradores no están en conocimiento de la práctica óptima (best practice). Software popular de clientes y servidores DNS se adapta a las prácticas deficientes y dificulta así el uso eficiente y la divulgación de la práctica óptima.

Estoy tratando de resumir en esta sección *best practice* para algunos casos comunes (NO para todas las situaciones), lo que no concuerda necesariamente con la experiencia de lectores experimentados en Internet. En corto: Lo presentado es solo mi punto de vista, nada mas.

Términos usados:

Caché local un programa que consulta la base de datos DNS a solicitud de un programa cliente en la computadora local, le retorna el resultado requerido o una respuesta negativa, y memoriza la respuesta durante un cierto tiempo para acelerar futuros queries sobre la misma computadora

Caché externo realiza la misma función como un caché local, pero también acepta queries de programas clientes en computadoras remotas.

Servidor DNS un programa que maneja una parte de la base de datos DNS y que acepta queries de clientes locales o remotos, pero solo contesta queries para los cuales tiene un registro disponible.

Servidor DNS local solo acepta queries desde la computadora local, normalmente desde un cache local o externo.

Servidor DNS externo acepta queries desde computadoras remotas.

LAN/Red privada una red, en la cual se utilizan números IP reservados para crear dominios en redes aislados. Estos números no se utilizan en Internet, y pueden reutilizarse en diferentes redes físicas. Estas redes y los números IP se denominan *redes privadas*.

3.1. Configuración de computadora cliente

Sistemas Operativos Unix configurar un caché local

Otros utilizan cachés externos (remotos)

En ambos casos se configura uno o más números de cachés o servidores remotos (*name-server*) a los cuales se envían queries.

En muchos sistemas Unix es común seguir también la segunda práctica.

3.2. LAN sin conexión externa

Configuración de un servidor DNS externo en una o mas computadoras en la LAN.

Opcional:

Configuración de uno o varios servidores DNS locales y en la misma computadora un cache externo, que envía sus queries al servidor local y a los otros caches externos.

3.3. LAN con conexión externa

Es como la configuración opcional en 3.2. Los cachés externos además de enviar queries a los servidores de la LAN envían queries a cachés externos.

Este escenario en muchos casos es reducido de tal forma, que todos los clientes locales de la LAN utilizan uno o varios cachés externos.

3.4. Dominio público

Configuración de uno o varios servidores DNS externos. Estos son consultados por cachés de dominios remotos sobre registros del dominio.

Configuración de uno o varios caches externos, estos son consultados por computadoras del mismo dominio.

3.5. Dominio público asegurado

La práctica común es, seccionar el dominio en una parte con contacto directo al Internet, incluyendo un gateway (pasarela) que contacta con una parte "interna" del dominio. El gateway restringe el acceso de computadoras de dominios remotos a las computadoras "internas" realizando así la función de un *firewall*.

La configuración del DNS es idéntico a 3.4, con la salvedad que los servidores y uno o más cachés externos están detrás del firewall en la parte "interna". El firewall permite a todos los clientes, internos o del Internet remoto acceso a los cachés externos.

4. Redundancia

Hay básicamente dos razones por los cuales se introducen servidores de bases de datos redundantes:

- Si uno de ellos falla, uno de los servidores redundantes puede asumir el servicio y
- Se puede distribuir la carga de solicitudes a dos o más servidores y de esta manera acelerar el acceso de los clientes a la información requerida.

La parte negativa de la redundancia es, que hay que mantener copias idénticas de la información en todo servidor redundante. Este corresponde a mayor trabajo administrativo y riesgo adicional de fallas.

La mejor práctica es, utilizar un mecanismo automatizado para la actualiqzación de un dominio, e incluir en este la duplicación de los datos en los servidores secundarios con cada cambio realizado.

La transferencia de los archivos necesarios debe hacerse con un programa que no permite la modificación involuntaria de su contenido - ejemplo: ssh. Para minimizar la cantidad de información transferida se puede usar un programa de compresión y/o transferencia diferential, ejemplo: rsync. En una sola frase:

rsync bajo ssh es actualmente la mejor forma de actualizar datos remotos de manera confiable.

Tradicionalmente se realiza esta duplicación mediante "transferencias de zonas" (zone transfer) a través de un protocolo que es parte del sistema DNS. Este protocolo no es eficiente ni confiable.

5. BIND, djbdns y otro(s)

El programa "oficial" para el servicio DNS en Internet es BIND - Berkeley Internet Name Daemon. BIND combina la función de servidor y caché en un solo programa. En toda la historia de su desarrollo se han visto problemas de seguridad y problemas de fiabilidad.

Dan Bernstein es el autor del paquete de programas djbdns, que son optimizados en seguridad, velocidad y fiabilidad. djbdns separa las tareas de servidor DNS y caché (nameserver) en diferentes programas. La configuración de djbdns es completamente diferente a la de BIND y requiere aprendizaje desde cero, una desventaja para administradores que conocen este primer programa bien.

Existe por lo menos otra alternativa: maradns que provee también un servidor DNS diseñado para seguridad.

6. Referencias

Existe una gran cantidad de literatura en papel y en forma electrónica sobre DNS. Para la documentación oficial de BIND recomiendo visitar las páginas Web de los servidores sam.uni.edu.ni, magma.com.ni, loghog.uni.edu.ni y visitar el directorio doc/bind-doc.

La página Web de Daniel Bernstein, que tiene una excelente y compacta discusión de DNS, BIND y sus problemas se encuentra en junto con mucha otra información valiosa.

Linux-Howtos (también en los servidores arriba mencionados en doc/HOWTO/)

http://axs.org/~cp/DNS.html

http://www.dns.net/dnsrd/docs/

http://www.psionic.com/

7. Copias y Legalidades

 Cabe señalar, que prácticamente toda la información brindada aquí es extraída de fuentes externos, como los creadores de Internet y las personas que lo siguen desarrollando. Newton decía "Si veo lejos es, porque estoy sentado en los hombros de gigantes.

El documento fue elaborado durante una asesoría para la Universidad Nacional de Ingeniería y el proyecto ICT financiado por SIDA - Suecia, y forma parte de la documentación elaborado a fin de proveer información y formación básica a todo el equipo de trabajo y al grupo meta involucrado.

Puede bajarlo en formato PDF (Acrobat) aquí, o en formato html empacado en un archivo zip.