T2 – Domain Name System

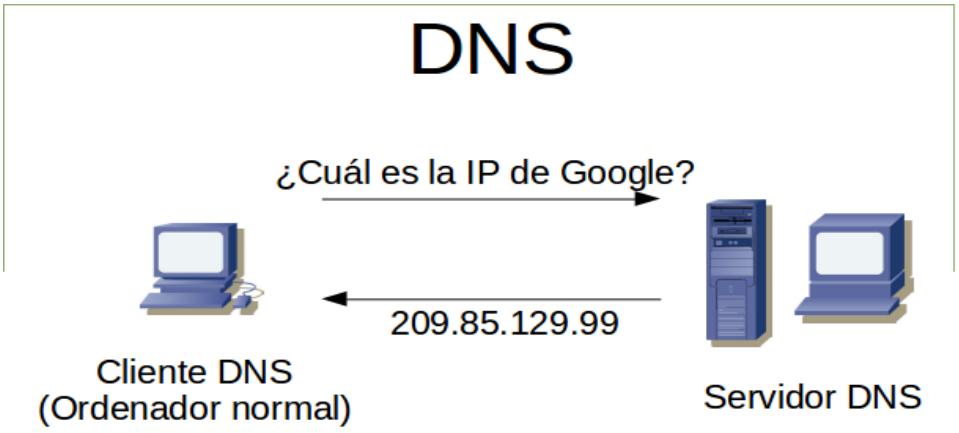
Domain Name System (DNS)	
Función	Resolución (traducción) de nombres de dominio a direcciones IP
Puertos	53/UDP (Normalmente), 53/TCP

Ubicación en la pila de protocolos

Aplicación	DNS
Transporte	TCP o UDP
Red	IP (IPv4, IPv6)

Estándares
RFC 1034 (1987) RFC 1035 (1987)

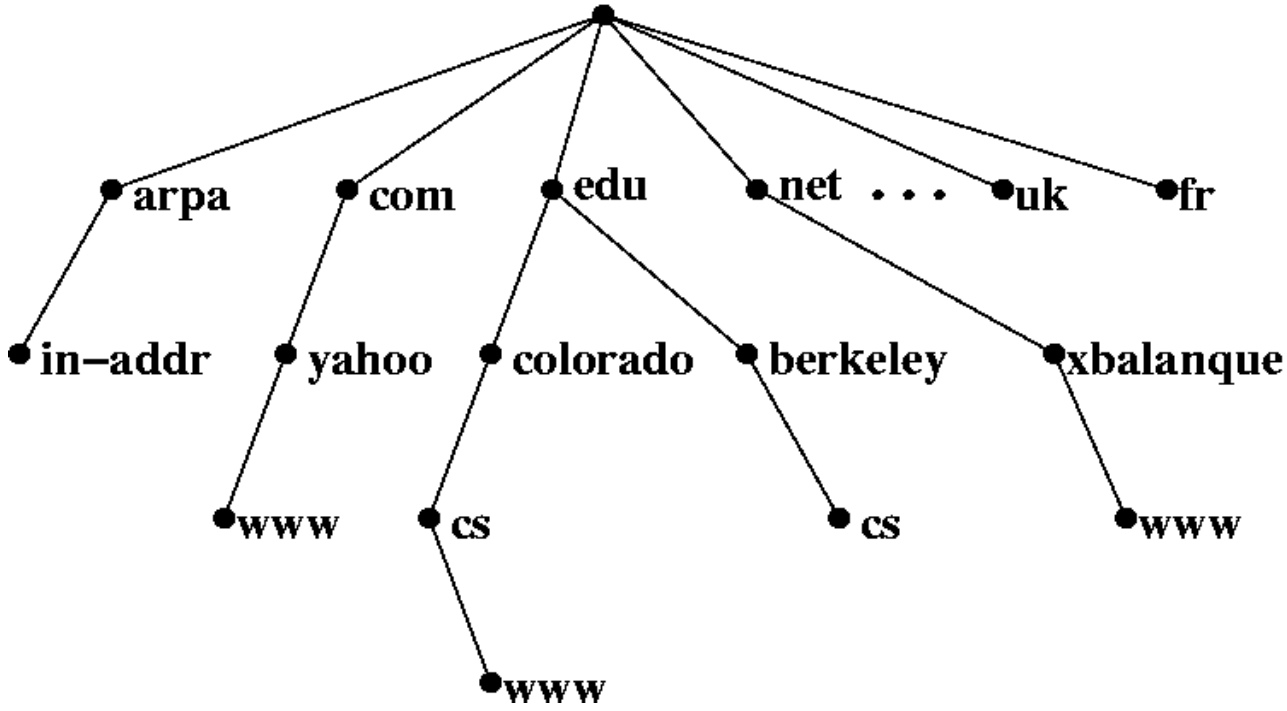
Domain Name System o ***DNS*** (Sistema de Nombres de Dominio). Su función principal es traducir o resolver un nombre DNS (fácil de recordar para las personas) en la dirección IP que tiene el equipo, con el propósito de poder localizar y acceder a ese equipo.



El servidor DNS utiliza 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 diferentes 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.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio FTP de winzip.com es 200.64.128.4, la mayoría de la gente llega a este equipo especificando ftp.winzip.com 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, el DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet. En un inicio, se utilizaba un archivo llamado *HOSTS* que contenía todos los nombres de dominio conocidos. El crecimiento explosivo de la red causó que el sistema de nombres centralizado en el archivo hosts no resultara práctico y en 1983, Paul V. Mockapetris publicó los RFC 882 y RFC 883 definiendo lo que hoy en día ha evolucionado hacia el DNS moderno (estos RFC han quedado obsoletos por la publicación en 1987 de los RFC 1034 y 1035).



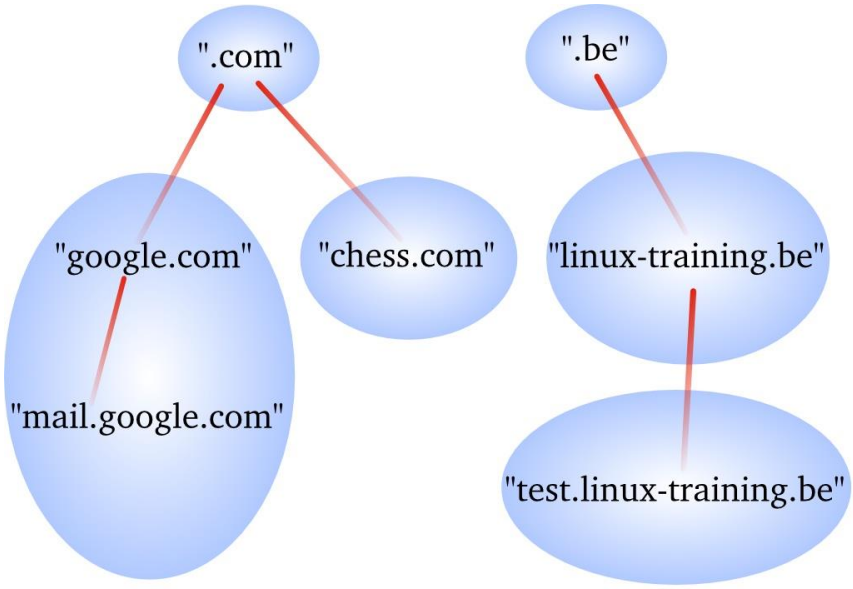
Componentes

Para la operación práctica del sistema DNS se utilizan tres componentes principales:

- Los **Clientes**: Un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS.
- Los **Servidores DNS**: Contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.

- Y las **Zonas de autoridad**. Una zona de autoridad es una parte del espacio de nombres de dominio sobre la que es responsable un servidor DNS. (Por ejemplo: futbol.com, araba.euskotren.eus, sonido.net, etc.)

En la siguiente imagen, cada uno de los globos azules sería una zona de autoridad.



Entendiendo las partes de un nombre de dominio

Un nombre de dominio usualmente consiste en dos o más partes (técnicamente «etiquetas»), separadas por puntos cuando se las escribe en forma de texto. Por ejemplo, www.example.com o es.wikipedia.org

- A la etiqueta ubicada más a la derecha se le llama **dominio de nivel superior** (en inglés *top level domain*). Como .**com** en www.ejemplo.com o **org** en es.wikipedia.org
- Un **dominio de segundo nivel** (a menudo llamado simplemente **dominio**) consiste en una etiqueta a la izquierda del dominio de primer nivel, por ejemplo: moda.net, futbol.com, alegria.org
- También puede haber una etiqueta a la izquierda del dominio, con lo que tenemos un **subdominio**. Esta subdivisión puede tener hasta 127 niveles, y cada etiqueta puede contener hasta 63 caracteres, pero restringidos a que la longitud total del nombre del dominio no exceda los 255 caracteres, aunque en la práctica los dominios son casi siempre mucho más cortos.
- Finalmente, la parte más a la izquierda del nombre DNS suele expresar el nombre de la máquina (en inglés *hostname*) o el servicio que da. El resto del nombre de dominio simplemente especifica la manera de crear

una ruta lógica a la información requerida. Por ejemplo, en el nombre DNS www.elorrieta.com, www hace referencia al servicio que se ofrece.

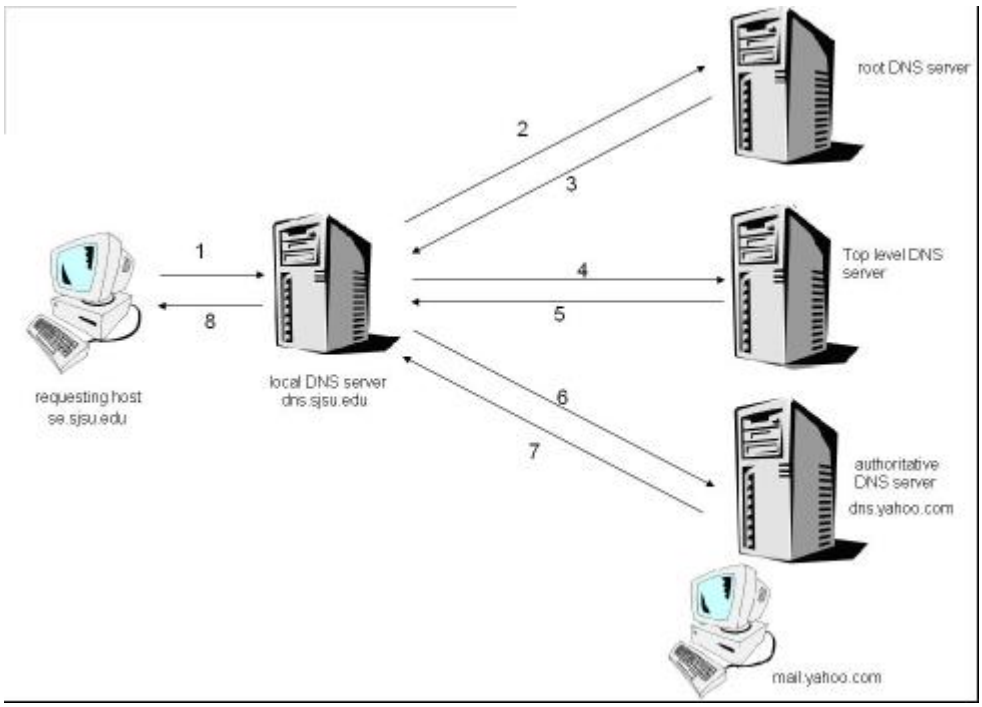
El DNS consiste en un conjunto jerárquico de servidores DNS. Cada dominio o subdominio tiene una o más **zonas de autoridad** que publican la información acerca del dominio y los nombres de servicio.

En el nivel más alto de la jerarquía de servidores DNS están los 13 servidores raíz. Esos servidores, distribuidos por todo el mundo (como se ve en el mapa),

responden a las consultas no con la IP final que buscamos, sino que nos dirigen a otro servidor de menos nivel que sabe más sobre lo que preguntamos. Por ejemplo, si preguntamos por la IP de **www.historia.com** a un servidor raíz, nos dará la dirección del servidor DNS que se encarga de los **.com**.

Cuando preguntemos a ese servidor DNS encargado de los .com, nos remitirá al servidor DNS autoritativo para la zona **historia.com**.

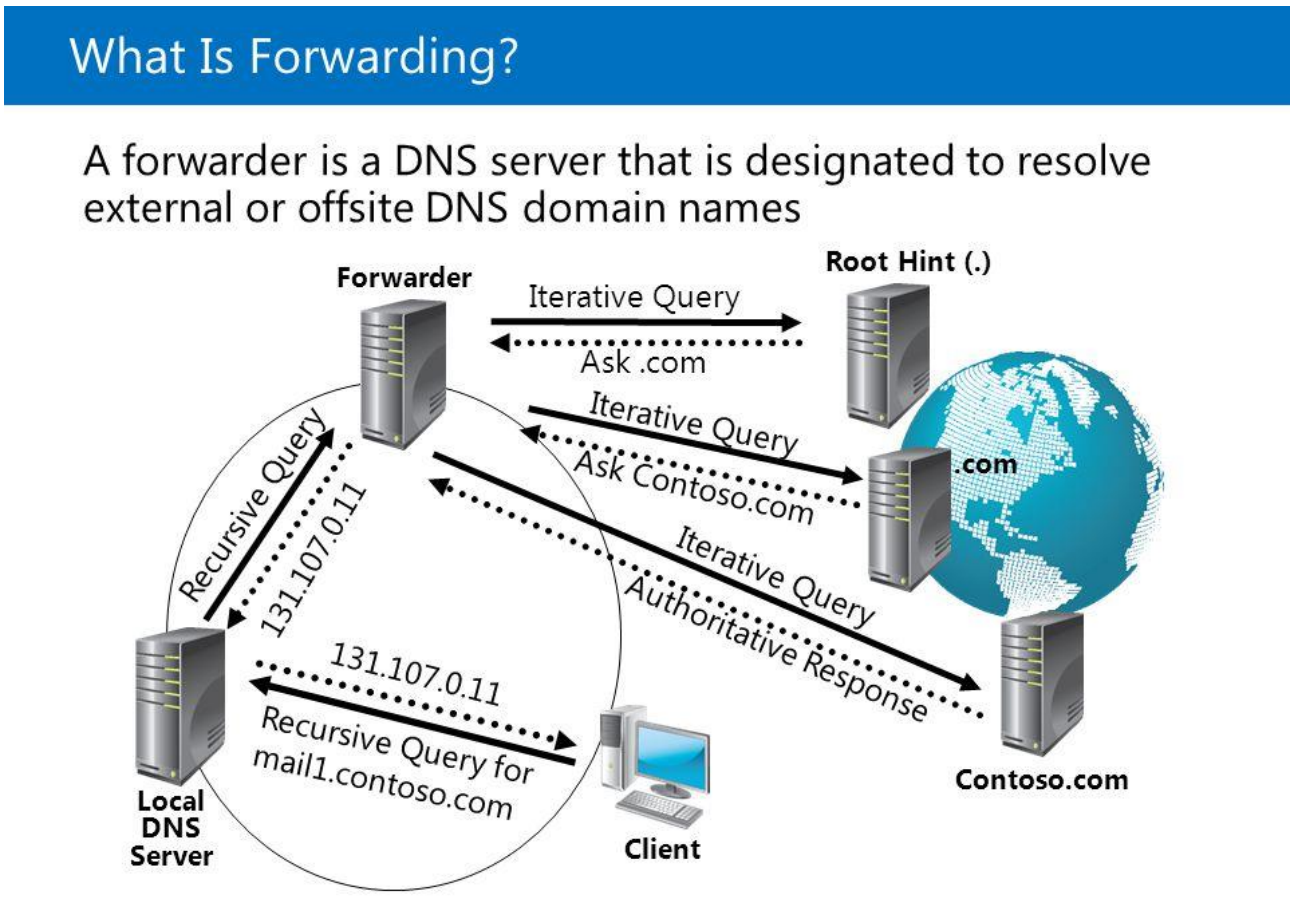
Por fin, preguntaremos al servidor DNS que guarda historia.com y nos dará la IP de **www.historia.com**



Reenviadores

Cuando el servidor DNS sólo puede consultar a los servidores DNS raíz, tiene que hacer muchas consultas y a menudo no obtiene una respuesta en un tiempo prudencial.

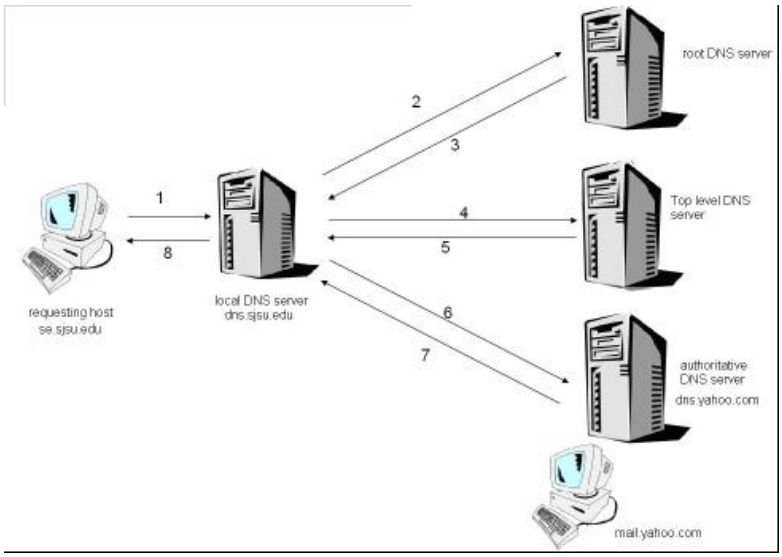
Para mejorar la situación, es habitual configurar en el servidor DNS los llamados reenviadores o forwarders. Cuando existen, el servidor DNS les preguntará a ellos en vez de ir a la raíz.



Tipos de resolución de nombres de dominio

Existen dos tipos de consultas que un cliente o servidor DNS pueden hacer a otro servidor DNS, la iterativa y la recursiva.

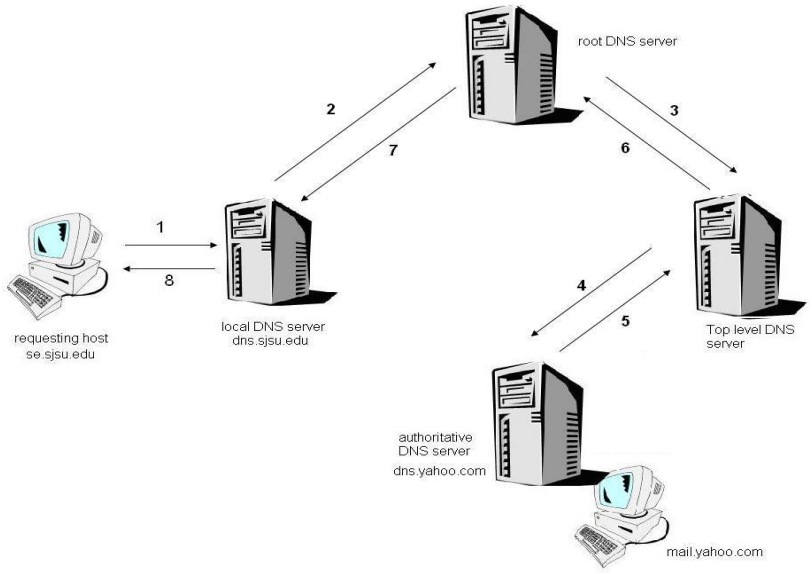
Resolución iterativa



En la resolución iterativa, cuando el servidor DNS pregunta al servidor raíz, este le remite al servidor DNS de siguiente nivel y así sucesivamente.

En este caso, el que hace la pregunta acepta “la mejor respuesta” que el preguntado pueda darle, aunque no sea la que buscaba inicialmente, y con ella volverá a preguntar.

Resolución recursiva



En la resolución recursiva, cada servidor DNS al que preguntamos busca la respuesta final, aunque él tenga que preguntar a otros.

En este caso, el que pregunta sólo acepta la respuesta final o un mensaje de error indicando que no ha sido posible.

Las consultas recursivas entrañan una cierta peligrosidad para el servidor DNS.

Por ello, en el improbable caso de que nuestro servidor DNS de servicio a redes externas, debemos deshabilitar las consultas recursivas. De hecho, el Bind9 que se instala en Debian 8, tiene por defecto deshabilitadas las consultas recursivas.

Tipos de servidores DNS

- **Primarios o maestros:** Guardan los datos de un espacio de nombres en sus ficheros.
- **Secundarios o esclavos:** Obtienen los datos de los servidores primarios a través de una transferencia de zona.
- **Caché:** No contienen ninguna zona, ningún dato “propio”. Cuando se les realiza una consulta, consultan a su vez a los servidores DNS correspondientes, almacenando la respuesta en su base de datos para agilizar la respuesta a esa misma petición en el futuro continuo.

Tipos de registros DNS

- **A** = Address – (dirección) Este registro se usa para traducir nombres de servidores de alojamiento a direcciones IPv4.
- **AAAA** = Address – (dirección) Este registro se usa en IPv6 para traducir nombres de hosts a direcciones IPv6.
- **CNAME** = Canonical Name – (nombre canónico) Se usa para crear nombres de servidores de alojamiento adicionales, o alias, para los servidores de alojamiento de un dominio. Es usado cuando se están corriendo múltiples servicios (como FTP y servidor web) 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 corres múltiples servidores HTTP, con diferentes nombres, sobre el mismo host. Se escribe primero el alias y luego el nombre real. Ej. Ejemplo1 IN CNAME ejemplo2
- **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 nombre de dominio a una lista de servidores de intercambio de correo para ese dominio. Tiene un balanceo de carga y prioridad para el uso de uno o más servicios de correo.
- **PTR** = Pointer – (indicador) También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio. Se usa en el archivo de configuración del DNS reversiva.

Herramientas para consultas DNS

Hay muchas, como la veterana **nslookup**, o la mejor considerada **dig**. Algunos ejemplos de uso:

- nslookup www.marca.com -> pregunta al servidor DNS configurado en nuestro ordenador sobre www.marca.com

- nslookup www.marca.com 8.8.8.8 -> pregunta al servidor DNS 8.8.8.8 sobre www.marca.com

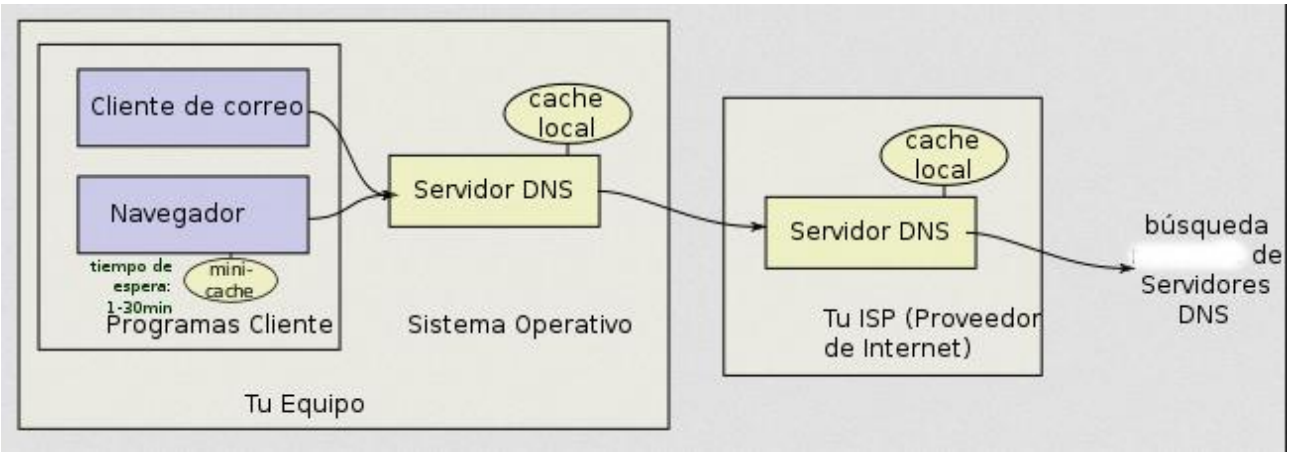
- dig www.marca.com -> pregunta al servidor DNS configurado en nuestro ordenador sobre www.marca.com

- dig @8.8.8.8 www.marca.com -> pregunta a Google Public DNS (8.8.8.8) sobre www.marca.com
- dig @8.8.8.8 www.marca.com MX -> pregunta a Google Public DNS (8.8.8.8) cuál es el servidor de correo de www.marca.com
- dig @8.8.8.8 www.marca.com AAAA -> pregunta a Google Public DNS (8.8.8.8) cuál es la IPv6 de www.marca.com

DNS en el mundo real

Los usuarios generalmente no se comunican directamente con el servidor DNS: la resolución de nombres se hace de forma transparente por las aplicaciones del cliente (por ejemplo, navegadores, clientes de correo y otras aplicaciones que usan Internet). Al realizar una petición que requiere una búsqueda de DNS, la petición se envía al servidor DNS local del sistema operativo. El sistema operativo, antes de establecer alguna comunicación, comprueba si la respuesta se encuentra en la memoria caché. En el caso de que no se encuentre, buscará la resolución en el fichero HOSTS del sistema y, si tampoco está ahí, la petición se enviará a uno o más servidores DNS.

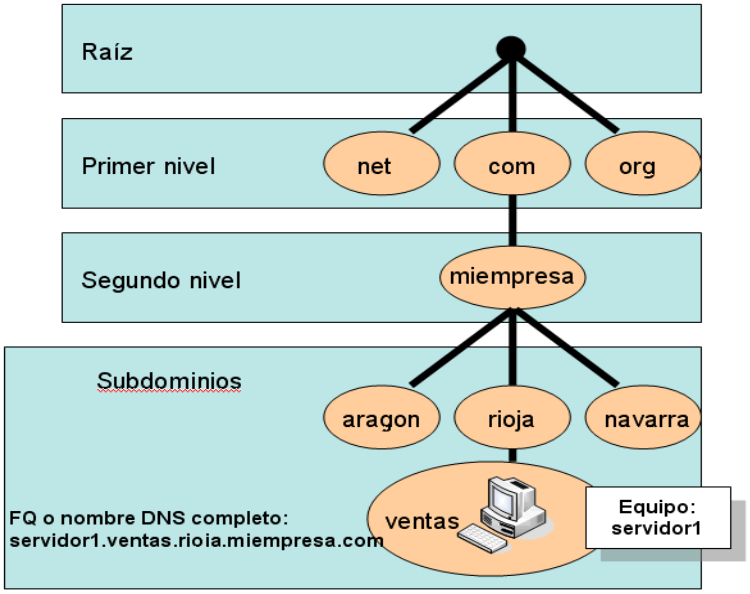
La mayoría de usuarios domésticos utilizan como servidor DNS el proporcionado por el proveedor de servicios de Internet. La dirección de estos servidores puede ser configurada de forma manual o automática mediante DHCP. Pero cada vez es más habitual que los administradores de red configuren sus propios servidores DNS (los de Google 8.8.8.8 y 8.8.4.4, los de OpenDNS 208.67.222.222 y 208.67.220.220, etc.)



En cualquier caso, los servidores DNS que reciben la petición, buscan en primer lugar si disponen de la respuesta en la memoria caché. Si es así, sirven la respuesta; en caso contrario, iniciarían la búsqueda de manera recursiva. Una vez encontrada la respuesta, el servidor DNS guardará el resultado en su memoria caché para futuros usos y devuelve el resultado.

Es importante añadir que el protocolo DNS generalmente transporta las peticiones y respuestas usando UDP, protocolo mucho más rápido que TCP. Hay algunas ocasiones en las que se usa TCP, como por ejemplo cuando DNS necesita enviar respuestas mayores de 512 bytes (límite de UDP) o cuando se realiza una transferencia de zona entre dos servidores, donde se utiliza TCP por razones de fiabilidad.

Jerarquía DNS



El espacio de nombres de dominio tiene una estructura arborescente. Las hojas y los nodos del árbol se utilizan como etiquetas de los medios. Un nombre de dominio completo de un objeto consiste en la concatenación de todas las etiquetas de un camino, separadas por puntos. Un nombre de dominio termina con un punto (aunque este último punto generalmente se omite, ya que es puramente formal). Un **FQDN** correcto (también llamado Fully Qualified Domain Name), es por ejemplo este: www.example.com. (incluyendo el punto al final).

Un nombre de dominio tiene una longitud máxima de 255 caracteres.

Los objetos de un dominio DNS (por ejemplo, el nombre del equipo) se registran en un archivo de zona, ubicado en uno o más servidores de nombres.

Links útiles

Como usar el comando NSLOOKUP en Windows, ejemplos prácticos

https://norfipc.com/redes/como-usar-comando-nslookup-windows.html