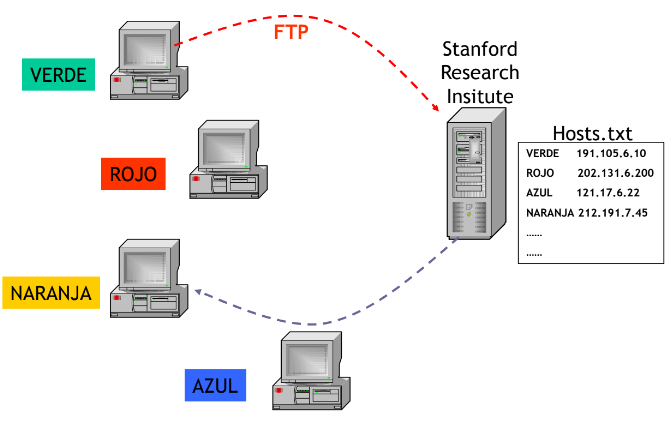
DNS

Domain name system.



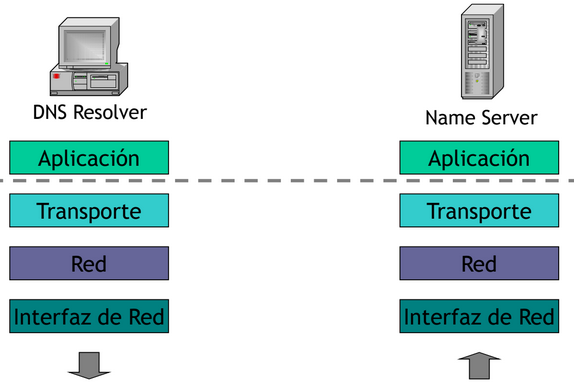
El Sistema de Nombres de Dominio o DNS es un **sistema de nomenclatura jerárquico** que **se ocupa de la administración del espacio de nombres de dominio** (Domain Name Space).

Su labor primordial **consiste en resolver las peticiones de asignación de nombres**. **Traduce un dominio en una IP**. Por ejemplo la ip de [www.ejemplo.es](http://www.ejemplo.es/) es 93.184.216.34.

**Es una base de datos distribuida y un espacio de nombres jerárquico. Todo host tiene configurado un servidor de nombres.**

El **sistema es cliente-servidor** y está **compuesto** **por**:

* **Resolvers:** **envía el pedido** de resolución entre la aplicación y el servicio de nombres. Es el cliente.
* **Name servers: reciben el pedido y resuelven el nombre** de Host a una dirección IP. Es el servidor.

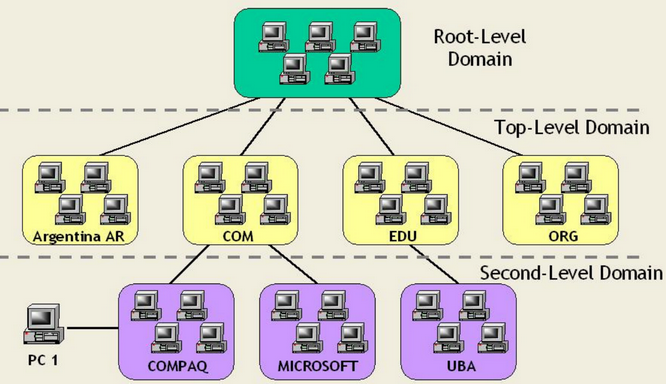


# Espacio de nombres jerárquicos

El espacio de nombres está construida en una estructura jerárquica de árbol.

|  |  |  |
| --- | --- | --- |
| Nivel | Explicación | Ejemplo |
| Root-level | Sin etiqueta | . |
| Top level | Terminación | .edu, .ar, .com, etc. |
| Second level | Pueden contener hosts u otros subdominios | Microsoft.com |
| Host names | Nombre completo | Sistemas.frba.utn.edu.ar |

* **Root-level domain:** es lo más alto de la jerarquía. Este nivel no utiliza una etiqueta, pero puede identificarse con el “.”. En realidad, aunque no lo escribamos, todo dominio tiene un punto al final. Por ejemplo “google.com.”.
* **Top-level domain:** es como termina, por ejemplo com, edu, ar, etc.
* **Second-level domain:** pueden contener host u otros dominios llamados sub-dominios. Por ejemplo el dominio microsoft.com puede poseer hosts: [ftp.microsoft.com](ftp://ftp.microsoft.com/) o subdominios como dev.microsoft.com. Para dar de alta un dominio se debe ir al proveedor top-level y registrar mi dominio.
* **Host names:** Es el **nombre completo**, se le suele decir **Fully Qualified Domain Name** (**FQDN**). Ejemplo sistemas.frba.utn.edu.ar



Sistema en forma de árbol. Se delega a cada entidad la administración del espacio de nombres. Incluyendo UTN, que es responsable de administra todo lo que es utn.edu.ar.

# Zonas de autoridad

Hay un servidor que es responsable del archivo de zonas.

Es una porción de dominio por la cual un servidor es responsable. Por ejemplo por edu.ar.

El DNS server responsable de la zona posee el archivo de la zona X que contiene la asociación nombre → IP para ese dominio.

Un único server puede mantener múltiples zonas.

En la práctica, hay infinitos root servers, distribuidos y replicados en todo el mundo. Un DNS tiene autoridad sobre una zona cuando posee el archivo de la zona (archivo que mapea un nombre a una IP).

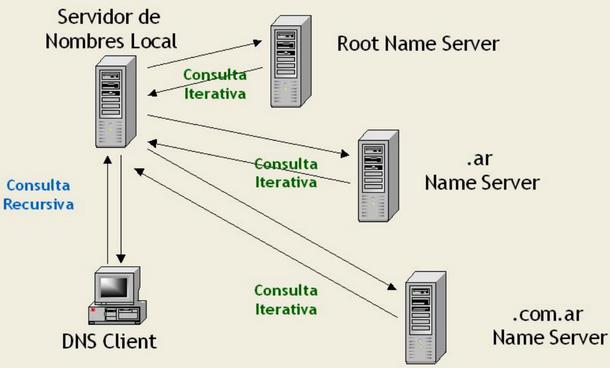
Un servidor DNS tiene que estar siempre activo para resolver las IP. Suelen administrar muchas zonas (de muchos clientes)

# Roles de los servidores DNS

* **Primary name server:** Los archivos de información originales de la zona se almacenan localmente.
* **Secondary name server:** Obtiene la información de zona de un master name server. Replican esa información (el original) para evitar un único punto de falla.
* **Master name server:** Fuente de información para un secondary server. Pueden ser Primary o Secondary servers.
* **Caching only:** No almacena información de zona. Lo que hacen es atender a consultas. Cachean las respuestas durante un tiempo que se lo da el servidor que le dio esa asociación. (el proveedor de internet ofrece dos servidores de dominio, que yo luego uso para resolver dominios).

# Resolución de nombres

La resolución de nombres convierte un nombre en una IP.



Si no tiene cacheado el dominio el servidor de nombres local, le pregunta por ejemplo por sistemas.utn.edu.frba.ar a root name server, este no lo sabe pero le dice que se fije en .ar name server y asi (esto es una consulta iterativa).

* Tipos de consultas:
* **Consulta recursiva:**   
  Quién consulta? una terminal le consulta al servidor de nombres local.  
  El servidor de nombres (recursivo) consultado está obligado a responder con los datos o con un error. Hace una serie de consultas hasta que obtienen la respuesta final (nunca una mera “pista”) o responden con un error. En caso de error, no se sigue consultando.  
  La respuesta puede estar cacheada o requerir muchas consultas.
* **Consulta iterativa:**Quién consulta? El servidor de nombres local a otros servidores de nombres?  
  El servidor consultado responde con su mejor respuesta, que no necesariamente es final. Puede ser el nombre resuelto o una referencia a otro servidor de nombres, de menor nivel, que pueda responder la consulta. (Va de root, navegando el árbol, buscando la respuesta final)
* **Consulta inversa**: El resolver solicita el nombre de Host asociado a una IP dada.

# Caching y TTL

(El ISP me suele dar un servidor de caching)

Los DNS Servers cachean las consultas iterativas. Cada entrada en cache tiene asociado un tiempo de vida (TTL), cuando este expira, la entrada es borrada. Ese TTL indica por cuánto tiempo sigue siendo válida la entrada, así el consultante no vuelve a consultar hasta que termine el TTL.

El TTL remanente es enviado al Resolver cuando se responde una consulta recursiva.

# Protocolos y puertos

El servicio DNS server escucha peticiones en el puerto 53, tanto de TCP como UDP (capa 4).

La **petición se realiza en UDP**. Si se recibe una respuesta truncada, se realiza nuevamente usando TCP.

# Resource records

En el archivo que esta almacenada la asociación de nombre e IP hay diferentes entradas:

* **Host Record (A):** asocia estáticamente un **nombre de un host con una dirección IP.** Comprende la mayor parte del archivo y lista todos los hosts dentro de la zona. Ejemplos:
  + www IN A 200.69.225.145: dice que www. se traduce a esa IP.
  + rhino IN A 200.26.65.12: dice que rhino se traduce a esa IP.
* **Mail exchange (MX):** asocia un **dominio de email con la dirección de los servidores de correo**. Ejemplos:
  + @ IN MX [10] mailhost: le pregunta la ip al servidor DNS de un registro MX de tal casilla mailhost.
  + @ IN MX [20] mail1.infovia.com.ar
* **Canonical name (CNAME):** permiten asociar **más de un nombre de Host a una única dirección IP (alias).** Ejemplos donde muestra que puedo conectarme a Rhino con esos dos alias.
  + Fileserver1 CNAME Rhino
  + ftp CNAME Rhino

# Registro de nombres

La administración local de TLD .ar lo realiza Cancilleria (MRECIC) en [www.nic.ar](http://www.nic.ar/).