JUSTIFICACIÓN DE DNS

PUEDE UTILIZARSE PARA REFERENCIAR SERVICIOS Y OTROS ELEMENTOS EN EL AMBITO DEL NOMBRE DE DOMINIO DEPENDIENDO DEL TIPO DE REGISTRO

- A => asociamos un nombre a una dirección IPv4
- AAA => asociamos un nombre a una dirección IPv6
- CNAME => cuando hay varios nombres de dominio apuntan a una única dirección IP
- NS => especificación de los servidores DNS
- SRV => referencia un servicio (dominio) a un nombre de nuestra red
- MX => referencia los servidores de correo
- PTR => resolución de IPv4 a un nombre de dominio

Características y utilidad del servicio DNS

DNS ofrece un servicio de almacenamiento y consulta de información

Descentralizado. La información se guarda en una base de datos distribuida entre múltiples equipos (servicios de nombres) y se indexa según un esquema de nombres jerárquico (espacio de nombres de dominio).

A los servidores de nombres se le pueden realizar preguntar y para ello, se usan programas (clientes DNS) que dialogan con los servidores en base a unas reglas (protocolo DNS).

Componentes

El servicio DNS se basa en los siguientes componentes

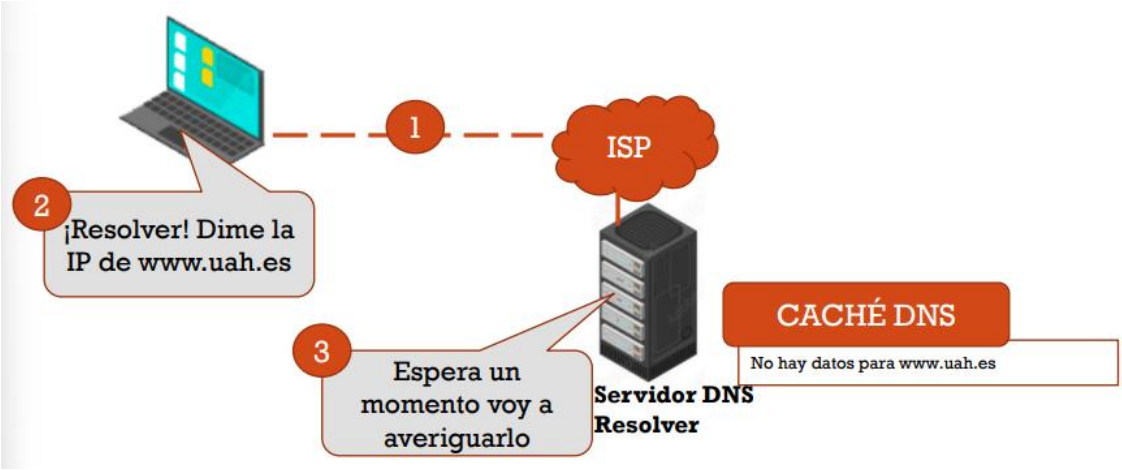
- **Espacio de nombres de dominio (Domain Name Space):** Conjunto de nombres que se pueden utilizar para identificar maquinas o servicios de una red
- **Bases de datos DNS:** Base de datos distribuida y redundante que almacena información sobre los nombres de dominio. Esta base de datos se organiza en **zonas** que almacenan la información en lo que se conoce como **registro de recursos** (RR, Resource Records).
- **Servidores de nombres (name servers) o servidores DNS:** Programas que guardan parte de la base de datos DNS (zonas) y que responden a preguntas sobre la información almacenada.
- **Clientes DNS (resolvers):** Programas que realizan preguntas a los servidores de nombres y procesan las respuestas para ofrecerle la información a los usuarios y/o a las aplicaciones que los invocan.
- **Protocolo DNS:** Conjunto de normas y reglas en base a las cuales “dialogan” los clientes y servidores DNS.

Funcionamiento

Se basa en el modelo cliente/servidor.

- **Los clientes DNS (resolvers)** preguntan a los servidores de nombres.
- **Los servidores** de nombres también se comunican entre sí:
    - Pueden realizar preguntas a otros servidores de nombres cuando no tienen la información por la que le han preguntado.
    - Pueden intercambiar información sobre sus zonas (transferencia de zona).

El usuario escribe en su navegador www.uah.es. El ordenador busca en su memoria caché si esta la dirección IP de www.uah.es En este caso, es la primera vez y no hay datos. Por lo tanto, debe pedir ayuda.

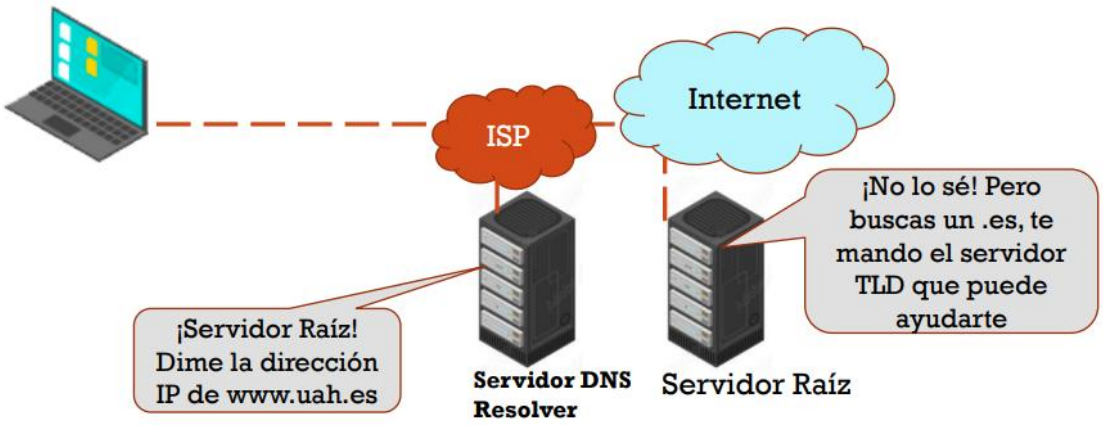


El ordenador acude al Resover, servidor DNS local que normalmente corresponde con el servidor DNS del ISP (Proveedor Servicio Internet). Le preguntara por la IP de www.uah.es El servidor, al recibir la petición, le pide que espere y pregunta en su caché. No tiene el dato en caché y debe acudir al servidor raíz

SERVIDOR RAÍZ

Es un servidor de nombres para la zona raíz del sistema de nombres de Dominio en Internet. Existen 13 servidores raíz específicos

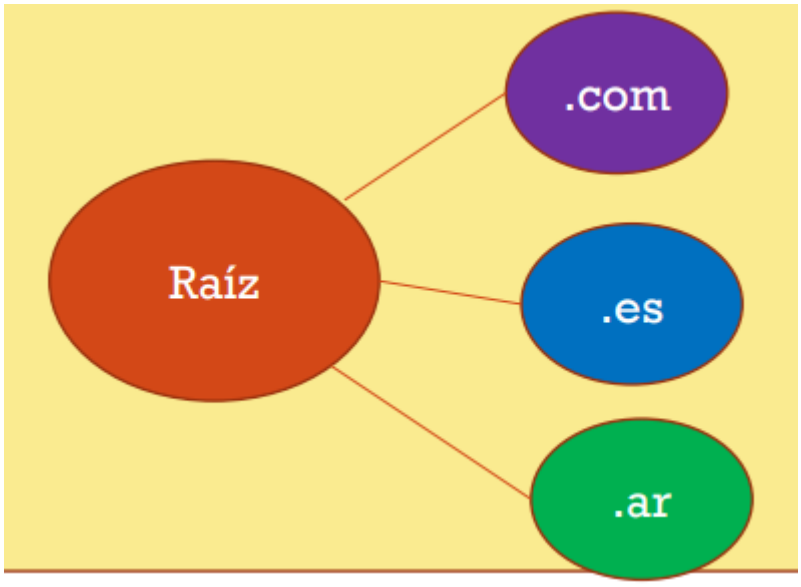
El ordenador acude al Resolver, servidor DNS local que normalmente corresponde con el servidor DNS del ISP (Proveedor Servicio Internet). Le preguntara por la IP de www.uah.es El servidor, al recibir la petición, le pide que espere y pregunta en su caché. No tiene el dato en caché y debe acudir al servidor raíz



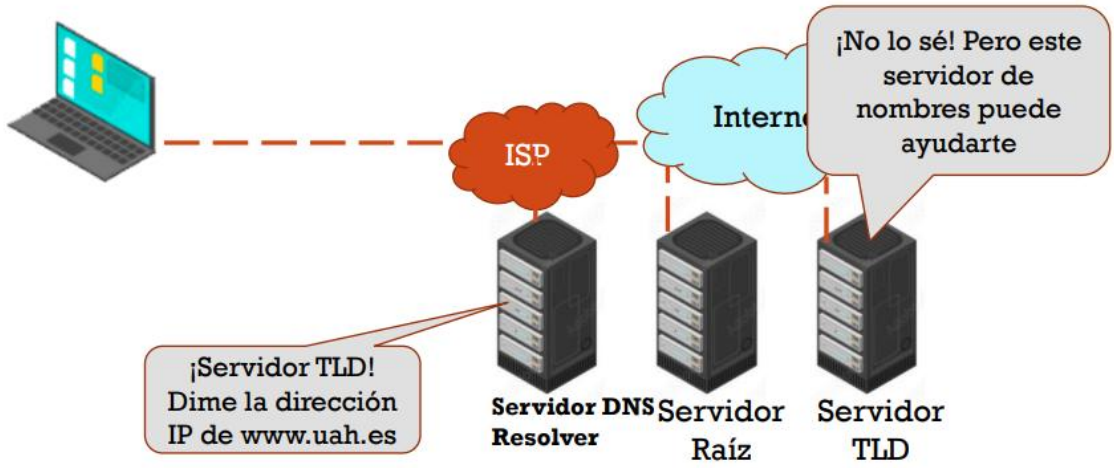
El Resolver no tuvo respuesta en su caché y consulta al Servidor Raíz, la función del servidor raíz no es guardar la IP de un servidor especifico, pero como ve que está pidiendo un dominio del tipo . es la da la IP del servidor TLD (Top Level Domain) que le puede ayudar

Servidor TLD (Top Level Domain)

Conjunto de servidores que almacenan direcciones de dominio de nivel superior, como .com .net .org



El Resolver no tuvo respuesta en su caché y consulta al Servidor Raíz, la función del servidor raíz no es guardar la IP de un servidor especifico, pero como ve que está pidiendo un dominio del tipo . es la da la IP del servidor TLD (Top Level Domain) que le puede ayudar

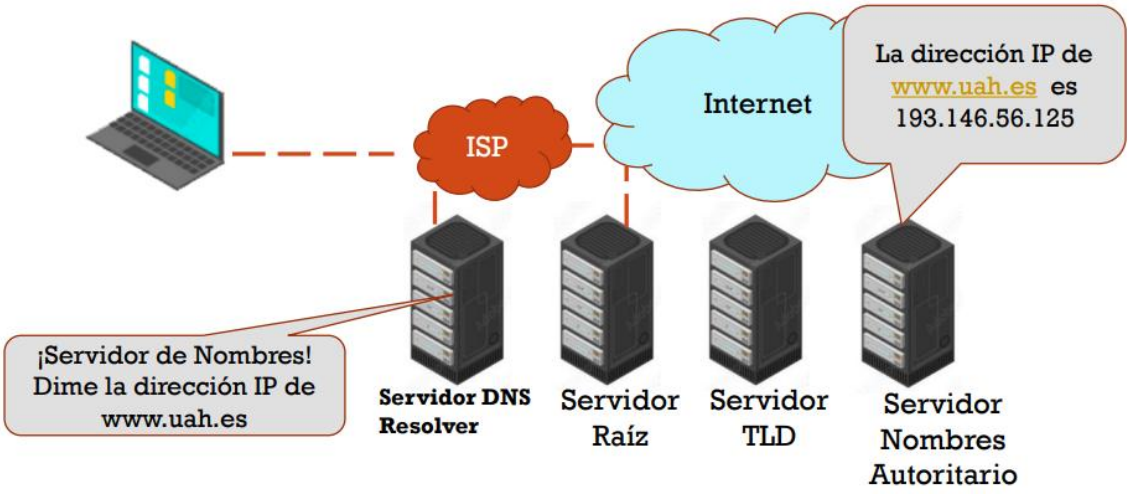


Una vez conectado con el servidor TLD pregunta por la IP. De igual manera que el paso anterior, como este servidor su función no es guardar las IPs de los sitios, le responde que no tiene esta información, pero le da la dirección del Servidor de Nombres Autoritarios que le puede ayudarle.

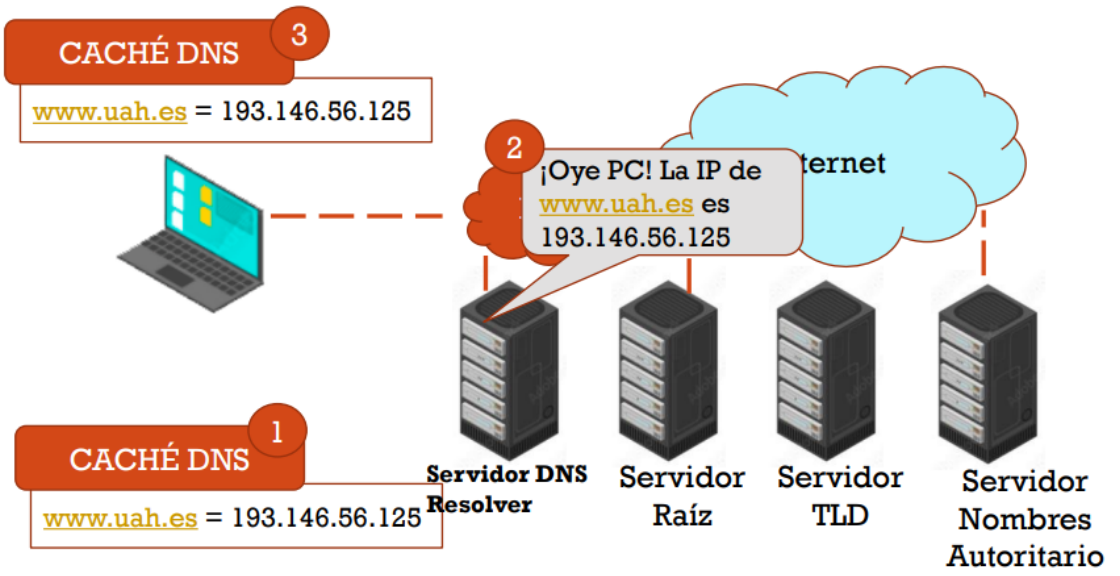
SERVIDOR DE NOMBRES AUTORITARIOS

Son servidores que almacenan información de direcciones IP de servidores específicos. Por ejemplo, el servidor de nombres autoritarios de uah.es tendría las direcciones IP de todos los servidores de uah.es

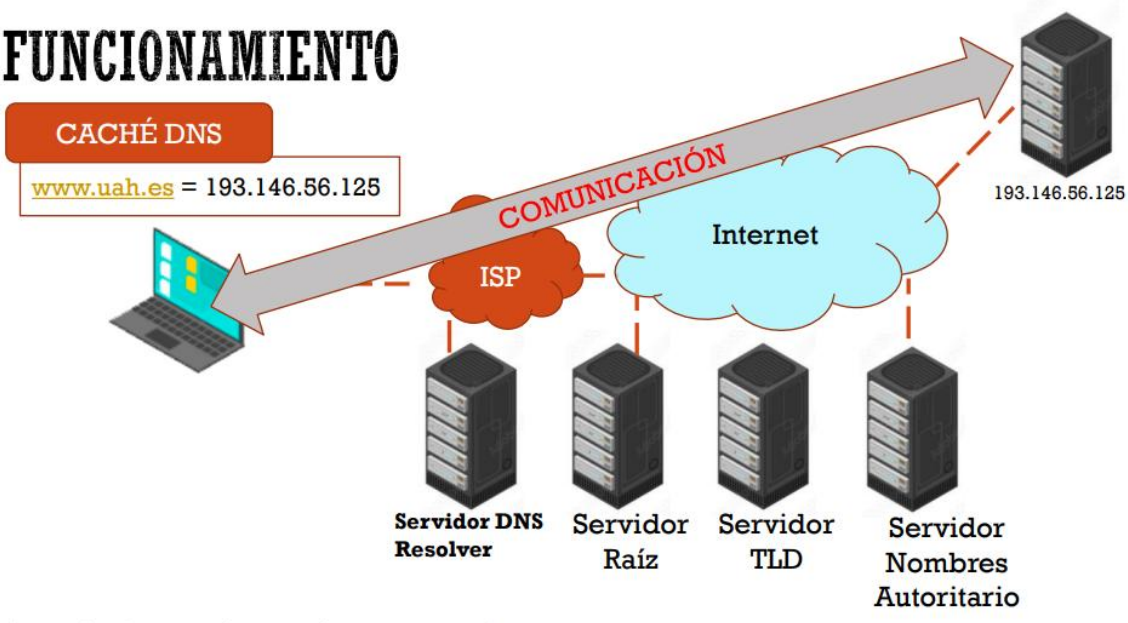
Una vez conectado con el servidor TLD pregunta por la IP. De igual manera que el paso anterior, como este servidor su función no es guardar las IPs de los sitios, le responde que no tiene esta información pero le da la dirección del Servidor de Nombres Autoritarios que le puede ayudarle.



Una vez conectado con el Servidor de Nombres Autoritario pregunta por la IP. Como la función de este servidor si es guardar las direcciones IPs de servidores específicos le responde con la dirección IP



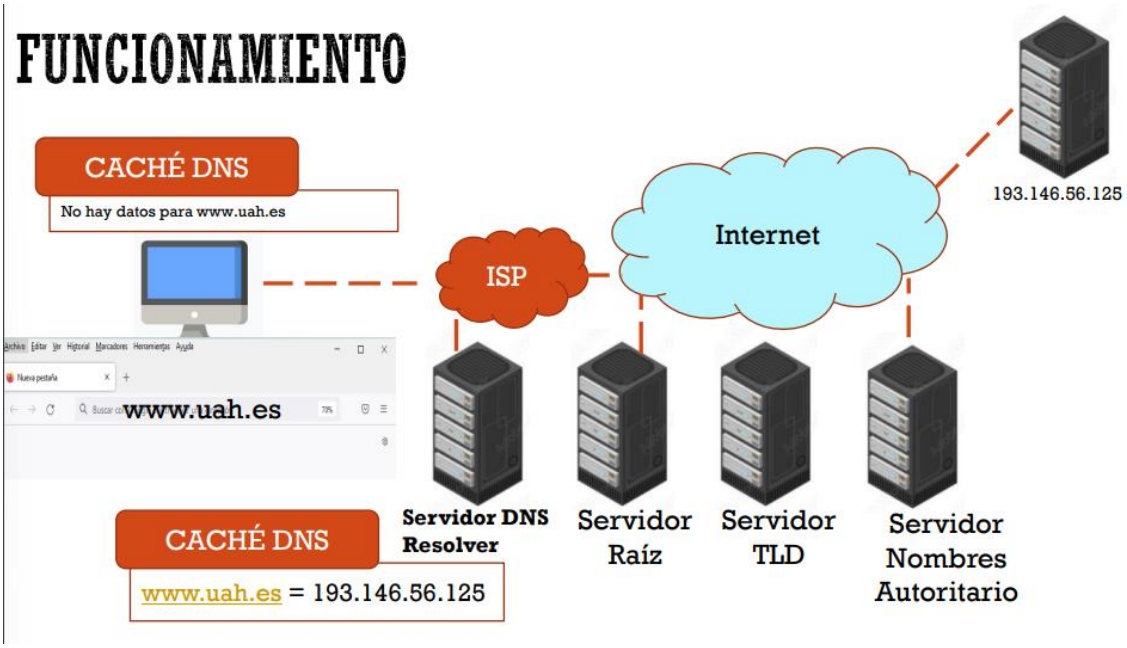
El resolver ya dispone de la dirección IP. Lo primero que hace es guardarla en su cache DNS y luego procede a informar de la petición. De la misma manera el ordenador guarda en su cache DNS la IP recibida



La máquina puede acceder a www.uah.es

Las próximas veces que vuelva a conectarse, no es necesario que consulte al Resolver porque ya dispone de esta información en su cache DNS

(esta cache no es permanente)



Supongamos que otro ordenador se conecta a www.uah.es. Su cache no tiene esta información y pide ayuda al Resolver. Este ya la tiene en su caché, por tanto, responde con la IP

- Con el comando nslookup podremos saber si el DNS está resolviendo correctamente los nombres y las IPs

Nombres de dominio

- El conjunto de nombres forma el denominado espacio de nombres de dominio que se puede representar mediante una estructura jerárquica organiza en forma de árbol. Cada nodo se separar de los otros nodos por un punto.
- Cada nombre de dominio puede estar formado por una o varias cadenas de caracteres separadas por puntos. No se distingue de mayúsculas ni de minúsculas.
- Puede tener un máximo de 63 caracteres y un mínimo de 2
- Solo pueden contener números, letras y guiones medios
- No se pueden empezar ni acabar con un guion
- Se pueden usar nombres que tengan como máximo 127 niveles y cada parte separada por un punto

- Ejemplos: “Google.es”

- La información DNS se distribuye en un gran numero de servidores en todo el mundo.
- Los servidores DNS se organizan en una estructura de árbol. Pueden ser:
    - **Servidores Raíz:** son 13. Conocen las direcciones IPs de los servidores TLD.
    - **Servidores Top Level Domain (TLD).** Cada servidor TLD conoce las direcciones IP de los servidores de nombres que resuelven sus dominios dentro de su propio dominio
    - **Servidores con autoridad.** Al menos 2 por ISP u organización. Almacenan la información sobre nombre de dominio y dirección IP, asociada a los hosts de la organización

Nombres de dominio

- Los nombres de dominio terminan en un ".·. esto es así porque el árbol de nombres de dominio empieza en el dominio "." Que se conoce como dominio raíz (realmente es un nombre nulo con 0 caracteres, pero se representa usando un ".").
- Como consecuencia de la organización jerárquica, es posible utilizar los términos dominio y subdominio. Por ejemplo, "Google.es" es un subdominio de "es."
- Los subdominios que cuelgan del dominio raíz se llaman de primer nivel o dominios de nivel superior (TLD, Top Level Domains).
- La información de los servidores raíz se puede encontrar en https://root-servers.org/
- En la parte inferior de la web se puede consultar la información de cada uno de estos 13 servidores raíz.
- Cada uno se identifica con las letras de "A" – "M"
- Todos ellos están replicados

Cuando se hace referencia a un dominio usando un nombre se puede emplear su nombre relativo o su nombre absoluto:

- **Nombre relativo:** Es necesario saber el contexto del dominio superior para determinar a que nombre se hacer referencia exactamente.
- **Nombres absolutos o completos** (**FQDN**, Fully Qualified Domain Names) : Nombre formado por todas las partes hasta el dominio raíz. El "." Final del dominio raíz permite distinguir si el nombre usado es FQDN o no. Normalmente no usamos él "." final de los FQDN en las aplicaciones, pero internamente si se utiliza

Nota: los usuarios no usamos el punto final de los nombres, pero internamente si se utiliza

Administración de nombres de dominio en internet. Delegación

La administración y organización del espacio de nombres de dominio de internet se distribuyes entre múltiples empresas y organizaciones, estando coordinada por la ICANN (Internet Corporation for Assigned Names and Numbers).

La ICANN es una organización sin ánimo de lucro que tiene el objetivo de garantizar que internet sea estable, operativa y segura.

Se encarga -entre otras- de administrar el dominio raíz y de mantener un registro de los dominios de nivel superior (TLD) existentes.

Servidores de nombres

Los servidores de nombres, también llamados servidores DNS, son programas que guardan información sobre nombres de dominio y responden a las preguntas que les realizan los clientes DNS y otros servidores de nombre. Almacenan, por tanto, una parte de la base de datos de DNS

Por defecto, escuchan en los puertos 53/TCP y 53/UDP.

ZONAS

- Los servidores de nombres mantienen información de una parte del espacio de nombres de dominio que se conoce como zona.
- Cuando un servidor DNS contiene una zona, se dice que es autorizado (authoritative) para esa zona
- Las zonas se almacenan en ficheros de texto o en bases de datos dependiendo del tipo servidor utilizado
- Cada una de las líneas del fichero se conoce como registro de recursos (RR, Resource Records). Existen distintos tipos de recursos, como se verá después.

asir.es	IN	NS	ns1.asir.es.
ns1.asir.es.	IN	A	118.100.162.100
pegaso.asir.es.	IN	A	118.100.162.101
www.asir.es.	IN	CNAME	pegaso.asir.es.

- Cuando un servidor DNS es autorizado para unza zona, es responsable de los nombres de dominio de la misma
- La organización que delega el servidor de nombres y por lo tanto la zona, puede decidir si delega o no alguno de sus subdominios
- Una zona no es lo mismo que un dominio. Un dominio es un subárbol del espacio de nombres de dominio. Los datos asociados a los nombres de un dominio pueden estar almacenados en una o varias zonas distribuidas en uno o varios servidores
- Un servidor DNS puede tener autoridad sobre varias zonas
- El servicio DNS permite almacenar una misma zona en varios servidores DNS, ofreciendo así balanceo de carga, rapidez, y mayor tolerancia a fallos.

Servidor de nombres maestro

También se llama primario o principal

Define una o varias zonas para las que es autorizado

Sus archivos de zona locales son de lectura y escritura, y es en ellos donde el administrador añade, modifica o elimina nombres de dominio

Funcionamiento:

- Si un cliente DNS u otro servidor DNS le pregunta por un nombre de dominio para el que, autorizado, consulta con los ficheros de zona y responde
- Si un cliente DNS u otro servidor DNS le pregunta por un nombre de dominio para el que no es autorizado, tendrá que buscar la información en otros servidores DNS o responder que no se conoce la respuesta

Servidor de nombres esclavo

También llamado secundario

Define una o varias zonas para las que es autorizado

La diferencia con un maestro es que obtiene los ficheros de zona de otro servidor autorizado para la zona mediante un proceso que se denomina transferencia de zona

Los ficheros de zona del servidor esclavo son de solo lectura. La modificación de los ficheros de zona se realiza en el servidor maestro

El funcionamiento ante las respuestas de los clientes es similar al de un servidor maestro.

se utilizan para:

- Reducir y reducir la carga entre varios servidores
- Favorecer la tolerancia a fallos
- Ofrecer respuestas más rápidas

Lo ideal es que los servidores DNS de una zona estén ubicados en redes y localizaciones diferentes para evitar que un problema les afecte simultáneamente y deje sin servicio de resolución a los nombres de dicha zona.

Servidor de nombres caché

Cuando un servidor DNS recibe una pregunta sobre un nombre de dominio de una zona para la que no es autorizado, es decir, de un nombre que no tiene información, puede preguntar (si así se ha configurado) a otros servidores para que le den la respuesta.

Si el servidor actúa como caché, guarda durante un tiempo (TTL, Time To Live) las respuestas a las ultimas preguntas que ha realizado a otros servidores de nombres.

Cada vez que un cliente DNS u otro servidor DNS le formula una pregunta, consulta en primer local en su memoria caché, ahorrándose la pregunta a otros servidores si ya la había hecho anteriormente.

Un servidor de nombres es solo caché (caching only server) cuando:

- No tienen autoridad sobre ningún dominio
- Pregunta a otros servidores para resolver las peticiones y guarda las respuestas en caché.

Servidores raíz (Root servers)

Existen un conjunto de servidores DNS autorizados para el dominio raíz ".", conocidos como servidores raíz (Root servers).

Contienen el fichero de la zona "." Que almacena cuales son los servidores DNS autorizados para cada uno de los dominios TLD

Los servidores raíz están bajo responsabilidad de la ICANN, pero son operados por un consorcio de organizadores.

Estos servidores son clave en el proceso de resolución de nombres de dominio en internet, y deben ser conocidos por todos los servidores DNS que respondan a preguntas sobre nombres para los que son autorizados.

Clientes DNS (resolvers)

Es cualquier software capaz de preguntar a un servidor DNS e interpretar sus respuestas

Los sistemas operativos incluyen un conjunto de librerías que hacen esta función, y son invocadas por las aplicaciones cuando se utiliza un nombre de dominio

Algunos se pueden configurar para mantener una caché de respuestas

Algunos sistemas también tienen archivos de texto en donde se pueden asociar direcciones IP con nombres que consultarían primero

Cada fichero de zona organiza su información en registros de recursos (RR, Resource Records) los cuales se envían entre las preguntas y respuestas entre cliente y servidores DNS

Formato general:

- **Nombre de dominio:** Con el que se asocia el recurso
- **TTL** (Time To Live): Es opcional y representa el numero de segundos que puede estar el registro en caché antes de ser descartado
- **Clase:** Define la arquitectura de protocolos usada. "IN" para la TCP/IP.
- **Tipo (de registro):** son diferentes en función del campo clase. Para IN hay varios (A, CNAME, NS,…)
- **Tipo-Dato:** Información asociada al nombre de dominio, y que varía en función del tipo de registro. Por ejemplo, para el tipo A, representa la dirección IP.

vives.asir.es.	7200	IN	A	193.101.21.48

Registro SOA

Es el primer registro de una zona y define una serie de opciones generales de la misma.

Los datos son:

- **MMAME:** Nombre FQDN del servidor de nombres maestro del dominio
- **Contacto:** Correo de la persona responsable del dominio, donde la "@" se ha reemplazado por "."
- **Número de serie (serial):** Versión del archivo de zona, y debe ser incrementado cada vez que se modifique. Se utiliza para las transferencias de zona.
- **Actualización (refresh):** Tiempo que esperan los servidores esclavos para preguntar al servidor maestro si hay cambios en la zona.
- **Reintentos (retry):** si falla la transferencia de zona, el tiempo que se espera antes de volver a intentarlo
- **Caducidad (expire):** Tiempo que el servidor esclavo está intentando contactar con el maestro para ver si hay cambios. Si este tiempo expira, el esclavo se declara como no autorizado, y no se responde sobre esa zona
- **TTL negativo (Time To Live):** Tiempo que se almacenan las respuestas negativas sobre esa zona.

```
asir.es.   IN   SOA      ns1.asir.es.    admin.asir.es. (
                         1               ; Número de serie
                         604800          ; Tiempo de refresco
                         86400           ; Tiempo de reintento
                         2419200             ; Tiempo de expiración
                         604800 )            ; TTL negativo
```

Registro A y AAAA

Los registros de recursos A (address) y AAAA (Address Address Address Address) establecen una correspondencia entre un nombre de dominio completamente cualificado (FQDN) y una dirección IP versión 4 y 6 respectivamente.

```
ns1.asir.es.        IN   A       193.100.200.25
ns2.asir.es.        IN   A       193.100.200.26
luis.asir.es.       IN   A       193.100.200.101
vives.asir.es.      IN   A       193.100.200.102
luis.asir.es.       IN   AAAA    2001:db8::63
vives.asir.es.      IN   AAAA    2001:db8::64
```

Registro NS

El registro de recursos NS (name server) permite establecer:

- Los servidores de nombres autorizados a una zona. Cada zona debe contener como mínimo, un registro NS. Los servidores DNS, pueden tener un nombre de la misma zona o de otras
- Quienes son los servidores de nombres con autoridad en los subdominios delegados. Cada zona debe contener, al menos, un registro NS por cada subdominio que haya delegado.

La parte derecha de un registro NS no debe ser un nombre de tipo CNAME (alias).

```
asir.es.        IN   NS   ns1.asir.es.      ; Servidor DNS maestro
asir.es.        IN   NS   ns2.asir.es.      ; Servidor DNS esclavo
asir.es.        IN   NS   dns.asir.org.     ; Servidor DNS esclavo

ns1.asir.es.    IN   A    193.48.54.100
ns2.asir.es.    IN   A    193.48.54.101

; Delegación
redes.asir.es.      IN   NS   ns1.redes.asir.es.   ; Delegación
sistemas.asir.es.   IN   NS   dns.asir.org.        ; Delegación

ns1.redes.asir.es.  IN   A    193.100.53.8
```

Registro CNAME

El registro de recursos CNAME (Canonical Name) permite crear alias para nombres de dominio especificados en registros A y AAAA

Un registro CNAME puede apuntar a un nombre de otro dominio

No se deben usar registros CNAME en la parte derecha de registros MX y NS. La parte derecha de estos recursos tiene que ser un nombre que aparezca en un registro de tipo A.

El uso de muchos CNAME perjudica el rendimiento de los servidores DNS.

```
vives.asir.es.      IN   A       193.100.200.101
luis.asir.es.       IN   CNAME   vives.asir.es.
www.asir.es.        IN   CNAME   www.servicios.es.
```

Registro MX

El registro de recursos MX (Mail Exchange) permite definir equipos encargados de la entrega de correo en el dominio. Son consultados por los agentes de transporte de correo SMTP

Un registro MX puede apuntar a un nombre de otro dominio

Se pueden definir varios registros MX para un mismo dominio, es decir, varios servidores de correo para ese dominio. En cada registro MX se especifica un numero positivo que determina en el caso de que existan varios registros MX. El numero mas pequeño tienen mayor preferencia.

La parte derecha no debe ser de tipo CNAME.

```
asir.es.              IN   MX  10  mail1.asir.es.
asir.es.              IN   MX  20  mail2.asir.es.
mail1.asir.es.        IN   A       193.100.200.221
mail2.asir.es.        IN   A       193.100.200.222
asir.es.        IN    MX  30  smtp.informática.es.
```

Registro PTR

El registro de recursos PTR (Pointer Record) establece una correspondencia entre nombres de direcciones IPv4 e IPv6 y nombres de dominios. Se utilizan en las zonas de resolución inversa.

En una misma zona no puede haber registros PTR IPv4 y registros PTR IPv6.

```
100.200.100.193.in-addr.arpa.      IN   PTR ns1.asir.es.
200.200.100.193.in-addr.arpa.      IN   PTR ns2.asir.es.
```

Transferencia de zona

Los servidores DNS que declaran zonas esclavas o secundarias obtienen los archivos de zona (los registros de recursos) de otros servidores DNS autorizados para esas zonas. A este proceso se le denomina transferencia de zona.

Los servidores maestros usan el puerto 53/TCP para el intercambio de datos en las transferencias de zona

Existen 2 tipos de transferencia de zona:

- Transferencias de zona completas (AXFR)
    - El maestro envía al servidor todos los datos de la zona.
- Transferencias de zona incrementales (IXFR)
    - El maestro envía al esclavo los datos que han cambiado desde la última transferencia de zona.
    - Reduce el numero de registros a enviar, por lo que consume menos recursos (ancho de banda, tiempo,…)