Tema 2: DNS. Servicio de nombres de dominio.

Índice

1. Introducción a DNS

En las redes TCP/IP, cada ordenador dispone de una dirección IP para poder comunicarse con el resto de ordenadores, igual que en las redes de telefonía cada teléfono dispone de un número de teléfono que le identifica y le permite comunicarse con el resto de teléfonos.

Trabajar con direcciones IP es incómodo para las personas por ser difíciles de recordar (132.116.15.138), ya que requeriría conocer en todo momento las direcciones IP de los equipos a los que queremos conectarnos. Para evitarlo utilizamos **nombres,** que son más fáciles de recordar y utilizar (**www.google.es, www.elpais.es, ...**).

Pero como la comunicación entre los ordenadores se realiza utilizando direcciones IP y no nombres, es necesario algún sistema que permita, a partir de los **nombres** de los ordenadores, averiguar las direcciones IP de los mismos.

> Ejemplo: *Cuando queremos acceder a la página web del buscador google, en la barra de direcciones del navegador escribimos: http://wwww.google.es. Nuestro ordenador tendrá que averiguar que IP se corresponde con* ***www.google.es*** *y una vez que lo ha averiguado (66.249.92.104) se conectará con el servidor usando esa IP para obtener la página web principal y mostrarla al usuario. Si en el navegador escribimos: http:// 66.249.92.104, ahorramos el paso de averiguar la dirección IP y directamente nos mostrará la página web inicial de google.*

2. Servicio y servidor DNS

2.1. Sistemas de nombres planos y sistemas de nombres jerárquicos

Los sistemas de nombres en general (no solo los usados en redes), pueden clasificarse en dos tipos:

- Sistemas de nombres planos:
  - No existe una jerarquía para clasificar esos nombres.
  - Ejemplos: DNI's, nombres de ciudades, de países, nombres de NETBIOS de Windows, etc
- Sistemas de nombres jerárquicos:
  - Usan nombres agrupados y clasificados según algún criterio (p.e., ditribución geográfica, tamaño, funcionalidad…).
  - Facilitan la administración y gestión distribuida.
  - Ejemplos: Números de teléfono fijo (*prefijo país+prefijo provincia+número)* , códigos postales o nombres de sistemas de ficheros *(/home/usuario1/documentos, /home/usuario2/Descargas…).*

DNS ofrece un sistema de nombres jerárquico.

En Internet, el uso de los **nombres o direcciones de dominio**, también conocidos como **URL** (Universal Resource Locator o Localizador Universal de Recursos) o **URI** (Uniform Resource Identifier o Identificador de Recurso Uniforme), oculta a los usuarios los complejos formatos de direcciones IP, tanto en su versión 4 como 6. Las URL o URI son un sistema de nombres jerárquico.

2.2. Historia de DNS

El servicio DNS apareció en 1983 de la necesidad de almacenar de forma estructurada los nombres de todos los servidores conectados a Internet.

El SRI (Stanford Research Institute) almacenaba en cada máquina un fichero llamado **hosts** con todos los nombres de dominio conocidos. Este fichero se actualizaba durante la noche con los nuevos nombres añadidos durante el día.

Internet fue creciendo y el tamaño del fichero **hosts** también, lo que desencadenó un enorme problema debido a la inconsistencia de un fichero **hosts** de un ordenador frente a otro por la posibilidad de duplicidad de nombres, ya que en aquel momento no había una autoridad que garantizara que cada nombre era único. Este fichero usaba nombres planos.

Para solucionar este problema, Paul Mockapetris definió el protocolo DNS (Domain Name System o Sistema de Nombres de Dominio) en 1986.

2.3. Características y utilidad del protocolo DNS

DNS es un servicio de **almacenamiento y consulta de información** sobre nombres de dominio y sus IP asociadas.

- La información se guarda en una **base de datos distribuida** entre múltiples equipos (servidores de nombres). Esto quiere decir que no existe una base de datos única donde se almacenan todas las direcciones IP existentes en el mundo, sino que cada servidor almacena los datos correspondientes a sus dominios.

- La base de datos de nombres se organiza según un **esquema de nombres jerárquico** (espacio de nombres de dominio). Cuando nuestro servidor DNS más inmediato no puede atender nuestra petición, la traslada al servidor DNS de rango superior para su resolución.

- A los servidores de nombres se les pueden realizar preguntas y para ello se usan programas (**clientes DNS**) que dialogan con los servidores en base a unas reglas (**protocolo DNS**).

DNS puede guardar varios tipos de información sobre cada nombre de dominio y por eso se puede usar para distintos propósitos. Lo normal es asociar direcciones IP con nombres de dominio, y por eso se suele usar para:

- Búsqueda de una dirección IP conocido su nombre de dominio (**resolución directa**). Por ejemplo, ¿cuál es la IP asociada al nombre www.asir.es?

- Búsqueda del nombre de dominio conocida su IP (**resolución inversa**). Por ejemplo, ¿cuál es el nombre o nombres de dominio asociados a la IP 200.100.89.25?

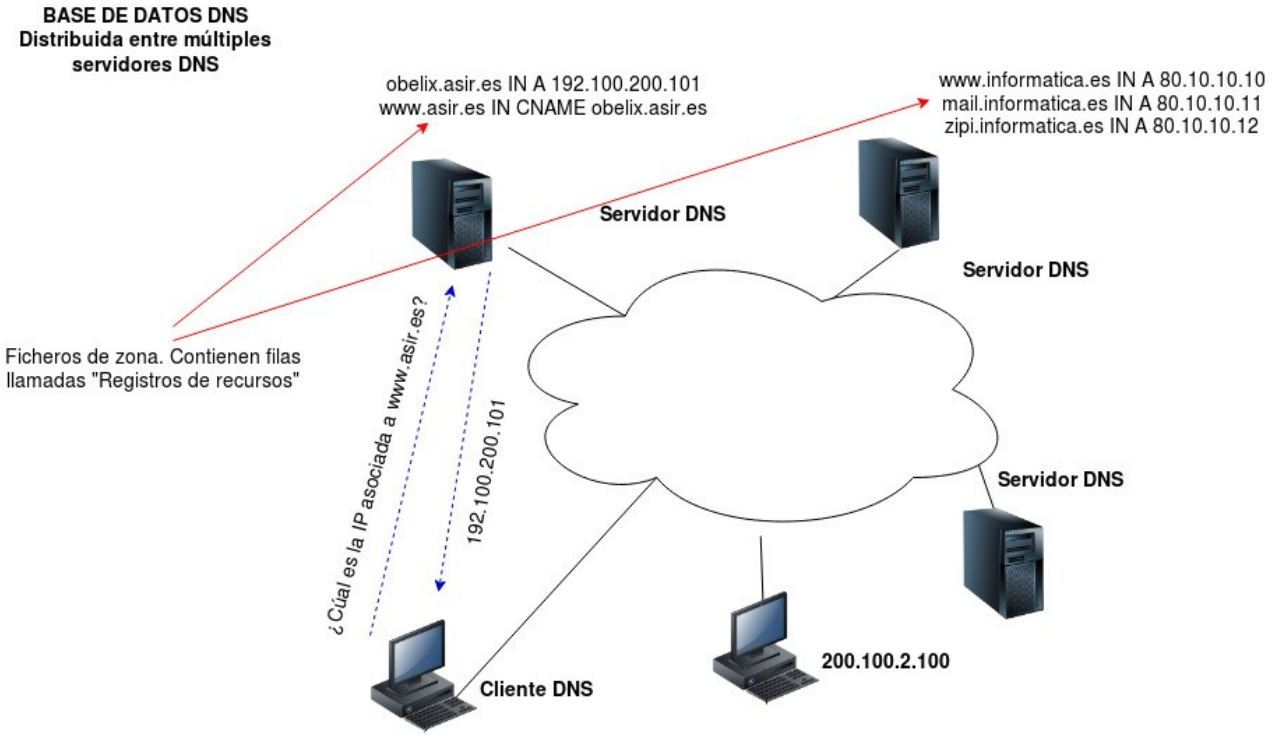
Los servidores DNS utilizan por defecto el **puerto 53** para atender a las consultas de resolución de nombres.

2.4. Componentes y funcionamiento

- **Espacio de nombres de dominio** (**domain name space**). Conjunto de nombres que se usan para identificar máquinas o servicios de una red.
- **Base de datos DNS.** Base de datos distribuida y redundante (duplicada) que almacena información sobre los nombres de dominio. Se organiza en **zonas** que almacenan información en **registros de recursos** (RR, resource records).
- **Servidores de nombres (o servidores DNS) (name servers).** Equipos con un programa (DNS) que guarda parte de la base de datos DNS (zonas) y que responden a preguntas sobre la información que almacenan. Por ejemplo, ¿cuál es la IP asociada al nombre www.asir.es)
- **Clientes DNS (resolvers)**. Programas que hacen preguntas a los servidores de nombres y procesan las respuestas para dar la información a los usuarios o/o aplicaciones que los invocan.
- **Protocolo DNS**. Conjunto de normas y reglas en base a las cuales dialogan los clientes y los servidores DNS.

El servicio DNS utiliza un modelo cliente-servidor:

- Los clientes DNS (resolvers) preguntan a los servidores de nombres.
- Los servidores de nombres también pueden preguntar a otros servidores de nombres cuando no tienen la información por la que les preguntan.



Actividad 1: En la terminal de tu máquina ejecutar el comando "**nslookup** www.google.com". Este comando consulta al servidor DNS configurado en el equipo y muestra la información obtenida, incluyendo la dirección del servidor DNS y la IP asociada al nombre de dominio.

3. El espacio de nombres de dominio

Un dominio o nombre de dominio es el nombre que identifica un sitio web. El dominio tiene que ser único en Internet. Por ejemplo, **google.es** es un dominio y **www.google.es** se corresponde con el nombre de dominio del sitio web de Google en España.

Un servidor web puede hospedar sitios web correspondientes a varios dominios y, un dominio, en principio, sólo puede apuntar a un servidor, aunque existe la posibilidad de dividir un dominio en **subdominios** y distribuirlos por distintos servidores.

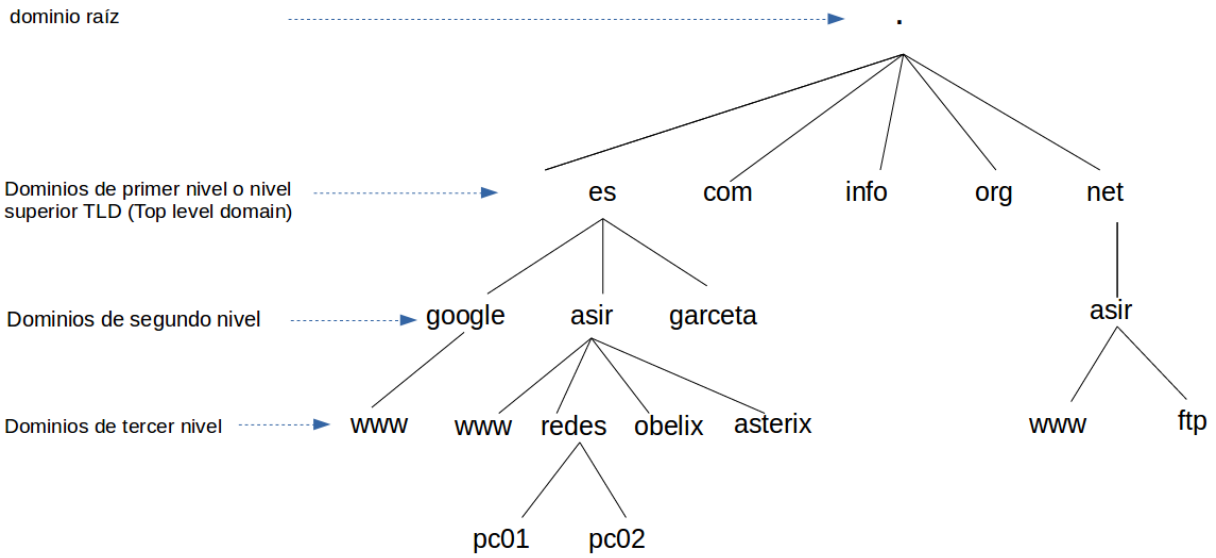
El servicio DNS se compone de una base de datos distribuida en la que se almacenan las asociaciones de nombres de dominios y direcciones IP para uno o varios dominios.

La base de datos de DNS está formada por **nombres de dominio**, donde cada nombre de dominio es una rama en un árbol invertido llamado **espacio de nombres de dominio**. El **espacio de nombres de dominio** es el conjunto de todos los nombres que se pueden usar para identificar máquinas o servicios de una red.

Cada nombre de dominio está formado por una cadena de caracteres que se divide en varios nombres separados por puntos y de izquierda a derecha.

Ejemplos de nombres de dominio:

- pc1.redes.asir.es.
- com.
- redes.asir.es.
- google.com.



El árbol comienza en el **nodo raíz situado en el nivel superior**. En el espacio de nombres de dominio, el nodo raíz se identifica mediante un nombre nulo (0 caracteres) que se representa mediante el carácter punto "**.**" y no suele aparecer escrito en el nombre de dominio.

Por debajo de él pueden existir un número indeterminado de nodos de nivel inferior.

Normalmente no se utilizar más de 5 ó 6 niveles. Por ejemplo, en lliurex.cult.gva.es se utilizan 4 niveles.

El nombre completo de un nodo está formado por el conjunto de nombres que forman la trayectoria desde ese nodo hasta el nodo raíz y expresados en orden inverso de sus niveles, es decir, de iabajo a arriba, como por ejemplo **www.curso.accesored.com.**, aunque se debe tener en cuenta que la raíz no se escribirá como parte del nombre de dominio, es decir, deberíamos haber escrito **www.curso.accesored.com**

No hay que confundir el nodo raíz con todos y cada uno de los separadores por los que está formado el nombre, ya que el carácter punto también se utiliza como separador de nombres.

- El nombre de dominio completo se llama *nombre de dominio completamente cualificado* o *Fully Qualified Domain Name (FQDN)* y es **absoluto**, ya que especifica la ruta completa de la jerarquía hasta llegar a cada elemento. El top de la raíz FQDN del servidor DNS deberá ser el carácter punto "**.**".

- También se puede hacer referencia a un nombre de dominio de forma **relativa** (por ejemplo, usando del nombre "asterix" para referirse a "asterix.asir.es". En este caso se debe conocer el dominio superior al que se refiere ese nombre para saber exactamente a qué hace referencia.

Cada equipo en la red deberá tener un único FQDN, pero se debe tener en cuenta que es posible que el equipo al que se haga referencia mediante el FQDN esté apagado o tenga algún tipo de problema.

3.1. Top Level Domain (TLD)

Por debajo de la raíz, en el **nivel superior o primer nivel**, también llamada **TLD** (Top Level Domain o Nivel Superior del Dominio), se encuentran nombres de dos tipos: genéricos propiamente dichos (.com, .org, .edu, …) y de país (.es, .ar, .it, .fr, .eu, …).

Los principales *TLD genéricos* son:

.com: Agrupa a organizaciones comerciales. Ejemplo: ibm.com

.edu: Reúne a organizaciones educativas universitarias. Ejemplo: uoc.ed

.net: Organizaciones dedicadas a Internet y a las telecomunicaciones. Ejemplo: php.net, ...

.org: Representa organizaciones no comerciales. Ejemplo: linuxdoc.org

.gov: Identifica organizaciones gubernamentales. Ejemplo: nasa.gov

Los *TLD de países* representan cada país mediante dos letras. Ejemplos: **.es** para España, **.fr** para Francia, **.de** para Alemania, ...

Puede ocurrir que los dominios geográficos de primer nivel contengan a su vez alguno de los dominios genéricos. Estos dominios serían de segundo nivel. Ejemplos: **com.fr, edu.es,** ...

Los dominios asociados a cada país son registrados por las autoridades locales que, en el caso de España, es **red.es** (entidad pública empresarial adscrita al Ministerio de Industria).

En la actualidad están ampliando la posibilidad de incluir nombres genéricos personalizados de cualquier tipo.

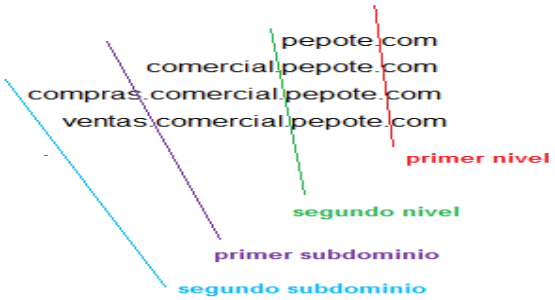
3.2. Two Level Domain (2LD)

En un **segundo nivel o 2LD** (Two Level Domain) aparece el nombre distintivo de la organización. Generalmente a la unión del **2lD** y **TLD** se le conoce como dominio.

Un **dominio** está formado por el espacio de nombres que comparten el mismo dominio de primer y segundo nivel, es decir, todos los nombres que hay por debajo de un dominio de segundo nivel en la jerarquía.

Dentro del **2LD** pueden definirse los **subdominios**, que aparecerán en la calificación del nombre de dominio separados por puntos y formarán el resto de los niveles hasta completar los 5 ó 6 que se suelen utilizar.

> *Ejemplo de dominio*: **pepote.com**, formado por los nombres comercial.pepote.com, compras.comercial.pepote.com y ventas.comercial.pepote.com



3.3. Registros DNS

En último lugar aparecerán los **registros DNS**, que normalmente estarán asociados a equipos concretos dentro del dominio.

La configuración de registros de recursos es muy variable, siendo un ejemplo:

> ***www****.pepote.com* → Servidor Web de la empresa (Páginas Web de la empresa con información de la empresa, tienda online, area de clientes, etc...).
>
> ***mail****.pepote.com* → Servidor de correo electrónico general de la empresa (correos corporativo de los empleados).
>
> ***mail****.comercial.pepote.com* → Servidor de correo electrónico comercial de la empresa (correo para relaciones entre clientes y empresa, como por ejemplo resolución de dudas, reclamaciones, etc...)
>
> ***ftp****.compras.comercial.pepote.com* → Servidor de descarga de ficheros de la zona de compras de la empresa (catalogo de productos, ofertas a clientes, etc...)
>
> ***ftp****.ventas.comercial.pepote.com* → Servidor de descarga de ficheros de ña zona de ventas de la empresa (manuales de uso de productos, documentación sobre reclamaciones, etc...)

3.4. Registrar nombres de dominios

Los dominios pueden ser registrados por entidades o personas físicas, es decir, reservar y pagar por el derecho de uso de un nombre de dominio durante un tiempo determinado, normalmente renovable de año en año, siempre y cuando no esté ya registrado.

Para poder registrar un dominio se debe acudir a un **registrador** (hostei, 1&1, etc) o empresa encargada de la gestión de los dominio de segundo nivel como *accesored.com.*

Una vez que se dispone del derecho de uso del dominio se puede asignar a una dirección IP concreta, crear sobre el subdominios, o realizar sobre él las acciones que se consideren oportunas.

- Los registradores dependen de los **operadores de registros** (en España, **red.es**) y estos a su vez del **ICANN** (*Internet Corporation for Assigned Names and Numbers*), responsable a nivel mundial del espacio de nombres de dominio. La ICANN se encarga de administrar el dominio raíz y mantener un registro de los dominios de nivel superior (TLD) existentes.

- El ICANN posee 13 servidores de nombres distribuidos por el mundo, que se llaman **Servidores Raíz** o **TNS** (Top Numbers Servers). Todos ellos tienen la misma información, de forma que se reparten o distribuyen el trabajo de resolución y además cada uno de ellos es una copia de seguridad del resto. En realidad no son 13 servidores individuales, sino que son 13 grupos de servidores, representando cada grupo un único servidor DNS raíz distribuido.

- Estos 13 servidores contienen información sobre los nombres de dominio de primer nivel (TLD) de todo el mundo, los cuales a su vez también estarán replicados y distribuidos. La ICANN delega la administración de cada TLD a una organización particular denominada "operador de registro". El operador de registro del dominio "es" es "Red.es".

3.5. Delegación

Como hemos dicho varias veces, la información sobre los nombres de dominio del servicio DNS se almacena en una base de datos distribuida entre múltiples servidores de nombres. Estos servidores son independientes unos de otros y su administración se basa en la **delegación**.

La delegación consiste en que la organización que administra un dominio "cede" la administración de uno, varios o todos los subdominios a otras organizaciones.

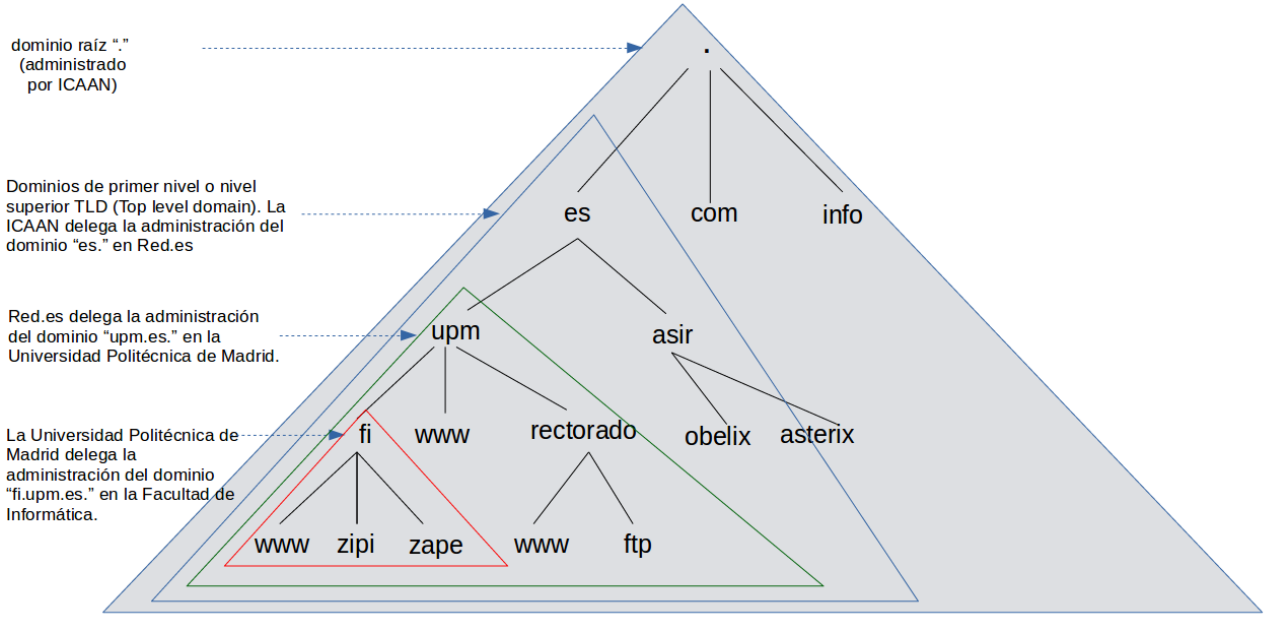
Como se ha explicado, la ICAAN administra el dominio raíz y delega la administración de cada dominio de primer nivel (TLD) en otras organizaciones (p.e., *Red.es* para "es"). Cada una de estas organizaciones puede delegar la administración de los dominios de segundo nivel en otras (p.e., *Red.es* delega la administración del dominio "upm.es" en la Universidad Politécnica de Madrid). A su vez, cada organización puede delegar la administración de sus subdominios en otras organizaciones (p.e., la Universidad Politécnica de Madrid puede delegar la administración del ubdominio "fi.upm.es" en la Facultad de Informática).

Esto no quiere decir que la división de un dominio en subdominios implique siempre delegar en otras organizaciones. Por ejemplo, la Universidad Politécnica de Madrid podría tener otro subdominio "rectorado.upm.es" administrado por la propia Universidad, sin delegar en nadie. Además, si una organización delega un subdominio en otra, no tiene por qué informar a "su superior" (p.e., la Universidad Politécnica de Madrid no tiene por qué informar a "Red.es" de que ha delegado el dominio "fi.upm.es".

La organización que administra un dominio es responsable de los nombres usados en ese dominio, de las IP asociadas a ellos y del funcionamiento y mantenimiento de los servidores de

nombres que almacenan esa información.

La delegación permite la gestión **descentralizada** de los nombres de dominio.



4. Servidores de nombres

Los servidores de nombres o servidores DNS son programas que guardan información sobre nombres de dominio y responden a preguntas de los clientes sobre esos nombres. Almacenan, por tanto, una parte del espacio de nombres.

4.1. Zonas

Ahora que sabemos que la administración de un dominio la llevan a cabo una o varias organizaciones, la pregunta que surge es ¿donde se guarda la información relativa a esos dominios?

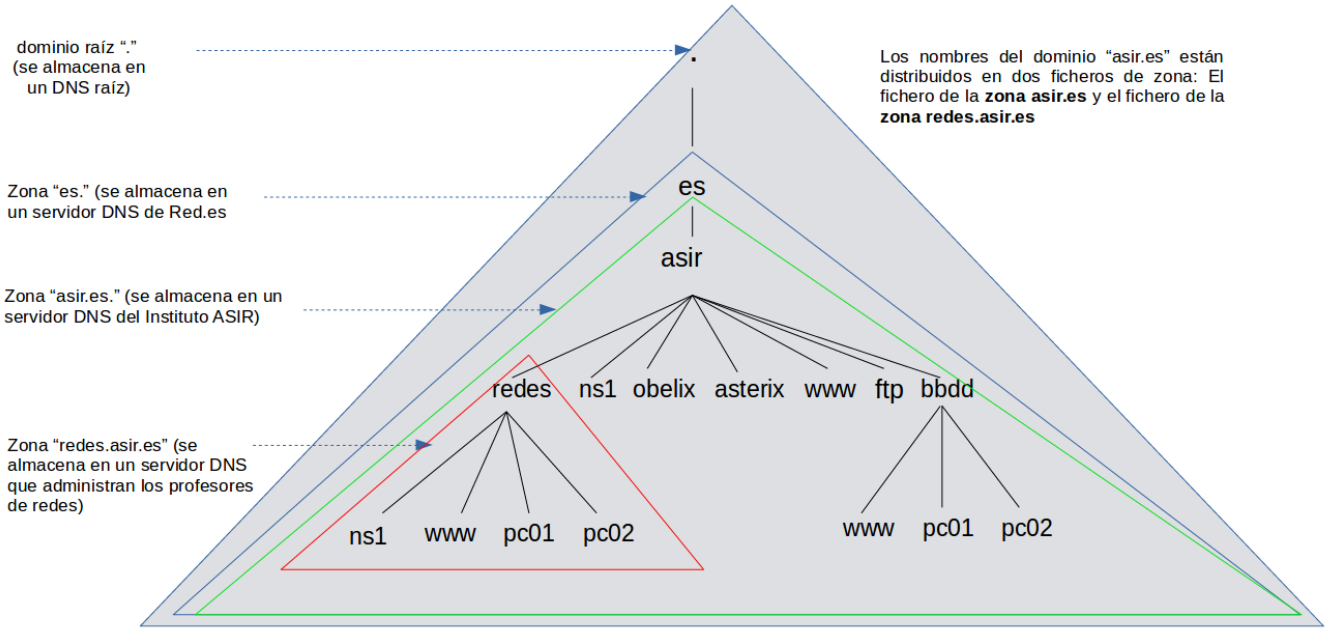
La información relativa a un dominio puede estar en uno o más servidores DNS de la red. La información almacenada por un servidor de cada uno de los dominios que controla constituye una **zona**, y está definida por un conjunto de registros de recursos sobre los que **el servidor DNS tiene autoridad.** La zona guarda la información relativa a la organización del dominio.

En un servidor DNS puede no existir ningún dominio (solo respondería a consultas sobre dominios externos), puede existir un único dominio (normalmente en un ámbito local o privado) o varios dominios (normalmente en ámbito de Internet o públicos). Además, la información que guarda el servidor DNS no tiene por qué ser el dominio completo, sino que puede ser sólo una parte (delegación). Cada dominio (o parte de dominio) es una zona.

Zona vs. dominio: Un dominio es **un subárbol del espacio de nombres** de dominio. La información del dominio (información de los nombres de ese dominio) puede estar almacenada en una o varias zonas distribuidas en uno o varios servidores DNS.

- Si en un ámbito local se quiere definir uno o varios dominios para la red de la empresa, deberá existir al menos un servidor DNS que guarde la información de estos dominios, en una zona para cada dominio.

- Un dominio podría llegar a crecer tanto que sea necesario dividirlo en subdominios.
- Incluso el dominio puede llegar a ser tan grande que merece la pena la cesión de autoridad de una parte del dominio (normalmente uno o más de sus subdominios) a otro servidor DNS. Esto es la **delegación de zona** que hemos visto antes.
- Pero también se podría tener un servidor DNS sin definir ninguna zona, por lo que no existirá ningún dominio local. En ese casp los servidores DNS funcionarán como **servidor DNS caché** *(la utilización de servidores DNS caché en un ámbito local acelera el acceso a las redes externas, ya que la resolución de nombres es mucho más rápida)*.



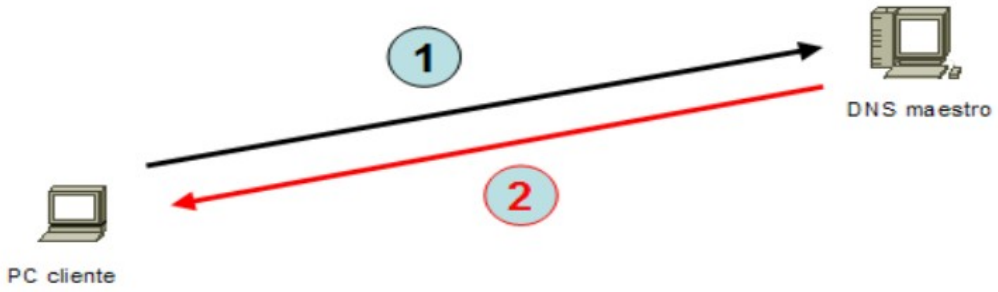
4.2.Clasificación de los servidores DNS

En el mundo existen miles de servidores DNS y no todos tienen las mismas características ni se comportan igual ante la solicitud de resolución de nombre. Básicamente se pueden distinguir 3 tipos:

4.2.1. Servidor maestro o primario

Es el servidor autorizado sobre un dominio o dominios definidos en uno o varios ficheros de zona, por lo que *puede resolver las consultas sobre los dominios en él definidos y se le permite modificar el fichero de asociación entre IP's y nombres de dominio (fichero de zona)*.

Cuando en un dominio existen varios servidores DNS, sólo uno de ellos deberá ser el autorizado (primario o maestro) y el resto serán servidores secundarios o esclavos.



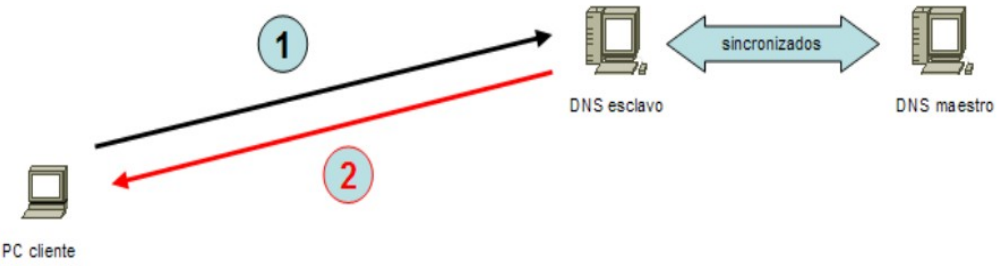
1) El cliente realiza una consulta a su DNS.

2) El servidor maestro dispone en su base de datos información sobre el nombre consultado, realiza la resolución y se le envía al cliente.

4.2.2. Servidor esclavo o secundario

Contienen información sobre uno o varias dominios, pero dicha información *es una copia de sólo lectura de la almacenada en el servidor maestro con el que se relaciona*. Es capaz de resolver las consultas sobre las dominios que controla sin necesidad de reenviar la información al maestro ni a ningún otro servidor y es perfectamente funcional por sí sólo dentro de sus dominios, aunque ***no tiene la capacidad de modificar los ficheros de configuración de IP's y nombres de dominio,*** por lo que tiene un dependencia funcional sobre el maestro.

Cuando el maestro realiza algún cambio en la configuración de alguno de sus dominios, modifica un identificador, y tras un periodo de tiempo prefijado de antemano, el esclavo consultará dicho identificador. Si es distinto al valor conocido por el esclavo, quiere decir que el maestro realizó algún cambio, por lo que el esclavo procederá a descargar la nueva información del maestro (**transferencia de zona**) para poder atender la resolución que se le puede llegar a plantear sobre los nuevos datos añadidos.



1) El cliente realiza una consulta a su DNS.

2) El DNS esclavo, con la base de datos del maestro sincronizada y replicada en él, busca en su base de datos información sobre el nombre consultado y en caso de encontrarla se le envía al cliente.

Las principales razones para implantar servidores DNS esclavos son:

- Reducir y repartir la carga entre varios servidores.
- Favorecer la tolerancia a fallos (el esclavo puede responder si falla el maestro).
- Obtener respuestas más rápidas.

**** La definición de maestro o esclavo se determina a nivel de zona, es decir, un servidor DNS puede ser a la vez maestro o primario para una o varias zonas y esclavo*

*o secundario para otra u otras. Por ejemplo, nuestro servidor DNS del instituto ASIR puede ser maestro para la zona **asir.es** y esclavo para la zona **dam.es***

Transferencia de zona

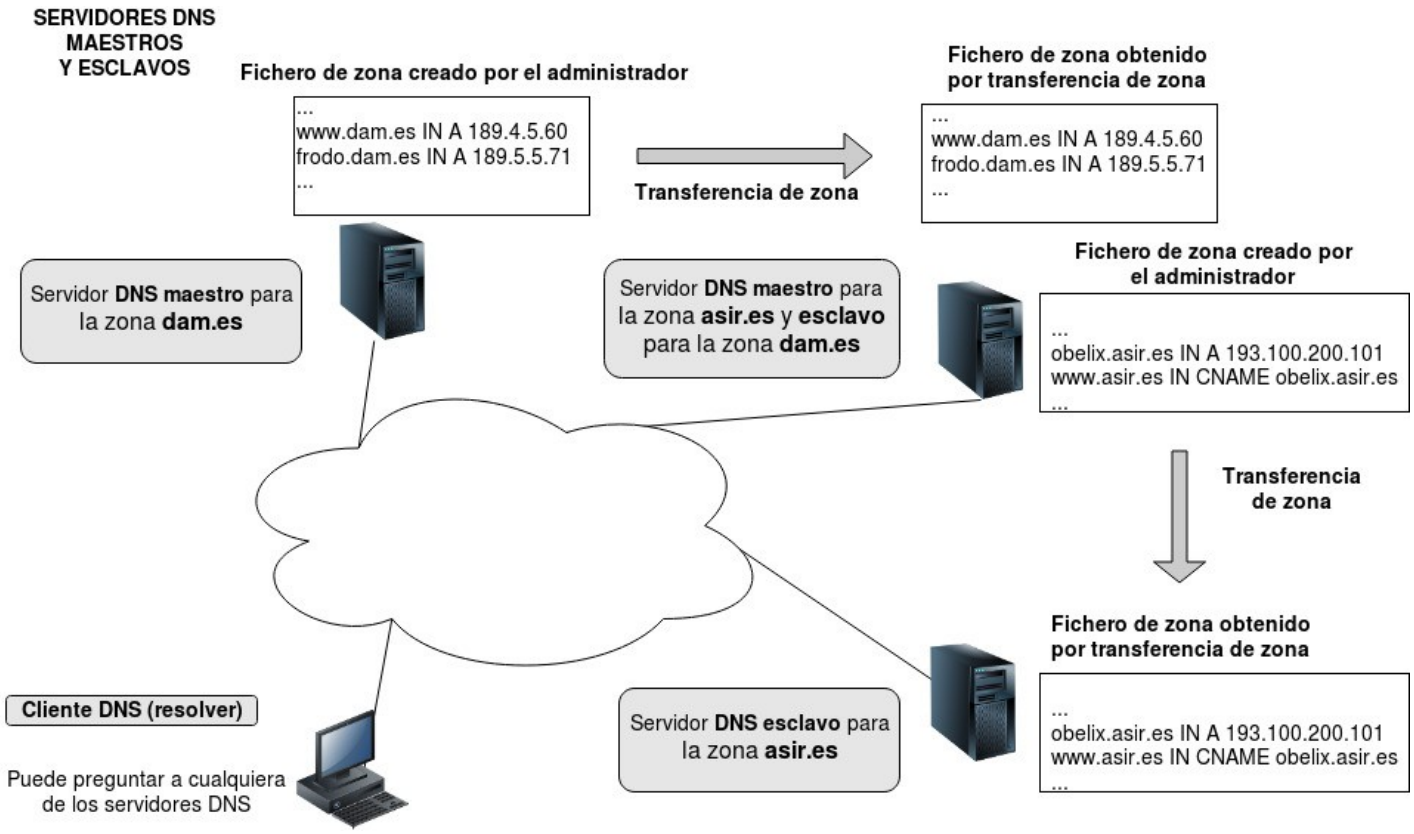
Los servidores esclavos reciben la información del maestro a través de la **transferencia de zona.**

Las transferencias de zona pueden ser **completas** (pasar toda la información completa) o **incrementales**, es decir, pasar sólo aquella información modificada.

El proceso de transferencia de zona se puede iniciar de una de dos maneras:

– El servidor maestro notifica al servidor o servidores esclavos cada vez que se produce un cambio sobre su dominio.

– El servidor o servidores esclavos preguntan al maestro si existe algún cambio y solicitarle la transferencia de zona. La pregunta del esclavo al maestro es nada más arrancar y el resto de las veces tras una tiempo de espera configurable.



4.2.3. Servidor caché/ reenvío:

El proceso de resolución de nombres es costoso, puesto que usa muchos recursos de los equipos y de la red. Para mejorar los tiempos de respuesta de las consultas y reducir la carga y tráfico de la red, los servidores de nombres pueden actuar como **servidores caché.**

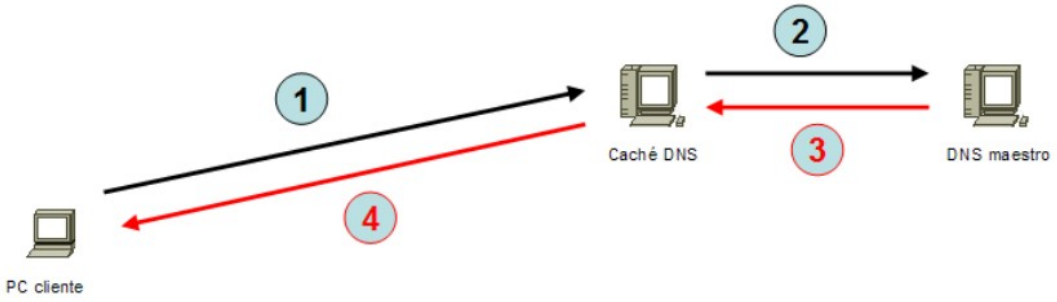
Cuando un servidor DNS recibe una pregunta sobre un nombre de dominio de una zona sobre la que no es autorizado (es decir, sobre el que no tiene información), puede preguntar a otros servidores para que le den la respuesta. Si el servidor actúa como caché, guardará durante un tiempo (**TTL, Time To Live**) las respuestas para que cuando otro cliente o servidor DNS pregunte por ese nombre se pueda dar la respuesta almacenada en caché, ahorrando tiempo y recursos.

Los servidores maestros o esclavos pueden ser servidores caché. Un servidor es solo caché (caching only server) cuando:

- No tienen autoridad sobre ningún dominio (no tienen fichero de zona) y no es capaz de realizar ninguna resolución por sí sólo.

- Cuando le hacen una consulta, él debe reenviarla a los servidores adecuados para responderla, y **guarda la respuesta en la caché**

Una vez resuelta la consulta, la almacenará en su memoria (caché) y la hará llegar hasta el cliente que la solicitó. De esta forma, si otro cliente pregunta más tarde por el mismo nombre de dominio, podrá enviarle la respuesta que tiene en caché sin necesidad de consultar a otros servidores.



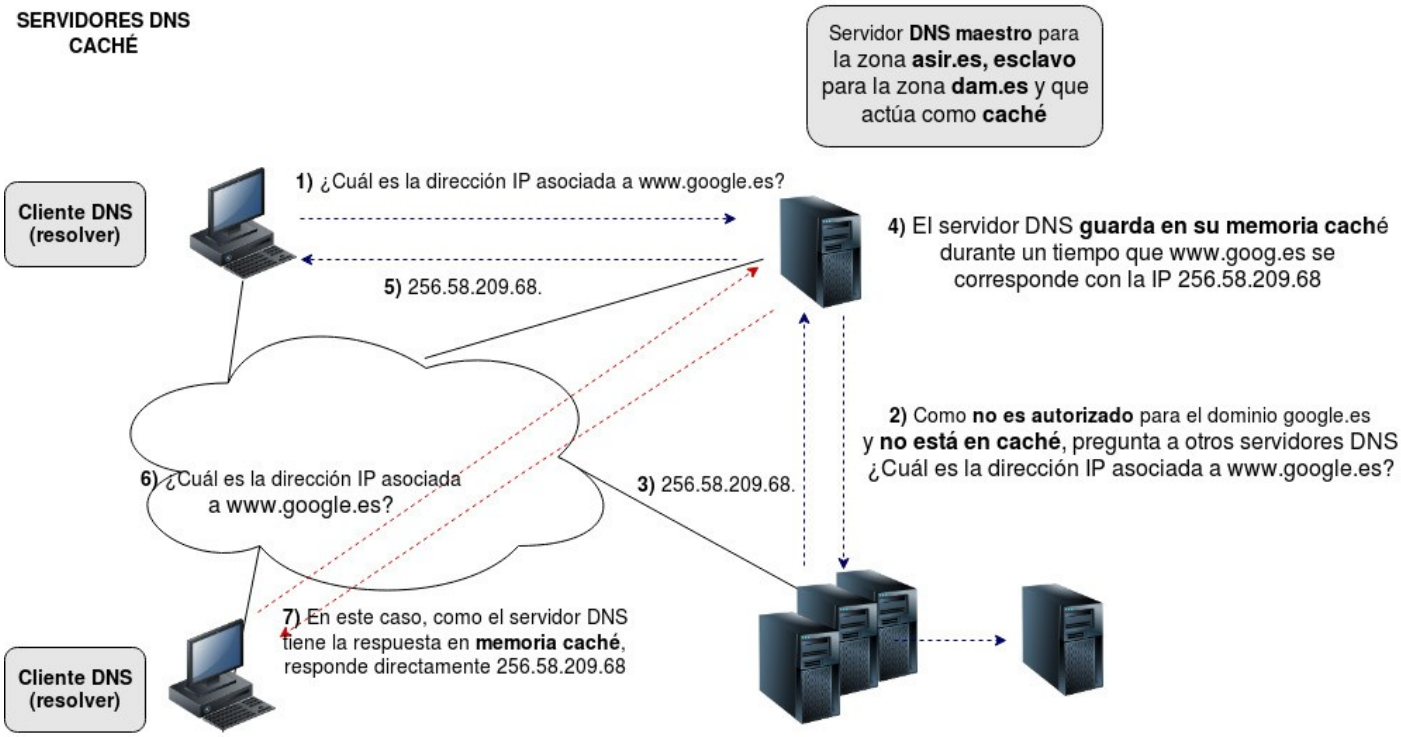
Servidor DNS solo caché

1) El cliente realiza una consulta a su DNS.

2) El DNS caché consulta su memoria caché en primer lugar. Si no encuentra la respuesta, reenvía la consulta al DNS de nivel superior.

3) La resolución de la consulta se almacena enla caché del DNS caché.

4) Se envía la resolución al cliente.



Lo normal dentro de una empresa medianamente grande, es disponer de servidores dedicados de cada uno de los tipos anteriores, pero en empresas no tan grandes, es muy normal encontrar un mismo servidor en el que se configura la posibilidad de ser maestro con caché, esclavo con caché, etc.

4.2.4. Servidor sólo autorizado:

Es un servidor DNS autorizado para una o varias zonas como maestro/esclavo y que no responde a preguntas sobre dominios que no tiene. No pregunta a otros servidores DNS, es decir, no tiene activada la recursividad (no puede hacer consultas recursivas), no es reenviador y no actúa como caché.

5. Clientes DNS (resolvers)

Los clientes DNS son aquellos equipos que solicitan el servicio de resolución de nombres para preguntar a un servidor DNS e interpretar sus respuestas.

El cliente intenta conectarse desde su máquina local a un servidor remoto mediante su URL (nombre de dominio), por lo que conecta con el servidor DNS que tenga configurado para que le devuelva la dirección IP de dicho equipo y poder así conectar con él.

El servidor DNS obtiene la información y responde al cliente con la IP del servidor remoto, posibilitando el acceso al sitio, todo ello de forma transparente al usuario.

Los principales tipos de consultas entre el cliente y el servidor DNS pueden ser recursivas e iterativas.

> Consulta recursiva: Una consulta es recursiva cuando se realiza a un servidor DNS y éste es capaz de resolverla, independientemente de si la resolución la tomó de su

caché, de su base de datos o fichero de zona, del reenvío a otro servidor DNS o de la consulta de los TNS.

Si al resolver la consulta obtuvo la información de su base de datos o fichero de zona (sobre la que es servidor autorizado), se dice que la respuesta es **autorizada** y en cualquier otro caso de respuesta resuelta se dice que la respuesta **NO es autorizada**.

Consulta iterativa: Es una consulta realizada desde un servidor DNS a otro, por ejemplo, una consulta realizada por un servidor DNS actuando como cliente para resolver un consulta que desconoce por no estar en su dominio controlado ni en su caché. No tiene por qué proporcionar una respuesta completa, sino que puede dar una respuesta parcial.

6. Resolución inversa

Se debe tener en cuenta que también existen las **resoluciones inversas**, proceso por el cual dada una dirección IP se obtiene el nombre de equipo.

La resolución inversa es utilizada por:

- Algunas aplicaciones para comprobar la identidad del equipo al que están conectados por temas de seguridad.
- Resolver problemas de red.
- Detección de spam.
- Seguir trazas de ataques informáticos.

De la misma forma que los nombres de dominio se resuelven efectuando consultas para cada componente de derecha a izquierda y el punto final indica el dominio raíz, las direcciones IP siguen el mismo esquema, donde el dominio se llama **in-addr.arpa**, siendo **.arpa** un TLD específico para consultas inversas e **in-addr** es el segundo nivel del dominio.

Ejemplo: para la IP (192.168.1.2) el servidor de nombres buscará los servidores **arpa.**, luego los servidores **in-addr.arpa.**, luego, en caso de existir en **192.in-addr.arpa.**, luego **168.192.in-addr.arpa.** y, por último, accederíamos al servidor **1.168.192.in-addr.arpa**., encontrando así el registro buscado: 2.1.168.192.in-addr.arpa.

Por lo tanto, las direcciones IP están escritas en orden inverso en el dominio **in-addr.arpa**; es decir, se utiliza una notación de puntos invertida.

Los protocolos obligan a la existencia de un dominio de resolución inverso por cada uno de los dominios de resolución directos, pudiéndose encontrar tanto en un servidor maestro como esclavo, aunque en nodo local es posible (aunque no recomendable) su funcionamiento sin la resolución inversa.

7. Registros de recursos.

Los diferentes servidores DNS que existen en una red almacenan la información relativa a los nombres de dominio DNS de las zonas en los llamados **Registros de Recursos**.

Un servidor DNS tendrá aquellos **Registros de Recursos** que le permitan responder a las peticiones de nombres relativas a la parte del espacio de nombres de dominio sobre la que tiene autoridad dicho servidor. De no encontrar la información buscada en sus **Registros de**

Recursos enviará la petición a otro servidor DNS para que la resuelva.

Desde el punto de vista de la administración, una zona no es más que un archivo que contiene determinados **Registros de Recursos** (base de datos) del espacio de nombres de dominio que identifican. También recibe el nombre de **zona de autoridad**, ya que mediante dichos registros se puede atender las peticiones de los clientes y resolverlas.

En dichas bases de datos se almacenan en filas o registros la asociación de IP y nombre dentro del dominio, siendo estos de distinta naturaleza según su función, entre ellos podemos destacar:

SOA

El registro de recursos **SOA** (Start Of Authority.- Inicio de autoridad) define una zona de autoridad y es de utilización obligatoria al describir la zona del dominio del maestro. Es el primer registro de recursos que deberá aparecer y especificará:

- El nombre del dominio.

- El servidor maestro de la zona.

-Cuenta de correos del responsable de la zona.

- Una serie de parámetros referentes a la relación entre el servidor maestro y el esclavo o esclavos asociados, tales como el identificador de serie, periodo de refresco de los servidores esclavos, frecuencia de reintentos del refresco, tiempo de espiración de registros del esclavo tras imposibilidad de refresco y TTL del caché.

NS

El registro de recurso **NS** (Name Server: Servidor de nombres).- Establece el servidor DNS con posibilidad de resolución sobre la zona, teniendo en cuenta que deberá existir uno como mínimo y con la posibilidad de poder existir varios servidores con posibilidad de resolver sobre la zona (secundarios o esclavos).

A

El registro de recursos **A** (Address: Dirección).- Establece una correspondencia entre un nombre de dominio completamente cualificado (FQDN) y una dirección IP. Cada registro **A** identifica un nombre de equipo dentro del dominio.

CNAME

El registro de recursos **CNAME** (Canonical NAME: Nombre canónico).- Crea un alias para cualquier nombre de equipo en el dominio, por lo que a partir de dicho momento, podrá utilizarse dicho alias como si del nombre real se tratara, es decir, el ordenador dispondrá de uno o más nombres en el dominio. Su principal utilidad es la de identificar distintos servicios en un mismo servidor.

PTR

El registro de recursos **PTR** (PoinTeR: Puntero).- Tiene un funcionamiento contrario a los registros **A**, es decir, asigna una dirección IP a un nombre de dominio completamente cualificado (FQDN). Este tipo de recursos se utilizan en la zona de resolución inversa.