UD 4: DNS

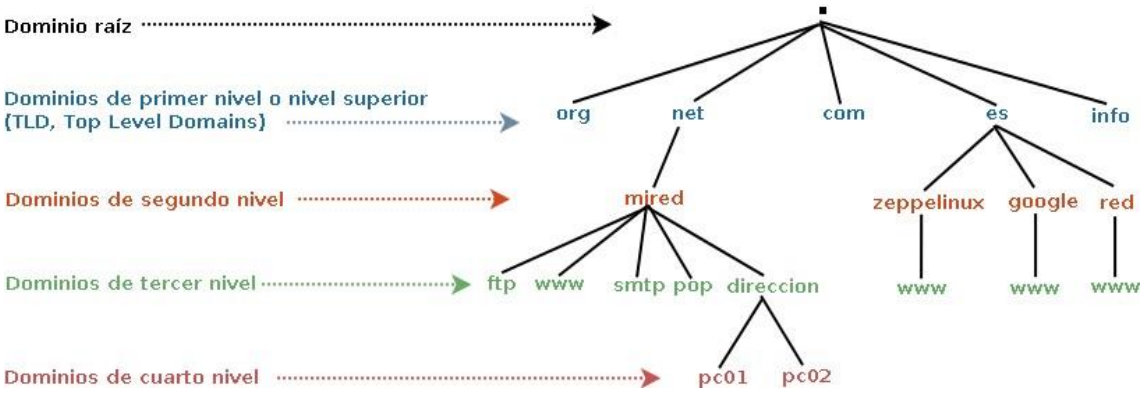
En una red TCP/IP, las máquinas se identifican mediante su dirección de red o número IP. Para las personas resulta más sencillo recordar un nombre que se asocia a una máquina concreta. La dirección IP de una máquina puede cambiar, pero el nombre no suele cambiar, o cambia menos a menudo. Es necesario un mecanismo que traduzca los nombres de las máquinas a direcciones IP. El servicio DNS permite que esta tarea se lleve a cabo.

El sistema de nombres de dominio (DNS) es el directorio telefónico de Internet. Las personas acceden a la información en línea a través de nombres de dominio como nytimes.com, espn.com, renfe.es, xunta.gal, etc. Los navegadores web interactúan mediante direcciones de Protocolo de Internet (IP). El DNS traduce los nombres de dominio a direcciones IP para que los navegadores puedan cargar los recursos de Internet.

Cada dispositivo conectado a Internet tiene una dirección IP única que otros equipos pueden usar para encontrarlo. Los servidores DNS suprimen la necesidad de que los humanos memoricen direcciones IP tales como 165.222.10.114 (en IPv4) o nuevas direcciones IP alfanuméricas más complejas, tales como 2400:cb00:2048:1::c629:d7a2 (en IPv6).

El **servicio DNS** se compone de una base de datos distribuida (integrada por varias máquinas conectadas en red) en la que se almacenan las asociaciones de nombres de dominios y direcciones IP.

El **espacio de nombres de dominio** está formado por los nombres válidos utilizados para identificar servicios o máquinas en una red. Se puede representar mediante **una estructura jerárquica** de **topología arbórea**, es decir, todos los nombres forman un árbol invertido donde cada nodo se separa de los otros nodos por un punto (.).

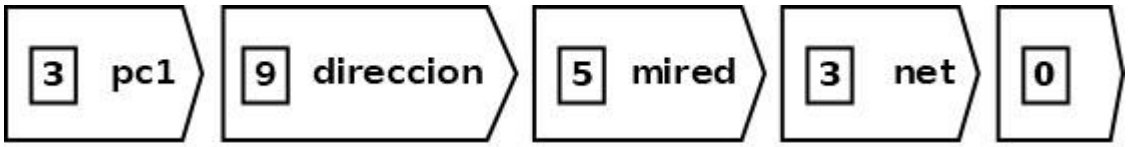


- El árbol comienza en el nodo raíz, situado en el nivel superior.
- Por debajo, puede existir un número indeterminado de nodos.
- Normalmente se utilizan hasta cinco niveles.
    - Por ejemplo, en edu.xunta.gal. se utilizan 3 niveles.
    - Los nombres se separan con un punto.
    - El dominio es, pues, cada uno de los subárboles que integran el árbol o espacio de nombres de dominio.
    - Físicamente un dominio no es más que un grupo de ordenadores.

NOMBRES DE DOMINIO

Los **nombres de dominio** pueden estar formados por una o más cadenas de caracteres separadas por **puntos** y no se distingue entre mayúsculas y minúsculas. Por ejemplo, www.renfe.es. es lo mismo que WWW.RENFE.ES.

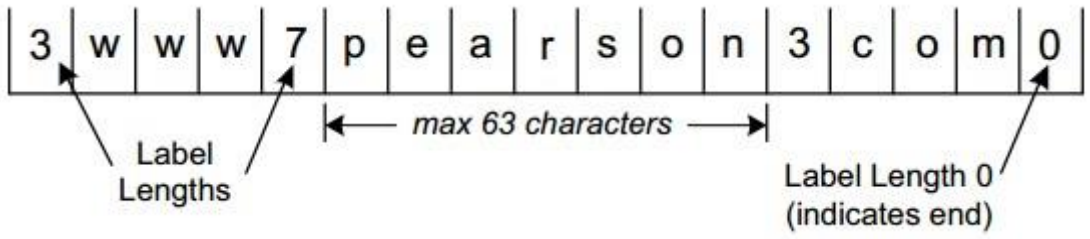
- Cada parte separada por **punto** o **nodo** del árbol tendrá como máximo **63 caracteres** de longitud.
- Los **nombres de dominio** podrán tener hasta un máximo de **127 niveles**.
- El total de un **nombre de dominio** no puede exceder de los **255 caracteres**.



Ejemplo de nombre de dominio:
pc1.direccion.mired.net.

Los nombres de dominio se expresan como secuencias de **etiquetas** (**labels**).

- Cada **etiqueta** está formada por un campo de longitud (**1 byte**) seguido por un número de bytes, indicado en dicho campo, conteniendo el nombre de la etiqueta.
- Todos los nombres de dominio terminan en el **dominio raíz**, el cual se representa con una etiqueta de **longitud 0** (ocupa 1 byte).
- La representación de un **nombre de dominio** no debe exceder los **255 bytes**.



DOMINIO RAÍZ

En teoría, todos los dominios deben de terminar con un punto (.). Es así porque el **árbol de nombres de dominio (espacio de nombres de dominio)** empieza con el dominio (.) que se conoce como **dominio raíz (root)**. En realidad, es un elemento nulo de **0** caracteres que se representa con un punto (.).

Un dominio se lee de derecha a izquierda, empezando por el punto (.), aunque en la práctica lo hacemos de izquierda a derecha. El punto inicial, generalmente se omite ya que los programas lo añaden por defecto y es meramente formal, pero en ocasiones, será necesario que indiquemos el nombre de dominio completo incluyendo el **dominio raíz**, es lo que se conoce como **nombres de dominio completos (Fully Qualified Domain Names, FQDN).**

DOMINIOS Y SUBDOMINIOS

Como consecuencia de la organización jerárquica del **espacio de nombres de dominios**, podemos utilizar los términos **dominio** y **subdominio**. Por ejemplo, «renfe.es.» es un subdominio del dominio «es.» y «www.renfe.es.» es un subdominio del dominio «renfe.es.».

Los **dominios** o **subdominios** que cuelgan del dominio raíz ((.)) se conocen como **dominios de primer nivel** o **dominios de nivel superior (Top Level Domains,**

TLD), los que cuelgan de los dominios **TLD** se denominan **dominios de segundo nivel** y así sucesivamente.

La administración del **espacio de nombres de dominio** de **Internet** la realizan múltiples empresas y organizaciones coordinadas todas por la **ICANN (Internet Corporation for Assigned Names and Numbers).**

La **ICANN** es una corporación de beneficio público, sin ánimo de lucro, con participantes de todo el mundo dedicados a mantener una **Internet** segura, estable e interoperable. Administra el **dominio raíz** y mantiene un registro de los **dominios de nivel superior (TLD)**. **InterNIC (Internet Network Information Center)** es una organización asociada a la **ICANN** que permite registrar **dominios TLD**. Los dominios asociados a cada país son registrados por las autoridades locales.

En España, **Red.es** tiene encomendada la autoridad de registro de los nombres de dominio de Internet bajo el indicativo de primer nivel correspondiente al país de España (.es).: https://www.nic.es, https://www.dominios.es**.**

Por tanto, para la creación de un dominio .es hay que solicitarlo en dominios.es o en algun agente registrador autorizado por red.es.

La **ICANN** clasifica los dominios de nivel superior **(Top Level Domain, TLD)** en:

- **Genéricos (generic TLD, gTLD).** Su nombre está relacionado con el propósito o el tipo de organización que lo utiliza.

Se clasifican a su vez en:

  - **Dominios patrocinados (sponsored TLD, sTLD):** Funcionan según las reglas de la entidad patrocinadora. Ejemplos de estos dominios son «.gov», «.edu», «.mil», «.aero», «.coop», «.travel», «.asia», «.Jobs»,…
  - **Dominios no patrocinados (unsponsored TLD, uTLD):** Funcionan según las reglas del **ICANN**. Ejemplos de estos dominios son «.com», «.org», «.net», «.info»,…
  - **Geográficos (country code TLD, ccTLD).**

Sus nombres contienen **sólo dos letras** en función del país o región. Las tareas de gestión y reglas de uso se delegan a una entidad del país o región. Ejemplos de estos dominios son «.es», «.us», «.gb», «.fr»,…

(ANEXO) Dominio.gal para Galicia: El .gal es el domino que corresponde a la comunidad autónoma de Galicia. Existe también un dominio .cat para Cataluña, y lo mismo con otras regiones. Son Aprobados por el ICANN y s**on dominios de primer nivel**. **NO** son dominios geográficos de dos letras. Para eso es necesario ser un estado reconocido por las Nacioness Unidas.

- **De infraestructura (arpa).**

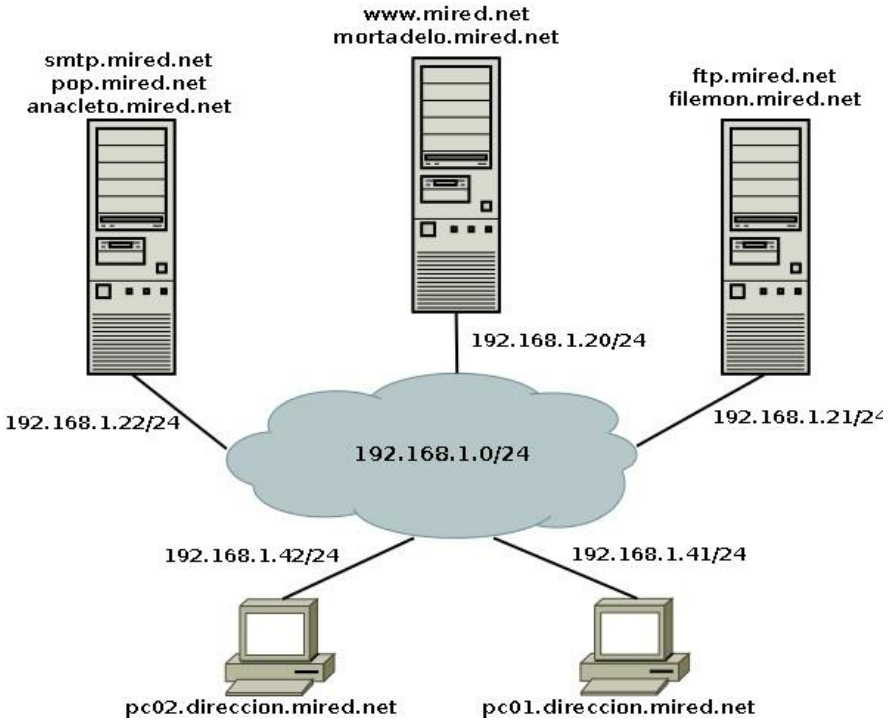
El dominio «.arpa» se utiliza para la infraestructura técnica de Internet. La **ICANN** lo administra en cooperación con la comunidad técnica de **Internet** bajo la dirección de la **IAB (Internet Architecture Board)**. Los dominios «in-addr-arpa.» e «ip6.arpa.» se utilizan para la **resolución inversa de direcciones**.

- **Dominios reservados.**

Existen nombres de **dominio de primer nivel** reservados para pruebas y de ejemplo que no entran en conflicto con nombres **TLD** actuales o futuros. Ejemplos de estos dominios son: «.test», «.example», «.invalid», «.localhost»,… Puede ocurrir que los dominios geográficos de primer nivel contengan a su vez alguno de los dominios genéricos. Estos dominios serían de segundo nivel (com.es, edu.au, org.uk, teso.org.es, etc.).

NOMBRES RELATIVOS Y ABSOLUTOS: FQDN

Imaginemos que usamos el dominio «mired.net.» para identificar todos los equipos de nuestra **red local**. Dicha red estará formada por varios equipos y cada uno se identificará con uno o varios nombres pertenecientes al dominio «mired.net.».



Según la figura anterior, si preguntamos por el nombre «www.mired.net.» sabremos que su **IP** es la **192.168.1.20**, pero si preguntamos por «www.google.es.» sabemos que es otra **IP** diferente. Si tan solo utilizamos «www» podríamos entender que se refiere al equipo «www.mired.net.» ya que en nuestra **red local** utilizamos el dominio «mired.net.». Pero ¿por qué tiene que ser este y no «www.google.es.» o «www.renfe.es.»? *Cuando se referencia un dominio se puede emplear su* ***nombre relativo*** *o su* ***nombre absoluto***.

- **Nombres relativos:** es necesario conocer el contexto del dominio superior para determinar a que nombre se hace referencia exactamente. Por ejemplo www, ftp, mortadelo, filemon.
- **Nombres absolutos:** nombre formado por todas las partes separadas por puntos desde el nodo correspondiente hasta el **dominio raíz**. Por ejemplo, «www.mired.net.». Los nombres expresados de esta forma se llaman **nombres de dominio completos (Fully Qualified Domain Names, FQDN)**.

El (.) al final del **dominio raíz** permite distinguir si el nombre usado es o no **FQDN**.

DOMINIOS Y ZONAS

El DNS se divide en muchas zonas diferentes. Estas zonas diferencian entre áreas gestionadas claramente en el espacio de nombres DNS. Una zona DNS es una parte del espacio de nombres DNS que está gestionada por una organización específica o un administrador. **Podríamos definir una Zona como**:

"*Una base de datos completa para un subarbol podado del espacio de dominios*".

Cada zona está bajo una autoridad y puede delegar la gestión de una parte del árbol. El origen del árbol del DNS contiene la zona raíz que contiene las delegaciones para los TLDs. Cada TLD constituye a su vez una zona del DNS, al igual que los dominios de segundo nivel y así sucesivamente. Cada una de estas zonas puede estar bajo una autoridad distinta.

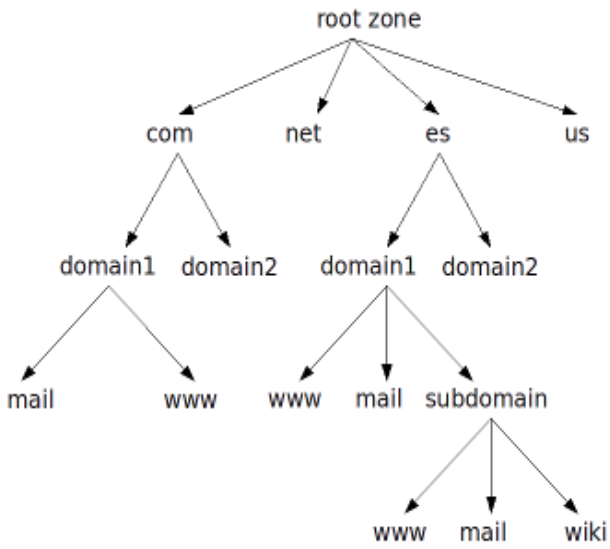
La zona DNS empieza en un dominio dentro del árbol y se puede extender hacia abajo en subdominios para que una entidad pueda gestionar múltiples subdominios.

Un error típico es asociar una zona DNS con un nombre de dominio o con un solo servidor DNS. De hecho, una zona DNS puede incluir varios subdominios y puede haber varias zonas en el mismo servidor. Las zonas DNS no están necesariamente separadas físicamente entre sí, se usan estrictamente para delegar el control.

Por ejemplo, imaginemos una zona hipotética del dominio pepitogrillo.com y tres de sus subdominios: support.pepitogrillo.com, community.pepitogrillo.com y blog.pepitogrillo.com. Supongamos que el blog es un sitio robusto e independiente que necesita administración por separado, pero las páginas de asistencia y de comunidad están asociadas más estrechamente con pepitogrillo.com y se pueden gestionar en la misma zona que el dominio principal. En este caso, pepitogrillo.com así como los sitios de asistencia y comunidad estarían todos en una zona, mientras que blog.pepitogrillo.com tendría su propia zona.

En este esquema podemos ver varios niveles de la estructura del DNS, arriba del todo, en el origen, está la zona raíz, que es gestionada por la ICANN y contiene las delegaciones a las zonas de los TLDs, estos contienen las delegaciones de cada dominio (domain1, domain2, etc.…) los cuales constituyen zonas independientes y así sucesivamente con los subdominios.

Las zonas contienen información de los recursos que componen esa zona y se divide en Registros de Recursos (RR) y esta información se almacena en ficheros de zona.



DNS es una base de datos distribuida y permite su administración descentralizada mediante la delegación de dominios.

La administración descentralizada de **DNS** se basa en la **delegación**. La delegación de dominios **DNS** consiste en que la organización que administra un dominio transfiere a otras organizaciones uno, varios o todos los dominios que administra. La **ICANN** administra el **dominio raíz** y delega en otras organizaciones los dominios **TLD**. A su vez, las organizaciones que administran los dominios **TLD**, pueden delegar en otras organizaciones los **dominios de segundo nivel**. A su vez, cada organización puede delegar la administración de sus subdominios en otras organizaciones.

La organización que administra un dominio es la responsable de los nombres usados en ese dominio, las **IPs** asociadas a dichos nombres y el mantenimiento y la administración de los servidores de nombre que alojan dichos dominios.

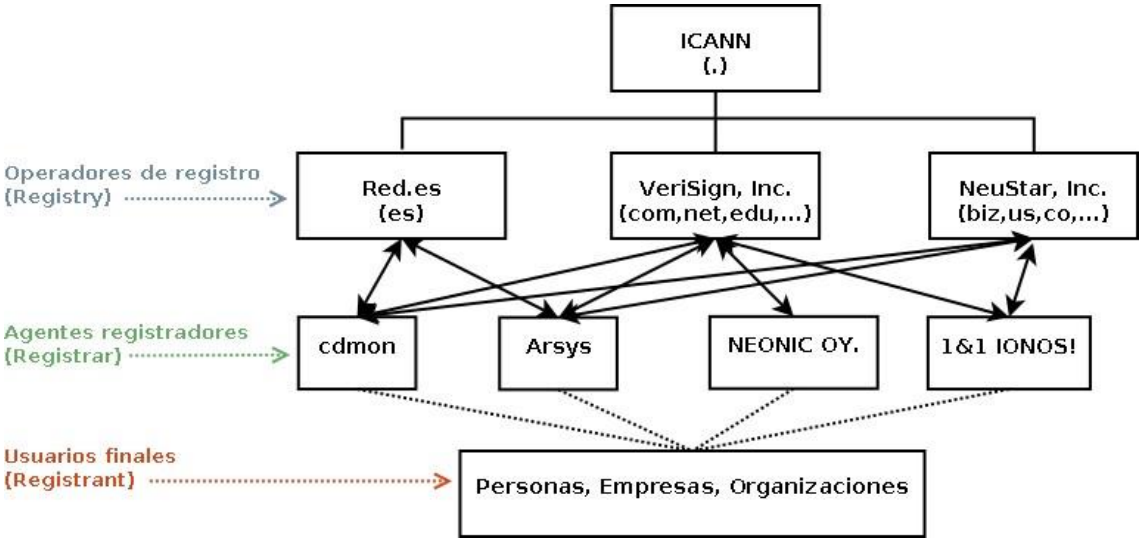
El dominio puede ser dividido en subdominios por el administrador y delegar el control de cada uno. La autoridad que se hace cargo de la delegación debe asumir también la responsabilidad de mantener actualizados los registros de recursos de ese subdominio. Pero delegación no significa independencia, sino coordinación. La división de un dominio en subdominios no implica siempre una cesión de autoridad.

Básicamente, registrar un dominio consiste en reservar un nombre durante un tiempo, normalmente se registra por un año y se va renovando el registro anualmente. Tras registrarlo, se podrán crear subdominios y asociar IPs al dominio o subdominios, además de asociar al dominio o subdominios la información que se considere oportuna.

Las organizaciones denominadas registradores (registrar) podrán registrar nombres de dominio de segundo nivel, por ejemplo: pepitogrillo.es.

Los nombres de dominio podrán ser registrados a través de los denominados agentes registradores (registrar). Estos, asesoran a los registradores (registrant) y tramitan la solicitud haciendo de intermediarios con los operadores de registro (registry). Los operadores de registro también pueden actuar como agentes registradores. Los agentes registradores deben de estar acreditados por los operadores de registro y tienen autoridad para asignar parte del precio que cuesta el registro.

REGISTRO DE DOMINIOS. AGENTES REGISTRADORES.



¿Qué son los dominios y zonas?

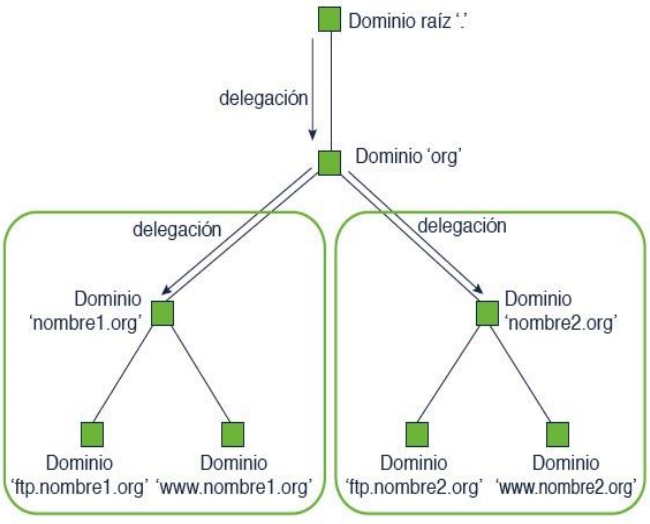
- El servidor de nombres almacena información acerca de algunas partes o zonas del espacio de nombres de dominio.
- Se dice que el servidor de nombres tiene autoridad sobre la zona.
- Por lo tanto, un servidor de nombres podrá tener autoridad sobre varias zonas.
- La zona es un archivo que contiene determinados registros de la base de datos del espacio de nombres de dominio, que identifican a uno o más dominios.

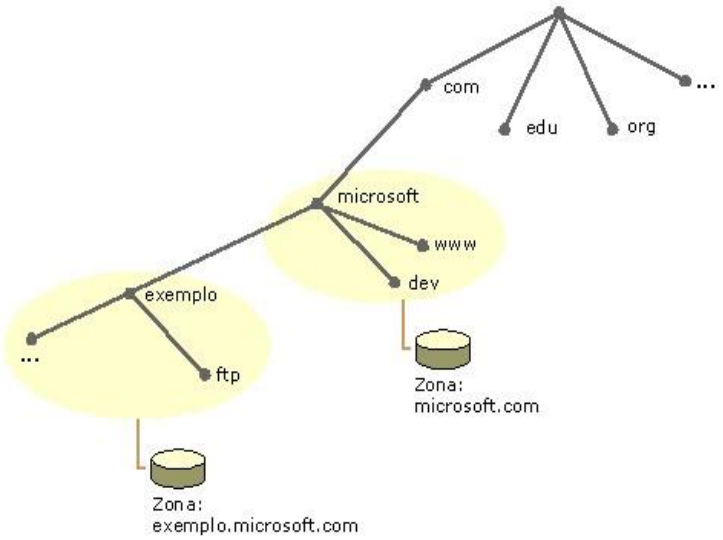
- La acción de cesión de la autoridad.
    - Por parte del dominio padre, sobre alguno de sus subdominios.
    - La puede volver a retomar cuando el dominio padre decida.
- Permite llevar a cabo una administración descentralizada.

- Es decir, el dominio puede ser dividido en subdominios por el administrador del dominio.
- Y el control de cada subdominio puede ser delegado.

- La condición es que la autoridad que asume la delegación debe asumir también la responsabilidad de mantener actualizados los datos.
  - Registros de recursos de ese subdominio.

- Delegación no significa independencia, sino coordinación.
  - Si al padre le consultan acerca de nombres incluidos en uno de sus subdominios delegados, puede hacer referencia a ellos.
  - Ya que mantiene enlaces con ellos
- La división de un dominio en subdominios no implica siempre la cesión de la autoridad sobre ellos.
  - Un dominio puede subdividirse en diferentes subdominios y el dominio mantener la autoridad sobre ellos.
  - Pero también puede delegar la autoridad de alguno de sus subdominios.





SERVIDORES DE NOMBRES

Los **servidores de nombres de dominio** o **servidores DNS**, son programas encargados de guardar información sobre **nombres de dominio**. La utilidad de los **servidores DNS** es enlazar el dominio con su correspondiente **IP** y responder a las preguntas que los **clientes DNS** y otros **servidores DNS** les hacen sobre los dominios que administran. Por lo tanto, cada **servidor DNS** almacena una parte de la **base de datos DNS**. Por defecto, el **servicio DNS**, escucha por los puertos **53/TCP** y **53/UDP.**

- **Servidor primario o maestro:**

Un **servidor maestro** o **primario**, define una o varias **zonas** de las que es **autorizado**. Sus **archivos de zona** son de lectura y escritura y es en ellos donde el administrador del servidor añade, modifica o elimina nombres de dominio.

- Si un **cliente DNS** u otro **servidor DNS** le pregunta por algún nombre de dominio para el que **es autorizado**, consulta con los **ficheros de zona** y responde a la pregunta.
- Si un **cliente DNS** u otro **servidor DNS** le pregunta por algún nombre de dominio para el que **no es autorizado**, tendrá que preguntar a otros **servidores DNS** o responder que no conoce la respuesta.
- Obtiene la información de sus zonas de sus archivos locales.
- Todas las modificaciones sobre una zona se llevan a cabo en el servidor primario.

- **<u>Servidor secundario (esclavo)</u>:**

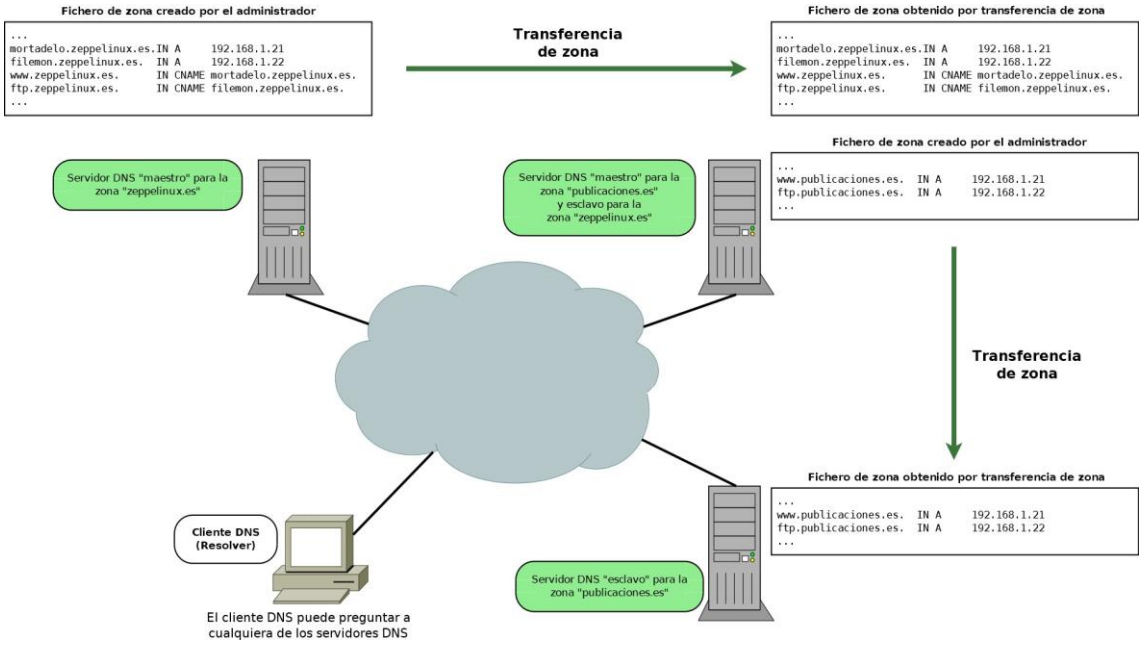
Un **servidor esclavo** o **secundario** define una o varias **zonas** para las que es **autorizado**. La diferencia con respecto a un **servidor maestro** es que los **ficheros de zona** los obtiene de otro **servidor autorizado** para la **zona**, normalmente, de un **servidor maestro** mediante un procedimiento denominado **transferencia de zona**. Los **ficheros de zona** de los **servidores esclavos** son de solo lectura y por lo tanto, el administrador no tiene que editarlos. La modificación de los **archivos de zona** debe realizarla el **servidor maestro** que transfiere la zona. El funcionamiento de como responden a los **clientes DNS** o a otros **servidores DNS** es similar al de un **servidor maestro**.

Un servidor puede ser **maestro** para una o varias **zonas** y al mismo tiempo ser **esclavo** para otras. Pueden existir varios **servidores esclavos** para una misma zona. Las razones de su existencia pueden deberse a:

- Reducir y repartir la carga entre varios servidores DNS.
- Favorecer la tolerancia a fallos.
- Ofrecer mayor rapidez.

Lo ideal es que los **servidores DNS** para una misma **zona** estén ubicados en redes y localizaciones diferentes para evitar que, si ocurre algún problema no les afecte simultáneamente y deje sin servicio de resolución a los nombres de esa **zona**.

SERVIDORES DE NOMBRES: CLASIFICACIÓN.



- **<u>Servidor Caché</u>**:

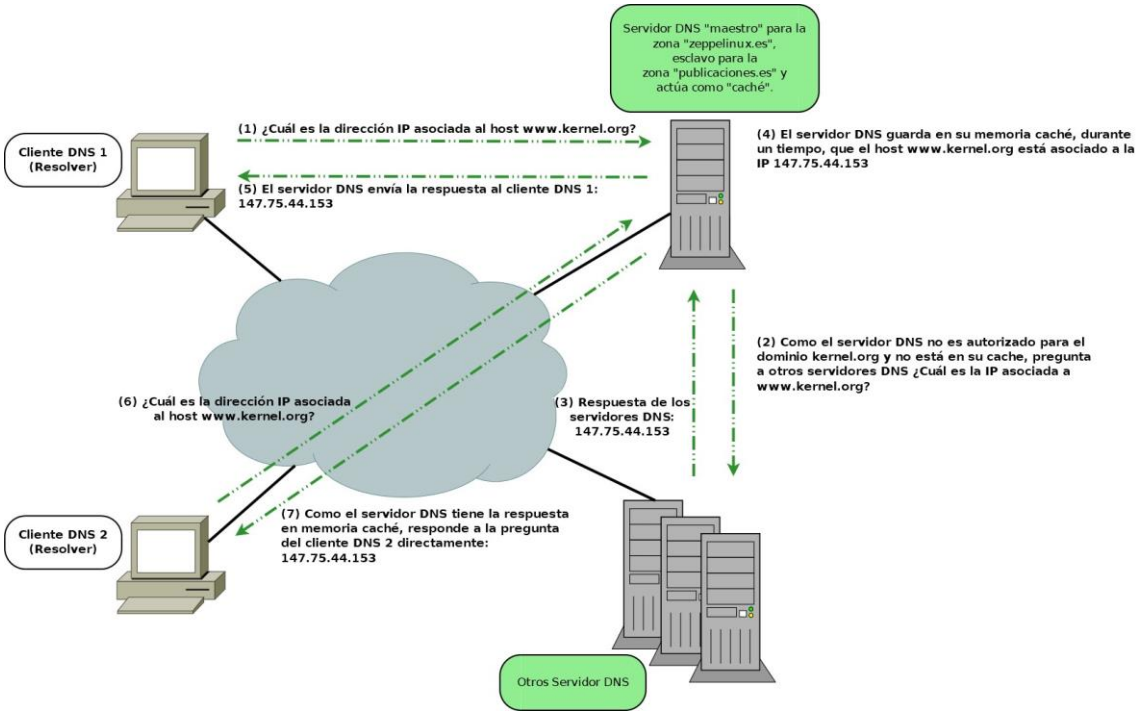
Los **servidores DNS** se configuran como **servidores cache** para mejorar los tiempos de respuesta de las consultas, reducir la carga de los equipos y disminuir el tráfico de red.

Cuando un **servidor DNS** recibe una pregunta sobre un dominio para el cual no es **autorizado**, es decir, de un nombre del cual no tiene información, puede preguntar, si así está configurado, a otros servidores para obtener la respuesta. Si el servidor actúa como **cache**, guarda durante un tiempo (**TTL: Time To Live**) las respuestas a las últimas preguntas que ha realizado a otros **servidores DNS**. Cada vez que un **cliente DNS** u otro **servidor DNS** le formula una pregunta, comprueba si tiene la respuesta en su **memoria cache**, si la tiene, no tendrá que preguntar a otro **servidor DNS** por la pregunta.

Un **servidor DNS** es **solo cache (cache only server)** cuando:

- No tiene **autoridad** sobre ninguna **zona**.
- Pregunta a otros **servidores DNS** para resolver las preguntas de los **clientes DNS** y las guarda en su **memoria cache**.

En el siguiente gráfico se explica como dos **clientes DNS** hacen preguntas a un mismo **servidor DNS** que es autorizado para algunas zonas y además actúa como caché.



- **<u>Servidor Reenviador</u>**:

Cuando a un **servidor DNS** se le hace una pregunta sobre un **nombre de dominio** del que no dispone información (**no es autorizado**), este puede preguntar a otros **servidores DNS**.

Un **reenviador (forwarder)** es un **servidor DNS** que otros **servidores DNS** designan para reenviarle consultas. Son utilizados para minimizar las consultas y el tráfico de peticiones **DNS** desde una red hacia **Internet**. Además, permiten a los equipos locales utilizar su cache DNS para minimizar los tiempos de respuesta.

- **<u>Servidor autoritativo</u>**:

Un servidor DNS autoritativo es un servidor que alberga realmente registros de recursos DNS y es responsable de los mismos. Este es el servidor al final de la cadena de búsqueda DNS que responderá con el registro del recurso consultado.

Un servidor de nombres autoritativo puede satisfacer solicitudes con sus propios datos sin necesidad de consultar a otros recursos, ya que es la fuente final de verdad para ciertos registros DNS. Un servidor DNS es autoritativo para una zona si contiene los registros de recursos para dicha zona.

Cada zona puede tener uno o más servidores DNS autoritativos.

- Uno de ellos debe ser primario.

- Si tiene varios, el resto puede ser secundario o caché.

NOTA: Un **Servidor solo autorizado (authoritative only)** es aquel que es **autorizado** para una o varias **zonas** como servidor **maestro** y/o **esclavo** y no responde a preguntas que no sean relativas a sus **zonas**. Es decir, no tiene activada la **recursividad**, no es **reenviador** y no actúa como **caché**.

Servidor autoritativo

- Si es servidor primario:
    - Los registros de recursos para la zona se encuentran en los archivos de la zona, almacenados en el sistema de archivos del propio servidor DNS.
- Si es servidor secundario
    - Los registros de recursos de la zona se cargan desde otro servidor de nombres (primario).
    - Utilizando el proceso de transferencia de zona.
- Si es servidor caché:
    - Utiliza el método de búsquedas recursivas.
    - Los resultados de las búsquedas que realiza los va almacenando en la caché.

CLIENTES DNS O RESOLVER

ES todo programa capaz de preguntar a un **servidor DNS** e interpretar sus respuestas.

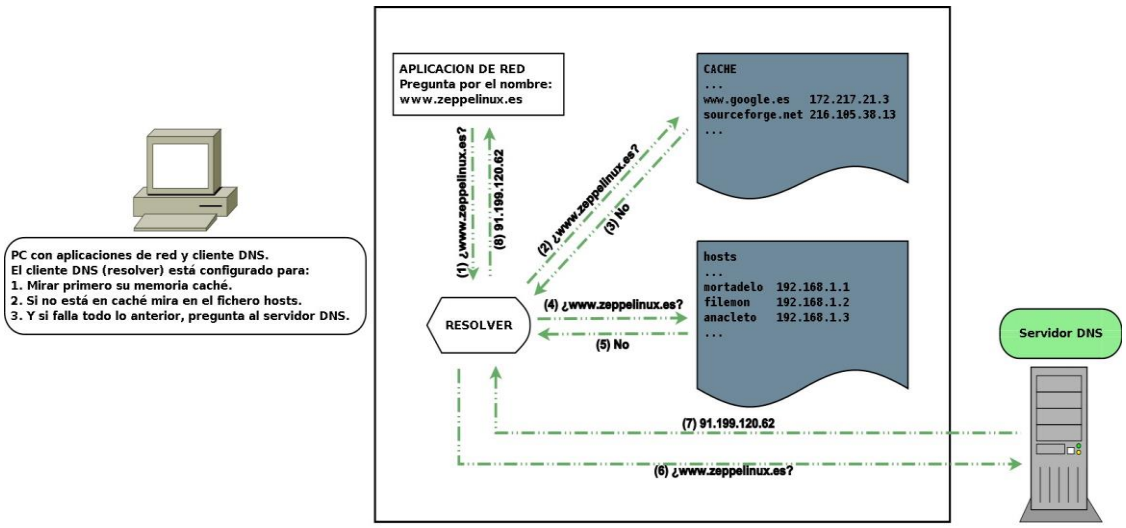
Los **sistemas operativos** incluyen o permiten instalar un conjunto de librerías que se encargan de realizar estas funciones. Dichas librerías son invocadas por las aplicaciones (clientes FTP, navegadores web, clientes de correo, etc.) cuando estas manejan **nombres de dominio**. Los **clientes DNS** mantienen una **memoria caché** de respuestas, al igual que los **servidores DNS**, de tal manera que minimizan el uso de la red y aumentan el rendimiento.

La forma en la que los **clientes DNS** resuelven los **nombres de dominio** es configurable. En la mayoría de **sistemas operativos** existen ficheros de texto en los

que se pueden asociar **direcciones IP** a **nombres de dominio** o de **hosts**, y se puede configurar si el **cliente DNS** consultará, en primer lugar, estos archivos para hacer la resolución. También es posible habilitar o no la **caché** de respuestas.

Cuando una aplicación quiere resolver un nombre invoca al **cliente DNS**. La configuración habitual es de la siguiente forma:

- La aplicación pregunta al **cliente DNS (resolver)** por un **nombre de dominio** o de **host**.
- El **resolver**, si así está configurado, consulta la **caché** que se almacena en memoria. Si el nombre ya está almacenado en la **caché**, entrega la respuesta a la aplicación.
- Si el nombre a buscar no se encuentra en la **caché**, el **resolver** buscará en el fichero **hosts** del equipo. En sistemas **UNIX/Linux** el archivo es /etc/hosts y en los sistemas **Windows** el archivo es %SYSTEMROOT%\system32\drivers\etc\hosts. Si el nombre está almacenado en el archivo **hosts**, entrega la respuesta a la aplicación.
- Si el nombre a buscar no se encuentra en el archivo **hosts**, el **resolver** realiza una consulta **recursiva** al **servidor DNS** que esté configurado y entregará la respuesta de este a la aplicación.



Existen programas/comandos que funcionan como **clientes DNS (resolvers)** y permiten definir qué tipo de consulta se quiere realizar a un **servidor DNS**. Son utilizados para depurar u obtener información de **servidores DNS** y del **proceso de resolución**. Algunos de estos programas son **nslookup**, **dig** y **host.**

- Mecanismo por el que se traducen los nombres de máquinas a direcciones IP.

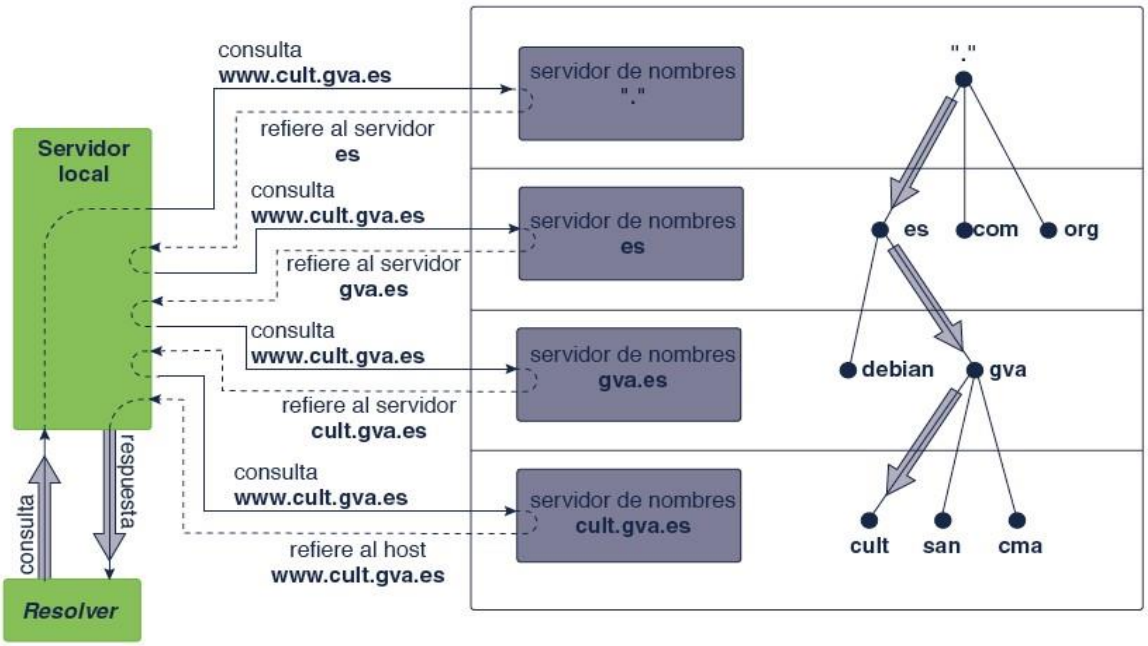
- El usuario intenta conectarse desde su máquina local a un servidor remoto mediante su URL (nombre). Se ha de transformar en una IP concreta.
- El cliente DNS de la máquina local debe hacer la consulta al servidor DNS mediante los resolvedores (resolvers).
- El servidor DNS responde obteniéndose la IP del servidor remoto y accediendo al sitio.
- Todo ello de forma transparente al usuario.

Tanto los **clientes DNS** como los **servidores DNS** consultan a otros **servidores DNS** para resolver **nombres de dominio**. Las consultas a un **servidor DNS** pueden ser **recursivas** o **iterativas.**

MÉTODOS DE BÚSQUEDA: ITERATIVA

Búsqueda iterativa:

- El DNS local devuelve la mejor respuesta que puede ofrecer al cliente en función del contenido de su caché.
- Pero si no dispone de la información indica la IP del siguiente servidor de nombres autorizado a preguntar, comenzando siempre por un servidor raíz.
- Éste le refiere al servidor del nivel siguiente que lo contiene, y el servidor local vuelve a lanzar la petición al servidor referido.
- Éste si no dispone de la información solicitada, le refiere al servidor del nivel siguiente que lo contiene. el DNS local vuelve a lanzar la petición al este servidor y así sucesivamente.



MÉTODOS DE BÚSQUEDA: RECURSIVA.

Búsqueda recursiva**:**

- Se realiza una petición de resolución de nombre al DNS local.
- Si el servidor no dispone de la información va a buscarla al DNS con autoridad que la contiene.
- El DNS local asume la responsabilidad de dar una respuesta al cliente consulta a los otros servidores en nombre del cliente.

RESOLUCIÓN DE NOMBRES: ESQUEMA.

El usuario hace una petición de una URL desde su navegador web. La resolución del nombre dado a través de la URL sigue los pasos:

El cliente DNS (resolvedor) consulta a un servidor DNS local. El DNS local, ¿tiene información sobre el dominio consultado?

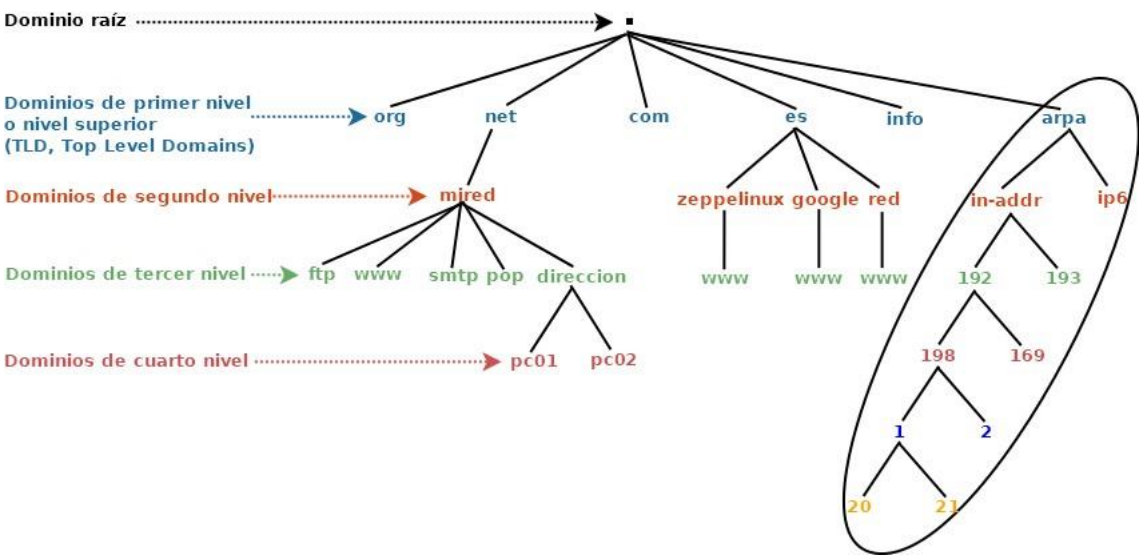
- SÍ: devuelve registros del recurso (RR).
- NO: ¿Lo tiene en la caché?
  - SÍ: devuelve registros del recurso
  - NO: existen dos posibilidades.:
    - Hacer una **consulta recursiva**
    - Hacer una **consulta iterativa**

RESOLUCIÓN INVERSA:

La **resolución inversa** consiste en obtener información de un **nombre de dominio** preguntando por la **dirección IP** en vez de preguntar por el **nombre de domino** como hemos hecho en artículos anteriores. Por ejemplo, preguntar cual o cuales son los **nombres de dominio** asociados a la **dirección IP** 8.8.8.8.

Normalmente la **resolución inversa** se utiliza, por ejemplo, para resolver problemas de red, detectar **spam** en los servidores de correo, seguir la traza de un ataque, conocer que nombres aloja un servidor de **hosting**, para comprobar la identidad del cliente, por temas de seguridad etc.

El funcionamiento de la **resolución de direcciones IP** es igual al de la **resolución de nombres de dominio**. Las **direcciones IP** se tratan como nombres que cuelgan del dominio «in-addr.arpa» para las direcciones **IPv4**, y del dominio «ip6.arpa» para las direcciones **IPv6**.



Por ejemplo, el dominio «www.zeppelinux.es» lo leemos y escribimos de izquierda a derecha, pero su **estructura jerárquica** es de derecha a izquierda, el dominio más alto de la jerarquía es el dominio raíz «.», después «es», después «zeppelinux» y por último «www».

Cuando usamos una **dirección IP**, por ejemplo «192.198.1.21», para realizar una **pregunta DNS inversa**, en realidad estamos preguntando por el **nombre de dominio** «21.1.198.192.inaddr.arpa». La estructura jerárquica de la **dirección IP**, tratada como nombre de dominio, es de derecha a izquierda, comenzando por el dominio «in-addr.arpa».

.arpa (**Address and Routing Parameter Area**) es un **dominio de nivel superior genérico** utilizado sólo para la infraestructura de **Internet**. Los subdominios de .arpa o dominios de segundo nivel «in-addr.arpa» e «ip6.arpa» son usados por los **servidores DNS inversos** para la obtención de direcciones **IPv4** e **IPv6** respectivamente. Cuando **mapeamos una dirección IP** estamos asociando la **dirección IP** al nombre en el dominio .arpa. Por ejemplo la dirección «192.198.1.21» es mapeada al nombre «21.1.198.192.in-addr.arpa».

Los **servidores DNS** almacenan **zonas de resolución inversa** con **registros de recursos (RR)** que asocien **nombres de dominio** con **direcciones IP**. Las **zonas de resolución inversa** pueden ser **maestras** o **primarias** y **esclavas** o **secundarias**. **Las zonas de resolución directa e inversa son independientes** y es responsabilidad de los administradores de los **servidores DNS** que dichas **zonas contengan información coherente y que no existan discrepancias**.

No es obligatorio que la entidad que administra una **zona de resolución directa** de un dominio tenga que administrar la **zona de resolución inversa** que se corresponda con las direcciones IPs asociadas a dicho dominio.

El proceso de **resolución inversa** es similar al de **resolución directa**. Las **direcciones IP** se tratan como **nombres de dominio**. Por lo tanto, existen consultas **recursivas**, **iterativas**, **cache**, **TTL**, etc. Por ejemplo, si un **cliente DNS** realiza una **consulta recursiva** de la **IP** 192.198.1.21 a un **servidor DNS**, éste, si no lo tiene en **cache**, iniciará una serie de **consultas iterativas** a los **servidores DNS raíz**, a los **servidores autorizados** para el dominio 192.in-addr.arpa y así sucesivamente.

De la misma forma que los nombres de dominio se resuelven efectuando consultas para cada componente de derecha a izquierda, las direcciones IP siguen el mismo esquema. Su dominio raíz se denomina in-addr.arpa. Las direcciones IP están escritas en orden inverso en el dominio in-addr.arpa (es decir, utiliza una notación de puntos invertida, algo lógico, ya que las redes se diferencian por los primeros valores de su dirección IP). Cada servidor de nombres de dominio autoritario requiere una zona de resolución inversa.

- Ejemplo:

Para la IP 192.168.1.2.,

1- el DNS buscará los servidores arpa.
2- Luego los servidores in-addr.arpa.
3- Después 192.in-addr.arpa.
4- El siguiente 168.192.in-addr.arpa;
5- Y, por último, los servidores 1.168.192.in-addr.arpa. Aquí se encontrará el buscado: 2.1.168.192.in-addr.arpa.

Las direcciones IP están escritas en orden inverso en el dominio in-addr.arpa. Se utiliza una notación de puntos invertida.