

DNS

Sistema de Nombre de Dominio

1.- Introducción

Para poder comunicarse con un ordenador necesitamos saber su dirección IP. Dado que las direcciones IP son difíciles de memorizar o recordar necesitamos asignar a las direcciones nombres significativos, por ejemplo, para poder ver la página web de la universidad de Valencia, www.uv.es, necesitaríamos saber la dirección IP del servidor web de esta, que en este caso es *147.156.1.46*, lo mismo para cualquier otra página web que se nos ocurra, www.yahoo.com, www.sun.com, robotica.uv.es, etc. Este método es inviable y engorroso.

En los comienzos de Internet se utilizaba una única tabla centralizada de traducción de nombres a direcciones. En los 70 el ARPANET estaba formada por unos cientos de máquinas y un sólo archivo, *HOSTS.TXT*, que contenía toda la información que se necesitaba sobre esas máquinas. El centro de información de red del Departamento de defensa disponía de la versión maestra de la tabla y otros sistemas realizaban una copia regularmente.

Con el paso del tiempo y cuando Internet, con los protocolos TCP/IP “explotó”, este método, como podemos imaginar, presento serios inconvenientes, entre los que podemos destacar los siguientes:

- El tráfico y la carga de red para la máquina que contenía las tablas que hacía posible el mapeo era desbordante.
- La consistencia del archivo era muy difícil de mantener, cuando el *HOST.TXT* llegaba a una máquina muy lejana era ya obsoleto.
- No se podía garantizar la no duplicidad de nombres, dado que mantener una administración central en una red Internacional era algo muy complicado.
- El método era claramente no Escalable.

Conclusión, el método se convirtió en obsoleto y muy ineficiente a medida que aumentaron el número de máquinas. Es entonces cuando surgió un nuevo sistema de resolución de nombres, *DNS (Domain Name System)*, que solucionó los problemas anteriores.

DNS, el Sistema de Nombres de Dominio

El Sistema de Nombres de Dominio (DNS, Domain Name System) básicamente es un esquema que permite asignar nombres significativos de alto nivel a grandes conjuntos de máquinas y direcciones IP. El esquema es jerárquico y basado en dominio utilizando una Base de Datos Distribuida para implementarlo. Se utiliza un mecanismo Cliente/Servidor, donde unos programas llamados servidores de nombres contienen información acerca de un segmento de la base de datos y la ponen a disposición de los clientes, llamados *resolvers*. Los llamados *resolvers* son rutinas de biblioteca que crean preguntas y las envían en forma de paquete UDP a un servidor DNS local. Este devuelve al resolver la dirección IP correspondiente al nombre solicitado en la pregunta.

El servicio DNS los podemos situar en la arquitectura de TCP/IP como protocolo de aplicación. Véase la siguiente figura:

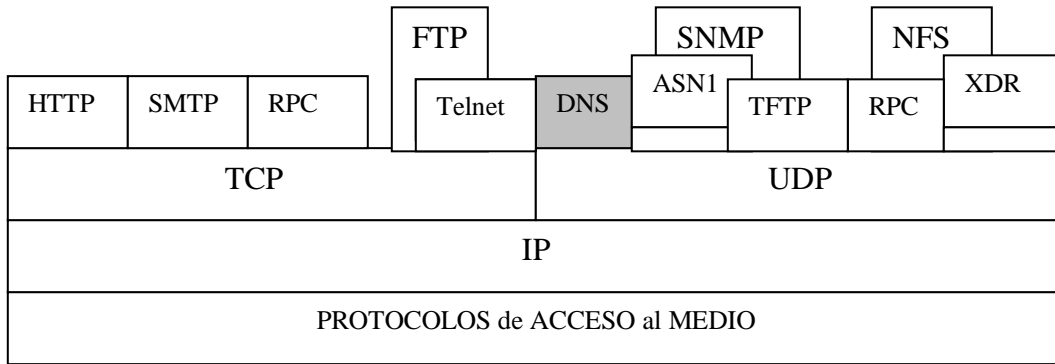


Figura 1: Modelo TCP/IP

Gracias a la estructura y funcionamiento del DNS se eliminaron los problemas inherentes al sistema de archivo plano. A continuación describimos brevemente el porqué:

- *Carga de la red y de los hosts:* este problema ya no existe debido a que la información está distribuida por toda la red, al tratarse de una bdd distribuida.
- *Duplicidad de Nombres:* el problema se elimina debido a la existencia de dominios controlados por un único administrador. Puede haber nombres iguales pero en dominios diferentes.
- *Consistencia de la Información:* ahora la información que está distribuida es actualizada automáticamente sin intervención de ningún administrador.

2.- DNS en detalle

El Sistema de Nombres de Dominio lo podemos desglosar en dos conceptos independientes: el primero, especifica la sintaxis del nombre y las reglas para delegar la autoridad respecto al nombre. Y el segundo especifica la implementación en ordenadores de la base de datos distribuida que transforma de una manera eficiente los nombres a direcciones IP.

Nombres de Dominio

Como dijimos anteriormente el DNS se basa en un esquema jerárquico de nombres denominado *nombre de dominio*. Un *nombre de dominio* consiste en una secuencia de etiquetas separadas por un punto. Por ejemplo, *robotica.uv.es*, contiene tres etiquetas, el dominio de nivel inferior es *robotica.uv.es*, el segundo nivel de dominio es *uv.es*, y el nivel superior es *es*. Como jerarquía que es podemos apreciar que el dominio de nivel local corresponde con la primera etiqueta, y el de nivel superior la última etiqueta.

Como veremos posteriormente, en la práctica un dominio es un índice en la base de datos de DNS. Un dominio puede ser una máquina o puede ser un nodo del cual pueden partir otros dominios (o ambas cosas a la vez).

En Internet se ha decidido particionar el nivel superior en dos tipos de dominios, los geográficos y los genéricos. Con los primeros se pretende dividir los recursos a direccionar por país (por ej, *uv.es*), también son conocidos como ISO3166 . Con los segundos se pretende un división en función del tipo de organización. A continuación podemos ver una tabla con algunos de los dominios genéricos más utilizados:

Nombre de Dominio	Significado
COM	Organizaciones comerciales, Microsoft.com, ibm.com
EDU	Universidades, Instituciones academicas,...
GOV	Instituciones Gubernamentales
MIL	Organizaciones militares
ORG	Organizaciones no comerciales
NET	Grupos relacionados con la Red
INT	Organizaciones Internacionales
De reciente aparición	
TV	Televisións
FM	Emisoras de radio
...	...

Todos los dominios en Internet pueden representarse mediante un árbol. Las hojas del árbol serían los dominios que ya no contiene más dominios (subdominios, aunque este término no esta definido es bastante utilizado). Entonces, cada dominio en Internet estaría definido por la trayectoria hacia arriba desde él a la raíz (esta está vacía). El árbol tendría la siguiente forma:

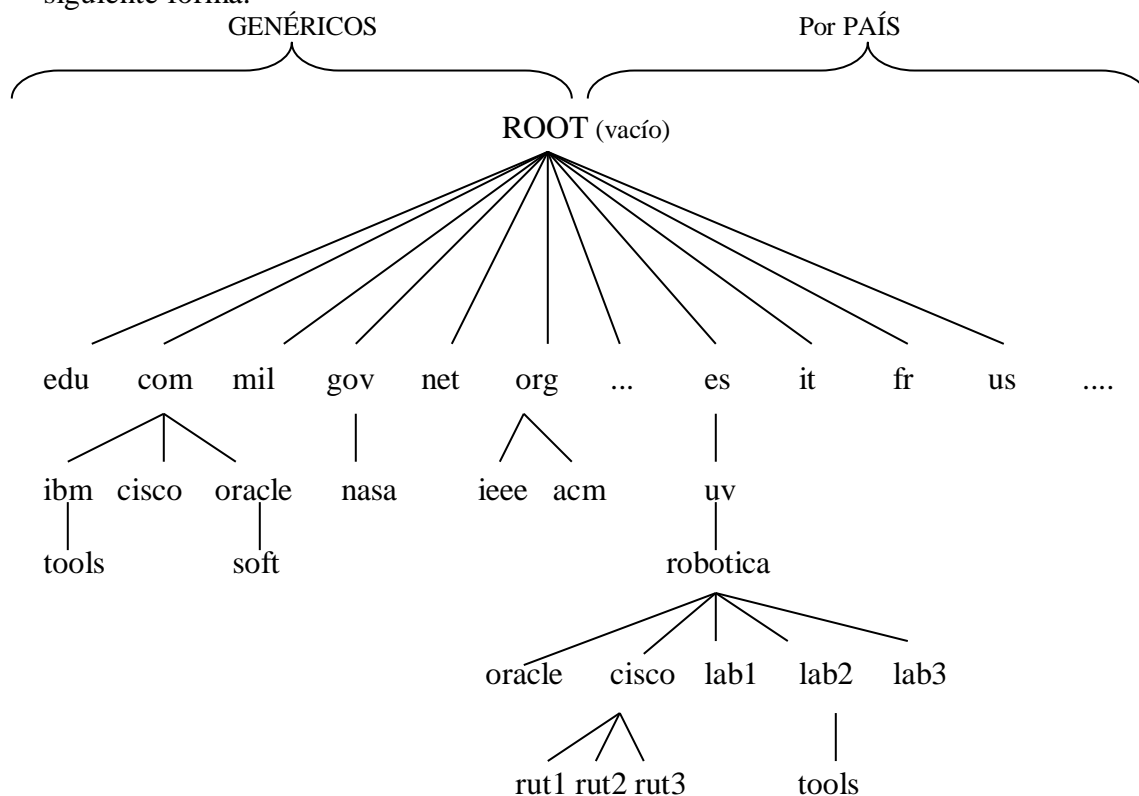


Figura 2: árbol de la jerarquía de nombres de Internet

Como puede verse en el árbol al ser jerárquico no hay conflicto cuando dos nombres son iguales, mientras pertenezcan a dominios distintos. En la figura 2, por ejemplo, esto se da con *oracle.com* y *oracle.robotica.uv.es*.

Los nombres pueden ser texto ascii de hasta 63 caracteres de longitud, mientras que los nombres de trayectoria completa (desde la hoja hasta la raíz) no debe sobrepasar los 255 caracteres.

Delegación de la Autoridad

La organización que posee un Nombre de Dominio, como por e.j. *uv.es*, es responsable del funcionamiento y mantenimiento de los servidores de nombres que traducen sus propios nombres a direcciones. Se crea entonces un administrador local quien bajo su responsabilidad introduce altas, bajas y cambios de forma rápida y precisa. E incluso puede delegar parte de los dominios que caen bajo su responsabilidad en otro administrador.

Para ver más claramente la relación entre la jerarquía de nombres y la delegación de la autoridad para los nombres veamos el siguiente ejemplo (véase la figura 2): una máquina del Instituto de Robótica de la Universidad de Valencia tiene el nombre de dominio oficial *oracle.robotica.uv.es*. El nombre de la máquina fue registrado por el administrador local de la red del mencionado Instituto. El Administrador de esta red local había obtenido previamente autorización para la administración del subdominio *robotica.uv.es* de una Autoridad de la red Universitaria, es decir, del Administrador de la red *uv.es*. Este a su vez había obtenido permiso de la Autoridad que Administra el dominio geográfico *.es*. Quién a su vez había obtenido el permiso para administrar el dominio superior geográfico de la Autoridad de Internet.

Para aclarar más si cabe el concepto de delegación de Autoridad, cuando alguien (Administrador, Entidad, Grupo,..) recibe la responsabilidad de Administrar un dominio, a partir de ese dominio es él el único responsable de administrar como mejor crea conveniente todos los subdominios que caen bajo el nodo que él administra. Consecuencia de esto lo podemos ver en el dominio superior *us*. La autoridad que lo administra a creído conveniente dividirlo en un segundo nivel por estado. De esta forma quién quiera conectarse bajo el dominio de EE.UU, *us*, deberá hacerlo obligatoriamente bajo un dominio de segundo nivel. Por ejemplo, imaginemos la empresa *ComputerUncleTom* situada en *Virginia* en EE.UU. La empresa desea conectarse a internet bajo el dominio superior *us*. Ésta no podría hacerlo directamente, debería conectarse como dominio de segundo nivel, es decir, *computeruncletom.va.us*

Registro de Recursos

Cuando un *resolver* da un nombre al DNS para que este le responda, el nombre dado puede transformarse en más de un aspecto en el sistema de dominio. Es decir, la respuesta no tiene porque se únicamente una dirección IP, sino que pueden ser muchos

tipos de recursos, como por ejemplo, una dirección que sólo acepta correo electrónico. Por tanto, cuando el cliente envía al DNS el nombre del objeto o recurso que busca indica el tipo de objeto que busca (también existe la posibilidad de pedir todos los recursos asociados con el nombre).

Los datos del DNS se almacenan como una serie de entradas de texto, llamadas *Registros de Recursos* (RR). Un RR esta formado por cinco tuplas y tiene el siguiente formato:

[Nombre_dominio] [TTL] [Clase] Tipo Dato_Registro(Valor)

Adicionalmente se pueden añadir comentarios en la misma línea incluyendo al principio del comentario ; .

El Primer campo, *Nombre_dominio*, indica el nombre de dominio. Puede haber más de un registro por dominio. Este campo a veces puede omitirse, en ese caso siempre se toma por defecto el último nombre de domino indicado con anterioridad.

El campo *TTL*, se refiere al tiempo de vida, e indica la estabilidad del registro, es decir, cuanto tiempo debe guardarse en caché después de almacenarse.

El campo *Clase* se refiere al tipo de información. Actualmente sólo se utiliza *IN*, para información de Internet. Este campo si se omite, al igual que el campo *Nombre* se toma el último valor indicado con anterioridad. A veces, el orden de los campos *TTL* y *Clase* pueden intercambiarse, no dando a confusión dado que *TTL* es numérico.

El campo *Tipo* indica el tipo de registro, puede contener algunos de los siguientes valores (los más importantes):

Tipo de Registro	Descripción
SOA	Inicio de autoridad, Start Of Authority), identifica el dominio o la zona y se fijan una serie de parámetros para esta zona.
NS	El nombre de dominio se hace corresponder con el nombre de una computadora de confianza para el dominio, es decir, un servidor de nombres.
A	Dirección IP de un host. Si este tiene varias direcciones IP, multihomed, habrá un registro diferente por cada una de ellas.
CNAME	Es un alias que se corresponde con el nombre canónico verdadero.
MX	Se trata de un intercambiador de correo (Mail eXchanger), es decir, un dominio dispuesto a aceptar solo correo electrónico.
TXT	Texto, es una forma añadir comentarios a la Base de Datos. Por Ej., para dar la dirección posta del dominio miempresa.com .
PTR	Apuntador, hace corresponder una dirección IP con el nombre de un sistema. Usado en archivos dirección-nombre.
HINFO	Información del Host, tipo y modelo de computadora.
MINFO	Información de Buzón o lista de correo.
WKS	Servicios públicos (Well-Known Services). Puede listar los servicios de las aplicaciones disponibles en el ordenador.

Volviendo a la estructura general del RR el campo valor será un número o texto ascii dependiendo del tipo de registro.

También decir, que el orden en la tabla de los RR no es significativo.

Ahora presentamos un ejemplo (ficticio) del tipo de información que podríamos encontrar en la base de datos del dominio de una empresa conectada a Internet, en este caso *computeruncltom.va.us* :

```
;
;Fichero Configuración
;Datos autorizados para computeruncltom.va.us
;
computeruncltom.va.us. 86400 IN      SOA      (1; Serie
                                28800 ;Refrescar cada 8 horas
                                3600  ;Reintentar cada hora
                                604800 ;Expirar al cabo 1 semana
                                86400 ) ;El defecto es un dia

;información de la empresa
computeruncltom.va.us. 86400 IN      TXT      "Empresa de Informatica"
computeruncltom.va.us. 86400 IN      TXT      "Virginia, EE.UU"
;Servidores de correo
computeruncltom.va.us. 86400 IN      MX       1 correo.computeruncltom.va.us
computeruncltom.va.us. 86400 IN      MX       2 postal.computeruncltom.va.us
;Nuestros servidores de nombres
computeruncltom.va.us. 86400 IN      NS       mesa.computeruncltom.va.us
computeruncltom.va.us. 86400 IN      NS       silla.computeruncltom.va.us
;Direcciones de hosts
correo.computeruncltom.va.us.      86400 IN      A        192.253.253.2
postal.computeruncltom.va.us.      86400 IN      A        192.253.253.3
start.computeruncltom.va.us.      86400 IN      A        192.253.253.4
start.computeruncltom.va.us.      86400 IN      A        192.253.253.5
start.computeruncltom.va.us.      86400 IN      HINFO    Linuix SuSE 7.2
mesa.computeruncltom.va.us.      86400 IN      A        192.253.253.6
silla.computeruncltom.va.us.      86400 IN      A        192.253.253.7

;Alias
www.computeruncltom.va.us. 86400 IN CNAME start.computeruncltom.va.us
ftp.computeruncltom.va.us. 86400 IN CNAME start.computeruncltom.va.us
...
...
```

A continuación describimos el significado de cada línea (omitimos la líneas que son comentarios, ;...):

- En la primera línea damos información del dominio que estamos administrando.
- En la línea siguiente damos información textual de nuestro dominio, en este caso a que se dedica la empresa y donde se localiza.
- En la cuarta y quinta línea estamos facilitando nuestros servidores de correo, es decir, máquinas que recibirán todo el correo dirigido a quiensea@computeruncltom.va.us Primero se intentará con la máquina de nombre *correo* y en caso de que esta fallará se intentaría con *postal*.
- Las líneas seis y siete contienen información de nuestros servidores de nombres

- A continuación indicamos las direcciones IP de nuestras máquinas. En esta sección véase que damos información del sistema operativo de una nuestra máquinas, *start*, que además es mutihomed.
- Por último, indicamos los alias, en este caso www.computeruncletom.va.us y ftp.computeruncletom.va.us. Nótese que de esta forma nuestra máquina *start* será un servidor web y un servidor ftp.

En este ejemplo no hemos puesto las direcciones IP a usar para buscar los dominios de nivel superior, están son facilitadas por los servidores raíz.

Servidores de nombres y zonas de autoridad

Toda la información acerca de un espacio de dominio se guarda en una computadora que llamamos Servidor de Nombres. Esto es la implementación física del llamado programa servidor que antes hemos mencionado.

Generalmente, los servidores tienen información completa acerca de una parte del espacio de dominio de nombres, que llamamos *zona de autoridad*. Más exactamente una *zona* es la porción del espacio de nombres de dominio de la que es responsable un determinado servidor DNS. La zona de autoridad de estos servidores abarca al menos un dominio y también pueden incluir subdominios, aunque a veces los servidores de un dominio puede delegar sus dominios en otros servidores.

La diferencia entre una *zona* y un *dominio* es que la primera contiene los nombres de dominio y datos que representan a un dominio y un *dominio* es un nombre a que agrupa a otras máquinas o dominios inferiores.

Veamos a continuación una forma de dividir el espacio de nombres de la figura 2:

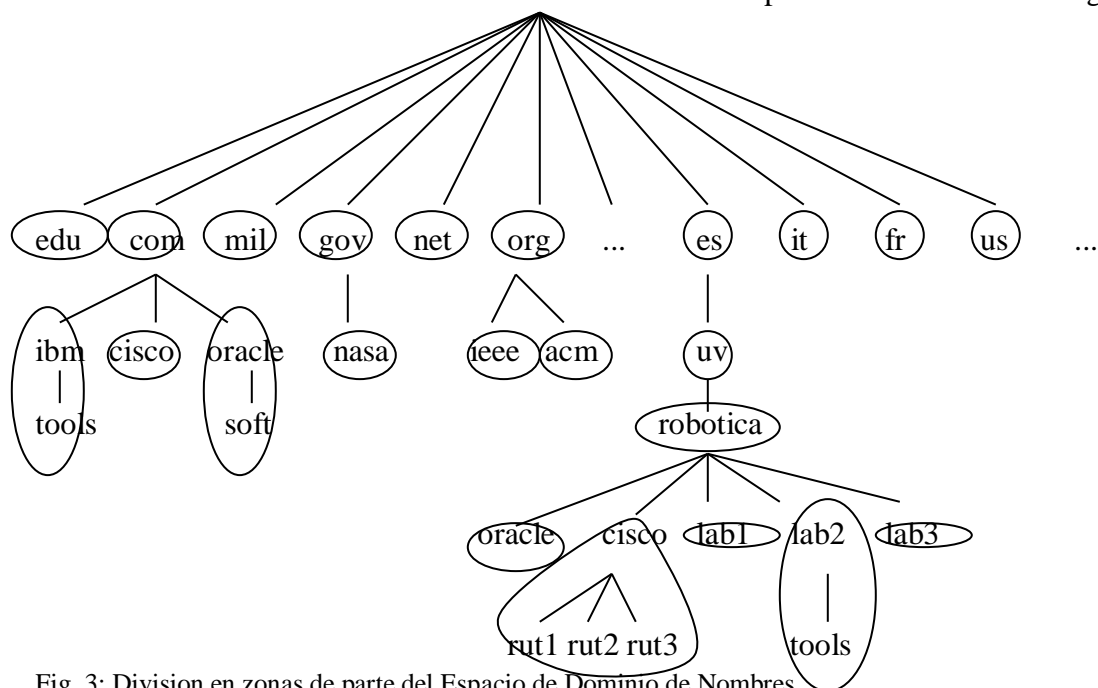


Fig. 3: División en zonas de parte del Espacio de Dominio de Nombres.

Cada zona tendrá asignada un servidor de nombres primario que obtiene su información de su base de datos local y uno o más servidores secundarios que obtienen su información del servidor de nombres primario. Recordemos que (delegación de autoridad) el lugar donde se colocan los límites de una zona dentro de una zona es responsabilidad del administrador de esa zona.

Hasta ahora hemos nombrado sólo dos tipos de servidores los Primarios y los Secundarios. Según la configuración del servidor podemos encontrarnos con cuatro tipos de servidores, desempeñando cada uno una función distinta. Veamos en detalle cada uno de ellos en la siguiente tabla:

Tipo de Servidor	Descripción
Primarios (<i>Primary Name Servers</i>)	Almacenan la información de su zona en una base de datos local. Son responsables de mantener la información actualizada y cualquier cambio debe ser notificado a este servidor
Secundarios (<i>Secondary Name Servers</i>)	Son aquellos que obtienen los datos de su zona desde otro servidor que tenga autoridad para esa zona. El proceso de copia de la información se denomina <i>transferencia de zona</i> .
Maestros (<i>Master Name Servers</i>)	Los servidores maestros son los que transfieren las zonas a los servidores secundarios. Cuando un servidor secundario arranca busca un servidor maestro y realiza la transferencia de zona. Un servidor maestro para una zona puede ser a la vez un servidor primario o secundario de esa zona. Estos servidores extraen la información desde el servidor primario de la zona. Así se evita que los servidores secundarios sobrecargen al servidor primario con transferencias de zonas.
Locales (<i>Caching-only servers</i>)	Los servidores locales no tienen autoridad sobre ningún dominio: se limitan a contactar con otros servidores para resolver las peticiones de los clientes DNS. Estos servidores mantienen una <i>memoria caché</i> con las últimas preguntas contestadas. Cada vez que un cliente DNS le formula una pregunta, primero consulta en su memoria caché. Si encuentra la dirección IP solicitada, se la devuelve al cliente; si no, consulta a otros servidores, apunta la respuesta en su memoria caché y le comunica la respuesta al cliente.

El proceso de resolución de nombres de dominio

La resolución de un nombre de dominio es la traducción del nombre a su correspondiente dirección IP. En este proceso como dijimos anteriormente hay dos partes el cliente, *Resolver*, y el servidor, *el DNS*.

Un *Resolver* tiene las siguiente tareas:

- Interrogar al Servidor de nombres, DNS
- Interpretar las respuestas, que pueden ser RR o errores
- Y devolver información al programa que ha solicitado la resolución

Para este proceso de traducción los *Resolvers* pueden formular dos tipos de preguntas: recursivas e iterativas:

- Cuando un cliente formula una pregunta *recursiva* a un servidor DNS, éste debe intentar por todos los medios resolverla aunque para ello tenga que preguntar a otros servidores
- Si el cliente formula una pregunta *iterativa* a un servidor DNS, este servidor devolverá o bien la dirección IP si la conoce o si no, la dirección de otro servidor que sea capaz de resolver el nombre

Veamos un ejemplo: queremos visualizar en el browser la página web de la dirección www.uv.es. En primer lugar, el navegador tiene que resolver el nombre de dominio a una dirección IP. Después podrá comunicarse con la correspondiente dirección IP, abrir una conexión TCP con el servidor y mostrar en pantalla la página principal de la Universidad de Valencia. Los pasos que se van produciendo a lo largo del proceso de resolución los podemos resumir en los siguientes:

1. Nuestro ordenador (cliente DNS) formula una *pregunta recursiva* a nuestro servidor DNS local (generalmente el proveedor de Internet).
2. El servidor local es el responsable de resolver la pregunta, aunque para ello tenga que reenviar la pregunta a otros servidores. Si el usuario a solicitado información local, el servidor extrae la respuesta de su propia base de datos. Si la información solicitada es sobre un ordenador externo, el servidor comprueba primero su caché de consultas recientes, si la respuesta esta aquí entonces la devuelve (no es de confianza). Suponemos que no conoce la dirección IP asociada a www.uv.es; entonces formulará una *pregunta iterativa* al servidor del dominio raíz.
3. El servidor del dominio raíz no conoce la dirección IP solicitada, pero devuelve la dirección del servidor del dominio *es*.
4. El servidor local reenvía la pregunta iterativa al servidor del dominio *es*.
5. El servidor del dominio *es* tampoco conoce la dirección IP preguntada, aunque sí conoce la dirección del servidor del dominio *uv.es*, por lo que devuelve esta dirección.
6. El servidor local vuelve a reenviar la pregunta iterativa al servidor del dominio *uv.es*.

7. El servidor del dominio *uv.es* conoce la dirección IP de www.uv.es y devuelve esta dirección al servidor local.
8. El servidor local por fin ha encontrado la respuesta y se la reenvía a nuestro ordenador. Al mismo tiempo la respuesta es almacenada en la caché para futuras referencias. El tiempo máximo que permanece la información almacenada en la caché se configura en los servidores de confianza.

Preguntas inversas

Los clientes DNS también pueden formular *preguntas inversas*, es decir, conocer el nombre de dominio dada una dirección IP. Para evitar una búsqueda exhaustiva por todo el espacio de nombres de dominio, se ha creado un dominio especial llamado *in-addr.arpa*. Cuando un cliente DNS desea conocer el nombre de dominio asociado a la dirección IP *w.x.y.z* formula una pregunta inversa a *z.y.x.w.in-addr.arpa*. La inversión de los bytes es necesaria debido a que los nombres de dominio son más genéricos por la derecha, al contrario que ocurre con las direcciones. Véase la figura siguiente:

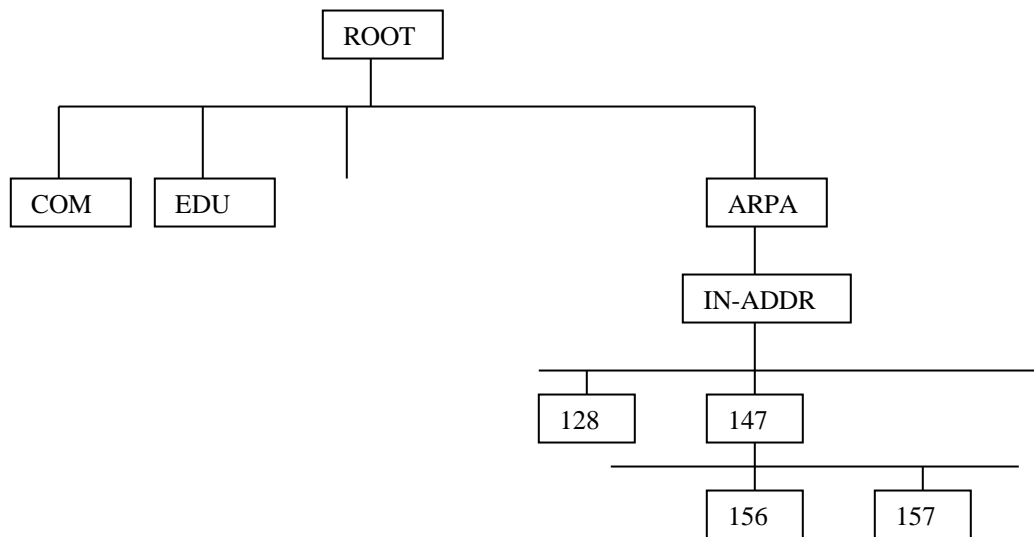


Fig.4 . Árbol para la resolución Inversa

La organización que posee una dirección de red es responsable de registrar todas sus traducciones de dirección a nombre en la base de datos del DNS. Esto se hace en una tabla que es independiente de las correspondencias entre nombre y direcciones. Como puede verse en el árbol de la fig. 4, el subárbol especial de dominio *in-addr.arpa* se creó para apuntar hacia todas esas tablas de red. Cuando se colocan las direcciones en el árbol, tiene sentido poner el primer número en la parte superior y bajar poco a poco.

Formato de los mensajes del servidor de dominios

Los mensajes de consulta entre clientes y servidores de DNS tienen un formato establecido. Este formato es el siguiente:

IDENTIFICACIÓN	PARÁMETROS
Nº DE SOLICITUDES	Nº DE RESPUESTAS
Nº DE AUTORIDAD	Nº DE REGISTROS ADICIONALES
Consulta/s (sección de solicitudes)	
RR de respuestas (sección de respuestas)	
RR de autoridad (sección de respuestas)	
RR con información adicional (sección de respuestas)	

TABLA 1: Formato de un mensaje de servidor DNS.

El cliente envía una solicitud en forma de mensaje formateado y el servidor añade la información requerida a la consulta original. El formato de mensaje visto permite al cliente hacer varias solicitudes en un solo mensaje.

A continuación vamos a describir los campos del mensaje:

- *IDENTIFICACIÓN*: este campo es para hacer corresponder una respuesta con su petición
- *PARÁMETROS*, especifica la operación solicitada y el tipo de respuesta, véase la siguiente tabla:

Bit del Campo	Significado
0	Operación: 0 → Solicitud 1 → Respuesta
1-4	Tipo de Solicitud: 0 → Estándar 1 → Inversa 2 → Terminado 1 3 → Terminado 2
5	Activado si se tiene una respuesta autorizada
6	Activado si el manejo esta truncado
7	Activado si se desea recursión
8	Activado si la recursión está disponible
9-11	Reservado
12-15	Tipo de Respuesta: 0 → Sin Error 1 → Error de formato en la solicitud 2 → Falla en el servidor 3 → El nombre no existe

- *NÚMERO DE SOLICITUDES*, proporcionado en una consulta y en una respuesta.
- *NÚMERO DE RESPUESTAS*, este campo es rellenado por el servidor.
- *NÚMERO DE REGISTROS DE AUTORIDAD*, proporcionado en una respuesta. La información de los registros de autoridad incluye los nombres de los servidores que contienen los datos de confianza.

- *NÚMERO DE REGISTROS ADICIONALES*, relleno en la respuesta. La información incluye las direcciones de los servidores de confianza.
- *CONSULTA/S*, normalmente un mensaje contiene una única consulta, pero como hemos dicho anteriormente se permite concatenar varias peticiones en la sección de consulta. Esta sección contiene los campos siguientes:

Campo	Descripción
Nombre	Nombre de dominio o dirección IP (en el subárbol IN-ADDR.ARPA)
Tipo	Tipo de consulta, A, NS,...
Clase	IN para Internet, se representa como 1

- Las tres secciones siguientes de respuestas, se estructuran todas ellas de la misma forma:

Campo	Descripción
Nombre	Nombre del nodo para este registro
Tipo	Tipo de registro, SOA, A,..
Clase	IN
TTL	Tiempo de vida
RDLENGTH	Tamaño del campo de datos
RDATA	Información del tipo de registro

En la sección *RR de autoridad* se identifica a los servidores de nombres de confianza para el dominio.

Y en la sección *RR de información adicional* se proporciona información adicional como pueden ser las direcciones IP de los servidores de nombres de confianza.

Bibliografía:

Libros de Texto

- Tanenbaum, Andrew S.: *Redes de Computadoras, 3ª Ed.* Prentice-Hall, 1997.
- Comer, Douglas E.: *Redes Globales de información con Internet y TCP/IP. Vol. 1, 3ª Ed.* Prentice-Hall

RFC's principales

- RFC 920: Domain Requierments
- RFC 1101: DNS Encoding of Network Names and Other Types
- RFC 1033 : Domain Administrators Operations Guide
- RFC 1034: Domain Names – Concepts and Facilities
- RFC 1035: Domain Names – Implementation and Specification
- RFC 1591: Domain Name System Structure and Delegation
- RFC 1183: New RR Types

Links de interés

- <http://www.dns.net/dnsrd/>
- <http://ww.itu.int/>
- <http://www.arrakis.es/~pjleon/rfc-es/> [Algunos RFC's en castellano]
- <http://www.cis.ohio-state.edu/hypertext/information/rfc.html> [Especificaciones y estándares de Internet]
- <http://www.crynwr.com>
- <http://www.cis.ohio-state.edu/hypertext/information/rfc.html> [Especificaciones y estándares de Internet]
- <http://dmoz.org/World/Español/Computadoras/Internet/Protocolos/> [Selección de páginas web en castellano que tratan sobre los protocolos de Internet]
- <http://www.linux.org> [DNS how-to]