DESPLIEGUE DE APLICACIONES WEB UD-4

SERVICIOS DE RED IMPLICADOS EN EL DESPLIEGUE DE UNA APLICACIÓN WEB (DNS)

ÍNDICE

[INTRODUCCIÓN 4](#_Toc158038555)

[SISTEMAS DE NOMBRES PLANOS Y JERÁRQUICOS 4](#_Toc158038556)

[A. ELEMENTOS DEL SISTEMA DE NOMBRES DE DOMINIO 5](#_Toc158038557)

[1) Nombres de dominio 5](#_Toc158038558)

[2) Dominios raíz 5](#_Toc158038559)

[3) Dominios y subdominios 6](#_Toc158038560)

[4) ¿Quién gestiona los dominios en España? 7](#_Toc158038561)

[5) ¿Cómo saber quién o qué ha registrado un nombre de dominio? 7](#_Toc158038562)

[6) Operaciones que podemos realizar con un dominio 8](#_Toc158038563)

[B. ZONAS 8](#_Toc158038564)

[1) Servidores DNS autorizados y no-autorizados 9](#_Toc158038565)

[C. TIPOS DE FICHEROS RR 10](#_Toc158038566)

[1) Conceptos previos 10](#_Toc158038567)

[a. $TTL (*Time To Live*) 11](#_Toc158038568)

[b. $ORIGIN 11](#_Toc158038569)

[c. Formato general de los RR 11](#_Toc158038570)

[2) Tipos de registros 11](#_Toc158038571)

[a. Registro A (*Address*) 11](#_Toc158038572)

[b. Registro AAAA 11](#_Toc158038573)

[c. Registro CNAME (*Canonical Name*) 12](#_Toc158038574)

[d. Registro NS (*Name Server*) 12](#_Toc158038575)

[e. Registro MX (Mail Exchange) 12](#_Toc158038576)

[f. Registro SOA (*Start Of Authority*) 13](#_Toc158038577)

[g. Registro PTR (*Pointer Record*) 13](#_Toc158038578)

[h. Registro HINFO 14](#_Toc158038579)

[i. Registro TXT (*Plain Text*) 14](#_Toc158038580)

[HERRAMIENTAS O CLIENTES DNS 14](#_Toc158038581)

[A. nslookup 14](#_Toc158038582)

[B. dig 16](#_Toc158038583)

[C. host 21](#_Toc158038584)

[D. WHOIS 21](#_Toc158038585)

[RESOLUCIÓN INVERSA 21](#_Toc158038586)

[A. MAPEO DE DIRECCIONES Y EL DOMINIO ARPA 21](#_Toc158038587)

[B. ZONAS DE RESOLUCIÓN INVERSA 22](#_Toc158038588)

[C. PROCESO DE RESOLUCIÓN 22](#_Toc158038589)

[TIPOS DE CONSULTAS: RECURSIVAS E ITERATIVAS 23](#_Toc158038590)

[A. CONSULTAS ITERATIVAS 23](#_Toc158038591)

[B. CONSULTAS RECURSIVAS 24](#_Toc158038592)

[TIPOS DE SERVIDORES DNS 25](#_Toc158038593)

[A. SERVIDOR MAESTRO O PRIMARIO 25](#_Toc158038594)

[B. SERVIDOR ESCLAVO O SECUNDARIO 25](#_Toc158038595)

[C. SERVIDOR CACHÉ 26](#_Toc158038596)

[D. SERVIDOR *FORWARDER* (REENVIADOR) 27](#_Toc158038597)

[E. SERVIDOR SÓLO AUTORIZADO 28](#_Toc158038598)

[F. SERVIDORES RAÍZ 28](#_Toc158038599)

# INTRODUCCIÓN

El sistema de **nombres de dominio o DNS (*Domain Name System*)** proporciona un mecanismo eficaz para llevar a cabo la resolución de nombres de dominio a direcciones IP. De manera general se utiliza el puerto 53 para este servicio.

De esta manera podemos escribir directamente en nuestra barra de navegación del cliente la dirección web <https://www.youtube.com/> y dirigirnos a su web directamente sin necesidad de escribir la dirección IP en su lugar (en este caso 142.250.200.142).

Así mismo este servicio DNS permite la **resolución inversa**, es decir, que a partir de una dirección IP podemos obtener el nombre de dominio asociado.

Este servicio permite independencia de la IP sobre el nombre de dominio, lo cual se puede traducir en que por ejemplo podamos cambiar la IP asociada a nuestro dominio de forma **transparente** para el usuario. Mientras que el usuario seguirá accediendo a [www.miweb.es](http://www.miweb.es), un día lo podría estar haciendo a la IP 162.143.10.10 y al día siguiente tras un cambio de IP lo estuviera haciendo a la 173.120.43.21 sin que él haya tenido que ser consciente de este cambio.

Además, es usual que un mismo dominio se identifique con más de una IP como medida de redundancia contra una hipotética caída del sistema o como un sistema de balanceo de cargas. Otros servicios proporcionados por el DNS son la identificación de los servidores de correo de un dominio, de cada uno de los hosts que pertenecen a la red, servidores de impresión, etc.

# SISTEMAS DE NOMBRES PLANOS Y JERÁRQUICOS

Durante la existencia de ARPANET, los nombres de los equipos se centralizaban en un archivo llamado host.txt (el actual /etc/hosts de Linux) que incluía el nombre del equipo y su IP. Esto es lo que se conoce como un **sistema de nombres plano** y puede ser adecuado para redes pequeñas, pero no es escalable para redes grandes y mucho menos en Internet.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

## ELEMENTOS DEL SISTEMA DE NOMBRES DE DOMINIO

El **espacio de nombres de dominio** **(*Domain Name Space)*** está formado por los nombres válidos utilizados para identificar servicios o máquinas en una red.

Estos nombres se pueden representar mediante un esquema en árbol invertido donde cada nodo se separa de los otros por un punto (.).

Diagrama

Descripción generada automáticamente

1. 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, de forma que [www.miweb.es](http://www.miweb.es) y [WwW.MIWeb.es](http://WwW.MIWeb.es) son exactamente lo mismo.

Estos nombres de dominio además se leen de derecha a izquierda y se expresan como secuencias de **etiquetas o labels**.

Imagen que contiene Forma

Descripción generada automáticamente

1. Dominios raíz

Todos los dominios deben terminar con un punto (.), o al menos así dice la teoría, en la práctica nunca escribimos por ejemplo [www.google.com](http://www.google.com)..

Esto es así porque el **árbol de nombres de dominio** empieza con un dominio que se escribe con un punto y es conocido como **dominio raíz o *root domain***. En realidad, es un elemento nulo de 0 caracteres que se representa con un punto.

Debido a que los dominios se leen de derecha a izquierda, el punto es el inicio de todo dominio, pero generalmente se omite ya que los programas lo añaden por defecto, aun así, en ocasiones será necesario que indiquemos el nombre de dominio completo incluyendo el dominio raíz. Estos nombres completos como por ejemplo aulavirtual33.educa.madrid.org. es lo que se conoce como **nombres de dominio completos o FQDN (*Fully Qualified Domain Names*)**.

1. Dominios y subdominios

Debido a la organización jerárquica del espacio de nombres de dominio, nos surgen los nombres de dominio y subdominio. Por ejemplo youtube.es. es un subdominio del dominio es. y, [www.youtube.es](http://www.youtube.es) es un subdominio del dominio youtube.es.

Los dominios o subdominios que cuelgan directamente del dominio raíz se conocen como **dominios de primer nivel o dominios de nivel superior o TLD (*Top Level Domains*)**, aunque (junto con el punto) también reciben el nombre de ***root zone*** y son gestionados por el organismo IANA (*Internet Assigned Numbers Authority*) que es la entidad que supervisa, entre otras cosas, esos servidores raíz de nombres de dominio DNS. Estos TLD son por ejemplo: .es, .com, .edu, .dev… Y se pueden consultar en la web de [IANA](https://www.iana.org/domains/root/db).

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza baja

A partir de los TLD cuelga un segundo nivel de dominios o dominios de segundo nivel, de estos cuelgan los dominios de tercer nivel, de estos los de cuarto nivel, etc.

1. ¿Quién gestiona los dominios en España?

En España el agente encargado de los dominios es [dominios.es](https://www.dominios.es/es), en esta web podremos por ejemplo comprobar la disponibilidad de un dominio y, de esa manera poder reservarlo.

Interfaz de usuario gráfica, Texto, Sitio web

Descripción generada automáticamente

En base al dominio que le mandemos comprobar nos informará de cuales están disponibles y cuales no lo están:

Interfaz de usuario gráfica

Descripción generada automáticamente

En el caso de que lo estén podremos registrarlo bien utilizando un agente registrador (por ejemplo, IONOS) o la propia web de dominio.es.

Esta web es responsabilidad del organismo estatal [Red.es](http://www.red.es/).

1. ¿Cómo saber quién o qué ha registrado un nombre de dominio?

Para conocer qué persona o empresa ha registrado un nombre de dominio podemos utilizar la herramienta o servicio WHOIS del ICANN.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

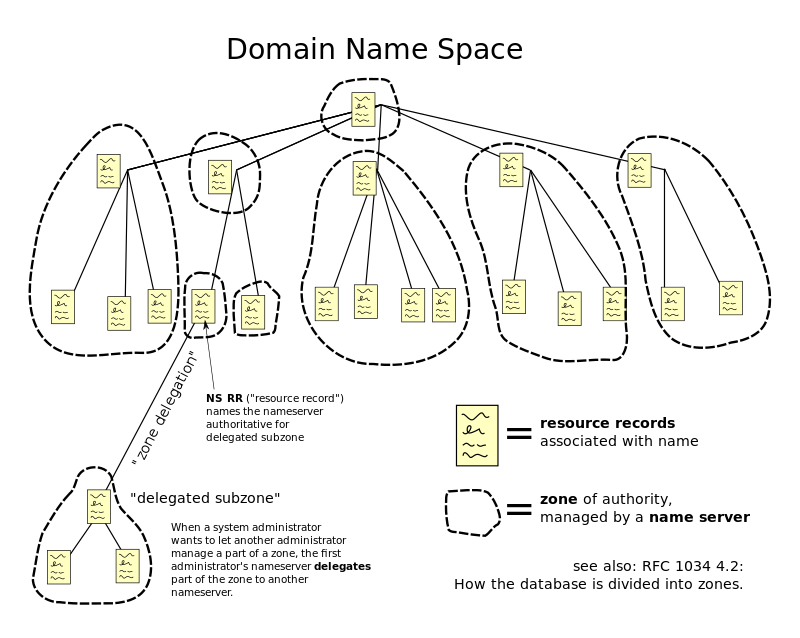
Descripción generada automáticamente

1. Operaciones que podemos realizar con un dominio

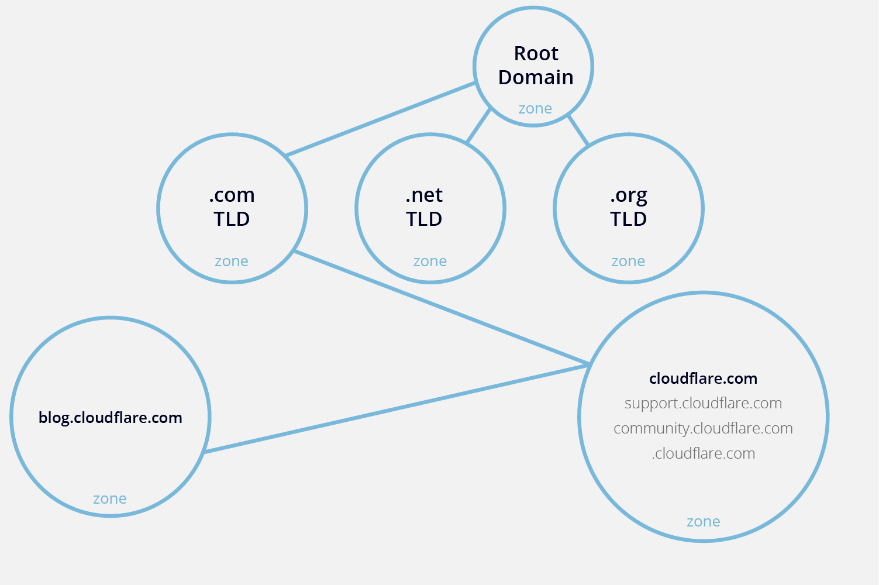
Con un dominio podemos hacer diferentes tipos de operaciones como comprarlo, renovarlo, cancelarlo o darlo de baja.

## ZONAS

Una zona es una porción del espacio de nombres de dominio en el DNS cuya responsabilidad administrativa recae sobre un único responsable.



Es decir, **una zona no es lo mismo que un dominio**. Un dominio es un subárbol del espacio de nombres de dominio y los datos asociados a los nombres de un dominio pueden estar almacenados en una o varias **zonas** que, a su vez, pueden estar **distribuidas en uno o varios servidores DNS.** Por tanto, **una zona es una porción de un dominio.**



De forma que en cada zona se tiene acceso a una porción de la información, pero no a toda, no hay ningún espacio de dominios que guarde absolutamente toda la información de los dominios de Internet.

Esta información se puede encontrar tanto en **archivos de texto** como en **bases de datos**.

Por ejemplo, vamos a analizar el siguiente archivo de zona:

Texto

Descripción generada automáticamente

Cada una de las líneas recibe el nombre de **registros de recurso o RR (*Resource Records*)** y definen el tipo de datos en el DNS. Su función es almacenar datos sobre nombre de dominio y direcciones de IP, de forma que cada uno de los elementos de la primera columna está asociado con la tercera columna. Esta asociación puede ser o bien directa asociando nombre e IP o bien indirecta asociando un nombre con un alias que tiene una asociación directa con IP.

Existen diferentes tipos de archivos de registro: A, AAAA, PTR… cada uno con una función concreta.

Un ejemplo de archivo de zona es el siguiente:

Texto

Descripción generada automáticamente

1. Servidores DNS autorizados y no-autorizados

Cuando un servidor DNS es autorizado para una zona, es el responsable de los nombres de dominio para esa zona. Por ejemplo, en nuestro archivo de zona ns1.deaw.es. es el servidor autorizado para la zona deaw.es y en él se definen los nombres que cuelgan de deaw.es como por ejemplo [ftp.deaw.es](ftp://ftp.deaw.es) o natos.deaw.es.

La organización que administra el servidor DNS y por lo tanto la zona, puede delegar o no alguno de sus subdominios. Por ejemplo, supongamos que de deaw.es cuelgan los subdominios teoria.deaw.es y practicas.deaw.es y se decide delegar sólo el subdominio practicas.deaw.es. Esto implicaría que existirá otro servidor DNS autorizado para el dominio practicas.deaw.es que almacenará el fichero de zona para dicho dominio.

En otros casos los servidores DNS no tendrán toda la información del archivo de zona para un dominio específico. En su lugar, mantienen un archivo de caché que contiene los resultados de todas las consultas realizadas en el pasado para las cuales han obtenido respuestas autorizadas. Cuando se realiza una consulta DNS, el servidor busca en el archivo de caché y devuelve la información disponible, estos son los servidores DNS no-autorizados.

Por último, hay que destacar que un servidor DNS puede ser autorizado sobre varias zonas, por ejemplo, el mismo servidor DNS puede ser autorizado para la zona deaw.es. y para la zona seguridadinformatica.es..

Un dibujo de una persona

Descripción generada automáticamente con confianza baja

Es decir, los servidores autoritativos o autorizados son los que tienen acceso a los ficheros de zona, los contienen en su interior mientras que los servidores no-autoritativos o no-autorizados no tienen acceso a estos ficheros.

## TIPOS DE FICHEROS RR

1. Conceptos previos

Antes de ver los ficheros RR con detenimiento vamos a tener en cuenta una serie de conceptos importantes.

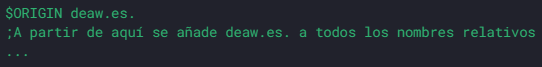
1. $TTL (*Time To Live*)

El TTL o tiempo de vida determina, en segundos, durante cuánto tiempo son válidos los RR. Pueden indicarse en semanas ($TTL 1W), días ($TTL 7D), horas ($TTL 168H) o minutos ($TTL 10080M).

Por tanto, el TTL indica cuánto tardaran en aplicarse los cambios que le hagamos a un RR desde que los hacemos. Debe declararse al inicio del archivo de zona.

1. $ORIGIN

La directiva $ORIGIN define el nombre de dominio que será añadido al final de cualquier nombre que no cabe en punto (nombres relativos o no cualificados) en los RR para así transformarlos en FQDN. Si un nombre acaba en punto, se considera un nombre FQDN y no se utilizaría $ORIGIN.



1. Formato general de los RR

El formato con el que introducen los RR en los archivos de zona es el siguiente:



Por ejemplo:



1. Tipos de registros
2. Registro A (*Address*)

Son los registros principales del DNS y su función es enlazar un dominio o un subdominio con una dirección IPv4. Mediante el uso de este tipo de registro podemos tener servicios distintos en varias máquinas.

Un reloj digital

Descripción generada automáticamente con confianza media

1. Registro AAAA

Su función es enlazar un dominio o un subdominio con una dirección IPv6.

1. Registro CNAME (*Canonical Name*)

Su funcionalidad es la de crear alias del dominio de un host. Es particularmente útil para suministrar nombres alternativos relacionados con diferentes servicios en el mismo equipo, si estos corren bajo una misma dirección IP.

Por tanto, van a asociar un dominio a otro ya existente creando un alias, de esta forma el nuevo dominio tendrá la IP asociada al dominio previamente existente.

Imagen de la pantalla de un video juego

Descripción generada automáticamente con confianza media

Hay que tener en cuenta que un CNAME también puede apuntar a un nombre de otro dominio.

Texto

Descripción generada automáticamente con confianza media

1. Registro NS (*Name Server*)

Asocia un nombre de dominio con las direcciones de los servidores de dominio que almacenan sus registros. Determinan los servidores que comunicarán la información DNS de un dominio (los autorizados). Deben definirse dos registros NS para dominio.

Es decir, cuántos servidores DNS tienen ficheros de zona (son servidores autoritativos).

Texto

Descripción generada automáticamente

1. Registro MX (Mail Exchange)

Hace referencia al registro de intercambio de correo y sirven para resolver un dominio de correo (usuario@dominio), asociando un dominio con un servidor de correo electrónico. Se le puede asignar una prioridad para que cuando se intente hacer el envío se haga con el de mayor prioridad, si éste falla que lo intente con el siguiente y así sucesivamente.

Un reloj digital en la pantalla

Descripción generada automáticamente con confianza baja

1. Registro SOA (*Start Of Authority*)

Permite proporcionar información sobre el servidor de DNS primario de la zona. Contiene información de la zona, la versión de la base de datos y otros parámetros que definen cómo se comporta el servidor DNS para un dominio.

Su función es la de coordinar un DNS primario con los DNS secundarios que le van a ayudar a trabajar sobre una zona. Este fichero cada cierto tiempo se copia del DNS primario al secundario para que ambos lo tengan.

Si la información que recibe el DNS secundario es más moderna que la que tiene registrada, la actualiza. Si es más antigua, la deshecha.

Entre la información que se puede indicar está el host de origen, número de serie, tiempo de actualización, tiempo de reintento, tiempo de caducidad o el tiempo de vida.

Texto

Descripción generada automáticamente

1. Registro PTR (*Pointer Record*)

Devuelve el nombre del dominio partiendo de una dirección IP.

También se le llama registro inverso, ya que funciona al contrario que un registro tipo A.

Un reloj digital

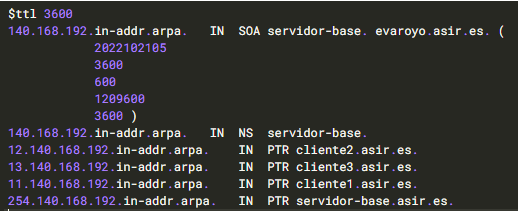
Descripción generada automáticamente con confianza baja

Aunque también se podría ver así:

Tabla

Descripción generada automáticamente con confianza baja

Este sería un ejemplo de archivo de zona inversa que está formado por varios PTR:



Estos ficheros siempre tienen una terminación in-addr.arpa. La IP del servidor se coloca al revés por ejemplo la IP 192.168.140.12 se pondría 12.140.168.192.

Los archivos de zona inversa cumplen la función contraria de los archivos de orden directa, es decir, en este caso convierten una dirección IP en una dirección de dominio.

1. Registro HINFO

Guarda información adicional del equipo, como el tipo de CPU, el sistema operativo instalado. No es conveniente utilizarlo por seguridad.

1. Registro TXT (*Plain Text*)

Almacena información de texto útil para otros cometidos no relacionados con el DNS pero que se pueden mostrar a los clientes. Las cadenas tienen un límite de 255 caracteres y se utilizan por ejemplo para almacenar claves de cifrado o, por ejemplo, para demostrar ante proveedores (Google) que se tiene acceso a la gestión de un dominio o para luchar contra el spam en correo electrónico.

Texto

Descripción generada automáticamente

# HERRAMIENTAS O CLIENTES DNS

## nslookup

Es un programa para consultar servidores DNS. Se utiliza para saber si un servidor DNS resuelve correctamente los nombres DNS y las direcciones IP, para solucionar problemas frecuentes de los servidores DNS o, para diagnosticar problemas ocasionales de configuración en los servidores DNS.

Podemos obtener la dirección IP asociada a un nombre DNS y viceversa, además podremos preguntar a los servidores de nombres información relativa a los RR de la zona de las que son autorizados.

Se usa en dos modos:

* **Interactivo:** Permite al usuario consultar los servidores DNS para obtener información sobre varios hosts y dominios o para listar los hosts de un dominio.
* **No interactivo:** Se usa para presentar sólo el nombre y la información solicitada para un host o nombre DNS.

Por ejemplo, si queremos consultar el RR de tipo A debemos utilizar el comando nslookup [dirección\_dominio] en nuestra terminal:

Texto

Descripción generada automáticamente

El server y el address son las direcciones de nuestro servidor DNS que nos está contestando, lo que nos interesa son las dos líneas de abajo, que nos dicen que el nombre de dominio educa.madrid.org responde a la IP 193.146.123.119.

Si el dominio tuviera registros de tipo AAAA veríamos lo siguiente:

Texto

Descripción generada automáticamente

Los registros A y AAAA son la opción por defecto de nslookup, si queremos consultar el resto de registros, tenemos que usar la opción -query o -type seguida del tipo de registro. Por ejemplo, para consultar los NS:

Texto

Descripción generada automáticamente

De forma que educa.madrid.org utilizan los servidores chico.rediris.es y sun.rediris.es. RedIRIS (Red de Interconexión de los Recursos InformáticoS de las universidades y centros de investigación) se encarga de proveer servicios de conexión a Internet a dichas instituciones.

Para consultar los MX de gmail.com usaríamos el siguiente comando:

Texto, Tabla

Descripción generada automáticamente

En el caso del SOA veríamos lo siguiente:

Texto

Descripción generada automáticamente

Y en el caso de los RR de tipo TXT esto:

Texto

Descripción generada automáticamente

## dig

Es un programa utilizado para preguntar a los servidores DNS.

Herramienta utilizada para solucionar problemas de DNS gracias a su flexibilidad, facilidad de uso y claridad en la presentación de la información. Normalmente, dig se usa pasándole argumentos desde la línea de comandos, pero también tiene un modo de operar por lotes, leyendo las consultas desde un archivo.

Cuando ejecutamos el comando dig sin argumentos se realiza una consulta de los NS raíz o root servers.

Tabla

Descripción generada automáticamente

Si le añadimos un dominio consultaremos la información de este:

Texto, Tabla

Descripción generada automáticamente

También contamos con la posibilidad de usar un nameserver específico, es decir, obligar que un determinado nameserver sea el que nos responda.

Texto, Tabla

Descripción generada automáticamente

También tenemos la opción ANY que nos devuelve todos los tipos de registros disponibles para el dominio especificado.

Tabla

Descripción generada automáticamente

Si por el contrario queremos consultar un registro en específico de un dominio, por ejemplo A, NS, MX, CNAME… debemos hacerlo siguiendo la estructura:

dig [REGISTRO\_A\_CONSULTAR] dominio

Tabla

Descripción generada automáticamente

Dig también nos permite hacer debug ante problemas de resolución de DNS, para ello utilizaremos el parámetro +trace, lo que nos permitirá ver la traza de saltos y saltos de la petición hasta llegar al servidor autoritativo que ofrece la respuesta del registro:

Tabla

Descripción generada automáticamente

Este parámetro es similar a traceroute:

Texto

Descripción generada automáticamente

También podemos hacer una resolución inversa, es decir, a partir de una IP conseguir el nombre de dominio asignado usando el parámetro -x:

Tabla

Descripción generada automáticamente

La forma de leer cada uno de estos registros es la siguiente:

Texto, Tabla

Descripción generada automáticamente

Servidor que responde.

Tiempo que tarda la respuesta.

Indica si el servidor que responde es autoritativo (1) o no lo es (0).

Respuesta obtenida.

Registro por el que se pregunta.

## host

Host es una herramienta CLI sencilla y fácil de usar para realizar consultas DNS, que traducen nombres de dominio a direcciones IP y viceversa. También se utiliza para consultar los registros DNS de las zonas que almacenan los servidores DNS, probar y validar el servidor DNS y la conectividad a Internet, registros de correo no deseado y listas negras, diagnóstico de problemas en el servidor DNS...

## WHOIS

Aunque no es una herramienta de diagnóstico DNS sí que nos ofrece información sobre el registro del dominio.

Whois es un protocolo que permite realizar consultas a bases de datos que contienen información; del usuario, empresa u organización que registra un nombre de dominio y/o una dirección IP en Internet. El protocolo whois se encapsula en TCP y solo especifica el intercambio de peticiones y respuestas, no el formato de datos a intercambiar. Por eso, los resultados de las consultas whois pueden variar dependiendo de la base de datos whois a la que se pregunte.

# 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 explicado en apartados anteriores.

## MAPEO DE DIRECCIONES Y EL DOMINIO ARPA

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.

Gráfico, Diagrama, Gráfico radial

Descripción generada automáticamente

Cuando usamos una dirección IP, por ejemplo 192.168.1.21, para realizar una pregunta DNS inversa, en realidad estamos preguntando por el nombre de dominio 21.1.168.192.in-addr.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 192.168.1.21 es mapeada al nombre 21.1.168.192.in-addr.arpa.

## ZONAS DE RESOLUCIÓN INVERSA

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.

Texto

Descripción generada automáticamente

## PROCESO DE RESOLUCIÓN

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...

Por ejemplo, si un cliente DNS realiza una consulta recursiva de la IP 192.168.1.21 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.

# TIPOS DE CONSULTAS: RECURSIVAS E ITERATIVAS

## CONSULTAS ITERATIVAS

Son aquellas en las que el servidor DNS proporciona una respuesta parcial.

Por ejemplo:

1. El cliente DNS realiza una solicitud de resolución del nombre de dominio aulavirtual33.educa.madrid.org.
2. El servidor DNS solicita al servidor autoritativo para org. (IP: 123.123.123.123) la IP del DNS que se encarga de madrid.org. (IP 15.15.15.15).
3. El servidor DNS solicita ahora al servidor autoritativo para madrid.org.. (IP l5.15.15.15) la IP del servidor DNS de educa.madrid.org. (IP 90.90.90.90).
4. El servidor DNS solicita ahora al servidor autoritativo para educa.madrid.org.. (IP 90.90.90.90) la IP del servidor DNS de aulavirtual33.educa.madrid.org. (IP 71.71.71.71).
5. El servidor DNS resuelve la solicitud generada por el cliente DNS (IP 71.71.71.71).

Existen 4 posibles respuestas:

* Positivas: se devuelve información sobre el dominio consultado.
* Negativa: no se pude resolver el nombre de dominio.
* Referencia: el servidor DNS indica a otros servidores a los que se le puede consultar para resolver la pregunta.
* Error: debido a un fallo en la red.

Diagrama

Descripción generada automáticamente

## CONSULTAS RECURSIVAS

Son aquellas en las que el servidor DNS da una respuesta completa o exacta.

Consiste en que el servidor DNS solicita a otro servidor que consiga la resolución de IP y una vez que esto ocurre (este nuevo servidor puede resolver por iteración o delegando en un tercer DNS), el servidor DNS le da el resultado al cliente que ha realizado la solicitud.

La respuesta puede ser de 3 tipos:

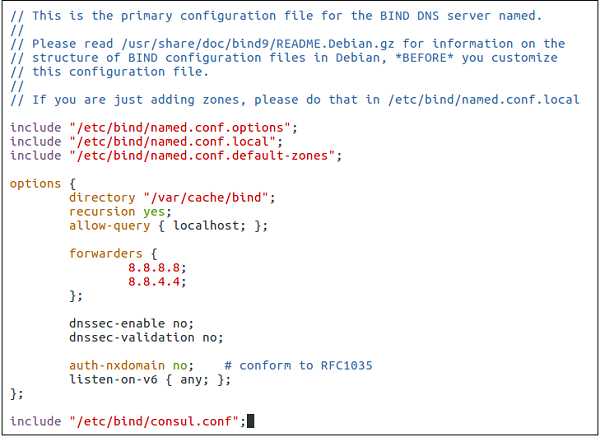
* Positiva: se devuelve información sobre el dominio consultado.
* Negativa: no se puede resolver el nombre del dominio.
* Error: debido a un fallo en la red.

Diagrama

Descripción generada automáticamente

Para que un servidor pueda ser recursivo y, de esa forma, poder preguntar a otros servidores DNS, tenemos que configurarlo, para ello dentro del bloque *options* del fichero de configuración de opciones (named.conf.options):

* El servidor debe tener un bloque *forwarders* donde tiene servidores DNS a los que preguntar si no conoce la respuesta.



Para poder ser un servidor que reciba preguntas de otros servidores, debe estar configurado para ello:

* Opción *recursion* con valor *yes*.
* Un bloque *allow-recursion* que contendrá una serie de IPs o redes a las que se le permitirá la recursión hacia este servidor.

Texto

Descripción generada automáticamente

Por último, si además se quiere que este servidor funcione como servidor caché en el archivo de configuración:

* Hay que establecer un directorio (*directory*) donde almacenar la información que le llegará de otros servidores, por ejemplo “/var/cache/bind”. Por tanto, en este directorio se guardarán las respuestas que se obtengan de los *forwarders* que hayamos establecido.

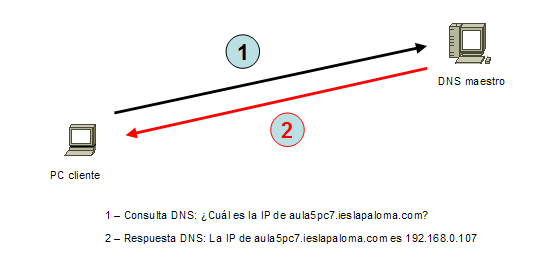


# TIPOS DE SERVIDORES DNS

## SERVIDOR MAESTRO O PRIMARIO

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.



## SERVIDOR ESCLAVO O SECUNDARIO

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 **sólo 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 para esto suelen ser:

1. Reducir y repartir la carga entre varios servidores DNS.
2. Favorecer la tolerancia a fallos.
3. 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.

Diagrama

Descripción generada automáticamente

## SERVIDOR CACHÉ

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 sólo caché (*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.

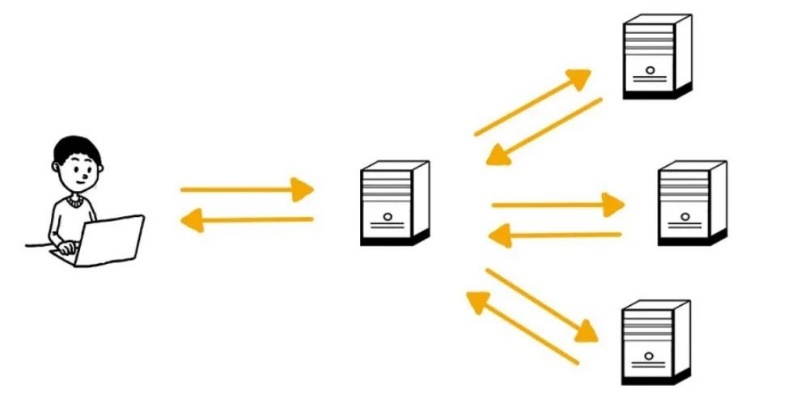
Diagrama

Descripción generada automáticamente

## SERVIDOR *FORWARDER* (REENVIADOR)

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.



## SERVIDOR SÓLO AUTORIZADO

Un servidor **sólo 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 cache.

## SERVIDORES RAÍZ

En Internet existen un conjunto de servidores DNS autorizados para el dominio raíz ., conocidos como **servidores raíz (*root servers*)**. Contienen el fichero de la zona . que contiene información sobre los servidores DNS autorizados para cada uno de los dominios TLD.

Son una **parte fundamental de Internet**, son el primer paso en la traducción (resolución) de los nombres de host en direcciones IP, que se utilizan en la comunicación entre los hosts de Internet. Son claves en el proceso de resolución de nombres de dominio en Internet, y **deben de ser conocidos por todos los servidores DNS** que respondan a preguntas sobre nombres para los que no son autorizados.

Existen 13 servidores raíz en toda Internet y cada uno de ellos tiene múltiples copias distribuidas por todo el mundo, es decir, que físicamente no solo son 13 servidores. Cada conjunto de copias de uno de los 13 servidores se identifica por una misma IP. Cuando un cliente realiza una pregunta a una IP de un servidor raíz, los routers de Internet encaminan la pregunta hacia la copia más cercana mediante un procedimiento denominado *anycasting*.

Los nombres de los servidores raíz son de la forma letra.root-servers.net, donde letra va desde la A a la M.

