IES N1 Gijón

Principado de Asturias
Consejería de Educación

UNIDAD DE TRABAJO 2

Servicios DNS

Celia C. Pellico Llera

Cofinanciado por la Unión Europea

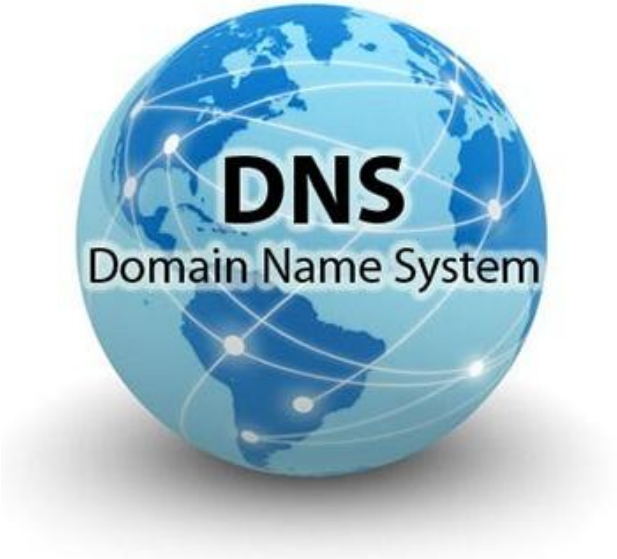
Contenidos

1. Introducción. El servicio DNS. Conceptos
2. Servidores de nombres de dominio
3. Bases de datos del protocolo DNS
4. Clientes DNS (resolvers)
5. Proceso de resolución
6. Resolución inversa
7. DNS Dinámico (DDNS)
8. Comandos
9. Servicios de DNS en la nube
10. Seguridad DNS
11. Whois

1. Introducción. El servicio DNS. Conceptos

Los equipos informáticos se comunican entre sí mediante una dirección IP como **193.147.0.29**. Sin embargo nosotros preferimos utilizar nombres como *www.educastur.es* porque son más fáciles de recordar y porque ofrecen la flexibilidad de poder cambiar la máquina en la que están alojados (cambiaría entonces la dirección IP) sin necesidad de cambiar las referencias a él.

El DNS (siglas en inglés de **Domain Name System**, Sistema de Nombres de Dominio) tiene por objeto facilitar esta tarea y permite traducir una dirección del tipo www.google.es a una dirección IP y viceversa.





DNS Explicado Fácilmente

Por lo tanto, DNS es una base de datos distribuida, con información que se usa para traducir los nombres de dominio en números de protocolo de Internet (IP).

Un poco de historia

A principios de la década de los 80, las páginas Web no existían y el número de servidores era escaso.
Entonces todos los Host tenían la lista de nombres de dominio y la actualizaban diariamente. Se trataba de un sistema de nombres planos.
En el archivo **hosts.txt** en Windows o **hosts** en Linux, se tenía una lista de nombres con su respectiva dirección IP. Todavía se pueden usar estos ficheros a nivel de una LAN.



DNS Explicado Su Historia
Que es y Como Funciona

A mediados de los años 80, a medida que el número de equipos de la red aumentaba, el tamaño del archivo host iba creciendo, lo que desencadenó una serie de problemas:

- Sobrecarga del servidor que contenía el fichero (**hosts.txt**) como consecuencia del aumento de tamaño del fichero y del número de descargas.
- Tráfico de actualización y sobrecarga de la red.
- Aumento de la probabilidad de duplicidad de nombres.
- Dificultad para administrar el fichero y gestionar las múltiples peticiones de nombres nuevos.

En 1983 se introdujo un nuevo sistema, **DNS**, que ofrece características tales como escalabilidad, administración descentralizada, velocidad,…

Características del sistema DNS

- Es un servicio de almacenamiento y consulta de información de nombres y direcciones de red.
- La información se almacena en una base de datos distribuida. Por tanto, diferentes equipos (servidores DNS) son los responsables de la gestión de dominios.
- El espacio de nombres de dominio se indexa de forma jerárquica.
- Los servidores de nombres responden a consultas según las reglas del protocolo DNS.
- Un servidor de nombres puede almacenar varios tipos de información sobre cada uno de los dominios que gestiona y puede responder a consultas de diferentes tipos.
- Los tipos de consultas más habituales que puede responder un servidor DNS son:
  - **Resolución de nombres** (búsqueda directa): obtener información asociada a un nombre de dominio.

    Por ejemplo: ¿Cuál es la dirección IPv4 asociada al nombre **www.educastur.com**?
  - **Resolución inversa** de direcciones (búsqueda inversa): obtener el nombre simbólico a partir de una dirección IP.

    Por ejemplo: ¿Cuáles son los nombres de dominio que están asociados a la dirección **88.151.18.99**?
  - **Resolución de servidores de correo**: donde dado un nombre de dominio, por ejemplo ies1.es, se puede obtener la dirección de red del servidor al cual debe realizarse la entrega de correo a direcciones de correo del dominio **@ies1.es**.

Sistema de nombres planos vs jerárquicos

Un **sistema de nombres planos** no tiene ninguna jerarquía que permita clasificar un nombre (no hay posibilidad de agrupamiento). Un sistema de nombres planos implica una gestión centralizada y única para todo el espacio de nombres.
Por ejemplo: los DNI, los nombres de ciudades, etc.

Los **sistemas de nombres jerárquicos** usan nombres agrupados y clasificados según algún criterio (distribución geográfica, funcionalidad, tamaño,…), por lo que existe una jerarquía a la hora de construir un nombre completo.

Al contrario que los sistemas de nombres planos, los sistemas de nombres jerárquicos facilitan la administración y la gestión distribuida.

Por ejemplo: una dirección postal, nombre de un archivo en el sistema de ficheros (C:\Sistemas en Red\Unidad1\ejercicio1.doc).

DNS utiliza un sistema de nombres jerárquico.

Componentes

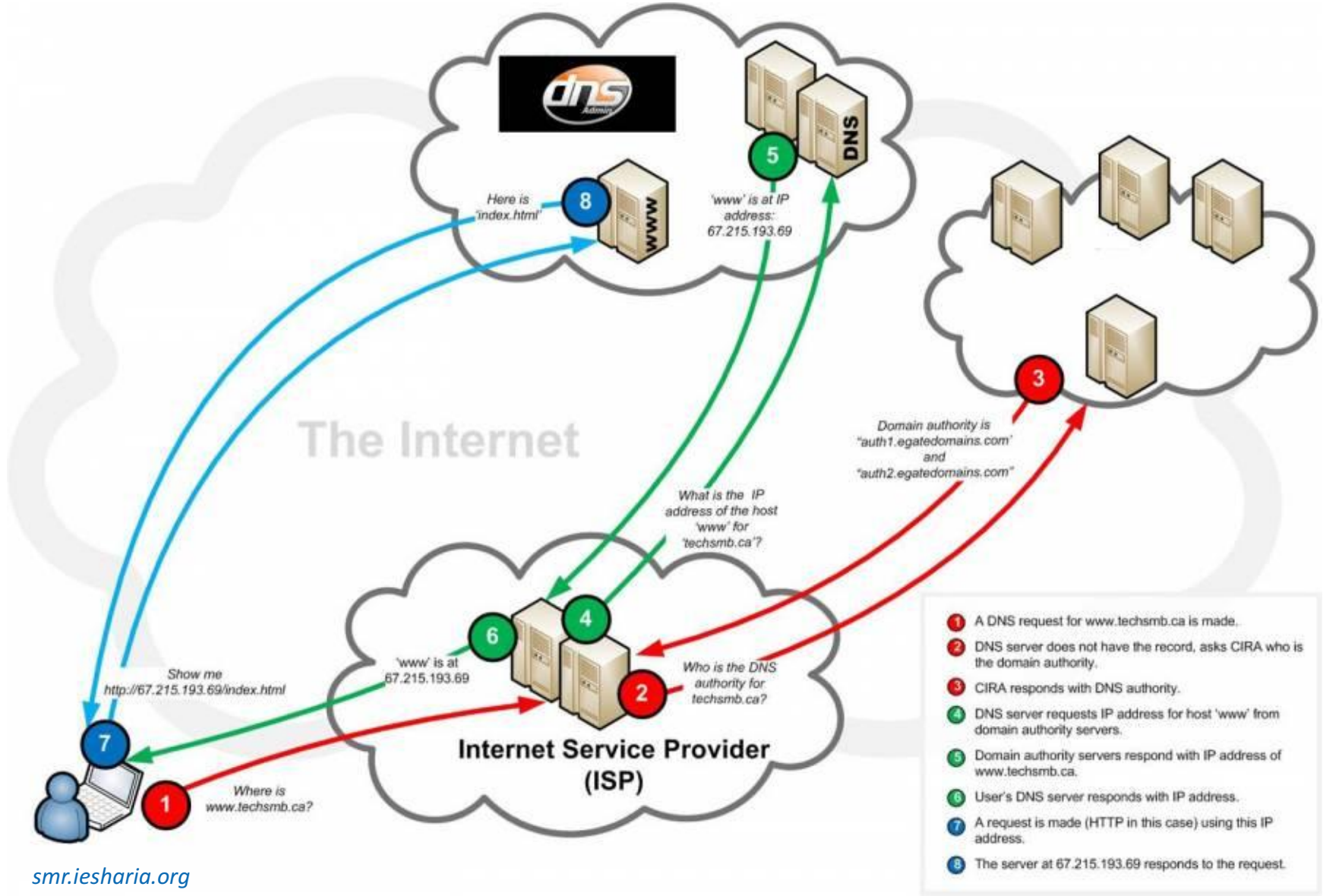
- **Espacio de nombres de dominio**. Conjunto de nombres que se pueden utilizar para identificar máquinas o servicios de una red.
- **Base de datos DNS**. Base de datos ***distribuida*** y ***redundante*** que almacena información sobre los nombres de dominio. Esta base de datos se organiza en zonas que almacenan la información en lo que se conoce como ***Registros de Recursos*** (**RR**, Resource Records).
- **Servidores de nombres** (o Servidores DNS). Programas que guardan parte de la base de datos DNS y que responden a preguntas sobre la información almacenada (como, por ejemplo, ¿cuál es la dirección de www.google.es?).
- **Clientes DNS** (***resolvers***). Programas que realizan preguntas a los servidores de nombres.
- **Protocolo DNS**. Conjunto de normas y reglas en base a las que dialogan los clientes y los servidores DNS.

Funcionamiento

El funcionamiento del servicio DNS se basa en el modelo cliente/servidor.

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

Un esquema de funcionamiento del servicio de DNS para mostrar una URL en un servidor Web podría ser el siguiente:



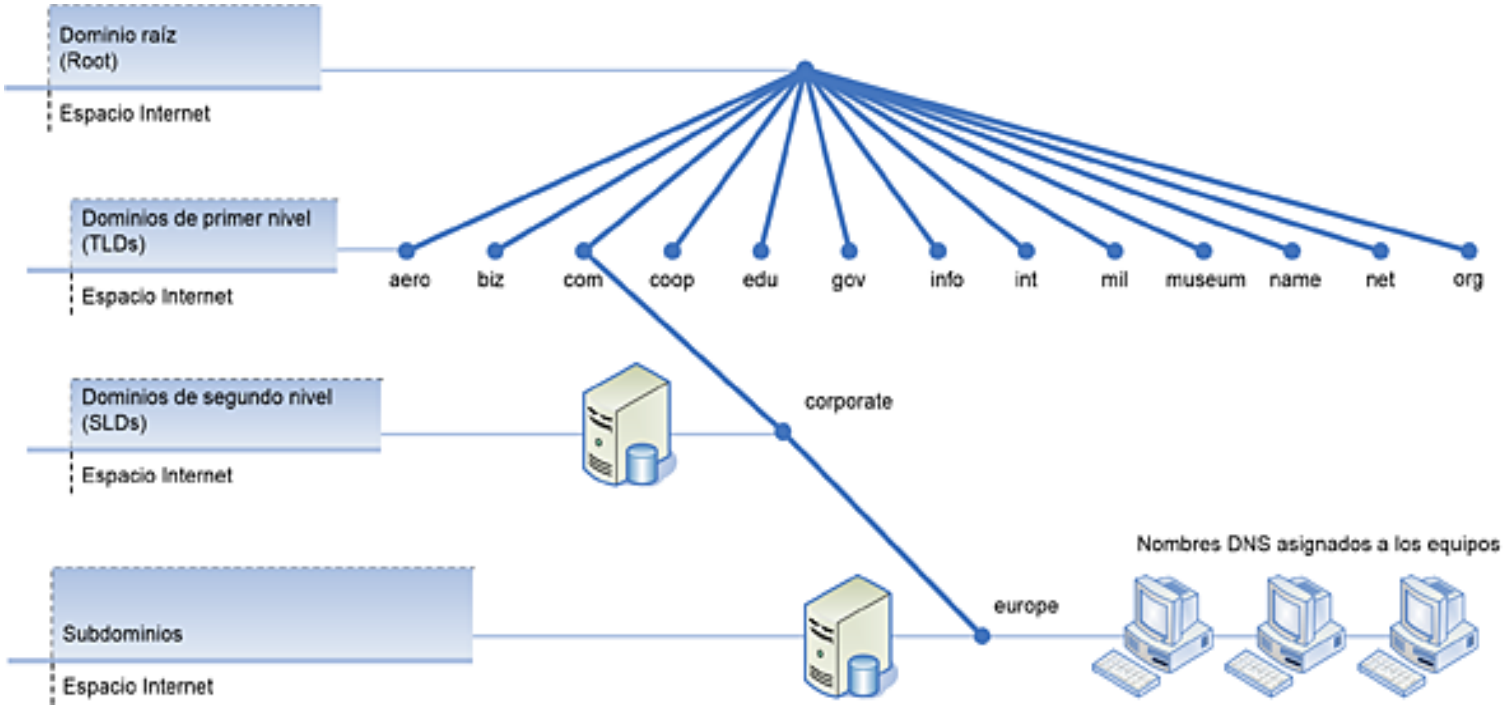
smr.iesharia.org

Espacio de nombres de dominio

El **espacio de nombres de dominio** es el conjunto de nombres que se pueden utilizar para identificar máquinas o servicios de una red. Tiene una estructura de árbol invertido. **Cada nombre de dominio está formado por una o varias cadenas de caracteres** (no distingue mayúsculas/minúsculas) **separadas por puntos**.
Cada punto añade un nivel al árbol.



Los nombres de dominio y la organización de los servidores DNS



www.ediciones-eni.com

Se pueden usar nombres que tengan como máximo **127 niveles**, y cada parte separada por puntos (es decir cada nivel, subdominio o nodo del árbol) puede tener como máximo **63 caracteres**. En total, un nombre de dominio no puede superar **255 caracteres** y puede contener letras, dígitos y, dentro de los caracteres especiales, únicamente los guiones.

El árbol de nombres de dominio empieza en el dominio "**.**" conocido como dominio raíz (**root**). Realmente es un nombre nulo con 0 caracteres, pero se representa con un punto.

- Los **nombres absolutos** están formados por todas las partes separadas por puntos, desde el nodo correspondiente hasta el nodo raíz. Se llaman nombres de dominio completos **FQDN** (**F**ully **Q**ualified **D**omain **N**ames). El punto final del dominio raíz permite distinguir si el nombre usado es FQDN o no.
- Los **nombres relativos** se refieren a un equipo por su nombre (*host* en Linux o *Nombre de equipo* en Windows), pero debemos conocer el nombre del dominio al que pertenece.

Al escribir URLs, no utilizamos el "." final de los nombres **FQDN** en los navegadores, clientes de correo, etc. pero internamente si se utiliza.

Los subdominios del dominio raíz se denominan **TLD** (***T**op **L**evel **D**omain*), "dominios de nivel superior" o "dominios de primer nivel".

Uso de dominios

Se utiliza un dominio, por ejemplo **ies1.es**, para designar un conjunto de hosts y/o subdominios agrupados según algún criterio.

Por ejemplo, en la red del instituto, podríamos poner ***pc1.a301.ies1.e***s, ***pc2.a301.ies1.es***, ***pc3.a301.ies1.es…*** para nombrar los equipos del aula **A301** del centro. Siguiendo el mismo criterio, los equipos del aula **B104** serían ***pc1.b104.ies1.es***, etc.

Además, otros servicios del instituto, no asociados a un aula concreta, podrían tener nombres como: ***www.ies1.es*** (web), ***ftp.ies1.es*** (transferencia de ficheros), **smtp.ies1.es** (correo), etc.

Por tanto, se puede agrupar los nombres en subdominios por alguna razón jerárquica, o simplemente para poner nombre a los hosts finales en el dominio de la empresa.

Un servidor DNS tiene los nombres de dominio y de servicios que están bajo su **autoridad delegada**.

Administración de nombres de dominio. Delegación

La administración y organización del espacio de nombres de dominio de Internet se distribuye entre múltiples empresas y organizaciones, estando coordinada por la **ICANN**. La ICANN es una organización sin ánimo de lucro que tiene el objetivo de garantizar que Internet sea estable, operativa y segura. Se encarga, entre otras funciones, de administrar el dominio raíz y de mantener un registro de los dominios de nivel superior (**TLD, *Top Level Domain***) existentes. Es quien "decide" que dominios de primer nivel van a existir.

InterNIC es la organización asociada a la ICANN que permite registrar dominios TLD.

ICANN (*Internet Corporation for Assigned Names and Numbers*, Corporación de Internet para la Asignación de Nombres y Números).
Es una organización sin ánimo de lucro que tiene el objetivo de garantizar que Internet sea estable, operativa y segura.

En el caso de los .es los reparte **nic.es**, que forma parte de **red.es** del Gobierno de España.

La administración de cada TLD (incluyendo la gestión y el registro de los dominios de segundo nivel dentro del TLD) es delegada en una administración particular. Estas organizaciones se denominan operadores de registro (**registry operators**) o patrocinadores (sponsors) y están acreditadas por la ICANN.

Los dominios de nivel superior, **TLD** (**T**op **L**evel **D**omain), son clasificados por la ICANN desde un punto de vista administrativo en **Genéricos**, **Geográficos**, **arpa** y **reservados**.

Genéricos (gTLD, generic TLD). Nombre significativo en función del propósito o el tipo de organización que lo utiliza.

- ***Dominios no patrocinados***. Operan según las reglas del ICANN.
  Ejemplos: .com (organizaciones comerciales), .org (organizaciones no comerciales), .net (internet y/o telecomunicaciones), .biz, .info, .name, .pro
- ***Dominios patrocinados***. Operan según las reglas de una entidad que soporta su patrocinio.
  Ejemplos: .aero, .asia, .cat, .coop, .edu, .gov, .int, .jobs, .zara, .aeg, .airbus,…

Geográficos (ccTLD, country code TLD). Nombres de dos letras en función de países o regiones. Las tareas de gestión y políticas de uso se delegan en una entidad del país o territorio (el gobierno de cada país determina la entidad en cuestión).
Ejemplos: es (España), fr (Francia), de (Alemania), co (Colombia),…

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

Reservados. Serie de nombres de dominio de primer nivel reservados para que puedan usarse en pruebas privadas. Dominios reservados son: .test, .example, .invalid, .localhost

Cuando queramos alquilar un dominio, sólo podemos hacerlo con uno de segundo nivel. Es decir, éste siempre tendrá que terminar en ***.com***, ***.es***, ***.fr***, ***.org***, etc. Para el público en general y empresas no se permite comprar un domino de primer nivel.

Delegación

La administración descentralizada de DNS se basa en la **delegación**. Es una administración *descendente*.

La organización que administra un dominio puede ceder la administración de uno, varios o todos de sus subdominios a otras organizaciones. La autoridad superior puede delegar la administración coordinando los resultados.

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

Por ejemplo:
Si alquilamos el dominio ***asir.es*** y conseguimos un registrador ICANN que nos delegue, podríamos configurar ***modulos. asir.es***, ***smtp. asir.es***, ***ftp. asir.es***, etc.

Agentes registradores de dominios

Registrar un dominio consiste en "reservar" el uso del nombre de dominio durante un tiempo determinado (habitualmente un año) para poder crear subdominios y asociar el nombre y/o los subdominios con direcciones de red u otra información.

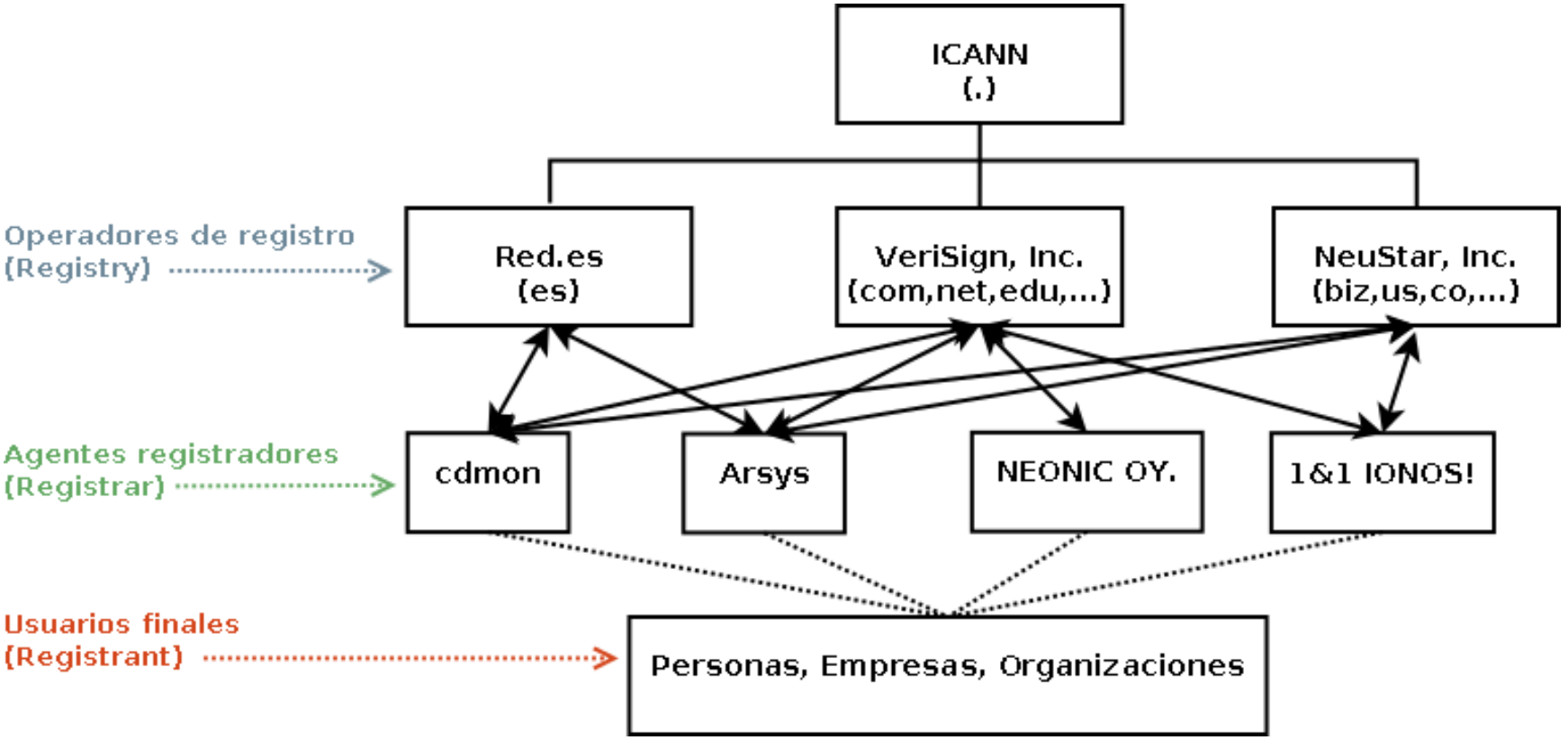
Hay diferentes normas según el TLD bajo el que se registran, o el uso que se les va a dar.

Un nombre de dominio de segundo nivel (como *educastur.es*, *pangerardo.com*, etc.) puede ser registrado mediante diferentes compañías llamadas **agentes registradores** (*registrar*), personas físicas o jurídicas, que actúan como intermediarios con los **operadores de registro** (*registry*) que también pueden ser agentes registradores directamente.

Los *agentes registradores* deben estar acreditados por los **agentes de registro** y pueden cobrar un recargo al registrador (*registrant*) sobre el precio indicado por los agentes de registro.



https://www.dominios.es/agentes-registradores/nuestros-agentes-registradores


ICANN
(.)
Operadores de registro
(Registry)
Red.es
(es)
VeriSign, Inc.
(com,net,edu,...)
NeuStar, Inc.
(biz,us,co,...)
Agentes registradores
(Registrar)
cdmon
Arsys
NEONIC OY.
1&1 IONOS!
Usuarios finales
(Registrant)
Personas, Empresas, Organizaciones

2. Servidores de nombres de dominio

También llamados **Servidores DNS**, o simplemente DNS, son programas que guardan información sobre nombres de dominio y responden a las preguntas que les realizan los clientes DNS y otros servidores de nombres. Almacenan, por lo tanto, una parte de la base de datos DNS.

Dominio DNS - Zona DNS

Un **dominio DNS** es cualquier *subárbol* de la estructura DNS. Se puede hablar del dominio raíz (que incluye todo), del dominio «.es» (que incluye todos los equipos bajo «.es»), etc.

Los **servidores** son responsables de conocer únicamente una parte pequeña del espacio de nombres de dominio, por ejemplo, un único subdominio. La parte de un dominio de la que el servidor es directamente responsable se denomina **zona**.

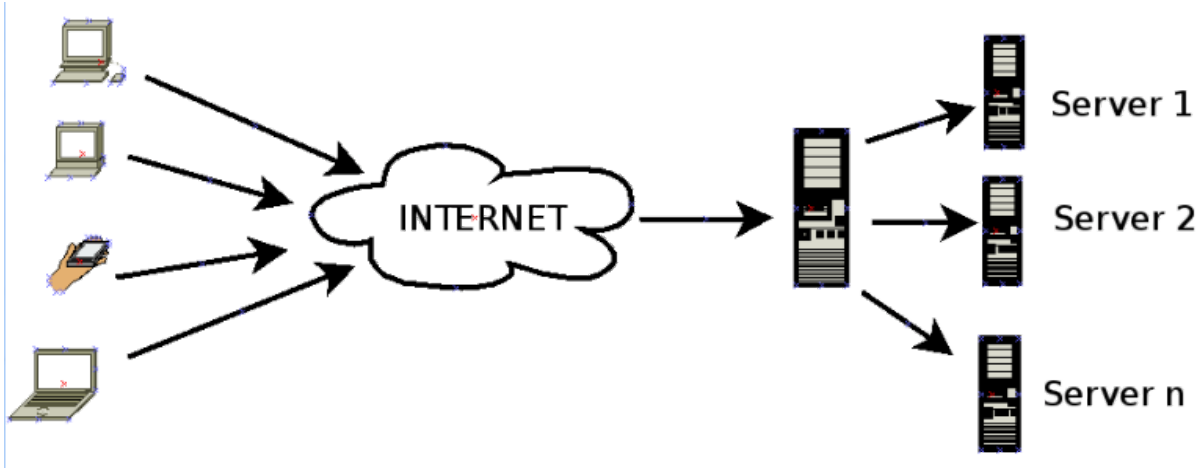
> Cada vez que se ***delega*** un dominio se está creando una nueva zona separada del dominio padre. Esto implica que se tiene que configurar un nuevo servidor DNS para el dominio delegado.

Las zonas se almacenan de diferentes formas según el software DNS que se utilice. Pueden ser ***archivos de texto plano***, ***bases de datos*** o también objetos en un directorio **LDAP** (Lightweight Directory Access Protocol) - protocolo ligero de acceso a directorios).

Los archivos de zona contienen información sobre nombres y direcciones IP de una o más partes de un dominio DNS. Un servidor que contenga toda la información sobre una zona se considera **autorizado** para esa zona y se le denomina **autoritativo**. Un servidor de nombres puede tener autoridad sobre varias zonas.

Además, el servicio DNS permite almacenar una misma zona en varios servidores DNS, ofreciendo así ***balanceo de carga***, rapidez y una mayor **tolerancia a fallos**.

El **balance o balanceo de carga** es un concepto usado en informática que se refiere a la técnica usada para compartir el trabajo a realizar entre varios procesos, ordenadores, discos u otros recursos. Está íntimamente ligado a los sistemas de multiprocesamiento, o que hacen uso de más de una unidad de procesamiento para realizar labores útiles.
El *balance de carga* se mantiene gracias a un *algoritmo* que divide de la manera más equitativa posible el trabajo, para evitar así los denominados *cuellos de botella*.



Principales tipos de servidores de nombres

Según la función que realizan, clasificamos los servidores de nombres en distintos tipos: maestro, esclavo, cache, reenviador o autoritativo.

Un servidor DNS puede asumir varias de estas funciones, es decir, un DNS puede ser maestro para una zona y esclavo para otra zona, o puede ser *forwarder* y *cache* a la vez, etc.

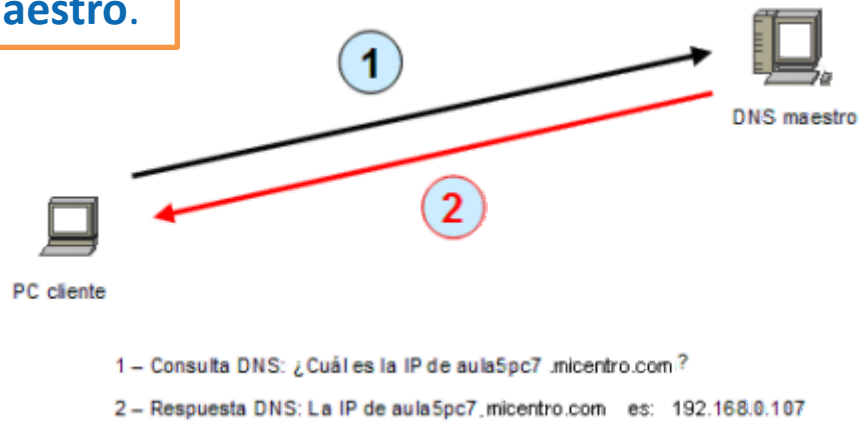
Servidor Maestro (Master) o Primario

Es un servidor autosuficiente donde el administrador del sistema podrá actualizar, modificar o añadir nombres de dominio para gestionar las zonas para las que es autoritativo.

Resuelve consultas DNS de clientes u otros servidores en base al contenido de sus archivos de zona. Si recibe consultas para zonas en las que no es autoritativo, consulta a otros servidores DNS o responde que no conoce la respuesta a la consulta.

Debemos tener al menos uno si nos han delegado una zona o dominio.

Cada zona sólo puede tener un servidor maestro.



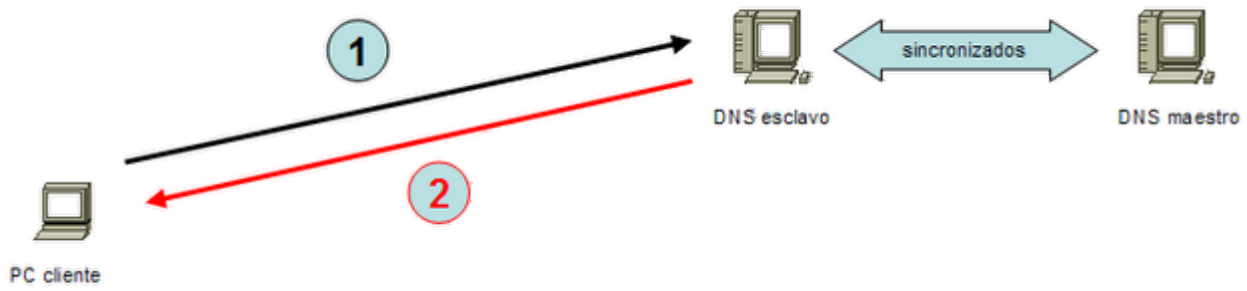
Servidor Esclavo o Secundario

Define una o varias zonas para las que es autorizado. La diferencia con un maestro es que obtiene los ficheros de zona de otro servidor autorizado para la zona (normalmente un servidor maestro) mediante un proceso que se **llama transferencia de zona**.

Los archivos de zona de un servidor esclavo son solo de lectura, por lo que el administrador no puede (ni debe) editarlos. Esa tarea se realizará en el servidor primario.

La definición de maestro o esclavo se determina a nivel de zona; así un servidor puede ser maestro para una o varias zonas y esclavo para otras.

Una zona puede tener cero o muchos servidores secundarios por razones de balanceo de carga, alta disponibilidad o mejora del rendimiento de las consultas.



Servidor Cache

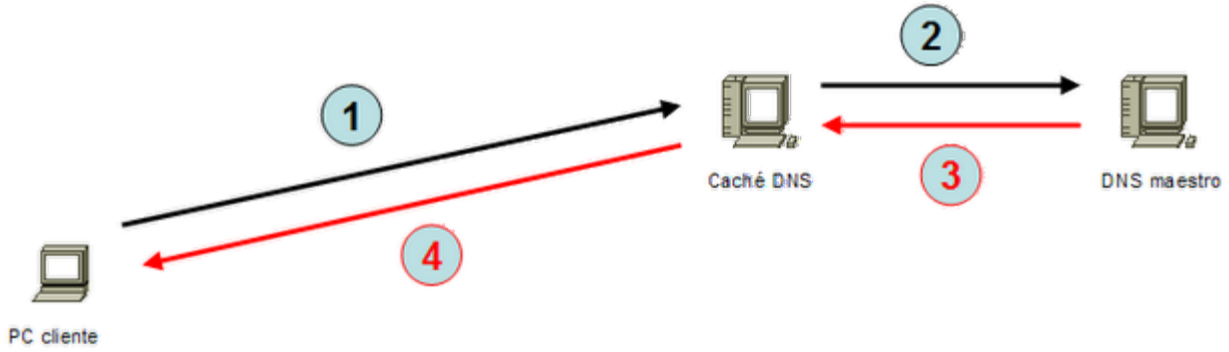
Cuando un servidor DNS recibe una pregunta sobre un nombre de dominio de una zona para la que no es autorizado, puede preguntar a otros servidores para que le den la respuesta.

Si el servidor actúa como caché **guarda durante un tiempo limitado (TTL) las respuestas a las últimas preguntas** que ha realizado a otros servidores de nombres. Se define el tiempo que se guardarán en caché las respuestas positivas (suele ser un día o más) y las respuestas negativas (dos o tres semanas).

Cada vez que un cliente u otro servidor le formula una pregunta, consulta en primer lugar en su memoria caché, mejorando así los tiempos de respuesta y disminuyendo o la carga de los equipos como el tráfico de red.

Un servidor DNS es "**sólo *cache***" (*caching only server*) cuando:

- No es autoritativo de ningún dominio.
- Guarda en la memoria *cache* las respuestas de otros servidores a las consultas realizadas para resolver desde la *cache* (si es posible) las consultas de los clientes.

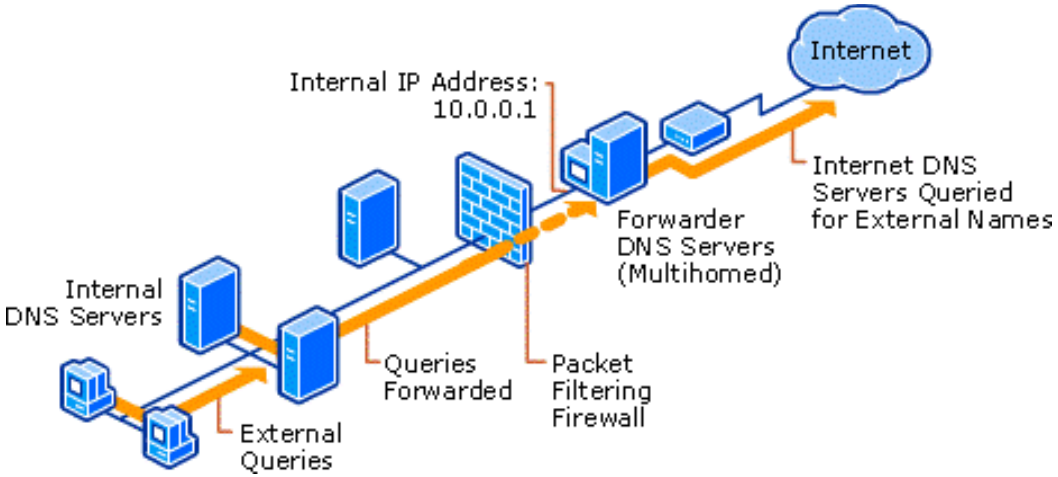


Servidor Reenviador (forwarder)

Es un servidor DNS que recibe las peticiones de todos los servidores DNS de una red. Un servidor reenviador se configura para minimizar las consultas DNS al exterior en una red corporativa en la que existen varios servidores DNS. De esta forma se minimiza el tráfico DNS en conexiones lentas, caras o congestionadas.

El DNS *forwarder* se diferencia del DNS *cache* en que no hace consultas recursivas sino que actúa como cliente de otro servidor DNS cuando la consulta que recibe no la puede resolver de forma local desde la *cache* o desde las zonas que gestiona.

La configuración de un servidor reenviador no se hace en el servidor que va a realizar esas funciones, sino en los servidores DNS que van a utilizar este tipo de servicio. Es decir, esta opción se configura en aquellos servidores DNS en los que se quiere que todas las peticiones externas, en vez de dirigirse a la raíz, se dirijan al reenviador.



Servidor DNS solo autoritativo

Un servidor DNS solo autoritario únicamente responde autoritariamente a consultas sobre zonas de las que es maestro o esclavo.

No soporta el servicio de caché ni el de consultas recursivas. Cuando le llega una consulta es porque:

- La respuesta no está en la *cache* del cliente
- El servidor DNS del proveedor no tiene la respuesta en la *cache* o ha caducado , realiza una consulta recursiva y necesita obtener una respuesta de un servidor autoritativo de la zona del nombre a buscar.

La designación de este tipo de servidores consiste en indicar ***recursion no;*** en su fichero de configuración. Con esto se desactiva la cache y las consultas recursivas.

Software DNS

- **ISC BIND9** (Mozilla Public License)
- **Servidor DNS de Microsoft** (Propietario)
- **PowerDNS** (GPL)
- **NSD** (open source)
- **SimpleDNSplus** (propietario)
- **Cisco Network Registrar** (propietario)
- **Dnsmasq** (GPL)

Servidores raíz (root servers)

Son un conjunto de servidores DNS autorizados para el dominio raíz "**.**" que apunta a los servidores de los dominios TLD autorizados (com, edu, org, net, uk, es, fr, cat, eus, tv, etc.)
Están gestionados por ICANN, aunque operados por un consorcio de organizaciones.
Son **13** y cada uno de ellos tiene múltiples copias distribuidas por todo el mundo. Cada conjunto de copias de uno de los trece servidores se identifica por una misma IP. Cuando un cliente realiza una pregunta a una de estas IP, los routers de Internet encaminan la pregunta hacia la copia más cercana.
En realidad son 13 direcciones IP gestionadas por más de un servidor que responden por *anycast*. Este conjunto de direcciones IP de los 13 servidores raíz está almacenado en un fichero que forma parte de la instalación estándar de cualquier DNS.

Estos servidores son clave para el funcionamiento del servicio DNS.



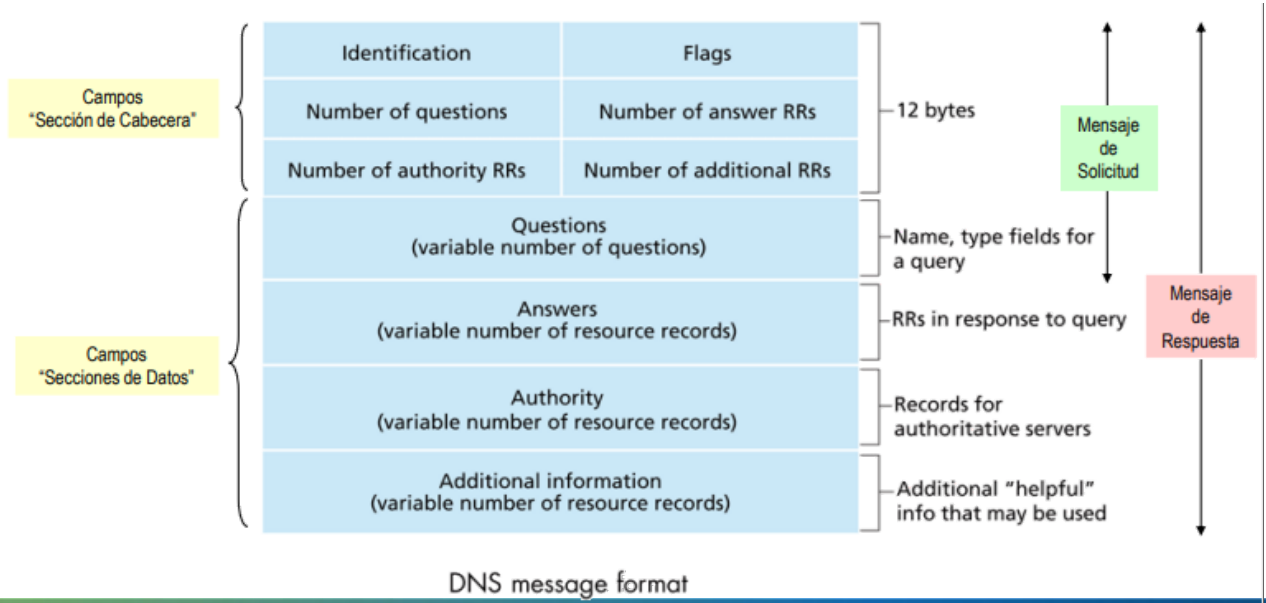
List of Root Servers

HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Protocolo DNS

Determina el conjunto de normas que regula el diálogo entre clientes y servidores DNS.

- Las **consultas** DNS usan **53/UDP** y las **transferencias** de zona usan **53/TCP** como puertos y protocolos de transporte.
- En el formato de los mensajes DNS de **solicitud** se usan los siguientes campos:
  - ***Header:*** Indica las secciones presentes y tipo de mensaje (entre otros datos).
  - ***Question:*** Campos que definen una consulta a un DNS.
- En el formato de los mensajes DNS de **respuesta** se usan los siguientes campos:
  - ***Header:*** Indica las secciones presentes y tipo de mensaje (entre otros datos).
  - ***Question:*** Campos que definen una consulta a un DNS.
  - ***Answer***: Registros de Recursos (RR) de respuesta a la consulta.
  - ***Authority*** (opcional): RR que apuntan a los servidores DNS autoritativos.
  - ***Additional*** (opcional): RR que contienen información adicional.



DNS message format

3. Bases de datos del protocolo DNS

El servicio DNS gestiona una base de datos distribuida entre múltiples servidores DNS que almacenan ficheros de zona con información sobre nombres de dominio.

Cada fichero de zona organiza esta información en Registros de Recursos (**RR**, Resource Records) que sirven para especificar la relación entre un nombre de dominio y una dirección IP.

Estructura

El formato de cada registro de recursos es el siguiente:

Propietario	***[TTL]***	***Clase***	***Tipo***	***RDATA***
www.educastur.es.	*7200*	*IN*	*A*	*192.168.85,152*

- **Propietario**: es el nombre de host o del dominio DNS al que pertenece este recurso. Puede contener:
  - Un nombre de host/dominio completamente cualificado o no.
  - El símbolo "@" que representa el nombre de la zona que se está describiendo.
  - Una cadena vacía, en cuyo caso, equivale al propietario del registro de recursos anterior.
- **TTL** (Time To Live): Tiempo de vida, indica el tiempo durante el cual esa entrada puede ser considerada válida, es decir, el tiempo que estará almacenada esta entrada en la caché. Este campo es opcional; si se omite, se toma el valor que se haya definido como global a todos los registros de una zona.
- **Clase**: define la familia de protocolos en uso. Suele ser siempre "**IN**", que representa Internet.
- **Tipo**: identifica el tipo de registro (A, AAAA, SOA, NS, CNAME, MX, PTR).
- **RDATA**: los datos del registro de recursos.

Los principales tipos de registros de recursos son:

SOA *Start Of Authority (Inicio de autoridad).*

NS *Name Server (Nombre de servidor).*

A *Address (Dirección).*

PTR *PoinTeR (Puntero).*

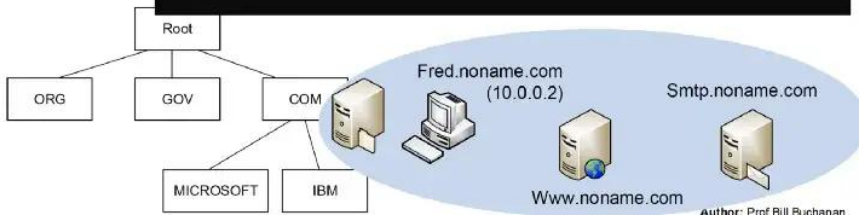
CNAME *Canonical NAME (Nombre canónico).*

MX *Mail eXchange (Intercambio de correo).*

SRV *SeRVice (Servicio).*

```
$TTL    86400 ; 24 hours could have been written as 24h or 1d
$ORIGIN noname.com.
@  IN   SOA     ns1.noname.com.      Host.noname.com (
                2002011887  ; serial
                21600       ; refresh every 6 hours
                3600        ; retry after 1 hour
                604800      ; expire after 1 week
                86400 )     ; minimum TTL of 1 day

    IN   NS  ns1.noname.com. ; Name Server
    IN   MX  10 mail.noname.com. ; mail server
    IN   A   10.0.0.1
noname.com.     IN   A   10.0.0.1
fred IN   A   10.0.0.2 ; maps a domain name to an IP address
www     IN   CNAME  noname.com. ; define a common name of a host
ftp     IN   CNAME  noname.com.
smtp    IN   CNAME  noname.com.
```



BIND (Berkeley Internet Name Domain) es el servidor de DNS más comúnmente usado en Internet, especialmente en sistemas Unix, en los cuales es un estándar de facto. Está patrocinado por Internet Systems Consortium.

En BIND el archivo de configuración se llama ***named.conf*** y los registros están en otros archivos que suelen denominarse ***db***.

Registro SOA

El registro de recursos **SOA** (Start of Authority) es el primer registro de una zona y define una serie de opciones generales de la misma. **Para cada zona debe existir uno y sólo uno registro SOA**.

Un ejemplo de registro SOA sería el siguiente *(el **;** -punto y coma- marca un comentario)*:

```
asir.local.     IN      SOA     ns1.asir.local.     admin.asir.local. (
                                1                   ; número de serie
                                604800              ; tiempo de refresco
                                86400               ; tiempo de reintento
                                2419200             ; tiempo de expiración
                                604800  )           ; TTL negativo
```

ns1.asir.local. → **Nombre** FQDN del servidor DNS maestro del dominio

admin.asir.local. →**Correo** de la persona responsable del dominio. Se reemplaza el primer punto por @

1 → Indica la **versión del archivo de zona**, y debe ser incrementado cada vez que el archivo se modifique. Es práctica común usar el formato *aaaammdd* y agregarle dos dígitos más para los cambios que se hacen en el archivo el mismo día. Los servidores secundarios consultan el registro SOA para realizar transferencias de zona. Si ha cambiado realizan la transferencia.

604800 → **Actualización/Refresco**. Tiempo en segundos que esperan los servidores esclavos para preguntar al maestro si hay cambios en la zona. Se recomiendan valores entre 1200 y 43200 (12 horas). Si se usan notificaciones se puede usar un valor muy alto.

86400 →**Reintento**. Si la transferencia de zona ha fallado, indica el tiempo que espera el servidor secundario antes de volver a intentarlo. Es un valor menor que el tiempo de actualización.

2419200 →**Caducidad/Expiración**. Tiempo que un servidor esclavo puede estar sin contactar con el primario para comprobar la zona. Si el tiempo expira, considera que algo ha pasado y se declara como no autorizado para la zona, y por lo tanto, no responde a preguntas sobre esa zona.

604800 → **TTL negativo**. Tiempo durante el que se almacenan las respuestas negativas sobre esa zona.

Registro NS

El registro de recursos **NS** (Name Server) establece el servidor o servidores autorizados en una zona.

```
asir.local.                 IN    NS    ns1.asir.local.          ;Servidor DNS maestro
asir.local.                 IN    NS    ns2.asir.local.          ;Servidor DNS esclavo.
asir.local.                 IN    NS    dns.asir.org.            ;Servidor DNS esclavo
....
ns1.asir.local.             IN    A     193.100.200.100
ns2.asir.local.             IN    A     193.100.200.200
;Delegación de subdominio
asir2srein.srein.local.     IN    NS    ns1.asir2srein.asir.local.   ;subdominio asir2srein delegado
```

- Cada zona debe contener como mínimo un registro NS.
- Los servidores DNS pueden tener un nombre de la misma zona o de otras.
- Cada zona debe contener, al menos, un registro NS por cada subdominio que haya delegado.
- La parte derecha de un registro NS **no** puede ser un nombre de tipo CNAME

Registro A

El registro de recursos **A** (Address) establece una correspondencia entre un nombre de dominio completamente cualificado (FQDN) y una dirección **IPv4**.

```
ns1.asir.local.   IN    A     193.100.200.100
ns2.asir.local.   IN    A     193.100.200.200
....
```

Registro AAAA

El registro de recursos **AAAA** (Address) establece una correspondencia entre un nombre de dominio completamente cualificado (FQDN) y una dirección **IPv6**.

```
obelix.asir.local.   IN    A      193.100.200.101
obelix.asir.local.   IN    AAAA   2001:db8::63
....
```

Registro PTR

El registro de recursos **PTR** (Pointer Record) establece una correspondencia entre nombres de direcciones IPv4 e IPv6 y nombres de dominio. Se utilizan por tanto en las zonas de resolución inversa.
En una misma zona no puede haber registros PTR IPv4 y registros PTR IPv6. Existen por lo tanto zonas de resolución inversa IPv4 y zonas IPv6.

```
100.200.100.193.in-addr.arpa.   IN   PTR   ns1.asir.local.
200.200.100.193.in-addr.arpa.   IN   PTR   ns2.asir.local.
101.200.100.193.in-addr.arpa.   IN   PTR   obelix.asir.local.
```

Registro CNAME

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

```
obelix.asir.local.   IN   A       193.100.200.101
www.asir.local.      IN   CNAME   obelix.asir.local.
bd.asir.local.       IN   CNAME   obelix.asir.local.
```

Un registro CNAME puede apuntar a un nombre de otro dominio.

```
obelix.asir.local   IN   A       193.100.200.101
.
obelix.asir.local   IN   CNAME   www.educastur.es.
.
```

No se pueden usar registros CNAME para servidores DNS (registros NS) ni para servidores de correo (registros MX).

Registro MX

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

asir.local.	IN	MX	10	mail1.asir.local.
asir.local.	IN	MX	20	mail2.asir.local.
asir.local.	IN	MX	30	smtp.informatica.es.
mail1.asir.local.	IN	A		193.100.200.221.
mail2.asir.local.	IN	A		193.100.200.222

Un registro MX puede apuntar a un nombre de otro dominio.

Es posible definir varios registros MX para un mismo dominio, es decir, varios servidores de correo para un mismo dominio. En cada registro MX se especifica un número positivo (entre 0 y 65535) que determina la preferencia en el caso de que existan varios registros MX. Tiene más preferencia el número más pequeño.

La parte derecha de un registro MX no debe ser un nombre tipo CNAME.

Registro SRV

Permiten especificar de forma genérica la ubicación de los servidores para un servicio, protocolo y dominio DNS determinados.

El formato de un registro SRV es:

servicio.protocolo.nombre	*TTL*	*clase*	*SRV*	*prioridad*	*peso*	*puerto*	*destino*
_http._tcp.asir.local.		IN	SRV	0	5	80	www.asir.local.
_ldap._tcp.asir.local.		IN	SRV	0	0	389	www.asir.local.

Delegación de subdominios y Registro GLUE (Glue Records)

- Si el nombre del DNS autoritativo del subdominio a delegar se encuentra en el subdominio
  - Se añade un registro **NS** en la zona padre que define el DNS autoritativo en la zona delegada.
  - Se añade un registro **A** asociado a la IP del DNS autoritativo para la zona delegada (registro **GR**).
- Si el nombre del DNS autoritario del subdominio a delegar no se encuentra en el subdominio
  - Se añade un registro NS en la zona padre que define el DNS autoritario de la zona delegada
  - No se añade registro A asociado, ya que el cliente DNS podrá acceder al dominio en el que esté alojado el servidor autoritario para el subdominio. No habrá por tanto *glue record*.

Los **Glue Records** son un tipo especial de registro DNS que proporciona la dirección IP de un servidor DNS **cuando ese servidor reside bajo el mismo dominio que está intentando resolver**. Sin ellos, se crearía un bucle infinito, y la página web o los servicios de correo dejarían de funcionar. No todos los usuarios de dominios necesitan configurarlos, son fundamentales para aquellos que buscan mayor control y personalización de su infraestructura DNS.

Supongamos que nuestro dominio es *midominio.com*, y queremos usar nuestros propios servidores DNS con nombres como *ns1.midominio.com* y *ns2.midominio.com*, para gestionar nuestros subdominios y tener más control. Para resolver *midominio.com*, el sistema necesita saber quiénes son sus servidores de nombres, que son *ns1.midominio.com* y *ns2.midominio.com*. Pero para resolver *ns1.midominio.com*, el sistema necesitaría preguntar a *ns1.midominio.com* (o ns2.midominio.com), lo cual es imposible porque aún no conoce su dirección IP. Tendríamos un problema de referencia circular o bucle infinito.

Aquí es donde los Glue Records tienen su función operando como un «*pegamento*» que **vincula el nombre del servidor de nombres** (*ns1.midominio.com*) **directamente a su dirección IP**, y esta información se almacena en los servidores DNS de nivel superior (los TLD como ***.com*** o ***.es***). De esta forma, cuando un resolver DNS busca midominio.com, los servidores TLD ya le proporcionan la IP de ns1.midominio.com junto con el nombre, rompiendo el bucle.

Configurar un registro GR

Para cada Glue Record, debemos proporcionar:

- El **nombre completo de nuestro servidor de nombres** (p. ej. ns1.midominio.com, ns2.midominio.com).
- La **dirección IP pública del servidor donde reside ese servidor de nombres**. Es fundamental que esta IP sea correcta y accesible públicamente. Usaremos la IP IPv4 y, si nuestra infraestructura lo soporta, también la IPv6.

```
asir.local.                 IN   NS   ns1.asir.local.          ;Servidor DNS maestro
asir.local.                 IN   NS   ns2.asir.local.          ;Servidor DNS esclavo.
asir.local.                 IN   NS   dns.asir.org.            ;Servidor DNS esclavo
....
ns1.asir.local.             IN   A    193.100.200.100
ns2.asir.local.             IN   A    193.100.200.200
;Delegación de subdominio
asir2srein.srein.local      IN   NS   ns1.asir2srein.asir.local  ;subdominio asir2srein delegado
ns1.asir2srein.asir.local   IN   A    193.100.202.100            ;glue record
```

Cambios en la dirección IP del servidor DNS

Si la dirección IP de nuestro servidor DNS personalizado cambia, debemos **actualizar el Glue Record** en nuestro registrador de dominio. Los Glue Records no se actualizan automáticamente como un registro A normal en nuestra zona DNS. Si la IP cambia y no actualizamos el Glue Record, nuestro dominio dejará de resolverse correctamente.

Transferencias de zona

La transferencia de zona es el mecanismo que usan los servidores de DNS para replicar la base de datos de un servidor maestro a uno o más servidores DNS esclavos. Este proceso garantiza que los cambios realizados en el servidor maestro se reflejen correctamente en los servidores esclavos, fundamental para mantener las bases de datos actualizadas de manera coherente.

El objetivo es que todos los servidores autoritarios para una misma zona tengan la información de sus registros sincronizada de forma consistente.

Los servidores primarios utilizan el puerto **53/TCP** para el intercambio de datos.

Existen 2 tipos de transferencias de zona:

- **Completa (AXFR)**. El servidor primario (*master*) envía al secundario (*slave*) los datos de la zona. La solicitud del secundario es una petición AXFR para una transferencia completa.
- **Incremental (IXFR)**. Como las transferencias de zonas con muchos RR pueden llevar mucho tiempo y recursos (procesamiento, ancho de banda, etc.) se introdujeron las transferencias incrementales. En este caso, el servidor primario envía al secundario solo los datos que han cambiado desde la última transferencia. El servidor secundario envía una petición IXFR para obtener una transferencia incremental.

4. Clientes DNS (resolvers)

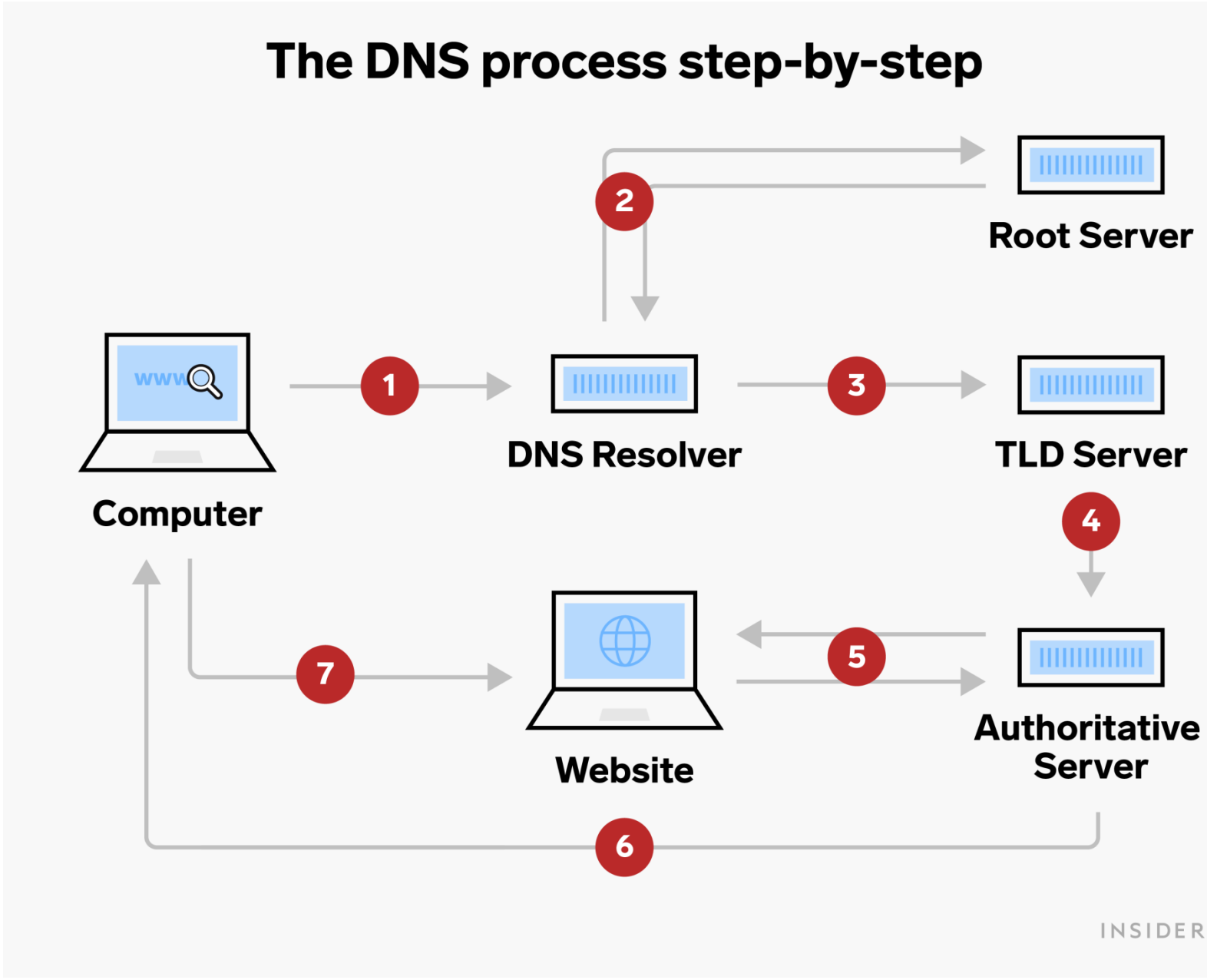
Un resolver es cualquier software capaz de preguntar a un servidor DNS e interpretar sus respuestas.

Los SO incluyen o permiten instalar un conjunto de librerías, denominadas ***stub resolver***, que realizan esta función. La forma en la que se resuelven nombres de dominio en un SO es configurable.

La configuración más habitual para este proceso es:

- El resolver consulta la ***caché*** de resolución de nombres del hosts almacenada en memoria (si está configurada) .
- Si el nombre buscado no está en la caché, busca en el archivo ***hosts*** local del equipo. Si tampoco encuentra el nombre en ese archivo, el resolver efectuará una ***consulta recursiva*** al servidor de nombres que esté configurado.
- Si no se alcanza el servidor DNS anterior, se intenta con el segundo configurado, y así por cada servidor DNS configurado en el sistema.
- Finalmente le entregará la respuesta a la aplicación.

El archivo host se encuentra en linux en **/etc/hosts**; y en Windows en c:**%SYSTEMROOT%\system32\drivers\etc\hosts**

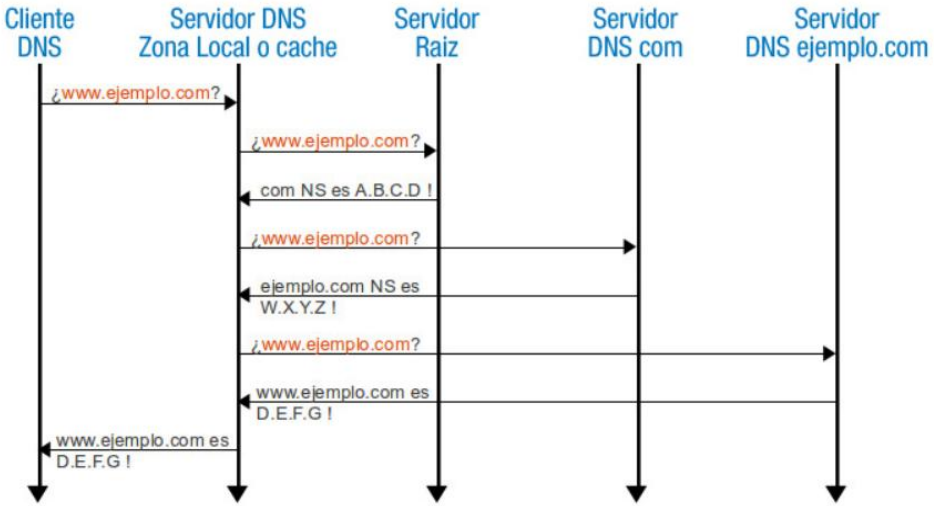

The DNS process step-by-step
Root Server
2
Computer
1
DNS Resolver
3
TLD Server
4
7
Website
5
Authoritative Server
6
INSIDER

5. Proceso de resolución

Los clientes y los servidores DNS consultan a otros servidores para resolver nombres de dominio. Las consultas a un servidor DNS pueden ser de dos tipos: **recursivas** o **iterativas**.

Consultas recursivas

Una consulta recursiva es aquella que se hace a un servidor con la recursividad activada; **tiene que dar una respuesta completa o exacta**.



Hay tres posibles respuestas:

- **Positiva**, es decir, devuelve la información del nombre por el que se ha preguntado, indicando además si es autoritativa o no.
- **Negativa**, devuelve ***NXDOMAIN*** lo que indica que el nombre no se pudo resolver (**N**on e**X**istent **D**omain).
- De **error**, por ejemplo, que no se puede preguntar a otros servidores por un fallo en la red.

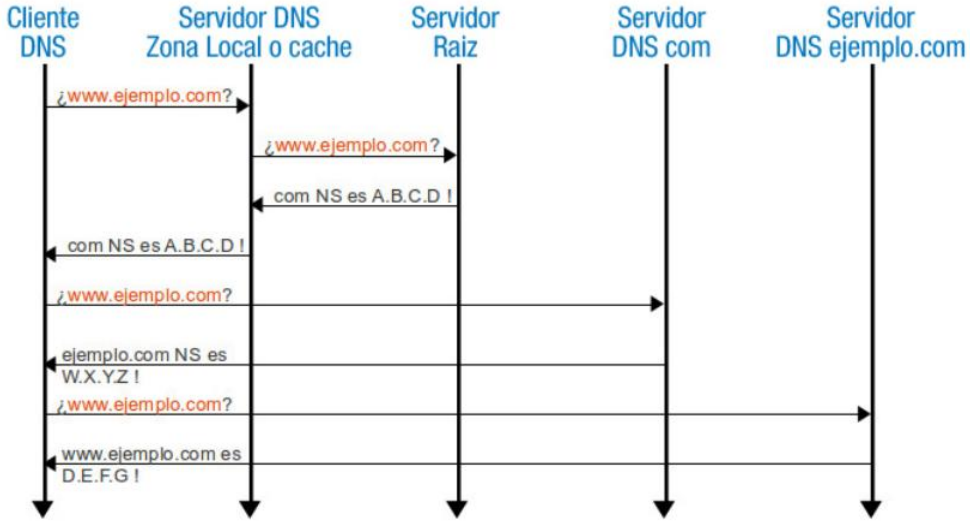
Cuando un servidor tiene activada la recursividad y recibe una consulta:

- Si es autorizado para alguna zona (maestro o esclavo) comprueba sus archivos de zona. Si encuentra la respuesta responde indicando que la respuesta es *autoritativa* (*Authoritative answer*) .
- Si no encuentra la respuesta o no es autorizado y actúa como caché, consulta su caché de respuestas anteriores. Si encuentra la respuesta responde indicando que la respuesta es *no autoritativa* (Non-*Authoritative answer*) .
- En otro caso:

1. Si tiene configurados reenviadores (*forwarders*), reenvía la consulta recursiva a otro servidor DNS. La respuesta que obtenga se la traslada al cliente o al servidor que le preguntó.
2. Si no tiene configurados reenviadores:
   a. Inicia una serie de consultas iterativas a otros servidores DNS.
   b. Los servidores DNS consultados devuelven referencias a otros servidores DNS que se usan para realizar nuevas preguntas.
   c. La recursividad finaliza cuando un servidor autorizado del espacio de nombres proporcione una respuesta, positiva o negativa.

Consultas iterativas

Una consulta iterativa o no recursiva es aquella que se hace a un servidor con la recursividad desactivada. Puede proporcionar una respuesta parcial.



Hay cuatro posibles respuestas:

- **Positiva**, es decir, da la información del nombre por el que se ha preguntado.
- **Negativa**, indica que el nombre no se pudo resolver (***NXDOMAIN***).
- Indicando una **referencia** a otros servidores, a los que se puede acudir para resolver la pregunta.
- De **error**, por ejemplo, que no se puede preguntar a otros servidores por un fallo en la red.

Cuando un servidor recibe una consulta iterativa:

•Si es autorizado para alguna zona (maestro o esclavo) comprueba sus archivos de zona. Si encuentra la respuesta responde indicando que la respuesta es autoritativa.

•Si no encuentra la respuesta o no es autorizado y actúa como caché, consulta su caché de respuestas anteriores. Si encuentra la respuesta responde indicando que la respuesta es no autoritativa.

•Si no se encuentra respuesta exacta con el nombre, devuelve una referencia que apunta a un servidor DNS que está autorizado para un nivel inferior del espacio de nombres del dominio. Esta referencia será la que devuelva al servidor que le hizo la consulta iterativa para continuar su proceso de resolución (proceso recursivo).

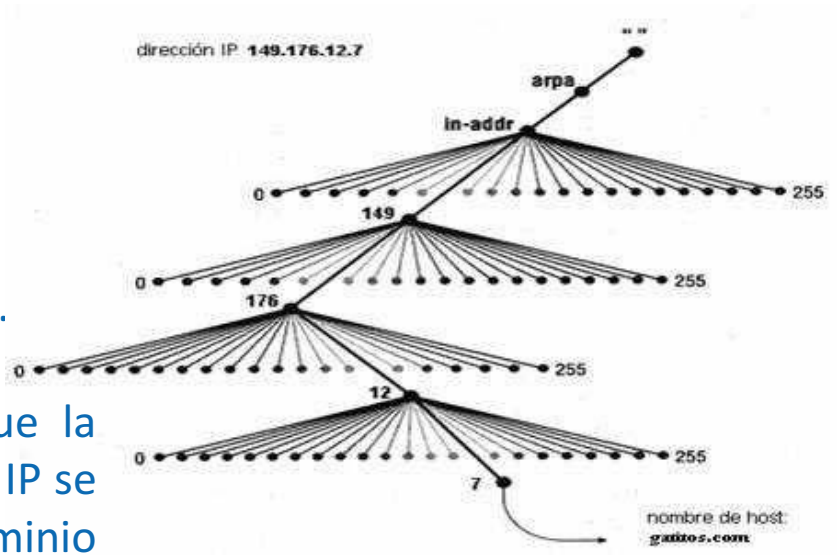
Las consultas iterativas son realizadas por servidores a otros servidores DNS después de haber recibido una consulta recursiva (y no encontrar la respuesta ni en sus archivos de zona ni en su caché).

6. Resolución inversa

Una consulta inversa a un servidor consiste en preguntar por un nombre de dominio conocida una dirección IP.

Los motivos para realizar esta consulta pueden ser:

- 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.
- etc.



La resolución de direcciones IP funciona igual que la resolución de nombres de dominio. Las direcciones IP se tratan como nombres, donde cada byte es un dominio que cuelga de los dominios "***in-addr.arpa***" para direcciones IPv4, e "***ip6.arpa***" para las direcciones IPv6.

La resolución funciona igual que la resolución directa, siendo el dominio raíz "***in-adr- arpa***" y los subdominios vienen dados por los bytes de la dirección en orden inverso. Por ejemplo: el dominio inverso para las direcciones **192.168.22.0/24** sería **22.168.192.in-addr.arpa.**

Los servidores DNS tienen que almacenar zonas de resolución inversa con registros de recursos que asocien nombres de dominio con direcciones IP.

Las zonas directa e inversa son independientes, y es responsabilidad de los administradores que contengan información coherente y que no haya discrepancias.

7. DNS dinámico (DDNS)

Para que los usuarios tengan acceso a los recursos DNS correctamente, es fundamental que los servidores de nombres estén actualizados.

La actualización de los registros de recursos de un archivo de zona se puede realizar **manual** o **dinámicamente** lo que es útil cuando las direcciones IP también se asignan de forma dinámica.

- En las **actualizaciones manuales** el ***administrador*** crea, elimina o modifica registros de recursos editando los ficheros de zona. Si una red tiene un servidor DHCP, las tareas de actualización crecen considerablemente.
- Con las **actualizaciones dinámicas**, los registros de recursos de un fichero de zona pueden ser actualizados por una ***fuente externa*** (no el administrador). Pueden ser realizadas directamente por los equipos (cliente DNS/servidor DNS) o por servidores DHCP.

Los proveedores de acceso a Internet (ISP) asignan una dirección IP por DHCP al router que nos conecta a su red (a no ser que contratemos una IP fija). Existen webs que ofrecen el servicio de DNS dinámico en Internet: permiten registrar un nombre DNS y actualizar su dirección IP en tiempo real (DynDNS, No-ip, EasyDNS, ZoneEdit, Cdmon,…)

Lo más habitual es configurar un programa en el router de conexión a Internet o en un equipo de la red para que actualice el servidor DNS cuando la IP asignada por DHCP cambie. Los routers que se comercializan actualmente suelen tener integrados estos programas.

8. Comandos

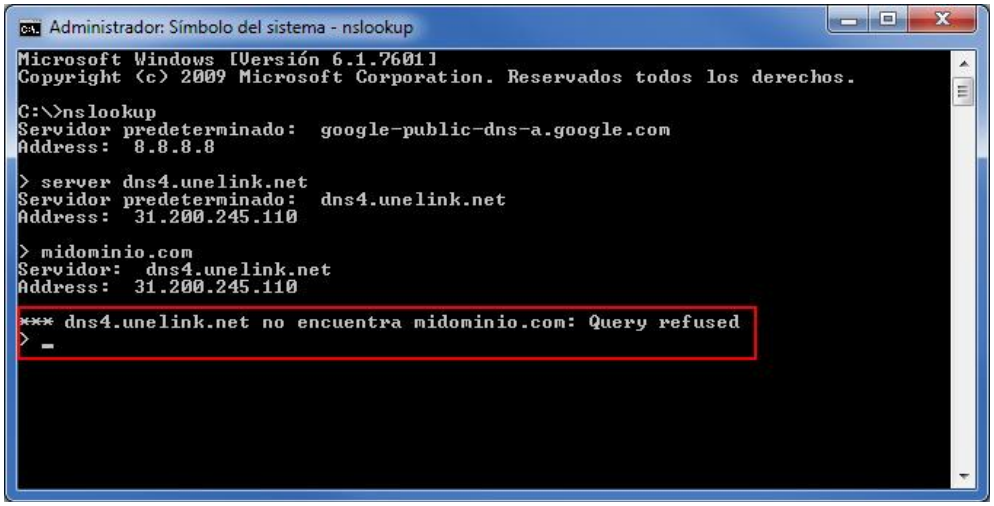
Se ejecutan desde el *terminal* Linux y el ***PowerShell*** (o el *cmd*) en Windows. Algunos no vienen de forma predeterminada (se instalan). Su forma general (y más básica) de ejecución es *comando URL.*

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.

Con nslookup podemos obtener la dirección IP asociada a un nombre DNS y viceversa.

Además, podemos preguntar a los servidores de nombres información relativa a los registros de recursos (RR) de la/s zona/s de las que son autorizados. Funciona tanto en Linux como en Windows.



dig (**D**omain **I**nformation **G**roper)

Es un programa utilizado para preguntar a los servidores DNS. Se utiliza 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 (CLI), pero también tiene un modo de operar por lotes, leyendo las consultas desde un archivo. Funciona tanto en Linux como en Windows.

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, etc. Funciona tanto en Linux como en Windows.

ping

Es una utilidad de diagnóstico en redes de computadoras que comprueba el estado de la comunicación del anfitrión local con uno o varios equipos remotos de una red que ejecuten. Funciona tanto en Linux como en Windows.

9. Servicios DNS en la nube

Gestionados por un proveedor en la nube, ofrecen ventajas como:

- **Alto rendimiento:** La distribución de su infraestructura hace que las consultas se resuelvan rápidamente desde ubicaciones cercanas al usuario.
- **Fiabilidad:** El servicio distribuido es más resistente a fallos.
- **Rentabilidad:** Suele ser una opción más económica que alojar, configurar y mantener servidores DNS propios.
- **Escalabilidad:** Se adaptan mejor al aumento del volumen de consultas.
- **Seguridad**: Están dotados de diversas funciones de seguridad y elementos redundantes.



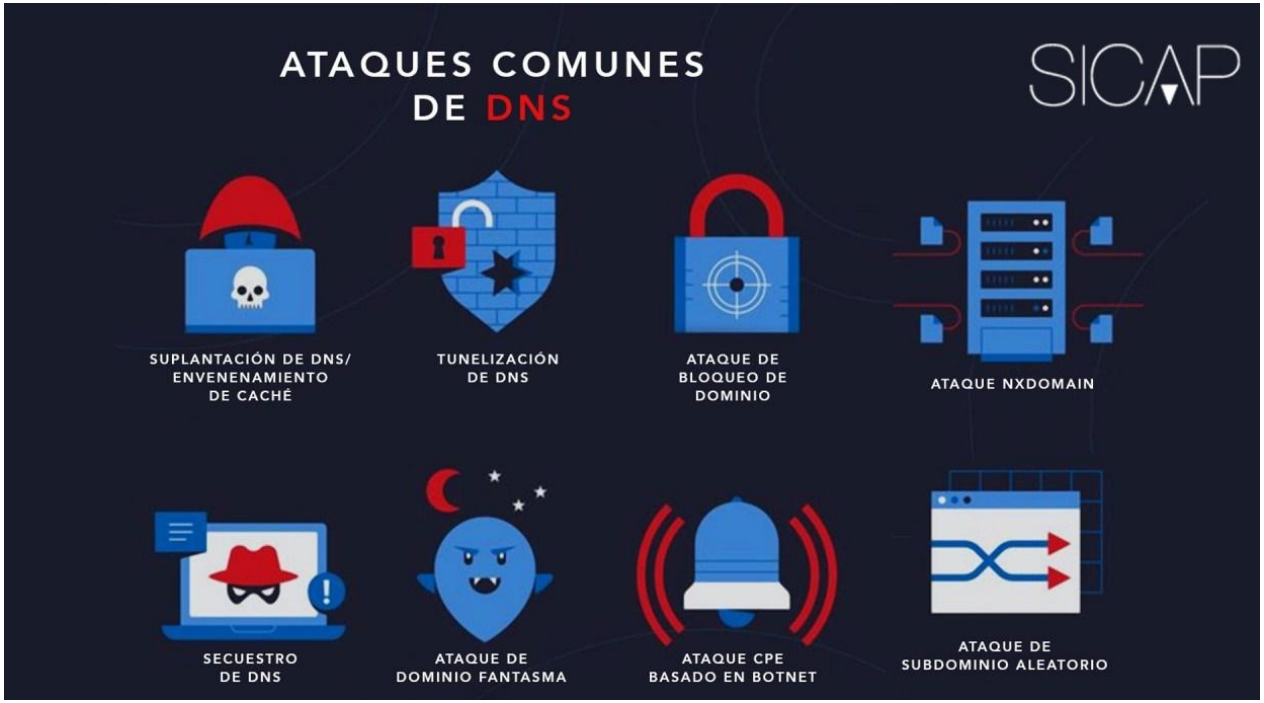
Servidores DNS en la nube populares son:

Google Cloud DNS
Cloudflare DNS
OpenDNS de CISCO
Oracle Cloud
…

10. Seguridad DNS

El servicio DNS está en el punto de mira de los potenciales atacantes pues es un servicio vital para el funcionamiento de Internet.

En su origen se diseñó como un sistema abierto sin contemplar aspectos de seguridad. Además, su seguridad es difícil de gestionar al ser un servicio distribuido formado por varios componentes que se comunican entre sí.



Ataques comunes

Algunos de los **ataques más comunes** que afectan a la infraestructura DNS son:

- **Ataques de denegación de servicio DNS:** interrumpen los servicios DNS, lo que hace que no sea posible acceder a los sitios que sirven. Estos ataques podrían consumir recursos del servidor solicitando dominios inexistentes (NXDOMAIN), subdominios aleatorios, o realizar un ataque DoS distribuido (DDoS) contra un servidor DNS.
- **Falsificación de DNS:** es similar al secuestro de DNS, pero el objetivo son los resolvers DNS, que almacenan en caché los registros DNS solicitados habitual o recientemente. Un ataque de falsificación de DNS o *envenenamiento de caché* introduce registros DNS falsos en la caché de un resolver; entonces las solicitudes de esos dominios se direccionan a un sitio web controlado por el atacante.
- **Amplificación DDoS DNS:** se aprovecha de servicios que se comunican por UDP y que tienen respuestas mucho mayores que la solicitud correspondiente. Estos factores permiten a un atacante enviar solicitudes al servicio y que sus respuestas, mucho mayores, se envíen al objetivo. Un ataque de amplificación DNS inunda el objetivo con respuestas DNS, lo que consume ancho de banda y satura los servidores objetivo.
- **Tunelización DNS:** aprovecha los permisos del tráfico DNS para atravesar los firewalls corporativos. Estos ataques utilizan el tráfico DNS para mover los datos entre el malware y el servidor de datos controlado por el atacante.

Además de los ataques existentes, surgen nuevas formas de ataques DNS, como por ejemplo, ataques DNS impulsados por IA o exploits DNS de día cero.

Mecanismos de seguridad

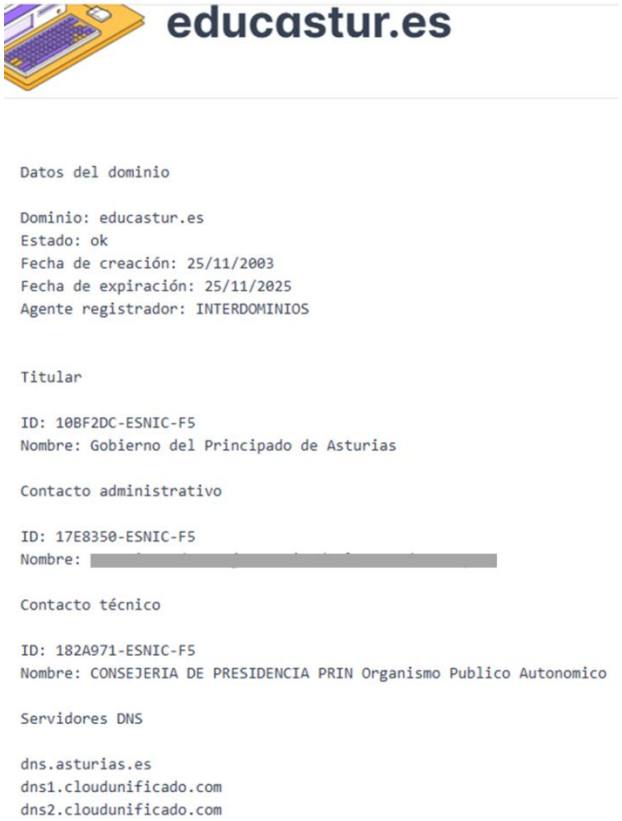
Algunas opciones para mitigar los ataques DNS son:

- **DNSSEC:** DNSSEC es un protocolo de seguridad que firma las respuestas de los servidores DNS. Esto ayuda a proteger contra el secuestro y la falsificación de DNS autenticando los datos devueltos al cliente.
- **Infraestructura redundante:** el funcionamiento de los ataques DoS contra la infraestructura DNS consiste en enviar al servidor DNS objetivo más tráfico del que puede manejar. Mediante el sobreabastecimiento de los servidores y la utilización del enrutamiento anycast, es posible equilibrar la carga de tráfico entre varios servidores. Esto garantiza la disponibilidad si un servidor está sobrecargado o deja de funcionar.
- **Firewall DNS:** un firewall DNS se sitúa entre el servidor de nombres autoritativos de un dominio y los resolvers recursivos de los usuarios. El firewall puede limitar la velocidad de las solicitudes como protección contra los ataques DDoS o filtrar el tráfico para bloquear las solicitudes maliciosas o sospechosas.
- **DNS encriptado:** por defecto, el DNS es un protocolo no encriptado ni autentificado. DNS sobre HTTPS (DoH) y DNS sobre TLS (DoT) proporcionan encriptación y autenticación.

DNSSEC, asegurando la integridad y autenticidad de tu dominio web (incibe)

11. Whois

Whois es una base de datos distribuida que informa de los datos de un dominio DNS. Esta base de datos puede ser usada para obtener información sobre el usuario registrante, el registrador o el listado de servidores de nombres.



Su protocolo que permite realizar consultas a bases de datos que contienen información sobre el titular (persona, empresa u organización) que registra un nombre de dominio o un rango de direcciones IP.

El protocolo whois sólo indica el intercambio de consultas y respuestas, no el formato de los datos. Esto implica que el resultado de la consulta whois puede ser diferente en función de la base de datos whois que se consulte.

Se pueden realizar consultas whois en sitios web especializados (habitualmente registradores de nombres) o utilizando un programa cliente.

Puede presentar problemas de privacidad o ser fuente de información para *spammers*.

Las personas o entidades que lo deseen, pueden evitar que sus datos sean de acceso público mediante Whois.

REFERENCIAS

Bibliografía

Servicios de red e internet. García Sánchez, Álvaro. Sanz Rodríguez, Javier. González Sotillo, Álvaro. Enamorado Sarmiento, Luis. Garceta Grupo Editorial.

Servicios en Red. Andreu Gómez, Joaquín . Editorial Editex

Webgrafía

Wikipedia

recursostic.educacion.es

www.cloudflare.com

Otros…

