SERVICIOS EN RED

C.F.G.M. SISTEMAS MICROINFORMÁTICOS Y REDES

Profesor: Jorge Martín Cabello

UD 3. EL SERVICIO DNS

REV 1.1

Tabla de contenido

1. DNS (Domain Name Dystem)

1.1. Definición

El servicio DNS (Domain Name System) o sistema de nombres de dominio , es un sistema de asocia las direcciones IP de una red de ordenadores con direcciones alfanuméricas legibles y gestionables para los usuarios de la red.

En una red TCP/IP, las máquinas se identifican mediante su dirección de red o número IP. Para las personas resulta más sencillo recordar un nombre que se asocia a una máquina concreta. También es más fiable, ya que la dirección IP puede cambiar, pero no así el nombre.

Es necesario un mecanismo que traduzca los nombres de las máquinas a direcciones IP. El servicio DNS permite que esta tarea se lleve a cabo.

DNS ofrece un servicio de almacenamiento y consulta de información. La información se guarda en una base de datos distribuida entre múltiples equipos y la indexa según esquema de nombres jerárquico. A los servidores de nombres se les pueden realizar preguntas y para ello se usan los programas que dialogan con los servidores en base a unas reglas (protocolo DNS).

DNS puede almacenar varios tipos de información sobre cada nombre de dominio y por ello se puede utilizar para diferentes propósitos. Lo habitual es asociar direcciones IP con nombres de dominio y por eso se utiliza comúnmente para:

- Resolución de nombres (búsqueda directa).
- Resolución inversa de direcciones (búsqueda inversa).
- Resolución de servidores de correo.

También se puede utilizar DNS para otros propósitos: balanceo de carga, obtención de claves públicas, ubicación de servidores para un servicio predeterminado...

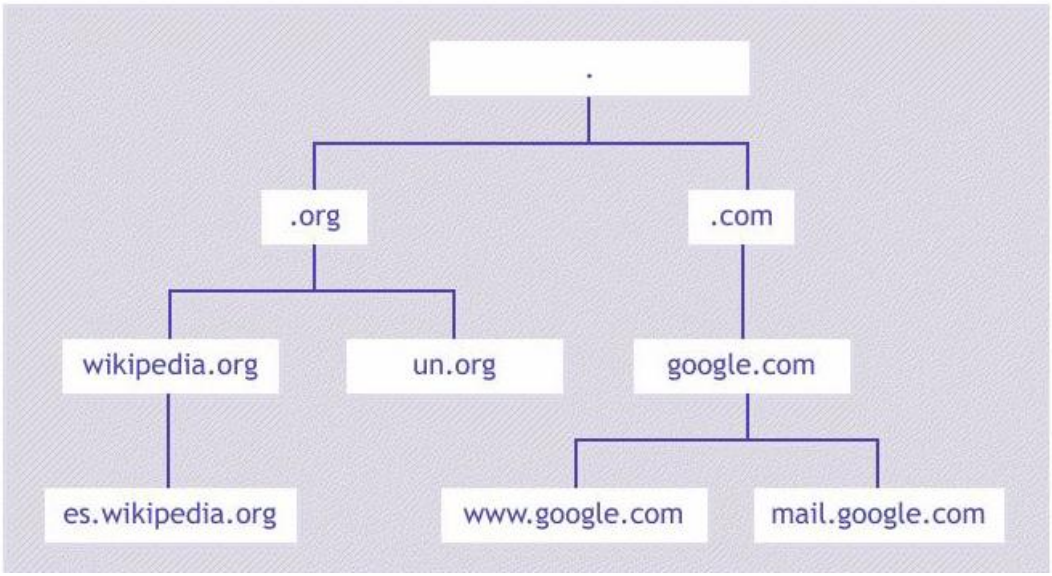
1.2. El espacio de nombres de dominio

El servicio DNS se compone de una base de datos distribuida (integrada por varias máquinas conectadas en red) en la que se almacenan las asociaciones de nombres de dominios y direcciones IP. Esta base de datos está clasificada por nombres de dominio, donde cada uno puede considerarse una rama en un árbol invertido llamado **espacio de nombres de dominio.**

El árbol comienza en el nodo raíz, situado en el nivel superior. Por debajo, puede existir un número indeterminado de nodos.

Normalmente se utilizan hasta cinco niveles. El nombre completo de un nodo está formado por el conjunto de nombres que forman el itinerario desde ese nodo hasta la raíz.

Los nombres se separan con un punto. El dominio es, pues, cada uno de los subárboles que integran el árbol o espacio de nombres de dominio.



El nivel superior o primer nivel (TLD Top Level Domain) está formado por los dominios que descienden directamente del dominio raíz. No pueden ser comprados por los usuarios. Se dividen en 3 grupos: Infraestructura , Dominio genéricos (gTDL) y Dominios geográficos (ccTDL)

Tablas subdivisión TLD		
TLD	Dominios	
Infraestructura	Utilizado para obtener el FQDN	.arpa
gTLD Dominios genéricos	(uTLD) No patrocinados. Estos dominios pueden ser alquilados sin restricciones. Están gestionados por el ICANN.	.com, .org, .net, .int, .gov, .info, .name, .biz
	(sTLD) Existen limitaciones a la hora de contratar estos dominios. Están patrocinados por diferentes instituciones.	.aero, .asia, .cat, .coop, .edu, .jobs, .mobi, museu.pro, .tel, .travel, .xxx
ccTLD Dominios geográficos	Creados por IANA. Existen unos 243 gestionados por los distintos gobiernos mediante organizaciones propias.	.es, .uk, .eu, .us

Estos dominios son gestionados por la ICANN y el siguiente nivel y todos los nodos jerárquicos dependientes de el los gestiona la entidad propietaria del dominio.

1.3. FQDN [nombre de dominio completo]

FQDN (Fully Qualified Domain Name) Es un nombre de dominio inequívoco que especifica la ubicación exacta de un equipo dentro de la jerarquía del dominio. El nombre de dominio completo de un equipo específico o host en Internet. El FQDN consta de dos partes: el nombre de host y el nombre de dominio. Un ejemplo es miequipo.midominio.com.

1.4. Delegación de dominios

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

El dominio puede ser dividido en **subdominios** por el administrador y delegar el control de cada uno.

La autoridad que se hace cargo de la delegación debe asumir también la responsabilidad de **mantener actualizados los registros de recursos** de ese subdominio.

Pero delegación no significa independencia, sino **coordinación.** La división de un dominio en subdominios no implica siempre una cesión de autoridad.

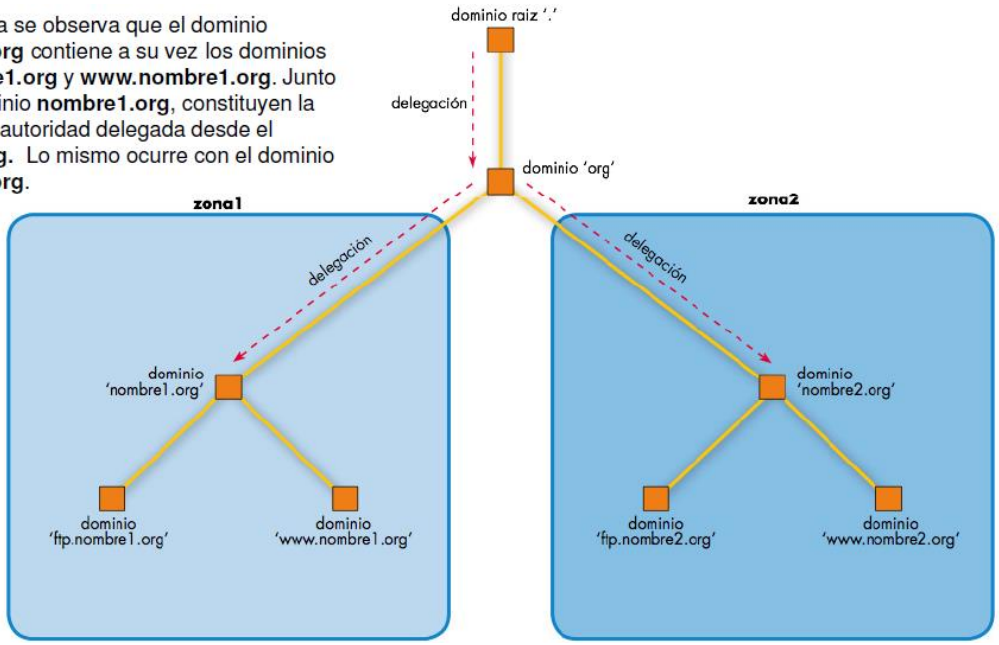
1.5. Dominios y Zonas

Ya sabemos que cada dominio puede dividirse en subdominios dependientes jerárquicamente en forma de árbol.

La zona es la parte de la base de datos de nombre de dominio alojada en el servidor DNS. Puede ser gestionada por más de un servidor. Entre los distintos servidores de una zona existe una relación jerárquica donde el **servidor autoritativo** de la zona es el que tiene la base de datos de la información completa de la zona.

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

En la Figura se observa que el dominio **nombre1.org** contiene a su vez los dominios **ftp.nombre1.org** y **www.nombre1.org**. Junto con el dominio **nombre1.org**, constituyen la **zona1** con autoridad delegada desde el dominio **org.** Lo mismo ocurre con el dominio **nombre2.org**.



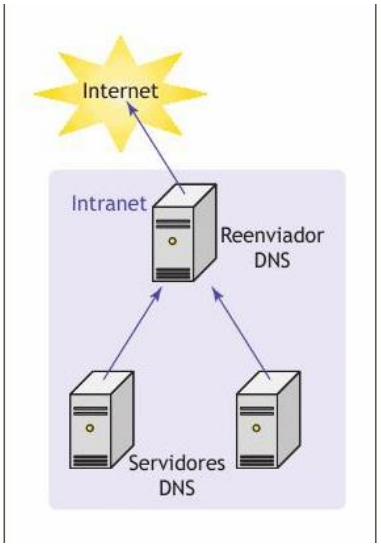
Los servidores de nombres se pueden clasificar en los tipos siguientes:

Servidores autoritativos.

- **Servidor primario (maestro):** en él se llevan a cabo todas las modificaciones sobre una zona.
- **Servidor secundario (esclavo):** contiene una copia de solo lectura de los archivos de zona. El servidor primario le comunica los datos de la zona (altas y modificaciones) a través de peticiones de zona.

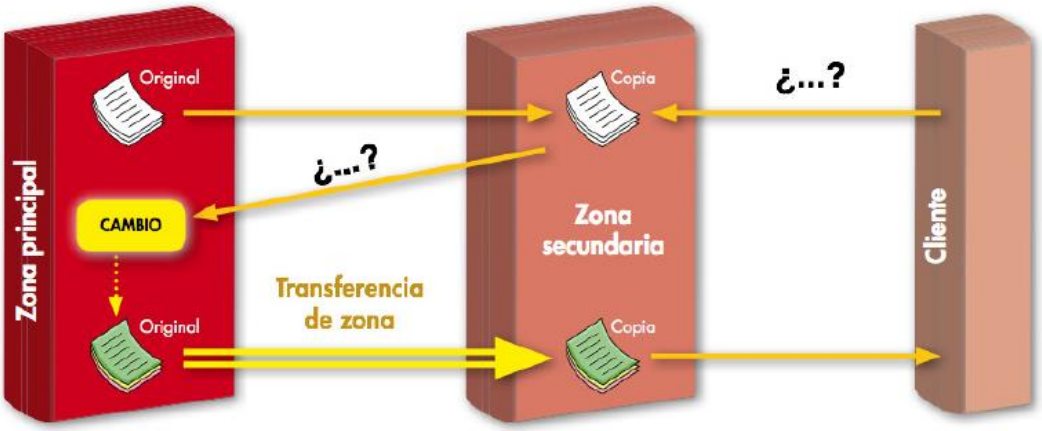
Servidores No Autoritativos.

- **Reenviadores:** Cuando en una rede tenemos varios servidores DNS en una red se puede configurar un servidor fordwarder para unificar las peticiones DNS a internet de toda la red.
- **Servidor caché:** Es un servidor intermedio que trabaja en la zona secundaria. No contiene ningún tipo de información acerca de la base de datos de la zona. Cuando se les realiza una consulta ellos preguntan a su servidor secundario y este les da la resolución. Almacenan copias de las peticiones y las resoluciones de las mismas para próximas consultas.



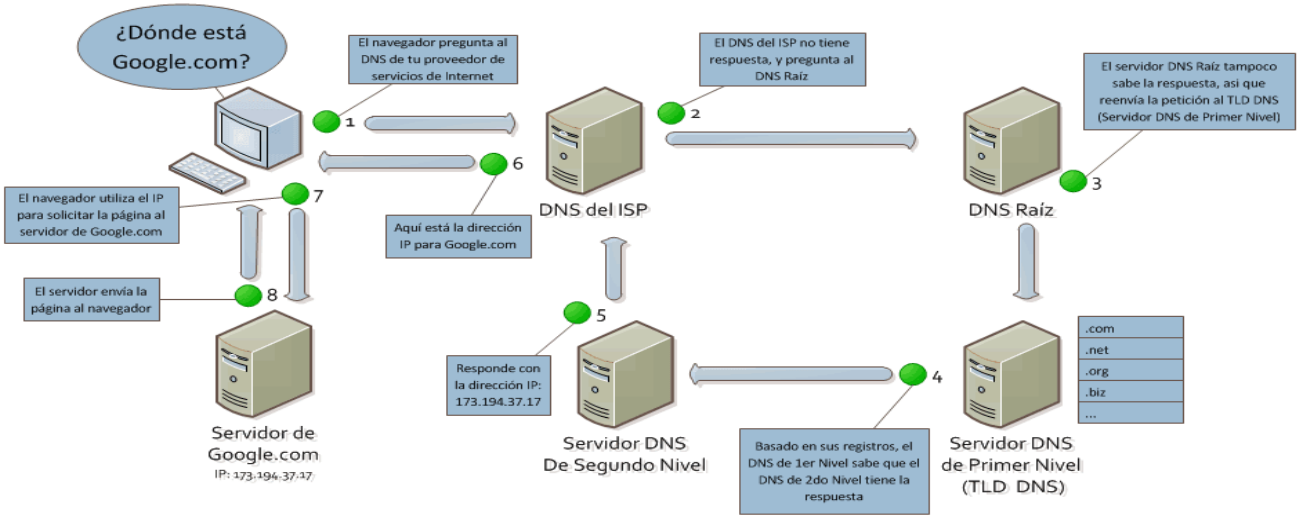
La información de las zonas se obtiene a través de la red mediante la **transferencia de zona** en los casos**:**

- Se guardan o actualizan los datos del servidor principal.
- Iniciamos el servidor secundario.
- Cuando caduca el tiempo de actualización.



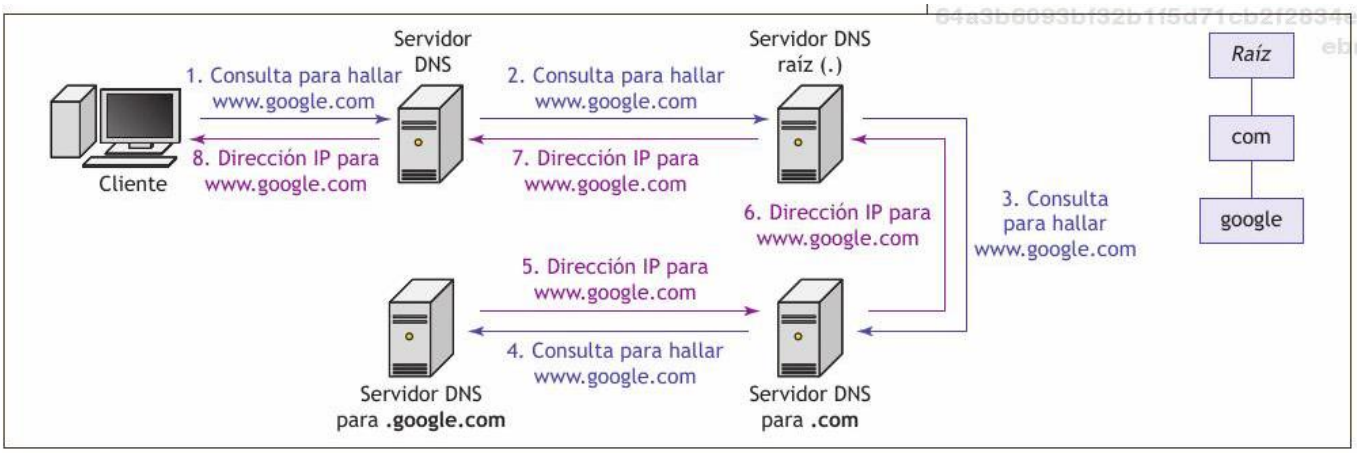
2. FUNCIONAMIENTO DE DNS

2.1. Consultas recursivas e interactivas.

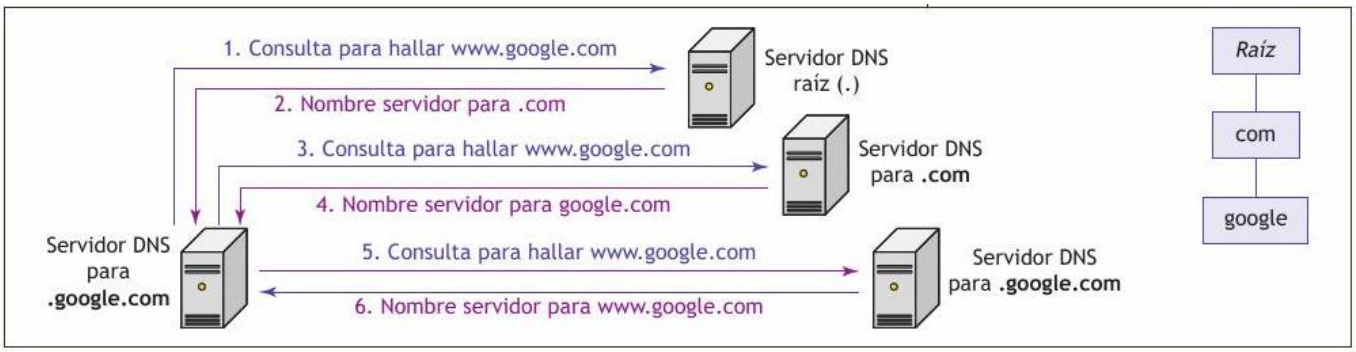


La actividad principal de un servidor DNS es contestar consultas, tantos de un cliente como de otro servidor DNS. Según el modo en que se envían las consultas las podemos clasificar en dos tipos:

Consultas recursivas: El cliente realiza una consulta a un servidor y este responde con la resolución que tiene en su base de datos local. En caso de no tenerla debe de elevar la petición a otros servidores DNS en nombre del cliente.



Consultas interactivas: El cliente realiza una consulta a un servidor DNS y este si no tiene la resolución en su base de datos remite al cliente la dirección de otro servidor DNS para que el cliente le pregunte al mismo. Este proceso se puede repetir tantas veces como sea necesario hasta llegar al servidor DNS adecuado.

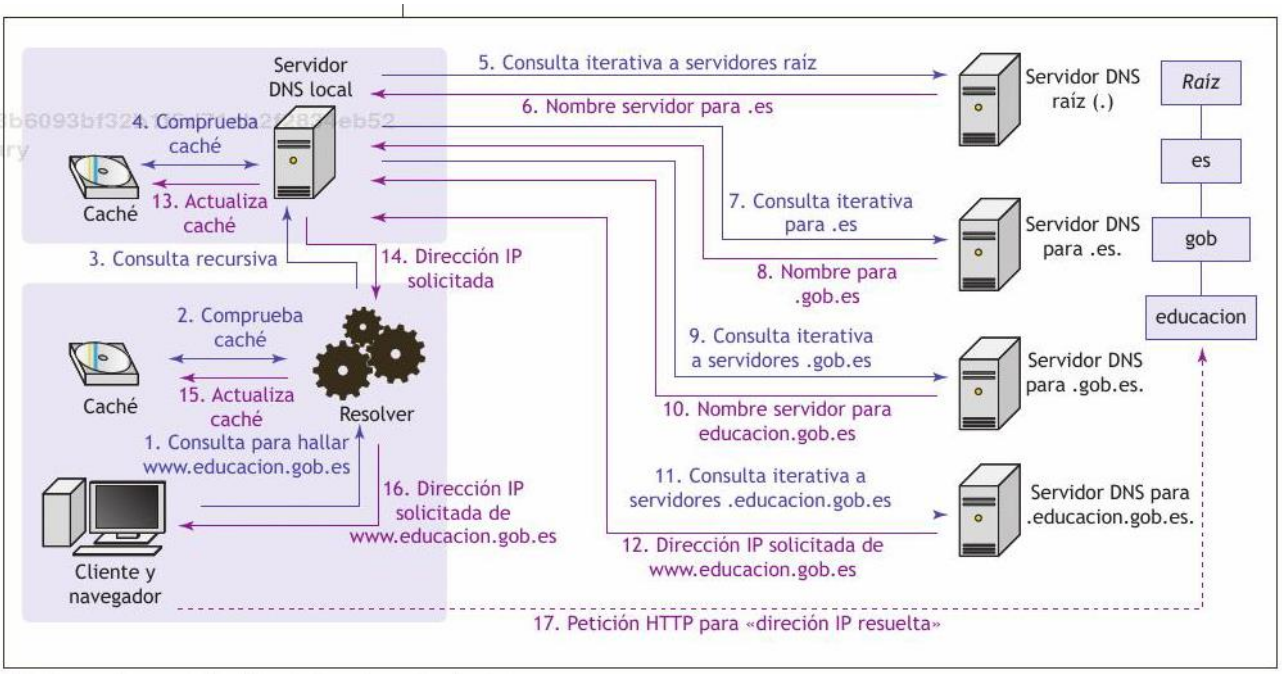


2.2. Resolvers

Son programas del sistema operativo que hacen de interfaz entre las aplicaciones de usuario y el sistema DNS. Dentro del software del sistema informático se encarga de atender las peticiones de las aplicaciones que funcionan con los protocolos http, ftp, telnet,…Devuelve la resolución de forma compatible con el formato de la aplicación.

Los resolvers usan una memoria caché donde guardan los resultados de peticiones anteriores resueltas. De este modo pueden agilizar el proceso de resolución y resolverlas hacer peticiones al servidor DNS.

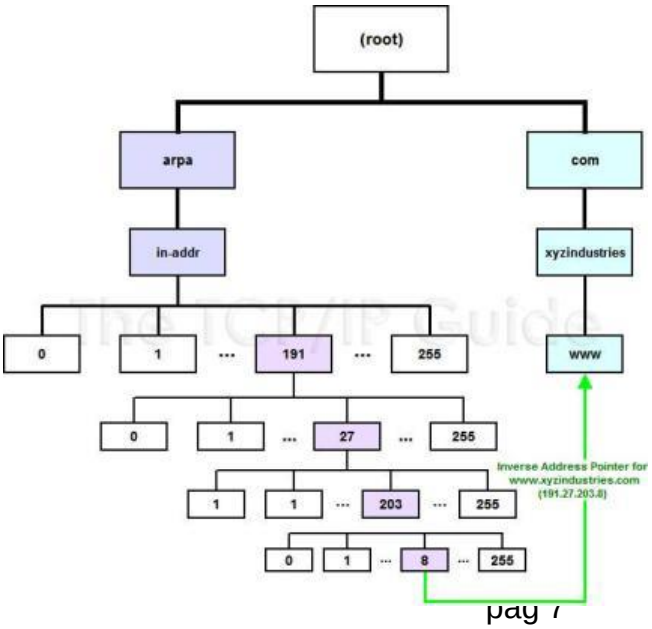
Los resolvers resuelven las peticiones de las aplicaciones con resoluciones directas o inversas.



2.3. Resoluciones Inversas.

En las **resoluciones directas** se pregunta por un dirección IP a partir de un nombre de dominio.

En las **resoluciones inversas** se preguntar por un nombre partiendo de una dirección IP. Esta resolución es posible ya que el sistema implementa un nodo especial llamado “arpa” . Es un subárbol especial que tiene un único dominio de primer nivel llamado in-addr-arpa y de el cuelga una jerarquía numérica que cubre el espacio de direcciones IP con el nombre de dominio asociado según el sistema de direcciones IP . Por ejemplo



para IPv4 de cada nodo cuelgan 4 nodos y cada uno se dividen en 256 subdominios.

3. LA BASE DE DATOS DNS. TIPOS DE REGISTROS.

Un DNS es una base de datos distribuida formada por los llamados archivos de zona que se encuentran distribuidos entre los servidores de nombres.

Estos archivos contienen registros que se conocen como **RR** (registros de recursos), relacionados con nombres de dominio. La información solo es útil para las personas responsables de la administración de un dominio, dado que el funcionamiento de los servidores de nombre de dominio es completamente transparente para los usuarios.

Ya que el sistema de memoria caché permite que el sistema DNS sea distribuido, los registros para cada dominio tienen una duración de vida que se conoce como **TTL** (tiempo de vida). Esto permite que los servidores intermediarios conozcan la fecha de caducidad de la información y por lo tanto que sepan si es necesario verificarla o no.

Por lo general, un registro de recurso RR de DNS contiene la siguiente información: (RR A)

Propietario (FQDN)	TTL	Tipo	Clase	RData
es.ccm.net	3600	A	IN	163.5.255.85

Propietario: indica el nombre de dominio debe (FQDN), en el que se encuentra el recurso que se define (RData) en el RR.

Tipo: un valor sobre 16 bits que define el tipo de recurso descrito por el registro. El tipo de recurso puede ser uno de los siguientes:

- **A**: Los registros de dirección A, **(**Address**)** asocian nombres de host a direcciones IP dentro de una zona. Son los más numerosos dentro del archivo.

Campos del registro de recurso dirección (RR A)			
NombreDominio	IN	A	IP
tirant.gva.es.	IN	A	172.16.100.127

- **AAA**: como A pero para direcciones IPv6
- **CNAME** (nombre canónico): Estos registros son llamados también alias**,** si bien son conocidos como entradas de *nombre canónico* **(**CNAME, Canonical Name**).** Su uso más común es utilizar para apuntar a un único host más de un nombre, así se simplifican procesos como albergar simultáneamente un servidor web y otro FTP en un mismo equipo.

Campos del registro de recurso nombre canónico (RR CNAME)			
NombreDominio	IN	CNAME	Nombre canónico o IP
ftp.edu.gva.es.	IN	CNAME	www.edu.gva.es.

- **MX** (*Mail eXchange*): El registro MX es el registro de Intercambio de correo **(**Mail eXchange**).** Indica que host se encarga del procesamiento del correo electrónico de ese dominio..
- **NS:** El Registro NS. (siglas de Name Server), contiene los servidores de nombre de ese dominio, lo que permite que otros servidores de nombres vean los nombres de su dominio. Habrá tantos registros NS como servidores primarios y secundarios de la zona.

Campos del registro de recurso nombre de servidor (RR NS)			
NombreDominio	IN	NS	Nombre servidor
gva.es.	IN	NS	tirant.gva.es.

- **PTR**: es un puntero que apunta a un servidor para búsquedas inversas.

Campos del registro de recurso puntero (RR PTR)			
IPInversa.in-addr.arpa	IN	PTR	Nombre canónico
254.16.77.195.in-addr.arpa	IN	PTR	inf16254.gva.es.

- **SOA**: Se forma con una serie de parámetros a tener en cuenta

  - **Host Origen:** Host donde se mantiene el archivo (primario).
  - **Correo electrónico:** Del responsable de la BD. La arroba (@) se sustituye por un punto (.), debido a que @ representa el dominio raiz de la zona.
  - **Numero de serie:** La versión de ese archivo. Aumenta cada vez que el archivo cambia.
  - **Tiempo de actualización:** Tiempo que espera un servidor de nombres secundario para ver si el archivo ha cambiado, y por lo tanto pedir una **transferencia de zona**.
  - **Tiempo de reintento:** Tiempo que espera un servidor de nombres secundario para iniciar una nueva transferencia de zona en el caso de que falle este procedimiento.
  - **Tiempo de caducidad:** Tiempo que el servidor de nombres secundario intentará descargar una zona. Cuando pase, se rechaza la información antigua.
  - **Tiempo de vida:** Tiempo en el que el servidor de nombres mantiene la caché cualquier registro del recurso de este archivo en base de datos.
  - **TXT**. Puede contener cualquier información

Campos del registro de recurso inicio de autoridad (RR SOA)						
NombreDominio	IN	SOA	nsPrimario	admin.nsPrimario	(ops)	
gva.es.	IN	SOA	ninot.gva.es.	admincorreo.gva.es.	(2012020700; 14400; 300; 604800; 7200);	Número de serie Actualización Reintento Caducidad Valor TTL

Clase: la clase puede ser **IN** (relacionada a protocolos de Internet, y por lo tanto, es el sistema que utilizaremos en nuestro caso), o **CH** (para el sistema caótico).

RDATA: estos son los datos relacionados con el registro de recursos. La información que contienen dependerá del tipo de registro:

- A: dirección IP de 32 bits;
- CNAME: FQDN del alias;
- MX: FQDN o IP del servidor de correo. En caso de varios se puede establecer prioridad;
- NS: FQDN del servidor autoritario del dominio, puede ser primario o secundario;
- PTR: el nombre de dominio para el registro inverso;
- SOA: varios campos FQDN del servidor primario , dirección correo administrador, tiempos, ……

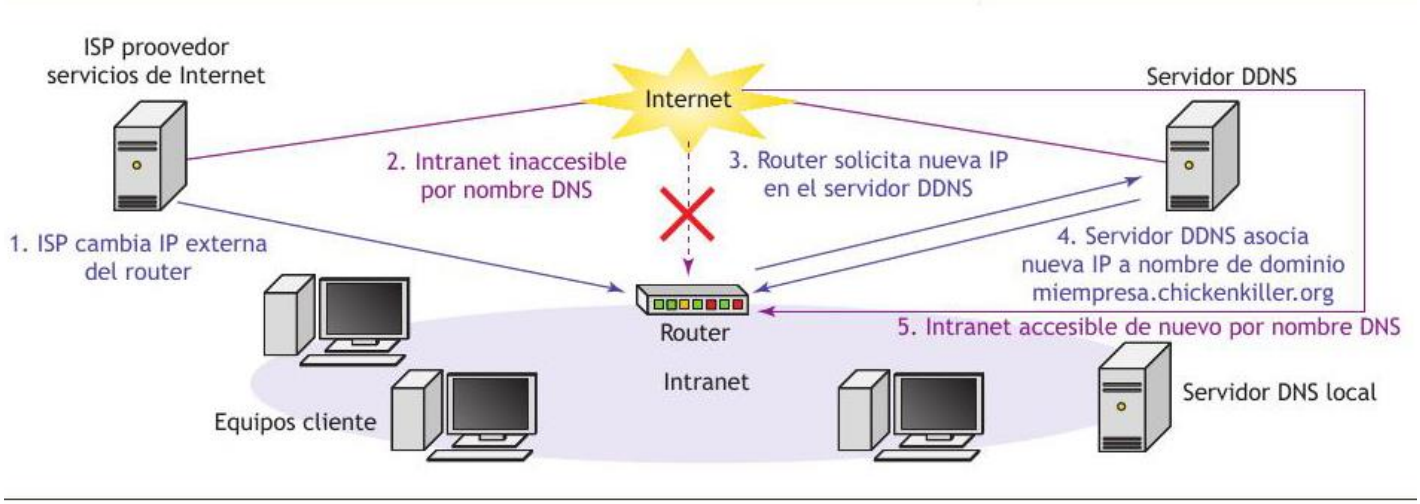
4. DYNAMIC DNS

Las siglas **DDNS** se refieren al concepto **Sistema Dinámico de Nombres de Dominio,** un mecanismo que permite la asignación de un nombre de dominio a una máquina con dirección IP dinámica. A menudo el proveedor de Internet proporciona una IP pública dinámica a nuestro ordenador. De esta forma impide que se puedan dar servicios en internet al no tener una Ip permanente que se pueda asociar al registro A de un dominio. Sin embargo, con un DNS dinámico se puede configurar un sitio web doméstico sin necesidad de utilizar un hosting externo siempre y cuando se mantenga activo el servidor durante las 24 horas del día.

El sistema se basa en un software que actualiza de forma automática la IP de nuestro router.

DynDNS ofrece este servicio DDNS gratuitamente (www.dyndns.com).

Otra opción para este servicio es www.no-ip.com.


ISP proovedor
servicios de Internet
Internet
Servidor DDNS
2. Intranet inaccesible
por nombre DNS
3. Router solicita nueva IP
en el servidor DDNS
1. ISP cambia IP externa
del router
4. Servidor DDNS asocia
nueva IP a nombre de dominio
miempresa.chickenkiller.org
Router
5. Intranet accesible de nuevo por nombre DNS
Intranet
Equipos cliente
Servidor DNS local