DNS

DAW RETO 3

¿Qué es DNS?

- Domain Name System o DNS (Sistema de Nombres de Dominio).
- Su función más importante es traducir nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red.
- Traducir IPs en nombres y nombres en IPs.

¿Por qué DNS?

- En el momento que tenemos muchas direcciones IP va a ser difícil recordarlas todas.
- Es más fácil recordar un nombre
  - Por ejeplo: egibide.org
- Lo utilizamos para navegar por internet.
  - Si configuramos en manual: introducimos todos los parámetros.
  - Si configuramos en automático: nos lo ofrece el servidor dhcp.

COMPONENTES

- PARA LA OPERACIÓN PRÁCTICA DE DNS UTILIZAMOS 3 COMPONENTES:
  - **CLIENTES**: Genera peticiones DNS de resolución de nombres a un servidor.
  - **SERVIDORES DNS**: Contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.
  - **ZONAS DE AUTORIDAD:** Es una parte del espacio de nombre de dominio sobre la que es responsable un servidor DNS, que puede tener autoridad sobre varias zonas. (Ej: .org, .com...)

PARTES DE UN NOMBRE DE DOMINIO

- Consiste en dos o más partes (etiquetas), separadas por puntos. (www.example.com)
- A la **etiqueta ubicada más a la derecha** se le llama dominio de nivel superior (top level domain, TLD).
- **Cada etiqueta a la izquierda** especifica una subdivisión o subdominio. En teoría, esta subdivisión puede tener hasta 127 niveles, y cada etiqueta puede contener hasta 63 caracteres, pero restringidos a que la longitud total del nombre del dominio no exceda los 255 caracteres.
- **La parte más a la izquierda** expresa el hostname. Suele ser el nombre del servicio que ofrecen.

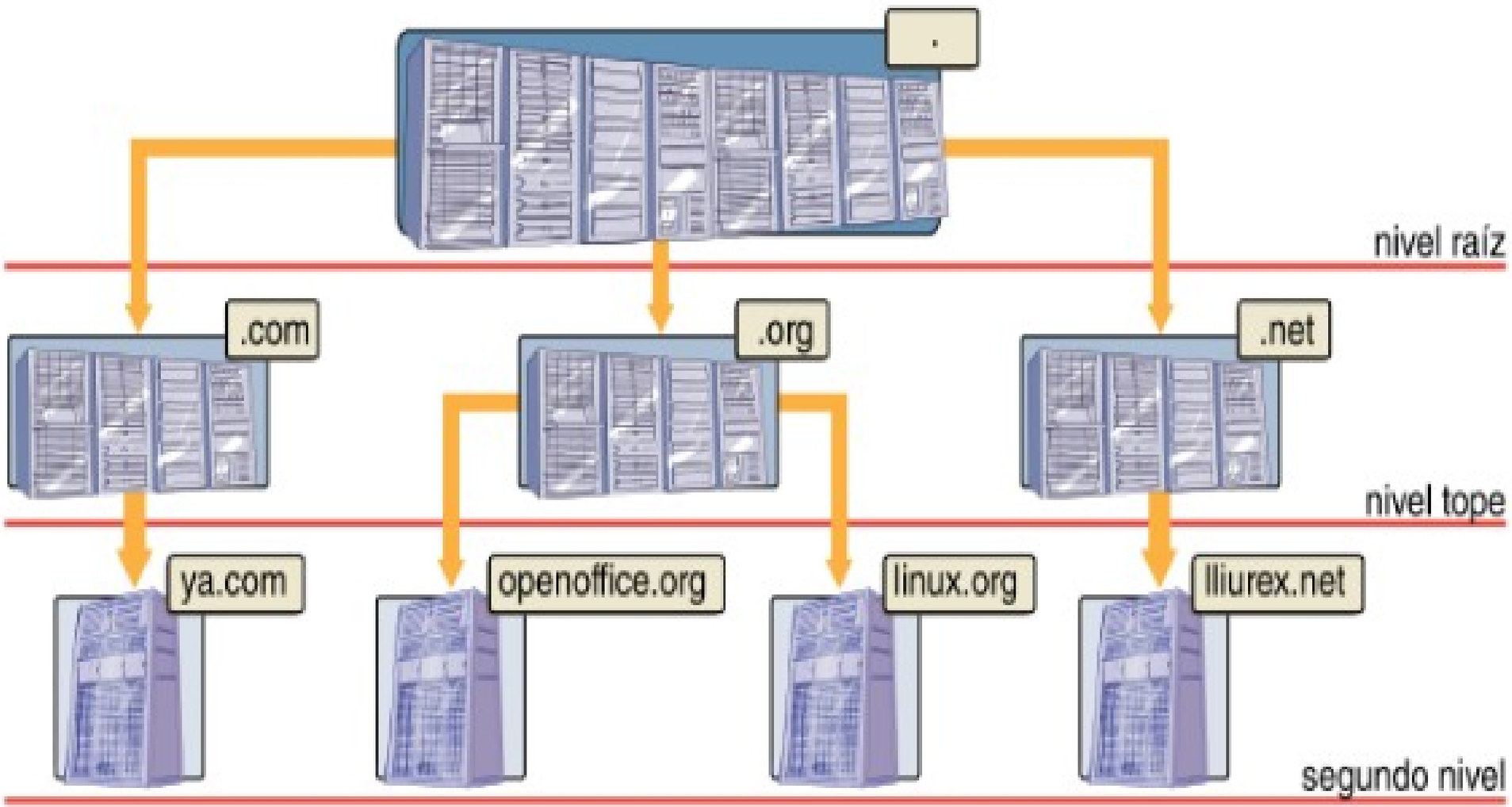
ESPACIO DE NOMBRES DE DOMINIO

- El servicio DNS se compone de una **base de datos distribuída** (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,** aunque calculando llegan a 127 **((255-3)/2)+1=127**.

ESPACIO DE NOMBRES DE DOMINIO

- Normalmente llegan **hasta 5 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 sub-árboles que integran el árbol** o espacio de nombres de dominio.

ESPACIO DE NOMBRES DE DOMINIO



TOP LEVEL DOMAIN

- Los TLDs (Top Level Domain) son los **dominios de primer nivel**. Son los que representan el texto después del último punto de un dominio. Ej: El TLD de www.google.es es **.es**
- Indican la actividad a la que pertenecen, determinan el carácter de la entidad o su ubicación.
- Se llaman así porque reflejan el nivel más elevado de categorización de un nombre en Internet.
- Es el eslabón más alto de la jerarquía de la red.
- Los dividimos en: **Genéricos y de país.**

REGISTRO DE DOMINIOS

- La ICANN (Internet Corporation for Assigned Names and Numbers) o Corporación para la Asignación de Nombres y Números de Internet es una corporación sin ánimo de lucro encargada de la gestión de los dominios.
- En 1998: IANA (Internet Assigned Numbers Authority) + InterNIC (Internet Network Information Center) = ICANN
- El registro de sus dominios era gestionado por Network Solutions . Inc hasta que fue privatizado en noviembre de 1999.

REGISTRO DE DOMINIOS

- DATOS PARA REGISTRAR UN DOMINIO:
- **Registrante o titular (Registrant)**
- **Contacto Administrativo (Administrative Contact)**
- **Contacto técnico (Technical Contact)**
- **Contacto de Pago (Billing Contact)**
- **Duración**
- **Servidores DNS:** Nos van a indicar como mínimo dos servidores donde se encuentran los registros del dominio.
- NOTICIA

REGISTRO DE DOMINIOS

- Tres tiempos que afectan a los servidores:
- **Tiempo de actualización (refresh): Cada cuánto tiempo el servidor secundario** obtiene o copia la información de las zonas de un servidor primario.
- **Tiempo de reintentos (retry): Si el servidor primario está caído cada cuánto tiempo** se va a reintentar obtener o copiar la información de las zonas.
- **Tiempo de caducidad (expire): Si el servidor primario sigue caído durante este** tiempo la información de zonas se borrará del servidor secundario.

DOMINIOS Y ZONAS

- **Los registros DNS se organizan en zonas:** cada zona coincide con un dominio (o subdominio) o un rango de direcciones IP (ya que generalmente se proveen direcciones IP en rangos consecutivos).
- El servidor de nombres tiene autoridad sobre la zona.
- La zona en realidad es un archivo que contiene determinados registros de la base de datos del espacio de nombres de dominio.

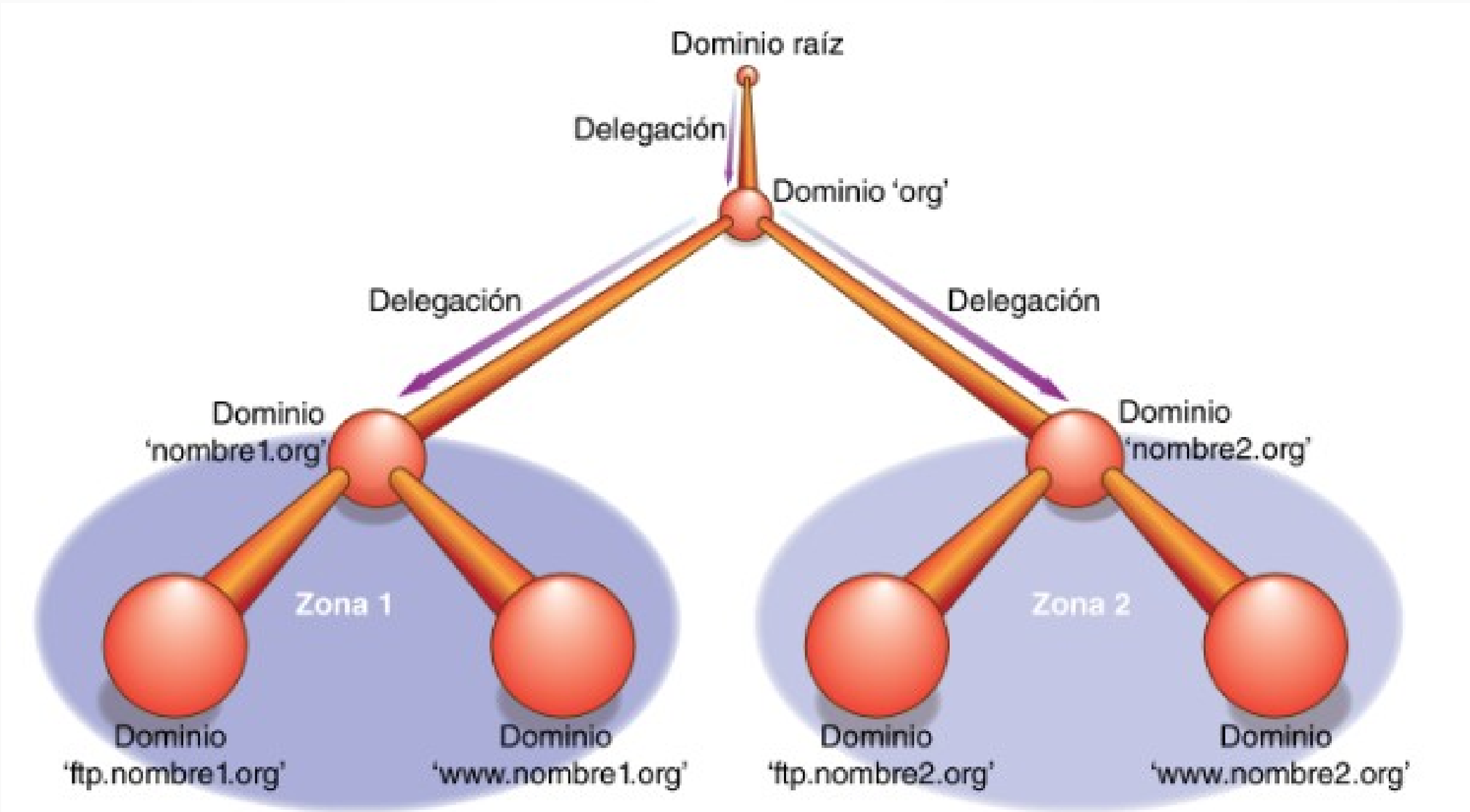
DOMINIOS Y ZONAS

- Estos registros identifican a uno o más dominios.
- Mediante estos registros la zona puede atender a las peticiones de los clientes y por ello también se les llama zonas de autoridad.
- Por lo tanto, la generación de zonas se hace mediante la delegación de autoridad.

DOMINIOS Y ZONAS

- En la siguiente figura se observa que el dominio nombre1.org contiene a su vez los dominios ftp.nombre1.org y www.nombre1.org y, junto con el domino nombre1.org, constituyen la zona1 con autoridad delegada desde el dominio org.
- Lo mismo ocurre con nombre2.org
- → VER DIAPOSITIVA SIGUIENTE

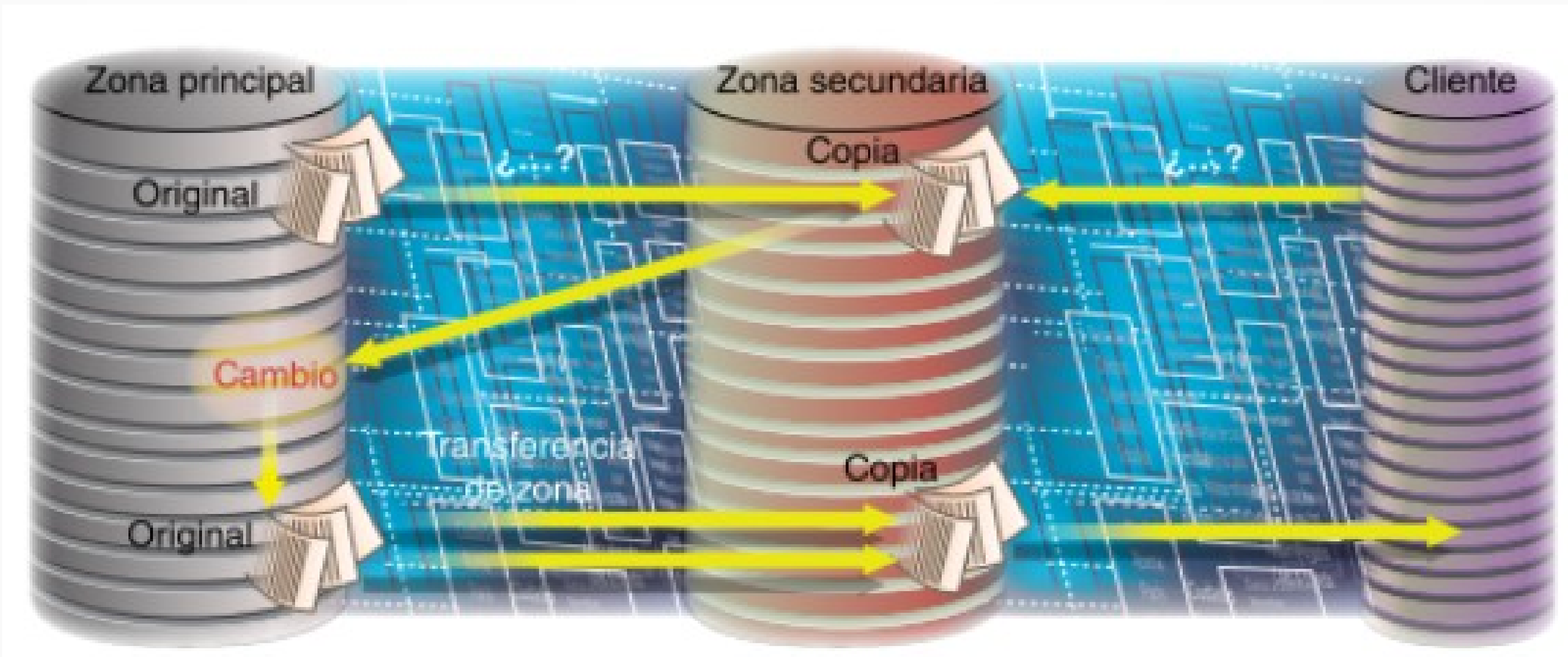
DOMINIOS Y ZONAS



SERVIDORES DE DOMINIO

- **Servidor primario (maestro):** Obtiene la información de sus zonas de sus archivos locales. Todas las modificaciones sobre una zonas se llevan acabo aquí.
- **Servidor secundario (esclavo):** Obtiene la información de sus zonas de otro servidor (primario) que tiene autoridad sobre esas zonas. Contiene una copia de solo lectura de los archivos de zona.
- **Servidor caché:** Solo atiende consultas de los clientes DNS (resolvedores) sobre nombres de dominio. No contiene ningún tipo de información acerca de la zona.

SERVIDORES DE DOMINIO



BASES DE DATOS DEL PROTOCOLO DNS

- Cada servidor DNS mantiene una base de datos y el formato de dichas bases de datos son archivos de texto.
- Para resolver nombres los servidores consultan las zonas, que contienen registros de recursos (RR), que describen la información del dominio DNS.
- Cada registro de recursos tiene este formato:

PROPIETARIO TTL CLASE TIPO RDATA

BASES DE DATOS DEL PROTOCOLO DNS

- La descripción de los campos de los RR es:
  - **Propietario:** nombre de máquina o dominio DNS a la que pertenece el recurso.
  - **TTL (Time To Live):** tiempo de vida, en segundos, del registro en la caché.
  - **Clase**: familia de protocoles en uno. Suele tomar IN de internet.
  - **Tipo**: varía en función del campo clase.
  - **RDATA:** información específica del tipo de recurso. Por ejemplo, para un registro clase IN y tipo A este campo especifica una IP.

TIPOS DE REGISTRO

Nombre de recurso	Tipo de registro	Función
Inicio de autoridad	**SOA**	Identifica al servidor autoritario de una zona y sus parámetros de configuración.
Servidor de nombres	**NS**	Identifica servidores de nombres autorizados para una zona.
Dirección	**A**	Asocia un nombre de dominio FQDN con una dirección IP.
Puntero	**PTR**	Asigna una dirección IP a un nombre de dominio completamente cualificado. Para las búsquedas inversas.
Registro de correo	**MX**	Indica máquinas encargadas de la entrega y recepción de correo en el dominio.
Nombre canónico	**CNAME**	Permite asignar uno o más nombres a una máquina.
Text	**TXT**	Almacena cualquier información.
Servicio	**SRV**	Ubicación de los servidores para un servicio.

TIPOS DE REGISTRO

```
a) actividades.net.  IN A 68.67.66.65
b) actividades.net.  IN NS ns1.serversuniv.com
```

a) `IN` significa Internet

`A` es el registro de dirección

Por tanto, la línea indica que la dirección IP para el dominio actividades.net es `68.67.66.65`

b) `IN` significa Internet.

`NS` indica que el tipo de registro es un registro de servidor de nombres

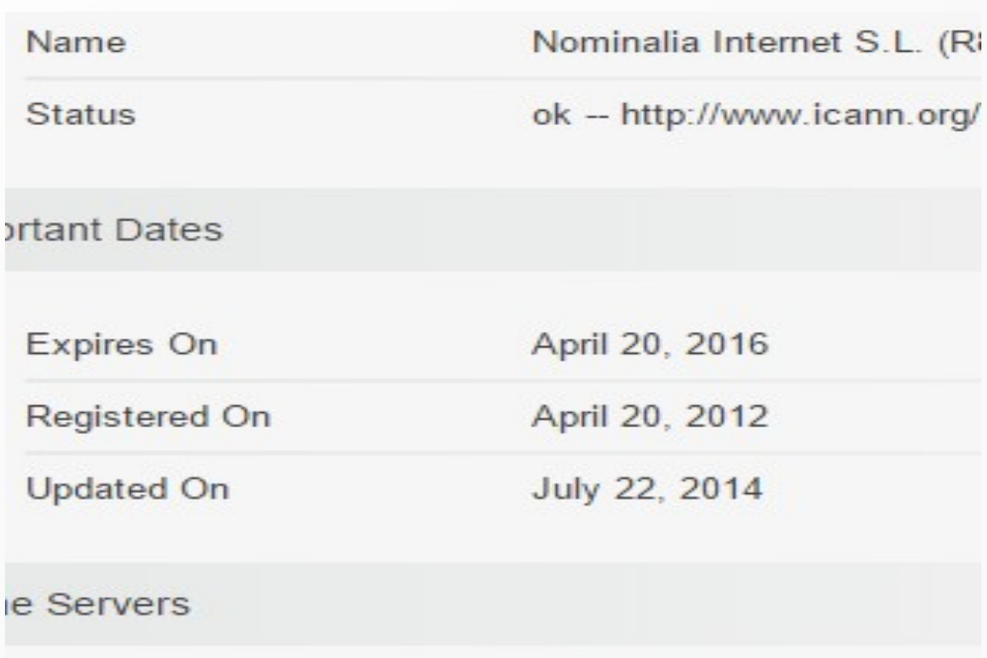
Por tanto, la línea indica que ns1.serversuniv.com es el servidor autoritario para el dominio `actividades.net`

```
s0.test.com        IN MX 0 s0.test.com
                      IN MX 2 s1.test.com
                      IN MX 4 s2.test.com
```

Indica que el servidor de correo será elegido por prioridad. Primero accederá a `s0.test.com` y, si no puede por alguna razón, lo intentará en `s1.test.com`. Si sucede lo mismo lo intenterá, por último, en `s2.test.com`.

WHOIS

- WHOIS es un protocolo basado en petición/respuesta que se utiliza para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio o una dirección IP en Internet.
- WIN: who.is
- LINUX: install whois



Name	Nominalia Internet S.L. (R
Status	ok -- http://www.icann.org/
ortant Dates	
Expires On	April 20, 2016
Registered On	April 20, 2012
Updated On	July 22, 2014
e Servers	

NSLOOKUP

- Es una herramienta que perite consultar un servidor de nombres y obtener infromación relacionada con el dominio o el host y así diagnosticar los eventuales problemas de configuración que pudieran haber surgido en el DNS.
- En definitiva, es para saber si el DNS está resolviendo correctamente los nombres y las Ips.
- MODO NORMAL: nslookup [-opcion][host][servidor]
- MODO INTERACTIVO: nslookup

DIG

- Permite realizar consultas sobre servidores de DNS, pero a diferencia de nslookup, solo funciona para Linux.
- Dig <@servidor>[opciones][nombre][tipo]

Pero podéis preguntar a DNS específicos (para ver si hay DNS poisoning o spoofing) o por registros específicos. Os pongo algunos ejemplos:

- *dig @8.8.8.8 smythsys.es* Realiza la consulta al servidor de Google 8.8.8.8
- *dig MX @8.8.8.8 smythsys.es* Pregunta por el registro MX. Puedes hacerlo en el que queramos ANY, NS, A, MX, SIG,SOA...
- *dig ANY smythsys.es* Consulta (en este caso en local) TODOS los registros.
- *dig +trace @8.8.8.8 smythsys.es* MUY útil porque te muestra todos los pasos que sigue hasta recibir la respuesta final.
- *dig -x 8.8.8.8* Para ver el reverse DNS. Otra opción muy usada.

HOST

- El comando Host se usa para encontrar la dirección IP del dominio dado y también muestra el nombre de dominio para la IP dada.
- SINTAXIS: host [-opcion] dominio/ip

-a	**Muetra todos los registros DNS para el hostname dado.**
-C	Muetra los registros SOA y los servidores de nombres autorizados.
-d	Es equivalente a -v.
-l	Lista todos los hosts en un dominio usando AXFR.
-t	Se utiliza para seleccionar el tipo de query. Tipo de Query: CNAME,NS,SOA,KEY etc,.
-W	Especifica cuánto esperar para una respuesta.
-v	El host genera el salida verbose.
-T	Utiliza TCP en vez de UDP para querys al servidor de nombres. Esto está implícito en querys que requieran TCP, como las peticiones AXFR.

ARCHIVO HOSTS

- El archivo hosts de un ordenador es usado por el sistema operativo para guardar la correspondencia entre dominios de Internet y direcciones IP.
- Es un método que usa el sistema operativo para resolver nombres de dominios.
- Antes cuando no había servidores DNS, el archivo hosts era el único encargado de hacerlo.
- Es un texto plano y puede ser editado por el admin.
- Su ubicación depende del SO.

ARCHIVO HOSTS

- USOS:
- Redirigir dominios locales: Es útil para probar páginas web mientras son desarrolladas por los programadores.
- Bloquear contenidos: Podemos bloquear publicidad y páginas web redirigiendo estos lugares.