

DNS

Salvador Mira Gregori
IES Pere Maria Orts



INTRODUCCIÓN

DNS = Domain Name System / Domain Name Service

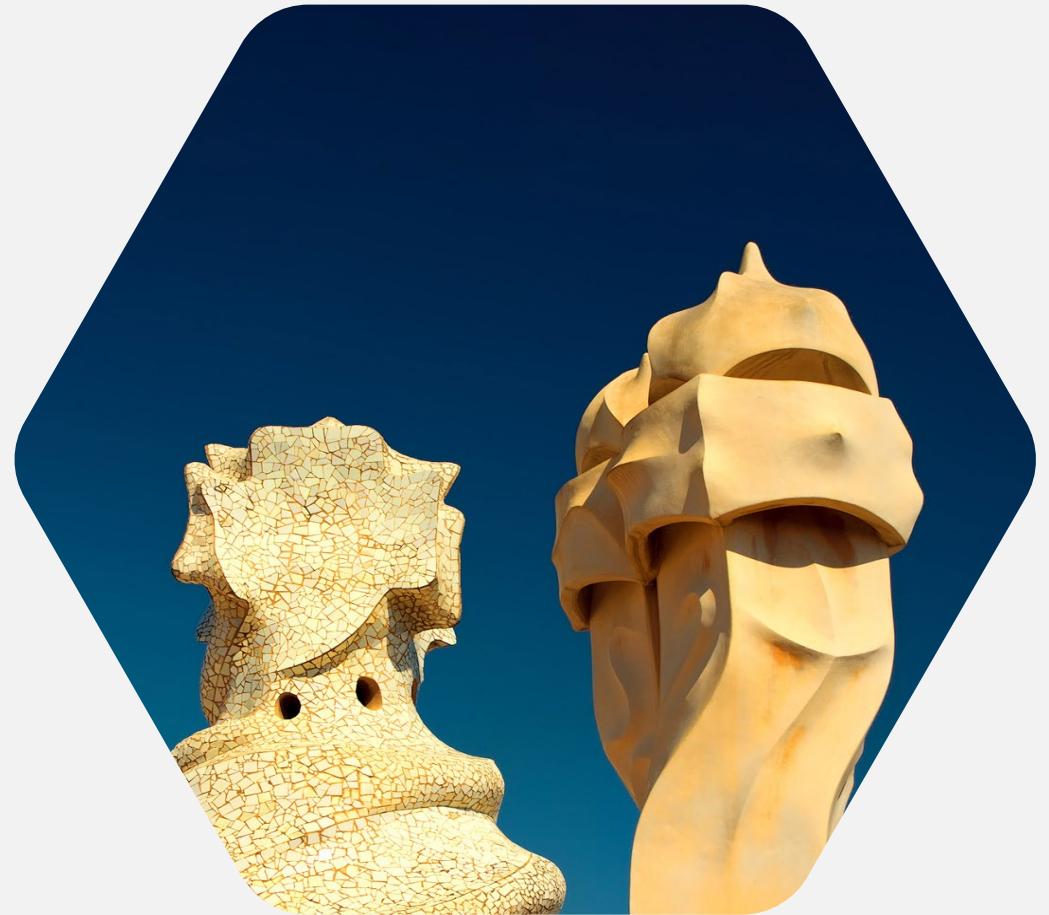
DNS es un servicio de red que convierte entre nombres de red y sus correspondientes IPs

Debemos distinguir entre

- Nombres de dominio: .org .net .qualitypixels.net .google.com
- Nombres de host: pc1, a112, impresora1, ...

Hosts: ordenadores, impresoras, routers, servidores, etc.

Los hosts tendrán un nombre de equipo y al menos una dirección IP



INTRODUCCIÓN

Averiguar servidores DNS configurados

- Windows: **ipconfig /all**
- Linux: **cat /etc/resolv.conf**

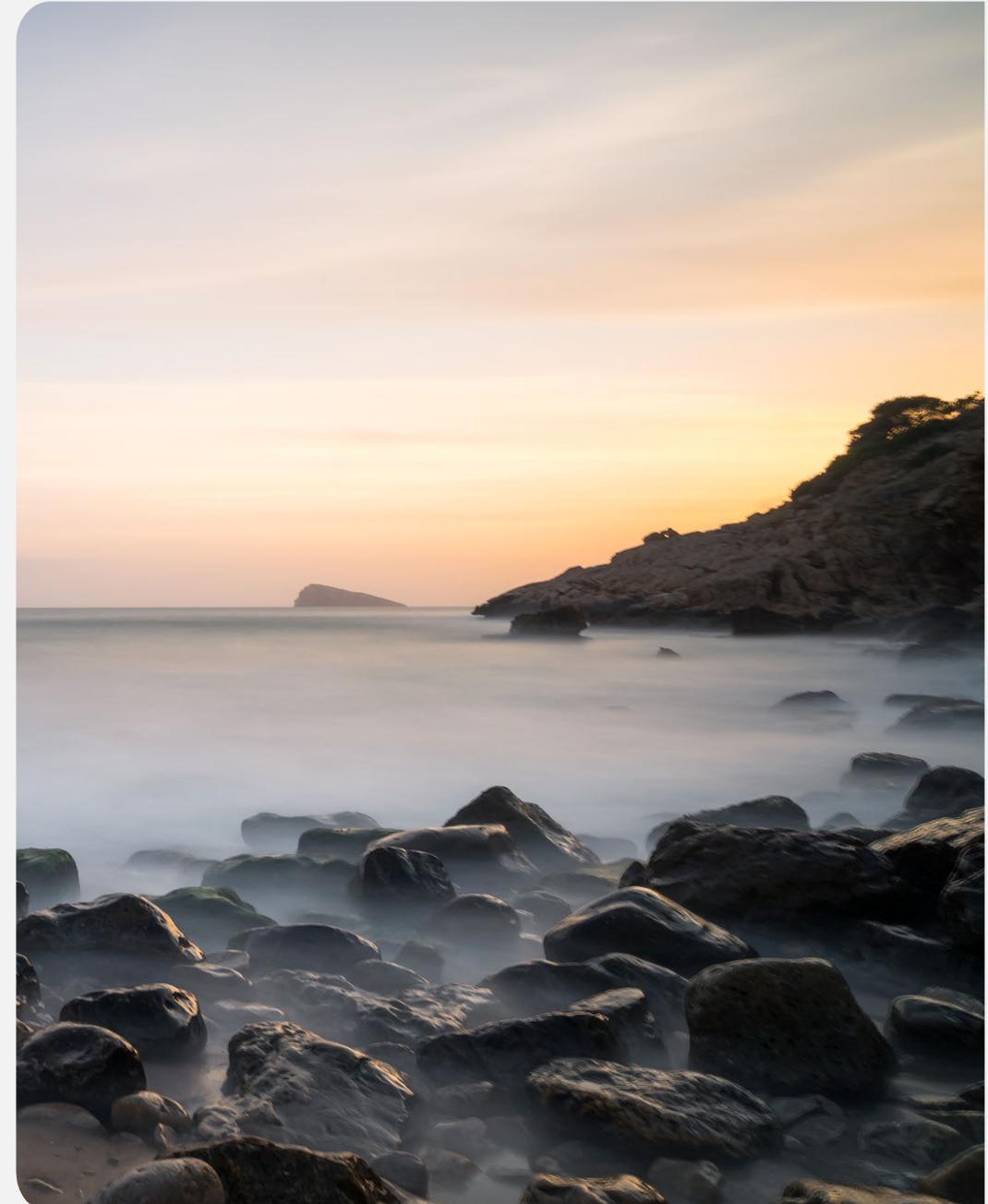
Previamente a existir DNS (1971-72) se usaba un fichero de texto local de asociación de IPs y nombres:
hosts.txt

Se puede seguir usando:

- **/etc/hosts**
- **C:\Windows\System32\drivers\etc\hosts**

El mayor problema es que cada ordenador puede tener una versión distinta del fichero

Primera versión de DNS: 1985



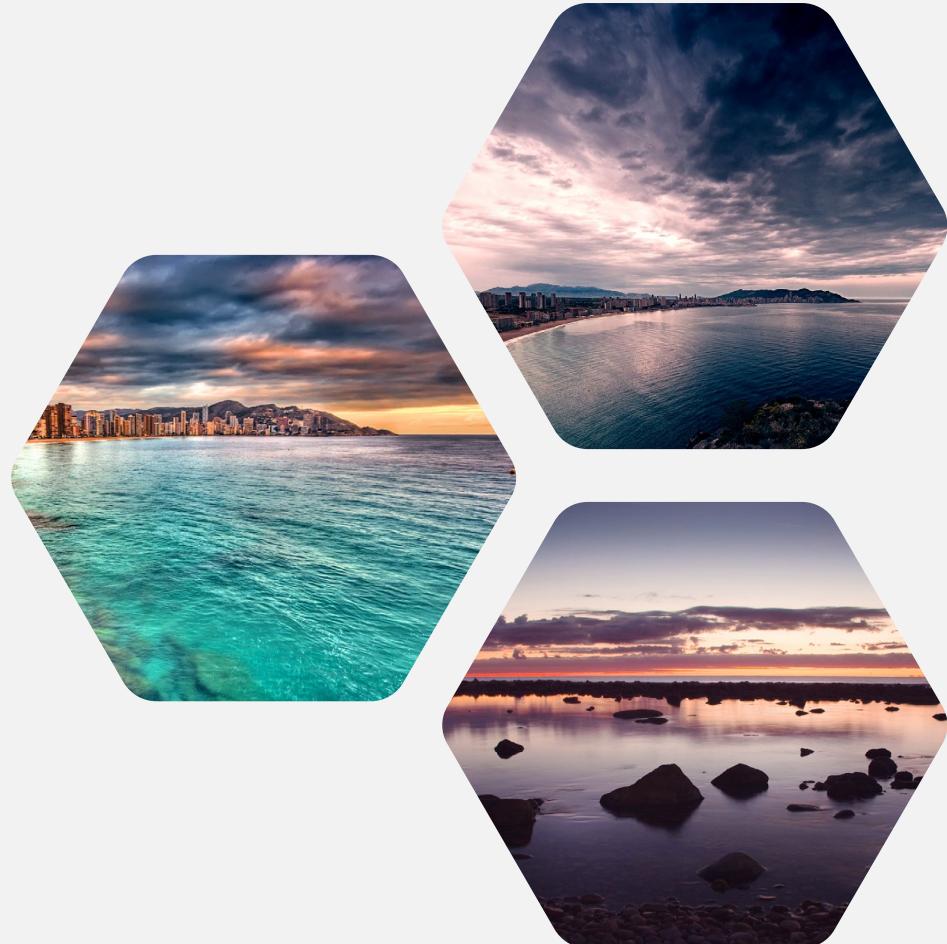
DNS

CONCEPTOS BÁSICOS

DNS es una **base de datos distribuida de nombres e IPs**

Esta base de datos está constituida por **Ficheros de Zonas**

- Cuando un equipo solicita una resolución de nombres, el servidor DNS consultará, en primer lugar, sus ficheros de zonas
- En Linux y usando el servidor bind9, podemos encontrar las zonas configuradas en el lugar indicado en `/etc/bind/named.conf.local`



DNS

CONCEPTOS BÁSICOS

```
:/etc/bind$ cat ./named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "ies.pmo" {
    type master;
    file "/var/lib/bind/ies.pmo.hosts";
};
```

```
:~$ ls /var/lib/bind/ -l
total 12
-rw-r--r-- 1 root bind 414 may 13 08:24 archive.ubuntu.com.hosts
-rw-r--r-- 1 root bind 708 may 16 2013 ies.pmo.hosts
-rw-r--r-- 1 root bind 466 sep  8 19:43 ubuntu.com.hosts
:~$
```

DNS

CONCEPTOS BÁSICOS

```
:/etc/bind$ cat /var/lib/bind/ies.pmo.hosts
$ttl 38400
ies.pmo.      IN      SOA     Serveis2012. administrador (
                                1359278912
                                10800
                                3600
                                604800
                                38400 )
ies.pmo.      IN      NS      Serveis2012.
www.ies.pmo.   IN      A       192.168.90.3
oraculo1.ies.pmo. IN      A       172.17.25.1
oraculo2.ies.pmo. IN      A       172.17.25.2
wsus.ies.pmo.  IN      A       192.168.90.2
web.ies.pmo.   IN      CNAME   www
moodle.ies.pmo. IN      CNAME   www
cisco.ies.pmo. IN      CNAME   www
campus.ies.pmo. IN      CNAME   www
update.ies.pmo. IN      CNAME   wsus
nas1.ies.pmo.   IN      CNAME   oraculo1
nas2.ies.pmo.   IN      CNAME   oraculo2
192.168.0.3.ies.pmo. IN      PTR     www
192.168.0.2.ies.pmo. IN      PTR     wsus
172.17.25.1.ies.pmo. IN      PTR     oraculo1
172.17.25.2.ies.pmo. IN      PTR     oraculo2
ies.pmo.        IN      A       192.168.90.3
ns.ies.pmo.     IN      A       192.168.90.1
sqlserver.ies.pmo. IN      A       192.168.90.4
```

NIVELES DE DNS

Dominio raíz: ":"

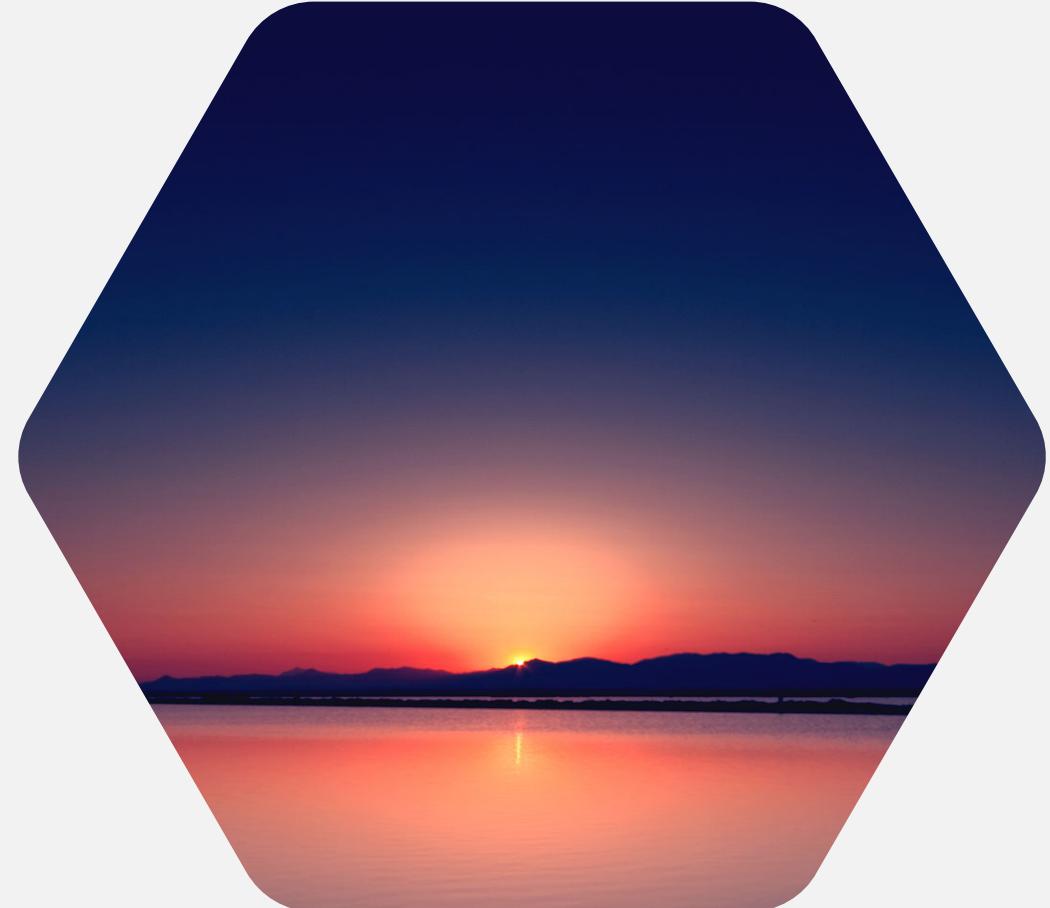
- Se encuentra en primer lugar de la base de datos distribuida de DNS
- Gestionado por los root servers

Dominios de primer nivel: TLD (Top Level Domains)

- Delegado en los servidores encargados de los dominios de primer nivel
- .com, .edu, .net, .org, ...
- .es, .uk, .it, .fr, ...
- .adult, .barcelona, .business, .fashion, ...
- Lista completa en <https://www.iana.org/domains/root/db>

Dominios (y servidores de dominio)

- Subdominios de un nivel anterior
- yahoo.com, Instagram.com, ...



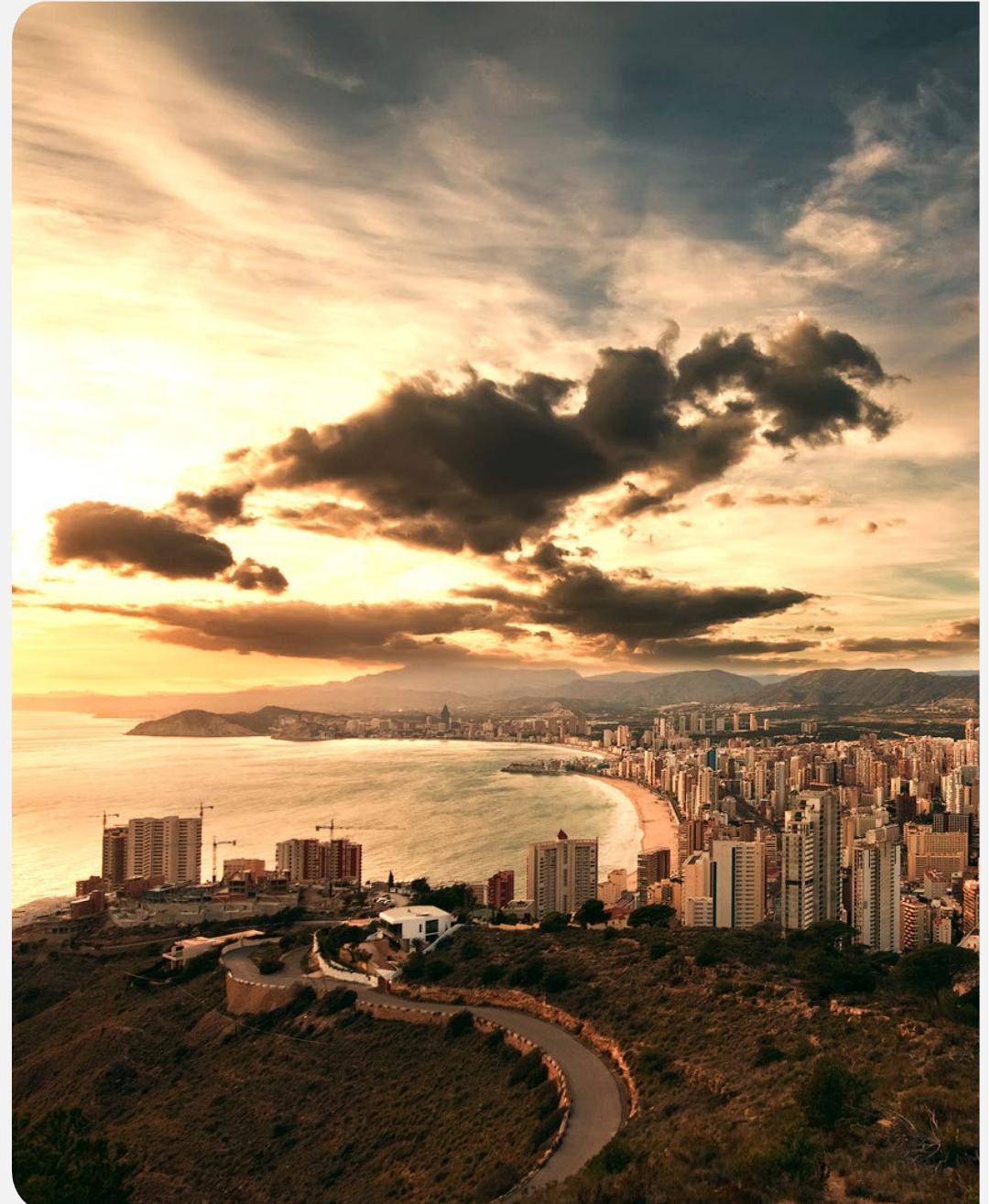
NIVELES DE DNS

Los **servidores raíz** (root servers) **conocen** quienes son los **servidores TLD** y cuáles son sus direcciones IP

Los **servidores TLD** **conocen** a los **servidores DNS** de sus **subdominios** y cuáles son sus direcciones IP

Nombres de dominio totalmente cualificados: FQDN

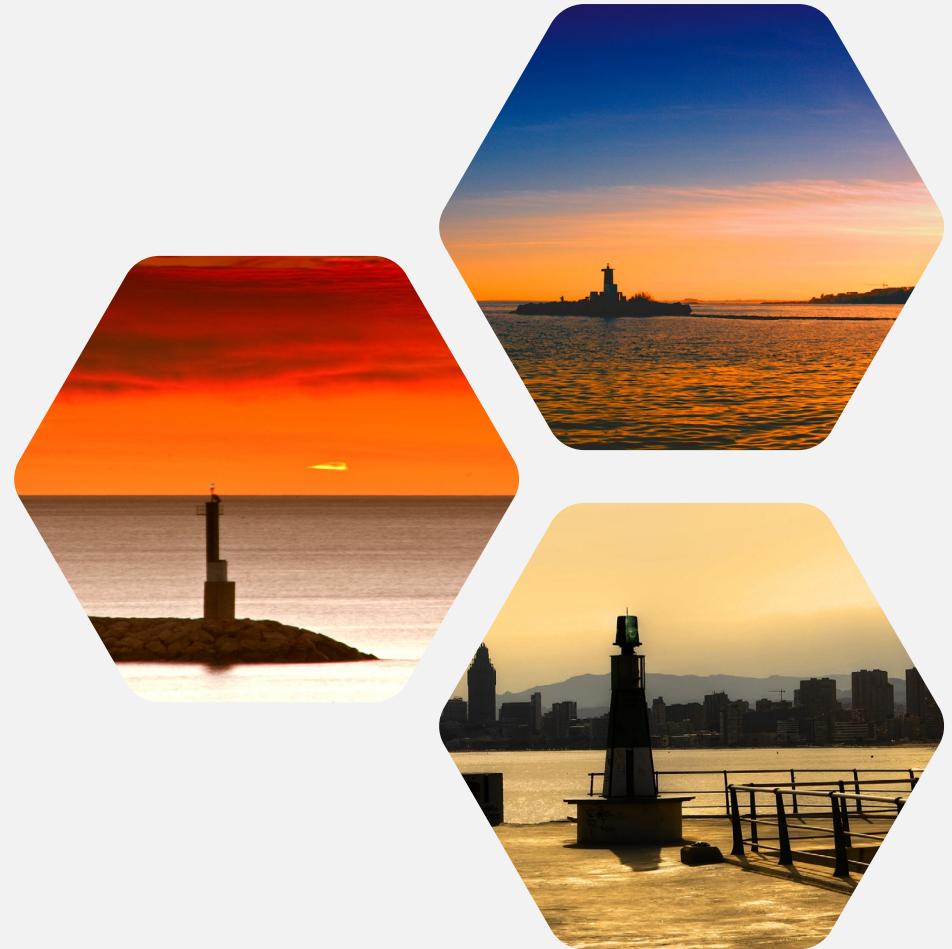
- Compuestos por el **nombre de host**, el **nombre de los subdominios**, el **nombre del TLD**, y **acabado en punto**
- Cada parte se separa por un punto de la siguiente parte, y cada **dominio acaba en punto** (representación de los root servers)
- Ej **www.yahoo.com.**, **mail.google.com.**, **smtp.iesperemaria.com.** ...
- **www**, **mail**, y **smtp** corresponden a nombres de host dentro de sus dominios correspondientes



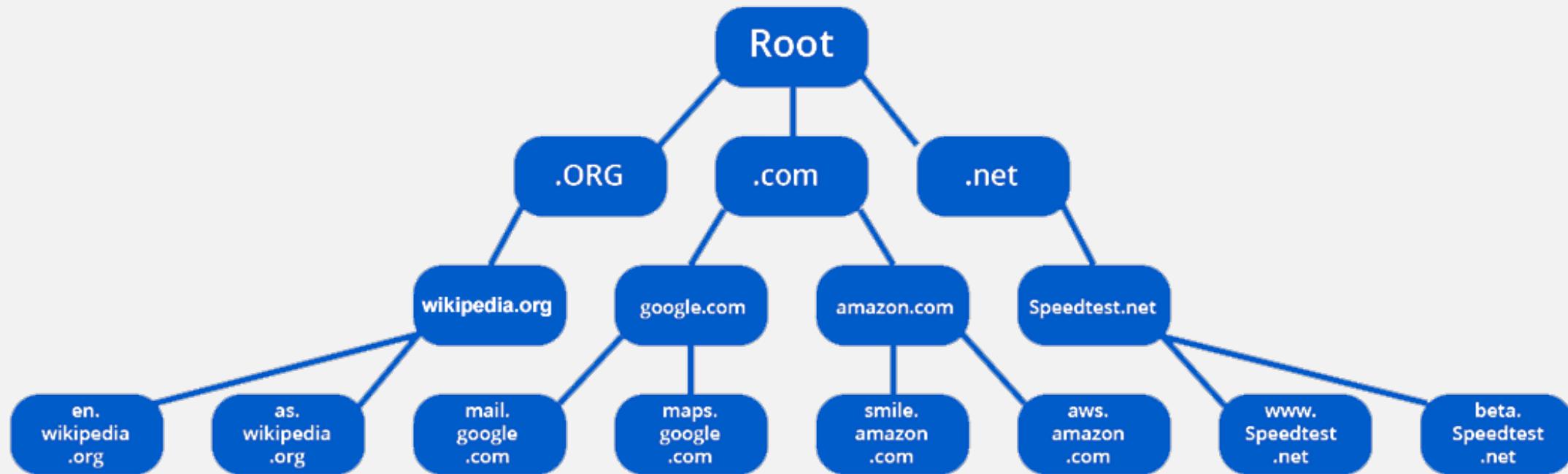
NIVELES DE DNS

Tomando como ejemplo `smtp.iesperemaria.com`.

- Los **root servers** conocen dónde están los **servidores** que gestionan el **TLD .com**
- Los servidores **TLD de .com conocen** dónde está el **servidor** de nombres en el que se define el dominio `iesperemaria.com`.
- El **servidor DNS** en que tiene la **autoridad** sobre `iesperemaria.com`. conoce de las IPs de todos sus hosts, entre ellos el host `smtp.iesperemaria.com`.
 - Esta información la tiene en un **archivo de definición de zona**



NIVELES DE DNS



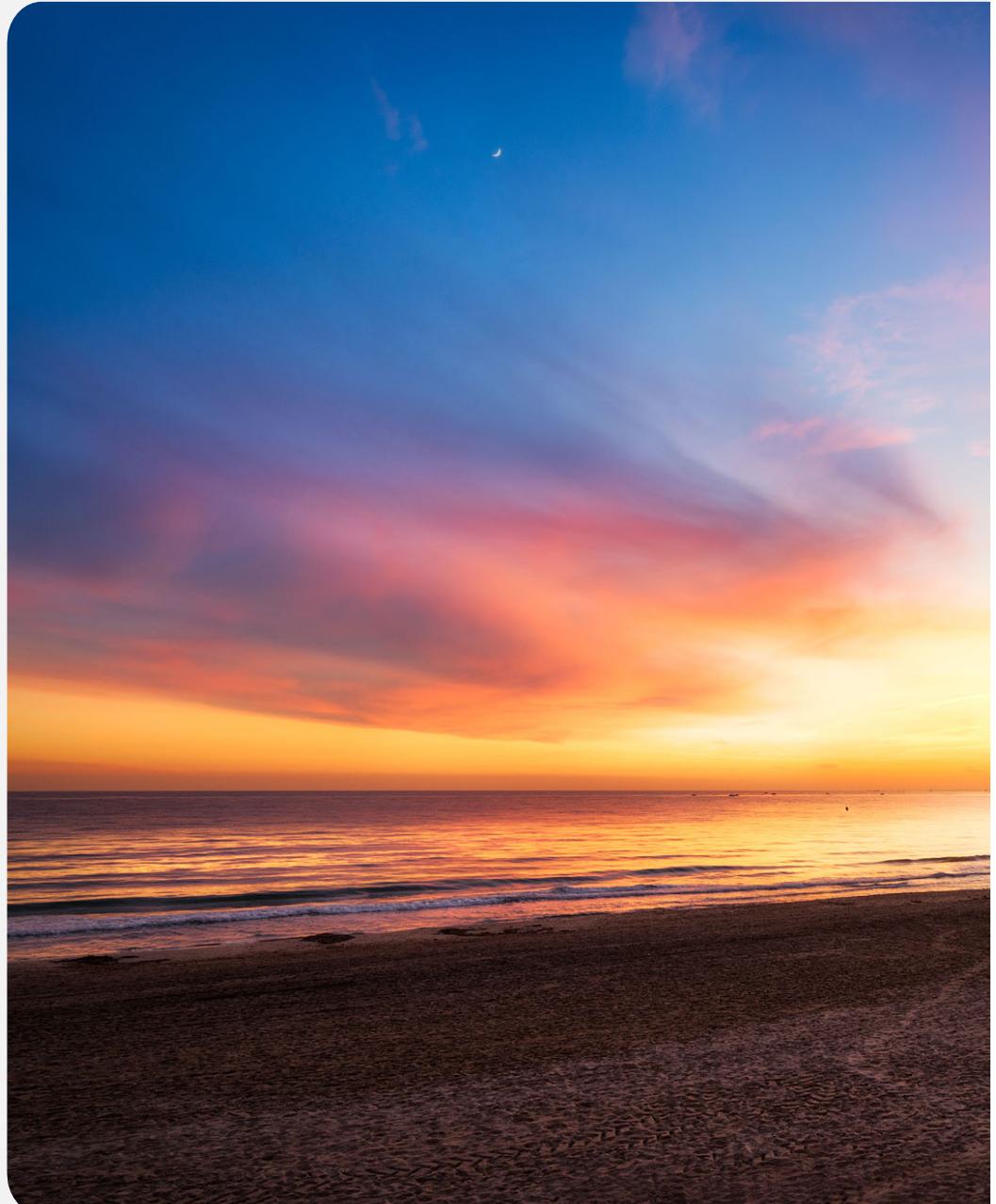
BÚSQUEDAS DNS

Los equipos conectados a una red IP deben conocer un servidor DNS que hará el proceso de resolución de nombres

- Los equipos son clientes DNS
- Mantienen su propia caché de DNS para maximizar la velocidad

Las situaciones típicas respecto a los servidores DNS configurados en los clientes son:

- Los **DNS servers** pertenecen al mismo dominio que nuestro equipo
- Los **DNS servers** son de un ISP
- Los **DNS servers** son sólo una **caché de DNS**



BÚSQUEDAS DNS

El cliente lanza **peticiones recursivas** a sus servidores DNS

Una **petición recursiva** indica al siguiente de la cadena que debe continuar la consulta hasta:

- Resolver la dirección completamente
- Determinar que el nombre no existe en la red

Si el servidor DNS conoce la IP correspondiente al nombre la devolverá

- En caso contrario, lanzará una búsqueda que podrá ser iterativa o recursiva
- Normalmente, los servidores DNS harán búsquedas iterativas



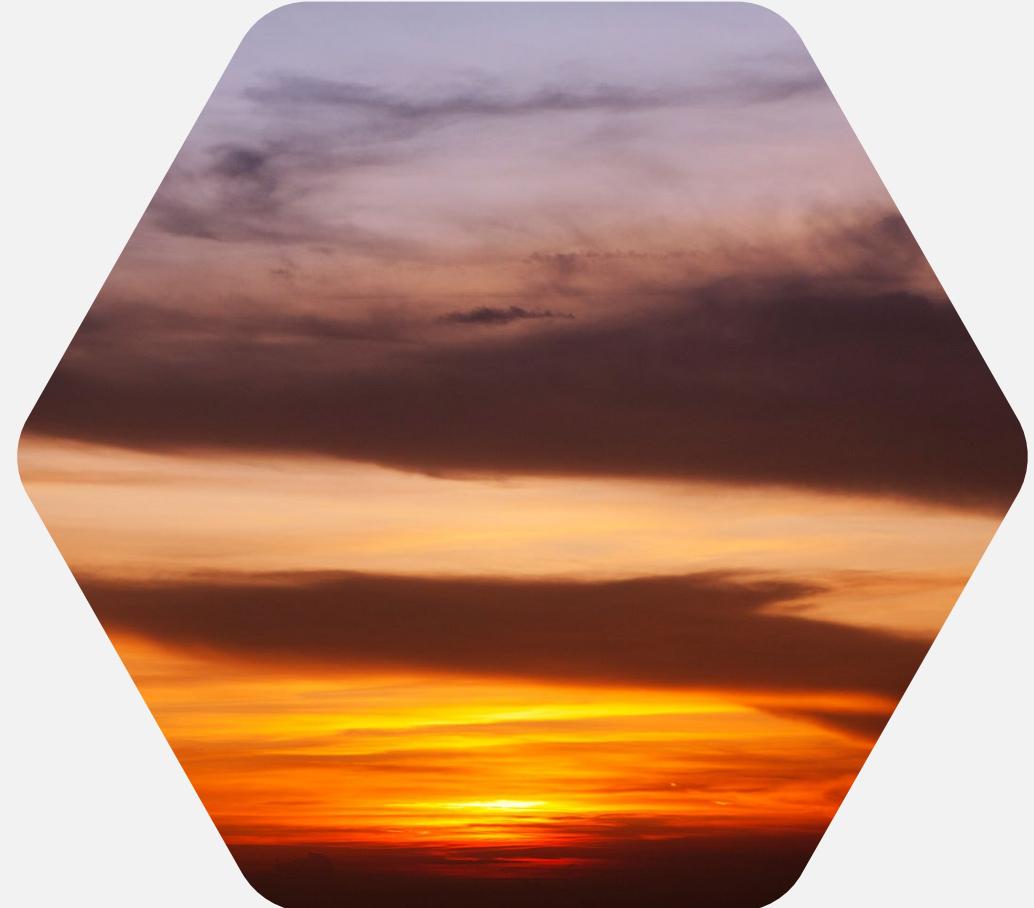
BÚSQUEDAS DNS

EJEMPLO

Supongamos que queremos resolver la dirección IP de www.yahoo.com., y que esta sea supuestamente 72.30.2.43

Por otra parte, supongamos también que en nuestra configuración de red, el **servicio de DNS** nos lo proporciona nuestro **ISP**, y que esta sea 10.5.1.8

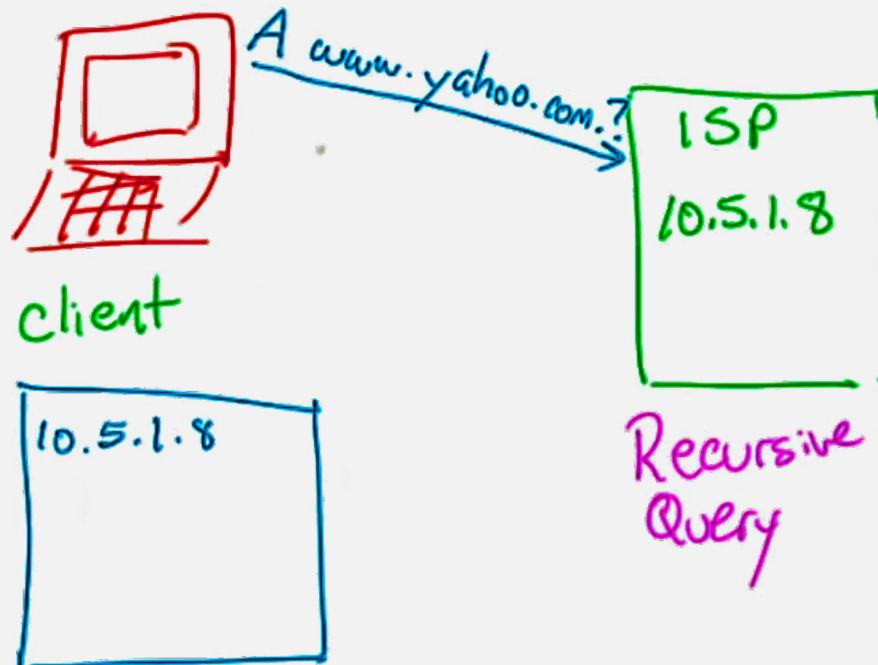
En primer lugar, **el cliente consulta su caché**, y si la dirección no está allí, lanzará una **búsqueda recursiva al servidor DNS en el ISP**



BÚSQUEDAS DNS

EJEMPLO

DNS Resolving Host to IP Address
www.yahoo.com → 72.30.2.43



BÚSQUEDAS DNS

EJEMPLO

Si el servidor DNS del ISP no tiene información acerca de [www.yahoo.com.](http://www.yahoo.com), lanzará una consulta a algún root server (búsqueda iterativa), preguntando por www.yahoo.com. En el ejemplo, el root server consultado corresponde con **198.41.0.4**

Como los root servers no tienen información sobre [www.yahoo.com.](http://www.yahoo.com), pero sí información respecto de los TLD de .com, devolverán al DNS server del ISP a qué nuevo servidor o servidores puede consultar

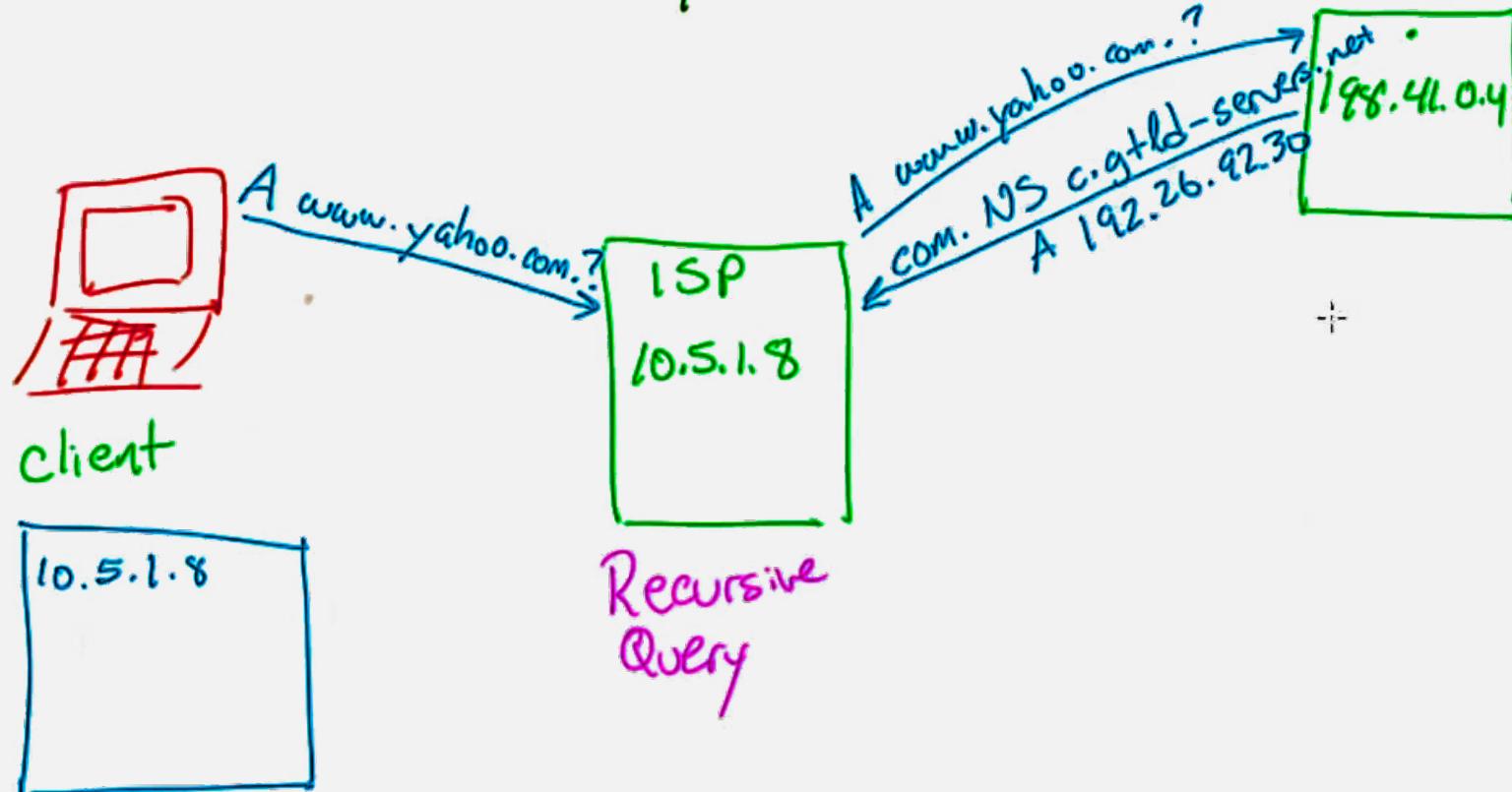
Este nuevo servidor a consultar podrá ser, por ejemplo, [c.gtld-servers.net.](http://c.gtld-servers.net), cuya IP es **192.26.92.30**



BÚSQUEDAS DNS

EJEMPLO

DNS Resolving Host to IP Address
 $\text{www.yahoo.com} \rightarrow 72.30.2.43$



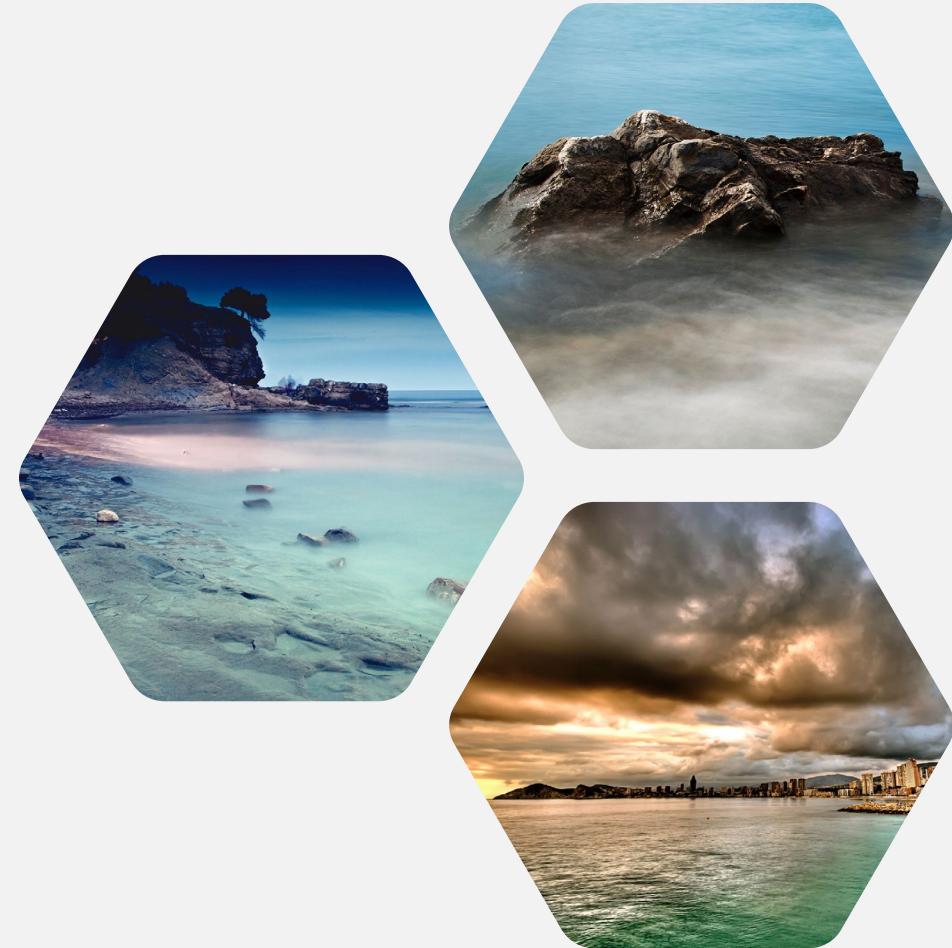
BÚSQUEDAS DNS

EJEMPLO

El servidor **c.gtld-servers.net.** tampoco tiene información sobre la dirección **www.yahoo.com.**, pero al ser un servidor TLD para **.com**, sí que sabrá cuál es el servidor de nombres con autoridad para yahoo.com

En su respuesta al DNS server del ISP le informará sobre este **servidor DNS autoritativo**, al que le preguntará sobre **www.yahoo.com.**

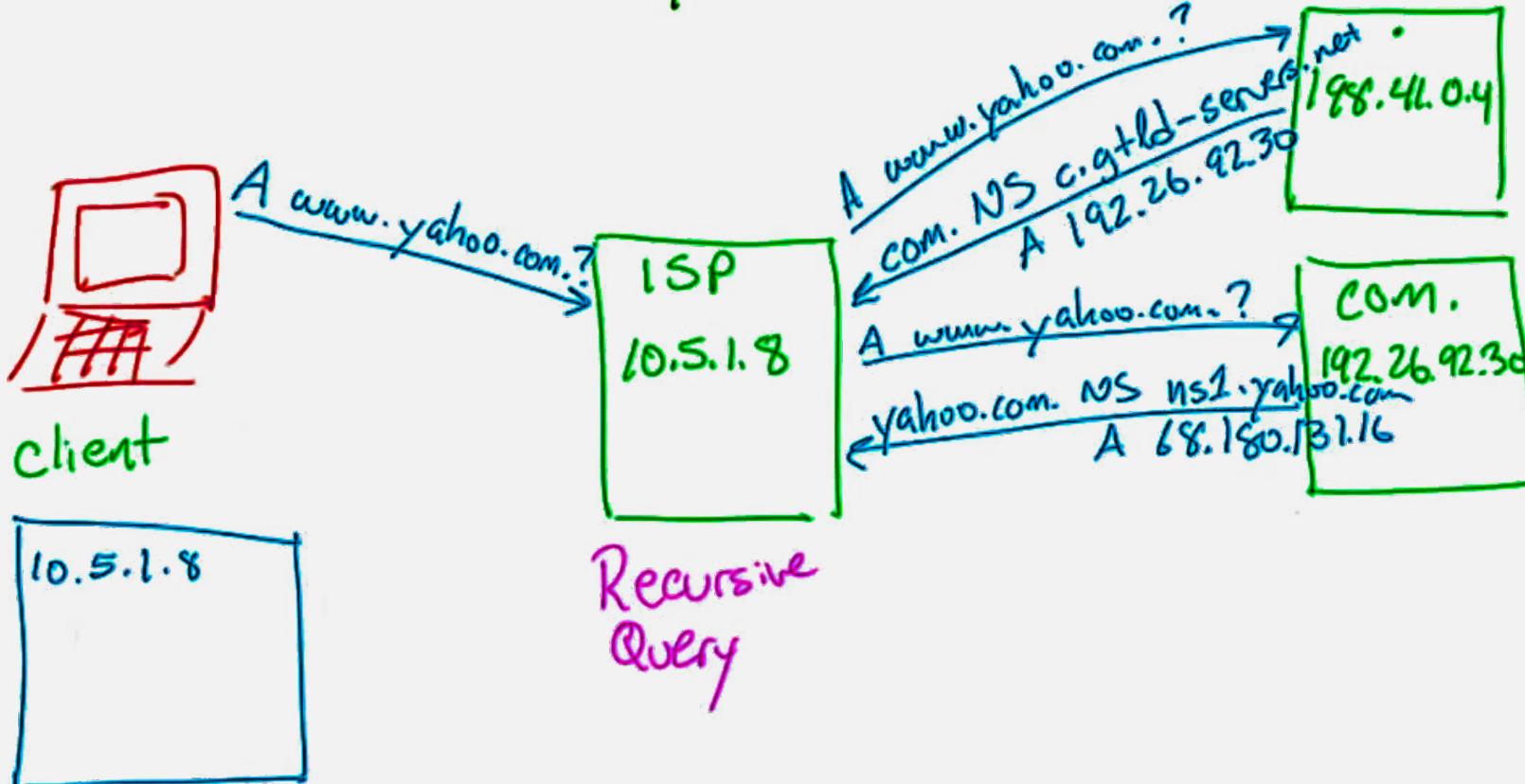
Este servidor autoritativo podría ser, por ejemplo, **ns1.yahoo.com** con la IP **68.180.131.16**, y sí que contendrá información acerca de www.yahoo.com.



BÚSQUEDAS DNS

EJEMPLO

DNS Resolving Host to IP Address
www.yahoo.com → 72.30.2.43



BÚSQUEDAS DNS

EJEMPLO

Cuando el DNS del ISP consulte a ns1.yahoo.com. obtendrá al dirección de www.yahoo.com.

Tras obtener esta dirección, así como todas las direcciones anteriores de los DNS que ha ido consultando, quedará(n) almacenada(s) en la caché

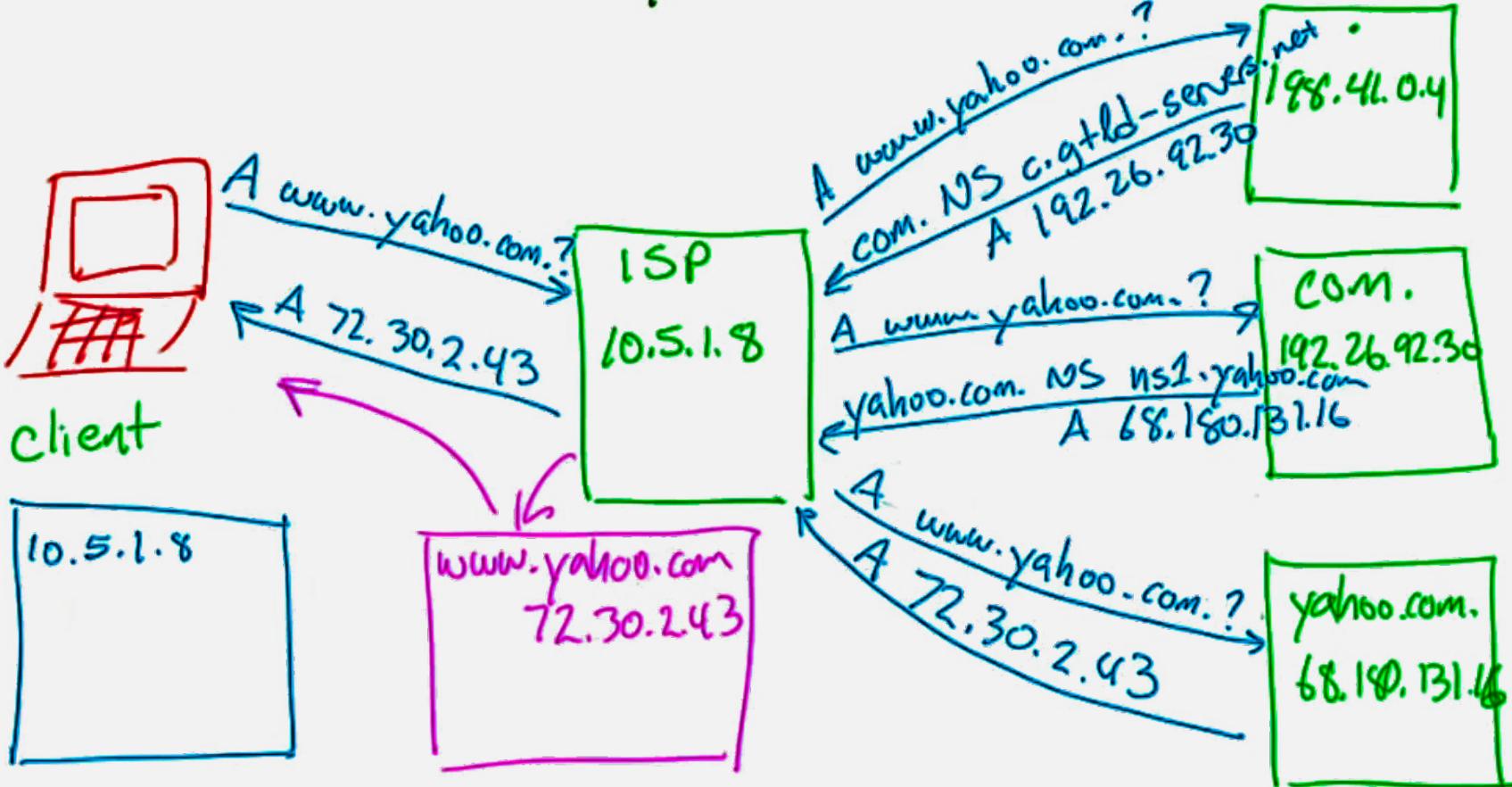
- La próxima vez no hará falta dar tantos pasos para resolver la dirección solicitada



BÚSQUEDAS DNS

EJEMPLO

DNS Resolving Host to IP Address
 $\text{www.yahoo.com} \rightarrow 72.30.2.43$



TIPOS DE REGISTROS DNS

A (A record)

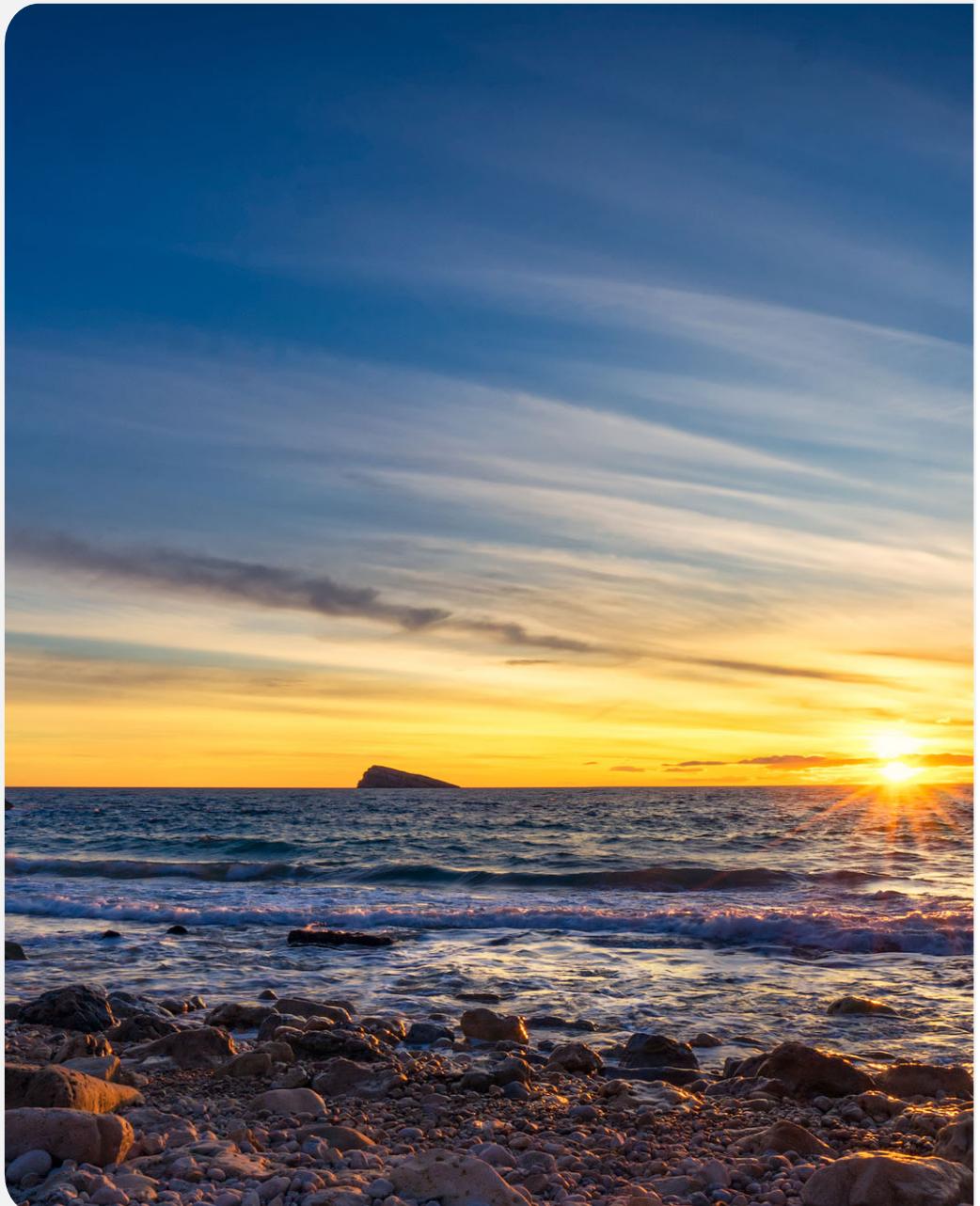
- Asociación de nombre e IP
- Ej. www ↔ 62.75.152.41
- Equivalente en IPv6: registro AAAA

SOA (Start of Authority)

- Indica cuales son los parámetros principales de la zona
- Cada zona solo puede tener un registro SOA

NS (Name Server)

- Identifica el **servidor DNS con autoridad** sobre el dominio
- En el dominio de nivel superior se tiene que tener conocimiento acerca del servidor o de los servidores con autoridad sobre cierto dominio



TIPOS DE REGISTROS DNS

MX record

- Contiene la dirección de un **intercambiador de correo, MTA**



SRV record

- Asocia **nombres con servidores y servicios específicos**
- Algunos protocolos (SIP, LDAP, XMPP,...) requieren este tipo de registros
- Requieren especificar el puerto en el que el servidor escucha para el servicio especificado



CNAME – Canonical Name

- Sirve para definir alias a otros nombres ya definidos

TIPOS DE REGISTROS DNS

TXT record

- Permite asociar un texto arbitrario a un nombre de dominio
- Pueden servir como documentación
- Algunos proveedores los suelen utilizar para verificar la propiedad sobre un nombre de dominio
- Ejemplo: “google-site-verification=rx0xyZounnZasA8Z7oaD3c14JdjS9aKSWvsR1EbUSIQ”

Existen muchos otros tipos de registros, que se pueden consultar en

https://es.wikipedia.org/wiki/Anexo:Tipos_de_Registros_DNS



FORWARDERS

REENVIADORES DNS

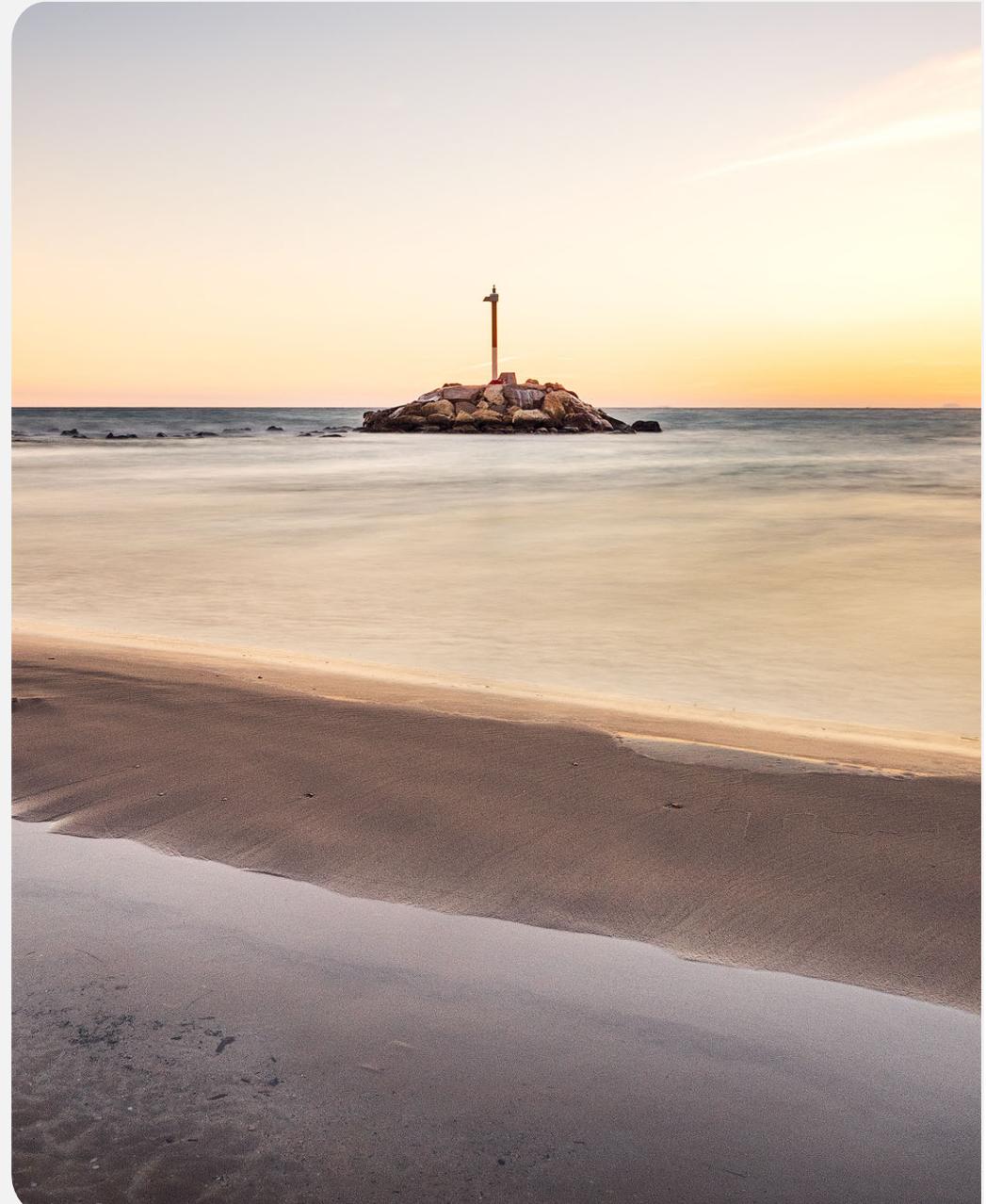
Los servidores DNS pueden funcionar como **reenviadores**:

Pueden ser la autoridad sobre un **dominio local**...

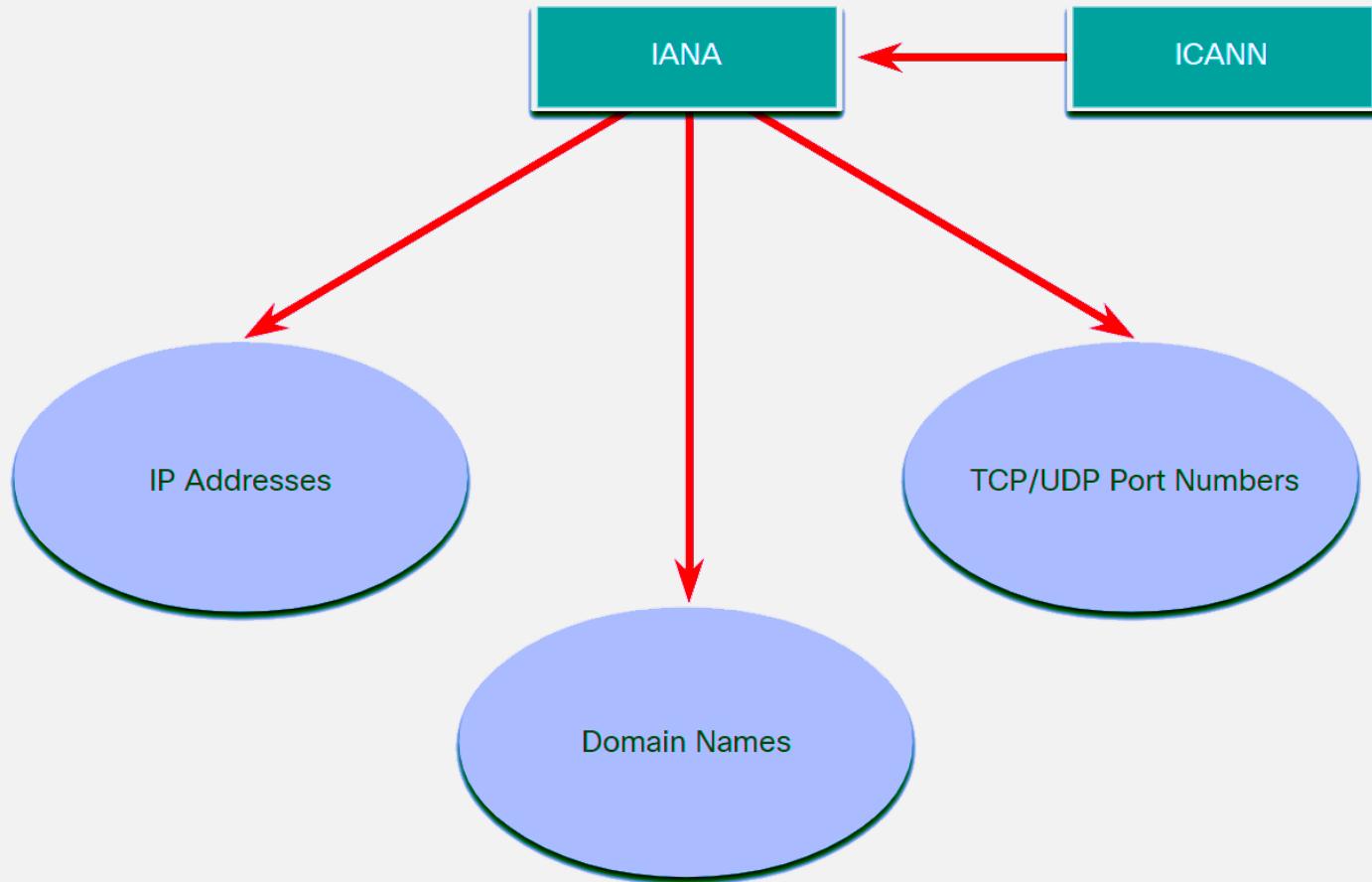
... y **reenviar** todas las **consultas** sobre direcciones que no sean del dominio local a otros servidores

DNS (como clientes), en lugar de hacer la búsqueda iterativa desde los **root servers**

Además, como todo servidor DNS, **mantienen una caché** de las direcciones resueltas



RESPONSABILIDAD SOBRE LOS DNS



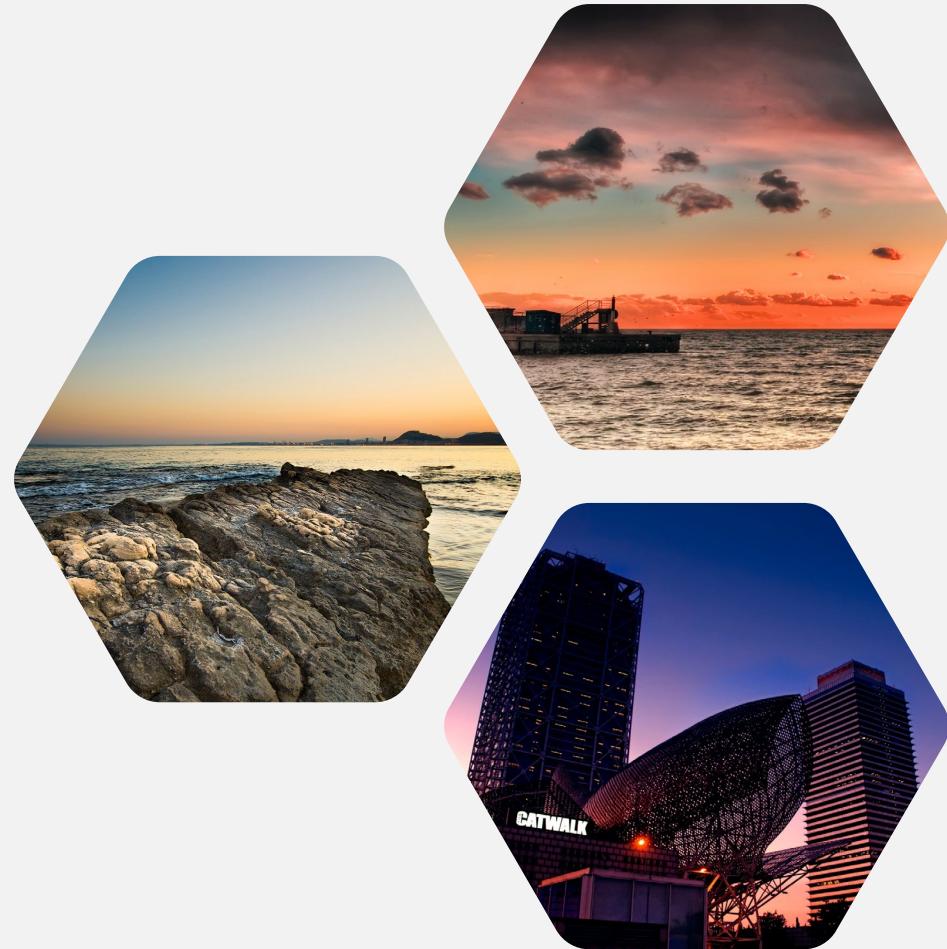
RESPONSABILIDAD SOBRE LOS DNS

Internet Corporation for Assigned Names and Numbers (ICANN)

Es una **organización sin ánimo de lucro**

Se encarga de **asignar las direcciones del protocolo IP**, los **identificadores de protocolo**, la gestión de las funciones del sistema de nombres de dominio y la administración de los **servidores raíz del DNS**

Acredita a los registradores de dominios (**registars**) para los TLDs

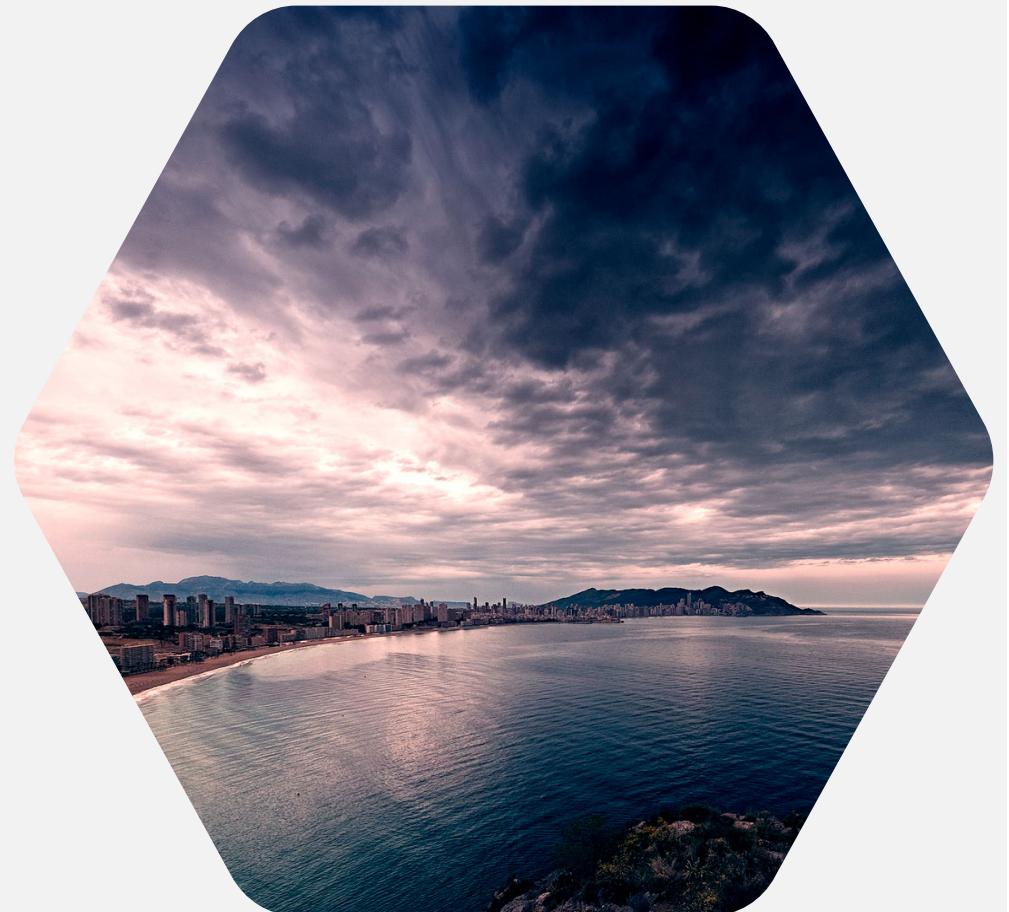


RESPONSABILIDAD SOBRE LOS DNS

IANA: Internet Assigned Numbers Authority

- Mantiene y publica las zonas de los root servers
- Asigna el espacio de nombres de Internet a los registradores (RIRs)
- Supervisa las operaciones sobre los root servers y los registradores en los TLD

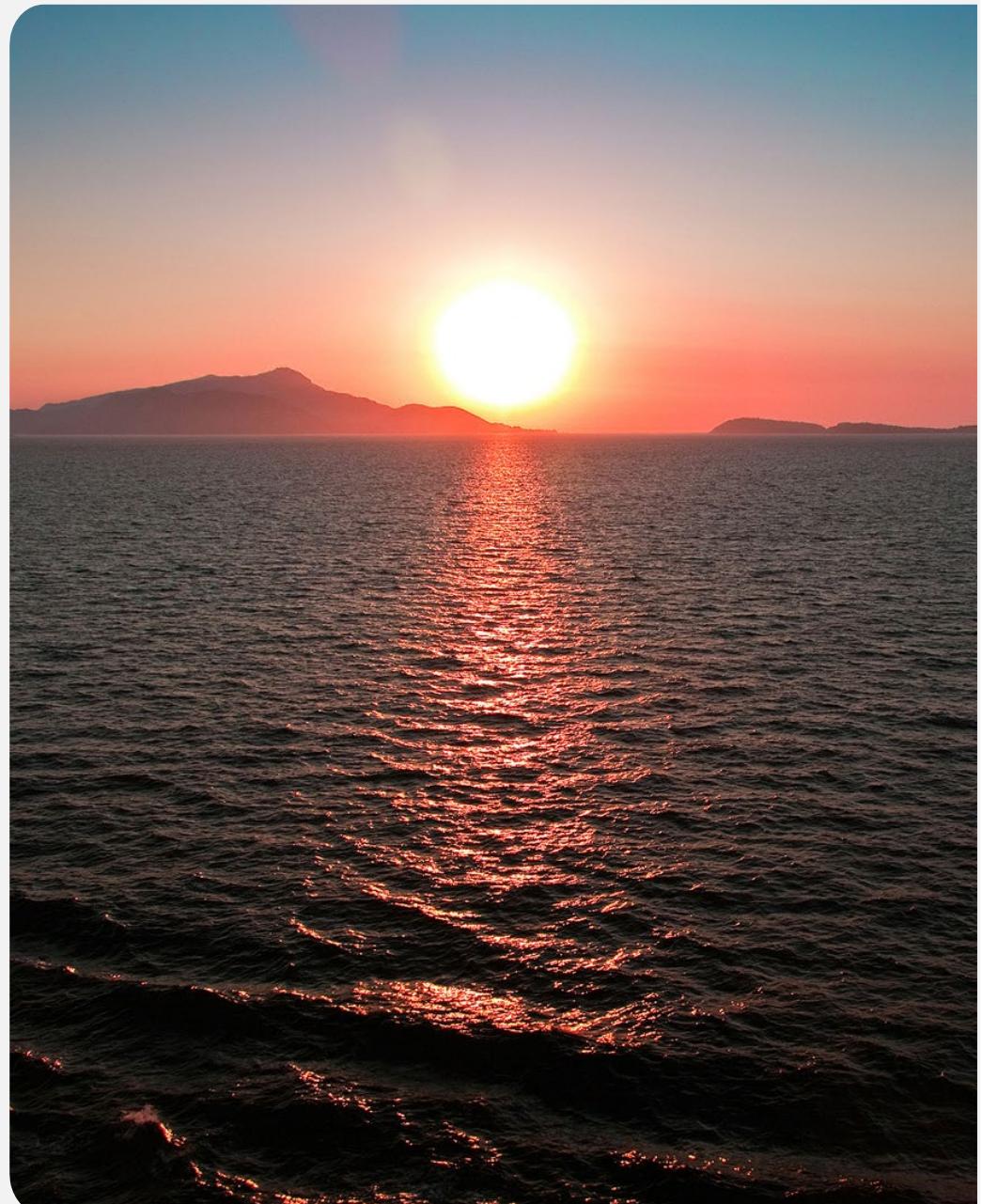
Los registrar deben actualizar todos los servidores de un TLD con las altas, bajas y modificaciones de los servidores de autoridad para los dominios que registran



RESPONSABILIDAD SOBRE LOS DNS

Operadores de los root servers

- 12 operadores
- 13 root servers (distribuidos en muchos sitios)
- Se puede consultar esta información en
<https://root-servers.org/>



DNS INVERTIDO

RESOLUCIÓN INVERSA

El DNS invertido, o resolución inversa, mapea IPs con nombres, al contrario que el DNS "normal"

Utiliza un dominio raíz denominado `in-addr.arpa`

Los registros contienen las direcciones IP escritas en orden inverso, como nombres de host en `in-addr.arpa`.

Estos **registros** son del tipo PTR (punteros)

Ejemplo:

- registro de tipo A: `qualitypixels.net` → `80.58.61.250`
- registro tipo PTR: `250.61.58.80.in-addr.arpa` → `www.somtic.net`



SERVIDORES ESCLAVOS

Los **servidores maestros** (o primarios) son aquellos en los que se permite la configuración y modificación de una zona y sus registros

Los **servidores esclavos** (o secundarios) contienen zonas de solo lectura, que se sincronizan con los servidores maestros

La información se transfiere entre maestros y esclavos a través de la red

