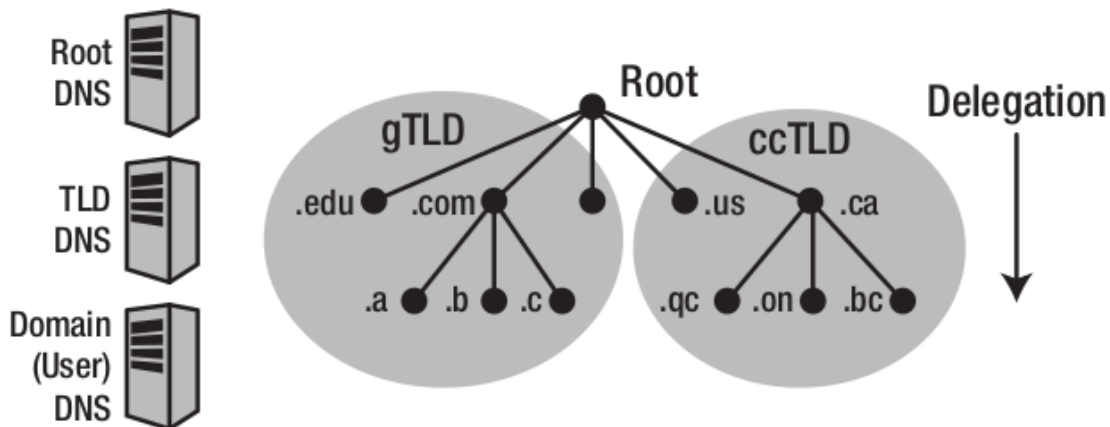


DNS (BIND9)

Bibliografía: <http://fpg.x10host.com/DNS/index.html>

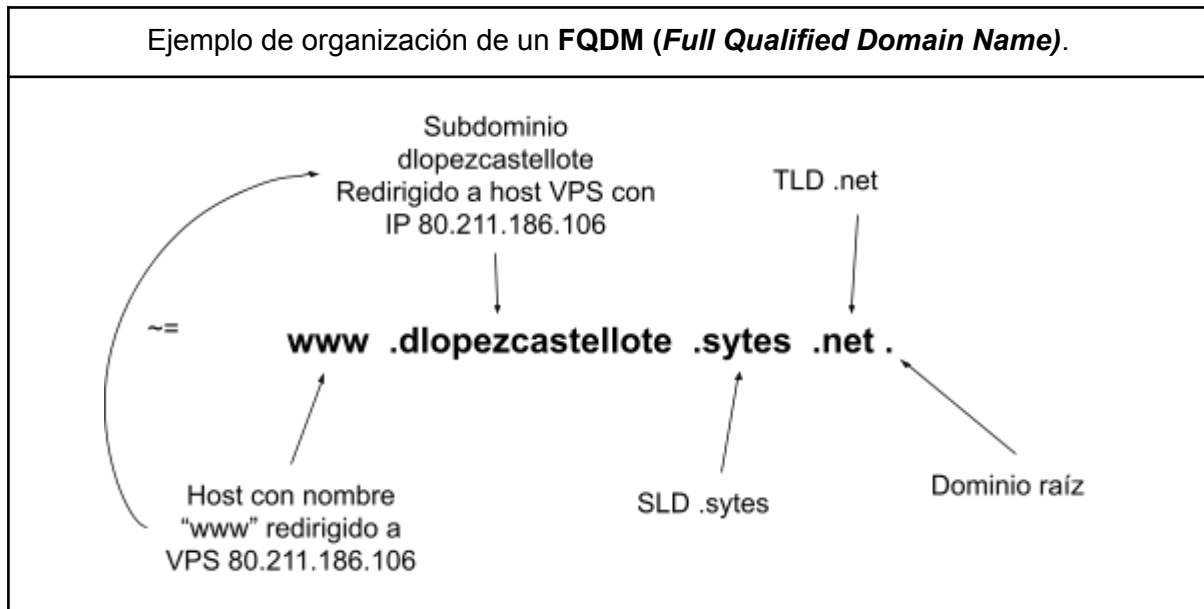
Conceptos generales

Puerto por defecto: 53	Protocolo de transporte utilizado: UDP
------------------------	--



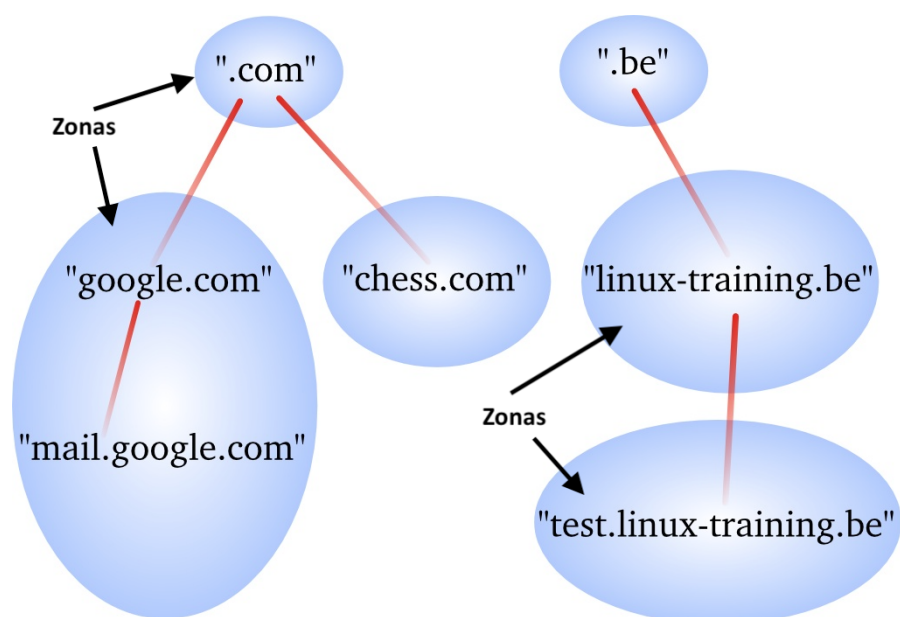
- **Dominio raíz (root).** El "." Es administrado por la ICANN.
 - El dominio raíz es gestionado a través de los **servidores raíz**, que son 13 en total, los cuales son conocidos por todos los otros DNS existentes en el mundo (se definen en un fichero especial de zona en el DNS, donde se indica cuáles son estos servidores, sus IPs, etc).
 - A cada uno de estos DNS raíz (los cuales son en realidad unos 200 servidores en total) se les ha asignado un FQDM (*Full Qualified Domain Name*), que va desde "a.root-servers.net" hasta "m.root-servers.net".
- **TLD (Top Level Domain).** Dominios de primer nivel. Se diferencian:
 - **gTLD** (TLD genéricos). .com, .net, .org, etc. Son administrados por la ICANN. Ejemplo de los .com: "a.gtld-servers.net", ..., "m.gtld-servers.net". Los gTLD tienen una subdivisión:
 - **sTLD (Sponsor TLD).** Son los TLD patrocinados, que permiten representar a comunidades específicas, y deben tener un patrocinador responsable de su administración (ej. .aero, .asia, .museum, .cat, .gal, .eus ...)
 - **ccTLD (Country Code TLD).** Dominios de código de país, como por ejemplo: .es, .us, .uk, .nz... [siempre son 2 caracteres]. La ICANN los **delega** a los países.
- **Autoridad de un dominio:** Es la persona u organización responsable de la explotación y organización del mismo.

- **Delegación de un dominio** (o subdominio): La autoridad de un dominio puede delegar la organización de niveles más bajos del nombre del dominio (típicamente subdominios).
- **Registradores acreditados de dominios**: Organizaciones en las que delega la ICANN responsabilidades limitadas para la venta y administración de trozos de la jerarquía de nombres de dominio.



Concepto de zona

- **Zona**. La organización y administración de un dominio se puede dividir en zonas, donde puede existir un responsable encargado de cada una de ellas.



Ficheros de *hosts* y *nsswitch*

Fichero de *hosts*

Sistema Operativo	Localización
GNU/Linux - Unix	/etc/hosts
Windows XP / 2003 / Vista / 7 / 8 / 10	C:\Windows\System32\drivers\etc\hosts
Mac OS	/private/etc/hosts

Ejemplo (vemos cómo se pueden asignar varios nombres a una misma IP)

```
127.0.0.1      localhost
192.168.1.1    router.asir.com    router
192.168.1.10   www.asir.com      www
```

Fichero */etc/nsswitch.conf*

- Este fichero nos permite buscar cierto tipo de información administrativa (hosts, passwd, group, shadow, networks, etc.), especificando qué fuentes queremos comprobar (qué bases de datos) y en qué orden se harán estas comprobaciones.

Ejemplo del fichero */etc/nsswitch.conf*.

```
passwd:      compat
group:       compat
shadow:      compat
gshadow:     files

hosts:      files mdns4_minimal [NOTFOUND=return] dns
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
```

La línea de **hosts** permite definir el orden en el que se realizarán las búsquedas para la resolución de los nombres de los hosts. En este caso, **primero es *files* (se refiere al fichero */etc/hosts*)**; después *mdns4_minimal [NOTFOUND=return]* (es un protocolo que

permite consultar en una red local las IPs de los equipos de la siguiente forma):

- `ping pc1.local` → si el nombre del equipo es “pc1”, este protocolo realizará una petición multicast, para que el equipo con nombre “pc1” (el nombre del equipo se define en `/etc/hostname`) responda con su IP.
- Es importante tener en cuenta que sólo afectará a las peticiones acabadas en `.local`, dejando la resolución del resto al siguiente mecanismo en la lista (el dns).

Si modificamos la línea y la dejamos así:

```
hosts:          dns files mdns4_minimal [NOTFOUND=return]
```

estamos indicando que queremos que se consulte primero el DNS para la resolución del nombre que estamos buscando.

DNS utilizado en un host (Linux Debian)

- Para indicar el servidor DNS que queremos configurar en nuestro equipo local, suponiendo que sea una distribución de Linux basada en Debian, lo podríamos hacer de la siguiente manera.
- Configuramos una IP estática al equipo e indicamos qué servidores de nombres queremos utilizar. Suponiendo que tenemos instalado un DNS en la red local que será el encargado de resolver los nombres (en la IP 192.168.1.254) y la IP que queremos asignar al equipo es 192.168.1.200:

Editamos el fichero `/etc/network/interfaces`

```
# Interfaz loopback
auto lo
iface lo inet loopback
# Interfaz del adaptador de red
auto enp0s3
iface enp0s3 inet static
    address 192.168.1.200
    netmask 255.255.255.0
    gateway 192.168.1.1
    dns-nameserver 192.168.1.254
    dns-search davidlopezcastellote.com # Esto sirve para que si
hacemos un ej. "ping c1" resuelva a "ping
c1.davidlopezcastellote.com"
```

Para que el cambio se haga efectivo, podemos hacer varias cosas:

- `/etc/init.d/networking restart`
- `ip addr flush enp0s3` (necesario hacerle el down y el up!!)
- `ifdown enp0s3; ifup enp0s3`

- Finalmente, el fichero en el que deben aparecer los servidores de nombres utilizados en nuestro equipo es `/etc/resolv.conf`:

```
nameserver 192.168.1.254
```

- **davidlopezcastellote.com:** 80.211.186.106. Fijémonos que nos devuelve ADDITIONAL SECTION, indicándonos

Consultas cacehadas

A continuación se muestra como el DNS hace uso de la caché; la primera consulta al dominio tarda 346msec, mientras que la segunda tarda 143msec.

```
MacBook-Pro-de-David-5:~ david$ dig elpais.es

; <<>> DiG 9.10.6 <<>> elpais.es
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 58211
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;elpais.es.                IN      A

;; ANSWER SECTION:
elpais.es.                56      IN      A      108.128.37.20
elpais.es.                56      IN      A      34.255.250.210

;; AUTHORITY SECTION:
elpais.es.                86400   IN      NS      ns4.p04.dynect.net.
elpais.es.                86400   IN      NS      ns3.p04.dynect.net.
elpais.es.                86400   IN      NS      ns1.p04.dynect.net.
elpais.es.                86400   IN      NS      ns2.p04.dynect.net.

;; Query time: 346 msec
;; SERVER: 192.168.1.254#53(192.168.1.254)
;; WHEN: Sun Jan 26 18:50:32 CET 2020
;; MSG SIZE rcvd: 156

MacBook-Pro-de-David-5:~ david$ dig elpais.es

; <<>> DiG 9.10.6 <<>> elpais.es
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 15865
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;elpais.es.                IN      A

;; ANSWER SECTION:
elpais.es.                29      IN      A      34.255.250.210
elpais.es.                29      IN      A      108.128.37.20

;; AUTHORITY SECTION:
elpais.es.                86373   IN      NS      ns2.p04.dynect.net.
elpais.es.                86373   IN      NS      ns1.p04.dynect.net.
elpais.es.                86373   IN      NS      ns3.p04.dynect.net.
elpais.es.                86373   IN      NS      ns4.p04.dynect.net.

;; Query time: 143 msec
;; SERVER: 192.168.1.254#53(192.168.1.254)
;; WHEN: Sun Jan 26 18:51:00 CET 2020
```

Comando nslookup

```
MacBook-Pro-de-David-5:~ david$ nslookup google.com
Server:      192.168.1.254
Address:     192.168.1.254#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.17.14

MacBook-Pro-de-David-5:~ david$
MacBook-Pro-de-David-5:~ david$
MacBook-Pro-de-David-5:~ david$ nslookup davidlopezcastellote.com
Server:      192.168.1.254
Address:     192.168.1.254#53

Name:   davidlopezcastellote.com
Address: 192.168.1.133

MacBook-Pro-de-David-5:~ david$
```

Indica que el DNS no es autoritativo de la respuesta

En este caso no indica nada, porque el DNS sí que es autoritario de la respuesta que ha ofrecido

```
MacBook-Pro-de-David-5:~ david$ nslookup web.davidlopezcastellote.com
Server:      192.168.1.254
Address:     192.168.1.254#53

web.davidlopezcastellote.com canonical name = www.davidlopezcastellote.com.
Name:   www.davidlopezcastellote.com
Address: 192.168.1.133
```

Indica una respuesta canónica

Comando host

```
MacBook-Pro-de-David-5:~ david$ host dlopezcastellote.dev
dlopezcastellote.dev has address 185.199.109.153
dlopezcastellote.dev has address 185.199.108.153
dlopezcastellote.dev has address 185.199.110.153
dlopezcastellote.dev has address 185.199.111.153
dlopezcastellote.dev mail is handled by 10 mx3.emailowl.com.
dlopezcastellote.dev mail is handled by 10 mx2.emailowl.com.
dlopezcastellote.dev mail is handled by 10 mx1.emailowl.com.
MacBook-Pro-de-David-5:~ david$ host web.davidlopezcastellote.com
web.davidlopezcastellote.com is an alias for www.davidlopezcastellote.com.
www.davidlopezcastellote.com has address 192.168.1.133
MacBook-Pro-de-David-5:~ david$
```