

Protocolo DNS

Resolución de nombres en Internet

✉ José Domingo Muñoz

🏫 IES Gonzalo Nazareno · Dos Hermanas

📖 SRI · Servicios de Red e Internet

01

Conceptos sobre DNS

Nombres, zonas y registros

¿Qué es DNS?

" **Domain Name System** es el protocolo que permite **guardar y consultar información** asociada a un nombre de dominio: dirección IP de un equipo, nombre asociado a una IP, servidor de correo de un dominio...

IDEAS CLAVE

- Las redes funcionan con **direcciones IP**, las personas con **nombres**
- DNS es el **directorio jerárquico** que traduce de uno a otro a escala global
- Es **distribuido**: ningún servidor conoce todos los nombres
- Su funcionamiento se basa en **delegación** entre dominios

 El servicio escucha por defecto en el puerto **53**, sobre **UDP** (consultas) y **TCP** (transferencias y respuestas grandes).

Tipos de nombres

HOSTNAME

- **Una sola palabra** que identifica al equipo
- Se guarda en `/etc/hostname`

FQDN — *FULLY QUALIFIED DOMAIN NAME*

- Hostname + **dominio completo**:
`macaco.gonzalonazareno.org.`
- Identifica al equipo de forma **inequívoca**

DOMAIN NAME

- Sucesión de nombres separados por **puntos**
- Ejemplo: `gonzalonazareno.org`

DOMINIO RAÍZ

- Es el **punto final**: todo nombre acaba en `.`

TLD — *TOP LEVEL DOMAIN*

- Dominios bajo el raíz: `com`, `org`, `es` ...

Zonas DNS

" Una **zona** agrupa la información de un nombre de dominio. El servidor que guarda una zona es su **autoridad**.

RESOLUCIÓN DIRECTA

- Conjunto de nombres bajo un dominio
- Permite obtener la **IP** a partir del **nombre**
- En `gonzalonazareno.org` : `macaco` , `www` , `dit` , `openstack` ...

RESOLUCIÓN INVERSA

- Permite obtener el **nombre** a partir de la **IP**
- Depende del **direccionamiento** de red
- Útil para registros de correo, *logs* y comprobaciones

 El **fichero de zona** es un archivo de texto donde se guardan los **registros** (cada tipo de información tiene su propio tipo de registro).

Autoridad sobre una zona

- El **servidor DNS** que guarda el **fichero de una zona** es su **servidor con autoridad**
- En el propio fichero de zona se declara con un **registro NS**
- Conviene tener **varios** servidores con autoridad por zona:
 - **Maestro** — servidor principal donde se edita la zona
 - **Esclavos** — sincronizan automáticamente con el maestro
- Los servidores con autoridad sobre el **dominio raíz** se llaman ***root servers***



Hay **13 conjuntos** de root servers identificados con letras (A–M); cada uno se replica con *anycast* en cientos de ubicaciones por todo el mundo.

Tipos de registros más usados

REGISTRO	PARA QUÉ SIRVE
SOA	<i>Start of Authority</i> — metainformación de la zona
NS	Servidor con autoridad sobre la zona
A	Dirección IPv4 de un nombre
AAAA	Dirección IPv6 de un nombre
CNAME	Alias — otro nombre que apunta al "real"
MX	Servidor de correo del dominio
PTR	Resolución inversa (IP → nombre)
TXT	Texto libre (SPF, DKIM, verificación...)

02

Resolución de consultas

Recursión, caché y tipos de servidor

Consulta DNS por recursión

Cuando un equipo necesita resolver un nombre, sigue este flujo:

1. Comprueba la **resolución estática** (`/etc/hosts` , NSS)
2. Si no lo encuentra, consulta al **servidor DNS** configurado en `resolv.conf`
3. Pueden pasar **tres cosas**:

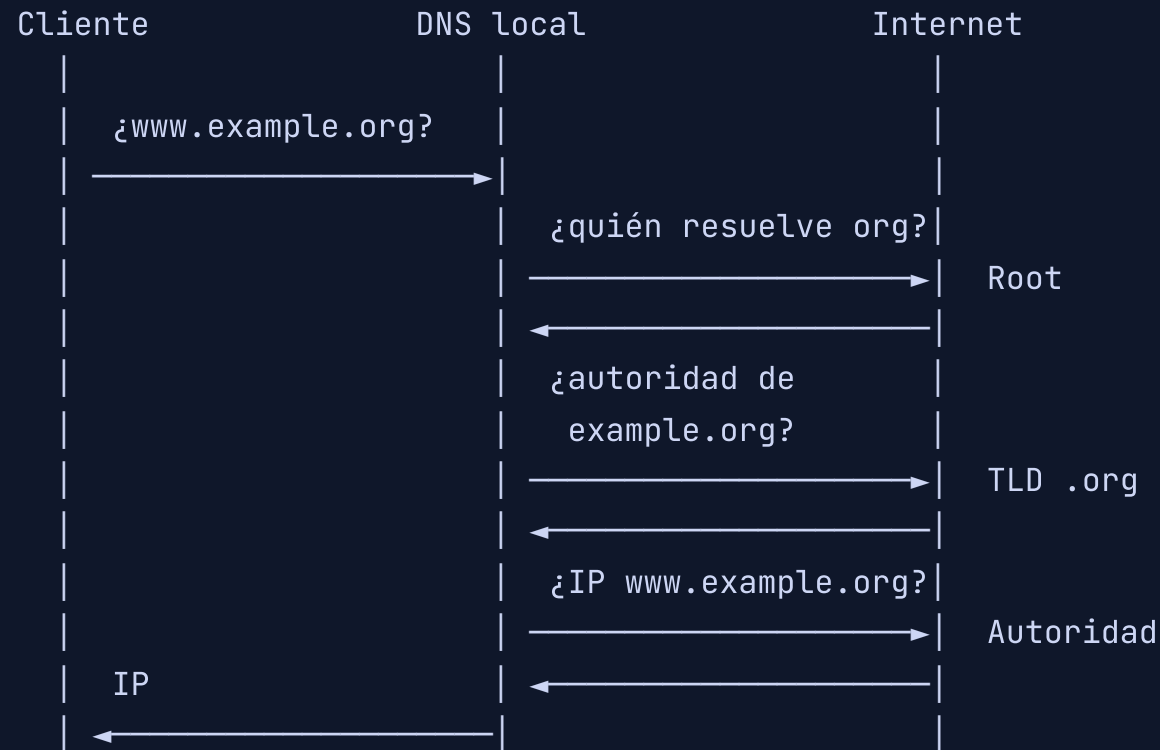
SI EL SERVIDOR LO CONOCE

- **Tiene autoridad** sobre el dominio → responde directamente
- **Lo tiene en caché** de una consulta previa → responde directamente

SI NO LO CONOCE

- Pregunta a los **root servers**
- Estos derivan al **TLD** correspondiente
- El TLD deriva al servidor **con autoridad** del dominio
- Se devuelve la respuesta y se **guarda en caché**

Esquema de la resolución



El cliente hace **una sola pregunta**; toda la cadena de consultas la realiza el servidor DNS local.

Tipos de servidores DNS

SERVIDOR RECURSIVO

- Resuelve **cualquier consulta** preguntando él mismo a la jerarquía
- Mantiene **caché** de respuestas
- Es el típico de los proveedores y de las redes locales

SERVIDOR FORWARD

- **Reenvía** las consultas a otro servidor
- No resuelve por sí mismo desde la raíz

SERVIDOR CON AUTORIDAD

- Responde **sólo** sobre las zonas que aloja
- No hace recursión
- Es la fuente "oficial" de los registros del dominio

SERVIDOR CACHÉ

- Sólo guarda respuestas previas
- Útil como capa intermedia para acelerar consultas

DNS en una red local

¿Y si el servidor DNS configurado en `resolv.conf` está en **nuestra propia red**?

- Las resoluciones se hacen **más rápidas**: lo que esté en caché no se vuelve a preguntar a Internet
- Si tenemos **servicios internos** con nombres propios, podemos crear una **zona local**: el servidor DNS tendrá autoridad sobre ella y resolverá esos nombres a **IPs privadas**
- El servidor **DHCP** de la red repartirá ese DNS local a los clientes

 Esto permite tener nombres como `impresora.lan` o `servidor.lan` sin depender de DNS externos ni tocar `/etc/hosts` en cada equipo.

03

DNS en el Gonzalo Nazareno

Un mismo dominio, dos vistas

Dos zonas para `gonzalonazareno.org`

El dominio `gonzalonazareno.org` tiene **dos zonas de resolución directa** distintas:

VISTA PÚBLICA (INTERNET)

- Servidores DNS con autoridad alojados en la empresa **CDMON**
- `openstack.gonzalonazareno.org` resuelve a la **IP pública:** `5.196.224.198`

VISTA INTERNA (INTRANET)

- Servidor DNS con autoridad: `macaco`
(`172.22.0.1`)
- `openstack.gonzalonazareno.org` resuelve a `172.22.0.3` (**simio**, proxy inverso)



Es un caso clásico de **split-horizon DNS**: la respuesta depende de desde dónde se pregunte.

Desde casa (vista pública)

```
$ dig ns gonzalonazareno.org
```

```
;; ANSWER SECTION:
```

```
gonzalonazareno.org.      21599      IN         NS         ns2.cdmon.net.  
gonzalonazareno.org.      21599      IN         NS         ns4.cdmondns-01.org.  
gonzalonazareno.org.      21599      IN         NS         ns1.cdmon.net.  
gonzalonazareno.org.      21599      IN         NS         ns5.cdmondns-01.com.  
gonzalonazareno.org.      21599      IN         NS         ns3.cdmon.net.
```

```
$ dig openstack.gonzalonazareno.org
```

```
;; ANSWER SECTION:
```

```
openstack.gonzalonazareno.org. 0 IN CNAME macaco.gonzalonazareno.org.  
macaco.gonzalonazareno.org.    0 IN A      5.196.224.198
```

Desde el aula (vista interna)

```
$ dig ns gonzalonazareno.org

;; ANSWER SECTION:
gonzalonazareno.org.      86400      IN        NS      dns.gonzalonazareno.org.

$ dig openstack.gonzalonazareno.org

;; ANSWER SECTION:
openstack.gonzalonazareno.org. 86400 IN CNAME  simio.gonzalonazareno.org.
simio.gonzalonazareno.org.      86400 IN  A      172.22.0.3
```

 El mismo nombre devuelve **respuestas distintas** según el servidor DNS al que se pregunte: el del aula tiene su propia zona con autoridad.

04

Ejercicio práctico

Consultas DNS con `dig`

La herramienta `dig`

`dig` permite hacer **consultas DNS** desde la línea de comandos y ver toda la respuesta del servidor.

SINTAXIS

```
dig [tipo de registro] [@servidor DNS] consulta_DNS
```

- El **tipo de registro** por defecto es `A`
- El **servidor DNS** por defecto es el de `/etc/resolv.conf`
- La respuesta aparece en la sección **ANSWER SECTION**

⚠ Si no tienes `dig` instalado, añade el paquete `dnsutils`: `sudo apt install dnsutils`.

Tipos de registro habituales con `dig`

TIPO	INFORMACIÓN QUE DEVUELVE
<code>A</code>	Dirección IPv4 (valor por defecto)
<code>AAAA</code>	Dirección IPv6
<code>NS</code>	Servidores con autoridad sobre la zona
<code>MX</code>	Servidores de correo del dominio
<code>CNAME</code>	Alias del nombre consultado
<code>SOA</code>	Metainformación de la zona
<code>TXT</code>	Registros de texto (SPF, DKIM, verificaciones...)
<code>-x <IP></code>	Resolución inversa de la dirección IP

Ejercicio — direcciones IP

Obtén la dirección **IP** de los siguientes dominios:

- `www.gonzalonazareno.org`
- `www.debian.org`

PISTA

```
dig www.gonzalonazareno.org
dig www.debian.org
```

 Fíjate en la sección `ANSWER SECTION` : puede haber un `CNAME` intermedio antes de llegar al registro `A` con la IP final.

Ejercicio — servidores con autoridad

Obtén los **servidores con autoridad** de los dominios:

- Dominio **raíz** (`.`)
- `es`
- `gonzalonazareno.org`

PISTA

```
dig ns .  
dig ns es  
dig ns gonzalonazareno.org
```

 El dominio raíz se representa con un punto: `.`. Devolverá los **13 root servers** (de `a.root-servers.net` a `m.root-servers.net`).

Ejercicio — servidores de correo

Obtén los **servidores de correo (MX)** de los dominios:

- `gonzalonazareno.org`
- `us.es`

PISTA

```
dig mx gonzalonazareno.org  
dig mx us.es
```

 Cada registro `MX` incluye una **prioridad** (número entero más bajo = más prioritario). Si el principal no responde, el correo se intenta entregar al siguiente.

Ejercicio — tipo de registro

¿Qué **tipo de registro** resuelve los siguientes dominios?

- `www.josedomingo.org`
- `informatica.gonzalonazareno.org`

PISTA

```
dig www.josedomingo.org
dig informatica.gonzalonazareno.org
```

 Mira la `ANSWER SECTION`: si aparece un `CNAME`, el nombre es un **alias** de otro; si aparece un `A` directamente, hay una IP asociada al propio nombre.

Ejercicio — resolución inversa

En clase: ¿a qué **nombre** corresponde la dirección IP `172.22.0.1` ?

PISTA

```
dig -x 172.22.0.1
```

 La resolución inversa se hace con la opción `-x`. La respuesta llega como un registro `PTR` en la `ANSWER SECTION`.

Trucos útiles con `dig`

```
# Consulta a un servidor DNS concreto
dig @8.8.8.8 www.debian.org

# Respuesta corta (sólo la IP / dato relevante)
dig +short www.debian.org

# Sin las secciones de cabecera y estadísticas
dig +noall +answer www.debian.org

# Seguir la cadena desde los root servers
dig +trace www.gonzalonazareno.org

# Consulta inversa
dig -x 172.22.0.1
```



`+trace` es muy útil para entender cómo se navega la jerarquía DNS desde el dominio raíz hasta el servidor con autoridad.

SRI · UNIDAD 5 — PROTOCOLO DNS

¡Gracias!

DNS → Servidor BIND en la práctica

 José Domingo Muñoz

 IES Gonzalo Nazareno · Dos Hermanas

 SRI