

DNS

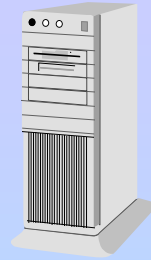
Domain Name System

Sistema de nombres de dominio

Administración de Sistemas y Redes

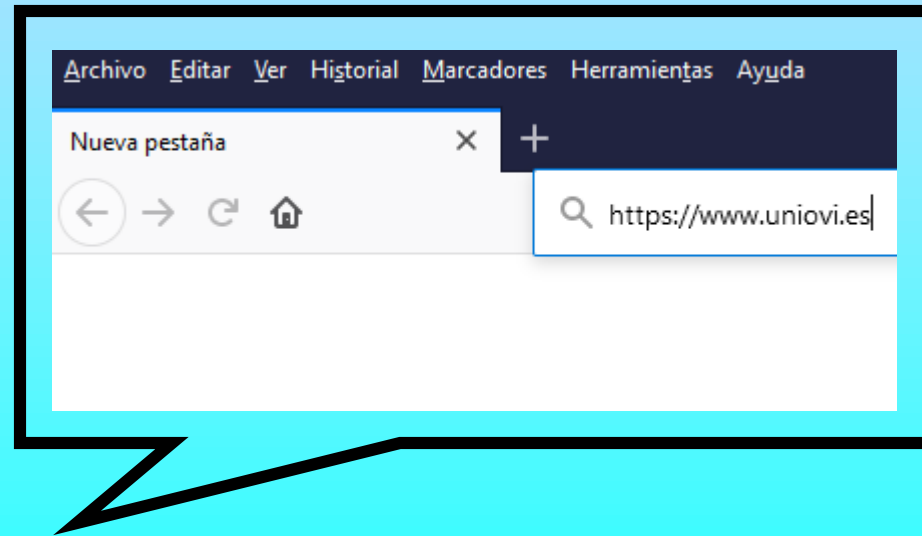
José A. Corrales

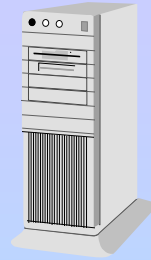
ja@uniovi.es



servidor DNS
resolvedor
p.ej. 1.1.1.1

uso habitual

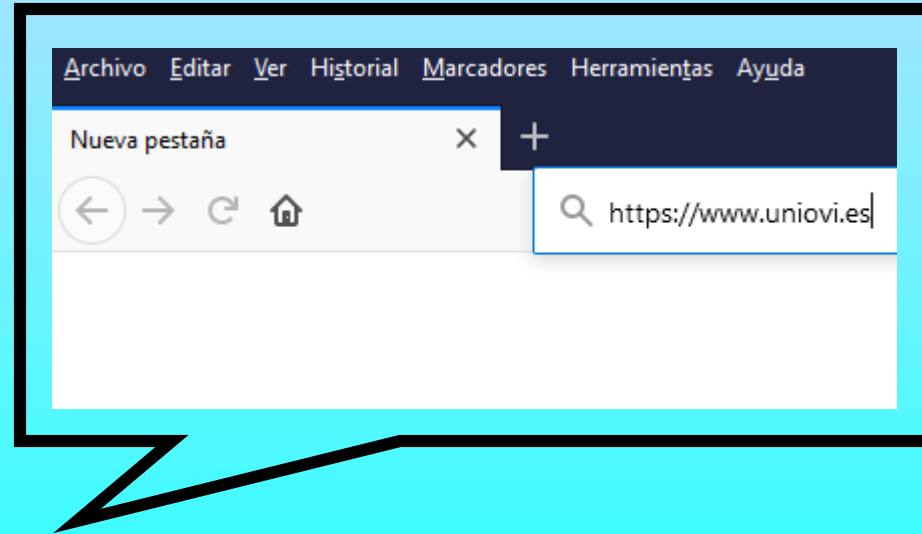


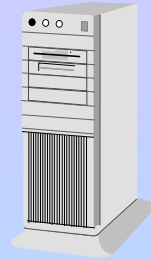


servidor DNS
resolvedor
p.ej. 1.1.1.1

uso habitual

¿www.uniovi.es?

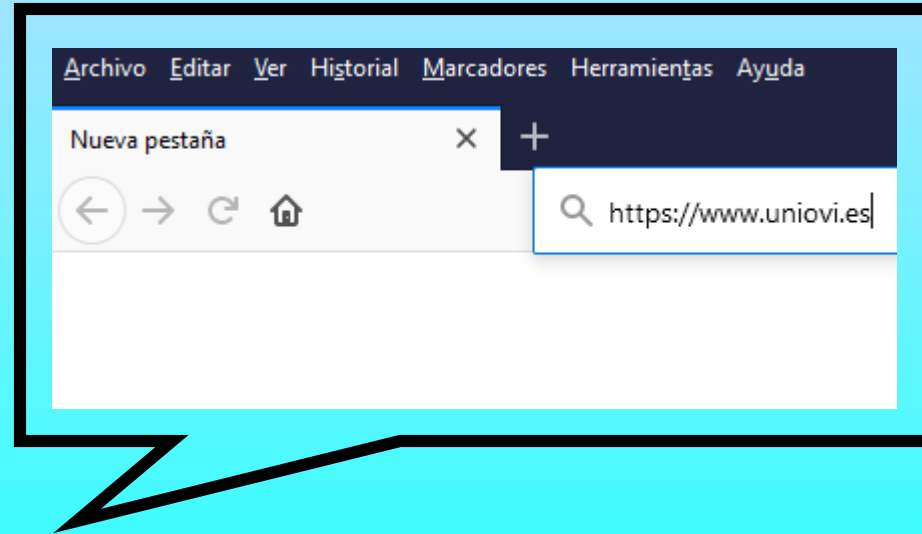


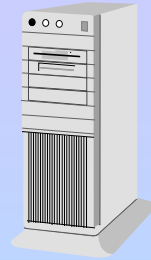


servidor DNS
resolvedor
p.ej. 1.1.1.1

uso habitual

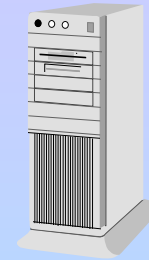
156.35.233.101





servidor DNS
resolvedor
p.ej. 1.1.1.1

156.35.233.101



get https://www.uniovi.es/

uso habitual



DNS: resolvers públicos (IPv4 e IPv6)

- de Cloudflare:
 - 1.1.1.1 y 1.0.0.1
 - 2606:4700:4700::1111 y 2606:4700:4700::1001
- de OpenDNS:
 - 208.67.222.222 y 208.67.220.220
 - 2620:0:ccc::2 y 2620:0:ccd::2
- de Google (peor política de privacidad):
 - 8.8.8.8 y 8.8.4.4
 - 2001:4860:4860::8888 y 2001:4860:4860::8844

DNS

- es un sistema global de Internet
- es distribuido (constituido por miles de servidores)
- permite a usuarios y aplicaciones emplear nombres de dominios en vez de direcciones IP para acceder a otros servicios

¿Cómo son los nombres?

- estructura jerarquizada
- servidores raíz
- .es (ccTLD, dominio de nivel superior)
- .uniovi.es
- .ccu.uniovi.es
- ejemplos: pinon.ccu.uniovi.es (también pueden existir ccu.uniovi.es y uniovi.es)

TLDs (dominios de nivel superior)

Los dominios de nivel superior pueden ser:

- genéricos (gTLDs): .com, .edu, .org, .net, .gov, .mil
 - patrocinados (sTLDs): .cat, .museum, .travel, .xxx
 - nuevos (nTLDs): .taxi, .shop, .berlin, .madrid
- de país (ccTLDs): .es, .fr, .uk, .us, .de, .ch, .as (American Samoa)
- internacionalizados (IDN ccTLDs): .中国, .pφ, مصر.
- otros: .arpa (infraestructura), .test (pruebas), .invalid (no válido)

Algunos problemas

<http://google.com/> (falso)

<http://google.com/> (auténtico)

El primero de los dos tiene la letra cirílica "omicrón" (decimal 1086) en vez de la latina "o" (decimal 111). A simple vista es indistinguible.

Tipos (roles) de servidores DNS

- **resolvedores:** reciben nombres y devuelven direcciones IP (o a la inversa) y otras informaciones. Por ejemplo 1.1.1.1 es un resolvedor público de Cloudflare que se puede usar para hacer cualquier tipo de consulta
- **autoritativos:** permiten definir nombres de equipos de una organización. Por ejemplo 156.35.14.2 es quien define los nombres bajo el dominio uniovi.es, pueden ser maestros (primarios) o esclavos (secundarios, empleados como backup automatizado de primarios)
- **raíz:** disponibles para todo el planeta, proporcionan información sobre los dominios de nivel superior (TLDs)

¿Qué información dan? (1)

Cuando se hace una consulta sobre un nombre completo (por ejemplo `pinon.ccu.uniovi.es`) pueden proporcionar:

- A (dirección IPv4)
- AAAA (dirección IPv6)
- SOA (autoridad, es decir quién define el nombre)
- NS (quién es servidor de nombres para el nombre consultado)
- MX (estafeta de correo entrante)
- TXT (texto arbitrario pero frecuentemente usado para SPF -correo-)

¿Qué información dan? (2)

- CNAME (alias para otro nombre completo)
- CAA (autoridades certificadoras)
- HINFO (información HW y SW del equipo, en desuso)
- LOC (posición: latitud, longitud y altura, en desuso)
- información sobre DNSSEC:
 - DNSKEY (clave)
 - RRSIG (firma)
 - NSEC (siguiente registro seguro)
 - DS (firmante)

¿Qué información dan? (3) Resolución inversa

Además de la resolución directa vista antes, proporcionan también la resolución inversa, es decir dada una dirección IP proporcionan el nombre asociado

- PTR (pointer)

Ejemplo

```
$ORIGIN aic.uniovi.es.
```

```
trasgu      A          156.35.105.130
```

```
            HINFO     "SIEMENS" "LINUX"
```

```
            MX         10 mail.uniovi.es.
```

```
            MX         10 mail2.uniovi.es.
```

```
            MX         30 mail3.uniovi.es.
```

```
            MX         40 mail4.uniovi.es.
```

```
            LOC        40 41 0.000 N 4 11 0.000 W 0.00m 0.00m 10000m 10m
```

\$ORIGIN .

\$TTL 172800 ; 2 days

UNIOVI.ES IN SOA enol.si.uniovi.es. dnsmaster.si.uniovi.es. (
2004032801 ; serial
86400 ; refresh (1 day)
7200 ; retry (2 hours)
2592000 ; expire (4 weeks 2 days)
172800 ; minimum (2 days)
)

NS dana.si.uniovi.es.

NS enol.si.uniovi.es.

NS zeus.etsimo.uniovi.es.

NS horru.lsi.uniovi.es.

NS ineco.nic.es.

\$TTL 0 ; 0 seconds

MX 10 mail.uniovi.es.

MX 10 mail2.uniovi.es.

MX 30 mail3.uniovi.es.

MX 40 mail4.uniovi.es.

TXT "v=spf1 mx a:relay.uniovi.es -all"

LOC 43 21 13.000 N 5 52 24.000 W 228.00m 0.00m 10000m 10m

Consultas (Windows, Linux)

pueden ser:

- recursivas (resuelve todo hasta el final)
- iterativas (se intenta obtener la mejor respuesta posible)
- no recursivas (entradas ya existentes en la cache del servidor)

```
C:\> nslookup
```

```
Servidor predeterminado:  localhost
```

```
Address:  127.0.0.1
```

```
>
```

Consultas

```
> www.uniovi.es
```

```
Server:  localhost
```

```
Address: 127.0.0.1
```

```
Non-authoritative answer:
```

```
Name:    www.uniovi.es
```

```
Address: 156.35.233.101
```

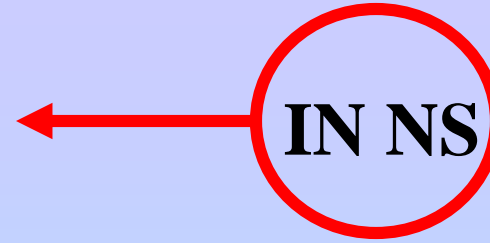
¿Cómo funciona un servidor DNS?

- intenta resolver la petición de una forma recursiva, comenzando por la raíz
- siempre busca primero en su cache local
- si no tiene la entrada en su cache entonces consulta a un servidor raíz
- el servidor raíz no suele dar la respuesta exacta sino una referencia sobre la que hacer la siguiente consulta
- repite el proceso anterior hasta que obtiene la respuesta a la consulta
- un servidor DNS de tipo cache solo resuelve nombres, no es autoritativo para ningún dominio. Se comporta como una cache.

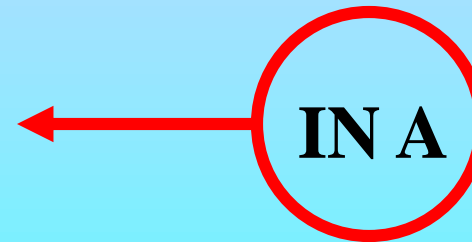
; Data file for initial cache data for root domain servers.

```
.      417496 IN   NS    E.ROOT-SERVERS.NET.
.      417496 IN   NS    F.ROOT-SERVERS.NET.
.      417496 IN   NS    G.ROOT-SERVERS.NET.
.      417496 IN   NS    H.ROOT-SERVERS.NET.
.      417496 IN   NS    I.ROOT-SERVERS.NET.
.      417496 IN   NS    J.ROOT-SERVERS.NET.
.      417496 IN   NS    K.ROOT-SERVERS.NET.
.      417496 IN   NS    L.ROOT-SERVERS.NET.
.      417496 IN   NS    M.ROOT-SERVERS.NET.
.      417496 IN   NS    A.ROOT-SERVERS.NET.
.      417496 IN   NS    B.ROOT-SERVERS.NET.
.      417496 IN   NS    C.ROOT-SERVERS.NET.
.      417496 IN   NS    D.ROOT-SERVERS.NET.
```

```
A.ROOT-SERVERS.NET. 503896 IN   A     198.41.0.4
B.ROOT-SERVERS.NET. 503896 IN   A     128.9.0.107
C.ROOT-SERVERS.NET. 503896 IN   A     192.33.4.12
D.ROOT-SERVERS.NET. 503896 IN   A     128.8.10.90
E.ROOT-SERVERS.NET. 503896 IN   A     192.203.230.10
F.ROOT-SERVERS.NET. 503896 IN   A     192.5.5.241
G.ROOT-SERVERS.NET. 503896 IN   A     192.112.36.4
H.ROOT-SERVERS.NET. 503896 IN   A     128.63.2.53
I.ROOT-SERVERS.NET. 503896 IN   A     192.36.148.17
J.ROOT-SERVERS.NET. 503896 IN   A     198.41.0.10
K.ROOT-SERVERS.NET. 503896 IN   A     193.0.14.129
L.ROOT-SERVERS.NET. 503896 IN   A     198.32.64.12
M.ROOT-SERVERS.NET. 503896 IN   A     202.12.27.33
```



(dice quién es servidor
de nombres, en este
caso de ‘.’)



(dice cuál es la dirección
IPv4 que corresponde a
ese nombre)

Ejemplo con la orden dig (Linux)

Muestra la traza de la consulta al servidor 1.1.1.1 sobre el nombre horru.lsi.uniovi.es

```
$ dig +trace +all horru.lsi.uniovi.es @1.1.1.1
```

a uno de los raíz: ¿quién resuelve "es"?

a uno de ellos: ¿quién resuelve "uniovi.es"?

a uno de ellos: ¿quién es "horru.lsi.uniovi.es"?

Ejemplo con la orden host (Linux)

```
$ host horru.lsi.uniovi.es 1.1.1.1
```

```
Using domain server:
```

```
Name: 1.1.1.1
```

```
Address: 1.1.1.1#53
```

```
Aliases:
```

```
horru.lsi.uniovi.es has address 156.35.119.120
```

```
horru.lsi.uniovi.es mail is handled by 10 primera.net.uniovi.es.
```

```
horru.lsi.uniovi.es mail is handled by 20 llar.net.uniovi.es.
```

```
horru.lsi.uniovi.es mail is handled by 20 xanes.net.uniovi.es.
```

```
horru.lsi.uniovi.es mail is handled by 40 boreal.net.uniovi.es.
```

```
horru.lsi.uniovi.es mail is handled by 50 cabera.net.uniovi.es.
```

Ejemplo con nslookup (Windows, Linux)

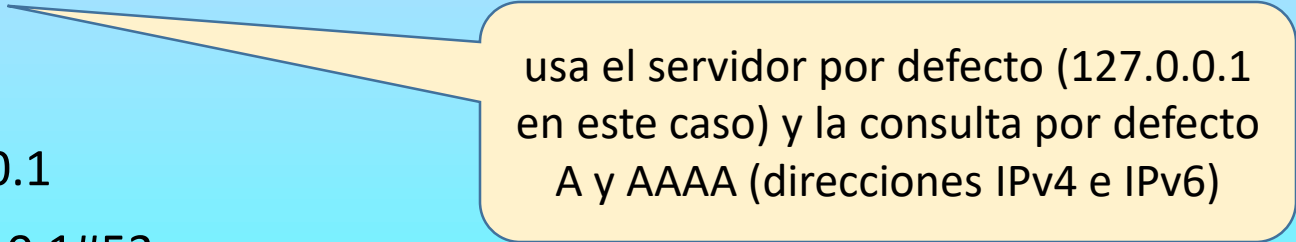
La siguiente secuencia de comandos se hace desde un equipo externo a la red de la Universidad de Oviedo y que además es un servidor DNS, es decir se consulta a sí mismo (127.0.0.1):

```
$ nslookup
```

```
> www.uniovi.es
```

```
Server:      127.0.0.1
```

```
Address:     127.0.0.1#53
```



usa el servidor por defecto (127.0.0.1 en este caso) y la consulta por defecto A y AAAA (direcciones IPv4 e IPv6)

```
Non-authoritative answer:
```

```
Name: www.uniovi.es
```

```
Address: 156.35.233.101
```

Ejemplo con nslookup (Windows, Linux)

> google.com

Server: 127.0.0.1

Address: 127.0.0.1#53

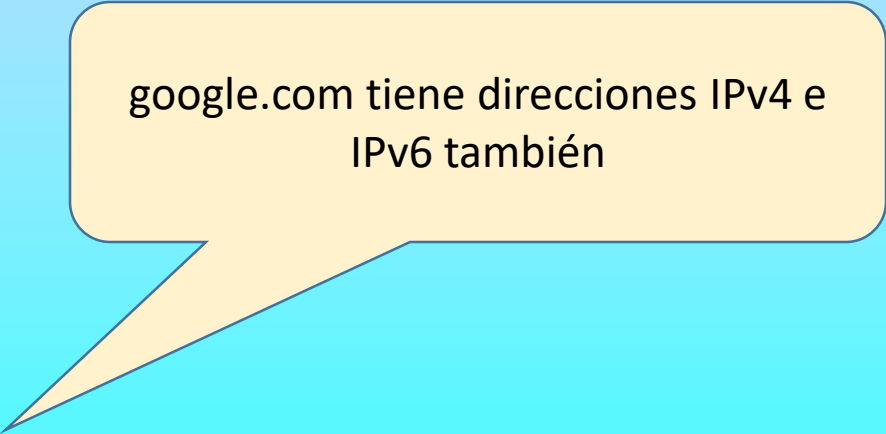
Non-authoritative answer:

Name: google.com

Address: 142.250.186.78

Name: google.com

Address: 2a00:1450:4001:811::200e



google.com tiene direcciones IPv4 e IPv6 también

Ejemplo con nslookup (Windows, Linux)

> server 1.1.1.1

Default server: 1.1.1.1

Address: 1.1.1.1#53

> hotmail.com

Server: 1.1.1.1

Address: 1.1.1.1#53

Non-authoritative answer:

Name: hotmail.com

Address: 204.79.197.212

se especifica un nuevo servidor a donde se realizarán las consultas

hotmail.com solo tiene dirección IPv4

Ejemplo con nslookup (Windows, Linux)

> set type=soa

> uniovi.es

Server: 1.1.1.1

Address: 1.1.1.1#53

Non-authoritative answer:

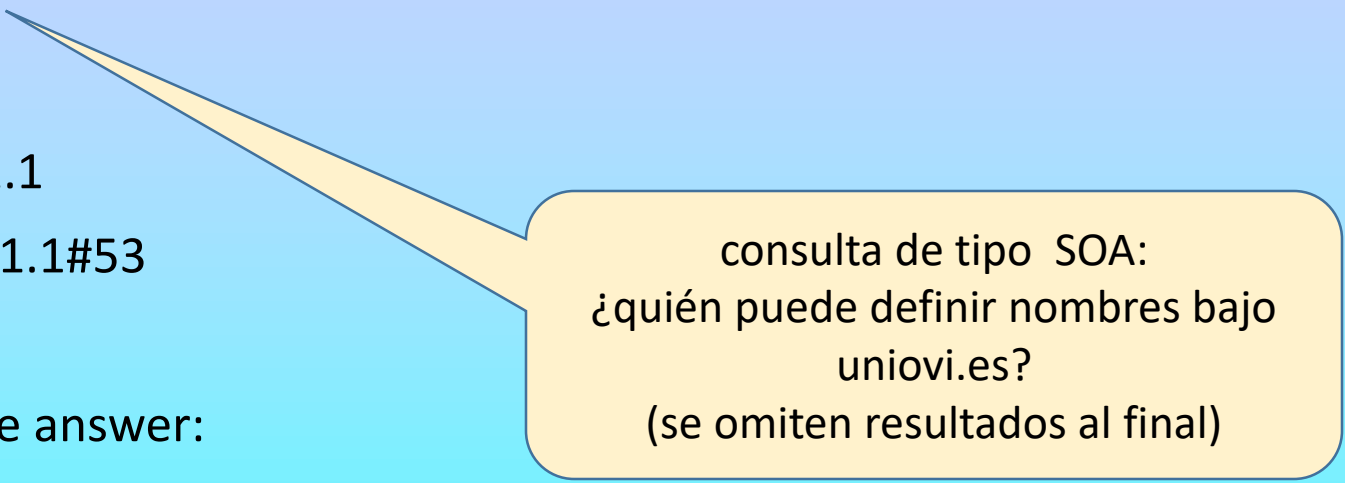
uniovi.es

origin = enol.si.uniovi.es

mail addr = redes.uniovi.es

serial = 2020081619

...



consulta de tipo SOA:
¿quién puede definir nombres bajo
uniovi.es?
(se omiten resultados al final)

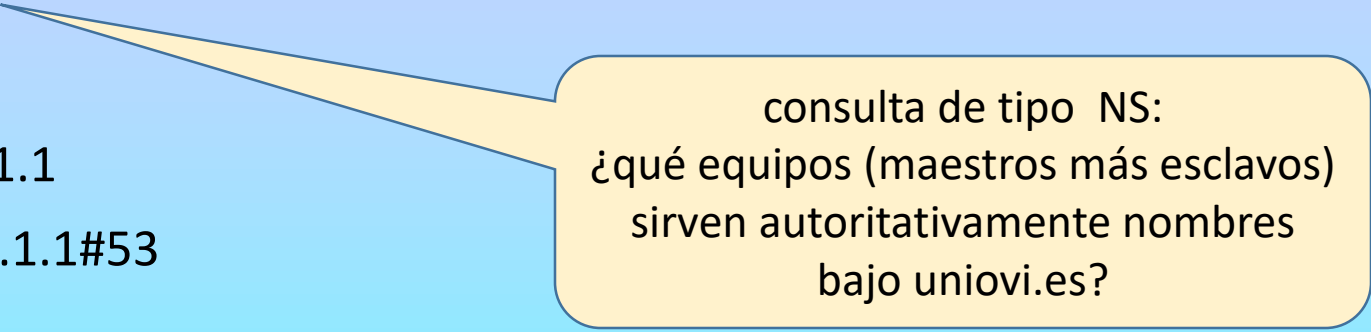
Ejemplo con nslookup (Windows, Linux)

```
> set type=ns
```

```
> uniovi.es
```

```
Server:      1.1.1.1
```

```
Address:     1.1.1.1#53
```



consulta de tipo NS:
¿qué equipos (maestros más esclavos)
sirven autoritativamente nombres
bajo uniovi.es?

Non-authoritative answer:

```
uniovi.es    nameserver = solid.net.uniovi.es.
```

```
uniovi.es    nameserver = chico.rediris.es.
```

```
uniovi.es    nameserver = zeus.etsimo.uniovi.es.
```

```
uniovi.es    nameserver = enol.si.uniovi.es.
```

```
uniovi.es    nameserver = sun.rediris.es.
```

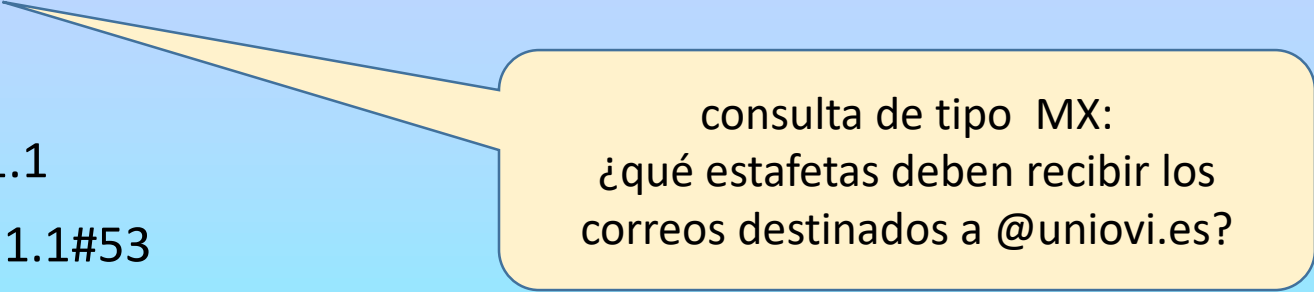
Ejemplo con nslookup (Windows, Linux)

```
> set type=mx
```

```
> uniovi.es
```

```
Server:      1.1.1.1
```

```
Address:     1.1.1.1#53
```



consulta de tipo MX:
¿qué estafetas deben recibir los
correos destinados a @uniovi.es?

Non-authoritative answer:

```
uniovi.es    mail exchanger = 10 mx02.puc.rediris.es.
```

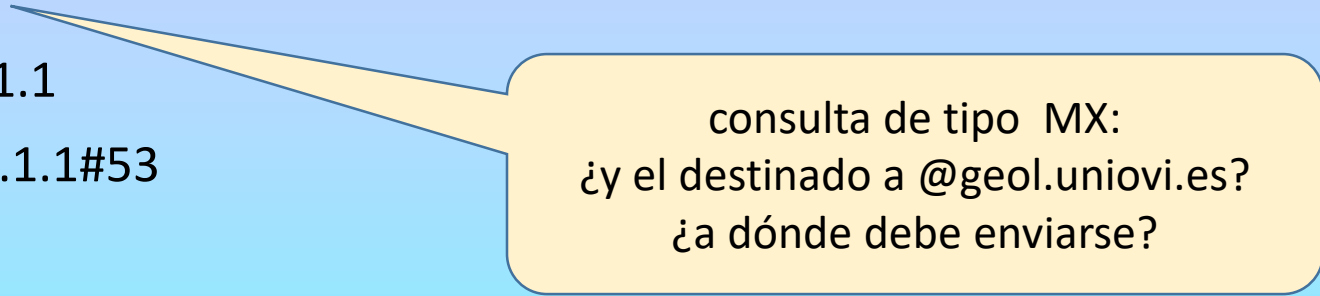
```
uniovi.es    mail exchanger = 10 mx01.puc.rediris.es.
```

Ejemplo con nslookup (Windows, Linux)

> geol.uniovi.es

Server: 1.1.1.1

Address: 1.1.1.1#53



consulta de tipo MX:
¿y el destinado a @geol.uniovi.es?
¿a dónde debe enviarse?

Non-authoritative answer:

geol.uniovi.es mail exchanger = 10 primera.net.uniovi.es.

geol.uniovi.es mail exchanger = 20 xanes.net.uniovi.es.

geol.uniovi.es mail exchanger = 40 boreal.net.uniovi.es.

geol.uniovi.es mail exchanger = 50 cabera.net.uniovi.es.

geol.uniovi.es mail exchanger = 20 llar.net.uniovi.es.

Ejemplo con nslookup (Windows, Linux)

```
> set type=ptr  
> 101.233.35.156.in-addr.arpa  
Server:      1.1.1.1  
Address:     1.1.1.1#53
```

resolución inversa, obsérvese el
formato de la consulta

Non-authoritative answer:

101.233.35.156.in-addr.arpa name = www.uniovi.es.

Ejemplo con nslookup (Windows, Linux)

```
> set type=a
```

```
> 156.35.233.101
```

```
Server:      1.1.1.1
```

```
Address:     1.1.1.1#53
```

resolución inversa, por comodidad
también se permite así

Non-authoritative answer:

```
101.233.35.156.in-addr.arpa  name = www.uniovi.es.
```

Ejemplo con nslookup (Windows, Linux)

> set type=aaaa

> facebook.com

Server: 1.1.1.1

Address: 1.1.1.1#53

consulta solo la dirección IPv6

Non-authoritative answer:

Name: facebook.com

Address: 2a03:2880:f12d:83:face:b00c:0:25de

Ejemplo con nslookup (Windows, Linux)

> set type=a

> server 156.35.14.2

Default server: 156.35.14.2

Address: 156.35.14.2#53

> coruxa.epsig.uniovi.es

Server: 156.35.14.2

Address: 156.35.14.2#53

Name: coruxa.epsig.uniovi.es

Address: 156.35.41.4

desde fuera de la universidad se consulta al servidor de la universidad sobre algo acabado en uniovi.es, obsérvese que no aparece el texto **Non-authoritative answer** de las consultas anteriores

Ejemplo con nslookup (Windows, Linux)

```
> set type=a
```

```
> server 156.35.14.2
```

```
Default server: 156.35.14.2
```

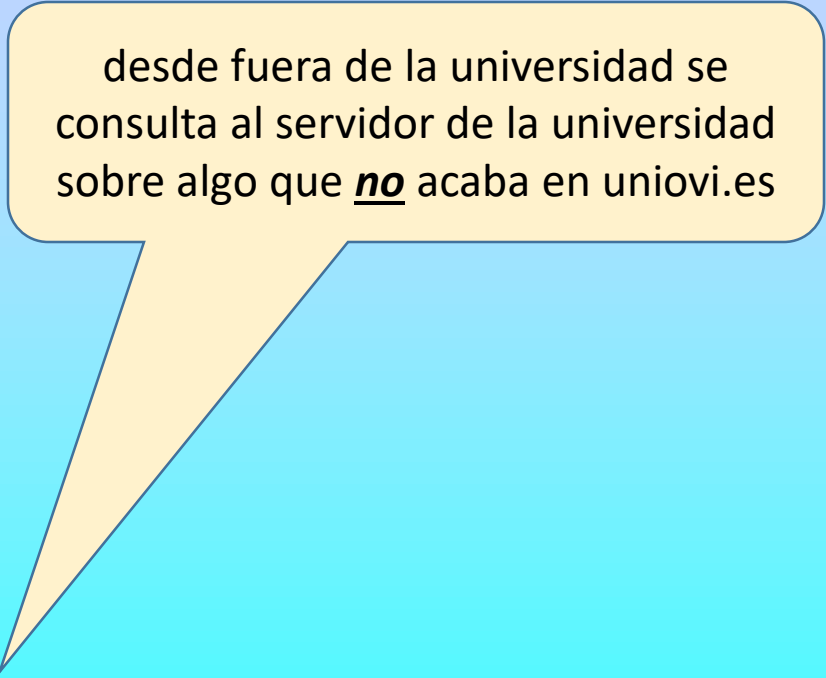
```
Address: 156.35.14.2#53
```

```
> google.com
```

```
Server:      156.35.14.2
```

```
Address:     156.35.14.2#53
```

```
** server can't find google.com: REFUSED
```



desde fuera de la universidad se consulta al servidor de la universidad sobre algo que **no** acaba en uniovi.es

¿Cómo debe configurarse un servidor DNS?

(Ejemplo con la organización as.local con los equipos internos 192.168.56.0/24)

- Para uso interno debe ser recursivo, es decir debe poder resolver cualquier cosa para cualquier equipo interno a nuestra organización
- Además debe ser autoritativo para todo lo definido bajo as.local
- Para uso externo debe resolver solamente los nombres definidos bajo as.local, de lo contrario sería un resolvedor público
- Los resolvedores públicos son objetivos de ataques y fuente de problemas de seguridad