

# DNS

## Definición

“El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.” (Wikipedia)

# Por qué DNS? Historia

En los 70s la tabla que relacionaba nombres con ips se almacenaba en un solo servidor y se distribuía por FTP a los clientes. Todavía existe ese fichero...

- /etc/hosts ( linux)
- /system32/drivers/etc/hosts (windows)

Esto ocasionaba problemas

- procedimiento no escalable
- mucho tráfico en el servidor y fichero host demasiado grande.
- inconsistente, tu host podía estar obsoleto en unas horas.
- con facilidad aparecían nombres duplicados.
- Esto provoca el surgimiento en 1983 del servicio DNS.



# DNS. El Creador



Paul V. Mockapetris (born 1948 in Boston Massachusetts, USA) is an American computer scientist and Internet pioneer, who, together with Jon Postel, invented the Internet Domain Name System (DNS).

# Características DNS

*El sistema DNS resuelve los anteriores problemas...*

***Carga de la red y de los hosts:*** este problema ya no existe debido a que la información esta distribuida por toda la red, al tratarse de una bdd distribuida.

***Duplicidad de nombres:*** el problema se elimina debido a la existencia de dominios pequeños controlados por un único administrador. Puede haber nombres iguales pero en dominios diferentes.

***Consistencia de la Información:*** ahora la información que esta distribuida es actualizada automáticamente sin intervención de ningún administrador.



# Características DNS

El Sistema de Nombres de Dominio tiene los siguientes **elementos principales**:

- **Un espacio de nombres de dominio DNS**, que especifica una jerarquía estructurada de dominios utilizados para organizar nombres.
- **Los servidores DNS**, que almacenan y responden a las consultas de nombres para los registros de recursos.
- **Los registros de recursos**, que asignan nombres de dominio DNS a un tipo específico de información. Como por ejemplo una IP.
- **Los clientes DNS**, también llamados “resolvers”, que hacen las consultas a los servidores.

# Características DNS

CLIENTE

PROTOCOLO

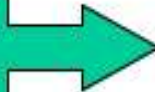
SERVIDOR

resolver

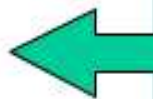


un library:  
gethostbyname()  
...

DNS query  
fqdn?



DNS response:  
<address IP>



Mensajes DNS  
transportados  
usualmente por UDP

Servicio DNS



Múltiples servers coordinados



# Características DNS

## Map of the Root Servers

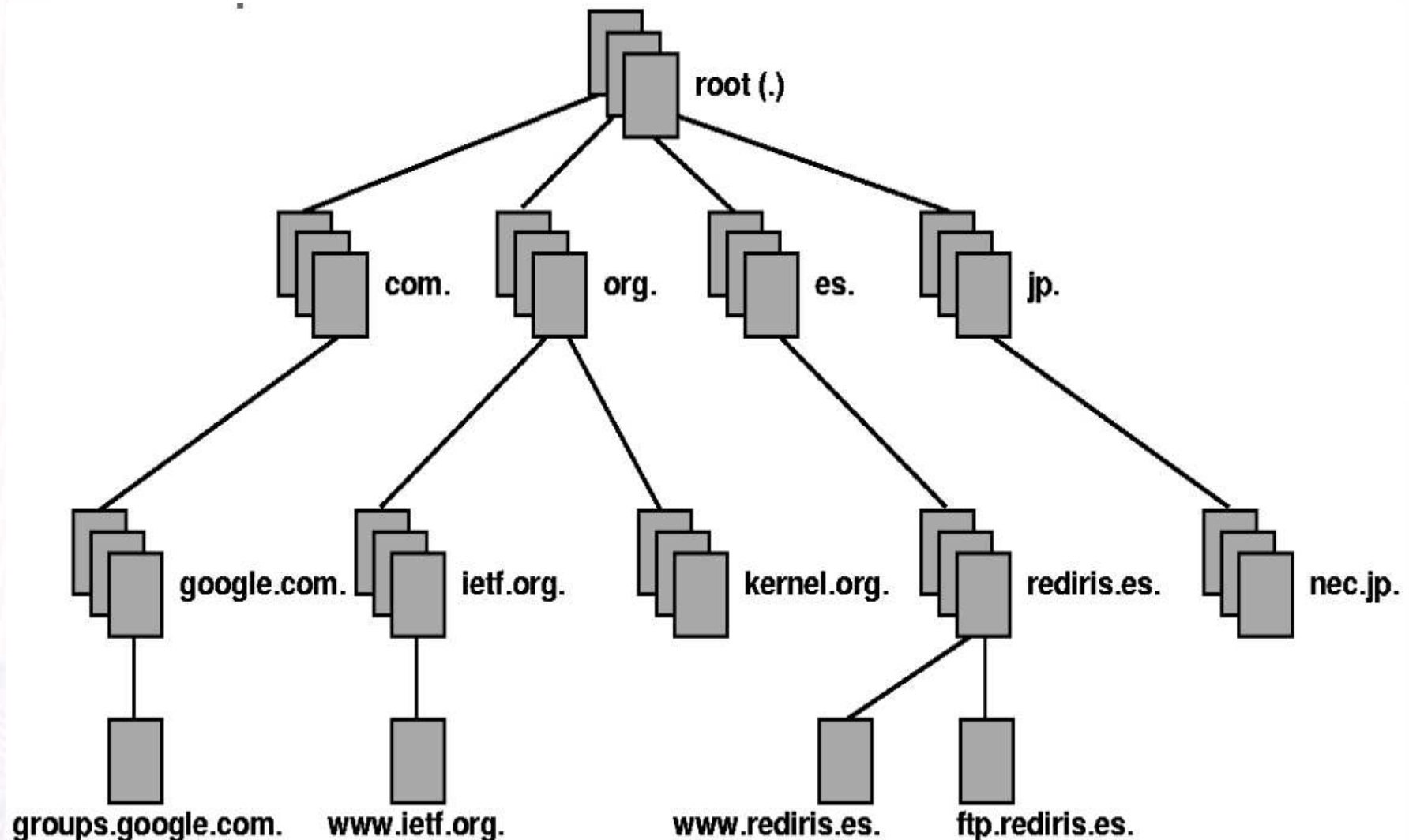


# Espacio de nombres de dominio

- DNS está organizado en **nombres de dominio**, donde cada nombre de dominio es una trayectoria en un árbol invertido llamado **espacio de nombres de dominio**. El árbol tiene una única raíz superior (root) y una profundidad máxima de 127 niveles.
- Se denomina **dominio** a cualquier **subárbol** del espacio de nombres de dominio. De esta forma, cada dominio puede contener, a su vez, otros dominios. Generalmente, los **hosts** están representados por las hojas del árbol.



# Espacio de nombres de dominio

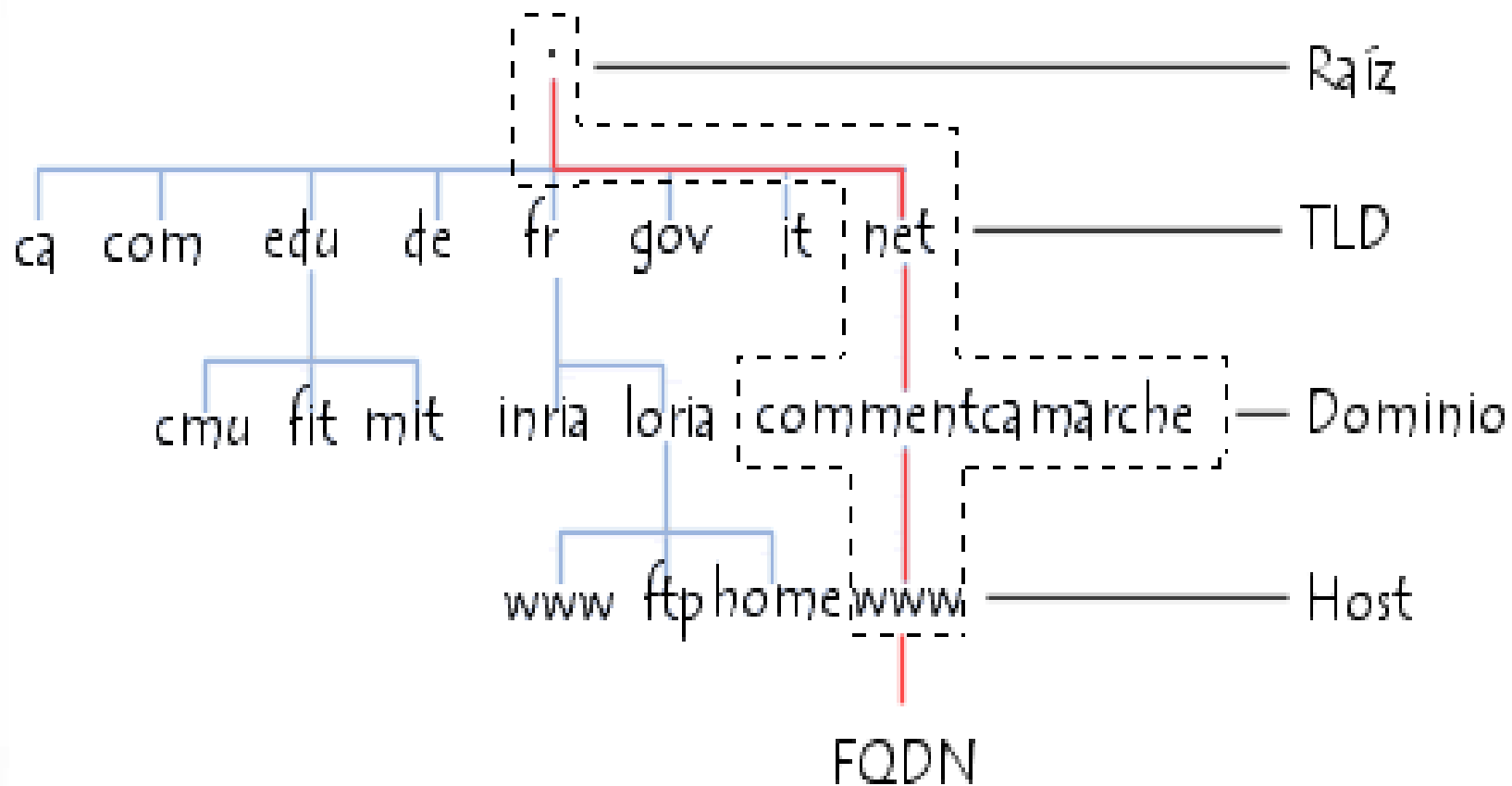


# Espacio de nombres de dominio

- Cada **nodo** en el árbol se identifica con una etiqueta no nula de hasta 63 caracteres, menos el nodo raíz, que tiene una etiqueta nula.
- El nombre de cualquier nodo está formado por la secuencia de etiquetas que forman la trayectoria desde dicho nodo hasta la raíz separadas por puntos.
- A una trayectoria desde un computador hasta el raíz se le conoce como nombre de dominio completamente cualificado o Fully Qualified Domain Name (**FQDN**).
- Al ser nula la etiqueta que identifica el nodo raíz, el FQDN de cualquier nodo del árbol siempre acaba con un punto.



# Espacio de nombres de dominio



FQDN= `www.commentcamarche.net`

# Espacio de nombres de dominio

La **ICANN** actualmente clasifica los dominios de nivel superior en tres tipos:

Dominios de nivel superior **geográficos** (ccTLD): Usados por un país o un territorio dependiente. Tienen dos letras: **.es, .fr, .de, .mx...**

- Dominios de nivel superior **genéricos** (gTLD): Usado por determinadas organizaciones (**.com, .org, .net** ...). Tiene tres o más letras de largo. La mayoría de los gTLDs están disponibles para el uso mundial menos algunos como **.mil** y **.gov**  
Los gTLDs se clasifican, a su vez en:
  - Dominios de nivel superior **patrocinados** (sTLD): Ej. **.aero, .cat, .museum...**
  - Dominios de nivel superior **no patrocinados** (uTLD): Ej. **.biz, .info, .name** y **.pro.**
- Dominios de nivel superior **de infraestructura**: El dominio de nivel superior arpa es el único confirmado.



# Delegación

El objetivo principal del diseño del sistema de nombres de dominio en forma jerárquica fue su **administración descentralizada**. Este objetivo se consigue a través de la **delegación**.

Una organización que administra un dominio puede dividirla en **subdominios**. Cada subdominio puede ser delegado a diferentes organizaciones, lo cual implica que esa organización será responsable de mantener los datos de ese subdominio.

# Delegación vs Subdominios

La división en subdominios y la delegación de dichos subdominios son cosas distintas.

Un dominio que tenga capacidad de autogestión (autoridad), siempre puede decidir subdividirse en diferentes subdominios. Posteriormente, se puede decidir delegar la autoridad de algunos sus subdominios en otras organizaciones.

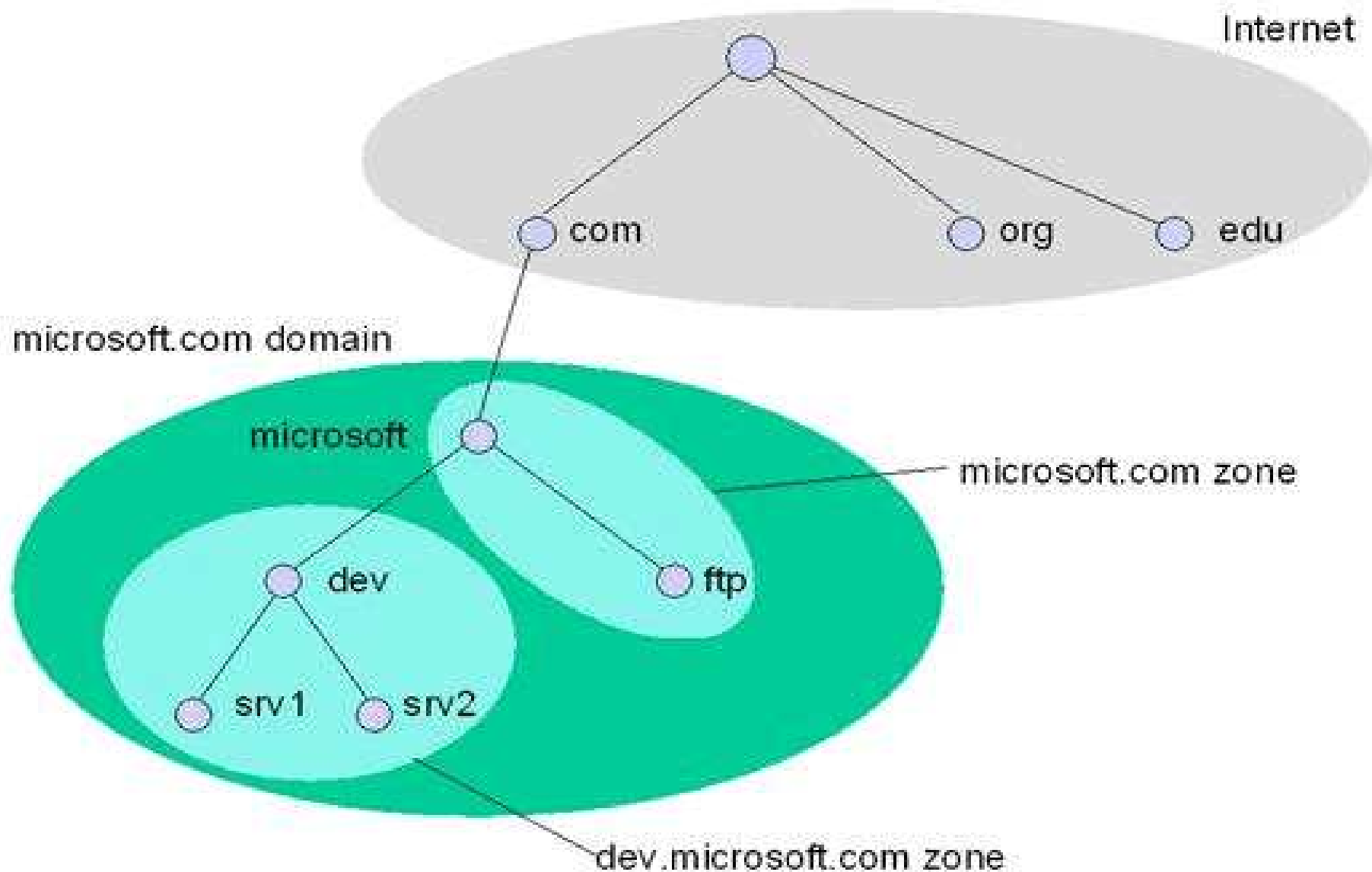


# Dominios y Zonas

**Cada servidor** de nombres posee información sobre una parte contigua del espacio de nombres. Dicha parte del espacio se denomina **zona**, y se dice que el servidor de nombres tiene **autoridad** sobre ella.

Un servidor de nombres puede tener autoridad sobre múltiples zonas, y obtiene la información que describe la zona (los registros de recursos) o bien de un fichero local o bien de otro servidor de nombres

# Dominios y Zonas





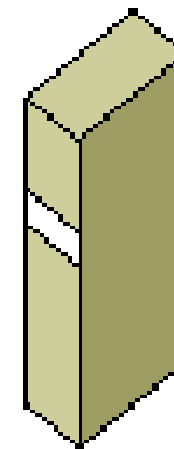
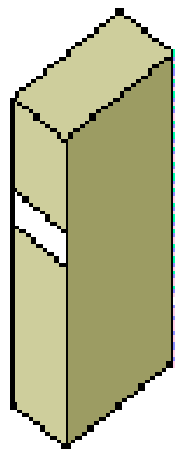
# Tipos de servidores DNS

- **Primarios o maestros:** Guardan los datos de una parte del espacio de nombres (zona) en sus ficheros. Las modificaciones, altas, o bajas de registros se realizan en estos servidores.
- **Secundarios o esclavos:** Obtienen los datos de zona de los servidores primarios a través de una **transferencia de zona**.
- **Locales o caché:** Funcionan con el mismo software, pero no contienen información de ninguna zona del espacio de nombres. Cuando los clientes les realizan una consulta, estos a su vez consultan a otros servidores DNS, almacenando la respuesta en caché para agilizar la repetición de estas peticiones en el futuro.

# Tipos de servidores DNS

Master server

Secondary server



1. SOA request

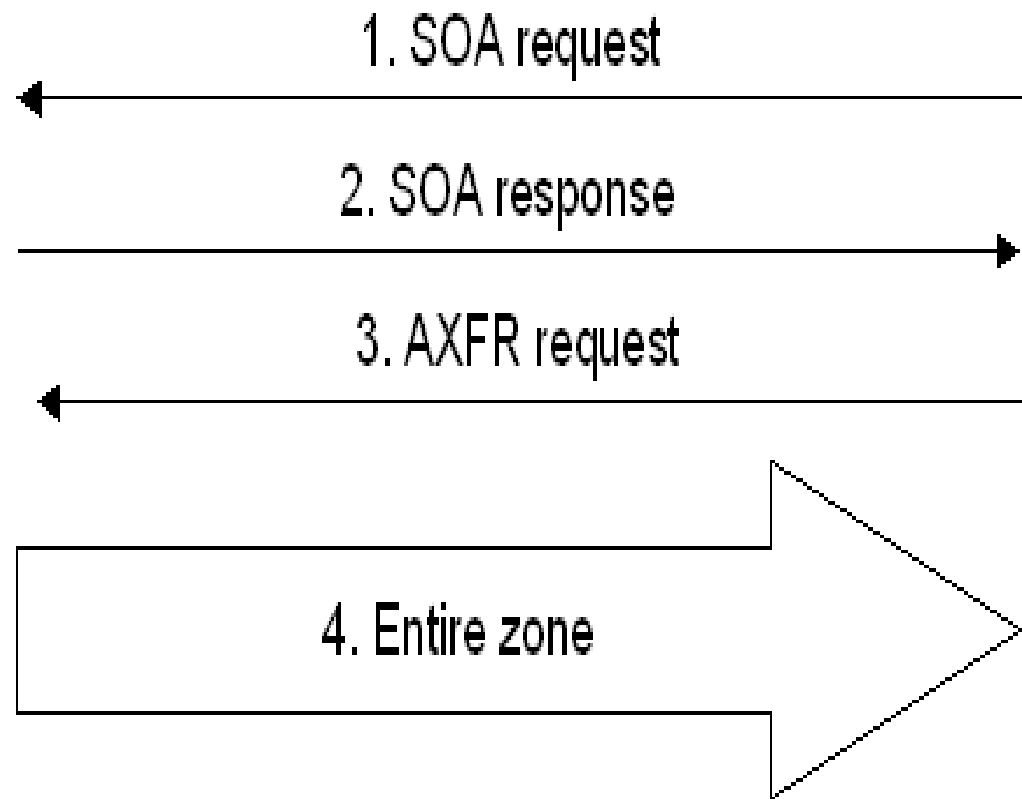
2. SOA response

3. AXFR request

DNS1

4. Entire zone

DNS2





# Transferencias de zona

Una **transferencia de zona** es el proceso por el que se copia el contenido de un archivo de zona DNS de un servidor DNS principal a un servidor DNS secundario.

Se producirá una transferencia de zona durante cualquiera de las siguientes situaciones:

- Al **iniciar** el servicio DNS en el servidor secundario.
- Cuando **expire** el tiempo de actualización.
- Cuando se **guardan** cambios en el archivo de zona primaria y hay una lista de notificación.
- Cuando se solicita de manera **manual**.

# Tipos de búsquedas DNS

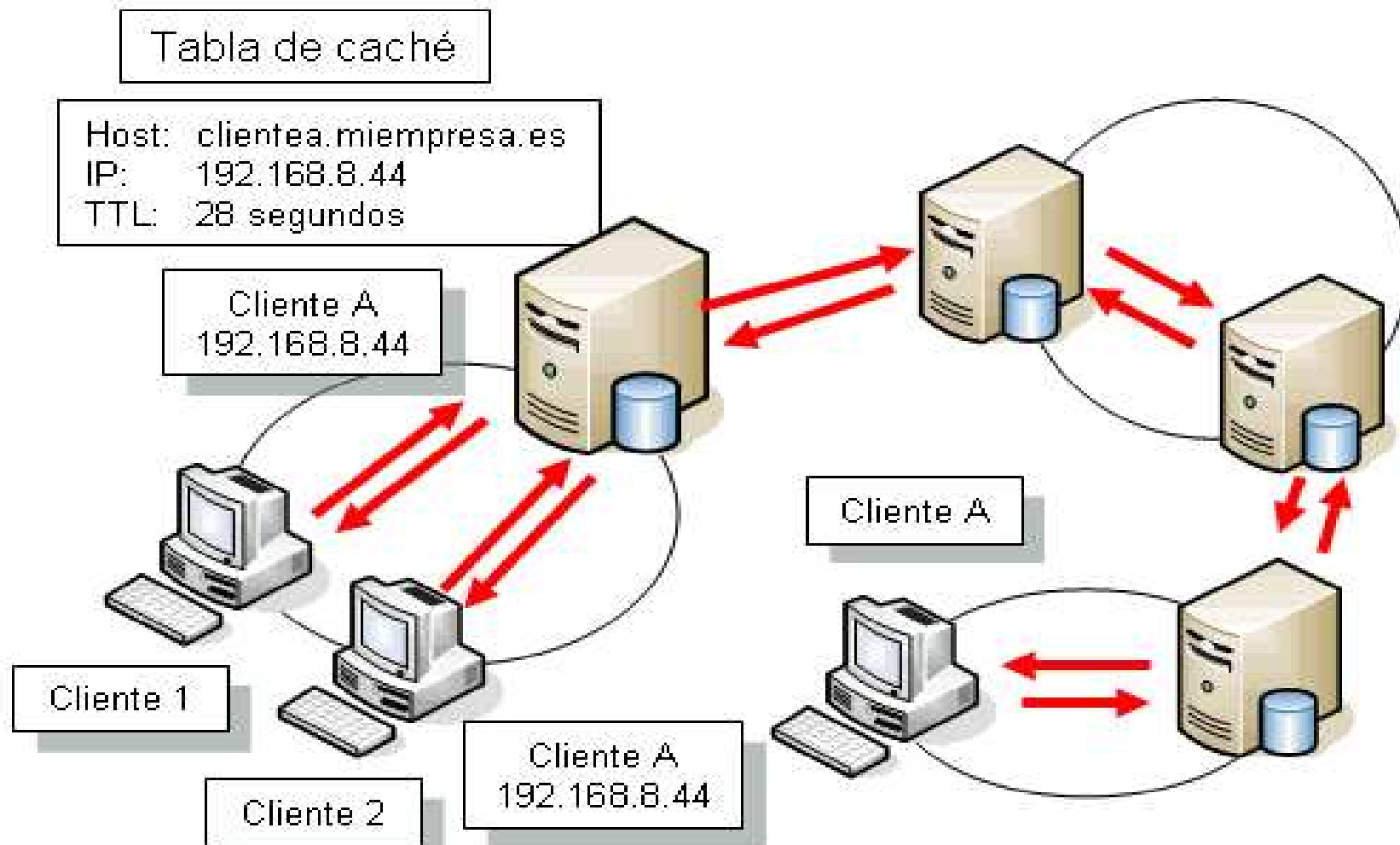
Existen dos tipos de búsquedas:

- Las iterativas.
- Las recursivas.

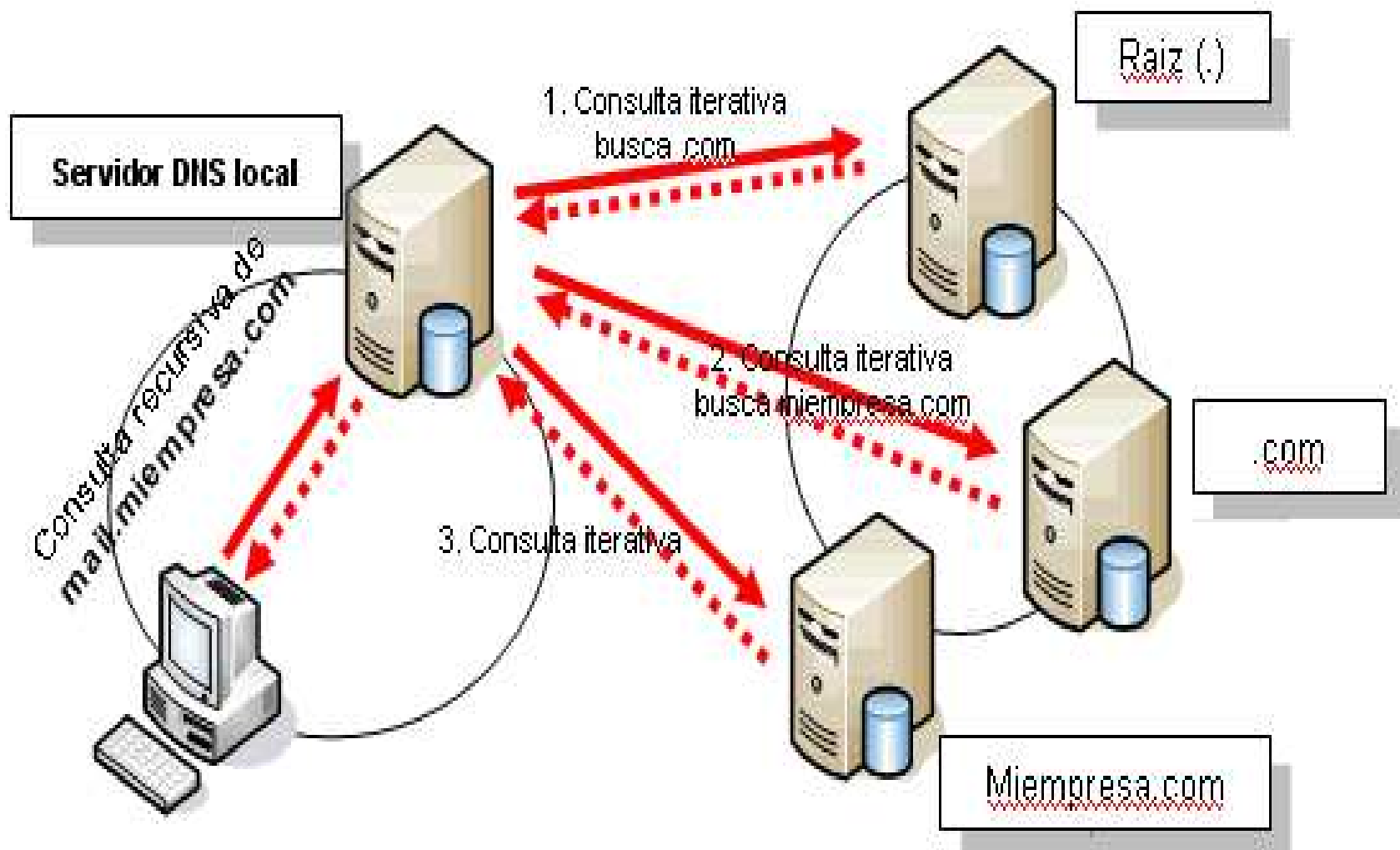




# Consulta recursiva



# Consulta iterativa





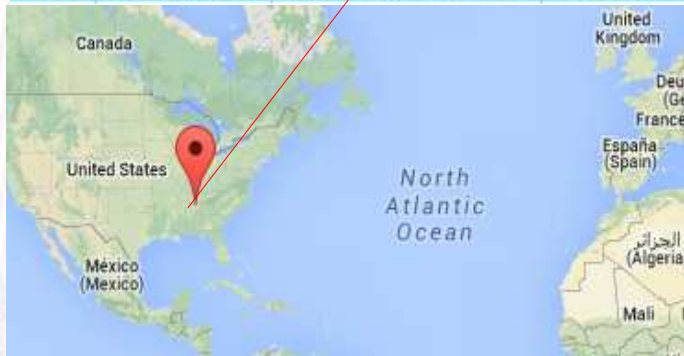
# Consulta iterativa

## Verificación !!

Desde un servidor DNS local hacemos un ping a `www.elmundo.es` Y analizamos el tráfico dns.

```
R45:~$ ping www.elmundo.es
(193.110.128.199) 56(84) b
```

1	0.000000	192.168.1.39	192.203.230.10	DNS	76	Standard query A www.elmundo.es
2	0.194682	192.203.230.10	192.168.1.39	DNS	502	Standard query response
3	0.195690	192.168.1.39	130.206.1.2	DNS	76	Standard query A www.elmundo.es
4	0.272703	130.206.1.2	192.168.1.39	DNS	230	Standard query response
5	0.273260	192.168.1.39	193.110.128.51	DNS	76	Standard query A www.elmundo.es
6	0.365443	193.110.128.51	192.168.1.39	DNS	290	Standard query response A 193.110.128.199



Host: **e.root-servers.net.**  
Alabama  
National Aeronautics and Space Association



Host: **sun.rediris.es.**  
Madrid  
RedIris



Hostname: **dns02.elmundo.es.**  
Madrid  
Unidad Editorial S.A



# Registros de Recursos

La información de los servidores DNS se almacena en sus **ficheros de zona**. Estos ficheros se componen de **Registros de Recursos**.

Propietario	TTL	Clase	Tipo	RDATA
WWW		IN	A	45.213.26.95

**Propietario:** nombre de host o del dominio DNS al que pertenece este recurso. Puede contener el símbolo "@" que representa el nombre de la zona que se está describiendo) o una cadena vacía (equivale al propietario del registro anterior).

**TTL:** (Time To Live) Tiempo de vida, generalmente expresado en segundos, que un servidor DNS o un resolver debe guardar en caché esta entrada antes de descartarla.

**Clase:** define la familia de protocolos en uso. Suele ser "IN" (de internet)

**Tipo:** identifica el tipo de registro.

**RDATA:** los datos del registro de recursos.



# Tipos de registros de recursos

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

# Ejemplo de fichero de zona

**\$TTL 86400**

Tiempo de vida por defecto de los registros del servidor.

```
@    IN    SOA    ns1.papafrita.test.  hostmaster.papafrita.test. (
                                           2001062501 ; serial
                                           21600    ; refresh
                                           3600     ; retry
                                           604800   ; expire
                                           86400    ) ; TTL
```

SOA

@	IN	NS		ns1.papafrita.test.
@	IN	NS		ns2.papafrita.test.
@	IN	MX	10	mail.papafrita.test.
@	IN	MX	20	mail2.papafrita.test.
@	IN	A		10.0.1.5
server1	IN	A		10.0.1.5
server2	IN	A		10.0.1.7
ns1	IN	A		10.0.1.2
ns2	IN	A		10.0.1.3
ftp	IN	CNAME		server1
mail	IN	CNAME		server1
mail2	IN	CNAME		server2
www	IN	CNAME		server2

Servidores dns. Cada dominio debe tener 2 para poder registrarse

Servidores de correo

Direcciones de todas las máquinas del dominio, incluidos los servidores que se definieron antes. Cuando un nombre no se termina con un ".", se sobreentiende que se completa con el nombre de dominio.

Alias



# Principales Registros de Recursos

**Registro SOA:** Registro de “Start of Authority”. Este registro indica la dirección del servidor principal de esa zona y datos relativos a la forma en la que se sincronizan los secundarios con el primario. Debe ser el primero en todo fichero de zona y debe estar siempre. Ejemplo:

**papafrita.est. SOA ns1.papafrita.test. master.papafrita.test. (**  
**2012022301 ; serial YYYYMMDDnn**  
**86400 ; tiempo de refresco ( 24 horas)**  
**7200 ; reintento ( 2 horas)**  
**3600000 ; caducidad (1000 horas)**  
**172800 ) ; TTL de respuesta negativa(2días)**

**papafrita.test.** indica el nombre del dominio que definimos. Se puede sustituir por @.

**ns1.papafrita.test.** Indica el servidor principal de la zona que estamos definiendo.

**master.papafrita.test** indica la dirección de correo electrónico del administrador

# Principales Registros de Recursos

**Registro NS:** El registro de recursos NS (Name Server) indica los servidores de nombres autorizados para la zona, tanto los servidores principales como los secundarios. Por tanto, cada zona debe contener, como mínimo, un registro NS.

**papafrita.test. IN NS ser1.papafrita.test.**

**IN NS ser2.papafrita.test.**

Si se deja en blanco el primer campo de un registro, significa que nos referimos al dominio que describe la zona. En este caso *papafrita.test*.



# Principales Registros de Recursos

**Registro A:** El tipo de registro de recursos A (Address) asigna un nombre de dominio completamente cualificado (FQDN) a una dirección IP, para que los clientes puedan solicitar la dirección IP de un nombre de host dado.

**ns1.papafrita.test. IN A 13.16.5.12**

Cuando no ponemos el “.” final, se completa con el nombre de dominio de nuestra zona, en este caso papafrita.test. El registro anterior y este de debajo son equivalentes.

**ns1 IN A 13.16.5.12**

# Principales Registros de Recursos

**Registro A:** El tipo de registro de recursos A (Address) asigna un nombre de dominio completamente cualificado (FQDN) a una dirección IP, para que los clientes puedan solicitar la dirección IP de un nombre de host dado.

**ns1.papafrita.test. IN A 13.16.5.12**

Cuando no ponemos el “.” final, se completa con el nombre de dominio de nuestra zona, en este caso papafrita.test. El registro anterior y este de debajo son equivalentes.

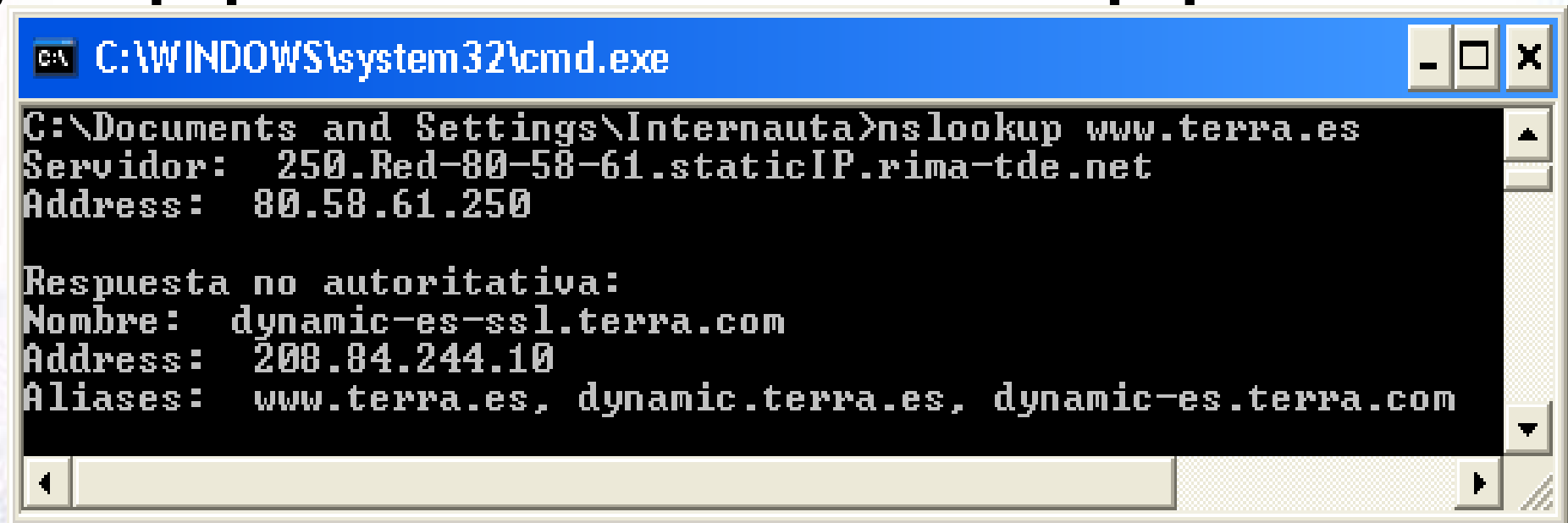
**ns1 IN A 13.16.5.12**



# Principales Registros de Recursos

**Registro CNAME:** El registro de nombre canónico (CNAME, Canonical NAME) crea un alias para el nombre de dominio especificado. Permiten dar varios nombres a la misma máquina y facilitan el mantenimiento de la zona ya que cuando haya que cambiar de ip una máquina solo tocamos un registro A y los cname se mantienen igual.

**grelo.papafrita.test. IN CNAME sr1.papafrita.test.**



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Internauta>nslookup www.terra.es
Servidor: 250.Red-80-58-61.staticIP.rima-tde.net
Address: 80.58.61.250

Respuesta no autoritativa:
Nombre: dynamic-es-ssl.terra.com
Address: 208.84.244.10
Aliases: www.terra.es, dynamic.terra.es, dynamic-es.terra.com
```

# Principales Registros de Recursos

**Registro MX:** El registro de recurso de intercambio de correo (MX, *Mail eXchange*) especifica un servidor de intercambio de correo para un nombre de dominio. Puesto que un mismo dominio puede contener diferentes servidores de correo, el registro MX puede indicar un valor numérico que permite especificar el orden en que los clientes deben intentar contactar con dichos servidores de correo.

**@ IN MX 0 correo.papafrita.test.**



# Principales Registros de Recursos

**Registro SRV:** Los registros de recurso de servicio (SRV, *SeRVice*) permiten especificar de forma genérica la ubicación de los servidores para un servicio, protocolo y dominio DNS determinados. El formato de un registro SRV es el siguiente:

**servicio.protocolo.nombre TTL clase SRV prioridad peso puerto destino**

Para el servidor de http del dominio *papafrita.test* sería

**http.tcp.papafrita.test. IN SRV 0 0 80 www1.papafrita.test.**

**http.tcp.papafrita.test. IN SRV 1 0 0 80 www2.papafrita.test.**

# Principales Registros de Recursos

**Registro PTR:** El registro de recursos PTR (PoinTeR), realiza la acción contraria al registro de tipo A, es decir, asigna un nombre de dominio completamente cualificado a una dirección IP.

**12.5.16.13.in-addr.arpa. IN PTR ser1.papafrita.test.**

O también

**12.5.16 IN PTR ser1.papafrita.test.**



# Comandos relacionados con DNS

**ping** como siempre nos permite saber si tenemos acceso a una máquina y si está encendida, de paso nos da su IP.

**nslookup** permite hacer consultas a los servidores dns, tanto directas como inversas.

**host** permite hacer búsquedas en DNS. Puede convertir nombres en direcciones y viceversa.

**dig** permite hacer consultas a servidores DNS, habitualmente para detectar problemas de configuración. Nos muestra los registros de recursos del servidor.