

UD3. Sistema de Nombres de Dominio. (DNS)



Despliegue de Aplicaciones Web
2º DAW

ÍNDICE

- INTRODUCCIÓN
- ¿QUÉ ES DNS?
- SISTEMA DE NOMBRES DE DOMINIO
 - DOMINIOS
 - ZONAS / DELEGACIÓN
 - FUNCIONAMIENTO
- BASES DE DATOS
- SERVIDORES DE NOMBRES
- DELEGACIÓN DE DOMINIO / GLUE RECORDS

1. INTRODUCCIÓN

- En una red **TCP/IP** las máquinas se **identifican** mediante una **dirección IP**.
- En **redes pequeñas** podríamos recordar todas las IP's asignadas a cada máquina.
 - ¿Cuántas direcciones somos capaces de memorizar?
 - Los nombres **son fáciles de recordar**

74.125.29.101 → GOOGLE.COM



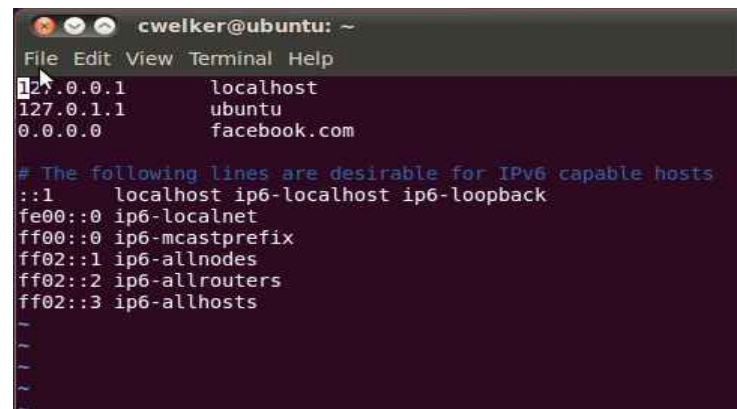
1. INTRODUCCIÓN

- Inicialmente, en **ARPANET**, se utilizaba un archivo `hosts.txt`, en el que se listaban todos los hosts y sus direcciones IP.
- Todas las **noches**, los **hosts conectados** a la red **obtenían** este **archivo** del sitio en el que se mantenía.
- Cuando **miles de hosts** se conectaron a la red se dieron cuenta de que **este método no podría funcionar**.

1. INTRODUCCIÓN

- Inconvenientes
 - El **tamaño** del archivo crecía de forma **considerable**.
 - Genera **mucho tráfico** en el servidor.
 - **Inconsistencias** entre copias locales / centrales.
 - **Duplicidad y conflictos** de nombres.

Actualmente se dispone del archivo **hosts** para su **uso local** tanto en sistemas operativos **unix, like-unix y windows**



```
cwelker@ubuntu: ~  
File Edit View Terminal Help  
127.0.0.1    localhost  
127.0.1.1    ubuntu  
0.0.0.0      facebook.com  
  
# The following lines are desirable for IPv6 capable hosts  
::1          localhost ip6-localhost ip6-loopback  
fe00::0      ip6-localnet  
ff00::0      ip6-mcastprefix  
ff02::1      ip6-allnodes  
ff02::2      ip6-allrouters  
ff02::3      ip6-allhosts
```

2. ¿QUÉ ES DNS?

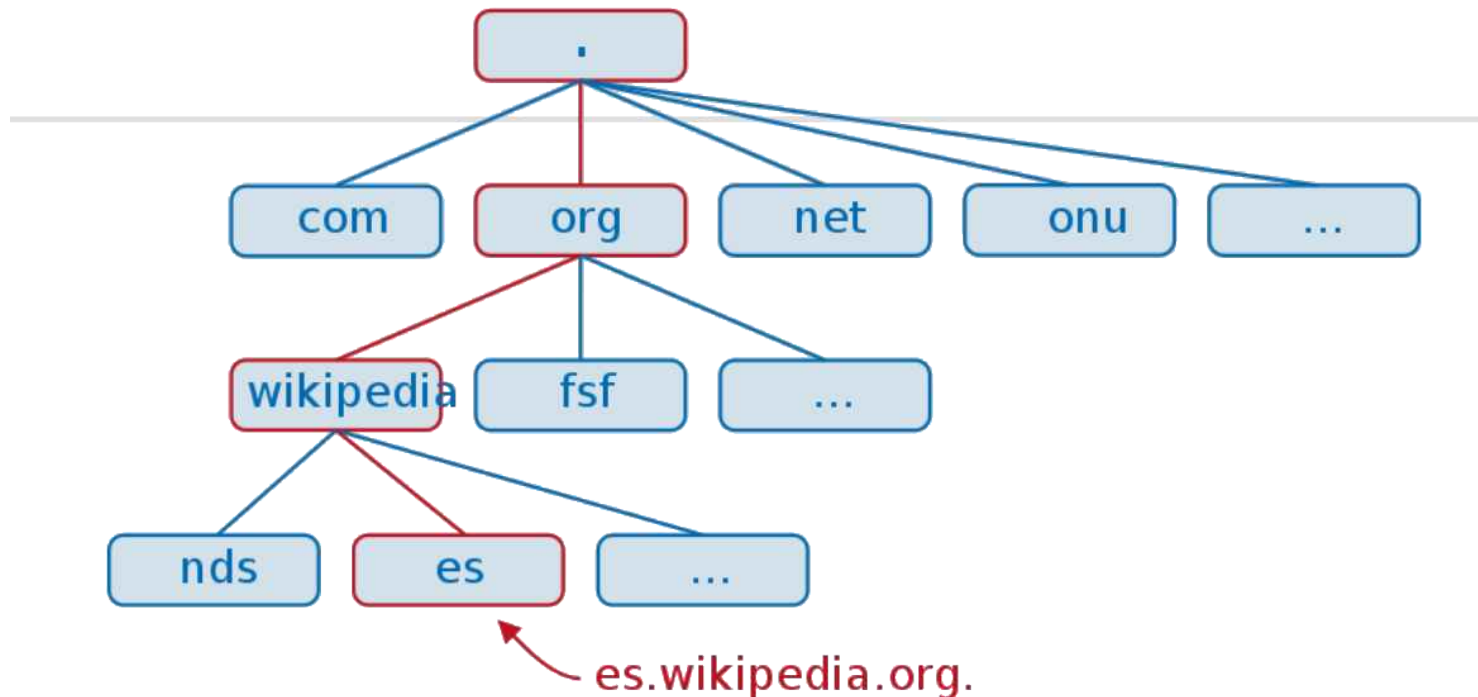
- **DNS** (Domain Name Server) o servidor de nombres de dominio proporciona un mecanismo de **traducción** de **nombres de dominio** en **direcciones IP** y viceversa.



¿Qué página se obtiene al acceder a la ip
164.132.156.96?

2.1 ESTRUCTURA Y FUNCIONAMIENTO

- Se trata de un **esquema de nombres jerárquico** que permite asignar nombres, basándose en el **concepto de dominio** y utilizando para su gestión una **base de datos distribuida**.

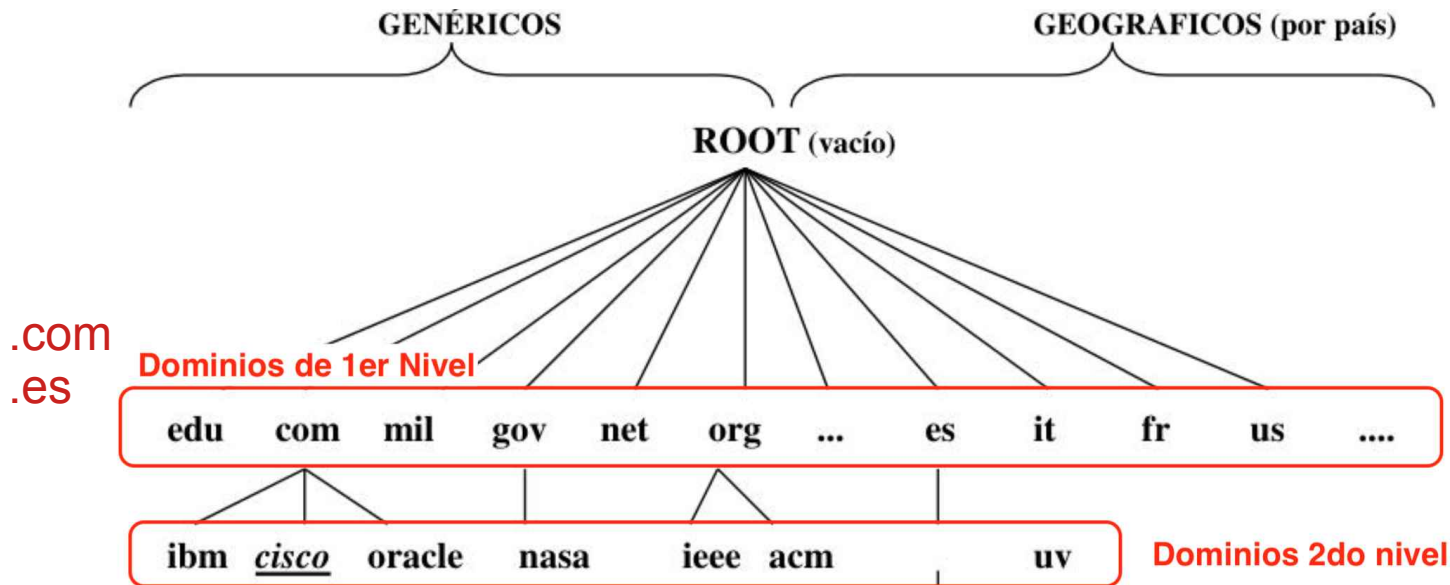


2.1 ESTRUCTURA Y FUNCIONAMIENTO

- Los nombres se organizan **jerárquicamente** en forma de árbol.
- El **nombre de dominio** correspondiente a cada nodo se define como la **secuencia** formada por las **etiquetas** de ese **nodo hasta el nodo raíz**, separados por un "." (camino).
- El **nodo raíz**, contiene una etiqueta vacía, por lo que todo dominio termina con un "."

3. SISTEMA DE NOMBRES DE INTERNET

- El **espacio de nombres** en Internet se divide en diferentes **dominios de nivel superior** (TLD).
- Cada uno de estos **dominios** se **divide** en **subdominios**, y estos, a su vez, también se subdividen.

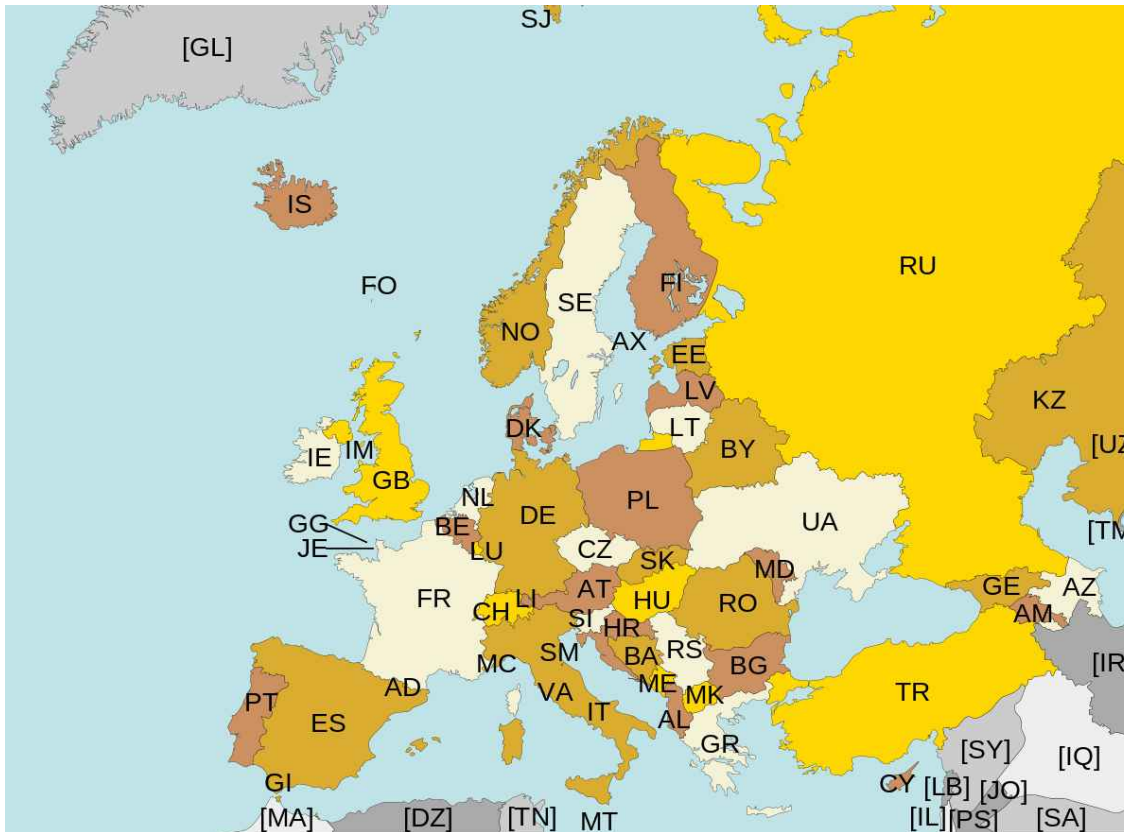


3.1 DOMINIOS DE NIVEL SUPERIOR (TLD)

- Los dominios de **nivel superior** o **TLD** (top-level domain) se dividen en dos categorías:
 - **Genéricos:** División por tipo de organización; **.com** (comercial), **edu** (instituciones educativas), **info** (información), **name** (nombres de personas) y **pro** (profesiones, como internacionales), **mil** (fuerzas armadas de Estados Unidos), **net** (proveedores de red) y **.org** (organizaciones no lucrativas)...
 - **De país:** incluyen una entrada para cada país, como se define en la **ISO 3166**; **.es** (españa), **it** (italia), **fr** (francia),...

3.1 DOMINIOS DE NIVEL SUPERIOR (TLD)

- **ISO 3166** - 2 caracteres



www.gva.es



TLD

3.2 NOMBRES DE DOMINIO

Nombres de dominio

- No distinción entre **mayúsculas** y **minúsculas**
- Cadena de hasta **255 caracteres**, formada por **etiquetas** (≤ 63 caracteres)

ddaw.cipfpbatoi.es

3 etiquetas → ddaw cipfpbatoi es

3.2 NOMBRES DE DOMINIO

- Los nombres de dominio pueden ser absolutos y relativos

- **Absoluto o FQDN (Fully Qualified Domain Name):**
Constituye el nombre de dominio completo de una red.

ddaw.cipfpbatoi.es .



Siempre termina
en “.”

- **Relativo o PQDN (Partial Qualified Domain Name):**
solo especificamos la parte del host relativa a un dominio:

ddaw (.cipfpbatoi.es.)

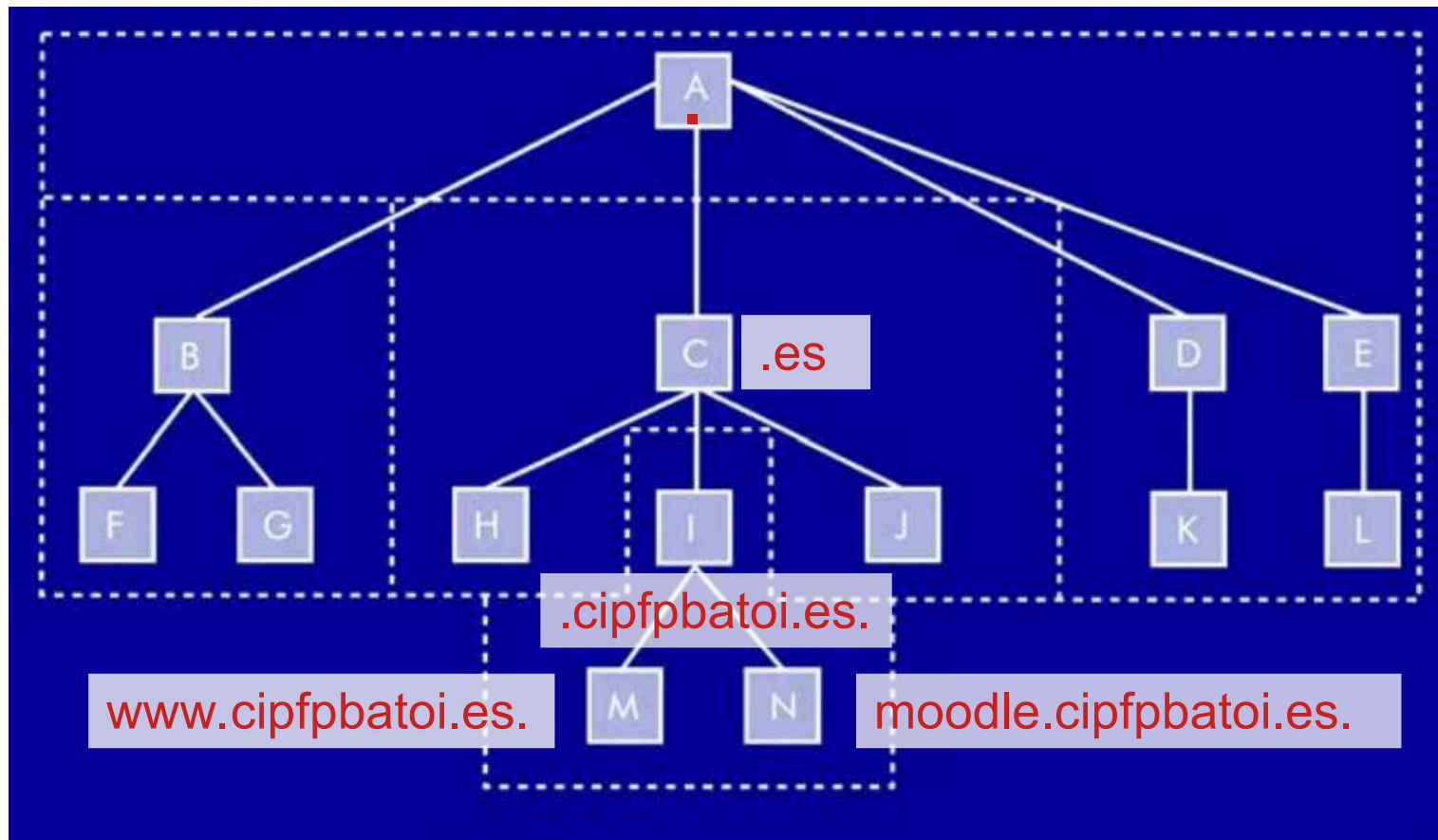
3.3 ESPACIO DE NOMBRES

Zonas y delegación

- El **espacio de nombres** de dominio se **divide** en **zonas**.
 - Cada una de las zonas se encuentra bajo el **control administrativo** de una organización.
 - La **responsabilidad** es **delegada** por la **organización** que se encuentra en el **nivel superior**.

3.3 ESPACIO DE NOMBRES

Zonas y delegación



3.3 ESPACIO DE NOMBRES

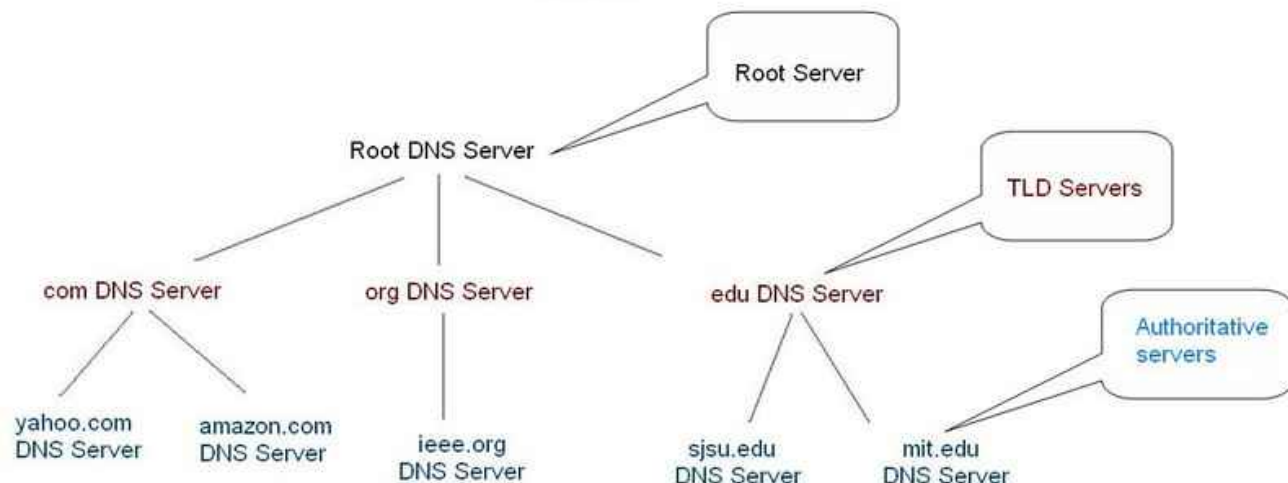
Zonas y delegación

- Los dominios de **nivel superior** son asignados por **IANA** (*Internet Corporation for assigned Names*).
 - La creación de nuevos nombres y su asignación es administrado por **ICANN** (Assigned Numbers Authority).
 - <http://www.iana.org/domains/root/db>
- **ICANN delega** automáticamente la responsabilidad de los **dominios geográficos** en instituciones locales de cada país.
 - España → **red.es**

3.3 ESPACIO DE NOMBRES

Zonas y delegación

- La **empresa u organización** responsable de cada zona puede:
 - Añadir o **quitar nodos** dentro de su zona.
 - **Modificar la información** de sus nodos.
 - Crear **nuevas sub-zonas** y **delegar su gestión** en otras autoridades administrativas.



3.3 ESPACIO DE NOMBRES

Zonas y delegación

- Ejemplos:
 - **Red.es** → **delega** la zona **CIPFPBatoi.es** en los servidores DNS del centro educativo.
 - **CIPFPBatoi** → **delega** la zona **mail.cipfpbatoi.es** en los servidores DNS de una empresa de envío de correos; *mailchimp, dr.sender...*
 - **CIPFPBatoi** → Crea nuevos nodos que corresponden a:
 - www.cipfpbatoi.es
 - moodle.cipfpbatoi.es
 - Intranet.cipfpbatoi.es

3.3 ESPACIO DE NOMBRES

Zonas y delegación

- En la parte superior de la jerarquía, existen **13 servidores** que comparten la responsabilidad de las **zonas de nivel superior**.
- De esta forma **se evita** que el servidor raíz se convierta en el **cuello de botella**.
- Algunos de los **servidores raíz** se implementan mediante **múltiples servidores geográficamente distantes**

3.3 ESPACIO DE NOMBRES

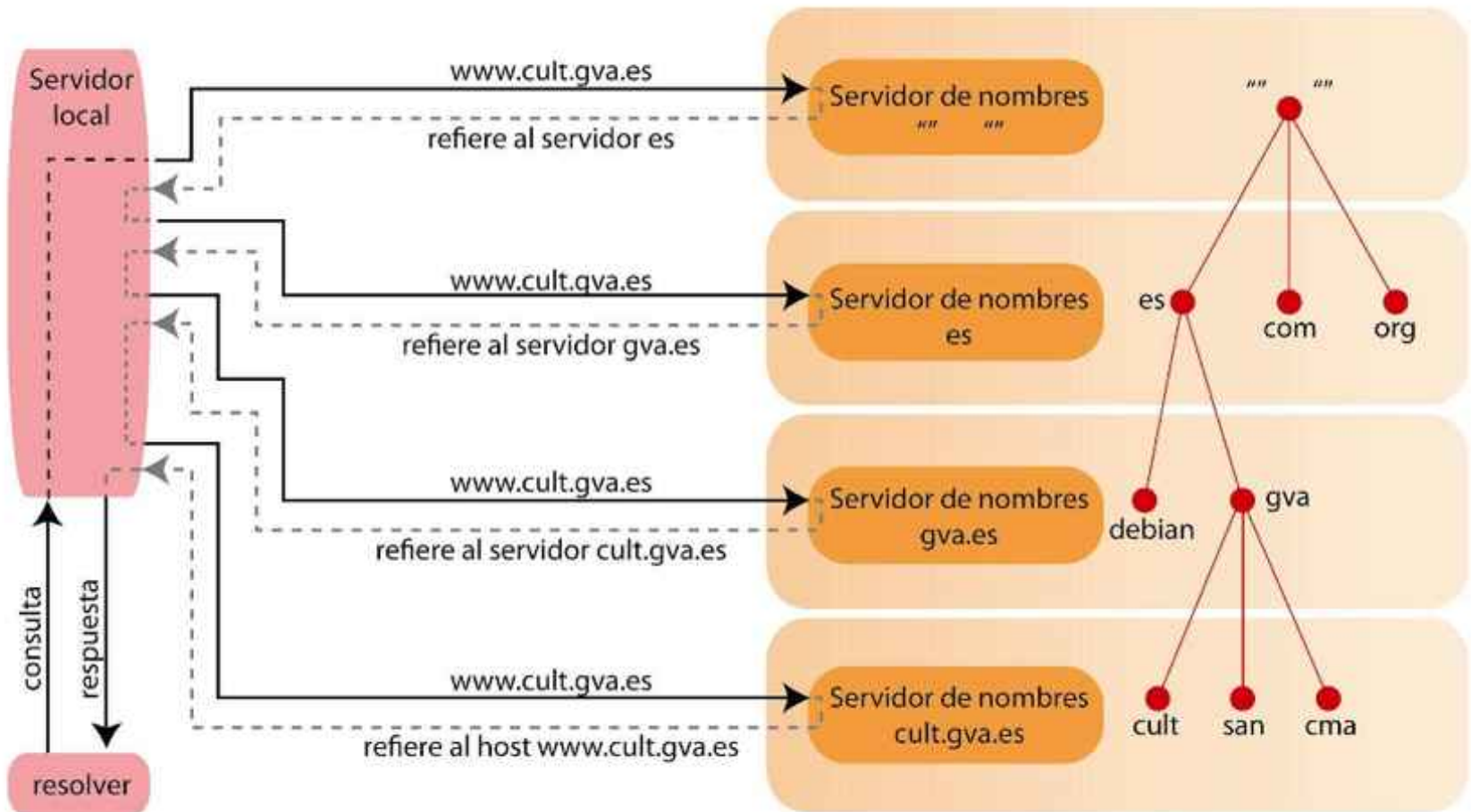
Zonas y delegación



3.4 FUNCIONAMIENTO

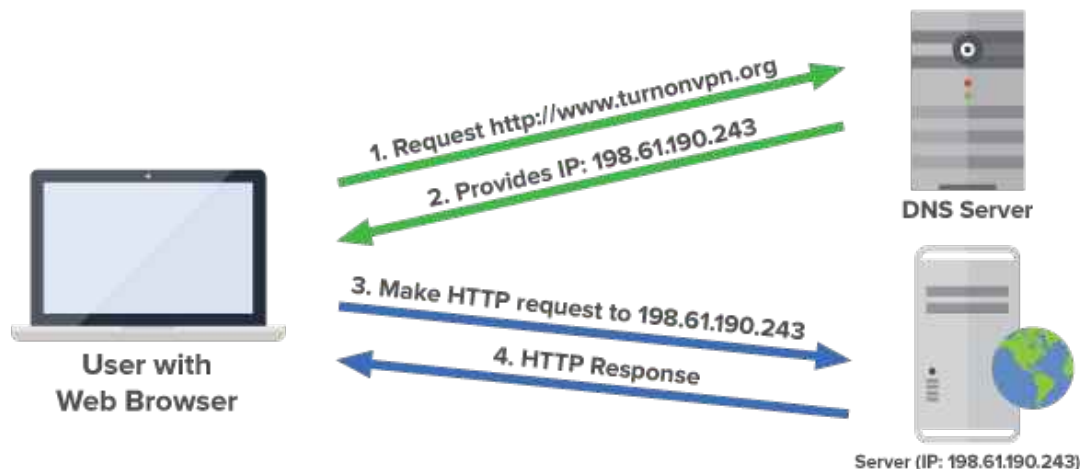
- La resolución de una nombre a una dirección IP requerirá los siguientes pasos:
 1. El programa de aplicación llama a un procedimiento de biblioteca (**resolver**) residente en el sistema operativo y le pasa el **nombre de dominio**.
 2. El **resolver** envía un **paquete UDP** al servidor **DNS configurado**.
 - a) Si el dominio recae sobre la jurisdicción del **servidor nombres**, éste devuelve una **respuesta autorizada** al resolver y éste a su vez se la pasa al programa de aplicación.
 - b) Si no se dispone de información, se debe **consultar** a los **servidores de nombres** de los niveles superiores.

3.4 FUNCIONAMIENTO



3.4 FUNCIONAMIENTO

- Para incrementar su eficiencia el sistema DNS utiliza una caché. Para informar de que la respuesta viene de memoria caché se marcará como **no autoritativa**.
- Para evitar que la información de la caché quede obsoleta, el **servidor DNS** proporciona junto a la respuesta un tiempo de vida (TTL) que define el tiempo en segundos que la información puede almacenarse en cache.



3.4 FUNCIONAMIENTO

- Cuando una consulta **no se encuentra** en el servidor local, existen 2 formas de generar la respuesta:
 - **Modo recursivo:** El propio **servidor** se ocupa de realizar **consultas** recursivas a **otros servidores** y solo **devolver** la **respuesta final** o un error (en caso de encontrarla).
 - **Modo interactivo:** La **respuesta únicamente** incluye una **referencia** al **servidor** que puede proporcionar **más información**. *(El cliente debe preocuparse de continuar realizando consultas hasta encontrar la que busca).*

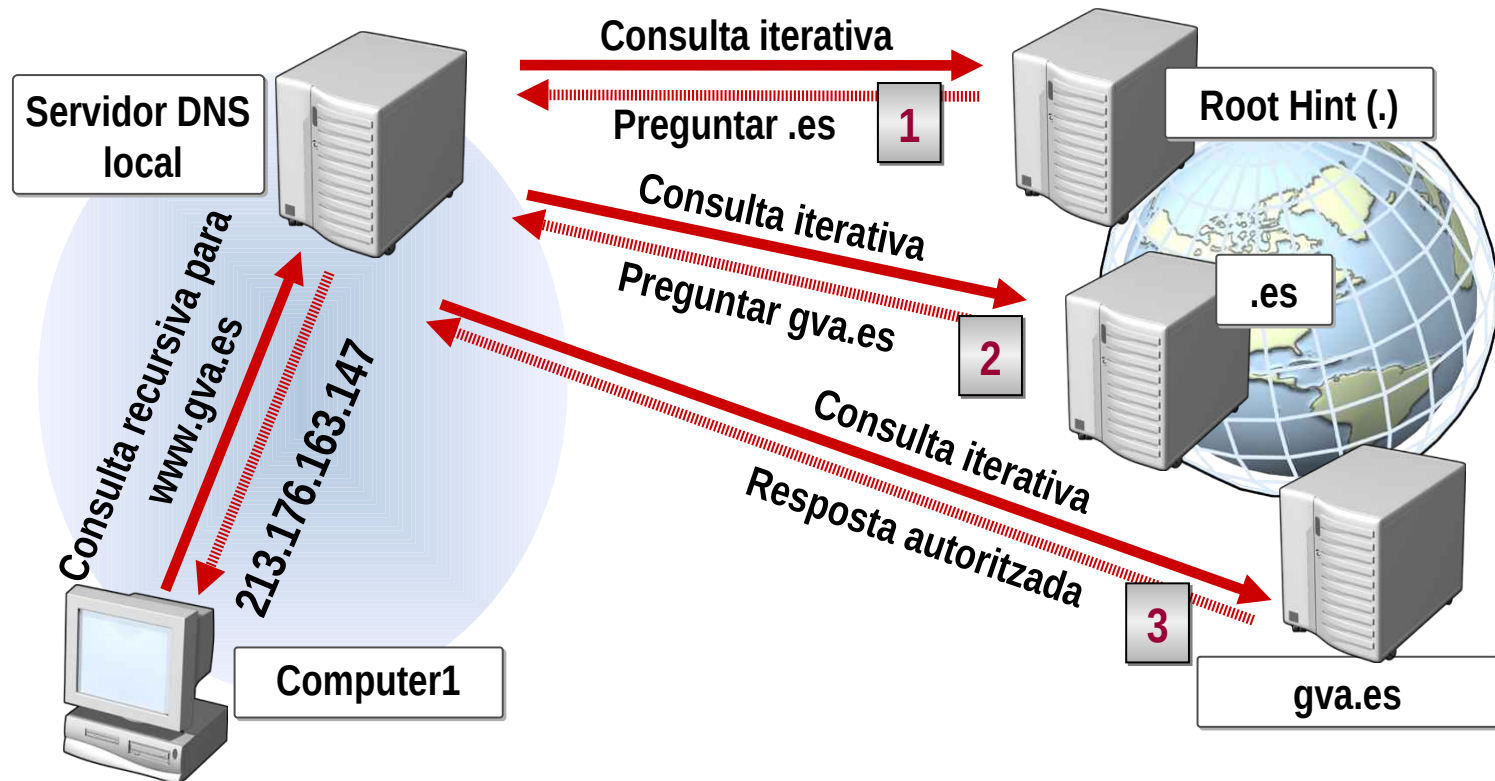
3.4 FUNCIONAMIENTO

- **Modo recursivo**



3.4 FUNCIONAMIENTO

- Modo interactivo



4. BASE DE DATOS

Resolución *inversa/directa*

- Los servidores DNS mantienen **2 base de datos** en **ficheros distintos** sobre una **misma zona**:
 - **Zona de traducción directa**: Obtención de la dirección **IP** a partir del **nombre de dominio** (*Acceso a una web a través del navegador,...*)
 - **Zona de resolución inversa**: Obtención del nombre de dominio a partir de la IP. (Autenticación de correos electrónicos,...)
 - Utilizan un dominio especial **in-addr-arpa** (*121.45.34.123.in-addr-arpa*)

4. BASE DE DATOS

Registro de Recursos

- Cada una de estas **bases de datos**, esta compuesta por un **conjunto de entradas** a las que denominamos **registro de recursos (RR)**
- Un registro de recursos se compone de:

Nombre de dominio	TTL	Clase	Tipo	Valor
moodle.cipfpbatoi.es	600	IN	A	147.156.167.210

TTL: Tiempo de vida.(Segundos)

Clase: Actualmente solo se utiliza IN (redes TCP/IP)

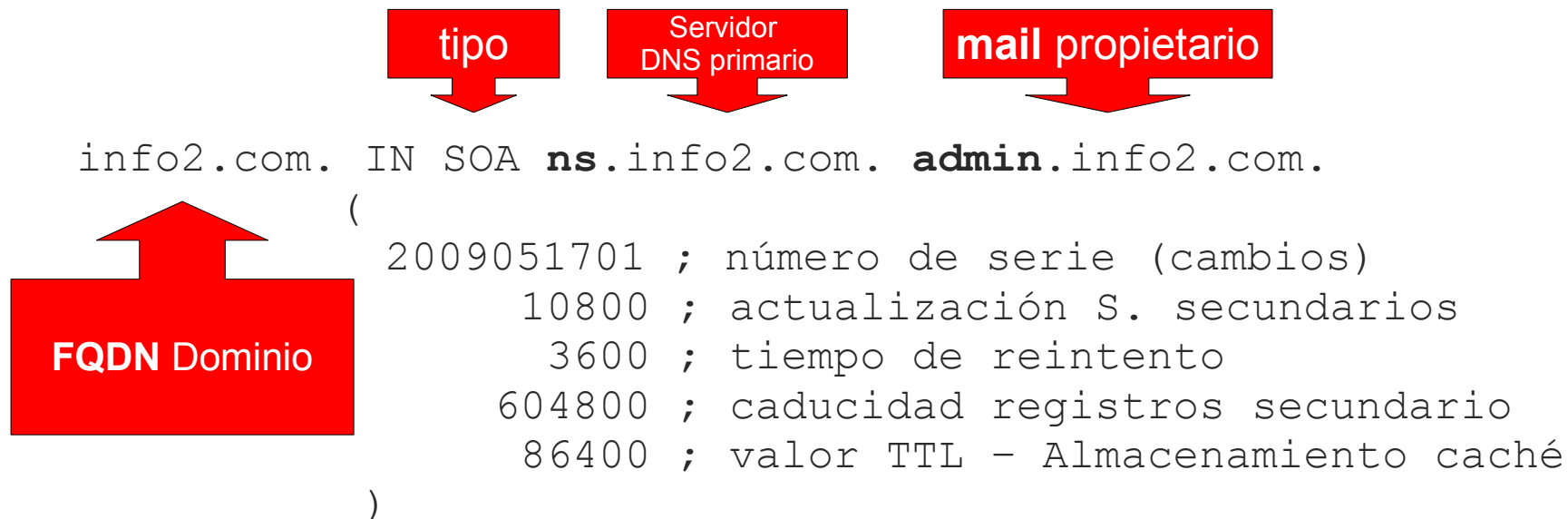
Tipo: Indica la funcionalidad del registro

Dato_Registro (Valor): Número o texto ASCII dependiendo del tipo de registro

4. BASE DE DATOS

Tipos de Registros

- **Registro SOA:** La configuración de cada zona comienza con el SOA (Start Of Authority).



Todos estos valores pueden indicarse en segundos o utilizando meta-carácteres para representar a las unidades de tiempo. Por ejemplo, **1W2D5H10M** especifica: 1 semana (**week**), 2 días (**day**), 5 horas (**hour**) y 10 minutos (**minute**).

4. BASE DE DATOS

Tipos de Registros

- **NS (Name Server):** Establece los servidores de nombres autorizados para la zona.

info2.com. IN NS servidor.info2.com.

Debe contener registros indicando tanto los servidores primarios como los secundarios

4. BASE DE DATOS

Tipos de Registros

- **A (Address):** Establece una correspondencia entre un nombre de dominio completamente cualificado (FQDN) y una dirección IP.

```
pc11.info2.com.    IN      A      192.168.2.100
```

- **PTR (PoinTeR, puntero):** Hace lo contrario que el registro A: asigna una dirección IP a un nombre de dominio completamente cualificado. Este tipo de recursos se utilizan en la resolución inversa.

```
1.2.168.192.in-addr.arpa  IN  PTR      pc11.info2.com.
```

4. BASE DE DATOS

Tipos de Registros

- **CNAME** (Canonic NAME, nombre canónico): crea un alias para el nombre de dominio especificado. Se asigna a un host que tiene una dirección IP válida y que responde a diversos nombres. Pueden declararse varios para un host.

```
prueba.info2.com. IN      CNAME  pc11.info2.com.
```

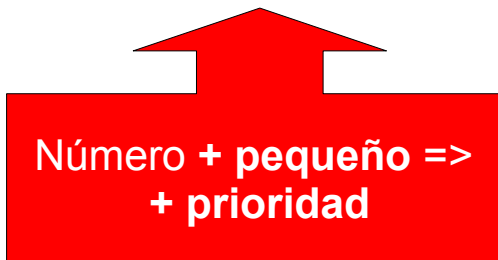
A la máquina pc11 se le asigna el alias «prueba»:

4. BASE DE DATOS

Tipos de Registros

- **MX** (Mail eXchange, intercambio de correo): Indica una o varias máquinas encargadas de la entrega de correo en el dominio. Si este posee varias máquinas como registros MX se puede indicar, mediante un valor numérico, el orden de preferencia

info2.com. IN MX 0 mail.info2.com.



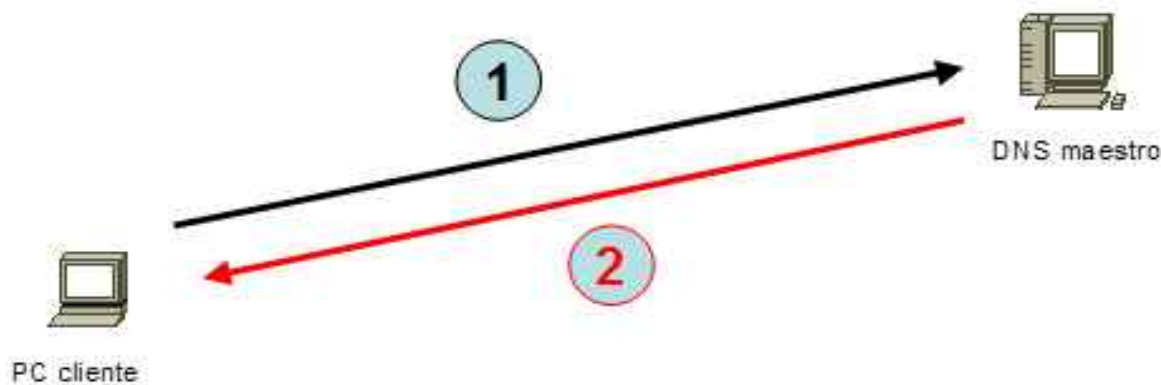
5. CLIENTES DNS

- Un **cliente DNS** es un programa que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS.
 - Se conocen como **Resolvers**
 - *Ej. Un navegador es una aplicación que hace llamadas al resolver del Sistema operativo para obtener las IP's a las que dirigirse.*

5. SERVIDORES DE NOMBRES

Tipos

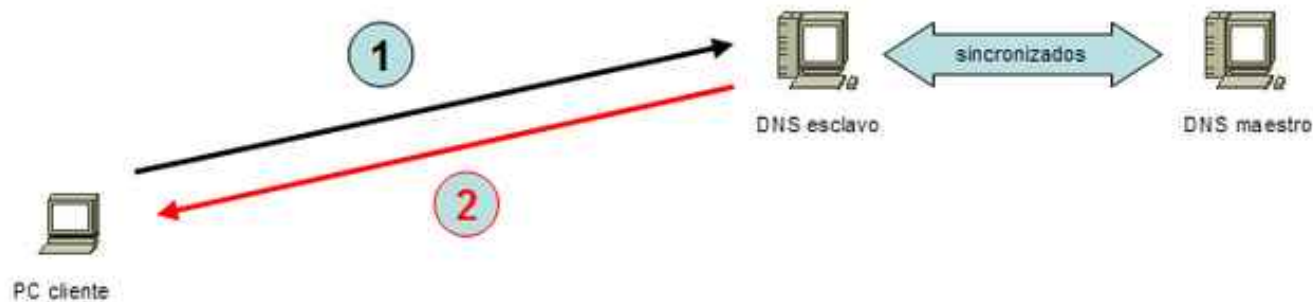
- Las especificaciones DNS definen dos tipos de servidores de nombres:
 - Servidores primarios o maestros:** lee los **datos** de la zona a partir de un **archivo** ubicado en el **mismo host**.



5. SERVIDORES DE NOMBRES

Tipos

- Servidores **secundarios** o **esclavos**: **obtiene** los **datos** de zona desde otro servidor de nombres autorizado para la zona, denominado servidor **maestro** o **primario**.

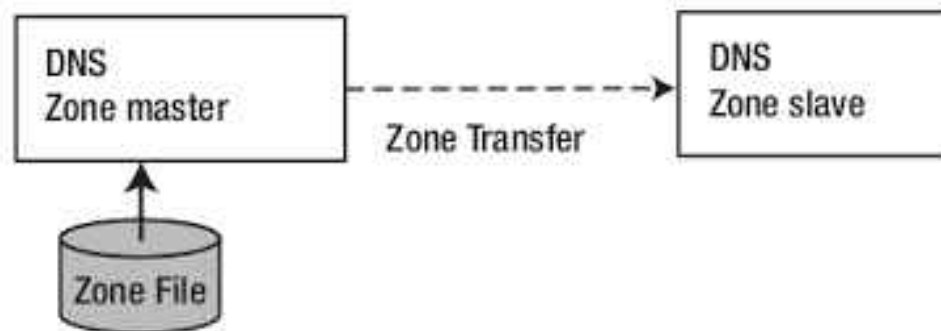


Cuando un **servidor secundario** se inicia, **contacta** con su **servidor maestro** y, si es necesario, descarga los datos sobre la zona. Esto se conoce como una **transferencia de zona**.

5. SERVIDORES DE NOMBRES

Tipos

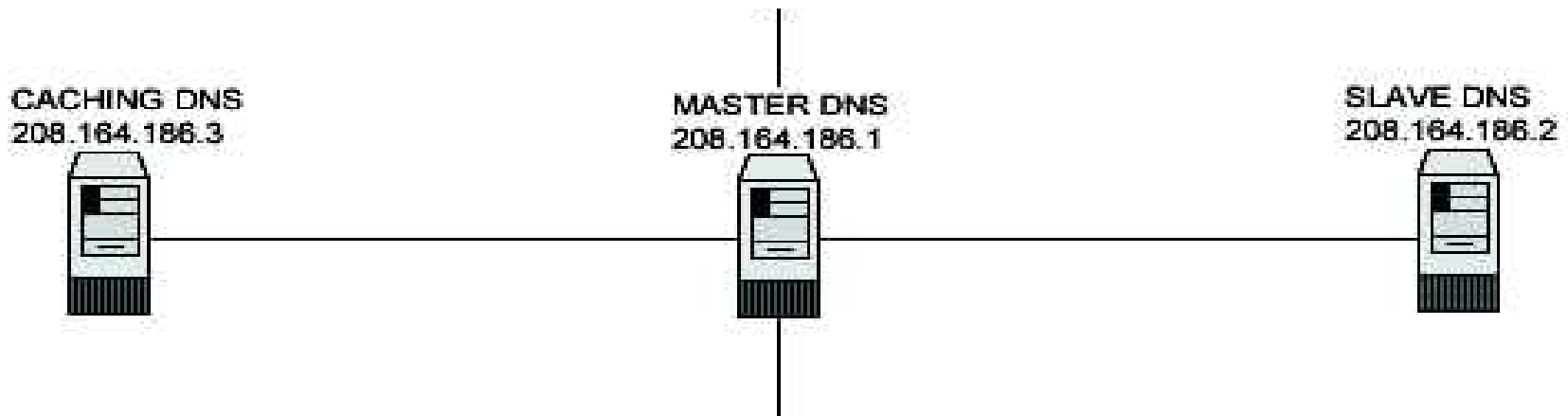
- Tanto el **servidor maestro** primario como los **esclavos** de una zona **están autorizados** para **dicha zona**.
- Los **archivos** que **cargan** los servidores **maestros**, se denominan **ficheros de zona**.
- Los **servidores esclavos**, normalmente, **respaldan los datos** que reciben mediante las **transferencias de zona** a un **fichero** de zona almacenado de forma **local**.



5. SERVIDORES DE NOMBRES

Tipos


- **Servidor DNS cache:** Solo atiende consultas de clientes DNS sobre nombres de dominios y almacena los resultados para posteriores usos. (*No mantiene configuración de zonas*)



6. DELEGACIÓN DE DOMINIOS

Registros glue

- Son registros o entradas de DNS necesarios para que un subdominio pueda actuar como servidor autoritativo de DNS para su dominio principal.
- Para realizar una **delegación de zona** se utilizan dos registros de recursos:
 - **Registro NS** → Proporciona el **FQDN** del **servidor** DNS de la zona.
 - **Registro A** → Asocia el **FQDN** con una **dirección IP**



Denominados **Registros Glue**
La zona padre
mantiene sobre la zona subordinada.

6. DELEGACIÓN DE DOMINIOS

Registros glue

- Ej. Si quisieramos **delegar** la **zona** `mail.info2.com` necesitaríamos introducir en el servidor DNS de la zona `info2.com` los siguientes registros:

```
mail.info2.com. IN NS ns.mail.info2.com.  
ns.mail.info2.com. IN A 1.2.3.4
```