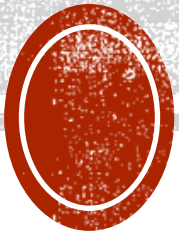
SERVICIOS DE NOMBRES DE DOMINIO (DNS)



OBJETIVOS

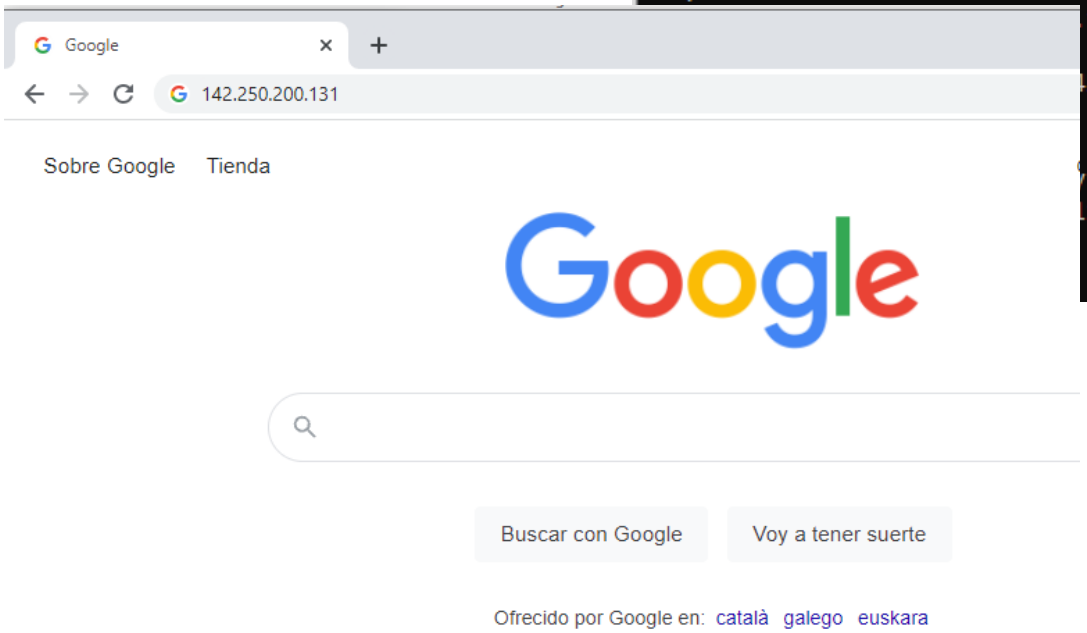
- Identificar y describir escenarios en los que surge la necesidad de un servicio de resolución de nombres
- Clasificar los principales mecanismos de resolución de nombres y describir la estructura, nomenclatura y funcionalidad de los sistemas de nombres jerárquicos.
- Instalar y configurar servicios jerárquicos de resolución de nombres, reenviar consultas de recursos externos a otro servidor de nombres y almacenar y distribuir las respuestas procedentes de otros servidores.
- Añadir registros de nombres correspondientes a una zona nueva, con opciones relativas a servidores de correo y alias y realizar transferencias de zona entre dos o más servidores.
- Implementar soluciones de servidores de nombres en direcciones IPs dinámicas
- Documentar los procedimientos de instalación y configuración

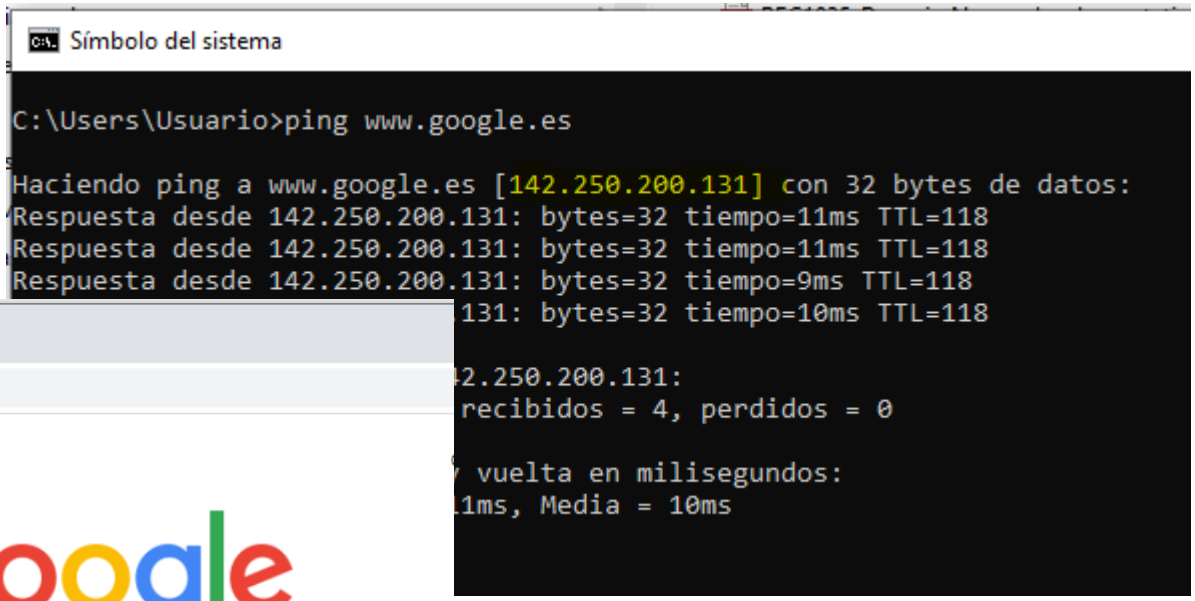
CONTENIDOS

- Introducción
  - Justificación
  - Historia
  - Características y utilidad
  - Funcionamiento
  - Componentes
  - Funcionamiento
- Espacios de nombres de dominio
  - Nombres de dominio
  - Dominio raíz. Subdominio
  - Nombres relativos y absolutos
  - Uso de nombres
  - Administración nombres de dominio
- Servidores de nombre
  - Zonas
  - Tipos
  - Servidor de nombre maestro y esclavo
  - Servidores de nombre caché
  - Servidor de nombre reenviador
  - Servidor de nombre autorizados
  - Servidor raíz
- Clientes
- Proceso de resolución
- Registros de recursos DNS
- Transferencia de zonas
- DNS Dinámico
- Seguridad

INTRODUCCIÓN

JUSTIFICACIÓN DE DNS





JUSTIFICACIÓN DE DNS

- En las redes TCP/IP son las direcciones IP las que identifican a los equipos.
- Las direcciones IP son números, mientras que a las personas les resulta más sencillo usar y recordar nombres.
- Para facilitar el uso de los servicios y recursos que ofrece una red, se han creado **sistemas de nombres** utilizados por **servicios de resolución de nombres** que permiten asociar nombres sencillos con direcciones numéricas.
- Ejemplo: ftp.uah.es se corresponde con la IP 193.146.56.125
- El principal servicio de resolución de nombres usado en TCP/IP es el servicio **DNS** (Domain Name System o Sistema de Nombres de Dominio).

Traducción de nombres a direcciones IP

JUSTIFICACIÓN DE DNS

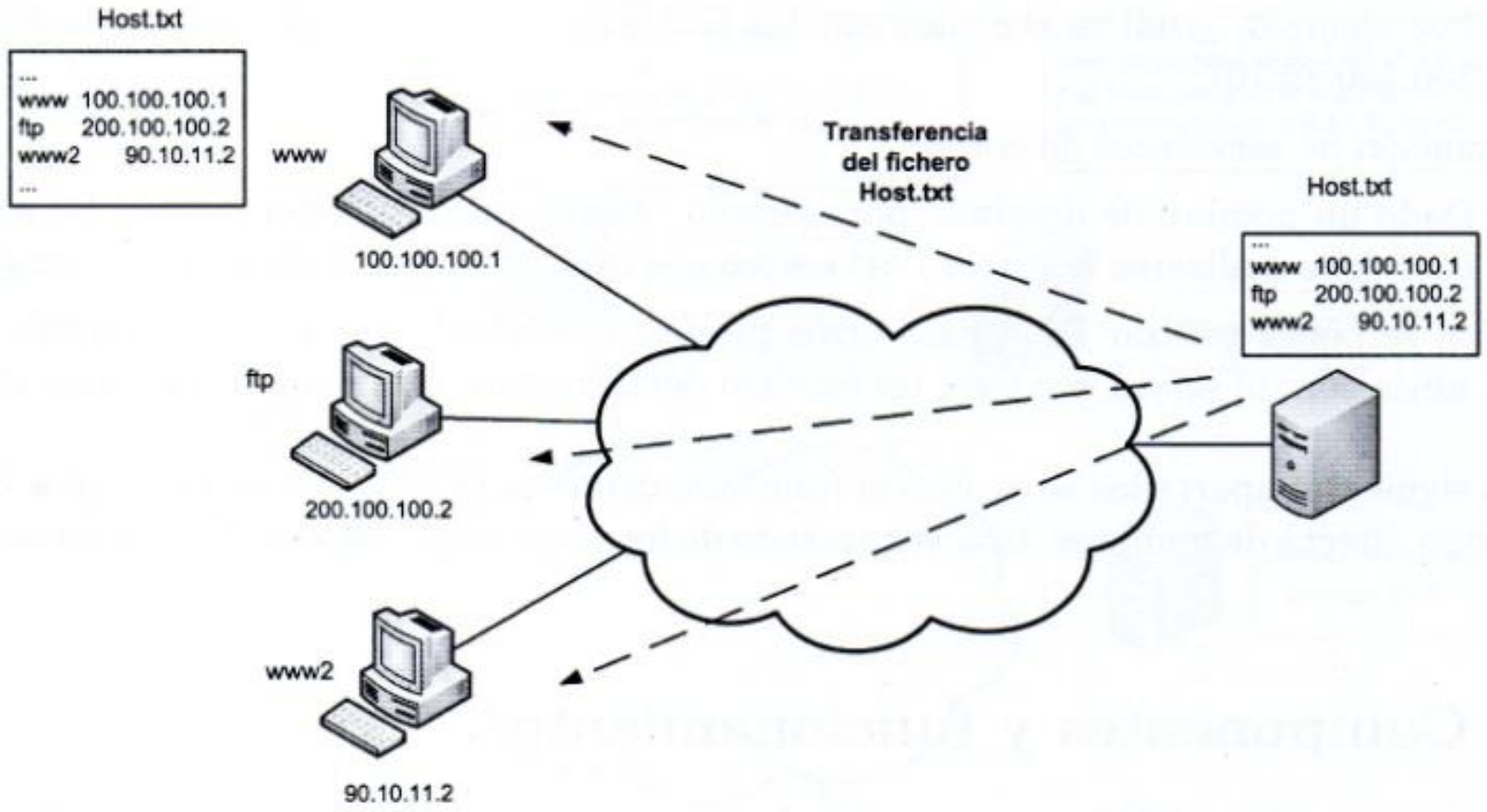
Puede utilizarse para referenciar servicios y otros elementos en el ámbito del nombre de dominio dependiendo del **tipo de registro**:

- A=> asociamos un nombre a una dirección IPv4
- AAA=> asociamos un nombre a una dirección IPv6
- CNAME => cuando hay varios nombres de dominio que apuntan a una única dirección IP
- NS => Especificación de los servidores DNS
- SRV => referencia un servicio (dominio) a un nombre de nuestra red
- MX => referencia los servidores de correo,
- PTR => resolución de IPv4 a un nombre de dominio

HISTORIA DE DNS

- En el comienzo de Internet, se usaba un sistema de nombres planos.
- La relación entre nombres de equipos (hosts) y direcciones IP se almacenaba en un archivo (**host.txt**) localizado en un servidor central. Los equipos de la red obtenían periódicamente por FTP el archivo y así podían usar los nombres que contenía.
- Inicialmente funcionaba bien, porque había pocos nombres y se actualizaba poco. A medida nº equipos en la red aumentaba:
  - Sobrecarga el servidor que contenía el fichero host por el aumento del tamaño y del tráfico.
  - Congestión de red por la descarga del fichero.
  - Probabilidad de duplicidad de nombres al usarse un sistema de nombres planos.
- Como alternativa, en 1983 se introduce DNS con características de escalabilidad, administración centralizada, velocidad, etc.

HISTORIA DEL DNS



Sistema de nombres basados en el archivo host.txt

CARACTERÍSTICAS Y UTILIDAD DEL SERVICIO DNS

- DNS ofrece un servicio de **almacenamiento y consulta de información**.

- **Descentralizado**. La información se guarda en una base de datos distribuida entre múltiples equipos (**servidores de nombres**) y se indexa según un esquema de nombres **jerárquico** (**espacio de nombres de dominio**).

- A los servidores de nombres se les pueden realizar preguntas y para ello, se usan programas (**clientes DNS**) que dialogan con los servidores en base a unas reglas (**protocolo DNS**).

CARACTERÍSTICAS Y UTILIDAD DEL SERVICIO DNS

- DNS puede almacenar **varios tipos de información** sobre cada **nombre de dominio** y por ello, se puede utilizar para diferentes propósitos. Lo habitual es asociar direcciones IP con nombres de dominio.
- Se utiliza para:
  - **Resolución de nombres (búsqueda directa):** Obtener información asociada a un nombre de dominio.
  - **Resolución inversa de direcciones (búsqueda inversa):** Inverso al anterior.
  - **Resolución de servidores de correo:** Dado un nombre de dominio, obtener el servidor a través del cual debe realizarse la entrega del correo electrónico.
  - También se puede utilizar para **otros propósitos:** balanceo de carga, obtención de claves públicas, ubicación de servidores para un servicio determinado, listas negras de spam,…

CARACTERÍSTICAS Y UTILIDAD DEL SERVICIO DNS

Domain Name System (RFC 1034 y 1035) incluye:

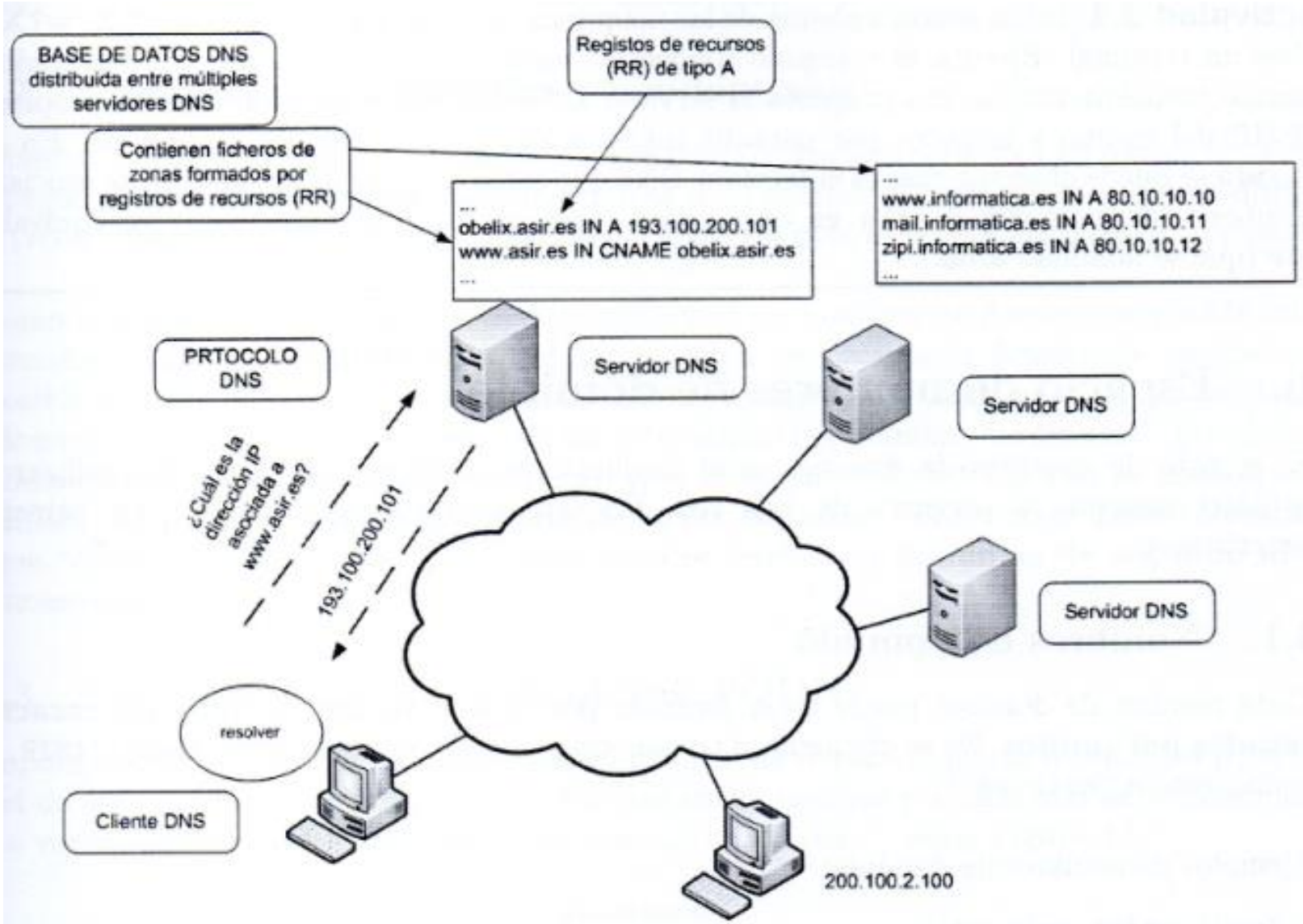
- Una sintaxis para los nombres
- Una base de datos distribuida implementada como una jerarquía de servidores de nombre
- Un protocolo de nivel de aplicación
  - Host, routers y servidores de nombre se comunican para resolver nombres

COMPONENTES

El servicio DNS se basa en los siguientes componentes:

- **Espacio de nombres de dominio (Domain Name Space):** Conjunto de nombres que se pueden utilizar para identificar máquinas o servicios de una red.
- **Base de datos DNS:** Base de datos distribuida y redundante que almacena información sobre los nombres de dominio. Esta base de datos se organiza en **zonas** que almacenan la información en lo que se conoce como **registros de recursos** (RR, Resource Records).
- **Servidores de nombres (name servers) o servidores DNS:** Programas que guardan parte de la base de datos DNS (zonas) y que responden a preguntas sobre la información almacenada.
- **Clientes DNS (resolvers):** Programas que realizan preguntas a los servidores de nombres y procesan las respuestas para ofrecerle la información a los usuarios y/o a las aplicaciones que los invocan.
- **Protocolo DNS:** Conjunto de normas y reglas en base a las cuales "dialogan" los clientes y servidores DNS.

COMPONENTES



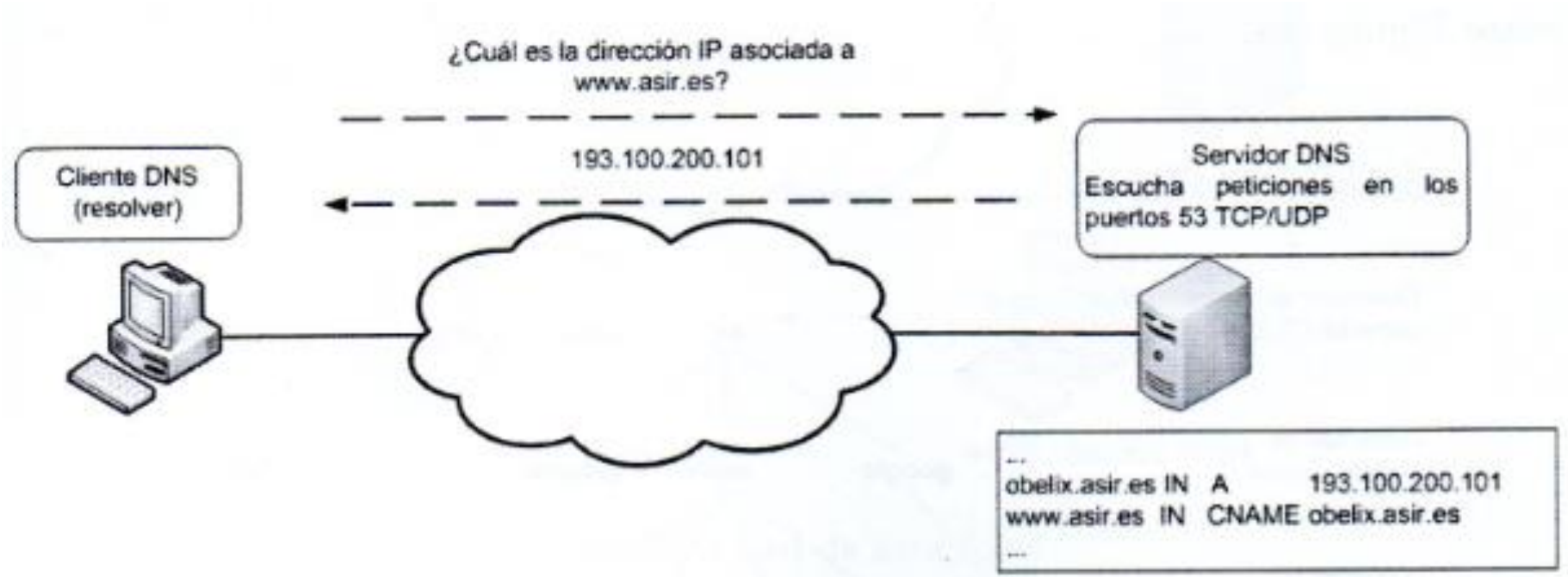
Componentes de un DNS

FUNCIONAMIENTO

Se basa en el **modelo cliente/servidor**:

- **Los clientes DNS (resolvers)** preguntan a los servidores de nombres.
- **Los servidores** de nombres también se comunican entre sí:
  - Pueden realizar preguntas a otros servidores de nombres cuando no tienen la información por la que le han preguntado.
  - Pueden intercambiar información sobre sus zonas (transferencias de zona).

FUNCIONAMIENTO



Funcionamiento servicio DNS

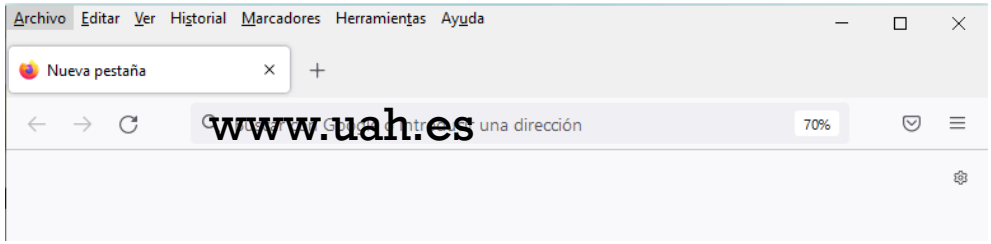
FUNCIONAMIENTO

- El DNS funciona como una guía telefónica, al encontrar el nombre de la persona puedes encontrar el teléfono y, entonces, realizar la llamada.

FUNCIONAMIENTO

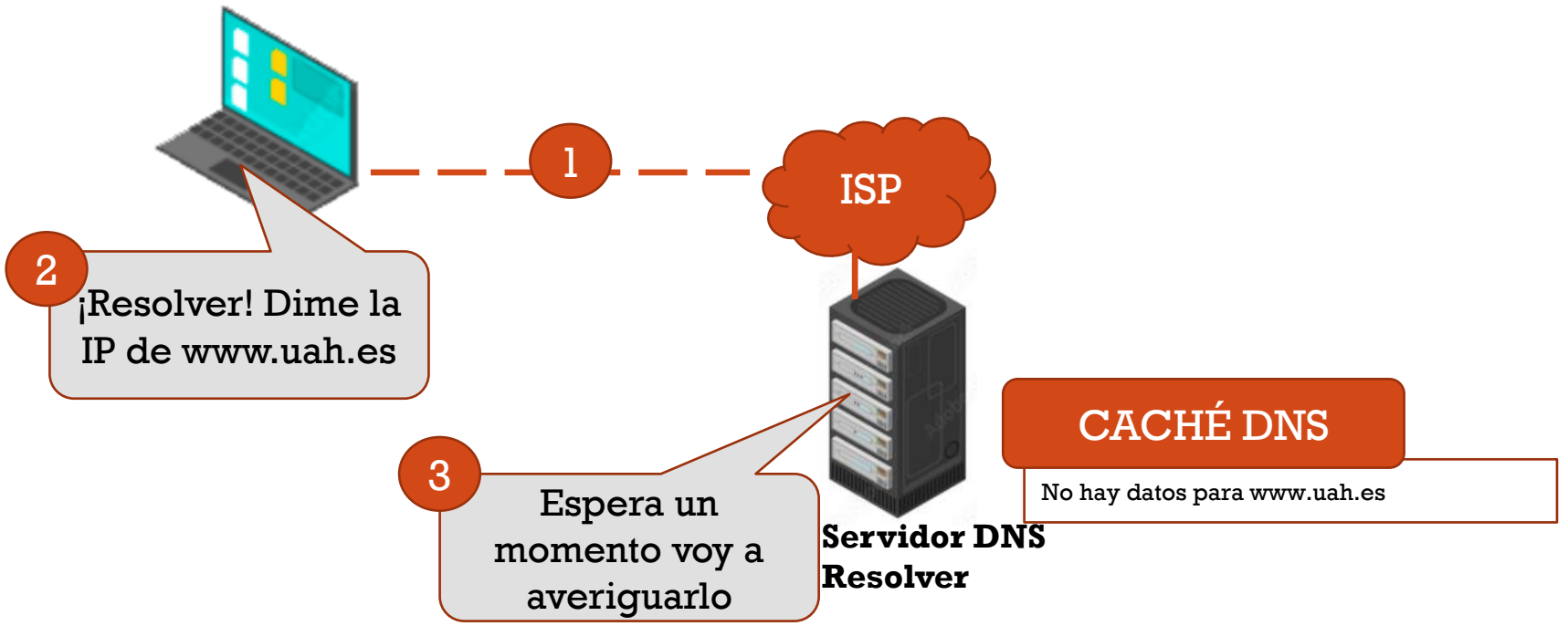
¿Qué sucede entre el ordenador y el servidor DNS cuando el primero intenta conectarse a una máquina utilizando el nombre en lugar de la dirección IP? Sea www.uah.es el nombre de la máquina con la cual se desea conectar.

FUNCIONAMIENTO



El usuario escribe en su navegador www.uah.es. El ordenador busca en su memoria caché si está la dirección IP de www.uah.es En este caso, es la primera vez y no hay datos. Por tanto, debe pedir ayuda

FUNCIONAMIENTO



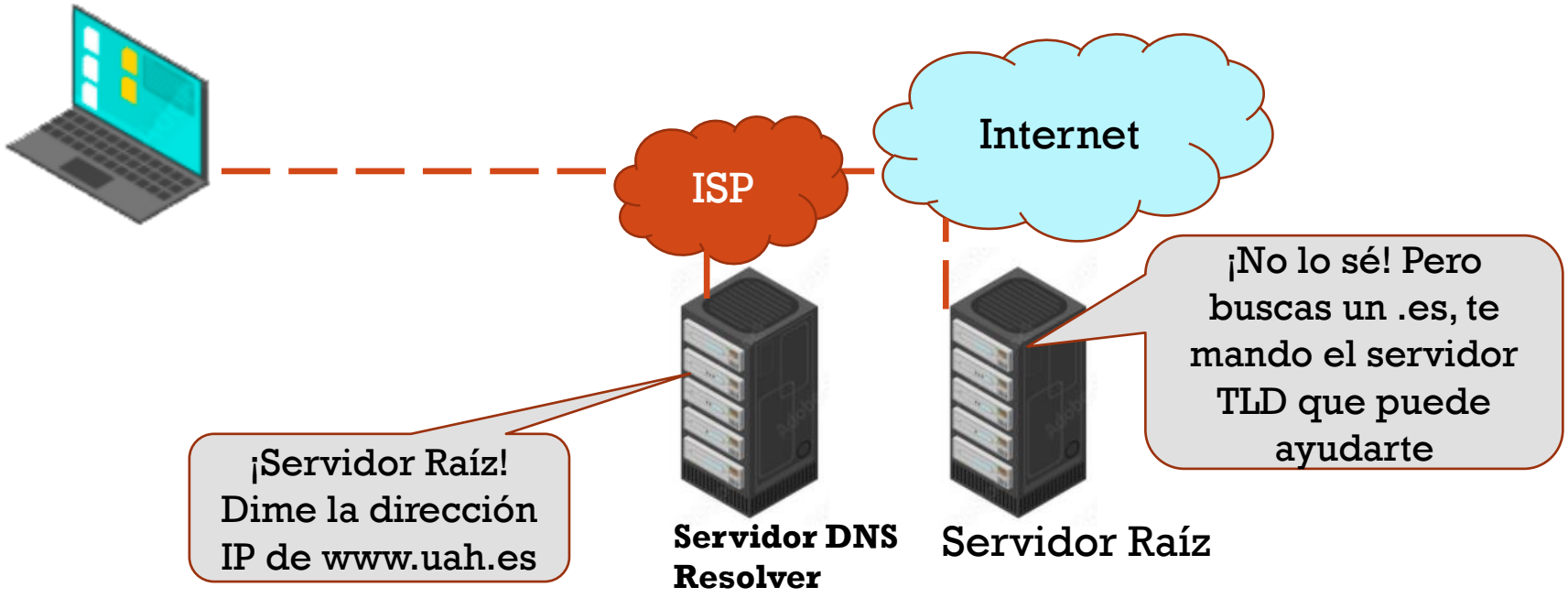
El ordenador acude al Resolver, servidor DNS local que normalmente corresponde con el servidor DNS del ISP (Proveedor Servicio Internet). Le preguntará por la IP de www.uah.es El servidor, al recibir la petición, le pide que espere y pregunta en su caché. No tiene el dato en caché y debe acudir al servidor raíz

FUNCIONAMIENTO

SERVIDOR RAÍZ
Es un servidor de nombres para la zona raíz del Sistema de Nombres de Dominio en Internet. Existen 13 servidores raíz específicos

El ordenador acude al Resolver, servidor DNS local que normalmente corresponde con el servidor DNS del ISP (Proveedor Servicio Internet). Le preguntará por la IP de www.uah.es El servidor, al recibir la petición, le pide que espere y pregunta en su caché. No tiene el dato en caché y debe acudir al servidor raíz

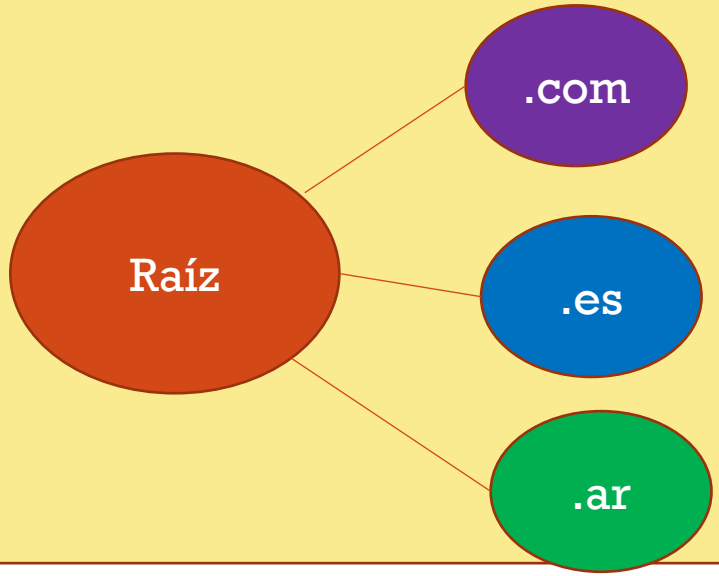
FUNCIONAMIENTO



El Resolver no tuvo respuesta en su caché y consulta al Servidor Raíz. La función del servidor raíz no es guardar la IP de un servidor específico, pero como ve que está pidiendo un dominio del tipo .es le da la IP del servidor TLD (Top Level Domain) que le puede ayudar

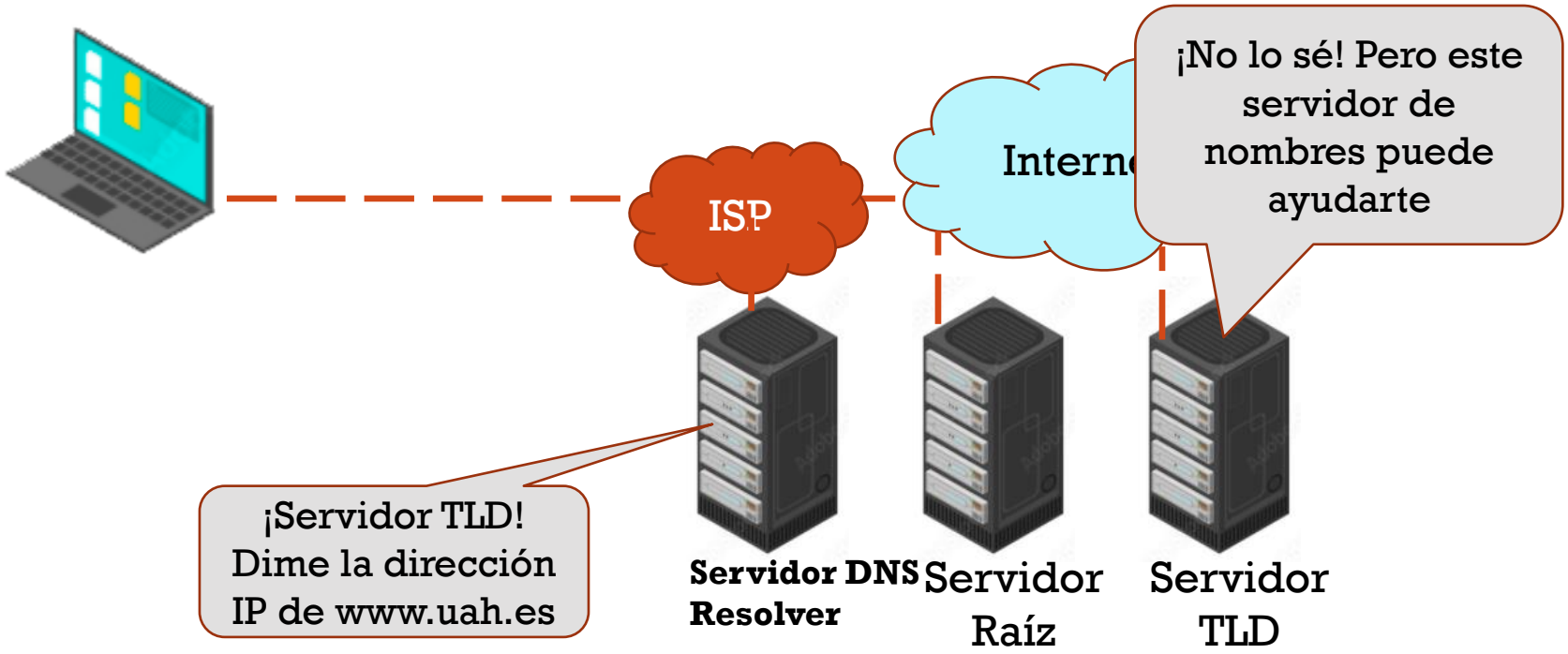
FUNCIONAMIENTO

SERVIDOR TLD (Top Level Domain)
Conjunto de servidores que almacenan direcciones de dominio de nivel superior, como .com .net .org



El Resolver no tuvo respuesta en su caché y consulta al Servidor Raíz. La función del servidor raíz no es guardar la IP de un servidor específico, pero como ve que está pidiendo un dominio del tipo .es le da la IP del servidor TLD (Top Level Domain) que le puede ayudar

FUNCIONAMIENTO



Una vez conectado con el servidor TLD pregunta por la IP. De igual manera que el paso anterior, como este servidor su función no es guardar las IPs de los sitios, le responde que no tiene esta información pero le da la dirección del Servidor de Nombres Autoritarios que puede ayudarle

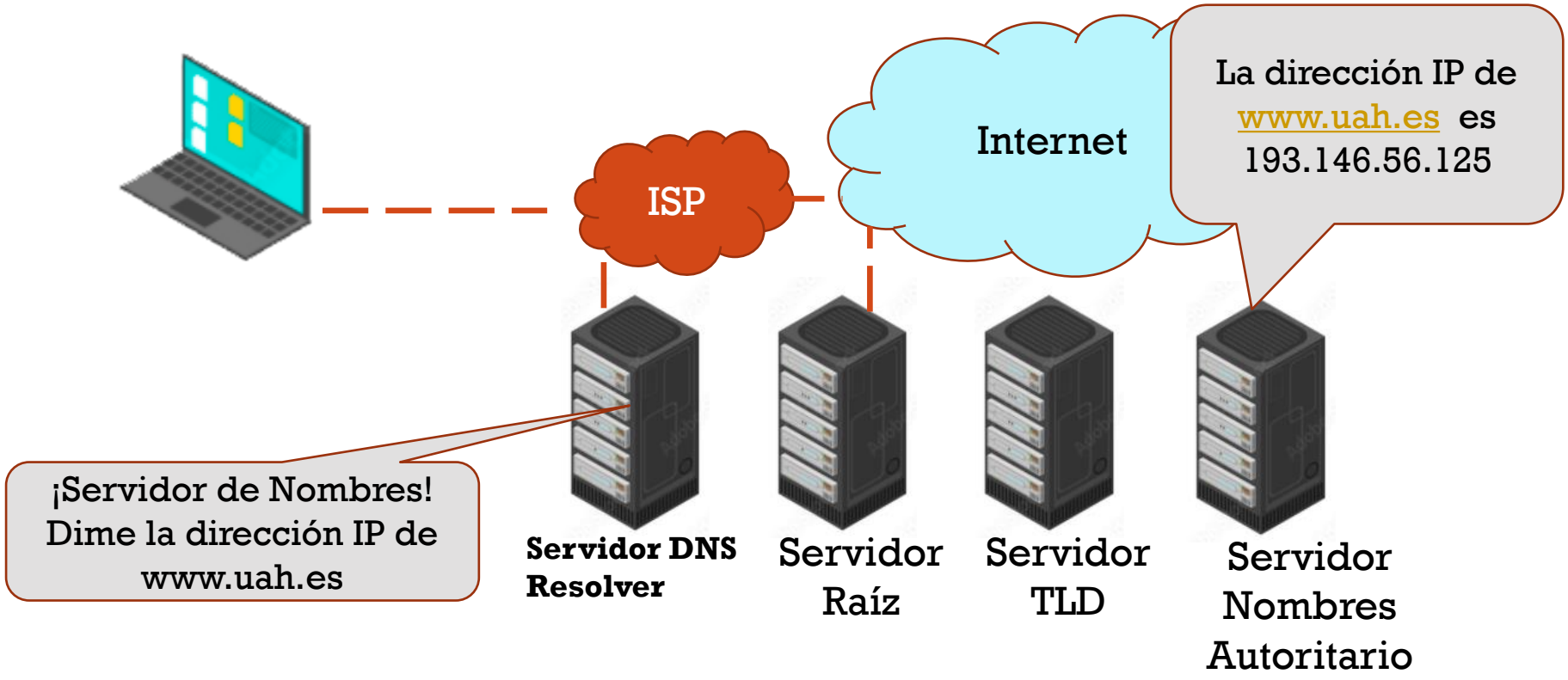
FUNCIONAMIENTO

SERVIDOR DE NOMBRES AUTORITARIOS

Son servidores que almacenan información de direcciones IPs de servidores específicos. Por ejemplo, el servidor de nombres autoritarios de uah.es tendría las direcciones IP de todos los servidores de uah.es

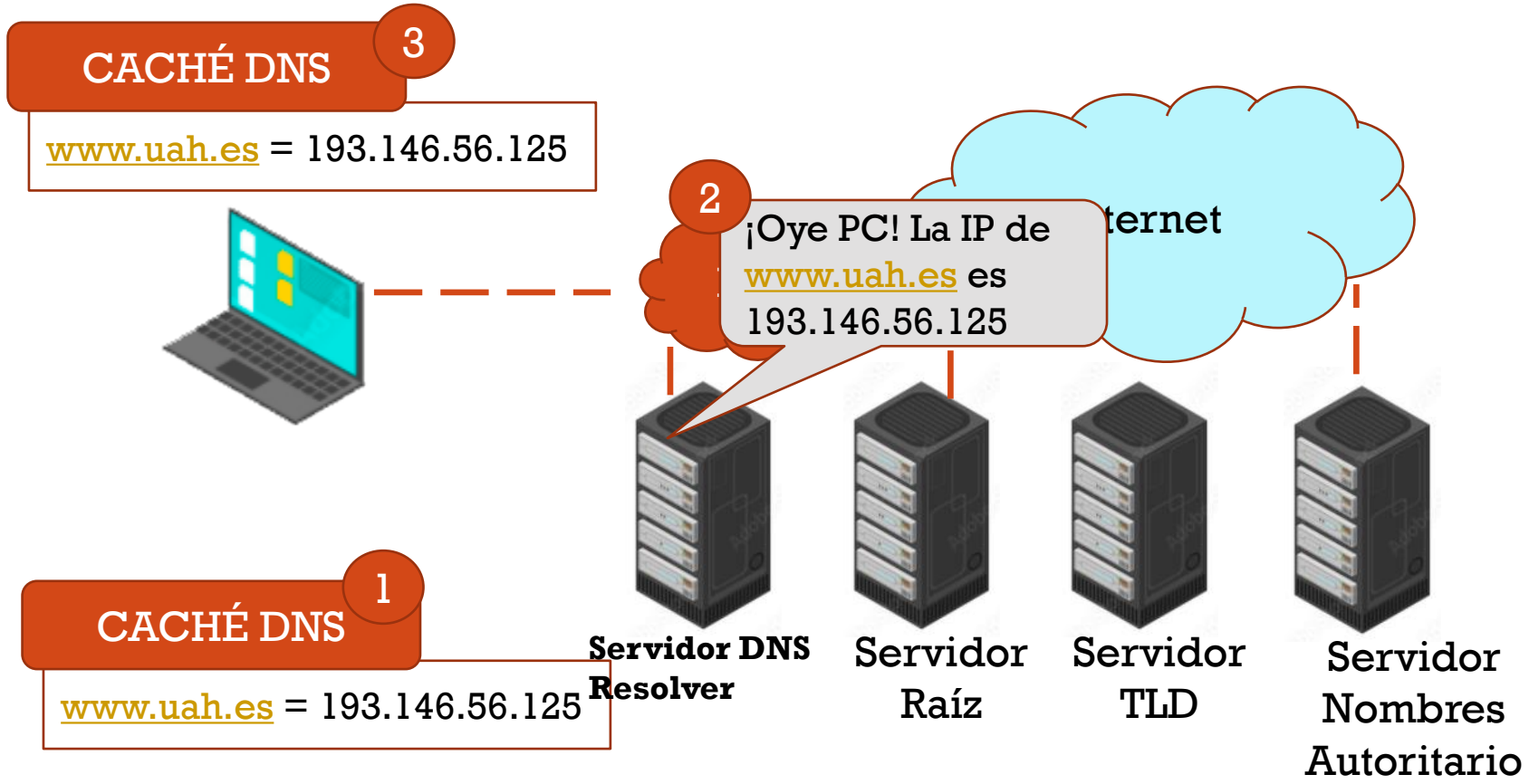
Una vez conectado con el servidor TLD pregunta por la IP. De igual manera que el paso anterior, como este servidor su función no es guardar las IPs de los sitios le responde que no tiene esta información pero le da la dirección del Servidor de Nombres Autoritarios que puede ayudarle

FUNCIONAMIENTO



Una vez conectado con el Servidor de Nombres Autoritario pregunta por la IP. Como la función de este servidor sí es guardar las direcciones IPs de servidores específicos le responde con la dirección IP

FUNCIONAMIENTO

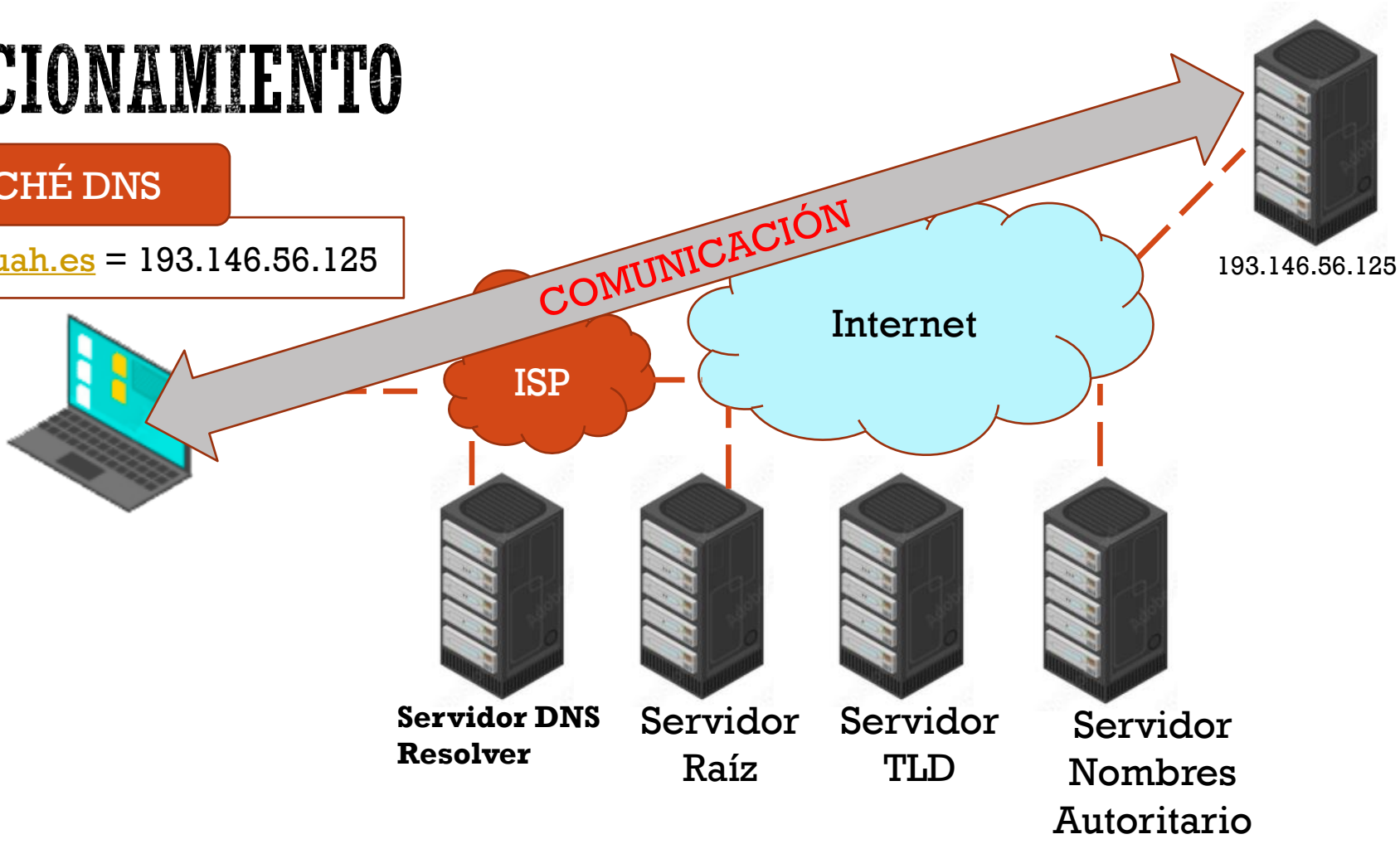


El Resolver ya dispone de la dirección IP. Lo primero que hace es guardarla en su Cache DNS y luego procede a informar de la petición. De la misma manera el ordenador guarda en su caché DNS la IP recibida

FUNCIONAMIENTO

CACHÉ DNS

www.uah.es = 193.146.56.125

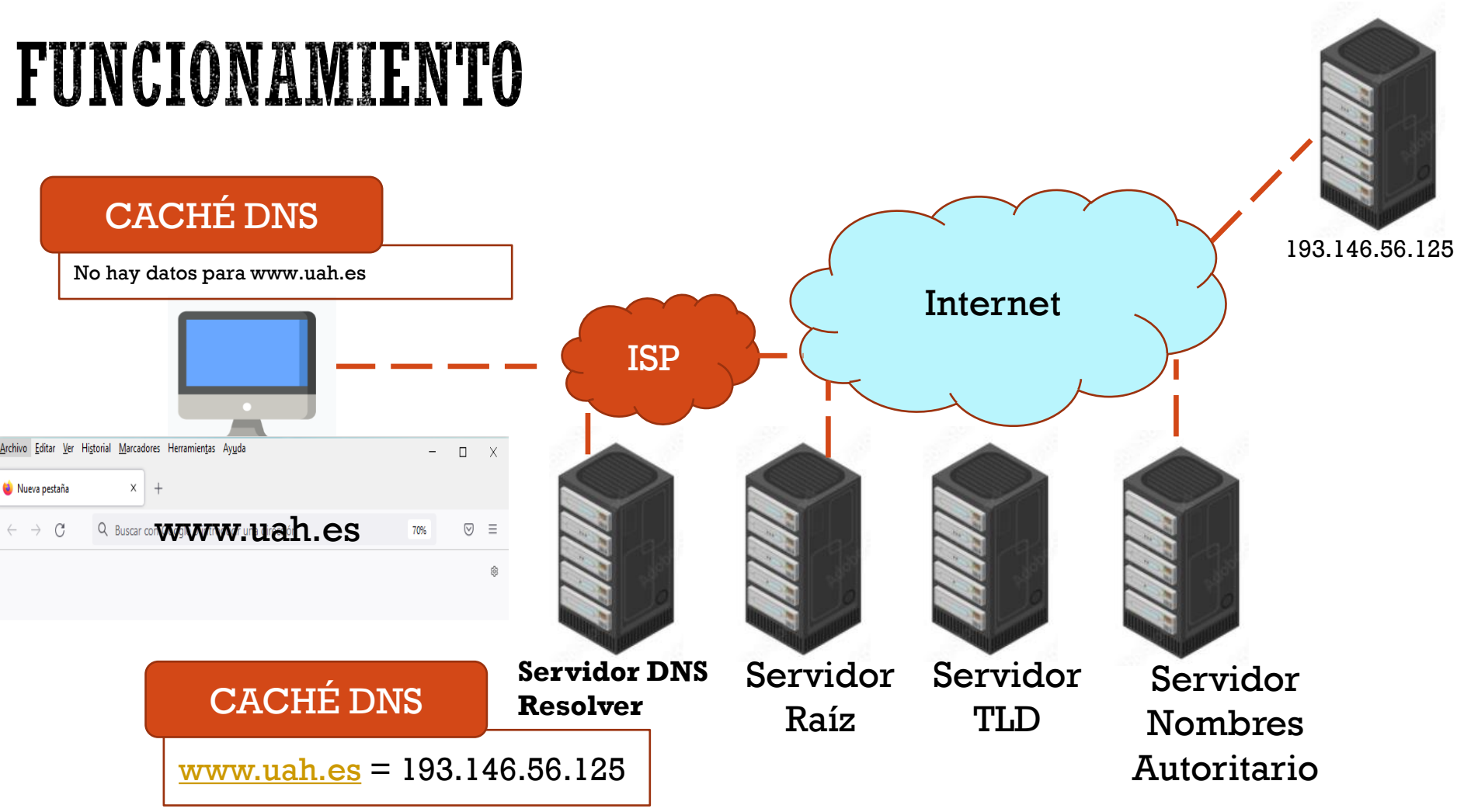


La máquina puede acceder a www.uah.es

Las próximas veces que vuelva a conectarse, no es necesario que consulte al Resolver porque ya dispone de esta información en su caché DNS

(Esta caché no es permanente)

FUNCIONAMIENTO

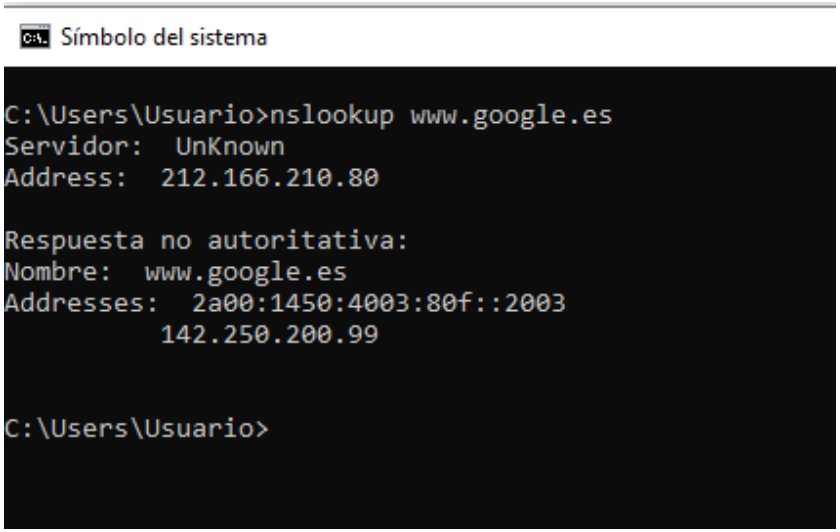


Supongamos que otro ordenador se conecta a www.uah.es. Su caché no tiene esta información y pide ayuda al Resolver. Este ya la tiene en su caché, por tanto responde con la IP

AHORA TÚ

- Desde una terminal ejecuta el comando

`nslookup www.google.es`



- Con el comando nslookup podremos saber si el DNS está resolviendo correctamente los nombres y las IPs

ESPACIO DE NOMBRES DE DOMINIO

NOMBRES DE DOMINIO

- El conjunto de nombres forma el denominado espacio de nombres de dominio que se puede representar mediante una estructura jerárquica organizada en forma de árbol. Cada nodo se separa de los otros nodos por un punto.
- Cada nombre de dominio puede estar formado por una o varias cadenas de caracteres separadas por puntos. No se distingue de mayúsculas de minúsculas.
- Puede tener un máximo de 63 caracteres y un mínimo de 2
- Solo pueden contener números, letras y guiones medios
- No pueden empezar ni acabar con un guion.
- Se pueden usar nombres que tengan como máximo 127 niveles y cada parte separada por un punto.

- Ejemplos: “google.es.”, “redes.asir.es.”

NOMBRES DE DOMINIO

Por organización

com	Organización comercial
net	Organización relacionada con la red
org	Otras organizaciones
edu	Institución educativa USA
…	

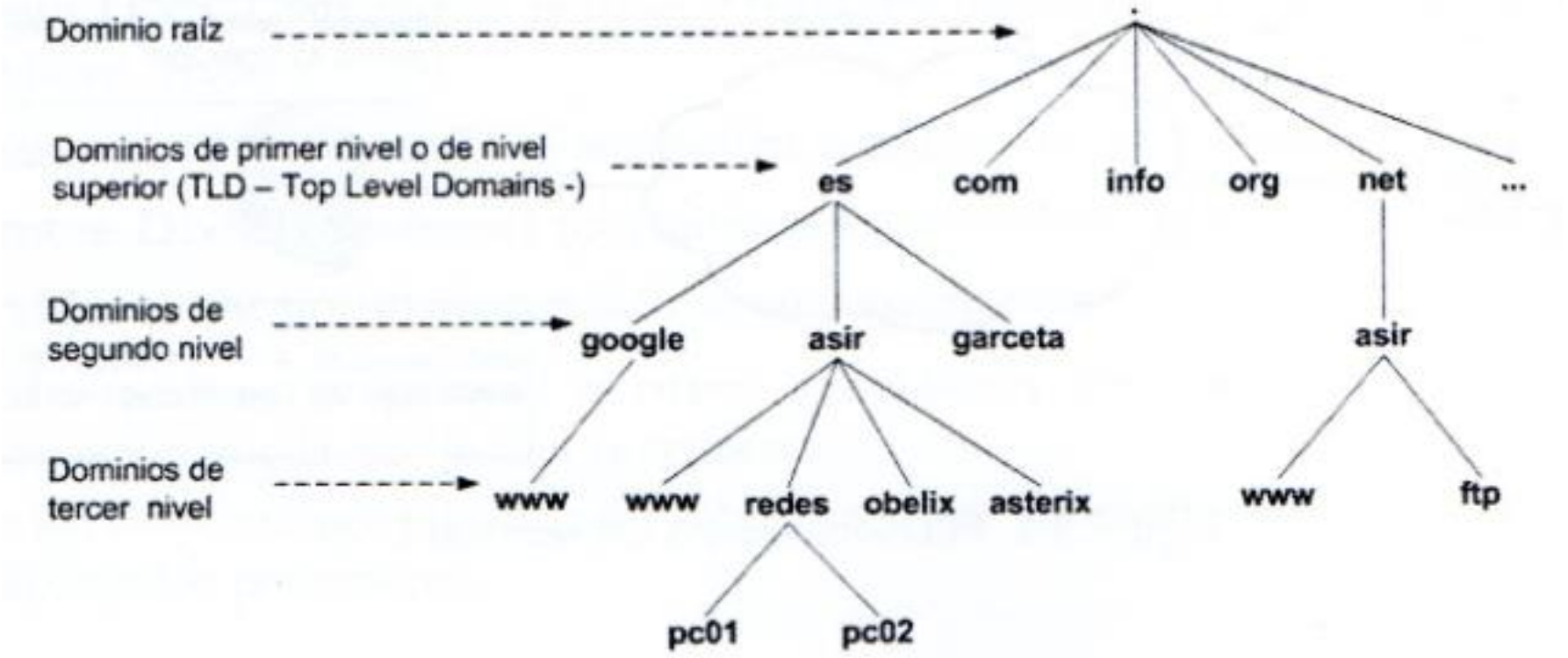
Por zona geográfica

es	**España**
uk	Reino Unido
ar	Argentina
….	

NOMBRES DE DOMINIO

- La información DNS se distribuye en un gran número de servidores en todo el mundo.
- Los servidores DNS se organizan en una estructura de árbol. Pueden ser:
  - Servidores Raíz: son 13. Conocen las direcciones Ips de los servidores TLD.
  - Servidores Top Level Domain (TLD). Cada Servidor TLD conoce las direcciones IP de los servidores de nombres que resuelven sus dominios dentro de su propio dominio.
  - Servidores con Autoridad. Al menos 2 por ISP u organización. Almacenan la información sobre nombre de dominio y dirección IP, asociada a los host de la organización

NOMBRES DE DOMINIO



Espacio de nombres de dominio

DOMINIO RAÍZ. DOMINIO Y SUBDOMINIO

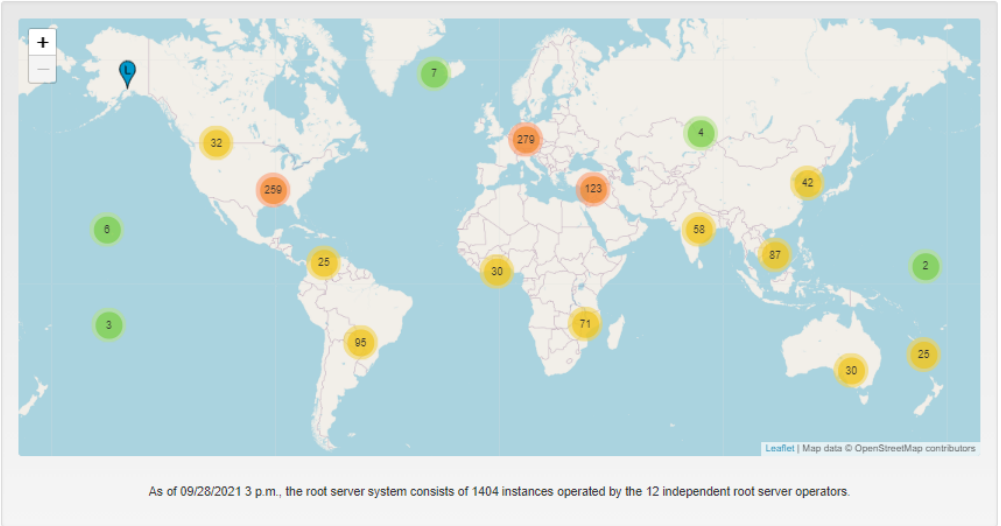
- Los nombres de dominio terminan en un ".". Esto es así porque el árbol de nombres de dominio empieza en el dominio "." que se conoce como dominio raíz (realmente es un nombre nulo con 0 caracteres, pero se representa usando un ".").

- Como consecuencia de la organización jerárquica, es posible utilizar los términos dominio y subdominio. Por ejemplo, "google.es." es un subdominio de "es."

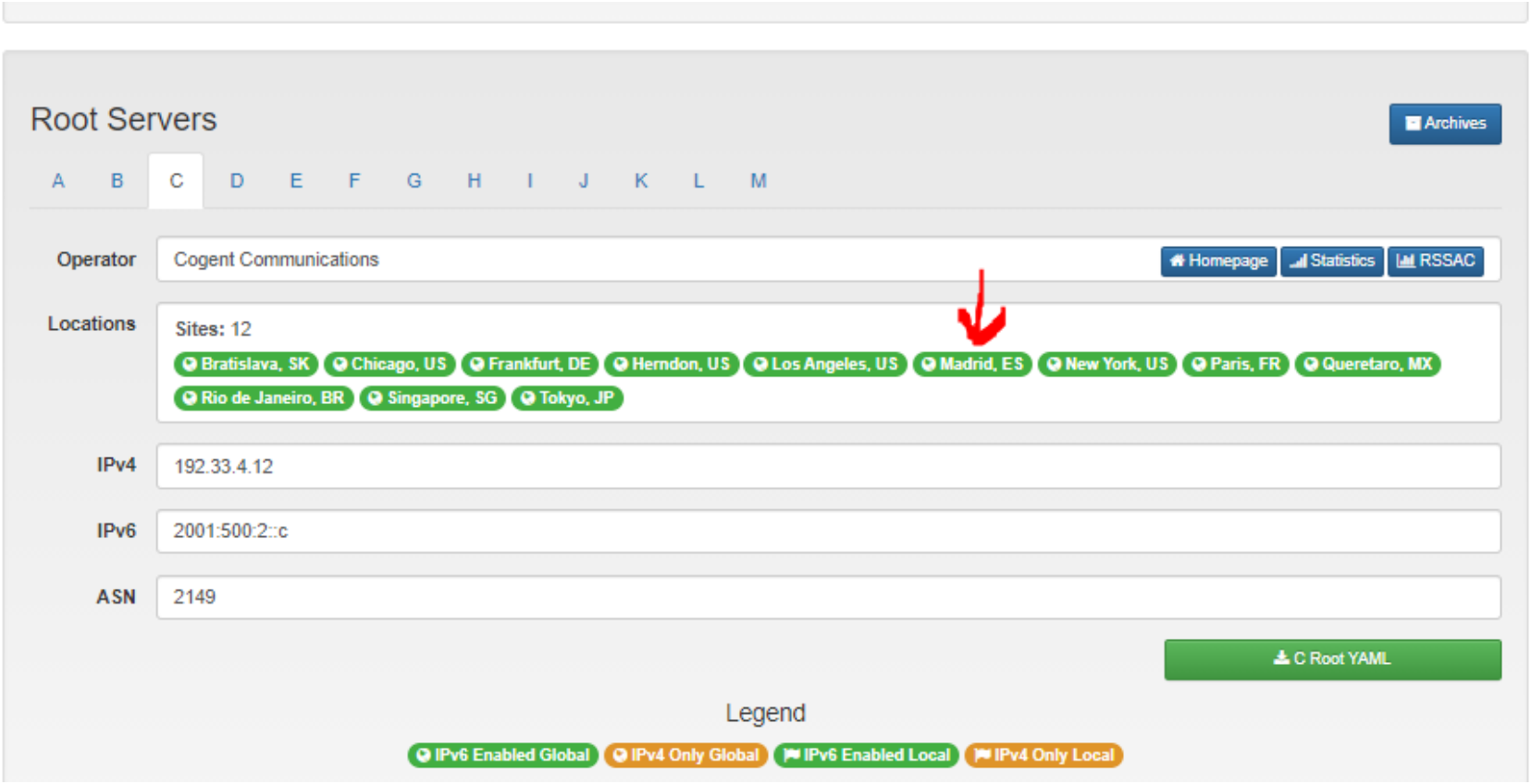
- Los subdominios que cuelgan del dominio raíz se llaman de primer nivel o dominios de nivel superior (TLD, Top Level Domains).

DOMINIO RAÍZ. DOMINIO Y SUBDOMINIO

- La información de los servidores raíz se puede encontrar en https://root-servers.org/
- En la parte inferior de la web se puede consultar la información de cada uno de estos 13 servidores raíz.
- Cada uno se identifica con las letras de "A" – "M"
- Todos ellos están replicados



DOMINIO RAÍZ. DOMINIO Y SUBDOMINIO



- A fecha de septiembre 2021 observamos las réplicas que tiene el servidor raíz C, teniendo en Madrid una de ellas.

NOMBRES RELATIVOS Y ABSOLUTOS. FQDN

Cuando se hace referencia a un dominio usando un nombre se puede emplear su nombre relativo o su nombre absoluto:

- Nombre relativo: Es necesario saber el contexto del dominio superior para determinar a qué nombre se hace referencia exactamente.

- Nombres absolutos o completos (FQDN, Fully Qualified Domain Names) : Nombre formado por todas las partes hasta el dominio raíz. El "." final del dominio raíz permite distinguir si el nombre usado es FQDN o no. Normalmente no usamos el "." final de los FQDN en las aplicaciones, pero internamente sí se utiliza.

Nota: los usuarios no usamos el punto final de los nombres, pero internamente sí se utiliza

USO DE DOMINIOS

- Lo habitual es usar un dominio para nombrar a un conjunto de host y/o subdominios que se agrupan según algún criterio:
  - Host de la misma red
  - Host de la misma empresa (en una o varias redes)
  - Host de la misma localización
  - Host del mismo ISP

- Pero no existe ninguna restricción de qué host y subdominios se agrupan en un dominio.

ADMINISTRACIÓN DE NOMBRES DE DOMINIO EN INTERNET. DELEGACIÓN

- La **administración y organización** del espacio de nombres de dominio de Internet se distribuye **entre múltiples empresas y organizaciones**, estando coordinada por la ICANN (Internet Corporation for Assigned Names and Numbers).

- La **ICANN es una organización sin ánimo de lucro** que tiene el objetivo de garantizar que Internet sea estable, operativa y segura.

- Se encarga –entre otras- de **administrar el dominio raíz** y de **mantener un registro de los dominios de nivel superior** (TLD) existentes.

ADMINISTRACIÓN DE NOMBRES DE DOMINIO EN INTERNET. DELEGACIÓN

- Los TLD son clasificados por la ICANN administrativamente en:
  - **Genércos (gTLD):** En función del propósito o el tipo de organización que los utiliza.
    - Dominios patrocinados (sTLD, sponsored TLD): Operan según las reglas de una entidad que soporta su patrocinio (Ej: aero, coop, edu, gov, travel)
    - Dominios no patrocinados (uTLD unsponsored TLD: Según las reglas del ICANN establecidas globalmente (Ej: com, info, org, net)
  - **Geográficos (ccTLD, county code TLD):** Nombres de dos letras establecidos en función de países o regiones (Ej: es, fr). Las tareas de gestión y políticas de uso se delegan en una entidad del país o territorio.
  - **Arpa**: Además, existe el dominio "arpa" que se utiliza para la infraestructura técnica de internet.
  - **Dominios reservados:** Reservados para pruebas privadas. (Ej: test, example, localhost)

AHORA TÚ

- Consulta en http://www.iana.org/domains/root/db información sobre el dominio "es.".
- En ese mismo lugar tienes un enlace a la URL para registrar servicios. Piensa en un dominio que quisieras registrar, y comprueba si está disponible. Si no está disponible, ¿Qué información tienes sobre ese dominio?
- Consulta el precio (tarifas) de un dominio ".es" según la web anterior, y según varios agentes registradores.

ADMINISTRACIÓN DE NOMBRES DE DOMINIO EN INTERNET. DELEGACIÓN

- La administración descentralizada de DNS se basa en la delegación.
- La **delegación consiste en que la organización que administra un dominio cede la administración de uno, varios o todos sus subdominios a otras organizaciones**.
- A su vez, cada organización puede delegar la administración de sus subdominios en otras organizaciones, y así sucesivamente.
- Por ejemplo, **ICANN administra el dominio raíz y delega la administración de los dominios TLD en otras organizaciones**.
- La división de un dominio en subdominios no implica siempre ceder su delegación. Además, si una organización delega un subdominio en otra, no tiene por qué informar a "su superior".
- La **organización que administra un dominio es responsable de los nombres usados en ese dominio, de las direcciones IP asociadas a ellos, y del funcionamiento y mantenimiento de los servidores que almacenan esta información**.

ADMINISTRACIÓN DE NOMBRES DE DOMINIO EN INTERNET. DELEGACIÓN

- **Registro de dominio:** Consiste en "reservar" el nombre durante un tiempo para poder crear subdominios y asociar el nombre y/o subdominios con direcciones IP o con la información que se considere oportuna.
- Los registradores pueden registrar nombres de dominio de segundo nivel. Existen diferentes normativas que determinan qué nombres se pueden registrar en función del uso que se le dará y del dominio TLD del que depende.
- Un nombre de dominio puede ser registrado a través de diferentes compañías, conocidas como **agentes registradores** (registrant).

SERVIDORES DE NOMBRE

SERVIDORES DE NOMBRES

- Los servidores de nombres, también llamados servidores DNS, son **programas que guardan información sobre nombres de dominio y responden a las preguntas que les realizan los clientes DNS y otros servidores de nombre**. Almacenan por tanto, una parte de la base de datos de DNS.

- Por defecto, escuchan en los **puertos 53/TCP y 53/UDP**

ZONAS

- Los servidores de nombres **mantienen información de una parte del espacio de nombres** de dominio que se conoce como **zona**.
- Cuando un servidor DNS contiene una zona, se dice que es **autorizado (authoritative)** para esa zona.
- Las **zonas se almacenan en ficheros de texto o en bases de datos** dependiendo del tipo servidor utilizado.
- Cada una de las líneas del fichero se conoce como **registro de recursos (RR, Resource Records)**. Existen distintos tipos de recursos, como se verá después.

asir.es	IN	NS	ns1.asir.es.
ns1.asir.es.	IN	A	118.100.162.100
pegaso.asir.es.	IN	A	118.100.162.101
www.asir.es.	IN	CNAME	pegaso.asir.es.

Fichero de zona de resolución directa

ZONAS

En DNS disponemos de tres **tipos** diferentes de **zonas**:

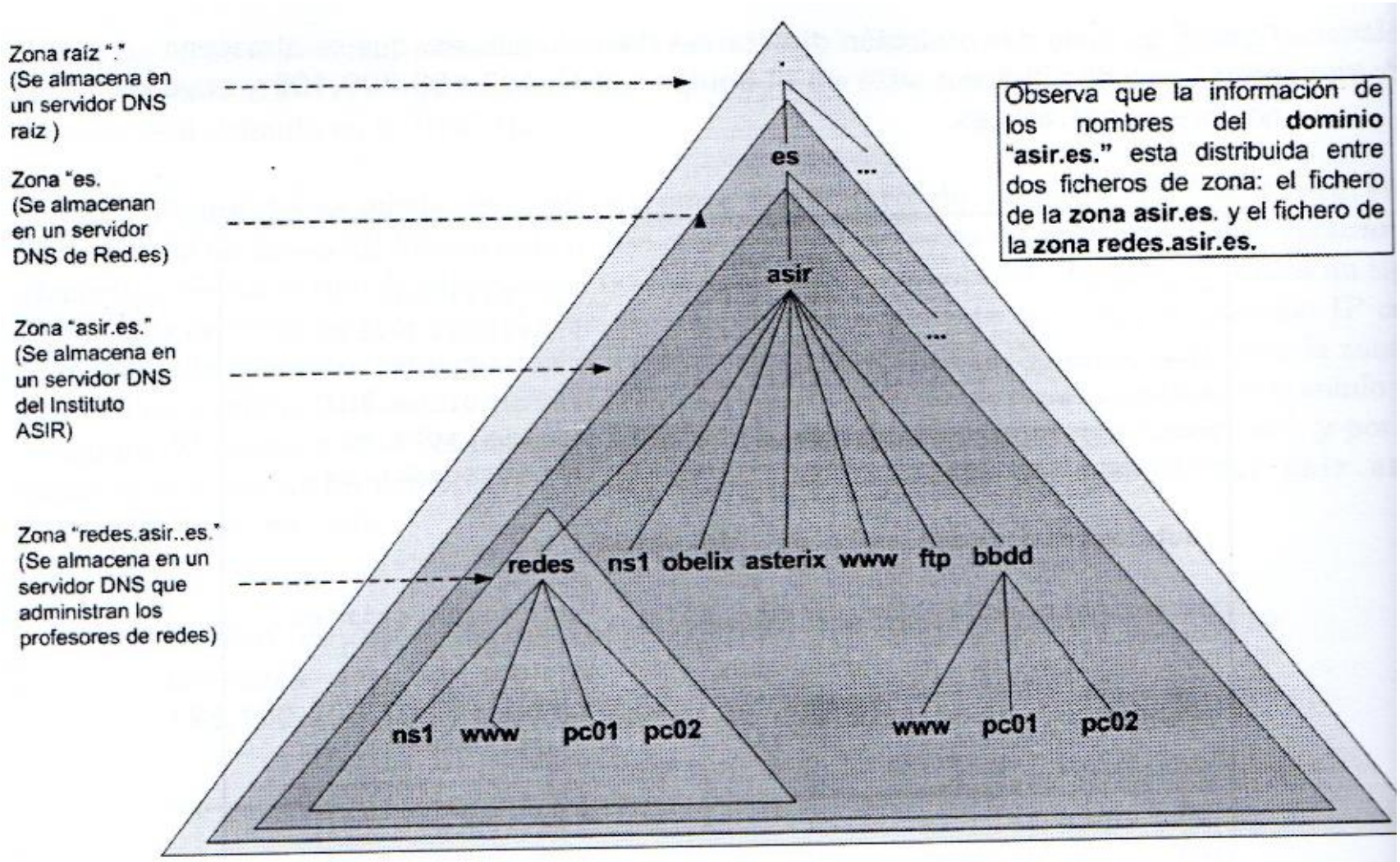
Zona primaria	Zona secundaria	Zona de rutas internas

• Es autoritativo para la zona
• Es el punto principal para la zona
• Se pueden alojar en:
  • Servicio de A.D
  • Fichero local en servidor DNS
	• Contiene toda la información de la zona primaria
	• Obtiene información transfiriéndose la zona de otro servidor DNS
	• No se pueden hacer cambios en los registros DNS
	• Nunca autoritativo para la zona
	• Útiles para :
	  • reducir el tráfico de red
	  • rápida resolución de nombres (especialmente cuando la zona primaria no está integrada en A.D)
		• Zonas que solo contienen información de los servidores que son autoritativos para las zonas
		• Útiles para distribuir detalles sobre dónde encontrar la información completa de las zonas
		• No contienen todos los datos de la zona

ZONAS

- Cuando un servidor DNS es autorizado para una zona, es responsable de los nombres de dominio de la misma.
- La organización que delega el servidor de nombres y por lo tanto la zona, puede decidir si delega o no alguno de sus subdominios.
- **Una zona no es lo mismo que un dominio**. Un dominio es un subárbol del espacio de nombres de dominio. Los datos asociados a los nombres de un dominio pueden estar almacenados en una o varias zonas distribuidas en uno o varios servidores.
- **Un servidor DNS puede tener autoridad sobre varias zonas.**
- El servicio DNS permite almacenar una misma zona en varios servidores DNS, ofreciendo así balanceo de carga, rapidez, y mayor tolerancia a fallos.

ZONAS


Zona raíz "."
(Se almacena en un servidor DNS raiz)
Zona "es.
(Se almacenan en un servidor DNS de Red.es)
Zona "asir.es."
(Se almacena en un servidor DNS del Instituto ASIR)
Zona "redes.asir..es."
(Se almacena en un servidor DNS que administran los profesores de redes)
Observa que la información de los nombres del dominio "asir.es." esta distribuida entre dos ficheros de zona: el fichero de la zona asir.es. y el fichero de la zona redes.asir.es.
.
es
...
asir
...
redes
ns1
obelix
asterix
www
ftp
bbdd
ns1
www
pc01
pc02
www
pc01
pc02

TIPOS DE SERVIDORES DE NOMBRE

- **Según la función** que realizan:
  - Maestro o primario
  - Esclavo o secundario
  - Caché
  - Reenviador (forwarding)
  - Solo autorizado
- Un mismo servidor DNS puede combinar varias de estas funciones simultáneamente.

SERVIDOR DE NOMBRES MAESTRO

- También se llama primario o principal
- Define una o varias zonas para las que es autorizado.
- Sus archivos de zona locales son de lectura y escritura, y es en ellos donde el administrador añade, modifica o elimina nombres de dominio
- Funcionamiento:
  - Si un cliente DNS u otro servidor DNS le pregunta por un nombre de dominio para el que es autorizado, consulta con los ficheros de zona y responde.
  - Si un cliente DNS u otro servidor DNS le pregunta por un nombre de dominio para el que no es autorizado, tendrá que buscar la información en otros servidores DNS o responder que no conoce la respuesta.

SERVIDOR DE NOMBRES ESCLAVO

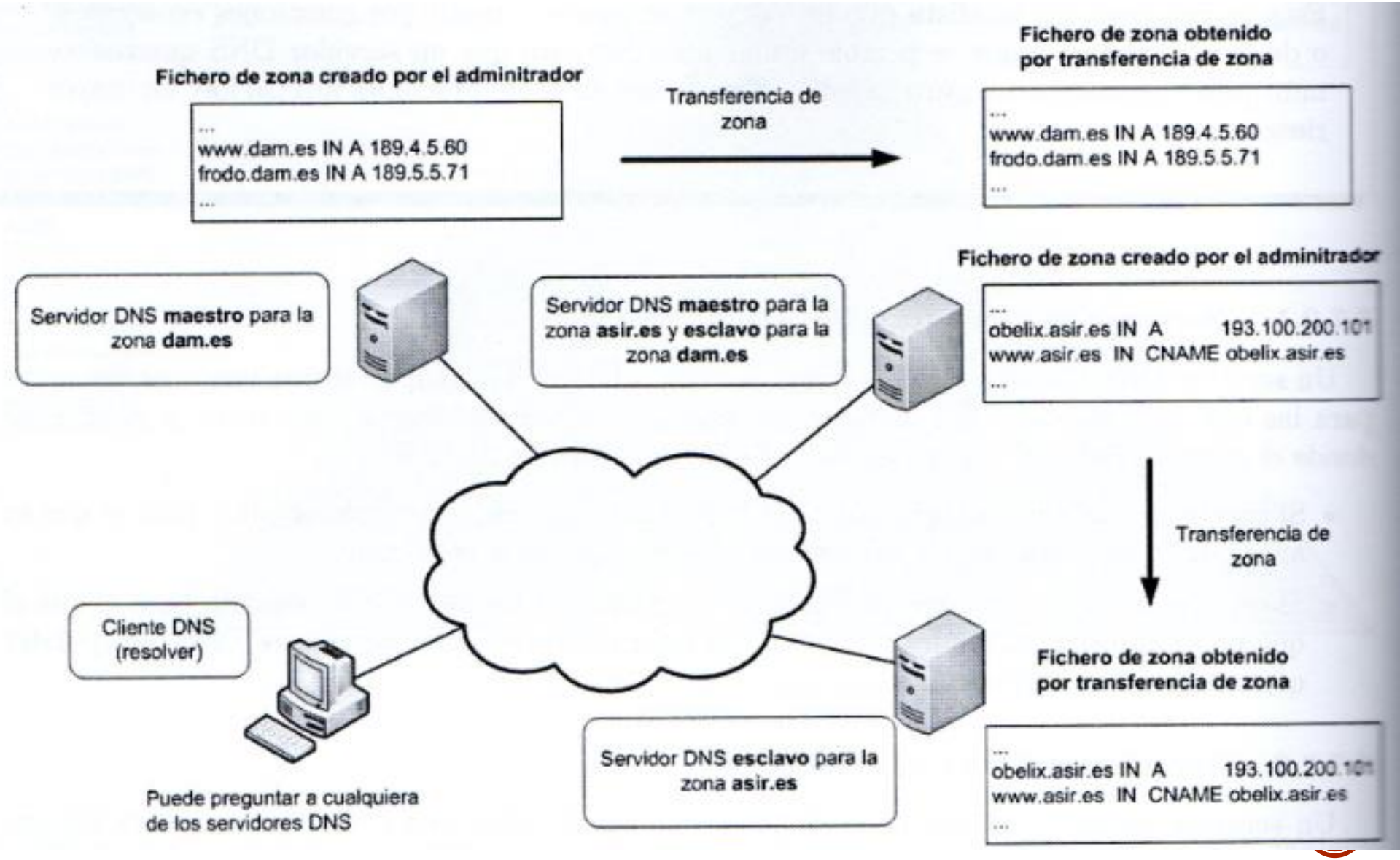
- También llamado secundario
- Define una o varias zonas para las que es autorizado.
- La diferencia con un maestro es que obtiene los ficheros de zona de otro servidor autorizado para la zona mediante un proceso que se denomina **transferencia de zona**.
- Los **ficheros** de zona del servidor esclavo son de **solo lectura**. La modificación de los ficheros de zona se realiza en el servidor maestro.
- El funcionamiento ante las respuestas de los clientes es similar al de un servidor maestro.

SERVIDOR DE NOMBRES ESCLAVO

- Se utilizan para:
  - Reducir y reducir la carga entre varios servidores.
  - Favorecer la tolerancia a fallos.
  - Ofrecer respuestas más rápidas.

- Lo ideal es que los servidores DNS de una zona estén ubicados en redes y localizaciones diferentes para evitar que un problema les afecte simultáneamente y deje sin servicio de resolución a los nombres de dicha zona.

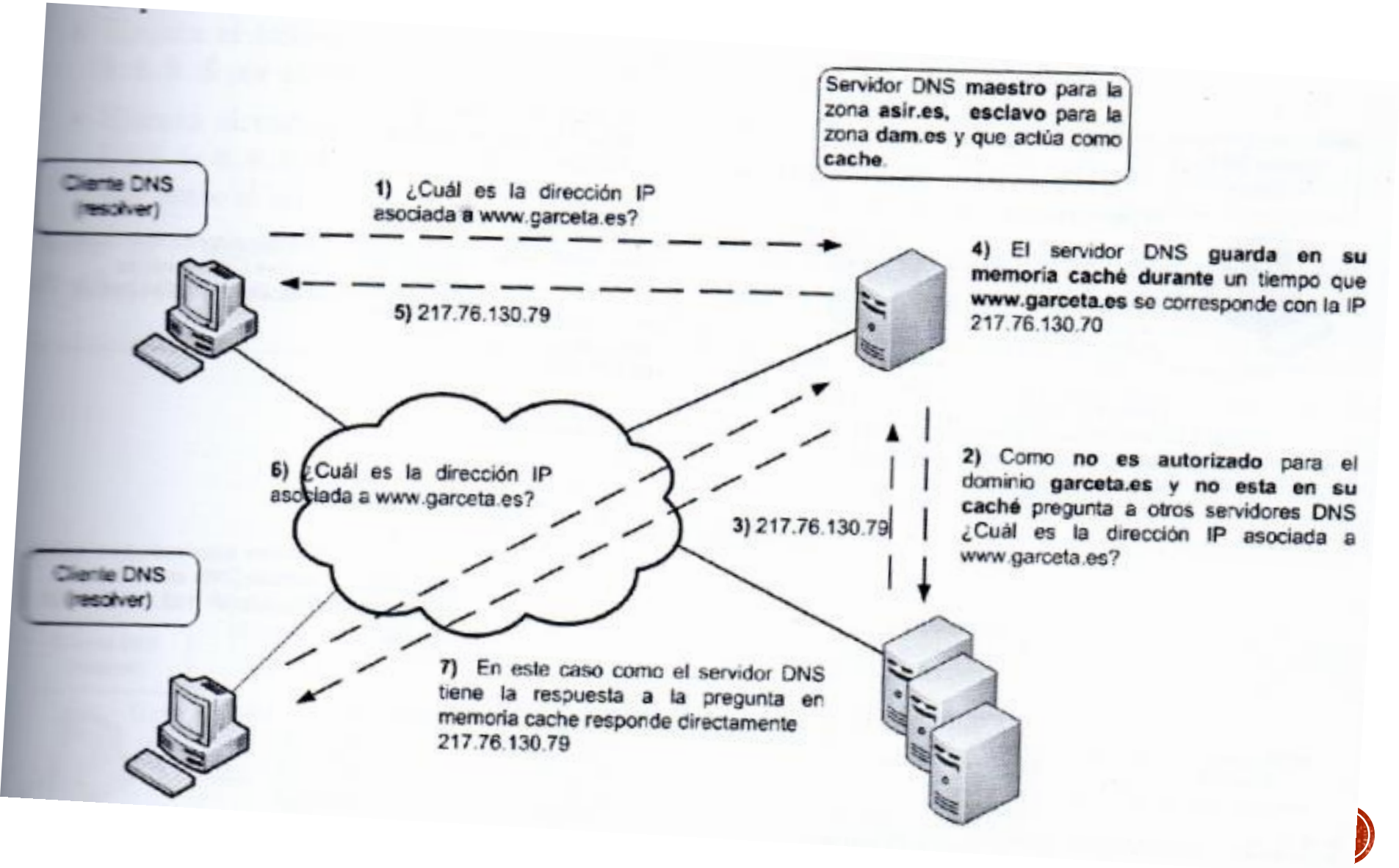
SERVIDOR DE NOMBRES ESCLAVO



SERVIDOR DE NOMBRES CACHÉ

- Cuando un servidor DNS recibe una pregunta sobre un nombre de dominio de una zona para la que no es autorizado, es decir, de un nombre que no tiene información, puede preguntar (si así se ha configurado) a otros servidores para que le den la respuesta.
- Si el servidor actúa como caché, guarda durante un tiempo (TTL, Time To Live) las respuestas a las últimas preguntas que ha realizado a otros servidores de nombres.
- Cada vez que un cliente DNS u otro servidor DNS le formula una pregunta, consulta en primer lugar en su memoria caché, ahorrándose la pregunta a otros servidores si ya la había hecho anteriormente.
- Un servidor de nombres es solo caché (caching only server) cuando:
  - No tiene autoridad sobre ningún dominio.
  - Pregunta a otros servidores para resolver las peticiones y guarda las respuestas en caché.

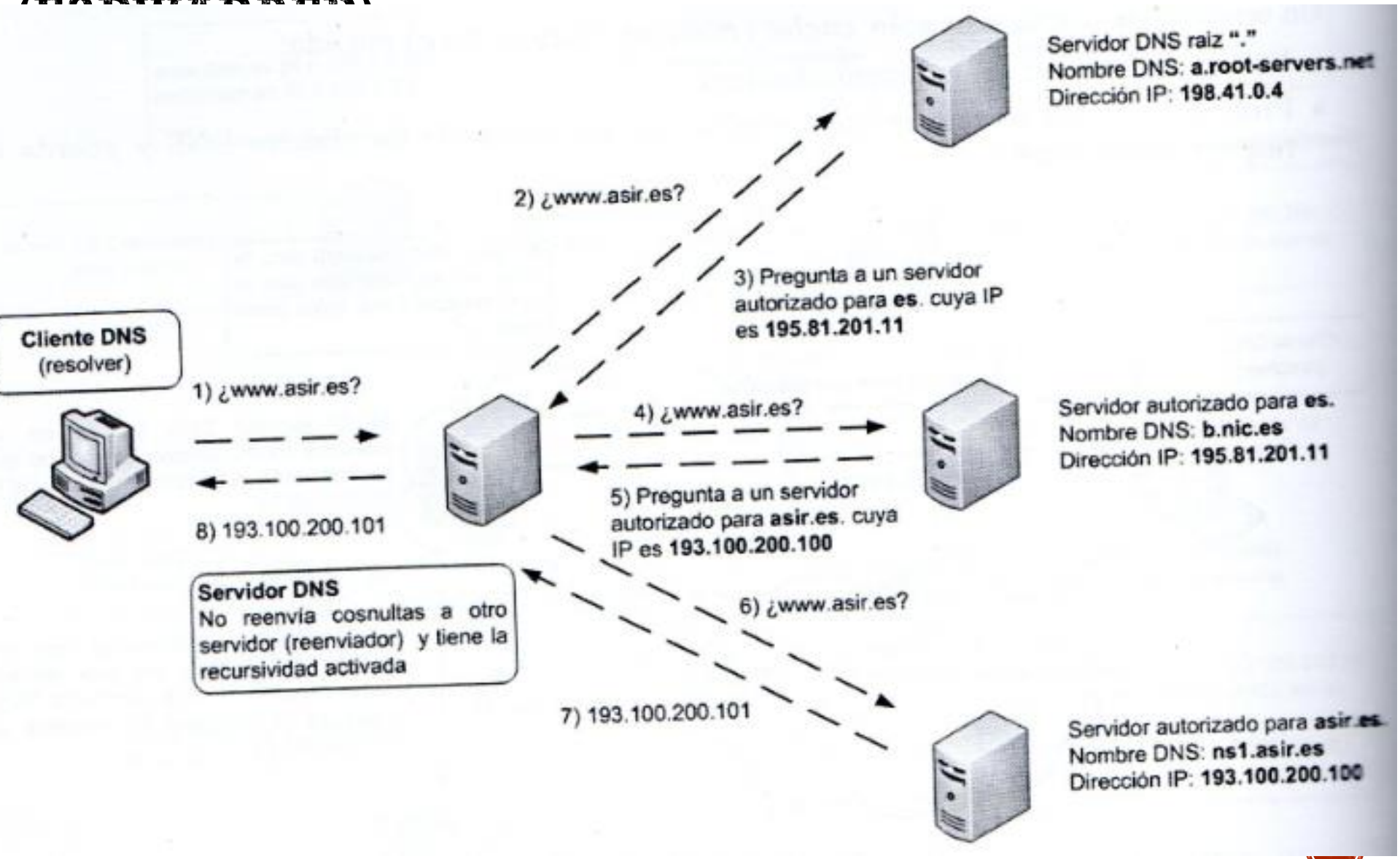
SERVIDOR DE NOMBRES CACHÉ



SERVIDOR DE NOMBRES REENVIADOR (FORWARDER)

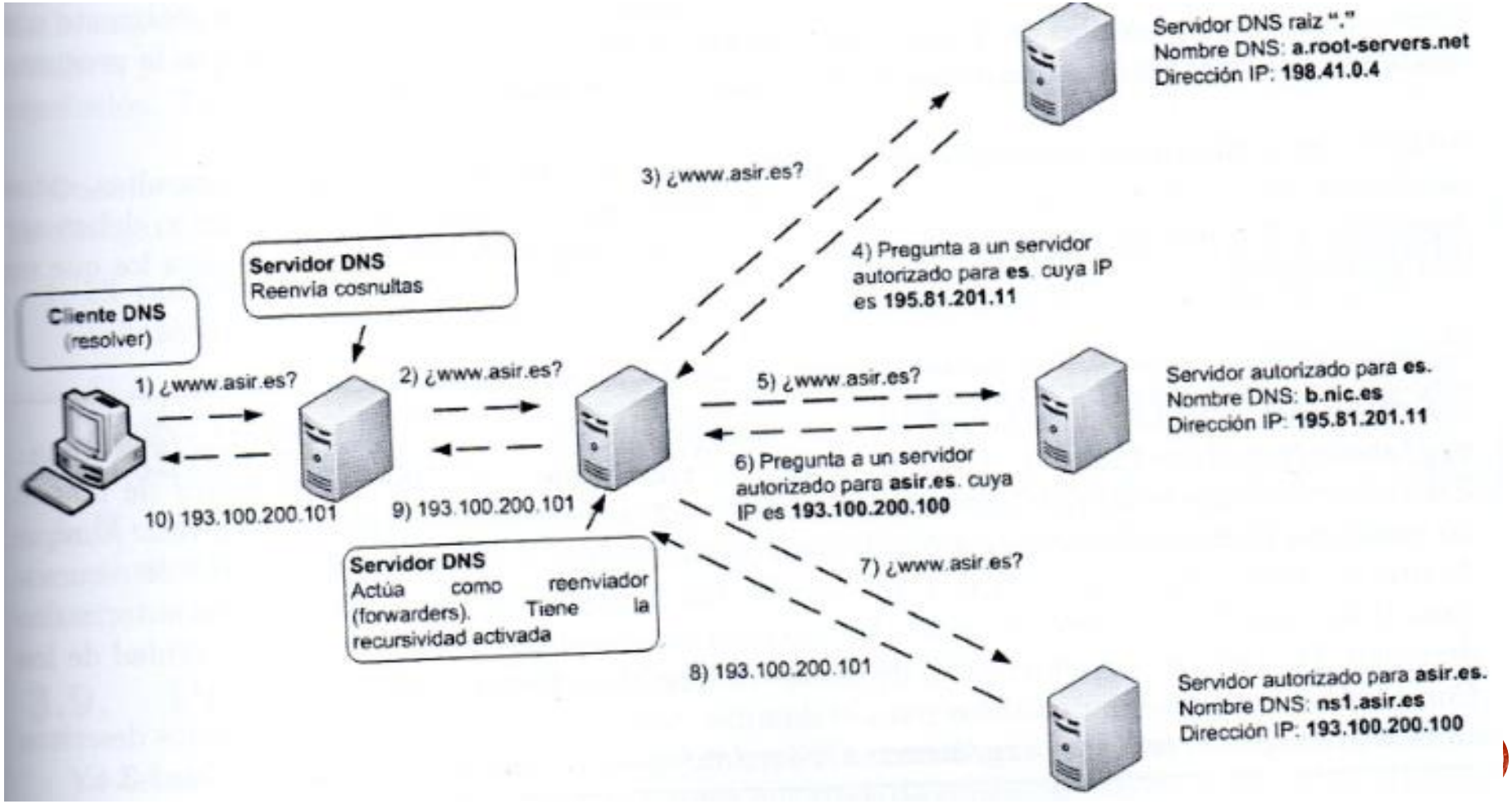
- Cuando un servidor DNS recibe una pregunta sobre un nombre de dominio del que no dispone información puede preguntar a otros servidores DNS.
- Hay dos posibilidades:
  - Procesa la consulta preguntando a diversos servidores DNS y empezando por los servidores DNS raíz.

SERVIDOR DE NOMBRES REENVIADOR (FORWARDER)



SERVIDOR DE NOMBRES REENVIADOR (FORWARDER)

- Reenvía la consulta a otro servidor DNS, que se denomina reenviador (forwarder), para que se encargue de resolverla.



SERVIDOR DE NOMBRES SOLO AUTORIZADO

- Un servidor de nombres es solo autorizado (authoritative only) cuando:
  - Es autorizado para una o varias zonas como maestro y/o esclavo.
  - No responde a preguntas que no sean relativas a sus zonas, es decir, no pregunta a otros servidores DNS. Esto implica que:
    - No tienen activada la recursividad
    - No es reenviador
    - No actúa como caché.

SERVIDORES RAÍZ (ROOT SERVERS)

- Existen un conjunto de servidores DNS autorizados para el dominio raíz ".", conocidos como servidores raíz (root servers).
- Contienen el fichero de la zona "." que almacena cuáles son los servidores DNS autorizados para cada uno de los dominios TLD.
- Los servidores raíz están bajo responsabilidad de la ICANN, pero son operados por un consorcio de organizaciones.
- Estos servidores son clave en el proceso de resolución de nombres de domino en Internet, y deben ser conocidos por todos los servidores DNS que respondan a preguntas sobre nombres para los que no son autorizados.

CLIENTES DNS

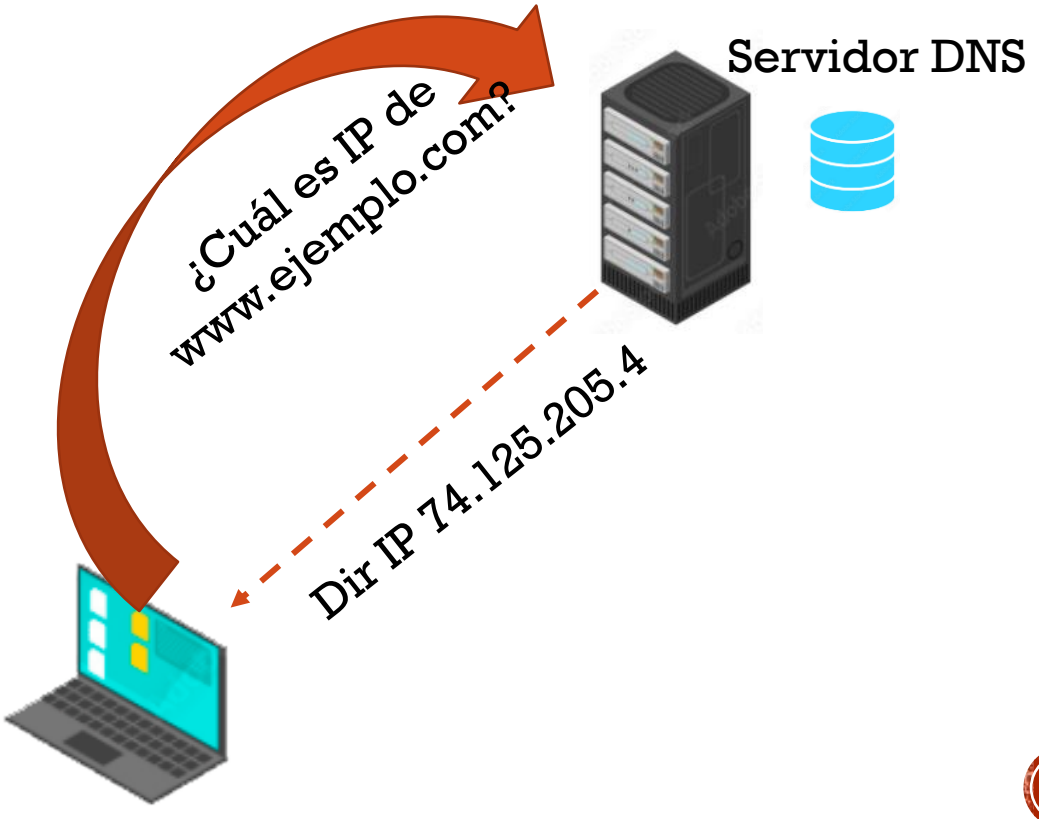
CLIENTES DNS (RESOLVERS)

- Es cualquier software capaz de preguntar a un servidor DNS e interpretar sus respuestas.
- Los sistemas operativos incluyen un conjunto de librerías que hacen esta función, y son invocadas por las aplicaciones cuando se utiliza un nombre de dominio.
- Algunos se pueden configurar para mantener una caché de respuestas.
- Algunos sistemas también tienen archivos de texto en donde se pueden asociar direcciones IP con nombres que consultarían primero.

PROCESO DE RESOLUCIÓN

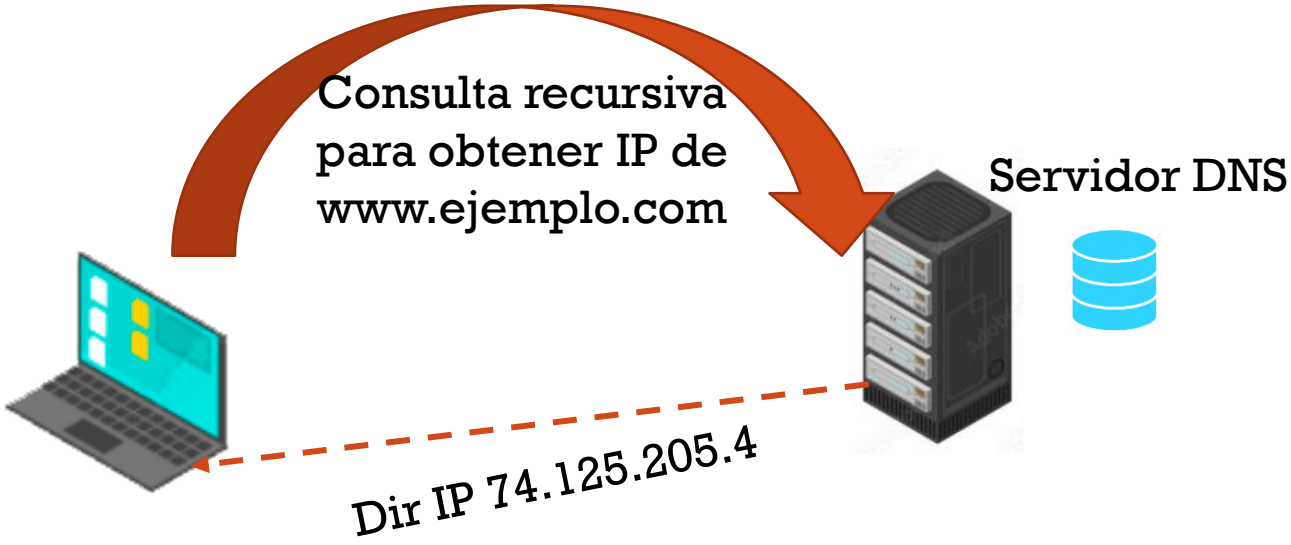
PROCESO DE RESOLUCIÓN

- Resolver un nombre de dominio: obtener la dirección IP asociada
- El ordenador lanza una consulta sobre www.ejemplo.com.
- ¿Cómo se resuelve esta consulta? Se distinguen dos tipos de consultas
  - Recursivas
  - Iterativas



CONSULTAS RECURSIVAS

- Es aquella en la que el **servidor tiene que dar una respuesta completa o exacta**.
- Esto es en clientes DNS iniciales, como en nuestro ordenador cuando queremos acceder a www.ejemplo.com El servidor DNS devuelve la IP si la tiene disponible localmente, sino la tiene se encargará de buscarla; siendo ahora clientes DNS y lanzando consultas iterativas



CONSULTAS RECURSIVAS

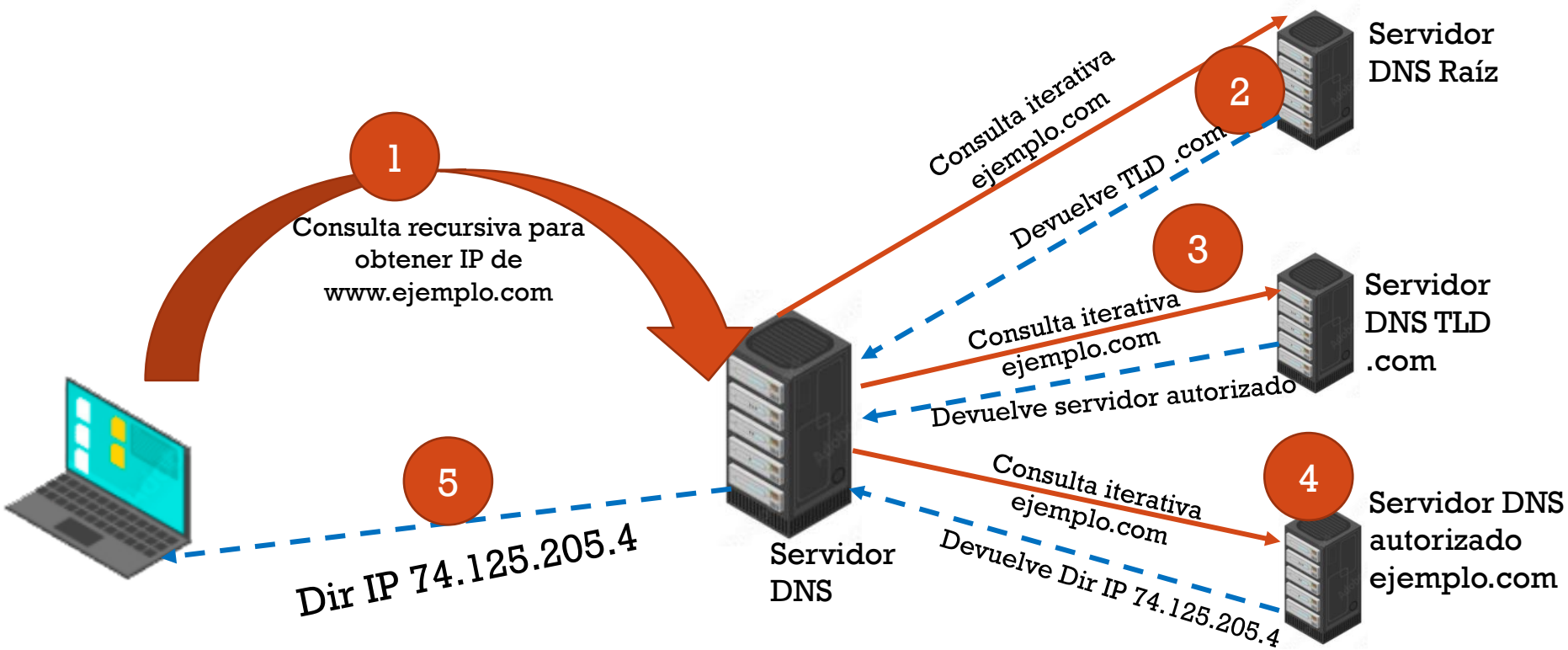
- Cuando recibe una consulta recursiva:
  - Si es autorizado para alguna zona, comprueba sus archivos de zona. Si encuentra la respuesta, responde indicando que la respuesta es autoritativa.
  - Si no encuentra la respuesta o no es autorizado y actúa como caché, consulta su caché. Si encuentra respuesta, la indica como respuesta no autoritativa.
  - En otro caso:
    - Si tiene configurados reenviadores, entonces reenvía la consulta recursiva a otro servidor DNS. La respuesta que obtenga se la traslada al cliente o al servidor que le preguntó.
    - Si no tiene reenviadores, inicia una serie de consultas iterativas a otros servidores DNS, que devuelven referencias a otros servidores DNS y termina cuando recibe una respuesta positiva o negativa.

CONSULTAS ITERATIVAS

- Es aquella en la que el servidor DNS puede proporcionar la **mejor respuesta posible** sin consultas externas adicionales
- El resultado de una consulta iterativa suele ser referencia a otros servidores DNS en la jerarquía de DNS. Este proceso se repite hasta llegar al servidor autorizado del domino

CONSULTAS ITERATIVAS

- Es aquella en la que el servidor DNS puede proporcionar la **mejor respuesta posible** sin consultas externas adicionales



CONSULTAS ITERATIVAS

- Los servidores TLD y servidores raíz están replicadas para aumentar fiabilidad
- Para mejorar el tiempo de respuesta, los servidores locales tienen dos mejoras:
  - Todos los servidores de nombre, periódicamente, se hacen una copia de los servidores raíz en un horario de mejor carga.
  - Cada servidor de nombre mantiene una caché de los nombres ya resueltos. Se registra dónde y cuándo se ha conseguido esa información. Tiene una fecha de caducidad, cuando se alcanza el tiempo establecido se elimina,

Caché DNS		
NOMBRE	DIRECCIÓN IP	TIEMPO DE VIDA
Ejemplo.com	74.125.205.4	3600

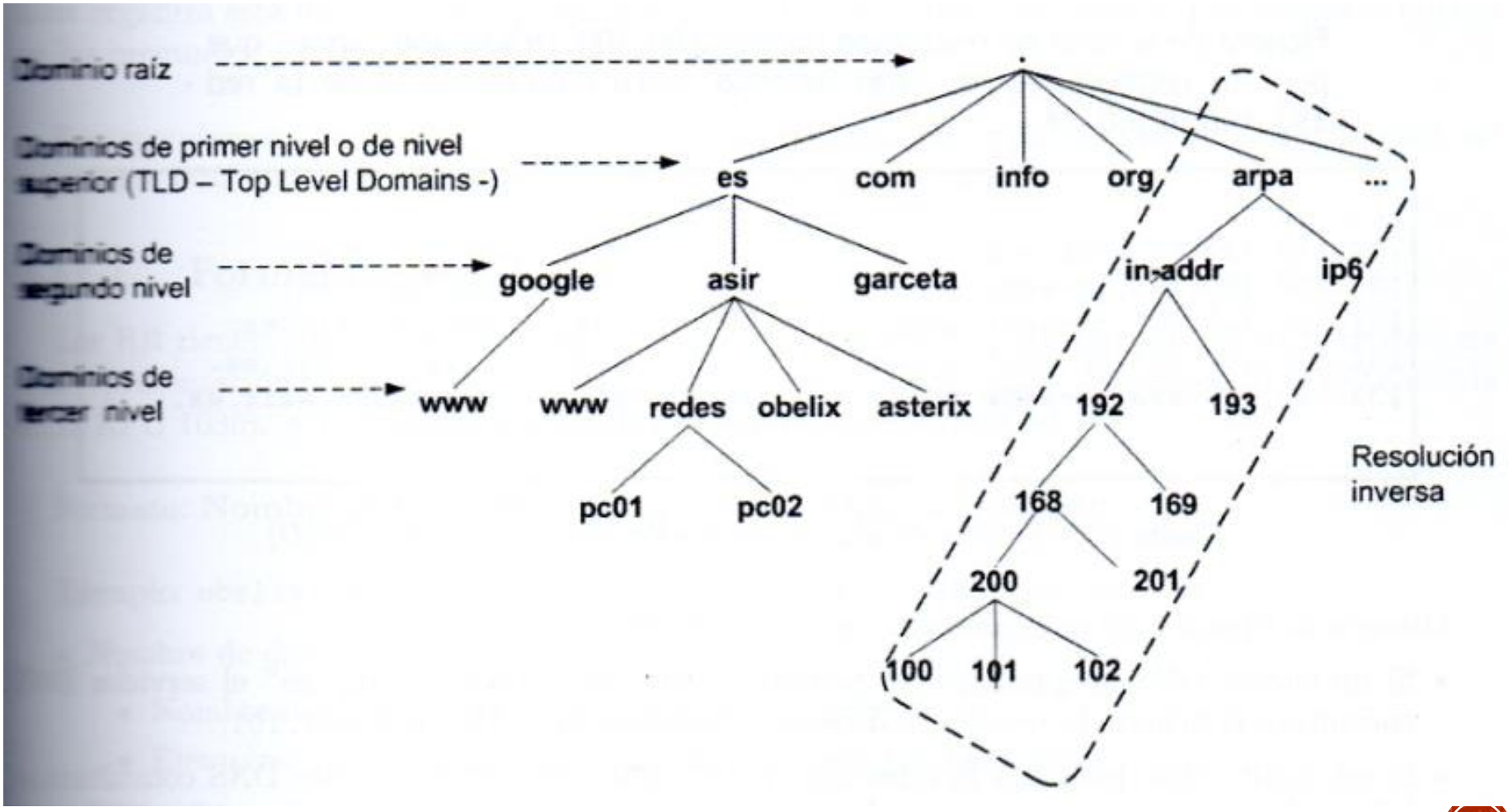
CONSULTAS ITERATIVAS

- Cuando un servidor recibe una consulta iterativa:
  - Si es autorizado para alguna zona, comprueba sus archivos de zona. Si encuentra respuesta, responde indicando que la respuesta es autoritativa.
  - Si no encuentra respuesta o no es autorizado y actúa como caché, consulta su caché de respuesta anteriores. Si tiene respuesta, responde indicando que la respuesta no es autoritativa.
  - Si no encuentra respuesta exacta con el nombre, devuelve una referencia que apunta a un servidor DNS que está autorizado para un nivel inferior del espacio de nombres de dominio.

RESOLUCIÓN INVERSA

- Una consulta inversa a un servidor DNS consiste en preguntar por una dirección IP en lugar de preguntar por un nombre de dominio.
- La resolución de direcciones IP funciona igual que la resolución de nombres de dominio. Las direcciones IP se tratan como nombres donde cada byte es un dominio que cuelga de los dominios "*in-addr.arpa*" para IPv4, e "*ip6.arpa*" para IPv6.
- Los nombres de dominio tienen una estructura jerárquica de derecha a izquierda, mientras que las IP tienen una estructura jerárquica de izquierda a derecha.

RESOLUCIÓN INVERSA



ZONAS DE RESOLUCIÓN INVERSA

- Los servidores de nombres tienen que almacenar zonas de resolución inversa con registros de recursos que asocien nombres de dominio con direcciones IP.
- Las zonas directas e inversas son independientes, y es responsabilidad de los administradores que contengan información coherente y que no existan discrepancias.
- No es obligatorio que quien administra la zona directa de un dominio, tenga que administrar la zona inversa correspondiente.
- El proceso de resolución inversa es similar al de resolución directa.

REGISTROS DE RECURSOS DNS

INTRODUCCIÓN

- Los servidores de nombres almacenan la información en registros
- Formato: (nombre, valor, tipo, ttl)
- TTL Tiempo en segundos

Tipo	Nombre	Valor
A (IPV4) o AAA(IPv6)	Nombre de un host	Dirección IP
Cname	Nombre es un alias	Nombre canónico
NS	Nombre de dominio	Nombre del servidor de nombres autorizados para el dominio

AL HACER UNA CONSULTA SE INDICA EL TIPO DE NOMBRE A RESOLVER

INTRODUCCIÓN

- Cada fichero de zona organiza su información en registros de recursos (RR, Resource Records) los cuales se envían entre las preguntas y respuestas entre cliente y servidores DNS.
- Formato general:
  - **Nombre del dominio**: Con el que se asocia el recurso
  - **TTL** (Time To Live): Es opcional y representa el número de segundos que puede estar el registro en caché antes de ser descartado
  - **Clase:** Define la arquitectura de protocolos usada. "*IN*" para la TCP/IP.
  - **Tipo (de registro):** Son diferentes en función del campo clase. Para IN hay varios (A, CNAME, NS,…)
  - **Tipo-Dato:** Información asociada al nombre de dominio, y que varía en función del tipo de registro. Por ejemplo, para el tipo A, representa la dirección IP.

vives.asir.es.	7200	IN	A	193.101.21.48

REGISTRO SOA

- Es el primer registro de una zona y define una serie de opciones generales de la misma.
- Los datos son:
  - MNAME: Nombre FQDN del servidor de nombres maestro del dominio.
  - Contacto: Correo de la persona responsable del dominio, donde la "@" se ha reemplazado por "."
  - Número de Serie (serial): Versión del archivo de zona, y debe ser incrementado cada vez que se modifique. Se utiliza para las transferencias de zona.
  - Actualización (refresh): Tiempo que esperan los servidores esclavos para preguntar al servidor maestro si hay cambios en la zona.

REGISTRO SOA

- **Reintentos (retry):** Si falla la transferencia de zona, el tiempo que se espera antes de volver a intentarlo.
- **Caducidad (expire):** Tiempo que el servidor esclavo está intentando contactar con el maestro para ver si hay cambios. Si este tiempo expira, el esclavo se declara como no autorizado, y no responde sobre esa zona.
- **TTL negativo (Time To Live):** Tiempo que se almacenan las respuestas negativas sobre esa zona.

```
asir.es.    IN    SOA       ns1.asir.es.    admin.asir.es. (
                                1               ; Número de serie
                                604800          ; Tiempo de refresco
                                86400           ; Tiempo de reintento
                                2419200             ; Tiempo de expiración
                                604800 )            ; TTL negativo
```

REGISTRO A Y AAAA

- Los registros de recursos A (Address) y AAAA (Address Address Address Addres) establecen una correspondencia entre un nombre de domino completamente cualificado (FQDN) y una dirección IP versión 4 y 6 respectivamente.

ns1.asir.es.	IN	A	193.100.200.25
ns2.asir.es.	IN	A	193.100.200.26
luis.asir.es.	IN	A	193.100.200.101
vives.asir.es.	IN	A	193.100.200.102
luis.asir.es.	IN	AAAA	2001:db8::63
vives.asir.es.	IN	AAAA	2001:db8::64

REGISTRO NS

- El registro de recursos NS (Name Server) permite establecer:
  - **Los servidores de nombres autorizados a una zona**. Cada zona debe contener, como mínimo, un registro NS. Los servidores DNS, pueden tener un nombre de la misma zona o de otras.
  - Quienes son **los servidores de nombres con autoridad en los subdominios delegados**. Cada zona debe contener, al menos, un registro NS por cada subdominio que haya delegado.
- La parte derecha de un registro NS no debe ser un nombre de tipo CNAME (alias).

REGISTRO NS

```
asir.es.    IN    NS    ns1.asir.es.     ; Servidor DNS maestro
asir.es.    IN    NS    ns2.asir.es.     ; Servidor DNS esclavo
asir.es.    IN    NS    dns.asir.org.    ; Servidor DNS esclavo

ns1.asir.es.    IN    A     193.48.54.100
ns2.asir.es.    IN    A     193.48.54.101

; Delegación
redes.asir.es.        IN    NS    ns1.redes.asir.es.    ; Delegación
sistemas.asir.es.     IN    NS    dns.asir.org.         ; Delegación

ns1.redes.asir.es.    IN    A     193.100.53.8
```

REGISTRO CNAME

- El registro de recursos CNAME (Canonical Name) permite crear alias para nombres de dominio especificados en registros A y AAAA.
- Un registro CNAME puede apuntar a un nombre de otro dominio.
- No se deben usar registros CNAME en la parte derecha de registros MX y NS. La parte derecha de estos recursos tiene que ser un nombre que aparezca en un registro de tipo A.
- El uso de muchos CNAME perjudica el rendimiento de los servidores DNS.

vives.asir.es.	IN	A	193.100.200.101
luis.asir.es.	IN	CNAME	vives.asir.es.
www.asir.es.	IN	CNAME	www.servicios.es.

REGISTRO MX

- El registro de recursos MX (Mail Exchange) permite definir equipos encargados de la entrega de correo en el dominio. Son consultados por los agentes de transporte de correo SMTP.
- Un registro MX puede apuntar a un nombre de otro dominio.
- Se pueden definir varios registros MX para un mismo dominio, es decir, varios servidores de correo para ese dominio. En cada registro MX se especifica un número positivo que determina la preferencia en el caso de que existan varios registros MX. El número más pequeño tienen mayor preferencia.
- La parte derecha no debe ser de tipo CNAME.

```
asir.es.              IN   MX   10   mail1.asir.es.
asir.es.              IN   MX   20   mail2.asir.es.
mail1.asir.es.        IN   A         193.100.200.221
mail2.asir.es.        IN   A         193.100.200.222
asir.es.        IN    MX   30   smtp.informática.es.
```

REGISTRO PTR

- El registro de recursos PTR (Pointer Record) establece una correspondencia entre nombres de direcciones IPv4 e IPv6 y nombres de dominios. Se utilizan en las zonas de resolución inversa.
- En una misma zona no puede haber registros PTR IPv4 y registros PTR IPv6.

```
100.200.100.193.in-addr.arpa.      IN    PTR ns1.asir.es.
200.200.100.193.in-addr.arpa.      IN    PTR ns2.asir.es.
```

TRANSFERENCIAS DE ZONAS

TRANSFERENCIA DE ZONA

- Los servidores DNS que declaran zonas esclavas o secundarias obtienen los archivos de zona (los registros de recursos) de otros servidores DNS autorizados para esas zonas. A ese proceso se le denomina transferencia de zona.
- Los servidores maestros usan el puerto 53/TCP para el intercambio de datos en las transferencias de zona.
- Existen 2 tipos de transferencia de zona:
  - Transferencias de zona completas (AXFR)
    - El maestro envía al servidor todos los datos de la zona.
  - Transferencias de zona incrementales (IXFR)
    - El maestro envía al esclavo los datos que han cambiado desde la última transferencia de zona.
    - Reduce el número de registros a enviar, por lo que consume menos recursos (ancho de banda, tiempo,…)

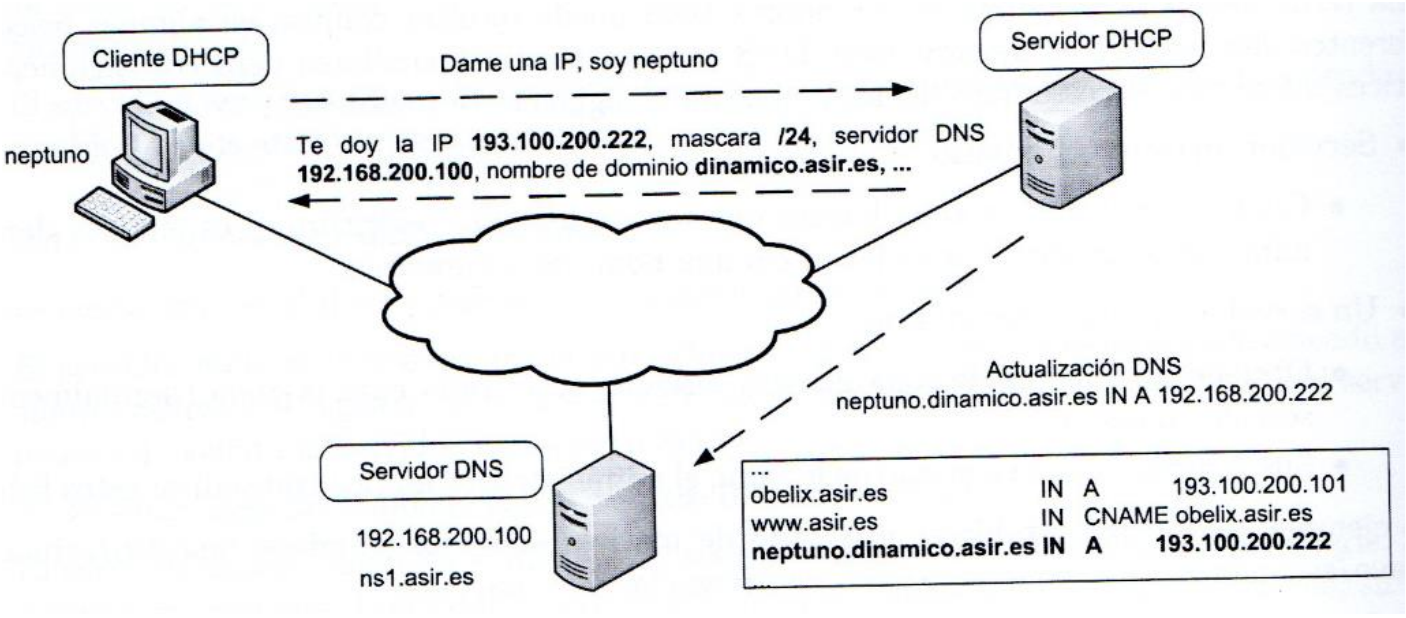
PROCESO DE TRANSFERENCIA DE ZONA

- Se inicia de dos formas:
  - El esclavo pregunta al maestro
  - El maestro notifica (NOTIFY) al esclavo que se han producido cambios en la zona.
- Pasos:
  - [Solo en NOTIFY]: Cuando se actualiza un archivo de zona, el servidor maestro envía un mensaje de notificación a los servidores esclavos.
  - El servidor esclavo solicita al servidor maestro su SOA. En el caso de [no NOTIFY], cuando se inicia por primera vez el esclavo, o cada cierto tiempo, se hace esta solicitud.
  - El maestro responde con el registro de recursos SOA.
  - El esclavo comprueba compara el número de serie devuelto con el suyo, y si es superior, sabe que su base de datos de registros no está actualizada.
  - El esclavo envía una petición AXFR o IXFR.
  - El maestro envía los datos de la zona al servidor secundario.

DNS DINÁMICO

DNS DINÁMICO (DDNS)

- Para que los usuarios tengan acceso a los recursos DNS correctamente, es fundamental que los servidores de nombres estén actualizados. La actualización se puede realizar:
  - Manualmente: Lo hace el administrador. Cuidado con clientes DHCP.
  - Dinámicamente.



SEGURIDAD

SEGURIDAD DNS

- DNS se diseñó como un sistema abierto y en sus especificaciones originales no se contemplaban aspectos de seguridad. Además, es complicado gestionar y administrar al ser un servicio distribuido por varios componentes que se comunican entre sí.
- DNS es un servicio vital para el funcionamiento de Internet, por lo que está en el punto de mira de potenciales atacantes.
- Amenazas:
  - Servidores DNS
    - Ataques contra el servidor
    - Modificación de los archivos de zona
    - Denegación de servicio (DoS)
  - Consultas de clientes a servidores
    - Envenenamiento de la caché del cliente, suplantando al servidor DNS remoto y enviando registros incorrectos.

SEGURIDAD DNS

- Consultas de servidores a otros servidores
  - Igual que de clientes a servidores
- Transferencia de zonas
  - Suplantación del servidor maestro que envía registros de recursos a los secundarios.
- Actualizaciones dinámicas a servidores DNS
  - Suplantación de la fuente externa que envía las actualizaciones al servidor DNS

- Mecanismos de seguridad:
  - Seguridad local en los servidores DNS
    - Configurar los privilegios, realizar copias de seguridad, crear servidores esclavos distribuidos en diferentes ubicaciones,…
  - Seguridad en la transferencia de zona
    - Lista de control de acceso, uso de cortafuegos
    - Algoritmos de claves secretas, mecanismos de autentificación Active Directory
  - Seguridad en consultas
    - Restringir a nivel IP qué clientes pueden preguntar a un servidor.

WHOIS

- Protocolo que permite realizar consultas a bases de datos que contienen información sobre el usuario, empresa u organización que registra un nombre de dominio y/o una dirección IP en internet.
- Existen webs especializadas:
  - http://www.whois.net
  - http://whois.domaintools.com
  - https://www.nic.es/sgnd/dominio/publicBuscarDominios.action

FUENTES

- "Servicios de Red e Internet".
  A. García Sánchez, A. González Sotillo
  Ed. Garceta

SERVICIOS DE NOMBRES DE DOMINIO (DNS)