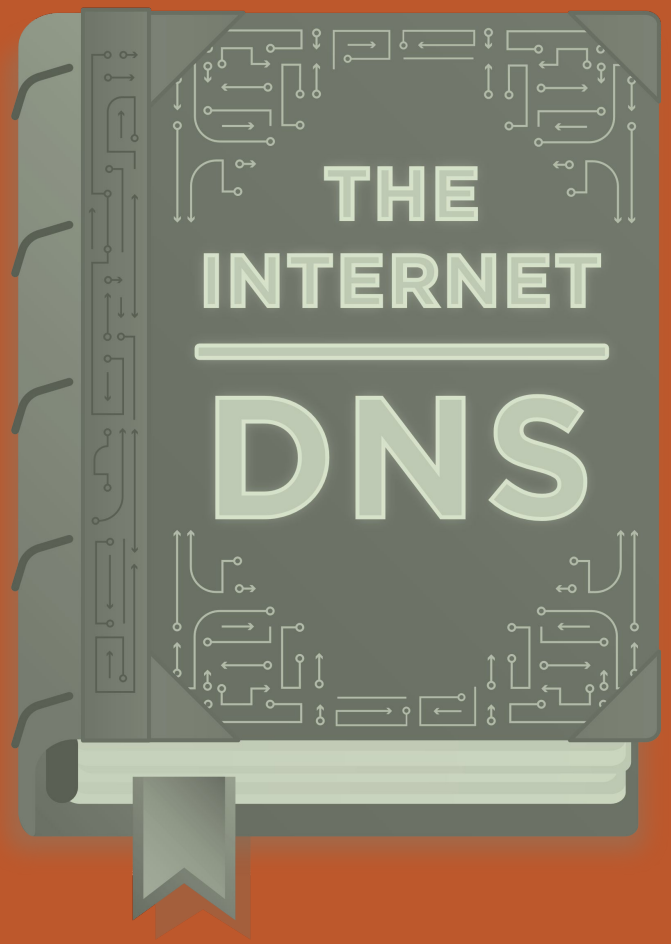
DNS

TEMA 3 - DAW



Los ordenadores se conectan entre sí usando direcciones IP

- Poco amigables para el usuario y difíciles de memorizar
- Mucho peor en IPv6: 2400:cb00:2048:1::c629:d7a2

Más fácil memorizar un nombre de dominio como *iesabastos.org*

Sistema de Nombres de Dominio (DNS):

Traducen nombres de dominio a direcciones IP

Introducción

Ventajas

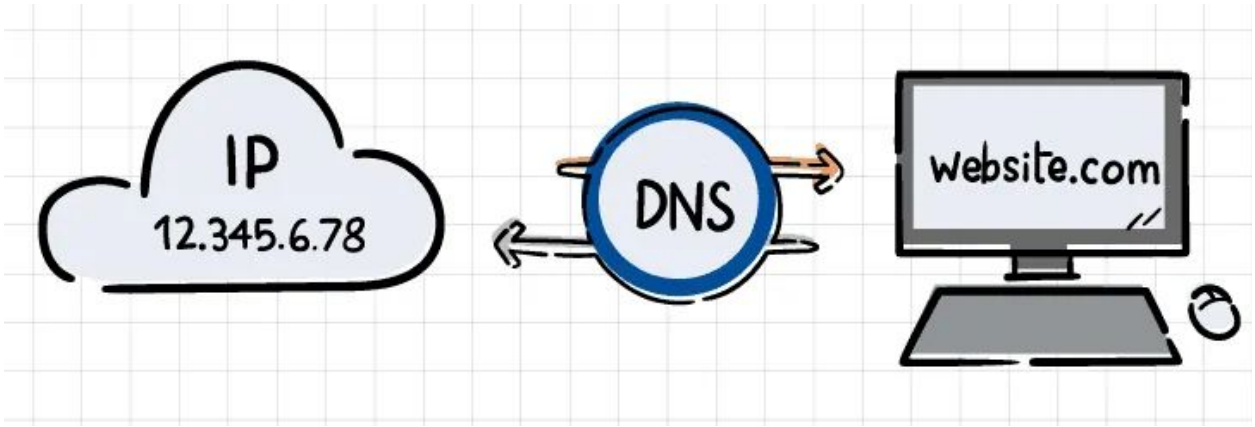
Más fácil de recordar

Más fiable: la IP puede cambiar

- Cambio de servidor
- Uso de CDN (Red de entrega de contenido)

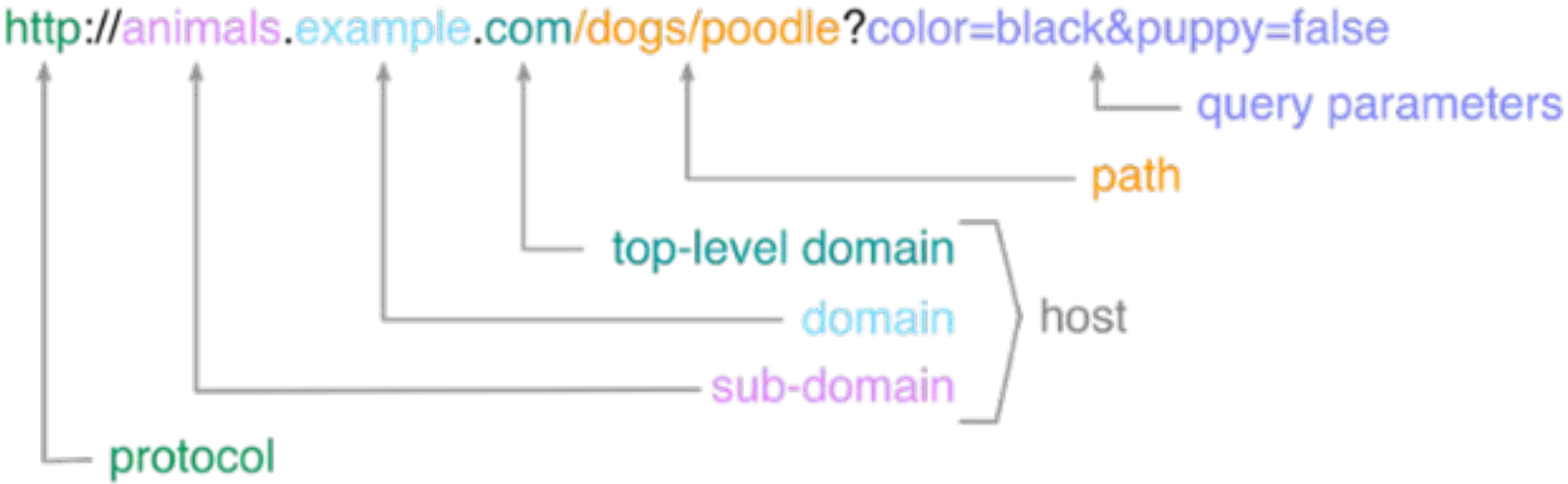
Desventajas

Seguridad: ataque de DNS



URL

URL = Protocolo + **NombreDominio** + Path + Query



Nombres de dominio

animals.example.com

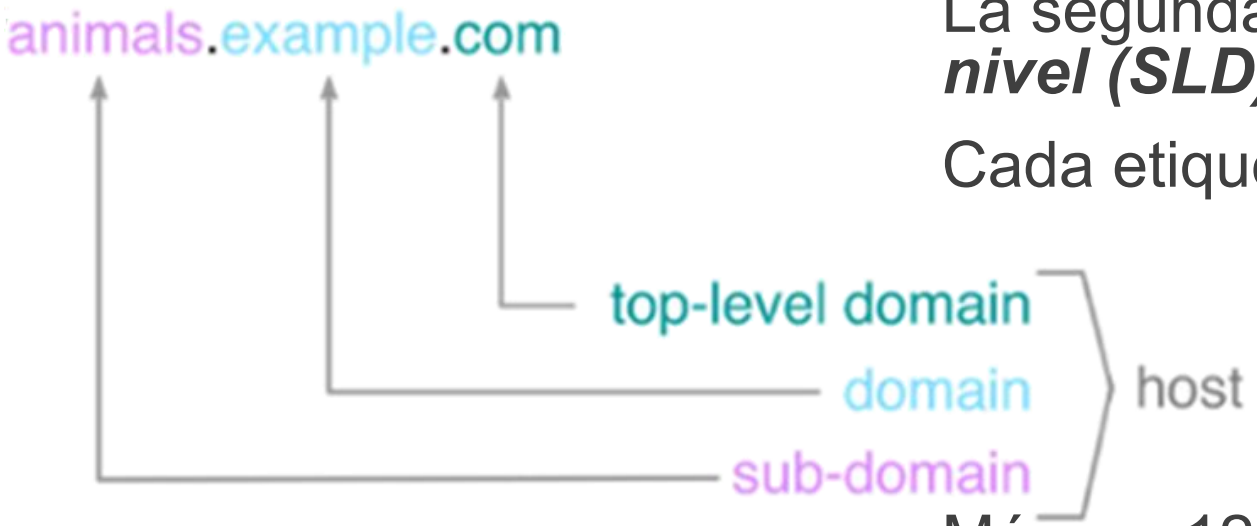
Formado por **dos o más etiquetas separadas por puntos**

Sintaxis de una etiqueta:

- Caracteres alfanuméricos y guión (-) como único símbolo permitido
- Longitud: entre 1 y 63 caracteres
- Comienza por letra y puede terminar por letra o número
- Mayúsculas no importan

Ojo! Las mayúsculas en el path sí importan

Nombres de dominio



La etiqueta de la derecha se llama ***dominio de nivel superior*** **(TLD)**

La segunda por la derecha ***dominio de segundo nivel (SLD)*** o simplemente dominio

Cada etiqueta a la izquierda es un ***subdominio***

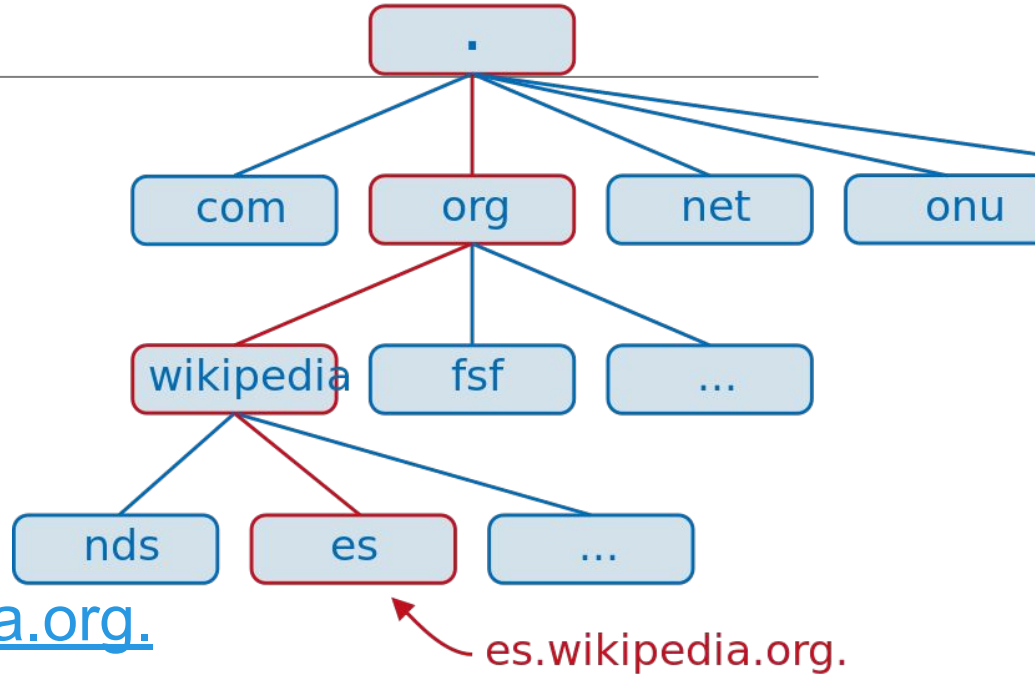
Máximo 127 subdominios sin superar los 255 caracteres

Nombres de dominio

Existe una jerarquía de nombres

Nodo raíz del que nacen los demás :

- No tiene nombre
- **Existe un punto a la derecha del todo que no se pone nunca**



www.es.wikipedia.org == www.es.wikipedia.org.

FQDN: Fully Qualified Domain Name

- Identifica de forma unívoca una máquina: `server.example.com.`

Registro de nombres

El nombre de dominio debe ser único

Una o varias autoridades que aseguren la unicidad

Internet Corporation for Assigned Names and Numbers (ICANN-IANA)

- Controla la creación de TLDs y mantiene un registro
- Delega el control de cada TLD a una entidad registral, que distribuye a su vez los SDL y mantiene un registro

Tipos de TLD

- De país (country code): ccTLD **`.es .eu .uk .ar .dj .fm`**
- Genéricos: gTLD **`.com .edu .org .net .coop .cat`**

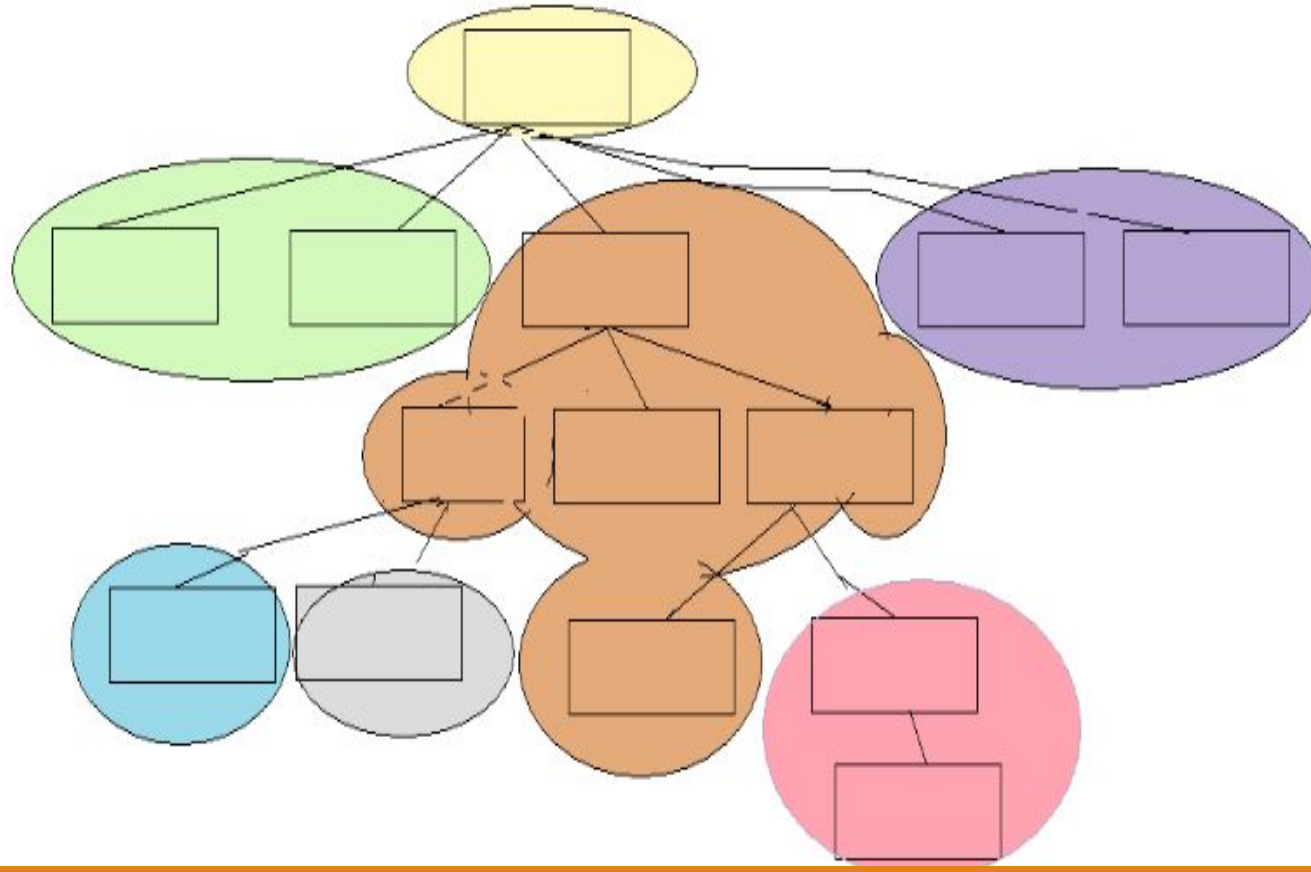
domain registry process

Zonas de autoridad

El espacio de nombres se divide en zonas de autoridad

- Contiguas y disjuntas por definición

Cada entidad registral es responsable del mantenimiento de la información en una zona de autoridad



Resolución de nombres

No existe un único lugar que almacene todo los nombres DNS

La base de datos de nombres DNS es **jerárquica** y **distribuida**

- Igual que lo son las autoridades registrales

Los servidores DNS sólo almacenan información de los dominios sobre los que tienen autoridad

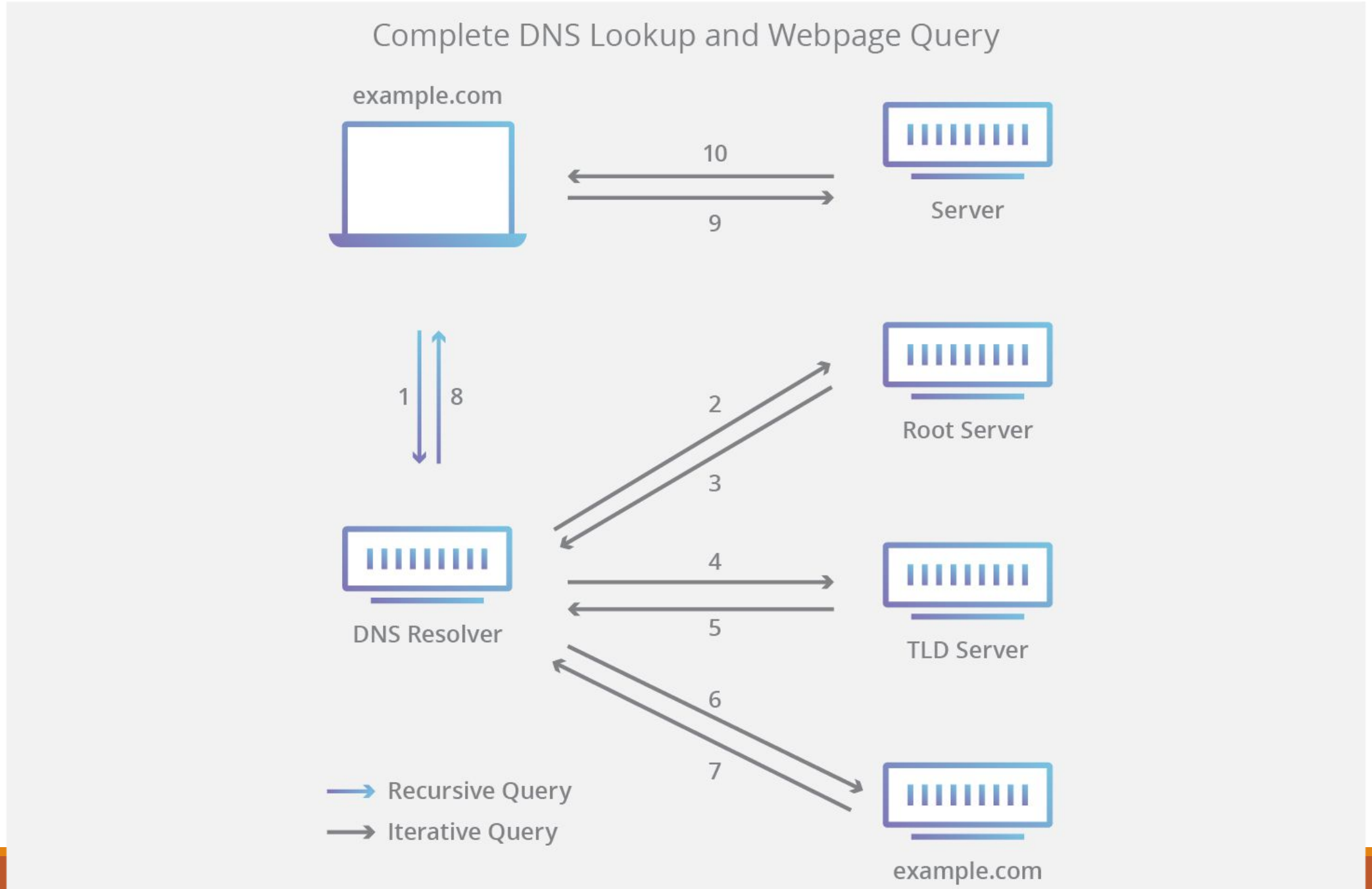
Resolución de nombres

Servidores implicados

- **Solucionador DNS**: recibe la petición de un cliente y trata de resolverla
- **Servidor de nombres raíz**: es el índice para encontrar los servidores TLD
- **Servidor de nombres TLD**: tiene la información de los dominios que comparten un mismo TLD
- **Servidor de nombres autoritativo**: última parada en la consulta DNS. Tiene las direcciones IP asociadas a todos los nombres de su zona de autoridad

Resolución de nombres - Símil

DNS	Biblioteca
Nombre de dominio	Palabra
Dirección IP	Significado de la palabra
Solucionador DNS	Bibliotecario al que le pedimos la definición de una palabra
Servidor de nombres raíz	Índice de la biblioteca que apunta a las diferentes estanterías que almacenan diccionarios con definiciones de palabras
Servidor TLD	Índice de una estantería de diccionarios
Servidor autoritativo	Diccionario con las definiciones de las palabras


Complete DNS Lookup and Webpage Query
example.com
10
9
Server
1
8
2
3
Root Server
DNS Resolver
4
5
TLD Server
6
7
Recursive Query
Iterative Query
example.com

Resolución de nombres - Pasos

1. Cliente consulta a un solucionador DNS (ejemplo.com)
2. Solucionador DNS consulta a un servidor de nombres raíz (.)
3. Servidor raíz responde con la IP de un servidor TLD (.com)
4. Solucionador DNS consulta a servidor TLD
5. Servidor TLD responde con la IP del servidor autoritativo de ejemplo.com
6. Solucionador DNS consulta a servidor autoritativo
7. Servidor autoritativo responde con la IP correspondiente al dominio solicitado (ejemplo.com)
8. Solucionador devuelve la IP al cliente que consultaba por ejemplo.com

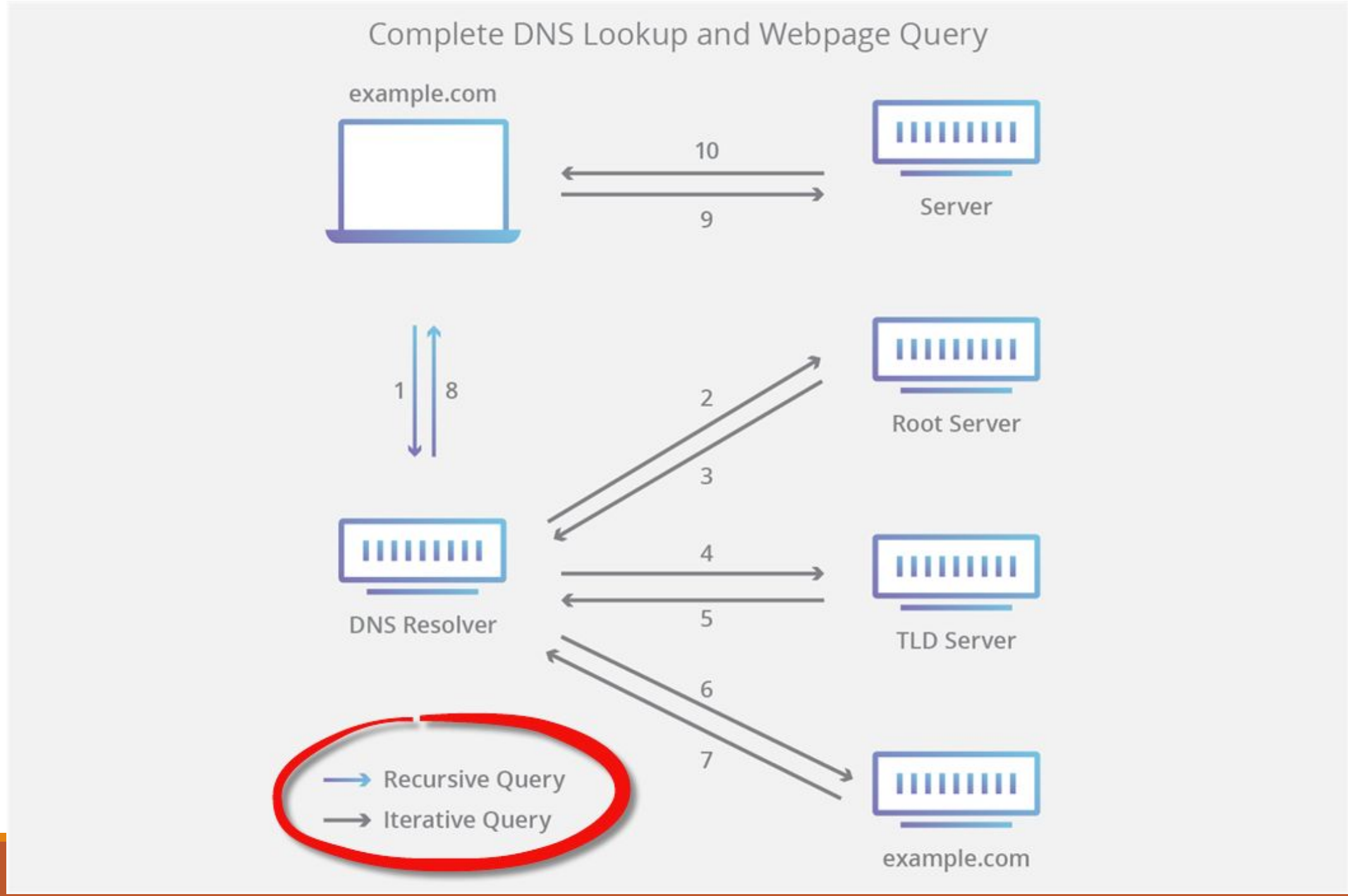
Tipos de Resolución

Resolución Iterativa

- Cuando un cliente realiza una consulta puede recibir la IP buscada o el nombre de otro servidor que está más cerca del objetivo
- El cliente vuelve a pedir al nuevo servidor la resolución del nombre

Resolución Recursiva

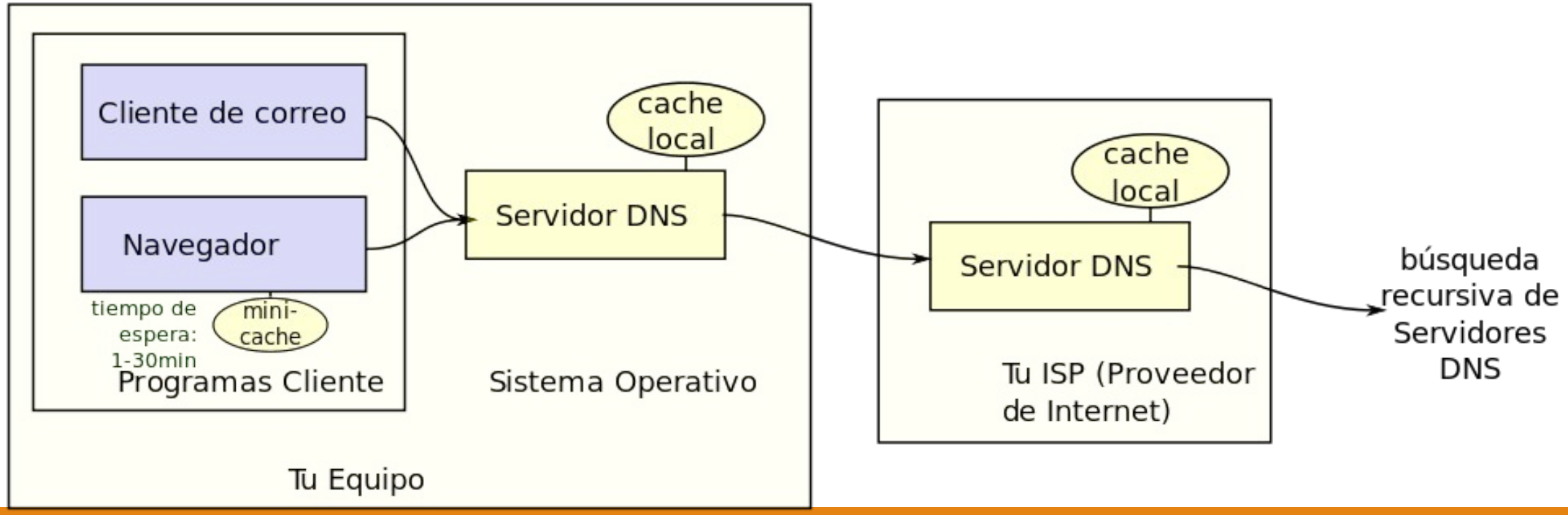
- El cliente pide la resolución del nombre y es responsabilidad del servidor de nombres (recursivo) realizar todas las consultas necesarias para conseguir la información
- No todos los servidores aceptan peticiones recursivas


Complete DNS Lookup and Webpage Query
example.com
10
9
Server
1
8
2
3
Root Server
DNS Resolver
4
5
TLD Server
6
7
Recursive Query
Iterative Query
example.com

Optimización de consultas

Almacenamiento en caché en ubicaciones más cercanas al cliente

Los datos se almacenan en caché durante un tiempo de vida (TTL)



Caché del servidor DNS

Más compleja para ahorrar más consultas:

- Si no tiene la IP pero tiene la dirección del servidor autoritativo, consulta a éste
- Si no tiene el servidor autoritativo pero tiene el servidor TLD, consulta a éste
- Si no tiene nada (improbable) consulta al servidor raíz. Sólo ocurrirá cuando se ha purgado la caché DNS

Caché DNS local

Windows

Consultar caché DNS local: **`ipconfig /displaydns`**

Borrar caché DNS local: **`ipconfig /flushdns`**

Linux

No tienen caché por defecto

Diferentes servicios de cacheo dependiendo de la distro

Registros de recursos DNS

Información que almacena un servidor para sus zonas de autoridad

Un registro tiene :

- Nombre: del nodo al que está asociado
- Tipo: existen diferentes tipos de registros
- Tiempo de vida (TTL): indica en segundos la frecuencia con la que el servidor actualizará la información del registro
- Información: dependiendo del tipo de registro

Tipos de registros más comunes

Tipo	Descripción	Función
A	Address	Devuelve una dirección IPv4 de 32 bits
AAAA	IPv6 Address	Devuelve una dirección IPv6 de 128 bits
CNAME	Canonical name	Alias de un nombre a otro: la búsqueda de DNS continuará reintentando la búsqueda con el nuevo nombre
MX	Mail Exchange	Asocia el nombre de dominio con una lista ordenada de servicios de correo electrónico
NS	Name Server	Indica el servidor de nombres autoritativo para un dominio
PTR	Pointer Record	Asocia un nombre de dominio a una IP (al contrario de un registro A) Útil para realizar búsquedas de DNS inverso
SOA	Start of authority	Información de una zona de autoridad, incluyendo servidor de nombres primario, email del administrador de dominio, el número de serie del dominio e indicaciones sobre los tiempos de refresco del servidor

Servidores Raíz

Esenciales: conocen las IP de los servidores TLD

Hay 13 servidores raíz (o grupos de servidores)

- Con 13 nombres y 13 IPs
- Desde a.root-servers.net hasta m.root-servers.net

Sistema de alta redundancia

- Además, cada servidor (raíz, TLD o autoritativo) también es redundante en sí mismo

https://dnswatch.com/dns-docs/root-server-locations

Servidores Redundantes

Tener un solo servidor por zona sería peligroso (fallos o alta demanda)

Una zona tiene al menos un **servidor DNS primario**

- Almacena los registros DNS y puede modificarlos

Puede tener varios **servidores secundarios**

- Almacenan copia de solo lectura de los registros DNS
- Reciben la información desde el servidor primario en un proceso llamado transferencia de zona

Esta práctica permite

- Redundancia y mayor resiliencia ante fallos
- Balanceo de carga

Transferencia de zona

Iniciada por el servidor secundario

- Le permite replicar la información de zona almacenada en un primario

¿Cuándo ocurre?

- Al iniciar el servidor secundario
- Cuando caduca el tiempo de actualización
- Cuando el servidor secundario recibe una notificación de modificación del fichero principal

Proceso

1. Consultar registro SOA
2. Si el nº versión ha cambiado se inicia la transferencia

Mejoras del sistema DNS

DNS Notify

- Permite al primario informar de cambios en el fichero de zona
- Reduce tiempo empleado por el secundario comprobando si tiene información actualizada
- Reduce tiempo que el secundario almacena registros desactualizados

Transferencia de zona incremental

- Permite trasferir sólo los cambios
- Reduce tiempo y ancho de banda utilizado en las trasferencias

Mejoras del sistema DNS

DNS Dinámico

- Cuando un servidor web tiene una IP dinámica necesitamos actualizar los registros DNS constantemente
- Se utiliza un software en el servidor que informa al servidor DNS de cada cambio de IP
- El servidor DNS podrá notificar los cambios a los servidores secundarios

DNS Inverso

Es una consulta DNS del nombre de dominio asociado a una determinada dirección IP

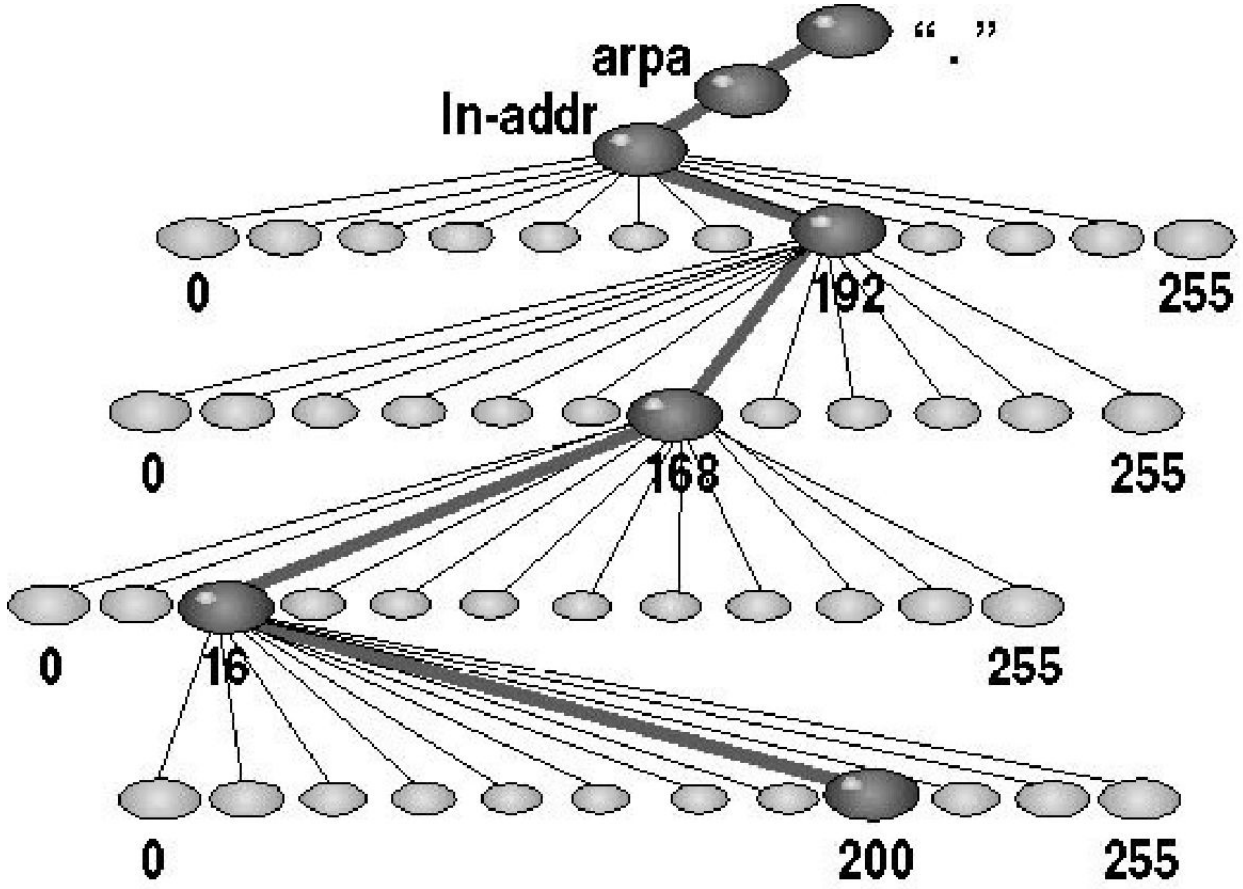
Usa una jerarquía numérica en el dominio “in-addr.arpa”

Los nombres se crean

- A partir de las direcciones IP con los segmentos invertidos
- Se añade al final “.in-addr.arpa”
- Ejemplo: para la IP 192.0.2.1 tenemos el nombre 1.2.0.192.in-addr.arpa

El nombre de dominio asociado a la IP se almacena en un registro PTR

DNS Inverso



Cada zona DNS es administrada por el ISP propietario de cada bloque de direcciones IPs

Para insertar un registro PTR debemos contactar con el ISP

Protocolo de transporte

DNS necesita ser rápido

UDP:

- La mayoría de las consultas

TCP:

- Para las respuestas largas (> 512 bytes). Por ejemplo: transferencias de zona

Puerto 53

- Tanto en UDP como en TCP

nslookup

Herramienta disponible en varios SOs, permite visualizar las peticiones DNS.
Modo interactivo **(nslookup en una consola)**

- **`<dominio> :`** resuelve la IP del dominio
- **`server <serverDNS> :`** cambia el serverDNS para las próximas peticiones
- **`<IP>`** : devuelve el nombre de dominio (DNS inverso)
- **`set type=A`** : solicita registros de dirección (A o AAAA)
- **`set type=ns`** : solicita el registro NS (muestra el servidor de nombres para un dominio)
- **`set type=mx`** : solicita el registro MX
- **`set type=any`** : solicita todos los datos de un dominio

Ejercicio 1

1. Comprueba cuál es el servidor DNS de tu máquina
   Windows: ipconfig /all
   Linux: cat /etc/resolv.conf
2. Cómo lo cambiarías
   Windows: GUI
   Linux: ~~editar resolv.conf~~

NSLOOKUP

1. Usa nslookup para saber la IP de www.google.es. ¿Qué servidor está dando la respuesta? ¿Es autoritativo?
   ```
   $ nslookup
   > www.google.es
   ```
2. Utiliza el servidor DNS 8.8.8.8 para obtener la IP de www.google.es. ¿Es autoritativo?
   **

Ejercicio 2

1. Cambia el tipo de registro a NS para conocer los servidores de nombres de www.google.es. Obten el servidor de nombres de www.google.es.
   ```
   > set type=ns
   > www.google.es
   ```
2. Intenta que el mismo servidor de nombres resuelva iesabastos.org. ¿Qué ocurre?
   ```
   > set type=ns
   > iesabastos.org
   ```
3. Obtén un listado de los servidores de nombres autorizados para el dominio “es”
   ```
   > set type=ns
   > es
   ```
4. Obtén un listado de los servidores raíz
   ```
   > set type=ns
   > .
   ```

Ejercicio 3

1. Utiliza la herramienta www.intodns.com para conocer los servidores DNS a los que se pregunta antes de llegar el servidor autoritativo para resolver los siguientes nombres de dominio

   upv.es google.es google.com iesabastos.org

2. El protocolo WHOIS permite realizar consultas a una base de datos para conocer el propietario de un dominio o IP.
   Utiliza la página www.mrdomain.com/es/whois/ para conocer el los datos de registro de los dominios anteriores