IES Abastos – DAW 7K
Despliegue de Aplicaciones Web
Oscar Pereira

Apuntes DNS

El **DNS (Domain Name System)** es un sistema que traduce nombres de dominio legibles por humanos (como www.ejemplo.com) en direcciones IP numéricas (como 192.168.1.1) que las computadoras utilizan para identificarse en una red. Funciona como una "agenda telefónica" de Internet, permitiendo a los usuarios acceder a sitios web utilizando nombres fáciles de recordar en lugar de series de números.

Ventajas del DNS

1. **Facilidad de uso**: Permite a los usuarios acceder a sitios web utilizando nombres en lugar de direcciones IP numéricas, lo que es más intuitivo y fácil de recordar.
2. **Escalabilidad**: Es un sistema distribuido y jerárquico, lo que permite manejar millones de dominios sin colapsar.
3. **Redundancia**: Los servidores DNS están replicados en múltiples ubicaciones, lo que garantiza alta disponibilidad y resistencia a fallos.
4. **Actualizaciones dinámicas**: Permite cambios en las direcciones IP asociadas a un dominio sin afectar al usuario final.
5. **Organización**: Facilita la gestión de redes al asignar nombres lógicos a dispositivos y servicios.

Desventajas del DNS

1. **Vulnerabilidades de seguridad**: Es susceptible a ataques como el **envenenamiento de caché DNS** o el **secuestro de DNS**, que pueden redirigir a los usuarios a sitios maliciosos.
2. **Dependencia de servidores**: Si los servidores DNS fallan o están sobrecargados, los usuarios no pueden acceder a los sitios web.
3. **Latencia**: Las consultas DNS pueden introducir retrasos en la carga de páginas web, especialmente si los servidores están lejos geográficamente.
4. **Complejidad de gestión**: Configurar y mantener servidores DNS requiere conocimientos técnicos avanzados.
5. **Centralización**: Aunque es un sistema distribuido, gran parte de la infraestructura DNS está controlada por unas pocas organizaciones, lo que puede generar riesgos de monopolio o censura.

Protocolo de transporte

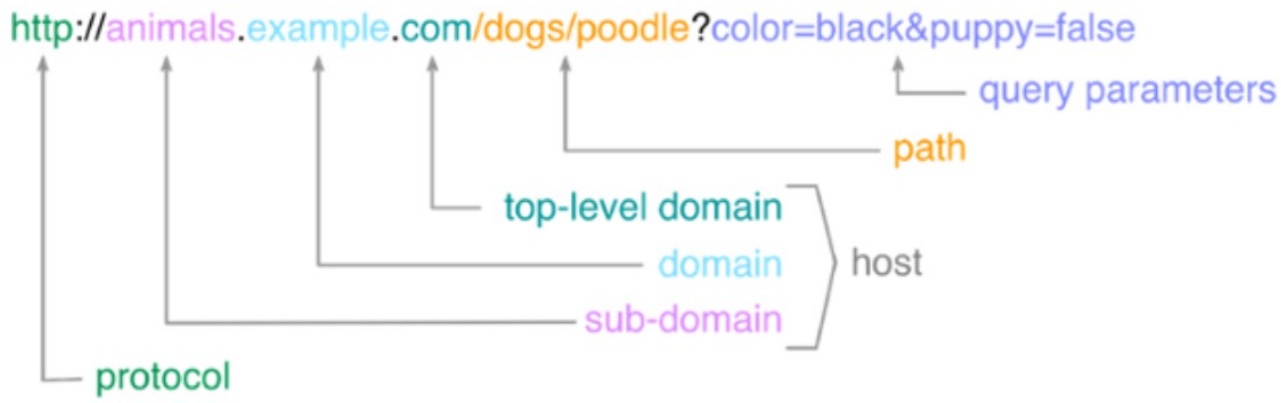
DNS necesita ser rápido

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

URL



Nombres de Dominio

1. **Estructura**:
    - Formado por dos o más etiquetas separadas por puntos.
    - Ejemplo: `www.ejemplo.com`.
2. **Sintaxis de una etiqueta**:
    - Caracteres permitidos: alfanuméricos y guión (`-`).
    - Longitud: entre 1 y 63 caracteres.
    - Debe comenzar por letra y puede terminar por letra o número.
    - Las mayúsculas no importan en el dominio, pero sí en el **path** (ruta).
3. **Partes de un dominio**:
    - **TLD (Dominio de Nivel Superior)**: La etiqueta más a la derecha (ej: `.com`, `.org`).
    - **SLD (Dominio de Segundo Nivel)**: La segunda etiqueta por la derecha (ej: `ejemplo` en `ejemplo.com`).
    - **Subdominios**: Cada etiqueta a la izquierda del SLD (ej: `www` en `www.ejemplo.com`).

4. **Límites**:
    - Máximo de 127 subdominios.
    - Longitud total no puede superar 255 caracteres.
5. **Jerarquía**:
    - El **nodo raíz** no tiene nombre y se representa con un punto al final (no se escribe).
    - Ejemplo: `www.es.wikipedia.org` es igual a `www.es.wikipedia.org.`
6. **FQDN (Fully Qualified Domain Name)**:
    - Identifica de forma única una máquina en la red.
    - Incluye todas las etiquetas hasta el nodo raíz.
    - Ejemplo: `server.example.com.`

Este sistema permite organizar y acceder a recursos en Internet de manera estructurada y jerárquica.

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

Proceso de Registro de un Dominio

1. **Registrant (Titular)**:
    - Es la persona o organización que solicita y posee el nombre de dominio.
    - Elige el nombre de dominio y lo registra a través de un **registrar**.
2. **Reseller (Revendedor)**:
    - Actúa como intermediario entre el **registrant** y el **registrar**.
    - Ofrece servicios de registro de dominios, pero no tiene acceso directo a la base de datos de dominios.
3. **Registrar (Registrador)**:
    - Empresa acreditada por **ICANN** para vender nombres de dominio al público.
    - Verifica la disponibilidad del dominio y gestiona el proceso de registro.
    - Ejemplos: GoDaddy, Namecheap, Google Domains.
4. **Registry Operators (Operadores de Registro)**:
    - Organizaciones que gestionan y mantienen las bases de datos de un **TLD** específico (como `.com`, `.es`, etc.).
    - Se encargan de asegurar que los dominios sean únicos dentro de su TLD.
    - Ejemplos: Verisign (para `.com`), EURid (para `.eu`).
5. **ICANN (Internet Corporation for Assigned Names and Numbers)**:
    - Organización global que supervisa el sistema de nombres de dominio y direcciones IP.
    - Acredita a los **registrars** y aprueba la creación de nuevos **TLDs**.
    - Garantiza la unicidad y estabilidad del sistema DNS.

Zonas de Autoridad

El espacio de nombres de DNS se divide en **zonas de autoridad,** cada zona es una porción contigua y disjunta del espacio de nombres.

1. **Responsabilidad**:
    - Cada **entidad registral** es responsable de mantener la información dentro de su zona de autoridad.
    - Esto incluye gestionar los registros DNS (como direcciones IP, servidores de correo, etc.) para los dominios dentro de esa zona.
2. **Características**:
    - **Contiguas**: Las zonas cubren un rango continuo de nombres de dominio.
    - **Disjuntas**: No se superponen entre sí, cada nombre de dominio pertenece a una única zona.
3. **Funcionamiento**:
    - Las zonas permiten una administración descentralizada del DNS.
    - Cada zona tiene uno o más **servidores de nombres (nameservers)** que responden a consultas sobre los dominios dentro de esa zona.
4. **Ejemplo**:
    - Una entidad puede ser responsable de la zona `example.com`, gestionando todos los subdominios como `www.example.com`, `mail.example.com`, etc.

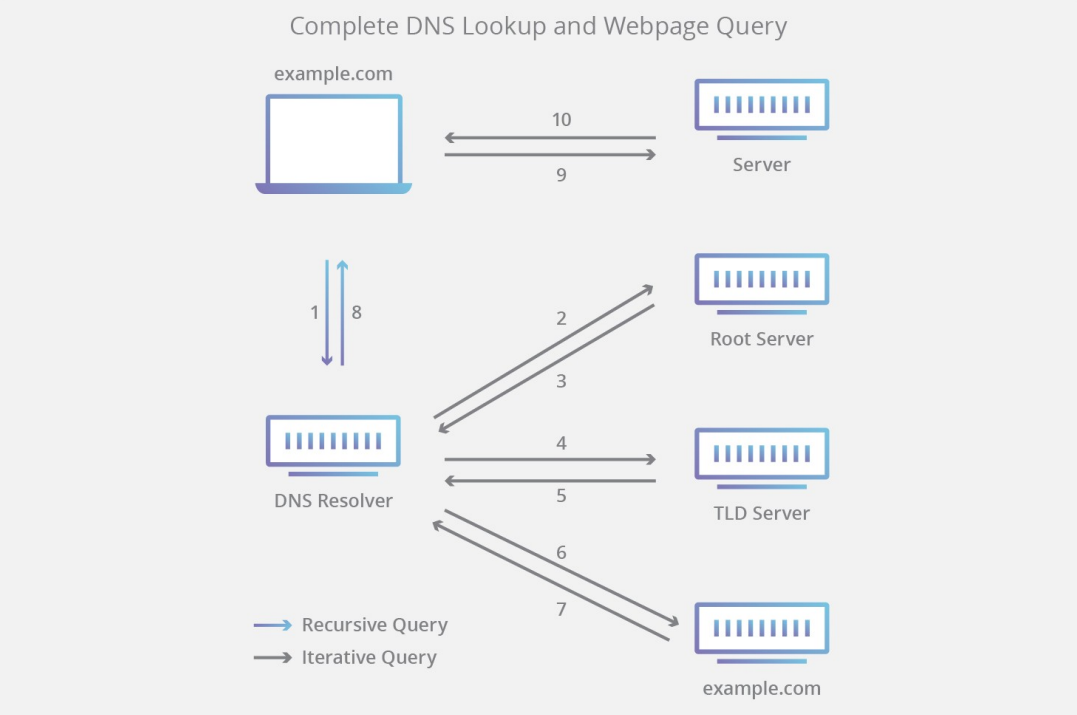
En resumen, las **zonas de autoridad** organizan el espacio de nombres de DNS en áreas manejables, delegando la responsabilidad de mantenimiento a entidades específicas para garantizar un funcionamiento eficiente y escalable.

Resolución de nombres

Base de Datos Distribuida:

- No existe un único lugar que almacene todos los nombres DNS.
- La base de datos de nombres DNS es **jerárquica** y **distribuida**, al igual que las autoridades registrales.

2. **Funcionamiento de los Servidores DNS**:
    - Cada servidor DNS solo almacena información sobre los dominios sobre los que tiene **autoridad**.
    - La resolución de nombres implica la colaboración de varios servidores DNS.
3. **Servidores Implicados**:
    - **Solucionador DNS (Resolver)**:
        - Recibe la petición de un cliente (por ejemplo, un navegador).
        - Se encarga de iniciar y gestionar el proceso de resolución del nombre.
    - **Servidor de Nombres Raíz (Root Server)**:
        - Es el punto de partida en la búsqueda.
        - Proporciona la dirección de los servidores TLD correspondientes.
    - **Servidor de Nombres TLD (Top-Level Domain Server)**:
        - Contiene información sobre los dominios que comparten un mismo TLD (como `.com`, `.es`).
        - Indica la dirección del servidor autoritativo para el dominio específico.
    - **Servidor de Nombres Autoritativo (Authoritative Server)**:
        - Es la última parada en la consulta DNS.
        - Almacena las direcciones IP asociadas a los nombres de dominio dentro de su **zona de autoridad**.
4. **Proceso de Resolución**:
    - El **solucionador DNS** recibe una consulta (por ejemplo, `www.ejemplo.com`).
    - Consulta al **servidor raíz** para obtener la dirección del servidor TLD correspondiente (`.com`).
    - El **servidor TLD** indica la dirección del **servidor autoritativo** para `ejemplo.com`.
    - El **servidor autoritativo** responde con la dirección IP asociada a `www.ejemplo.com`.
    - El solucionador devuelve la IP al cliente, permitiendo la conexión.



Existen varios tipos de resolucion DNS.

Resolución Iterativa

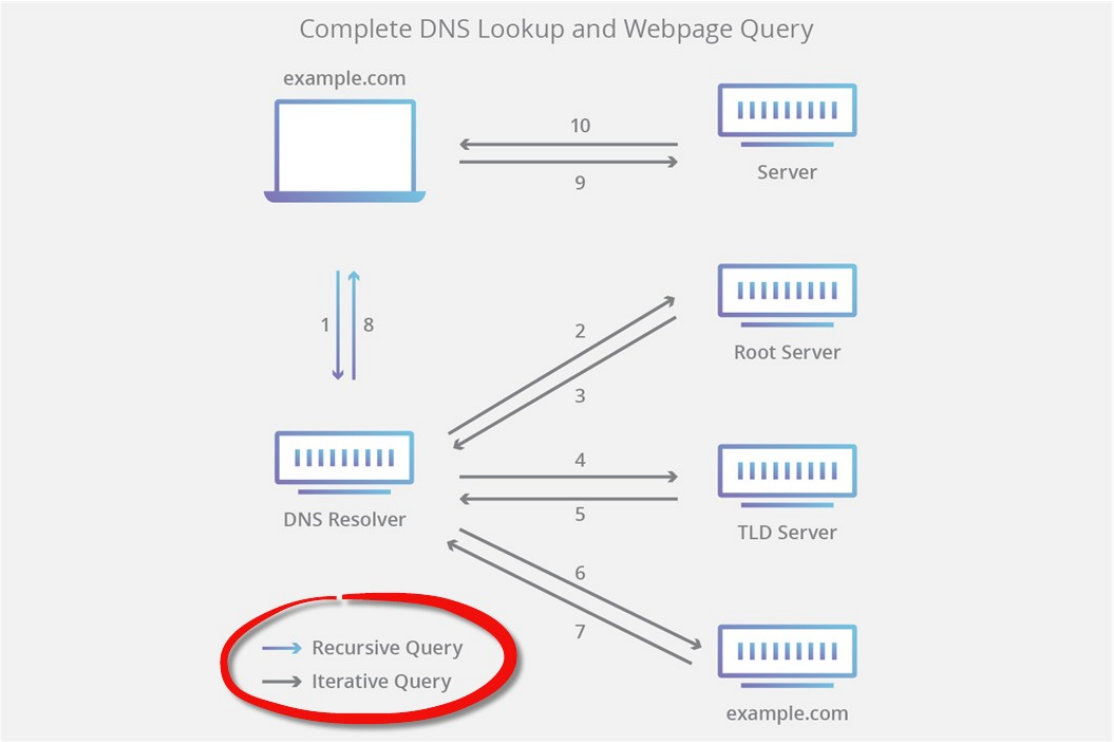
Cuando un cliente realiza una consulta puede recibir la IP buscada o el nombre de otro servidor que está más cerca del objetivo

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

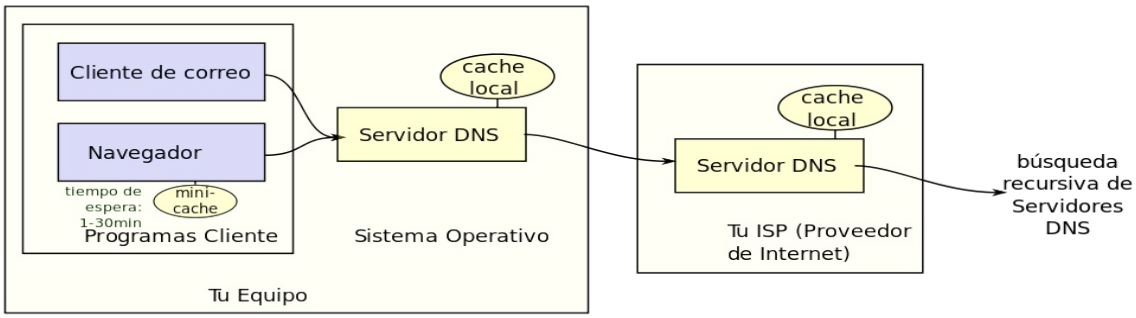
No todos los servidores aceptan peticiones recursivas



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 DNS

1. **Funcionamiento de la Caché DNS**:
    - La caché DNS almacena respuestas anteriores para reducir el número de consultas y acelerar la resolución de nombres.
    - Es más compleja para optimizar el proceso:
        - Si no tiene la IP, pero tiene la dirección del **servidor autoritativo**, consulta directamente a este.
        - Si no tiene el servidor autoritativo, pero tiene la dirección del **servidor TLD**, consulta a este.
        - Si no tiene nada (raro), consulta al **servidor raíz** (solo ocurre cuando la caché se ha purgado).
2. **Caché DNS en Windows**:
    - **Consultar la caché DNS local**:
        - Comando: `ipconfig /displaydns`.
        - Muestra las entradas DNS almacenadas en la caché.
    - **Borrar la caché DNS local**:
        - Comando: `ipconfig /flushdns`.
        - Elimina todas las entradas de la caché DNS.
3. **Caché DNS en Linux**:
    - Por defecto, Linux no tiene una caché DNS local habilitada.
    - Dependiendo de la distribución, se pueden usar servicios de caché DNS como:
        - **systemd-resolved** (en distribuciones con systemd).
        - **dnsmasq** (común en entornos de red pequeños).
        - **nscd** (Name Service Caching Daemon).
    - Para gestionar la caché, se deben usar los comandos específicos del servicio instalado.

Registros de Recursos DNS

Los **registros de recursos DNS** son la información que un servidor DNS almacena para sus zonas de autoridad. Cada registro contiene:

1. **Estructura de un Registro**:
    - **Nombre**: El nodo o dominio al que está asociado.
    - **Tipo**: Indica el tipo de registro (por ejemplo, A, MX, NS, etc.).
    - **TTL (Time to Live)**: Tiempo en segundos que el registro puede permanecer en la caché antes de ser actualizado.
    - **Información**: Depende del tipo de registro (por ejemplo, una dirección IP, un nombre de servidor, etc.).

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 continúa con el nuevo nombre.
MX	Mail Exchange	Asocia el dominio con una lista ordenada de servidores de correo electrónico.
NS	Name Server	Indica el servidor de nombres autoritativo para un dominio.
PTR	Pointer Record	Asocia una dirección IP a un nombre de dominio (usado en búsquedas DNS inversas).
SOA	Start of Authority	Contiene información sobre la zona de autoridad, como el servidor primario, email del admin, número de serie y tiempos de refresco.

Ejemplos de Registros

1. **Registro A**:
    - Nombre: `www.ejemplo.com`
    - Tipo: A
    - TTL: 3600
    - Información: `192.168.1.1`
2. **Registro MX**:
    - Nombre: `ejemplo.com`
    - Tipo: MX
    - TTL: 14400
    - Información: `10 mail.ejemplo.com`

3. **Registro CNAME**:
    - Nombre: `web.ejemplo.com`
    - Tipo: CNAME
    - TTL: 7200
    - Información: `www.ejemplo.com`
4. **Registro SOA**:
    - Nombre: `ejemplo.com`
    - Tipo: SOA
    - TTL: 86400
    - Información: `ns1.ejemplo.com admin.ejemplo.com 2023101501 7200 3600 1209600 3600`

Servidores Raíz

1. **Función**:
    - Conocen las direcciones IP de los **servidores TLD** (Top-Level Domain).
    - Son esenciales para iniciar la resolución de nombres DNS.
2. **Estructura**:
    - Hay **13 servidores raíz** (o grupos de servidores) distribuidos globalmente.
    - Nombres: Desde `a.root-servers.net` hasta `m.root-servers.net`.
    - Cada nombre tiene una dirección IP asociada.
3. **Redundancia**:
    - Cada servidor raíz es altamente redundante, con múltiples instancias físicas en diferentes ubicaciones.
    - Esto garantiza alta disponibilidad y resistencia a fallos.

Servidores Redundantes

1. **Necesidad de Redundancia**:
    - Un solo servidor por zona es riesgoso (fallos o alta demanda).
    - Cada zona tiene al menos un **servidor DNS primario** y varios **servidores secundarios**.
2. **Funciones**:
    - **Servidor Primario**:
        - Almacena los registros DNS y permite modificarlos.
    - **Servidores Secundarios**:
        - Almacenan una copia de solo lectura de los registros DNS.
        - Reciben la información del servidor primario mediante **transferencia de zona**.
3. **Ventajas**:
    - **Redundancia**: Mayor resiliencia ante fallos.
    - **Balanceo de carga**: Distribución de consultas entre servidores.

Transferencia de Zona

1. **Proceso**:
    - Iniciado por el servidor secundario.
    - Replica la información de zona almacenada en el servidor primario.
2. **Cuándo Ocurre**:
    - Al iniciar el servidor secundario.
    - Cuando caduca el tiempo de actualización.
    - Cuando el servidor secundario recibe una notificación de cambios en el servidor primario.
3. **Pasos**:
    - El servidor secundario consulta el registro **SOA** (Start of Authority).
    - Si el número de versión ha cambiado, se inicia la transferencia.

Mejoras del Sistema DNS

1. **DNS Notify**:
    - Permite al servidor primario notificar a los secundarios sobre cambios en el fichero de zona.
    - **Ventajas**:
        - Reduce el tiempo que los secundarios pasan comprobando actualizaciones.
        - Minimiza el tiempo con registros desactualizados.
2. **Transferencia de Zona Incremental**:
    - Transfiere solo los cambios en lugar de toda la zona.
    - **Ventajas**:
        - Reduce el tiempo y el ancho de banda utilizado.
3. **DNS Dinámico (DDNS)**:
    - Útil cuando un servidor tiene una **IP dinámica**.
    - **Funcionamiento**:
        - Un software en el servidor informa al servidor DNS de cada cambio de IP.
        - El servidor DNS actualiza los registros y notifica a los secundarios.
    - **Ventajas**:
        - Mantiene los registros DNS actualizados en tiempo real.

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 se convierte en 1.2.0.192.in-addr.arpa

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

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