

Blueprint Arquitectónico del Servicio DNS

Funcionamiento, Contenerización y Sincronización Dinámica

ESTRUCTURA DEL CONTENEDOR

IMAGEN: internetsystemsconsortium/bind9

PUERTOS: 53/tcp, 53/udp

VOLUMEN_CONFIG: /etc/bind/

VOLUMEN_ZONAS: /var/lib/bind/



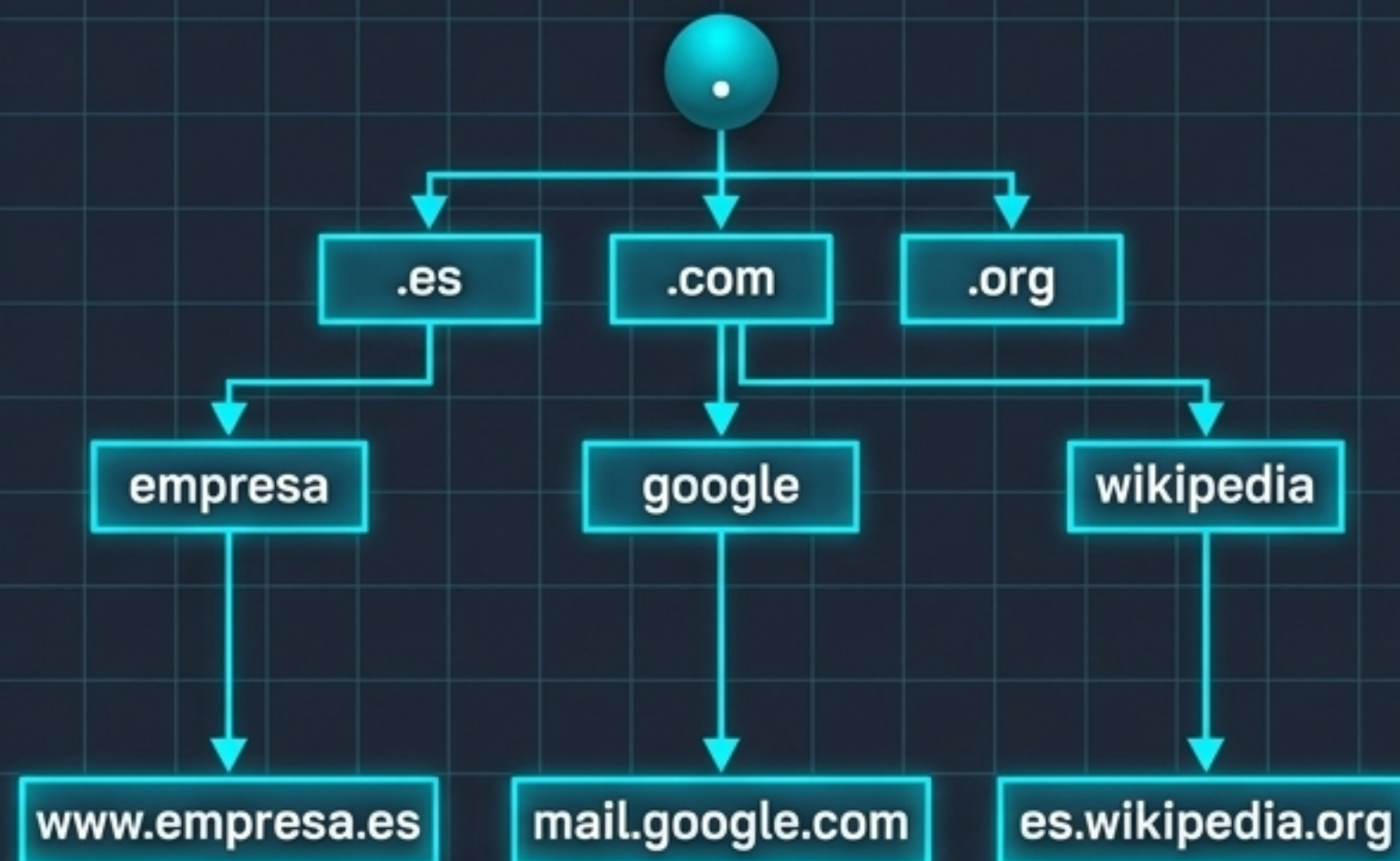
SINCRONIZACIÓN & FLUJO			
TIPO SERVIDOR	ROL	COLOR	ESTADO
PRIMARIO	MASTER	CIAN	ACTIVO (AUTORIDAD)
SECUNDARIO	SLAVE	NARANJA	SINCRONIZADO (REDUNDANCIA)

Sistemas Planos (Ej. NetBIOS/WINS)



- No utilizan jerarquía.
- Imposibles de escalar globalmente porque los nombres colisionan.
- Gestión totalmente centralizada.

Sistemas Jerárquicos (DNS)



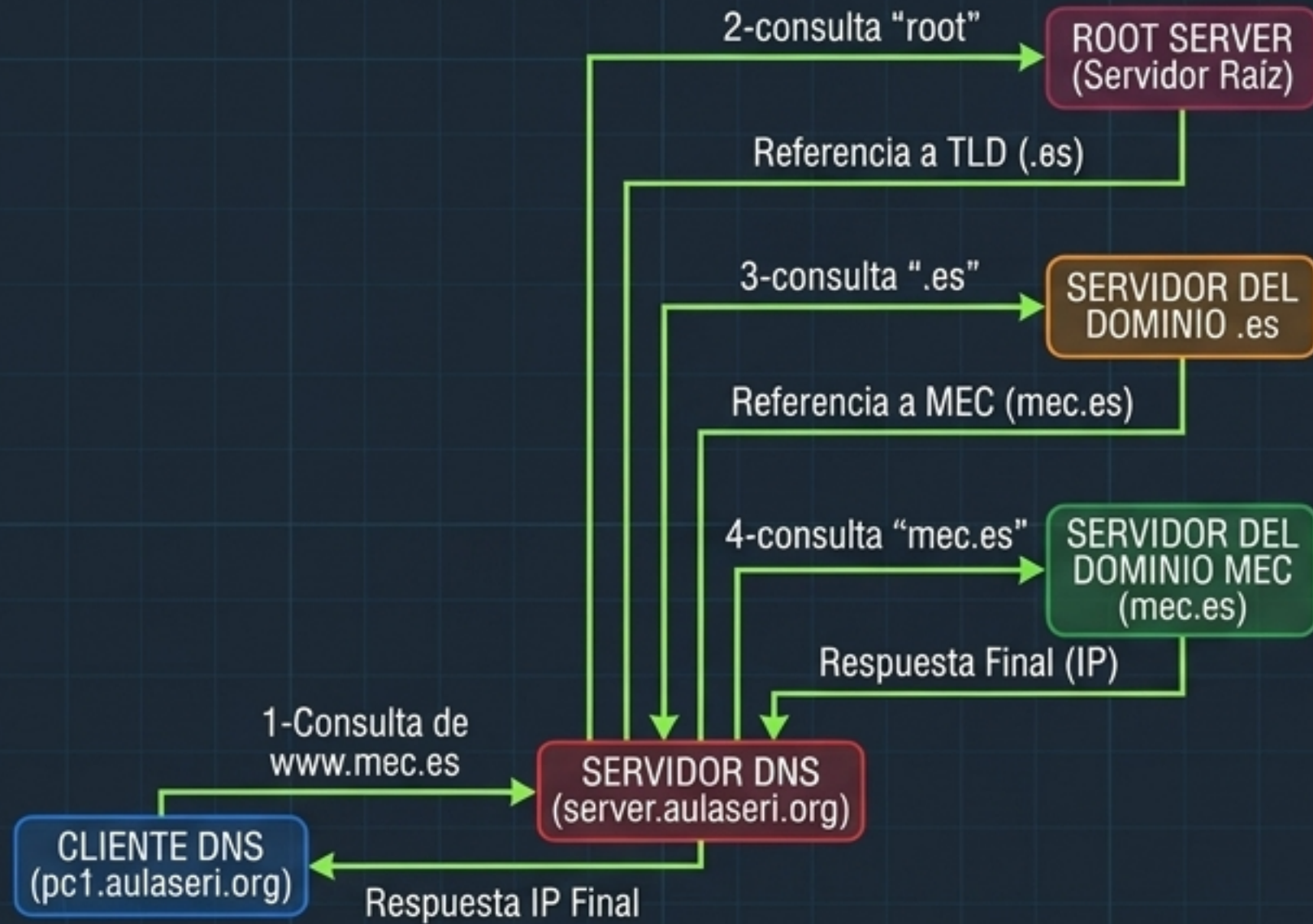
- Árbol distribuido de dominios.
- Permite nombres idénticos (ej. www) en diferentes organizaciones sin colisión.

Reglas del FQDN (Fully Qualified Domain Name)

Máximo 63 caracteres por nivel, 255 caracteres en total.
Siempre termina en un punto (.) que representa la raíz del árbol.

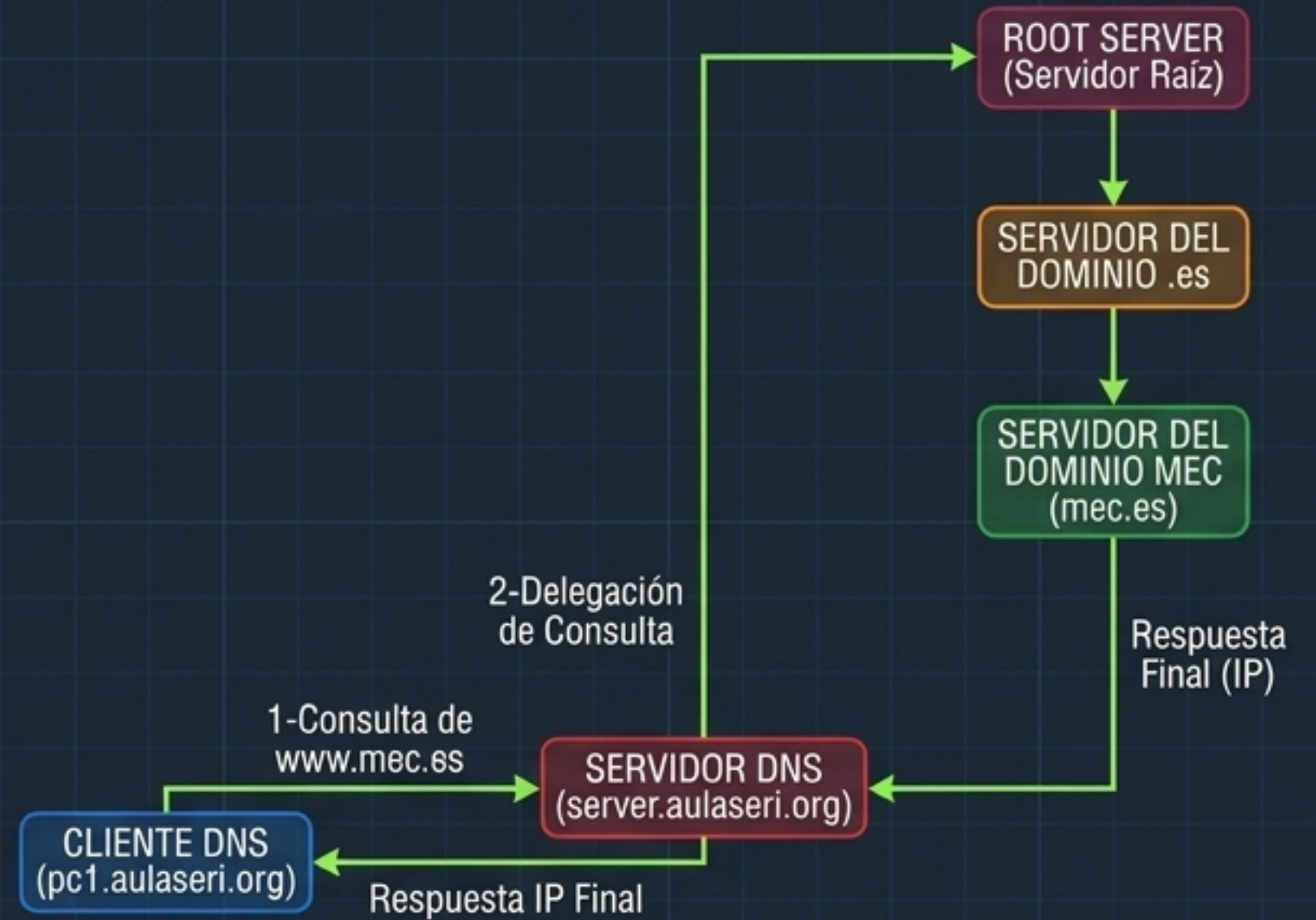
→ nombreEquipo.subdominio.dominio.tld.

RESOLUCIÓN ITERATIVA



El servidor local asume el trabajo de recorrer la jerarquía. Recibe "referencias" (referrals) de otros servidores y lanza nuevas consultas secuenciales.

RESOLUCIÓN RECURSIVA

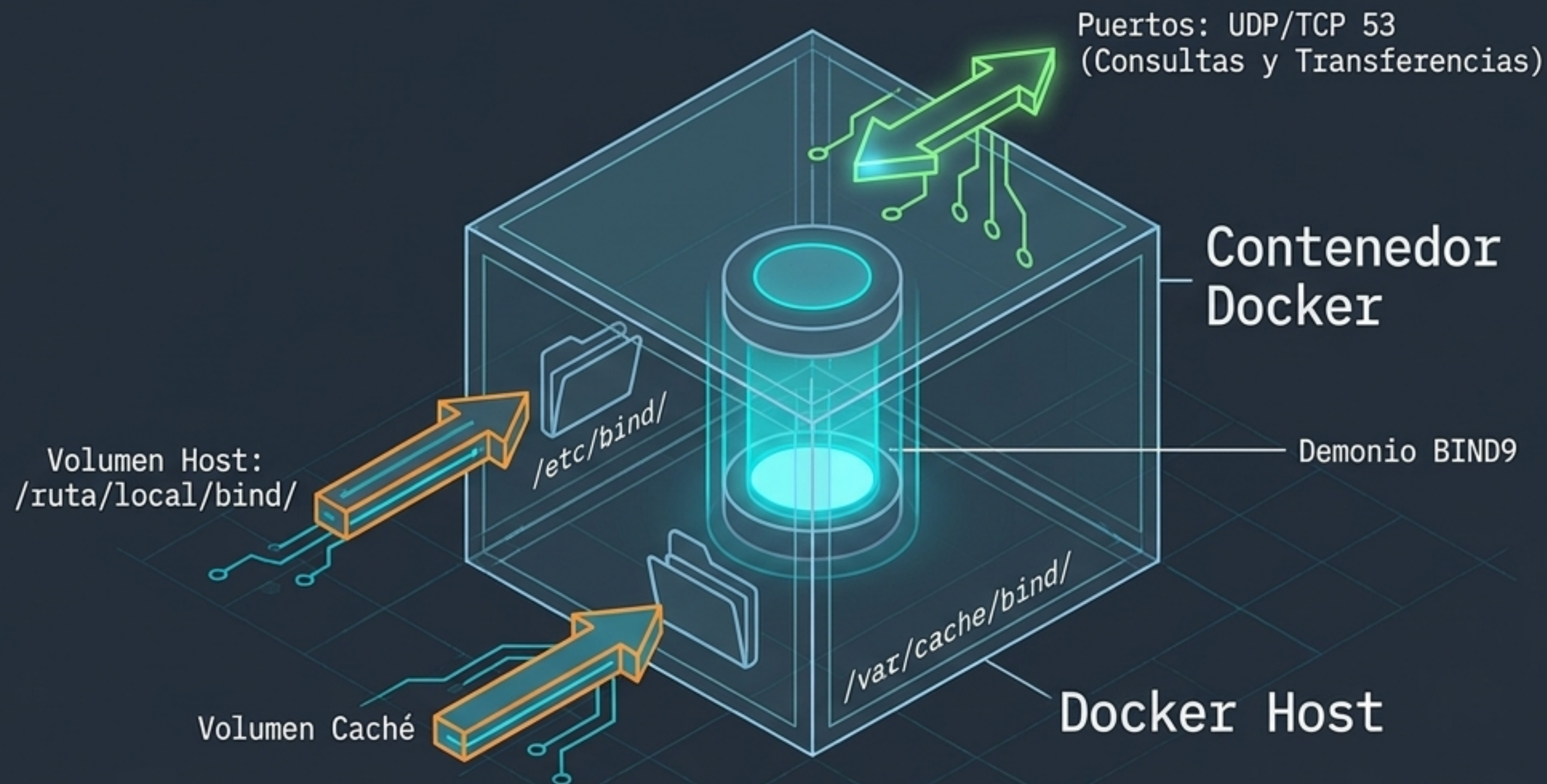


El cliente delega toda la carga. El servidor DNS resuelve la cadena jerárquica completa en segundo plano antes de devolver la IP final.

Matriz de Roles del Servidor DNS



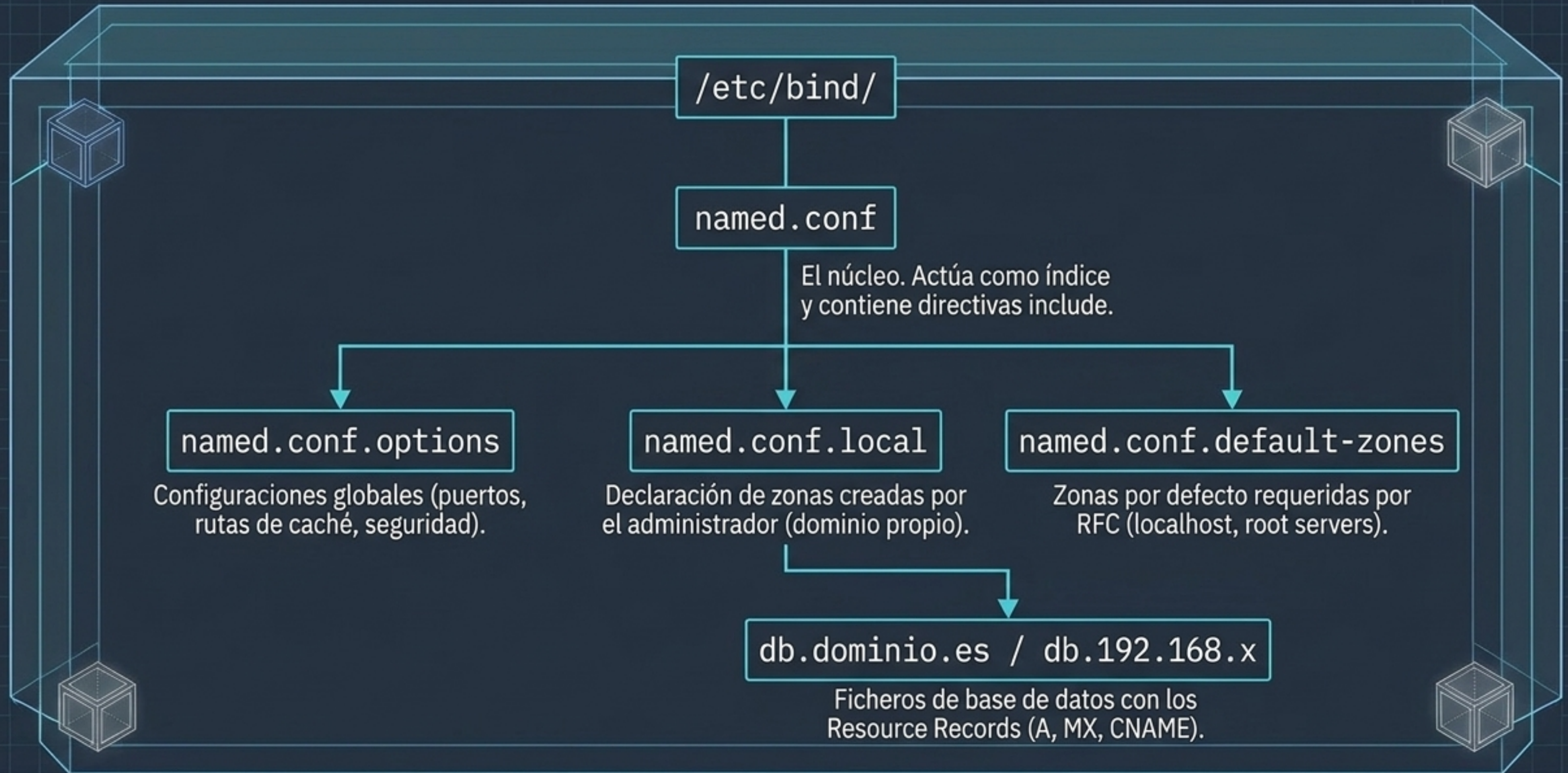
	Maestro (Primario)	Esclavo (Secundario)	Caché	Reenviador (Forwarder)
¿Tiene autoridad?	Sí	Sí	No	No
Origen de Datos	Fichero local (.db)	Transferencia de zona del Maestro	Consultas recientes en RAM	Otro servidor DNS
Capacidad de Edición	Lectura y Escritura	Solo Lectura	No aplicable	No aplicable
Función Principal	Origen de la verdad absoluta	Redundancia y balanceo de carga	Reducir latencia en la red local	Minimizar tráfico externo



Paradigma Contenerizado

El servicio DNS se aísla de la red del host. Toda la configuración persistente se inyecta mediante volúmenes de Docker, separando la lógica de la aplicación (el motor BIND9) de la infraestructura.

Estructura de Archivos de Configuración BIND9



Deep Dive: Configuración del Servidor Primario (named.conf.local)



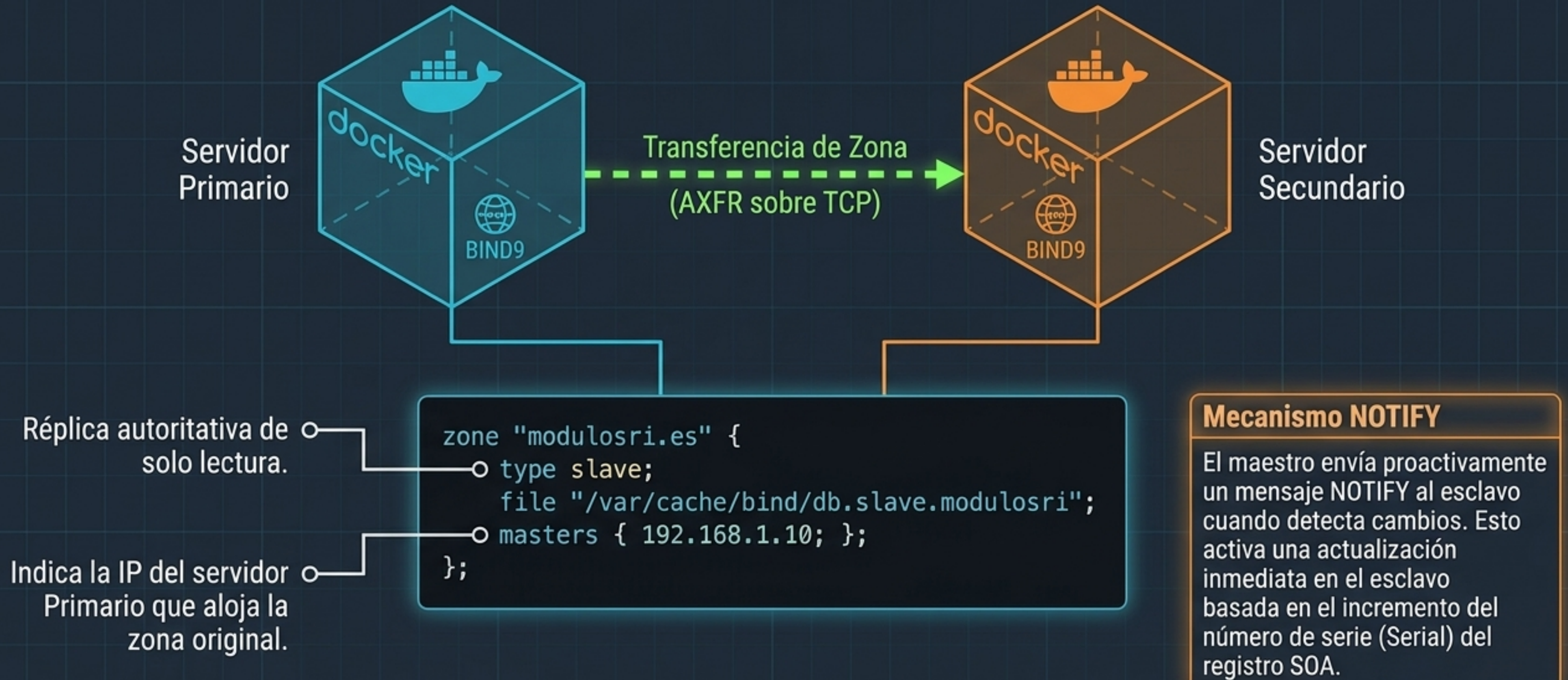
```
zone "modulosri.es" {  
    type master;  
    file "/etc/bind/db.modulosri.es";  
    allow-transfer { 192.168.1.15; };  
};
```

Define la autoridad absoluta de lectura y escritura sobre la zona.

Ruta absoluta dentro del contenedor donde reside la base de datos de la zona.

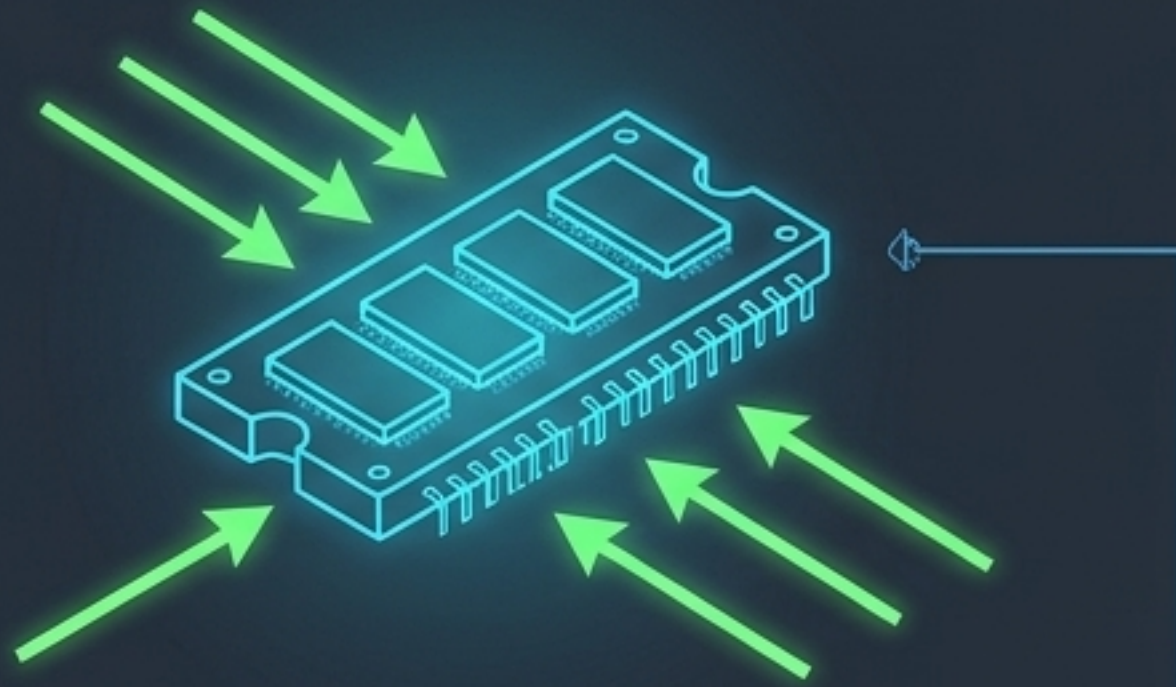
Seguridad de red. Solo permite que las IPs de los servidores Secundarios extraigan una copia completa de la zona.

Deep Dive: Configuración del Servidor Secundario y Transferencia de Zona



Deep Dive: DNS Solo Caché vs. Forwarder

Servidor Solo Caché



Resuelve consultas recursivas en nombre del cliente y guarda los resultados directamente en RAM hasta que expira el TTL (Time To Live). No tiene zonas propias definidas.

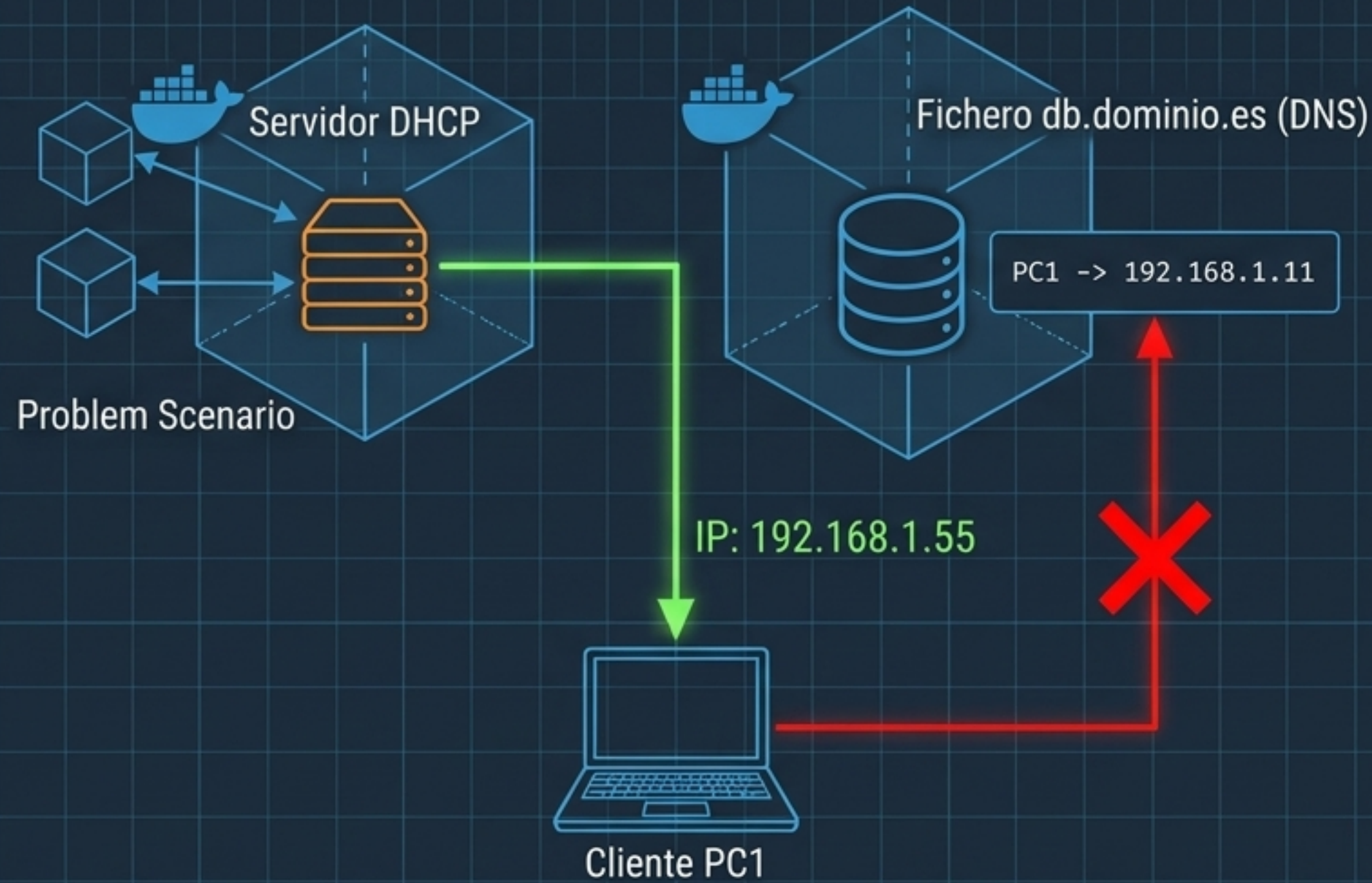
```
recursion yes;
```

Servidor de Reenvío (Forwarder)



Minimiza el tráfico local. Actúa como proxy delegando absolutamente todas las consultas no locales a un servidor externo más potente (ej. ISP o Google).

```
forwarders { 8.8.8.8; 8.8.4.4; };  
forward only;
```

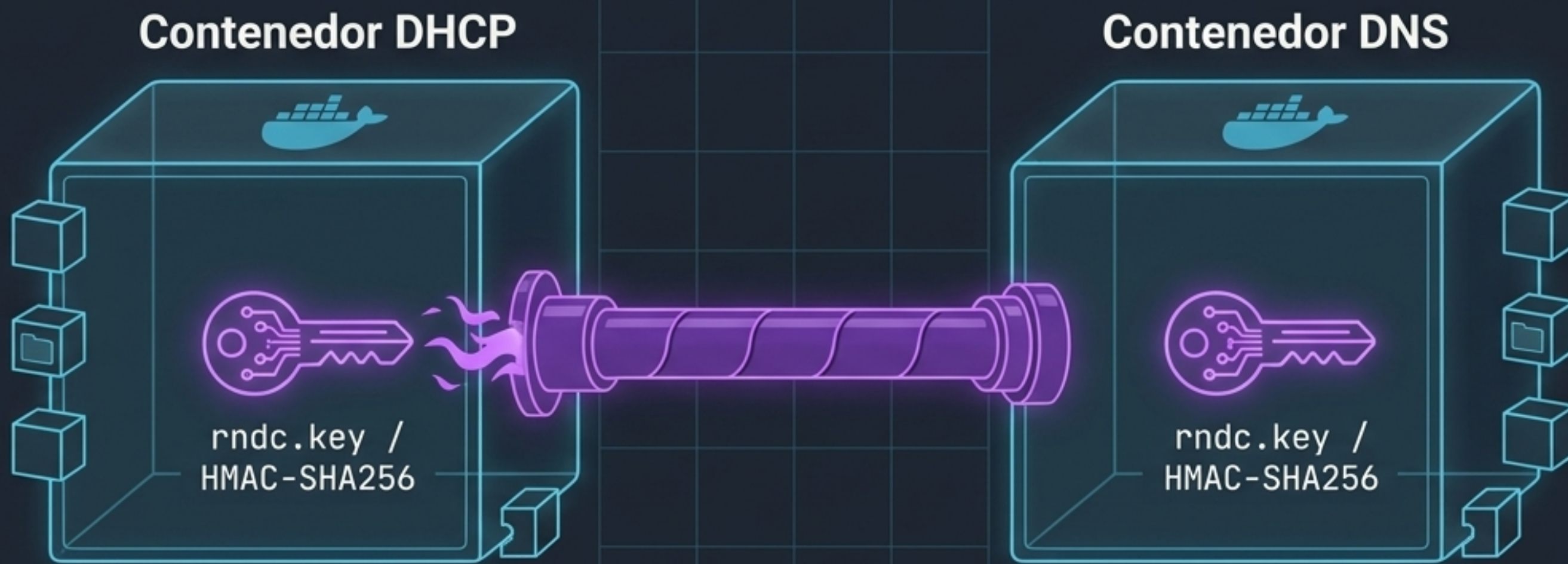


La Fricción Estática

En redes locales modernas, el protocolo DHCP cambia las direcciones IP constantemente según las concesiones (leases). Un fichero DNS estático y manual queda obsoleto casi de inmediato, imposibilitando la resolución por nombre de los equipos locales.

¿Cómo permitimos que el servidor DHCP edite automáticamente el archivo de zona del contenedor DNS sin comprometer la seguridad?

Solución: DNS Dinámico (DDNS) y TSIG



DNS Dinámico (DDNS) y TSIG

La solución es habilitar un canal de actualización en tiempo real. El algoritmo TSIG (Transaction Signature) utiliza una clave criptográfica compartida entre ambos servicios. Solo los demonios que posean y validen esta llave exacta están autorizados para inyectar y modificar dinámicamente los registros de zona.

DNS (named.conf.local)

```
include "/etc/bind/ddns.key";  
  
zone "dominio.es" {  
    type master;  
    allow-update { key "DDNS_UPDATE"; };  
};
```

DHCP (dhcpcd.conf)

```
include "/etc/bind/ddns.key";  
  
ddns-update-style interim;  
ddns-domainname "dominio.es";
```



Nota Operativa: Al conceder una IP, el demonio DHCP se comunica automáticamente con BIND9. BIND9 registra los cambios en vivo escribiendo archivos binarios temporales con extensión .jnl (Journal) junto a la base de datos principal.

Validación de Configuración y Consultas DNS



Paso 1: Validación Sintáctica (Pre-Ejecución)

`named-checkconf`

Verifica la estructura y sintaxis de named.conf.

`named-checkzone dominio.es db.dominio.es`

Verifica la integridad de los Resource Records y el serial.



Paso 2: Herramientas de Consulta (Cliente)

`dig www.dominio.es`

Análisis detallado de cabeceras, tiempos y troubleshooting profundo.

`nslookup`

Herramienta clásica, interactiva y multiplataforma.

`host`

Comando ágil para el mapeo rápido y directo de nombre a IP.

Importante: Reiniciar siempre el contenedor tras validar cambios en ficheros estáticos.

`docker restart dns_bind9`