Módulo: DESPLIEGUE DE APLICACIONES WEB

UT1
El Servicio de DNS

INTRODUCCION

En una red TCP/IP, las máquinas se identifican mediante su dirección de red o número IP. Para las personas resulta más sencillo recordar un nombre que se asocia a una máquina concreta.

También es más fiable, ya que la dirección IP puede cambiar, pero no así el nombre.

Es necesario un **mecanismo que traduzca los nombres de las máquinas a direcciones IP**. El servicio DNS permite que esta tarea se lleve a cabo.

Antiguamente se utilizaba un fichero local donde se almacenaban dichas traducciones. Este archivo consta de IP y nombre de dominio. En Linux se corresponde con /etc/hosts y en Windows con C:\Windows\System32\drivers\etc\hosts. Evidentemente la utilización de este sistema no es viable en la actualidad. De ahí que apareciera una servicio que se gestione de forma distribuida (en millones de servidores DNS) y jerárquica, que es el actual servicio de DNS.

El DNS se utiliza para distintos propósitos. Los más comunes son:

- **Resolución de nombres**: Dado el nombre completo de un host (por ejemplo blog.smaldone.com.ar), obtener su dirección IP (en este caso, 208.97.175.41).
- **Resolución inversa de direcciones**: Es el mecanismo inverso al anterior. Consiste en, dada una dirección IP, obtener el nombre asociado a la misma.
- **Resolución de servidores de correo**: Dado un nombre de dominio (por ejemplo gmail.com) obtener el servidor a través del cual debe realizarse la entrega del correo electrónico (en este caso, gmail-smtp-in.l.google.com).

Por tratarse de un sistema muy flexible, es utilizado también para muchas otras funciones, tales como la obtención de claves públicas de cifrado asimétrico y la validación de envío de e-mails.

ESPACIO DE NOMBRES DE DOMINIO

Cualquier dispositivo en la red debe de tener una IP para poder acceder al mismo. Si queremos que dicho dispositivo se pueda acceder mediante un nombre (nombre de dominio) necesita disponer de dos cosas:

- nombre de dispositivo o hostname. Por ejemplo: www, aulavirtual, gestion, etc.
- sufijo dns: Por ejemplo: jacuela.com, iescuravalera.es, abc.es

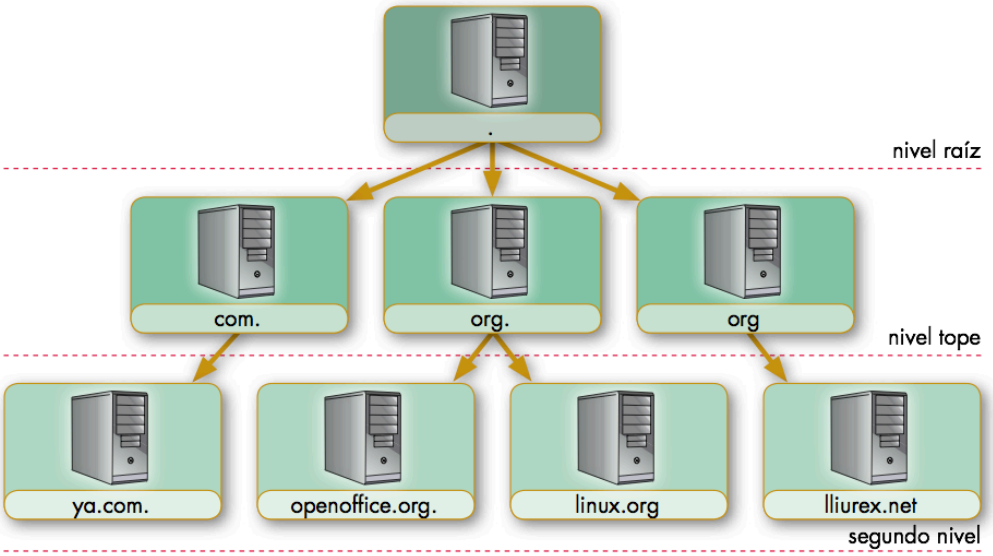
A la suma de nombre de dispositivo y sufijo dns se le llama FQDN (Fully Qualified Domain Name). Este FQDN debe terminar en un punto, <<.>>, para indicar que ahí acaba el nombre completo. También se le conoce como **dirección web** o URL, aunque este último término es más amplio.

Ejemplos:

www.jacuela.es.
aulavirtual.iescuravalera.es.
www.abc.es.

Como vemos, estos nombres completos siguen una estructura jerarquizada, compuesta por un árbol invertido, donde el nodo raíz situado en el nivel superior (nivel 0) es el punto <<.>>. Por debajo, puede existir un número indeterminado de nodos. Normalmente se utilizan hasta cinco niveles. En cada grupo debe haber un máximo de 63 caracteres y el nombre completo o FQDN no debe exceder de los 255 caracteres.

nodo5nivel.nodo4nivel.nodo3nivel.nodo2nivel.nodo1nivel.



Nivel1

El nivel superior o nivel1 se le conoce como TLD (top level domain) y está formado por los dominios que descienden directamente del dominio raíz. El organismo internacional IANA es quien gestiona los TLD y decide los que hay. A su vez, IANA puede delegar ciertos TLDs a otras entidades. Por ejemplo, en España, el dominio .es lo gestiona la empresa pública NIC.ES

Hay TLDs relacionados con paises: .es .co.uk .fr .eu .de
Hay TLDs genéricos que han estado desde el principio: .com .edu .net .org .gov
Hay otros TLDs de nueva aparición: .travel .xxx

- Si queremos que un equipo sea accesibles desde Internet, es decir, que sean públicos, deben de usar un TLD de la IANA y **gestionado por un servidor DNS público**.

- En el ámbito de una red privada, yo puedo escoger el TLD que quiera (.local, .localdomain, .institutodelmal,~~.es~~) y llegar a tener equipos del tipo:

  pc1.local. impresora.localdomain. despliegue.local.

Nivel 2

El nivel2 del árbol de dominio es el formado por los dominios de segundo nivel. Estos dominios son elegidos por el usuario, siempre y cuando estén libres y **si queremos que sean públicos, debemos de pagar por ellos**. Hay muchas empresas que nos permiten la compra de dominios de segundo nivel. Basta con introducir el dominio que queramos y

nos dirán si esta disponible o no, incluso nos ofrecerán alternativas. Algunas empresas (agentes registradores) ofrecen dominios de segundo nivel gratuitos por un tiempo.

Algunas empresas son: Arsys (española y de calidad), Godaddy, Hostinguer, Hostalia, etc.

Normalmente, además de comprar un nombre de dominio, también reservamos un espacio de alojamiento, siempre y cuando queramos tener alojada nuestro proyecto web en un servidor externo (hosting). Estos agentes registradores suelen ofrecer "pack" con ambas cosas, nombre de dominio + alojamiento (hosting).

No es obligatorio que ambas cosas estén en el mismos agente. Yo puedo reservar el nombre de dominio con un agente y el hosting con otro agente distinto.

Nivel3

El nivel3 y superiores son gratuitos y los escoge el dueño o propietario del dominio de segundo nivel al que pertenezcan.

A este tercer nivel tengo dos opciones:

- Crear un nombre de máquina para acceder a la web.

  www.jacuela.com miweb.jacuela.com daw.iesramonarcas.es

- Crear un subdominio. Esto es útil para montar otra web independiente a la web principal. Por ejemplo, crear un blog.

  blog.jacuela.com

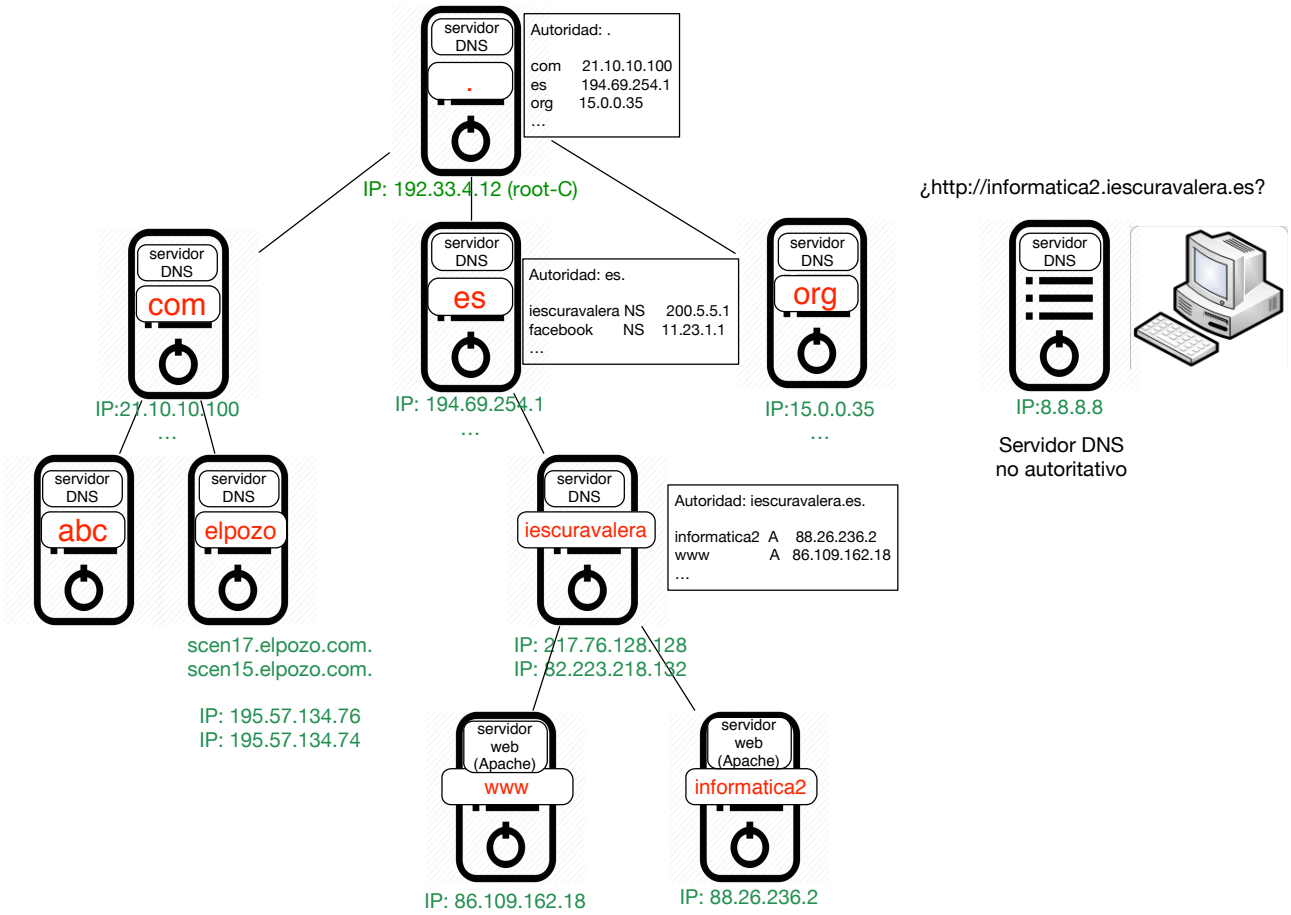
El usuario no sabe si una dirección web (blog.jacuela.com) es un subdominio o un nombre de máquina, pero da igual. Son tareas del administrador del dominio.

ARQUITECTURA DEL SERVICIO DE DNS

De cara al usuario, el DNS es una máquina con su correspondiente IP a la que se le lanzan consultas. Podemos usar el DNS que queramos, siempre que esté preparado para ello. Los ISP's suelen tener sus propios servidores DNS. Google puso hace años dos servidores DNS público para que la gente los usara. Son el 8.8.8.8 y el 8.8.4.4. Ultimamente esta en boca o nuevo, el 1.1.1.1, del que dicen que es más seguro y con mayor privacidad para el usuario.

https://1.1.1.1/es-ES/dns/

En realidad, es servicio de DNS es una base de datos pública, jerarquizada y distribuida.



Podemos encontrarnos los siguientes elementos:

- **Espacio de nombres de dominio (*domain name espace*)**. Conjunto de nombres que se pueden utilizar para identificar máquinas o servicios de una red.
- **Zona**: una zona es cualquier nodo (menos el nodo hoja) del espacio de nombres de dominio. Existen la zona <<.es.>>, la zona <<.com.>>, la zona <<iescuravalera.es.>>
- **Registro de Recursos (Resource Records RR)**. Base de datos o tabla de una zona, dónde se almacena información de esa zona.
- **Servidor DNS autorizado** (Name Server NS). Es una máquina que gestiona una zona concreta y responde a preguntas de dicha zona. Dicha máquina tiene una IP y un nombre. Podemos hablar de "el NS que gestiona la zona .es", o podemos hablar de "el NS que gestiona la zona iescuravalera.es", o podemos hablar de "el NS que gestiona la zona punto <<.>>".
- **Servidor DNS no autorizado**. Es una máquina que no gestiona ninguna zona concreta, pero a la que se le puede preguntar para que nos resuelva una consulta. Ejemplos serian los DNS de Google 8.8.8.8 y 8.8.4.4
- **Clientes DNS (*resolvers*).** Programas que realizan preguntas a los servidores de nombres y procesan las respuestas para ofrecer la información a los usuarios o a las aplicaciones

Al conjunto de todos los RR de todas las zonas es lo que conocemos como Base de datos DNS y al conjunto de todos los Servidores DNS que gestionan las zonas es lo que llamamos de forma genérica el Servicio de DNS.

Los servidores que gestionan la zona punto <<.>> son los denominados root-servers. Hay un total de 13 root servers, cada uno con su IP. Además, cada servidores tiene réplicas. En total, hay cientos de root servers. Esto es así porque al ser la raíz del árbol, si cayeran, el servicio de DNS dejaría de funcionar y se paralizaría Internet.

http://www.root-servers.org

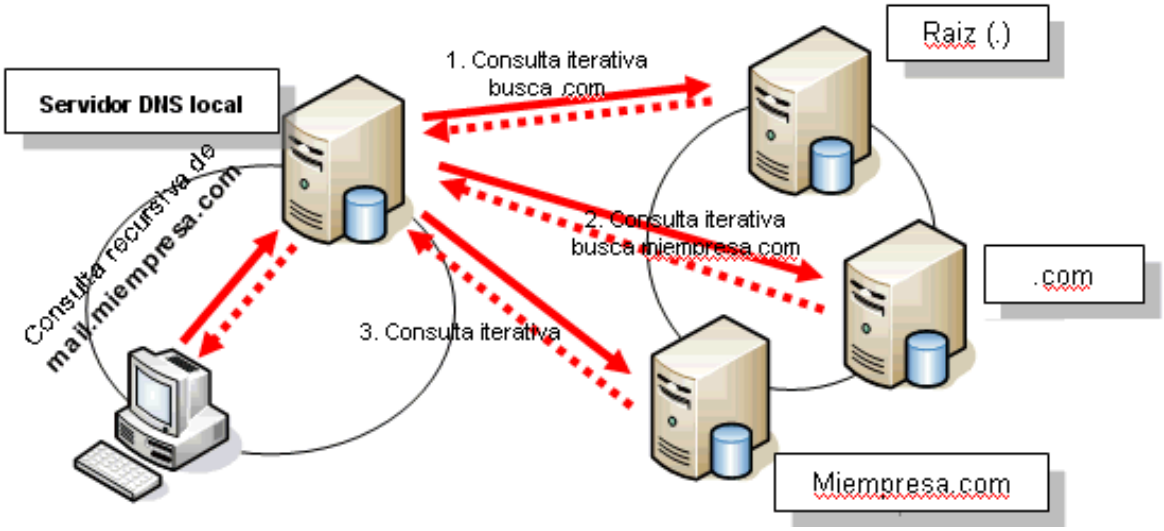
Cada nodo del árbol (a excepción de los nodos hoja) tiene su servidor DNS y este almacena una tabla (archivo de zona) con los registros de recursos <<RR>> de dicha zona. Los registro de recursos son de varios tipos:

- A (Address): registro de máquina o host
- NS (Name Server): registro de ServidorDNS de una zona
- CNAME (Canonical Name): registro de alias (nombre alternativo a un host)
- MX (Mail Exchange): registro de servidor de correo
- SOA: registro principal con las especificaciones de la zona
- PTR (Pointer): registro de puntero inverso. Usado para la resolución inversa
- TXT (Text): permite asociar información adicional a un dominio. Esto se utiliza para otros fines, como el almacenamiento de claves de cifrado.

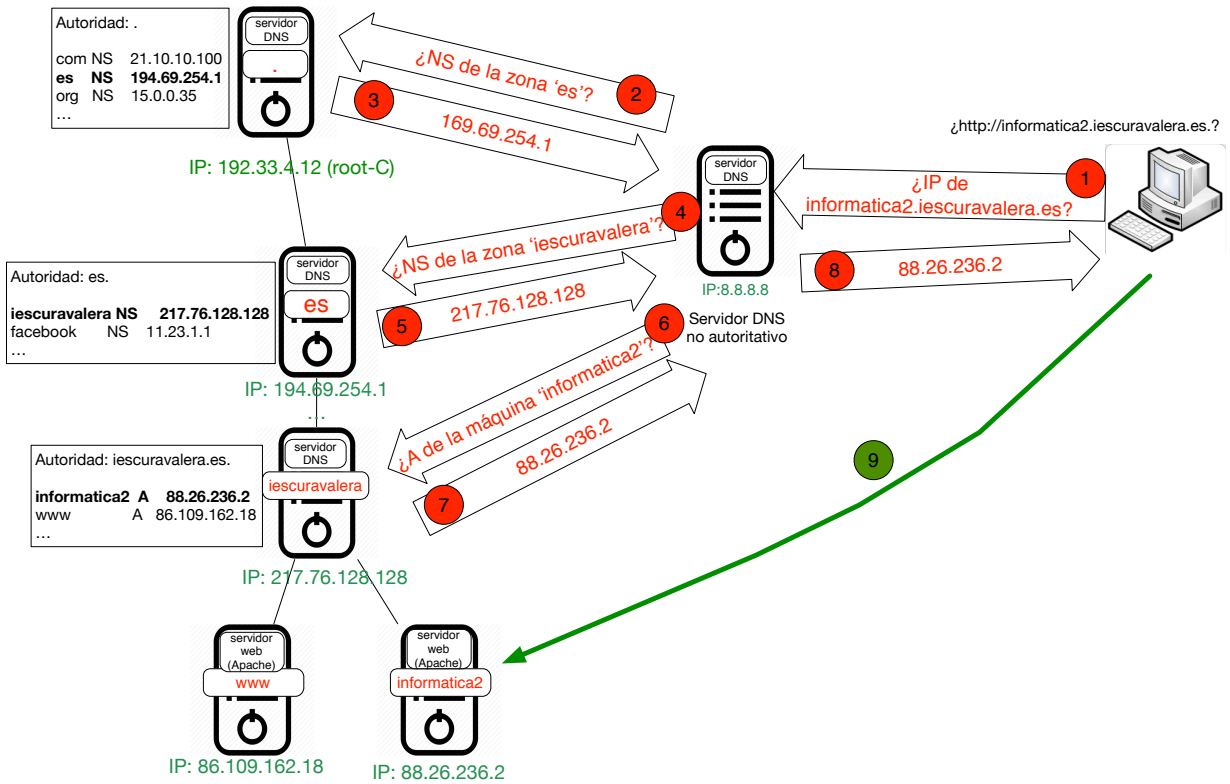
EL PROCESO DE RESOLUCIÓN DE NOMBRES

Cuando una aplicación (cliente) necesita resolver un FQDN, el cliente de DNS (*resolver*) de nuestro ordenador hace una consulta al servidor DNS que tengamos configurado. Si el servidor DNS conoce el dato, lo proporcionará. En caso contrario, se desencadena el proceso de resolución del nombres:

1. El servidor de nombres inicial consulta a uno de los servidores raíz (cuya dirección IP debe conocer previamente).
2. Este devuelve el nombre del servidor a quien se le ha delegado la sub-zona.
3. El servidor inicial interroga al nuevo servidor.
4. El proceso se repite nuevamente a partir del punto 2 si es que se trata de una sub-zona delegada.
5. Al obtener el nombre del servidor con autoridad sobre la zona en cuestión, el servidor inicial lo interroga.
6. El servidor resuelve el nombre correspondiente, si este existe.
7. El servidor inicial informa al cliente el nombre resuelto.



Ejemplo de resolución de la IP <<informatica2.iescuravalera.es>>



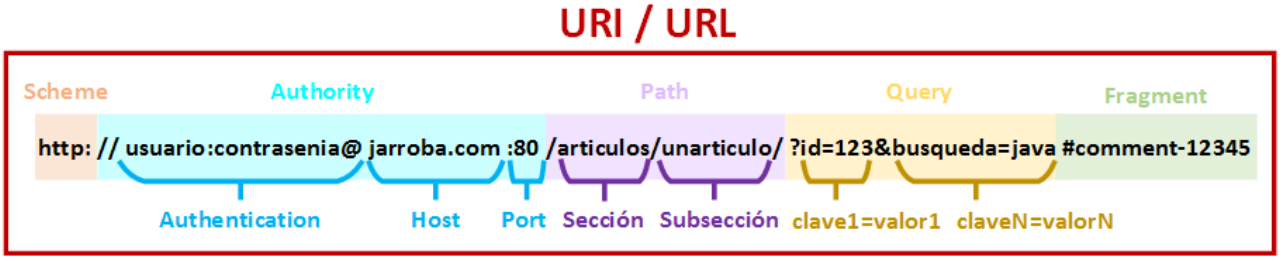
URL o Uniform Resource Locator

Cualquier recurso al que se pueda acceder tiene asociado un localizador. Normalmente asociamos la URL a la dirección de una página web, pero el concepto de URL es más general.

La URL puede ser una cadena de acceso para:

- acceder a una página web no segura –> http://www.gogle.com
- conectarse por FTP a un servidor remoto –> ftp://pedro:1234@jacuela.com:21
- acceder a una página de una subcarpeta –> http://www.jacuela.com/gestion/
- acceder a un servidor mediante el protocolo SAMBA –> smb://192.168.8.104
- acceder a un archivo local –> file:///C:/carpeta/archivo.exe

La URL esta formada por varias partes, de las cuales, no todas son obligatorias de incluir dependiendo del recurso y el protocolo de acceso.



Las partes de una URL son:

- scheme: es el protocolo o esquema de acceso al recurso. Existen muchos protocolos

  - http: acceso a página web no segura
  - htttps: acceso a página web segura
  - ftp: acceso a servidor ftp para transferir archivos
  - smb: acceso a una carpeta o archivo mediante SAMBA
  - mailto: para enviar un correo electrónico

- authentication: si el recuso requiere credenciales de acceso, se especifican delante del host, de la forma <<usuario:contraseña@>>

- host: es el FQDN del servidor que contiene el recurso. Será traducido en una IP por el DNS

- port: es el puerto de acceso. Si no lo incluimos, se tomará el puerto por defecto del protocolo. Si queremos acceder al recurso por un puerto distinto al por defecto, debemos de indicarlo.
- path: ruta dentro del servidor donde se encuentra el recurso
- query / fragment: opciones para acceder al recurso.

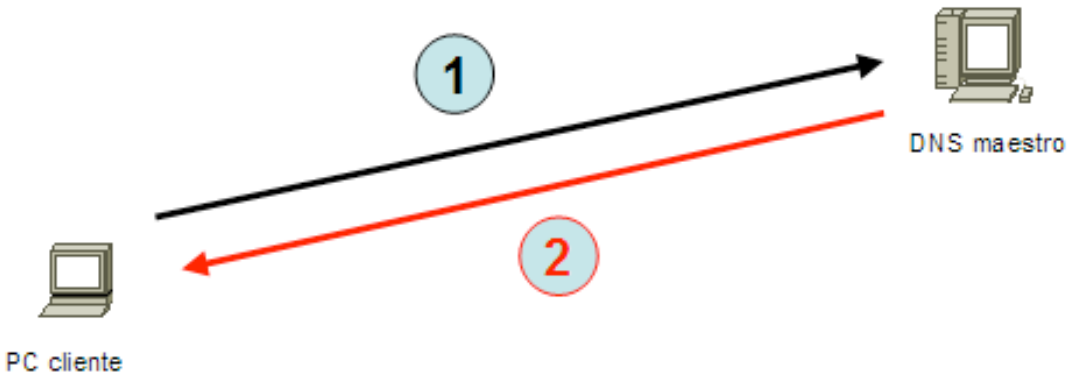
TIPOS DE SERVIDOR DNS

El servidor DNS normalmente admite tres modos de funcionamiento

- Servidor DNS maestro
- Servidor DNS esclavo
- Servidor caché DNS

Servidor DNS maestro

En este modo de funcionamiento, nuestro servidor se comporta como un auténtico servidor DNS para nuestra red local. Atenderá directamente a las peticiones de resolución de direcciones pertenecientes a la red local y reenviará a servidores DNS externos las peticiones del resto de direcciones de Internet.

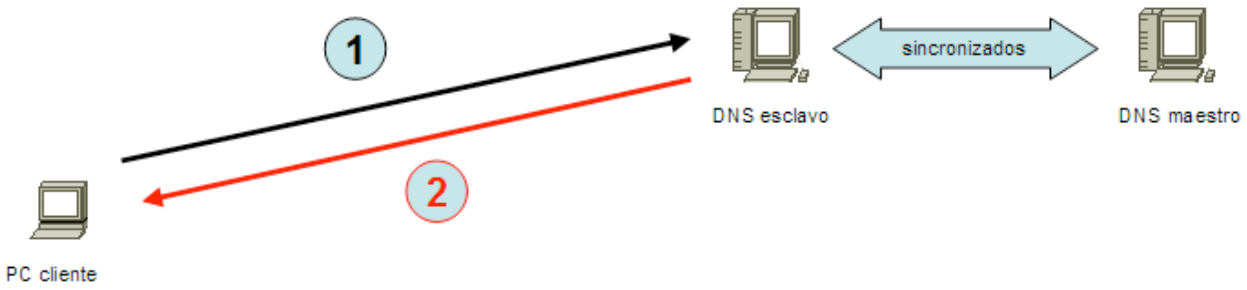


1 – Consulta DNS: ¿Cuál es la IP de aula5pc7.ieslapaloma.com?

2 – Respuesta DNS: La IP de aula5pc7.ieslapaloma.com es 192.168.0.107

Servidor DNS esclavo

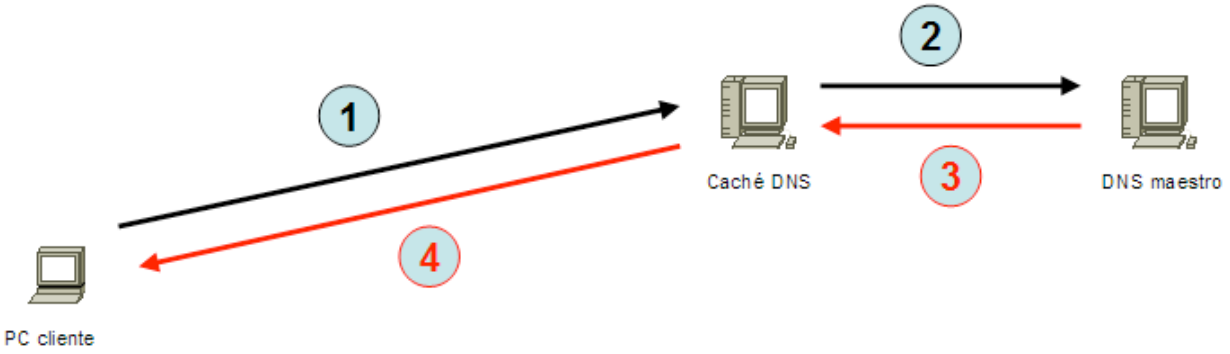
Un servidor esclavo actuará como un servidor espejo de un servidor DNS maestro. Permanecerá sincronizado con el maestro. Se utilizan para repartir las peticiones entre varios servidores aunque las modificaciones solo se realicen en el maestro o en el caso de que no se pueda acceder al maestro. En redes locales salvo por razones de disponibilidad, es raro que exista la necesidad de tener dos servidores DNS ya que con uno será suficiente.



Servidor caché DNS

En este modo de funcionamiento, nuestro servidor se comporta como si fuera un auténtico servidor DNS para nuestra red local aunque realmente no sea un servidor DNS propiamente dicho. Cuando recibe una petición de DNS por parte de un cliente de nuestra red, la trasladará a un DNS maestro que puede estar en nuestra red o fuera, almacenará en una memoria caché la respuesta y a la vez la comunicará a quien hizo la petición. Si un segundo cliente vuelve a realizar la misma petición, como nuestro servidor tiene la respuesta almacenada en su memoria caché, responderá inmediatamente sin tener que cursar la petición a ningún servidor DNS de Internet.

Disponer de un servidor caché DNS en nuestra red local aumenta la velocidad de la conexión a Internet pues cuando navegamos por diferentes lugares, continuamente se están realizando peticiones DNS. Si nuestro caché DNS almacena la gran mayoría de peticiones que se realizan desde la red local, las respuestas de los clientes se satisfarán prácticamente de forma instantánea proporcionando al usuario una sensación de velocidad en la conexión.



Consulta a un cache DNS. En caso de fallo, se redirecciona hacia un DNS maestro

USO DEL DNS PRIVADO EN UNA RED LOCAL

Para algunas redes de área local donde haya muchos equipos y cuente con servidores de acceso frecuente, puede ser interesante instalar un DNS local. Este se encargará de hacer las traducciones de las máquinas de mi LAN y no será público, es decir solo tienen sentido dentro de mi red local.

Básicamente, es conveniente montar un servidor local de DNS por los siguientes motivos:

- Uso como DNS cache, para agilizar el acceso a Internet: Al tener un servidor de nombres en nuestra propia red local (que acceda al DNS de nuestro proveedor o directamente a los root servers) se agiliza el mecanismo de resolución de nombres, manteniendo en caché los nombres recientemente usados en la red y disminuyendo el tráfico hacia/desde Internet.

- Simplificar la administración de la red local: Al contar con un DNS propio (ya sea uno o varios servidores de nombres) es posible definir zonas locales (no válidas ni accesibles desde Internet) para asignar nombres a cada uno de los hosts de la LAN. De esta forma es posible, por ejemplo, referirnos a la impresora de red como “hplaser.mired.local” en vez de “192.168.0.2” y a nuestro servidor de correo interno como “smtp.mired.local” en vez de “192.168.0.3“. (Pensemos, por ejemplo, que ocurriría con las configuraciones de las aplicaciones si un día decidimos cambiar el esquema de direcciones IP de nuestra red.)