TEMA 3: Servicio de nombres de dominio

3.1-Necesidad

Cada máquina conectada a Internet se identifica con un número único que está compuesto de 32 dígitos binarios, conocido como **dirección IP**.

DNS (Domain Name Server, Servidor de nombres de dominio). A través del servicio DNS podremos preguntar por un nombre de dominio y se nos devolverá la dirección IP correspondiente. También se puede hacer la tarea contraria: preguntar por una dirección IP y obtener el dominio correspondiente.

3.2-Espacio de nombres de dominio

Espacio de nombres de dominio. Sistema de nombres jerárquico que organiza los nombres en forma de árbol invertido (raíz arriba y abre las ramas hacia abajo) y permite controlar que no se repiten nunca dos nombres iguales. **Está organizado como una raíz sin etiqueta, seguida de los dominios genéricos de primer nivel y de los nombres que eligen las organizaciones conectadas a la red.** Cada dominio puede subdividirse en otros dominios, hasta llegar al final de la estructura que son los nombres de los ordenadores.

3.3-Clasificación de dominios

El control de las direcciones y dominios de Internet lo gestiona la **ICANN** (Internet Corporation for Asigned Names and Numbers, Corporación de Internet para la Asignación de Nombres y Números).

Dominios de primer nivel. Son los que cuelgan directamente de la raíz y los clasificamos según su uso en:

- Los genéricos fueron los primeros en existir (com para empresas, org para organizaciones sin ánimo de lucro, int para organizaciones internacionales, edu para organizaciones educativas….
    - Los no patrocinados (com, org, net,...) funcionan según las reglas globales de la ICANN
    - Los dominios patrocinados (gov, edu, mil,...) que son gestionados por entidades concretas, aunque son creados previamente por la ICANN
- Los geográficos son dominios de dos letras que hacen referencia generalmente a países (es, it, de, us, etc.) aunque no siempre (eu, Unión Europea). Son creados por el ICANN y las tareas de gestión de estos dominios están delegadas en los correspondientes gobiernos que generalmente cuentan con entidades que se encargan de ello.
- El dominio arpa es un dominio de primer nivel que se usa exclusivamente para la tarea de los DNS de traducir direcciones IP con dominios
- Los dominios reservados son dominios de primer nivel que no existen y queda asegurado que nunca existirán. Son **test, example, localhost e invalid** que se

utilizan para hacer pruebas y prácticas de manera que no interfieran en el servicio DNS real.

Dominios de segundo nivel. Están disponibles para cualquier persona o entidad que los quiera comprar, siempre que no estén ya ocupados. De hecho ni siquiera es necesario pertenecer a los grupos que lo definen, así una empresa puede comprar un dominio org y un organización sin ánimo de lucro puede comprar un com. El registro de estos dominios sólo lo puede hacer la empresa que gestione el dominio de primer nivel donde colgará, pero la compra se puede hacer a través de muchos intermediarios que pueden tener precios muy distintos.

3.4-Gestión Administrativa

La ICANN decide los dominios de primer nivel que van a existir, pero no los gestiona directamente, sino que delega esa gestión en una entidad por un periodo de tiempo que, después será renovado o asignado a otra entidad.

En el proceso de registro de un dominio intervienen tres términos que son tan parecidos que pueden crear confusión: **registro, registrador y registrante**.

Whois es una base de datos distribuida que contiene los datos de los dominios. Se puede consultar desde algunas web. En Linux también desde la consola con: **whois dominio**. Se pueden hacer consultas de dominios de cualquier nivel (es, cat, …) y aparecerán los datos del registrante y del registrador.

Una de las tareas que tiene que realizar una entidad cuando se encarga de un dominio es mantener servidores DNS que permitan localizar a todos los equipos de su subárbol.

Zonas DNS y dominios DNS. Un dominio es el conjunto de todos los nodos que se agrupan bajo él, el subárbol completo. La zona es solamente el conjunto de nodos cuyas direcciones se gestionan directamente, es decir, no están delegadas:

  - La **zona raíz:** Sólo conoce las direcciones de los servidores DNS de los dominios de primer nivel.
  - La **zona .es:** Sólo conoce las direcciones de los servidores DNS de sus dominios de segundo nivel, como empresa.es.
  - La **zona .empresa.es:** Sólo conoce las direcciones IP de los equipos de la empresa.
- Cuando una entidad se hace responsable de un dominio gestiona todo el dominio (a veces delegándolo) pero sólo mantiene las direcciones de su zona.

3.5-Funcionamiento DNS

Hay dos tipos de ordenadores en el sistema DNS: los clientes sólo hacen consultas y los servidores responden a las consultas y buscan direcciones IP de servidores desconocidos.

- El cliente DNS hace una consulta al servidor que tenga configurado como servidor DNS. Si este servidor conoce el dato lo suministra.
- Si nuestro servidor DNS no conoce el dato le hará la pregunta al servidor DNS de la zona raíz que lo único que puede suministrar es la dirección del servidor de primer nivel que conoce el dato.

- Nuestro servidor DNS consulta al servidor de primer nivel indicado, que devolverá la dirección del servidor de segundo nivel que conoce el dato
- Nuestro servidor DNS consulta al servidor de segundo nivel indicado, que proporcionará la dirección que buscamos

Consultas iterativas y recursivas

- La consulta iterativa dará resultado inmediato sólo si el servidor consultado tiene la respuesta. Si no es así, sólo informará del siguiente servidor a quien preguntar.
- La consulta recursiva hace trabajar al servidor hasta dar con la respuesta o concluir que hay un error.

No todos los servidores aceptan consultas recursivas, ninguno de la zona raíz las acepta. Es buena idea a la hora de configurar el servidor, no aceptarlas desde fuera de nuestra red local.

Resolución inversa. Cuando lo que queremos es obtener dominios a partir de direcciones IP, hablamos de **resolución inversa**

Almacenamiento de nombres en caché. Cada vez que se realiza una consulta, la respuesta (del servidor autorizado) va acompañada del TTL (Time To Live, tiempo de vida) que es el tiempo durante el cual se considera válida esa respuesta (normalmente 1 o 2 días). El servidor DNS que ha hecho la consulta, guardará el resultado. Si volvemos a preguntar antes de que pase ese tiempo nos dará la misma respuesta sin necesidad de volver a hacer esa consulta.

- Puesto que el servidor DNS de nuestro ISP atiende a muchos clientes, todas las consultas sobre el mismo dominio tienen la respuesta mientras dure el TTL sin necesidad de lanzar la consulta más allá, con lo que el tráfico se reduce considerablemente
- Además, el servidor DNS almacena todos los otros datos intermedios que obtiene para la consulta, todos esos que podemos ver cuando ejecutamos un dig dominio +trace. Por cierto, los números que aparecen junto a cada dato son los TTL en segundos para ese dato.
- Los clientes DNS también pueden tener una caché con la misma finalidad

3.6-Servidores DNS

Los servidores DNS son ordenadores que mantienen en ejecución un programa que permite aceptar consultas DNS. El puerto 53 es el que se usa habitualmente para este servicio. Los servidores DNS de zona deberían estar funcionando permanentemente.

Se dice que la respuesta a una consulta que ha sido resuelta por el servidor de su dominio es una respuesta autoritativa.

Tipos de servidores DNS:

- **Servidores de zona:** Encargados de mantener las direcciones de su zona. Son los que dan respuestas autoritativas para todas las consultas sobre los equipos de su zona.
  - **Servidores de zona primarios: (o maestros)** En cada zona hay un único servidor primario. Guarda los datos originales y es sobre el que actúa directamente el administrador del servicio. Mantiene los datos aunque se reinicie.
  - **Servidores de zona secundarios: (o esclavos)** En cada zona hay uno o varios servidores secundarios. Guardan copia de los datos, obtenida periódicamente del servidor primario. Cuando se reinicia necesita obtener una copia de nuevo.
- **Reenviador:** (forwarders) Es un servidor DNS que recibe todas las peticiones de la red, con objeto de minimizar las consultas al exterior. Todos los demás servidores DNS de la red se configurarán para dirigir las consultas al reenviador.
- **Caché:** Sólo almacena en caché las consultas que hace con objeto de reducir consultas y no sobrecargar los servidores de zona. Por ejemplo, un ISP puede tener un servidor caché para no asignar a sus clientes directamente su servidor de zona.

3.7-Registros del DNS

La información que almacena la base de datos de un servidor DNS se estructura en registros. Cada registro contiene los siguientes datos:

- **Nombre de dominio:** que es la entrada a partir de la que se hace la búsqueda. Por ejemplo, www.iesmurgi.org. Debes recordar que es necesario terminar los dominios en punto (.) para que sean tratados como dominios absolutos.
- **Clase:** En nuestro caso siempre será IN (Internet).
- **Tipo:** El tipo de registro de que se trata, que puede ser A, AAA, CNAME, NS, etc. Hay unos 30 tipos de registro.
- **TTL:** Tiempo de vida (en segundos) que se dará a la información de este registro. Si no aparece el TTL en el registro la información se servirá con el TTL por defecto.
- **Datos:** Es el dato de respuesta que el servidor devuelve.

3.8-DNS Dinámico

El sistema DNS está preparado para direcciones IP estáticas, pero la realidad es que con frecuencia las direcciones son dinámicas y esto puede generar algún problema hasta que se actualizan las bases de datos. Hay dos formas de solucionar este problema: una adecuada para administradores de zona y otra adecuada para usuarios.

DNS dinámico para administradores de zona. Consiste en configurar el cliente DNS de los equipos cuyas IP pueden cambiar para que cuando ocurran esos cambios informen a su servidor de forma automática. Y también habrá que configurar el servidor DNS para que acepte ese mecanismo de actualización.

DNS dinámico para usuarios. Existen empresas que ofrecen el servicio de DNS dinámico (dyndns, no-ip) y normalmente tiene un coste económico. En el equipo que cambiará de IP se instala un software que informa de esos cambios y el proveedor del servicio modificará los datos de zona. No forma parte del DNS estándar pero es muy útil para usuarios sin conocimientos. A veces este servicio se ofrece mediante un dominio de tercer nivel, por ejemplo, midominio.no-ip.org, pero también se puede conseguir el DNS dinámico con nuestro propio dominio.

3.9-Clientes DNS

Cuando contratamos una conexión a Internet con un ISP, éste nos proporciona las direcciones IP de sus servidores DNS, normalmente dos, que debemos configurar como principal y alternativo.

Si en el contrato se incluye un router que gestiona el propio ISP, ese router ya vendrá configurado con los servidores DNS de tu proveedor, de modo que en el cliente de tu ordenador sólo tendrás que ajustarlo para que reciba esos datos de forma automática por DHCP.

Si ya dispones de un router propio serás tú el que tenga que anotar las DNS. Puedes hacerlo en el router para que las proporcione vía DHCP o puedes hacerlo en cada equipo de la red