Sistema de Nombre de Dominio: DNS

Acerca del protocolo DNS (Domain Name System)

DNS (acrónimo de Domain Name System) es una base de datos distribuida y jerárquica, que almacena la información necesaria para los nombres de dominio. Sus usos principales son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico correspondientes para cada dominio. El DNS nació de la necesidad de facilitar a los seres humanos el acceso hacia los servidores disponibles a través de Internet permitiendo hacerlo por un nombre, algo más fácil de recordar que una dirección IP.

Los Servidores DNS utilizan **TCP** y **UDP**, en el puerto **53** para responder las consultas. Casi todas las consultas consisten de una sola solicitud UDP desde un Cliente DNS, seguida por una sola respuesta UDP del servidor. Se realiza una conexión TCP cuando el tamaño de los datos de la respuesta exceden los 512 bytes, tal como ocurre con tareas como transferencia de zonas.

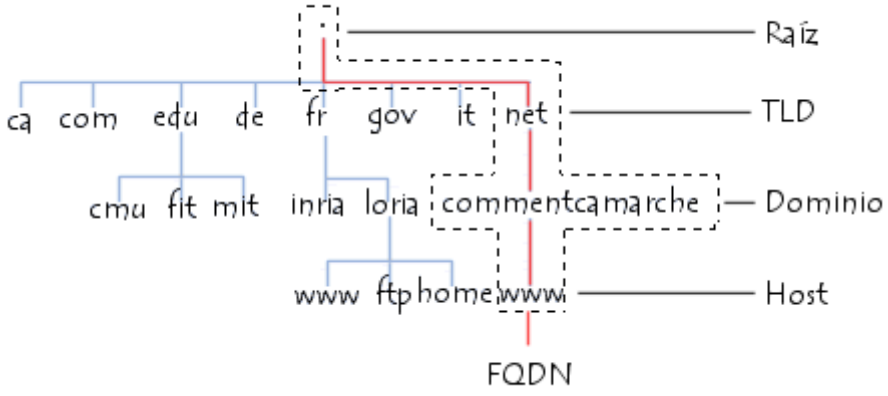
DNS opera a través de tres componentes: Clientes DNS, Servidores DNS y Zonas de Autoridad.

NIC (Network Information Center)

NIC (acrónimo de Network Information Center o Centro de Información sobre la Red) es una institución encargada de asignar los nombres de dominio en Internet ya sean nombres de dominio genéricos o por países, permitiendo personas o empresas, montar sitios de Internet a través de un ISP, mediante un DNS. Técnicamente existe un NIC por cada país en el mundo y cada uno de éstos es responsable por todos los dominios con la terminación correspondiente a su país. Por ejemplo: NIC España es la entidad encargada de gestionar todos los dominios con terminación .es, la cual es la terminación correspondiente asignada a los dominios de España.

Estructura del Sistema DNS

El sistema DNS se basa en una estructura de arbórea en donde se definen los dominios de nivel superior (llamados **TLD**, *Dominios de Nivel Superior*); esta estructura está conectada a un nodo raíz representado por un punto.



Cada nodo del árbol se llama nombre de dominio y tiene una *etiqueta* con una longitud máxima de 63 caracteres.

Por lo tanto, todos los nombres de dominio conforman una estructura arbórea inversa en donde cada nodo está separado del siguiente nodo por un punto (".").

El extremo de la bifurcación se denomina host, y corresponde a un equipo o entidad en la red. El nombre del ordenador que se provee debe ser único en el dominio respectivo, o de ser necesario, en el sub-dominio. Por ejemplo, el dominio del servidor Web por lo general lleva el nombre *www*.

La palabra "dominio" corresponde formalmente al sufijo de un nombre de dominio, es decir, la recopilación de las etiquetas de nodo de la estructura arbórea, con excepción del ordenador.

El nombre absoluto está relacionado con todas las etiquetas de nodo de una estructura arbórea, separadas por puntos y que termina con un punto final que se denomina la dirección **FQDN** (*Nombre de Dominio totalmente calificado*). Por tanto, FQDN especifica la posición absoluta del nodo en el árbol jerárquico del DNS.

La profundidad máxima de una estructura arbórea es 127 niveles y la longitud máxima para un nombre FQDN es 255 caracteres. La dirección FQDN permite ubicar de manera única un equipo en la red de redes.

Desde 2004, a solicitud de varios países de Europa, existe el estándar **IDN** (acrónimo de Internationalized Domain Name) que permite caracteres no-ASCII,

codificando caracteres ***Unicode*** dentro de cadenas de *bytes* dentro del conjunto normal de caracteres de **FQDN**. Como resultado, los límites de longitud de los nombres de dominio **IDN** dependen directamente del contenido mismo del nombre.

Servidores DNS

Hay dos tipos de servidores de nombres:

- **Servidor Maestro**: También denominado Primario. Obtiene los datos del dominio a partir de un archivo alojado en el mismo servidor.

- **Servidor Esclavo**: También denominado Secundario. Al iniciar obtiene los datos del dominio a través de un Servidor Maestro (o primario), realizando un proceso denominado transferencia de zona.

Los Servidores DNS responden dos tipos de consultas:

- **Consultas Iterativas** (no recursivas): El cliente hace una consulta al Servidor DNS y éste le responde con la mejor respuesta que pueda darse basada sobre su caché o en las zonas locales. Si es imposible dar una respuesta, la consulta se reenvía hacia otro Servidor DNS repitiéndose este proceso hasta encontrar al Servidor DNS que tiene la Zona de Autoridad capaz de resolver la consulta.
- **Consultas Recursivas**: El Servidor DNS asume toda la carga de proporcionar una respuesta completa para la consulta realizada por el Cliente DNS. El Servidor DNS desarrolla entonces Consultas Iterativas separadas hacia otros Servidores DNS (en lugar de hacerlo el Cliente DNS) para obtener la respuesta solicitada.

Zonas de Autoridad y Tipos de Registros

Las **Zonas de Autoridad** permiten al Servidor Maestro o Primario cargar la información de una zona. Cada Zona de Autoridad abarca al menos un dominio y, posiblemente, sus sub-dominios, si estos últimos son imposibles de delegar a otras zonas de autoridad.

Por tanto, un DNS es una base de datos distribuida que contiene registros que se conocen como **RR** (*Registros de Recursos*), relacionados con nombres de dominio.

Ya que el sistema de memoria caché permite que el sistema DNS sea distribuido, los registros para cada dominio tienen una duración de vida que se conoce como **TTL** (*Tiempo de vida*). Esto permite que los servidores intermediarios conozcan la fecha de caducidad de la información y por lo tanto que sepan si es necesario verificarla o no.

Por lo general, un **registro** de DNS contiene la siguiente información:

Nombre de dominio (FQDN)	**TTL**	**Tipo**	**Clase**	**RData**
es.terra.net	3600	A	IN	83.5.64.95

- **Nombre de dominio**: el nombre de dominio debe ser un nombre FQDN, es decir, debe terminar con un punto. En caso de que falte el punto, el nombre de dominio es relativo, es decir, el nombre de dominio principal incluirá un sufijo en el dominio introducido;
- **Tipo**: un valor sobre 16 bits que define el tipo de recurso descrito por el registro. El tipo de recurso puede ser uno de los siguientes:

Tipo de Registro.	**Descripción.**
A (Address)	Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección **IPv4** de 32 bits.
AAAA	Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección **IPv6** de 128 bits.
CNAME (Canonical Name)	Registro de nombre canónico que hace que un nombre sea alias de otro. Los dominios con alias obtienen los sub-dominios y registros DNS del dominio original.
MX (Mail Exchanger)	Registro de servidor de correo que sirve para definir una lista de servidores de correo para un dominio, así como la prioridad entre éstos.
PTR (Pointer)	Registro de apuntador que resuelve direcciones IPv4 hacia los nombres anfitriones. Es decir, hace lo contrario al registro A. Se utiliza en zonas de **Resolución Inversa**.
NS (Name Server)	Registro de servidor de nombres, que sirve para definir una lista de servidores de nombres con autoridad para un dominio.
SOA (Start of Authority)	Registro de inicio de autoridad, encargado de especificar el **Servidor DNS** Maestro (o Primario) que proporcionará la información con autoridad acerca de un dominio de Internet,

	dirección de correo electrónico del administrador, número de serie del dominio y parámetros de tiempo para la zona.
SRV (Service)	Registros de servicios, encargados de especificar información acerca de servicios disponibles a través del dominio. Protocolos como **SIP** (SessionInitiation Protocol) y **XMPP** (Extensible Messaging and Presence Protocol) suelen requerir registros **SRV** en la zona para proporcionar información a los clientes.
TXT (Text)	Registros de texto, encargados de permitir al administrador insertar texto arbitrariamente en un registro DNS. Este tipo de registro es muy utilizado por los servidores de listas negras **DNSBL** (DNS-based Blackhole List) para la filtración de Spam. Otro ejemplo de uso sería el caso de las VPN, donde suele requerirse un registro **TXT**, para definir una firma digital que será utilizada por los clientes.

- **Clase**: la clase puede ser **IN** (relacionada a protocolos de Internet, y por lo tanto, éste es el sistema que utilizaremos en nuestro caso), o **CH** (para el sistema caótico);
- **RDATA**: estos son los datos relacionados con el registro. Aquí se encuentra la información esperada según el tipo de registro:
    - A: la dirección IP de 32 bits:
    - CNAME: el nombre de dominio;
    - MX: la prioridad de 16 bits, seguida del nombre del ordenador;
    - NS: el nombre del ordenador; PTR: el nombre de dominio
    - PTR: el nombre de dominio;
    - SOA: varios campos.

Resolución de nombres de dominio

El mecanismo que consiste en encontrar la dirección IP relacionada al nombre de un ordenador se conoce como "**resolución del nombre de dominio**". La aplicación

que permite realizar esta operación (por lo general, integrada en el sistema operativo) se llama "resolución".

Cuando una aplicación desea conectarse con un host conocido a través de su nombre de dominio (por ejemplo, "es.terra.net"), ésta interroga al servidor de nombre de dominio definido en la configuración de su red. De hecho, todos los equipos conectados a la red tienen en su configuración las direcciones IP de ambos servidores de nombre de dominio del proveedor de servicios.

Entonces se envía una solicitud al primer servidor de nombre de dominio (llamado el "**servidor de nombre de dominio principal**"). Si este servidor de nombre de dominio tiene el registro en su caché, lo envía a la aplicación; de lo contrario, interroga a un servidor de nivel superior (en nuestro caso un servidor relacionado con el TLD ".net"). El servidor de nombre de nivel superior envía una lista de servidores de nombres de dominio con autoridad sobre el dominio (en este caso, las direcciones IP de los servidores de nombres de dominio principal y secundario de autoridad para el *.net*).

Entonces el servidor de nombres de dominio principal con autoridad sobre el dominio será interrogado y devolverá el registro correspondiente al dominio del servidor.