DNS (Domain Name System)

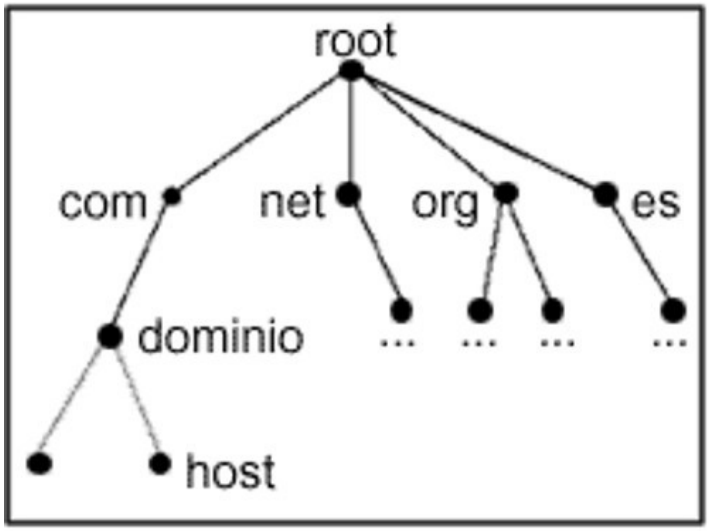
Un sistema de nombres es un mecanismo que permite traducir un nombre a una dirección permitiendo la localización de un ordenador.

Hay 2 tipos:

- sistemas de nombres planos: No hay jerarquía y solo permite clasificar un nombre dentro de una categoría.

- sistemas de nombres jerárquicos: Hay jerárquia a la hora de construir el nombre completo del ordenador.

El sistema de nombres DNS es jerárquico, es decir, tiene estructura de arbol de forma que cada nodo tiene significado.



- El servicio DNS responde a peticiones de número de ip de un nombre o nombre de un número de ip. La principal tarea que realiza es asociar nombres e ip, con ello facilita el recuerdo de los recursos que deseamos acceder. Utiliza un sistema de nombre jerárquico.
- DNS escucha en el puerto UDP número 53

Dominios

- Cada dominio se especifica con varios grupos de caracteres (nodo) separados por puntos. El número máximo de caracteres de cada nodo es 63. El número máximo de nodos o niveles es 127. Los niveles superiores son los grupos de caractéres más a la derecha. Hay un nivel raiz que no tiene caracteres y por tanto no aparece.
- El conjunto de todos los dominios se llama espacio de nombres de dominio y se puede representar en forma de árbol invertido, de ahí el nombre también utilizado de árbol de nombres de dominio
- Para la operación práctica del sistema DNS se utilizan tres componentes principales:
    - Clientes DNS: Un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS (Por ejemplo: ¿Qué dirección IP corresponde a nombre.dominio?);

    - Servidores DNS: Que contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.
    - Zonas de autoridad, porciones del espacio de nombres de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio y posiblemente sus subdominios, si estos últimos no son delegados a otras zonas de autoridad.
- FQDN, Fully Qualified Domain Name, nombre de dominio completamente cualificado, es el nombre completo de un nodo. **Debe incluir el punto final, que es el nivel raíz.**
- Los dominios del primer nivel o nivel tope se llaman dominios TLD (Top Level Domain). Los hay genéricos gTLD (.com, .org, .edu, ...) y geográficos ccTLD (.es, .us, .eu, ...)
- Los dominios de segundo nivel son los que usuario puede comprar, esto es lo que en la práctica todos llamamos dominio. Por ejemplo en www.suarezdefigueroa.es. (suarezdefigueroa sería el dominio de segundo nivel)
- A partir del segundo nivel nos podemos encontrar con algunos registros que reservan ciertos dominios de segundo nivel, de forma que se pueden registrar dominios de tercer nivel bajo estos. Por ejemplo, '.com.es' está reservado para crear dominios de tercer nivel, como 'empresa.com.es'.

  Tradicionalmente, este tercer nivel corresponde al equipo, por ejemplo, www.suarezdefigueroa.es es el equipo que aloja la página web del dominio suarezdefigueroa.es
- Nombres relativos y absolutos. Los nombres de dominio absolutos terminan con "." (ej. “suarezdefigueroa.es.”) y los relativos no, necesitando saber el contexto del dominio superior para determinar de manera única su significado verdadero.

Registro de dominios

- Base de datos Whois, es una base de datos distribuida (y con replicas) que guarda los datos de los dominios de internet, por tanto hay muchos servidores DNS conteniendo esta base de datos. Cada servidor DNS tiene autoridad sobre una parte (subarbol, llamada zona) de esta base de datos (arbol). Un servidor puede delegar parte del subarbol en otros (estos se encargarán de mantener actualizada la información). ICANN es la institución que controla todo el arbol y que delega cada TLD a un organismo, por ejemplo en España el .es lo gestiona Red.es, estos organismos se llaman registry. Entre estos organismos y el usuario final hay otros intermediarios llamados registrar, a estos es a los que compramos un determinado dominio. El usuario se llama registrant.
- El registro de dominios es el proceso por el cual una persona pasa a tener el control sobre un nombre de dominio a cambio de pagar una cierta cantidad de dinero a un registrador:

  Elegir un dominio.
    - Verificar la disponibilidad del nombre de dominio deseado en algún registrador.
    - Ingresar los datos personales.
    - Elegir la cantidad de tiempo que el dominio permanecerá registrado.
    - Pagar el dominio

Una vez arrendado, el registrante debe configurarlo con una URL a la cual redireccionar o una IP.

El registrant del dominio debe esperar un tiempo para que el dominio sea reconocido en todos los servidores de Internet.

El registrar contacta con ICANN y realiza el proceso de forma transparente para el registrant.

El nuevo dominio funciona, y resuelve a la IP apropiada en el servidor DNS usado, pero no en el resto de servidores DNS del mundo. Poco a poco se va propagando el cambio al resto de servidores (propagación DNS).

Finalmente la página ya es accesible mediante un nombre de dominio desde cualquier computadora.

- Transferencia de Zona: es el mecanismo que permite actualizar la informacion a los servidores secundarios a partir de los archivos de zona contenidos en el primario
- Delegación. DNS es una base de datos distribuida y por lo tanto permite su administración descentralizada. La delegación de dominios es el mecanismo que permite llevar a cabo la administración descentralizada. Es decir, el dominio puede ser dividido en subdominios y el control de cada subdominio puede ser delegado. Debe asumir también la responsabilidad de mantener los datos actualizados.
- ICANN es una organización sin fines de lucro que opera a nivel internacional, responsable de asignar espacio de direcciones numéricas de protocolo de Internet (IP), identificadores de protocolo y de las funciones de gestión [o administración] del sistema de nombres de dominio de primer nivel genéricos (gTLD) y de códigos de países (ccTLD), así como de la administración del sistema de servidores raíz. Básicamente ICANN es responsable de la coordinación de la administración de los elementos técnicos del DNS para garantizar una resolución unívoca de los nombres, de manera que los usuarios de Internet puedan encontrar todas las direcciones válidas.

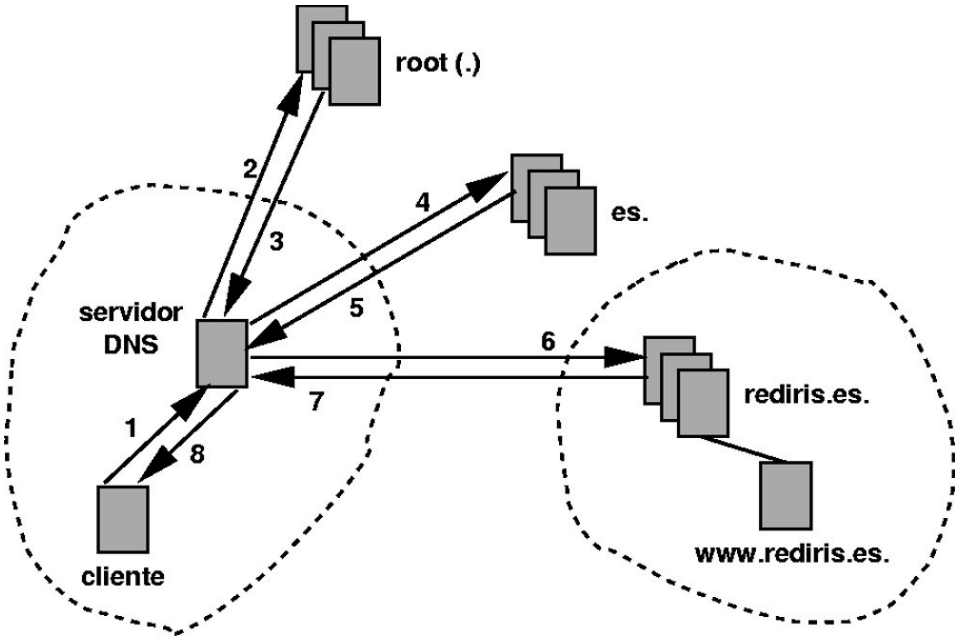
  Para ello, se encarga de supervisar la distribución de los identificadores técnicos únicos usados en las operaciones de Internet, y delegar los nombres de dominios de primer nivel (como .com, .info, etc.).”

Clasificación

Clasificación de servidores dns:

- Servidor raiz. Como es muy complejo tener todos los dominios mundiales guardados en un solo servidor se recurre a la delegación, así los servidores DNS que tienen autoridad sobre niveles altos delegan en servidores DNS de niveles inferiores. Hay 13 servidores DNS encargados del nivel superior (raíz)
- Servidor DNS primario (maestro): obtiene la información de su propia base de datos, las actualizaciones se realizan en su base de datos. Para cada dominio deberá haber varios servidores authoritative, al menos dos: uno de ellos será el primario (o maestro), y los demás serán secundarios (o esclavos) del primero. Por tanto, los dns primarios y secundarios son autoritativos.
- Servidor DNS secundario (esclavo): obtiene la información de un servidor primario (mediante la transferencia de zona). Pide esta información cada cierto tiempo para mantenerse actualizado. Se mantienen estas copias para seguridad y para que descarguen de trabajo a los primarios.

- Servidor DNS caché (local) : almacena la información de las consultas que se van realizando para evitar tenen que volver a realizarlas. Los datos son guardados con una caducidad (indicada por TTL o "tiempo de vida") para evitar obsolencencia. Se guardan tanto las resoluciones como las solicitudes negativas, cuando un dominio no existe, esto se llama caché negativa.
- Reenviador DNS.- Servidor DNS designado por otros servidores DNS internos para su uso en consultas para resolver nombres de dominio DNS externos o fuera del dominio local.



Búsquedas

Tipos de búsquedas:

- búsqueda recursiva. El servidor dns realiza todo el trabajo (si no conoce la respuesta consulta los servidores raiz, una vez estos le dan la ip de los servidores con autoridad en la zona TLD pregunta a estos y asi sucesivamente)
- búsqueda interactiva. El cliente realiza todo el trabajo. Este tipo es más habitual para evitar cargar de trabajo a los servidores DNS.
- búsqueda inversa. Existe un dominio especial in-addr.arpa para bloques IPv4 e ip6.arpa para bloques IPv6 que permiten realizar búsquedas inversas (a partir de la ip saber el nombre)

La base de datos

La base de datos DNS se organiza en Registros de recursos (Resource Records) o simplemente RR. Un RR está formado por:

[Propietario] [TTL] [Clase] Tipo Dato_Registro(Valor)

El Primer campo, Propietario, indica el nombre de host o del dominio DNS al que pertenece este recurso. Puede contener un nombre de host/dominio (completamente cualificado o no), el símbolo "@" (que representa el nombre de la zona que se está describiendo) o una cadena vacía (en cuyo caso equivale al propietario del registro de recursos anterior).

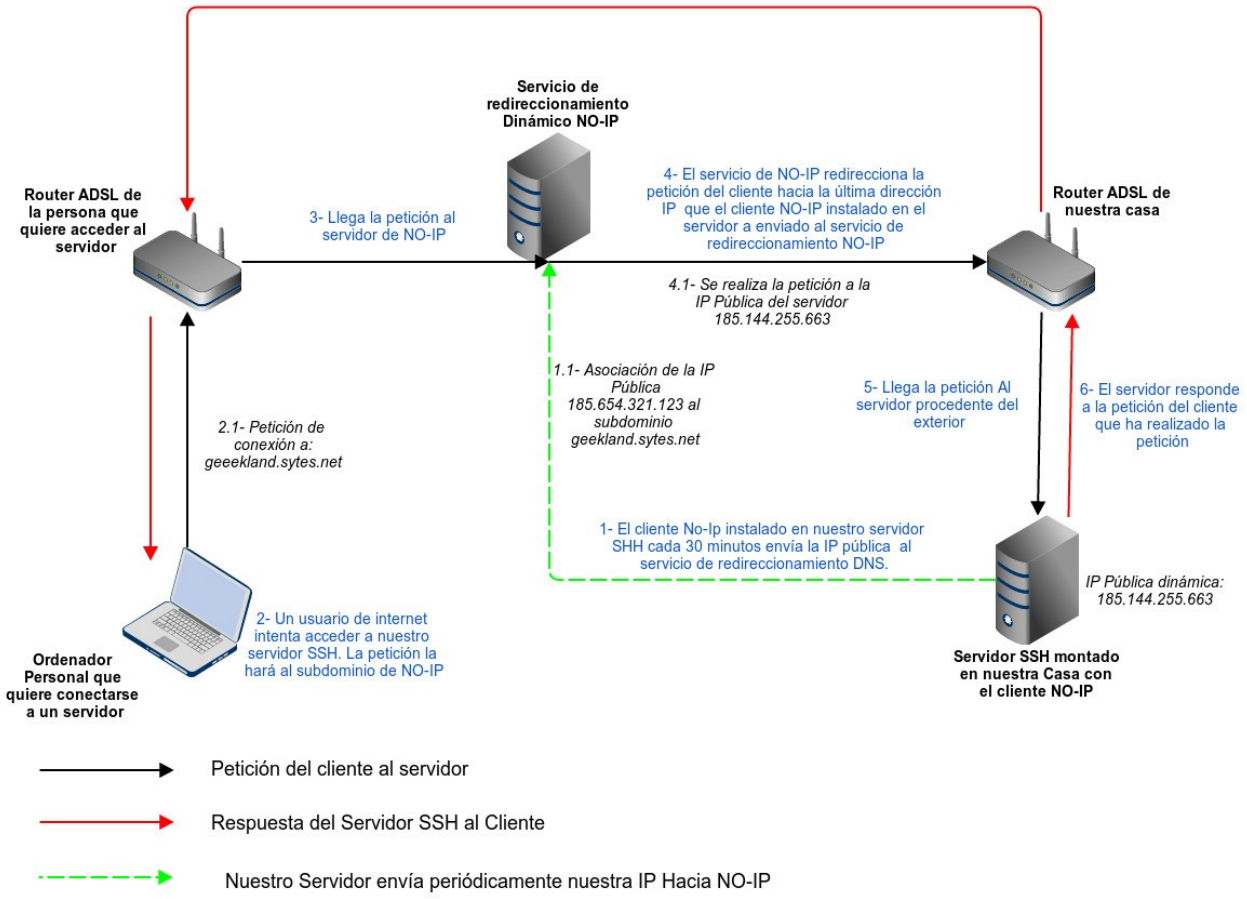
El campo TTL, se refiere al tiempo de vida, e indica la estabilidad del registro, es decir, cuanto tiempo debe guardarse en caché después de almacenarse.

El campo Clase se refiere al tipo de información. Actualmente sólo se utiliza IN, para información de Internet. Este campo si se omite, al igual que el campo Nombre se toma el último valor indicado con anterioridad. A veces, el orden de los campos TTL y Clase pueden intercambiarse, no dando a confusión dado que TTL es numérico.

El campo Tipo indica el tipo de registro, puede contener algunos de los siguientes valores (los más importantes):

TIPO DE ENTRADA	FUNCION	EJEMPLO
SOA	Comienzo de Zona con Autoridad (Start Of zone Authority), es decir, servidor primario de la zona. Marcan el comienzo de un dominio (una zona), suelen ser el primer registro de cada dominio en un Servidor de Nombres de Dominio	@ IN SOA sdf.es. root.sdf.es. (1 ; Serial 604800 ; Refresh 86400 ; Retry 2419200 ; Expire 604800) ; Default TTL
NS	Un servidor de nombres con autoridad para una una determinada zona (ip del servidor con información sobre la zona). Cada zona debe contener registros indicando tanto los servidores principales como los secundarios. Portanto, cada zona debe contener, como mínimo, un registro NS.	sdf.es. 7200 IN NS dns.sdf.es. ó bien (sin TTL @=sdf.es) @ IN NS dns.sdf.es.
A	Una dirección IP de una máquina	www.sdf.es. 14400 IN A 88.2.188.98
AAAA	Una dirección IPv6 de una máquina	www.sdf.es. IN AAAA 2002:abcd::1
CNAME	para definir un alias, habitualmente si se estan ejecutando varios servicios (ftp,...) cada servicio tiene su entrada ftp.dominio.es	www.suarezdefigueroa.es. 345600 IN CNAME www.sdf.es.
MX	El registro de recurso de intercambio de correo (MX, Mail eXchange) especifica un servidor de intercambio de correo para un nombre de dominio. Puesto que un mismo dominio puede contener diferentes servidores de correo, el registro MX puede indicar un valor numérico que permite especificar el orden en que los clientes deben intentar contactar con dichos	sdf.es. IN MX 0 correo.sdf.es.

	servidores de correo.	
PTR	El registro de recursos PTR (PoinTeR) o puntero, realiza la acción contraria al registro de tipo A, es decir, asigna un nombre de dominio completamente cualificado a una dirección IP.	98.188.2.88.in-addr.arpa. IN PTR www.suarezdefigueroa.es.
SVR	Permite indicar los servicios que ofrece el dominio, excepto dns (NS) y correo (MX). La estructura del registro es: servicio.protocolo.nombre TTL clase SRV prioridad peso puerto destino	http.tcp.sdf.es. IN SRV 0 0 80 www.sdf.es. http.tcp.sdf.es. IN SRV 10 0 80 www2.sdf.es.



DNS dinámico

DNS dinámico es un sistema que permite la actualización en tiempo real de la información sobre nombres de dominio situada en un servidor de nombres, es decir, permite trabajar con ips dinámicas asociandolas a un nombre de forma que aunque la ip cambia el nombre permanece fijo y es la forma de acceder al recurso.

El uso más común que se le da es permitir la asignación de un nombre de dominio de Internet a un ordenador con dirección IP variable (dinámica). Esto permite conectarse con la máquina en cuestión sin necesidad de tener que rastrear las direcciones IP. Tenemos 2 enfoques para tratar este mecanismo:

actualizar la ip pública en servidores dns como no-ip, dyndns ... y otro dentro de la zona, los clientes dinámicos envian la información al servidor dns de la zona para que la mantenga actualizada o bien sincronizamos el servidor dhcp con el servidor dns.

El archivo hosts

El archivo hosts es un archivo de texto que resuelve los nombres antes que el servidor dns, se encuentra en el directorio de windows system32/drivers/etc y en ubuntu en /etc. Cada entrada consiste en una dirección IP, uno o más espacios en blanco y el nombre de dominio asociado a esa IP. Podemos entrar las páginas más visitadas para acelerar la carga. Evitar la navegación por un dominio poniendo una ip falsa.

Hay también un protocolo muy similar a DNS para windows WINS, este permite registrar nombres de recursos de red NetBIOS y resolver éstos a sus direcciones IP correspondientes; se suele utilizar en estaciones de trabajo que ejecutan versiones antiguas de sistemas operativos de Microsoft