# Servicios de red implicados en el despliegue de una aplicación web.

## 1.-Servicio de nombres de dominio (DNS)

Debe existir algo que nos traduzca los nombres a IPs o viceversa. Sí, este algo no es otro que el **servidor DNS** o un archivo de texto, denominando **hosts**, como el archivo **/etc/hosts** en sistemas GNU/Linux.

Puede convivir en una misma máquina un servidor DNS y el archivo /etc/hosts, pero primero se intentará la resolución IP/Nombre mediante el archivo /etc/hosts y en caso de no encontrar correspondencia, actuará el servidor DNS.

El fichero **/etc/hosts** permite **alias** de nombres de dominios, esto es, una misma IP puede apuntar a nombres distintos. Cada línea del fichero comenzará con una IP y en la misma línea separados por espacios o tabuladores puedes escribir los nombres de dominios correspondientes. El primer nombre, el más cercano a la IP, es considerado el principal, los demás son alias de éste.

## 1.1.- Ventajas del DNS.

El DNS permite que cualquier cambio efectuado solamente en un servidor se replique en todos los servidores DNS que la configuración permita.

Cualquier cambio es dinámico: configuras solamente un servidor y éste se encarga de replicar el cambio.

Cada servidor DNS se ocupa de su zona, eso no imposibilita el acceso a otras zonas y por lo tanto, a la visibilidad y conectividad de otros dominios que no dependan de ese servidor DNS.

Una zona DNS es aquella parte del DNS para la cual se ha delegado la administración, es decir, cuando configuras un dominio en un servidor DNS éste debe pertenecer a una zona.

Tipos de zonas:

* **Zona de búsqueda directa:** las resoluciones de esta zona devuelven la dirección IP correspondiente al recurso solicitado.
* **Zona de búsqueda inversa:** las resoluciones de esta zona buscan un nombre de equipo en función de su dirección IP.

Los servidores DNS no solamente sirven para la resolución de nombres de Internet, también se pueden utilizar en redes locales.

Cuando un usuario de la red local intenta acceder a un recurso local, podrá utilizar nombre en lugar de direcciones IP. Si el usuario desea acceder fuera de la red local a algún recurso en Internet, el DNS local nunca podrá llevar a cabo dicha resolución y se la traslada al siguiente servidor DNS (en Internet) en su jerarquía de servidores DNS, hasta que la petición sea satisfecha.

* Ping 192.168.200.100
* Ping cliente.local

En ambos casos, deberías obtener la misma respuesta. Esto suele ser muy útil cuando los hosts reciben su IP por DHCP ya que puede ocurrir que desconozcamos la IP que tiene cierto equipo pero sí conocer su nombre en el dominio, que será invariable.

Ventajas:

1.- Desaparece la carga excesiva en la red y en los hosts: ahora la información esta distribuida por toda la red, al tratarse de una base de datos distribuida.

2.- No hay duplicidad de nombres: el problema se elimina debido a la existencia de dominios controlados por un único administrador. Puede haber nombres iguales pero en dominios diferentes.

3.- Consistencia de la información: ahora la información que está distribuida es actualizada automáticamente sin intervención de ningún administrador.

## 1.2.- Nombres de dominio.

Para la redirección deberá existir un servidor DNS que las resuelva o bien, en su defecto o a mayores, deberán existir las entradas correspondientes en el fichero del sistema local **/etc/hosts.** En caso de coexistir, primero se prueba la resolución en el fichero y luego en el servidor.

Si estás pensando en pocos equipos a resolver el nombre de dominio la simplicidad del fichero  te permitiría no tener que montar un servidor, pero si el número de equipos que deben resolver el nombre en IP es elevado, el sistema del fichero es complicado de mantener y deberías pensar en montar un servidor DNS.

La complejidad radica en que en el fichero **/etc/hosts** los cambios son estáticos, así, para actualizar o activar un nuevo cambio debe editarse en todos los ficheros /etc/hosts implicados.

Ejemplo:

* Primero, se debe averiguar que servidor DNS resuelve el domino raíz 'org' a una IP.
* Segundo, una vez obtenida esa IP que gobierna el dominio raíz 'org', se le pregunta por la IP del servidor DNS que gobierna el subdominio 'debian' bajo 'org'.
* Tercero, una vez obtenida la IP del servidor DNS que gobierna el dominio 'debian.org' se le pregunta por la IP del equipo 'www.debian.org'

Bien, pues no existe un número limitado de redirección de consultas, lo que sucede es que las consultas se van escalando hasta encontrar un servidor DNS que las resuelva, y escalando y escalando puede ser que las consultas se resuelvan en los últimos servidores DNS a los cuales se puede preguntar: los servidores raíz.

Todos los servidores DNS son servidores caché, lo que significa que recuerdan las consultas efectuadas. Es más, los equipos clientes, desde donde se hace la consulta a través del navegador también poseen una memoria caché DNS, de tal forma que antes de a preguntar al servidor DNS, se mira en la caché del propio sistema operativo, y si se obtiene la respuesta, el proceso se ha acabado.

***El sistema DNS en realidad es una base de datos distribuida, que permite la administración local de segmentos que juntos componen toda la base de datos local. Los datos de cada segmento están disponibles para toda la red a través de un esquema cliente-servidor jerárquico.***

## 1.2.1.-¿Cómo es un nombre de dominio?

**Primero**: Los puntos separan dominios y subdominios, empezando de derecha a izquierda tendrás dominios de primer nivel y dominios de segundo, tercer, …, n-ésimo nivel, denominados subdominios. Así:

* **org** es el dominio de primer nivel que identifica a organizaciones.
* **debian** es un subdominio, en este caso dominio de segundo nivel bajo org, que identifica al nombre de la organización o al nombre de la empresa, sucursal, etc.
* **www** es un subdominio, en este caso dominio de tercer nivel bajo debian, que identifica al equipo donde está colgada la página web, esto es, identifica el servidor web que aloja la página web. Es el dominio www que el servidor DNS redirecciona a la IP del servidor web.
* **Segundo**: **http://** es el protocolo de hypertexto que permite la correcta visualización de la página web en el navegador. Es lo que el navegador autocomplementa en caso de no estipular uno propio en la barra de direcciones URL con en nombre de dominio.

Los dominios de primer nivel identifican el tipo de página web que solicitas o bien la localización de la misma:

* **net** identifica redes.
* **com** identifica comercio.
* **es** identifica localización España.
* **tk** identifica localización Tokelau.

Esto suele ser lo común, más no es obligatorio.

A nivel gramatical los dominios deben cumplir una serie de requisitos. Por ejemplo:

* Sólo pueden estar compuestos de letras (alfabeto inglés), números y guiones ("-").
* No pueden empezar o terminar por guiones.
* Tienen que tener menos de 63 caracteres sin incluir la extensión, y más de uno o dos dependiendo del dominio de primer nivel.

Hoy día ya es posible registrar dominios con caracteres de otras lenguas no inglesas, como la ñ o la ç. Estos dominios se denominan **multilingües**.

## 1.2.2.-Jerarquía de nombres de dominio.

El espacio de nombres de dominio está organizado de forma jerárquica. El nivel más alto es el dominio raíz, que se representa como un punto ( . ) y el siguiente nivel en la jerarquí se llama dominio de nivel superior (TLD).

Sólo hay un dominio raíz, pero muchos TLDs y cada TLD se llama dominio secundario del dominio raíz.

El dominio raíz es el dominio principal, ya que está un nivel por encima de un TLD y cada TLD, a su vez, pueden tener muchos dominios hijos. Los hijos de los dominios de nivel superior se llaman de segundo nivel, los del segundo nivel se llaman de tercer nivel, los del tercer nivel de cuarto, y así sucesivamente.

Por lo tanto el DNS, organiza los **hostname** en una jerarquía de dominios separados por el carácter punto '.'. Un **dominio** es una colección de nodos relacionados de alguna forma.

* rrhh.departamento.empresa.org
* marketing.departamento.empresa.org
* contabilidad.consultas.empresa.org

Donde:

* La empresa agrupa sus nodos en el **dominio** de primer nivel "org". Éste es un TLD.
* La empresa tiene un **subdominio**, dominio de segundo nivel "empresa" bajo "org". Así "empresa" es un dominio de segundo nivel, hijo del TLD "org".
* A su vez puedes encontrar nuevos **subdominios** dentro, en este caso: "departamento" y "consultas". Es decir, dominios de tercer nivel, hijos a su vez del dominio de segundo nivel "empresa".
* Finalmente, un nodo que tendrá un nombre completo conocido como totalmente cualificado o **FQDN**, que es la concatenación de: TLD, dominio de segundo nivel, dominio de tercer nivel, etc.

El símbolo del dominio raíz es el punto situado más a la derecha del nombre del dominio.

Sólo hay una raíz de dominio, pero hay más de 250 dominios de nivel superior, clasificados en los siguientes tres tipos:

* **TLD de código de país** (ccTLD): dominios asociados con países y territorios. Hay más de 240 ccTLD. Están formados por 2 letras, por ejemplo: **es, uk, en, y jp.**
* Dominios de nivel superior **genéricos** (gTLD): están formados por 3 o más letras. A su vez se subdividen en:
  + **Dominios de internet patrocinados** (sTLD): representan una comunidad de intereses, es decir, detrás existe una organización u organismo público que propone el dominio y establece las reglas para optar a dicho dominio. Por ejemplo: **edu, gov, int, mil, aero, museum.**
  + **Dominios de internet no patrocinados** (uTLD). Sin una organización detrás que establezca las reglas para optar a dicho dominio. La lista de gTLD incluye: **com, net, org, biz, info.**

<https://data.iana.org/TLD/tlds-alpha-by-domain.txt>

## 1.3.-Servidores de raíz.

La organización que gestiona globalmente los servidores raíz por concesión del gobierno estadounidense es la **ICANN**, la cual 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. Aunque en un principio estos servicios los desempeñaba **IANA** y otras entidades bajo contrato con el gobierno de EE.UU., actualmente son responsabilidad de ICANN.

**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.

***Las empresas, ciudades u organizaciones podrán registrar sus propios dominios genéricos, tras la decisión adoptada el 20 de Junio de 2011 por la ICANN en Singapur.***

Los servidores raíz son entidades distintas. Hay 13 servidores raíz o, más precisamente, 13 direcciones IP en Internet en las que pueden encontrarse a los servidores raíz.

Todos estos servidores almacenan una copia del mismo archivo que actúa como índice principal de las agendas de direcciones de Internet. Enumeran una dirección para cada dominio de nivel principal (.com, .es, etc.) en la que puede encontrase la propia agenda de direcciones de ese registro.

Las entidades encargadas de operar los servidores raíz son bastante autónomas pero, al mismo tiempo, colaboran entre sí y con ICANN para asegurar que el sistema permanece actualizado con los avances y cambios de Internet.

Los **trece** servidores raíz DNS se denominan por las primeras trece letras del alfabeto latino, de la **A** hasta la **M** (A.ROOT-SERVERS.NET., B.ROOT-SERVERS.NET., …, M.ROOT-SERVERS.NET.), y están en manos de 9 organismos y corporaciones diferentes e independientes, principalmente universidades, empresas privadas y organismos relacionados con el ejercito de EE.UU. Aproximadamente la mitad depende de organizaciones públicas estadounidenses.

<http://www.internic.net/zones/named.root>

<https://root-servers.org/>

## 1.4.- Funcionamiento del cliente DNS.

Cuando utilizas en un programa un nombre DNS, éste debe ser resuelto a una IP. Entonces, un cliente DNS busca el nombre que se utiliza en el programa, consultando los servidores DNS para resolver el nombre. Cada mensaje de consulta que envía el **cliente** contiene tres grupos de información, que especifican una pregunta que tiene que responder el servidor:

* Un nombre de dominio DNS especificado, indicado como un nombre de dominio completo (FQDN).
* Un tipo de consulta especificado, que puede establecer un registro de recursos por tipo o un tipo especializado de operación de consulta.
* Una clase especificada para el nombre de dominio DNS.

Las consultas DNS se resuelven de diferentes formas:

* A veces, un cliente responde a una consulta localmente mediante la información almacenada en la caché obtenida de una consulta anterior.
* El servidor DNS puede utilizar su propia caché de información de registros de recursos para responder a una consulta.
* Un servidor DNS también puede consultar, o ponerse en contacto con otros servidores DNS, en nombre del cliente solicitante para resolver el nombre por completo y, a continuación, enviar una respuesta al cliente. Este proceso se llama **recursividad**.
* Además, el mismo cliente puede intentar ponerse en contacto con servidores DNS adicionales para resolver un nombre. Cuando un cliente lo hace, utiliza consultas adicionales e independientes en función de respuestas de referencia de los servidores. Este proceso se llama **iteración**.

En general, el proceso de consulta DNS se realiza en dos partes:

* La consulta de un nombre comienza en un equipo cliente y se pasa al solucionador (resolver), el servicio Cliente DNS, para proceder a su resolución.
* Cuando la consulta no se puede resolver localmente, se puede consultar a los servidores DNS según sea necesario para resolver el nombre.

## 1.4.1.- Consultas recursivas.

El cliente DNS formula una consulta a tu servidor DNS preferido. Cuando el servidor DNS recibe una consulta, primero comprueba si puede responder la consulta en las zonas configuradas localmente en el servidor, esto es, en las zonas que posee autoridad. Así, pueden ocurrir dos situaciones:

1. Si el nombre consultado existe, esto es, coincide con un registro de recursos correspondiente en la información de zona local, el servidor responde con autoridad y usa esta información para resolver el nombre consultado.

2. Si el nombre consultado no existe, esto es, no existe ninguna información de zona para el nombre consultado, a continuación el servidor comprueba si puede resolver el nombre mediante la información almacenada en la caché local de consultas anteriores.

De nuevo, se dan dos situaciones:

a. Si el servidor preferido puede responder al cliente solicitante con una respuesta coincidente de su caché, finaliza la consulta y responde con esta información.

b. Si el servidor preferido no puede responder al cliente solicitante con una respuesta coincidente de su caché, el proceso de consulta puede continuar y se usa la **recursividad** para resolver completamente el nombre. Esto implica la asistencia de otros servidores DNS para ayudar a resolver el nombre. De forma predeterminada, el servicio cliente DNS solicita al servidor que utilice un proceso de recursividad para resolver completamente los nombres en nombre del cliente antes de devolver una respuesta. El servidor DNS se configura, de forma predeterminada, para admitir el proceso de recursividad como se muestra en el gráfico siguiente.

Para que el servidor DNS realice la recursividad correctamente, primero necesita información de contacto útil acerca de los otros servidores DNS del espacio de nombres de dominio DNS. Esta información se proporciona en forma de **sugerencias de raíz**, una lista de los registros de recursos preliminares que puede utilizar el servicio DNS para localizar otros servidores DNS que tienen autoridad para la raíz del árbol del espacio de nombres de dominio DNS. Los servidores raíz tienen autoridad para el dominio raíz y los dominios de nivel superior en el árbol del espacio de nombres de dominio DNS.

Un servidor DNS puede completar el uso de la recursividad utilizando las sugerencias de raíz para encontrar los servidores raíz. En teoría, este proceso permite a un servidor DNS localizar los servidores que tienen autoridad para cualquier otro nombre de dominio DNS que se utiliza en cualquier nivel del árbol del espacio de nombres.

Aunque el proceso de consulta recursiva puede usar muchos recursos cuando se realiza como se describe anteriormente, tiene algunas ventajas en el rendimiento para el servidor DNS. Por ejemplo, durante el proceso de recursividad, el servidor DNS que realiza la búsqueda recursiva obtiene información acerca del espacio de nombres de dominio DNS.

Esta información se almacena en la caché del servidor y se puede utilizar de nuevo para ayudar a acelerar la obtención de respuestas a consultas subsiguientes que la utilizan o concuerdan con ella. Con el tiempo, esta información almacenada en caché puede crecer hasta ocupar una parte significativa de los recursos de memoria del servidor, aunque se limpia siempre que el servicio DNS se activa y desactiva.

## 1.4.2.- Consultas iterativas.

La iteración es el tipo de resolución de nombres que se utiliza entre clientes y servidores DNS cuando se dan las condiciones siguientes:

* El cliente solicita el uso de recursividad, pero ésta se encuentra deshabilitada en el servidor DNS.
* El cliente no solicita el uso de recursividad cuando consulta el servidor DNS.

Una solicitud iterativa de un cliente informa al servidor DNS de que el cliente espera la mejor respuesta que el servidor DNS pueda proporcionar inmediatamente, sin entrar en contacto con otros servidores DNS.

Cuando se utiliza la iteración, un servidor DNS responde al cliente en función de su propio conocimiento específico acerca del espacio de nombres, sin tener en cuenta los datos de los nombres que se están consultando.

Cuando se proporciona una referencia, el cliente DNS asume la responsabilidad de continuar efectuando consultas iterativas a otros servidores DNS configurados para resolver el nombre.

Cuando se utiliza la iteración, un servidor DNS puede ayudar en la resolución de la consulta de un nombre además de devolver su mejor respuesta propia al cliente. En la mayor parte de las consultas iterativas, un cliente utiliza su lista de servidores DNS configurada localmente para entrar en contacto con otros servidores de nombres a través del espacio de nombres DNS si su servidor DNS principal no puede resolver la consulta.

## 1.4.3.-Consultas inversas.

En la mayoría de la consultas DNS los clientes normalmente realizan una búsqueda directa. Este tipo de consulta espera recibir una dirección IP como respuesta a la consulta. Pero, DNS también proporciona un proceso de búsqueda inversa, es decir, buscar un nombre de host a través de una dirección IP. Así, una búsqueda inversa busca la respuesta a una pregunta tipo como la siguiente: ¿Cuál es el nombre DNS del host que utiliza la dirección IP 192.168.200.100?.

DNS no se diseñó originalmente para aceptar este tipo de consulta. Un problema de compatibilidad con el proceso de consulta inversa es la diferencia en la forma en que el espacio de nombres DNS organiza e indexa los nombres, y cómo se asignan las direcciones IP. Si el único método para responder a la pregunta anterior fuera buscar en todos los dominios del espacio de nombres DNS, una consulta inversa llevaría demasiado tiempo y requeriría un procesamiento demasiado largo como para ser útil.

Entonces, para resolver este problema, en el estándar DNS se definió y se reservó un dominio especial para las **IP versión 4,** el dominio **in-addr.arpa**, en el espacio de nombres DNS de Internet con el fin de proporcionar una forma práctica y confiable para realizar las consultas inversas. Al crear el espacio de nombres inverso, los subdominios del dominio in-addr.arpa se crean con el orden inverso de los números en la notación decimal con puntos de las direcciones IP. ***100.200.168.192.in-addr.arpa.***

Este orden inverso de los dominios para el valor de cada octeto es necesario porque, a diferencia de los nombres DNS, cuando se leen las direcciones IP de izquierda a derecha se interpretan al contrario. Cuando se lee una dirección IP de izquierda a derecha, se ve desde su información más general (una dirección IP de red) en la primera parte de la dirección a la información más específica (una dirección IP de host) que contienen los últimos octetos. Por esta razón, se debe invertir el orden de los octetos de las direcciones IP cuando se crea el árbol del dominio in-addr.arpa..

Finalmente, el árbol del dominio in-addr.arpa, tal como se crea en DNS, requiere que se defina un tipo de registro de recursos adicional: el registro de recursos de puntero (PTR). Este registro de recursos se utiliza para crear una asignación en la zona de búsqueda inversa que, normalmente, corresponde a un registro de recurso de dirección (A) de host con nombre para el nombre del equipo DNS de un host en su zona de búsqueda directa.

**El dominio in-addr.arpa se usa en todas las redes TCP/IP que se basan en el direccionamiento del Protocolo de Internet versión 4 (IPv4). Para el Protocolo de Internet versión 6 (IPv6) se usa un nombre de dominio especial diferente, el dominio ip6.arpa.**

Ten en cuenta que, si el servidor DNS no puede responder el nombre de la consulta inversa, se puede utilizar la resolución DNS normal (ya sea la recursividad o la iteración) para localizar un servidor DNS con autoridad para la zona de búsqueda inversa y que contenga el nombre consultado. En este sentido, el proceso de resolución de nombres utilizado en una búsqueda inversa es idéntico al de una búsqueda directa.

## 1.5.- Tipos de servidores DNS.

Dependiendo de la configuración y funcionamiento de los servidores, éstos pueden desempeñar distintos papales:

* Servidores primarios: estos servidores almacenan la información de su zona en una base de datos local. Son los responsables de mantener la información actualizada y cualquier cambio debe ser notificado a este servidor.
* Servidor maestro: los servidores maestros son los que transfieren las zonas a los servidores secundarios. Cuando un servidor secundario arranca busca un servidor maestro y realiza la transferencia de zona. Un servidor maestro para una zona puede ser a la vez un servidor primario o secundario de esa zona. Se evita sobrecarga en los servidores primarios con transferencias de zonas.
* Servidores secundarios: o esclavos, aunque a su vez pueden ser maestros de otros servidores secundarios. Son aquellos que obtienen los datos de su zona desde otro servidor que tenga autoridad para esa zona. El proceso de copia de la información se denomina transferencia de zona.
* Sevidores sólo cache: