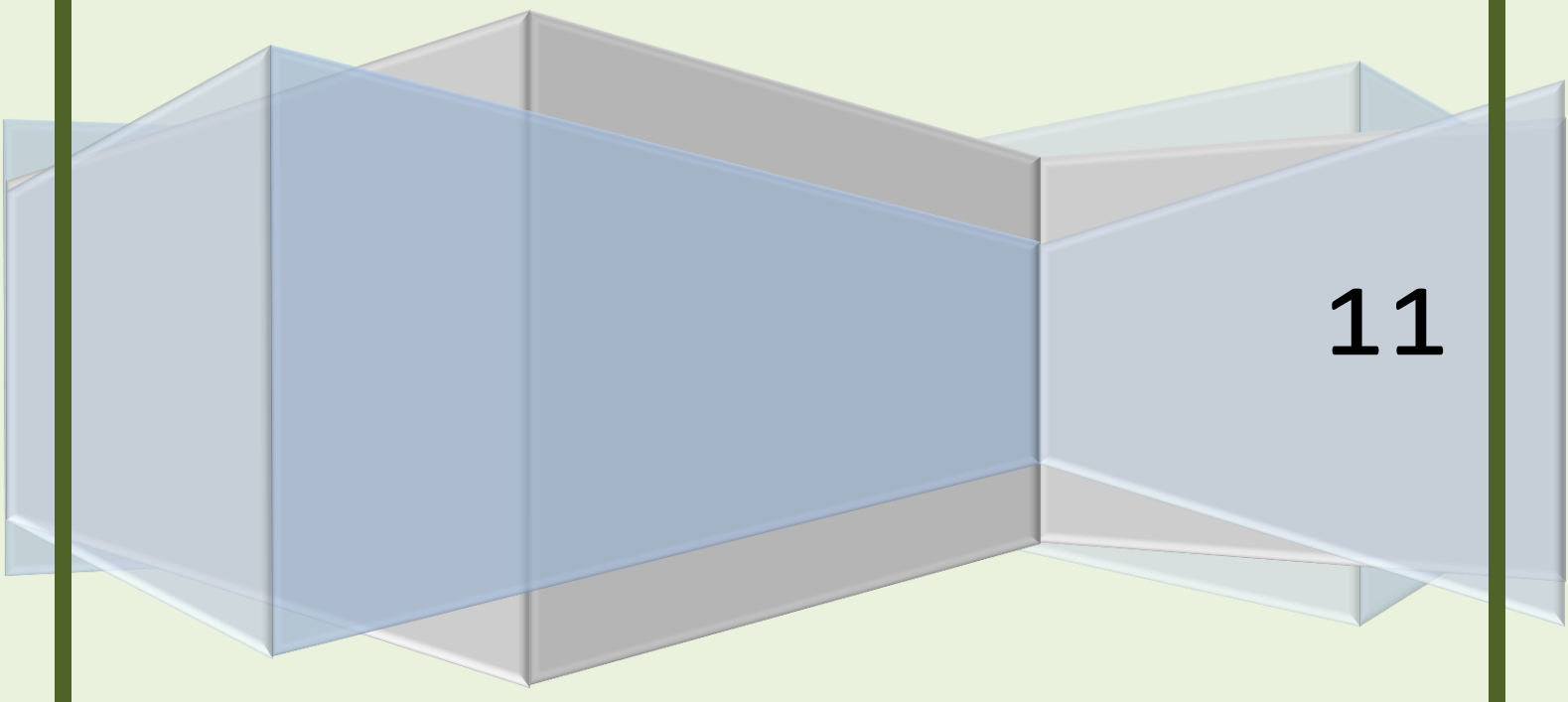
2º ASIR

SERVICIOS DE RED E INTERNET

VICEN MORALES

UD3 -DNS



11

ÍNDICE UD3 –INSTALACIÓN Y ADMINISTRACIÓN DE SERVICIOS DE NOMBRE DE DOMINIO.

Introducción a los servicios de nombres de dominio.

- **Sistemas de nombres planos y jerárquicos.**
- **Historia del DNS.**
- **Componentes del servicio de nombres de dominio:**
  - **–Espacios de nombres de dominio (name space)**
  - **–Bases de datos DNS (registro de recursos).**
  - **–Servidores de nombres (servidores DNS).**
  - **–Clientes DNS (resolutores – "resolvers")**
  - **–Protocolo DNS.**
- **Espacio de nombres de dominio:**
  - **–Nombres de dominio.**
  - **–Dominio raíz. Dominios y subdominios.**
  - **–Nombres relativos y absolutos. FQDN.**
  - **–Uso de dominios.**
  - **–Administración de nombres de dominio en Internet:**
    - **Delegación. Dominio raíz. ICANN.**
    - **Dominios TLD y Operadores de registro.**
    - **Registros de dominios en Internet. Agentes registradores.**

Servidores de nombres de dominio (DNS):

- **–Zonas. Autoridad. Registro de recursos (RR).**
- **–Tipos de servidores de nombres DNS.**
  - **Servidor maestro o primario.**
  - **Servidor esclavo o secundario.**
  - **Servidor caché.**
  - **Servidor reenviador (forwarding)**
  - **Servidor solo autorizado.**
- **–Software comercial de servidores de nombres de dominio.**
- **–Servidores raíz.**

Clientes DNS (Resolutores – "resolvers" de nombres)

Proceso de resolución de un nombre de dominio.

- **–Consultas recursivas.**
- **–Consultas iterativas.**
- **–Caché y TTL.**
- **–Recursividad y caché.**

Resolución inversa:

–Mapeo de direcciones y dominio arpa.

–Zonas de resolución inversa. Proceso de resolución.

–Delegación y resolución inversa.

Registros de recursos DNS:

–Formato general.

–Tipos de registros: SOA, NS, A, AAAA, A6, CNAME, MX, SRV, PTR.

–Delegación y Glue Record.

Transferencias de Zona:

–Tipos de transferencias de zona: Completa e Incremental.

–Proceso de transferencias de zona.

DNS Dinámico (DDNS o Dynamic DNS):

–Actualizaciones manuales.

–Actualizaciones dinámicas.

–DNS dinámico en Internet.

Protocolo DNS

Seguridad DNS

–Vulnerabilidades, amenazas y ataques.

–Mecanismos de seguridad.

UD3 – INSTALACIÓN Y ADMINISTRACIÓN DE SERVICIOS DE NOMBRES DE DOMINIO

INTRODUCCIÓN A LOS SERVICIOS DE NOMBRES DE DOMINIO

El Servicio de Nombres de Dominio (DNS) es una forma sencilla de localizar un ordenador en Internet. Todo ordenador conectado a Internet se identifica por su dirección IP: una serie de cuatro números de hasta tres cifras separadas por puntos. Sin embargo, como a las personas les resulta más fácil acordarse de nombres que de números, se inventó un sistema (DNS - Domain Name Server) capaz de convertir esos largos y complicados números, difíciles de recordar, en un

sencillo nombre.

Los nombres de dominio no sólo nos localizan, además garantizan nuestra propia identidad en la red. Al igual que en el mundo real existen diferentes formas de identificación como puede ser el DNI, el carnet de conducir, la huella digital, etc. en Internet el dominio constituye el principal medio de identificación.

En realidad el servicio de nombres de dominio tiene más usos y mucho más importantes que el anterior. Por ejemplo, este servicio es fundamental para que el servicio de correo electrónico funcione.

Un Servidor de Nombres de Domino es una máquina cuyo cometido es buscar a partir del nombre de un ordenador la dirección IP de ese ordenador; y viceversa, encontrar su nombre a partir de la dirección IP.

Ejemplo de resolución de nombres

¿Qué es lo que pasa entre un ordenador y el servidor DNS cuando el primero intenta conectarse con una máquina utilizando el nombre en lugar de la dirección IP? Sea www.uned.es el nombre la máquina con la cual se desea conectar:

El ordenador local contacta con su servidor DNS (servidor-uno) (que se tiene configurado en el ordenador), y le solicita la dirección IP de www.uned.es.

El servidor DNS mira en sus tablas de asignación, y si no lo encuentra entre los datos que guarda con las ultimas peticiones que ha servido, manda una petición a uno de los "servidores raíz" de Internet el cual averiguará qué servidor de nombres resuelve el dominio "uned.es"

El servidor raíz responderá a servidor-uno (servidor DNS del ordenador local) con la dirección del servidor que resuelve direcciones "uned.es". En este caso 62.204.192.21.

Servidor-uno hará una petición a 62.204.192.21, preguntando qué dirección IP tiene "www.uned.es".

62.204.192.21 mira en sus tablas y devuelve la dirección IP de "www.uned.es " a servidor-uno, servidor-uno manda la dirección IP encontrada al ordenador local que la usará para conectarse con www.uned.es.

Todo esto pasa en tan solo unos pocos milisegundos (más o menos), por lo que generalmente no se nota el retraso entre que se escribe la dirección nemotécnica y se resuelve cuál es su dirección IP.

SISTEMAS DE NOMBRES PLANOS Y JERÁRQUICOS

El sistema de nombres DNS es un sistema jerárquico, es decir, tiene estructura de árbol de forma que cada nodo del árbol tiene un significado.
Por el contrario, los nombres NetBIOS que usa Windows es un espacio de nombres plano, una lista de nombres posibles, sin agrupamientos de ningún tipo.
En un espacio de nombres planos, todos los nombres deben ser absolutamente únicos: no puede haber 2 máquinas con el mismo nombre. Para organizaciones grandes, esto no sirve, pues podría haber conflictos de nombres, todos los Administradores tendrían que conocer todos los nombres usados en toda la red, para no repetirlos.
Con los nombres jerárquicos ese problema se resuelve. Así, un ejemplo de nombres jerárquicos es el espacio de los nombres de personas: nombre+apellido+mote+...; otro ejemplo, el espacio de nombres de los ficheros en disco (se pueden crear ficheros con el mismo nombre siempre que estén en otra carpeta): disco\carpeta\subcarpeta\+...+nombre.

Cada dominio es como una carpeta: no es sólo un ordenador, sino un espacio de alojamiento en el que se pueden añadir nombres de ordenadores. En la parte superior del árbol DNS está la raíz. La raíz es el área de alojamiento a la que se conectan los dominios (igual que el directorio raíz de un disco).
Cada dominio puede tener subdominios. Se separa cada subdominio de su dominio padre con un ".".
Un nombre DNS completo, incluyendo el nombre de host y todos sus dominios y subdominios hasta llegar al host (por orden), se llama un nombre de dominio totalmente cualificado (FQDN) y se escribe con la raíz en el lado derecho, seguida de los nombres de dominio y subdominio (por orden) Añadidos a la izquierda de la raíz, y, por último, el nombre del host.

SISTEMAS DE NOMBRES PLANOS Y JERÁRQUICOS

- *Sistema de nombres planos:* Cada nombre es independiente de los demás. No existe ninguna jerarquia ni relación entre ellos, de manera que el nombre no aporta otra información que la identificación del host.

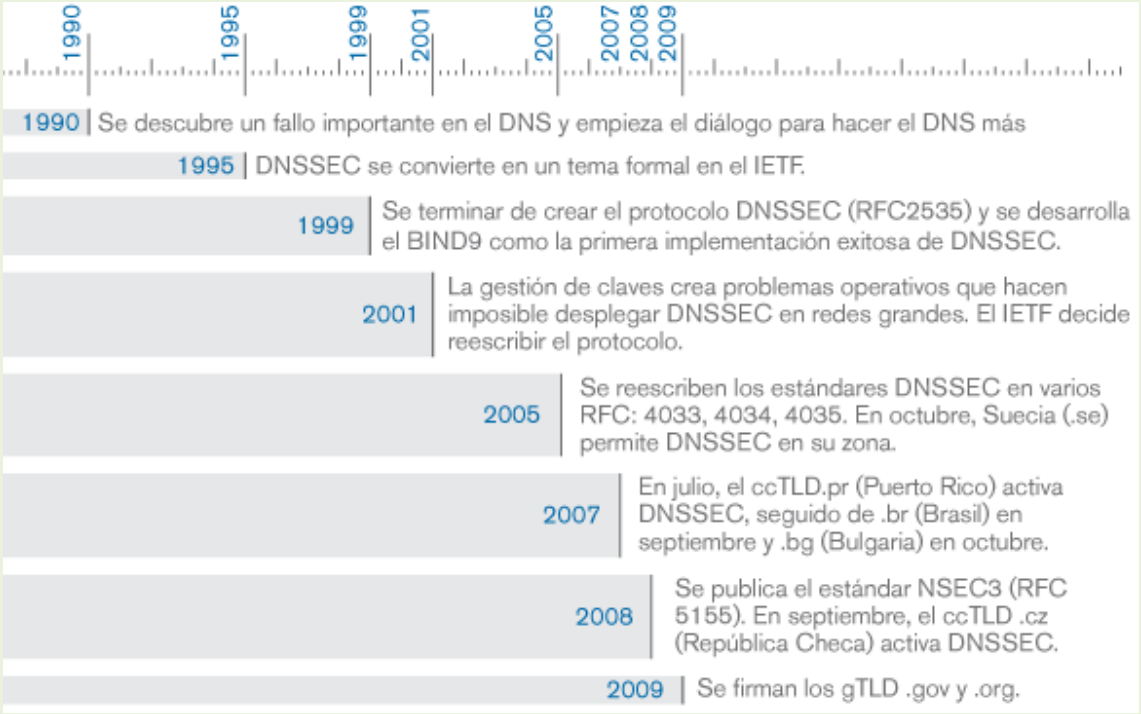
Ejemplo
El DNI es un sistema de nombres planos 11111111X -> Pepito Palotes Partidos

- *Sistema de nombres jerárquicos:* Existe una jerarquía de nombres que establece la manera de construir el nombre de un host. El propio nombre aporta información de la pertenencia del host a determinada categoría

Ejemplo
La dirección postal es un sistema de nombres jerárquico C/ La Encrucijada, 33, Mislata, Valencia, España -> Pepito Palotes Partidos

HISTORIA DEL DNS

La historia del DNS empezó en los primeros tiempos de Internet cuando aún era una red pequeña que dependía del Departamento de Defensa de los EEUU. Los nombres de Host de los equipos estaban listados en un solo fichero HOSTS centralizado en un solo servidor. Ese archivo era descargado regularmente en los equipos que necesitaban resolver nombres. Pronto se dieron cuenta de que era necesario un nuevo sistema que ofreciese escalabilidad y administración descentralizada. Este servicio fue introducido en 1984.



Para qué sirve DNS
Sirve para que el usuario cuando no recuerde los IP, en cambio recuerda solamente los nombres lógicos... Ej: www.pymsolutions.com no 212.34.137.93

Es un sistema que ayuda a los usuarios de Internet a utilizar la red de una forma más sencilla.

Como concepto general se puede decir que DNS es una base de datos distribuida.

La estructura de la base de datos de DNS es similar a la estructura de directorios de UNIX. Dicha estructura es como un árbol invertido con la raíz (representada por un punto ".")

Estas direcciones IP son únicas, lo cual quiere decir que cada computador tiene su propia dirección IP y que esta es diferente del resto de direcciones IP existentes.

Que hace DNS

Conversión del nombre común local a la dirección física única de la conexión de red del dispositivo.

· Arquitectura C/S de dos niveles.
El DNS es necesario para nuestras aplicaciones de manera que puedan convertir los nombres que nosotros utilizamos en nombres comprensibles para las máquinas (Direcciones IP) y proveer al usuario final de una forma cómoda de comunicarse.
Sin embargo, el uso de estas direcciones IP es complicado para nosotros, ya que no es fácil recordarlas, por lo que preferimos utilizar nombres con algún significado, a los que estamos acostumbrados en la vida diaria.

Los ordenadores pueden trabajar con números mucho mejor, las personas tratan mejor con nombres. Por tal razón nació un sistema que substituye las direcciones IP de los ordenadores con nombres de direcciones que al usuario le sean claras.

Para ello fue creado un sistema que está organizado de forma jerárquica como el sistema de las direcciones IP. Un nombre de una dirección (domain name) de es este sistema pertenece a un top-level-domain. Cada parte individual de tales direcciones son separadas por puntos como las direcciones IP. Ejemplos de tales direcciones son por ejemplo yahoo.com, mozilla.org o selfhtml.com.ar.

Top-level-domains se encuentran al final del nombre de dominio. Se trata más que todo de abreviaturas correspondientes. Tales abreviaturas son los identificadores de los países o identificadores de tipos. Ejemplos son:
de = Alemania
at = Austria
ch = Suiza
it = Italia
my = Malasia
com = comercial
org = organización
net = red general
edu = escuelas superiores estadounidenses
gov = entidades públicas estadounidenses
mil = entidades militares estadounidenses

Muchas personas dudan que este esquema de direcciones pueda ser eficiente en el futuro. Ya existen ideas para la reestructuración del direccionamiento de redes

y ordenadores hosts.

Actualmente (al momento del cierre de redacción del actual documento) surgen nuevos top-level-domains. Los siguientes están programados:

biz = compañías
pro = grupo de profesiones con prohibición publicitaria (abogados, asesores fiscales, médicos.)
name = personas privadas
info = servicios de información de todo tipo
museum = museos
aero = compañías de aviación, aeropuertos, agencias de viaje etc.
coop = cooperativas, organizaciones, sindicatos

Al momento del cierre de redacción de este documento ya están disponibles info y biz, name han de seguir.

Cada uno de esos top-level-domains representa un cierta administración, para la cual existe una "entidad administrativa" que se encarga de ofrecer los nombres dominios dentro de su campo de administración. Su Ud desea adjudicar un nombre como minombre.de, entonces tiene que reservar el nombre en la DENIC (Deutsches Network Information Center = Centro Alemán de Información de Redes). Proveedores comerciales se encargan de hacer esto por Ud. El nombre deseado lo recibe tan sólo si el nombre aún no ha sido adjudicado por alguna otra persona o entidad. Muchas personas vivas han reservado nombres de firmas para así vendérselas14/3 muy caras cuando decidan tener una representación en internet (en España esto no es posible). Actualmente ya no es posible hacer esto, sin embargo todavía hay casos en que los juzgados tienen que decidir quien recibe un determinado nombre. Esto sucede cuando 2 o más firmas desean reservar el mismo nombre. Al final sólo una de las firmas puede recibir el nombre. Por la escasez de nombres, las direcciones con nombres bien largas se han vuelto muy populares por ejemplo hoy-voy-a-ir-al-cine.

Los propietarios de nombres dominios pueden adjudicar sub-level-domains. Así podemos ver que el propietario del dominio seite.net ha adjudicado sub-dominios como java.seite.net o javascript.seite.net.

COMPONENTES DEL SERVICIO DE NOMBRES DE DOMINIO:

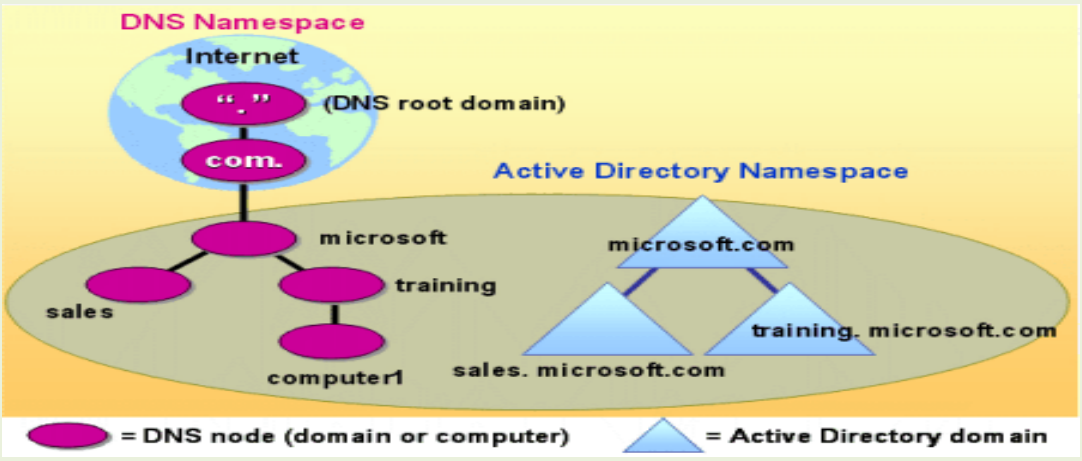
- **Espacios de nombres de dominio (name space)**
- **Bases de datos DNS (registro de recursos)**
- **Servidores de nombres (servidores DNS)**
- **Clientes DNS (resolutores – "resolvers")**
- **Protocolo DNS**

Espacios de nombres de dominio (name space)

En programación, un espacio de nombres (del inglés name space), en su acepción más simple, es un conjunto de nombres en el cual todos los nombres son únicos.

Un espacio de nombres es un contexto en el que un grupo de uno o más identificadores pueden existir. Un identificador definido en un espacio de nombres está asociado con ese espacio de nombres. El mismo identificador puede independientemente ser definido en múltiples espacios de nombres, eso es, el sentido asociado con un identificador definido en un espacio de nombres es independiente del mismo identificador declarado en otro espacio de nombres. Los lenguajes que manejan espacio de nombres especifican las reglas que determinan a qué espacio de nombres pertenece una instancia de un identificador.

En programas grandes o en documentos no es infrecuente tener cientos o miles de identificadores. Los name spaces (O técnicas similares como la emulación de name spaces) disponen de un mecanismo para ocultar los identificadores locales. Proporcionan los medios para agrupar lógicamente los identificadores relacionados en sus correspondientes name spaces, haciendo así el sistema más modular.



Bases de datos DNS (registro de recursos).

Un DNS es una base de datos distribuida que contiene registros que se conocen como RR (Registros de Recursos), relacionados con nombres de dominio. La siguiente información sólo es útil para las personas responsables de la administración de un dominio, dado que el funcionamiento de los servidores de nombre de dominio es completamente transparente para los usuarios.

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.kioskea.net	3600	A	IN	163.5.255.85

- 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:

A: este es un tipo de base que hace coincidir el nombre canónico con la dirección IP. Además, pueden existir varios registros A relacionados con diferentes equipos de la red (servidores).

CNAME (Nombre Canónico): Permite definir un alias para el nombre canónico. Es particularmente útil para suministrar nombres alternativos relacionados con diferentes servicios en el mismo equipo.

HINFO: éste es un campo solamente descriptivo que permite la descripción en particular del hardware del ordenador (CPU) y del sistema operativo (OS). Generalmente se recomienda no completarlo para evitar suministrar información que pueda ser útil a piratas informáticos.

MX (Mail eXchange): es el servidor de correo electrónico. Cuando un usuario envía un correo electrónico a una dirección (user@domain), el servidor de correo saliente interroga al servidor de nombre de dominio con autoridad sobre el dominio para obtener el registro MX. Pueden existir varios registros MX por dominio, para así suministrar una repetición en caso de fallas en el servidor principal de correo electrónico. De este modo, el registro MX permite definir una prioridad con un valor entre 0 y 65,535:

NS: es el servidor de nombres de dominio con autoridad sobre el dominio.

PTR: es un puntero hacia otra parte del espacio de nombres de dominios.

SOA (Start Of Authority (Inicio de autoridad)): el campo SOA permite la descripción del servidor de nombre de dominio con autoridad en la zona, así como la dirección de correo electrónico del contacto técnico (en donde el carácter "@" es reemplazado por un punto).

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.

Servidores de nombres (servidores DNS).

Los equipos llamados servidores de nombres de dominio permiten establecer la relación entre los nombres de dominio y las direcciones IP de los equipos de una red.

Cada dominio cuenta con un servidor de nombre de dominio, llamado servidor de nombre de dominio principal, así como también un servidor de nombre de dominio secundario, que puede encargarse del servidor de nombre de dominio principal en caso de falta de disponibilidad.

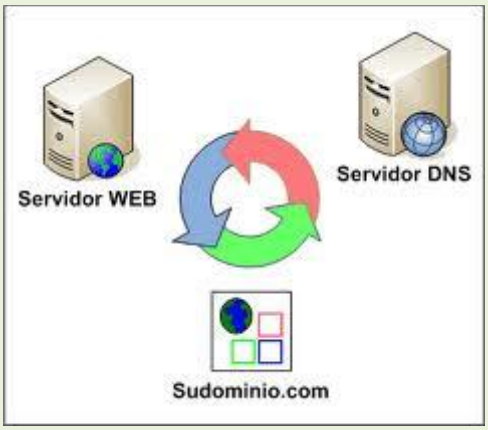
Cada servidor de nombre de dominio está especificado en el servidor de nombre de dominio en el nivel superior inmediato, lo que significa que la autoridad sobre los dominios puede delegarse implícitamente. El sistema de nombre es una arquitectura distribuida, en donde cada entidad es responsable de la administración de su nombre de dominio. Por lo tanto, no existe organización alguna que sea responsable de la administración de todos los nombres de dominio.

Los servidores relacionados con los dominios de nivel superior (TLD) se llaman "servidores de dominio de nivel superior". Son 13, están distribuidos por todo el mundo y sus nombres van desde "a.root-servers.net" hasta "m.root-servers.net".

El servidor de nombre de dominio define una zona, es decir, una recopilación de dominios sobre la cual tiene autoridad. Si bien el sistema de nombres de dominio es transparente para el usuario, se deben tener en cuenta los siguientes puntos:

- Cada equipo debe configurarse con la dirección de un equipo que sea capaz de transformar cualquier nombre en una dirección IP. Este equipo se llama Servidor de nombres de dominio. No se alarme: cuando se conecta a Internet, el proveedor de servicios automáticamente modificará los parámetros de su red para hacer que estos servidores de nombres de dominio estén disponibles.
- También debe definirse la dirección IP de un segundo Servidor de nombres de dominio (Servidor de nombres de dominio secundario): el servidor de nombres de dominio secundario puede encargarse del servidor de nombres de dominio principal en caso de fallas en el sistema.

El servidor que se utiliza con más frecuencia se llama BIND (Berkeley Internet Name Domain). Es un software gratuito para sistemas UNIX, fue desarrollado inicialmente por la Universidad de Berkeley en California y en la actualidad está mantenido por ISC (Internet Systems Consortium).



Clientes DNS (resolutores – “resolvers”)

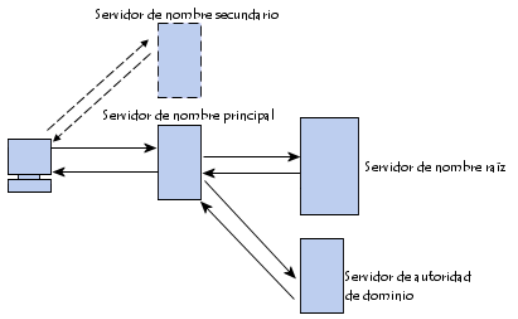
El mecanismo que consiste en encontrar la dirección IP relacionada al nombre de un ordenador se conoce como "resolución del nombre de dominio". La aplicación que permite realizar esta operación (por lo general, integrada en el sistema operativo se llama "resolución".

Cuando una aplicación desea conectarse con un host conocido a través de su nombre de dominio (por ejemplo, "es.kioskea.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 para cómofunciona.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 (en nuestro caso www).



Protocolo DNS.

Este protocolo se utiliza para poder recordar de manera sencilla las direcciones IP. De esta manera surge el concepto de nombres de dominio. Gracias a esto podemos asignar a una dirección IP un nombre, además de que es más fiable porque la dirección IP de un servidor puede cambiar pero el nombre no lo hace. Podemos decir entonces que el DNS es un sistema jerárquico y distribuido que permite traducir nombres de dominio en direcciones IP y viceversa. Otro uso común de este es para los servidores de correo a través del nombre de dominio de correo como por ejemplo “www.Hotmail.com“. Dado un dominio puede leerse de derecha a izquierda por ejemplo “www.google.es” seria “.es” el dominio más alto.

Cada dominio es como si terminase con un “.” Por eso nuestro dominio seria “www.google.es“y el punto al final es el elemento raíz de nuestro árbol y lo que indica al cliente que debe de empezar la búsqueda en los root Server. Estos root Server son los que tienen los registros TLD que son los dominios de nivel superior ósea los que no pertenecen a otro dominio, como son “com, org, net, es, etc.” Actualmente hay 13 TLD en todo el mundo y 10 de ellos se encuentran en estados unidos, uno en Estocolmo, otro en Japón, y el último en Londres. Si alguna catástrofe hiciese que estos 13 servidores dejasen de operar provocaría un gran apagón de Internet y causaría estragos a nivel mundial.

Estos servidores dice que dominios de primer nivel existen y cuáles son sus servidores de nombres recursivamente los servidores de esos dominios dicen que subdominios existen y cuales don sus servidores.

Cada componente de dominio incluyendo la raíz, tiene un servidor primario y varios secundarios. Todos tienen la misma autoridad para responder por ese dominio, pero el primario es el único sobre el que se pueden hacer modificaciones de manera que los secundarios son reaplicas del primario.

Casi todos los servidores de nombres utilizan un software llamado bind que es un software de libre distribución utilizado por la mayoría de sistemas UNIX.

Una herramienta útil que encontramos para probar si un dominio se resuelve correctamente es el domando “nslookup“. Se trata de un cliente DNS que nos sirve para obtener direcciones IP a través del dominio y viceversa.

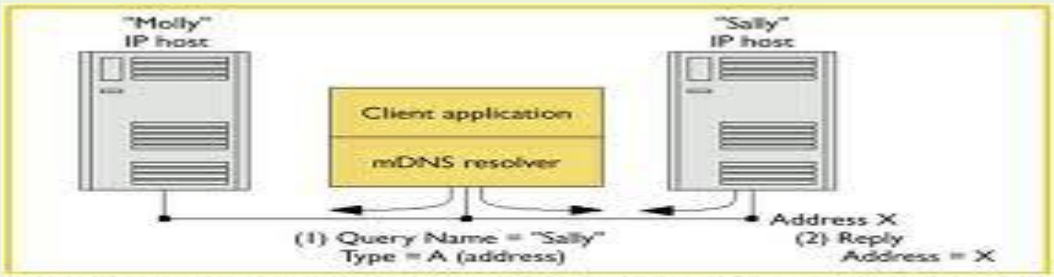


Figure 2. Multicast DNS protocol interaction. The client obtains the IP address for the host named "Sally" by issuing a request to a well-known multicast address and awaiting a reply.

Aplicaciones de DNS Muchas implementaciones de DNS proporcionan tres utilidades bastante comunes para consultar a servidores de nombres:

host Obtiene una dirección IP asociada con un nombre de host o un nombre de host asociado con una dirección IP.

nslookup Permite localizar información acerca de los nodos de red, examinar los contenidos de la base de datos de un servidor de nombres y establecer la accesibilidad a servidores de nombres.

dig Permite probar los servidores de nombres, reunir grandes volúmenes de información de nombres de dominio y ejecutar simples consultas de nombres de dominio.

- ESPACIO DE NOMBRES DE DOMINIO:

- **Nombres de dominio.**
- **Dominio raíz. Dominios y subdominios**
- **Nombres relativos y absolutos. FQDN**
- **Uso de dominios**
- **Administración de nombres de dominio en internet:**
- **Delegación. Dominio raíz. ICANN**
- **Dominios TLD y Operadores de registro**
- **Registros de dominios en Internet. Agentes registradores**

El espacio de nombres de dominio que se especifica en el DNS tiene una estructura de árbol invertido. Cada elemento el árbol (interno u hoja) se etiqueta con un nombre que puede tener hasta 63 caracteres. El comienzo del árbol se denomina raíz del sistema DNS y tiene una etiqueta vacía.

NOMBRES DE DOMINIO.

Un nombre de dominio es una cadena de caracteres alfanuméricos, que cumple un formato y normas establecidos, en la que se traduce una dirección IP de una máquina.
Los nombres de dominio constituyen la clave para el funcionamiento de Internet. Desde el punto de vista técnico, a la vez que identifican los equipos conectados a la red ya que resuelven las direcciones IP, permiten su fácil localización y hacen amigable el uso de Internet.
Precisamente esta amigabilidad ha potenciado el crecimiento de Internet en todo el mundo y por tanto, ha contribuido a que Internet se haya constituido en una herramienta para el desarrollo económico, social y cultural de los pueblos.
Desde el punto de vista comercial, los nombres de dominio, como marca, sirven para identificar todo tipo de entidades como Organismos, Empresas, personas físicas... junto con los servicios que prestan.

DOMINIO RAÍZ. DOMINIOS Y SUBDOMINIOS.
El dominio raíz es la parte superior del árbol, que representa un nivel sin nombre; a veces se muestra como dos comillas vacías (“”), que indican un valor nulo. Cuando se utiliza un nombre de dominio DNS, empieza con un punto (.) para designar que el nombre se encuentre en la raíz o en el nivel más alto de la

jerarquía del dominio. En este caso, el nombre de dominio DNS se considera completo e indica una ubicación exacta en el árbol de nombres. Los nombres indicados de esta forma se llaman nombres de dominio completos (FQDN, Fully Qualified Domanin Names).

Dominios son un nombre de dos o tres letras que se utilizan para indicar un país o región, o el tipo de organización usa un nombre. Por ejemplo ".com", que indica un nombre registrado para usos comerciales o empresariales en internet.

Subdominios son nombres adicionales que pueden crear una organización y se derivan del nombre de dominio registrado de segundo nivel. Incluyen los nombres agregados para desarrollar el árbol de nombres de DNS en una organización y que la dividen en departamentos o ubicaciones geográficas.

NOMBRES RELATIVOS Y ABSOLUTOS. FQDN.
Los nombres de dominio absolutos terminan con "."(ej. "univalle.edu.co.") y los relativos no, necesitando saber el contexto del dominio superior para determinar de manera única su significado verdadero.

Los nombres relativos son nombres que completan su nombre en función del dominio del cual están registrados. Por ejemplo en el dominio uv.es, la máquina con el nombre relativo "glup.irobot", tomará como nombre absoluto "glup.irobot.uv.es".

Por tanto, el nombre absoluto no requiere de ninguna referencia a un dominio, dado que es un nombre completo. Para indicar que un nombre absoluto, terminará su nombre con ".", en caso contrario, al nombre relativo que termina sin "." Se le añade la coletilla del dominio.
Esta distinción es importante y hay que tenerla en cuenta al configurar los registros del DNS, dado que si algún registro por descuido es dejado si ".", el DNS añadirá su dominio. Por ejemplo, en el caso de tener un registro con valor "glup.uv.es" si "." En el valor de un registro, el DNS cuando consulte dicho registro devolverá "glup.uv.es.uv.es".

Un **nombre de dominio completo** (**FQDN**), a veces conocido como un *nombre de dominio absoluto* , es un nombre de dominio que especifica su ubicación exacta en la jerarquía del árbol del sistema de nombres de dominio (DNS). En él se especifica todos los niveles de dominio, incluyendo el dominio de nivel superior y el dominio raíz. Un nombre de dominio completo se caracteriza por su ambigüedad, ya que sólo se puede interpretar de una manera.

Por ejemplo, dado un dispositivo con un nombre de host local *myhost* y un nombre de dominio primario *example.com*, el nombre de dominio completo es *myhost.example.com.* El nombre de dominio completo por lo tanto, identifica de forma exclusiva el dispositivo, si bien puede haber muchas máquinas en el mundo llamado *myhost*, sólo puede haber un *myhost.example.com* . En el sistema

de nombres de dominio, y sobre todo, en el DNS los archivos de zona , un nombre de dominio completo se especifica con un final de puntos. Por ejemplo,

somehost.example.com. especifica un nombre de dominio absoluto que termina con una etiqueta vacía dominio de nivel superior.

El dominio raíz del DNS no tiene nombre, que se expresa en una etiqueta vacía, lo que resulta en un nombre de dominio termina con el separador de punto. Sin embargo, muchos de resolución de DNS proceso de un nombre de dominio que contiene un punto en cualquier posición de ser completo, o añadir el punto final necesario para la raíz del árbol de DNS. Resolución de proceso de un nombre de dominio, sin un punto como incondicional y añadir automáticamente el nombre del sistema por defecto de dominio y el punto final.

USO DE DOMINIOS

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 (a través de mecanismos como SPF).

ADMINISTRACIÓN DE NOMBRES DE DOMINIO EN INTERNET:

El sistema de nombres de dominio está coordinado por la Internet Corporation for Assigned Names and Numbers (ICANN). 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.)."

DELEGACIÓN. DOMINIO RAÍZ. ICANN.

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.

Una característica del espacio de nombres de dominio es que se realiza una gestión independiente de cada dominio, pues bien, esta gestión independiente está relacionada con lo que se denomina proceso de delegación. El proceso de delegación es por el cual el gestor de un determinado dominio delega la tarea de gestión, incluyendo el mantenimiento de servidores DNS, de un dominio hijo en una entidad determinada, habitualmente el propietario del dominio. Esto permite que el domino que hace la delegación (dominio padre) se vea liberado de parte de las tareas que, de otra forma, le corresponderían.
ICANN, delega la gestión de ccTLC .es a la empresa pública Red.ES , eso significa que ICANN ya no se encargará de gestionar el alta y baja de dominios bajo .es y que, por lo tanto, los servidores DNS asociados a la raíz (servidores raíz), lo único que sabrán del dominio .es son las direcciones IP de los servidores DNS que Red.ES haya configurado. A cambio, Red.ES tendrá que configurar y mantener funcionando un grupo de servidores de nombres que conozcan más datos de dominio .es. Este proceso se puede repetir varias veces, como de hecho suele ocurrir. Una vez que ICANN ha delegado el dominio .es, Red.ES deberá gestionar el alta del dominio "mi-empresa.sa.es" y de hecho lo hace. Sin embargo, Red.ES cuando crea el dominio "mi-empresa-sa.es" inmediatamente lo delega a "Mi empresa SA" para que, de esta forma sea la propia empresa la que dé de alta, por ejemplo "www.mi-empresa-sa.es"y , más importante, para que sea la empresa (y no Red.ES) la que configure y mantenga los servidores DNS del dominio de segundo nivel. El único dato que suministrarán los servidores DNS de Red.ES sobre el dominio "mi-empresa-sa.es" es la lista de los servidores DNS del dominio de segundo nivel (mi.empresa.sa.es). Por lo tanto, debido al proceso de delegación, la mayor parte de la información que suministrarán los servidores DNS raíz y los servidores DNS de los que TLD será únicamente un "puntero" a los servidores DNS del dominio que estamos buscando.

DOMINIO TLD Y OPERADORES DE REGISTRO

La extensión a la extrema derecha en un nombre de dominio (como .com o .net) es denominada dominio de primer nivel, o TLD (Top-Level Domain).

Hay más de 270 dominios de primer nivel de varios tipos:

Los TLDs genéricos no patrocinados (gTLDs), o dominios internacionales, son .com, .net, .org, .int, .arpa, .biz, .info, .name y .pro. Los TLDs no patrocinados operan sin cualquier organización patrocinadora y frecuentemente tienen menos restricciones para el registro que los TLDs patrocinados.

Los TLDs genéricos patrocinados (gTLDs) incluyen a .edu, .gov, .mil, .aero, .cooper, .museum, .jobs, .mobi, .travel, .tel, .cat, y .asia. Un TLD patrocinado es un dominio especializado que tiene un patrocinador que representa la comunidad a la cual sirve el TLD.

Los TLDs de dos letras (.br, .ar, .mx, .uk, .de, etc.) corresponden a las abreviaturas oficiales de más de 250 países y territorios. Estos dominios son denominados TLDs con códigos de países o ccTLDs, en forma abreviada. Cada uno posee un operador de registro designado, que opera el ccTLD según las políticas locales (por ejemplo, para registrar un nombre en algunos ccTLDs, hay que ser residente local).

El registro de los dominios internacionales .com y .net es un proceso sencillo y objetivo y puede ser realizado por cualquier persona, entidad o empresa, y no exige ningún tipo de documentación específica. Se trata de dominios bien conocidos y utilizados a nivel mundial que proporcionan visibilidad y credibilidad, además de garantizar la identidad de su negocio en Internet.

¿Cuál es el operador de registro (registry) de los TLD .com, .net, .es?

Acreditación VeriSign.

Verisignes la autoridad competente para la gestión de los dominios en Internet de .com, .net, .cc y .tv.
Las principales funciones de Verisign incluyen las relacionadas con la tramitación de solicitudes y asignación de dominios de acuerdo con la normativa correspondiente,
así como la realización de las funciones técnicas necesarias para garantizar el correcto funcionamiento del sistema de dominios .com, .net, .cc y .tv en la red global de Internet.

Acreditación ESNIC

ESNIC es la autoridad competente para la gestión del registro de dominios de Internet bajo el código de país.

Las principales funciones de ESNIC incluyen las relacionadas con la tramitación de solicitudes y asignación de dominios de acuerdo con la normativa correspondiente,
así como la realización de las funciones técnicas necesarias para garantizar el correcto funcionamiento del sistema de dominios bajo .es en España y en la red global de Internet.

REGISTRO DE DOMINIOS EN INTERNET. AGENTES REGISTRADORES

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.

El procedimiento es el siguiente:

1. Elegir un dominio.
2. Verificar la disponibilidad del nombre de dominio deseado en algún registrador.
3. Ingresar los datos personales.
4. Elegir la cantidad de tiempo que el dominio permanecerá registrado.
5. Pagar el dominio, normalmente con tarjeta de crédito (o también por transferencia bancaria)
6. Una vez comprado, el ahora dueño del dominio (registrante) debe configurarlo con la URL a la cual redireccionar,IP del servidor al que encontrará mediante la DNS, servidor DNS usada por este.
7. El dueño del dominio debe esperar un tiempo para que el dominio sea reconocido en todos los servidores de Internet. Para los dominios .com y .net la demora es entre 4 y 8 horas, y para otros es generalmente entre 24 y 48 horas. En ese período:
8. El registrador contacta con ICANN y realiza el proceso de forma transparente para el registrante.
9. Se avisa al registrante que el dominio fue registrado.
10. 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). Como cada uno tiene distintos tiempos de actualización y parámetros de caché distintos, pasan varias horas hasta que todos los servidores DNS del mundo conocen cómo hacer la resolución del dominio.

11. La página ya es accesible mediante un nombre de dominio desde cualquier computadora.

Los datos necesarios para registrar un dominio son:

- Registrador oficial de dominios: Empresa registradora oficial inscrita en ICANN la cual se encarga de preservar los datos de los registros.

- Propietario del dominio: Persona o entidad que figura como propietario y legítimo dueño por el periodo de registro.

- Contacto administrativo: Persona o entidad designada por el propietario que figura como administrador de los datos del dominio en favor del propietario.

- Contacto técnico: Persona o entidad que se encarga de la manutención de los números DNS del dominio para su correcto funcionamiento y enlace en la red.

- Contacto de facturación: Persona o entidad que se encargará de realizar el pago por las correspondientes renovaciones del dominio.

- DNS (**Domain Name Servers**) (**Servidor de Nombres de Dominio**): Estos números (mínimo 2) figuran en el registro de los dominios y muestran las direcciones IPs de los servidores que se harán cargo de las peticiones al dominio y de redirigir las mismas a donde proceda según la naturaleza de cada petición.

Los Agentes Registradores son entidades acreditadas por red.es que actúan en cualquier trámite relacionado con el registro de dominios ".es", con la finalidad de asesorar a los usuarios finales, agilizar la tramitación y ofrecerles una serie de servicios adicionales, tales como correo electrónico, servicios Web, alojamiento de páginas personales, registro de patentes y marcas, etc…

- 1&1
- 1API
- 123 DOMAIN.EU
- ABANSYS
- ACENS
- ACTIVE 24
- ARGORED
- ARRAKIS
- ARSYS
- ASCIO
- AVANZAS
- AXARnet
- BB ONLINE
- CDMON
- CENTRORED
- CHIVALGES
- CLARKE, MODET & CO.

- COMALIS
- COMVIVE
- CONFIGBOX
- CORE Internet Council of Registrars
- CPS-DATENSYSTEME
- CSC Corporate Domains, Inc.
- DIGITAL VALUE
- DIGIVAL
- DINAHOSTING
- DOCUMENTDATA ANSTALT
- DOMAINCLUB
- DOMAININFO
- DOMAIN PROTECT
- DOMENESHOP
- DOMESTIKA
- EASYNET
- ELZABURU

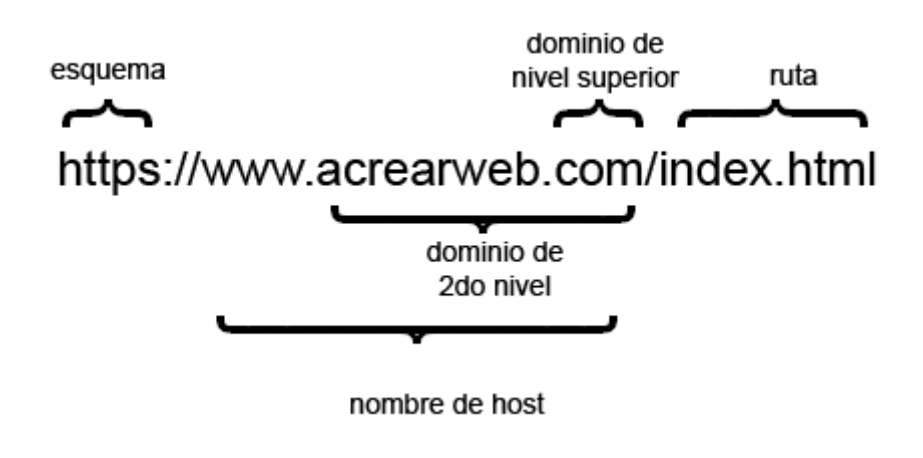
- ENTORNO DIGITAL
- EPAG Domainservices
- EURODNS
- GANDI SAS
- GRAVITYNET
- HERRERO Y ASOCIADOS
- HOSPEDAJE Y DOMINIOS
- HOSTINET
- IBERCOM
- IDECNET
- IGARCOM
- IMPRESIONES WEB
- INDOM
- INFORTELECOM
- INSTRA CORPORATION
- INTERDOMAIN
- INTERDOMINIOS
- INTERNET NAMES
- INTERNETWORX
- INTERNETX
- IP MIRROR PTE. LTD.
- IS-FUN
- J.ISERN PATENTES Y MARCAS
- KEY SYSTEMS
- MAILCLUB
- MARCARIA
- MARKMONITOR
- MESHDIGITAL

- NAMEBAY
- NAMESHIELD
- NameWeb BVBA
- NEODIGIT
- NEMETIC

- NERION NETWORKS
- NETIM
- NEXICA
- NOMINALIA
- NOM-IQ LTD
- OPENPROVIDER
- OVH
- PDR
- PIENSA SOLUTIONS
- PLANETDOMAIN
- PONS PATENTES Y MARCAS
- RECOL
- REDCORUNA
- REALTIME REGISTER
- REGISTER.ES
- SAFENAMES LTD
- SANE SYSTEMS
- SARENET
- SCIP
- SERDATA
- SERVEISWEB
- STRATO
- SIOSI
- SOGITECK
- SYNC
- TUCOWS
- TU DOMINIO
- UBILIBET
- UNITED DOMAINS
- VARIOMEDIA
- VIRTUALPYME
- WEBFUSION
- WEIS

SERVIDORES DE NOMBRES DE DOMINIO (DNS):

- **Zonas. Autoridad. Registro de recursos (RR)**
  Autoridad del Dominio



Un ***dominio*** de Internet es una red de identificación asociada a un grupo de dispositivos o equipos conectados a la red Internet.

El propósito principal de los nombres de dominio en Internet y del sistema de nombres de dominio (DNS), es traducir las direcciones IP de cada nodo activo en la red, a términos memorizables y fáciles de encontrar. Esta abstracción hace posible que cualquier servicio (de red) pueda moverse de un lugar geográfico a otro en la red Internet, aun cuando el cambio implique que tendrá una dirección IP diferente.

Es importante no confundir el URL y el nombre de dominio; el siguiente ejemplo ilustra la diferencia entre una URL (Uniform Resource Locator) y un nombre de dominio:

URL: http://www.example.net/index.html
Nombre de dominio: *www.example.net*
Nombre de dominio registrado: *example.net*

Por otro lado, la ***autoridad de dominio*** se refiere al cálculo de la autoridad de un sitio con respecto a otros, es decir, la autoridad del dominio es lo que determina que, dados dos sitios, por ejemplo, de igual contenido semántico y de igual relevancia a la búsqueda del usuario, el dominio que tenga mayor autoridad es el que saldrá mejor posicionado.

Para calcular la autoridad de un sitio se toman en consideración muchas otras variables aparte de la cantidad de enlaces que la página pueda tener.
De modo que dominar estos aspectos del posicionamiento web, y como Google elabora sus páginas de resultado, nos ayudará a dirigir de forma más eficiente nuestros esfuerzos para alcanzar mejores rankings.

Registro de Recursos (RR) (1/3)

Cada entrada en la tabla de un DNS contiene información, no sólo de las direcciones IP, sino de un registro de recursos, con 5 campos o tuplas

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

Cuando un cliente (a través de un *resolver*) pregunta por un nombre de dominio al DNS, lo que recibe son los RR asociados a ese nombre y por tanto la función real del DNS es relacionar los dominios de nombres con los RR

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

shackleton.uv.es 600 IN A 147.156.167.210

Nombre_dominio: puede haber más de un registro por dominio. Este campo a veces puede omitirse, tomando por defecto el último nombre de domino indicado con anterioridad.

TTL: tiempo de vida. Indicando la estabilidad del registro (tiempo que se guarda en la caché).

La información altamente estable tiene un valor grande (86400 seg. = 1 día)

La información volátil recibe un valor pequeño (60 seg.)

Clase: Actualmente sólo se utiliza *IN*, para información de Internet. Este campo si se omite, se toma el último valor indicado con anterioridad

Dato_Registro(Valor) es un número o texto ASCII dependiendo del tipo de registro.

Normalmente existen varios RR por dominio

Indica el tipo de registro. Los más utilizados son:

Tipo de Registro	*Descripción*
SOA *Start Of Authority*	Inicio de autoridad, identificando el dominio o la zona. Fija una serie de parámetros para esta zona.
NS *Name Server*	El nombre de dominio se hace corresponder con el nombre de una computador a de confianza para el dominio o servidor de nombres.
A *Address*	Dirección IP de un host en 32 bits. Si este tiene varias direcciones IP, multihomed, habrá un registro diferente por cada una de ellas.
CNAME	Es un alias que se corresponde con el nombre canónico verdadero.
MX	Se trata de un intercambiador de c orreo (Mail eXchanger), es decir, un dominio dispuesto a aceptar solo correo electrónico.
TXT	Texto, es una forma de añadir comentarios a la Base de Datos. Por Ej., para dar la dirección postal del dominio.
PTR	Apuntador, hace corresponder una dirección IP con el nombre de un sistema. Usado en archivos dirección -nombre, la inversa del tipo A.
HINFO	Información del Host, tipo y modelo de computadora y SO
WKS	Servicios públicos (Well -Known Services). Puede listar los servicios de las aplicaciones disponibles en el ordenador.

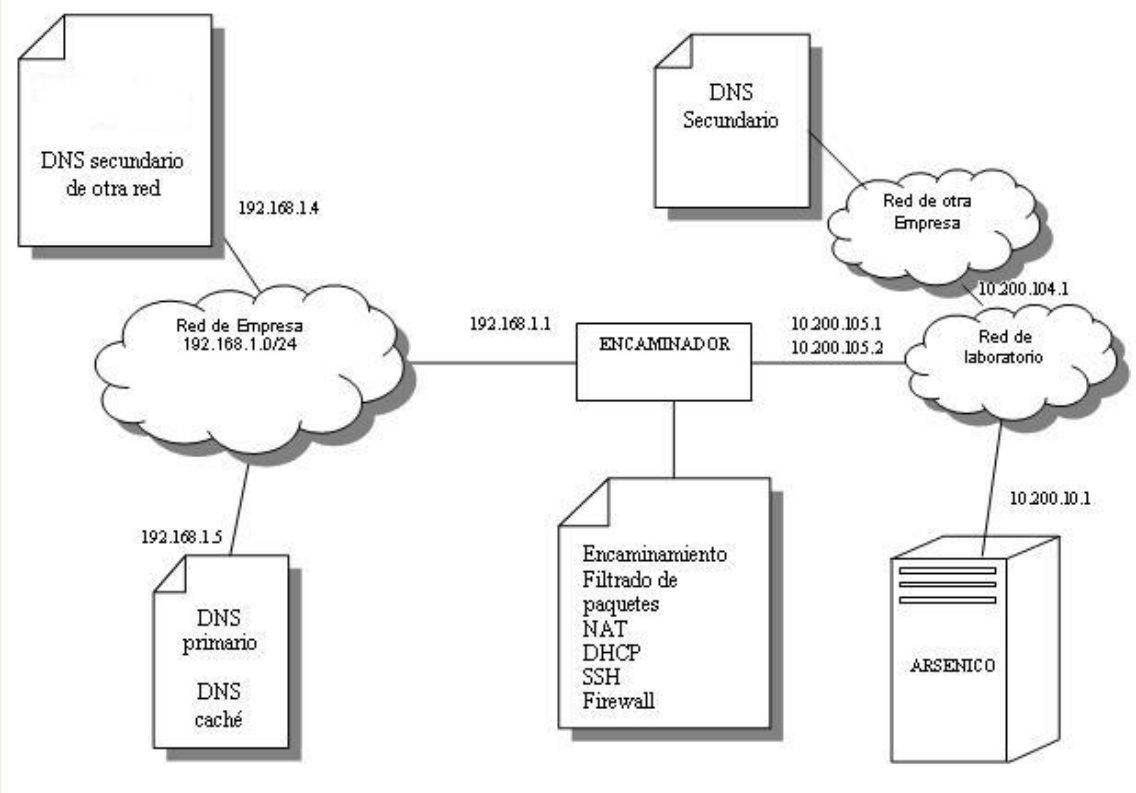
Después de crear una zona, es necesario agregarle registros de recursos adicionales. Los registros de recursos (RR) más comunes para agregar son:

- *Host (A)* para asignar un nombre de dominio DNS a una dirección IP que utiliza un equipo.
- *Alias (CNAME)* para asignar un nombre de dominio DNS con alias a otro nombre canónico o principal.
- *Agente de intercambio de correo (MX)* para asignar un nombre de dominio DNS al nombre de un equipo que intercambia o reenvía el correo.
- *Puntero (PTR)* para asignar un nombre de dominio DNS inverso basado en la dirección IP de un equipo que señala al nombre de dominio DNS directo de ese equipo.
- *Ubicación de servicios (SRV)* para asignar un nombre de dominio DNS a una lista especificada de equipos host de DNS que ofrecen un tipo específico de servicio, como los controladores de dominio de Active Directory.

○ Tipos de servidores de nombres DNS

- **Servidor maestro o primario**
- **Servidor esclavo o secundario**
- **Servidor caché**
- **Servidor reenviador (forwarding)**
- **Servidor solo autorizado**

TIPOS DE SERVIDORES DNS



Servidores DNS primarios o maestros (primary name servers)

Estos servidores **tienen autoridad sobre una zona** y **responden con autoridad** a preguntas relacionas sobre FQDNs dentro de esa zona.

"Tener autoridad sobre una zona" significa básicamente que son los encargados de guardar y proporcionar la "información oficial" sobre esa zona. Dicha información se almacena en un archivo alojado en su disco duro local denominado **archivo de zona**.

El archivo de zona contiene, a su vez, lo que se denomina **registros de recursos**: cada registro asocia una IP con un nombre de dominio. En estos servidores, el archivo de zona se actualiza **generalmente de forma manual**.

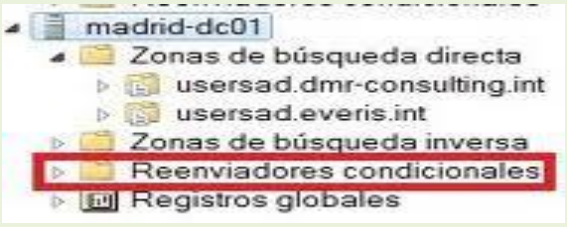
Servidores DNS secundarios o esclavos (secondary name servers)

Un servidor de nombres secundario tiene autoridad sobre una zona, pero obtiene la información de esa zona copiandola de un servidor primario utilizando un proceso llamado **transferencia de zona**. Para permanecer sincronizado, los servidores de nombres secundarios consultan a los primarios regularmente (típicamente cada tres horas) y ejecutan la transferencia de zona si el primario ha sido actualizado.

Servidores DNS caché (caching-only servers)

Los servidores DNS caché no tienen autoridad sobre ninguna zona: se limitan a contactar con otros servidores para resolver las peticiones que les llegan. Los servidores caché mantienen una **memoria caché** con las últimas preguntas contestadas. Cada vez que un cliente DNS le formula una pregunta, primero consulta en su memoria caché. Si encuentra la dirección IP solicitada, se la devuelve al cliente; si no, consulta a otros servidores, apunta la respuesta en su memoria caché y le comunica la respuesta al cliente.

Servidores reenviadores (forwarding)



Un reenviador es un servidor de Sistema de nombres de dominio (DNS) de una red que se utiliza para reenviar consultas DNS para nombres DNS externos a servidores DNS que se encuentran fuera de la red interna. También dependiendo de el propósito del servicio se pueden hacer redirecciones condicionales, dependiendo del nombre de dominio solicitado.
Los reenviadores se conocen de tal manera cuando se encarga de recibir consultas de otros servidores DNS que no pueden resolver ellos mismos.
Un servidor DNS de una red se designa como reenviador haciendo que los demás servidores DNS de la red le reenvíen las consultas que no pueden resolver localmente.
Con un reenviador se pueden solucionar nombres de dominio de fuera de la red como nombres en Internet así mejorando la resolución de nombres para los equipos en la red.

Reenviadores condicionales

Un reenviador condicional es un servidor DNS de una red que se utiliza para reenviar consultas DNS de acuerdo con el nombre de dominio DNS de la consulta. Por ejemplo, se puede configurar un servidor DNS de modo que reenvíe todas las consultas que reciba para los nombres que terminen con widgets.ejemplo.com a la dirección IP de un servidor DNS específico o a las direcciones IP de varios servidores DNS.

SERVIDOR AUTORIZADO

Un servidor DNS puede estar autorizado o no para el espacio de nombres de la consulta. Esta *autorizado* quiere decir que un servidor DNS aloja una copia principal o secundaria de una zona DNS. Si el servidor DNS está autorizado para el espacio de nombres de la consulta, el servidor DNS realizará una de las acciones siguientes:

Comprobar la caché, comprobar la zona y devolver la dirección IP solicitada.
Devolver un número de autorización.

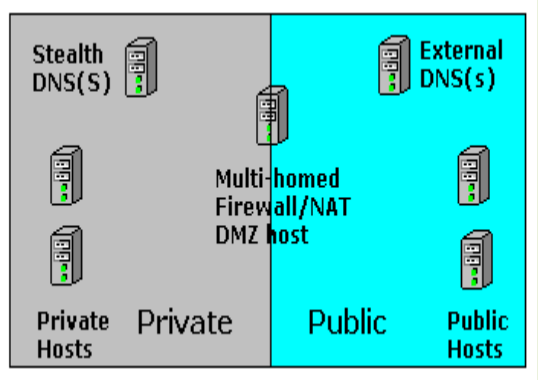
Servidor de nombre stealth / DMZ / SPLIT

Un servidor stealth está definido como el servidor de nombres que no aparece in ningún lugar publicamente visible para el dominio. Brevemente puede ser definido con las siguientes características:

1. Se necesita un DNS público para los servicios que deben tener contacto con el exterior (e-mail, etcétera)
2. La organización encargada del DNS no requiere que el mundo exterior pueda observar alguno de los servidores internos, ni por consultas ni por transferencia de zona ya que compromete el servicio de DNS.

La configuración de Stealth se puede observar a continuación:

Split (Stealth) Server configuration



Software comercial de servidores DNS

Simple DNS Plus Es un servidor de DNS y DHCP de fácil uso. Puedes usar el programa para hacer funcionar correctamente tu propio servidor DNS Internet/Intranet aún sin tener tu propio dominio registrado. Además mejora la velocidad del acceso a Internet. Simple DNS Plus simplifica la configuración de un servidor de DNS y la configuración TCP/IP de tu red, y le da a los ordenadores de tu red nombre reales en vez de los difíciles números de la dirección IP de cada uno de ellos. Por ejemplo, puedes llamar tu servidor de correo electrónico "mail", tu servidor proxy "proxy", y tu servidor Web de tu Intranet "Web"; evitándote tener que escribir las direcciones IP completas de cada uno de ellos. Además puedes hacer funcionar múltiples servidores DNS en la misma máquina, y el programa soporta transferencia de zonas y notificación de zona actualizada. El programa se aloja en la bandeja del sistema de Windows.

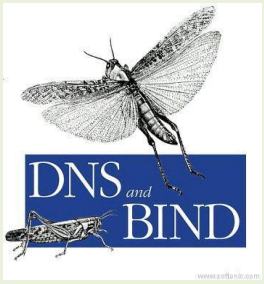
OPENDNS

Porque es **más rápido** y posee funciones de **protección** (anti-phishing y otros).

Características:

- Generalmente **más rápido** que nuestro proveedor de acceso a Internet (estos poseen enormes servidores, con un caché DNS importante)
- Más **fiable** (OpenDNS es muy fiable y sus servidores tienen una disponibilidad del 100%)
- **Autocorrección** de pequeños errores al teclear (google.cmo → google.com)
- Proposición automática (Motor de búsqueda) si el dominio no existe.
- **Protección anti-phishing** (OpenDNS está conectado directamente a PhishTank.com)
- El servicio es **gratuito**
- No hay necesidad de instalar ningún programa (sólo la dirección del DNS por configurar)
- Cuando queremos podemos dejar de utilizar OpenDNS.

BIND



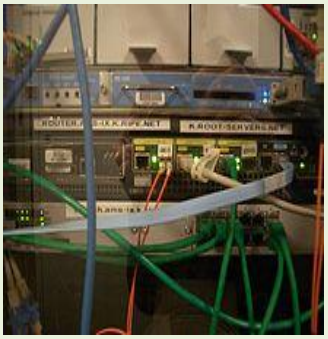
BIND (Berkeley Internet Domain, anteriormente: Berkeley Internet Name Daemon) es el servidor de DNS más comúnmente usado enInternet, especialmente en sistemas Unix, en los cuales es un Estándar de facto. Es patrocinado por la Internet Systems consortium. BIND fue creado originalmente por cuatro estudiantes de grado en la University of California Berkeley y liberado **por primera vez en el 4.3 BSD.**

D*UAL DHCP DNS SERVER*

Dual DHCP DNS Server es a la vez un servidor DHCP para asignar/renovar las direcciones de host, mientras que el servidor DNS intenta resolverlas primer desde los nombres asignados DHCP, luego desde la caché y, como último recurso, intentaría resolverla desde un servidor DNS externo.

Brinda soporte para un modo DHCP estático e Ips estáticas, DNS dinámicas actualizadas de forma automática desde el servidor DHCP, y ofrece la posibilidad de funcionar y cooperar con otros servidores DHCP.

Servidor Raíz



Un **servidor raíz** (*root server* en inglés) es el servidor **de nombre de dominio (DNS)**que sabe dónde están los servidores de nombres autoritarios para cada una de las zonas de más alto nivel en Internet.

Funcionamiento

Dada una consulta de cualquier dominio, el servidor raíz proporciona al menos el nombre y la dirección del servidor autorizado de la zona de más alto nivel para el dominio buscado. De manera que el servidor del dominio proporcionará una lista de los servidores autorizados para la zona de segundo nivel, hasta obtener una respuesta razonable.

Internet

Existen 13 servidores raíz en toda Internet, cuyos nombres son de la forma *letra.root-servers.org*, aunque siete de ellos no son realmente servidores únicos, sino que representan múltiples servidores distribuidos a lo largo del globo terráqueo (ver tabla siguiente). Estos servidores reciben miles de consultas por segundo, y a pesar de esta carga la resolución de nombres trabaja con bastante eficiencia.

El Servidor Raíz de ICANN

Inicial		Empresa	Lugar	IPv4	IPv6
A		VeriSign	distribuido (anycast)	198.41.0.4	2001:503:ba3e::2:30
B	ns1.isi.edu	USC-ISI	Marina Del Rey, California, EEUU	192.228.79.201	2001:478:65::53
C	c.psi.net	Cogent Communications	distribuido (anycast)	192.33.4.12	
D	terp.umd.edu	University of Maryland	College Park, Maryland, EEUU	128.8.10.90	
E	ns.nasa.gov	NASA	Mountain View, California, EEUU	192.203.230.10	
F	ns.isc.org	ISC	distribuido (anycast)	192.5.5.241	2001:500:2f::f
G	ns.nic.ddn.mil	U.S. DoD NIC	distribuido (anycast)	192.112.36.4	
H	aos.arl.army.mil	U.S. Army Research Lab	Aberdeen Proving Ground, Maryland, EEUU	128.63.2.53	2001:500:1::803f:235
I	nic.nordu.net	Autonómica	distribuido (anycast)	192.36.148.17	2001:7fe::53
J		VeriSign	distribuido (anycast)	192.58.128.30	2001:503:c27::2:30
K		RIPE NCC	distribuido (anycast)	193.0.14.129	2001:7fd::1
L		ICANN	distribuido (anycast)	199.7.83.42	2001:500:3::42
M		WIDE	distribuido (anycast)	202.12.27.33	2001:dc3::35

- CLIENTES DNS (Resolutores – "resolvers" de nombres)

Los autores del estándar de DNS (RFCs 1034, 1035 y muchos posteriores) lo describen basándolo en un modelo de diseño que sigue el Berkeley Name Daemon (BIND); este modelo incluye la noción de que todos los servidores en realidad son básicamente el mismo tipo de código, e incluye la notación para ficheros de datos de zona que usa BIND. Desafortunadamente el diseño de BIND tal como lo presentan los RFCs adolece de una indeseable complejidad, y ha producido algunos contratiempos de seguridad; el diseño de djbdns está basado en un modelo de diseño mucho más simple, que vamos a describir. También, y por desgracia, esto ha producido un problema de terminología: existen varias funciones que puede desempeñar un servidor de DNS, y que no se distinguen claramente en la terminología DNS tradicional, porque BIND las lleva a cabo todas a la vez; según están separadas en djbdns, es importante darles nombres bien definidos.

Llamaremos bilioteca resolutora a la biblioteca de rutinas que un programa cliente utiliza para realizar una búsqueda; llamaremos al demonio de apoyo al que ésta envía la petición un resolutor recursivo, y llamaremos a la autoridad última que son la fuente final de la información servidores de nombres autorizados.

Esto lamentablemente lleva a más explicaciones: pero tenga en cuenta que aunque sean más detallados, hacen dos tareas: primero, describen con precisión las tareas que se están realizando; y segundo, son razonablemente consistentes con el uso tradicional.

Cuando una estación desea establecer una conexión con una dirección DNS, llama a la rutina del sistema o resolvedor que primero comprueba si puede obtener la dirección IP a través de una tabla local o almacenada de forma temporal de una consulta anterior. Si no la encuentra enes atable, envía un mensaje con el protocolo UDP a la dirección del servidor DNS que tenga condifutado por defecto, que normalmente es el más próximo. Este servidor consulta primero en sus registros de recursos de zona la dirección solicitada y devuelve la dirección IP si la encuentra. Si no la encuentra ahí, consusltará entonces la table local donde están almacenadas temporalmente consultas anteriores. En caso de que tampoco la encuentre ahí, puede consultar otros servidores DNS, operación que se denomina consulta recursiva. Finalmente el resolvedor devuelve la dirección IP solicitada a la estación o hosts.

- PROCESO DE RESOLUCIÓN DE UN NOMBRE DE DOMINIO

- **Consultas recursivas**
- **Consultas iterativas**
- **Caché y TTL**

- **Recursividad y caché**

Proceso de resolución de un nombre de dominio

El **resolver** o **cliente DNS** es la parte del sistema operativo encargada de resolver nombres de dominio cuando otros clientes (clientes web, clientes de correo, herramientas de red, etc.) así se lo solicitan.

La **resolución de un nombre de dominio** es la traducción de un FQDN a su correspondiente dirección IP.

Proceso

El proceso de resolución sería el siguiente:

1. En un programa del equipo local el usuario utiliza un **nombre de dominio** totalmente cualificado (FQDN).
2. A continuación, el programa solicita al **resolver** la resolución de ese nombre. Su modo de actuación depende del sistema operativo:

GNU/Linux:

1º El resolver compara el nombre solicitado con el del propio host. Si es el mismo, el nombre queda resuelto a la IP local. Para ello utiliza la información que encuentra en el archivo /etc/hostname (que le informa del nombre de máquina local) y la concatena con la indicada en la directiva **domain** del archivo /etc/resolv.conf si la hubiera.

2º En caso de no haber resuelto el nombre, el resolver consulta los datos del archivo /etc/hosts. Se trata de un archivo de texto que contiene por cada línea una **dirección IP** y su correspondiente **nombre de dominio** separados por un espacio o más (las líneas que empiezan con el carácter 'almohadilla' son comentarios y no son tenidas en cuenta). Si el resolver encuentra aquí la respuesta a su consulta detiene el proceso.

3º En caso contrario, el resolver comprueba que en la **caché** del resolver no está la respuesta a la consulta en cuestión. Si está presente en ella, el resolver ofrece este dato a la aplicación que lo solicitó y termina el proceso.

4º Finalmente, si aún no se ha resuelto el nombre, el resolver procede a consultar al primer **servidor DNS** que figure en el archivo /etc/resolv.conf.

Windows:

1º El resolver compara el nombre solicitado con el del propio host. Si es el mismo, el nombre queda resuelto a la IP local.

2º Se carga en la **caché del resolver** el contenido del archivo hosts. Este archivo de Windows es un archivo de texto idéntico al utilizado por GNU/Linux.

3º Se intenta resolver el nombre utilizando la **caché del resolver** (que, aparte del contenido del archivo host, incluirá también las respuestas a consultas DNS realizadas anteriormente). Si la consulta no coincide con una entrada de la caché, el proceso de resolución continúa.

4º El resolver consultará al **servidor DNS preferido** (establecido de manera gráfica por el usuario) tal y como se especifica a continuación.

5º Cuando el servidor DNS recibe la consulta del resolver, primero comprueba su **archivo de zona** (en caso de que lo tenga). Si el nombre consultado coincide con algún registro de su archivo de zona, el servidor DNS **responde al resolver con autoridad**.

6º Si no existe ninguna información en la zona para el nombre consultado, a continuación el servidor comprueba si puede resolver el nombre mediante la información almacenada en su **caché local** (que contendrá resultados de consultas anteriores). Si aquí se encuentra una coincidencia, el servidor responde con esta información. Si aun no se ha conseguido una respuesta a la consulta, lo más normal es que el servidor DNS siga intentando por todos los medios resolverla, bien preguntando a otros servidores DNS que tenga configurados (denominados **forwarders**) o bien preguntando directamente a los **servidores raiz**.

7º Finalmente, cuando el servidor DNS obtiene por uno de los dos medios la respuesta la envía al resolver. La respuesta se almacena tanto en la **caché del servidor DNS** consultado como en la **caché local del resolver**.

Cómo funcionan las consultas recursivas

Una consulta recursiva es aquélla realizada a un servidor DNS, en la que el cliente DNS solicita al servidor DNS que proporcione una respuesta completa a la consulta El servidor DNS comprueba la zona de búsqueda directa y la caché para encontrar una respuesta a la consulta.

Cómo funcionan las consultas iterativas

Una consulta iterativa es aquélla efectuada a un servidor DNS en la que el cliente DNS solicita la mejor respuesta que el servidor DNS puede proporcionar sin buscar ayuda adicional de otros servidores DNS. El resultado de una consulta iterativa

suele ser una referencia a otro servidor DNS de nivel inferior en el árbol DNS
Consulta iterativa Sugerencias Raiz(.)

Dns Cache

La caché de la DNS almacena en nuestros PCs entradas positivas y negativas. Las positivas son aquellas en las que la "DNS Lookup" tuvo éxito y pudimos conectar con la web que deseábamos visualizar.

Las entradas negativas son aquellas que quedan registradas como consecuencia de algún intento fallido de la "DNS Lookup" que nos impidió acceder a la página web.

El problema surge cuando la caché de la DNS guarda esas entradas negativas y, aunque la web ya se encuentre disponible y se pueda acceder sin problemas, Windows nos seguirá indicando **"DNS ERROR!".**

TTL

Todos los registros DNS tiene la propiedad TTL, que especifica el tiempo máximo que otros servidores DNS y aplicaciones deben mantener en caché ese registro. Si el valor es 0, entonces no se mantiene ningún caché y los cambios que se realicen en el registro se registrarán en el momento.

Cuando se decide el tiempo TTL, se debe tener en cuenta cuan a menos se cambiará el record (registro). Por el caché, los cambios en un registro DNS no alcanzarán toda la red hasta que el TTL no haya expirado. Si se quieren cambios rápidos, debe elegirse un TTL bajo.

De todas maneras, el cacheo ayuda a reducir el tráfico de la red. Mientras más alto el TTL, más tiempo se quedará guardado el registro en otros servidores DNS del mundo. Por lo tanto, se necesitarán menos peticiones al servidor DNS original (una buena razón para configurar el TTL en un valor alto).

- RESOLUCIÓN INVERSA:

- **Mapeo de direcciones y dominio arpa**
- **Zonas de resolución inversa. Proceso de resolución**
- **Delegación y resolución inversa**

Resolución Inversa DNS

La resolución DNS más común es la hecha para traducir un nombre para una dirección IP, pero esa no es el único tipo de resolución DNS. Hay también la resolución denominada inversa, que hace la traducción de una dirección IP a un nombre.

En un inicio la resolución inversa se utilizaba como mecanismo auxiliar de seguridad para los servidores en la Internet, comparando los resultados de una resolución inversa contra la resolución directa del nombre para dirección IP. En el caso de los resultados iguales, se permitía, por ejemplo, el acceso remoto al servidor.

Actualmente algunos servidores de FTP no permiten conexión a partir de direcciones IP que no tengan resolución inversa configurada. Es posible encontrar también servidores HTTP (web), configurados para hacer la resolución inversa cuando una computadora inicia una conexión. Esa información es almacenada en archivos de registros (logs) para futuro procesamiento o para generación de estadísticas. En estos casos, cuando la dirección IP de la computadora no posee resolución inversa habrá un atraso en la conexión debido al tiempo gastado en el intento de hacer la resolución inversa.

Dominio arpa

.arpa es un dominio de Internet genérico de nivel superior usado exclusivamente para la infraestructura de Internet.

El dominio .arpa fue establecido en 1985 para que facilitara la transición hacia los sistemas DNS y luego ser eliminado. La red ARPANET fue la predecesora de Internet creada en el Departamento de Defensa de los Estados Unidos por la Agencia de Proyectos de Investigación Avanzada (ARPA), y cuando el sistema de DNS's comenzó a funcionar los dominios de ARPANET fueron inicialmente convertidos al nuevo sistema añadiéndoles .arpa al final. Otras redes también fueron convertidas al nuevo sistema usando pseudo-dominios, añadiendo al final dominios como .uucp o .bitnet, aunque estos nunca fueron añadidos a los dominios genéricos de Internet.

Funcionamiento de la resolución inversa

Para la resolución inversa fueron creados nombres de dominio especiales: in-addr.arpa para bloques IPv4 e ip6.arpa para bloques IPv6.

Para poner la dirección IP dentro de la jerarquía de nombres DNS, es necesario hacer una operación para crear un nombre que represente la dirección IP dentro de esa estructura.

En la jerarquía de nombres del sistema DNS la parte más a la izquierda es la más específica y la parte a la derecha la menos específica. Pero en la numeración de direcciones IP eso está invertido, es decir, lo más específico es lo que está más a la derecha en una dirección IP, por lo que para resolver eso se debió hacer una operación invirtiendo cada parte de la dirección IP y luego añadir el nombre de dominio reservado para la resolución inversa (in-addr.arpa o ip6.arpa)

Por ejemplo, considerando la dirección IPv4 10.0.0.1. Para colocarla en el formato necesario, se debe invertir cada byte (Un byte es lo mismo que 8 bits) y añadir el dominio para resolución inversa al final: 1.0.0.10.in-addr.arpa

Delegación

Hemos comentado que los dominios de primer nivel destinados a los países son gestionados por estos a su voluntad. Ésto es posible porque estos dominios están *delegados* en administradores propios al país, de forma que son éstos los que los gestionan. Dicha delegación de *autoridad* sobre un dominio se puede realizar a cualquier nivel del espacio de nombres, de manera que si se dispone un dominio de segundo nivel para una empresa, se podrían crear dominios de niveles inferiores según la estructura organizativa de la empresa, por poner un ejemplo.

Más concretamente, la delegación consiste en la cesión del control de una *zona* del espacio de nombre a otro servidor DNS. Una zona es una porción del espacio de nombres, de forma que se posee autoridad desde el nodo raíz de dicha zona dentro del árbol jerárquico, pudiendo crear o eliminar nuevos subdominios a partir del nivel en el que se encuentre dicho nodo raíz.

La diferencia entre dominio y zona suele ser confusa en un principio. Se trata de dos conceptos relacionados en diferentes capas: dominio es un concepto del espacio de nombres, mientras que zona es la forma en la que se distribuye la autoridad sobre un determinado dominio. Así pues, un dominio contiene todas las máquinas que están dentro de dicho dominio, incluidos subdominios, mientras que una zona incluye solo las máquinas del dominio que cuelgan del subdominio sobre el que se posee la autoridad. Podría decirse que las zonas es la forma en la que se distribuye el control sobre el espacio de nombres, y, por lo tanto, que son una causa directa de la delegación de autoridad sobre el espacio de nombre.

Responsables de Delegación para IPv4

La delegación DNS de resolución inversa para direcciones IPv4 debe ser hecha respetando los límites de bytes de cada parte de la dirección IP, esto es:

- la delegación del primer byte, lo que representa un bloque de prefijo /8
- la delegación del según byte lo que representa un bloque de prefijo /16
- la delegación del tercer byte que representa un bloque de prefijo /24.

Responsables de Delegación para IPv6

- En el caso de direcciones IPv6 no existe esa restricción, siendo posible delegar cada conjunto de 4 bits de la dirección IPv6, lo cual contiene 128 bits representados en notación hexadecimal separados en 8 grupos de 16 bits cada.
- Por ejemplo, considerando la dirección IPv6 2001:0DB8:0000:0000:0000:0000:0000:0001, se tendría la siguiente representación en la jerarquía DNS para resolución inversa: 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.B.D.0.1.0.0.2.ip6.arpa

- REGISTROS DE RECURSOS DNS:

- **Formato general**
- **Tipos de registros SOA, NS, A, AAAA, A6, CNAME, MX, SRV, PTR**
- **Delegación de Glue Record**

Registros de Recursos (RR)

Para resolver nombres, los servidores consultan sus zonas. Las zonas contienen *registros de recursos* que constituyen la información de recursos asociada al dominio DNS. Por ejemplo, ciertos registros de recursos asignan nombres descriptivos a direcciones IP.

El formato de cada registro de recursos es el siguiente:

Propietario TTL Clase Tipo RDATA

Dónde:

- **Propietario**: 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).
- **TTL**: (*Time To Live*) Tiempo de vida, generalmente expresado en segundos, que un servidor DNS o un resolver debe guardar en caché esta entrada antes de descartarla. Este campo es opcional. También se puede expresar mediante letras indicando días (d), horas (h), minutos (m) y segundos (s). Por ejemplo: "2h30m".
- **Clase**: define la familia de protocolos en uso. Suele ser siempre "IN", que representa Internet.
- **Tipo**: identifica el tipo de registro.
- **RDATA**: los datos del registro de recursos.

A continuación se describen los principales tipos de registros de recursos: SOA, NS, A, PTR, CNAME, MX y SRV.

Registro de Recurso SOA

Cada zona contiene un registro de recursos denominado Inicio de Autoridad o SOA (*Start Of Authority*) al comienzo de la zona. Los registros SOA incluyen los siguientes campos (sólo se incluyen los que poseen un significado específico para el tipo de registro):

- **Propietario**: nombre de dominio de la zona.
- **Tipo**: "SOA".
- **Persona responsable**: contiene la dirección de correo electrónico del responsable de la zona. En esta dirección de correo, se utiliza un punto en el lugar del símbolo "@".
- **Número de serie**: muestra el número de versión de la zona, es decir, un número que sirve de referencia a los servidores secundarios de la zona para saber cuándo deben proceder a una actualización de su base de datos de la zona (o *transferencia de zona*). Cuando el número de serie del servidor secundario sea *menor* que el número del maestro, esto significa que el maestro ha cambiado la zona, y por tanto el secundario debe solicitar al maestro una transferencia de zona. Por tanto, este número debe ser incrementado (manualmente) por el administrador de la zona cada vez que realiza un cambio en algún registro de la zona (en el servidor maestro).
- **Actualización**: muestra cada cuánto tiempo un servidor secundario debe ponerse en contacto con el maestro para comprobar si ha habido cambios en la zona.
- **Reintentos**: define el tiempo que el servidor secundario, después de enviar una solicitud de transferencia de zona, espera para obtener una respuesta del servidor maestro antes de volverlo a intentar.
- **Caducidad**: define el tiempo que el servidor secundario de la zona, después de la transferencia de zona anterior, responderá a las consultas de la zona antes de descartar la suya propia como no válida.
- **TTL mínimo**: este campo específica el tiempo de validez (o de vida) de las respuestas "negativas" que realiza el servidor. Una respuesta negativa significa que el servidor contesta que un registro no existe en la zona.

  Hasta la versión 8.2 de BIND, este campo establecía el tiempo de vida por defecto de todos los registros de la zona que no tuvieran un campo TTL específico. A partir de esta versión, esto último se consigue con una *directiva* que debe situarse al principio del fichero de la zona. Esta directiva se especifica así:

  $TTL tiempo

  Por ejemplo, un tiempo de vida por defecto de 30 minutos se establecería así:

  $TTL 30m

  Un ejemplo de registro SOA sería el siguiente:

```
Admon.com.  IN  pc0100.admon.com  hostmaster.admon.com..
        (

          1             ; Número de serie
          3600          ; actualización 1 hora
          600           ; reintentar 10 minutos
          86400         ; caducar 1 día
          60            ; TTL 1 minuto

        )
```

Registro de Recurso NS

El registro de recursos NS (*Name Server*) indica los servidores de nombres autorizados para la zona. Cada zona debe contener registros indicando tanto los servidores principales como los secundarios. Por tanto, cada zona debe contener, como mínimo, un registro NS.

Por otra parte, estos registros también se utilizan para indicar quiénes son los servidores de nombres con autoridad en subdominios delegados, por lo que la zona contendrá al menos un registro NS por cada subdominio que haya delegado.

Ejemplos de registros NS serían los siguientes:

```
Admon.com.              IN  NS   pc100.admon.com..
Valencia.admon.com.     IN  NS
pc0102.valencia.admon.com.
```

Registro de Recurso A

El tipo de registro de recursos A (*Address*) asigna un nombre de dominio completamente cualificado (FQDN) a una dirección IP, para que los clientes puedan solicitar la dirección IP de un nombre de host dado.

Un ejemplo de registro A que asignaría la dirección IP 158.42.178.1 al nombre de dominio pc101.valencia.admon.com., sería el siguiente:

```
Pc0101.valencia.admon.com.   IN  A     158.42.178.1
```

Registro de Recurso 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. Este tipo de recursos se utilizan en la denominada *resolución inversa*, descrita en"Servidores de nombresy zonas"..

Un ejemplo de registro PTR que asignaría el nombre pc0101.valencia.admon.com. a la dirección IP 158.42.178.1 sería el siguiente:

1.178.42.158.in-addr.arpa. IN PTR pc0101.admon.valencia.com..

Registro de Recurso CNAME

El registro de nombre canónico (CNAME, *Canonical NAME*) crea un alias (un sinónimo) para el nombre de dominio especificado.

Un ejemplo de registro CNAME que asignaría el alias controlador al nombre de dominio pc0102.valencia.admon.com, sería el siguiente:

```
Controlador.valencia.admon.com..
            IN    CNAME   pc0101.valencia.admon.com.
```

Registro de Recurso 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 servidores de correo.

Un ejemplo de registro de recurso MX que define al servidor pc0100 como el servidor de correo del dominio admon.com, sería el siguiente:

```
Admon.com.   IN   MX   0   pc0100.admon.com..
```

Registro de Recurso SRV

Con registros MX se puede especificar varios servidores de correo en un dominio DNS. De esta forma, cuando un proveedor de servicio de envío de correo necesite enviar correo electrónico a un host en el dominio, podrá encontrar la ubicación de un servidor de intercambio de correo. Sin embargo, esta no es la forma de resolver los servidores que proporcionan otros servicios de red como WWW o FTP.

Los registros de recurso de servicio (SRV, *SeRVice*) permiten especificar de forma genérica la ubicación de los servidores para un servicio, protocolo y dominio DNS determinados.

El formato de un registro SRV es el siguiente:

```
servicio.protocolo.nombre  TTL  clase  SRV
                    prioridad  peso  puerto  destino
```

Dónde:

- El campo servicio específica el nombre de servicio: http, telnet, etc.
- El campo protocolo especifica el protocolo utilizado: TCP o UDP.

- nombre define el nombre de dominio al que hace referencia el registro de recurso SRV.
- Los campos TTL y clase ha sido definidos anteriormente.
- prioridad específica el orden en que los clientes se pondrán en contacto con los servidores: los clientes intentarán ponerse en contacto primero con el host que tenga el valor de prioridad más bajo, luego con el siguiente y así sucesivamente.
- peso: es un mecanismo de equilibrio de carga.
- puerto: muestra el puerto del servicio en el host.
- destino: muestra el nombre de dominio completo para la máquina compatible con ese servicio.

Un ejemplo de registros SRV para los servidores Web del dominio admon.com., sería:

```
http.tcp.admon.com.  IN  SRV   0  0  80  www1.admon.com..
http.tcp.admon.com.  IN  SRV  10  0  80  www2.admon.com..
```

Definición de la delegación

Para que una zona especifique que uno de sus subdominios está delegado en una zona diferente, es necesario agregar un *registro de delegación* y, generalmente, el denominado "registro de pegado" (*glue record*). El registro de delegación es un registro NS en la zona principal (padre) que define el servidor de nombres autorizado para la zona delegada. El registro de pegado es un registro tipo A para el servidor de nombres autorizado para la zona delegada, y es necesario cuando el servidor de nombres autorizado para la zona delegada también es un miembro de ese dominio (delegado).

Por ejemplo, si la zona admon.com deseara delegar la autoridad a su subdominio valencia.admon.com, se deberían agregar los siguientes registros al archivo de configuración correspondiente de la zona admon.com:

```
Valencia.admon.com.        IN  NS  pc0102.valencia.admon.com.
pc0102.valencia.admon.com. IN  A 138.42.178.2
```

Tipos de zonas

Aunque distintas implementaciones de DNS difieren en cómo configurar las zonas, generalmente existe un fichero que indica sobre qué zonas tiene autoridad el servidor, indicando para cada una el fichero que contiene la información de dicha zona (si el servidor es primario para la zona), o la dirección del servidor maestro a quien preguntar por ella (si es secundario).

En general, existen tres tipos distintos de zonas: zonas de búsqueda directa, zonas de búsqueda inversa y zonas de "sugerencia raíz". Un servidor DNS puede tener autoridad sobre varias zonas directas e inversas, y necesita poseer información sobre las "sugerencias raíz" si desea responder a sus clientes sobre registros de

zonas sobre las que no posee autoridad. A continuación se describe cada tipo brevemente.

Zona de búsqueda directa

Las zonas de búsqueda directa contienen la información necesaria para resolver nombres en el dominio DNS. Deben incluir, al menos, registros SOA y NS, y pueden incluir cualquier otro tipo de registros de recurso, excepto el registro de recursos PTR.

Zona de búsqueda inversa

Las zonas de búsqueda inversa contienen información necesaria para realizar las búsquedas inversas. La mayor parte de las consultas proporcionan un nombre y solicitan la dirección IP que corresponde a ese nombre. Este tipo de consulta es el descrito en la zona de resolución directa.

Pero existen ocasiones en que un cliente ya tiene la dirección IP de un equipo y desea determinar el nombre DNS de ese equipo. Esto es importante para los programas que implementan la seguridad basándose en el FQDN que se conecta y también se utiliza para la solución de problemas de red TCP/IP.

Si el único medio de resolver una búsqueda inversa es realizar una búsqueda detallada de todos los dominios en el espacio de nombres DNS, la búsqueda de consulta inversa sería demasiado exhaustiva como para realizarla de forma práctica.

Para solucionar este problema se creó un dominio DNS especial para realizar búsquedas "inversas", denominado in-addr.arpa.. Este dominio utiliza un orden inverso de números en la notación decimal de las direcciones IP. Con esta disposición se puede delegar la autoridad de miembros inferiores del dominio in-addr.arpa. a las distintas organizaciones, a medida que se les asigna identificadores de red de clase A, B o C.

Sugerencias de los servidores del Dominio Raíz

El archivo de "sugerencias raíz" (*root hint*), denominado también archivo de sugerencias de caché, contiene la información de host necesaria para resolver nombres fuera de los dominios en los que el servidor posee autoridad. En concreto, este archivo contiene los nombres y las direcciones IP de los servidores DNS del dominio punto (.) o raíz.

Glue Record Un glue record es un A record el cual es creado como parte de una delegación. Si una zona se delega a un nameserver cuyo hostname es un descendiente de esa zona particular, entonces se debe incluir un glue record para ese hostname en la delegación.

- TRANSFERENCIAS DE ZONA:

- **Tipos de transferencias de zona: Completa e Incremental**
- **Proceso de transferencias de zona**

En aquellas zonas en las que existen diferentes servidores de nombres con autoridad (uno principal o maestro y uno o varios secundarios o esclavos), cada vez que se realizan cambios en la zona del servidor maestro, estos cambios deben replicarse a todos los servidores secundarios de esa zona. Esta acción se lleva a cabo mediante un mecanismo denominado transferencia de zona. Existen dos tipos de transferencia de zonas: completa e incremental.

Transferencia completa de zona

En una transferencia completa de zona, el servidor maestro para una zona transmite toda la base de datos de zona al servidor secundario para esa zona.

Los servidores secundarios siguen los siguientes pasos a la hora de realizar una transferencia de zona:

1. El servidor secundario para la zona espera el tiempo especificado en el campo Actualizar del registro SOA y luego le pregunta al servidor maestro por su registro SOA.
2. El servidor maestro responde con su registro SOA.
3. El servidor secundario para la zona compara el número de serie devuelto con su propio número y si este es mayor que el suyo, solicita una transferencia de zona completa.
4. El servidor maestro envía la base de datos de la zona completa al servidor secundario.

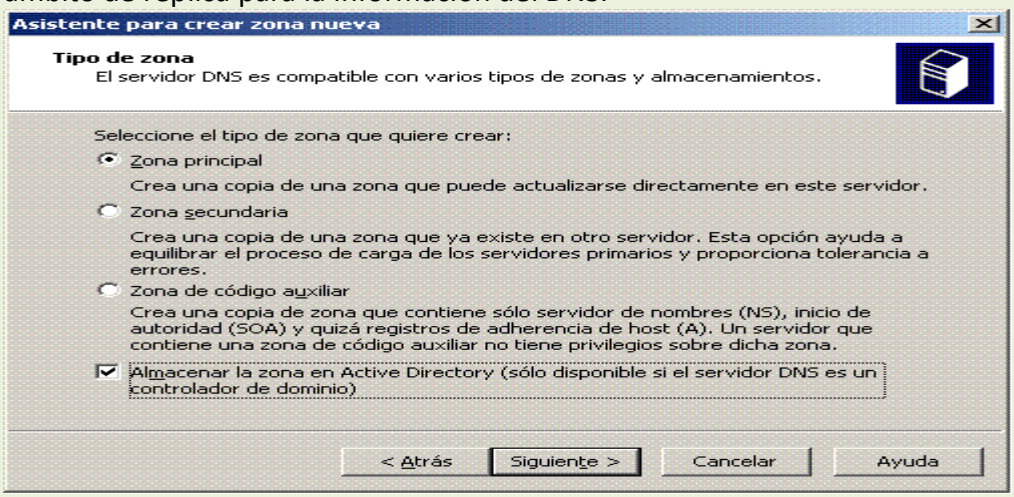
Si el servidor maestro no responde, el servidor secundario lo seguirá intentando después del intervalo especificado en el campo Reintentos del registro SOA. Si todavía no hay respuesta después del intervalo que se especifica en el campo Caduca desde la última transferencia de zona, este descarta su zona.

Transferencia incremental de zona

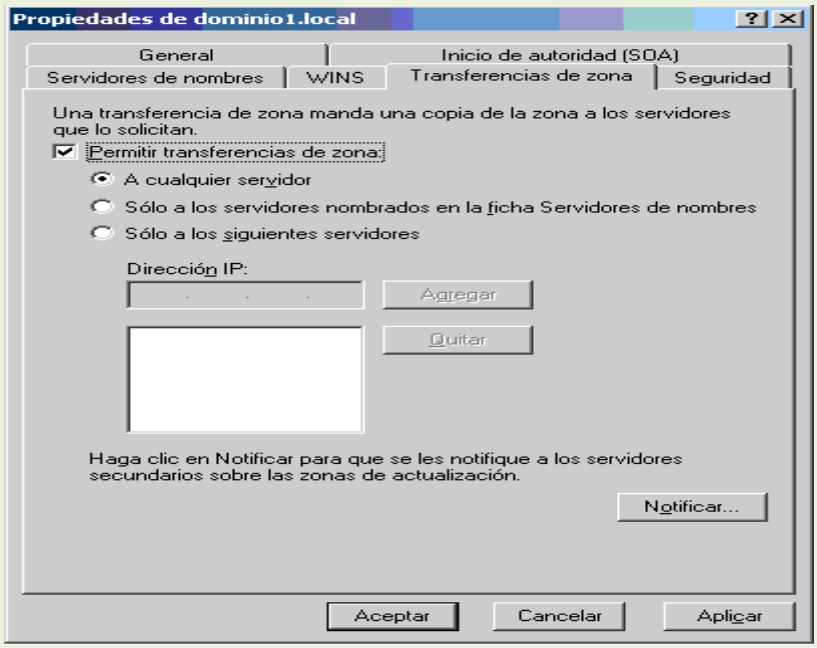
Las transferencias completas de zona pueden consumir gran ancho de banda de la red. Para poder solucionar este problema se define la transferencia incremental de zona, en la cual sólo debe transferirse la parte modificada de una zona.

La transferencia incremental de zona funciona de forma muy similar a la transferencia completa. En este caso, el servidor secundario para la zona comprueba el número de serie del registro SOA del maestro con el suyo, para determinar si debe iniciar una transferencia de zona, la cual en este caso sería incremental (sólo de los cambios realizados).

Transferencias de zona siempre se inician por el servidor DNS secundario. El servidor DNS principal simplemente responderá a la petición para una transferencia de zona.
Cuando se agrega un nuevo servidor DNS a la red y se configura como un nuevo servidor secundario en una zona existente, dicho servidor realiza una transferencia inicial completa de la zona para obtener y replicar una copia total de los registros de recursos de la zona. En la mayor parte de implementaciones anteriores de servidores DNS, este método de transferencia completa de una zona también se utiliza cuando la zona necesita actualizarse después de haber experimentado cambios. Para los servidores DNS que ejecutan Windows Server 2003, el servicio DNS admite **la *transferencia de zona incremental*;** un proceso revisado de transferencia de zona DNS para cambios intermedios.
Almacenar la zona en active directory (solo disponible si el servidor DNS es un controlador de dominio)
Al marcar esta opción , en la siguiente pantalla del asistente, nos va a pedir el ámbito de replica para la información del DNS.



Es decir podremos indicarle si queremos replicar la zona a: - A Todos los servidores DNS del bosque. - A Todos los servidores DNS del dominio. - A todos los controladores de. dominio. Una vez creada la zona, también se puede configurar para que esta sea transferida a otros servidores DNS, usando zonas secundarias, stub o como hemos visto anteriormente mediante la opción de tenerla almacenada en el directorio activo.
Para poder permitir que la zona se propague debemos:
Abrir la consola de administración del servicio de DNS Acceder a las propiedades Nos situamos en la pestaña "Transferencias de zona" Y marcamos la opción Permitir transferencias de zona Vamos a tener tres elecciones: **A cualquier servidor A los servidores que se han listado en la pestaña de nombres de servidores A los servidores que se indique en la lista que aparece en esta misma pestaña (debemos rellenarlos nosotros a mano)**


Propiedades de dominio1.local
General
Inicio de autoridad (SOA)
Servidores de nombres
WINS
Transferencias de zona
Seguridad
Una transferencia de zona manda una copia de la zona a los servidores que lo solicitan.
Permitir transferencias de zona:
A cualquier servidor
Sólo a los servidores nombrados en la ficha Servidores de nombres
Sólo a los siguientes servidores
Dirección IP:
Agregar
Quitar
Haga clic en Notificar para que se les notifique a los servidores secundarios sobre las zonas de actualización.
Notificar...
Aceptar
Cancelar
Aplicar

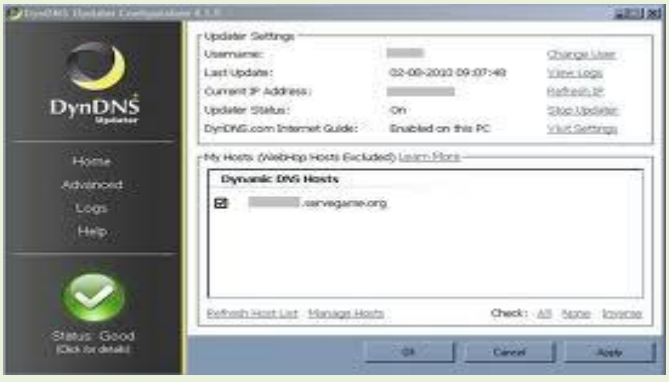
- DNS DINÁMICO (DDNS o Dynamic DNS):

- **Actualizaciones manuales**
- **Actualizaciones dinámicas**
- **DNS dinámico en Internet**

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. 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.

El DNS dinámico hace posible, siendo de uso frecuente gracias a lo descrito, utilizar software de servidor en una computadora con dirección IP dinámica, como la suelen facilitar muchos proveedores de Internet para particulares (por ejemplo para alojar un sitio web en el ordenador de nuestra casa, sin necesidad de contratar un hosting de terceros -aunque los hay gratuitos y hay que tener en cuenta que los ordenadores caseros posiblemente no estén tan bien dotados, a diferencia de los de aquellos, para estar encendidos permanentemente, sin olvidar el aumento del coste de la factura eléctrica-).

Otro uso útil que posibilita el DNS dinámico es poder acceder al ordenador en cuestión por medio del escritorio remoto.



Este servicio es ofrecido, incluso de forma gratuita, por DynDNS, No-IP, CDmon y FreeDNS.

Actualizaciones manuales. La actualización manual consiste en la modificación de los ficheros de la base de datos de DNS para asignar una dirección Ip a un nombre de dominio. Porblemas:

- Afrontar la posibilidad de errores al manipular los ficheros de la Base de Datos del *DNS*.
- Realización de una copia de seguridad, actualización "a mano" de los ficheros de la Base de Datos,
- Re-inicializar el servidor de *DNS* para que los cambios tuvieran efecto.

Actualizaciones dinámicas. La actualización dinámica permite a los equipos cliente DNS guardar y actualizar dinámicamente sus registros de recursos con un servidor DNS siempre que se produzcan cambios. Esto disminuye la necesidad de

administrar de forma manual los registros de zona, especialmente para los clientes que mueven o cambian ubicaciones con frecuencia y utilizan DHCP para obtener una dirección IP. **DNS dinámico en Internet.** Cuando nos conectamos a Internet, el proveedor a través del que nos conectamos nos asigna una IP de Internet que habitualmente cambia. Para solucionar el problema cada vez que se inicia el servidor, o cuando deseemos, envía nuestra IP actual a la empresa que nos proporciona el DNS dinámico, para que nuestro subdominio se dirija a la IP que tenemos en cada momento.

- PROTOCOLO DNS

Este protocolo se utiliza para poder recordar de manera sencilla las direcciones **IP**. De esta manera surge el concepto de nombres de **dominio**. Gracias a esto podemos asignar a una dirección IP un nombre, además de que es más fiable porque la dirección IP de un servidor puede cambiar pero el nombre no lo hace. Podemos decir entonces que el **DNS** es un sistema jerárquico y distribuido que permite traducir nombres de dominio en direcciones IP y viceversa. Otro uso común de este es para los servidores de correo a través del nombre de dominio de correo como por ejemplo “www.Hotmail.com“. Dado un **dominio** puede leerse de derecha a izquierda por ejemplo “www.google.es” seria “.es” el dominio más alto.

Cada dominio es como si terminase con un “.” Por eso nuestro dominio seria “www.google.es“y el punto al final es el elemento **raíz** de nuestro **árbol** y lo que indica al cliente que debe de empezar la búsqueda en los root Server. Estos root Server son los que tienen los registros **TLD** que son los dominios de nivel superior ósea los que no pertenecen a otro dominio, como son “com, org, net, es, etc.” Actualmente hay 13 **TLD** en todo el mundo y 10 de ellos se encuentran en estados unidos, uno en Estocolmo, otro en Japón, y el último en Londres. Si alguna catástrofe hiciese que estos 13 servidores dejasen de operar provocaría un gran apagón de Internet y causaría estragos a nivel mundial.

Estos servidores dice que dominios de primer nivel existen y cuáles son sus servidores de nombres recursivamente los servidores de esos dominios dicen que subdominios existen y cuales don sus servidores.

Cada componente de **dominio** incluyendo la raíz, tiene un servidor primario y varios secundarios. Todos tienen la misma autoridad para responder por ese dominio, pero el primario es el único sobre el que se pueden hacer modificaciones de manera que los secundarios son reaplicas del primario.

Casi todos los servidores de nombres utilizan un software llamado **bind** que es un software de libre distribución utilizado por la mayoría de sistemas unix.

Una herramienta útil que encontramos para probar si un dominio se resuelve correctamente es el domando "**nslookup**". Se trata de un cliente **DNS** que nos sirve para obtener direcciones IP a través del **dominio** y viceversa.

Aplicaciones de DNS Muchas implementaciones de DNS proporcionan tres utilidades bastante comunes para consultar a servidores de nombres:
- **host** Obtiene una dirección IP asociada con un nombre de host o un nombre de host asociado con una dirección IP.
- **nslookup** Permite localizar información acerca de los nodos de red, examinar los contenidos de la base de datos de un servidor de nombres y establecer la accesibilidad a servidores de nombres.
- **dig** Permite probar los servidores de nombres, reunir grandes volúmenes de información de nombres de dominio y ejecutar simples consultas de nombres de dominio.

- SEGURIDAD DNS

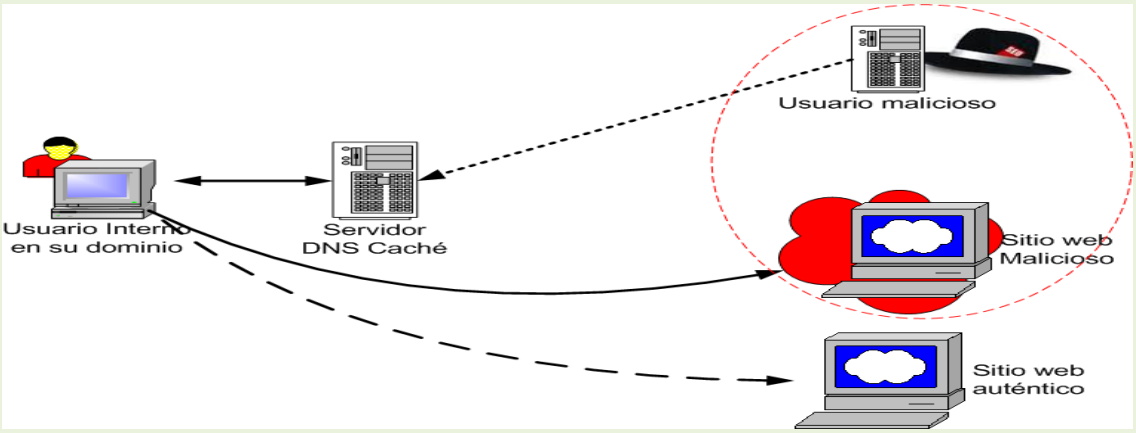
- **Vulnerabilidades, amenazas y ataques**
- **Mecanismos de seguridad**

El sistema de nombres de dominio (DNS, *Domain Name System*) se diseñó originalmente como un protocolo abierto y, por tanto, es vulnerable a intrusos. El DNS de Windows Server 2003 ha mejorado su capacidad para impedir un ataque en la infraestructura DNS mediante la adición de características de seguridad

VULNERABILIDADES

Seguridad en DNS:
Caché Poisoning

- El caché Poisoning es una técnica por la cual es posible engañar a un servidor DNS y hacerle creer que recibió información auténtica y válida
- El servidor luego cachea esa información y la utiliza para responder otras consultas hasta la duración el TTL de los RRs cacheados
- Robo de información



Estas vulnerabilidades se producen debido a una libre interpretación a la hora de implementar este protocolo. DNS utiliza mensajes con un formato determinado, que son interpretados por el mecanismo de resolución de nombre a dirección IP. Un mensaje puede ser una búsqueda o una respuesta. Por la implementación propia del protocolo, en determinadas circunstancias, una respuesta puede solicitar otra respuesta. Ello puede causar un flujo de mensajes capaces de generar un ataque de denegación de servicio (DoS).

También es posible implementar una consulta que aparente ser originada por el equipo local en el puerto 53 (usado por defecto), de tal modo que el servidor se responderá a sí mismo en un ciclo de respuestas que podría causar que el sistema exceda los recursos disponibles, produciéndose un ataque de denegación de servicio.

Son afectados los siguientes productos:
- Axis
- JH Software
- Sprint
- Cisco
- Juniper
- VeriSign
- DNRD
- Men & Mice
- WindRiver
- Hewlett-Packard
- MyDNS
- JDNSS
- Posadis

Con la herramienta PorkBind podemos analizar vulnerabilidades que afectan a la seguridad de servidores DNS. Una vez descubierta la vulnerabilidad nos indica cómo solucionarla con su correspondiente link de CVSS v2.0 y OVAL. Entre las vulnerabilidades que chequea se encuentra la popular vulnerabilidad reportada por Dan Kaminsky.

Las vulnerabilidades que detecta son:

- Envenenamiento de la cache.
- Denegación de servicios vía maxdname.
- Desbordamiento de buffer a través de consulta inversa.
- Desbordamiento de buffer a través de TSIG.
- Desbordamiento de buffer a través de nslookup.
- Acceso a través de variables de entorno.
- Desbordamiento de buffer a través de nslookup.
- Denegación de servicio a través de dns_message_findtype.
- Modificación del puntero nulo SIG RR.
- Denegación de servicios.
- Denegación de servicios vía puntero nulo SIG RR.
- Ejecución de código arbitrario.
- Envenenamiento de la cache.
- Envenenamiento de la cache.
- Envenenamiento de la cache (de Dan Kaminsky).

AMENAZAS

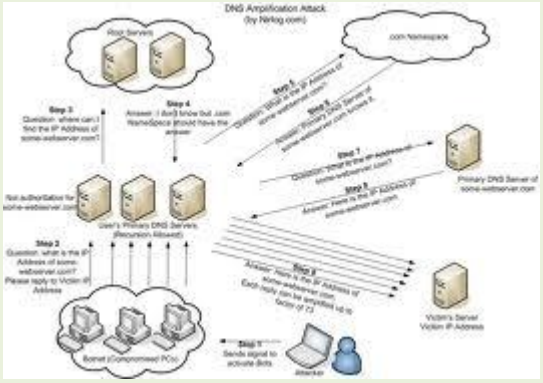
Éstas son las formas comunes en que los intrusos pueden amenazar su infraestructura DNS:

- La ocupación es el proceso mediante el cual un intruso obtiene los datos de zona DNS para obtener los nombres de dominio DNS, nombres de equipo y direcciones IP de recursos de red importantes. Un intruso suele empezar un ataque utilizando estos datos DNS para obtener un diagrama u ocupación, de una red. Los nombres de equipo y dominio DNS suelen indicar la función o ubicación de un dominio o equipo para ayudar a los usuarios a recordar e identificar los dominios y equipos con mayor facilidad. Un intruso se aprovecha del mismo principio DNS para aprender la función o ubicación de dominios y equipos en la red.
- Un ataque por servicio denegado se produce cuando un intruso intenta denegar la disponibilidad de los servicios de red desbordando uno o varios servidores DNS de la red con consultas recursivas. Cuando un servidor DNS se desborda con consultas, el uso de la CPU alcanzará su nivel máximo y el servicio del Servidor DNS dejará de estar disponible. Sin un servidor DNS completamente operativo en la red, los servicios de red que utilicen DNS dejarán de estar disponibles para los usuarios de la red.

- La modificación de datos es un intento del intruso (que ha ocupado una red mediante DNS) de utilizar direcciones IP válidas en paquetes IP que ha creado él mismo, de manera que proporciona a estos paquetes la apariencia de proceder de una dirección IP válida de la red. Esto se denomina comúnmente IP ficticia. Con una dirección IP válida (una dirección IP dentro del rango de direcciones IP de una subred), el intruso puede tener acceso a la red y destruir datos o realizar otro tipo de ataque.

- La redirección se produce cuando un intruso puede redirigir consultas de nombres DNS a servidores que él controle. Un método de redirección incluye el intento de contaminar la caché DNS de un servidor DNS con datos DNS erróneos que pueden dirigir consultas futuras a servidores que controle el intruso. Por ejemplo, si se realizó una consulta originalmente para ejemplo.microsoft.com y la respuesta de referencia proporcionó el registro de un nombre externo al dominio microsoft.com, como usuario-malintencionado.com, el servidor DNS utilizará los datos de la caché de usuario-malintencionado.com para resolver la consulta de dicho nombre. La redirección puede realizarse siempre que el intruso disponga de

acceso de escritura a datos DNS, como ocurre, por ejemplo, con las actualizaciones dinámicas no seguras.



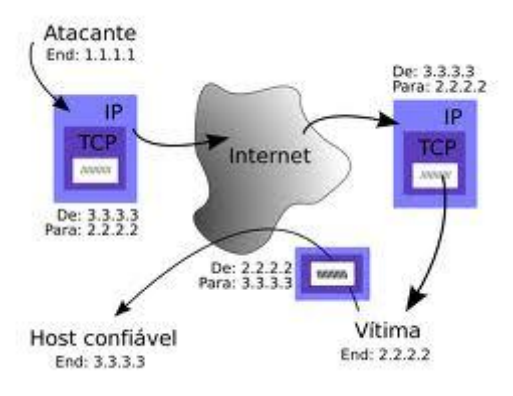
ATAQUES

Algunos de los ataques más comunes que se presentan en un servicio de DNS son los siguientes:

- Ataque de negación del servicio (DOS): este ataques se presenta cuando el servidor DNS se ve inundado con un número muy grande de requerimientos reconocidos que pueden eventualmente forzar al procesador a ser usado más allá de sus capacidades recordemos que un procesador Pentium dos de 700 MHz puede soportar hasta 10,000 consultas por segundo; de esta manera se podría evitar que el servidor de DNS siga prestando servicio de manera normal este tipo de ataque no requiere el una gran cantidad de conocimiento por parte del atacante este tipo es extremadamente efectivo, llegando en casos extremos a provocar el reinicio del servidor de red o deteniendo por completo la resolución de nombres, la imposibilidad de resolver nombres por medio del servidor de DNS puede evitar el acceso de los usuarios a cualquier recurso de Internet, tal como, correo electrónico o páginas de hipertexto, en el caso de los sistemas Windows 2000 y 2003 que funcionan con directorio activo evita la autenticación de los usuarios y por tanto no permite el acceso a cualquier recurso de red.

- Footprinting: los intrusos pueden lograr una gran cantidad de información acerca de la infraestructura de la red interceptando los paquetes de DNS para de esta manera lograr identificar sus objetivos, capturando el tráfico de DNS los intrusos pueden aprender acerca del sistema de nombres del dominio, los nombres de las máquinas, y el esquema de IP que se emplea en una red. Esta información de red revela la funcionalidad de ciertas máquinas presentes en la misma permitiendo al intruso decidir cuáles son los objetivos más fructíferos y otra forma de atacarlos.

- IPSoopfing: los intrusos pueden utilizar una IP legítima a menudo obtenida por medio del ataque anterior para ganar acceso a la red a sus servicios para enviar paquetes que pueden provocar daños dentro de la red a nombre de una máquina que no hace parte de la red, engañando al sistema identificándose con una IP de que no les corresponde a este proceso se le llama Spoofing. Esta manera pueden pasar diferentes filtros están diseñados para bloquear el tráfico de IP desautorizadas dentro de la red. Una vez han logrado acceso a los computadores y servicios usando esta técnica el atacante puede causar gran cantidad de daños pues dentro de la red se supone que las IP les pertenecen al segmento local.



- Redireccionamiento en este tipo de ataque de un intruso causa que el servidor de DNS redireccione todas las consultas de resolución de nombres aún servidor incorrecto que está bajo el control del atacante el atacante de lograr esta técnica

mediante la corrupción o envenenamiento del caché del servidor utilizando actualizaciones dinámicas.

MECANISMOS DE SEGURIDAD

Un mecanismo de seguridad informática es una técnica o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y/o la disponibilidad de un sistema informático.

Existen muchos y variados mecanismos de seguridad informática. Su selección depende del tipo de sistema, de su función y de los factores de riesgo que lo amenazan.

Clasificación según su función:

Preventivos: Actúan antes de que un hecho ocurra y su función es detener agentes no deseados.

Detectivos: Actúan antes de que un hecho ocurra y su función es revelar la presencia de agentes no deseados en algún componente del sistema. Se caracterizan por enviar un aviso y registrar la incidencia.

Correctivos: Actúan luego de ocurrido el hecho y su función es corregir la consecuencias.

Según un informe del año 1991 del Congressional Research Service, las computadoras tienen dos características inherentes que las dejan abiertas a ataques o errores operativos

1.-Una computadora hace exactamente lo que está programada para hacer, incluyendo la revelación de información importante. Un sistema puede ser reprogramado por cualquier persona que tenga los conocimientos adecuados.

2.-Cualquier computadora puede hacer sólo aquello para lo que está programada, no puede protegerse a sí misma contra un mal funcionamiento o un ataque deliberado a menos que este tipo de eventos haya sido previsto de antemano y se hayan puesto medidas necesarias para evitarlos.

Los propietarios de computadoras y los administradores utilizan una gran variedad de técnicas de seguridad para protegerse:

1. Restricciones al acceso Físico: Esta consiste en la aplicación de barreas y procedimientos de control , como medidas de prevención y contramedidas ante amenazas a los recursos de información confidencial.

ALGUNOS MECANISMOS DE SEGURIDAD

- Intercambio de autenticación: corrobora que una entidad, ya sea origen o destino de la información, es la deseada. (Ej. Certificados)

- Cifrado: garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados. (Ej. 3DES)

- Integridad de datos: este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, para verificar que los datos no han sido modificados. (Ej. Funciones Hash)

- Firma digital: este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos ordinarios. (Ej. E-facturas)

- Control de encaminamiento: permite enviar determinada información por determinadas zonas consideradas clasificadas. (Ej. Líneas punto a punto, VPNs)

- Unicidad: consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. (Ej. fechado electrónico)