2011

TEMA 3: DNS

Álvaro Primo Guijarro

Servicios de red e Internet

12/12/2011

Contenido

Introducción a los servicios de nombres de dominio

Servicio de nombres de dominio

Introducción

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 cual 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.

Sistema 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

En Internet, la comunicación entre los equipos y los humanos se facilita por el hecho de que los primeros tienen asignado un nombre, de esta forma, recordamos más facil el nombre de una máquina ya que podemos asociar este a la organización o lugar en el que se encuentra, sin tener que memorizar la dirección de IP del equipo. Por ejemplo, pocos de nosotros sabemos que la máquina www.cnn.com tiene las direcciones de IP 207.25.71.22 (una de ellas).

Este concepto se conoce como Sistema de Nombres de Dominio, (DNS por sus siglas en inglés, Domain Name System), el cuál nació en la década de los 80's. Creado por Paul Mockapetris en conlaboración con Jon Postel de la Universidad del Sur de California y posteriormente, Paul Vixie. Juntos desarrollaron lo que hasta ahora conocemos como el DNS (BIND, Barkeley Internet Name Domain), un sistema cliente/servidor, distribuido y jerárquico, características que se describen a detalle en los RFC2 1033, 1034 y 1035 y que son muy parecidas a uns sistema de archivos de UNIX... pero distribuido.

Originalmente, el uso del DNS involucró solamente instituciones académicas, de investigación y por supuesto, la milicia de los EEUU. Eran los tiempos en que las universidades empezaban a realizar su conexión a las múltiples redes, entre ellas BitNet. Algo empezaba a trascender y era importante establecer un orden en cuanto a los equipos que ingresaban a la red.

Se crearon entonces los nombres de dominio genéricos de primer nivel (gTLD=generic Top-level Domain), .com, .net y .org, es decir, se habían creado estas tres clasificaciones con el fin de ubicar el tipo de entidades que buscaban tener presencia en Internet. Además de estos gTLD se empezó por delegar los sufijos nacionales (nTLD=national Top-level Domain) a los países que se fueran conectando a la red. De esta forma, a México se le asigno el .mx a finales

de 1988 cuando el ITESM, Campus Monterrey se conecta de manera dedicada al Internet, este nTLD empieza a operar desde 1ro. de Febrero de 1989. Así cada país obtuvo su propio nTLD, incluso EEUU, el cual tiene el .us. También existen unos nombres de dominio especiales, sTLD, que son sólo para los EEUU: .mil, .edu y .gov3.

Las organizaciones que administran los nTLD por lo general son instituciones académicas, como es el caso del .mx y el ITESM, sin embargo el caso de los gTLD es diferente, estos originalmente fueron administrados por el Stanford Research Institute Network Information Center (SRI-NIC), de la Universidad de Stanford en Menlo Park, California, pero pronto cambiaría a InterNIC.

En 1992, la Fundación Nacional de Ciencias de los EEUU (NSF, National Science Foundation) quien administraba el backbone de Internet (en ese entonces NSFNET) decide licitar la operación del InterNIC y en 1993, através de un convenio de cooperación, le otorga esta función a la empresa Network Solutions Inc.(NSI), posteriormente, esta empresa sería adquirida por el grupo Science Application International Corporation, (SAIC), originario de San Diego y que se distingue por sus multimillonarios contratos federales (Agencia de Seguridad Nacional, CIA, Marina de los EEUU)

Cuando NSI obtuvo el contrato, se estableció un apoyo de cuatro millones USD por parte de la NSF a NSI, para realizar la función del registro de los gTLD. No obstante, en 1994, el grupo SAIC compra esta empresa y su experiencia en contratos federales le ayuda a re-negociar el contrato previo. De esta forma, logra que se empiece a cobrar $50 USD anuales por cada nombre de dominio, estableciendo que el 30% de estas cuotas se irían a un fondo de infraestructura administrado por la NSF.

Aqui empezaron los problemas, aunque la operación de NSI fue buena, en mi opinión, muchos consideraban que el servicio debía mejorarse, tomando en cuenta las utilidades que esta empresa percibía por la operación de InterNIC. De hecho, este margen de utilidad le permitió a NSI empezar a cotizarse en la bolsa (NASDAQ: NSOL).

Para mediados de 1996, Jon Postel, el director del Internet Assignet Numbers Authority (IANA), y organismo administrador de las direcciones de IP y nombres de dominio, realizó una propuesta en la que contemplaba la creación de 150 nuevos nombres de dominios genéricos, gTLD, así como el .com, .net y .org. Esta propuesta pronto tuvo efectos importantes y finalizó en la formación de un grupo que se encargaría de discutir el re-diseño de los gTLD.

De esta forma, en Noviembre de 1996 nació el Internet-International Ad Hoc Committee (IAHC) impulsado por la Internet Society (ISOC), a los tres meses de haberse creado se generó el reporte final, en donde se planteaban las recomendaciones y requerimientos para un nuevo esquema de gTLD, este documento recibiría el nombre de Memorando de Entendimiento para los Nombres de Dominio genéricos de Nivel Superior.

El IAHC se disolvió en Mayo del 97 para dar paso al generic Top level Domain Memorandum of Understanding (gTLD-MoU), documento respaldado por organizaciones de todo el mundo,

entre ellas la Organización Mundial de la Propiedad Industrial (WIPO), Union Internacional de Telecomunicaciones (ITU), Internet Society , MCI y por Latino América sólo NIC-México. En este documento se plasman los acuerdos alcanzados durante esos ocho meses de discusión y consenso, en los que por cierto no estuvo ningún representante del gobierno de país alguno.

Todo marchaba sobre ruedas, el gTLD-MoU contemplaba nuevos gTLD (.firm, .shop, .web, .arts, .rec, .info, .nom, una administración múltiple y distribuída de los gTLD, por ejemplo, que más de una organización pudiera registrar nombres de dominio bajo .com, la creacion de un consejo central (CORE, Council of Registrars) formada por las organizaciones que fungirían como nuevos InterNICs, y dos cuerpos más de soporte al nuevo esquema, Policy Advisory Group (PAB) y el Policy Oversigt Committee (POC). Así mismo, se contemplaba en esta propuesta un esquema que permitiera cambiar de registro, es decir, portabilidad de los nombres de dominio, esto aseguraba, según el gTLD-MoU, que todos los registros dieran un servicio de calidad.

Así, el nuevo esquema requería de un inversión para el complejo sistema que debería consolidar la información de los 89 registros aceptados. Para esto CORE estableció una contrato con Emergent Corp para el desarrollo del nuevo esquema distribuido de DNS (new DNS Shared Registry System). Todo estaba listo pues, para que en Marzo de 1998 empezaran a operar los 89 registros en todo el mundo, aceptando asi solicitudes de dominio bajo los siete nuevos nombres de dominio genéricos.

El 30 de Enero, menos de dos meses antes de la fecha de inicio de operaciones del gTLD-MoU, el Gobierno de los Estados Unidos hace acto de presencia, en algo que parecia no apto para políticos. A través del Departamento de Comercio (DoC) publica un documento, conocido como Green Paper, en el cual, Ira Magaziner, asesor de Bill Clinton establece la postura de la Casa Blanca en materia de nombres de dominio. No pasaron muchas horas para que los principales actores de la industria enviaran sus comentarios al DoC expresando su desacuerdo.

En resumen, este documento desconocía la autoridad y el consenso del gTLD-MoU y por lo tanto de las organizaciones que lo representaban, a pesar de que el CORE ya estaba listo para iniciar operaciones. Su propuesta era esperar y planear mejor las cosas, como si veinte meses no hubieran sido suficientes en un medio ambiente tan dinámico como es Internet, y se concretaba a proponer una nueva organización que supliera al IANA en la coordinación de los gTLD y direcciones de IP para empezar funciones el 30 de Septiembre de 1998.

Este hecho provocó una cantidad impresionante de comentarios en contra del Green Paper, los cuales según el DoC, se tomarían en cuenta para generar una inciativa global. Así, el 5 de Junio de 1998, el Gobierno de los EEUU, através del DoC emitió un documento conocido como White Paper, en el cual, practicamente se retractaban de algunos aspectos que habían planteado originalmente en el Green Paper.

Aunque no tan polémico como el anterior, este documento era de alguna forma los planteamientos finales del Gobierno de los EEUU para realizar la transición en la administración de Internet. A grandes rasgos, se limitaba a buscar una nueva organización central que supliera al IANA, de hecho se buscaba que fuera privatizada (sin fondos del gobierno) pero que fuera sin fines de lucro. Los aspectos en la generación de nuevos nombres

de dominio genéricos, gTLD, se dejaban a consideración de esta nueva organización, conocida ahora como el Nuevo IANA (nIANA).

El tiempo cada vez era más corto, por lo que surgieron organizaciones que buscaban acelerar las decisiones necesarias para el lanzamiento del nIANA. Entre ellas, una organizacción con las siglas GIAW, que posteriormente fue IFWP, (International Forum for the White Paper). Fue esta organización quien se encargo de realizar la primer consulta para discutir puntos escenciales en el cumplimiento del White Paper, y le llamó la consulta de las Américas, la cual tuvo lugar en Reston VA, EEUU. A pesar del enfoque continental que se intentó darle, sólo hubo tres representantes de América Latina, CABASE de Argentina y NIC-México.

A esta reunión le siguieron otras convocadas por la Asociación de ISP en Europa (EuroISPA) y por la Comission Europea en Bruselas Bélgica, teniendo como resultado un consenso más global, representativo del continente europeo.

Es un hecho que el actual staff del IANA se mantendrá de manera operativa en el nIANA, sin emabrgo esto no es materia de discusión. Lo que se pretende definir es la estructura del nIANA. Se ha hablado de tres cuerpos que se encargarían de las direcciones de IP, los nombres de dominio de primer nivel TLD y los protocolos, respectivamente, además de un cuarto, en el que estarían representados los intereses de los primeros tres, así como de los principales grupos de interés (stakeholders) de Internet (usuarios, ISPs, etc).

La segunda reunión convocada por el IFWP fue sostenida en Ginebra, Suiza, en el marco del INET'98, una serie de eventos que realiza la ISOC anualmente. De todas las reuiones, esta ha sido sin duda la más representativa, con participantes latinos y africanos, inclusive. Se busca que haya una tercera reunión en Singapur, para escuchar las propuestas de Asia-Pacífico.

El resultado de estas reuniones de trabajo dará la pauta en el establecimientos de las reglas que aplicarán a Internet en los próximos años. Es imperativo que los stakeholders se involucren de manera activa en estos procesos y colaboren en la definición de lo que hoy día es su negocio.

Servidores de nombres de dominio (DNS)

Zonas

Zona de Búsqueda Directa.- Las resoluciones de esta zona devuelven la dirección IP correspondiente al recurso solicitado; este tipo de zona realiza las resoluciones que esperan como respuesta la dirección IP de un determinado recurso.

Zona de Búsqueda Inversa.- Las resoluciones de esta zona buscan un nombre de recurso en función de su dirección IP; una búsqueda inversa tiene forma de pregunta del estilo "¿Cuál esel nombre DNS del recurso de red que utiliza una dirección IP dada?".

Autoridad

Los registros de **comienzo de autoridad SOA** ("Start of Authority record"), marcan el comienzo de un dominio (una zona), suelen ser el primer registro de cada dominio en un Servidor de Nombres de Dominio y contienen una serie de datos sobre la zona que se muestran a continuación:

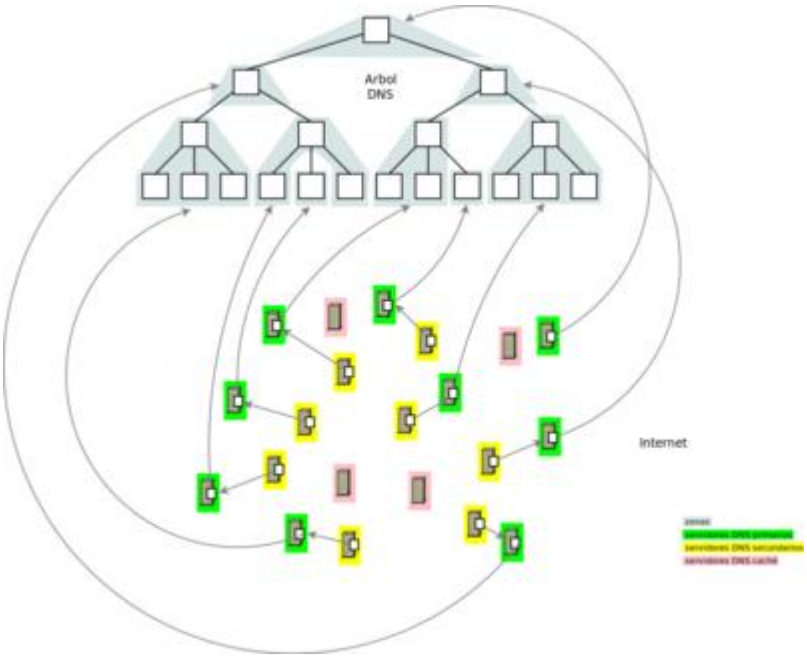
- **MNAME** Nombre de dominio del servidor DNS constituido como servidor primario para la zona.
- **RNAME** Nombre de dominio que indica la dirección de correo de la persona responsable de la zona.
- **SERIAL** Número entero de 32 bits correspondiente a la copia original de la zona. Este valor se y crementa con cada actualización, se conserva en las transferencias de zona, y puede ser utilizado como verificación.
- **REFRESH** Número de 32 bits representando el intervalo de tiempo antes que la zona deba ser actualizada.
- **RETRY** Número de 32 bits representando el intervalo de tiempo que debe consentirse antes de establecer que una petición de actualización ha fallado.
- **EXPIRE** Número de 32 bits que especifica el límite máximo de tiempo que puede transcurrir antes que la zona deje de ser "autoridad".
- **MINIMUM** Número entero de 32 bits señalando el valor mínimo del parámetro TTL que debe ser utilizado para cualquier exploración de la zona.

Registro de recursos RR

Los datos asociados con cada dominio de nombres está contenida en los llamados registro de recursos (resource records) o simplemente RR. Los RR describen todos los hosts en la zona y marca toda delegación de subdominios.

Los archivos que los servidores de nombres primarios utilizan son llamados archivos de datos (data files). Estos archivos de datos contienen registro de recursos que describen la zona.

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)

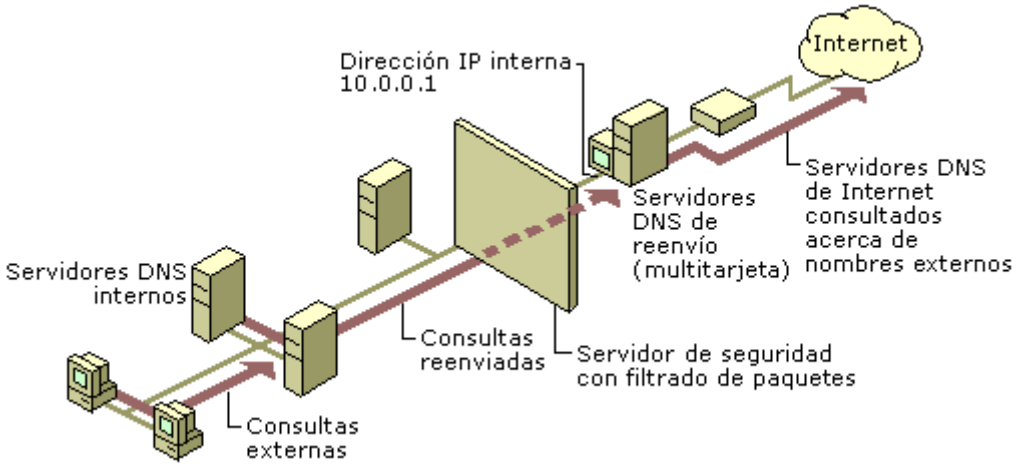
Un servidor de nombres secundario tiene autoridad sobre una zona, pero obtiene la información de esa zona copiandola de un servidor primario utilizando un proceso llamado **transferencia de zona**. Para permanecer sincronizado, los servidores de nombres secundarios consultan a los primarios regularmente (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.

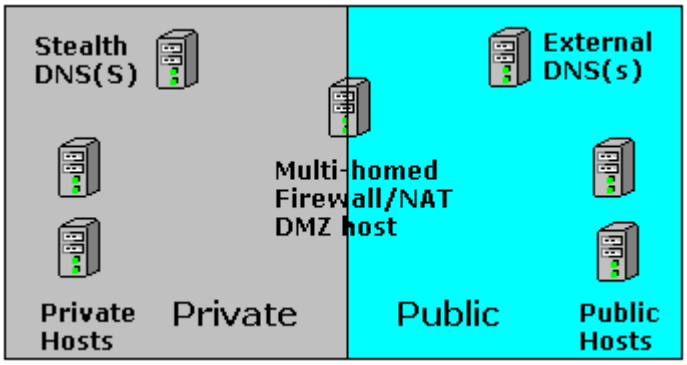
Servidor de nombre stealth / DMZ / SPLIT

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 servidores DNS

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

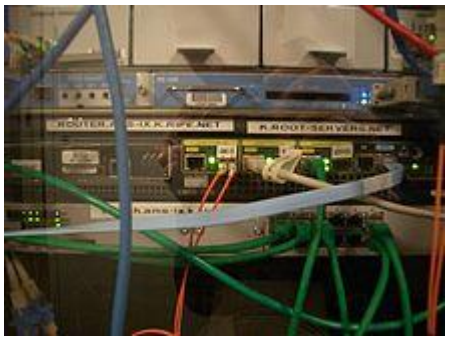
BIND (*Berkeley Internet Name Domain*, anteriormente : *Berkeley Internet Name Daemon*) es el servidor de DNS más comúnmente usado en Internet, especialmente en sistemas Unix, en los cuales es un Estándar de facto. Es patrocinado por la Internet Systems Consortium. BIND fue creado originalmente por cuatro estudiantes de grado en la University of California, Berkeley y liberado por primera vez en el 4.3BSD. Paul Vixie comenzó a mantenerlo en 1988 mientras trabajaba para la DEC.

DUAL 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

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

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).

PROTOCOLO DNS

El DNS (Domain Name System) o *Sistema de Nombres de Dominio* es una base de datos jerárquica y distribuida que almacena información sobre los nombres de dominio de redes cómo Internet.

Este protocolo se utiliza para poder recordar de manera sencilla las direcciones **IP.**

Gracias a los nombre de dominio 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.

Es un sistema jerárquico y distribuido que permite traducir nombres de dominio en direcciones IP y viceversa.

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 causaria estragos a nivel mundial.

Estos servidores dice que dominios de primer nivel existen y cuales 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 réplicas del primario.

DNS Dinámico (DDNS o Dynamic DNS)

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.

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.

TRANSFERENCIAS DE ZONA

Una transferencia de zona es el término utilizado para hacer referencia al proceso mediante el que el contenido de un archivo de zona DNS se copia desde un servidor DNS principal a un servidor DNS secundario.

Se producirá una transferencia de zona durante cualquiera de los siguientes escenarios:

- Al iniciar el servicio DNS en el servidor DNS secundario.
- Cuando caduca el tiempo de actualización.
- Cuando se guardan los cambios en el archivo de zona principal y hay una notificación lista.

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.

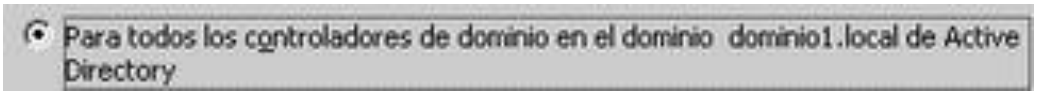
Debido al importante papel que desempeñan las zonas en DNS, se pretende que éstas estén disponibles desde varios servidores DNS en la red para proporcionar disponibilidad y tolerancia a errores al resolver consultas de nombres. En caso contrario, si sólo se utiliza un servidor y éste no responde, se pueden producir errores en las consultas de nombres de la zona. Para que otros servidores alojen una zona, son necesarias transferencias de zona que repliquen y sincronicen todas las copias de la zona utilizadas en cada servidor configurado para alojar la 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.

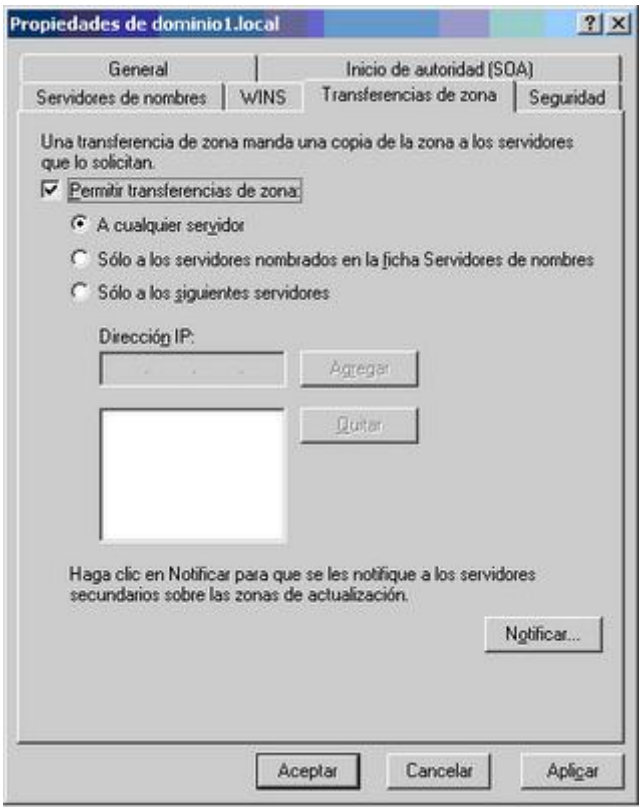


Una vez creada la zona, también se puede configurar para que esta sea transferida a otros servidores DNS, usando zonas secundarias, stub o como hemos visto anteriormente mediante la opción de tenerla almacenada en el directorio activo.

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)



Es decir si ya tenemos montado nuestro servidor, y queremos pasar el dns tendríamos que convivir con los dos controladores en nuestro escenario y propagar las DNS, de alguna de las maneras habladas en la entrada.

DNS DINAMICO

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.

Espacio de nombres de dominio:

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* , [1] 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 [nota 1] , 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.

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.

Procedimiento de registro

El procedimiento es el siguiente:

1.
    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)

2. 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.
3. 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:
    1. El registrador contacta con ICANN y realiza el proceso de forma transparente para el registrante.
    2. Se avisa al registrante que el dominio fue registrado.
4. 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.
5. La página ya es accesible mediante un nombre de dominio desde cualquier computadora.

Datos necesarios para registrar un dominio

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.

Algunos de 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
- SYNC

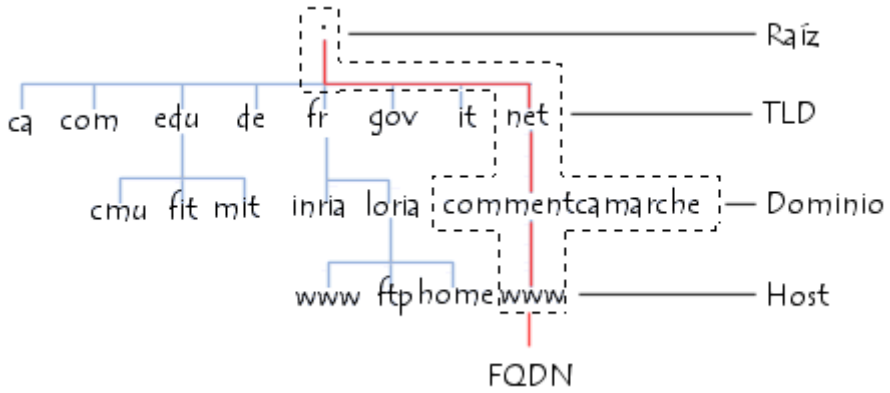
Componentes del servicio de nombres de dominio

Espacio de nombre

Un espacio de nombre jerárquico que permite garantizar la singularidad de un nombre en una estructura arbórea, como por ejemplo sistemas de archivo Unix.

Un sistema de servidores de distribución que permite que el espacio de nombre esté disponible.

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



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

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

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

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

El nombre absoluto está relacionado con todas las etiquetas de nodo de una estructura arbórea, separadas por puntos y que termina con un punto final que se denomina la dirección FQDN (Nombre de Dominio totalmente calificado). La profundidad máxima de una estructura arbórea es 127 niveles y la longitud máxima para un nombre FQDN es 255 caracteres. La dirección FQDN permite ubicar de manera única un equipo en la red de redes. Por lo tanto, es.kioskea.net. es una dirección FQDN.

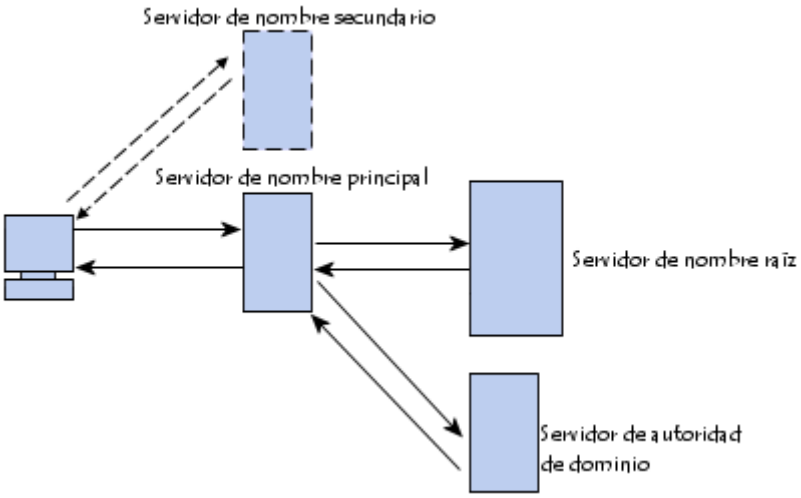
Resolución de nombres de dominio

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

Cuando una aplicación desea conectarse con un host conocido a través de su nombre de dominio (por ejemplo, "es.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).



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.primoguijarro.com	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:
  es.kioskea.net. IN MX 10 mail.commentcamarche.net.
- **NS:** es el servidor de nombres de dominio con autoridad sobre el dominio.
- **PTR:** es un puntero hacia otra parte del espacio de nombres del 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 de dominio

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 (resolutor – “resolvers”)

La resolución de nombres de DNS se produce cuando un resolutor, en un host, envía a un servidor de DNS un mensaje de solicitud con un nombre de dominio. El mensaje de solicitud indica al DNS que busque el nombre y devuelva ciertos RR. El mensaje de solicitud contiene el nombre de dominio a buscar y un código que indica los registros que se deben devolver.

Un cliente envía una solicitud de DNS pidiendo al servidor de DNS todos los registros A de kona.midominio.com. La respuesta a la solicitud contiene la entrada de solicitud y los RR de respuesta.

Resolución de alias

Si el resolutor intenta realizar resolución de nombres de un nombre que indique el usuario, no sabe a priori si el nombre se refiere a un RR (A) de host o a un CNAME. Si se refiere a un CNAME, el servidor puede devolver el CNAME. Sin embargo, en este caso, el CNAME debe resolverse todavía. Para evitar tráfico extra de DNS, cuando un servidor de DNS devuelve un CNAME en respuesta a una búsqueda de registro de host, el servidor de DNS también devuelve el registro A relativo al CNAME.

El cliente de DNS envía una solicitud de DNS al servidor de DNS solicitando el registro Host de nsl.midominio.com, que en realidad es un alias de kona.midominio.com. En la respuesta de DNS existen dos RR de respuesta. El primero es el RR CNAME de nsl.midominio.com, que contiene el nombre canónico. El segundo RR de respuesta es el registro Host de kona.midominio.com, que contiene la dirección de IP de este equipo.

Caché del resolutor de DNS

Un host de IP podría necesitar ponerse en contacto periódicamente con otro host y por tanto necesitaría resolver un nombre concreto de DNS muchas veces, como por ejemplo el nombre del servidor de correo electrónico. Para evitar tener que enviar solicitudes a un servidor de DNS cada vez que el host quiere resolver el nombre, Windows implementa una caché especial de información de DNS.

```
G:\>IPCONFIG /DISPLAYDNS

Configuración IP de Windows 2000

   localhost.
   ----------------------------------------
     Nombre de registro. . : localhost
     Tipo de registro . . .: 1
     Tiempo de vida  . . . : 31532890
     Longitud de los datos : 4
     Sección . . . . . . . : Answer
     Un registro (Host). . :
                     127.0.0.1


   1.0.0.127.in-addr.arpa.
   ----------------------------------------
     Nombre de registro. . : 1.0.0.127.in-addr.arpa
     Tipo de registro . . .: 12
     Tiempo de vida  . . . : 31532890
     Longitud de los datos : 4
     Sección . . . . . . . : Answer
     Registro PTR. . . . . :
                     localhost
```

El servicio Cliente de DNS hace caché de los RR recibidos en las respuestas a las solicitudes de DNS. La información se mantiene durante un Período de vida, TTL (Time To Live), y se puede utilizar para responder solicitudes posteriores. De forma predeterminada, la caché utiliza el valor de TTL recibido en la respuesta de solicitud de DNS. Cuando se resuelve una solicitud, el servidor autoridad de DNS en el dominio resuelto define el TTL para un RR dado.

Puede utilizar el comando IPCONFIG con la opción /DISPLAYDNS para mostrar el contenido actual de la caché del resolutor.

Caché negativa

El servicio Cliente de DNS también proporciona caché negativa. La caché negativa ocurre cuando no existe un RR de un nombre de dominio solicitado o cuando el propio nombre de dominio no existe, en cuyo caso se guarda la falta de resolución. La caché negativa evita repetir solicitudes adicionales de RR o dominios que no existen.

Si se realiza una solicitud a un servidor de DNS y la respuesta es negativa, las siguientes solicitudes al mismo nombre de dominio se responden negativamente durante un tiempo predeterminado de 300 segundos. Para evitar guardar en la caché información negativa anticuada, cualquier información de solicitud respondida negativamente se mantiene durante un período de tiempo inferior al que se utiliza para las respuestas positivas.

Con la caché negativa se reduce la carga en los servidores de DNS, pero estarán disponibles los RR relevantes, y se podrán enviar solicitudes posteriores para obtener la información.

Si se realiza una solicitud a todos los servidores de DNS y no está disponible ninguno durante un tiempo predeterminado de 30 segundos, las solicitudes posteriores por nombre fallarán inmediatamente en lugar de esperar los plazos. De esta forma se puede ahorrar tiempo en servicios que utilizan DNS durante el proceso de arranque, sobre todo cuando se arranca de la red.

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 por que l a 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 causaria 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.

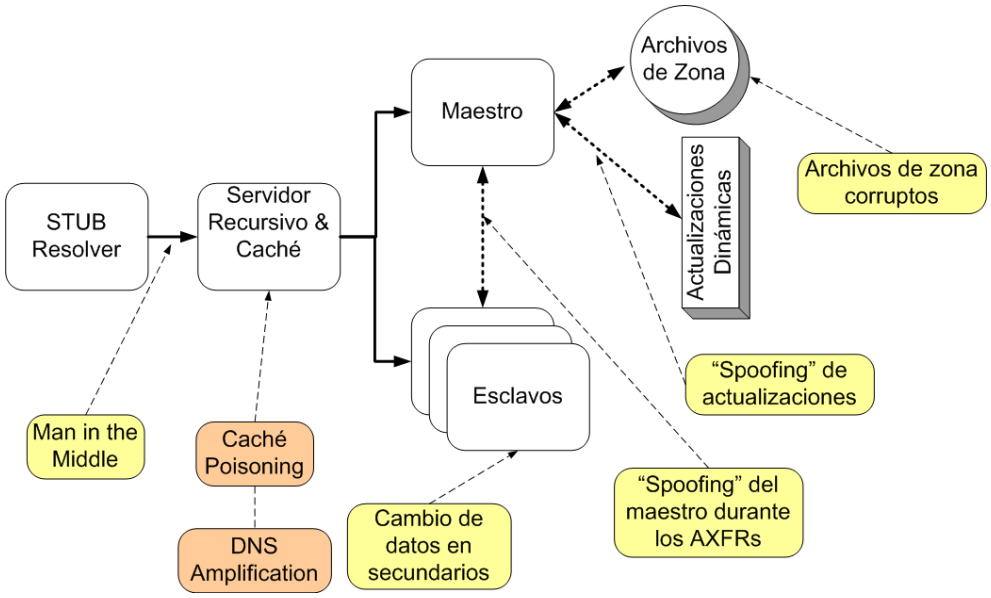
Cada componente de dominio incluyendo la raíz, tiene un servidor primario y varios secundarios. Todos tienen la misma autoridad para responder por ese dominio, pero el primario es el único sobre el que se pueden hacer modificaciones de manera que los secundarios son reaplicas del primario.

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.

SEGURIDAD DNS

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

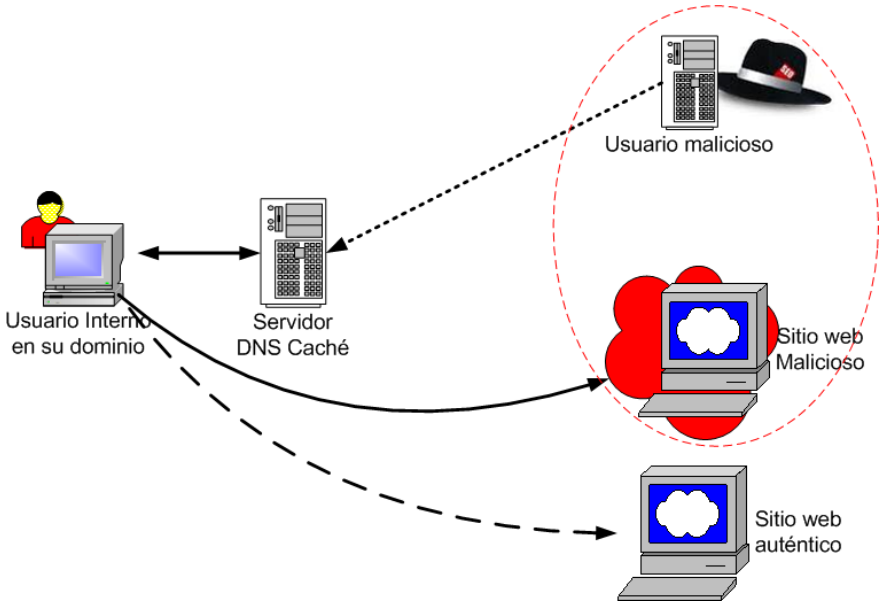
VULNERABILIDADES



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.

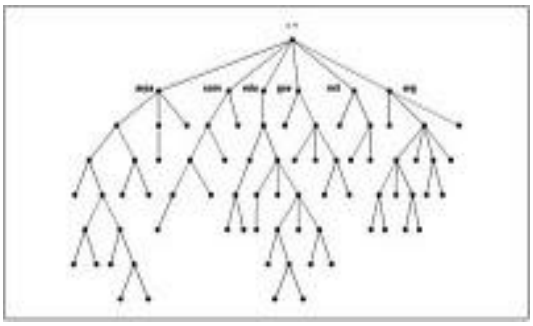
Son afectados los siguientes productos:
- Axis
- JH Software
- Sprint
- Cisco
- Juniper
- VeriSign
- DNRD
- Men & Mice
- WindRiver
- Hewlett-Packard
- MyDNS
- JDNSS
- Posadis

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

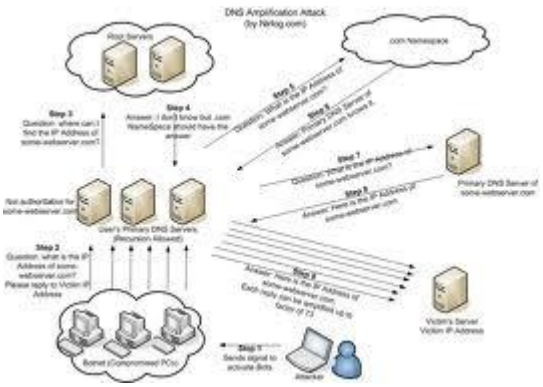
Éstas son las formas comunes en que los intrusos pueden amenazar su infraestructura DNS:

- 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.

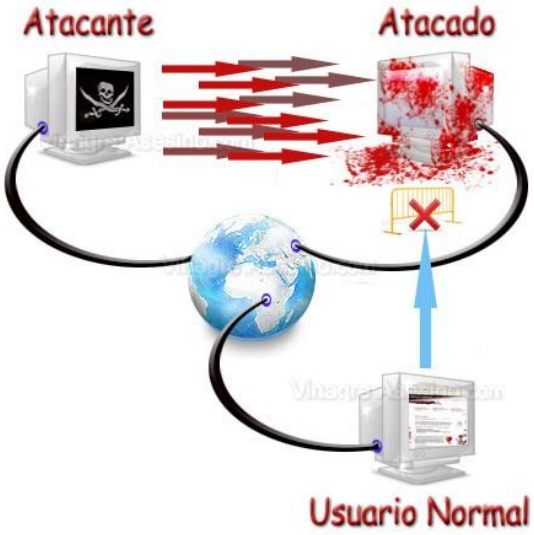
- La redirección se produce cuando un intruso puede redirigir consultas de nombres DNS a servidores que él controle. Un método de redirección incluye el intento de contaminar la caché DNS de un servidor DNS con datos DNS erróneos que pueden dirigir consultas futuras a servidores que controle el intruso. 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.



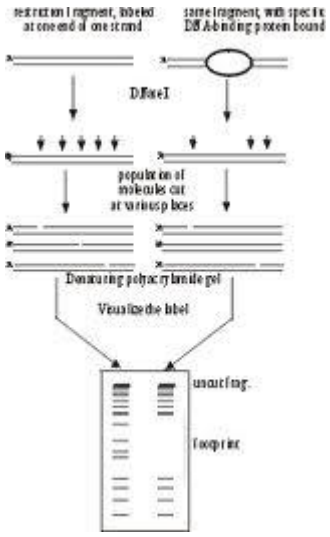
ATAQUES

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

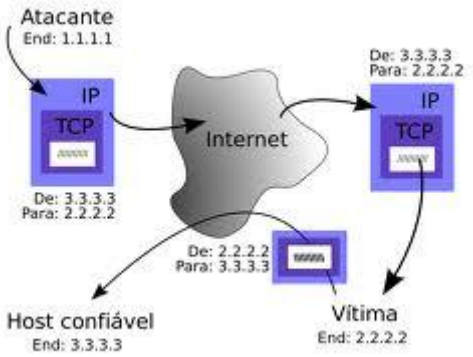
- **Ataque de negación del servicio (DOS):** este ataques se presenta cuando el servidor DNS se ve inundado con un número muy grande de requerimientos reconocidos que pueden eventualmente forzar al procesador a ser usado más allá de sus capacidades recordemos que un procesador Pentium dos de 700 MHz 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)