INSTALACIÓN Y ADMINISTRACIÓN DE SERVICIOS DE NOMBRES DE DOMINIO

MARÍA ÁNGELES PEÑASCO SÁNCHEZ- 2º ASIR- DNS

ÍNDICE

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.

Introducción a los servicios 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.

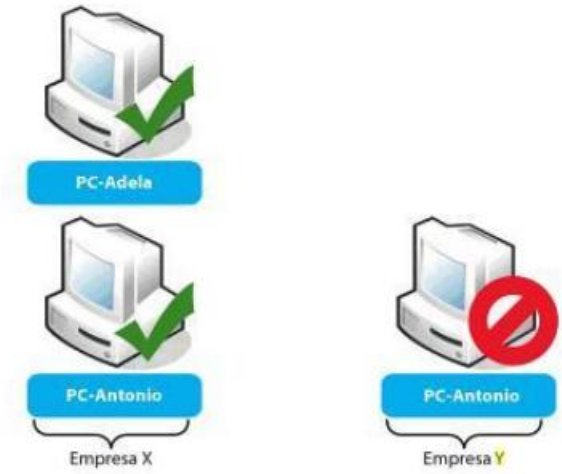
Un Servidor de Nombres de Domino es una máquina cuyo cometido es buscar a partir del nombre de un ordenador la dirección IP de ese ordenador; y viceversa, encontrar su nombre a partir de la dirección IP.

Sistemas de nombres planos y jerárquicos.

La razón de ser de un sistema de nombres en Internet es la de posibilitar la asociación de un determinado nombre que identifica a un ordenador, por ejemplo, pc-antonio a la dirección IP de ese ordenador: 157.22.52.2. Un sistema de nombres, en términos generales, es por lo tanto eso: un mecanismo que permite traducir un nombre a una dirección que permite localizar un determinador ordenador.

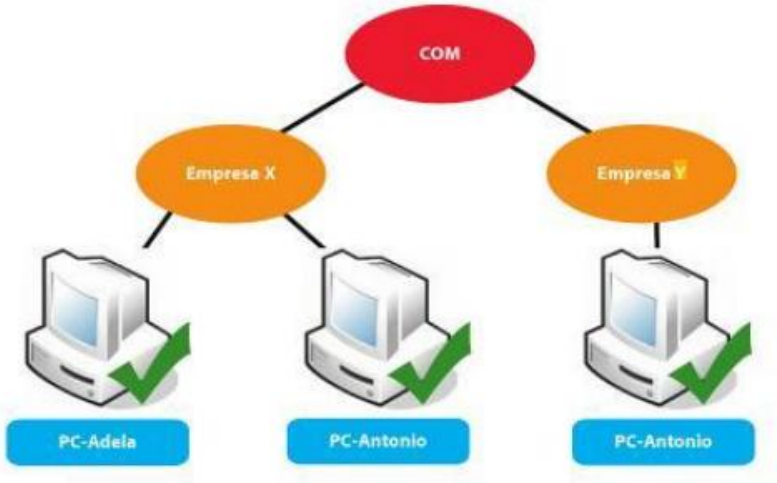
En general, podemos clasificar los sistemas de nombres en dos grandes grupos:

- Sistemas de nombres planos: son aquellos en los que no hay ninguna jerarquía que permita clasificar un nombre (y por tanto un ordenador) dentro de una categoría (categoría podría ser una ubicación geográfica o. por ejemplo, la pertenencia de ese ordenador al departamento de ventas frente al de contabilidad). El número de DNI de una persona es un ejemplo de sistema de nombres plano: el número de DNI permite identificar a una persona pero este número no indica dónde vive esa persona.



Sistema plano: no pueden existir dos pc-antonio.

- Sistemas de nombres jerárquicos: son aquellos en los que existe una jerarquía a la hora de construir el nombre completo de ese ordenador. En este caso, al leer el nombre completo de un ordenador, se puede determinar su ubicación geográfica en el mundo o a qué departamento pertenece dentro de la empresa. Por ejemplo, la dirección postal de una persona es un ejemplo de sistema de nombres jerárquico: en una carta siempre debe aparecer el país, la provincia, la población, la calle, etc., eso permite identificar a una persona, distinguirla de otra que se llama igual pero que vive en otro sitio, e incluso ubicarla geográficamente.



Sistema jerárquico: pueden existir dos pc-antonio.

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 fácil 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 colaboración 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 unos sistema de archivos de UNIX... pero distribuido.

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.

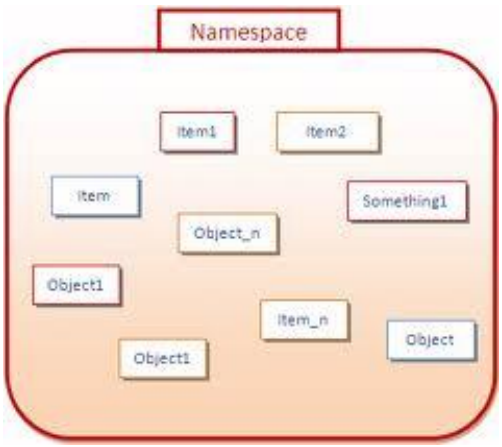
Componentes del servicio de nombres de dominio

–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:

      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 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.

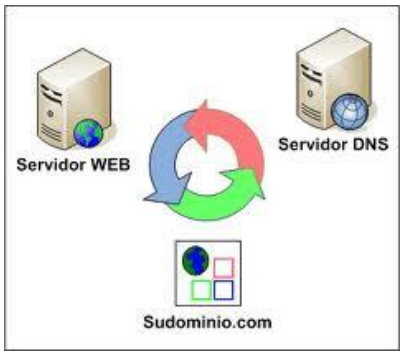
Cada servidor de nombre de dominio está especificado en el servidor de nombre de dominio en el nivel superior inmediato, lo que significa que la autoridad sobre los dominios puede delegarse implícitamente. El sistema de nombre es una arquitectura distribuida, en donde cada entidad es responsable de la 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 System Consortium).



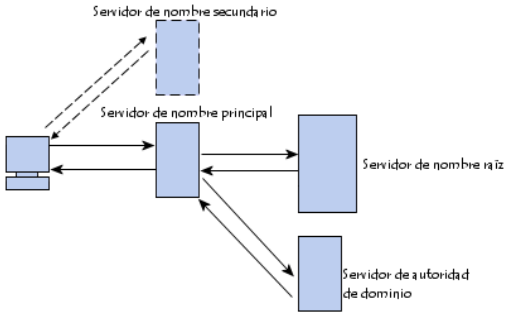
–Clientes DNS (resolutores – “resolvers”)

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.

Espacio de nombres de dominio

–Nombres de dominio.

El Sistema de nombres de dominio (DNS) se definió originalmente en los RFC 1034 y 1035. Estos documentos especifican elementos comunes a todas las implementaciones de software relacionadas con DNS, entre los que se incluyen:

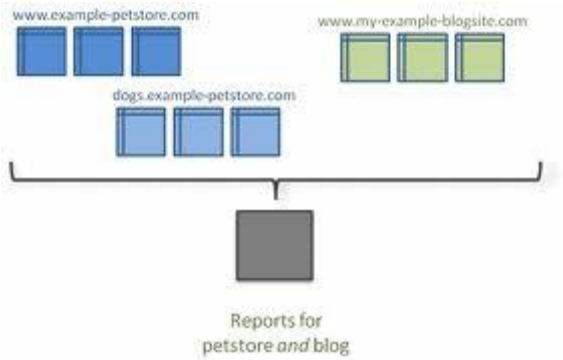
- Un espacio de nombres de dominio DNS, que especifica una jerarquía estructurada de dominios utilizados para organizar nombres.
- Los registros de recursos, que asignan nombres de dominio DNS a un tipo específico de información de recurso para su uso cuando se registra o se resuelve el nombre en el espacio de nombres.
- Los servidores DNS, que almacenan y responden a las consultas de nombres para los registros de recursos.
- Los clientes DNS, también llamados solucionadores, que consultan a los servidores para buscar y resolver nombres de un tipo de registro de recursos especificado en la consulta.

–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 Domain 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.



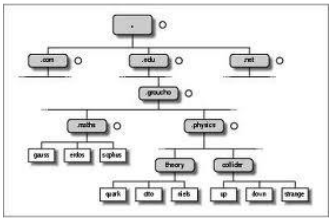
–Nombres relativos y absolutos. FQDN.

Los nombres de dominio absolutos terminan con “.” 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 sí “.”, 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.



–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:

- 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.

- Dominios 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.

- Registros 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.

Servidores de nombres de dominio (DNS)

–Zonas. Autoridad. Registro de recursos (RR).

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 es el 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 incrementa 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 de nombres DNS.

- Servidor maestro o primario.

El servidor primario es la fuente autorizada de toda la información acerca de un dominio específico. Él carga la información de un archivo mantenido localmente por el administrador. Este archivo (archivo de zona) contiene la información más precisa acerca de una porción de la jerarquía de dominios sobre la cual el servidor tiene autoridad. La configuración de un servidor primario requiere un conjunto de archivos: archivos de zona para el dominio regular y para el dominio reverso, el archivo de configuración del servidor, el archivo de cache y el archivo loopback.

- Servidor esclavo o secundario.

Un servidor secundario transfiere un conjunto completo de información de dominio desde el servidor primario. El archivo de zona es transferido desde el servidor primario y es guardado como un archivo local de disco (a esta operación se le llama transferencia de zona). Solamente se requieren el archivo de inicio, el archivo de cache y el archivo loopback. Un servidor secundario es considerado también primario ya que tiene una copia exacta de los archivos del servidor primario, lo cual lo hace autoridad.

- Servidor caché.

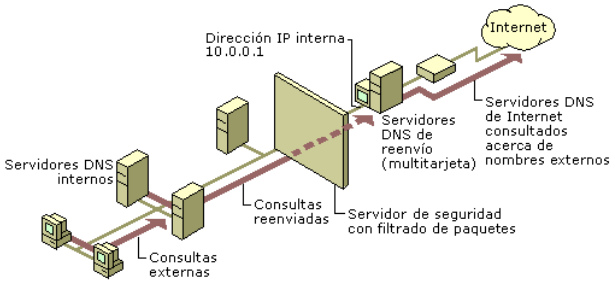
Un servidor de sólo cache corre el software del servidor, pero no tiene los archivos de base de datos del servidor. Aprende las respuestas de otros servidores de nombres, la guarda y la usa para responder preguntas futuras sobre esa misma información. Solamente requiere de un archivo de cache (con información acerca de los root servers a los cuales debe preguntar). Se dice que este tipo de servidor no es autoritario ya que la información que obtiene es de segunda mano. El archivo de configuración del servidor mantiene los parámetros de funcionamiento, apuntadores a los archivos de datos del dominio y direcciones de servidores remotos.

- Servidor reenviador (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 del 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.



- Servidor solo autorizado.

Los servidores DNS especificados mediante este procedimiento se agregan a las direcciones IP de los servidores presentes en el registro de recursos del servidor de nombres (NS) existente de la zona. Normalmente, sólo tiene que ejecutar este procedimiento en la zona principal al agregar servidores DNS para que actúen como servidores secundarios y también para especificar que se reconozcan estos servidores como autorizados cuando se responda a consultas de los datos de la zona.

–Software comercial de servidores de nombres de dominio.

Simple DNS Plus

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.

–Servidores 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)

Resolutores de DNS

En Windows 2000, el resolutor de DNS es un componente del sistema que realiza solicitudes de DNS a otro u otros servidores de DNS. La pila de TCP/IP de Windows 2000 se configura, normalmente, con la dirección de IP de al menos un servidor de DNS al que el resolutor envía una o más solicitudes de información de DNS.

En Windows 2000, el resolutor forma parte del servicio Cliente de DNS. Este servicio se instala automáticamente cuando se instala TCP/IP y se ejecuta como parte del proceso Services.Exe. Como la mayoría de los servicios de Windows 2000, el servicio Cliente de DNS se activa en el dominio System de Windows 2000.

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 2000 implementa una caché especial de información de DNS.

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.

Proceso de resolución de un nombre de dominio

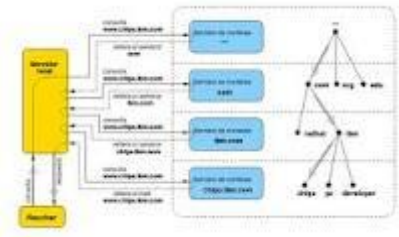
–Consultas recursivas.

En las resoluciones recursivas, el servidor no tiene la información en sus datos locales, por lo que busca y se pone en contacto con un servidor DNS raíz, y en caso de ser necesario repite el mismo proceso básico (consultar a un servidor remoto y seguir a la siguiente referencia) hasta que obtiene la mejor respuesta a la pregunta.

Cuando existe más de un servidor autoritario para una zona, Bind utiliza el menor valor en la métrica RTT para seleccionar el servidor. El RTT es una medida para determinar cuánto tarda un servidor en responder una consulta.

El proceso de resolución normal se da de la siguiente manera:

1. El servidor A recibe una consulta recursiva desde el cliente DNS.
2. El servidor A envía una consulta recursiva a B.
3. El servidor B refiere a A otro servidor de nombres, incluyendo a C.
4. El servidor A envía una consulta recursiva a C.
5. El servidor C refiere a A otro servidor de nombres, incluyendo a D.
6. El servidor A envía una consulta recursiva a D.
7. El servidor D responde.
8. El servidor A regresa la respuesta al resolver.
9. El resolver entrega la resolución al programa que solicitó la información.



–Consultas iterativas.

Las resoluciones iterativas consisten en la respuesta completa que el servidor de nombres pueda dar. El servidor de nombres consulta sus datos locales (incluyendo su caché) buscando los datos solicitados. El servidor encargado de hacer la resolución realiza iterativamente preguntas a a los diferentes DNS de la jerarquía asociada al nombre que se desea resolver, hasta descender en ella hasta la máquina que contiene la zona autoritativa para el nombre que se desea resolver.

–Caché y TTL.

Cada vez que un servidor de nombres envía una respuesta, lo hace adjuntando el tiempo de validez de la misma (TTL o "tiempo de vida"). Esto posibilita que el receptor, antes la necesidad de volver a resolver la misma consulta, pueda utilizar la información previamente obtenida en vez de realizar un nuevo requerimiento.

Esta es la razón por la cual los cambios realizados en el DNS no se propagan instantáneamente a través del sistema. Dependiendo de la naturaleza de los mismos (y de la configuración de cada servidor), la propagación puede tardar desde algunos minutos hasta varios días. Correo electrónico y resolución de nombres

–Recursividad y caché.

Aunque es cierto que algunas configuraciones de servidor de nombres recursivo-son (descuidada) denominado "caché", por ejemplo, RHEL / Fedora / CentOS, que es un nombre muy malo para esa función - ya que el almacenamiento en caché es ortogonal a la recursividad.

Teóricamente, se podría escribir un servidor de nombres que hace servicio recursivo, pero no caché sus resultados. (Eso sería un poco perverso, y yo no sé de ninguna.) Por el contrario, los paquetes de servidor de nombres caché, pero que no saben nada acerca de cómo recurse y en lugar de hacer menos útil servicio interactivo alternativas son comunes: dnsmasq, pdnsd, etc...

Resolución inversa

–Mapeo de direcciones y dominio arpa.

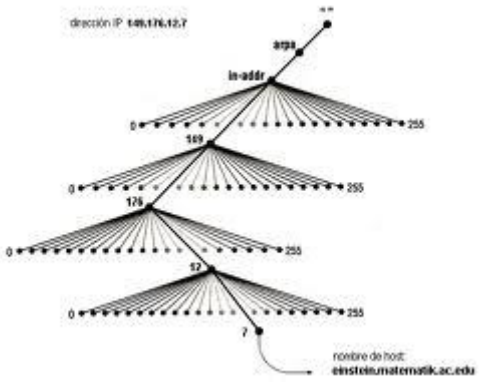
La resolución DNS más común es la hecha para traducir un nombre para una dirección IP, pero esa no es el único tipo de resolución DNS. Hay también la resolución denominada inversa, que hace la traducción de una dirección IP a un nombre.

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 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.



–Zonas de resolución inversa. Proceso de resolución.

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 y resolución inversa.

Hemos comentado que los dominios de primer nivel destinados a los países son gestionados por estos a su voluntad. Esto 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.

Registros de recursos DNS

–Formato general.

Formato de los registros de recursos DNS

Todos los registros de recursos tienen un formato definido que utiliza los mismos campos de nivel superior, según se describe en la tabla siguiente.

Campo	Descripción
Propietario	Indica el nombre de dominio DNS que posee un registro de recursos. Este nombre es el mismo que el del nodo del árbol de la consola donde se encuentra un registro de recursos.
Tiempo de vida (TTL)	Para la mayor parte de los registros de recursos, este campo es opcional. Indica el espacio de tiempo utilizado por otros servidores DNS para determinar cuánto tarda la información en caché en caducar un registro y descartarlo. En un registro de recursos individual, puede especificar un TTL específico para el registro que suplante el TTL mínimo (predeterminado) heredado del registro de recursos de inicio de autoridad. También se puede utilizar el valor cero (0) para el TTL en los registros de recursos que contengan datos volátiles que no estén en la memoria caché para su uso posterior una vez se complete la consulta DNS en curso.

Clase	Contiene texto nemotécnico estándar que indica la clase del registro de recursos. Por ejemplo, el valor "IN" indica que el registro de recursos pertenece a la clase Internet, que es la única clase que admite el DNS de Windows Server 2003. Este campo es obligatorio.
Tipo	Contiene texto nemotécnico estándar que indica el tipo de registro de recursos. Por ejemplo, el texto nemotécnico "A" indica que el registro de recursos almacena información de direcciones de host. Este campo es obligatorio.
Datos específicos del registro	Un campo de longitud variable y obligatoria con información que describe el recurso. El formato de esta información varía según el tipo y clase del registro de recursos.

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

SOA

El registro SOA (Start of Authority) es el segundo registro que nos encontramos en un archivo de zona. Debe haber uno (y solo uno) por cada archivo de zona directo o inverso que creemos.

Su sintaxis es:

- zona es o bien el nombre de la zona (¡terminado en punto!) o bien la letra @.
- Nombre DNS primario indica el FQDN del servidor donde está almacenado el archivo de zona (¡terminado en un punto!).
- Email Administrador es la dirección de email de la persona responsable de este dominio (la arroba se remplaza con un punto y la dirección entera también termina con un punto).
- Numero Serie indica el número de versión del archivo de zona. Sirve de referencia a los servidores DNS secundarios para saber cuando deben hacer una transferencia de zona. Si el número de serie del servidor secundario es menor que el número de serie del primario significa que este ha cambiado su información. Este número debe ser incrementado de forma manual por el administrador de red cada vez que realiza un cambio en el archivo de zona. Una costumbre es la de escribir los número de serie como AAAAMMDDNN, es decir 4 cifras para el año, 2 para el mes, 2 para el día y una o dos para el numero de revisión dentro de ese día (01, 02, etc.).
- actualización es el intervalo, en segundos, tras el cual los servidores secundarios deben comprobar el registro SOA del servidor primario, con el fin de verificar si la información del dominio ha cambiado. El valor típico es de una hora (3600).
- reintento especifica el tiempo que el servidor secundario espera antes de volver a intentar una transferencia de zona que haya fallado.
- caducidad es el tiempo en segundos tras el cual un servidor DNS secundario que no haya podido realizar transferencias de zona en todo ese tiempo descartará los datos que posee. El valor típico es de 42 días, o sea 3600000.
- TTL mínimo antiguamente (en versiones 8.3 de BIND y anteriores) establecía el tiempo de validez en segundos para permanecer en cachés de otros servidores o de resolvers. En la actualidad esto se consigue con la directiva $TTL, por lo que el valor indicado en este campo se ignora.

NS

Este tipo de registro representa o indica quienes son los servidores DNS con autoridad sobre esa zona, tanto maestros como secundarios. Por tanto, cada archivo de zona debe contener, como mínimo, un registro NS.

Su sintaxis es:

Dominio IN NS FQDNservidorDNS

Donde:

- dominio es el nombre de dominio completamente cualificado de la zona sobra la que tiene autoridad el servidor DNS que estemos especificando. Si esta zona coincide con la zona que se está definiendo en el archivo de zona, puede dejarse en blanco o escribir una @.
- FQDNservidorDNS es el nombre de dominio completamente cualificado del servidor DNS que estamos especificando.

A

El registro A establece una correspondencia entre un nombre de dominio completamente cualificado y una dirección IP.

Su sintaxis es:

nombreHost IN A IPcompleta

Donde:

- nombreHost es únicamente el nombre de un host de nuestro dominio.
- IPcompleta es la dirección IP de ese host.

CNAME

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

Su sintaxis es:

Alias IN CNAME nombreHost

Donde:

- alias es únicamente un nombre de host.
- nombreHost es únicamente el nombre de host indicado anteriormente en un registro A.

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 utiliza únicamente para resolución inversa.

Su sintaxis es:

IPsinParteDeRed IN PTR FQDNhost

Donde:

- IPsinParteDeRed es la parte de host de la dirección IP de la máquina escrita al revés.
- FQDNhost es el nombre de dominio totalmente cualificado del host (¡terminado en punto!).

MX

Este registro permite indicar cuáles son los servidores de correo de nuestro dominio. Además permite, en caso de tener varios servidores, establecer el orden de consulta o de preferencia. Este orden establece que los valores menores tienen más prioridad.

Su sintaxis es:

Dominio IN MX prioridad FQDNhost

Donde:

- dominio puede dejarse en blanco o usar la letra @.
- prioridad es un número entero que puede omitirse.
- FQDN-host es el nombre completamente cualificado del host que hará las funciones de servidor de correo para la zona que estamos definiendo.

–Delegación y Glue Record.

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 158.42.178.2

Transferencias de Zona

–Tipos de transferencias de zona: Completa e Incremental.

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.

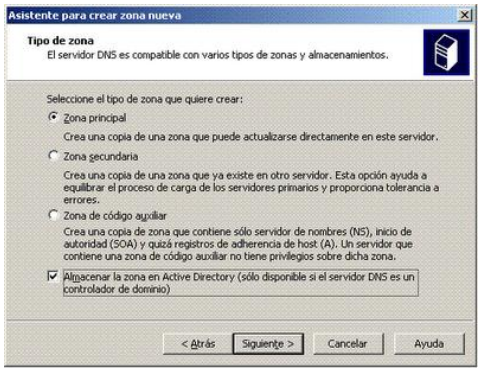
Debido al importante papel que desempeñan las zonas en DNS, se pretende que éstas estén disponibles desde varios servidores DNS en la red para proporcionar disponibilidad y tolerancia a errores al resolver consultas de nombres. En caso contrario, si sólo se utiliza un servidor y éste no responde, se 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.

–Proceso de transferencias de zona.

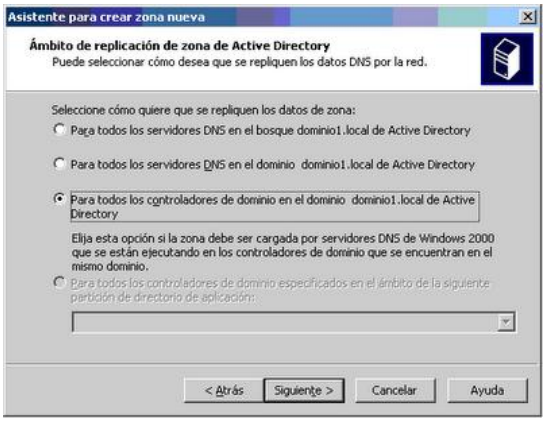
Almacenar la zona en active Directory (solo disponible si el servidor DNS es un controlador de dominio)

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)

DNS Dinámico (DDNS o Dynamic DNS)

–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.
Problemas:

- 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

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 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.

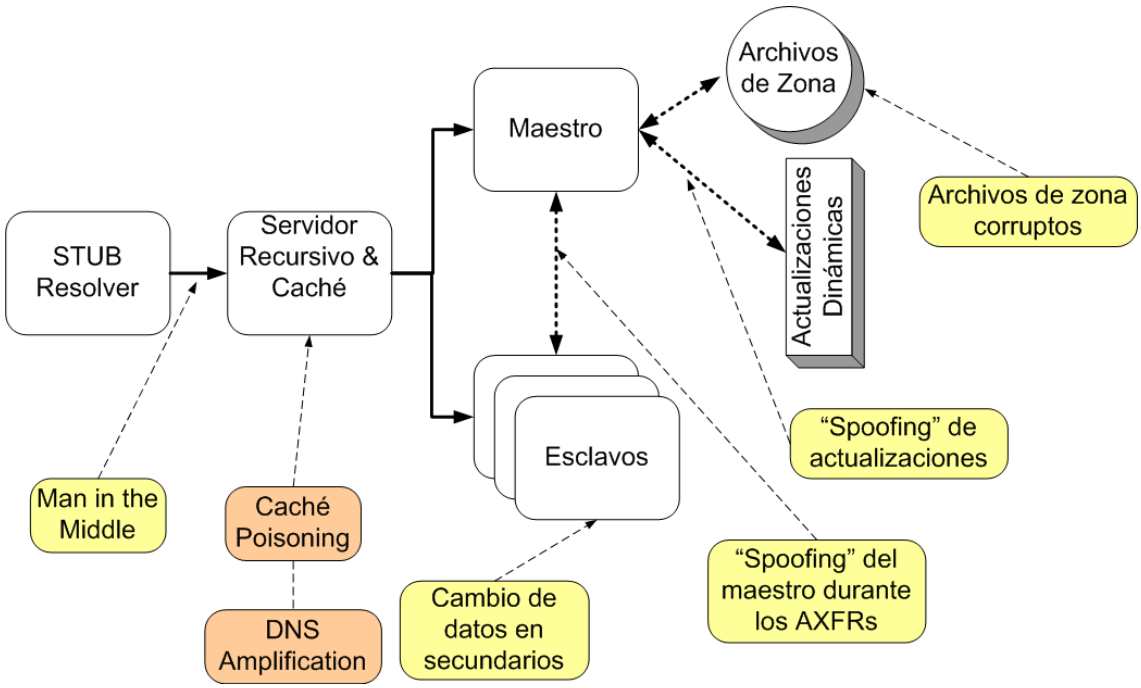
Cada componente de dominio incluyendo la raíz, tiene un servidor primario y varios secundarios. Todos tienen la misma autoridad para responder por ese dominio, pero el primario es el único sobre el que se pueden hacer modificaciones de manera que los secundarios son réplicas del primario.

Seguridad DNS

–Vulnerabilidades, amenazas y ataques.

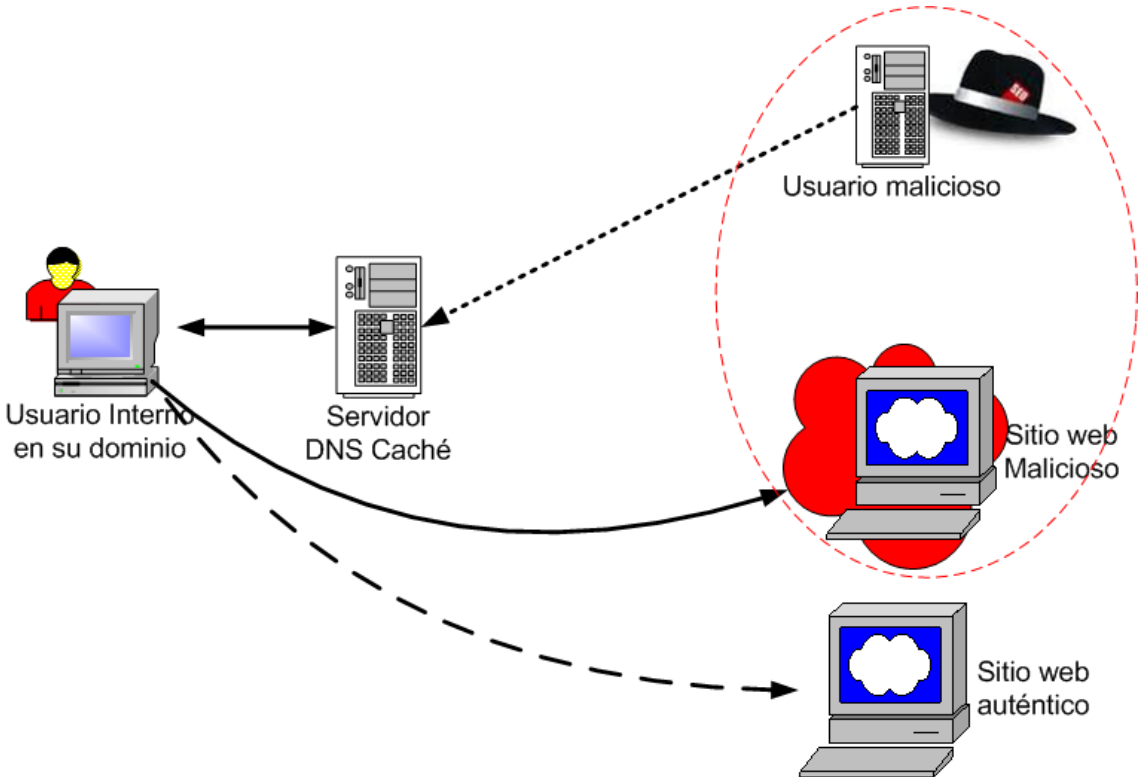
El sistema de nombres de dominio (DNS, *Domain Name System*) se diseñó originalmente como un protocolo abierto y, por tanto, es vulnerable a intrusos. El DNS de Windows Server 2003 ha mejorado su capacidad para impedir un ataque en la infraestructura DNS mediante la adición de características de seguridad

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.

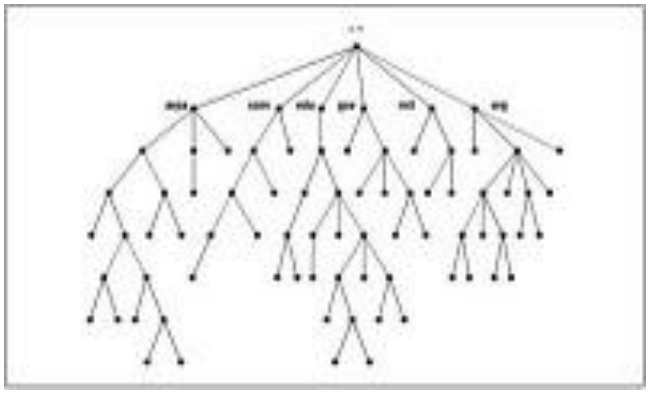
Son afectados los siguientes productos:
- Axis
- JH Software
- Sprint
- Cisco
- Juniper

- 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).

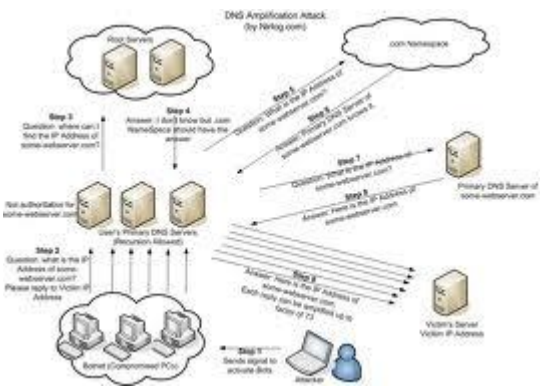


Éstas son las formas comunes en que los intrusos pueden amenazar su infraestructura DNS:

- 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.

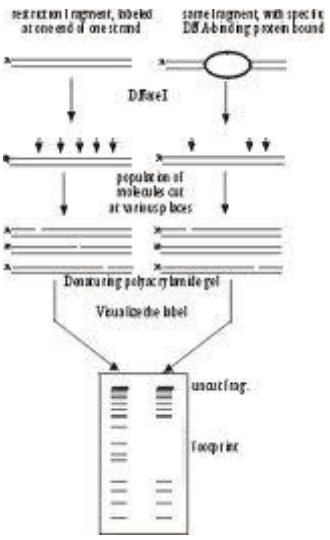


ATAQUES

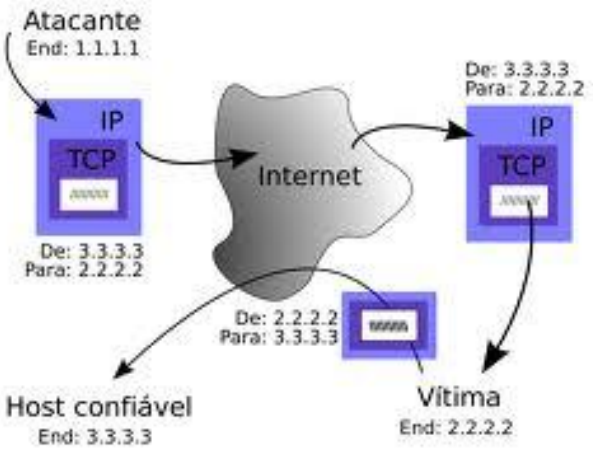
Algunos de los ataques más comunes que se presentan en un servicio de DNS son los siguientes:

- 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.

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)