UD 3: Instalación y administración de servicios de nombres de dominio.

Esperanza Elipe Jimenez

I.E.S.GREGORIO PRIETO 2º Asir 11/12

INDICE

Introducción de un servidor DNS

¿Qué hace un servidor DNS?

Un servidor DNS proporciona resolución de nombres para redes basadas en TCP/IP. Es decir, hace posible que los usuarios de equipos cliente utilicen nombres en lugar de direcciones IP numéricas para identificar hosts remotos. Un equipo cliente envía el nombre de un host remoto a un servidor DNS, que responde con la dirección IP correspondiente. El equipo cliente puede entonces enviar mensajes directamente a la dirección IP del host remoto. Si el servidor DNS no tiene ninguna entrada en su base de datos para el host remoto, puede responder al cliente con la dirección de un servidor DNS que pueda tener información acerca de ese host remoto, o bien puede consultar al otro servidor DNS. Este proceso puede tener lugar de forma recursiva hasta que el equipo cliente reciba las direcciones IP o hasta que se establezca que el nombre consultado no pertenece a ningún host del espacio de nombres DNS especificado.

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.

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

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.

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

El espacio de nombres DNS funciona parecido al espacio de nombres de los ficheros de un ordenador. Por tanto el espacio de nombres DNS es una jerarquía de dominios DNS y nombres de ordenador individuales organizados en una estructura tipo árbol que llamamos, “árbol de nombres”.

HISTORIA DEL DNS

Sistema de Nombres de Dominio (DNS por sus siglas en inglés, Domain Name System), el cuál nació en la década de los 80′s.

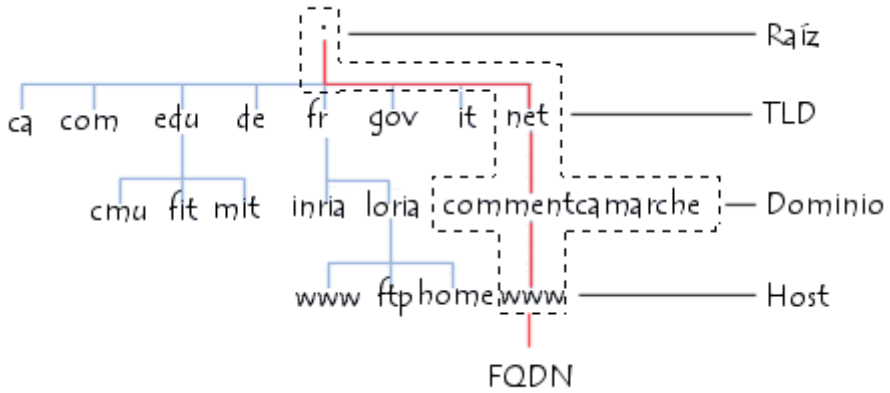
Creado por Paúl Mockapetris en colaboración con Jon Postel de la Universidad del Sur de California y posteriormente, Paúl Vixie. Juntos desarrollaron lo que hasta ahora conocemos como el DNS (BIND, Barkeley Internet Name Domain), un sistema cliente/servidor, distribuido y jerárquico.

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.

COMPONENTES DEL DNS

ESPACIO DE NOMBRE

La estructura del sistema DNS se basa en una estructura de arbórea en donde se definen los 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.

TIPOS DE REGISTROS (base de datos)

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**: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** :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
- **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** *(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 DOMINIOS

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

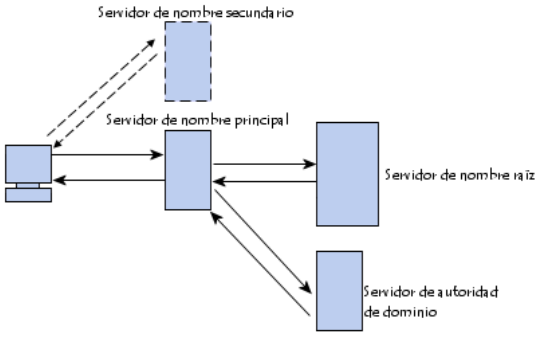
organización alguna que sea responsable de la administración de todos los nombres de dominio.

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.

RESOLUCION DEL NOMBRE 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*).

Protocolo DNS

El DNS usa el concepto de espacio de nombres distribuido. Los nombres simbólicos se agrupan en zonas de autoridad, o más comúnmente, zonas. En cada una de estas zonas, uno o más hosts tienen la tarea de mantener una base de datos de nombres simbólicos y direcciones IP y de suministrar la función de servidor para los clientes que deseen traducir nombres simbólicos a direcciones IP. Estos servidores de nombres locales se interconectan lógicamente en una árbol jerárquico de dominios.

Cada zona contiene una parte del árbol o subárbol y los nombres de esa zona se administran con independencia de los de otras zonas. La autoridad sobre zonas se delega en los servidores de nombres. Normalmente, los servidores de nombres que tienen autoridad en zona tendrán nombres de dominio de la misma, aunque no es imprescindible. En los puntos en los que un dominio contiene un subárbol que cae en una zona diferente, se dice que el servidor / servidores de nombres con autoridad sobre el dominio superior delegan autoridad al servidor / servidores de nombres con autoridad sobre los subdominios. Los servidores de nombres también pueden delegar autoridad en sí mismos; en este caso, el espacio de nombres sigue dividido en zonas, pero la autoridad para ambas las ejerce el mismo servidor . La división por zonas se realiza utilizando registros de recursos guardados en el DNS:

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

- **host**
  Obtiene una dirección IP asociada con un nombre de host o un nombre de host asociado con una dirección IP.
- **nslookup**
  Permite localizar información acerca de los nodos de red, examinar los contenidos de la base de datos de un servidor de nombres y establecer la accesibilidad a servidores de nombres.
- **dig**
  Permite probar los servidores de nombres, reunir grandes volúmenes de información de nombres de dominio y ejecutar simples consultas de nombres de dominio.

ESPACIO DE NOMBRES DE DOMINIO.

Cuando usamos el término espacio de nombres nos referimos a un conjunto de nombres en el cuál todos los nombres son únicos.

El DNS distingue:

1. **Un único espacio de nombres de dominio públicos:** estos nombres están asociados obligatoriamente con equipos con dirección IP pública.
2. **Infinitos espacios de nombres de dominio privados:** que incluyen todos los nombres de dominio que no se encuentran en el espacio anterior. Estos nombres suelen ser utilizados por equipos con IPs privadas que pretenden ser sólo accesibles desde otros equipos de su misma LAN.

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.

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. “pepe.edu.com.”) 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 "casa.irobot", tomará como nombre absoluto "casa.irobot.uv.es".

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 "casa.uv.es" si "." En el valor de un registro, el DNS cuando consulte dicho registro devolverá "casa.uv.es.uv.es".

Un nombre de dominio completo (FQDN) 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,*214.95.170.41*).

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*).

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.).”

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).

Registros de dominios en Internet. Agentes registradores.

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.

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.

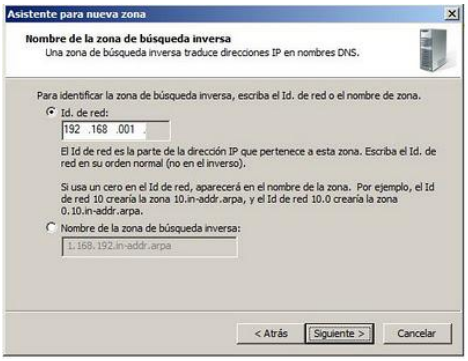
ESNIC es la autoridad competente para la gestión del registro de dominios de Internet bajo el código de país.Las principales funciones de ESNIC incluyen las relacionadas con la tramitación de solicitudes y asignación de dominios de acuerdo con la normativa correspondiente,así como la realización de las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

Servidores de nombres de dominio (DNS):

Zonas. Autoridad. Registro de recursos (RR).

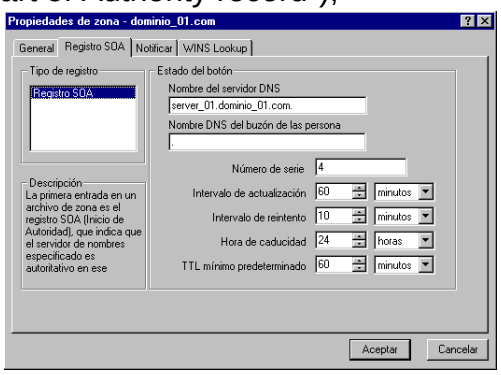
Zona de Búsqueda Directa.- Las resoluciones de esta zona devuelven la dirección IP correspondiente al recurso solicitado; este tipo de zona realiza las resoluciones que esperan como respuesta la dirección IP de un determinado recurso.

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 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 de nombres DNS.

El lado servidor de DNS es un demonio llamado named. Existen tres tipos de configuración diferentes de servidores de nombres los cuales requieren que el sistema local ejecute el software named.

• PRIMARIO.

El servidor primario es la fuente autorizada de toda la información acerca de un dominio especifico. 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.

• **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.

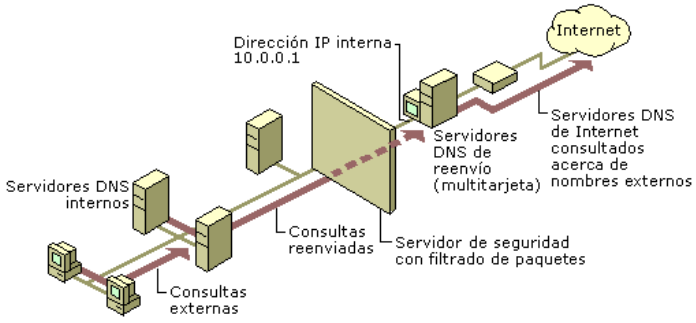
• **SÓLO CACHE.**

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, las guarda y las 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.

- **REENVIADOR DNS**.

Servidor DNS designado por otros servidores DNS para ser invocado en consultas de resolución de recursos que se encuentran ubicados en dominios que no son gestionados por el DNS local.



- **SERVIDOR AUTORIZADO**

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

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

Software comercial de servidores de nombres de dominio.

Simple DNS Plus

Es un servidor de DNS y DHCP de fácil uso.

Puedes usar el programa para hacer funcionar correctamente tu propio servidor DNS Internet/Intranet aún sin tener tu propio dominio registrado. Además mejora la velocidad del acceso a Internet.

Simple DNS Plus simplifica la configuración de un servidor de DNS y la configuración TCP/IP de tu red, y le da a los ordenadores de tu red nombre reales en vez de los difíciles números de la dirección IP de cada uno de ellos.

Por ejemplo, puedes llamar tu servidor de correo electrónico "mail", tu servidor proxy "proxy", y tu servidor Web de tu Intranet "Web"; evitándote tener que escribir las direcciones IP completas de cada uno de ellos.

Además puedes hacer funcionar múltiples servidores DNS en la misma máquina, y el programa soporta transferencia de zonas y notificación de zona actualizada.

El programa se aloja en la bandeja del sistema de Windows.

BIND

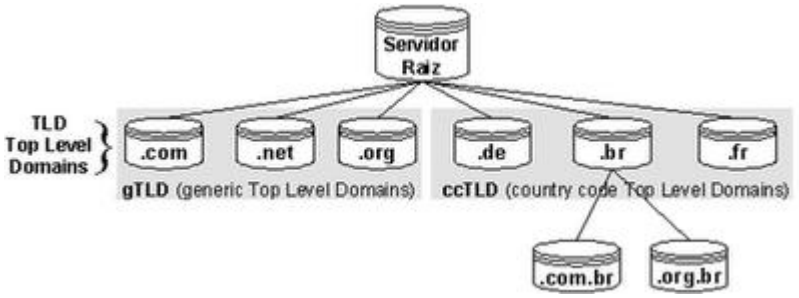
BIND es el servidor de DNS más comúnmente usado en Internet, especialmente en sistemas Unix, en los cuales es un Estándar de facto. Es patrocinado por la Internet Systems Consortium. BIND fue creado originalmente por cuatro estudiantes de grado en la University of California, Berkeley y liberado por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

Servidores Raíz (Root Name Servers, RNS)

Los RNS saben cuáles servidores de nombres tienen autoridad para los dominios superiores. Si se les hace una pregunta acerca de un subdominio, los servidores raíz maestros pueden al menos proveer los nombres y direcciones de los servidores de nombres con autoridad para el segundo nivel de dominios a los cuales un dominio pertenece. Cada servidor interrogado da, al que pregunta, información de cómo “estar más cerca” de la respuesta que está

buscando o provee él mismo una respuesta. Lo que hacen los RNS es proveer punteros desde los dominios superiores a los servidores de nombres de los dominios inferiores.

Por ejemplo para conseguir el servidor de nombres del dominio ve. se debe interrogar a los servidores raíz.



Los RNS, así como los NS normales, son muy importantes en la resolución de un nombre dentro de un dominio particular. Debido a que son tan importantes, DNSprovee mecanismos para asegurar siempre el servicio utilizando redundancia (servidores secundarios) o aliviando la carga de los servidores primarios y root (usando caching). Sin embargo, en ausencia de mecanismos como el caching, la resolución debe empezar en los servidores de raíz maestros.

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:

   - **Windows**:

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

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

- **GNU/Linux**:

  - 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.
  - 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.
  - 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.
  - 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.**

3. 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.
4. 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.

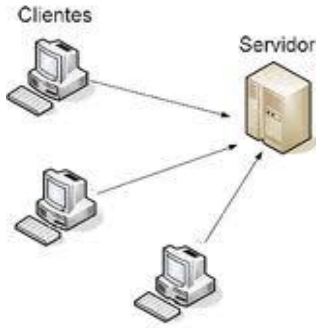
5. **Finalmente**, cuando el servidor DNS obtiene por uno de los dos medios la respuesta la envía al resolver. La respuesta se almacena tanto en la caché del servidor DNS consultado como en la caché local del resolver.

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.

```
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
```

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.

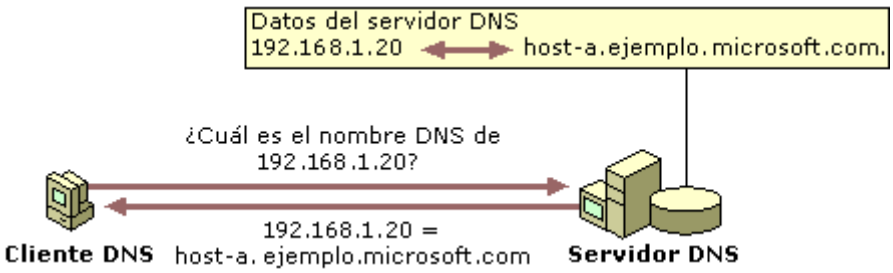
Si se realiza una solicitud a un servidor de DNS y la respuesta es negativa, las siguientes solicitudes al mismo nombre de dominio se responden negativamente durante un tiempo predeterminado de 300 segundos. Para evitar guardar en la caché información negativa anticuada, cualquier información de solicitud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

Resolución inversa:

Zona de Búsqueda Inversa: Las resoluciones de esta zona buscan un nombre de equipo en función de su dirección IP, de forma que pueden encontrar y contactarse con cualquier equipo o servidor perteneciente al dominio DNS sólo utilizando su IP.



Para que este proceso funcione, hay que utilizar un servidor ficticio denominado in-address-arpa (utilizado para IPv4), hay que asignarlo en un fichero de configuración utilizando el registro PTR.

Para utilizar ese dominio especial, es necesario utilizar un registro de recurso (RR) adicional, en este caso es el registro de puntero (PTR), encargado de relacionar la IP del equipo con su nombre DNS. El registro de recurso PTR es un registro de recursos de impresora (Registro de puntero). Este registro conecta el nombre del servidor con la IP, complementándose con el tipo de registro A utilizado en las búsquedas directas.

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 10.33.3.3. 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: 3.3.33.10.in-addr.arpa

Registros de recursos DNS:

Como ya hemos visto, cada servidor DNS primario mantiene un **archivo de zona** para **resolución directa** (de un nombre de dominio se obtiene la IP asociada) de la zona sobre la que tiene autoridad y, en algunos casos, otro **archivo de zona inverso** para la resolución inversa.

Ambos archivos son siempre archivos de **texto plano**, tanto si el servidor DNS corre en GNU/Linux o en Windows.

Cada archivo de zona contiene lo que ya conocemos como **registros de recursos**. Los principales **tipos** de registros de recursos son los siguientes.

TTL

La primera línea que hemos de indicar en un archivo de zona debe establecer el valor **Time to Live (TTL)** (**Tiempo de vida**). Su sintaxis es:

```
$TTL tiempo
```

Donde tiempo es el tiempo que cualquier registro de recurso de este archivo puede permanecer en la caché de otro servidor DNS. Si un registro de recurso especifica su propio valor TTL, esta directiva se ignora para dicho recurso. Si solo aparece un número (por ejemplo, $TTL 3600), se interpreta como segundos, pero para dar mayor claridad, se pueden usar semanas ($TTL 1w), días ($TTL 7d), horas ($TTL 168h) o minutos ($TTL 10080m).

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 IN SOA nombreDNSprimario emailAdministrador (
        numeroSerie
        actualizacion
        reintento
        caducidad
        TTLminimo )
```

Donde:

- **Zona** es o bien el nombre de la zona (¡terminado en punto!) o bien la letra @.
- **NombreDNSprimario** indica el FQDN del servidor donde esta almacenado el archivo de zona (¡terminado en un punto!).
- **EmailAdministrador** 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).
- **NumeroSerie** indica el número de version del archivo de zona. Sirve de referencia a los servidores DNS secundarios para saber cuando deben hacer una transferencia de zona. Si el numero de serie del ervidor 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

- **Actualizacion** 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.
- **TTLminimo** 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.

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

Por ejemplo, si estamos definiendo un archivo de zona para **ASIR.local** e incluimos los siguientes registros:

```
@                    IN NS  asterix.ASIR.local.
                     IN NS  obelix.ASIR.local.
ventas.ASIR.local  IN NS  ideafix.empleados.ASIR.local.
```

estamos indicando que los servidores con autoridad sobre la zona ASIR.local son asterix.ASIR.local. y obelix.ASIR.local.. Además, también indicamos que el servidor primario para la zona ventas.ASIR.local es ideafix.empleados.ASIR.local..

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.

NombreHost puede ser omitido en el registro A para indicar que estamos asociando una IP al nombre de la zona. Así, si consideramos un archivo de zona de ejemplo para la zona example.local que contenga:

```
      IN A 10.0.1.3
server1 IN A 10.0.1.5
```

Las peticiones de resolución para example.local son resueltas a la 10.0.1.3, mientras que las solicitudes para server1.example.local son resueltas a la 10.0.1.5.

Es recomendable que exista **sólo un registro IN A por cada dirección IP**.

CNAME

El registro CNAME crea un alias 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.

En el ejemplo siguiente, un registro A vincula un nombre de host a una dirección IP, mientras que un registro CNAME apunta al nombre host comúnmente usado www para este.

```
server1 IN A      10.0.1.5
www     IN CNAME  server1
```

PTR

El registro de recursos PTR (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 reves.
- **FQDNhost** es el nombre de dominio totalmente cualificado del host **(terminado en punto).**

MX

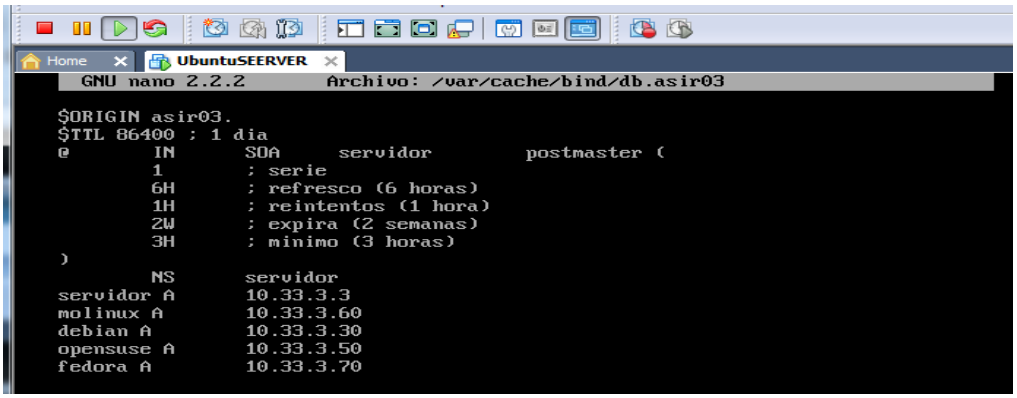
Este registro permite indicar cuáles son los servidores de correo de nuestro dominio. Además permite, en caso de tener varios servidores, establecer el orden de consulta o de preferencia. Este orden establece que los valores menores tienen mas prioridad.

Su sintaxis es:

```
dominio  IN MX  prioridad FQDNhost
```

Donde:

- **Dominio** puede dejarse en blanco o usar la letra @.
- **Prioridad** es un numero entero que puede omitirse.
- **FQDN-host** es el nombre completamente cualificado del host que hara las funciones de servidor de correo para la zona que estamos definiendo.



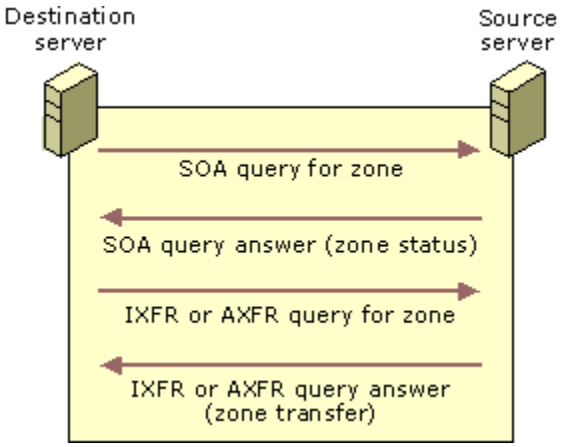
Delegación y Glue Record.

Glue Record

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

TRANSFERENCIA 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.



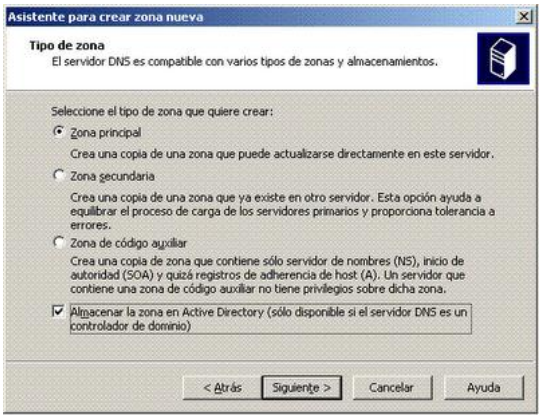
Se producirá una transferencia de zona durante cualquiera de los siguientes escenarios:

- 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.

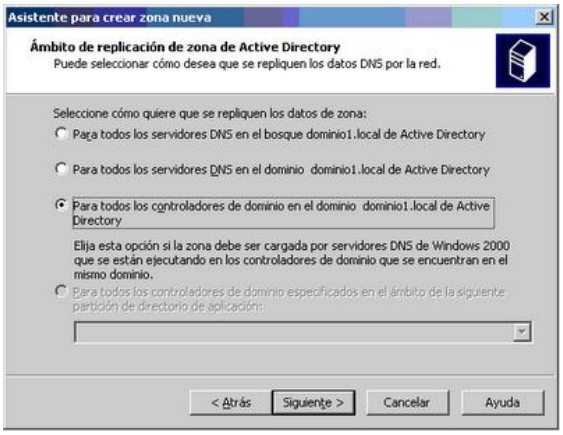
Cuando se agrega un nuevo servidor DNS a la red y se configura como un nuevo servidor secundario en una zona existente, dicho servidor realiza una transferencia inicial completa de la zona para obtener y replicar una copia total de los registros de recursos de la zona. En la mayor parte de implementaciones 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

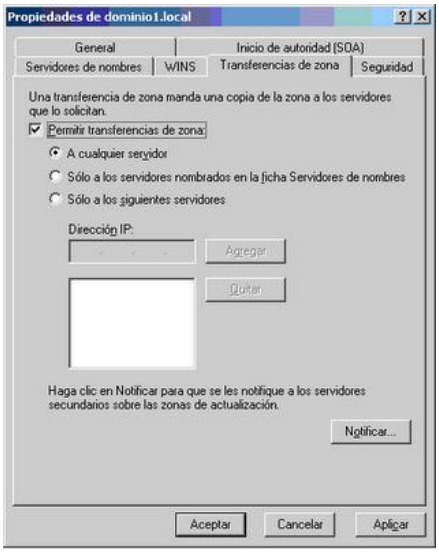
directorio activo.

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 Dinámico (DDNS o Dynamic DNS)

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.

Actualizaciones manuales.

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

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

Actualizaciones dinámicas.

La actualización dinámica permite a los equipos cliente DNS guardar y actualizar dinámicamente sus registros de recursos con un servidor DNS siempre que se produzcan cambios. Esto disminuye la necesidad de administrar de forma manual los registros de zona, especialmente para los clientes que mueven o cambian ubicaciones con frecuencia y utilizan DHCP para obtener una dirección IP.

DNS dinámico en Internet.

Cuando nos conectamos a Internet, el proveedor a través del que nos conectamos nos asigna una IP de Internet que habitualmente cambia. Para solucionar el problema cada vez que se inicia el servidor, o cuando deseemos, envía nuestra IP actual a la empresa que nos proporciona el DNS dinámico, para que nuestro subdominio se dirija a la IP que tenemos en cada momento.

PROTOCOLO DNS

El DNS usa el concepto de espacio de nombres distribuido. Los nombres simbólicos se agrupan en zonas de autoridad, o más comúnmente, zonas. En cada una de estas zonas, uno o más hosts tienen la tarea de mantener una base de datos de nombres simbólicos y direcciones IP y de suministrar la función de servidor para los clientes que deseen traducir nombres simbólicos a direcciones IP. Estos servidores de nombres locales se interconectan lógicamente en una árbol jerárquico de dominios.

Cada zona contiene una parte del árbol o subárbol y los nombres de esa zona se administran con independencia de los de otras zonas. La autoridad sobre zonas se delega en los servidores de nombres. Normalmente, los servidores de nombres que tienen autoridad en zona tendrán nombres de dominio de la misma, aunque no es imprescindible. En los puntos en los que un dominio contiene un subárbol que cae en una zona diferente, se dice que el servidor / servidores de nombres con autoridad sobre el dominio superior delegan autoridad al servidor / servidores de nombres con autoridad sobre los subdominios. Los servidores de nombres también pueden delegar autoridad en sí mismos; en este caso, el espacio de nombres sigue dividido en zonas, pero la autoridad para ambas las ejerce el mismo servidor . La división por zonas se realiza utilizando registros de recursos guardados en el DNS:

Aplicaciones de DNS

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

- **host**
  Obtiene una dirección IP asociada con un nombre de host o un nombre de host asociado con una dirección IP.
- **nslookup**
  Permite localizar información acerca de los nodos de red, examinar los contenidos de la base de datos de un servidor de nombres y establecer la accesibilidad a servidores de nombres.
- **dig**
  Permite probar los servidores de nombres, reunir grandes volúmenes de información de nombres de dominio y ejecutar simples consultas de nombres de dominio.

SEGURIDAD DNS

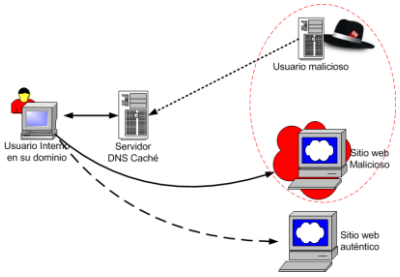
El sistema de nombres de dominio (DNS, *Domain Name System*) se diseñó originalmente como un protocolo abierto y, por tanto, es vulnerable a intrusos. El DNS de Windows Server 2003 ha mejorado su capacidad para impedir un ataque en la infraestructura DNS mediante la adición de características de

seguridad

VULNERABILIDADES

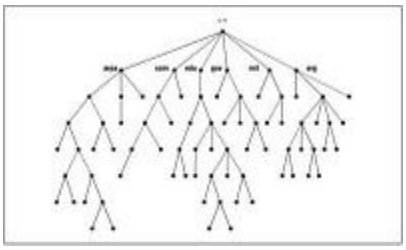
Caché Poisoning

- 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).

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.**

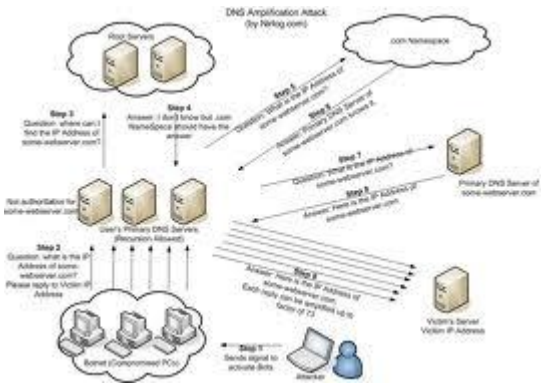
- **Denegación de servicios vía puntero nulo SIG RR.**
- **Ejecución de código arbitrario.**
- **Envenenamiento de la cache.**
- **Envenenamiento de la cache.**
- **Envenenamiento de la cache (de Dan Kaminsky).**

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.
- 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