2. Servicio DNS

2.1. Definición

DNS es una abreviatura de Sistema de Nombres de Dominio (*Domain Name System*), un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios. La asignación de nombres DNS se utiliza en las redes TCP/IP, como Internet, para localizar equipos y servicios con nombres sencillos. Cuando un usuario escriba un nombre DNS en una aplicación, los servicios DNS podrán traducir el nombre a otra información asociada con el mismo, como una dirección IP.

Por ejemplo, la mayoría de los usuarios prefieren un nombre fácil de utilizar como *www.upm.es* para localizar un equipo (como un servidor Web o de correo electrónico) en la red. Un nombre sencillo resulta más fácil de aprender y recordar. Sin embargo, los equipos se comunican a través de una red mediante direcciones numéricas. Para facilitar el uso de los recursos de red, los servicios de nombres como DNS proporcionan una forma de asignar estos nombres sencillos de los equipos o servicios a sus direcciones numéricas.

2.2. Descripción del servicio DNS

2.2.1. Nombres de dominio

El Sistema de Nombres de Dominio (DNS) se definió originalmente en los documentos de Petición de comentarios (RFC, *Request for Comments*) 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 utilizar 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, que consultan a los servidores para buscar y resolver nombres de un tipo de registro de recursos especificado en la consulta.

2.2.2. Descripción del espacio de nombres de dominio DNS

El espacio de nombres de dominio DNS, como se muestra en la figura 4.7, se basa en el concepto de un árbol de dominios con nombre. Cada nivel del árbol puede representar una rama o una hoja del árbol. Una rama es un nivel donde se utiliza más de un nombre para identificar una colección de recursos con nombre. Una hoja representa un nombre único que se utiliza una vez en ese nivel para indicar un recurso específico.

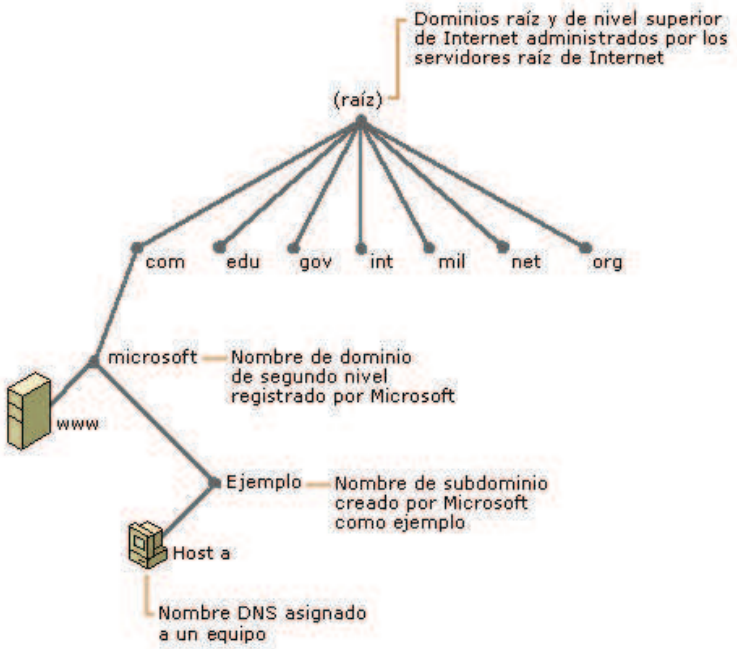

Figura 4.7: Ejemplo de un espacio de nombres de dominio

El gráfico anterior muestra cómo Microsoft es la autoridad asignada por los servidores raíz de Internet para su propia parte del árbol del espacio de nombres de dominio DNS en Internet. Los clientes y los servidores DNS usan las consultas como el método fundamental para resolver los nombres en el árbol como información específica de los tipos de recurso. Los servidores DNS proporcionan esta información a los clientes DNS en las respuestas a las consultas, quienes, a continuación, extraen la información y la pasan al programa solicitante para resolver el nombre consultado.

En el proceso de resolución de un nombre, tenga en cuenta que los servidores DNS funcionan frecuentemente como clientes DNS, consultando a otros servidores para resolver completamente un nombre consultado.

2.2.2.1. Cómo se organiza el espacio de nombres de dominio DNS

Cualquier espacio de nombres de dominio DNS que se utiliza en el árbol es, técnicamente, un dominio. Por ejemplo, el nombre de dominio DNS registrado para Microsoft *(microsoft.com.)* se

conoce como un dominio de segundo nivel. Esto se debe a que el nombre tiene dos partes (llamadas etiquetas) que indican que se encuentra dos niveles por debajo de la raíz o la parte superior del árbol. La mayor parte de los nombres de dominio DNS tienen dos etiquetas o más, cada una de las cuales indica un nuevo nivel en el árbol. En los nombres se utilizan puntos para separar las etiquetas.

Además de los dominios de segundo nivel, en la tabla 4.2 se describen otros términos que se utilizan para describir los nombres de dominio DNS según su función en el espacio de nombres.

Tipo de nombre	Descripción	Ejemplo
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 en un nombre de dominio DNS, empieza con un punto (.) para designar que el nombre se encuentra 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*).	Un sólo punto (.) o un punto usado al final del nombre, como "ejemplo.microsoft.com.".
Dominio de nivel superior	Un nombre de dos o tres letras que se utilizan para indicar un país o región, o el tipo de organización que usa un nombre.	".com", que indica un nombre registrado para usos comerciales o empresariales en Internet.
Dominio de segundo nivel	Nombres de longitud variable registrados que un individuo u organización utiliza en Internet. Estos nombres siempre se basan en un dominio de nivel superior apropiado, según el tipo de organización o ubicación geográfica donde se utiliza el nombre.	"microsoft.com.", que es el nombre de dominio de segundo nivel registrado para Microsoft por el registrador de nombres de dominio DNS de Internet.
Subdominio	Nombres adicionales que puede 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.	"ejemplo.microsoft.com.", que es un subdominio ficticio asignado por Microsoft para utilizarlo en nombres de ejemplo de documentación.
Nombre de recurso o de host	Nombres que representan una hoja en el árbol DNS de nombres e identifican un recurso específico. Normalmente, la etiqueta de la izquierda de un nombre de dominio DNS identifica un equipo específico en la red.	"host-a.ejemplo.microsoft.com.", donde la primera etiqueta ("host-a") es el nombre de host DNS de un equipo específico en la red.

Tabla 4.2: Términos utilizados para describir los nombres de dominio DNS

Un dominio es simplemente un subárbol del espacio de nombres. El nombre de un dominio es el nombre del nodo raíz correspondiente. Un dominio agrupa un conjunto de hosts y/o subdominios que se relacionan de acuerdo a cierto criterio, ya sea geográfico u organizacional. En el DNS cada dominio es administrado por una organización o empresa determinada. Ésta puede decidir dividir el o los dominios que administra en subdominios, así como asignar la administración de éstos a otras entidades. Cada dominio puede contener tanto subdominios como hosts independientes, al igual que un directorio posee subdirectorios y ficheros a la vez.

El DNS en la actualidad sigue ciertos patrones en cuanto a su organización. Ésta se basa en niveles de acuerdo a la posición del dominio. El nivel superior o primer nivel lo forman aquellos dominios descendientes del dominio raíz. Los fundamentales se listan a continuación:

- ***Com***: Agrupa a organizaciones comerciales. Ejemplos: *ibm.com*, *yahoo.com*, *redhat.com*, etc.

- ***Edu***: Reune a organizaciones de propósitos educacionales. Ejemplos: *berkeley.edu*, *cornell.edu*, etc.

- ***Net***: Agrupa a organizaciones dedicadas al desarrollo de las redes. Ejemplos *rpmfind.net*, *nic.net*, *computing.net*, etc.

- ***Org***: Reune a organizaciones no comerciales. Ejemplos: *linuxdoc.org*, *ibiblio.org*, *linux.org*, *insflug.org*, etc.

- ***Gov***: Agrupa a organizaciones gubernamentales. Ejemplo: *nasa.gov*, *nsf.gov*, etc.

Como parte del espacio de nombres de dominio también existen dominios de primer nivel que designan zonas geográficas. Sus nombres representan a todos los países a través de dos letras. Ejemplos: *es* para España, *au* para Australia, *de* para Alemania, etc. Para ver a todos los dominios geográficos de primer nivel puede consultarse *http://www.iana.org/cctld/cctld-whois.htm*. Puede ocurrir que los dominios geográficos de primer nivel contengan a su vez algunos de los dominios organizativos de primer nivel. Ejemplos: *edu.au*, *org.uk*, etc.

2.2.3. Delegación

Como ya se ha expresado anteriormente una de las ventajas fundamentales de la estructura distribuida del DNS es la descentralización de su administración. El mecanismo que permite resolver un nombre completamente es la **delegación**. La organización propietaria de un dominio puede dividir éste en varios subdominios y delegar a su vez todo lo concerniente al mantenimiento de la información relacionada y su accesibilidad, a cada uno de estos subdominios. Los dominios de segundo nivel pueden dividirse también en otros subdominios continuando el mecanismo de delegación.

En resumen, el término delegación se refiere a que la organización encargada de un dominio determinado asigne la responsabilidad de sus subdominios a otras organizaciones.

2.2.4. Servidores de nombres de dominio

Los programas encargados de agrupar y mantener disponible la información asociada a un espacio de nombres de dominio se conocen como servidores de nombres de dominio. Estos servidores usualmente administran la información referente a una parte del dominio, la cual se conoce como zona. Entonces se dice que el servidor tiene autoridad sobre la zona. El mismo servidor puede estar autorizado para varias zonas.

Una zona se diferencia de un dominio en que ésta no necesariamente incluye la información asociada a los subdominios de éste, aunque puede hacerlo. En este último caso no se produce la delegación a los subdominios incluidos por parte del servidor del dominio padre.

Algunos de los tipos de servidores de nombres que existen son:

- ***Maestros***: Almacena los registros de las zonas originales y tienen la autoridad de un cierto espacio de nombres donde buscan respuestas concernientes a dicho espacio de nombres.

- ***Esclavo***: Responde también a las peticiones que provienen de otros servidores de nombres y que se refieren a los espacios de nombres sobre los que tiene autoridad. Los servidores esclavos obtienen la información de espacios de nombres de servidores de nombres maestros a través de una *zona de transferencia*, en la que el esclavo manda al servidor maestro una petición que se llama *NOTIFY* para una determinada zona y el maestro responde si el esclavo está autorizado para recibir la transferencia.

- ***Caching-only***: Ofrece servicios de resolución de nombres a direcciones IP pero no tiene ninguna autoridad sobre zonas. Las respuestas en general se pone en un caché que se encuentra en la base de datos almacenada en la memoria durante un periodo fijo, la cual está especificada por la zona importada y así obtener una resolución más rápida para otros clientes DNS después de la primera resolución.

- ***Forwarding***: Hace que determinados servidores de nombres lleven a cabo la resolución. Si alguno de estos servidores no puede efectuar la resolución, el proceso se para y la resolución se anula.

La posibilidad de definir más de un servidor de nombres de dominio para una misma zona permite tener redundancia de la información, mayor tolerancia ante el fallo de algún servidor y accesibilidad por parte de todos los hosts de la red. Y todo esto se logra sin tener que actualizar los datos manualmente lo cual puede ocasionar errores e inconsistencias en la información de la zona.

Un servidor de nombres puede ser primario para unas zonas y secundario para otras.

Existe un conjunto de servidores de nombres de dominio que controlan el dominio raíz y conocen todos los servidores autorizados para los dominios de primer nivel. Estos servidores son claves en el proceso de resolución de nombres de dominio. Actualmente existen catorce servidores raíces distribuidos en su inmensa mayoría en el territorio de los Estados Unidos, los otros se encuentra en Japón, Suecia, Gran Bretaña y España.

2.2.5. Resolvers

Los *resolvers* son los clientes que acceden a los servidores de nombres. Cualquier programa que necesite información de un espacio de nombres de dominio utiliza un *resolver*. Los *resolvers* realizan las siguientes funciones:

- Consultan a un servidor de nombres de dominio
- Interpretan la respuesta (ésta puede ser válida o un error)
- Retornan la información al programa que la solicitó

Los *resolvers* no son programas independientes, sino que son rutinas compiladas dentro de aquellos que las requieren, por ejemplo: los comandos *ping, telnet, ftp*, navegadores como el Netscape, Internet Explorer y otros.

2.2.6. Proceso de resolución de nombres

Para satisfacer las solicitudes de los *resolvers,* los servidores de nombres no solamente retornan información acerca de las zonas para la que están autorizados, también tienen que hacerlo de aquellas para las que no lo están. Este proceso se denomina **resolución**.

Gracias a que el espacio de nombres de dominio tiene estructura de árbol, sólo es necesario por parte del servidor de nombres conocer un punto de este árbol: los nombres y los números IP de los servidores de nombre del dominio raíz (servidores raíces).

De esta forma, cualquier servidor de nombres para resolver un nombre determinado (o realizar otro tipo de consulta), sólo necesitará conocer algún servidor raíz y consultarlo. Éste le devolverá la dirección del servidor del subdominio correspondiente (dominio de primer nivel), el cual a su vez puede referir a otro servidor y así sucesivamente se va completando el proceso de resolución que puede concluir exitosamente o no.

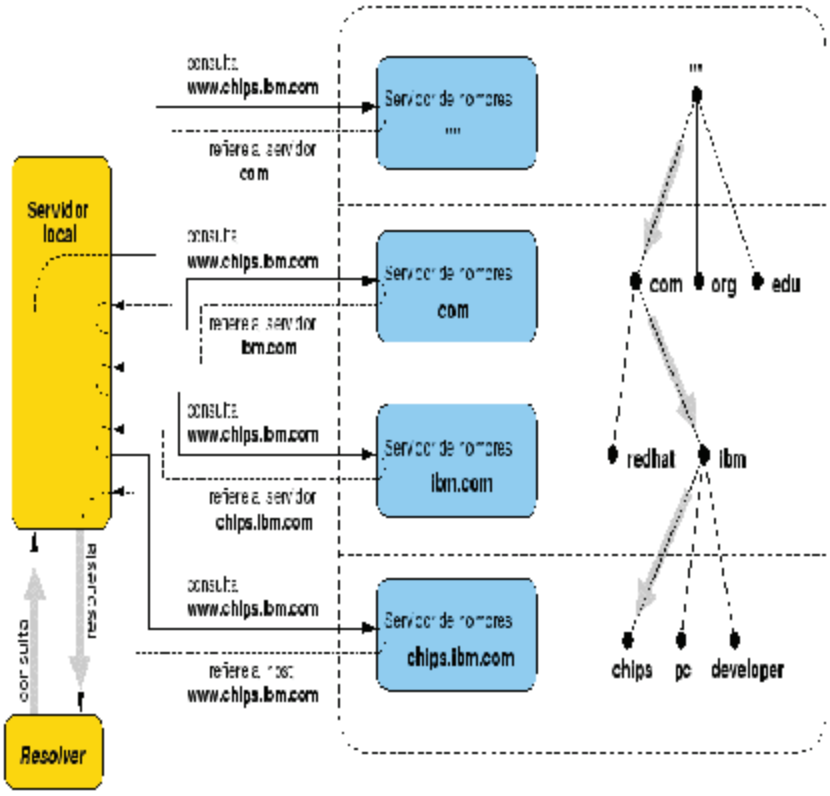

Figura 4.8: Proceso de resolución del nombre de dominio www.chips.ibm.com

La figura 4.8 muestra el proceso de resolución del nombre *www.chips.ibm.com*. En esta se aprecia como el servidor de nombres interrogado consulta a su vez a todos los servidores autorizados para cada uno de los dominios que contienen al nombre de dominio en cuestión.

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

1. La consulta de un nombre comienza en un equipo cliente y se pasa al solucionador, el servicio Cliente DNS, para proceder a su resolución.

2. Cuando la consulta no se puede resolver localmente, se puede consultar a los servidores DNS según sea necesario para resolver el nombre.

Estos dos procesos se detallan en las secciones siguientes.

?? **Parte 1: El solucionador local**

En la figura 4.9 se muestra un resumen del proceso de consulta DNS completo.

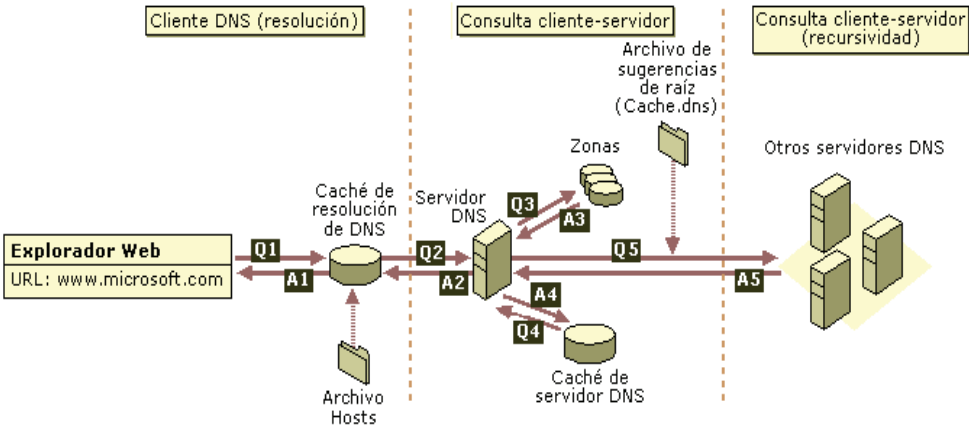

Figura 4.9: Proceso de consulta DNS del nombre DNS www.microsoft.com

Como se muestra en los pasos iniciales del proceso de consulta, en un programa del equipo local se utiliza un nombre de dominio DNS. A continuación, la solicitud se pasa al servicio Cliente DNS para proceder a su resolución mediante la información almacenada en la caché local. Si el nombre consultado se puede resolver, se responde a la consulta y el proceso finaliza.

La caché del solucionador local puede incluir información de nombres obtenida de dos orígenes posibles:

?? Si un archivo Hosts está configurado localmente, las asignaciones de nombre a dirección de host de ese archivo se cargan con anterioridad en la caché cuando se inicia el servicio Cliente DNS.

?? Los registros de recursos obtenidos en las respuestas de consultas DNS anteriores se agregan a la caché y se mantienen durante un período.

Si la consulta no coincide con una entrada de la caché, el proceso de resolución continúa con la consulta del cliente al servidor DNS para resolver el nombre.

?? **Parte 2: Consultar un servidor DNS**

Como se indicó en la figura 4.9, el cliente consulta un servidor DNS preferido. El servidor real utilizado durante la parte de la consulta inicial cliente-servidor del proceso se selecciona de una lista global.

Cuando el servidor DNS recibe una consulta, primero comprueba si puede responder la consulta con autoridad en función de la información de registro de recursos contenida en una zona configurada localmente en el servidor. Si el nombre consultado coincide con un registro de recursos correspondiente en la información de zona local, el servidor responde con autoridad y usa esta información para resolver el nombre consultado.

Si no existe ninguna información para el nombre consultado, a continuación el servidor comprueba si puede resolver el nombre mediante la información almacenada en la caché local de consultas anteriores. Si aquí se encuentra una coincidencia, el servidor responde con esta información. De nuevo, si el servidor preferido puede responder con una respuesta de su caché que concuerda al cliente solicitante, la consulta se finaliza.

Si el nombre consultado no encuentra una respuesta coincidente en su servidor preferido, ya sea en su caché o en su información de zona, el proceso de consulta puede continuar y se usa la recursión para resolver completamente el nombre. Esto implica la asistencia de otros servidores DNS para ayudar a resolver el nombre. De forma predeterminada, el servicio Cliente DNS pregunta al servidor si va a utilizar un proceso de recursión para resolver completamente los nombres en nombre del cliente antes de devolver una respuesta. En la mayor parte de los casos, el servidor DNS se configura, de forma predeterminada, para admitir el proceso de recursión como se muestra en la figura 4.10.

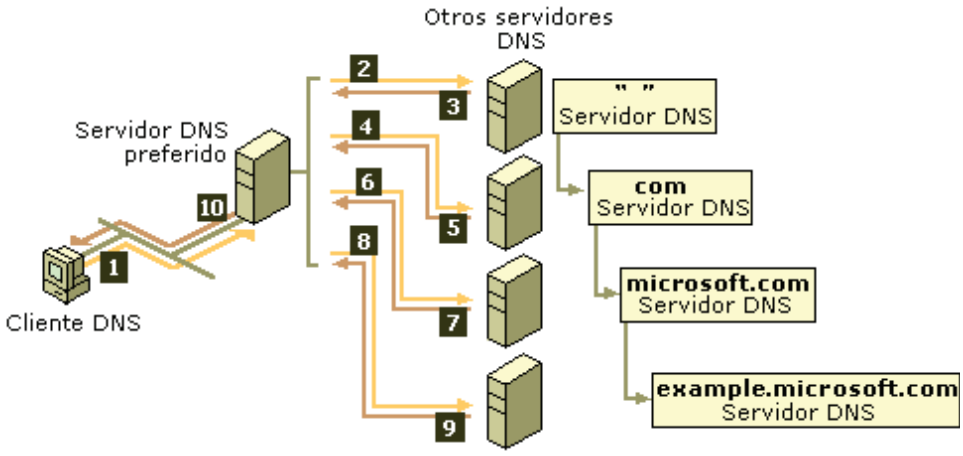

Figura 4.10: Proceso de consulta recursiva de DNS

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

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

Por ejemplo, piense en la posibilidad de usar el proceso de recursión para localizar el nombre "host-b.ejemplo.microsoft.com." cuando el cliente consulte un único servidor DNS. El proceso ocurre cuando un servidor y un cliente DNS se inician y no tienen

información almacenada en la caché local disponible para ayudar a resolver la consulta de un nombre. Se supone que el nombre consultado por el cliente es para un nombre de dominio del que el servidor no tiene conocimiento, según sus zonas configuradas.

Primero, el servidor configurado por defecto analiza el nombre completo y determina que necesita la ubicación del servidor con autoridad para el dominio de nivel superior, "com". A continuación, utiliza una consulta iterativa al servidor DNS "com" para obtener una referencia al servidor "microsoft.com". Después, desde el servidor "microsoft.com" se proporciona una respuesta de referencia al servidor DNS para "ejemplo.microsoft.com".

Finalmente, se entra en contacto con el servidor "ejemplo.microsoft.com.". Ya que este servidor contiene el nombre consultado como parte de sus zonas configuradas, responde con autoridad al servidor original que inició la recursión. Cuando el servidor original recibe la respuesta que indica que se obtuvo una respuesta con autoridad a la consulta solicitada, reenvía esta respuesta al cliente solicitante y el proceso de consulta recursiva se completa.

Aunque el proceso de consulta recursiva puede usar muchos recursos cuando se realiza como se describe arriba, tiene algunas ventajas en el rendimiento para el servidor DNS. Por ejemplo, durante el proceso de recursión, el servidor DNS que realiza la búsqueda recursiva obtiene información acerca del espacio de nombres de dominio DNS. Esta información se almacena en la caché del servidor y se puede utilizar de nuevo para ayudar a acelerar la obtención de la respuesta de consultas subsiguientes que la utilizan o concuerdan con ella. A lo largo del tiempo, esta información almacenada en caché puede crecer hasta ocupar una parte significativa de los recursos de memoria del servidor, aunque se limpie siempre que el servicio DNS se activa y desactiva.

2.2.7. Caché y tiempo de vida (TTL)

Hasta ahora puede concluirse que los servidores raíces reciben todas las consultas que se realizan cada instante en Internet. Otros servidores, no necesariamente los del dominio raíz, también pueden estar muy sobrecargados. Es por ello que las implementaciones del DNS proveen el mecanismo de *caché* que no es más que una facilidad que utilizan los servidores de nombres durante el proceso de resolución con vistas a disminuir el número de consultas necesarias para obtener una información determinada. Esta facilidad se implementa utilizando un *caché* de las respuestas a las consultas más recientes. Por ejemplo, supongamos que se haya resuelto recientemente el nombre *www.chips.ibm.com*, si a continuación se desea consultar cierta información acerca del nombre *www.developers.ibm.com* no será necesario interrogar a un servidor raíz para conocer los servidores del dominio *com*, ni tampoco a alguno de estos para el dominio *ibm*, gracias a que ya está "*cacheada"* la dirección de un servidor del dominio *ibm* y es a partir de éste donde comenzará el proceso de resolución.

Como se ha dicho, existen servidores de nombres que sólo realizan *caché*. Estos no son autoritarios de ninguna zona. Lo único que hacen es guardar en su *caché* las respuestas que le dan otros servidores cada vez que son consultados.

Los servidores de nombres no deben almacenar en sus *cachés* la información a la que acceden por un tiempo indefinido, pues entonces sería imposible la actualización de ésta una vez sea cambiada en los servidores autorizados para ello. A cada dato de un dominio se le asocia por parte de su administrador un tiempo de vida o TTL (*Time To Live*), transcurrido este tiempo, cualquier servidor que lo tenga almacenado en su *caché* debe volver a interrogar al servidor autorizado de la zona a la que pertenece el dato.

Para decidir el tiempo de vida de cada dato en un dominio hay que establecer que importa más: la consistencia o el rendimiento. Un TTL pequeño permitirá que la información sea consistente casi siempre, pues los datos expirarán rápidamente obligando a descargarlos del *caché* y a obtener los nuevos valores de los servidores autorizados. En cambio, producirá un mayor número de consultas a través de la red y esto empeorará el rendimiento del servidor y extenderá a su vez el tiempo promedio de resolución. Por el contrario, un TTL grande, mejorará el desenvolvimiento de los servidores y acortará el tiempo del proceso de resolución, pero puede provocar que la información se mantenga inconsistente durante mucho tiempo.

2.2.8. Estructura de la base de datos del DNS

A cada nombre de dominio en el DNS se le pueden asociar varias informaciones. Para los nombres de dominio asociados a un host, la principal información es su número IP, pero también se le pueden hacer corresponder varios alias, indicar una descripción de la máquina (procesador y sistema operativo), etc.

Los registros más importantes son:

?? **El registro SOA**

SOA significa *Start Of Authority* e informa que todos los registros de recursos que le siguen están autorizados a dicho dominio. Los datos asociados con un registro SOA son los siguientes:

- ***origin**:* Es el nombre canónico del servidor de nombres primario para este dominio, y generalmente se da como absoluto, es decir, con un punto al final.

- ***contact**:* Es el nombre de la persona responsable para este dominio. Es parecido a una dirección de correo electrónico normal, a excepción que la arroba se remplaza con un punto. También termina con un punto.

- ***serial**:* Es un número que indica la versión del archivo de zona, y debe ser incrementado cada vez que el archivo se modifique. Es importante porque los servidores secundarios solicitan el registro SOA en ciertos intervalos, para verificar el serial. Si éste ha cambiado, entonces transfieren el archivo completo para actualizarse. Una práctica muy común es utilizar la fecha en el formato *aammdd* y agregarle dos dígitos más para los cambios que se hacen al archivo en el mismo día. De tal manera, un serial típico podría ser 2001032201.

- ***refresh**:* Es el intervalo, en segundos, para las revisiones que hacen los servidores secundarios del registro SOA, con el fin de verificar si la información del dominio ha cambiado. El valor típico es de una hora (3600).

- ***retry**:* Es el tiempo, en segundos, que un servidor secundario debe esperar para reintentar una conexión por *refresh* que ha fallado. El valor recomendado es de 10 minutos (600 segundos).

- ***expire**:* Si un servidor secundario no ha podido comunicarse con su servidor primario para verificar que no haya habido cambios a la zona (mediante su registro SOA), descartará la información que tiene después de este periodo dado en segundos. El valor típico es de 42 días, o sea 3600000.

- ***minimum**:* Este es el número de segundos empleado en los registros del archivo que no especifican su campo ttl (*time to live*).

?? **El registro A**

Este registro sirve para asociar un nombre de máquina con una dirección IP. El único dato para este tipo de registro es la dirección IP en su forma estándar xxx.xxx.xxx.xxx. Debe haber sólo un registro A por cada dirección IP en el archivo, aunque es posible asignarle a una máquina más de una dirección mediante varios registros A.

?? **El registro NS**

Mediante un registro NS es posible designar un servidor que deberá responder para todas las peticiones que involucren un determinado subdominio. Esto es importante porque permite delegar la asignación de nombres y facilita el manejo de dominios complejos.

Designar un servidor de nombres, sin embargo, no basta. Se necesita definir en alguna parte del archivo la dirección de este servidor, mediante un registro A, por supuesto.

?? **El registro PTR**

Un registro PTR se utiliza para relacionar una dirección IP con un nombre de máquina, exactamente al revés que un registro tipo A. Estos registros aparecen en los archivos de zonas para la resolución inversa.

En cada registro sólo aparece una fracción de la dirección IP: la dirección se completa porque a cada nombre que no termina en un punto se le agrega el origen.

Los nombres de máquinas aparecen siempre en los registros PTR en su forma canónica, es decir, con el dominio completo. El punto es necesario porque de no aparecer se le agregaría erróneamente el origen.

?? **El registro MX**

Los registros MX sirven para anunciar a los programas de intercambio de correo, una máquina que se encarga de administrar el correo de un determinado dominio.

?? **El registro CNAME**

Este registro sirve para asignarle un nombre alternativo o alias a una máquina.

Todos estos tipos de datos se conocen como *Resource Records* (RR) y se asocian a los nombres de dominios.

2.2.9. Resolución inversa

El proceso de resolución en el DNS no sólo permite traducir nombres a direcciones IP, también se puede hacer el proceso inverso, dado un número IP determinar el nombre principal asociado a esta. Esta facilidad permite que los programas puedan producir su salida en un formato más humano, por ejemplo el subsistema de trazas en lugar de colocar los números IP de las máquinas en las salidas que genera puede utilizar sus nombres. Este tipo de traducción también permite hacer ciertos chequeos de autorización por parte de algunos servidores que en función de ello dan determinadas facilidades de acceso.

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

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

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

Por esta razón, se debe invertir el orden de los octetos de las direcciones IP cuando se crea el árbol del dominio *in-addr.arpa*. Con esta colocación, la administración de las ramas inferiores del árbol DNS *in-addr.arpa* se puede dejar a las organizaciones ya que se les asigna un conjunto de direcciones IP específicas o limitadas dentro de las clases de direcciones definidas en Internet.

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

La figura 4.11 muestra un ejemplo de una consulta inversa iniciada por un cliente DNS (host-b) para aprender el nombre de otro host (host-a) basándose en su dirección IP, 192.168.1.20.

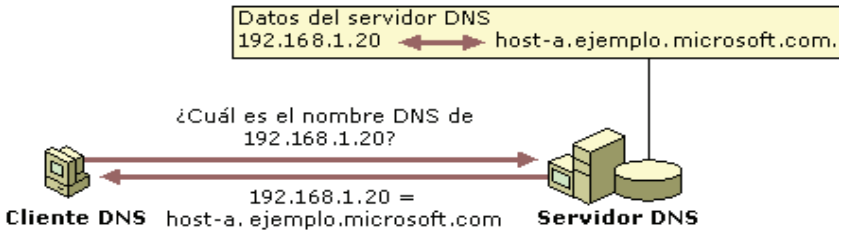

Figura 4.11: Proceso de consulta inversa de DNS

El proceso de búsqueda inversa que se muestra en esta ilustración se produce en los siguientes pasos:

1. El cliente, "host-b", consulta al servidor DNS un registro de recursos de puntero (PTR) que asigna la dirección IP 192.168.1.20 a "host-a".

2. Ya que esta consulta se realiza en los registros de puntero, el solucionador invierte la dirección y agrega el dominio *in-addr.arpa* al final de la dirección inversa. De esta manera, forma el nombre de dominio completo ("20.1.168.192.in-addr.arpa.") que se va a buscar en una zona de búsqueda inversa.

3. Una vez localizado, el servidor DNS con autoridad en "20.1.168.192.in-addr.arpa" puede responder con la información del registro de puntero PTR. Esto incluye el nombre de dominio DNS para "host-a", lo que completa el proceso de búsqueda inversa.

2.2.10. Zonas y domínios

2.2.10.1. Diferencia entre zonas y dominios

Una zona se inicia como una base de datos de almacenamiento para un único nombre de dominio DNS. Si se agregan otros dominios debajo del dominio que se utilizó para crear la zona, estos dominios pueden formar parte de la misma zona o pertenecer a otra zona. Una vez agregado un subdominio, a continuación, se puede:

?? Administrar e incluir como parte de los registros de la zona original, o bien

?? Delegar a otra zona creada para admitir el subdominio.

Por ejemplo, la figura 4.12 muestra el dominio *microsoft.com*, que contiene nombres de dominio para Microsoft. Cuando el dominio microsoft.com se crea por primera vez en un sólo servidor, se configura como una zona única para todos los espacios de nombres DNS de Microsoft. Sin embargo, si el dominio microsoft.com tiene que utilizar subdominios, estos subdominios se deben incluir en la zona o delegarse a otra zona.

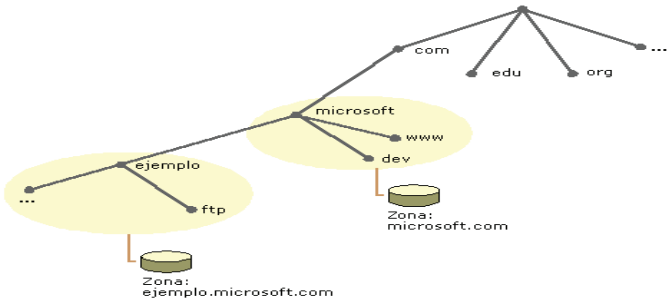

Figura 4.12: Espacio de nombre del dominio Microsoft.com

En este ejemplo, el dominio *example.microsoft.com* muestra un subdominio nuevo, el dominio *example.microsoft.com*, que se delega de la zona microsoft.com y se administra en su propia zona. Sin embargo, la zona *microsoft.com* necesita contener algunos registros de recursos para proporcionar la información de delegación que hace referencia a los servidores DNS que tienen autoridad para el subdominio delegado *example.microsoft.com*.

Si la zona *microsoft.com* no usa la delegación para un subdominio, los datos del subdominio permanecen como parte de la zona *microsoft.com*. Por ejemplo, el subdominio *dev.microsoft.com* no está delegado, pero está administrado por la zona *microsoft.com*.

2.2.10.2. Por qué son necesarias la replicación de zonas y las transferencias de zona

Debido al importante papel que desempeñan las zonas en DNS, se pretende que estén disponibles desde más de un servidor DNS en la red para proporcionar disponibilidad y tolerancia a errores cuando se resuelven consultas de nombres. En caso contrario, si sólo se utiliza un servidor y éste no responde, las consultas de nombres en la zona pueden fallar. Para que otros servidores alojen una zona, se requieren las transferencias de zona con el fin de replicar y sincronizar todas las copias de la zona que utiliza cada servidor configurado para alojar la zona.

Cuando se agrega un servidor DNS nuevo a la red y se configura como un servidor secundario nuevo para una zona existente, 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 requiere actualizarse después de haber realizado cambios en la misma. Para Windows Server 2003, el servicio DNS admite la *transferencia de zona incremental*, un proceso revisado de transferencia de zonas DNS para cambios intermedios.

2.2.10.3. Transferencias de zona incrementales

Las transferencias de zona incrementales se describen en el documento RFC 1995 como un estándar DNS adicional para replicar zonas DNS. Cuando un servidor DNS que actúa como origen para una zona y los servidores que copian la zona de él admiten las transferencias incrementales, se ofrece un método más eficiente de propagación de los cambios y las actualizaciones de la zona.

En las implementaciones DNS anteriores, la solicitud de una actualización de datos de zona requería una transferencia completa de toda la base de datos de la zona mediante una consulta AXFR. Con la transferencia incremental, en su lugar se puede utilizar un tipo de consulta alternativo (IXFR). Esto permite al servidor secundario extraer sólo los cambios de zona que necesita para sincronizar su copia de la zona con su origen, ya sea una copia principal o secundaria de la zona que mantiene otro servidor DNS.

Con las transferencias de zona IXFR, primero se determinan las diferencias entre el origen y las versiones replicadas de la zona. Si se descubre que las zonas tienen la misma versión, como indica el campo de número de serie del registro de recursos de inicio de autoridad (SOA) de cada zona, no se realiza ninguna transferencia.

Si el número de serie de la zona en el origen es mayor que el del servidor secundario solicitante, se realiza una transferencia sólo de los cambios en los registros de recursos (RR) de cada versión incremental de la zona. Para realizar una consulta IXFR correcta y enviar los cambios, el servidor DNS de origen de la zona debe mantener un historial de cambios de zona incrementales para utilizarlo al responder a estas consultas. El proceso de transferencia incremental requiere bastante menos tráfico en la red y las transferencias de zona se completan mucho más rápidamente.

2.3. Instalación del servidor DNS

Antes de nada, se debe configurar en la máquina el protocolo TCP/IP con una dirección IP estática.

Se deben de cumplir las siguientes configuraciones TCP/IP en los equipos que ejecutarán el servicio DNS:

1. Asignar una dirección IP estática.

2. Configurar el nombre de dominio y host en el servidor que ejecutará DNS.

Para hacer esto, haga clic en **Avanzadas** dentro de las **Propiedades de TCP/IP**. Sobre la pestaña de **DNS en la configuración avanzada de TCP/IP** verifique que la dirección DNS en **Direcciones DNS** es correcta y después escriba el nombre de dominio en el cuadro de dialogo de **Nombre de Dominio DNS**.

El proceso de instalación de DNS ejecuta las siguientes acciones:

- Instalar el servicio DNS y arrancar dicho servicio automáticamente sin reiniciar el equipo.
- Instalar la consola de DNS y añadir un acceso directo al menú de Herramientas Administrativas. La consola DNS se utiliza para administrar local y remotamente los servidores de nombres DNS.
- Crea el directorio *systemroot\system32\Dns*, el cual contendrá los siguientes ficheros de la base de datos:
  - **Domain_name.dns**: El fichero de la base de datos de la zona usado para traducir los nombres de host a direcciones IP.
  - **z.y.x.w.in-addr.arpa**: El fichero de inversión que se usa para convertir las direcciones IP en nombres de host.
  - **CACHE.DNS**: Contiene la información que requiere el host para resolver nombres que están fuera del dominio autoritativo.
  - **Boot**: Controla el arranque del servicio DNS.
  - **Dns.log**: Contiene los logs que el sistema hace del servicio DNS.

Para instalar el servidor DNS en el sistema Windows Server 2003, se deberán seguir los siguientes pasos:

1. Abra **Añadir o quitar programas** en el panel de control, marque **Añadir o quitar componentes de Windows** y haga clic en **Siguiente**.
2. En los componentes de Windows, haga clic en **Servicios de red** y después en **Detalles**.
3. Seleccione el **Sistema de nombres de dominio DNS** y haga clic en **OK**.
4. Si se pide, proporcione el path completo hacia el fichero de distribución de Windows Server 2003 y después seleccione **Continuar**.

2.4. Configuración del servidor DNS

2.4.1. Configuración de zonas

Una zona es una porción del espacio de nombres de dominio que se define por el recurso registrado y que se almacena en un fichero de la base de datos de la zona. Este fichero guarda la información que se usará para resolver los nombres de host direcciones IP y direcciones IP

en nombres de host. Cuando se configura una zona, se determina el tipo de fichero de base de datos de la zona que se almacenará en el servidor DNS.

Para crear una zona haga clic en **DNS** en las **herramientas Administrativas**. Sobre la pestaña de **Acción**, pulse la opción **crear una zona nueva**. Si acaba de instalar el servidor y no hay configuradas zonas, hágalo seleccionando la pestaña **Configurar el servidor**, se iniciará un asistente que le guiará para configurar el servidor DNS creando zonas de búsqueda directas e inversas.

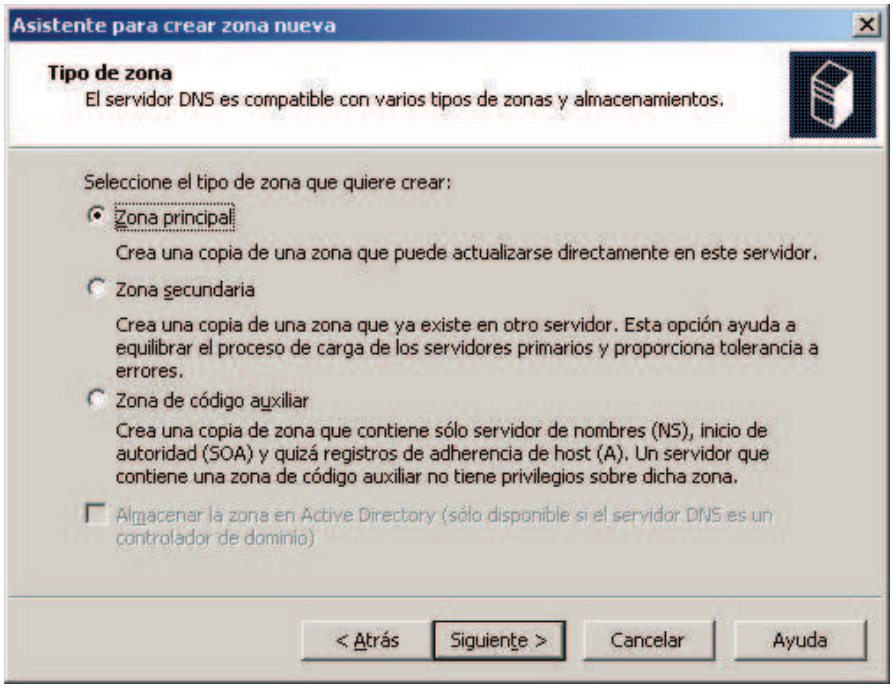

Figura 4.13: Asistente para crear una zona nueva de DNS

El Servicio DNS en Windows Server 2003 permite crear zonas integradas en el Directorio Activo, las cuales son zonas primarias que se guardan en el Directorio Activo. De todas formas, las zonas primarias y secundarias se llaman zonas primarias y secundarias estándar en Windows Server 2003.

Para añadir una zona principal estándar, abra la consola de DNS, haga clic con el botón derecho del ratón sobre el servidor apropiado y pulse **Crear una zona nueva**. En el asistente de creación de zonas nuevas, haga clic en **siguiente**. Sobre **Seleccionar un tipo de zona**, haga clic sobre **Principal estándar** y después, haga clic en **Siguiente**. El asistente le pedirá si quiere una zona de búsqueda directa o una zona de búsqueda inversa.

Cuando se selecciona **Zona de búsqueda directa**, el asistente le pide que especifique un nombre. Después se crea automáticamente la zona, el fichero de la base de datos de la zona, el registro SOA y NS. El contenido del fichero de la base de datos de la zona se replica entonces a todos los controladores de dominio.

Cuando se selecciona **Zona de búsqueda inversa**, el asistente le pide especificar la identificación de red y la máscara de subred, y verifica el nombre de la zona. Después el

asistente crea la zona automáticamente, el fichero de la base de datos y los registros SOA y NS.

2.4.2. Agregar registros DNS

Una vez creadas las zonas de búsqueda directa e inversa, puede dar de alta máquinas en el DNS. Para ello sitúe el cursor del ratón en la zona donde quiere dar de alta el registro y haga clic en el botón derecho, aparecerá la figura 4.14:

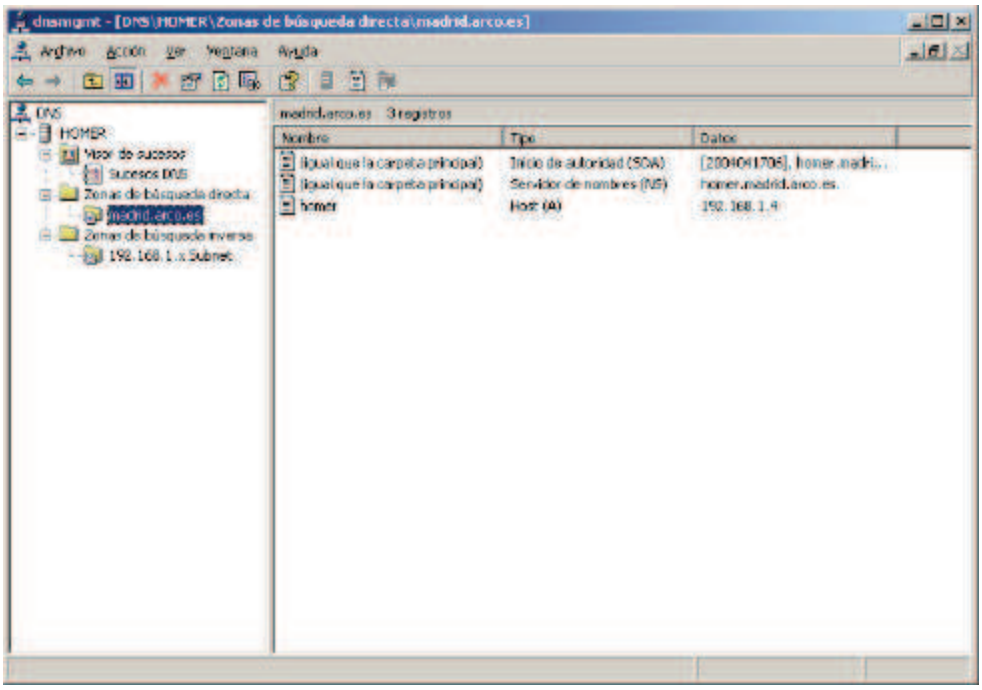

Figura 4.14: Consola de administración del servicio DNS

2.5. Herramientas para consultar a un servidor DNS

Las herramientas para interrogar al DNS permiten simular en cierta medida el comportamiento de los *resolvers* al permitir consultar a los servidores de DNS para detectar problemas en la configuración y/o funcionamiento del sistema. También pueden servir para obtener la información real que brinda este mecanismo de forma directa y sencilla.

La herramienta principal por excelencia para consultar a un servidor de nombres, ya sea para obtener información real o para chequear su configuración, es el programa *nslookup*.

2.5.1. El programa `nslookup`

Este programa posee dos modos en su comportamiento:

- ***Interactivo***: permite realizar un número ilimitado de consultas diversas acerca de distintos hosts y dominios utilizando a varios servidores de DNS. Provee un *prompt* en el cual se podrán ejecutar distintos comandos en correspondencia con las acciones a realizar. Para finalizar, se pulsará `Ctrl-D` o utilizar el comando `exit`.

- ***No interactivo***: se utiliza para realizar una única consulta para devolver sólo la información exacta de un host o un dominio a partir de un servidor.

El primer modo se obtiene cuando se invoca `nslookup` sin argumentos o cuando el primer argumento es "-" y el segundo, un nombre de dominio o una dirección IP de un servidor de DNS. En cambio el modo no interactivo se alcanza dado que se indica como primer argumento el nombre o dirección IP del host buscado y como segundo, opcionalmente, el nombre o la dirección del servidor a consultar. Además se pueden indicar opciones para expresar que tipo de información se buscará y como se hará.

En el modo interactivo se expresan a través del comando *set*. Los comandos más utilizados en el modo interactivo son:

- ***<nombre> [servidor]***

- ***<dirección IP> [servidor]***: devuelve información acerca del host dado su nombre o dirección IP a través de un servidor si se indica y sino, del servidor por defecto.

- ***server <servidor>***

- ***lserver <servidor>***: cambia el servidor de DNS por defecto. El primero emplea el servidor actual para resolver este nombre y el segundo utiliza el servidor por defecto anterior.

- ***Root:*** coloca como servidor por defecto a uno de los servidores del dominio raíz.

- ***ls [opción] <dominio> [> <fichero>]***

- ***ls [opción] <dominio> [>> <fichero>]:*** lista la información disponible para un dominio. Opcionalmente esta se escribe o se añade en el fichero especificado. Por defecto se muestran los records del tipo Address (A). Las opciones pueden ser:

    - ***-t <tipo>:*** lista los *records* del tipo especificado pertenecientes al dominio.

    - ***-a:*** lista los nombres canónicos y los alias de los hosts pertenecientes al dominio. Es equivalente a "`-t CNAME`".

- ***-d:*** lista todos los *records* presentes en el dominio. Es equivalente a "`-t ANY`".
- ***-h:*** lista la información del procesador y del sistema operativo correspondiente a los hosts del dominio. Es equivalente a "`-t HINFO`".
- ***-s:*** lista los servicios conocidos que ofrecen los hosts del dominio. Es equivalente a "`-t WKS`".

- ***Help:*** imprime una ayuda breve acerca de los posibles comandos.
- ***Exit:*** se utiliza para salir.
  - ***set <opción>[=<valor>]:*** permite fijar el valor de las opciones que modifican el comportamiento de todas las consultas subsiguientes. Las opciones se describen a través de una palabra, algunas poseen un valor asociado. Entre las opciones válidas se encuentran:
    - ***all:*** imprime los valores actuales de las opciones activadas.
    - ***class=<valor>:*** cambia la clase actual. Los posibles valores son *IN*, *HESIOD*, *CHAOS* y *ANY*.
    - ***[no]debug:*** habilita o deshabilita el modo de "*debug*".
    - ***domain=<dominio>:*** establece el dominio por defecto.
    - ***srchlist=<dominio1>/<dominio2>/.../<dominioN>:*** establece la lista de dominios para buscar los nombres de dominio relativos (aquellos que no contienen ningún punto por defecto). Para expresar que no se utilice esta lista en la resolución se puede colocar un punto al final del nombre a resolver. Se admite un máximo de seis nombres de dominios en la lista.
    - ***querytype=<valor>***
    - ***type=<valor>:*** cambian el tipo de *record* a devolver en una consulta. Por defecto es el *record Address*.
    - ***retry=<n>:*** indica el número de reintentos a realizar. Por defecto es igual a cuatro.
    - ***timeout=<n>:*** indica el tiempo en segundos que se espera por la respuesta a una consulta. En cada reintento este número se duplica. Por defecto es cinco segundos.
    - ***root=<host>:*** cambia el nombre del servidor del dominio raíz.

Ejemplos:

```
C:\> nslookup sion
Server:  alma.upm.es
Address:  192.168.100.2

Name:    sion.upm.es
Address:  192.168.200.4

C:\>  nslookup - alma.upm.es
Default Server:  alma.upm.es
Address:  192.168.100.2
> set srchlist=upm.es/linux.upm.es/windows.upm.es
> set all
Default Server:  alma.upm.es
Address:  192.168.100.2

Set options:
nodebug      defname      search       recurse
nod2         novc         noignoretc   port=53
querytype=A  class=IN     timeout=5    retry=2
root=f.root-servers.net.
domain=upm.es
srchlist=upm.es/linux.upm.es/windows.upm.es

> ls -t MX upm.es
$ORIGIN upm.es
*       1D IN MX    10 maildi
*       1D IN MX    20 odin
> set type=ns
> upm.es
Server:  alma.upm.es
Address:  192.168.100.2

upm.es              meserver = alma.upm.es
upm.es       nameserver = odin.upm.es
alma.upm.es       internet address = 192.168.100.2
odin.upm.es       internet address = 192.168.200.4
> exit

# nslookup -type=soa upm.es
Server:  alma.upm.es
Address:  192.168.100.2

upm.es
    origin = upm.es
    mail addr = alina.maildi.upm.es
    serial = 66
    refresh = 10800 (3H)
    retry   = 900 (15M)
    expire  = 604800 (1W)
    minimum ttl = 86400 (1D)
```