1 Servidores DNS y DHCP en Windows 2003

1.1 Servidores DNS. Teoria.

Todos los hosts con TCP/IP tienen una dirección de IP única que se utiliza para la comunicación con otros equipos de la red. Un equipo trabaja fácilmente con direcciones de IP, pero no las personas; los usuarios suelen identificar los sistemas por un nombre. Para facilitar una comunicación efectiva y eficiente, los usuarios deben poder referirse a los equipos por un nombre y permitir que su equipo use su dirección de IP transparentemente.

En los primeros días de ARPANET, el antecesor de la Internet actual, sólo existía un pequeño número de equipos conectados a la red. El Centro de Información de Red (NIC), ubicado en el Instituto de Investigaciones de Stanford, SRI (Stanford Research Institute), era el responsable de compilar en un único archivo, HOSTS.TXT, los nombres y direcciones de todos los equipos. Los administradores debían mandar un mensaje al SRI, quien actualizaba el archivo HOSTS.TXT. A continuación, los usuarios de ARPANET debían descargar la nueva versión del archivo HOSTS.TXT mediante el Protocolo de transferencia de archivos (FTP).

Con el crecimiento de ARPANET, resultaba obvio que este método no permitía crecer apropiadamente por las siguientes razones clave:

- El ancho de banda consumido para transmitir las versiones actualizadas de un archivo de host de ARPANET sería proporcional al cuadrado del número de hosts en la ARPANET. Con un número de hosts creciendo exponencialmente, el impacto a largo plazo probablemente sería de una sobrecarga que ningún host podría mantener.

- El archivo de host plano y estático significaría que no podría haber dos equipos en la ARPANET con la misma dirección. Al crecer el número de hosts, crece el riesgo de añadir nombres duplicados, así como la dificultad de intentar un control centralizado.

- La naturaleza de la red subyacente estaba cambiando -los grandes equipos de tiempo compartido con que se había construido ARPANET se estaban viendo desplazados por estaciones de trabajo- y cada una necesitaba un nombre de host único. Podría ser difícil, sino imposible, de controlar centralizadamente.

Con el crecimiento de ARPANET, resultaba más claro que se necesitaba una solución mejor. Se generaron varias propuestas según el concepto de servicio de nombres distribuido, que se basaban en un espacio de nombres jerárquico. Nacieron las RFC 882 y 883, donde se describe el diseño de un sistema de nombres de dominio, basado en una base de datos distribuida que contiene información generalizada de recursos. Este diseño evolucionó, y las RFC 1034 y 1035 describen el servicio del Sistema de nombres de dominio (DNS) que se usa hoy en Internet.

Descripción general de DNS en Microsoft Windows 2000.

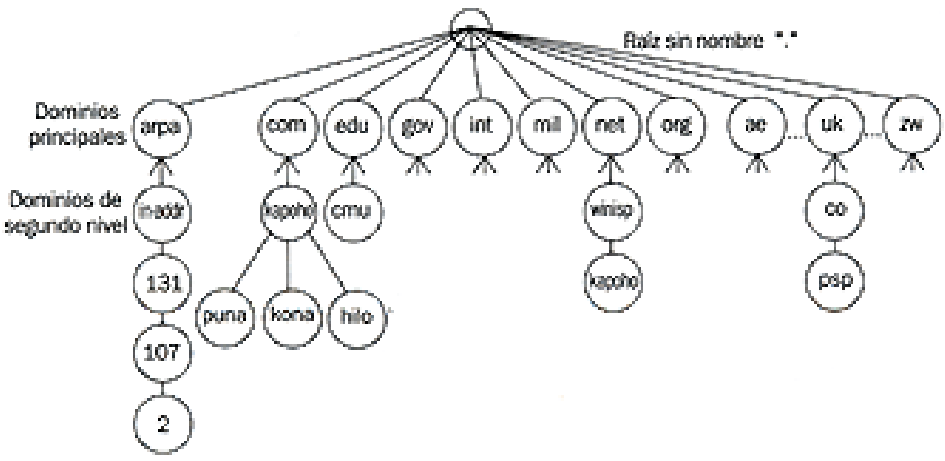
Para facilitar las comunicaciones entre equipos se les puede dar un nombre en un espacio de nombres. El espacio de nombres concreto define las reglas para dar nombre a un equipo y cómo se resuelve un nombre en una dirección de IP. Cuando un equipo se comunica con otro debe resolver, o convertir, un nombre de equipo en una dirección de IP según las reglas del espacio de nombres utilizado. Esta resolución se puede realizar mediante un servicio de resolución de nombres.

Existen dos espacios de nombres principales y métodos de resolución de nombres que se usan en Windows 2000: NetBIOS, implementado por el Servicio de Nombres de Internet de Windows (WINS) y DNS.

Términos clave DNS.

DNS es un servicio de nombres estándar del IETF. El servicio de DNS permite que un equipo cliente de la red registre y resuelva nombres de dominio de DNS. Estos nombres se utilizan para encontrar y acceder a recursos de otros equipos de la red o de otras redes como Internet. Los tres componentes principales de DNS son los siguientes:

- Espacio de nombres de dominio y los registros de recursos (RR) asociados. Una base de datos distribuida de información de nombres.
- Servidores de nombre de DNS. Servidores que mantienen el espacio de nombres de dominio y los RR y responden a las peticiones de los clientes de DNS.
- Resolvedores de DNS. Facilidad con la que un cliente de DNS se pone en contacto con servidores de nombre de DNS y envía peticiones de nombre para obtener información de registros de recursos.



El espacio de nombres de dominio está estructurado de manera jerárquica en un árbol que empieza en una raíz sin nombre para todas las operaciones de DNS. En el espacio de nombres de DNS cada nodo y cada hoja en el árbol del espacio de nombres de dominio representan un dominio con nombre. Cada dominio puede tener dominios hijos adicionales.

Nombre de Dominio.

Cada nodo en el árbol de DNS tiene un nombre distinto, llamado etiqueta (label) como se le denomina en la RFC 1034. Cada etiqueta de DNS puede tener entre 1 y 63 caracteres y el dominio raíz no tiene caracteres.

Un nombre de dominio concreto es la lista de etiquetas en la ruta desde el nodo nombrado hasta la raíz del árbol de DNS. La convención de DNS es que las etiquetas que componen un nombre de dominio se leen de izquierda a derecha, desde lo más concreto hasta la raíz, por ejemplo, www.midominio.com. Este nombre completo también se denomina nombre de dominio completo, FQDN (Fully Qualified Domain Name).

Los nombres de dominio se puede almacenar en mayúsculas o en minúsculas, pero todas las comparaciones y funciones de dominios se definen como insensibles a mayúsculas y minúsculas en la RFC 1034. Por tanto, www.midominio.com es idéntico a WWW.MIDOMINIO.COM para las operaciones de nombrado de dominios.

Dominios Superiores.

Un dominio superior es un dominio de DNS directamente debajo de la raíz. Resulta difícil crear nombres adicionales, al menos en Internet. Las tres categorías de dominios superiores son las siguientes:

- <ARPA>. Es un dominio especial, se usa en la actualidad para búsqueda inversa de nombres.
- Dominios de 3 letras. Existen siete dominios superiores de 3 caracteres. (en la actualidad, estos nombres se han incrementado con algunos más).
- Nombres de 2 letras para los países. Estos dominios con código de país se basan en los nombres de país de la Organización Internacional de Normalización (ISO) y se usan, principalmente, por compañías y organizaciones fuera de los EE.UU. La excepción es UK, que utiliza .UK como dominio superior, aunque el código de país de ISO es GB.

Registros de recursos de DNS.

Un registro de recurso es un registro que contiene información relacionada con un dominio que puede contener la base de datos de DNS y que puede solicitar y usar un cliente de DNS. Por ejemplo, el RR de host de un dominio concreto mantiene la dirección de IP de tal dominio (host); un cliente de DNS podrá utilizar este RR para conseguir la dirección de IP para el dominio.

Cada servidor de DNS contiene los RR relacionados con aquellas porciones del espacio de nombre de DNS para el que es autoridad, o para el que puede responder las solicitadas por un host.

Cuando un servidor de DNS es autorizado para una porción del espacio de nombres de DNS, dichos administradores del sistema son los responsables de asegurar que la información sobre esa porción del espacio de nombres de DNS es correcta. Para aumentar la eficiencia, un servidor de DNS dado puede hacer caché de los RR relativos a un dominio de cualquier parte del árbol de dominios.

Cada RR contendrá un conjunto de información común, como la siguiente:

- Propietario. Indica el dominio de DNS en el que se encuentra el registro de recurso.
- TTL. Tiempo que utilizan otros servidores de DNS para determinar durante cuanto tiempo se hace caché de la información de un registro antes de descartarla. Para la mayoría de los RR, este campo es opcional. El valor de TTL se mide en segundos, con un valor de 0 que indica que el RR contiene datos volátiles que no se deben guardar en caché. Por ejemplo, los registros SOA tienen un valor de TTL predeterminado de 1 hora. De esta forma se evita que otros servidores mantengan en caché estos registros durante largos períodos de tiempo, lo que podría retrasar la propagación de cambios.
- Clase. Para la mayoría de los RR, este campo es opcional. Cuando se utiliza, contiene un texto mnemónico que indica la clase de un RR. Por ejemplo, una clase con IN indica que el registro pertenece a la clase Internet (IN). Alguna vez existieron muchas clases, como CH para Chaos Net, pero en la actualidad sólo se usa la clase IN.
- Tipo. Este campo es requerido y mantiene un texto mnemónico estándar que indica el tipo del RR. Por ejemplo, el mnemónico A indica que el RR guarda la información de dirección (Address) del host.
- Datos específicos del registro. Es un campo de tamaño variable que contiene información que describe el recurso. Este formato de información varía de acuerdo con el tipo y clase del RR.

Los archivos de zona de DNS estándar contienen el conjunto de RR de dicha zona en un archivo de texto. En este archivo de texto, cada RR se encuentra en una línea separada y contiene todos los elementos de datos anteriores, como un conjunto de campos de texto separados por espacios en blanco. En el archivo de zona, cada RR consta de los elementos de datos anteriores, aunque diferentes registros pueden contener registros con formatos ligeramente diferentes para datos específicos.

Registros de recursos que admite Windows 2000.

Existen numerosos tipos de RR definidos en las RFC 1035, 1036 y posteriores. La mayoría de los tipos de RR ya no se necesitan ni se usan, aunque todos esos están disponibles en Windows 2000. Los RR usados más habitualmente, son:

- Dirección de host (A) [Adress 32 bits] Este RR contiene un RR dirección de host que hace corresponder un nombre de dominio de DNS con una dirección de IPv4 de 32 bits.

  Tipo. A

  Sintaxis. Propietario A dirección_IPv4

  Ejemplo. kona A 10.10.2.200

- Nombre canónico (CNAME) [canonical name] El RR nombre canónico (CNAME) permite a los administradores de red crear un alias de otro nombre de dominio. El uso de RR CNAME se recomienda para su uso en los siguientes escenarios:

  Cuando un host especificado en un RR (A) de la misma necesita cambiar de nombre. Por ejemplo, si necesita cambiar el nombre de kona.midominio.com a hilo.midominio.com, crearía una entrada CNAME para kona.midominio.com que apuntase a hilo.midominio.com.

Cuando un nombre genérico de un servicio conocido, como ftp o www, se necesita resolver a un grupo de equipos individuales, cada uno con un RR (A) individual. Por ejemplo, podría querer que www.midominio.com fuese un alias de kona.midominio.com y hilo.midominio.com. Un usuario que accediese a www.midominio.com normalmente no advertiría qué equipo realmente sirve la solicitud.

Este RR hace corresponder un alias o nombre de dominio de DNS alternativo en el campo Propietario (Owner) con un nombre canónico, real, de DNS. Debe haber también un RR (A) para el nombre de dominio de DNS canónico, que se debe resolver a un nombre de dominio de DNS válido en el mismo espacio de nombres. El nombre canónico completo debería terminar con un punto («.»).

Tipo. CNAME

Sintaxis. Alias CNAME Nombre_canónico o alias

Ejemplo. ns1 CNAME alias.midominio.com.

- Puntero (PTR) [Pointer reverse] Este RR que se usa para los mensajes de búsqueda inversa de nombre apunta en la dirección de IP del campo Propietario (Owner) otra ubicación en el espacio de nombres de DNS como especifica el nombre_de dominio_objetivo. Normalmente, se usa sólo el árbol de dominio in-addr.arpa para la búsqueda inversa de la correspondencia dirección-nombre. En la mayoría de los casos, cada registro proporciona información que apunta a otra ubicación de un nombre de dominio de DNS, como un RR A de dirección de host en una zona de búsqueda inversa.

  Tipo. PTR

  Sintaxis. Propietario PTR nombre_de_dominio_objetivo

  Ejemplo. 200 PTR kona.midominio.com

- Localizador de servicio (SRV) [Server] El RR SRV (Service Locator) permite a un equipo localizar un host que disponga de un cierto servicio, como el Controlador de dominio del Active Directory de Windows 2000. De esta forma el administrador puede tener múltiples servidores, cada uno proporcionando un servicio similar basado en TCP/IP que se puede localizar con una única operación de solicitud de DNS. Este registro se usa, principalmente, para disponer del AD de Windows 2000, donde todos los RR de DNS relevantes se pueden incluir automáticamente en el DNS.

  Tipo. SRV

  Sintaxis. nombre_del_protocolo_de_servicio SRV preferencia peso Puerto objetivo

  Ejemplo._ldap._tcp.dc _msdcs 600 SRV 0 100 389 kona.midominio.com

Los RR se pueden asociar a cualquier nodo del árbol de DNS, aunque los RR no existirán en algunos dominios; por ejemplo, los RR Puntero (PTR) se encuentran sólo en los dominios debajo del dominio in-addr.arpa. Por ello, los dominios superiores, como microsoft.com, pueden tener RR individuales -por ejemplo, un registro de Intercambio de correo (MX) para el correo que se envíe a Microsoft Corporation-, así como disponer de subdominios que también podrían disponer de RR individuales; por ejemplo, eu.microsoft.com, que tiene un registro de host www.eu.microsoft.com.

Operación de Solicitud de DNS

Un cliente efectúa una operación de solicitud a un servidor de DNS para conseguir parte o toda la información de RR relacionada con un determinado dominio, por ejemplo, para determinar qué registro o registros de hosts (A) se mantienen sobre el dominio llamado midominio.com. Si el dominio existe y también el RR solicitado, el servidor de DNS devolverá la información solicitada en un mensaje de respuesta a la solicitud. El mensaje de respuesta devolverá tanto la solicitud inicial como la respuesta con los registros relevantes, suponiendo que el servidor de DNS pueda conseguir los RR necesarios.

La solicitud de DNS, a la que se refiere la RFC 1034 como solicitud estándar, contiene un nombre de dominio objetivo, un tipo de solicitud y una clase de solicitud. La solicitud contendrá una solicitud de uno o varios RR concretos que se desean obtener, o una solicitud que devuelva todos los RR relativos al dominio.

Solicitud inversa

Una solicitud inversa es aquella en la que se solicita a un servidor de DNS el nombre de dominio de DNS de un host con una determinada dirección de IP. Los mensajes de Solicitud de búsqueda inversa son, realmente, solicitudes estándar, pero relacionadas con las zonas de búsqueda inversa.

Las zonas de búsqueda inversa se basan en el nombre de dominio in-addr.arpa y mantiene, principalmente, los RR de PTR.

La creación de zonas de búsqueda inversa y el uso de RR de PTR para identificar los hosts son partes optativas del estándar de DNS. Las zonas de búsqueda inversa no son obligatorias en Windows 2000, aunque algunas aplicaciones de red pueden configurarse para que usen las zonas de búsqueda inversa como forma adicional de seguridad.

Las solicitudes inversas se describieron originalmente en la RFC 1032, pero ya están obsoletas. Una solicitud inversa significa buscar un nombre de host por su dirección de IP y utilizar una operación de solicitud de DNS no estándar. El uso de las solicitudes inversas está limitado a algunas de las primeras versiones de NSLOOKUP.EXE, una utilidad para probar y resolver problemas del servicio de DNS. El servidor de DNS de Windows 2000 reconoce y acepta los mensajes de solicitud inversa y responde con una <simulación>.

Clases de solicitudes de DNS

Las solicitudes de DNS pueden ser de dos clases: recursivas o iterativas.

Una solicitud recursiva es una solicitud de DNS que se envía a un servidor de DNS en la que el host solicitante pregunta al servidor de DNS para que le proporcione una respuesta completa a la solicitud, aunque ello signifique que tenga que ponerse en contacto con otros servidores para obtener la respuesta. Cuando se envía una solicitud recursiva, el servidor de DNS usa un conjunto de solicitudes iterativas a otros servidores de DNS como intermediario del host solicitante para conseguir la respuesta a la solicitud.

Una solicitud iterativa es una solicitud de DNS que se envía a un servidor de DNS en el que el host solicitante pide que se devuelva la mejor respuesta que el servidor de DNS pueda proporcionar sin buscar ayuda adicional de otros servidores de DNS.

En general, los equipos envían solicitudes recursivas. Los equipos suponen que el servidor de DNS conoce la respuesta a la solicitud, o puede encontrarla. Por otra parte, un servidor de DNS

normalmente enviará solicitudes iterativas a otros servidores de DNS si no puede responder a la solicitud con la información de que dispone.

Operación de Actualización de DNS

Una operación de actualización de DNS la envía un cliente a un servidor de DNS para actualizar, añadir o eliminar algunos o todos los RR de información relacionada con un determinado dominio, por ejemplo, para actualizar el registro de host del equipo con nombre kona.midominio.com para que apunte a 10.10.1.100. La operación de actualización también se denomina actualización dinámica.

Resolución de nombres: Resolutor 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.

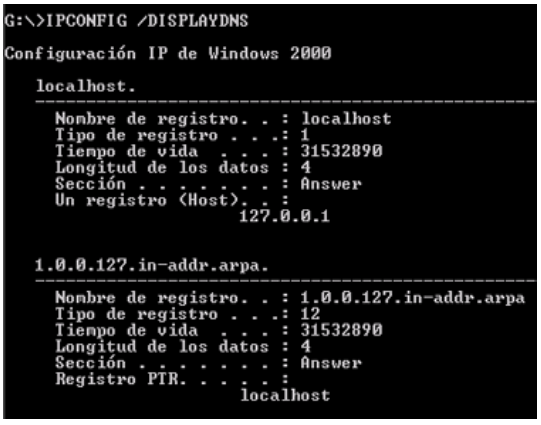
En Windows 2000, el resolutor forma parte del servicio Cliente de DNS. Este servicio se instala automáticamente cuando se instala TCP/IP y se ejecuta como parte del proceso Services.Exe. Como la mayoría de los servicios de Windows 2000, el servicio Cliente de DNS se activa en el dominio System de Windows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

Caché del resolutor de DNS

Un host de IP podría necesitar ponerse en contacto periódicamente con otro host y por tanto necesitaría resolver un nombre concreto de DNS muchas veces, como por ejemplo el nombre del servidor de correo electrónico. Para evitar tener que enviar solicitudes a un servidor de DNS cada vez que el host quiere resolver el nombre, Windows 2000 implementa una caché especial de información de DNS.



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

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

Caché negativa

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

Si se realiza una solicitud a un servidor de DNS y la respuesta es negativa, las siguientes solicitudes al mismo nombre de dominio se responden negativamente durante un tiempo predeterminado de 300 segundos.

Para evitar guardar en la caché información negativa anticuada, cualquier información de solicitud respondida negativamente se mantiene durante un período de tiempo inferior al que se utiliza para las respuestas positivas. Con la caché negativa se reduce la carga en los servidores de DNS, pero estarán disponibles los RR relevantes, y se podrán enviar solicitudes posteriores para obtener la información.

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

La orden IPCONFIG puede ser usada con el parámetro /FLUSHDNS para vaciar la caché del resolutor, con lo que también eliminamos la caché negativa.

Delegación de zona

DNS es una base de datos distribuida de información diseñada específicamente para superar las limitaciones de la resolución de nombres anterior con el archivo HOSTS.TXT. La clave de DNS para manejar grandes espacios de nombres/redes, como Internet, es su capacidad para delegar la administración de dominios. Se produce una delegación de zona cuando la responsabilidad de los RR de un subdominio se traslada del propietario del dominio principal al propietario del subdominio.

En el núcleo de Internet existen 13 servidores raíz, denominados de A.ROOTSERVERS.NET a M.ROOT-SERVERS.NET. Los servidores raíz están extensamente distribuidos. Mantienen datos de todos los dominios de nivel superior, como los .com, .org y .net, así como para los dominios geográficos como .uk y .jp. Estos servidores raíz permiten a los hosts de Internet tener un acceso a toda la base de datos de DNS. Por debajo de los dominios raíz y superior están los dominios y subdominios de las organizaciones individuales. En algunos dominios superiores existen niveles jerárquicos adicionales. Por ejemplo, en el domino .uk existe un subdominio co.uk para las compañías de UK (por ejemplo, psp.co.uk) y ac.uk para las instituciones académicas (por ejemplo, ic.ac.uk para el Imperial College).

La delegación ocurre como una división del DNS en las responsabilidades para los dominios debajo de la división que se delega del dominio superior. En el dominio midominio.com está el subdominio jh.midominio.com. La responsabilidad para el dominio subordinado se ha delegado a un servidor diferente.

Para implantar la delegación, la zona superior debe tener tanto un RR A como un registro de Servicio de nombre (NS), ambos apuntando a la nueva raíz de dominio delegado.

Cliente de actualización dinámica de DNS

En grandes redes, conseguir toda la información de RR necesaria en el DNS y mantenerla actualizada puede ser una tarea importante. El mantenimiento de los registros de hosts, en algunos entornos, puede ser un trabajo a tiempo completo para una o más personas. Para simplificar esta tares, Windows 2000 incluye la actualización dinámica de DNS, como se describe en la RFC 2136.

Mediante el DNS dinámico, los clientes envían un mensaje de registro de DNS al servidor de DNS, indicándole que actualice el registro (A) para el host. Además, si el cliente es también cliente de DHCP, cada vez que ocurre un suceso de dirección, por ejemplo, una concesión de una nueva dirección o una renovación de dirección, como parte del proceso de administración de las concesiones de DHCP, el cliente de DHCP envía la Opción 81 al servidor de DHCP junto con su nombre completo. La Opción 81 indica al servidor de DHCP que registre el RR PTR por él. Los equipos con Windows 2000 que se configuran estáticamente registrarán el RR (A) y el RR PTR en el servidor de DNS esos mismos.

Si un cliente de DHCP de Windows 2000 se comunica con un servidor de DHCP de menor nivel que no maneja la Opción 81, el cliente registra un RR PTR por sí mismo. El servidor de DNS de Windows 2000 es capaz de manejar las actualizaciones dinámicas.

Este mecanismo, donde el cliente actualice el registro (A) y el servidor de DHCP actualice el registro PTR, es el elegido porque sólo el cliente conoce qué direcciones de IP en el host se corresponden con el nombre del host. El servidor de DHCP puede que no sea capaz de realizar correctamente el registro del RR (A) debido a un conocimiento parcial. Si resulta apropiado también se puede configurar el servidor de DHCP para registrar ambos registros en el DNS.

Soporte para IPv6

IP versión 6 (IPv6) es una nueva versión del Protocolo Internet. Aunque Windows 2000 no se venderá con una pila de TCP/IP IPv6 nativo, el servidor de DNS de Windows 2000 admite IPv6 mediante la implantación de elementos de funcionalidad adicional, entre ellas las siguientes:

RR *AAAA*. Es un nuevo tipo de registro que se define para guardar una dirección de IPv6 de un host. Un host de IPv6 multinodo, por ejemplo, un host con más de una dirección de IPv6, debe tener más de un registro *AAAA*. El RR *AAAA* es similar al recurso (A), pero utilizando un tamaño de dirección mayor. La dirección de IPv6 de 128 bits se codifica en la porción de datos de un RR *AAAA* en el orden de los bytes de red, primero el Byte de mayor orden.

Solicitud *AAAA*. Una solicitud *AAAA* para un nombre de dominio concreto en la clase Internet devolverá todos los RR *AAAA* asociados en la sección respuesta de una respuesta. Una solicitud de tipo *AAAA* no realiza un procesamiento adicional de sección.

Dominio IP6.INT. Este dominio se usa para la función de búsqueda inversa para los hosts de IPv6, como se usa el dominio in-addr.arpa con las direcciones de IPv4.

De forma similar al dominio in-addr.arpa para IPv4, una dirección de IPv6 se representa como un nombre en el dominio IP6.INT por una secuencia de nibbles separados por puntos con el sufijo <.IP6.INT.> . La secuencia de nibbles se codifica en orden inverso; es decir, el nibble de menor orden se codifica en primer lugar, colocando el nibble de mayor orden el último. Cada nibble se

representa por un dígito en hexadecimal. Por ejemplo, el nombre de dominio de búsqueda inversa correspondiente a la dirección 4321:0:1:2:3:4:567:89a:b sería b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.INT.

Por último, para disponer de IPv6, todos los tipos de solicitud de DNS que realizan un procesamiento adicional de la sección A, como los tipos de solicitud NS o intercambio de correo (MX), deben admitir tanto los registros A como los AAAA y deben realizar cualquier procesamiento asociado a ambos tipos de registros. Esto quiere decir que el servidor de DNS añadirá cualquier dirección de IPv4 relevante y cualquier dirección de IPv6 relevante disponible localmente a la sección adicional de una respuesta cuando se procese cualquier solicitud.

1.2 Instalación y configuración de un servidor DNS.

Los servidores DNS son una parte esencial de una red basada en TCP/IP además de una parte esencial del Active Directory. Microsoft recomienda la instalación de DNS en cada controlador de dominio cuando se utilice Active Directory. Esta solución permite al servidor DNS dinámico de Windows 2000 utilizar Active Directory para almacenar información de la zona, permitiendo de este modo la réplica con múltiples maestros completa de la zona por medio de Active Directory, simplificando la tarea de conseguir la tolerancia a fallos y haciendo menos difícil la administración del DNS.

Es fundamental instalar DNS en el controlador primario que forme el raíz del árbol en un bosque nuevo. Si no se instaló DNS en el controlador de dominio durante la instalación de Windows 2000, es posible añadirlo, aunque son necesarios ciertos pasos de configuración que pueden dificultar mucho la puesta en marcha del Active Directory.

Configuración del servicio DNS

Las zonas son los cerebros del DNS; por lo tanto, el servidor DNS es inútil hasta que se configuren las zonas del dominio. Las zonas permiten almacenar porciones del espacio de nombres del DNS de forma que un único servidor DNS pueda servir una porción del espacio de nombres.

Cuando se configuran los dominios, hay que comenzar por el dominio de nivel más alto. Después hay que crear los subdominios y delegar el control de los dominios a otros servidores DNS si fuese necesario.

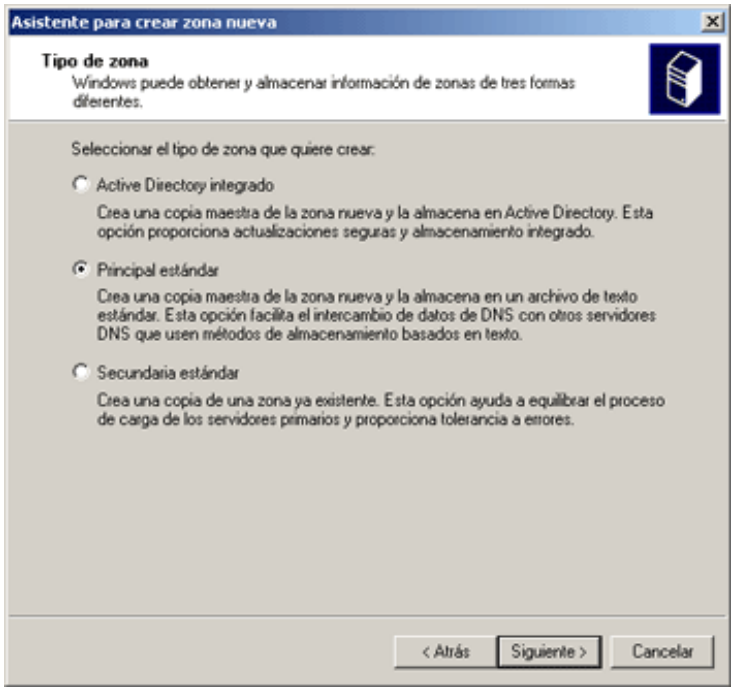
Los dos tipos de zonas que es necesario tomar en consideración son las zonas de búsqueda directa y las zonas de búsqueda inversa.

- Las zonas de búsqueda directa son los tipos de zonas que se asocian normalmente con servidores DNS; ellas devuelven una dirección IP cuando se les proporciona un nombre DNS. Estas zonas se suelen crear automáticamente cuando instalamos el Active Directory, de modo que no tendremos que crearlas a mano. Sin embargo, su creación no es inmediata, y suelen necesitar que exista cierta actividad dentro del dominio antes de que se creen correctamente.

- Las búsquedas inversas se utilizan menos a menudo, aun siendo importantes de todos modos. Proporcionan la capacidad de asignar un nombre DNS a una dirección IP, algo que los Servicios de Internet Information Server (IIS) también utilizan para sus archivos de registro y herramientas de solución de problemas como Nslookup. Es importante destacar que estas zonas de busqueda inversa no se crean automáticamente, y tendremos que crearlas siempre a mano.

Creación de una nueva zona

Para crear una nueva zona de búsqueda directa en el servidor DNS para que los clientes puedan obtener la dirección IP de un nombre DNS, hay que seleccionar DNS en la carpeta Herramientas administrativas, Seleccionar el servidor DNS en el árbol de la consola. Escoger entonces Crear una zona nueva en el menú Acción para iniciar el Asistente para crear zona nueva. Hay que pulsar Siguiente para comenzar a utilizar el asistente.



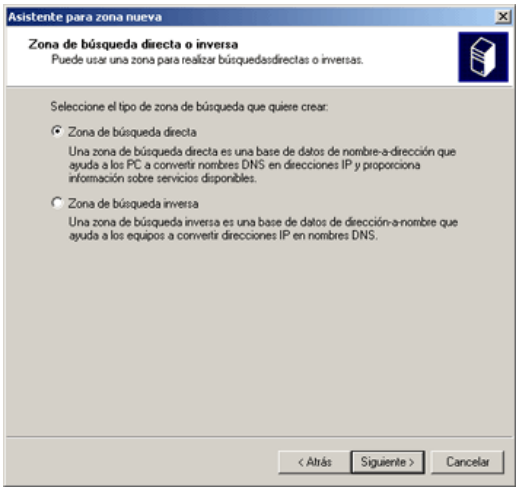
Tipo de Zona: En esta ventana hay que escoger una de las siguientes opciones y pulsar entonces Siguiente para continuar:

Active Directory integrado: Se debe utilizar si todos los controladores de dominio ejecutan Windows 2000. Esta opción también se puede utilizar en una red mixta si los servidores UNIX son compatibles con el DNS de Microsoft.

Principal estándar: Se debe utilizar si el servidor DNS ejecuta Windows 2000 pero no es un controlador de dominio.

Secundaria estándar: Se debe utilizar si el servidor DNS está alojado en servidores UNIX. También se debe utilizar si este servidor va a tener privilegios de sólo lectura en la zona para toda la información obtenida del servidor DNS principal.

Zona de búsqueda directa o inversa. Esta ventana nos permite escoger el tipo de zona que queremos crear.

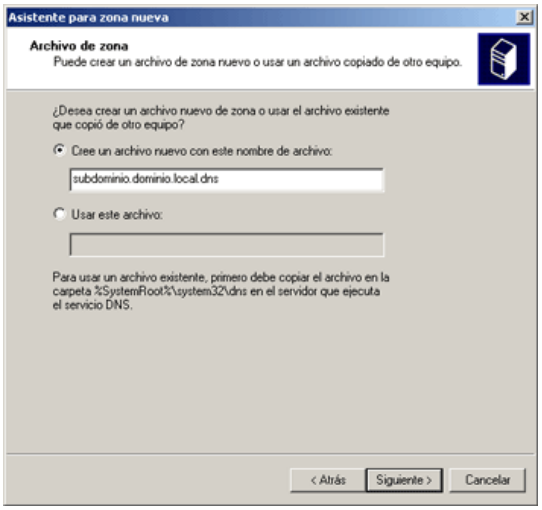


Zona de búsqueda directa: Es la que permite a los clientes buscar los equipos de la red a través de los nombres, convirtiendo los nombres DNS a direcciones IP.

Zona de búsqueda inversa: Las zonas de búsqueda inversa permiten a los clientes obtener el nombre DNS de un host a partir de una dirección IP, lo que resulta útil para herramientas de solución de problemas como Nslookup. Y realizar una búsqueda inversa junto con los archivos de registro de IIS permite el registro de un nombre DNS en lugar de una dirección IP. Para crear una zona de busqueda inversa tenemos que indicar la parte fija de las direcciones IP de nuestra red. Normalmente en nuestro caso siempre creamos la zona de busqueda inversa como 192.168.x.x.

Nombre de Zona: Introducir el nombre DNS para la zona en el cuadro de texto Nombre y pulsar Siguiente

Si se ha escogido la instalación de una Zona Active Directory Integrada, se creará ahora. Si se está creando una Zona principal estándar, seguirá el proceso de instalación. Para una Zona secundaria estándar se abre la ventana Servidores maestros DNS. Hay que introducir las direcciones IP de los servidores maestros de los cuales se desea copiar la información de zona, pulsando Agregar después de introducir cada una. Se puede utilizar el botón Examinar para buscar servidores. Se pueden utilizar los botones Arriba y Abajo para organizar las direcciones IP en el orden en el que se deseen contactar. Hay que pulsar Siguiente cuando se haya terminado y pulsar después Finalizar para completar la configuración de la zona secundaria.



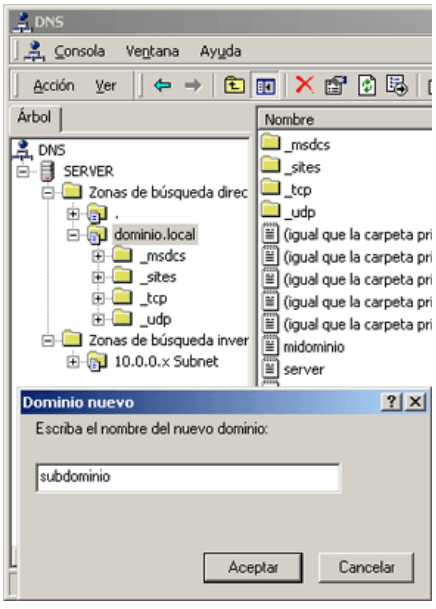
Archivo de Zona: Nos permitirá elegir el archivo que queremos utilizar para la Zona DNS que estamos creando.

Cree un archivo nuevo con este nombre de archivo: introducir el nombre que se le quiere dar al archivo de zona o utilizar el que se proporciona.

Usar este archivo: Para utilizar una archivo de zona existente para almacenar la información de la zona, hay que copiar el archivo a la carpeta %SystemRoot%\System32\DNS. Esta es la opción a elegir si estamos importando una Zona DNS desde otro sistema.

Creación de subdominios y delegación de autoridad

En muchos entornos de red grandes es necesario crear subdominios y delegar su administración a otras zonas DNS que estén alojadas en otros servidores DNS. Este paso elimina la situación de tener un enorme espacio de nombres alojado en una única zona de un único servidor. Por lo tanto, se debería tener una zona que contuviera el dominio raíz dominio.com además del subdominio marketing.dominio.com; sin embargo, se debería tener el subdominio subdominio.dominio.com y sus subdominios delegados a una zona separada administrada por otro servidor DNS.

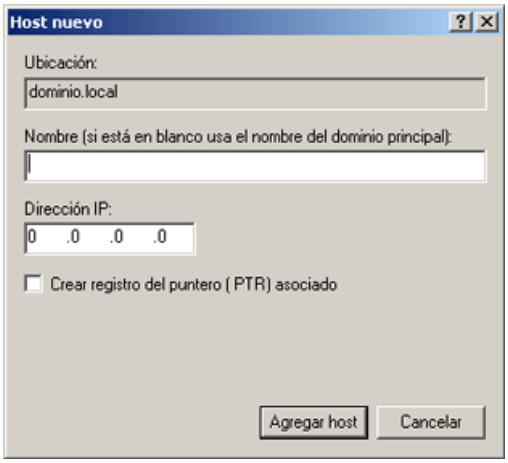


Hay que asegurarse de que se tiene un registro de host creado para el servidor DNS en la Zona de búsqueda directa y un registro del puntero para el servidor DNS en la Zona de búsqueda inversa. Puede que el DNS no los cree automáticamente (especialmente el registro del puntero), por lo que conviene verificar ambos; en otro caso el servidor podría no funcionar.

Conviene observar que las zonas deben tener un espacio de nombres contiguo, por lo que no es posible combinar subdominios de diferentes ramas del espacio de nombres y situarlos en una única zona: sería necesario crear zonas separadas para cada parte no contigua del dominio.

Agregación de registros de recursos del host

Después de crear las zonas y los subdominios se deberían añadir registros de recursos (RR) para el servidor del dominio y cualquier otro servidor con direcciones IP estáticas o reservas de IP (servidores DHCP, servidores WINS, enrutadores, etc.). El servidor DNS no funcionará adecuadamente sin un registro de host y un registro del puntero, este último no se creará de forma automática.



- Seleccionar la zona y dominio o subdominio al cual pertenece el host y escoger entonces Host nuevo en el menú Acción.
- Introducir el nombre del host o dejar el cuadro Nombre en blanco para utilizar el nombre del dominio principal. Hay que introducir la dirección IP del host.
- Seleccionar Crear registro del puntero (PTR) asociado para crear un RR para el host en la zona de búsqueda inversa.
- Pulsar Agregar host y rellenar después los campos para cualquier registro de host adicional que se quiera crear o pulsar Realizado.

Cuando instalamos el DNS por primera vez, veremos como aparecen algunos hosts del tipo A con nombre de host y que sin embargo no están creados en la zona de búsqueda inversa. Estos host hay que borrarlos de la zona directa y volver a crearlos de la forma que se ha explicado.

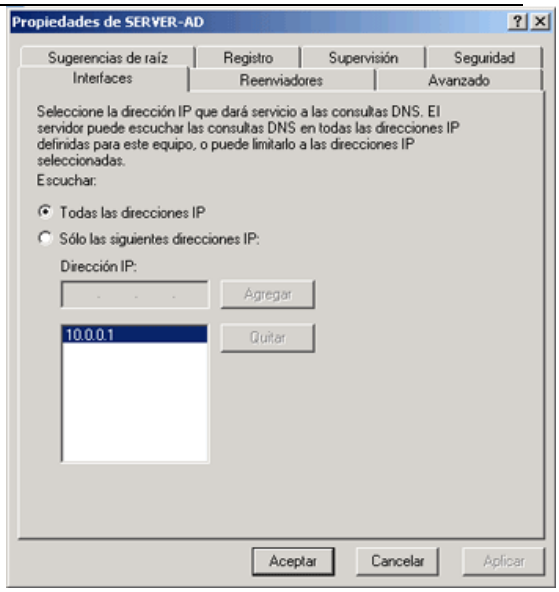
Para actualizar manualmente el archivo de zona, hay que seleccionar la zona que se desea actualizar y escoger entonces Actualizar archivo de datos del servidor en el menú acción.

Interoperación con otros servidores DNS

De forma predeterminada, el servidor DNS de Windows 2000 realiza transferencias de zona rápidas con compresión de datos y envío de múltiples registros de recursos en cada mensaje. Este método de transferencia de zona funciona con todos los servidores DNS de Windows y servidores DNS BIND versión 4.9.4 o posterior. Si se necesita realizar transferencias de zona con servidores BIND anteriores a la versión 4.9.4, será necesario desactivar este método de transferencia de zona rápida. Hay que seleccionar el servidor DNS en el árbol de la consola y escoger propiedades en el menú Acción. Después hay que pulsar la pestaña Avanzado y desactivar la casilla de verificación Enlazar secundarios.

1.3 Administración del servidor DNS.

Pestaña Interfaces.



En el caso de los servidores DNS multitarjeta (que funcionan en ordenadores con varias tarjetas de red), puede configurar el servicio DNS para habilitar de forma selectiva y enlazar sólo con las direcciones IP que especifique con la consola DNS. De forma predeterminada, el servicio DNS enlaza con todas las interfaces IP configuradas para el equipo. Esto puede incluir:

- Cualquier dirección IP adicional configurada para una conexión de red única.
- Direcciones IP individuales configuradas para cada conexión diferente donde haya instaladas más de una conexión de red en el equipo servidor.

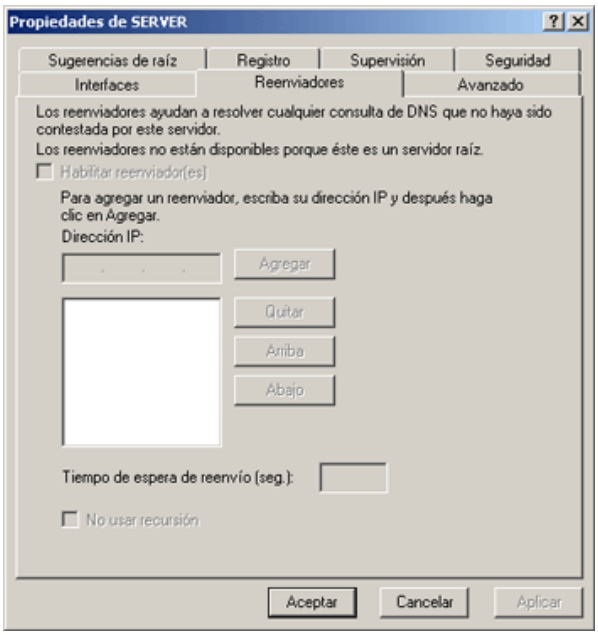
En el caso de los servidores DNS multitarjeta, puede restringir el servicio DNS para las direcciones IP seleccionadas. Cuando se utilice esta característica, el servicio DNS sólo atenderá y responderá a las peticiones DNS que se envíen a las direcciones IP especificadas en la ficha Interfaz de las Propiedades del servidor.

De forma predeterminada, el servicio DNS atiende en todas las direcciones IP y acepta todas las solicitudes de clientes enviadas a su puerto de servicio predeterminado (UDP 53 o TCP 53 para solicitudes de transferencia de zona). Algunos interpretadores de nombres DNS (incluidos los clientes de la versión original de Windows 95) requieren que la dirección de origen de una respuesta DNS sea la misma que la dirección de destino que se utilizó en la consulta. Si estas direcciones son diferentes, los clientes pueden rechazar la respuesta. Para adaptar estos interpretadores de nombres, puede especificar la lista de interfaces permitidas para el servidor DNS. Cuando se establezca una lista, el servicio DNS enlazará sockets sólo a las direcciones IP permitidas utilizadas en el equipo.

Además de para admitir clientes que requieren el uso de enlaces explícitos, especificar las interfaces puede ser útil por otras razones:

- Si, por razones administrativas, no desea utilizar algunas direcciones IP o interfaces en un equipo servidor multitarjeta.
- Si el equipo servidor está configurado para utilizar un gran número de direcciones IP y no desea el gasto agregado que supone enlazarlas todas.

Pestaña Reenviadores



Ningún servidor de nombres será capaz de responder a las consultas de todos los clientes; algunas veces los clientes solicitarán un nombre DNS que no se encuentra en ninguna de las zonas administradas por el servidor DNS. En estos casos, se puede configurar un servidor DNS para que reenvíe la petición a otro servidor DNS con más probabilidad de tener el registro en su zona o archivo caché. Esta capacidad se necesita más frecuentemente para resolver nombres externos a la red en la que residen los clientes.

Cuando un cliente quiere resolver un nombre fuera de la red interna, se puede configurar un servidor DNS interno para que reenvíe la consulta a un servidor DNS externo a la red, quizás al otro lado de un cortafuego. Este servidor de nombres externo puede entonces realizar consultas más a fondo fuera de la red si es necesario y devolver los resultados al servidor DNS reenviador. Para configurar el servidor DNS de forma que reenvíe las consultas no resueltas a otro servidor DNS, hay que seguir estos pasos:

(Por razones de seguridad, un único servidor DNS reenviará por regla general las peticiones de la red interna a un servidor DNS al otro lado de un cortafuego. El resto de los servidores DNS internos reenvían sus consultas al reenviador designado para que sean pasadas al servidor de nombres externo (o resueltas a partir del archivo caché del reenviador).

- En el árbol de la consola, hay que seleccionar el servidor DNS sobre el que se desea activar el reenvío, y escoger después propiedades en el menú Acción.
- Escoger la ficha Reenviadores y seleccionar la casilla de verificación Habilitar reenviador(es).
- Introducir las direcciones IP del servidor o servidores DNS a los cuales se desea reenviar las consultas no resueltas, pulsando el botón Agregar tras introducir cada una.
- Antes de avanzar al siguiente servidor de la lista de servidores a los que reenviar consultas, hay que introducir la cantidad de tiempo que se desea emplear en contactar con un servidor DNS.
- Para configurar el servidor DNS como un servidor esclavo -un servidor que no trata de resolver ninguna consulta a partir de sus propios archivos de zona o caché- hay que seleccionar la casilla de verificación No usar recursión

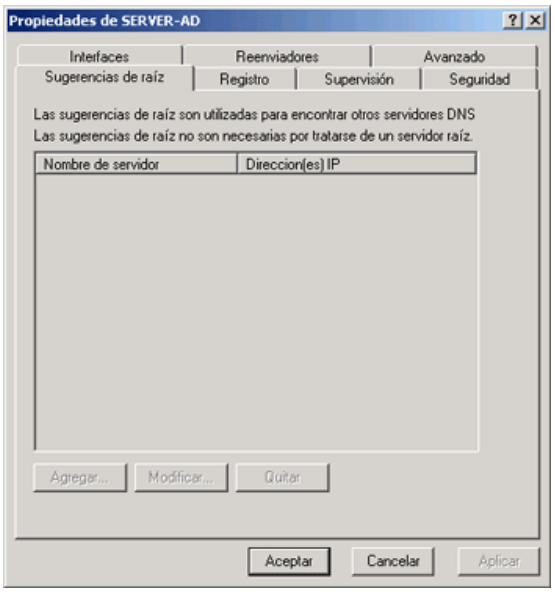
Pestaña Avanzadas

Cuando se inicia el servicio, los servidores DNS de Windows 2000 utilizan los valores de configuración del servidor obtenidos de los parámetros establecidos en el archivo de información de inicio, en el Registro de Windows 2000 o en los valores predeterminados que proporciona la integración de Active Directory.

En la mayoría de las situaciones, los valores predeterminados de la instalación son aceptables y no deberían necesitar modificaciones. Sin embargo, cuando sea necesario puede utilizar la consola DNS para ajustar los siguientes parámetros avanzados, que permiten adaptarse a las situaciones y necesidades especiales de distribución.

Pestaña Sugerencias de Raíz

Las sugerencias de raíz se utilizan para preparar los servidores autoritativos para zonas que no sean de raíz, a fin de que puedan aprender y descubrir servidores autoritativos que administran dominios de un nivel superior o de otros subárboles del espacio de nombres del dominio DNS. Estas sugerencias son esenciales para los servidores autoritativos de niveles inferiores del espacio de nombres cuando localicen y busquen servidores en estas condiciones.



Por ejemplo, suponga que un servidor DNS (Servidor A) tiene una zona llamada sub.ejemplo.microsoft.com. En el proceso de respuesta a una consulta de un dominio de nivel superior, como el dominio microsoft.com, el Servidor A necesita ayuda para ubicar un servidor autoritativo (como el Servidor B) de este dominio.

Para que el Servidor A encuentre al Servidor B o cualquier otro servidor autoritativo para el dominio microsoft.com, es necesario que pueda consultar a los servidores raíz del espacio de nombres DNS.

Los servidores raíz pueden remitir el Servidor A a los servidores autoritativos del dominio com. A su vez, los servidores del dominio com pueden ofrecer referencia al Servidor B u otros servidores autoritativos para el dominio microsoft.com.

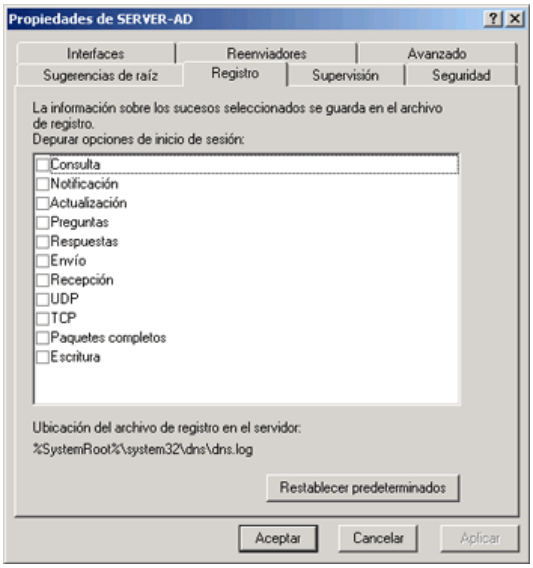
Las sugerencias de raíz utilizadas por el Servidor A deben tener sugerencias útiles para los servidores raíz a fin de que este proceso localice al Servidor B (u otro servidor autoritativo), como se pretende.

Pestaña Registros

Para los servidores DNS de Windows 2000 se pueden utilizar las siguientes opciones de registro de depuración:

Consulta: Registra consultas recibidas por el servicio del Servidor DNS desde los clientes.

Notificar: Registra mensajes de notificación recibidos por el servicio del Servidor DNS desde otros servidores.



Actualización: Registra actualizaciones dinámicas recibidas por el servicio del Servidor DNS desde otros equipos.

Preguntas: Registra el contenido de la sección de preguntas de cada mensaje de consulta DNS procesado por el servicio del Servidor DNS.

Respuestas: Registra el contenido de la sección de respuestas de cada mensaje de consulta DNS procesado por el servicio del Servidor DNS.

Envío: Registra los distintos mensajes de consulta DNS enviados por el servicio del Servidor DNS.

Recepción: Registra los distintos mensajes de consulta DNS recibidos por el servicio del Servidor DNS.

UDP: Registra las distintas solicitudes DNS recibidas por el servicio del Servidor DNS a través de un puerto UDP.

TCP: Registra las distintas solicitudes DNS recibidas por el servicio del Servidor DNS a través de un puerto TCP.

Paquetes completos: Registra los distintos paquetes completos escritos y enviados por el servicio del Servidor DNS.

Escritura: Registra los distintos paquetes escritos completamente por el servicio del Servidor DNS y devueltos a la zona.

De forma predeterminada, todas las opciones de inicio de registro de depuración están deshabilitadas. Cuando se habilitan de forma selectiva, el servicio del Servidor DNS puede realizar un registro adicional a nivel de seguimiento de tipos seleccionados de sucesos o mensajes para solucionar problemas generales y depurar el servidor.

El registro de depuración puede emplear muchos recursos; esto afectará al rendimiento global del servidor y consumirá espacio en disco. Por lo tanto, sólo debe utilizarse temporalmente cuando se necesite información más detallada acerca del rendimiento del servidor.

Dns.log contiene actividad de registro de depuración. Se encuentra en la carpeta windir\System32\Dns.

Ficha Inicio de Autoridad (SOA)

Las zonas se basan en el concepto de autoridad de servidor. Cuando se configura un servidor DNS para cargar una zona, utiliza dos tipos de registros de recursos para determinar las propiedades autorizadas de la zona.

Primero, el registro de recursos de inicio de autoridad (SOA) indica el nombre de origen de la zona y contiene el nombre del servidor que es el origen principal de información acerca de la zona. También indica otras propiedades básicas de la zona.

Ficha Servidores de Nombres

Muestra los servidores de nombres (NS) configurados para el servidor o la zona de la manera siguiente:

Cuando esta lista se muestra en la ficha Sugerencias de raíz, que se encuentra en las propiedades de servidor DNS correspondientes, presenta sugerencias de raíz que contienen los servidores raíz

que el servidor debe utilizar y a los que debe hacer referencia para resolver nombres. En los servidores raíz, este campo debe estar en blanco.

Cuando esta lista se muestra en la ficha Servidores de nombres, que se encuentra en las Propiedades de zona correspondientes, presenta los servidores DNS configurados actualmente como autoridades para la zona. En la mayor parte de los casos, esto incluye todos los demás servidores que están configurados como secundarios de la zona.

Ficha WINS

El Servicio de nombres Internet de Windows (WINS) se puede usar para buscar nombres DNS que no se pueden resolver mediante la consulta del espacio de nombres de dominio DNS. Para ejecutar la búsqueda WINS, se utilizan dos tipos de registros de recursos específicos que se pueden habilitar para cualquier zona cargada mediante el servicio DNS:

El registro de recursos WINS, que se puede habilitar para integrar la búsqueda WINS en las zonas de búsqueda directa

El registro de recursos WINS-R, que se puede habilitar para integrar la búsqueda inversa WINS en las zonas de búsqueda inversa

Los servicios WINS y DNS se utilizan para proporcionar la resolución de nombres para el espacio de nombres NetBIOS y el espacio de nombres de dominio DNS, respectivamente. Aunque DNS y WINS pueden proporcionar un servicio de nombres útil e independiente a los clientes, WINS se necesita, principalmente, para proporcionar compatibilidad con los clientes y programas antiguos que requieren compatibilidad con los nombres NetBIOS.

Sin embargo, el servicio DNS puede funcionar con WINS para proporcionar búsquedas de nombres combinados en los dos espacios de nombres cuando en una información de zona no se encuentra la resolución de un nombre de dominio DNS. Para proporcionar esta interoperabilidad, se ha definido un nuevo registro (el registro WINS) como parte del archivo de base de datos de zonas.

El registro de recursos WINS es específico para Windows 2000 Server y versiones anteriores de Windows NT Server, y se puede conectar sólo al dominio de origen de una zona. La presencia de un registro de recursos WINS puede indicar al servicio DNS que utilice WINS para buscar las consultas directas de nombres de host o nombres que no se encuentran en la base de datos de zonas. Esta funcionalidad es especialmente útil en la resolución de nombres que requieren los clientes que no admiten WINS (por ejemplo, UNIX) para los nombres de los equipos que no se registraron con DNS, como los equipos con Windows 95 o Windows 98.

Usar búsqueda directa WINS: Para impedir que el registro WINS sea replicado a cualquier servidor secundario por motivos de compatibilidad (los servidores DNS no Microsoft no soportan registros WINS-R), hay que seleccionar la casilla de verificación No replicar este registro.

Dirección IP: Introducir la dirección IP de cada servidor WINS que se quiera consultar, pulsando Agregar tras introducir cada una.

1.4 Protocolo DHCP.

Para que un host con TCP/IP se comunique correctamente con otro, ambos deben estar configurados apropiadamente. Requieren una dirección de IP válida y única, una máscara de subred y una dirección de pasarela predeterminada, aunque se puede omitir si el host sólo se va a comunicar en la subred local. Para redes mayores se necesita configurar otros elementos, como la dirección de IP de un servidor de DNS, la dirección de IP de un servidor WINS y los tipos de nodo NetBIOS.

En grandes redes, asegurar que todos los hosts se han configurado correctamente puede ser una tarea de administración y gestión importante, especialmente en redes dinámicas con usuarios móviles con ordenadores portátiles. La configuración manual o la reconfiguración de un gran número de equipos es una tarea que lleva mucho tiempo y un error en la configuración de un host puede hacer que sea imposible que se comunique con el resto de la red.

DHCP es un protocolo cliente-servidor que simplifica la administración de la configuración de los clientes de IP y la asignación de los datos de configuración de IP. Mediante DHCP, el administrador define todos los parámetros de configuración necesarios en un servidor central, quien proporciona a los hosts toda la información de configuración de IP.

DHCP proporciona tres ventajas clave en la planificación, diseño y mantenimiento de una red de IP:

- Administración centralizada de las configuraciones de IP. El administrador de DHCP puede administrar de manera centralizada toda la información de configuración de IP. De esta forma se elimina la necesidad de configurar manualmente los hosts individualmente cuando se implanta por primera vez TCP/IP o cuando se necesitan cambios en la infraestructura de IP.

- Sencillez en la configuración de IP de host. Mediante DHCP se asegura que los clientes de DHCP obtienen parámetros de configuración de IP precisos y en tiempo, sin intervención del usuario. Como la configuración es automática se elimina gran parte de los problemas.

- Flexibilidad. Utilizando DHCP, el administrador aumenta su flexibilidad para el cambio de la información de configuración de IP, lo que permite que el administrador cambie la configuración de IP de manera sencilla cuando se necesitan los cambios.

Todos los Windows 2000 Server (incluyendo Server, Advanced Server y Data Center Server) incluyen el servicio Servidor de DHCP, que se instala como opcional. Todos los clientes de Microsoft Windows instalan automáticamente el servicio cliente de DHCP como parte de TCP/IP, incluidos Windows 2000, Windows NT 4.0, Windows 98 y Windows 95.

Funcionamiento de DHCP.

Los hosts utilizan el protocolo DHCP para obtener una concesión inicial, renovar una existente y detectar servidores de DHCP no autorizados.

Obtención de una concesión inicial.

La adquisición de una concesión inicial ocurre la primera vez que un cliente de DHCP arranca.

1. El cliente de DHCP difunde, en primer lugar, el mensaje DHCPDISCOVER para buscar un servidor de DHCP. Como el host no tiene dirección de IP, se comunica con el servidor de DHCP mediante un mensaje de difusión en el área local.

2. Si hay más de un servidor de DHCP que puede proporcionar al cliente de DHCP una dirección de IP válida, es posible que el cliente reciba una o más respuestas DHCPOFFER. Si ocurre esto, el cliente elige la «mejor» de ellas, que en Windows 2000 será la primera recibida. Para ayudar al cliente a decidir cuál es la mejor oferta, el mensaje DHCPOFFER contiene valores para las opciones que el cliente había solicitado y que se configuran en el servidor de DHCP que la entrega. Cualquier servidor de DHCP que recibe un mensaje DHCPDISCOVER y puede asignar al cliente de DHCP una concesión, enviará un mensaje DHCPOFFER con la dirección de IP ofrecida y valores de opción.

3. Si el cliente puede aceptar esta concesión, envía una DHCPREQUEST al servidor de DHCP, solicitando la dirección de IP ofrecida. Esta solicitud también contendrá todas las opciones de configuración que el cliente de DHCP desea obtener.

4. El mensaje final, DHCPACK, se envía desde el servidor de DHCP hasta el cliente de DHCP para confirmar que el cliente tiene la dirección de IP y los valores de las opciones solicitadas que especificó el administrador de DHCP en el servidor.

Renovación de una concesión

Los clientes de DHCP intentarán renovar la concesión tras cada reinicio o a intervalos regulares después del inicio del cliente de DHCP.

La renovación de una concesión supone sólo dos mensajes de DHCP, DHCPREQUEST y DHCPACK. Si el cliente de DHCP renueva una concesión mientras se reinicia, se usan paquetes de IP de difusión para enviar estos mensajes. Si la renovación de la concesión se realiza mientras se está ejecutando el cliente de DHCP, el cliente y el servidor de DHCP se comunican mediante dirección IP unicast.

Cuando un cliente obtiene una concesión, DHCP proporciona los valores para las opciones de configuración solicitadas por el cliente. Reduciendo el tiempo de concesión, el administrador fuerza a los clientes a solicitar periódicamente una renovación de la concesión y obtener detalles actualizados de configuración. Puede ser útil cuando el administrador desea cambiar la configuración de IP de una subred.

Un cliente de DHCP intenta en primer lugar volver a conseguir su concesión a la mitad del tiempo de concesión, conocido como T1. Si falla el cliente intentará de nuevo una nueva renovación de la concesión al 87,5 por 100 del tiempo de concesión, conocido como T2. Si no se consigue obtener la concesión antes de que expire (por ejemplo, si el servidor de DHCP no está accesible), en cuanto expira la concesión el cliente libera la dirección de IP e intenta conseguir una nueva concesión.

Cambios en subredes y servidores.

Si el cliente de DHCP solicita una conexión mediante un mensaje DHCPREQUEST y el servidor de DHCP no puede cumplir (por ejemplo, cuando se traslada un portátil a una subred distinta), el servidor de DHCP envía un mensaje DHCPNAK al cliente. El cliente conseguirá una nueva concesión usando el proceso de adquisición de concesión inicial.

Cuando arranca un cliente de DHCP difunde un mensaje DHCPREQUEST para renovar su concesión. Ello le asegura que la solicitud de renovación de DHCP se envía al servidor de DHCP que proporciona direcciones de DHCP para la subred en la que se encuentra ahora el cliente, que puede ser distinta de la del servidor de DHCP que proporcionó la concesión inicial. Cuando el servidor de DHCP recibe la difusión, compara la dirección del cliente de DHCP solicitante con el ámbito configurado en el servidor. Si es imposible satisfacer la solicitud del cliente, el servidor de DHCP envía un DHCPACK y el cliente consigue una nueva concesión.

Si el cliente de DHCP no es capaz de localizar ningún servidor de DHCP cuando se reinicia, para renovar su concesión envía una difusión de ARP (Address Resolución Protocol, Protocolo de Resolución de Direcciones) para la pasarela predeterminada que se obtuvo anteriormente, si la hubo. Si la dirección de IP de la pasarela predeterminada se resuelve correctamente, el cliente de DHCP supone que se encuentra situado en la misma red donde obtuvo su concesión actual que continúa usando.

Si la difusión de ARP del cliente enviada para la pasarela predeterminada no recibe respuesta, el cliente supone que el cliente se ha trasladado a una red que no dispone actualmente de servicios de

DHCP, como la red de casa, y se autoconfigura él mismo mediante APIPA (Automatic Prívate IP Addressing, Dirección privada IP automática (169.254.x.x)). Una vez autoconfigurado a sí mismo, el cliente de DHCP intentará, cada 5 minutos, localizar un servidor de DHCP.

Detección de servidores de DHCP no autorizados

Como parte de la inicialización del servicio de DHCP, todos los servidores de DHCP realizan una detección de servicios rogue. Si el servidor no está autorizado en el Active Directory, se apaga.

La detección de servidor rogue comienza con la inicialización del servidor de DHCP enviando una solicitud DHCPINFORM para determinar si existen otros servidores de DHCP inicializados en cualquier red conectada. Si es así, estos servidores responden con un mensaje DHCPACK que contiene el nombre del dominio en el que tienen autorización.

Si se encuentran otro servidor de DHCP, el servicio de DHCP de Windows 2000 que está arrancando se conecta con el Active Directory y envía una serie de llamadas LDAP para descubrir si está autorizado o no. Si el servidor no está autorizado, el servicio termina. Esta detección se lleva a cabo una vez cada hora por el servidor de DHCP para detectar nuevos servidores no autorizados.

Si está activado el registro de sucesos de DHCP, se escribe un mensaje en el registro de sucesos de DHCP.

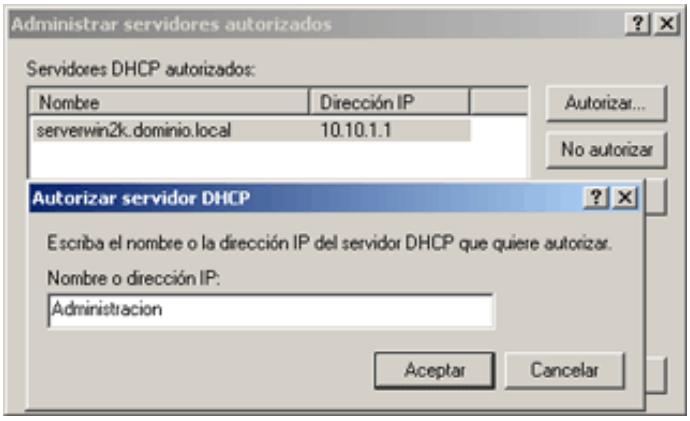
Configurando un servidor DHCP.

El servidor DHCP reduce enormemente la tarea administrativa de configurar estaciones de trabajo con una dirección IP y la configuración TCP/IP apropiada para la red. Antes de instalar el servidor DHCP hay que determinar el esquema de direcciones IP. También se deben completar estos pasos adicionales antes de instalar DHCP:

- Determinar el intervalo de direcciones IP libres y únicas que manejará el servidor DHCP además de cualquier dirección IP que sea necesario excluir para soportar hosts con direcciones IP estáticas.
- Hacer una lista de los servidores para los que se desea reservar una IP (como servidores DNS y WINS).
- Si el servidor DHCP utilizará direcciones IP registradas en Internet, hay que registrar las direcciones IP con el ISP
- Actualizar todos los controladores de dominio Windows NT 4 a Windows 2000.
- Determinar los requisitos de hardware y de almacenamiento del servidor DHCP
- Configurar manualmente las direcciones estáticas en el equipo donde se instalará el servicio DHCP

Para instalar el servidor DHCP, hay que seguir estos pasos:

Si se desea instalar el servicio DHCP en un servidor que no sea controlador de dominio, será necesario comunicárselo a Active Directory. Después de la instalación hay que abrir DHCP desde el menú Herramientas administrativas. Hay que resaltar DHCP en el árbol de la consola y escoger después Examinar servidores autorizados en el menú Acción. Hay que pulsar Agregar y escribir después el nombre o la dirección IP del servidor DHCP a autorizar.



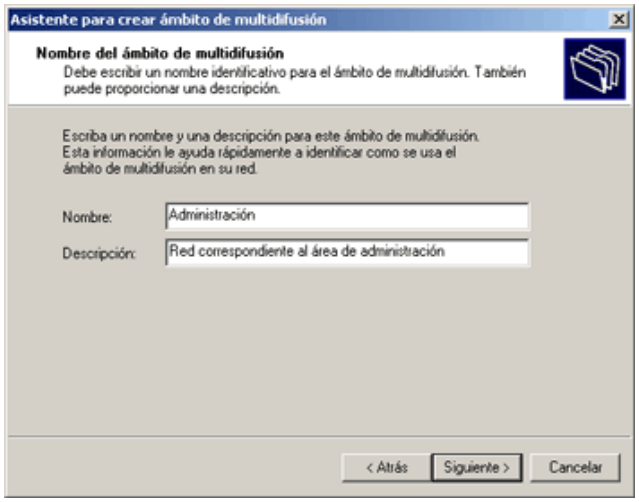
Si se piensa utilizar múltiples servidores DHCP en una subred para realizar equilibrio de carga y tener redundancia, hay que configurar un superámbito en cada servidor DHCP que contenga todos los ámbitos válidos de la subred como ámbitos miembro. Hay que configurar entonces el ámbito miembro en cada servidor para que tenga excluidas las direcciones de los otros servidores de forma que no aparezcan direcciones en ninguna de las colas de direcciones de los servidores. Una buena división consiste en darle el 80 por 100 de las direcciones al servidor DHCP principal y el 20 por 100 al servidor secundario.

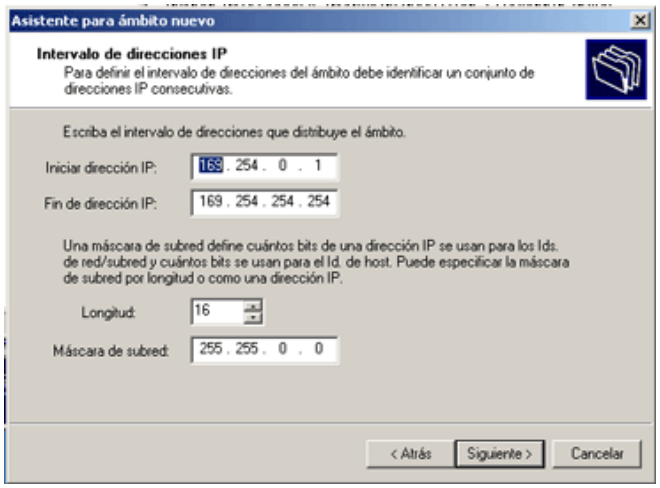
Creación de un nuevo ámbito.

Ahora ya se puede ejecutar el Administrador DHCP y crear un nuevo ámbito de direcciones IP para que las gestione el servidor DHCP. Pero antes de hacer esto, hay que asegurarse de que se conoce el intervalo de direcciones IP aprobado, qué direcciones IP son necesarias excluir para los sistemas con direcciones IP estáticas y qué direcciones son necesarias reservar para servidores DNS o WINS. Para abrir el Administrador DHCP y crear el nuevo ámbito, hay que seguir los siguientes pasos:

1. Escoger DHCP del menú Herramientas administrativas.
2. Seleccionar el servidor DHCP en el árbol de la consola. Seleccionar el menú Acción y escoger Ámbito nuevo para ejecutar el Asistente para ámbito nuevo.
3. Pulsar Siguiente e introducir el nombre y la descripción del ámbito que servirán para distinguir este ámbito de otros. Pulsar Siguiente.

4. Introducir la dirección IP por la que se desea que comience el ámbito en el campo Iniciar, e introducir la dirección IP por la que se desea qué finalice el ámbito en el campo Fin.
5. Introducir la máscara de subred de la red en el cuadro Máscara de subred, o utilizar el cuadro Longitud para ajustar la longitud de la máscara de subred. Después, pulsar Siguiente.





6. Para excluir un intervalo de direcciones del ámbito, en el cuadro Iniciar dirección IP, hay que introducir la dirección IP de comienzo para el intervalo de exclusión; en el cuadro Fin de dirección IP hay que introducir la dirección IP final del intervalo de exclusión. Después hay que pulsar Agregar. Hay que añadir las exclusiones que sean necesarias y pulsar Siguiente cuando se haya terminado.

7. Especificar la duración de la concesión a los clientes y pulsar Siguiente. Conviene utilizar concesiones más largas en redes sin servidores DHCP redundantes para permitir más tiempo de recuperación de un servidor DHCP sin conexión antes de que los clientes pierdan sus concesiones, o para minimizar el tráfico de red a expensas de una renovación de direcciones menos frecuente. También se pueden utilizar concesiones más largas si las direcciones del ámbito son abundantes (al menos un 20 por ciento disponible), la red es estable y los equipos rara vez se mueven. Por el contrario, los ámbitos que soportan clientes que acceden telefónicamente pueden tener concesiones más cortas y, por lo tanto, funcionar bien con menos direcciones.

8. Para configurar las opciones de DHCP, hay que pulsar Configurar estas opciones ahora; en otro caso, hay que pulsar Configuraré estas opciones más tarde. Si se selecciona Configuraré estas opciones más tarde hay que pulsar Finalizar para completar la instalación del ámbito.

9. Si se decide especificar las opciones de DHCP, hay que introducir las puertas de enlace (enrutadores) que se desea que utilicen los clientes en el cuadro Dirección IP, pulsando el botón Agregar después de introducir cada uno. Cuando se haya terminado de introducir puertas de enlace hay que pulsar Siguiente.

10. Introducir el nombre de dominio del dominio en el cuadro Dominio primario, y añadir las direcciones IP de los servidores DNS en el cuadro Dirección IP, pulsando Agregar tras introducir cada una. Hay que pulsar Siguiente cuando se haya terminado.

11. En el cuadro Dirección IP de Servidores WINS, hay que introducir las direcciones de todos los servidores WINS que se hayan configurado en la red para asignar direcciones IP a los nombres NetBIOS de los clientes de nivel inferior. Pulsar Siguiente.

12. Para activar el ámbito inmediatamente, hay que pulsar Activar este ámbito ahora; en caso contrario, hay que pulsar Activaré este ámbito más tarde. Hay que pulsar Siguiente y pulsar después Finalizar para completar la configuración del ámbito.

Autorización del servidor DHCP y activación de los ámbitos.

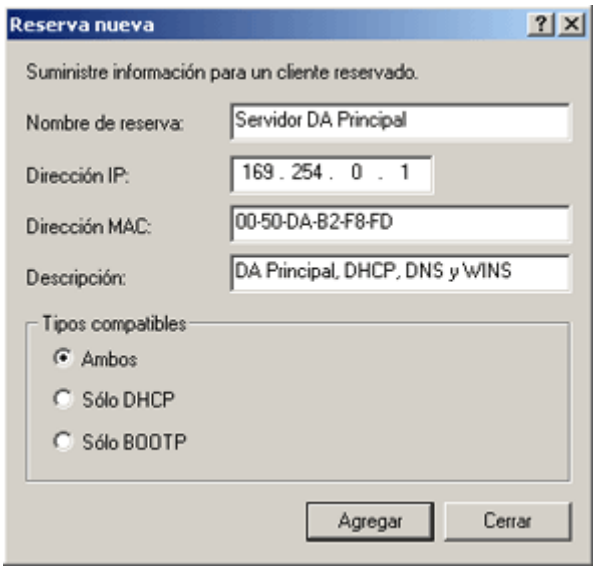
Después de configurar el servidor DHCP y crear los ámbitos, es necesario activar los ámbitos antes de que cualquier cliente pueda utilizar el servidor para obtener direcciones IP Antes de que se puedan activar los ámbitos, el servidor tiene que ser autorizado a realizar concesiones, a menos que se haya instalado DHCP en un controlador de dominio, en cuyo caso el servidor DHCP será autorizado automáticamente la primera vez que se añada el servidor a la consola Administrador DHCP. La autorización de un servidor DHCP es una opción importante que proporciona Windows 2000 para reducir la capacidad de los hackers de configurar servidores DHCP corrompidos: servidores no autorizados configurados para proporcionar direcciones IP falsas a los clientes. Para autorizar el servidor DHCP después de instalar el servicio, hay que seguir los siguientes pasos:

- En el Administrador DHCP hay que seleccionar DHCP en la raíz del árbol de la consola.
- Escoger Administrar servidores autorizados en el menú Acción.
- Seleccionar Autorizar en el cuadro de diálogo Administrar servidores autorizados.
- Introducir el nombre o la dirección IP del servidor en el cuadro de texto proporcionado y pulsar Aceptar.
- Verificar que la información es correcta en el cuadro de diálogo que se muestra y entonces pulsar Sí. Hay que pulsar Aceptar para cerrar el cuadro de diálogo Administrar servidores autorizados.
- Para activar un ámbito hay que seleccionarlo en el árbol de la consola y escoger después Activar en el menú Acción.

No se debe activar un ámbito hasta que se hayan terminado de seleccionar todas las opciones deseadas. Una vez activado un ámbito, el comando Activar del menú cambia a Desactivar. No se debe desactivar un ámbito a no ser que vaya a ser retirado permanentemente de la red.

Reservando direcciones.

Las reservas son elementos prácticos que se pueden utilizar en lugar de las direcciones IP estáticas (que requieren exclusiones) para todos los servidores (excepto servidores DHCP) que necesiten mantener una dirección IP específica, como servidores DNS y WINS. Al utilizar reservas en lugar de direcciones estáticas se garantiza que un servidor tendrá una dirección IP consistente proporcionando al mismo tiempo la capacidad de recuperar la dirección IP en el futuro si el servidor es retirado de la circulación o movido. Se debería crear la reserva en todos los servidores DHCP que podrían servir potencialmente al cliente reservado.



Para añadir una reserva de dirección a un ámbito:

1. Pulsar con el botón derecho del ratón en la carpeta Reservas bajo el ámbito deseado y escoger Reserva nueva en el menú contextual.
2. Introducir el nombre de la reserva en el cuadro Nombre de reserva.
3. Introducir la dirección IP para el cliente en el cuadro Dirección IP e introducir la dirección MAC del cliente en el cuadro Dirección MAC.
4. Introducir una descripción para la reserva en el cuadro Descripción.
5. Determinar a qué tipo de cliente se desea permitir que utilice la reserva seleccionando Sólo DHCP, Sólo BOOTP o Ambos. A continuación, pulsar Agregar.

Para obtenerla dirección MAC hay que ir al equipo cliente y escribir ipcongif /all en el símbolo del sistema. La dirección MAC se muestra como dirección física.

Activación de las actualizaciones dinámicas de un servidor DNS

Los servidores DHCP y DNS de Windows 2000 soportan ahora actualizaciones dinámicas con un servidor DNS, una característica que cualquier administrador que haya tenido que gestionar un servidor DNS de Windows NT 4 estático (o similar) apreciará. Los clientes Windows 2000 pueden actualizar dinámicamente sus registros de búsquedas directas ellos mismos con el servidor DNS después de obtener una nueva dirección IP de un servidor DHCP

Además, el servidor DHCP de Windows 2000 soporta también actualización dinámica de registros DNS para clientes anteriores a Windows 2000 que no lo puedan hacer ellos mismos. Esta característica sólo funciona actualmente con los servidores DHCP y DNS de Windows 2000.

Para permitir que un servidor DHCP actualice dinámicamente los registros DNS de sus clientes, hay que seguir los siguientes pasos:

1. Seleccionar el ámbito o el servidor DHCP en el cual se desea permitir actualizaciones dinámicas.
2. En el menú Acción, escoger Propiedades y pulsar después la pestaña DNS.
3. Seleccionar la casilla de verificación Actualizar automáticamente la información del cliente DHCP en DNS.
4. Para actualizar los registros DNS de un cliente basándose en el tipo de petición DHCP que hace el cliente y sólo cuando sea solicitado, hay que seleccionar la opción Actualizar DNS sólo a la petición del cliente DHCP
5. Para actualizar siempre los registros de búsqueda directa e inversa de un cliente, hay que seleccionar la opción Actualizar siempre DNS.
6. Seleccionar la casilla de verificación Descartar las búsquedas directas al caducar la concesión para permitir que el servidor DHCP borre el registro de recurso Host de un cliente cuando su concesión DHCP caduque y no sea renovada.
7. Seleccionar la casilla de verificación Habilitar actualizaciones para clientes DNS que no sean compatibles con actualizaciones dinámicas para permitir que el servidor DHCP actualice los registros de búsqueda directa e inversa de los clientes que no pueden actualizar sus propios registros de búsqueda directa. Si no se selecciona esta casilla de verificación, el servidor DHCP no actualizará dinámicamente los registros DNS de los clientes que no sean Windows 2000.

Si se tienen servidores DNS estáticos como los de Windows NT 4, estos servidores no podrán interactuar dinámicamente cuando las configuraciones de los clientes DHCP cambien. Esta incompatibilidad puede provocar búsquedas fallidas en los clientes DHCP Para evitar este problema, hay que actualizar los servidores DNS estáticos con un DNS que soporte DNS dinámico (Windows 2000). Es decir, vuelvo a desaconsejar fervientemente que se monten redes mixtas con servidores NT y 2000 trabajando en el mismo entorno.

Uso de Ipconfig para liberar, renovar o verificar una concesión

En un equipo que ejecuta Windows con DHCP activado se puede ejecutar una utilidad de línea de comandos para liberar, renovar o verificar la concesión de dirección del cliente. En el símbolo del sistema (o en la ventana Ejecutar) hay que utilizar alguno de los siguientes comandos:

- Para liberar una concesión de un cliente, hay que escribir Ipconfig/release.
- Para renovar una concesión, hay que escribir Ipconfig/renew.
- Para verificar la concesión del cliente, hay que escribir Ipconfig/all.

Con clientes Windows 95/98 hay que utilizar Winipcfg con los mismos parámetros. El programa Ipconfig es útil a la hora de solucionar problemas porque muestra cada detalle de la configuración TCP/IP actual.