

Instalación, configuración y administración de servidores DNS

Tabla de Contenidos

1. Instalación, configuración y administración de servidores DNS.....	2
1.1 Conceptos Generales de DNS.....	2
1.2 Servidor DNS en Windows 2000.....	4
1.2.1 Instalación del Servicio de DNS.....	4
1.2.2 Configuración del Servicio de DNS.....	7
1.2.3 Configuración de DNS dinámico.....	12
1.2.4 Configurando Clientes.....	12
1.2.5 Monitorización del Servicio.....	13
1.3 Servidor DNS en Linux.....	15
1.3.1 Registros de Recursos.....	15
1.3.2 Resolvers.....	16
1.3.3 Archivo /etc/host.conf.....	17
1.3.4 El archivo /etc/resolv.conf.....	17
1.3.5 Utilización de named.....	18

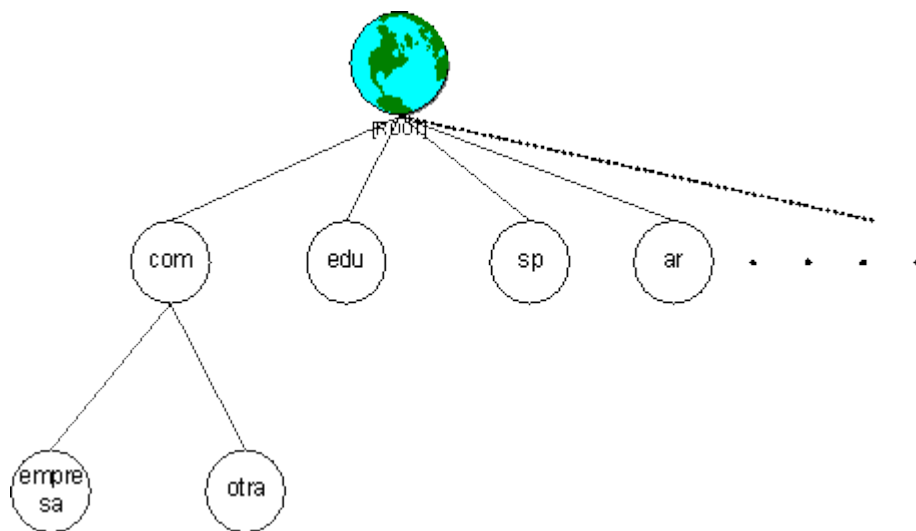


1. Instalación, configuración y administración de servidores DNS.

1.1 Conceptos Generales De DNS

Primeramente se presenta un repaso de algunos conceptos del sistema de nombres de dominio (DNS Domain Name System). DNS establece una jerarquía de nombres para redes TCP/IP. Permite asociar una dirección IP con un nombre. Los nombres de dominio son más fáciles de recordar y más estables que las direcciones IP. Un conjunto de máquinas actúa como servidoras de nombres, permitiendo la traducción desde nombre de dominio a dirección IP y viceversa.

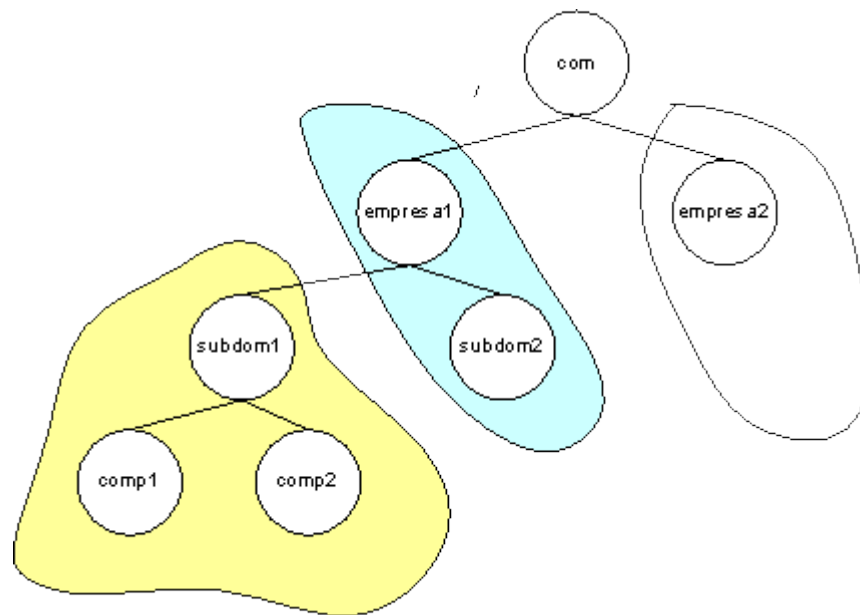
En la siguiente figura vemos un esquema de la jerarquía:



Originalmente los nombres de primer nivel eran: COM, EDU, GOV, MIL, NET, ORGA, ARPA, INT y de país (ES de España, FR de Francia, UK de Reino Unido...). Actualmente se agregaron nuevos nombres como TV, INFO, NAME, etc. Cada nodo en el espacio jerárquico, representa una partición de la base de datos de DNS. Un nombre completamente cualificado (*FQDN fully qualified domain name*) describe a una computadora (host) en una jerarquía de dominios. Por ejemplo *c1.miempresa.com* representa la computadora c1 en el dominio miempresa.com. DNS utiliza FQDN para

resolver nombres a direcciones IP.

El espacio de nombres de dominio se particiona en *zonas* que se utilizan para distribuir las tareas administrativas a diferentes grupos. Cada zona engloba un espacio de nombres de dominio contiguo. Las zonas no pueden solaparse. Existe un servidor de nombres primario por cada zona y posiblemente uno o más secundarios. En el siguiente diagrama se ve una partición válida de zonas:



El servidor primario contiene la base de datos primaria para la zona. Todos los cambios sobre la estructura y nombres de una zona se realizan sobre el servidor primario. Los servidores secundarios mantienen una copia de la base de datos llamada base de datos secundaria. Mediante un procedimiento llamado transferencia de zona, los servidores secundarios actualizan periódicamente su base de datos mediante consultas al servidor primario.

Los servidores DNS permiten dos tipos de consultas: directa y reversa (forward y reverse). La primera resuelve un nombre en una dirección IP y la de reversa resuelve una dirección IP en un nombre.



1.2 Servidor DNS En Windows 2000

1.2.1 Instalación Del Servicio De DNS

La instalación del servicio de DNS puede realizarse tanto al instalar el servidor como posteriormente. Básicamente, la instalación del servicio realiza tres cosas: instala el administrador y agrega un vínculo en Herramientas Administrativas del menú de Inicio; crea una carpeta que contiene los archivos de la base de datos DNS en:

- %systemroot%\System32\DNS

Y, por último, agrega un clave en el registro de Windows 2000 para el servicio:

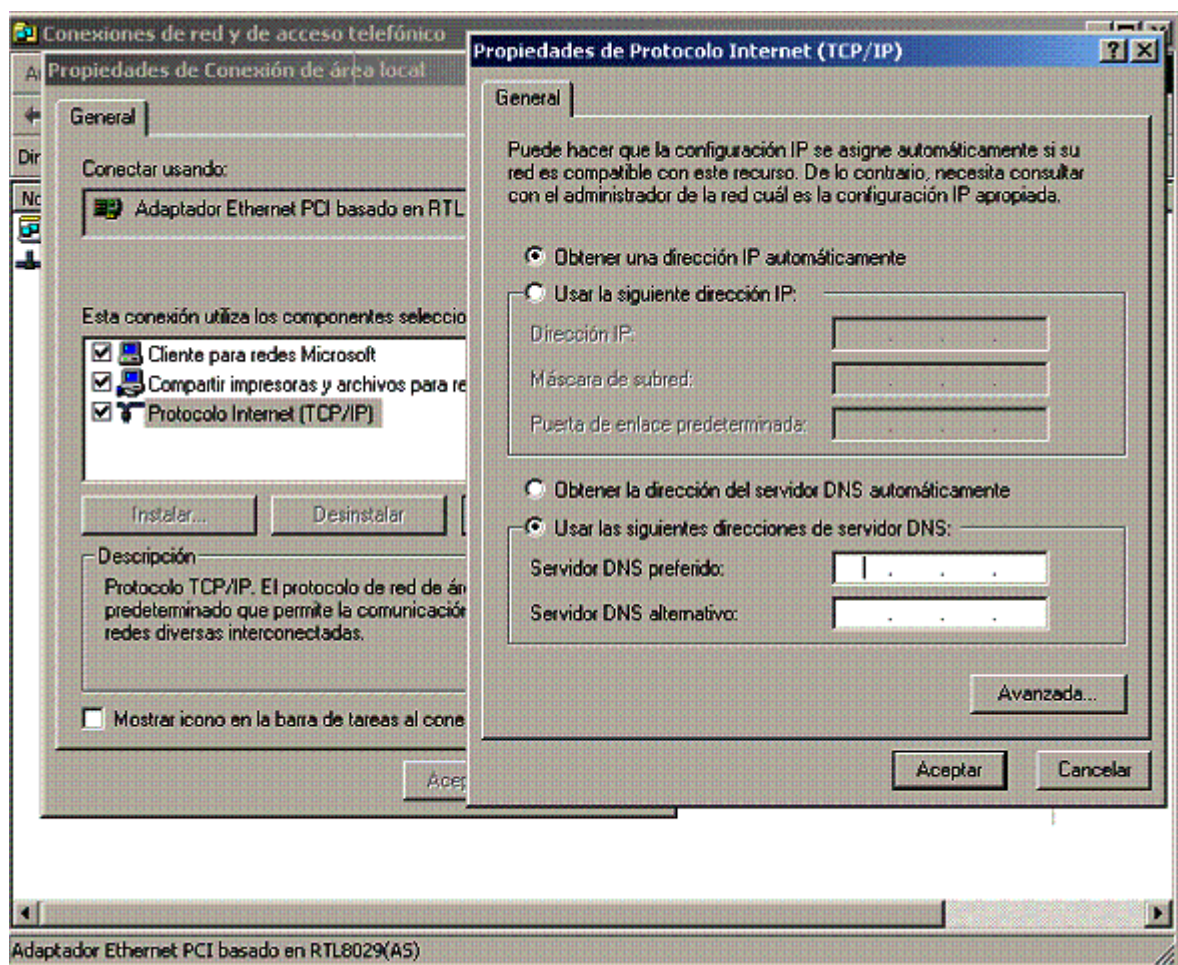
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DNS

Para instalar el servicio de DNS es necesario que el servidor tenga una dirección IP fija asignada y que la configuración de TCP/IP tome al servidor como servidor de nombres. En la figura se ve el lugar donde se asigna manualmente la dirección IP del servidor de nombres. Si se selecciona la opción de obtener la dirección del servidor DNS, automáticamente debe asegurarse de configurar el servidor DHCP para que asigne correctamente.

Los pasos seguidos para la configuración son:

1. Acceder como Administrador
2. Click-derecho en *Mis sitios de Red*
3. Click en *Propiedades*. Aparece la ventana de *Conexiones de Red y de acceso telefónico*
4. Click-derecho en *Conexión de área local* y entonces click *Propiedades*. Aparece la ventana de propiedades de *Conexión de área local* donde se puede ver el adaptador de red y los protocolos utilizados en la conexión.
5. Seleccionar *Protocolo de Internet (TCP/IP)* y Click en *Propiedades* Aparece el diálogo de Propiedades de Protocolo de Internet (TCP/IP).
6. Si se encuentra en el servidor, *debe* acceder la dirección IP y la máscara de subred correspondiente. En caso contrario, puede solamente indicar la dirección del servidor de nombres. Si se encuentra en un cliente y la red utiliza asignación es automática por DHCP entonces puede dejar seleccionada la opción: *obtener la dirección del servidor DNS automáticamente*.





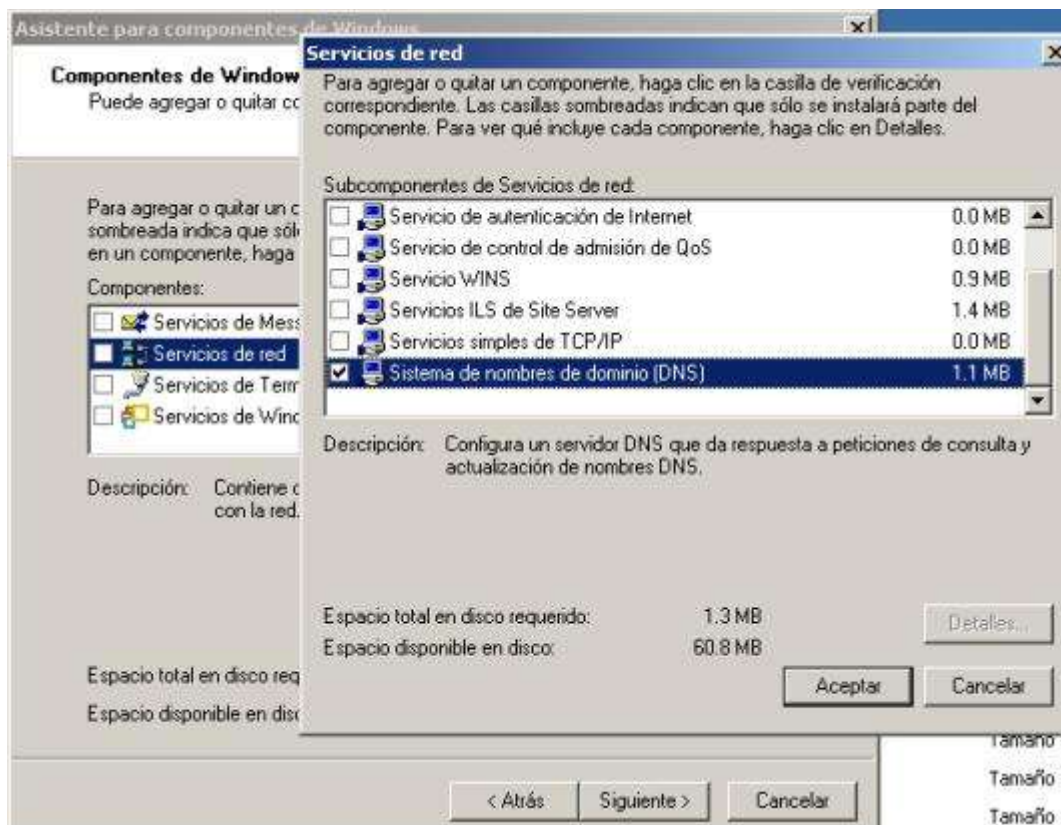
Si no se ha instalado el servicio DNS durante la instalación del Windows 2000, se deben seguir los siguientes pasos para la instalación del servicio de servidor de nombres:

1. Acceder como Administrador
2. Abrir el Panel de Control y Doble-click en *Agregar o quitar Programas*. Aparece la ventana de *Agregar o quitar Programas*.
3. Click en *Agregar o quitar componentes de Windows*. Aparece el asistente de Componentes de Windows.
4. Click en *Servicios de Red* (no seleccionar el check-box a la izquierda del componente)
5. Click *Detalles*.



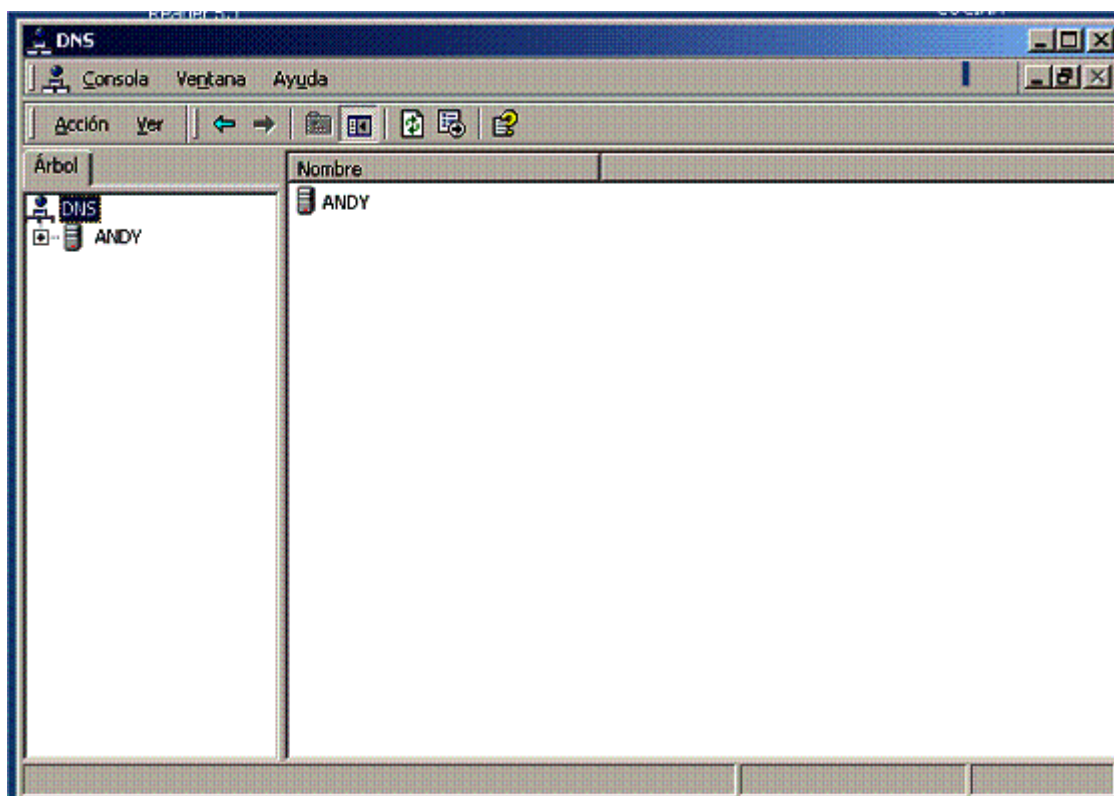
6. En la lista de subcomponentes de servicios de red seleccionar el *check-box* a la izquierda de *Sistema de Nombres de Dominio*
7. Click *OK*. Se retorna a la ventana de *Componentes de Windows*.
8. Click *Siguiente*
9. Si aparece el dialogo de Insertar CD-ROM, hacerlo y luego de un tiempo en el cual se copian los componentes al sistema se selecciona el botón de *Finalizar*.
10. Cerrar las ventanas de Componentes de Windows y Agregar o quitar Programas

En la siguiente figura se ve la ventana para la instalación del servicio DNS.



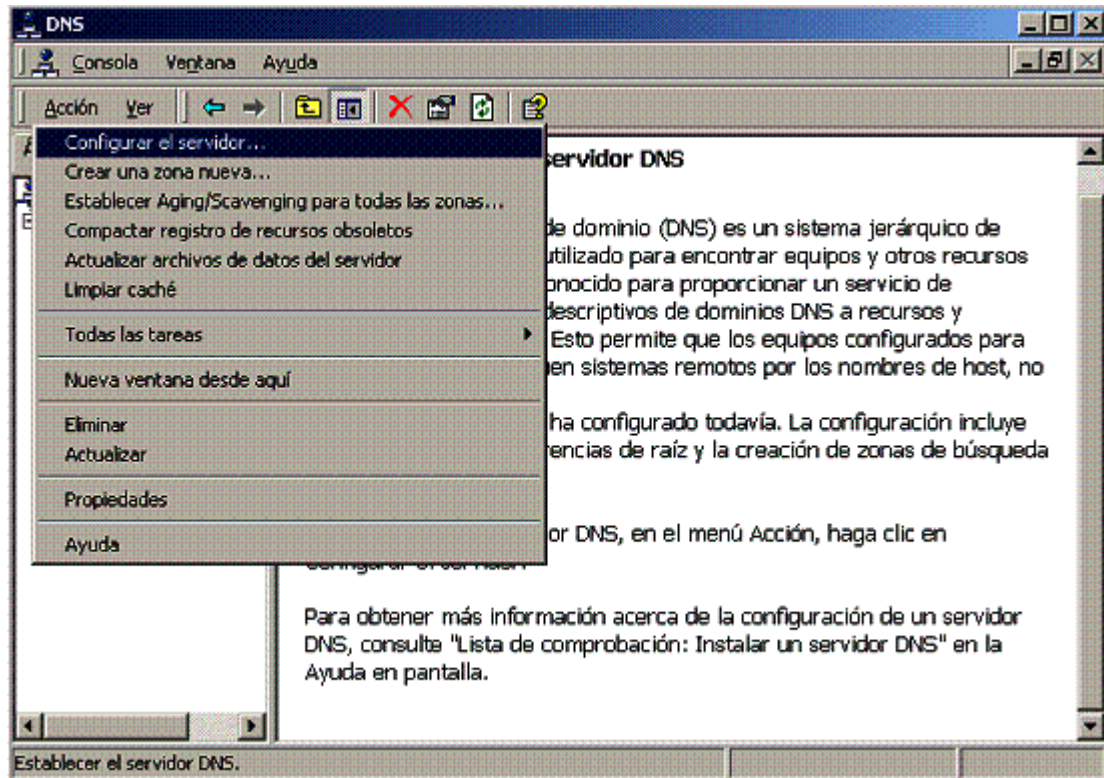
1.2.2 Configuración Del Servicio De DNS

Una vez instalado el servicio, es posible configurarlo mediante la herramienta de DNS. Para abrir la herramienta de administración hay que ir a Inicio/Herramientas Administrativas/ DNS, entonces se abre la ventana que muestra la siguiente figura:

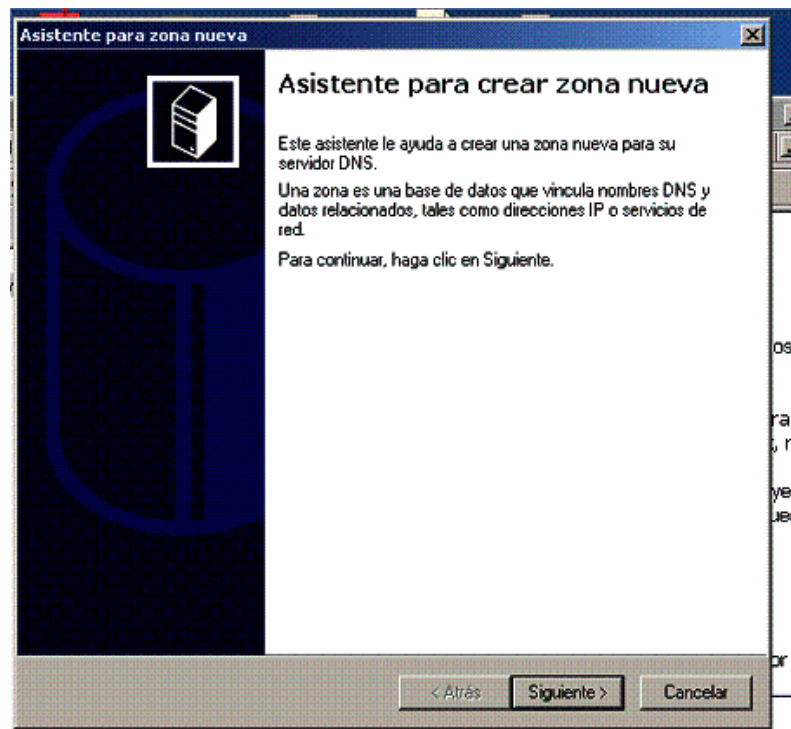


En la figura se ve un solo servidor llamado ANDY. Para que el servidor de nombres funcione, es necesario configurar al menos una zona de búsqueda directa. Desde el menú de Acción, elija *Configurar el servidor* como se ve en la figura.



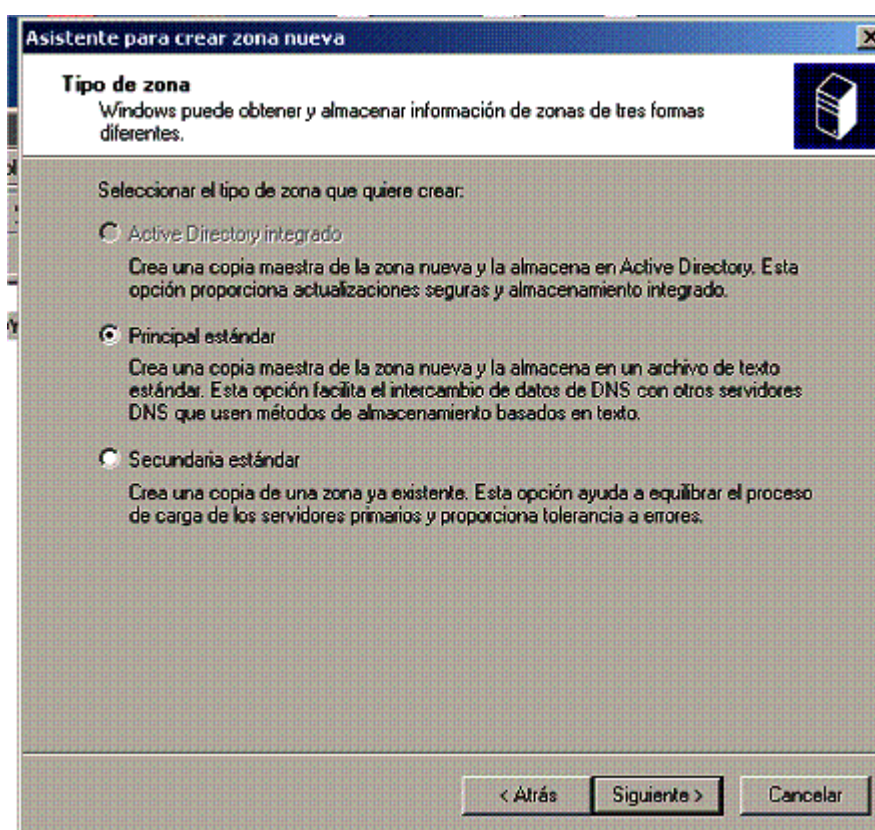


Luego se muestra el asistente para la configuración



Haciendo click en *Siguiente*, se presenta la pantalla para seleccionar el tipo de zona que se va a crear. Hay tres tipos de Zonas:

- **Active Directory Integrado:** Almacena la copia de la base maestra en *Active Directory*. Si *Active Directory* no se encuentra instalado, la opción aparece desactivada.
- **Primaria Estándar:** Tiene la copia maestra de la nueva zona y la guarda en un archivo de texto. Facilita el intercambio de información con otros servidores DNS basados en texto.
- **Secundaria Estándar:** Es una réplica de una zona existente. Este tipo de zona es de lectura solamente y la base de datos se almacena en archivos de texto. Al crear este tipo de zonas es necesario especificar el servidor DNS primario o maestro desde el cual se transferirá la información. Las zonas secundarias proveen redundancia y reducen la carga sobre el servidor de nombres primario.



Se selecciona Principal Estándar para el servidor primario se hace *click* en *Siguiente*. Luego hay que establecer el nombre del dominio, por ejemplo midominio.com y en la próxima pantalla el nombre del archivo donde se almacenará la base de datos. Por lo general el nombre sugerido por defecto es suficiente. Las próximas figuras muestran las pantallas correspondientes.

Asistente para crear zona nueva

Nombre de zona
¿Qué nombre desea dar a la zona nueva?

Escriba el nombre de la zona (por ejemplo, "ejemplo.microsoft.com."):

Nombre:

< Atrás Siguiente > Cancelar

Asistente para zona nueva

Archivo de zona
Puede crear un archivo de zona nuevo o usar un archivo copiado de otro equipo.

¿Desea crear un archivo nuevo de zona o usar el archivo existente que copió de otro equipo?

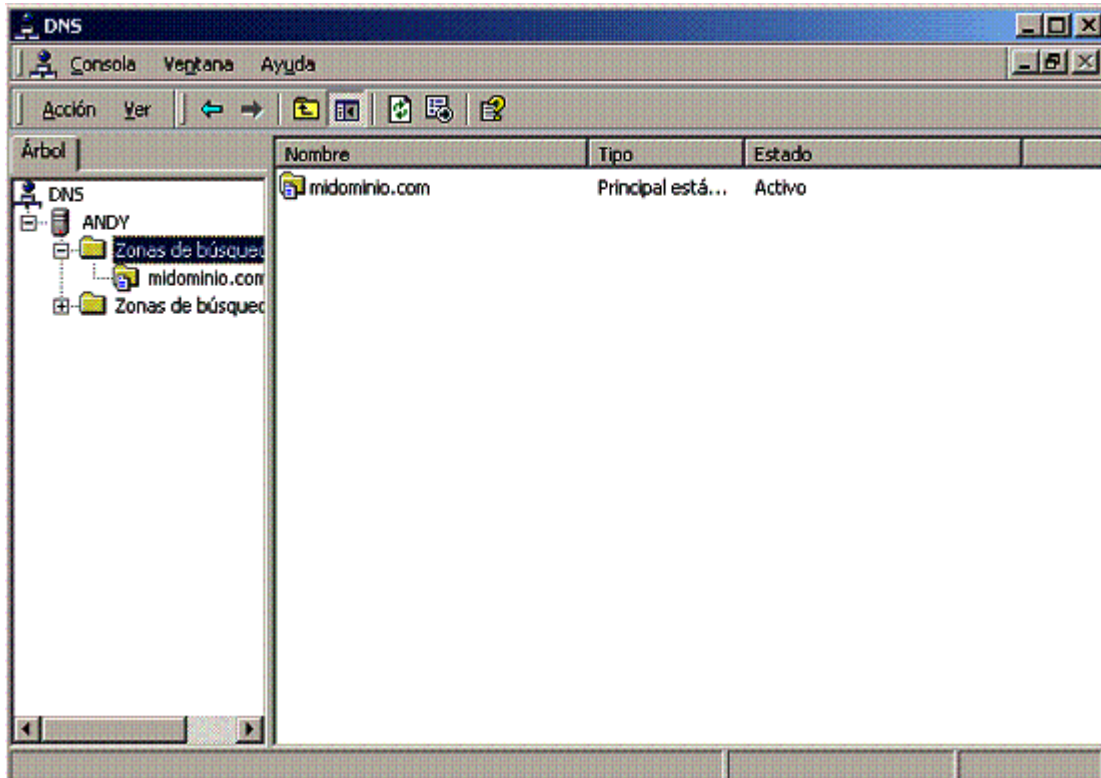
☒ Cree un archivo nuevo con este nombre de archivo:

☐ Usar este archivo:

Para usar un archivo existente, primero debe copiar el archivo en la carpeta %SystemRoot%\system32\dns en el servidor que ejecuta el servicio DNS.

< Atrás Siguiente > Cancelar

Una vez creada la zona, ésta aparece en el árbol de la herramienta administrativa de DNS como se ve en la siguiente figura.



Ahora se está en condiciones de agregar *registros de recursos*. Los *registros de recursos* son entradas en la base de datos de la zona. Para agregar un *registro de recurso*, es necesario realizar *click-derecho* en la zona correspondiente, luego *Nuevo* y seleccionar el tipo de registro que se quiere agregar. Automáticamente ya se generan dos registros agregados: SOA (Start of Authority) y NS (Name Server). Tipos de registros son: **A** que lista la relación nombre-IP para una zona de búsqueda directa, **MX** que identifica el *mail exchange* para un dominio, **CNAME** que permite la creación alias, es decir que más de un nombre apunte a la misma dirección IP, etc.



1.2.3 Configuración De DNS Dinámico

Para evitar el trabajo de actualizar manualmente la base de datos maestra cada vez que se produce un cambio en la red del servicio de DNS, se incluye una capacidad llamada DNS dinámica (DDNS Dynamic DNS). Con esta capacidad, otros servidores de nombres y clientes pueden realizar actualizaciones sobre la base de datos de la zona. Es posible configurar una lista de servidores autorizados a realizar actualizaciones dinámicas. DDNS y DHCP interactúan para mantener actualizados los registros con los nombres-IP de las computadoras que usan el servicio de asignación automática de direcciones IP. El servicio de DHCP se encarga de limpiar los registros cuando expira el alquiler de la dirección.

Para configurar DDNS se deben seguir los siguientes pasos:

1. En la herramienta de DNS realizar un click-derecho sobre la zona que se quiere configurar y click en *Propiedades*.
2. En la pestaña General bajo Actualizaciones dinámicas, se debe seleccionar alguna de las opciones que son:
 - a. Ninguna: No permite actualizaciones dinámicas
 - b. Permitir Actualizaciones: Permite actualizaciones dinámicas para la zona.
 - c. Permitir Actualizaciones Seguras: Sólo para Active Directory y solamente permite actualizaciones que usan un protocolo llamado DNS seguro.

1.2.4 Configurando Clientes

Si la obtención de direcciones IP se realiza mediante un servidor DHCP debidamente configurado, entonces basta con dejar en la pantalla de *Propiedades del protocolo de Internet (TCP/IP)* seleccionada la opción: *obtener la dirección del servidor DNS automáticamente*.

En caso de querer realizar una configuración manual, se deberían seguir los siguientes pasos (una vez verificado que el cliente tiene instalado TCP/IP):

1. Click-derecho en *Mis sitios de Red*

2. Click en *Propiedades*. Aparece la ventana de *Conexiones de Red y de acceso telefónico*
3. Click-derecho en *Conexión de área local* y entonces click en *Propiedades*. Aparece la ventana de propiedades de *Conexión de área local* donde se puede ver el adaptador de red y los protocolos utilizados en la conexión.
4. Seleccionar *Protocolo de Internet (TCP/IP)* y Click en *Propiedades*. Aparece el diálogo de *Propiedades de Protocolo de Internet (TCP/IP)*.
5. Seleccionar *Usar las Siguietes direcciones de Servidor DNS*. Escribir la dirección IP del servidor de nombres y de un servidor alternativo, si se desea. Es importante que diversos clientes cuenten con distintos servidores apuntando algunos al primario y otros a alguno de los secundarios, si los hubiera. De esta manera, se reduce la carga en el servidor primario.
6. Seleccionar *Avanzada* y luego la pestaña *DNS*.
7. Allí se pueden agregar más servidores DNS si se cree conveniente y cambiar el orden de utilización de los mismos con las flechas. El cliente siempre comienza dirigiendo la búsqueda por el servidor superior de la lista. Si éste no responde, entonces envía la consulta al siguiente y así sucesivamente.
8. En *Sufijo DNS para esta conexión* escribir el nombre de dominio del DNS.
9. En *agregar DNS Sufijos (en Orden)* agregar los nombres de los dominios a buscar, en orden. Cuando se busca un nombre en la base de datos, el servidor DNS primero busca por el nombre solamente y si no lo encuentra entonces combina el nombre con cada sufijo especificado.
10. Click *Aceptar*.

1.2.5 Monitorización Del Servicio

La monitorización del servicio puede realizarse desde la herramienta DNS haciendo click-derecho en el servidor y luego eligiendo la pestaña *Monitorizar*. Desde allí, es posible realizar dos tipos de pruebas: consulta simple o recursiva. La primera equivale a una consulta local mientras que la segunda es más compleja y prueba el nombre del servidor mediante una llamada recursiva a otro servidor. De todas formas la herramienta por excelencia para probar los servidores es nslookup que se utiliza desde la línea de comandos. Nslookup funciona en modo interactivo y no interactivo. Si se desea una consulta simple basta con usar el modo no interactivo. La sintaxis es:

nslookup [-opción ...] [computadora a buscar] - [server]]

```
C:\>nslookup yahoo.com
Servidor: 192.168.1.100
Address: 192.168.1.100

Respuesta no autoritativa:
Nombre: yahoo.com
Addresses: 66.218.71.112, 66.218.71.113, 66.218.71.114
```

En modo interactivo se ejecuta nslookup y entonces se presenta un prompt para acceder las opciones. Al finalizar se debe acceder *exit*. Para una lista completa de opciones se ingresa ?.



1.3 Servidor DNS En Linux

Se verá como configurar DNS en un sistema Linux. Aunque la mayoría de los sistemas Linux cuentan con interfaz gráfica que permite configurar distintos servicios, en general es conveniente conocer como se guarda esa información de configuración en los diversos archivos de texto y como se puede levantar un servicio manualmente. Así no importa la interfaz gráfica o utilitario siempre se sabe que se está haciendo.

Los datos de los nombres de dominio se guardan en los servidores de nombre. El sistema BIND utilizado en servidores Unix/Linux (BIND es Berkeley Internet Domain Server) almacena la información en archivos de texto con etiquetas asociadas que se denominan RR (Registro de Recursos). En realidad un servidor de nombres se encarga de relacionar nombres con registros de recursos.

1.3.1 Registros De Recursos

Nombre de Dominio	Tiempo de Vida	Tipo	Clase	Valor
-------------------	----------------	------	-------	-------

El RR tiene el siguiente formato

El nombre de dominio indica el dominio al que pertenece el registro, el tiempo de vida indica la estabilidad del registro que se mide en segundos. La clase se relaciona con el tipo de red, para Internet siempre es IN. El campo *tipo* indica el tipo del registro. Existen diferentes tipos registros de recursos, por ejemplo

 NS	Máquinas Servidoras de Nombre
 MX	Máquinas que intercambian Correo
 A	Dirección IP de un Host
 CNAME	Para realizar alias

SOA Comienzo de Autoridad

Un ejemplo de una entrada con MX sería:

empresa.com 86400 IN MX servidormail.otro.com

Indicando el servidor de correo correspondiente. A continuación se muestra un ejemplo de archivo registro de recursos para un dominio imaginario miempresa.com

```
miempresa.com      86400 IN SOA ns.miempresa.com. admin.miempresa.com. (
3                  ; número de serie
86400              ; refresh
300                ; retry en 5 minutos
2592000            ; expira 30 días
86400              ; mínimo 24 hs. ttl por defecto
)
miempresa.com      86400 IN MX 1 mail1.miempresa.com
miempresa.com      86400 IN MX 2 mail2.miempresa.com
comp1.miempresa.com 86400 IN A    234.56.78.9
www.miempresa.com  86400 IN CNAME comp1.miempresa.com
ftp.miempresa.com  86400 IN CNAME comp1.miempresa.com
```

En los servidores secundarios sólo se cuenta generalmente con archivos básicos de configuración y toman la información de los servidores primarios que a su vez guardan la información en lo que se llama *database files*.

1.3.2 Resolvers

Para que el sistema pueda utilizar la resolución de nombres de DNS lo primero es configurar el *resolver* local. Resolvers son un conjunto de librerías que se encargan de resolver (como su nombre lo indica) una solicitud de nombre. Es decir consultan al servidor de nombres, reciben e interpretan las respuestas del mismo, devuelven la información al programa cliente que la solicitó. Por ejemplo, hay dos rutinas principales en las librerías resolvers: *gethostbyname* y *gethostbyaddr* que permiten obtener la dirección IP a partir del nombre de dominio u obtener el nombre a partir de la dirección IP respectivamente.



1.3.3 Archivo */etc/host.conf*

Este archivo contiene información de configuración para el sistema de resolución de nombres. El formato de este archivo es el siguiente: las opciones deben ubicarse en diferentes líneas y los campos deben separarse con blancos, el símbolo # (cardinal) indica comentario hasta el fin de línea.

Las opciones se ven en la siguiente tabla:

order	Determina el orden en que se utilizarán los servicios de configuración. (ej bind para usar el servidor de nombres, hosts para usar el archivo /etc/hosts.) El orden en que se ubiquen determina el orden en el cual el servicio intenta resolver un nombre.
multi	Puede ser <i>on</i> u <i>off</i> Sirve para indicar si una máquina del archivo /etc/hosts puede tener varias direcciones IP.
alert	También puede usarse <i>on</i> u <i>off</i> . Activa o desactiva el registro de intentos de dar un nombre falso. O sea permite detectar intentos de spoof.
trim	Toma como argumento un nombre de dominio y remueve dicho nombre antes de hacer una búsqueda en el archivo /etc/hosts. O sea que si se especifica <i>midominio.com</i> y se busca <i>maquina.midominio.com</i> , se buscará en el archivo /etc/hosts entradas con el nombre <i>maquina</i> . Esto es útil con el dominio local evitando poner el nombre y sólo escribiendo en /etc/hosts el nombre de la máquina en cuestión.
nospoof	Puede ser <i>on</i> u <i>off</i> . Y se utiliza cuando se realiza una búsqueda inversa para evitar que algún servidor entregue un nombre falso. El problema es que recarga el trabajo del servidor considerablemente.

1.3.4 El Archivo */etc/resolv.conf*

Este archivo contiene una lista de servidores de nombre a utilizar, en caso de utilizarse los servicios BIND. Si esta lista se encuentra vacía, entonces se considera que la propia máquina es el servidor (o sea es local).

La siguiente tabla lista las opciones de */etc/resolv.conf*

nameserver	Especifica la dirección IP de un servidor de nombres
search	Es una lista de dominios a probar. En caso de que no se haya especificado un dominio como parte de una consulta y sólo se haya especificado el nombre del host.
domain	Especifica el nombre del dominio local.

Ejemplo

```
#Dominios local
domain    miempresa.com
#servidor de nombres
nameserver 235.67.98.2
```

1.3.5 Utilización De Named

El demonio de servicios de nombres en Linux es generalmente *named*. La ejecución de *named* puede (y es la opción más recomendada) realizarse al iniciar el sistema. También es posible iniciarla manualmente con el siguiente comando:

```
#/usr/sbin/named
```

Cuando el programa *named* se inicia, lee el archivo *named.boot* y los archivos de zona que se especifiquen en él. Recibirá archivos de zonas de servidores principales y empieza a escuchar peticiones por el puerto 53.

La siguiente tabla muestra las opciones del archivo *named.boot*

directory	Indica el directorio donde se encuentran los archivos de zonas (pueden ponerse varios repitiendo la opción) La ubicación estándar es <i>/var/named</i>
secondary	Indica a <i>named</i> a trabajar como un servidor secundario. Tiene como parámetros un nombre de dominio, una lista de direcciones y un nombre de archivo. Debe proporcionarse al menos una dirección IP del servidor primario.
cache	Contiene la lista de servidores de nombre raíz. Toma un nombre de dominio y un archivo como parámetros Este comando permite a <i>named</i> hacer un cache local y resolver nombres más allá de la zona en la que esté autorizado
primary	Toma como argumentos un nombre de dominio y un archivo. Declara al servidor local primario para el dominio. Carga la información de la zona del archivo dado como parámetro.
forwardes	Lleva como argumento una lista de direcciones. Las direcciones especifican servidores de nombre a los que <i>named</i> puede preguntar si no puede encontrar la respuesta en su cache local
slave	Indica que el servidor será esclavo. O sea nunca realizará consultas recursivas sino que las redirigirá a los servidores especificados en la opción anterior (<i>forwardes</i>)

Como en Windows, es posible utilizar el comando *nslookup* para verificar el funcionamiento del servidor de nombres.