

# Sistema de nombres de dominio (DNS)

## SUMARIO

- El sistema de nombres de dominio (DNS)
- DNS en sistemas GNU/Linux
- DNS en sistemas Windows

## OBJETIVOS

- Determinar las ventajas del uso del servicio DNS.
- Mostrar la estructura básica del funcionamiento del protocolo DNS.
- Instalar, configurar y arrancar un servidor DNS.
- Habilitar el uso de este servicio en un cliente DNS.
- Establecer los mecanismos de comprobación necesarios para asegurar el correcto funcionamiento de este servicio.
- Aplicar todas estas operaciones tanto en sistemas GNU/Linux como en sistemas Windows.

14251 km  
8855 mi INDIA

2890 km  
1796 mi CANADÁ

7846 km  
4875 mi MARRUECOS

8406 km  
5220 mi ALEMANIA

XCARET

2527 km  
1570 mi ECUADOR

HAWAII 7305 km  
4539 mi

5911 km  
3673 mi BRASIL

GRECIA 10263 km  
6377 mi

2277 km  
1415 mi COLOMBIA

13557 km  
8424 mi KENIA

6208 km  
3957 mi CHILE

## 1 > Sistema de nombres de dominio (DNS)

### 1.1 > ¿Qué es el servicio DNS?

El DNS (Domain Name System) o sistema de nombres de dominio es un sistema que hace legibles para los usuarios las direcciones IP. Para ello, asocia direcciones numéricas con direcciones alfanuméricas, como por ejemplo 173.194.34.16 con www.google.com.

Este sistema es una base de datos jerárquica y distribuida que permite localizar equipos y servicios mediante nombres alfanuméricos fáciles de recordar. Sin DNS el usuario debería acceder a los recursos mediante el uso de las direcciones IP, lo que resultaría muy engorroso. Además, como estas pueden cambiar, sería muy complicado mantener una lista actualizada de direcciones.

### 1.2 > Nombres de dominio

Cuando hablamos del sistema de nombres de dominio en realidad nos referimos a la base de datos que relaciona direcciones IP con nombres de un ordenador o de un conjunto de ellos.

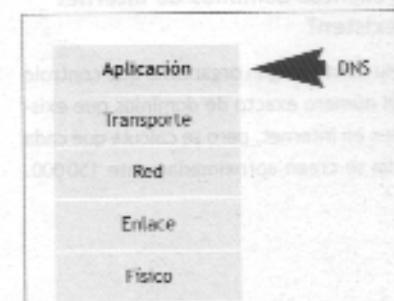
DNS nació en los primeros tiempos de Internet, cuando el Departamento de Defensa de los Estados Unidos creó una pequeña red de ordenadores llamada ARPANET destinada a la investigación. Los nombres de los ordenadores de esta red se administraban con un único archivo llamado hosts.txt. Este contenía la relación entre el nombre del equipo y su dirección IP y era compartido por todos los equipos de la red, lo que permitía consultarla y actualizarla cuando fuera necesario. A esta manera de relacionar nombre e IP se le conoce como **sistema de nombres planos**.

Conforme creció la red y aumentó su complejidad, se hizo necesaria la creación de un nuevo sistema de nombres que fuera más versátil y permitiera una mayor escalabilidad.

Así, en 1984 apareció el DNS, un sistema descentralizado, escalable y jerárquico, en forma de árbol. A esta manera de relacionar nombre e IP se le conoce como **sistema de nombres jerárquicos**. En un sistema de este tipo los nombres del ordenador contienen información de su localización, lo que permite que puedan existir en redes diferentes ordenadores con el mismo nombre.

El sistema de numeración telefónico, por ejemplo, tiene una estructura jerárquica. Cualquier número de abonado, como puede ser el 917017000, contiene información que permite encaminar la llamada a través de la red telefónica:

9	1	701	7000
Prefijo	Código del área	Código de la central	Código abonado
	Madrid	Gran Vía	Secretaría de Cultura



2.1. DNS en el modelo TCP/IP.

Organismos especializados en la gestión de dominios

El ICANN (Internet Corporation for Assigned Names and Numbers) es el encargado de los directorios, como .com, .org o .net.

Los dominios asociados a cada país se hallan registrados por sus gobiernos. En España los gestiona el nic.es, integrado en red.es.

### Espacio de nombres

¿Cuántos dominios de Internet existen?

No existe ningún organismo que controle el número exacto de dominios que existen en Internet, pero se calcula que cada día se crean aproximadamente 150.000.

Los datos que gestiona un DNS se conocen como **nombres de dominio** y están organizados en forma de árbol invertido. Cada nodo del árbol se llama **dominio** y recibe una etiqueta, por ejemplo .com.

El nombre de dominio de un nodo se crea mediante la concatenación de todas las etiquetas, comenzando por dicho nodo y terminando con el nodo raíz. Para representarlo de forma escrita, unimos las etiquetas de derecha a izquierda separándolas por puntos, por ejemplo www.google.com.

En el sistema DNS un nodo puede tener un nombre de hasta 63 caracteres. La profundidad de nodos está limitada a 127 niveles.

El primer nodo se conoce como **raíz** (root) y se representa mediante el símbolo del punto.

Para acceder, por ejemplo, a Wikipedia escribiremos:

www	.wikipedia	.org	.com
Servicio	Nodo nivel 2	Nodo nivel 1	Nodo raíz

Como podemos ver, la dirección se escribe en sentido contrario a la búsqueda, es decir, empezando por la hoja y acabando por la raíz.

### FQDN (*fully qualified domain name*)

Nos indica el nombre completo de una dirección IP, comenzando por el nodo y acabando con la raíz.

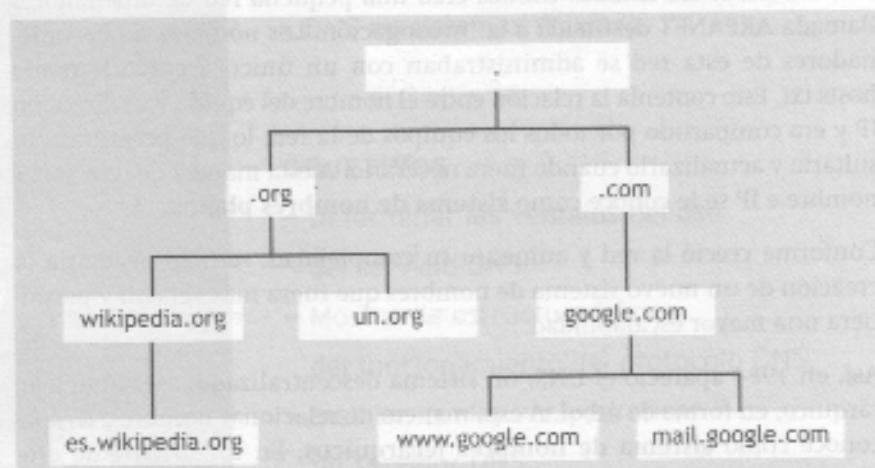
Utilizado, por ejemplo, por el dominio .arpa, su estructura sería:

1.100.168.192.in-addr.arpa

Con ella accederíamos al nombre de dominio de la IP 192.168.100.1.

Un **dominio absoluto** finaliza con un punto:

www.google.com.



2.2. Estructura jerárquica del DNS.

La estructura jerárquica también permite la gestión de los nodos de manera autónoma.

ICANN, como se muestra en la figura 2.2, gestiona el dominio de primer nivel (.org), pero Wikipedia gestiona su nodo, lo que permite añadir más subniveles. Esto se conoce como **delegar**.

El servicio DNS no suele utilizarse de manera independiente, sino acompañado de otros servicios (como DHCP, HTTP, FTP, etc.) que serán explicados a lo largo del libro.

En la figura 2.2, también puede observarse cómo Google administra los servicios de su dominio de manera autónoma.

### Dominios genéricos (TLD)

Los dominios de primer nivel o raíz, también llamados TLD (*Top Level Domains*), no pueden ser comprados por los usuarios. Cuando se desea adquirir un dominio, debemos hacernos con uno de segundo nivel.

Los dominios de primer nivel, gestionados por Estados e instituciones independientes, se dividen en tres grandes grupos:

- Infraestructura.
- Dominios genéricos (gTLD).
- Dominios geográficos (ccTLD).

En la tabla siguiente se muestran las subdivisiones de cada uno de estos dominios:

Tablas subdivisión TLD

TLD	Dominios	
Infraestructura	Utilizado para obtener el FQDN	.arpa
gTLD Dominios genéricos	(uTLD) No patrocinados. Estos dominios pueden ser alquilados sin restricciones. Están gestionados por el ICANN.	.com, .org, .net, .int, .gov, .info, .name, .biz
	(sTLD) Existen limitaciones a la hora de contratar estos dominios. Están patrocinados por diferentes instituciones.	.aero, .asia, .cat, .coop, .edu, .jobs, .mobi, .museo, .pro, .tel, .travel, .xxx
ccTLD Dominios geográficos	Creados por IANA. Existen unos 243 gestionados por los distintos gobiernos mediante organizaciones propias.	.es, .uk, .eu, .us

La adquisición de un dominio en Internet se denomina **registro de dominio**. Para ello, el usuario o registrador ha de contactar con la empresa registradora autorizada por ICANN y se comprueba en primer lugar que el dominio deseado no pertenece a nadie. Una vez aceptadas las condiciones, la empresa registradora contacta con el ICANN y realiza los trámites. De este modo en unas horas el dominio estará disponible.

A partir del año 2004 el ICANN permitió registrar dominios IDN (*internationalized domain name*) o nombres de dominio internacionalizados, que son los que contienen caracteres específicos de lenguas como el cirílico, el chino, el árabe, el griego, etc. Estos también posibilitan añadir acentos y registrar dominios con la letra «ñ». Algunos ejemplos de IDN son:

中國 .中国 .рФ

### Actividades propuestas

1. Busca dos empresas registradoras autorizadas en España.

### 1.3 > Zonas

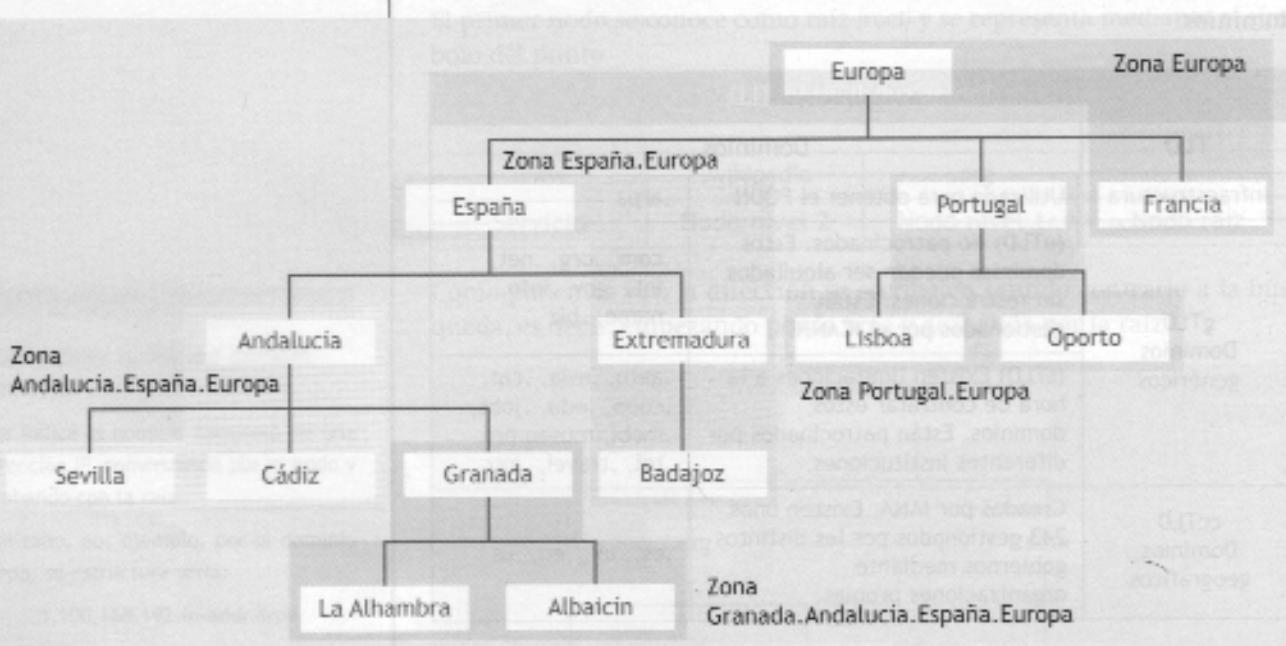
#### Zona y dominio

Un dominio puede dividirse en subdominios. Por ejemplo, para el nombre de dominio google.com, google es un subdominio del TLD .com. El dominio, por tanto, estaría formado por el subárbol, para el cual el nodo raíz es google. La zona son las diferentes partes contiguas del árbol administradas por uno o más servidores DNS autoritativos.

La parte de la base de datos de nombres de dominio alojada en el servidor DNS recibe el nombre de **zona**. Una zona puede ser gestionada por más de un servidor. Estos tienen bases de datos con la información completa sobre la zona, por lo que se les conoce como **servidores autoritativos**.

La estructura jerárquica DNS se basa en una relación cliente/servidor. Cuando un cliente o host quiere acceder a algún lugar, realiza una pregunta al servidor DNS, el cual consultará su base de datos e intentará responder a la pregunta.

La siguiente figura muestra una estructura formada por dominios y zonas.



2.3. Estructura de zonas y dominios.

#### Whois

Es un protocolo que nos permite acceder a una base de datos que determina el dueño de un nombre de dominio o dirección IP.

En la actualidad podemos encontrar un gran número de páginas web que nos permiten realizar esta consulta.

Los dominios son los rectángulos; en este ejemplo tenemos 14. Estos dominios forman cinco zonas. El nombre del dominio correspondiente a cada zona se determinará según los nodos que contenga.

Toda zona debe tener, al menos, dos servidores autoritativos: el primario, que contiene los ficheros que forman la base de datos de la zona, y el secundario, que obtiene estos ficheros del primero mediante transferencia.

La zona primaria es la que está supervisada por el servidor primario y existe únicamente una. El servidor primario contiene la base de datos que servirá de origen para realizar todas las copias que sean necesarias para los servidores secundarios. Aunque reiniciemos el servidor esta base de datos no se borrará.

La zona secundaria la forman los servidores secundarios. Puede haber tantas zonas secundarias como servidores. Cuando reiniciamos el servidor secundario, la base de datos normalmente debe replicarse de nuevo a partir de la zona primaria.

## Transferencia de zona

La transferencia de zona es la operación mediante la cual un servidor primario transfiere el contenido del archivo de la base de datos de zona DNS a un servidor secundario. Esta operación siempre la inicia el servidor secundario. La transferencia se produce cuando:

- Iniciamos el servicio DNS en el servidor secundario.
- Caduca el tiempo de actualización.
- Se guardan los cambios en la base de datos de la zona principal.

## Delegación

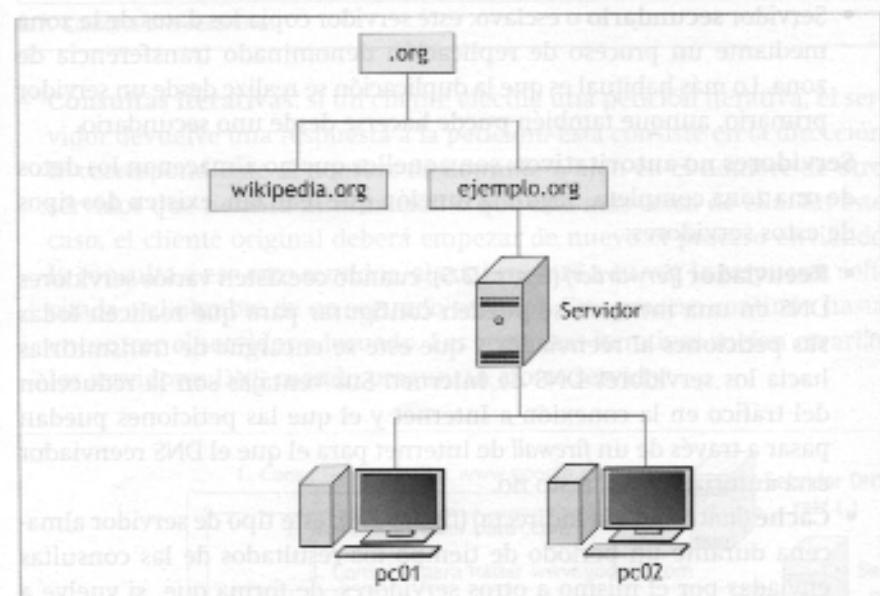
A pesar de que ICANN o su sección IANA supervisan la creación de dominios a través de empresas gestoras o de estados, no tienen capacidad técnica para gestionarlos. El modelo jerárquico DNS permite traspasar, en la mayoría de los casos, a su propietario. Esta operación se conoce como **delegación**.

La nueva entidad gestora tiene la capacidad de crear nuevos subdominios y debe mantener los servidores DNS de su dominio.

El dominio de nivel superior que ha delegado la administración pierde el control de la nueva zona y únicamente conoce la dirección de los servidores DNS de la misma.

La zona de nivel superior se conoce como **zona padre** y la de nivel inferior como **hijo**.

En la siguiente figura podemos ver un ejemplo:



2.4. Delegación de dominios.

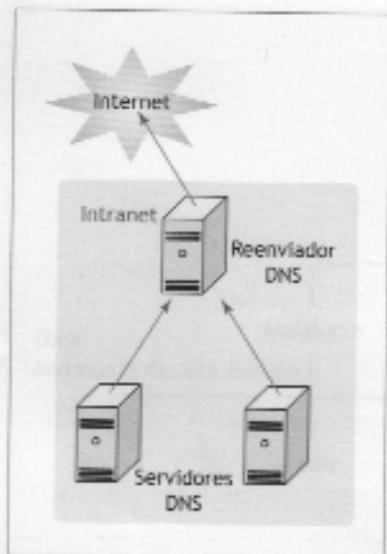
ICANN, como se muestra en la figura, otorga la delegación del dominio gTLD `ejemplo.org` a la empresa Ejemplo. A partir de ahora, la única información que poseerá el dominio padre gestionado por ICANN serán las direcciones IP de los servidores DNS de la empresa Ejemplo.

## 2 > Funcionamiento del DNS

en los sistemas operativos

Modelo TCP/IP	
Aplicación	Transporte
DNS	TCP (53) UDP (53)

sobre el cual el nodo hace las peticiones de zona con las diferentes partes distintas del árbol administradas por una o más servidores DNS autoritativos.



2.5. DNS no autoritativo que actúa como reenviador.

El servicio de nombres de dominio se implementa a través del protocolo DNS. Este estándar especifica que, para la comunicación que se realice entre el cliente y el servidor, se haga uso del puerto 53 tanto para mensajes UDP como TCP.

### 2.1 > Clasificación de servidores de nombres

Los servidores de nombres son la parte más importante del DNS, ya que almacenan y gestionan información sobre los dominios y responden a las consultas de resolución de nombres que realizan los clientes. Estos servidores pueden implementarse sobre dispositivos dedicados o software ejecutado sobre máquinas que también realizan otras tareas.

Atendiendo a la cantidad de datos que almacenan, podemos diferenciar dos categorías de servidores de nombres:

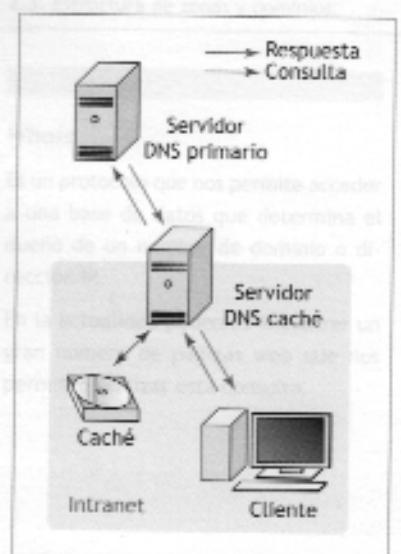
- **Servidores autoritativos:** son los encargados de almacenar la información completa de la zona. Debe haber al menos uno por zona. En general, las zonas tienen dos o más servidores autoritativos sobre diferentes redes para mantener activo el servicio ante fallos que puedan surgir. En función de si los datos que contienen son originales o no, existen dos tipos de estos servidores:

- Servidor **primario** o maestro: es el servidor que mantiene los datos, nombres DNS, originales de una zona completa. Permite configurar las zonas, como por ejemplo dar de alta y de baja los nombres de dominio.
- Servidor **secundario** o esclavo: este servidor copia los datos de la zona mediante un proceso de replicación denominado transferencia de zona. Lo más habitual es que la duplicación se realice desde un servidor primario, aunque también puede hacerse desde uno secundario.

- **Servidores no autoritativos:** son aquellos que no almacenan los datos de una zona completa. Según la función que realizan, existen dos tipos de estos servidores:

- **Reenviador (forwarder)** (figura 2.5): cuando coexisten varios servidores DNS en una intranet, se pueden configurar para que realicen todas sus peticiones al reenviador y que este se encargue de transmitirlas hacia los servidores DNS de Internet. Sus ventajas son la reducción del tráfico en la conexión a Internet y el que las peticiones puedan pasar a través de un firewall de Internet para el que el DNS reenviador está autorizado y el resto no.

- **Caché (hint o por vía indirecta)** (figura 2.6): este tipo de servidor almacena durante un periodo de tiempo los resultados de las consultas enviadas por él mismo a otros servidores, de forma que, si vuelve a recibir la misma petición, el servidor la devolverá desde su caché sin tener que realizar el proceso de consulta completo. Este procedimiento lo deja en manos de servidores en los que confía, para que estos hagan la consulta completa en su nombre. Sirve para descongestionar servidores que reciben grandes cantidades de peticiones o zonas con alta carga en la red.



2.6. DNS no autoritativo que actúa como caché.

## 2.2 > Consultas recursivas e iterativas

La actividad principal de un servidor DNS es contestar consultas, tanto de un cliente como de otro servidor DNS. Según el modo en que se envían las consultas, las podemos clasificar en dos tipos:

- **Consultas recursivas:** cuando un cliente realiza una petición recursiva a un servidor, este debe responder con la información que guarda en su base de datos local. Si no la tiene, debe hacerse cargo de encontrarla en nombre del cliente, enviando nuevas peticiones a otros servidores. El cliente original solo envía una petición y recibe la información o bien un mensaje de error indicando que no existe. Las consultas recursivas suelen generarlas los clientes DNS, aunque la figura 2.7 muestra una consulta recursiva reenviada por un servidor.

### Sabías que...

Los DNS raíz no aceptan consultas recursivas porque se consideraría un abuso y saturaría el sistema.

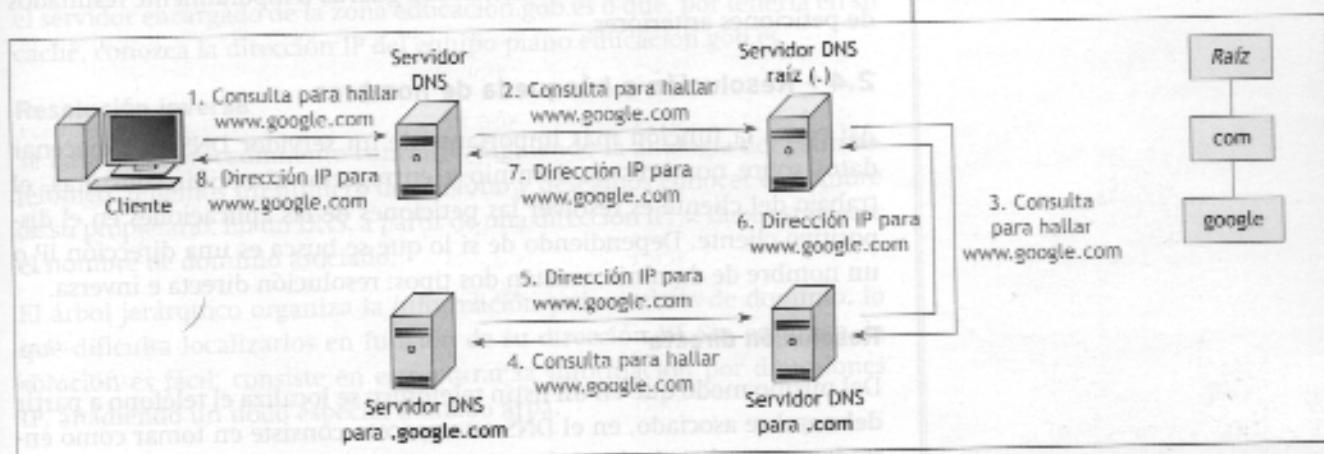


Figura 2.7. Consulta DNS recursiva.

- **Consultas iterativas:** si un cliente efectúa una petición iterativa, el servidor devuelve una respuesta a la petición. Esta consiste en la dirección IP correspondiente al nombre de dominio o bien en el nombre de otro servidor que tiene la información o que está más cerca de ella. En este caso, el cliente original deberá empezar de nuevo el proceso enviando la consulta a ese otro servidor, el cual enviará a su vez la respuesta solicitada o el nombre de un segundo servidor. Este proceso continúa hasta encontrar el servidor adecuado. Las consultas iterativas suelen crearlas los servidores DNS cuando preguntan a otro servidor.



Figura 2.8. Consulta DNS iterativa.

### 2.3 > Clientes DNS (resolvers)

Los clientes DNS, también conocidos como resolvers, son programas que hacen de interfaz entre las aplicaciones de usuario y el DNS. Por ejemplo, un resolver recibe una petición de un programa, como puede ser un navegador web, telnet o FTP, en forma de llamada al sistema operativo, y devuelve la información en forma compatible con el formato de esa aplicación.

El resolver se localiza en la misma máquina que la aplicación que requiere sus servicios, pero puede necesitar consultar servidores de nombre situados en otros equipos.

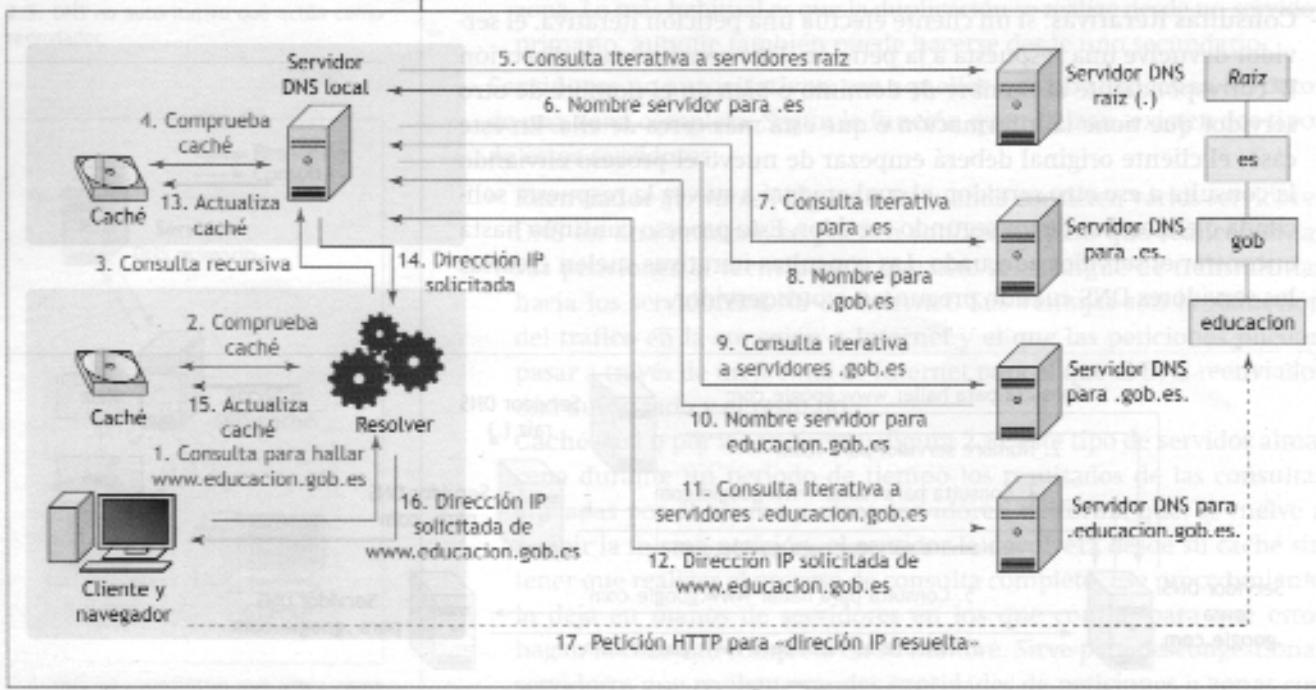
Una de sus funciones más importantes es eliminar retrasos en la red y aliviar la sobrecarga de consultas sobre los servidores de nombres. Esto lo hace mediante el uso de su caché, donde guarda temporalmente resultados de peticiones anteriores.

### 2.4 > Resolución o búsqueda de nombres

Así como la función más importante de un servidor DNS es almacenar datos sobre nombres de dominio y entregarlos al recibir consultas, el trabajo del cliente es resolver las peticiones de las aplicaciones en el dispositivo cliente. Dependiendo de si lo que se busca es una dirección IP o un nombre de dominio, existen dos tipos: resolución directa e inversa.

#### Resolución directa

Del mismo modo que en un listín telefónico se localiza el teléfono a partir del nombre asociado, en el DNS este proceso consiste en tomar como entrada un nombre de dominio y determinar su correspondiente dirección IP. Esta es la función más utilizada.



2.9. Proceso de resolución directa de nombres de dominio.

Por ejemplo, si un cliente DNS tiene la necesidad de localizar el equipo piano.educacion.gob.es desde cualquier lugar del mundo, será necesario que realice una petición a su servidor DNS. Lo más probable es que su servidor no conozca ese dominio, por lo que empezará buscando la raíz del árbol, es decir, preguntando por la parte más genérica del nombre: .es. Si el servidor raíz es autoritativo para esa zona, devolverá la dirección IP correspondiente; sin embargo, si no lo es, devolverá el nombre del servidor responsable para el dominio de primer nivel (.es).

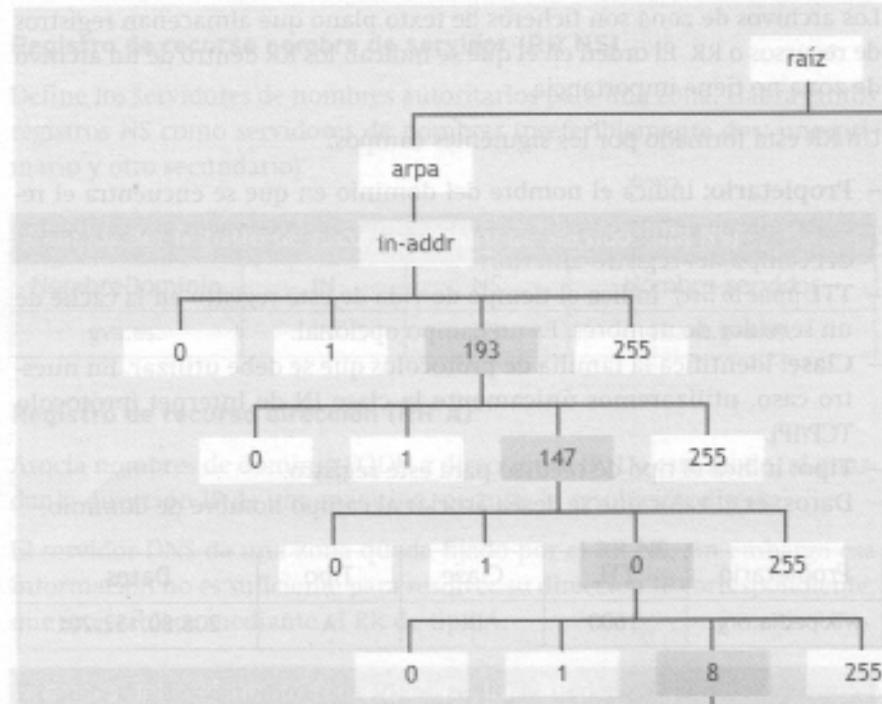
Ahora se deberá consultar a ese servidor si es autoritativo para la zona educación.gob.es. Si no lo es, no conocerá la dirección IP que buscamos, pero sí al servidor autoritativo en gob.es.

Y así continuaremos descendiendo en el árbol de dominios hasta localizar el servidor encargado de la zona educación.gob.es o que, por tenerla en su caché, conozca la dirección IP del equipo piano.educacion.gob.es.

### Resolución inversa

Se basa en el procedimiento contrario. Siguiendo la analogía del listín telefónico, tenemos un número de teléfono y deseamos conocer el nombre de su propietario. En un DNS, a partir de una dirección IP, se debe establecer el nombre de dominio asociado.

El árbol jerárquico organiza la información por nombres de dominio, lo que dificulta localizarlos en función de su dirección IP. Sin embargo, la solución es fácil: consiste en estructurar la información por direcciones IP, añadiendo un nodo especial llamado arpa.



2.10. Dirección inversa 8.0.147.193.in-addr.arpa.

(ops)	Número de serie
Actualización	00000000000000000000000000000000
Reintento	00000000000000000000000000000000
Caducidad	00000000000000000000000000000000
Valor TTL	00000000000000000000000000000000

Sabías que...

A veces se utiliza el símbolo arroba (@) para representar el nombre de la zona que se define. Por ejemplo:

• 192.168.1.100@es

• 192.168.1.100@arpa

• 192.168.1.100@arpa.in-addr.es

• 192.168.1.100@arpa.in-addr.es.arpa

• 192.168.1.100@arpa.in-addr.es.arpa.es

• 192.168.1.100@arpa.in-addr.es.arpa.es.mec

• 192.168.1.100@arpa.in-addr.es.arpa.es.mec.piano

Puntero a dirección inversa para piano.mec.es (193.147.0.8)

Por lo tanto, se añade un subárbol con una jerarquía numérica que convive con la jerarquía de nombres de dominio.

Ese subárbol se implementa utilizando un nombre de dominio especial, `in-addr.arpa`, situado dentro del dominio reservado de primer nivel `.arpa`.

Descendiendo, se despliega una jerarquía numérica que cubre todo el espacio de direcciones IP y que consiste en lo siguiente:

- En el primer nivel dentro de `in-addr.arpa` existen 256 subdominios, desde el 0 al 255. Por ejemplo, `195.in-addr.arpa`.
- Dentro de cada subdominio de primer nivel hay 256 subdominios más de segundo nivel, organizados de la misma forma. Por ejemplo, `77.195.in-addr.arpa`.
- Una vez más, cada uno de ellos contendrá otros 256 subdominios de tercer nivel. Por ejemplo, siguiendo los casos que utilizamos antes, `0.147.193.in-addr.arpa`.
- Por último, tendremos 256 equipos para cada uno de los anteriores, en el cuarto nivel, describiendo completamente la dirección IP inversa. Para el ejemplo tendríamos la dirección inversa `8.0.147.193.in-addr.arpa` para el nombre del equipo `piano.mec.es`.

## 2.5 > Base de datos DNS. Tipos de registros

La base de datos DNS contiene los llamados **archivos de zona**, distribuidos entre los servidores de nombres. Estos archivos permiten asociar los nombres de dominio con direcciones IP.

Los archivos de zona son ficheros de texto plano que almacenan registros de recursos o RR. El orden en el que se indican los RR dentro de un archivo de zona no tiene importancia.

Un RR está formado por los siguientes campos:

- **Propietario:** indica el nombre del dominio en que se encuentra el recurso que se define en el RR. Si este campo aparece vacío, toma el valor del campo del registro anterior.
- **TTL (time to live):** indica el tiempo de vida de este registro en la caché de un servidor de nombres. Es un campo opcional.
- **Clase:** identifica la familia de protocolos que se debe utilizar. En nuestro caso, utilizaremos únicamente la clase IN de Internet (protocolo TCP/IP).
- **Tipo:** indica el tipo de recurso para este registro.
- **Datos:** es el valor que se desea asociar al campo nombre de dominio.

Propietario	TTL	Clase	Tipo	Datos
wikipedia.org.	3600	IN	A	208.80.152.201

A continuación se describen los tipos de RR más comunes para la clase IN que pueden aparecer en un archivo de zona: inicio de autoridad (RR SOA), nombre de servidor (RR NS), dirección (RR A), nombre canónico (RR CNAME), puntero (RR PTR) e intercambio de correo-e (RR MX).

### Dig

`Dig` es una herramienta que permite realizar consultas a un servidor DNS para que responda con los registros de recursos de una zona determinada.

Existe una gran diversidad de páginas web que ofrecen este servicio en Internet.

### Iptools

Herramienta online que muestra los RR de la base de datos DNS.



### Registro de recurso inicio de autoridad (RR SOA)

Indica dónde comienza una zona y el servidor de nombres que tendrá su autoridad. Únicamente puede haber un registro de tipo SOA por cada zona.

Campos del registro de recurso inicio de autoridad (RR SOA)

NombreDominio	Tipo	SOA	nsPrimario	admin.nsPrimario	(ops)
gva.es.	IN	SOA	ninot.gva.es.	admincorreo.gva.es.	(2012020700; 14400; 300; 604800; 7200); Número de serie Actualización Reintento Caducidad Valor TTL

El significado de los campos utilizados es el siguiente:

- **NombreDominio:** el nombre de dominio que describe la zona.
- **nsPrimario:** especifica el nombre del servidor de nombres primario.
- **admin.nsPrimario:** indica la dirección de correo del administrador del dominio. En este caso la arroba (@) se sustituye por un punto (.)
- **ops:** son un conjunto de parámetros que se utilizan para definir la comunicación entre el servidor de nombre primario y los secundarios.

En el registro SOA se establecen algunas opciones que describen tiempos cuyo valor se expresa en segundos. Para hacer más fácil su legibilidad, se pueden indicar en formato semana (week), día (day), hora (hour) y minuto (minute). En el ejemplo, el registro de zona RR SOA quedaría así:

(2012020700 4h 5m 1w 2h)

### Registro de recurso nombre de servidor (RR NS)

Define los servidores de nombres autoritarios para una zona. Habrá tantos registros NS como servidores de nombres (preferiblemente dos: uno primario y otro secundario).

Campos del registro de recurso nombre de servidor (RR NS)

NombreDominio	Tipo	NS	Nombre servidor
gva.es.	IN	NS	tirant.gva.es.

### Registro de recurso dirección (RR A)

Asocia nombres de dominio FQDN a direcciones IP. De este modo, al guardar la dirección IP de una máquina, permite la resolución directa.

El servidor DNS de una zona queda fijado por el RR NS, sin embargo esa información no es suficiente para resolver su dirección IP correspondiente, que se establece mediante el RR de tipo A.

Campos del registro de recurso dirección (RR A)

NombreDominio	Tipo	A	IP
tirant.gva.es.	IN	A	172.16.100.127

### Registro de recurso nombre canónico (RR CNAME)

Permite crear un alias o nombre alternativo para un nombre de nodo real, es decir, hacer referencia a un mismo equipo usando distintos nombres.

Campos del registro de recurso nombre canónico (RR CNAME)

NombreDominio	IN	CNAME	Nombre canónico o IP
ftp.edu.gva.es.	IN	CNAME	www.edu.gva.es.

Estos registros permitirán acceder a un equipo haciendo referencia al servicio que se quiera usar y no a su nombre real. Siguiendo el ejemplo, los clientes podrán acceder al servidor de educación de la Generalitat Valenciana tanto con www.edu.gva.es como con ftp.edu.gva.es.

Pero, ¿no sería más sencillo usar siempre el mismo nombre independientemente del servicio al que se quiera acceder? Puede que sea así en el caso de tener un solo servidor, pero en empresas que distribuyen sus servicios en varias máquinas o que puedan hacerlo en un futuro, los registros de alias permiten acceder al servicio deseado independientemente de si está instalado en una máquina o en otra. Es más, en el caso de cambiarlo de un servidor a otro, usando los alias el usuario no notaría la diferencia.

### Registro de recurso puntero (RR PTR) o registro inverso

Relaciona una dirección IP con un nombre de dominio completamente cualificado. Se necesita un registro PTR por cada subred de la zona.

Campos del registro de recurso puntero (RR PTR)

IPInversa.in-addr.arpa	IN	PTR	Nombre canónico
254.16.77.195.in-addr.arpa	IN	PTR	inf16254.gva.es.

### Registro de recurso intercambio de correo-e (RR MX)

Define un servidor de correo para el dominio. Si se indican varios servidores de correo, se puede establecer la prioridad anteponiéndoles un número.

Campos del registro de recurso intercambio de correo-e (RR MX)

NombreDominio	IN	MX	num	Servidor correo
gva.es.	IN	MX	10	gollum.gva.es.

## Actividades propuestas

2.. A través de la herramienta *Dig*, implementada en *IpTools*, averigua los datos completos de:

- El RR de tipo SOA para la zona wikipedia.org. Necesitarás marcar la opción *Dig*, dejar vacío el campo siguiente e incluir la zona en el campo *Host/IP*.
- El RR de tipo NS para la zona wikipedia.org.
- El RR de tipo A para la zona wikipedia.org.
- El RR de tipo CNAME para la zona www.wikipedia.org.

### 3 > Evolución del protocolo DNS

Cada vez son más usuarios los que utilizan las redes de comunicación, lo que ha provocado la aparición de nuevas necesidades y amenazas que han hecho avanzar y perfeccionar el protocolo DNS. Así han surgido, entre otros, el DDNS o DNS dinámico y el DNSSEC o DNS seguro.

#### 3.1 > Actualizaciones dinámicas (DDNS)

El protocolo DDNS (Dynamic DNS) establece la forma de actualizar en tiempo real la base de datos gestionada por un servidor de nombres. DDNS permite que un cliente añada, reemplace o elimine los registros de recursos de un servidor DNS primario, mediante un tipo especial de mensajes.

Existen dos escenarios donde se emplea este protocolo: en el acceso desde Internet y en un servidor DNS local.

##### Acceso desde Internet

Si configuramos un ordenador para que ofrezca determinados servicios al público, este debe ser visible desde Internet. Para poder acceder a él, será necesario conocer la dirección IP o el nombre de dominio del router al que se conecta. Sin embargo, cada vez es más frecuente que los ISP (proveedores de servicios de Internet) asignen a sus usuarios una dirección IP de rango, diferente de una sesión a otra, llamada **dirección IP dinámica**. Surge entonces el problema de que la dirección IP con la que se identifica el equipo en Internet puede variar en cuestión de semanas, días u horas.

Para solucionar este inconveniente, DDNS permite la utilización de un nombre de dominio propio a clientes con direcciones IP dinámicas.

Este servicio lo ofrecen portales como freedns.afraid.org, que entregan un nombre de dominio cuyo registro de recursos RR A es modificado cada vez que el ISP del cliente cambia la dirección IP.

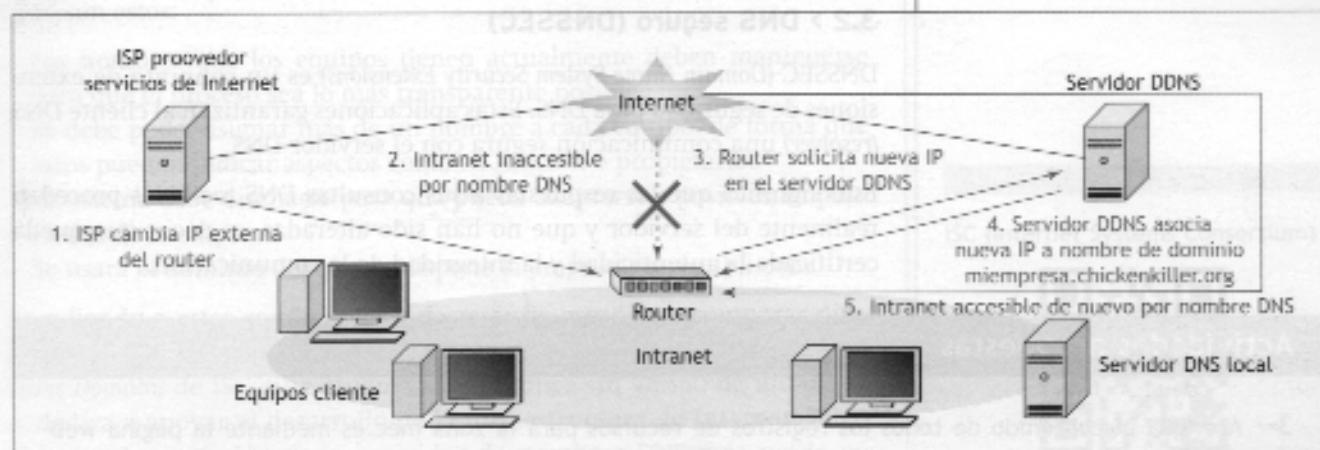
El encargado de solicitar la actualización es el cliente, de forma que el cambio de dirección IP es comunicado al servidor DNS del portal.

Proveedores de DNS dinámico

Lista de proveedores de DNS dinámico:



<http://dnslookup.me/dynamic-dns>



2.11. DDNS con servidor DNS externo.

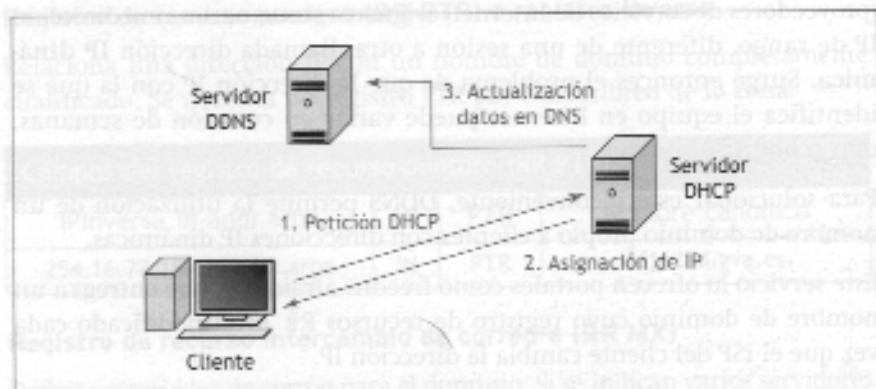
### Acceso desde un servidor DNS local

En una red local donde se añaden continuamente equipos nuevos o se modifica su nombre, es necesario actualizar la información que administra el servidor DNS de la zona local; en particular, la dirección IP y/o el nombre de dominio.

Esa gestión se puede realizar manualmente, sin embargo se dispone de la actualización dinámica del servidor DNS para automatizar dicha tarea. El mecanismo más sencillo utiliza el servidor DHCP, encargado de asignar direcciones IP dinámicamente a equipos de la red. Este tipo de servidor lo veremos en la siguiente unidad.

Simplificando el proceso, los pasos que realiza se describen a continuación (figura 2.12):

1. El cliente DHCP envía una petición al servidor DHCP para que le suministre una dirección IP.
2. El servidor DHCP responde enviando una dirección IP.
3. Una vez el equipo cliente queda configurado, el servidor DHCP remite una petición de actualización al servidor DDNS que contiene la dirección IP asignada, solicitando que actualice su base de datos y la asocie con el nombre de dominio que ya posee.



2.12. DNS dinámico con DNS local.

### 3.2 > DNS seguro (DNSSEC)

DNSSEC (Domain Name System Security Extensions) es un conjunto de extensiones de seguridad para DNS. Estas aplicaciones garantizan al cliente DNS (*resolver*) una comunicación segura con el servidor DNS.

Esto significa que las respuestas a sus consultas DNS recibidas proceden realmente del servidor y que no han sido alteradas, es decir, que queda certificada la autenticidad y la integridad de la comunicación.

### Actividades propuestas

3. Averigua el contenido de todos los registros de recursos para la zona `mec.es` mediante la página web [network-tools.com/nslookup](http://network-tools.com/nslookup). Anota los servidores de dominio, el autoritativo, el de correo-e y sus direcciones IP.

## 4 >> DNS en sistemas GNU/Linux

Hoy es un día importante, vuestra primera jornada de trabajo en la empresa ServPubli. Siguiendo el plan de trabajo pactado con sus representantes, vais a empezar con el primero de los problemas planteados: la implantación de un servicio de resolución que permita traducir nombres a direcciones IP.

En las reuniones previamente mantenidas os dijeron que los trabajadores de la empresa tienen dificultades a la hora de usar las direcciones IP para acceder remotamente, desde sus puestos de trabajo, a los distintos equipos de la red de la empresa. Los trabajadores no tienen estudios informáticos, solo usan los ordenadores a nivel de usuario, por lo que les cuesta tanto memorizar las direcciones como relacionarlas con los servicios que ofrecen los equipos a los que quieren acceder.

Después de estudiar la red, el trabajo que desarrollan los empleados y la perspectiva de crecimiento, proponéis a la empresa que, además de usar el servicio DNS para navegar por Internet, este se utilice también para resolver los nombres de los ordenadores de la red de área local.

Para defender la opción que planteáis, presentáis a la empresa los siguientes argumentos:

- Los empleados recordarán más fácilmente los nombres que las direcciones IP.
- Los nombres de equipo, si se asignan correctamente, pueden dar información sobre la máquina a la que hacen referencia y la función que esta desempeña.
- Como el DNS tiene una estructura jerárquica, en el caso de que la empresa crezca, se adaptaría muy bien a las nuevas necesidades.
- La base local de datos que relaciona los nombres con las direcciones IP se configura y se mantiene en un único equipo: el servidor DNS.
- En el caso de cambiar la dirección IP de alguno de los equipos de la red de la empresa, los empleados podrán seguir accediendo a estos con los mismos nombres.

Los requisitos que ServPubli os ha planteado para poner en marcha el servicio son estos:

- Los nombres que los equipos tienen actualmente deben mantenerse para que el proceso sea lo más transparente posible.
- Se debe poder asignar más de un nombre a cada equipo, de forma que estos puedan indicar aspectos como su función o propietario.
- El sistema debe diseñarse para que pueda adaptarse a posibles ampliaciones de la empresa.
- Se usará el dominio del que ya dispone la empresa: servpubli.com.

Atendiendo a estas condiciones y después de estudiar y comparar diferentes opciones, habéis decidido usar la versión 9 de BIND (Berkeley Internet Name Domain) de ISC, una organización pública sin ánimo de lucro que se dedica a apoyar el desarrollo de la infraestructura de Internet. BIND es la implementación de un servidor de nombres DNS más usada en Internet.

para que se acceda

información relevante

que se adapte

ISC (Internet Systems Consortium)



<http://www.isc.org>

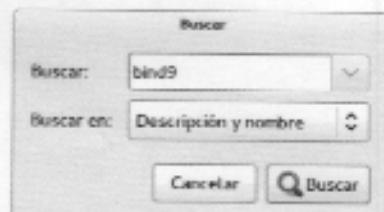
**Datos de acceso**

Usuario: adminservidor

Contraseña: S3rvId@r

**Paquete que se debe instalar**

bind9

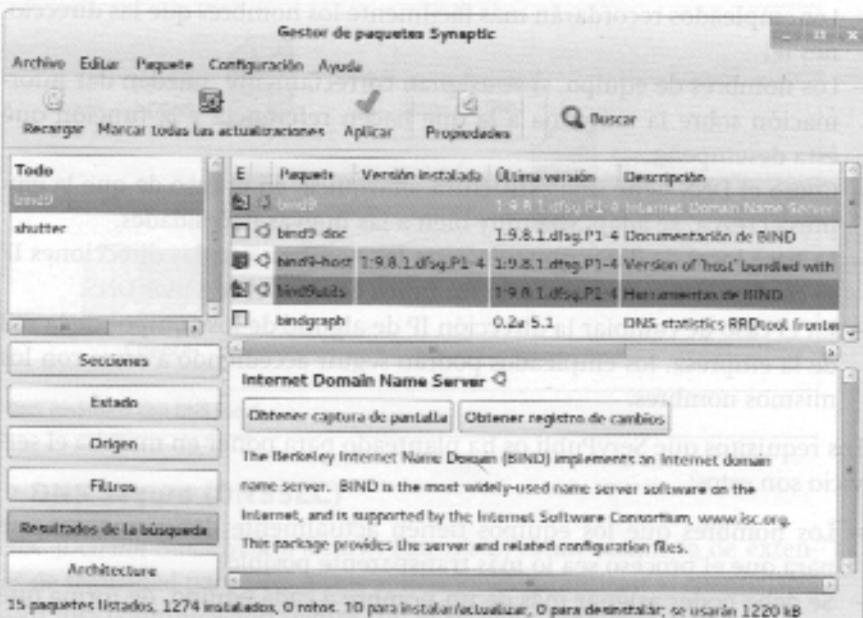


2.13. Herramienta Buscar.

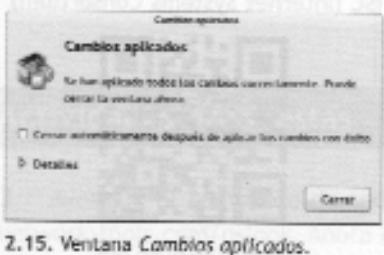
**4.1 > Instalación del servidor**

Para instalar el servidor DNS, debes seguir estos pasos:

1. Abre una sesión gráfica en el servidor.
2. Abre el gestor de paquetes Synaptic.
3. Haz clic en el botón Recargar para actualizar la lista de paquetes disponibles en los repositorios de Internet que tienes configurados. Espera unos segundos mientras termina este proceso.
4. Haz clic sobre el botón Buscar para acceder a la herramienta de búsqueda.
5. Escribe bind9 en el cuadro de texto (figura 2.13) y haz clic en el botón Buscar.
6. Selecciona bind9 haciendo clic sobre el nombre del paquete y lee la información adicional mostrada debajo de la lista de paquetes.
7. Haz doble clic en la casilla de verificación que está delante del nombre del paquete seleccionado (de este modo lo marcas para instalar).
8. Se abrirá un diálogo que advierte que para poder instalar bind9 es necesario marcar otros paquetes. Haz clic en el botón Marcar para permitir estos cambios adicionales.
9. Asegúrate de que la casilla de verificación del paquete bind9 está marcada y haz clic sobre el botón Aplicar para iniciar el proceso de instalación (figura 2.14).



2.14. Selección de paquetes.



2.15. Ventana Cambios aplicados.

10. Se abrirá la ventana Resumen que muestra información sobre la instalación que vas a realizar. Has de analizarla y hacer clic en el botón Aplicar para comenzar la descarga de los paquetes. Durante este proceso se abre la ventana de diálogo Aplicando los cambios, que se cerrará al finalizar la instalación para dar paso a la ventana Cambios aplicados (figura 2.15).
11. Haz clic sobre el botón Cerrar del diálogo Cambios aplicados.
12. Haz clic en el botón Cerrar de la ventana de Synaptic.

## 4.2 > Configuración del servidor

Una vez que el servidor DNS ha sido instalado, es el momento de configurar los siguientes elementos para poder resolver las peticiones de los clientes:

- La relación entre los nombres de los ordenadores de la red de área local y sus correspondientes direcciones.
- La relación entre las direcciones IP de los ordenadores de la red de área local y sus correspondientes nombres.

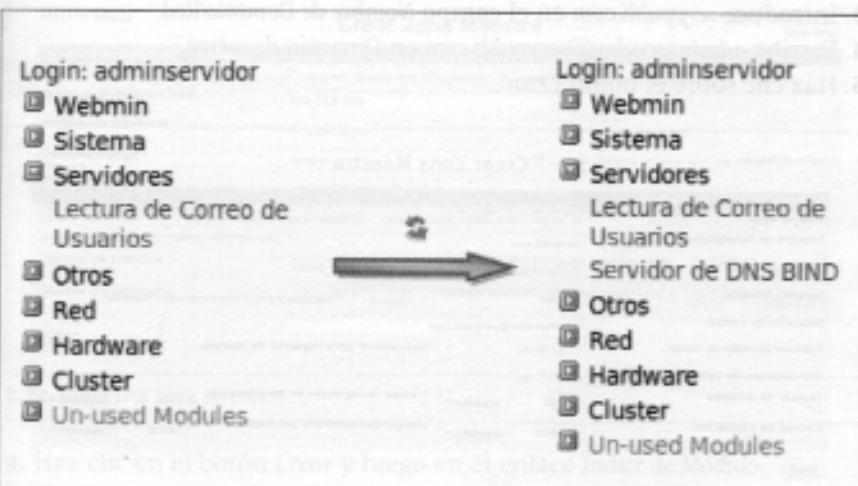
Entonces, ¿no es preciso configurar el servidor DNS para que pueda resolver los nombres y direcciones de Internet? El servidor DNS es capaz de traducir estas direcciones sin necesidad de configurar ningún parámetro adicional. Cuando este servidor recibe una petición de un cliente para resolver un nombre o una dirección externa, propaga la consulta a otros servidores DNS externos.

La información de configuración de la red y del hardware de la empresa ServPubli está detallada en el epígrafe 2.1 de la Unidad 1. Repásala antes de realizar los siguientes ejemplos y actividades.

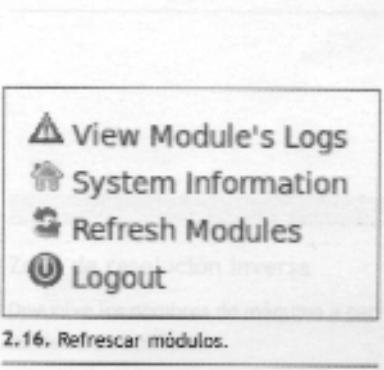
### Acceso al módulo del servidor de DNS BIND

Para actualizar la lista de servidores disponibles desde Webmin, sigue estas indicaciones:

1. Abre el navegador web en el servidor y accede a Webmin.
2. Haz clic sobre el enlace **Servidores** del menú principal de Webmin. Este menú se halla en el lado izquierdo de la ventana.
3. Puedes observar que, aunque acabas de instalar el servidor DNS, este no aparece en la lista de servidores disponibles. Haz clic sobre el enlace **Refresh Modules** (figura 2.16) para que Webmin agregue el servidor DNS en su menú. Espera unos segundos mientras Webmin busca los módulos instalados.
4. Ahora ya se puede ver el enlace **Servidor de DNS BIND** en la sección **Servidores** (figura 2.17).



2.17. Servidores disponibles.



2.16. Refrescar módulos.

Archivos de configuración  
Los archivos de configuración de la red  
192.168.100.100  
http://192.168.100.100/

Archivo de declaración de zonas locales  
`/etc/bind/named.conf.local`

Sistema administrado  
 Conexiones locales

Archivo de configuración de la zona servpubli.com  
`/var/lib/bind/servpubli.com.hosts`

### Creación de una zona maestra de resolución directa

A continuación vas a crear la zona maestra donde se relacionarán los nombres de los equipos de las empresas con sus correspondientes direcciones IP. Para ello sigue estas indicaciones:

1. Abre Webmin y accede al enlace *Servidor de DNS BIND* de la sección *Servidores* de su menú principal.
2. Haz clic sobre el enlace *Crear una nueva zona maestra* de la sección *Zonas DNS Existentes* (figura 2.18).

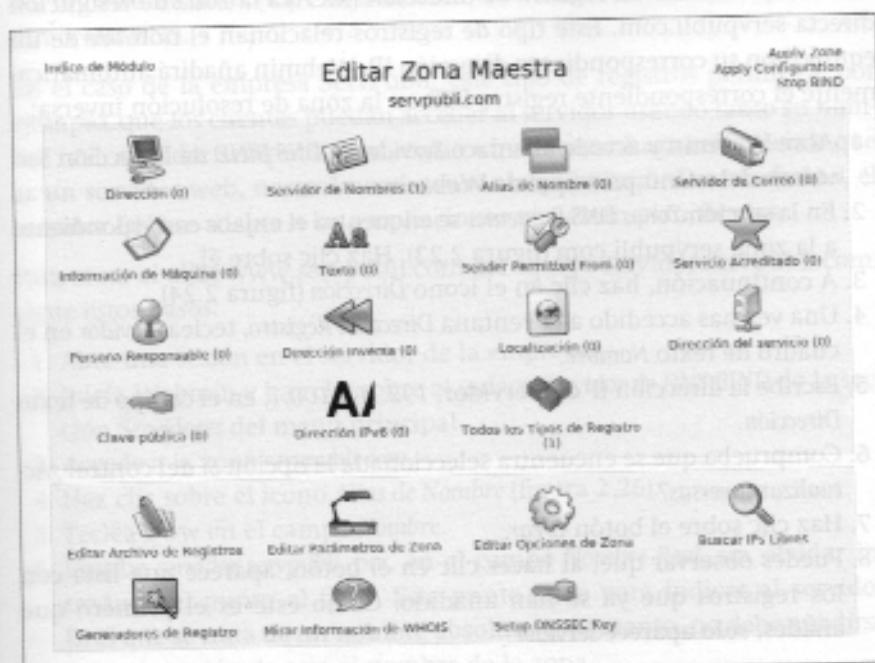


2.18. Módulo del servidor de DNS BIND.

3. Introduce `servpubli.com` en el campo *Nombre de Dominio/Red*.
4. Escribe `adminservidor@servpubli.com` en *Dirección de correo*.
5. Haz clic sobre el botón *Crear*.

2.19. Crear zona maestra.

6. Al crear la zona se abre la ventana Editar Zona Maestra (figura 2.20). Haz clic sobre el enlace Índice de Módulo.



2.20. Editar zona maestra.

7. Haz clic en el enlace *Apply Configuration* para guardar los cambios; este se halla en la esquina superior derecha del índice de módulo (figura 2.21).

#### Creación de una zona maestra de resolución inversa

1. Abre Webmin y accede al enlace Servidor de DNS BIND de la sección Servidores del menú principal.
2. Haz clic en el enlace *Crear una nueva zona maestra*.
3. Introduce los datos tal y como aparecen en la figura 2.22, sin olvidar seleccionar la opción *Inversa* en el control *Tipo de zona*.

2.22. Crear una zona inversa.

4. Haz clic en el botón *Crear* y luego en el enlace *Índice de Módulo*.
5. Por último, haz clic en *Apply Configuration* del índice de módulo para guardar los cambios.

Apply Configuration  
Stop BIND  
Buscar Documentos..

2.21. Aplicar configuración.

#### Zona de resolución inversa

Devuelve los nombres de máquina a partir de su dirección IP.

#### Archivo de configuración

El archivo de configuración de la zona 192.168.100 es:

/var/lib/bind/192.168.100.rev

2.23. Zona servpubli.com.

2.24. Registro de dirección.

### Creación de un registro de dirección

Ahora vas a añadir un registro de dirección (RR A) a la zona de resolución directa servpubli.com. Este tipo de registros relacionan el nombre de un equipo con su correspondiente dirección IP. Webmin añadirá automáticamente el correspondiente registro PTR en la zona de resolución inversa:

1. Abre Webmin y accede al enlace *Servidor de DNS BIND* de la sección *Servidores* del menú principal de Webmin.
2. En la sección *Zonas DNS Existentes* se encuentra el enlace correspondiente a la zona servpubli.com (figura 2.23). Haz clic sobre él.
3. A continuación, haz clic en el ícono Dirección (figura 2.24).
4. Una vez has accedido a la ventana *Dirección Registro*, teclea servidor en el cuadro de texto *Nombre*.
5. Escribe la dirección IP del servidor, 192.168.100.1, en el campo de texto *Dirección*.
6. Comprueba que se encuentra seleccionada la opción *Sí* del control *Actualizar inversa?*
7. Haz clic sobre el botón *Crear*.
8. Puedes observar que, al hacer clic en el botón, aparece una lista con los registros que ya se han añadido. Como este es el primero que añades, solo aparece *servidor*.

2.25. Añadir registros de dirección.

9. Accede al enlace *Índice de Módulo*.
10. Haz clic en *Apply Configuration* del Índice de módulo para guardar los cambios.

## Actividades propuestas

4\*\* Consulta la información de configuración de la red y del hardware de la empresa ServPubli que encontrarás en el epígrafe 2.1 de la Unidad 1 y crea los registros de dirección correspondientes al resto de equipos e impresoras. Ten en cuenta que no hace falta que vuelvas al índice de módulo para aplicar la configuración cada vez que crees un registro, sino que puedes hacerlo de una sola vez cuando hayas introducido todos los registros.

5\*\* Crea un registro de dirección que relacione el nombre mail con la dirección IP 192.168.100.1. No olvides indicar que se actualice la zona de resolución inversa correspondiente.

### Creación de un registro de alias

Un registro de alias (RR CNAME) crea un nombre alternativo para una dirección DNS.

En el caso de la empresa ServPubli, este tipo de registros permitirá, por ejemplo, que los clientes puedan acceder al servidor usando tanto su nombre real, servidor.servpubli.com, como un alias que haga referencia a que es un servidor web, normalmente www.servpubli.com. De esta forma, el servidor DNS se adapta a las ampliaciones que están planificadas.

Para crear el alias www.servpubli.com del equipo servidor.servpubli.com, sigue estos pasos:

1. Abre una sesión en el servidor de la empresa.
2. Inicia Webmin y haz clic sobre el enlace Servidor de DNS BIND de la sección Servidores del menú principal.
3. Accede a la zona servpubli.com.
4. Haz clic sobre el ícono Alias de Nombre (figura 2.26).
5. Teclea www en el campo Nombre.
6. Escribe servidor.servpubli.com. en el campo Nombre Real, sin olvidar introducir el punto al final. Este punto sirve para indicar al servidor DNS que se trata de un nombre absoluto y, por tanto, no debe añadirse a continuación de este el nombre de la zona.
7. Haz clic sobre el botón Crear.
8. Puedes observar que, al hacer clic en el botón, aparece una lista con los registros ya añadidos.

Nombre	TTL	Nombre Real
www	Por defecto	servidor.servpubli.com.

Botones: Crear, Seleccionar todo, Eliminar seleccionados, Registrar a lista de zonas, Mostrar a tipos de registro.

2.27. Añadir registros de alias.

9. Accede al enlace Índice de Módulo para volver al menú principal de Servidor de DNS BIND.
10. Haz clic en Apply Configuration para guardar los cambios.

### Actividades propuestas

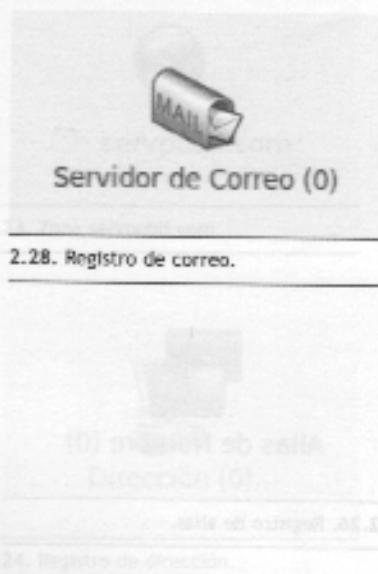
6. Crea los alias de servidor para los siguientes servicios:

a) DNS

b) DHCP

c) FTP

d) Proxy



2.28. Registro de correo.

2.24. Registro de direcciones.

### Creación de un registro de correo

Los registros de correo (RR MX) permiten hacer referencia al servidor de correo mediante un nombre. Sigue estas indicaciones:

1. Abre una sesión en el servidor de la empresa.
2. Inicia Webmin en el navegador web y accede al enlace **Servidor de DNS BIND** de la sección **Servidores** del menú principal.
3. Accede a la zona **servpubli.com**.
4. Haz clic sobre el ícono **Servidor de Correo** (figura 2.28).
5. Una vez has accedido a la ventana **Servidor de Correo Registros** (figura 2.29), teclea **mail** en el cuadro de texto **Nombre**.
6. Escribe el nombre FQDN del servidor de la empresa en el campo de texto **Servidor de correo**, es decir, **servidor.servpubli.com**.
7. Introduce el valor **10** en el campo **Prioridad** para, en el caso de tener más de uno, permitir la selección del servidor de correo a utilizar.
8. Haz clic sobre el botón **Crear**.
9. Puedes observar que, al hacer clic en el botón, aparece una lista con los registros que ya se han añadido.

Nombre	FQDN	Prioridad	Servidor de Correo
mail	servidor.servpubli.com	Por defecto	10

2.29. Añadir registros de correo.

10. Accede al enlace **Índice de Módulo**.

11. Haz clic en **Apply Configuration** del Índice de módulo para guardar los cambios.

### Arranque del servicio

Desde la instalación y durante todo el proceso de configuración, el servidor DNS ha estado activo y actualizado cada vez que has aplicado los cambios de configuración.

Si alguna vez necesitas parar el servicio sin detener todo el sistema, puedes hacerlo desde el enlace **Stop BIND** que aparece en la parte superior derecha de cualquiera de las ventanas de configuración del módulo **Servidor de DNS BIND**.

Para volver a lanzar este servicio solo tienes que hacer clic sobre el enlace **Start BIND** que ha sustituido al enlace de parada del servidor.

### Actividades propuestas

4. Consulta la información de los registros.

### 4.3 > Configuración del cliente

Vas a cambiar la configuración de los clientes para que realicen las consultas al servidor DNS local, de modo que serán capaces de resolver tanto los nombres y direcciones locales como los de Internet.

#### Configuración del cliente

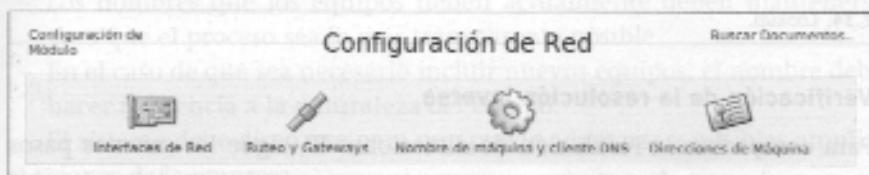
Sigue estos pasos para configurar el DNS de un cliente:

1. Arranca el cliente y accede con el usuario admincliente.
2. Haz clic en el Menú de red y elige la opción Editar las conexiones.
3. Accede a la pestaña Cableada, elige Conexión cableada 1 y haz clic en el botón Editar.
4. Selecciona la pestaña Ajustes de IPv4 y deja los valores como aparecen en la figura 2.30.
5. Haz clic sobre el botón Guardar y después en Cerrar.

#### Configuración del servidor como cliente DNS

Para que el equipo servidor sea capaz de resolver los nombres de la red de la empresa, debe configurarse a sí mismo como su servidor DNS. Como no puedes cambiar la información de configuración de red que recibe el servidor de ServPubli por medio de su servidor DHCP, vas a configurar manualmente su tarjeta de red externa y otros parámetros con la misma información que ofrece el servidor DHCP:

1. Abre la aplicación Webmin en el servidor.
2. Accede al módulo Configuración de red de la sección Red del menú.
3. Haz clic sobre el enlace Nombre de máquina y cliente DNS.
4. Añade 0.0.0.0 en el primer lugar de la lista Servidores DNS.
5. Haz clic sobre el botón Salvar para guardar los cambios.
6. Ahora haz clic sobre el enlace Router y Gateways.
7. Elige la opción Gateway del control Router por defecto y escribe la dirección IP del router por defecto por el que estás saliendo ahora. Si no la conoces, puedes consultar la pestaña Active configuration.
8. Haz clic sobre el botón Salvar para guardar los cambios.
9. Accede ahora al enlace Interfaces de red.
10. Haz clic sobre el nombre de la interfaz externa del router, eth0.
11. Activa la opción Static configuration de la sección IPv4 address.
12. Teclea la dirección en el campo Dirección IP. Si no la conoces, consulta la pestaña Interfaces activas ahora de Interfaces de red.
13. Escribe la máscara en el campo Máscara de Red. Si no la conoces, consulta la pestaña Interfaces activas ahora de Interfaces de red.
14. Para terminar, haz clic en el botón Salvar y Aplicar.



2.31. Configuración de red.

#### Datos de acceso

Usuario: admincliente

Contraseña: Cli3nt09

#### Edición de conexión cableada 1

Nombre de la conexión		Cableada cableada 1	
<input type="checkbox"/> Conectar automáticamente			
Cableada	Seguridad RDP 1a	Ajustes de IPv4 Ajustes de IPv6	
dirección	Método	Manual	
Dirección	Máscara de red	Puerta de enlace	Adelante
192.168.100.116	255.255.255.0	192.168.100.1	Manejar...
Servidores DNS:	192.168.100.1, 0.0.0.0		
Dominios de bloqueo:			
IP del cliente DHCP:			
<input checked="" type="checkbox"/> Requiere dirección IPv4 para que esta conexión se complete			Manejar...
<input checked="" type="checkbox"/> Disponible para todos los usuarios			
		<input type="button" value="Cancelar"/>	<input type="button" value="Guardar..."/>

2.30. Edición de la conexión de red.

#### Archivo de configuración del cliente DNS

/etc/resolv.conf

#### Resolver en Linux

En los sistemas GNU/Linux existe un conjunto de procesos, conocido por el término en inglés resolver, que se encarga de hacer las peticiones al servidor DNS.

Resolver forma parte del sistema, por lo que no hace falta instalarlo.

## Proceso del servidor DNS

/usr/sbin/named

## 4.4 > Comprobaciones

Las comprobaciones del DNS se realizan en el cliente y en el servidor.

### Verificación del estado del servicio

Sigue estos pasos para asegurarte de que se está ejecutando el servidor:

1. Abre Webmin en el navegador web del servidor.
2. Despliega el menú Otras y haz clic sobre el enlace Estado de Sistema y de Servidor.
3. Localiza el servicio BIND DNS Server y comprueba que, a su derecha, hay un símbolo de color verde que indica que funciona correctamente.

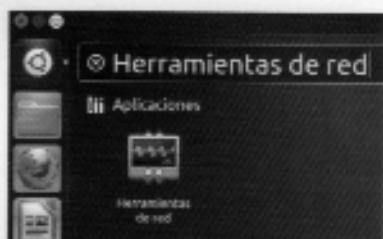
Monitoreando	En host	Estado	Monitoreando	En host	Estado
<input type="checkbox"/> DHCP Server	Local		<input type="checkbox"/> PostgreSQL Database Server	Local	
<input type="checkbox"/> Internet and RPC Server	Local		<input type="checkbox"/> MySQL Database Server	Local	
<input type="checkbox"/> Postfix Server	Local		<input type="checkbox"/> Apache Webserver	Local	
<input type="checkbox"/> NPS Server	Local		<input type="checkbox"/> Squid Proxy Server	Local	
<input type="checkbox"/> Extended Internet Server	Local		<input type="checkbox"/> QMail Server	Local	
<input type="checkbox"/> BIND DNS Server	Local		<input type="checkbox"/> Samba Servers	Local	
<input type="checkbox"/> Sendmail Server	Local				

2.32. Estado del sistema y del servidor.

### Verificación de la resolución directa

Para comprobar la resolución de nombres, sigue estas indicaciones:

1. Arranca el cliente y abre una sesión con el usuario administrante.
2. Haz clic sobre el botón Inicio y teclea Herramientas de red (figura 2.33). Luego pulsa la tecla <Intro>.
3. En la ventana que aparece, selecciona la pestaña Lookup (figura 2.34).
4. Escribe servidor.servpubli.com en el cuadro Dirección de red.
5. Haz clic en el botón Lookup y comprueba la dirección IP.



2.33. Ejecutar herramientas de red.

Nombre	TTL	Tipo de dirección	Tipo de registro	Dirección
servidor.servpubli.com.	38400	IN	A	192.168.100.1
servpubli.com.	38400	IN	NS	servidor.

2.34. Lookup.

### Verificación de la resolución inversa

Para comprobar la resolución de direcciones IP, sigue los mismos pasos que en el apartado anterior, con una excepción: esta vez debes escribir 192.168.100.1 en el cuadro Dirección de red.

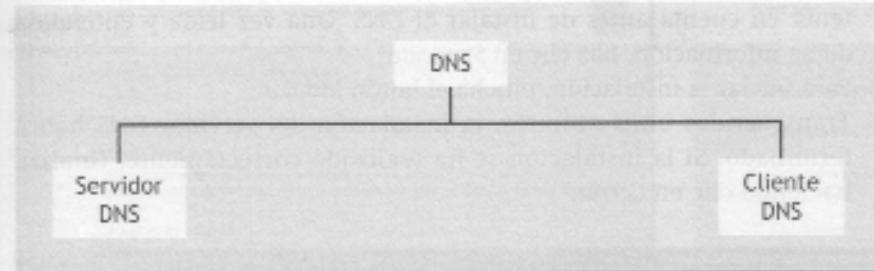
## 5 >> DNS en sistemas Windows

Según la propuesta de trabajo pactada con la empresa ConRecuerdos.org, la primera tarea que debéis realizar es la implantación de un servicio de resolución de nombres.

La empresa os ha dicho que sus trabajadores tienen dificultades cuando desean acceder desde sus puestos de trabajo a los distintos equipos de la red interna mediante direcciones IP. Los empleados utilizan los ordenadores con un nivel de usuario y tanto memorizar las direcciones como relacionarlas con los servicios que ofrecen los equipos a los que quieren acceder no les resultan tareas fáciles ni cómodas.

Después de estudiar la red, el trabajo que desarrollan los empleados y la perspectiva de crecimiento, proponéis a la empresa que, además de usar el servicio DNS para acceder a Internet, también se utilice para acceder a la red de área local. Para defender esta propuesta, presentáis los siguientes argumentos:

- El empleado recuerda mejor un nombre de equipo que su dirección IP.
- La administración de la base de datos que relaciona los nombres de equipo con sus correspondientes IP se lleva a cabo de manera centralizada.
- Como el DNS tiene una estructura jerárquica, en el caso de que la empresa crezca, se adaptaría muy bien a las nuevas necesidades.
- Cuando se cambie la IP de algún equipo en la red de la empresa, los empleados seguirán accediendo a este con el mismo nombre.
- El servidor DNS ya viene incluido, de manera predeterminada, en Windows Server 2008. El servicio en Windows cumple los estándares especificados en el conjunto de RFC aprobadas y publicadas por el Internet Engineering Task Force (IETF) y otros grupos de trabajo.



2.35. Infraestructura DNS en Windows Server 2008.

Antes de empezar a trabajar con el servidor DNS debéis estudiar los requisitos y la información que os ha proporcionado ConRecuerdos.org:

- Los nombres que los equipos tienen actualmente deben mantenerse para que el proceso sea lo más transparente posible.
- En el caso de que sea necesario incluir nuevos equipos, el nombre debe hacer referencia a la naturaleza del equipo.
- El sistema debe diseñarse para que pueda adaptarse a posibles ampliaciones de la empresa.
- Se usará el dominio conrecuerdos.org del que ya dispone la empresa.

### Para saber más

Puedes obtener soporte técnico de Microsoft para el servicio DNS en la siguiente URL:



[http://xurl.es/dns\\_ms](http://xurl.es/dns_ms)

### Recuerda

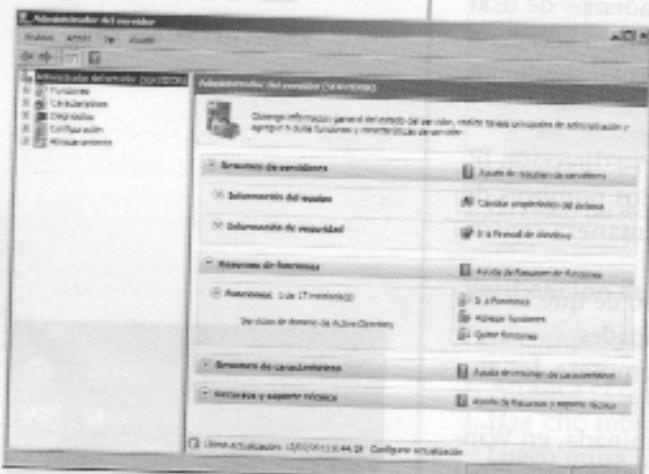
Los datos para acceder como usuario administrador son:

- Usuario: adminservidor
- Contraseña: S3rvidor

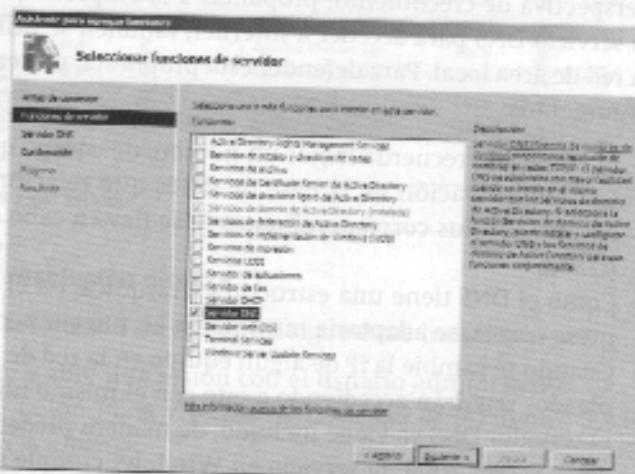
## 5.1 > Instalación del servidor

Para instalar el servidor DNS, sigue estas indicaciones:

1. Haz clic en el botón **Inicio** y selecciona la opción **Administrador del servidor**. En la nueva ventana que aparece (figura 2.36), pincha la opción **Agregar funciones**, que se encuentra en el bloque **Resumen de funciones** de la parte derecha de la ventana.
2. A continuación aparece el *Asistente para agregar funciones*. La primera ventana informa sobre las comprobaciones previas que debes realizar para instalar correctamente cualquier tarea en el servidor. Léelas atentamente y haz clic sobre el botón **Siguiente**.
3. En la ventana **Seleccionar funciones de servidor** (figura 2.37), marca la casilla de verificación **Servidor DNS** y pincha **Siguiente**.

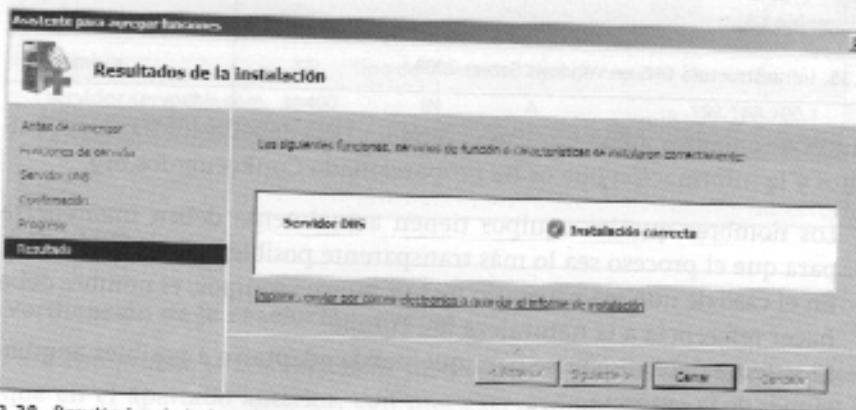


2.36. Ventana Administrador del servidor.



2.37. Seleccionar funciones de servidor.

4. La ventana **Servidor DNS** comenta algunas características que se deben tener en cuenta antes de instalar el DNS. Una vez leída y entendida dicha información, haz clic en **Siguiente**.
5. Para iniciar la instalación, pincha el botón **Instalar**.
6. Transcurridos unos minutos, la instalación del servidor DNS habrá terminado. Si la instalación se ha realizado correctamente, finaliza haciendo clic en **Cerrar**.



2.38. Resultados de la instalación.

### Editor del registro

La información del servicio DNS en el editor del registro se encuentra en la siguiente clave:

HKEY\_LOCAL\_MACHINE\System  
CurrentControlSet\Services\DNS

## 5.2 > Configuración del servidor

### Creación de una zona de búsqueda directa

La zona de búsqueda directa sirve para relacionar los nombres de los equipos con sus direcciones IP. En el caso de que el servidor se encuentre en un dominio de Active Directory, este tipo de zona se crea automáticamente al realizar la instalación del servicio DNS.

### Creación de una zona de búsqueda inversa

Vas a configurar una zona inversa, que se utiliza para traducir direcciones IP a nombres. Para ello sigue estos pasos:

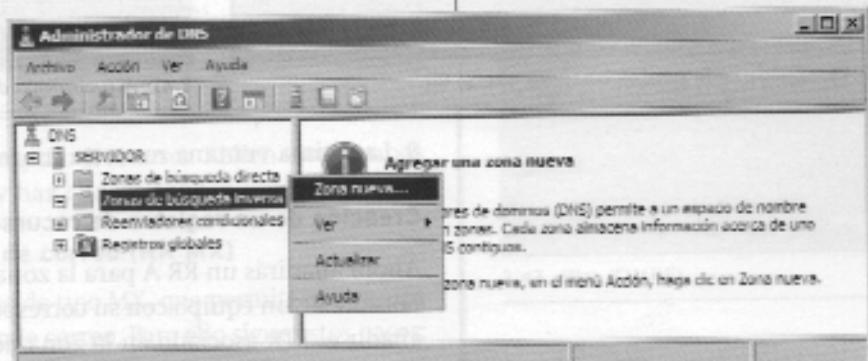
1. Abre la ventana *Administrador de DNS*.
2. Haz clic con el botón secundario del ratón en la opción *Zonas de búsqueda inversa* que se encuentra en *DNS / SERVIDOR*. En el menú contextual que aparece, selecciona *Zona nueva* (figura 2.39).
3. Se inicia entonces el Asistente para crear zona nueva. Haz clic en *Siguiente*. En la ventana *Tipo de zona* (figura 2.40), selecciona la opción *Zona principal* y pincha *Siguiente*.
4. En la ventana *Ámbito de replicación de zona de Active Directory* (figura 2.41), elige la opción *Para todos los servidores DNS en este dominio: ConRecuerdos.org* y haz clic en *Siguiente*.

**CONSEJO** Algunas organizaciones utilizan el nombre de su dominio para nombrar las zonas inversas. Por ejemplo, si tu dominio es *ConRecuerdos.org*, podrías nombrar la zona inversa *192.168.100.in-addr.arpa*.

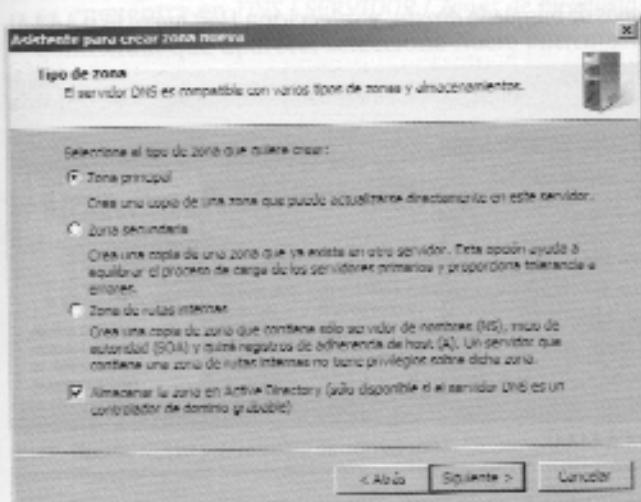
### Administrador de DNS

Una vez instalado el servicio DNS, puedes administrarlo yendo a la ruta:

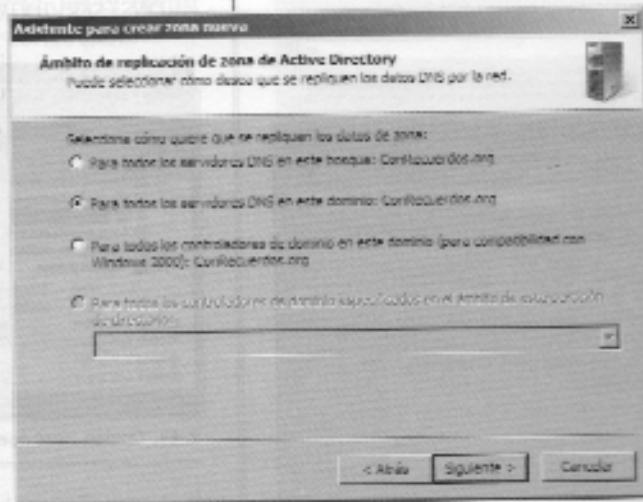
**Inicio / Herramientas administrativas / DNS**



2.39. Opción Zona nueva...



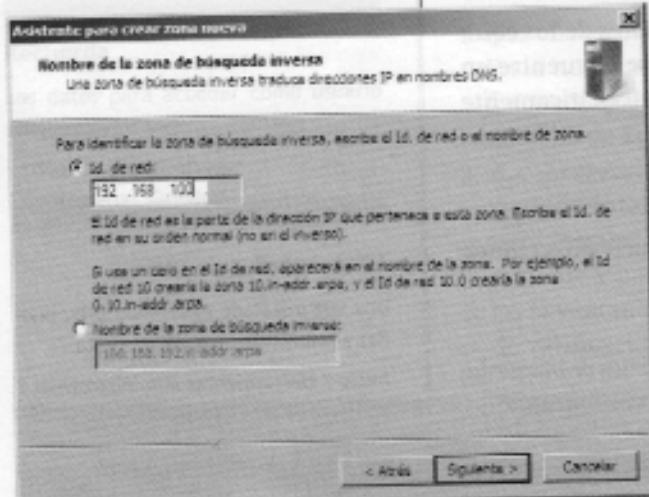
2.40. Ventana Tipo de zona.



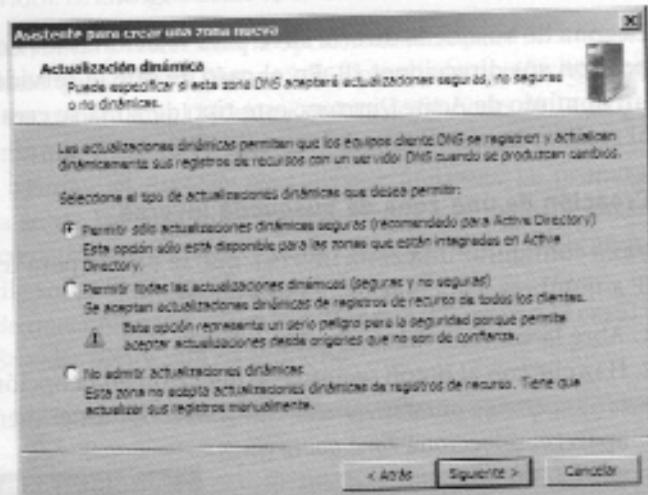
2.41. Ventana Ámbito de replicación.

5. En la ventana *NOMBRE de la zona de búsqueda inversa*, deja seleccionada la opción *Zona de búsqueda inversa para IPv4*. A continuación, haz clic sobre el botón *Siguiente*.
6. Escribe el *Id. de red* (figura 2.42), es decir 192.168.100, y haz clic en *Siguiente*.

7. En la ventana **Actualización dinámica** (figura 2.43) deja seleccionado Permitir solo actualizaciones dinámicas seguras y haz clic en **Siguiente >**.



2.42. Nombre de la zona de búsqueda inversa (II).



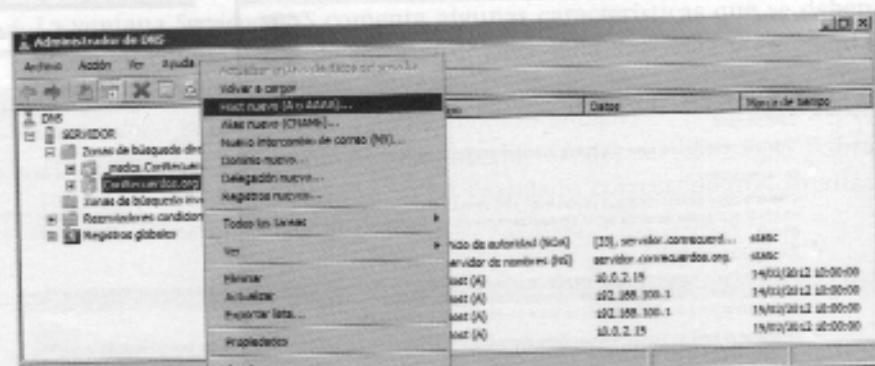
2.43. Actualización dinámica.

8. La última ventana muestra un resumen. Haz clic en el botón **Finalizar**.

### Creación de un registro de recurso de dirección (RR A)

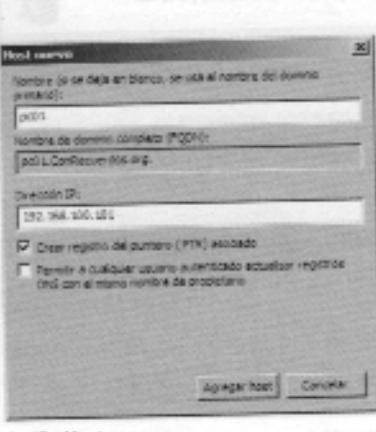
Ahora añadirás un RR A para la zona de búsqueda directa, que relaciona el nombre de un equipo con su correspondiente dirección IP. También puedes añadir el PTR asociado en la zona de búsqueda inversa. Sigue estos pasos:

1. Abre el Administrador de DNS.
2. Haz clic con el botón secundario en la zona **ConRecuerdos.org** situada en **DNS / SERVIDOR / Zonas de búsqueda directa**, y selecciona **Host nuevo (A o AAAA)**.



2.44. Opción Host nuevo (A o AAAA).

3. A continuación aparece el cuadro de diálogo **Host nuevo**. Rellena los campos como se muestra en la figura 2.45 y haz clic en **Agregar host**.



2.45. Host nuevo.

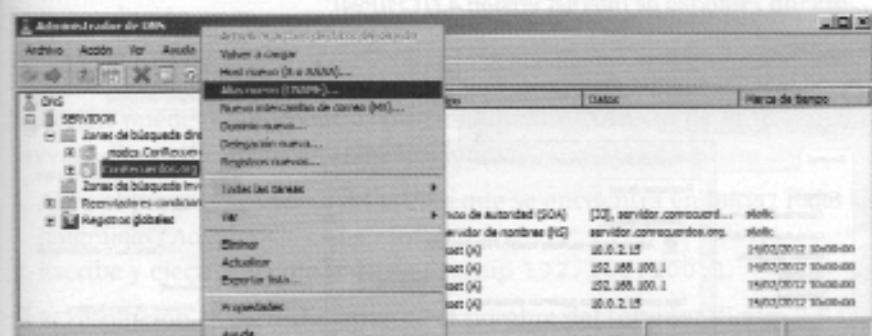
## Actividades propuestas

7. Crea los RR A correspondientes al resto de equipos e impresoras, según se indica en la Unidad 1.

## Creación de un registro de recurso de alias (RR CNAME)

Vas a añadir un alias nuevo para la zona directa siguiendo estos pasos:

1. Abre el Administrador de DNS.
2. Pincha el botón secundario en la zona *ConRecuerdos.org*, que se encuentra en *DNS / SERVIDOR / Zonas de búsqueda directa*. En la ventana de contexto que aparece, selecciona *Alias nuevo (CNAME)*.



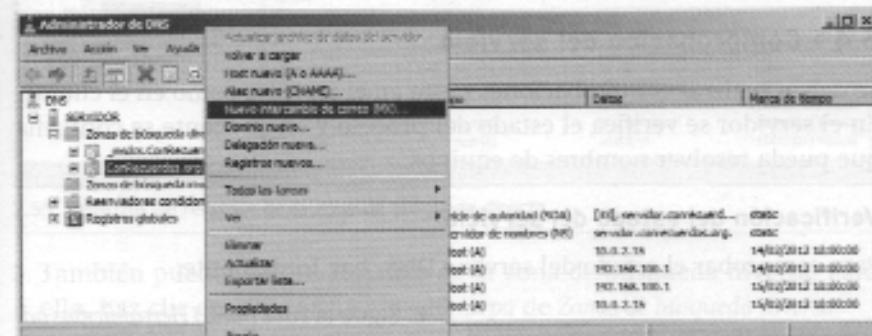
2.46. Opción *Alias nuevo (CNAME)*...

3. Aparece el cuadro de diálogo *Nuevo registro de recursos*. Rellena los campos como se muestra en la figura 2.47 y haz clic en *Aceptar*.

## Creación de un registro de recurso de correo (RR MX)

Ahora vas a añadir el registro de recurso de tipo MX, que permite utilizar un nombre que haga referencia al servidor de correo. Para ello sigue estos pasos:

1. Abre el Administrador de DNS.
2. Haz clic con el botón derecho del ratón en la zona *ConRecuerdos.org* que se encuentra en *DNS / SERVIDOR / Zonas de búsqueda directa*. En el menú contextual que aparece, selecciona *Nuevo intercambio de correo (MX)*.



2.48. Opción *Nuevo intercambio de correo (MX)*.

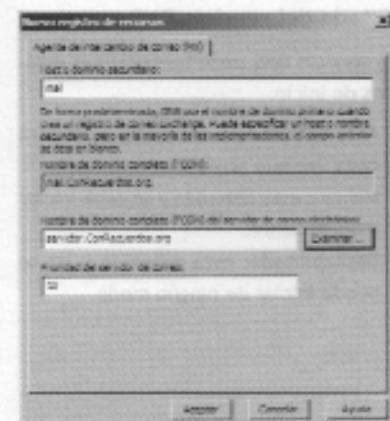
3. Aparece el cuadro de diálogo *Nuevo registro de recursos*. Rellena los campos como se muestra en la figura 2.49 y haz clic en *Aceptar*.

## Consejo

Si ya tienes abierto el administrador de DNS, puedes crear los otros tipos de registros de recursos (CNAME y MX) con un clic del botón secundario sobre la zona de búsqueda directa.



2.47. Alias (CNAME).



2.49. Agente de intercambio de correo (MX).

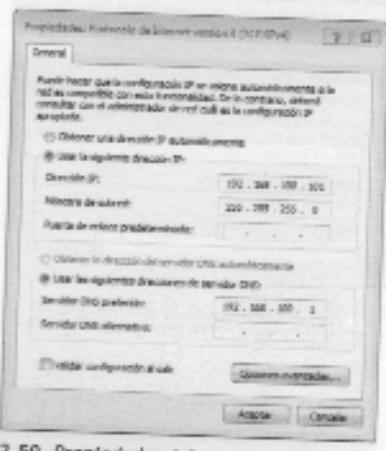
## Actividades propuestas

8. Crea un RR CNAME para los servicios DNS, DHCP, FTP y Proxy.

**Datos de acceso**

Usuario: admincliente

Contraseña: Cl3nt3@

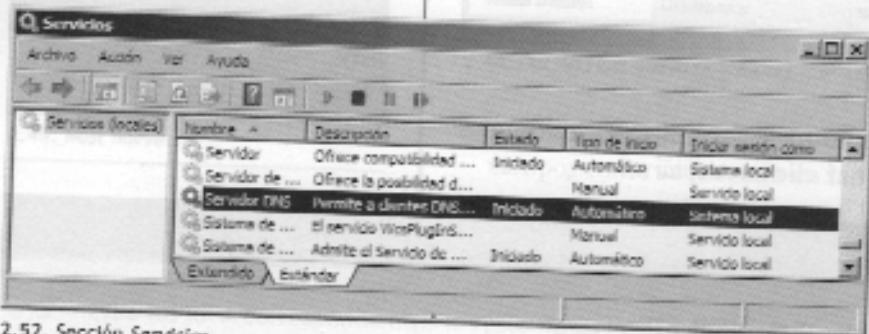


2.50. Propiedades del protocolo TCP/IPv4.

**Estado del servicio DNS**

El servicio DNS tiene tres posibles estados de inicio:

- Automático: está iniciado y se iniciará cada vez que arranca el ordenador.
- Manual: está detenido y se debe iniciar manualmente.
- Deshabilitado: está detenido y no se puede iniciar de ningún modo.

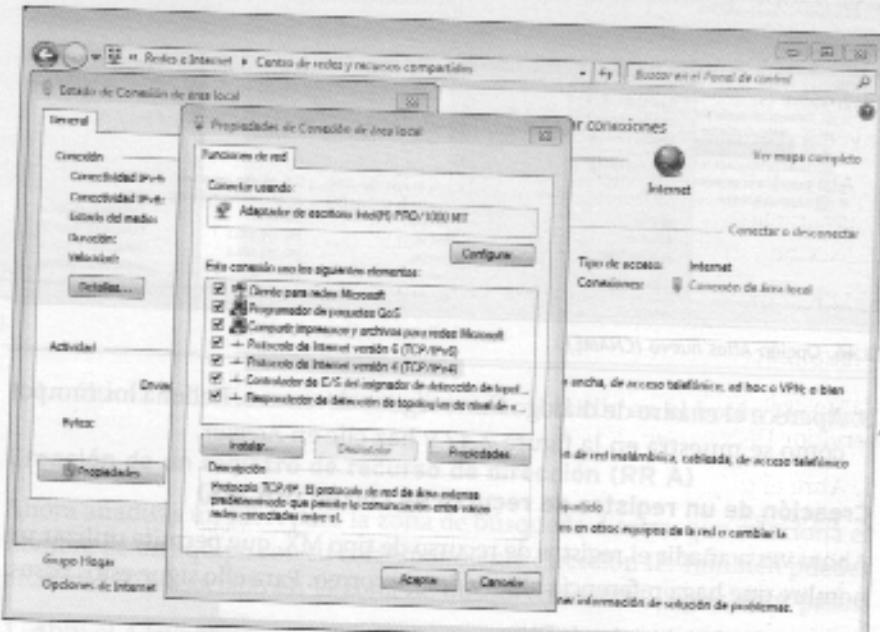


2.52. Sección Servicios.

**5.3 > Configuración del cliente**

Para configurar el servicio DNS en el cliente debes seguir estos pasos:

1. Ve a **Inicio / Panel de control / Redes e Internet / Centro de redes y recursos compartidos** y haz clic en **Conexión de área local**.
2. Pincha el botón **Propiedades**.
3. En la ventana **Propiedades de Conexión de área local** haz doble clic sobre la opción **Protocolo de Internet versión 4 (TCP/IPv4)**.



2.51. Ruta de Propiedades de Conexión de área local.

4. Ahora indica la IP del servidor DNS en el cuadro de texto **Servidor DNS preferido** (figura 2.50), es decir, escribe la dirección 192.168.100.1.

**5.4 > Comprobación del servicio**

Se deben realizar comprobaciones tanto en el servidor como en el cliente. En el servidor se verifica el estado del proceso y en el cliente se confirma que pueda resolver nombres de equipos.

**Verificación del estado del servicio**

Para comprobar el estado del servicio DNS, haz lo siguiente:

1. Sigue la ruta **Inicio / Herramientas administrativas** y haz clic en **Servicios**.
2. En la ventana que aparece (figura 2.52), busca el servicio **Servidor DNS**. Una vez encontrado, si el campo **Estatus** tiene el valor **Iniciado** y en **Tipo de inicio** aparece **Automático**, significa que el servicio DNS está en funcionamiento y que se iniciará automáticamente cada vez que arranque el equipo servidor.

### Verificación de la resolución directa

Para comprobar si la resolución directa de los equipos que se encuentran en la zona del servidor DNS funciona correctamente, sigue estas indicaciones:

1. Abre el programa Símbolo del sistema, que se encuentra en Inicio / Todos los programas / Accesorios.
2. Escribe y ejecuta el comando nslookup servidor.conrecuerdos.org.

Si la resolución es correcta, aparecen las dos IP del servidor (figura 2.53).

### Verificación de la resolución inversa

También puedes comprobar el funcionamiento correcto de la resolución inversa. Para ello, sigue estas indicaciones:

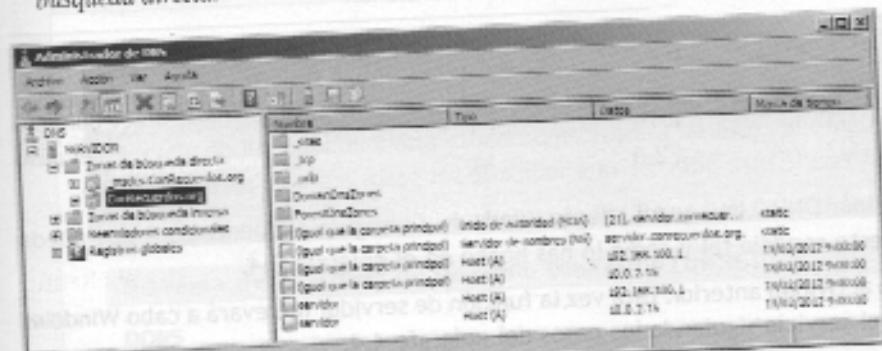
1. Abre el programa Símbolo del sistema que se encuentra en Inicio / Todos los programas / Accesorios.
2. Escribe y ejecuta el comando nslookup 192.168.100.1.

Si la resolución es correcta, aparece el nombre del servidor (figura 2.54).

### Visualización de los registros

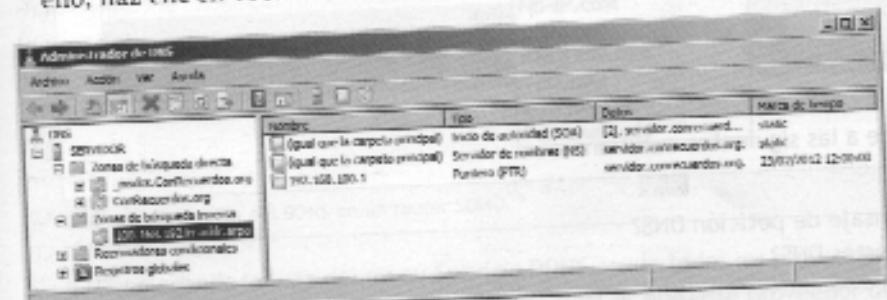
Para ver la lista con todos los registros de recursos creados en las zonas del servidor DNS, sigue estas indicaciones:

1. Abre el servicio DNS.
2. Si deseas ver los registros de la zona de búsqueda directa, haz clic en la opción ConRecuerdos.org, que se encuentra en DNS / SERVIDOR / Zonas de búsqueda directa.



2.55. Registros de recursos de la zona de búsqueda directa.

3. También puedes ver los registros de la zona de búsqueda inversa. Para ello, haz clic en 100.168.192.in-addr.arpa de Zonas de búsqueda inversa.



2.56. Registros de recursos de la zona de búsqueda inversa.

```
C:\Windows\system32\cmd.exe
C:\>nslookup servidor.conrecuerdos.org
Servidor: 192.168.100.1
Nombre: servidor.conrecuerdos.org
Dirección: 192.168.100.1
192.168.100.1
```

2.53. nslookup por nombre.

```
C:\Windows\system32\cmd.exe
C:\>nslookup 192.168.100.1
Servidor: servidor.conrecuerdos.org
Address: 192.168.100.1
Nombre: servidor.conrecuerdos.org
Dirección: 192.168.100.1
```

2.54. nslookup por IP.