UD 2

DOMAIN NAME SYSTEM

[1 Definición 2](#_Toc21296603)

[1.1 Nombres del ordenador 2](#_Toc21296604)

[1.2 Introducción al Sistema de Nombres de Dominio 2](#_Toc21296605)

[1.3 Espacio de nombre 2](#_Toc21296606)

[1.4 Delegación 3](#_Toc21296607)

[1.5 Servidores de nombres de dominio 4](#_Toc21296608)

[1.6 Resolución de nombres de dominio 4](#_Toc21296609)

[1.7 Tipos de zonas 5](#_Toc21296610)

[1.8 Dominios de nivel superior 5](#_Toc21296611)

[2 Tipos de DNS 6](#_Toc21296612)

[2.1 Servidor DNS maestro 6](#_Toc21296613)

[2.2 Servidor DNS esclavo 7](#_Toc21296614)

[2.3 Servidor caché DNS 7](#_Toc21296615)

[3 Tipos de registros 8](#_Toc21296616)

[4 Servidor DNS en Linux 9](#_Toc21296617)

[4.1 Instalación 9](#_Toc21296618)

[4.2 Configuración 9](#_Toc21296619)

[4.3 Comprobación de la configuración 11](#_Toc21296620)

[4.4 Puesta en marcha del servicio 11](#_Toc21296621)

[4.5 Comprobando el servidor de nombres DNS 11](#_Toc21296622)

[5 Servidor DNS en Windows 2012 Server 12](#_Toc21296623)

[5.1 Instalación 12](#_Toc21296624)

[5.2 Configuración 15](#_Toc21296625)

[5.3 Testeando el servidor 21](#_Toc21296626)

# Definición

Cada equipo conectado directamente a Internet tiene al menos una dirección IP específica. Sin embargo, los usuarios no desean trabajar con direcciones numéricas, como por ejemplo 198.105.232.4, sino con un nombre de dominio o más específicamente, con direcciones (llamadas direcciones FQDN) como por ejemplo www.example.com.

Es posible asociar nombres en lenguaje normal con direcciones numéricas gracias a un sistema llamado DNS (**Sistema de Nombres de Dominio**, *Domain Name System*).

Esta correlación entre las direcciones IP y el nombre de dominio asociado se llama **resolución de nombres de dominio** (o **resolución de direcciones**).

## Nombres del ordenador

Al comienzo de TCP/IP, puesto que las redes no eran muy extensas, o en otras palabras que el número de equipos conectados a la misma red era bajo, los administradores de red crearon archivos llamados tablas de conversión manual. Estas tablas de conversión manual eran archivos secuenciales, por lo general llamados *hosts* o *hosts.txt*, y asociaban en cada línea la dirección IP del equipo con el nombre literal relacionado, denominado nombre del ordenador.

En Linux existe el archivo */etc/hosts* y en Windows podemos encontrar el archivo *C:/Windows/system32/drivers/etc/hosts.txt*.

## Introducción al Sistema de Nombres de Dominio

Sin embargo, el anterior sistema de tablas de conversión exigía una actualización manual de las tablas para la totalidad de los equipos en caso de incluir o modificar el nombre de una máquina. Por lo tanto, con el aumento en tamaño de las redes y sus interconexiones, fue necesario implementar un sistema de gestión para los nombres que fuese jerárquico y fácil de administrar. El sistema llamado Sistema de Nombres de Dominio (DNS) fue desarrollado en noviembre de 1983 por Paul Mockapetris (RFC 882 y RFC 883) y luego revisado en 1987 en las RFC 1034 y 1035. El DNS ha sido sometido a varias RFC.

Este sistema ofrece:

* Un **espacio de nombre** jerárquico que permite garantizar la singularidad de un nombre en una estructura arbórea, como por ejemplo sistemas de archivo Unix.
* Un sistema de **servidores de distribución** que permite que el espacio de nombre esté disponible.
* Un sistema de **cliente** que permite "resolver" nombres de dominio, es decir, interrogar a los servidores para encontrar la dirección IP que corresponde a un nombre.

## Espacio de nombre

La estructura del sistema DNS se basa en una estructura de arbórea en donde se definen los dominios de nivel superior (llamados **TLD**, Dominios de Nivel Superior, *Top-Level Domain*); esta estructura está conectada a un nodo raíz representado por un punto.

.

com

net

es

…

google

eu

yahoo

edu

fr

it

ftp

linux

home

www

terra

sc01

ehu

www

profesor

RAÍZ

TLD

DOMINIO

*HOST*

FQDN

Cada nodo del árbol se llama nombre de dominio y tiene una etiqueta con una longitud máxima de 63 caracteres.

Por lo tanto, todos los nombres de dominio conforman una estructura arbórea inversa en donde cada nodo está separado del siguiente nodo por un punto (".").

El extremo de la bifurcación se denomina ***host***, y corresponde a un equipo o entidad en la red. El nombre del ordenador que se provee debe ser único en el dominio respectivo, o de ser necesario, en el sub-dominio. Por ejemplo, el dominio del servidor Web por lo general lleva el nombre www.

La palabra "dominio" corresponde formalmente al sufijo de un nombre de dominio, es decir, la recopilación de las etiquetas de nodo de la estructura arbórea, con excepción del ordenador.

El nombre absoluto está relacionado con todas las etiquetas de nodo de una estructura arbórea, separadas por puntos y que termina con un punto final que se denomina la **dirección FQDN** (Nombre de Dominio totalmente calificado, *Fully Qualified Domain Name*). La profundidad máxima de una estructura arbórea es 127 niveles y la longitud máxima para un nombre FQDN es 255 caracteres. La dirección FQDN permite ubicar de manera única un equipo en la red de redes. Por lo tanto, es.kioskea.net. es una dirección FQDN.

## Delegación

Es importante resaltar que el objetivo principal del diseño del sistema de nombres de dominio fue su administración descentralizada. Este objetivo se consigue a través de la ***delegación***. La delegación de dominios funciona de forma parecida a la delegación de tareas en una organización. Un responsable de proyecto divide el proyecto en pequeñas tareas y asigna (delega) la responsabilidad de las mismas a diferentes empleados.

De la misma forma, una organización que administra un dominio puede dividirla en subdominios. Cada subdominio puede ser delegado a diferentes organizaciones, lo cual implica que esa organización será responsable de mantener los datos (registros de recursos) de ese subdominio. Esa organización puede libremente cambiar los datos e incluso volver a dividir el dominio delegado en subdominios y delegarlos. El dominio padre solamente contiene enlaces a los responsables del subdominio delegado, de forma que pueda hacer referencia a ellos cuando se le planteen consultas sobre nombres en dicho subdominio delegado.

Realmente, la subdivisión de un dominio en subdominios y la delegación de dichos subdominios son cosas distintas. En primer lugar, un dominio que tenga capacidad de autogestión (autoridad), siempre puede decidir subdividirse en diferentes subdominios, manteniendo él en principio la autoridad sobre todos ellos. Posteriormente, la organización que gestiona el dominio puede decidir además delegar la autoridad de algunos (o todos) sus subdominios en otras organizaciones. La delegación es una acción que siempre decide el dominio padre, y éste puede revocarla cuando desee, volviendo a retomar la autoridad sobre el subdominio que había delegado.

## Servidores de nombres de dominio

Los equipos llamados servidores de nombres de dominio permiten establecer la relación entre los nombres de dominio y las direcciones IP de los equipos de una red.

Cada dominio cuenta con un servidor de nombre de dominio, llamado servidor de nombre de dominio principal, así como también un servidor de nombre de dominio secundario, que puede encargarse del servidor de nombre de dominio principal en caso de falta de disponibilidad.

Cada servidor de nombre de dominio está especificado en el servidor de nombre de dominio en el nivel superior inmediato, lo que significa que la autoridad sobre los dominios puede delegarse implícitamente. El sistema de nombre es una arquitectura distribuida, en donde cada entidad es responsable de la administración de su nombre de dominio. Por lo tanto, no existe organización alguna que sea responsable de la administración de todos los nombres de dominio.

Los servidores relacionados con los dominios de nivel superior (TLD) se llaman "**servidores de dominio de nivel superior**". Son 13, están distribuidos por todo el mundo y sus nombres van desde "a.root-servers.net" hasta "m.root-servers.net".

El servidor de nombre de dominio define una zona, es decir, una recopilación de dominios sobre la cual tiene autoridad. Si bien el sistema de nombres de dominio es transparente para el usuario, se deben tener en cuenta los siguientes puntos:

* Cada equipo debe configurarse con la dirección de un equipo que sea capaz de transformar cualquier nombre en una dirección IP. Este equipo se llama Servidor de nombres de dominio. No se alarme: cuando se conecta a Internet, el proveedor de servicios automáticamente modificará los parámetros de su red para hacer que estos servidores de nombres de dominio estén disponibles.
* También debe definirse la dirección IP de un segundo Servidor de nombres de dominio (Servidor de nombres de dominio secundario): el servidor de nombres de dominio secundario puede encargarse del servidor de nombres de dominio principal en caso de fallas en el sistema.

El servidor que se utiliza con más frecuencia se llama BIND (*Berkeley Internet Name Domain*). Es un software gratuito para sistemas UNIX, fue desarrollado inicialmente por la Universidad de Berkeley en California y en la actualidad está mantenido por ISC (*Internet Systems Consortium*).

## Resolución de nombres de dominio

El mecanismo que consiste en encontrar la dirección IP relacionada al nombre de un ordenador se conoce como "**resolución del nombre de dominio**". La aplicación que permite realizar esta operación (por lo general, integrada en el sistema operativo se llama "**resolución**".

Cuando una aplicación desea conectarse con un host conocido a través de su nombre de dominio (por ejemplo, "es.kioskea.net"), ésta interroga al servidor de nombre de dominio definido en la configuración de su red. De hecho, todos los equipos conectados a la red tienen en su configuración las direcciones IP de ambos servidores de nombre de dominio del proveedor de servicios.

Entonces se envía una solicitud al primer servidor de nombre de dominio (llamado el "servidor de nombre de dominio principal"). Si este servidor de nombre de dominio tiene el registro en su caché, lo envía a la aplicación; de lo contrario, interroga a un servidor de nivel superior (en nuestro caso un servidor relacionado con el TLD ".net"). El servidor de nombre de nivel superior envía una lista de servidores de nombres de dominio con autoridad sobre el dominio (en este caso, las direcciones IP de los servidores de nombres de dominio principal y secundario para cómofunciona.net).

Entonces el servidor de nombres de dominio principal con autoridad sobre el dominio será interrogado y devolverá el registro correspondiente al dominio del servidor (en nuestro caso www).

## Tipos de zonas

**Zona de Búsqueda Directa:** Las resoluciones de esta zona devuelven la dirección IP correspondiente al recurso solicitado. Realiza las resoluciones que esperan como respuesta la dirección IP un determinado recurso.

**Zona de Búsqueda Inversa:** Las resoluciones de esta zona buscan un nombre de equipo en función de su dirección IP; una búsqueda inversa tiene forma de pregunta, del estilo "¿Cuál es el nombre del equipo que utiliza la dirección IP 192.168.0.200?".

## Dominios de nivel superior

Hoy en día, los Dominios de Nivel Superior o ***Top-level Domains*** (TLD) están clasificados según la IANA (*Internet Assigned Numbers Authority*) en los siguientes grupos:

* **Country-code top-level domains (ccTLD)**: correspondientes a países o territorios, a cada cual le corresponde un dominio de dos letras. Con algunas excepciones históricas, a cada territorio le corresponde el mismo código que tiene en el estándar ISO 3166: **uk** para Reino Unido, **it** para Italia o **jp** para Japón.
* **Generic top-level domains (gTLD)**: o dominios genéricos, formados de tres o más caracteres. El núcleo de estos dominios lo forman **com**, **info**, **net** y **org**. Además, los dominios **biz**, **name** y **pro** también son considerados genéricos, pero han sido designados como restringidos, porque es necesaria alguna acreditación para registrarse en ellos.

Históricamente, el grupo de dominios de nivel superior genéricos ha ido incluyendo dominios creados en los primeros años del desarrollo del sistema de nombres de dominio y que ahora están controlados por agencias u organizaciones que restringen su utilización a diferentes tipos de actividades. Así, dominios como **edu**, **gov**, **int** y **mil** son considerados dominios de nivel superior patrocinados por delante de dominios temáticos de nueva creación (como por ejemplo, **jobs**). Todos los dominios que no tienen una designación de país o territorial suelen ser referidos en este grupo de TLDs genéricos.

|  |  |
| --- | --- |
| **gTLD** | **USO DESTINADO** |
| aero | Industria aérea |
| asia | Compañías, organizaciones e individuos en la región Asia-Pacífico |
| biz | Uso empresarial (*business*) |
| cat | Lengua/cultura catalana |
| com | Organizaciones comerciales, hoy en día no está restringido |
| coop | Cooperativas |
| edu | Organizaciones de educación post-secundaría de los EEUU |
| gov | Entidades gubernamentales de los EEUU a niveles federales, estatales y locales |
| info | Sitios de información, hoy en día no está restringido |
| int | Organizaciones internacionales establecidas por tratados |
| jobs | Sitios relacionados con el trabajo |
| mil | Militares de los EEUU |
| mobi | Sitios de abastecimiento de dispositivos móviles |
| museum | Museos |
| name | Familias e individuos |
| net | Originalmente para infraestructuras de red, hoy en día no está restringido |
| org | Originalmente para organizaciones que no reunían las condiciones de los demás gTLDs, hoy en día no está restringido |
| pro | Ciertas profesiones |
| tel | Servicios que unían la red telefónica e Internet |
| travel | Agencias de viajes, aerolíneas, hoteles, oficinas de turismo, etc. |
| xxx | Pornografía |

* **Infraestructure top-level domain**: este grupo está formado por un solo dominio, **arpa** (*Address Routing Parameter Area*).

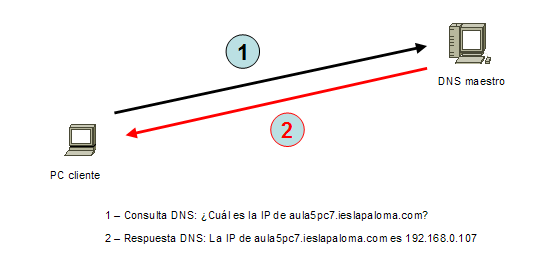
# Tipos de DNS

El servidor DNS admite tres modos de funcionamiento

* Servidor DNS maestro
* Servidor DNS esclavo
* Servidor caché DNS

## Servidor DNS maestro

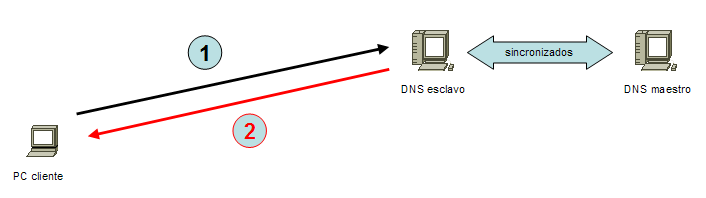
En este modo de funcionamiento, nuestro servidor se comporta como un auténtico servidor DNS para nuestra red local. Atenderá directamente a las peticiones de resolución de direcciones pertenecientes a la red local y reenviará a servidores DNS externos las peticiones del resto de direcciones de Internet.



**Consulta a un DNS maestro**

## Servidor DNS esclavo

Un servidor esclavo actuará como un servidor espejo de un servidor DNS maestro. Permanecerá sincronizado con el maestro. Se utilizan para repartir las peticiones entre varios servidores aunque las modificaciones solo se realicen en el maestro. En redes locales salvo por razones de disponibilidad, es raro que exista la necesidad de tener dos servidores DNS ya que con uno será suficiente.

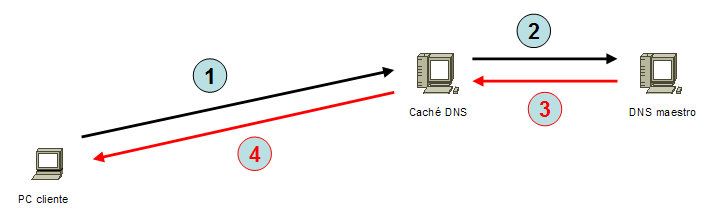
**Consulta a un DNS esclavo**

## Servidor caché DNS

En este modo de funcionamiento, nuestro servidor se comporta como si fuera un auténtico servidor DNS para nuestra red local aunque realmente no sea un servidor DNS propiamente dicho. Cuando recibe una petición de DNS por parte de un cliente de nuestra red, la trasladará a un DNS maestro que puede estar en nuestra red o fuera, almacenará en una memoria caché la respuesta y a la vez la comunicará a quien hizo la petición. Si un segundo cliente vuelve a realizar la misma petición, como nuestro servidor tiene la respuesta almacenada en su memoria caché, responderá inmediatamente sin tener que cursar la petición a ningún servidor DNS de Internet.

Disponer de un servidor caché DNS en nuestra red local aumenta la velocidad de la conexión a Internet pues cuando navegamos por diferentes lugares, continuamente se están realizando peticiones DNS. Si nuestro caché DNS almacena la gran mayoría de peticiones que se realizan desde la red local, las respuestas de los clientes se satisfarán prácticamente de forma instantánea proporcionando al usuario una sensación de velocidad en la conexión.

Es un modo de funcionamiento de sencilla configuración ya que prácticamente lo único que hay que configurar son las direcciones IP de un DNS primario y de un DNS secundario. Muchos routers ADSL ofrecen ya este servicio de caché, tan solo hay que activarlo y configurar una o dos IPs de servidores DNS en Internet. En los PCs de nuestra red local podríamos poner como DNS primario la IP de nuestro router y como DNS secundario una IP de un DNS de Internet.

**Consulta a un cache DNS. En caso de fallo, se redirecciona hacia un DNS maestro**

# Tipos de registros

Un DNS es una base de datos distribuida que contiene registros que se conocen como RR (Registros de Recursos), relacionados con nombres de dominio. La siguiente información sólo es útil para las personas responsables de la administración de un dominio, dado que el funcionamiento de los servidores de nombre de dominio es completamente transparente para los usuarios.

Ya que el sistema de memoria caché permite que el sistema DNS sea distribuido, los registros para cada dominio tienen una duración de vida que se conoce como TTL (Tiempo de vida). Esto permite que los servidores intermediarios conozcan la fecha de caducidad de la información y por lo tanto que sepan si es necesario verificarla o no.

Por lo general, un registro de DNS contiene la siguiente información:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nombre de dominio (FQDN) | TTL | Tipo | Clase | RData |
| www.google.es. | 3600 | A | IN | 74.125.232.210 |

* **Nombre de dominio**: el nombre de dominio debe ser un nombre FQDN, es decir, debe terminar con un punto. En caso de que falte el punto, el nombre de dominio es relativo, es decir, el nombre de dominio principal incluirá un sufijo en el dominio introducido;
* **Tipo**: un valor sobre 16 bits que define el tipo de recurso descrito por el registro. El tipo de recurso puede ser uno de los siguientes:
  + **A**: este es un tipo de base que hace coincidir el nombre canónico con la dirección IP. Además, pueden existir varios registros A relacionados con diferentes equipos de la red (servidores).
  + **CNAME (Nombre Canónico)**: Permite definir un alias para el nombre canónico. Es particularmente útil para suministrar nombres alternativos relacionados con diferentes servicios en el mismo equipo.
  + **HINFO**: éste es un campo solamente descriptivo que permite la descripción en particular del hardware del ordenador (CPU) y del sistema operativo (OS). Generalmente se recomienda no completarlo para evitar suministrar información que pueda ser útil a piratas informáticos.
  + **MX (Mail eXchange)**: es el servidor de correo electrónico. Cuando un usuario envía un correo electrónico a una dirección (user@domain), el servidor de correo saliente interroga al servidor de nombre de dominio con autoridad sobre el dominio para obtener el registro MX. Pueden existir varios registros MX por dominio, para así suministrar una repetición en caso de fallas en el servidor principal de correo electrónico. De este modo, el registro MX permite definir una prioridad con un valor entre 0 y 65,535:

es.kioskea.net. IN MX 10 mail.commentcamarche.net.

* + **NS**: es el servidor de nombres de dominio con autoridad sobre el dominio.
  + **PTR**: es un puntero hacia otra parte del espacio de nombres del dominios.
  + **SOA (Start Of Authority (Inicio de autoridad))**: el campo SOA permite la descripción del servidor de nombre de dominio con autoridad en la zona, así como la dirección de correo electrónico del contacto técnico (en donde el carácter "@" es reemplazado por un punto).
* **Clase**: la clase puede ser IN (relacionada a protocolos de Internet, y por lo tanto, éste es el sistema que utilizaremos en nuestro caso), o CH (para el sistema caótico);
* **RDATA**: estos son los datos relacionados con el registro. Aquí se encuentra la información esperada según el tipo de registro:
  + **A**: la dirección IP de 32 bits:
  + **CNAME**: el nombre de dominio;
  + **MX**: la prioridad de 16 bits, seguida del nombre del ordenador;
  + **NS**: el nombre del ordenador; PTR: el nombre de dominio
  + **PTR**: el nombre de dominio;
  + **SOA**: varios campos.

# Servidor DNS en Linux

Para montar el servidor DNS hemos utilizado una máquina con Ubuntu y el paquete BIND. BIND (Berkeley Internet Name Domain, anteriormente: Berkeley Internet Name Daemon) es el servidor de DNS más comúnmente usado en Internet, especialmente en sistemas Unix, en los cuales es un standard de facto. Fue creado originalmente en la Universidad de California, y actualmente propiedad del Internet Systems Consortium.

## Instalación

Para instalar BIND simplemente abrimos la consola (Aplicaciones/Accessorios/Terminal) y escribimos el siguiente comando:

**sudo apt-get install bind9**

## Configuración

Los archivos de configuración que tendremos que modificar en el servidor DNS son los siguientes:

* ***/etc/bind/named.conf***
* ***/etc/bind/named.conf.options***
* ***/etc/bind/named.conf.local***
* ***/etc/bind/db.si2.com***
* ***/etc/bind/db.172.20.102***

En el resto de ordenadores de la red, sólo habrá que modificar el siguiente archivo:

* ***/etc/resolv.conf.***

### /etc/bind/named.conf

El archivo *named.conf* en realidad no es necesario que lo modifiquemos. Este archivo almacena la configuración de las diferentes zonas generadas por defecto en el momento de la instalación.

### /etc/bind/named.conf.local

Para modificar el archivo */etc/bind/named.conf.local* podemos utilizar cualquier editor de textos, como gedit o vi. Para crear este fichero con gedit abriremos el terminal y escribiremos:

**sudo gedit /etc/bind/named.conf.local**

Una vez abierto tendremos que poner lo siguiente (lo que hay tras el carácter # son comentarios).

**#Esta es la definición de la zona. Cambia si2.com por tu nombre de dominio**

**zone “si2.com” {**

**type master;**

**file “/etc/bind/db.si2.com”;**

**};**

#Aquí definimos la zona de resolución inversa. Cambia 102.20.172 por la dirección de tu red

**zone “102.20.172.in-addr.arpa” {**

**type master;**

**file “/etc/bind/db.172.20.102″;**

**};**

### /etc/bind/named.conf.options

A continuación modificamos el fichero */etc/bind/named.conf.options*. En este fichero especificaremos aquellos servidores DNS de Internet que resolverán los nombres de dominio que nuestro servidor DNS local no pueda resolver. Será necesario especificarlos para que los ordenadores de nuestra red salgan a Internet.

**options {**

**directory “/var/cache/bind”;**

**forwarders {**

**80.58.0.33;**

**62.42.230.24;**

**};**

**};**

Tendremos que cambiar las IP 80.58.0.33 y 62.42.230.24 por los servidores DNS de nuestro ISP.

### /etc/bind/db.si2.com

Después tendremos que crear el fichero de definición de zona */etc/bind/db.si2.com*. En este fichero es donde pondremos todos los nombres de máquinas y direcciones IP que conocerá nuestro servidor DNS.

**$TTL 604800**

**;Cambia si2.com por el nombre de tu dominio**

**;Cambia dns por el nombre de tu servidor de nombres**

**si2.com. IN SOA si2.com. dns.si2.com. (**

**;Las siguientes líneas no es necesario que las modifiquemos**

**2006081401;**

**28800;**

**3600;**

**604800;**

**38400)**

**;Cambia las siguientes líneas si es necesario**

**;si2.com por el nombre de tu dominio**

**;dns por el nombre de tu servidor de nombres**

**si2.com. IN NS dns.si2.com.**

**si2.com. IN MX 10 mail.si2.com.**

**;Cambia los nombres máquinas y direcciones IP por las de tu red**

**mail IN A 172.20.102.2**

**dns IN A 172.20.102.3**

**dns2 IN A 172.20.102.4**

**pc01 IN A 172.20.102.5**

**pc02 IN A 172.20.102.6**

**pc03 IN A 172.20.102.7**

**pc04 IN A 172.20.102.8**

**;Así para el resto de equipos de la red**

**;Lo siguiente es un alias. Para que desde el navegador podamos poner**

**;www.si2.com en lugar de dns.si2.com**

**www IN CNAME dns**

**ftp in CNAME dns2**

### /etc/bind/db.172.20.102

A continuación creamos el archivo de zona de resolución inversa /*etc/bind/db.172.20.102* con el siguiente contenido:

**;Cambia si2.com por el nombre de tu dominio**

**;Cambia dns por el nombre de tu servidor de nombres**

**$TTL 604800**

**@ IN SOA si2.com. dns.si2.com. (**

**2006081401;**

**28800;**

**3600;**

**604800;**

**38400)**

**;Cambia si2.com por el nombre de tu dominio**

**;Cambia dns por el nombre de tu servidor de nombres de dominio**

**;El número que aparece delante de IN PTR es el último octeto de la dirección IP de la máquina**

**;172.20.102.3 para dns, 172.20.102.4 para dns2, 172.20.102.5 para pc01….**

**;Cambia las direcciones IP y nombres por los de tu red**

**@ IN NS dns.si2.com.**

**2 IN PTR mail.si2.com.**

**3 IN PTR dns.si2.com.**

**4 IN PTR dns2.si2.com.**

**5 IN PTR pc01.si2.com.**

**6 IN PTR pc02.si2.com.**

**7 IN PTR pc03.si2.com.**

**8 IN PTR pc04.si2.com.**

### /etc/resolv.conf (en los clientes)

En cada uno de los ordenadores de la red habrá que modificar el fichero */etc/resolv.conf*. Este fichero tendrá el siguiente contenido:

**//Cambia 172.20.102.3 por la IP de tu servidor de nombres**

**//Cambia si2.com por el nombre de tu dominio**

**nameserver 172.20.102.3**

**search si2.com**

## Comprobación de la configuración

A partir de la versión 9 de BIND se incluyen dos herramientas software para chequear la sintaxis y semántica de los archivos que describen las zonas y el archivo de configuración principal named.conf. Dichas herramientas son: **named-checkzone** y **named-checkconf**.

Una vez configurado el servidor DNS, si se quiere hacer una comprobación sintáctica del archivo de configuración named.conf hay que ejecutar:

**named-checkconf**

La salida muestra los errores que genera. Si no genera salida, está todo correcto.

En el caso de los archivos de zona hay que ejecutar:

**named-checkzone si2.com /etc/bind/db.si2.com**

(cambiando si2.com por el nombre de tu dominio)

Este comando genera la siguiente salida si todo está correcto:

**zone si2.com/IN: loaded serial 1 OK**

## Puesta en marcha del servicio

Para poner en marcha el servidor utilizaremos la orden:

**service bind9 start**

Si queremos parar el servidor utilizaremos:

**service bind9 stop**

Para reiniciar el servidor, es decir, para pararlo y volver a iniciarlo:

**service bind9 restart**

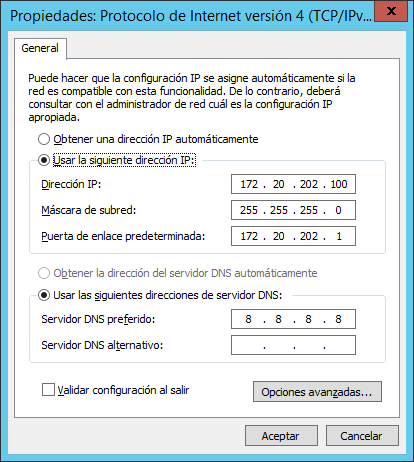
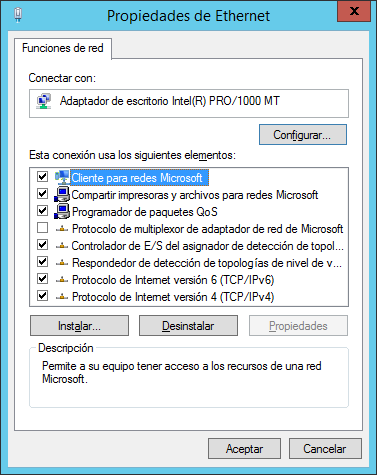
## Comprobando el servidor de nombres DNS

Para comprobar si el servidor DNS funciona correctamente no tenemos más que colocarnos en un cliente, abrir una terminal y ejecutar la orden ***nslookup***. Así, y basándonos en el ejemplo anterior, la orden ***nslookup dns.si2.com*** debería devolvernos la IP 172.20.102.3 mientras que la orden ***nslookup 172.20.102.3*** nos devolvería el nombre *dns.si2.com*.

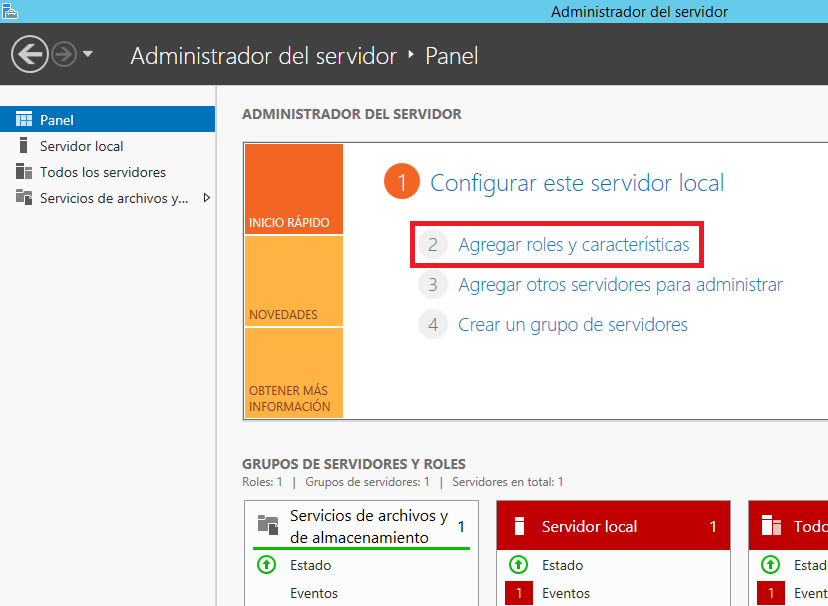
# Servidor DNS en Windows 2012 Server

## Instalación

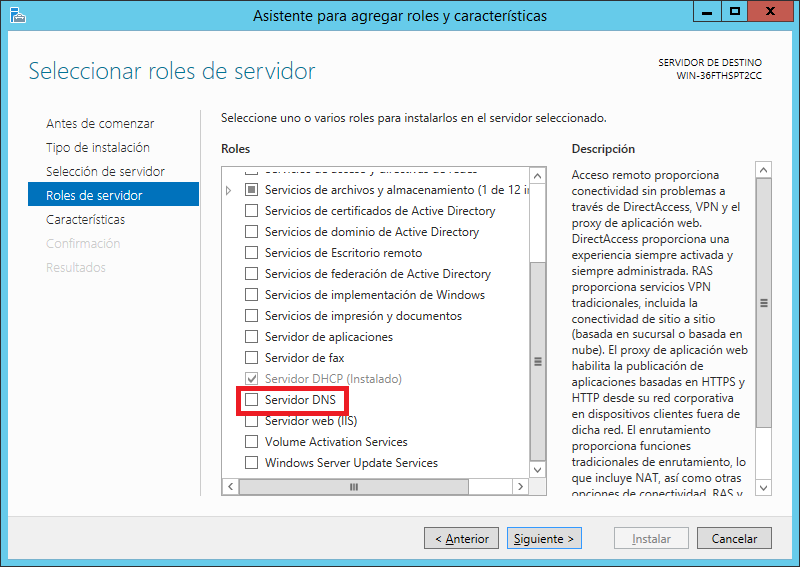
Antes de instalar el servidor DNS, vamos al centro de redes y recursos compartidos y asignamos una dirección IP estática al Windows 2008 Server



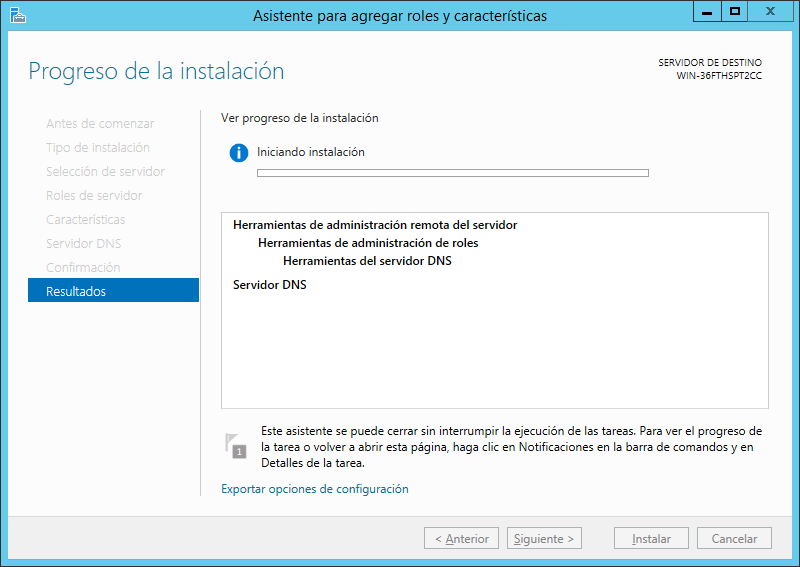
Una vez configurada la red vamos a *Inicio 🡪 Administrador del servidor,* abrimos *Funciones* y clicamos en *Agregar funciones* para instalar el servidor DNS



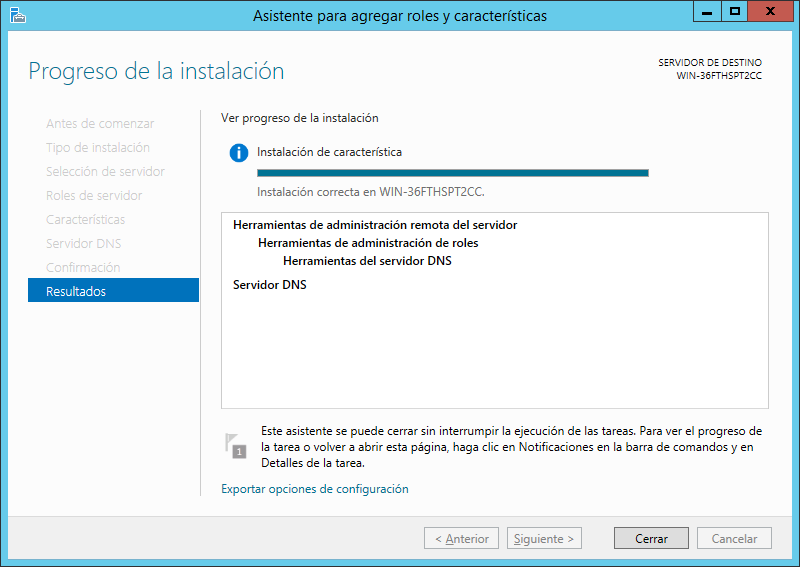
Escogemos la función *Servidor DNS* que vamos a instalar desde la lista de funciones disponible. y continuamos con el asistente de configuración



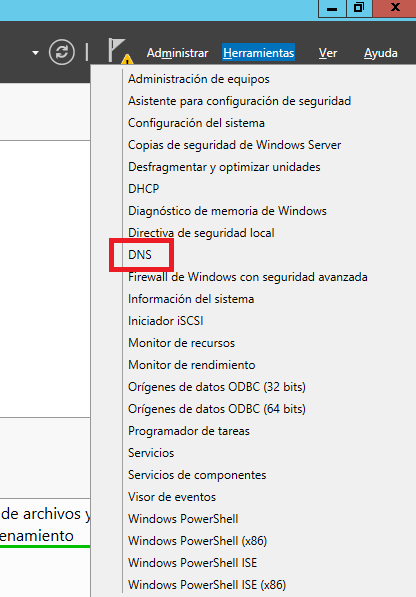
Al finalizar el asistente clicamos en Instalar para que comience la instalación.



Finalmente aparecerá una ventana informándonos de que la instalación se ha completado de manera satisfactoria.



Cerramos el asistente y el *Administrador del servidor* y vamos a *Inicio 🡪 Herramientas administrativas 🡪 DNS*

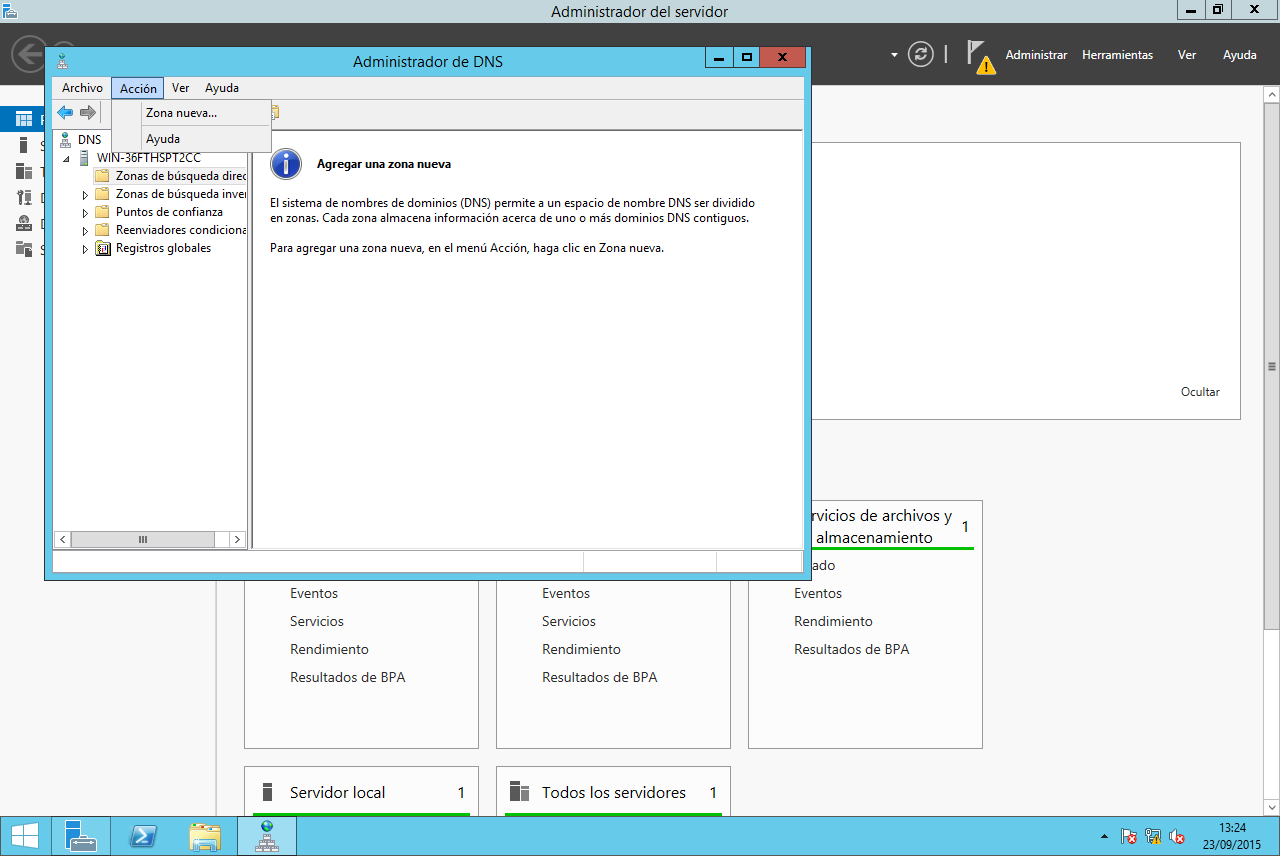


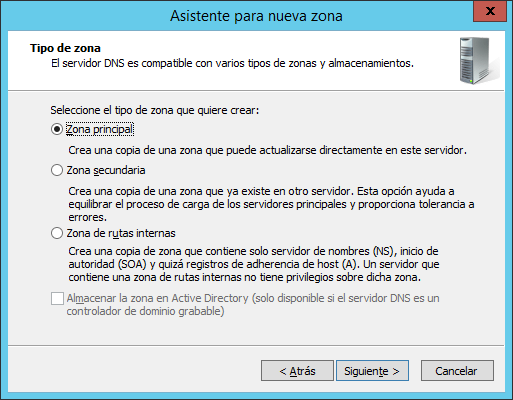
## Configuración

Una vez abierto el Administrador de DNS, podemos observar que no existe ninguna zona de búsqueda directa o inversa definida. Vamos a crear ambas zonas.

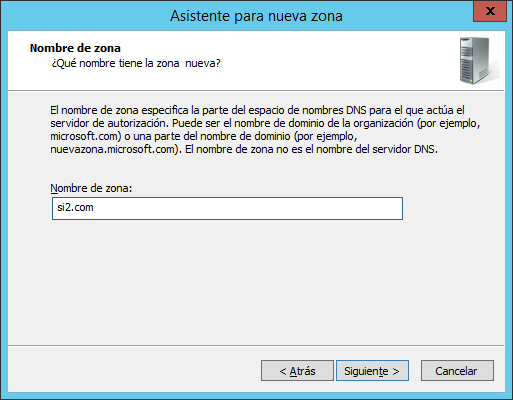
### Zona de búsqueda directa

Hacemos clic con el botón derecho en Zonas de búsqueda directa🡪 *Zona nueva* y el asistente para la creación de una zona nueva nos guiará en el proceso. En primer lugar tendremos que decidir el tipo de zona que queremos crear. Elegiremos *Zona principal*

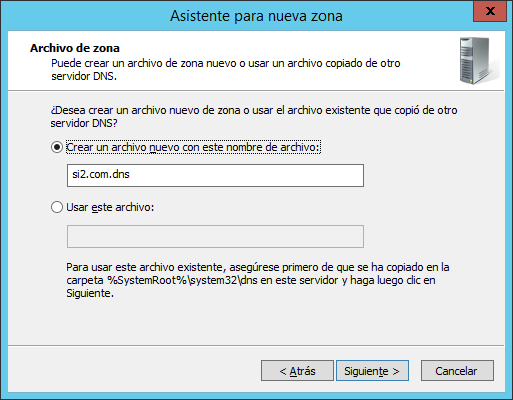




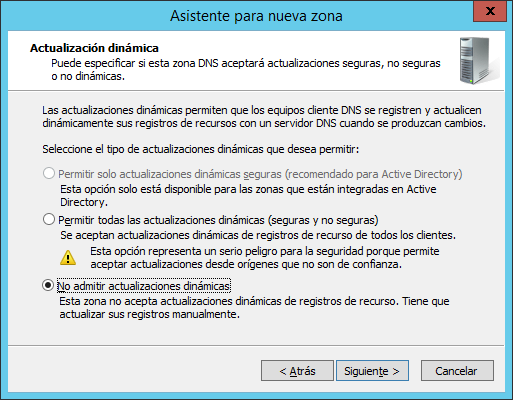
En el siguiente paso introduciremos un nombre de zona. En nuestro caso ***si2.com*** que será el nombre de nuestro dominio.



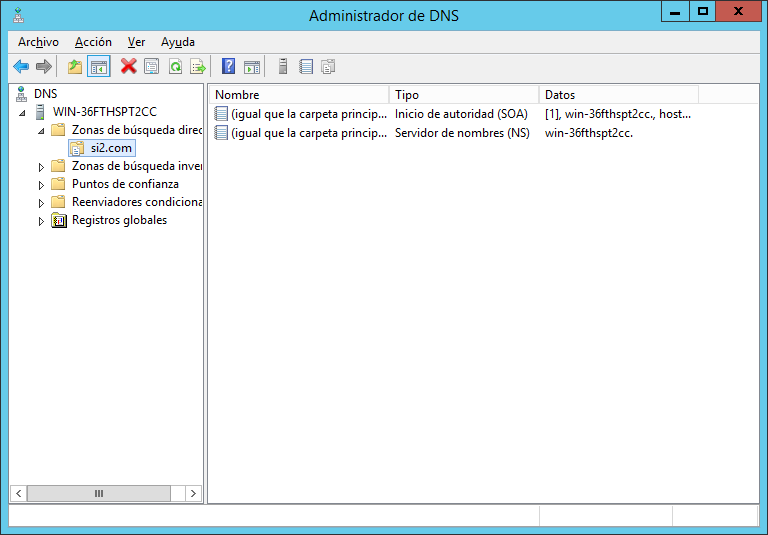
A continuación seleccionamos el nombre del archive que contendrá la información de la zona.



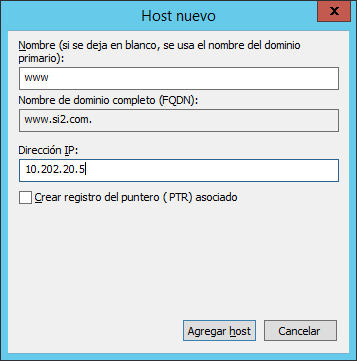
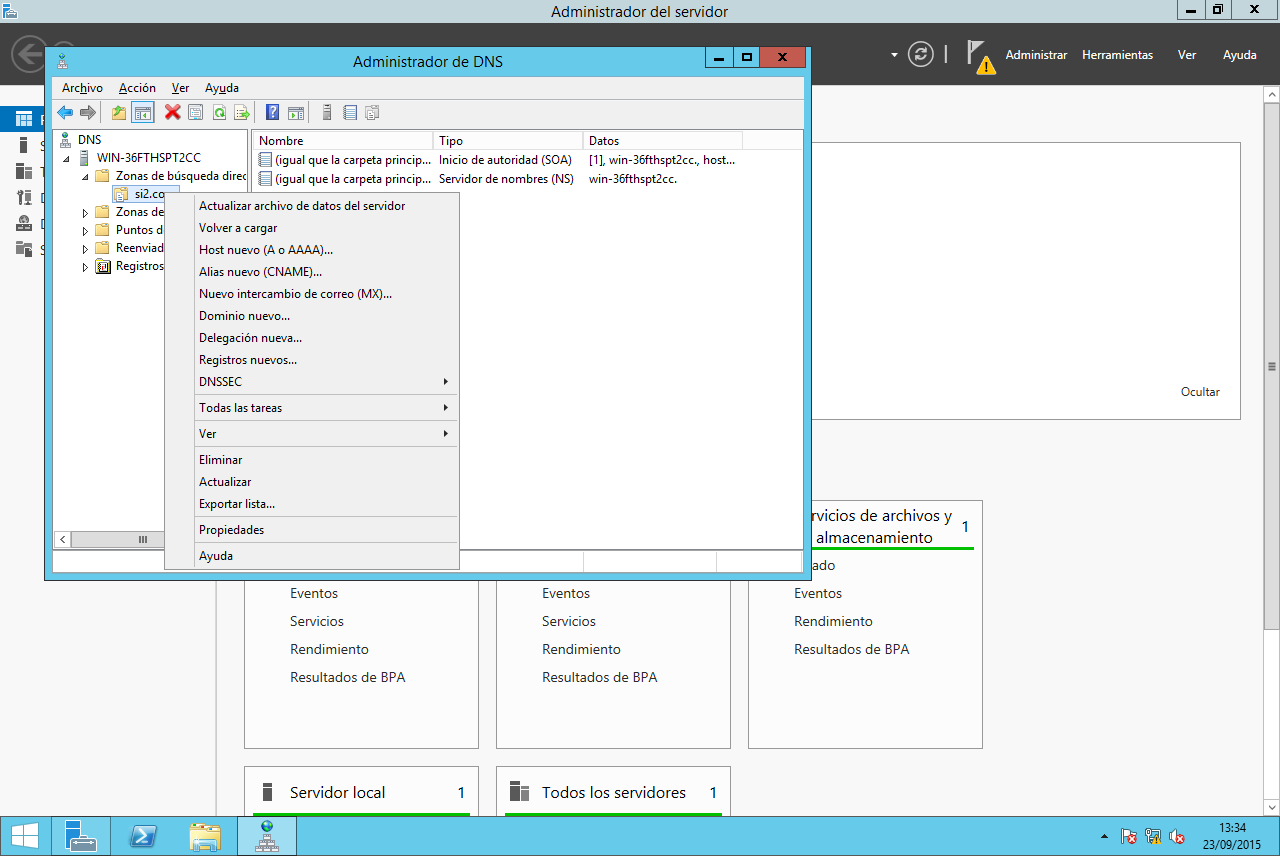
El siguiente paso nos da la posibilidad de escoger actualizaciones dinámicas. Elegiremos *No admitir actualizaciones dinámicas.*

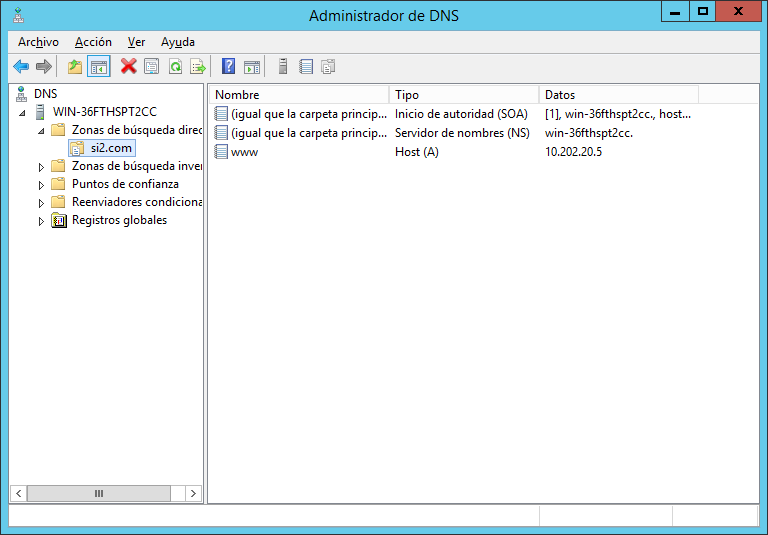


Finalmente aparece un breve resumen de la zona. Finalizamos podemos ver que se ha creado la zona ***si2.com.*** Se han creado 2 registros.. SOA (Start of Authority) y NS (Name Server)



Una vez aquí podemos crear los registros necesarios dentro de la zona. Clic con el botón derecho y *Host Nuevo (A o AAAAA*)



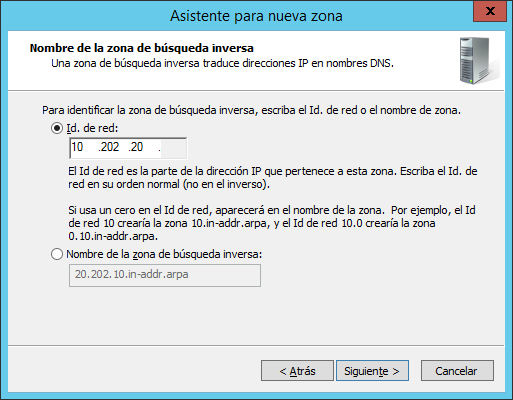


También podremos crear registros CNAME (alias) y MX (Mail Exchange). Otra opción para incluir los host es añadiéndolos al dominio pero para ello necesitamos tener instalado el Directorio Activo.

### Zona de búsqueda inversa

La creación de la zona de búsqueda inversa es similar al de la zona de búsqueda directa. El asistente preguntará si se quiere crear una zona principal o secundaria y si deseamos que la zona de búsqueda inversa sea para IPv4 o IPv6. Seleccionaremos IPv4 e introduciremos el ID de red. Solamente los 3 primeros bytes. (Suponemos mascara /24).

El nombre de la zona se escribe automáticamente mientras escribimos el Id. de la red.

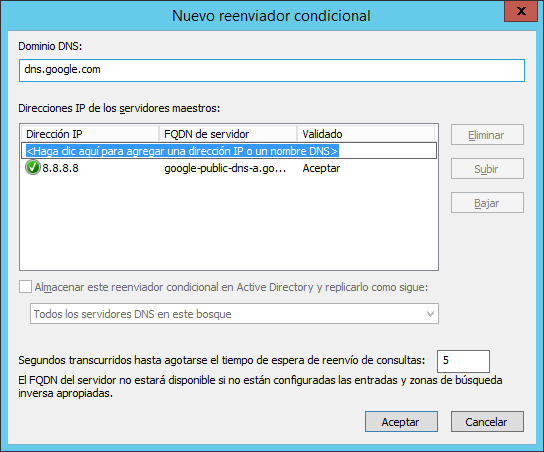


A continuación seleccionamos que no deseamos actualizaciones dinámicas y finalizamos el asistente

**En la zona de búsqueda inversa debe haber un registro por cada registro que tengamos en la zona de búsqueda directa.**

### Reenviadores

Podemos definir reenviadores para responder a las peticiones que nuestro DNS no es capaz de responder. Para ello vamos a *Reenviadores condicionales.* Clic derecho Nuevo reenviador condicional y añadimos el nombre y la IP en la ventana que aparece.



## Testeando el servidor

Una vez que tenemos el servidor DNS funcionando debemos testearlo para asegurarnos de que funciona correctamente. Para ello usaremos la terminal de un PC cliente y ejecutaremos los comandos ***nslookup www.si2.com*** y ***nslookup 192.168.50.4.***