

CFGM. Servicios en red

Unidad 2

Servicio de nombres de dominio (DNS)



2 Servicio de nombres de dominio (DNS)

CONTENIDOS

1. El servicio DNS
2. Configuración del cliente DNS
3. Base de datos del protocolo DNS
4. Servidores de nombres de dominio
5. Instalación y configuración del servicio DNS en un servidor GNU/Linux
6. Configuración de un servidor DNS secundario en Ubuntu GNU/Linux
7. Configuración del servidor DNS con Windows 2008 Server
8. DNS dinámico (DDNS)
9. DNS con IPv6

2 Servicio de nombres de dominio (DNS)

1. El servicio DNS

En una red TCP/IP, las máquinas se identifican mediante su dirección de red o número IP. Para las personas resulta más sencillo recordar un nombre que se asocia a una máquina concreta. También es más fiable, ya que la dirección IP puede cambiar, pero no así el nombre.

Es necesario un mecanismo que traduzca los nombres de las máquinas a direcciones IP. El servicio DNS permite que esta tarea se lleve a cabo.

1.1. El espacio de nombres de dominio

El servicio DNS se compone de una base de datos distribuida (integrada por varias máquinas conectadas en red) en la que se almacenan las asociaciones de nombres de dominios y direcciones IP. Esta base de datos está clasificada por nombres de dominio, donde cada uno puede considerarse una rama en un árbol invertido llamado **espacio de nombres de dominio**.

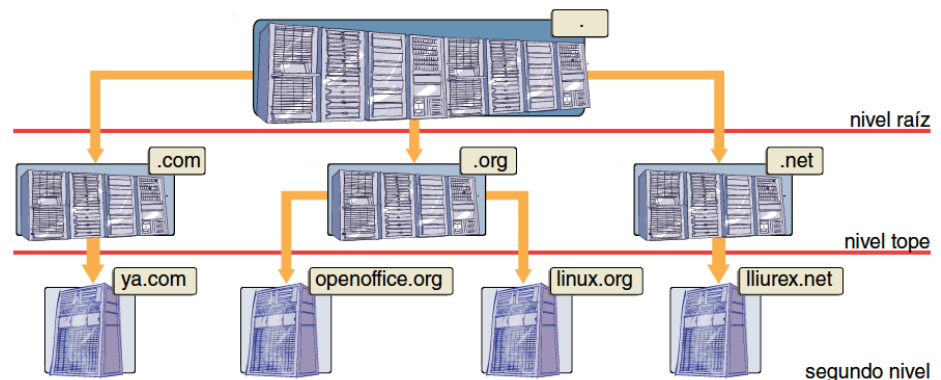
El árbol comienza en el nodo raíz, situado en el nivel superior.

Por debajo, puede existir un número indeterminado de nodos.

Normalmente se utilizan hasta cinco niveles.

El nombre completo de un nodo está formado por el conjunto de nombres que forman el itinerario desde ese nodo hasta la raíz. Los nombres se separan con un punto.

El dominio es, pues, cada uno de los subárboles que integran el árbol o espacio de nombres de dominio.



2 Servicio de nombres de dominio (DNS)

1. El servicio DNS

1.1. El espacio de nombres de dominio

El nivel superior o primer nivel (TLD) está formado por los dominios que descienden directamente del dominio raíz. **Los principales TLD genéricos son:**

TLD	Descripción
com	Agrupar organizaciones comerciales. Ejemplos: google.com, yahoo.com, strands.com.
edu	Reúne organizaciones educativas universitarias. Ejemplos: eada.edu, ortegaygasset.edu, mit.edu.
net	Agrupar organizaciones dedicadas a Internet y a las telecomunicaciones. Ejemplos: rpmfind.net, listas.net, php.net.
org	Reúne organizaciones no comerciales. Ejemplos: linuxdoc.org, ubuntu.org, linux.org, insflug.org.
gov	Agrupar organizaciones gubernamentales de EEUU. Ejemplos: nasa.gov, nsf.gov, whitehouse.gov.
int	Se usa en organizaciones internacionales. Ejemplos: redcross.int, interpol.int, coe.int
name	Se emplea para nombres de personas.
mobi	Es propio de empresas de telefonía móvil o servicios para móvil.



¿Sabías que...?

El espacio de nombres de dominio es jerárquico. Internet se divide en cientos de dominios:

- Genéricos: .com, .edu, .gov, .int, .mil, .net, .org.
- De país: una entrada por país: .es, .fr, .uk, etc.
- Otros: .aero, .biz, .coop, .info, .pro, .name, .museum, .firm, .store, .nom, .arts, etc.

Cada dominio se divide en subdominios:

- máquina.subdominio.subdominio...dominio, etc.

Cada nivel va delegando autoridad en los niveles inferiores.

Puede ocurrir que los dominios geográficos de primer nivel contengan a su vez alguno de los dominios genéricos. Estos dominios serían de segundo nivel (com.es, edu.au, org.uk, teso.org.es, etcétera.).



2 Servicio de nombres de dominio (DNS)

1. El servicio DNS

1.2. La delegación de dominios

DNS es una base de datos distribuida y permite su administración descentralizada mediante la delegación de dominios.

El dominio puede ser dividido en **subdominios** por el administrador y delegar el control de cada uno. La autoridad que se hace cargo de la delegación debe asumir también la responsabilidad de **mantener actualizados los registros de recursos** de ese subdominio.

Pero delegación no significa independencia, sino **coordinación**. La división de un dominio en subdominios no implica siempre una cesión de autoridad.

1.3. ¿Qué son los dominios y las zonas?

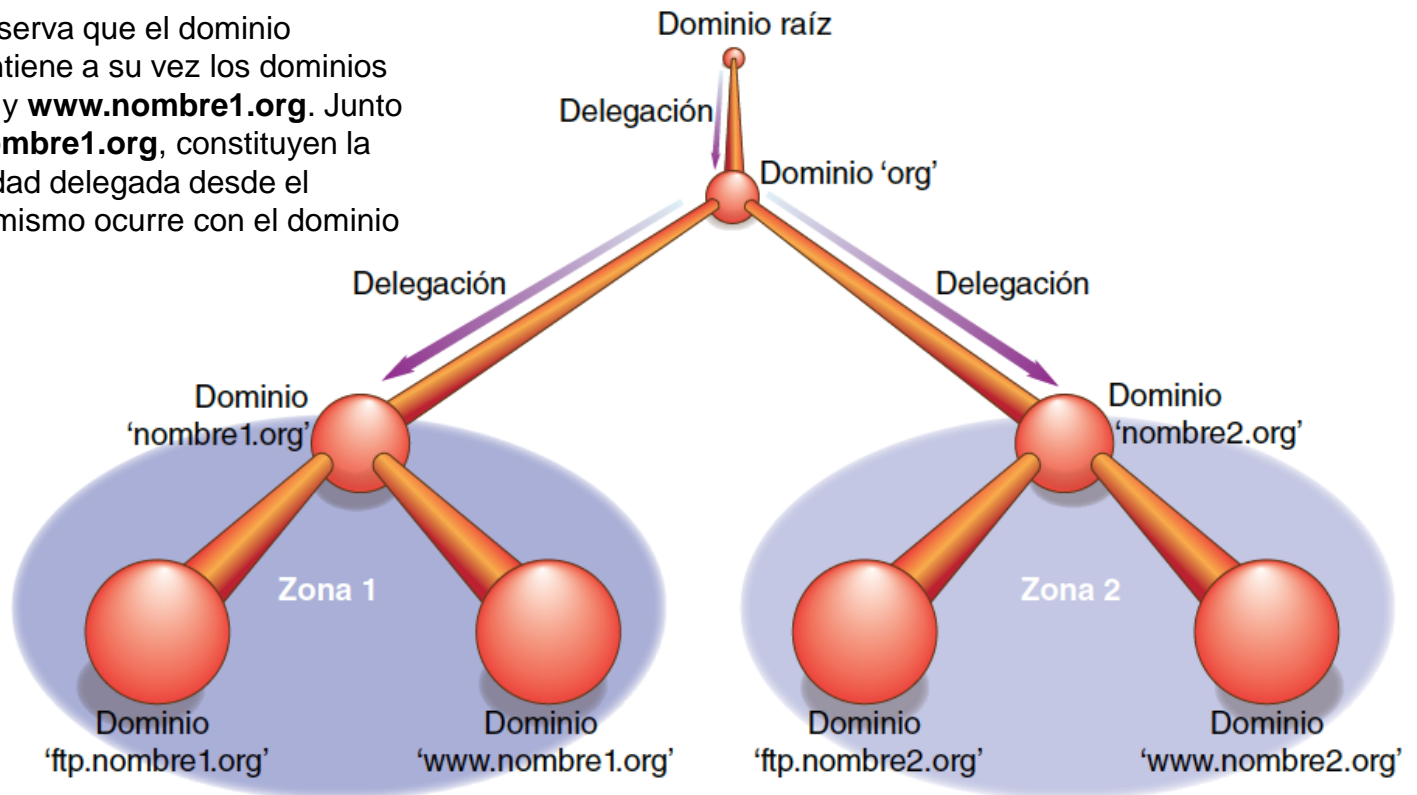
- El servidor de nombres almacena información acerca de algunas partes o zonas del espacio de nombres de dominio.
- Se dice que el servidor de nombres tiene autoridad sobre la zona.
- Por lo tanto, un servidor de nombres podrá tener autoridad sobre varias zonas.
- La zona es un **archivo** que contiene determinados **registros** de la base de datos del espacio de nombres de dominio, que identifican a uno o más dominios.
- La generación de zonas se hace mediante la delegación de autoridad.

2 Servicio de nombres de dominio (DNS)

1. El servicio DNS

1.3. ¿Qué son los dominios y las zonas?

En la figura se observa que el dominio **nombre1.org** contiene a su vez los dominios **ftp.nombre1.org** y **www.nombre1.org**. Junto con el dominio **nombre1.org**, constituyen la **zona1** con autoridad delegada desde el dominio **org**. Lo mismo ocurre con el dominio **nombre2.org**.



2 Servicio de nombres de dominio (DNS)

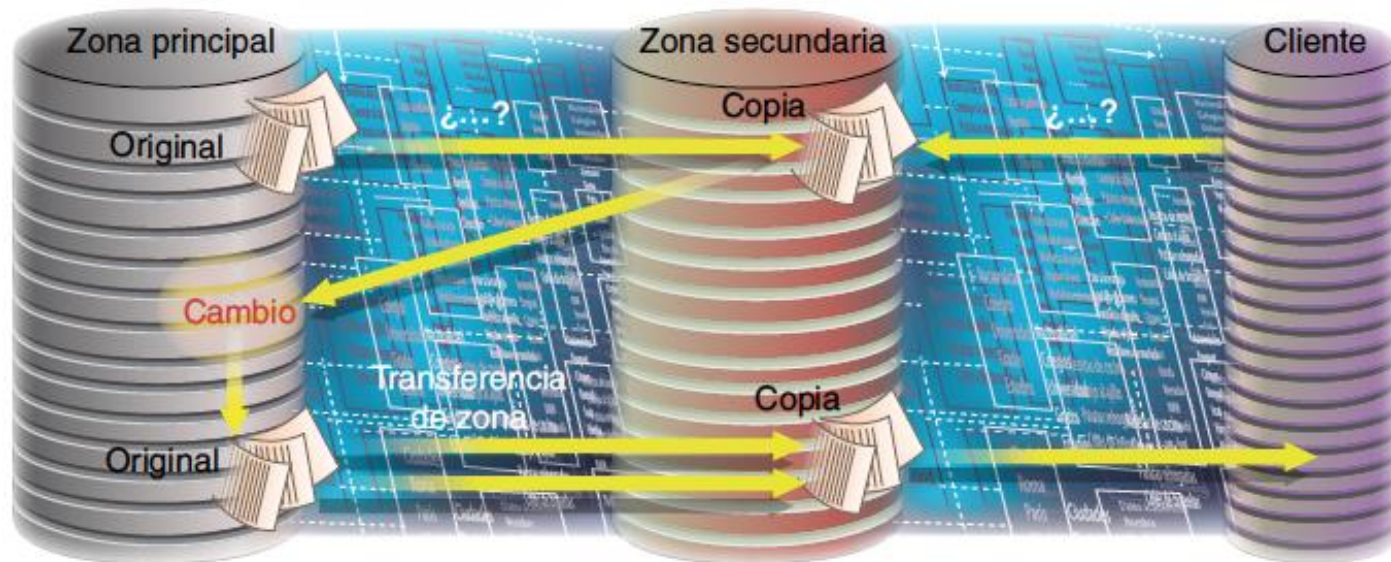
1. El servicio DNS

1.3. ¿Qué son los dominios y las zonas?

Los servidores de nombres se pueden clasificar en los tipos siguientes:

1. **Servidor primario (maestro):** en él se llevan a cabo todas las modificaciones sobre una zona.
2. **Servidor secundario (esclavo):** contiene una copia de solo lectura de los archivos de zona.
3. **Servidor caché:** No contiene ningún tipo de información acerca de la zona y se utiliza para acelerar las consultas.

La información de las zonas se obtiene a través de la red mediante la **transferencia de zona**.

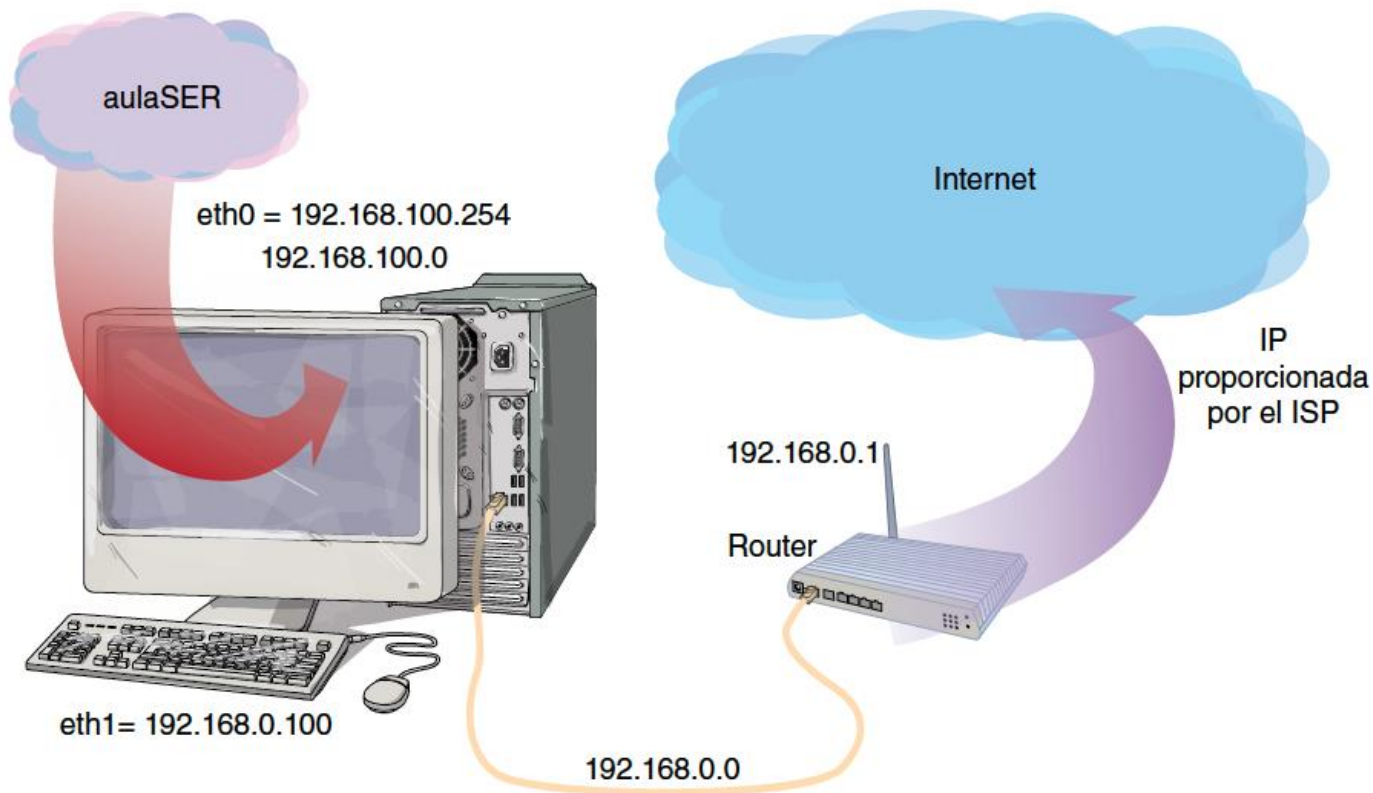


2 Servicio de nombres de dominio (DNS)

1. El servicio DNS

1.4. Red ejemplo y base para el desarrollo de la unidad

Estructura de la red aulaSER.com según el esquema 2:



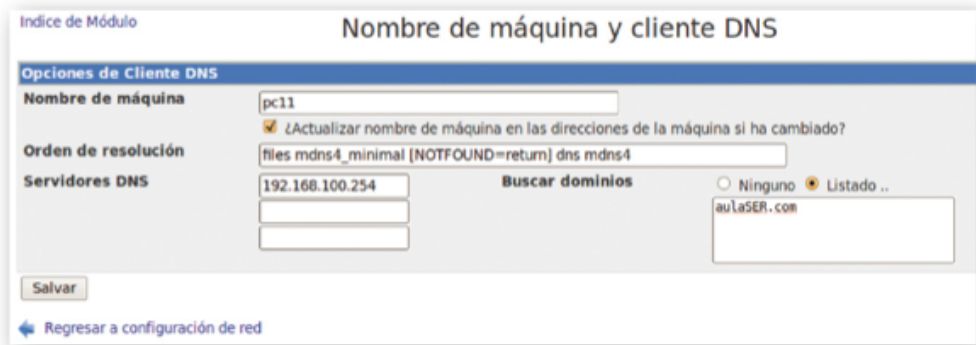
2 Servicio de nombres de dominio (DNS)

2. Configuración del cliente DNS

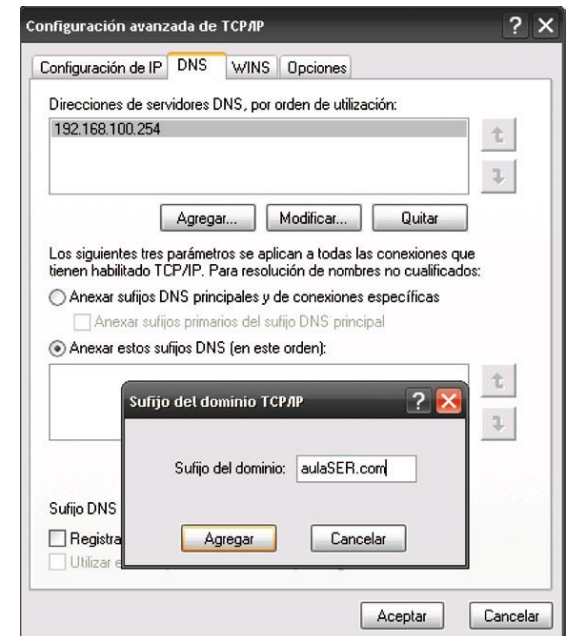
El cliente del servicio de nombre de dominio (DNS) se denomina *resolver*. Sus principales tareas son:

- Interrogar al servidor de nombres.
- Interpretar respuestas (que pueden ser registros RR o errores).
- Devolver información al programa que la solicita.

Los archivos de configuración implicados para Ubuntu GNU/Linux son `/etc/resolv.conf` y `/etc/host.conf`, pero también se puede configurar utilizando la herramienta Webmin.



En Windows se configura editando las propiedades de la conexión de área local



2 Servicio de nombres de dominio (DNS)

3. Base de datos del protocolo DNS

El formato y los campos de los registros de recursos son los siguientes:

- **Propietario:** nombre de máquina o dominio DNS al que pertenece el recurso. Puede contener el símbolo @, que representa el nombre de la zona descrita.
- **TTL (Time To Live):** tiempo de vida, en segundos, del registro en la caché. Es un campo opcional y se expresa en días (d), horas (h), minutos (m) y segundos (s). El cero (0) no se almacena en caché.
- **Clase:** familia de protocolos en uso. Suele tomar el valor «IN» de Internet, que representa una red TCP/IP.
- **Tipo:** varía en función del campo Clase.
- **RDATA:** información específica del tipo de recurso. Por ejemplo, para un registro de clase IN y tipo A este campo especifica una dirección IP.

Los principales tipos de registros de recursos son:

Nombre de recurso	Tipo de registro	Función
Inicio de autoridad	SOA	Identifica al servidor autoritario de una zona y sus parámetros de configuración.
Servidor de nombres	NS	Identifica servidores de nombres autorizados para una zona.
Dirección	A	Asocia un nombre de dominio FQDN con una dirección IP.
Puntero	PTR	Asigna una dirección IP a un nombre de dominio completamente cualificado. Para las búsquedas inversas.
Registro de correo	MX	Indica máquinas encargadas de la entrega y recepción de correo en el dominio.
Nombre canónico	CNAME	Permite asignar uno o más nombres a una máquina.
Text	TXT	Almacena cualquier información.
Servicio	SRV	Ubicación de los servidores para un servicio.



2 Servicio de nombres de dominio (DNS)

4. Servidores de nombres de dominio

Existen varias aplicaciones de servicios para servidores de nombres de dominio. La más utilizada es Bind (www.isc.org/products/BIND/), disponible bajo licencia BSD.

La ejecución de un servidor DNS (utilizando Bind9) en una máquina implica la ejecución en el sistema del proceso `named`, cuyo archivo de configuración es `/etc/bind/named.conf`. Este archivo es el lugar donde se le dice a Bind qué debe hacer, dónde y cómo.

La primera línea del archivo es una declaración *include* en la que se integra el archivo `named.conf.options`, donde se encuentran las opciones globales del servidor.

La última línea del archivo es otra declaración *include*, del archivo `named.conf.local`, donde se definen las zonas locales.

Las principales sentencias del archivo `named.conf.options` son:

- **acl**: define listas de direcciones IP para permitir o denegar el acceso al servidor de nombres. Su sintaxis es:

Queremos definir la lista de control de acceso *redes* que incluya todas las máquinas de las redes 192.168.100.0/24 y 192.168.0.0/16, y la máquina independiente 192.168.110.5. Para ello, especificaremos:

```
acl redes { { 192.168.100/24; 192.168/16; 192.168.110.5; } };
```

- **options**: controla las opciones de configuración del servidor y de otras sentencias. Sólo debe aparecer una vez en el archivo de configuración. Dentro de la sentencia `options` se pueden encontrar las declaraciones `directory`, `allow-query`, `blackhole`, `forwarders` y otras.



2 Servicio de nombres de dominio (DNS)

4. Servidores de nombres de dominio

Las principales sentencias del archivo `named.conf` son:

- **zone:** permite definir las zonas y describir sus configuraciones. Existen cuatro tipos:
 1. **Zona maestra (master zone):** alberga la copia principal de los datos de la zona.
 2. **Zona esclava (slave zone):** contiene datos que se obtienen como resultado de la duplicación de la información de una zona maestra.
 3. **Zona oculta (hint zone):** cuando se hacen peticiones a una zona que no se conoce, ésta ofrece información relativa a los servidores de la raíz.
 4. **Zona de reenvío (forward zone):** indica al servidor de nombres que redirija las peticiones de información sobre la zona hacia otros servidores.
- **include:** sentencia que se utiliza para incluir los archivos que contienen las opciones y las zonas locales.

```
include "/etc/bind/named.conf.local";
```

A partir de Bind9 se incluyen dos herramientas para chequear la sintaxis y semántica de los archivos que describen las zonas y el archivo `named.conf`. Son: `named-checkzone` y `named-checkconf`.

Una vez configurado el servicio DNS, si se quiere hacer una comprobación sintáctica del archivo de configuración `named.conf`, hay que ejecutar como administrador (*root*): `$sudo named-checkconf`. La salida indica los errores que detecta. Si no genera salida, está todo correcto.

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

```
$sudo named-checkzone aulaSER.com /etc/bind/db.aulaSER.com
```

2 Servicio de nombres de dominio (DNS)

4. Servidores de nombres de dominio

4.1. Resolución inversa

De la misma forma que los nombres de dominio se resuelven efectuando consultas para cada componente de derecha a izquierda, las direcciones IP siguen el mismo esquema.

Su dominio raíz se denomina **in-addr.arpa**.

Las direcciones IP están escritas en orden inverso en el dominio *in-addr.arpa* (es decir, utiliza una notación de puntos invertida, algo lógico, ya que las redes se diferencian por los primeros valores de su dirección IP). Cada servidor de nombres de dominio autoritario requiere una zona de resolución inversa.



2 Servicio de nombres de dominio (DNS)

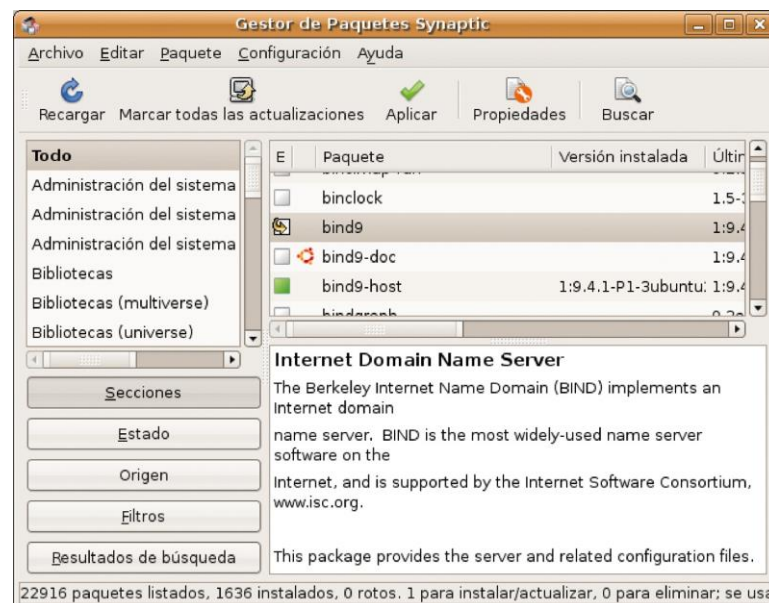
5. Instalación y configuración del servicio DNS en un servidor GNU/Linux

Para instalar el servicio DNS Bind9, hay que abrir el gestor de paquetes Synaptic (Sistema > Administración) y buscar *Bind9*. A continuación, se selecciona la instalación pulsando el botón derecho sobre la línea del paquete Bind9 y luego se pulsa en *Aplicar los cambios*.

El servicio DNS está compuesto por dos programas:

1.El dominio *named*: servidor de nombres de dominio que contiene la base de datos con información relativa a un segmento de la red y que responde a las peticiones.

2.El *resolver* (cliente): genera las peticiones. Se trata de un conjunto de rutinas que permiten que los clientes accedan a los servidores de nombres para resolver la búsqueda de una dirección IP asociada a un nombre.



En el directorio `/etc/bind/` se encuentra `named.conf` y el resto de archivos de configuración.

El archivo `named.conf` no se suele modificar. Las zonas específicas del servidor DNS que se configuran se definen en `/etc/bin/named.conf.local` y se incluyen al final de este archivo con un *include*.

Para lanzar el servicio debemos ejecutar la orden siguiente:

```
# /etc/init.d/bind9 start
```


2 Servicio de nombres de dominio (DNS)

6. Configuración de un servidor DNS secundario en Ubuntu GNU/Linux

Los servidores secundarios permiten descargar el tráfico DNS en redes en las que se consulte a menudo una zona.

Si el servidor primario o maestro se mantiene inactivo por alguna razón, el servidor secundario ofrecerá una resolución de nombres en esa zona mientras el primario no esté disponible.

Nombre de la zona secundaria

IP del servidor primario.

Indice de Módulo

Crear Zona Subordinada

Apply Configuration
Stop BIND

Opciones de nueva zona subordinada

Tipo de Zona ☒ Reenvío (Nombres a Direcciones) ☐ Inversas (Direcciones a Nombres)

Nombre de Dominio/Red

Archivo de Registros ☐ Ninguno ☒ Automático

Servidores Maestros

Puerto de Servidor ☒ Por defecto ☐ puerto

Crear

Indice de Módulo

Servidor de nombre Registros

Apply Zone
Apply Configuration
Stop BIND

En aulaSER.com

Añadir Registro Servidor de nombres

Nombre de Zona Tiempo de vida ☒ Por defecto ☐ segundos

Servidor de Nombres (Los nombres absolutos deben de terminar con un .)

Crear

Seleccionar todo. | Invertir selección.

Nombre	TTL	Servidor de Nombres
<input type="checkbox"/> aulaSER.com.	Por defecto	servidor.aulaSER.com.

Seleccionar todo. | Invertir selección.

Delete Selected

2 Servicio de nombres de dominio (DNS)

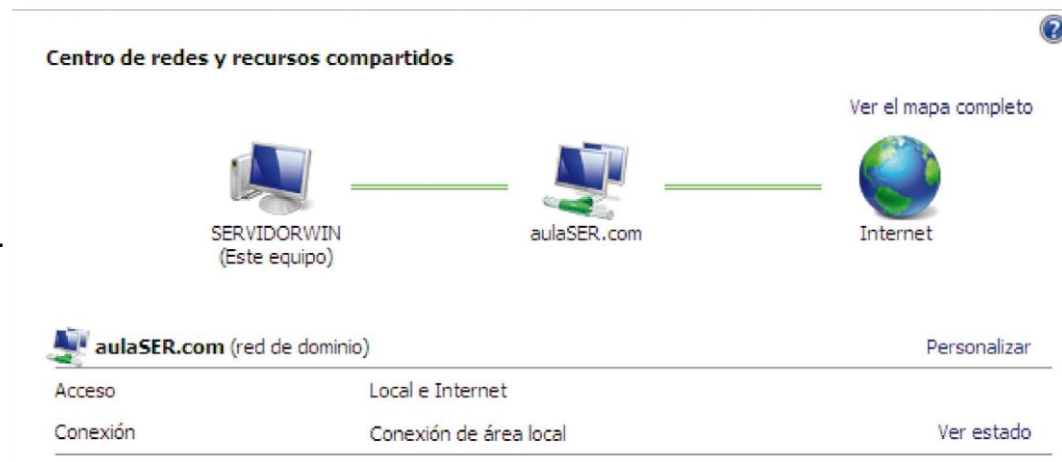
7. Configuración del servidor DNS con Windows 2008 Server

En Windows 2008, el servicio DNS, integrado en Active Directory, realiza las siguientes **funciones**:

- **Resolución de nombres, tanto directa como inversa**, siguiendo el esquema de funcionamiento explicado al principio de la unidad.
- **Integración de los nombres de dominio asignados por Active Directory y los nombres de dominio de DNS.** Ambos siguen la misma estructura jerárquica de nombres, aunque representan dos espacios de nombres distintos, ya que almacenan distinta información. No obstante, las máquinas y dominios DNS son los mismos que los de Active Directory.

Con la instalación de Active Directory tenemos ya definido el dominio raíz, además de haber instalado un controlador de dominio local. También se debe tener en cuenta que:

- El servidor se configura como el primer controlador de dominio de Active Directory de un nuevo bosque.
- Antes de instalar y configurar el servicio DNS, hay que revisar las conexiones de red.
- Para instalar el servicio DNS conviene tener una IP estática.



2 Servicio de nombres de dominio (DNS)

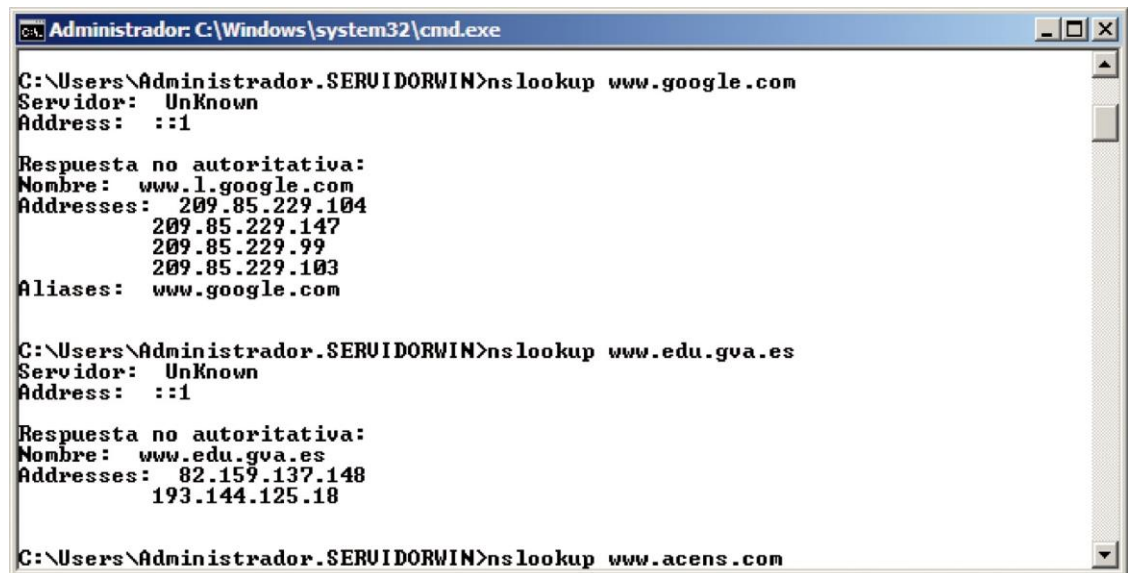
7. Configuración del servidor DNS con Windows 2008 Server

Una vez instalado el servicio, deberemos supervisar los registros de dirección, así como otras configuraciones DNS. La zona de búsqueda directa tiene el nombre del dominio creado al instalar Active Directory.

A continuación, crearemos la zona de búsqueda inversa en el servidor DNS.

Para comprobar que el servidor DNS funciona, abriremos un navegador web y escribiremos su URL, por ejemplo: **\\servidor.aulaSER.com**

Entonces ejecutaremos la orden `nslookup` para ver si, desde el servidor, se resuelven los nombres.



```
Administrador: C:\Windows\system32\cmd.exe

C:\Users\Administrador.SERUIDORWIN>nslookup www.google.com
Servidor: UnKnown
Address: ::1

Respuesta no autoritativa:
Nombre: www.l.google.com
Addresses: 209.85.229.104
           209.85.229.147
           209.85.229.99
           209.85.229.103
Aliases: www.google.com

C:\Users\Administrador.SERUIDORWIN>nslookup www.edu.gva.es
Servidor: UnKnown
Address: ::1

Respuesta no autoritativa:
Nombre: www.edu.gva.es
Addresses: 82.159.137.148
           193.144.125.18

C:\Users\Administrador.SERUIDORWIN>nslookup www.acens.com
```

2 Servicio de nombres de dominio (DNS)

8. DNS dinámico (DDNS)

Las siglas DDNS se refieren al concepto **Sistema Dinámico de Nombres de Dominio**, un mecanismo que permite la asignación de un nombre de dominio a una máquina con dirección IP dinámica.

A menudo el proveedor de Internet proporciona una IP pública dinámica a nuestro ordenador. De esta forma se impide que se transforme en un servidor DNS. Sin embargo, con un DNS dinámico se puede configurar un sitio web doméstico sin necesidad de utilizar un hosting externo siempre y cuando se mantenga activo el servidor durante las 24 horas del día.

DynDNS ofrece este servicio DDNS gratuitamente (www.dyndns.com).

Otra opción para este servicio es www.no-ip.com.

The screenshot shows the DynDNS.com website. At the top, there is a navigation bar with links for About, Services, Account, Support, and News. Below this, a large banner features a Yin-Yang symbol and the text "LIKE YIN AND YANG. Buy Custom DNS and get Domain Registration for just \$10." To the right of the banner, there is a section for "New to DynDNS.com?" with a "Take our new tour" button. Below this, there are sections for "DNS Services" (DNS for static and dynamic IP address) and "MailHop Services" (Ensure reliable email delivery). A search bar is located below these sections. At the bottom, there is a "News" section with a headline "Outage Causes Multiple Website Failures (DynDNS Customers Not Affected)". Below the news section, there are four columns of links: "Resources" (What is DNS?, DNS Tools, Home Solutions, Business Solutions), "Services" (DNS Hosting, Free Dynamic DNS, Email Relay, Domain Names), "Support" (DynStatus, Knowledge Base, 24/7 Premier Support, Update Clients), and "Follow Us" (Our News, Twitter @dyninc, LinkedIn, DNS Ninjas | Facebook). The footer contains copyright information and links for Legal Notices, Privacy Policy, and Contacts.

2 Servicio de nombres de dominio (DNS)

9. DNS con IPv6

Es importante que los servidores DNS sean capaces de hacer peticiones de resolución de nombres sobre ambos tipos, ya que no toda la infraestructura de DNS soporta IPv6, y debe asegurarse la compatibilidad con los servidores ya existentes.

Al ser DNS independiente del protocolo de transporte, las peticiones y respuestas pueden ser transmitidas sobre IPv6 o IPv4, independientemente del tipo de información transportada.

El servidor DNS BIND soporta IPv6 para GNU/Linux, y Windows DNS Server para plataformas Windows.

Habilitar la escucha del servidor por IPv6:

```
options {  
    directory "/var/named/";  
    listen-on-v6 { any; };  
};
```

Registros AAA:

Comprobamos que existe la zona de nuestro dominio `/var/lib/bind/aulaSER.com.hosts` y editamos el archivo.

Registros PTR:

Los ficheros de zona para resolución inversa de direcciones IPv6 contendrán solamente direcciones IPv6. En `/etc/named.conf` se declara la zona de resolución inversa correspondiente al prefijo.

Comprobación:

Comprobaremos que el servidor está escuchando en las direcciones IPv6 e IPv4 en el puerto 53 de DNS con `netstat -atunp`. Haremos consultas al servidor utilizando `dig any ipv6.aulaSER.com` o `dig any ipv4-ipv6. aulaSER.com`.

Doble pila (IPv4 e IPv6)

Para facilitar la transición se ha optado por el uso simultáneo de ambos protocolos, pero en pilas separadas



2 Servicio de nombres de dominio (DNS)

Créditos:

Autores del libro del alumno

Elvira Mifsud Talón y Raül V. Lerma-Blasco

Edición

Estudio177.com

Eugenia Arrés López

Isabel Bermejo

Miguel Montanyà