

UNIDAD 4

Servidor de nombres de dominio (DNS)

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 172.194.34.16 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 engoroso. 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 usuarios 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 de área	Código de la central	Código de abonado
	Madrid	Gran Vía	Secretaría de Cultura

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 en **nic.es**, integrado en **red.es**.

Espacio de nombres

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*.

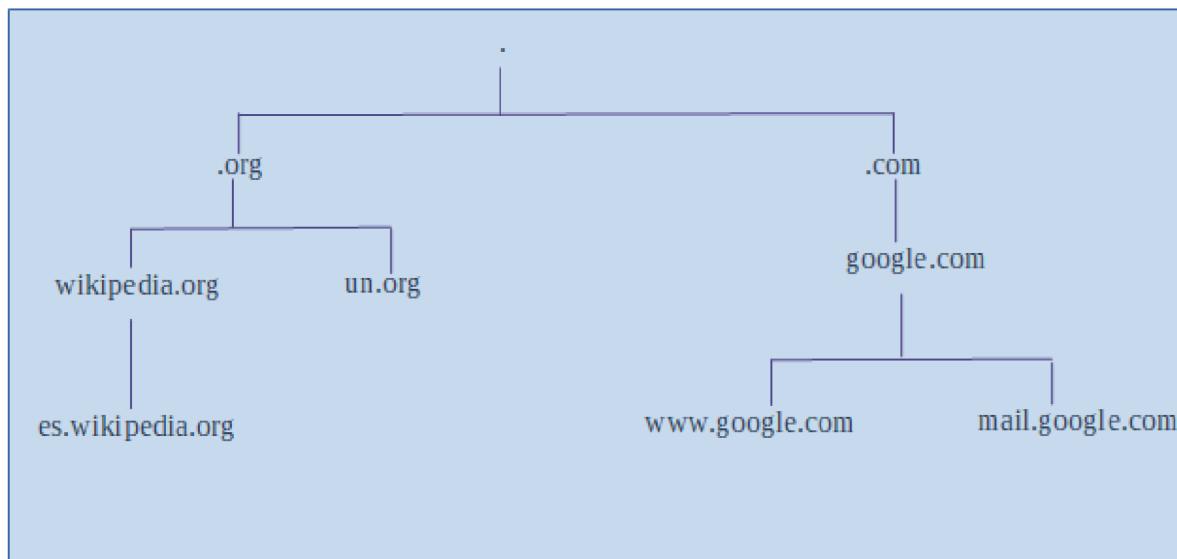
El nombre de dominio de un nodo se crea mediante la concatenación de todas las etiquetas, comenzando por dicho nodo y terminando con el nodo raíz. Para representarlo de forma escrita, unimos las etiquetas de derecha a izquierda separándolas por puntos, por ejemplo *www.google.com*. En el sistema DNS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

www	.wikipedia	.org	.
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.



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

ICANN, como se muestra en la anterior figura, 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 en próximas unidades.

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

FQDN (Fully Qualified Domain Name)

El término Fully Qualified Domain Name (FQDN) se refiere a la dirección completa y única necesaria para tener presencia en Internet. Está compuesta por el nombre de host y el de dominio y se utiliza para localizar hosts específicos en Internet y acceder a ellos mediante la resolución de nombres.

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

www.google.com.

Dominios genéricos

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 o 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:

Comparativa entre disponer o carecer del servicio DHCP		
TLD	Dominios	
Infraestructura	Utilizado para obtener el FQDN	.arpa
gTLD Dominios genéricos	(uTLD) No patrocinados. Éstos 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, museu.pro, .tel, .travel, .xxx
ccTLD Dominios geográficos	Creados por la 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.

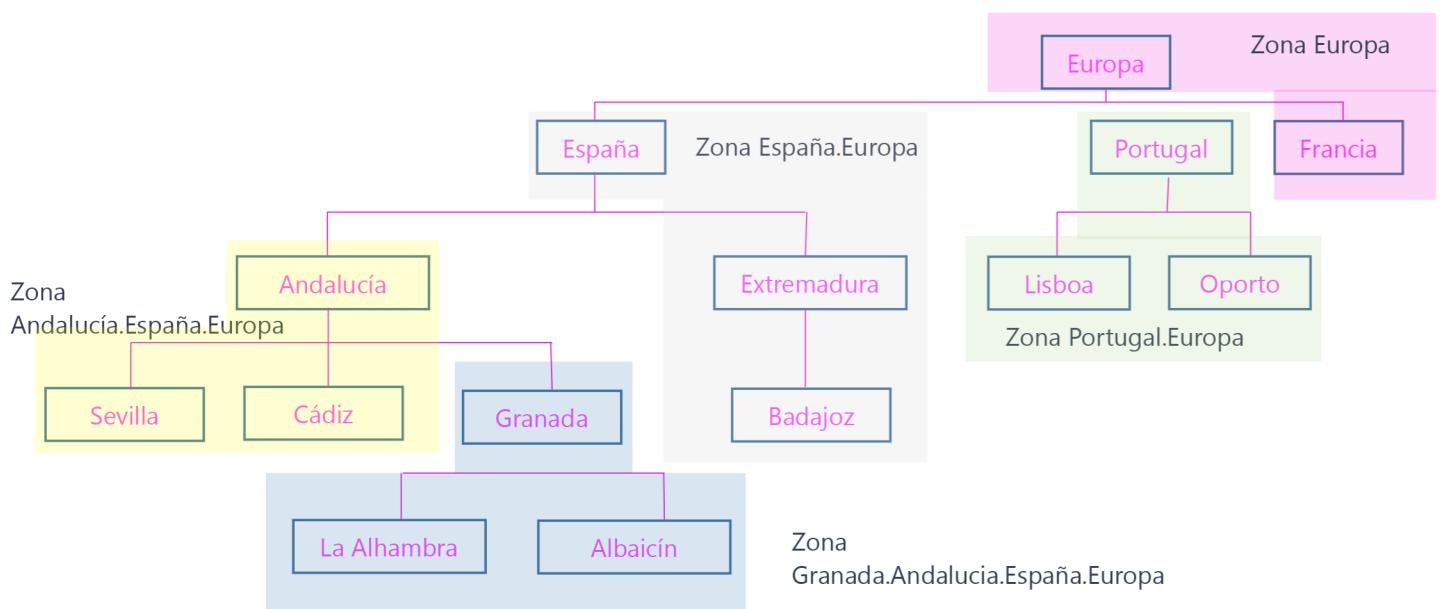
A partir del año 2004 ICANN preveía el permitir registrar dominios IDN (*internationalized domain name*) o nombres de dominio internacionalizados, que son los que contienen caracteres específicos de lenguas como el cirílico, el chino, el árabe, el griego, etc. Estos también posibilitan añadir acentos y registrar dominios con la letra “ñ”. En la práctica todavía no se pueden registrar.

1.3 Zonas

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.



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 la 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 contiene 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

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.

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.

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

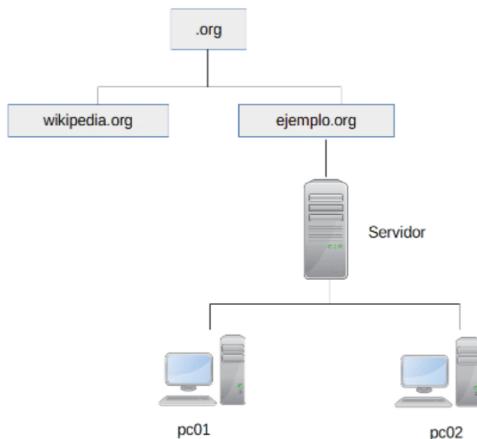
A pesar de que ICANN o su sección IANA supervisan la creación de dominios a través de empresas gestoras o de estados, no tienen capacidad técnica para gestionarlos. El modelo jerárquico DNS permite traspasarlos, en la mayoría de los casos, a su propietario. Esta operación se conoce como **delegación**.

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:



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

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.

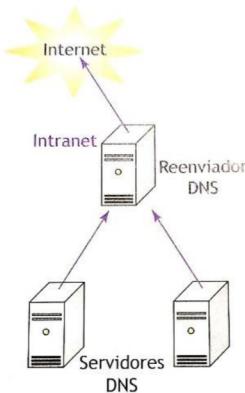
Comparativa entre disponer o carecer del servicio DHCP	
Aplicación	Transporte
DNS	TCP (53) UDP (53)

2.1 Clasificación de servidores de nombres

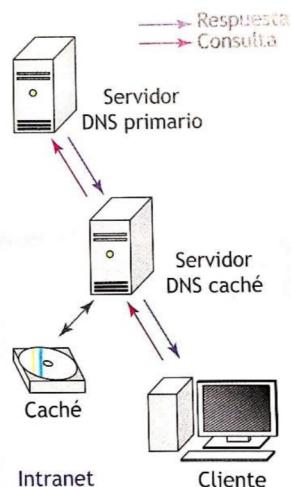
Los servidores de nombres son la parte más importante del DNS, ya que almacenan y gestionan información sobre los dominios y responden a las consultas de resolución de nombres que realizan los clientes. Estos servidores pueden implementarse sobre dispositivos dedicados o software ejecutado sobre máquinas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



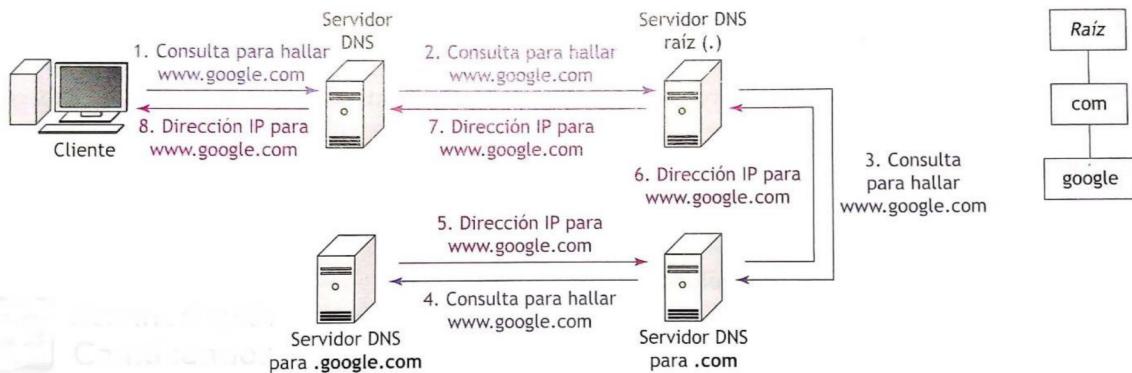
- **Caché:** este tipo de servidor almacena durante un periodo de tiempo los resultados de las consultas enviadas por él mismo a otros servidores, de forma que, si vuelve a recibir la misma petición, el servidor la devolverá desde su caché sin tener que realizar el proceso de consulta completo. Ese procedimiento 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.



2.2 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 en la figura siguiente se muestra una consulta recursiva reenviada por un servidor.



- **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.



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

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 esta 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 retrazos 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.

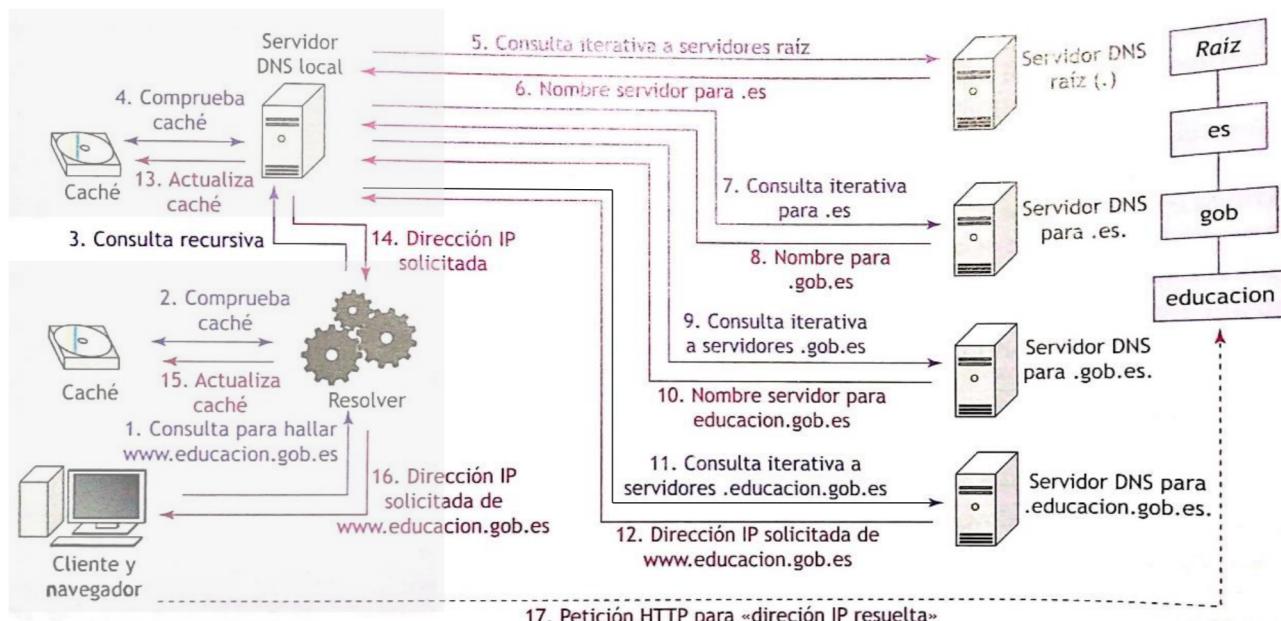
Resolución directa

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.

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 si 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.

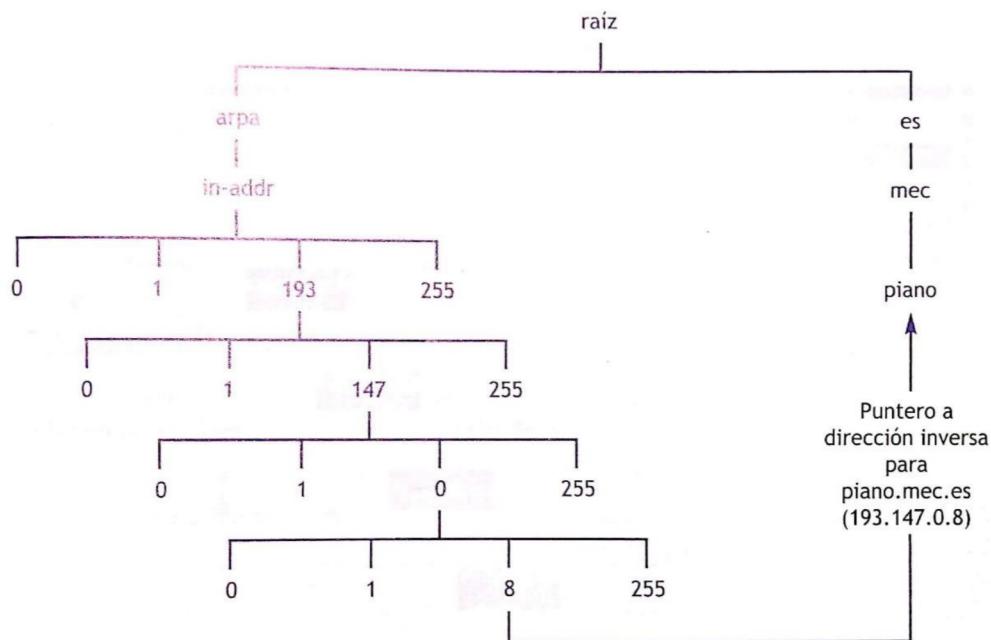


Resolución inversa

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*.



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 los siguientes:

- En el primer nivel dentro de *in-addr.arpa* existen 256 subdominios, desde el 0 al 255. Por ejemplo, *193.in-addr.arpa*.
- Dentro de cada subdominio de primer nivel hay 256 subdominios más de segundo nivel, organizados de la misma forma. Por ejemplo, *147.193.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*.

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

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.
- **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 (*Start of Authority*) (RR SOA), nombre de servidor (RR, NS), dirección (RR A), nombre canónico (RR CNAME), puntero (RR PTR) e intercambio de correo-e (RR MX).

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	IN	SOA	nsPrimario	admin.nsPrimario	(ops)	
jccm.es.	IN	SOA	dulcinea.jccm.es.	admincorreo.jccm.es.	(2021020700; 14400; 300; 604800; 7200);	Número de serie Actualización Reintentos 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.
 - o Número de serie: este número lo utilizan los servidores secundarios para saber si la copia que ellos tienen de la zona está o no actualizada. Los secundarios se actualizan si el número que tienen es menor que el del primario. El esquema que se suele seguir es YYYYMMDDnn, es decir, YYYY es año, MM el mes, DD el día, nn el número de actualización de ese día.
 - o Actualización: indica cada cuanto tiempo deben los secundarios contactar al primario para comprobar si se ha actualizado la zona.
 - o Reintento: indican cada cuanto tiempo deben los secundarios reintentar una actualización de zona.
 - o Expiración: indica el tiempo, en segundos, durante el cual un secundario puede estar sin contactar con el primario para comprobar la zona.
 - o TTL: indica el tiempo durante el cual se debe almacenar en la caché una respuesta negativa de cualquier otro servidor.

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 quearía así:

(2021020700 4h 5m 1w 2h)

Actividad propuesta

1. Usando el programa *dig*, obtén el SOA de *google.com* ¿Cada cuánto tiempo se actualizan los servidores secundarios? ¿A quién habría que enviar un correo en caso de problemas con el dominio?
2. Usando el programa *whois* averigua a qué teléfono hay que llamar en el caso de que tengamos un problema con el dominio *dreamhost.com*
3. Utilizando el mismo comando, ¿podemos averiguar a quién hay que avisar para el dominio *albaytar.es*? Si con el comando no funciona, lo puedes descubrir por otros medios.

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	Valor	Nombre servidor
jccm.es.	IN	NS	dulcinea.jccm.es.

Actividad propuesta

4. Usando el programa *dig*, obtén las entradas NS de *google.com* ¿Cuántos servidores existen para esa zona?

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 inversa.

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	IN	A	IP
dulcinea.jccm.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.jccm.es.	IN	CNAME	www.edu.jccm.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 Junta de Castilla-La Mancha tanto como www.edu.jccm.es como ftp.edu.jccm.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 (FQDN). 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.jccm.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 puntero (RR PTR)				
NombreDominio	Tipo	MX	num	Servidor correo
mail.jccm.es.	IN	MX	10	gollum.jccm.es.

Ejemplo de base de datos DNS

redes.com.	IN SOA	ns.redes.com.
		admin-redes@gmail.com. (
		2007030702 ; Número de serie
		86400 ; Refresco
		7200 ; Reintento
		2592000 ; Expiración
		172800) ; Ttl
redes.com.	IN NS	ns.redes.com.
redes.com.	IN MX	mailhost.redes.com.
ns.redes.com.	IN A	193.147.184.6
mercurio.redes.com.	IN A	193.147.184.7
venus.redes.com.	IN A	193.147.184.8
tierra.redes.com.	IN A	193.147.184.9
marte.redes.com.	IN A	193.147.184.9
www.redes.com.	IN CNAME	mercurio.redes.com.
mailhost.redes.com.	IN CNAME	venus.redes.com.
gestion.redes.com.	IN NS	ns.gestion.redes.com.
sistemas.redes.com.	IN NS	ns.sistemas.redes.com.
ns.gestion.redes.com.	IN A	212.135.11.45
ns.sistemas.redes.com.	IN A	212.146.13.145

Ejemplos de uso del comando dig

En la siguiente dirección tenéis ejemplos interesantes:

<https://rm-rf.es/como-usar-el-comando-dig-ejemplos/>

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 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.

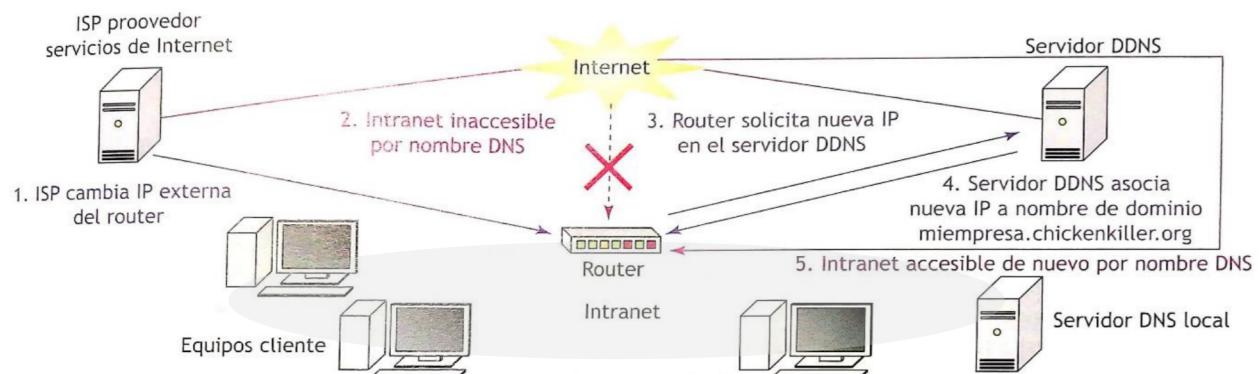
Acceso desde Internet

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 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 *duckdns*, 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.



Acceso desde un servidor DNS local

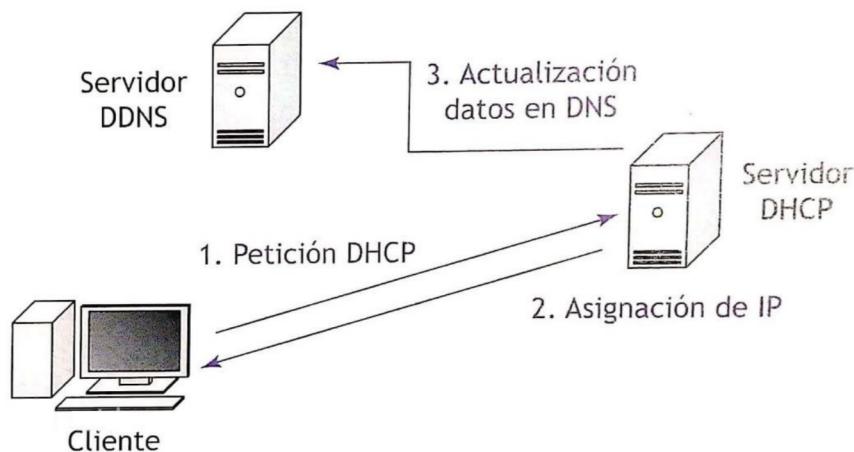
En una red local donde se añaden continuamente equipos nuevos o se modifica su nombre, es necesario actualizar la información que administra el servidor DNS de la zona local; en particular, la dirección IP y/o el nombre de dominio.

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.

Simplificando el proceso, los pasos que realiza se describen a continuación:

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.



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.

4. DNS en sistemas Linux

Hoy es un día importante, vuestra primera jornada de trabajo en la empresa CieloAzul. 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 CieloAzul 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 éstos 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: cieloazul.com.

Atendiendo a estas condiciones y después de estudiar y comparar diferentes opciones, se ha 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.

4.1 Instalación del servidor

Para instalar el servidor DNS, se deben 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 (Reload)* para actualizar la lista de paquetes disponibles en los repositorios de Internet que tienes configurados. Espera unos segundos mientras termina el proceso.
4. Haz clic sobre el botón *Buscar (Search)* para acceder a la herramienta de búsqueda.

5. Escribe *bind9* en el cuadro de texto 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 clic en la casilla de verificación que está delante del nombre del paquete seleccionado y haz clic en *Mark for Installation*.
8. Asegúrate de que la casilla de verificación del paquete *bin9* está marcada y haz clic sobre el botón *Aplicar* para iniciar el proceso de instalación.
9. 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*.
10. Haz clic sobre el botón *Cerrar* del diálogo *Cambios realizados*.
11. Haz clic en el botón *Cerrar* de la ventana Synaptic.

4.2. Configuración del servidor

Antes que nada, es importante configurar el servidor con una IP fija puesto que es la manera correcta de actuar. Es evidente de que nuestro servidor tiene una IP fija ya que así lo hemos configurado, pero vamos a informar a Webmin de esta configuración. Para ello nos vamos a *Red-interfaces de red*. Elegimos la tarjeta correspondiente (comprobad que la tarjeta que aparece es la de la red interna, sino tendréis que darla de alta) y la configuraremos con la IP fija 192.168.10.2 y la máscara correspondiente. No olvidar aplicar la configuración en *Configuración de red*.

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.

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 haya 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 *Reajusta Módulos* 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*.

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 la empresa 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* del menú principal.
2. Haz clic sobre enlace *Crear una nueva zona maestra*.
3. Introduce *cieloazul.com* en el campo *Nombre de Dominio/Red*.
4. Escribe *adminservidor@cieloazul.com* en *Dirección de correo*.
5. Haz clic sobre el botón *Crear*.
6. Al crear la zona se abre la ventana *Editar Zona Maestra*. Haz clic sobre el enlace *Regresar al Índice del módulo*, arriba a la izquierda.
7. Haz clic en el enlace *Aplicar Configuración* para guardar los cambios; este se halla en la esquina superior derecha del índice de módulo.

Archivo de declaración de zonas locales

/etc/bind/named.conf.local

Archivo de declaración de la zona cieloazul.com

/var/lib/bind/cieloazul.com.hosts

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* en la sección *Zonas DNS Existentes*.
3. Introduce los datos tal y como aparecen en la siguiente figura, sin olvidar seleccionar la opción *Inversas* en el control *Tipo de zona*.

Opciones de nueva zona maestra	Crear Zona Maestra	Apply Configuration	
Tipo de zona	Reenvío (Nombres a Direcciones) <input checked="" type="radio"/> Inversas (Direcciones a Nombres) <input type="radio"/>	Stop BIND	
Nombre de Dominio/Red	192.168.10		
Archivo de Registros	Automático <input checked="" type="radio"/>		
Servidor Maestro	ubuntuserver.	¿Añadir registro NS para servidor maestro?	
Dirección de correo	adminservidor@cieloazul.com		
¿Utilizar plantilla de zona?	Si <input checked="" type="radio"/> No <input type="radio"/>	Dirección IP para registros de plantilla	
Add reverses for template addresses?	Si <input checked="" type="radio"/> No <input type="radio"/>		
Tiempo de refresco	10800 segundos	Tiempo de reintento de transferencia	3600 segundos
Tiempo de expiración	604800 segundos	Tiempo que está viva por Defecto	38400 segundos

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

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 192.168.10 es:
 /var/lib/bind/192.168.10.rev

Creación de un registro de dirección

Ahora vas a añadir un registro de dirección (RR A) a la zona de resolución directa cieloazul.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 cieloazul.com. Haz clic sobre él.
3. A continuación, haz clic en el ícono *Dirección*.
4. Una vez has accedido a la ventana *Dirección Registros*, teclea ubuntuserver en el cuadro de texto *Nombre*.
5. Escribe la dirección IP del servidor, *192.168.10.2*, en el campo de texto *Dirección*.
6. Comprueba que se encuentra seleccionada la opción Sí del control *¿Actualizar inversas?*
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 han añadido. Como este es el primero que añades, solo aparece ubuntuserver.
9. Accede al enlace *Regresar al índice del módulo*.
10. Haz clic en *Aplicar configuración* del índice de módulo para guardar los cambios.

Ahora solo queda añadir los registros para el resto de los equipos de la red de la misma forma (cliente1, cliente2, cliente3, cliente4).

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

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

1. Inicia Webmin y haz clic sobre el enlace *Servidor de DNS BIND* de la sección *Servidores* del menú principal.
2. Accede a la zona *cieloazul.com*
3. Haz clic sobre el ícono *Alias de Nombre*.
4. Teclea *www* en el campo *Nombre*.

5. Escribe *ubuntuserver.cieloazul.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.
6. Haz clic sobre el botón *Crear*.
7. Puedes observar que, al hacer clic en el botón, aparece una lista con los registros ya añadidos.
8. Accede al enlace *Regresar al índice del módulo* para volver al menú principal de *Servidor de DNS BIND*.
9. Haz clic en *Aplicar configuración* para guardar los cambios.

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. Inicia Webmin en el navegador web y accede al enlace *Servidor de DNS BIND* de la sección *Servidores* del menú principal.
2. Accede a la zona *cieloazul.com*
3. Haz clic sobre el ícono *Servidor de Correo*.
4. Una vez has accedido a la ventana *Servidor de correo*, teclea *mail* en el cuadro de texto *Nombre*.
5. Escribe el nombre FQDN del servidor de la empresa en el campo de texto *Servidor de correo*, es decir, *ubuntuserver.cieloazul.com*.
6. 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.
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.
9. Accede al enlace *Regresar al índice del módulo*.
10. Haz clic en *Aplicar configuración* del índice de módulo para guardar los cambios.

Arranque del servicio

Desde la instalación y durante todo el proceso de configuración, el servicio 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 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.

A veces no funciona bien utilizar Webmin para parar y arrancar servicios. Entonces debemos usar línea de comandos para que todo funcione. En el caso del servidor DNS los comandos que se usan son:

- `service bind9 status`: comprobar el estado del servicio.
- `service bind9 stop`: detener el servicio.
- `service bind9 start`: iniciar el servicio.
- `service bind9 restart`: reiniciar el servicio.

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 los pasos para configurar el DNS de un cliente:

1. Arranca el cliente y accede.
2. Haz clic en el *Gestor de red* y elige la opción *Editar las conexiones* (botón derecho).
3. Accede a la pestaña *Cableada*, elige *Conexión cableada 1* y haz doble clic.
4. Selecciona la pestaña *Ajustes de IPv4* y pon en el campo *Servidores DNS* el valor *192.168.10.2*.
5. En el campo *Dominios de búsqueda* escribir *cieloazul.com*. Así no habrá que escribir todo el dominio.
6. Haz clic sobre el botón *Guardar* y después en *Cerrar*.

Archivo de configuración del cliente DNS

/etc/resolv.conf

Resolver en Linux

En los sistemas 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

Para comprobar que funciona correctamente puedes utilizar la orden *ping* con alguno de los nombres añadidos a la base de datos del DNS, desde los clientes.

También puedes, si está activo el servidor HTTP, poner el nombre del servidor en el navegador desde los clientes.

Finalmente, para comprobar más en profundidad el funcionamiento, tienes que probar las órdenes de resolución que están en el fichero correspondiente del classroom.

4.4 Configuración de un DNS secundario

Los servidores secundarios son necesarios por dos razones. En primer lugar, porque permiten descargar el tráfico de consultas DNS en redes en las que se consulta a menudo en una zona. En segundo lugar, si el servidor primario o maestro está inactivo por algún motivo, el servidor secundario ofrecerá resolución de nombres en esa zona mientras el primario no esté disponible.

El servidor secundario debe estar físicamente en una máquina diferente y debidamente actualizado para ofrecer el servicio en condiciones. Es decir, todos los cambios que se realizan en la zona del maestro deberán replicarse en el secundario de la zona a través de la transferencia de zona.

Para llevarlo a cabo vamos a clonar el servidor *ubuntuserver* y le vamos a cambiar el nombre por el de *secundario*. Después, en el secundario, vamos a borrar completamente (purgar) el paquete de servicio DNS, lo vamos a instalar otra vez y lo vamos a configurar como secundario.

Clonar el servidor *ubuntuserver*

Para hacerlo debemos seguir los siguientes pasos:

1. Irnos a VirtualBox, y con las máquinas cerradas elegimos la máquina *ubuntuserver*.
2. Le damos a botón derecho y pulsamos en *Clonar*.
3. Le ponemos el nombre *secundario*.
4. Marcamos en la lista desplegable *Generar nuevas direcciones MAC de todos los adaptadores de red*.
5. En la siguiente pantalla elegimos *Clonación completa*, para poder arrancar los dos servidores a la vez.

Cambiar el nombre de la máquina clonada

Hasta ahora sólo le hemos cambiado el nombre en VirtualBox. Podemos comprobar que la máquina clonada tiene el mismo nombre que la original utilizando la orden *hostname*.

Tenemos que cambiárselo también en la propia máquina. Para eso seguimos los siguientes pasos:

1. Vamos al fichero */etc/hostname* y cambiamos el nombre de *ubuntuserver* por *secundario*.
2. Luego abrimos el fichero */etc/cloud/cloud.cfg* y buscamos una línea que pone *preserve_hostname: false*. Cambiamos *false* por *true*, y guardamos el fichero.
3. Finalmente cambiamos el nombre a la máquina con la orden:
`sudo hostname secundario`
4. Reiniciamos la máquina y ya está.
5. Para comprobarlo, cuando se reinicie la máquina podemos poner *hostnamectl*. Nos mostrará el nombre, si lo hemos hecho bien, y más información.

Cambiar la configuración de red

La máquina clonada tiene la misma configuración que la máquina original. Por eso vamos a tener que cambiar la configuración de la red. Para ello seguimos los siguientes pasos:

1. En la configuración de la máquina en VirtualBox vamos a poner la primera tarjeta en modo *adaptador puente*. La idea es que nuestra máquina virtual sea como una máquina

real más dentro de la red.

2. Entramos en la máquina y en la configuración de la primera tarjeta ponemos IPv4 Manual, dirección IP: le sumamos 100 a la del anfitrión (si es la 192.168.1.101 ponemos 192.168.1.201), máscara 255.255.255.0, puerta enlace: 192.168.1.1, DNS: 8.8.8.8). Puede que esa dirección esté ocupada en la red y no funcione. Comprueba que no está siendo utilizada, y si es así, elige la siguiente dirección libre. (¿Cómo comprobaríamos que no está siendo utilizada?).
3. Apagamos y encendemos la conexión de la tarjeta. Ya tendremos Internet.

En cuanto a la segunda tarjeta, la que nos da acceso a la red interna, cambiamos la IP por 192.168.10.3. Apagamos y encendemos también esta tarjeta. Para comprobar si está dentro de la red interna puedes hacerle ping desde algún cliente.

Reinstalar el paquete bind9

Procedemos a desinstalar, y purgar, el paquete bind9. Es para evitar conflictos pues al clonar el servidor tenemos también la configuración de bind9 y eso podría darnos conflictos. Para eso ponemos la orden:

```
sudo apt-get remove --purge bind9
```

Con esto quita el paquete, los enlaces y los archivos de configuración. Si no ha podido borrar los ficheros de configuración los borramos a mano (nos da un mensaje si no ha podido).

Ahora volvemos a instalar *bind9* con el método que elijamos.

Entramos en Webmin, reajustamos módulos y comprobamos que el servidor DNS está totalmente limpio.

Configurar servidor secundario

Seguimos los siguientes pasos:

1. Como hemos hecho con el servidor primario, ponemos los valores de IP y red en Webmin (elegid la tarjeta adecuada y si no está creada pues crearla).
2. Vamos a hacer que los propios servidores hagan de clientes DNS. Para ello nos vamos a *Red-Configuración de red*, a la sección *Hostname y cliente DNS* y ponemos como servidor DNS su propia dirección IP y como DNS secundario al secundario. En los dominios de búsqueda ponemos cieloazul.com. En el segundo servidor hacemos lo mismo, pero con las direcciones cambiadas. No olvidar guardar la configuración y aplicarlas.
3. Luego nos vamos al primer servidor y en el servidor DNS, en la zona cieloazu.com añadimos como nuevo servidor de nombres a *secundario.cieloazul.com*. (no olvidar el punto final).
4. En la sección de direcciones añadimos la dirección correspondiente al segundo servidor.
5. En la lista de zonas vamos a configurar la zona de resolución inversa. Nos metemos en ella y añadimos al servidor de nombre secundario. (no hace falta introducir nada en el nombre de zona pues Webmin lo adivina). Podemos revisar todos los registros que tenemos en la zona con el botón *Todos los tipos de registro* en *Editar Zona Maestra*. Podemos comprobar si todo va bien.
6. Ahora que tenemos todo configurado en el servidor principal nos podemos ir al servidor

secundario. Lo primero es *crear una nueva zona subordinada*. Crearemos una zona de resolución directa que será *cieloazul.com*. (no olvidar el punto final). Le indicamos que nuestro servidor maestro corresponde con la dirección 192.168.10.2. Le damos a crear y a aplicar cambios. Nos aparecerá la zona secundaria (o subordinada) creada. En este caso al pasar el puntero del ratón por encima no cambiará a azul, sino a verde. También podemos ver que no se ha transferido ningún registro desde la zona principal. De todas formas, comprobamos que puede realizar la transferencia mediante el botón *Prueba de transferencia de zona*. El sistema nos indica que falla pues falta el comando *dig*. Lo arreglamos instalando el paquete *dnsutils* utilizando Webmin. Para ello nos vamos a *Sistema-Paquetes de Software*, y buscamos el paquete y lo instalamos (lo podemos buscar por APT). Una vez instalado probamos de nuevo si la zona se puede transferir. Si todo ha ido bien nos dice que ha podido realizar el test de transferencia.

7. Hay que tener claro que hasta ahora no ha habido ninguna transferencia efectiva, ya que en el servidor secundario no están los registros del primario de forma automática. Probamos a aplicar los cambios y a reiniciar bind9. Una vez reiniciado, y si la transferencia no ha tenido lugar es interesante realizar un status. Puede que al hacerlo veamos que hay un error en el que nos indica que no es posible realizar la transferencia por un problema de permisos. Lo que sucede es que al intentar bind utilizar el fichero de zonas (*/var/lib/bind/cieloazul.hosts*) no puede pues no es el propietario, ya que es root. Lo mismo sucede con el fichero del servidor secundario. La solución es sencilla, cambiar el propietario de ambos ficheros a bind:bind (propietario y grupo). Eso tenéis que averiguar cómo hacerlo.
8. Una vez solucionado el problema reiniciáis ambos servidores y al secundario se le habrá transferido la zona del primario. Lo podemos ver porque en el servidor secundario se habrán añadido los registros del primario. Además, nos muestra cuándo se ha realizado la última transferencia.
9. Nos vamos al servidor secundario y creamos una zona subordinada de resolución inversa. En el nombre de dominio ponemos 192.168.10 y en los servidores maestros ponemos 192.168.10.2. Si se nos produce un error por fallar un comando NDC es porque todavía no hemos establecido la configuración del RNDC. Sirve para configurar el acceso de control remoto del demonio del servidor DNS. Para ello nos vamos a *Servidor de DNS BIND*, y le damos al botón *Configurar RNDC*. Lo único que tenemos que hacer es decirle que sí, y aplicar la configuración. Ahora nos vamos a la zona inversa y vemos que ha recibido los registros del servidor maestro (si no los ha recibido igual es que tienes que reiniciar el servidor).
10. Podemos hacer que las actualizaciones del servidor maestro se propaguen a los servidores esclavos. Para ello nos vamos a la lista de zonas y en los valores por defecto de zona marcamos en *¿Notificar a las subordinadas acerca de los cambios?* Ahora cualquier cambio que se realice en el servidor primario, como agregar un alias, se propagará al secundario.

Caso práctico 1: instalación y configuración de un servidor DNS en Ubuntu Server

Peso: 20% de la nota de la unidad.

Objetivo

Instalar y configurar el servicio DNS en un servidor de Linux.

Consideraciones

Si has ido siguiendo los pasos que se muestran en la unidad ya tienes hecha esta práctica.

Evaluación

Para que el profesor compruebe que has realizado la práctica de forma satisfactoria, el profesor tendrá en cuenta:

- Que el proceso que ejecuta el servidor está en funcionamiento. Puedo preguntar que muestres el proceso que lo está ejecutando.
- Que el puerto que utiliza el servidor está operativo. Puedo preguntar que muestres el puerto que está siendo utilizado por el servicio.
- Que, al realizar pruebas desde el propio servidor, y desde un cliente, con las órdenes específicas, el alumno sabe utilizarlas y funcionan correctamente.
- Que se conocen los ficheros de configuración y su contenido.

Calificación

Para establecer la nota en la práctica se sumará:

- La observación directa del profesor (entre 0 y 2 puntos).
- El correcto funcionamiento del servidor (entre 0 y 5 puntos).
- La exactitud de las respuestas a las preguntas del profesor (entre 0 y 3 puntos).

Caso práctico 2: instalación y configuración de un servidor DNS secundario en Ubuntu Server

Peso: 25% de la nota de la unidad.

Objetivo

Instalar y configurar el servicio DNS en un servidor secundario de Linux.

Consideraciones

El proceso se realiza sobre la máquina virtual Ubuntu Server que has creado en tu ordenador con la IP que te corresponda. Los pasos son los que vienen en la unidad.

Puedes probar su funcionamiento ya que puedes realizar consultas desde los clientes, e incluso desde los servidores, a un servidor o a otro.

También puedes probarlo agregando un alias al servidor principal y que se propague al secundario.

Y una forma más de probarlo es haciendo que se pare el servidor primario y entonces las consultas las debe de resolver el secundario.

Evaluación

Para que el profesor compruebe que has realizado la práctica de forma satisfactoria, el profesor tendrá en cuenta:

- Que el proceso que ejecuta el servidor está en funcionamiento.
- Que el puerto que utiliza el servidor está operativo.
- Que los cambios que se realizan en el primario se propagan al secundario.
- Que cuando se detiene el servidor primario y se le realiza una consulta la resuelve el secundario (es lo más importante).
- Que, al realizar pruebas desde el propio servidor, y desde un cliente, con las órdenes específicas el alumno sabe utilizarlas y funcionan correctamente.
- Que se conocen los ficheros de configuración y su contenido.

Se valorará también:

- Que el servidor permite realizar consultas desde un ordenador externo correctamente. Para ello se puede comprobar con el ordenador de un compañero. El profesor lo testeará en su propio ordenador introduciendo los valores que le indique el alumno.

Calificación

Para establecer la nota en la práctica se sumará:

- La observación directa del profesor (entre 0 y 2 puntos).
- El correcto funcionamiento del servidor secundario (entre 0 y 3 puntos).
- La exactitud de las respuestas a las preguntas del profesor (entre 0 y 5 puntos).