SERVICIO DNS

Servicio DNS (Domain Name System)

El sistema de nombres de dominio DNS (Domain Name System) proporciona un mecanismo eficaz para llevar a cabo la resolución de nombres de dominio a direcciones IP.

El servicio DNS no sólo permite hacer la resolución de nombres de dominio a direcciones IP, sino también la resolución inversa. Es decir, a partir de una IP averiguar el nombre de dominio.

El servicio DNS proporciona independencia del nombre de dominio respecto a la IP.

Sistemas de nombres planos y jerárquicos

El problema de la identificación de equipos se produce desde el principio de la existencia de las redes de ordenadores y no es algo específico de TCP/IP. Hacía falta un *lenguaje humano* para realizar esta identificación.

En los albores de las redes, cuando ARPANET (la red predecesora de Internet), los nombres los equipos se centralizaban en un archivo llamado host.txt (/etc/hosts en Linux), que incluía el nombre del equipo y su IP. Esto es lo que se conoce como un ***sistema de nombres plano***. Puede ser adecuado para redes pequeñas pero no es escalable ni práctico en redes grandes y mucho menos en Internet.

Sistemas de nombres planos y jerárquicos

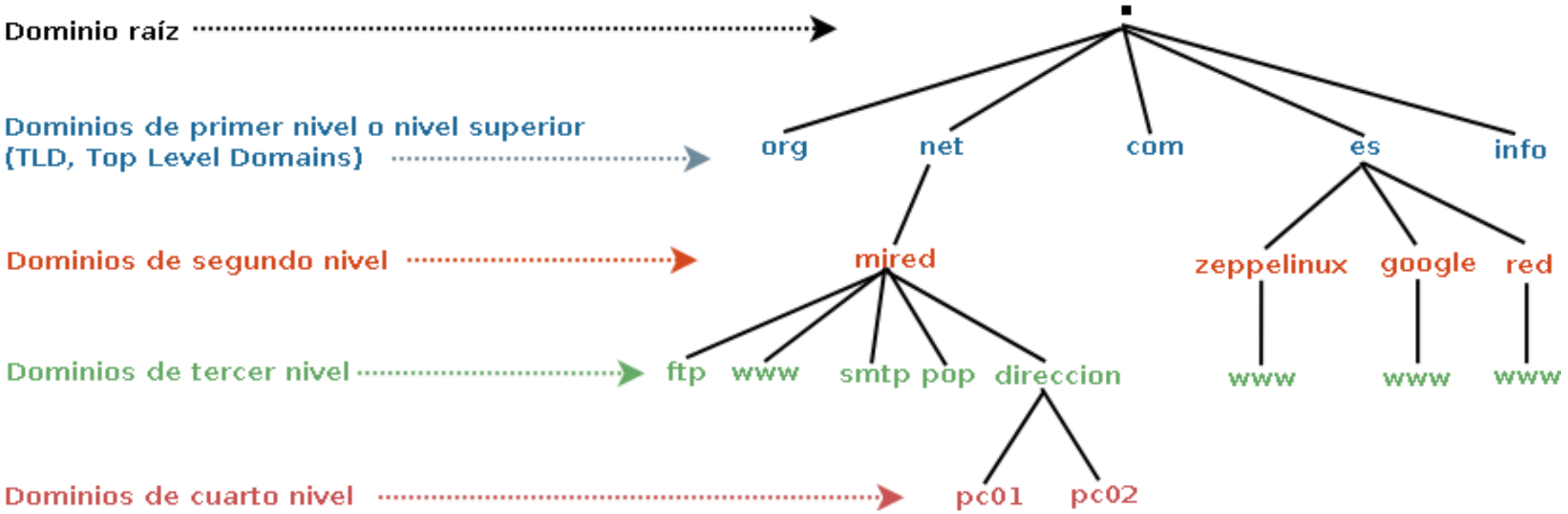
```
[root@portatil ~]# cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1     localhost.localdomain   localhost   localhost
::1           localhost6.localdomain6 localhost6
192.168.1.1   router routerWF
192.168.1.31  server1   escriptori  pare
192.168.1.32  estacio1  dormitori   mare
192.168.1.33  estacio2  nen         jocs    supercrac
```

Elementos del sistema de nombres de dominio

- El espacio de nombres
- Nombres de dominio
- Dominios raíz
- Dominios y subdominios

El **espacio de nombres de dominio** está formado por los nombres válidos utilizados para identificar servicios o máquinas en una red. Se puede representar mediante una **estructura jerárquica de topología arbórea**, es decir, todos los nombres forman un árbol invertido donde cada nodo se separa de los otros nodos por un punto

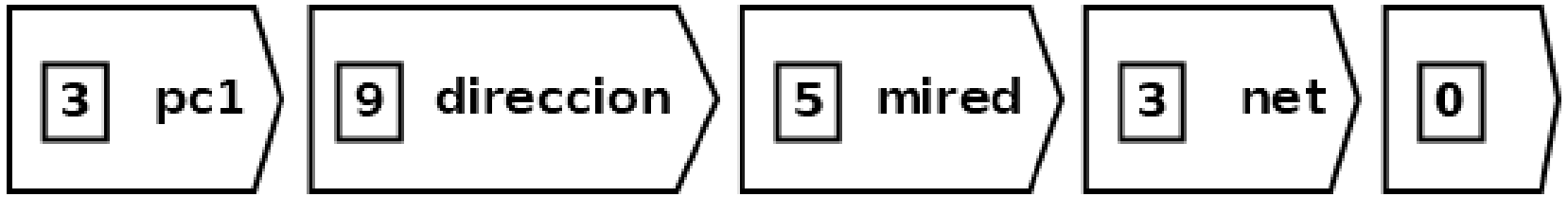
Elementos del sistema de nombres de dominio



Elementos del sistema de nombres de dominio

Los nombres de dominio pueden estar formados por una o más cadenas de caracteres separadas por puntos y no se distingue entre mayúsculas y minúsculas. Por ejemplo, www.deaw.es. es lo mismo que WWW.deaw.ES..

Los nombres de dominio se expresan como secuencias de **etiquetas (labels)**.



Ejemplo de nombre de dominio:
pc1.direccion.mired.net.

Elementos del sistema de nombres de dominio

Dominios raíz

En teoría, todos los dominios deben de terminar con un punto (.). Es así porque el árbol de nombres de dominio (espacio de nombres de dominio) empieza con el dominio . que se conoce como dominio raíz (root).

Un dominio se lee de derecha a izquierda, empezando por el punto ., aunque en la práctica lo hacemos de izquierda a derecha. El punto inicial, generalmente se omite ya que los programas lo añaden por defecto y es meramente formal.

Elementos del sistema de nombres de dominio

Dominios y subdominios

Como consecuencia de la organización jerárquica del espacio de nombres de dominios, podemos utilizar los términos dominio y subdominio. Por ejemplo, deaw.es. es un subdominio del dominio es. y www.deaw.es. es un subdominio del dominio deaw.es..

Los dominios o subdominios que cuelgan del dominio raíz . se conocen como dominios de primer nivel o dominios de nivel superior (Top Level Domains, TLD), los que cuelgan de los dominios TLD se denominan dominios de segundo nivel y así sucesivamente

Zonas

Una zona es una porción del espacio del espacio de nombre de dominio en el DNS cuya responsabilidad administrativa recae sobre un único responsable.

Los servidores que gestionan la zona tienen información completa sobre ella y se dice que son autorizados para esa zona.

Las **zonas** se almacenan en **archivos de texto** o en **bases de datos**, según el tipo de software que se utilice para montar el **servidor DNS** y de como se configure.

Zonas

```
...
deaw.es.          IN NS      ns1.deaw.es.
ns1.deaw.es.      IN A       192.168.1.20
natos.deaw.es. IN    A       192.168.1.21
waor.deaw.es.     IN A       192.168.1.22
www.deaw.es.      IN CNAME   natos.deaw.es.
ftp.deaw.es.      IN CNAME   waor.deaw.es.
...
```

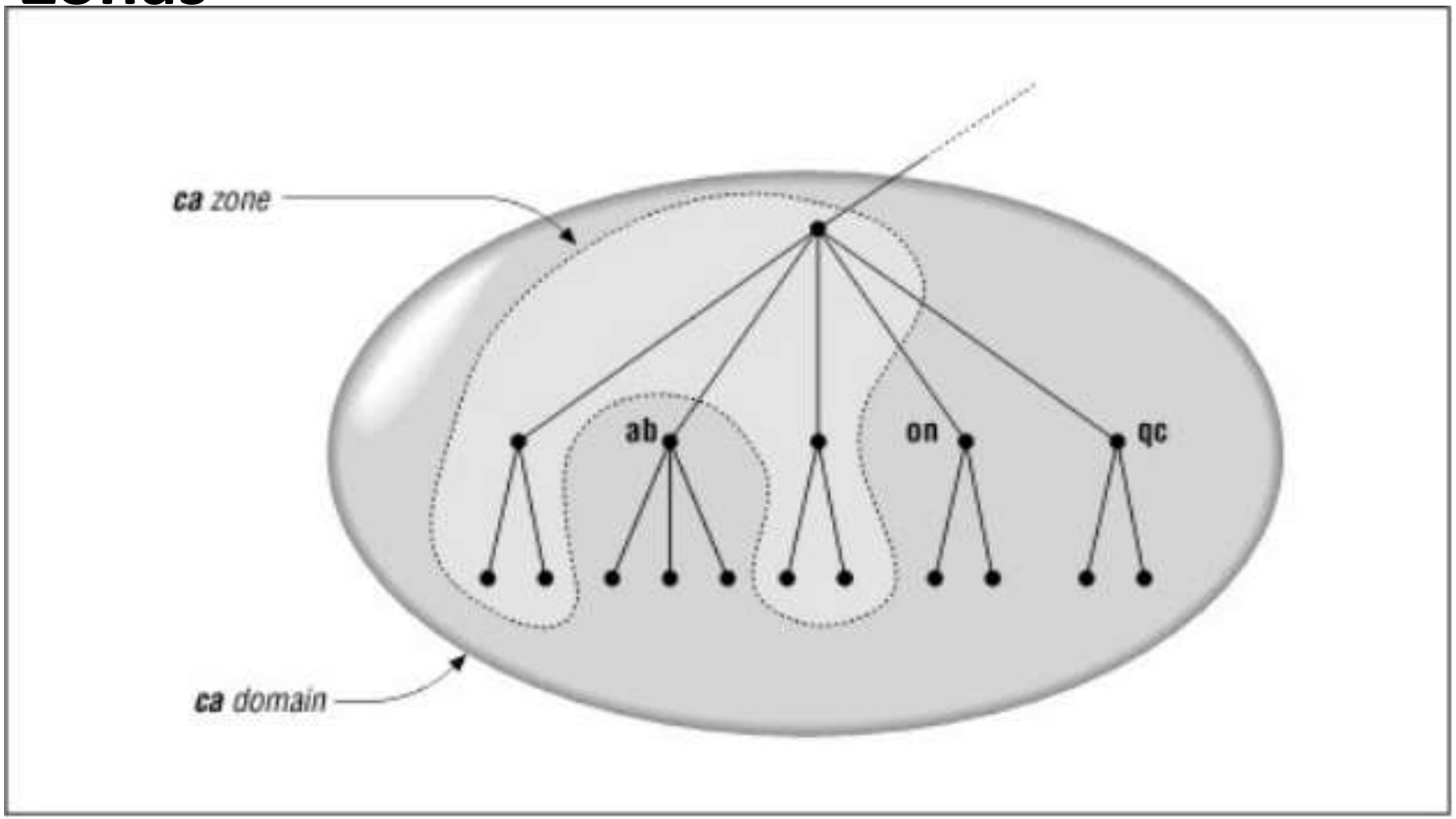
A cada una de las líneas del fichero se las conoce como registros de recurso (RR: Resource Records) y definen los tipos de datos en el Domain Name System (DNS). Se utilizan para almacenar datos sobre nombres de dominio y direcciones IP. Una base de datos o fichero de zona está formada por una serie de registros de recursos. Cada registro de recurso da información pertinente sobre un objeto determinado. Por ejemplo, los **registros de tipo (A)** asocian un nombre de host con una dirección IP, y los **registros de puntero de búsqueda inversa (PTR)** asocian una dirección IP con un nombre de host y un **registro (NS)** define un servidor DNS para la zona. El servidor DNS utiliza estos registros de recurso para resolver las consultas de los hosts de su zona.

Zonas

Cuando un **servidor DNS es autorizado** para una zona, es el responsable de los nombres de dominio para esa zona. En nuestro ejemplo, ns1.deaw.es es el servidor autorizado para la zona deaw.es. y en él se definen los nombres que cuelgan de deaw.es como por ejemplo, www.deaw.es, ftp.deaw.es, natos.deaw.es, etc.

Una zona no es lo mismo que un dominio. Un **dominio** es un **subárbol del espacio de nombres de dominio** y los datos asociados a los nombres de un **dominio** pueden estar almacenados en una o varias **zonas**, distribuidas en uno o varios **servidores DNS**.

Zonas



Tipos de RR (Resource Record)

$TTL (Time To Live)

El TTL o tiempo de vida determina, en segundos, durante cuánto tiempo son validos los RR. Pueden indicarse en semanas ($TTL 1W), días ($TTL 7D), horas ($TTL 168H) o minutos (10080M).

En otras palabras, el TTL indica cuánto tiempo tardarán en aplicarse los cambios que le hagamos a un RR desde que los hacemos. Debe declararse al inicio del archivo de zona.

Tipos de RR (Resource Record)

$ORIGIN

La directiva $ORIGIN define el nombre del dominio que será añadido al final de cualquier nombre que no acabe en punto (nombres relativos o no cualificados) en los RR, para así transformarlos en nombres FQDN (fully qualified domain name). Si un nombre acaba en punto, se considera un nombre FQDN y no se utilizaría $ORIGIN.

Su sintaxis o forma de escribirlo será:

```
$ORIGIN nombre-dominio
```

Por ejemplo:

```
$ORIGIN deaw.es.
;A partir de aquí se añade deaw.es. a todos los nombres relativos
```

Tipos de RR (Resource Record)

Registro SOA (Start Of Authority): Especifica información autoritaria sobre una zona DNS, incluyendo el servidor de nombre primario, el email del administrador, el número de serial o versión de la zona, y varios temporizadores.
Ejemplo:

```
deaw.es.    IN    SOA    ns1.deaw.es.    super.deaw.es. (
              20190425001 ; serial
              604800  ; refresh (7 días)
              86400   ; retry (1 día)
              2419200 ; expire (28 días)
              604800 )    ; TTL negativo (7 días)
...
```

Tipos de RR (Resource Record)

Registro NS (Name Server):Cuando se delega la administración de subdominios en otros servidores, este registro indica cuáles son esos servidores autorizados.

```
...
deaw.es.     IN  NS  ns1.deaw.es.     ;Servidor DNS maestro
deaw.es.     IN  NS  ns2.deaw.es.     ;Servidor DNS esclavo
deaw.es.     IN  NS  dns.deaw.net.    ;Servidor DNS esclavo

ns1.deaw.es.     IN  A   192.168.10.20
ns2.deaw.es.     IN  A   192.168.10.21

;DELEGACIÓN
practicas.deaw.es.  IN  NS  ns1.practicas.deaw.es.
redes.deaw.es.  IN  NS  dns.deaw.net.
```

Tipos de RR (Resource Record)

El registro A (Address), también conocido como registro de dirección, establece una correspondencia entre un nombre de dominio completamente cualificado (FQDN) y una dirección IP versión 4.

```
...
ns1.deaw.es.         IN  A   192.168.10.20
ns2.deaw.es.         IN  A   192.168.10.21
natos.deaw.es.  IN   A   192.168.10.22
...
```

Tipos de RR (Resource Record)

El **registro CNAME (Canonical Name)** permite crear alias para nombres de dominio especificados en registros A.

```
...
natos.deaw.es.  IN  A   192.168.1.22
www.deaw.es.        IN  CNAME   natos.deaw.es.
ftp.deaw.es.        IN  CNAME   natos.deaw.es.
...
```

Un registro CNAME también puede apuntar a un nombre de otro dominio.

```
...
www.deaw.es.    IN  CNAME   www.deaw.com.
...
```

Tipos de RR (Resource Record)

El **registro MX (Mail Exchange)** permite definir los servidores encargados de la entrega de correo en el dominio y la prioridad entre ellos. Su sintáxis es la siguiente:

```
...
deaw.es.     IN  MX  10  mail1.deaw.es.
deaw.es.     IN  MX  20  mail2.deaw.es.

mail1.deaw.es.  IN  A   192.168.1.100
mail2.deaw.es.  IN  A   192.168.1.101
...
```

Tipos de RR (Resource Record)

El **registro PTR (Pointer Record)** establece una correspondencia entre direcciones IPv4 e IPv6 y nombres de dominio. Se utilizan en las zonas de resolución inversa.

En el caso de un bloque IPv4 de prefijo /24, por ejemplo el 192.168.1.0/24, los registros PTR serían los siguientes:

```
...
20.1.168.192.in-addr.arpa.    IN    PTR    ns1.deaw.es.
21.1.168.192.in-addr.arpa.    IN    PTR    ns2.deaw.es.
22.1.168.192.in-addr.arpa.    IN    PTR    natos.deaw.es.
...
```

Tipos de RR (Resource Record)

El **registro TXT (plaint text)** permite asociar información adicional a un dominio mediante múltiples cadenas de texto, con una longitud máxima de 255 caracteres cada una de ellas. Por ejemplo, utilizado para almacenar claves de cifrado.

```
...
@   IN  TXT     "Servidor maestro de Servicios en Red"
@   IN  TXT     "Servidor maestro de Servicios en Red"
```

Tipos de RR (Resource Record)

El **registro TXT (plaint text)** permite asociar información adicional a un dominio mediante múltiples cadenas de texto, con una longitud máxima de 255 caracteres cada una de ellas. Por ejemplo, utilizado para almacenar claves de cifrado.

```
...
@   IN  TXT     "Servidor maestro de Servicios en Red"
@   IN  TXT     "Servidor maestro de Servicios en Red"
```

Tipos de Servidores DNS

Servidor maestro o primario

Un servidor maestro o primario, define una o varias zonas de las que es autorizado. Sus archivos de zona son de lectura y escritura y es en ellos donde el administrador del servidor añade, modifica o elimina nombres de dominio.

- Si un cliente DNS u otro servidor DNS le pregunta por algún nombre de dominio **para el que es autorizado**, consulta con los ficheros de zona y responde a la pregunta.

- Si un cliente DNS u otro servidor DNS le pregunta por algún nombre de dominio **para el que no es autorizado**, tendrá que preguntar a otros servidores DNS o responder que no conoce la respuesta.

Tipos de Servidores DNS

Servidor esclavo o secundario

Un servidor esclavo o secundario define una o varias zonas para las que es autorizado. La diferencia con respecto a un servidor maestro es que los ficheros de zona los obtiene de otro servidor autorizado para la zona, normalmente, de un servidor maestro mediante un procedimiento denominado transferencia de zona. Los ficheros de zona de los servidores esclavos son de solo lectura y por lo tanto, el administrador no tiene que editarlos. La modificación de los archivos de zona debe realizarla el servidor maestro que transfiere la zona.

El funcionamiento de como responden a los clientes DNS o a otros servidores DNS es similar al de un servidor maestro. Un servidor puede ser maestro para una o varias zonas y al mismo tiempo ser esclavo para otras.

Tipos de Servidores DNS

Servidor esclavo o secundario

Pueden existir varios servidores esclavos para una misma zona. Las razones para esto suelen ser:

- Reducir y repartir la carga entre varios servidores DNS.
- Favorecer la tolerancia a fallos.
- Ofrecer mayor rapidez.

Lo ideal es que los servidores DNS para una misma zona estén ubicados en redes y localizaciones diferentes para evitar que, si ocurre algún problema no les afecte simultáneamente y deje sin servicio de resolución a los nombres de esa zona.

Fichero de zona creado por el administrador

```
...
mortadelo.zeppelinux.es.IN A     192.168.1.21
filemon.zeppelinux.es.  IN A     192.168.1.22
www.zeppelinux.es.      IN CNAME mortadelo.zeppelinux.es.
ftp.zeppelinux.es.      IN CNAME filemon.zeppelinux.es.
...
```

Transferencia de zona

Fichero de zona obtenido por transferencia de zona

```
...
mortadelo.zeppelinux.es.IN A     192.168.1.21
filemon.zeppelinux.es.  IN A     192.168.1.22
www.zeppelinux.es.      IN CNAME mortadelo.zeppelinux.es.
ftp.zeppelinux.es.      IN CNAME filemon.zeppelinux.es.
...
```

Servidor DNS "maestro" para la zona "zeppelinux.es"

Servidor DNS "maestro" para la zona "publicaciones.es" y esclavo para la zona "zeppelinux.es"

Fichero de zona creado por el administrador

```
...
www.publicaciones.es.  IN A     192.168.1.21
ftp.publicaciones.es.  IN A     192.168.1.22
...
```

Transferencia de zona

Fichero de zona obtenido por transferencia de zona

```
...
www.publicaciones.es.  IN A     192.168.1.21
ftp.publicaciones.es.  IN A     192.168.1.22
...
```

Cliente DNS (Resolver)

Servidor DNS "esclavo" para la zona "publicaciones.es"

El cliente DNS puede preguntar a cualquiera de los servidores DNS

Tipos de Servidores DNS

Servidor caché

Los servidores DNS se configuran como servidores cache para mejorar los tiempos de respuesta de las consultas, reducir la carga de los equipos y disminuir el tráfico de red.

Cuando un servidor DNS recibe una pregunta sobre un dominio para el cual no es autorizado, es decir, de un nombre del cual no tiene información, puede preguntar, si así está configurado, a otros servidores para obtener la respuesta. Si el servidor actúa como cache, guarda durante un tiempo (TTL: Time To Live) las respuestas a las últimas preguntas que ha realizado a otros servidores DNS. Cada vez que un cliente DNS u otro servidor DNS le formula una pregunta, comprueba si tiene la respuesta en su memoria cache, si la tiene, no tendrá que preguntar a otro servidor DNS por la pregunta.

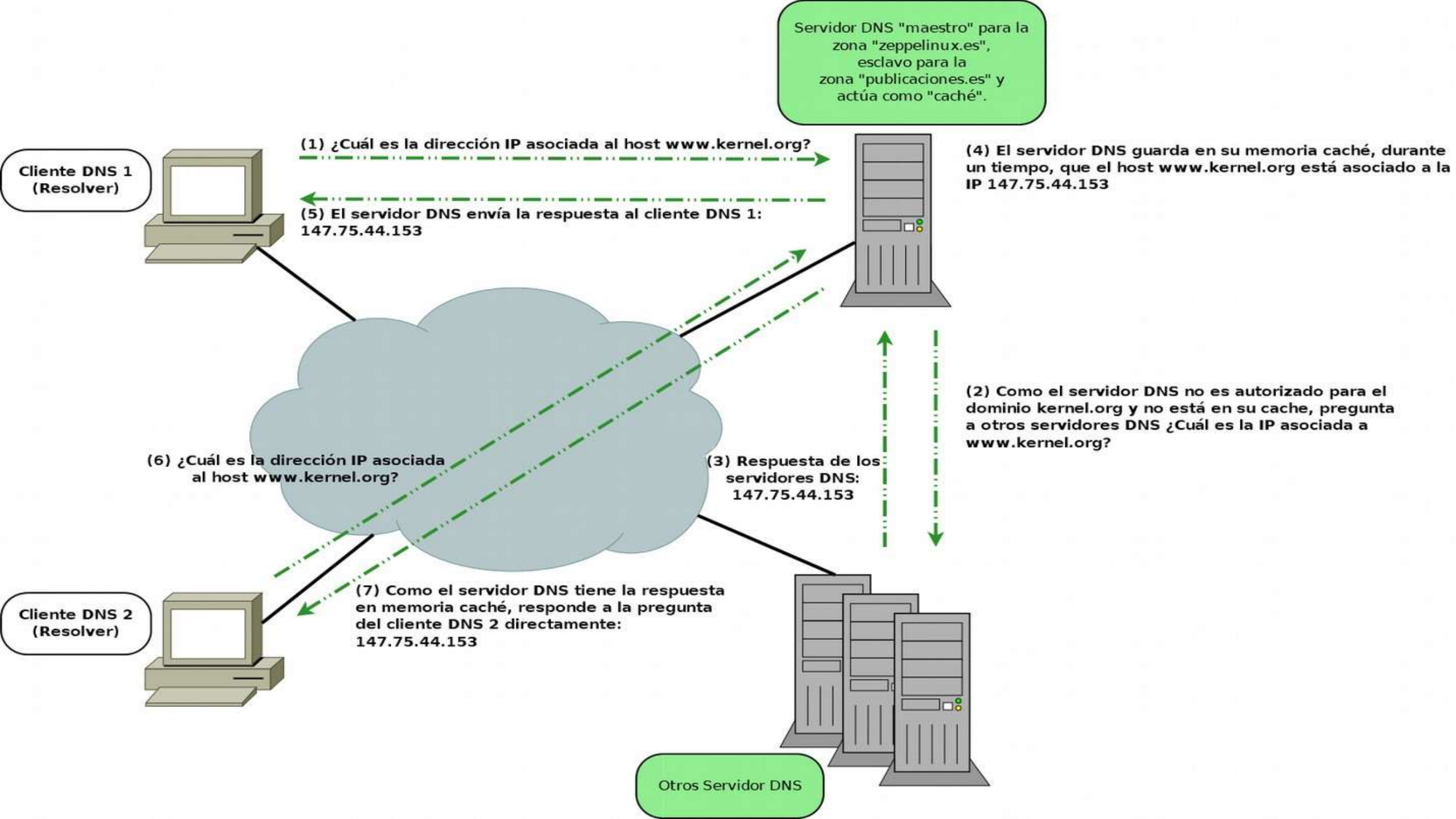
Tipos de Servidores DNS

Servidor caché

Un servidor DNS es solo cache (cache only server) cuando:

- No tiene autoridad sobre ninguna zona.
- Pregunta a otros servidores DNS para resolver las preguntas de los clientes DNS y las guarda en su memoria cache.

En la imagen siguiente se explica cómo dos clientes DNS hacen preguntas a un mismo servidor DNS que es autorizado para algunas zonas y además actúa como caché.


Servidor DNS "maestro" para la zona "zeppelinux.es", esclavo para la zona "publicaciones.es" y actúa como "caché".
Cliente DNS 1 (Resolver)
(1) ¿Cuál es la dirección IP asociada al host www.kernel.org?
(5) El servidor DNS envía la respuesta al cliente DNS 1: 147.75.44.153
(4) El servidor DNS guarda en su memoria caché, durante un tiempo, que el host www.kernel.org está asociado a la IP 147.75.44.153
(2) Como el servidor DNS no es autorizado para el dominio kernel.org y no está en su cache, pregunta a otros servidores DNS ¿Cuál es la IP asociada a www.kernel.org?
(3) Respuesta de los servidores DNS: 147.75.44.153
(6) ¿Cuál es la dirección IP asociada al host www.kernel.org?
(7) Como el servidor DNS tiene la respuesta en memoria caché, responde a la pregunta del cliente DNS 2 directamente: 147.75.44.153
Cliente DNS 2 (Resolver)
Otros Servidor DNS

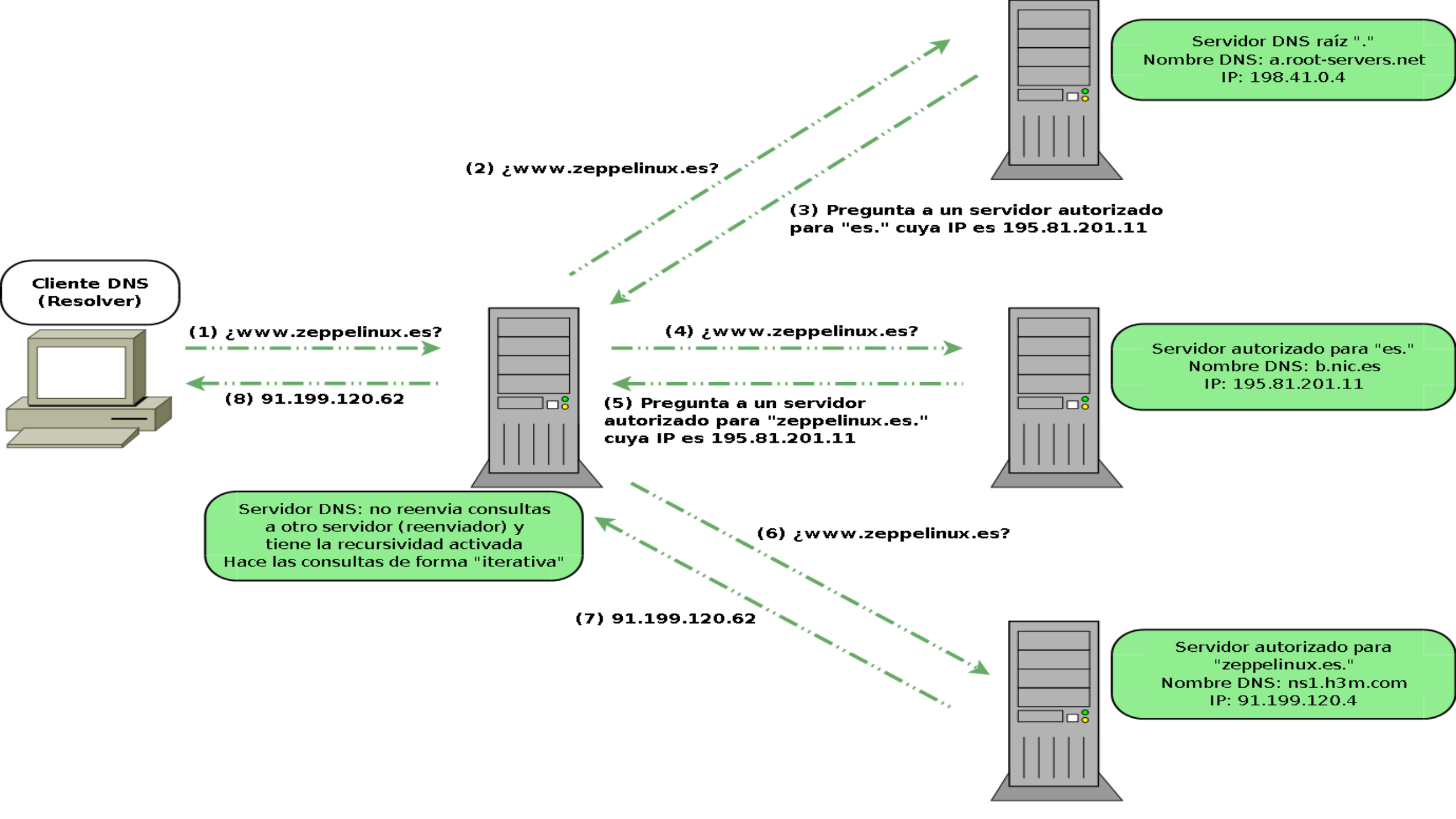
Tipos de Servidores DNS

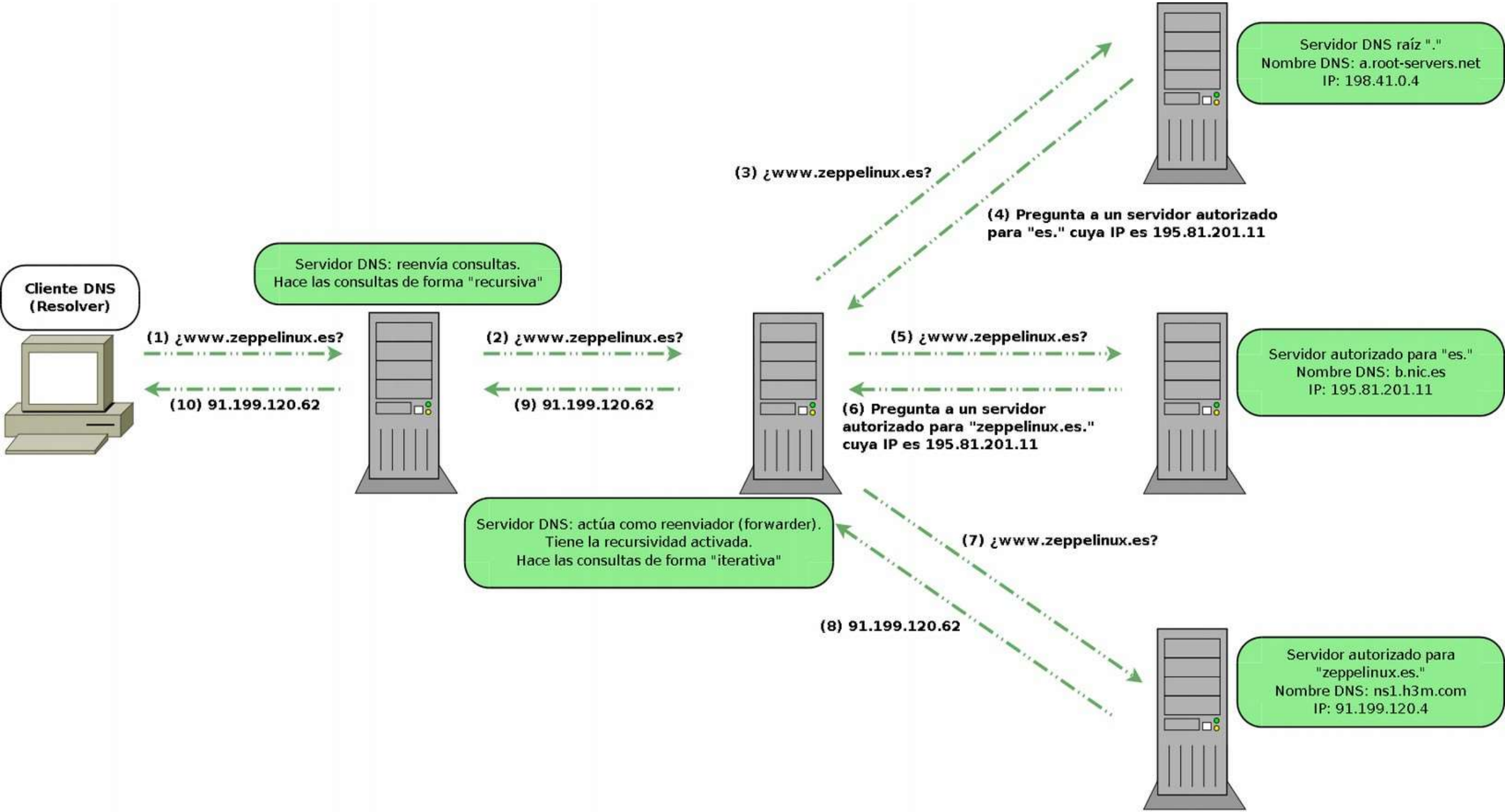
Servidor forwarder (reenviador)

Cuando a un servidor DNS se le hace una pregunta sobre un nombre de dominio del que no dispone información (no es autorizado), este puede preguntar a otros servidores DNS. Simplificando, existen dos formas de procesar las consultas:

- El servidor DNS procesa la consulta preguntando a diversos servidores DNS y empezando por los servidores DNS raíz. Consulta iterativa.
- El servidor DNS reenvía la consulta a otro servidor DNS, denominado reenviador (forwarder), para que se encargue de resolverla. Consulta recursiva.

Visto esto, un reenviador (forwarder) es un servidor DNS que otros servidores DNS designan para reenviarle consultas. Son utilizados para minimizar las consultas y el tráfico de peticiones DNS desde una red hacia Internet. Además permiten a los equipos locales utilizar su cache DNs para minimizar los tiempos de respuesta.


Servidor DNS raíz "."
Nombre DNS: a.root-servers.net
IP: 198.41.0.4
(2) ¿www.zeppelinux.es?
(3) Pregunta a un servidor autorizado para "es." cuya IP es 195.81.201.11
Cliente DNS (Resolver)
(1) ¿www.zeppelinux.es?
(8) 91.199.120.62
(4) ¿www.zeppelinux.es?
(5) Pregunta a un servidor autorizado para "zeppelinux.es." cuya IP es 195.81.201.11
Servidor autorizado para "es."
Nombre DNS: b.nic.es
IP: 195.81.201.11
Servidor DNS: no reenvia consultas a otro servidor (reenviador) y tiene la recursividad activada
Hace las consultas de forma "iterativa"
(6) ¿www.zeppelinux.es?
(7) 91.199.120.62
Servidor autorizado para "zeppelinux.es."
Nombre DNS: ns1.h3m.com
IP: 91.199.120.4


Servidor DNS raíz "."
Nombre DNS: a.root-servers.net
IP: 198.41.0.4
(3) ¿www.zeppelinux.es?
(4) Pregunta a un servidor autorizado para "es." cuya IP es 195.81.201.11
Servidor DNS: reenvía consultas.
Hace las consultas de forma "recursiva"
Cliente DNS (Resolver)
(1) ¿www.zeppelinux.es?
(2) ¿www.zeppelinux.es?
(5) ¿www.zeppelinux.es?
Servidor autorizado para "es."
Nombre DNS: b.nic.es
IP: 195.81.201.11
(10) 91.199.120.62
(9) 91.199.120.62
(6) Pregunta a un servidor autorizado para "zeppelinux.es." cuya IP es 195.81.201.11
Servidor DNS: actúa como reenviador (forwarder).
Tiene la recursividad activada.
Hace las consultas de forma "iterativa"
(7) ¿www.zeppelinux.es?
(8) 91.199.120.62
Servidor autorizado para "zeppelinux.es."
Nombre DNS: ns1.h3m.com
IP: 91.199.120.4

Tipos de Servidores DNS

Servidor solo autorizado

Un Servidor solo autorizado (authoritative only) es aquel que es autorizado para una o varias zonas como servidor maestro y/o esclavo y no responde a preguntas que no sean relativas a sus zonas. Es decir, no tiene activada la recursividad, no es reenviador y no actúa como cache.

Servidores raíz

En Internet existen un conjunto de servidores DNS autorizados para el dominio raíz ., conocidos como servidores raíz (root servers). Contienen el fichero de la zona . que contiene información sobre los servidores DNS autorizados para cada uno de los dominios TLD.

Los servidores raíz son una parte fundamental de Internet, son el primer paso en la traducción (resolución) de los nombres de host en direcciones IP, que se utilizan en la comunicación entre los hosts de Internet. Son claves en el proceso de resolución de nombres de dominio en Internet, y deben de ser conocidos por todos los servidores DNS que respondan a preguntas sobre nombres para los que no son autorizados.

Tipos de Servidores DNS

Servidores raíz

Existen 13 servidores raíz en toda Internet y cada uno de ellos tiene múltiples copias distribuidas por todo el mundo, es decir, que físicamente no solo son 13 servidores. Cada conjunto de copias de uno de los 13 servidores se identifica por una misma IP. Cuando un cliente realiza una pregunta a una IP de un servidor raíz, los routers de Internet encaminan la pregunta hacia la copia más cercana mediante un procedimiento denominado anycasting.

Los nombres de los servidores raíz son de la forma letra.root-servers.net, donde letra va desde la A a la M.

;Hostname	Dirección IP	Administrador
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern Californ
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, In
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Tipos de consultas: recursivas e iterativas

Consultas recursivas

Una consulta recursiva es aquella en la que el servidor DNS da una respuesta completa o exacta. Pueden darse tres tipos de respuesta:

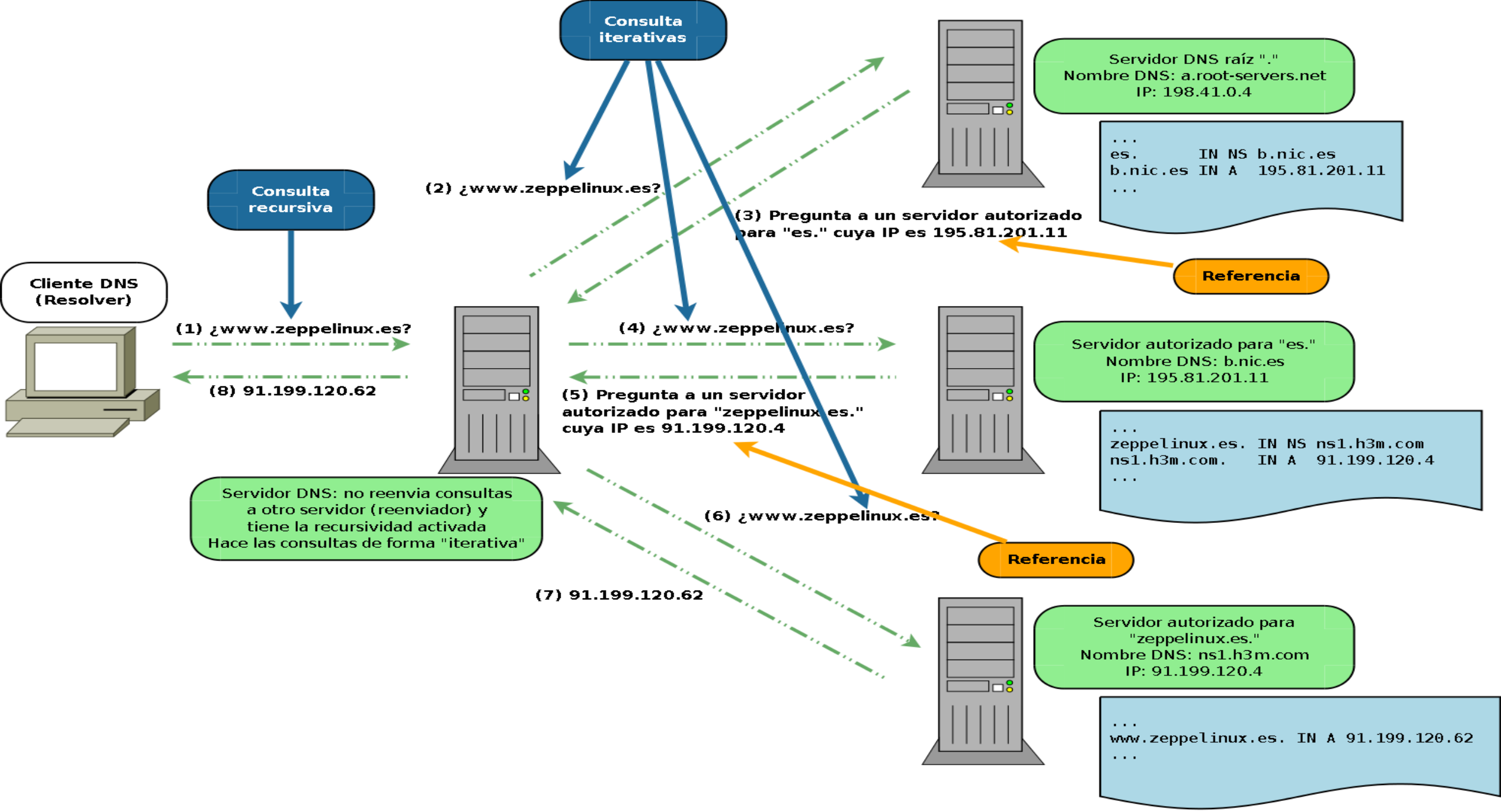
- Positivas: se devuelve información sobre el dominio consultado
- Negativas: no se puede resolver el nombre de dominio
- Error: debido a un fallo en la red

Tipos de consultas: recursivas e iterativas

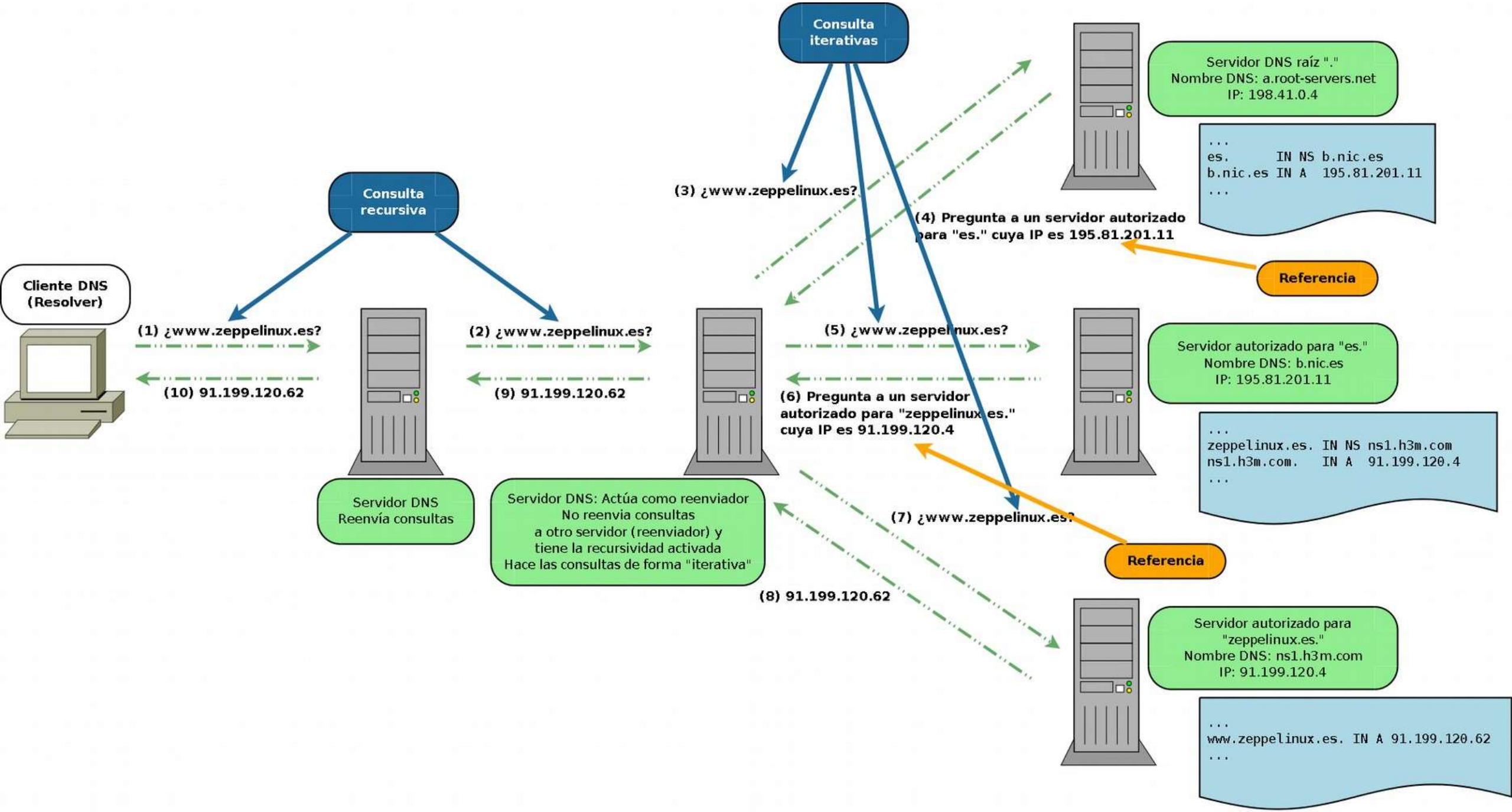
Consultas iterativas

Una consulta iterativa es aquella en la que el servidor DNS proporciona una respuesta parcial. Existen cuatro posibles respuestas:

- Positivas: se devuelve información sobre el dominio consultado
- Negativas: no se puede resolver el nombre de dominio
- Referencia: el servidor DNS indica a otros servidores a los que se le puede consultar para resolver la pregunta
- Error: debido a un fallo en la red



Ejemplo de resolución DNS nº 1



Ejemplo de resolución DNS nº 2

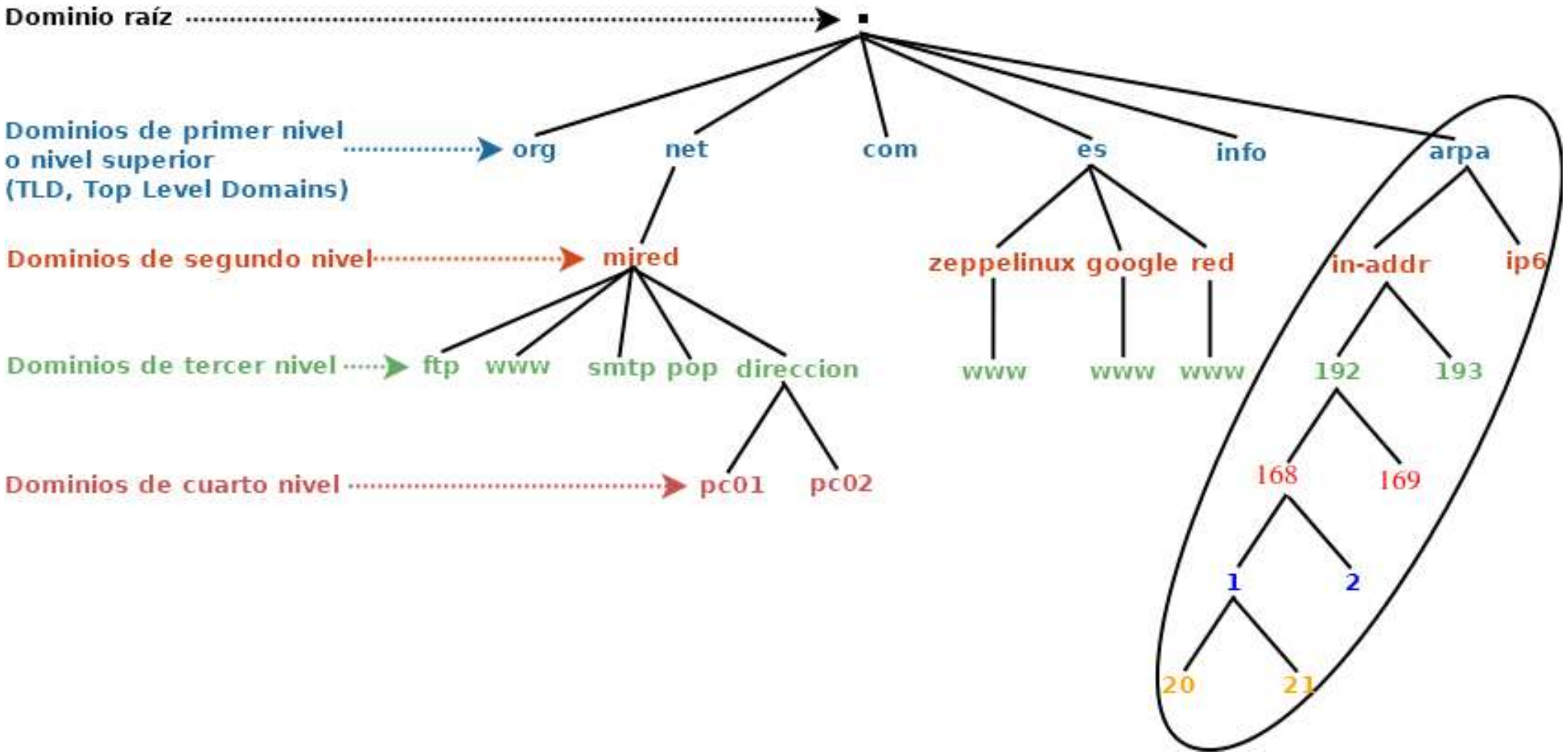
Resolución inversa

La resolución inversa consiste en obtener información de un nombre de dominio preguntando por la dirección IP en vez de preguntar por el nombre de dominio como hemos explicado en apartados anteriores.

Mapeo de direcciones y el dominio arpa

El funcionamiento de la resolución de direcciones IP es igual al de la resolución de nombres de dominio. Las direcciones IP se tratan como nombres que cuelgan del dominio in-addr.arpa para las direcciones IPv4, y del dominio ip6.arpa para las direcciones IPv6.

Resolución inversa



Resolución inversa

Cuando usamos una dirección IP, por ejemplo 192.168.1.21, para realizar una pregunta DNS inversa, en realidad estamos preguntando por el nombre de dominio 21.1.168.192.in-addr.arpa. La estructura jerárquica de la dirección IP, tratada como nombre de dominio, es de derecha a izquierda, comenzando por el dominio in-addr.arpa.

.arpa (Address and Routing Parameter Area) es un dominio de nivel superior genérico utilizado sólo para la infraestructura de Internet. Los subdominios de .arpa o dominios de segundo nivel «in-addr.arpa» e «ip6.arpa» son usados por los servidores DNS inversos para la obtención de direcciones IPv4 e IPv6 respectivamente.

Cuando mapeamos una dirección IP estamos asociando la dirección IP al nombre en el dominio .arpa. Por ejemplo la dirección 192.168.1.21 es mapeada al nombre 21.1.168.192.in-addr.arpa.

Resolución inversa

Zonas de resolución inversa

Los servidores DNS almacenan zonas de resolución inversa con registros de recursos (RR) que asocien nombres de dominio con direcciones IP. Las zonas de resolución inversa pueden ser maestras o primarias y esclavas o secundarias.

Las zonas de resolución directa e inversa son independientes y es responsabilidad de los administradores de los servidores DNS que dichas zonas contengan información coherente y que no existan discrepancias.

No es obligatorio que la entidad que administra una zona de resolución directa de un dominio tenga que administrar la zona de resolución inversa que se corresponda con las direcciones IPs asociadas a dicho dominio.

Resolución inversa

```
...
deaw.es.              IN  NS      ns1.deaw.es.
ns1.deaw.es.          IN  A       192.168.1.20
natos.deaw.es.   IN   A       192.168.1.21
waor.deaw.es.         IN  A       192.168.1.22
altea.deaw.es.        IN  A       192.168.1.23
www.deaw.es.          IN  CNAME   natos.deaw.es.
ftp.deaw.es.          IN  CNAME   waor.deaw.es.
...
```

Archivo de zona de resolución inversa 1.168.192.in-addr.arpa que permite resolver consultas inversas sobre direcciones IP de la red 192.168.1.0/24

```
...
1.168.192.in-addr.arpa.      IN  NS  ns1.deaw.es.
20.1.168.192.in-addr.arpa.   IN  PTR ns1.deaw.es.
21.1.168.192.in-addr.arpa.   IN  PTR natos.deaw.es.
22.1.168.192.in-addr.arpa.   IN  PTR waor.deaw.es.
123.1.168.192.in-addr.arpa.  IN  PTR altea.deaw.es.
...
```

Resolución inversa

Proceso de resolución

El proceso de resolución inversa es similar al de resolución directa. Las direcciones IP se tratan como nombres de dominio. Por lo tanto, existen consultas recursivas, iterativas, cache, TTL...

Por ejemplo, si un cliente DNS realiza una consulta recursiva de la IP 192.168.1.21 a un servidor DNS, éste, si no lo tiene en cache, iniciará una serie de consultas iterativas a los servidores DNS raíz, a los servidores autorizados para el dominio 192.in-addr.arpa y así sucesivamente.

Heramientas

Nslookup

Es un programa para consultar servidores DNS. Se utiliza para saber si un servidor DNS resuelve correctamente los nombres DNS y las direcciones IP, para solucionar problemas frecuentes de los servidores DNS o, para diagnosticar problemas ocasionales de configuración en los servidores DNS.

Con nslookup podemos obtener la dirección IP asociada a un nombre DNS y viceversa, además, podemos preguntar a los servidores de nombres información relativa a los registros de recursos (RR) de la/s zona/s de las que son autorizados.

nslookup se usa de dos modos: interactivo y no interactivo. El modo interactivo permite al usuario consultar los servidores DNS para obtener información sobre varios hosts y dominios o para listar los hosts de un dominios. El modo no interactivo se usa para presentar solo el nombre y la información solicitada para un host o nombre DNS.

Heramientas

```
[redacted] ~ $ nslookup cisco.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   cisco.com
Address: 72.163.4.185
Name:   cisco.com
Address: 2001:420:1101:1::185
```

```
[redacted] $ nslookup -type=ns cisco.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
cisco.com       nameserver = ns3.cisco.com.
cisco.com       nameserver = ns1.cisco.com.
cisco.com       nameserver = ns2.cisco.com.

Authoritative answers can be found from:
```

```
[redacted] ~ $ nslookup
> set type=ns
> cisco.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
cisco.com       nameserver = ns2.cisco.com.
cisco.com       nameserver = ns1.cisco.com.
cisco.com       nameserver = ns3.cisco.com.

Authoritative answers can be found from:
>
```

Heramientas

Dig

Es un programa utilizado para preguntar a los servidores DNS.

Herramienta utilizada para solucionar problemas de DNS gracias a su flexibilidad, facilidad de uso y claridad en la presentación de la información. Normalmente, dig se usa pasándole argumentos desde la línea de comandos (CLI), pero también tiene un modo de operar por lotes, leyendo las consultas desde un archivo.

Este comando funciona tanto en sistemas operativos UNIX/Linux como en Windows

Heramientas

Host

Host es una herramienta CLI sencilla y fácil de usar para realizar consultas DNS, que traducen nombres de dominio a direcciones IP y viceversa. También se utiliza para consultar los registros DNS de las zonas que almacenan los servidores DNS, probar y validar el servidor DNS y la conectividad a Internet, registros de correo no deseado y listas negras, diagnóstico de problemas en el servidor DNS...

Whois

Aunque no es una herramienta de diagnóstico DNS si que nos ofrece información sobre el registro del dominio.

Whois es un protocolo que permite realizar consultas a bases de datos que contienen información; del usuario, empresa u organización que registra un nombre de dominio y/o una dirección IP en Internet. El protocolo whois se encapsula en TCP y solo especifica el intercambio de peticiones y respuestas, no el formato de datos a intercambiar. Por eso, los resultados de las consultas whois pueden variar dependiendo de la base de datos whois a la que se pregunte.