Servicio de nombres de dominio (DNS)

Despliegue de aplicaciones web

2º DAW

CONTENIDOS

- Sistemas de nombres planos vs. jerárquicos.
- Características y funcionamiento del servicio DNS.
- Espacio de nombres de dominio. Nombres de dominio. Dominios y subdominios. Delegación. Registro de nombres de dominio.
- Servidores de nombres. Zonas, tipos de servidores y servidores raíz.
- Clientes DNS (resolvers).
- Proceso de resolución. Consultas recursivas e iterativas. Caché y TTL.
- Resolución inversa.
- Bases de datos DNS. Tipos de registros de recursos.
- Transferencias de zona.
- Actualizaciones de DNS dinámicas.
- Seguridad DNS.
- Whois.

OBJETIVOS

- Identificar y describir escenarios en los que surge la necesidad de un servicio de resolución de nombres.
- Clasificar los principales mecanismos de resolución de nombres y describir la estructura, nomenclatura y funcionalidad de los sistemas de nombres jerárquicos.
- Instalar y configurar servicios jerárquicos de resolución de nombres, reenviar consultas de recursos externos a otro servidor de nombres y almacenar y distribuir las respuestas procedentes de otros servidores.
- Añadir registros de nombres correspondientes a una zona nueva, con opciones relativas a servidores de correo y alias y realizar transferencias de zona entre dos o más servidores.
- Implementar soluciones de servidores de nombres en direcciones “ip” dinámicas.
- Documentar los procedimientos de instalación y configuración.

INTRODUCCIÓN

La dirección IP, que identifica a los equipos en las redes TCP/IP, son fáciles de manejar para las máquinas pero pueden resultar complicados de utilizar y memorizar para las personas. A estas les resulta más sencillo usar y recordar nombres (www.google.es, iesvelazquez.org, …).

Para facilitar el uso de los servicios y recursos que ofrece una red se han creado sistemas de nombres utilizados por servicios de resolución de nombres que permiten asociar nombres sencillos con direcciones numéricas. Los servicios de nombres almacenan las direcciones y sus nombres (por ejemplo www.iesjulioverne.es se corresponde con 212.170.93.73). El proceso por el cual “se traduce” entre un nombre y una dirección numérica es lo que se denomina “resolver el nombre”.

El principal servicio de resolución de nombres usado en redes TCP/IP y por tanto en internet es el servicio DNS (Domain Name System).

Sistemas de nombres planos y jerárquicos.

Los sistemas de nombre se pueden clasificar en dos tipos:

Sistemas de nombres planos:

- Uso de nombres sin ningún tipo de agrupamiento.
- No existe una jerarquía que permita clasificar dichos nombres.
- El nombre no aporta otra información que la identificación del host. Ejemplo: PC1, PC2, ...

Sistemas de nombres jerárquicos:

- Uso de nombres agrupados y clasificados según algún criterio (distribución geográfica, funcionalidad, etc)
- El nombre de cada equipo de una red que representa la pertenencia del equipo a una organización jerarquizada u organizada en forma de árbol.
- En Internet se usa un sistema de nombres jerárquico para identificar ordenadores. (www.mec.es indica el ordenador www perteneciente al dominio mec.es).
- Facilita la administración y gestión distribuida.

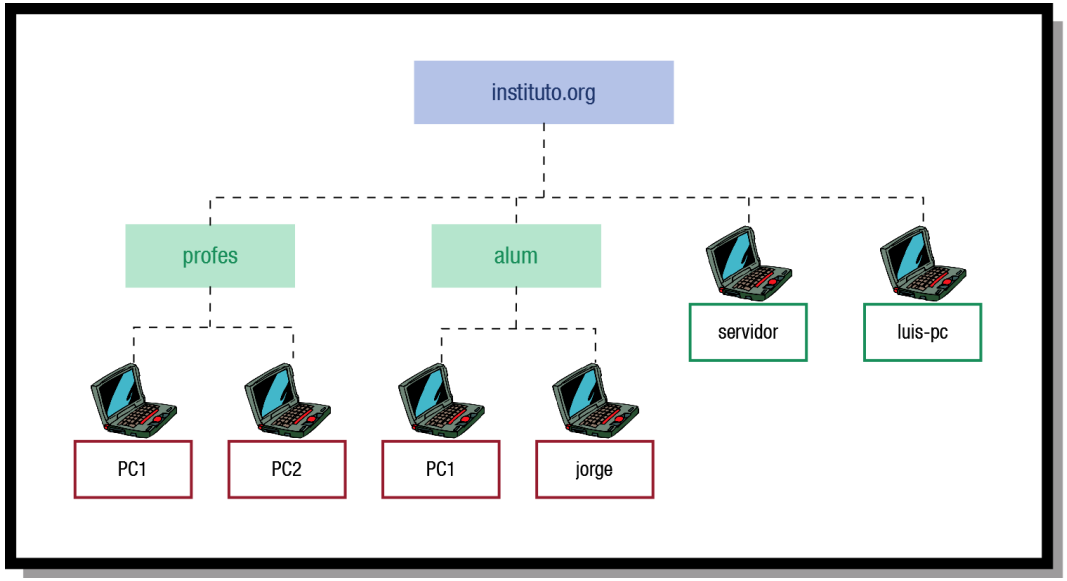
El servicio DNS.

DNS es un protocolo de nivel de aplicación que establece las normas de funcionamiento de un servicio de nombres jerárquico basado en dominios.

Dentro de una red (y de internet por tanto) puede haber varios servidores DNS. Un servidor no tiene porque resolver todos los nombres de la red. DNS se basa en que la resolución y administración de los nombres se realiza de forma distribuida entre todos los servidores existentes en dicha red.

Se basa en una organización en dominios y subdominios. Un determinado dominio tendrá un nombre y todos sus miembros comparten ese nombre.

En un dominio puede haber subdominios que se comportarán como dominios.
Cada servidor DNS se encarga de una o varias zonas. Cada una de estas zonas contiene información para resolver los nombres de las máquinas de uno o más dominios.



El servicio DNS.

Un nombre DNS de un ordenador comienza por su hostname (identificador dentro del dominio) seguido de los nombres de los subdominios y dominios a los que pertenece separados con el carácter punto y leídos desde el dominio inferior al superior, es decir, en orden inverso a la organización jerárquica.

Normalmente se utiliza para:

- Resolución de nombres (búsqueda directa): obtener la información asociada a un nombre de dominio, (p.e. dirección IP asociada al nombre del dominio)
- Resolución inversa de direcciones (búsqueda inversa): mecanismo inverso al anterior. (p.e. nombres de dominio asociados a una dirección IP).
- Resolución de nombres de correo: dado un nombre de dominio “gmail.com” obtener el servidor a través del cual debe realizarse la entrega del correo electrónico “gmail-smtp-in.l.google.com”.
- También se puede utilizar DNS para: balanceo de carga, ubicación de servidores de un servicio determinado, listas negras de spam, etc.

Componentes y funcionamiento del servicio DNS.

Componentes

- Espacio de nombres de dominio (domain name space). Conjunto de nombre que se pueden utilizar para identificar máquinas o servicios de una red.
- Base de datos DNS. Base de datos distribuida y redundante que almacena información (p.e. direcciones IP) sobre los nombres de dominio. Esta base de datos se organiza en zonas que almacenan la información RR (resource records)
- Servidores de nombres (servidores DNS, name servers). Programas que guardan parte de la base de datos DNS (zonas) y que responden a preguntas sobre la información almacenada.
- Clientes DNS. Programas que realizan “preguntas” a los servidores de nombres y procesan las respuestas para ofrecerle la información a los usuarios y/o aplicaciones que los invocan.
- Protocolo DNS. Conjunto de normas y reglas en base a las cuales “dialogan” los clientes y servidores DNS.

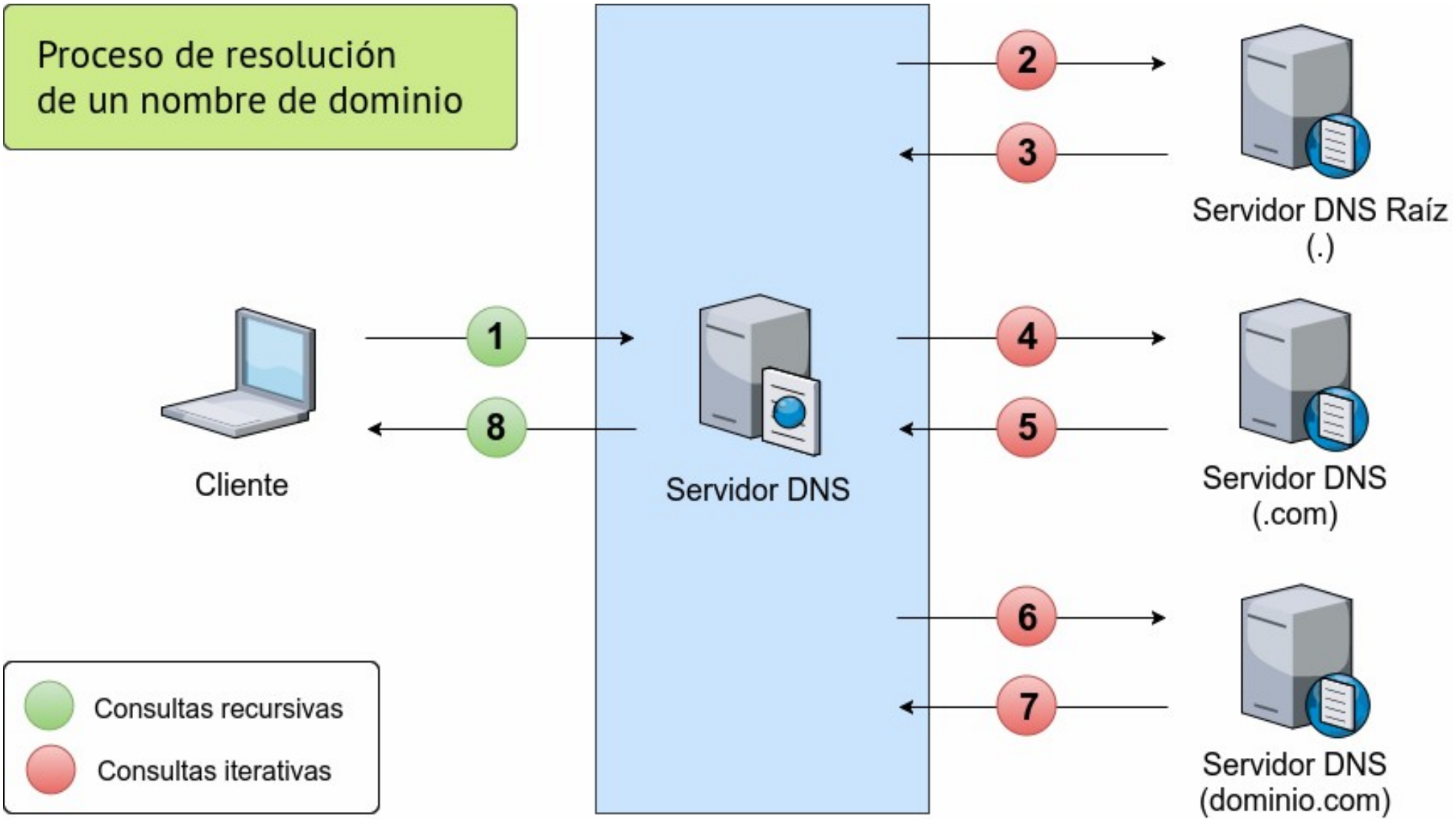
Componentes y funcionamiento del servicio DNS.

Funcionamiento.

Una aplicación (cliente)envía un requerimiento al servidor de nombres configurado en el sistema para resolver una dirección. Este servidor de nombres, normalmente, es el provisto por el ISP. Este servidor local se conoce también como resolver. Un servidor DNS escucha a los clientes en el puerto UDP 53 (también tcp 53).

1. El servidor de nombres consulta a uno de los servidores raíz (conoce su IP)
2. El servidor raíz devuelve el nombre del servidor zona.
3. El servidor inicial interroga al nuevo servidor.
4. El nuevo servidor que posee autoridad sobre la zona interrogada devuelve el nombre del servidor que posee el dominio buscado.
5. El servidor DNS inicial interroga al servidor del dominio buscado.
6. El nuevo servidor resuelve el nombre correspondiente, si este existe.
7. El servidor inicial informa al cliente el nombre resuelto.

Componentes y funcionamiento del servicio DNS.



El espacio de nombres de dominio.

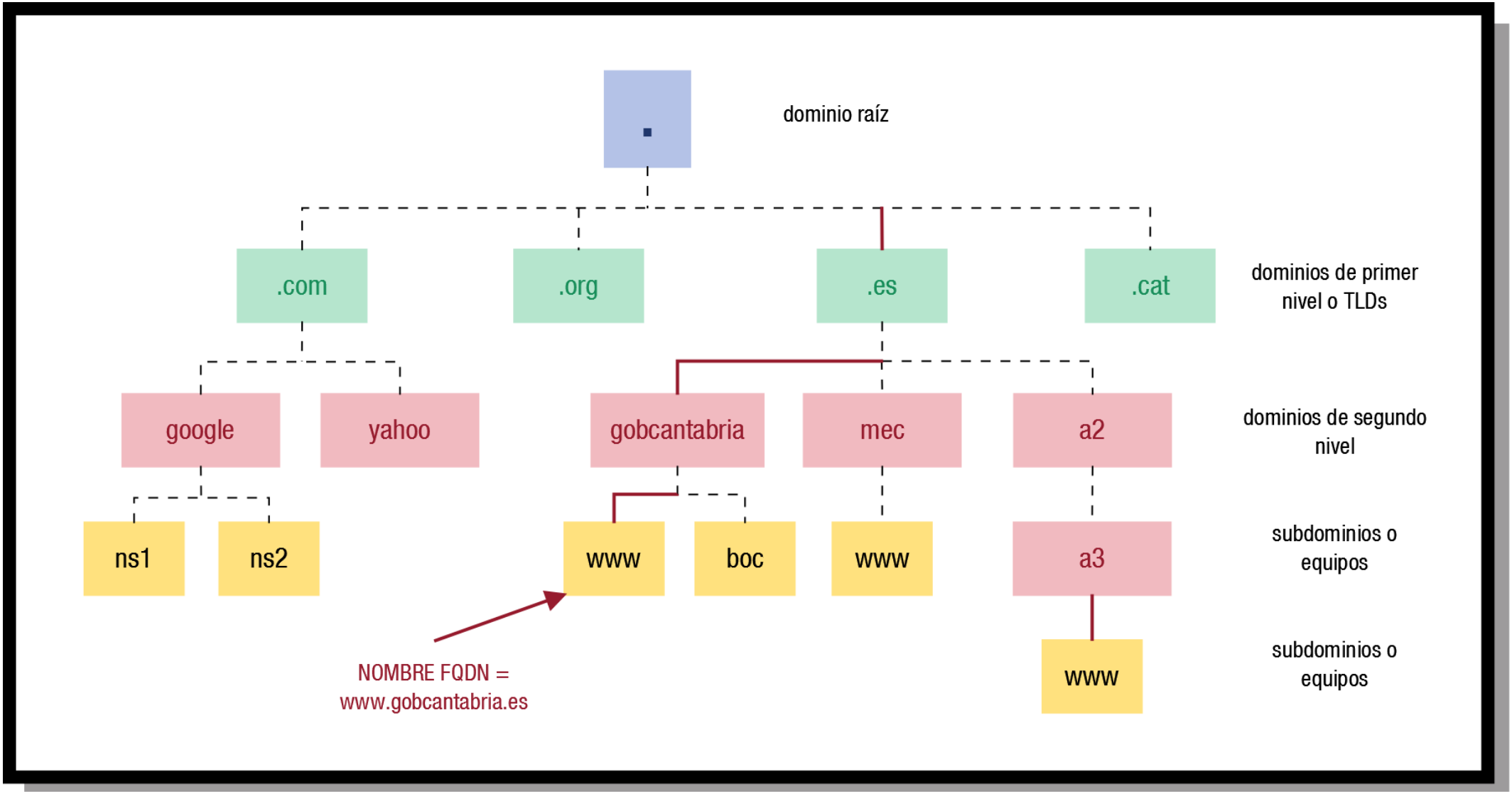
El espacio de nombres de dominio es una base de datos distribuida entre múltiples servidores DNS y que almacena los nombres DNS de equipos junto con sus direcciones IP. Es una estructura jerárquica organizada en forma de árbol con varios niveles de dominio. Pueden ser:

- Nombre relativo: hace falta saber el contexto del nivel superior para saber a que nombre hace referencia exactamente (www, PC1, …)
- Nombre absoluto: nombre formado por todas las partes separadas por puntos. se denominan Fully Qualified Domain Names (FQDN). Un FQDN **termina en un punto** que representa al dominio raíz. Importante al configurar servidor DNS.

Cada elemento del árbol se etiqueta con un nombre de hasta 63 caracteres. Y cada elemento se identifica en el sistema de nombres con un FQDN. Un FQDN representa el nombre de un elemento cualquiera en el espacio de nombres. Un nombre FQDN tiene esta estructura:

nombreEquipo.subdominio.dominioSegundoNivel.dominioPrimerNivel.

El espacio de nombres de dominio.



Tipos de dominios.

Dentro de la estructura jerárquica que hemos visto existen los siguientes tipos de dominios:

- Dominio raíz: de este dominio cuelga toda la estructura del espacio de nombres DNS. Se simboliza con un punto. Bajo el directorio raíz hay dominios de primer nivel. El organismo que se encarga de su gestión es ICANN.
- Dominios de primer nivel: son dominios que en la estructura del espacio de nombres DNS se encuentran bajo el dominio raíz. También se le llama TLD. (Top Level Domain) Dominios de este tipo son .com, .org y .es entre otros. Bajo un TLD hay dominios de segundo nivel. De la gestión de un dominio de primer nivel se encargará una determinada organización (del .es se encarga red.es). Los servidores DNS de este nivel contienen información relativa a los servidores de dominio de segundo nivel dependientes del dominio.

Tipos de dominios.

- Dominios de segundo nivel: son los dominios que se encuentran bajo los TLDs. Cada uno de estos dominios está registrado a favor de una determinada entidad (empresa, universidad, órgano, persona, etc.). La entidad propietaria del dominio es la encargada de la gestión del dominio. Cada dominio de este tipo puede tener uno o varios servidores DNS con información sobre máquinas, subdominios y otros servidores. Cuando una entidad desea disponer de un dominio, debe registrarlo ante un registrador oficial autorizado por ICANN.
- Subdominios: Son dominios que hay bajo un dominio de segundo nivel o bajo otro subdominio. Un subdominio no tiene que ser registrado como un dominio de segundo nivel. En un subdominio puede haber servidores encargados de toda la gestión del subdominio aunque también esa gestión se puede llevar a cabo desde los servidores de segundo nivel.

Dominios de primer nivel.

ICANN tiene actualmente autorizados un gran número de dominios de primer nivel o TLDs. En un principio, estableció dos tipos de TLDs:

- gTLD: Dominios de primer nivel genéricos. En un principio se establecieron seis dominios de este tipo y todos tenían tres letras.
  - .com: orientado a objetivos comerciales.
  - .net: para entidades que están relacionadas con Internet.
  - .org: para organizaciones.
  - .int: reservado a organismos internacionales. Deben cumplir unas restricciones.
  - .mil: reservado a organismos de carácter militar. Deben cumplir unas restricciones.
  - .edu: reservado a instituciones educativas. Deben cumplir unas restricciones.
- ccTLD: dominios geográficos o de país. Se simbolizan con dos letras representativas del nombre del país. Son dominios de este tipo .es para España, .fr para Francia ...

Dominios de primer nivel.

- Un dominio genérico especial es .arpa, se utiliza para la infraestructura técnica de Internet. ICANN lo administra.
- Se han creado otros dominios genéricos como .biz (para empresas), .gov (para organismos de gobierno) y otros que incluso tienen más de tres letras como .info.
- Dentro de los gTLD se pueden considerar otros subtipos como:
  - sTLD: patrocinados por fundaciones independientes. Como .aero para aeropuertos y .travel para agencias de viaje, .cat patrocinado por la Fundación puntCat.
  - nTLD: nuevos dominios, .blog, .shop,...
- Hay nombres de dominio de primer nivel reservados para pruebas privadas ("test", "example", "invalid" y "localhost").

Delegación DNS

La delegación DNS es el proceso por el cual el gestor de un determinado dominio delega la tarea de gestión, incluyendo el mantenimiento de servidores DNS.

- ICANN delega la gestión de ccTLD .es a la empresa pública Red.es, se encargara de gestionar el alta y baja de dominios bajo .es.
- Una vez que ICANN ha delegado el dominio .es, Red.es deberá gestionar el alta del dominio, Sin embargo cuando Red.es crea el dominio lo delega a la empresa dueña del dominio para que esta de de alta el dominio que quiera crear para poder acceder a su página web y sea la empresa la que se encargue de configurarlo y mantenerlo.
- Esta última puede a su vez delegar subdominios en otras entidades.
- En el caso de que una organización delegue los subdominios en otra no tiene que informar a “su superior” de esta delegación.

Servidores de nombres

La resolución de nombres DNS es realizada por los servidores DNS, la gestión del sistema de nombres DNS se lleva a cabo de forma distribuida entre múltiples servidores de la red. En función del nivel del espacio de nombres en el que resuelvan, los servidores DNS pueden ser:

- Servidores raíz o root servers.
- Servidores de dominio de primer nivel.
- Servidores de dominio de segundo nivel.
- Servidores de subdominio.

Los servidores raíz contienen información para resolver en el dominio raíz. Esa información indica cuales son esos servidores y que direcciones IP tienen así como cuales son los nombres y direcciones IP de los servidores de dominios de primer nivel.

Hay 13 servidores raíz principales aunque hay otros muchos repartidos por todo el mundo que contienen información copia de alguno de los principales

Tipos de servidores de nombres.

Según la función que realizan, los servidores de nombres pueden clasificarse en:

- Servidor maestro o primario: define una o varias zonas para las que está autorizado. Sus archivos de zona locales son de lectura y escritura (el administrador puede añadir, modificar o eliminar nombres).
  - ➔ Si un cliente DNS u otro servidor le pregunta por un nombre para el que está autorizado, consulta con los ficheros de zona y responde.
  - ➔ En caso de preguntarle por un nombre para el que no está autorizado, tendrá que buscar la información en otros servidores o responder que no conoce la respuesta.
- Servidor esclavo (o secundario): define una o varias zonas para las que es autorizado. Los ficheros de zona del servidor esclavo son de solo lectura y los recibe de otro servidor autorizado (maestro).

Tipos de servidores de nombres.

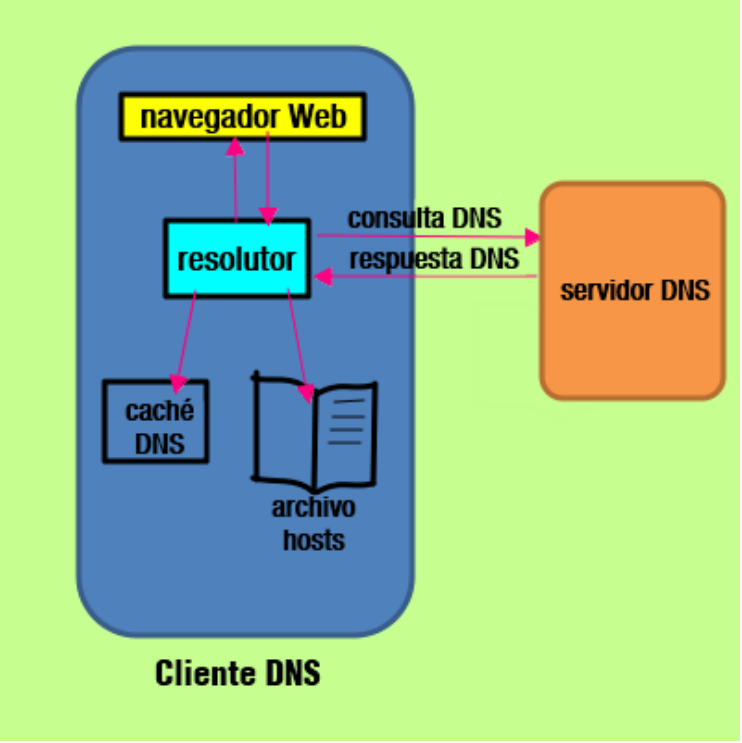
- Servidor caché: cuando un servidor DNS recibe una pregunta sobre una zona para la que no es autorizado, puede preguntar a otros servidores. Si el servidor actúa como caché guarda durante un tiempo (TTL, Time To Live) las respuestas a las últimas preguntas.
- Servidor reenviador (forwarder): es un servidor DNS al que otros servidores utilizan para reenviarle las consultas y que se encargue de resolverlas.
- Servidor solo autorizado: se trataría de un servidor DNS que:
  - ➔ Es autorizado para una o varias zonas como maestro y/o esclavo.
  - ➔ No responde a preguntas que no sean relativas a sus zonas (no es reenviador, no actúa como caché).

Clientes DNS (resolvers).

Los clientes DNS realizan sus consultas a través de resolutores. Un resolutor es un proceso que se ejecuta a petición de un programa que usa un nombre DNS para establecer una conexión.

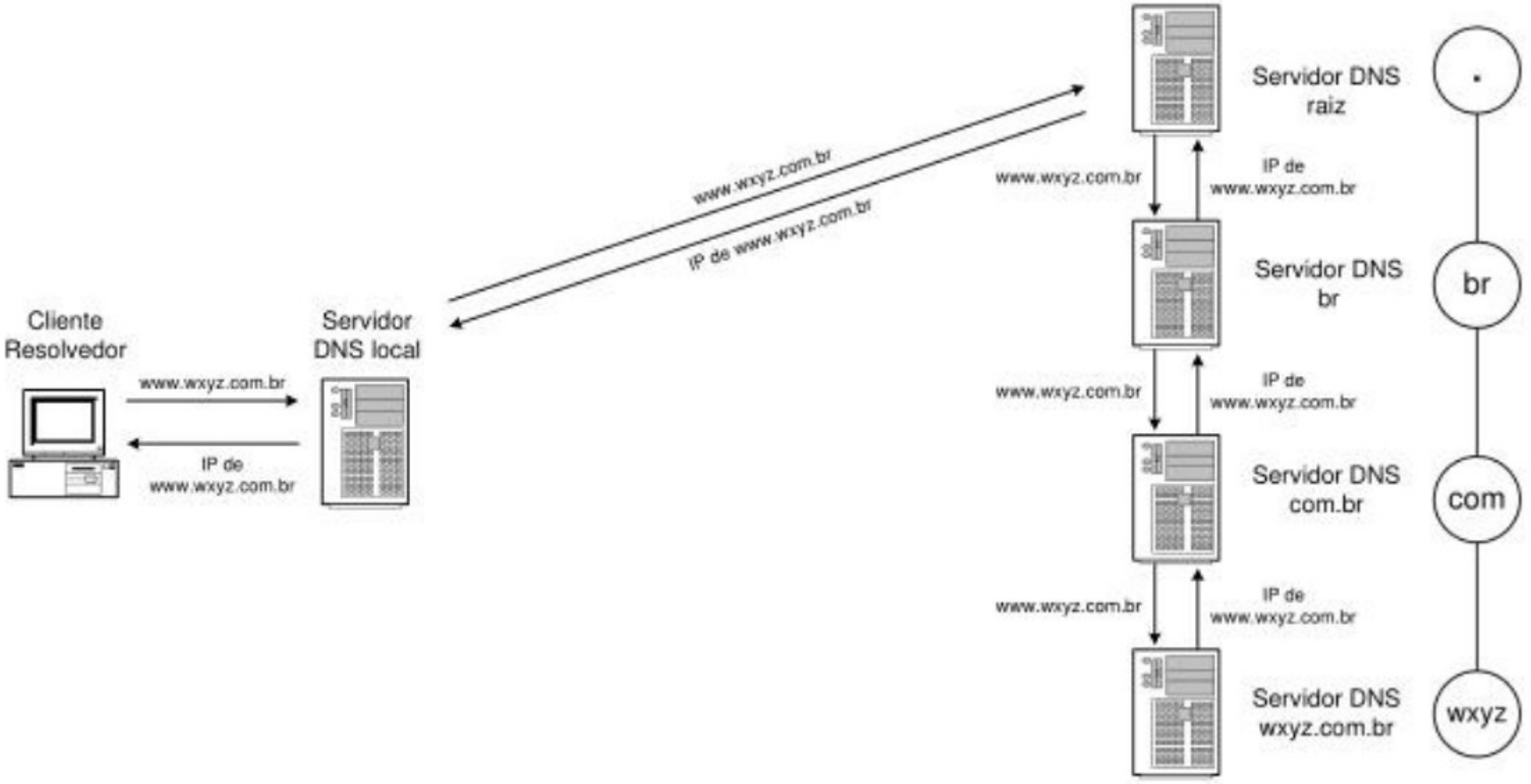
Cuando una aplicación quiere resolver un nombre invocará al resolutor:

1. El resolver consulta la caché de resolución de nombres del host. Si obtiene una respuesta positiva se la entrega a la aplicación.
2. Si el nombre buscado no está en la caché, buscará en el archivo hosts local del equipo.
3. Si el nombre buscado no está en el archivo hosts, el resolver efectuará una consulta al servidor de nombres que esté configurado y le entregará la respuesta a la aplicación.



Las consultas a un servidor DNS puede ser de 2 tipos: recursiva, iterativa.

Proceso de resolución. Consulta recursiva.



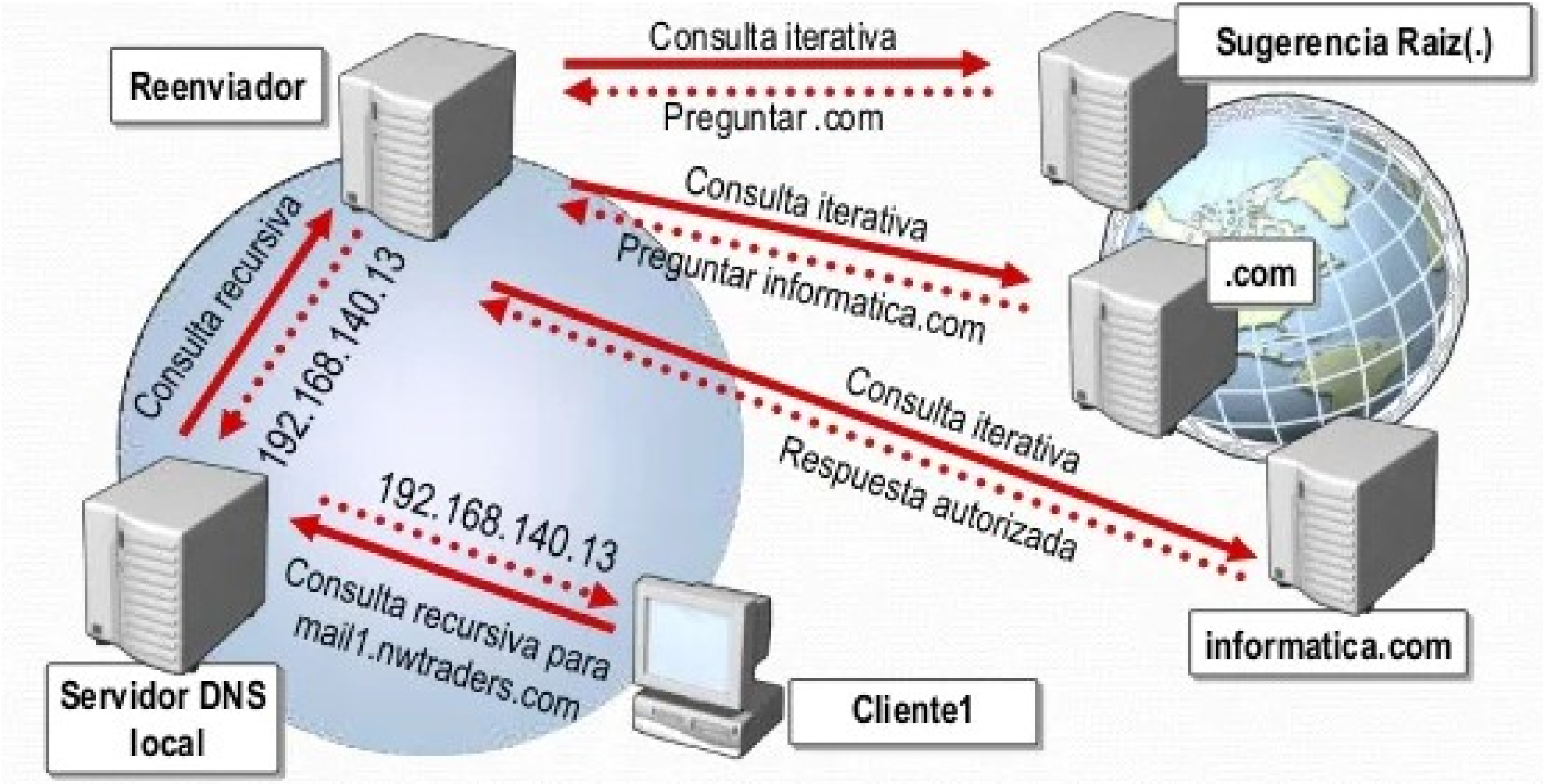
Proceso de resolución. Consulta recursiva.

Una consulta recursiva es aquella en la que el servidor tiene que dar una respuesta completa o exacta:

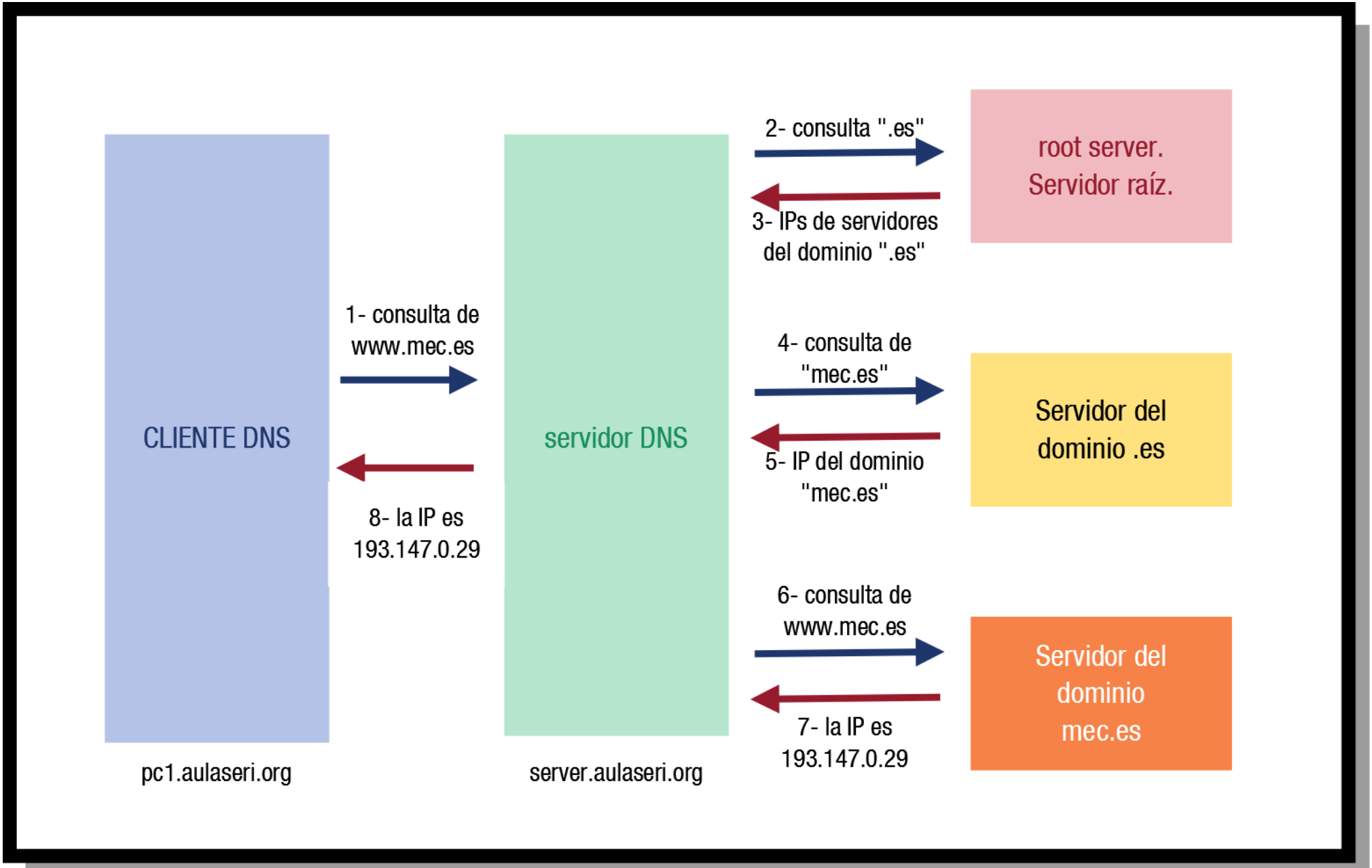
- Respuesta positiva, el nombre por el que se ha preguntado. En ella se indica si es autorizada o no. No es posible saber si el servidor que responde con autoridad es maestro o esclavo del dominio preguntado.
- Respuesta negativa, indica que el nombre no se puedo resolver (NXDOMAIN).
- Una indicación de error (ejemplo, no se pudo obtener una respuesta de otros servidores por fallos de la red.

Realmente las consultas recursivas solo se producen entre el cliente y el servidor local y entre este y el reenviador si existe.

Proceso de resolución. Consulta recursiva.



Proceso de resolución. Consulta iterativa.



Proceso de resolución. Consulta iterativa.

Una consulta iterativa (no recursiva) es aquella en la que el servidor DNS puede proporcionar una respuesta parcial. Hay 4 posibles respuestas:

- Respuesta positiva, el nombre por el que se ha preguntado. En ella indicará si es autorizada o no.
- Respuesta negativa: indica que el nombre no se puede resolver (NXDOMAIN).
- Respuesta indicando una referencia a otros servidores, autorizados o no, a los que se puede preguntar para resolver la pregunta (una referencia no es válida como respuesta a una consulta recursiva).
- Una indicación de error.

Las consultas iterativas son realizadas por servidores a otros servidores DNS después de haber recibido una consulta recursiva (no encontrando respuesta en sus archivos de zona o caché.

Proceso de resolución. Caché y TTL

Los clientes y servidores DNS mantienen en memoria caché (en caso de estar configurados) las respuestas a las preguntas que realizan otros servidores. El tiempo que guardan las respuestas en caché se denomina TTL (Time To Live) y se define en los archivos de zona de los servidores DNS preguntados.

Los clientes y servidores DNS almacenan en caché:

- Respuestas positivas. Registros de recursos de nombres resueltos.
- Respuestas negativas. Información de que no existen registros de recursos para un nombre consultado. Impiden las solicitudes adicionales para nombres que no existen.

En los ficheros de zona se define el tiempo que se guardarán en caché las respuestas positivas y las respuestas negativas.

La RFC 1912 recomienda que el valor TTL positivo sea de 1 día o mayor. La RFC 2308 indica que el máximo valor del TTL negativo sea 3 horas.

Para que un servidor DNS pregunte a otros servidores cuando recibe consultas recursivas tiene que tener activada la recursividad.

Resolución inversa.

En las resoluciones que hemos visto hasta el momento (directa) se obtiene una dirección IP a partir de un nombre de dominio.

También se puede realizar la consulta contraria, es decir obtener un nombre de dominio a partir de una dirección IP (inversa). Este tipo de resoluciones se utilizan con mucha menos frecuencia que la opuesta, se puede realizar y se usa, por ejemplo, como medida de seguridad.

Un cliente DNS consulta el nombre DNS www.mibanco.com y recibe como respuesta la IP 193.5.5.5. Puede ocurrir que mediante alguna técnica nos hayan enviado una IP que no corresponda al nombre DNS consultado para dirigirnos a otro sitio web fraudulento. Se puede verificar que la IP 193.5.5.5 corresponde realmente a www.mibanco.com solicitando la resolución inversa de esa dirección IP.

Resolución Inversa. Mapeo direcciones IP y dominio arpa.

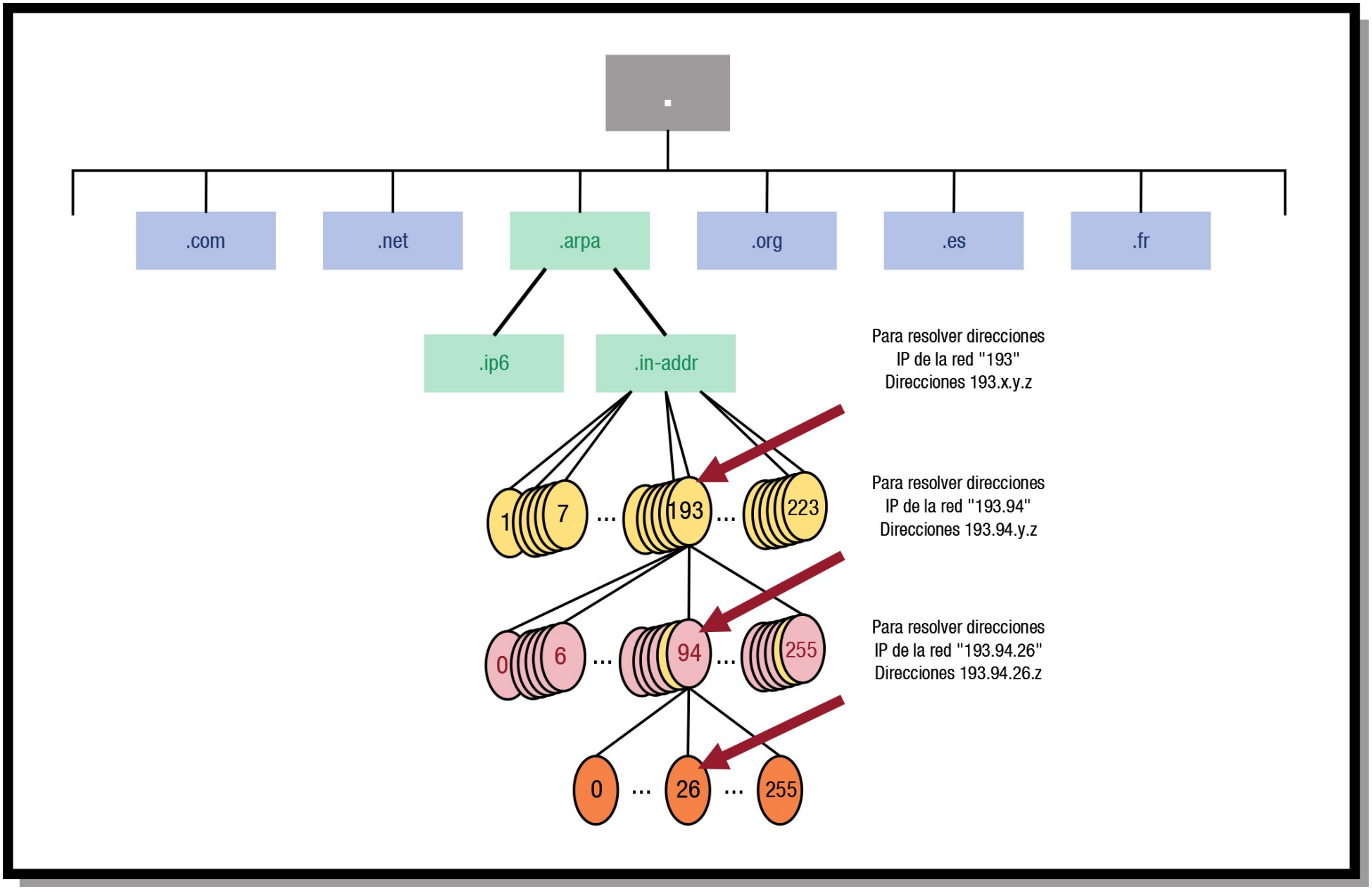
Para las resoluciones inversas se utiliza el dominio de primer nivel ".arpa" con sus correspondientes servidores:

- "in-addr.arpa" para resolver direcciones IPv4
- "ip6.arpa" para resolver direcciones IPv6.

Cualquier organización que tenga en propiedad una dirección de red debe responsabilizarse de tener servidores DNS que resuelvan inversamente las direcciones IP pertenecientes a la dirección de red.

- Cualquier nmobre de dominio www.midominio.es lo leemos y escribimos de izquierda a derecha, pero su estructura jerárquica es contraria: primero el raíz "**.**", después "**es**", después "**midominio**" y finalmente "**www**".
- Al realizar una consulta inversa (193.94.26.11) realmente estamos preguntando por el nombre de dominio "**11.26.94.193.in-addr.arpa.**".

Resolución Inversa. Mapeo direcciones IP y dominio arp



Resolución Inversa. Zonas de resolución inversa.

Los servidores de nombres tienen que almacenar zonas de resolución inversa con registros de recursos (RR) que asocien nombres de dominio con direcciones IP.

Las zonas directas e inversas son independientes, y es responsabilidad de los administradores que contengan información coherente y que no existan discrepancias.

Si administramos un dominio y asociamos un nombre con una IP pública contratada con un ISP tendremos que contactar con este para que modifique su zona inversa e incluya nuestro nombre de domino, si queremos que las consultas inversas a esa ip se resuelvan con el nombre apropiado.

Ejemplos fichero zonas resolución directa e inversa:

```
...
midominio.es.          IN   NS   ns1.midominio.es.
ns1.midomino.es.       IN   A    195.85.200.120
pc1.midominio.es.      IN   A    195.85.200.121
pc2.midominio.es.      IN   A    195.85.200.122
pc3.midominio.es.      IN   A    195.85.200.123
...
```

```
...
200.85.195.in-addr.arpa.          IN   NS   ns1.midominio.es.
120.200.85.195.in-addr.arpa.      IN   PTR  ns1.midominio.es.
121.200.85.195.in-addr.arpa.      IN   PTR  pc1.midominio.es.
122.200.85.195.in-addr.arpa.      IN   PTR  pc2.midominio.es.
133.200.85.195.in-addr.arpa.      IN   PTR  pc3.midominio.es.
...
```

Registro de recursos DNS. Formato.

El servicio DNS gestiona una base de datos distribuida entre múltiples servidores DNS que almacenan ficheros de zona con información sobre nombres de dominio. Cada fichero de zona organiza esta información en registros de recurso (RR) los cuales se envían en las preguntas y respuestas entre cliente y servidores DNS.

Formato:	NombreDeDominio	[TTL]	Clase	Tipo	Tipo-Dato
Ejemplo:	pc1.midominio.es	7200	IN	A	195.85.200.121

- NombreDeDominio: nombre del dominio con el que se asocia el recurso.
- TTL (Time To Live): n.º segundos que puede estar el registro en caché antes de ser descartado. Un TTL “0” indica que no debe ser almacenado en caché.
- Clase: define la arquitectura de protocolos utilizada. Para el caso TCP/IP sería IN.
- Tipo: tipo de registro. Diferentes en función del campo clase. Para IN podría ser (A, CNAME, NS, MX…).
- Tipo de dato: información asociada a nombre de dominio. Varía en función del tipo de registro. Por ejemplo para tipo A, dirección IP.

Tipos de registros. Registro SOA.

El registro SOA (Start Of Authority) es el primer registro de una zona y define una serie de opciones generales de la misma.

```
midominio.es.      IN    SOA      ns1.midominio.es.      admin.midominio.es.(
                                  1            ; N.º de serie
                                  604800       ; Tiempo de refresco
                                  86400        ; Tiempo de reintento
                                  2419200      ; Tiempo de expiración
                                  604800)      ; TTL negativo
```

```
paco@ServerPaco:~$ dig us.es soa

; <<>> DiG 9.18.30-0ubuntu0.22.04.1-Ubuntu <<>> us.es soa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7011
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;us.es.                         IN      SOA

;; ANSWER SECTION:
us.es.                  14400   IN      SOA     onix.us.es. redes.us.es. 2024121901 14400 7200 604800 14400

;; Query time: 48 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Dec 19 12:22:55 CET 2024
;; MSG SIZE  rcvd: 81
```

Tipos de registros. Registro SOA.

Los datos asociados con un registro SOA son los siguientes:

- MNAME: nombre FQDN del servidor de nombres maestro del dominio. Ejemplo: ns1.midominio.es
- Contacto (contact): correo de la persona responsable del dominio. Similar a una dirección de correo normal, salvo que la @ se reemplaza por un ".". admin.midominio.es
- Número de serie: indica la versión del archivo de zona y debe ser incrementado cada vez que el archivo se modifique. Es usual utilizar fecha en formato "aaaammdd" agregándole 2 dígitos si los cambios se hacen el mismo día.
- Actualización(refresh): tiempo que esperan los servidores esclavos para preguntar al servidor maestro si hay cambio de zona. Valores entre 1200 y 43200.
- Reintentos (retry): si la transferencia de zona ha fallado, indica el tiempo que espera el secundario antes de volver a intentarlo. Valores inferiores al tiempo de actualización.
- Caducidad (expire): determina el tiempo que el servidor esclavo puede estar intentando contactar con el maestro para ver si hay cambios de zona. Si el tiempo expira no responde a preguntas sobre esa zona.
- TTL negativo (Time To Live): tiempo mínimo que se almacenan las respuestas negativas sobre esa zona. Diferente al TTL de los RR.

Tipos de registros. Registro NS.

El registro de recursos NS (Name Server) permite establecer:

- El/los servidores de nombres autorizados en una zona.
- Cada zona debe contener, como mínimo, un registro NS.
- Quienes son los servidores de nombres con autoridad en los subdominios delegados.
- Cada zona debe contener, al menos, un registro NS por cada subdominio que haya delegado.

```
midominio.es.        IN   NS   ns1.midominio.es.     ; Servidor DNS maestro
midominio.es.        IN   NS   ns2.midominio.es.     ; Servidor DNS esclavo

ns1.midominio.es.    IN   A    195.85.200.120
ns2.midominio.es.    IN   A    195.85.200.121

;Delegación
sub.midominio.es.    IN   NS   ns1.sub.midominio.es.      ; Delegación
```

Tipos de registros. Registro A y AAA

El registro de recursos A (Address) establece una correspondencia entre un nombre de dominio completamente cualificado (FQDN) y una dirección IPV4.

El registro de recursos AAAA establece una correspondencia entre nombres de dominio completamente cualificado (FQDN) y una dirección IPV6.

```
ns1.midominio.es.   IN   A      195.85.200.120
ns2.midominio.es.   IN   A      195.85.200.121
pc1.midominio.es.   IN   A      195.85.200.122
pc2.midominio.es.   IN   A      195.85.200.123
Pc1.midominio.es.   IN   AAAA   ::ffff:c355:c87a
Pc2.midominio.es.   IN   AAAA   ::ffff:c355:c87b
```

Tipos de registros. Registro CNAME.

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

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

No se deben usar registros CNAME en la parte derecha de registros MX y NS. La parte derecha de estos recursos tiene que ser un nombre que aparezca en un registro de tipo A.

El uso de muchos CNAME perjudica el rendimiento de los servidores DNS. Cuando se pregunta por un registro CNAME hay que buscar dos veces en el fichero de zona para encontrarlo.

```
pc1.midominio.es.      IN   A       195.85.200.122
alias1.midominio.es.   IN   CNAME   pc1.midominio.es.
bd.midominio.es.       IN   CNAME   pc2.midominio.es.
www.midominio.es.      IN   CNAME   www.otrodominio.es.
```

```
midominio.es.          IN   NS      dns.midominio.es. ;Mal, dns es un CNAME

midominio.es.          IN   NS      ns1.midominio.es. ;Bien.

ns1.midominio.es.      IN   A       195.85.200.120
dns.midominio.es.      IN   CNAME   ns1.midominio.es.
```

Tipos de registros. Registro MX

El registro MX (Mail Exchange) permite definir equipos encargados de la entrega de correo en el dominio. Son consultados por los agentes de transporte de correo SMTP.

Un registro MX puede apuntar a un nombre de otro dominio.

Es posible definir varios registros MX para un mismo dominio, es decir, varios servidores de correo para ese dominio. En cada registro MX se especifica un número positivo (0 – 65535) que determina la preferencia en el caso de que existan varios registros MX.

La parte derecha de un registro MX no debe ser un nombre de tipo CNAME.

```
midominio.es.          IN   MX     10   mail1.midominio.es.
midominio.es.          IN   MX     20   mail2.midominio.es.
...
mail3.midominio.es.    IN   MX     30   smtp.informatica.es.
...
mail1.midominio.es.    IN   A           195.85.200.125
mail2.midominio.es.    IN   A           195.85.200.126
```

Tipos de registros. Registro SRV y PTR

El registro SRV (Services Record) permite definir equipos que soportan un servicio en particular.

Windows usa los registros SRV en los servidores DNS de un dominio para identificar controladores de dominio, servidores Kerberos, servidores web, servidores de correo, etc.

El registro PTR (Pointer Record) establece una correspondencia entre nombres de direcciónes IPv4 e IPv6 y nombres de dominio. Se utiliza por tanto en las zonas de resolución inversa.

En una misma zona no puede haber registros PTR IPv4 y registros PTR IPv6. Existen zonas de resolución inversa IPv4 y zonas IPv6.

```
121.200.85.195.in-addr.arpa.   IN   PTR   ns1.midominio.es.
122.200.85.195.in-addr.arpa.   IN   PTR   ns2.midominio.es.
123.200.85.195.in-addr.arpa.   IN   PTR   pc1.midominio.es.
```

Delegación y registro pegamento (Glue Record)

La organización que administra un servidor de nombres y por tanto, sus zonas, puede decidir delegar algunos de sus subdominios a otros servidores de nombres. Se puede diferenciar 2 casos:

- El nombre del servidor DNS autorizado del subdominio (en el que se delega) se encuentra dentro del propio subdominio.
  - Hay que añadir un registro NS en la zona del padre para la zona delegada.
  - Hay que añadir un registro de tipo A para indicar la dirección IP del servidor de nombres autorizado para la zona delegada.
    - A este tipo de registros se les denomina “glue record” (une zona “hija” con zona “padre”)
    - En caso de no colocar este o hacerlo incorrectamente, parte del espacio de nombre quedará inaccesible.
    - Los servidores de un dominio padre deben conocer la dirección IP de los servidores de todos sus subdominios.

```
midominio.es.              IN   NS  ns1.midominio.es.     ; Servidor DNS maestro
...
ns1.midominio.es.     IN   A   195.85.200.120
...
;Delegación
sub.midominio.es.          IN   NS  ns1.sub.midominio.es.      ; Delegación
ns1.sub.midominio.es.      IN   A   195.85.200.140   ;Glue Record
```

Delegación y registro pegamento (Glue Record)

- En el caso de que el servidor DNS del subdominio (delegado) no se encuentre en el subdomino:
  - Hay que añadir un registro NS en la zona del padre que define el servidor de nombres autorizado para la zona delegada.
  - No hace falta (ni se añade) un registro de tipo A para indicar la dirección IP del servidor de nombres autorizado para la zona delegada.
    - Es un error incluir registros de pegamento para nombres de host que no los necesitan.
    - Por norma se deben incluir registros A unicamente para los hosts que están dentro del dominio o cualquiera de sus subdominios.

```
midominio.es.          IN   NS   ns1.midominio.es.    ; Servidor DNS maestro
midominio.es.          IN   NS   ns2.midominio.es.    ;Servidor DNS esclavo
midominio.es.          IN   NS   dns.midominio.org.   ;Servidor DNS esclavo

ns1.midominio.es.      IN   A    195.85.200.120
ns2.midomino.es.       IN   A    195.85.200.121

;Delegación
sub2.midominio.es.     IN   NS   dns.midominio.org.   ; Delegación
```

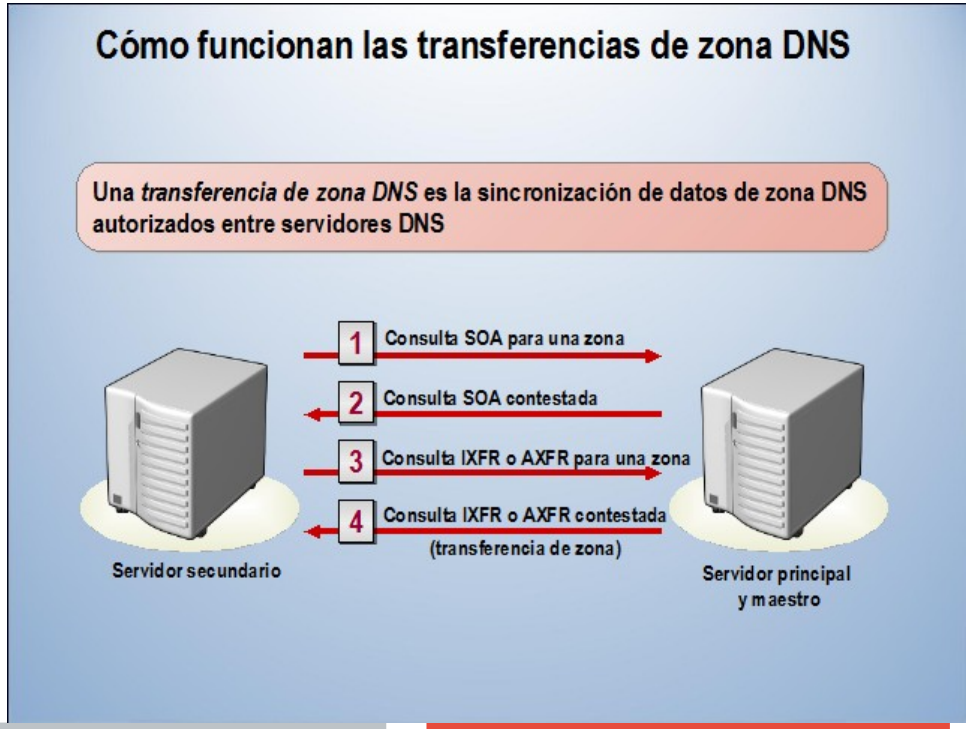
Transferencias de zona.

Las zonas pueden ser primarias y secundarias. Una zona secundaria siempre será copia de una zona primaria.

Los servidores secundarios realizan cada cierto tiempo una actualización de la zona. Para ello solicitan al servidor primario el envío de una copia de la zona primaria. Esta copia enviada actualiza los registros en la zona secundaria.

El proceso de actualización de una zona secundaria con una copia de la zona primaria se llama transferencia de zona.

Cuando se inicia, un servidor secundario solicita una transferencia de zona al primario. En el secundario se puede configurar cada cuanto tiempo deben realizar las transferencias de zona. Especialmente para zonas que contienen mucha información, se suelen realizar transferencias de zona incrementales en las que sólo se envían los datos modificados en la zona desde la última transferencia.



Transferencias de zona. Tipos

- Transferencia de zona completas (AXFR): el servidor maestro le envía al servidor esclavo todos los datos de la zona. Una petición AXFR de un servidor esclavo a uno maestro es una solicitud para una transferencia de zona completa. Las especificaciones originales para el servicio DNS (rfc 1034, rfc 1035) solo contemplaban este tipo de transferencia.
- Trasferencia de zona incremental (IXFR): la transferencias completas de zonas con muchos registros consumen ancho de banda y pueden llegar a tardar un tiempo considerable según condiciones de la red y tamaño de la zona. Para evitar esto en la rfc 1995 se introdujeron transferencias de zona incrementales.

  En este tipo de transferencias el servidor maestro le envía al esclavo solo los datos que han cambiado desde la última transferencia de zona.

DNS Dinámico (DDNS)

Para tener acceso a los recursos los servidores NDS deben estar actualizados. Esta actualización puede realizarse manualmente o dinámicamente.

- Actualizaciones manuales: el administrador crea, elimina o modifica los RR editando los ficheros de zona.
- Actualizaciones dinámicas: se crean o modifican los registros de recursos por parte de una fuente externa sin edición de los ficheros de zona por parte del administrador, pueden realizarse:
  - ➔ Directamente por los equipos: configurar el cliente DNS de cada equipo, configurar el servidor DNS para que permita actualizaciones dinámicas por parte de los equipos.
  - ➔ Por parte del servidor DHCP: configurar adecuadamente el servidor DHCP, configurar adecuadamente los clientes DHCP para que envíen su nombre al servidor DHCP o configurar el servidor DHCP para que les asigne un nombre, configurar el servidor DNS para que permita actualizaciones dinámicas por parte del servidor DHCP.

Las actualizaciones dinámicas pueden suponer un riesgo para la seguridad. Si una fuente externa no autorizada consigue enviar actualizaciones dinámicas al servidor, sus ficheros de zona serán “envenenados”.