14/09/2024

Stoyanov Angel Krasimirov

Servicio en red: DNS

Tipos de servidores

Tipos de zonas y registros

Ejemplificado

Índice

DNS

DNS[3] (Servidor de Nombres de Dominios. En inglés, *Domain Names Server*) Es un **servicio en red** que nos permite **traducir nombres de dominios** a sus respectivas **direcciones IP** y viceversa.

Historia

Este servicio nació para poder solventar el problema que presentaba tener que **recordar** direcciones IP (numéricas) para conectarse a los servidores y servicios en red.

Los humanos tienen una **importante deficiencia** a la hora de **relacionar cosas con sistemas numéricos**, en comparación con sistemas alfanuméricos. Esto probó ser un gran problema en los inicios de lo que conocemos hoy como Internet. En aquel entonces, **cada persona recopilaba**, personalmente, las direcciones IPv4 de los **servidores** y **servicios en red** de su interés, así como **contactos** (ordenadores personales).

Para solventar este problema, se decidió **centralizar** esta recopilación de información (direcciones IP) en un único servidor, séase, **archivo**. Y, para poder distinguir las direcciones entre sí, se decidió nombrarlas. Aquí es donde nació la idea de los nombres, en vez de números, usábamos **caracteres alfanuméricos para identificar cada dirección**.

Esto funcionó perfectamente hasta que internet experimentó un **crecimiento exponencial** liderado por empresas emprendedoras y empresarios. Tener de esta forma los registros resultó ser **poco práctico** (imposible a día de hoy), por lo que Jon Postel junto con Paul Mockapetris definen en 1983 lo que sería el **precursor** de lo que conocemos como DNS.[3]

Tipos de servidores DNS

Principalmente, existen tres tipos de servidores de nombres de dominio: **Principales** (*Maestros*), **Secundarios** (*Esclavos*) y **Cache**.

Principales

El servidor DNS Principal o Maestro es aquel que **posee la autoridad** sobre la **zona que administra**. Sobre una zona **solo puede existir un servidor autoritario** y, por ende, un servidor principal. Responden **peticiones** a **resolutores** (*resolver*, en inglés).

Secundarios

Los servidores DNS Secundarios o Esclavos son idénticos que los Principales, excepto en estos puntos:

- Puede haber un **número arbitrario** de servidores secundarios.
- **No son autoritarios**. No tienen la autoridad sobre la zona por la que responden.

Su función se centra en la **mejora de la disponibilidad** y la **distribución de carga**. Son servidores que **copian información** (zonas) de los servidores principales a los que han sido asignados, siempre que estos los **autoricen** (de confianza. En inglés, *trusted*).

Cache

Estos servidores son **intermediarios** entre los clientes y el resto de servidores DNS, en pos de **reducir la carga** de la red. **Guardan** y **revisan** consultas anteriores y, en defecto de estas, **realizan nuevas consultas** en nombre de los clientes.

Zonas

Las zonas en un servidor DNS son **niveles de dominios**. Por ejemplo, "`angelkrasimirov.es`" es el dominio de la zona "`angelkrasimirov`", que a su vez se encuentra definida en la zona "`es.`". Dicha zona **se encontrará guardada**, generalmente, **en un archivo** llamado "`db.angelkrasimirov.es`" localizado en el **servidor principal** (*maestro*) del dominio.

Existen dos tipos de zonas. Las de resolución o búsqueda **directa** y resolución o búsqueda **inversa**.

De Resolución Directa

Las zonas de búsqueda directa se centran en **resolver nombres** a **direcciones IP**. Son las **más importantes**, en ellas se basa el concepto DNS. En estas zonas podemos encontrar una gran variedad de **tipos de registros**.

Registros más comunes			
ID	Nombre	Nombre en inglés	Descripción
A	Dirección IPv4	*Address IPv4*	Relacionan un nombre con una dirección IPv4
AAAA	Dirección IPv6	*Address IPv6*	Relacionan un nombre con una dirección IPv6
MX	Intercambio de Correo	*Mail Exange*	Definen el nombre del servidor de correo
CNAME	Nombre Canónico	*Canonical Name*	Definen un alias para un nombre
SOA	Autoridad de la Zona	*Start of Authority*	Define información básica acerca de una zona de la que se es autoritario

De Resolución Inversa

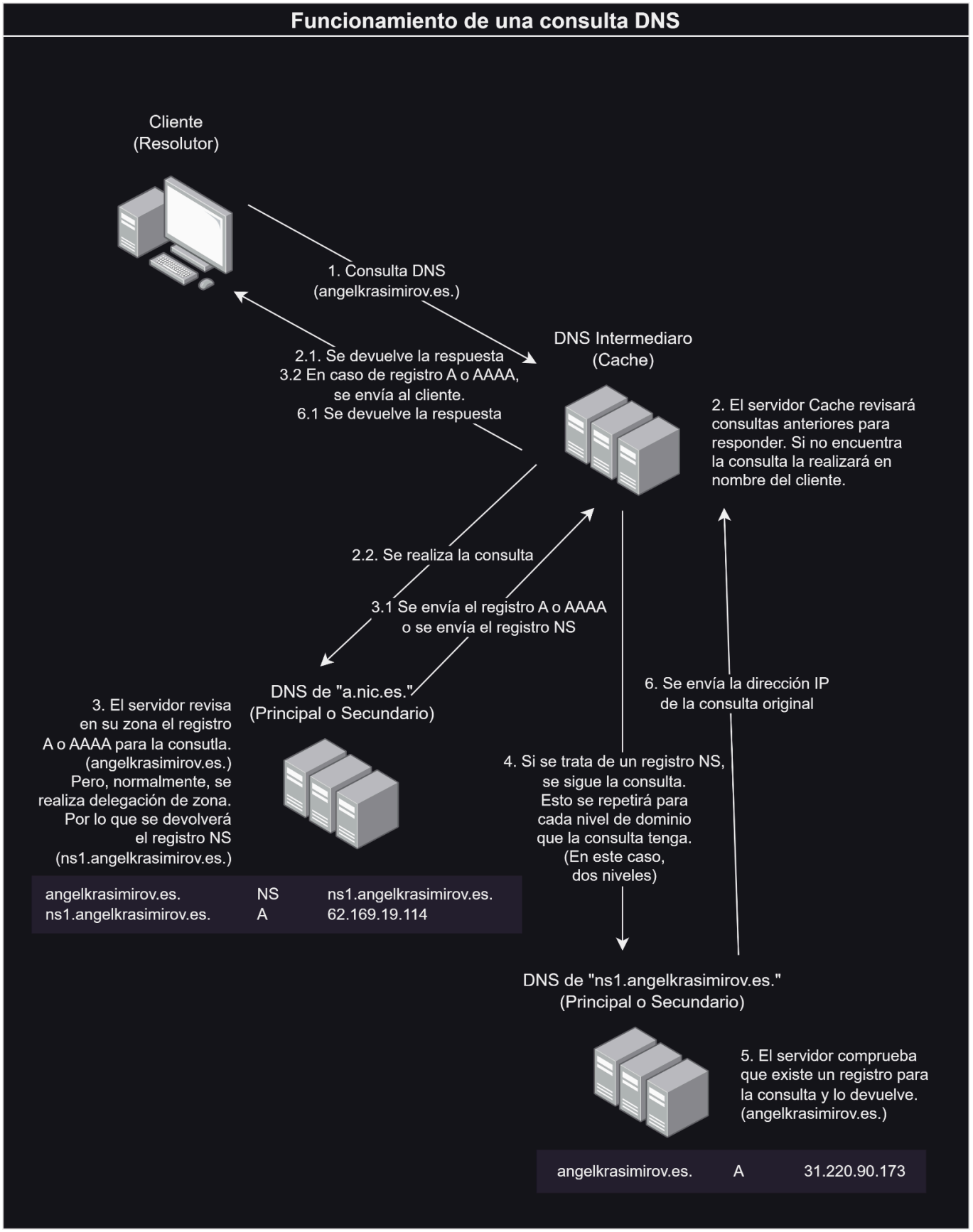
Estas zonas son las antípodas de las búsquedas directas, pues su función es resolver **direcciones IP** a **nombres**. En ellas se **invierten** las direcciones IP y se define qué nombres están relacionados con dichas direcciones.

La resolución inversa ha perdido popularidad con los años, llegando a ser algo completamente opcional para un servidor DNS. Es decir, no se espera que un servidor DNS provea, de forma obligatoria, zonas para la búsqueda inversa. Sin embargo, en el caso de **servidores de correo**, prevalece la necesidad de establecer zonas de búsqueda inversa como **método de seguridad**. Puesto que estas son utilizadas por otros para **verificar** que los correos recibidos son, en efecto, del servidor de correo correcto.

Estas zonas se caracterizan por tener un solo tipo de registro, el **PTR** (Registro de Recurso. En inglés, *Point Record*). Su función es **relacionar una dirección IP con un nombre**.[7]

Consulta DNS

Una consulta DNS se basa en realizar **diferentes peticiones** hasta **encontrar** el resultado deseado o alcanzar el **final de la cadena**. El final de dicha cadena está determinado por el servidor que proporciona el nivel de dominio que estamos buscando. En este ejemplo vemos una consulta **iterativa**.[8]



Registros de zona

En el siguiente ejemplo, vamos a ver un archivo de la zona directa de un dominio llamado "`example.com.`". Veremos que es cada registro y cómo funciona, línea por línea.

Ejemplo

```
ORIGIN example.com.
TTL   86400
@           IN          SOA         dns1.example.com. hostmaster.example.com. (
                                    2001062501 ; serial
                                    21600 ; refresh after 6 hours
                                    3600 ; retry after 1 hour
                                    604800 ; expire after 1 week
                                    86400 ) ; minimum TTL of 1 day

            IN          NS          dns1.example.com.
            IN          NS          dns2.example.com.

dns1        IN          A           10.0.1.1
            IN          AAAA        aaaa:bbbb::1
dns2        IN          A           10.0.1.2
            IN          AAAA        aaaa:bbbb::2
;
;
@           IN          MX 10       mail.example.com.
            IN          MX 20       mail2.example.com.
mail        IN          A           10.0.1.5
            IN          AAAA        aaaa:bbbb::5
mail2       IN          A           10.0.1.6
            IN          AAAA        aaaa:bbbb::6

; This sample zone file illustrates sharing the same IP addresses for multiple
services:

services    IN          A           10.0.1.10
            IN          AAAA        aaaa:bbbb::10
            IN          A           10.0.1.11
            IN          AAAA        aaaa:bbbb::11
ftp         IN          CNAME       services.example.com.
www         IN          CNAME       services.example.com.
```

Desglose

```
ORIGIN example.com.
```

El campo "`ORIGIN`" (en español, origen) no es un registro, sino una pseudo variable. Nos permite definir el dominio que administrará la zona que estamos configurando, para, más adelante, utilizar el carácter "`@`" para representar el mismo, en este caso "`example.com.`" Es completamente opcional.

Cuando vemos un **signo de puntuación al final** de un nombre significa que es un **FQDN** (Nombre de Dominio Totalmente Cualificado. En inglés, *Fully Qualified Domain Name*).[5]

```
TTL    86400
```

"`TTL`" significa Tiempo de Vida (en inglés, *Time To Live*). Tampoco se considera un registro, sino meramente un campo. Define, en segundos, el tiempo que cada registro será **guardado** por los servidores de tipo cache. Afecta la disparidad que existe entre el cliente y los cambios realizados.

```
@           IN          SOA         dns1.example.com. hostmaster.example.com. (
                                    2001062501 ; serial
                                    21600 ; refresh after 6 hours
                                    3600 ; retry after 1 hour
                                    604800 ; expire after 1 week
                                    86400 ) ; minimum TTL of 1 day
```

Recordemos que "`@`" es una pseudo variable, y será traducida a, en este caso, "`example.com.`"

Lo primero que vemos es "`IN`"[3]. Significa **Internet** y es la **clase del registro** al que precede. A día de hoy, es difícil ver registros de clases diferentes que "`IN`", por lo que, prácticamente, se puede considerar como la única clase existente, aunque sea falso.

El registro "`SOA`"[4] significa "Autoridad de la Zona" (en inglés, *Start of Authority*) y define la autoridad sobre un dominio, en este caso "`example.com.`". También, define una serie de parámetros e información básica.

> Lo primero que se define es el **MNAME** (Nombre del Maestro. En inglés, *Master Name*). Es el servidor DNS que será primario (autoritativo) de la zona. En este caso "`dns1.example.com.`".
>
> Luego definimos el **RNAME** (Nombre del Responsable. En inglés, *Responsible Name*). Es el nombre de dominio del correo de la entidad responsable de la zona.
> En este caso es "`hostmaster.example.com.`", aunque en realidad se traduce a "`hostmaster@example.com.`". Porque la primera etiqueta se convierte en la parte anterior al "`@`" en una dirección de correo electrónico, el resto de etiquetas confirman la parte posterior.
>
> Luego se abren unos paréntesis para ingresar una serie de parámetros numéricos separados por saltos de línea. El primero siendo **SERIAL**. Un número de 32 bits que identifica la **versión** actual de la zona. Cada vez que esta se actualiza, se incrementa en uno. Muy útil cuando existen servidores secundarios, pues así saben en qué versión se encuentran. En este caso el identificador está en "`2001062501`", que no tiene por qué decir que sea la versión dos mil un millonésima sesenta y dos milésima quingentésima primera, pues se puede inicializar en cualquier valor deseado.

El siguiente es **REFRESH**, refresco o actualización. Define, en segundos, el tiempo que han de esperar los servidores secundarios antes de intentar **renovar su información** respecto al servidor primario. En este caso "`21600`" segundos.

Luego tenemos **RETRY**, reintentar. Define, en segundos, el tiempo que debe pasar antes de que los servidores secundarios consideren el primario como **caído**. En este caso "`3600`" segundos.

Como penúltimo parámetro, tenemos **EXPIRE**. Define, en segundos, el tiempo durante el cual los servidores secundarios seguirán proveyendo la zona tras haber pasado el tiempo de RETRY. En este caso "`604800`" segundos.

Por último, está **MINIMUM**. Aunque en el pasado fuese diferente, hoy en día define, en segundos, el TTL. Será usado si el campo TTL no hubiera sido establecido. En este caso "`86400`" segundos.

```
            IN          NS          dns1.example.com.
            IN          NS          dns2.example.com.
```

Tras el registro "`SOA`" se han asignado dos más a este. Ambos son registros "`NS`"[6] que definen los servidores DNS a los que se puede acudir para encontrar la zona de "`example.com.`". En este caso se definen dos, "`dns1.example.com.`" y "`dns2.example.com.`", con el objetivo de mejorar la disponibilidad y la distribución de carga.

```
dns1        IN          A           10.0.1.1
            IN          AAAA        aaaa:bbbb::1
dns2        IN          A           10.0.1.2
            IN          AAAA        aaaa:bbbb::2
```

Los registros "`A`"[6] y "`AAAA`"[6] asignan a un nombre una dirección IPv4 o IPv6, respectivamente. En este caso se han asignado direcciones tanto IPv4 como IPv6 a los nombres "`dns1`" y "`dns2`". Cuando el nombre que se escribe no es un FQDN, quiere decir que le precede al nombre de dominio de la zona, que sí es FQDN. En este caso "`dns1.example.com.`" y "`dns2.example.com.`".

```
@           IN          MX 10       mail.example.com.
            IN          MX 20       mail2.example.com.
mail        IN          A           10.0.1.5
            IN          AAAA        aaaa:bbbb::5
mail2       IN          A           10.0.1.6
            IN          AAAA        aaaa:bbbb::6
```

El registro "`MX`"[6] (Intercambio de Correo. En inglés, *Mail Exange*) define el nombre del servidor de correo de la zona. Los correos que vayan dirigidos a dicha zona serán enviados a estos servidores. El número que sucede al identificador del registro indica la preferencia. En este caso, "`mail.example.com.`" tiene una preferencia de `10` y "`mail2.example.com.`" una preferencia de `20`.

Luego, mediante registros "`A`" y "`AAAA`", se definen las direcciones IP de estos servidores.

```
services    IN          A           10.0.1.10
            IN          AAAA        aaaa:bbbb::10
            IN          A           10.0.1.11
            IN          AAAA        aaaa:bbbb::11
```

Como podemos ver, se están usando registros tipo “A” y “AAAA”. Pero, existen más de uno para el mismo nombre. Esto se hace para mejorar la disponibilidad y la distribución de carga, pues facilita a los clientes varias opciones para un mismo servicio.[1][2]

```
ftp         IN          CNAME       services.example.com.
www         IN          CNAME       services.example.com.
```

Por último vemos el registro “CNAME”[6]. Define un alias para un nombre. En este caso “`ftp.example.com.`” será exactamente lo mismo que “`services.example.com.`”. Lo mismo para “`www.example.com.`”, que será exactamente lo mismo que “`services.example.com.`”.

Fuentes

1. RFC 1034 (en inglés). Para contrastar información de otras fuentes.
2. RFC 1035 (en inglés). Para contrastar información de otras fuentes.
3. DNS Wikipedia. Información general.
4. Registro SOA Wikipedia (en inglés). Información detallada acerca del registro SOA y sus parámetros.
5. Nombre de Dominio Totalmente Cualificado Wikipedia (en inglés). Información detallada acerca del funcionamiento de los FQDN.
6. Tipos de Registros DNS Wikipedia (en inglés). Listado de los tipos de registros DNS.
7. Registro tipo PTR Wikipedia (en inglés).
8. Consulta DNS (en inglés). Diferencia y funcionamiento de las consultas iterativas y recursivas.

Complementarias

Fuentes complementarias usadas para contrastar información, pero no incluidas en la elaboración de este documento.

- ¿Qué es DNS? Información general, detallando procesos con explicaciones claras e ilustraciones.
- Tipos de servidores DNS (en inglés). Información breve pero concentrada acerca de los tipos de servidores DNS.
- ¿Qué es una zona DNS? (en inglés). Información aclarativa acerca de las zonas DNS.
- ¿Cómo funciona la resolución inversa? (en inglés). Información aclarativa acerca de la resolución inversa y su funcionamiento.

No disponibles al público

Fuentes no disponibles al público al momento de elaborar este documento.

- **UD_1_Servicios de red.odt**. Documento a modo de teoría adjuntado en el campus.
  Hash del documento, utilizando "`sha256sum`":
  `2f5cfc58770fa6d828607b2af3d744ad92f2c000693b4d5b2dba72ddbe58b7a9`