Conceptos e operacións básicas con DNS
Despregamento de Aplicacións Web

IES de Teis
Curso 2020-2021

Índice

1. A01. Conceptos e operacións básicas con DNS

1.1 Introdución

Nesta actividade exporemos, de maneira introdutoria, os principais mecanismos de resolución de nomes de dominio.

Para iso teremos que comezar por analizar os escenarios nos que aparece a necesidade de contar cun servizo de resolución de nomes de dominio e cales son os mecanismos que mellor se adaptan a cada situación.

Unha vez feito isto, describiremos a estrutura, a nomenclatura e a funcionalidade dos sistemas de nomes xerárquicos.

1.2 Actividade

1.2.1 Que é DNS?

Grazas ao sistema de nomes de dominio ou DNS (polas siglas en inglés de *Domain Name System*), os sistemas conseguen conectarse uns cos outros de maneira máis sinxela. Sen DNS, os equipos (e os usuarios que os empregan) teríanse que conectar empregando unicamente enderezos numéricos coñecidos como enderezo IP.

Un nome de dominio, a miúdo denominado simplemente dominio, é un nome sinxelo de lembrar e asociado a un enderezo IP físico de Internet. Trátase dun nome único que se amosa despois de www. nos enderezos web e despois do signo @ nos enderezos de correo electrónico.

DNS é unha base de datos distribuída e xerárquica que almacena información asociada a nomes de dominio tanto en redes locais como en Internet. Aínda que como base de datos o DNS é capaz de asociar distintos tipos de información a cada nome, os usos máis comúns son a asignación de nomes de dominio a enderezos IP e a localización dos servidores de correo electrónico de cada dominio.

Os motivos para descentralizar a BBDD, principalmente, son:

- Evitar ter un único punto de fallo.
- Balancear a carga xa que o volume de tráfico é importante.
- Evitar retardos derivados da distancia que pode existir a unha única BBDD centralizada.
- Favorecer a escalabilidade do sistema.

A asignación de nomes a enderezos IP é certamente a función máis coñecida de DNS. Ademais de ser máis doado de recordar, o nome é máis fiable. O enderezo numérico podería cambiar por moitas razóns, sen que teña que cambiar o nome, ou mesmo podería darse o caso de que houbese máis dunha páxina web aloxada no mesmo servidor e que este teña soamente un enderezo IP, sendo necesario acceder empregando o nome de dominio para que o servidor web diferencie a que sitio se quere acceder.

Pode consultarse unha introdución ao sistema de nomes de dominio (DNS) no RFC 1034 na seguinte ligazón https://www.ietf.org/rfc/rfc1034.txt

1.2.2 Funcionamento de DNS

Para a operación práctica do sistema DNS utilízanse tres compoñentes principais:

- Os *clientes DNS* (resolvers ou resolutores), que son programas executados na computadora do usuario e que xera peticións DNS de resolución de nomes a un servidor DNS (por exemplo: Que enderezo IP corresponde a nome.dominio?).
- Os *servidores DNS* (name servers), que contestan as peticións dos clientes.
- *Zonas de autoridade*, que son porcións do espazo de nomes de dominio que almacenan os datos. Cada zona de autoridade abrangue polo menos un dominio e posiblemente os seus subdominios, se estes últimos non son delegados a outras zonas de autoridade.

Un nome de dominio usualmente consiste en dúas ou máis partes (chamadas tecnicamente etiquetas), separadas por puntos. Por exemplo: www.xunta.es ou www.google.es.

Á etiqueta situada máis á dereita chámaselle *dominio de nivel superior (Top Level Domain)*. Como *es* en www.google.es. Cada etiqueta á esquerda especifica unha subdivisión ou subdominio.

En teoría, esta subdivisión pode ter ata 127 niveis, e cada etiqueta conter ata 63 caracteres, pero restrinxido a que a lonxitude total do nome do dominio non exceda os 255 caracteres. Sen embargo, na práctica, os dominios son case sempre moito máis curtos (para que sexan doados de recordar).

Finalmente, a parte máis á esquerda do dominio adoita expresar o *nome da máquina* (en inglés, *hostname*), aínda que isto non ten porque ser exactamente así.

Os nomes de dominio están estruturados en forma de árbore dende a raíz (representada por un ". ") ata ou nivel inferior. A esta estrutura chámaselle *espazo de nomes de dominio*. Cada nivel sepárase do superior por un punto. Aos dominios que se atopan xusto debaixo do dominio raíz chámaselles dominios de primeiro nivel.

Cabe destacar que os *FQDN (fully qualified domain name)* rematan en punto, aínda que este sempre se soe omitir.

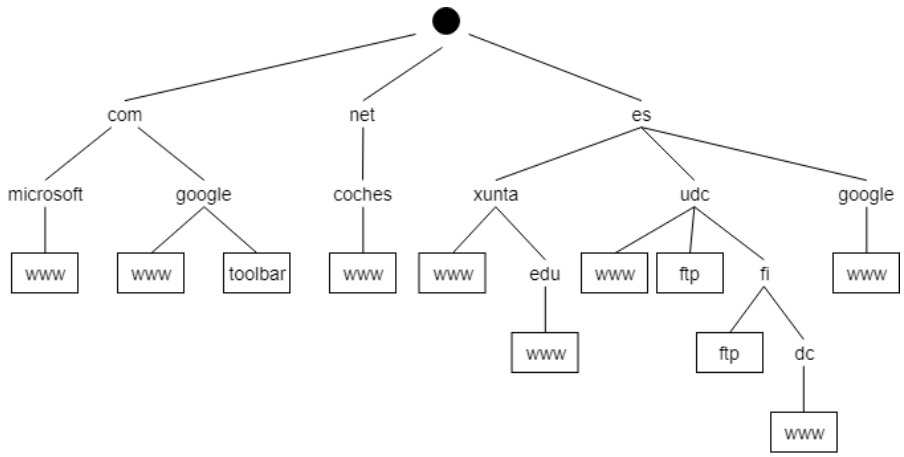

Figura 1 – Espazo de nomes de dominio.

Pode consultarse a implementación e especificación do sistema de nomes de dominio (DNS) no RFC 1035 na seguinte ligazón https://www.ietf.org/rfc/rfc1035.txt

1.2.3 Resolución nos clientes

Os usuarios domésticos non adoitan realizar directamente consultas de resolución de nomes, senón que son as aplicacións de cliente (navegadores web, clientes FTP, etc.) as que realizan esas consultas de modo transparente para os usuarios.

O proceso para resolver un nome de dominio nun equipo cliente realízase segundo a seguinte orde (aínda que esta pode ser alterada):

- Equipo cliente comproba se o nome a consultar é o seu propio nome.
- Compróbase o ficheiro *hosts*:
  - En Windows este ficheiro está en *C:\Windows\System32\drivers\etc\hosts*
  - En equipos Linux en */etc/hosts*
- Compróbase a caché DNS local (nalgunhas distribucións de Linux, como Debian, a caché DNS pode que non se utilice e para activala habería que instalar o paquete nscd).
- En caso de que o equipo cliente non consiga resolver o nome de dominio mediante ningún dos métodos anteriores envíase unha consulta ao servidor DNS configurado en primeiro lugar. Só se non consigue contactar con este, probará co seguinte (isto quere dicir que se obtemos como resposta do primeiro servidor que non existe o nome buscado, NON se lle vai a preguntar ao seguinte para ver se este o coñece).

Proba, nun equipo con Windows, a consultar a caché DNS local mediante o comando `ipconfig /displayDNS` e a baleirala mediante o comando `ipconfig /flushDNS`.

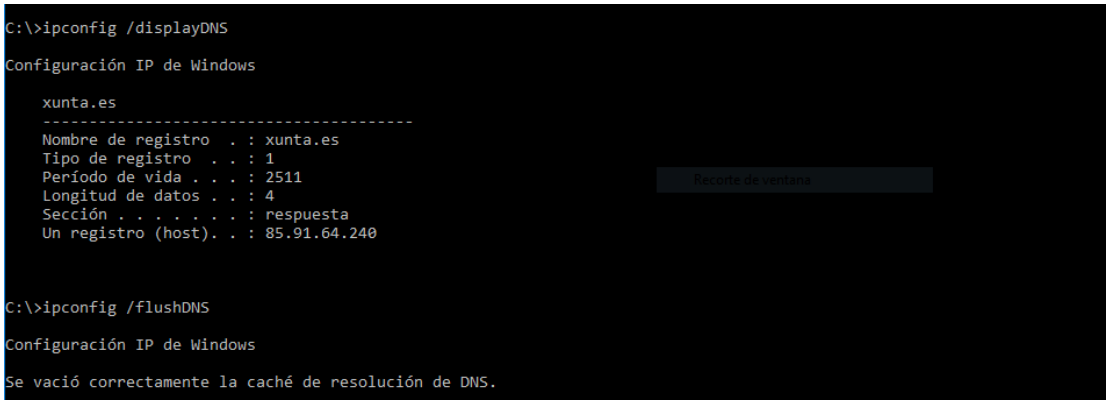

Figura 2 – Comandos de consulta e borrado de caché DNS en Windows.

1.2.4 Tipos de consulta

No sistema DNS existen diferentes tipos de consulta para cada situación. Son os seguintes:

- ***Consulta recursiva***: o equipo cliente solicítalle ao servidor DNS que lle responda coa solución para a consulta realizada ou cun erro que indique que o recurso solicitado non existe.

  Neste último caso, o servidor DNS non pode referir ao cliente a outro servidor DNS. Como consecuencia disto, o servidor DNS que recibe unha consulta recursiva pregunta a outros servidores ata que obtén a solución ou ata que obtén un erro porque o recurso solicitado non existe.

- ***Consulta iterativa***: o equipo que actúa como cliente permite que o servidor DNS lle responda coa mellor solución que poida dar baseada na súa caché ou na información das súas zonas.

  Se o servidor DNS consultado non ten unha coincidencia exacta para o nome de dominio solicitado, a mellor resposta que pode retornar ao cliente é unha referencia a un *servidor DNS autoritativo* para o nivel máis baixo do espazo de nomes do dominio (servidor raíz). O cliente, con esa referencia obtida, continúa o proceso ata que chega ao servidor DNS que é autoritativo para o nome consultado ou ata que obtén un erro.

  Este proceso iterativo recibe comunmente o nome de *"walking the tree"* e é o tipo de consulta que adoita iniciar un servidor DNS que intenta resolver unha consulta recursiva dun cliente.

1.2.5 Proceso típico de resolución

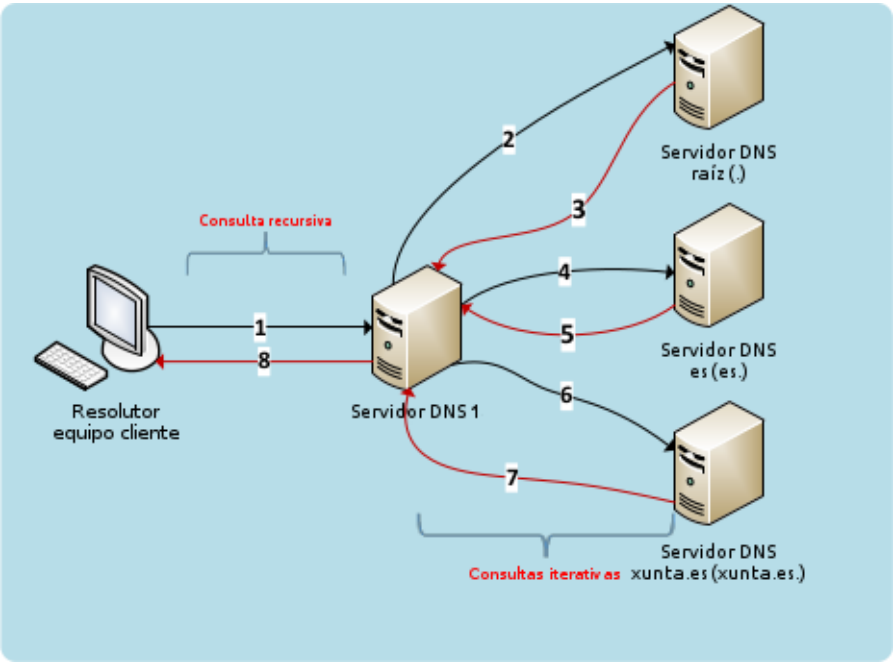

Figura 3 – Esquema de resolución dunha consulta DNS.

Imaxina que dende o teu ordenador na túa casa queres abrir no navegador o sitio http://edu.xunta.es. O proceso típico de resolución sería o seguinte:

- Ao escribir a URL no navegador iníciase un proceso, totalmente transparente para o usuario, coa fin de resolver o nome de dominio *edu.xunta.es*.
- Seguramente o navegador web empregado mantén unha caché propia coas últimas consultas feitas (hai que ter coidado con isto cando se están a facer probas). Se non atopa coincidencia na súa caché pásalle a consulta ao resolutor do sistema.
- O resolutor do sistema consulta se o nome solicitado é o propio da máquina onde se fai a consulta (neste caso non o é).
- O resolutor consulta o ficheiro hosts para ver se hai unha coincidencia.
- O resolutor consulta a caché do equipo (se ten tal caché).
- (1) No caso de que todo o anterior non arroxe ningún resultado, o resolutor contacta co primeiro servidor DNS que ten configurado (normalmente este foi proporcionado por un servidor DHCP, aínda que tamén pode configurarse de maneira estática) e realízalle unha consulta recursiva para o nome de dominio *edu.xunta.es*. Este servidor DNS, "Servidor DNS 1", debe retornar ou a resposta ou unha mensaxe de erro.

- (2) "Servidor DNS 1" comproba a súa caché (no caso de que a teña) e as zonas que ten configuradas (se ten algunha) para ver se pode responder a consulta. No caso de que non sexa capaz de responder por el mesmo, contactará cun servidor raíz e realizaralle unha consulta iterativa para o nome *edu.xunta.es*.
- (3) O servidor raíz non coñece a resposta para a consulta, polo que responde cunha referencia ao servidor autoritativo para ou dominio *.es*.
- (4) "Servidor DNS 1" contacta co servidor autoritativo para o dominio .es realizándolle unha consulta iterativa para *edu.xunta.es*.
- (5) O servidor autoritativo para o dominio .es non coñece a resposta completa, polo que responde cunha referencia ao servidor DNS autoritativo para *xunta.es*.
- (6) "Servidor DNS 1" contacta co servidor autoritativo para xunta.es realizándolle unha consulta iterativa para *edu.xunta.es*.
- (7) O servidor autoritativo para o dominio xunta.es coñece a resposta completa, polo que responde co IP correspondente ao nome *edu.xunta.es*.
- (8) "Servidor DNS 1" respóndelle ao cliente co IP para *edu.xunta.es*.

1.2.6 Tipos de servidores DNS

Existen diferentes tipos de servidores DNS dependendo do rol que vaian a realizar:

- **Recursive DNS Server**. É un tipo de servidor DNS empregado tipicamente para responder ás consultas recursivas realizadas polos equipos clientes. Está configurado para preguntar a outros servidores DNS ata que atopa a resposta para a consulta (proceso iterativo). Polo tanto contestaralle ao resolutor do cliente coa IP correspondente ou cunha mensaxe de erro.
- **Caching DNS Server**. É un servidor DNS recursivo que, para intentar evitar ter que comezar un proceso iterativo de consulta cada vez, o que fai é almacenar as respostas obtidas durante un período determinado de tempo.

  Por exemplo, se lle preguntamos a un servidor DNS caché por *www.xunta.es* e non ten a resposta almacenada na súa caché, comprobará se ten almacenado na caché o enderezo do servidor DNS para *xunta.es*. No caso de telo, preguntaralle a este servidor DNS por *www.xunta.es*. No caso de non ter na súa caché o enderezo dun servidor DNS de *xunta.es*, comprobará se ten o enderezo para un servidor DNS de .es. No caso de que si o teña, preguntaralle por un servidor de *xunta.es*. Se tampouco ten o enderezo dun servidor DNS para *.es*, comezaría o proceso iterativo "normal" preguntándolle a un servidor DNS raíz. A idea é reducir o número de consultas ao mínimo posible.
- **Forwarding DNS Server**. Este tipo de servidores están configurados para reenviar a consulta que non poden resolver a outro servidor DNS. No canto de comezar eles o proceso iterativo de resolución, realizan unha consulta recursiva a outro servidor DNS. Desta maneira o consumo de recursos é mínimo. Ademais este tipo de servidores tamén manteñen unha caché coas respostas obtidas para acelerar as respostas.
- **Authoritative-only DNS Server**. É un tipo de servidor DNS que só e capaz de responder as consultas iterativas para os rexistros das zonas para as cales el é o servidor responsable. No caso de consultarlle por un nome de dominio non incluído nos seus ficheiros de zona, respóndelle ao cliente dicíndolle que non coñece a resposta e, no mellor dos casos, proporciónalle unha referencia a un servidor que si pode resolvela.

É posible configurar un servidor DNS que combine as características de máis dun dos tipos explicados. Por exemplo, un servidor DNS pode configurarse para actuar como un servidor

recursivo con caché para clientes locais e para que actúe como un servidor que só responde a consultas iterativas para os dominios para os que é autoritativo para o resto de clientes.

De feito este tipo de configuración é moi típico xa que permite que os clientes locais empreguen o servidor para resolución recursiva e ademais permite dar resposta a peticións globais sobre o noso dominio.

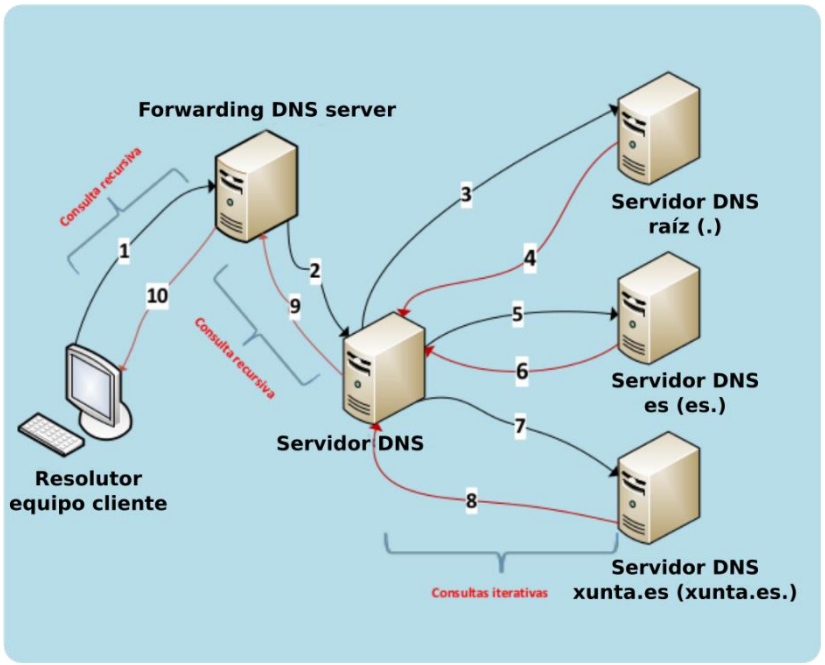

Figura 4 – Forwarding DNS server (servidor DNS de reenvío).

1.2.7 Tipos de zonas DNS

Os termos zona e dominio poden chegar a confundirse. Unha zona contén a información necesaria para resolver nomes pertencentes a un ou varios dominios. Unha zona non é máis que un arquivo que se almacena nun servidor DNS e que contén unha parte de toda a información do espazo de nomes DNS. Polo tanto é unha parte da base de datos distribuída correspondente ao espazo de nomes DNS.

Relacionado con isto, convén ter claros os seguintes conceptos:

- Unha zona almacénase nun servidor DNS e, nese caso, dise que o servidor ten autoridade sobre a zona ou que é un servidor autorizado da zona.
- Un servidor DNS pode ter autoridade sobre varias zonas.
- DNS permite que un espazo de nomes DNS se divida en zonas.
- Para cada nome de dominio DNS incluído nunha zona, a zona convértese na fonte autorizada de información acerca deste dominio.
- Os arquivos de zona mantéñense en servidores DNS.
- Un único servidor DNS pódese configurar para aloxar ningunha, unha ou varias zonas.
- Cada zona pode estar autorizada para un dominio DNS ou para máis dun (sempre que sexan contiguos na árbore DNS).
- Unha zona está constituída por varios rexistros. Cada rexistro serve para resolver un nome DNS ou, no seu caso, un enderezo IP. Tamén os rexistros teñen outras funcións como, por exemplo, indicar cales son os servidores DNS da zona ou os servidores de correo.

- Unha zona pode albergar os rexistros de recursos para un dominio ou os rexistros de recursos para varios dominios.
- Unha zona pode aloxar máis dun dominio só se os dominios son contiguos; é dicir, están conectados mediante unha relación directa.

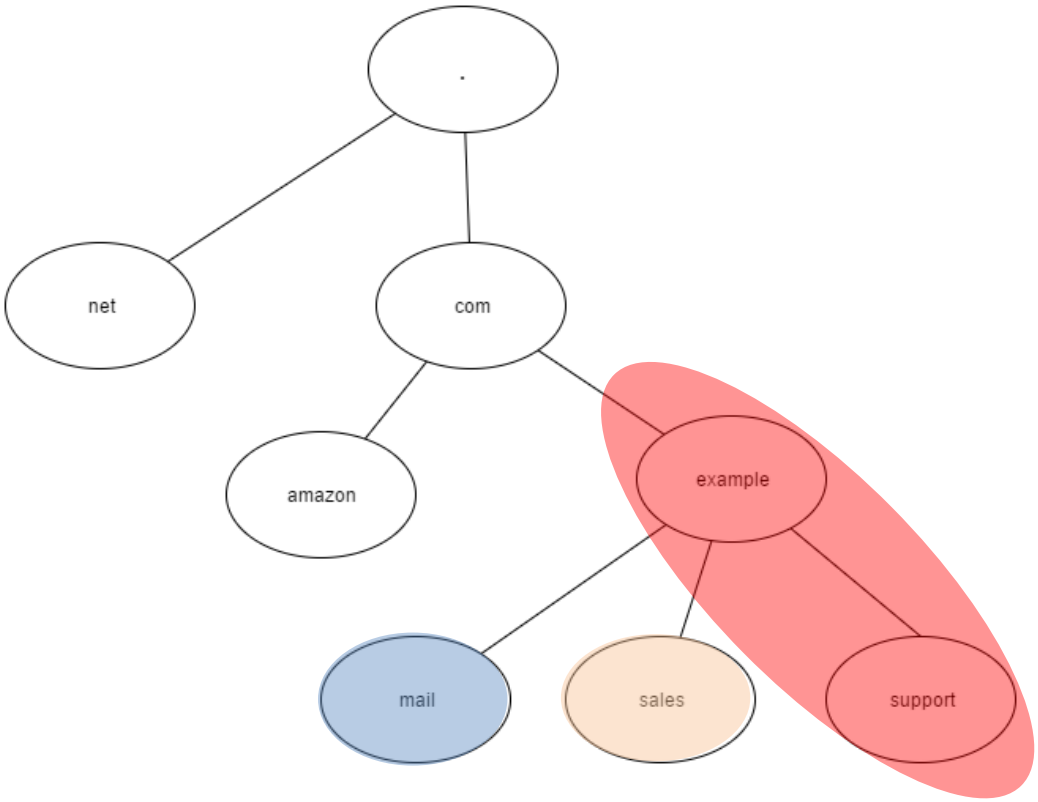

Figura 5 – Exemplo de distintas zonas dentro da árbore de nomes de dominio.

Na ilustración hai tres zonas representadas:

- example.com
- mail.example.com
- sales.example.com

A primeira zona (example.com) está autorizada para dous dominios contiguos (example.com e support.example.com), mentres que cada unha das outras dúas zonas (mail.example.com e sales.example.com) representan un único dominio.

Podemos distinguir zonas de dous tipos:

- Zona principal. Unha zona principal é onde se crean e administran rexistros de recursos.
- Zona secundaria. Unha zona secundaria é unha copia da zona principal de só lectura (por motivos de dispoñibilidade, seguridade, etc.). Os rexistros da zona secundaria non poden modificarse. Os administradores só poden modificar rexistros da zona DNS principal.

Unha vez que se decidiu se a zona é de tipo principal ou secundario, debe decidirse en que tipo de zona de procura se almacenan os rexistros de recursos. Podendo ser:

- Zona de procura directa. Almacena nomes de dominio e os IPs que lles corresponden.
- Zona de procura inversa. Almacena IPs e os nomes de dominio que lles corresponden.

Figura 6 – Exemplo de resolución directa e inversa do FQDN www.marca.com por medio da ferramenta nslookup.

1.2.8 Tipos de rexistros DNS

Un rexistro de recursos (RR) contén información para procesar consultas DNS.

Unha vez instalado o servizo *Servidor DNS* xa se poden engadir asignacións entre nomes de host e enderezos IP. Estas asignacións denomínanse rexistros de recursos en DNS e existen moitos tipos diferentes:

- A = Address (enderezo). Este rexistro úsase para traducir nomes de servidores de aloxamento a enderezos IPv4.
- AAAA = Address (enderezo) Este rexistro úsase en IPv6 para traducir nomes de hosts a enderezos IPv6.
- CNAME = Canonical NAME (nome canónico). Úsase para crear un alias, por exemplo, cando se están correndo múltiples servizos (como ftp e servidor web) nun servidor cun só enderezo IP. Cada servizo ten a súa propia entrada de DNS (como ftp.exemplo.com. e www.exemplo.com.). Isto tamén se emprega cando corres múltiples servidores HTTP, con diferente nomes, sobre o mesmo host.
- NS = Name Server (servidor de nomes). Define a asociación que existe entre un nome de dominio e os servidores de nomes que almacenan a información dese dominio.
- MX = Mail eXchange (rexistro de intercambio de correo). Asocia un nome de dominio a unha lista de servidores de intercambio de correo para ese dominio.
- PTR = Pointer (indicador). Tamén coñecido como 'rexistro inverso', funciona á inversa do rexistro A, traducindo IPs en nomes de dominio.
- SOA = Start Of Authority (autoridade da zona). Proporciona información sobre o servidor DNS primario da zona.
- TXT = Text (información textual). Permitelles aos dominios identificarse de modos arbitrarios.

📖 Listado completo de tipos de rexistros DNS: https://en.wikipedia.org/wiki/List_of_DNS_record_types