

Función

DNS, que sus siglas significan Domain Name System.

Por lo general solemos escribir en el navegador direcciones con el formato por ejemplo, **www.google.com.ar**, pero tenemos en claro que significa eso?, a que se refiere esa dirección?, si a las páginas web se llega mediante una dirección IP porque es la forma de identificar una máquina en una red, de eso se trata, esos son los DNS, es una tecnología basada en una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio, sirve para resolver nombres en las redes, es decir, conocer la IP de la máquina donde está alojado el dominio al que queremos acceder.

Ahora bien, ¿para que querría utilizar este mecanismo?.

En una red pequeña, sería sencillo conocer la dirección IP de cada una de las máquinas a las que queremos acceder, pero en el caso que estemos queriendo acceder a una IP entre miles y miles como son las diferentes páginas web, gmail, google, facebook, etc etc etc, sería casi imposible recordar cada una de ellas, cada vez que estemos queriendo acceder, para ello se les asigna una dirección fácil de recordar.

Por lo tanto, la función más importante es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

Los usuarios, por lo general no se comunican directamente con un servidor DNS, esto se hace de forma transparente a través de navegadores, clientes de correo, etc. Cuando se realiza una petición, ésta se envía al servidor DNS local del sistema operativo, comprobando si la respuesta se encuentra en memoria caché, si no es así, se enviará a uno o más servidores DNS en busca de una.

Por lo general la mayoría de usuarios domésticos utilizan como servidor DNS el proporcionado por el proveedor de servicios de Internet. La dirección de estos servidores puede ser configurada de forma manual o automática mediante DHCP. En otros casos, los administradores de red tienen configurados sus propios servidores DNS

Historia

Haciendo un poco de historia....

En primer instancia, SRI alojaba un archivo llamado Hosts, este mismo, contenía todos los nombres de dominio conocidos. La red tuvo un crecimiento tan grande que esta metodología dejó de ser práctica.

En 1983 Paul Mockapetris publicó RFCs 882 y 883 que posteriormente a partir de 1987 quedaron obsoletos y fueron reemplazados por los 1034 y 1035.

Los RFC (Request for comments) son una serie de publicaciones que describen diversos aspectos del funcionamiento de internet y otras redes de computadoras. Cada RFC constituye un monográfico o memorando que ingenieros o expertos en la materia han hecho llegar al IETF (Internet Engineering Task Force). Cada uno tiene un número y un título asignado para que no pueda repetirse. Antes de que un documento tenga la consideración de RFC, debe seguir un proceso muy estricto para asegurar su calidad y coherencia.

Se necesita de tres partes para poder traducir los nombres en la red, Cliente DNS, Servidor DNS y Zonas de autoridad.

TCP/IP Host table

En unix se encuentra en `/etc/hosts`

En windows (a partir de 2003) se encuentra en `C:\Windows\System32\drivers\etc\hosts`

Es un fichero almacenado en el directorio `/etc/hosts/` en el servidor Unix o en un directorio relevante de nuestro sistemas operativos. La host table lista línea a línea los nombres de los host de Internet y sus direcciones IP asociadas. La host table maestra está compilada y almacenada en las máquinas del Network

Information Center (NIC)—nic.ddn.mil en /netinfo/hosts.txt y un vistazo a su tamaño (medio megabyte) nos puede decir el porqué no nos gustaría encargarnos de su mantenimiento. Tal y como crece Internet, los nombres de dominio son actualizados y añadidos cada hora (al menos), y no es práctico para cada servidor de Internet almacenarlo para sus usuarios.

Espacio de nombres de dominio

El espacio de nombres de dominio DNS, se basa en el concepto de un árbol de dominios con nombre. Cada nivel del árbol puede representar una rama o una hoja del mismo. Una rama es un nivel donde se utiliza más de un nombre para identificar un grupo de recursos con nombre. Una hoja representa un nombre único que se utiliza una vez en ese nivel para indicar un recurso específico

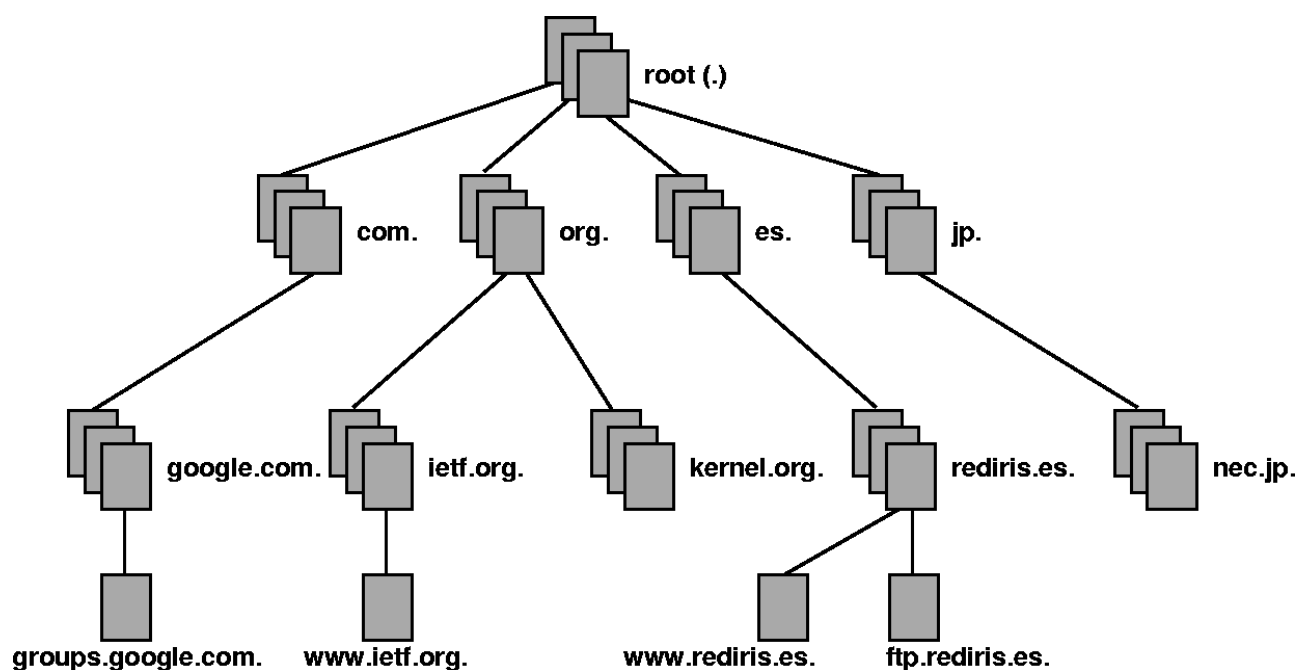
En que influye la jerarquía de DNS en la resolución del dominio...

Tiene una jerarquía arborescente, el nombre del dominio consisten en la concatenación de todas las etiquetas del camino.

Las etiquetas son cadenas alfanuméricas (con '-' como único símbolo permitido), deben contar con al menos un carácter y un máximo de 63 caracteres de longitud, y deberá comenzar con una letra (y no con '-'), ver RFC 1035.

Un nombre de dominio se escribe siempre de derecha a izquierda. El punto en el extremo derecho de un nombre de dominio separa la etiqueta de la raíz de la jerarquía.

Este primer nivel es también conocido como dominio de nivel superior (TLD - Top Level Domain).



Dominio de primer nivel o tld “Top Level Domain”

El primer nivel es el que está a la derecha del nombre del dominio y se utiliza para indicar un país, una región o el tipo de organización que usa un nombre. es decir, .com, .net etc... por ejemplo, en el dominio **www.yahoo.com**, el primer nivel es .com

Los que siguen son los dominios de primer nivel que veremos con frecuencia:

Dominio	Descripción
edu	Instituciones universitarias
com	Organizaciones comerciales.
org	Organizaciones no comerciales.
	Pasarelas y otras redes administrativas.

net	
mil	El ejército.
gov	El gobierno.

Este primer nivel está controlado por organizaciones distintas dependiendo del tipo de dominios, por ejemplo, los famosos .com y .net los controla Verisign, los regionales una organización de cada país. Cada país suele tener su propio dominio de primer nivel codificado con las dos letras del país definidas en la tabla ISO-3166. Por ejemplo, en España se usa el dominio es; en México se usa mx; en Argentina, ar, etc. Por debajo de cada dominio de primer nivel, cada país organiza los dominios a su manera. Algunos crean a segundo nivel una serie de dominios. Por ejemplo, en Argentina encontramos los dominios com.ar para las empresas, y org.ar para las organizaciones sin ánimo de lucro. Otros países, como España, ponen directamente como nombres de segundo nivel las instituciones o empresas que los solicitan. Por ejemplo, tenemos hispalinux.es.

Por supuesto, el hecho de que un nombre esté en uno de estos dominios nacionales, no implica que la máquina esté realmente en ese país; significa simplemente que ha sido registrada en el NIC de ese país. Un fabricante sueco puede tener oficinas en Australia y tener sus ordenadores de allá registrados en el dominio se.

Dominios de segundo nivel

Nombres registrados que un individuo u organización utiliza en Internet. La entidad o empresa que controla un dominio de primer nivel, es la que a su vez delega los nombres de segundo nivel, por ejemplo, el segundo nivel de yahoo.com, sería yahoo, que estaría delegado por Verisign, que es la organización que controla los dominios de primer nivel .com y .net.

En la página iana.org/domains/root/db se puede ver una lista de las organizaciones que controlan los dominios genéricos de primer nivel.

Para usar un nombre de dominio de segundo nivel, por ejemplo "minombre.com ó minombre.es", es necesario pagar un mantenimiento a la organización que controla este TLD, o en ocasiones (como sucede con los nombres genéricos), hay uno o más vendedores autorizados llamados "registradores". La lista de registradores autorizados para dominios genéricos puede encontrarse en la página del ICANN.

Dominios de tercer nivel o subdominios

El tercer nivel, también conocido como subdominios, están a la izquierda del segundo, por ejemplo, en “shop.yahoo.com” “shop” sería un subdominio y en “www.yahoo.com” “www” sería un subdominio.

Cuando pagamos por un dominio y se nos cede su gestión administrativa y técnica (delegación), debemos facilitar al registrador o entidad que controla el TLD de nuestro dominio, al menos dos servidores DNS, que serán “autoritativos” para el dominio que hemos comprado (normalmente se encarga de esto nuestro proveedor de Internet), estos servidores deben estar configurados correctamente para utilizar los distintos servicios de nuestro dominio en Internet (páginas web, email, etc.), apuntando el nombre o nombres a las direcciones IP correspondientes.

Entre las cosas que podemos controlar desde el servidor DNS de nuestro dominio de segundo nivel, están los posteriores niveles o subdominios, por ejemplo, el conocido www, no es más que un subdominio o dominio de tercer nivel, que puede configurarse desde nuestro servidor de nombres (DNS).

Por ejemplo, en el caso del dominio intervia.com, existe además un dominio de tercer nivel www.intervia.com, que en este caso apunta a la misma dirección IP que el dominio principal, aunque esto no tendría por qué ser así, por ejemplo, hay muchos dominios que tienen configurado www.midominio.com como dominio principal para las páginas web, pero no han configurado el nombre principal del dominio, por lo que cuando tratamos de cargar midominio.com (sin www), obtenemos un error. Esto se debe a que el nombre principal no se configuró en el servidor DNS del dominio.

En el caso de algunos dominios regionales la entidad encargada del registro además de controlar el segundo nivel, controla también el tercer nivel de algunos nombres para obtener más combinaciones, por ejemplo, los dominios del Reino Unido para uso comercial son .co.uk, aunque también existen .net.uk, .org.uk y .me.uk (entre otros), esto mismo ocurre con los dominios de Japón, Portugal, Argentina, Brasil y España, entre otros. En ese caso, lo que controlaríamos desde nuestro servidor de nombres sería el cuarto y posteriores niveles.

Una vez que disponemos de un dominio registrado, podemos delegar los siguientes niveles para que sean controlados por otros servidores de nombre, por ejemplo, nosotros podríamos delegarlo que sea intervia.com, apuntándolo a otro servidor DNS, que a su vez podría hacer lo mismo, es decir, es todo una cadena de delegaciones, donde el nivel anterior controla a los siguientes, y por tanto, en último término es el ICANN quien controla todos los nombres de Internet, ya que controla la zona root, que es el nivel de base.

Zona root alternativa

Dado que quien controla la zona root controla todos los nombres de Internet, es decir, el ICANN, **¿qué pasaría si hubiera una zona root alternativa?...**

De hecho esto ya ocurrió, una empresa llamada **new.net** montó su propia zona root alternativa, creando infinidad de nuevos TLDs como .agente, .amor, .arte, .book, .chat, .club, .deporte, .xxx y así hasta casi cien nuevos TLDs.

El problema es que **su zona no está soportada por ningún buscador**, por lo que si buscamos en Google, nunca encontraríamos este tipo de dominios y al no estar en los servidores de raíz. Estos dominios no eran accesibles a no ser que se modifica la configuración del sistema operativo. Tal vez debido a esto, hace ya tiempo de new.net no funciona.

Subdirectorios

Por último, no hay que confundir **los subdirectorios del disco duro** del servidor con los nombres de dominio. Se diferencian porque siempre **empiezan por una barra “/” y están a la derecha del nombre de dominio**. Por ejemplo, en www.yahoo.com/news/ el nombre de dominio sería “www.yahoo.com” y /news/, es un subdirectorio o carpeta dentro de ese servidor (*igual que las carpetas de nuestro disco duro*).

Sintaxis de los nombre de los dominios

Los únicos caracteres operativos permitidos para un nombre de dominio son:

- o Los pertenecientes al alfabeto inglés: de la 'a' a la 'z'.
- o Los dígitos del 0 al 9. (No es aconsejable un nombre con sólo dígitos)
- o El guión: - (no puede ser ni el primero ni el último carácter del nombre)

No hay distinción entre minúsculas y mayúsculas.

Ø Las longitudes máximas y mínimas de un nombre de dominio son:

- o Para los .com,.org,.net, hay un máx. de 64 y un mínimo de 2.
- o Para el .es: como máximo 63 y como mínimo 3.

Ø No se podrán registrar ninguno de los siguientes nombres: edu, com, gov, mil, org, int, net, arpa, firm, store, web, arts, rec, info, o nom.

Ø No se podrá registrar ningún nombre que coincida con: protocolos, aplicaciones o terminología de Internet (por ejemplo: telnet, ftp, email, www, web, smtp, http, tcp, dns, wais, news, rfc, ietf, mbone, bbs).

Mecanismos de resolución de direcciones

La claridad conceptual sobre resolución de nombres iterativa y resolución de nombres recursiva. En la primera, el servidor encargado de hacer la resolución realiza iterativamente preguntas de tipo NS a los diferentes DNS de la jerarquía asociada al nombre que se desea resolver, hasta descender en ella hasta la maquina que contiene la zona autoritativa para el nombre que se desea resolver. En la resolución recursiva, la maquina que desea resolver un nombre hace una pregunta directa a un servidor DNS no necesariamente autoritativo, y este se encarga de gestionar ya sea iterativamente o recursivamente la resolución de esta pregunta. Normalmente la librería de resolución, embebida en el sistema operativo, solicita resolución recursiva y los servidores DNS realizan resolución iterativa.

ejemplo.com.

La primer búsqueda será solicitando IP al ., esto significa que al root (.), le preguntará cual es la IP del servidor ejemplo.com, a su vez este servidor consultará a la siguiente rama del árbol, en este caso sería a com. si conoce la IP de la etiqueta ejemplo. Y así recursivamente hasta llegar al servidor que sea capaz de responder la IP del dominio o agotar las etiquetas y no haber obtenido respuesta.

Consultas DNS

Antes que nada presentemos a nslookup y dig y que cosas podremos preguntarles:

Como primera función básica Nslookup y Dig serán capaces de mediante una IP o un dominio como argumento decirnos cuál es la dirección legible para el usuario o viceversa, así como también podremos conseguir la dirección IP o nombre completo del servidor de mail.

Tipos de consultas en los servidores DNS

A (Address): Se utiliza para traducir nombres de hosts del dominio a direcciones IP, es el valor predeterminado.

ANY (Cualquiera): Toda la información que exista.

CNAME (Canonical Name): Devuelve una lista de alias, si existen para el nombre verdadero (canonical).

NS (Name Server): Especifica el nombre para un dominio.

MX (Mail Exchange): Especifica el servidor encargado de recibir el correo electrónico para el dominio.

PTR (Pointer): Lo inverso del registro A, realiza la traducción de direcciones IP a nombres de host.

TXT (Text): Permite extraer información adicional a un dominio.

Reverse lookup

Es la función que mediante una IP es capaz de resolver cuál es el dominio utilizado para esa dirección.

La consulta con los diferentes programas sería:

dig 173.194.42.127 PTR

en nslookup seria:

```
set type=PTR
173.194.42.127
```

Client lookup

en dig
dig google.com.ar NS

en nslookup

```
set type=NS
google.com.ar
```

nslookup

Mas Ejemplos:

```
nslookup [-option ...] [host-to-find | -[server]]
```

```
nslookup google.es
```

La respuesta será:

```
nslookup google.com.ar
```

```
Server:      127.0.1.1
Address:     127.0.1.1#53
```

Non-authoritative answer:

```
Name: google.com.ar
Address: 173.194.42.88
Name: google.com.ar
Address: 173.194.42.87
Name: google.com.ar
Address: 173.194.42.79
Name: google.com.ar
Address: 173.194.42.95
```

Lo que se hizo con este comando es preguntarle al servidor DNS configurado en nuestra maquina, en este caso 127.0.0.1 y le preguntamos cuales son las IP publicas del dominio google.com.ar

También es posible utilizar otro Servidor DNS, para ello simplemente especificamos el servidor que utilizaremos en el comando (en este caso uno de lo servidores DNS publicos de google).

```
nslookup google.com.ar 8.8.8.8
```

```
Server:      8.8.8.8
Address:     8.8.8.8#53
```

Non-authoritative answer:

```
Name: google.com.ar
Address: 173.194.42.120
Name: google.com.ar
Address: 173.194.42.127
Name: google.com.ar
Address: 173.194.42.119
Name: google.com.ar
Address: 173.194.42.111
```

Para utilizar el modo interactivo solo basta con ejecutar el comando nslookup sin argumentos, ingresamos en la consola interactiva del comando.

Otro ejemplo podría ser el de pedir información acerca de los servidores de email de un dominio, para esto tenemos la opción "q=mx" o "type=mx" que se fija con el comando "set", entonces podemos hacer algo como esto:


```
set type=mx
> google.com.ar
Server:      127.0.1.1
Address:     127.0.1.1#53
```

Non-authoritative answer:

```
google.com.ar mail exchanger = 30 alt2.aspmx.l.google.com.
google.com.ar mail exchanger = 50 alt4.aspmx.l.google.com.
google.com.ar mail exchanger = 20 alt1.aspmx.l.google.com.
google.com.ar mail exchanger = 10 aspmx.l.google.com.
google.com.ar mail exchanger = 40 alt3.aspmx.l.google.com.
```

Authoritative answers can be found from:

```
google.com.ar nameserver = ns3.google.com.
google.com.ar nameserver = ns4.google.com.
google.com.ar nameserver = ns1.google.com.
google.com.ar nameserver = ns2.google.com.
aspmx.l.google.com internet address = 64.233.186.26
aspmx.l.google.com has AAAA address 2800:3f0:4003:c00::1a
alt1.aspmx.l.google.com internet address = 74.125.133.26
alt1.aspmx.l.google.com has AAAA address 2a00:1450:400c:c04::1b
alt2.aspmx.l.google.com internet address = 74.125.136.27
alt2.aspmx.l.google.com has AAAA address 2a00:1450:4013:c01::1a
alt3.aspmx.l.google.com internet address = 74.125.205.27
alt4.aspmx.l.google.com internet address = 74.125.200.27
ns1.google.com internet address = 216.239.32.10
ns2.google.com internet address = 216.239.34.10
ns3.google.com internet address = 216.239.36.10
ns4.google.com internet address = 216.239.38.10
```

Otras veces tenemos la necesidad de saber a que dominio pertenece cierta IP pública, simplemente con poner la IP el servidor DNS nos hace un DNS inverso:

```
set type=ptr
> 8.8.8.8
Server:      127.0.1.1
Address:     127.0.1.1#53
```

Non-authoritative answer:

```
8.8.8.8.in-addr.arpa name = google-public-dns-a.google.com.
```

Authoritative answers can be found from:

```
8.in-addr.arpa nameserver = ns2.level3.net.
8.in-addr.arpa nameserver = ns1.level3.net.
ns1.level3.net internet address = 209.244.0.1
ns2.level3.net internet address = 209.244.0.2
```

Dig

Dig Permite hacer consultas a los servidores DNS, para comprobar si el DNS está correctamente configurado en nuestra máquina. Permite consultar el mapeo de nombres a IPs y de IPs a nombres.

- dig dominio.com NS : sirve para preguntar cuál es el servidor DNS de un dominio.
- dig dominio.com MX : sirve para preguntar cuál es el servidor de correo de un dominio.
- dig www.dominio.com : sirve para preguntar cuál es el equipo www de un dominio.

Host

host Sirve para encontrar la dirección IP del dominio dado y también muestra el nombre de dominio para la IP dada.

- -a : muestra todos los registros DNS para el hostname dado.
- -C : muestra los registros SOA y los servidores de nombres autorizados.
- -l : lista todos los hosts en un dominio usando AXFR.
- -t : se utiliza para seleccionar el tipo de query. Tipo de Query: CNAME, NS, SOA, KEY, etc.
- -W : especifica cuánto tiempo se debe esperar para obtener una respuesta.
- -v : el host genera la salida verbose.
- -d : equivalente a -v.
- -T : utiliza TCP en vez de UDP para queries al servidor de nombres

El formato de un mensaje DNS .

16 bit 16 bit

Identificación

Parámetros

Número de Solicitud

Número de respuesta

Número de autoridad

Numero adicional

Número de autoridad Numero adicional

Sección Solicitud

Sección respuesta

Sección autoridad

Sección de información adicional

Identificación: Identifica al mensaje, se emplea para llevar la correspondencia entre solicitudes y respuestas. -
Parámetros:

- * bit 1: Valor 0 = solicitud, valor 1 = respuesta.
- * bit 1 a 4: Tipo de consulta: Valor 0 = estándar, valor 1 = Inversa (existen valor 3 y 4 en desuso).
- * bit 5: Seteado si la solicitud es autoritativa.
- * bit 6: Seteado

si el mensaje es truncado.

- * bit 7: Seteado si se requiere recursión.
- * bit 8: Seteado si la recursión está disponible.
- * bit 9 a 11: Reservados.
- * bit 12 a 15: (Tipo de respuesta)
 - valor 0 = sin error
 - valor 1= Error de formato en solicitud,
 - valor 2 = falla en servidor,
 - valor 3 = nombre inexistente.

- Numero de...: Lleva la cuenta del número de mensajes que se cursan en las secciones que le siguen en el formato.
- Sección solicitud: contiene las consultas deseadas, consta de tres sub-campos: Nombre de Dominio (longitud variable), Tipo de consulta (Host, mail, etc) y Clase de consulta (permite definir otros objetos no estándar en Internet).
- Sección respuesta, autoridad e información adicional: consisten en un conjunto de registros que describen nombres y sus mapeos correspondientes.

DNS, Registros

Los archivos del DNS

Un archivo de base de datos del servidor de nombres, (archivo DNS), es un archivo de zona. Contiene los registros de los dominios de la que es autoridad esa zona. Es decir es el archivo en el cual se encuentran los datos que resuelven las peticiones de nombres asociadas en direcciones IP. Se compone de una serie de registros que se verán a continuación.

Registro SOA

Se forma con una serie de parámetros a tener en cuenta (se explicarán más adelante en detalle)

Host Origen: Host donde se mantiene el archivo.

Correo electrónico: Del responsable de la BD. La arroba (@) se sustituye por un punto (.), debido a que @ representa el dominio raíz de la zona.

Número de serie: La versión de ese archivo. Aumenta cada vez que el archivo cambia.

Tiempo de actualización: Tiempo que espera un servidor de nombres secundario para ver si el archivo ha cambiado, y por lo tanto pedir una transferencia de zona.

Tiempo de reintento: Tiempo que espera un servidor de nombres secundario para iniciar una nueva transferencia de zona en el caso de que falle este procedimiento.

Tiempo de caducidad: Tiempo que el servidor de nombres secundario intentará descargar una zona. Cuando pase, se rechaza la información antigua.

Tiempo de vida (Time to live): Tiempo en el que el servidor de nombres mantiene la caché cualquier registro del recurso de este archivo en base de datos.

Registro NS

El Registro NS. (siglas de Name Server), contiene los servidores de nombre de ese dominio, lo que permite que otros servidores de nombres vean los nombres de su dominio.

Registro MX

El registro MX es el registro de Intercambio de correo (Mail eXchange). Indica que host se encarga del procesamiento del correo electrónico de ese dominio.

Registro A

Los registros de dirección A, (Address) asocian nombres de host a direcciones IP dentro de una zona. Son los más numerosos dentro del archivo.

Registro CNAME

Estos registros son llamados también alias, si bien son conocidos como entradas de nombre canónico (CNAME, Canonical Name). Su uso más común es utilizar para apuntar a un único host más de un nombre, así se simplifican procesos como albergar simultáneamente un servidor web y otro FTP en un mismo equipo.

Dominios Registración

¿Quien provee un dominio?

Para registrar un dominio, en argentina disponemos del servicio público del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto (MRECIC), nic.ar, aquí podemos consultar disponibilidad o incluso dar de alta un nuevo dominio terminados en .ar.

Consultar disponibilidad de dominio:

<https://nic.ar/buscarDominio.xhtml> ingresar el dominio que se desea consultar.

Para registrar un dominio es necesario tener un usuario registro en nic.ar, consultar disponibilidad y ahí tendremos la opción de solicitarlo. Claro que en Argentina antes era gratuito y hoy tiene un costo de \$160 por año.

Para más información sobre registros de dominios:

<https://nic.ar/tutoriales.xhtml>

RFCS utilizados en Protocolos DNS

- RFC 952 DOD INTERNET HOST TABLE SPECIFICATION
- RFC 1032 DOMAIN ADMINISTRATORS GUIDE
- RFC 1033 DOMAIN ADMINISTRATORS OPERATIONS GUIDE
- RFC 1034 DOMAIN NAMES – CONCEPTS AND FACILITIES
- RFC 1035 DOMAIN NAMES – IMPLEMENTATION AND SPECIFICATION
- RFC 1101 DNS Encoding of Network Names and Other Types
- RFC 1122 Requirements for Internet Hosts — Communication Layers
- RFC 1123 Requirements for Internet Hosts — Application and Support
- RFC 1183 New DNS RR Definitions
- RFC 1348 DNS NSAP RRs
- RFC 1535 A Security Problem and Proposed Correction With Widely Deployed DNS Software
- RFC 1536 Common DNS Implementation Errors and Suggested Fixes
- RFC 1537 Common DNS Data File Configuration Errors
- RFC 1591 Domain Name System Structure and Delegation (Informational)
- RFC 1611 DNS Server MIB Extensions
- RFC 1612 DNS Resolver MIB Extensions
- RFC 1706 DNS NSAP Resource Records
- RFC 1712 DNS Encoding of Geographical Location
- RFC 1750 Randomness Recommendations for Security
- RFC 1876 A Means for Expressing Location Information in the Domain Name System
- RFC 1886 DNS Extensions to support IP version 6

- RFC 1982 Serial Number Arithmetic
- RFC 1995 Incremental Zone Transfer in DNS
- RFC 1996 A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
- RFC 2052 A DNS RR for specifying the location of services (DNS SRV)
- RFC 2104 HMAC: Keyed-Hashing for Message Authentication
- RFC 2119 Key words for use in RFCs to Indicate Requirement Levels
- RFC 2133 Basic Socket Interface Extensions for IPv6
- RFC 2136 Dynamic Updates in the Domain Name System (DNS UPDATE)
- RFC 2137 Secure Domain Name System Dynamic Update
- RFC 2163 Using the Internet DNS to Distribute MIXER Conformant Global Address Mapping (MCGAM)
- RFC 2168 Resolution of Uniform Resource Identifiers using the Domain Name System
- RFC 2181 Clarifications to the DNS Specification
- RFC 2230 Key Exchange Delegation Record for the DNS
- RFC 2308 Negative Caching of DNS Queries (DNS NCACHE)
- RFC 2317 Classless IN-ADDR.ARPA delegation
- RFC 2373 IP Version 6 Addressing Architecture
- RFC 2374 An IPv6 Aggregatable Global Unicast Address Format
- RFC 2535 Domain Name System Security Extensions
- RFC 2536 DSA KEYs and SIGs in the Domain Name System (DNS)
- RFC 2537 RSA/MD5 KEYs and SIGs in the Domain Name System (DNS)
- RFC 2538 Storing Certificates in the Domain Name System (DNS)
- RFC 2539 Storage of Diffie-Hellman Keys in the Domain Name System (DNS)
- RFC 2540 Detached Domain Name System (DNS) Information
- RFC 2541 DNS Security Operational Considerations
- RFC 2553 Basic Socket Interface Extensions for IPv6
- RFC 2671 Extension Mechanisms for DNS (EDNS0)
- RFC 2672 Non-Terminal DNS Name Redirection
- RFC 2673 Binary Labels in the Domain Name System
- RFC 2782 A DNS RR for specifying the location of services (DNS SRV)
- RFC 2825 A Tangled Web: Issues of I18N, Domain Names, and the Other Internet protocols
- RFC 2826 IAB Technical Comment on the Unique DNS Root
- RFC 2845 Secret Key Transaction Authentication for DNS (TSIG)
- RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering
- RFC 2915 The Naming Authority Pointer (NAPTR) DNS Resource Record
- RFC 2929 Domain Name System (DNS) IANA Considerations
- RFC 2930 Secret Key Establishment for DNS (TKEY RR)
- RFC 2931 DNS Request and Transaction Signatures (SIG(0)s)
- RFC 3007 Secure Domain Name System (DNS) Dynamic Update

- RFC 3008 Domain Name System Security (DNSSEC) Signing Authority
- RFC 3071 Reflections on the DNS, RFC 1591, and Categories of Domains
- RFC 3090 DNS Security Extension Clarification on Zone Status
- RFC 3110 RSA/SHA-1 SIGs and RSA KEYS in the Domain Name System (DNS)
- RFC 3123 A DNS RR Type for Lists of Address Prefixes (APL RR)
- RFC 3152 Delegation of IP6.ARPA
- RFC 3197 Applicability Statement for DNS MIB Extensions
- RFC 3225 Indicating Resolver Support of DNSSEC
- RFC 3226 DNSSEC and IPv6 A6 aware server/resolver message size requirements
- RFC 3258 Distributing Authoritative Name Servers via Shared Unicast Addresses
- RFC 3363 Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)
- RFC 3364 Tradeoffs in Domain Name System (DNS) Support for Internet Protocol version 6 (IPv6)
- RFC 3425 Obsoleting IQUERY
- RFC 3445 Limiting the Scope of the KEY Resource Record (RR)
- RFC 3467 Role of the Domain Name System (DNS)
- RFC 3490 Internationalizing Domain Names In Applications (IDNA)
- RFC 3491 Nameprep: A Stringprep Profile for Internationalized Domain Names (IDN)
- RFC 3492 Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)
- RFC 3493 Basic Socket Interface Extensions for IPv6
- RFC 3513 Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3596 DNS Extensions to Support IP Version
- RFC 3597 Handling of Unknown DNS Resource Record (RR) Types
- RFC 3645 Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)
- RFC 3655 Redefinition of DNS Authenticated Data (AD) bit
- RFC 3658 Delegation Signer (DS) Resource Record (RR)
- RFC 3757 Domain Name System KEY (DNSKEY) Resource Record (RR) Secure Entry Point (SEP) Flag
- RFC 3833 Threat Analysis of the Domain Name System (DNS)
- RFC 3845 DNS Security (DNSSEC) NextSECure (NSEC) RDATA Format
- RFC 3901 DNS IPv6 Transport Operational Guidelines
- RFC 4025 A Method for Storing IPsec Keying Material in DNS
- RFC 4033 DNS Security Introduction and Requirements
- RFC 4034 Resource Records for the DNS Security Extensions
- RFC 4035 Protocol Modifications for the DNS Security Extensions
- RFC 4074 Common Misbehavior Against DNS Queries for IPv6 Addresses
- RFC 4159 Deprecation of "ip6.int"

- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4255 Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints
- RFC 4343 Domain Name System (DNS) Case Insensitivity Clarification
- RFC 4367 What's in a Name: False Assumptions about DNS Names
- RFC 4398 Storing Certificates in the Domain Name System (DNS)
- RFC 4408 The DNSSEC Lookaside Validation (DLV) DNS Resource Record
- RFC 4431 Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1
- RFC 4470 Minimally Covering NSEC Records and DNSSEC On-line Signing
- RFC 4634 US Secure Hash Algorithms (SHA and HMAC-SHA)
- RFC 4641 DNSSEC Operational Practices

Más sobre tipos de registros DNS

Tipo A – Retorna una dirección IPv4 de 32-bit, más comúnmente utilizado para ubicar nombres de host para una dirección IP de una máquina.

Tipo AAAA - Retorna una dirección IPv6 de 128-bits, más comúnmente utilizado para ubicar nombres de host para una dirección IP de una máquina.

Tipo NS – Delega una zona DNS para utilizar los servidores autoritativos de nombres. es decir, *a quién tengo que preguntar para saber acerca de los registros de dominio.com.*

Tipo MX - Asigna un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio. ejemplo: *toharia.com MX 1 aspmx.l.google.com, toharia.com MX 5 alt1.aspmx.l.google.com.*

En la práctica, cuando un servidor SMTP (es decir, que envía correo) tiene que enviar un correo a *diego@toaria.com*, inspecciona los registros MX para *toharia.com*, y envía el correo al de mayor prioridad que encuentre disponible (en este caso, empezaría por *alt1.aspmx.l.google.com*, y luego seguiría con el resto).

Tipo CNAME - (Nombre Canónico) Se usa para crear nombres de hosts adicionales, o alias, para los hosts de un dominio. Es usado cuando se están corriendo múltiples servicios (como ftp y servidor web) en un servidor con una sola dirección ip. Cada servicio tiene su propia entrada de DNS (como *ftp.string.com.* y *www.string.com.*). esto también es usado cuando se ejecutan múltiples servidores http, con diferentes nombres, sobre el mismo host.

Tipo SOA - (Autoridad de la zona) Proporciona información sobre el servidor DNS primario de la zona, como el correo electrónico del administrador del dominio, el número serial del dominio, y los tiempos de refrescado o actualización. Se forma con una serie de parámetros a tener en cuenta

- **Host Origen:** Host donde se mantiene el archivo.
- **Correo electrónico:** Del responsable de la BD. La arroba (@) se sustituye por un punto (.), debido a que @ representa el dominio raíz de la zona.
- **Número de serie:** La versión de ese archivo. Aumenta cada vez que el archivo cambia.
- **Tiempo de actualización:** Tiempo que espera un servidor de nombres secundario para ver si el archivo ha cambiado, y por lo tanto pedir una **transferencia de zona**.
- **Tiempo de reintento:** Tiempo que espera un servidor de nombres secundario para iniciar una nueva transferencia de zona en el caso de que falle este procedimiento.
- **Tiempo de caducidad:** Tiempo que el servidor de nombres secundario intentará descargar una zona. Cuando pase, se rechaza la información antigua.
- **Tiempo de vida:** Tiempo en el que el servidor de nombres mantiene la caché cualquier registro del recurso de este archivo en base de datos.

Tipo PTR - También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo direcciones IP's en nombres de dominio.

Tipo SRV - Permite indicar los servicios que ofrece el dominio.

Tipo SPF - Sender Policy Framework - Ayuda a combatir el Spam. En este registro se especifica cual o cuales hosts están autorizados a enviar correo desde el dominio dado. El servidor que recibe, consulta el SPF para comparar la IP desde la cual le llega, con los datos de este registro. Normalmente, los spammers envían correo electrónico desde direcciones recopiladas en internet (y a direcciones recopiladas en internet), para que sea más difícil identificar el correo como *spam*. Sin embargo, si el filtro *antispam* está bien implementado, mirará el registro SPF del dominio del remitente de un correo entrante, y si la dirección IP origen del correo no está entre las admitidas en dicho registro, lo marcará como *spam*.

Registro SOA , mas detalles ;

Nombre

Define el nombre principal de la zona. El @ es una abreviatura a la zona actual, es decir, para */pri.elbauldelprogramador.com* en este ejemplo. El nombre del servidor maestro para esta zona es *ks3277174.kimsufi.com*. Esto significa que en el archivo *named.conf* existe una entrada que apunta y este archivo vuelve a su vez a la entrada en el archivo de configuración.

Clase

Existen varios tipos de clases DNS. En nuestro caso solo se usará la clase *IN* o *Internet*, usadas para definir el mapeo entre la dirección IP y *BIND*.

Tipo

El tipo de registro para el recurso DNS, en el ejemplo de arriba, el tipo es *SOA*.

Nombre del servidor

Nombre completo del servidor de nombres primario. Debe acabar en un punto.

Dirección de correo

Dirección de correo de la persona responsable del dominio. Nota cómo se sustituye el símbolo @ por un punto.

Número de serie

Normalmente tiene el formato *YYYYMMDD* (El uso del formato de número de serie recomendado por IETF (*Internet Engineering Task Force*) y RIPE (**Réseaux IP Européens**) es obligatorio para muchos dominios registrados en algunas zonas DNS de alto nivel, mayoritariamente europeas. Si su dominio está registrado en una de estas zonas y su registrador no acepta su número de serie SOA, el uso del formato de número de serie recomendado por IETF y RIPE debería solucionar esta incidencia.

Los servidores que usan la sintaxis UNIX-timestamp para configurar zonas DNS. UNIX timestamp es el número de segundos desde el 1 de enero del 1970 (Unix Epoch). El timestamp 32-bit finalizará el 8 de julio del 2038.

RIPE recomienda usar el formato *YYYYMMDDNN* , donde *YYYY* es el año (cuatro dígitos), *MM* es el mes (dos dígitos), *DD* es el día del mes (dos dígitos) y *nn* es la versión para día (dos dígitos). El formato *YYYYMMDDNN* no finalizará hasta el año 4294) con dos dígitos más al final que indican el número de serie del día. El número de serie es útil para indicarle al servidor DNS secundario cuando debe actualizarse. Si el servidor esclavo al comprobar el número de serie ha cambiado, realizará una transferencia de zona (**zone transfer**).

Refresh o actualización

En este campo indica al servidor DNS esclavo o secundario con qué frecuencia debería comprobar el estado del maestro. El valor está representado en segundos. En cada ciclo de refresco, el esclavo realiza la comprobación para saber cuando es necesaria una transferencia de zona (**zone transfer**). En el ejemplo el valor es 7200

Retry o reintento

Frecuencia con la que el esclavo debería conectarse al maestro en caso de una conexión fallida.

Expiry o expiración

Cantidad total de tiempo en la que el esclavo debería reintentar ponerse en contacto con el maestro antes de que expiren los datos que contiene. Referencias futuras serán dirigidas a los servidores root.

TTL mínimo

Este campo define el tiempo de vida (*Time To Live*) para el dominio en segundos. Sirve para responder a peticiones de subdominios que no existen en los registros. Cuando esté configurado, el servidor DNS responderá con una respuesta del tipo **no domain** o **NXDOMAIN**. Dicha respuesta será cacheada. El TTL establece la duración del cacheo para la respuesta.

Después de estos campos, se especifican los servidores de nombres para el dominio. **NS** es el acrónimo de **Name Server**. Como se ha visto un poco más arriba, el servidor de nombres principal del ejemplo es *ks3277174.kimsufi.com*. También se define el servidor DNS secundario o esclavo, en este caso *ns.kimsufi.com*.

Además de los registros *NS*, se definen los registros **MX**, que identifican el servidor de correo para el dominio, el número 10 define la prioridad del servidor de correo. Así como el registro de tipo **A**, que asocia un nombre a una dirección ip.

En el ejemplo existe un único registro **MX**, pero puede haber más. Por ejemplo:

MX 10 mail.elbauldelprogramador.com.

MX 20 mail.otrodominio.com.

Si se envía un email al dominio, el servidor de correo que envía el email intenta conectarse a *mail.elbauldelprogramador.com* ya que tiene prioridad 10, si no puede establecer conexión, lo intentará con ** mail.otrodominio.com**.

El último tipo de registro que vamos a ver es el de tipo **CNAME** (*Canonical Name*). Se suele referir a ellos como registros alias del tipo **A**. Por ejemplo:

ftp CNAME www

significa que *ftp.elbauldelprogramador.com* es un alias de *www.elbauldelprogramador.com*. Es decir, *ftp.elbauldelprogramador.com* apunta al mismo servidor que *www.elbauldelprogramador.com*. Un registro **CNAME** debe apuntar a un registro de tipo **A** y solo de tipo **A**.

En el siguiente artículo se verá el archivo de zona inversa y la configuración del servidor DNS secundario, así como el uso del comando *dig*.

Cuando se está enviando una consulta a un servidor DNS. Si la consulta es correcta, el sitio web se abrirá; de lo contrario, recibirá un mensaje de error. El registro de estas consultas correctas e incorrectas se guarda en una ubicación de almacenamiento temporal del equipo denominada caché DNS. DNS comprueba siempre la caché antes de hacer una consulta a un servidor DNS y si encuentra que un registro coincide con la consulta, DNS usa ese registro en lugar de enviar la consulta al servidor. Esto permite que las consultas sean más rápidas y reduce el tráfico de la red e Internet.