Domain Name System

Revisión: 2025-05-21

Glosario

Las siguientes definiciones fueron tomadas del [RFC7719], sección 2, 4 y 6

Domain name	Section 3.1 of [RFC1034] talks of "*the domain name space*" as a tree structure. "Each node has a label, which is zero to 63 octets in length. ... The domain name of a node is the list of the labels on the path from the node to the root of the tree. ... To simplify implementations, the total number of octets that represent a domain name (i.e., the sum of all label octets and label lengths) is limited to 255. Any label in a domain name can contain any octet value.
Fully qualified domain name (FQDN)	This is often just a clear way of saying the same thing as "domain name of a node", as outlined above. However, the term is ambiguous. Strictly speaking, a fully qualified domain name would include every label, including the final, zero-length label of the root: such a name would be written "`www.example.net.`" (note the terminating dot). But because every name eventually shares the common root, names are often written relative to the root (such as "`www.example.net`") and are still called "fully qualified". This term first appeared in [RFC819].
Label	The identifier of an individual node in the sequence of nodes identified by a fully qualified domain name.
Alias	The owner of a CNAME resource record, or a subdomain of the owner of a DNAME resource record [RFC6672]. See also "canonical name".
Canonical name	A CNAME resource record "*identifies its owner name as an alias, and specifies the corresponding canonical name in the RDATA section of the RR.*" (Quoted from [RFC1034], Section 3.6.2) This usage of the word "canonical" is related to the mathematical concept of "canonical form".
CNAME	"*It is traditional to refer to the owner of a CNAME record as 'a CNAME'. This is unfortunate, as 'CNAME' is an abbreviation of 'canonical name', and the owner of a CNAME record is an alias, not a canonical name.*" (Quoted from [RFC2181], Section 10.1.1)
RR	An acronym for resource record. ([RFC1034] Section 3.6.)

RRset

A set of resource records with the same label, class and type, but with different data. (Definition from [RFC2181]) Also spelled RRSet in some documents. As a clarification, "same label" in this definition means "same owner name". In addition, [RFC2181] states that "the TTLs of all RRs in an RRSet must be the same". (This definition is definitely not the same as "the response one gets to a query for `QTYPE=ANY`", which is an unfortunate misunderstanding.)

TTL

The maximum "time to live" of a resource record. "*A TTL value is an unsigned number, with a minimum value of 0, and a maximum value of `2147483647`. That is, a maximum of `2^31 - 1`. When transmitted, the TTL is encoded in the less significant 31 bits of the 32 bit TTL field, with the most significant, or sign, bit set to zero.*" (Quoted from [RFC2181], Section 8) (Note that [RFC1035] erroneously stated that this is a signed integer; that was fixed by [RFC2181].)

The TTL "*specifies the time interval that the resource record may be cached before the source of the information should again be consulted*". (Quoted from [RFC1035], Section 3.2.1) Also: "*the time interval (in seconds) that the resource record may be cached before it should be discarded*". (Quoted from [RFC1035], Section 4.1.3). Despite being defined for a resource record, the TTL of every resource record in an RRset is required to be the same ([RFC2181], Section 5.2).

The reason that the TTL is the maximum time to live is that a cache operator might decide to shorten the time to live for operational purposes, such as if there is a policy to disallow TTL values over a certain number. Also, if a value is flushed from the cache when its value is still positive, the value effectively becomes zero. Some servers are known to ignore the TTL on some RRsets (such as when the authoritative data has a very short TTL) even though this is against the advice in [RFC1035].

There is also the concept of a "default TTL" for a zone, which can be a configuration parameter in the server software. This is often expressed by a default for the entire server, and a default for a zone using the $TTL directive in a zone file. The $TTL directive was added to the master file format by [RFC2308].

Apex

The point in the tree at an owner of an `SOA` and corresponding authoritative NS RRset. This is also called the "*zone apex*". [RFC4033] defines it as "*the name at the child's side of a zone cut*". The "apex" can usefully be thought of as a data-theoretic

> description of a tree structure, and "origin" is the name of the same concept when it is implemented in zone files. The distinction is not always maintained in use, however, and one can find uses that conflict subtly with this definition. [RFC1034] uses the term "top node of the zone" as a synonym of "apex", but that term is not widely used. [...]

Clientes DNS

E42. *{W}* Utilizando herramientas de línea de comandos determine cuál es el servidor de nombres que es autoridad para cada uno de los `FQDN`:

- `google.com.`
- `itba.edu.ar.`
- `pampero.it.itba.edu.ar.`

Revise los paquetes enviados, y sus respuestas.

E43. Determine cuales son los servidores que manejan el correo electrónico entrante para cada uno de los siguientes dominios FQDNS:

- `google.com.`
- `itba.edu.ar.`
- `it.itba.edu.ar.`

E44. ¿Cuales son todos los servidores de nombre que entran en juego para resolver `pampero.it.itba.edu.ar` partiendo desde un *root server*?

E45. **dig** tiene una opción `trace`. ¿para qué sirve dicha opción? Contrastar su resultado con el punto anterior.

E46. *{W}* Utilizar **whois** para obtener información de los dominios: `clarin.com`, `google.com`, `facebook.com`, `lanacion.com.ar`, `itba.edu.ar`, `apple.com`.

DNS y HTTP

E47. Realizar los cambios necesarios para que al ingresar en un *User Agent HTTP* (**curl**, Google Chrome, ...) a `http://foo.pdc.lab`, en realidad se acceda `http://protos.foo/` (no se debe ver modificada la URL en el browser). ¿Qué sucede y por qué?

Aviso

Puede obtener diferentes resultados si realiza las pruebas conectado desde la red del laboratorio y fuera de ésta. Se requiere una solución estable.

E48. Suponga que en el ejercicio anterior se permite que la URL en el browser pueda ser modificada. ¿Puede encontrar otra solución?

Configuración de DNS Server

Se quiere configurar un servidor DNS que sea autoridad de la zona `foo.pdc.lab`. Dicha zona deberá mantener nombres para su host y algunos otros hosts de la red en la que se encuentra. Configurar también un alias para cada uno de estos hosts.

E49. De existir, borrar los archivos `/etc/named.caching-server.conf`, `/var/named/chroot/etc/named.caching-server.conf`.

E50. Crear la zona correspondiente a su dominio (forward mapping zone y reverse zone). La configuración de named se encuentra en `/etc/bind`. Establezca una variedad de registros, con diferentes TTL.

E51. Indicarle al daemon que reinicie. Observar el mensaje almacenado en el log, elaborar conclusiones en base al mismo.

E52. Comprobar usando las utilidades **dig**, **host** y **nslookup** que su dominio esté configurado correctamente.

E53. Asegurarse que su host esté utilizando al servidor DNS configurado como su servidor DNS primario

E54. {W} Investigar en named que son los forwarders. Sniffear paquetes haciendo uso y sin hacer uso de forwarders para ver los paquetes que generan el servidor DNS cuando le hacen consultas.

Bibliografía

[RFC819] *The Domain Naming Convention for Internet User Applications, [https://tools.ietf.org/html/rfc819]*. The Internet Engineering Task Force. August 1982.

This RFC is an attempt to clarify the generalization of the Domain Naming Convention, the Internet Naming Convention, and to explore the implications of its adoption for Internet name service and user applications.

[RFC1033] *Domain Administrators Operations Guide [https://tools.ietf.org/html/rfc1033]*. The Internet Engineering Task Force. November 1987.

This RFC provides guidelines for domain administrators in operating a domain server and maintaining their portion of the hierarchical database. Familiarity with the domain system is assumed

[RFC1034] *Domain names - concepts and facilities [https://tools.ietf.org/html/rfc1034]*. The Internet Engineering Task Force. November 1987.

This RFC is the revised basic definition of The Domain Name System. It obsoletes RFC-882. This memo describes the domain style names and their used for host address look up and electronic mail forwarding. It discusses the clients and servers in the domain name system and the protocol used between them.

[RFC1035] *Domain names - implementation and specification [https://tools.ietf.org/html/rfc1035]*. The Internet Engineering Task Force. November 1987.

This RFC is the revised specification of the protocol and format used in the implementation of the Domain Name System. It obsoletes RFC-883. This memo documents the details of the domain name client - server communication.

[RFC2181] *Clarifications to the DNS Specification [https://tools.ietf.org/html/rfc2181]*. The Internet Engineering Task Force. July 1997.

This document considers some areas that have been identified as problems with the specification of the Domain Name System, and proposes remedies for the defects identified.

[RFC2308] *Negative Caching of DNS Queries [https://tools.ietf.org/html/rfc2308]*. The Internet Engineering Task Force. March 1998.

RFC1034 provided a description of how to cache negative responses. It however had a fundamental flaw in that it did not allow a name server to hand out those cached responses to other resolvers, thereby greatly reducing the effect of the caching. This document addresses issues raise in the light of experience and replaces RFC1034 Section 4.3.4.

[RFC4033] *DNS Security Introduction and Requirements [https://tools.ietf.org/html/rfc4033]*. The Internet Engineering Task Force. March 2005.

The Domain Name System Security Extensions (DNSSEC) add data origin authentication and data integrity to the Domain Name System. This document introduces these extensions and describes their capabilities and limitations. This document also discusses the services that the DNS security extensions do and do not provide. Last, this document describes the interrelationships between the documents that collectively describe DNSSEC.

[RFC6672] *DNAME Redirection in the DNS [https://tools.ietf.org/html/rfc6672]*. The Internet Engineering Task Force. June 2012.

The DNAME record provides redirection for a subtree of the domain name tree in the DNS. That is, all names that end with a particular suffix are redirected to another part of the DNS. This document obsoletes the original specification in RFC 2672 as well as updates the document on representing IPv6 addresses in DNS (RFC 3363)

[RFC7719] *DNS Terminology [https://tools.ietf.org/html/rfc7719]*. The Internet Engineering Task Force. DECEMBER 2015.

The DNS is defined in literally dozens of different RFCs. The terminology used by implementers and developers of DNS protocols, and by operators of DNS systems, has so-

metimes changed in the decades since the DNS was first defined. This document gives current definitions for many of the terms used in the DNS in a single document.

[RFC3912] *WHOIS Protocol Specification [https://tools.ietf.org/html/rfc3912]*. The Internet Engineering Task Force. September 2004.

This document updates the specification of the WHOIS protocol, thereby obsoleting RFC 954. The update is intended to remove the material from RFC 954 that does not have to do with the on-the-wire protocol, and is no longer applicable in today's Internet. This document does not attempt to change or update the protocol per se, or document other uses of the protocol that have come into existence since the publication of RFC 954.

[ISC-DNS] *DNS RFC [https://www.isc.org/community/rfcs/dns/]*. Internet Systems Consortium.

The Domain Name System protocols are more than 20 years old, and many of the older RFCs are obsolete, but there still exist clients running software implementing the very oldest protocols. Here are the RFCs pertaining to DNS.

[domainsroot] *Domain Name Services [https://www.iana.org/domains]*. Internet Assigned Numbers Authority.

IANA is responsible for management of the DNS root zone. This role means assigning the operators of top-level domains, such as .uk and .com, and maintaining their technical and administrative details.

[dig(1)] *DNS lookup utility*. BIND9.

dig (domain information groper) is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use and clarity of output. Other lookup tools tend to have less functionality than dig.

[nslookup(1)] *nslookup - query Internet name servers interactively*. BIND9.

nslookup is a program to query Internet domain name servers. Nslookup has two modes: interactive and non-interactive. Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain. Non-interactive mode is used to print just the name and requested information for a host or domain.

[nsswitch.conf(5)] `nsswitch.conf` - *Name Service Switch configuration file*. Linux Programmer's Manual.

The Name Service Switch (NSS) configuration file, `/etc/nsswitch.conf`, is used by the GNU C Library to determine the sources from which to obtain name-service information in a range of categories, and in what order. Each category of information is identified by a database name.

[resolv.conf(5)] `nsswitch.conf` - *Name Service Switch configuration file*.

> The Name Service Switch (NSS) configuration file, `/etc/nsswitch.conf`, is used by the GNU C Library to determine the sources from which to obtain name-service information in a range of categories, and in what order. Each category of information is identified by a database name.