

DNS

Domain Name System

Basado en Kurose & Ross “*Computer Networking: A Top Down Approach Featuring the Internet*”. 3ed

DNS: Domain Name System

Personas:

muchos identificadores:

- DNI, pasaporte, Nro de seguro, nombre, etc.

Host y router en Internet:

- Dirección IP (32 bit) – usada para direccionar datagramas (ideal para router)
- “nombre”, e.g., www.yahoo.com – son usados por humanos

Domain Name System:

- *Base de datos distribuida* implementada en una jerarquía de muchos *servidores de nombres*
- *Protocolo de capa aplicación* permite a host, routers, y servidores de nombre comunicarse para *resolver* nombres (traducción dirección/nombre)
- No está orientado al uso directo de los usuarios.

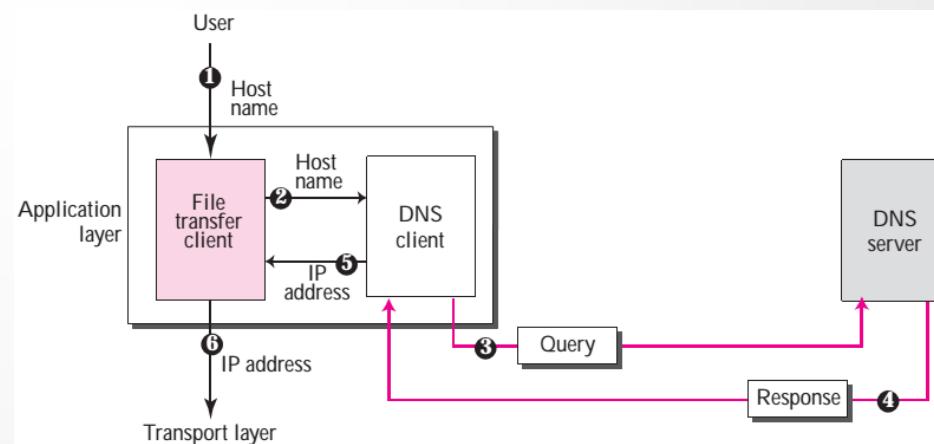
DNS

Servicios DNS

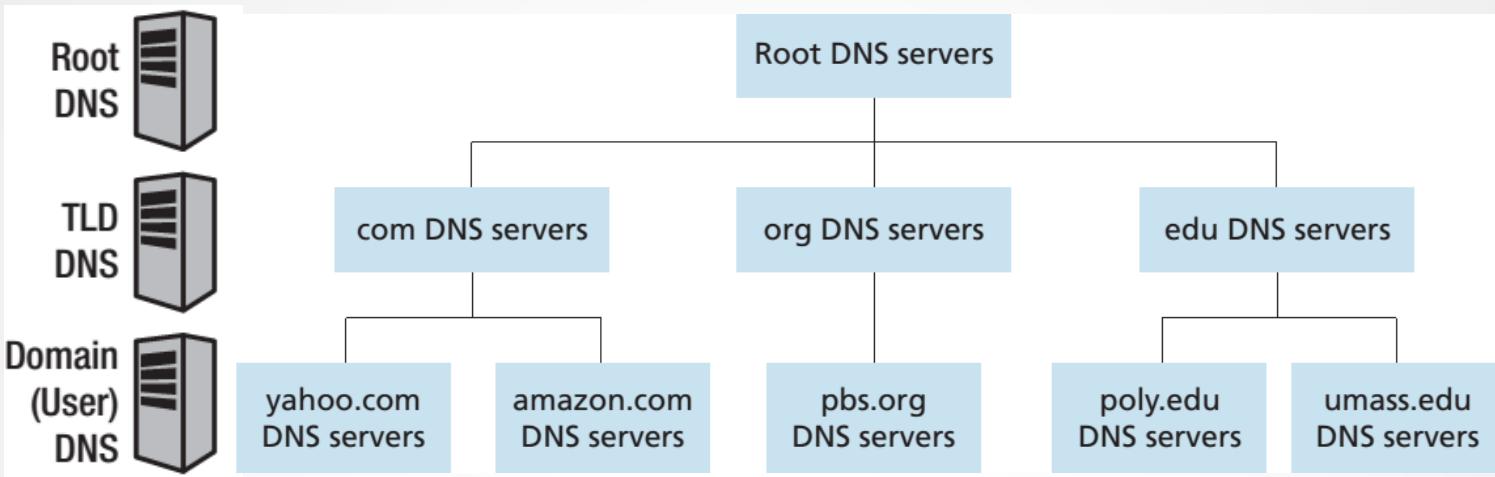
- Traducción de nombre de host a dirección IP
- Alias para host
 - Nombre canónico o alias
 - Nombre canónico: CNAME en RFC 1035
- Alias para servidor de correo
- Distribución de carga
 - Servidores Web replicados: conjunto de direcciones IP para un nombre canónico (e.g. relay1.west-coast.amazon.com), servidor DNS rota entre direcciones IP

¿Por qué no centralizar DNS?

- Único punto de falla
- Volumen de tráfico, muchos necesitan el DNS
- Sería una base de datos centralizada distante con grandes retardos de acceso.
- Mantenimiento: Es mejor que cada dominio gestione sus nombres
Porque no es *scalable!*



Base de datos jerárquica y distribuida

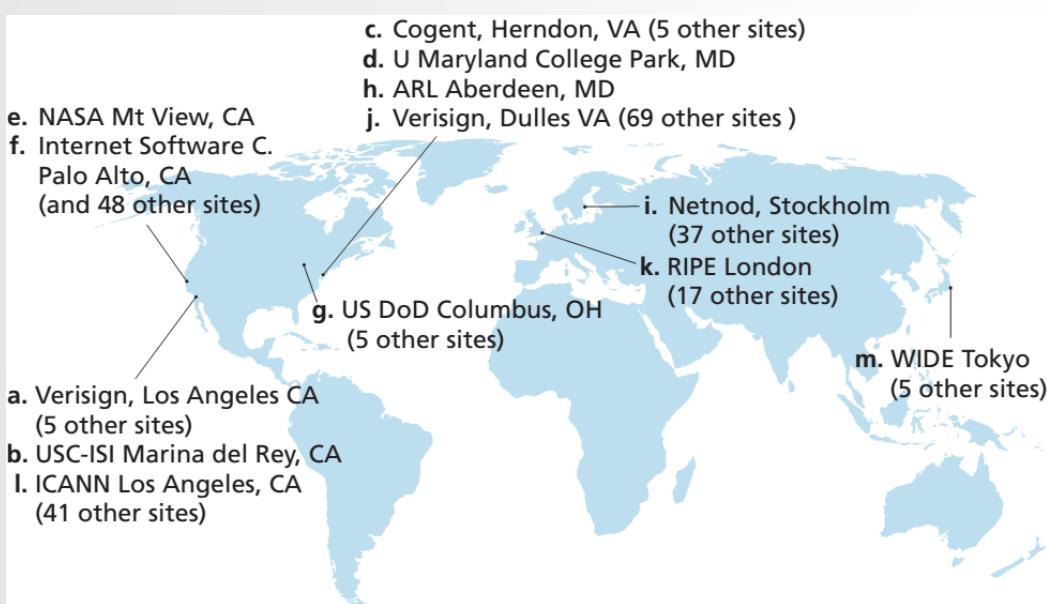


Cliente desea IP de www.amazon.com; 1^{ra} aprox. :

- Cliente consulta al servidor raíz para encontrar servidor DNS de com
- Cliente consulta servidor DNS TLD (Top Level Domain) de *com* para obtener servidor DNS de *amazon.com*
- Cliente consulta servidor DNS *amazon.com* para obtener dirección IP de *www.amazon.com*

DNS: servidores de nombre raíz

- Son contactados por servidor de nombre local cuando no puede resolver un nombre.
- La lista actual de servidores se mantiene en <https://www.iana.org/domains/root/servers>
- Servidor nombre raíz:
 - Contacta servidor de nombre autorizado de la zona superior (por ejemplo *COM*) si mapeo del nombre es desconocido para él
 - Obtiene mapeo (propio o desde otro servidor raíz)
 - Retorna mapeo al servidor de nombre local

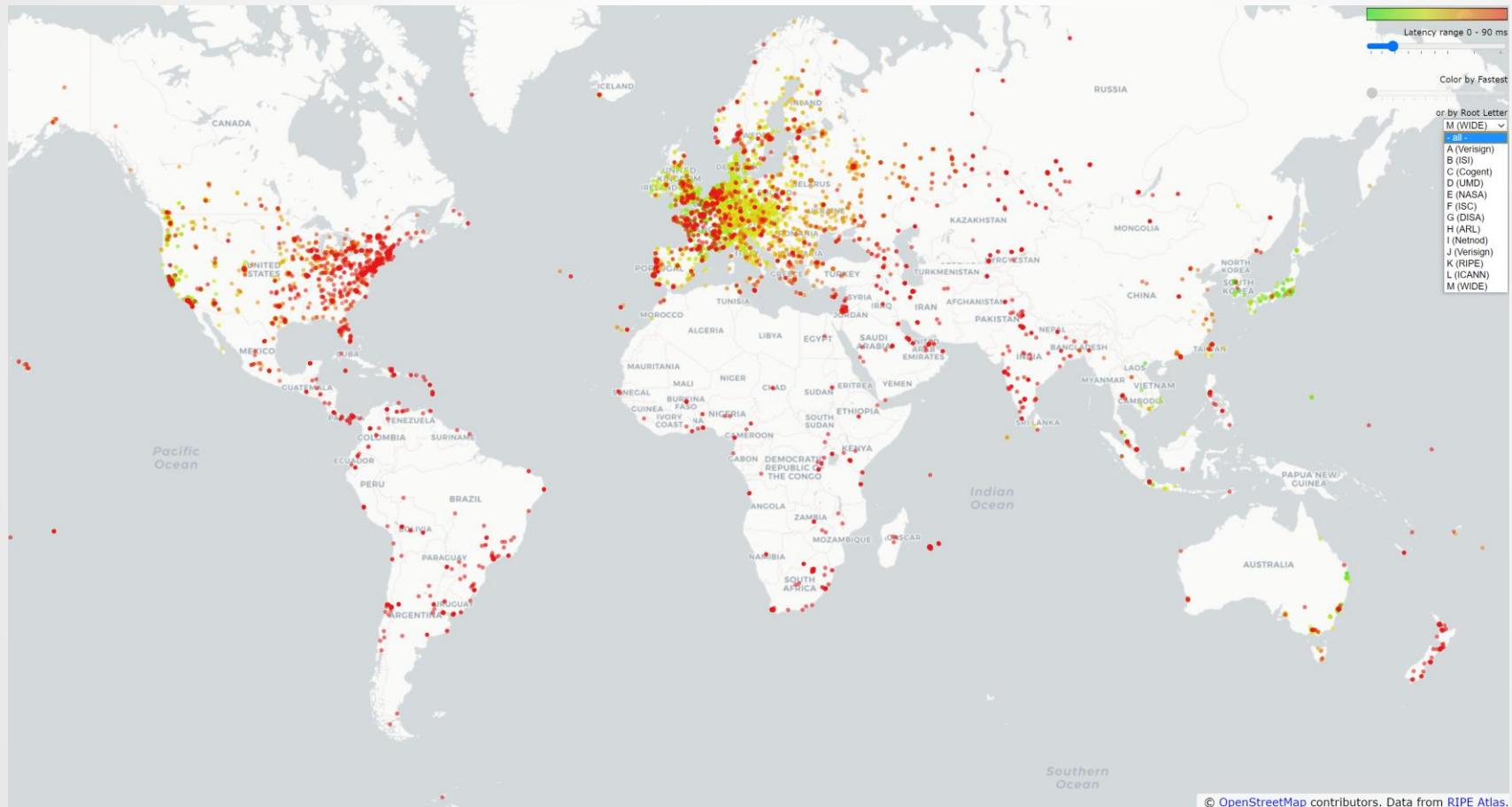


List of Root Servers

HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

DNS: Servidores a nivel mundial

- El siguiente gráfico muestra los servidores de nombre de dominio de acuerdo a datos de RIPE, al 04/02/2023):



TLD y Servidores Autorizados

- **Top-level domain (TLD) servers:** responsable por com, org, net, edu, etc., y todos los dominios superiores de cada país: uk, fr, ca, jp, pe, etc..
 - Network solutions mantiene servidores para el TLD de com
 - Educause para el TLD de edu
 - NIC (network information center) para el TLD de pe (www.nic.pe)
- **Servidores DNS autorizados:** son servidores DNS de las organizaciones y proveen mapeo autorizado entre el nombre de host y su dirección IP.
 - Éstos pueden ser mantenidos por la organización o el proveedor de servicio

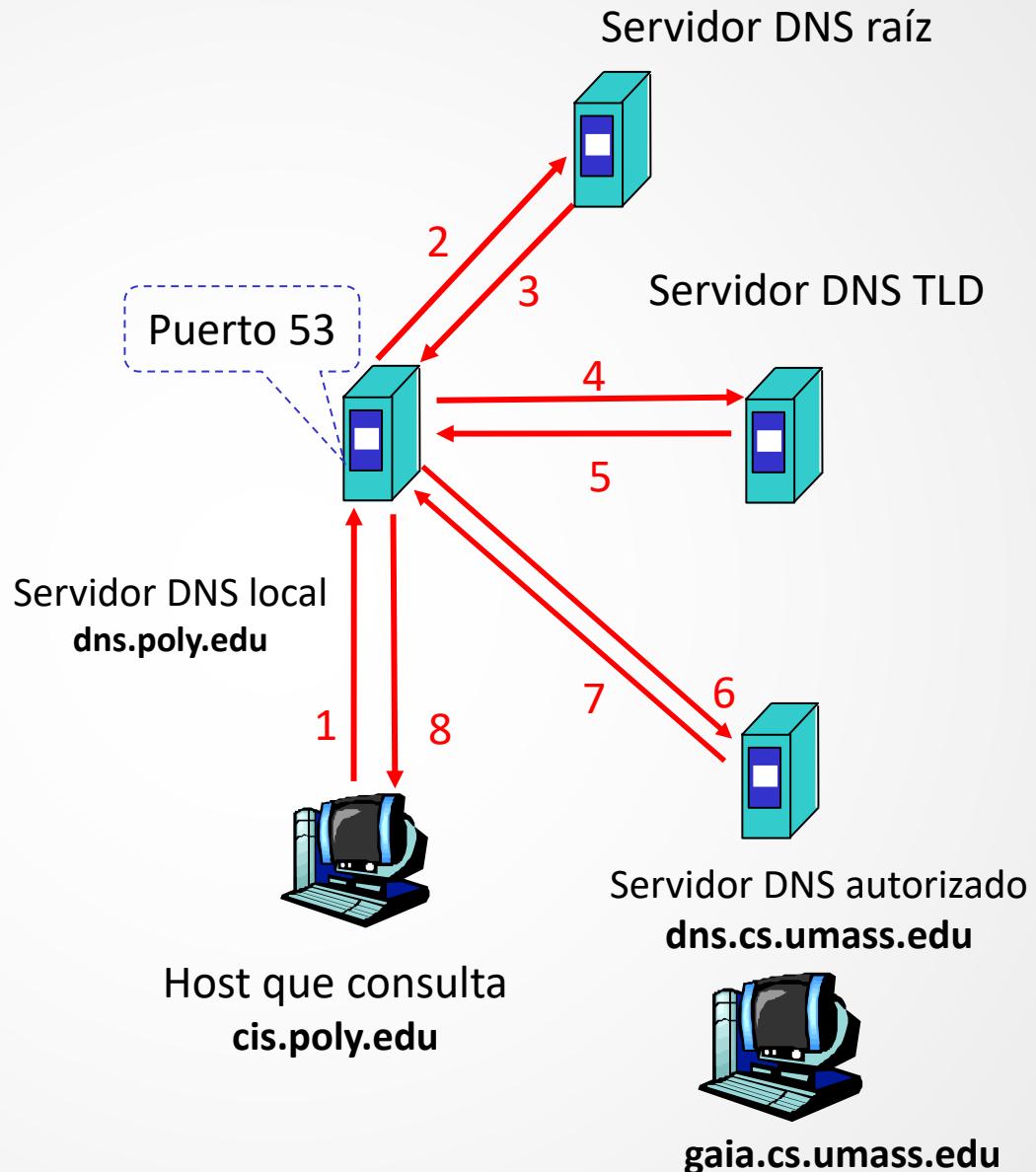
Servidor de nombre local

- No pertenece estrictamente a la jerarquía
- Cada ISP (ISP residencial, compañía, universidad) tiene uno.
 - También son llamados “servidor de nombre por omisión” (default name server)
- Cuando un host hace una consulta DNS, ésta es enviada a su servidor DNS local
 - Actúa como proxy, re-envía consulta dentro de la jerarquía.

Ejemplo 1

Consulta iterativa:

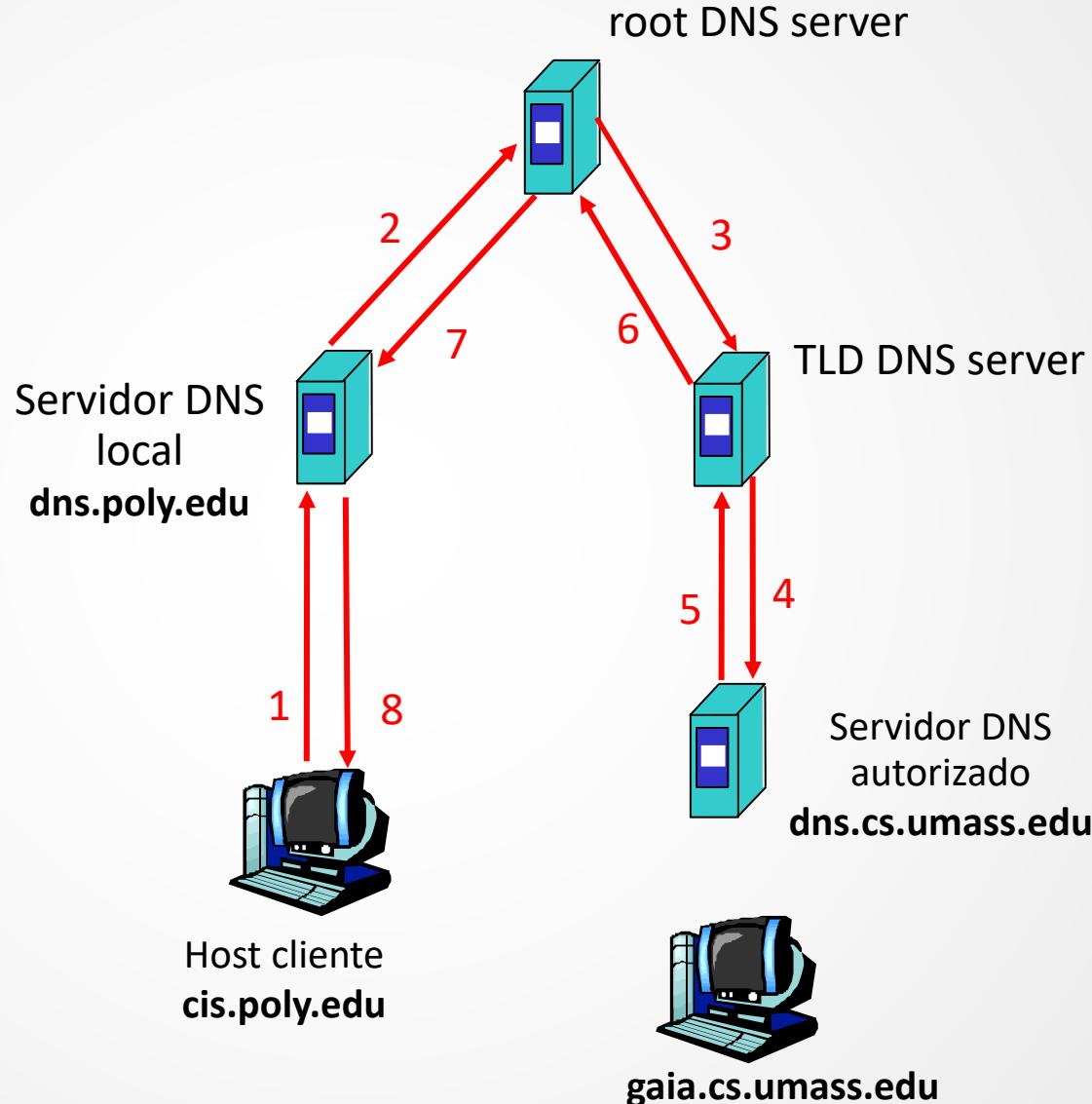
- Host en cis.poly.edu quiere la dirección IP de gaia.cs.umass.edu
- Servidor contactado responde con el nombre del servidor a contactar
- “Yo no conozco este nombre, pero pregunta a este servidor”



Consultas Recursivas

Consulta recursiva :

- Pone la carga de la resolución de nombre al servidor contactado.
- ¿Qué pasa en situaciones de alta carga?



Ejemplo

- Ejemplos de consultas:

```
C:\Users\ecp>nslookup -type=mx sunarp.gob.pe
Servidor: dns.google
Address: 8.8.8.8

Respuesta no autoritativa:
sunarp.gob.pe    MX preference = 10, mail exchanger = ASPMX2.GOOGLEMAIL
sunarp.gob.pe    MX preference = 10, mail exchanger = ASPMX3.GOOGLEMAIL
sunarp.gob.pe    MX preference = 1, mail exchanger = ASPMX.L.GOOGLE.COM
sunarp.gob.pe    MX preference = 5, mail exchanger = ALT1.ASPMX.L.GOOGLE
sunarp.gob.pe    MX preference = 5, mail exchanger = ALT2.ASPMX.L.GOOGLE

C:\Users\ecp>nslookup -type=soa sunat.gob.pe
Servidor: dns.google
Address: 8.8.8.8

Respuesta no autoritativa:
sunat.gob.pe
primary name server = app2.sunat.gob.pe
responsible mail addr = hostmaster.app2.sunat.gob.pe
serial = 2022121605
refresh = 10800 (3 hours)
retry = 3600 (1 hour)
expire = 604800 (7 days)
default TTL = 60 (1 min)

C:\Users\ecp>nslookup -debug openai.com
-----
Got answer:
HEADER:
opcode = QUERY, id = 1, rcode = NOERROR
header flags: response, want recursion, recursion avail.
questions = 1, answers = 1, authority records = 0, additional = 0

QUESTIONS:
8.8.8.in-addr.arpa, type = PTR, class = IN
ANSWERS:
-> 8.8.8.in-addr.arpa
name = dns.google
ttl = 16287 (4 hours 31 mins 27 secs)
```

Ejemplo

- Luego:
\$ nslookup 200.37.189.196
- Finalmente:
\$ nslookup www.google.com
- Y
\$ nslookup 74.125.67.104

```
C:\Users\User7>nslookup 200.37.189.196
Servidor: google-public-dns-a.google.com
Address: 8.8.8.8

Nombre: qenqo.uandina.edu.pe
Address: 200.37.189.196

C:\Users\User7>
```

```
C:\Users\User7>nslookup www.google.com
Servidor: google-public-dns-a.google.com
Address: 8.8.8.8

Respuesta no autoritativa:
Nombre: www.google.com
Addresses: 2800:3f0:4003:c00::67
          181.64.131.155
          181.64.131.185
          181.64.131.158
          181.64.131.177
          181.64.131.166
          181.64.131.147
          181.64.131.143
          181.64.131.173
          181.64.131.181
          181.64.131.170
          181.64.131.157
          181.64.131.172
          181.64.131.151
          181.64.131.187
          181.64.131.162
```

```
C:\Users\User7>nslookup 74.125.67.104
Servidor: google-public-dns-a.google.com
Address: 8.8.8.8

Nombre: 104.67.125.74.bc.googleusercontent.com
Address: 74.125.67.104
```

DNS: Cache y actualización de registros

- Una vez que un servidor de nombre conoce un mapeo, éste *guarda* el mapeo
 - Las entradas del cache expiran (desaparecen) después de algún tiempo
 - Servidores TLD típicamente están en cache de los servidores de nombre locales
 - Así los servidores de nombre raíz no son visitados con frecuencia
- Mecanismos de Actualización/notificación están bajo diseño por el IETF (Internet Engineering Task Force)
 - RFC 2136
 - <http://www.ietf.org/html.charters/dnsind-charter.html>

Registros DNS

DNS: es una base de datos distribuida que almacena registros de recursos (resource records, **RR**)

Formato RR: **(name, value, type, ttl)**

- Type=A
 - **name** es un hostname
 - **value** es una dirección IP
- Type=NS
 - **name** es un dominio (e.g. foo.com)
 - **value** es la dirección IP (nombre) del servidor autorizado que sabe cómo obtener las direcciones IP de este dominio.
- Type=CNAME
 - **name** es un alias para algún nombre real
 - www.ibm.com es realmente servereast.backup2.ibm.com
 - **value** es el nombre real
- Type=MX
 - **value** es el nombre del servidor de correo asociado con **name**

Registros DNS

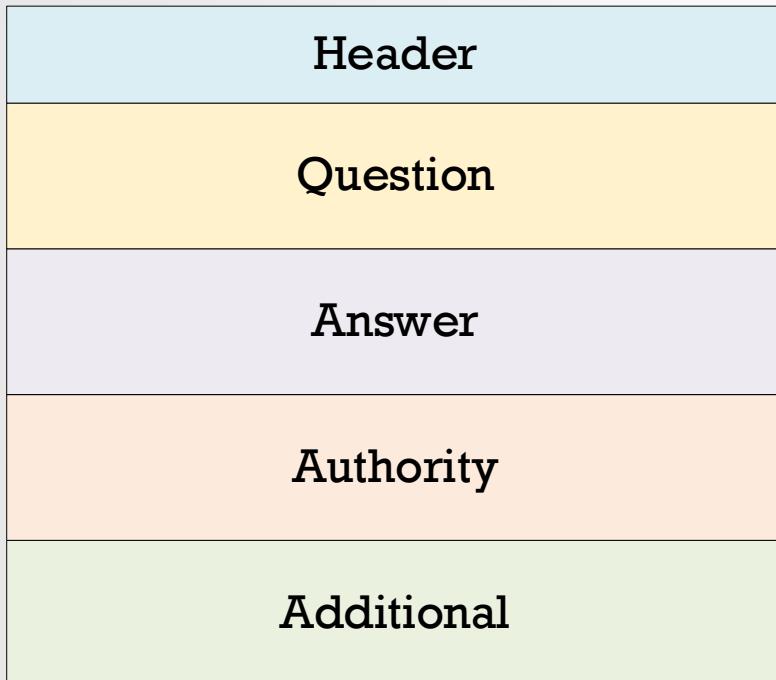
Otros registros DNS

- **A** — IPv4 address
 - **AAAA** — IPv6 address
 - **AFSDB** — AFS database location
 - **APL** — Address prefix list
 - **AXFR** — Authoritative zone transfer
 - **CAA** — Certification authority authorization
 - **CDNSKEY** — Child copy of a DNSKEY
 - **CDS** — Child copy of DS
 - **CERT** — Cryptographic certificate
 - **CNAME** — Canonical name
 - **CSYNC** — Child-to-parent synchronization
 - **DHCID** — DHCP identifier
 - **DLV** — DNSSEC lookaside validation
 - **DNAME** — Delegation name
 - **DNSKEY** — Cryptographic key for DNSSEC
 - **DS** — Delegation signer
 - **EUI48** — MAC address (EUI-48)
 - **EUI64** — Mac address (EUI-64)
 - **HINFO** — Host information
 - **HIP** — Host identification protocol
 - **HTTPS** — HTTPS binding
 - **IPSECKEY** — Cryptographic key for IPsec
 - **IXFR** — Incremental zone transfer
 - **KEY** — Cryptographic key for DNSSEC (obsoleted by DNSKEY)
 - **KX** — Key exchange
 - **LOC** — Geographical location
 - **MX** — Mail exchange
 - **NAPTR** — naming authority pointer
 - **NS** — Name server
 - **NSEC3** — Next secure (version 3)
 - **NSEC3PARAM** — Parameter for NSEC3
 - **NSEC** — Next secure (obsoleted by NSEC3)
 - **NXT** — DNSSEC key (obsoleted by NSEC)
 - **OPENPGPKEY** — Public key for OpenPGP
 - **OPT** — EDNS option
 - **PTR** — Canonical name pointer
 - **RP** — Responsible person
 - **RRSIG** — Resource record signature for DNSSEC
 - **SIG** — Resource record signature for DNSSEC (obsoleted by RRSIG)
 - **SMIMEA** — S/MIME association
 - **SOA** — Start of authority
 - **SSHFP** — Public key fingerprint for SSH
 - **SVCB** — Service binding
 - **SRV** — Service locator
 - **TA** — Trust authorities for DNSSEC
 - **TKEY** — Transaction key
 - **TLSA** — Certificate association for TLS
 - **TSIG** — Transaction signature
 - **TXT** — Human-readable text
 - **URI** — Uniform resource identifier
 - **ZONEMD** — Message digest for DNS zones



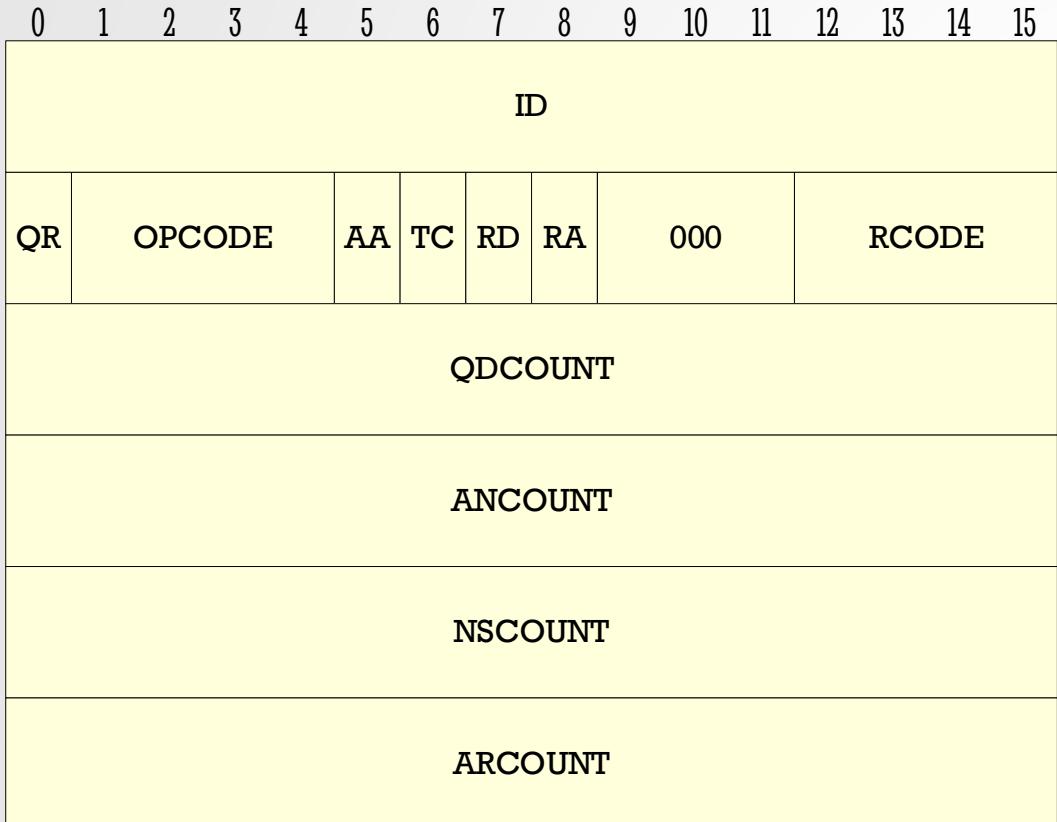
Mensaje DNS

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15



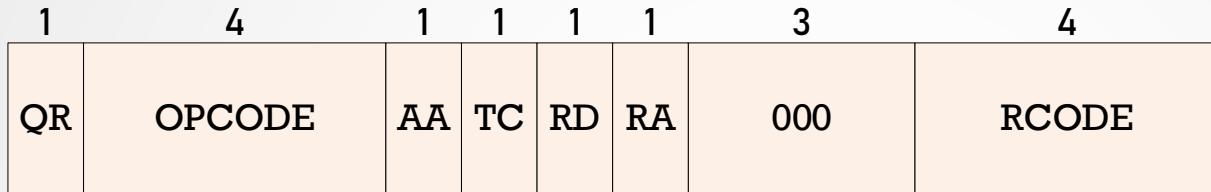
- *Question* – La consulta al servidor de nombres.
- *Answer* – RRs de respuesta a la consulta.
- *Authority* – RRs apuntando hacia la autoridad.
- *Additional* – RRs con información adicional.

Mensaje DNS - Header



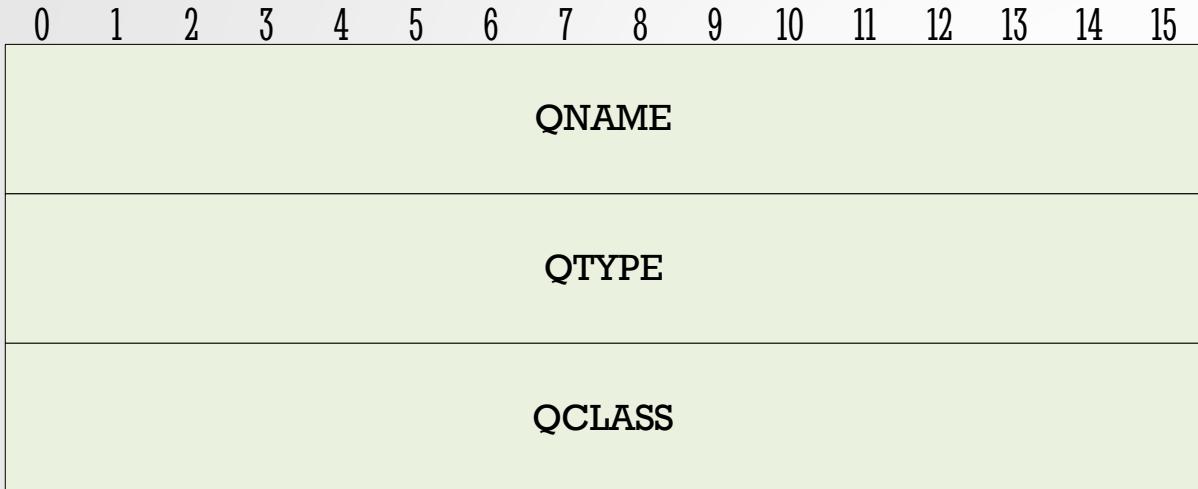
- *ID – Identificador que debe coincidir entre la consulta y la respuesta*
- *QDCOUNT – Cantidad de registros en la sección Query*
- *ANCOUNT – Cantidad de registros en la sección Answer (0 en mensajes de consulta)*
- *NSCOUNT – Cantidad de registros en la sección Authority (0 en mensajes de consulta)*
- *ARCOUNT – Cantidad de registros en la sección Additional (0 en mensajes de consulta)*

Mensaje DNS - Flags



- *QR (query/response)* – Indica si es una consulta o una respuesta
 - 0 – Consulta
 - 1 - Respuesta
- *OPCODE* – Tipo de consulta o respuesta
 - Standard Query (0)
 - Inverse Query (1)
 - Server Status Request (2)
- *AA (Authoritative answer)* – Respuesta autorizada
 - 1 – el servidor de nombres es autorizado
- *TC (truncated)* – Mensaje truncado
 - 1 – la respuesta tenía más de 512 bytes y se truncó a 512.
- *RD (recursión desired)* – Consulta recursiva
 - 1 – el cliente desea una respuesta recursiva
- *RA (recursión available)* – Indica si el servidor soporta consultas recursivas (solo en mensajes de respuesta)
- *RCODE* – Código de error en la respuesta

Mensaje DNS - Question

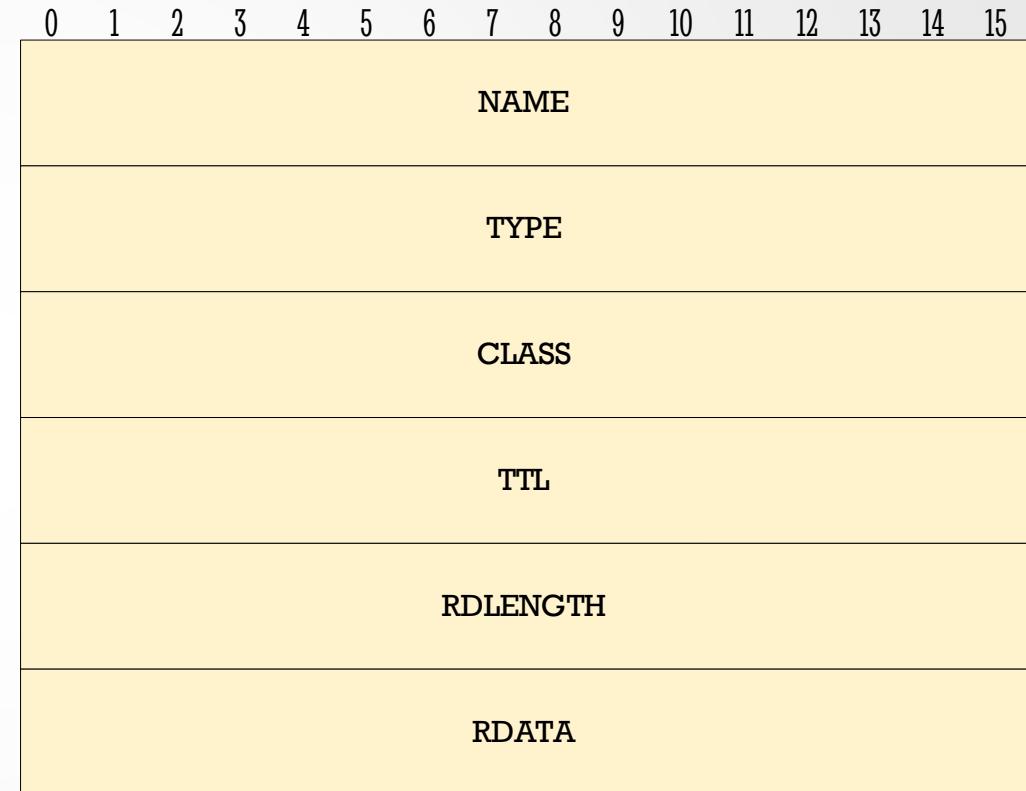


Contiene uno o mas RR. Presente en mensajes de consulta y respuesta

- *QNAME – Contiene un nombre de dominio representado como una secuencia de etiquetas*
- *QTYPE – Contiene un código de 2 bytes que especifica el tipo de RR por el que se consulta (SOA, A, NS, PTR, ANY, etc.)*
- *QCLASS – Contiene la clase del registro (normalmente IN)*

Mensaje DNS – Answer, Authority, Additional

- **Answer section:** contiene uno o mas RR. Presente solo en mensajes de respuesta. incluye la respuesta del servidor al cliente.
- **Authoritative section:** contiene uno o mas RR. Presente solo en mensajes de respuesta. Brinda información (nombre de dominio) sobre uno o mas servidores autorizados a la consulta.
- **Additional Information section:** consiste de uno o mas RR. Presente solo en mensajes de respuesta. Proporciona información adicional que puede ayudar al resolver.
 - NAME – Contiene el nombre del nodo al que el RR pertenece
 - TYPE – Contiene el código del RR
 - CLASS – Contiene la clase del RR (IN para Internet)
 - TTL – Contiene el tiempo de vida de RR en segundos
 - RDLENGTH – Contiene la longitud de la sección RDATA
 - RDATA – Contiene los datos correspondientes al RR, el formato varía según el tipo de RR



Inserción de registros en DNS

- Ejemplo: Recién se crea una empresa “Novatech”
- Debemos registrar el nombre Novatech.com en un **administrador de dominio** (e.g., Network Solutions)
 - Necesitamos proveer el nombre y la dirección IP de nuestro servidor de nombre autorizado (primario y secundario)
 - El administrador del dominio inserta dos RRs en el servidor TLD com:
 - (Novatech.com, dns1. Novatech.com, NS)
 - (dns1.Novatech.com, 200.0.0.254, A)
- Incorporar en el servidor autorizado un registro tipo A para www.Novatech.com y un registro tipo MX para novatech.com
 - (www.Novatech.com, 200.0.0.253, A)
 - (Novatech.com, email.Novatech.com, MX)
- En Perú debemos acceder al portal <https://punto.pe/> para arrendar un nombre de dominio.

SERVICIO DE DOMINIOS EN EL PERU

The screenshot shows a web browser window with the following details:

- Tab Bar:** .pe Punto Pe - Dominios en el Perú | Los 20 años de Internet en el Perú | +
- Address Bar:** https://www.nic.pe/search.php?dom_ini=redes.edu.pe
- Search Results:** Diccionario de la lengua... English to Spanish Tra... The Object of the Pre... Direct Object Pronouns Direct Object English Grammar: Dire...
- Header:** .pe Acerca de Punto.pe Tarifas y formas de pago Ayuda Contáctanos Whois INGRESA Carrito
- Search Form:** Encuentra tu dominio
- Text:** .pe, .com.pe, .org.pe, .net.pe, .nom.pe, .edu.pe, .mil.pe, .gob.pe
- Message:** ¡Tu dominio está libre!
- Important Note:** **IMPORTANTE:** Los dominios edu.pe, mil.pe y gob.pe son dominios de carácter restringido para instituciones educativas, militares y gobierno peruano. El control de dicho registro es expost. Antes de registrar por favor leer las Nuevas Políticas para el Registro de Nombres de Dominios Peruanos .PE y el Contrato de Servicio de Registro de Nombres de Dominio .pe.
- Domain Selection:** Escoge tu dominio:
 redes.edu.pe
 redes.nom.pe
 redes.net.pe
- Text:** Quiero un **.edu.pe**, **.gob.pe** y/o un **.mil.pe** (Dominios restringidos)
- Button:** Agregar al carrito de compras
- Table:** Tarifas a precio de lista

Periodo	Precio
1 año	\$/.110
2 años	\$/.200
3 años	\$/.295
4 años	\$/.385
5 años	\$/.465

- Notes:**
 - * Los precios incluyen impuestos.
 - * Los precios están indicados en nuevos soles.
 - * El costo de Cambio de Titularidad es equivalente a 1 año de registro.

SERVICIO DE DOMINIOS EN EL PERU

Encuentra tu dominio .pe, .com.pe, .org.pe, .net.pe, .nom.pe, .edu.pe, .mil.pe, .gob.pe

Lo sentimos, uandina.edu.pe ya ha sido registrado

¡Pero tienes estos dominios disponibles!

IMPORTANTE: Los dominios edu.pe, mil.pe y gob.pe son dominios de carácter restringido para instituciones educativas, militares y gobierno peruano. El control de dicho registro es expost. Antes de registrar por favor leer las Nuevas Políticas para el Registro de Nombres de Dominios Peruanos .PE y el Contrato de Servicio de Registro de Nombres de Dominio .pe.

Escoge tu dominio:

uandina.pe
 uandina.org.pe
 uandina.nom.pe
 uandina.net.pe
 uandina.com.pe

Quiero un .edu.pe, .gob.pe y/o un .mil.pe (Dominios restringidos)

SERVICIO DE DOMINIOS EN EL PERU

The screenshot shows the homepage of the yachay.lat website. At the top, there is a navigation bar with links for 'Dominios', 'Hosting', 'Correo', 'Empresas', a shopping cart icon with '0' items, and a user account icon. Below the navigation bar, a large banner features a woman smiling and the text 'Proyecta tu negocio en grande'. To the left of the banner, there is a call-to-action text 'Crea tu tienda online ¡hoy mismo!' and a search bar with the placeholder 'ej. example.com' and a 'Buscar' button. At the bottom of the page, there are several price boxes for different domain extensions: '.pe' S/103.00 Soles, '.com.pe' S/103.00 Soles, '.com' S/52.69 Soles, '.co' S/131.87 Soles, '.lat' S/131.87 Soles, '.io' S/258.72 Soles, '.net' S/66.98 Soles, and '.org' S/68.52 Soles. A link 'Ver todos los precios' is located at the bottom center.

SERVICIO DE DOMINIOS EN EL PERU



Acerca de Punto.pe

Desde sus inicios, el .pe ha sido administrado por la Red Científica Peruana, institución que ha desempeñado por más de 29 años la función de Network Information Center en el Perú. A través de su gestión, el .pe ha logrado preservar la estabilidad de los dominios peruanos y la operatividad de Internet, así como obtener una mayor representación digital de las comunidades peruanas en el escenario global.

El .pe es responsable de garantizar el normal funcionamiento de los elementos técnicos del DNS, de manera que los usuarios de Internet puedan validar correctamente las direcciones de sus dominios. Para ello se encarga de delegar los nombres de dominios de segundo y tercer nivel y supervisar la distribución de identificadores técnicos usados en las operaciones de Internet.

[Historia del NIC.PE](#)
[Política de registro](#)
[Normas y procedimientos](#)
[Tarifas y formas de pago](#)
[Comercializadores](#)
[Contáctanos](#)

Comercializadores

¿Quieres ser un comercializador de Punto.pe?

[Regístrate aquí](#)

Periodo	.com.pe	.pe	nom.pe net.pe org.pe	edu.pe gob.pe mil.pe
1 año	S/ 110	S/ 110	S/ 20	S/ 110
2 años	S/ 200	S/ 200	S/ 36	S/ 200
3 años	S/ 295	S/ 295	S/ 54	S/ 295
4 años	S/ 385	S/ 385	S/ 70	S/ 385
5 años	S/ 465	S/ 465	S/ 85	S/ 465

REFERENCIAS

- Annieahujaweb2020. “*DNS Message Format*”. <https://www.geeksforgeeks.org/dns-message-format/>
- Carson. “*DNS Message – How to Read Query and Response Message*”. <https://cabulous.medium.com/dns-message-how-to-read-query-and-response-message-cfebcb4fe817>
- Cloudflare Inc. “*What is DNS? | How DNS Works*”. <https://www.cloudflare.com/es-es/learning/dns/what-is-dns/>
- Cloudflare Inc. “*Understanding How Facebook Disappeared from the Internet*”. <https://blog.cloudflare.com/october-2021-facebook-outage/>
- ISC. “*Mapa de servidores DNS en el mundo*”. <https://atlas-vis.isc.org>.
- J. Carlos. “*Formato de un Mensaje DNS*”. <https://www.zeppelinlinux.es/formato-de-un-mensaje-dns/>
- Nslookup.io. “*DNS Record Types*”. <https://www.nslookup.io/learning/dns-record-types/>
- RFC 1035 – “*Domain Names – Implementation and specifications*”. <https://www.ietf.org/rfc/rfc1035.txt>.
- Teamques10. “*Explain DNS Message Format with Neat Diagram*”. <https://www.zeppelinlinux.es/formato-de-un-mensaje-dns/>