# LLIÇÓ 01
# DNS PROTOCOL

**TEORIA**

## INTRODUCCIÓ

A una xarxa TCP/IP els nodes s'identifiquen mitjançant una adreça IP. Recordar números IP a una xarxa petita pot ser una tasca senzilla, no obstant això, la tasca es complica quan el número de nodes creix. Per tant, es fa necessari implementar un mecanisme en "llenguatge humà" que permeti a l'usuari identificar d'una manera més natural els nodes, aquest mecanisme consisteix en utilitzar un nom per identificar al node. Per al esser humà:

- Resulta molt més fàcil recordar un nom que una adreça IP.
- El nom és un mecanisme més fiable, ja que la adreça IP pot canviar.

## SISTEMA DE NOMS PLÀ

La primera solució aportada per assignar noms als nodes, va consistir en utilitzar un sistema de noms pla. Aquest sistema consistia en distribuir un fitxer de text entre els nodes a partir d'una copia central que es mantenia a un del nodes.

Aquest fitxer s'anomena hosts i descriu cada host amb la seva corresponent adreça IP, a més a més permet definir alies. Es pot trobar a:

| Sistema | Ubicació fitxer hosts |
|---|---|
| Linux | /etc/hosts |
| Windows | /Windows/system32/drivers/etc/hosts |

Exemple fitxer hosts

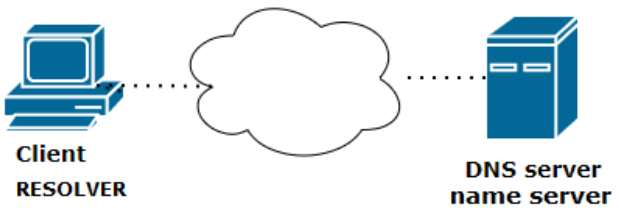
```
[root@pc~]# cat /etc/hosts
127.0.0.1    localhost
::1          localhost
192.168.1.1  router
192.168.1.31 server escriptori pare
192.168.1.32 pc01   dormitori  mare
192.168.1.33 pc02   nen        jocs
```

Es pot usar pera a definir nodes en xarxes petites, però no és escalable a xarxes gran i molt menys a Internet.

## DOMAIN NAME SYSTEM

### DEFINICIÓ

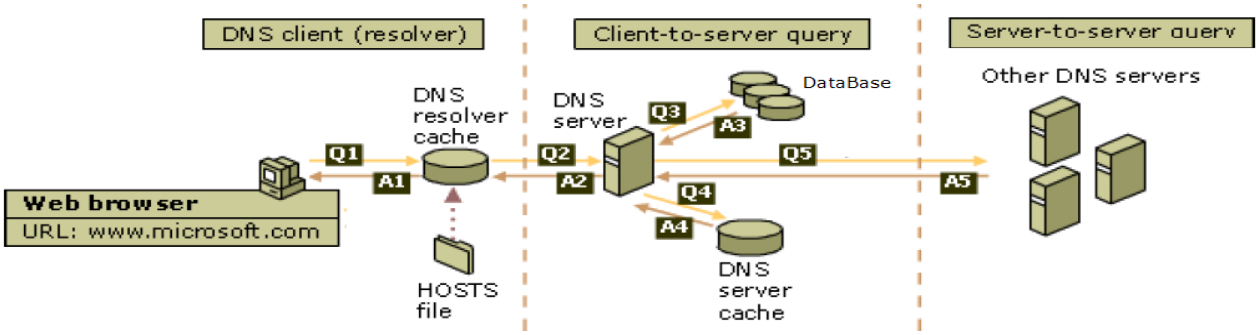
El 1983 sorgeix el protocol Domain Name System (**DNS**) per aportar una solució escalable i pràctica. DNS es un protocol del nivell d'aplicació que segueix el model client-servidor.



**DNS server** software que manté una base de dades de noms i respon a les consultes dels clients i d'altres servidors DNS. A les maquines que tenen instal·lat aquest software se les anomena **name server**. El servidors DNS tenen memòries cache per emmagatzemar les consultes mes habituals i millorar el temps de resposta.

Alguns servidors DNS son: BIND, DNSMasq, NSD, Microsoft DNS, Power DNS, Simple DNS plus, Knot DNS, Mara DNS,...

**Resolver** software a la maquina client que realitza consultes a un servidor. Con que el servidors DNS podem fer-se consultes entre sí, moltes vegades s'implementa com un servidor DNS. Al sistemes operatius es tracta de un servei en execució que respon a les consultes dels altres programes.



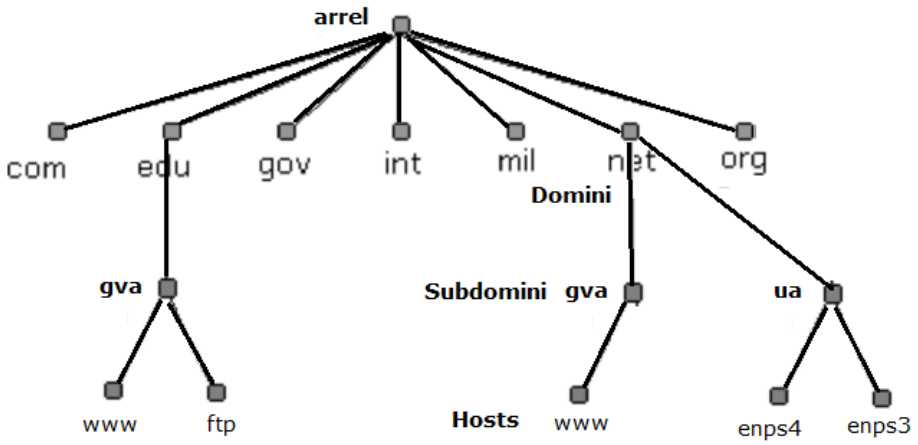

A DNS no solament es pot fer la resolució de noms a adreces IP, sinó també la resolució inversa, es a dir, a partir d'una IP esbrinar el nom.

DNS està definit a les RFC 1034, 1035 i 1886 (IPv6) i utilitza els següents ports.

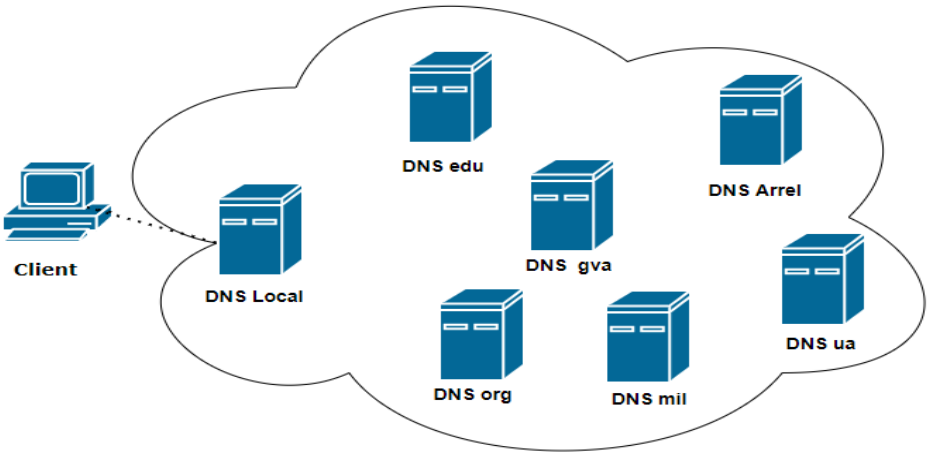
| | Protocol | Servidor port | Client port |
|---|---|---|---|
| Resolució de nom | UDP | 53 | Efímer |
| Resolució de nom > 512 bytes | TCP | 53 | Efímer |
| Transferències entre servidors | TCP | 53 | Efímer |

**DNS es basa en una base de dades distribuïda que defineix un espai jeràrquic de noms de domini**.

- **Jeràrquic.** S'organitza en forma de arbre, començant per un domini arrel que es subdivideix en subdominis que també es poden tornar a dividir. Es podem fer fins a 127 nivells.



- **Distribuïda.** La informació per la definició de aquest arbre no és a un repositori central sinó que es troba repartida per parts entre diferents servidors DNS**.**




- **Nom de Domini.** Nom que se assigna a cada node del arbre. Cada nom pot tindre como a màxim 63 caràcters sense distingir majúscules i minúscules. No es pot repetir dintre del mateix nivell d'un arbre (nodes germans). Per construir el nom d'un node del arbre es separa cada nom per un punt "." El nom total des de una fulla pot tindre 255 caràcters com a màxim.

| | |
|---|---|
| **Arrel** | El seu nom de domini es la cadena buida. |
| **Nom absolut** | **FQDN** Full qualified domain name.<br>Es el nom de un node del arbre des de la seva posició al arbre fins al arrel, per tant, termina sempre en un punt. Aquest nom es únic per a tot l'espai de noms.<br>www.gva.edu.<br>www.gva.net.<br>gva.edu. |
| **Nom relatiu** | Es el nom de un node del arbre però sense arribar al arrel. Normalment se ha de completar via software per obtenir el nom absolut.<br>ftp<br>gva.edu |

- **Domini.** Nom que se assigna a cada node del arbre i tota la resta del sub-arbre que penja d'ell. Per al exemple anterior:
  Edu es un domini que conté el subdomini gva
  Net es un domini que conté dos subdominis gva i ua
  ua es un subdomini de Net que defineix les maquines enps3 i enps4

- **Delegació de dominis.** Mecanisme que permet descentralitzar l'administració de la base de dades DNS mitjançant la divisió del domini en subdominis, cedint el control de cada subdomini a un altre autoritat (altre servidor DNS) a condició de mantenir els registres de recursos del subdomini.

- **Espai de noms.** El domini arrel i tots el seus subdominis.

## DOMINI ARREL

Hi ha 13 servidors DNS arrel a tot Internet. Això no vol dir que hi hagi 13 servidors físics, cada operador utilitza equips redundants per oferir un servei fiable. A més a més en la actualitat s'utilitza també el adreçament anycast per accedir al servidors arrels. El noms del servidors arrels són de la forma **lletra.root-servers.net**. Així el seus noms i adreces actuals son:

| Lletra | IPv4 | ubicació |
|---|---|---|
| A | 198.41.0.4 | Distribuït, anycast |
| B | 192.228.79.201 | Marina del Rey – California - US |
| C | 192.33.4.12 | Distribuït, anycast |
| D | 199.7.91.13 | College park – Maryland - US |
| E | 192.203.230.10 | Mountain View – California - US |
| F | 192.5.5.241 | Distribuït, anycast |
| G | 192.112.36.4 | Distribuït, Anycast |
| H | 128.63.2.53 | Aberdeen – Maryland - US |
| I | 192.36.148.17 | Distribuït, Anycast |
| J | 192.58.128.30 | Distribuït, Anycast |
| K | 193.0.14.129 | Distribuït, Anycast |
| L | 199.7.83.42 | Distribuït, Anycast |
| M | 202.12.27.33 | Distribuït, Anycast |

Podeu consultar la distribució i redundància dels servidors arrels a tot el món al següent enllaç root-servers

Cadascú d'aquest servidors guarden una copia de la zona de definició dels dominis de primer nivell o **TLD** (Top Level Domain). Aquesta zona TLD es definida por la ICANN però es controlada per el Departament de Comerç dels Estats Units.

La ICANN distingeix actualment el següents grups per els TLD.

- **ccTLD** country code TLD (dos caràcters)
  Identifiquen els països. Alguns exemples son: es, fr, dk, de, jp, it
  Ací pots consultar una llista mes ampla: ccTLD
- **gTLD** genèric TLD (tres o més caràcters)
  - sTLD sponsored TLD
    Exemples: edu, gov, jobs, museum, cat, ...
    Ací pots consultar una llista mes ampla: sTLD
  - uTLD unsponsored TLD
    Exemples: hoteles,
- **.arpa**
  Utilitzat per la ICANN per la seua pròpia infraestructura.

Podeu consultar la definició de la llista de servidors arrels i de la zona arrel als següents enllaços:

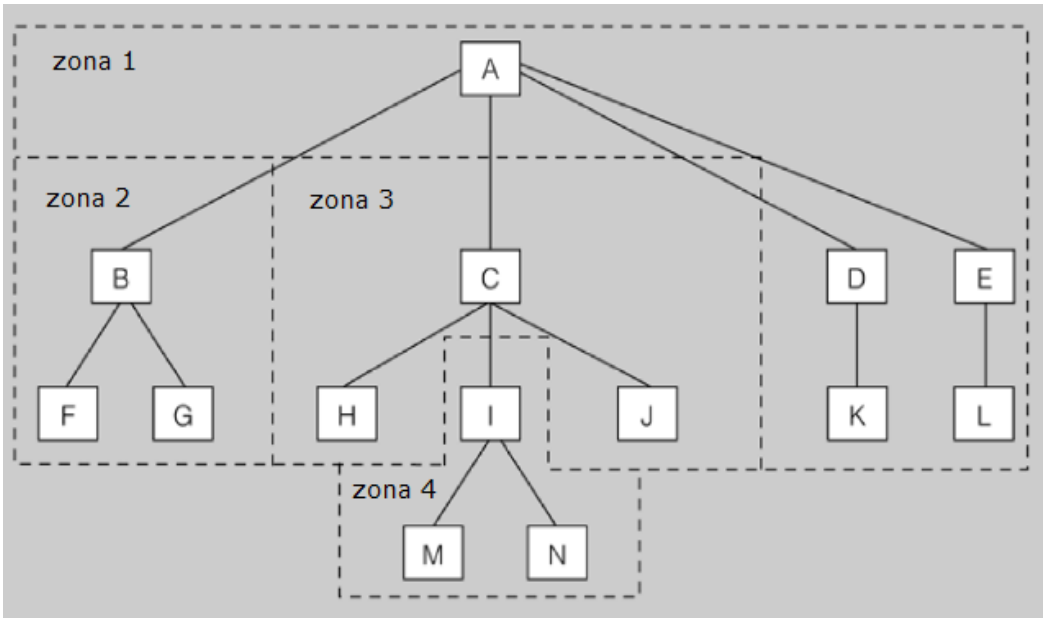
Llista de servidors arrels. (root hints zone)
TLD definits als servidors arrels (root zone)

# BASE DE DADES

## ZONA

Cada servidor DNS manté en la seva base de dades la informació d'una **part de l'espai de noms** anomenada **zona**. Una zona pot coincidir con un domini però no es necessari. Els servidors que gestionen la zona tenen informació completa sobre la zona i es diu que tenen **autoritat** respecte a ella. Un servidor DNS pot definir una o més zones, a més a mes una zona pot ser gestionada per mes de un servidor DNS. Un servidor DNS pot delegar l'administració de un part de la seva zona a altres servidors DNS, en aquest cas perd la autoritat sobre la zona delegada però pot recuperar la informació a partir dels DNS delegats.

Al exemple es pot veure un espai de noms amb quatre zones i catorze dominis.




A la especificació de la base de dades al servidor DNS hi hauran al menys els següents fitxers de zona:

- Zona de resolució directa

  Aquesta zona manté les associacions del noms de domini a adreces IP.
- Zona de resolució inversa.

  Aquesta zona manté les associacions de cada adreça IP amb el seu nom de domini canònic.
- Zona de resolució inversa de la adreça de loopback.

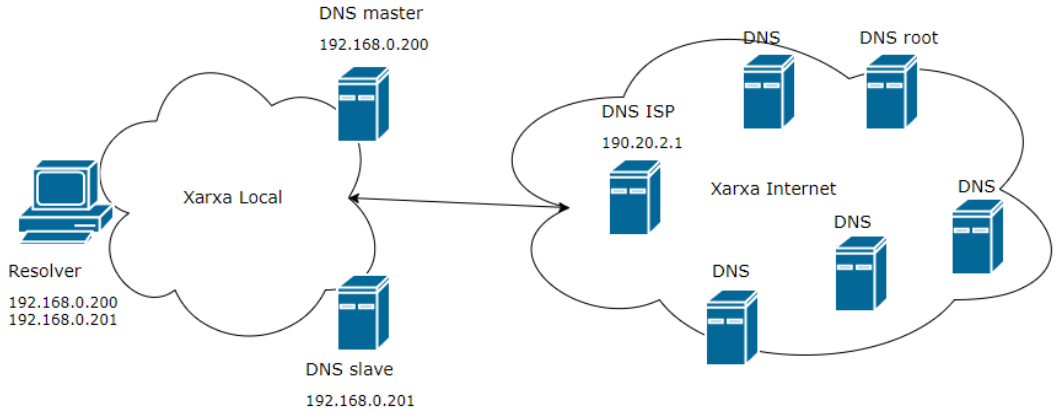
  Aquesta zona manté la traducció inversa de les adreces de loopback.
- Zona root.

  Aquesta zona manté les adreces dels nodes DNS arrels.

La forma en que un servidor defineix les seves zones a la base de dades varia d'un tipus de servidor a altre.

## Exemple configuració de zones a BIND9

Utilitzaren el següent exemple per la configuració.




La configuració del servei (named) i les zones es fan al fitxer /etc/bind/named.conf.

Normalment no es modifica el fitxer per introduir les noves zones i opcions. Per això s'utilitzen el fitxers que hi ha sota la directiva include.

| | |
|---|---|
| named.conf.options | Opcions globals de configuració |
| named.conf.local | zones noves definides |

Com es pot veure a la imatge hi ha zones per defecte definides que no cal modificar.

```
include "/etc/bind/named.conf.options";

# Be authoritative for the localhost forward and
# broadcast zones as per RFC 1912.
zone "."{
         type hint;
        //Tipus servidor definit per a zona cache
         file "/etc/bind/db.root";};
zone "localhost."
{
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa."
{
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa."
{
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa."
{
        type master;
        file "/etc/bind/db.255";
};

include "/etc/bind/named.conf.local";
```

A BIND9 es poden definir zones de diversos tipus:

| | |
|---|---|
| Master | Es una zona autoritativa. Es a dir, a aquesta zona es defineixen els registres que associen noms e IP i a la inversa |
| Slave | Es tracta d'una copia completa d'una zona autoritativa. |
| Stub | Es tracta d'una copia parcial d'una zona autoritativa. |
| Forward | Es tracta de una zona en la que no hi ha definició sinó que les consultes se reenvien a altres servidors. |
| Hint | Es tracta de la zona on som definits els servidors arrels |

* A les zones master i slave se les anomenava abans primària i secundària respectivament.

A més a més es podem utilitzar diferents opcions globals per modificar el comportament del servidor per exemple:

| | |
|---|---|
| Listen-on | Especifica la IP on el servei escolta les peticions. |
| Forwarders | Especifica la IP dels servidors DNS al que es farà un reenviament sinó s'aconsegueix resoldre localment la consulta |
| acl | Especifica una llista de IPs per complir una condició.<br>Exemple acl redies {192.168.0/24;}. |

Per definir una zona s'utilitza la següent estructura, encara que pot tindre mes opcions.

```
zone "<domini FQDN>" {
     type (master,slave,stub,forward,hint);
     file   "fitxer-definicio-registres";
};
```

```
master directa  node 192.168.0.200
zone "ies.com" {
  type master;
  file "/etc/bind/ies.com.db";
  allow-transfer {192.168.0.201;};
};
```

```
master inversa node 192.168.0.200
zone "0.168.192.in-addr.arpa"{
type master;
file "/etc/bind/0.168.192.db";
allow-transfer {192.168.0.201;};
};
```

```
slave directa node 192.168.0.201
zone "ies.com" {
   type slave
   file "/etc/bind/ies.com.db";
   masters {192.168.0.200;};
```

```
slave inversa node 192.168.0.201
zone "0.168.192.in-addr.arpa"{
type slave;
file "/etc/bind/0.168.192.db";
masters {192.168.0.200;};
};
```

Forwarding s'ha de fer als dos servidors a les opcions globals

```
forwarders {
      190.20.2.1;
};
```

En aquest cas no hem utilitzat una zona tipus forward ja que el que es vol es que qualsevol consulta que no pugi resoldre amb autoritat per el servidor es reenviï al servidor DNS del ISP.

## REGISTRES

La base de dades que defineix una zona es basa en diferents tipus de registres de recursos (RR). Per a la seva definició s'utilitza el següent format.

**<propietari> <classe> [ttl] <tipus> rdata**

| | |
|---|---|
| **Propietari** | Nom del domini que s'està definit |
| **Classe** | IN – Internet |
| **TTL** | Opcional. Indica el temps de vida de aquest registre a cache.<br>Es pot expressar dies (d), hores (h), minuts (m) o segons (s).<br>Si conté un 0 indica que no es té que emmagatzemat a cache.<br>Exemples: 4h40m , 2300 (no indica res, per tant segons). |
| **TIPUS** | Tipus de registre |

| | |
|---|---|
| SOA | Identifica al servidor com autoritari d'una zona i permet definir els seus paràmetres de configuració |
| NS | Identifica el servidors de noms autoritzats per la zona |
| A | Associa un nom FQDN a una adreça IPv4 |
| AAAA | Associa un nom FQDN a una adreça IPV6 |
| PTR | Associa una adreça IP a un nom FQDN |
| MX | Indica els servidors de correu definits a la zona |
| CNAME | Permet assignar un àlies a un nom canònic |
| TXT | Registre per emmagatzemar qualsevol informació |
| SRV | Ubicació dels servidors per a un servei. |
| HINFO | Informació sobre el tipus de host |
| MB | Informació sobre una bústia de correu |
| MG | Informació sobre un grup de correu |
| WKS | Llista de serveis del host |
| NULL | Registre buit |

| | |
|---|---|
| **RDATA** | valor associat al registre |

Al fitxers de definició de registres de la zona es podem usar les següents directives.

- $ORIGIN defineix el nom base a partir del qual es formen el noms FQDN per els noms relatius. Si no hi es, aleshores es fa $ORIGIN=nom de la zona.
- $TTL defineix el temps per defecte per guardar un registre a la cache, sinó se ha especificat al propi registre. Si no se indica el seu valor per defecte es de 1 h.

L'estàndard DNS permet fer abreviacions en els fitxers de definició de zona per tal de facilitar-ne la sintaxi. Les més importants són:

- @ per utilitzar el valor de $ORIGIN.
- El espai en blanc per indicar que es repeteix el valor del registre anterior.
- Als noms de domini relatius (no acabats en punt) se'ls afegeix automàticament $ORIGIN per formar un nom FQDN.

**SOA**

El registre de recurs SOA o start of authority (inici de definició de zona amb autoritat) diu que el fitxer de zona on es troba és la millor font de dades per a la zona, que el servidor de noms és autoritari per a la zona. Acostuma a ser el primer RR que hi ha en el fitxer de zona, tot i que no és obligatori. Per cada fitxer de zona hi ha d'haver només un registre SOA. Un registre SOA té el format:

NAME. IN SOA MNAME. RNAME. (OPCIONS-SLAVES)

| | |
|---|---|
| NAME. | nom FQDN de domini de la zona |
| IN | classe del registre Internet |
| SOA | tipus de registre SOA |
| MNAME. | nom FQDN del host que defineix la zona master |
| RNAME. | email FQDN del administrador de la zona. La @ es substitueix per un "." |
| OPCIONS-SLAVES | Paràmetres per a definir la comunicació entre les zones master i slave. |
| SERIAL | Número de sèrie de la versió de les dades. A cada canvi de les dades el número s'incrementa. Les zones slaves actualitzaran el seus registres quan el seu número serial sigui menor al de la zona master. Una forma de construir aquest número es amb el format yyyymmddnn, per exemple, 2022120601 para el primer canvi del dia 06/12/2022. |
| REFRESH | Indica cada quant de temps la zona slave ha de consultar la zona master per comprovar els canvis i actualitzar-se. |
| RETRY | Indica el temps de espera per tornar a fer un "refresh" després de haver fallat. |
| EXPIRE | Indica el temps de caducitat de la zona slave. Si no se ha refrescat abans la zona slave es considera sense autoritat. |
| NXDOMAIN TTL | Temps de validesa a la cache del missatge NXDOMAIN. Aquest missatge es rep quan no se ha pogut resoldre una consulta. |

*El temps es pot definir en segons (opció per defecte) o amb els caràcters especials W-week, D-day, H-hour, M-minute, S-seconds

Exemple

```
ies.com. IN SOA nsmaster.ies.com. admin.nsmaster.ies.com.
(2022120601    ;serial number
      10800    ;refresh          3H
        900    ;retry            15M
     604800    ;expire           1W
      86400    ;NXDOMAIN TTL     1D
)
```

**NS**

El registre de recurs NS o name server (servidor de noms) defineix un servidor de noms autoritatiu per a la zona. Hi haurà tantes entrades NS com servidors de noms autoritatius hi ha en la zona. L'estàndard DNS en recomana almenys dos (un de primari o master i un de seguretat secundari o slave). Un registre NS te el següent format:

NAME. IN NS MNAME.

| | |
|---|---|
| NAME. | nom FQDN de domini de la zona |
| IN | classe del registre Internet |
| NS | tipus de registre NS |
| MNAME. | nom FQDN del host servidor |

Exemple

```
ies.com. IN NS nsmaster.ies.com.
ies.com. IN NS nsslave.ies.com.
```

**A**

Un registre de recurs A o address (adreça) associa un nom de host a una adreça IP (resolució directa). Per cada nom de host de la xarxa caldrà disposar d'una entrada on s'associï el nom del host a la seva adreça IP. Un host pot tindre més de una IP associada al seu nom (multi-homed).

Els noms definits en els registres de tipus A són noms canònics. Un host es pot identificar per més d'un nom, però només un és el nom canònic (original), la resta són àlies. Els noms canònics es defineixen amb el tipus de registre A. Els àlies es defineixen amb el tipus de registre CNAME.

Un registre A te el següent format:

NAME. IN A IP

| | |
|---|---|
| NAME. | nom FQDN |
| IN | classe del registre Internet |
| A | tipus de registre A |
| IP | IP associada al nom |

Exemple

```
nsmaster.ies.com. IN A 192.168.0.200
nsslave.ies.com.  IN A 192.168.0.201
pc1.ies.com. IN A 192.168.0.1
pc1.ies.com. IN A 192.168.0.10
pc2.ies.com. IN A 192.168.0.2
```

**CNAME**

Els registres de recurs CNAME o canonical name (nom canònic) associen un àlies a un nom canònic. Un registre CNAME consta dels camps:

NAME. IN CNAME CANONICALNAME | IP

| | |
|---|---|
| NAME. | nom FQDN del alies |
| IN | classe del registre Internet |
| CNAME | tipus de registre CNAME |

| | |
|---|---|
| CANONICALNAME | nom canonical definit a un registre A |
| IP | En lloc de un nom canonical es pot utilitzar la IP del registre A, això serveix per diferenciar aquells registres A de tipus multi-homed. |

Exemple

```
nsprimary.ies.com.    IN CNAME nsmaster.ies.com.
nssecondary.ies.com. IN CNAME nsslave.ies.com.
contable.ies.com.     IN CNAME 192.168.0.1  ;alies per IP en un A multi-homed
```

**PTR**

Un registre de recurs PTR o pointer (punter) associa una adreça IP al nom de host pertinent (resolució inversa). Cal una entrada PTR per a cada interfície de xarxa de la zona. Un registre PTR consta dels camps:

IPINVERSA.IN-ADDR.ARPA. IN PTR CANONICALNAME

| | |
|---|---|
| IPINVERSA | Es tracta de invertir el bytes de la IP, per exemple, la 192.168.0.1 de forma inversa seria 1.0.168.192 |
| IN-ADDR.ARPA. | Identifica la IP como inversa. |
| IN | classe del registre Internet |
| PTR | tipus de registre PTR |
| CANONICALNAME | nom canonical definit a un registre A |

Exemple

```
200.0.168.192.IN-ADDR.ARPA. IN PTR nsmaster.ies.com.
201.0.168.192.IN-ADDR.ARPA. IN PTR nsslave.ies.com.
1.0.168.192.IN-ADDR.ARPA. IN PTR pc1.ies.com.
10.0.168.192.IN-ADDR.ARPA. IN PTR pc1.ies.com.
2.0.168.192.IN-ADDR.ARPA. IN PTR pc2.ies.com.
```

**MX**

Un registre MX mail exchanger (servidor de correu electrònic) defineix un servidor de correu. Es pot posar una entrada MX per a cada servidor de correu, però no és obligatori que n'hi hagi cap. Aquest registres s'utilitzen en les consultes dels servidors de correus. El programari del servidor de correu (MTA) s'encarrega de consultar els registres MX. Quan un usuari envia un correu electrònic, l'MTA envia una consulta de DNS per identificar els servidors de correu dels destinataris del correu. L'MTA estableix una connexió SMTP amb aquests servidors de correu, segons la seua prioritat. Un registre MX consta dels camps:

NAME. IN MX NUM MAILSERVER

| | |
|---|---|
| NAME. | nom canonical definit a un registre A. |
| IN | classe del registre Internet |
| MX | tipus de registre MX |
| NUM | Número de prioritat con respecte a altres servidor MX definits. El menor valor es el més prioritari. |
| MAILSERVER | Nom FQDN del servidor de correu |

Exemple

```
ies.com. IN MX 10 mail.ies.com.
mail.ies.com. IN A 192.168.0.220
```

Un correu enviat per exemple a usuario@ies.com establirà connexió SMTP amb el servidor de correu mail.ies.com. que es troba a la adreça 192.168.0.200

**SRV**

Un registre SRV (servei) especifica els servidors disponibles per fer un servei o protocol determinat. Un registre SRV consta dels camps:

SERVEI.PROTOCOL.NAME. IN SRV PRIORITAT PES PORT CANONICALNAME

| | |
|---|---|
| SERVEI | nom del servei: ftp, http, ssh, … |
| PROTOCOL | TCP o UDP |
| IN | classe del registre Internet |
| SRV | SRV |
| PRIORITAT | Ordre en el que es client es posaran en contacte. Major prioritat el número mes baix. |
| PES | Mecanisme de balanceig de carrega. |
| PORT | Port de servei |
| CANONICALNAME | nom canonical definit a un registre A |

Exemple

```
ftp.tcp.ies.com.  IN SRV 0 0 21 ftp.ies.com.
http.tcp.ies.com. IN SRV 0 0 80 http.ies.com.
ftp.ies.com.  IN A 192.168.230
http.ies.com. IN A 192.168.231
```

## TIPUS DE SERVIDORS

En funció de com el servidor te configurades les seves zones i opcions globals podem trobar el següents tipus de servidors.

| | |
|---|---|
| **Master** | El servidor te definida una zona de tipus master sobre la que te autoritat. També se l'anomena primari. |
| **Slave** | El servidor te definida una zona de tipus slave sobre la que te autoritat. També se l'anomena secundari. |
| **Forwarder** | El servidor te definida alguna zona i per les consultes que no son de la seues zones reenvia les sol·licituds a altres servidors i guarda les respostes a la seua memòria cache. |
| **Forwarder caché** | El servidor no te definida cap zona i solament fa reenviaments a altres servidors i guarda les respostes a la seua memòria cache. |

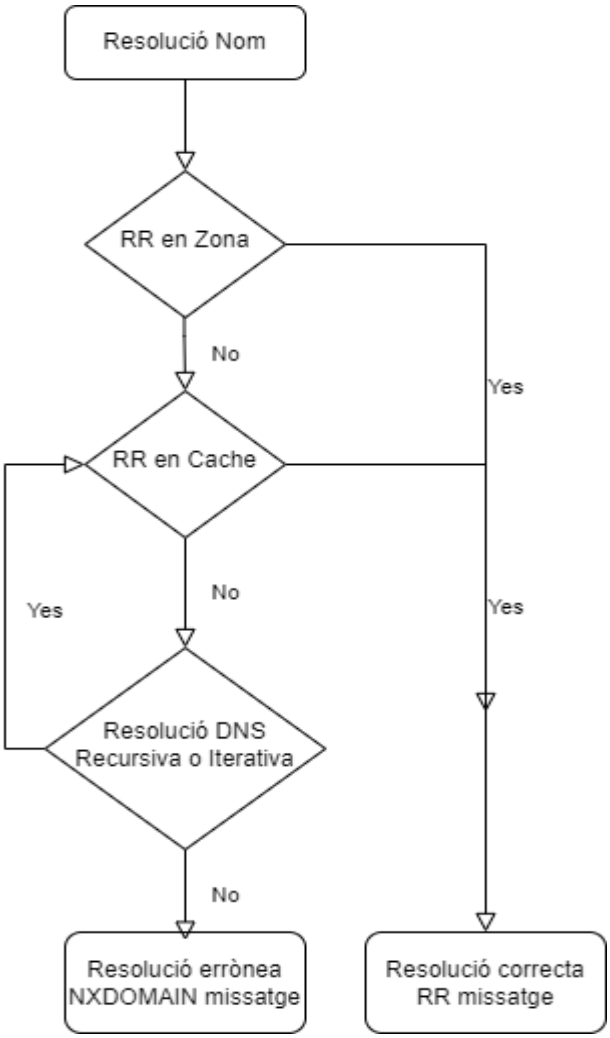
Cal dir que un servidor pot ser master per una zona, slave para altra zona i al mateix temps pot ser de tipus forwarder per a la resta de peticions.

## CONSULTES

Les consultes DNS per la resolució de noms de domini podem ser de dos tipus: recursives o iteratives.

A gran mode, el procés de resolució d'un nom a un servidor DNS seguirà els següents passos:

1. El servidor consultarà les seves zones per trobar un registre com a resposta a la consulta. Si el troba la seva resposta serà autoritativa. Si no el troba anirà al pas 2.
2. El servidor consultarà la seva memòria cache per trobar un registre com resposta a la consulta. Si el troba la seva resposta serà no autoritativa. Si no el troba anirà al pas 3.
3. El servidor reenviarà la consulta a altres servidors DNS de forma recursiva o iterativa. Si rep una resposta la emmagatzemarà a la memòria cache i respondrà de forma no autoritativa. Si no rep cap resposta a les hores no es pot resoldre el nom i tornarà un missatge de error NXDOMAIN.




### RECURSIVA

En les consultes recursives el servidor DNS ha de tornar una resposta, es ha dir, o respon amb el RR que resol la consulta o amb un missatge d'error.

Si el servidor DNS no sap inicialment la resposta perquè no hi es a la seva zona o a la seva cache, haurà de consultar a altres servidor DNS per tractar de resoldre-la.

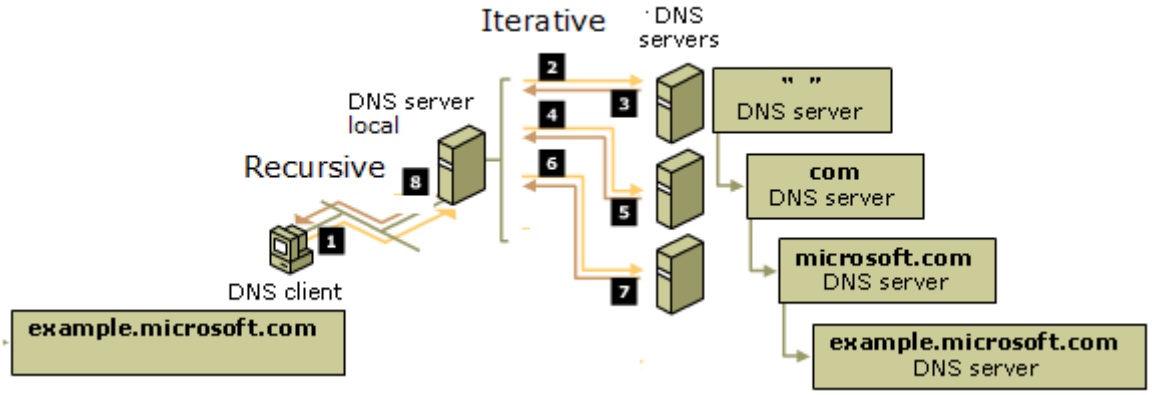
Este tipus de consultes es solen produir entre els clients resolvers i els DNS locals, com per exemple el DNS de un ISP o un altre servidor DNS de la seva xarxa. També es sol utilitzar entre un servidor DNS i el seus servidors DNS forwarders.

### ITERATIVA

En les consultes iteratives el servidor DNS proporciona la millor resposta que té, aquesta resposta pot ser la solució a la consulta o una referencia a un altre servidor DNS de nivell inferior. Una vegada es rep la referencia a un servidor es torna a fer una consulta iterativa con aquest servidor.

Este tipus de consultes es solen produir entre servidors DNS. Quan un servidor no sap resoldre una consulta inicia una consulta iterativa amb el servidors DNS arrels, començant de aquest manera tot el procés iteratiu.

Exemple.




1 DNS client fa una consulta recursiva, per el nom example.microsft.com, a DNS local i es manté a la espera de una resposta.

2 DNS local no troba a les seves zones ni a l cache cap registre per a respondre a la consulta. Inicia el procés de iteració i fa una consulta iterativa a un servidor DNS arrel.

3 Es servidor DNS arrel contesta con la millor de les seues respostes, en aquest cas es .com i una llista de servidors per aquest domini. El servidor DNS local guarda en cache la resposta

4 DNS local fa una consulta iterativa a un servidor DNS de domini .com

5 El servidor DNS de domini .com contesta con la millor de les seues respostes, en aquest cas microsoft.com i una llista de servidors per aquest domini. El servidor DNS local guarda en cache la resposta

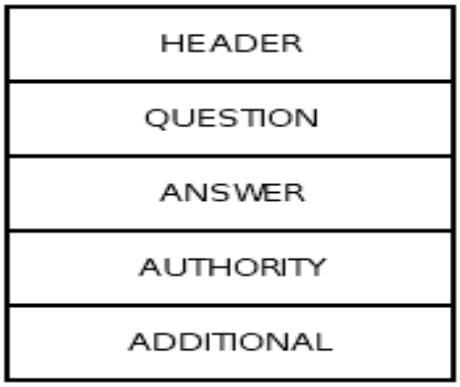
6 DNS local fa una consulta iterativa a un servidor DNS de domini microsoft.com

7 El servidor DNS de domini microsoft.com contesta con la millor de les seues respostes, en aquest cas es el registre de exemple.microsoft.com. El servidor DNS local guarda en cache la resposta i termina les iteracions.

8 El servidor DNS local respon al DNS client amb el registre que resol la consulta exemple.microsoft.com

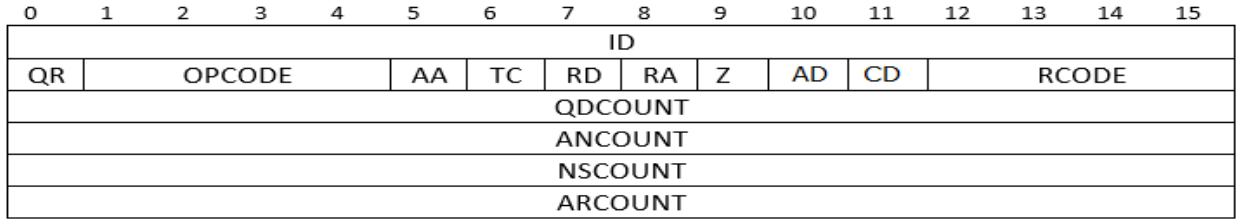
## MISSATGES

El missatges DNS s'utilitzen per les consultes de resolució de noms i el intercanvi de informació entre el servidors DNS. El seu format es el següent.



## HEADER

Es la capçalera del missatge. Te els següents camps.




**ID** 2 bytes**.** Número de identificació de la consulta.

**Flags** 2 bytes**.** Indican tota la informació sobre la consulta.

| Flag | Bit | | |
|---|---|---|---|
| QR | 0 | Tipus missatge | 0-query<br>1-response |
| OPCODE | 1-4 | Tipus consulta | 000 – standard query<br>001 – inverse query<br>010 – server status query<br>La resta de combinacions no s'utilitzen |
| AA | 5 | Bit autoritat | 0-non authoritative answer<br>1-authoritative answer |
| TC | 6 | Bit truncament | 0-message not truncated<br>1-Message truncated |
| RD | 7 | Bit recursivitat | 0-non recursive query<br>1-recursive query |
| RA | 8 | Bit recursivitat al servidor | 0-recursion not avaible<br>1-recursion avaible |
| Z | 9-11 | Bit reservat | 0-reserved |
| AD | 10 | Bit autenticació dades | 0-authority section was not authenticated<br>1-authority section was authenticated |
| CD | 11 | Bit autenticació obligatòria | 0-no authenticated data is acceptable for query<br>1-only authenticated data is acceptable for query |
| RCODE | 12-15 | Tipus resposta | 0000-no error<br>0100-format error in query<br>0010-server failure<br>0001-name does not exits |

**QDCount** 2 bytes. Número registres a la secció de preguntes.

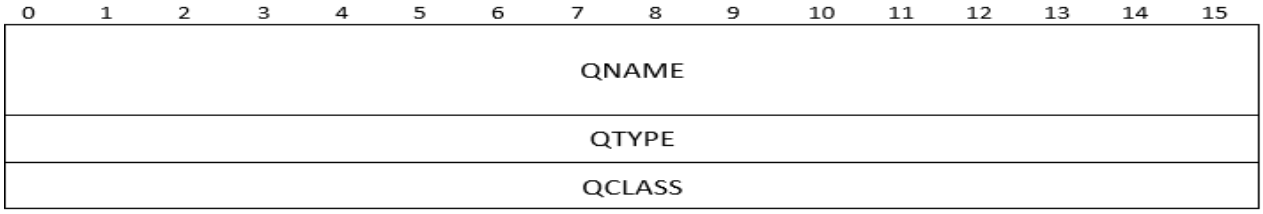
**ANCount** 2 bytes. Número registres a la secció de respostes.

**NSCount** 2 bytes. Número registres a la secció de autoritat.

**ARCount** 2 bytes. Número registres a la secció addicional.

### QUESTION

Pregunta que es fa al servidor DNS, te el següent format:




| | | |
|---|---|---|
| QNAME | n bytes | Nom de domini per el que es pregunta |
| QTYPE | 2 bytes | Tipus de registre |
| | <Type> | A, PTR, etc... |
| | AXFR | zona especial de transferència |
| | MAILB | tots els registres de mail |
| | * | qualsevol tipus |
| QCLASS | 2 bytes | Tipus de classe del registre |
| | <class> | IN, CH |
| | * | qualsevol classe |

### ANSWER

Registre o registres de la resposta.

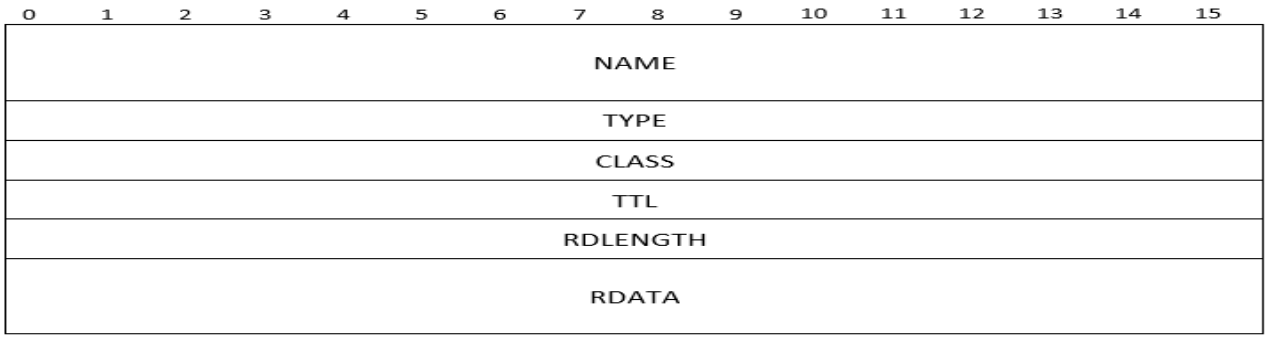
### AUTHORITY

Registre del servidors que tenen autoritat sobre la resposta.

### ADDITIONAL

Registres addicionals sobre la resposta.

Aquest 3 últims camps tenen el següent format.




| | | |
|---|---|---|
| NAME | n bytes | Nom del propietari del registre |
| TYPE | 2 bytes | Tipus de registre |
| CLASS | 2 bytes | Tipus de classe |
| TTL | 4 bytes | Temps de vida assignat al registre en segons |
| RDLENGTH | 2 bytes | Número de bytes del camp RDATA |
| RDATA | n bytes | Dades del registre |

Exemple de consulta DNS

```
[root@portatil ~]# host -a uoc.es
Trying "uoc.es"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14091
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;uoc.es.        IN  ANY

;; ANSWER SECTION:
uoc.es.     82747 IN  NS  tibet.uoc.es.
uoc.es.     82747 IN  NS  nepal.uoc.es.

;; AUTHORITY SECTION:
uoc.es.     82747 IN  NS  nepal.uoc.es.
uoc.es.     82747 IN  NS  tibet.uoc.es.

;; ADDITIONAL SECTION:
nepal.uoc.es.   73649 IN  A 213.73.40.47
tibet.uoc.es.   76582 IN  A 213.73.40.45

Received 124 bytes from 127.0.0.1#53 in 2 ms
```

## EVOLUCIÓ

Els protocols DNS han evolucionat molt gràcies a les noves necessitats provocades per l'increment exponencial de les xarxes. Una de les principals vies en evolució és el DDNS o dinàmic DNS i el DNSSEC o DNS segur.

### DDNS

El protocol DDNS (dynamic DNS) permet que les dades del servidor DNS s'actualitzin en temps real. El principal ús és permetre que clients amb adreces IP dinàmiques puguin disposar d'un nom de domini (a pesar que la seva adreça IP varia d'una sessió a una altra). Un mecanisme consisteix a permetre que els servidors DHCP es comuniquin amb els servidors DNS i els notifiquin les actualitzacions a la base de dades de DNS que cal fer.

### DNSSEC

El protocol DNS data de la dècada dels 80, una època on la funcionalitat estava per damunt de la seguretat. Els servidors DNS treballen amb bases de dades distribuïdes on emmagatzemen els registres amb la informació dels dominis i els seus IP, les transferències de zones i les consultes es fan en clar, es a dir, sense xifrar. Les deficiències de seguretat existents en aquest protocol ho fan susceptible de falsificació dels registres, amb els riscos consegüents de redirecció a llocs maliciosos i suplantació, entre d'altres.

Per donar solució a aquests problemes es va dissenyar DNSSEC (Domain Name System Security Extensions). **DNSSEC** afegeix una capa de seguretat addicional al protocol DNS que **permet comprovar la integritat y autenticitat de les dades.** Es basa en l'ús de la **criptografia asimètrica**. Cada servidor DNS te dues claus diferents, una pública que és transmesa a la resta de servidors i s'utilitza per a xifrar i una altra privada que només la coneix el servidor i que es utilitzada per a desxifrar.