Universitatea Politehnica București, Facultatea de Electronică Telecomunicații și Tehnologia Informației

Temă de casă - SOA

Serverul DNS - Linux

Profesor Coordonator: Aflorei Victor

Conf.dr.ing Ștefan Stăncescu Master IISC

Ianuarie 2015

# 

Cuprins

[1. Sistemul DNS (Domain Name System) 3](#_Toc411196232)

[1.1 Descriere generală 3](#_Toc411196233)

[1.2 Spațiul de nume DNS 4](#_Toc411196234)

[1.3. Servere DNS 5](#_Toc411196235)

[1.3.1. Zone DNS și rolul serverelor 5](#_Toc411196236)

[1.3.2. Tipuri de servere DNS asociate unei zone 6](#_Toc411196237)

[2. Clienţi DNS şi interogare 7](#_Toc411196238)

[2.1Cine sunt clienţii DNS 7](#_Toc411196239)

[2.2 Tipuri de interogări și scenarii de utilizare 8](#_Toc411196240)

[2.3. Rezoluția inversă 9](#_Toc411196241)

[3. Protocolul DNS 9](#_Toc411196242)

[4. Bibliografie 11](#_Toc411196243)

# 1. Sistemul DNS (Domain Name System)

## 1.1 Descriere generală

După cum știm, un protocol reprezintă un set de reguli prin care se poate realiza comunicare "pe aceeași limbă" între două calculatoare. Într-o rețea pot exista mai multe conversații, fiecare calculator putând "discuta" cu fiecare, și de aceea este necesară o identificare a fiecărui interlocutor din punctul de vedere al protocolului de comunicație folosit. De exemplu, într-o topologie broadcast, pe un același mediu fizic avem mai multe stații fiecare cu placa (sau plăcile!) ei de rețea, și implicit cu una sau mai multe entități MAC; modalitatea în care se face identificarea celor două capete ale schimbului de date este prin folosirea *adreselor fizice*.

De asemenea, la nivelul 3 OSI, pentru a face posibil schimbul de date între stații care nu se mai află în aceeași rețea, ci la distanță de câteva rețele interconectate, a fost nevoie de introducerea *adreselor logice*, ce formează, spre deosebire de cele fizice, un spațiu de adrese structurat, făcând astfel posibilă rutarea. Transmiterea unităților de date de nivel rețea se face apelând la serviciile nivelului legătură de date; acestuia trebuie să i se furnizeze o adresă fizică pentru a putea ști către cine să trimită datele în cauză. De aici necesitatea de *rezolvare a unei adrese logice în adresă fizică*. Un astfel de exemplu este funcția îndeplinită de protocolul ARP din stiva TCP/IP, care "traduce" din adrese IP în adrese MAC.

Dacă lucrurile s-ar fi oprit aici, în ziua de azi am scrie 64.58.76.229 în loc de www.yahoo.com, și în general nu am mai avea nici Network Neighborhood în Windows, nici site-uri cu nume; tot internetul ar fi o mare de adrese IP, făcând mult mai dificilă navigarea (asta în cazul în care ar mai fi cunoscut dezvoltarea pe care a căpătat-o până acum). Din fericire există ceva ce ne salvează de calvarul memorării a zeci de numere, și anume protocolul DNS - Domain Name System.

În general, DNS este privit, la modul intuitiv, ca "protocolul care transformă numele în adresă IP". Trebuie menționat că aceasta este doar una din funcțiile sale, care are de fapt în spate un întreg mecanism ce face posibilă, printre altele, navigarea comodă; materialul de față încearcă să clarifice modul de lucru al DNS. DNS nu este singurul care oferă un spațiu de nume pentru ușurința adresării între calculatoare; un astfel de serviciu oferă și NETBIOS din familia de sisteme de operare Windows. Desigur, acesta are alte principii de funcționare, însă este des confundat ca funcții cu DNS-ul datorită coexistenței celor două protocoale în sistemul de operare mai sus amintit.

Încercări de realizare a unei echivalențe nume-calculator există de mult timp; soluția aleasă inițial era aceea a unui fișier *hosts.txt* administrat de o autoritate centrală la nivel de internet, pe care fiecare administrator de rețea trebuia să și-l copieze prin ftp odată la câteva zile. Desigur că odată cu dezvoltarea extraordinară a internetului, metoda nu mai fiabilă, în primul rând datorită dimensiunilor fișierului în cauză, și apoi din cauza flexibilității reduse (practic administratorul unei anume rețele putea opera foarte greu modificări în configurarea DNS, el trebuind să contacteze pentru fiecare schimbare autoritatea centrală). De aceea DNS vine cu ideea unei baze de date realziate de data acesta distribuit, și anume în așa fel încât atât stocarea informațiilor cât și administrarea lor să se facă ierarhizat.

Pentru a realiza funcția de *rezolvare de nume* (name resolution), protocolul DNS trebuie să aibă în spatele său la fel ca și protocoalele de nivel 2 și 3, un spațiu de indentificatori (adrese). Aceștia sunt puși în corespondență cu spațiul de adrese IP. Vom începe prin a detalia 3 noțiuni de bază:

1. spațiul de nume DNS și felul în care este el structurat;

2. servere DNS - unde și cum este păstrată informația referitoare la acest spațiu;

3. clienți DNS - modul în care un calculator poate accesa această informație pentru a realiza rezoluția de nume.

## 1.2 Spațiul de nume DNS

În cadrul protocolului DNS nu discutăm despre „adrese” sau „identificatori”, ci despre nume DNS. Toate numele DNS formează spațiul de nume DNS. Asemenea adreselor IP, numele DNS formează un spațiu structurat și anume un arbore în care în fiecare nod se află o etichetă, ca în figură, calculatoarele fiind frunzele arborelui. Fiecare etichetă poate avea până la 64 de caractere; nu sunt permise decât litere, cifre și semnul „-” (nu underscore!). Numele unui calculator se determină citind etichetele de la frunza ce-i aparține până la rădăcină: www-infoacad-ro-. Separarea etichetelor în nume se face prin punct, așadar un nume DNS „oficial” este [www.infoacad.ro](http://www.infoacad.ro). Rădăcina (root) se notează cu punct („ . ”).

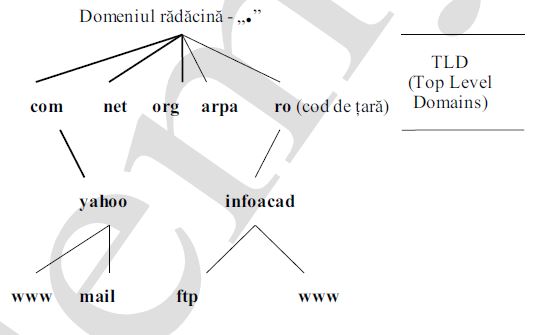


Figura 1.1 Spațiul de nume DNS

O ramură a arborelui împreună cu tot ce se află sub ea se numește domeniu și se denumește după aceeași regulă: de exemplu, domeniul infoacad.ro. Un domeniu se poate la rândul său împărți în subdomenii; în afară de rădăcină (primul nivel al arborelui – vezi figura 1.1) toate domeniile sunt practic subdomenii. Pe primul nivel se situează domeniile numite TLD (Top Level Domains), care pot fi generice (cele pe care le găsim ca terminații la toate site-urile pe care navigăm: com (site-uri comerciale), net (rețele), org (orhanizații), biz (bussiness), info, tv, arpa – cu un rol special ce va fi prezentat ulterior) sau etichetele de două litere ce reprezintă codul de țară (ro, tw, uk, etc.) – așa numitele ccTLD (country code TLC).

Un nume complet (de la frunză până la rădăcină, specificând și rădăcina prin punct) este ceea ce se numește un FQDN (Fully Qualified Domain Name); el este echivalentul căii absolute din sistemul de fișere. Prin analogie, un nume DNS care nu se termină cu punct este echivalentul unei căi relative; așa cum o cale relativă primea un prefix, în același fel, în unele contexte (în special ân fișierul zonă) numele DNS incomplete vor primi un sufix. De aceea, în astfel de contexte este foarte importantă prezența punctului la sfârșitul unui nume DNS. [1]

De exemplu, dacă calculatorul pe care lucrăm face parte din domeniul infoacad.ro și încercăm să dăm comanda „ping xyz”, calculatorul va încerca să rezolve numele xyz.ifoacad.ro. Așadar, există o deosebire între **„xyz.infoacad.ro.”** și **„xys.infoacad.ro”** din punct de vedere al unoara dintre aplicații.

## 1.3. Servere DNS

### 1.3.1. Zone DNS și rolul serverelor

Ideea de bază ce faxilitează stocarea și administrarea distribuită a DNS este aveea de delegare – un server se „ocupă” doar de o parte din spațiul de nume DNS, nu neapărat de un domeniu întreg (adică de o ramură întreagă a arborelui). Astfel, un domeniu poate fi distribuit pe mai multe servere. Mai exact, un server gestionează una sau mai multe zone, informația referitoare la ele găsindu-se în fișierul zonă.

O zonă DNS este acea porțiune din spațiul de nume care se află pe un singur server și care practic stochează o porțiune a bazei de date DNS – mai exact o porțiune ce pornește dintr-un nod (domeniul origine) și se poate extinde în jos cuprinzând subdomenii până la întâlnirea cu o altă zonă (zone cut) sau cuprinzând întregul domeniu. Relația zonă-domeniu este ilustrată în figura alăturată.[1] Pe un server pot fi stocate mai multe zone; o zonă poate cuprinde un domeniu întreg sau doar o parte a sa, eventuale subdomenii aparținând de alte zone create în acest scop. O zonă poate cuprinde atât domeniul de bază (în figură, infoacad.ro) cât și o parte din subdomeniile sale sau niciunul. În cazul nostru, prima zonă se află pe serverul 1 și se stochează informație despre domeniul infoacad.ro și frunzele sale, precum și despre subdomeniul ccna.infoacad.ro împreună cu frunzele asociate. În schimb, sarcina stocării lui domeniului unix.infoacad.ro îi revine serverului 2.

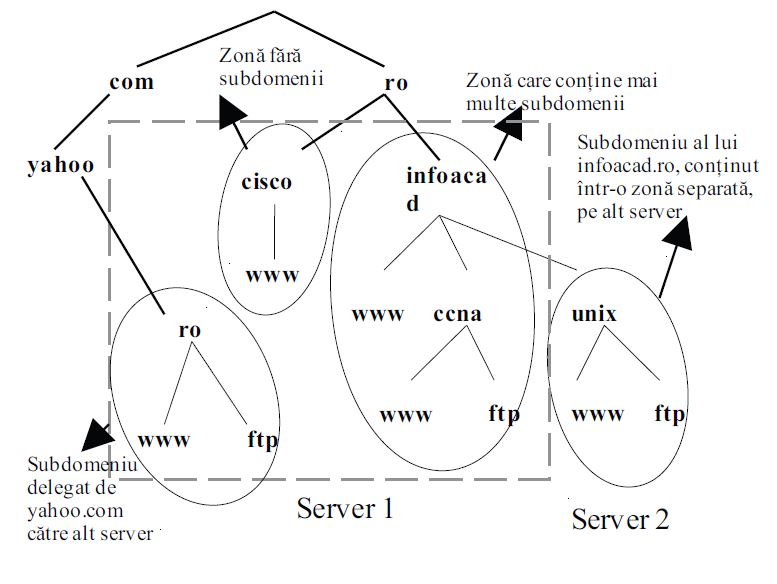


Figura 1.2 Zone DNS și rolul serverelor

Un server care stochează fișierul pentru o anumită zonă se numește autoritativ pentru zona în cauză. De exemplu, în figură, serverul 1 este autoritativ pentru zona infoacad.ro și subdomeniul ccna.infoacad.ro, pe când serverul 2 este autoritativ pentru zona unix.infoacad.ro.

Fișierul zonă reprezintă o porțiune a marii baze de date pe care o realizează sistemul DNS. În această calitate, el reprezintă un ansamblu de înregistrări numite RR – Resource Records. Spre deosebire de bazele de date obişnuite, unde fiecare înregistrare avea o compoziţie prestabilită la crearea bazei de date, aici numărul de câmpuri ale unei înregistrări depinde de tipul înregistrării.[2]

### 1.3.2. Tipuri de servere DNS asociate unei zone

O zonă DNS poate fi găzduită pe unul sau mai multe servere DNS – unul primar şi zero sau mai multe secundare. Serverul primar este cel pe care se creează şi se poate modifica informaţia zonei, pe când sercerele secundare doar îşi copiază zona de pe serverul primar.

*Notă: un software de server DNS instalat pe o staţie poate stoca mai multe zone, jucând rolul de server primar pentru o parte dintre ele şi de server primar pentru celelalte.*

Iată caracteristici ale celor două tipuri de servere:

1. **serverul primar** – serverul primar al unei zone este unic şi obligatoriu, fiind declarat în fişierul zonă prin intermediul înregistrării de tip SOA. Este singurul pe care se pot aduce modificări zonei (ex: creare sau modificare de corespondenţe nume-adresă, adăugare/eliminare roluri de staţii, etc);[2]

2. **servere secundare** – o zonă poate avea zero sau mai multe servere secundare şi este recomandat să aibă cel puţin unul. Aceste servere acţionează ca nişte mirror-uri (copii) READ-ONLY ale primarului, sincronizându-se periodic cu acesta, prin procedeul numit transfer de zonă. Fiecare zonă are o versiune; serverele secundare nu vor efectua transferul de zonă decât dacă versiunea serverului primar este superioară. Dacă un secundar nu reuşeşte să-şi actualizeze zona o perioadă lungă de timp (configurabilă), valabilitatea copiei stocate încetează şi el nu mai este autoritativ pentru zona în cauză.[2]

*Observaţie: deoarece un server secundar al unei zone are în memoria sa informaţia zonei (fie ea obţinută prin copiere) el este server autoritativ pentru zona în cauză.*

Prezenţa serverelor secundare oferă următoarele avantaje:

1. **redundanţa** – dacă serverul primar se află în imposibilitate de a răspunde la interogări (defect al staţiei, conexiune internet nefuncţională, etc), serverele secundare vor răspunde în continuare, asigurând prezenţa pe internet a domeniului/domeniilor în cauză.

2. **load sharing** – serverele secundare, fiind autoritative, răspund permanent la interogările legate de zona în cauză, ajutând serverul primar. Sistemul DNS este de aşa natură gândit încât sarcina se va distribui în mod egal.

# 2. Clienţi DNS şi interogare

## 2.1Cine sunt clienţii DNS

Toată această desfăşurare de forte nu şi-ar avea rostul dacă nu ar exista beneficiarul întregului sistem – clientul DNS. El este acela care vrea să ştie, de exemplu, „cine este [www.yahoo.com](http://www.yahoo.com)” – sau mai bine spus care este adresa corespunzatoare acestui nume. Clientul DNS, deși deseori are în spate factorul uman, e reprezentat de fapt printr-un modul al sistemului de operare numit resolver-ul DNS, ce reprezintă ansamblul bibliotecilor de funcții și resurse necesare rezoluției DNS. Resolver-ul primește din partea aplicației utilizatorului jobul de a „traduce” numele DNS în adrese IP, contactând în acest scop unul din serverele DNS configurate în sistem. Procesul constă în trimiterea unui query (interogare) de la resolver către serverul DNS, cu semnificația „trimite-mi valoarea asociată numelui X al resursei de tip Y”. Cu alte cuvinte, în cazul [www.yahoo.com](http://www.yahoo.com), „care e adresa IP asociată înregistrării de tip A cu numele [www.yahoo.com](http://www.yahoo.com)?”. Serverul DNS va trimite fie răspunsul, fie o eroare în cazul în care rezoluția nu s-a putut efectua.

Pentru a răspunde la o astfel de întrebare, serverul dispune de mai multe surse de informație, a căror ordine de interogare/utilizare poate fi în general stabilită de către administratorul sistemului de operare:

1. **unul din fișierele zonă găzduite** – dacă serverul DNS este autoritativ pentru zona conținută în interogare, serverul răspunde folosind informația locală;

2. **fișierul hosts** – atât în Windows cât și în Linux/Unix dispunem de acest fișier, în care se pot introduce corespondente statice IP-nume;

3. **memoria cache proprie** – odată ce a rezolvat un nume, serverul „ține minte” răspunsul o perioadă de timp în această memorie, astfel încât poate răspunde rapid la o aceeași întrebare care sosește din nou, minimizând timpii de răspuns și traficul;

4. **alte servere** – serverul nostru poate contacta servere DNS ajutătoare care i-ar putea oferi răspunsurile pe care nu le are.

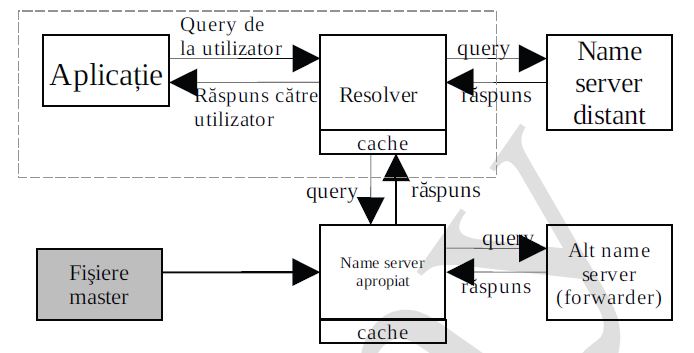


Figura 1.2 Schimbul de mesaje DNS

Resolver-ul DNS are configurate local unul sau mai multe servere, către care poate trimite query-uri când are de rezolvat un nume (spre exemplu, îm Linux ele stau în fișierul */etc/resolv.conf*). Odată primit răspunsul, informația conținută în el este reținută o perioadă te timp limitată în cache-ul local al resolverului dacă acesta există, permițând urgentarea unor query-uri ulterioare și în același timp minimizarea traficului DNS în rețea. În Windows spre exemplu se poate vizualiza conținutul cache-ului DNS cu comanda **ipconfig/displaydns.**

## 2.2 Tipuri de interogări și scenarii de utilizare

Există două moduri de lucru distincte ale rezoluției DNS:

- **interogare iterativă** – clientul trimite un query către server, punându-i condiția de a răspunde imediat (fără a mai contacta alte servere) – fie autoritativ, fie din cache (non-autoritativ), fie cu o referință (referral), adică indicându-i clientului o listă de servere „cât mai apropiate” de domeniul din întrebare;[1]

- **interogare recursivă** – clientul trimite o singură întrebare și îi cere serverului să-i dea fie un răspuns pozitiv, fie unul negativ, serverul având libertatea de a contacta orice alte servere consideră necesare pentru aflarea răspunsului. Este o modalitate de lucru foarte comodă pentru client, care „pune la muncă” serverul în numele său. Un server poate accepta sau nu o interogare recursivă (aspect reglabil din configurarea serverului).[1]

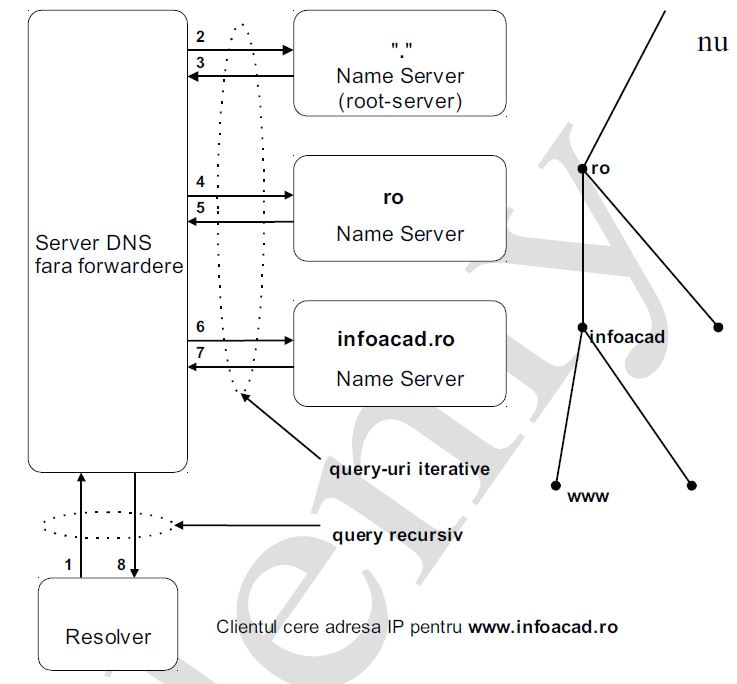


Figura 2.2 Interogarea DNS

Un server care a primit un query recursiv și care este autoritativ pentru zona în cauză și nici nu poate răspunde din cache are două posibilități:

1. serverul DNS poate avea definite așa-numitele forwarders, adică un număr de servere ajutătoare, către care „pasează” automat query-urile la care nu știe să răspundă.

2. dacă serverul nu are forwarders, el se poate folosi de root hints – liste de servere responsabile cu zona „.” (rădăcina). Serverul va încerca să parcurgă arborele DNS cu interogări iterative, de sus în jos, pe drumul delegării, până când află răspunsul pe care îl caută. Să luăm exemplul din figura alăturată: clientul încearcă să rezolve [www.infoacad.ro](http://www.infoacad.ro), în acest scop contactând serverul propriu. Serverul nu este autoritativ și nu are nici în cache nimic util, așa că demarează procesul de căutare: interoghează iterativ unul dintre serverele de root, care îi va răspunde cu lista serverelor autoritative pentru zona „ro” (către care are delegare directă). Serverul nostru alege unul din listă și îl interoghează iterativ, căpătând astfel lista serverelor autoritative pentru infoacad.ro. Unul dintre acestea din urmă va oferi în sfârșit răspunsul căutat.

## 2.3. Rezoluția inversă

Rezoluția DNS inversă presupune rezolvarea adreselor IP în nume. De remarcat că până acum am vorbit doar despre rezoluția directă, deoarece acestea sunt două noțiuni total separate – prin DNS nu se realizează echivalențe între adrese IP și nume, ci doar corespondențe în câte unul din sensuri. De aceea în internet nu toate numele care se rezolvă direct se pot rezolva și invers, ci doar o mică parte.

Rezoluția inversă a fost gândită pentru a lucra tot pe structura DNS; acest lucru este facilitat de faptul că adresele IP, la fel ca și numele DNS, formează o structură ierarhizată, fiind posibilă o punere în corespondență a celor doi arbori de identificatori. Există un domeniu DNS alocat special rezoluției inverse și anume **in-addr.arpa**. Echivalența între arbori se bazează pe faptul că prefixul de rețea acționează ca un fel de domeniu: toate subrețelele sunt incluse în rețeaua mamă, la fel cum subdomeniile sunt incluse în domeniu. Drumul către adresa 10.20.30.40 (un exemplu fictiv) va arăta ca în figura alăturată: sub domeniul arpa se află domeniul 10, care înglobează toate subrețelele de forma 10.x.y.z. Dedesubt se va afla domeniul 20, corespunzător tuturor rețelelor de forma 10.20.x.y. Mai jos, domeniul 30, pentru rețelele 10.20.30.x, iar printre alte frunze ale acestui domeniu se află și 40.

Se observă că numele DNS ce trebuie căutat pentru rezoluția inversă a adresei 10.20.30.40 este: **40.30.20.10.in-addr.arpa.** Ca regulă generală, pentru rezoluția inversă a unei adrese x.y.z.t, se apelează numele format din adresa pusă invers terminat în in-addr.arpa: t.z.y.x.in-addr.arpa.

Din figura alăturată se desprinde clar ideea că rezoluția directă și inversă se realizează pe ramuri diferite ale arborelui, și deci sunt duă operații independente, necondiționându-se în niciun fel una pe cealaltă.

*Atenție!! În cazul rezoluției inverse nu se mai solicită serverului un RR de tip A, ci unul PTR (pointer)*

# 3. Protocolul DNS

DNS este un protocol de nivel aplicație ce folosește ca protocol de nivel transport UDP sau TCP, portul 53. Datagramele UDP au lungime maximă de 512 octeți, de aceea este posilbil ca în cazul unui răspuns prea lung acesta să fie trunchiat la 512 octeți (indicându-se acest lucru clientului). Acesta din urmă va repeta query-ul, de data aceasta folosind protocolul TCP ca protocol de transport. DNS mai folosește TCP și pentru transferurile de zonă între servere.

Formatul unui mesaj DNS este cel din Figura 3.1, câmpurile având următoarele semnificații:

1. header - informația de control a protocolului DNS;

2. question - câmp în care se specifică interogarea (numele și tipul de RR ale înregistrării căutate);

3. answer - lista de răspunsuri la interogarea efectuată;

4. authority - aici sunt specificate serverele autoritative pentru domeniul din întrebare; câmpul poate lipsi;

5. additional - aici se face clarificarea unor RR-uri apărute mai sus (de exemplu, dacă în zona de authority este prezentă o resursă NS care pointează către o etichetă X, în câmpul adițional va exista un RR de tip A corespunzător resursei X care va clarifica adresa acesteia); și acest câmp poate lipsi din răspuns.

|  |
| --- |
| HEADER |
| QUESTION |
| ANSWER |
| AUTHORITY |
| ADDITIONAL |

Figura 3.1. Formatul unui mesaj DNS

Headerul DNS conține următoarele câmpuri:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ID | | | | | | | |
| QR | Opcode | AA | TC | RD | RA | Z | RCODE |
| QDCOUNT | | | | | | | |
| ANCOUNT | | | | | | | |
| NSCOUNT | | | | | | | |
| ARCOUNT | | | | | | | |

Figura3.2. Header-ul DNS

1. ID - un număr pe baza căruia se identifică corespondetele interogare - răspuns;

2. QR - query/response; indică dacă mesajul reprezintă o întrebare (0) sau un răspuns (1);

3. Opcode - codul operației; poate fi query direct (1), invers (2), sau cerere de raport de stare a serverului (3);

4. AA - authoritative answer; flag ce indică faptul că răspunsul vine din partea unui server autoritativ pentru domeniul din întrebare;

5. TC - truncation; indică trunchierea mesajului la 512 octeți;

6. RD - recursion desired; este setat atunci când clientul efectuează o interogare recursivă. Serverul poate să accepte sau nu, indicând acest lucru prin flagul RA;

7. RA - recursion available; indică posibilitatea serverului de a lucra în modul recursiv pentru interogarea în cauză;

8. RCODE - response code; are valoare informativă dacă mesajul este un răspuns, indicând codul acestuia;

9. QDCOUNT - numărul de înregistrări din câmpul *question* al mesajului DNS;

10. ANCOUNT - numărul de răspunsuri din câmpul *answer*;

11. NSCOUNT - numărul de servere autoritative din *authority*;

12. ARCOUNT - numărul de RR-uri din câmpul *additional*.

Înregistrarea unui domeniu; managementul domeniilor

*Înregistrarea* unui domeniu este operațiunea de introducere a unei intrări noi în baza de date DNS. Pentru a face această operațiune este necesa să știm cine menține această bază de date și cui ne adresăm dacă vrem să cumpărăm un domeniu.

Din acest punct de vedere, autoritatea supremă în internet este ICANN - Internet Corporation for Assigned Names and Numbers; ICANN este o organizație non-profit privată care are responsabilitatea managementului global al spațiului de adrese IP și al celui de nume DNS, incluzând menținerea celor 13 servere de root. ICANN a preluat acest job de la IANA - Internet Assigned Numbers Authority, care lucra sub contract cu guvernul USA.

Adresarea este mai departe delegată către autorități continentale: RIPE - Reseaux IP-Europeens, APNIC - Asia/Pacific Information Center, INTERNIC - autoritatea centrală; IP pentru America. Fiecare dintre acestea face delegarea autorității pentru subdomenii TLD către *registrars,* adică acele entități care intereacționează cu clientul efectuând înregistrarea efectivă a domeniului. Pentru TLD - urile public disponibile (.com, .net, .org etc.) există la ora actuală aproximativ 170 de registrări; înregistrarea ccTLD-urilor se face de către autoritățile naționale.

# 4. Bibliografie

1. DNS and BIND, 5th Edition - [Cricket Liu, Paul Albitz](http://shop.oreilly.com/product/9780596100575.do#tab_04_2), O'Reilly Media, May 2006

2. DNS For Dummies -[Blair Rampling](http://www.dummies.com/store-search.html?query=Blair+Rampling), [David Dalan](http://www.dummies.com/store-search.html?query=David+Dalan), February 2003

3. http://en.wikibooks.org/wiki/Communication\_Networks/DNS

4. https://www.freebsd.org/doc/handbook/network-dns.html

5. https://www.isc.org/downloads/bind/