**ROMÂNIA**

**MINISTERUL APĂRĂRII NAŢIONALE**

**ACADEMIA TEHNICĂ MILITARĂ „FERDINAND I”**

**FACULTATEA DE SISTEME INFORMATICE ȘI SECURITATE CIBERNETICĂ**

**Specializarea: Calculatoare şi sisteme informatice pentru apărare şi securitate naţională**



**Implementare server DNS**

Îndrumător: Realizat de:

Slt. Inginer VAMAN Adina Sd. Sg. DRAGOMIR Alexia-Ioana

Sd. Sg. SOFIANU Gabriela

Cuprins

[Capitol 1 - Introducere 3](#_Toc182386780)

[1.1. Scopul proiectului 3](#_Toc182386781)

[1.2. Lista definițiilor 3](#_Toc182386782)

[1.3. Descrierea generală a aplicației 3](#_Toc182386783)

[1.4. Diagrama DNS 4](#_Toc182386784)

[1.5. Formatul pachetelor DNS 5](#_Toc182386785)

[1.6. Modul de funcționare al DNS-ului 6](#_Toc182386786)

[1.7. Obiectivele proiectului 6](#_Toc182386787)

[Capitol 2 – Descrierea testelor 7](#_Toc182386788)

# Capitol 1 - Introducere

# 

## 1.1. Scopul proiectului

Scopul principal al proiectului este implementarea și dezvoltarea unui server DNS, care să răspundă corect la diferite cereri de transformare a numelor de domenii în adrese de rețea. Serverul nostru va traduce numele de domenii în adresele IP corespunzătoare, permițând navigarea și comunicarea pe Internet (ex.: [www.mta.ro](http://www.mta.ro) --> 142.250.181.228 ).

## 1.2. Lista definițiilor

DNS (Domain Name System) este un sistem esențial pentru funcționarea internetului, având rolul de a traduce numele de domenii ușor de înțeles de către utilizatori (cum ar fi „example.com”) în adrese IP numerice (precum „192.0.2.1”) necesare pentru localizarea și accesarea resurselor de pe internet. În esență, DNS funcționează ca un „director telefonic” al internetului, permițând dispozitivelor să identifice și să comunice între ele prin asocierea numelui de domeniu cu adresa IP corespunzătoare.

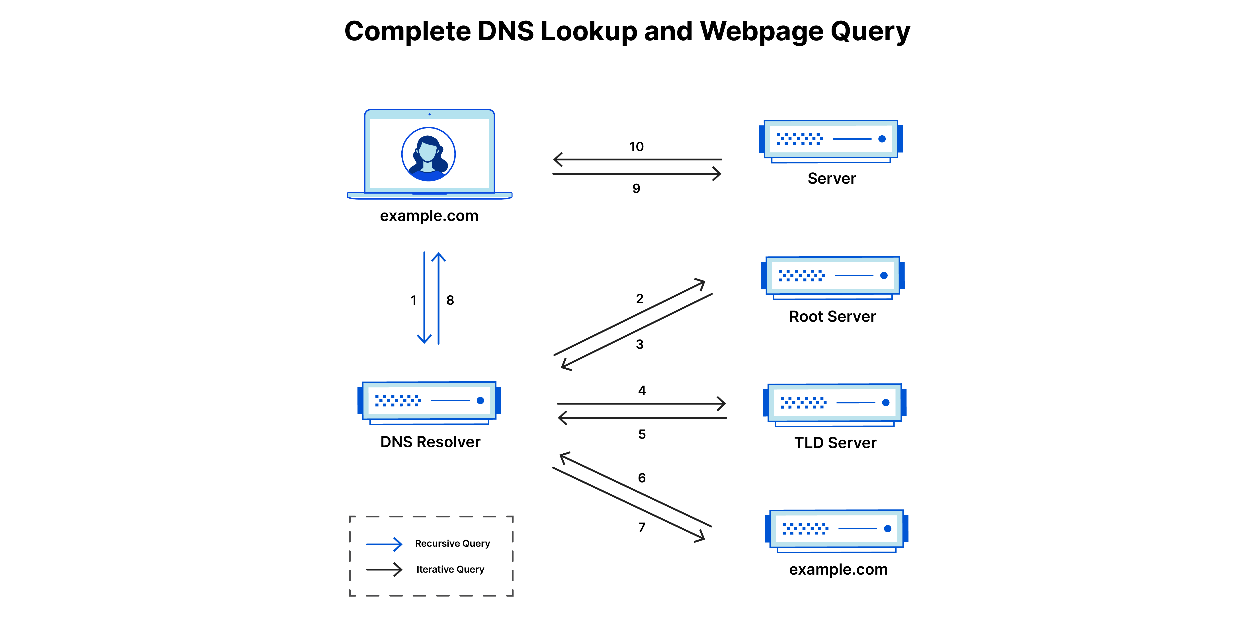
## 1.3. Descrierea generală a aplicației

Această aplicație reprezintă o implementare a unui server DNS (Domain Name System) în limbajul C, rulând pe sistemul de operare Linux. Scopul serverului DNS este de a răspunde solicitărilor de rezolvare a numelor de domenii, oferind utilizatorilor adresa IP asociată unui anumit nume de domeniu și asigurând o comunicare corectă între dispozitive.

Serverul implementat va avea următoarele funcționalități de bază pentru a simula un server DNS funcțional:

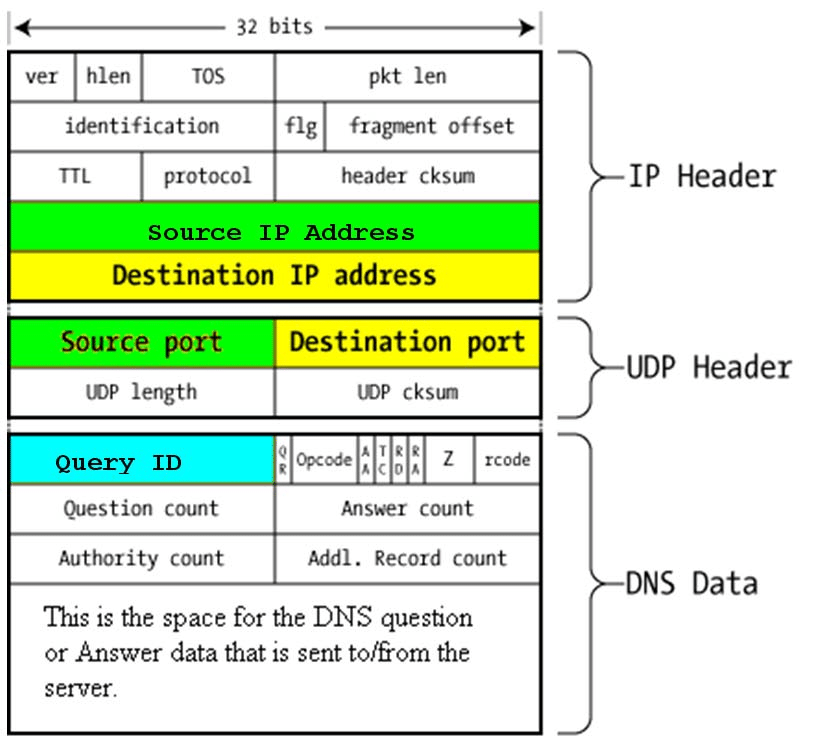
* Serverul rulează un socket UDP pe portul standard DNS (53) pentru a primi cereri de la clienți;
* Utilizând sistemul de socket-uri din Linux, serverul gestioneză conexiunile și primește pachetele DNS de la client;
* Serverul descifrează pachetul DNS primit, care include antetul (header-ul), întrebările (queries) și, opțional , secțiunile de răspuns, autoritate și informații suplimentare. Parsarea pachetului este necesară pentru a înțelege ce tip de cerere a făcut clientul (de exemplu, A pentru IPv4, AAAA pentru IPv6, NS pentru server de nume, etc.).
* Serverul DNS caută bază de date locală de tip fișier sau simulează una prin intermediul structurilor de date (de ex: un arbore sau un hash map) pentru a găsi adresa IP asociată numelui de domeniu cerut.
* Dacă adresa IP nu este disponibilă în baza de date locală, serverul poate simula o eroare de tip "Non-Existent Domain" sau un răspuns fără date (empty response).
* După ce găsește adresa IP corespunzătoare cererii, serverul trebuie să construiască un pachet DNS de răspuns, incluzând antetul și răspunsul cu adresa IP.
* Răspunsul DNS este trimis înapoi clientului utilizând socket-ul UDP prin care a primit cererea.
* Serverul trebuie să gestioneze diverse erori care pot apărea, inclusiv cereri nevalide, domenii inexistente, și probleme de conexiune. Va returna mesaje de eroare corespunzătoare în pachetele DNS de răspuns.
* Serverul oferă o funcție de logging pentru a înregistra cererile DNS și răspunsurile, facilitând depistarea eventualelor probleme.
* Serverul DNS poate implementa o funcție de cache pentru a stoca răspunsurile frecvent cerute, optimizând astfel timpul de răspuns pentru cererile ulterioare pentru același nume de domeniu. Datele din cache ar trebui să fie gestionate prin TTL (Time To Live) pentru a șterge răspunsurile expirate. Vom încerca să implementăm această funcționalitate.

## 1.4. Diagrama DNS



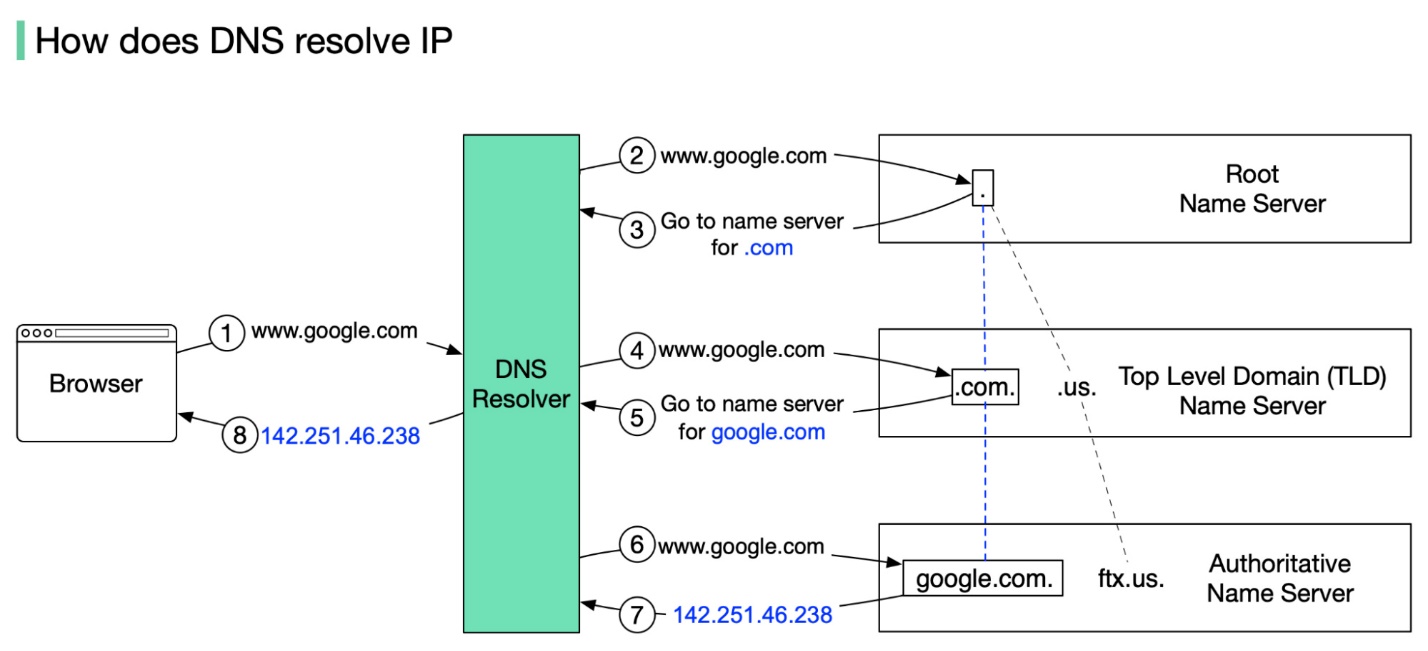
Sursă: [https:/www.cloudflare.com/learning/dns/what-is-dns/](https://www.cloudflare.com/learning/dns/what-is-dns/)

## 1.5. Formatul pachetelor DNS



Sursă: <https://www.researchgate.net/figure/The-configuration-of-an-IP-packet-for-DNS_fig2_242782899>

## 1.6. Modul de funcționare al DNS-ului



Sursă: <www.gbu-presnesnkij.ru>

## 1.7. Obiectivele proiectului

* **Configurarea zonelor DNS**: Serverul trebuie să gestioneze corect fișierele din zonă, definind relația dintre numele de domenii și adresele IP asociate. Aceasta implică configurarea fișierelor pentru zona principală și pentru subdomenii.
* **Gestionarea TTL**: Serverul trebuie să respecte valoarea TTL specificată în fișierele de zonă, controlând cât timp un răspuns rămâne în cache, pentru a echilibra între răspunsuri rapide și consistența datelor.
* **Subdomenii și forward DNS**: Serverul trebuie să ofere suport pentru subdomenii (sub.exemplu.com) și să fie capabil să transmită cererile pentru domenii necunoscute către alte servere DNS dacă este cazul.
* **Cache DNS**: Implementarea unei funcționalități de caching este esențială pentru a reduce timpul de răspuns la cererile DNS repetate și pentru a optimiza performanța serverului prin evitarea răspunsurilor redundante.
* **Testarea și validarea performanței**: Serverul DNS trebuie testat pentru a valida timpii de răspuns, comportamentul în scenarii de încărcare și stabilitate generală. Aceste teste vor ajuta la asigurarea faptului că serverul poate susține un număr semnificativ de cereri simultane fără a afecta negativ performanța.

# Capitol 2 – Descrierea testelor

|  |  |
| --- | --- |
| Numărul și textul cerinței | Testare Configurare zonă DNS |
| Modalitate de testare | -Se configurează o zonă DNS pentru un domeniu/subdomeniu;  - Se salvează modificările și se repornește serverul;  -Se rulează comanda *nslookup* și se compară rezultatele. |
| Rezultatul așteptat | Serverul răspunde cu adresa IP configurată pentru domeniul/subdomeniul respectiv. |
| Rezultatul obținut |  |
| Observații |  |
| Calificativ test |  |

|  |  |
| --- | --- |
| Numărul și textul cerinței | Testare TTL și Cache DNS |
| Modalitate de testare | -Se configurează o intrare cu un TTL scurt;  -Se efectuează o interogare DNS și se reține timpul de răspuns;  -Se repetă interogarea imediat și se observă dacă serverul răspunde din cache;  -După expirarea TTL se efectuează o nouă interogare și se verifică dacă serverul efectuează o căutare externă. |
| Rezultatul așteptat | Serverul folosește cache-ul între cereri și actualizează răspunsul la expirarea TTL. |
| Rezultatul obținut |  |
| Observații |  |
| Calificativ test |  |

|  |  |
| --- | --- |
| Numărul și textul cerinței | Testare forward DNS |
| Modalitate de testare | -Se configurează serverul pentru forward DNS către un server extern;  -Se interoghează un domeniu necunoscut (ex.: [google.com](http://www.google.com));  -Se verifică dacă serverul DNS returnează un răspuns valid prin forward. |
| Rezultatul așteptat | Serverul returnează un răspuns corect după forward către serverul DNS extern. |
| Rezultatul obținut |  |
| Observații |  |
| Calificativ test |  |

|  |  |
| --- | --- |
| Numărul și textul cerinței | Testare subdomenii |
| Modalitate de testare | -Se configurează subdomenii multiple;  -Se interoghează fiecare subdomeniu și se verifică răspunsurile. |
| Rezultatul așteptat | Fiecare subdomeniu configurat este rezolvat cu adresa IP corectă. |
| Rezultatul obținut |  |
| Observații |  |
| Calificativ test |  |