

Capitolul 2

Internet - notiuni de baza

Pentru a intelege mai bine arhitectura si functionarea Internet-ului, sunt cateva notiuni de baza ce trebuie definite, cum ar fi:

- adrese IP si hosturi
- arhitectura client-server
- porturi
- nume de domenii si sistemul DNS

2.1 Adrese IP

Internet-ul consta din retele interconectate (LAN-uri) ce contin hosturi interconectate. Un **host** este un calculator ce este conectat la o retea (fie retea LAN din care face parte sau un calculator conectat prin dial-up la retea ISP-ului) prin care are acces la Internet. Fiecare host conectat la Internet trebuie sa aiba o adresa unica pentru a putea avea acces la Internet. Aceasta adresa, care este formata din 32 de biti (adica 4 octeti), este numita **adresa IP** (Internet Protocol). Din numarul de biti al unei adrese rezulta ca in total pot fi 4.294.967.296 de valori unice. Exprimarea uzuala a acestei adrese este sub forma zecimala, fiind reprezentata ca 4 cifre zecimale despartite prin puncte, specificand valoarea zecimala a celor 4 octeti. Fiecare cifra zecimala poate avea valori intre 1 si 254.

De exemplu: 193.254.231.35 este adresa IP al serverului vega.unitbv.ro

Octetii sunt folositi nu pentru a separa numerele, ci pentru a crea asa numitele **clase de adrese**, care pot fi atribuite unei organizatii, institutii. Octetii impart adresa IP in doua parti distincte: partea de **retea** si partea de **host**. Partea de retea identifica retea din care face parte calculatorul, iar partea de host este numarul unic al calculatorului in acea retea.

Exista 5 clase de adrese IP, care sunt indicate in tabelul 2.1:

| Clasa | Prima cifra din adresa | Nr. de retele si hosturi |
|-------|------------------------|--------------------------------------|
| A | 1-126 | 127 retele si 16 milioane de hosturi |
| B | 128-191 | 16384 retele si 65534 hosturi |
| C | 192-223 | 2 milioane de retele si 254 hosturi |
| D | 224-239 | adrese multicast |
| E | 240-255 | utilizate pentru experimente |

Tabelul 2.1: Clase de adrese IP

Apartenenta unei adrese IP la o anumita clasa se poate face prin verificare primului numar zecimal din adresa, asa cum este indicat si in tabelul 2.1. Astfel in exemplul anterior se poate observa, ca prima cifra este 193, deci este vorba de o adresa de clasa C.

La clasa **A** prima cifra (adica primul octet) reprezinta numarul de retele ce se pot defini cu adresa respectiva, iar restul de trei cifre sunt folosite pentru definirea hosturilor. Deci o adresa IP de clasa A se foloseste unde este nevoie de putine retele si foarte multe hosturi in cadrul fiecarei retele.

La clasa **B** primii doi octeti reprezinta partea de retea si restul partea de host. Clasa **C** utilizeaza primii trei octeti pentru definirea retelei si ultimul octet desemneaza adresa hosturilor. Adresele de clasa C sunt utilizate cand sunt foarte multe hosturi si maxim 254 de hosturi in fiecare retea.

Clasa **D** este folosita pentru **multicast** - adresarea unui grup de calculatoare dintr-o retea. Clasa **E** este folosita pentru scopuri experimentale.

Pentru a obtine adresa retea dintr-o adresa IP, se seteaza la 0 toti bitii in partea de host. De exemplu adresa retelei din care face parte serverul vega este 193.254.231.0

2.1.1 Adrese IP speciale

Adresa de clasa A 127.0.0.0 nu este utilizata pentru a adresa o retea sau un host ci utilizata pentru interfata de retea software a unui calculator, numita interfata **loop-back**. Interfata nu are hardware asociat, si nu este fizic conectat la retea. Este utilizata pentru a efectua teste software de retea fara a crea probleme de trafic in retea. Interfata loop-back are in general adresa 127.0.0.1.

Adresa **broadcast** (de difuzare) este utilizata pentru a trimite mesaj la toate calculatoarele din aceeasi retea. O adresa broadcast este cea in care toti bitii din partea de host a adresei

IP sunt setati la 1. De exemplu pentru adresa de clasa C 193.254.231.0, adresa broadcast este 193.254.231.255.

Figura 2.1 arata doua segmente de retea (2 retele distincte interconectate printr-un ruter, ce utilizeaza adrese de clasa C. Daca un host (ruterul) apartine ambelor segmente atunci are 2 adrese IP (cate una pentru fiecare retea). Adresele de retea sunt 192.168.2.0 si 192.168.4.0.

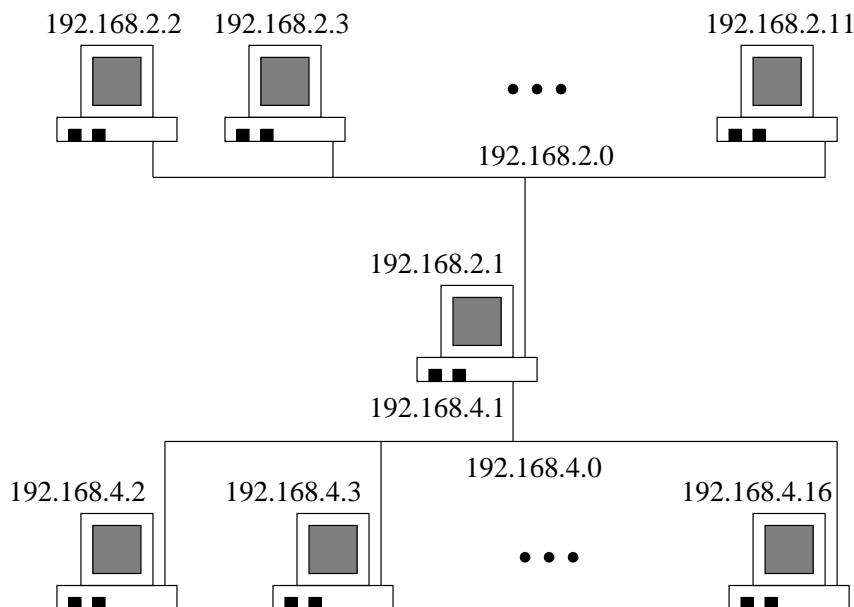


Figura 2.1: Doua segmente de retele

Fiecare din clasele de adrese A, B si C au cateva adrese care au o semnificatie speciala. Acestea nu sunt niciodata atribuite unui host conectat direct la Internet. Servesc ca adrese IP pentru intranet-ul unei organizatii. **Intranet** este o retea privata bazata pe protocolul TCP/IP, ce apartine unei organizatii, si nu este neaparat conectata la Internet. Intranet-ul este accesibil numai utilizatorilor autorizati (membrii, angajatii organizatiei).

Adresele IP rezervate pentru retelele private sau intranet-uri mai sunt numite adrese **nerutabile**, pentru ca nu pot fi rutate spre Internet.

| Clasa | Adrese IP rezervate pentru retele private |
|-------|---|
| A | 10.0.0.0 - 10.255.255.255 |
| B | 172.16.0.0 - 172.31.255.255 |
| C | 192.168.0.0 - 192.168.255.255 |

Tabelul 2.2: Adrese IP rezervate

Adresele IP sunt alocate la nivel de tara si de aceea daca o organizatie sau ISP doreste conex-

iune la Internet, trebuie sa contacteze aceasta autoritate centrala. In acest fel este garantata unicitatea adreselor IP. In Romania aceasta organizatie este **RNC** (**R**eteaua **N**ationala de **C**alculatoare - www.rnc.ro).

Adresele rezervate pentru retele private nu sunt alocate de organizatia centrala, si pot fi utilizate de orice organizatie.

2.2 Arhitectura Client-Server

Pentru realizarea aplicatiilor folosite in Internet se foloseste arhitectura client-server, pentru ca permite o implementare efectiva a serviciilor Internet. Pentru intelegerea functionarii diferitelor servicii existente pe Internet este necesara cunoasterea acestui concept.

Termenul **server** are un dublu inteles:

- din punct de vedere **hardware** este un calculator specializat/dedicat ce ofera anumite servicii altor calculatoare din retea, administreaza resursele retelei (fisiere, imprimante)
- din punct de vedere **software** este un program ce ruleaza pe un calculator (ce poate fi un calculator server) si care ofera informatii si servicii altor programe care il apeleaza.

In modelul client-server conceptul de server este privit din punct de vedere software.

Calculatoarele ce ofera servicii (Web, mail, FTP) pentru alte calculatoare sunt servere, iar cele care se conecteaza la ele sunt clienti. Atunci cand un utilizator se conecteaza la o adresa pentru a vizualiza o pagina web, la adresa respectiva ruleaza un server care raspunde la cererile de la unul sau mai multi clienti.

Client este un program ce ruleaza pe un calculator (host), pornit de catre utilizator, si care cere informatii sau foloseste serviciile oferite de serverele de pe Internet. Exemple de programe client sunt:

- clienti web: navigatoare web (Netscape, Internet Explorer, etc.) ce afiseaza continutul oferit de serverele web
- clienti mail: programe folosite de utilizatori pentru a citi si transmite mesaje e-mail
- clienti ftp: cu ajutorul acestora utilizatorii transfera fisiere de pe serverele ftp pe calculatorul local.

Majoritatea host-urilor de pe Internet sunt clienti la un moment dat. Este posibil ca serverul si clientul sa ruleze pe acelasi calculator, dar in general acestea se afla pe calculatoare diferite.

Calculatoarele ce ruleaza programe client nu au multe cereri de rezolvat care sa necesite resurse mari, astfel incat chiar si un PC cu performante medii poate fi folosit pentru conectarea la Internet si pentru rularea programelor client.

Atat serverul cat si clientul trebuie sa utilizeze acelasi "limbaj" pentru a putea comunica. Acest limbaj este protocolul utilizat pentru a trimite cereri (client) si pentru raspunde la cereri (server).

Exemple de protocoale:

- HTTP este utilizat de serverul web si navigator pentru a transfera paginile web.
- SMTP folosit de catre serverul si clientul de mail pentru a schimba mesajele e-mail

Un calculator poate rula mai multe aplicatii ce ofera servicii pe Internet, deci pot fi mai multe servere (din punct de vedere software) pe acelasi calculator. De exemplu serverul vega ruleaza software ce permite sa fie server Web, server FTP si server de mail. Utilizatorul, folosind un client specific se conecteaza la serverul corespunzator pentru a transmite informatia necesara sau sa ceara serviciile sale. De exemplu prin navigator un utilizator se conecteaza la serverul de web, sau cand trimite mail comunica cu serverul de mail pentru a transmite mesaje.

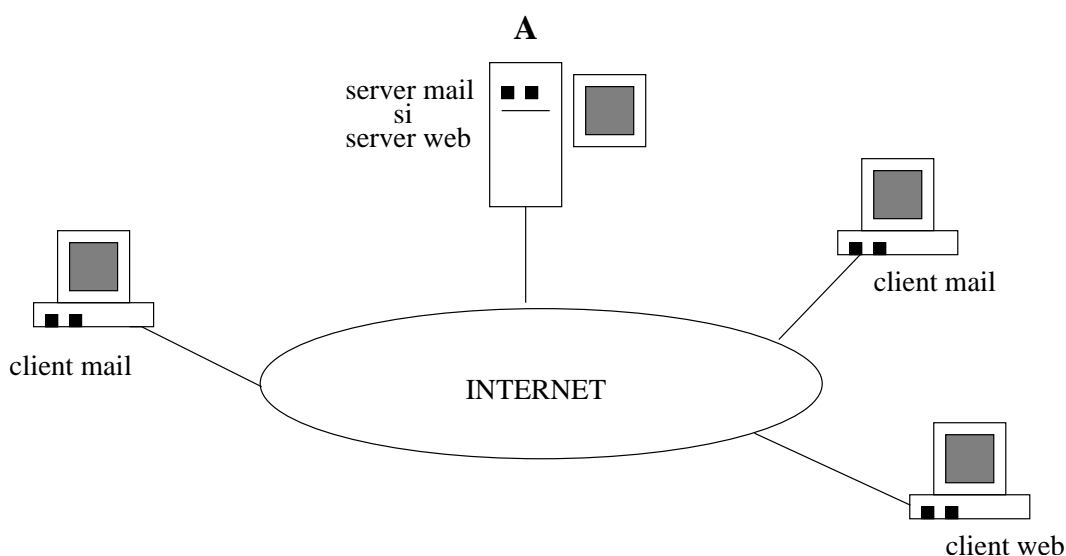


Figura 2.2: Mai multe servere pe acelasi calculator si clienti multipli

Hosturile ce ruleaza programe server trebuie sa aiba performante foarte bune (viteza si resurse de stocare). Trebuie sa faca fata la un volum mare de trafic si la un numar destul de mare de conectari simultane, cum ar fi la serverele web sau de mail, astfel incat calculatoarele obisnuite nu satisfac pe deplin cerintele unui server Internet.

O aplicatie server este pornita la punerea in functiune a calculatorului, iar apoi intra in asa numita stare de asteptare, asteptand cereri de la aplicatii client. Serverul ce poate primi cereri

de la mai multi clienti in acelasi timp este numit **concurrent**. Majoritatea serverelor de pe Internet sunt concurente: web, ftp, mail. Programele server mai sunt numite si **daemon-uri**, de exemplu daemon ftp.

In figura 2.2 se poate observa ca hostul **A** ruleaza mai multe servere la care sosesc cereri de la mai multi clienti, si pe care serverul trebuie sa fie in stare sa le serveasca.

2.3 Porturi

Cand un client se conecteaza la un calculator, trebuie sa ii "spuna" ce serviciu (program server) vrea sa acceseze, cu ce program (server) vrea sa comunice. Selectarea serverului din setul de servere ce ruleaza pe un calculator este realizat prin asa-numitele **porturi**. Fiecare server "asculta" pe un anumit port dedicat, si clientul daca vrea sa acceseze acel server trebuie sa trimita pachetele la portul respectiv.

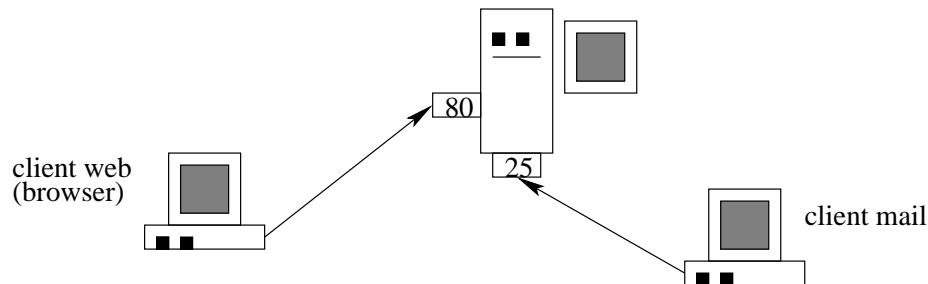


Figura 2.3: Conectarea la acelasi calculator pe porturi diferite

Fiecare serviciu cunoscut are un port prestabilit pe care il foloseste. In tabelul 2.3 sunt mentionate porturile pentru cateva servicii cunoscute.

Tabelul 2.3 indica porturile implicite utilizate de serverele listate, dar nu este obligatoriu ca acestea sa fie folosite. Serverele pot fi configurate sa asculte pe alte porturi decat cele prestabilite. Insa atunci utilizatorul trebuie sa specifice in programul client la ce port vrea sa se conecteze.

De exemplu daca un server web este instalat sa ruleze pe portul 1200 la adresa `www.xxx.com`, atunci utilizatorul trebuie sa specifice portul in URL in felul urmatoare:

`http://www.xxx.com:1200`

Daca s-ar introduce doar `www.xxx.com`, adica s-ar omite numarul portului, atunci clientul ar incerca conectarea la portul 80, pentru ca acela este portul implicit pentru un server web.

| Protocol(serviciu) | Port |
|--------------------|------|
| ftp | 21 |
| telnet | 23 |
| smtp | 25 |
| nameserver | 53 |
| finger | 79 |
| http | 80 |
| pop3 | 110 |

Tabelul 2.3: Cateva porturi binecunoscute

2.3.1 Servere proxy

Un **server proxy** este localizat la punctul de iesire catre Internet al unei organizatii. Serverul proxy poate monitoriza si intercepta toate cererile ce sunt transmise catre Internet sau ce intra dinspre Internet. Astfel un server proxy ofera:

- partajarea conexiunii intre mai multe calculatoare (**mascare adrese IP**)
- filtrarea cererilor
- imbunatatirea performantelor

Un server proxy poate procesa cereri HTTP si/sau FTP.

Accesul la Internet necesita ca fiecare calculator sa aiba o adresa unica in retea Internet. In cazul conectarii unei retele LAN la Internet, nu toate hosturile trebuie sa aiba adrese IP reale(rutabile). Se pot folosi adrese IP nerutabile pentru toate calculatoarele din retea si numai o singura adresa rutabila (reala) pentru hostul care asigura accesul spre Internet - serverul proxy. Toate cererile care vin de la statiile retelei vor fi preluate de catre serverul proxy, acesta avand rolul de a trimite mai departe cererile cu adresa IP proprie, deci efectuand **mascarea** adreselor interne din retea. Dupa ce primeste raspunsul la o cerere, le trimite inapoi statiilor de la care au sosit cererile. In figura 2.4 este aratat intregul proces. Prin mascarea adreselor IP serverele proxy ofera un mod eficient si ieftin de a partaja o singura adresa IP de catre statiile unei retele. Aceasta inseamna atat o economie importanta de adrese IP, cat si financiara.

Filtrarea cererilor este scopul initial si motivul de securitate pentru care s-au creat serverele proxy. Serverele proxy pot inspecta tot traficul (de iesire si intrare) si pot permite sau nega transmiterea informatiilor. Serverul proxy poate fi utilizat in special pentru a nu permite accesul utilizatorilor interni la anumite adrese web (pe baza adresei, sau a continutului acestora). Serverul proxy poate sa faca si autentificarea utilizatorilor, astfel ca se poate urmari ce anume

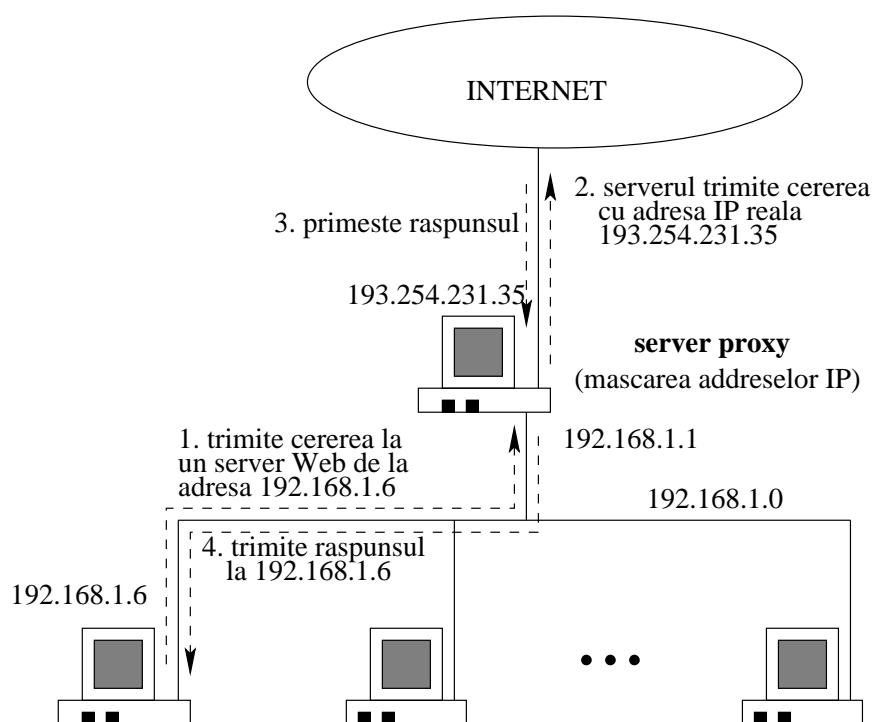


Figura 2.4: Mascarea adreselor IP

face fiecare utilizator. Pentru proxy-urile HTTP aceasta inseamna momorarea fiecarui URL vizitat, iar la proxy-urile FTP orice fisier descarcat.

Imbunatatirea performatelor folosind servere proxy se numeste functia de **cache** si serverul in acest caz se numeste **proxy cache**. La fiecare acces catre Internet, serverul proxy verifica daca cererea facuta pentru o pagina web sau un fisier de pe un server FTP este deja pe hard-disk-ul sau. In caz afirmativ informatia este trimisa catre client fara intarziere. Daca nu se afla pe serverul proxy, acesta transfera informatia de pe Internet, este salvata local pentru eventualele cereri ulterioare dupa care este trimis la clientul care a facut cererea. Astfel traficul catre Internet poate scade radical si creste viteza de acces spre exterior.

2.4 Nume de domenii

Fiecare calculator accesibil in Internet are o adresa IP unica, pe baza caruia poate fi accesata de catre alte calculatoare. Insa pentru oameni este mult mai usor sa retina un nume decat un sir de cifre, de aceea au aparut numele de domenii. Fiecare calculator pe langa adresa IP are si un nume de domeniu corespunzator. Exemple:

- www.unitbv.ro

- www.eeng.dcu.ie
- www.fbi.gov
- www.yahoo.com
- ftp.deltanet.ro

Numele de domenii sunt organizate ierarhic, cum este aratat in figura 2.5.

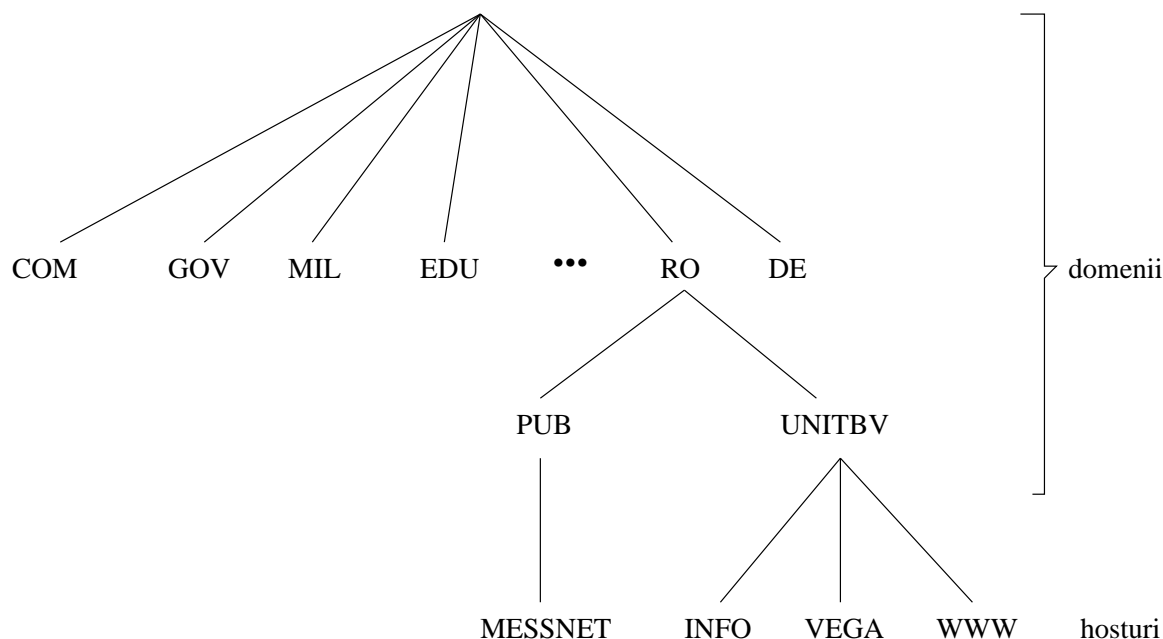


Figura 2.5: Structura ierarhica a numelor de domenii

Formatul general al numelor de domenii este: **hostname.second_level.first_level**.

Primul nivel (domeniu), numit nivelul superior (**TLD - Top Level Domain**) este cel mai puțin specific, și indică tipul organizației sau țara careia îi aparține hostul respectiv. Există sute de nume de domenii în acest nivel, printre care .COM, .EDU, .MIL, .GOV, .ORG și combinații de două litere pentru fiecare țară.

În fiecare TLD există foarte multe domenii la nivelul doi (subdomenii) ce identifică organizația, cum ar fi **google**, **yahoo**, **unitbv**, **pub**, etc. Numele în primul nivel sunt unice, însă la nivelul doi pot exista duplicate (în TLD-uri diferite) cum ar fi **linux.com** și **linux.org**, care sunt calculatoare diferite. Orice organizație poate înregistra un nume de domeniu la nivelul doi, cu condiția ca numele respectiv să nu existe deja. Subdomeniul este în general numele sau prescurtarea numelui organizației, de exemplu: **whitehouse.gov** sau **unitbv.ro**. Pot exista mai multe nivele de subdomenii până la 127, dar rar sunt utilizate mai mult de patru (de exemplu **eeng.dcu.ie**).

Numele host reprezintă numele serverului din subdomeniul respectiv. Trebuie să se facă distinc-

tia între domeniu (unitbv.ro) și un host (vega.unitbv.ro). Domeniul este un grup de subdomenii sau un grup de host-uri, iar host-ul este cel mai inferior nivel al ierarhiei.

Deoarece numele de domenii trebuie să fie unice trebuie să fie o singură organizație la nivel de țară, ce controlează această listă ca să se asigure că nu există duplicate. În România această organizație este **RNC**. Asemenea organizații mențin o bază de date ce conține informații despre proprietarul domeniului și serverele DNS pentru fiecare domeniu.

Existența unei organizații centrale pentru administrarea numelor de domenii din primul nivel este importantă, însă acesta nu poate menține informația legată de fiecare subdomeniu, unde pot exista zeci sau sute de hosturi în fiecare. Astfel subdomeniile mențin informațiile legate de hosturile lor și au responsabilitatea asigurării numelor unice în domeniul respectiv.

Sapte noi domenii de nivel superior au apărut în 2001, primele noi domenii introduse după anul 1988. Acestea sunt .aero, .BIZ, .coop, .INFO, .MUSEUM, .NAME, .pro. Cele scrise cu majuscule au fost deja aprobate și s-a început înregistrarea domeniilor de nivel doi (mai multe informații puteți găsi la pagina ICANN).

În România înregistrarea noilor subdomenii în domeniul .ro este supervizată de către **RNC** (www.rnc.ro).

2.5 Sistemul DNS (Domain Name System)

DNS este sistemul de adresare pe Internet, fiind cea mai mare bază de date distribuită, fără de care Internet-ul nu ar putea funcționa, și folosește pentru **translatarea numelor de domenii în adrese IP**. Scopul acestui sistem este de a permite unui calculator de pe Internet să afle ce adresă IP corespunde numelui de domeniu al unui host, deoarece în Internet toate pachetele între calculatoare se transmit pe baza adresei IP, și nu pe baza numelui de domeniu. Este o parte foarte importantă a Internet-ului care însă este ascunsă, transparentă pentru utilizator.

Pentru a se conecta la un server utilizatorii ar putea folosi adresa IP al unui host în loc de numele de domeniu. De exemplu în navigator s-ar putea scrie adresa **64.58.76.223** și s-ar încărca pagina web de la **www.yahoo.com** pentru că acesta este adresa IP pentru Yahoo. Sau se poate trimite mai la adresa `szekelyg@[193.254.231.35]` în loc de `szekelyg@vega.unitbv.ro`. Însă pentru oameni este mult mai ușor să rețină numele de domeniu decât un șir de cifre, astfel maparea între adrese IP și nume de domenii este necesară.

Sistemul DNS la începuturile Internet-ului era un fișier **host.txt** care se afla pe un server FTP anonim, și oricine se putea conecta la acel server. Fișierul conținea informație despre toate hosturile conectate la ARPANET, adică numele de domeniu și adresa IP pentru fiecare host în parte. Acest fișier era mereu reactualizat pe serverul FTP și administratorii care doreau

sa comunice schimbari legate de hosturile lor trimiteau prin email schimbarile, care apoi erau reactualizate pe serverul FTP. Deasemenea administratorii se conectau periodic (2-4 zile) pentru a transfera pe hosturile proprii noul fisier reactualizat (figura 2.6).

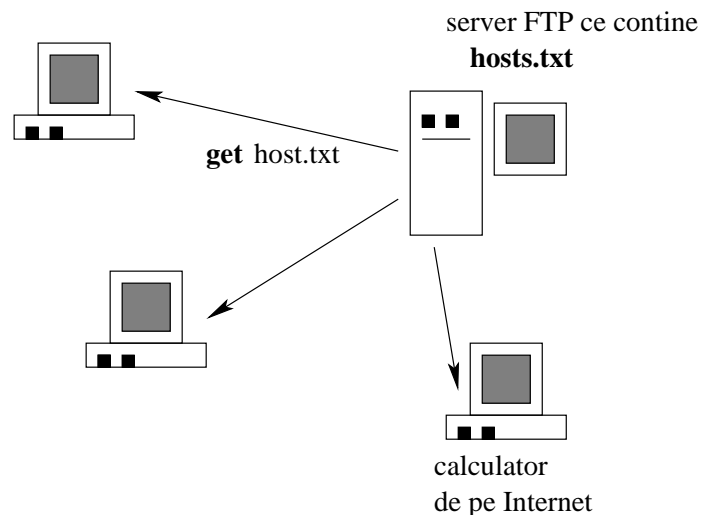


Figura 2.6: Sistemul DNS la inceputuri

Sistemul a functionat multi ani, inasa odata cu cresterea hosturilor pe INTERNET de la cateva sute, incarcarea serverului FTP a devenit prea mare, si nici metoda nu mai era functionala.

In **1984** Paul Mockapetris (USC - Information Sciences Institute) a proiectat arhitectura sistemului DNS care se utilizeaza si in ziua de azi. In acest sistem informatia DNS este distribuita in toata reseaua Internet, nu exista un singur calculator care are toata informatia de mapare intre adrese IP si nume de domenii. Fiecare domeniu sau subdomeniu mentine informatia legata de hosturile sale avand un server DNS, si o autoritate centrala retine informatia unde se afla informatia pentru fiecare domeniu in parte.

Organizatia care se ocupa de inregistrarea domeniilor la al doilea nivel (yahoo.com, linux.org, mit.edu), alocarea adreselor IP si alte responsabilitati legate de sistemul DNS este **ICANN** (**I**nternet **C**orporation for **A**ssigned **N**ames and **N**umbers - www.icann.org).

Pentru a intelege cum functioneaza sistemul DNS sa luam exemplul urmator: cand utilizatorul introduce o adresa in browser, de exemplu **www.altavista.com**, calculatorul se conecteaza la serverul DNS local pentru a afla adresa IP al numelui de domeniu respectiv (figura 2.7). Daca serverul a mai primit o cerere pentru acelasi domeniu atunci a retinut adresa lui si o transmite calculatorului. Daca serverul nu are memorata adresa IP a numelui cerut, atunci va incerca sa afle adresa de la un alt server. Serverul DNS local va trimite cererea la unul din serverele de baza (root nameservers) din Internet. Adresa IP a acestor servere (13 servere) este memorata pe fiecare server DNS pentru a fi gasite.

Aceste servere de baza au informatia despre serverele DNS care raspund de domeniile din nivelul superior (.com, .gov, .edu, .uk etc.) In exemplu nostru daca cautam `www.altavista.com`, serverul de baza care este contactat de catre serverul DNS local va intoarce adresa serverului DNS care are informatii despre domeniul .com. Serverul local va contacta serverul al carei adresa l-a primit care la randul lui va transmite inapoi adresa serverului DNS care raspunde de domeniul `altavista.com`.

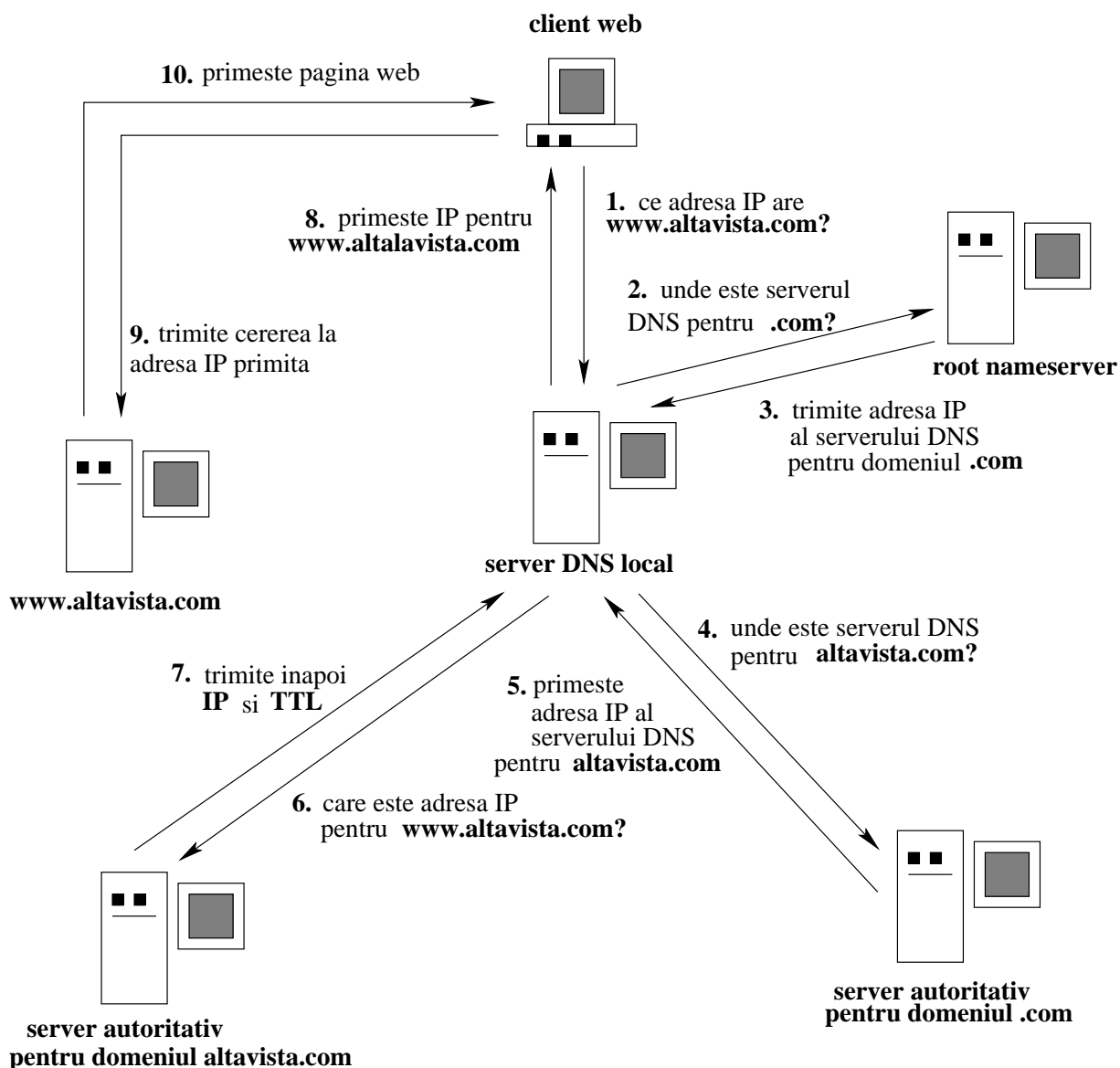


Figura 2.7: Functionarea sistemului DNS

Acest ultim server DNS va transmite inapoi adresa IP al serverului `www.altavista.com`, cat si valoarea **TTL** (**T**ime **T**o **L**ive) care reprezinta timpul cat va fi retinut de catre serverul local

adresa IP pentru acest nume de domeniu. Avand IP-ul numelui de domeniu cerut navigatorul va face conectarea la serverul web si se va transfera pagina web.

Toate aceste operatii sunt efectuate de fiecare data cand un utilizator introduce un nume de domeniu cand cere transferarea unei pagini web, trimitere de e-mail, conectare la server de stiri etc. Practic un utilizator poate face zilnic sute de cereri DNS fara sa stie.

Valoarea TTL este foarte importanta, pentru ca daca adresa IP a unui nume de domeniu s-ar memora pe serverul DNS local, iar acel nume de domeniu ar schimba adresa IP, practic acel nume de domeniu nu ar mai fi accesibil pentru ca s-ar inecra conectarea la vechea adresa IP, care a fost memorata pe serverul DNS local.

DNS utilizeaza un numar larg de servere (name server), organizate ierarhic si distribuite pe tot globul. Exista servere locale, root si autoritative. Aceste servere comunica intre ele pentru a rezolva cererea primita de la un client. Serverele root mentin informatia despre serverele DNS pentru nivelul de domeniu superior. Pentru nivelul superior sau un subdomeniu serverele autoritative raspund de mentinerea informatiei de mapare intre numele de domeniu al hosturilor si adresele IP corespunzatoare. Serverele autoritative sunt de asemenea servere locale pentru o anumita organizatie. Serverele locale se afla in cadrul organizatiilor, universitati, facultati, ISP-uri.

In sistemul DNS se utilizeaza si conceptul de caching, pentru a reduce numarul de mesaje DNS schimbat in retea si pentru a reduce intarzierea la rezolvarea numelor de domenii. Cand un server DNS primeste o cerere de rezolvare a unui nume, acesta o memoreaza (cache). Cand soseste o noua cerere pentru acelasi nume, serverul va sti adresa. O adresa memorata va fi stearsa dupa o anumita perioada de timp (TTL), in general intre o zi si o saptamana.

Dupa cum s-a vazut DNS este un sistem complex, o baza de date distribuita pe tot globul. Zilnic rezolva miliarde de cereri pentru miliarde de nume printr-o retea de mii de servere DNS. De fiecare data cand un utilizator trimite un mail sau se acceseaza o pagina web face cereri la mai multe servere DNS aflate in diferite locuri in lume. Deasemenea ofera flexibilitate: in cazul schimbarii adresei IP din diverse motive utilizatorul va gasi hostul pe baza numelui de domeniu, deoarece numele de domeniu ramane si sistemul DNS va gasi noua adresa IP corespunzatoare numelui de domeniu.

Gasirea proprietarului unui nume de domeniu si vizualizarea inregistrarii se poate face la adresa **www.uwhois.com**. Pentru a vedea o inregistrare a unui subdomeniu in domeniul TLD .ro efectuati o cautare pe pagina **whois.rotld.ro**.