

PROTOCOALE DE COMUNICAȚIE : LABORATOR 9

Protocolul DNS

Responsabil: Alecsandru PATRASCU

Cuprins

Obiective	1
Prezentarea laboratorului	1
Protocolul DNS	2
Spatiul de nume	2
Algoritmul de interogare	3
Inregistrari de resurse	3
Servere de nume	4
API DNS	5
Apelul gethostbyname()	5
Apelul gethostbyaddr()	6
Structura hostent	6
Aplicație	6
Referințe	7

Obiective

În urma parcurgerii acestui laborator studentul va fi capabil să:

- Opereze cu ierarhia spațiilor de nume și să identifice tipurile de domenii, subdomeniile.
- Să folosească algoritmul de interogare folosit de DNS.
- Să identifice tipurile de resurse pentru diverse domenii și clasa acestora.
- Să folosească un set minimal de funcții pentru aflarea informațiilor unui host.

Prezentarea laboratorului

Programele se referă rareori la sisteme gazda, cutii postale și alte resurse prin adresa lor binară. În loc de numere binare se utilizează șiruri ASCII, cum ar fi user@cs.pub.ro. Cu toate acestea rețeaua înțelege numai adrese binare, deci este necesar un mecanism care să convertească șirurile ASCII în adrese de rețea. Protocolul care se ocupă de aceasta se numește DNS (Domain Name System - Sistemul numelor de domenii). Esența DNS-ului constă dintr-o schemă ierarhică de nume de domenii și a unui sistem de baze de date distribuite pentru implementarea acestei scheme de nume. Protocolul este definit în RFC-urile 1034 și 1035.

Protocolul DNS

Spatiul de nume

DNS organizează numele resurselor într-o ierarhie de domenii. Un domeniu reprezintă o colecție de sisteme gazda care au unele proprietăți în comun, cum ar fi faptul ca toate aparțin unei aceleiași organizații sau faptul ca toate sunt situate geografic în același perimetru.

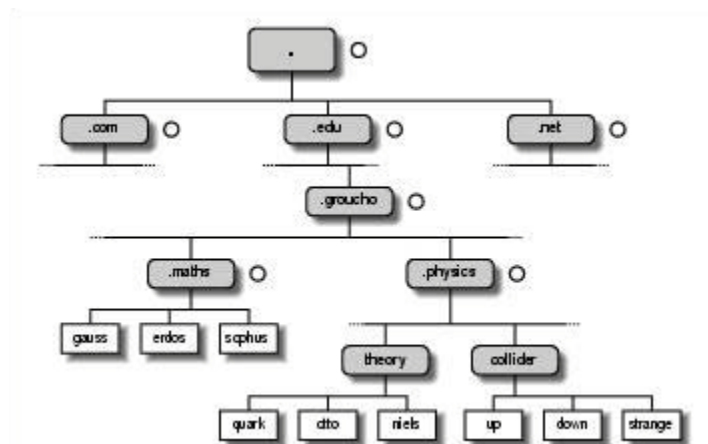


Figura 1: O porțiune a spațiului numelor de domenii din Internet

Fiecare domeniu este partiționat în subdomenii și acestea sunt, la rândul lor, partiționate s.a.m.d. Toate aceste domenii pot fi reprezentate ca un arbore, după cum se poate vedea în Figura 1. Frunzele arborelui reprezintă domenii care nu au subdomenii (dar care conțin totuși sisteme). Un domeniu frunza poate conține de la un singur sistem gazda până la mii de sisteme gazda.

Domeniile de pe primul nivel se împart în două categorii: generice și de țări. Domeniile generice sunt com (comercial), edu (instituții educaționale), gov (guvernul SUA), int (organizații internaționale), mil (forțele armate ale SUA) și org (organizații nonprofit). Domeniile de țări includ o intrare pentru fiecare țară, după cum se definește în ISO 3166. Fiecare domeniu este denumit de calea în arbore până la rădăcina. Componentele sunt separate prin punct. Astfel departamentul de inginerie de la SUN poate fi eng.sun.com în loc de numele în stil UNIX /com/sun/eng.

Numele de domenii pot fi absolute sau relative. Un nume absolut de domeniu (fully qualified domain name - FQDN) este un nume de domeniu care nu permite nici o ambiguitate cu privire la locația relativă la rădăcina arborelui de nume de domenii. Astfel de nume absolute de domenii se termină cu punct (de exemplu eng.sun.com.). În contrast un nume relativ de domeniu este un nume care are sens numai relativ la un anume domeniu DNS altul decât cel root.

Numele de domenii nu fac distincție între litere mici și litere mari, astfel edu sau EDU înseamnă același lucru. Componentele numelor pot avea o lungime de cel mult 64 de caractere, iar întreaga cale de nume nu trebuie să depășească 255 de caractere.

Fiecare domeniu controlează cum sunt alocate domeniile de sub el. De exemplu, Japonia are domeniile ac.jp și co.jp echivalente cu edu și com. Olanda nu face nici o distincție și pune toate organizațiile direct sub nl. Pentru a crea un nou domeniu se cere permisiunea domeniului în care va fi inclus. De exemplu, dacă un grup VLSI de la Yale dorește să fie cunoscut ca vlsi.cs.yale, acesta are nevoie de permisiunea celui care administrează cs.yale.edu. Similar, o nouă universitate care dorește obținerea unui domeniu va trebui să ceară permisiunea administratorului domeniului edu. În acest mod sunt evitate conflictele de nume și fiecare domeniu poate ține evidența tuturor subdomeniilor sale. Odata ce un nou domeniu a fost creat și înregistrat el poate crea subdomenii, fără a cere permisiunea de la cineva din partea superioară a arborelui.

Algoritmul de interogare

Conceptele cu care DNS lucreaza sunt:

1. Server DNS - Stații care rulează programe de tip server de DNS care conțin informații asupra bazelor de date DNS și despre structura numelor de domenii;
2. Resolver DNS - Programe care folosesc cereri DNS pentru interogarea unor servere DNS. Modul în care se derulează procesul de interogare DNS este cel din Figura 2.

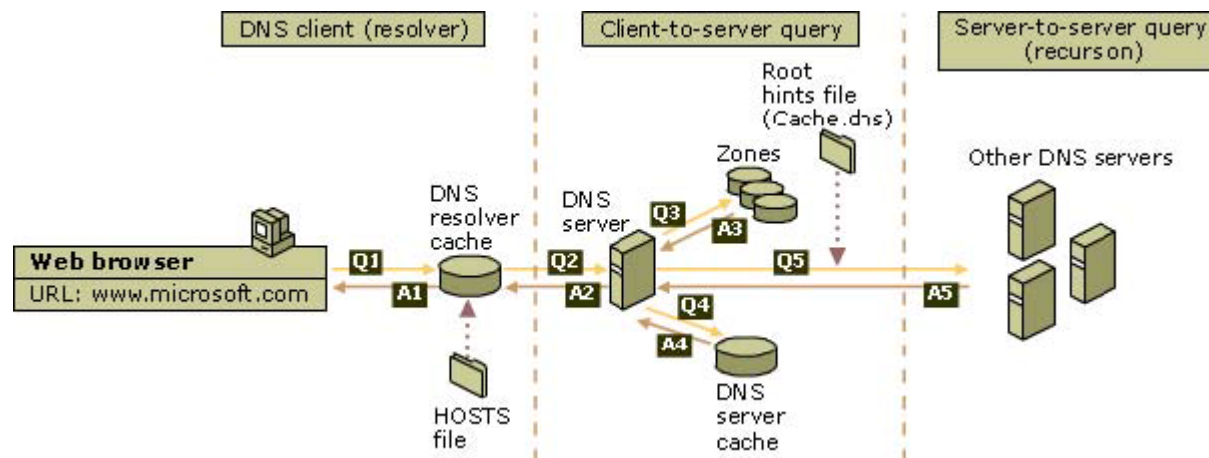


Figura 2: Procesul de interogare DNS

Înregistrări de resurse

Fiecărui domeniu, fie ca este un singur calculator gazda, fie un domeniu de nivel superior, îi poate fi asociată o mulțime de înregistrări de resurse (resource records). Pentru un singur sistem gazda cea mai obișnuită înregistrare de resursă este chiar adresa IP, dar există multe alte tipuri de înregistrări de resurse.

Atunci când procedura resolver trimite un nume de domeniu DNS, ceea ce va primi ca răspuns sunt înregistrările de resurse asociate acelui nume. Astfel adevărata funcție a DNS este să realizeze corespondența dintre numele de domenii și înregistrări de resurse.

O înregistrare de resursă este un 5-tuplu. Cu toate că, din rațiuni de eficiență, înregistrările de resurse sunt codificate binar, în majoritatea expunerilor ele sunt prezentate ca text ASCII, câte o înregistrare de resursă pe linie. Formatul pe care îl vom utiliza este următorul:

1	Nume_domeniu	Timp_de_viata	Tip	Clasa	Valoare
---	--------------	---------------	-----	-------	---------

unde:

- Nume_domeniu precizează domeniul căruia i se aplica aceasta înregistrare. În mod normal există mai multe înregistrări pentru fiecare domeniu și fiecare copie a bazei de date păstrează informații despre mai multe domenii. Acest câmp este utilizat ca cheie de căutare primară pentru a satisface cererile. Ordinea înregistrărilor în baza de date nu este semnificativă. Când se face o interogare despre un domeniu sunt returnate toate înregistrările care se potrivesc cu clasa cerută.
 - Câmpul Timp_de_viata da o indicație despre cât de stabilă este înregistrarea.
 - Câmpul Tip precizează tipul înregistrării. Cele mai importante tipuri sunt prezentate în Tabelul 1
- O înregistrare SOA furnizează numele sursei primare de informație despre zona serverului de nume, adresa de e-mail a administratorului, un identificator unic și diverși indicatori și contoare de timp.

Tabelul 1: Tipuri de înregistrări DNS

Tip	Semnificație	Valoare
SOA	Start autoritate	Parametrii pentru aceasta zona
A	Adresa IP a unui sistem gazda	Intreg pe 32 de biți
MX	Schimb de posta	Prioritate, domeniu dispus sa accepte posta electronica
NS	Server de Nume	Numele serverului pentru acest domeniu
CNAME	Nume canonic	Numele domeniului
PTR	Pointer	Pseudonim pentru adresa IP
HINFO	Descriere sistem gazda	Unitate centrala si sistem de operare in ASCII
TXT	Text	Text ASCII neinterpretat

Cel mai important tip de înregistrare este înregistrarea A (adresa). Ea păstrează adresa IP de 32 de biți a sistemului gazda. Următoarea ca importanta este înregistrarea MX. Aceasta precizează numele domeniului pregătit sa accepte posta electronica pentru domeniul specificat. Înregistrările specifica numele severului. Ca exemplu de informație ce se poate găsi in baza de date DNS a unui domeniu:

```

1 ; Authoritative Information on physics.groucho.edu.
2 @ IN SOA niels.physics.groucho.edu.
3 janet.niels.physics.groucho.edu. {
4 1999090200 ; serial no
5 360000 ; refresh
6 3600 ; retry
7 3600000 ; expire
8 3600 ; default ttl
9 };
10 ; Name servers
11 IN NS niels
12 IN NS gauss.maths.groucho.edu.
13 gauss.maths.groucho.edu. IN A 149.76.4.23
14 ;
15 ; Theoretical Physics (subnet 12)
16 niels IN A 149.76.12.1
17 IN A 149.76.1.12
18 name server IN CNAME niels
19 otto IN A 149.76.12.2
20 quark IN A 149.76.12.4
21 down IN A 149.76.12.5
22 strange IN A 149.76.12.6
23 ...
24 ; Collider Lab. (subnet 14)
25 boson IN A 149.76.14.1
26 muon IN A 149.76.14.7
27 bogon IN A 149.76.14.12
28 ...

```

Servere de nume

Teoretic un singur server de nume poate conține întreaga baza de date DNS si poate sa răspundă tuturor cererilor. In practica, acest server poate fi atât de încărcat, încât sa devina de neutilizat. Pentru a evita probleme asociate cu existenta unei singure surse de informație, spațiul de nume DNS este împărțit in zone care nu se suprapun. O posibila astfel de împărțire este cea din Figura 3.

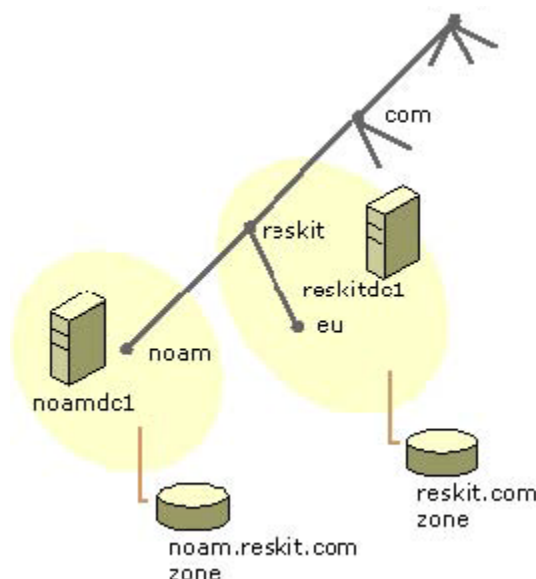


Figura 3: O parte din spatiul numelor DNS reprezentand impartirea in zone

Fiecare astfel de zona conține cate o parte a arborelui precum si numele serverilor care păstrează informația autorizata despre acea zona. Normal o zona va avea un server de nume primar, care preia informația dintr-un fișier de pe discul propriu, si unul sau mai multe servere de nume secundare, care iau informația de pe serverul primar. Pentru a îmbunătăți fiabilitatea, unele servere pentru o zona pot fi plasate chiar in afara zonei.

Plasarea limitelor unei zone este la latitudinea administratorului ei. Aceasta decizie este luata in mare parte pe baza numărului de servere de nume care se doresc a se folosi si a locației acestora. Atunci când un resolver are o cerere referitoare la un nume de domeniu, el transfera cererea unuia din serverele locale de nume. Daca domeniul este sub jurisdicția serverului de nume el va întoarce înregistrări de resurse autorizate. O înregistrare autorizata (authoritative record) este cea care vine de la autoritatea care administrează înregistrarea si astfel este întotdeauna corecta. Înregistrările autorizate se deosebesc de înregistrările din memoria ascunsa, care pot fi expirate.

Daca totuși domeniul se afla la distanta, iar local nu este disponibila nici o informație despre domeniul cerut, atunci serverul de num trimite un mesaj de cerere la serverul de nume de pe primul nivel al domeniului solicitat. De mentionat ca metoda de interogare este cunoscuta ca metoda de interogare recursiva (recursive query), deoarece fiecare server care nu are informația ceruta o caută in alta parte si raportează.

API DNS

Aplicațiile Internet se folosesc de apelurile de sistem *gethostbyname()* si *gethostbyaddr()*, precum si de structura *hostent*.

Apelul *gethostbyname()*

```

1 #include <netdb.h>
2
3 struct hostent *gethostbyname(const char *name);

```

Funcția primește ca argument un nume simbolic sub forma unui șir de caractere și întoarce un pointer la o structură ce indică o serie de caracteristici ale mașinii UNIX respective, sau NULL în caz de eroare.

Apelul `gethostbyaddr()`

```
1 #include <netdb.h>
2
3 struct hostent *gethostbyaddr(const char *addr, int len, int type);
```

Funcția `gethostbyaddr()` caută informații despre un host pornind de la adresa sa IP. În caz de eroare va întoarce NULL. Parametrii acestei funcții sunt:

- `type` Specifică familia de adrese (`AF_INET` pentru adrese de tip internet).
- `addr` Reprezintă un pointer la un buffer ce conține adresa, dată în formatul specific familiei de adrese din care face parte.
- `len` Specifică lungimea bufferului anterior.

Structura `hostent`

Structura `hostent` este definită astfel:

```
1 #include <netdb.h>
2
3 struct hostent
4 {
5     char *h_name;
6     char **h_aliases;
7     int h_addrtype;
8     int h_length;
9     char **h_addr_list;
10 }
```

unde:

- Numele mașinii respective, cât și alte nume sub care ea este cunoscută (alias-uri) sunt continute în primele două câmpuri ale acestei structuri: `h_name` și `h_aliases`.
- Câmpul `h_addrtype` conține în cazul mașinilor ce au atribuite adrese IP valoarea constantei `AF_INET`.
- Câmpul `h_length` indică lungimea binară a tipului de adresă utilizat (în cazul adreselor IP această lungime este de 4 octeți).
- Ultimul câmp reprezintă un vector de adrese sub care această mașină e recunoscută în rețea. Fiecare astfel de adresă este de fapt un șir de `h_length` octeți.

Aplicație

În cadrul laboratorului curent, nu o să folosim API-ul prezentat mai sus, ci vom face o implementare mai low-level a unui DNS resolver, populând manual headerul și parsând manual rezultatele. Urmăriți scheletul de cod pentru a implementa clientul (parte de lansat query este deja făcută). Clientul primește ca argumente opționale numele pentru care să facă query (default: "www.google.com") și serverul către care se face query (default: "8.8.8.8"). Exemple de apel:

```
1 ./clientdns_lab  
2 ./clientdns_lab wikipedia.org  
3 ./clientdns_lab wikipedia.org 8.8.4.4
```

Puteți urmări secțiunea "4. MESSAGES" a RFC 1035 pentru a vedea formatul mesajelor trimise/primate.

Referințe

1. RFC 1034 – <http://www.ietf.org/rfc/rfc1034.txt>
2. RFC 1035 – <http://www.ietf.org/rfc/rfc1035.txt>
3. ISO 3166 – http://userpage.chemie.fu-berlin.de/diverse/doc/ISO_3166.html
4. Setarea unui server de DNS in Linux din "Linux Network Administrators Guide" - <http://www.faqs.org/docs/linux-network/x-087-2-resolv.html>
5. DNS-HOWTO – <http://www.linux.org/docs/ldp/howto/DNS-HOWTO.html>