Protocoale de nivel aplicaţie:

DNS

DNS

Servicii oferite:

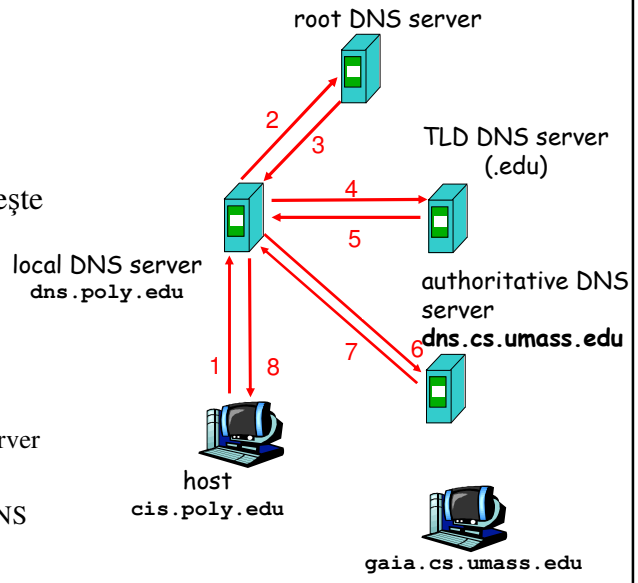
- translaţie Hostname ↔ IP address
- Host aliasing
  - Canonical and alias names
- Mail server aliasing
- Load balancing
  - servere web (ex: www.google.com) cu un singur nume canonic şi multe adrese IP

Realizare: bază de date distribuită

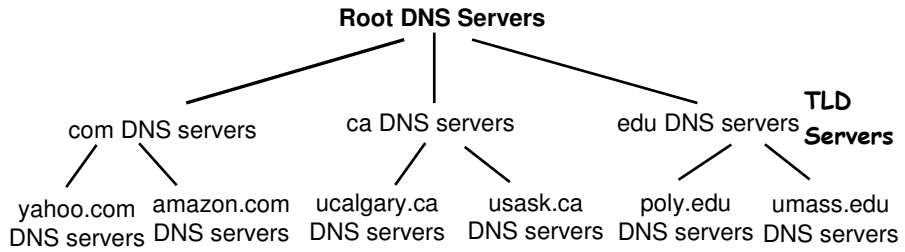
Arhitectura DNS

- Host cis.poly.edu doreşte adresa IP a hostului gaia.cs.umass.edu
- Infrastructura:
  - Client resolver
  - Local DNS server
  - Authoritative DNS Server
  - Root DNS Server
  - Top-Level Domain DNS Server
- exemplul este *iterativ*

(interogare servere multiple)

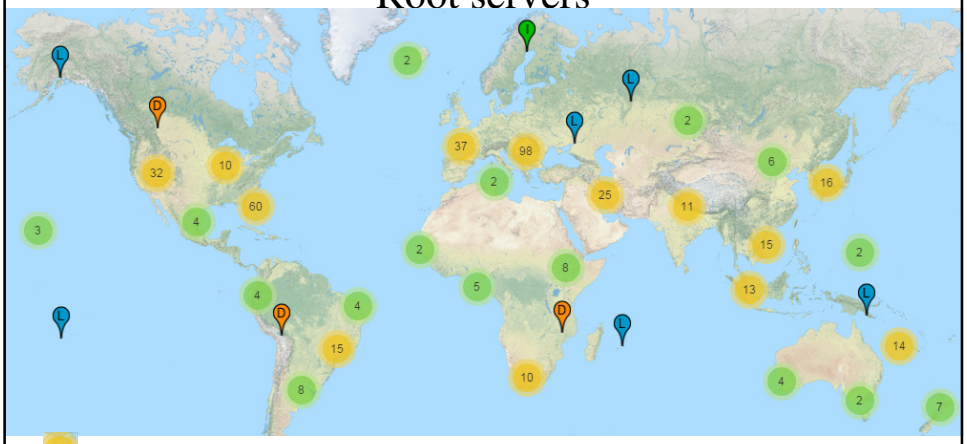


Arhitectura DNS

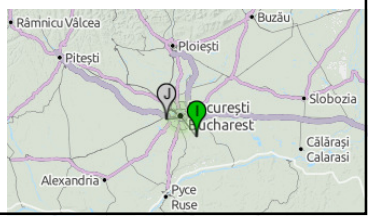


- Arhitectură ierarhică
- root DNS servers nu au înregistrări de host, ci doar de servere autoritative pt. TLD
- TLD = Top-Level Domain (.com, .edu, .gov etc)
- ccTLD = country-code TLD (.ro, .ca, .fr etc)

Root servers



- 10 = 10 servere (se poate detalia)
- A.root-servers.net ... M.root-servers.net (13 servere, dar fiecare are multe instanţe)
- sute de servere în total (multi-homed)
- o instanţă a I.root-servers.net şi una J.root-servers.net în Ro



root servers: fişierul *named.root* (parţial)

```
.                       3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.     3600000      AAAA  2001:503:BA3E::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     192.228.79.201
;
; FORMERLY C.PSI.NET
;
.                       3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     3600000      A     192.33.4.12
;
; FORMERLY TERP.UMD.EDU
;
.                       3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.     3600000      A     128.8.10.90
;
; FORMERLY NS.NASA.GOV
;
.                       3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.     3600000      A     192.203.230.10
;
; FORMERLY NS.ISC.ORG
;
.                       3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     3600000      A     192.5.5.241
F.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:2F::F
```

domeniul .in-addr.arpa

- pînă acum: translaţie nume → adresă
- invers (*reverse lookup*): translaţie adresă → nume

- exemplu: cine are adresa 141.85.43.10 ?
- răspuns: www.elcom.pub.ro

- .ro este TLD cel mai din *dreapta*
- 141. este octetul cel mai semnificativ, cel mai din *stînga*

- deci, scris ca DNS:
  - domeniul de top va fi .141
  - sub el va fi .85.141 (domeniul pentru care NS de la UPB este autoritativ)
  - sub el va fi .43.85.141 (domeniul pentru care NS de la *elcom* este autoritativ)
  - hostul va fi 10.43.85.141
  - toate sînt sub TLD numit .in-addr.arpa
  - **hostul este 10.43.85.141.in-addr.arpa.**

autoritativ vs. *non-autoritativ*

- autoritativ: un server întoarce un răspuns din baza sa de date
- non-autoritativ: un server întoarce un răspuns primit printr-o altă interogare DNS
- Exemplu: (program de interogare manuală: *nslookup*)

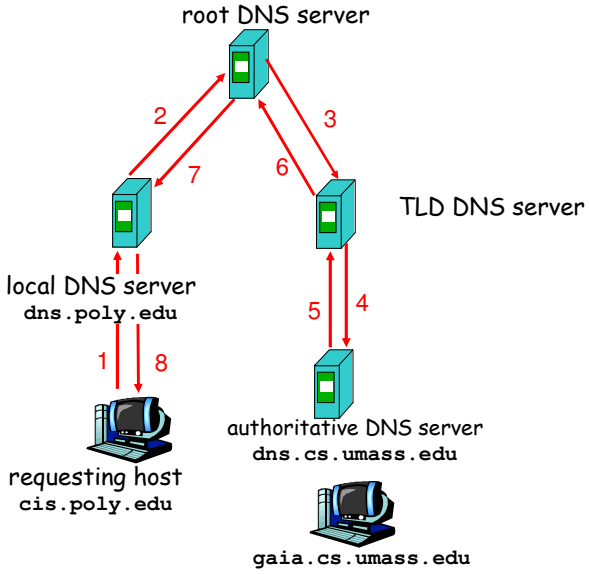
```
root@matrix:~# nslookup
> www.elcom.pub.ro
Server:         141.85.43.10
Address:        141.85.43.10#53

Name:   www.elcom.pub.ro
Address: 141.85.43.10
> www.yahoo.com
Server:         141.85.43.10
Address:        141.85.43.10#53

Non-authoritative answer:
www.yahoo.com   canonical name = fd-fp3.wg1.b.yahoo.com.
Name:   fd-fp3.wg1.b.yahoo.com
Address: 46.228.47.114
Name:   fd-fp3.wg1.b.yahoo.com
Address: 46.228.47.115
```

recursiv vs. *iterativ*

- recursiv: serverul local rezolvă cererea pînă la capăt, interogînd cîte servere e nevoie
- dezavantaj: încărcare mare
- iterativ: serverul local întoarce adresa unui alt server din lanţ, în loc de răspuns (în afara cazului cînd e autoritativ)
- întotdeauna o cerere către root server este iterativă, la fel şi pt. TLD servers



exemplu recursiv (de comparat cu cel iterativ)

exemplu de *dns query*, p. 1

- Exemplu: (program de interogare manuală: *dig*)

```
root@matrix:~# dig +trace www.harvard.edu

; <<>> DiG 9.8.1-P1 <<>> +trace www.harvard.edu
;; global options: +cmd
.                       21926   IN      NS      c.root-servers.net.
.                       21926   IN      NS      f.root-servers.net.
.                       21926   IN      NS      j.root-servers.net.
.                       21926   IN      NS      l.root-servers.net.
.                       21926   IN      NS      a.root-servers.net.
.                       21926   IN      NS      g.root-servers.net.
.                       21926   IN      NS      m.root-servers.net.
.                       21926   IN      NS      d.root-servers.net.
.                       21926   IN      NS      h.root-servers.net.
.                       21926   IN      NS      k.root-servers.net.
.                       21926   IN      NS      b.root-servers.net.
.                       21926   IN      NS      e.root-servers.net.
.                       21926   IN      NS      i.root-servers.net.
;; Received 496 bytes from 141.85.43.10#53(141.85.43.10) in 14 ms
```

exemplu de *dns query*, p. 2

```
;; Received 496 bytes from 141.85.43.10#53(141.85.43.10) in 14 ms

edu.                    172800  IN      NS      a.edu-servers.net.
edu.                    172800  IN      NS      c.edu-servers.net.
edu.                    172800  IN      NS      d.edu-servers.net.
edu.                    172800  IN      NS      f.edu-servers.net.
edu.                    172800  IN      NS      g.edu-servers.net.
edu.                    172800  IN      NS      l.edu-servers.net.
;; Received 268 bytes from 198.41.0.4#53(198.41.0.4) in 388 ms

harvard.edu.            172800  IN      NS      externaldns-c1.harvard.edu.
harvard.edu.            172800  IN      NS      externaldns-c2.harvard.edu.
harvard.edu.            172800  IN      NS      externaldns-c3.br.harvard.edu.
;; Received 171 bytes from 192.42.93.30#53(192.42.93.30) in 193 ms

www.harvard.edu.        300     IN      CNAME   d1mldapedjoasw.cloudfront.net.
;; Received 76 bytes from 128.119.3.185#53(128.119.3.185) in 121 ms

root@matrix:~#
```

DNS caching

- un NS introduce în cache orice *mapping* rezolvat
  - intrările în cache dispar după un timp
  - timpul de cache = cîmpul TTL din înregistrarea autoritativă (configurat de administratorul fiecărui domeniu)
  - serverele TLD se află, tipic, mereu în cache-ul serverelor locale
  - root-servers TTL = 3600000 sec = 1000 ore
    - consecinţă: root-servers interogate rar

Înregistrări DNS

DNS: resource records (RR)

RR format: **(name, value, type, ttl)**

- Type=A
  - **name** is hostname
  - **value** is IP address
- Type=AAAA
  - **name** is hostname
  - **value** is IPv6 address
- Type=NS
  - **name** is domain (e.g. foo.com)
  - **value** is IP address of authoritative name server for this domain
- Type=CNAME
  - **name** is alias name for some "cannonical" (the real) name `www.ibm.com` is really `servereast.backup2.ibm.com`
  - **value** is cannonical name
- Type=MX
  - **value** is name of mailserver associated with **name**

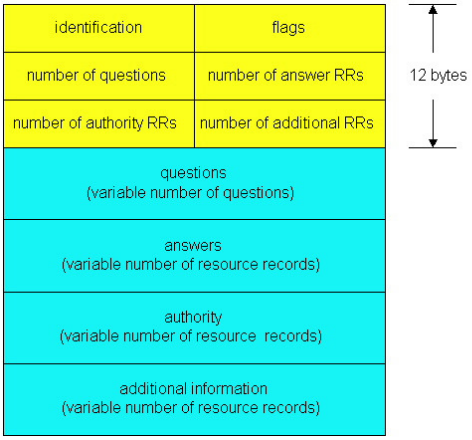
Vezi *exemple* în fişierele de configurare pentru *company.com*

Protocolul DNS; mesaje

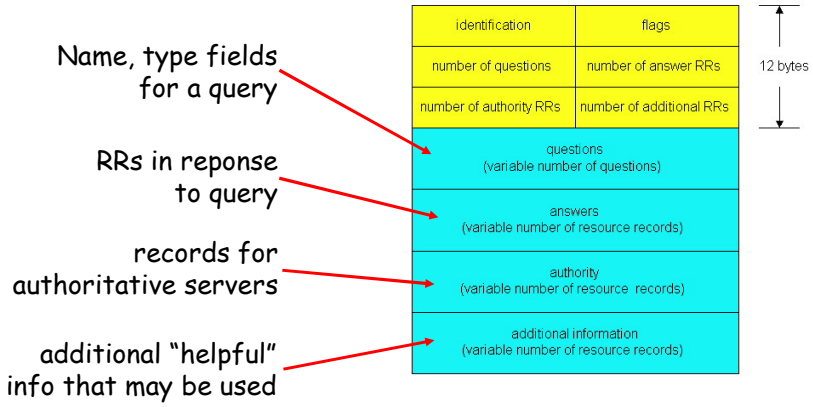
- protocol UDP, port 53
- acelaşi format de mesaje pentru *query* şi *reply*

msg header

- identification: număr pe 16 biţi pt. cerere; răspunsul conţine acelaşi număr
- flags:
  - *query* or *reply*
  - recursion desired
  - recursion available
  - reply is authoritative



Mesaje DNS



Mesaje protocol DNS (1)

```
root@matrix:~# dig www.harvard.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13115
;; flags: qr rd ra; QUERY: 1, ANSWER: 9, AUTHORITY: 4,
   ADDITIONAL: 4
;; QUESTION SECTION:
;www.harvard.edu.                IN      A
;; ANSWER SECTION:
www.harvard.edu.         77      IN      CNAME
   d1mldapedjoasw.cloudfront.net.
d1mldapedjoasw.cloudfront.net. 60 IN     A       54.230.129.64
d1mldapedjoasw.cloudfront.net. 60 IN     A       54.230.129.116
d1mldapedjoasw.cloudfront.net. 60 IN     A       54.230.130.68
d1mldapedjoasw.cloudfront.net. 60 IN     A       54.230.130.140
d1mldapedjoasw.cloudfront.net. 60 IN     A       54.230.130.181
d1mldapedjoasw.cloudfront.net. 60 IN     A       54.240.184.147
d1mldapedjoasw.cloudfront.net. 60 IN     A       54.230.128.23
```

Mesaje protocol DNS (2)

```
d1mldapedjoasw.cloudfront.net. 60 IN    A       54.230.128.52
;; AUTHORITY SECTION:
d1mldapedjoasw.cloudfront.net. 1608 IN  NS      ns-971.awsdns-
  57.net.
d1mldapedjoasw.cloudfront.net. 1608 IN  NS      ns-1225.awsdns-
  25.org.
d1mldapedjoasw.cloudfront.net. 1608 IN  NS      ns-1641.awsdns-
  13.co.uk.
d1mldapedjoasw.cloudfront.net. 1608 IN  NS      ns-261.awsdns-
  32.com.
;; ADDITIONAL SECTION:
ns-261.awsdns-32.com.   95796   IN      A       205.251.193.5
ns-971.awsdns-57.net.   114924  IN      A       205.251.195.203
ns-1225.awsdns-25.org.  23268   IN      A       205.251.196.201
ns-1641.awsdns-13.co.uk. 165200 IN      A       205.251.198.105
;; Query time: 200 msec
;; SERVER: 141.85.43.10#53(141.85.43.10)
;; WHEN: Tue Mar 17 13:12:34 2015
;; MSG SIZE  rcvd: 405
```

Mesaje protocol DNS (3)

```
root@matrix:~# tcpdump -n -s 0 port 53
13:09:39.723245 IP 141.85.43.58.58643 > 141.85.43.10.53:
  30881+ A? www.harvard.edu. (33)
13:09:39.723726 IP 141.85.43.10.53 > 141.85.43.58.58643:
  30881 9/4/4 CNAME d1mldapedjoasw.cloudfront.net., A
  54.230.128.209, A 54.230.129.113, A 54.230.130.170, A
  54.230.131.17, A 54.240.184.74, A 54.240.184.101, A
  54.240.184.182, A 54.230.128.5[…](405)
```

Sintaxa tcpdump request DNS:

```
src > dst: id op? flags qtype qclass name (len)
+ = recursion desired
```

Sintaxa tcpdump reply DNS:

```
src > dst:  id op rcode flags a/n/au type class data (len)
a/n/au = nr. de raspunsuri, nr. de inregistari NS si nr.
  de raspunsuri suplimentare (9/4/4)
```

Exemplu de configurare

Fişierele de configurare BIND (*Berkeley Internet Name Domain)* pentru NS-ul domeniului *company.com*

- /etc/named.conf
- /etc/named.boot
- /etc/domain/localhost
- /etc/domain/127.0.0
- /etc/domain/company.com
- /etc/domain/192.168.42

- /etc/resolv.conf (pe orice PC, nu doar pe NS)

/etc/named.conf

```
// This is an example of a name server configuration for BIND version 8.

// This is the directory where the rest of the files reside.
options {
directory "/etc/domain";
};

zone "." {
type hint;
file "named.root"; // This file should be picked up from
}; // ftp://ftp.rs.internic.net/domain/named.root

zone "localhost" {
type master;
file "localhost";
};

zone "0.0.127.in-addr.arpa" {
type master;
file "127.0.0";
};

zone "company.com" {     // The file "company.com" should reside in
type master;             // the /etc/domain/ directory, and you
file "company.com";      // have to create it yourself.
};

zone "42.168.192.in-addr.arpa" { // The file "192.168.42" should reside in
type master;                     // the /etc/domain/ directory, and you
file "192.168.42";               // have to create it yourself.
};
```

/etc/named.boot

```
directory /etc/domain

cache . named.root
; This file should be picked up from
; ftp://ftp.rs.internic.net/domain/named.
root

primary localhost localhost
primary 0.0.127.in-addr.arpa 127.0.0

;------------------------------------------------------------------

primary company.com company.com
; The file "company.com" should reside in
; the /etc/domain/ directory, and you
; have to create it yourself.

;------------------------------------------------------------------
; This is the part of the DNS database that will translate your IP

primary 42.168.192.in-addr.arpa 192.168.42
; The file "192.168.42" should reside in
; the /etc/domain/ directory, and you
; have to create it yourself.
```

/etc/domain/localhost

```
; The serial number was generated in the year 1998, month 09
; (September), the 29th day of the month, and it was the first version
; (00) that day.

; If you change this file, you must restart the "named" process.

localhost. SOA dns.company.com. hostmaster.company.com. (
1998092900 ; Serial number
86400 ; Refresh 1 day
7200 ; Retry 2 hours
3600000 ; Expire 41.67 days
172800 ) ; Minimum TTL 2 days

localhost. NS dns.company.com.

localhost. A 127.0.0.1
```

OBS: SOA = Start Of Authority

/etc/domain/127.0.0

```
0.0.127.in-addr.arpa. SOA dns.company.com. hostmaster.company.com. (
1998092900 ; Serial number
86400 ; Refresh 1 day
7200 ; Retry 2 hours
3600000 ; Expire 41.67 days
172800 ) ; Minimum TTL 2 days

0.0.127.in-addr.arpa. NS dns.company.com.

1.0.0.127.in-addr.arpa. PTR localhost.
```

/etc/domain/company.com

```
company.com. SOA dns.company.com. hostmaster.company.com. (
1998092900 ; Serial number
86400 ; Refresh 1 day
7200 ; Retry 2 hours
3600000 ; Expire 41.67 days
172800 ) ; Minimum TTL 2 days

company.com. NS dns.company.com.
; This is the hostname of your name server.

company.com. NS ns2.isp.net.
; This is the hostname of a slave name server.

company.com. MX 0 mailserver.company.com.
; This is the hostname of your mailserver;

; The following is the list of computers at your site

dns.company.com. A 192.168.42.2
mailserver.company.com. A 192.168.42.3
computer1.company.com. A 192.168.42.12
server-nt.company.com. A 192.168.42.17
www.company.com. A 192.168.42.33
pc1.company.com. A 192.168.42.51
pc2.company.com. A 192.168.42.52
pc3.company.com. A 192.168.42.53
macserver.company.com. A 192.168.42.217
```

/etc/domain/192.168.42

```
42.168.192.in-addr.arpa. SOA dns.company.com. hostmaster.company.com. (
1998092900 ; Serial number
86400 ; Refresh 1 day
7200 ; Retry 2 hours
3600000 ; Expire 41.67 days
172800 ) ; Minimum TTL 2 days

42.168.192.in-addr.arpa. NS dns.company.com.
; This is the hostname of your name server.

42.168.192.in-addr.arpa. NS ns2.isp.net.
; This is the hostname of a slave name server.


; The following is the list of computers at your site.
2.42.168.192.in-addr.arpa. PTR dns.company.com.
3.42.168.192.in-addr.arpa. PTR mailserver.company.com.
12.42.168.192.in-addr.arpa. PTR computer1.company.com.
17.42.168.192.in-addr.arpa. PTR server-nt.company.com.
33.42.168.192.in-addr.arpa. PTR www.company.com.
51.42.168.192.in-addr.arpa. PTR pc1.company.com.
52.42.168.192.in-addr.arpa. PTR pc2.company.com.
53.42.168.192.in-addr.arpa. PTR pc3.company.com.
217.42.168.192.in-addr.arpa. PTR macserver.company.com.
```

/etc/resolv.conf

```
# /etc/resolv.conf
search company.com
nameserver 192.168.42.2
nameserver 4.4.4.4
nameserver 8.8.8.8
```

OBS: /etc/resolv.conf nu face parte din configurarea nameserverului, ci a resolverului; se va afla pe TOATE calculatoarele din domeniu, nu doar pe nameserver.

Bibliografie

- *Computer Networking: A Top Down Approach Featuring the Internet*, 3rd edition, Jim Kurose, Keith Ross Addison-Wesley, 2005
- RFCs 882, 883, 1034, 1035
- exemplu: `https://www.ripe.net/ripe/docs/ripe-192`