Domain Name System (DNS)

Petr Grygárek

Domain Name System

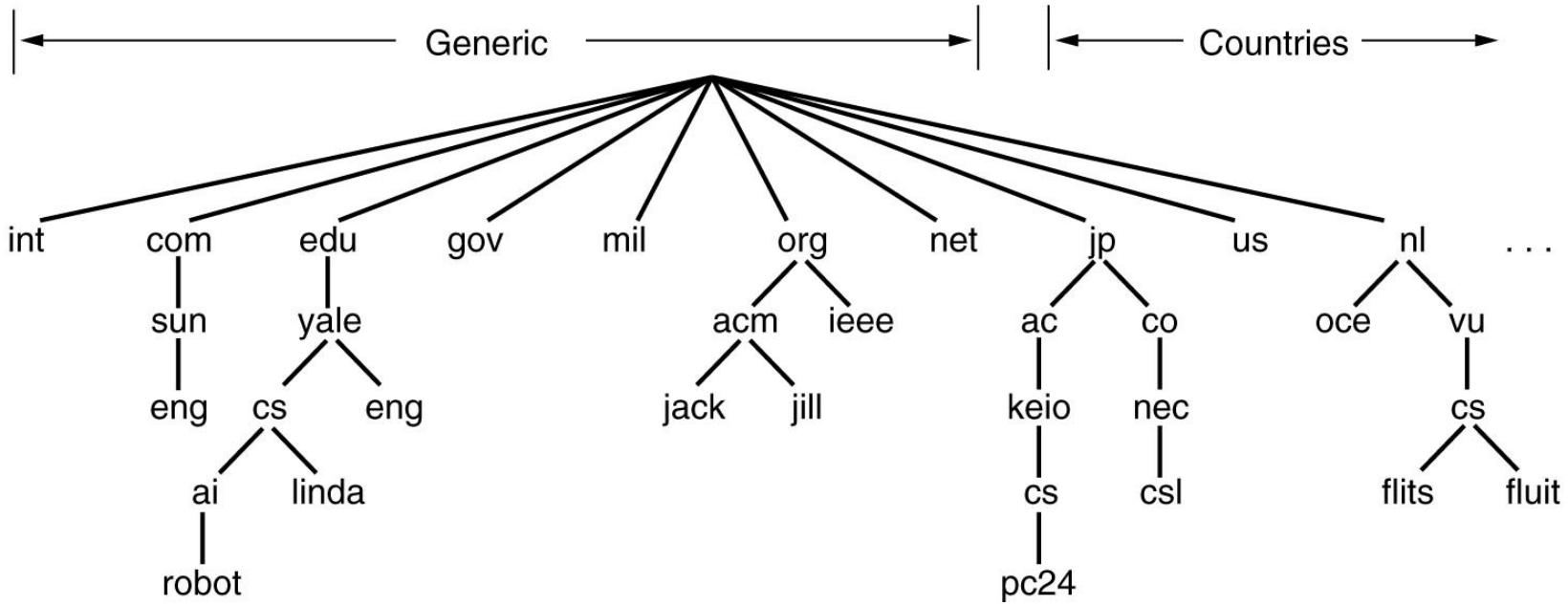
- jmenná služba používaná v Internetu
- mapování logických ("doménových") jmen na IP adresy
  - (a další mapování)
- RFC 1034, 1035 definují koncepci, jmenný prostor a protokol klient(resolver)-server, (resp. server-server)
- využívá distribuovanou databázi, DNS servery
  - ("name servery", "jmenné servery")

Doménová jména

- hierarchická (stromová) struktura jmenného prostoru
  - každý uzel lze identifikovat doménovým jménem
  - doména - skupina jmen se společnou pravou stranou
  - kořenem stromu doména "."
- doménové jméno vytvořeno spojením jména uzlu stromu se všemi jmény uzlů na cestě ke kořeni, oddělovačem tečka
  - délka komponenty max. 63 znaků
  - celková délka jména max. 256 znaků
  - case insensitive
  - dnes snahy o rozšíření použitelné znakové sady (používat s rozmyslem !)

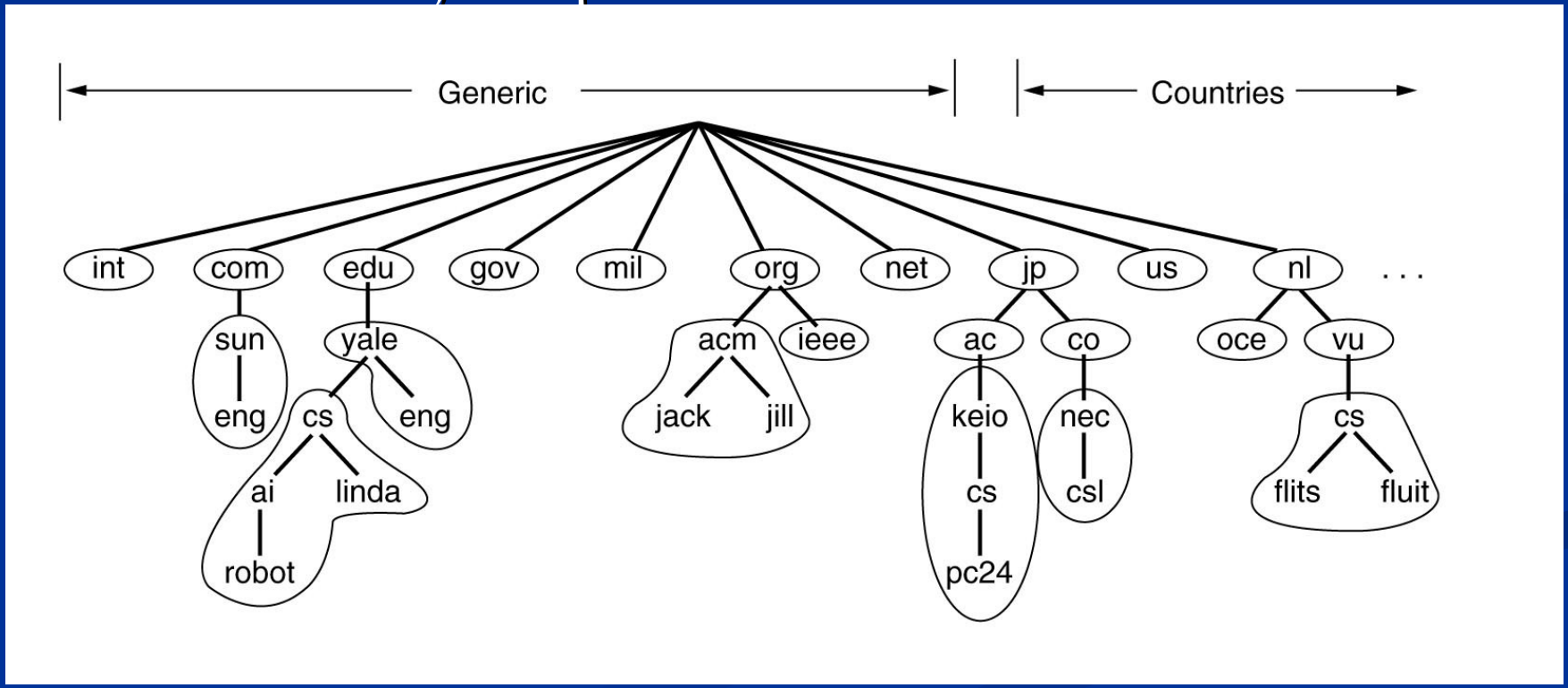
Strom doménových jmen

- domény nejvyšší úrovně:
  - generické domény: .edu, .com, .mil, .gov, .net, .org
  - označení států: .cz, .uk, .at, ...



Zóna

- část stromu uložená na jednom DNS serveru (a spravovaná separátně)
- DNS server je autoritativní pro domény obsažené v jím spravované zóně



Vyhledávání v DNS databázi

- Provádí SW klienta („resolver“) nebo rekurzivní DNS server
- Po komponentech jména, začíná se od root serverů
  - Jejich adresy nakonfigurovány pevně v DNS resolverech
- Při dotazu na jméno, které není pod správou dotazovaného NS:
  - Odmítnutí dotazu
  - Rekurzivní vyhledání a neautoritativní odpověď

Primární a sekundární name servery

- Data zóny permanentně uložena v souborech na primárním serveru
  - sekundární servery periodicky testují u primárního, zda mají aktuální verzi DB; pokud ne, vyžádají transfer databáze od primárního serveru ("zone transfer")
    - při změnách v DB na primárním NS nutno změnit číslo verze (detekce změny zvýšením čísla)
  - Odpověď primárního i sekundárního NS autoritativní
- caching-only DNS servery - nejsou autoritou pro žádnou doménu, jen provádějí rekurzivní překlad a caching

Resolver

- Část SW klienta, který provádí komunikaci s DNS serverem
- Konfigurace:
  - default domain pro relativní jména
  - první a záložní (rekurzivní) jmenné servery
  - u některých systému, které provádějí vyhledání samy, konfigurace seznamu kořenových jmenných serverů

Komunikační protokol DNS

- Resolver - jmenný server
- Jmenný server - jmenný server

- Běžné dotazy a odpovědi nad UDP (port 53)
- Dlouhá data a transfer zóny z primárního na sekundární server nad TCP (port 53)

Záznamy databáze DNS (Resource Records)

- univerzální formát
  - Doménové jméno
  - Typ záznamu
  - Data proměnné délky
    - Interpretace rozdílná podle typu záznamu
  - Time to live
    - doba, po kterou se záznam smí držet v cache klientů (typicky hodiny až dny)
    - při změně záznamu v DNS může trvat hodiny až dny, než se projeví v celém Internetu

Nejdůležitější typy záznamů DNS

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

Příklad konfiguračního souboru DNS serveru

```
; Authoritative data for cs.vu.nl
cs.vu.nl.        86400   IN  SOA     star boss (952771,7200,7200,2419200,86400)
cs.vu.nl.        86400   IN  TXT     "Divisie Wiskunde en Informatica."
cs.vu.nl.        86400   IN  TXT     "Vrije Universiteit Amsterdam."
cs.vu.nl.        86400   IN  MX      1 zephyr.cs.vu.nl.
cs.vu.nl.        86400   IN  MX      2 top.cs.vu.nl.

flits.cs.vu.nl.  86400   IN  HINFO   Sun Unix
flits.cs.vu.nl.  86400   IN  A       130.37.16.112
flits.cs.vu.nl.  86400   IN  A       192.31.231.165
flits.cs.vu.nl.  86400   IN  MX      1 flits.cs.vu.nl.
flits.cs.vu.nl.  86400   IN  MX      2 zephyr.cs.vu.nl.
flits.cs.vu.nl.  86400   IN  MX      3 top.cs.vu.nl.
www.cs.vu.nl.    86400   IN  CNAME   star.cs.vu.nl
ftp.cs.vu.nl.    86400   IN  CNAME   zephyr.cs.vu.nl

rowboat                  IN  A       130.37.56.201
                         IN  MX      1 rowboat
                         IN  MX      2 zephyr
                         IN  HINFO   Sun Unix

little-sister            IN  A       130.37.62.23
                         IN  HINFO   Mac MacOS

laserjet                 IN  A       192.31.231.216
                         IN  HINFO   "HP Laserjet IIISi" Proprietary
```

Konvence zónového souboru

- @ - implicitní doména
- Pokud v levé části vypuštěno jméno, bere se to z minulého řádku
- Jména neukončená tečkou jsou relativní a doplňují se hodnotou direktivy $ORIGIN
- Direktivou $TTL lze stanovit implicitní hodnotu pro Time to live.

Propojení jmenných serverů (příklad pro www.vsb.cz)

V databázi DNS (všech) root serverů:

cz.	NS	dns-server.eunet.cz.
dns-server.eunet.cz.	A	120.0.1.2

V databázi DNS serveru dns-server.eunet.cz:

vsb.cz.	NS	dns.vsb.cz.
dns.vsb.cz.	A	158.196.1.100

V databázi DNS serveru dns.vsb.cz:

www.vsb.cz.	A	158.196.1.200

Reverzní domény

- mapování IP adres na doménová jména
- doména **in-addra.arpa.**, pak rozděleno na NS nižších úrovní po bajtech IP adresy (od nejvyššího řádu)
- tyto NS provozují kontinentální správní organizace, poskytovatelé a jednotlivé organizace
- Delegují se reverzní domény pro adresy třídy B (velké organizace a poskytovatelé) a třídy C

Příklad:

Doménové jméno pro záznam k reverznímu překladu adresy 158.196.146.10 je 10.146.196.158.in-addr.arpa.

Delegace reverzních domén u beztřídních adres

- RFC 2317 (1998)
- Řeší problém, kdy při každé změně PTR záznamu je třeba kontaktovat poskytovatele, který provozuje DNS server reverzní domény pro všechny své podsítě
  - tedy v podstatě při každé změně jména stroje nebo zavedení nového stroje (A a PTR záznamy musí párovat)
- Řeší se odkazy (alias - CNAME) z DNS serveru reverzní domény poskytovatele pro všechny adresy podsítě na speciální jméno domény na DNS serveru zákazníka

Praktické příklady

Příklad 1
Nalezení jména homel.vsb.cz.

1. Kdo je zodpovědný za doménu . ?

```
dig -t NS .

;; ANSWER SECTION:
.                    457010   IN      NS      A.ROOT-SERVERS.NET.
.                     57010   IN      NS      B.ROOT-SERVERS.NET.
.                    457010   IN      NS      C.ROOT-SERVERS.NET.
   …
.                    457010   IN      NS      M.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.     126521   IN      A       198.41.0.4
B.ROOT-SERVERS.NET.     558521   IN      A       192.228.79.201
C.ROOT-SERVERS.NET.     558521   IN      A       192.33.4.12
   …
M.ROOT-SERVERS.NET.     558522   IN      A       202.12.27.33
```

2. Kdo je zodpovědný za doménu cz. ?

```
dig @A.ROOT-SERVERS.NET. -t NS cz

;; ANSWER SECTION:
cz.                     172800  IN      NS      SUNIC.SUNET.SE.
cz.                     172800  IN      NS      NS-EXT.VIX.COM.
cz.                     172800  IN      NS      NS.TLD.cz.
cz.                     172800  IN      NS      NSS.TLD.cz.
cz.                     172800  IN      NS      NS-CZ.RIPE.NET.
cz.                     172800  IN      NS      NS2.NIC.FR.

;; ADDITIONAL SECTION:
SUNIC.SUNET.SE.         172800  IN      A       192.36.125.2
NS-EXT.VIX.COM.         172800  IN      A       204.152.184.64
NS.TLD.cz.              172800  IN      A       217.31.196.10
NSS.TLD.cz.             172800  IN      A       217.31.200.10
NS-CZ.RIPE.NET.         172800  IN      A       193.0.12.60
NS2.NIC.FR.             172800  IN      A       192.93.0.4
```

3. Kdo je zodpovědný za doménu vsb.cz. ?

```
dig @sunic.sunet.se. -t NS vsb.cz.

;; ANSWER SECTION:
vsb.cz.                 25493   IN      NS      decsys.vsb.cz.
vsb.cz.                 25493   IN      NS      ns.ces.net.

;; ADDITIONAL SECTION:
ns.ces.net.             108971  IN      A       195.113.144.233
decsys.vsb.cz.          25493   IN      A       158.196.149.9
```

4. Zeptáme se na homel.vsb.cz

```
dig @decsys.vsb.cz -t A homel.vsb.cz.
```

(technická poznámka: někdy je vhodné uvést jméno NS adresou - @158.196.149.9 (problémy s IPv6 adresami a záznamy AAAA))

```
;; ANSWER SECTION:
homel.vsb.cz.          86400   IN      A       158.196.149.49

;; AUTHORITY SECTION:
vsb.cz.                86400   IN      NS      ns.ces.net.
vsb.cz.                86400   IN      NS      decsys.vsb.cz.

;; ADDITIONAL SECTION:
ns.ces.net.            86400   IN      A     195.113.144.233
decsys.vsb.cz.         86400   IN      A     158.196.149.9
```

Příklad 2
Reverzní překlad adresy 158.196.149.79

Formulace dotazu

Budeme se ptát na jméno
79.149.196.158.in-addr.arpa.

a typ záznamu PTR.

1. Kdo je zodpovědný za doménu . ?

```
dig -t NS .

;; ANSWER SECTION:
.                   457010  IN      NS      A.ROOT-SERVERS.NET.
.                    57010  IN      NS      B.ROOT-SERVERS.NET.
.                   457010  IN      NS      C.ROOT-SERVERS.NET.
   …
.                   457010  IN      NS      M.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.     126521  IN      A       198.41.0.4
B.ROOT-SERVERS.NET.     558521  IN      A       192.228.79.201
C.ROOT-SERVERS.NET.     558521  IN      A       192.33.4.12
   …
M.ROOT-SERVERS.NET.     558522  IN      A       202.12.27.33
```

2. Kdo je zodpovědný za doménu arpa. ?

```
dig @A.ROOT-SERVERS.NET -t NS arpa.

;; ANSWER SECTION:
arpa.           518400  IN      NS      A.ROOT-SERVERS.NET.
arpa.           518400  IN      NS      B.ROOT-SERVERS.NET.
…
arpa.           518400  IN      NS      M.ROOT-SERVERS.NET.


;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.     3600000 IN      A   198.41.0.4
B.ROOT-SERVERS.NET.     3600000 IN      A   192.228.79.201
…
M.ROOT-SERVERS.NET.     3600000 IN      A   202.12.27.33
```

3. Kdo je zodpovědný za doménu in-addr.arpa. ?

```
dig @A.ROOT-SERVERS.NET -t NS in-addr.arpa.

;; ANSWER SECTION:
arpa.           518400  IN      NS      A.ROOT-SERVERS.NET.
arpa.           518400  IN      NS      B.ROOT-SERVERS.NET.
…
arpa.           518400  IN      NS      M.ROOT-SERVERS.NET.


;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.     3600000 IN      A   198.41.0.4
B.ROOT-SERVERS.NET.     3600000 IN      A   192.228.79.201
…
M.ROOT-SERVERS.NET.     3600000 IN      A   202.12.27.33
```

4. Kdo je zodpovědný za doménu 158.in-addr.arpa ?

```
dig @A.ROOT-SERVERS.NET -t NS 158.in-addr.arpa

;; ANSWER SECTION:
158.in-addr.arpa.    86400    IN       NS    indigo.ARIN.NET.
158.in-addr.arpa.    86400    IN       NS    epazote.ARIN.NET.
158.in-addr.arpa.    86400    IN       NS    figwort.ARIN.NET.
158.in-addr.arpa.    86400    IN       NS    chia.ARIN.NET.
158.in-addr.arpa.    86400    IN       NS    dill.ARIN.NET.
158.in-addr.arpa.    86400    IN       NS    BASIL.ARIN.NET.
158.in-addr.arpa.    86400    IN       NS    henna.ARIN.NET.
```

Všimněte si, že jde o dost dávno přidělený rozsah adres, primární DNS server reverzní domény neprovozuje RIPE, jako např. pro 194.in-addr.arpa.

5. Kdo je zodpovědný za doménu 196.158.in-addr.arpa ?

```
dig @ indigo.ARIN.NET. -t NS 196.158.in-addr.arpa

;; AUTHORITY SECTION:
196.158.in-addr.arpa.   86400   IN    NS    decsys.vsb.cz.
196.158.in-addr.arpa.   86400   IN    NS    ns.ces.net.
196.158.in-addr.arpa.   86400   IN    NS    ns.ripe.net.
```

6. Jaké je jméno k 158.196.149.79 ?

```
dig @decsys.vsb.cz -t PTR 79.149.196.158.in-addr.arpa.

;; ANSWER SECTION:
79.149.196.158.in-addr.arpa. 86400 IN   PTR     webmel.vsb.cz.

;; AUTHORITY SECTION:
196.158.in-addr.arpa.   86400   IN      NS      decsys.vsb.cz.
196.158.in-addr.arpa.   86400   IN      NS      ns.ces.net.
196.158.in-addr.arpa.   86400   IN      NS      ns.ripe.net.

;; ADDITIONAL SECTION:
ns.ces.net.             86400   IN      A       195.113.144.233
ns.ripe.net.            66132   IN      A       193.0.0.193
decsys.vsb.cz.          86400   IN      A       158.196.149.9
```

Příklad 3
Delegace beztřídních adres 11.2.3.64/27

Reverzní překlad sítě 11.2.3.64/27

- Poskytovatel: zóna 3.2.11.in-addr.arpa.
  - DNS server odkazovaný ze serveru pro doménu 2.11.in-addr.arpa.

```
65 IN CNAME 65.64.3.2.11.in-addr.arpa.
66 IN CNAME 66.64.3.2.11.in-addr.arpa.
…
94 IN CNAME 94.64.3.2.11.in-addr.arpa.

64 IN NS ns1.customer1-subnet.com.
64 IN NS ns2.customer1-subnet.com.
```

- Zákazník:1 zóna 64.3.2.11.in-addr.arpa.
  - DNS server ns1.customer1-subnet.com, ns2.customer1-subnet.com

```
65 IN PTR a.mydomain.com.
66 IN PTR b.mydomain.com.
…
94 IN PTR x.mydomain.com.
```

Alternativní zápis

- Poskytovatel: zóna 3.2.11.in-addr.arpa.
  - DNS server poskytovatele je odkazovaný ze serveru pro doménu 2.11.in-addr.arpa.
  - Zákazníkovi poskytovatel přidělil síť 11.2.3.0/24, ten ji chce rozdělit na 4 podsítě (lokality) a delegovat na 4 nezávislé DNS servery

```
65 IN CNAME 65.64/27.3.2.11.in-addr.arpa.
66 IN CNAME 66.64/27.3.2.11.in-addr.arpa.
…
94 IN CNAME 94.64/27.3.2.11.in-addr.arpa.

64/27 IN NS ns1.customer1-subnetA.com.
64/27 IN NS ns2.customer1-subnetA.com.
```

(podobně pro další podsítě)

- Zákazník: zóna 64/27.3.2.11.in-addr.arpa.
  - DNS serveru ns1.customer1-subnetA.com, ns2.customer1-subnetA.com

```
65 IN PTR a.mydomain.com.
66 IN PTR b.mydomain.com.
…
94 IN PTR x.mydomain.com.
```

Návaznost DNS na elektronickou poštu

e-mail: nekdo@domena.com

- MX záznam pro doménové jméno *domena.com* (např. *domena.com MX posta.domena.com*)
  - Lze uvést i více záznamů s různou prioritou
- A záznam pro *posta.domena.com* určí IP adresu této poštovní brány

Dynamická DNS (DDNS)

- RFC 2136
- dynamická DNS, umožňuje dynamické registrování IP adres k doménovým jménům
- užitečné při použití dynamického přidělování adres (DHCP)
- problém s autentizací
- prakticky se zatím příliš nepoužívá