Curs 4
DNS

Gestiunea serviciilor de rețea (GSR)
27 octombrie 2016

Departamentul de Calculatoare, Comunitatea RLUG

Cuprins

DNS — la ce "e bun"

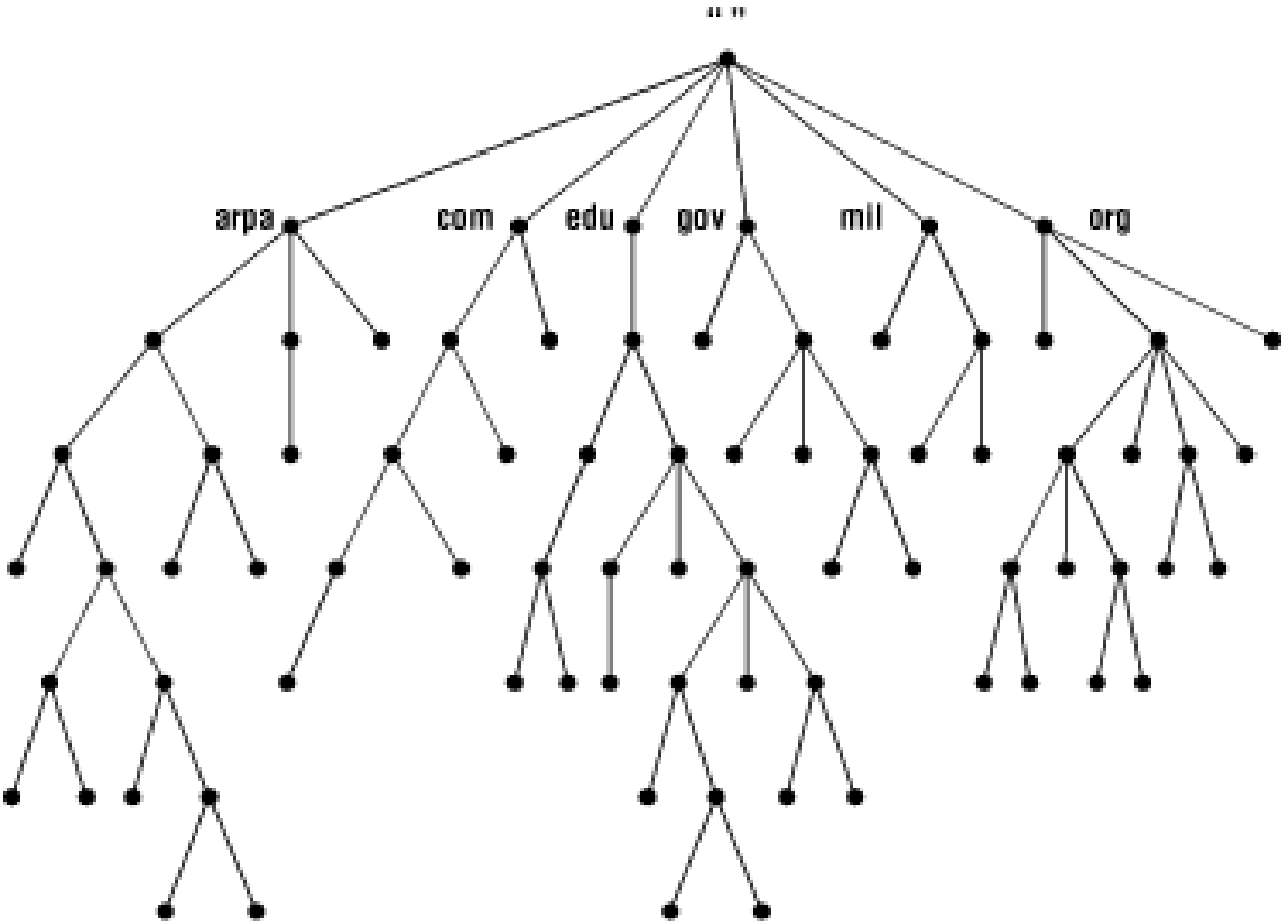
- Face conversia între nume de domenii și adrese IP (`forward`)
  - `cs.pub.ro` ⇒ `141.85.241.52`
- Face conversia între adrese IP și nume (`reverse`)
  - `141.85.241.52` ⇒ `ha-webserver-02-pub.curs.pub.ro.`
- ... sau, altfel spus, decuplează partea de infrastructură față de cea de client

Un pic de istorie: ARPANET, hosts.txt și DNS

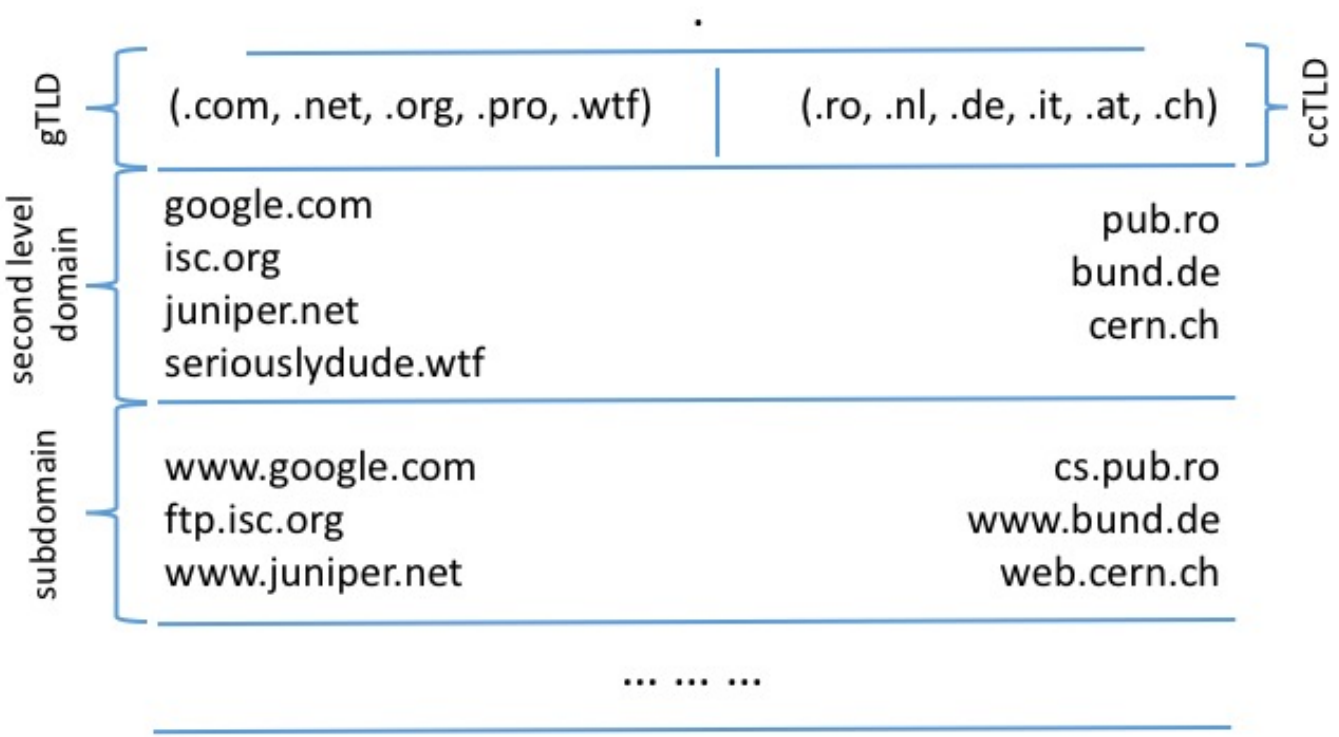
- ARPANET și `hosts.txt` (`http://jim.rees.org/apollo-archive/hosts.txt`)
- `Paul Mockapetris` și `Jon Postel` inventează noțiunea de DNS în 1983
  - `RFC882` și `RFC883`
  - standardul curent este `RFC1035`
  - pe lângă el exista și altele pentru diverse extensii și idei de imbunătățiri
    - `https://www.isc.org/community/rfcs/dns/`

Ierarhia DNS

- DNS este organizat ierarhic și începe de la .



Ierarhia DNS — Exemplu



- Sunt servere globale de DNS responsabile pentru `.`
- `a ... m.root-servers.net`
- Distribuite în toata lumea, fiecare `root server` având aceeași adresă IP, indiferent unde este localizat fizic
- Lista cu locațiile se află la `http://www.root-servers.org`
- `i.root-servers.net` are o instanță și în București

Tipuri de înregistrări DNS

- Informațiile în DNS sunt stocate sub formă de înregistrări numite RR (Resource Records)
- Cele mai des utilizate RR sunt:
  - `SOA` — Start of Authority
  - `NS` — Name Server
  - `A` — Address Record (`glue`)
  - `MX` — Mail Exchanger
  - `CNAME` — Canonical Name Record
  - `PTR` — Pointer Record
- Lista "completă": `https://en.wikipedia.org/wiki/List_of_DNS_record_types`

DNS - zonă de tip forward

Zonă DNS forward (bind)

```
$TTL   86400
@   IN   SOA   ns1.example.com.   hostmaster.example.com.  (
        2016102718 ; serial
        3H ; refresh
        15 ; retry
        1w ; expire
        3h ) ; NXDOMAIN ttl
    IN   NS   ns1.example.com.
    IN   NS   ns2.example.com.
    IN   MX   10 mail1.example.com.
    IN   MX   20 mail2.example.com.
$ORIGIN   example.com.
ns1   IN   A   192.168.1.1
ns2   IN   A   192.168.1.2
www   IN   A   192.168.1.3
ftp   IN   CNAME   www
mail1   IN   A   192.168.1.4
mail2   IN   A   192.168.1.5
```

DNS - zonă de tip reverse

Zonă DNS reverse (bind)

```
$TTL 86400 @   IN   SOA   ns1.example.com.   hostmaster.example.com.  (
        2016102718 ; serial
        3H ; refresh
        1H ; retry
        1W ; expire
        1h ) ; NXDOMAIN ttl
    IN   NS   ns1.example.com.
    IN   NS   ns2.example.com.
$ORIGIN 1.168.192.in-addr.arpa.
1   IN   PTR   ns1.example.com.
2   IN   PTR   ns2.example.com.
3   IN   PTR   www.example.com.
4   IN   PTR   mail1.example.com.
5   IN   PTR   mail2.example.com.
```

DNS resolvers

- Un `resolver` este o `bibliotecă` sau un `program/aplicație` care știe să facă interogari DNS
- Pe Linux, `glibc` vine cu funcționalitate inclusă de `resolver`
  - `/etc/resolv.conf` este fișierul de configurare pentru această bibliotecă
- `BIND`, în configurație specială este folosit ca și resolver recursiv și DNS cache

Propagarea inregistrarilor în DNS

- După efectuarea unor modificări în DNS, trece un timp până când ele sunt vizibile în Internet
- Viteza de propagare depinde de câțiva factori:
  - valoarea `TTL` a înregistrărilor modificate
  - comportamentul resolverelor recursive folosite de clienți
- Când sunt făcute modificări dese în DNS este bine ca `TTL` să fie mic (minim 5m conform RFC)
- Când sunt făcute rar modificări în DNS este bine ca `TTL` să fie mai mare (4/8/12/24h)
- Diferența între un `TTL` mic și un `TTL` mare se vede în volumul de trafic generat de servrele de DNS

DNS Caching

- Pentru micșorarea latenței răspunsurilor și a traficului DNS, serverele de DNS implementează funcționalități de `cache`
- Atunci când un server intermediar primește un răspuns, acesta este ținut în `cache` până la expirarea `TTL`
- Pentru cereri similare pentru aceeași înregistrare, răspunsul va fi servit din `cache`

DNS — MX RR

- Prioritatea MX este invers proporțională cu valoarea trecută în înregistrare

```
IN   MX   10   mail1.example.com
IN   MX   20   mail2.example.com
```

- `mail1` va fi preferat față de `mail2`

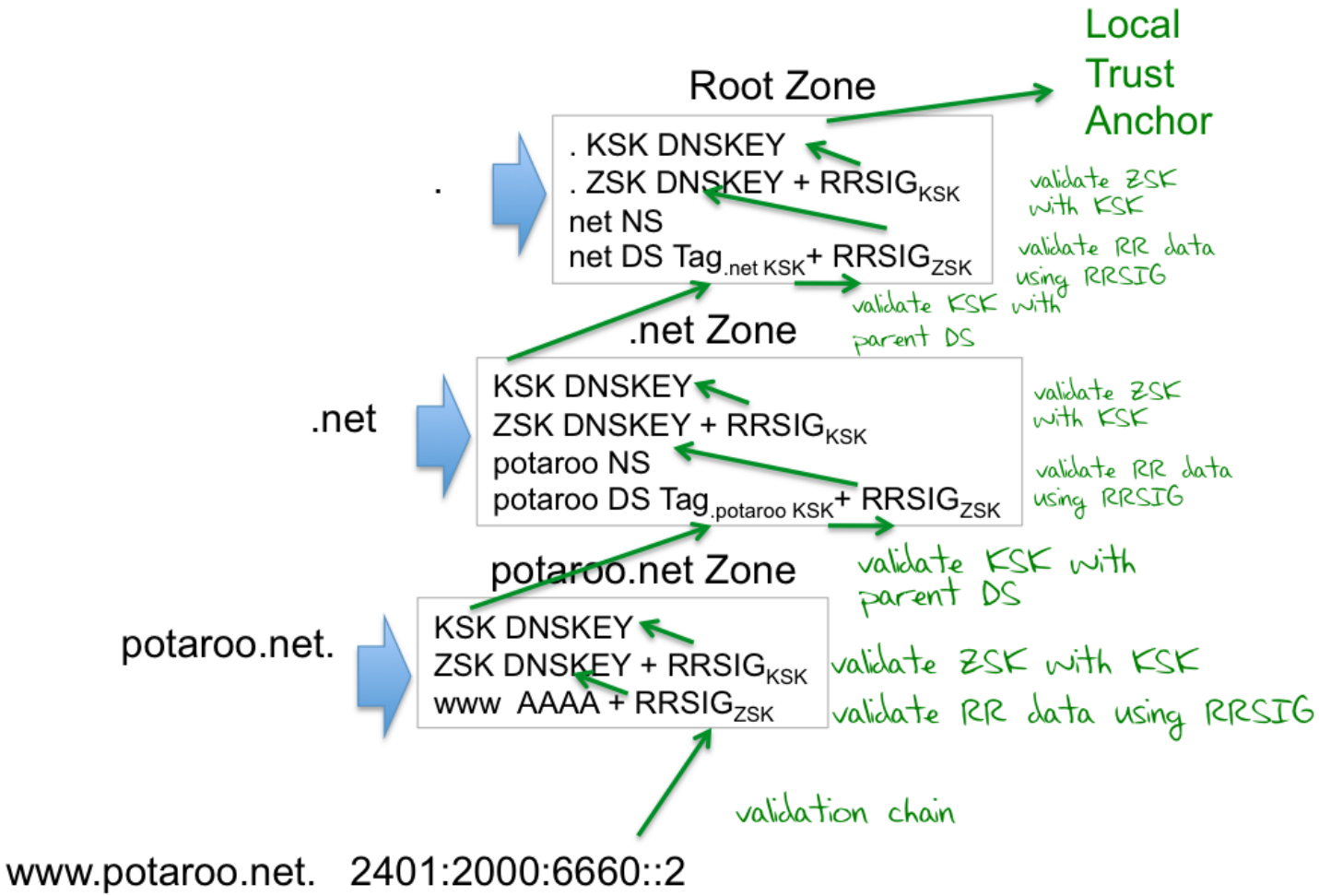
- DNS folosește portul 53, protocol UDP și TCP pentru funcționare
- Uzual, majoritatea cererilor sunt servite folosind UDP
- Mărimea maximă a unui pachet DNS pe UDP nu trebuie sa depășească 512 bytes
- Când se întâmplă acest lucru?
  - Atunci când răspunsul conține un număr mare de înregistrări
- În cazul unui răspuns mai mare de 512 bytes, clientul inițiază o conexiune TCP către serverul DNS și efectuează cererea folosind acest protocol

Cuprins

Despre DNSSEC

- Validarea digitală a înregistrărilor DNS
- Terminologie
  - KSK — Key Signing Key
  - ZSK — Zone Signing Key
  - DS — Delegated Signer
  - RRSIG — Resource Record Signature

DNSSEC — Exemplu



Q&A

Q & A

Cuprins

BIND

- `Daemon` de DNS (rulează pe sisteme sub numele de `named`)
- Este dezvoltat de către ISC (`http://www.isc.org`)
- Poate fi configurat în mod `autoritativ`, `cache` (numit și `resolver recursiv`)
- Fișierul principal de configurare este `/etc/named/named.conf`
- Directorul de configurare al zonelor este `/var/named`

named.conf — master

/etc/named/named.conf

```
options {
  directory "/var/named";
  allow-transfer { "none"; };
  allow-recursion { 192.168.1.0/24; };
};
zone "." {
  type hint;
  file "root.hints";
};
zone "example.com" IN {
  type master;
  file "example.com-zone";
  allow-transfer { 192.168.1.2; };
};
```

named.conf — slave

/etc/named/named.conf

```
options {
  directory "/var/named";
  allow-transfer { "none"; };
  allow-recursion { 192.168.1.0/24; };
};
zone "." {
  type hint;
  file "root.hints";
};
zone "example.com" IN {
  type slave;
  file "example.com-zone";
  masters { 192.168.1.1; };
};
```

Transfer de zone

- Transferul de zone se face din direcția `master` spre `slave` și este inițiat de `slave`
  - `AXFR` — Tranfer complet
    - la primul transfer de zonă între `master` și `slave`
    - atunci când a trecut o perioada mai lungă de timp decât valoarea `expiry` din zonă
  - `IXFR` — Transfer incremental
    - atunci când s-au modificat (adăugat/modificat/șters) una sau mai multe înregistrări
- Transferul de zonă folosește protocolul `TCP` pentru comunicare

Demo

Resurse utile

- https://www.isc.org/community/rfcs/dns/
- https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
- https://kb.isc.org/article/AA-00845/0/BIND-9.9-Administrator-Reference-Manual-ARM.html
- https://www.cloudflare.com/dns/dnssec/how-dnssec-works/