Az Internet DNS: elv és konfiguráció

Pásztor Miklós

2022. június 15.

Tartalomjegyzék

1. A DNS feladata, kialakulása

A feladat

- Az Interneten számok (*IP címek*) azonosítanak gépeket
- Emberek számára ez
  - Nem kifejező
  - Nehezen megjegyezhető

Megoldandó

- *Név* → *Cím* megfeleltetés
  - Haszna: pl. `telnet arizona.edu`
- *Cím* → *Név* megfeleltetés
  - Haszna: pl. `traceroute arizona.edu`

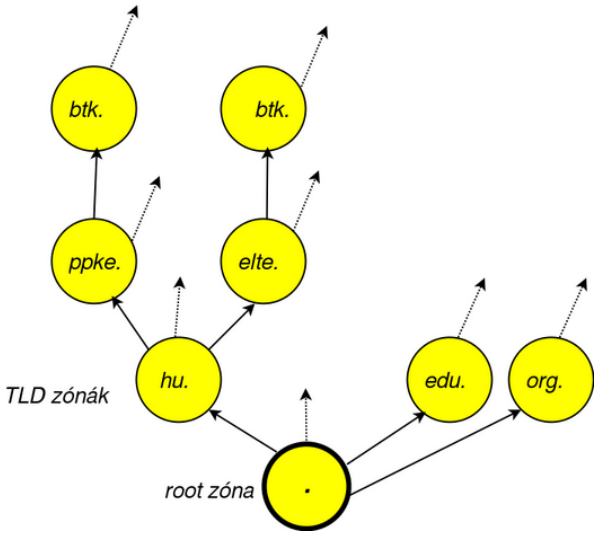
Első megoldás: host táblák

- Központi, szétküldött fájl
- Soronként tartalmaz egy-egy név-IP cím megfeleltetést
- Kezdetben használták
- Nem skálázható: *„does not scale”*
- Máig is él:
  - Unixokon: `/etc/hosts`
  - Windows-okon: `system32\drivers\etc\hosts`
  - Példa: `https://someonewhocares.org/hosts/`

Jelenlegi megoldás: hierarchikus, osztott adatbázis

- A nevek hierarchikusan épülnek fel
- A hierarchia egyes szintjein önállóan döntenek
- Minden szinten tovább lehet delegálni
- A feloldás rekurzívan történik a hierarchián
- Nagyon jól skálázható: ma sok százmilliómillió név, sok százezer névszerver
  - Egyedül a `.com` alatt több mint 159 millió elágazás (delegálás)
- Forrás: `http://www.domaintools.com/statistics/tld-counts/`
- A `https://domainnamestat.com/statistics/tld/others` nagyobb számokat mutat...

Példa



Kitérő: az Internet kezdeteiről, és természetéről. . .

- A 70-es években
  - Amerikai egyetemeken
  - Kreatív, szerény, gyakorlatias hozzáállás
  - *„We reject kings, presidents and voting. We believe in rough consensus and running code."*

Az Internet alapdokumentumai: RFC-k

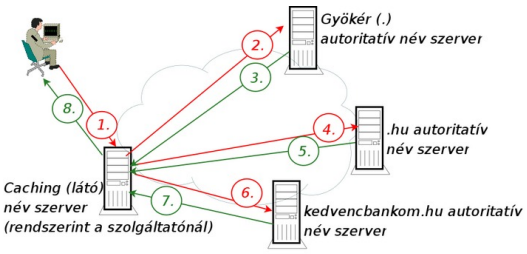
- Request For Comments - RFC
- Az Internet működését leíró szabványok RFC-k
  - Nem minden RFC ilyen
  - Vannak pl. tájékoztató, sőt polemikus és tréfás RFC-k
  - Kibocsátó: IETF (Internet Engineering Task Force)
  - `https://www.ietf.org`
  - (Elő)készítők: munkacsoportok (working groups)
  - *Bárki* bekapcsolódhat

Internet protokollok

- A hálózati elemek beszélgetésének szabályai
  - Réteges építkezés (v.ö. ISO/OSI modell)
  - A protokollokat RFC-k írják le
  - Néha elavulnak - új változatot új RFC ír le
  - Az RFC-k sorszámot kapnak
  - Például: RFC821 → RFC2821 = SMTP, levelező protokoll
  - Internet szabvány feltétel:
    - Legalább 2 független, forráskódban is hozzáférhető implementáció

2. Alapelvek

Név feloldás



1. www.kedvencbankom.hu ?
2. www.kedvencbankom.hu ?
3. Nem tudom, de itt vannak a .hu név szerverei!
4. www.kedvencbankom.hu ?
5. Nem tudom, de itt vannak kedvencbankom.hu név szerverei!
6. www.kedvencbankom.hu ?
7. www.kedvencbankom.hu A rekordja: 111.22.33.44 (autoritatív válasz)
8. www.kedvencbankom.hu A rekordja: 111.22.33.44 (nem autoritatív válasz)

A DNS-ben használt nevek

- RFC1034, RFC1035
- A nevek pontokkal elválasztott *label*-ekből állnak
- Azok a nevek, amik `host` neveként is szerelhetnek
  - Csak alfanumerikus karakterekből és a `-` (dash) karakterből épülhetnek fel
    - LDH (`Letter, Digit, Hyphen`) karakterek
  - Kis /nagybetű nem számít
  - Hiererchia balról jobbra
    - Fordítva, mint a könyvtárstruktúra

Kliens-szerver elv

- Szerver: DNS szerver
  - Az *osztott, hierachikus* adatbázis adatait szolgáltatja
    - Az adatbázis egy részéért felelős lehet, azt mondjuk: *autoritatív*
  - Sok operációs rendszer alatt
  - Nem feltétlenül autoritás — ilyenkor csak a többi szervertől tanult neveket szolgáltatja
  - Kapcsolat a többi szerverrel
  - Cache !!
- Kliens: rezolver = stub rezolver
  - Gyakorlatilag minden IP szoftvernek része
  - Legalább egy szervert látnia kell
  - Konfigurációs paraméter

A kommunikáció

- UDP felett, az 53-as porton történik
  - Néha (pl. zóna transzfernél) TCP 53-as port
  - Újabban esetleg HTTPS, TLS, QUIC felett
- A név fán a gyökértől kezdve lépésről lépésre a hiararchia szerint
- Pl. a `www.btk.elte.hu` név feloldásának lépései
  - `.` név szerverét kérdezve
  - `.hu` név szerverét kérdezve
  - `.elte.hu` név szerverét kérdezve

A DNS szerverek kettős feladata

- *Látni*
  - Az elosztott adatbázist kérdezni szerte az interneten
  - Elnevezés: *rekurzív* névszerver = *caching* névszerver = *resolving* névszerver
- *Mutatni*
  - A rájuk tartozó részről a többi szerver számára adatokat szolgáltatni
  - Elnevezés: *autoritatív* névszerver = *hiteles* névszerver
- Egy-egy névszerver elláthatja mindkét feladatot, de ez nem tanácsos

Rezolver konfiguráció

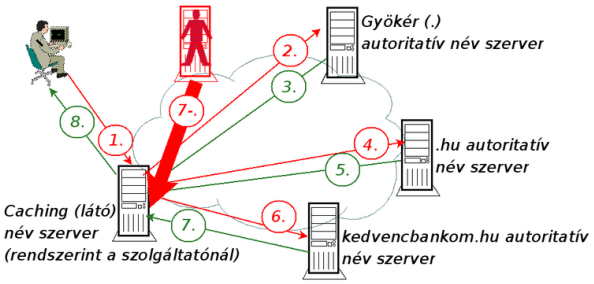
- Minden TCP/IP-t használó gépen szükséges
- IP címmel kell megadni
- Több lehet (primary, secondary)
- Elvben az internet bármely pontján
- Célszerűen: hálózati értelemben közel levő
- A DNS szerverek korlátozhatják, hogy honnan — mely IP címekről — hajlandók rekurzív kérést elfogadni
- Vannak mindenki számára elérhető rekurzív névszerverek (nyílt rekurzív névszerverek)
  - Feledékenységből és/vagy hozzá nem értésből
  - Szándékosan, nagy gonddal üzemeltetve. Pl. `1.1.1.1` (Cloudflare)

Cache, TTL

- A DNS szerverek a megtudott nevekre emlékeznek
- Haszon
  - Gyorsabb feloldás
  - Hálózat kímélése
- Hogy meddig van a cache-ben egy rekord, azt a *név gazdája* dönti el
  - *Nem* a cache-elő név szerver gazdája
- Minden rekordhoz tartozik egy ilyen idő: *TTL* (Time To Live).

3. Veszélyek

DNS cache poisoning / cache mérgezés



1. www.kedvencbankom.hu ?
2. www.kedvencbankom.hu ?
3. Nem tudom, de itt vannak a .hu név szerverei!
4. www.kedvencbankom.hu ?
5. Nem tudom, de itt vannak kedvencbankom.hu név szerverei!
6. www.kedvencbankom.hu ?

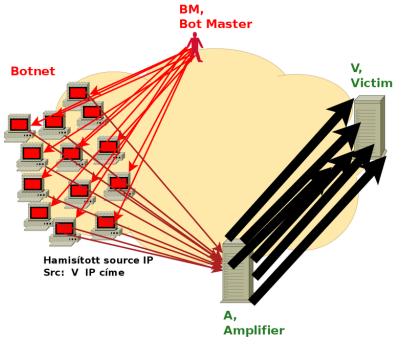
7-. www.kedvencbankom.hu A rekordja:
111.6.6.6 (autoritatív válasz) !!!

DNS cache poisoning: védekezés

- Becsempészhetnek a 3-. és 5-. lépésben is rosszindulatú rekordot
- A nyílt rekurzív szerverek növelik a veszélyt
- 2008-ban Dan Kaminsky felfedezte, hogy nagyobb a fertőzésveszély mint gondolták: nem nehéz jó választ elhitetni
- Ennek hatására több név szerver program új változattal jelentkezett
  - Több véletlen a kérdés rekordban
- A DNSSEC (RFC4033 és társai) egy védekezési mód
- Más (alkalmazás szintű) biztonsági intézkedéseket is kell használni
  - SSH, TLS
    - Fontos, hogy *„kézzel” ellenőrizzük* a kulcsokat!

DNS amplification / DNS erősítéses támadás

DDoS erősítő



Tulajdonságok

- A DNS válaszok jóval nagyobbak lehetnek mint a kérdés
  - Különösen DNSSEC esetén
- A nyílt rekurzív névszerverek különösen alkalmasak erősítő szerepre

4. Segédeszközök

Segédprogramok

- Csak a DNS rendszerben való böngészésre
  - DNS intelligencia
  - Tetszőleges szervertől kérdezhetünk
  - `nslookup`
    - Klasszikus
    - Sok platformon
  - `host, dig`: unixokon
- Web-es felület: `http://users.itk.ppke.hu/~pasztor/cgi-bin/dns.cgi`

Grafikus konfiguráló segédprogramok

- Webmin
  - Többfajta rendszeradminisztációs feladatra
  - `https://www.webmin.com`
  - Ingyenes (BSD-like licensz)
- Szolgáltatók saját maguk által kezelt név szerverekhez adnak ilyet
- Ezek használata nem pótolja a hozzáértést :-)

5. DNS építőelemek

Domain

- Minden elem domain
  - Nem csak IP cím lehet, hanem
    - tovább delegálás
    - levelezési info
    - hardware info
    - *sok minden más*
- A név fa egy pontja

Zóna

- A fának egy egyben kezelt ága
  - A mutató szerver szempontjából egy egység
  - Egy szerver rendelkezhet több zóna felett
  - Példa:
    - root zóna: a TLD-k zónája
    - `elte.hu` , `arizona.edu` ...

Primary (master), secondary (slave) szerverek

- Egy zónát több szerver is szolgáltat(hat)
- Mind autoritás — kívülről nem lehet megállapítani, melyik master, melyik slave
- Hagyományosan egy elsődleges = *master*, a többi másodlagos = *slave*
  - Használatos még a primary/secondary kifejezés is
  - Nem összekeverendő a resolvernél használt primary/secondary fogalommal!
- A secondaryk időről időre tükrözik a primary adatait
  - Csak akkor töltenek le adatot, ha van változás
  - Konfigurációs (SOA rekordban eldöntött) paraméterek

Gyökér (root) domain

- Pont olyan mint akármely domain
  - Intranetnél ezt kihasználják
- A szerverei szét vannak szórva az interneten
  - Ld. `https://www.root-servers.org` weblapja
- 2005 óta Budapesten is, az ISZT segítségével: `k.root-servers.net` egy példánya
- Anycast technológia
- 13 szerver
- Minden látó (rekurzív) szerverbe be kell konfigurálni!
- Fontos, hogy mindig elérhetők legyenek
- Maga a zóna nyilvánosan elérhető: `https://www.iana.org/domains/root/files`

Top level domain-ok

- Eredetileg felhasználó típusa szerint
  - `edu` – oktatási intézmény
  - `gov` – kormányzati intézmény
  - `org` – közhasznú intézmény
  - `com` – kereskedelmi intézmény
- Az Internet nemzetközivé válásával országkódok
  - Pl: `cz, it, jp`
  - ISO 3166 kódok
    - `https://www.iso.org/iso-3166-country-codes.html`
- Manapság egy domain név birtoklása üzleti érték
- Új top level domainek jelentek meg 2013-ban

Domain nevek
- FQDN = Fully Qualified Domain Name
- Rövidíve (jobb oldalát lehagyva)
  - Használható
  - Nem egyértelmű
- A hierarchikus felépítés miatt
  - FQDN egyértelmű

Inverz leképezés
- IP címből név
- Visszavezetik név leképezésre
- Speciális domain: `IN-ADDR.ARPA`
- Az IP címet fordított sorrendben kell írni
  - Pl: `67.84.225.193.in-addr.arpa`
- A segédprogramok automatikusan megfordítják
- Sokszor elfelejtkeznek róla!

Name szerver programok
- Klasszikus: BIND (Berkeley)
- Zónák szempontjából
  - `master` (`primary`)
  - `slave` (`secondary`)
  - `caching only`
- Cache-elnek
  - A cache-t inicializálják a root szerverek címeivel
    - Ez a `root.hints` fájl

Caching only szerver, forwarder
- Érdemes minden lokális hálózaton legalább egy DNS szervert futtatni
- Rendszerint ez csak rekurzív feladatokat lát el (caching-only névszerver)
- Forwarder: „proxy”-t használó rekurzív névszerver
  - Mielőtt az interneten érdeklődne, először ezt kérdezi
  - Nagyobb, hatékonyabb lesz a cache

Zóna fájl
- Az adatbázis adatait tartalmazza
- Elemei: Resource Rekordok (RR)
- Legfontosabbak:
  - Start Of Authority (SOA)
  - Name Server (NS)
  - Address (A)
  - Pointer (PTR)
  - Canonical Name (CNAME)
  - Mail eXchanger (MX)

6. Fontosabb rekordok

SOA rekord

Globális zóna adatok

```
elte.hu.                7191 IN SOA darmol.elte.hu. netadmin.noc.elte.hu. (
                                2022050202 ; serial
                                900        ; refresh (15 minutes)
                                1800       ; retry (30 minutes)
                                86400      ; expire (1 day)
                                7200       ; minimum (2 hours)
                                )
```

SOA (folyt.)
- A legtöbb adat a secondaryk-nak szól
- Szokás a sorszámba a dátumot betenni
  - `ÉÉÉÉHHNNVV` forma (az 5. évezredig jó)
- A sorszámot FONTOS növelni
- Ha a refresh, retry nagy

  - Kiméli a secondary-kat, de:
  - Változások lassabban terjednek
- Expiration ideig lehet, hogy nem vesszük észre, ha elrontottunk valamit!

Idő értékek a SOA rekordban
- Bind-nál `W` (hét), `D` (nap), `H` (óra) is megadható
- Refresh
  - Ennyi időnként néz a secondary a primaryra
  - Bind-nál azonnali letöltés: notify
- Retry
  - Ha nem sikerül ennyi idő múlva próbálkozik a secondary
- Expiration
  - Ennyi ideig tartja az adatokat a secondary, ha nem talál a primary-val kapcsolatot

Nem megfelelő értékek
- Értelmetlen értékek
  - refresh > expire
  - retry > refresh
  - ttl > expire
- Célszerűtlen érték
  - Kicsi TTL
    - De változás előtt érdemes ideiglenesen kicsire választani
    - Kivárni `régiTTL + újTTL` időt
    - Ez után változtatni
    - Így legfejebb `újTTL` ideig lesz elavult adat a cache-ekben
  - Kicsi vagy túl nagy refresh

TTL a SOA rekordban
- A 8.2 változatú Bind-ig: default
- Manapság: negatív cache — RFC2308
  - A „nincs ilyen” (`NXDOMAIN`) választ is cache-elik a rekurzív szerverek
  - A default-ra új derektíva: `$TTL`
  - A TTL-t rekordonként később felülbírálhatjuk

Address rekord
- Név – IP cím hozzárendelés

```
ludens.elte.hu A 157.181.2.1
```

- Nem szabad az inverz bejegyzésről elfeledkezni

NS rekord
- Egy aldomain autoritását tovább delegálja
- Az apuka és a gyerek zónában is szerepel
  - A *gyerek* zónában autoritatív adat
  - Hiba (de gyakran előfordul), hogy nem ugyanazt látjuk a gyereknél mint az apukánál

```
cs.berkeley.edu.   NS   ns.cs.berkeley.edu.
```

- Ajánlatos több NS rekordot használni
- Az argumentumban szereplő gép gazdája a felelős!!!

Glue rekord
- Az apuka zónába kényszerülő A rekord
- Példa:
  - `.pl` delegálja az `elte.pl`-t
  - az (egyik) szerver az `eltegw.elte.pl` lesz
    - Éppen a *most* delegált zónában van a név szerver
  - Az `eltegw.elte.pl`-t fel kell vennünk a `.pl` zónába

```
eltegw.elte.pl  A 12.13.14.15
```

Lame delegálás

- Az apuka zóna szerint autoritás
- Mégsem mutatja a zónát
- Okok
  - Hardver hiba (ritkán)
  - Ember-ember kommunikáció hiányossága
    - A secondary gazdája nem szólt, hogy megszűnt a gép, változott a neve
    - A primary gazdája nem szólt, hogy kér secondary-t
  - Rossz konfiguráció
- Példa: Az `terminus.inext.hu` láma a `zwodka.hu` zónára (2022. június 8-án)

CNAME rekord

- Kanonikus név (alias)

```
www.jpte.hu.     CNAME   alfa.pte.hu.
```

- Leggyakoribb felhasználás: szolgáltatás jelölése
- Ha valami CNAME, akkor nem lehet pl. `MX`, `TXT`,... is!
- A jobb oldalán álló domain célszerűen `A`

MX rekord

- Mail eXchanger
- Levél célállomást jelöl

```
pm.me.                  1200    IN      MX      5 mail.protonmail.ch.
pm.me.                  1200    IN      MX      10 mailsec.protonmail.ch.
```

- Az első paraméter prioritás, nem súly!
  - Először is a kisebbet próbálja használni a levelezőszerver
- Felhasználásai:
  - Csak levelezésen át kapcsolódók (pl. `fido.net`)
  - Intézmény címzés egyszerűsítés: pl. `kovacs@kft-neve.hu`

SRV rekord

- Szolgáltatás (service) meghatározására
- Az MX rekord általánosítása
- RFC2782 írja le
- Szerkezete:

  `_Service._Proto.Name TTL Class SRV Priority Weight Port Target`
- Példák:

```
_sip._udp.itk.ppke.hu.  86400 IN SRV 0 0 5060 voip.itk.ppke.hu.
   _xmpp-server._tcp.niif.hu.  600 IN SRV 10 0 5269 n1.xmpp.niif.hu.
```

HINFO és TXT rekord

- Emberek tájékoztatására szolgál
- `HINFO` = Hardware információ
  - Hardware és szoftver neve

```
EECS.mit.edu.       HINFO   "DEC/VAXSTATION-II" "UNIX"
huearn.sztaki.hu    HINFO   "IBM" "VM/CMS"
```

- `TXT` = Text
  - Tetszőleges szöveget tartalmazhat

```
$host -t txt pl.
pl           TXT     "ccTLD of Poland"
```

Szellemes TXT használat

- Clamav vírusírtó kurrens adatbázis változata

```
dig -t txt current.cvd.clamav.net. +short
"0.103.6:62:26566:1654682400:1:90:49192:333"
```

Delegálás az in-addr.arpa zónákban

- Az IP címtartományokkal gazdálkodók delegálják
- Rendszerint szolgáltatók
- /8 (A osztály): `a1.in-addr.arpa`
- /16 (B osztály): `b1.b2.in-addr.arpa`
- /24 (C osztály): `c1.c2.c3.in-addr.arpa`
- Az IP címet fordítva írjuk:
- `193.1.2.3` esetén `3.2.1.193.in-addr.arpa`

PTR rekord

- Az `in-addr.arpa` – olyan, mint más domain
- Címhez domain nevet rendel

```
1.109.225.193.in-addr.arpa PTR communio.hcbc.hu
```

- Az egyenes és inverz delegálás nem jár feltétlen együtt
- A hierarchiából egyértelmű, hogy hol a hiányosság

```
dig +trace -x 193.1.2.3
```

7. Ékezetek használata a DNS-ben

Ékezetes domain nevek

- Köznyelvi szavakat akarunk domain névként használni
- A domain névként csak LDH karaktereket: `[a-z0-9-]` használhatunk
  - Bár tetszőleges bináris információ lehet a DNS rekorokban
- Akarunk-e használni tetszőleges karaktersorozatot, például csupa írásjelből álló domain nevet?
  - Vélhetőleg nem

Ékezetes DNS?

- NEM!
- IDN = Internationalized Domain Names
- IDNA - International Domain Names in Applications
- 2001. decemberében IETF döntés
  - IDN 2003: RFC3490, IDN 2008: RFC5890
- A DNS szerkezet nem változik, az alkalmazások konvertálnak IDN/LDH közt
- Előnyök
  - Nem kell a DNS protokollt változtatni
  - Nem kell a DNS infrastruktúrát változtatni
  - A régi alkalmazások/domain nevek békén maradhatnak

ACE - Ascii Compatible Encoding

- Eszköz, mely lehetővé teszi, hogy az alkalmazás alatt semmi ne változzon
- Az IDN karaktereket tartalmazó (ISO-10616) karaktersorozatot LDH karakterek segítségével kódoljuk
- Előtét miatt nem keverjük „közönséges” névvel (pl. `bq--`)
- Több javaslat született: BRACE, DUDE, RACE, ...

Punycode

- Adam Costello (Berkeley Egyetem) munkája, RFC3492
- Az ascii karkakterek változatlanok maradnak
- Nem a karaktereket, hanem a karakter-pozíció párokat kódolja
- Nem is ezeket a párokat, hanem ezek különbségeit
- Nagyon tömör – sokszor tömörebb, mint az utf8!
- Előtét: `xn--`

Példák

```
xn--megszentsgtelenthetetlensgeskedseitekrt-jpdqgg5m
xn--1caaaaaaaaaa (áááááááááá)
xn--rvz-dla6d (árvíz)
xn--rdi-ela6g (rádió)
xn--szolglтat-41a6r (szolgáltató)
```

Libidn

- Stringprep, punycode és IDNA implementáció
- Library + utilityk
  - `idn` nevű unixos utility
- Simon Josefsson munkája
- Szabad (LGPL) szoftver
- Az interneten látható IDN eszközök többsége ezen alapul
- `https://www.gnu.org/software/libidn/`
- libidn2: IDNA2008-at is támogat

IDN a .hu alatt

- Csak magyar nyelvű domain nevek
- Megengedett karakterek: LDH, ékezetes kis betűk
- Nem vezetünk be kötegeket
  - Más nyelveken célszerű egyszerre több nevet lefoglalni egy regisztációkor (más írásmóddal ugyanaz a szó)

8. IPv6 a DNS-ben

IPV6-tal kapcsolatos rekordok

- Az IPV6 nem 4, hanem 16 byte-os IP címeket használ
- Az IP címek hierarchikusak
- `AAAA` rekord
  - Az A rekord pontos megfelelője
  - 16 hexa szám
  - A 0-k elhagyhatók
  - Példa:

```
www.niif.hu.   AAAA    2001:738:0:420::b
```

- Két kettőspont közti rész: 4 hexa digit, más szóval *nibble*

IPV6-tal kapcsolatos rekordok (folyt.)

- Inverz delegálás
- `ip6.arpa`
- Nibble határon lehet delegálási határt adni
- A zónáról információ az ICANN-tól:
  - `http://stats.research.icann.org/dns/ip6_report/`

9. Digitális aláírás a DNS-ben

DNS üzenetek digitális aláírása - TSIG

- RFC2845
- Szimmetrikus kulcsú titkosítást használ
- Új DNS rekord típus: `TSIG`
- A küldő röptében generálja
- A fogadó ellenőrzés után eldobja
- A DNS üzenet `ADDITIONAL` részében
- Egy közös kulcs, az idő, és az éppen átvitt rekord alapján képződik a tartalma
- DNS *rekordokat* is aláírhatunk digitálisan – DNSSEC
  - Sokkal bonyolultabb
  - Egész napos téma!

TSIG konfigurálás zóna transzferhez

- `named.conf` részlet:

```
Allow-transfer {key sec_key.;}

key sec_key {
 algorithm hmac-md5;
 secret "uaSBjcmVhdG9yIHNwaXJpdHVzLCBtZW50ZXMgdHVvcnVtIHZpc2l0YSEK";
 };

server 193.225.86.1 {
keys {sec_key;};
 };
```

10. A .hu TLD alatti regisztrálás

Regisztrálás a .hu alatt

- Az ISZT (Internet Szolgáltatók Tanácsa) szabályozza
- Információk: `https://domain.hu`
  - Nem csak a `.hu`, hanem a második szintű közdomainek alá is itt lehet regisztrálni
- Ellenőrző script: `https://info.domain.hu/webregcheck/hu`
- Leggyakoribb gondok
  - Legalább két név szerver szolgáltassa a zónát
  - Legalább két név szerver különböző hálózaton legyen

DNS intraneten

- Ál root szerver
- A `.` zóna SOA-ját tartalmazó szerver
- Nem szükséges egyszintű top level domain delegáció
- Az inverz domain(oka)t is delegálni kell
- A nem-root szervereken az ál-root ot kell a `.` autoritásának megadni (rendszerint a cache fájlban)

Olvasnivaló

- `https://powerdns.org/hello-dns/`
- `https://www.ietf.org/rfc`
- `https://www.ripe.net`
- `https://www.domain.hu`
- `https://www.dnssec.com`
- `http://users.itk.ppke.hu/~mpasztor/dnslap.html`