

# DNS – Domain Name System

## NÉVFELOLDÁSI RENDSZER

Varga Tibi 2020

# Domain Naming System


Domain név és IP cím megfeleltetési rendszer

- **Ez egy alkalmazásrétegbeli protokoll:**


a gépek, név kiszolgálókkal kommunikálnak, hogy feloldják a neveket, azaz **IP cím/név átalakítás történik**.

A DNS protokoll felhasználási területei:

- Lekérdezés:

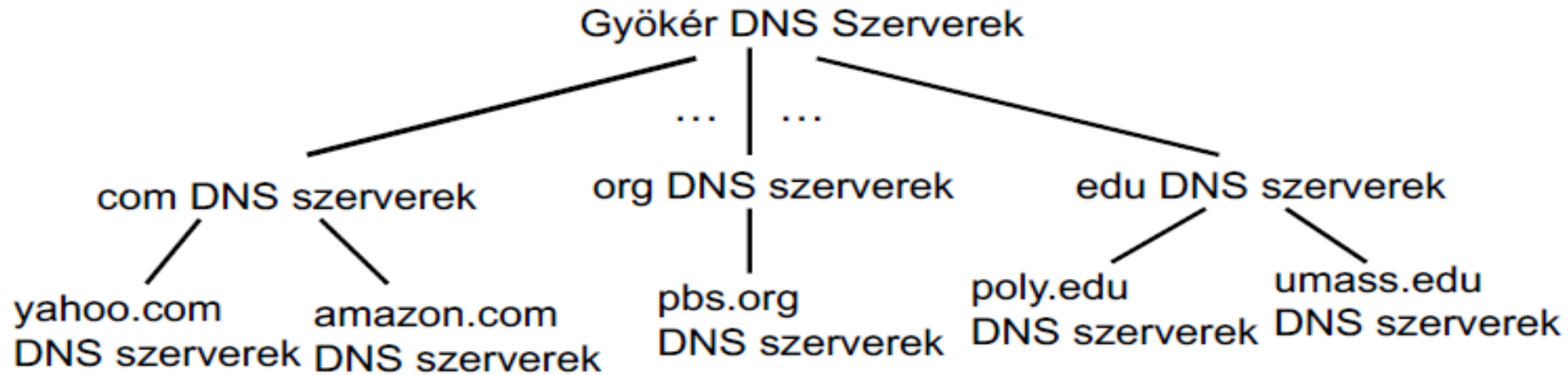
- DNS kliens böngésző vagy smtp  DNS szerver
- UDP 53 port rövid, gyors üzenetváltás (TCP is 53 porton de lassabb megbízhatóbb)

- Zónaletöltés két DNS szerver között

- Elsődleges DNS szerver  másodlagos DNS szerver
- TCP 53 hosszabb, megbízhatóbb

# A DNS struktúra

## A DNS: hierarchikus, elosztott adatbázis rendszer



- a kliens az `www.amazon.com` IP címére kíváncsi;
- Első közelítés: a kliens megkérdezi a gyökér szervert a `com` DNS szerverről
- a kliens megkérdezi a `.com` DNS szervert az `amazon.com` DNS szerverről
- a kliens megkérdezi az `amazon.com` DNS szervert a `www.amazon.com` IPcíméről

# A DNS zóna és névszerverek

## Zóna

- Minden tartomány egészének adatit tároló adatbázis
- A DNS nevével azonosítjuk (pl. kisnyuszi.hu.)

## DNS szerver

- Egy vagy több zónát tárol, szolgál ki

## Elsődleges/másodlagos DNS szerver

- Egy adott zónára vonatkozóan
  - Elsődleges: írható és olvasható
  - Másodlagos: csak olvasható
- Minden esetben pontosan 1 elsődleges és legalább 1 másodlagos kell
  - ➔ hibatűrés
  - ➔ terheléselosztás és skálázhatóság

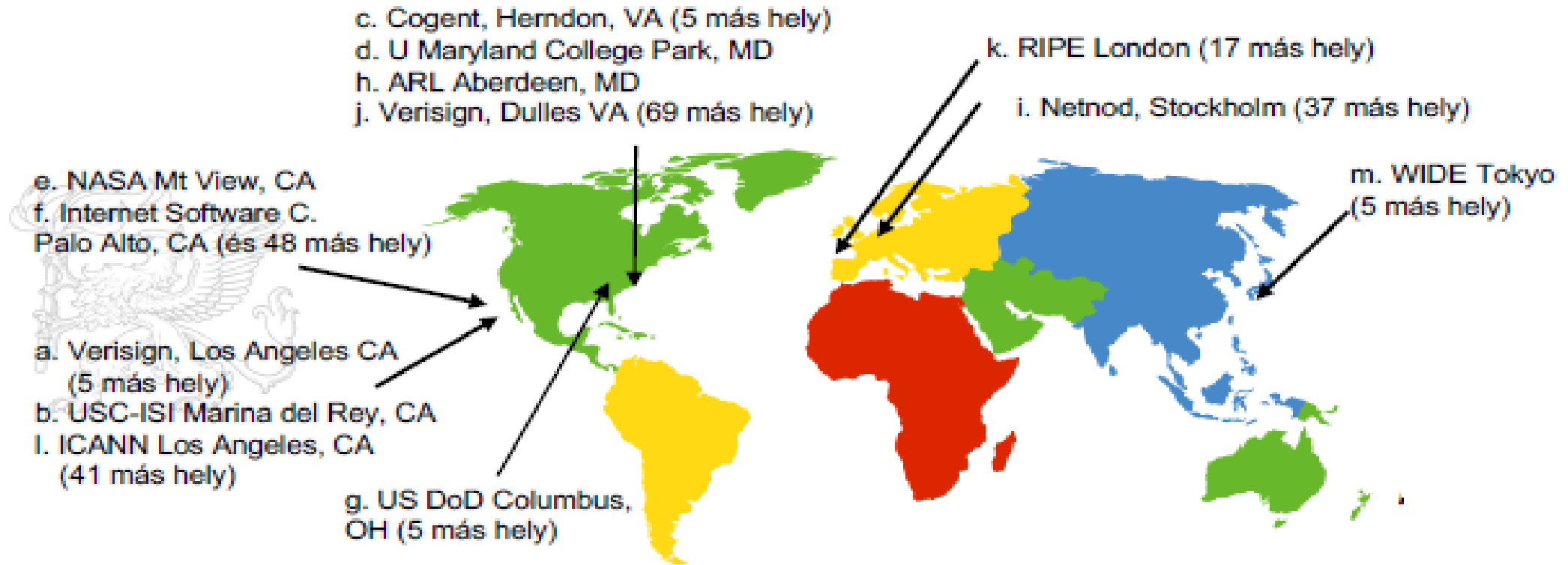


# Gyökér DNS szerverek

- A gyökér névszerver:

Globálisan 16 logikai gyökér névszerver létezik, de minden “szerver” sokszor van replikálva

Gyökérzóna: legmagasabb szintű DNS zóna



# TLD, felelős DNS szerverek

## **Felsőszintű tartomány (TLD) szerverek:**

- Az IANA adminisztrálja (Internet Assigned Numbers Authority)
- ország kód top-level domains (ccTLD): pl. .hu
- generic top-level domains (gTLD): pl. .org, .edu, .net, .com, .gov,
- .mil infrastructure top-level domains: egy van, az .arpa

## **Felelős DNS szerverek:**

- a szervezetek saját DNS szerverei, felelős átváltást biztosítanak a szervezet IP címe és nevesített gépei között
- ezt maga a szervezet vagy egy szolgáltatás biztosító kezelheti

# Helyi DNS szerver

- Minden ISP (lakossági ISP, cég, egyetem) rendelkezik eggyel - ezt nevezik “alapértelmezett név szerver”-nek
- amikor egy gép DNS lekérdezést indít akkor a helyi DNS kiszolgálónak küldi el
- van saját gyorsítótára a legutóbbi név – cím hozzárendelésekről (ez elavult is lehet!)
- egy átjátszóként továbbítja a kérést a hierarchiába

# Névfeloldás menete

(0. Böngésző gyorsítótára)

1. Helyi gép gyorsítótára

2. Helyi gépen „hosts” fájl

3. Lekérdezés DNS szerverektől

- Ha van DNS szerver megadva
  - Lekérdezés az elsődleges DNS szervertől, ha elérhető (rekurzív)
- Ha nincs DNS szerver megadva
  - vagy nem elérhetők, akkor lekérdezés valamely root NS-től, majd a hivatkozott NS-ektől (iteratív)

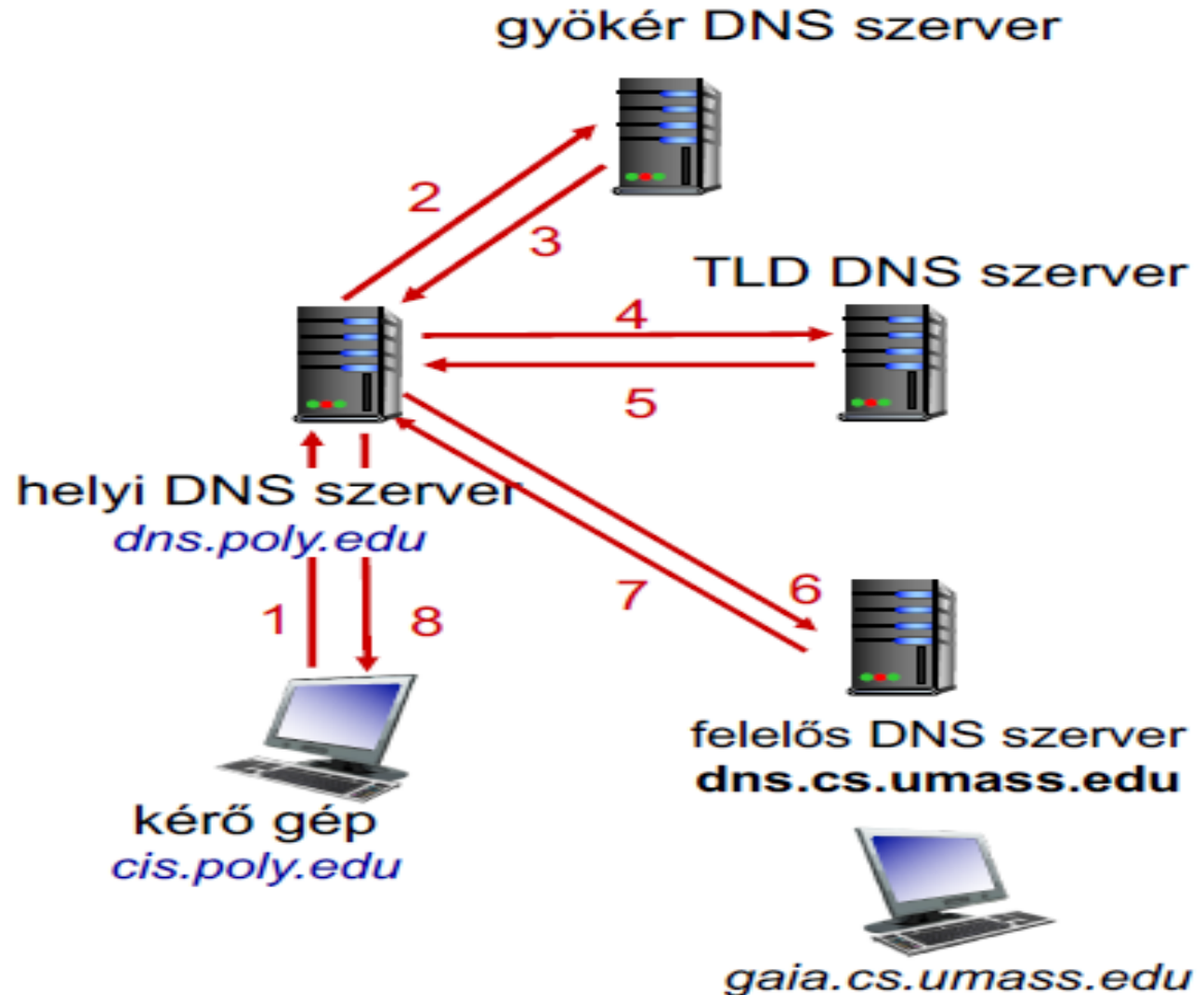


# Iterált DNS név feloldás

A cis.poly.edu gép a gaia.cs.umass.edu IP címére kíváncsi

## Az iterált lekérdezés:

A megszólított  
szerver egy szerver  
címével válaszol:  
“Én nem tudom a  
választ, de kérdezd  
meg őt”

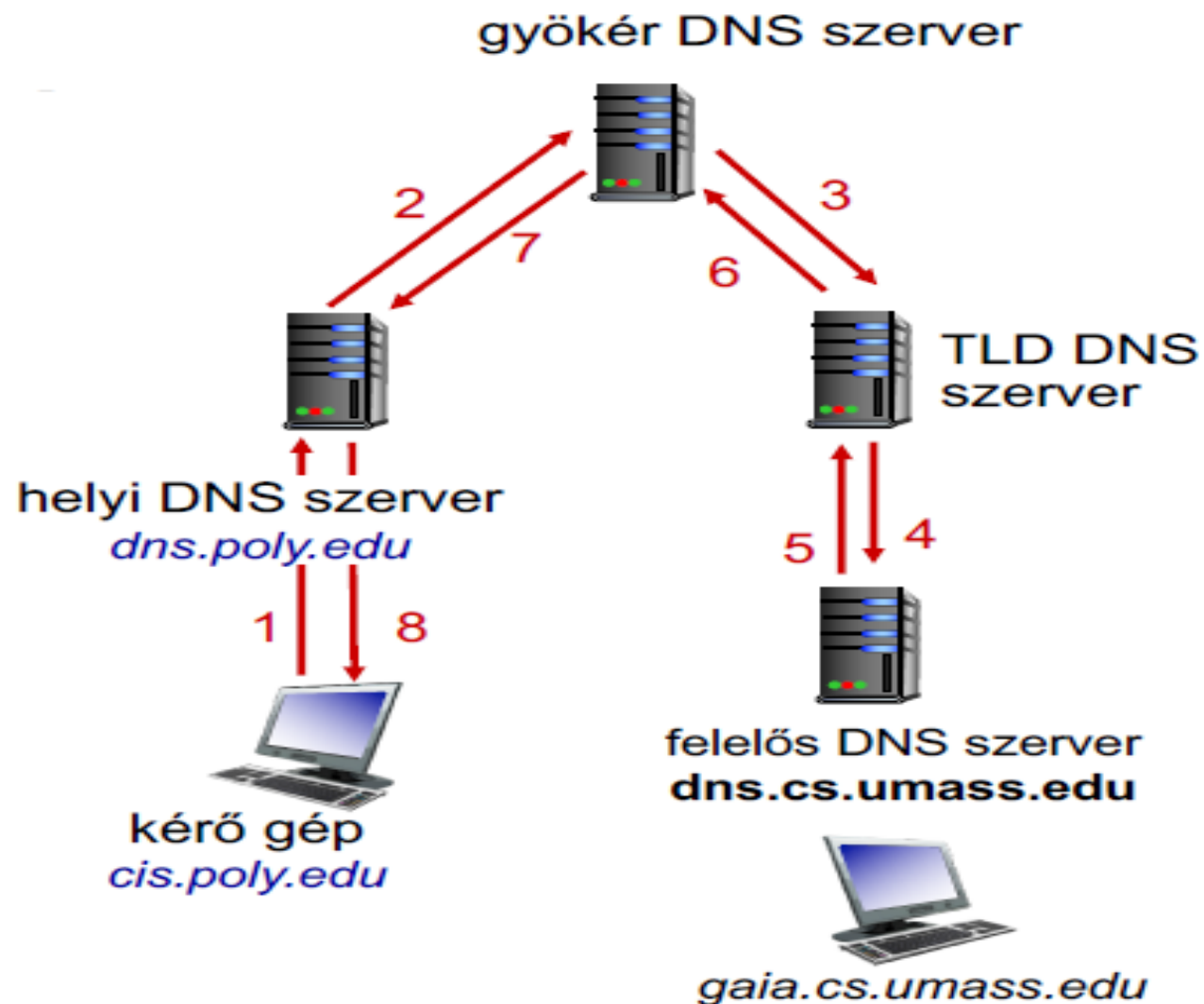


# Rekurzív DNS név feloldás

A cis.poly.edu gép a gaia.cs.umass.edu IP címére kíváncsi

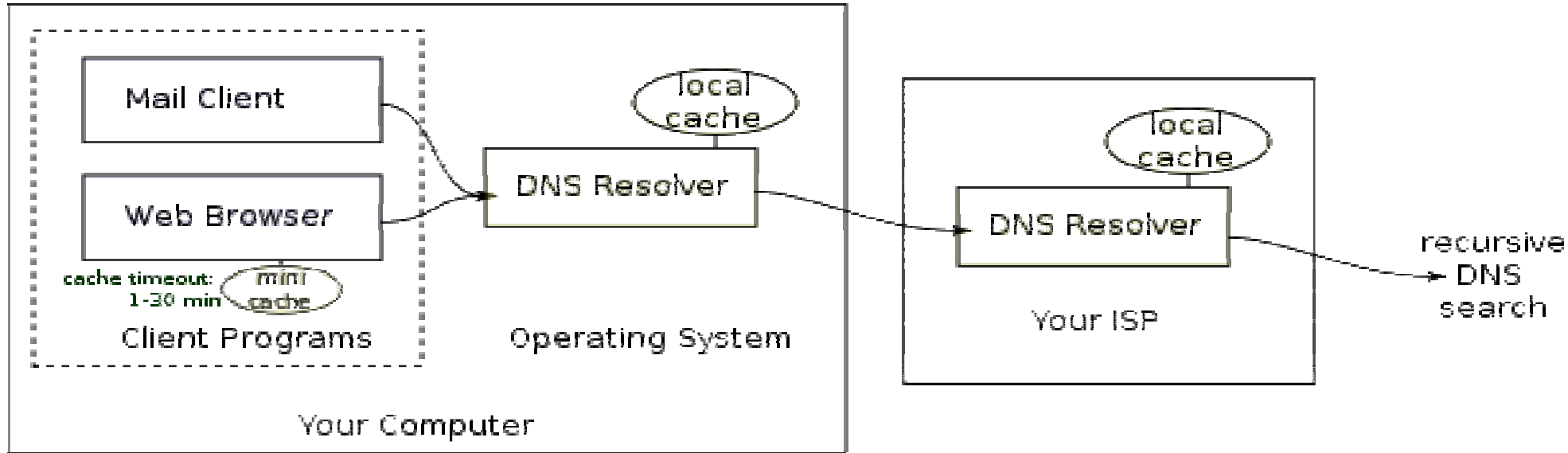
**A rekurzív lekérdezés:**

- **DNS-es szerverek nem végeznek minden kliensnek ilyen feloldást, csak a konfigurációban megadottaknak.**
- a névfeloldás terhét a felkeresett szerverre teszi
- nagy terhelés a hierarchia magasabb rétegeiben



# Névfeloldás gyorsítótárral

1. A DNS-kéréseket a helyi gépen az operációs rendszer oldja fel egységesen
2. **DNS gyorsítótár (cache)** a helyi gépen és a DNS szerveren



- Minden rekordnak **TTL-je (Time To Live)** valódi másodpercben megadva → elévülés
- **Authoritatív válasz:** ha a rekordért felelős szerverek valamelyikétől származik a válaszol
- **Nem autoritatív:** ha gyorsítótárból származik

# Cache -- TTL

A névszerverek tárolják egy ideig a feloldást, hogy ha legközelebb kéri tőle azonnal tudja a választ

- hálózati forgalom csökkenése
- gyors névfeloldás

A tárolás idejét a zóna adminisztrátora adja meg a zóna leírásánál

- TTL – Time To Live
- Ennyi másodpercig tárolják a cache szerverek az adatokat

# DNS bejegyzések

DNS: egy erőforrás bejegyzéseket tároló elosztott adatbázis (RR)

- RR formátum: (név, érték, típus, ttl)

## Fontosabb bejegyzések az adatbázisban:

A – Host rekord (név -> IPv4 hozzárendelés)

NS – Name Server (DNS szerver)

CNAME – Canonical Name (további nevek)

MX – Mail Exchange (Levelező szerver)

SOA - SOA (Start of Authority) - adminisztratív adatok:

- az elsődleges DNS szerver neve, zóna verziószáma (ez alapján a szinkronizálás), kapcsolattartó e-mail címe....

PTR – Pointer (IP -> név)

SRV – Service (szolgáltatás)

AAAA – IPv 6 cím hozzárendelés

# DNS lekérdezések nslookup parancsal

- nslookup paran - Linux és Windows CMD-ben is használatos

## A parancs alakjai:

**Alap eset:** nslookup [kapcsoló=opció] [domain név vagy IP cím] [server]

Példák:

Alap: **nslookup gdszeged.hu**

type kapcsolóval, mx opcióval mail szerverre:

**nslookup -type=mx gdszeged.hu**

query kapcsolóval, ns opcióval IPv4 név szerverre:

**nslookup -query=ns gdszeged.hu**

Lekérdezés speciális névszerverrel (Google)

**nslookup gdszeged.hu 8.8.8.8**

# DNS lekérdezés nslookup parancsal

Összes elérhető DNS adat lekérdezés query kacsolóval és any opcióval:

**nslookup -query=any google.com**

Fordított IP lekérdezés: **nslookup 210.113. 12.123**

## Fontosabb opciók:

<b>any</b>	Minden információ
<b>a</b>	32 bites IPv4-címmel tér vissza,
<b>aaaa</b>	128 bites IPv6-címmel tér vissza,
<b>ns</b>	Kijelöli egy DNS-zóna számára használható autoritatív névkiszolgálókat.
<b>mx</b>	A tartománynévhez rendelt levéltovábbító ügynökök listája
<b>cname</b>	A tulajdonos kanonikus vagy elsődleges neve.
<b>soa</b>	Irányadó információk a DNS-zónáról
<b>srv</b>	Általános szolgáltatás-helymeghatározó rekord, újabb protokollok számára

# DNS beállítás Linuxban

- A DNS beállításokat az **/etc/resolv.conf** állomány tartalmazza.

```
tibi@server:/etc/netplan$ cat /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "systemd-resolve --status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0
```



# Hosts fájl

- A DNS előtt is volt névfeloldás. Ezeket hosts fájlokkal oldották meg, konkrétan ez a fájl neve. **Linuxban** az */etc/host* állományban, **Windowson** a *C:\Windows\System32\drivers\etc\hosts* .
- Ezek a **hosts fájlok ma is megtalálhatók minden gépen és használhatók is.** Egy ilyen nevű állományban tárolták az IP címeket és a hozzájuk tartozó neveket. Ezek az állományok azonban idővel igen nagyra nőttek. Nagyon sűrűn kellett változtatni azokat. A hálózatok növekedése miatt egyre több ember, egyre gyakrabban töltötte le a fájlokat, így szükségszerűvé vált egy újabb megoldás A DNS.
- **/etc/hosts**
  - 195.199.200.48 jupiter.zold.and
  - 180.123.5.24 mars.sarga.and
  - 210.100.205.8 venus.piros.and
  - 208.24.243.238 pluto.lila.and