Windows rendszeradminisztráció és Microsoft szerveralkalmazások támogatása

4. óra

Kocsis Gergely,
Supák Zoltán

2017.03.08/2017.03.22.

DNS

Névfeloldás

Mivel hálózatok felhasználói emberek, természetes igény, hogy a hálózat csomópontjaira ne csak az IP cím segítségével, hanem valamilyen név megadásával is lehessen hivatkozni.

A legegyszerűbb megoldás egy **szótárfájl** alkalmazása, mely IP cím – név összerendeléseket tartalmaz. (hosts fájl)

A hálózatba kötött csomópontok számának növekedésével a fájl menedzsmentje lokálisan kivitelezhetetllenné válik. Megoldás: fájl letöltése központi **hosts szerver**ekről.

A fájlok méretének növekedésével és a módosítások gyakoriságának emlekedésével a központi fájl is kezelhetetlenné válik. Megoldás: Központi dinamikus elosztott adatbázis alkalmazása → **DNS**.

DNS

A DNS (Domain Name System) egy hierarchikus tartomány-alapú névkiosztási séma, melyet elosztott adatbázis, segítségévell valósítanak meg, RFC 1034, 1035

A DNS legszélesebb körben ismert alkalmazása az IP címekhez történő névhozzárendelés az Interneten, ugyanakkor egyrészt segítségével más erőforrások is cimkézhetők, másrészt igen széles körben használatos vállalati és magánhálózatok kialakításakor is.

A tartománynevek rendszere (DNS) három fő komponensből áll:

1) Tartománynevek tere és erőforrásrekordok
2) Névszerverek
3) Címfeloldó (resolver) programok

DNS

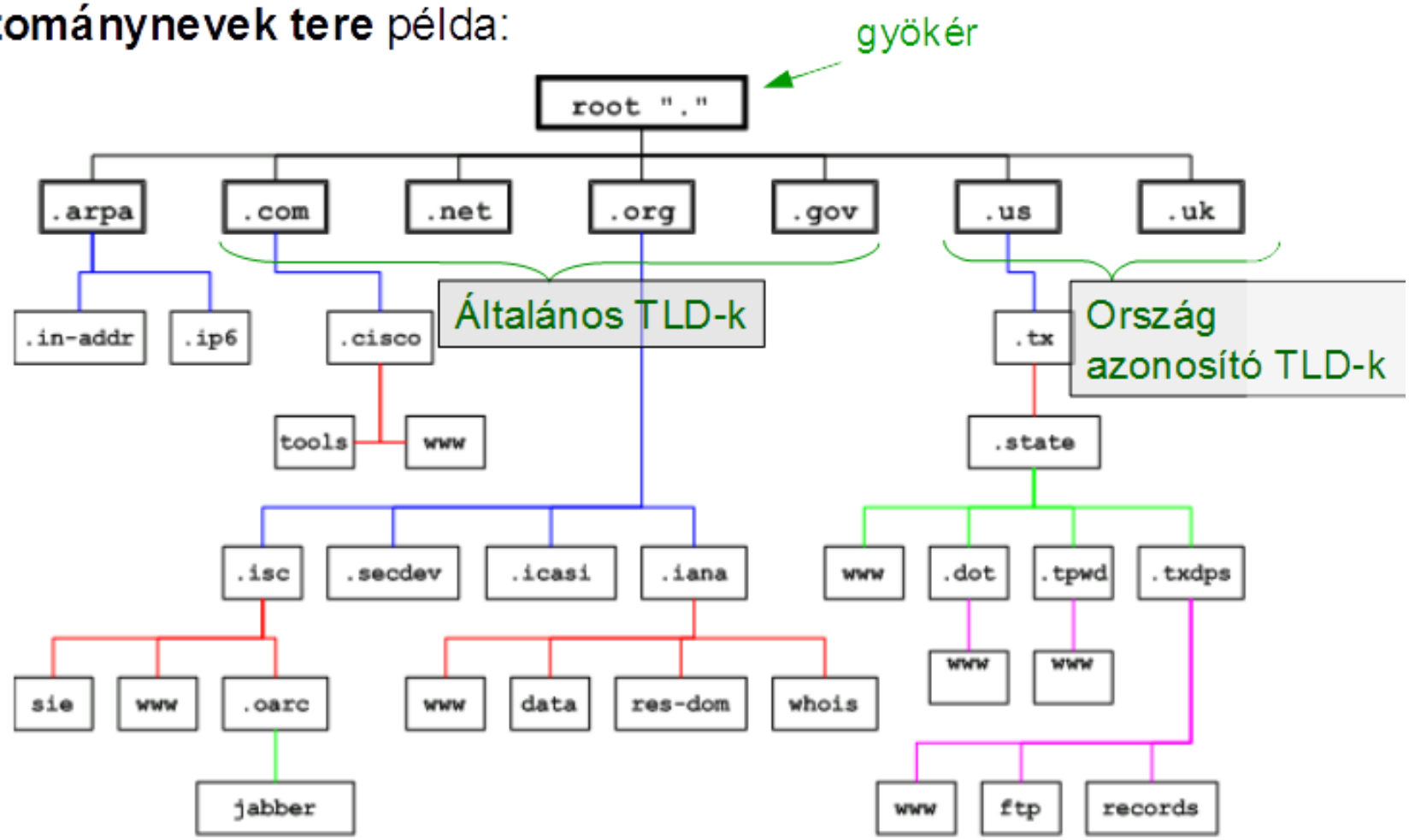
Tartománynevek tere és erőforrásrekordok

- Fa típusú gráf, melyben minden csúcs egy erőforráshalmazt reprezentál.
- A csúcsokhoz egy (max. 63 bájt hosszúságú) címkét rendelünk.
- Két testvér csúcs címkéje nem lehet azonos.
- A zéró hosszúságú címke („null címke”) a gyökér számára kizárólagosan foglalt.
- A kis- és nagybetűk között nem teszünk különbséget, de célszerű megtartani a forrás írásmódját.

Abszolút tartománynév: A tartománynevek terében bármely csúcs egyértelműen reprezentálható a csúcstól a gyökérig vezető utat leíró címkesorozattal.

DNS

Tartománynevek tere példa:

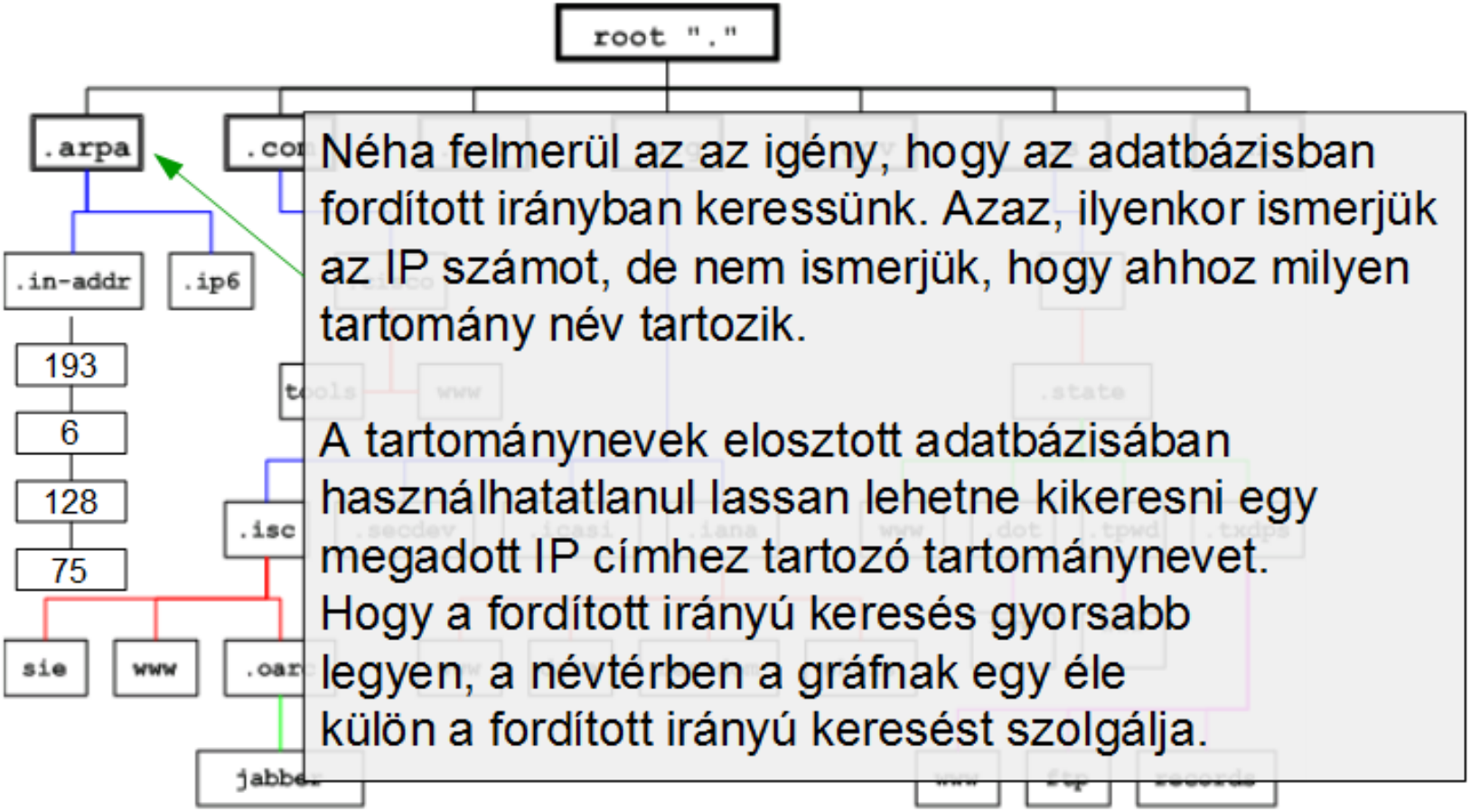


Ebben a gráfban egy abszolút nél pl: www.tped.state.ta.us

http://www.cisco.com/web/about/security/intelligence/dns-bcp.html (u.l. 2015.11.18)

DNS

Tartománynevek tere példa:



Néha felmerül az az igény, hogy az adatbázisban fordított irányban keressünk. Azaz, ilyenkor ismerjük az IP számot, de nem ismerjük, hogy ahhoz milyen tartomány név tartozik.

A tartománynevek elosztott adatbázisában használhatatlanul lassan lehetne kikeresni egy megadott IP címhez tartozó tartománynevet. Hogy a fordított irányú keresés gyorsabb legyen, a névtérben a gráfnak egy éle külön a fordított irányú keresést szolgálja.

http://www.cisco.com/web/about/security/intelligence/dns-bcp.html (u.l. 2015.11.18)

DNS

Tartománynevek tere és **erőforrásrekordok**

- A tartománynevek egy-egy csomópontot specifikálnak.
- A csomópontokhoz egy erőforrás-halmaz társítható.
- Az információs erőforrások ún. erőforrás rekordokban (Resource Record, RR) tárolódnak.
- Az erőforrás rekordok sorrendje lényegtelen.
- **Az erőforrás rekordok mezői:**

Tulajdonos: Az a tartománynév, amelyhez a RR tartozik.
Osztály: 16 bites érték, mely egy protokollcsaládot/protokollt azonosít.
IN: az internet protokollcsalád
CH: A Chaos protokollcsalád (Moon A. David, Chaosnet, https://dspace.mit.edu/bitstream/handle/1721.1/6353/AIM-628.pdf?sequence=2)
Élettartam (TTL): 32 bites érték: A RR max. felhasználhatósági ideje (sec).
Típus: 16 bites érték a típus szerinti tagoláshoz.
Adat

DNS

Tartománynevek tere és **erőforrásrekordok**

Legfontosabb RR típusok:

Típus	Adat	Leírás
A	32 bites IP cím (IN osztály esetén).	A tulajdonos hálózati címe
CNAME	Tartománynév	Egy alias névhez kanonikus név rendelése
HINFO	Tetszőleges sztring.	CPU, op. rsz. információk meghatározása
MX	16 bites prioritás érték és egy tartománynév.	Levélforgalmazó (mail exchange) megadása
NS	Egy host tartományneve	Névszerver rendelése a tartományhoz
PTR	Egy tartománynév	Pointer a névtér egy másik területére
SOA	Több mezőből álló rekord	Hitelességi (authority) zóna specifikációja

DNS erőforrás rekordok

Forward lookup zone:

- A: (Address) IP címhez nevet rendel
- MX: (Mail eXchange) levelező szerver
- SRV: (Service) szolgáltatás helymeghatározó (MX helyett pl.)
- NS: (Name Server) adott zónában dolgozó szerver címe
- SOA: (Start Of Authority) zóna információk, admin e-mail, TTL
- CNAME: (Canonical NAME) Aliashoz tartozó eredeti név

Reverse lookup zone:

- PTR: (PoinTeR record) mutató kanonikus névre

DNS

Tartománynevek tere és erőforrásrekordok

A tartománynevek tere két (természetes) módon darabolható:

1.) Az osztálytagozódás alapján.
A különböző osztályok parallel névtér-faként foghatók fel.
A tartománynév-tér (fa) éleinek átvágásával.

2.) Ha a tartománynevek terében bizonyos éleket „átvágunk”, akkor a maximálisan összefüggő részgráfok szintén fa struktúrájúak.

Egy ilyen maximálisan összefüggő részgráfot **zónának** nevezünk.

Egy zóna reprezentálható a gyökérhez legközelebbi csúcsának tartománynevével.

Az „átvágásokat” nyilván kell tartanunk.

http://courses.ischool.berkeley.edu/i253/f11/internet#(24) (u.l. 2015.11.18)

DNS

Névszerverek

Információt tárolnak a tartománynevek gráfjáról.

Tartománynevekhez tartozó erőforrás rekordokat tárolnak.

Kérdéseket (lekérdezéseket) válaszolnak meg.

Minden szerver **authoritatív** az általa kezelt zónában és **nem authoritatív** az általa csak cachelt információkra.

DNS szerver típusok:

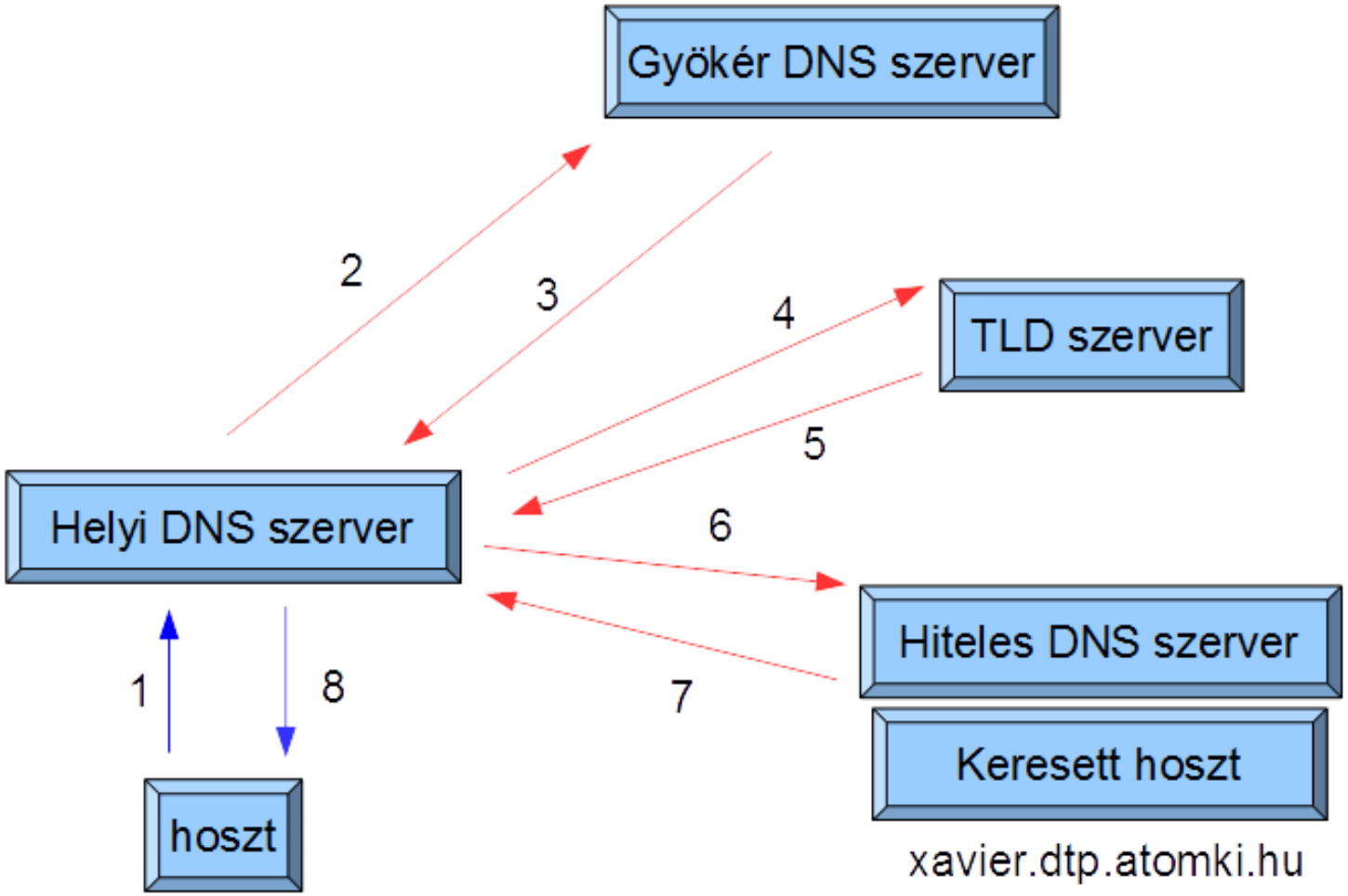
Gyökér DNS szerverek (összesen 13 db. A-M-ig)

TLD (Top Level Domain) szerverei. Pl országok szerverei (hu, fr, com ...)

Hiteles DNS szerverek: minden olyan szervezet, mely nyilvánosan elérhető hosztokat üzemeltet, nyilvános DNS bejegyzéseket kell, hogy szolgáltasson. Ezt saját hiteles DNS szerverén keresztül teheti meg.

Helyi DNS szerver: Nem tartozik szorosan a DNS hierarchiába, ugyanakkor fontos a szerepük pl a chachelés miatt.

DNS lekérdezés működése



Kérdés: xavier.dtp.atomki.hu

DNS lekérdezés működése

Nem rekurzív (iteratív) módszer:

- Szerver oldalon a legegyszerűbb megvalósítás.
- Minden névszerverben implementált.
- A kliensnek lehetősége nyílik az információk értékelésére.

Rekurzív módszer:

- Kliens oldalon a legegyszerűbb megvalósítás.
- A szerveren megvalósítható átmeneti tárolás (cache).
- Opcionális, mind a szerveren, mind a kliensen implementált-nak kell lennie.
- A szerver minden válaszában egy bit (RA) jelzi az implementációt.
- A kliens a kérdésben egy bittel (RD) jelzi a rekurzív igényt.

DNS

Címfeloldó (resolver) programok

A címfeloldó programok a felhasználói programok és a névszerverek közötti interfészek.

A címfeloldás ideje lehet kicsi (millisec.) pl. helyi adatokból felépített válasz esetén, de lehet nagy (több sec.) névszerverek adatait kérdezve.

A címfeloldás kliens oldala általában platformfüggő.

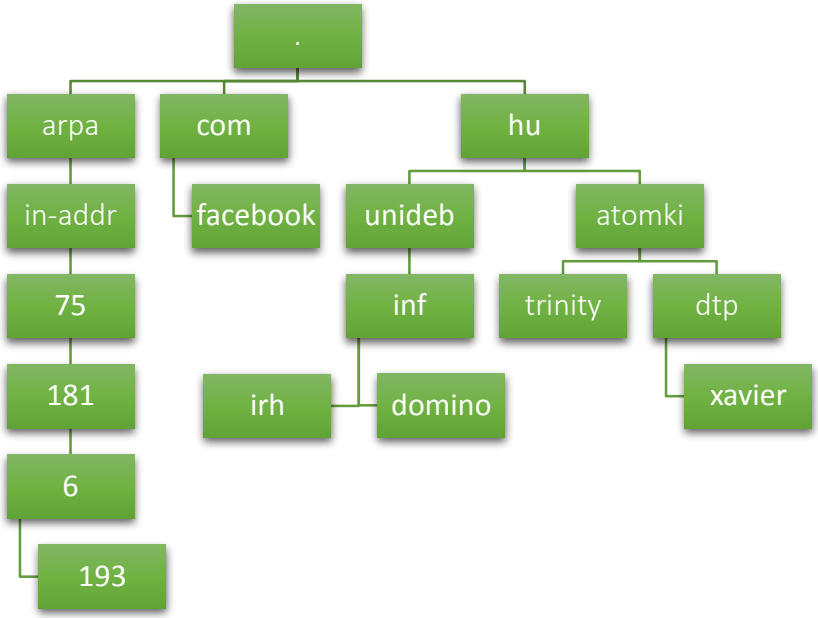
Általános funkciók:

Gépnév → gépcím meghatározás
Gépcím → gépnév meghatározás
Általános lekérdezési funkció

DNS zónák

Forward lookup zone:
Hagyományos zóna a gyökértől indulva szintenként egy-egy új információrészt tartalmaz az FQDN feloldásához

Reverse lookup zone: Fordított zóna. A gyökérből indulva az arpa, majd az in-addr szintek után négy szinten old fel egy IPv4 címet. Az ág végén egy PTR rekkord mutat az ip címhez rendelt aliasra.



Authoritative és non-authoritative DNS szerver

- Egy DNS kérés feloldása lehet rekurzív és iteratív
- Kérést DNS kliens és szerver is indíthat
- Egy szerver lehet authoritatív, vagy nem authoritatív

- Az authoritatív szerver kétféle választ adhat
  - A névhez tartozó IP
  - Nem létező név

- A nem authoritatív szerver válasza a következőktől függ
  - Tartalmazza-e a kért nevet a cache
  - Átirányítás külső hálóra (forwarder segítségével)
  - Root hint (Gyökér szerver megkérdezése)

DNS zóna típusok

Elsődleges (primary) zóna: A DNS adatbázis írható-olvasható másolata. Az információt tároló és nyújtó szerver azonos.

Másodlagos (secondary) zóna: A DNS adatbázis csak olvasható másolata. Csak más szerveren keresztül frissülhet.

Csonka (stub) zóna:Az elsődleges zóna olyan másolata, mely csak az authoritatív szerver megállapításához szükséges információt tartalmazza

Active Directory Integrált zóna A DNS információkat az AD DS (Domain Services) tárolja és kezeli. Így teszi lehetővé pl a szimultán szerkesztést stb.

WINS és NetBIOS

WINS (Windows Interet Name Service): A WINS szerver NetBIOS-IP cím hozzárendeléseket tárol. A kliens indulásakor felveszi vele a kapcsolatot és bejelenti saját adatait. Kommunikáció során szintén hozzá fordul.

Több folyamat során is broadcast alapú. Nincs hierarchia, mint a DNS esetén -> nem skálázható.

NetBIOS név: 16 bájtos azonosító.

Mára leginkább csak a visszafelé kompatibilitás miatt használjuk. Elterjedtebb a DNs használata helyi hálókon is.

Ajánlott olvasmány

MS: A DNS-rendszer alapjai, O365 link

Egyéb: Ha nem megy a DNS: http://hvg.hu/tudomany/20150403_minden_oldal_akadozik_teljes_upc_kaosz

Linkek

- RobTex: https://www.robtex.com/
- IANA Root Zone Mgmt: https://www.iana.org/domains/root

  (root database, root zone file, etc)
- Root servers: http://www.root-servers.org/
- Zónafájl felépítése: https://support.microsoft.com/en-us/kb/163971
- DNS konfigurációjának ellenőrzése: http://www.domain.hu/domain/regcheck/
- Split DNS namespace
  - DNS támadások: https://technet.microsoft.com/en-us/library/cc755131.aspx
  - hogyan védekezzünk: https://technet.microsoft.com/en-us/library/cc770636.aspx
- Regisztrált domai-nevek száma alapján készült térkép:

  http://thenextweb.com/insider/2016/03/10/the-world-according-to-domains/

Gyakorlati feladat
DNS szerver telepítése és beállítása