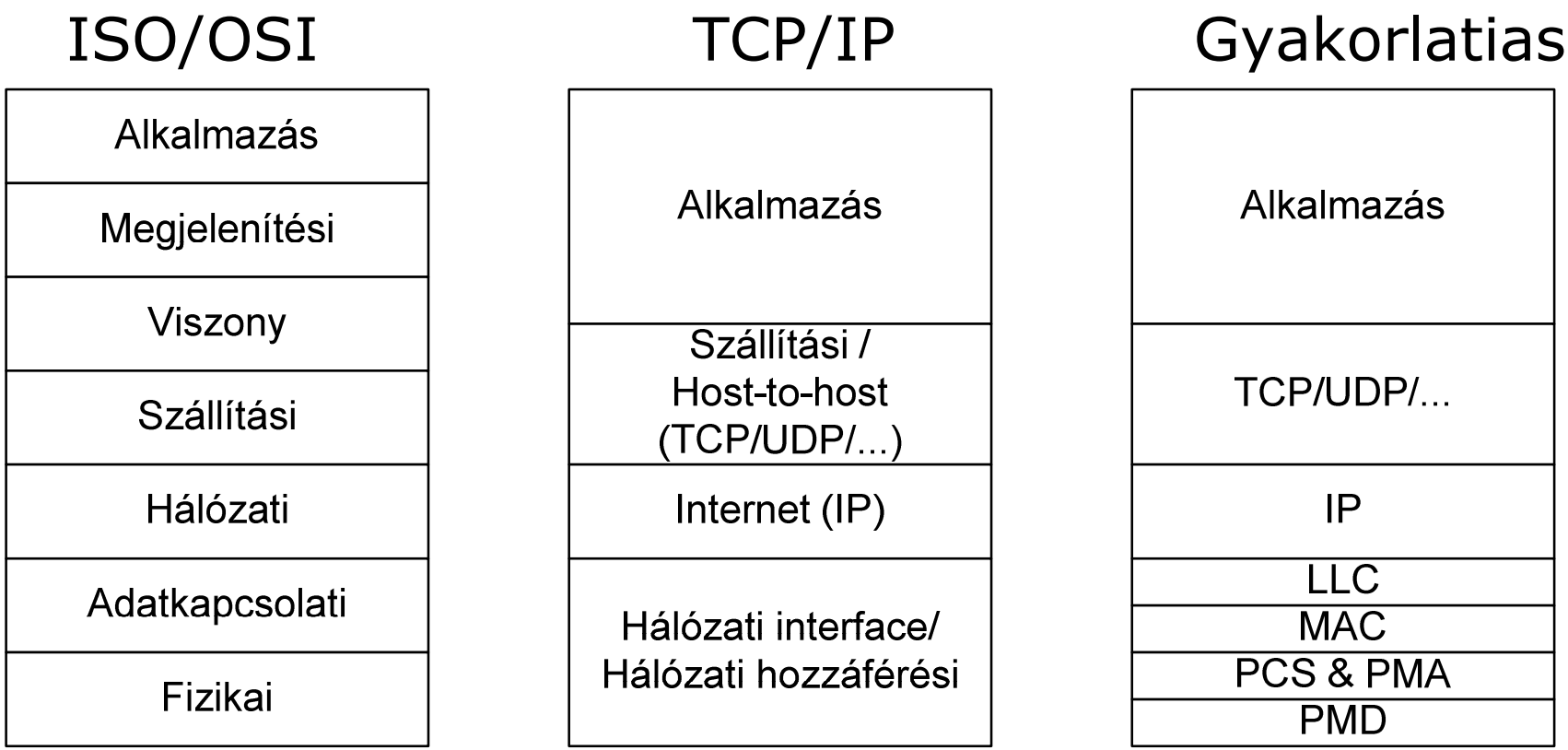
Hálózati alkalmazások, alkalmazásprotokollok, infrastrukturális szolgáltatások

Alkalmazások hálózati kapcsolata
Névfeloldási szolgáltatás
Levelezési rendszerek
Webes rendszerek

TCP/IP architektúra és az ISO/OSI rétegmodell



IP: Internet Protocol

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

LLC: Logical Link Control

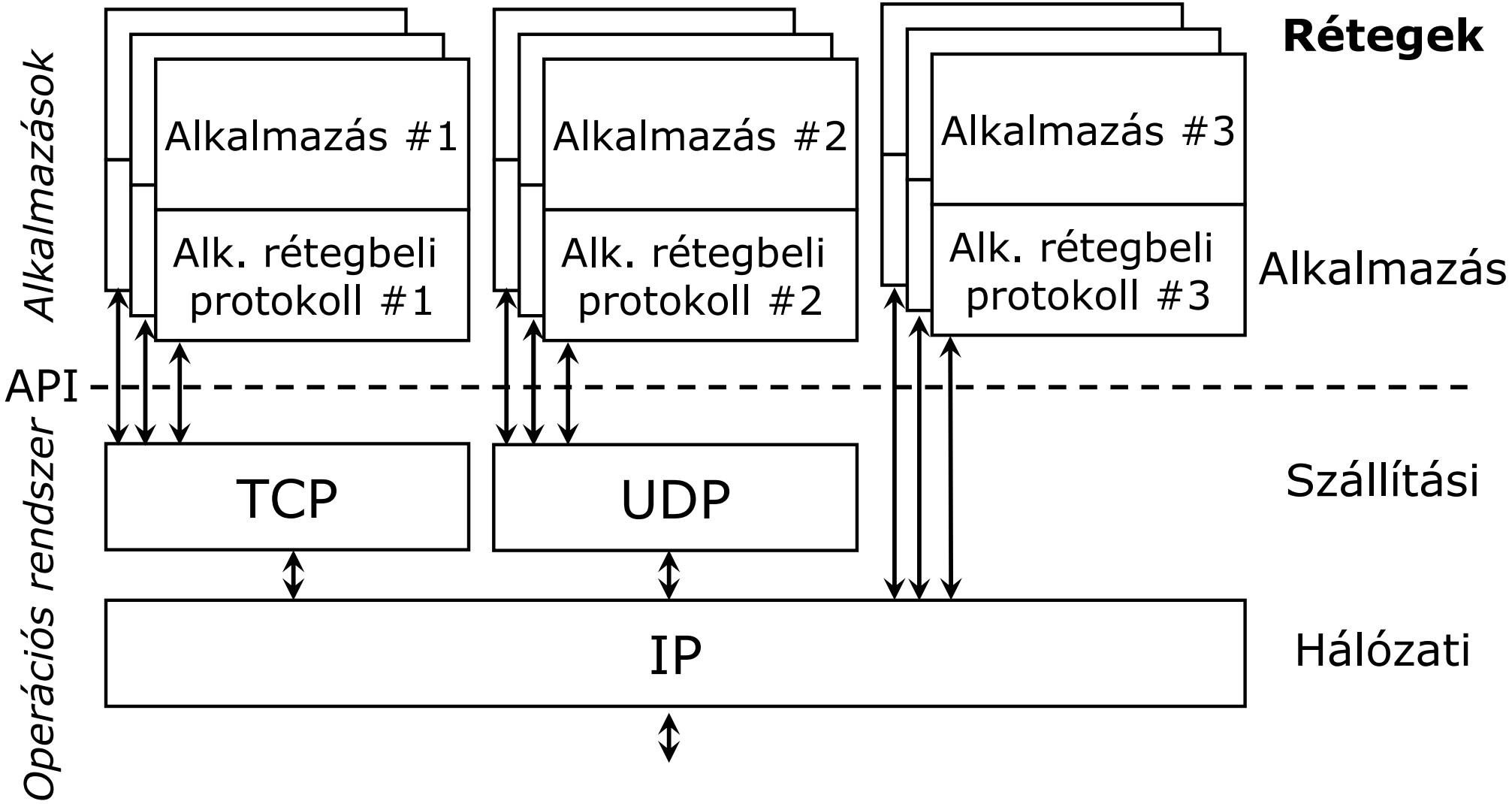
MAC: Medium Access Control

PCS: Physical Coding Sublayer

PMA: Physical Medium Attachment

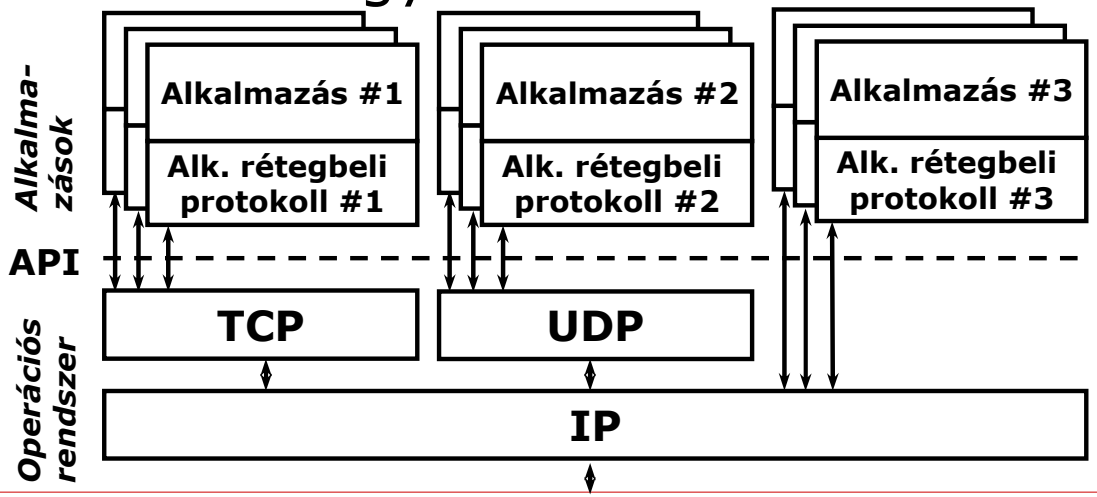
PMD: Physical Medium Dependent

Alkalmazások kapcsolata az alsóbb rétegekkel



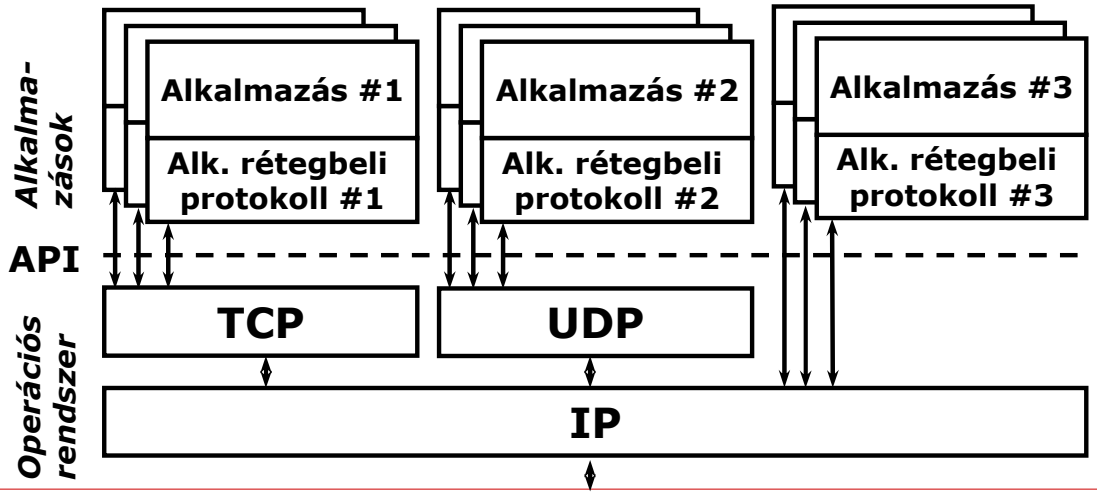
Alkalmazás-rétegbeli protokollok

- Legtöbbször az alkalmazásban kerül implementálásra
  - Alkalmazás logikájához szorosan kapcsolódik
  - Egy alkalmazás-rétegbeli protokollt tipikusan kevés (0..1..2) alkalmazás használja
- Mégis szükséges szabványosítani
  - Alkalmazások együttműködése



Alkalmazások környezete

- Alsóbb rétegeket – mint szolgáltatásokat – az operációs rendszer biztosítja
- Elfedi a tényleges rétegeket, és csak egy interfészt (API: Application Programming Interface) biztosít
  - Vö. SAP (Service Access Point)
- Ennek rendszerhívásait használva létrehozható a kívánt kommunikációs csatorna, illetve annak az alkalmazás által használható végződése (socket)



Kliens-szerver architektúra

- Kliens
  - Kapcsolatot kezdeményező ügyfél
- Szerver
  - Szolgáltatást nyújtó kiszolgáló

- Kliensnek a szolgáltatást meg kell címeznie
  - IP-cím (vagy DNS név) + szállítási protokoll + portszám

Port-hozzárendelés

- Szerveren
  - Szolgáltatást azonosítja
    - egy port maximum egy szolgáltatáshoz lehet hozzárendelve
  - Statikus
  - 1-65536 tartományból tipikusan 1-1023-ig
- Kliensen
  - Dinamikusan kerül kiosztásra a még nem használtak közül (beleértve a szolgáltatásokat)
  - 1-65536 tartományból 1024-65535-ig

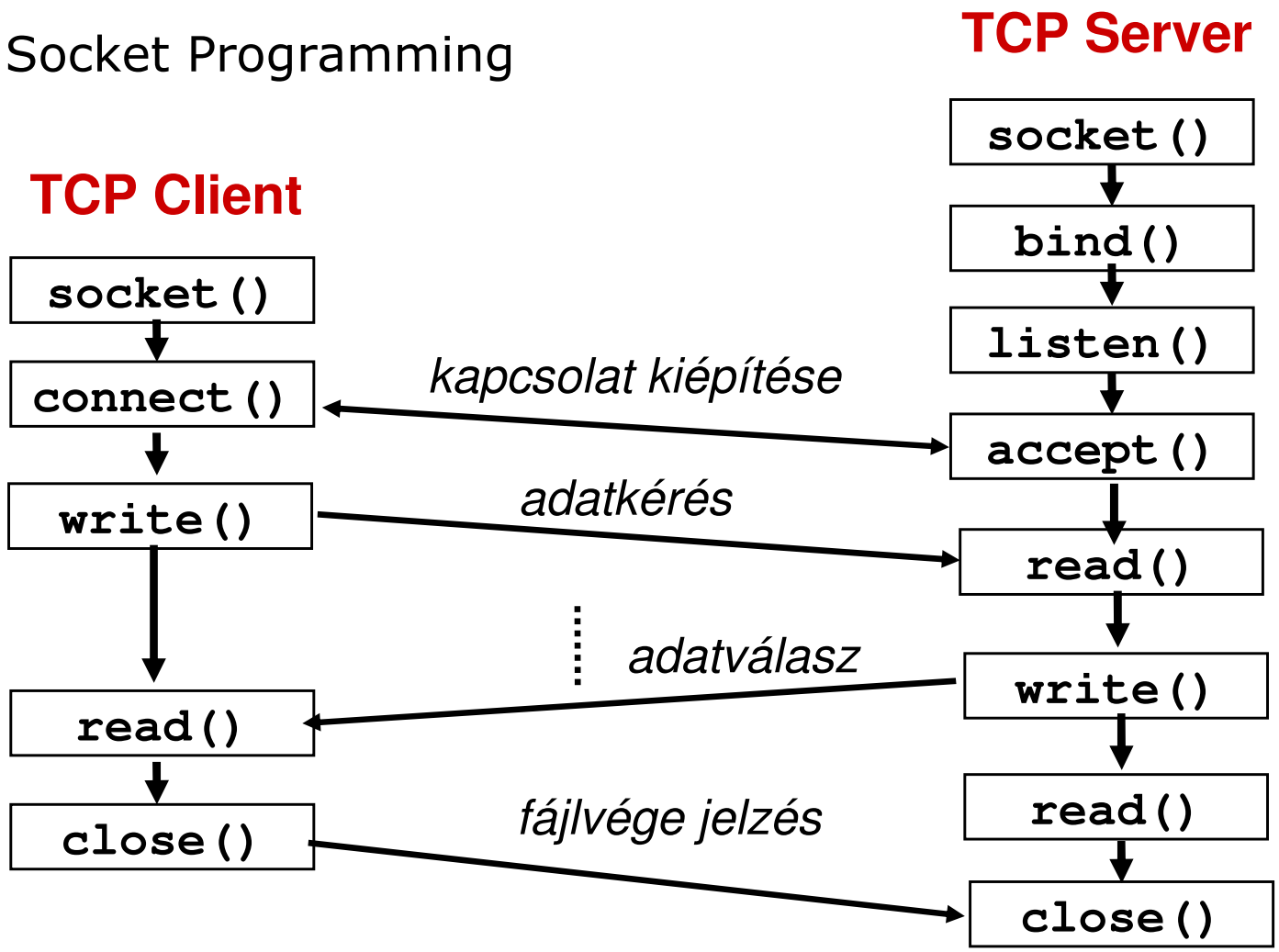
Példák protokollokra és portokra

- IP protokollok (kezdeti lista az RFC 790-ben)
  - 1: Internet Control Message Protocol (ICMP)
  - 2: Internet Group Management Protocol (IGMP)
  - 6: Transmission Control Protocol (TCP)
  - 8: Exterior Gateway Protocol (EGP)
  - 17:User Datagram Protocol (UDP)
  - 89:Open Shortest Path First (OSPF)
  - 132: Stream Control Transmission Protocol (SCTP)
- Ugyanígy TCP és UDP portokra
  - Az alkalmazás igényei (megbízhatóság) szerint
- Az IANA* felügyeli ezeket az azonosítókat

* Internet Assigned Numbers Authority

TCP kommunikáció sockethívásokkal

Socket Programming



Milyen alkalmazás milyen szállítási rétegbeli protokollon?

	IP	UDP	TCP
Kapcsolatorientált	✘	✘	✓
Megbízható	✘	✘	✓
Üzenetméret (tipikus)	rövid	rövid	hosszú
Adattovábbítás jellege	datagram	datagram	bitstream pipe
Portkezelés	✘	✓	✓
Overhead	minimális	kicsi	nagy
Alkalmazások	vezérlési és menedzsment •ICMP, IGMP •Routing	multimédia -átvitel, névfeloldás	fájlátvitel, web, levelezés

Infrastrukturális szolgáltatások

DNS – Domain Name System

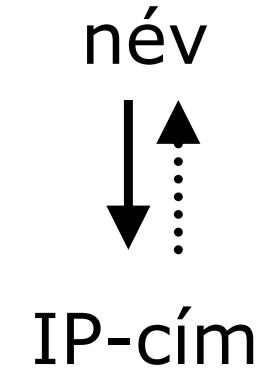
DHCP – Dynamic Host Configuration Protocol

Névfeloldási rendszer

DNS – Domain Name System

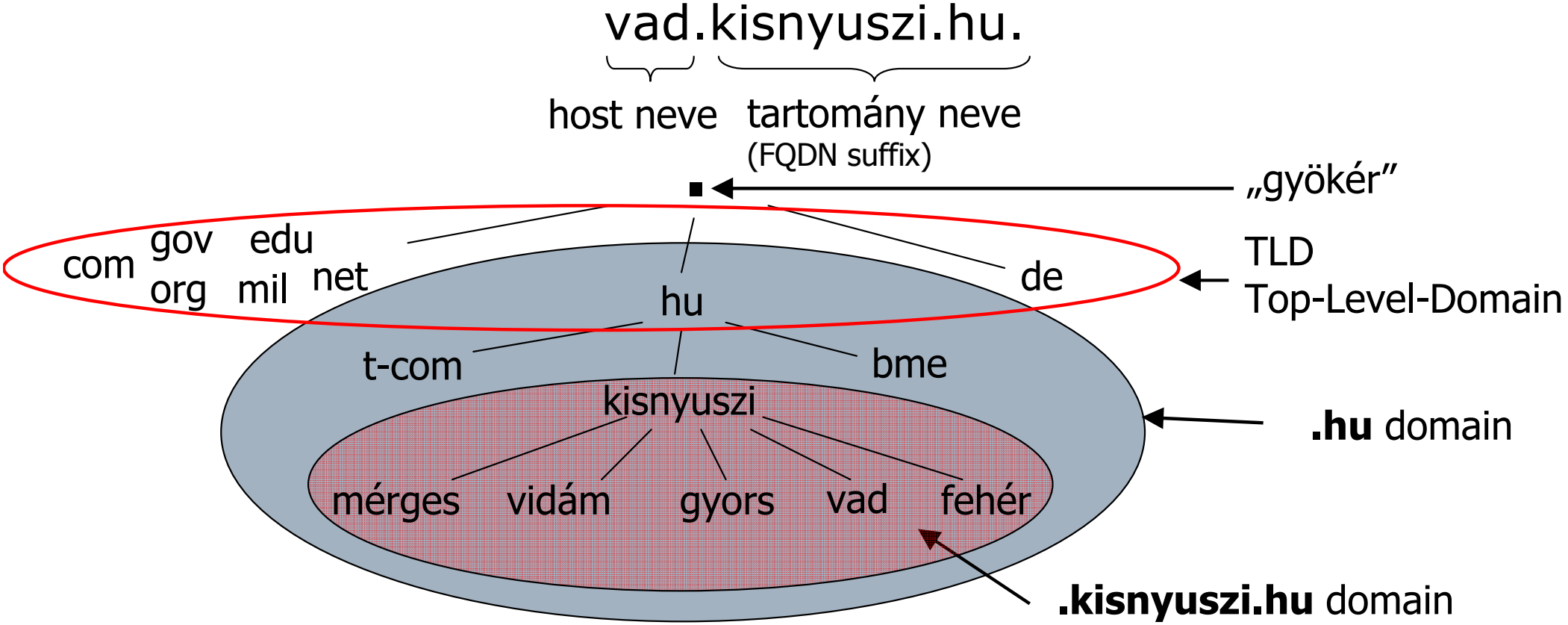
A névfeloldás szerepe és követelményei

- Eltérő reprezentációk közötti megfeleltetés
  - Humán: könnyen megjegyezhető, beszédes nevek
  - Gépi: IP-címek
  - → névfeloldás
- Követelmények:
  - Jó skálázhatóság
  - Hibatűrőség
  - Aktuális információk



A DNS (Domain Name System) névtere

- Hierarchikus
- Állomások azonosítása: FQDN (Fully Qualified Domain Name)

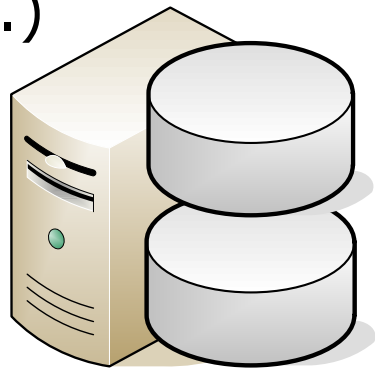


A DNS névtér „csúcsa”

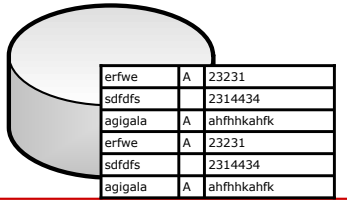
- Root (gyökér):
  - „.” – ponttal jelölik
  - Elméletileg minden FQDN emiatt ponttal zárul
  - Valójában világszerte kb. 16 DNS szerver szolgáltatja
- Top level domains: a név utolsó része
  - Az IANA adminisztrálja
    (Internet Assigned Numbers Authority)
  - country code top-level domains (ccTLD): pl. .hu
  - generic top-level domains (gTLD): pl. .org, .edu, .net, .com, .gov, .mil
  - infrastructure top-level domains: egy van, az .arpa

A DNS zóna és névszerverek

- Zóna
  - Minden tartomány csúcsát csúcsának vagy egészének adatit tároló adatbázis
  - A DNS nevével azonosítjuk (pl. kisnyuszi.hu.)
- DNS szerver
  - Egy vagy több zóna 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
  - Szinkronizálás monoton növekvő verziószám alapján



A zóna elemei: rekordok

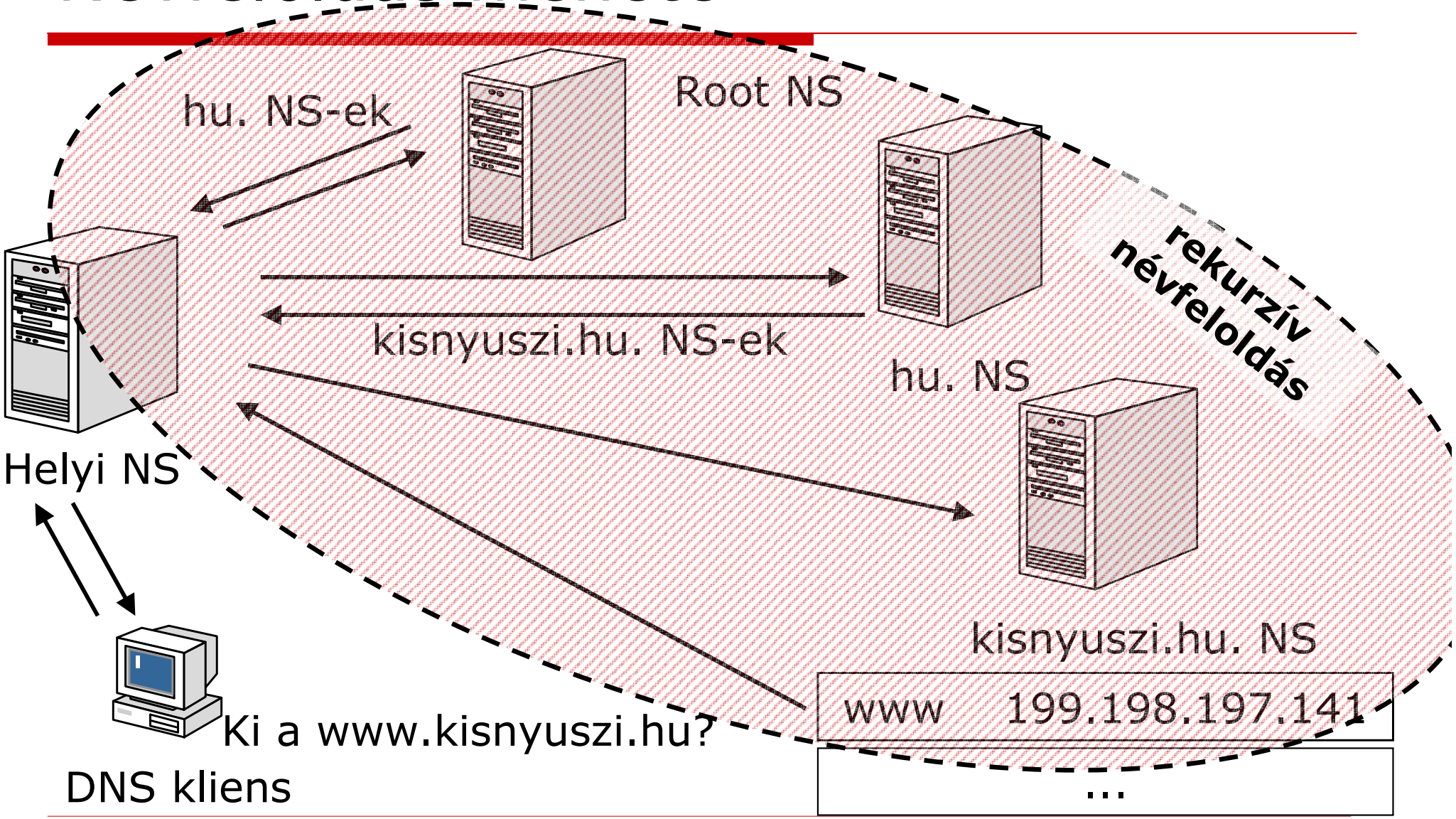


- SOA (Start of Authority)
  - adminisztratív adatok
    - az elsődleges DNS szerver neve
    - zóna verziószáma (ez alapján a szinkronizálás)
    - kapcsolattartó e-mail címe
- A (Address)
  - név – IP-cím
  - a legtipikusabb felhasználás
- CNAME (Canonical Name)
  - más néven „alias”
  - név – név összerendelés
- PTR (Pointer)
  - IP-cím – név
  - ún. reverse zónában
- NS (Name Server)
  - az adott zónát kiszolgáló DNS szerverek
  - legalább kettő kell
- MX (Mail Exchange)
  - SMTP kiszolgálót azonosít
  - Több is megadható preferenciával (prioritással)
- SRV (Service Locator)
  - MX általánosítása
  - tetszőleges szolgáltatásra

Altartományok (subdomain)

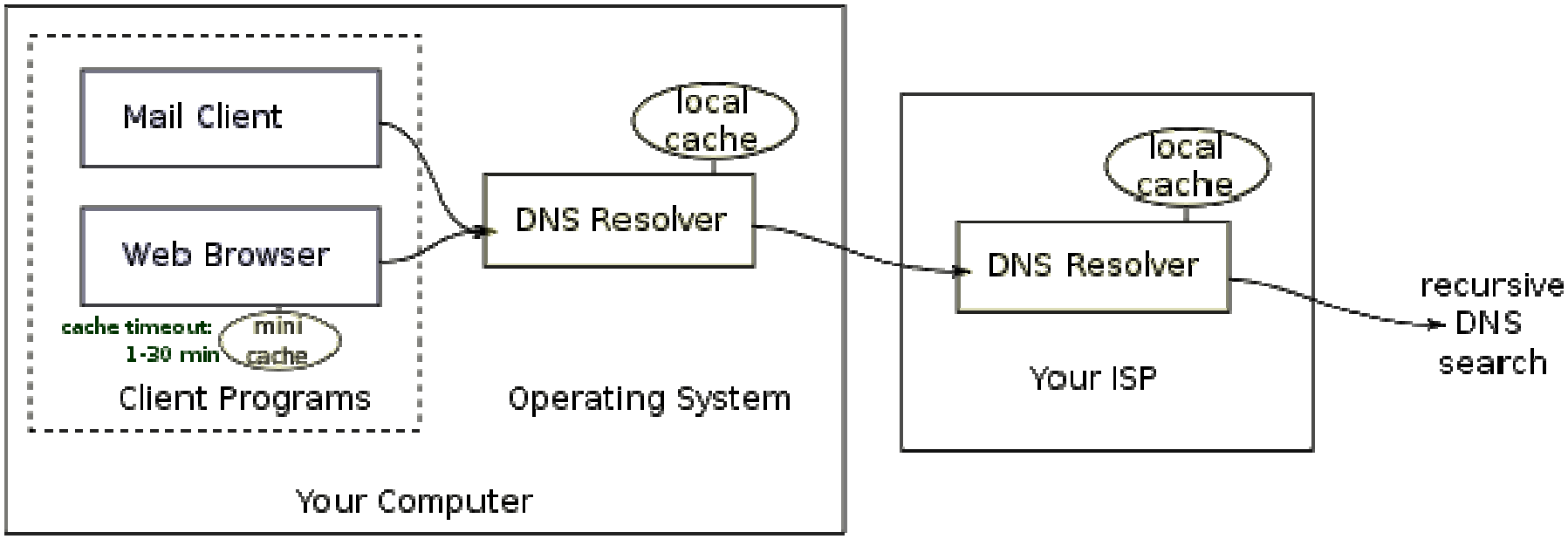
- delegálhatóság

Névfeloldás menete



Névfeloldás gyorsítótárral

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



- Minden rekordnak TTL-je (Time To Live) valódi másodpercben megadva → elévülés

Névfeloldás menete

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
       - Az a cache-ből kiszolgál vagy névfeloldást végez
     - Lekérdezés a másodlagos DNS szervertől, ha meg van adva és az elsődleges nem érhető el
   - Ha nincs DNS szerver megadva vagy nem elérhetők, akkor lekérdezés valamely root NS-től

A DNS mint protokoll

- A DNS protokoll felhasználási területei:
  - Lekérdezés:
    - DNS kliens ⇔ DNS szerver
    - UDP 53 ← rövid, gyors üzenetváltás
  - Zónaletöltés
    - Elsődleges DNS szerver ⇨ másodlagos DNS szerver
    - TCP 53 ← hosszabb, megbízhatóbb
- Protokollüzenetek tartalma
  - Kérés
    - Rekord típusa
    - Név vagy IP-cím
  - Válasz
    - Egy vagy több elemű lista
      - Ebből „véletlenszerűen” (round-robin) választ

DHCP

Dynamic Host Configuration Protocol

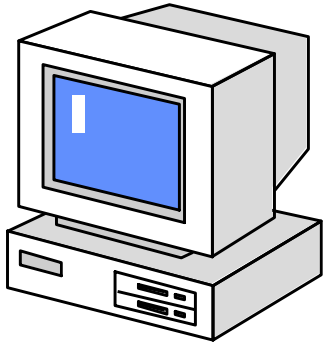
Általában a DHCP-ről

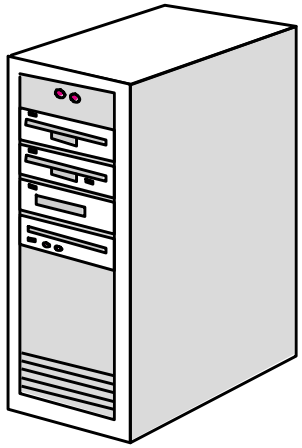
- Mi a DHCP?
  - IP-beállításokat oszthatunk ki vele dinamikusan
- Előnyei:
  - Nem kell tudni, hogy milyen címeket osztottunk már ki
  - Kliensek egyszerű beállítása.
  - Módosítások központilag
  - Mobilitás hálózatok között (eltérő beállítások)

IP cím igénylése

DHCP szerver

Igénylő



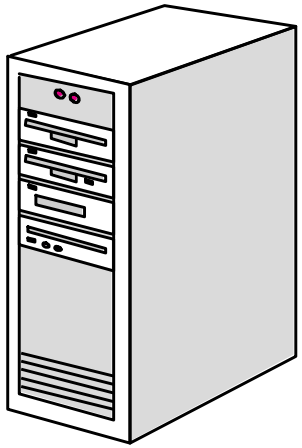


1. DISCOVER
Bérlet kérése

2. OFFER
Bérleti ajánlat

3. REQUEST
Bérlet kiválasztása

4. ACK
Bérlet nyugtázása



DISCOVER és OFFER
Bérlet kérése és felajánlása

- Kérés:

  0.0.0.0-tól → 255.255.255.255-nek
  (még nincs IP-címe) (bárkinek)

- Ajánlat:

  255.255.255.255-nek ← 192.168.1.1-től
  (bárkinek; nem címezhető) (egy DHCP szerver címe)

- Ajánlat tartalma
  - IP-cím
  - Alhálózati maszk
  - Bérleti idő
  - DHCP szerver IP címe

REQUEST és ACK
Bérlet kiválasztása és nyugtázása

- Kiválasztás
  - az első ajánlatot (pl. ha több DHCP szerver)
  - Kiválasztási üzenet:
    - 0.0.0.0-tól 255.255.255.255-nek
    - Az üzenet tartalma
      - kért IP cím
      - DHCP szerver IP címe
- Nyugta
  - 192.168.1.1-től, 255.255.255.255-nek
  - Nyugtázó üzenet tartalma
    - ajánlott IP cím
    - alhálózati maszk
    - bérleti idő

Bérleti idő (TTL)

- Bérleti időbeli kezelése
  - Félidőben hosszabbítási kérés
  - 7/8 TTL-nél új igénylése
- Hosszú vagy rövid TTL
  - Rövid mellett
    - Ha a kliens szabálytalanul távozik a hálózatból (a bérletét nem adja vissza)
    - Ha a kliens szabálytalanul újraindul (nem adja vissza a bérletét, és még újat is igényel)
    - A beállításváltozások gyorsan életbe lépjenek
  - Hosszú mellett
    - Ne legyen nagy hálózati forgalom

Ami DHCP-vel beállítható…
DHCP opciók, paraméterek

- **0x01 Subnet Mask (alhálózati max)**
- **0x0F Domain Name (FQDN suffix)**
- **0x03 Router (alapértelmezett átjáró(k))**
- **0x06 DNS (DNS szerver(ek))**
- **0x0C Host Name (gép neve is kioszthető)**
- 0x1F Router Discovery
- 0x21 Static Route
- 0x2B Vendor Specific (gyártófüggő beállítások)
- 0x2C WINS
- 0x2E NBT
- 0x2F Node Type
- **0x32 Requested Address (igényelt IP-cím)**
- **0x33 Lease Time (TTL)**
- **0x36 DHCP Server (DHCP szerver IP-címe)**
- **0x37 Parameter Request List (igényelt paraméterek listája)**
- **0x3A Renewal Time (megújítási idő)**
- 0x3B Rebinding Time
- 0x3C Client Class Information
- 0x4D User Class Information
- 0xF9 Static Route CIDR

Stb…

DHCP egyéb alkalmazása

- DHCP hibatűrés
  - Több DHCP használata egy hálózatban, de diszjunk IP-címtartományok osztása
- DHCP kiterjesztése
  - A routerek nem engedik át a DHCP üzeneteket
  - A routerekre ún. „DHCP Relay Agent”-et telepítve az továbbítja a DCHP forgalmat a DHCP szerverek és kliensek között
- Bootolás hálózatról
  - a DHCP kiegészítéseként tekinthető BOOTP protokollal
- IPv6-ban minden router egyben DHCP szerver is

Szöveg- és fájlátvitel

Telnet

FTP – File Transfer Protocol

Telnet

- Egyik legrégebbi alkalmazás
- Távoli parancssor
  - Parancsok elküldése
  - Visszajelzések megjelenítése
- Még ma is alkalmazzák főként hálózati eszközök egyszerű hálózati adminisztrációjára
- Nem biztonságos (jelszavak védelem nélkül)
  - SSH (Secure Shell) helyette

FTP – File Transfer Protocol

- Az egyik legelső fájlátvitelre tervezett protokoll
- RFC 959
- TCP 21-es port
  - Ha a TCP 20-as portot használjuk adatcsatornaként, akkor ez csak vezérlés
- Parancsok
  - open – kapcsolat létrehozása
  - ls – aktuális könyvtár listázása
  - put – feltöltés
  - get – letöltés
  - delete – törlés
  - bye – kapcsolat lebontása
  - …
- Adattípus figyelembevétele (~ megjelenítési réteg)
  - ASCII
  - Binary

Levelező rendszerek

SMTP – Simple Mail Transfer Protocol

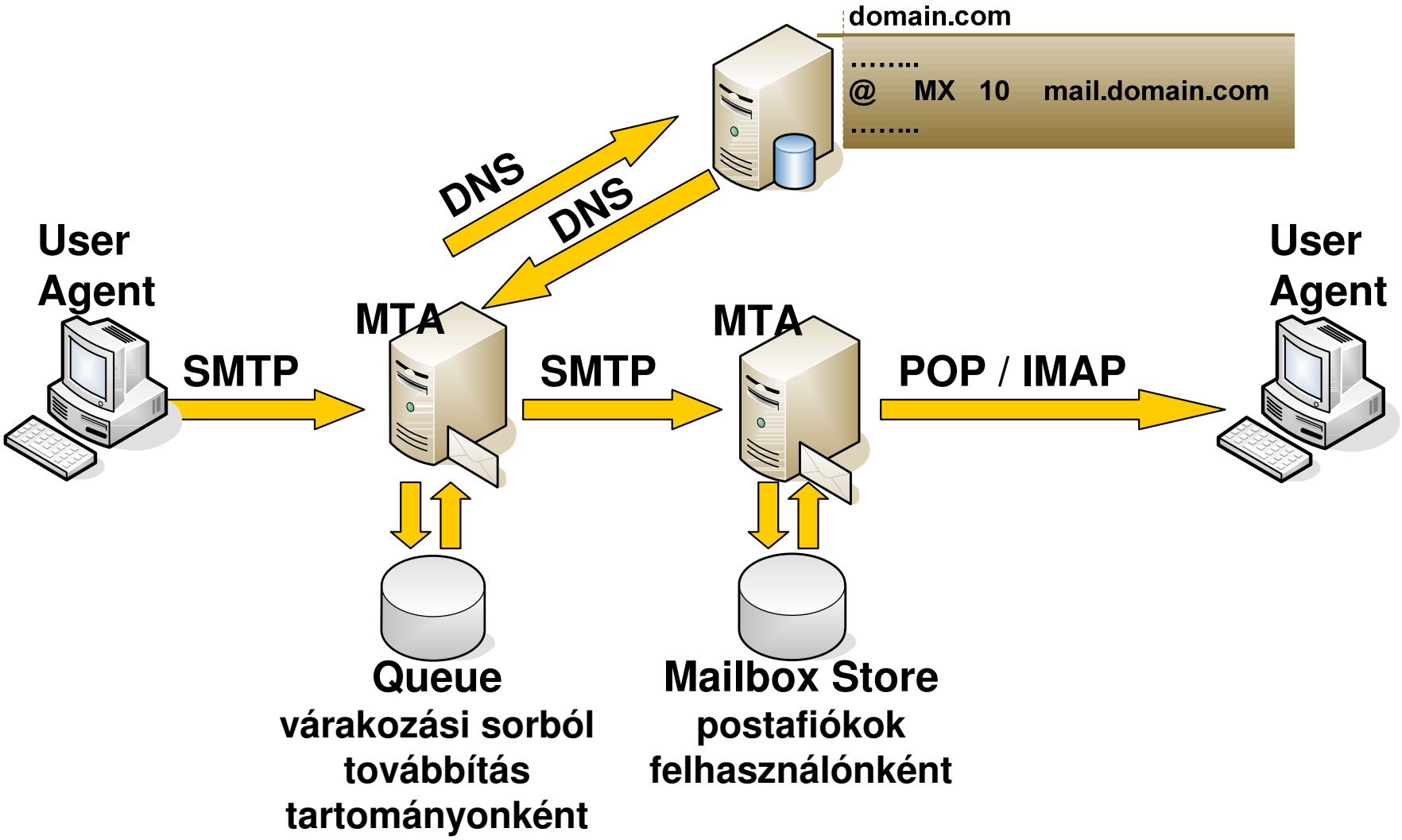
POP3 – Post Office Protocol v3

IMAP4 – Internet Message Protocol v4

Levelező rendszerek

- Komponensek
  - User Agent (levelező kliens)
  - MTA (Mail Transfer Agent) (SMTP szerver)
- Használt protokollok
  - SMTP: levél továbbításra
  - POP3: levelek lekérdezése
  - IMAP4: levelek lekérdezése
- Cél meghatározása
  - DNS segítségével (MX rekord)

Levelező rendszerek



Levelek lekérdezése – POP3 és IMAP4

- POP3
  - Post Office Protocol version 3
  - RFC 1939, 1957, 1725
  - Parancsorientált
  - TCP 110-es port
  - Levelek lekérdezésére
  - POP3S
    - POP3 TLS tikosítással
    - TCP 995
- IMAP4
  - Internet Message Protocol version 4
  - RFC 2060, 1731, 1730
  - Parancsorientált
  - TCP 143-as port
  - Levelek lekérdezésére
  - IMAP4S
    - IMAP4 TLS tikosítással
    - TCP 993
  - Intelligensebb a POP3-nál:
    - Könyvtárstruktúra támogatása
    - Keresés támogatása
    - Nem törli automatikusan a szerveren tárolt leveleket

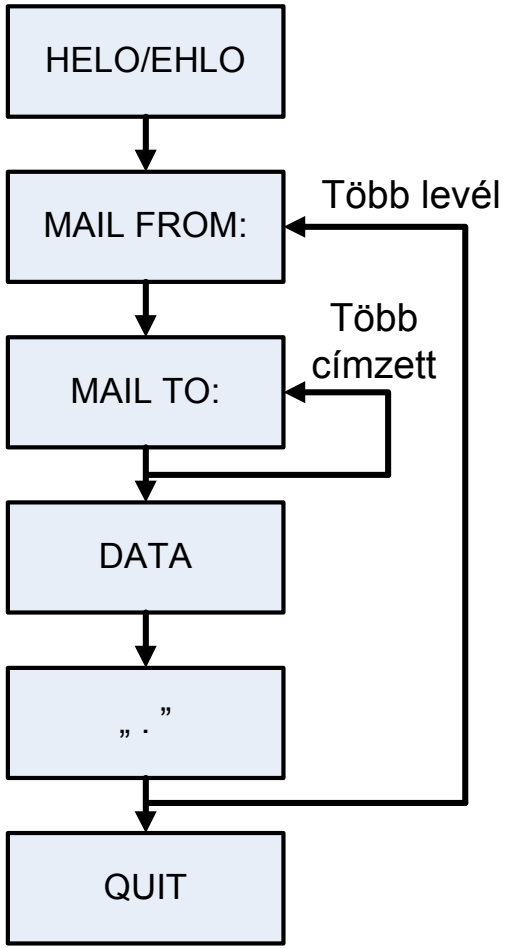
SMTP – Simple Mail Transfer Protocol

- RFC 821, 822
- Levelek továbbítására (első „killer application”)
- Parancsorientált állapotkódokkal
- TCP 25-ös port
- SMTP relay
  - Nem közvetlen továbbítás
  - Egy (vagy több) SMTP (relay) szerver közbeiktatásával
- SMTPS (SMTP Secure)
  - SMTP TLS csatornában
  - TCP 465
- Kiterjesztések:
  - RFC 2197, 1830, 1845, 1869, 1870, 1891, 1985, 2034
  - ESMTP
    - Extended SMTP
    - Kibővített parancskészlet és funkcionalitás

A leggyakoribb SMTP parancsok

- HELO
  - Üdvözlés
  - ESMTP esetén EHLO
- MAIL FROM:<feladó e-mail címe>
- RCPT TO:<címzett e-mail címe>
- DATA
  - Adat következik
- <CR><LF>.<CR><LF>
  - Adat vége
- QUIT
  - SMTP kapcsolat bontása
- VRFY <e-mail cím>
  - Létezik-e az adott e-mail cím
- HELP
- NOOP
  - Kapcsolat ellenőrzése, fenntartása

Tipikus kapcsolat folyamatábrája



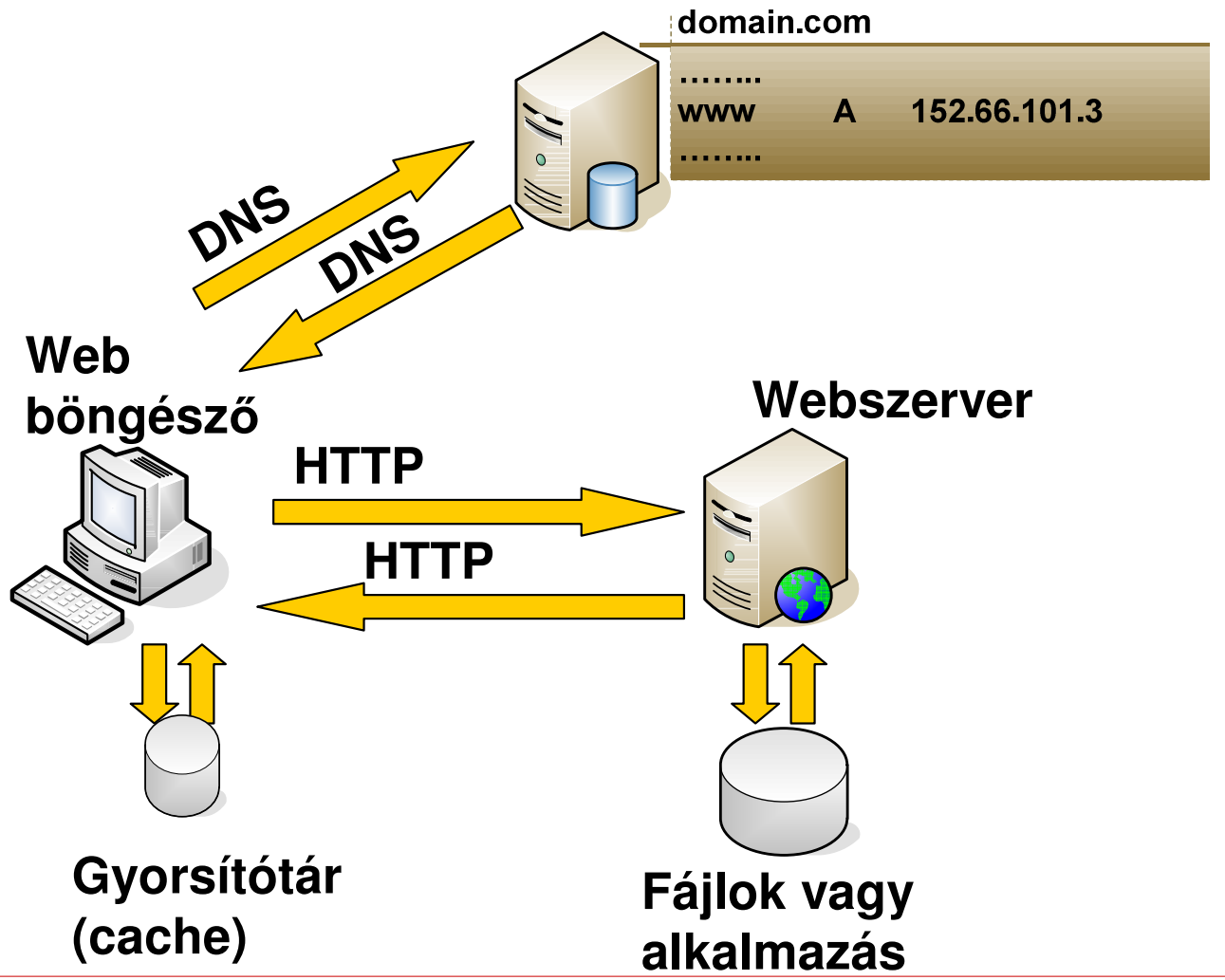
Példa egy SMTP kommunikációra

S: 220 lappfold.fi
C: HELO bme.hu
S: 250 Hello bme.hu, pleased to meet you
C: MAIL FROM: <jogyerek@bme.hu>
S: 250 jogyerek@bme.hu... Sender ok
C: RCPT TO: <mikulas@lappfold.fi>
S: 250 mikulas@lappfold.fi ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Kedves Mikulás!
C: Jó gyerek voltam. Hozzál sok csokit!
C: Köszönöm,
C: Jógyerek Jóska
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 lappfold.fi closing connection

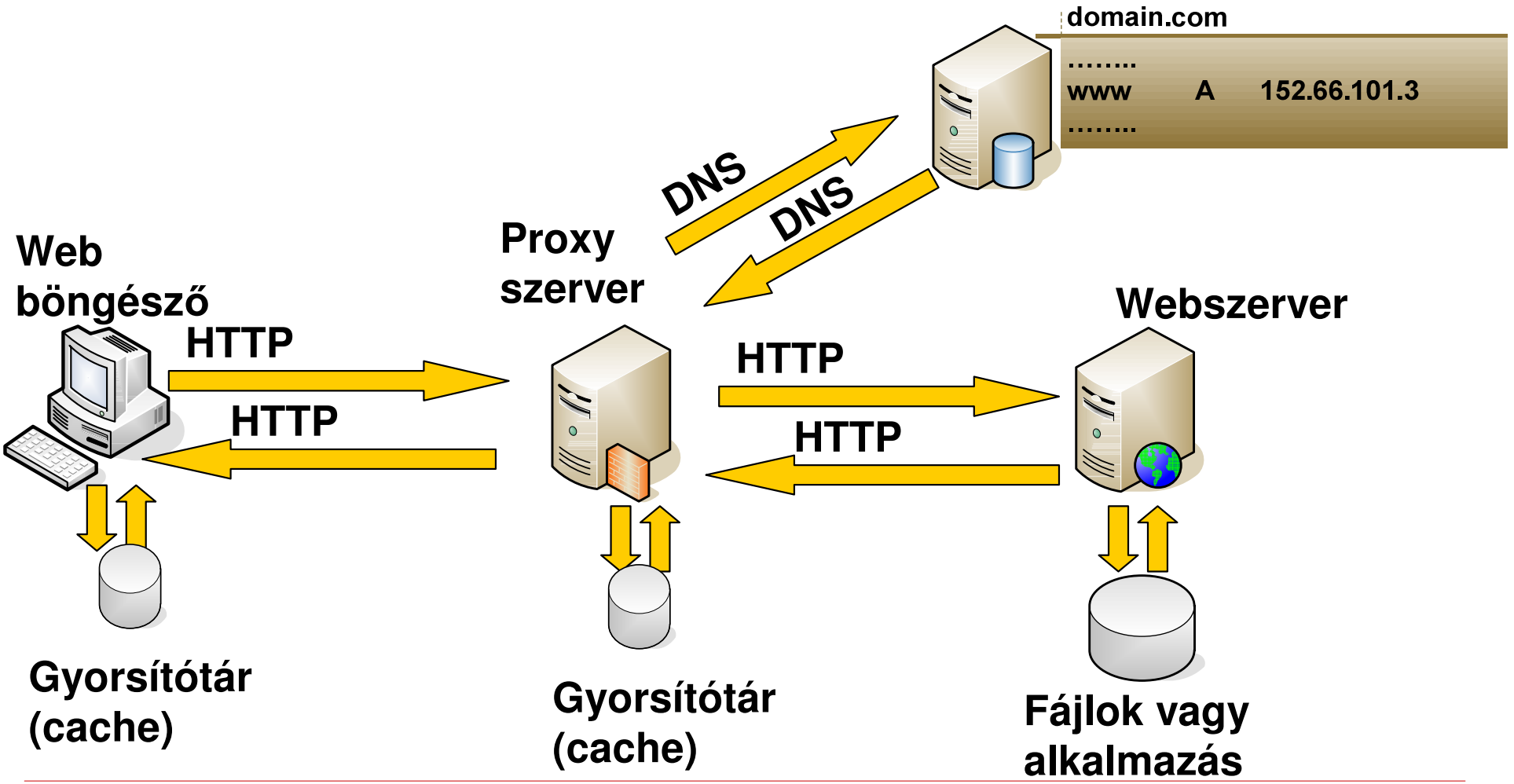
Webes rendszerek

HTTP – HyperText Transfer Protocol

Webes rendszerek



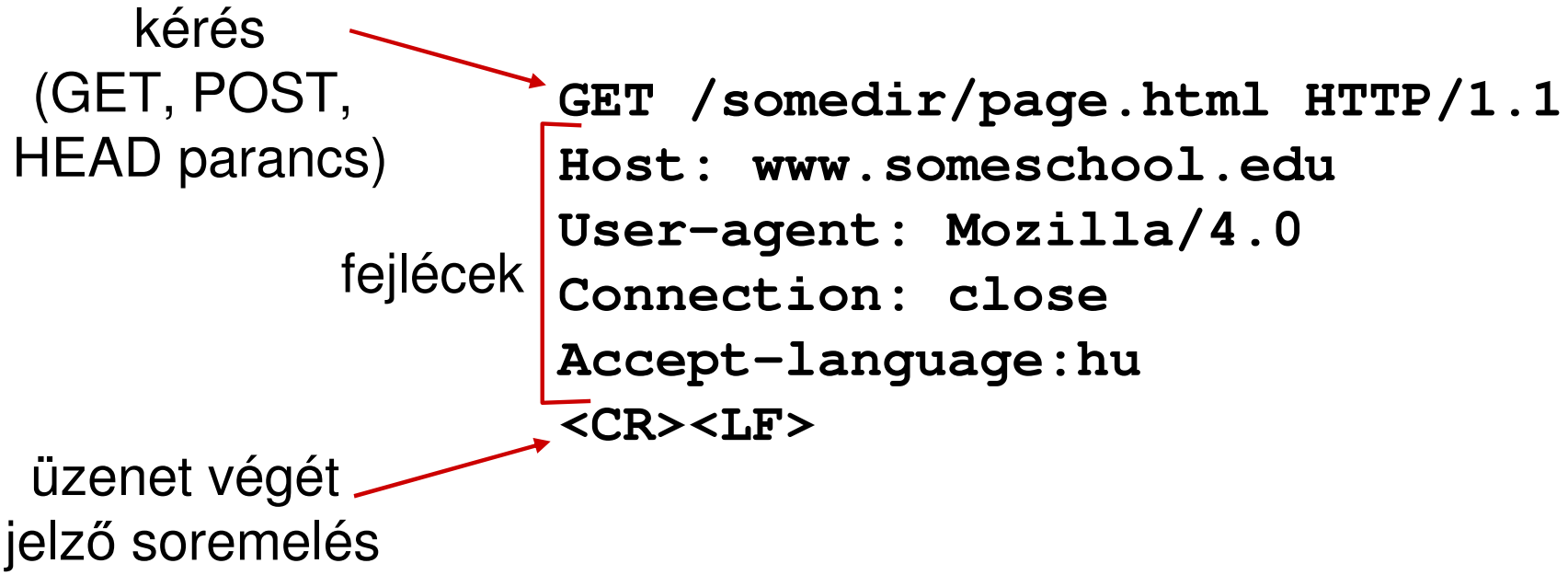
Webes rendszerek proxyval



HTTP – HyperText Transfer Protocol

- RFC 2068
- Web
  - Tim Berners-Lee, CERN
  - a második „killer application”
- Parancsorientált állapotkódokkal
- Speciális fejlécek
- TCP 80
- Proxy
  - Kliens nevében jár el
  - Főként a hatékony gyorsítótárazás miatt
  - NAT helyett
  - Általában TCP 8080

Példa egy HTTP kérésre



Gyakori HTTP parancsok

- GET <URL> HTTP/1.1
  - adott URL tartalmának lekérése
- HEAD
  - mint a GET, de csak a metaadatokat adja vissza
- POST
  - a kliens ezzel tud adatokat küldeni a szervernek
- PUT
  - a POST-hoz hasonló, fájlfeltöltésre alkalmas
- DELETE
  - adott URL tartalmának törlése

Gyakori HTTP fejlécek

- Accept: elfogadható MIME típus
- Accept-Charset: elfogadható karakterkészlet
- Allow: szerver által támogatott parancsok
- Authorization: támogatott hitelesítési módok
- Content-Encoding: tömörítés típusa
- Content-Length: tartalom mérete
- Content-Type: MIME típus
- Date: lekérés dátuma és ideje
- From: a látogató e-mail címe (nem authentikációra)
- Pragma: nem meghatározott paraméter (pl. „no-cache”)
- Referer: a hivatkozó oldal URL-je
- Retry-After: 503 utáni újrapróbálkozási idő
- Server: szerver neve és verziója
- User-Agent: böngésző neve és verziója
- WWW-Authenticate: Hitelesítési információk (credentials)

Példa egy HTTP válaszüzenetre

állapotkód

fejlécek

```
HTTP/1.1 200 OK
Connection close
Date: Thu, 06 Aug 1998 12:00:15 GMT
Server: Apache/1.3.0 (Unix)
Last-Modified: Mon, 22 Jun 1998 …...
Content-Length: 6821
Content-Type: text/html
```

adat
(pl. a kért
HTML fájl)

```
data data data data data ...
```

Gyakori HTTP állapotkódok

Kód	Jelentés	Leírás
200	OK	
201	Created	POST sikeres
202	Accepted	Kérés elfogadva
204	No content	Nincs semmi a kliensnek
400	Bad request	Hibás kérés
401	Unauthorized	Hitelesítés szükséges
403	Forbidden	Hozzáférés megtagadva
404	Not found	Nem található
500	Internal Server Error	Belső szerver hiba
503	Service Unavailable	Pillanatnyilag nem szolgálható ki

HTTP alkalmazási területei

- HTML
  - statikus oldalak
    - Beágyazott tartalommal (pl. képek)
  - dinamikus oldalak
    - PHP, ASP, JSP, CGI, DHTML, ASPX, (ActiveX Control)
- Fájl le- és feltöltés
  - Kiegészítés: WebDAV
    - HTTP parancs- és fejléc-bővítmény
    - FTP-hez hasonló fájlkezelés
    - Hozzáféréskezelés (meg van nyitva írásra, ennek megújítása)
- Webszolgáltatások (WebService)
  - RPC-hez hasonló távoli eljáráshívás
  - SOAP
    - HTTP-n XML alapú kérés/válasz
- Protokollalagút
  - Más protokollokat HTTP-be csomagolva visznek át
  - Tűzfalak kijátszása (HTTP 80-as port mindenhol engedélyezve)

HTTP biztonság

- Hitelesítés
  - Névtelen hozzáférés (Anonymous)
  - Alapvető (Basic)
    - Base64 kódolás
  - Digest
    - Challenge/response alapú
  - Integrált (Integrated)
    - LANMan
    - NTLM
    - Kerberos
  - Tanúsítvány (Certificate)
  - Egyéb
- HTTPS
  - HTTP SSL-en (PKI:RSA; DES, 3DES)
  - TCP 443

HTTP áttekintés

- Webes rendszerek
- HTTP-ről általában
- HTTP parancsok
- HTTP fejlécek
- HTTP kódok
- HTTP proxy és cache
- Gyakori hitelesítési protokollok
- HTTPS: biztonságos HTTP
- WebDAV
- Gyakori alkalmazásai:
  - HTML: statikus és dinamikus oldalak
  - Fájl le- és feltöltés
  - Webszolgáltatások (SOAP)
  - Protokollalagút

Összefoglalás

- Alkalmazások hálózati kapcsolata
  - Portok és socketek használata
- Infrastrukturális szolgáltatások
  - DNS – Névfeloldási szolgáltatás
  - DHCP
- Szöveg- és fájlátvitel
  - Telnet, FTP
- Levelezési rendszerek
  - SMTP, POP3, IMAP4
- Webes rendszerek
  - HTTP