

5. gyakorlat

Ismétlés

Számítási példák

Illusztrációk

Demonstrációk

Tartalom

- Policing/Traffic shaping (Varga Endre)
 - „Leaky bucket” – „lyukas vödör”
 - „Token bucket” – „token vödör”
- MPLS (Simon Vilmos)
 - Gyakorlati felhasználás
 - Egy példa
- DNS szerver a gyakorlatban

Tartalom

- SMTP és HTTP – kliens nélkül
(Szeifert Gergő és Barabás Miklós)
- E-mail és webserverver a gyakorlatban
- VPN és tűzfalak – előadás
- NAT és tűzfal a gyakorlatban
 - Egy nagyvállalati tűzfal
(Microsoft Internet Security and
Acceleration Server (ISA))

Policing / Traffic shaping

„Leaky bucket” – „lyukas vödör”
„Token bucket” – „token vödör”

(Varga Endre)

Részletes anyag hamarosan feltöltésre kerül!

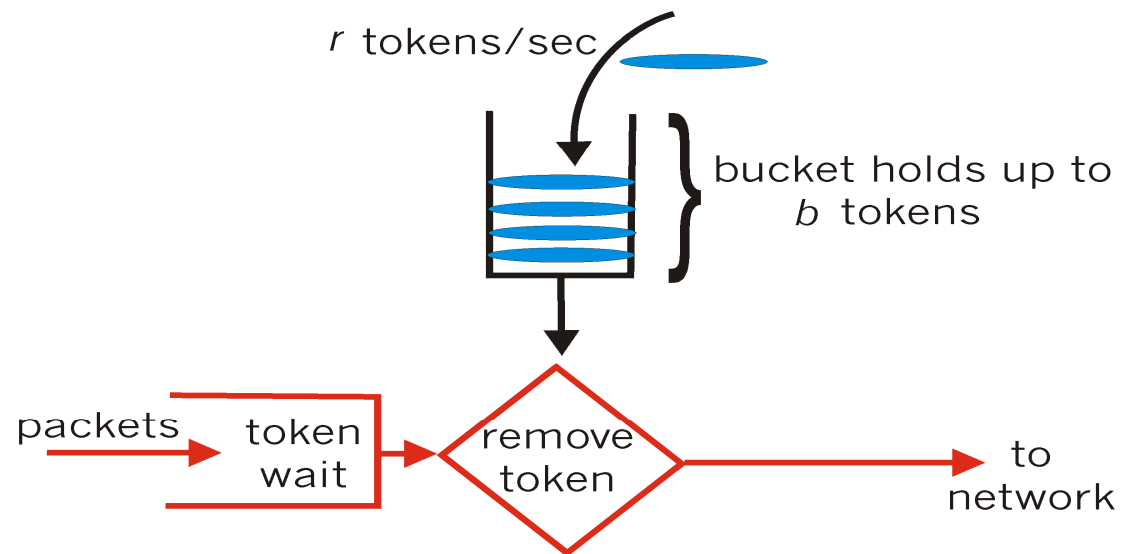
Forgalomleírás és policing

A policing és a forgalomleírás eszköze: a token bucket (token vödör)

A vödör formálja (szűri) a forgalmat: küldhetünk b méretű borsztöt, de az átlagsebesség csak r lehet

Ezeket a paramétereket (is) használjuk a TSpec-ben

- A vödörbe r sebességgel töltődnek a tokenek
- Legfeljebb b token lehet benne, ha már tele van, a beérkező tokenek elvesznek, túlsordulnak
- Ha egy n hosszú csqg érkezik, kivesz n token a vödörből (ha van annyi) és továbbításra kerül
- Ha nincs: ...



MPLS a gyakorlatban

Multi-Protocol Label Switching

(Simon Vilmos)

Részletes anyag hamarosan feltöltésre kerül!

Motiváció

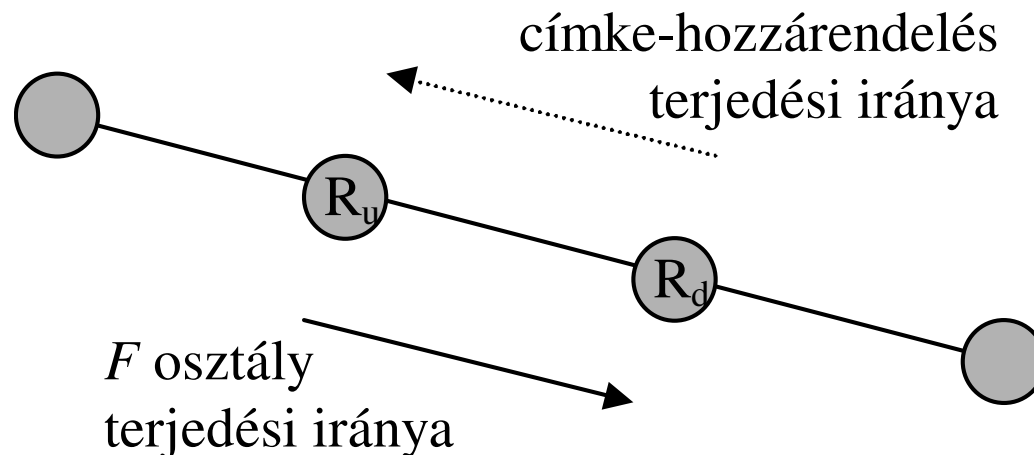
- Hagyományos IP routerekben:
 - Fogadja a bejövő csomagot, előfeldolgozás
 - Meghozza a routing döntést
 - Megfelelő forgalmi osztályokba sorolja a beérkező csomagot
 - Komplex feladat, hardware-rel nem támogatható.
 - Kimenő interface-en sorbanállítás (QoS)
- Nem skálázható router terhelés!

MPLS alapelve

- Egyes osztályokhoz címkéket (label) rendelhetünk
 - ami az osztály rendeltetési helyét írja le
 - elég az egész osztályt csupán a címkét megvizsgálva továbbküldeni
- Router feladata
 - táblázatból kikeresi a bejövő csomag címkéje alapján a következő címkét és az irányt, amerre ki kell küldenie
 - **Label Switched Router (LSR)**

Címkék

- A **címke (label)**: rövid, rögzített hosszúságú azonosító, helyi érvényű, LSR szabadsága



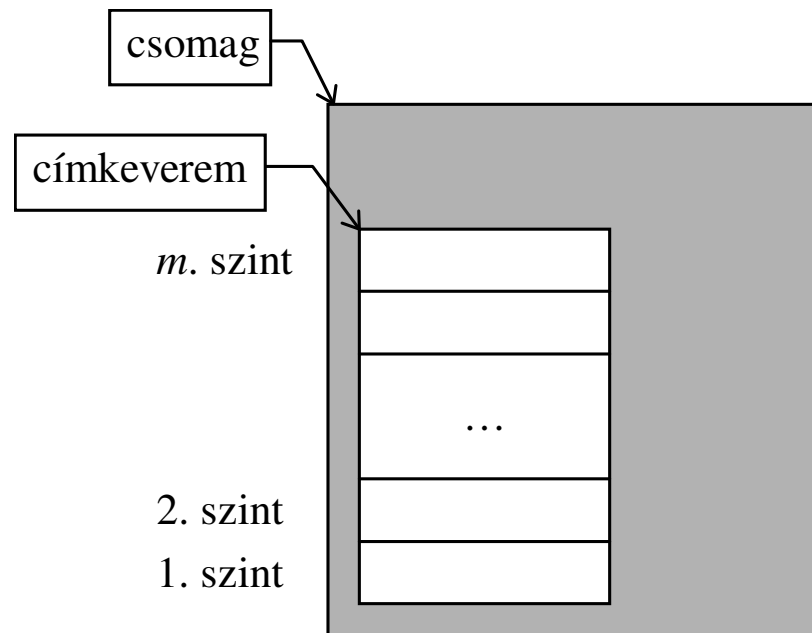
- Lehet közöttük egy nem-MPLS alapú alhálózat van: az MPLS technológia szempontjából átlátszó

Címkeelosztási protokoll – LDP (Label Distribution Protocol)

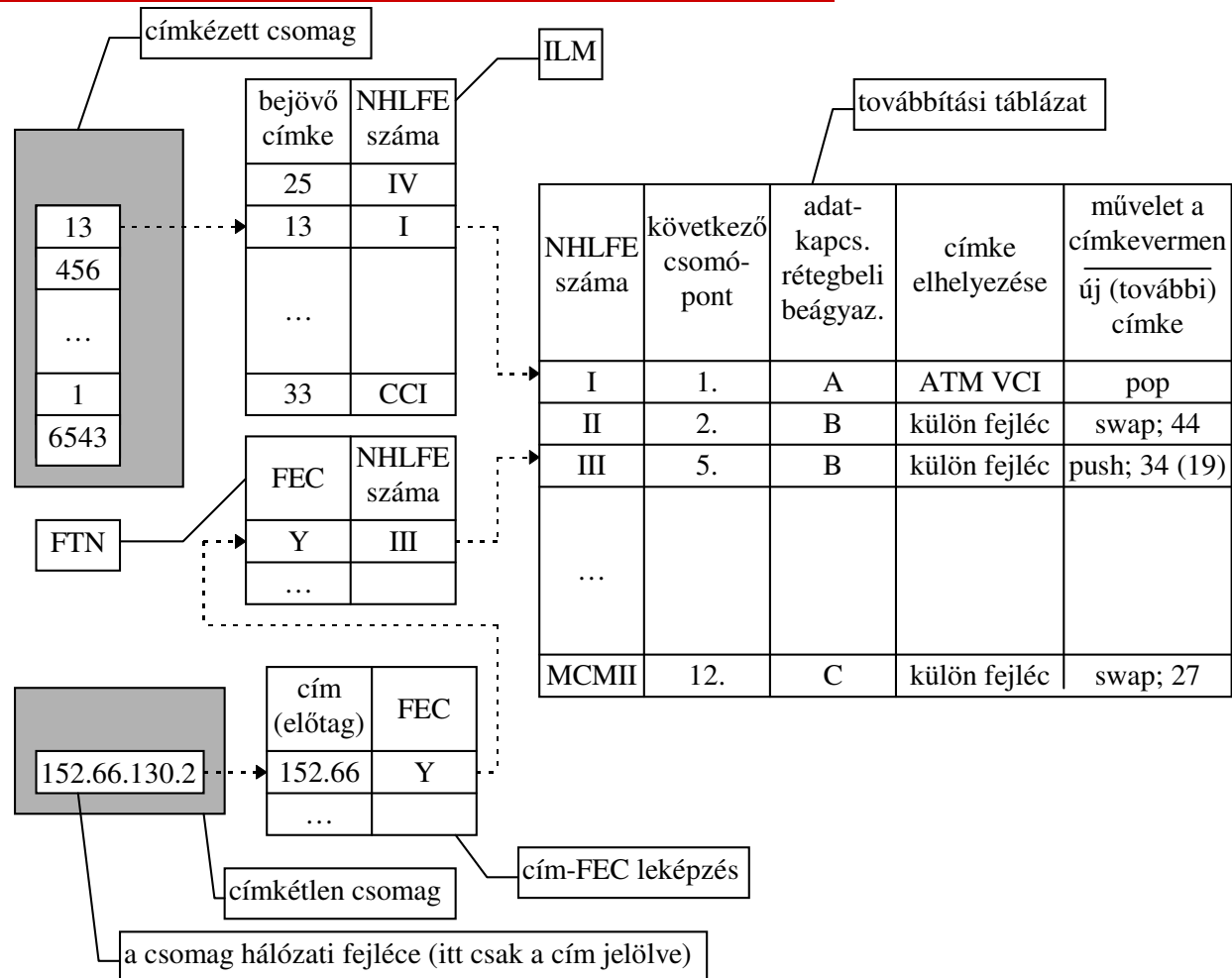
- **elosztó társak (LDP peers)**
- megegyeznek az elosztás részleteiben
 - **kérés szerinti elosztás (downstream-on-demand)**
 - Egy LSR kérheti egy osztály számára címke hozzárendelését a lefelé eső LSR-től
 - **kérés nélküli elosztás (downstream)**
 - A lefelé eső LSR közölheti a hozzárendelést kérés nélkül is, pl. mikor döntött róla
- a létrejött megállapodás csak kettejükre tartozik, az esetleg közbeeső csomópontokra nem

Címke verem (label stack)

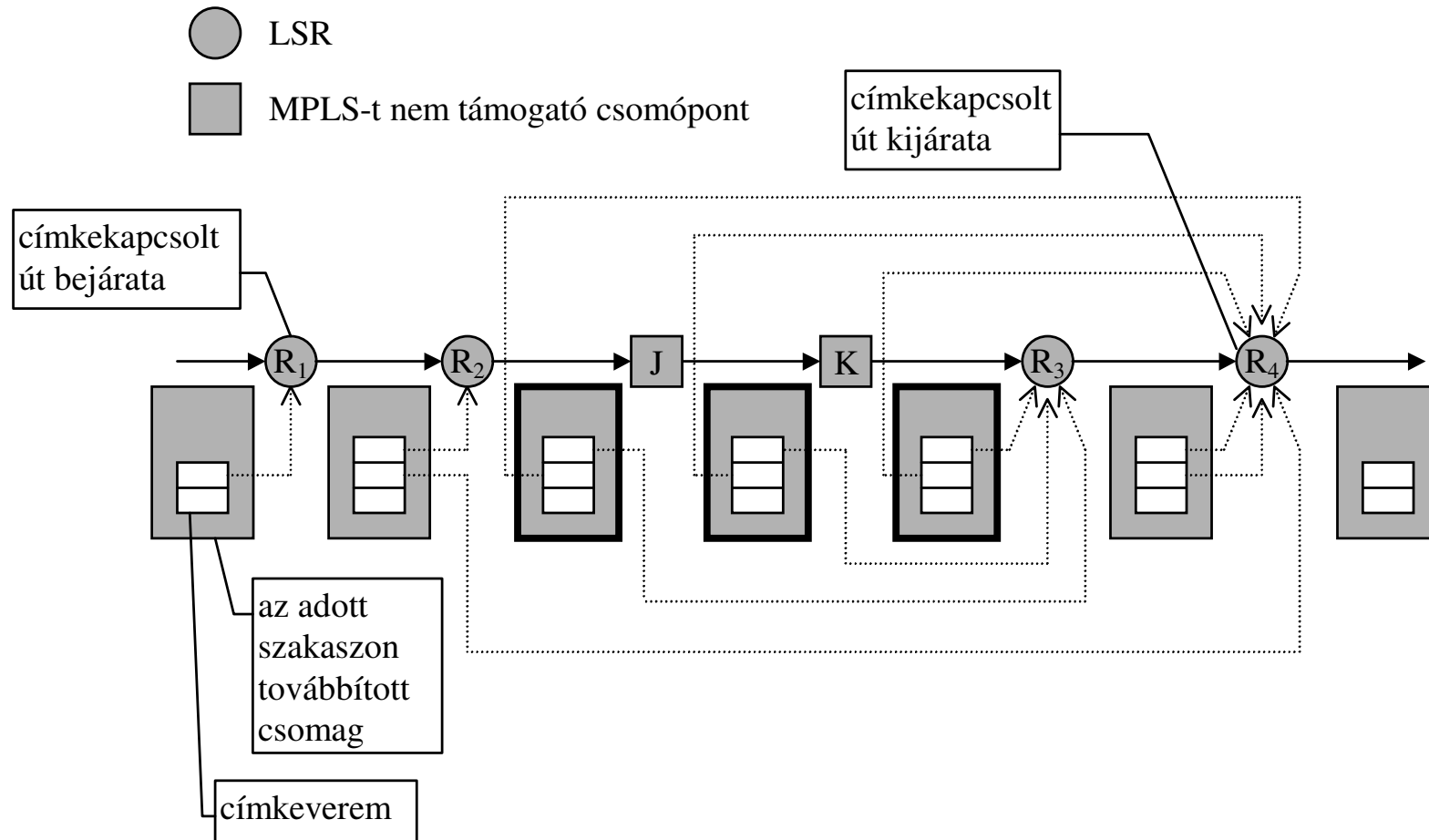
- Több címke tartozik egy csomaghoz
- Az útvonal kiválasztásában viszont mindig csak a legfelső címke vesz részt
 - függetlenül attól, hogy hányan vannak alatta a veremben és korábban mi volt rápakolva



Példa: csomagok továbbítása

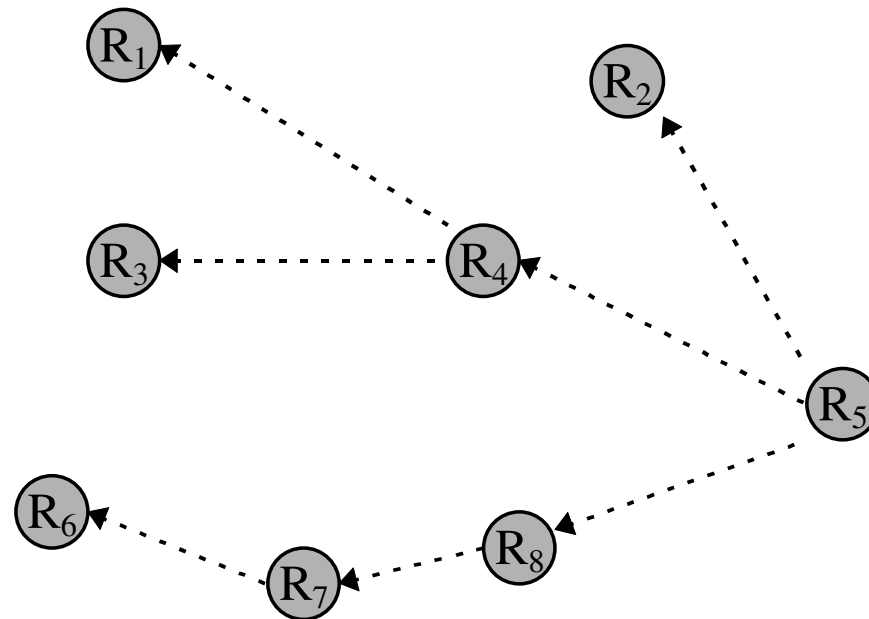


Példa: Címkekapcsolt út (Label Switched Path)

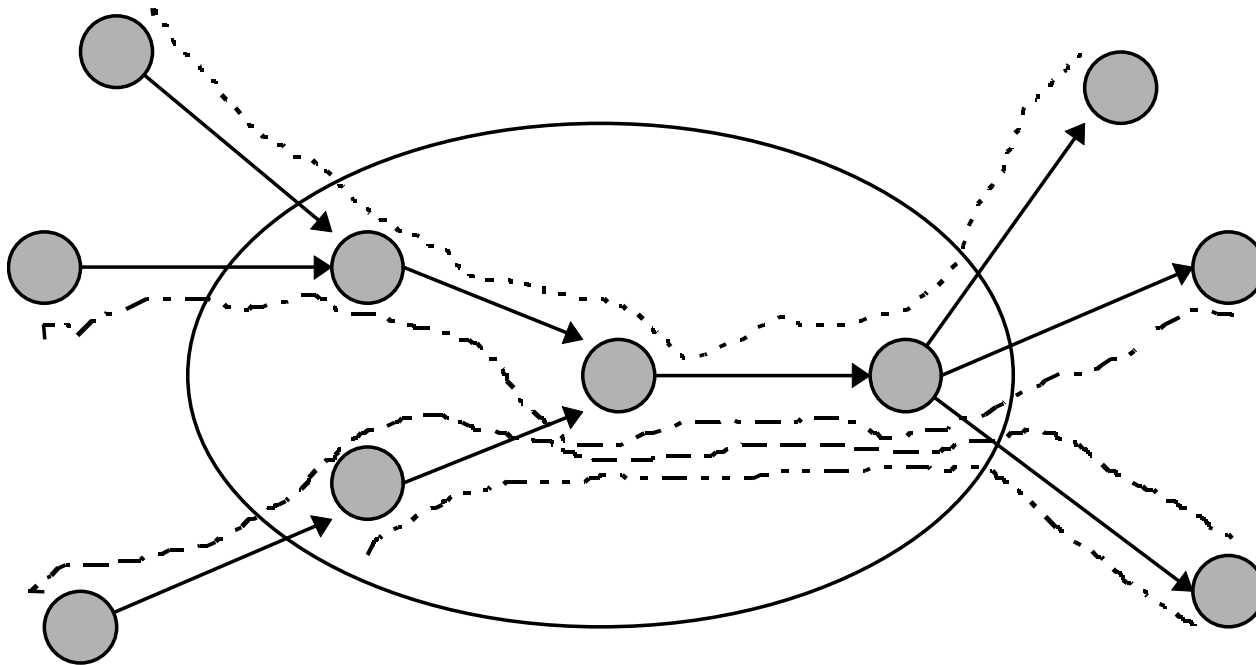


Egy rendezetten felépülő LSP fa

- Biztosítani akarjuk, hogy a forgalom valamilyen meghatározott úton haladjon
 - nem érint egy csomópontot kétszer
 - a forgalom nem terheli túl a továbbító csomópontokat
 - egy meghatározott nyomvonalat kövessen



Osztályegyesítés



Alkalmazása

- ❑ Forgalomvizsgálat (traffic analysis)
- ❑ Forgalommenedzsment (traffic engineering)
- ❑ Több útvonalas forgalom
- ❑ Csoportos üzenetek küldése ún. **multicast fák**
- ❑ VPN (Virtual Private Network)

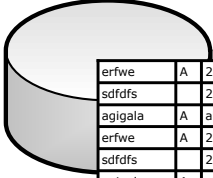
DNS

DNS névfeloldás - nslookup DNS szerver a gyakorlatban

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 elérhető, akkor lekérdezés valamely root NS-től

A zóna elemei: rekordok



erfwe	A	23231
sdfdfs		2314434
agigala	A	ahfhkahfk
erfwe	A	23231
sdfdfs		2314434
agigala	A	ahfhkahfk

- 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

SMTP és HTTP

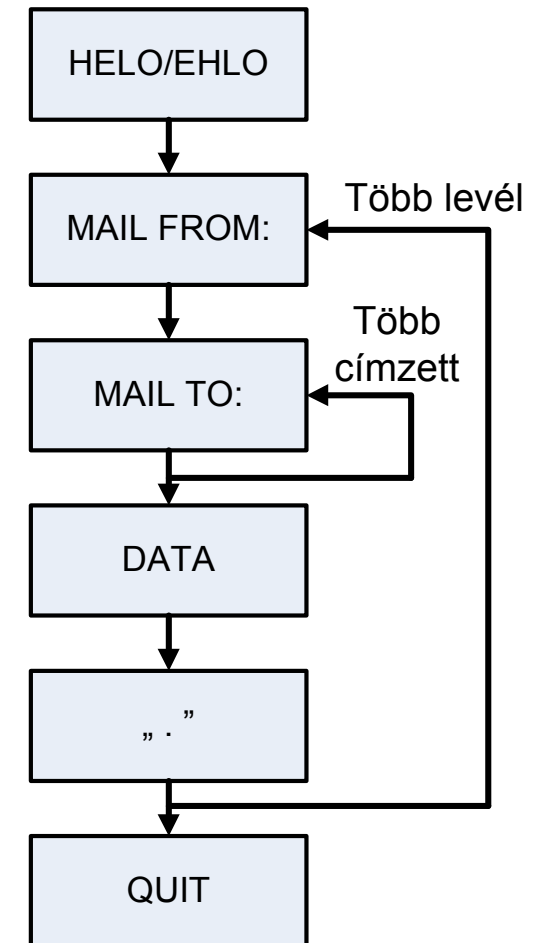
Kliens nélkül (telnettel)

(Szeifert Gergő és Barabás Miklós)

A leggyakoribb SMTP parancsok

- HELO
 - Üdvözlés
 - ESMTP esetén EHLO
- MAIL FROM:<feladó e-mail címe>
- RCPT TO:<címzett e-mail címe>
- DATA
 - Adat következnek
- <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

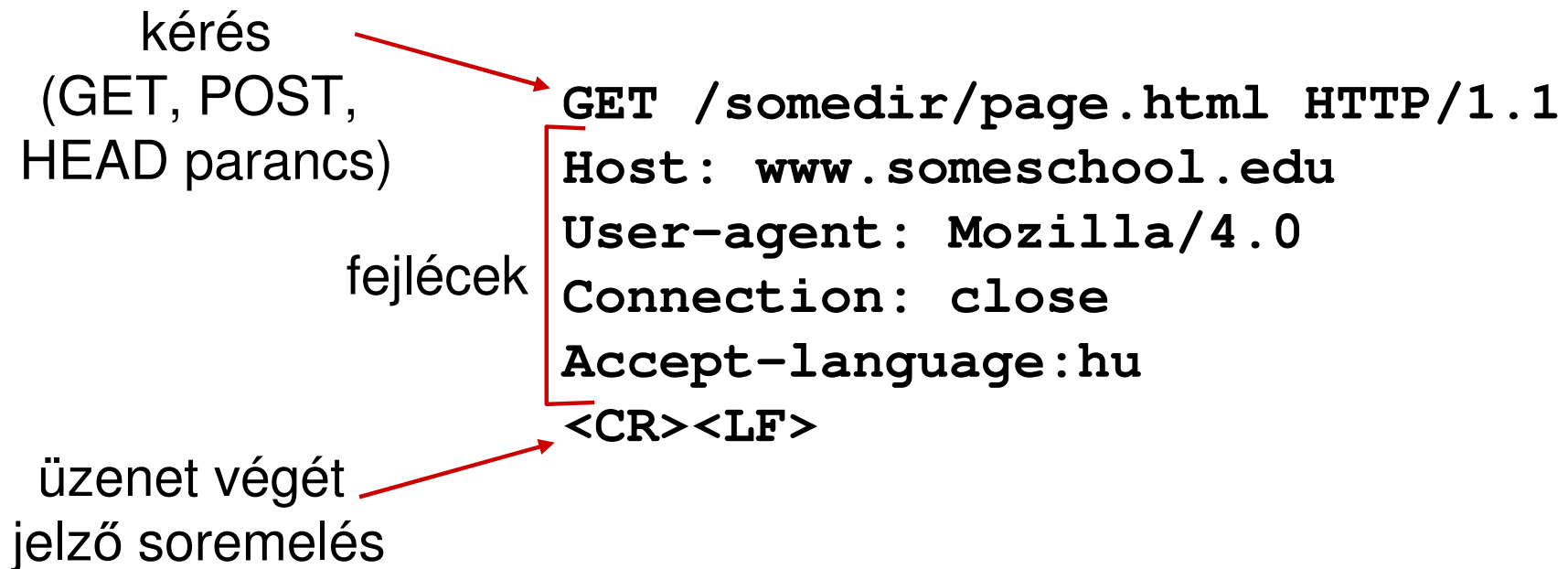
Tipikus kapcsolat folyamatábrája



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. Hozzá sok csokit!
C: Köszönöm,
C: Jógyerek Jóska
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 lappfold.fi closing connection
```

Példa egy HTTP kérésre



Példa egy HTTP válaszüzenetre

állapotkód

HTTP/1.1 200 OK

fejlécek

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 ...

E-mail és webszerver

Microsoft Exchange Server

Microsoft Internet Information Server (IIS)

Hálózatbiztonság

II. rész

További számonkérések

□ pótZH

- 2009. május 13. (szerda) 17:00-19:00
- HSZK (R épület, 3-4. emelet)
- Beosztás a moodle-ön!

□ pótpótZH

- 2009. május 19. (kedd) 8:00-10:00
- HSZK (R épület, 3-4. emelet)

□ Vizsgák

- 1. és 2. héten kedden
- 3. és 4. héten kedden és csütörtökön
- 9:00-11:00

Egyéb információk

- Követelmények
 - Sikeres 1. és 2. kisZH
 - Heti tesztekből legalább 8 (nem pótolható)
 - Heti tesztekből legalább 36 pont
- Szerdai óra
 - Összefoglalás
 - Videó
 - Rövidített (pótZH miatt)
- Moodle új címen
 - <http://moodle.hit.bme.hu>
- Csütörtöki heti teszt
 - Alkalmazások
 - Hálózatbiztonság