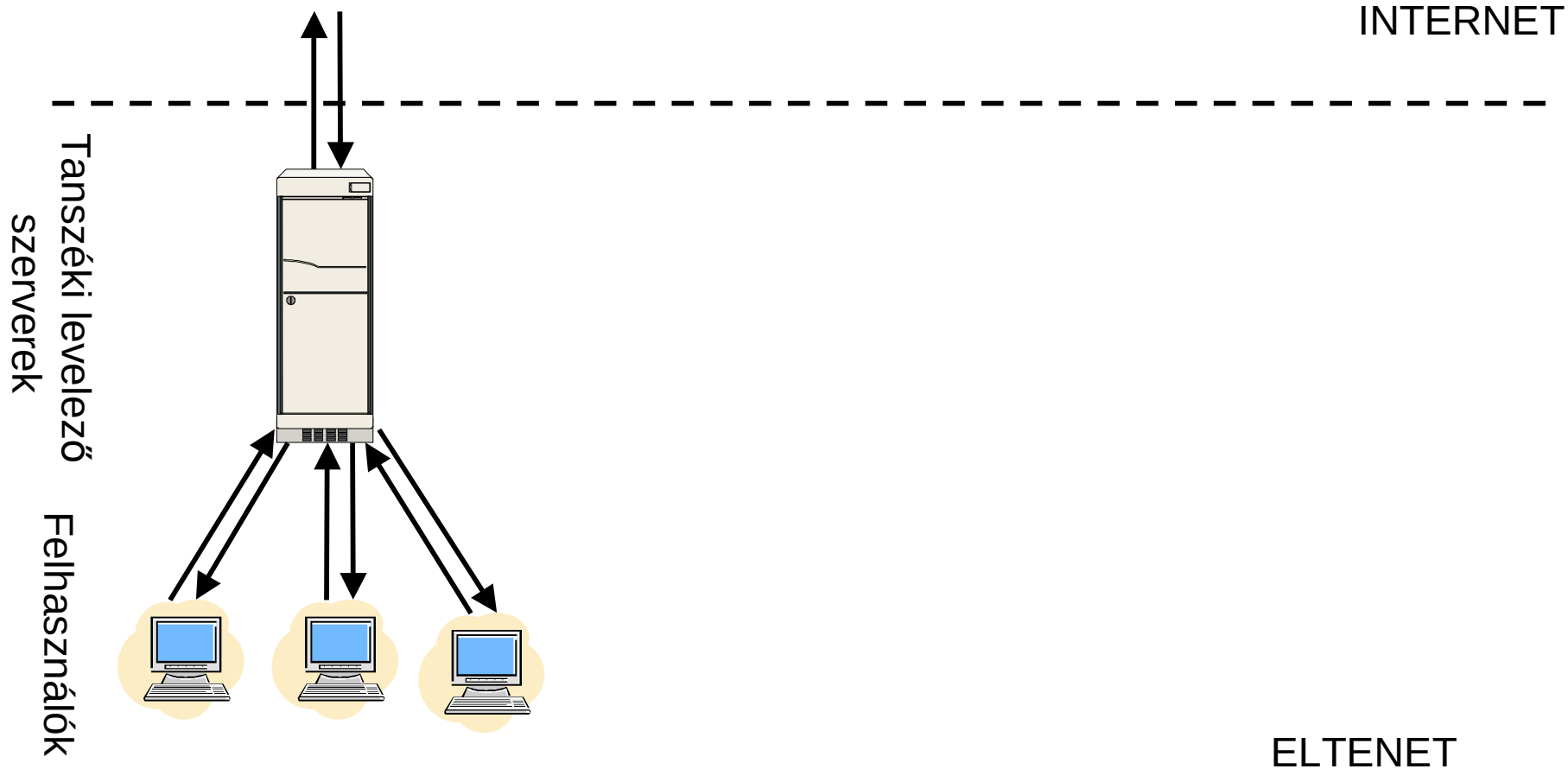
Levelezés az ELTE-n, avagy hogyan szűrünk mi

Debreceni Dalma, Turi Péter
ELTE Információtechnológiai Központ
postmaster@elte.hu

Amiről szó lesz ...

- Történeti áttekintés:
  - őskáosz
    - A felmerült problémák
  - egy szebb új világ
    - ... ami még mindig nem tökéletes
- Hogyan szűrünk most?
- Mérési adatok, eredmények

Levelezés – a kezdetek

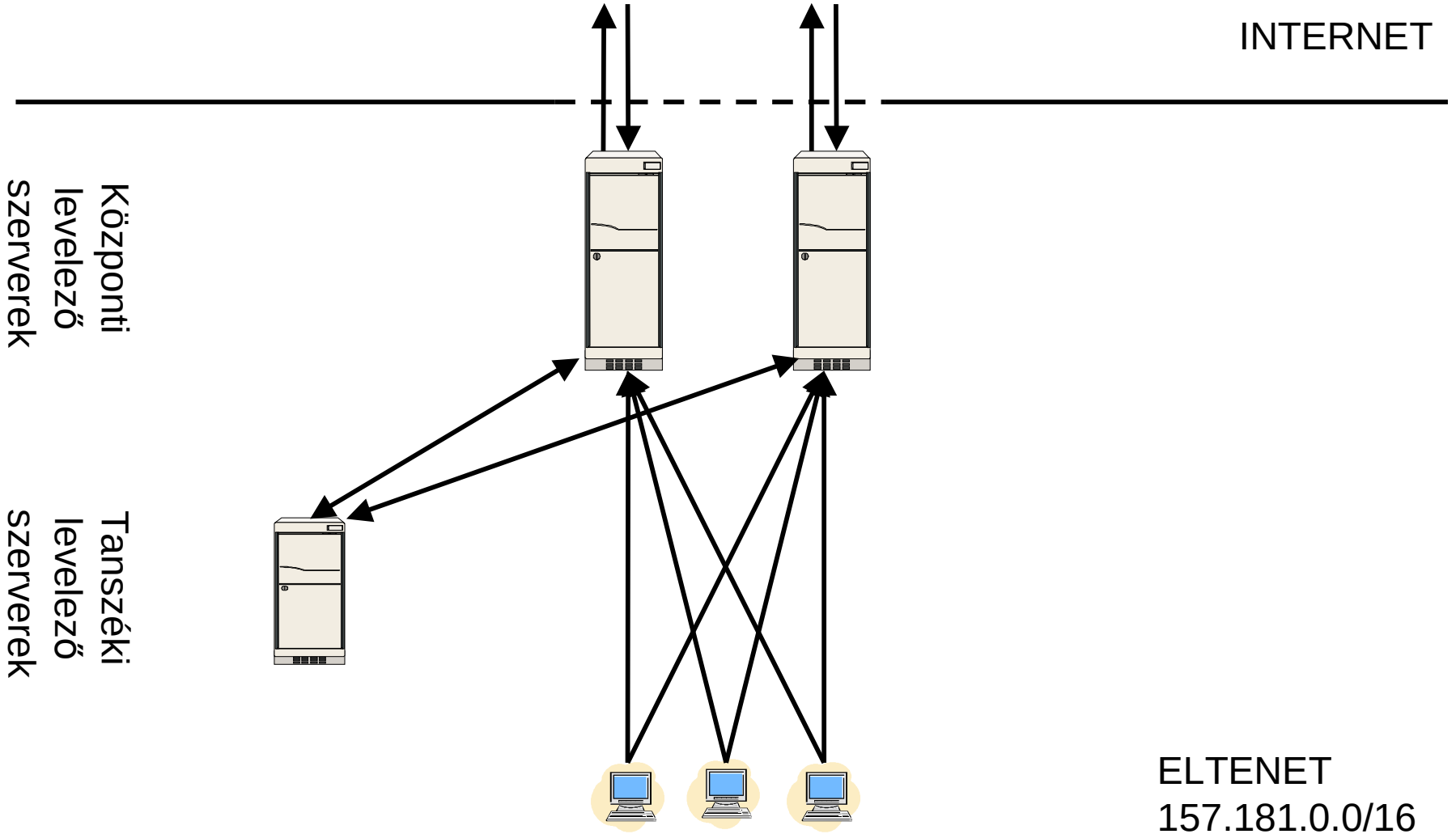


ELTENET
157.181.0.0/16

Problémák

- ELTENET-ért az ITK a felelős, minket vonnak felelősségre
  - nincsenek levelezési naplóink (Ki spammelt?, Elment a levelem?)
  - nem ellenőrizhető a HBONE szabályzat betartása (Üzleti felhasználás, külső domainek)
- Szórványszerverek alul képzett rendszergazdákkal
  - open relay
  - egyéb konfigurációs hibák

Központosított levelezés



Problémák ... újra

- A fenti problémákat megoldja, de
  - túlterhelhető gépek (CPU, IO)
  - a leveleket mindenképpen elfogadjuk
  - felhasználói ellenállás a változásokkal szemben
  - kellene “láthatatlan” központi vírus és spam szűrés
  - spam nem csak attól spam, hogy a spamassassin azt mondja

Megoldások

- Túlterhelhető gépek
  - IO: azonnal nem kézbesíthető levelek külön szerveren való tárolása
- A leveleket mindenképpen elfogadjuk
  - levél átvétel közbeni szűrés (SMTP)
  - ne generáljunk felesleges levelet a vírusról

Jelenleg

Kapcsolódik a kliens.

Kitiltottuk az adott gépet? (Ha igen, viszlát)

Kliens mondja: *HELO*!
Tényleg köszön? És ha igen, akkor mekkorát hazudik?

MAIL FROM, RCPT TO

- Greylist
- Tiltólisták
- ORDB
- SPF
- visszapattanó levelek esetén egy címzett
- feladó ellenőrzése (sender verify)
- címzett ellenőrzése

DATA

- Visszapattanó levelek esetén valódi(nak tűnő) feladó
- Vírus és spam szűrés
  - korlátok
  - jelölés módja (fejlécek)
  - visszapattintott vírusok (és spamek)
  - hibás mime

Terhelési adatok – az eredmény