Központi felhasználómenedzsment

Központosított felhasználómenedzsment

- Samba 4
- NIS
- LDAP

NIS

- Network Information System
- Korábbi neve Sun Yellow Pages (YP)
- Konfigurációs állományok adatbázisa (pl. jelszavak)
- Egy mester (elsődleges) szerver és több szolga (másodlagos) szerver
- Konfigurációs állományok módosítása csak a mester szerveren
- Minden Unix rendszer támogatja

NIS

- Pl. /etc/password → jelszó térkép
- Letöltve a másodlagos szerverekre
- A NIS kliensek nem a lokális password állományt használják, hanem lekérdezik a szervert
- NFS-el kiegészíthető
  ha a felhasználó bárhonnan jelentkezik be,
  ugyanaz a saját könyvtára

NIS térképek

- Minden szöveges konfigurációs állományból egy bináris adatbázis-állomány
- Tartomány
- /var/yp/ és /var/yp/tartománynév/
- 2 mező: kulcs és érték
- Egy keresett adathoz 3 információ szükséges: tartománynév (NIS-gyakorlat), térképnév (passwd.byname), kulcs (geza)

NIS szerver beállítás

- NIS doménnév megadása
  - nem kell azonos legyen a DNS tartománnyal
  - biztonsági ajánlás: eltérő név

Szerver beállítás

- Ez a host legyen egyben NIS ügyfél is
- Gyors map disztribúció
- Engedélyezi jelszavak cseréjét (GECOS: teljes név; shell)
- Egyéb általános beállítások
  - yp forráskönyvtár: /etc
  - Jelszavak összeolvasztása: shadow→passwd
  - Csoportok összeolvasztása: gshadow→group
  - Minimális UID és GID (ez alatt nem oszt szét=titkos)

Szerver térképek beállítása

- Mi lesz elérhető a hálózaton: group, hosts, mail, netid, passwd, rpc, services, shadow
- Ki kérdezheti le?
- Kötelező:
  - Hálózati maszk: 255.0.0.0
  - Hálózat: 127.0.0.0
- Mindenki:
  - Hálózati maszk: 0.0.0.0
  - Hálózat: 0.0.0.0

Módosítások érvényesítése

- Ha a közzétett adatbázisok közül valamelyikben módosítunk, pl. új felhasználó felvétele
- Akkor a bináris (közzétett) adatbázist is módosítani kell:
- cd /var/yp
- make –C
- Konfig. áll. /var/yp/Makefile

Kliens beállítása

- szerver is lehet NIS kliens, ilyenkor 127.0.0.1
- egyébként pl.: 192.168.xxx.xxx

Kézi beállításhoz kiegészítés

- RPC portmappernek futnia kell
- /etc/passwd –ben kiegészítő sor:
  - +::::::
- /etc/shadow –ben kiegészítő sor:
  - +::::::::
- /etc/group –ban kiegészítő sor:
  - +:::

Néhány parancs

- yppasswd – NIS jelszócsere
- ypchfn – GECOS infók cseréje
- ypchsh – shell csere
- ypwhich – szerver nevének lekérdezése
- ypdomainname – NIS tartománynév lekérdezés és csere
- hostname

Name Service Switch

- /etc/nsswitch.conf
- Milyen sorrendben történjen a keresés az egyes adatbázisokban és konfigurációs állományokban – hálózati információk (passwd, group, aliases, hosts, netmasks, etc.)
- Felépítés: szolgáltatás : specifikációk
- nis, nis-plus, files, db, dns, compat

Name Service Switch

- Pl.:

```
passwd:     files ldap
hosts:      files ldap dns
netmasks:   files
```

LDAP

- Lightweight Directory Access Protocol
- Kliens-szerver protokol címtár szolgáltatás eléréséhez
- **slapd** – a szolgáltatást nyújtó démon
- slurpd - szerverek közötti replikáció kiszolgálója
- Kliens-szerver modellen alapul
- Egy vagy több LDAP szerveren tárolt adatból épül fel az LDAP fa
- Az LDAP kliens egy LDAP szerverhez csatlakozik, és felteszi a kérdéseit
- A szerver a válasszal reagál, vagy egy mutatóval, hol talál több információt a kliens

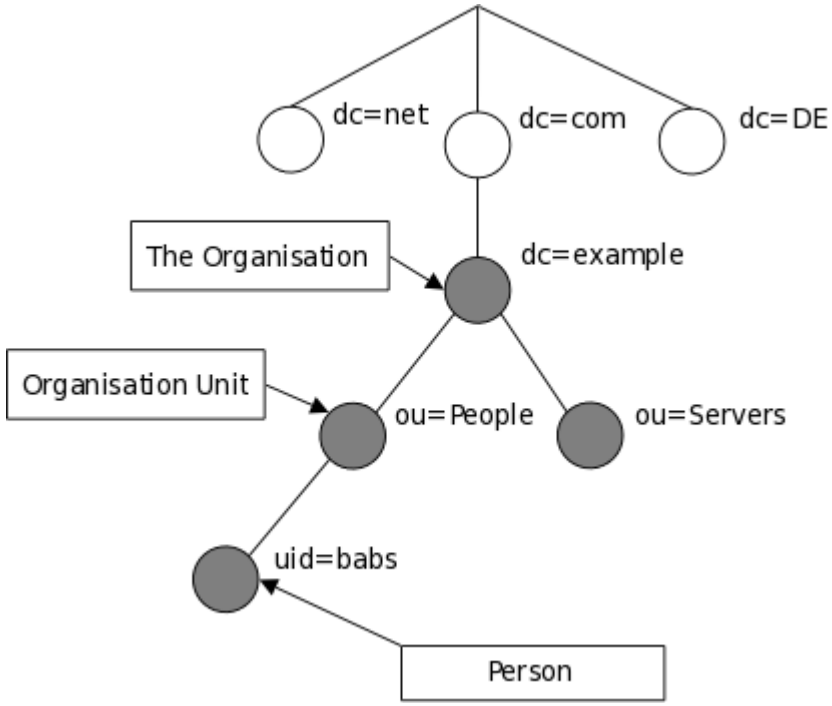
Adatbázisok

- Három különböző, szabadon választható háttér adatbázis használható:
  - **LDBM**, a nagy teljesítményű merevlemez alapú adatbázis
  - SHELL, az adatbázis interfész tetszőleges UNIX parancs vagy shell-script eléréséhez
  - PASSWORD, az egyszerű jelszó adatbázis

Az LDBM adatbázis

- 4 bájtos egyedi azonosítók minden adathoz
- Fő indexe az id2entry, ami a bejegyzések egyedi azonosítóit (entry's unique indentifier - EID) összerendeli saját szöveges ábrázolásával
- Importálás és exportálás LDIF formátumban (LDAP Data Interchange Format)
- A bejegyzéseket objektum orientált hiearchikus formában tárolja

Internet tartomány név alapú fastruktúra



- DIT: directory information tree
- Hivatkozás a bejegyzésre:RFC4514,
- DN: distinguished name: uid=babs,ou=People,dc=example,dc=com
- RDN: Relative Distinguished Name uid=babs

DC – Domain Component
CN – Common Name
OU – Organizational Unit

LDIF

```
dn: o=Nns, c=Hu
o: Nns
objectclass: organization

dn: cn=Halász Gábor, o=Nns, c=Hu
cn: Halász Gábor
sn: Halász
gn: Gábor
mail: halasz.g@nns.hu
objectclass: person
```

Felépítés

- dn - distinguished name (megkülönböztő név) - a bejegyzés nevéből áll, megtoldva a név elérési útjával vissza a címtár hiearchia csúcsáig
- alapvető objektum osztályok:
  - **Group** (csoport), független objektumok rendezetlen listája vagy objektumok csoportja
  - **Location** (elhelyezkedés), az országok nevei és leírásuk
  - **Organization** (szervezet)
  - **People** (személy)

Bejegyzések

- Egy bejegyzés (attribútum) több objektumosztályhoz is tartozhat
- cn: Halász Gábor (commonName)
- givenname: Gábor
- surname: Halász
- mail: halasz.g@nns.hu
- A person objektumosztályban
  - cn és sn attribútumok **szükségesek**
  - telephoneNumber, seeAlso és userpassword jellemzők **engedélyezettek**, de nem szükségesek

Attribútum szintaxis

- Minden attribútumnak meghatározott szintaxis definíciója van
- bin - binary (bináris)
- ces - case exact string (betűnagyságnak meg kell egyeznie az összehasonlítás során)
- cis - case ignore string (betűnagyságnak nem kell egyeznie az összehasonlítás során)
- tel - telephone number string (olyan, mint a cis, de a <-> kihagyásával)

Az LDAP szerver konfigurálása

- hely: /usr/local/etc/openldap vagy /etc/openldap
- állomány: slapd.conf
- (slapd.oc.conf és slapd.at.conf)

slapd.conf

```
# megjegyzés - ezek az egész adatbázisra érv.
<globális konfigurációs lehetőségek>
# első adatbázis
database <backend 1 type>     <backend 1 beáll.>
# második adatbázis
database <backend 2 type>     <backend 2 beáll.>
# további adatbázis definíciók
```

LDAP szerver indítása

- önállóan (LDBM esetén ez ajánlott)
  $(ETCDIR)/slapd [<opciók>]*

- inetd-vel indítva

Accessing LDAP

- Add, modify, and delete entries with `ldapadd`, `ldapmodify`, and `ldapdelete`
- Search the LDAP database with `ldapsearch`
  - Bind as some DN or anonymously

```
ldapsearch -D "cn=Directory Manager" -h ldaphost -b
  "dc=cims,dc=nyu,dc=edu" "uidNumber=9876" gecos
```

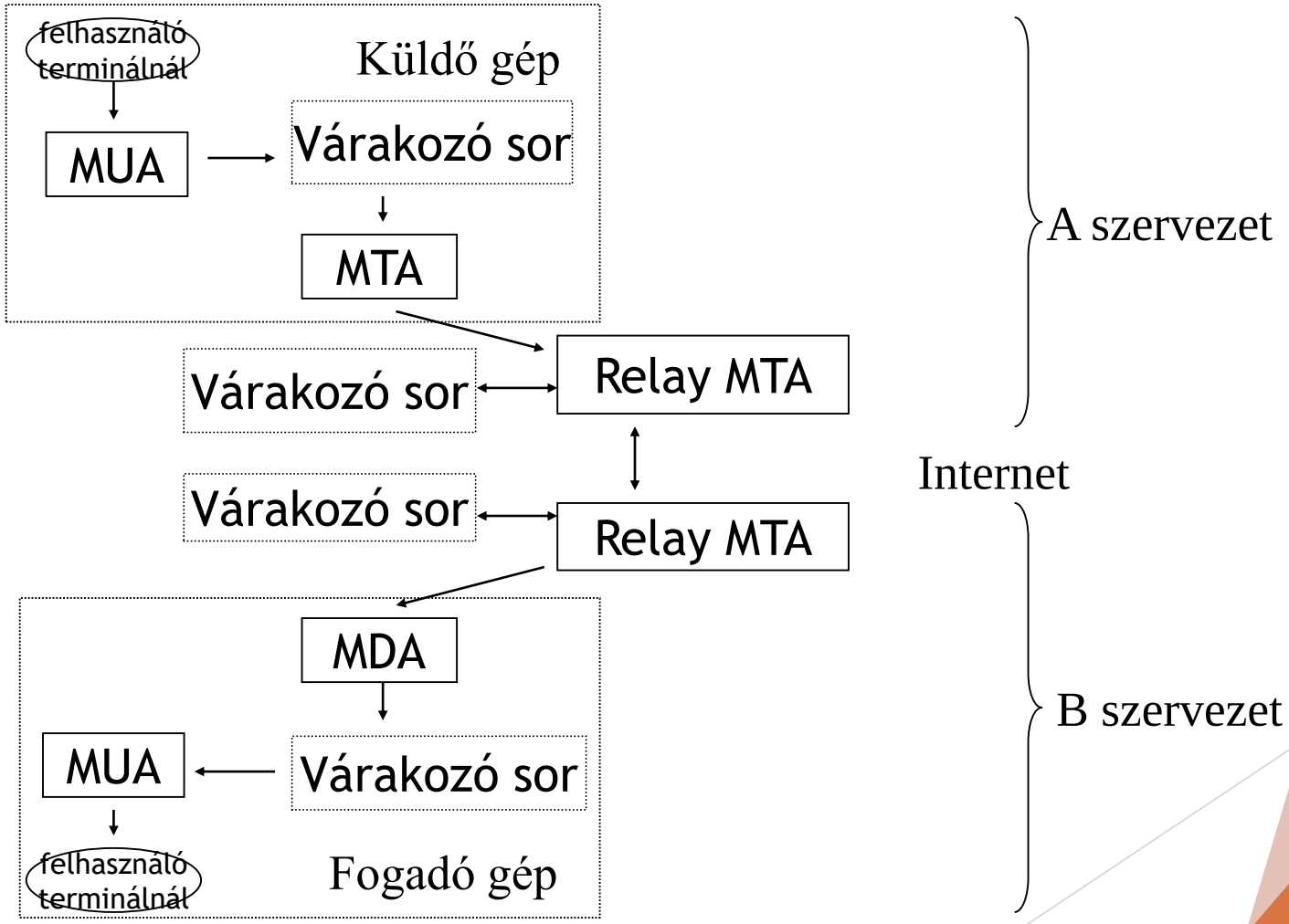
- Access to information is controlled by an access control list, e.g. password hashes are not available through anonymous bind

Levelezés

Fontos protokollok

- SMTP - Simple Mail Transfer Protocol
- POP3 - Post Office Protocol
- IMAP - Internet Message Access Protocol
- HTTP

SMTP - hagyományosan



SMTP

- **Application-level protocol on TCP**
- **Mail system is performed by two agents.**
  - MTA(mail transfer agent): Postfix, Exim, Sendmail, Qmail, Courier
  - MUA (mail user agent): Thunderbird, Outlook, Eudora, Evolution
- **Communication between two MTAs uses NVT (Network Virtual Terminal) 7 bit ASCII.**
  - Commands are sent by the client to the server.

- Typical message format
  - One part generated by sender's MTA.
  - The other part generated by sender's user agent.
- E-mail is composed of three pieces.
  - Envelope : used by the MTAs for delivery.
  - Header : used by the user agents.
  - Body : the content of the message.

※ *Note : each line transferred using the DATA command must be less than 1000 bytes*

generated by sender's MTA

generated by sender's user agent

```
Received: by client.ac.kr. (4.1/SMI-4.1)
          id AA004303; Mon, 20, Aug 98 12:30:34 MST
Message-Id: <98082033245.AA004303@client.ac.kr>
From: sender@client.ac.kr (Sender)
Date: Mon, 20, Aug 1998 12:30:33 -0070
Reply-To: receiver@server.ac.kr
X-Phone: +1 343 342 2345
X-Mailer: Mail User's shell(7.5.4 10/23/98)
To: receiver@server.ac.kr
Subject: Just testing mail.

hello, this is a testing mail.
bye..
```

Szerverek lekérdezése

```
hallgato@hallgato-desktop:~$ host -a -v -t mx google.com
Trying "google.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53257
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 13, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      MX

;; ANSWER SECTION:
google.com.             900     IN      MX      100 google.com.s9a1.psmtp.com.
google.com.             900     IN      MX      200 google.com.s9a2.psmtp.com.
google.com.             900     IN      MX      300 google.com.s9b1.psmtp.com.
google.com.             900     IN      MX      400 google.com.s9b2.psmtp.com.
```

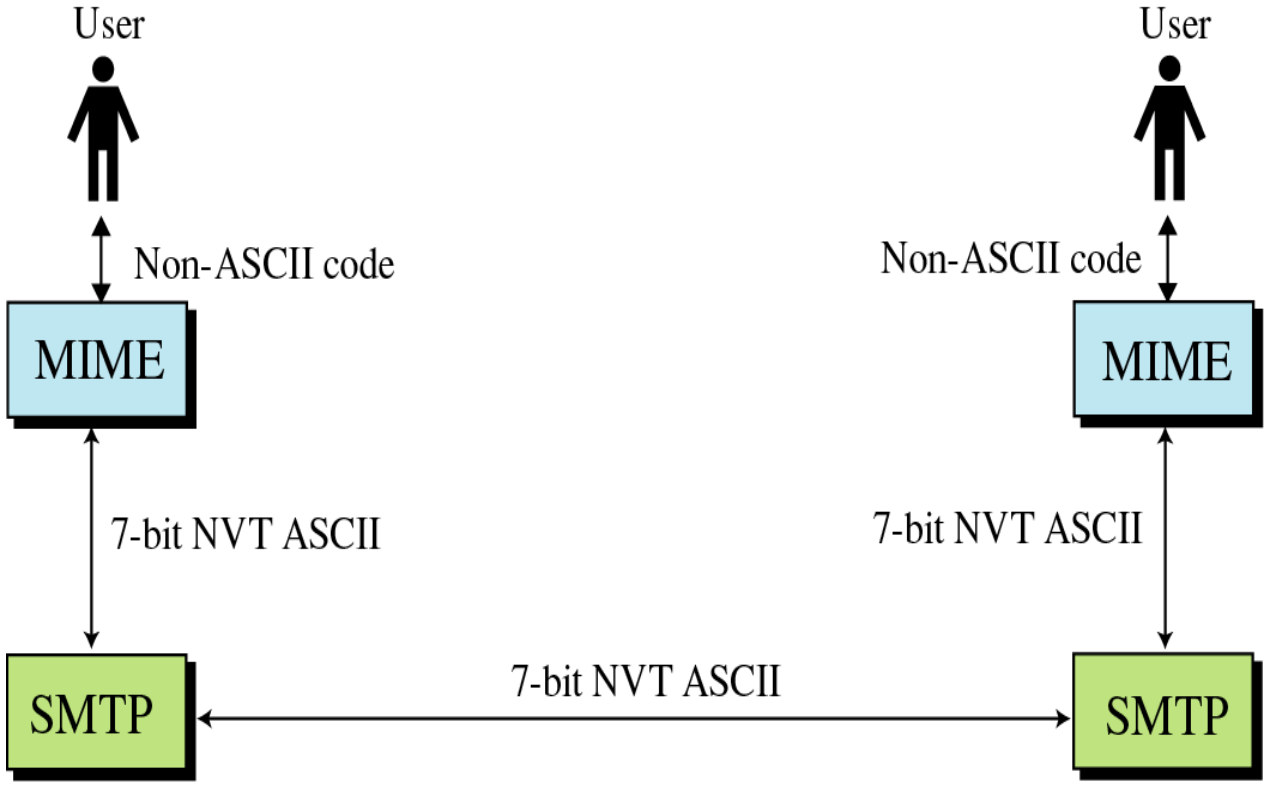
Limitations in SMTP

- Only uses NVT 7 bit ASCII format
  - How to represent other data types?

- No authentication mechanisms
- Messages are sent un-encrypted
- Susceptible to misuse (Spamming, faking sender address)

Solution: SMTP extensions

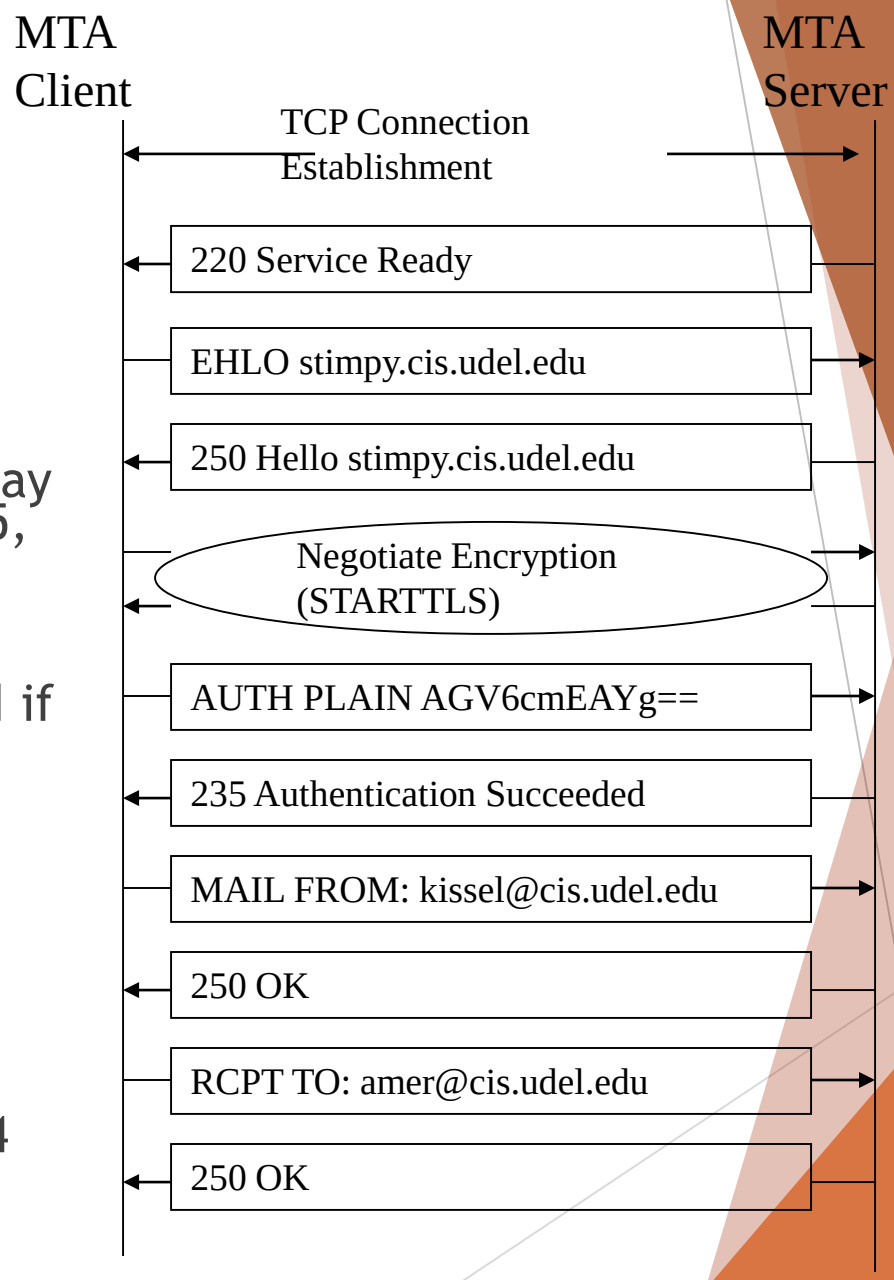
- MIME – Multipurpose Internet Mail Extensions
  - Transforms non-ASCII data to NVT (Network Virtual Terminal) ASCII data
    - Text
    - Application
    - Image
    - Audio
    - Video



RFC 1425, 1426, 1521

SMTP AUTH

- Allows the server to provide features only to known users and limit others.
- Various authentication methods may be used (PLAIN, LOGIN, CRAM-MD5, etc.)
- Encryption is highly recommended if not enforced by MTA.
- Ex. AUTH PLAIN
  - Simple
  - Usage: AUTH PLAIN <id>\0<user>\0<password>
  - Authentication string is Base64 encoded



RFC 1869, 2554, 2595

Email can be faked…

HELO stimpy.eecis.udel.edu

MAIL FROM: cis-dept@cis.udel.edu

RCPT TO: amer@cis.udel.edu

DATA

From: Department Chair

To: Dr. Paul Amer

Subject: CISC856

Dr. Amer,

By department decree all students in your CISC856 TCP/IP class are hereby to be given automatic A's.

Thank you,

Department Chair

.

QUIT

Solutions

- Email signatures (PGP)
- Sender Policy Framework (SPF)

MTAs and Mail Access Protocols

- The MTA delivers email to the user's mailbox
- Can be complex with numerous delivery methods, routers, and ACLs
- Exim, Postfix, Sendmail

- The Mail Access Protocols are used by the users to retrieve the email from the mailbox
  - POP3
  - IMAP4

Post Office Protocol v3

- Simple
- Allows the user to obtain a list of their Emails
- Users can retrieve their emails
- Users can either delete or keep the email on their system
- Minimizes server resources

Internet Mail Access Protocol v4

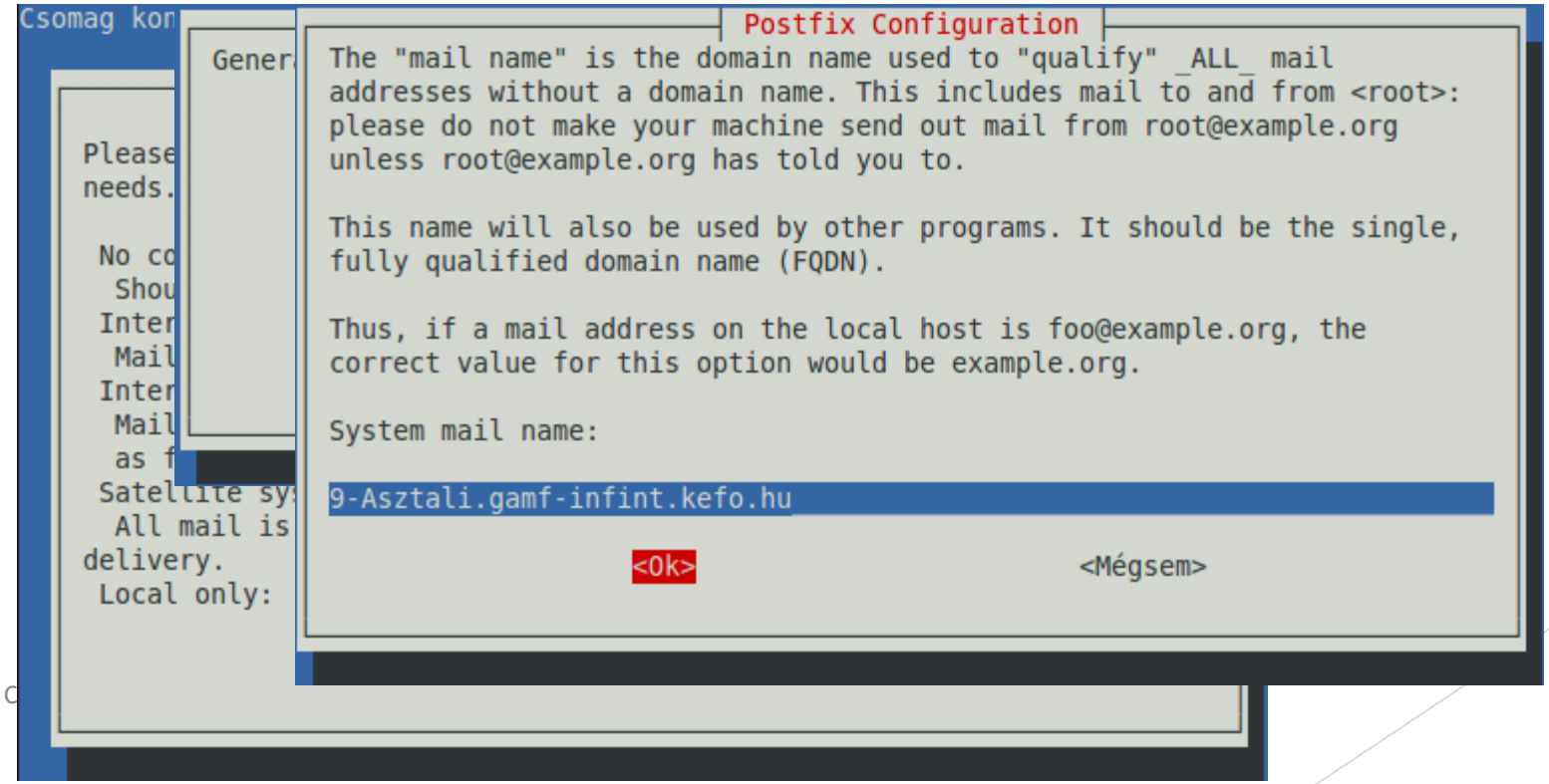
- Has more features than POP3
- User can check the email header before downloading
- Emails can be accessed from any location
- Can search the email for a specific string of characters before downloading
- User can download parts of an email
- User can create, delete, or rename mailboxes on a server

Levelező szerver

- Mail Transfer Agent – levelek fogadása és küldése (szerver)
  - **Postfix**
  - exim4
- Levélszűrés – spam és vírus felismerés
  - Amavis-new
  - Spamassassin
  - Clamav
- Mail Delivery Agent
  - **Dovecot**
  - Cyrus
  - Courier
- Levelezési lista
  - Mailman

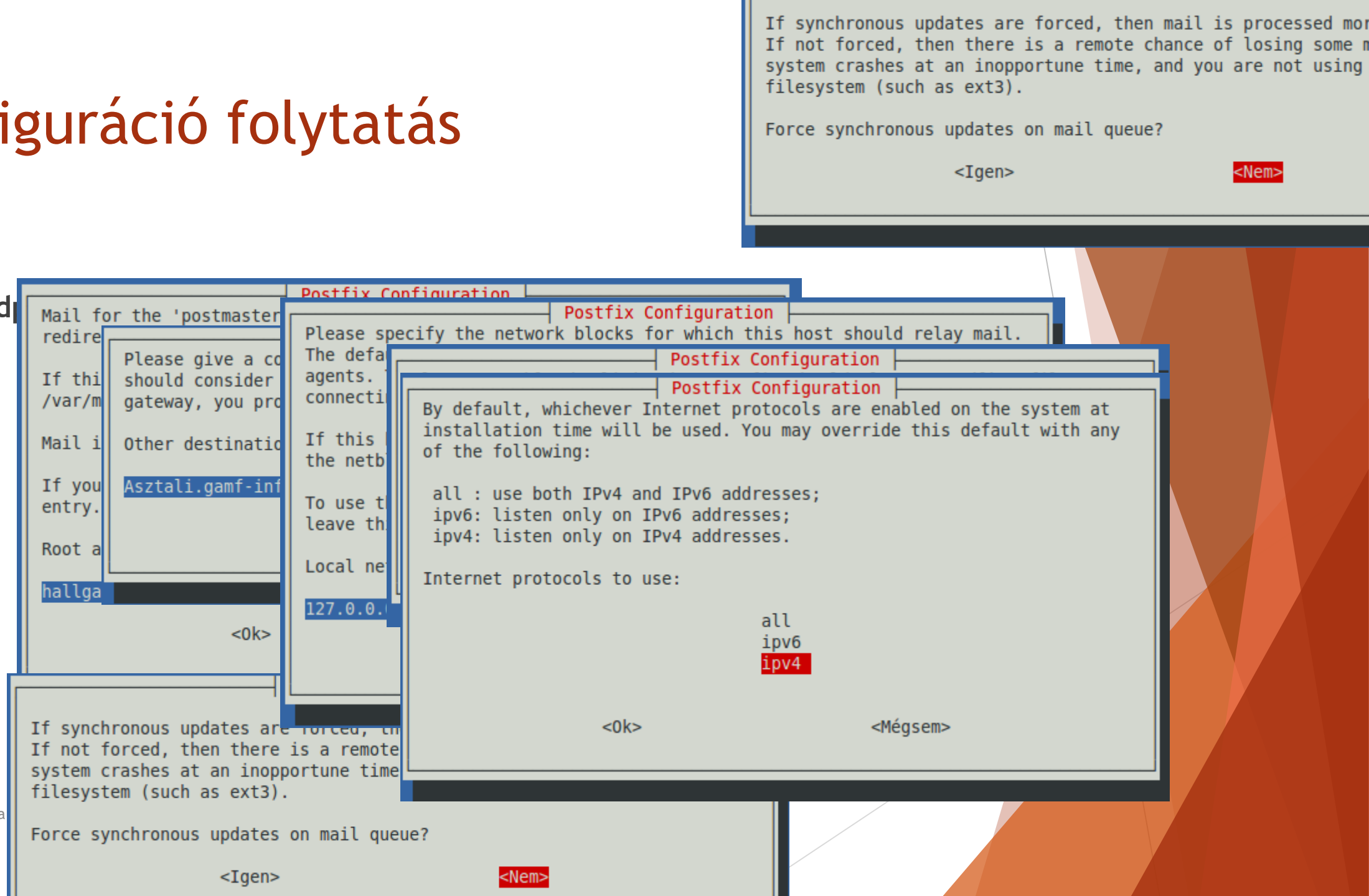
Postfix

- MTA – levelek küldése és fogadása
- sudo apt-get install postfix



Konfiguráció folytatás

- sudo dp



További beállítások

- Levelek tárolásásra szolgáló könyvtár megadása
- TLS-t alkalmazó SASL hitelesítési mechanizmus beállítása (SMTP-AUTH) – egy hitlesítésszolgáltató által kiadott vagy "önaláírású" tanúsítvány szükséges
- Lehetséges SASL megvalósítások: Dovecot SASL (postfix-dovecot csomag) és Cyrus SASL