Analysis of Current Authentication Deployment

and

Analysis of Alternative Schemes

Each System uses one or more of the various Authentication and Information Services:

User Systems	Authentication Service
Labs Academic Staff stations Safecom Internet Proxy	AD: Acad
WIFI UNIX TimeSharing Servers JTT Mail (not exchange) Moodle	LDAP
Admin Stations Exchange Internet Proxy (admin)	AD: Admin

- Presumably, any new authentication and information system for users would need to provide all these services.

- Alternatively, we could stop providing services like:
  - Moodle
  - Webmail
  - JTT
 - Gmail
  - Linux timesharing
  - Web proxy

"Acct" Account Creation Software maintains data consistency by updating all authentication services.

Mazak (Maztal) lets users create their account once they have paid required school fees. "Mazak" accesses "Acct" backend to create accounts.

Assuming non-elimination of services, a new scheme would provide current services:
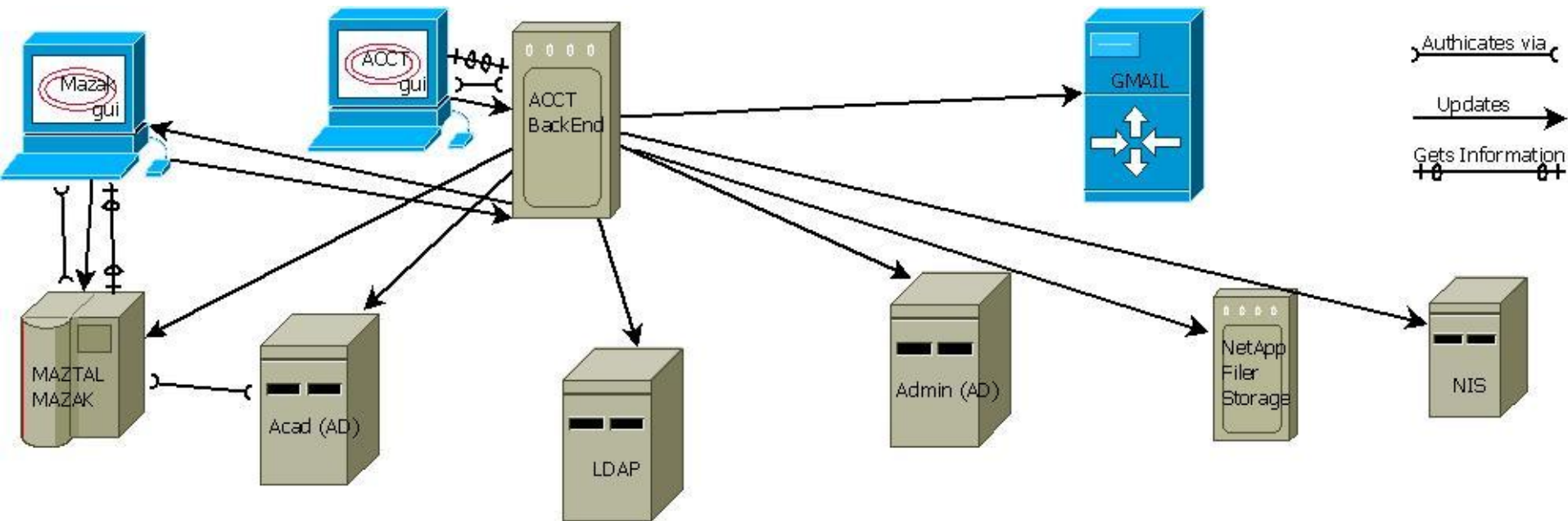
- The current system relies on a separate management system to maintain Data Consistency.

- This is provided by ACCT and its backend (command -line scripts).

- There are two alternative ways to organize these data bases.

# Alternative 1:   Microsoft Active Directory as Master
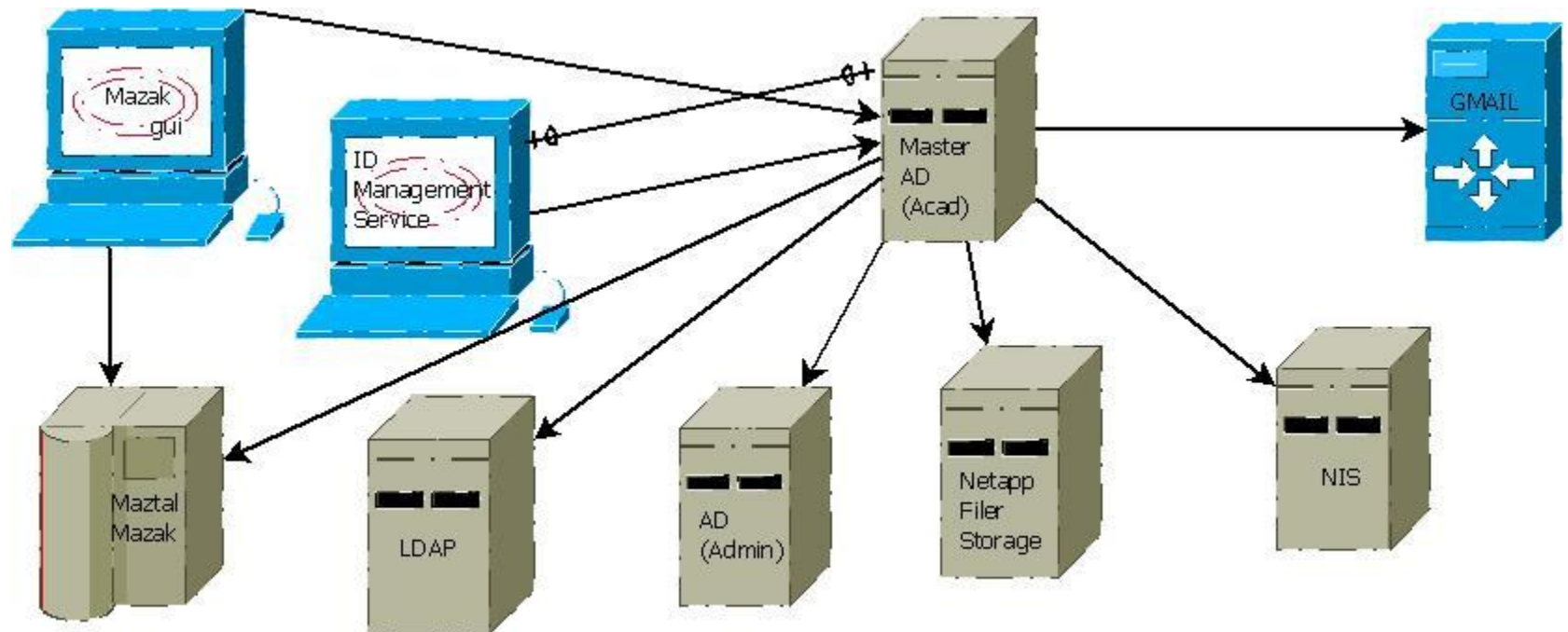
Pros:
1. Only need to update one system.
2. Other systems would be updated by AD
3. Other systems would continue providing current services

Cons:
1. AD must be made to update NIS, LDAP, Maztal, Quotas on NetApp
2. Still involves maintaining heterogeneous pool of Authentication
 and DB services.
3. Does not really simplify anything
4. Requires buying or making a new GUI for ID management and installing it

Alternative 2:   AD only Approach
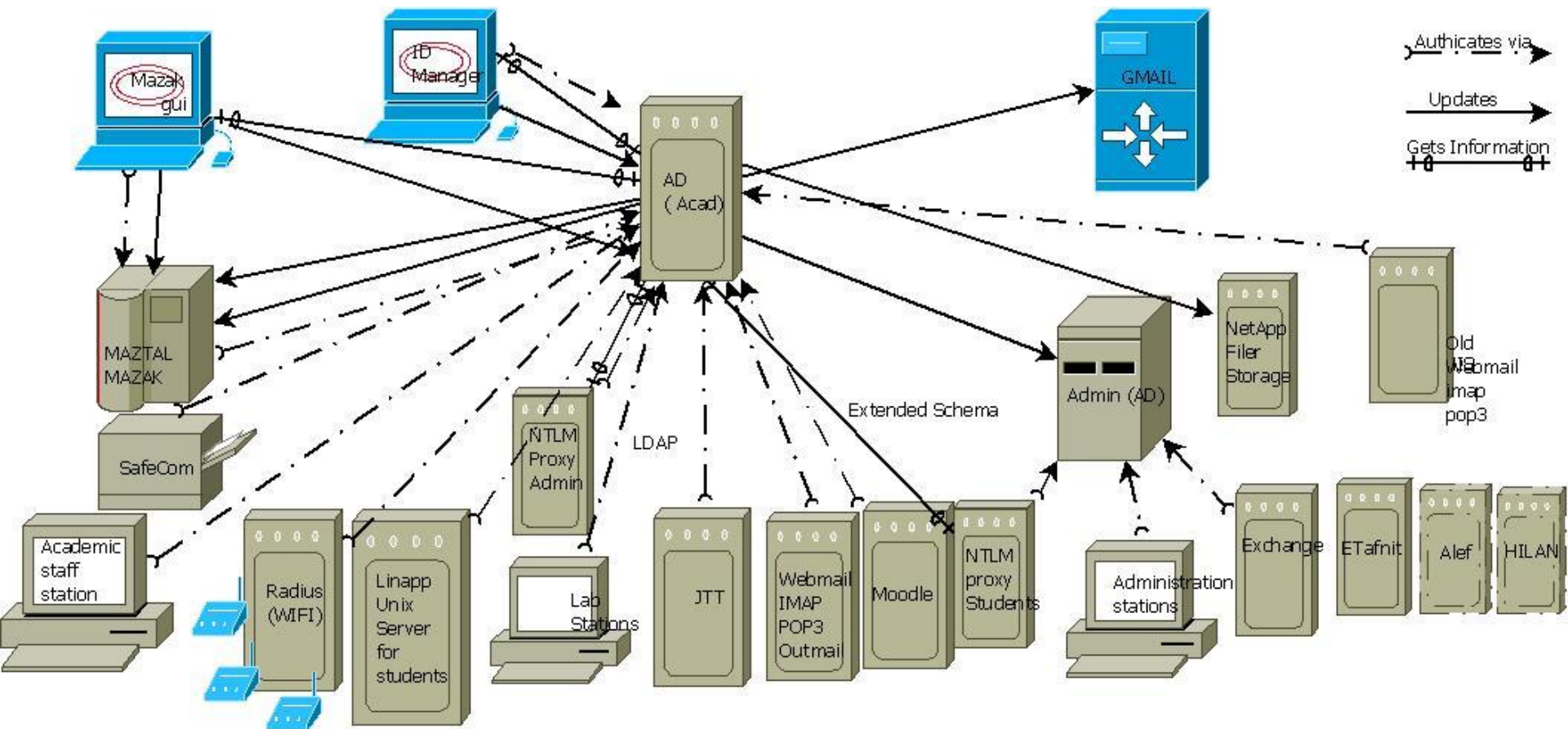
Pro:
1. ID management software for AD already exists
2. Sounds more straightforward

Con:
1. Requires migrating a lot of services to authenticate via AD, may not be possible

2. Requires changing the AD Schema , something which has been considered likely to cause problems.

3. Does not really achieve MS only, since various other systems will still exist and need to be updated.

4. Has all the problems of the first alternative, but for LDAP and NIS

5. Need to buy ID management software, or write it and implement it ($$)

"Mazak" and "Acct" could easily improved to :

• allow users to change their passwords

• generate replacements for forgotten passwords

Amiram and I were working on this just before he left.