Exchange Pilot as a new Messaging infrastructure at CERN

Alberto Pace, for the IT/IS group - April 2002

alberto.pace@cern.ch   http://cern.ch/alberto.pace

Electronic Mail at CERN

- **The current services have been designed in 1996 - 97**
- **Dedicated infrastructure, dedicated team.**
- **Mandated to offer an IMAP-based mail service, an LDAP-based email address database, Mailing lists handling and news feeds**
- **Very successful service:**
  - **Unanimously adopted site wide**
  - **Number of mailboxes in excess of 15'000**
  - **Very reliable**

Why a new infrastructure ?

- **New requirements have appeared**
  - **Personal / Shared Calendar with delegated authoring**
  - **Integration with PDAs, offline work and disconnected clients**
    - **With the possibility of merging back changes made on both sides (secretary scenario)**
  - **Web access to all services**
  - **Better security (SSL) and antivirus protection**
  - **Single logon, Voice Mail, Telephone integration, instant messaging, video conference, …**
- **CERN global manpower reduction**
  - **2700 -> 2000 staff members, more focus on LHC**
  - **Coverage during the extended Christmas shutdown**
  - **Directives to reduce costs**
  - **Personnel, Money, Industrial Services (P+M+I)**

Objectives

- **Cost reduction**
  - **Cheaper server hardware providing more resources**
  - **Leverage from existing experience and services**
    - **Same hardware used for Win, Web services and PC farms**
  - **Potentially save 50K+ per year**
- **Increased functionality**
  - **Addressing user community requirements**
- **Leverage on PC & W2K technology and existing skills**
  - **Reducing diversity, hence simplifying the operations**
  - **Use of existing procedures (e.g. installations, backup, interventions, alarm & monitoring, etc.)**
  - **Economy of scale with same team for Web / Mail / Windows**
  - **All external interfaces based on standard protocols for interoperability**

Infrastructure for the Pilot

- **8 Server PCs**
  - **4 Back-end (message store)**
  - **2 Front End (Routing, Web access, …)**
  - **2 spare**
- **Dimensioned to be "out" scalable by adding additional servers**
- **As the pilot has to investigate also behavior under heavy load, the pilot infrastructure is designed to be able host the full laboratory load**
- **In the final infrastructure, we believe that a final architecture with 12 servers (8 message stores) should be sufficient**
- **No licenses needed at this stage**
  - **Part of our MSDN / Premier Support Service agreement**

Addressing Requirement

- **Increased Security**
  - **In addition to normal IMAP and POP, enable SSL for client that supports it**
    - **Open ports imap(143), imaps(993), pop(110), pops(995)**
    - **In the long term consider to close ports imap(143) & pop(110)**
  - **Enable Authenticated SMTP service (versus the anonymous service today) with mail routing and relaying allowed**
  - **Enable secure Web Mail access over SSL for any browser (including legacy>= 4)**
    - **Open both http (80) and https (443) ports with port 80 being redirected to port 443**
  - **Install Antivirus software, scan message stores, Incoming and outgoing messages**
  - **Enable MAPI (secure and encrypted) in order to support native Exchange clients (Outlook)**
  - **Synchronize Mail accounts with Web/Win accounts. Single sign-on for Mail/Web/Win services**

Single Sign-on

- **Why single sign-on increases security ?**
  - The user is an insecure component of the security chain if he has nothing to protect
  - Proliferation of accounts and passwords results in users not protecting their credentials on services they seldom use
  - By coupling multiple services together, we enforce security, because here or there, every person has something to protect (eg: mail, data in home directory, …)
  - Current working group is considering (again) a proposal to synchronize AFS and Win/Mail/Web passwords

Addressing Requirement

- **Enable "Calendaring"**
  - **Native Exchange clients (Outlook) support with MAPI enabled**
  - **Personal calendar in every mailbox**
  - **Access to "shared" calendar**
  - **Allows authoring delegation (secretary scenario)**
  - **Allows publishing of Agenda/Calendars on the web**
  - **Basic calendar functionality accessible cross platform using the Web interface, Read/Write mode**
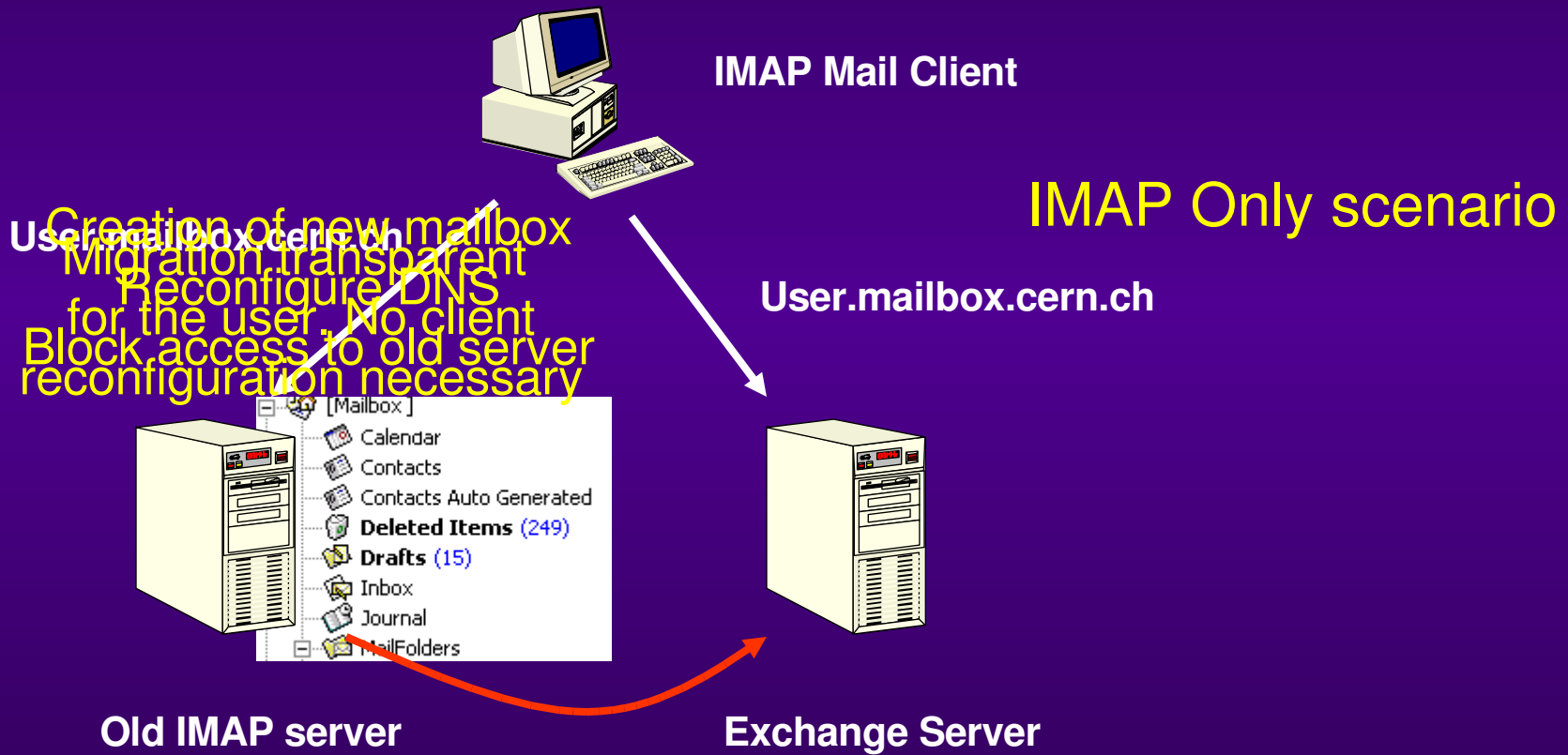 - **Complete shared calendaring possible through public folders**

Addressing Requirement

- **Access to news**
  - **News feeds directed into public folders**
  - **Access to newsgroup also using the Web interface**
- **Explore new possibilities**
  - **Generalized use of e-groups (NICE2000 group manager). Same e-group objects can be referenced to set permissions but also as mailing list**
  - **Public folders for collaboration, document store, web site, …**
  - **Fax, SMS, telephony gateways**
  - **Web integration**
  - **Voice mail**

Migration strategies - Phase 1

IMAP Mail Client

IMAP Only scenario

User.mailbox.cern.ch

Creation of new mailbox
Migration transparent
for the user. No client
reconfiguration necessary

User.mailbox.cern.ch
Reconfigure DNS
Block access to old server

```
[Mailbox]
  Calendar
  Contacts
  Contacts Auto Generated
  Deleted Items (249)
  Drafts (15)
  Inbox
  Journal
  MailFolders
```

Old IMAP server

Exchange Server

**Asynchronous overnight
migration of the message store**

Migration strategies – Phase 2

IMAP Mail Client

User wants extra features

Client is reconfigured
From IMAP to MAPI

Usermailbexcern.ch

Server name should
change to mmm.cern.ch

- [Mailbox]
  - Calendar
  - Contacts
  - Contacts Auto Generated
  - **Deleted Items** (249)
  - **Drafts** (15)
  - Inbox
  - Journal
  - MailFolders
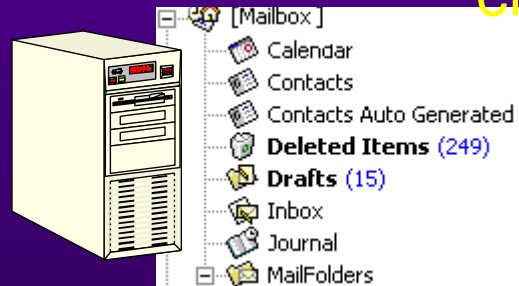
Exchange Server

Mail Client Support Models
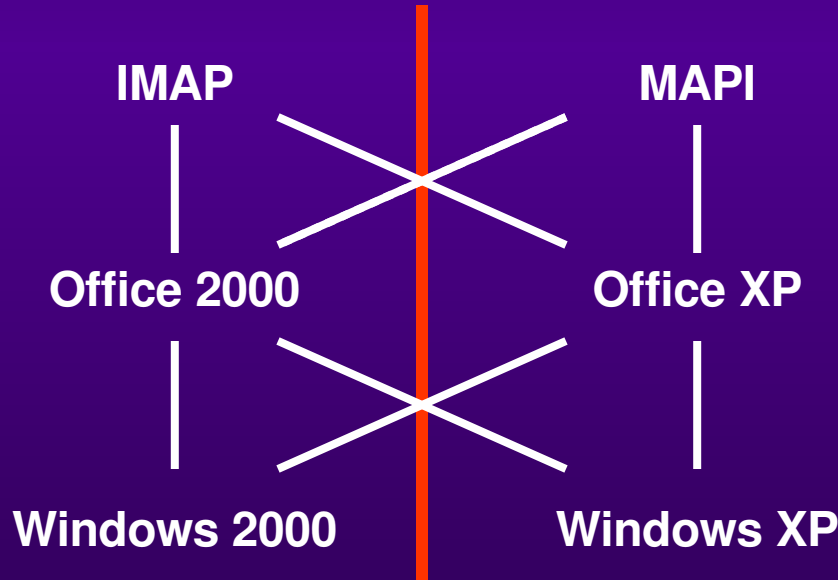
2 Models ?

8 Models ?
(just for windows mail clients)

3 Models …

IMAP

MAPI

Office 2000

Office XP

Windows 2000

Windows XP

Current Plan

- **Prototype (4Q01-1Q02)**
  - Explore possibilities, alternative architectures, initial how-to's, sources of worries, prepare questions
  - Understand initial costs
  - Collect initial experience in order to propose a Pilot
- **Pilot (2Q02-3Q02)**
  - **Ensure User needs are satisfied**
  - **Identify potential problems, limitations**
  - **Identify cost & extra work needed**
  - **Identify risks and long term costs**
  - **Limited (or targeted) at a well-know user community**
  - **Identify potential migration issues**
  - **Prepare training and documentation needs**
- *Deployment (3Q02-1Q03) -* subject to successful pilot and management approval
  - *Open to everybody*
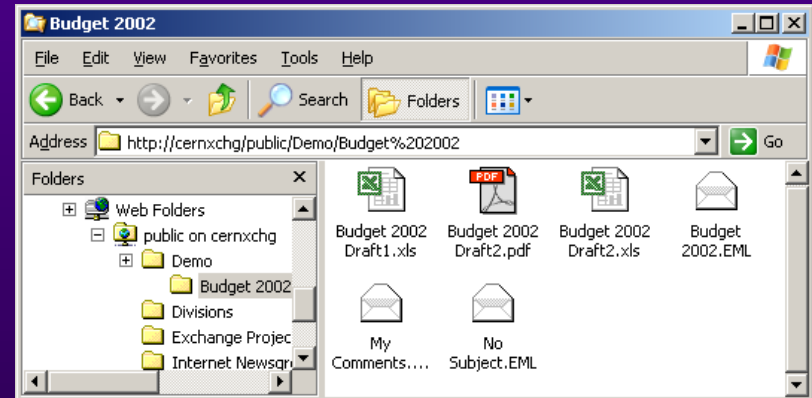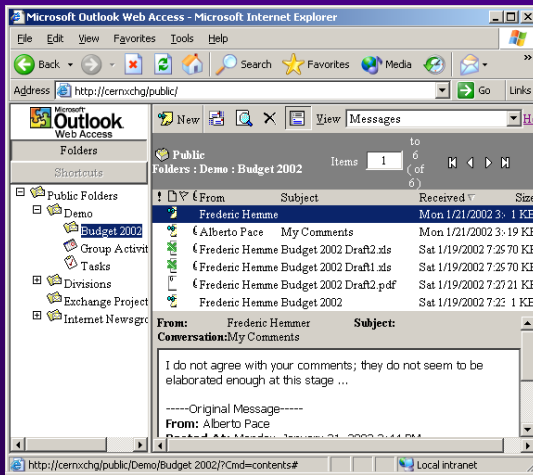 - *Migration plans understood and applied*

Outlook
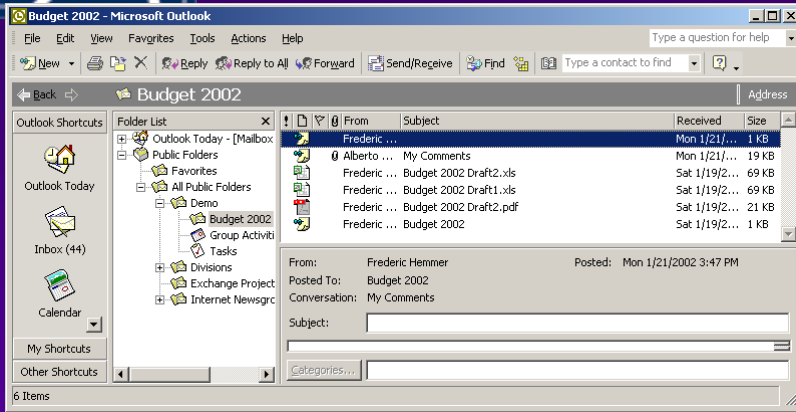
Netscape 4.75 on lxplus
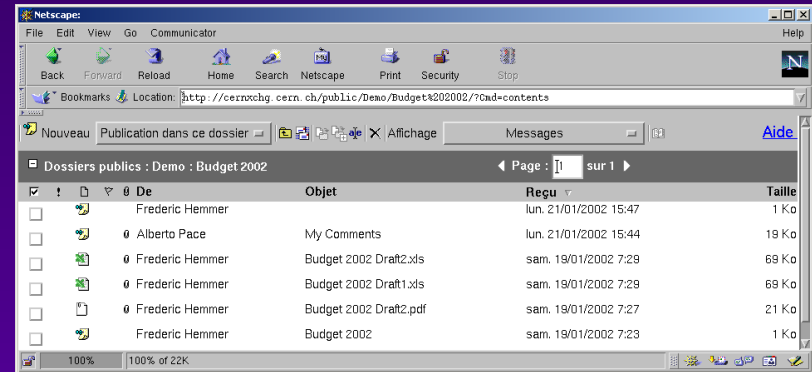
Internet Explorer

Web folder

Conclusion

- For the user
  - Exchange 2000 could give opportunity to long outstanding requests:
    - Mail, Calendar and more
    - Web access to most of the features
    - Does not rely on any particular client (browser >= 4)
  - and allowing group collaboration
    - e-groups and "groupware"
- For IT/IS
  - While taking into account the constant search for economy
    - Maintenance/Server replacement at least 30% cheaper (per year) assuming 13000 users
  - And address manpower issues
    - by consolidating on a platform that we have to support anyway
    - reducing diversity requires less specialization
    - mail expertise currently limited to two individuals could expand to 7-8 persons
  - as well as potential integration of other products/security features
- An opportunity for offering more services & coverage for a global reduced/constant cost

http://cern.ch/mail
http://cern.ch/web
http://cern.ch/win
http://cern.ch/it-div-is-techmeet