Report on Centralization of Infrastructure Computing

Prepared for the Information Technology Council

Desktop Systems Advisory Council Implementation Group (DIG)

January 15, 2004
Contents

1. Executive Summary

2. Detailed Findings and Recommendations
   a) Active Directory
   b) Anonymous File Transfer Protocol (FTP) Services
   c) Calendaring
   d) Central Authentication
   e) Directory Services
   f) Electronic Mail

3. Case Study Findings

4. Appendices
   Appendix A – Focus Group Attendees
   Appendix B – UCAR Directory Data Flow Diagram
Executive Summary

This report outlines the findings and recommendations of the Desktop Systems Advisory Committee (DSAC) Implementation Group (DIG) regarding the potential for centralization of computing services at UCAR, based on the Information Technology Council (ITC) directive of June 2003.

Background

In August 2001, the DSAC presented a strategic plan to the ITC for consideration. It included a number of recommendations for centralization that the ITC was not prepared to act upon. Accordingly, the ITC recommended establishing a working group of senior managers and senior systems administrators to investigate further the issues and impacts of centralization.

Assessments of possible services to consider, including the equipment and personnel costs currently associated with providing these services continued over the next 13 months. After divisional review, the DIG submitted a draft report of findings and recommendations to the ITC in June 2003. The ITC directed DIG to continue to look at centralization, but to limit its focus to a detailed analysis of six computer services with potential for some degree of centralization at UCAR rather than on organizational issues.

The ITC Directive

The following services were selected for preliminary analysis, as they all have some component that has already been partially centralized:

- Active Directory
- Anonymous File Transfer Protocol (FTP)
- Calendaring
- Central Authentication
- Directory Services
- Electronic Mail

The ITC defined the following goals for centralization:

- Improve quality of service to user community
- Meet common needs across the organization
- Improve security
- Achieve cost-effectiveness and economies of scale
- Maintain technical diversity among staff
The ITC requested that an analysis of selected services include the following:

- Current state, including deficiencies
- Proposed improvements
- Description of proposed centralized service
- Pros and cons of centralization (including divisional impacts, where possible)
- Recommended time frame for implementation
- Costs (to the extent possible)

Finally, the ITC also recommended that the DIG research and analyze case studies on centralization efforts that could be relevant to UCAR.

**Observations**

During the process of reviewing centralization options, focus group input and case study responses, the following high level observations emerged that were common to all services:

- An evolutionary approach to centralized services is favorable as opposed to a revolutionary approach. This is recognized in our recommendations, which incrementally expand current centralized services from within divisions hosting them.

- All of the services evaluated are closely interrelated and need to be tightly coordinated and integrated: the issue of governance or oversight must be addressed. One deficiency of the current state is that various committees, many with overlapping memberships, serve in an advisory role to providers of centralized services. This will be increasingly ineffective as services are further centralized.

- All centralized services should have Service Level Agreements (SLAs).

- Overcoming resistance to change and achieving buy-in requires strong direction and support from management to ensure the success of centralization efforts. Continuous collaboration between end users and systems administrators is required to ensure that needs are being fulfilled.

- Centralized service providers should base decisions to implement high-availability systems on required service levels and risk assessments.

- The FTE cost for services requiring 24 x 7 support can be reduced by sharing high level technical staff and utilizing existing support infrastructure, such as SCD’s computer operations staff, wherever possible.

- Some centralized services are not cost-effective without critical mass. There is a risk of underutilization and continued duplication of costs when participation in a centralized service is made optional.

- Centralizing services provides opportunities to manage and improve security effectively.
As part of the analysis process, the DIG hosted a separate focus group session for each service between October 29 and December 4, 2003. Technical and non-technical representatives from across the organization attended the focus sessions. (See Appendix A for a list of focus group attendees).

The DIG defined a uniform service analysis template, which independent DIG sub-teams compiled independently for each of the six services. The template includes the following components: strengths, weaknesses, opportunities, challenges, risks, and recommendations for improvements. The strengths and weaknesses sections refer to the current situation; opportunities, challenges, and risks apply to potential further centralization. The detailed findings and recommendations are available in Section 2 of this report.

DIG identified specific funding requirements wherever there was sufficient information to do so. However, in some cases funding requirements can only be specified after task forces complete the recommended detailed analyses. For each case where the DIG recommends further study, the DIG is prepared to recommend task force members to ITC upon their approval to proceed with the recommendation.

**Recommendations**

<table>
<thead>
<tr>
<th>Active Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Active Directory (AD) is a specific directory service that is a central component of a network of Microsoft Windows platforms. AD provides a means to manage the identities and relationships that make up the network.</td>
</tr>
</tbody>
</table>

**AD is a database run on Windows servers that provides systems administrators with the capability to administer accounts and machines centrally. The AD also provides directory services, with which end users authenticate themselves on PC's and locate networked resources such as printers, shared folders, and other information in the directory.**

<table>
<thead>
<tr>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ITC should consider mandating participation in the CIT domain for all divisions and users inside the UCAR security perimeter wherever technically feasible.</td>
</tr>
<tr>
<td>Recommended Timeframe: 6 Months</td>
</tr>
</tbody>
</table>

| 2. Strengthen the CIT by defining an explicit Service Level Agreement and identifying appropriate backup resources and provisions for 24x7 coverage. |
| Recommended Timeframe: 10 Months |

| 3. The Active Directory Task Force (ADTF), which governs the policies of the CIT domain, should continue to sponsor and coordinate education and forums for information exchange among systems administrators and end users for cross-divisional collaboration. |
| Recommended Timeframe: 10 Months |

| 4. The ADTF should fill existing vacancies by adding one to two staff members. |
| Recommended Timeframe: Ongoing |
FTP (File Transfer Protocol) is a service that allows an individual to transfer files between computers on the Internet. FTP is a simple network protocol, but the term is also used to refer to this type of file sharing service. An FTP client program initiates a connection to a remote computer running FTP server software. After the connection is established, the client can list, send and/or receive files. To connect to an FTP server, a client requires a username/password combination as set by the server. Most public FTP archives follow a naming convention that accepts a username of “anonymous“ with the password being the email address of the user of the client.

**Anonymous FTP**

**Recommendations**

1. SCD should investigate implementation of a central FTP proxy server solution. If technically feasible, it should be implemented and the FTP protocol should be blocked at the security perimeter.
   
   Recommended Timeframe: 1 year

2. If a central FTP proxy server solution proves to be not feasible, continue with the status quo.
   
   Recommended Timeframe: 1 year

3. Create a service level agreement for centralized FTP services upon implementation.
   
   Recommended Timeframe: 1 year

---

**Calendaring**

Calendaring is defined as computing infrastructure that supports the electronic scheduling of people and resources (meeting rooms, A/V equipment, etc.). This infrastructure consists of communications protocols, client side software, web/server-side software and the server hardware. The client-side calendaring software provides views of resource scheduling and allows meeting organizers to quickly see free blocks of time that are common to all resources requested for an event. The tools also identify any scheduling conflicts and notify appropriate parties when they or resources they are responsible for are requested.

**Recommendations**

1. Create a research and development task force to pursue the following:
   - LINUX client support from MeetingMaker (MM)
   - Kerberos Authentication
   - New features from MM and developments in the calendaring industry
   
   Recommended Timeframe: 9 Months

2. Approve a term appointment of 1 FTE for one year for a collaborative effort between F&A and SCD to integrate MM and Room Reservation System (RRS) using the recently purchased application programming interface (API).
   
   Recommended Timeframe: 1 year

3. Release the MM API to other UCAR developers.
   
   Recommended Timeframe: 18-24 months

4. Division directors and group heads and should promote the use of Meeting Maker for cross-divisional and group-wide meetings.
   
   Recommended Timeframe: 6 months
## Central Authentication

Central authentication is a service that provides trusted electronic confirmation for identity verification. Modes of operation include acceptance of verifiable information in the form of user provided credentials (passwords, tokens, biometrics, etc.) used to generate a timely authoritative response granting or denying access. Commonly, these transactions occur over a network via a client/server connection.

Potential applications include a single sign-on capability where an individual is granted access to a wide array of resources, usually for a predefined period of time, following a single authentication.

### Recommendations

1. The ITC should support and endorse the central authentication project currently under way in Security Administration (ok?) and assure that appropriate resources are available to complete the effort in a timely manner.

   Recommended Timeframe: TBD

2. CSAC should ensure divisional input is acquired and evaluated in conjunction with the Kerberos project. Additionally, CSAC should develop corporate policies for items such as password complexity and retention.

   Recommended Timeframe: TBD

## Directory Services

Directory services are a structured repository of information on people and resources within an organization, facilitating management and communication. Within the UCAR centralized directory service context the focus is on an authoritative source for information about people. A directory service of this type would include basic information such as, name, location, and e-mail address. Additional desirable information includes the person’s affiliation and classification. (e.g., visitor, employee, university user, etc.) Finally, coupled with authentication it is possible in a directory service to also store relational information such as references to authorization levels or roles. All of this information is of importance for both human and software agents that can make use of this infrastructure.

### Recommendations

1. Develop a unified policy to manage privacy and security issues.

   Recommended Timeframe: 6-9 months


   Recommended Timeframe: Test beds in place; work concurrent to Recommendation #1

3. Based on the recommendations of the UCAR Directory Information Study (UDIS) task force, create a centralized, authoritative source for directory information that is robust, highly accessible and that supports divisional autonomy.

   Recommended Timeframe: 1-2 years

4. Initiate a collaborative effort between F&A and SCD to develop and implement the centralized directory services, using a representative cross-section of potential users to define and review requirements.

   Recommended Timeframe: 3-6 months

5. Create a service level agreement for centralized directory services upon implementation.

   Recommended Timeframe: 1 year
## Electronic Mail

A world-wide system of electronic communication in which an individual can compose a message containing ASCII text and/or binary attachments under specified conditions on a client system, which can then be transmitted over networks to one or more recipients. Operations include sending, storing, processing, and receiving information through a series of client and server systems, which process messages utilizing accepted formats, protocols, and software that adhere to accepted standards. A message is composed with the appropriate software on a client system, which then relays it on to a server system, that in turn relays it to a server at the final destination, where the message is stored for later retrieval by a client system on the remote end.

## Recommendations

1. **Appoint a task force to assess the risks associated with centralized inbound and outbound mail services and recommend high availability solutions as appropriate.**

   Recommended Timeframe: 4-6 months

2. **Charge the Computer Security Advisory Council (CSAC) to evaluate the impacts of additional security features that could be provided with a mandated centralized outbound mail delivery system and to submit the appropriate recommendations to ITC.**

   Recommended Timeframe: 4-6 months

3. **Create a Service Level Agreement for current centralized electronic mail services.**

   Recommended Timeframe: 4-6 months

4. **Consult with Legal to consider creating a UCAR policy regarding electronic mail archives.**

   Recommended Timeframe: 1-2 months

5. **Form a task force to design and implement a centralized mailbox solution to be deployed in a phased approach.**

   Recommended Timeframe: Initial system online, 1 year
   Division migration to centralized service: + 6 months
Case Study Summary

At the ITC's request to research and analyze centralization efforts at other relevant institutions, the DIG distributed a survey to the following institutions, of which five (*) responded.

- University of Illinois - Urbana-Champaign *
- University of Colorado - Boulder
- National Renewable Energy Laboratory *
- NOAA/Forecast Systems Lab *
- Los Alamos National Laboratory *
- Argonne National Laboratory *
- Ball Aerospace Corporation

The survey covered questions relating to the size and physical structure of the organization, the original goal and final outcome of the centralization effort, the process used and duration of effort, and the hurdles, impacts, and retrospective thoughts. While the results were somewhat varied, several common themes emerged:

- Corporate mandates and network security often played a key role in the decision to centralize services.

- The top reasons to centralize were cost savings and consistency of services while the top reasons against it were the challenge to meet diverse needs of end users and to maintain a high level of customer service.

- The length of time it took to implement centralization from start to finish was measured in years, not months.

- Political obstacles (the impact of which was often underestimated) appeared when centralization was proposed for services that more directly impacted user support.

- In most cases, there were cost savings associated with the centralization.

- The centralized services were, in general, "commodity services" while some de-centralization did co-exist.
Definition

The Active Directory (AD) is a specific directory service that is a central component of a network of Microsoft Windows platforms. AD provides a means to manage the identities and relationships that make up the network.

AD is a database run on Windows servers that provides systems administrators with the capability to administer accounts and machines centrally. The AD also provides directory services, with which end users authenticate themselves on PCs and locate networked resources such as printers, shared folders, and other information in the directory.

Current Service

Background

AD is a technology implemented and managed within Finance and Administration (F&A). High-level policies and design decisions for AD are the responsibility of the Active Directory Task Force (ADTF), a working group of the Desktop Systems Advisory Committee (DSAC). The ADTF implemented a UCAR-wide AD domain, referred to as the “CIT Domain” (CIT), which creates hierarchically distributed groupings of Windows resources for all participating divisions. Management of the CIT is distributed. F&A supports and maintains the top-level domain for UCAR, based on direction provided by the ADTF. Divisional personnel manage and have authority over their respective divisional resources known as organizational units (OUs).

Although participation in the CIT domain is opt-in, a majority of divisions participate in the CIT and are fully migrated. SCD initially opted out of participation in the CIT and implemented a separate AD structure, but SCD and F&A are collaborating to bring SCD into the AD by addressing issues such as 24x7 support. UNIDATA is outside the security perimeter and therefore cannot participate.

<table>
<thead>
<tr>
<th>Divisions Participating in the CIT by Status</th>
<th>ACU, ASP, ATD, CGD, COSMIC, DPC, F&amp;A, MMM, RAP, VSP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opted in/Fully migrated</td>
<td>GLOBE, JOSS</td>
</tr>
<tr>
<td>Opted in/Partially migrated</td>
<td>SCD, HAO</td>
</tr>
<tr>
<td>Opted Out</td>
<td>COMET</td>
</tr>
</tbody>
</table>

Few if any of UCAR’s divisions have universal membership in CIT. Some PC’s cannot be joined for technical reasons; some are outside of administrative control for arbitrary reasons; some are owned by other institutions and are guests on our network.
**Physical Infrastructure**

To provide full redundancy and high availability, F&A hosts the CIT on three domain controllers, which are physically distributed across each of UCAR’s three main campuses: Mesa Lab, Foothills Lab, and Center Green. The multiple domain controllers provide redundancy in case of server or partial network failure. All three domain controllers are synchronized automatically and functional at all times; fail-over is automatic.

**Related Services**

F&A provides two additional services in conjunction with the CIT:

- **Software Update Services (SUS)** is a central server for automating application of Microsoft operating system patches. Group policy in AD facilitates patching. Participating divisions test patches for two weeks before deployment.

- **Symantec Antivirus Server (SAV)** is a central server for automating distribution of anti-virus definition files, ensuring that clients receive new files within 24 hours of release. Divisions that do not wish to maintain SAV servers may point their clients directly to it.

Technologies behind AD are used to differing degrees. For example, ATD uses Group Policy Objects to install software and ACD authenticates against the AD Kerberos Server. While not entirely dependent on AD, some divisions utilize SUS to keep vulnerable PCs patched with critical updates.

**Support Resources And Funding**

F&A provides all personnel and equipment required to operate the top-level of the CIT domain. F&A dedicates an average of .25 FTE per year to CIT administration and up to an additional .5 FTE per year for CIT projects. The FTE dedicated for divisional OU administration varies and divisions also provide resources to test domain upgrades. The project to upgrade AD to Windows Server 2003 will require .5 FTE from F&A and testers from each participating division for approximately 7 months.

Equipment for the CIT includes three domain controllers and two update servers, which cost approximately $5000 per server and are replaced every three to four years. After the domain controllers are upgraded in 2004, F&A will use the existing servers to create a dedicated test environment.

Each client computer accessing the domain requires a client access license (CAL), which costs approximately $5.00; UCAR is currently licensed for 1,650 CALs.
Strengths

1. **Widespread participation in the CIT across UCAR/UOP/NCAR supports inter-divisional and inter-entity file sharing and collaboration.**

   The CIT provides a means to share files across divisional and entity boundaries, reducing the need to send email attachments or the intervention of system administrators to create unique file-sharing privileges or solutions. It also facilitates cross-divisional appointments and staff reassignments.

2. **The current AD implementation streamlines software support in the UCAR Windows environment, is reliable, and provides redundancy.**

   AD is available to any group in the organization whose system administrators can manage an OU. Distributed administration provides OU administrators the measure of control they need to be responsive to staff needs. The AD and related services can be used to provide centralized and automated software installation and critical security updates for Windows operating systems. The AD is relatively easy to use for systems administrators and users.

3. **The AD contributes to improved security for Windows platforms.**

4. **The current ADTF governance model works well.**

   The ADTF manages issues and policies associated with the AD and gains buy-in from participating divisions before implementation. Divisions are notified of proposed changes and provided adequate mechanisms for response and input.

Weaknesses

1. **Top-level administration expertise is heavily concentrated in one person.**

   Responsibility for CIT administration lies within F&A IT’s Operations group. While several staff members have the authority and ability to administer top-level domain privileges, specific expertise and certification is limited to one staff member. In the event of a serious issue, such as the need to restore an entire OU, responsiveness could be limited.

2. **Not all divisions and programs participate. Without full divisional participation, the advantages of file sharing are diminished.**

   Not having all divisions as CIT members means that extraordinary measures must be taken to provide access to CIT resources. For example, SCD implemented a CITRIX server solution to provide access to CIT resources, which may not be the easiest solution for the end-user to understand and use.

3. **There is no explicit Service Level Agreement (SLA) or provision for 24 X 7 coverage.**

   While AD has a great deal of fault tolerance built into it, there is not an identified plan for support for those groups that have 24x7 operational requirements. While F&A generally has staff on-call, it is difficult to support an explicit SLA for 24x7 coverage.
4. There is limited training for features of AD.
   Many UCAR users are not fully aware of how to use the CIT’s file sharing capabilities (the “U drive”) and other services. There is no formal education and/or training process.

**Opportunities**

1. If used by all divisions within UCAR, the AD can:
   - Enhance file sharing and collaboration between divisions and computers including UNIX Samba-served shares.
   - Streamline staff changes such as a staff member moving to another division, shared appointments, or a divisional merger or split in the organization.
   - Provide a more manageable security structure for our Windows resources in terms of corporate deployment of service packs, administration tools, deployment tools, and anti-virus tools. The Kerberos-based password system offered by AD may be a tie-in for Unix and Windows users to use common authentication.

2. Increased collaboration and sharing of common practices among divisions and programs.

**Challenges**

1. Administration of the CIT domain requires coordination and collaboration among divisions and programs.
   a. While AD schema changes are not recommended, if necessary, they must be coordinated to support all divisions.
   b. Currently, there are inconsistent group policies for each OU, making it more challenging to leverage the AD for joint appointments and shared divisional appointments. The AD is not supported equally on all systems.

2. Mobile computers and interoperability issues are challenging to manage.
   All divisions reported that they are dealing with some technical challenges, such as visitor laptops and legacy operating systems. Integration with other operating systems (Mac, Unix, Linux) and the constant shift of desktop systems complicate this challenge. Maintaining interoperability with other platforms and non-domain members and users is also a challenge.

3. Competing corporate cultures and ownership issues.
Risks

1. Single Point of Failure
With the implementation of a single, top-level Windows domain, it is possible that a domain problem could affect the entire organization, rather than a single division or program.

2. Security
Since the AD is a Windows-specific solution, there is a risk of vulnerability to viruses which target the AD and an increased dependency on a single vendor.

Recommendations

1. The ITC should consider mandating participation in the CIT domain for all divisions and users inside the UCAR security perimeter, whenever technically feasible. Exceptions would have to be approved by the ITC.

   The ADTF’s goal is to deploy an AD that will support a standard level of Windows service for the organization at large. Two years of planning, technical development, and exceptional cooperation among the divisions have gone into the UCAR-wide AD implementation.

   Recognizing that the success of a UCAR-wide AD depends on the participation of all divisions in our organization, the ITC expressed strong support for the AD in May 2002. This support was based not only on AD’s ability to meet the ADTF’s goal, but also on CSAC’s endorsement of AD as a means of controlling the increasing problem with viruses and worms by facilitating Windows software updates.

2. Strengthen the CIT by identifying an explicit Service Level Agreement (SLA) and the appropriate backup resources and provisions for 24X7 coverage.

   We also recommend provision of 24x7 support through a policy statement that provides avenues by which after-hours problems might be remedied. Related to 24x7 support, we recommend that additional personnel be trained and prepared to handle top-level domain administration as a backup to the existing top-level administrator in F&A.

3. The ADTF should continue to sponsor and coordinate education and forums for information exchange among systems administrators and end users for cross divisional collaboration.

4. ADTF should add one to two members to fill existing vacancies.
Definition

FTP, or File Transfer Protocol, is a client/server service that allows an individual to transfer files between computers on the Internet. FTP is a simple network protocol, but the term is also used to refer to this type of file sharing service. An FTP client program initiates a connection to a remote computer running FTP server software. After the connection is established, the client can list, send and/or receive files. To connect to an FTP server, a client requires a username/password combination as set by the server. Most public FTP archives follow a naming convention that accepts a username of “anonymous” with the password being the email address of the user of the client.

Current Service

Currently within UCAR most divisions and programs provide their own local anonymous FTP service. SCD maintains such a service as well and allows non-SCD users to make use of their server directly or through a proxy service. There are a few groups making use of this service from SCD.

The most common hardware platforms used for FTP by groups are Sun systems running Solaris and Intel systems running Linux. In order to accommodate setting ports for passive FTP, required by the security perimeter for semi-exposed hosts, the open-source “wuftpd” and “vsftp” servers are generally used.

Apart from disk space and network bandwidth, the system demands of FTP are small. The service is usually hosted on inexpensive systems or on servers that are already performing other tasks, so the computer costs are low, excluding storage. All groups represented at the focus group meeting reported that the amount of time spent configuring, maintaining, and supporting their anonymous FTP servers was minimal.

Many divisions and programs use their anonymous FTP service to share data with outside organizations for scientific/engineering collaboration efforts, and in many cases have large disk space requirements. This sharing is accomplished by either uploading data to or downloading data from the UCAR/UOP/NCAR anonymous FTP servers by the outside groups. The uploading capability requires a writable area on the server. Also required are “restricted” or “guest” ftp accounts, which require entering a username and password for access, but confine the user to a subset of the system once logged in. UCAR security policy prevents valid individual usernames for this purpose, since FTP passwords are not encrypted when transmitted over the Internet. The consensus from the focus group meeting is that this functionality needs to be maintained if anonymous FTP services are centralized.

Note that writable anonymous FTP has security considerations. If writable directories are visible to the public, history shows that unscrupulous groups will use them to share and distribute files, hijacking the server’s disk space and bandwidth; these files are usually of an illicit nature, such as digital forms of copyrighted texts or software. Writable directories must therefore be hidden on servers.

Additionally, many of the reporting groups share their anonymous FTP disk space via NFS to other UNIX hosts or via Samba to Microsoft Windows hosts. This can either be inbound or outbound to the server, but is implemented as a mechanism to get data to the anonymous FTP
server. This functionality would also need to be maintained if anonymous FTP services are centralized.

**Strengths**

1. Flexibility: the anonymous FTP services as they stand now are easily configured and modified by the divisional staff to suit any special needs of local projects, and changes can be implemented on the divisional priority schedule.

2. Autonomy: Control over the servers and their configuration is maintained at the division and program level, as well as governing policies such as scrub time and data and files that are allowed to be shared.

3. Low Cost: In many cases, the FTP servers at UCAR/UOP/NCAR are shared resources with other software or services. This service does not require a large amount of system resources or FTE time to maintain.

4. Scalability: With individual group control over the hardware, it is a simple matter to add or remove disk space allocated to the anonymous FTP service.

**Weaknesses**

1. Limit of 32 ports for passive FTP: In the current Internet environment, the majority of FTP users require connection via "passive FTP", which requires the FTP server to accept data connections from the client; a set of 32 ports have been opened for such connections, which limits servers to 32 simultaneous connections.

2. Currently, some servers may not have enough disk space available to meet their needs, and have limited ability to expand this resource.

3. This service is implemented in many divisions and programs at UCAR/NCAR, so it appears as a duplication of effort across divisions.

4. Finding certain types of data may be confusing for outside users who do not know which group may be responsible for the data they are seeking.

5. Having multiple upload areas increases the security risk to UCAR/NCAR, and there may be legal issues involving distribution of some types of data.

**Opportunities**

1. High Availability: 24/7 maintenance, better performance, redundant, robust hardware.

2. Software updated in a timely manner, less of a security risk.

3. Distributed (shared) management among the divisions and programs.
4. Consistent disk structure and naming conventions, may reduce data overlap between groups.

5. Integration with the Community Data Portal.

6. Less administration to be done by the groups themselves.

Challenges

1. Making log files available from a central server for usage tracking could be problematic. Log files for each group may need to be separated.

2. Administration of a centralized server could be complicated due to conflicting needs of the various groups making use of the service. This includes policies such as disk space quotas, backup policies, account management, and file retention times.

3. If NFS mounting of files on the central server is not supported, then some groups may need to modify procedures (including automated procedures) for managing files. This could be a significant impact.

4. Groups with special needs such as a direct connection to the SCD MSS would need to be accommodated.

Risks

1. Confusion among the community about where to go for their favorite data.

2. Maintaining an adequate response time to user needs: problems and changes.

3. Complexity for lightweight users to get/put data may be too high.

4. As with any centralized service, concern over single point of failure.

5. Adequate disk space allocated to groups, otherwise the central service will not be used.

Recommendations

1. The majority of centralization benefits can be realized, while preserving the benefits of distribution, by implementing an FTP proxy mechanism. This would allow FTP transactions to be forwarded by a single, centrally-managed server to the individual group servers that already exist, without requiring those servers to be exposed to the Internet for possible attack. SCD should investigate implementation of a central FTP proxy server solution. If this mechanism is feasible, it should be implemented and the FTP protocol should be blocked at the security perimeter.

2. If an ftp proxy mechanism turns out to be infeasible, the status quo of distributed divisional FTP servers should be maintained.

3. If the central proxy is implemented, a service level agreement for a centralized FTP should be developed.
DSAC Implementation Group
2c. Service Analysis: Calendaring

Definition

Calendaring is defined as computing infrastructure that supports the electronic scheduling of people and resources (meeting rooms, A/V equipment, etc.). This infrastructure consists of communications protocols, client side software, web/server-side software and the server hardware. The client-side calendaring software provides views of resource scheduling and allows meeting organizers to quickly see free blocks of time that are common to all resources requested for an event. The tools also identify any scheduling conflicts and notify appropriate parties when they or resources they are responsible for are requested.

Current Service

Following the DSAC (Desktop Systems Advisory Council) recommendation, the decision was made in July 1999 to adopt Meeting Maker as the meeting scheduling product for UCAR/UOP/NCAR. This followed a 12-month period of testing and evaluation which involved 22 divisional and department representatives and an all day hands on comparison of three products. Based on cross platform requirements at the time (client support for UNIX (Solaris), Windows and Macintosh platforms), the feature list, a web solution and the user interface, among other criteria, Meeting Maker was selected. It was implemented on Finance and Administration servers in December 1999 and has been housed, upgraded and supported by F&A since then.

It is important to note that there is no single mandated calendaring solution at UCAR. Though Meeting Maker is available to anyone who wishes to use it, a wide variety of usage within groups or departments exists presently. Some groups use it widely or their administrative staff uses it exclusively and successfully, other groups have traditionally allowed their users great autonomy in selecting a solution and do not feel ready to mandate one. Finally, there are some groups that feel the Meeting Maker solution does not work for them for a variety of reasons and are not likely to change unless the product or solution changes.

Current Software

Meeting Maker server and client software, v. 7.3 is currently licensed for the entire organization. Meeting Maker Web Services API, for testing in 2004-5, Meeting Maker Intellisync module for CE, blackberry Personal Digital Assistants (PDAs).

Room Reservation System, developed and supported by SCD to accommodate the specific requirements for conferences and conference services. Functionality has been added to meet additional needs over the past seven years.

Small pockets of individuals or groups use a variety of commercially available scheduling software.
Current Hardware

- Meeting Maker: Sun Solaris 8 server ($9000)
- Partial use of Apache server for mm web application ($3000)

Software Maintenance Costs:

<table>
<thead>
<tr>
<th>Description</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1400 Licenses</td>
<td>$9,650</td>
</tr>
<tr>
<td>Meeting Maker Web Services</td>
<td>10,000</td>
</tr>
<tr>
<td>Amortized Solaris server</td>
<td>3,000</td>
</tr>
<tr>
<td>Apportioned Web Server</td>
<td>1,000</td>
</tr>
<tr>
<td>Intellisync software licensing</td>
<td>500</td>
</tr>
</tbody>
</table>

Personnel Costs Organization Wide:

<table>
<thead>
<tr>
<th>Category</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT .5 FTE SAIL</td>
<td>$32,500</td>
</tr>
<tr>
<td>Divisional support</td>
<td>&lt;.03 FTE: 26,200</td>
</tr>
</tbody>
</table>

The Meeting Maker server has performed well with minimal unscheduled down time (both times related to the network) and only two scheduled weekend upgrades during the past four years. There are currently 1142 registered maker accounts, some of which not actively used. Typical numbers of users logged into the Meeting Maker vary throughout the day, peaking at approx 375-400. There are also small pockets of users who employ other calendaring solutions. There is no consistency among these.

Strengths

1. The Meeting Maker solution was cited as intuitive and easy to use. It is available to anyone in the organization who wishes to use it. Having a solution for the organization means that individual groups don’t have to research and implement their own calendaring solution.

2. Groups that use it report that it is efficient and saves time and energy.

3. You can schedule across the organization and the software is scalable.

4. It supports PDAs and has a web version. Other individual features were noted as strengths.

5. The three native clients for Solaris, Windows and Macintosh, including Mac OS X platforms work well.

6. Where groups have strongly encouraged its use, Meeting Maker has been effective. Not well known is Meeting Maker’s current limited but expanding support for the open standard protocol known as ICAL.
**Weaknesses**

1. The most frequent observations were detailed criticisms of the interface; for example, lack of multiple calendar views.

2. Also highly important is the lack of a native Linux client. Within the past two years, it is apparent that in the scientific divisions, the move is away from Solaris to Linux and Mac OS X. The Solaris base of users has shrunk considerably.

3. The major issues regarding the web client are that it is not full featured and robust.

4. Lack of integration with the Room Reservation System, privacy concerns and email notification are shortcomings.

5. If not used actively, it causes ambiguity among staff attempting to schedule.

**Opportunities**

1. Sharing information of solutions, for example, Linux clients accessing Meeting Maker via a Solaris window, could benefit the entire organization in the short run.

2. Communicating UCAR’s needs to the software vendor and their responsiveness could encourage us to expand its use. The tool now exists to integrate the room reservation system and Meeting Maker in some fashion.

3. If UCAR/UOP/NCAR had a research and development team for calendaring, we could investigate products that more fully support the open standard calendaring protocol iCAL. This would allow scheduling across organizations, beyond UCAR borders, and personal selection of client software.

**Challenges**

1. Widespread and active use of a calendaring product are important for a successful collaborative organization wide solution. Two things are problematic. Either users do not like the software or do not like having an electronic scheduler period. The latter can be an issue of control over one’s own time and how it is managed.

2. The most consistent observations from the focus session were that not everyone is using Meeting Maker and this causes problems.

**Risks**

1. Spending money at the organization level for a tool that is not universally used is wasteful.

2. On a personal level some individuals do not want to lose control over their time, since it can be allocated electronically.
Recommendations

1. Because of the work that the more technical groups do, Linux is and for the foreseeable future will be an important desktop platform. With this in mind viable solutions need to be investigated to support this important segment of the user base. UCAR/UOP/NCAR would benefit from a research and development team which could pursue a number of initiatives: contacting the vendor to press for Linux client support, pursue the issue of Kerberos authentication, and continue the dialogue on features and improvements and monitor developments in the calendaring industry.

2. DIG recommends the ITC approve a term appointment of 1 FTE for one year for a collaborative effort between F&A and SCD to pursue the integration of Meeting Maker and the Room Reservation System using the recently purchased API from Meeting Maker.

3. Release the MM API to other UCAR developers.

4. Finally, Division Directors and Group Heads should promote the use of Meeting Maker, minimally for cross-and group-wide meetings.
Definition

Central authentication is a service that provides trusted electronic confirmation for identity verification. Modes of operation include acceptance of verifiable information in the form of user provided credentials (passwords, tokens, biometrics, etc.) used to generate a timely authoritative response granting or denying access. Commonly, these transactions occur over a network via a client/server connection.

Potential applications include a single sign-on capability where an individual is granted access to a wide array of resources, usually for a predefined period of time, following a single authentication.

Current Service

Central authentication service is currently provided by SCD. Multiple central services make use of the current system including the Finance and Administration Applications Portal (Time Card, UCARFlex, Advance Notice, ...), UCAR web service, and GateKeeper access, among others. Use of the current central authentication system is primarily concentrated within SCD and F&A. Single sign-on capabilities are not currently available between the resources listed above. Many divisions currently use central authentication systems internal to the division based on industry standard protocols like YP/NIS, Kerberos, or even locally developed solutions.

Current System

TIS fwtk authsrv
RADIUS shim
Platform: Red Hat Linux on Intel architecture provided by SCD

New System:

Kerberos V, both MIT Kerberos and Heimdal Kerberos
TIS fwtk authsrv shim (to be developed)
RADIUS shim
Platforms: Debian Linux stable, OpenBSD, and FreeBSD on Intel architecture, purchased with security admin (indirect) funds

Current Costs:

Personnel: $25,000 (3 hours per week system maintenance, avg.)
Hardware: $4,800
Software: no charge
Maintenance contracts: none, hardware replacement handled with in-house spares
New Costs:

Personnel: $25,000 (3 hours per week system maintenance, avg.)
Hardware: $4,800
Software: $6,000 (shim development by in-house personnel)
Maintenance contracts: none, hardware replacement handled with in-house spares

Personnel notes: Time does not include user account addition and removal, which is delegated to division personnel.

Hardware notes: $1,200 per kerberos server, total of 3 systems at present already purchased. Replacement interval 3 years. Hardware spare: $1,200, still to be purchased.

Proposed Service

UCAR Security Administration has presented an implementation schedule for a new corporate-wide central authentication system based on Kerberos version 5. Development on a testbed system started in mid-November 2003 and is currently planned to extend through May 2004. On completion of the project, divisions can on an opt-in basis begin converting access control management over to the centralized system. Over the long term, as more and more resources utilize the central authentication system, the value of single sign-on will emerge. Divisional costs for managing disparate authentication systems will be reduced as well as costs for lost for forgotten passwords.

Strengths

1. Diversity and number of different authentication systems currently in use limit damage in the event of a compromise of a single user account or password

2. Simplicity and flexibility of a well known and well understood system for adding, removing, and updating local authentication databases (ease of maintenance).

Weaknesses

1. Difficulty for users in remembering multiple different passwords for different systems and confusion around which password is used.

2. Difficult division-wide/corporate-wide password management and lack of resources to address the problem

3. Potentially insecure because users have too many passwords and are more likely to choose easy passwords or write them down
Opportunities

1. Potential for single sign-on capability and central password management. In the event of a security emergency, any number of accounts could be locked-out very quickly to isolate and minimize damage.

2. Simplicity for users by reducing the number of passwords required

3. Increased security through better password policy management and use of more secure protocols

4. Leverages built-in password management support available in some operating systems and work already done by some divisions

Challenges

1. Legacy systems may be difficult/impossible to retrofit to central authentication

2. Mobile/laptop systems may have inconsistent or problematic authentication while off the network (on travel).

3. Questions and concerns about high availability, single point-of-failure, and operational issues in using a central system

4. Provision of timely technical support and user education for a central system

5. Compatibility with existing systems and applications like Meeting Maker, BiTech, RAS, and Web services and differing requirements of each

6. Compatibility with emerging technologies like grid computing

Risks

1. Ability of a central system to encompass most or all needs

2. Password policy causing users to be less secure with passwords or not resolving current problems

3. Ability to create a simple to use, secure, and robust system and the implications if it should be unavailable

4. Single sign-on is a more attractive security target and the consequences of a security compromise could be magnified
Recommendations

1. DIG recommends ITC support and endorse the Kerberos V project already in-progress and assure that appropriate resources are made available to complete the effort in a timely manner.

2. DIG recommends ITC should task CSAC with gathering divisional input on the project. Additionally, CSAC should develop corporate policies on items like password complexity and password retention.

3. DIG recommends provision of 24x7 support for existing and recommended services through a policy statement that provides avenues by which after-hours problems might be remedied. Related to 24x7 support, it is recommended that additional personnel be trained and prepared to respond to administration of these services as warranted.
DSAC Implementation Group
2e. Service Analysis: Directory Services

Definition

Directory services are a structured repository of information on people and resources within an organization, facilitating management and communication. Within the UCAR centralized directory service context the focus is on an authoritative source for information about people. A directory service of this type would include basic information such as, name, location, e-mail address. Additional desirable information includes the person’s affiliation and classification. (i.e. visitor, employee, university user, etc.) Finally, coupled with authentication it is possible in a directory service to also store relational information such as references to authorization levels or roles. All of this information is of importance for both human and software agents that can make use of this infrastructure.

Current Service

Currently within UCAR there is not an authoritative service for directory information as described above. A number of divisions maintain their own databases, spreadsheets, static lists or other methods for managing user information. Both F&A IT and SCD because of their specific missions have what approximates a directory service, but neither one is authoritative. F&A specifically has a richer set of information for all UCAR/NCAR employees. While SCD with its set of community users of computing resources and the gatekeeper accounts has both employee and university community member information.

The current methods grew up around a very specific and clear need from various groups to authenticate, authorize and manage resources. The system grew in an adhoc manner over a number of years in the absence of a well defined protocol. (See Appendix B – courtesy of UDIS) This diagram illustrates the complexity of the current process. Keep in mind that this diagram represents internal processes that result in the creation of files or population of LDAP servers that are then used by other divisions/programs. Many groups start with this base data then manipulate it further to meet the needs of their own environment.

Information about people is used throughout the organization in varied forms. Some of the most basic uses are the creation and maintenance of phone, e-mail, and web based lookup services for use by employee’s. Behind the scenes this information is coupled with authorization information for applications such as the gatekeeper, time card and travel applications. Additionally, charges for resources are tracked on a per user basis for remote access services (RAS), access to the mass storage system as well as computational resources. Other uses of people information include collection of contact information of researchers, collaborators or visitors that utilize data, software programs or other resources.

Current Software

High End: Oracle, Informix (Part of larger systems for F&A and SCD)

Medium End: MySQL, FileMaker Pro
Single User: MS Access, Excel, Flat Files

In general, many divisions and programs utilize flat files generated by SCD and use that information to populate systems that require people information.

Current Hardware

It is safe to say that because of the autonomy of the current system to quantify the hardware used is a monumental task. Nearly every division or program has at least one machine that serves people information, and in many cases, pockets of information that only exist on personal PC’s. The requirements are relatively modest, and are hosted on systems that have spare cycles.

Strengths

The strength of the existing system is the strong autonomy for each division or program. With this autonomy it is easy to adapt or modify the type, process, and amount of directory information they utilize. This allows for a high level of adaptability based on individual program needs.

Weaknesses

1. The current methods in place at UCAR for handling this kind of information are widely distributed across divisions and a high degree of replication, duplication of effort, and other inefficiencies exist. While there is no authoritative source for “people” information both F&A IT and SCD maintain two separate systems that are the nearest approximation. At least two kinds of inefficiencies are occurring during the current processes: those relating to people (e.g., two specific people inputting the same information manually) and those relating to organizational overlap of information (e.g., two entities maintaining the same information).

2. The existing system is a combination of many different databases, file outputs, and data flows. Some of the processing of information occurs at different frequencies (i.e. monthly, daily, twice daily, instantly). As a result data can be inconsistent, missing, or out of sync. This results in confusion and irritation and an overall lack of confidence in the quality of data.

Opportunities

1. An authoritative source would reduce the collection and entry of similar data across the organization.

2. As envisioned, a central directory service if carefully implemented can continue to allow the same level of autonomy as they enjoy now. As clients of the service, divisions or programs could utilize the authoritative source for their base information and extend it for division or program specific needs.
3. The architecture of the system must lend itself to flexible use so that divisions that need mission specific information can utilize the central service for authoritative information and augment appropriately from there. Concepts such as an agreed upon unique identifier are critical components of the design that must be well thought out.

Challenges

1. A central service is not without challenges. In order to be successful the user forum feedback clearly indicated it must not be harder to update information than it is now.

2. The directory service must have the appropriate level of policy and procedures defined so that the information in the directory is accurate enough to use widely across the organization. Examples of important policy issues are: Who can access what information? Who and how can information be updated? What information is suitable for a central repository? What policies need to be in place for privacy concerns for employee’s and external people who have some affiliation with UCAR. If the creation of policy is too cumbersome or too slow the system will not be used in favor of specific directories developed within the divisions or programs.

Risks

1. Failure to include the appropriate core set of data required by the various groups, could result in divisions/programs retaining their current data sources.

2. While autonomy is clearly valued the existing system offers significant exposure to UCAR because of varied levels of security and policy that protect information covered under privacy laws. A centralized system still has some risk of exposing private data if inappropriately designed but offers many key benefits. Primary among these benefits are manageability. It is a far more tractable problem to test and verify correct protection of information in a centralized system than twenty disparate systems scattered across the organization, not to mention easier to correct problems quickly if a problem does occur.

3. Increase SPAM if data available via the Internet

Recommendations

1. Develop a unified policy to manage privacy and security issues

2. A clear consensus has developed around utilizing LDAP as a protocol for serving directory information. This directory information would be back ended by one or more authoritative database sources.

3. Directory services have a broad benefit to the organization and should be implemented. As a centralized service, UCAR would for the first time have an authoritative source for people information; greatly enhancing accuracy. Particular attention should be paid to an implementation that is robust, highly available and maintains as much division autonomy as possible.
4. DIG recommends that an authoritative directory service should be created. SCD and F&A have a majority of the resources and mutual interests in this area it is recommended that a collaborative effort be started to implement a solution. To prevent the implementation from being only useful to these two groups it is also recommended that a representative cross section of the organization provide requirements and review the implementation design.

5. Create a service level agreement for centralized directory services upon implementation.
**Definition**

A world-wide system of electronic communication in which an individual can compose a message containing ASCII text and/or binary attachments under specified conditions on a client system, which can then be transmitted over networks to one or more recipients. Operations include sending, storing, processing, and receiving information through a series of client and server systems, which process messages utilizing accepted formats, protocols, and software that adhere to accepted standards. A message is composed with the appropriate software on a client system, which then relays it on to a server system, that in turn relays it to a server at the final destination, where the message is stored for later retrieval by a client system on the remote end.

**Current Service**

There are three distinct functions provided within an electronic mail system:

- inbound mail delivery
- outbound mail delivery
- user mailboxes.

It is not necessary, and may not be desirable, to have all of these functions provided by the same (group of) machines. Ancillary electronic mail services (static aliases, electronic mail lists, electronic mail access) may also be provided as part of a mail system, and again, may be distributed to other machines.

At UCAR/NCAR, inbound mail delivery is 100% centralized for groups within the security perimeter, and optional for those outside. This service is provided by a high-availability cluster supported by SCD known as the "mdir/mscan" cluster. These servers provide a store-and-forward system to process incoming electronic mail before routing it to user mailbox systems. Three additional actions are performed on all incoming mail: virus checking, SPAM blocking, and SPAM rating. Virus scanning is provided by proprietary software. SPAM blocking is performed by subscription to black hole list(s), and SPAM rating is performed by the open source software SPAMassasin. Interpretation of the SPAMassasin rating header is left to the destination user on the mailbox system. This is usually done via procmail or filters set up in the mail client software. The mdir/mscan systems were designed to be scalable and could accommodate a significant increase in traffic by adding additional nodes. The mdir/mscan cluster does not provide user mailboxes and as such does not have end-user logins.

Outbound mail delivery is currently available through the mdir/mscan system for divisions that choose to utilize it. Use of the central outbound mail service has not been enforced and very few groups use this service, choosing instead to use the division/program servers for outbound mail delivery.

The majority of divisions/programs currently support user mailboxes and outbound mail delivery services. In some cases, larger groups provide these services for smaller entities that do not have systems support staff (e.g. SCD provides support for the NCAR Director's Office).
Personnel support for the server systems is significant when new servers are being designed and installed. Once installed, however, the systems are generally quite stable.

An aggregate of 2 FTE effort is being duplicated across the organization for mail server support. The majority of ongoing system administration support is spent assisting users with issues related to use of client software, as attested to in the forum discussions. There are inconsistent policies and procedures organization wide regarding high-availability systems, electronic mail archives, and storage quotas. Implementation decisions are left to each division/program. Only two divisions (SCD, ACD) have implemented high-availability systems.

There is a wide variety of client software supported at the division/program level including multiple text-based clients, multiple GUI clients, and in some groups Web mail. All groups support the Internet Message Access Protocol (IMAP) protocol and to a lesser extent the Post Office Protocol (POP) protocol. Some divisions/programs provide IMAP/S and/or POP/S for secure electronic mail access for users external to the perimeter (home users, travel). Web mail is also provided by SCD for use organization wide, however, current performance issues have resulted in divisions/programs providing Web mail directly. Electronic mail distribution lists and static aliases are also being provided by most divisions/programs for internal use and by SCD for organizational use. Mailman is the preferred software for lists.

**Current Software**

Mail delivery: Postfix, sendmail, Netscape mail server

Mail Protocols: IMAP, POP, IMAP/S, POP/S

Mail Client Software: Netscape, Mozilla, MS Explorer, MS Outlook, Eudora, elm, pine, mutt, xemacs, CDE Mail, KDE Mail, Mail, mail, dtmail, MediaMail, ICemail, mulberry, twig, mh, Zmail, SquirrelMail, Web Mail, macmail, mutt, MS, Evolution

**Current Hardware**

The mdir/mscan cluster of systems for inbound and outbound mail are running on Intel architectures with the Linux operating system. The division/program servers are running on either Sun systems running the Solaris operating system or Intel systems running Linux.

**Current Costs**

Central Servers provided by SCD

- Personnel: $48,988.00
- Hardware: $43,000.00
- Maintenance: $2,500.00

Division/Program Servers (combined organizational wide):

- Personnel: $118,758.00
- Hardware: $96,910.00
- Maintenance: $7,460.00
Strengths

1. Divisions/programs at present have the flexibility to implement the protocols and client software that meets the needs of their staff. Direct end user support benefits staff.

2. System administration staff can stay current with emerging mail technologies.

3. There is no organizational single point of failure for mailbox servers. Should a divisional server fail it only affects one division.

4. The central mdir/mscan system is a high-availability cluster.

5. The single entry point for electronic mail provides an effective solution for virus and SPAM control.

Weaknesses

1. There are no standards, policies and/or procedures relating to electronic mail, most notably the archival of electronic mail messages.

2. Inconsistent service is being provided across the organization with numerous mail clients being supported.

3. Standard server configurations and software patch levels are not enforced. CSAC provides minimal requirements (different from standards) to address security issues. Functional requirements are left to the discretion of each division/program.

4. There is poor cross-divisional support for the many joint appointments and collaborative efforts. An extended power outage at the Mesa Lab would halt all inbound mail delivery.

Opportunities

1. With the increase in cross-divisional collaboration and joint appointments within the organization, a more productive environment would be provided if staff had the capability to access their electronic mail from any system within the organization.

2. New technology could be made available consistently to the organization, rather than deployment being dependent on the priorities and resources of individual groups.

3. With high availability systems at alternate locations, business continuity problems would be mitigated.

4. With centralized mail service, troubleshooting problems could potentially be easier to resolve.

5. The potential exists to provide services that would allow users to easily "customize" their mail filters, spam blocks, auto-forwarding, and auto-reply.

6. Provide SMTP service for external or remote users.
Challenges

1. As with any change in services, especially where consistent policies and procedures need to be implemented there will be some trade offs. With respect to electronic mail there are also legal issues that need to be addressed. These need to be developed so that the ability of staff to do their work is not compromised, but that a cost-effective and manageable system is available.

2. Responsiveness to staff could potentially be a problem. A solution would need to be developed to provide quick response to staff on routine issues at the division/program level with a mechanism for escalating the resolution to a higher level.

3. Development of comprehensive transition and education plans for system administration staff and end users of the service is critical.

4. Provide support for a command line interface.

Risks

1. If the new service does not provide the existing capabilities and adopt new technologies as appropriate in a reasonable timeframe, groups may revert back to providing their own service.

2. If the appropriate commitment to hardware and personnel to support the service is not made the service will have the potential to fail.

3. If the appropriate representation is not involved in policy development, buy-in will be difficult.

4. Legal liabilities may exist if the appropriate policies and procedures are not developed and enforced.

Recommendations

1. **Inbound/Outbound Mail Delivery High Availability**

   As stated above, inbound mail delivery is already centralized within the organization and is scalable to meet future needs with minimal increase in equipment and FTE. The one notable weakness is that an extended power outage or catastrophic event at the Mesa Lab would halt all inbound mail delivery. Current plans for installation of a generator system at the Mesa site will mitigate this vulnerability. However, it is recommended that a complete risk assessment be conducted to determine the risks associated with centralized inbound and outbound mail services and recommend high availability solutions as appropriate. Possible solutions may include replication of the service at an alternate site, multiple and distributed Internet access points, and alternate support personnel to provide 24x7 support. Any additional features implemented will also increase the reliability/availability to the central outbound mail delivery system, as the functions are located on the same machines.
2. **Outbound Mail Delivery**

Centralized outbound mail delivery can provide additional features such as outbound virus scanning, mechanisms that would make it difficult for spammers to forge "ucar.edu" user addresses as senders, and provide an authenticated Simple Mail Transport Protocol (SMTP) service that outside users could access. Modifications at the division/program level are minimal to make use of the existing central outbound mail service, and the incremental cost to accommodate the increased load is small. It is recommended that the CSAC be charged to fully evaluate the impacts of the additional security features that could be provided with a mandated centralized outbound mail delivery system and to submit the appropriate recommendations to the ITC regarding a transition to a mandated central outbound delivery system.

3. **Service Level Agreements**

We also recommend provision of 24x7 support for existing and recommended services through a policy statement that provides avenues by which after-hours problems might be remedied. Related to 24x7 support, it is recommended that additional personnel be trained and prepared to respond to administration of these services as warranted.

4. **Legal Issues Related to Electronic Mail Archives**

Regardless of all other actions, a UCAR policy regarding electronic mail archives needs to be developed.

5. **Centralize Mailbox Servers**

Centralization of user mailboxes is a more complex issue than the other mail system components. Technical and policy decisions are more visible to the end user and would directly affect work practices organization wide. The benefits include the ability to provide a consistent suite of services, software, and policies across the organization. The costs will be in the hardware, software, maintenance, and personnel costs for implementing and supporting a new central server system. Staff impacts will be the time required to reconfigure electronic mail clients, and if necessary, for staff to learn new mail client software as support for older packages is dropped in favor of client software that is compatible with the features available with newer mail protocols. The one-time staff impacts of this process can be mitigated with carefully developed education and transition plans.

It is recommended that a phased-in centralized electronic mailbox solution be implemented. To that end, it is recommended that a task force be formed to design and implement a centralized mailbox solution. The design should include a high-performance, high-availability system, provide for adequate disk storage with mirroring technology, and an appropriate archival system. All components of the system should be scalable to accommodate a phased implementation. Specifications for software to support an enterprise class mailbox solution should be included, with the merits of both open source and commercial software investigated. Estimates for FTE support should be included that would provide for backup staff support for the system. In addition, the task force should assess the impacts to the organization, develop appropriate transition and education programs, and work with divisions and legal staff.
to develop appropriate policies and procedures. This task force would have an ongoing commitment to ensure that the deployed solution evolves appropriately over time. The system would be opt-in or opt-out determined either at the division level or by the end user.
3. Case Study Findings

Following are the responses we have received to date from other institutions that have centralized computing services. From each of the following there were written responses and some informal phone conversations. Written responses are included in their entirety. It should be noted that some individuals indicated that these were their personal viewpoints and should not be considered the official position of the institution. We have not received responses from CU or Ball Aerospace.

National Renewable Energy lab
- 1200 workers (staff, contractors, students
- 5 campuses

University of Illinois - Urbana-Champaign
- Large public university
- 3 campuses: Chicago, Springfield and Urbana-Champaign
- 67,600 students, 5,400 faculty, 7,000 staff members

NOAA/Forecast Systems Lab
- 220 Staff
- Single campus
- Interact with (collaborate on projects, provide supercomputer resources/services, provide/receive large volumes of data/products, etc.) hundreds of entities in this country and abroad (including UCAR/NCAR, NWS/NCEP, numerous NWS WFOs, FAA, AFWA, universities, Taiwan Central Weather Bureau, etc.)

Argonne National Laboratory
- Minimal centralization

Los Alamos National Laboratory
- One 43 square mile site.
- About 8,000 University of California employees, ~2,500 contractors, and ~1,000 visitors on-site every day.

What group initiated a centralization of computer support services?

- Executive management initially. However, the degrees of centralization was reviewed by staff and management across the lab during a re-engineering effort.
- Given the size of the organization, there was always some centralization of computer support services for as long as I remember. However, there was a second level of centralization within each college or department. For example, our department had many central services, while individual faculty also had their own computer operations.
- Certain core services have always been done by the central organization. i.e. provision of the network backbone connection, purchase and coordination of site licensed software and others.
During the past few years, the pendulum started to swing back towards a more centralized architecture. This was in part due to NOAA setting up mandatory centralized services such as e-mail gateways in Washington, DC and Seattle, X.500 directory, etc. At FSL, we succeeded implementing a central e-mail server and have eliminated most division mail servers.

As mentioned above, several centralization issues were mandated by our higher level management (NOAA and DOC). Implementation of the required IT security measures also necessitated several services to be centralized.

ITS has worked with lab management to centralize additional services, but not anywhere near all of them. The fact that centralization of services makes sense, saves funds, and helps the users to do their job better has carried and continues to carry relatively little weight with the staff. In general, staff strongly resists changes and many feel that they can do the job better. It's just human nature.

For all of ANL, we are not centralized. While centralization of some things makes sense, the lab is to diverse in needs and requirements to have a complete cookie cutter model on what is being done.

About half of the Laboratory desktop systems are managed from a central organization. About 1/4 are managed by local people in organizations. About 1/4 are self-managed.

What was the original goal of the centralization effort?

- Reduced costs through economies of scale and standards where practical
- Increased interoperability between systems and processes throughout the lab
- Allow researchers to focus on their areas of research and not be interrupted to provide IT support functions.
- Ensure that central IT services fully serve the teaching, research and service missions of the university through partnership and collaborations with individual units on campus
- Provide better and more consistent computer and network services for the lab
- Simplify procedures
- Save money
- Standards, interoperability and cost savings

What did the implementation solution look like and how was it different from the original goals?

- The outcome was consistent with objectives. The whole governance process for IT investments is a lot more complex that what we thought. It continues to evolve.
- The implemented solution is too complex to describe in words. The UIUC Campus Information Technologies and Educational Services (CITES) provides approximately 75 services to the University of Illinois at Urbana-Champaign, including an array of services in the following categories:

  Calendaring
  Classroom Technologies
  Computer Facilities
  Computing Accounts
  Departmental Services
  Educational Technologies
  Electronic Directory
Email
Networking & Remote Access
Passwords
Security
Software (Media and Licensing)
Telecommunications

- So far, the results are somewhat mixed. Good progress has been made in implementing DOC/NOAA-mandated services and IT security. We are encountering more difficulties in areas that impact users directly; for example, web services, ftp-ing data in/out the lab, etc.
- We tried for institutional funding for desktop management. Didn't happen so we have a fee-for-service organization managing about half of the Lab desktops.

What was the process used for the project from inception to completion and how long did it take to complete?

- Like everywhere else, NREL's IT environment is in a state of perpetual change. Steering committees are used to govern large investments and all business system projects. Implementation took 18 months.
- It was not a single project that created CITES at UIUC. Rather, it was an evolution over three decades of a centralized facility to provide computing and telecommunication services to the campus.
- The FSL centralization is far from complete. Setting up an IT architecture group has helped some. As in earlier transitions (to/from centralization), the centralization process is taking time, measured in years, not months.

What were the arguments for and against centralization?

For:

- Reduced costs
- Better integration of IT resources and information
- Linkages to Laboratory objectives
- As you can see from the above category of services (UIUC), it is a waste of precious resources for each unit to replicate the same or similar types of services
- Scales of economy and reduced cost
- Lack of resources within individual units or lack of uniformity in availability of locally provided services (The Haves vs. the Have Nots)
- The other reason for centralization is, of course, IT security. ITS has set up centrally managed firewalls, IDS, VPN for remote access, and secure wireless for the lab - all centrally managed.
- Some centralization was mandated by DOC/NOAA
- Centralization made sense and saved money
- Resulted in better services
- Cost savings and interoperability plus a more consistent security model

Against:

- User flexibility-users better understand their own need
• Centralization leads to poorer customer service
• A single solution does not work for a large organization like UIUC with different stakeholders
• Highly heterogeneous computing environments that are widely distributed across a campus
• The central operation is not in touch with individual needs of faculty and staff in different departments
• Centralization took away researchers’ freedom of action
• Hindered lab staff doing their work
• Most importantly, people were very resistant to any kind of change
• While centralization of some things makes sense, the lab is to diverse in needs and requirements to have a complete cookie cutter model on what is being done.
• Some prefer local control

What were the cost savings or cost increases of this action?

• The resulting IT organization provided a smaller set of “needed” services with a budget reduced by 40%. IT support staff greatly increased their level of expertise as a result of simplifying the environment.
• Don’t have a comparison since it was always there.
• This is difficult to quantify. FSL was able to release several sys admins, reduced the number of machines providing centralized services, saved the associated maintenance costs, etc.
• Hard to say other than we believe that our central organization is consistent with industry total cost of ownership practices (e.g. Gartner). Our ratio is generally one technician for 90 desktops.

What specific services were centralized?

• Helpdesk, email, networks, cyber security, desktop support, system administration of server resources
• For a complete list, see http://www.cites.uiuc.edu/services/index.html
• E-mail, DNS, some data services, data storage, web services - not all these are yet complete.
• There are some things that are being done more centralized. The CIS group offers various services that divisions can make use of if they want/need. ex: mail servers, web servers, backup services, Active Directory. Use of these services is split. MCS does it all on their own as we exceed the capabilities of CIS servers. Others like ES, CI, and the OPs areas use the central services heavily. Most of the bigger divisions are split in how they do things. They will use the MS-AD services, but have their own mail and web servers.
• Desktop support, electronic software distribution, configuration management.
• Our network services have been centralized since the early 1990's.

How was buy-in achieved? What were the hurdles?

• Collaborated extensively with “key users” in the definition of what services were valued and to be supported centrally. User community was very diverse in its views and everyone was not satisfied.
• There wasn't a uniform degree of buy-in for all of the above services. It was felt that some computer services like system administration, hardware maintenance, etc. were better performed locally within each department or even a group (provided resources are available)
• Most important was that people are inherently against any kind of change: "I have been doing it this way for years, why should I change now?"
• Best buy-in was achieved by working with users and helping them to continue doing their work, albeit often differently from the way they used to.
• We have an information architecture effort where standards are proposed, commented on and adopted in a grass roots, voluntary participation model. Our measurements indicate that we generally get 90% buy-in.
• Hurdles are that some people just prefer to do it themselves. That has been OK in the past but increasing security requirements are leading us away from voluntary compliance to mandatory compliance.

Was information and training provided for centralization of computing services adequate?

• It was decided that "free" training for standard software applications was to be provided to staff. I believe it was adequate.
• Yes. Many, many opportunities for training were available to faculty, staff and students.
• No, you can never provide enough information and training. The rule of 5 to 10 always holds; 5-10% of people don't get the message, no matter what you do.

What was the impact of this change to your work environment?

• The environment became easier to support as a result of simplifying the environment
• Required much more effort to develop a clear understanding of organizational requirements of IT investments.
• For the most part, very positive. As mentioned above, however, system administration, software installation and hardware repair facilities were less successful, from my POV. These services were slow for our needs. The general feeling amongst faculty was that if their group's computer failed for some reason, it must be repaired IMMEDIATELY. In general, faculty had no patience for a 1-2 day turn around for response.
• Wherever they provide a useful service at little or no additional cost to us, we try to take advantage of it. However, when it comes to supporting end-users and departmental computing needs (i.e. e-mail, web services, number crunching), while they have options for purchasing such things at significant cost, we prefer to invest that money in our own staff and resources where we can better customize them to meet our needs. If we were to outsource these functions to them, we'd basically have to take their one-size-fits-all model, which is insufficient for some of our needs.
• The only major thing we've switched from departmental to centralized while I've been here that I can think of right now, is that we've recently started taking full advantage of the directory and authentication services provided by the central organization (LDAP and Active Directory).
• Making any change is always an additional burden on the staff. Over the last few years, ITS staff was reduced significantly (more than 25%), so the centralization effort has and continues to take its toll.
• If centralization is for sysadmin/hardware and that type of support the FSL model is actually rather good. Extremely good folks, staying very current, working under amazing overload of course, all driven by a trouble ticket system that actually works.

What changes in the quality of service did you experience?

• Drastically improved IT infrastructure availability
• Improved customer satisfaction as measured by monthly surveys
• Better integration of corporate information and IT resources
• Accountability for IT investments
• Much improved cyber security
• We (ITS) think that the lab is receiving better services following centralization; some users seem to agree, others do not.

In retrospect, what might have been done differently?

• Initially, significant cost saving where going to be achieved by the strict adherence to desktop standards. We failed to fully understand the cultural implications. As a result, some good will was lost in an attempt to implement. We came to our senses and found balance, but it was painful. The standards that we wanted to implement were validated with key representatives from the user community. Therefore, we did not anticipate the backlash we experienced.
• There was often little dialog between individual units and the central organization. The sys admins in our department always felt that dictates were coming down from a central organization on many issues (e.g., security, networking, etc.) with little opportunity to influence them. Other than periodic boiler-plate QOS surveys and questionnaires on new products and services, the units or the faculty/staff had little influence on how things were down at the central level.
• Better, more frequent and detailed information dissemination to lab staff on the planned centralization and related changes would have been helpful.
• Management buy-in and support are critical to making a centralization effort succeed.
• Go mandatory sooner.
Attendance at the November 3, 2003 DIG Forum on Active Directory:

<table>
<thead>
<tr>
<th>Name</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tim Fredrick</td>
<td>ACD</td>
</tr>
<tr>
<td>Herb Poppe</td>
<td>SCD</td>
</tr>
<tr>
<td>Aaron Anderson</td>
<td>SCD</td>
</tr>
<tr>
<td>Pat Waukau</td>
<td>MMM</td>
</tr>
<tr>
<td>Ted Russ</td>
<td>JOSS</td>
</tr>
<tr>
<td>Diane Norman</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Linda Zhang</td>
<td>RAP</td>
</tr>
<tr>
<td>Anne-Marie Tarrant</td>
<td>RAP</td>
</tr>
<tr>
<td>Kay Sandoval</td>
<td>MMM</td>
</tr>
<tr>
<td>Jose Castilleja</td>
<td>MMM</td>
</tr>
<tr>
<td>Sudie Kelly</td>
<td>MMM</td>
</tr>
<tr>
<td>Mark Moore</td>
<td>CGD</td>
</tr>
<tr>
<td>Wendy Derman</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Ron Lull</td>
<td>HAO</td>
</tr>
<tr>
<td>Mark Uris</td>
<td>SCD</td>
</tr>
<tr>
<td>Eric Gilbert</td>
<td>HAO</td>
</tr>
<tr>
<td>Peter Fox</td>
<td>HAO</td>
</tr>
<tr>
<td>Mark Bradford</td>
<td>JOSS</td>
</tr>
<tr>
<td>Shawn Winkelman</td>
<td>F&amp;A</td>
</tr>
</tbody>
</table>

Attendance at November 18, 2003 DIG Forum on Anonymous FTP:

<table>
<thead>
<tr>
<th>Name</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bill Boyd</td>
<td>MMM</td>
</tr>
<tr>
<td>Mark Bradford</td>
<td>JOSS</td>
</tr>
<tr>
<td>Bob Campbell</td>
<td>SCD</td>
</tr>
<tr>
<td>Garth D’Attillo</td>
<td>ASP</td>
</tr>
<tr>
<td>Terri Eads</td>
<td>RAP</td>
</tr>
<tr>
<td>Peter Fox</td>
<td>HAO</td>
</tr>
<tr>
<td>Barry Gamblin</td>
<td>HAO</td>
</tr>
<tr>
<td>Karl Hanzel</td>
<td>COMET</td>
</tr>
<tr>
<td>Heather Harris</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Mark Moore</td>
<td>CGD</td>
</tr>
<tr>
<td>Diane Norman</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Bob Rilling</td>
<td>ATD</td>
</tr>
<tr>
<td>Mike Schmidt</td>
<td>UNIDATA</td>
</tr>
<tr>
<td>Jeff Stolte</td>
<td>RAP</td>
</tr>
<tr>
<td>Steve Waltman</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Pat Waukau</td>
<td>MMM</td>
</tr>
<tr>
<td>Shawn Winkleman</td>
<td>F&amp;A</td>
</tr>
</tbody>
</table>
## Attendance at November 2003 DIG Forum on Calendaring:

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diane Norman</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Cheryl Cristanelli</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Lucy Warner</td>
<td>UCAR Comm</td>
</tr>
<tr>
<td>Mike Daniels</td>
<td>ATD</td>
</tr>
<tr>
<td>Charlie Martin</td>
<td>ATD</td>
</tr>
<tr>
<td>Jose Castilleja</td>
<td>MMM</td>
</tr>
<tr>
<td>Penny Warfel</td>
<td>MMM</td>
</tr>
<tr>
<td>Mary Hanson</td>
<td>MMM</td>
</tr>
<tr>
<td>Kay Sandoval</td>
<td>MMM</td>
</tr>
<tr>
<td>Scott Hayes</td>
<td>SCD</td>
</tr>
<tr>
<td>Mark Uris</td>
<td>SCD</td>
</tr>
<tr>
<td>Belinda Housewright</td>
<td>SCD</td>
</tr>
<tr>
<td>Anne-Marie Tarrant</td>
<td>RAP</td>
</tr>
<tr>
<td>Rhonda McGaffic</td>
<td>RAP</td>
</tr>
<tr>
<td>Mark Bradford</td>
<td>JOSS</td>
</tr>
<tr>
<td>Gene Martin</td>
<td>JOSS</td>
</tr>
<tr>
<td>Garth D'Attilo</td>
<td>ACD/ASP</td>
</tr>
<tr>
<td>Mic Stremel</td>
<td>DLESE, NSDL</td>
</tr>
<tr>
<td>Eilene McIlvain</td>
<td>DLESE, NSDL</td>
</tr>
<tr>
<td>Mark Moore</td>
<td>CGD</td>
</tr>
<tr>
<td>Mike Schmidt</td>
<td>UNIDATA</td>
</tr>
<tr>
<td>Liz Chapin</td>
<td>HAO</td>
</tr>
<tr>
<td>Eric Gilbert</td>
<td>HAO</td>
</tr>
<tr>
<td>Terri Eads</td>
<td>RAP</td>
</tr>
<tr>
<td>Tres Hofmeister</td>
<td>RAP</td>
</tr>
<tr>
<td>Aaron Anderson</td>
<td>SCD</td>
</tr>
<tr>
<td>Pat Waukau</td>
<td>MMM</td>
</tr>
<tr>
<td>Shawn Winkelman</td>
<td>F&amp;A</td>
</tr>
</tbody>
</table>
### Attendance at December 4, 2003 DIG Forum on Central Authentication Services:

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aaron Andersen</td>
<td>SCD</td>
</tr>
<tr>
<td>Bill Boyd</td>
<td>MMM</td>
</tr>
<tr>
<td>Mark Bradford</td>
<td>JOSS</td>
</tr>
<tr>
<td>Peter Burkholder</td>
<td>DLESE</td>
</tr>
<tr>
<td>Bo Connell</td>
<td>SCD</td>
</tr>
<tr>
<td>Terri Eads</td>
<td>RAP</td>
</tr>
<tr>
<td>Peter Fox</td>
<td>HAO</td>
</tr>
<tr>
<td>Tim Fredrick</td>
<td>ACD</td>
</tr>
<tr>
<td>Barry Gamblin</td>
<td>HAO</td>
</tr>
<tr>
<td>Karl Hanzel</td>
<td>COMET</td>
</tr>
<tr>
<td>Rich Johnson</td>
<td>SCD</td>
</tr>
<tr>
<td>Mark Moore</td>
<td>CGD</td>
</tr>
<tr>
<td>Diane Norman</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Mike Schmidt</td>
<td>UNIDATA</td>
</tr>
<tr>
<td>Pat Waukau</td>
<td>MMM</td>
</tr>
<tr>
<td>Steve Waltman</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Karl Werner</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Shawn Winkelman</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Greg Woods</td>
<td>SCD</td>
</tr>
</tbody>
</table>

### Attendance at October 29, 2003 DIG Forum on Directory Services

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aaron Andersen</td>
<td>SCD</td>
</tr>
<tr>
<td>Bill Boyd</td>
<td>MMM</td>
</tr>
<tr>
<td>Bobbie Abdallah</td>
<td>HAO</td>
</tr>
<tr>
<td>Chris Burghart</td>
<td>ATD</td>
</tr>
<tr>
<td>Diane Norman</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Garth D’Attilo</td>
<td>ASP</td>
</tr>
<tr>
<td>Ginger Caldwell</td>
<td>SCD</td>
</tr>
<tr>
<td>Greg Woods</td>
<td>SCD</td>
</tr>
<tr>
<td>Leif Magden</td>
<td>SCD</td>
</tr>
<tr>
<td>Mark Bradford</td>
<td>JOSS</td>
</tr>
<tr>
<td>Mark Moore</td>
<td>CGD</td>
</tr>
<tr>
<td>Mike Daniels</td>
<td>ATD</td>
</tr>
<tr>
<td>Mike Schmidt</td>
<td>UNIDATA</td>
</tr>
<tr>
<td>Pat Waukau</td>
<td>MMM</td>
</tr>
<tr>
<td>Peter Burkholder</td>
<td>DLESE</td>
</tr>
<tr>
<td>Shawn Winkelman</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Ted Russ</td>
<td>JOSS</td>
</tr>
<tr>
<td>Tres Hofmeister</td>
<td>RAP</td>
</tr>
<tr>
<td>Victor Tisone</td>
<td>HAO</td>
</tr>
<tr>
<td>Wendy Derman</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Michael Leon</td>
<td>GLOBE</td>
</tr>
</tbody>
</table>
### Attendance at November 7, 2003 DIG Forum on Electronic Mail

<table>
<thead>
<tr>
<th>Name</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tim Fredrick</td>
<td>ACD</td>
</tr>
<tr>
<td>Mike Daniels</td>
<td>ATD</td>
</tr>
<tr>
<td>Brandon Slaten</td>
<td>ATD</td>
</tr>
<tr>
<td>Ron Ruth</td>
<td>ATD</td>
</tr>
<tr>
<td>Mark Moore</td>
<td>CGD</td>
</tr>
<tr>
<td>Karl Hanzel</td>
<td>COMET</td>
</tr>
<tr>
<td>Mic Stremel</td>
<td>DLESE</td>
</tr>
<tr>
<td>Heather Harris</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Diane Norman</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Steve Waltman</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Shawn Winkleman</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Carol Smith</td>
<td>F&amp;A</td>
</tr>
<tr>
<td>Peter Fox</td>
<td>HAO</td>
</tr>
<tr>
<td>Barry Gamblin</td>
<td>HAO</td>
</tr>
<tr>
<td>Mark Bradford</td>
<td>JOSS</td>
</tr>
<tr>
<td>Bill Boyd</td>
<td>MMM</td>
</tr>
<tr>
<td>Jose Castilleja</td>
<td>MMM</td>
</tr>
<tr>
<td>Pat Waukau</td>
<td>MMM</td>
</tr>
<tr>
<td>Terri Eads</td>
<td>RAP</td>
</tr>
<tr>
<td>Tres Hofmeister</td>
<td>RAP</td>
</tr>
<tr>
<td>Jeff Stolte</td>
<td>RAP</td>
</tr>
<tr>
<td>Anne-Marie Tarrant</td>
<td>RAP</td>
</tr>
<tr>
<td>Deirdre Gary</td>
<td>RAP</td>
</tr>
<tr>
<td>Aaron Andersen</td>
<td>SCD</td>
</tr>
<tr>
<td>Ginger Caldwell</td>
<td>SCD</td>
</tr>
<tr>
<td>John Fox</td>
<td>SCD</td>
</tr>
<tr>
<td>Greg Woods</td>
<td>SCD</td>
</tr>
<tr>
<td>Doug Smith</td>
<td>UNIDATA</td>
</tr>
</tbody>
</table>
UCAR Directory Data Flow Diagram
29-Nov-2001 (JC) -- *click for detail

DSAC Implementation Group
Appendix B: UCAR Directory Data Flow Diagram