Departmental Computing Plan

Neil Hoggarth,
Departmental Computer Officer,
University Laboratory of Physiology,
Oxford.

September 8, 2005

Abstract

This document describes the various computing related facilities and services which are provided and organised at a Departmental level. It discusses the policy objectives we have identified, gives a description of the implementation which we have used to meet these objectives and documents the detailed operational procedures required for running the file server and network.
# Contents

1 Introduction 6

2 Policy 7

2.1 The Network . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

2.2 Administrative Information . . . . . . . . . . . . . . . . . . . . 8

2.2.1 User Accounts . . . . . . . . . . . . . . . . . . . . . . . . 8

2.2.2 Host Information . . . . . . . . . . . . . . . . . . . . . . . 9

2.3 Network File Services . . . . . . . . . . . . . . . . . . . . . . . 9

2.3.1 Personal File Storage . . . . . . . . . . . . . . . . . . . . . 10

2.3.2 Shared File Storage . . . . . . . . . . . . . . . . . . . . . . 10

2.3.3 Shared Software . . . . . . . . . . . . . . . . . . . . . . . . 11

2.4 Print Services . . . . . . . . . . . . . . . . . . . . . . . . . . . . 11

2.5 Electronic Mail . . . . . . . . . . . . . . . . . . . . . . . . . . . . 12

2.6 Information Services . . . . . . . . . . . . . . . . . . . . . . . . 13

2.6.1 WWW Service . . . . . . . . . . . . . . . . . . . . . . . . . . 13

2.6.2 Other Remote File Transfer Services . . . . . . . . . . . . . 13

2.7 Security . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

2.7.1 Availability . . . . . . . . . . . . . . . . . . . . . . . . . . . 15

2.7.2 Backup . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 15

2.7.3 Network Firewalls . . . . . . . . . . . . . . . . . . . . . . . 16

2.7.4 Critical Software Updates . . . . . . . . . . . . . . . . . . . 16

2.7.5 Anti-Virus Provision . . . . . . . . . . . . . . . . . . . . . . 17

2.8 Archival Storage . . . . . . . . . . . . . . . . . . . . . . . . . . 17

2.9 User Support . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 18
# Implementation

3.1 The Network ........................................ 19
   3.1.1 Network Hardware ............................. 19
   3.1.2 Protocols and Routing .......................... 21

3.2 The Departmental Servers ............................ 23

3.3 Administrative Databases ........................... 23
   3.3.1 The *people* File .............................. 26
   3.3.2 Passwords .................................... 27
   3.3.3 The *machines* File ........................... 28
   3.3.4 The Domain Name System and the Internet ....... 29

3.4 Network File Services ............................... 31
   3.4.1 NFS file services .............................. 31
   3.4.2 Unix Clients .................................. 31
   3.4.3 DOS Clients ................................... 34
   3.4.4 Windows Clients ................................ 35
   3.4.5 Shared Software For PC Clients ............... 38
   3.4.6 Macintosh Clients .............................. 39
   3.4.7 Other Clients .................................. 40
   3.4.8 The */home/willis* Filesystem ................. 40

3.5 Electronic Mail ..................................... 43
   3.5.1 Routing, Transport and Delivery ............... 43
   3.5.2 Reading and Composition ....................... 47

3.6 HTTP Services ...................................... 48
   3.6.1 Departmental Web Pages ......................... 49
   3.6.2 Users’ Personal Web Pages ...................... 50
   3.6.3 Third-Party File Upload ........................ 50
   3.6.4 Remote File Management and Transfer .......... 51
   3.6.5 Web-based Email Interface ..................... 52
   3.6.6 Web-based Interface to the “Req” Request Tracker .. 52
   3.6.7 User Authentication ............................ 53
   3.6.8 Database Storage ............................... 53
3.7 Availability of the Departmental Servers ....................... 53
  3.7.1 Disk Mirroring ............................................ 54
  3.7.2 Duplication of the Departmental Servers ................ 56
  3.7.3 Availability of the Network ............................... 58
3.8 Backup .......................................................... 58
  3.8.1 Offsite Backup .............................................. 60
3.9 Software Updates ................................................ 60
  3.9.1 Windows 2000, XP and 2003 ............................... 60
  3.9.2 SUSE Linux .................................................. 61
  3.9.3 Red Hat Linux .............................................. 61
3.10 Anti-Virus Measures ............................................. 61
3.11 Writing CD-ROMs ............................................... 62
3.12 Clock Synchronization ........................................... 62
  3.12.1 Unix Clients .............................................. 63
  3.12.2 Windows 95 Clients ....................................... 63
  3.12.3 Windows 2000/XP Clients ................................. 63
  3.12.4 DOS Clients ............................................... 64
3.13 The “Req” Request Tracking System ............................. 64

4 Procedures ......................................................... 66
  4.1 Modifying The Network Databases — General Guidelines .... 66
  4.2 Connecting Devices To The Network ............................ 67
    4.2.1 Preparing the Administrative Databases .................. 67
    4.2.2 Connecting a Solaris Client ............................. 68
    4.2.3 Connecting an IRIX 6.5 Client ........................... 68
    4.2.4 Connecting a Linux Client ............................... 71
    4.2.5 Connecting a DOS Client ................................ 73
    4.2.6 Connecting a Windows 95 Client ........................ 73
    4.2.7 Connecting a Windows 2000 or Windows XP Client ...... 75
    4.2.8 Deriving HOSTID For PC Clients .......................... 75
    4.2.9 Connecting a Macintosh ................................. 77
    4.2.10 Connecting Other Devices .............................. 77
4.3 Managing User Accounts
   4.3.1 Creating a New User Account
   4.3.2 Enabling a User Account
   4.3.3 Closing a User Account
4.4 Restoring Files From Backup
   4.4.1 Restoring From Local Backup Tape
   4.4.2 Restoring From The HFS
4.5 Shutting Down or Rebooting Willis or Wren
   4.5.1 Alternative Boot Devices
4.6 Hardware Problems and Maintenance Contracts
   4.6.1 Calling Sun Service
   4.6.2 Calling SGI Support
   4.6.3 Network Maintenance
Chapter 1

Introduction

The Department has a diverse and decentralized organizational structure. The various research groups within the Department have a considerable degree of autonomy. Much of the computing equipment within the Department is purchased, owned and operated by the research groups, rather than being a Departmental resource. The Department’s principle IT rôle is providing the network and various network based services.

It is not our intention to dictate to research groups concerning the organisation of their computers nor the extent to which they should make use of the centralized services on offer. In general the document describes how the various centralized services are expected to operate where groups decide to make use of them. However the document does discuss some aspects of network administration and use which have to be correctly coordinated if problems are not to arise. Owners and users of computers attached to the network are required to observe the guidelines laid down concerning such matters.

This document is periodically updated, tracking the policies and implementation details of the Departmental computing facilities as they change. It therefore serves both as a guide to what is available to potential users of the services and as a technical reference to staff who make use of and maintain the services. It describes not only how the systems are set up but also why they were set up the way that they are.

This document exists in both on-line hypertext\(^1\) and printed forms. The two forms are derived from the same source and are intended to be equivalent. The on-line version is by its very nature more current and may contain references or types of content which cannot be properly represented on paper — if discrepancies occur between the two versions then the on-line version should be considered definitive.

\(^1\)http://www.physiol.ox.ac.uk/Computing/plan/departmental-computing.html
Chapter 2

Policy

This chapter describes in general terms the various computing facilities and services provided by the Department and its objectives in providing them.

2.1 The Network

The Department shall provide a network which links together the computers based within it, provides convenient access to various internal computing related resources and provides access to external resources and information sources via the University network and the global Internet.

The network infrastructure provided shall be organized such that it is as flexible as possible. It should be able to accommodate future growth, internal re-organisation and developments in networking technology. Internally the network shall not rely on any particular transport protocols or routing arrangements. Any node should be able to address directly packets to any other node, or make broadcasts received by all nodes on the network (this implies that any management and segregation of network traffic is based on bridging and switching techniques rather than routing techniques). See section 3.1.1 for a detailed discussion of the current physical organization of the infrastructure.

The internal network shall be connected to external networks via a router operated by OUCS. See section 3.1.2 for a discussion of the routing arrangements in place and the transport protocols which can be exchanged with external networks.

Many services which are required for members of the Department to do their job effectively are dependent on the network infrastructure. The Department shall take steps to ensure that the network service is as reliable as possible. See section 3.7.3 for details of current planning concerning this matter.
2.2 Administrative Information

Note: In this document the word “administrate” and its derivatives typically refers to administration of the network, rather than administration of the Department.

There are various sets of information used by computers on the network for administrative purposes. Examples include lists of the authorised users of the network and the various computers connected to it, the names of the devices attached to the network and their associated network addresses and the correct port numbers to use for various services.

The Department shall operate centralized databases providing administrative information and make them available for the machines on the network to consult. Computers attached to the network shall use information provided by the network databases wherever possible, in order to minimize administrative workload and maintain consistency across the network.

The Departmental file server shall act as the master information server for the network, holding definitive versions of all the administrative files. Where possible, replicas of the various information services shall be established — holding copies of the master’s information and maintaining the information service if the master server is unavailable for some reason.

2.2.1 User Accounts

In order to promote the effective use of facilities such as network file services and electronic mail, each person within the Department shall have a unique identity which they can use to access the Department’s computers. This identity consists of a unique username, user ID number and password. For historical reasons this is referred to as a computer “account”, although no direct charges are made for computer or network use on a person by person basis.

All members of staff, research workers and graduate students in the Department shall have an account. Requests for accounts for other persons (such research collaborators from outside the Department) can be made in writing or by e-mail to Computing. All reasonable requests will be favourably considered.

Leaders of research groups and persons with responsibility for Departmental staff should keep Computing informed about new arrivals to and departures from the Department so that the list of active users can be kept current.

Each account is associated with a named individual who has authorisation to use the Department’s facilities. Account information can and will be used to track the actions and limit the privileges of the account owner. Users must not allow others to use their accounts.

All computers attached to the network should make use of user information from the Departmental databases to identify and authenticate users wherever possible.
2.2.2 Host Information

Each computer (or other device) attached to the network shall be registered with the Computing. Computing shall maintain a database of all the devices attached to the network, recording such information as:

- hardware address information (ie. the IEEE 802 Media Access Control address).
- any protocol specific address information (eg. IP addresses).
- the hostname associated with the device.
- the type of device.
- the owner or principle user of the device.

Maintaining a proper record of such information is important to enable to computing staff to monitor adequately the network, trace networking problems, etc. A detailed discussion of the form in which this information is held, and the mechanisms by which it is made available to machines on the network, can be found in section 3.3.3.

All computers attached to the network should make use of the hostname and network addressing information available from the Departmental databases wherever such information is required.

Where resources need to be assigned to network devices on a unique basis (such as hostnames and IP addresses) responsibility for their allocation shall rest with Computing. Computing shall also be responsible for any coordination between internal host information and external information databases, such as the Internet Domain Name System.

2.3 Network File Services

Network file services enable computers attached to the network to access files stored on other computers in the same way that they access files on their own disks. There are three ways in which a centralized network file service can be particularly useful to the Department; “personal file storage”, “shared file storage” and “shared software”. Each of these is discussed in detail below.

The Department and the research groups within it own a wide variety of computer platforms covering various different hardware architectures, operating systems and capabilities. The Department shall provide a unifying network file service which can cater to all the popular types of client machine in use. Currently most of the computers attached to the Departmental network fall into one of four basic types:

- Unix systems.
• IBM compatible PCs running MS-DOS (including those running MS-DOS and the MS-Windows 3.1 user interface).

• IBM compatible PCs running a 32 bit Microsoft Windows operating system (such as Windows 95 or Windows NT).

• Apple Macintoshes.

See section 3.4 for discussions of the various facilities used to provide services to each of these client types.

2.3.1 Personal File Storage

For each registered user of the network the Department shall provide an area where personal data, configuration files, documents, mail folders, etc can be stored and make this area accessible to the user over the network from any of the types of client machine discussed above. This area is referred to as a user’s “home directory”.

Storing personal files in their home directories offers users several key advantages:

• It allows users to access a single set of working files from different computers depending on which machine is the most appropriate for the task in hand, is the most convenient, or is available.

• It provides an easy to use way to transfer, store and manipulate files which they wish to use in conjunction with other centrally provided services, such as the Departmental World Wide Web server.

• Files stored on a network file server can be protected by a centralized backup regime. If a user’s important files are stored on a network file server which has high quality, frequent backup provision this reduces the backup requirements for client machines (although users are strongly urged to give proper consideration to a backup and retrieval strategy for their own machines as well). See section 2.7 for a discussion on the Department’s policies concerning availability of services and backup provision.

The Departmental shall, however, only provide a limited amount of storage for users in research groups. The Department considers the provision of large scale disk storage to be the responsibility of the user’s research group (where “large scale” is anything more than a few hundreds of megabytes). Research groups purchasing disk storage are encouraged to make it available to their members in the form of an network file service rather than in the form of many separate disks associated with individual PCs and workstations.

2.3.2 Shared File Storage

The Department shall provide network storage facilities where groups of users can share simultaneous access to collections of files. These facilities shall be
accessible to users over the network from any of the types of client machine discussed above. Such a facility is useful when a number of people do similar, overlapping jobs (the secretarial staff for example, or the staff who cooperate to provide IT support in the Department) or for academic staff and students working on a project where they need to share data, programs or results.

A discussion of the current implementation of shared network storage can be found in section 3.4.8.

2.3.3 Shared Software

The Department shall store on the network file service copies of application programs and utilities and make them available for running on any computer within the Department which wishes to make use of them.

Each software package need only to be installed once and when it needs updating then only one installation needs to changed. This approach is intended to reduce the administrative workload on the Department’s computing staff, free end users from much of the workload associated with maintaining the software and give users easy access to potentially useful software which they might not otherwise be inclined to invest time in.

It also has the potential to provide significant cost savings to the Department as a whole. Network or site licencing deals are often available which are considerably cheaper than buying multiple individual copies of a program. Sharing “floating” network licences across the network can be more cost effective than buying a licence for each machine which might occasionally be required to run a given application. Storing a single centralized copy of a popular application also reduces the amount of disk space used across the Department.

Documentation concerning the current shared software available shall be provided in Computing Information section\(^1\) of the Departmental Web pages.

2.4 Print Services

Provision of printing facilities is largely the responsibility of individual groups within the Department. There are several printers owned and operated by the Department, however, such as the laser printer in the Graduate Student’s computer room and the colour printers in Photography.

Where such facilities are provided, they shall be made accessible to computers over the network wherever possible.

\(^1\)http://www.physiol.ox.ac.uk/Computing/
2.5 Electronic Mail

The Department shall encourage the use of electronic mail by staff and students for internal and external correspondence.

Personal e-mail addresses shall follow the normal Oxford University convention—each registered user within the Department shall have an e-mail address of the form “firstname.lastname@physiol.ox.ac.uk”. In addition each user also has an e-mail address based on their Departmental username, of the form “username@physiol.ox.ac.uk”. The first type of address shall be the preferred form but username form has two important purposes:

- it ensures that users who were using e-mail before the preferred form of address was introduced will continue to receive messages which are addressed to their old addresses.
- it ensures that any automatically generated messages from computer systems within the Department which are sent to a username will be delivered to the appropriate person.

In line with University policy, the Department shall encourage the use of e-mail applications which utilise IMAP (the Internet Message Access Protocol, RFC 2060) for folder access and which support message bodies conforming to the MIME specifications (Multipurpose Internet Mail Extensions, RFC 2046). See section 3.5.2 for a discussion of the e-mail software currently supported and recommended by the Department.

The Department shall provide a mail server which can be accessed via the IMAP protocol. Use of this service is not mandatory. The Department shall use the mail routing facilities offered by OUCS to enable members of the Department to receive their e-mail on any computer system of their choice (as a consequence of this policy, no computer in the Department should regard unqualified addresses or addresses qualified with the domain physiol.ox.ac.uk as local — all such mail must be passed to the OUCS mail routing system for forwarding to the correct point of delivery).

The standards governing the Internet e-mail system require that each domain has associated with it an address “postmaster”, mail to which must be delivered to a human with responsibility for handling mail problems associated with the domain. Computing shall act as postmasters for the Department’s Internet domain (receiving and handling any messages addressed to postmaster@physiol.ox.ac.uk). Any user in the Department who has queries concerning e-mail or who experiences problems with the e-mail service should refer the matter to Computing in the first instance. Computing shall also act as the primary liaison between the Department and OUCS in matters relating to e-mail.

---

2. http://www.oucs.ox.ac.uk/email/oxford/index.xml?ID=body.1#iv.2
4. http://mirror.ox.ac.uk/Mirrors/ftp.isi.edu/in-notes/rfc2060.txt
5. http://mirror.ox.ac.uk/Mirrors/ftp.isi.edu/in-notes/rfc2046.txt
2.6 Information Services

2.6.1 WWW Service

The Department shall provide an Internet World Wide Web (WWW)\(^6\) service. This service shall be used to disseminate three different classes of document:

- Information intended for readers in the outside world, providing an “online publishing” capability for the Department and its members.
- Internal information and documentation intended for readers in the Department.
- References and links to on-line resources around the Internet, for the convenience of users in the Department.

The Departmental WWW server shall have the capability to distribute files from a nominated subdirectory within each registered user’s home directory, thus providing all users of the network with an easy to use WWW publishing capability. The document “Using the Web Server”\(^7\) explains the mechanics of making WWW pages available.

Objects or documents which are hyperlinked, directly or indirectly, from official Departmental pages may be regarded by outside readers as endorsed, approved or “published” by the Department. The Department shall offer links to collections of pages maintained by research groups and shall not normally offer links to individuals. Group pages may contain links to personal pages of group members; each research group shall have (and must exercise) editorial responsibility for the on-line content that is so linked.

2.6.2 Other Remote File Transfer Services

There are broadly speaking three types of file transfer between the Departmental file server and machines in remote locations not served by the normal file service which the Department needs to support:

- Authenticated transfers: the transfer of personal or shared files to or from the Departmental file server by persons who have Departmental network accounts.
- Third-party downloads: where a person with a Departmental network account wishes to make files available for copying to a person or persons without an account.
- Third-party uploads: where a person with a Departmental network account wishes to receive files from a person without an account.

\(^6\)http://www.w3.org/WWW/
\(^7\)http://www.physiol.ex.ac.uk/Computing/Using_the_Web_Server.html
Historically Internet sites have handled such transfers via an FTP service (the File Transfer Protocol, RFC 959\textsuperscript{8}), with a cleartext username and password for authenticated transfers and an “anonymous FTP” account with limited privileges and no password for third-party transfers. However, the Department no longer operates an FTP service: this was decommissioned in December 2001 due to security problems with the software that was being used to provide it, as well as a desire to eliminate the use of cleartext authentication credentials.

The preferred mechanism for file transfers is now HTTP (the Internet Hyper-text Transfer Protocol, RFC 2616\textsuperscript{9}), which has the advantage of widely deployed support in terms of clients (web browsers and file transfer tools such as wget), cross-network accessibility (even sites with stringent network filtering or firewalls typically offer some sort of web service to HTTP clients) and transport-level security (encryption of the the protocol exchange in order to protect authentication credentials, and/or the data in transit, from unauthorised interception or monitoring). Details of how the various different classes of file transfer task are implemented by the Department’s web server can be found in section 3.6.

### 2.7 Security

Computer and network security is a wide ranging issue. Garfinkle and Spafford [1] offer a useful operational definition of computer security:

> A computer is secure if you can depend on it and its software to behave as you expect.

Within this broad definition there are various aspects with which the Department should be concerned:

**Control** Preventing unknown and unauthorised individuals gain access to the network or any of the computer systems attached to it.

**Confidentiality** Protecting information from being read or copied by anyone who has not been explicitly authorized by the owner of that information.

**Integrity** Protecting information and programs from being deleted or altered in any way without the permission of the owner.

**Availability** Protecting services such that they are not degraded or made unavailable unexpectedly, whether by equipment failure, disaster or malicious act.

The computing staff are aware of the issues involved and attempt to behave responsibly to ensure confidentiality and integrity. Some of the other provisions discussed in this document touch on these areas (the policy concerning user accounts is intended to provide a degree of control and audit, for example) and

\textsuperscript{8}http://mirror.ox.ac.uk/Mirrors/ftp.isi.edu/in-notes/rfc959.txt

\textsuperscript{9}http://mirror.ox.ac.uk/Mirrors/ftp.isi.edu/in-notes/rfc2616.txt
the Department has developed policy and implemented mechanisms concerning availability.

Computing shall have formal responsibility and authority for ensuring control and integrity of Departmental computing facilities. Note that any compromised device attached to the network presents a potential threat to the integrity and confidentiality of the network itself. Computing’s responsibility shall extend to ensuring control over and integrity of all devices attached to the network. Access to the Departmental network shall be conditional on the acceptance of Computing’s authority in such matters.

2.7.1 Availability

Much of the activity which takes place in the Department is now reliant on the network services and infrastructure described in this document. Interruptions to these services are extremely disruptive to both the work of the research groups and the administration of the Department. The reliability and availability of the equipment and the services it provides are of key importance.

Where possible and cost effective the Department shall seek to arrange facilities and services such that they continue to be provided in the face of equipment failure or damage. Where this is not possible, the Department shall have planning in place in order to minimize the time taken to restore services. Discussions of the current provisions concerning availability of the network and the services provided by the file server are given in chapter 3.

The Department shall ensure that adequate provision is made for the maintenance of the network hardware, the file server and other computers involved in providing Departmental services. Details of the current procedures for calling for maintenance support for the network and the file server are given in chapter 4.

2.7.2 Backup

The Departmental servers shall be protected by a backup regime which provides protection for all the installed filesystems. In addition to user files and programs stored on the exported filesystems this also protects the network administration databases, the installed system software and the current configuration of the system (collectively these items represent a very substantial amount of invested time and effort).

At any time it should be possible to restore individual files or the system as a whole to the state that pertained:

- at the end of any weekday (Monday — Friday) in the previous week, including the end of the previous weekday.
- at the end of any week in the previous month, including the end of the previous week and excluding weeks where the Friday falls during either the Christmas or Easter “shutdown” period.
at the end of any month (the first backup made in any month is to be retained indefinitely).

The objective of a backup regime is to protect against the failure of disks and computers ("disaster recovery"). It is important to make clear that the objective is not to provide long term data storage for users (for policy relating to long term storage see section 2.8). In particular, the retention of monthly backups for an indefinite period should not be interpreted as an open-ended archival commitment on the part of the Department. No guarantees are made concerning the long term stability of the media used to store the backups, nor is any guarantee made concerning the long term availability of devices for reading historical backup media.

The backup regime operated by the Department is intended for the protection of the Departmental servers only. As a matter of policy it is intended that mass storage devices in a research group should be covered by backup arrangements made by that research group, and the owners and users of such systems are strongly urged to give the subject of backup their careful consideration (this need not be expensive or involve much administration — research groups could, for example, make use of the OUCS Hierarchical File Server (HFS) for backup).

2.7.3 Network Firewalls

The Department does not operate any "firewall" restrictions on network traffic. As outlined in the Network Policy, connectivity within the Departmental network is unrestricted, passing any and all Ethernet frames. Further more, TCP/IP and IPX connectivity between the Departmental network and the University backbone is not restricted by the Department (though some restrictions may be imposed by OUCS at the backbone router).

Communications between hosts on the Departmental network and the wider Internet beyond the University are subject to the restrictions of the University Firewall. Members of the Department should be aware that this firewall is relatively permissive, and that connection to the Departmental network is therefore a relatively unfiltered connection to the public Internet. This has important consequences for the security standards that must be applied to network attached devices.

2.7.4 Critical Software Updates

In order to provide control, confidentiality, integrity and availability, it is important that any known flaws in the operating system or application software used on computer systems in the Department are rectified in a timely manner.

Computer systems connected to the Departmental network should use operating systems and applications software for which active support and software

\[\text{http://hfs.ox.ac.uk/local/}\]
\[\text{http://www.oucs.ox.ac.uk/network/restricted/}\]
updates are available. Whenever software updates are available which fix critical bugs or address security flaws in installed software, these updates should be applied as soon as possible. Given the number of systems on the network it is preferable if such updates can be applied in an automated fashion, with little or no manual intervention required, and the Computing staff shall endeavour to provide and support the use of automated update mechanisms.

See the implementation chapter for a discussion of the automated update mechanisms for various operating systems currently deployed in the Department.

If network users within the Department choose not to utilise automated updates (or need to use operating systems and sensitive applications for which such updates are not available), then they have a responsibility to remain informed about potential problems (subscribing to announcement services offered by software vendors, for example) and to obtain and manually apply important software updates in a timely fashion. Responsible conduct in this respect shall be a condition of access to the network.

Computing staff should monitor relevant information sources (vendor security announcements, CERT announcements, security-related mailing lists and newsgroups, etc) on a frequent basis, in order to be able to react to newly discovered software vulnerabilities and emerging security threats in an informed fashion.

2.7.5 Anti-Virus Provision

All Windows-based personal computers on the Departmental network should be protected by anti-virus software. This software must be actively maintained and the virus signatures on which it depends must be updated on a frequent basis. The Department shall offer an anti-virus package which provides automated updates of the software and virus signature database. The current Departmental provision is documented in the the implementation chapter.

Owners of Windows-based PCs who choose not to make use of the departmentally provided solution must take personal responsibility for the installation and active maintenance of equivalent protection. Responsible conduct in this respect shall be a condition of access to the network.

2.8 Archival Storage

Some data require long term storage. Typically this need arises for large data sets which it would be inconvenient or impossible to leave on primary disk storage but which will (or might) be needed for reference in the future. The desired properties for such storage are that it should have a low cost per megabyte stored, that it should be stable over long periods of time, that it should be easy to store and preferably that it should be easy for users to access when they wish to refer to the archived data.
The Department shall encourage the use of CD-ROM as an archival storage media. For maximum portability we recommend that the data are stored on the discs such that the discs conform to the ISO 9660 standard. ISO 9660 is an agreed international standard for the format CD-ROM discs and conforming CDs can be read by all the computer platforms of interest to the Department.

The Department shall provide an ISO 9660 conformant CD recording service which can be used to create CD-ROMs containing users’ data. Members of the Department intending to use this service to archive their files should refer to the document “The CD Recording Service”\textsuperscript{12}, which explains the restrictions to filenames and directory structure imposed by the ISO standard and outlines several optional extensions to the standard which the service provided by the Department can support.

2.9 User Support

The primary responsibilities of the Computing staff shall be the planning, operation and maintenance of:

- the network infrastructure.
- the file and e-mail servers.
- the various network based services described in this document.
- the computerization of undergraduate practical classes.

and the routine administration of the network (provision of user accounts, connection of new machines, etc).

Requests and enquires from members of the Department relating to these activities should be sent via e-mail to computing@physiol.ox.ac.uk. All requests submitted in this manner are logged in a computerized request tracking system.

To cope with situations where a request cannot be handled via e-mail (the setting of an initial password on a new user account, for example) a member of Computing staff will be available for consultation between 2 and 3pm each day.

In addition to the user support issues resulting from these direct responsibilities, there is a considerable demand for general computing support and advice within the Department. There is no formal Departmental provision for such support and few of the research groups provide such support internally. This tends to impact on the Computing Staff’s ability to discharge their responsibilities with respect to the network, as users tend to approach them for assistance concerning any problem which is vaguely IT related. The situation can only worsen in future with the expansion of the Department and the ever increasing application of computing in all aspects of the Department’s work.

\textsuperscript{12}http://www.physiol.ox.ac.uk/Computing/The_CD_Recording_Service/
Chapter 3

Implementation

This chapter describes in technical detail the way in which the computing facilities and services provided by the Department are implemented.

3.1 The Network

3.1.1 Network Hardware

Figure 3.1 shows the various components and interconnections which make up the Departmental network.

The networking hardware in the main building is concentrated in five network distribution points, which are referred to by the Computing Staff using the labels “DP1” to “DP5”. The Oxford Centre for Gene Function is served by a further three distribution points.

DP1 is in room A62 and serves the east end of the main building.

DP2 is in room B25 and serves the west end of the main building.

DP3 is in room A65 and serves the east-end (neuroscience) extension.

DP4 is in room A42 and serves the west-end (cardiac) extension.

DP5 is a wall mounted data cabinet in the corridor outside of room C29 and serves the converted classroom 2 area (Physiome and Sports Medicine).

OCGF DP1 is in room 00.36 (basement) and serves the basement, ground and first floors of the OCGF.

OCGF DP2 is in room 20.26 (first floor) and serves the second and third floors of the OCGF.

OCGF DP3 is a wall mounted data cabinet in the corridor just inside the main door to the annex, serving the annex (the OCGF annex is located in the Old Observatory).
The computers and other networked devices owned by users in the Department are attached to RJ45 wall sockets throughout the buildings. A separate category 5 UTP (unshielded twisted pair) cable runs from each of these wall sockets to one of the distribution points, where it terminates at a patch panel.

Connections to “the outside world” are provided by a multiple core fibre optic (62.5/125 multi-mode) cables from the Museum Lodge, one of which enters the Physiology main building through the basement and then runs up to DP1, and the other which enters the OCGF basement and runs to OCGF DP1.

The basic cabling infrastructure is intended to be extremely flexible. The network technologies used and the network topology is largely determined by the way things are interconnected within two centralized distribution points and the equipment used there. Future upgrades or reorganizations can be achieved by making changes at the distribution points without rewiring the whole building.

As the network is currently configured there are four different network technologies in use, all of which are derivatives of Ethernet:

10BASE-T: 10Mbit/s Ethernet on category 5 UTP cable.
10BASE-F: 10Mbit/s Ethernet on fibre optic cable.
100BASE-TX: 100Mbit/s Ethernet on category 5 UTP cable.
100BASE-FX: 100Mbit/s Ethernet on fibre optic cable.

At the heart of each distribution point is an Ethernet switch (or stack of switches). Traffic between the four different regions of the main building is
carried by a series of 100BASE-TX links which connect the various distribution-
point switches into a tree structure rooted in DP1.

In DP 1 and 2, the switches are connected to stacks of Ethernet hubs, which
are connected in turn to the patch panels to provide the network service to the
network sockets throughout the building. The hub stacks are organized so as
to provide separate Ethernet segments for each floor in the building, and also
to provide separate segments for several research groups who have paid extra
for this privilege. Each port on the switches can provide either 10BASE-T or
100BASE-TX and automatically detects which speed is appropriate, so each of
the network segments connected to the switches can run at either 10Mbits/s or
100Mbits/s (many of the segments are currently 10Mbit/s, however several of
the groups that have a network segment of their own have opted to replace their
Ethernet hubs with 100Mbit/s switches).

In DP 3 and 4, end user connections are patched directly into the distribution
point switches. Similarly, a few key servers connect directly to the DP1 and 2
switches rather than sharing a network segment with other machines.

The two fibre based Ethernet technologies are used for connections to points
external to the main building. 100BASE-FX is used to connect the Departmental
network to the University backbone network (at the Departmental network
end this fibre connects to a module in the back of the DP1 switch). 10BASE-
FL is used to connect the Ethernet hub in the Old Observatory building to the
Departmental network (the 10BASE-FL feed for the observatory comes from a
module in the back of one of the “first floor” Ethernet hubs in DP1).

The switches bridge intelligently between their various interfaces – they mon-
itors the packets they receive on all their interfaces and learn the media access
control (MAC) addresses associated with the various devices on each network
segment. Network traffic which is addressed to a specific MAC address will only
be bridged into the appropriate network segment, whereas network broadcasts
(and traffic addressed to MAC addresses which have not yet been learnt) will
be bridged into all the network segments. Confining the traffic to only those
segments where it needs to go results in a system which has the throughput
advantages of a subnetted network but without introducing the administrative
complications which subnetting and routing would involve.

3.1.2 Protocols and Routing

Within the confines of the Department the network is designed to be protocol
neutral. Users may utilize any transport layer protocols which they require to
connect devices at an intra-Departmental level. However, most of the
devices on the network use the TCP/IP suite of protocols and any computers
which make use of Internet services or electronic mail will require these proto-
cols. Users of the network are therefore strongly encouraged to use TCP/IP in
preference to other network protocols where feasible.

The OUCS backbone router provides connectivity to external networks. It
can provide routing for two different network protocols:
IP is the transport protocol used on the Internet. TCP/IP traffic can be exchanged between the Department and other parts of the University, other UK institutions connected to JANET\(^1\) and any other network on the global Internet.

IPX is the transport protocol used primarily for Novell Netware file services. IPX traffic can be exchanged between the Department and any other network within the University. Although IPX routing facilities are available OUCS have expressed a wish to deprecate IPX in favour of IP where possible (the latest generation of backbone router handles IP routing in hardware, but uses a much more resource intensive software routing scheme for handling IPX).

The OUCS backbone router advertises itself as an IP and IPX router periodically using appropriate broadcasts.

Until recently routing for a third network protocol, AppleTalk, was available as an option. AppleTalk is used by the file and print sharing systems on Apple Macintosh computers. There is AppleTalk traffic on our local network, but we have never made use of the facility to have AppleTalk traffic routed between our network and other networks in the University. OUCS is attempting to discontinue the use of AppleTalk on the latest generation of the backbone (as with IPX, above) and the Department has indicated to OUCS that it will not require AppleTalk routing (though internal use of AppleTalk between Macintoshes and between the Departmental file server and Macintoshes continues).

OUCS sometimes provide units with bridging for network protocols which cannot be routed, such as NetBEUI, and for a variety of broadcast and multicast traffic. This is, again, a service that OUCS has offered historically, but which they now wish to deprecate. Such bridging is not enabled on the Physiology router — in our case only routed IP and IPX traffic is exchanged with the backbone.

The IP network currently has the following basic parameters:

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network base address</td>
<td>163.1.248.0</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.252.0</td>
</tr>
<tr>
<td>Default router</td>
<td>163.1.251.254</td>
</tr>
<tr>
<td>Broadcast address</td>
<td>163.1.251.255</td>
</tr>
</tbody>
</table>

This sets an upper limit on the number of Departmental hosts of 1021, the legal IP addresses ranging from 163.1.248.1 to 163.1.251.253.

Wherever possible IP hosts on the network should be dynamically configured. The Departmental file server (which is also the master information server for the network) can supply IP address information dynamically to hosts using the Reverse Address Resolution Protocol (RARP, RFC 903\(^2\)), the IP/UDP Bootstrap Protocol (BOOTP, RFC 951\(^3\)), or the Dynamic Host Configuration

\(^1\)http://www.ja.net/
\(^2\)http://mirror.ox.ac.uk/Mirrors/ftp.isi.edu/in-notes/rfc903.txt
\(^3\)http://mirror.ox.ac.uk/Mirrors/ftp.isi.edu/in-notes/rfc951.txt
Protocol (DHCP, RFC 2131\(^4\)). BOOTP and DHCP are preferred over RARP as they allow more information to be transferred to the client (in addition to its own IP address the client is informed which netmask, default router and DNS server to use).

The OUCS backbone router also acts as a seed router for the AppleTalk protocol — the Department has an allocated network number for AppleTalk networking and the seed router ensures that all the AppleTalk devices on the network use the correct network number when they start up. This ensures that should AppleTalk routing ever be enabled between the Department and another network within the University the AppleTalk devices in the Department will already be using the correct address.

3.2 The Departmental Servers

The Department currently employs two main servers, a matched pair of Sun Microsystems\(^5\) SunBlade 1000 workstations. At the time of writing these run the Solaris 9 operating system (Sun’s version of System V Release 4 UNIX). The two machines are known by the hostnames “Willis” (located in the Computing Office, Rm A37) and “Wren” (located in network distribution point 1, Rm A62). The two servers normally serve a variety of distinct roles:

**Willis** normally provides the file service, print spooling service, backup service, and is the master server for the various network information services.

**Wren** normally provides the email service and web services.

As described in section 3.7.2, some scenarios in the Department’s disaster recovery planning call for one of the machines to take on all of the services. To this end, all the data and configuration files which are unique to Willis are duplicated on Wren, and vice versa (with synchronisation of any changes taking place nightly).

The Department provides general purpose Unix shell services to members of the Department using several other Sun machines (retired, older generations of the Willis hardware): “Hooke” and “Hal” (both are Ultra 1/140 workstations, located in Rm A37).

3.3 Administrative Databases

Wherever possible computers attached to the Department’s network make use of the Network Information Service protocol (NIS, formerly known as “Yellow Pages”). Computing administers a NIS domain named “physiol”. Note that a NIS domain is a distinct and separate concept from the various other types

\(^4\)http://mirror.ox.ac.uk/Mirrors/ftp.isi.edu/in-notes/rfc2131.txt

\(^5\)http://www.sun.com/
of “domain” mentioned in this document, such as the DNS domains and NT domains.

Willis acts as the master NIS for the domain, where definitive versions of all the administrative files for the network are held. Several other Unix workstations within the Department (including Wren) act as secondary information servers; they hold copies of the master’s information and can maintain the information service if the master server is unavailable for some reason. The various servers are spread around the Department, both in terms of geography and network topology. This minimises the risk that multiple servers will become unavailable due to power trips or network problems.

The Department also operates some other information services to cater for situations where some of our client machines are not able to consult NIS databases. Examples include the DNS service and user authentication services for Windows 95 clients. These services are also normally provided by the Departmental file server and efforts are made to “tie” the non-NIS information services to the NIS databases which are already being maintained.

There are three directories on the NIS master which are of significance. The directory /home/willis/admin/nis contains the source files for the NIS maps discussed below (as well as the people and machines files), and the various scripts which are used to manipulate them. The directory /var/yp contains the live databases and the Makefile which is used to generate them from the source files. The directory /var/named contains the database files for the DNS server daemon (in.named).

There are fifteen main tables of information available from the Departmental NIS servers:

**passwd** holds all the usernames which are valid for use with Department’s computers, along with the associated encrypted password, UID, principle GID, full name, Unix home directory and preferred login shell. This database is made from the file passwd, which is in turn built from the file people.

**group** Groups are the normal Unix mechanism for allowing multiple users to share access to a resource without granting access to all users. For example, a file is owned by both the user who created them and the user’s group – read, write and execute privileges can be set for group members independently of the rest of the user population. All the group names valid for use with the Department’s computers are listed, along with the GID associated with the group and a list of all the usernames of users who are members of the group. This database is made from the file group.

**pc.home & pc.away** hold information which is used by the BWLOGIN program, run by client PCs using the Beame & Whiteside networking software. The pc.home map gives a mapping between usernames and the B&W share name which should be used for the user’s P: drive. It also states the default permission flags which should be given to files which the user creates using Beame & Whiteside. The pc.home database is made from the file pc.home, which is in turn built from the file people. The pc.away
The database is made from the file called `pc.away` and contains two entries which give the share names which should be used for the N: and O: drives. Placing this information in a NIS map makes it possible to change the location of these resources without distributing a new version of the login program.

**hosts** holds the mappings between IP addresses of the Department’s computers and their human readable hostnames. This database is made from the file `hosts`, which is in turn built from the file `machines`.

**ethers** holds the mappings between Media Access Control (MAC) addresses and hostnames (the name of the database is an anachronism – the MAC address of a network interface is sometimes called its “ethernet address” but this document avoids this usage, as not all the networking in the Department is Ethernet based). This database is built from the file `ethers` which is in turn built from the file `machines`.

**netgroup** holds lists of users and machines which are grouped together for network access reasons – for example the “physiolpc” netgroup which lists all the PCs which are allowed to use PC file services from the file server or the “stein_lab” group which lists all the users permitted to log in to the Stein group’s Unix machines.

**networks** gives the mappings between symbolic network names and their associated network numbers. This database is not much used – it contains an entry assigning a name to the Department’s network number. The database is built from the file `networks`.

**netmasks** gives the network masks used to implement IP subnetting. This contains an single entry to subnet 163.1 (the Universities class B network number) using a mask of 255.255.252.0 – this give the correct netmask for the Departmental network. It is potentially misleading about the rest of the 163.1 network, much of which isn’t subnetted with that netmask, but as systems on the Departmental network don’t maintain routing tables for any subnet outside of the Department this problem is not significant.

**services, rpc & protocols** hold mappings between symbolic names and numbers for various different parts of the networking protocols. The services map relates service names to TCP and UDP port numbers. The rpc map relates human readable names to RPC (Remote Procedure Call) program numbers. The protocols map relates networking protocol names to the protocol numbers used by the Unix kernel. These databases are built from the files `services`, `rpc` and `protocols`. The files were created by merging the standard `/etc/services`, `/etc/rpc` and `/etc/protocols` files from SunOS 4.1.3, SunOS 5.3, IRIX 5.2 and OSF/1 V3.0 and, in the case of `services`, adding a few extra entries to support programs in the `/usr/local` structure.

**publickey & netid** hold information used by the Secure RPC (Remote Procedure Call) system. The publickey map holds a Diffie-Hellman cryptographic key pair for each user registered for Secure RPC and is generated from the file `publickey`. The netid map holds information on the mappings between netnames and UID/GIDs or hostnames. There is no source
file for the netid map – it is an alternative representation of the information from the passwd and hosts files.

ypservers lists the hostnames of all the machines on the network which run NIS servers. This map is used when the master NIS server has updated a database to discover the names of all the slave servers to which updated copies of the databases should be sent (refer to the NIS command ypupdate for more details). There is no source file for this map, it was generated by the ypinit command when the master NIS server was set up.

The actual number of NIS maps is larger because some of the databases are indexed several different ways. For example, there is a passwd map sorted by username and a passwd map sorted by UID but the information held in the two maps is the same.

All the NIS maps described are databases which are part of a normal Sun NIS installation – with the exception of the “pc.home” and “pc.away” maps which are a local additions. The other major local adaption of the system is the idea of combining data from several of the source files into a single file. These combined files don’t correspond directly to NIS maps – the NIS Makefile has been modified so that just as the map depends on its source file the source file depends on the combined database file. For maps which are managed in this way the database administrator does not make updates to the source file directly – updates are made to the combined database file which is then processed to yield the expected source file before the normal makedbm operation to make the NIS map. The combined database files are held in /home/willis/admin/nis along with the NIS map source files.

3.3.1 The people File

The people file contains a union of several different sets of information, all relating to users:

- The “static” parts of the passwd file (the username, UID, login GID, full name and home directory).
- The pc.home information – resource to be mounted as P: and default file creation mode to be set by BWLOGIN.
- The user’s /home/willis and /home/mail disk quotas. If these fields are empty then the current system defaults are used. A zero indicates that no quota limits are applied to the individual. A positive number is a non-default quota allocation, expressed in kilobytes. The numbers given are normally “soft limits”. In the (unusual) case were a non-default hard limit is also specified the two numbers are listed seperated by a slash: “soft-limit/hard-limit”.
- A “status” field — this is an administrative tool which allows accounts to be switched on and off. There are five different status categories which the system recognises. ACTIVE: an active user who has an encrypted
password and a valid shell in the `passwd` file. INACTIVE: an inactivated user who has an encrypted password but no shell — the account has been turned off for some reason. NEW: an account that has been created but is not in use yet — the user needs to see the Computing staff to set a password. OLD: old user who can no longer log in. NP: no password — a pseudo user with no login associated with it (eg. the “dump” user for backups).

- A “comment” field — this allows the addition of some descriptive text giving additional identification to the user. Sometimes a job title is given, or sometimes the initials of the research group leader with whom the user works or, in the case of a non-member of the Department some indication of who the user collaborates with in the Department. This information is intended to assist in the maintenance of accounts.

There are three programs which are used to process the `people` file:

`mkpasswd.pl` is a Perl script which reads the `people` file and outputs both the NIS `passwd` file and a new `/etc/passwd` file for the file server. This program is triggered by the NIS Makefile when the `people` file is newer than the `passwd` file.

`mkpchome.sh` is a Bourne Shell script which reads the `people` file and outputs the `pc.home` file. This program is triggered by the NIS Makefile when the `people` file is newer than the `pc.home` file.

`mkquota.pl` is a Perl script which reads the `people` file and updates the `/home/willis` disk quotas (ideally this functionality would actually belong in `mkpasswd.pl` but it slowed that program down so much that it was decided to separate the quota functions out into a distinct program which could be triggered by `cron` once a day).

### 3.3.2 Passwords

The scheme used for changing passwords is rather different from that which is conventionally used in a NIS based Unix environment. Normally the NIS master server runs a daemon called `yppasswd` and users can run the program `yppasswd` on any of the NIS clients to change their password. `yppasswd` passes the change request to the `yp passwd` daemon on the server. If the change is accepted the NIS passwd map is updated and pushed to all the slave servers. There are several reasons why this arrangement doesn’t fit well with our requirements:

- These days most of our users are not Unix users. It makes sense to standardize on a single set of instructions for the changing of passwords which can be given to all members of the Department.
- The liberal use of NIS within the Department’s network and between the main server and various other trusted hosts elsewhere in Oxford means that our passwd map gets quite widely distributed. It is therefore very
desirable that the encrypted passwords stored in this map are not vulnerable to “dictionary attack”. We therefore want to replace the normal password change program with one which implements extensive checks on the suitability of passwords before allowing their use.

- Proper provision of SMB file services for Windows NT machines require the use of an authentication mechanism which the file server cannot implement using the encrypted password field of a Unix passwd file. We therefore need to store SMB password details separately from Unix password details. The way we have chosen to keep the two sets of password details synchronised for any given user is to have a custom password change program which updates both sets of records.

The network NIS master server does not run yppasswdd and any attempt to run yppasswd on a Unix client should fail. Users are required to make an SSH connection to “willis.physiol.ox.ac.uk” and log in with their normal username and password. Normal users don’t get a shell on Willis — they see a small menu which allows them to take a couple of minor administrative actions, including changing their password. The menu shell invokes a passwd program in the directory /home/willis/admin/bin, which is a binary wrapper around the Perl script passwd.pl in the same directory. This script implements the functionality of the standard Unix passwd program, with the following additions:

- It checks the acceptability of the password, both by applying a few simple tests (is it long enough?, does it contain an obvious date or the user’s own name?, etc) and then by trying to look up the word in a password cracking word list. This second stage should eliminate most words, names and obvious combinations and permutations of such words and names. The word list was compiled by combining dictionaries for most major languages and includes lists of Latin, technical, scientific and medical terms as well.

- The password is fed through the standard Unix encryption mechanism and the resulting encrypted password string is inserted into the source file for the NIS passwd map.

- The password and the username are passed to the smbpasswd program. This calculates the NT and LanManager hash values for the password and inserts them into the Samba password file (/etc/private/smbpasswd).

- A NIS make process is spawned, so that the NIS passwd map will be updated from the revised source file and pushed to the slave servers.

3.3.3 The machines File

The machines file lists collects together all available relevant information about all the networked devices on the Department’s network. Lines in the file have the following form:

08:00:20:0b:25:95 163.1.248.21 motor.physiol motor # Sun Sparc II - Rm 331 - JFS

28
The elements on a line are white space separated and are, reading left to right:

- Media access control (MAC) address.
- IP address.
- Canonical hostname. This must have the form “hostname.physiol”.
- Hostname aliases. There must be at least one alias, of the form “hostname” (i.e. the canonical name less the “.physiol” qualification) and this must be the first alias defined. Any number of further aliases can be defined as required, although they must be unqualified.
- Comments, prefixed with a # character to separate them from the aliases.

Conventionally the type of computer, its physical location and the research group which owns it are recorded here.

This is effectively an adaption of the format of the hosts file, with the MAC address prefixing each line.

The machines file is processed by the Perl script mkhosts.pl. This generates a hosts file, a special version of the hosts file to be used by the DNS (dnshosts), an ethers file and /etc/dhcpd.conf – the configuration file for the daemon on the file server which services BOOTP and DHCP requests.

The special MAC address of “00:00:00:00:00:00” is used to indicate hosts for which the MAC address is not currently known. Such lines do not generate corresponding output in the ethers file or the DHCPd configuration file.

The dnshosts file is the same as the main hosts file, except that the canonical hostname has been removed. The mkhosts.pl script now invokes the Perl script h2n to convert the dnshosts file into a set of DNS database files. Finally, the mkhosts.pl sends a signals to the DNS and DHCP server daemons to instruct them to re-load their database files.

3.3.4 The Domain Name System and the Internet

Information about the network addresses of computers and their hostnames is available from two different sources:

- the Departmental NIS hosts map, which contains name and IP address information about the machines on the local network.
- the Internet Domain Name System (DNS), which is a distributed database which can provide information about all computers connected to the global Internet (this includes the networked machines in the Department). Local machines require information about remote machines from the DNS whenever they need to interact with hosts outside of the Department. Remote machines often require the DNS to provide information about machines within the Department (many remote sites need to be able to convert our
IP addresses into hostnames in order to implement access controls, for example). A machine which has an NIS hostname of “name.physiol” has a corresponding name in the DNS, “name.physiol.ox.ac.uk”. Note that a DNS domain is a distinct and separate concept from the various other types of “domain” mentioned in this document, such as the NIS domains and NT domains.

Additionally, the NIS servers perform DNS lookups on any request which cannot be satisfied from the NIS hosts map. This makes the NIS hosts map appear to be definitive for the whole Internet from the perspective of the systems which rely on NIS. This setup has one unfortunate side effect. When an IP address is converted into a hostname the DNS returns a fully qualified domain name (eg “ermine.ox.ac.uk”). A similar reverse lookup which is satisfied by information from our NIS hosts map returns a partially qualified name, in the form used by the University hosts file (eg. “willis.physiol”). This is untidy and can be confusing at times. Names of machines within the department do not appear correctly embedded in the name space used for all other machines in the world. So, for example, a rule designed to limit access to a particular service to machines within Oxford must be formulated along the lines of “if the name of the requesting machine ends in .ox.ac.uk or if the name of the requesting machine ends in .physiol then ...”. In some ways it would be desirable to re-arrange the NIS hosts map such that the proper name of each machine in the Department was given in its fully qualified DNS form. There are problems with undertaking this change, however, not least of which are the number configuration and access control files on the various Unix systems which are written on the basis of the current arrangements.

Others client machines (such as the PCs and Macintoshes) are only able to consult the DNS for host information. OUCS are responsible for maintaining the official Oxford DNS databases and perform updates only daily. This means that changes to the official DNS databases often lag behind changes made to the local network, which can be inconvenient. We therefore operate our own DNS service for the benefit of clients on the local network, in parallel with the official DNS service provided by OUCS. All DNS lookup requests by clients on the local network are sent first to Willis. If the request relates to the local network then Willis responds with information from our own databases (as described above, the DNS database on Willis is derived from the machines file and is reloaded into the name server daemon every time an update to the NIS hosts database takes place). If the request relates to an external machine then Willis forwards the request to the appropriate remote name server and relays the response that it receives back to the client (information that is obtained in this fashion is cached on Willis so that subsequent requests for the same information can be provided more rapidly and less network traffic is generated). Thus all machines within the Department see address changes and additions on the local network immediately, whether they use NIS or DNS for host name resolution.

As far as the rest of the Internet is concerned authoritative data concerning hostname and Internet addresses is held by OUCS. Therefore, whenever a permanent change is made to our hosts file then that change must be communicated to the appropriate authorities at OUCS (this is normally done via a
password protected Web interface\(^6\)).

Computing run a *cron* task once a day which compiles a list of differences between the current hosts file and the corresponding information in the University wide hosts file.

### 3.4 Network File Services

There are two main filesystems which the Department makes available to client machines on the network:

- `/home/willis`, which holds the users' personal files and the shared file areas. Each user has a subdirectory named after them, so that a user with username “abc” owns a directory called `/home/willis/abc`.
- `/export`, which holds shared software.

Each of these filesystems is protected by disk mirroring and daily backups.

#### 3.4.1 NFS file services

Sun’s NFS (Network File System) protocol is the native file sharing mechanism provided by the file server. It is used to provide file services for Unix based client systems and those using the MS-DOS operating system.

The NFS sharing setup on the server is controlled by the configuration file `/etc/dfs/dfstab` (see the `dfstab` manual page for details). The various clients are categorised into groups according to type when they are connected to the network and access to the various filesystems NFS exported by the file server is controlled using a series of NIS netgroups.

#### 3.4.2 Unix Clients

Unix clients use NFS file services from the file server. NFS client software is normally available as a standard part of the operating system on Unix clients.

Each Unix client has entries in its `/etc/fstab` or `/etc/vfstab` file to mount the following NFS resources at boot time:

- *willis*: `/home/willis` as `/home/willis`. Each user can then access their personal file area and any of the shared file areas from the file server. The personal file area mounted from the Departmental server may or may not be utilized as a user’s “home directory” on client machine — they might choose to use a file storage area on the client machine or one provided by an NFS file server within their research group.

\(^6\)http://networks.oucs.ox.ac.uk/cgi-bin/safeperl/networks/ipnos
• willis:/usr/local as /usr/local. This makes the shared software available to users of the machine.

Under the /usr/local filesystem there is a conventional tree layout of Unix software:

bin executable programs for end users.

include C and C++ header files for the libraries in lib.

info GNU documentation files for use with Emacs info mode.

lib library archives, shared object files and configuration files which are architecture specific.

man on-line manual pages.

sbin executable programs used by the system and the system administrators.

share miscellaneous files which are portable between different architectures.

Some parts of the tree (bin, sbin, lib and include) are specific to the "architecture" (processor type and the operating system version) of the client machine. When /usr/local is first mounted these subdirectories are those which are suitable for file server's own architecture. Client machines which have the same architecture as the file server can therefore use the mounted /usr/local tree directly. To cater for client machines with architectures which differ from that of the file server a variety of alternative architecture dependent directories are stored under the directory /usr/local/arch. There is a subdirectory of arch named after each supported client architecture. Each such subdirectory contains bin, sbin, lib and include directories for the architecture concerned.

Clients which need to make use of these alternative architecture directories perform several NFS mounts to overlay the appropriate architecture dependent directories on top of the basic /usr/local structure. Typically the /etc/fstab file on the client system will contain entries of the following form, to make the appropriate NFS mounts at boot time:

willis:/usr/local/usr/local nfs rw,bg
willis:/usr/local/arch/arch-name/bin /usr/local/bin nfs rw,kg
willis:/usr/local/arch/arch-name/include /usr/local/include nfs rw,kg
willis:/usr/local/arch/arch-name/lib /usr/local/lib nfs rw,kg
willis:/usr/local/arch/arch-name/sbin /usr/local/sbin nfs rw,kg

A considerable saving in disk space can be made by sharing those parts of the directory tree which are not architecture independent. At the time of writing, three different client architectures are supported:

• SPARC based Sun machines running the Solaris 9 operating system, or later version (this is the file server's own architecture the arch subdirectory for it isn’t used for overmounting — the directory exists to hold a few files however and is named sparc-sunos5).
- MIPS based Silicon Graphics machines running the IRIX 6.5 operating system, or later version (arch subdirectory name mips-irix6).

- Intel based PCs running Linux (arch subdirectory name ix86-linux). Binaries are generally compiled to be runnable on Red Hat Linux 6.1, or later version, though there are some recent builds that require Red Hat 7.1.

In principle we aim to keep the various various architectures in step — installing the same software on all supported platforms. This allows the Department to offer a relatively uniform working environment across all the various supported platforms.

There is also an arch subdirectory for SPARC based machines running Solaris 2.6 (named sparc-sunos5.6). This is retained for the benefit of a handful of Sun machines that can’t run Solaris 9. This architecture is only semi-supported — the intention is that no new software will be built for this architecture and that the only updates that will be applied will be those required to address security problems.

**Login Under Unix**

User’s home directories should contain a .profile file. This file is read as a series of commands whenever a Bourne Shell (/bin/sh) is started as the user’s login shell.

The default .profile file starts by reading commands from a centralized profile, /usr/local/etc/Profile.generic. This, in turn, determines the architecture of the machine (using the uname command) and reads commands from a profile which Computing has prepared for that architecture. This sets up the user’s environment such that it is ready to make use of both the facilities of the local machine and the various software installed in /usr/local. Environment variables such as PATH, MANPATH, LD_LIBRARY_PATH, etc are initialized so that the /usr/local software can be run and documentation read by simply referring to the programs by name. Control then returns to .profile — the user can change the subsequent parts of the file in order to create a customized environment.

One of the environmental variables which the user can modify to set their preferences is SHELL. This specifies the shell that they actually prefer to type commands at (the Bourne Shell is fine for scripting but is a poor interactive environment). The last thing that the .profile does is to exec the preferred shell, replacing itself with a running copy of that shell. The shell that is started in this way inherits its environment from the login shell.

Unix users may have any shell they wish listed in the NIS passwd map but it is recommended that they use the Bourne Shell, in order to take advantage of this mechanism.

The .profile file isn’t processed when logging in to a workstation running the XDM graphical login manager. Conventionally, XDM runs a program called
.xsessions in the user’s home directory after logging a user in. The default .xsessions file we provide is a Bourne Shell script which reads commands from the user’s .profile (after first setting a special flag in the environment to prevent the final exec operation described above) and then reads commands from the user’s .xinitrc file, which contains a list of all X clients that the user wishes to run at login. This approach should ensure that the environment that the user sees when logged in on a graphical display should be the same as that which they get when logging in by other means.

The graphical login arrangements under IRIX on Silicon Graphics machines are slightly different. The IRIX login manager spawns a login shell owned by the user, gets it to print out its environment, captures this and then applied that environment to the processes it creates for the user. The overall effect is the same.

3.4.3 DOS Clients

Note: This section applies to all client machines which use MS-DOS based network drivers including machines which run the Windows 3.1 graphical user interface.

MS-DOS clients use NFS file services from the file server. The clients run the Beame & Whiteside TCP/IP stack and NFS client software, which is available to the Department at no cost through a University wide site licence. Note that users should not obtain media for Beame & Whiteside directly from the OUCS shop or attempt to install it themselves. The Department has its own customised version of the software and its installation routine which is easier to use and takes account of the way that local services are configured.

The file server runs a daemon process called bwnfsd which provides authentication and network print services to Beame & Whiteside clients.

A locally written program called BWLOGIN is provided with the customised version of the Beame & Whiteside software. This prompts a user for a username and password and then uses that information to mount network file services onto the PC.

BWLOGIN consults the NIS map “pc.home” to find the Beame & Whiteside share name for the user’s home directory and their preferred Unix permission mode for file creation. The information in the “pc.home” map is derived from the people file. BWLOGIN runs net link to map the specified share name to the drive letter p: and then runs net prot to set the default permission for the drive. The “pc.home” information was originally stored in the NIS because it was thought to be desirable to be able to mount an arbitrary home directory resource. In practice all users are now strongly encouraged to always use their personal directory on the file server for p: and use another drive letter (q: is common) for any other personal NFS storage to which they may have access.

BWLOGIN consults another NIS map, “pc.away”, to obtain two further Beame & Whiteside share names. BWLOGIN runs net link to map the specified share names to the drive letters n: and o:. These drives are used to provide the
shared software for PC clients. The “pc.away” information is stored in the NIS because of the extra flexibility this gives (changes can be made to the provision of the n: and o: services without distributing a new version of the BWLOGIN program, for example).

If a batch file p:\pcconfig\bwnfs\drives.bat exists then BWLOGIN runs it. As p: has just been linked from the user’s own home directory this gives the user an opportunity to list any net link and net prot commands which they want run every time they log in. This facility can be used to provide a personal setup of network drives and printers.

If a batch file c:\bwnfs\drives.bat exists then BWLOGIN runs this as well. This gives us an opportunity to list any net link and net prot commands which are to be run every time any user logs into a particular machine. This facility can be used to provide a machine specific setup of network drives and printers.

BWLOGIN runs a virus check of the client machine’s RAM, master boot record and a few key files on the hard disk which are primary candidates for virus infection, warning the user if anything amiss is discovered.

Finally, BWLOGIN checks for the existence of a text file n:\motd.txt and displays it to the user if it exists. This provides a “message of the day” facility for PC users similar to that which is provided the /etc/motd login banner which is seen by Unix users.

3.4.4 Windows Clients

Note: This section only applies to client machines running 32-bit Windows operating systems, such as Windows 95, Windows 98 or Windows NT. For the purposes of file sharing, machines which run Windows 3.1 are DOS Clients. Wherever reference is made to “Windows 95” the comments invariably apply to Windows 98 as well (unless otherwise noted).

Windows 95 and Windows NT based clients use SMB (“Server Message Block”, also known as “LanManager” or “Microsoft Networking”) file services from the file server. This allows us to make use of the native file sharing client software which is included with these operating systems rather than adding a third party product, as we do in the case of DOS clients. SMB can be carried over a variety of different network transport protocols — the Department only supports the use of the TCP/IP protocol for this purpose, however.

SMB file services are provided on the file server using a free software package called “Samba”. The main components of the Samba suite are a pair of daemons called nmbd (which provides a NetBIOS name service, allowing SMB clients to find the server) and smbd (which services the actual SMB requests). These daemons are started on demand by instd — normally there is a single nmbd process running and a separate smbd process for each client system connected.

The Samba daemons are configured using the file /etc/smb.conf (see the smb.conf manual page for details). The smb.conf file controls various system
parameters and the mapping between SMB share names and the corresponding directories on the file server, in addition to specifying access control based on NIS netgroups (in a similar fashion to the way that the dfstab file governs access for NFS clients). The smb.conf file specifies shares for the /export/pc-public and /export/pc-club directories used to provide shared software for PC clients, the various shared file areas and networked printers. Shares for user home directories are created using a special Samba feature — accessing \willis\homes gives the home directory belonging to the user making the connection.

Proper provision of SMB file services to newer Windows variants requires that the server is able to authenticate clients using an encrypted challenge/response protocol. There is a less sophisticated authentication protocol (which involves sending clear text usernames and passwords over the network) but in the absence of support for the encrypted authentication protocol:

- All Windows NT systems will refuse to connect to a server without first asking the user to retype their password (the intention here is to make clear to the user that their password is about to be sent over the network to a server and give them a chance to decline to reveal the password).

- Systems running Windows NT 4.0sp3 (and later versions) or Windows 98 (and later versions) take an even harder line. They refuse to connect to file servers at all, unless they support the encrypted authentication protocol.

- Roving profiles for Windows NT systems do not work.

To be able to support encrypted authentication the server must have at its disposal hash functions calculated from the clear text of each user’s password, as described in the section on the changing of passwords (see §3.3.2).

**Login Under Windows 95 / 98 / ME**

Note that, for convenience, we will refer to the original Windows 95 release and its direct successors (such as Windows 98, Windows 98SE and Windows ME) collectively as “Windows 95”, except were the distinction between versions is significant.

Windows 95 clients are configured with the option “Log on to Windows NT Domain”, and have their domain set to “Physiology”. The Samba suite doesn’t actually provide proper Windows NT Domain capabilities. However, Windows 95 doesn’t actually use the full NT Domain protocol to talk to a Domain controller. It simply attempts to determine which machine is acting as browse master for the workgroup “Physiology” and then tries to make an SMB connection to a share called netlogon on that machine (which will be the Departmenal file server).

Assuming the user has provided a correct username/password combination they will now have a temporary mapping to the \willis\netlogon share and an SMB connection to the file server which will last for the duration of their login session. The client runs a batch file on the netlogon share called win95.bat.
(this filename is provided by the Samba server, and is generated automatically based on the client architecture detected by the Samba program). This batch file duplicates the functionality of BWLOGIN in the MS-DOS environment — it maps the p:, n: and o: drives, it runs personal drive mapping batch file from p:\pcconfig\smb\drives.bat, runs a machine specific drive mapping batch file from c:\smb\drives.bat and runs a Windows program which displays the n:\motd.txt file if one exists.

Note that the drives.bat files used by MS-DOS and 32-bit Windows are in different locations. This is necessary, as the syntax of the drive mapping commands and the format of the sharenames used in the two systems are different. Unfortunately, for a user who uses both DOS and Windows systems, this means that they have two separate sets of drive mapping preferences to maintain.

The Windows 95 machine also automatically initializes the Windows registry hive HKEY_CURRENT_USER from a file user.dat which is loaded from the user’s home directory on the server. When the user logs out the same registry hive is saved back to the user.dat file. This ensures that any personal preferences stored in the Windows registry “rove” around the network, following the user wherever they log in.

**Login Under Windows NT / 2000 / XP**

Note that, for convenience, we will refer to the original Windows NT version 4 and its direct successors (such as Windows 2000 and Windows XP) collectively as “Windows NT” or just “NT”, except were the distinction between versions is significant.

Login under Windows NT is a different problem to login under other PC based operating systems, in that the Windows NT operating system itself properly supports separate users, with usernames, passwords and different privileges associated with each account. There are two different ways in which NT user authentication system can work:

- The “Workgroup” model, where each NT system on the network uses a local database of users. The systems are grouped into Workgroups, but this is simply a convenience so that associated systems are shown together in graphical displays of the network, etc. There is no security associated with the Workgroup as such.

- The “Domain” model, where one or more NT Server systems on the network are nominated as “Domain Controllers”. One server will be the “Primary Domain Controller” (PDC) and any subsequent controllers set up in the same domain become “Backup Domain Controllers” (BDCs), which mirror the information on the PDC. Each NT system which participates in a domain uses information from the domain controllers to authenticate users. Note that an NT domain is a distinct and separate concept from the various other types of “domain” mentioned in this document, such as the NIS domains and DNS domains.
The Samba software now emulates enough of a Windows NT 4.0 Domain Controller to allow it to act as a PDC for NT 4.0, Windows 2000 and Windows XP clients, and the Departmental file server acts as a PDC for the NT domain “PHYSIOLOGY”.

When NT clients are attached to the network they are “joined” to the PHYSIOLOGY domain and from then on it is possible to log in to the client using a username/password combination from the Departmental user list (in addition to any local accounts which are listed in the clients’ own security database).

Following a successful domain login, NT clients make a temporary connection to the \willis\netlogon share and run a logon batch file in a fashion similar to that described for Windows 95 clients. In this case the batch file is WinNT.bat for NT 4.0 clients and Win2K.bat for Windows 2000 or Windows XP clients.

The user’s personal roving profile is loaded from the directory ntprofile, in their home directory.

3.4.5 Shared Software For PC Clients

The file area on the Departmental file server dedicated to storing shared PC applications consists of two subdirectories of the filesystem which is mounted as /export.

The directory /export/pc-public contains freely distributable programs and utilities for which the University has an unrestricted site licence. The various types of PC client connect to this directory as the drive n: when the user logs in.

The directory /export/pc-club contains commercial software for which the Department has bought licences, and may in future wish to charge for access to. The various types of PC client connect to this directory as the drive o: when the user logs in.

Both of the directories are structured in a similar way. They contain a series of subdirectories, each of which contains the files of a particular software package. The pc-public directory also contains two subdirectories bin and bat (a client PC sees these as n:\bin and n:\bat respectively). The bin subdirectory contains small, stand alone executable programs and utilities which do not require their own subdirectory structure. The bat subdirectory contains various MS-DOS batch files, including a number of scripts which act as a wrapper for DOS programs stored elsewhere in the pc-public and pc-club structures — these wrappers allow client computers to be set up with only n:\bin and n:\bat in their PATH environment variable, rather than PATH having to be altered to reference all the possible applications which the client might want to access. These scripts can also initialize the environment and any configuration files which the program might require before calling the application proper.

Each package of Windows software stored on n: or o: normally has a setup script which prepares a user’s PC for using the software and adds the program items to the appropriate program groups on the user’s desktop. These scripts
are stored on the n: drive using names of the form n:\setxxx.exe (where xxx is some abbreviation of the name of the package). These scripts are written using a Windows scripting tool called WISE. Documentation concerning the packages available and giving setup instructions for each is available from the computing section of the Departmental Web pages.

Wherever possible the software is set up to place files controlling configuration, user preferences, etc on the network p: drive. This, in combination with the use of roving user profiles for Win32 applications which use the Windows registry, means that software provided by the network:

- is configurable on a per-user basis, without the preferences of various users of a package interfering with each other.
- maintains a consistent configuration for a given user, independent of the machine at which the user is working.

It is worth noting that, while these are worthy objectives, the underlying assumptions of the PC culture mean that it is often difficult (and in some cases impossible) to get DOS and Windows software to work properly this way.

3.4.6 Macintosh Clients

Apple Macintoshes use the AppleTalk Filing Protocol (AFP) over the AppleTalk networking protocol to communicate with the file server. The file server uses the Columbia AppleTalk Package, aka “CAP”, to enable it to support these protocols. The CAP daemons are started on the file server by the boot script /etc/init.d/S99local-cap.

Services are accessed using the normal tools provided by the Macintosh operating system — the Chooser is selected from the Apple menu, the user clicks “AppleShare” and then selects “Willis” from the resulting list of file servers.

Two network volumes are normally provided by the file server to Apple clients. The user’s home directory on the file server is available as the volume “Home Directory”. An area of the file server containing some freely available Macintosh software is available as the volume “Network Resources”.

The “Network Resources” volume corresponds to a subdirectory of the file-server’s /export filesystem called mac-public. This contains Macintosh software and utilities which are freely distributable or for which the University has an unrestricted site licence.

Unfortunately it has been found that when applications program are run directly from the Network Resources volume only one copy of the application at a time can run. It is therefore necessary for the applications to be copied from the network volume to local disk of each Macintosh. For Macintosh applications then, the file server acts as a superior distribution mechanism.

---

7 http://www.physiol.ox.ac.uk/Computing/
rather than as the transparent file service which was originally intended. This is unfortunate but appears to be intrinsic to the way Macintosh filesystems and applications work.

The bulk of the software made available is in the subfolder “Network Applications”. The intention is that this folder can be dragged as is to the hard disk finder window on any Mac to install the software locally. There are a few programs which cannot be installed in this fashion (such as the MacSPIRS ERL client, which writes various files to the System folder during installation) and the installation materials for these programs are made available in separate directories so that they can be installed over the network.

There is an additional directory, /export/mac-club, which is not currently made available to any client. This directory has been set aside for holding network licenced Macintosh software, if such a service is ever offered. The directory is currently empty.

3.4.7 Other Clients

In addition to the main classes of client machine there is a lower level of support for any “non-standard” clients which are able to make use of the services offered. While the Department cannot devote resources or time in supporting other options any client device which can make use of the provided NFS, SMB or AppleTalk file service may do so, subject to Computing’s approval. As with other aspects of the Departmental service, anyone using “unusual” equipment or systems in conjunction with the file server must keep the Computing staff informed.

Note: There are security implications involved in providing NFS service to an insecure system and this will only be permitted where Computing is satisfied that the client implements a reasonable security model.

3.4.8 The /home/willis Filesystem

The Quota System

Storage space on the /home/willis and /home/mail filesystems is a limited resource. With a large user community to serve and a finite amount of disk space available we need to apply restrictions to ensure a reasonably fair sharing of resources, discourage wasteful use and ensure that the filesystems do not fill up (if the filesystems ever become entirely full then writes to user directories will start to fail — quite apart from the inconvenience that this would cause users, much of the software which uses home directories to store configuration information would start to malfunction).

A two stage system of “quotas” is operated. This uses facilities which are provided as part of the server’s operating system. Each user has two limitations applied to them, known as the “soft quota” and the “hard quota”. The hard quota is the amount of disk usage that the user may not exceed at any time.
The soft quota is a lower limit, which the user is allowed to exceed for limited periods of time. The current defaults used on our system are:

- **Soft quota:** 100Mbytes
- **Hard quota:** 750Mbytes
- **Soft time limit:** 7 days

The soft and hard quota figures can be varied on a per-user basis. The time limit is a global system parameter. The difference between the hard and the soft quotas effectively forms a disk space “overdraft” facility for the users, allowing them to temporarily borrow reasonably sized chunks of network storage. This is useful in terms of moving data from one client machine to another, preparing data for use with the Departmental CD mastering service, etc.

The soft quota is intended to be negotiable and flexible (it is, in a sense, our opening bid in the inevitable haggle with users over disk usage). Requests for moderate increases in the soft quota are normally granted without question. However it is Departmental policy that large scale storage is expected to be provided by the user’s research group and the quotas agreed with users tend to reflect this, preventing the long term storage of more than a few hundreds of megabytes.

The hard quota is less frequently re-negotiated or relaxed, although (free space permitting) it may be increased or entirely removed for strictly limited periods (hours, or a day or so at most) in order to allow a user to accomplish something such as a file transfer which cannot easily be handled any other way.

A description of the quota system from a user perspective is given in the document “Understanding Your Quota”\(^9\).

The quota system can be controlled using various Solaris utilities (see the manual pages for `quota`, `edquota` and `quotaon` for example) but most day to day administration of quotas on Willis is performed by making changes to the relevant field in a user’s entry in the `people` file. A `cron` task run nightly uses the information stored there to update all the `/home/willis` quotas. *Note in particular* that if `edquota` alone is used to modify a user’s quota then the `cron` job will undo these changes. The only circumstances where one might want to run `edquota` manually are to grant a soft quota increase in a situation where the soft limit expiry time falls within the current working day (in this case one has to use `edquota` manually, to head off the impending expiry, and change the `people` file, to make the change permanent) or if one wishes to make a strictly time limited change to a quota (a change can be made with `edquota` alone and the change will be effective until midnight, when it will be reversed automatically without further manual intervention — this approach can be used to relax the hard quota for a few hours or to reset the soft quota timer without causing a permanent increase in the soft quota itself).

\(^9\)http://www.physiol.ox.ac.uk/Computing/Understanding_Your_Quota.html
File Sharing Mechanisms

The file sharing discussed in section 2.3.2 can be implemented using the Unix group mechanisms provided by the operating system on the file server.

Where a group of people want to share access to a collection of and each person is to have unrestricted access (i.e. any member of the group can create, read, write and delete any file in the shared collection) this is implemented using subdirectories of `/home/willis/secretarial`, with one subdirectory per group of users. The name `secretarial` results because the initial sharing use which was considered was collections of files shared between secretarial staff and collections shared between between academics and their secretaries. In retrospect the mechanism which has been established has a wider applicability and a name like `/home/willis/shared` would be more appropriate (a symbolic link, named “shared” and pointing to “secretarial” is now provided in the `/home/willis` filesystem — allowing either name to be used).

The files and directories under a given group subdirectory are arranged to be publically readable and writable (Unix permission mode 777). Access to the contents of each group subdirectory is governed by the Unix permission mode of the subdirectory — typically this is mode 770, allowing full access to the directory owner, full access to the group owning the directory and no access to other users. The fact that each directory has both an owner and a group associated with it allows us to economise on the number of Unix groups we need to create and manage. For example, in order to allow a number of different users to each have a personal collection of files which they share with the secretarial staff we need only define a group which contains all the secretaries. Each collection of files is then put in its own subdirectory which is owned by the user in question and has its group ownership assigned to the secretaries. Without this sort of mechanism we would have to maintain a large number of overlapping groups (“User A plus all the secretaries”, “User B plus all the secretaries”, etc. and any changes to the list of secretaries would need to be made in many groups rather than one).

The way that users see the shared area varies depending on the type of client that they are using:

- Unix users work with files and directories under the appropriate subdirectory of `/home/willis/secretarial`. The user needs to use the `umask` and/or `chmod` commands appropriately to ensure that any files and directories that they create have the appropriate permissions.
- DOS users map `\willis\home\willis\secretarial` to the drive letter `s:`. The conventional place to do this is in the user’s personal `drives.bat` file so that the mapping is done automatically at login. A Beame and Whiteside `net prot` command should also be included in the `drives.bat` file, to set the file creation mode appropriately.
- Windows 95/NT users map the share `\willis\secfiles` to the drive letter `s:`. The conventional place to do this is in the user’s personal `drives.bat` file so that the mapping is done automatically at login. In this
3.5 Electronic Mail

3.5.1 Routing, Transport and Delivery

Figure 3.2 shows some of the computers which make up the e-mail system and illustrates how mail flows between them. This figure is intended to be illustrative of a few key features of the system and doesn’t feature all the computers or possible protocol interconnections — for example the OUCS system “Herald” holds mail for a number of Physiology users.

There are three basic rôles which a computer involved in the mail system
can have:

- A **Mail Router** knows, based on the envelope address, where mail should be sent.
- A **Mail Hub** takes delivery of a message, recognises it as being addressed to a local user and stores it on behalf of the user.
- A **Mail Client** provides the user interface. It communicates with a Mail Hub to retrieve the user’s messages, allows the user to read them in a convenient format and offers facilities such as message filing, sorting and composition.

Sometimes a single system takes on several of these roles; for example, using the above terminology a traditional Unix multi-user time-share system such as the OUCS machine “Ermine” operates as both a hub and a client.

In the Departmental mail scheme the OUCS computer “Oxmail” is the mail router. In fact there are a number of OUCS computers that perform mail routing and header re-writing. This collection of computers handles more load than could be manage by a single computer and also provides multiple redundancy, so that the University mail system does not fail if a single computer suffers a fault. Using mail exchanger (MX) records in the DNS the collection of mail routing computers are made to appear to the rest of the University and the Internet as a single computer. For convenience Oxmail is referred to throughout this document as though it were a single system.

It is an intentional design feature of the system that there can be an arbitrary number of mail hubs. The Department runs a mail hub (a Sun system of identical specification to the main file server, called “Wren”, with a role-specific alias “mail.physiol.ox.ac.uk”) to which users’ mail is sent by default, but any user can ask OUCS (directly, or through Computing) to have their mail routed for delivery to any suitable computer system in the University.

The mail routing tables on Oxmail are the only definitive source of information concerning the preferred mail hub of each user in the Department. This is why, as a matter of policy, all e-mail intended for a physiol.ox.ac.uk address (even person-to-person within the Department) must be routed via Oxmail.

The personal computer or workstation on the user’s desk (or in some shared area such the Graduate Students Computer Room) normally acts as the mail client.

In order to understand the mail routing scheme used by the Department it is important to recognise a the distinction between envelope addresses and the addresses which users see in message headers. When one machine transfers a message to another they use the Simple Mail Transfer Protocol (SMTP). This protocol is documented in RFC 2821\(^{10}\). The format of the messages transferred is documented in RFC 2822\(^{11}\). The e-mail addresses of the sender and the recipient or recipients appear twice; the “envelope addresses” are part of the

\(^{10}\)http://mirror.ox.ac.uk/Mirrors/ftp.isi.edu/in-notes/rfc2821.txt
\(^{11}\)http://mirror.ox.ac.uk/Mirrors/ftp.isi.edu/in-notes/rfc2822.txt
SMTP transaction and in the “header addresses” (the From:, To:, Cc:, etc. lines that the user sees) are part of the message transferred. The envelope addresses are used to route the messages from machine to machine. The message headers are information for the user and the software which is used to read and compose messages — they aren’t used as part of the routing and delivery process at all. Typically the two sets of addresses start off being the same. However, different transformations may be applied to the envelope and the message headers as the mail makes its way from machine to machine and the two sets of addresses can soon differ from each other (even without this extensive address re-writing which our system uses this often occurs in normal e-mail transactions — examples include the deletion of Bcc: headers while retaining the addresses of the recipient or recipients so specified in the envelope, or the forwarding of mail from one system to another, where the envelope address is changed to reflect the forwarding address but the address actually used by the sender remains a matter of record in the headers).

All mail transport processing on the Department’s Unix computers use a version of the Sendmail12 software (version 8.12.8 at the time of writing). The source code for this software is freely available13. UCB Sendmail version 8 is preferred over the vendor supplied Sendmail software distributed with the various versions of Unix in use because it is easier to configure and maintain and offers uniform behaviour over all the Unix versions in use.

The mail clients of Wren simply send all outgoing messages to Wren, unaltered, for processing. Messages are relayed using SMTP. The various mail clients in use on personal computers normally have a configuration option which allows this to be set up by simply specifying the name of the mail hub. Unix based mail clients achieve the same effect by running Sendmail with a very basic configuration file. The mail programs on client systems should, if possible, qualify local addresses with the Department’s domain name. Otherwise local addresses should be left unqualified, to allow the mail hub to apply the correct qualification.

The Sendmail daemon on Wren qualifies any unqualified addresses with the Department’s domain name (so user becomes user@physiol.ox.ac.uk). It then routes messages as follows:

- It accepts any messages which have a recipient envelope address of the form username@something.physiol.ox.ac.uk for final delivery. Such messages will normally have come from Oxmail, and have this form of recipient envelope address because Oxmail has re-written it as part of the process of routing the message for delivery.

- It passes all other messages to Oxmail for header re-writing and routing. Such messages will normally have come from a mail client.

Oxmail applies the following processes to all the messages it receives, whether from another computer within the University or from the Internet:

12http://www.sendmail.org/
13http://www.mirror.ac.uk/sites/ftp.sendmail.org/pub/sendmail/
• If a mail address of the form username@physiol.ox.ac.uk appears in the message headers “From:” or “Cc:” it rewrites the address into the “Full Name” form of the address.

• If the domain portion of the envelope recipient address is one of the domains within the University it looks up the address in the mail routing tables and determines the appropriate delivery address for the message and sends it to the appropriate mail hub for final delivery.

• Otherwise it looks the domain portion of the envelope recipient address up in the DNS and routes the message across the Internet to the intended recipient’s organisation.

Several examples to illustrate how this fits together (for convenience we shall assume that the user’s mail hub is Wren — much the same processes apply at other mail hubs):

Mail from a member of the Department to an external address: The sender composes his or her message and dispatches it. The sender’s address is either username or username@physiol.ox.ac.uk in both the SMTP envelope and the headers. The message goes from the user’s machine to Wren. If the sender address is a bare username then it is qualified to username@physiol.ox.ac.uk in both the envelope and the headers. Willis sends the message to Oxmail, which re-writes the sender address into the preferred first.last@physiol.ox.ac.uk form and then sends the message on.

Mail from an external address to the Department: The sender typically addresses their message using the first.last form. Oxmail is the best MX host for the domain physiol.ox.ac.uk so the message is transferred to Oxmail. Oxmail re-writes the envelope recipient address to reflect the preferred mailbox of the user — in our example this will be something like username@mail.physiol.ox.ac.uk. The header recipient address isn’t changed. The message is then transferred from Oxmail to Wren, and Wren accepts delivery and places the message in the user’s mailbox.

Mail from person to person within the Department: This basically works like a combination of the first two cases. By the time that Wren has ensured that addresses are qualified the sender address looks something like user1@physiol.ox.ac.uk, the recipient address looks something like user2@physiol.ox.ac.uk (or the corresponding first.last form) and the envelope and header addresses match. The message is then sent to Oxmail. The header addresses and the sender envelope address are transformed into the first.last form. The recipient envelope address is transformed into user2’s preferred mailbox address and the message is then sent on to user2’s mail hub, where it is accepted for delivery.

For messages which are accepted for delivery on Wren, the Procmail\textsuperscript{14} mail delivery agent is used. A global /etc/procmailrc file is used to:

\textsuperscript{14}http://www.procmail.org/
Neuter executable content which is delivered by mail. The message body is filtered to re-write any HTML tags which are normally used to introduce scripting or embed executable content, and any message attachments which have filenames which would normally make the attachment executable by Windows (.bat, .exe, .com, .pif, etc) are renamed to prevent users from accidently starting them.

Catagorize the message using SpamAssassin\textsuperscript{15}. SpamAssassin uses a series of heuristic tests to assign a “score” to each message and then applies a threshold to the total score to decide whether to catagorize a message as “spam” (unwanted junk mail) or “clean”.

Our SpamAssassin installation is configured to make no visible changes to the message — the catagorization reached and other reporting details are attached to the message in the form of extra message headers, which can then be used as triggers for subsequent filtering, if the person receiving the message decides to do so.

Users’ can provide a .procmailrc file in their home directory to control final delivery of their mail. This configuration file could be used to sort the messages received from different mailing lists into different folders, filter messages based on SpamAssassin headers, trigger vacation style automated responses, etc.

3.5.2 Reading and Composition

Assuming that a user’s mail is stored on Wren, there are several different ways that it can be accessed:

- The directory containing the mailboxes on Wren (/var/mail) is exported via NFS. Unix workstations can mount this directory locally as if it were their own mail spool directory. Any Unix based mail program will then allow the user to read their mail. Use of this mechanism is discouraged, in favour of the use of IMAP based clients.

- Wren offers an IMAP service (Internet Message Access Protocol, RFC 2060\textsuperscript{16}) which enables users on networked machines read both their incoming mailbox and any other folders which they have stored in their home directory.

- Wren offers a POP3 service (Post Office Protocol, RFC 1939\textsuperscript{17}) which enables users on networked machines to transfer messages from their incoming mailbox to the client machine.

\textbf{Note:} Use of the POP3 service is generally discouraged, but it can be useful in some unusual situations and is unavoidable in some circumstances.

\textsuperscript{15}http://spamassassin.org/
\textsuperscript{16}http://mirror.ox.ac.uk/Mirrors/ftp.isi.edu/in-notes/rfc2060.txt
\textsuperscript{17}http://mirror.ox.ac.uk/Mirrors/ftp.isi.edu/in-notes/rfc1939.txt
The IMAP and POP3 daemons used on Wren are those available in source code form from the University of Washington\textsuperscript{18}.

Users may use any mail reading/composition program ("mail user agent" or "MUA") on any platform which can make use of the services provided. However we recommend and support the following software, and users who choose to make use of other programs are expected to support themselves:

- On Unix clients we recommend \textbf{Pine} (preferably using IMAP rather than NFS to access folders). Any member of the Department who lacks access to a Unix system in their own group can access Pine by making a SSH connection to “\texttt{m5.physiol.ox.ac.uk}”, logging in with their normal Departmental username and password and then typing the command \texttt{pine}.

- On 32-bit Windows (9x, ME, NT, 2000, XP), Unix and newer Macintosh clients we support \textbf{Netscape Messenger}, using IMAP to access folders rather than POP3 or “movemail”.

- On Windows 3.1 we support \textbf{ECSmail}, using IMAP to access folders.

- On older Macintosh clients which cannot cope with Netscape Messenger, we support \textbf{Eudora Light}, using POP3 to access folders. Eudora takes mail out of the user’s system mailbox and stores it in its own set of folders (which are stored in the user’s home directory, separate from the main mail folders). A user must decide either to use Eudora or to make use all the other mail programs but not both. Users who wish to read mail on older Macintoshes without using Eudora can log in to the system “\texttt{m5.physiol.ox.ac.uk}” remotely, and use Pine.

- Using any web browser, members of the Department can access their mail folders by using the Department’s web mail interface\textsuperscript{19}.

Other than the restrictions on using Eudora, noted above, all these mail programs should inter-operate cleanly. Users may change from MUA to MUA and find the same collection of messages in each environment (although, unfortunately, other features such as “address books” are internal to the program concerned and do not transfer from one environment to another).

\section{3.6 HTTP Services}

Web services on the Departmental network are provided by the server “Wren”, using a variety of rôle specific aliases, running the Apache HTTP server\textsuperscript{20} software.

The Apache daemon is a process called \texttt{httpd} and it is started at boot time by the script \texttt{/etc/rc3.d/S92local-httpd}. It is configured using various files

\footnotetext[18]{ftp://ftp.cac.washington.edu/imap/}
\footnotetext[19]{http://mail.physiol.ox.ac.uk/}
\footnotetext[20]{http://httpd.apache.org/}
in the `/etc/apache` directory. The software is installed under the directory `/usr/local/apache`.

There are three important optional components which are included in our build of Apache:

- **mod\_php.**\(^{21}\)** PHP is a server-side scripting language. It operates as a preprocessor: HTML pages on our server are processed through mod\_php, which executes embedded PHP code fragments before the page is sent to the requester. The Departmental pages use PHP to include “boilerplate” page fragments which provide the standardized, site-wide navigation links, and PHP scripting can also be used to process web based forms and similar dynamic pages.

- **mod\_perl.**\(^{22}\)** which allows Perl modules to be linked into the httpd process. This is used by the WING web mail software and a locally written authentication module which can be used to verify a username and password against the Departmental passwd database.

- **mod\_ssl.**\(^{23}\)** which allows encryption of connections to the web server using the “Secure Sockets Layer” (SSLv2/v3) or “Transport Layer Security” (TLSv1, RFC 2246\(^{24}\)) protocols. Encrypted connections are required whenever Departmental usernames and passwords are used for authentication.

### 3.6.1 Departmental Web Pages

The Department’s main web presence is can be found at the address:

http://www.physiol.ox.ac.uk/

The document tree that provides the content for this site can be found on Wren in the directory `/usr/local/apache/physiol/htdocs`. Standard PHP routines that are used by all the pages in the Departmental site can be found in the `/include/` subdirectory.

That content of the site which is relatively static (the “About the Department” or “Contact Details” sections, and the various “Links” pages, for example) is typically edited and updated by the Computing staff. Wherever possible, however, sections of the web that need to be actively maintained are turned over to the owners of the information concerned; this is typically accomplished by creating a Unix filesystem symbolic link in the main document tree which points to a directory in the responsible author’s home directory, or an appropriate shared directory accessible to a group of authors. Examples include the “Admin” and “Library” sections, and many of the sub-pages of the “Research Groups” section.

\(^{21}\)http://uk.php.net/
\(^{22}\)http://perl.apache.org/
\(^{23}\)http://www.modssl.org/
\(^{24}\)http://mirror.ox.ac.uk/Mirrors/ftp.isi.edu/in-notes/rfc2246.txt
In some areas we are attempting to reduce the requirement on information providers within the Department to edit raw HTML/PHP pages (or have the Computing staff do this for them). Increasingly we are attempting to replace such pages by CGI programs (typically written in Perl) with a database backend. In such cases information is provided or updated by users who fill out web forms, information is stored in database tables, and pages containing the information are dynamically created by CGI programs that query the database and then embed the required information in pre-prepared HTML templates. Examples of this approach include the Research Interests section of the Graduate Studies pages and the “Lunch Club” seminar programme.

3.6.2 Users’ Personal Web Pages

Each person with a network account is able to manage their own piece of web space on the Departmental server. Users can make files available to the web by placing them in a subdirectory of their home directory called public_html. The contents of a public_html then show up on the web under URLs of the form http://www.physiol.ox.ac.uk/~username/.

A brief description of the process of publishing files in this way can be found under the heading “Using the Web Server” in the Computing section of the Departmental web.

In addition to providing personal web pages, this facility provides the mechanism for third-party file downloads discussed in section 2.6.2. Members of the Department can use the Departmental server to transfer files to third parties by placing them in their public_html directories and advising the intended recipient of the URL.

3.6.3 Third-Party File Upload

The mechanism for third-party file uploads discussed in section 2.6.2 is provided by a pair of CGI programs is located at http://www.physiol.ox.ac.uk/xfer/. One page provides an upload form accessible to anyone, the other page provides a download form that is only accessible to authenticated users. Both programs use the Unix setuid mechanism to run under the ownership of a pseudo-user, “xfer”.

Uploaded files are stored under the directory /home/willis/xfer, which is readable/writable only by the xfer user. A hard quota for the xfer user is used to limit the amount of space on the file server that uploaded files may use. The upload program generates a unique six-digit reference number for each upload session, and creates a subdirectory named after this number under the xfer directory. All files uploaded as part of a session are placed in the session specific subdirectory. Careful filtering of the uploaded filenames is used to prevent the upload from being written to a parent directory. This scheme is intended to prevent the upload from accidentally or deliberately adding or

25http://www.physiol.ox.ac.uk/Computing/Using_the_Web_Server.html

50
overwriting files elsewhere in the server filesystem.

The upload reference number should be noted by the person who conducted the upload, and then communicated to the intended recipient of the files within the Department. The recipient visits the download page and, after user authentication, the download program prompts the user for the reference number. Given a valid reference number the download page lists links for the files stored in the relevant xfer subdirectory. User authentication ensures that files uploaded by persons unconnected with the Department may not subsequently be download by other such persons — failure to impose this condition runs the risk that our server will be used, without our knowledge, for distribution or storage of illegal material (such as stolen proprietary software or pornography). The system of reference numbers provides a degree of privacy between authorised members of the Department — one authenticated user is unlikely to gain accidental access to files intended for another (care must be exercised when passing reference numbers from sender to intended recipient, however, if there are stringent privacy concerns about the files).

The cron.daily housekeeping script removes all uploaded files older than seven days, and any empty upload directories, preventing a backlog of uploaded files from exhausting the xfer quota.

3.6.4 Remote File Management and Transfer

We use CGI software called WebRFM\(^{26}\) to provide authenticated HTTP access to both personal and shared files stored on the file server. WebRFM provides two levels of access:

- an HTML form-based layer, which allows a wide variety of file management tasks (upload, download, renaming, deletion, editing) to be conducted from any web browser. This form-based interface can be accessed by using the link “Web-based File Manager” in the Computing section of the Departmental web.

- a direct HTTP layer that implements a class 1 WebDAV\(^{27}\) server. WebDAV is a set of extensions to the HTTP protocol and is used by a variety of web-enabled file management applications such as the “Web Folders” feature of Microsoft Internet Explorer, or the “publish via HTTP” features of Netscape Composer.

Access to the directory that contains the files.cgi program is restricted such that username and password authentication over an SSL secured connection is required. The files.cgi program itself a setuid-root C program, which changes the user ID and group IDs of the process to match the user ID and group IDs of the username that authentication module has already checked, then executes the main WebRFM Perl code, which can be found in the directory /usr/local/lib/WebRFM.

\(^{26}\)http://www.geocities.com/SiliconValley/Horizon/7772/webrfm.html
\(^{27}\)http://www.webdav.org
3.6.5 Web-based Email Interface

Users who are away from the Department and without access to a correctly configured IMAP client are able to access their IMAP mail folders, as well as composing and sending new mail, using a web based interface at the URL http://mail.physiol.ox.ac.uk/.

This service is provided using the WING software developed by OUCS for the Herald mail cluster. WING consists of a web front-end which uses a collection of mod_perl modules and a daemon process called “mailed”. One mailed daemon is spawned for each login session — this effectively forms a bridge between the stateless HTTP protocol and the stateful, connection-oriented IMAP protocol.

Users’ information, personal preferences, address book and session information is held in a PostgreSQL database entitled “wing”.

At system boot time the script /etc/rc3.d/S91local-wing clears any stale session information from the database and starts the master mailed process. Note the ordering of S90local-postgres, S91local-wing and S92local-httpd: the database is made ready first, then the WING backend is made ready, and only then is the web server started (which has the effect of making the WING front end available to the users).

Users log in to WING using their Physiology username and password. However, unlike all the other authenticated web services that we operate, WING does not use the local Physiology authentication module: the username and password entered at WING login are verified by being used to authenticate the IMAP connection.

The current WING installation does not use SSL to protect usernames and passwords. We intend to fix this shortly when a newer version of the software is installed.

3.6.6 Web-based Interface to the “Req” Request Tracker

The request tracking system used by the Computing staff has a web-based front end located at https://req.physiol.ox.ac.uk/.

The CGI programs that provide the content for this site can be found on Wren in the directory /usr/local/apache/webreq/htdocs. Access to the directory is restricted such that username and password authentication over an SSL secured connection is required.

There are two programs in the directory: webreq.pl is a Perl script which implements the interface, and index.cgi is a setuid-root wrapper program which changes user ID to match the user ID of the username given in the HTTP authentication phase before executing webreq.pl.

http://users.ox.ac.uk/%7Embeattie/wing/
3.6.7 User Authentication

With the exception of the WING interface, all the web services which use Physiology usernames and passwords for authentication are based on a local mod_perl authentication module, “Apache::AuthPhysiol”. The code for this module is stored on Wren in the directory /usr/local/apache/lib/perl.

A requirement for password authentication can be imposed on a particular directory by creating a .htaccess file similar to:

```
AuthType Basic
AuthName Physiology
PermAuhenHandler Apache::AuthPhysiol
require valid-user
SSLRequireSSL
```

This grants access on presentation of any valid username and password combination — we limit access to specific usernames by changing the “require” directive to something like:

```
require user username1 username2 username3
```

The “SSLRequireSSL” directive forbids access unless the pages are accessed over an SSL/TLS encrypted connection. Everywhere that the AuthPhysiol module is used, SSL/TLS connections should be mandated. The intention of this restriction is to ensure that Physiology username and passwords are not passed over public networks in the clear.

CGI programs that reside in directories protected in this way can use the environment variable “REMOTE_USER” to discover the username that was presented during authentication, and know that Apache has already verified that the user is who they claim to be.

3.6.8 Database Storage

Database storage for the WING service and various CGI based applications on the web server is provided using the PostgreSQL database management system, installed on Wren in the directory /usr/local/pgsql. The PostgreSQL daemon (postmaster) is started at boot time by the script S90local-postgres in the directory /etc/rc3.d. The postmaster process runs under a pseudo-account “postgres”.

3.7 Availability of the Departmental Servers

Willis and Wren are vital components of much of the computing provision in the Department. In addition to the visible services that most users are aware

\[29\text{http://www.postgresql.org/}\]
Table 3.1: Names and utilization of the disk devices, at SCSI target level.

<table>
<thead>
<tr>
<th>Description</th>
<th>Solaris Device Name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal 18Gbyte Disk</td>
<td>c1t1d0</td>
<td>OS</td>
</tr>
<tr>
<td>20Gbyte RAID partition</td>
<td>c7t0d0</td>
<td>OS</td>
</tr>
<tr>
<td>330Gbyte RAID partition</td>
<td>c7t1d0</td>
<td>File storage</td>
</tr>
</tbody>
</table>

of (such as file services, email, etc) these systems provide network administrative functions such as the NIS and are, for example, constantly issuing renewed DHCP leases for many of the machines on the network. Many networked computers within the Department cease to be usable even as stand-alone machines if the central servers are unavailable.

Obviously, therefore, it is vital that the servers and network hardware be extremely reliable, available to do their job 24 hours a day, 7 days a week and, in the event of a problem, that restoration of service should be as rapid as possible.

- We protect against loss of service due to hard disk problems by using a system of redundant disk arrays on the servers.
- We provide for rapid re-introduction of service following a hardware failure of Willis or Wren by duplicating all critical data and configuration information on both servers.
- We provide for rapid re-introduction of service following a hardware failure of the network infrastructure by making available at short notice supplies of equipment to replace units which fail.

3.7.1 Disk Mirroring

The disk storage attached to Willis and Wren is identical, and in both cases consists of one internal FC-AL disk with a capacity of 18Gbytes and one external Sun StorEdge 3310 disk array. The disk array is equipped with six (out of a possible maximum twelve) 72Gbyte SCSI disks and a hardware RAID controller.

The disk arrays are arranged in a RAID 5 configuration, with a single logical drive of approximately 350Gbytes capacity. This logical drive is then partitioned into two, one partition of approximately 20Gbytes and one of approximately 330Gbytes.

These storage devices are presented to the operating system using the device designations listed in table 3.1.

The FC-AL internal disk and the 20Gbyte partition on the RAID array are used to store the server’s operating system, and each is further sub-partitioned to contain the various standard filesystems that make up a Solaris installation (/usr, /var, /var/mail), plus an alternate root filesystem (/alt) and a swap partition. The corresponding sub-partitions on the internal drive and the RAID
Table 3.2: The filesystems and their associated metadevices

<table>
<thead>
<tr>
<th>Willis mnt point</th>
<th>Wren mnt point</th>
<th>Metadevice</th>
<th>Physical device(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>/</td>
<td>d0 (mirror)</td>
<td>c1t1d0s0/c7t0d0s0</td>
</tr>
<tr>
<td>swap</td>
<td>swap</td>
<td>d10 (mirror)</td>
<td>c1t1d0s1/c7t0d0s1</td>
</tr>
<tr>
<td>/usr</td>
<td>/usr</td>
<td>d20 (mirror)</td>
<td>c1t1d0s3/c7t0d0s3</td>
</tr>
<tr>
<td>/var</td>
<td>/var</td>
<td>d30 (mirror)</td>
<td>c1t1d0s4/c7t0d0s4</td>
</tr>
<tr>
<td>/var/mail</td>
<td>/var/mail</td>
<td>d40 (mirror)</td>
<td>c1t1d0s5/c7t0d0s5</td>
</tr>
<tr>
<td>/alt</td>
<td>/alt</td>
<td>d50 (mirror)</td>
<td>c1t1d0s6/c7t0d0s6</td>
</tr>
<tr>
<td>/export</td>
<td>/alt/export</td>
<td>d100 (soft part.)</td>
<td>c7t1d0s0</td>
</tr>
<tr>
<td>/home/willis</td>
<td>/alt/home/willis</td>
<td>d101 (soft part.)</td>
<td>c7t1d0s0</td>
</tr>
<tr>
<td>/home/mail</td>
<td>/home/mail</td>
<td>d102 (soft part.)</td>
<td>c7t1d0s0</td>
</tr>
</tbody>
</table>

array are combined together into two-way metamirrors, using Sun’s Solaris Volume Manager software, and the filesystems and swap area are built on those mirrored components.

The 330Gbyte partition on the RAID array is used to store the /home/willis, /home/mail and /export filesystems. The filesystems are built on “soft partitions” — a feature of Solaris Volume Manager which allows multiple filesystems to be allocated from a single storage pool, without the pool being strictly partitioned up at setup time. When initially created the three filesystems occupied around half the available storage. The soft partitions can subsequently be expanded into the remaining space as required, or additional soft partitions can be created in the space, without disturbing the existing contents of the filesystems.

Table 3.2 shows all the filesystems and swap areas, and the metadevices on which they reside, effectively summarising the information in the system configuration files /etc/vfstab and /etc/lvm/md.tab.

The servers should be able to continue in service as normal in the event of the failure of any one disk.

If the RAID array should fail completely (through multiple drive failures, or a failure in the RAID controller, cabling or SCSI controller) then the filesystems /export, /home/willis and /home/mail would become unavailable. The server operating system itself, and all the system configuration, would remain intact and operational due to the mirror partitions on the internal system disk. This would greatly ease and speed the process of recovery from the RAID problems.

There is a serial connection between both servers and their respective RAID arrays, allowing access to the firmware menus used to monitor and reconfigure the arrays. The serial connections are plugged into serial port “B”, and use a serial protocol of 8-bit characters, no parity, one stop bit (“8N1”) at 38400kbps. It should be possible to connect to the array firmware from the host Sun by running the command:

tip -38400 /dev/ttyb
Sun make available online documentation for the 3310 array firmware\textsuperscript{30} and the Solaris Volume Manager\textsuperscript{31}. The commands of particular relevance in administering the disk mirroring and soft partitions are:

- **metadb** for creating and deleting replicas of the metadevice state database.
- **metainit** for initializing metadevices.
- **metattach** for attaching metadevices to metamirrors, or adding space to soft partition.
- **metadetach** for detaching metadevices from metamirrors.
- **metastat** for querying the state of the system.

### 3.7.2 Duplication of the Departmental Servers

As has previously been discussed, the Department operates two main servers, “Willis” and “Wren”, which have substantially similar specifications and disk storage arrangements, but which normally perform distinct and different roles. Willis is tasked with file and print serving, and is the master repository for various network information services (the NIS, DNS, etc). Wren is tasked with providing email and web services, and also hosts the Department’s PostgreSQL databases (since various web-based applications are the primary users of those databases).

Beyond the operating system partitions (which are substantially identical on the two servers) there are three main filesystems on the servers which contain unique, local data: `/home/willis`, which contains users personal and shared files; `/home/mail`, which contains IMAP folders; and `/export`, which contains networked software for use by client machines. A copy of each of these filesystems is held on both servers — Willis holds the “active” copy of `/home/willis` and `/export` and a backup of `/home/mail`, whereas Wren holds the active copy of `/home/mail` and backups of `/home/willis` and `/export`.

As part of Willis’s nightly housekeeping (the shell script `cron.daily` in the directory `/home/willis/admin/bin`, which is run from the root crontab at 22:00 each evening) a snapshot of each “active” filesystem is copied to its backup counterpart on the other server. This backup operation uses a program called `rsync`, which updates the backup copy in a bandwidth-efficient manner (copying only the parts of files which have changed since the previous synchronisation operation). Wren constantly runs a rsync process in background “daemon” mode, waiting for connections from Willis. The rsync daemon is configured using a file `/etc/rsyncd.conf`, which requires that connections originate from Willis’s IP address and are authenticated with a secret username and password. The requisite shared secret is stored in `/etc/rsync.password` on Willis and `/etc/rsyncd.secrets` on Wren (both files have ownership and permissions such that they are readable only by root).

\textsuperscript{30}http://docs.sun.com/source/817-3711-10/index.html
\textsuperscript{31}http://docs.sun.com/db/doc/817-2530
The active /home/willis and /export filesystems are NFS mounted on Wren from Willis (as they would be on a general purpose Unix workstation in the Department). The backup copies of those filesystems are therefore mounted under an alternative root directory /alt, making the pathnames for the backups /alt/home/willis and /alt/export. Willis doesn’t remote mount the /home/mail filesystem, so the backup copy of /home/mail on Willis is mounted under its normal name.

To summarise: Willis and Wren are identically specified machines, running the same operating system software, with the same data. All that distinguishes one from the other is:

- the services that they run (as a result of daemons either started at boot time by scripts in /etc/rc3.d or launched on demand from the inetd supervisor process, which is configured by way of the /etc/inetd.conf file)
- the mount points used for various filesystems (controlled by the configuration file /etc/vfstab)
- the filesystems that are NFS exported (controlled by the configuration file /etc/dfs/dfstab.
- the network interfaces (physical and virtual) that are configured and the IP addresses allocated to them (controlled by various configuration files matching the pattern /etc_hostname.*, where the wildcard component is the interface name).

All of the substantial differences between the two configurations are held in the /etc directory, or subdirectories thereof. We can convert a machine from the Willis rôle to the Wren rôle, or vice-versa, by substituting an appropriate /etc and rebooting. To this end Willis carries a backup copy of wren:/etc, stored as /etc.wren, and Wren carries a backup copy of willis:/etc, stored as /etc.willis, and both systems carry a directory /etc.both which contains a manually constructed union of the two configurations. The intention is that in a crisis either hardware setup may take on either rôle, or that a single machine can adopt both rôles in the event of a catastrophic failure of the other set of hardware, by a simple renaming the /etc directories and a reboot. So in the event of a failure of Wren, for example, the machine filling the Willis rôle could be configured to double as the mail and web server in addition to its normal duties by running a command line such as the following:

```
mv /etc /etc.willis; mv /etc.both /etc; /sbin/init 6
```

Note that rôle switching between the servers is intended as a remedy of last resort and should not be undertaken lightly. All existing connections by clients to the servers will be severed. As synchronisation of the active filesystems to their backups only takes place nightly the current day’s changes to files or mail folders will be lost. It is also extremely important that only one set of hardware take up a given rôle at any one time, or chaos will ensue. Before starting a
machine in the “both” rôle the other set of hardware should be powered down and preferably physically isolated from the network.

The original intention was that the servers in the two rôles would be entirely independent of each other. Currently, however, there are still some dependencies in the Wren rôle upon services normally provided by the Willis rôle (notably NFS access to the active /home/willis filesystem). As things stand Willis will offer its services independently of whether or not Wren is running, but the converse is not true.

### 3.7.3 Availability of the Network

Our planning concerning network availability focusses on rapid replacement of failed equipment, rather than redundant provision. Refer to figure 3.1 for a reminder of the various hardware components that make up the network.

Replacement is provided for by:

- holding in the Computing Office at least one spare unit of each of the main models of hub, switch and interface module.
- subscription to the OUCS Network Hardware Support scheme\(^\text{32}\).

An inventory of the network equipment and contact details for OUCS Network Control are listed in section 4.6.

### 3.8 Backup

As a matter of policy the backup system on the Departmental file server is intended for backing up the two main servers — the owners of other systems on the network are expected to make their own provision for backing up their own local storage.

The backups are automatically scheduled for late evening (at 22:00 — by which time the filesystems are hopefully relatively idle) using the Unix cron mechanism. The backups are organised using the shell script backup, which is stored in the directory /home/willis/admin/backup. The backup script is designed to act as a wrapper around the standard Solaris backup utility ufsdump, providing a way of applying it easily to multiple filesystems.

The backup script is controlled by a file called “backup table”. A backup table contains a series of lines specifying:

- The mount-point of the filesystem to be backed up.
- A flag used to indicate to the backup script whether this is the last filesystem which is stored on a tape when doing full backups.

\(^{32}\)http://www.oucs.ox.ac.uk/network/lan/
Table 3.3: Contents of a backup tape.

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Full backup tape-number / record-number</th>
<th>Incremental backup record-number</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>1 / 1</td>
<td>1</td>
</tr>
<tr>
<td>/var</td>
<td>1 / 2</td>
<td>2</td>
</tr>
<tr>
<td>/var/mail</td>
<td>1 / 3</td>
<td>3</td>
</tr>
<tr>
<td>/usr</td>
<td>1 / 4</td>
<td>4</td>
</tr>
<tr>
<td>/alt</td>
<td>1 / 5</td>
<td>5</td>
</tr>
<tr>
<td>/export</td>
<td>1 / 6</td>
<td>6</td>
</tr>
<tr>
<td>/home/willis</td>
<td>2 / 1</td>
<td>7</td>
</tr>
<tr>
<td>/home/mail</td>
<td>2 / 2</td>
<td>8</td>
</tr>
</tbody>
</table>

Full backups of all the filesystems on Willis are performed on Friday evenings. These backups span two tape cartridges (currently the first six filesystems on the tape labelled “vol 1/2” and the last two filesystems on the tape labelled “vol 2/2”). Incremental backups relative to the previous full backup are performed each evening from Monday to Thursday — incremental backups of all eight filesystems fit on a single tape).

The default backuptab file stores the filesystem in the order given in table 3.3. Backup occurs after the daily bi-directional file synchronization between the servers, so a full backup of Willis also effectively backs up the /home/mail filesystem from Wren.

The first Friday backup taken in a month is labelled with the date of the backup and is stored indefinitely. Subsequent Friday tapes are labelled “Week 2”, “Week 3”, “Week 4” and “Week 5” (referring to the week of the month in which they were taken) — these tapes are re-used month on month until the tape drive error correction rate indicates that they need replacing.

The tapes used on the other evenings of the week are simply labelled “Monday”, “Tuesday”, “Wednesday” and “Thursday”. These tapes are re-used week on week until they need replacing.

The tape drive can hold up to 8 tapes simultaneously. When one tape is ejected the next is automatically loaded in its place. When the last tape is ejected the drive automatically loads the first tape again. Normally only the first six tape slots are occupied, with the “Monday” tape in slot 1, the “Tuesday” tape in slot 2, etc. The two tapes for Friday normally occupy slots 5 and 6. At some point during each week the Friday tapes written the previous week are unloaded, and the next set of Friday tapes are loaded (a reminder email about this task is sent to the operator on Monday morning).

Refer to section 4.4.1 for information on how to retrieve information from the backup tapes.
3.8.1 Offsite Backup

The dated full backup sets produced at the start of each month are stored at the Computer Manager’s flat, rather than in the Department. This ensures that even in the event of large scale destruction affecting the server, the reserve server and the backup tapes in the Computer Officer’s room the programs, configuration information, administrative databases and user files will be preserved (although in the worst case the information preserved may be up to a month out of date).

As an additional “offsite backup” precaution the file server is backed up to the OUCS Hierarchical File Server (HFS) once a week, in the early hours of each Wednesday morning. The HFS operates on an “incremental forever” principle. Each time the system is backed up any files which have changed since the last backup are stored. The HFS keeps the last two versions of each file. In the event that a file is removed its backups are kept for 90 days.

The HFS client software is stored under the directory /opt/tivoli/tsm. The scheduler software (which automatically responds to backup requests initiated by the HFS) is started by the init program when the machine boots. A manual backup can be initiated or a files restored using the dsmc command. Refer to section 4.4.2 for instructions on file retrieval.

3.9 Software Updates

3.9.1 Windows 2000, XP and 2003

The Department operates a server providing Microsoft Software Update Services (SUS). The SUS server downloads critical updates from Microsoft, which are then held in a queue pending approval by the Computing staff. Once updates are approved client systems can download them from the SUS server much as they would if accessing the Microsoft Windows Update servers over the Internet. The inclusion of the local approval step makes it tenable for us to use entirely automated updates on the client machines, a step that we do not feel we could take if the updates were applied to client systems directly from the Microsoft servers, without local control over the nature and timing of the updates.

Windows systems in the Department which are using the automatic update system are configured to connect to the SUS server daily, download any newly approved updates, and apply them. If an update requires a system restart then the user is prompted before this takes place, allowing the reboot to be performed when convenient. All other user interaction is disabled — the check for updates, downloading, and installation all happens as an unprompted background process.

The Windows registry settings which configure a client to make use of the automatic update mechanism are available on the file server in the file n:sus\susOn.reg.

---

33http://hfs.ox.ac.uk/local/
A similar collection of registry settings which disables the use of the automatic update mechanism (to reset the configuration of a computer that is leaving the Physiology network, or to enable manual access to Windows Update for users that wish to take direct responsibility for apply updates) are available on the file server in the file `n:sus\susOff.reg`.

### 3.9.2 SUSE Linux

SUSE is the Department’s current “preferred” Linux distribution.

We maintain a local copy of the SUSE update packages for all current releases, using `rsync` to update this on a nightly basis from the JISC National Mirror Service\(^\text{34}\).

SUSE systems in the Department are configured to check for updates on the file server on a daily basis, using the SUSE supplied “YaST Online Update” (aka “YOU”) utility.

### 3.9.3 Red Hat Linux

The Department still has a number of workstations running Red Hat Linux 7.3 and 9. Formal support for this software has been terminated by Red Hat, however critical updates are still available, provided by a community-supported collaboration known as the Fedora Legacy Project\(^\text{35}\).

Red Hat systems in the Department have the “yum” software provided by Fedora Legacy installed, and check for updated software on a nightly basis using the mirror of Fedora Legacy updates provided by the OUCS Mirror Server\(^\text{36}\).

### 3.10 Anti-Virus Measures

The Department uses Sophos\(^\text{37}\) Anti-Virus, a product for which the University has a site-license agreement.

Sophos is normally installed on Windows systems as a matter of routine when they are inspected for connection to the network, though this step may be skipped if the owner of a machine has alternative anti-virus provision which is actively maintained and updated (for example, short-term visitors or users with laptops which primarily connect to networks in colleges and or other Departments may well be better served by their existing anti-virus package and update arrangements).

The automated update feature of the Sophos package is enabled at installation, and regularly checks a Samba share on the main file server for updated soft-

\(^{34}\)http://mirror.ac.uk/
\(^{35}\)http://fedoralegacy.org/
\(^{36}\)http://mirror.ox.ac.uk/sites/download.fedoralegacy.org/
\(^{37}\)http://www.sophos.com/
ware and IDE files (virus signatures). The Computing staff install the monthly Sophos updates on this share as they are released, and inbetween monthly updates also frequently install additional IDE files as and when required to address new virus strains which are particularly wide-spread or considered particularly dangerous.

### 3.11 Writing CD-ROMs

CD-ROM recording is carried out using the software packages “cdrecord” and “mkisofs”\(^\text{38}\), running on the Departmental workstation “Hal”. These programs are combined using a locally produced script, cdwrite.

Files to be written are normally collected together in the user’s home directory, or other place that Hal can access via NFS. The cdwrite script uses mkisofs to compose an ISO 9660 filesystem image (using a temporary file on a disk local to Hal) and then copies the image file to the CD writer.

### 3.12 Clock Synchronization

It is useful to be able to synchronize the clocks on the various computers in the Department. This makes timestamps in distributed filesystems properly consistent, keeps date and time in e-mail traffic correct, makes it possible to compare timestamped log file entries on different machines, etc.

The Internet Network Time Protocol (NTP, RFC 1305\(^\text{39}\)) offers a standard way to synchronize timekeeping among a set of distributed time servers and clients. OU CS offers an NTP Service\(^\text{40}\).

The arrangement of NTP servers is hierarchical. UKERNA\(^\text{41}\) operate a number of “stratum-1” time servers which are synchronized to highly accurate and stable time sources (such as radio signals from atomic clocks provided by national laboratories, Global Positioning System receivers, etc). OUCS have four “stratum-2” servers which synchronize with these “stratum-1” servers. The Department operates two “stratum-3” servers which synchronize with the OUCS servers:

- **ntp0.physiol.ox.ac.uk** (which is currently an alias for “Willis”) synchronizes with the OUCS servers **ntp2.ox.ac.uk** and **ntp3.ox.ac.uk**, plus two external servers which offer a public stratum-2 NTP service (**bear.zoo.bt.co.uk** and **ntp2b.mcc.ac.uk**).

- **ntp1.physiol.ox.ac.uk** (which is currently an alias for “Wren”) synchronizes with the OUCS servers **ntp0.ox.ac.uk** and **ntp1.ox.ac.uk**,  

\(^{38}\)http://www.fokus.gmd.de/research/cc/glone/employees/joerg.schilling/private/cdrecord.html  
\(^{39}\)http://mirror.ox.ac.uk/Mirrors/ftp.isi.edu/in-notes/rfc1305.txt  
\(^{40}\)http://www.oucs.ox.ac.uk/network/ntp/  
\(^{41}\)http://www.ukerna.ac.uk/
plus two external servers which offer a public stratum-2 NTP service (ntp2.tuxfamily.net and ntp2d.mcc.ac.uk).

Note: Access to the OUCS time servers is controlled — applications to set up or change Departmental time servers are made by sending e-mail to the address timelord@ox.ac.uk.

Client machines within within the Department are synchronized by one of two possible methods:

- Operating as stratum-4 NTP clients of one or both of the Departmental time servers.
- Periodically resetting their time-of-day clock to match information available from one of the Departmental time servers.

3.12.1 Unix Clients

Unix clients run the ftp://ftp.ox.ac.uk/pub/comp/src/ntp/, written by David Mills of the University of Delaware.

There are three principle commands, ntpdate, ntpd, and ntpq. These programs are installed in /usr/local/bin for Linux and SGI machines; Solaris comes with its own xntpd and ntpdate binaries, which are used in preference to the ones in /usr/local). At boot time each Unix machine runs ntpdate, which queries the Departmental NTP servers and sets the local time and date correctly, and then starts the daemon xntpd which periodically polls the Departmental NTP servers and makes small adjustments to the local clock to keep it as stable and as closely synchronized to “real time” as possible. The NTP daemon is configured using the file /etc/ntp.conf.

3.12.2 Windows 95 Clients

Windows 95 provides a command (net time) which allows the local clock to be reset to match the clock on a file server. A net time command is run as part of the Windows 95 login script and synchronizes the local clock with that on Willis every time a user logs in to the client. After being set correctly the local clock on the client will drift slowly from the correct time but so long as a user logs in occasionally the errors should be minimal.

3.12.3 Windows 2000/XP Clients

Windows 2000 and XP have the facility to use SNTP (the Simple Network Time Protocol) to communicate with NTP servers. As part of normal network setup of such machines we configure them to use ntp0.physiol.ox.ac.uk as an SNTP synchronisation source. The time service on the client (w32time them

\footnote{public domain NTP software suite}
periodically contacts one of the Departmental stratum-3 NTP servers to correct the client clock.

3.12.4 DOS Clients

The Beame & Whiteside NFS client software includes a program (bwtime) which allows the local clock to be reset to match the clock on a host providing the Internet Time Protocol (RFC 868\textsuperscript{43}). Willis offers an RFC 868\textsuperscript{44} service (the Time protocol is one of the internal services implemented in \texttt{inetd} under Unix).

Some of the DOS client machines run \texttt{bwtime} in their \texttt{autoexec.bat} files, though this isn't universal. On some machines the \texttt{bwtime} program hangs the machine, so the command is commented out or removed from \texttt{autoexec.bat} and the user or users of the machine are expected to manually maintain their system clock at a “reasonable” value. Time stamps generated by DOS clients should therefore be regarded as unreliable.

As with Windows 95 clients some clock drift will occur between resettings. As long as the machine is restarted periodically this should not be significant.

3.13 The “Req” Request Tracking System

Requests which are e-mailed to \texttt{computing@physiol.ox.ac.uk} are handled using a computerized request tracking system called “ReqNG”. This is based on the original Req system, which is described in the paper “Managing the Ever-growing To Do List”\textsuperscript{45} (neither Req nor ReqNG are actively developed or maintained any longer — the existing ReqNG installation serves our requirements adequately, but if we were to look for an alternative at some time in the future then RT\textsuperscript{46} would probably be the replacement of choice).

All requests to the computing staff should come in through the \texttt{computing} mail alias and all responses by the staff should be copied to the mail alias as well as being sent to the original requester. Each new request is allocated a unique request number. All the message traffic relating to a particular request is kept in a separate log file, in addition to being copied to the members of the computing staff.

For each request, Req keeps track of:

- The owner (ie the member of the computing staff who is working on the problem).
- How old the request is.
- How long it has been since the user received a reply about the problem.

\textsuperscript{43}http://mirror.ox.ac.uk/Mirrors/ftp.isi.edu/in-notes/rfc868.txt
\textsuperscript{44}http://mirror.ox.ac.uk/Mirrors/ftp.isi.edu/in-notes/rfc868.txt
\textsuperscript{45}http://www.ccs.neu.edu/home/remy/documents/req.html
\textsuperscript{46}http://www.bestpractical.com/rt/
• The status: “open”, “stalled” or “resolved”.

• Who made the request.

The directory `/usr/local/req` holds most of the files associated with Req. Various commands are installed in `/usr/local/bin` (on Solaris only):

`q` is a command line program for listing the request queue.

`req` is a command line interface for operating on requests (many operations on a request can also be triggered by including an “X-Request-Do:” message header in a mail message to the computing mail alias — see the `req` manual page for details).

`tkreq` is a TCL/Tk based GUI front end for `q` and `req`. There is also a WWW interface called Webreq\(^47\) which performs a very similar function.

\(^47\)https://req.physiol.ox.ac.uk/
Chapter 4

Procedures

This chapter provides step by step guidelines for many of the routine procedures involved in running the Department’s computing related facilities and services.

4.1 Modifying The Network Databases — General Guidelines

Many of the administrative actions involve updates to the NIS maps. The source files for the NIS maps are stored in /home/willis/admin/nis. The permissions of the files and directories are such that they can only be modified by members of the Unix group “staff”. The source files are kept under the control of the Revision Control System (RCS, refer to the rcsintro man page for an overview).

The working version files are normally stored with “read only” permission. In order to obtain an editable copy of the file to work on you must run the command:

```
co -l filename
```

This is called “checking out” the file for editing.

When the editing is completed you should run the command:

```
ci -u filename
```

This “checks in” your changes to the RCS history file and creates a read only working file.

Going through the RCS procedure when changing administrative files has three important effects:
It locks the file against simultaneous update by several users — if someone has checked out the file for editing then another system administrator cannot start editing the file until it is checked back in.

It is possible to roll back changes very quickly if there are problems — a previous version of the file can be fetched from the archive at any time, either by version number or time and date (see the manual page for `co`).

It provides a historical log of who made changes to which files and when they changed them.

Note that to get the benefit of RCS, changes to the source files should be made as a normal user, not using a root account.

### 4.2 Connecting Devices To The Network

#### 4.2.1 Preparing the Administrative Databases

This section describes the steps that need to be taken on the Departmental file server prior to setting up a new device on the Departmental network. After the steps described in this section have been performed the device itself should be configured in accordance with the steps set out in the appropriate following section.

Before you start, ascertain the proposed hostname of the device, its MAC address, the type of device involved, its location and who owns it.

The MAC address is normally printed on the network interface card. The diagnostic software supplied with many network interface cards can also be used to find MAC addresses. Sun workstations print their MAC address as part of the power on banner. The serial number of SGI workstations corresponds to the MAC address.

- Log in to Willis, using a normal (unprivileged) username, and change directory to `/home/willis/admin/nis`.
- Check out editable copies of the `machines` and `netgroup` files from the Revision Control System (RCS). The `co` command will not let you obtain an editable copy of a file which already in the process of being modified by another user.
- Add an entry to the `machines` file, assigning the next free IP address available in the 163.1.248 - 163.1.251 address range. Lines have the following form:

  `<MAC address> <IP address> <canonical hostname> <alias> [...][# <comment>]

  The canonical hostname has the form “hostname.physiol” and the first alias must be “hostname”. As many additional aliases as are required can be specified.
The comment normally describes the type of device, its location and indicates the owner, principle user or owning research group.

- Edit the `netgroup` file. The device will normally be added to a netgroup depending on its type (SPARC based workstations in “physiol\sun4”, Apple Macs in “physiol\mac”, etc). The “physiol\pc” group is made up of a number of sub-groups. Add PC hostname a PC sub-group appropriate to the research group concerned if such a sub-group exists, otherwise add it to the highest numbered “misc\pc” sub-group.

- Check in the edited `machines` and `filenamenetgroup` files to the RCS archives. Supply an appropriate comment when prompted (eg. “added pe-xyz for the abc group”).

- Change directory to `/var/yp` and `su` to an admin account. Run `make` to build the NIS maps.

### 4.2.2 Connecting a Solaris Client

We use Sun’s “JumpStart” installation technology to install and configure new Sun workstations for the network. A copy of the Solaris 9 installation media can be found in the directory `/export/install` on Willis. JumpStart configuration files are in the subdirectory `JumpStart`. To perform a JumpStart install:

- Add an appropriate rule for the hostname to the `rules` file. The “profile” chosen controls the software packages to be installed and the disk partitioning to be used. `profile.workstation` should be suitable, or provide a suitable starting point for the creation of a custom profile if needed. Run `make` as root to check the rules file and profile when you are finished.

- On Willis, run the following as root:

  ```
  cd /export/install/Solaris_9/Tools
  ./add_install_client -c willis:/export/install/JumpStart \
  -p willis:/export/install/JumpStart <hostname> sun4u
  ```

- Boot the client using the following command line at the boot PROM “ok” prompt:

  ```
  boot net - install
  ```

  An entirely “hands-off” Solaris installation should then take place, after which the machine will run the shell script `finish.sh` to perform various local customizations.

### 4.2.3 Connecting an IRIX 6.5 Client

These instructions apply to a “vanilla” installation of IRIX 6.5. For a machine which has already been set up on the network to some extent these instructions could act as a check list for ensuring that things are setup in the “standard” fashion.
• Check the file `/etc/hosts`. It should contain an entry for “localhost” (with IP address 127.0.0.1), and an entry for the the name of the workstation, both with “.physiol” part as the principle name and without (as an alias). It may also contain the various multicast addresses which SGI normally put in the file.

• Edit the file `/etc/sys_id`. Ensure that it contains the correct name and that this is unqualified (remove the “.physiol” part of the name if present).

• Edit the file `/etc/config/ifconfig-1.options`. It should contain the line:

```plaintext
netmask 0xffffffff
```

• Edit the file `/var/yp/ypdomain`. It should contain the line:

```plaintext
physiol
```

• Run the following commands to ensure that the system is configured correctly:

```plaintext
chkconfig firsttimeprograms off
chkconfig network on
chkconfig nfs on
chkconfig timed off
chkconfig timeslave off
chkconfig yp on
chkconfig sendmail.cf off
```

• Change directory to `/var/X11/xdm`.

• Edit the file `/etc/xdm-config`. To turn on the XDM authentication mechanism there should be a line:

```plaintext
DisplayManager*authorize: on
```

In standard IRIX installations this is either commented out, or reads “off” rather than “on” (depending on IRIX version). Fix it such that it reads “on” and is uncommented.

• Edit the files `Xsession`, `Xsession-remote` and `Xsession.dt`. Each of them may contain a line which reads “/usr/bin/X11/xhost +”. Comment out these lines.

• Edit `/etc/passwd` to set up an admin account for yourself (duplicate the root line and modify the username and GCOS fields appropriately – conventionally the username of an admin account is the same as you use for your normal account with the phrase “admin” tacked on the end). Repeat for any other users who require admin access. There are various accounts in the default IRIX password file which have no password associated with them – the encrypted password fields are blank. Place a * symbol in each of these encrypted password fields.

Add a line containing a “+” symbol at the end (which grants login accounts to all the users named in the Departmental password file) or add a series

69
of lines of the form “+username”, one for each user who is allowed to use the machine. If a netgroup listing a group of authorised users exists then a single line of the form “+@group_name” could be used instead.

Set a password on the new admin account or accounts with the `passwd` command. Alternatively the encrypted password fields for the admin users could be copied from corresponding accounts on other systems. Similarly set a password for the root account. This password will be required in future to bring the system up single user.

- Edit the file `/etc/group` and add a line containing a “+” symbol at the end, to include all the NIS group entries.
- Reboot the system, to start and configure the networking.
- Check the network interface configuration. The command `ifconfig -a` should report something like:

```
ec0: flags=0832<UP,BROADCAST,NOTRAILERS,RUNNING,FILTMULTI,MULTICAST>
    inet 163.1.248.47 netmask 0xffffff00 broadcast 163.1.251.255
lo0: flags=1843<UP,LOOPBACK,RUNNING,MULTICAST,CKSUM>
    inet 127.0.0.1 netmask 0xff000000
```

The “inet” field for interface should show the correct IP address for the host. The other fields should appear exactly as shown.

Note that for some machines the primary network interface may not be called “ec0”.

- Check the routing table. The command `netstat -r` should report something like:

```
Routing tables
    Destination Gateway Flags MTU RTT RTTvar Use Interface
      localhost localhost UH 0 0 0 10410 lo0
    crick.physiol localhost UH 0 0 0 4152 lo0
      default router.physiol UG 0 0 0 170453 ec0
    physiol crick.physiol U 0 0.438 0.438 613164 ec0
BASE-ADDRESS.MCA crick.physiol U 0 0 0 3156 ec0
```

(the gateway field for the destination network “physiol” should be the name of the host).

- Add the following lines to `/etc/fstab`:

```bash
willis:/var/mail /var/mail nfs rw,bg,noac 0 0
willis:/home/willis /home/willis nfs rw,bg 0 0
willis:/usr/local /usr/local nfs rw,bg 0 0
willis:/usr/local/arch/mips-irix6/bin /usr/local/bin nfs rw,bg 0 0
willis:/usr/local/arch/mips-irix6/sbin /usr/local/sbin nfs rw,bg 0 0
willis:/usr/local/arch/mips-irix6/1ib /usr/local/lib nfs rw,bg 0 0
willis:/usr/local/arch/mips-irix6/include /usr/local/include nfs rw,bg 0 0
```

Add any other remote filesystems which you want to use to `/etc/fstab` using the same format.

Create empty directories `/usr/local` and `/home/willis` (and any other mount points that you require) if they do not already exist. Use the command `mount -a` to mount all the additional filesystems you have specified.
Use the command `mount` to check that the all the filesystems have been mounted correctly.

Run the following, so that the system uses the “message of the day” file from the file server:

```
rm /etc/motd
ln -s /usr/local/etc/motd /etc
```

Assuming that your home directory is on one of the filesystems which has been mounted, and that you have included yourself in the list of users allowed access to the system, it should now be possible to log in using your normal username. Logged in as a normal user you should now find that the software in `/usr/local/bin` is now accessible and working.

It should already be possible to read mail with any of the usual mail applications as a result of mounting the mail spool directory from Willis. Check that this works by sending yourself some mail on another system and reading it on the new system. Do not try sending mail from the new system at this stage.

Change directory to `/`. Run the command:

```
tar -xf /usr/local/etc/sgi-additions.tar
```

This creates the files needed for the xntpd daemon, installs a DNS resolver configuration file which points to the name server on Willis and changes the `/etc/TIMEZONE` file.

Run:

```
/usr/local/lib/sendmail.install
/usr/local/etc/ssh.setup
```

Reboot the system again. Check that the system date/time looks correct and ensure that the xntpd and sendmail daemons started and are working as expected.

Edit the `/etc/inetd.conf` file and comment out all the lines by prefixing each with a “#” symbol, then uncomment the services “sgi-dgl”, “sgi_fam”, “sgi_pcsd”. If the machine will be an NFS server then also uncomment “mountd”, “sgi_mountd” and “rstatd”.

### 4.2.4 Connecting a Linux Client

New Linux installations should be a recent release of the Red Hat Linux distribution. During the installation process choose the “workstation” profile, even if the machine will offer network services of some sort (the “server” profile installs every possible server software package that anyone could conceivably ever want — it is better to start with a smaller software base and add individual software components as required).
During installation set up the primary Ethernet interface to be configured via DHCP (post-installation this can be accomplished by running the utility `netconfig`).

Boot the machine and check that the network is configured appropriately (run `ifconfig -a` and check the address details listed for eth0, make sure that name resolution and networking are working by running something such as `ping willis`).

- Ensure that the portmap and ypbind services are turned on:
  ```
  chkconfig portmap on
  chkconfig ypbind on
  ```

- Edit `/etc/yp.conf` and add the line:
  ```
  domain physiol broadcast
  ```

- Edit `/etc/sysconfig/network` and add the line:
  ```
  NISDOMAIN=physiol
  ```

- Reboot the system and check that NIS is working. The command `ypwhich` should give the name of the NIS server to which the machine has bound. The command `ypcat passwd` should produce a listing of the Departmental passwd map, etc.

- NFS mount the Departmental Unix software directories, and run the installation script file in the `js` subdirectory of the Linux area:
  ```
  mount willis:/usr/local /usr/local
  /usr/local/arch/ix86-linux/js/install.sh
  ```

  Adds various files to the local system, ensures that various network services are turn off or on as appropriate, and generates SSH keys for the host if they do not already exist. If host keys are generated then the public keys should be added to the `/usr/local/etc/ssh_known_hosts` file on the file server.

- Reboot the system again. Check that the expected NFS filesystems have been mounted from the Departmental servers, and that daemons added in the previous step (such as `ntp` and `sshd`) have started.

- It should now be possible to add Departmental users to the system by adding `“+username”` or `“+@netgroup”` type entries to the `/etc/passwd` file.
4.2.5 Connecting a DOS Client

These instructions assume that you have a working, non-networked installation of DOS (and optionally Windows 3.1) already on the machine and that the machine has a high density 3.5" floppy drive.

It is also assumed that you are using a 3C509 network card with the default configuration (IRQ 10, I/O Base Address 0x300), that this card has been physically installed and that the default configuration does not cause any hardware conflicts.

- Obtain the customised BWNFS install disks from the draw labelled “Networking” on Tim’s desk.
- Put disk number 2 in the floppy drive.
- At a DOS prompt change drives to the floppy drive and run the command `setup`.
- When prompted, change the drives.
- When the process is finished, edit `c:\autoexec.bat` and `c:\config.sys` files. The `setup` program will have added some lines to the startup files. Ensure that the lines have been added in a reasonable place and tidy up.
- There will be a line in `autoexec.bat` of the form:

  `c:\bwtcp\bwnfs pc-name /d:10 /r:4096 /w:4096`

  Change the string “pc-name” to reflect the true name of the machine (there is a length limitation, so conventionally the bare name, without the “.physiol” qualification is used).

- Edit the line which sets the HOSTID environment variable and assign a value (details of the method used to derive the correct value are given in section 4.2.8).
- Reboot the machine, and test that you can log in and map drives in the normal fashion.
- If the machine runs Windows, start it and install the Beame and Whiteside program groups (Program Manager menus, File → New → Program Group and use the group files `BWAPPS.GRP` and `BWDAEMON.GRP`).

4.2.6 Connecting a Windows 95 Client

These instructions assume that you have a networking card which Windows 95 recognises and has provided a driver for.

- Open the Network control panel.
Go to the “Configuration” tab. You require the following networking components:

- The client “Client for Microsoft Networks”.
- The adaptor for the particular network card in use.
- The protocol “TCP/IP”.

Add any components which are missing and then remove any that are surplus to requirements (it is best do additions and removals in that order — higher level components tend to disappear if they have no lower level components to bind to).

Go to the “Identification” tab and enter the name of the computer (bare hostname, without “.physiol” part) and set the workgroup to “physiology”.

Set the “Primary Network Logon” to “Client for Microsoft Networks”.

Select the “Client for Microsoft Networks”. Click the button “Properties”. Tick the box “Log on to Window NT domain” and set the domain name to “physiology”. Click “OK”.

Select the “TCP/IP” protocol. Click the button “Properties”. Ensure that “Obtain address automatically” is selected under the “IP address” tab (this should be the default state). Go to the “DNS Configuration” tab, select “Enable DNS” and enter the hostname (unqualified) and DNS domain name “physiol.ox.ac.uk”. Click “OK”.

Click “OK” in the Network control panel. You will be asked if you want to reboot the machine. Click “Yes”.

When the machine comes back up it should start with the “Enter Network Password” login dialogue, with three editable fields; “Username”, “Password” and “Domain”. You should be able to log in using your normal username and password and have the logon batch file run.

From the Start menu run the command n:\netready. This sets various registry entries to the defaults we require, sets up the automatic downloading of a policy file from the network and sets the machine up correctly to run network software which is managed by the Lock Tools suite. You will be required to enter the unique HOSTID value for the machine (details of the method used to derive the correct value are given in section 4.2.8).

Restart the machine when prompted. Log in and out a couple of times, until the message noting that you haven’t logged in to the machine before and offering you the opportunity to store a personal profile appears (this shows that the machine has successfully downloaded the policy file and implemented the policies contained in it). Answer “Yes” to the question.

From the Start menu run the command n:\setfp. This installs the F-Provirus protection software.
4.2.7 Connecting a Windows 2000 or Windows XP Client

These instructions assume that you have a networking card which Windows recognises and has provided a driver for. Note that you need to be able to log in as an administrator to carry out the procedures listed below.

- Open the Network control panel and bring up the properties of the appropriate local area connection.
- Select the “TCP/IP” protocol. Click the button “Properties”. Ensure that “Obtain an IP address automatically” and “Obtain a DNS server address automatically” are selected. If you make any changes then you will be asked if you want to reboot the machine — click “Yes” in this instance.
- Check that the TCP/IP networking and DNS resolution is okay using ping, telnet, etc.
- Open the System control panel and go to the “Network Identification” tab and then click “Properties”. Enter the name of the computer (bare hostname, without “.physiol” part), click “More” and set the “Primary DNS Suffix” to “physiol.ox.ac.uk”. “OK” all the dialogue boxes and reboot to make the change effective.
- Re-open System control panel “Network Identification”, “Properties” dialogue. Change the “Domain” to “PHYSIOLOGY”. When prompted for the credentials of a user authorised to add computers to the domain, enter the username “root” and the corresponding password (this is a shared secret known to the Computer Officer and Computing Assistant, and is independent of the true root password on the domain controller). Reboot when prompted.
- Map \willis\pc-public as n: (remember that you need to specify a valid Departmental username in the “Connect As” field).
- From the Start menu run the command n:\netready, to install local customizations into the Registry and startup procedure. Restart again when prompted.
- From the Start menu run the command n:\setfp. This installs the F-Prot virus protection software. Enable automatic updates using an account with the domain “PHYSIOLOGY”, the username “sweepupd” and the corresponding password.

4.2.8 Deriving HOSTID For PC Clients

The environment variable HOSTID is used by the Lock Tools licence management system to identify the machine on which an application is running. It is a two character string, the characters must be valid for inclusion into a DOS style filename and each machine must use a unique value. As each machine
Table 4.1: “Shifted” Hexadecimal Digits

<table>
<thead>
<tr>
<th>Original digit</th>
<th>Shifted digit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>C</td>
</tr>
<tr>
<td>1</td>
<td>H</td>
</tr>
<tr>
<td>2</td>
<td>I</td>
</tr>
<tr>
<td>3</td>
<td>J</td>
</tr>
<tr>
<td>4</td>
<td>K</td>
</tr>
<tr>
<td>5</td>
<td>L</td>
</tr>
<tr>
<td>6</td>
<td>M</td>
</tr>
<tr>
<td>7</td>
<td>N</td>
</tr>
<tr>
<td>8</td>
<td>O</td>
</tr>
<tr>
<td>9</td>
<td>P</td>
</tr>
<tr>
<td>A</td>
<td>Q</td>
</tr>
<tr>
<td>B</td>
<td>R</td>
</tr>
<tr>
<td>C</td>
<td>S</td>
</tr>
<tr>
<td>D</td>
<td>T</td>
</tr>
<tr>
<td>E</td>
<td>U</td>
</tr>
<tr>
<td>F</td>
<td>V</td>
</tr>
</tbody>
</table>

is already assigned a unique IP address the HOSTID is derived from the IP address, encoded such that it will fit into two characters.

The parameters of our network are such that all the IP addresses fall into one of four adjacent ranges:

- 163.1.248.1 – 163.1.248.255
- 163.1.249.0 – 163.1.249.255
- 163.1.250.0 – 163.1.250.255
- 163.1.251.0 – 163.1.251.254

The IP address of a PC is turned into a HOSTID as follows:

- The least significant byte of the address is written as a two digit hexadecimal number.
- In the case of a 163.1.248.X address this number is the HOSTID.
- In the case of a 163.1.249.X address the first digit is replaced by a “shifted” representation. See table 4.1.
- In the case of a 163.1.250.X address the “shift” is applied to the second digit, rather than the first.
- In the case of a 163.1.251.X address the “shift” is applied to both the digits.

Table 4.2 summarizes the “number” ranges that these rules produce.
### Table 4.2: HOSTID “number” ranges

<table>
<thead>
<tr>
<th>IP address</th>
<th>HOSTID range</th>
</tr>
</thead>
<tbody>
<tr>
<td>163.1.248.X</td>
<td>00 -- FF</td>
</tr>
<tr>
<td>163.1.249.X</td>
<td>G0 -- VF</td>
</tr>
<tr>
<td>163.1.250.X</td>
<td>G0 -- FV</td>
</tr>
<tr>
<td>163.1.251.X</td>
<td>GG -- VV</td>
</tr>
</tbody>
</table>

#### 4.2.9 Connecting a Macintosh

- Open the “Network” control panel (“AppleTalk” control panel in System 7.5.2 or later). Ensure that AppleTalk services are going via Ethernet.

- An Apple Macintosh with a network connection should be able to connect to the AppleShare file service on Willis using the Chooser. Log on with your normal username and password.

- Select both the “Home Directory” and “Network Resources” volumes, and tick the boxes to have them remounted at startup.

- Drag the folder “Network Applications” from the “Network Resources” volume to the hard disk.

- Open the “MacTCP” control panel (“TCP/IP” control panel in System 7.5.2 or later). Select Ethernet and configure the machine to obtain its IP configuration via DHCP (or BOOTP, on older Macs that lack a DHCP option).

#### 4.2.10 Connecting Other Devices

Devices which do not fit into any of the above categories can be connected to the network — obviously no item by item procedures can be given which cover all the possibilities. The procedures for connecting the established types of machine can be used as a guide to what needs to be done, in conjunction with whatever documentation is provided with the device. An outline to basic network configuration is:

- The device should be registered in the various databases, like any other.

- If an IP capability is required configuration of the various IP parameters should be done via BOOTP/DHCP, if possible.

- If BOOTP/DHCP configuration is not an option then the device should, if possible, use RARP to establish its own IP address at startup (if the device needs to communicate off the local network or use IP broadcasts then additional manual configuration of netmask, gateway, etc. will probably be required).
If the device supports neither BOOTP/DHCP nor RARP it needs to be manually set up with the assigned IP address and the basic IP parameters of our network.

If the device is able to make use of NFS, SMB or AppleShare file services then it may be configured to connect to the Departmental file server (in the case of NFS access Computing must be satisfied that the device implements an adequate security model before this will be permitted).

4.3 Managing User Accounts

4.3.1 Creating a New User Account

- Check out an editable copy of the people file.
- Add a new entry at the end of the file for the new user. There are twelve fields on a line, separated by colons.

  - **username** Normally the initials of the person owning the account. Remember to search the file for the chosen string, to check that the given username is not already in use.
  - **status** Normally you would use the string “NEW”, unless the user is actually present and ready to set a password immediately, in which case you would use “ACTIVE”.
  - **uid** Add one to the uid number of the preceding line. The file is supposed to be sorted in uid order, so there should be no problems with clashes, but it is prudent to do a string search for the given uid to ensure that it is unique.
  - **gid** Users are normally assigned default group 110 (physiol).
  - **full name** The full name of the user (middle names and initials normally omitted).
  - **home directory** Home directory for the NIS passwd map. Normally /home/willis/username.
  - **BWNFS home directory** Resource mapped as p: by bwlogin. Normally \willis\home\willis\username.
  - **BWNFS file mode** Default value for Unix permission mode used for files created by BWNFS. Usual value is 755 (user read, write and execute; group read and execute; other read and execute).
  - **flags** Normally blank (insert the string “WillisUser” to grant permission for interactive logins to Willis).
  - **netgroups** This field should be blank (as Acorn used to say in cryptic fashion throughout their manuals “Reserved for future use”).
  - **quota** Normally blank (indicating default Willis quotas).
Some form of identification for the person (so that they can be tracked down at some point in the future when we’ve forgotten who they were and why we gave them an account). Sometimes a job title is given, often the research group with which the user is associated is used (initials of supervisor).

Save and quit.

- Check in the people file, entering a suitable comment (“added user xyz for the Bloggs group”).
- Change directory to /var/yp, su to an admin account and and run make to update the NIS.
- Run the command:

  /usr/local/etc/default_setup username

  Note that all users must have a /home/willis/username directory, even if their principle home directory (listed in the NIS) is elsewhere.
- If the user is present, and you set the status field in the people file to ACTIVE, they should set a password. Refer to section 4.3.2.
- Register the user with OUCS for e-mail. Send a message to registration@oucs.ox.ac.uk of the following form:

  Dear User Registration,
  Could you add e-mail routing for a new user in Physiology, please?
  Full name: Fred A Bloggs
  University Card No: 2118108
  Address: fred.bloggs@physiol.ox.ac.uk
  Outgoing address: fab@physiol.ox.ac.uk
  Deliver to: fab@mail.physiol.ox.ac.uk

  E-mail should start working for the new user the following morning (assuming the request gets acted on today, which is by no means certain).
  The delivery address might not be username@mail — it depends on the preference of the user, but if they don’t express a desire to have their mail elsewhere this is the default choice.

4.3.2 Enabling a User Account

The user must be standing by to set a password.

- Check out the people file.
- Find the line in the file which relates to the user concerned and change the status field (second on the line) to read “ACTIVE”.

79
• Check the file back in (supplying a suitable comment), su to an admin account and run `make` in the `/var/yp` directory.

• SSH to “willis.physiol.ox.ac.uk” and log in under the user’s username.

• Choose the option “Change your network password”.

• Get the user to type the password of their choice. Caution the user against selecting “bad” passwords, such as names, dictionary words, dates, car registration numbers or similar personal information.

### 4.3.3 Closing a User Account

• Check out the `people` file.

• Find the line in the file which relates to the user concerned and change the status field (second on the line) to read “OLD”.

• Check the file back in, supplying a suitable comment (eg. “closed username account - user left department”).

• su to an admin account and run `make` in the `/var/yp` directory.

### 4.4 Restoring Files From Backup

#### 4.4.1 Restoring From Local Backup Tape

Before attempting to restore files from backup make sure that you properly understand the description of the backup cycles given in section 3.8.

Identify the tape or tapes that you need for the restore. To restore files to the state that they were on some evening of the last week you require the incremental (“Monday” – “Thursday”) tape in question and the full backup (dated or “Week X” Friday) tapes which preceded that incremental. If going back further than a week, identify the full backup tapes which is most likely to capture the state in which you are interested.

Identify the dump record number for the particular filesystem in which you are interested (refer to table 3.3).

The restored files can be brought back either in their original location or in some temporary location (to avoid overwriting the current versions). In the first case you need to make the root of the filesystem involved the current directory (so, for example, if restoring files on `/home/willis` run `cd /home/willis`). In the second case you need to make some temporary location the current directory (such as `/tmp` or `/var/tmp`). Ensure that the filesystem you choose has enough space to accommodate the files you intend to bring back. If you use `/tmp` remember that on Willis this is a tmpfs memory based filesystem; it is the amount of free swap space that you need to be concerned about.
Files are restored with the `ufsrestore` command. Note that the Willis L8 tape library is device `/dev/rmt/1`, and you will need to specify this device to `ufsrestore` with an `-f` option. You need to position the at the appropriate record by add the `-s dumpnumber` option to your `ufsrestore` command line. To restore the entire contents of filesystem, use `ufsrestore -r`. To restore interactively a selected file or files use `ufsrestore -i` (the program will read the first part of the dump to get the directory structure and then present you with a prompt — navigate your way round the dump archive with `cd` and `ls`, add the files that you require to the list of those to be extracted using `add` and start the extraction process with the command `extract`).

So, putting it all together to provide a concrete example, if you are restoring from the third record of a tape, and want to interactively choose some files or directories from the backup, then the `ufsrestore` command line would look like this:

```
ufsrestore -isf 3 /dev/rmt/1
```

If you use interactive mode then at the end of the restore process you will be asked the question “Set owner/mode for . (y/n)?”. **Answer “no” to this question!** If you answer “yes” then the permissions on the current directory will get changed, typically such that normal users can’t write there. If you are restoring in somewhere like `/tmp` then this can cause chaos!

If you are doing a full restore and have an incremental tape as well as a full backup tape then restore the full backup tape first and then repeat the process with the incremental tape. Note that this doesn’t quite put the filesystem back to its original state — any files present at the time of the full backup and deleted between that time and the taking of the incremental backup will have been “reincarnated” by the restore process.

If you are restoring a few selected files and have reason to believe that the files in question might have been modified between the full backup and the incremental backup then you may be able to save time by going straight to `ufsrestore -i` on the incremental tape. If everything you want is on that tape then you can just extract the file or files directly, without having to bother with restoring from the full backup.

### 4.4.2 Restoring From The HFS

- To restore a named file to its original location:
  
  `dsmc restore <pathname-of-file>`

- To restore a named file to a new location:
  
  `dsmc restore <original-pathname> <new-pathname>`

- To restore a directory tree:
dsmc restore -subdir=yes '<pathname-of-directory>/*'

Consult the online help in the dsmc program for details of more involved operations, such as restoring the version of a file previous to the current version (the HFS software calls this the “inactive” instance of the file).

4.5 Shutting Down or Rebooting Willis or Wren

Correct shutdown procedures must be followed if the file server needs to be switched off for some reason.

A reboot is sometimes required after a major change to the configuration of the machine, installation of new system software or patches, etc. A reboot might also be used as a last resort to attempt to sort things out if the system is behaving erratically and no other fix can be found (the instructions which follow assume this circumstance — attempting to ensure a safe close down while relying on as little as possible of the system working correctly).

The instructions which follow are equally applicable to any of the other Departmental Sun machines.

Normally the Willis console runs an X server and the CDE login manager. Make sure that the monitor is switched on (button and power LED bottom right hand side of the screen) and press Shift to wake up the X screen saver.

If the system is in some sort of trouble then the less of the system that you rely upon the more likely you are to get a to a usable command line. To this end: open the “Options” menu and choose the “Command Line Login” item, hit return to get a login prompt, then log in as root directly using an admin account (don’t use a usual username followed by su).

To reboot, ensure that you are in the root directory and type:

```
/sbin/init 6
```

This should shutdown the system and then initiate an auto reboot to the multi-user state. In place of “6” there are other “run levels” which can be used:

```
init 0 Shutdown to boot PROM. Safe to turn the power off.
init 1 Bring the system to the “administrative state”. Most of the services are shut down but the appropriate file systems are mounted, as though the system was about to go to the multi-user state.
init 5 Shutdown the operating system and power down the system.
init s Single user state. Before going single user the system prompts you for the root password. You need to supply the real root password. An admin account password will not do.
```
If you cannot log in to an admin account then hold down the key marked Stop (top left hand of the keyboard) and press A. This should drop you straight into the boot PROM monitor program (the same effect can be triggered by unplugging and reconnecting the keyboard). From the PROM monitor “ok” prompt you should immediately type “sync” and press “Return”. This attempts to flush any dirty filesystem buffers back to the disks and then reboots the machine to the multi-user state without further intervention. The other PROM monitor command which might be of relevance is “boot” — this does what the name suggests!

4.5.1 Alternative Boot Devices

In the event that the internal disk has failed the system will not be able to boot automatically. The root filesystem is mirrored on both Willis and Wren, however, so there are alternative boot commands that you can use to attempt to start the system at the “ok” prompt:

- `boot /pci@8,600000/scsi@1/disk@1`
- `boot /pci@8,600000/scsi@1,1/disk@1`

Both mirror devices are present on Willis, only the latter is present on Wren. Labels have been attached to both machines giving the alternative device paths suitable for booting.

4.6 Hardware Problems and Maintenance Contracts

4.6.1 Calling Sun Service

System serial numbers for the machines covered by the Sun support contract are listed in table 4.3. This includes the main file server (hostname “Willis”) and the reserve file server (hostname “Hooke”). In addition to the systems themselves, the support contract also covers any genuine Sun peripheral connected to one of the machines.

Telephone 01276 691974. You will be asked for the system serial number, whether the problem is hardware or software related and a brief description of the problem. Different priority levels can be assigned to calls and Sun aim to deliver different response times depending on the customer’s own assessment of the priority. In the event of a serious problem with Willis and Wren be sure to impress on the Sun representative taking the problem description that this is an “Urgent” call — the support contract specifies a 4 hour on-site response in such cases. You should be ready to note down the call reference number which you will be assigned after you have described the problem (if you need to call back subsequently concerning the same problem quote the call reference rather than the serial number).
Table 4.3: Sun system serial numbers

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Serial</th>
<th>Model</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hal</td>
<td>726M0390</td>
<td>Ultra 1/140</td>
<td>Department</td>
</tr>
<tr>
<td>Hooke</td>
<td>649M0168</td>
<td>Ultra 1/140</td>
<td>Department</td>
</tr>
<tr>
<td>Marr</td>
<td>TW90400278</td>
<td>Ultra 10</td>
<td>AJP</td>
</tr>
<tr>
<td>Saros</td>
<td>724MC493</td>
<td>Ultra 30</td>
<td>McDonnell-Pew</td>
</tr>
<tr>
<td>Ull</td>
<td>714MC4BD</td>
<td>Ultra 30</td>
<td>JFS/RCM</td>
</tr>
<tr>
<td>Valhalla</td>
<td>713M0153</td>
<td>Ultra 1/140</td>
<td>JFS/RCM</td>
</tr>
<tr>
<td>Wheatstone</td>
<td>TW95078493</td>
<td>Ultra 10</td>
<td>AJP</td>
</tr>
<tr>
<td>Willis</td>
<td>045A0F83</td>
<td>SunBlade 1000</td>
<td>Department</td>
</tr>
<tr>
<td>Wren</td>
<td>045A0F94</td>
<td>SunBlade 1000</td>
<td>Department</td>
</tr>
</tbody>
</table>

General practice for routine software support (operating system patches, etc) is to go through Malcolm Harper at the Computing Laboratory. Mr Harper has access to the SunSolve Online database and can FTP patches and similar material from Sun directly.

4.6.2 Calling SGI Support

We no longer have SGI hardware support.

4.6.3 Network Maintenance

There is little in the way of operational procedure to be observed concerning the network hardware — the switches and hubs normally run without needing any attention. The manuals and installation guides for the networking hardware are on the book shelf in B75. In the event of network problems it is safe to try turning the equipment off and then powering it back up. There are no special shutdown procedures to be observed and all the equipment should self test and restart, restoring configuration from non-volatile RAM.

The equipment is covered by a maintenance agreement with OUCS. Details of the equipment covered is in tables below. In the event of network hardware failure, telephone OUCS Network Control on 73268 to arrange a swap of the defective unit.

In order to minimize the duration of a network outage the failed equipment will typically be replaced by a Departmental spare of the same model, taken from the Computing Office (Rm A37), and the failed equipment then exchanged with OUCS under the Network Support Agreement (though the support agreement promises exchange within four working hours, Monday-Friday, 08:30-17:30, so direct replacement of the failed equipment should also prove relatively timely, in the event of a Departmental spare being unavailable).
<table>
<thead>
<tr>
<th>Model</th>
<th>Serial</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>3C16980</td>
<td>7ZNV2278D98</td>
<td>east switch</td>
</tr>
<tr>
<td>3C16970</td>
<td>7ZNSB78130</td>
<td>100BASE-FX module</td>
</tr>
<tr>
<td>3C16671</td>
<td>7HYR139263</td>
<td>east-ground segment</td>
</tr>
<tr>
<td>3C16671</td>
<td>7GWV206096</td>
<td>east-ground segment</td>
</tr>
<tr>
<td>3C16671</td>
<td>7HYR139242</td>
<td>east-ground segment</td>
</tr>
<tr>
<td>3C16671</td>
<td>7GWV206026</td>
<td>east-1st-a segment</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>10BASE-FL module</td>
</tr>
<tr>
<td>3C16671</td>
<td>7HYR139266</td>
<td>east-1st-b segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV44590</td>
<td>east-2nd segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV44366</td>
<td>east-2nd segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV443c34</td>
<td>east-3nd segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV44523d</td>
<td>east-3nd segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV4afe94</td>
<td>east-3nd segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV4452bd</td>
<td>Parker segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV45095</td>
<td>Parker segment</td>
</tr>
<tr>
<td>3C16980</td>
<td>7ZNV1A717B8</td>
<td>Steinlab switch</td>
</tr>
<tr>
<td>3C16980</td>
<td>7ZNV788038</td>
<td>steinlab switch</td>
</tr>
<tr>
<td>3C16980A</td>
<td>7MMV5758ab8</td>
<td>Moore/Blakemore switch</td>
</tr>
<tr>
<td>3C16980A</td>
<td>7MMV62c1118</td>
<td>Thompson switch</td>
</tr>
</tbody>
</table>

Table 4.4: Network equipment serial numbers — Distribution Point 1 (Rm A62)

<table>
<thead>
<tr>
<th>Model</th>
<th>Serial</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>3C16980</td>
<td>7ZNV1a57d58</td>
<td>west switch</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV29670</td>
<td>west-ground segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV44734</td>
<td>west-ground segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV27332d</td>
<td>west-ground segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV4b2e16</td>
<td>west-mri segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV36a60</td>
<td>west-1st segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV296920</td>
<td>west-1st segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV2723490</td>
<td>west-2nd segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV35560</td>
<td>west-2nd segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV442b0</td>
<td>west-2nd segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV4af2f</td>
<td>west-2nd segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV27234bd</td>
<td>west-2nd segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV3bf60</td>
<td>west-3rd segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV28a49c</td>
<td>west-3rd segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV3bf640</td>
<td>west-3rd segment</td>
</tr>
<tr>
<td>3C16406</td>
<td>7TSV4af22f</td>
<td>west-3rd segment</td>
</tr>
<tr>
<td>3C16980A</td>
<td>7MMV5758b38</td>
<td>Vaughan-Jones switch</td>
</tr>
<tr>
<td>3C16980</td>
<td>7ZNV3907bb8</td>
<td>Noble switch</td>
</tr>
<tr>
<td>3C16980</td>
<td>7ZNV4a95998</td>
<td>Robbins switch</td>
</tr>
<tr>
<td>3C16980</td>
<td>7ZNV4a9278</td>
<td>Robbins switch</td>
</tr>
<tr>
<td>3C16980</td>
<td>7ZNV46e0d38</td>
<td>Paterson switch</td>
</tr>
<tr>
<td>3C16980A</td>
<td>7MMV65ba9f8</td>
<td>Paterson switch</td>
</tr>
</tbody>
</table>

Table 4.5: Network equipment serial numbers — distribution point 2 (Rm B25)
### Table 4.6: Network equipment serial numbers — distribution point 3 (Rm A65)

<table>
<thead>
<tr>
<th>Model</th>
<th>Serial</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>3C17204</td>
<td>7NPVI77768e40</td>
<td>Neuro-extension switch</td>
</tr>
<tr>
<td>3C17204</td>
<td>7NPVI77a6bc0</td>
<td>Neuro-extension switch</td>
</tr>
<tr>
<td>3C17204</td>
<td>7NPVI77a6580</td>
<td>Neuro-extension switch</td>
</tr>
<tr>
<td>3C17204</td>
<td>7NPVI77a5140</td>
<td>Neuro-extension switch</td>
</tr>
</tbody>
</table>

### Table 4.7: Network equipment serial numbers — old observatory (Rm 414)

<table>
<thead>
<tr>
<th>Model</th>
<th>Serial</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>3C16671</td>
<td>7HYR139227</td>
<td>east-1st-a segment</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>10BASE-FL module</td>
</tr>
</tbody>
</table>

86
Bibliography