Chapter 9:
Dealing with problems

9.1 Overview

The important thing to remember is that computers do crash. Even assuming no software bugs and perfectly working hardware, accidents can and will still happen. Power cuts are a major cause of problems, with lightning a close second.

The first rule to remember is **take frequent back-ups**. This applies especially to Econet File Servers, where the users themselves have absolutely no control over their file integrity. In many cases a File Server may be your only mass storage device. Sooner or later **IT WILL FAIL**. The only guarantee against disaster is to take a back-up every day.

Reliability of the File Server can be improved in other ways too. The ideal environment is a firm shelf in a well ventilated position, out of direct sunlight, where people are unable to shake the machine. If possible the File Server should be left switched on at all times. Winchester discs are most likely to be damaged during the critical power-on sequence, when the heads are not flying in the normal way but are rubbing on the surface of the disc.

9.2 What to do if the File Server crashes

The most likely symptom is all the computers attempting to access the File Server return the error **Not listening** or **Station 254 not present**. If *any* machines are still communicating with the File Server then it is a not a problem with the File Server.

If the performance of the machine varies on its position in the network then suspect the clock speed. A standard problem is that a BBC machine has problems loading a large file, this is because the clock is running too fast or too slow. Check that both terminators are plugged into the far ends of the network. Similar problems may occur if the network has been installed with long spurs : see section 9.4 for debugging a correctly installed network, see the clock manual for installing a network for the first time.

Press the release disc button, if this has no observable effect then turn the MDFS off at the keyswitch. Restart the File Server, make a backup copy of the File Server discs then telephone SJ Research to report the problem.

9.2.1 Mains Electricity

It is always worthwhile checking mains installation if you are getting computers crashing or line-drivers blowing. A simple and cheap tester can be obtained from RS components, part number 424-709. This device can be used to test all sockets, including mains extension leads.

9.3 Network security

This section deals with the problems of protecting data on Econet systems generally and on SJ Research File Servers in particular.

There are two separate areas to be considered, accidental and deliberate interference. Accidental problems can be further subdivided into *mistakes* by the users such as saving one program over another, or deleting too many files with an injudicious wildcard; and *external accidents* such as turning off the File Server at the wrong time or a lightning strike. Deliberate interference also divides into two categories: *snooping* or passive activities to gain access to other people's data, and *wrecking* or active alteration of the data.

9.3.1 Accidents

No-one can guard against mistakes completely but users can easily be protected from many of the more

common errors.

The most common ways that beginners lose files are:

1. Saving over a file with a new program of the same name.
2. Saving a *null* program (in the case of Basic this will be two bytes long) because they have not typed **OLD** after pressing <Break>.
3. Using wildcards in a delete statement with more effect than intended.

Encourage users to use names which are meaningful. Ten characters is enough to choose a sensible name, especially if the use of hyphens and underlines is encouraged.

Suggest that users check their saves with a ***INFO <filename>** after each save, and explain how to check the file length. Alternatively use ***OPT 1,1** to display this information automatically.

Beginners can be given a lot of protection by initially giving their directory a default access which is locked (for example ***DEFACCESS LWR/**). The disadvantage of this is that it is then necessary to type ***ACCESS <filename> -L** before a new version can be saved over the existing one. If you plan to use programs like EDWORD which do not allow * commands then this is a disaster!

Beginners may also appreciate the **No Short Saves** option which can be set by the system manager using the EDITPASS program. There is also an option to require the use of ***ENABLE** before any wild card delete operation is permitted.

9.3.2 Recovering from Mistakes

Lost files can be recovered fairly readily if the system manager has been careful about taking regular backup discs (using the system in Utility Mode). It is recommended that copies of all current discs are taken weekly (more often if there is critical data), and stored in a safe, preferably locked, place. It then becomes relatively simple to insert the backup disc, recover the lost file from it, then remove and put away the backup again.

Backup discs may be used in rotation, but there is a lot to be said for keeping long term archive discs as well. The reason for this is that it may not become apparent that a file has been lost or corrupted until some considerable time has elapsed, and that all the backups may have been rotated through the system by then.

9.3.3 Deliberate Interference

Care When Logging On

One of the most common security hazards is using an unprotected machine. Before doing anything sensitive, remember to run *PROT on your computer. In particular, this is worth doing BEFORE logging on as a system privileged user. If you do not do this, your memory can be examined by any other machine with the appropriate software. (Note that this problem is not specific to SJ Research File Servers, and indeed remains a problem even if there is no File Server on the network at all.) Protected status is cleared by <Ctrl-Break>.

Remembering to Log Off After a Session

The File Server and your local station both store information about you. Pressing <Ctrl-Break> or even switching off your local machine will not affect the File Server's status, so that only a small amount of trial and error will allow another user to re-enter the system from the same terminal (you can show this to be so by switching off your own terminal and typing '*USERS' from another machine.). **It is essential for any user who is concerned about security to type *BYE before leaving his terminal.**

It is also good practice to turn off your machine after a session, in case any secret information has been left lying around in RAM (the EDITPASS program is a good example of this).

Passwords

If a user gains access to your files in a *legal* way, there is very little that you can do about it (but see the next section for one way of limiting the damage.)

The difficulty in ascertaining someone's password by trial and error increases rapidly with the number of letters in the password. Remember too that numbers and other non-alphabetic keys (!,-,_,(,) etc) can be used. The password is governed by the same restrictions as for filenames. All passwords should be at least five letters long, preferably more. The maximum length is ten characters. Users should not use passwords which might be guessed easily by others (do not use your wife's name, phone number or car number, nor do we recommend the use of characters from Tolkien, 2000AD or Hitch-hiker's !).

Take care that you do not leave your system unprotected whilst you are still learning it: it is very hard to re-establish security once it has been broken. One enterprising hacker managed to add a command to EDITPASS, to save a copy of the password file into his own directory. By placing a <ctrl-U> character before and a <ctrl-F> character after his code, he ensured that it would not be listed on the screen of a BBC Micro.

Keys and Key Discs

The Modular Disc File Server requires the key switch on its front panel to be turned to the SYST position before any system privileged operations are permitted. Make use of this feature all the time, ensuring that you do not leave the key in the SYST position if you do not require system operations.

The File Server can be further protected from unauthorised use by having only one (or a few) discs on which system privileged users exist in the password file. These discs can be kept locked up except when system operations are required. Before performing a system privileged operation press the RELEASE DISCS button and change one of the discs for that containing the system user(s).

Snooping and Wrecking

Provided that passwords do not fall into the wrong hands, the opportunities for deliberate meddling can be fairly limited. Obviously it is useful to make all sensitive areas of the disc **Private**. Non-private directories can also be made reasonably secure by setting the access to **WR/**. Note that if the Default access includes public access, there will always be a period during the creation of a new file when other people can read it, even if it is then rapidly set to WR/.

Care when not using the network

Remember that the network is still active, even if you are not using it. For example if you are editing files to a local disc, your screen can still be viewed ! This could have serious consequences if you were writing exam papers, for example. Use the program *PROT (preferably in your boot file where it will be run every time you log on) to avoid all but the most dedicated hacker. The 100% safe way to avoid hacking is to unplug your system from the network when doing work of a particularly sensitive nature.

9.3.4 Special Techniques

Limiting the Opportunity for Damage

Editing the password file may only take place when the File Server key-switch is in the system position. This editing allows a system privileged key-holder to remove everyone's access to a particular account (including his own access) and then *lock* the password file. In this state, no-one may access private files that have been saved in that account, not even the key-holder. The password file will have to be re-edited to enable access again. This technique may have some use for files which are frequently read but only rarely changed (e.g. libraries or time-table information), which may be made WR/R and saved into an account which is not normally accessible. Take care not to remove your own access (as system manager) to account 0, otherwise you will not be able to edit the password file.

Restricting read access to files and restricting write access more.

General Principle: Allocate two accounts, one for read access only and one for full read-write access.

Create a private directory in the Write account, with auxiliary access in the Read account and Defaccess WR/R. Only those users with access to one or other (or both) of the two accounts will be able to see or enter this directory.

When a new file is created within this directory, set the auxiliary account to the write account, thereby removing from the read account the owner access to the files, giving them intermediate, *read-only* access rights.

Example: Pupil Reports are required to be available for inspection by any member of staff, but only the master in charge should be able to alter them. The master in charge should have accounts 2 and 3, the other staff account 3, and the rest of the users access to neither account.

Method:
1. The creator selects the place where he wishes the new directory to appear.
2. *CDIR reports
3. *ACCOUNT reports 02 (03)
4. *ACCESS reports +P
5. *DIR reports
6. *DEFACCESS WR/R

The directory is now ready for use. When saving a new file, type:

7. *SAVE <file name> 0+0
8. *ACCOUNT <file name> (2)

then save the file you want as <file name>. This avoids a malicious user writing to the file between it being saved and its access being changed.

9.4 Debugging the network hardware

This Section contains a guide to finding faults on an Econet system.

If you are having problems which result in no communication at all, or only unreliable communication between computers on the network, then follow this procedure:

1. Unplug everything from the network, and make a very small network comprising one BBC Microcomputer, the Econet clock, a File Server and one terminator, with the necessary leads and adaptors to connect them all together. Open the clock box and turn on PERIOD switches 4 and 5 (marked 2 us and 4 us respectively) and turn on MARK switch 4 (marked 1 us). All other switches should be off.

2. Hold down letter N on the BBC Microcomputer, and press and release <Break>, then release N. This should appear at the top of the screen

```
BBC Microcomputer

Econet station nnn

BASIC

>
```

If the second line reads **Econet station nnn No clock**, then suspect the clock, but first try the same experiment with different connecting leads and a different BBC Microcomputer. Check the clock by plugging it directly into the Econet socket of the File Server and find whether the **No clock** light goes out.

3. If the BBC Microcomputer does not give a **No clock** message, then try logging on to the File Server with the command ***I AM 0.254 <user id.>**. If there is a pause of about a minute, followed by **Not listening** or **Line jammed**, then continue on to step 4. If there is a prompt > after a short period, or an error message like **User not known** or **Incorrect password**, then you can conclude that the File Server and one BBC Microcomputer are functioning correctly, and proceed to step 7.

4. Reset the File Server station number to 254 as described in Section 7.4 (This step does not apply to RM380Z File Servers, but the Econet card in the RM380Z should be checked, to make sure that its station identifier links are correct.) Try logging on again as described in step 3 -- if this now functions, the File Server real-time clock had failed, either because the unit had not been switched on for more than about 6 months, or because of a hardware fault (contact your dealer or SJ Research in this case). Note that you will have to reset the time (and on the FDFS, the Baud rate) after this step. If the File Server now functions, proceed to step 7, otherwise continue.

5. Check the installation and operating instructions for the File Server to check that all has been done correctly. If you still cannot log on, then contact your dealer or SJ Research for advice.

6. It is still possible to check the network communication without a File Server. You will have to key in the following short program, which checks that the network and Econet interfaces function correctly. It can also be used to check an Acorn Level 2 File Server hardware, by stopping the program, then pressing <Ctrl-Break> on the File Server computer.

Key in this program (you do not of course need the REM statements):

```
 10REM Program to test Econet
 20
 30 DIM X% 20
 40REPEAT
 50 INPUT "Station to test : "stn%
 60 Y%=X% DIV 256
 70 ?X%=1
 80REM this is the reason code for 'send string'
 90 X%?1=stn% : X%?2=0
100REM X%?2 = network number for multiple networks
110 $(X%+3)="*| Are you there ??"
120 A%=&14
130 CALL &FFF1 : REM Osword
140UNTIL FALSE
```

It would be wise to save this program, and also NETMON and STATIONS (if you have managed to get them off the File Server) on to local disc or cassette.

The program will repeatedly prompt for station numbers, and will execute the same call that *NOTIFY uses, sending string **Are you there ??** to each station specified. The target station must have its protection byte *unset* -- the easiest way to do this on a BBC microcomputer is to press <Ctrl-Break> on every station. For Masters and Econet Terminals the ***UNPROT** command is available.

Start with only two BBC Microcomputers on a short network with just the clock, one terminator, and connecting leads and adaptors. Check that you can send the message from one to the other. Sending the message only one way in fact causes a bi-directional communication, so fully tests both network interfaces.

Possible errors are (note that some of these errors only appear after the computer has been trying for about a minute):

`No clock`	You should have checked this already by pressing <N-Break> on each computer (see step 2).
`Net error` or `Line jammed`	First try unplugging the terminator, and replacing it with the other one. If this does not cure the problem, then try replacing the connecting leads one at a time. Finally, replace the BBC Microcomputers one at a time. If you still cannot make contact between any two computers, check that you do not have any consistency errors: check that your connecting leads are wired pin 1 to pin 1 etc. (it is easiest to do this with a multimeter and an assistant), and ensure that whoever did the Econet upgrades to your BBC Microcomputers ran the full test (using a special Econet tester). If the network has worked in the past, it is possible that a lightning strike or large transient mains voltage pulse has destroyed all the SN75159 Econet line driver chips -- replace one or two and try the test again.
`Not listening`	Check first that the protection byte is not set, by typing <Ctrl-Break> on the destination computer, and re-run the program. If it still fails, follow the instructions under Net error.

If some or all of the BBC Microcomputers fail to communicate, then try new SN75159 Econet line driver chips (the chip should be in a socket). They can blow if there is a large transient voltage pulse on the network, such as that due to a local lightning strike.

To help avoid a repetition of this, SJ Research sell transient suppressor boxes to absorb transients of this type, and protect the computers.

7. If some or all of the BBC Microcomputers function in the very short network, but not in the main network, then first check that the network connections are all correct. The easiest way to do this is with a multimeter (set to an ohms range) and a special DIN plug wired with resistors as shown in Fig. 1 below.

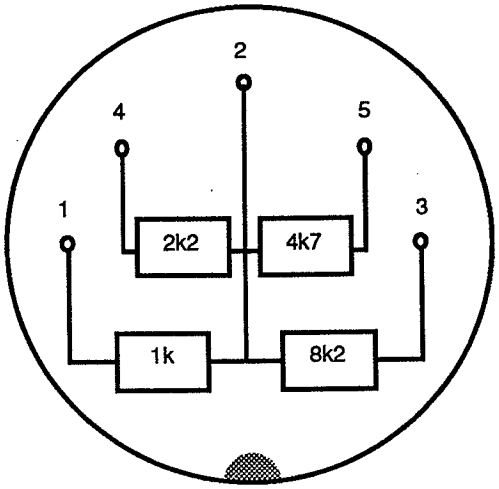

Fig 1 Test Plug (viewed from solder side)

Unplug the clock, terminators and all computers (including the File Server). Plug the test plug into a socket in the network. At each socket outlet on the network poke one of the prods into the centre pin (pin 2) of the DIN socket. Then check that the resistances are as follows:

pin 1 to pin 2 1k
pin 4 to pin 2 2k2
pin 5 to pin 2 4k7
pin 3 to pin 2 8k2

If any of these measured resistances differ significantly from these values, suspect an open or short circuit in the network. Remember that the network is split in the middle at the clock box, so the test plug will have to be plugged in on one side, and then on the other.