

Local Area Network Management

Introduction

This document discusses the tasks associated with management of Local Area Networks (LANs). All LANs require regular administration and management in order to function efficiently and effectively. A Network Administrator is required to perform a range of duties in order to achieve this efficiency and effectiveness. These include maintaining system security, implementing backup strategies, installing software, upgrading software, managing data storage and ensuring provision of virus protection.

Training Administrators

In some cases, schools may choose to retrain existing staff to take on the role of Network Administrator. Other schools may choose to outsource this service. Schools may also wish to develop their own support networks within local groups and via e-mail through the Internet to share ideas and experiences regarding computer network administration. Your District Technology Adviser can also offer advice in this area.

If the school intends to take on the network administration tasks itself, an appropriate training course for the school Network Administrator is desirable. Specific *Network Administrator* training courses are available for various network platforms (Novell Netware, Windows NT Advanced Server, Apple Macintosh Workgroup Server etc). These are normally provided by commercial training centres, and in some cases, accreditation is available. Some TAFE colleges also offer similar training courses however these are normally spread out over a longer period of time.

The school may wish to consider using funding for the Computer Coordinator resource as a way to support management of the computer network in this way.

The use of a second or third person to shadow the main network administrator or the sharing of administration tasks among two or three staff will reduce the dependency on one person in the school. Situations where only one administrator is managing the whole network should be avoided. In the case where this person leaves the school or is not available for a period of time, it would mean the entire network administration knowledge in the school would also be unavailable.

The alternative is outsourcing some or all administration tasks to an external service provider. Many commercial network administration providers offer a dial-up administration service whereby the provider accesses the system via a phone link to perform many administrative tasks at a much cheaper rate than incurred through site visits. This may be particularly useful for schools in country areas where access to technology professionals may be costly due to distances involved. Some tasks such as software installation would most likely have to occur on-site.

Regardless of whether the school chooses to perform its own administration or have it outsourced, it is highly recommended that comprehensive details of the school's computer network such as layout, configurations and software licences be produced and updated as necessary. Methods for automating common administration functions such as printer queue maintenance, backup processes and user setup should also be developed and documented for future referral. Master passwords for all parts of the system should be written in a book and stored in the school safe.

It is also helpful to produce a list of work practices or rules for the use of computers and affix them near each workstation. This will help reinforce the school's policy with regard to the use of computers and the local area network.

Regular Maintenance Tasks

Aside from system backup and software installation which are discussed in separate sections, some of the regular maintenance tasks include:

- workstation network client set-up;
- network interface card testing/installation/replacement;
- cable testing;
- cable patching;
- purging of deleted files;
- new user setup;
- user password maintenance;
- user support;
- printer / peripheral configuration and maintenance;
- general troubleshooting.

These tasks are vital to the continued operation of the school's computer network.

Backup, Recovery and Contingency Planning

When it reaches the stage that the school is utilising either a centralised or distributed application and data system, it is vital that system downtime be avoided or at least minimised.

If any of the following components of the network fail, all (or at least some) of the system will be unavailable for use:

- 1 AC Power (blackout / surge / spike / brownout);
- 2 **File server(s)**;
— hard disk / hard disk controller;
— power supply;
— **motherboard**;
— network interface card.
- 3 **Hubs** (particularly those connected to the servers);
- 4 **Cable backbone**.

The school's contingency (or disaster recovery) plan should provide solutions to be able to recover (quickly) from any of the component failures mentioned above.

As examples, the following solutions are available:

- **Uninterruptible Power Supply** (UPS) for server(s) and hubs;
- tape backup system to regularly backup server hard disks;
- hard disk **mirroring**;
- server mirroring;
- duplication of cable backbone;
- avoiding single points of failure.

As an absolute minimum, a UPS for the server(s) with server shutdown capability and a reliable tape backup strategy must be incorporated in the contingency plan.

File server: one of the machines in a local network that serves as a data storage centre i.e. a place where all the shared data files used throughout the network are stored.

motherboard: this is where the electronic circuits are located for processing and storing data.

hub: hardware or software device that contains multiple independent but connected modules of network and Internetwork equipment. Hubs can be active (where they repeat signals through them) or passive (where they do not repeat, but merely split, signals through them).

cable backbone: this type of cabling links together the various segments of a LAN e.g. potentially linking multiple buildings or floors.

uninterruptible power supply: a UPS is a basic unit for ensuring an 'even' flow of power to a fileserver. 'Brown/black outs', power surges / spikes and power cuts can all be accommodated e.g. when a power cut occurs, the UPS can broadcast a pre-recorded message over the network warning users to save their work and then turn off (down) the file server correctly.

mirroring: this is the process of making a duplicate backup copy.

Security

There are two forms of security:

- 1 *Physical* security (to avoid theft, fire, water and wilful physical damage);
- 2 *Data* security (to avoid loss / corruption of data and applications and to maintain privacy).

1 Physical Security

It is important to store vital network components such as servers, hubs and routers in secure locations such as a strongroom. Most of this equipment needs little or no administration and should be safely stored to avoid theft or damage from fire. Components such as cabling should be concealed in conduit wherever possible and should not be easily visible when run outside buildings. Similarly, components such as main power switchboards should always be kept locked.

2 Data Security

If data security has not been investigated thoroughly before configuring the system, difficulties and frustrations may arise. A system could be developed so it is easy to “break” into through a very lax security framework, allowing students to access parts of the system and cause data damage. On the other hand, it could be too difficult to navigate because of the overuse of passwords and tight restrictions. Effective data security involves the allocation of trustee rights to users or groups of users for specific parts of each server and the allocation of passwords where appropriate. Network-aware menu systems that restrict access to sensitive areas of the system (such as MS-DOS), providing Read-Only access to application areas on the servers and the protection and regular changing of sensitive passwords can ensure effective and secure use of your network system. As a general rule, only allocate each user the minimum rights necessary.

Data Storage and Management

The issue of data storage can be complex. In a networked situation, it is usually best to store all important data files on a fileserver rather than on floppy diskettes or on local hard disks in workstations or standalones. The reason for this is that the school’s contingency plan should include total and regular backup of all fileservers while there may not be any direction to

backup local workstations.

Losing documents or other data files through corruption or accidental deletion when there are no backups will require the manual recreation of those files. This is both time-consuming and avoidable.

If it is decided that all important data storage is to be on the fileserver(s), then it is important to ensure adequate disk space is available to allow this to occur. A tape backup solution must also be provided which is capable of duplicating this amount of data storage. Tape backups should be stored in a secure area, preferably away from the fileserver. Backup tapes could be destroyed or stolen if stored together with the server.

When setting up data storage areas on a file server, it should be noted that staff may require separate areas of the disk where they have private use and shared use. A user's private folder should not be visible to other users while the shared folder should be visible to all users. Separate shared folders can be created for staff and students.

If it is decided that no data is to be stored on the server(s) and all files are to be saved at the local workstation or on floppy diskette, then it is vital that individual users be aware of their own responsibility to make their own backups of any data files they create.

Regardless of the method of data storage chosen, it is up to the user to periodically remove unwanted, old or outdated data files from the system to free up valuable disk space. The Network Administrator should regularly check available disk space to ensure sufficient capacity is available at all times.

Backup Strategies

Regular backups of data on servers minimises the risk of data loss and damage caused by disk failures, virus infection or network problems. Backup procedures should be carefully planned and adhered to.

Commercial backup programs such as *Backup Exec* are available to facilitate the procedures required for effectively managing this aspect of data security. These are best used in conjunction with tape-drive hardware, which uses media capable of storing high volumes of data. Data drives and tapes are available in different capacities depending on requirements. Typically, a tape drive capable of backing up the contents of the server hard disk(s) to one tape is ideal.

The basic types of backup procedures are:

- Full backup, in which all selected files are copied onto a tape.
- Incremental, in which backup occurs only for files which have been changed or created since the last full or incremental backup.

In developing a backup plan, consider the following:

- Storage of data tapes should occur in a secure environment such as the school safe where fire, water and theft risks are minimised.
- Periodically verify data tape reliability in recovering files.
- A full backup should preferably fit on one data tape cartridge.
- Label tapes with date, time and type of backup (Full or Incremental)
- Rotate the backup media.
- Conduct a full backup each week, an incremental backup daily and archive full backup tapes on a monthly basis.
- Server access to the tape backup system should be on an authorised, password protected basis only.

Upgrading Existing Software and Installing New Software

Installing software on file servers is very different to installing software on standalone computers. For this reason it is important to obtain specialist advice if the school's Network Administrator is not familiar with the various models of networked software installation.

Because a server-based network is a centralised computer system, the entire concept of its use is to generate and follow standards and standardisation. It is recommended that decisions be made on which specific products are to be chosen for each category of computer use.

For example, for the task of general word processing, the school could standardise on either *Microsoft Word* or *Word Perfect* — but not both. Perhaps an integrated product such as *Claris Works* or *Microsoft Works* could cover several categories of computer use. The reason for choosing one product in each category is to standardise file formats for ease of data transfer and to streamline staff training requirements. The selection of specific software for networked use across the school should always be made by the school's technology committee.

The processes of upgrading to new versions of existing software and installation of new software involves not only how to make the new software available to users, but how to ensure the new software will be used efficiently. This may involve formal training, in-service training or peer support. Whichever method of staff training is chosen, the goal should be to ensure the continued use and acceptance of technology throughout the change.

Computer Viruses

Computer viruses are a separate concern for network administrators. As these can potentially be devastating to a computer network, it is imperative that measures be taken to avoid infection. The best way to avoid infection is the education of users. Understanding what a virus is and how it spreads, and adopting work practices among users to ensure infection cannot occur is the first step.

Virus protection software is the safety net in case a virus manages to get through good work practices.

What is a Computer Virus?

All viruses are computer programs written by a person or persons - they are not biological. To be classed a virus, the program must have the ability to replicate and migrate from computer to computer. This can be either via diskette or across a network. As well as propagating, viruses inherently cause damage. There are other 'rogue' programs to be aware of such as *Logic Bombs*, *Trojan Horses* and *Worms* which are not viruses, but can be equally damaging.

How Does a Virus Spread?

All viruses hide somewhere on a floppy disk or a hard disk. Most viruses fall into the following categories:

- *Boot Sector / Partition Table Viruses*
These live in the boot areas of disks and load into memory whenever the computer is booted. They infect each diskette placed in the drive.
- *Executable File Viruses*
These attach themselves to executable files (programs) and function whenever the infected program is loaded. They infect other uninfected programs when they are loaded.

- **Multi-Partite Viruses**
These viruses are made up of separate components and can be almost undetectable whilst at the same time infecting every file on your computer.
- **Macro Viruses**
These are embedded in macros defined within certain word processing documents or spreadsheet files. They are transferred by the sharing of the infected documents.

Some Effects of Viruses

The damage that a virus can cause is limited only by the imagination of its author. Some of the typical effects include:

- degradation of processing speed;
- inappropriate screen messages;
- corruption of printouts;
- file deletion;
- corruption of files and **File Allocation Tables (FAT)**;
- low-level formatting of disks.

File allocation Tables: a record keeping structure DOS uses to keep track of the location of every file on the disk i.e. like an index.

How to Avoid Viruses

Viruses are getting “smarter” everyday, becoming harder to detect and there are thousands of different viruses in circulation. It is almost impossible to totally avoid viruses however, these suggestions should help.

- 1 Ensure that complete and regular backups are maintained for all computer systems;
- 2 Use an up-to-date *virus scanning* program on both file servers and workstations;
- 3 Be wary of all disks that have come from external sources (even from home);
- 4 Do NOT participate in copyright infringement;
- 5 Write-protect all original program diskettes before using them; and
- 6 Install virus scanning software that *automatically* scans for viruses.

What if a Virus is Found?

If the steps above were followed, this shouldn't happen, but if it does, follow the steps below:

- 1 Switch off the computer and place a sign to let others know the computer is infected;

- 2 Isolate all diskettes associated with that computer. It is likely that some or all are infected as well;
- 3 Attempt to find the possible source of the virus;
- 4 Ask for help if unsure of how to remove the virus; and
- 5 Reinforce the steps listed above to avoid future viruses.

Removing a Virus

The removal of computer viruses from both standalone computers and from network file servers can be a complex, time-consuming procedure. Further information and evaluation copies of virus removal programs is available from the following Website:

<http://www.vet.com.au>

■ ■ ■