

Preventative Maintenance

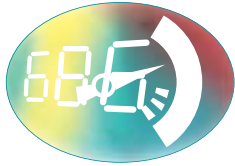
Preventative Maintenance Contents

PvM 1	Topic introduction – Aim and objectives of this topic	1
PvM 2	Overview – An introduction to the process	1
PvM 3	Implementation guide – How to implement the process	4
PvM 4	Operations guide – The ongoing operation of the process	9
PvM 5	Review – Summary and checklist	10
Appendices		13
Glossary		38

Key

Glossary term: [Glossary term](#)

Cross reference: [Cross reference](#)



Preventative Maintenance

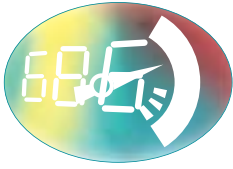
© Becta 2004

You may reproduce this material free of charge in any format or medium without specific permission, provided you are not reproducing it for profit, material or financial gain. You must reproduce the material accurately and not use it in a misleading context. If you are republishing the material or issuing it to others, you must acknowledge its source, copyright status and date of publication.

Publication date March 2004

Originally published online in September 2003 as part of the Becta website
<http://www.becta.org.uk/tsas>

While every care has been taken in the compilation of this information to ensure that it is accurate at the time of publication, Becta cannot be held responsible for any loss, damage or inconvenience caused as a result of any error or inaccuracy within these pages. Although all references to external sources (including any sites linked to the Becta site) are checked both at the time of compilation and on a regular basis, Becta does not accept any responsibility for or otherwise endorse any product or information contained in these pages, including any sources.



Preventative Maintenance

PvM 1 Introduction to Preventative Maintenance

Would you like to reduce network downtime and increase the life expectancy of your network components? This is just some of what preventative maintenance can help you to achieve...

PvM 1.1

Aim

The aim of this section is to introduce the topic of preventative maintenance and to help you implement the process in your school with a minimum amount of preparation and training.

PvM 1.2

Objectives

The objectives of this section are to enable you to:

- understand the concept and benefits of preventative maintenance
- understand what is involved in the process of preventative maintenance
- implement preventative maintenance in your school
- continue to operate preventative maintenance
- review your implementation and summarise your progress.

PvM 2 Overview

PvM 2.1

What is preventative maintenance?

In order for your network to work properly, every piece of the network must work properly. Preventative maintenance is concerned with anything that can be done to prevent any component of your network from failing. This includes:

- **client** computers (also referred to as workstations) – PCs, Apples, laptops, PDAs
- **servers** – the computers controlling specific parts of the network
- peripherals – devices such as printers, whiteboards or scanners that are connected to client or server computers
- **devices** such as **hubs, switches, bridges** and **routers** that are used to control the network
- the equipment used to connect the network together, whether cables or wireless devices, or a combination of the two
- the software running on all this equipment.

Each of the above components will have a particular maintenance requirement. The Preventative Maintenance implementation guide (PvM 3) will help you determine the best approach to maintenance activities for your network. The Preventative Maintenance operations guide (PvM 4) will help you keep the network in good working order.

As well as ongoing maintenance activities, the best preventative maintenance programme starts with careful thought about the quality of the items you buy and the effort made to install, service and keep track of those items.

PvM 2.2

Why use preventative maintenance?

Research shows that the cost of maintaining and operating ICT equipment over the lifetime of the components can be at least double that of the initial outlay for purchase of the equipment. An effective preventative maintenance programme can drastically reduce the cost associated with the day-to-day operation of the equipment.

Implementing a preventative maintenance programme will enable you to detect and prevent many **problems** before they become **incidents** by ensuring that the individual items that comprise your network are operating as reliably as possible. Some of the benefits you can expect are:

- reduced network downtime
- increased life expectancy of network components, eliminating premature replacement of parts
- more economical use of technical staff because they are working to a schedule rather than on reacting to repair breakdowns
- timely routine repairs mean fewer large-scale repairs
- lower repair costs, because there will be fewer secondary failures (when parts fail in service they often damage other parts)
- reduced product rejects, rework and scrap, owing to better overall equipment condition
- identification of equipment with excessive maintenance costs, indicating the need for corrective maintenance, operator training or replacement of obsolete equipment
- improved safety conditions and quality.

Combining your preventative maintenance programme with effective network monitoring will also provide a means of measuring the effectiveness of the maintenance activities.

PvM 2.3

Who uses preventative maintenance?

All schools that use ICT equipment should implement preventative maintenance measures. This applies to schools running standalone computer equipment as well as to those that have computer networks.

Internal or external technical support staff carry out most of the preventative maintenance activities in the school. If your school's technical support is provided by an external party, you can use the information on preventative maintenance tasks to ensure that they are performing the tasks necessary to keeping your network running at peak performance.

How does preventative maintenance work?

There are three main elements to preventative maintenance: design, maintenance and preparation. The preventative maintenance process flowchart illustrates this.

Design

This involves setting up the network in such a way as to minimise the possibility of component or network failure.

Examples

- Ensuring that **servers** have an uninterruptible power source
- Installing a **firewall** to keep the network secure
- Putting in adequate ventilation for heat-sensitive devices

Maintenance

This means carrying out periodic maintenance tasks on network equipment to reduce the risk of early component failure.

Examples

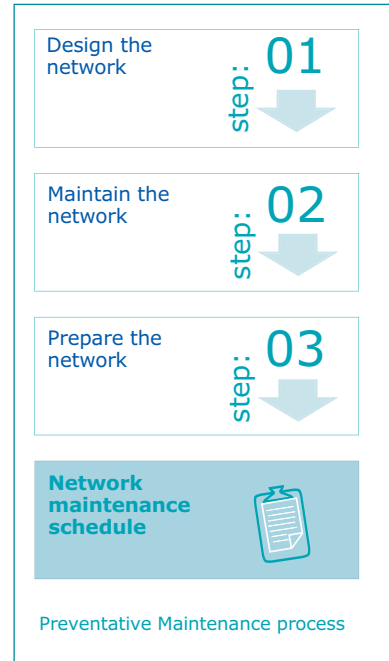
- Keeping print heads clean in printers
- Blowing dust out of PCs
- Checking disk space and keeping track of system logs

Preparation

This entails putting systems in place to minimise the impact on the network when components do fail.

Examples

- Maintaining a stock of spare equipment
- Keeping detailed documentation on network components so that they can be quickly rebuilt
- Backing up critical data (and testing the back-ups)
- Knowing who is responsible for each part of the school network



What does preventative maintenance cost?

Preventative maintenance has two main costs: capital and revenue.

Capital costs include:

- choosing good quality components for the network rather than always basing your purchasing decisions on price
- duplicating critical parts of the network to minimise the impact of component failure
- buying a stock of spare parts for the network
- investing in data-backup systems and other security measures.

These costs will vary from school to school depending on the needs of the network. Early tasks in implementing preventative maintenance measures are to evaluate the needs of the network and to budget for the necessary equipment.

Revenue costs include the need to provide technical support personnel to carry out maintenance tasks. A good rule of thumb is to have one technician for every 150 pieces of equipment. Provision may be:

- an onsite technician or technicians
- technical support shared with other schools
- technicians provided via a support contract with an outside agency.

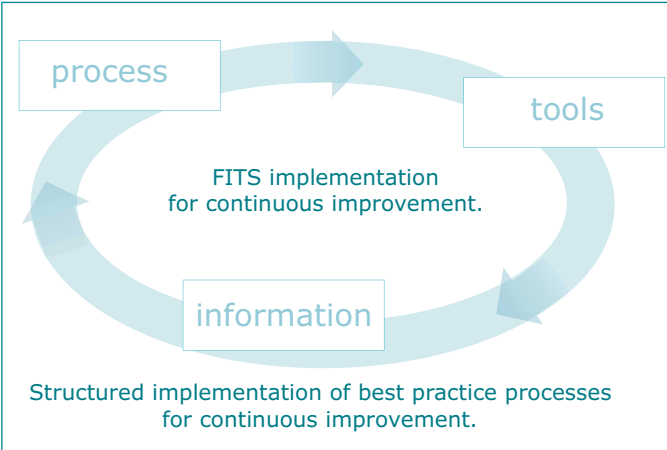
In all cases it is important to ensure:

- coverage for holidays and sicknesses
- clear understanding of the range of tasks to be performed in order to prevent problems
- implementation of an agreed, documented programme of preventative maintenance.

PvM 3 Implementation guide

PvM 3.1 What needs to be done?

As described in the overall FITS implementation approach, we recommend a phased approach to implementing new processes.



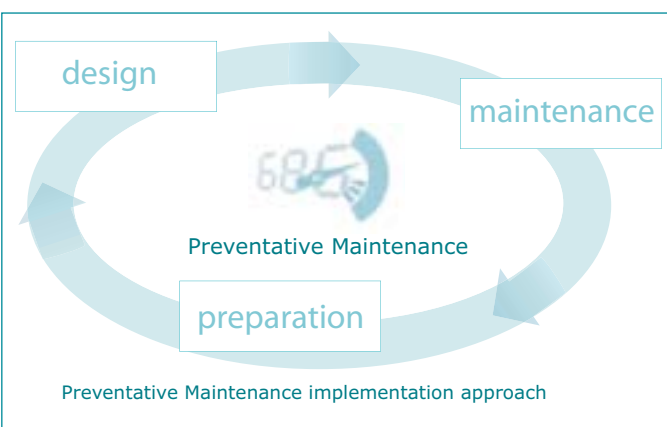
The diagram shows a circular process with three main components: 'process', 'tools', and 'information'. Arrows indicate a clockwise flow between them. In the center, it says 'FITS implementation for continuous improvement.' Below the cycle, it states 'Structured implementation of best practice processes for continuous improvement.'

The FITS ethic is 'keep it simple'. FITS also promotes a cyclic approach to its implementation: start small and make continuous improvements.

This first set of material introduces the processes with easy-to-follow instructions and simple tools to use. When you have implemented the processes, you will use the tools to gather information to make further improvements and thus enter the next cycle.

This process of refinement allows you to implement best practice in manageable, bite-size pieces. You will therefore reap the benefits from an early stage and not be overwhelmed by extra work.

The FITS preventative maintenance implementation approach is for people with little free time to spend on implementing processes and procedures and whose day-to-day activities are unpredictable and must take priority.



The diagram shows a circular process with three main components: 'design', 'preparation', and 'maintenance'. Arrows indicate a clockwise flow between them. In the center, it says 'Preventative Maintenance'. Below the cycle, it states 'Preventative Maintenance implementation approach'.

Our aim is to help you begin to remove some of the unpredictability by introducing best practice processes in small steps and so begin to realise the benefits as quickly as possible.

To ensure maximum network reliability, each of the three elements of preventative maintenance needs to be addressed:

Design

Set up the network in such a way as to minimise the possibility of component or network failure. This includes ensuring that all critical equipment is protected from failure and that the network is secure from malicious or accidental damage.

Maintenance

Carry out periodic maintenance tasks on network equipment to reduce the risk of early component failure.

Preparation

Put systems in place to minimise the impact on the network when components do fail. This includes maintaining a stock of spare equipment, keeping detailed documentation on network components and having a plan for remedial action.

PvM 3.2

Who does it?

The person who is responsible for managing the school's ICT should work with the technician to implement preventative maintenance suitable for the school environment.

PvM 3.3

Prepare to implement

Since preventative maintenance has three elements, you will need to have a plan to implement all three. The order, however, is not too important and which is the most urgent for your school situation will depend on a number of factors, including:

- current budget set aside for acquiring capital equipment
- age and state of the network infrastructure
- level of training and expertise of technical staff.

Start with design if:

- you are planning a new network or a major upgrade to an existing network
- you have particular concerns over network security
- the school does not already have network use policies in place.

Start with maintenance if:

- network performance is poor
- there is a higher-than-usual failure rate for network devices
- network equipment is old or of poor quality.

Start with preparation if:

- data is not currently backed up regularly
- the network is not clearly and fully documented
- responsibilities in the event of a failure are not clear.

PvM 3.4

Implement preventative maintenance

PvM 3.4.1

Design your network

There are three steps to designing a network to minimise the chance of failure:

- Do it right
- Duplicate it
- Document it

Step 1 Do it right

Allocating sufficient time to correct installation and set-up of network components is the most effective element of preventative maintenance. No matter if equipment is supposed to work, could work, or even has worked in the past, it cannot be considered correctly installed until it has been adequately tested.

So what do I do?

- Before making any changes to your network, plan the changes on paper.
- Install a firewall (see [Appendix G](#)).
- Install antivirus software (see [Appendix A](#)).
- Check that the network equipment is installed in such a way as to minimise the chances of physical damage.

Step 2 Duplicate it

Once any network element has been installed and tested, then duplicate it wherever possible. There are three areas of duplication to keep in mind: installed equipment, redundancy and implementation.

Installed equipment

For each type of device on your network consider buying an exactly matching spare item. The main advantage is to provide a means to quickly replace a faulty or suspect device. This may not always be possible for more expensive items and is probably more appropriate where you have multiple items such as workstations installed. When determining what spare equipment to purchase, consider the following questions:

- How critical is the device? Can your network manage without it? And for how long?
- How many devices of this type are there? Is it possible to reconfigure (borrow) existing equipment to temporarily cover the loss?
- Can you have a reciprocal arrangement with other local schools?

Redundancy

Wherever possible, copy data. Consider keeping data only on the server and install a RAID array (see [Appendix E](#)) to ensure that data is not lost.

Connections should be resilient to failure. Consider how data might travel around the network if cables are damaged or a switch fails. Are there multiple paths to each device? Are there fallbacks for the internet connection?

Implementation

Where possible, configure items the same way. Create a software image of a workstation that you know is working well and use it to build new (and repair faulty) workstations.

Doing something the same way every time has several benefits.

- You achieve quicker and more thorough testing of the configuration.
- If you do something the same way each time, the configuration gets fully tested until all the issues can be resolved and the set up is as smooth as it can be. The more testing you perform, the sooner any **problems** should show up and the easier it is to make things right.
- Fixes and upgrades are easier.
- When there is a requirement to fix or upgrade a component, it is far easier to do it for one configuration than it is for multiple variants.

By doing it as right as possible the first time, you can make components work better for longer periods of time than if you implement 'quick and dirty' shortcuts. Duplicating implementations allows configurations to be tested more quickly and thoroughly than doing custom configurations, and it makes fixes and upgrades much easier to implement.

So what do I do?

- Ensure that all critical network components have duplication or fail-safe built in (see [Appendix I](#)).
- Set up a RAID system (see [Appendix E](#)).
- Implement a backup-and-restore process for all data on your network (see [Appendix B](#)).
- Develop an image for computers on your network and use that image to install new computers.

Step 3 Document it

Documenting the configuration of your network and the set up of its components gives you a strong base from which maintain, upgrade and fix it.

Unless there is access to a great deal of information about each component of a network, it is almost impossible to maintain it.

- If you don't know which directory an application is in, how can you upgrade it?
- If you don't know what the address settings are for the network interface card (NIC), how can you configure the new network driver?
- If you don't know which make and model of NIC the computer has, how can you know what driver to use, let alone how to configure it?
- If you don't know where the network outlets are and what their numbers are, how can you move or add equipment?

This information has to be known in order for there to be any maintenance of the system. It can either be done on an ongoing, systematic basis, or else be done in a panic at the last minute. One way or the other, you have to write down the information before you can make any plans, purchase any equipment, or implement any fixes or changes. Having it in your head is not enough.

Documenting a system is not a one-time affair. The network keeps changing and it is important to keep track of its current status. Use FITS [Change Management](#) to ensure that all ICT infrastructure changes you make minimise the possibility of introducing additional [incidents](#) and [problems](#). Change Management will also help you keep your ICT equipment records up to date in your [configuration-management database](#). There is no hyphen between configuration and management.

If you do it right, duplicate it and document it, there is every reason to expect a reasonably well running and maintainable network. Even if you don't do it right or duplicate it, you have a good chance of ultimate success as long as you document what you are doing. The more documenting you do, the more reliable and maintainable your network becomes. The less documenting you do, the less reliable and maintainable your network becomes.

So what do I do?

- Collect together in one safe place all manufacturers' manuals and instructions that came with the equipment. Cross-reference each document to the equipment to which it relates.
- Create [physical topology](#) and [logical topology](#) maps of the network set up.
- Manage any ICT infrastructure changes to the network components, layout or set up (see Change Management).

PvM

3.4.2

Maintain your network

A network is not just computers; network maintenance is therefore not just concerned with blowing dust out of PCs. Each component of the network (cabling, server, workstation, peripheral and so on) has its own special usage and maintenance concerns that must be dealt with in order to provide maximum network reliability.

Items that require regular attention include:

- maintaining PC workstations
- maintaining Apple workstations (see [Appendix C](#))
- maintaining servers (see [Appendix D](#))
- maintaining printers and scanners

- maintaining switches, hubs and routers (see [Appendix F](#))
- maintaining cabling.

So what do I do?

- Set up a maintenance schedule for the network components and identify responsibility for carrying out the listed tasks (see [Appendix H](#)).

PvM 3.4.3

Prepare your network for failure

While proper preventative maintenance of any sort provides the opportunity to detect and correct problems before they become incidents, it cannot prevent all failures. However, by following the advice in this guide you will be able to establish an effective preventative maintenance programme that will minimise the effects of [problems](#) when they do occur. It will also put you in a position to rectify [incidents](#) with a minimum of fuss, outlay and disruption to the users of your network.

So what do I do?

There are measures you can take to ensure that, when components fail, you can repair the network in the fastest possible time. These include:

- maintaining a stock of spare equipment (see [Appendix I](#))
- using [Configuration Management](#) to keep detailed documentation on network components so that you can quickly rebuild them
- backing up critical data – and testing the back-ups (see [Appendix B](#))
- using [Service Level Management](#) to identify who is responsible for what.

PvM 3.5

Review the implementation

To be effective, your preventative maintenance programme needs to be built on a strong foundation of:

- doing the job right the first time
- duplicating systems and installations whenever possible
- documenting all configurations and procedures.

If you cannot get everything done exactly right, then by duplicating your work you can simplify debugging and upgrading. If you are unable to achieve duplication, then by documenting everything you do, you can understand the scope of what you're dealing with before you try to implement [changes](#) or repairs. Without documentation, you will waste much effort during maintenance, upgrades or disaster recovery.

How can you be sure the measures you have put in place are effective?

- Measure, over time, the results of the [Incident Management](#) process. You should see the number of [incidents](#) fall.
- Check the output from the [Problem Management](#) process. You should see a drop in recurring [problems](#).

PvM 4 Operations guide

PvM 4.1

What needs to be done?

Once you have developed a preventative maintenance schedule for the network in your school, it is important to ensure that the tasks listed on the schedule are carried out. The actual maintenance tasks will be determined by the type and quantity of equipment covered by the schedule.

Any errors discovered during routine maintenance tasks should be reported as **incidents** to ensure that records of their detection, diagnosis and resolution are kept.

You should ensure that any changes to the network are reflected in **changes** to the maintenance schedule.

PvM 4.2

When does it need to be done?

The frequency of maintenance activities will also be determined by the type and quantity of equipment covered by the schedule. The following list is only a rough guide to appropriate timings for general activities.

- Daily
- Weekly
- Monthly
- Quarterly
- Annually

The list is for guidance only and details of how to perform the tasks may be found in the Appendices. The actual frequency of tasks needs to be customised for use in your school and will be determined by factors such as:

- particularly heavy use of devices
- manufacturer's advice for specific devices
- the environment in which the equipment is used or stored
- the quality (robustness) of the equipment
- experience of previous preventative maintenance activities (some devices are best left alone).

Daily

- Check server error and usage logs to identify potential problems.

Weekly

- Check disk space on servers.
- Clean paper dust out of printers.
- Ensure that antivirus software is up to date.

Monthly

- Check batteries on laptops and mobile devices.

Quarterly

- Clean dust out of workstations.
- Clean keyboards, mice and other moving parts.

Annually

- Test uninterruptible power supplies.
- Check network wiring.
- Review the effectiveness of the preventative maintenance programme.

PvM 4.3

Who does it?

The person who carries out technical support in the school should perform the above tasks. Some of these tasks require technical expertise and a thorough understanding of network technologies.

PvM 4.4

How is it measured?

The technical support staff along with the school leadership team should conduct an annual review of the suitability and cost effectiveness of the preventative maintenance programme.

Check the number of incidents reported to see if an effective preventative maintenance programme shows a decline in incidents raised by users and a rise in incidents resulting from **problems** uncovered during maintenance activities. Any recurring problems not eliminated by the preventative maintenance programme should be investigated to see if any underlying trends can be identified. This may lead to a change of maintenance activities or frequency.

PvM 4.5

Resources

For these resources see the Appendices.

- Maintaining Apple workstations ([Appendix C](#))
- Maintaining servers ([Appendix D](#))
- Maintaining switches, hubs and routers ([Appendix F](#))

PvM 5 Review of Preventative Maintenance

The purpose of this section is to help you review your implementation and ongoing operation of preventative maintenance, check your understanding of the process, examine what a successful implementation should look like and what you should have achieved by introducing it into your school. This will help you to assess how successful its introduction has been and point you back to the relevant sections in the Preventative Maintenance process that you should revisit to make improvements, if these are necessary.

Start by reading the sections included in the recap of Preventative Maintenance. When you have refreshed your memory and considered your own implementation alongside these descriptions, work through the checklist to identify any areas that you should revisit and perhaps re-implement or reinforce.

PvM 5.1

Recap of Preventative Maintenance

In preventative maintenance we explained the importance of, as far as possible, preventing the components on your network from failing; to minimise the number of incidents reported; and to improve the reliability and availability of ICT to users in the school.

We gave you an overview of preventative maintenance and an implementation guide giving step-by-step instructions to help you implement a preventative maintenance process that we believe is appropriate for the needs of schools. An operations guide gave you a list of ongoing activities that the process requires in order for you to keep it going and to reap the benefits.

Check your understanding of the process by following PvM 5.1.1 to PvM 5.1.4 below.

Step	Tasks
<p>Design your network.</p>	<p>The three Ds of designing your network</p> <ol style="list-style-type: none"> 1 Do it right – the correct installation and set-up of network components is the most effective element of preventative maintenance, so: <ul style="list-style-type: none"> • plan properly any changes to your network • install a firewall for internet and WAN connections • install antivirus software with up-to-date definition files • minimise the possibility of physical damage to network equipment. 2 Duplicate it – your network equipment – wherever possible, so: <ul style="list-style-type: none"> • for each type of device on your network consider buying a matching spare for quick replacement • consider redundancy for critical equipment such as RAID for servers, multiple paths for network traffic or back-up internet connections • consider duplicating configurations for workstations by creating a standard software image. 3 Document it – know what you need to maintain, so: <ul style="list-style-type: none"> • collect together all manufacturers' manuals and instructions • create physical and logical topology maps of the network • manage ICT infrastructure changes to network components, layout or set-up.
<p>Maintain your network</p>	<p>Each component of your network has its own special usage and maintenance concerns that you must deal with in order to provide maximum network reliability. A maintenance schedule is a useful tool to help you maintain your network regularly.</p>
<p>Prepare your network for failure</p>	<p>Even with a sound preventative maintenance schedule, failures will still occur. There are measures you can take to ensure that, when components do fail, you can repair the network in the fastest time possible. These include:</p> <ul style="list-style-type: none"> • making sure that you know when something has failed by using network monitoring or through incident reports • maintaining a stock of spare equipment • storing detailed documentation on network components • backing up critical data • identifying who is responsible for preventative maintenance.

What you should expect now that you have implemented Preventative Maintenance

- A regular maintenance schedule for the components of the network should be in place and followed.
- Your network gets very few major network outages, which means higher availability for the ICT users.
- You experience minimal occurrences of virus infection and malicious attack by hackers.
- You have spare equipment you can use to resolve some incidents.
- Your network components have increased life expectancy.

What you should have achieved through Preventative Maintenance

- Because you implement redundancy in critical equipment such as servers, network paths and internet connections, your network experiences fewer major outages.
- Using your own spare network components enables you to resolve incidents quickly by replacing faulty hardware.
- You have protected your network by putting a firewall in place to stop malicious attacks.
- You have protected your network by putting antivirus software in place to stop attacks by viruses, worms and Trojan horses.
- There will be fewer failures caused by ICT infrastructure changes if a change management process is used alongside preventative maintenance.
- Your network suffers fewer failures caused by environmental and physical damage.
- You have improved the life expectancy and reliability of network components, which reduces the cost of replacing equipment.

Benefits of having implemented Preventative Maintenance

- You can provide a stable and reliable network as a result of the correct installation and set-up of network components.
- A firewall protects your network from any attack through your internet connection.
- Antivirus software protects your network from viruses, worms and Trojan horses.
- Any hardware failures will have minimal impact on the availability of the ICT services because you have duplicated your critical network equipment and components.
- In the event of a hardware failure, your store of spare equipment allows you to swap out the faulty item and restore the ICT service quickly.
- A regular maintenance schedule has increased the reliability and lifetime of your network equipment.
- A regular back-up schedule ensures that you are able to restore data in cases of data loss caused by network failure.

Checklist

Use this checklist to identify any areas of preventative maintenance that have not been entirely successful. Then reinforce them by revisiting and re-implementing the relevant section of the FITS process.

Characteristics of a successful implementation	FITS section to revisit if implementation has not yet been successful
A firewall is in place for internet and WAN connections.	PvM 3.4.1 Design your network Step 1 Appendix G Installing a firewall
Antivirus software is in place and regularly updated to protect all servers and workstations on the network.	PvM 3.4.1 Design your network Step 1 Appendix A Installing antivirus software
Duplication and fail-safe are built into all critical network components.	PvM 3.4.1 Design your network Step 2 Appendix I Developing fail-safes Appendix E Set up a RAID system

Characteristics of a successful implementation	FITS section to revisit if implementation has not yet been successful
You have implemented a backup-and-restore process for all data on your network.	PvM 3.4.1 Design your network Step 2 Appendix B Implementing a backup-and-restore process
You have documented the configuration of your network and the set-up of its components.	PvM 3.4.1 Design your network Step 3 See also Network Monitoring NM3.3 Implement Step 1
A maintenance schedule for the network components is in operation.	Appendix H Setting up a maintenance schedule Appendix D Maintaining servers Appendix F Maintaining switches, hubs and routers Appendix C Maintaining Apple workstations

If the above characteristics are all true of your school, congratulations on implementing a successful preventative maintenance process! The next steps for you are to continue operating the process as described in the Preventative Maintenance operations guide (PvM 4) and establish the process firmly. Work through this checklist at regular intervals to help you check that everyone responsible continues to carry out all aspects of the process. You can then refer to the relevant sections above to address any shortfalls as they arise.

Appendices

PvM Appendix A Installing antivirus software

What is a virus?

A virus is a program or piece of code loaded onto your computer without your knowledge that runs against your wishes. Viruses can replicate themselves. All computer viruses are manmade.

Types of virus and virus-like programs

Viruses

A virus is a manmade program or piece of code that causes an unexpected, usually negative, event. Viruses are often disguised games or images with clever marketing titles. Even a simple virus is dangerous because it can quickly use all available memory and bring your system to a halt. An even more dangerous type of virus is one capable of bypassing security systems to transmit itself across networks.

Worms

Computer worms are viruses that reside in the active memory of a computer and duplicate themselves. They may send copies of themselves to other computers through email or internet relay chat (IRC). A worm is a special type of virus that can replicate itself and use memory, but it cannot attach itself to other programs.

Trojan horses

A Trojan horse program is a malicious program that pretends to be a benign application but which purposely does something the user does not expect. Although not a true virus, since it does not replicate, a Trojan horse can be just as destructive as a virus.

How a network can become infected with a virus

The widespread adoption of email through the years has been accompanied by the development of malicious code – that is, email viruses and attacks. Email has provided hackers and crackers with an easy way to distribute harmful content to internal networks. School networks have been breached by worms and viruses, as well as by crackers, through the use of email. Hackers can easily breach the protection offered by a **firewall** by tunnelling through the email **protocol**. A typical firewall cannot protect against such email attacks, because it does not analyse email and its contents.

Because email messages can include file attachments, hackers can send infected files and hope that the recipient will open them, as happened with Melissa and Manwella. Yet other methods exist which allow a skilled and possibly malevolent hacker to inject code through email and run custom-made applications automatically while the end user reads the email text. Such problems have been around since the use of HTML in email and have been exploited by notorious worms such as the KaKworm, BubbleBoy and Nimda.

Methods that may be used to attack your email system

- Attachments with malicious content
- Emails with malformed MIME headers
- HTML mail with embedded scripts
- Malicious ActiveX controls and Java applets

Although most viruses gain access to your network via email, they may also be introduced via a floppy disk or CD-ROM containing a virus.

What is antivirus software?

A piece of antivirus software is a program that runs on a computer to detect and neutralise viruses and worms. You can either run the software from time to time (typically at boot time) to detect viruses or leave it running continuously on the computer to provide a higher level of protection.

Why install antivirus software?

Because computers on a network are connected together, a virus on one workstation can easily spread around the network and cause serious damage. The only prudent response to this risk is to prevent viruses getting onto your network in the first place. Antivirus software is the tool you need to combat this threat. Without antivirus software installed, your network is vulnerable to serious disruption and loss of data.

Choosing antivirus software for your school

There are several approaches to using antivirus software on school networks: access it online as required, load it on every workstation, install it only on key workstations and have it server based.

Online – run as needed

Antivirus software is not loaded on any workstation but is accessed online as required:

Advantages	Disadvantages
<p>Some online antivirus checkers are free.</p> <p>Every workstation can be covered.</p> <p>There is only a small load on workstations.</p>	<p>It may be time-consuming and slow to use.</p> <p>Heavy internet bandwidth is required.</p> <p>Checking is a one-off process – antivirus programs cannot usually be left running to provide extra protection.</p> <p>It requires active participation by the user of the workstation.</p> <p>Use may result in internet pop-ups and unsolicited email.</p>

This solution may be suitable for schools on a very limited budget.

Every workstation

Antivirus software is loaded on each workstation on your network:

Advantages	Disadvantages
Every workstation is covered. Viruses from floppy disks and CD-ROMs can be easily detected.	It is expensive to buy licences for a large number of workstations. Each time the antivirus software is updated, you have to load the updates on every workstation (this may be as often as once a day).

Selected workstations

Antivirus software is loaded on key workstations on your network:

Advantages	Disadvantages
<ul style="list-style-type: none">• It is a less expensive option.• There are fewer workstation installations to manage.	<ul style="list-style-type: none">• Only some workstations are covered.• Each time the antivirus software is updated, you have to load the updates on every antivirus-protected workstation (this may be as often as once a day).• You need to keep track of which workstations are covered. <p>A separate clean workstation needs to be allocated for checking out floppy disks and CD-ROMs before you load them onto workstations without the antivirus software on them.</p>

Server based

Antivirus software is loaded and controlled from a network server:

Advantages	Disadvantages
<ul style="list-style-type: none">• Every workstation is covered.• It is not as expensive as buying individual licences for a large number of workstations.• Viruses from floppy disks and CD-ROMs can be easily detected.• Only one master copy of the antivirus software needs to be kept up-to-date	<ul style="list-style-type: none">• Server-based antivirus software is more expensive than client-based software.

This solution is suitable for large or complex networks.

There are many suppliers of antivirus software for workstations and a more limited selection selling server-based solutions. Most packages are available on a trial basis. It would be worth trying several to see which is the most suitable for your school. In most cases it should be possible to negotiate a substantial reduction for an educational site licence.

Maintaining your antivirus software to keep it effective

Of all the applications on your network, the antivirus software is the most important to keep up to date.

New viruses appear almost daily and the ability of your network to resist attack will depend on the currency of the virus definition files. The antivirus software manufacturers update these files regularly to provide protection from the latest viruses. Purchase of most antivirus software includes a year's free updates. Further updates usually involve extra outlay.

To ensure maximum protection, it is also important to distribute the updated virus definition files as soon as possible to all workstations running the antivirus software.

PvM Appendix B Implementing a backup-and-restore process

What is a backup-and-restore process?

Most people understand the importance of backing up critical data. But most of the time back-ups, if done at all, happen in a haphazard way – usually after losing some data.

Particularly where data is stored on the [server](#), you need to implement a formal and routine back-up process. Of course, data back-up is of no use unless there is a corresponding process for recovering and restoring the data.

This guide will show you how to implement a data backup-and-restore process that should ensure that you never lose critical data again.

Why back up?

Computers can and do fail and they sometimes fail in ways that render the data stored on them unrecoverable. In addition, there are disasters to consider. If your server room were to be destroyed by fire or flood, you could rebuild the servers – but could you restore the data? Sometimes data simply needs to be restored because a user has accidentally deleted a vital file. How can you be sure the data is available when required?

A system that ensures a minute-by-minute back-up of all data on your network may be prohibitively expensive for your school. On the other hand, backing up data on floppy disks once a year will probably not give you the level of protection you need. The following section will help you choose the right system for your school.

Choosing an appropriate back-up system for your school

When choosing a back-up system, consider the following factors first.

- How dynamic is the data stored on the server? How often does it change and in what ways does it change?
- How much data needs to be backed up, and at what rate is the amount of data growing?
- How much time is available to make the back up?
- If a partial or complete restore of data is required, how quickly must it take place? As a rule of thumb, restoring data takes twice as long as the original back-up.
- Do you need to be able to restore all the data in one go or can you do it by individual files?
- How often does data need to be backed up? Will nightly back-ups suffice or does some critical administration data need more frequent back-up?
- How many copies of data back-up are required? Multiple copies may require additional back-up systems or may use the same back-up systems more than once – thereby requiring extra back-up time.

Once you have an idea of your backup-and-restore needs, you can proceed to acquire the necessary hardware and software to create and manage your back-ups.

When choosing a back-up technology, consider the following factors:

- reliability of the hardware and the media
- cost
- storage capacity
- likely frequency of restorations
- the importance of fitting the entire back-up onto a single piece of media. This last may determine whether the back-ups can be unattended (in the early hours of the morning, for example) or whether staff need to change media during the back-up process.

Different types of back-up technology

The table describes different types of back-up technologies, their approximate costs, and the relative pros and cons of each:

Technology	Approximate cost of drive	Approximate cost of media	Media capacity	Pros	Cons
Zip drives	£150	£15	200Mb	Random access	Very low capacity Slow speed
Jaz drives	£500	£100	1Gb	Random access	Low capacity Slow speed
CD-ROM/ CD-RW drives	£200	£1-£5	650Mb	Random access	Low capacity Slow speed Media not reusable
DVD-ROM/ DVD-RW drives	£500	£10	6Gb	Random access Large capacity	Slow speed
QIC-80 drives	£250-£500	£30	5-20Gb	Very low drive cost/Mb	Slower than other tapes
DAT DDS-1	£500	£20	2-4Gb	High drive cost/Mb	Low tape capacity
DAT DDS-2	£800	£25	8Gb	Low tape cost/Mb	More expensive than DDS-1
8mm tape	£1,500	£50	8Gb	Proven technology	No longer cost competitive with DAT Slow tape seek times
Digital linear tape (DLT)	£3,000	£50	80Gb	Very reliable Very fast High capacity Low media cost/Mb	Expensive drive

If you have a requirement for backing up large amounts of data and, if you can afford it, go for the digital linear tape system. The tapes are very reliable and have a large capacity. If you need more than 80Mb, there are 220Mb DLT drives available or you could consider an inexpensive robotic auto-changer that can manage up to five tapes.

If you need a more modest system, then consider backing up your data onto either CD or DVD with incremental back-ups on a DAT drive.

Each of the above technologies should come with backup-management software to help you manage your backup-and-restore process.

Using the back-up system

Most network operating systems maintain special information for each file on the system. One of these is called the archive bit, which indicates the back-up status of the file. When a user modifies a file, its archive bit is set to 'on', indicating that the file should be backed up. When the back-up is accomplished, the archive bit is cleared. Using this archive bit and your back-up software, you can make different types of back-ups: full, incremental and differential.

- **Full back-up**

All selected directories and files are backed up, regardless of their archive bit state. Full back-ups clear the archive bit on all the backed-up files when they are finished.

- **Incremental back-up**

Only the files with their archive bit set are backed up. This backs up all files changed since the last full or incremental back-up. Incremental back-ups clear the archive bit of the files that are backed up.

- **Differential back-up**

This is similar to the incremental back-up in that it backs up only files with their archive bits set. The difference is that differential back-ups leave the archive bit set. Subsequent differential back-ups will back up those files again, plus any new ones that have been modified.

Why are there different types of back-up?

To do a full back-up of your data every night may not be feasible for the following reasons.

- A full back-up may take too much time.
- A full back-up may require that staff be present to swap media (when one disk or tape is full and a new blank needs to be inserted in the drive).
- A full back-up may reduce the lifespan of your back-up media and drives by giving them extra work to do.

On the other hand, doing only incremental back-ups may increase the risk of data loss. So it is best to combine the back-up approaches by using a combination of back-up types. One common way to mix these types is to perform a full back-up of the system once a week and perform only incremental or differential back-ups each day.

You now need to plan a back-up rotation strategy that addresses how back-up media is rotated. Back-up rotations are designed to accomplish the following goals:

- rebuild the system with the most recent possible data in case of a catastrophic failure
- restore files from older media that may have been accidentally erased or damaged without anyone noticing the potential loss of data at the time
- protect against back-up media failure

- protect the data from an environmental failure, such as a fire, that might destroy the original system and data.

The most common rotation system is called the 'grandfather-father-son (GFS) system. Usually this uses eight tapes. The system works as follows:

- Label four of the tapes as 'Monday' to 'Thursday' and four others as 'Friday1' to 'Friday4'.
- Every Monday to Thursday, make an incremental or differential backup using one of the labelled tapes and replacing the data stored on the previous week.
- Each Friday make a full back-up using the tape for whichever Friday in the month you are on (1-4).
- In addition, on the last day of each month make a month-end tape which you store off site and never reuse. This is your fail-safe in case of environmental failure at the school.

Testing the back-up system

No matter how sophisticated or comprehensive your back-up system is, you will never know if it works unless you actually test it. Without testing, you can have no confidence in the backups as errors may creep into the back-up system. Examples of such errors include:

- failed backup software – the backup software simply fails and when you restore the data from the backup media, many files are missing or corrupted
- incomplete data – the backup may be configured to back-up only part of the data
- magnetic interference – tapes are susceptible to damage if stored near a magnetic field such as a loudspeaker
- encryption – when the back-up software was installed and configured, someone set it up to write encrypted backup tapes and now nobody knows what the password is
- old version – an old back-up tape cannot be restored because it can only be read by an earlier version of the back-up software
- poor quality media – cheaper media may degrade and be unreadable when needed
- tape breakage – a back-up tape breaks during the back-up and is sent off site without anyone noticing.
- Back-up crash – if the server crashes during an unattended back-up, it is not always obvious that the back-up has not completed.

These are just some of the things that can go wrong. The important thing is to realise that there is a number of things that can go wrong with a back-up operation. Some of those things will be intermittent. Others may affect all back-ups, meaning that all your back-ups will be useless.

The only way to tell if your backups are working is to actually load a back-up tape and see if the data is correctly restored. This may be difficult or impossible if you have filled the hard disk to capacity. However, testing your back-ups is such an important activity that it really is worth either reducing your disk usage to less than half of your hard disk, or finding another hard disk so that you can perform a test restore.

When testing back-ups always ask yourself if you would feel comfortable erasing your hard disk right now, and restoring it from your backups.

PvM Appendix C Maintaining Apple workstations

To keep your Apple workstation in top condition, here are some simple procedures you can perform, together with our recommended maintenance schedules, starting with the things you should do every day.

The suggested schedules are for a typical Mac owner. If you use a lot of publishing, video or multimedia applications, you may need to perform these procedures more often.

Daily maintenance procedures

Back up your data files

Backing up your data is the only way to recover from disaster. If your hard drive fails, the files it contains will be lost for ever.

The simplest back-up method is to copy important files to a diskette or removable hard disk. Permanent back-up archives should be created using recordable CDs or magneto-optical (MO) drives. If you have a server on your network, consider at least storing your most critical files on one of the server's hard drives instead of the local workstation drives.

Back-up software will make backing up your files easier. You can use:

- free back-up utilities, which often ship with removable drives
- shareware back-up utilities, which are available for download from the internet
- commercial back-up software, which is often the most effective but also the most expensive option.

Restart your computer

Sometimes when a program is closed it leaves a small residual amount of memory allocated (known as memory leakage). This memory is not available for other applications or program data to use. Eventually, depending on how many programs are opened and closed, a significant amount of memory may be used up in this way.

If the memory gets seriously low and you try to open a large document or launch an application that uses lots of memory, the residual memory can prevent the new data from loading correctly. This can cause freezes, out-of-memory errors and applications that crash. Having to restart by powering off and on without closing the computer properly can lead to hard drive corruption and more serious problems in the future. Restarting the computer flushes the memory completely, so you can start afresh with all your memory space available.

Weekly maintenance procedures

Check your hard drive for errors

Once each week you should run Disk First Aid (it comes free with your system software) or a commercial hard disk diagnostic and repair utility to eliminate any errors and corruptions. These can occur for any number of reasons, and eventually they will cause the drive to fail.

To check (and repair) your internal hard drive, you will need to start up your computer using something other than the internal hard drive as the 'boot disk' (the drive that contains the system software currently running the machine). You can use the Disk Tools diskette that came with your computer (the Mac looks to the diskette drive first when searching for usable system software) or your system software CD (holding down the 'C' key during start-up forces the machine to use the system software on your CD-ROM).

Be sure you are using the newest version of Disk First Aid for your computer by visiting the Apple website and downloading the latest version. And, for more

advanced software that will repair a wider range of hard drive problems and provide additional diagnostic/repair benefits, consider purchasing a commercial or shareware package.

Check your system for viruses

Viruses generally are not a problem for Macs. When last counted (2003), there were only about 63 known Macintosh viruses. If you do get a virus, however, it can eventually erase data files, system files, fonts and applications.

There are commercial virus removers suitable for use on Macs. Check the guide to installing antivirus software to determine the best approach to dealing with viruses. Even if your Apple computer has been infected with a virus, there is a feature built into the QuickTime settings that will prevent the virus becoming alive. To do this, you open up the QuickTime Settings control panel, and find the 'Enable AutoPlay' (or 'Enable CD AutoPlay') option and 'uncheck' the box to turn it off. Restart your computer to implement the changes. If your computer does not have a QuickTime Settings control panel, you are using an older version of the QuickTime software. Only QuickTime v2.5 or higher contains this control panel. Visit the Apple website to download the latest version. Without it, your computer is at risk of infection.

Back up your less-critical documents

In addition to backing up your data files daily, once a week you should back up your system, applications, fonts and utilities folders. Backing up these files will allow you to recover from catastrophes much faster. Be sure to check for hard drive corruptions and virus infections before backing up or your back-ups may have the same problems.

Monthly maintenance procedures

Monthly maintenance procedures

The desktop database consists of two invisible files that remember everything stored on your hard drive, and how the Finder should display them. This is no easy job, especially when you have thousands of files. Sometimes, especially after forced restarts or system crashes, the desktop database gets corrupted. The most obvious signs of corruption are file icons that do not look right, missing files, aliases that are unable to find their originals, or data files that cannot find the original application which created them.

To rebuild your desktop, restart your computer. Then, as soon as you hear the start-up chime, hold down both the 'Option' key and 'Command' (Apple) key on your keyboard. Eventually you will see a message asking if you're sure you want to rebuild the desktop. Click on 'Yes'. The computer will then rebuild the desktop database for every mounted disk. Each disk and drive contains its own database.

Apple's built-in 'desktop rebuild' command attempts to rebuild the database using the existing database information. If portions of the database are severely corrupted, the bad parts can still be present in your new database. There is a free utility called TechTool from MicroMat that helps make rebuilding much easier. It completely erases the desktop database and rebuilds it from scratch, eliminating the possibility of including corruptions in your new database.

Clean your computer and peripherals

Computers produce static electricity, which attracts airborne dust, smoke and other debris. These can build up on your monitor screen, stick to the casing, or be sucked inside the computer by the fan. In addition, the natural oils and perspiration on your hands can also get inside your mouse or left on your keyboard keys.

The following should be part of your monthly routine:

Activity	Directions
Clean your monitor screen	Turn the computer and monitor off. Use diluted glass cleaner (dilute 1:1 with water). Spray it on a clean, lint-free cloth and wipe away the dirt. Never spray liquid cleaner directly on the screen as it can get inside the case, and never use full-strength cleaner as it might remove the monitor screen's anti-glare coating.
Clean your computer casings	Turn the computer and monitor off. Use diluted glass cleaner (dilute 1:1 with water). Spray it on a clean, lint-free cloth and wipe away the dirt. Never spray liquid cleaner directly on the screen as it can get inside the case, and never use full-strength cleaner as it might remove the monitor screen's anti-glare coating.
Clean your mouse	Wipe the outside as described for the computer casing. Then, turn the mouse over and remove the bottom plate – twist to unlock. Wipe the ball clean using a lint-free cloth. Remove any dirt on the rollers by gently scrubbing them using a cotton swab moistened with alcohol. Never use a sharp object to scrape the rollers as it might scratch them permanently.
Clean your mouse	<p>Wipe the outside as described for the computer casing. Then, turn the mouse over and remove the bottom plate – twist to unlock. Wipe the ball clean using a lint-free cloth. Remove any dirt on the rollers by gently scrubbing them using a cotton swab moistened with alcohol. Never use a sharp object to scrape the rollers as it might scratch them permanently.</p> <p>Leave the mouse 'open' for a few minutes to dry completely, and then reassemble. Never disconnect the mouse or keyboard while the computer is running as this can damage the motherboard.</p>
Clean your keyboard	Turn your keyboard upside down and shake it vigorously to dislodge all the grit, paper clips, staples and crumbs that have accumulated inside. Wipe the outside as described for the computer casing. You can clean the keys using a cotton swab saturated with alcohol or spray cleaner. Never spray or pour anything directly on the keyboard. Use only gentle pressure when cleaning the keys to avoid damaging the individual key springs. Let the keyboard dry completely before using. Never disconnect the mouse or keyboard while the computer is running as this can damage the motherboard
Get rid of the dust	Using a clean cloth or cotton swab moistened with alcohol, wipe away any visible dust that has accumulated behind or under the computer, or in the vent holes and other openings in the casing, disk drive slot, and so on. Never stick a cotton swab deep inside the diskette drive or CD-ROM drive slot, as this might misalign the read/write heads. Instead, use a small electronics vacuum to remove dust from the casing openings, drive slots and keyboard.
Use compressed air with caution	Many computer shops sell small cans of compressed air to help keep your computer free of dust. Make sure the dust is removed and not just blown to another part of the computer. Be careful when using compressed air near the CD-ROM or diskette drive openings, as dust forced inside can damage the drive mechanisms and read/write heads.
Don't ever oil or lubricate anything	There is no part of a computer that could benefit from oil or lubrication. Grease, oil, WD-40 and other lubricants will cause permanent damage to the electronic components and mechanical devices inside your computer.
Be wary of diskette and CD drive cleaners	Most drive-cleaning kits work by scraping dust and dirt from the drive's read/write heads. Too much use can cause permanent damage to the heads.

Quarterly maintenance procedures

Defragment your hard drive

When you create and save a new document, the computer writes it onto the hard drive wherever it finds a big enough space. If you make changes to that document and save again, the computer only saves the parts that have been changed, and it writes those changes somewhere else on the disk. Over time, all these changes can result in a single document that consists of many little pieces scattered around your drive. That is called disk fragmentation.

When a disk is fragmented, your computer cannot access or store files efficiently and may slow down as the drive has to work harder to load and save files. The extra work may reduce the life span of your drive, while the desktop database has more items to keep track of, which increases the risk of database corruption.

To defragment a drive:

- before starting, check the drive with a disk repair utility to remove any corruptions that could cause problems
- back up critical files before you start, as there is a slight chance that system problems may occur during the defragmenting process which could damage the files on your disk drive
- use a defragmentation utility to defragment the disk, running the program for each disk on your system.

The process of defragmenting picks up all the files on your disk, joins the various pieces back together into one file, and places them back on the disk in a neat and orderly fashion. You can reduce disk fragmentation by using the 'Save As' command as the 'Save As' command creates a brand new file on the disk, all in one piece.

Zap your PRAM

Parameter RAM (PRAM) is a small memory chip on your computer's motherboard that remembers the parameters (settings) you've chosen in various control panels, such as screen display options, mouse speed settings, memory settings, network connections, desktop image settings and clock settings. If your PRAM gets corrupted by improper shutdowns or two applications that try to control the same settings, the computer can act strangely – as if it has forgotten how you like to work.

To zap the PRAM:

- restart the computer and immediately hold down four keys:
COMMAND-OPTION-P-R
- the computer will restart a second time but keep holding down the
COMMAND-OPTION-P-R keys
- the computer will restart a third time – now release the keys and let the
computer start normally
- when the computer has finished booting, open the control panels and enter
your preferred settings.

To make PRAM zapping easier, use the free MicroMat TechTool utility, which completely erases the contents of the PRAM so you can start afresh.

The PRAM is able to remember your settings, even when the machine is turned off, because a small battery on the motherboard provides just enough electricity to let it remember things. If your computer frequently loses the PRAM settings the battery may be dead. Some Macs will not even start up if this battery dies.

Annual maintenance procedures

'Clean sweep' your system

Most Apple service providers recommend that once a year or after every 2,000 hours of use you should give the computer a thorough clean and then erase the hard drive and reinstall all your applications and system software. A process called a 'clean sweep.'

A clean sweep will need to be carefully planned.

- Obtain the latest versions of the Mac OS (operating system), patches, enhancements and bug fixes for all your applications.
- Back up everything on your hard drive.
- Write down all your software serial numbers and important internet connection information, local dial-up numbers, DNS addresses, passwords and so on.
- If you are considering incorporating any hardware upgrades such as installing more memory, replacing your hard drive or installing a graphics accelerator, have the parts ready, along with any software and instructions the manufacturer has provided.

Read this section very carefully before opening the computer casing.

Before working inside a computer, you must discharge all static electricity from yourself and your work area. Failure to do so could permanently damage your computer. Computer shops sell inexpensive grounding wrist straps for this purpose. If you do not have a grounding strap, follow these steps to discharge all static electricity:

- Make sure the computer's power is turned off, and all peripherals (keyboard, mouse, monitor, scanner, etc) are disconnected from the computer. Leave the power cord connected to both the computer and the electrical outlet.
- Open the computer's plastic case and gently touch the metal frame inside the computer. Any static charge you are carrying should pass safely through the computer's power supply and into the earth wire of your home or office electrical system.
- Once you have discharged the static electricity, do not move away from your work area! Immediately unplug the power cord from the computer and get to work. If you move around the room, you may develop another static charge!

On some models, the motherboard slides in and out of a hole in the back of the computer. Do not remove the motherboard until you have simultaneously touched both the computer's metal frame and also the work surface where you intend to rest the motherboard. The work surface may have its own static charge.

Warning!

If you have an 'all-in-one' Mac (such as an iMac) that has a built-in monitor, never open the plastic casing. Some components attached to the monitor store dangerous levels of electricity even when the computer is turned off and unplugged. Touching these components can result in severe injury or death.

Activity	Instructions
Remove dust	<p>With the case open and all static electricity safely discharged, use a very small, very soft paintbrush and a can of compressed air to loosen any accumulated dust and blow it away.</p> <p>Be sure to hold the air can upright at all times, or the liquid propellant may hit the motherboard.</p> <p>Pay special attention to removing dust from the drive mechanisms, the power supply, the cooling fan, and the processor. Blow from the inside towards the outside.</p>

Activity	Instructions
Install any new hardware	<p>Be sure to wear the anti-static grounding wristband or take the precautions outlined above to prevent static build up.</p> <p>Remove any redundant hardware and replace with new components. Add any other new items and close the computer casing.</p>
Format the hard drive	<p>Reconnect all hardware peripherals and plug everything in. Insert the Mac OS CD-ROM into the computer and start it up. If starting from the CD, hold down the 'C' key. Once the machine has booted up, reformat the hard drive with the newest version of Apple's Drive Setup utility software.</p> <p>Reformatting the drive will eliminate all corruptions, identify and mark any physical problems in the drive storage media and install the newest drivers that tell your computer how to communicate with the hard drive.</p>
Reload the operating system	<p>Load the new system software (Mac OS) on your freshly formatted drive, restart the machine and check the drive with Disk First Aid or your hard drive repair utility to make sure that everything is as it should be.</p>
Install drivers and applications for new hardware	<p>One by one, install the drivers and applications for any new hardware you added to the computer.</p> <p>Read all the Readme files, remove any unnecessary files, test each device as soon as it is installed, and restart the machine after each step.</p>
Re-install applications and data	<p>One by one, re-install the newest versions of each software application, any fonts you own, and any data files that you need to have available. Most data files can be left on your back-up disks.</p> <p>Set the control panels and preferences back to the way you prefer, organise as you go, read all the Readme files, remove any unnecessary files, test each software application as soon as it is installed, and restart the machine after each step.</p>

Although the entire clean sweep process can take several hours, when you have finished you will have a 'brand new' computer that is completely bug free and stable.

PvM Appendix D Maintaining servers

Your **server** is the most critical component on your network, often accomplishing many tasks such as:

- ensuring that printers are available to everyone on the network, and regulate printing so that it happens in an orderly fashion
- providing virus protection to all clients on the network
- sharing information from central CD-ROMs
- creating nightly back-ups of important information stored on servers or clients
- monitoring **network traffic** and warning of impending trouble
- displaying information from shared databases such as student records, lesson plans, attendance information, or lists of web links
- ensuring that only authorised users can see sensitive information
- providing a centre where applications can be stored, updated, and delivered to clients.
- It is therefore very important to make sure your servers are in good health at all times. this line should not be bulleted.

One aspect to consider is whether your server is working too hard. You may want to consider installing and running more than one server and assigning specific tasks to specific servers if:

- some of your application programs require a great deal of processing power (that is, they require a server all to themselves in order to run efficiently)
- your network is very large (perhaps more than 500 clients) and includes many different kinds of network services such as email, access to the internet, web publishing, and databases (accounting, student records, or computer-based instruction systems)
- your network includes extremely sensitive information that would be protected best if it occupied a server separate from all others (unauthorised users can be denied access to everything on this server, or even to the part of the network where it resides).

Whatever your server configuration, servers that run reliably have one common characteristic: someone watches them like a hawk. Someone knows their **baseline** performance, detects any variation from that, takes appropriate action to ensure undetected incidents don't become **problems** and logs any actions taken.

For the systems you believe to be critical, make sure that someone performs the following preventative maintenance every day. At least two technical staff should know how to perform all preventative maintenance procedures.

Daily server maintenance

Although each type of server requires different daily procedures, certain tasks are common to all server types.

- Use the server logs. Servers keep logs of internal errors. Technical staff should be familiar with the location of all these logs, check them daily, and attend to any errors immediately.
- Use the server statistics. Servers also keep many different kinds of usage statistics such as collisions among data packets on the network, percentage of server processor utilisation and peaks in network traffic. Technical staff should become familiar with how these statistics look at different times of the day and be suspicious of any unexplained variation from normal behaviour. They should take action to keep the machine at its baseline performance.
- Check the system daily. Major software systems keep logs of their activity and errors, as well. Technical staff should check each of these major systems daily. These systems include email, web servers, accounting programs and student records databases.
- Keep a record of error messages. Whenever errors occur technical staff should print any error messages and keep them permanently in a logbook. If they take action to address an incident or problem, they should record the date of the action, their names, and a summary of the steps taken. Over time, these logbooks provide invaluable troubleshooting and support tools. Technical staff can look back to see how they solved an incident or problem, or how one solution caused another set of incidents or problems.

Monthly server maintenance

Restart the server. Most servers need to be restarted periodically. In part, restarting clears hidden difficulties in memory that may rise at an unexpected moment to bring your server down. Additionally, restarting exercises all the components of your system such as hard disks, memory and network connections. Restarting tests a computer and sometimes forces a failure that otherwise might occur at a more inconvenient moment. Many schools bring their servers down once every month or two.

Six-monthly server maintenance

Test all procedures. Support staff should simulate procedures for starting servers in an emergency. Most servers provide diagnostic tools for booting (starting) and helping to identify the source of incidents and problems. The tools for booting include special disks or tapes. These disks and tapes must be prepared ahead of time, when the server is healthy. Technical staff should know the location of these boot disks/tapes, and they should test the boot procedures periodically. Most disks and tapes degrade over time, and many sites recreate their boot disks or tapes periodically to refresh them. In addition to emergency boot procedures, servers provide diagnostic software. Staff should know how to locate and use this software.

General guidelines for server maintenance

You may find the following general guidelines helpful.

- Keep a list of all system passwords in a secure location. All support staff should know the location of passwords. They should keep the list up to date. Make sure that passwords to privileged accounts (system manager, administrator and so forth) change frequently.
- Post and maintain a list of emergency support telephone numbers, customer identification numbers and all additional numbers required to secure support.
- Have a support contract from the manufacturer for your most complex systems (accounting, student records and so forth). While your ICT staff should still have thorough knowledge of all your equipment and be responsible for its daily care, outside experts can be invaluable in times of trouble.

PvM Appendix E Setting up RAID

What is RAID?

RAID is an acronym for 'redundant array of inexpensive disks'. RAID is a technique using two or more disk drives in combination for fault tolerance and performance. RAID disk drives are used frequently on servers but aren't generally necessary for personal computers.

There are number of different ways to use multiple disks together in a RAID scheme and these are known as RAID levels. There are many different RAID levels, and some manufacturers have developed their own variations. Although this can make RAID confusing, the four levels of most interest to schools are 0, 1, 3, and 5:

- Level 0 provides data striping (spreading out blocks of each file across multiple disks) but no redundancy. This improves performance, but does not deliver fault tolerance.
- Level 1 provides disk mirroring, which gives good data protection but no performance benefit.
- Level 3 is the same as Level 0, but also reserves one dedicated disk for error-correction data. It provides good performance and some degree of fault tolerance.
- Level 5 provides data striping at the byte level and also stripe error-correction information. This results in excellent performance and good fault tolerance.

Why install RAID?

The basic idea of RAID is to spread a server's data across multiple disks seamlessly. For example, a single file might be spread across four or five disks. The RAID system manages all those parts so that when a file is opened the RAID system accesses all the appropriate disks and reassembles the file.

The immediate benefit is that the multiple disks perform much more quickly than a single disk. This is because all the disks work independently on finding their own

data and sending it to the controller to be assembled. A single disk drive would be limited by a single disk head and would take much longer to gather the same amount of data. In fact, the performance of a RAID system increases as you add more disks to the array.

You might think that by spreading data across multiple disks you are increasing the chance of data loss due to disk failure. RAID addresses this by creating checksums and error correction, so that if one or more disks are damaged the data can still be retrieved. This makes for a very efficient and cost-effective way to manage your data.

Choosing appropriate RAID for your school network

The following guide will help you decide which RAID system is most appropriate for your school:

RAID system	Feature	Main consideration
Level 0	Good performance but no protection	Low cost
Level 1	Data duplication but no performance benefit	Data redundancy
Level 3	Good performance with some fault tolerance	Data protection
Level 5	Better performance plus good fault tolerance	Efficiency and protection

Installing RAID on your server

Pre-installation

- **Configuration**

Choose the configuration that meets your performance, storage, availability, and serviceability needs. Stick with standard configurations for the best price/performance and ease of service, unless your requirements dictate otherwise. Ask the difficult questions before buying anything. The higher your availability requirements, the more redundancy and component removability you require.

- **Back up**

Ensure that your back-up device and procedures are adequate to handle the increased storage in the time available.

- **Power**

Ensure clean power and UPS protection.

- **Interference**

Check for nearby sources of electromagnetic interference, such as banks of modems on web servers.

- **Load**

Is the system totally loaded already? Will the addition of one more device, especially a high-performance RAID array, push the load limit over the edge?

- **SCSI interface**

Is the interface fast enough to avoid bottlenecking the new high-performance equipment?

- **Service**

Decide who will perform remedial service.

- **Spare parts**

Do you need spare parts?

- **Performance benchmark**

This is so that you can test how much faster everything runs with the new high-performance storage. Time your longest batch jobs and measure client response to lengthy transactions before and after installation.

- **Capacity assessment**

Based on performance benchmarks, you can make a reasonable estimate of how many users you can support on the existing server before you need to add another one.

During installation

- **Scheduled downtime**

Make sure that there will be enough time to install the system properly. Allow plenty of time and anticipate that it will take longer than expected.

- **Test period**

The more critical the application, the longer the new systems need to bed in. Several days of running diagnostics, exercises and representative applications is a reasonable precaution to take before committing your entire school network to a new RAID system.

- **Training**

Make sure one or (preferably) two or more people are trained on the system. Training includes setting up RAID arrays, swapping components, rebuilding arrays, simulating failures and, most importantly, practising what to do in the event of actual failures.

After installation

- **Protection of your data**

RAID is no different from any other storage device when it comes to protection from viruses and accidental or deliberate deletions. Implement the same file-protection and record-locking strategies you would use on a non-RAID system.

- **Data back-up**

Typically, RAID systems significantly increase your total storage capacity. Make sure you do a complete back-up frequently and incremental back-ups at least daily. Test data restoration periodically to ensure that you remember how to do it and to check that the tape system is working properly.

- **Data security**

Make extra back-ups and keep copies off site.

PvM Appendix F Maintaining switches, hubs and routers

Purchasing, installing and maintaining switches

When you purchase and install a **switch**, you should review and apply the following criteria.

- Your switches must be compatible with your physical and data link level protocols. If you are running a **10BaseT** Ethernet network, then you must purchase a 10BaseT switch.
- Some switches can accommodate more than one physical or data-link level protocol. For example, modern switches accommodate both 10BaseT and 100BaseTX protocols. It is wise to purchase a switch with at least one 100BaseTX port, since you can interconnect your switches via their high-speed ports to improve network performance (even if the remainder of your network uses 10BaseT).

- If you purchase a switch that accommodates more than one protocol, then make sure that it automatically senses which protocol is being used on each port. Auto-sensing switches ensure that you can connect any part of the network to any switch port. (Older switches required you to attach each segment of the network to a port compatible with its physical and data-link level protocol. Keeping the segments and ports straight presents a management challenge.)
- Purchase switches from a known manufacturer whose support you trust. Make sure that the manufacturer provides a competitive warranty.
- If possible, install your switches in a room that is cool and free of dust. Additionally, plug your switches into an uninterruptible power supply (UPS) to ensure that they receive clean power.

Purchasing, installing and maintaining hubs

When you purchase a hub, you may wish to keep the following information in mind.

- Like switches, your hubs must be compatible with your physical and data-link level protocols. If you are running a 10BaseT Ethernet network, you must purchase 10BaseT hubs. Some hubs, called multiprotocol hubs, can accommodate more than one physical and data-link level protocol. If you purchase a multiprotocol hub, make sure that it automatically senses which protocol is being used on each port. Auto-sensing hubs ensure that you can connect any part of the network to any hub port. (Older hubs required you to attach each segment of the network to a port compatible with its physical and data-link level protocol. Keeping the segments and ports straight presents a management challenge.)
- Make sure that your hub includes an AUI port (connector). (AUI is an abbreviation for attachment unit interface.) AUI ports are intended to connect with a kind of cabling called thick coaxial cable (like that used for cable TV). While this cable is no longer often used for Ethernet networks, AUI ports are versatile in the sense that they can be fitted with adapters to connect to many different kinds of cable (for example, thin coaxial cable or fibre).
- Also make sure that your hub includes a crossover port. Unlike regular hub ports, which connect hubs to clients, servers or peripherals, a crossover port connects one hub to another. Some hubs can be stacked. Stackable hubs look like one giant hub to the network. That is to say, the Ethernet restriction on the number of hubs that can be traversed in a single network does not apply to stacked hubs
- Purchase hubs from a known manufacturer whose support you trust. Make sure the manufacturer provides a competitive warranty.
- If possible, install your hubs in a room that is cool and free of dust. Additionally, plug your hubs into an uninterruptible power supply (UPS) to ensure that they receive clean power.

Purchasing, installing and maintaining routers

When you purchase and install a router, you may wish to keep the following points in mind.

- It is best to purchase all your routers from a single manufacturer. Purchasing routers from a single manufacturer ensures that the software you use to configure and manage the routers via the network will be compatible across devices. It is very important to be able to monitor and manage routers across the network if you want to keep things running smoothly. Make sure that your router manufacturer offers a wide variety of routers, including models for local area networks, dial-up connections, and wide area networks so that you can continue to purchase from the same manufacturer as your network grows. Consult other schools to see which router manufacturers they have used and liked.

- Before you purchase a router, you should draw a picture of your network, including the place where you intend to put the router. Then label the **segments** on either side of the router with the kind of cable used as well as with the protocols that will travel across the router to and from each segment. Your router must accommodate the cable types on all adjacent segments. In addition, the router must be compatible with protocols that appear on both sides of the router.
- Before installing a router, choose the router model(s) that you need. Document the protocols in use, the kind of information that will be exchanged on the attached network, the kinds of information that may be restricted, the number of users and their patterns of usage. Match the router's capabilities to your particular network needs.
- Routers are often expensive. Your router should be easily upgraded so that you need not replace the entire device as your network incorporates additional kinds of cable or protocols. Ask manufacturers about the particular expansion modules they offer, and what is involved in purchasing, installing, and maintaining them.
- If your school plans to deliver multimedia applications over the internet, choose a router that is capable of providing QoS (quality of service) services. Multimedia applications require a fast, steady stream of data to function properly. To deliver this increased performance, internet standards organisations have defined options that allow routers and other network devices to reserve the bandwidth they need on the internet. Such equipment assures QoS, for specified purposes. If you are planning for multimedia delivery over the internet, you may wish to make sure that your router does so.
- Price should not be the determining factor in purchasing a router. Routers, like servers, are key components of your network. It is far better to purchase reliable equipment from recognised manufacturers than to suffer equipment breakdowns or malfunctions.
- Like switches and hubs, routers need to be installed in a room that is cool and free of dust. Additionally, plug your routers into an uninterruptible power supply (UPS) to ensure that they receive clean power.

PvM Appendix G Installing a firewall

What is a firewall?

A firewall is a system that stands between your **network** and the internet and acts as a gatekeeper, allowing in trusted friends and keeping out known or suspected enemies.

A firewall can be a single **device** such as a **router**, computer or dedicated hardware appliance which has software capable of making the decisions needed to monitor the flow of data to and from your school's network.

Why install a firewall?

If your school network is connected to the internet, you need a firewall. There are so many different ways in which your network can be compromised. Some of them include:

- denial of service attacks
- SYN flooding
- ICMP redirects
- ping of death
- forged email
- spoofing and impersonation.

Hackers are constantly finding new ways to damage your network so, although you don't need to understand what all the above mean, you do need to ensure that your network is protected from such attacks.

A firewall is your first line of defence. Firewalls, however, cannot protect you at all from another major source of attack; computer viruses, Trojan horses or other destructive programs. For protection from these you need to install a good antivirus program (see [Appendix A](#)).

Choosing a firewall for your school

In most cases your internet service provider or broadband supplier will offer a firewall as part of its solution. However, it may be worth checking that it meets the requirements of your school.

Installing and managing your own local firewall solution can often be more complicated and costly than using the solution already provided for you. If you choose to operate your own firewall, there are two techniques that are relevant to school networks: network-based firewall and application-based firewall.

Network-based firewall

A network-based firewall (also called packet filtering) works by filtering packets. It can be set up to block traffic by creating filters for:

- IP addresses (you can specify individual or ranges of addresses)
- Protocols (such as UDP or TCP)
- port numbers (to identify connections between applications such as FTP or Telnet)
- direction (filtering can be based on whether the network packet is coming into the network or being sent out by a network user to the internet).

Packet filters come in many forms, but the most common are built into standalone routers that sit between your modem and the rest of the network.

This simple and cheap device maybe adequate if your network is relatively small (up to 50 workstations) or if you are connected to the internet via a dial-up modem.

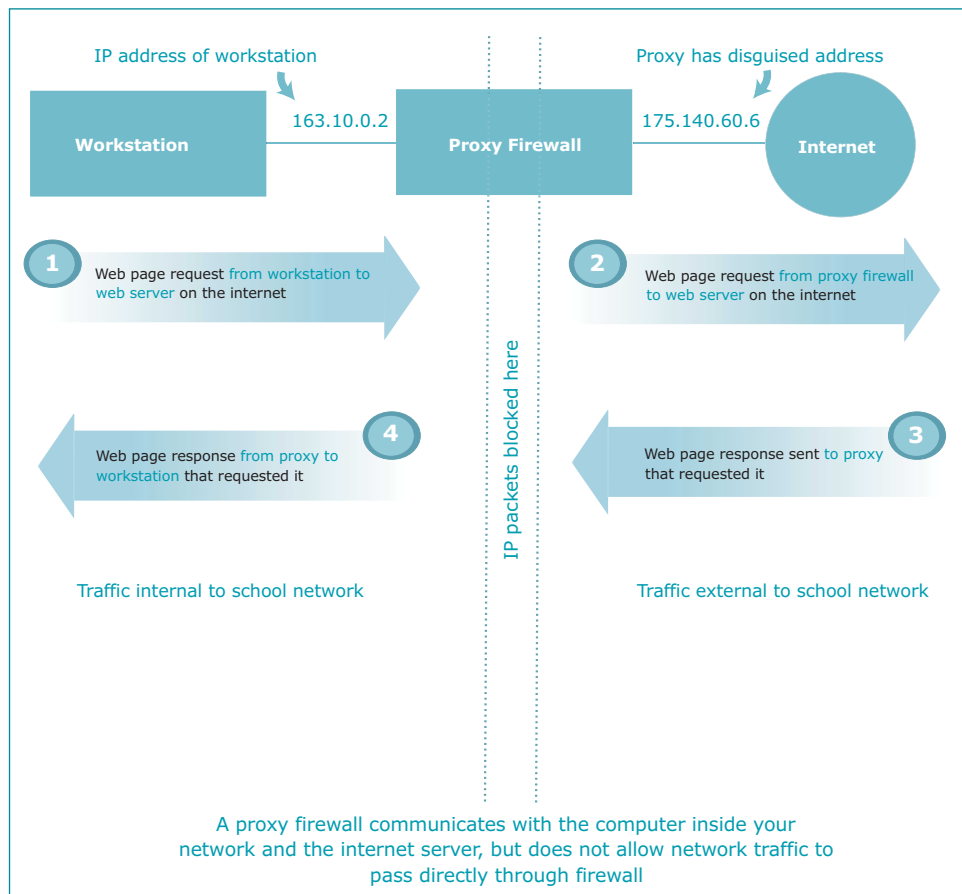
Although packet filters make decisions based on the header information in a packet, they do not understand the application protocols such as FTP or HTTP. Thus it is easy for a hacker to exploit known problems with application protocols, and problems can ensue if the packet filter allows the packet to enter the network.

If your network requires a greater level of protection, you should consider installing a proxy firewall.

Application-based firewall

An application-based firewall (also known as an application gateway or proxy firewall) provides protection for your network at the application layer. It performs this function by managing connections to and from the outside world. A proxy firewall acts as a middleman for the users on one network to interact with services on the other network. This interaction usually uses a technique known as network address translation (NAT), where the addresses on the internal network are not directly exposed to the external network.

In the application-based firewall the proxy takes care of translating the address so that the connections can take place. A proxy firewall never allows a packet to pass through the firewall.



This is a more complex solution but should be adopted for larger networks where there is a lot of internet-based traffic.

Proxy firewalls are implemented by installing a software application on a computer. For networks up to 250 workstations the software may share a computer with other applications such as an email server. For larger networks (250+ workstations) the software will need to run on a dedicated computer to ensure optimum performance of your internet connection.

Most major software suppliers sell firewall software. The choice for your school may be based on the following criteria:

- cost
- operating system used
- compatibility with existing applications
- ease of installation and use.

In addition, there are many freeware and shareware packages available. It is worth downloading and trying out some of these cheaper options before committing your school to an expensive proprietary system.

Maintaining your firewall to keep it effective

The problem with security is that the environment is always changing. As soon as a bug on an operating system or application is found and exploited by a hacker, someone comes up with a fix. As soon as the fix is applied, something else crops up. When you set up a firewall to protect your network, you must perform tests to be sure that it does what you think it does.

The problem with testing, however, is that you already know what you're looking for when you create and execute the test. To keep on top of things you should also:

- monitor the data collected by any auditing or logging functions the firewall provides
- look for attempts to breach the firewall
- watch for unusual activity
- check the internet for the latest information on security issues
- keep your firewall software up-to-date.

If you find you are being attacked, the best option is to use a utility such as TRaceRT to locate the source of the attack and notify your ISP.

PvM Appendix H Setting up a maintenance schedule

Determining when to carry out maintenance

You need to carry out some types of preventative maintenance more often than others. The frequency of preventative maintenance may depend on:

- how much each type of equipment is used
- the environment in which the equipment is used or stored
- **problems** identified as part of the **Problem Management** process.

A typical school network will always have a number of occurrences of equipment failure. These necessarily take precedence over routine maintenance activities. Keeping a plan of maintenance tasks will allow you to reschedule those activities that have to be delayed.

The other issue facing a preventative maintenance programme is simply remembering to do the tasks. It is one thing to decide that the read/write heads on floppy disks need cleaning every six months, but how will you remember when the six months are up? One way to address this issue is through the use of a preventative maintenance schedule, which will remind you of when perform key maintenance activities. Some software preventative maintenance activities can also be automated.

Automating preventative maintenance

There are software-related preventative maintenance activities that can be automated. By using system tools that automatically run programs at a specific time, you can set up your system to perform various software checks and maintenance activities without having to remember to do them yourself. Most modern operating systems either have this capability built in, or support third-party software packages that will do it for you. Of course, you cannot perform hardware-related maintenance such as cleaning or adjustments automatically.

The following is a list of activities that can be set to run automatically:

- checking the file system for errors
- checking all hard disks for read errors
- scanning all hard disks and files for viruses
- defragmentation of all hard disk volumes.

Preventative maintenance schedule

A preventative maintenance schedule can take many forms. There are commercial software programs available that will allow you to schedule and track your maintenance activities. The simplest method, however, is a chart that shows various maintenance activities and how often they should be done. These allow you to set up a calendar so that you remember to do your maintenance tasks. Once you have set up a schedule, you can translate it to actual dates to help you remember when to perform various preventative maintenance activities.

Software procedures, which often should be performed daily, are best done using some sort of automated program scheduler. For tasks you perform at longer intervals, you can simply mark the activity down on a calendar. If you have appointment book software, you can put reminders for the key maintenance tasks.

When setting up a maintenance plan it is important not to make the schedule too aggressive, otherwise maintenance becomes tiresome and it is likely that none will get done.

As many maintenance activities require you to open up a computer, it may be helpful to have an annual 'clean the computer day'. This allows you to keep your workstations running at top form without having to open them up several times a year.

The frequency of maintenance tasks is determined in part by the prevailing conditions of the PC itself and the environment in which it is kept. For example, if the PC is subject to constant abuse or vandalism, then you will need to make the cleaning routine more frequent.

Sample maintenance schedule

The sample schedule below for maintenance of a PC is organised by recommended frequency. The right-hand column is for those activities that can normally be set to run automatically using a program scheduler.

Preventative maintenance activity	Recommended frequency	Automatic
Scan hard disk file systems for errors	Weekly	Yes
Scan for viruses	Weekly	Yes
Clean CRT screen	Weekly	Yes
Defragment hard disks	Weekly	Yes
Scan for hard disk read errors	Weekly	Yes
Clean mouse	Monthly	No
Check for full hard disk volumes and remove unnecessary files	Monthly	No
Update virus definition files	Monthly	Sometimes
Check that power protection devices are still protecting the system	Quarterly	No
Check power supply fan for ventilation and dirt build-up; clean if necessary	Quarterly	No
Update emergency boot floppies	Quarterly	No
Clean floppy disk-drive internals and read/write heads	Quarterly (depending on use)	No
Check processor temperature; inspect heat sink and fan to ensure that they are working	Annually (or whenever case is opened)	No

Preventative maintenance activity	Recommended frequency	Automatic
Check hard disk for temperature and vibration	Annually (or whenever case is opened)	No
Back up CMOS information	Annually	No
Clean exterior of case	Annually	No
Clean exterior of monitor	Annually	No
Check and clean interior, motherboard and expansion cards if necessary	Annually	No
Check internal connections and cables	Annually	No
Clean keyboard	Annually	No

PvM Appendix I Developing fail-safes

What is a fail-safe?

All network equipment will fail eventually. The equipment may reach the end of its useful life, it may fail because of physical (malicious or accidental) damage, or it may be the victim of environmental damage such as a power spike, lightning strike or overload from adjacent equipment. A fail-safe is any method or device used to reduce the chance of failure.

Why install fail-safes?

Installing fail-safes on your network will involve extra cost, but this must be weighed against the cost of replacing expensive network **devices**, the time taken to track down the **problem** and the disruption resulting from the network downtime while the problem is resolved.

While some fail-safe techniques can be expensive to implement, many are well within the range of a school budget. The following section outlines some methods of minimising the chances of network failure and will help you decide the most appropriate level of protection for your school's network.

Choosing appropriate fail-safes for your school

There are four types of fail-safe:

- a protective device such as an uninterruptible power supply (UPS) to protect network equipment from a specific threat (in this case, power failure or power fluctuations)
- a duplicate device connected and working as part of the network such as a RAID array or a secondary cable run
- a hot standby – a duplicate device ready to connect in place of a failed component (the device already loaded with the correct software and configuration to enable the quickest possible swap)
- a spare device that you can configure to replace a failed network component.

The following tables list network components most likely to require fail-safes and identify possible solutions to protect against component failure:

Components requiring protective devices

Component	Risk	Fail-safe options	Pros and cons
Server	Power surge or failure	Uninterruptible power supply (UPS)	UPSs can be expensive but one UPS can supply power to multiple servers and critical devices such as switches.
Workstations	Power surge or failure	Mains surge protectors	Surge protectors are often incorporated in power distribution strips.

Components requiring duplicate devices

Component	Risk	Fail-safe options	Pros and cons
Data	Loss of data due to corruption or disk failure	RAID array (see Appendix E)	RAID arrays can be configured with relatively inexpensive disks and provide a high level of protection for your data.
Cables	Malicious or accidental break to cable runs	Alternative cable path to destination	Duplicating cable runs may be expensive but a break in a cable can be very time consuming to trace and may result in large parts of the network being unavailable for a long time.
Printers	General failure of printer such as paper jam	Duplicate printing facility, if possible on a different part of the network	Additional printers for critical administration tasks can be connected at low cost. Being mechanical devices, printers are prone to failure.

Components requiring duplicate devices

Component	Risk	Fail-safe options	Pros and cons
Data	Loss of data due to corruption or disk failure	Data back-up (see Appendix B)	Of all the fail-safe methods, this is probably the most important to implement.
Servers	General failure	Duplicate spare server preloaded with required software and configured with correct interface boards	A server is an expensive part of the network but is often the most critical component, managing internet access, email and so on. You will need to weigh the cost of dedicating a spare computer to this task against the level of disruption likely to be caused by server failure and the time it would take to source and build a replacement.
Workstations	General failure	Duplicate spare workstation preloaded with required software and configured with correct interface boards	This option is only worth considering if you have a large number of workstations that have common applications and set-up.

Glossary

10Base-T	A networking standard that supports data transfer rates up to 100 Mbps (100 megabits per second). 10Base-T is based on the older Ethernet standard but is 10 times faster than Ethernet; it is often referred to as Fast Ethernet. Officially, the 10Base-T standard is IEEE 802.3u. Like Ethernet, 10Base-T is based on the CSMA/CD LAN access method.
AppleTalk	Inexpensive LAN (local area network) architecture built into all Apple Macintosh computers and laser printers. AppleTalk supports Apple's LocalTalk cabling scheme, as well as Ethernet and IBM Token Ring. It can connect Macintosh computers and printers, and even PCs if they are equipped with special AppleTalk hardware and software.
Asset	Component of a business process. Assets can include people, accommodation, computer systems, networks, paper records, fax machines, etc.
Availability	Ability of a component or service to perform its required function at a stated instant or over a stated period of time. It is usually expressed as the availability ratio: the proportion of time that the service is actually available for use by customers within the agreed service hours.
Availability Management	To ensure that ICT services are available for use consistently as agreed.
Bandwidth	The amount of data that can be transmitted in a fixed amount of time. For digital devices, the bandwidth is usually expressed in bits per second (bps).
Baseline	A snapshot or a position which is recorded. Although the position may be updated later, the baseline remains unchanged and available as a reference of the original state and as a comparison against the current position.
Bridge	A device that connects two LANs (local area networks), or two segments of the same LAN that use the same protocol, such as Ethernet or Token Ring.
Buffer	A temporary storage area, usually in RAM. The purpose of most buffers is to act as a holding area, enabling the CPU to manipulate data before transferring it to a device.
Build	The final stage in producing a usable configuration. The process involves taking one or more input configuration items and processing (building) them to create one or more output configuration items (eg software compile and load).
Capacity	Ability of available supply of processing power to match the demands made on it by the business, both now and in the future.
Capacity Management	To ensure that all ICT processing and storage capacity provision match present and evolving needs.
Category	Classification of a group of configuration items, change documents, incidents or problems.
Change	The addition, modification or removal of approved, supported or baselined hardware, network, software, application, environment, system, desktop build or associated documentation.

Change Management	The managed and recorded introduction of changes to hardware, software, services or documentation to minimise disruption to ICT operation and maintain accurate configuration information.
Client	The client part of a client/server architecture. Typically, a client is an application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an email client is an application that enables you to send and receive email.
Client/server architecture	A network architecture in which each computer or process on the network is either a client or a server. Servers are powerful computers or processes dedicated to managing disk drives (file servers), printers (print servers) or network traffic (network servers). Clients are PCs or workstations on which users run applications. Clients rely on servers for resources such as files, devices and even processing power.
Configuration management database (CMDB)	A database which contains all relevant details of each ICT asset, otherwise known as a configuration item (CI), and details of the important relationships between CIs.
Configuration Management	Implementing and maintaining up-to-date records of ICT hardware, software, services and documentation, and showing the relationships between them.
Definitive software library (DSL)	<p>The library in which the definitive authorised versions of all software CIs are stored and protected. It is a physical library or storage repository where master copies of software versions are placed. This one logical storage area may in reality consist of one or more physical software libraries or filestores. They should be separate from development and test filestore areas. The DSL may also include a physical store (fire-proof safe, for example) to hold master copies of bought-in software. Only authorised software, strictly controlled by Change Management and Release Management, should be accepted into the DSL.</p> <p>The DSL exists not directly because of the needs of the Configuration Management process, but as a common base for the Release Management and Configuration Management processes.</p>
Device	Any computer or component that attaches to a network.
Error trap	A signal informing a program that an event has occurred. When a program receives an interrupt signal, it takes a specified action (which can be to ignore the signal). Interrupt signals can cause a program to suspend itself temporarily to service the interrupt.
Ethernet	A LAN (local area network) architecture developed in 1976 by Xerox Corporation in co-operation with DEC and Intel. Ethernet uses a bus or star topology and supports data transfer rates of 10 Mbps. The Ethernet specification served as the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. Ethernet is one of the most widely implemented LAN standards.
FDDI (Fibre Distributed Data Interface)	A set of ANSI protocols for sending digital data over fibre optic cable. FDDI networks are token-passing networks, and support data rates of up to 100 Mbps (100 million bits) per second. FDDI networks are typically used as backbones for wide area networks.
Financial Management	To ensure that the ICT and technical resources are implemented and managed in a cost-effective way.

Firewall	A system designed to prevent unauthorised access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorised internet users from accessing private networks connected to the internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
Gateway	A node on a network that serves as an entrance to another network. In schools, the gateway is the computer that routes the traffic from a workstation to the outside network that is serving web pages. In homes, the gateway is the ISP that connects the user to the internet.
Gigabit	When used to describe data transfer rates, it refers to 10 to the 9th power (1,000,000,000) bits. Gigabit is abbreviated Gb, as opposed to gigabyte, which is abbreviated GB.
HTTP (hypertext transfer protocol)	The underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the web server directing it to fetch and transmit the requested web page.
Hub	A connection point for devices in a network. Hubs are commonly used to connect segments of a LAN (local area network). A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
ICT	The convergence of information technology, telecommunications and data networking technologies into a single technology.
Incident	Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service.
Incident Management	To detect, diagnose and resolve ICT incidents as quickly as possible and minimise their adverse impact on normal operation.
ITIL	The OGC IT Infrastructure Library – a set of guides on the management and provision of operational IT services.
LAN	A computer network that spans a relatively small area. Most local area networks (LANs) are confined to a single building or group of buildings.
LocalTalk	The cabling scheme supported by the AppleTalk network protocol for Macintosh computers. Most local area networks that use AppleTalk, such as TOPS, also conform to the LocalTalk cable system. Such networks are sometimes called LocalTalk networks.
Logical topology	The logical topology is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices.
MAC (media access control) address	Each device on a network can be identified by its MAC address, a hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the data link control (DLC) layer of the OSI reference model is divided into two sub-layers: the logical link control (LLC) layer and the MAC layer. The MAC layer interfaces directly with the network media. Consequently, each different type of network media requires a different MAC layer.

Management information base (MIB)	A management information base (MIB) is a database of objects that can be monitored by a network management system. Both SNMP and RMON use standardised MIB formats that allow any SNMP and RMON tools to monitor any device defined by a MIB.
Network	A group of two or more computer systems linked together. The two types of computer networks of interest to schools are LANs (local area networks) and WANs (wide area networks).
Network interface card (NIC)	A network interface card (NIC) is an expansion board inserted or built into a computer so that the computer can be connected to a network. Most NICs are designed for a particular type of network, protocol, although some can serve multiple networks.
Network traffic	The load on a communications device or system.
Node	A processing location. A node can be a workstation or some other device, such as a printer. Every node has a unique network address, sometimes called a data link control (DLC) address or media access control (MAC) address.
OSI reference model	The OSI (open system interconnection) model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station, and back up the hierarchy.
Packet	A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data.
Packet switching	Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.
Peer-to-peer network	A type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client/server architectures, in which some computers are dedicated to serving the others.
Physical topology	The physical layout of devices on a network. Every LAN (local area network) has a topology – the way the devices on a network are arranged and how they communicate with each other.
Port	In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.
Problem	The underlying cause of an incident or incidents.
Problem Management	The detection of the underlying causes of incidents and their resolution and prevention.
Protocol	An agreed format for transmitting data between two devices.
Protocol stack	A set of network protocol layers that work together. The OSI reference model that defines seven protocol layers is often called a stack, as is the set of TCP/IP protocols that define communication over the internet.

Proxy server	A server that sits between a client application, such as a web browser, and a real server. It intercepts all requests to the real server to see if it can fulfil the requests itself. If not, it forwards the request to the real server.
Release Management	To plan, test and manage the successful implementation of software and hardware. To define release policy and to ensure that master copies of all software are secured centrally.
Remote monitoring (RMON)	Remote monitoring (RMON) is a network management protocol that allows network information to be gathered at a single workstation. For RMON to work, network devices such as hubs and switches must be designed to support it.
Request for change	Form or screen used to record details of a request for a change to any CI within an infrastructure, or to procedures and items associated with the infrastructure.
Router	A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs (local area networks) or WANs (wide area networks) or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect.
Segment	A section of a network that is bounded by bridges, routers or switches. Dividing an Ethernet into multiple segments is one of the most common ways of increasing available bandwidth on the LAN.
Server	A workstation or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files. Any user on the network can store files on the server. A print server is a computer that manages one or more printers, and a network server is a computer that manages network traffic. A database server is a computer system that processes database queries.
Service Continuity Management	To minimise the impact on ICT service of an environmental disaster and put in place and communicate a plan for recovery.
Service Desk	The single point of contact within the school for all users of ICT and the services provided by Technical Support.
Service level agreement	Written agreement between a service provider and the customer(s) that documents agreed service levels for a service.
Service Level Management	The process of defining, agreeing and documenting required service levels and ensuring that these levels are met.
Simple network management protocol (SNMP)	A set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in management information bases (MIBs) and return this data to the SNMP requesters.
Star topology	A LAN (local area network) that uses a star topology in which all nodes are connected to a central computer. The main advantages of a star network are that one malfunctioning node does not affect the rest of the network and that it is easy to add and remove nodes.
Switch	A device that filters and forwards packets between segments of a LAN (local area network). Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI reference model and therefore support any packet protocol.

TCP/IP (Transmission Control Protocol/Internet Protocol)	The suite of communications protocols used to connect hosts on the internet. TCP/IP uses several protocols, the two main ones being TCP and IP.
Token ring	A type of computer network in which all the computers are arranged (schematically) in a circle. A token, which is a special bit pattern, travels around the circle. To send a message, a computer catches the token, attaches a message to it, and then lets it continue to travel around the network.
Topology	The shape of a LAN (local area network) or other communications system. Topologies are either physical or logical.
User datagram protocol (UDP)	A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It is used primarily for broadcasting messages over a network.
WAN	A computer network that spans a relatively large geographical area. Typically, a wide area network (WAN) consists of two or more LANs (local area networks). Computers connected to a wide area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the internet.
Workstation	Any computer connected to a LAN (local area network).