Appendix E
Malawi College of Medicine

Malawi College of Medicine (MedCol) was opened in 1991 as part of the University of Malawi. The College is in Blantyre in the Southern Region of Malawi. Its main campus is located along Mahatma Gandhi road in the Mandala area with the Queen Elizabeth Central Hospital, where its clinical departments are situated, all within walking distance.

Currently the College has a student population of over 200 students, with students from Lesotho, Zimbabwe, Uganda and Nigeria.

1. Introduction

A wide area computer network was installed at Malawi College of Medicine (ColMed) in April 2002. The system suffered from the teething problems common to rapidly growing networks where Internet access has just been offered for the first time. Additional problems, such as massive virus attacks, resulted in the system becoming largely ineffective. Consequently, user confidence in the system was lost.

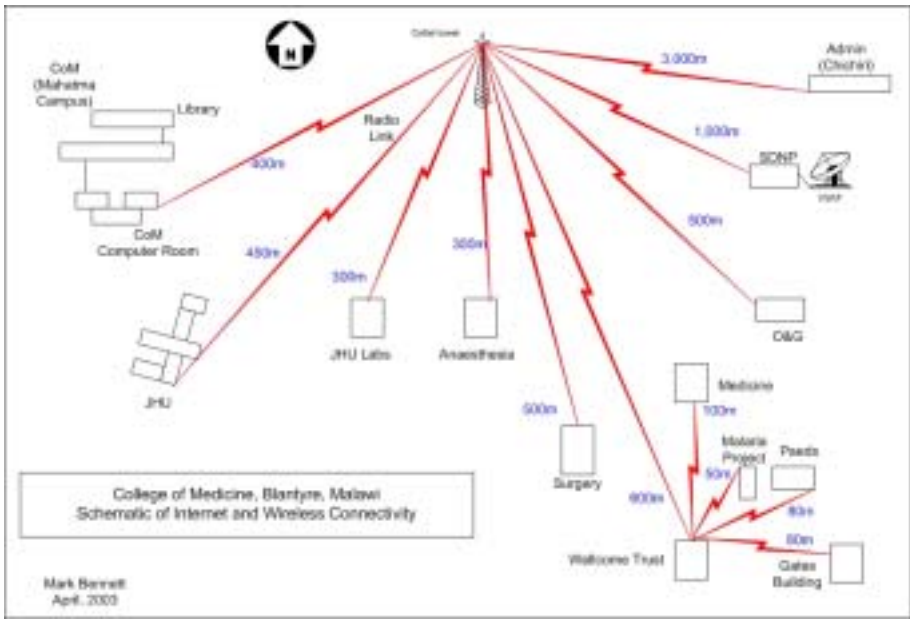
This case study looks at Colmed as representative of the problems common to newly installed networks.

2 The network

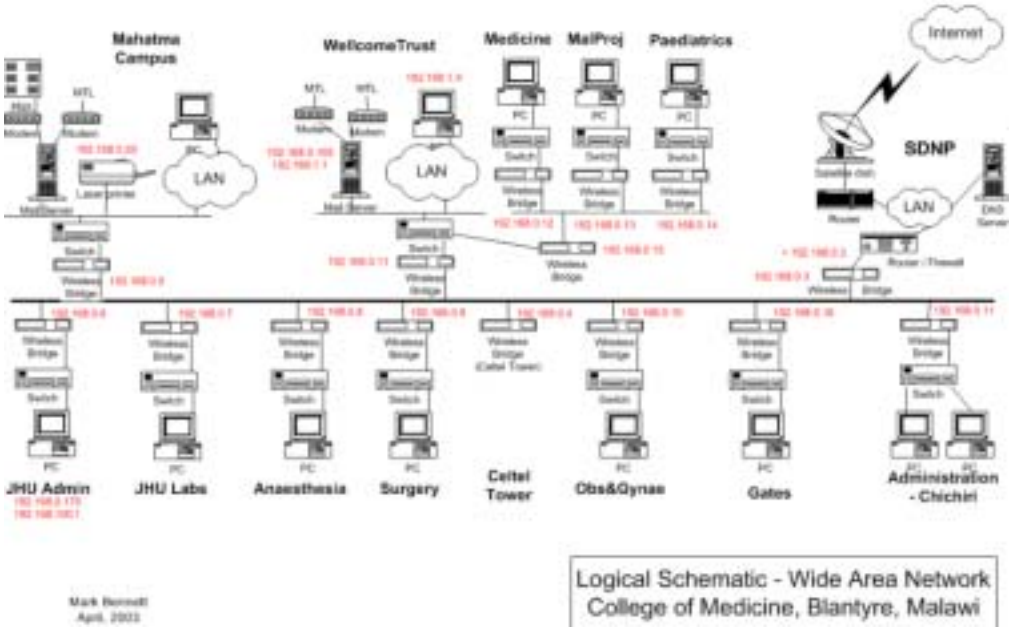
In April 2002 a wide area network was installed at the College of Medicine (Colmed) to provide various services, primary amongst which was Internet access. All departments at the College had been linked together with a wireless network. This network also had a wireless connection to the local ISP, which has a VSAT connection to the Internet backbone. Departments that did not already have a local area network also had one installed at this time. The wide area network (WAN) linked over 150 PCs at the Mahatma Campus and all 11 teaching departments around the Queen Elizabeth Central Hospital (OECH), the Wellcome Trust Labs and the Blantyre Malaria Project. Since then, the network continued to grow as more departments and more PCs were added. The Library now also forms part of the network and networked PCs currently numbers 250. All staff, students, administrators and researchers have access to the computers on the network.

International bandwidth to the Internet is 128 kbps.

The diagram below shows the wireless network.



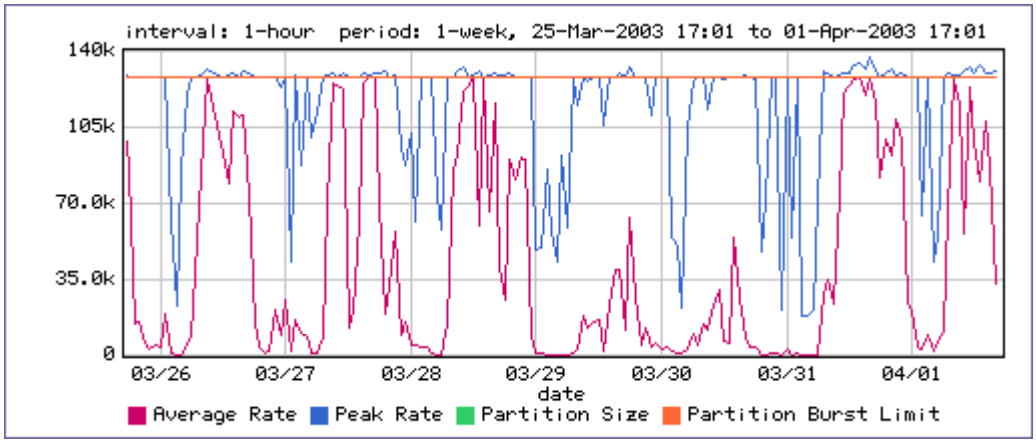
Internet connection is provided by SDNP (www.sdnp.org.mw) The server at SDNP belongs to the College and is named 'colmed'. The college website is also hosted at this server and is available at www.medcol.mw. Below is another representation of the network, showing the Internet connection at SDNP.



2.1. Problems

The problems that were experienced during the first year can be split into human and technical issues. Some of these problems have recently been addressed. Original problems included:

- International bandwidth to the College was completely congested. Bandwidth is set at 128 Kilobits per second (Kbps) and is provided all the way to the Internet backbone. This is hardly enough for the number of users, but was the amount that could originally be afforded. The bandwidth use was not being measured. Once monitoring was switched on it turned out that this 128k was fully used (and therefore saturated) during the entire working day and beyond.



- The wireless wide area network traffic was completely congested and the network needed splitting, as per its original design. It appeared that the wireless network could not cope with the degree of traffic that was being placed on a point-to-multipoint network, and many data packets were being thrown away (and therefore had to be retransmitted). At certain times of day up to 80% of packets between any two points were being lost. However, it appeared likely that the basic network infrastructure was sound as at certain other times of day, for example late in the evening, the system did appear to become fully effective.
- There was far too much unnecessary traffic on the wide area network that should not have been there, including low-level protocols (and routing, sharing, etc.).
- There was some incorrect routing on the network, which meant that traffic was not finding its way out quickly enough and too many packets were going freely around the network.
- There had been a significant increase in the number of users and in the kind of activity that they were undertaking.
- There had been massive virus attacks, and no anti-virus measures were in place to scan incoming e-mail messages. It had previously been assumed that all mail (which is the primary source of virus transmission) had been being scanned on the MS Exchange servers. However this turned out not to be the case and the only machines that were in any way protected were those that had Norton Anti-Virus corporate editions installed, which was only the more recent machines. It appeared that in particular the viruses OpaServ (which tries to spread by finding any machines which are sharing resources), Brasil and Klez were very widespread and they were consuming up to 80% of the international bandwidth by in turn trying to propagate outside the network back onto the Internet. They were also likely to be consuming a considerable amount of internal bandwidth on the WAN and were of course damaging various machines on the network onto which they were spreading.
- There was no control of web usage in place, and no content filtering to try and stop inappropriate material (e.g. games, music, pornography, etc.) being freely browsed. Precious bandwidth was thus being used on non-essential activities.
- IT support was highly reactive rather than proactive, and thus most time was spent by the IT team dealing with those calls that were being made to them (frequently by mobile phone) from users who had what they considered urgent issues with their PCs. Little time and thought was therefore being given to the major network problems that were occurring. The College only had one full time IT support person and one part-time IT support person. The Wellcome Trust's own IT Manager was spending most of his time dealing with work at the Trust itself.
- The IT support staff could not cope with the number of users within the College, particularly bearing in mind the widespread area that is covered by the College, Hospital and Administration.
- The IT support was not being monitored or controlled by any higher levels of management

and there were no particular reporting structures.

- There was no monitoring of network traffic or reviewing of the server logs or of the mail logs and no software was in place to deal with all of this. So when the network became slower the reasons for this were not obvious.
- The original plan to split the network and the wireless system into three had not yet been considered.
- No backups were being done on the Exchange server. At one time mail had been lost from this machine and there had been a hard disk crash. There was no way of restoring this data and thus user confidence in the entire mail system had been lost. Many users had therefore turned to using Yahoo even for internal mail, perhaps without realise how it operates. In turn web-based mailers use significant amounts of external bandwidth and therefore slow the network down.
- There is no equipment redundancy for the critical components at either the Mahatma Campus or SDNP. Likewise, all traffic is routed through links for which no redundancy is provided.
- A number of machines were really under specified for the tasks that were being asked of them.
- Users were becoming frustrated that certain facilities were not available. For example, they could not pick up their mail when they were away from the College, either at home or outside the country.
- No website had been created, nor a shared resource for internal material.
- No network monitoring tools were in place to see what kind of traffic was actually traversing the network at a low protocol level.
- It was not clear who with the College Management knew about the problems associated with the network.
- There was no dial-in service being provided for users who were working from home or around the rest of Malawi. (The original MTL line had been removed and no further ones installed).
- File sharing was not under control. There was no security on some of the machines that were found to be shared and it appeared to be possible to view the contents of certain computers and even files containing examination results on PCs where owners were not aware of the implication of the arrival of a network.
- The main servers at the Mahatma Campus were connected to UPS, but the Powerchute software was not installed. When there was a mains power failure, the machines would continue to run until the battery failed, instead of shutting down gracefully. Therefore they continued to be in danger of losing data.
- Data-fax was being used at the JHU Unit and this and other cases were found of potentially large files being transmitted overseas during the working day, thus blocking any other kinds of more normal traffic such as web page requests.
- The wireless network had been reconfigured in some cases without recalculating new link budgets.
- In their frustration with the slowness of the network users were regularly dialling into outside ISPs and therefore compromising the security of the network with the possibility of introducing new viruses and other sources of unprotected data.
- Anybody could link their computer onto the College network, there being no attempts to force authentication.
- There was no security on the wireless network, and although it was unlikely that it was being compromised it would have been possible for other people around the area to also join onto the network.
- There was a problem with the machine at SDNP, which is owned by the College of Medicine and which acts as a firewall. It was periodically crashing as it did not have

enough resources, including memory, and there was no information provided on traffic levels or bandwidth used and this machine was felt to be very vulnerable as a potential single point of failure.

- There has been no sub division of the Mahatma Campus from the main network and therefore a lot of traffic that should have stayed with the Mahatma Campus was finding its way onto the larger network.
- The student machines within the Mahatma Campus were obtaining their IP addresses automatically using DHCP and therefore it was not possible to distinguish their activity from that of other users or to tighten their particular usage options.
- There was no way of forcing anyone on the network to adhere to usage policies, nor any particular attempt made to do so.
- There was a very low hit rate on the ISA proxy caches at all 3 sites for a reason that had not been determined. Rates were as low as about 10% whereas they should have been at least 50% and therefore fetching pages from abroad was wasting a lot of international bandwidth when other users had already viewed them recently.
- There was also no pre-population of ISA caches to take advantage of the unused bandwidth that was available during the night.
- The default web pages opened by Internet explorer did not appear to have been well set and therefore pages were being downloaded which were never used.
- There was no backup domain controller in place to provided protection in times of failure of the main server.
- The IT department is understaffed.
- There are a number of critical single points of failure on the network with no back-up options in place. These include the Celtel tower and SDNP.

3. Servers and optimisation

3.1 Network

Upgrading of the Colmed server at SDNP (which acts as the firewall, and mail relay), in order to improve speed at the network entry point. This is because DansGuardian proved to be too resource intensive for this low powered machine.

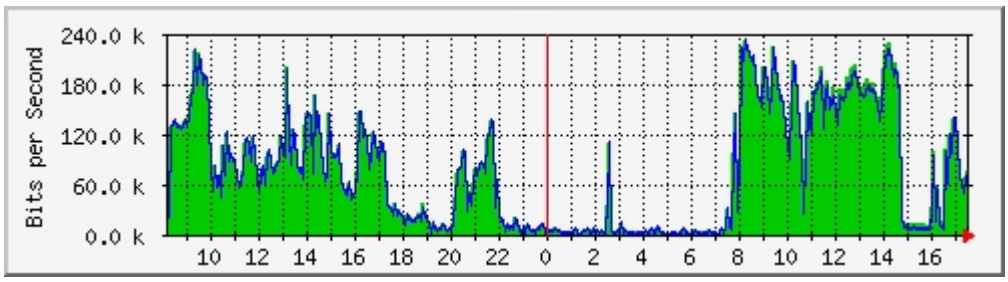
A second server has been ordered for the network perimeter, to split the functions of the firewall between a box that will look after web traffic and one that will look after e-mail. This will make it possible to run content filtering on a more powerful machine. The mail machine will also have the job of doing the virus scanning. If this is done on a dedicated mail machine, this resource intensive process will no longer slow down web traffic.

Routing changes at SDNP means data packets found their way more quickly to the Internet.

3.2 Monitoring

The logs from the Exchange mail server, the Squid proxy, DANSGuardian, and other sources are analysed with Sawmill software, which is available on several of the computers.

MRTG software, which is available free of charge, is installed on ‘colmed’ and is used to analyse the traffic passing to and from the router on the College network onto the Internet port at SDNP. See example below, which is now available at
https://www.medcol.mw/mrtg/medcol-router



MRTG is also going to be implemented to analyse the output of the traffic levels on most of the other wireless units, when they have been SNMP – enabled.

At SDNP data from Packet Shaper is also available to analyse traffic patterns, and protocol distribution.

3.3 Content filtering and control

Content filtering of all web traffic is done with DANSGuardian software on the colmed server with a one-year subscription to download its regularly updated blacklist at a cost of $60.

Any unsuitable or wasteful websites that are found to be used by students that are not on the existing regular blacklist list can be added to it manually so that they are duly blocked.

The amount of time for which students and anyone else should have access to web based mail should be limited. Likewise, recreational use of the Internet can be kept to non-working-day periods. (All of this is controllable within ISA or DansGuardian). If necessary, the graph of student usage and lists of the sites that they have visited can be posted on notice boards to indicate that the College is aware of the kind of activities that they are undertaking. It is better that all of these things are done electronically rather than by human intervention or by watching over people's shoulders, which is both human resource intensive and probably dissuades people from undertaking the kind of work that they actually should be doing (for their project based assignments on the Internet and access to journals and so forth).

3.4 Mail

The use of web-based mailers is being gradually phased out. There should be very few people who actually need to use web mail once confidence is restored in the main mail server with the 'medcol.mw' mail addresses.

Visiting scientists may be given special permission for using web mail.

If users from the College need to access their mail when abroad or outside Blantyre, they can do so over the web by using Outlook web access or POP mail in taking their mail directly off the servers at the Mahatma Campus or Wellcome Trust John Hopkins.

Mail will be scanned for viruses on the colmed server before being delivered to the Exchange server.

3.5 Ongoing efforts

A programme is already in place at the College to upgrade the operating system software and so that most computers run Windows 2000 or Windows XP. All the computers that are running Windows 95, 98 or ME will continue to pose a problem to network management and security.

Authentication from proxy servers will be put in place so that no computer can connect to the Internet without first having to offer a password. This will breach a number of the existing security gaps.

The wireless network will be split into three segments as originally designed but not implemented initially due to cost constraints.

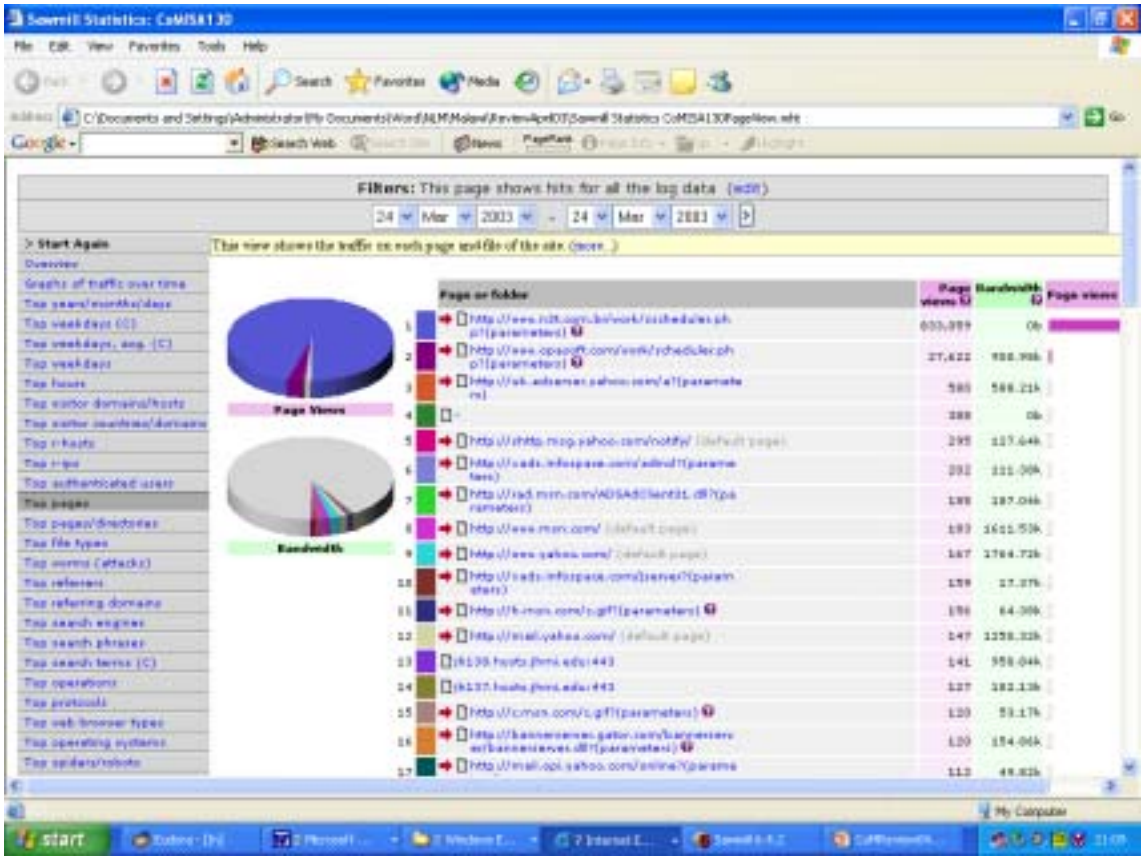
College authorities and individual heads of department will be informed of the monitoring tools now at their disposal, so that they will note what is being undertaken on the network – and particularly the link to the Internet:

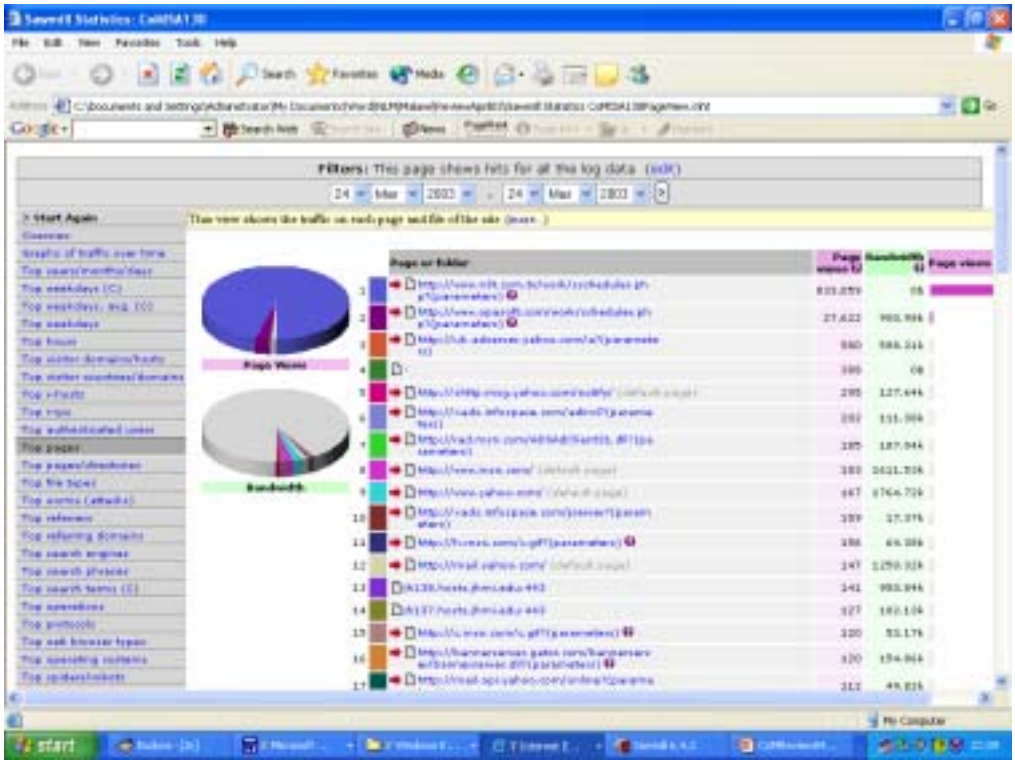
- Main websites browsed and bandwidth consumed etc
- Main e-mail users and volumes of mail

- Monitoring will not compromise personal privacy

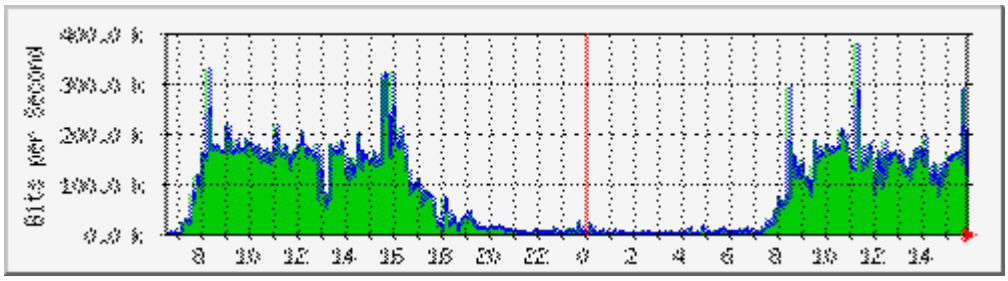
Certain times of day will be allowed for some activities such as reading web based email, which might then be blocked at other times.

Mail sizes can be set according to the amount of traffic that can be reasonably expected to be borne by the network and once the system is stable bandwidth can then be increased. See some sample screenshots below of the output of such usage analysis:

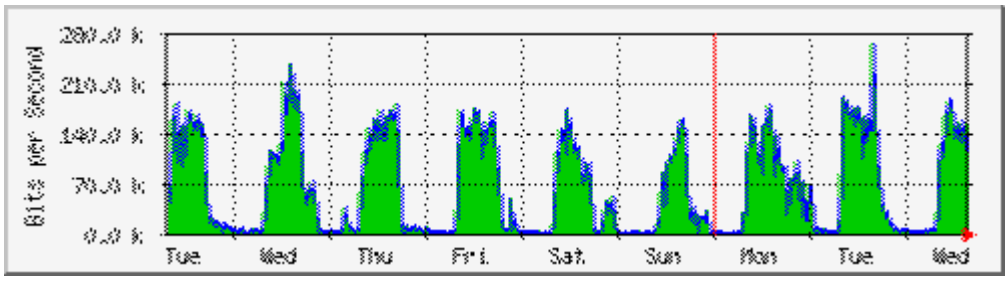




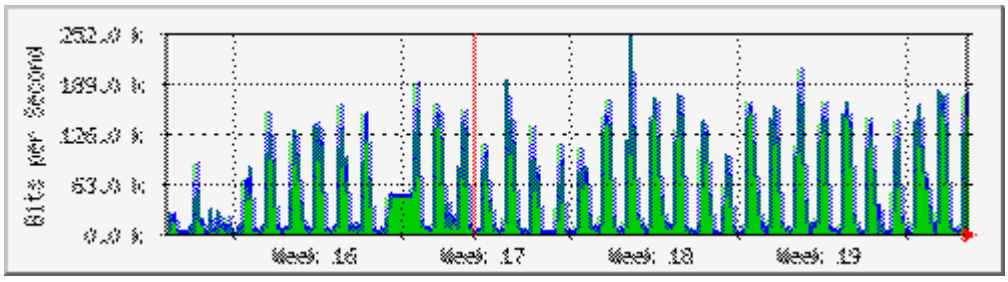
Likewise, the graphs from MRTG (see below) can be seen around the network in graphical format and the amount of traffic on each particular section can help to determine where congestion might occur in the future.



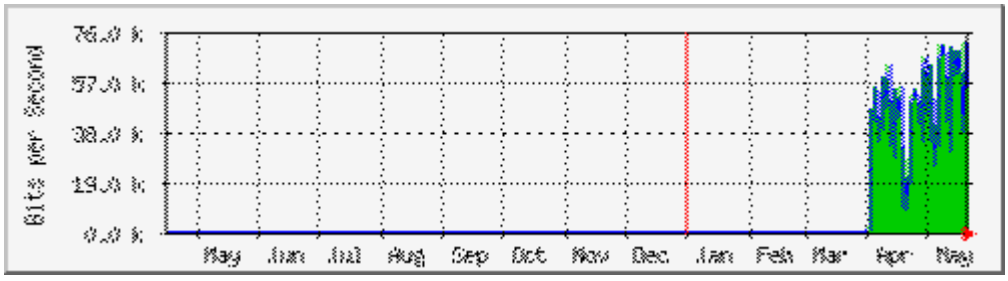
(`Daily' Graph (5 Minute Average))



`Weekly' Graph (30 Minute Average)



`Monthly' Graph (2 Hour Average)



`Yearly' Graph (1 Day Average)

Students will be separated out onto their own logical network in terms of addressing, although they will remain physically on the main network. The usage agreements will be strengthened and action taken if anybody is found to be violating them.

The non-IP traffic that is currently going around the network should be blocked from leaving any particular building at the bridge level.

This will significantly cut down the amount of traffic on the wide area network and also it is likely to reduce some of the security breaches that are occurring at the current time. Also non-essential IP traffic, such as NetBios requests, can be blocked at port level.

Although some security measures are already in place, work is in progress to improve security as a whole, both in the case of access and sharing of files on particular computers, and on the network as a whole at firewall and bridge levels.

Once all the issues mentioned above have been addressed, it should be possible to increase the external bandwidth purchased from SDNP in order to improve Internet speed. 128k is not sufficient for a user base which by then will include the Gates building and serve around 300 PCs

It is planned to increase the bandwidth to 256k into the College and 128k going out. Bandwidth can remain asymmetrical as far more web traffic will come in than other traffic that leaves the College.

It may also be possible to buy further bandwidth on a burst excess basis - that is by using bandwidth from the ISP that is not being used by other customers at any particular time and then losing when it is again used by those customers.

A proper management and reporting structure for the IT department will be instated, just as there are for other departments, complete with job descriptions, formal budgeting, resource allocation, reporting, project management, and so forth.

The above department then needs to plan for future growth. Its first task is to write an IT policy and strategy to cover the next 5 years and this needs to be adopted into the long-term vision of the College. The policy needs to cover the infrastructure aspects of IT, and, separately, the academic aspects.

A comprehensive IT training programme for staff (academic, research, administrative, support) will be designed and funding and resources sought. The College has a major new resource, which is likely to remain under-utilised until everyone is brought up to a common level awareness of what is available and how it can be most beneficially used for both teaching and administration. Once staff levels have been raised appropriately, assistance can be sought to revise both the curriculum and the approaches to teaching to make use of the new technology and of the enormous resources available via the Internet, including access to staff elsewhere who could continue to be part of the mentoring and teaching process.

4. Charging

A system for charging is being considered to generate revenue, which could be used to either assist with staff salaries or to provide more material for the IT unit.

5. Security

The RAV Anti-Virus programme was installed on the ‘colmed’ server and scans all incoming and outgoing mail from the College. The $400 cost incurred with the installation of this program compares very favourably with the Norton corporate products on the three servers, which would have cost up to $1100 per machine.

6. Conclusion

A major new resource such as Internet connectivity requires appropriate support in both human, funding, and infrastructure terms. The speed with which the system arrived; the lack of sufficient and trained staff on the ground; coupled with the fact that the technology was not one with which most of the College Management were familiar, led to significant problems, and the network became apparently out of control. In turn this lead to a lack of confidence.

This by no means an uncommon experience for organisations and companies. The Internet is the fastest growing technology in history – its usage increase is exponential – and whereas in

some contexts the problem can be solved by throwing in more money and bandwidth this is not appropriate to the College, which has other high priority calls on its very limited funding.

The IT audit carried out, and the work done subsequently, has shown that the problems experienced can readily be brought back under control given an appropriate level of resources.

The most important conclusion, therefore, is to properly institutionalise the functions associated with the network. The IT unit must form a key part of the College management infrastructure, just as (for example) the library does. It will become a wholly critical resource without which the College cannot operate effectively. This therefore needs to be taken into account in terms of its management and funding.