Appendix D
Makerere University

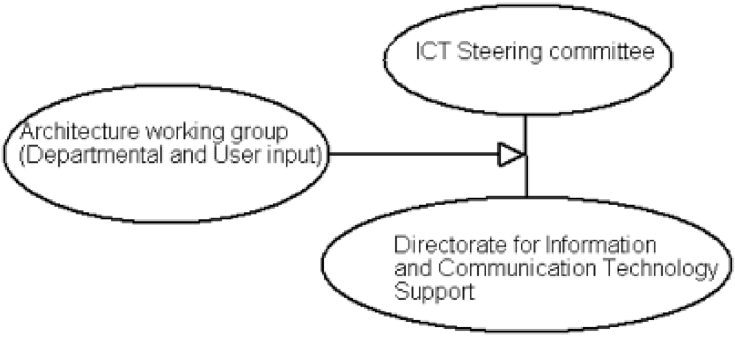
Makerere University had its humble beginning in 1922 as a technical school with 14 students. Today, Makerere University offers day and evening classes to 22000 undergraduates and 3000 postgraduate students.

It is located on Makerere hill, 5km to the north of Kampala city centre in Uganda.

1. Introduction

Makerere University has about 22,000 undergraduates and 3,000 postgraduates. The Makerere University Network is referred to as MAKNET, and is implemented and supported by the Directorate for Information and Communication Technology Support (DICTS), which is also responsible for IT related projects.

DICTS, in turn, is part of, and reports to the ICT Implementation Committee (ICTIC) -which will be renamed to the ICT Steering Committee (ICTSC). This Committee takes high level and budgetary decisions about the direction of ICT aims and projects. The Director of DICTS is the secretary to this committee. There is also the Architecture Working Group (AWG), which is composed of representatives from all faculty level academic units as well as administrative units. The aim is to “provide a forum for the development and continuous review of the University's information architecture, ensuring that it conforms to the common vision of the end users”.


ICT Steering committee
Architecture working group (Departmental and User input)
Directorate for Information and Communication Technology Support

Departments that wish to implement ICT related projects or advice, might get some of these done by an external company, “only if cost-effective and if the expertise involved is not (yet) available in the University and will (cannot) not be developed by DICTS”. However, DICTS as a unit is competitive in this respect, because it is a not-for-profit unit of the University.

In order to prevent a situation where a low-status ICT manager (low-status in reporting level and/or compensation) “has difficulty getting the necessary information from general management level in the strategic planning process and aligning ICT policies with the vision of general management and general strategies”, the director of DICTS is be placed “at a hierarchical level at least equal to that of the Librarian or Director Planning Department, hence he/she will report to the Vice Chancellor”.

The functions of DICTS are stated to be:

> a central service unit that provides expert services and guidance to all academic and administrative units of the university. With the competent staff DICTS is able to offer excellent service to the user units.

In addition to being part of the University community, DICTS aims at cost recovery rather than profit. This implies that our charges are a lot more favourable than those of competent commercial firms around town.

DICTS provides Internet connection, networking and web design services to the local community. DICTS has the following departments:
Helpdesk
Network administration
Network management unit
Email system

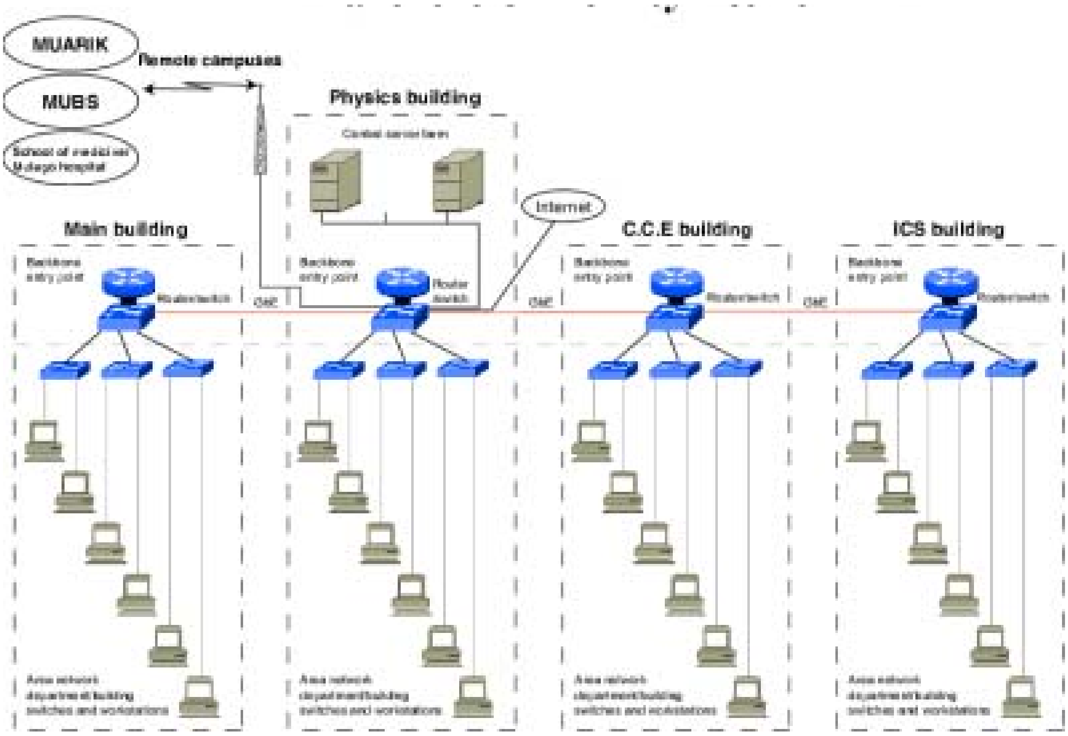
The progress and planning of the various DICTS projects since 2000 and extending to 2004 can be viewed at http://www.makerere.ac.ug/makict/progress/index.htm

2. The Network

The university has two connections to the Internet. The connection via MTN Uganda is 512 Kbps downlink, and 256 Kbps uplink. The main campus link is 1 Mbps via Uganda Telecom (with a 512 Kbps uplink). These two links carry about 144GB per month, as measured by the bandwidth manager.

There is a fibre optic backbone that connects the physics building, the CCE and ICS buildings on the main campus. As can be seen in the diagram below, there are onward radio links to the School of Medicine at the Mulago hospital, as well as to the MUARIK (Makerere University Agricultural Research Institute, Kabanyolo Network) and MUBS (Makerere University Business School Network) campuses.

With a high speed, buried fibre-optic cable backbone there is no need of placing the servers close to the users. Therefore, most servers (Mail, Web, Administrative, Library, etc) are kept in one room (currently in the Physics building, but planned to move to the new ICS building) where they benefit from cooling, air-filtering, UPS, backup-facilities and physical protection.



3. Optimisation

3.1 Proxying

There are two proxy servers, one for each Internet link. The diagram attached shows their location in the backbone. A bandwidth manager sits between the proxy servers and the layer 3 switch at Physics. This is layout is designed so that traffic from both cache servers can be shaped by the bandwidth manager before being delivered to faculties. The cache servers do not peer (share cached documents) at the moment.

They are both Pentium 4 machines with 128 memory. Since they serve a very large network, this small amount of memory is found to be a serious bottleneck, and more has been ordered. (Apart from the memory required for the operating system and other applications, Squid requires 10 MB of RAM for every 1 GB of cache).

Every web connection is forced to pass through the cache servers by employing transparent proxying, using Squid. The advantages are that transparent proxying frees the network team from setting up individual browsers to work with proxies. This is very useful in a large network.

Using transparent proxying, you intercept their web requests and redirect them through the proxy, which is why this method is also sometimes referred to “TCP hijacking”.

Filtering of pornographic sites is done not by content inspection but rather by blocking known pornographic sites. This is done by using url_regex in Squid. In the squid.conf file, the section below does the filtering.

```
#BLOCKING PORN SITES
acl porn url_regex "/usr/local/squid/etc/porn1"
http_access deny porn all
```

This file (porn1) contains a list of porn sites and is upgraded regularly. It can be downloaded from http://members.lycos.co.uk/njadmin

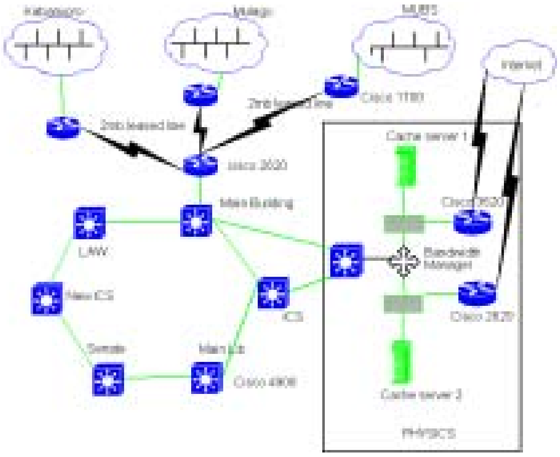
3.2 Limiting P2P sharing

Makerere only allow TCP connections that originate from their network. In this way the amount of bandwidth used by peer to peer programs like Kazaa is halved. This is done using extended access-lists at the gateway routers, with the "established" keyword

3.3 Ensuring that the proxy is not bypassed

Transparent proxying can work in two distinct ways as described in the Squid documentation (see www.squid-cache.org/Doc/FAQ/FAQ-17.htm). The first way is if the Squid proxy is “already in the path of the packets (i.e. it is routing between your proxy users and the Internet)”, for example if Squid is installed on a Linux firewall machine (running iptables), or on a UNIX-based router.

The second possibility is to rely on a Cisco router using its "route maps" feature, or equivalent features on layer-4 switches from other vendors. Makerere university opted for the second approach, and rely on CISCO routers to do policy routing at the gateway router to redirect all



web traffic to the Squid server, as indicated in the diagram. This layout has the advantage that if the proxy server fails the network administrator can remove the policy routes and connection to the Internet resumes without proxying.

3.4 Cisco configuration

The Cisco configuration that directs web request to the proxy server work with an extended access-list which is set like this:

```
access-list 110 deny tcp host 192.168.1.2 any eq www
access-list 110 permit tcp 192.168.1.0 0.0.0.255 any eq www
```

Where 192.168.1.2 is the IP address of the Squid box, and 192.168.1.0/24 is the network address space for the network. This matches web traffic for all hosts. The policy routes look like this:

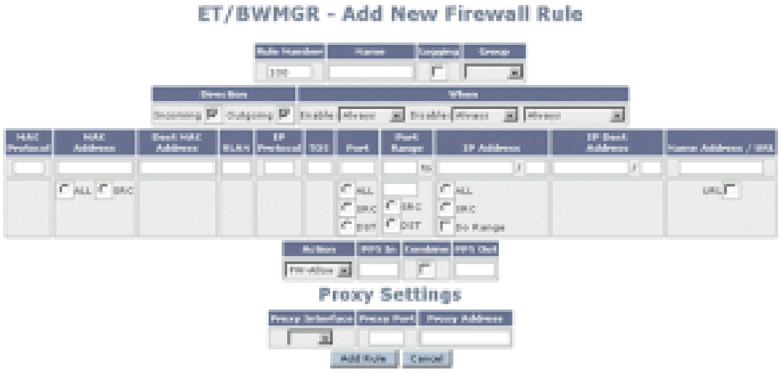
```
route-map cache-map permit 10
match ip address 110
set ip next-hop 192.168.1.2
```

The above routes all traffic matched by access-list 110 and sends them to 192.168.1.2. Finally, the policy route is applied to an interface, in this case the ethernet port where the traffic arrives first:

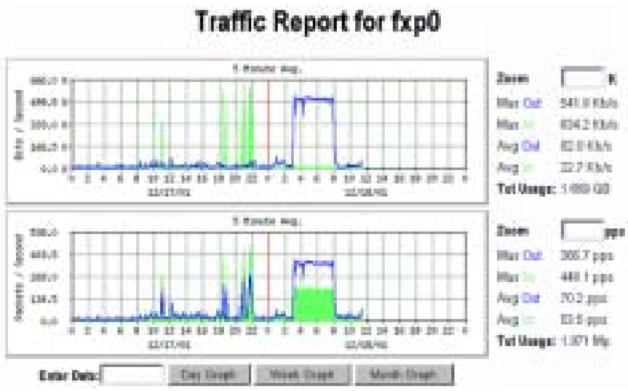
```
interface FastEthernet0
 ip address 192.168.1.1 255.255.255.0
 no ip directed-broadcast
 ip policy route-map cache-map
```

3.5 Bandwidth Management

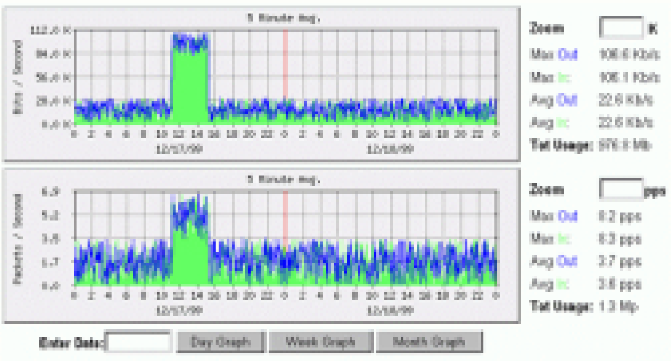
There is an ET/BWMGR Bandwidth Manager from Emerging Technologies (see www.etinc.com) near the edge of the network. It is available as a standalone appliance which plugs into your existing network, or as a software add-on for Linux or FreeBSD operating systems. It has a web based control interface. It connects to networks using 5 network interfaces. The administrator can create independent bridge groups, which enable the administrator to manage bandwidth from two ISPs. The box works like a switch, and when 2 Ethernet ports are grouped together, they are not aware of the remaining 3 ports and vice versa. In the case of Makerere University, the BWMGR is like 2 switches, one for each ISP link. The device is very good at managing bandwidth, protocols, priorities and providing statistics. Some screenshots follow.



ET/BWMGR - Add New Firewall Rule



Traffic Report for fxp0



Zoom □ K
Max Out 106.6 Kb/s
Max In 106.1 Kb/s
Avg Out 22.6 Kb/s
Avg In 22.6 Kb/s
Tot Usage: 976.8 Mb

Zoom □ pps
Max Out 8.2 pps
Max In 8.3 pps
Avg Out 3.7 pps
Avg In 3.8 pps
Tot Usage: 1.3 Mp

Enter Date: □

The bandwidth manager has many features such as a web based management interface, bi-directional bandwidth limiting and allocation, integrated firewall and its own monitoring and reporting. The bandwidth manager can also be used for p2p Traffic Control (KaZaA, Morpheus, etc)

3.6 Mail system

The university uses Postfix with Amavis virus scanner. Every incoming mail is passed on to Amavis before it is delivered to the final mailbox. Amavis relies on Sophos anti-virus for detecting infected mail. Infected mail is quarantined and both recipient and sender are informed.

Postfix uses a MySql database to lookup e-mail ids. This was chosen to avoid having Unix system users as e-mail users. This makes it harder for hackers to guess system users passwords. It also makes it easy for administrators to write user administration interfaces using PHP. Instructions on how Postfix was set up with MySql support can be found at http://kummefryser.dk/HOWTO In future the University plans to switch to LDAP.

Since Makerere have their own web mail system, the use of other web mail sites like Yahoo and Hotmail is limited to after 1700 hrs and before 0900 hrs during week-days. All this is done using squid web cache and proxy. Sqwebmail (www.inter7.com/sqwebmail.html) is used for the web mail services. This is a CGI program that picks mail off users mail directories. The use of mailboxes is avoided to limit user woes due to mailbox locking. Sqwebmail was found to be fast since no TCP protocols (POP, IMAP) are needed to collect mail.

External web mail is blocked the same way as other unwanted sites. The difference that it is only blocked between 900hrs and 1700hrs.

The part of the squid.conf file that does this follows. The file /usr/local/squid/etc/webmail contains a list of web based mail URLs

```
acl LOUSY_SITES url_regex "/usr/local/squid/etc/webmail"
acl COME_BACK_LATER time M T W H F 09:00-17:00
http_access deny LOUSY_SITES COME_BACK_LATER all
```

Notice that the access lists are placed next to each other to ensure and AND kind of logic.

3.7 Ongoing efforts

- Deploying a web-based download scheduler whereby users can schedule their downloads to occur at night when our links are free. This system will also cache downloaded files for other users to get locally.
- Installing a protocol analyser in order to ascertain what percentage of our bandwidth is used by HTTP, Mail, FTP and other protocols in order to deploy traffic prioritisation. The product that is being installed is Cflow (http://www.caida.org/tools/measurement/cflowd)
- Installing a log analyser so that we can tell which sites are visited frequently, in order to allocate more bandwidth to those destinations.

4. Make or buy policy

Makerere University has an interesting policy on the "make or buy" question, when it comes to implementing new services or systems:

Key factors that favour the make decision include the following:

- A customized ICT application or service that is totally responsive to the institution's very specific needs.
- Increased ease in developing software due to the growth of Rapid Application Development tools and systems.
- Ease of adapting software to rapidly changing user needs without having to co-ordinate the requirements with vendors.
- Developing professional competence in software development.

Key factors that favour the buy decision include the following:

- Ability to gain access to specialized skills that cannot be retained or for which there is insufficient need to have continuously available.
- Cost. Building software is still extremely costly.
- Staff utilization.
- Ability to make short-term commitment for ICT development support instead of having to make major investment in staff recruitment and professional training.

5. Security

- The network is built with switches “since this nearly eliminates the possibility for users of "snooping" accounts and passwords from the net”.
- All links to between switches (except the radio links) is optical fibre.
- Encrypted communication methods (like SSH instead of telnet, HTTPS,.....) will be used by all university critical systems (e.g. financial, student databases and so on).
- Authentication is required to access all systems.

6. Library Information System (MakLIBIS)

The aim of the MakLIBIS project is to implement an integrated on-line Library Information System. This includes:

- A Circulation Control System.
- A Catalogue Maintenance System.
- On-line Catalogue Access.
- The ability to sharing resources (catalogues) among libraries at different locations.
- Acquisitions Control, including search of on-line sources of publications, on-line access to book dealers and book publishers and order placement, checking in, query on-order records.
- Serials Ordering and Control.
- On-line access from any workplace to Reference and Information Services (indexes, abstract, etc) in the University library and other universities and institutes.
- Statistical reporting and management information provision.

6.1 Implementation issues

This project is still in an early phase, and involves much effort costs in converting current paper files into computer files.

More information about this project is available at
http://www.makerere.ac.ug/makict/documents/policydoc/annex1/maklibis.htm

7. Other notable ICT projects

Faculty of Social Sciences Black board e-learning centre.
See http://ccd.ss.mak.ac.ug

Collaboration Programme
University of Bergen and Makerere University. See http://www.uib.no/makerere-uib/englishversion.htm

Uganda Development Gateway.
Led by DICTS, the Uganda Development Gateway (UDG) "will be an Internet portal for information on sustainable development and poverty reduction - offering a common space for dialogue and exchange of experience, knowledge, ideas, tools, information, data and other resources. It will have a powerful search engine that will help users navigate through the ocean of development information available locally and on the Internet to find useful information and resources about development".

It aims to enable "Ugandans and other people in the development field to exchange ideas and build knowledge-sharing communities, the UDG aims to harness the use of advanced technologies in support of sustainable development and poverty reduction."
The gateway is at http://www.udg.or.ug

Academic records information system (ARIS)

Financial management and information system (FINIS)

Human resource information system (HURIS)

8. Connecting to MAKNET

In addition to the fair use policy, DICTS also has a short set of guidelines / requirements for departments / faculties to join the network. These guidelines ensure that the head of the department takes responsibility of the network in his department, and the network is not just something that is installed by DICTS and left there without ownership.

Case study contact

Joseph Kimaili
Network Administrator
Email: joe@dicts.mak.ac.ug
Tel: 256 77 594029