





# Information Systems Delivery in a Tiered Security Environment

Anne Strachan, Tony Shaw, and Donna Adams

Network & Information Systems Management, University of Paisley

## 1 Introduction/Environment

The University of Paisley, located in the South-West of Scotland, operates across several campuses at dispersed geographical locations (Figure 1). The University was originally located only on one site at Paisley, but due to mergers etc. has now expanded to another site in Paisley itself, to Ayr, and more recently, to Dumfries as part of a joint project with Glasgow University. It has undergone rapid changes not only to its student population and the structures of the courses it offers, but also to its organisational structures, particularly on the academic side. This rapidly changing environment continues to make demands for appropriate information services.






A prime example of how changes are evolving is demonstrated by the way in which the University manages its portfolio of modules. A module is a basic taught unit that can be studied individually or can constitute an element of a named course which full-time students normally pursue. The management of this information has changed from being a central management function to one in which responsibility is devolved to the individual academic divisions, a corollary of which is the acknowledgement of different individual rights in maintaining the information content.

These changes have occurred concurrently with a rapid expansion in part-time students as the University has focused on being a major provider of education for wider access. In fact, Paisley is the leading institution in Scotland which is committed to wider access with recent funding allocation reflecting this commitment.

### 1.1 Network and Information System Resources

#### Network and Information Systems Management

Network and Information Systems Management (NISM) is a technical support department of the University of Paisley and is responsible for both Information Technology and Information Systems strategy. This includes overseeing both network operations and network planning and undertaking information systems design, development and support. It also plays a key role in IT services development which includes network development and information services development whilst ensuring appropriate security. The department comprises approximately 33 staff consisting of 1 director, 9 application developers, 8 systems and network staff, 10 frontline support staff, 3 administration staff and 2 procurement staff. There is a total of 1100 staff in the University.



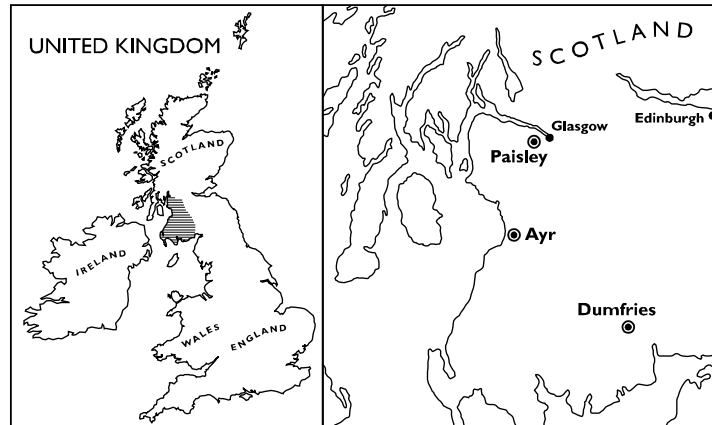


Figure 1: Location of Paisley campus

At an operational level, NISM staff are responsible for managing most of the network services including Netware application servers, a number of Unix servers used by University Administration, Unix servers that form part of the Campus-wide information service and non-departmental (i.e. not owned by specific academic departments) World Wide Web servers. This responsibility involves the routine administration of a range of Netware and Unix servers as well as the management of the University staff e-mail system. In general, NISM has no responsibility for operational aspects of student services, particularly with respect to teaching and learning, but does provide technical advice to staff working in this area.

The University's main business systems are also the responsibility of the department. These include the Admissions and Enrolment systems, all the Examination systems and other support systems that enable changes and additional information to be recorded about students. Changes to current student information is maintained separately as transactional data, and is periodically distributed as a service to satellite systems to enable them to update their local records. These satellite systems are the responsibility of the departments that developed them.

### Network Overview

1. The University's central network and systems consists of a category 5 cabled network within buildings. Four pairs of fibres run from each building to a central computer room via building switches or hubs to the central switch. The switches provide ATM connection and the hubs 10Mbytes connection to each virtual LAN. There are approximately 3000 connected data points.
2. The core central network is managed by a combination of in-house management and selective outsourcing of various aspects of the service.

### Systems Overview

1. There are approximately 39 central systems. These consist of a mix of NT, Unix and Netware server running core application and print services to staff, central network services, such as firewall, domain name service and mail systems, and student record information systems. All internal systems are managed in-house with external consultants being involved where necessary as a mechanism to enable change and provide skills transfer.

## 2 Paper Outline

As the network has developed with an increasing demand and need for access to appropriate information and/or use of information systems, the approach to delivering information systems has used a framework model in order to focus on requirements. In considering this approach, the paper examines:

- The development of an Information Systems model and the subsequent technical model for the network infrastructure.
- The benefits that have resulted from these framework models.
- The evolution of an example application in conjunction with the development of the framework models.

## 3 Information Services Model

The design of the network was influenced by several factors. Although some factors are not relevant to the current discussion, an important one was the realisation there were different categories of user with widely differing requirements, not least of which were differing security constraints. Consequently, an Information Systems model was developed initially describing the proposed services from a user perspective. This influenced the subsequent development of the technical model.

The relationship between the sets of services is shown in Figure 4. Clearly staff potentially have access to a wider range of services than either students or the public. Note the initial classification of staff does not distinguish between academic and other staff, although there will be differences in terms of service requirements at a local level.

This model is intended to encompass virtually all foreseeable requirements but does not include some occasional specialist facilities. It is assumed that the establishment of any specialist facilities will be a very closely controlled process including authorisation of the connection of items to the network and appropriate security controls. This represents a significant change from previous practice where there has been very limited control over the connection of users (both internal and external to the University) to the network.

## 4 Tiered Network Structure

NISM were initially responsible for the original administration network, although other separate networks existed at the Paisley site. However, in 1996, NISM took over responsibility for the entire network, although at that time the campus network comprised a disjoint

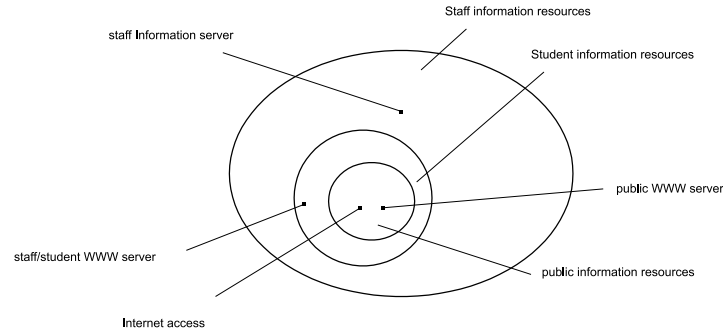


Figure 4: Information access for different user groups

collection of single networks and a single Wide Area Network (WAN) linking Paisley and Ayr. At the start, much effort was put into designing an appropriate technical model for the network infrastructure and services, whilst taking into consideration emerging requirements especially with respect to Teaching and Learning and remote access. In addition, issues relating to security and associated network management had also to be considered. The result was a hierarchy of separate networks being established in 1997.

Figure 2 illustrates the principle of the technical model, the main characteristics of which are:

- It is hierarchical with the ability for users on one network to access directly devices on any other network lower down the hierarchy.
- All networks are monitored and controlled to an appropriate level.
- Server resources can be located as appropriate to the user category that they service.
- There is a public network to meet the requirement of increased availability to Internet resources without unreasonable overheads on user administration activities.

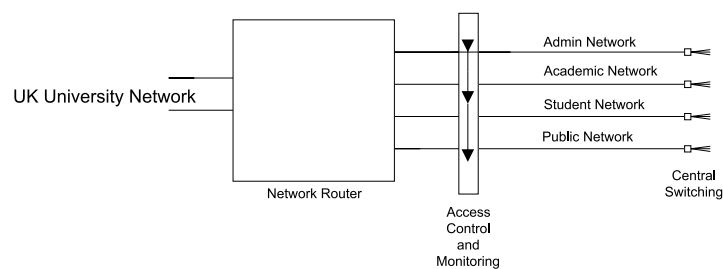


Figure 2: Network infrastructure technical model

At the outset the desire was to move towards a more structured information services environment where basic good practice in the areas of security, standards and service provision could exist. This resulted in different networks being identified for administration,

academic and student users, and also the public. The public network would be the home for resources such as the public web server. The resultant tiered security environment has subsequently directed the deployment of information services at both LAN and WAN sites. Figure 3 illustrates how various services relate to different user groups.

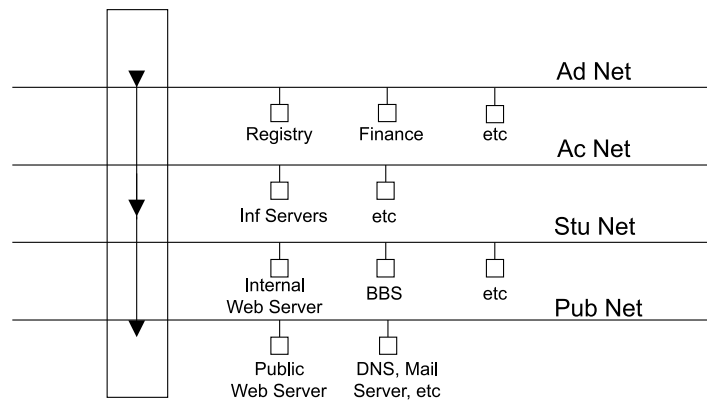


Figure 3: Service distribution in relation to the model

Development of a managed WAN, which had to support the four-tier network model including traffic prioritization, took place in late 1997, in conjunction with the establishment of a commercial firewall for protection of the network. Concurrent with these technical developments was the development of a University security policy. This ensured that access issues were carefully considered and that the different requirements relating to the four networks (and any subsets of these) could be incorporated into the policy.

In planning the WAN, attention focused on what type of service was required at the various locations and which ones justified being connected to the WAN. So, for example, the needs of others including student residences would be met through remote access.

#### 4.1 Tiered Network Benefits

There have been various benefits resulting from the network model including the following:

- The way in which it has been relatively straightforward to configure the network firewall in line with the different networks/user classifications.
- The extent to which the model has served to help structure discussions on planning and expenditure. At a time when financial resources are limited the model has made it easier to balance the technical planning and expenditure requirements associated with the different network/user classification.
- The framework has also enabled the needs of the many to take precedence over the wants of the few. That is, the model has helped ensure that emphasis has been placed

on identifying the key requirements of each of the user categories rather than be dominated and distracted by, for example, individual departmental perspectives.

## 5 Example Application

The selected application example facilitates the maintenance of the definitive description of each module called a Module Descriptor. At the start, the original 'system' was paper-based with documents being sent from academic departments to Registry and held there as the definitive source. All updates were handled in the same way. In 1995 this was followed by a freestanding computer-based system based in Registry whose purpose was to act as a primary information collection mechanism. This system comprised a Module Administration application and a Data Entry application which allowed data from amended paper-based Module Descriptors to be entered. All new Module Descriptors and amendments to existing ones were handled centrally by Registry staff in this way. 1995 marked the beginning of various computer-based applications to tackle this issue.

Subsequently, the overall system provided for version control such that two versions of a module were allowed to exist at one time. This was handled by using two databases, one termed the Planning database, the other the Live database. The current version of a Module was held in the Live database and the new version was held in the Planning database. Information in the Planning database was transferred to the Live database at a predetermined time dictated by Registry. However, due to staff resources and volume of work due to the proliferation of modules, the task became unmanageable. This situation was exacerbated as awareness of the deficiencies of the module descriptor database content became more apparent when the application allowing Module details to be viewed became available in 1996. This awareness increased with the availability of updated browser facilities via the student intranet in September 1997. It should be noted that the process for managing the modules was handled by manual procedures under the control of Registry.

The initial applications were operated centrally under the control of one department. Despite the original requirement which had been for a central operation, no secondary mechanism having been specified, this was really the only effective way of implementing the system at the time. Security was achieved simply by locating the application within the department and relevant staff had access to the entire collection of modules. However, with the development of the network, a facility to search for and view the module information was relatively easy to provide, the main consideration being the location of the database with respect to the tiered network. The original database and application remained accessible for editing purposes by the one department. A copy of the database was located on an appropriate server accessible by both staff and students to allow read-only access. No other security provisions were needed as the view facility was read only and the database was not the original on which editing took place.

As a result of various pressures, the situation was reassessed, which also coincided with some requirements changes. In reviewing the purpose of the application, the principle established when developing the Information Systems model was applied. That is, users were classified to focus on the applications required and help prioritize the work. In this way five groups of users were identified, each requiring to access the data in some way.

Three user types needed to be given explicit permission and access to carry out necessary functions. Figure 5 indicates in general terms which database each group would want access to and what they would want to do. The specific details were further elaborated during the development process.

User Class	Database Access	Functions Required
Modules Database Administrator	Planning	Administration Data entry/edit Information retrieval/viewing
	Active	Administration Data entry/edit Information retrieval/viewing
Registry Staff	Planning	Data entry/edit Information retrieval/viewing
	Active	Information retrieval/viewing
Learning & Teaching Custodians	Planning	Data entry/edit Information retrieval/viewing
	Active	Information retrieval/viewing
Other Academic Staff	Planning	Information retrieval/viewing
	Active	Information retrieval/viewing
Students	Active	Information retrieval/viewing

Figure 5: Resulting user classification

It was acknowledged the task of maintaining the module information was too great for Registry alone and the decision was taken to allow authorized users to be able to change that information for which they are responsible. This raised issues of delivery and security on the data editing application which hitherto had not needed to be addressed. A web-based application delivered over the intranet was deemed the best way forward, with the modules database suitably located on the staff network, which is accessible by administrative users. All staff have a network login identifier. Novell Netware uses the Lightweight Directory Access Protocol (LDAP) mechanism for authenticating users and this mechanism was employed by the application to verify users. Once in the application, a secondary mechanism was needed to ensure that only those users who had the authority to edit specific modules could do so.

Currently, further changes are in progress, partly as a result of recommendations from the Quality Assurance Agency and partly as a result of streamlining procedures in response to the academic restructuring that has taken place. The net effect is that the existing database will have to be restructured and the applications rewritten. However, by developing a

model of user classification it will be much easier to get the user groups to focus on their needs and to be able to prioritize the applications.

## 6 Conclusions from the Evolution of the Application

### 6.1 Factors Promoting Change

Over time, there have been various factors which have emerged to promote change. These are summarized as follows:

- A centrally managed operation was unable to cope with the amount of work that resulted.
- The academic community wanted access to reliable current information.
- There was a need for better and more reliable information for students.
- Within the University there was an apparent need for change in working practice.
- The network developments provided a means to devolve operations securely.
- There was a need for a more efficient and effective information management process.

### 6.2 Issues

- Conceptually, the data concerned is relatively simple. However, the organizational process is complex and generally not well understood. It is further complicated by organizational restructuring provoking a need to rethink the process.
- User classification was a difficult concept to promote, and still can be. Many academics regard it as a right to have access to any and all information the University may have.
- One overarching application versus multiple applications. Allied to user classification, this is another difficult concept for some users who find it hard to understand that multiple applications, relating to different types of users, can run against the same underlying database. This led to a misconception that classification was a mechanism to be used to prevent users from having any access, rather than to provide the required access.
- Deployment of a service whilst maintaining security and appropriate access does require more careful thought, a necessary requirement when addressing sensitive data.
- Who the person is to drive a project forward and be responsible for the project management process, including resourcing.

### 6.3 Benefits

- Removal of the workload and responsibility for maintaining Module Descriptors from the Registry staff, although they still have full access.
- Devolving responsibility from a central administrative department has empowered academic staff to take ownership of their Module Descriptors with the attendant responsibility to maintain their currency.
- The information management process is more efficient and effective.
- From an application development perspective, there may be opportunities for the re-use of application components across the various user groups.
- Staff and students have more confidence in the University's module information.





## 7 Concluding Remarks

Security issues and attendant data protection matters are of paramount concern to IT staff, but not to most users. One of the difficulties in pursuing any project is in getting the users to appreciate there are security issues here that affect projects.

Other, less complex applications have been delivered by the intranet, and the framework model of user classification has been a useful one to employ. For example, a classification of Course Administrator was identified and a suite of applications developed to support this role. This was carried out in consultation with a small group of course administrators. Access to the application was restricted to this small group of users only. The LDAP mechanism of authentication is used in all cases where applications deal with personal data. Authorization to use a particular application is controlled by an access table. There may be further controls within an application, such as that within the module editor which restricts users to their own set of modules.

