Implementation of a multi-site, wireless network at Northumbria University

Dave Warley BSc(Hons) MIEE, Project Manager, IT Services, Northumbria University

Contents

Abstract

Northumbria University has recently implemented a wireless network infrastructure combining Cisco® hardware with the Citrix MetaFrame® presentation server software. This combination of technologies has allowed some of the major concerns relating to wireless networks to be addressed in a highly cost effective manner, avoiding the need for specialised gateway servers and eliminating the need to rely on Wireless Encryption Protocol (WEP) as a security mechanism. As the University is already familiar with both Cisco® and Citrix® we were able to carry out the surveying, installation and configuration using our own staff, resulting in further

cost savings.

The network covers two campuses in more than ten separate buildings. Nearly 70 access points were deployed, in conjunction with a central system management facility. The network supports several open access hotspots, teaching rooms, lecture theatres, an Internet café and two libraries. The network is configured in a manner similar to open public access networks and allows students to use their own equipment with minimal reconfiguration. Access is controlled by the Cisco® equipment so that the only directly accessible service is the University's standard student desktop, provided by the Citrix® application server. The Citrix® service is also responsible for authentication, authorisation and data encryption. To date the service has attracted in excess of 2,300 different users since going live in September 2003.

The combination of technologies has resulted in a highly flexible, manageable and secure wireless service. Students have the same access to software applications and file space as campus hardwired facilities and the remote access service.

Introduction

Northumbria University has several open access IT facilities at various locations. Demand for these facilities is always high, with lengthy queues forming at peak times. There was clearly a need to increase access to IT services for students. In addition, increasing numbers of students have their own wireless-enabled notebook and laptop computers. Wireless technology appeared to offer a solution to this problem. It was thought that wireless access points could be used to provide both conventional hotspots and fixed point terminals. The fixed point terminals would use wireless both to save having to hardwire each node and to provide a degree of flexibility should they need to be moved.

The University makes extensive use of the Citrix® application presentation suite. This product enables central management and configuration of applications and whole desktop environments. Citrix® is a thin client technology in which the applications are executed on one or more remote servers, with only screen updates being transmitted across the network. This results in low bandwidth use on the network, and allows applications to be used on lower specification equipment such as elderly PCs and dedicated terminals. All activity is logged, allowing the University to gather statistics on usage and thus to customise the service accordingly. Multiple servers can be used for application presentation, giving a degree of fault tolerance and redundancy. The applications offered to the student body range from mind mapping software and the Microsoft Office package through to specialist applications for individual schools, such as Engineering. The centralised management of the service allows access to applications to be restricted to authorised users, thus aiding licence management.

The University's network infrastructure is based on Cisco® equipment.

Service requirements and constraints

User Support

In order to minimise the potential increase in demand for user support services, and to avoid any disputes concerning liability, it was decided that students would be expected to configure their own equipment. Recognising that this may prove a challenge for the less technically able, a series of step-by-step guides were prepared in both printed and online formats. The

availability of the wireless network was to be indicated by the presence of hotspot signs and posters giving advice on how to connect to the network. These signs would take the form of both a small logo bearing images and larger posters with more detailed instructions. Also, some informal workshops were held.

Coverage

Coverage was required in a wide variety of locations. The University has a number of seating areas where students tend to congregate. Academic staff had previously expressed interest in having wireless networking facilities in some of the larger lecture theatres and in certain teaching areas. The Library and Students' Union were also identified as areas where wireless networking could be used as a useful supplement to the existing library IT provision. In common with many institutions, Northumbria occupies a diverse collection of buildings ranging from Grade I listed terraces to newly built modern teaching facilities. Each of these types of buildings had areas where wireless coverage would be desirable, but it was far from clear what impact the physical structures of such a range of building types would have on the project.

It was decided that we would use equipment complying to the 802.11b standard as this offered the maximum range of coverage. Our intended use of Citrix® technology led us to be confident that bandwidth would not be a problem, and this has since proved to be the case. Some access points regularly attract over forty concurrent connections.

Security

Security is always taken seriously at the University and this project was no different. The industry press has raised concerns about apparent weaknesses in the Wired Equivalent Privacy (WEP) protocol, which is used to encrypt wireless network data. It was decided that WEP could not be relied on as the sole security mechanism. Fortunately, the University has considerable experience of Citrix®'s encryption mechanisms, and had recently implemented Secure Sockets Layer (SSL). This combination of SSL and Citrix® encryption seemed to offer the most promising solution, being a balance between an acceptable level of risk and technical complexity.

Guest Access

It was decided at a very early stage that there would be no provision for Guest, or Anonymous, user access. Only users who had already been issued with a University ID and password would be able to authenticate via the Citrix® service and thus gain access to the academic network. A mechanism for issuing IDs and passwords to visitors to the University, such as consultants and external examiners, was already in place and well established. It was decided that there was little benefit to be had, and considerable administrative overheads to be incurred, by enforcing registration of each client device that was to access the wireless network. Not requiring registration also eliminates any delay between staff, students and visitors receiving notification of their network IDs and being able to access the full range of networked services, wireless included. Effectively, students' notebook and laptop computers can connect 'out of the box'.

Maintenance

Other key requirements were reliability and ease of maintenance. The service would be required to operate continuously with the minimum of technical support. The University is constantly reviewing and striving to improve the level of support available to students but twenty four hour technical support is not yet practical. There are also heavy operational demands on technical staff such as network engineers. Therefore the service had to be as near to maintenance free as possible, and have a high potential for remote management.

Feasibility study / site survey / cost comparisons

Feasibility

Several small scale tests and pilot schemes were conducted to establish whether there was a sufficient level of interest to justify investment. These schemes attracted very positive feedback from the user community and were useful learning exercises in their own right. The initial focus was on identifying a solution that would allow the University to have strict control over the available service via a wireless connection, rather than simply enabling direct access to the academic network.

Having agreed a preference not to require hardware registration, it was recognised that there was a need for some form of monitoring and alerting facility that would allow our network administrators to identify and respond to any inappropriate activity quickly.

Surveying

All surveying was carried out by University staff, saving the cost of contracting out the work. This approach also allowed the surveying to be scheduled around the University's normal activities, such as examinations, with the minimum of effort and disruption, as well as exploiting staffs' knowledge of the existing network and buildings layout.

The University purchased handheld survey equipment for initial site surveying. This was backed up by a Fluke Networks OptiView™ network analyser for detailed pre- and post-installation. This surveying was carried out once the initial site surveying had given a rough impression of the number of access points needed and the coverage that could be achieved.

Cost Comparisons

Initially we examined low cost access points intended for the small business and domestic markets. However it was found that these devices would incur relatively high support costs due to the lack of any central management and configuration facilities. It was also found that they were prone to a failure to respond to client devices for no apparent reason, requiring a manual reboot. Power supply was also an issue as a domestic mains supply would be required for each access point, restricting the locations where they could be installed and incurring more cost. For these reasons it was decided that the cheaper access points would be a false economy. We decided to use Cisco Aironet® 1200 Series access points which, although more costly to purchase, were felt would be more cost effective to run in the longer term. The main features guiding this decision were the Aironet's power over LAN capability,

the availability of a central management tool, the capacity for expansion by fitting a second card, and integration within the existing Cisco® based network.

Project planning

Academic liaison contacts were approached and asked to give some indication of which locations they would like to have considered for wireless coverage. Having drawn up a list of over 130 potential locations, these were then prioritised and estimates of the work required were produced. The target date for having a significant number of areas covered by wireless was the start of Semester 1 in September 2003. It was recognised that we would be unable to provide coverage to all of the locations identified with the Schools Liaison committee, hence the decision to prioritise. This allowed us to focus our installation work on the thirty top priority locations, aiming for the Semester 1 deadline, with the remaining lower priority locations receiving coverage as resources and funds became available over time.

Security is always a high priority consideration at Northumbria University. Radius servers, gateway (or edge) servers with built in security features, and dynamic WEP were all investigated. However it was quickly recognised that it was possible to force wireless network traffic to be routed directly to our existing Citrix® service, which uses the Secure Sockets Layer (SSL) protocol for initial user credential transmission and 128 bit encryption thereafter. By taking this approach we would be enforcing a robust level of security without having to invest in additional technologies, all of which would bring extra costs and possible risk.

Procurement

In accordance with the University's financial regulations at the time, an Invitation To Tender (ITT) for the supply of wireless access points, network switches, routers and network analysis equipment was issued. Three potential suppliers responded and the contract to supply was awarded to SkyNet Systems Ltd. A key stipulation of the ITT was that we would be able to vary the quantities required as installation progressed. This clause was essential as we realised it was impossible to predict accurately the precise number of access points and switches that would be needed until detailed surveying had been carried out.

Implementation

The first stage of implementation was to assess the capability of the existing network infrastructure to meet our requirements. Due to the relatively new nature of the technology, we were very reluctant to have wireless network traffic on the same infrastructure as our existing traffic. Recognising the likely cost of installing a dedicated backplane for the wireless traffic, the preferred solution was a Virtual Local Area Network (VLAN) which we would be able to implement using Cisco® equipment. However, this would have involved a large amount of network reconfiguration during the student registration and induction period. As any possible disruption to the network during this period was judged to be an unacceptable risk, an alternative solution had to be found. There were already plans to install a separate fibre optic network infrastructure to take some of the load off the existing infrastructure. By bringing this work forward it was possible to make temporary use of this network to carry the wireless traffic. This allowed the project to proceed without risking disruption to the main network. As the University entered the lower risk phase of its business cycle we were able to begin implementing a VLAN, releasing the fibre network for its original purpose.

During this process it was found that at least twenty-five new Cisco Catalyst® network switches would have to be installed. Due to the effort put into prioritising locations to have wireless coverage in the planning stage, it was possible to phase the installation of switches in such a way that access points could quickly be fitted in high priority areas intended to have wireless coverage.

Two models of access gateways were evaluated. These were found to be adequate for their intended purpose but were ultimately rejected in favour of controlling network traffic via the Cisco® routers. The limitation of this approach is that the user has to enter the URL of the Citrix® service correctly. While this can be problematic for users new to the service, a comprehensive series of user guides are available and new users soon seem to become accustomed to it.

Operational performance and reliability

Take up

Peak concurrent usage has been recorded at over 90 individual students and is rising. One of the more popular hotspots regularly attracts between ten and twenty concurrent users, with no discernible degradation in performance. The use of Citrix® means that users experience very high levels of performance as all application processing is carried out remotely.
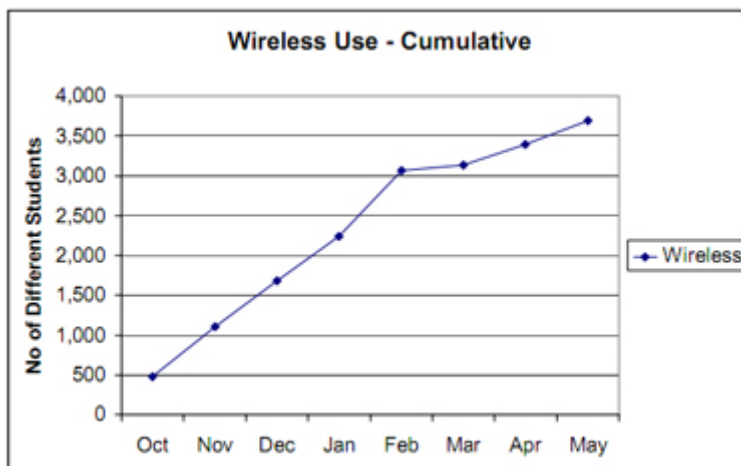


first eight months of operation.

[1]

Roaming users

In the event of a session being interrupted, the Citrix® service will allow users to reconnect within one hour. This has proved popular with students using loaned laptops who can use the machine until the battery is exhausted, then simply swap the machine, reconnect to their original session, and carry on where they left off.

Hardware

The Cisco Aironet® access points are easily expanded by adding a second wireless card should the need arise. This expandability was one of the main attractions of the Cisco

equipment. A Cisco Wireless LAN Solution Engine® is used to centrally configure, manage ...he Wireless LAN Solution Engine® in
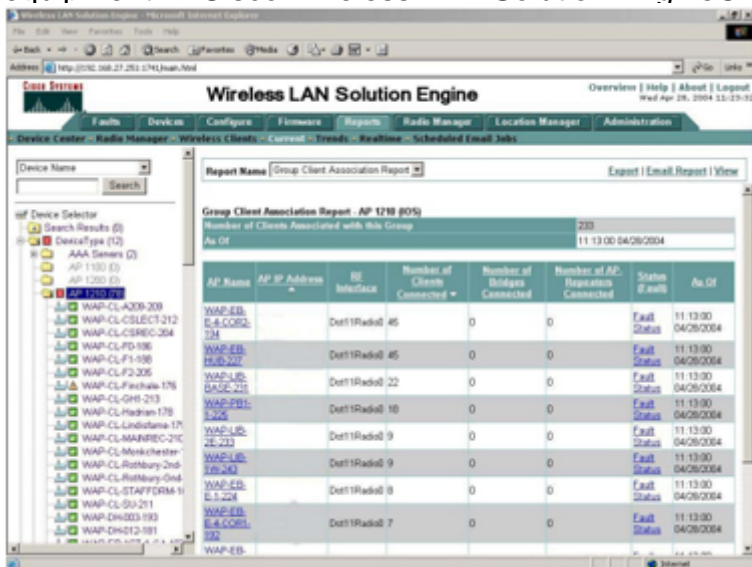
[2]

Laptops are available on loan in the Library and in a group study area in the School of Built Environment. This facility has proved to be very popular with students.

It was decided that it would be inappropriate for the University to insist on a particular make of wireless card to be used by students. This was largely because extensive testing revealed that, provided the card was 802.11b compatible, there was little difference between makes. The fact also had to be taken into consideration that some students were coming to the University with wireless devices built into their laptops and it would have been impractical to insist that they buy a second card to use our network.

To date there have been no technical problems with the access points and just one malfunction in a network switch. There have been complaints of slow response times in one of the most popular group working areas. The situation is under observation with a view to adding a second card to this access point if complaints persist.

Software

The Citrix® hosted desktop application has performed well despite the addition of the wireless network. This is possibly due to a planned programme of continuous expansion of the supporting infrastructure.

Benefits of project

As wireless networking becomes more established we are finding that greater numbers of students, and increasingly staff, are expecting some form of wireless facilities on campus. We suspect it will not be long before wireless access is expected as part of the normal portfolio of services offered by a modern University.

The availability of hotspots, loaned laptops and casual access points has greatly enhanced an already popular group working area in the library. Students engaged in group learning

activities are able to access and share learning materials, personal files and material on the Internet, all via the wireless network. This combination of wireless, thin client and e-learning technologies enables the University to offer a much richer learning environment than was previously the case.

The decision only to allow wireless users to connect to the Citrix® desktop services has the added benefit of ensuring that all Internet traffic is routed via the University's central firewalls and web site blocking software, preventing inappropriate use.

The delivery of a consistent desktop, application set and access to user file space is also seen as a considerable benefit. Students are presented with the same look and feel of desktop regardless of which access route they choose to use, i.e. the same level of service is offered by campus hardwired desktop machines, the University's remote access service 'Desktop Anywhere', and now the wireless network.

Lessons learned

- A reliable and manageable network infrastructure is essential.

- The ongoing management and maintenance of the access points and related equipment should be given serious consideration from the outset.

- Site surveys can be carried out by in-house staff provided they are given appropriate equipment and possess the relevant skills.

- Wireless networks involve a lot more wires than the name would suggest.

- Deployment of a wireless network does not necessarily lead to an increase in administration costs.

Summary

We believe that the students' learning experience is further enhanced by the use of a single standard student desktop accessible in a variety of ways. Northumbria University students can now use Microsoft Outlook, desktop publishing, computer based training and technical references, Microsoft Office applications, Microsoft Project, statistical packages, a range of online learning support resources, and their personal file space. They have access to these services from any of six open access IT suites, from desktop machines in our Cybercafé, and via the Internet. Wireless networking has allowed the University to further enhance the service.

Trademarks

Cisco®, Catalyst®, Aironet® and Wireless LAN Solution Engine® are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the US and certain other countries.

Citrix® and MetaFrame® are registered trademarks or trademarks of Citrix Systems, Inc. in the United States and other jurisdictions.

OptiView™ is a trademark of Fluke Networks Inc.

Links

[1] https://community-stg.jisc.ac.uk/system/files/images/wtas-northumbria-01.jpg
[2] https://community-stg.jisc.ac.uk/system/files/images/wtas-northumbria-o2.jpg