Published on *Jisc community* (https://community-stg.jisc.ac.uk)

Development of a Secure Campus 802.11b Wireless Network

Geoff Constable, Hefin James and Ian Jones,

University of Wales, Aberystwyth

Contents

Summary

During the summer break of 2003 the Network Development Team at University of Wales, Aberystwyth (UWA) drew up a list of requirements for the purchase of wireless APs. The most important requirements included value for money, range of use, remote management, statistics gathering and (as far as possible) a future-proof upgrade path. The equipment of three manufacturers was assessed by everyday use and also load-testing. The Cisco® Aironet® 1200 was selected as the most suitable wireless AP for deployment and this was also evaluated for compatibility with a number of wireless cards in common use.

The need for a secure solution, protecting users' equipment and also protecting the UWA LAN was paramount. The solution chosen allowed for added value to be gained from equipment already deployed at the University: the VPN server used to enable secure dial-in by remote users. A spare port on this server enabled wireless users to login to the remote access service before logging in (with a different ID and password) to the UWA LAN.

Deployment was incremental and early experience was gained by limited deployment at popular public areas. Support staff were trained to handle enquiries relating to the service and publicity material was distributed. The service continues to grow modestly in usage and popularity, and its use is closely monitored to ensure adequacy of coverage. So far the solution deployed has proved to be reliable and robust, and has not experienced any problems. On current projections, it is expected to continue to be a scaleable solution for the foreseeable future.

Introduction

This case study follows the process that has led to the introduction of a supported wireless service at University of Wales, Aberystwyth (UWA), from initial concept through to full service. Two key requirements were:

1. that access should be easy to accomplish and self-configurable for the end user, with no need to involve UWA staff in the registration and use of the service. This implied that wireless APs (access points) should be configured to be open, with no encryption or Wireless Equivalent Privacy key enabled.
2. that use of the wireless network should not compromise security for the end user or the UWA network.

To meet these key requirements, the solution was to create a dedicated wireless VLAN (Virtual Local Area Network), and to use the second network connection on UWA's existing VPN (Virtual Private Network) service. The case study explores the implications and explains this choice of solution in detail.

Equipment was selected and deployed, with the intention that the infrastructure used would form the basis of an expandable service. During this initial phase of development, various wireless APs and wireless PC cards were tested. The experience gained in the initial, limited deployment has allowed the rapid further development of the wireless network to its current state, where most public areas are covered with some connectivity and there are wireless APs available on all three of the UWA campuses. The case study:

- considers the requirements for a scalable, future-proof wireless network deployment in a university environment
- includes the test and evaluation details, and results, for various manufacturers' wireless APs
- includes details of the configuration of the wireless APs for this deployment
- gives timescales for the project as it moved from initial development to a supported service
- includes results of testing of various manufacturers' wireless PC cards
- reports the current state of the service development, and any problems encountered since its availability to the general student and staff population

- considers lessons learned from the service development and deployment
- offers advice for the deployment of wireless APs, especially regarding ease-of-access for users and defending the security of the institution LAN.

Background

Prior to the introduction of wireless APs on campus during 2003, the University had no WLAN (wireless local area network) access provision to the UWA LAN or the Internet. There was no wireless provision by other commercial Internet Service Providers in the town either, as far as was known.

There were laptop users amongst students and staff, who accessed the LAN via Ethernet NIC (Network Interface Card) cards. These could be brought onto campus and connected to the network temporarily for Internet access, using wired points provided for this purpose at public workstation rooms and teaching rooms. These intermittent connection points had to be shared between laptop users, and there were typically only two connection points available in a public workstation room. At the time the project began, only fifteen of these temporary wired access points were available. These continue to be used in parallel with the wireless provision, and more are planned for this academic year. Statistics monitoring, anecdotal evidence and feedback from student users indicated that the provision of these points was insufficient to meet demand – therefore the provision was comparatively low while demand was increasing.

Evidence also pointed to an increasing number of laptop users, and amongst these the number with wireless cards had also increased. Wireless cards were becoming a standard component of a laptop bought ‘off the shelf’ and so enquiries about the availability of a wireless service were beginning to trickle in.

A new University department was being developed at this time, and the department’s staff requested wireless access throughout the building that was being built to house it. This was to cut the costs of furnishing the building, by saving the need for extensive cabling. There was also a growing general awareness of the benefits of wireless provision to mobile users such as students. This was becoming apparent from articles and features in the general and networking press, and also from the deployment of wireless access by some of the retail food, drink and hotel chains.

Service Requirements and Constraints

Any wireless access service deployed on the network needed to meet a number of distinct requirements.

- The wireless service should be at least as easy to access and use as a wired connection.
- Potential users should be able to self-configure their devices in order to take advantage of the service.
- UWA staff should not need to act or intervene when users register for, and use, the service.
- The wireless service should not compromise security for the end user or the UWA network.
- The service should be accessible to users of Windows, Linux® and Macintosh operating systems (these are all represented amongst the user-base at UWA).

- The solution adopted should be scalable from a single wireless AP through to complete wireless coverage: from one user through to potential thousands.
- The service should be capable of being introduced incrementally as funds become available.
- The service should be accessible by laptop/notepad devices and by other wireless non-PC equipment (e.g. PDAs – Personal Digital Assistants).
- The wireless APs should be remotely manageable by UWA networking staff.
- Data throughput, wireless range, deployment and installation costs should reflect the best value for the financial resources available for the project.
- If possible, the hardware should be upgradeable to support new and emerging alternative wireless protocols.
- The selected wireless APs should be pollable by SNMP (Simple Network Monitoring Protocol), to allow for automatic monitoring of the service and the gathering of statistics.
- In keeping with UWA policy, the solution should be simple and useable enough for the UWA network team to deploy, support and manage in-house.
- The service should be accessible from teaching areas throughout the University (lecture theatres and seminar rooms, etc.), with the eventual aim of full coverage throughout the University.

An additional technical constraint was that the range of the wireless APs should allow the desired coverage without needing additional extensions to the existing wired LAN. Ideally the equipment would also be capable of being powered in-line, i.e. using power over Ethernet, thus avoiding the need for additional expense in extending power cabling to the units.

There were also financial limitations and time constraints. The decision to start experimenting and evaluating different solutions was taken prior to the summer recess of 2003. Funds saved on other networking projects had allowed for a small trial to take place during summer 2003, and £5,000 had been identified for the 2003–2004 academic year, commencing August 2003. The aim was to extend the reach of the proposed service as far as possible during that time, for the funds available, whilst still meeting the requirements outlined above. The intention thereafter was to allocate £5,000 per annum until full campus coverage was achieved. The funds outlined here were quite separate from the cost of the deployment in the new departmental building, although a trial deployment would kill two birds with one stone as it would also allow for an evaluation of suitable equipment for the new building.The service would initially be deployed in main library foyers – one in each of the three University campuses. Eventually access would be rolled out to all of the University’s four main libraries. The plan was to make the service available in areas where the public congregate to eat, drink, relax or study. As well as the library foyers this includes:

- a large concourse with tables, chairs and food/drink vending machines (and outside seating area) known as the Geography Concourse
- the foyer, cafeteria, bar and picnic area of the Aberystwyth Arts Centre (a department of the University of Wales)
- the paved open area in front of the Arts Centre (a popular point for students and staff to congregate)
- Brynamlwg, the staff social club.

Selection of Suitable Wireless Technology

The wireless technologies available at the time included 802.11, 802.11b and 802.11a. Although ratified at the same time as 802.11b, 802.11a has never reached a significant degree of market share in the UK. While initially popular in the US, there were questions about its range, and also interference from and with adjacent wireless services (such as public services, radio sets, etc.). Its higher frequency also means that it is more subject to loss of signal and interference from the built environment and natural obstacles. Additionally, 802.11b equipment cost less at the time of the project.

At that time, 802.11g was also emerging. This appeared to offer a higher bandwidth alternative to the widely available 802.11b solutions, though the impact of 802.11b cards would reduce any bandwidth advantages accrued from 802.11g. As mentioned in the requirements section above, a criterion for the selection of wireless APs was that they should have a viable upgrade path, i.e. should allow any emerging wireless technology to be deployed, either by a software, firmware or hardware upgrade. Because 802.11g was immature at that time, provision has been made for its eventual deployment from the existing wireless APs.

The market leader, and at the time the most tried and tested technology in the UK, was 802.11b. This technology also offered the cheapest of the solutions under consideration, and so it was this solution that was explored further.

UWA is a typical rural campus university, with buildings scattered around a hillside, separated by paths and lawns, car parks, gardens, etc. Although the entire campus is situated on a steep hill, the geography posed no unusual challenges.

Security Considerations and Solution

As stated in the requirements section, the security of wireless users and the UWA LAN, as well as the physical security of the wireless APs themselves, was of prime importance when considering the potential use of the network. This would mean that people with wireless enabled devices who were not bona fide users would not be able to access the UWA LAN (and the Internet); and that legitimate users of the system could access all the same services via a wireless connection that they could using a wired connection, but have no ‘back door’ access to services or material that they were not entitled to view or use. In short, the experience, rights and privileges of a wireless user should be the same, and as far as possible feel the same, as any wired user. This meant that users should be verified and authenticated before gaining access to the network.

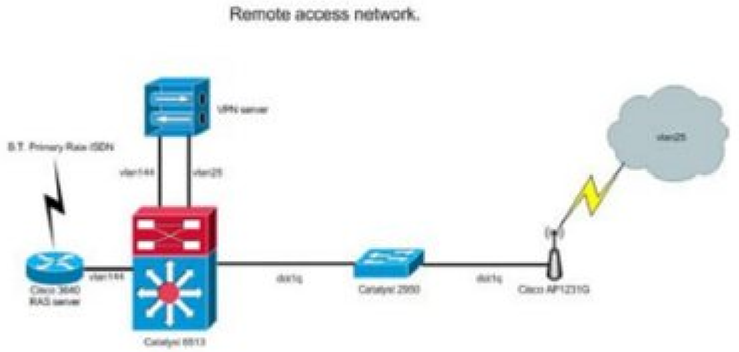
Initially the Wireless Encryption Protocol (WEP) was examined to see if it would solve the problem of unauthorised users. This protocol is designed to stop unwelcome use of a wireless network by exchanging an encrypted 64 or 128 bit key between the network and the wireless card in the device. Drawbacks to WEP include the facts that it can slow down access to the LAN via the wireless connection, it adds another layer of complexity to the means of access (which should be self-configurable), and there are security flaws inherent in the use of the protocol itself (cf. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html [1]). A determined hacker could feasibly gain access to the network despite the deployment of WEP.

UWA already offered a dial-in service for at-home users to gain access across the public telephone system, using an analogue telephone line, an ISDN line or broadband technology such as ADSL. This Remote Access Service (RAS) has been in place since 1997 and has been comparatively problem-free both for users and network administrators. The RAS relies on the deployment of a VPN that links dial-in users directly to the UWA LAN as if they were part of that LAN. Users must register for the RAS service before they can use it, and they are supplied with a RAS password which must be different from their usual network password.

(Since July 2001, this service has been supported by a dedicated VPN server located on the UWA LAN. The VPN server is running on a standard Windows 2000 Server installation on a 1Ghz PC. The RAS service is running on a Cisco® 3640 with primary rate ISDN and digital modem cards. The service supports 18 simultaneous modem users of the dial-in service.)

It was soon realised that, logically, there are parallels between accessing the LAN through dial-in across a public telephone service and accessing the LAN by using an open, public wireless network. Allowing wireless users the potential to access the wireless network, but not the LAN itself, does not actually compromise UWA security. In fact, because of the double-level password entry process, this method may be more secure than access through a public workstation on the LAN.

Therefore a spare port on the VPN server was identified and used. This is connected to an Ethernet switch, which is in turn connected directly, or indirectly (but logically) using a VLAN, he network.



[2]

Figure 1. Interconnection of the RAS, VPN and wireless services.

This means that when users with a wireless device use their wireless software to locate a service, the local wireless network ‘tsunami’ (the default Cisco® identifier) will be seen, and this can be accessed by any person who has wireless equipment while they are at one of the University’s wireless hotspots. However, they will not be able to see anything else – it will be impossible to access the Internet or the UWA LAN unless they have previously registered for the RAS service, and they will be challenged and authenticated every time they use the service. Once they are connected to the UWA network, all of their activity while connected will be logged.

All wireless APs deployed are on the same logical VLAN. While the wireless device is not connected to the network (i.e. until the user has been authenticated), it still needs to have an address to which to route IP packets, and for this purpose it is given a private IP address using DHCP (Dynamic Host Configuration Protocol). By default, wireless devices send out a broadcast DHCP request when they are first connected. The user then has to be authenticated. Secure communications continue between the client and the VPN server using this private address, until the user has been authenticated, when a ‘real’, public and routable

IP address is allocated to the device. The communications between VPN client and server are then sustained using a well-known security protocol, either PPTP (Point-toPoint Tunnelling) or IPsec, and a routable ‘real’ IP address is then ascribed. This VPN set-up means that communication between the client (laptop, etc.) and the server are secure across the wireless section of their path, where there would otherwise be a possibility of hacking into these communications by other wireless users.

The VPN server was purchased exclusively to service the needs of home users. When it was purchased, it was not envisaged that there would be another potential use for it. However, there was a spare interface available, and so the service was developed to make use of it.

This solution still allows users who are connected to ‘tsunami’, the wireless network, to ‘see’ each other’s computers in a peer-to-peer relationship, without actually accessing the UWA LAN. This potentially means that non-UWA users could open peer-to-peer connections to swap files, play games, etc. While this potential is there, this is not a problem that has made itself felt as yet. Most users wish to connect to the Internet and/or the UWA network, and so would register and get a RAS ID in the legitimate way. However, if they wished to use their computers in this out-of-LAN fashion, they could potentially slow down the performance of other wireless AP users. This is something that the team is aware of and is monitoring, so that IP addresses that never request a VPN connection can be managed appropriately. So far it has not tackled one, as the problem is currently theoretical rather than real.

Project Planning

The whole project was dependent on the work of the NDT (Network Development Team) leader, Hefin James, with support from team members, so project management was kept informal.

However, there were clear steps and a defined timetable for the project. These can be defined as follows:

Timescale (2003)	**Task**
By June	Identification of suitable wireless technolog
June – week 1	Configuration of VPN to support wireless
June – week 1	Identification of suitable wireless APs for te evaluation
June – weeks 2/3	Test and evaluation of selected wireless AP requirements criteria

June – week 4	Deployment and use of first selected wirele
July	Testing of wireless NICs for interoperability
July	Early use and experience by limited group
August	Deployment of first library wireless AP
August	Training of front-line support staff in wireles
August onwards	Development of user help and support web
August onwards	Development of a policy on wireless deploy
September onwards	Continued incremental deployment of wirel public areas

Costs for the process have been mentioned in Section 3. The first wireless AP was to be purchased from spare cash which had been allocated to another project, but was surplus and therefore available for this purpose. Five thousand pounds was available from August 2003 for the first year. This would not include network development staff time, but would include the cost of any necessary cabling (network and/or power supply).

Equipment Test, Evaluation, Comparison and Selection

The wireless APs for test and evaluation were selected from research in the press, reviews, white papers and data sheets available on manufacturers', resellers' and trade press websites. The most important selection and evaluation criteria were ease and scalability of remote management, data throughput and extent of coverage (or 'range'). Of these, the latter – the extent of coverage that the wireless AP gave – was the single most important selection criterion.

Three wireless AP models were selected for testing. These were:

- NETGEAR® WG602
- D-Link® DWL7000 (http://www.dlink.com/products/?pid=14 [3])
- Cisco® Aironet® 1200 (http://www.cisco.com/en/US/products/hw/wireless/ps430/index.html [4])

The network engineer responsible for the project tested each of the units informally by installing them, configuring them, and then accessing the LAN across the wireless link, using a wireless enabled laptop PC. He then walked around the vicinity of the wireless AP and noted the extent of the coverage.

Stress testing between the laptop and the UWA network was conducted by timed transfers of bulky files, observed performance of large streamed files, etc.

It should be noted that the test results and conclusions reached at that time might not still apply to this set of products, as manufacturers are adding functionality and updating their products continuously. For similar reasons, these might not necessarily be the particular wireless APs that would be selected for testing if the same process was started now.Data throughput during load testing was found to be more or less consistent using the different wireless APs, but some differentiators between the products were immediately apparent, particularly those that set the Cisco® Aironet® solution apart from the others. The Cisco® Aironet® 1200:

- was more expensive
- offered scaleable remote management
- had a greater range (up to 50% more in some cases)
- allowed for in-line power supply (with the additional purchase of a small add-on hardware module)
- was supplied with a lockable mounting cradle for a secure physical attachment to the wall.

	a	b	g	RM	802.1q	SNMP
NETGEAR® WG602		Y	Y	---	---	---
D-Link DWL7000	a	Y	Y	web	---	---
Cisco® Aironet® 1200	a	Y	Y	Y	Y	Y

Table 1. Features of the tested wireless APs summarised.
Features: a = 802.111a support; b = 802.11b support; g = 802.11g support; RM = remote management (web, telnet); 802.1q = support for VLAN standard; SNMP = support for the Simple Network Monitoring Protocol; 802.1p = support for the Layer 2 Quality of Service standard; Upgrade? = whether there is a software/firmware-based upgrade path for the product. This table is based on manufacturers' information at the time of writing (August 2004), not at the time of the project analysis. Despite this, there are only minor specification differences.

As can be seen from Table 1, the Cisco® Aironet® 1200 solution met more of the defined requirements for the wireless network points than any of the other wireless APs that had been selected for test and evaluation. Although more expensive, the Cisco® Aironet® 1200 offered the nearest fit to the requirements and the greatest physical coverage (from the same test point), and appeared to offer the prospect of the best return on investment.

Before final selection, however, the engineer also tested the interoperability between the Cisco® Aironet® wireless AP and some sample laptop wireless NIC cards. This was to ensure that users of a cross-section of popular wireless cards would be able to get satisfactory connectivity and throughput. It also reassured the deployment team that these cards would interwork satisfactorily with the VPN service and the solution that had been deployed. The wireless NIC cards tested were:

- NETGEAR® MA401
- Buffalo Air Station (WLI-CB-G54A)
- Cisco® Aironet® 350
- ATI AT-WCL452
- Linksys WPC51AB.

All of these cards were found to interoperate successfully and easily with the Cisco® Aironet® 1200 wireless AP. Load tests were conducted as previously, with the different cards in place. As with the wireless APs, the throughput was fairly consistent using different cards, but the range of these wireless cards was found to vary considerably (although care was taken to test under the same conditions and in the same location). The Buffalo Air Station also comes with a socket for deploying an external aerial in order to boost the card's range.

One interworking problem was found during the process of this testing. During tests, a laptop driven by an Intel Centrino processor was found not to interwork with the wireless APs using 802.11b or g when set to channel 12-13. Intel's Centrino wireless LAN product has been designed to permit legal operation world-wide in regions in which it is approved. Operation on channels 12-14 is not permitted in all regulatory regions of the world. Consequently the wireless LAN feature is limited to operate on channels 1-11 and will not support channels 12, 13 and 14.

Procurement

At the time the wireless APs were selected and procured, Cisco® offered only the Aironet® 1100 and the Aironet® 1200. The former, though cheaper, did not offer an upgrade path for future enhancements of the protocol or the implementation. This was an important requirement, so a 1200 solution was selected.

There are three resellers of Cisco® equipment in the UK education market. The procurement process consisted of sending e-mails to the different suppliers and seeing what prices could be negotiated. The supplier – Skynet Systems – was then selected purely on the basis of best value for money. The ordered goods were covered by a standard sixty day warranty, but no further warranty or support was purchased, in line with the current practice at UWA for equipment of this nature. Spare equipment is held in stock in case of failure.

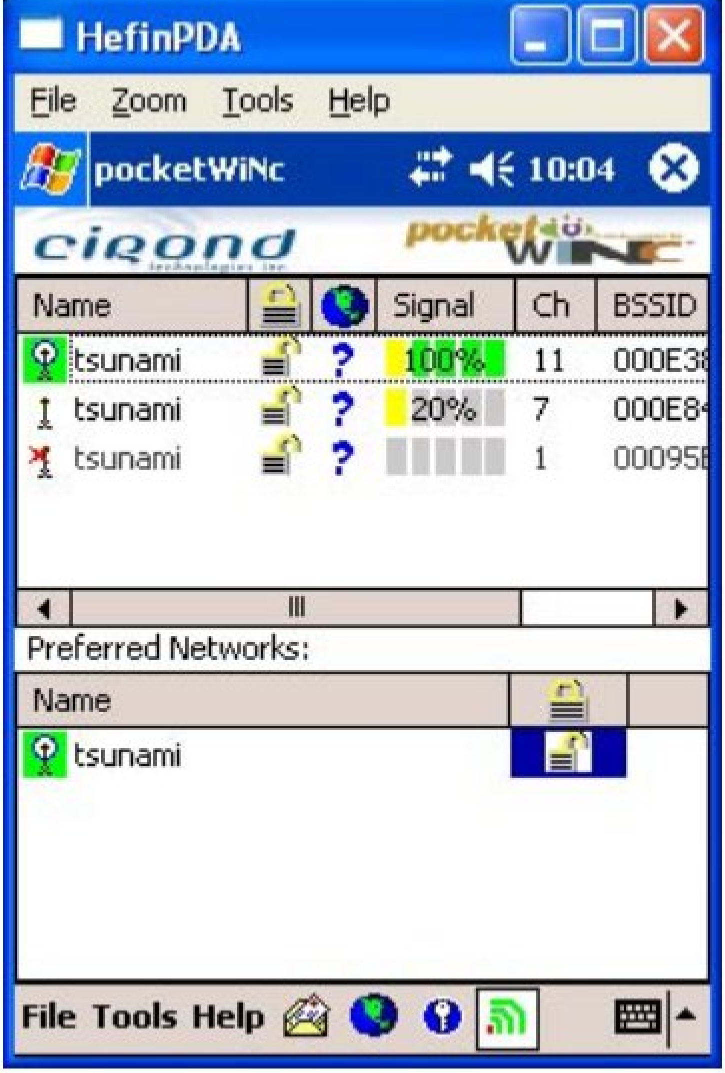
AIR-AP1220B-E-K9	802.11b AP with CBus Slot (to enable expansion), ETSI Configuration (European version of the product)	£350.00
AIR-ANT4941	2.4 GHz, 2.2 dBi Dipole Antenna with RP-TNC Connector	£10.00
AIR-PSINJ1200	Power injector for 1200 series AP (to enable power-over-Ethernet)	£25.00

Table 2. Wireless AP and initial deployment costs.

Implementation

In order to make sure all deployment was done securely, all wireless APs that were deployed were on the same logical VLAN. The first access point to go live was the one in the network development team’s office. After installation in a wall-mounted bracket, various members of staff were invited to try out the access for a week or two. Following positive feedback after further use, installation and deployment began in earnest when the first wireless AP was deployed in a library.

Obvious candidate locations for early deployment were (as mentioned in Section 3) the foyers of the main libraries, and the University’s Arts Centre. The assistant directors of the Library and Information Services department were consulted for further candidate locations. For each location selected, the wireless AP was taken to the location, and then a member of the Network Development Team would literally walk around the selected area with a laptop to detect the limits of coverage. The laptop obviously has a wireless card configured to use the service, but it also used a free program called Netstumbler (http://www.netstumbler.com [5]) to assess the strength of the signal received at various positions in the target area. Software for this purpose is also available for a wireless-enabled PDA – an example is made by Cirond (http://www.cirond.com [6]) with its Pocket WinC software. After a 30 day evaluation, the software can be purchased for a very reasonable price. Figure 2 illustrates a screen of the



Name			Signal	Ch	BSSID
tsunami		?	100%	11	000E3
tsunami		?	20%	7	000E8
tsunami		?		1	00095

Preferred Networks:

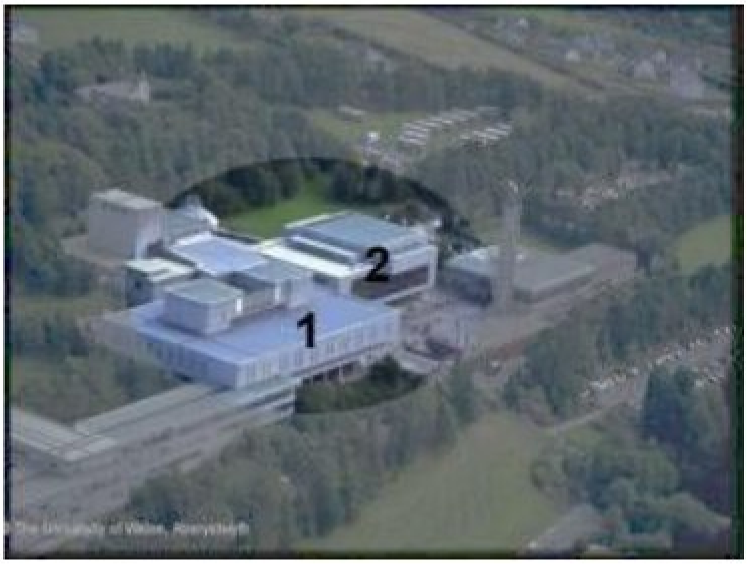
Name	
tsunami	

[7]

Figure 2. Cirond pocketWinC wireless connectivity tool in use on a PDA. This screen-dump was taken while in the NDT office. Three wireless APs have been detected: there is a wireless AP adjacent to the PDA and 2-3 metres away (the 100% signal), there is a wireless AP down the corridor and 20-30 metres away (the 20% signal), and there is a wireless AP in a different building some 60-70 metres away (the item with a red cross and no percentage figure).

Both of these applications have been found to be extremely useful for deciding the best location for wireless APs in order to ensure suitable coverage. The Hugh Owen Library is the main University library and houses books, periodicals, study areas and staff locations. It is a typically large university library (see Figure 3 below). Using the software described above, the optimal positions for locating the wireless APs were found. The library is located on three floors and the wireless APs are positioned on the middle of these, covering that floor as well as the floors below and above. Four wireless APs has been found to be sufficient for full coverage of this building. Experience has shown that depending on the nature of the built environment in any particular location, the coverage from the Cisco® Aironet® wireless APs can vary from 10 metres to 40 metres; and the ‘best’ locations are found by using the laptop or PDA running the applications described above, and a combination of educated guesses, and trial and error. For comparison, at the Arts Centre it was found that just a single wireless

AP provides coverage for the foyer, ticket area, two cafes and bar. It also provides coverage djacent building — the Student Union —

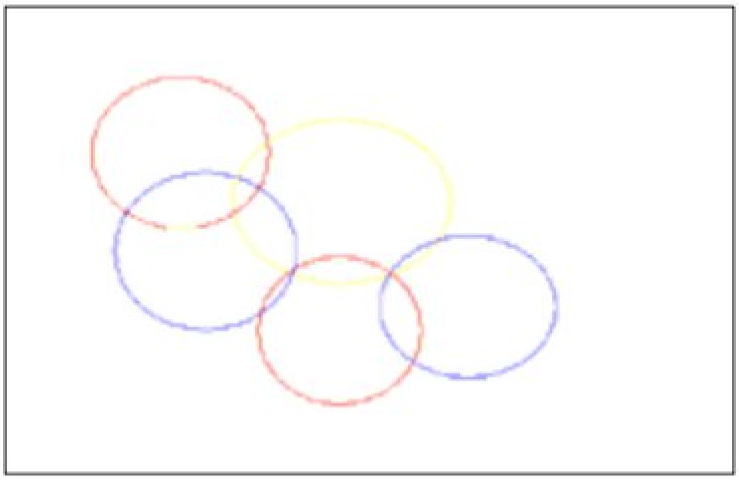


[8]

Figure 3. Approximate extent of service from the wireless APs deployed at the Hugh Owen Library (1) and the Arts Centre (2).

The physical installation of the wireless APs is comparatively straightforward. The Cisco® Aironet® comes with a mounting cradle that needs to be fixed to the wall. The wireless AP itself is placed in the cradle and can then be locked into place. The wired LAN is then attached through the UTP interface. All wireless APs have been placed at such a height that a ladder is needed to access them.

Care must be taken when setting radio channels on wireless APs. The transmitter's modulator sends the signal on a configurable channel. There are potentially fourteen channels available, each with an identified frequency centre. These centres are 0.005Ghz apart. In order to avoid possible clashes and avoid interchannel interference, it is recommended that channels 1, 6 (or 7) and 11 are used in the UK (channels 12-14 are not for use in the US, so this also maintains global compatibility). It is important to be sure that areas covered by wireless APs have boundaries with areas covered by wireless APs set at different channels. There will inevitably be some interconnection between wireless AP areas of coverage, and this will ensure that those areas do not allow users to be in two different wireless zones that are set at the same channel (and therefore frequency). This is illustrated in Figure 2, which is in an area where three zones are accessible, but the 'Ch' (Channel) column in the display indicates that the three channels are set to channel 1, channel 7 and channel 11. Some wireless APS on the market have a feature that auto-detects adjoining channels in use and sets its own channel accordingly, so as not to cause a clash.



[9]

Figure 4. The distribution of channels in adjoining wireless enabled zones.

Attention also needs to be paid to the number of users congregating at particular hotspots and their typical uses. Experience shows that up to 30 people can share a connection at a location without seeing any detriment to the quality of service their applications are receiving, as long as they are using the connection for fairly light-weight applications (e.g. checking e-mail, accessing files, simple web surfing). If they are using more demanding applications (such as live streaming, download of multimedia files, telephony or video applications), then it would only take five or six users for the applications to start to be affected by congestion, and their performance to slow down. The wireless network designer must take this into consideration when deploying wireless APs. If the area to be designated a hotspot is likely to be heavily used in this way, then it makes sense to overlap wireless AP ranges by providing three wireless APs, each using a different frequency. These should then auto-balance and share the network load between themselves.

It is intended that for the next round of wireless APs, to be purchased and deployed for the 2004-5 academic year, optimal locations will be ascertained through a combination of the WinC software on a PDA together with GPS software running on a laptop. The deployment of this next round will not only be concerned with extending the area of coverage, but also improving the quality of the existing coverage, bearing in mind the wireless AP:user ratio at the different locations. Currently the deployment has been comparatively sparse (with the emphasis being on getting coverage at all of the key areas). With an increase in future service uptake expected, it will be important to maintain the quality of service that the user experiences at all of the existing hotspots, as well as simply extending the number of hotspots.

The first wireless AP to be installed in the Hugh Owen Library, the main campus library, was installed in a Green Card Area, where dedicated, bookable PCs, chairs and desks are available for those with disabilities or alternative learning needs. This area is situated close to the Library Advisory Service and Help Desk, which fields enquiries of every kind relating to IT at the University. The advisors were shown the wireless client configuration process and the wireless AP was installed. Posters that had been designed to advertise the location of wireless hostspots were also put up in the area (see Figure 5 below). This very soon stimulated enquiries from would-be users and early experience was gained. The library hotspot was the only one available on the campus for a few weeks, and the ‘softly, softly’ approach to deployment and awareness raising allowed networking and advisory staff to evaluate usage and identify any major problems. Fortunately there were none of these, and the second phase (commencing August 2003) of further deployment and publicity was anticipated with some confidence. During this time web pages detailing the location of wireless APs were drawn up, ‘How-To’ guides detailing the steps involved in setting up a device to use the wireless service were written, and the Acceptable Deployment Policy was drawn up. All of these would provide material for a more cohesive awareness raising campaign as soon as further hotspots were available for use. Once the first wireless APs were installed, there followed a fairly aggressive extension of the service to cover all of the three main libraries, the Geography concourse (a sitting/eating/drinking area), Brynamlwg (the staff social club), etc. This was accompanied by the aforementioned publicity campaign in general University publicity material, staff newsletters, etc. Of course the service is to a certain extent self-advertising, as users are fairly conspicuous.

By the end of the 2003-4 academic year there were fifteen wireless APs deployed. Three of these are not advertised for public use, as they have been installed for the use of particular departments. To protect the UWA network, staff at these departments must login for use of UWA LAN and Internet services via the VPN server, in the same way as mobile users do. If these unpublicised departmental locations were to be discovered by a ‘rogue’ user (and the user had a RAS/VPN password) then they would be able to piggy-back on to the UWA LAN by standing outside the offices of the relevant department, but this activity would be ‘noted’ by the system, logged and – depending on the extent of the problem – action could be taken.

[10]

Figure 5. Publicity Posters. Bilingual signs were produced early on to notify users when they are in an area of wireless LAN connectivity – a Wireless Hotspot.

User Support

As mentioned above, once the first wireless APs were installed it was necessary to publicise and support the emerging service. This was done by a number of means, which included:

- putting up bilingual Wireless hotspot posters at locations covered by the wireless APs
- providing a map of those hotspots at: http://www.inf.aber.ac.uk/wireless/ [11]
- adding ‘how-to’ pages to the relevant parts of the Information Services website, at: http://www.inf.aber.ac.uk/wireless/wireless-howto.asp [12]
- using a staff training session to update helpdesk and support staff on the service and common errors
- announcing the service in the weekly e-mail received by all staff at UWA.

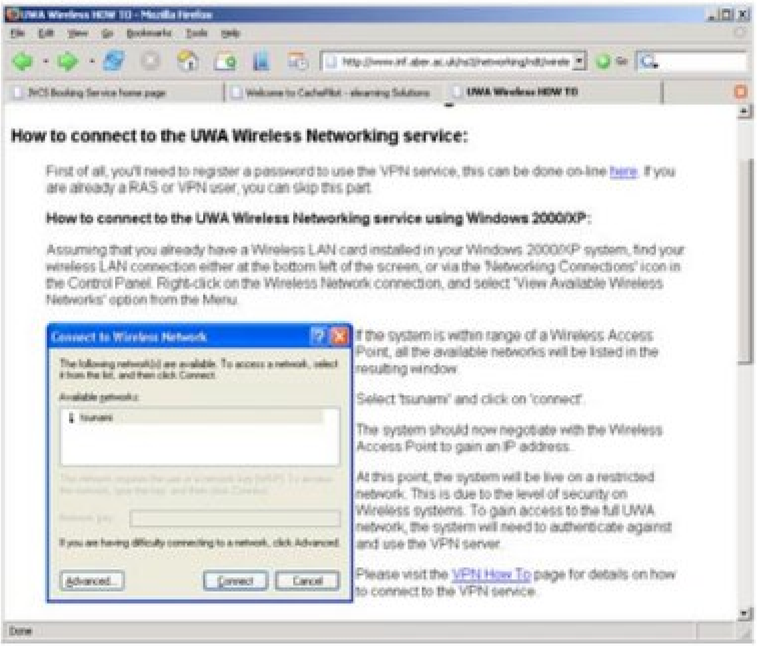
As wireless was now being heavily promoted in the computer press, the possibility was anticipated that someone might purchase a wireless AP and/or wireless card(s) independently and deploy them within their department, office or hall. In order to offer support and advice to those wishing to install local wireless links, and to keep track of this activity, a policy for the deployment of wireless was also developed and publicised. This is an extension of current UWA I.S. policy on attaching anything to the network independently. The UWA Wireless Policy can be found at:

http://www.aber.ac.uk/en/is/regulations/wireless/ [13]

From the users' point-of-view, the registration and configuration process is remarkably simple, and is a process that most competent laptop users should be able to complete without the need for further explanation and support. The user accesses the service after completing the following steps:

- using a web form to register for a RAS password
- configuring the wireless card referring to the manufacturer's instructions and the UWA Wireless 'how-to' pages

tion!



[14]

UWA Wireless HOW TO - Mozilla Firefox

How to connect to the UWA Wireless Networking service:

First of all, you'll need to register a password to use the VPN service, this can be done on-line here. If you are already a RAS or VPN user, you can skip this part.

How to connect to the UWA Wireless Networking service using Windows 2000/XP:

Assuming that you already have a Wireless LAN card installed in your Windows 2000/XP system, find your wireless LAN connection either at the bottom left of the screen, or via the 'Networking Connections' icon in the Control Panel. Right-click on the Wireless Network connection, and select 'View Available Wireless Networks' option from the Menu.

Connect to Wireless Network

The following network(s) are available. To access a network, select it from the list, and then click Connect.

Available networks:

tsunami

If you are having difficulty connecting to a network, click Advanced.

If the system is within range of a Wireless Access Point, all the available networks will be listed in the resulting window.

Select 'tsunami' and click on 'connect'.

The system should now negotiate with the Wireless Access Point to gain an IP address.

At this point, the system will be live on a restricted network. This is due to the level of security on Wireless systems. To gain access to the full UWA network, the system will need to authenticate against and use the VPN server.

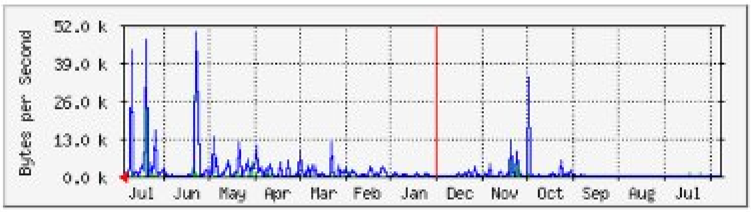
Please visit the VPN How To page for details on how to connect to the VPN service.

Figure 6. UWA wireless how-to web pages: http://www.inf.aber.ac.uk/wireless/wireless-howto.asp [12]

Operational Performance and Reliability

The individual wireless APs that have been installed, and the service that they provide collectively, have proved to be reliable, with no component having failed, crashed or 'disappeared from view' as yet. The service has now been in place and in use for almost a year.

The VPN server provides real-time monitoring but does not log on a per-user basis in a way that can generate statistics for the service. However, the graph of service usage smoothed over a year shows a steady – if gradual – increase in the amount of use, with one or two very large blips (possibly caused by a single user doing something demanding on a particular day) – see Figure 7. The DHCP logs show that as of August 2004 there were over 50 different devices connecting to the wireless service, which is an encouraging sign.



[15]

Figure 7. Wireless network usage, July 2003 – July 2004 (time: right-to-left).

Between July and September there is only the use associated with the piloting activities conducted through the summer. Between October and mid-December 2003, usage begins to pick up, and then steadily increases between January and July 2004.

In common with the rest of the UWA LAN, the service is being monitored continuously, and all usage is logged. Indications are that the service is popular with staff and students, and the Information Services helpdesk has anecdotally reported an increase in calls relating to the configuration of the RAS/VPN or wireless set-up to enable wireless laptop access. An increasing number of students and staff have made their way to the Network Development office carrying a wireless enabled laptop, and the most common configuration problem occurs when people do not realise they have to manually switch on power to their internal wireless cards. Fortunately, this is easily recognised and remedied.

The effort of training support staff to deal with common wireless errors has proved to be valuable in ensuring the smooth uptake of the service. It is anticipated that there will be more laptop users than ever before with the next academic year, and most of these will have wireless enabled devices. There is also an increasing number of staff who need to set up wireless on their machine prior to travelling to attend project meetings and conferences etc., where they will be using their laptops to connect to the local network and will access services across the Internet.

Benefits of the Project

As mentioned in the previous section, it is difficult to remotely access – and thus generate – usage statistics for the VPN server. However, the DHCP logs and the graph in Figure 7 (above) show that the wireless service has been taken up by an increasing number of users. It has enabled users to connect easily to their e-mail and other network services from a variety of teaching locations and more informal settings. It has allowed teaching staff to come to enabled teaching rooms and seamlessly access their filestore and/or the net, from their own machine, and with the minimum of fuss.

It has also enhanced the attractiveness to students of the University as a place to study. Open, mobile access to network services is the current demand and expectation of many prospective and current students, and it is anticipated that this will continue to be the case.

Lessons Learned

In general, the deployment of a wireless network available in most popular public congregating locations has been smooth and relatively straightforward.

One practical lesson learnt about laptop users is that if power is available, they will use it, and this can result in trailing power cables in public areas. Publicity now includes a reminder to be careful not to leave potentially dangerous power cables trailing across public walkways.

Costs per annum for the project have remained steady, but the same amount of money as of August 2004 would allow the purchase of almost double the amount of wireless APs that it purchased eighteen months previously. Whether this drop in prices of wireless equipment will continue remains to be seen.

Appendix 1. Aieronet® 1200 Configuration

This configuration is offered for those familiar with the Cisco® command line interface. It should be read in conjunction with Figure 1.

```
!

hostname air13

!

enable secret 5 $1$Toq5$.5PKUplEyKr99rn61Qt6P1

!

username xxxxx privilege 2 password 7 xxxxxxxxxxxxx

username xxxxx privilege 15 password 7 xxxxxxxxxxxxx

ip subnet-zero

!

!<a number of aaa authentication commands have been omitted here>

!

! start configuration of the wireless interfaces

! including layer 2 bridging between the wireless and ethernet VLANs

!
```

```
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid tsunami
    vlan 25
    authentication open
    guest-mode
 !
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 rts threshold 2312
 channel 2442
 station-role root
 no dot11 extension Aironet®
!
interface Dot11Radio0.2
 encapsulation dot1Q 2 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.25
 encapsulation dot1Q 25
 no ip route-cache
 bridge-group 25
 bridge-group 25 subscriber-loop-control
 bridge-group 25 block-unknown-source
 no bridge-group 25 source-learning
 no bridge-group 25 unicast-flooding
 bridge-group 25 spanning-disabled
!
! start configuration of the ethernet interfaces! including layer 2 bridging between the wireless and ethernet VLANs
!
interface FastEthernet0
 no ip address
 no ip route-cache
 speed 100
 full-duplex
 ntp broadcast client
!
interface FastEthernet0.2
 encapsulation dot1Q 2 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.25
 encapsulation dot1Q 25
 no ip route-cache
 bridge-group 25
 no bridge-group 25 source-learning
 bridge-group 25 spanning-disabled
!
interface BVI1
 ip address dhcp
 no ip route-cache
!
! <a number of configuration commands concerning access-lists, snmp
! and ntp configuration are omitted here
!
End
```

Trademarks:

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

D-Link® is a registered trademark of D-Link Corporation or its subsidiaries in the United States or other countries.

NETGEAR® is a registered trademark of NETGEAR Inc.

Source URL: https://community-stg.jisc.ac.uk/library/advisory-services/development-secure-campus-80211b-wireless-network

Links
[1] http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
[2] http://community.ja.net/system/files/images/wtas-uwa-casestudy01.jpg
[3] http://www.dlink.com/products/?pid=14
[4] http://www.cisco.com/en/US/products/hw/wireless/ps430/index.html
[5] http://www.netstumbler.com/

[6] http://www.cirond.com/
[7] http://community.ja.net/system/files/images/wtas-uwa-casestudy02.jpg
[8] http://community.ja.net/system/files/images/wtas-uwa-casestudy03.jpg
[9] http://community.ja.net/system/files/images/wtas-uwa-casestudy04.jpg
[10] http://community.ja.net/system/files/images/wtas-uwa-casestudy05.jpg
[11] http://www.inf.aber.ac.uk/wireless/
[12] http://www.inf.aber.ac.uk/wireless/wireless-howto.asp
[13] http://www.aber.ac.uk/en/is/regulations/wireless/
[14] http://community.ja.net/system/files/images/wtas-uwa-casestudy06.jpg
[15] http://community.ja.net/system/files/images/wtas-uwa-casestudy07.jpg