Wireless Security

QUESTnet 2007

Paul Hardaker
IT Infrastructure Manager

Kim Armstrong
Telecoms Team Leader &
Wireless LAN Project Manager

UWS Wireless Project 2006/7

- Background – UWS
- The Project – An overview
- Request for Proposal
- Request for Tender
- Selected Solution
- Project Implementation

University of Western Sydney

- Six main campuses (Penrith, Campbelltown, Bankstown, Parramatta, Blacktown, Hawkesbury).
- Over 400 buildings.
- Around 390 teaching spaces, including 50 lecture theatres.
- Approximately 35,000 students.
- Minimal wireless networking prior to 2006.

Wireless Project - Outline

- DEST funding of $2.1M for ‘06.
- Objective: Wireless access for UWS students.
- Request for Proposal issued in September ‘05.
- Request for Tender issued in January ‘06.
- Optus/AlphaWest/Nortel/Mercury consortium selected April ‘06.
- Installation commenced in July ‘06, and was largely complete by February ‘07.

Request for Proposal

- 100% wireless coverage.
- Differentiated Access by user/device.
- Differentiated Service (QoS).
- Authentication integrated with existing UWS ID/password databases plus support for EduRoam.
- Admission Control.
- Data encryption.
- Intrusion Detection/Prevention (IDS/IPS).
- Node identification/location/isolation.
- Admin/Management & monitoring tools.

RFP – Key Findings

- “Thin” AP technology preferred (cost, features & management) but currently proprietary.
- 100% coverage too expensive.
- Wireless IDS/IPS systems can be very expensive.
- Network Admission Control systems are independent of physical network system (wireless/wired).

Request for Tender

- Wireless LAN:
  - "Thin" wireless LAN system to teaching spaces, libraries, student residences, cafeterias only;
  - RADIUS-based authentication system;
  - Basic IDS/IPS (ie, rogue detection only);
  - Admin/Management;
  - Differentiated access & service.
- Admission Control System:
  - Policy server;
  - Admission Control Servers (in-band);
  - Admission Control Client.

Options, Compromises & Decisions

- Wireless LAN:
  - Equipment options: Cisco, Nortel, Aruba, Enterasys, Meru, Strix – all pretty good;
  - Design & Implementation: very variable;
  - Authentication/encryption models: 802.1X/WPA and VPN;
  - Basic IDS/IPS (Rogue AP detection/isolation) – standard for all;
- Admission Control:
  - Cisco Clean Access, InfoExpress CyberGatekeeper, Nortel TunnelGuard (VPN only).
  - Requires additional hardware/software.
  - (at the time) Cisco & Microsoft main players; neither part of the industry forum; zero product offerings from Microsoft; no agreed standards.

Optus/Nortel Solution

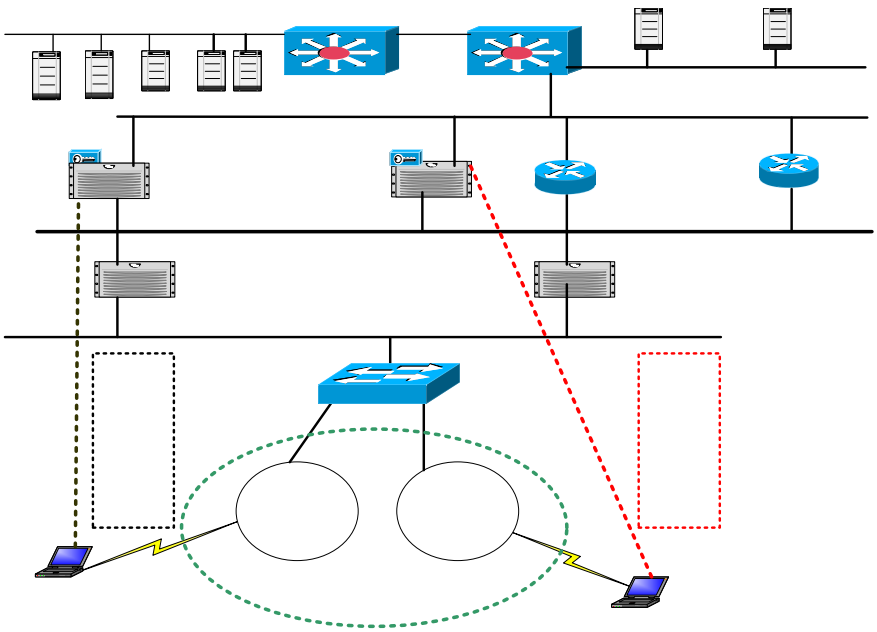
- Nortel equipment:
  - 2300 “adaptive” APs – mainly indoor;
  - 7220 “mesh” APs – mainly outdoor;
  - VPN-based security model:
    - Multi-platform support;
    - Included an admission control capability with no additional hardware;
    - Extensible to non-WLAN applications;
- Implementation by Mercury Solns (RF), and Alphawest (PM & PS).

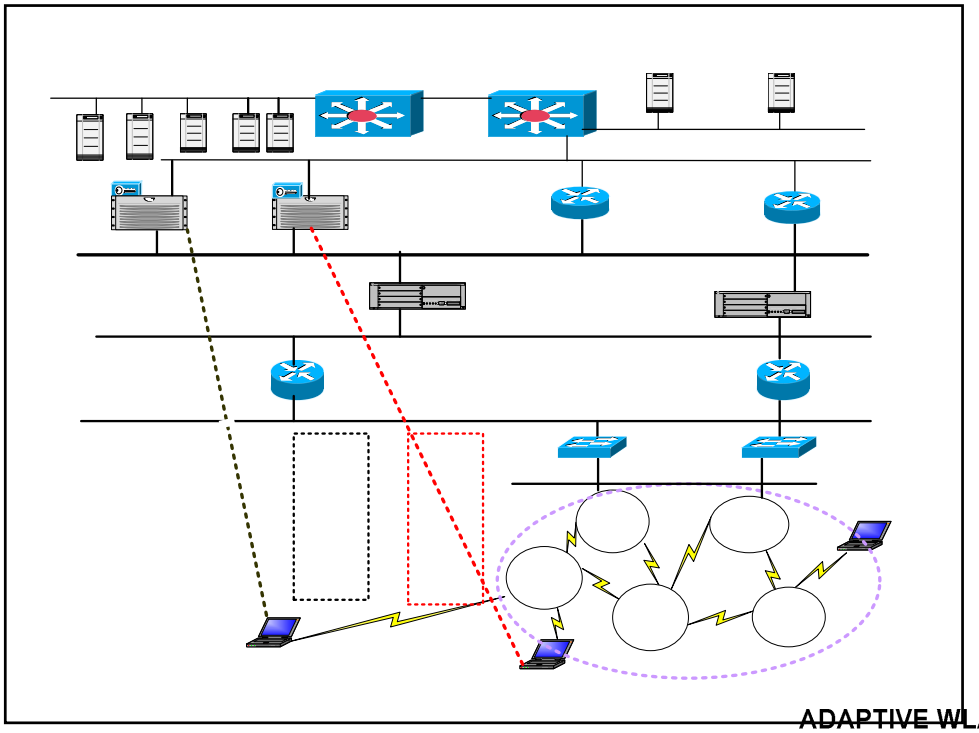
Differentiated Access

- What we wanted:
  - UWS-standard laptop to have full access and as close to “wired access” experience as possible.
  - Non-standard laptop to have restricted access.
- What we got:
  - Staff (like) users, regardless of equipment, have full access,
  - Student (like) users, regardless of equipment, have restricted access.

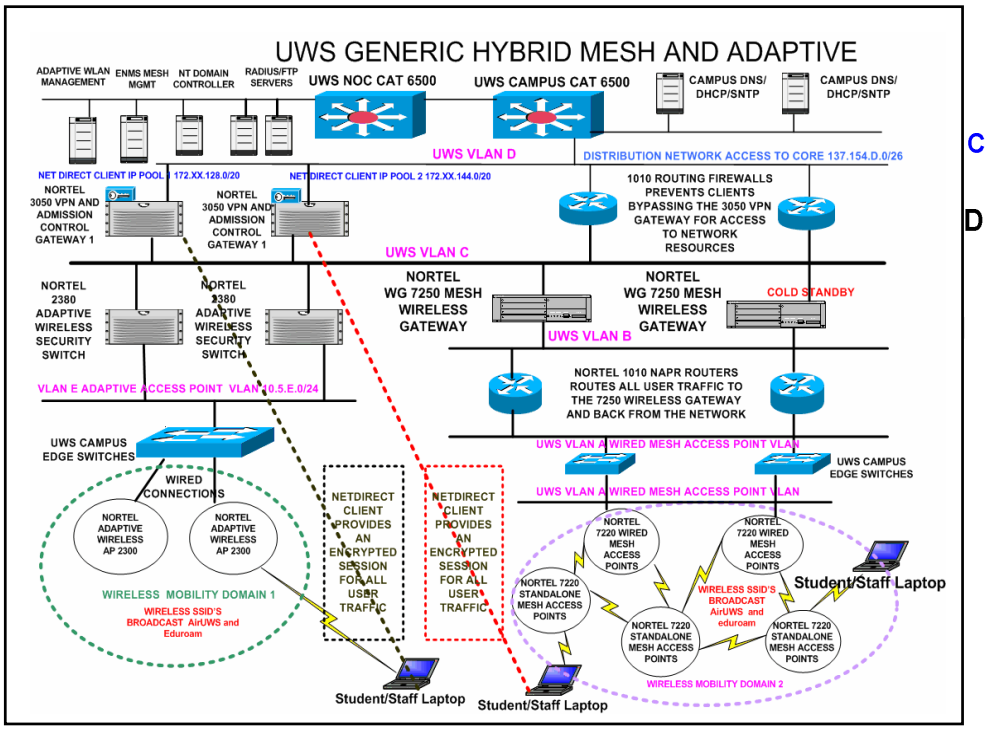
Client Software

- What we wanted:
  - Staff (like) users/devices – client software Ok.
  - Student (like) users/devices – no client software.
- What we got:
  - Java-based VPN and Admission control client for both.





ADAPTIVE WLAN MANAGEMENT ENMS MESH MGMT NT DOI CONTRO



CLIENT IP POOL 1 172.XX.1

D

3

Differentiated Access Summary

Type of user	Admission Control requirements	Access Control requirements	Access method on W2K, XP, MacOS 10, Linux	Authentication method	Encryption
Staff-like user	Strong	Weak	NetDirect	Captive Portal	SSL (terminating on 3050 from user device)
	TunnelGuard	3050 ACL		Uses LDAP	Used during authentication
				Between the 3050 and the Campus Windows domain Controller	
Student-like user	Weak	Strong	NetDirect	Captive Portal	SSL (terminating on 3050 from user device)
	TunnelGuard	3050 ACL		Uses LDAP	Used during authentication
				Between the 3050 and the Campus Windows domain Controller	
edu-person	N/A	Cisco/Firewall approach	802.1 x supplicant	802.1x, RADIUS	WPA/TKIP

Learnings

University of Western Sydney

- Adaptive WLAN equipment – great; mesh equipment works Ok – some issues with RF design and installation.
- Differentiated Access: Ok, but could be much better..
- Java-based VPN client generally Ok.
- No Mac/Linux version of TunnelGuard (admission control client) – but due any day.
- Team from Alphawest and Nortel – exceptional.

Over to Kim

UWS Wireless Logistics and Implementation

UWS installed:

- 61 outdoor
- 391 indoor access points across 6 campus precincts.

Each device required:

- Power either 48vdc or 240vac
- Network connectivity (not every outdoor device required physical connection).

Key aspects to implementation

- RF Survey

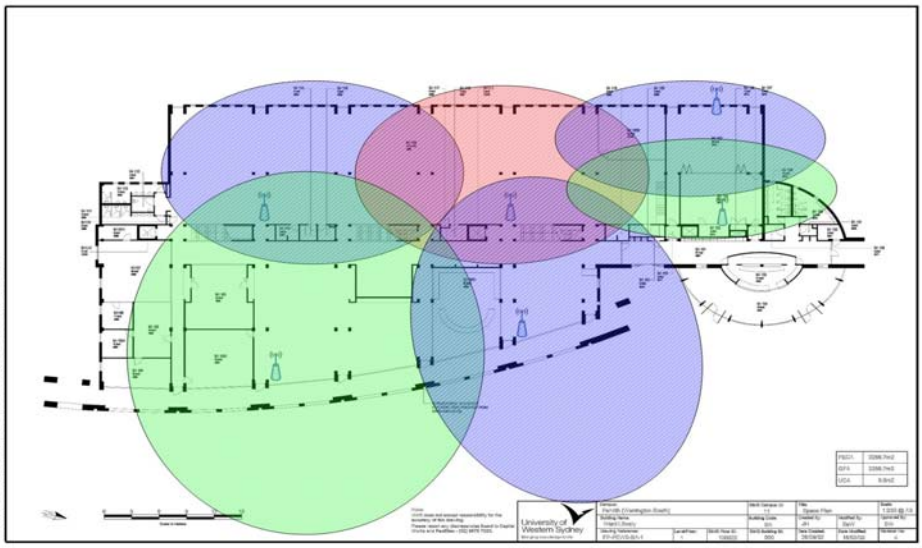
You need to understand your environment, existing sources of RF interference and how RF will behave such as penetration to surrounding areas, attenuation etc.

Do not let any vendor tell you RF survey is unnecessary and their equipment will automatically auto tune power levels and frequency allocation – RUBBISH

RF Survey

- RF survey also helps determine optimum location and quantity of APs determined by no of expected users and desired throughput.
- RF survey help identify difficult areas in terms of access for cabling or installation
- Outcome of survey should be a report and series of plans depicting locations and recommended channel spacings, and identifying any interference issues.

Sample RF Survey Plan



Getting started

- UWS decided to build the backend first as it was going to take considerable time to cable and install the proposed no of APs.
- While the final design and beginning of the network layer 2 & 3 components was getting underway, a series of cable quotations for each campus were written and issued.
- This was very time consuming process requiring every proposed AP location be photographed – an audit on switches, available ports, power mdf/frame capacity, patch lead requirements both quantity and length and type (UWS uses Krone and Systimax) to be assessed

Indoor Equipment Considerations

- Placement of AP
- How many APs in a given location
- Powering and patching an AP
- Final installation and testing of an AP

Placement of APs

- All indoor APs are mounted on the ceiling or in some cases a wall. No attempt was made to hide them – main reasons ease of locating them, being able to see information lights, the same applied to the data outlet.
- It is a lot easier to mount on wood and gyprock than concrete – a consideration for physical placement (reduced cost in terms of conduiting and installation time).
- Try and maintain same polarisation where multiple APs are in close proximity.

Placement of AP

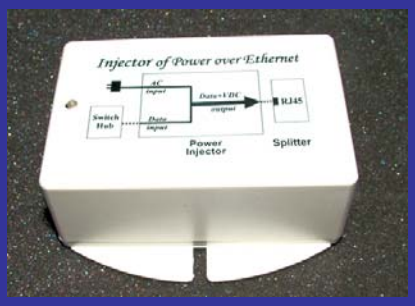
How many APs

- Our performance model allows for 20 users per AP
- In larger areas such as lecture theatres seating hundreds of people, we adopted a model of 20% of the population would uptake the wireless and installed APs on this basis.

- No of APs= (room capacity x uptake)/no users per AP
- Eg 300 seat lecture theatre
- No of APs = (300 x 20/100) / 20
  =3

We installed APs initially in the more difficult areas to access typically at the highest points in the specific room, leaving the more accessible areas to add extra APs as the need arises.

Powering APs



- Up to 3 APs connected to a network switch, individual power injectors are used.
- The power injector sits between the AP and the switch and uses two patch leads, one between the switch and the injector and the other between the injector and the data outlet .
- Each power injector requires a 240 volt GPO.

Powering APs

- For 3-5 APs connected to a network switch, a six port power injector is used. This is a 19 inch rack mounted device with a single power cord and presents a tidier solution, than individual injectors. The six port power injector, like the single sits between the AP and the switch and uses two patch leads per AP.

Powering APs

- For 6 or more APs connected to a network switch, power is provided by a Cisco POE switch. Only a single patch lead is required.
- UWS uses orange patch leads to denote wireless connections.

Installing and testing APs

- Installation work needs to be planned and scheduled particularly in Uni environment
- Our teaching hours are 8am -10pm including weekends – requiring shift work to be done in some campuses
- Test the AP before specialised equipment is taken away from site

High Lift Equipment?

- Check access paths
- Check doorway clearances
- Check lift dimensions – particularly load capacity – if necessary get a lift technician when moving EWP in lifts
- Check floor loadings – you may need a structural engineer to inspect your location and provide a safe working certificate or report – this also goes for outdoor areas on suspended slabs
- Find a safe parking area that has access to power
- Do an OH&S risk assessment before you start, involve your properties and OH&S teams, and get a work method statement – it's a lot easier than a government agency inquiry after an incident.

Lack of planning

Outdoor APs

- Require power
- Some require network connectivity
- Signage – RF warning
- Mounting Hardware
- Access to AP firmware for non network connected APs.
- Alignment – vertical and horizontal

Typical Outdoor AP

- UWS and contractors came up with a universal bracket system to suit most applications
- All outdoor APs have a 25 meter cable to an accessible point to allow diagnostics via laptop

Lessons learned

- Don’t underestimate the time required to plan, install and document.
- Insist on work plans and review regularly – involve other areas of your business
- Do a proof of concept first testing every conceivable device you are likely to use Mac PC different O/S.
- Don’t be afraid to get up on roof tops and look around
- Have more of everything than you think you need i.e. patch leads POE

How did it go

- Overall very well
- Strong commitment by all vendors
- Positive response from students and staff
- Outstanding efforts by Optus Alphawest Nortel Air Communications Consortium

University of Western Sydney

Questions?