Oxford University

Wireless networking

Roger Treweek

Oxford University Computing Services

Why Wireless?

- Being sold as
  - Any time, any place, any how
  - Even on a mountain side?

- However
  - You do need an access point nearby
  - And, potentially, lots of them

Why Wireless?

- There are some obvious locations
  - Lecture rooms
  - Libraries
  - Hard-to-wire areas
- Or for specific reasons
  - Conferences
  - Meetings
  - Mobility

Wireless Problems

- Security – out of the box product is insecure
- Privacy – snooping – passwords, data
- ‘Hub’ style operation – anyone can see all traffic
- Hacker tools readily available
- Performance

Wireless Technology

- 802.11b
  - 2.4Ghz, 11 Mbps
- 802.11g
  - 2.4 Ghz, 54 Mbps
- 802.11a
  - 5 Ghz, 54 Mbps

802.11b

- Wi-Fi standard
- Most common
- 2.4 Ghz spectrum is crowded
- 3 non-overlapping channels
- Limited users per access-point

802.11g

- Uses same 2.4Ghz spectrum as 802.11b
- 3 non-overlapping channels
- 802.11b card usage reduces throughput
- Same coverage
- More users per access-point

802.11a

- Uncrowded spectrum – for now!
- 8 non-overlapping channels
- Reduced coverage area
- More users per access-point

Data Rates

	Data rate (Mbps)	Throughput (Mbps)	Throughput (%802.11b)
802.11b	11	6	100%
802.11g (+ 802.11b)	54	7	117%
802.11g	54	22	367%
802.11a	54	25	417%

Ranges

Data rate	802.11a	802.11g	802.11b
54	45ft - 13m	90ft - 27m	
36	65ft- 19m	100ft - 30m	
18	110ft - 33m	180ft-54m	
12	130ft - 39m	210ft-64m	
11		160ft-48m	160ft-48m
6	165ft- 50m	300ft - 91m	
2		270ft-82m	270ft-82m
1		410ft-124m	410ft-124m

Site Survey

- Site survey is recommended
- Use same make/model as it is intended to employ
- Consider main coverage areas
- Number of access-points & location
- Interference issues
  - Channel allocation
  - Power settings

Security

- Wireless access is insecure
- It is ‘in the air’
- No respecter of boundaries
- Hacker tools freely available
- Clear text transmission
- Anyone can use

Security

Three areas to consider

- Authorized users only
- Encrypted transmissions
- Accountability of usage

Authorized Users

- Username/password required
  - 802.1x
    - IEEE standard
    - Uses EAP to provide variety of authentication methods eg RADIUS
  - WPA
    - Wi-Fi Protected Access
    - May be a container to 802.1x
    - Changes due this summer
  - 802.11i
    - Due to address further issues

Authorized Users

- MAC address
  - Scaling / management issues
- Gateway
  - VPN
  - Captive portal

Secure Transmission

- WEP – Wired Equivalent Privacy
- WPA uses rotating keys
- VPN
- Secure protocols only – ssh, ssl etc

Accountability

- Important to be able to track usage
  - Harder to trace than for wired connections
  - Identification of compromised machines
  - Cease-and-desist notices
  - ‘Illegal’ or harmful activity

Connection Options

- Three main options used
  - VPN
  - 802.11x, WPA
  - Gateway
- Use may be determined by type of user

VPN

- Users connect to private network
- Only allowed access to VPN server
- User authorisation by server
- Encrypted connection
- Logging by server

802.1x, WPA

- 802.1x
  - User authorisation before any access
  - Choice of authorisation method
  - No encryption
- WPA
  - Uses 802.1x
  - Key changes for encryption
  - Changes due

Gateway

- Usually web page for authorisation

- Bluesocket
  - Commercial but popular in uk academia
  - Lots of features
- NoCat
  - open source

Types of Users

- Staff
- Students
- Visitors
  - Meetings
  - Conferences

Staff

- Members of the University, long term use
- VPN possible
- WPA possible
- MAC & WEP
  - If small group
  - Secure protocols used

Students

- Like staff, university members, long term

- VPN
- WPA
- Gateway?

Visitors

- Hardest group to handle!
  - One day only
  - Conference attendees
  - Limited periods eg week, month etc
  - Not university members
  - May be at short notice

Visitors

- Cannot use VPN
  - May need VPN to access home site
- Gateway is most common method
  - Especially if very short term
  - Pre-created accounts
- 802.1x, WPA
  - For longer term visitors?

Rules and Recommendations

- OUCS have published current thinking
- Approved by ICTC
- Typically used at other sites

- Rules / Requirements
- Recommendations / Guidance

- http://www.oucs.ox.ac.uk/network/wireless

Rules

- Only authorised networks allowed
- Must be registered with OUCS
- Must be separate from any other network
- User authorisation required

Rules

- Strong data encryption must be used
- Clients must not offer services that compromise security
- All associations must be recorded

Recommendations

- 802.11b standard supported
- Wi-Fi approved equipment should be used
- Only IP should be used
- Use minimum necessary power levels

Recommendations

- Pick your channel allocations
- High bandwidth applications should not be used

OUCS Pilot

- Early days
- Testing various options
- Aim to produce standards
- Central vs Unit based schemes

Conclusions

- Not a substitute for wired connections
- Security is paramount
- Changing marketplace

Any Questions?