Surveying

Surveying should be used at three different stages in the deployment of a wireless network.

- ?n initial survey should be done at the planning stage to determine where access points should be located.
- ?nce the installation is complete, a survey should be done to confirm that the performance is as expected.
- Periodic re-surveys should then be done to check for changes in the wireless environment: i.e. new sources of noise or attenuation or additional access points appearing. A re-survey may also be required if problems are reported: if this suggests that changes to existing access points or additional access points are needed then a further planning and post-installation survey should be performed.

Although each type of survey is likely to use the same equipment, each uses different information and has different aims, as described in the following sections.

Planning

The first stage in planning a wireless network should be to list, and mark on a copy of the floor plan, the areas where good wireless coverage is a priority. Even if the aim is to have coverage throughout the building, there will be some areas such as corridors or storerooms where a lower level of performance is acceptable. Given the constraints on channels, particularly in the 2.4GHz band used by IEEE 802.11b and 802.11g, achieving optimum performance everywhere is unlikely. Priority areas will probably depend on the motivation for installing the wireless network. In some cases they will include meeting rooms or other areas where visitors will congregate; in others the offices of senior staff will be the highest priority.

Once the priority areas have been identified, look for places nearby where it will be easy to install an access point. This will require a connection to the wired LAN and also a source of power. Some access points can take their power from the Ethernet connection: though these are likely to cost more than devices with separate power points, they may well be cheaper in total once the alternative of providing extra mains sockets is included. Access points also need to be physically secure – loose laid access points have proved tempting to casual thieves – but security fastenings must be chosen carefully to avoid interfering with the radio signal.

One access point is then needed: for accurate predictions, this should be the same type as it is planned to use in the installation. This should be placed in the first priority location and turned on. No network connection is required at this stage of surveying, just mains power, so a long mains extension may be useful. The signal strength, noise level and signal/noise ratio should then be measured, using whatever measurement tool has been chosen, at a number of points around the access point. In particular, coverage should be checked in those priority areas that are within range. Elsewhere the aim should be to identify the points where the

available bandwidth is likely to drop below the theoretical maximum: typically where the signal strength falls below -70dBm or where the signal/noise ratio is less than about 15dB. Drawing a line through these points will create a rough contour map of the wireless coverage. The access point should then be moved to the next priority area that was not adequately covered from the first position and the process repeated until all the required areas have been covered.

During the planning survey it may be useful to note areas where there are high noise levels, as well as the channel number and SSID of any wireless signals that are already present in the area, since these are likely to constrain the installation unless they can be removed. If possible, note any features that are likely to be temporary and where a later re-survey may give different results. One site found that scaffolding erected by painters made their initial survey of the area almost useless.

Wireless signals are likely to leak out of most buildings. This can be checked as a matter of information at the planning stage; however, a determined attacker who can choose his own receiving aerial is likely to be able to pick up a signal from any building that is not specifically designed to screen radio transmissions. Wireless networks that are not intended to be open to the whole world need to be protected by encryption and authenticated access (see Reference 12 [1]), not by relying on signals to be contained within a physical structure.

The result of this pre-installation survey should be a series of locations where access points are needed, together with a map of the areas covered by radio signals from each of them. The next stage in planning is to allocate frequencies to the planned access points, using the map to ensure that frequencies do not overlap. If this is not possible then it may be necessary to remove one or two planned access points and move others to maintain adequate coverage. If a small but high-priority area causes overlap problems then it may be possible to provide a dedicated access point with a reduced transmission power strength (most access points have this as a configuration option), possibly in combination with a directional aerial to shape the area of coverage to that required.

Post-Installation

Once the access points have been installed according to the plan, a post-installation survey should be performed to check that the network is operating as predicted. This should be done by walking round the area, and in particular the identified priority areas, recording the signal strength, noise level and signal/noise ratios. These values should be recorded on a second copy of the map, and kept for comparison with future re-surveys.

Since the aim of the post-installation survey is to ensure that users are satisfied with the performance of the network, it is useful to test the network as users will experience it at various points around the building. This can be done by simply noting at different locations the network bandwidth as reported by the wireless connection properties on a laptop, or by running some typical user applications, such as web browsing or VPN connections, and checking that performance is acceptable. If real network applications are used, these should be chosen so that their performance depends on the wireless LAN with the effects of other networks and servers reduced as far as possible. Ideally the applications should be accessed from a lightly-loaded local server, otherwise there is a risk that the tests will actually record wide area network performance or server load.

Re-survey (Fault Finding and Rogue Access Points)

The wireless LAN should be regularly re-surveyed, ideally at least monthly, to ensure that it continues to provide good service. Re-surveys may also be required if users report problems, though in this case it may be possible to concentrate the survey in a particular area. Planned changes to the wireless equipment, such as hardware or firmware upgrades, should also be followed by a re-survey to confirm that they have not affected the service in unintended ways. Re-surveys should be performed at times of year and day when the network is being actively used, since the aim is to identify problems that may affect real users.

The aim of a re-survey should be to identify any changes from the original post-installation survey, so it should be carried out in the same way as the original. In particular the re-survey should seek to identify:

- new or changed sources of wireless noise
- new or changed areas of high signal attenuation
- new access points that may have appeared since the original survey.

New noise sources will usually result from new equipment that has been installed or switched on since the original survey. These should be obvious when maps of the radio noise level from the original survey and the re-survey are compared. New noise sources will often be unavoidable: the best that can be done is to try to get warning of any changes and to influence their design or location to have the least effect on the existing wireless network. A noise source is likely to reduce the performance of the wireless LAN in the area around it. While it may be possible to counteract this by installing a new access point, there may be no channel available that will not disrupt the network in adjacent areas. In the worst case, a strong source of radio frequency noise may make the area around it unusable for wireless networks.

Changes to signal attenuation are more likely to arise from changes of use to parts of the building, and should be apparent when comparing past and present maps of signal strength. Information from the commercial sector suggests that tanks of tropical fish can significantly alter wireless coverage: in the education sector, ranks of metal filing cabinets, paper stores or bookshelves are perhaps more likely sources of problems. Changes to the structure of the building may also change signal attenuation, for example if reinforced fire doors are installed. Changes to signal attenuation should be easier to counter than new noise sources since, by definition, they should reduce the interference from other radio signals; however, there may still be problems finding an appropriate channel if a new access point has to be installed.

Wireless access points are cheap and easy to connect, and academics and students have proved very willing to install their own unofficial wireless networks by simply buying an access point or Apple Airport and plugging it in to a network socket. Unexpected types of equipment, including integrated audiovisual systems and fruit machines, have been found to contain built-in access points. Such rogue access points are likely to choose channels at random and can severely disrupt the carefully planned channel allocation of the official wireless network, as well as cause serious security problems by allowing unrestricted access into the organisation’s internal network. There is no technical way to prevent rogue access points appearing: the best that can be done is to adopt a policy that gives the organisation the right

to control all use of wireless LAN devices within its premises (see for example the Sheffield University Wireless Network Base Station Connection Policy, Reference 11 [2]) and to detect rogues as soon as possible by monitoring and re-surveys. In most cases, rogue access points are set up by individuals who are either dissatisfied with the official service or do not know that it exists, so publicising the official service and resolving problems with it may well be the best preventive measure. A number of universities have policies and processes that allow departments to fund their own access points as part of the official service: these have been highly effective both in extending the wireless service into new areas and reducing the number of rogue access points that appear. The ability to join a campus-wide wireless network appears to be sufficient benefit that departments will accept increased technical and management requirements on the access points they buy.

Wireless signals may also arrive from access points in adjacent areas. In many buildings, transmissions from an access point are likely to penetrate at least one floor or ceiling. This can be an advantage where the whole building is occupied by the same organisation, in that the number of access points needed to cover all floors may be reduced, but it can make surveying and tracing the source of signals more complicated. Where signals arrive from other organisations, either above or below or in adjacent premises, these are likely to be more of a problem and are best resolved by negotiation, perhaps pointing out the privacy issues of transmitting at full power.

A more serious problem in future may be malicious rogue access points, set up to masquerade as the official network in order to steal information or user passwords. Users should be educated in how to distinguish between a genuine network and a rogue (see the Janet factsheet Safe Use of 802.1x Wireless Networks [3]) and to report any suspicious activity. Malicious rogues have been discussed extensively in the press: if they become a common problem then they will require more frequent surveys or automated monitoring systems to detect and locate them.

Commercial survey and mapping tools will often automatically identify changes in wireless signals between past and present surveys, and may be able to suggest how to re-design the network around them. For example the Ekahau tool can subtract the signal from known access points to leave the location of a rogue access point very plain (Figure 14).

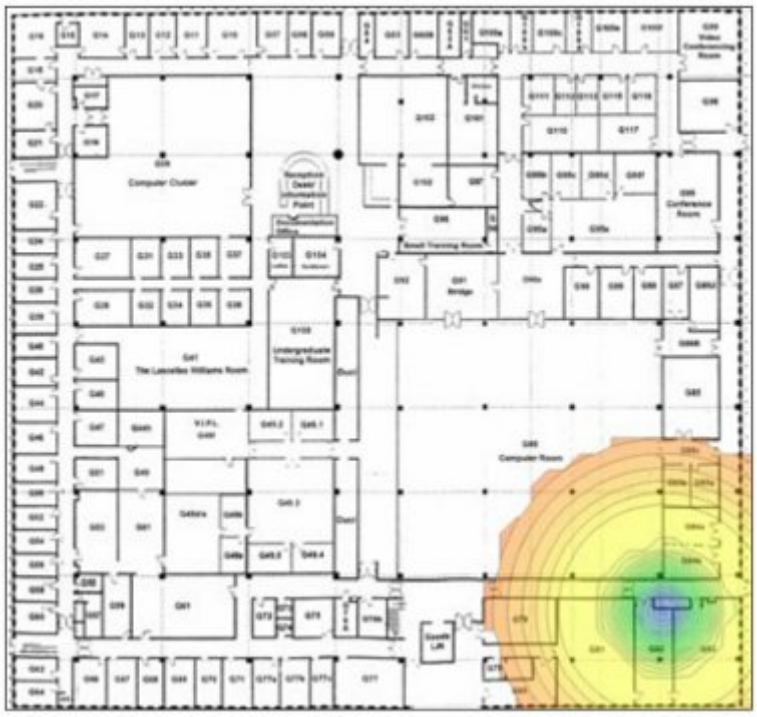
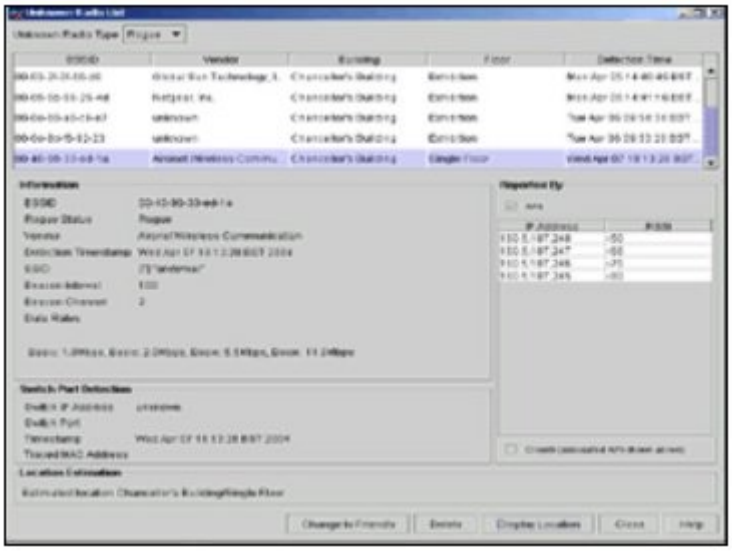

[4]

Figure 14: Rogue Access Point Detected by Ekahau Site Survey™.

Continuous monitoring systems such as Cisco®'s WSLE, where access points record each others' signals, can immediately detect the appearance of a rogue access point and give an


s signal as measured by access points

[5]

Figure 15: Cisco® WLSE Alert for Rogue Access Point.

Different systems offer a variety of alerting and diagnostic tools to help identify and locate new access points.

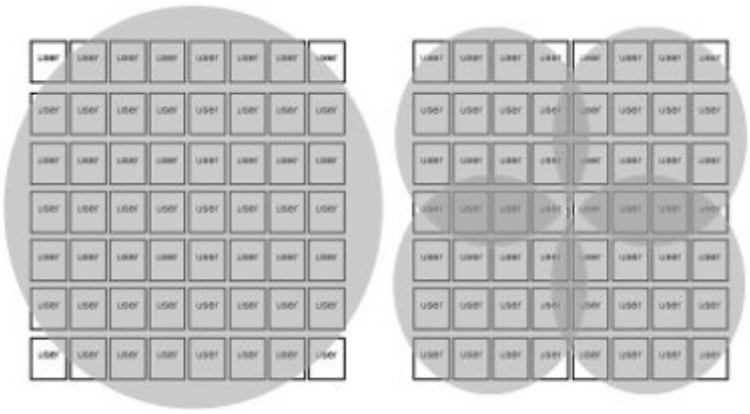
Other Techniques

Reduced Power

Most access points transmit at a power of 100mW (20dBm). Many allow this power to be reduced as part of the confi guration. Although it may seem strange to reduce the area covered by an access point deliberately, there are situations where this may be useful; for example, to fi ll in small gaps in wireless coverage or to increase the density of access points in a given area.

Some buildings may have areas where it is important to provide wireless coverage but where a signal cannot be obtained from the existing installed access points. In this case it may be possible to provide a dedicated access point close to the area, but using a reduced transmitter power to avoid conflicts with signals from adjacent access points. Such installations are likely to require some experimentation to achieve the right balance of local coverage and lack of interference: the same survey techniques should be used to map both coverage and interference at different transmit powers. Normally the access point should be configured to the lowest power that gives acceptable performance in the area of interest.

The nominal 11Mbit/s or 54Mbit/s bandwidth available from a single wireless channel will be shared among all the users who connect to the same access point and channel. Where a large number of users are expected in a small area, for example in a conference hall, a single channel may not provide sufficient bandwidth for all the users in the 30m diameter circle around the access point. In these circumstances it may be possible to increase the total bandwidth available by installing a large number of access points, each transmitting on a reduced power. The intended effect can be seen by comparing the two diagrams in Figure 16, which shows how halving the range of each access point and increasing the number can, in theory, reduce the number of people sharing an access point and quadruple the total available



[6]

Achieving this in practice is likely to require a great deal of experimentation and fi ne tuning of transmitter powers to achieve a reliable performance. Problems of interference and different amounts of signal attenuation are likely to be much greater in such a densely packed area. Since humans themselves can significantly attenuate wireless transmissions, tuning may well be required as people move into and around the space. High-density installations have been successful where sufficient support was available – for example, one IETF meeting was reported as having a grid of access points at 5 metre spacing across the ceiling of the

conference hall. However, these represent the limits of what wireless technology can do.

Links
[1] http://community.ja.net/library/advisory-services/references#12
[2] http://community.ja.net/library/advisory-services/references#11
[3] http://community.ja.net/library/advisory-services/safe-use-8021x-wireless-networks
[4] http://community.ja.net/system/files/images/wtas-surveying-tg-14.jpg
[5] http://community.ja.net/system/files/images/wtas-surveying-tg-15.jpg
[6] http://community.ja.net/system/files/images/wtas-surveying-tg-16.jpg