



# Surveying Wireless Networks

**Technical Guide**

## UKERNA Technical Guides

UKERNA Technical Guides are one of a series of user guides available to JANET customers. Technical Guides contain detailed technical information and are intended for technical support staff at JANET sites, network specialists, or those with a particular interest in the specialist area.

If you have any queries or comments about the Guide or would like to obtain copies, please contact:

JANET Customer Service

UKERNA

Atlas Centre, Chilton, Didcot

Oxfordshire, OX11 0QS

Tel: 0870 850 2212

Fax: 0870 850 2213

E-mail: [service@janet.ac.uk](mailto:service@janet.ac.uk)

Further details of the documents in this series are available at:

<http://www.ja.net/documents/>



---

# Contents

<b>Table of Figures</b>	<b>4</b>
<b>1 Introduction</b>	<b>5</b>
<b>1.1 Wireless Standards</b>	<b>7</b>
<b>2 Wireless LAN Basics</b>	<b>9</b>
<b>2.1 Wireless Frequencies</b>	<b>11</b>
<b>2.2 Signal Strength</b>	<b>12</b>
<b>2.3 Noise</b>	<b>13</b>
<b>2.4 Signal/Noise Ratio</b>	<b>14</b>
<b>3 Surveying Tools</b>	<b>15</b>
<b>3.1 Signal, Noise, S/N measurement</b>	<b>17</b>
<b>3.2 Maps</b>	<b>20</b>
<b>4 Surveying</b>	<b>23</b>
<b>4.1 Planning</b>	<b>25</b>
<b>4.2 Post-Installation</b>	<b>26</b>
<b>4.3 Re-survey (fault finding and rogue access points)</b>	<b>26</b>
<b>4.4 Other Techniques</b>	<b>29</b>
<b>4.4.1 Reduced power</b>	<b>29</b>
<b>5 References</b>	<b>31</b>
<b>Wireless LAN Basics</b>	<b>31</b>
<b>Papers on interpreting different measures of signal strength</b>	<b>31</b>
<b>Wireless Survey Tools</b>	<b>31</b>
<b>Wireless Policies</b>	<b>31</b>
<b>Other UKERNA Wireless Publications</b>	<b>31</b>

## Table of Figures

<b>Figure 1: Effect of Wireless Channel Overlap</b>	<b>11</b>
<b>Figure 2: Ideal Theoretical Allocation of Three Channels</b>	<b>12</b>
<b>Figure 3: Signal Strength versus Distance from Access Point</b>	<b>13</b>
<b>Figure 4: Cisco® Aeronet Signal Strength Meter</b>	<b>17</b>
<b>Figure 5: Netstumbler Listing Available Access Points</b>	<b>17</b>
<b>Figure 6: Netstumbler Signal Strength Graph</b>	<b>18</b>
<b>Figure 7: Kismet Listing Available Access Points</b>	<b>18</b>
<b>Figure 8: Kismet Showing Access Point Characteristics</b>	<b>19</b>
<b>Figure 9: AirMagnet® Diagnostic, Survey and Alarms Screens</b>	<b>19</b>
<b>Figure 10: Manual Survey Using Netstumbler</b>	<b>20</b>
<b>Figure 11: Ekahau Site Survey™</b>	<b>21</b>
<b>Figure 12: Cisco® WLSE Initial Map</b>	<b>22</b>
<b>Figure 13: Cisco® WLSE Map with Data from Laptop</b>	<b>22</b>
<b>Figure 14: Rogue Access Point Detected by Ekahau Site Survey™</b>	<b>28</b>
<b>Figure 15: Cisco® WLSE Alert for Rogue Access Point</b>	<b>28</b>
<b>Figure 16: Reducing Power to Increase Access Point Density</b>	<b>29</b>

# 1 Introduction

Wireless networks are a useful complement to a wired network, allowing network connections to be obtained anywhere within an area rather than only at fixed network connection points. However, wireless networks suffer from a number of problems that do not affect wired networks, in particular that the medium they use to transmit packets is a scarce resource subject to physical limits. Whereas the capacity of a wired network can be increased indefinitely by adding more cables, a wired network only has available a finite (and in some cases very small) number of frequencies. Since the frequency band they use is unlicensed, wireless networks must also compete with other users of the same radio band. They may also be subject to interference from accidental generators of radio frequency noise.

Wireless networks therefore need to be even more carefully planned than wired networks. They must take account of the surrounding environment to a much greater degree. Wireless surveys are a vital tool in planning and managing wireless networks: if a wireless installation is not based on a survey and supported by regular re-surveys then it is likely to provide a very unsatisfactory service.

This Technical Guide aims to provide all the information needed to perform wireless surveys and design networks around them. It begins with some basic information about wireless networks and their radio transmissions, then looks at the tools that are needed to perform a survey, and finally the processes of surveying and planning a wireless network.

Various tools, both free and commercial, are used as illustrations in the document. Mention of a particular tool should not be seen as a recommendation: these are merely the tools with which members of UKERNA's Wireless Advisory Group and their colleagues happen to be familiar. Thanks are due to the members of that group who have contributed to the document and also to the vendors who have provided screenshots and other information. Copyright in those images is held by Cisco® and AirMagnet® respectively.

## 1.1 Wireless Standards

The Guide is concerned with wireless local area network standards in the IEEE 802.11 family. A full list of these standards can be found in UKERNA's factsheet on Wireless 802.11 Standards (see Reference 13). The most commonly used standards, IEEE 802.11b and 802.11g, use the same frequencies in the 2.4GHz band and have the smallest number of separate frequencies available to them, so surveying is most critical when using these technologies. The same principles apply to the IEEE 802.11a standard; however, this uses a different frequency band, 5GHz, with more separate frequencies and, at the time of writing, fewer applications competing for the same frequencies. Surveying is still important for IEEE 802.11a, but the resulting installation plans are likely to be easier to work out.



## 2 Wireless LAN Basics

### 2.1 Wireless Frequencies

The IEEE 802.11b and 802.11g standards define a single range of radio frequencies from 2.412GHz to 2.472GHz that are to be used for wireless network transmissions. Within this range, thirteen frequencies are defined as channels, numbered from 1 to 13, with each channel separated from the next by a difference of 5MHz. Unfortunately the characteristics of radio transmitters mean that the signal for each channel is in fact 25MHz wide, so that the channels overlap. As shown in Figure 1, to avoid overlapping signals interfering with one another it is necessary to use channels that are at least five apart. Figure 1 shows that channels 1 and 6 can be used together without overlap, but they cannot be used at the same time as channels 2, 3, 4 or 5.

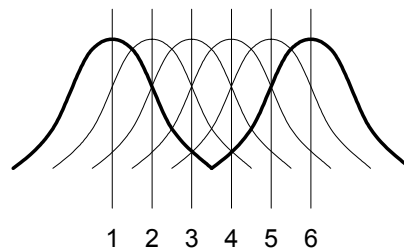


Figure 1: Effect of Wireless Channel Overlap.

If two access points transmit signals from the same or overlapping channels into the same area then their signals are likely to interfere, resulting in poor and unreliable reception. In practice this means that only three different channels can be used in any given area. The channels typically used are 1, 6 and 11. Channels 12 and 13 are not used in the USA so many laptops and other wireless devices will not recognise them. A Cisco® technical note has details of the radio spectrum used and the signals seen by users in overlap areas (see Reference 1).

The IEEE 802.11a standard uses a different range of frequencies around 5GHz but allows for eight to twelve non-overlapping channels, depending on country and product. Channel identifiers run from 34 to 64. To avoid overlaps in an 802.11a network, channels should be allocated that are at least four apart. Allocating channels for an 802.11a network should therefore be much easier than for 802.11b or 802.11g.

The restriction on channels applies to access points covering the same area, but also to access points covering adjacent areas. If the aim is to have complete wireless coverage throughout a building by providing multiple access points, then there will inevitably be places that receive signals from two or more access points. To avoid channel overlaps causing a poor signal in these areas, the access points must use different channels, again separated by at least five channel numbers (or four for 802.11a). Planning which access point uses which channel therefore becomes a map colouring exercise, with the requirement that no two adjacent areas are the same colour and, for 802.11b or 802.11g, that only three colours are available. As shown in Figure 2, if access points were placed in a regular grid with perfect transmission of radio signals from all of them, then three channels would be sufficient to cover an area with no overlaps. However, this ideal situation is only likely to be realised on a flat playing field, and certainly not inside a building where walls and furniture are likely to distort the areas of coverage and limit where access points can be located. Mathematical theory says that in some circumstances four different colours are needed to colour a map, so an ideal allocation of 802.11b or 802.11g channels may be impossible. In these cases it will be necessary to compromise on either coverage or performance.

To obtain consistent performance from a wireless network, each access point should be fixed to transmit on a single, pre-defined channel. Some types of access point offer a simple installation mode where the access point will choose a channel itself based on the other signals present.

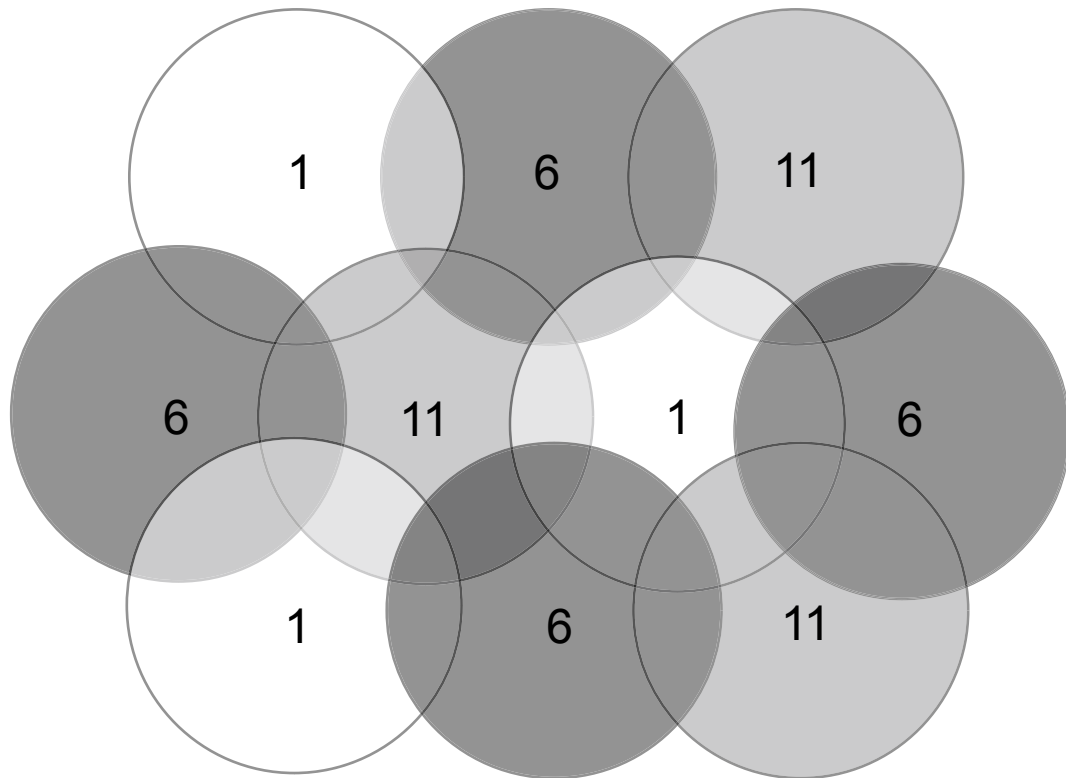


Figure 2: Ideal Theoretical Allocation of Three Channels.

However, this does not allow for human considerations such as areas where good performance is particularly important. The behaviour of such systems when new access points appear is also very uncertain. Automatic selection of wireless channel is therefore best avoided.

Fortunately it is only the access points that need to be configured to use a particular radio channel. Laptops and other wireless client devices will normally look for transmissions on all frequencies and select one without needing manual configuration.

## 2.2 Signal Strength

Like any radio or sound signal, a wireless network transmission gets ‘quieter’ the further you are located from the transmitter. The ‘loudness’ of the signal is measured as signal strength relative to some reference signal: for wireless LANs this reference level is usually 1 milliwatt. Because sensitive wireless cards can receive and use a signal that is a minute fraction of the strength at the access point, the logarithm of the ratio is usually quoted, rather than writing very long decimal fractions. The resulting values, in units of decibel milliwatts (dBm), can look strange at first, but with practice they are easy to deal with. Positive values mean the signal is stronger than the reference level; negative values mean it is weaker. A 1 milliwatt signal therefore corresponds to a value of 0dBm; the weakest signal that can be used by a typical IEEE 802.11g laptop card is -94dBm, but at this level the maximum data rate will only be 1Mbit/s. As the signal strength increases, so does the possible data rate, with the theoretical maximum of 54Mbit/s for IEEE 802.11g achieved by the same card at a signal strength of -71dBm (corresponding to about 200 times stronger than the minimum signal).

Signal strength decreases as distance from the transmitter increases, and hence so do data rate and sensitivity to noise. In the open air the signal strength from a normal 802.11g access point will usually drop to unusable levels at a distance of about 100m, with the data rate decreasing at distances more than about 30m from the access point (indoors these ranges are likely to be reduced by at least 20%). Typical bandwidths available at different ranges from an 802.11b/g access point are shown in Figure 3.

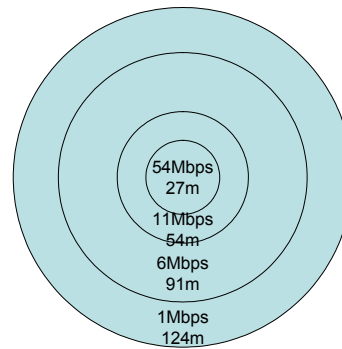


Figure 3: Signal Strength versus Distance from Access Point.

If there are materials other than air between the transmitter and the receiver (walls, ceilings, windows or even people or piles of paper) then these will reduce the signal strength much more quickly and hence reduce the effective range. A table of different materials and their effect on wireless network signals is available from Intel (see Reference 2).

The power of wireless transmitters is limited by law, so it is not possible to increase signal strength simply by increasing the transmitter power. However, it may be possible to address particular problem areas by using a directional aerial to concentrate the signal. Different types and positions of aerials on receiving equipment may also result in one client receiving a stronger signal than another. Laptops with receiving aerials built into a screen, and therefore perpendicular to the signal, are likely to perform better in areas of low-strength signals than those that use a PCMCIA card where the aerial is likely to be close to a human or desk that will be absorbing the signal. Client aerial differences are more likely to provide an indication of a problem than a solution to it: if an area suffers from low signal strength then the only permanent solution is to install another access point.

## 2.3 Noise

Not all radio transmissions are generated by access points, and those that come from other sources may sometimes drown out the wireless network signal. Radio frequency noise is therefore another area that should be checked during a wireless survey. Both the 2.4GHz band used by 802.11b and 802.11g and the 5GHz band used by 802.11a are unlicensed so many different types of equipment may transmit in these frequencies, either accidentally or deliberately. Other types of radio transmitter using the 2.4GHz band include cordless telephones and Bluetooth devices, while microwave ovens, RF lights and other electrical devices may also generate noise as a side effect of their operation. At present there is less competition for frequencies in the 5GHz band used by 802.11a networks but this situation is likely to change as other devices move into that frequency band.

Noise may also be generated by wireless networks themselves if their signals are damaged by the environment so as to become unusable. The most common cause of a wireless transmission being reduced to nonsense is multi-path reception, where a signal reaches the receiver by different routes (for example because it is reflected off a concrete wall) and interferes with itself. It has also been reported that panels of wire-reinforced glass in swinging doors can cause serious noise problems as they cause a rapidly changing diffraction pattern in the signal, while passing traffic outside a wall appeared to generate a rapidly changing pattern of reflections that reduced network performance.

The level of radio frequency noise in an area is measured in the same way as the signal strength, and with the same reference level, so is also recorded in dBm.

## 2.4 Signal/Noise Ratio

Obviously, if there is a high level of background noise then a higher signal strength will be needed. A particularly useful measure for identifying problems in a radio environment is therefore the difference between the wanted signal and the unwanted noise. No matter how strong the signal, if it is drowned out by a similar level of noise then the performance of the wireless network will be poor. Since the values used to measure signal and noise strength are logarithms, simply subtracting the noise level from the signal strength gives the signal/noise ratio. If the signal level is less than 10dB higher than the noise level (corresponding to noise a tenth as loud as the signal), then the data rate and the reliability of the wireless network are likely to be significantly reduced.

Although dBm are the correct engineering units to use to measure radio signal and noise levels, different wireless LAN devices may use other scales in an attempt to be more user-friendly. However these rarely give as much information as a dBm value. Web sites suggesting how to interpret these values are listed in References 3-4.

### 3 Surveying Tools

The basic tools for performing a wireless network survey are therefore a device that can measure signal and noise levels and calculate the signal/noise ratio, and a map of the area to record these values. Some survey tools are listed in References 5-10.

#### 3.1 Signal, Noise, S/N Measurement

Although it is possible to survey a wireless network using signal strength or signal/noise ratio alone, it will be much easier to trace problems if measurements of signal, noise and signal/noise ratio are available and recorded separately. If problems appear after a wireless network has been installed then it will be particularly important to determine whether these are due to a reduction in signal strength or an increase in noise level.

The most accurate tool for measuring radio signals is a dedicated radio frequency meter; however, results adequate for most purposes can be obtained using a wireless enabled laptop or PDA. Many of these come with a software application to display the current signal strength and noise level; for example, the signal strength meter provided with the Cisco® Aeronet® card is illustrated in Figure 4.



Figure 4: Cisco® Aeronet® Signal Strength Meter.

Other software applications may display additional useful information; for example the free Netstumbler program for Windows® shows the MAC address, wireless channel, protocol and (where available) SSID (service set identifier) of each access point within range (Figure 5). The Vendor field is derived from the first six octets of the MAC address, so it may be inaccurate for recently allocated addresses or where the access point allows its MAC address to be changed.



Figure 5: Netstumbler Listing Available Access Points.

Note that Netstumbler displays the current signal, noise and signal/noise ratio as well as the historical strongest signal (Signal+), weakest noise (Noise-) and greatest signal/noise ratio (SNR+). For surveying, these historical maxima and minima are the opposite of what is wanted: the weakest signal, strongest noise and least signal/noise ratio would be much more useful. For example the SNR+ value of 15 shown in Figure 5 might suggest that the network would be usable whereas the instantaneous value of 9 suggests that there are likely to be problems.

A better indication in conditions of poor reception can be obtained by Netstumbler's graph of signal strength and noise level for an access point (Figure 6). Here the low and fluctuating signal strength and the low signal/noise ratio suggest that the network service is likely to be unreliable at this distance from the access point.

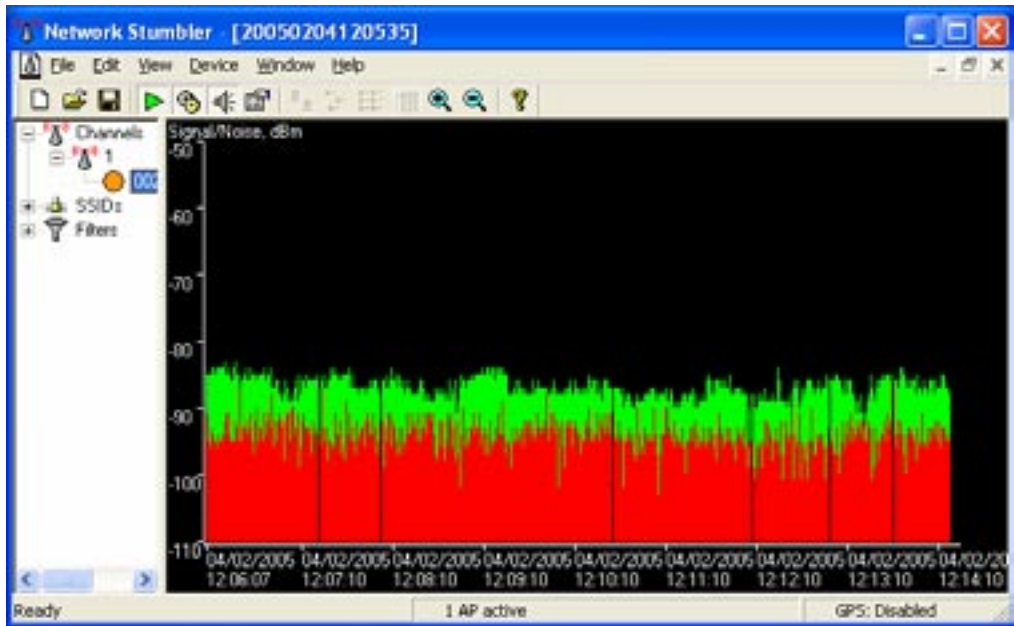


Figure 6: Netstumbler Signal Strength Graph.

A version of Netstumbler, called Ministumbler, is available for Pocket PC PDAs.

Wavemon and Kismet (Figures 7-8) are similar open-source tools for Linux® that can be used to list available networks, their signal strength and other characteristics. Kismet can also be used to capture packets and attempt to break WEP encryption keys: note that in the UK it

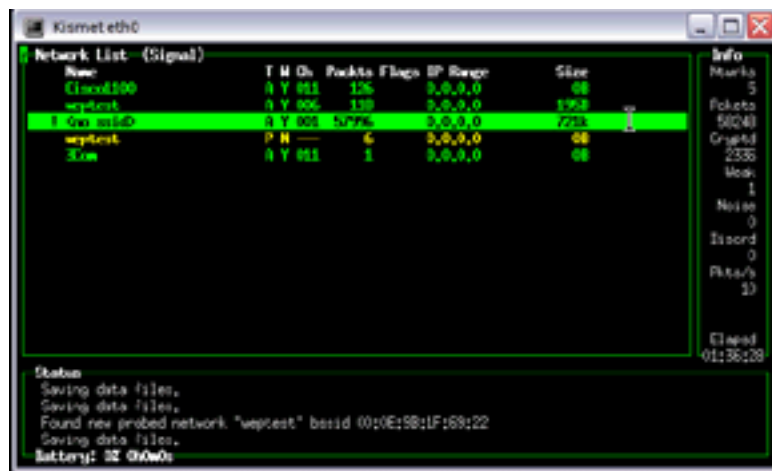


Figure 7: Kismet Listing Available Access Points.

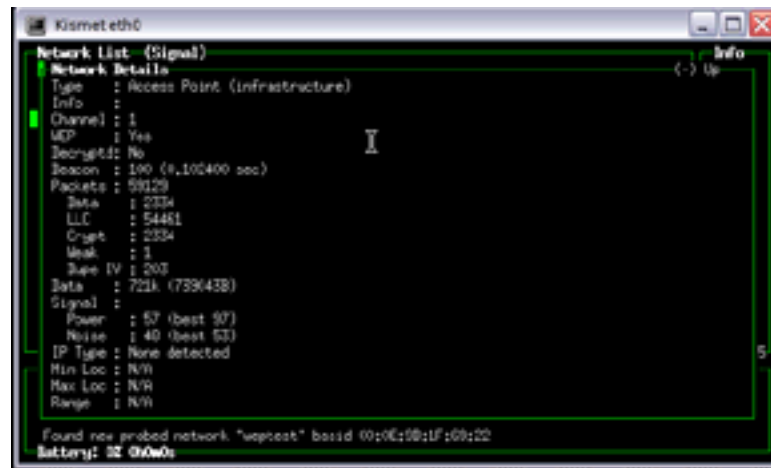


Figure 8: Kismet Showing Access Point Characteristics.

would be a serious criminal offence to do this without the authorisation of the owner of the network.

Dedicated wireless network survey programs exist, and are capable of interpreting values such as signal strength and channel number to identify possible problems quickly. For example the AirMagnet™ program runs on either a Windows® laptop or PocketPC PDA, and provides diagnostics for the process of connecting to a wireless network (Figure 9, left), warnings of potential security issues (Figure 9, right), and the normal signal strength and other measures (Figure 9, centre).



Figure 9: AirMagnet™ Diagnostic, Survey and Alarms Screens.

Whichever tool is used for the survey, the aim is to obtain values at points throughout the area covered by a wireless network for the poorest signal strength and highest noise level, to determine whether the performance of the network is likely to be adequate. When surveying with a laptop or PDA it should be used consistently, for example with the screen always open to the same extent and the same number of people around it (human bodies can significantly attenuate the wireless signal). However, at each point in the survey a number of different orientations should be tried to find the worst case signal. If you survey with your laptop carefully aligned to point directly at the access point, you can be sure that your users will randomly choose to sit in the worst possible alignment! For the same reason, when doing a survey, try to ensure that doors are shut, lights and equipment turned on, and the environment as hostile to wireless networks as it is likely to be in real use. If it is only possible to survey and install a wireless network when the building is empty during the vacation then adjustments are likely to be needed once people return.

### 3.2 Maps

The results of a wireless survey need to be related to the layout of the building. The easiest way to represent this is on a map. Floor plans of most buildings will exist somewhere: if there is no convenient electronic version then estates departments or site plans may provide a convenient starting point for copying. These may even give an early warning of likely sources of wireless noise (e.g. lift shafts and electrical plant rooms) or high signal attenuation (e.g. reinforced fire doors).

A wireless survey can be carried out using pencil and paper techniques, simply marking on the map the points where measurements were taken, writing in the signal strength or signal/noise ratio at each point and drawing rough contours of equal signal value by eye. This should certainly be sufficient to identify problem areas where there is either a high level of noise or a low level of signal. Figure 10 shows signal strengths measured using Netstumbler in an office area with two access points installed. The two dotted lines show the estimated boundaries where the signal strength from each access point drops below -70dBm – the level at which the available bandwidth is likely to be reduced. Throughout the area the noise level was found to be very low, below -95dBm, so the map of signal/noise ratio shows the same pattern.

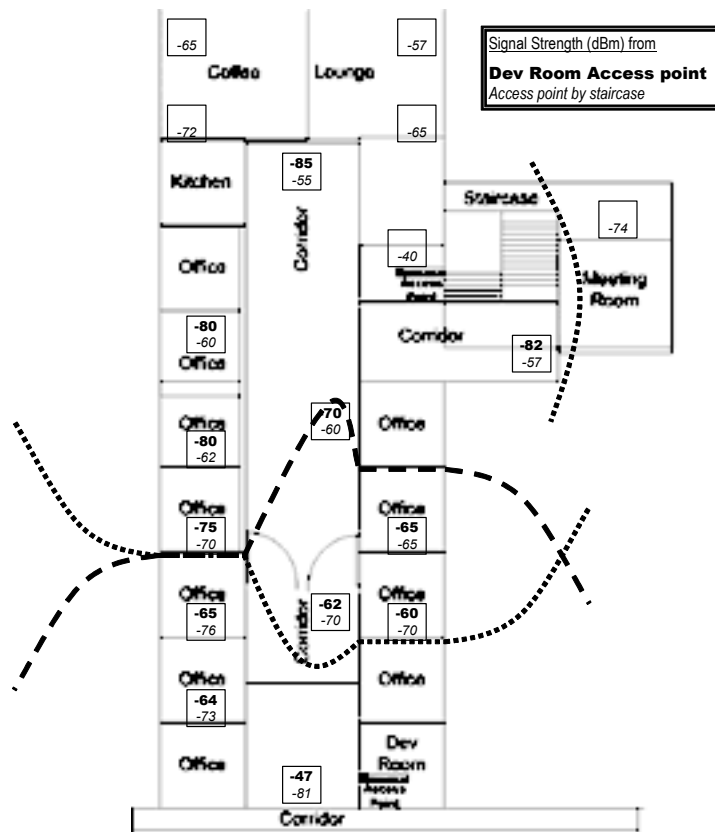


Figure 10: Manual Survey Using Netstumbler.

Even from this basic survey (which took less than 30 minutes) it appears that the offices on the left side of the corridor by the swing doors may suffer from reduced performance, as the signals from both access points are close to the -70dBm limit. If sufficient frequencies are available, these offices might benefit from an additional access point. The meeting room on the right hand side of the plan was not a priority area, so the low signal strength in that area was not considered to be a problem.

Alternatively, computer mapping software can be used to input a scanned version of the base map and the measured values to produce a more professional looking contour map. Remember, however, that a contour map cannot reveal information it has not been given: signal strengths

displayed in areas that have not actually been surveyed are at best a mathematical estimate and may be misleading.

Commercial software packages combine the data gathering and mapping processes; for example Ekahau's Site Survey™ program (Figure 11) collects information as the person doing the survey walks round the building. Each time the person clicks on their current position on the map, the software records the signal strength and other parameters of all access points within range. This allows the software to build maps of wireless coverage, noise, data rate and channel overlaps, as well as suggesting locations for additional access points to improve coverage.



Figure 11: Ekahau Site Survey™.

Cisco®'s WLSE (Wireless LAN Solutions Engine) (Figure 12) allows an even simpler approach, where access points listen to the signals from each other to establish a map of signal strength. Once the locations of the access points are identified by clicking on the base map and the map scale is established by entering a measured distance, the access points themselves can generate an initial map of interpolated signal strength.

This can only provide an estimate of the signal in the spaces between the access points, so the system allows additional data points to be collected from a laptop carried around the area of coverage to give a more accurate map (Figure 13).

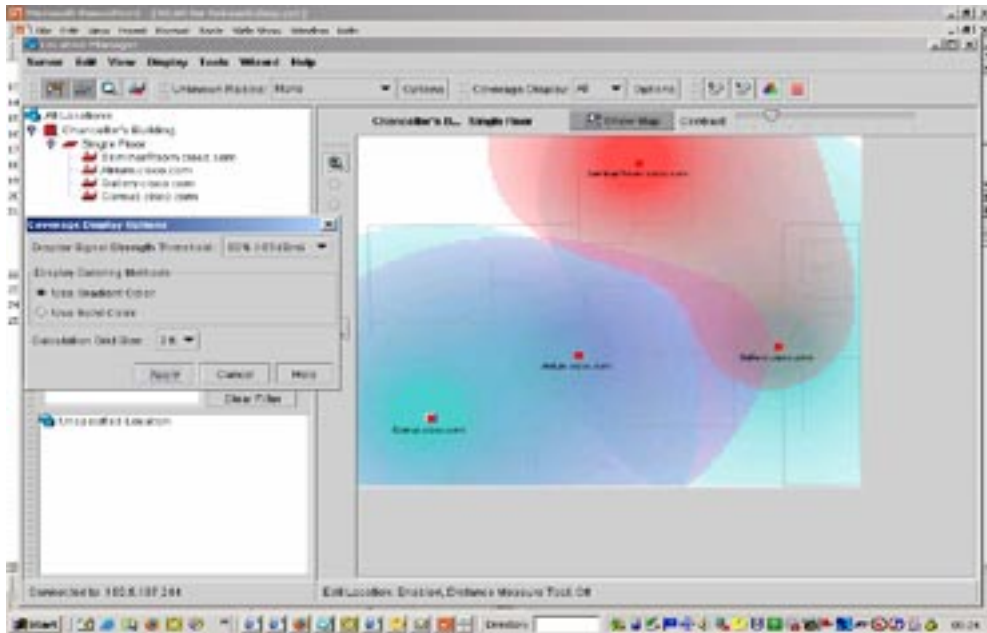


Figure 12: Cisco® WLSE Initial Map.

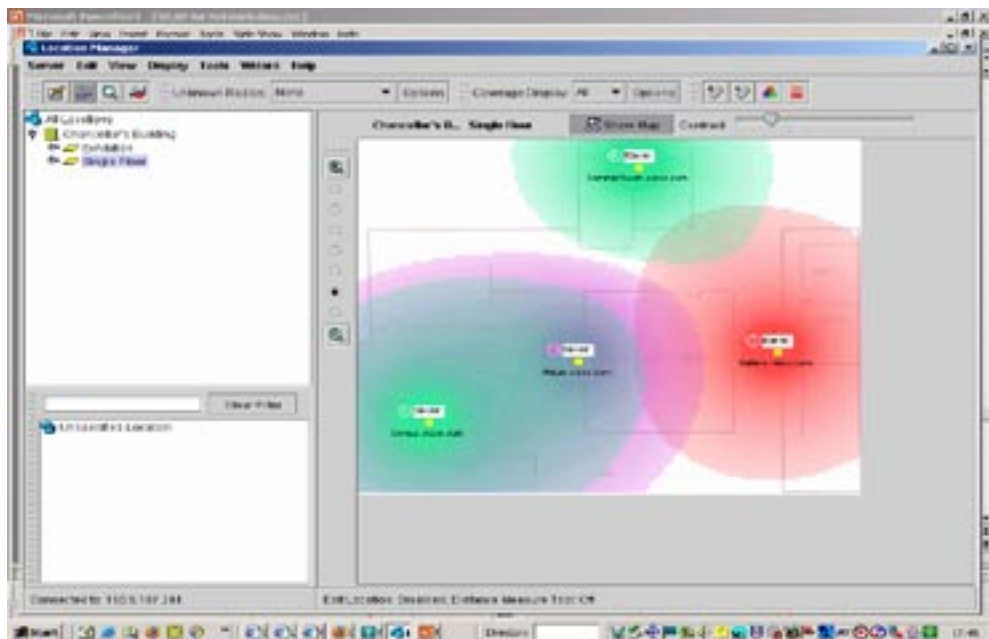


Figure 13: Cisco® WLSE Map with Data from Laptop.

## 4 Surveying

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

- An initial survey should be done at the planning stage to determine where access points should be located.
- Once 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.

### 4.1 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), 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.

## 4.2 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.

## 4.3 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) 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 UKERNA factsheet *Safe Use of Wireless Networks*, Reference 14) 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).

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 estimate of its location by comparing the strength of its signal as measured by access points in different locations (Figure 15).

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

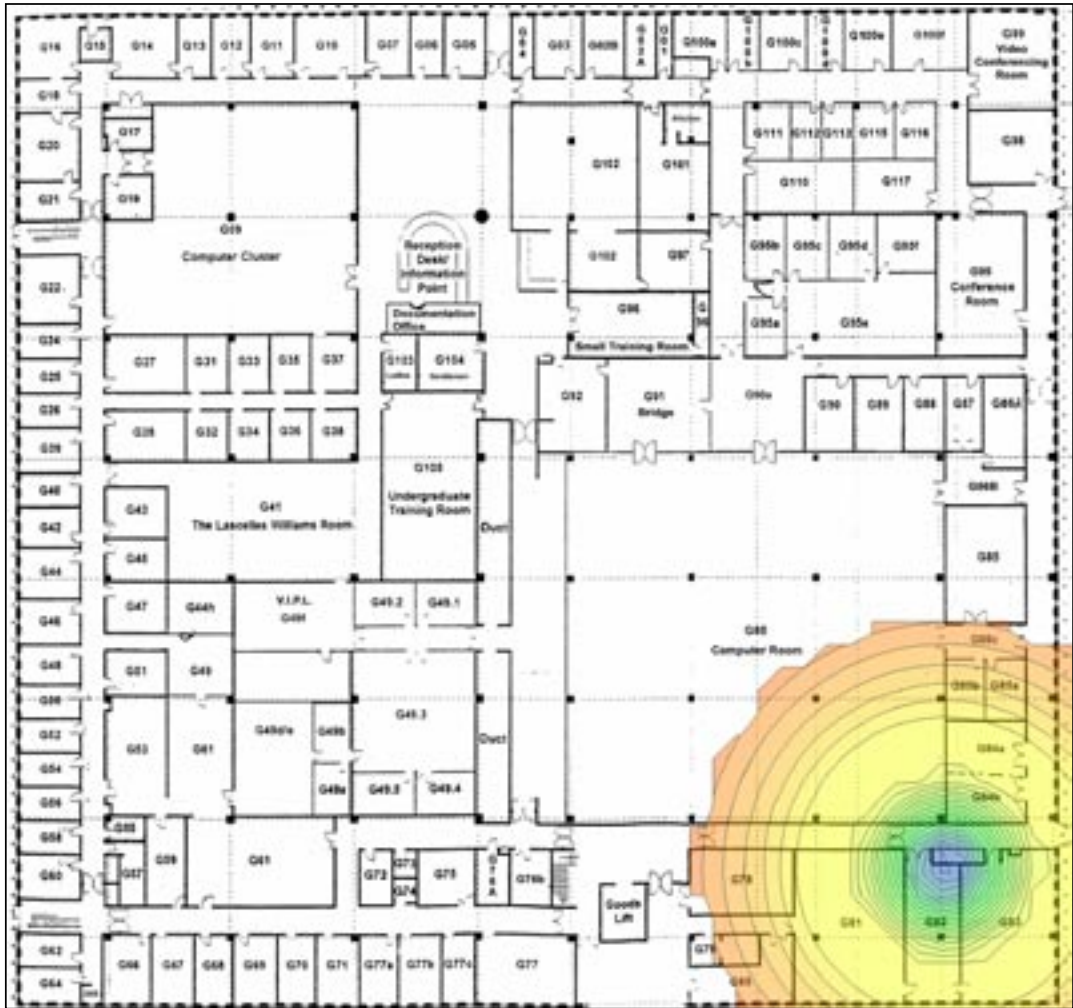


Figure 14: Rogue Access Point Detected by Ekahau Site Survey™.

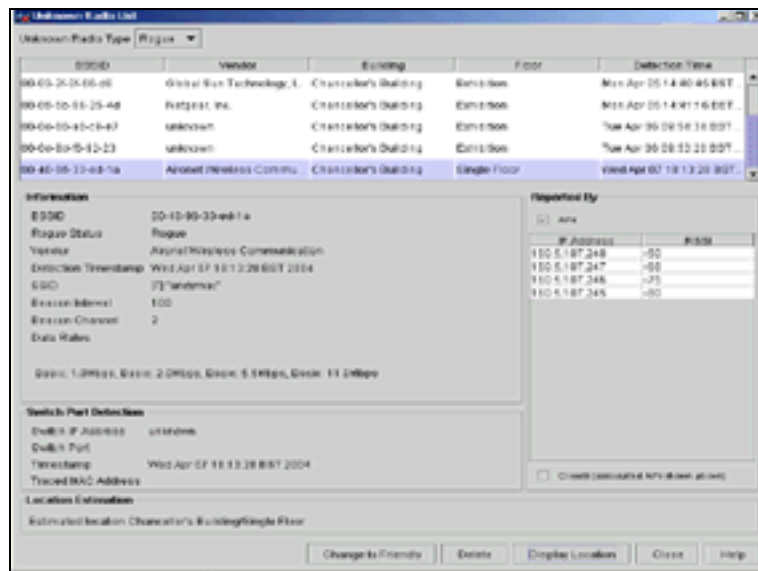


Figure 15: Cisco® WLSE Alert for Rogue Access Point.

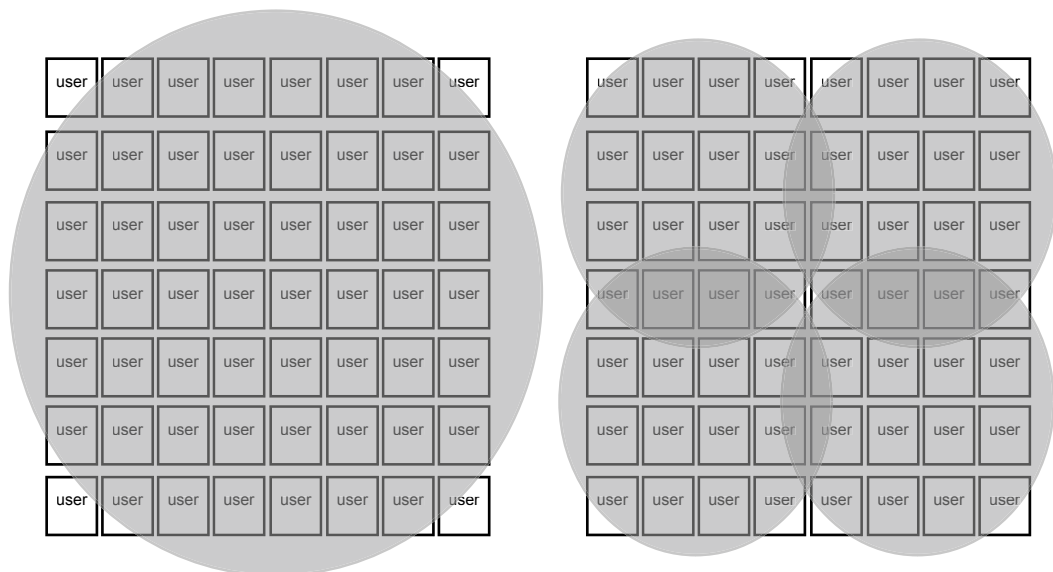
## 4.4 Other Techniques

### 4.4.1 Reduced Power

Most access points transmit at a power of 100mW (20dBm). Many allow this power to be reduced as part of the configuration. 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 fill 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 bandwidth.



*Figure 16: Reducing Power to Increase Access Point Density.*

Achieving this in practice is likely to require a great deal of experimentation and fine 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.



## 5 References

### Wireless LAN Basics

- 1 Cisco® paper on allocating channels without overlaps:  
[http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\\_technical\\_reference09186a00802846a2.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00802846a2.html)
- 2 Intel table of attenuation effects of different materials.  
<http://www.intel.com/business/bss/infrastructure/wireless/deployment/considerations.htm>

### Papers On Interpreting Different Measures of Signal Strength

- 3 WildPackets Inc. describe how to interpret the Receive Signal Strength Indicator values generated by various wireless cards at:  
[http://www.wildpackets.com/elements/whitepapers/Converting\\_Signal\\_Strength.pdf](http://www.wildpackets.com/elements/whitepapers/Converting_Signal_Strength.pdf)
- 4 Ohio State University interpret the signal strength values reported by Windows® at:  
<http://is.med.ohio-state.edu/Wireless%20FAQ.htm>

### Wireless Survey Tools

- 5 Ekahau: <http://www.ekahau.com/products/sitesurvey/>
- 6 Netstumbler/Ministumbler: <http://www.netstumbler.com/>
- 7 Kismet: <http://www.kismetwireless.net/>
- 8 Wavemon: <http://www.janmorgenstern.de/projects-software.html>
- 9 Cisco®: <http://www.Cisco.com/en/US/products/sw/cscowork/ps3915/index.html>
- 10 AirMagnet®: <http://www.AirMagnet.com/>

### Wireless Policies

- 11 Sheffield University Wireless Network Base Station Connection Policy  
<http://www.shef.ac.uk/cics/guidelines/wireless.html>

### Other UKERNA Wireless Publications

- 12 Wireless Security factsheet (for network managers)  
<http://www.ja.net/documents/factsheets/wireless-security.pdf>
- 13 Wireless 802.11 Standards factsheet  
<http://www.ja.net/documents/factsheets/wireless802.pdf>
- 14 Safe Use of Wireless Networks factsheet (for users)  
<http://www.ja.net/documents/factsheets/058-Safe-Wireless.pdf>

## Tell us what you think

Technical Guides are produced and published by UKERNA for use within the JANET Community. We welcome your comments on all aspects of this document and on any other UKERNA publication. Please direct feedback to JANET Customer Service, at the address below, or e-mail us directly at:

**documentation@ukerna.ac.uk**

UKERNA manages the networking programme on behalf of the higher and further education and research community in the United Kingdom. JANET, the United Kingdom's education and research network, is funded by the Joint Information Systems Committee (JISC).

For further information please contact:

JANET Customer Service  
 UKERNA  
 Atlas Centre, Chilton, Didcot  
 Oxfordshire, OX11 0QS

Tel: 0870 850 2212  
 Fax: 0870 850 2213  
 E-mail: service@janet.ac.uk

### Copyright:

This document is copyright The JNT Association trading as UKERNA. Parts of it, as appropriate, may be freely copied and incorporated unaltered into another document unless produced for commercial gain, subject to the source being appropriately acknowledged and the copyright preserved. The reproduction of logos without permission is expressly forbidden. Permission should be sought from JANET Customer Service.

### Trademarks:

JANET®, SuperJANET® and UKERNA® are registered trademarks of the Higher Education Funding Councils for England, Scotland and Wales. The JNT Association is the registered user of these trademarks.

AirMagnet™ is a trademark of AirMagnet Inc.

Apple® and Airport® are registered trademarks of Apple Computer Inc., registered in the U.S. and other countries.

Ekahau Site Survey™ is a trademark of Ekahau, Inc. in Finland and/or other jurisdictions.

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

The term 'Linux'® is a registered trademark of Linus Torvalds.

### Disclaimer:

The information contained herein is believed to be correct at the time of issue, but no liability can be accepted for any inaccuracies.

The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas such as internet addressing, and consequently URLs and e-mail addresses should be used with caution.

The JNT Association cannot accept any responsibility for any loss or damage resulting from the use of the material contained herein.

### Availability:

Further copies of this document may be obtained from JANET Customer Service at the above address.

This document is also available electronically from: [http://www.ja.net/documents/technical\\_guides.html](http://www.ja.net/documents/technical_guides.html)



© The JNT Association 2005

JISC

