

Wireless Networking

A computer network connects computers and associated hardware together, allowing them to share facilities and swap information. Traditionally they are connected with wires, now normally called Ethernet. However, it is now possible (and easy) to connect them wirelessly by using radio waves just like mobile phones, televisions and radios do. In fact, communication across a wireless network is a lot like two-way radio communication. Here's what happens:

1. A computer's wireless unit (a wireless network 'card') translates data into a radio signal and transmits it using an antenna.
2. A wireless router (the bit that connects everything together and perhaps to the internet) which often includes a broadband modem for the internet connection receives the signal and decodes it. It may send the information to the Internet using a physical, wired connection.



The process also works in reverse, with the router receiving information from the Internet, translating it into a radio signal and sending it to the computer's wireless adapter.

In order for the equipment manufacturers to make something that could be used by everyone, the IEEE (Institute of Electrical and Electronic Engineers) established a standard called 802.11 a/b/g/n. The letter at the end really means the speed that the system works at, with n being the fastest (and a working on a different frequency – so ignore it). The other wireless standard is Bluetooth. For more information see the links at the end of this paper.

There are numerous benefits in using a wireless network including portability, reduction in wiring costs (great for temporary projects), pretty easy to set up and add machines to and can save time and money saved if it is difficult to run wires into or around your building.



However, the disadvantages are that it can be slow (if you are sharing large amounts of data, but not normally for the internet), the signal strength can vary (due to interference), the distances computers can be apart is not great and they must be set up with security.

Costs of setting a wireless network up have come down considerably and the speeds they work at have gone up considerably but there are some simple points to help make your network better.

It is very likely that you are running old drivers and firmware on your wireless devices, so do the right thing and check the manufacturer's website to see if there are any newer versions. As well as the possibility of speeding things up and squashing the odd bug you may get some new features too.

It's best to use equipment from the same manufacturer so that there are no clashing idiosyncrasies.

Wireless networking uses a common, open frequency, 2.4 GHz. There are a number of other devices that use this frequency including Wireless Video Senders, Bluetooth enabled devices, DECT portable handsets, Baby Monitors, Microwave Ovens and other wifi networks. So make sure that you choose 'channels' which do not conflict. You can get some of this information by downloading a free program called [NetStumbler](#). The only non overlapping channels that 802.11b/g WiFi hardware uses are 1, 6 & 11.

It is really important to consider the best location for your access point to provide coverage across as wide an area as possible. Most people locate their AP near to the main phone point, for the majority of us though this is closer to the outside of the building than the centre. This will cause coverage problems in itself (as half the signal is going outside), so try to place the device in the middle of the building.

Walls block signals, especially thick ones. If your signal is having a problem getting through a wall, try using more directional antenna on the access point to direct the signal to the intended areas. You can also boost the received signal by adding a better antenna to your laptop card or desktop Wireless card. The antenna that comes with your device tends to be a stick like object. The signal radiates from it like a ripple on a pond with the stick in the middle, so point it accordingly.

If that doesn't help then in some cases you are just going to have to buy a few more access points. You can link these together using a 'powerline' type network device which is where you use your electricity sockets like network points. This technology has significantly improved recently.

In order to make you network secure make sure that it is encrypted. The simplest form is WEP. This is not very secure, but if you have new equipment there will be other options. One of the best things to do is to only allow named machines to be on the network. This means putting each computer's MAC address into the access point, or otherwise only allow fixed IP's to access the network.

If you want help with this, contact [Virtual Riders](#) (0845 337 2949).

For in depth explanations try:

<http://reviews.zdnet.co.uk/hardware/networking/0,39023970,10002769,00.htm>

http://guides.radified.com/magoo/guides/wireless/wireless_networking_01.htm

<http://www.ictHubKnowledgebase.org.uk/wirelessnetworks>

For a tutorial:

http://compnetworking.about.com/cs/homenetworking/a/homenetguide_2.htm

And for a list of what not to do.....

<http://www.pcfastlane.com/joomla/content/view/85/37/>