Wireless LANs – design and security

Operation of wireless local area network (WLAN) equipment is authorised by class licence under the Radiocommunications Act 1992. Equipment covered by a class licence is often described as operating in a ‘public park’, because all users operate in the same radiofrequency band and are subject to the same limits. Under the public park concept, use within the same frequency band is ‘uncoordinated’ and interference is avoided by the design of the equipment and by restricting power when operating the equipment.

Designing your WLAN

When designing your WLAN to operate in this ‘public park like’ frequency band, there are some things you can do to avoid interference. These measures will protect you and other users.

WLAN equipment operates by transmitting electromagnetic energy. This energy is transmitted (and received) through an antenna (this is true of any wireless equipment, for example, mobile phones, TVs or radios). Careful choice of the type and location of antennas used in your WLAN will help to ensure efficient functioning of your network.

There are power transmission limits on all equipment covered by radiocommunications class licences and ACMA mandated technical standards. Equipment supplied to the Australian market must be suitably labelled and comply with the relevant standards arrangements. Installation of WLAN systems with antennas that are different to those supplied by the manufacturer could cause allowed power levels to be exceeded, so installation should be carried out by qualified radiocommunications technicians.

In general terms, there are two sorts of antennas: directional and omni-directional. Directional antennas transmit power in a particular direction and omni-directional antennas transmit an equal amount of power in all directions. A directional antenna will transmit the same amount of power further than an equivalent omni-directional antenna. WLANs are usually supplied with an omni-directional antenna installed. However, it is possible to attach an external directional antenna to some of the current commercially available equipment (see diagram).

Using an external antenna to focus the radiated energy will increase the power and range of your WLAN equipment, but you must be careful not to transmit more power than is allowed under the class licence. It will also provide some control over where the energy of your WLAN is going.

With a directional antenna you can aim the power transmitted towards the location you want to transmit to, and limit unintentional energy ‘leakage’. This will reduce the chance of unwanted users connecting to your WLAN, as well as reducing your chance of causing interference to, and experiencing interference from other equipment using the same spectrum.

Some general guidelines are:

- limit leakage by pointing your directional antenna towards other users of your WLAN;
- use natural barriers, such as walls, buildings and hills to limit leakage; and
- remember that the higher the increase in power of an antenna the narrower the beam of energy is going to be.

An industry organisation known as the Wi-Fi Alliance aims to ensure equipment made by different manufacturers will be compatible. It has coined the term ‘Wi-Fi’ to signify equipment compliance, which is achieved by ensuring all equipment meets defined interoperability requirements during testing in an independent laboratory before manufacturers may use the Wi-Fi Certified logo. So look for the Wi-Fi logo when buying WLAN 802.11a, 802.11b, 802.11g and 802.11n draft based equipment.

IEEE 802.11 equipment and security

Most IEEE802.11 equipment uses either the Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access 2 (WPA2) security protocol. WPA is a standards-based, interoperable security technology that provides strong data protection by using a combination of encryption and user authentication methods. WPA2 is based on the IEEE802.11i amendment to the standard and uses a more advanced encryption technique than WPA. Both WPA and WPA2 overcome known weaknesses in their predecessor security protocol known as wireless equivalent privacy (WEP).

You need to be careful about unwanted transmission leakage from your WLAN because it can mean others gain access to the internet or your private files relatively easily. For this reason you should consider
your overall network set-up and security procedures and not rely on built-in security measures.

Securely deploying a WLAN is not fundamentally different than deploying any LAN. Secure deployment should include dealing with such things as:

- proving who users are;
- controlling what users can do;
- auditing actions;
- determining and managing how addresses are issued;
- watching for anomalous behaviour;
- restricting access to sensitive portions of the network;
- ensuring confidential information is properly encrypted in transit;
- configuring systems to offer only the minimum set of services; and
- ensuring that data is encrypted end-to-end rather than just over the air interface.

More information

More information about Wi-Fi compliance is on the Wi-Fi Alliance website.

There is more information about WLANs licensing and operation on the ACMA website as follows:

- Radiocommunications Class Licence (Low Interference Potential Devices) covering IEEE 802.11a, IEEE 802.11b, IEEE 802.11g and IEEE 802.11n draft equipment and an information paper.
- answers to frequently asked questions Wireless local area networks in the 2.4 GHz band accessing the public telecommunications network and related issues
- an industry fact sheet WLANs—licensing requirements

Please note: this document is intended as a guide only and should not be relied on as legal advice or regarded as a substitute for legal advice in individual cases.

![ Omni-directional antenna 
Directional antenna 
Lower gain antenna - wider beam 
Higher gain antenna - narrower beam ]