



7 - Wireless Local Area Networks (WLAN)

A Wireless Local Area Network (WLAN) provides for a radio connection with a wireline Local Area Network (LAN) over short distances primarily within building premises, campuses, warehouses, retail locations including restaurants for order processing. Additionally a WLAN is able to be created in an ad hoc network established by computing devices for a single session such as for file transfer or for presentations.

The most popular WLAN is the IEEE 802.11¹ standard that has been developed by the Institute of Electrical and Electronic Engineers (IEEE) for this wireless technology (for a description of the IEEE, see Box 6.1 in Chapter 6 – Wireless Personal Area Networks). The IEEE has been instrumental in developing standards for computing networks both wireline and wireless. The standard IEEE 802.3 is generally known as Ethernet and is used in most LANs throughout the world. A WLAN is able to be placed in areas where a wireline LAN would be impractical or too costly. The 802.11 standard is commonly known as Wi-Fi with other WLAN technologies being HomeRF and HiperLAN/2. However, a wireline LAN will continue to be a solution for network computing for sometime as it provides for greater data rates, security and access to the telecommunications carriers for Internet connectivity.

For online material: <http://www.sharedtechnology.net.au>

© Australian National Training Authority 2003

This work is copyright. You may download, display, print and reproduce this material in unaltered form only (retaining this notice) for your personal, non-commercial use or use within your organisation. Apart from any use as permitted under the Copyright Act 1968, all other rights are reserved. Requests for further authorisation should be directed to: Copyright Officer, Australian National Training Authority, GPO Box 3120, Brisbane, QLD 4001. The views and opinions expressed in this report are those of the authors and those consulted and do not necessarily reflect the views of the Australian National Training Authority (ANTA). ANTA does not give any warranty or accept any liability in relation to the content of the work.

Estimates of market size are continually being revised as vendors release projections and shipping data. At the time of preparing this report Allied Business Intelligence reported that the current volume of 23 million chipsets in 2003 are likely to increase with a compounding annual growth rate of 43% through to 2007 when shipments are forecast to be at 143 million per annum.² The versatility of this technology has been recognised by the British and United States armies have introduced this technology for use in combat.³

Technology Overview

The radio spectrum used for this technology is the in 2.4GHz and 5GHz bands. The 2.4GHz band is used by the Industrial, Scientific and Medical (ISM) band as well as cordless telephones and the Wireless Personal Area Networks (See Chapter 6) standard IEEE 802.15. Within this 2.4GHz spectrum there is the possibility of interference from these other communication devices as well as microwave ovens. This spectrum was chosen as it is unlicensed throughout most of the world and is available in Australia. The 5.8 GHz band is becoming increasingly popular for wider bandwidth products as there is no interference from cordless phones, microwave ovens and WLANs and WPANs which are not operating in this spectrum. The 5.2 GHz band, which can support among other things the European based HiperLAN/2 technology, will also increase in popularity.⁴

In Australia the spectrum is covered by a class licence under the *Radiocommunications Class Licence (Spread Spectrum) Devices* and allows apparatus, class and spectrum licences. Most enterprise WLANs will operate under class licences and allow anyone with permitted equipment to operate. The licence does not need to be applied for and there are no licence fees to pay. This class licence applies to equipment such as mobile handsets and cordless telephones. It is important that the equipment used stays within the power ranges prescribed.⁵ See Box 8.2 – Choice of Frequency for more information.

If a number of devices are to be connected to a WLAN, there is the possibility of interference occurring within the transmissions. In order to avoid this interference and to allow connections to be made on the same frequency, a Spread-Spectrum Technology (SST) is employed. There are two ways to accomplish this. One is to use a Frequency-Hopping Spread Spectrum (FHSS) where the signal is spread over the available spectrum but the data packets are “hopped” across specific frequencies. The two communicating devices know which frequencies to hop to for data collection. This is the method used by WPANs in the standard IEEE 802.15 (See Chapter 6 – Wireless Personal Area Networks).

The other method of spread spectrum is Direct Sequence Spread Spectrum (DSSS). This method works on the basis that the stream of information to be transmitted is divided into small pieces, each of which is allocated across to a frequency channel across the spectrum. A data signal at the point of transmission is combined with a higher data-rate bit sequence (also known as a chipping code) that divides the data according to a spreading ratio. The redundant chipping code helps the signal resist interference and also enables the original data to be recovered if data bits are damaged during transmission.⁶ This is the transmission method used in IEEE 802.11b.

Another transmission method is to transmit data in parallel and with a slow symbol rate so that it is longer than the delay spread. This is known as Orthogonal Frequency Division Multiplexing (OFDM). This transmission type is used by the standards IEEE 802.11a and 802.11g.

The types of transmission in spread spectrum and frequency division reduce the interference in wireless communications. However if there are a number of devices on the same WLAN, then there needs to be an orderly processing of data transfer. The IEEE 802.11 standard uses Carrier Sense Multiple Access/Collision Detection (CSMA/CD). This is the LAN access method used in Ethernet. When a device wants to gain access to the network, it checks to see if the network is quiet (senses the carrier). If it is not, it waits a random amount of time before retrying. If the network is quiet and two devices access the line at exactly the same time, their signals collide. When the collision is detected, they both back off and each wait a random amount of time before retrying.⁷ Additionally, a network allocation vector (NAV) indicates how much longer a current transmission will take and allows the network to “sense” how long to wait before sending a transmission.⁸

OSI Layers

The IEEE 802.11 is mapped to the first two layers of the Open Systems Interconnection (OSI – See Box 7.1) and are the Physical Layer (PHY) and the Medium Access Control (MAC).⁹ The Physical Layer defines the type of physical equipment necessary for the transmission and reception of communications. In WLANs this will include equipment designed for the particular spectrum spread or Orthogonal Frequency Division Multiplexing technologies to be used. The Medium Access Control, along with the Logical Link Control (LLC), handles errors in the physical layer, places bits into a frame, and puts the data into packets.¹⁰

The IEEE 802.11 also describes two types of WLANs. Each type is termed a Basic Service Set (BSS) and may be an *ad hoc* independent network using mobile devices or a network that is linked to mobile devices using an Access Point (AP) that is connected to fixed infrastructure. The Medium Access Control and the Medium Access Control-management functions allow the mobile stations to find each other in an *ad hoc* network and connect to the WLAN. Additionally, the Medium Access Control provides for encryption and power management services from the WLAN.¹¹

Security

Wireless transmissions are inherently insecure transmissions. The IEEE 802.11 standard incorporates security measures into the Medium Access Control and this is known as Wired Equivalent Privacy (WEP). As the name implies, this mechanism provides (or is supposed to provide) the equivalent level of privacy that would be expected in a wired LAN. When a data packet is sent, the Network Interface Card (NIC) within the devices encrypts the frame using an RC4 algorithm with a 40-bit key. (See Box 7.2). At the receiving end of the transmission, the access point or enabled device decrypts the data.

The encryption process uses a seed number supplied by the user of the sending device with a randomly generated 24 bit Initialization Vector (IV) and this initialization number can be changed for each frame transmission. The encryption process uses the seed number and puts this into a pseudo-random number

generator that provides a number of equal length to the data bytes that are transmitted in the expanded data with an additional 32-bit Integrity Check Value (ICV). The Integrity Check Value is a number that the receiving station uses to compare to the encryption number sent by the sending station. If there is any tampering, the user is notified.¹² The Wired Equivalent Privacy uses a 40 or 64-bit key to encrypt and decrypt the data. A 128-bit key is also being made available. However for each receiving station, the same key must be used and therefore each station must be manually configured with the same key.¹³

BOX 7.1 OPEN SYSTEMS INTERCONNECTION (OSI)

The OSI reference model was developed by the International Organisation for Standardization (ISO) in 1984. This is the primary model for computer networking and plays a significant role in interoperability. The model describes how information passes from one computer software application through to another computer's application. The model lists seven layers that provide for specific network functions. Each of these layers provides for a specific task to be completed independent of other layers.¹⁴

Layer 7 Application – This is the layer that provides application software with communications. The actual software application is not contained in the OSI model. It is at this level that the File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP) operate.

Layer 6 Presentation – This layer provides for the coding and conversion of data and ensures that the exchange is understandable. This layer provides for the exchange of data from one application to another through common data formats such as ASCII for text and Graphics Interchange Format (GIF). This layer also provides for data encryption and compression.

Layer 5 Session – This layer establishes, manages and disconnects the communication session between computers. This layer ensures that data is sent and retrieved from other computers. The Zone Information Protocol (ZIP) and Session Control Protocol (SCP) operate within this layer.

Layer 4 Transport – This layer manages the traffic across the network to another computer and ensures that the packets arriving are not coming too quickly, out of order or if they are missing. The Transport Control Protocol (TCP) included in this layer ensures that the data is received correctly.

Layer 3 Network – This layer prepares the address for the destination. It is at this layer that the network addresses are attached to the data packets and allow for data to be passed between different physical networks. The data can be sent through the same path (connection-oriented) or allow for each packet to take differing routes (connectionless).

Layer 2 Data Link – This layer formats and frames network packets. At this layer, a Media Access Control (MAC) sub-layer defines the way the network manages the data flow between multiple devices that are sending data simultaneously. At this layer, network characteristics are assigned, physical addresses are attached, error notification is made and flow control of data is managed. The network topology is also defined that consists of the data link layer specifications and how devices on the network are to be connected. The Institute of Electrical and Electronics Engineers (IEEE) has subdivided this layer into the Logical Link Control (LLC) and Media Access Control (MAC).

Layer 1 Physical – This layer defines the electrical, mechanical, procedural and functional specification for physically transferring data between computers and devices on the network. It is at this layer that voltage, timing of voltages changes, physical data rates, setting of maximum transmission distance and physical connectors.

Box 7.2 - WHAT IS RC4?

RC4 is a stream cipher designed by Rivest for RSA Data Security (now RSA Security). It is a variable key-size stream cipher with byte-oriented operations. The algorithm is based on the use of a random permutation. Analysis shows that the period of the cipher is overwhelmingly likely to be greater than 10100. Eight to sixteen machine operations are required per output byte, and the cipher can be expected to run very quickly in software. Independent analysts have scrutinised the algorithm and it is considered secure. <http://www.rsasecurity.com>.

The encryption key may be able to become known to a third party and therefore a Shared Key Authentication may be used. The initialization vector is able to extend the useable time of the key. The key remains constant while the initialization vector changes periodically. Therefore each new initialization vector creates a new key sequence which may change every message but this requires user attention.¹⁵

However this algorithm has not performed as well as it was intended. Additionally, users are not likely to change their encryption keys for each message or everyday. Consequently hackers are able to gain access to these keys and therefore the data. Development on improvements in security has included the 802.1x standard which is a port-based authentication and key distribution standard for 802 LANs whether they are wired or wireless.¹⁶

The Temporal Key Integrity Protocol (TKIP) that uses a 128-bit key among users and access points, uses this key with user's Medium Access Control (MAC) address and then adds a 16-octet initialisation vector which then produces the final key that is used for data encryption. The result is different key streams from each access point for every 10,000 packets transmitted thus providing for a significant enhancement in the network.¹⁷

Further encryption is believed to be required and this is likely to include an Advanced Encryption Standard (AES) that is in use by the United States Government.¹⁸ This new encryption standard will require new hardware as opposed to the Temporal Key Integrity Protocol encryption method that is able to be software driven.

Physical Range and Output of 802.11 communications

The IEEE 802.11 standard provided for a theoretical maximum data rate of 1 to 2 Mbps in the 2.4 GHz spectrum with an indoor range of 46 m and an outdoor range of 92 m.¹⁹ The initial standard was published in 1997 but since then the base standard has been revised to IEEE 802.11, 1999 and has allowed for further standards to be developed that provide for differing data rates, distance and physical layers.

At present the variety of standards is creating some confusion for users and a series of sometimes non-compatible infrastructures. As this technology is new there is still a period of trial and error to travel through to find the appropriate standard for particular applications. The first application likely to be refined for use is for file transfer and Internet access within WLANs and mobile devices as this is the largest market at present.²⁰

The Range of 802.11 standards

In the following paragraphs, there are listed the standards either approved or under development. There are three standards that refer to a communication method using a Physical Layer or a Medium Access Control layer. These are 802.11a, b and g and are listed first, rather than approach an explanation by alphabetic order. The other standards, 802.11d, e, f, h, and i, refer to various modifications required to ensure that the communication standards are of more benefit. Unfortunately due to the involvement of a range of hardware vendors, there will be some confusion until these matters are finally resolved.

Physical Layer Standards

802.11a – This was the first standard created to increase the data rate above 2 Mbps in the 802.11 standard and used the 5GHz spectrum with Orthogonal Frequency Division Multiplex modulation. The range for this is limited to around 8 m.²¹ The use of the 5GHz spectrum is allowed to be used in the United States but not globally.²² The Australian Communications Authority has adopted the 5GHz band as part of the Industrial Scientific and Medical (ISM) band and, therefore, this “a” standard is permissible.²³

This standard has had some difficulty in being established as the development of the radio required more design work and the “b” standard has gained a larger market share as less development was required. The intended data rate for this standard is a theoretical maximum of 54 Mbps and uses 12 channels.²⁴ This standard is not compatible with either “b” or “g” standards but some manufacturers are making chipsets that will allow for inter-compatibility.

802.11b – This standard was developed after the “a” standard and uses the 2.4GHz spectrum and Direct Sequence Spread Spectrum modulation. The theoretical maximum data rate is 11 Mbps with an indoor range of 30 m and an outdoor range of 60 m.²⁵ This technology is currently very popular in the United States and a global sales figure of 39 million units in 2006 is predicted. Chipsets for this standard have been available for a longer period and production costs much lower for chipsets and are estimated to be US\$5.40 in 2005.²⁶

In the “b” devices with higher data rates, a more efficient coding scheme is used and this is termed Complementary Code Keying (CCK) that spreads the length of the coding over more bits. Higher data rates can also be achieved using a coding mechanism called Packet Binary Convolutional Code (PBCC). Texas instruments improved this code to allow for 22 Mbps using a method called PBCC22.²⁷

One major application of this technology is for commercial WLANs. Equally applicable is home use where multiple users in a home environment can have access to the Internet using a broadband connection and an WLAN Access Point. An increasing number of public sites are becoming available for connection using this technology. At these public sites, individuals with enabled equipment are able to access the Internet for email and electronic commerce activities.

Microsoft Windows XP recognises a network interface card (NIC) in the device and prompts the user to connect with a WLAN when the presence of the WLAN is detected. This allows the user to physically take the device and discover WLANs where they exist. There are some limitations with this standard as only three

collocated networks are able to exist in an area. This will place limits on the number of users in a populated area.

802.11g – This standard uses the 2.4GHz spectrum and an Orthogonal Frequency Division Multiplex modulation. The data rate for this technology is a theoretical maximum of 54 Mbps with an indoor range yet to be confirmed. This standard was prepared to overcome some of the difficulties encountered with the implementation of the “a” standard and to increase the overall data rate. It was also agreed to make this standard compatible with the “b” standard and this required the inclusion of Complementary Code Keying (CCK) modulation. Additionally one vendor, Texas Instruments, requested the inclusion of Packet Binary Convolutional Code (PBCC) modulation as well.²⁸ Therefore there are a number of modulations included in this standard.

This standard is expected to be approved in 2003. Some observers have commented on the likely interference coming into the 2.4 GHz spectrum with WPAN (See Chapter 6 – Wireless Personal Area Networks) and 802.11b devices crowding the spectrum. Additionally the inter-operability issues still remain to be resolved.²⁹

Non-Physical Layer Standards

802.11d – This standard deals with issues relating to global use of the 802.11 standard and includes features as well as restrictions. Some of the issues include channelisation, hopping patterns and frequency requirements of operation in countries not supported by the current standards.

802.11e – As data networks have been designed to carry packets of data rather than voice communications (which use a circuit switching), packets of voice and video data which are time sensitive can become lost and cause a jittery result. This standard looks at the issue of Quality of Service (QoS). This includes packet scheduling so ensure that these types of packets are given a higher priority and avoid queuing.³⁰ This is a critical component for further developing this technology. However issues of Quality of Service for voice and multimedia also exist in a wired LAN.

802.11f – This standard looks at the issues of interoperability of equipment between vendors for Access Points. The goal of this is to increase the ubiquity of WLANs and allow for more reliable access while roaming. This standard also allows for users to install Access Points that are not all from the same vendor.

802.11h – This standard intends to supplement the Medium Access Control layer so that it complies with European regulations in the 5GHz spectrum. Europe uses the 5GHz spectrum for some radio and radar applications. There are two developments in this standard. One is the Transmission Power Control (TPC) that limits the power to be used in communications so that the minimum is used to transmit the data thereby reducing the likely interference encountered by safety or emergency equipment. The other is Dynamic Frequency Selection (DFS) which chooses the radio channel that will produce the least amount of interference with other devices such as radar.³¹

802.11i – This standard deals with the difficulties with the security of IEEE 802.11 and the Wired Equivalent Privacy (WEP). The level of protection available with Wire Equivalent Privacy has not lived up to its initial promise.³² This standard attempts to increase the security issues firstly through the use of Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) as described above in Security.

HiperLAN/2

HiperLAN/2 (also spelled HyperLAN/2) has been developed by the European Telecommunications Standards Institute (ETSI). This standard uses the 2.4GHz spectrum and an Orthogonal Frequency Division Multiplex (OFDM) modulation and is therefore similar to the 802.11g standard. The data rate for this technology is a theoretical maximum of 54 Mbps and supports voice, data and multimedia. The major differences are that *ad hoc* networks are not able to be created and all data traffic is through the access point, a Time Division Duplex (TDD) is used instead of the Carrier Sense Multiple Access/Collision Detection (CSMA/CD), and a Data Encryption Standard (DES) is used. The vendor Ericsson is promoting this WLAN in Europe and implementation in Australia may be possible however at this point 802.11a, b, or g are likely to dominate.³³

HomeRF

HomeRF is a WLAN that uses the 2.4GHz spectrum with a theoretical maximum 10Mbps throughput and supports voice, data and multimedia services. The theoretical range is around 70 m. This technology uses Time Division Multiple Access (TDMA) and Carrier Sense Multiple Access/Collision Detection (CSMA/CD) with a Frequency Hopping Spread Spectrum (FHSS). The market adoption and chipset production of this technology has not been to the level of either Bluetooth or 802.11 and it is unlikely to be greatly used in Australia.³⁴

Summary

This area of wireless local area networks does appear to be somewhat crowded. Intel's Centrino microprocessor is currently leading the way. It is expected that there will be many more manufacturers entering this area for general purpose and niche market applications. Continuing disruption is planned over the next five years.

IMPLICATIONS FOR THE SHARED TECHNOLOGY INDUSTRIES

Automotive

The WLAN technologies will be able to provide a radio link of on-board data to diagnostic equipment without the use of cables. This method may be used in personal automobile servicing for data transfer³⁵ with some estimates stating that 12 percent of vehicles will contain this technology by 2007.³⁶ However, the use of this technology will more likely be for fleet management and larger vehicles such as transport equipment or earth moving equipment where physical access and cable length may be more difficult.

There are some installations in place with transport and mining equipment where real-time data is collected via a satellite communications system. While this is a different technology to the WLAN, the principle of data transmission from vehicle to database is the same. For fleet vehicles that return to a depot for transfer of goods, such as courier services, this technology provides a quick method of down-loading client information, content of the vehicle as well as travel distance, fuel consumption and other fleet details.

For larger and more expensive vehicles, monitoring of vehicle performance is more critical in terms of cost efficiencies and maintenance requirements. Reconfiguration of engine attributes is able to be done remotely while the vehicle waits at a service bay and this may depend upon the loading of the vehicle or other aspects. Maintenance is also able to be assessed from on-board data transmitted to a service centre and only the necessary maintenance carried out, instead of a planned maintenance schedule based upon distance travelled.

Building and Construction

The WLAN technology provides for greater flexibility in communication design. As this technology is wireless and does not need structured cabling in working spaces, WLAN technologies are of benefit where office partitions are frequently reconfigured or where individuals change seating locations. This technology also allows for an easier retro-fit of some sensing devices such as thermostats for HVAC applications, as cabling is not necessary.³⁷

Architects and builders will need to become aware of the implications of using materials that reduce the efficiencies of WLAN radio transmissions. Collocation of interfering Industrial Scientific and Medical (ISM) spectrum equipment and access points will need to be planned for as devices such as video security links, lighting and other equipment.³⁸ Equally the positioning of the access points has become a major part of commissioning a WLAN system.

Engineering

A structured cable infrastructure will continue to be the preferred option in most instances however the use of a WLAN does have some advantages. As the 802.11 standard is designed to meet the 802.3 Ethernet standard, once the data from a device reaches the wired LAN, the data loses the encryption and other WLAN related attributes. Therefore the WLAN is a logical extension to the LAN when appropriate. The major benefit will be for environments where cabling is inappropriate due to frequent reconfiguration of a process or in a manufacturing facility with reconfiguration of the physical layout.

Additionally, where a service person is required to cover large areas within a facility to perform maintenance and troubleshooting, the WLAN provides for easy access to the Internet or the enterprise's intranet or database.³⁹

Electrical

Within new construction, system electricians are installing structured cabling and are being called upon to do more of the telecommunications infrastructure as well. At present, most cabling installers are providing cable up to the telecommunications equipment. As the technology becomes more common it is likely that the installer will be attaching WLAN access points to the network as another piece of communications equipment.

Site surveys will need to be undertaken in order to establish the correct location of the access points and to ensure that there is minimal interference with other equipment and access points once the location becomes operational. Additionally, location of the access points becomes important when it is recognised that the signal will travel outside of the physical premises and be available to non-secure locations.

Electronics

This industry will find that there will be an increasing number of devices entering that will have WLAN capability. These devices will also have embedded processors that will provide data to networks through a wireless connection. Members of this industry will be at the forefront in problem solving.

Information Technology

The transfer of files and data from mobile computing devices will continue to be the largest application for this technology. Network administrators and managers will need to ensure that the network remains secure. For cable-based equipment, the manager is able to control which devices are connected to a wired LAN but for wireless devices this is a growing concern, not only for security of data, but for the integrity of the network as well.⁴⁰

Network managers will need to continually monitor access and integrity of the system even after the introduction of the “more secure” Advanced Encryption Standard (AES) as “un-hackable” systems are unlikely to exist. Network managers will also need to closely monitor data transfer rates as more enabled devices connect to the network and an increase in other devices operating in the 2.4GHz spectrum become more popular.⁴¹

Applications of this technology will increase in retail, hospitality, services, warehousing and many others with the likely exception of the health industry. Enterprises will wish to ensure that data collected from transient users is managed as well as information relating to the premises is communicated back to the user. This will require development of databases and interfaces that allow the user access to content and other data.

Telecommunications

The United States have been using this technology for some time and are reaching a mature market. An initial use of this technology was to provide free-of-charge to clients of restaurants access to the Internet through these public access points called “hot-spots”. As the popularity of the technology grows through laptop computers being enabled as a standard, there is the opportunity for telecommunications carriers to start profiting from this popularity. It is for this reason that Wireless Internet Service Providers (WISPs) are beginning to build networks of such hotspots with access to the Internet as part of a subscription for wired Internet access.⁴² Some locations believed to be suitable for these “hot-spots” are consumer locations such as hotel lobbies, cafes, airports, petrol stations and other similar venues.

The WLAN technology when used with the WPAN technology (See Chapter 6 – Wireless Personal Area Networks) provides entry into another developing technology called Voice over Internet Protocol (VoIP) (See Chapter 5 – Next Generation Telecommunications Networks). This provides voice access through a mobile phone using WPAN technology to a laptop computer enabled with Voice over Internet Protocol software. This means that no call is placed on the mobile network as it is using the WLAN to an access point at a “hot spot” to the Internet. Using this combination of technologies, a pseudo fixed-wired telephone connection is made and calls are part of the down-load volume within a Wireless Internet Service Provider’s account. The result is savings in mobile calls but the down side is that cell hand over is not possible so the user needs to stay at that location. Quality of Service (QoS) may also be an issue.⁴³

-
- ¹ Institute of Electrical and Electronic Engineers. (1999). *ANSI/IEEE 802.11, 1999 Edition. Part 11: Wireless LAN and Medium Access Control (MAC) and Physical Layer (PHY) specifications*. Piscataway, NJ: Author.
 - ² Business Wire. *Wi-Fi IC Shipments Set to Top Expectations*. 16 January, 2003.
 - ³ Jenkins, C. (2003). Hi-tech diggers in global war trails. *The Australian*, 28 January, 2003. p 21.
 - ⁴ Australian Communications Authority. (2002). *Frequently asked questions: Wireless local area networks in the 2.4 GHz band—accessing the public telecommunications network and related issues*. Available: <http://www.aca.gov.au/consumer/faq/wlans.htm> Accessed: 10 February 2003.
 - ⁵ Australian Communications Authority. (2002). *WLANs - Licensing Requirements*. Canberra: Author. Available: <http://www.aca.gov.au/consumer/fsheets/industry/fsi26.pdf> Accessed: 10 February 2003.
 - ⁶ Hiller, K. (2002). *Wireless LANs: An Overview*. Gartner Dataquest. Reference Number: DPRO-88978.
 - ⁷ Marks, R. B., Gifford, I. D., & O'Harra, B. (2001). Standards from IEEE 802 Unleash the Wireless Internet. *IEEE Microwave Magazine*, 2(2), pp. 46-56. Available: http://iee802.org/16/docs/01/80216c-01_10.pdf Accessed: 11 February 2003.
 - ⁸ PricewaterhouseCoopers. (2002). *Technology Forecast: 2002-2004*. Menlo Park, CA: Author.
 - ⁹ The use of Media and Medium in this term are interchangeable. The IEEE uses both. See <http://www.ieee802.org/1/pages/802.1ac.html> and <http://standards.ieee.org/announcements/p1640app.html>
 - ¹⁰ Marks, R. B., Gifford, I. D., & O'Harra, B. (2001). Standards from IEEE 802 Unleash the Wireless Internet. *IEEE Microwave Magazine*, 2 (2), pp. 46-56. Available: http://iee802.org/16/docs/01/80216c-01_10.pdf Accessed: 11 February 2003.
 - ¹¹ Marks, R. B., Gifford, I. D., & O'Harra, B. (2001). Standards from IEEE 802 Unleash the Wireless Internet. *IEEE Microwave Magazine*, 2 (2), pp. 46-56. Available: http://iee802.org/16/docs/01/80216c-01_10.pdf Accessed: 11 February 2003.
 - ¹² Weatherspoon, S. (2000). Overview of IEEE 802.11b Security. *Intel Technology Journal Q2, 2000*. Available: http://www.intel.com/technology/itj/q22000/articles/art_5.htm Accessed: 10 February 2003.
 - ¹³ Configuring Wired Equivalent Privacy (WEP). Intel Corporation. Available: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a0080094581.shtml Accessed: 11 February 2003.
 - ¹⁴ Cisco. (2003). *Internetworking Basics*. Available: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm Accessed: 13 February, 2003.
 - ¹⁵ Weatherspoon, S. (2000). Overview of IEEE 802.11b Security. *Intel Technology Journal Q2, 2000*. Available: http://www.intel.com/technology/itj/q22000/articles/art_5.htm Accessed: 10 February 2003.
 - ¹⁶ Hiller, K. (2002). *Wireless LANs: An Overview*. Gartner Dataquest. Reference Number: DPRO-88978.
 - ¹⁷ Geier, J. (2002). *802.11 Security Beyond WEP*. 80211 Planet Tutorials. Available: http://metatag.tripod.com/howto/howto_802_1_1_Security_Beyond_WEP.htm Accessed: 13 February 2003.
 - ¹⁸ National Institutes of Standards and Technology. (2001). *Advanced Encryption Standard (AES): Questions and Answers*. Washington, DC: Commerce Department. Available:

- <http://www.csrc.nist.gov/encryption/aes/round2/aesfact.html> Accessed: 13 February 2003.
- ¹⁹ Hiller, K. (2002). *Wireless LANs: An Overview*. Gartner Dataquest. Reference Number: DPRO-88978.
- ²⁰ Hiller, K. (2002). *Wireless LANs: An Overview*. Gartner Dataquest. Reference Number: DPRO-88978.
- ²¹ Hiller, K. (2002). *Wireless LANs: An Overview*. Gartner Dataquest. Reference Number: DPRO-88978.
- ²² Hunn, N. (2002). *The Evolution of the Wireless LAN*. TDK Systems. London: Author. Available: <http://www.tdksystems.com/support/whitepapers> Accessed: 12 February 2003.
- ²³ Australian Communications Authority. (2002) *WLANS Interference Management*. Canberra: Author. Available: <http://www.aca.gov.au/frequency/rlan-im.pdf> Accessed 10 February, 2003.
- ²⁴ Hunn, N. (2002). *The Evolution of the Wireless LAN*. TDK Systems. London: Author. Available: <http://www.tdksystems.com/support/whitepapers> Accessed: 12 February 2003.
- ²⁵ Hiller, K. (2002). *Wireless LANs: An Overview*. Gartner Dataquest. Reference Number: DPRO-88978.
- ²⁶ Hunn, N. (2002). *The Continuing Evolution of the Wireless LAN: Hot Spots and the Banias Effect*. London: TDK Systems. Available: <http://www.tdksystems.com/support/whitepapers> Accessed: 12 February 2003.
- ²⁷ PricewaterhouseCoopers. (2002). *Technology Forecast: 2002-2004*. Menlo Park, CA: Author.
- ²⁸ Dulaney, K. (2002). *802.11g: A New Wireless Networking Standard*. Gartner Dataquest. Reference Number: T-15-3353.
- ²⁹ Dulaney, K. (2002). *802.11g: A New Wireless Networking Standard*. Gartner Dataquest. Reference Number: T-15-3353.
- ³⁰ PricewaterhouseCoopers. (2002). *Technology Forecast: 2002-2004*. Menlo Park, CA: Author.
- ³¹ Keene, I. (2002). *What to Expect from Wireless LAN Standards and When*. Gartner Dataquest. Reference Number: COM-15-2728.
- ³² PricewaterhouseCoopers. (2002). *Technology Forecast: 2002-2004*. Menlo Park, CA: Author.
- ³³ PricewaterhouseCoopers. (2002). *Technology Forecast: 2002-2004*. Menlo Park, CA: Author.
- ³⁴ Hiller, K. (2003). *Wireless Netowrking withHomeRF: An Introduction*. Gartner Research. Reference Number: DPRO-93769.
- ³⁵ Daimler Chrysler (2002). Data Greetings from Como. *Hightech Report, 2*. pp. 70-71.
- ³⁶ Long, M. (2002). *Bluetooth, Wi-Fi Get Ready to Hit the Road*. E-inSITE. 9 August, 2002. Accessed: 22 January, 2003.
- ³⁷ Continental Automated Buildings Association. (2002). *Technology Roadmap for Intelligent Buildings*. Ottawa, ON: Author. Available: http://www.caba.org/trm/TRM_English.pdf Accessed: 13 February 2003.
- ³⁸ Hundt, R. E., Newman, S., & Richards, J.E. (2002). Wi-Fi goes to Washington. *The McKinsey Quarterly, Autumn 2002*, pp. 150-152.
- ³⁹ Mintchell, G. A., & Yacano, F. (2002). Beam up some information, Scotty. *Control Engineering, 49(5)*. pp. 39-44.
- ⁴⁰ Hiller, K. (2002). *Wireless LANs: An Overview*. Gartner Dataquest. Reference Number: DPRO-88978.

-
- ⁴¹ Australian Communications Authority. (2002) *WLANS Interference Management*. Canberra: Author. Available: <http://www.aca.gov.au/frequency/rlan-im.pdf> Accessed 10 February, 2003.
- ⁴² Hunn, N. (2002). *The continuing Evolution of the Wireless LAN Hotspots and the Banias Effect*. London: TDK Systems. Available: <http://www.tdksystems.com/support/whitepapers> Accessed: 12 February 2003.
- ⁴³ Hunn, N. (2002). *Bluetooth - Saviour of GPRS*. London: TDK Systems. Available: <http://www.tdksystems.com/support/whitepapers> Accessed: 7 February 2003.