

Unclassified

DSTI/ICCP/TISP(2002)10/FINAL



Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

16-Apr-2003

English - Or. English

**DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY**

Cancels & replaces the same document of 14 April 2003

Working Party on Telecommunication and Information Services Policies

DEVELOPMENT OF WIRELESS LOCAL AREA NETWORKS IN OECD COUNTRIES

**DSTI/ICCP/TISP(2002)10/FINAL
Unclassified**

English - Or. English

JT00142903

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

FOREWORD

In December 2002, this report was presented to the Working Party on Telecommunications and Information Services Policy (TISP). It was recommended to be made public by the Committee for Information, Computer and Communications Policy in March 2003.

The report was prepared by Mr. Atsushi Umino of the OECD's Directorate for Science, Technology and Industry. It is published on the responsibility of the Secretary-General of the OECD.

Copyright OECD, 2003

Applications for permission to reproduce or translate all or part of this material should be made to:

Head of Publications Service, OECD, 2 rue André-Pascal, 75775 Paris Cedex 16, France.

TABLE OF CONTENTS

MAIN POINTS.....	4
I. INTRODUCTION.....	5
II. OVERVIEW OF WIRELESS LANs	7
2.1 What is a Wireless LAN?	7
2.2 Benefits of Wireless LANs	8
2.3 Disadvantages of Wireless LAN.....	9
2.4 Wireless LAN application.....	10
III. STANDARDISATION OF WIRELESS LAN.....	11
3.1 Activities of industry groups.....	11
3.2 Equipment standards for WLANs at 2.4 GHz and 5 GHz	12
3.3 Radio technology	18
IV. SECURITY OF WIRELESS LANs	20
4.1 Standard security features defined by IEEE	20
4.2 Vulnerabilities and risks	21
V. ALTERNATIVE WIRELESS TECHNOLOGIES	21
5.1 Bluetooth.....	21
5.2 HomeRF.....	23
5.3 3G.....	23
VI. IMPLICATIONS FOR REGULATION	24
6.1 Potential issues for regulation.....	24
6.2 Regulatory frameworks and initiatives by OECD countries.....	26
VII. IMPLICATIONS FOR MARKET COMPETITION.....	33
7.1 Developments of WLAN market competition	33
7.2 WLAN market development in some OECD countries.....	34
7.3 Community-based wireless networks	38
NOTES	39

MAIN POINTS

Wireless technology provides business executives, office workers, small businesses and residential users with expanded opportunities to connect to the Internet outside the limited area dictated by fixed networks. Wireless LAN (WLAN) standards enable anyone to set up a network easily and share a broadband Internet connection among several computers equipped with wireless Ethernet cards. With these advantages, WLAN systems have been implemented as an extension to, or as an alternative for, a wired LAN. WLANs have been growing in popularity in a number of vertical markets over the past few years among OECD countries. In recent years, access to WLANs in a public place through access points (hot spots) is gradually changing the face of the telecommunications industry.

The use of WLANs provides OECD governments with a number of policy challenges. While wireless technology has been led mainly by industry, governments are encountering some policy challenges as WLAN services grow in popularity. Some examples highlight policy issues raised for regulators:

- In view of the fact that most WLAN services are offered using radio frequency, governments need to ensure that sufficient spectrum is allocated for WLANs. In a number of OECD countries, however, the spectrum management plan has not been adapted to accommodate the needs of WLAN services.
- To ensure the best possible opportunities for economic growth in this area, it will be necessary to establish unified worldwide frequency bands for WLANs. The allocation of 5 GHz WLANs is one of the agenda items at the forthcoming World Radiocommunication Conference (WRC). After extensive sharing studies with the existing services, it seems highly probable that this aim will be achieved. The WRC allocation decision is expected to facilitate each government to make spectrum available.
- As WLANs allow a single subscriber to set up a network that a third party can access, “free rider” problems inevitably occur. What should the policy response be to the “free rider” problem?
- Although WLANs can easily be combined with IP telephony, the regulatory frameworks for IP telephony themselves are, for the moment, not sufficiently established in most OECD countries. Most regulations for telephony are still based on traditional copper networks.
- While operators of mobile telephones, represented by 3G, need a license to provide services, WLAN providers normally use unlicensed radio spectrum. Does this imply that there is an asymmetric regulatory framework?
- WLANs are targeting public access markets by installing access points at airports and hotels. Unlike mobile telephones, however, they do not actually ensure public access given that there is limited coverage. Unlike mobile systems WLAN commercial service providers need authority to provide services, and allow their customers to obtain access, in public places.

Policy and regulations for WLANs should be flexible allowing a variety of technological standards to compete and develop. Recent government regulatory actions relating to WLAN services should be of interest to other OECD countries. For example:

- In the United States, the FCC has reviewed its regulations on spread spectrum several times in order to accommodate new technological developments related to WLANs.
- In the United Kingdom, the Radiocommunications Agency (RA) further deregulated use of the 2.4 GHz band in July 2002 to permit operation of licence exempt public access services in addition to private systems. In February 2003, two bands at 5 GHz were opened to permit licence exempt use by both private and public access WLAN services.
- In France, the ART recently announced changes in the conditions of use of 2.4 GHz frequency bands in order to allow commercial WLAN services.
- In Japan, the MPHPT has revised the relevant regulations to allow outdoor use of 5 GHz band WLANs.

Spectrum congestion is the most important challenge facing the growth and development of WLAN services. As the number of users grows, it becomes increasingly difficult for systems to operate without degrading one another. This is especially acute in the 2.4 GHz band where in many countries there is widespread use of spread spectrum technologies that are particularly vulnerable to interference from each other and where services are operating without any form of interference mitigation technique. Technical studies in this band indicate that more than one co-located system causes significant service degradation. Anecdotal evidence suggests that noticeable effects may be widespread in some countries. Facing this situation, some OECD countries have started to endeavour to sort out the problem. In the United Kingdom, for example, the RA is conducting a monitoring exercise to attempt to establish the extent of the problem.

An important disadvantage of WLANs is security, which needs to be addressed to ensure the longer term development and diffusion of WLANs. WLANs also need to be put in perspective vis-à-vis a number of alternate technologies available on the market. Third generation (3G) networks are being deployed nation-wide in some countries. Fixed wireless access (FWA) is also being developed in a number of cities across the OECD and the use of satellite networks, wireless wide area networks and other mobile applications are growing. While WLANs could be one of the more competitive wireless networks in the long term, their success will depend on the range of service that can be offered as well as how they can compete with these other technologies. In turn, this may depend on whether any technical or regulatory barriers emerge which slow down WLAN development. OECD governments have placed much emphasis on the development of an information society and on eliminating the domestic digital divide. WLANs can help in achieving these ambitions, but governments need to ensure that the policy and regulatory environments are conducive to this technology and the spectrum resources are made available to help grow the use of this technology.

I. INTRODUCTION

Governments and industry are placing increasing priority on facilitating access to broadband. This policy and commercial objective is being facilitated by an expansion in the variety of broadband technologies available. In this context it is important to ensure that government policy and regulations allow for an environment where the various technologies can compete, and complement, each other. At present broadband access is being provided mainly on the basis of ADSL technologies or cable modems, but a rapidly developing alternative to these technologies is being provided through wireless networks. In many cases these wireless technologies are also an important complementary technology to fixed network access to broadband. Wireless networks, such as “Wi-Fi¹”, have a number of advantages that traditional broadband access does not have, especially in that they do not necessarily need a wired infrastructure. This allows companies and individuals to conduct their businesses or access Internet for other applications wire-

free for easy access and mobility. However, it should be emphasised that deregulated radio spectrum can offer, at best, only a “best endeavours” service.

Wireless networks can be divided into two main categories in the same way as traditional wired networks: wireless local area networks (WLANs) and wireless wide area networks (WWANs). As in the case of wired LANs, WLANs have a higher data rate with smaller coverage areas compared with WWANs. These WLANs are increasingly becoming a viable alternative, or an extension, to traditional wired networks. The focus of this paper is mainly on wireless LANs. This paper examines the state of wireless LANs including development of standards, business and home applications, and security issues, and examines the implications for regulation and market competition.

The applications of wireless LAN include “independent networks”, which are suitable for small or temporary peer-to-peer configurations, and “infrastructure networks”, offering fully distributed data connectivity via roaming.² While wireless LAN applications used to be a limited niche in the telecommunications market, they are currently rapidly penetrating into the market on a larger scale by providing broadband access in a convenient and inexpensive manner. With the recent proliferation of wireless data networks in homes, business and public spaces, a growing number of people use this method of communications. A range of users, from business travellers to apartment residents, are surfing Web sites on the Internet and collecting e-mail at various places such as airport lounges, coffee shops, or at home using portable devices. While WLANs have traditionally been used in warehouse, factory and retail-floor automation, use in offices has been increasing in recent years because of inexpensive products based on the IEEE 802.11 family of standards including IEEE 802.11b³ as well as growing numbers of public access points.

Some countries have dramatically increased the rate of use of wireless networks. In the United States, for example, it has been reported that the number of wireless LAN implementations doubled between 2001 and 2002.⁴ More than 1 million wireless LAN access points are said to be in use by more than 700 000 US enterprises.

There are a number of optimistic estimates about the future growth of the wireless LAN market. For example, the wireless LAN market is forecast to grow from USD 1.2 billion in 2001 to USD 3.1 billion in 2006 according to the Dell'Oro Group.⁵ Another analysis expects that there will be more than 100 000 local access points throughout the world within four years.⁶ In the United States, some analysts estimate that more than 5 million American households will migrate to mobile and high-speed broadband networks for their primary connection by 2006.⁷ There is another prediction that replacement of wired services by wireless access is expected to accelerate dramatically and will reach an additional 10 million wireless access users by 2005.⁸

Wireless access also stimulates the usage of broadband networks. At the University of Akron in the United States, for example, it has been reported that Internet use increased to three times its previous level after the school installed 802.11b transmitters throughout its campus in 2001. WLAN is also gaining popularity among mobile telephone operators, who can use it to offer users value-added services such as broadband Internet.⁹

One important factor in the deployment of wireless broadband networks is that WLANs in many countries have not proliferated as a result of government initiatives. These high-speed wireless data networks have been built from the bottom up rather than following top-down initiatives. In other words, it is industry that leads this technology and its applications whereas governments are seemingly slow to catch up with this movement from the policy perspective. However, some governments are beginning to be very keen on supporting WLAN projects. In the United Kingdom, for example, large numbers of WLANs have been installed to provide services to the publicly maintained education sector. This covers a wide range of

government-funded institutions from schools to informal adult education initiatives. Much of the funding for these projects has come in the form of government grants targeted to improve public access to broadband services. It should also be noted that one of the main reasons WLANs have proliferated is because users do not need to obtain licenses to operate WLAN devices.

II. OVERVIEW OF WIRELESS LANs

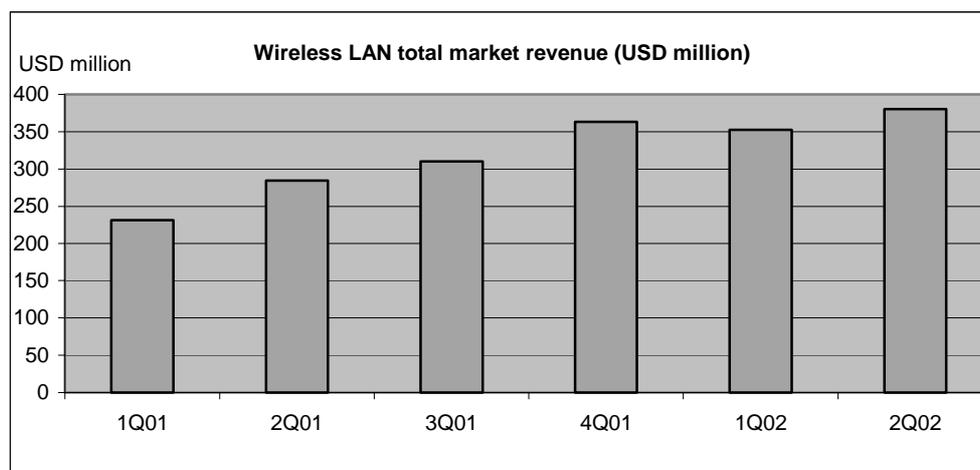
2.1 *What is a wireless LAN?*

A wireless LAN (WLAN) is a wireless local area network. That is, it is a high bandwidth, two-way data communications network using radio or infrared as the medium of transmission rather than optical fibre or copper cable and operating over a limited geographic area.¹⁰ The components of WLANs usually include two types of equipment: a wireless station and an access point, although peer-to-peer networking is sometimes employed. The wireless station is typically a laptop or personal computer (PC) equipped with a wireless network interface card (NIC). Such a card may also be installed in a desktop computer or handheld device, such as a personal digital assistant (PDA), or equipment in a kiosk. The NICs use radio frequencies or infrared beams to enable connections to the WLAN. For public access services, access points can be provided in a number of public places such as airports and coffee shops. The NIC automatically search through the channels to find WLANs. Once the NIC finds the correct channel, it starts “setting up a connection” with the access point.

While WLAN technologies were originally designed to complement the existing fixed-connection LANs, they can be used to replace wired access or to extend existing wired infrastructure. WLANs are being deployed not only in business but also by end-users as a cost-saving measure or for convenience. Instead of installing expensive wiring infrastructure, the WLAN user has access to communications by use of a small radio transmitter. Any computer with WLAN can potentially pick up the signal as long as it is within its reach.

WLANs are often not completely “wireless” in that supporting the wireless workstations are a number of existing wired broadband backbone networks. The exception to this is peer-to-peer networks, which may be created on ad hoc basis: for example, networks of laptop users exchanging documents during a meeting. The increasing prevalence of WLANs depends, in this context, on the development of existing broadband networks. At the same time, the growing popularity of WLANs is expected to provide an incentive for the construction of networks for shared use. It is now possible to envision a communications world consisting of base stations that connect to the Internet through wired broadband networks, and local connectivity.¹¹

WLANs emerged for business use in the early 1990s. At that time, however, speed limitations, lack of hardware compatibility, insufficient awareness among consumers, etc., slowed diffusion. As a result, most enterprises remained with their existing wired networks instead of moving to WLANs. However, many of these initial problems have been overcome, and now there is significant growth in the WLAN market. Worldwide, the 802.11 market, including 802.11b and 802.11a, has reportedly increased from revenues of USD 231.4 million in the first quarter of 2001 to USD 380.2 million in the second quarter of 2002.¹² During 2002, many businesses, which include such chains as McDonald’s, Starbucks Coffee, and MOS Burger, have been installing WLANs and creating “hot spots” one after another in certain model outlets for the convenience of their customers.¹³

Chart 1. Wireless LAN total market revenue between the first quarter of 2001 and second quarter of 2002

Source: Dell'Oro.

2.2 Benefits of wireless LANs

The cost of deploying WLANs is less than wired networks while having most of the capabilities of wired. There are no cabling and associated labour costs and the spectrum used is mostly deregulated. Network access can be set up rapidly permanently or for temporary use (*e.g.* a conference). In addition, WLANs provide opportunities for “third parties” to use the network free of charge. WLANs are also convenient. They provide users with more mobility and flexibility by allowing them to maintain broadband connection when they roam from one area of coverage to another. WLANs can also be a partial solution to the last-mile problem as well as to geographical digital divide in a longer term by providing community networks at a lower cost. WLANs also provide fast transmission speed with most WLANs transmitting at speeds of at least 2 Mbps and with typical maximum speeds of 10 Mbps.

A feature of WLANs that has captured public imagination is that they may be used to provide broadband access in public places and, sometimes at no perceived charge to the user. In some cases such public access results from the ability to use private corporate wireless networks aimed at providing service within a building, but that can be accessed outside of buildings because they are not fully secured. Such “free rides” can also be deliberate as a result of individuals setting up neighbourhood hot spots. The ability to access broadband networks free of charge from public locations has led to the concept of “warchalking”(see Box 1).

Box 1. Warchalking

Putting chalk marks on pavements and walls to show the location of wireless networks is becoming popular in some countries such as the United Kingdom and the US. This phenomenon, called “warchalking”, derives from the early days of telecommunications networks when hackers would engage in “wardialing”, the process of trying to find phone lines being used by computers that were ripe for hacking. Users looking for free Internet access drive or walk in the hope of finding areas where wireless access has “spilled” into the street. In this context, the so-called “wardriving” and “warwalking” phenomena have developed.

Unpaid access to wireless broadband networks has led to some major cable and telephone companies that provide broadband wired connections to complain that customers are violating their service agreements by giving others a “piggyback” using WLANs to extend the reach of wired broadband networks. For example, a spokesman for Time Warner Cable argued that free riding on WLANs was similar to cable theft.¹⁴ From a legal perspective, this issue may become important in the future.

2.3 *Disadvantages of wireless LAN*

A significant problem arising from the use of WLANs is security. In comparison with wired technology, the nature of radio transmission inevitably includes the possibility of eavesdropping. This issue will be dealt in a separate section of this paper.

As the numbers of systems in operation grow, services operating in close proximity result in service degradation. This is especially true where services are deployed outdoors or in public locations. This problem is particularly severe where spread spectrum technologies are used. IEEE standards 802.11 and 802.11b are frequency hopping spread spectrum modulation (FHSS) and direct sequence spread spectrum (DSSS) modulation respectively in the 2.4 GHz band. Both standards lack interference mitigation measures or any form of operational etiquette. Where services are co-located, degradation of operation is therefore inevitable. Further technical developments, mainly at 5 GHz band, seek to improve the potential for systems to co-exist by employing better modulation schemes (for example OFDM, orthogonal frequency division multiplexing), agreed channel plans, random back off, transmit power control (TPC) and dynamic frequency selections (DFS).

Another difficulty relates to the nature of radio propagation at microwave frequencies. In the frequency bands used for WLANs transmitter power limits are relatively low. WLANs are therefore a short-range networking solution. Users will find communications disrupted once they move out of range. A further difficulty is that there is no agreed international roaming standard. In order for roaming to work, frequency allocations must be unified, standards for operation must be harmonised, billing systems must be interoperable, and service operators must be sure of the ability of their partners to provide a similar quality of services.¹⁵ Even then systems from different vendors may not be inter-operable even if they employ the same technology and the same frequency band due to differences in implementation.

WLANs may also face difficulties in making a business case for investment. Costs to build a nation-wide proprietary wireless network in the United States are high (some estimates put this at around USD 1 billion) and the return on investment is at present not sure. Further, the free-riding phenomenon tends to put a damper on profit expectations.

It is likely that free wireless Internet services will continue for a period of time as a grassroots effort. However, there are potential customers, especially business users, who are willing to pay for a better quality of WLAN services. In many cases, business customers will be willing to pay monthly subscription fees to ensure continuous access as well as certain level of service and security. Widespread adoption of WLANs in businesses might lay the groundwork for individuals to set up their own WLAN access points. It must always be emphasised, however, that WLANs can never be more than a “best efforts” service where they operate in deregulated radio spectrum.

2.4 *Wireless LAN application*

There are a number of WLAN applications for businesses as well as residential users. Vertical markets such as health care, education, manufacturing, retail, and warehousing were early users of WLAN technology. For example, it has been suggested that WLANs shorten hospital visits because they deliver medical information to physicians and other hospital staff when and where they require it.¹⁶ By the same token, workers in warehouses can use a portable computer to verify the inventory by WLAN to see if an item is available. The use of WLANs at school is also gradually percolating in some OECD countries. In the United Kingdom, for example, thousands of schools use both 2.4 GHz and 5 GHz band enabled equipment to distribute broadband services and to provide wire free working in the classroom.

Nowadays, there is also a significant amount of interest in WLAN technologies in the public access markets. WLAN users have Internet access in local access points called “hot spots” such as coffee shops, hotels, train stations and airports. The hot spots allow portable computing devices equipped with wireless cards to connect to the Internet. This type of application is raising interest especially as new portable computing devices, such as PDAs, emerge. Thus, some private companies are developing a system for public WLAN services. For example, Cisco Systems is working with Internet service providers (ISPs) across Europe to equip international airports with wireless broadband technologies in an effort to enable broadband access for business travellers on the move.¹⁷ But, although the number of WLAN hot spots is growing rapidly in some OECD countries such as the United States, particularly in urban areas, they are still difficult to find in the most countries and in rural areas.

The SOHO (small office home office) market segment is viewed as particularly important for WLANs with some predictions estimating growth at about 40% between 2003 and 2006.¹⁸ In the arena of Wi-Fi telephony (discussed later) WLAN is expected to work as a means to provide ubiquitous telephone services, which are essential to the SOHO markets. It will be of great convenience that WLANs replace the need to install and pay for traditional Ethernet CAT5 cabling and jacks in the office infrastructure with a simpler as well as cost-effective solution, although not all telephony requires CAT5 cabling.

In very recent years, some new types of applications have emerged. For example, Air Canada has been using Wi-Fi networks to find people who are about to miss their flights and to process their tickets as well as give them seat assignments on the flight.¹⁹ In the United States, about 150 homes in Houston use WLAN to create wireless billboards in order to replace scribbled notes on kitchen refrigerators which serve as a family bulletin board. There is also a pilot project in which WLANs are used to help cook a meal.²⁰

WLANs also might provide an innovative application in combination with voice over IP technology, particularly in the arena of corporate telephony.²¹ Traditionally, voice and data networks have been separate. With the emergence of Voice over IP (VoIP) technology it has become possible to transmit telephone conversations over any packet-switched IP networks. As a result, IP telephony using wireless technology, which is called Wi-Fi telephony, has started to develop. IP networks are cost-effective but less secure compared with traditional telephony circuits. An increasing number of enterprises have adopted Wi-Fi telephony, where mobile users are easily identified. They usually have control over the coverage area, bandwidth utilisation as well as required Quality of Service (QoS) implementation. In this way, Wi-Fi users in the enterprise have the same features and accessibility to the corporate telephony system as their wired colleagues.

WLAN applications are also developing in residential areas. Residential IP telephone service can easily be made available if the cost of Wi-Fi telephones is equivalent to PSTN costs. In some countries contractors are now putting equipment for use of WLANs into each new home. For example, Canadian house builders in the towns of Embrun, Russell and Metcalfe are installing a wireless box of Storm Internet, a wireless ISP, in each house because a number of new buyers are not interested in a rural house if

it cannot get broadband Internet access.²² With a WLAN, multiple terminals can be connected to a single line, allowing everyone in the family to use the Internet at the same time if they choose.²³

Another technology that could be used in WLAN applications is ultra-wide band (UWB). The combination of low power, short range, and high data rate communications makes UWB a good match for home or office networking. UWB can also be used as a replacement for Bluetooth (described later) to provide wireless connection to peripherals.

III. STANDARDISATION OF WIRELESS LAN

The WLAN industry has emerged as one of the rapidly growing sectors in the telecommunications arena. It has been reported that worldwide sales of WLAN equipment, consisting of network interface cards, access points and bridges, reached USD 450 million in the first quarter of 2002, which is a three percent increase from the end of 2001 and 55% increase from the first quarter of 2001.²⁴ This market development owes much to the introduction of standardisation in WLAN products.

Standardisation has allowed WLANs to inter-operate between vendors. It implies that a variety of WLAN equipment can be used over the same wireless infrastructure. Standardisation has also benefited performance and cost. For example, standardisation has helped expand product lines and lower costs of components, lowering prices for users. The most important area of standardisation is that of standardising the frequency bands used to provide communications. A de facto worldwide band has developed at 2.4 GHz (2400-2483.5 MHz). This has happened because this band is designated for industrial, scientific and medical (ISM) use. However co-existence with true ISM devices is detrimental to the development of WLAN services and other bands are being sought. The three bands at 5 GHz (Band A-5150-5350 MHz, Band B-5470-5725 MHz and Band C-5725-5875 MHz) are considered to be the best candidates. However, to promote the greatest economic development it will be necessary for all three bands to be allocated to this service on a worldwide basis. WRC 2003 will consider bands A and B, whereas C is not on the agreed agenda.

3.1 *Activities of industry groups*

Proprietary equipment for WLANs operating at 2.4 GHz was available as early as 1992, and systems were in use at that time. In Europe, the European Telecommunications Standards Institute (ETSI) published ETS 300 328 specifying basic parameters for operation of both FHSS and DSSS in that band in 1993.

In 1992, ETSI also began to consider further development of higher bit rate WLANs. From this work came the publication of HiperLAN1 in 1996 and more recently HiperLAN2. Both standards were intended for operation at 5 GHz following the allocation of spectrum in Europe by CEPT in this band for WLANs. In the US, the FCC subsequently allocated the same bands for WLAN.

The Institute of Electrical and Electronic Engineers (IEEE) 802 LAN/MAN Standards Committee has established a series of standards referred to as 802.x. The original 802.11 standard was set up in June 1997 as the technology which provides for data rates up to 2 Mbps at 2.4 GHz band, using either Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS). It targeted the case in which both the workstation and the network are owned by the same entity. In this context, it was more or less a "wireless extension" to existing wired LANs.²⁵

In 1999, however, the IEEE amended its standard to introduce 802.11b which enables 11 Mbps wireless communication at 2.4 GHz using DSSS modulation technology. At the same time, it also approved 802.11a, which specified radios transmitting at 5 GHz and at speeds up to 54 Mbps using Orthogonal Frequency Division Multiplexing (OFDM) modulation technology.

The 802.11b products came on the market first starting in late 1999 as DSSS technology is easier to implement than OFDM. Since then, 802.11b products have been widely recognised as the standard of WLANs. The maturity of WLAN technology based on the 802.11b standard has spawned a variety of reliable, reasonably priced wireless products. However, DSSS technology may not work well with Bluetooth technology (described later), and thus some newer developments to enhance the capability have been introduced. It is in this context that new 802.11a products are building momentum.

In May 2001, the IEEE started to discuss the next-generation 802.11g specifications. In July 2001, however, the IEEE delayed a decision on technology standards for the 802.11g WLAN products.²⁶ At the May 2002 session of the IEEE, it was agreed to try and finally approve the 802.11g in May 2003.²⁷

The ETSI established another specification called HiperLAN/1, which can provide data rates of 20 Mbps at 5 GHz. HiperLAN/2 is a new WLAN standard for this type, which provides for data rates up to 54 Mbps at a physical layer to a variety of networks. This high speed access has been made possible by exploiting OFDM technology, which allows the transmission of high data rates over adjacent channels at a low complexity. The HiperLAN2 and IEEE 802.11a standards are identical at the PHY (physical) layer. It is at the MAC (medium access control) layer that they differ. 802.11a implements the standard 802.11 MAC, while the HiperLAN2 MAC is a new design implemented to be compatible with ATM type operation.

There are some other complementary standards such as Hiperaccess, which can provide data rates up to 25 Mbps, and Hiperlink, which is for short-range high-speed interconnection up to 155 Mbps at 17 GHz over a distance up to 150 meters. These variations are also expected to play an important part in the future.

Other industry groups besides IEEE have also addressed WLAN technology and applications. They contributed not only to implementing standardisation but also to other aspects as well. For example, the Wi-Fi Alliance, former Wireless Ethernet Compatibility Alliance (WECA), created an interoperability testing laboratory and introduced a “Wi-Fi” seal of approval for 802.11b to ensure WLAN compatible technology. The Wi-Fi Alliance began certification testing for 802.11a products in July 2002.²⁸ The WLAN Interoperability Forum (WLIF) was also created in May 1996 to develop an open interoperability specification for WLAN devices. This forum is independent of the IEEE 802.11 committee and focuses on WLAN interoperability.²⁹ Furthermore, the Wireless LAN Association (WLANA), which consists of 10 members from the WLAN market, intends to create greater awareness of wireless technology. This association is trying to create awareness of the benefits and uses of wireless devices, and how they can serve as a competitive advantage in various vertical markets. The primary members are a group of component and equipment vendors.³⁰ Another industry group includes the HiperLAN/2 Global Forum (H2GF), which promotes HiperLAN2 as a standard in order to accelerate its use in business and consumer industries.³¹

The activities of industry groups will help increase awareness of WLAN technology. For instance, membership of WLIF is open to any company and it will enable a variety of WLAN vendors to collaborate to raise awareness of the technology. For the purpose of increasing awareness for WLANs, some groups design and publicise a wireless configuration. For example, the H2GF conducts and publishes testing in relation to interoperability among HiperLAN/2 products.

3.2 *Equipment standards for WLANs at 2.4 GHz and 5 GHz*

There is a confusing range of different equipment available for operation of WLANs. Across the world the lack of unified frequency bands and operating parameters means that there are wide variations in equipment availability and suitability. The main radio frequency bands used are around 2.4 GHz and 5 GHz. Infrared technology may also be used but has largely been abandoned due to the physical

constraints that use of infrared places on range and path. Each WLAN technology has its own advantages. Accordingly, it is very difficult to choose the best technology. The following table briefly summarises the main WLAN standards.³²

Table 1. Main WLAN standards

Standard	Frequency band	Year approved	Comments
IEEE 802.11	2.4 GHz	July 1997	Frequency hopping spread spectrum ~2Mbit/s
IEEE 802.11a	5 GHz	September 1999	OFDM but without dynamic frequency selection (DFS) 20-54 Mbit/s.
IEEE 802.11b	2.4 GHz	September 1999	Direct sequence spread spectrum up to 11 Mbit/s
IEEE 802.11g	2.4 GHz	To be approved	OFDM or Direct sequence spread spectrum up to 54 Mbit/s similar to IEEE 802.11a&b standards but in the 2.4 GHz band
IEEE 802.11h	5 GHz	Awaiting the results of the WRC	International agreement on DFS parameters was reached in January 2003 at the ITU. The WRC in July 2003 will consider mandatory use of DFS in harmonised international frequency allocations for WLAN at 5 GHz
HIPERLAN 2	5 GHz	Awaiting the results of the WRC	
Bluetooth	2.4 GHz		FHSS bit rate less than 1 Mbit/s
IEEE 802.16	5 GHz (band C)	In development at the moment	Closely associated with the European HIPERMAN standard and intended for fixed wireless access.
HIPERMAN	5 GHz (band C)	In development	

Source: OECD.

No single standard is likely to emerge in the future to support WLANs. As with all radio technologies, different equipment and protocols suit different applications. Some researchers also mentioned that these specifications would be developed to co-exist with one another rather than to replace each other.³³

802.11b

When creating a WLAN standard at the 802.11 Working Group established by the IEEE 802 Executive Committee, 802.11b emerged as an extension to 802.11 with data rates of 1 and 2 Mbps in order to satisfy future needs. While 802.11a was also an extension of 802.11, 802.11b has been given great attention by the industry as a standard for WLANs. As mentioned earlier, 802.11b is well known as “Wi-Fi” (wireless fidelity) and this seal will provide users the assurance that products bearing this logo will work together. At the present economic juncture of the ICT industry 802.11b has now become one of the bright spots for the telecommunications as well as PC industries. Indeed, it has been reported that the number of 802.11b users grew from almost zero in early 2001 to more than 15 million at the end of 2001.³⁴

The 802.11b standard uses DSSS and can provide data rates up to 11 Mbps at 2.4 GHz. Sales of network cards for laptop and desktop computers as well as Wi-Fi access points are increasing rapidly. One difficulty of this standard, which uses 2.4 GHz, is that this frequency band is subject to potential interference including other wireless technologies such as Bluetooth, HomeRF, microwave ovens, cordless phones, and amateur radio.³⁵ It has been suggested that it will eventually be replaced by products that have higher data rates as well as better quality of service and security.

802.11a

The 802.11a standard uses a more modern radio technology, orthogonal frequency division multiplexing (OFDM), to offer data rates up to 54 Mbps in the 5 GHz bands. This technology has several advantages in comparison with currently standardised 802.11b. First, it offers a faster bit rate. It can transmit data up to five times faster than 802.11b. The justification for higher transmission speed lies in the fact that wireless vendors have faced the challenges of supporting increasing numbers of applications that need large bandwidth access, such as streaming video. This feature will have the potential to let wireless access be used for the most demanding applications.

OFDM technology does not have the particular vulnerability of spread spectrum techniques to interference from similar systems. 802.11a has been developed in conjunction with the development of HiperLAN2. Both standards intend to make faster and more interference resistant use of the cleaner, more plentiful radio spectrum offered at 5 GHz.

The increase in speed also resulted in a technical challenge caused by “delay spread”. Delay spread is caused by the echoing of transmitted radio frequency. Radio signals are always refracted by objects such as walls, floors and furniture so that a baseband processor is required to unravel the divergent received signals. In this context, an innovative technique, OFDM, used in European digital TV and radio transmission, has helped solve this problem.

Secondly, 802.11a has a large capacity. Up to 12 (or 19 in Europe) non-overlapping channels are available in most 5 GHz bands, in contrast to only three channels in the case of 2.4 GHz band. The total bandwidth available in the 5 GHz band, 200 MHz (455 MHz in Europe), is higher than in the 2.4 GHz band, 83.5 MHz. Therefore, 802.11a can support more broadband users simultaneously without conflict. The higher capacity of this technology will better support densely populated areas.

However, despite these advantages, there are some disadvantages, especially in the early stages of use: higher cost, range constraints, and limited product support. In addition, a critical disadvantage of 802.11a would be the fact that it is not physically compatible with 802.11b. For example, a 2.4 GHz 802.11b access point cannot work directly with a 5 GHz 802.11a network card. Yet, it is possible for the two technologies to communicate. For example, 802.11a users and 802.11b users can be connected to the same LAN and share network resources including broadband Internet access provided that suitable radio equipment for both frequency bands is installed.

The principle and essential disadvantage of 802.11a is that it does not include implementation of two vital interference mitigation techniques known as dynamic frequency selection (DFS) and transmit power control (TPC).

TPC is a well-known technique whereby when a radio link has been established the equipment lowers the transmit power level to the minimum needed to maintain that link. It has benefits for mobile equipment because it conserves battery power thus increasing operational time between recharging. For the purpose of radio spectrum management, it has huge benefits in cleaning the spectrum. It may be estimated that the number of potential co-existing systems with TPC is of the order of double where it is not deployed. Lack of TPC has huge implications for the economic development of the mass WLAN market since ultimately there is a physical limit to the number of co-existing systems. The aim of good design is to increase that limit to permit greater development. TPC also plays an important role in limiting the cumulative levels of radiation in this band, known as the noise floor. As the noise floor rises at 5 GHz it will tend towards causing interference to satellite and radar systems. When it reaches a certain level it will no longer be possible for these services to co-exist and under the present radio regulations it will be WLANs that will be legally bound to withdraw.

802.11a also lacks DFS and for this reason it is unlikely to be permitted to be used in widespread deployment in European countries. It is also possible that its operation will be curtailed or restricted in the US as concern grows over its interference potential to radar operation and other services sharing the band. DFS enabled equipment monitors the radio channel for the presence of other users. On detection it backs off, selects another free channel randomly, and moves to it. It continues to monitor throughout. This has the effect of spreading use across all the available channels again maximising the numbers of co-existing users and protecting other services otherwise prone to interference from the OFDM signal, principally, radar. The specification for DFS has been developed at the ITU and will be an internationally recognised measure.

Lack of TPC and DFS is a fatal flaw in the 802.11a standard and it is very likely that it will be superseded by the 802.11h version, which does include them.

802.11g

The 802.11g standard is defined as a technology for operation at 2.4 GHz which provides higher data rates than 802.11b, up to 54 Mbps, using OFDM. This technology is as fast as 802.11a with more security as well as compatibility with 802.11b. This standard also supports complementary code keying (CCK) modulation and allows packet binary convolutional coding (PBCC) modulation as an option for faster links. Moreover, it has lower costs, thanks to lower-frequency devices that are easier to manufacture, and less path loss than 802.11a.

The disadvantage of 802.11g is operation in the already cluttered 2.4 GHz band. This leads to its lower capacity (fewer available channels) when compared with 802.11a. While the OFDM modulation technology allows higher speeds, the total amount of bandwidth available in the 2.4 GHz frequency remains the same. Unlike 12 channels which are available in the 5 GHz band, 802.11g is still restricted to three channels in the 2.4 GHz band. In this context, some argue that 802.11g is merely a migration path toward the ultimate goal of wireless connectivity at 5 GHz.³⁶

802.11h

This standard is supplementary to the media access control (MAC) layer to comply with European regulations for 5 GHz WLANs. European radio regulations for the 5 GHz band require WLAN products to have TPC and DFS. While some European countries, such as Germany, Ireland, Netherlands and the United Kingdom, are allowing the use of 5 GHz WLANs with TPC and DFS, harmonised use of 5 GHz at a pan-European level may be a slow process. In the US, the FCC is in discussion with military authorities regarding implementation of DFS to protect radar services. It appears likely, therefore, that 802.11h will supersede the current 802.11a MAC layer.

HIPERLAN

HiperLAN was developed in European countries as a high speed WLAN standard. There are two types of specifications: HiperLAN/1 and HiperLAN/2. Both specifications have been adopted by the European Telecommunications Standards Institute (ETSI). They provide similar features and capabilities to 802.11 standards. HiperLAN/1 was developed as early as 1996 and offers data rates up to 20 Mbps in the 5 GHz range of the radio frequency spectrum. It now, however, appears unlikely that it will be widely adopted since it is based on GMSK modulation (similar to that used for GSM) and in the intervening time technology has moved on. HiperLAN/2 offers data rates up to 54 Mbps in the same radio frequency band. The PHY layer is the same as that of 802.11a and the two committees co-operated in the development process. Since the lower throughput of the common 802.11a MAC limits its use especially with multimedia applications, HiperLAN's high bit rate, though it may cost more, may be an effective alternative

technology for certain WLAN applications, particularly those involving transmission of video images. HiperLAN is based on asynchronous transfer (ATM) technology, and can perform better quality of service operation than 802.11 WLAN.

MMAC

In Japan, Multimedia Mobile Access Communications Systems (MMAC) are being developed by the MMAC Promotion Council.³⁷ They intend to transmit data at a high speed with seamless connections to optical fibre networks and include the following sub-systems. Their systems have the following features.

- High speed wireless access: Wireless access system which can transmit at up to 30 Mbps using the SHF and other band (3-60 GHz), providing high feature video telephone.
- Ultra high speed wireless LAN: Wireless LAN which can transmit up to 156 Mbps using the millimetre wave radio band (30-300 GHz), providing high quality TV conferences.
- 5GHz Band Mobile Access: ATM type wireless access and Ethernet type wireless LAN using 5GHz band, providing multimedia data transmission at up to 20-25 Mbps for multimedia information.
- Wireless Home-Link: Wireless home-link which can transmit up to 100 Mbps using the SHF and other band (3-60 GHz), providing multimedia data transmission between PCs and audio visual equipment that transmits multimedia information.

Regional differences

There are different frequencies approved for use in the United States, European countries, and Japan. Any WLAN product must meet the requirements for the country in which it is sold. For example, the following table shows the different frequency range to be used for frequency hopping physical layer implementation.³⁸

Table 2. Difference in frequency range

Lower limit	Upper limit	Regulatory range	Geography
2.402 GHz	2.480 GHz	2.400-2.4835 GHz	North America
2.400 GHz	2.4835 GHz	2.400-2.4835 GHz	Europe
2.400 GHz	2.497 GHz	2.400-2.497 GHz	Japan
2.447 GHz	2.473 GHz	2.445-2.475 GHz	Spain
2.448 GHz	2.482 GHz	2.4465-2.4835 GHz	France

Source: Wireless LAN Association.

Frequency bands available internationally for 5 GHz WLAN services

The following table is a summary of the frequency bands that have been made available for 5 GHz WLANs in a number of regions of the world. Bands A and B are on the agenda of WRC 2003, where it is hoped that agreement will be reached on parameters for their use on a worldwide basis for WLANs.

Table 3. Frequency bands available internationally for 5 GHz WLAN services

Region	A1) 4900-5000 MHz	A2) 5150-5250 MHz	A3) 5250-5350 MHz	B) 5470-5725 MHz	C) 5725-5875 MHz (ISM)
USA	Not allowed (*)	U-NII band FCC Part 15 subpart E	U-NII band FCC Part 15 subpart E	Not allowed	U-NII band FCC Part 15 subpart E 5725-5825 MHz
Power limit		50 mW indoor only	250 mW indoor/outdoor		1W indoor/outdoor
Power limit eirp		200 mW	1W		4W (FWA) 200 mW (point-to-point with highly directional antennas)
Licensing		Unlicensed	Unlicensed		Unlicensed
Coexistence/ Etiquette		None	None		None
Canada	Not allowed	RSS-210 Issue 3 Par. 6.2.2 (q1)	RSS-210 Issue 3 Par. 6.2.2 (q1)	Not allowed	RSS-210 Issue 3 Par. 6.2.2 (q1) 5725-5825 MHz
Power limit-transmitter		None stated Indoor use only	250 mW		1W
Power limit eirp		200 mW	1W		4W (FWA) 200 mW (point-to-point with highly directional antennas)
Licensing		Unlicensed	Unlicensed		Unlicensed
Coexistence/ Étiquette		None	None		None
Europe	Not allowed	ERC Decision (99)23	ERC Decision (99)23 Allowed in specific countries	ERC Decision (99)23 Allowed in specific countries	FWA
Power limit eirp		200 mW Hipertan indoor use only	200 mW Hipertan indoor only	1W Hipertan indoor/outdoor	25 mW
Licensing		Licence exempt	Licence exempt	Licence exempt	Unlicensed
Coexistence/ Etiquette		20 MHz channels assigned DFS & TPC mandatory	20 MHz channels assigned DFS & TPC mandatory	20 MHz channels assigned DFS & TPC mandatory	-
Japan	Ministerial ordinance for radio equipment: Art. 49-21	Ministerial ordinance for radio equipment: Art. 49-20.3	Under study	Not allowed	Not allowed
Power limit eirp	Approximately 200mW (unlicensed)	200 mW indoor use only			
Licensing	Mobile stations: Unlicensed (except eirp exceeds approximately 200mW) Base stations: licensed	Unlicensed			
Coexistence/ Etiquette	20, 10, 5 MHz channels assigned	20 MHz channels assigned			

**Table 3. Frequency bands available internationally for 5 GHz WLAN services
(cont'd)**

Region	A1) 4900-5000 MHz	A2) 5150-5250 MHz	A3) 5250-5350 MHz	B) 5470-5725 MHz	C) 5725-5875 MHz (ISM)
Australia	Not allowed	SP 1/00 - May 2000 Radiocommunications Class Licence (Low Interference Potential Devices) 2000	SP 1/00 – May 2000 Radiocommunications Class Licence (Low Interference Potential Devices) 2000		SP 1/00 - May 2000 Radiocommunications Class Licence (Low Interference Potential Devices) 2000
Power limit eirp		200 mW indoor use only	200 mW indoor use only		1W
Licensing		Class licence	Class licence		Class licence
Coexistence/ Étiquette		None	None		None

Source: OECD.

Note: (*) 4940-4990 MHz is allowed to Broadband PPDR (Public Protection and Disaster relief).

3.3 *Radio technology*

Both radio frequency technology and infrared transmission may be used for WLAN implementation. Infrared transmission uses high frequency light waves to transmit data. This technology is cost-effective as well as inexpensive for short-range wireless communications, but it has not been widely accepted because of the limitations of range and its inability to cover an obstructed path. Several radio technologies have been proposed for WLANs.

Since, for economic reasons, most WLANs are based on deregulated and license-free operation often in bands used primarily for other radio services it has been necessary to implement technologies that are interference resistant.

Spread spectrum technology, which is a wideband radio frequency technique, has been a well adopted and successful modulation scheme. The theory of spread spectrum was originally postulated by the Hollywood actress Hedy Lamarr during World War II and was used by the western military until the 1970s to send concealed communications. In this technology, a signal is transmitted using a code that either spreads the signal across the whole available bandwidth or causes it to hop from frequency to frequency in a pre-arranged pattern. The specially designed receiver then removes the unique code preventing illicit eavesdropping. This technology makes the signal difficult to recover without knowing a proprietary spreading code. It also has the benefit of making the system very tolerant of interference from other types of radio system. The spread spectrum modulation system is designed to trade off bandwidth efficiency for reliability and security. While this technology will consume more bandwidth than in the case of narrowband technology, it can coexist with other radio systems without disruption. It is however very vulnerable to interference from other spread spectrum systems since errors can be introduced into the transmitted codes.

The 802.11 standard allows two types of spread spectrum modulation techniques: frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS). Both systems are defined for operation in the 2.4 GHz frequency band, typically occupying the 83.5 MHz of bandwidth from 2.400 GHz to 2.483 GHz. With regard to security, they use data encryption methods to prevent unauthorised access as well as user authentication procedures to prevent unauthorised users from gaining access to sensitive data. The choice between FHSS and DSSS will depend on various factors in relation to users' applications as well as the environment that the system will be operating.³⁹ FHSS is slightly more resilient in the presence of interference from similar systems, but offers a lower bit rate. DSSS, often referred to as "true spread spectrum", is extremely vulnerable to coding errors.

Frequency hopping spread spectrum (FHSS)

FHSS is a transmission technology which is used where the data signal is modulated with a narrow-band carrier signal hopping in a random but predictable sequence from frequency to frequency. The FHSS physical layer has a choice of 22 hop patterns. This technique uses traditional narrowband data transmission with a regular change of the transmission frequency.⁴⁰ The transmission frequencies are determined by a spreading or hopping code. The FHSS works by transmitting the signal carrier for a short period of time from one band to another.

With FHSS, the signal hops from one frequency to another at a predetermined rate known only to the transmitter as well as receiver. The frequency hopping appear random to anyone who is not aware of the pre-arranged hop pattern. Some countries specify the number of frequencies. In the United States, for example, the FCC regulations require manufactures to use 75 or more frequencies per transmission channel with a maximum dwell time (the time spent at a particular frequency during any single hop) of 400 ms.⁴¹ In comparison with DSSS, FHSS is more secure and is used more extensively in military forces. This is because the frequency used in DSSS is fixed and the security provided by the DSSS chipping code is limited.

Direct sequence spread spectrum (DSSS)

This technique broadens the bandwidth needed to transmit a signal by modulating the data stream with a spreading code. With DSSS, a redundant chipping code (bit pattern) is transmitted with each signal burst, and the chipping sequence is known only to the transmitter and receiver. If one or more bits in the pattern are damaged during data transmission, the original data can be recovered on account of the redundancy of the transmission.⁴² Basically, the longer the chip, the greater the probability that original data can be recovered.

DSSS has a better bandwidth and range compared with FHSS, which is currently from 2 Mbps up to 11 Mbps. In addition, DSSS is more resilient to unlike interference than FHSS. As a consequence, DSSS is more widely implemented in commercial WLAN products. Currently, it is not working well with Bluetooth technology. This is because it is extremely vulnerable to interference from similar systems.

There are also techniques for transmitting large amounts of digital data over a radio wave. One of the most important from the point of view of WLAN would be orthogonal frequency division multiplexing (OFDM).

Orthogonal frequency division multiplexing (OFDM)

OFDM is designed to minimise the interference, or crosstalk, among channels and symbols comprising data stream. It is significantly less sensitive to inter-symbol interference because a special set of signals is used to build the composite transmitted signal.⁴³ With OFDM, a signal is split into several narrowband channels at different frequencies. It breaks the ceiling of the data bit rate by sending data in a massively parallel fashion. It also slows the symbol rate while packing many bits in each symbol transmission, making the symbol rate substantially slower than the data bit rate. While OFDM has been chosen as the transmission method for the European radio (DAB) and TV (DVB-T) standard, 802.11a, 802.11g and HiperLAN/2 also use OFDM in their physical layers.

IV. SECURITY OF WIRELESS LANs

Originally, WLANs were not designed for public use and thus are not very secure. They were initially intended as a replacement for wired Ethernet office networks for ranges under 100 metres. In addition, as most companies operate WLANs without employing special security measures, customers relying only on the original Wi-Fi specification are vulnerable to hackers. As a consequence, the greatest challenge for WLANs is to enhance security. Indeed, it has been reported that more than half of all those surveyed admitted having experienced at least one type of WLAN security incident over the past year.⁴⁴ In a normal hot spot, for example, people can technically see the contents of other PCs that are connected to the same network. Moreover, most default settings for WLAN access points and client card software are thought to be at a level that mandates no security at all.⁴⁵

4.1 *Standard security features defined by IEEE*

The IEEE has developed WLAN security systems in addition to establishing a series of WLAN standards. It established a wired equivalent privacy (WEP) protocol to protect data in the course of wireless transmission using 40-bit keys between users and access points. WEP does not address end-to-end security but focuses on the wireless portion of the connection.⁴⁶ A primary goal of WEP was to provide security to verify the identity of users' stations. In this context, it seeks to provide access control to the network by rejecting access that cannot be appropriately authenticated. While it addressed both cryptographic and non-cryptographic approaches for the authentication, the latter approach is especially important for WLANs. Traditional wired LANs, such as IEEE 802.3 (Ethernet), did not include encryption systems for the security because they were protected by the physical security mechanisms within premises. WLANs are not protected by such a physical boundary because their transmissions are not contained within the premises of a building because they are radio-based. Because of this WEP encryption was added to the IEEE 802.11 standard to ensure a comparable level of security for wired LANs.

Protection of privacy was the second goal of the WEP. The intent was to prevent eavesdropping. The standard supports the use of cryptographic techniques for the wireless interface. Generally, the degree of security enhances as the cryptographic key size increases. However, it has been shown that this approach for privacy is more or less vulnerable to certain attacks regardless of the key size.

Another goal was to maintain the integrity of data. It seeks to ensure that messages are not maliciously modified by an active attack. Significantly, the standard specification does not address key management for 802.11b. Thus, generating, distributing and destroying the related materials is left to those deploying WLANs. As a result, even if an enterprise recognises the necessity to change keys often, the task cannot be effective in a large WLAN environment.

IEEE 802.11 Task Group I (IEEE 802.11i) is currently working on extensions to WEP for incorporation within a future version of the standard. The Wi-Fi Alliance, or former Wireless Ethernet Compatibility Alliance (WECA), also formed a security subcommittee that is working closely with IEEE Task Group I. The goal of this subcommittee is to develop an interim solution that will be secure against attacks before the IEEE 802.11i standard is complete.

Some newer 802.11b products incorporate a system informally known as WEP2, which has been renamed by the IEEE as temporal key integrity protocol (TKIP). It uses 128-bit keys, but is compatible with WEP, and therefore vulnerable to the same attacks.⁴⁷

In October 2002, the Wi-Fi Alliance announced a new security specification on the basis of an IEEE standards effort called Wi-Fi Protected Access (WPA) to replace the WEP, which is expected to appear in Wi-Fi certified products during the first quarter of 2003. While IEEE 802.11i is working on a new and more effective security standard, it is not expected to ratify it until September 2003. The WPA includes mechanisms from the emerging 802.11i standard for both data encryption and network access control, with which users will have their own encryption key that can be set to change periodically. The Wi-Fi Alliance plans to adopt the full 802.11i standard as version 2 of WPA and start certification in early 2004.⁴⁸

4.2 Vulnerabilities and risks

Broadly speaking, all LANs are vulnerable to two types of attacks: active attacks, in which hackers gain access and can destroy or alter the data, and passive attacks, in which hackers gain access but can only eavesdrop on the data transmitted.⁴⁹ In either case, WLANs are more susceptible to these vulnerabilities than wired LANs.

WLAN security risks include: loss of data integrity, interception of wireless traffic, and unwanted access. Due to these risks, some defence-related institutions began to prohibit the use of WLANs. For example, Lawrence Livermore National Laboratory in California, a research institute for national defence based in the US, prohibited WLAN use because of security problems. Similarly, Los Alamos National Laboratory in New Mexico, a research institute for national defence based in the US, is reportedly also considering the prohibition of WLAN use.⁵⁰ Increasing WLAN security will help in increasing user confidence and in the longer term growth of this technology.

V. ALTERNATIVE WIRELESS TECHNOLOGIES

5.1 Bluetooth

Bluetooth wireless technology has been identified as a potential mass market user of the 2.4 GHz band. Originally developed by Ericsson Mobile Communications in 1994, it was designed to interconnect devices such as cellular phones, laptops, and PDAs with home and business phones as well as computers using short-range connections. Thereby it is touted as a low-cost, low-power, and low-profile technology.⁵¹ The Bluetooth Special Interest Group (SIG), which comprised companies such as Ericsson, IBM and Toshiba, created the first Bluetooth specification in July 1999. Both 802.11b and Bluetooth radios share common spectrum in the 2.45 GHz ISM band, but Bluetooth uses FHSS transmission. The target of both radio types are mainly business users. In the ISM band, Bluetooth technology is able to transmit data in a speed of up to 1 Mbps and achieves a throughput of approximately 720 Kbps.

While the roles of both technologies are to allow transmission of information between devices by a radio link, there is a clear difference in their roles. It is range of communication, which is used to differentiate between wireless technologies. While WWAN technologies, including cellular phones such as GSM, GPRS, CDMA etc., would be characterised by long range and high power consumption, WLAN technologies are suitable for the usage at medium power and medium range. Wireless Personal Area Network (WPAN) technologies have low power, short range consumption, and Bluetooth is also included in this area. Bluetooth can be used to connect almost any device to any other device within the range available.

Bluetooth has a range of approximately 10 metres compared with WLANs' range of up to 100 meters. Bluetooth is not intended to allow free-roaming users access to wireless networks. This limitation has reduced the popularity of Bluetooth in businesses and homes compared with the 802.11b standard. The following table summarises three classes of power management that Bluetooth provides.

Table 4. Classes of Bluetooth device and power management

Type of device	Power level	Estimated operating range
Class 3 devices	100 mW	Up to 100 metres
Class 2 devices	2.5 mW	Up to 10 metres
Class 1 devices	1 mW	0.1-10 metres

Source: Palowireless.

Bluetooth networks enable a so-called “master-slave relationship” maintained between network devices. Up to eight devices can be networked together in a master-slave relationship called “piconet”. In a piconet, one device plays a part of the master of the network with up to seven slaves connected directly to the network, thereby creating a chain of wireless networks. The master device controls the network, where devices in the piconet operate on the same channel and follow the same frequency hopping sequence. While Bluetooth permits the establishment of both peer-to-peer networks and networks based on fixed access points, the most popular use would be to interconnect mobile devices that are in the same area.

Like WLANs, Bluetooth has a number of benefits for users. For example, Bluetooth can replace cables for a variety of interconnections. It also enables file sharing between available devices. Bluetooth is supported by a variety of devices. Bluetooth may be used with a laptop, handheld device, desktop or any other types of available device. Bluetooth is expected to be utilised in office appliances and home appliances, in which a variety of applications are created including wireless conference rooms or wireless Internet banking.

There are some disadvantages in the use of Bluetooth. As noted above, its range is apparently much shorter than 802.11b. In this context, some contend that Bluetooth will never pose a serious threat to 802.11 equipment. In addition, costs for Bluetooth chips and other components are still high. With regard to security, Bluetooth did not address security services other than basic services such as ensuring authentication and protection of privacy. Therefore, other means to ensure security would be required to gain the confidence of users.

One of the most critical points for the use of Bluetooth is interference with 802.11b. It has been suggested that mutual interference between them will occur if the signals of both systems overlap in both frequency and time. Moreover, both technologies apply packet transmission and time division duplexing, which means that the transmission is intermittent.⁵² While it is true that they cause interference with each other, it is the nature of radio links to experience interference.⁵³ Technically speaking, both 802.11b and Bluetooth can coexist inasmuch as both devices located near each other do not use the same frequency at the same time. In addition, both technologies have extensive error checking and the ability to retransmit packets in case of occurrence of errors. Therefore, the consequence of interference, if any, is not lost data but decreased throughput.⁵⁴ Furthermore, the interference can be limited in itself because of different types of spread spectrum modulation techniques as well as incomplete overlap of the frequency sub-bands used. It has been reported that 802.11b would degrade to its slowest speed of 1 Mbps at worst cases and Bluetooth could suffer a 22% degradation of its 1 Mbps maximum data rate.⁵⁵ However, considerable degradation may well be significant for the operation of certain applications and could cause service failure.

In the meantime, some studies show that there is only a partial overlap between Bluetooth and 802.11b, and even with UMTS, and that these technologies are largely complementary from a market perspective.⁵⁶

5.2 HomeRF

HomeRF is a home networking standard developed by Proxim Inc. that combines the 802.11b and Digital Enhanced Cordless Telecommunication (DECT) portable phone standards into a single system.⁵⁷ While 802.11b was fundamentally designed for the corporate environment, HomeRF was developed to satisfy the needs in home networking applications from the outset. The specification was developed by the Home Radio Frequency Working Group as shared wireless access protocol (SWAP). It allows PCs, cordless telephones and other consumer devices to share and communicate voice as well as data in and around the home without the expense of running new wires.⁵⁸ HomeRF transmits data up to 10 Mbps with a range of up to 50 meters.⁵⁹ This range might be too short for most business users, but will be suitable for home applications. By the end of 2002, HomeRF proponents expect to achieve a data rate of 20 Mbps or faster. Some argue that HomeRF may be better as a technology to handle multi-media data than 802.11b.⁶⁰

HomeRF 2.0 uses a frequency hopping technology, which keeps the “data channel” shifting from one frequency to another many times a second. This technology is expected to make it very hard for someone to eavesdrop on the network. Also, HomeRF 2.0 has introduced the concept of a “network password” needed to join the network.

Using 2.4 GHz ISM band, HomeRF is subject to interference from other devices using the same frequencies such as 802.11b. However, HomeRF 2.0 does not interfere with Bluetooth technologies. It has been reported that HomeRF offers superior scalability in larger installations thanks to its frequency hopping technology, with support for up to 15 overlapping networks compared with three for WLANs.

5.3 3G

In some OECD countries, such as Japan, nationwide 3G wireless networks have already been rolled out. In Japan and Korea, there are reportedly nearly 5 million 3G users respectively.⁶¹ The progress of European carriers is relatively slow, but a number of countries have moved from so-called 2G to 2.5G in late 2000 and are developing their 3G infrastructure. The 3G system promises speeds up to 2 Mbps, but it is expensive to deploy the infrastructure.

It has been suggested that 802.11b applications will be a threat for 3G operators. Some point out that deployment of 3G mobile data network might be delayed significantly as carriers look to 802.11-based networks.⁶² One of the reasons behind these arguments is the fact that Wi-Fi is up to 30 times faster and arguably less expensive in terms of building and maintaining a network than 3G. In addition, WLANs are originally designed not as a system for supporting mobile users but as a simple cable replacement. What is more, unlike 3G, WLAN is the bottom-up technology rolled out by firms with no plans to make a profit in the telecommunications business. For example, firms introducing the Wi-Fi service throughout their stores are doing so to attract customers rather than as a means of entering the broadband business.

However, the Wi-Fi’s “threat” to 3G may be somewhat overstated. The biggest drawback facing WLAN providers would be the uncertainty surrounding WLAN service models for public access.⁶³ In addition, some technical issues such as access to radio spectrum, billing, roaming and security can also slow down the commercial development of WLANs.

On the contrary, some contend that Wi-Fi is far from a threat to 3G regardless of its uncertainty in the market. For example, the German regulator RegTP mentioned that these two systems would supplement each other effectively for the benefit of all market players.⁶⁴ Some view WLAN and 3G as complementary technologies that will result in more demand for frequencies in the 5 GHz band for new WLAN applications in addition to those in the 2.4 GHz band. Using WLAN frequencies for public applications can be in the interest of UMTS and can lead to success of UMTS. In particular, it has been suggested that 3G is

a more consumer-oriented technology whereas WLANs are arguably more focused on enabling those applications that are most demanded by businesses.⁶⁵ Moreover, WLANs are designed for provision of broadband access in small areas, which is contrary to the mobile networks, which cover wide areas across the country. In other words, 3G systems will be designed for ubiquitous coverage and true mobile use for vehicles (*i.e.* handing off from one cell to another), whereas Wi-Fi is really designed for short-distance use. While some companies are developing technology such as mesh networks that they claim will provide coverage to vehicles, the technology is still largely in development and unproven. The main advantage of UMTS is its mobility rather than the transmission rates. Furthermore, seamless roaming capabilities between 802.11b and 3G (UMTS) were demonstrated in September 2002.⁶⁶ This successful testing will enable mobile users to browse the Internet while roaming between Wi-Fi and 3G with no interruption in the session. Therefore, these two systems, intended for different purposes, can coexist and allow users to access essential broadband applications.

VI. IMPLICATIONS FOR REGULATION

6.1 *Potential issues for regulation*

The most critical issues for regulation would be whether WLAN operators need to be licensed or would require only approval or registration to enter the market. Currently, the use of 2.4 GHz band for 802.11b services requires no licence in a number of OECD countries, but some European countries seem to be taking the approach that only telecommunications operators licensed by the government can operate commercial WLAN networks. It would be preferable in order to stimulate WLAN growth to follow simple market entry procedures, such as allowing entry through equipment registration. It is likely that imposing excessive licensing requirement could slow down market competition and delay further development of WLANs. From this perspective, for example, the US uses a registration approach for approving equipment for non-licensed operation under Part 15 of the US Code of Regulations for Telecommunications (Title 47). However, it is important to mention that “unlicensed operation” means the devices must not cause harmful interference to other devices and must accept any interference received. There need to be some minimum requirements in order to ensure that regulators know who the market entrants are, can ensure that there is no frequency interference and, if necessary set some minimum standards for quality and/or security. Some form of entry control may eventually be necessary as a result of limitations on frequency. However, the most desirable way to ensure the security and quality of services would be through market competition.

It is also important to ensure the availability of radio spectrum for the provision of WLAN services. Based on the assumption that giving resources to businesses to create and deliver wireless services to benefit the public is essential, some OECD governments have recently taken action. In Japan, for example, the government has amended the relevant regulations to allow the outdoor use of the 5 GHz band for WLAN services. In the United Kingdom, the government has approved the expansion of the radio spectrum available by opening bands at 5 GHz to offer WLAN services.⁶⁷ In France, the regulator ART defined the conditions of provision of WLAN services at the band of 2.4 GHz in November 2002. By this decision, the service operators can install terminals for access using technologies in the 2.4 GHz band without authorisation.⁶⁸ In the United States, the Consumer Electronics Association (CEA), an industry group representing electronics manufacturers, called for the FCC to allocate additional spectrum in the 5 GHz band for unlicensed devices in July 2002.⁶⁹ It noted that the unlicensed spectrum below 5 GHz is becoming increasingly crowded and congested and that an additional 5 GHz allocation would encourage continued development of home networking technologies such as 802.11a. The FCC is considering this request.

Regulators need to be aware that use of radio spectrum for WLANs is a complex issue. The legal obligations on governments to protect the named primary users stem from radio regulations which constitute an international treaty. No spectrum is currently allocated to WLANs, so WLAN operators have to meet rigorous obligations in order to gain access to spectrum. Some of these restrictions may be lifted after the WRC 2003 if an international allocation at 5 GHz is agreed.

Some satellite broadcasting companies asked the regulator to impose some further regulations on Wi-Fi makers to avoid interference from radio signals. In the United States, for example, Sirius Satellite Radio and XM Satellite Radio have asked the FCC to act upon their request to minimise interference. At 5 GHz, satellites have a primary allocation and the FCC must consider this legal obligation. However, WLAN proponents claim that they should not face more regulations or add something to their equipment that could increase the cost because they cause no problems. For the moment, the FCC has taken no action on that in view of the fact that Wi-Fi networks are currently at an early stage. In Florida, a hamradio operator went to court to shut down a WLAN operator on the grounds that the apartment dwellers using this form of access were interfering with his radio.⁷⁰ Again, the ham has an official frequency allocation and therefore his interests have precedence. The electrical lighting industry also petitioned the FCC to permit the use of radio spectrum in a manner that would create difficulties for WLANs. Lights are ISM devices and may operate as they wish in ISM designated bands. Regulatory involvement might become necessary if clear evidence shows that interference problems can occur.⁷¹ At 2.4 GHz, there is significant anecdotal evidence of interference problems. In the United Kingdom, the RA is to conduct a monitoring exercise in an attempt to quantify the extent of the problem. The interference problem might be reduced when 5 GHz technologies, such as an 802.11a standard, are adopted in preference to the crowded band at 2.4 GHz. However, 802.11a operates in a frequency range occupied by US government radar systems and is facing similar concerns by other incumbent spectrum users.⁷²

Regulators must set parameters for the operation of WLANs that take account of the existence of other services sharing the spectrum while still permitting development of economically viable services. Thus the regulatory regime must not be too onerous but of course must take account of the physical problems of radio propagation in the face of unknown and presumably dynamically increasing levels of interference. To this end it is necessary for regulators to set basic radio parameters and other technical regulations that minimise the potential for system failure due to interference.

Wi-Fi networks allow a single paying subscriber to set up a local network that allows third parties to access the Internet. This has resulted in "neighbourhood networks". Any potential user passing by the vicinity of the signal can access the network free of charge without a password. Moreover, there are tools that amplify the radio signal to enable the delivery over an even larger area, such as public parks or a university campus.⁷³ The potential issue raised by the creation of such hot spots is whether they should be prevented or whether these hot spots should be ignored in the context of policy and regulations.

Although making available a free wireless network without the consent of the network provider or Internet service provider raises a number of legal implications, the costs in trying to monitor and control such hot spots are high. It is difficult to know how many of these "free wireless networks" are being operated. At the same time, the situation is complicated by some small Internet service providers which have promoted free wireless usage, expecting that their increase in customers can offset potential revenue loss from free-riding. Broadband providers in the United States are trying to crack down on Wi-Fi customers who set up WLAN systems that allow third parties to access Internet for free. In New York, for example, Time Warner Cable has identified 10 customers sharing bandwidth and cut off their services.⁷⁴

Wireless networks also raise legal issues related to the right to use public or private property to offer services. When operators intend to install necessary equipment for provision of WLAN services in public places such as airports and train stations, they have to use the property of a third party. In this case, they can be refused by the owner unless regulations allow operators to provide such services without the consent of a third party (*e.g.* as is the case for mobile telecommunication services where signals cannot be legally blocked in most countries). In Japan, for example, the Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT) did not approve the application from Mobile Internet Service Co. to make a consultation to install equipment for WLAN services in some train stations in Tokyo in August 2002. According to the Ministry, installation of the WLAN equipment inside the station is apparently aimed at providing “users in the property”, *i.e.* train users, with wireless services, which is not permitted under the existing telecommunications business law.⁷⁵ This type of regulation is likely to discourage WLAN companies from investing and could slow down the development of WLAN services. The right of WLAN service providers to use public spaces for the provision of services is an issue that needs to be examined and clarified. The legal basis for such use is likely to vary widely among the OECD countries. A related issue is the deployment of networks in private property, which is for public use (railway stations, airports, etc.).

Further reflection is needed to determine whether there are any policy implications that arise between 3G and WLAN services. The two services are both complementary and competitive but are subject to quite different regulatory frameworks. The most significant difference is that 3G operators have paid for spectrum as well as a mobile licence whereas WLAN providers are using mostly unlicensed spectrum. Does this result in asymmetric regulation? This would depend on the extent to which the two services are competitive rather than complementary. There will also be significant differences between the two services in terms of geographical coverage, and the fact that 3G users can access services in all public places whereas commercial WLAN service providers may need to obtain permission from railways, airports, commercial shopping areas, etc. to be able to provide services. Unlicensed spectrum cannot provide a defined quality of service since the radio environment is inherently unpredictable so a WLAN cannot be used to provide services that include a service obligation to the end user.

6.2 Regulatory frameworks and initiatives by OECD countries

One of the important points for regulators is to review the regulatory frameworks and initiatives taking into account the development of WLAN technologies and services. As noted earlier, the past few years have witnessed the development of a variety of industry standards among OECD countries, which is expected to expand the number of devices that will operate in the 2.4 GHz band. In terms of spectrum rules, for example, the regulations should allow for greater sharing of the spectrum by all devices in this band by removing unnecessary barriers to the introduction of non-interfering technologies. It should be noted that the regulations should be designed to provide WLAN market with the flexibility and a more diverse set of products that can operate efficiently in the unlicensed bands while controlling interference among spectrum devices.

International Telecommunication Union (ITU)

In order to guarantee the future growth of wireless LAN services, it is important for OECD countries to take the lead on Spectrum Harmonisation efforts, which will be discussed at the World Radiocommunication Conference (WRC) in June 2003. Agenda Item 1.5 is the Agenda Item that covers the mobile allocation of the 5150 - 5350 and 5470 - 5725 MHz to WLAN services. A worldwide allocation in these 5 GHz bands would allow manufacturers to be able to produce cheaper devices due to the economies of scale of developing the same devices for a single global marketplace. At the moment the European countries and countries in the Asia-Pacific region have indicated that they fully support a worldwide allocation to be made for WLANs in 5GHz at the WRC. The US position at the moment is to

make an allocation in 5150 – 5350 MHz at this conference and tentatively to support an allocation in 5470 – 5725 MHz similar to that already adopted in Europe if Dynamic Frequency Selection is proven to protect Radar Systems.

Australia

In Australia, there are three types of radio communications licences in addition to carrier licences: apparatus licences, class licences and spectrum licences. While apparatus licences authorise the operation of radio communications equipment for specific purposes, class licences will allow anyone to operate particular radio communications equipment. Spectrum licence is a form of licensing introduced by the Radiocommunications Act 1992, which authorises the use of spectrum space and give licensees the freedom to deploy any device service from any site within their spectrum space. WLAN providers, or users of WLAN devices, have been licensed to operate any of the spread spectrum transmitters used in the 2.4 GHz band under the class licence. They are also required to comply with a prescribed set of conditions that are intended to avoid destructive interference between users. However, WLAN operators that provide services in a single premise or on a non-commercial basis will be exempt from having to apply for carrier license, following the determination made in September 2002 by the Communications Minister. It is intended to preserve technological neutrality as well as encourage innovation. This decision removed an anomaly under which cable networks on single premises do not require carrier license whereas wireless networks on single premises did.

Austria

The allocation of frequencies for WLAN operation is regulated by the Austrian Regulatory Authority for Telecommunications and Broadcasting (RTR). A general license is granted for the use of WLANs that comply with the relevant technical parameters laid down in the radiointerface descriptions FSB-LD046 (WLANs in the 2.4 GHz frequency band) and FSB-LD407 (WLANs in accordance with 802.11a and HiperLAN Type 1). Most of the WLANs in Austria operate in accordance with the FSB-LD046 using the 2.4 GHz frequency band. The maximum equivalent isotropically radiated power is restricted to 100 mW, which is mandatory for access points as well as for wireless stations and may not be exceeded. This 2.4 GHz frequency band is not exclusively assigned for operation of WLANs. It is also used for other wireless applications, such as Bluetooth, as well as microwave ovens. Accordingly, the regulator does not exclude the possibility of interference in the operation.

The “indoor” operation of devices, which corresponds to FSB-LD047, is generally licensed. It should be noted that FSB-LD047 is only applicable for the frequency band 5150-5250 MHz. Since the frequency band 5470-5725 MHz is not available for civil applications, it is prohibited to operate HIPERLAN Type 2 devices at present.⁷⁶

Belgium

The use of WLAN equipment using both 2.4 GHz and 5 GHz is exempt from a licence if the legal dispositions, such as power output restrictions, are respected and the equipment has been notified by the manufacturer to the telecommunications regulator. With regard to wireless network deployment, the regulatory frameworks vary according to the type of networks. Private communication networks are subject to registration if they cross public territory and if these links exceed 300 meters, but otherwise no registration is required. Public communication networks are subject to an authorisation, but only registration will be required after July 2003. Community-based wireless networks, so-called “citizens networks”, do not require registration, but generate some concerns as often “home-made” equipment that does not comply with legal restrictions is used, such as in the case where power output is considerably

exceeded. Concerning standardisation, the Belgian approach is pragmatic based on market development, but it supports European standardisation efforts, mainly for security reasons.

Canada

Most WLAN products in Canada are operated in the 2.4 GHz license exempt band (2400-2483.5 MHz). This band has been open for many years, however only since the recent industry adoption of the IEEE 802.11b standard have opportunities for new and innovative suites of consumer equipment become available. This segment of the market is growing fast, and because of the license-exempt nature of the spectrum, there is some congestion in large urban centers resulting in interference with various products operating in the same band.

To ensure that Canadians are provided with the most advanced communications facilities and devices, in 1999 Industry Canada designated 300 MHz of spectrum in the 5 GHz band for the operation of license exempt wireless local area networks.

- The 5150-5250 MHz band includes a maximum EIRP of 200 mW (further limited to 10 mW in any 1 MHz band) and is limited to indoor use only.
- The 5250-5350 MHz band includes a maximum EIRP of 1 W; a limit of 250 mW transmitter power; and a power spectral density of 11 dBm in any 1 MHz band.
- The 5725-5825 MHz band includes a maximum EIRP of 4 W a limit of 1 W transmitter output power; and a power spectral density of 17 dBm in any 1 MHz band.

These bands are harmonized with the North American market place and beyond. Consumer networks mainly support neighbourhood point-to-point and point-to-multipoint high-speed wireless services in a cost-effective manner. These networks will enhance Canada's information infrastructure by facilitating wireless access and distribution, the creation of new wireless local area networks and a broad range of new products and service offerings. Emphasis is on applications for high-speed broadband multimedia comprising of voice, video and data.

EU

The EU Commission urged governments in France, Greece, Italy, Luxembourg and Spain to lift the prohibitions they have placed for WLANs in August 2002.⁷⁷ It indicated to the five countries that any unfair restrictions in the use of WLAN technology could be in breach of EU law.

Finland

The Finish Communications Regulatory Authority identified the 5 GHz frequency band for WLANs in compliance with the European HIPERLAN frequency decision. The frequency is applicable in the bands 5150-5350 MHz and 5470-5725 MHz. The radio frequency plan does not restrict the usage of these frequency bands for any other technologies than that of the HIPERLAN standard. Therefore, other wireless technologies may be used as far as the equipment does not interfere with other radio services more than equipment of HIPERLAN standard does. On the basis of the European HIPERLAN decision, the following technical requirements have been stipulated: *i*) in the frequency band 5150-5350 MHz, 200 mW equivalent isotropically radiated power is allowed for WLAN transmitters. In this band range, the equipment must only be used indoors. *ii*) in the frequency band 5470-5725 MHz, the corresponding limit is 1 W.

The Authority also identified other frequency bands, *i.e.* 3.4-3.6GHz, 10.15-10.3/10.5-10.65 GHz, 24.5-26.5 GHz, for broadband data transmission.⁷⁸

Germany

The Regulatory Authority for Telecommunications and Posts (Reg TP) concluded that WLANs would not pose a threat to UMTS competitively and that the two systems would complement each other effectively for the benefit of all market players. On this basis, Reg TP is prepared to provide further frequencies in the 5 GHz band for new WLAN applications in addition to those in the 2.4 GHz band. Before the decision, however, a public consultation process on the proposed general frequency assignment in the 5 GHz band was organised in July 2002 in order to ensure transparency of policy.⁷⁹ In November 2002, the RegTP published a general assignment of frequencies in the bands of 5GHz (5150 MHz – 5350 MHz and 5470 MHz – 5725 MHz) for general use of WLANs free of charge.

France

The French regulation allows private use of WLANs in the 2400-2483.5 MHz and 5150-5350 MHz bands under certain technical conditions. The regulator ART launched a public consultation process in December 2001 for the use of WLANs. This consultation aimed at examining the possibility of supplying telecommunications services using frequencies in the 2.4 and 5 GHz bands, which had been reserved for private networks, to the public. The ART announced in June 2002 that it would allow the creation of public WLAN hot spots in the 2.4 GHz and 5GHz frequency bands.

In November 2002, the ART adopted the decisions defining the conditions for WLAN use in the 2.4 GHz band. These decisions allow private companies, local governments and individuals in certain regions to provide both indoor and outdoor coverage in public spaces with high Internet traffic such as airports. In a number of areas⁸⁰, WLAN providers will be able to install the terminals of access without authorisation using technologies in the 2.4 GHz band with the following technical conditions:⁸¹

- The 2400-2454 MHz band is usable for outdoor use with a power lower than 100 mW (milliwatts).
- The 2454-2483.5 MHz band is usable for indoor use with a power lower than 100 mW and outdoor use with a power lower than 10 mW. For the private properties, this power can reach 100 mW for outdoor use with an authorisation of the Ministry of Defence.

The Minister of Industry approved the decision of the ART in December 2002, and this was published in the Official Journal in January 2003.

Ireland

The regulator, the Office of the Director of Telecommunications Regulation (ODTR), published a policy on “Strategic Management of the Radio Spectrum in Ireland” in May 2002. This policy stipulates that the use of permitted short range devices including WLANs is on a non-interference and non-protected basis. Namely, users of such spectrum must not cause interference to other authorised spectrum users and they cannot claim protection from interference from such services. The ODTR submitted a proposal to the Electronic Communications Committee (ECC) to consider the use of the frequency band of 5.8 GHz for WLAN devices to facilitate wireless access applications.⁸²

After the public consultation process, the ODTR finally established an order to exempt from licensing devices for provision of WLANs as well as FWA in the 5.8 GHz band in July 2002. This order also covers exemption from licensing devices for the provision of indoor WLANs in the band of 5150-5350 MHz utilising technologies such as 802.11a.⁸³

Japan

Most of the WLANs in Japan use 2.4 GHz band at present, largely because the band was implemented earlier. In order to cope with enhanced capability of the 2.4 GHz band WLANs by introducing the OFDM modulation method, the government has decided to amend the relevant regulations in January 2002. This has accelerated use of the WLANs in Japan.

Concerning the 5GHz band, the government decision in March 2000 to introduce indoor use of WLAN systems at the 5.2 GHz (5.15-5.25 GHz) band added momentum to the use of 5 GHz band WLANs in Japan. In October 2000, outdoor use of WLANs in the 5.3 GHz (5.25-5.35 GHz) band was not implemented, as the Telecommunication Technology Council of the former Ministry of Posts and Telecommunications (MPT) submitted a report indicating a potential interference with earth exploration satellites and weather radars. With the further demand to outdoor use of WLANs in the 5 GHz band, the Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT) decided to amend the relevant regulation in August 2002 to implement the outdoor use of the 5 GHz band (4.9-5.0 GHz and temporary use of 5.03-5.091 GHz until 2007) for WLANs after the sharing and compatibility studies with other existing services in the Telecommunication Council.⁸⁴ This is likely to stimulate the spread of WLANs and hot spot services in Japan.

In addition to the above, the 1000 MHz of quasi-millimeter wave band (24.75-25.25 GHz, 27.0-27.5 GHz) and 7000 MHz of millimetre wave band (59-66 GHz) are also available for WLAN systems, requiring no radio station license.

Furthermore, the MPHPT is drafting a mid-term to long-term strategy on the radio spectrum usage, the "radio policy vision" in order to establish a blueprint for reallocation of the radio spectrum for use by future wireless telecommunications networks. This is expected to be set up around mid-2003.

Korea

The Ministry of Information and Communication (MIC) established a 2002 Internet Initiative, which aimed at helping users to log on to the Internet anywhere, anytime, through mobile handsets, PDAs and notebook PCs, taking full advantage of the leading wireless and fixed-line Internet infrastructure in the world. In line with this initiative, the Ministry mentioned in May 2002 that it would jumpstart WLAN services among general public.

United Kingdom

In July 2002, the Radiocommunications Agency (RA) further deregulated the 2.4 GHz band to permit licence exempt operation of WLAN devices for commercial public access services. Previously only services operated for non-commercial reasons were permitted to operate under the licence exemption and other services required a licence to use the band. All equipment operating under the licence exemption must meet the technical parameters specified in Interface Requirement IR 2005. Equipment operators must also meet the requirements of the Telecommunications Act and some operators may therefore require specific authorisation to provide services.

At 5 GHz, following extensive public consultation, Bands A and B have been opened on a licence-exempt basis for the operation of mobile and nomadic services. Equipment must comply with Interface Requirement IR 2006, which was published in October 2002.

Band C at 5 GHz is still under study. It is intended that it will be opened for operation of short range Fixed Wireless Access services under similar technical parameters to those applied to band B. Since this service is intended to operate outdoors and at higher powers than those permitted in bands A and B, a light licensing regime has been proposed with the aim of providing co-ordination information to all operators and potential operators of services and to protect other services currently using this band. A separate Voluntary National Standard will be applied to this band. It is anticipated that the work to open the band will be completed by the middle of 2003. For all bands at 5 GHz a requirement for both DFS and TPC will be applied.

United States

In the United States, there has been intensive discussion on regulations for spectrum management to allow WLAN services. The rules on spread spectrum have been revised several times in order to accommodate technological developments and to promote innovative use of such bands as 915 MHz, 2.4 GHz, and 5.7 GHz. Two facts demonstrate the needs to modify the rules. First, the data rates achievable by spread spectrum devices have increased over the past years, which were not envisioned in the original rules. Second, the original rules were established in such a manner to highlight the interference immunity features of spread spectrum devices at the expense of higher speeds.

Devices operating in the 915 MHz (902-928 MHz), 2.4 GHz (2400-2483.5 MHz), and 5.7 GHz (5725-5850 MHz) bands have been unlicensed. In these non-licensed radio frequency devices, operation had been limited to FHSS and DSSS, both of which were permitted to use output powers of up to 1 watt under Section 15.247 of the FCC's rules. Yet most devices used lower power for various reasons, such as conserving battery life. Before 2002, digital modulation systems had not been allowed to operate because they did not meet the FCC's definition of a spread spectrum system.

The US rules permitted FHSS to operate in the 2.4 GHz band with a maximum output power of 1 watt. They specified that FHSS operating in this spectrum must use a minimum of 75 hopping channels with each channel having a 20 dB bandwidth no greater than 1 MHz, in order to avoid interference.⁸⁵ In response to the request filed by the HomeRF Working Group that FHSS operating in the 2.4 GHz band be permitted to use bandwidths of up to 5 MHz, the FCC published a Notice of Proposed Rule Making, allowing for the wider bandwidths in June 1999. The FCC believed that this suggestion would facilitate high-speed data links for such applications as WLANs. Under this proposal, the systems would utilise 75 hopping channels.⁸⁶

In August 2000, the FCC decided to release the First Report and Order to permit the wider bandwidths for FHSS. It allowed FHSS in the 2.4 GHz band to use bandwidth between 1 MHz and 5 MHz at a reduced power output of up to 125 mW. These wideband FHSS systems were allowed to use as few as 15 non-overlapping hopping channels provided that the total span of hopping channels is at least 75 MHz, because use of 75 hopping frequencies was generally not feasible for systems having a bandwidth in excess of 1 MHz. The FCC concluded that the rule changes would encourage competition with direct sequence technology to the benefit of consumers and that any technical constraints to higher data speeds using wider bandwidths can be overcome by appropriate equipment design. At this stage, however, FHSS with a bandwidth of up to 1 MHz were still required to use at least 75 non-overlapping hopping channels.⁸⁷

Since then, there have been several technological developments relevant to the spread spectrum rules. One salient development is an OFDM system, whereas another is a plan to introduce a new high data rate, digital transmission system called packet binary convolutional coding (PBCC) for operation in the 2.4 GHz band. In light of this situation, the FCC published Further Notice of Proposed Rule Making and Order in May 2001. It proposed the possibility to further relax the FHSS rules and to amend the rules to accommodate new digital transmission systems that have spectrum characteristics similar to spread spectrum systems, and to eliminate processing gain requirement for DSSS systems.⁸⁸

In the meantime, the FCC authorised limited commercial use of wireless devices based on ultrawideband (UWB), which are for short-range, high-speed transmissions and can be used to provide connectivity in home and office WLANs, as well as short-distance connections in February 2002.⁸⁹ The UWB equipment is required to meet emission levels specified by the FCC. The levels were determined, in part, based on protection requirements for terrestrial applications of the global positioning system (GPS) signal. The FCC adopted the limits, indicating that it would use the limits until it confirms that the levels are not needed to protect communications operations. Some congressmen have criticised the FCC for stifling a new technology by taking too conservative an approach.⁹⁰

In May 2002, the FCC published the Second Report and Order to provide for the introduction of new digital transmission technologies, to eliminate unnecessary regulations for spread spectrum systems, and to improve spectrum sharing by unlicensed devices in the 915 MHz, 2.4 GHz, and 5.7 GHz bands. Specifically, it allowed new digital transmission technologies, such as OFDM, to operate under the same rules as DSSS in these bands. Under the new rules (Section 15.247), digital modulation systems will be subject to the same power output maximum of 1 watt and power spectral density limits of 8 dBm per 3 kHz as DSSS. One of the focal points of discussion was whether these technologies may exhibit potential to cause interference to other devices. After extensive discussion, the FCC has finally concluded that there is no evidence that new digital systems are more likely to operate in such a way as to cause interference to incumbent technologies.

Another focal point was the necessity to amend the existing Unlicensed National Information Infrastructure (U-NII⁹¹) rules, whose upper limit was 5.725-5.825 GHz band, in order to allow for digitally modulated devices at 2.4 GHz band. On this point, the FCC declined to modify the U-NII rules to add the 915 MHz and 2.4 GHz bands as an alternative to regulation under the spread spectrum rules. It clarified that operation of digital devices in the 915 MHz, 2.4 GHz, and 5.7 GHz bands is best accommodated under the revised Section 15.247 rules for digitally modulated systems. As a consequence, digital devices will be permitted to operate in the 5.725-5.850 GHz band under the Section 15.247 rules as well as in the 5.725-5.825 GHz band under the U-NII rules.

The FCC also amended the rules to allow FHSS to use as few as 15 hopping channels with bandwidths up to 5 MHz and no minimum band occupancy requirements provided output power is reduced to 125 mW. It has concluded that there is no evidence to demonstrate that FHSS with bandwidths of 1 MHz or less cannot operate effectively with a minimum of 15 hopping channels with a power reduction. It also pointed out that the reduction of maximum peak power from 1 watt to 125 mW will offset increased potential for interference, caused by use of the reduced hopset, regardless of channel bandwidth. This amendment is expected to provide greater flexibility in WLAN operation without significantly increasing the risk of interference to other users.⁹²

At the same time, the FCC decided to eliminate processing gain requirements for DSSS systems.⁹³ Processing gain requirements were adopted as a means to ensure that manufacturers would not take advantage of the higher power levels afforded to spread spectrum devices by designing systems with wide bandwidths where much of the energy transmitted is not needed for communication. As the spread spectrum industry has increasingly matured, however, manufactures have an incentive to design their

systems to include processing gain so that their devices may operate properly when located near other radio frequency devices. Moreover, it has become increasingly difficult to determine true processing gain of certain DSSS systems because of a diversity of opinion within the industry regarding the definition of processing gain and the proper means to measure it. It has also been pointed out that these uncertainties on the processing gain requirement can be an impediment to the introduction of new technologies. In light of these factors, the FCC concluded that processing gain requirements should be removed.

VII. IMPLICATIONS FOR MARKET COMPETITION

7.1 *Developments of WLAN market competition*

At present the WLAN market is controlled by a small number of companies. For example, it has been estimated that five vendors control 88% of the US WLAN market.⁹⁴ However, increasing competition is likely to encourage vendors to allocate additional resources for research and development to create competitive advantages. An issue which may require further consideration is whether exclusive agreements to provide WLAN services in hot spots restrict competition. This issue may be important for hot spots in public places (airports, train stations, etc.) where single suppliers have an exclusive service contract.

The question of whether WLANs are highly profitable has been raised by some industry analysts on the basis that WLAN hot spot applications are basically not subject to “routine” usage. Most people use hot spots when travelling or going outside for a short period of time, and this usage is not part of their everyday life. However, the recent growth in new hot spots indicates that companies view this technology as one which provides future growth opportunities. For example, Starbucks, a coffee shop chain, together with Microsoft, planned to offer 802.11b wireless connections at Starbucks shops. High-speed wireless Internet service is now available at T-Mobile HotSpot in more than 1 000 Starbucks locations.⁹⁵ A subscription-based business model would be another possibility for market players.⁹⁶ WLAN providers might base their revenue model on pre-paid subscription plans targeted mainly at business travellers even though hot spot service will continue to be based on a pay-as-you-go system. It will also be increasingly important to grasp the users’ point of view, which is beyond the scope of this paper.

The development of WLAN market competition also can help accelerate the use of existing wired broadband networks. For example, WLAN use to browse as well as access e-mail from public places will appeal to a number of potential consumers. The advantage that business users can stay connected to the corporate LAN wherever WLAN is accessible can significantly boost the productivity of broadband-related equipment. In addition, the advent of wireless computing will create a reason for many PC users to go mobile, which will contribute to sales for PC vendors.⁹⁷ On the other hand, a wide variety of new telecommunications devices such as Internet Protocol phones and handheld computers will add to the usefulness of the network. WLANs will help further integrate different devices and allow mobility for devices which up to now had to rely on fixed access.

Roaming

Roaming agreements between WLAN carriers will be one of the important requirements for WLAN market development. Since no single wireless carriers can cover a sufficient number of locations for those who travel globally, it is important that users can use the WLAN infrastructure of several operators via roaming agreements between wireless ISPs. This type of agreement is expected to become common soon because it is necessary to ensure ubiquitous access to subscribers and it will allow carriers to extend their customer reach. Some roaming capabilities are developing. For example, some carriers such as Telia of Sweden and SkyNetGlobal of Australia have signed a roaming agreement with MobileStar of the United States.⁹⁸

In May 2002 several WLAN providers and hardware vendors established an industry association called Pass-One, which would facilitate WLAN roaming. It plans to set minimum service standards and make sure compliance of member networks so that users subscribing to WLAN service of one member may use that of another without barriers. While no schedule has been set for roaming to be offered to users yet, the association is open to other WLAN service providers.

In the absence of roaming agreements between WLAN carriers, however, users will have to set up a direct relationship with an operator in other geographic areas. This could take place through user-pay plans using credit card billing and access vouchers.⁹⁹

7.2 WLAN market development in some OECD countries

While WLAN services are still at an early stage in most OECD countries, some countries have recently been changing the dynamics and structure of the public access market with the emergence of various WLAN applications. While the following movements are merely some examples among OECD countries, this momentum is expected to rise dramatically in the near future.

Austria

The wireless ISP, eWAVE, announced in July 2002 that it is testing a combined WLAN solution in conjunction with Connect Austria, which is keen to build on its mobile portfolio with public access WLAN services.¹⁰⁰

Belgium

Availability of WLAN equipment is high, and almost 98% of it uses 802.11b and 802.11a standard. WLANs are often used for private communication networks operated by companies to ensure data transfer for Intranet and/or Internet access for employees.¹⁰¹ Public communication networks operated by “hot spot strategy” by some operators are also popular applications.¹⁰² This type of networks has been rapidly growing since 2002.

Canada

An increasing number of Canadian ISPs are turning to wireless technologies rather than simply reselling broadband services for the cable and telephone operators that own wired networks.¹⁰³ For those ISPs, WLANs have a great advantage in terms of low capital investment costs compared with wired networks.

Bell Canada announced in October 2002 that it was going to offer 802.11b WLAN services including consultation, network design and product acquisition, site preparation and installation, system configuration, security, testing and support.

Some companies have recently tried to combine WLAN and existing broadband services. For example, Vancouver-based FatPort announced an agreement with Covad, whereby Covad will provide the DSL backbone for FatPort’s broadband wireless Internet services. This agreement will allow FatPort and its US channel partners to deploy US wireless hot spots using FatPort wireless hardware.

Germany

T-Mobile, Deutsche Telecom’s subsidiary, is reportedly planning to introduce WLAN services providing high-speed public access networks in airport lounges, conference centres and hotels, where it can target business travellers.¹⁰⁴

Japan

NTT DoCoMo launched a WLAN service in Tokyo in July 2002. Local access point “Mzone” has been available in nine locations, and users, with a Wi-Fi card installed on their laptops are charged about USD 17 (JPY 2 000) a month for unlimited Internet access.¹⁰⁵ A variety of enterprises beyond telecommunications operators have also begun to provide WLAN services. For example, in combination with WLAN services provided by NTTCom, Mos Food Service, a hamburger chain in Japan, had begun to provide high-speed wireless Internet service at its outlets in Tokyo by the end of June 2002. Users have to be members of the “hot spot association” with a monthly subscription fee of USD 13.40 (JPY 1600).¹⁰⁶ Japan Airlines, in collaboration with IBM Japan and AT&T Global Service, also introduced WLAN services at the lounge of Narita Airport in July 2002.¹⁰⁷

There are other projects which are expected to add momentum to WLAN diffusion. For example, some railway companies such as East Japan Railway Co. (JR East) initiated an experimental project to offer WLAN service at stations in February 2002. This project is assisted by telecommunications operators such as Japan Telecom and KDDI as well as ISPs such as Nifty.¹⁰⁸ Some local governments have also initiated WLAN services. For example, the Tokyo metropolitan government began to offer experimental WLAN services in its prefecture hall buildings and a public library. This is the first governmental trial for provision of WLAN services in Japan.¹⁰⁹

In the meantime, it has been reported that some Japanese ISPs are beginning to connect with networks provided in some foreign countries, *i.e.* roaming, in order to offer WLAN services. For example, Nifty began to provide WLAN services (maximum speed of 11 Mbps) to its members in October 2002 by using networks of Gric Communications based in the United States. The charge for use is USD 0.33 (JPY 40) per minute regardless of the location of access points, which covers 10 countries (about 630 points). NEC’s Biglobe also began to offer WLAN services at public places such as hotels and airports by using the network of iPass Inc., based in the United States. The charge for use is USD 15 (JPY 1 800) per point a day.¹¹⁰

It is salient that IP telephony is gradually penetrating the market in Japan. Some telecommunications operators actually predict that there will be more than 10 million IP networks in Japan in three years.¹¹¹ In this context, Wi-Fi telephony, which combines WLAN and IP telephony, is expected to be prevalent in the near future. For example, NTT ME announced in October 2002 that it would begin experimental Wi-Fi telephony services. It will recruit about 500 monitors, who can use 41 access points for IP telephony, mainly installed in train stations, free of charge.¹¹² On the basis of these experimental services, NTT-ME will decide whether it will initiate commercial Wi-Fi telephony services.¹¹³

Korea

KT Corp. and Hanaro Telecom Inc. launched their commercial WLAN services in February 2002. They are available in public places such as hotels, airports and restaurant chains, allowing subscribers to surf the Internet through their PDAs and laptop computers.¹¹⁴ Reportedly, KT Corp. planned to invest USD 78 million (KRW 100 billion) into WLAN service (Nespot) deployment, whereas Hanaro Telecom planned to invest USD 35 million (KRW 45 billion) into the HanaFOS Anyway project in 2002.

Netherlands

The Dutch telecommunications operator, KPN, is developing an extended Internet service combining its GPRS network with WLANs and related hot spots.¹¹⁵

New Zealand

RoamAD, a wireless technology company, has deployed a 3 km² wireless network, based on the 802.11b standard, for demonstration within Auckland's central business district. This is a part of a plan to roll out a 100 km² metropolitan area network in the city.

Sweden

Ericsson, the telecommunications equipment manufacturer, announced in October 2002 that, jointly with other providers, it would develop and supply telecommunications operators with end-to-end solutions for WLAN access integrating hot spot access with mobile 2G and 3G networks.¹¹⁶ This plan is expected to allow users to roam between mobile and WLAN networks.

Switzerland

Monzoon Network has started providing public WLAN throughout the country. It was a Swiss WLAN pioneer founded in 2001, which operates a hot spot in the Swissotel Zurich-Oerlikon and another in the Swiss Airlines business lounge at the Zurich airport.¹¹⁷ In June 2002, Monzoon Network installed a number of new hot spots throughout the entire Zurich airport, including points at boarding and arrival areas.¹¹⁸

A number of hotels have already implemented Wireless LANs.¹¹⁹ From December 2002, Swisscom Mobile will provide public wireless LANs at some 100 hot spots (at busy public locations) across Switzerland. About 100 hot spots include main railway stations in Bern and Geneva, the Lucerne Cultural and Congress Centre, and all seminar hotels as well as sports centres in Davos. Other locations include a large number of Movenpick hotels throughout Switzerland and the Palazzatto Fevi in Locarno. New hot spots are being added all the time. All that is required to use public wireless LAN is a WLAN-compatible laptop or a pocket PC. As soon as the Internet browser is opened, the Swisscom Mobile homepage is automatically displayed and the user can obtain information free of charge about which hot spots are available, how they can be used, and what they have to offer. Swisscom mobile phone subscribers only need to register once via the hot spot startpage or the hotline, and afterwards they can log on using their mobile phone number and have a valid password sent to them via SMS. Customers of other Swiss network operators and visitors abroad can use the prepaid Value Card.¹²⁰

TOGEWANet, a WLAN-to-GSM integrator, announced in November 2002 the commercial release of its roaming system. The product offers seamless roaming for WLAN users between WLAN and GSM networks. The system includes roaming management, contracting, clearing and accounting services, IP/SS7 signalling convention and secure subscriber and authentication management based on GSM SIM cards.¹²¹

United Kingdom

British Telecom (BT) has launched a service called "BT Openzone" using WLAN hot spots, which offer connections of up to 500 Kbps. BT put this service into competition with mmO2, the mobile unit which separated from BT in 2001.¹²² BT is planning a commercial launch of 20 hot spots and expects to have 400 sites available by June 2003. According to BT, it hopes to have 4 000 hot spots across the United Kingdom by 2005. In line with this plan, BT announced a deal with the Costa coffee chain to offer WLAN services at five of its shops in London's City district in October 2002.¹²³

BT's public WLAN service uses the Wi-Fi standard and requires users to subscribe to BT Openzone. It is necessary for customers to be within 100 meters of a hot spot. As long as users are within the range of a hot spot and have the right software on their laptop or handheld device, they can access the Internet

several times faster than with other existing wireless connections. The subscription fee is USD 148 (GBP 95) a month plus VAT, or less than GBP 0.1 a minute if using a pay-as-you-go plan. At the same time, BT will be working with corporate customers to bring the Wi-Fi technology into their offices.¹²⁴ BT is reportedly expecting that the WLAN service will help it reach its goal of generating at least GBP 30 million a year by 2005.¹²⁵

Intel is also testing corporate Wi-Fi at London's Paddington station, along with Megabeam, a pan-European wireless ISP, in the United Kingdom. In July 2002, Megabeam announced an extensive agreement with Railtrack to install Wi-Fi hot spots based on 802.11b at nine London terminals and six regional stations.¹²⁶ WLAN systems have also been introduced at universities. For example, the London School of Economics set up wireless networks that students can use for Internet access in 2002.

Throughout the United Kingdom there are a number of community-based initiatives to use 2.4 GHz equipment (predominantly IEEE 802.11b) to bring broadband services to rural areas and towns. Many of these projects include or are driven by the needs of schools and the education sector. Thousands of United Kingdom schools are now connected to broadband services using 2.4 GHz links and many are now investing in IEEE 802.11a technology to provide WLAN services in the classroom. Many of the community groups are funded by a mix of private and public sector money, attracting grants, but also encouraging commercial users to pay towards services provided.

United States

A growing number of cities are setting up Wi-Fi access in public outdoor sites in the United States. In Pittsburgh, for example, an outdoor public Wi-Fi network (Pittsburgh Public Wireless Internet/PPWI) was launched by 3 Rivers Connect, a non-profit organisation funded by the state of Pennsylvania in May 2002.¹²⁷ A pair of antennae is installed in a building in the city centre, which provides the parks near the building with 10 Mbps Internet access. While this project is currently limited to two parks in the city centre free of charge, the organiser is planning to charge USD 20 a month for access once the network covers a four-square-mile area in the Pittsburgh city centre.

Intel Corporation, IBM, AT&T Wireless and several other wireless and Internet service providers have initiated Project Rainbow, exploring the feasibility of creating a company to deploy a network based on the 802.11 wireless data standard.¹²⁸ The companies are also considering a more ambitious plan to build a new wireless communications infrastructure that would tie in the nation's cellular carriers and offer a seamless transition from low-speed cellular data standards to 802.11. Intel Corporation is also considering introducing the wireless data standard to 20 million portable computers in 2003 and an additional 40 million portable and desktop computers in 2004. Cisco Systems announced in July 2002 that it had agreements with 19 international airports across Europe to launch WLAN services for business travellers.

NYCwireless provides free wireless Internet service using wireless technology to mobile users in public spaces throughout the New York City metropolitan area.¹²⁹ These public spaces include parks, coffee shops and building lobbies, and the organisation reportedly intends to work with public and other non-profit organisations to bring broadband wireless Internet to underserved communities. Thanks to this initiative, a free hot spot was set up in the Bryant Park, in midtown New York, in June 2002.

Some joint projects within the industry are also active in the United States. For example, T-Mobile, currently the largest wireless ISP in the country, announced in October 2002 that it would partner with American, Delta, and United Airlines to install WLAN networks in 100 passenger lounges in the US. At present, however, T-Mobile does not have interoperability agreements with competing providers of WLAN service.¹³⁰ In Virginia, several public libraries completed installation of WLAN system with the help of an award from the SBC Excelsior competitive grants programme.

Like in Canada, some WLAN providers have strategies to combine the service with existing broadband services for the purpose of increasing the availability of their technologies. For example, Surf and Sip will give away WLAN equipment to business owners who buy DirecTV DSL service. While the business must pay for the DSL service, it can offer wireless Internet service to customers, splitting the revenue with Surf and Sip.

7.3 *Community-based wireless networks*

There is a rapidly growing movement to form community-based wireless networks using the 802.11b standard among OECD countries. It is important to note that these initiatives are mostly based on a private or industry effort rather than through government initiatives. In areas where there is a lack of appropriate broadband alternatives, community-driven wireless networks are becoming much popular. In the United States, for example, several western communities have banded together to organise co-operative efforts to provide wireless services. The Sugarloaf Internet Cooperative and the Magnolia Road Internet Cooperative, both based in Colorado, use 802.11b technology to provide broadband services. The Magnolia Road Cooperative reportedly serves potential 400 households and charges a USD 50 membership fee as well as USD 50 for monthly service.

City-based wireless networks are also developing in the United States. In Seattle, for example, Seattle Wireless is making a not-for-profit effort to develop a community broadband wireless network within the city.¹³¹ The organisation calls it the “Metropolitan Area Network” in that it is not simply a WLAN service used in the home and business. In the Kansas City region, KCWireless.net is dedicated to bringing free wireless Internet access to the area using 802.11b network hardware.¹³²

Some organisations in Canada are also seeking to set up wireless community networks on a non-profit basis. For instance, Waterloo Wireless, a non-profit organisation, intends to provide free broadband wireless access to the communities of the regional municipality of Waterloo. Access points are going to be placed in houses, businesses, libraries and schools throughout the community to allow both PCs and mobile computers to be used for the access.¹³³

Wireless community networks are developing in Europe as well. In Switzerland, for example, Geneva Wireless is trying to establish a Wireless Community Network in Geneva, which aims to create a community network based on wireless cards supporting 802.11b standard for personal computers, laptops and personal digital assistants across the city.¹³⁴ In France, Paris-Sansfil, a not-for-profit organisation, is attempting to promote the development of free community wireless networks.¹³⁵ In Sweden, a Stockholm-based discussion group called Elektrosmog has been formed for those who are interested in wireless access to the Internet such as 802.11b.¹³⁶ In Spain, Zamora has become the first city to install a broadband wireless Internet access service through an initiative of Afitel, in collaboration with the city government as well as Azehos, a local business association. Users will need to subscribe to Afitel and install a Wi-Fi card with the monthly price of USD 8.60 (EUR 9.90).

In Australia, the Canberra Wireless Network is attempting to build a high-speed wireless network in some parts of Canberra.¹³⁷ A consortium called innaloo.net, based in Perth, has also been established for computer users who decided to build a small regional network connecting the Perth suburbs.¹³⁸ Leeming Wireless is trying to create a community run wireless network based on 802.11b compatible hardware in the Leeming/Willetton/Bullcreek area.¹³⁹

NOTES

1. Wi-Fi is a registered trademark belonging to the Wi-Fi Alliance, a US-based trade association, and refers to the IEEE 802.11b standard, which is one of the most popular WLAN technologies.
2. For example, see <http://www.uselink.com.tw/TWL-A11.htm>.
3. 802.11b is a wireless LAN specification developed by Institute of Electrical and Electronic Engineers (IEEE) as an extension to the 802.11 standard accepted in July 1997. Using direct sequence spread spectrum (DSSS) modulation, it provides up to 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band.
4. According to the Yankee Group. See http://www.yankeegroup.com/public/news_releases/news_release_detail.jsp?ID=PressReleases/news_august012002_wmec.htm.
5. See <http://www.delloro.com/PRESS/PressReleases/ESw073102.shtml>.
6. See Network World Fusion, 22 April 2002, <http://www.nwfusion.com/cgi-bin/mailto/x.cgi>.
7. http://www.isp-planet.com/research/2002/newtechs_020130.html.
8. This is predicted by International Data Corporation
See http://www.isp-planet.com/research/2002/newtechs_020130.html.
9. See <http://www.europemedia.net/shownews.asp?ArticleID=11183>.
10. See <http://www.wlana.org/learn/educate1.htm#over>.
11. See <http://www.corante.com/bottomline/20020301.shtml>.
12. The data is derived from Dell'Oro Group Inc.
13. For example, see http://jin.jcic.or.jp/trends/article/020910bus_r.html.
14. *New York Times*, 4 March 2002, <http://www.nytimes.com/2002/03/04/technology/04WIRE.html>.
15. See http://www.commweb.com/article/printableArticle?doc_id=COM20010921S0004.
16. See Jason Kane and David C. Yen, "Breaking the Barriers of Connectivity: an Analysis of the Wireless LAN", <http://gene.wins.uva.nl/~bcmndeur/6.pdf>.
17. In total, 19 airports in Europe, the Middle East and Africa are reportedly using the Cisco Mobile Office WLAN system. See <http://siliconvalley.internet.com/news/article.php/1382751>.
18. According to the prediction of Dell'Oro Group. See <http://www.nwfusion.com/news/2002/0801wlan.html>.
19. See <http://zdnet.com.com/2102-1105-937110.html>.

20. Ibid.
21. See <http://www.spectralink.com/products/pdfs/WP-Wi-Fi-Telephony-WECA.pdf>. Some argue that using Wi-Fi data links for real-time applications would be difficult while they can be used for packetised voice given that it is subject to interference from other unlicensed devices.
22. http://www.globeandmail.com/servlet/RTGAMArticleHTMLTemplate?tf=tgam/realtime/fullstory_print.html&cf=tgam/realtime/config-neutral&articleDate=20020802&slug=gtspeedhp&date=20020802&archive=RTGAM&site=Business.
23. Previously, families that wanted Internet access from multiple computers often connected the terminals to the same telephone line using a splitter.
24. See http://www.80211-planet.com/news/article/0,,1481_1143771,00.html.
25. Sorin M. Schwartz, Frequency Hopping Spread Spectrum (FHSS) vs. Direct Sequence Spread Spectrum (DSSS) in the Broadband Wireless Access and WLAN Arenas, http://www.cvcwireless.com/C3_freq_hop_vs_direct_seq.pdf.
26. See http://www.wirelesslanresource.com/news_12.shtml.
27. See http://grouper.ieee.org/groups/802/11/Reports/tgg_update.htm.
28. See <http://www.convergedigest.com/WiFi/wlanarticle.asp?ID=4262>.
29. The key members of WLIF include Casio, Data General, Fujitsu, HP, IBM, Intermec, Mitsubishi, Motorola, and Proxim.
See http://www.xilinx.com/esp/home_networking/industry_standards/wirelesslans.htm.
30. See <http://www.wlana.org/about/index.htm>.
31. See <http://www.hiperlan2.com/>.
32. WLANA, High-Speed Wireless LAN Options: 802.11a and 802.11g, <http://www.wlana.org/pdf/highspeed.pdf>.
33. For example, see http://asia.internet.com/asia-news/article/0,3916,161_1448581,00.html.
34. Andy Dorman, "Emerging Technology: Wireless Lan Standards", 6 February 2002, http://www.networkmagazine.com/article/printableArticle?doc_id=NMG20020206S0006.
35. For details, see <http://www.envara.com/doc/planetee.pdf>.
36. For example, see <http://www.internetnews.com/bus-news/print.php/801211>.
37. See <http://www.arib.or.jp/mmac/e/>.
38. WLANA, The IEEE 802.11 Wireless LAN Standard, <http://www.wlana.org/learn/80211.htm>. The frequency ranges are subject to the geography-specific regulatory authorities.
39. See WLANA, The IEEE 802.11 Wireless LAN Standard, <http://www.wlana.org/learn/80211.htm>.
40. See Jason Kane and David C. Yen, Breaking the Barriers of Connectivity: An Analysis of the Wireless LAN, <http://gene.wins.uva.nl/~bcmndeur/6.pdf>.

41. See <http://www.webopedia.com/TERM/F/FHSS.html>.
42. See <http://www.webopedia.com/TERM/D/DSSS.html>.
43. See <http://wireless.per.nl/telelearn/ofdm/>.
44. INT Media Research, "802.11 Wireless LAN Security: Usage, Expectations, and Strategies for the Future." Also see <http://www.internetnews.com/infra/article.php/1352541>.
45. See Network World Fusion, 15 July 2002, <http://www.nwfusion.com/cgi-bin/mailto/x.cgi>.
46. NIST, Tom Karygiannis and Les Owens, "Wireless Network Security: 802.11, Bluetooth™ and Handheld Devices", <http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf>.
47. Andy Dorman, "Emerging Technology: Wireless Lan Standards," 6 February 2002, http://www.networkmagazine.com/article/printableArticle?doc_id=NMG20020206S0006.
48. See <http://ww1.infoworld.com/cgi-bin/fixup.pl?story=http://www.infoworld.com/articles/hn/xml/02/10/31/021031hnwifi.xml&dctag=wireles>.
49. See "PSION TEKLOGIX, 802.11 Wireless LAN Security", http://partners.pSIONteklogix.com/assets/downloadable/80211_Security.pdf.
50. For details, see <http://japan.cnet.com/News/2002/Item/020131-5.html?rn>.
51. NIST, Tom Karygiannis and Les Owens, "Wireless Network Security: 802.11, Bluetooth™ and Handheld Devices", <http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf>.
52. See http://www.weca.net/downloads/BT_inf802_June_8.pdf.
53. See http://203.147.194.107/bluearticles/cc4_bluetooth802.11b_part2.asp.
54. "Wireless Networks: Safe, Secure, and Cost-Effective", September 2000, http://www.hp.com/sbso/productivity/howto/pdf/wp_wireless_networks.pdf.
55. Ibid.
56. Jim Zyren, "Reliability of IEEE 802.11Hi Rate DSSS WLANs in a High Density Bluetooth Environment, 8 June 1999, http://www.weca.net/downloads/Coexistence_Paper_Intersil_Aug18.pdf. Jaap C. Haartsen & Stefan Zurbes, "Bluetooth Voice and Data Performance in 802.11 DS WLAN Environment", 31 May 1999, http://www.weca.net/downloads/BT_inf802_June_8.pdf. HP Invent, "Wireless Networks: Safe Secure, and Cost-Effective", September 2000, http://www.hp.com/sbso/productivity/howto/pdf/wp_wireless_networks.pdf.
57. See http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci535092,00.html.
58. See <http://www.palowireless.com/homerf/about.asp>.
59. HomeRF 1.0 ran at 1.6 Mbps. HomeRF 2.0 increased the bandwidth to 10 Mbps. For details, see <http://www.homenethelp.com/web/explain/about-homerf-2.asp>.
60. For example, see http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci535092,00.html.

61. See *Network World Fusion*, 1 April 2002, <http://www.nwfusion.com/cgi-bin/mailto/x.cgi>. Also see <http://www.tca.or.jp/japan/daisu/yymm/0212matu.htm>.
62. For example, see http://www.80211-planet.com/news/print/0,,1481_1443821,00.html.
63. See <http://www.europemedia.net/shownews.asp?ArticleID=11339>.
64. See <http://www.europemedia.net/shownews.asp?ArticleID=11447>.
65. For example, see <http://www.instat.com/press.asp?ID=18&sku=MU0110SG>.
66. Lucent Technologies, a US-based telecommunications equipment manufacturer, announced this achievement. The result also addresses the need for combined billing system for services on the WLAN and 3G networks. See <http://www.europemedia.net/shownews.asp?ArticleID=12672>.
67. See <http://www.europemedia.net/shownews.asp?ArticleID=11056>.
68. <http://www.art-telecom.fr/index.htm>.
69. See <http://www.convergedigest.com/WiFi/wlanarticle.asp?ID=4433>.
70. The Mckinsey Quarterly, 8 November 2002, Number 4.
71. The US view is that these systems have no interference protection rights, even though much of the current discussion of 802.11 devices involves the possibility of allocating spectrum to such devices.
72. <http://news.com.com/2100-1033-877572.html?tag=rn>.
73. See 1 July 2002, *New York Times*, <http://www.nytimes.com/2002/07/01/technology/01WIFI.html?todayshdlines=&pagewanted=print&position=top>.
74. See <http://www.europemedia.net/shownews.asp?ArticleID=11452>.
75. To enable installation of WLAN equipment in public spaces such as train stations or airports, the Ministry is going to propose the amendment of the relevant law in 2003. See http://www.soumu.go.jp/s-news/2002/020808_4.html.
76. For details, see <http://www.rtr.at/web.nsf/englisch/Telekommunikation~Frequenzvergabe~Spektrum~Spektrum~WLAN-Spektrum>, [http://www.rtr.at/web.nsf/lookuid/F55D401D02289884C1256C5900403EC4/\\$file/Info_RLAN_Version_November_2002.pdf](http://www.rtr.at/web.nsf/lookuid/F55D401D02289884C1256C5900403EC4/$file/Info_RLAN_Version_November_2002.pdf).
77. See <http://www.europemedia.net/shownews.asp?ArticleID=11983>.
78. For details, see <http://www.ficora.fi/englanti/radio/RLANnotice.htm>.
79. See <http://www.regtp.de/en/aktuelles/pm/02605/index.html>.
80. These conditions are applicable to 58 departments as of February 2003.
81. See <http://www.art-telecom.fr/communiqués/communiqués/2002/index-07-11-2002.htm>.

82. For details, see http://www.odtr.ie/docs.asp?Type=Year&Year=2002&Image=images/docs_issued2002.gif.
83. See ODTR Media Release, July 30 2002, http://www.odtr.ie/press_releases.asp?yr=2002&Mth=7.
84. For details, see http://www.soumu.go.jp/s-news/2002/020807_6.html.
85. In addition, the average time of occupancy on any frequency must not exceed 0.4 seconds in any 30 second period.
86. Federal Communications Commission, Notice of Proposed Rule Making, FCC 99-149, 24 June 1999.
87. Federal Communications Commission, First Report and Order, FCC 00-312, 31 August 2000.
88. Federal Communications Commission, Further Notice of Proposed Rule Making and Order, FCC 01-158, 11 May 2001.
89. See <http://news.com.com/2100-1033-837683.html?feed.cnetbriefs>.
90. See 6 June 2002, *Network World Fusion*, <http://www.nwfusion.com/cgi-bin/mailto/x.cgi>.
91. U-NII devices were envisioned for relatively long distances compared with 802.11 devices operating at 2.4 GHz today.
92. Federal Communications Commission, Second Report and Order, FCC 02-151, 30 May 2002.
93. The rule required DSSS devices to have a processing gain of at least 10 dB.
94. Jason Kane and David C. Yen, "Breaking the Barriers of Connectivity: An Analysis of the Wireless LAN", <http://gene.wins.uva.nl/~bcmndeur/6.pdf>.
95. See <http://www.starbucks.com/retail/wireless.asp>.
96. http://www.isp-planet.com/research/2002/wlan_020116.html.
97. Research Brief, "Wireless LAN: The Next Killer Application", 17 May 2001, <http://www3.gartner.com/resources/97800/97856/97856.pdf>.
98. See Gunnar Almgren, "Roaming Between Wireless ISPs", April 2002, http://www.hco.se/kund/sf/pa6_en.pdf.
99. Gunnar Almgren, "Roaming Between Wireless ISPs", April 2002, http://www.hco.se/kund/sf/pa6_en.pdf.
100. See <http://www.europemedia.net/shownews.asp?ArticleID=11500>.
101. This type of network is subject to a registration procedure.
102. This type of network is currently subject to authorisation, but it will be subject to a registration procedure as of July 2003.
103. See http://www.globeandmail.com/servlet/RTGAMArticleHTMLTemplate?tf=lgam/realtime/fullstory_print.html&cf=lgam/realtime/config-neutral&articleDate=20020802&slug=gtspeedhp&date=20020802&archive=RTGAM&site=Business.
104. See <http://www.europemedia.net/shownews.asp?ArticleID=11500>.

105. DoCoMo Net, <http://www.nttdocomo.co.jp/info/new/release.html>.
106. See http://www.mos.co.jp/company/reference/press/press_020425.html.
107. See <http://www.jal.co.jp/lounge/topics/index.html>.
108. See <http://sg.biz.yahoo.com/020805/15/319tl.html>.
109. *Nihonkeizai shimbun*, 10 September 2002.
110. *Nihonkeizai shimbun*, 21 October 2002, p.13. Also see <http://japan.cnet.com/News/2002/Item/020625-3.html?rn>.
111. *Sankei shimbun*, 25 October 2002, p.10.
112. *Nihonkeizai shimbun*, 22 October 2002, p.15.
113. See http://www.ntt-bp.net/pc/whatsnew/021221_1.html.
114. See http://kn.koreaherald.co.kr/SITE/data/html_dir/2002/06/21/200206210017.asp.
115. See <http://www.europemedia.net/shownews.asp?ArticleID=11332>.
116. See <http://www.europemedia.net/shownews.asp?ArticleID=13286>.
117. See http://www.weroam.com/pdf/Netzwoche2_english.pdf.
118. See http://www-5.ibm.com/ch/eneews/pdf/swiss_monsoon_ibm_0702.pdf.
119. See <http://www.swiss-hotspots.ch>. Also see Telecom.paper, 23 October 2002, <http://www.telecom.paper.nl/java/updatelinks.js>.
120. http://www.swisscom.com/mr/content/media/20021127_EN.html.
121. See http://www.weroam.com/presse/nov02_english.htm.
122. See <http://www.europemedia.net/shownews.asp?ArticleID=11186>.
123. See <http://www.europemedia.net/shownews.asp?ArticleID=13420>.
124. See <http://www.btplc.com/Mediacentre/Agencynewsreleases/2002/an34.htm>.
125. See <http://www.europemedia.net/shownews.asp?ArticleID=11330>.
126. See <http://www.europemedia.net/shownews.asp?ArticleID=11564>.
127. See <http://news.com.com/2102-1033-918439.html>.
128. *The New York Times*, 16 July 2002, <http://www.nytimes.com/2002/07/16/technology/16WIRE.html?todaysh headlines=&pagewanted=print&position=top>.
129. See <http://www.nycwireless.net>.

130. See <http://staging.infoworld.com/articles/hn/xml/02/10/30/021030hnairlinewifi.xml?Template=/storypages/printfriendly.html>.
131. See <http://www.seattlewireless.net/>.
132. See <http://www.kcwireless.net/>.
133. See <http://uw-linux.uwaterloo.ca/WaterlooWireless/>,
<http://rtnews.globetechnology.com/servlet/ArticleNews/tech/RTGAM/20020802/gtspeed/Technology/techBN/>.
134. See <http://www.genevawireless.net>.
135. See <http://www.paris-sansfil.net/index.php/ParisSansFilMotivations>.
136. Membership is open and free of charge. See <http://elektrosmog.nu>.
137. See <http://www.air.net.au/>.
138. See <http://www.innaloo.net>.
139. See <http://www.leemingwireless.net>.