Wi-Fi

From Wikipedia, the free encyclopedia.

Wi-Fi, also, **WiFi**, **Wi-fi** or **wifi**, is a brand originally licensed by the Wi-Fi Alliance to describe the underlying technology of wireless local area networks (WLAN) based on the IEEE 802.11 specifications.

Wi-Fi was developed to be used for mobile computing devices, such as laptops, in LANs, but is now increasingly used for more applications, including Internet and VoIP phone access, gaming, and basic connectivity of consumer electronics such as televisions and DVD players, or digital cameras. There are even more standards in development that will allow Wi-Fi to be used by cars in highways in support of an Intelligent Transportation System to increase safety, gather statistics, and enable mobile commerce IEEE 802.11p.

A person with a Wi-Fi device, such as a computer, telephone, or personal digital assistant (PDA) can connect to the Internet when in proximity of an access point. The region covered by one or several access points is called a hotspot. Hotspots can range from a single room to many square miles of overlapping hotspots. Wi-Fi can also be used to create a Wireless mesh network. Both architectures are used in Wireless community network, municipal wireless networks like Wireless Philadelphia [1], and metro-scale networks like M-Taipei [2].

Wi-Fi also allows connectivity in peer-to-peer mode, which enables devices to connect directly with each other. This connectivity mode is useful in consumer electronics and gaming applications.

When the technology was first commercialized there were many problems because consumers could not be sure that products from different vendors would work together. The Wi-Fi Alliance began as a community to solve this issue so as to address the needs of the end user and allow the technology to mature. The Alliance created another brand "Wi-Fi CERTIFIED" to denote products are interoperable with other products displaying the "Wi-Fi CERTIFIED" brand.

History

Official Wi-Fi logo

Wi-Fi uses both single carrier direct-sequence spread spectrum radio technology, part of the larger family of spread spectrum systems and multi-carrier OFDM (Orthogonal Frequency Division Multiplexing) radio technology. Unlicensed spread spectrum was first authorized by the Federal Communications Commission in 1985 and these FCC regulations were later copied with some changes in many other countries enabling use of

this technology in all major countries. These regulations then enabled the development of Wi-Fi, its onetime competitor HomeRF, and Bluetooth.

The precursor to Wi-Fi was invented in 1991 by NCR Corporation/AT&T (later Lucent & Agere Systems) in Nieuwegein, the Netherlands. It was initially intended for cashier systems; the first wireless products were brought on the market under the name WaveLAN with speeds of 1 Mbit/s to 2 Mbit/s. Vic Hayes, who was the primary inventor of Wi-Fi and has been named the 'father of Wi-Fi,' was involved in designing standards such as IEEE 802.11b, 802.11a and 802.11g. In 2003, Vic retired from Agere Systems. Agere Systems suffered from strong competition in the market even though their products were high quality, as many opted for cheaper Wi-Fi solutions. Agere's 802.11a/b/g all-in-one chipset (code named: WARP) never made it to market, and Agere Systems decided to quit the Wi-Fi market in late 2004.

[edit]

Origin and meaning of the term "Wi-Fi"

Despite the similarity between the terms "Wi-Fi" and "Hi-Fi", statements reportedly [3] made by Phil Belanger of the Wi-Fi Alliance contradict the popular conclusion that "Wi-Fi" stands for "Wireless Fidelity".

According to Mr. Belanger, the Interbrand Corporation developed the brand "Wi-Fi" for the Wi-Fi Alliance to use to describe WLAN products that are based on the IEEE 802.11 standards. In Mr. Belanger's words, *"Wi-Fi and the yin yang style logo were invented by Interbrand. We (the founding members of the Wireless Ethernet Compatibility Alliance, now called the Wi-Fi Alliance) hired Interbrand to come up with the name and logo that we could use for our interoperability seal and marketing efforts. We needed something that was a little catchier than 'IEEE 802.11b Direct Sequence'."*

The Wi-Fi Alliance themselves invoked the term "Wireless Fidelity" with the marketing of a tag line, "The Standard for Wireless Fidelity," but later removed the tag from their marketing. The Wi-Fi Alliance now seems to discourage propagation of the notion that "Wi-Fi" stands for "Wireless Fidelity" but includes it in their knowledge base:

> To understand the value of Wi-Fi Certification, you need to know that Wi-Fi is short for "Wireless Fidelity," and it is the popular name for 802.11-based technologies that have passed Wi-FI certification testing. This includes IEEE 802.11a, 802.11b, 802.11g and upcoming 802.11n technologies.

Wi-Fi: How it works

The typical Wi-Fi setup contains one or more Access Points (APs) and one or more clients. An AP broadcasts its SSID (Service Set Identifier, "Network name") via packets that are called beacons, which are broadcast every 100 ms. The beacons are transmitted at

1 Mbit/s, and are of relatively short duration and therefore do not have a significant influence on performance. Since 1 Mbit/s is the lowest rate of Wi-Fi it assures that the client who receives the beacon can communicate at least 1 Mbit/s. Based on the settings (e.g. the SSID), the client may decide whether to connect to an AP. Also the firmware running on the client Wi-Fi card is of influence. Say two APs of the same SSID are in range of the client, the firmware may decide based on signal strength to which of the two APs it will connect. The Wi-Fi standard leaves connection criteria and roaming totally open to the client. This is a strength of Wi-Fi, but also means that one wireless adapter may perform substantially better than the other. Since Wi-Fi transmits in the air, it has the same properties as a non-switched ethernet network. Even collisions can therefore appear like in non-switched ethernet LAN's.

Channels

Except for 802.11a, which operates at 5 GHz, Wi-Fi uses the spectrum near 2.4 GHz, which is standardized and *unlicensed* by international agreement, although the exact frequency allocations vary slightly in different parts of the world, as does maximum permitted power. However, channel numbers are standardized by frequency throughout the world, so authorized frequencies can be identified by channel numbers.

The frequencies for 802.11 b/g span 2.400 GHz to 2.487 GHz. Each channel is 22 MHz wide and 5 MHz spacers between the channels are required. With the required spacers, only 3 channels (1,6, and 11) can be used simultaneously without interference.

Examples of Standard Wi-Fi Devices

Wireless Access Point (WAP)

A wireless access point (AP) connects a group of wireless stations to an adjacent wired local area network (LAN). An access point is similar to an ethernet hub, but instead of relaying LAN data only to other LAN stations, an access point can relay wireless data to all other compatible wireless devices as well as to a single (usually) connected LAN device, in most cases an ethernet hub or switch, allowing wireless devices to communicate with any other device on the LAN.

Wireless Routers

A wireless router integrates a wireless access point with an ethernet switch and an ethernet router. The integrated switch connects the integrated access point and the integrated ethernet router internally, and allows for external wired ethernet LAN devices to be connected as well as a (usually) single WAN device such as a cable modem or DSL modem. A wireless router advantageously allows all three devices (mainly the access point and router) to be configured through one central configuration utility, usually

through an integrated web server. However one disadvantage is that one may not decouple the access point so that it may be used elsewhere.

Wireless ethernet Bridge

A wireless ethernet bridge connects a wired network to a wireless network. This is different from an access point in the sense that an access point connects wireless devices to a wired network at the data-link layer. Two wireless bridges may be used to connect two wired networks over a wireless link, useful in situations where a wired connection may be unavailable, such as between two separate homes.

Range Extender

A wireless range extender (or wireless repeater) can increase the range of an existing wireless network by being strategically placed in locations where a wireless signal is sufficiently strong and near by locations that have poor to no signal strength. An example location would be at the corner of an L shaped corridor, where the access point is at the end of one leg and a strong signal is desired at the end of the other leg. Another example would be 75% of the way between the access point and the edge of its useable signal. This would effectively increase the range by 75%.

Wi-Fi vs. cellular

Some argue that Wi-Fi and related consumer technologies hold the key to replacing cellular telephone networks such as GSM. Some obstacles to this happening in the near future are missing roaming and authentication features (see 802.1x, SIM cards and RADIUS), the narrowness of the available spectrum and the limited range of Wi-Fi. It is more likely that WiMax will compete with other cellular phone protocols such as GSM, UMTS or CDMA. However, Wi-Fi is ideal for VoIP applications e.g. in a corporate LAN or SOHO environment. Early adopters were already available in the late '90s, though not until 2005 did the market explode. Companies such as Zyxel, UT Starcomm, Sony, Samsung, Hitachi and many more are offering VoIP Wi-Fi phones for reasonable prices.

In 2005, low-latency broadband ISPs started offering VoIP services to their customers. Since calling via VoIP is free or low-cost, VoIP enabled ISPs have the potential to open up the VoIP market. GSM phones with integrated Wi-Fi & VoIP capabilities are being introduced into the market and have the potential to replace land line telephone services.

Currently it seems unlikely that Wi-Fi will directly compete against cellular in areas that have only sparse Wi-Fi coverage. Wi-Fi-only phones have a very limited range, so setting up a covering network would be too expensive. Additionally, cellular technology allows the user to travel while connected, bouncing the connection from tower to tower (or

"cells") as proximity changes, all the while maintaining one solid connection to the user. Many current Wi-Fi devices and drivers do not support roaming yet and connect to only one access point at a time. In this case, once you are out of range of one "hotspot", the connection will drop and will need to be re-connected to the next one each time.

For these reasons, Wi-Fi phones are still best suited for local use such as corporate or home networks. However, devices capable of multiple standards, called converged devices, (using SIP or UMA) may well compete in the market. Top-tier handset manufacturers have announced converged dual-radio handsets. Converged handsets present several compelling advantages to mobile carriers:

- Efficient spectrum allocation, as more data-intensive services come online and bandwidth demands increase
- Improved in-building coverage in markets such as the US, where dropped calls are still a major cause of customer dissatisfaction
- Opportunities for mobile operators to offer differentiated pricing and services.

Commercial Wi-Fi

Commercial Wi-Fi services are available in places such as Internet cafes, coffee houses, hotels and airports around the world (commonly called Wi-Fi-cafés), although coverage is patchy in comparison with cellular.

In the US:

- T-Mobile provides HotSpots in many partner retail locations including many Starbucks, Borders Books, and a variety of hotels and airports.
- a Columbia Rural Electric Association subsidiary offers 2.4 GHz Wi-Fi service across a 3,700 mi^2 (9,500 km^2) region within Walla Walla and Columbia counties in Washington and Umatilla County, Oregon.
- WiSE Technologies provides commercial hotspots for airports, universities, and independent cafes in the US;
- Boingo Wireless has over 45,000 hotspots worldwide, including most major airports in the U.S.
- restaurant chain Panera Bread provides free Wi-Fi access at its restaurants.
- Other large hotspot providers include Wayport, iPass, and iBahn.
- There are also a number of aggregators of Wi-Fi, the main one being BOZII, they allow users access to over 250 networks including BT Openzone and Orange France, all with one username and password for a flat fee and no roaming charges.

In the UK:

- T-Mobile provides hotspots in many Starbucks and Airports in the UK too.
- BT Openzone provides many hotspots across the United Kingdom and Ireland, notably in most McDonalds restaurants, and have roaming agreements with T-

Mobile UK and ReadyToSurf. Their customers are also able to access hotspots managed by The Cloud.

In France:

- Ozone and OzoneParis In France, in September 2003, Ozone started deploying the OzoneParis network across the City of Lights. The objective: to construct a wireless metropolitan network with full Wi-Fi coverage of Paris. Ozone is also deploying its network in Brussels (Belgium) and other cities in France like Rennes. Ozone Pervasive Network philosophy is based on a nationwide scale.
- als@tis One of the largest Wireless Internet Service Provider for rural areas in France.

In other places:

- GlobeQUEST, under Globe Telecom, provides for prepaid Wi-Fi services for nearly all cafes in the Philippines
- Pacific Century Cyberworks provides hotspots in Pacific Coffee shops in Hong Kong;
- Vex offers a big network of hotspots spread over Brazil. Telefónica Speedy Wi-Fi has started its services in a new and growing network distributed over the state of São Paulo.
- Netstop provides hotspots in New Zealand;
- FatPort is Canada's oldest independent Wi-Fi HotSpot operator with coverage from coast to coast.

Universal efforts

Another business model seems to be making its way into the news. The idea is that users will share their bandwidth through their personal wireless routers, which are supplied with specific software. An example is FON, a Spanish start-up created in November 2005. It aims to become the largest network of hotspots in the world by the end of 2006 with 70000 access points. The users are divided into three categories: *linus* share Internet access for free; *bills* sell their personal bandwidth; and *aliens* buy access from bills. Thus the system can be described as a peer-to-peer sharing service, which we usually relate to software.

Although FON has received some financial support by companies like Google and Skype, it remains to be seen whether the idea can actually work. There are three main challenges for this service at the moment. The first is that it needs much media and community attention first in order to get through the phase of "early adoption" and into the mainstream. Then comes the fact that sharing your Internet connection is often against the terms of use of your ISP. This means that in the next few months we can see ISPs trying to defend their interests in the same way music companies united against free MP3 distribution. And third, the FON software is still in Beta-version and it remains to be seen if it presents a good solution of the imminent security issues.

Free Wi-Fi

While commercial services attempt to move existing business models to Wi-Fi, many groups, communities, cities, and individuals have set up free Wi-Fi networks, often adopting a common peering agreement in order that networks can openly share with each other. Free wireless mesh networks are often considered the future of the Internet.

Many municipalities have joined with local community groups to help expand free Wi-Fi networks (see Mu-Fi). Some community groups have built their Wi-Fi networks entirely based on volunteer efforts and donations.

For more information, see wireless community network, where there is also a list of the free Wi-Fi networks one can find around the globe.

OLSR is one of the protocols used to set up free networks. Some networks use static routing; others rely completely on OSPF. Wireless Leiden developed their own routing software under the name LVrouteD for community wi-fi networks that consist of a completely wireless backbone. Most networks rely heavily on open source software, or even publish their setup under an open source license.

Some smaller countries and municipalities already provide free Wi-Fi hotspots and residential Wi-Fi internet access to everyone. Examples include Estonia which have already a large number of free Wi-Fi hotspots throughout their countries.

In Paris, France, OzoneParis offers free Internet access for life to anybody who contributes to the Pervasive Network's development by making their rooftop available for the Wi-Fi Network.

Annapolis, Maryland is in the early phases (as of April 2006) of a pilot program to provide free, advertisement-financed Wi-Fi to all its residents. A private company, Annapolis Wireless Internet, will administrate the network. Users will only see local advertisements upon accessing the network. [4]

Unwire Jerusalem is a project to put free Wi-Fi access points at the main shopping centers of Jerusalem.

Many universities provide free Wi-Fi internet access to their students, visitors, and anyone on campus. Similarly, some commercial entities such as Panera Bread and Culver's offer free Wi-Fi access to patrons. McDonald's Corporation also offers Wi-Fi access, often branded 'McInternet'. This was launched at their flagship restaurant in Oak Brook, Illinois, USA, and is also available in many branches in London, UK.

However, there is also a third subcategory of networks set up by certain communities such as universities where the service is provided free to members and guests of the community such as students, yet used to make money by letting the service out to companies and individuals outside. An example of such a service is Sparknet in Finland.

Sparknet also supports OpenSpark, a project where people can share their own wireless access point and become as a part of Sparknet and OpenSpark community in return for certain benefits.

Recently commercial Wi-Fi providers have built free Wi-Fi hotspots and hotzones. These providers hope that free Wi-Fi access would equate to more users and significant return on investment.

Wi-Fi vs. amateur radio

In the US, (and Australia) a portion of the 2.4 GHz Wi-Fi radio spectrum is also allocated to amateur radio users. FCC Part 15 rules govern non-licenced operators (i.e. most Wi-Fi equipment users). Under Part 15 rules, non-licensed users must "accept" (e.g. endure) interference from licensed users and not cause harmful interference to licensed users. Amateur radio operators are licensed users, and retain what the FCC terms "primary status" on the band, under a distinct set of rules (Part 97). Under Part 97, licensed amateur operators may construct their own equipment, use very high-gain antennas, and boost output power to 100 watts on frequencies covered by Wi-Fi channels 2-6. However, Part 97 rules mandate using only the minimum power necessary for communications, forbid obscuring the data, and require station identification every 10 minutes. Therefore, expensive automatic power-limiting circuitry is required to meet regulations, and the transmission of any encrypted data (for example https) is questionable.

In practice, microwave power amplifiers are expensive and decrease receive-sensitivity of link radios. On the other hand, the short wavelength at 2.4 GHz allows for simple construction of very high gain directional antennas. Although Part 15 rules forbid any modification of commercially constructed systems, amateur radio operators may modify commercial systems for optimized construction of long links, for example. Using only 200 mW link radios and high gain directional antennas, a very narrow beam may be used to construct reliable links with minimal radio frequency interference to other users.

Wi-Fi and its support by operating systems

There are two sides to Wi-Fi support under an operating system. Driver level support and configuration and management support.

Driver support is usually provided by the manufacturer of the hardware or, in the case of Unix clones such as Linux and FreeBSD, sometimes through open source projects.

Configuration and management support consists of software to enumerate, join, and check the status of available Wi-Fi networks. This also includes support for various encryption methods. These systems are often provided by the operating system backed by a standard driver model. In most cases, drivers emulate an ethernet device and use the configuration and management utilities built into the operating system. In cases where

built in configuration and management support is non-existent or inadequate, hardware manufacturers may include their own software to handle the respective tasks.

Microsoft Windows

Microsoft Windows has comprehensive driver-level support for Wi-Fi, the quality of which depends on the hardware manufacturer. Hardware manufactures almost always ship Windows drivers with their products. Windows ships with very few Wi-Fi drivers and depends on the OEMs and device manufactures to make sure users get drivers. Configuration and management depend on the version of Windows.

- Earlier versions of Windows, such as 98 and ME do not have built-in configuration and management support and must depend on software provided by the manufacturer
- Microsoft Windows XP's current built-in configuration and management support is inconsistent and buggy [*citation needed*]. The original shipping version of Windows XP included rudimentary support which was dramatically improved in Service Pack 2. Support for WPA2 and some other security protocols require updates from Microsoft. To make up for Windows inconsistent and sometimes inadequate configuration and management support, many hardware manufacturers include their own software and require the user to disable Windows' built-in Wi-Fi support
- Microsoft Windows Vista is expected to have improved Wi-Fi support over Windows XP. Current betas automatically connect to unsecured networks without the user's approval. This is a large security issue for the owner of the respective unsecured access point and for the owner of the Windows Vista based computer because shared folders may be open to public access.

Apple Mac OS

Mac OS is a special case because Apple makes the operating system, the hardware, and the accompanying drivers and configuration and management software. Most Wi-Fi devices used under Mac OS fall under Apple's AirPort product line. All Intel based Mac's either come with or have the option to included AirPort Extreme cards. These cards are compatible with 802.11g. All of Apple's earlier models, starting with the iMac, have included AirPort slots and many included built-in antennas which connect to the AirPort cards. Some third party manufactures have developed Mac OS drivers and configuration and management software or have taken advantage of Apple's own AirPort software and just developed compatible drivers. Cards that work include the D-Link DWL-122 and Macsense Aeropad.

- Versions of Mac OS before 9 do not have any Wi-Fi support due to the fact that they are old and relatively unused at this point, and predate Wi-Fi.
- Mac OS 9 does not have built in support for configuration and management nor does it ship with any Wi-Fi drivers. Apple provides drivers and configuration and

management software for their AirPort cards for OS 9 as do a few other manufacturers.
- Mac OS X has excellent Wi-Fi support, including WPA2, and ships with drivers for Apple's own AirPort cards. The built-in configuration and management is extremely integrated throughout the operating system. Due to the outstanding software and the market share that Apple has over Wi-Fi devices under Mac OS X, third party software developers integrate with Apple's software and the end user experience is seamless. Many third-party manufacturers make compatible hardware along with the appropriate drivers which often integrate with Mac OS X's built-in configuration and management software, or they included their own software.

Unix and BSD Clones

Linux, FreeBSD and similar Unix-like clones have much courser support for Wi-Fi. Due to the open source nature of these operating systems, many different standards have been developed for configuring and managing Wi-Fi devices. The open source nature also fosters open source drivers which have enabled many third party and proprietary devices to work under these operating systems.

- Linux has a very good driver level support [*citation needed*]; however, not all distributions offer a convenient user interface for Wi-Fi configuration. For the few cards without native Linux drivers, NdisWrapper will allow most Windows drivers on x86 compatible Linux systems. Linksys Airgo true MIMO cards are some of the few cards that are not supported.
- FreeBSD has similar Wi-Fi support relative to Linux. Wi-Fi support under FreeBSD is best in the 6.x versions. All or most cards that use the Atheros chipset are supported, along with many others.

Advantages of Wi-Fi

- Allows LANs to be deployed without cabling, typically reducing the costs of network deployment and expansion. Spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless LANs.
- Wi-Fi silicon pricing continues to come down, making Wi-Fi a very economical networking option and driving inclusion of Wi-Fi in an ever-widening array of devices.
- Wi-Fi products are widely available in the market. Different brands of access points and client network interfaces are interoperable at a basic level of service. Products designated as Wi-Fi CERTIFIED by the Wi-Fi Alliance are interoperable and include WPA2 security.
- Wi-Fi networks support roaming, in which a mobile client station such as a laptop computer can move from one access point to another as the user moves around a building or area.
- Wi-Fi is a global set of standards. Unlike cellular carriers, the same Wi-Fi client works in different countries around the world.

- Widely available in more than 250,000 public hot spots and millions of homes and corporate and university campuses worldwide.
- As of 2006, WPA and WPA2 encryption are not easily crackable if strong passwords are used
- New protocols for Quality of Service (WMM) and power saving mechanisms (WMM Power Save) make Wi-Fi even more suitable for latency-sensitive applications (such as voice and video) and small form-factor devices.

Disadvantages of Wi-Fi

- Spectrum assignments and operational limitations are not consistent worldwide; most of Europe allows for an additional 2 channels beyond those permitted in the US; Japan has one more on top of that - and some countries, like Spain, prohibit use of the lower-numbered channels. Furthermore some countries, such as Italy, used to require a 'general authorization' for any Wi-Fi used outside an operator's own premises, or require something akin to an operator registration. For Europe; consult http://www.ero.dk for an annual report on the additional restrictions each European country imposes.
- EIRP in the EU is limited to 20dbm.
- Power consumption is fairly high compared to some other standards, making battery life and heat a concern.
- The most common wireless encryption standard, Wired Equivalent Privacy or WEP, has been shown to be breakable even when correctly configured.
- Wi-Fi Access Points typically default to an open (encryption-free) mode. Novice users benefit from a zero configuration device that works out of the box but might not intend to provide open wireless access to their LAN. WPA Wi-Fi Protected Access which began shipping in 2003 aims to solve these problems and is now generally available, but adoption rates remain low.
- Many 2.4 GHz 802.11b and 802.11g Access points default to the same channel, contributing to congestion on certain channels.
- Wi-Fi networks have limited range. A typical Wi-Fi home router using 802.11b or 802.11g with a stock antenna might have a range of 45 m (150 ft) indoors and 90 m (300 ft) outdoors. Range also varies with frequency band, as Wi-Fi is no exception to the physics of radio wave propagation. Wi-Fi in the 2.4 GHz frequency block has better range than Wi-Fi in the 5 GHz frequency block, and less range than the oldest Wi-Fi (and pre-Wi-Fi) 900 MHz block. Outdoor range with improved antennas can be several kilometres or more with line-of-sight.
- Wi-Fi pollution, meaning interference of a closed or encrypted access point with other open access points in the area, especially on the same or neighboring channel, can prevent access and interfere with the use of other open access points by others caused by overlapping channels in the 802.11g/b spectrum as well as with decreased signal-to-noise ratio (SNR) between access points. This is a widespread problem in high-density areas such as large apartment complexes or office buildings with many Wi-Fi access points.
- It is also an issue when municipalities or other large entities such as universities seek to provide large area coverage. Everyone is considered equal when they use

the band (except for amateur radio operators who are the primary licensee); often this causes contention when one user seeks to claim priority in this unlicensed band. This openness is also important to the success and widespread use of Wi-Fi, but makes Part 15 (US) unsuitable for "must have" public service functions.
- Wi-Fi networks can be monitored and used to read and copy data (including personal information) transmitted over the network when no encryption such as VPN is used.
- Interoperability issues between brands or deviations from the standard can disrupt connections or lower throughput speeds on other user's devices within range. Wi-Fi Alliance programs test devices for interoperability and designate devices which pass testing as Wi-Fi CERTIFIED.

Wi-Fi in gaming

Some gaming consoles and handhelds make use of Wi-Fi technology to enhance the gaming experience:

- The Wii features built-in Wi-Fi.
- The Nintendo DS handheld is Wi-Fi compatible, although it does not support WPA encryption, only the weaker WEP.
- The Sony PSP includes WLAN to connect to Wi-Fi hotspots or make wireless connections.
- The Xbox 360 features 1 Wi-Fi accessory: A wireless network adapter.
- The PlayStation 3 premium model ($599) features built-in Wi-Fi.

Wi-Fi and free software

For more details on this topic, see Comparison of Open Source Wireless Drivers.

- BSDs (FreeBSD, NetBSD, OpenBSD) have had support for most adapters since late 1998. Code for Atheros, Prism, Harris/Intersil and Aironet chips (from assorted Wi-Fi vendors) is mostly shared among the 3 BSDs. Darwin and Mac OS X, despite their overlap with FreeBSD, have their own unique implementation. In OpenBSD 3.7, more drivers for wireless chipsets are available, including RealTek RTL8180L, Ralink RT25x0, Atmel AT76C50x, and Intel 2100 and 2200BG/2225BG/2915ABG, due to at least in part of the OpenBSD's effort to push for open source drivers for wireless chipsets. It is possible that such drivers may be implemented by other BSDs if they do not already exist. The NdisWrapper is also available for FreeBSD.

- Linux: As of version 2.6, some Wi-Fi hardware is supported natively in the Linux kernel. Support for Orinoco, Prism, Aironet and Atmel are included in the main kernel tree, while ADMtek and Realtek RTL8180L are both supported by closed source drivers provided by the manufacturer and open source drivers written by the community. Intel Calexico radios are supported by open sourced drivers available at Sourceforge. Atheros and Ralink RT2x00 are supported through open source projects. As of Kernel 2.6.17, the Broadcom bcm43xx chipset, used on

cards such as Apple Airport Extreme, is supported. Otherwise, support for other wireless devices is available through use of the open source NdisWrapper driver, which allows Linux running on the Intel x86 architecture to "wrap" a vendor's Windows driver for direct use. At least one commercial implementation of the idea is also available. The FSF has some recommended cards[5] and more information can be found through the searchable Linux wireless site[6]

Trademark/certification

Wi-Fi and **Wi-Fi CERTIFIED** are trademarks of the **Wi-Fi Alliance** the trade organization that tests and certifies equipment compliance with the 802.11x standards.

Unintended and intended use by outsiders

The default configuration of most Wi-Fi access points provides no technological protection from unauthorized use of the network. Many business and residential users do not intend to close(secure) their access points but to leave them open for other users in the area. Some argue that it is proper etiquette to leave access points open for others to use just as one can expect to find open access points while on the road.

Measures to deter unauthorized users include suppressing the AP's service set identifier (SSID) broadcast, allowing only computers with known MAC addresses to join the network, and various encryption standards. Older access points (pre-2003) support only weak security measures which won't protect against a determined attacker armed with a packet sniffer and the ability to switch MAC addresses. Recreational exploration of other people's access points has become known as wardriving, and the leaving of graffiti describing available services as warchalking. These activities may be illegal in certain jurisdictions, but existing legislation and case-law is often unclear.

However, it is also common for people to unintentionally use others' Wi-Fi networks without explicit authorization. Operating systems such as Windows XP and Mac OS X automatically connect to an available wireless network, depending on the network configuration. A user who happens to start up a laptop in the vicinity of an access point may find the computer has joined the network without any visible indication. Moreover, a user intending to join one network may instead end up on another one if the latter's signal is stronger. In combination with automatic discovery of other network resources (see DHCP and Zeroconf) this could possibly lead wireless users to send sensitive data to the wrong destination, as described by Chris Meadows in the February 2004 RISKS Digest.