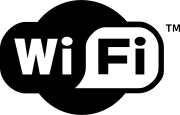
Wi-Fi

[](http://en.wikipedia.org/wiki/File:Wi-Fi_Logo.svg)

[http://en.wikipedia.org/skins-1.5/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:Wi-Fi_Logo.svg)

**Wi-Fi** (pronounced [/ˈwaɪfaɪ/](http://en.wikipedia.org/wiki/Wikipedia:IPA_for_English)) is a [trademark](http://en.wikipedia.org/wiki/Trademark) of the [Wi-Fi Alliance](http://en.wikipedia.org/wiki/Wi-Fi_Alliance) that may be used with certified products that belong to a class of [wireless local area network](http://en.wikipedia.org/wiki/Wireless_LAN) (WLAN) devices based on the [IEEE 802.11](http://en.wikipedia.org/wiki/IEEE_802.11)standards. Because of the close relationship with its underlying standard, the term *Wi-Fi* is often used as a synonym for IEEE 802.11 technology.

The [Wi-Fi Alliance](http://en.wikipedia.org/wiki/Wi-Fi_Alliance) is a global, non-profit association of companies that promotes WLAN technology and certifies products if they conform to certain standards of interoperability. Not every IEEE 802.11-compliant device is submitted for certification to the Wi-Fi Alliance, sometimes because of costs associated with the certification process and the lack of the Wi-Fi logo does not imply a device is incompatible with Wi-Fi devices.

Today, an IEEE 802.11 device is installed in many [personal computers](http://en.wikipedia.org/wiki/Personal_computer), [video game consoles](http://en.wikipedia.org/wiki/Video_game_console),[smartphones](http://en.wikipedia.org/wiki/Smartphone), [printers](http://en.wikipedia.org/wiki/Printer_(computing)), and other [peripherals](http://en.wikipedia.org/wiki/Peripheral), and virtually all [laptop](http://en.wikipedia.org/wiki/Laptop) or palm-sized computers.

[](http://en.wikipedia.org/wiki/File:Linksys_WRT54G_V1.jpg)

[http://en.wikipedia.org/skins-1.5/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:Linksys_WRT54G_V1.jpg)

Common consumer-quality Wi-Fi access point

Uses

**Internet access**

[](http://en.wikipedia.org/wiki/File:WIFI_Amp_Setup.JPG)

[http://en.wikipedia.org/skins-1.5/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:WIFI_Amp_Setup.JPG)

A roof mounted Wi-Fi antenna

A Wi - Fi enabled device such as a [personal computer](http://en.wikipedia.org/wiki/Personal_computer), [video game console](http://en.wikipedia.org/wiki/Video_game_console), [mobile phone](http://en.wikipedia.org/wiki/Mobile_phone), [MP3 player](http://en.wikipedia.org/wiki/MP3_player) or [personal digital assistant](http://en.wikipedia.org/wiki/Personal_digital_assistant) can connect to the [Internet](http://en.wikipedia.org/wiki/Internet) when within range of a [wireless network](http://en.wikipedia.org/wiki/Wireless_network)connected to the Internet. The coverage of one or more interconnected [access points](http://en.wikipedia.org/wiki/Wireless_access_point) — called a [hotspot](http://en.wikipedia.org/wiki/Hotspot_(Wi-Fi)) — can comprise an area as small as a few rooms or as large as many square miles covered by a group of access points with overlapping coverage. Wi-Fi technology has been used in [wireless mesh networks](http://en.wikipedia.org/wiki/Wireless_mesh_network), for example, in London.

In addition to private use in homes and offices, Wi-Fi can provide public access at [Wi-Fi hotspots](http://en.wikipedia.org/wiki/Hotspot_(Wi-Fi)) provided either free of charge or to subscribers to various commercial services. Organizations and[businesses](http://en.wikipedia.org/wiki/Business) such as airports, hotels and restaurants often provide free hotspots to attract or assist clients. Enthusiasts or authorities who wish to provide services or even to promote business in selected areas sometimes provide free Wi-Fi access. As of 2008 there are more than 300 metropolitan-wide Wi-Fi ([Muni-Fi](http://en.wikipedia.org/wiki/Municipal_wireless_network)) projects in progress. There were 879 Wi-Fi based [Wireless Internet service providers](http://en.wikipedia.org/wiki/Wireless_Internet_service_provider) in the [Czech Republic](http://en.wikipedia.org/wiki/Czech_Republic) as of May 2008.

[Routers](http://en.wikipedia.org/wiki/Router) which incorporate a [digital subscriber line](http://en.wikipedia.org/wiki/Digital_subscriber_line) modem or a [cable modem](http://en.wikipedia.org/wiki/Cable_modem) and a Wi-Fi access point, often set up in homes and other premises, provide [Internet](http://en.wikipedia.org/wiki/Internet)-access and [internetworking](http://en.wikipedia.org/wiki/Internetworking) to all devices connected (wirelessly or by cable) to them. One can also connect Wi-Fi devices in [ad hoc mode](http://en.wikipedia.org/wiki/Ad_hoc_mode) for client-to-client connections without a router. Wi-Fi also enables places which would traditionally not have network to be connected, for example [bathrooms](http://en.wikipedia.org/wiki/Bathroom), [kitchens](http://en.wikipedia.org/wiki/Kitchen) and [garden sheds](http://en.wikipedia.org/wiki/Garden_shed).

**Airport Wi-Fi**

In September of 2003, [Pittsburgh International Airport](http://en.wikipedia.org/wiki/Pittsburgh_International_Airport) became the first airport to allow and offer free Wi-Fi throughout its terminal. It is now commonplace.

**City-wide Wi-Fi**

[](http://en.wikipedia.org/wiki/File:Metro_Wireless_Node.jpg)

[http://en.wikipedia.org/skins-1.5/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:Metro_Wireless_Node.jpg)

A municipal wireless antenna in Minneapolis

In the early 2000s, many cities around the world announced plans for a city wide Wi-Fi network. This proved to be much more difficult than their promoters initially envisioned with the result that most of these projects were either canceled or placed on indefinite hold. A few were successful, for example in 2005,[Sunnyvale, California](http://en.wikipedia.org/wiki/Sunnyvale,_California" \o "Sunnyvale, California) became the first city in the [United States](http://en.wikipedia.org/wiki/United_States) to offer city wide free Wi-Fi. Few of the Municipal Wi-Fi firms have now entered into the field of Smart grid networks.

**Campus-wide Wi-Fi**

The first Wi-Fi network in the world was actually a campus based network. [Pittsburgh](http://en.wikipedia.org/wiki/Pittsburgh)'s [Carnegie Mellon University](http://en.wikipedia.org/wiki/Carnegie_Mellon_University) went live with the first-ever Wi-Fi network in 1994.

**Direct computer-to-computer communications**

Wi-Fi also allows communications directly from one computer to another without the involvement of an access point. This is called the *ad-hoc* mode of Wi-Fi transmission. This [wireless ad-hoc network](http://en.wikipedia.org/wiki/Wireless_ad-hoc_network) mode has proven popular with [multiplayer](http://en.wikipedia.org/wiki/Multiplayer) [handheld game consoles](http://en.wikipedia.org/wiki/Handheld_game_console), such as the [Nintendo DS](http://en.wikipedia.org/wiki/Nintendo_DS), [digital cameras](http://en.wikipedia.org/wiki/Digital_cameras), and other [consumer electronics](http://en.wikipedia.org/wiki/Consumer_electronics) devices. A similar method is a new specification called [*Wi-Fi Direct*](http://en.wikipedia.org/wiki/Wi-Fi_Direct)which is promoted by the Wi-Fi Alliance for file transfers and media sharing through a new discovery and security methodology.

**Future directions**

As of 2009 Wi-Fi technology had spread widely within business and industrial sites. In business environments, just like other environments, increasing the number of Wi-Fi access-points provides redundancy, support for fast [roaming](http://en.wikipedia.org/wiki/Roaming) and increased overall network-capacity by using more channels or by defining smaller [cells](http://en.wikipedia.org/wiki/Cellular_network). Wi-Fi enables wireless voice-applications ([VoWLAN](http://en.wikipedia.org/wiki/Voice_over_WLAN" \o "Voice over WLAN) or WVOIP). Over the years, Wi-Fi implementations have moved toward "thin" access-points, with more of the [network intelligence](http://en.wikipedia.org/wiki/Network_intelligence)housed in a centralized network appliance, relegating individual access-points to the role of mere "dumb" radios. Outdoor applications may utilize true [mesh](http://en.wikipedia.org/wiki/Mesh_networking) topologies. As of 2007 Wi-Fi installations can provide a secure [computer networking gateway](http://en.wikipedia.org/wiki/Gateway_(telecommunications)), [firewall](http://en.wikipedia.org/wiki/Firewall), [DHCP](http://en.wikipedia.org/wiki/DHCP) server, [intrusion detection system](http://en.wikipedia.org/wiki/Intrusion_detection_system), and other functions.

History

Wi-Fi uses both single-carrier [direct-sequence spread spectrum](http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum) radio technology (part of the larger family of [spread spectrum](http://en.wikipedia.org/wiki/Spread_spectrum) systems) and multi-carrier [orthogonal frequency-division multiplexing](http://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing) (OFDM) radio technology. The deregulation of certain radio-frequencies for unlicensed spread spectrum deployment enabled the development of Wi-Fi products, its onetime competitor [HomeRF](http://en.wikipedia.org/wiki/HomeRF" \o "HomeRF), [Bluetooth](http://en.wikipedia.org/wiki/Bluetooth), and many other products such as some types of cordless telephones.

Unlicensed spread spectrum was first made available in the US by the [FCC](http://en.wikipedia.org/wiki/Federal_Communications_Commission) in rules adopted on May 9, 1985[[12]](http://en.wikipedia.org/wiki/Wi-Fi#cite_note-11) and these FCC regulations were later copied with some changes in many other countries enabling use of this technology in all major countries. The FCC action was proposed by Michael Marcus of the FCC staff in 1980 and the subsequent regulatory action took 5 more years. It was part of a broader proposal to allow civil use of spread spectrum technology and was opposed at the time by mainstream equipment manufacturers and many radio system operators.

[](http://en.wikipedia.org/wiki/File:Wavelan_Half_ISA_2.4_GHz.jpg)

[http://en.wikipedia.org/skins-1.5/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:Wavelan_Half_ISA_2.4_GHz.jpg)

Half-size [ISA](http://en.wikipedia.org/wiki/Industry_Standard_Architecture) 2.4 GHz [WaveLAN](http://en.wikipedia.org/wiki/WaveLAN" \o "WaveLAN)card by [AT&T](http://en.wikipedia.org/wiki/AT%26T)

The precursor to Wi-Fi was invented in 1991 by [NCR Corporation](http://en.wikipedia.org/wiki/NCR_Corporation)/[AT&T](http://en.wikipedia.org/wiki/AT%26T) (later [Lucent Technologies](http://en.wikipedia.org/wiki/Lucent_Technologies) & [Agere Systems](http://en.wikipedia.org/wiki/Agere_Systems" \o "Agere Systems)) in[Nieuwegein](http://en.wikipedia.org/wiki/Nieuwegein), the Netherlands. It was initially intended for cashier systems; the first wireless products were brought on the market under the name [WaveLAN](http://en.wikipedia.org/wiki/WaveLAN" \o "WaveLAN) with speeds of 1 Mbit/s to 2 Mbit/s. [Vic Hayes](http://en.wikipedia.org/wiki/Vic_Hayes), who held the chair of IEEE 802.11 for 10 years and has been named the "father of Wi-Fi," was involved in designing standards such as [IEEE](http://en.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers) 802.11b, and 802.11a.

Key portions of the IEEE 802.11 technology underlying Wi-Fi (in its a, g, and n varieties) were determined to be infringing on [U.S. Patent 5,487,069](http://www.google.com/patents?vid=5487069), which was filed in 1993 by [CSIRO](http://en.wikipedia.org/wiki/CSIRO), an Australian research body. The patent has been the subject of protracted and ongoing legal battles between CSIRO and major IT corporations. In 2009, the CSIRO settled with 14 companies, including Hewlett-Packard, Intel, Dell, Toshiba, ASUS, Microsoft and Nintendo, under confidential terms. The revenue arising from these settlements to October 2009 is approximately AU$200 million.

Europe leads overall in uptake of wireless-phone technology but the US leads in Wi-Fi systems partly because they lead in laptop usage. As of July 2005, there were at least 68,643 Wi-Fi locations worldwide, a majority in the US, then the UK and Germany. The US and Western Europe make up about 80% of the worldwide Wi-Fi users. Plans are underway in areas of the US to provide public Wi-Fi coverage as a public free service. Even with these large numbers and more expansion, the extent of actual Wi-Fi usage is lower than expected. [Jupiter Research](http://en.wikipedia.org/wiki/Forrester_Research) found that only 15% of people have used Wi-Fi and only 6% in a public place.

Wi-Fi certification

Wi-Fi technology is based on IEEE 802.11 standards. The [IEEE](http://en.wikipedia.org/wiki/IEEE) develops and publishes these standards, but does not test equipment for compliance with them. The non-profit Wi-Fi Alliance was formed in 1999 to fill this void — to establish and enforce standards for interoperability and [backward compatibility](http://en.wikipedia.org/wiki/Backward_compatibility), and to promote wireless local area network technology. Today the Wi-Fi Alliance consists of more than 300 companies from around the world.[[22]](http://en.wikipedia.org/wiki/Wi-Fi#cite_note-21)[[23]](http://en.wikipedia.org/wiki/Wi-Fi#cite_note-22) Manufacturers with membership in the Wi-Fi Alliance, whose products pass the certification process, are permitted to mark those products with the Wi-Fi logo.

Specifically, the certification process requires conformance to the IEEE 802.11 radio standards, the [WPA and WPA2](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) security standards, and the [EAP](http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol) authentication standard. Certification may optionally include tests of IEEE 802.11 draft standards, interaction with cellular phone technology in converged devices, and features relating to security set-up, multimedia, and power saving.

The *Wi-Fi* name

The term *Wi-Fi* suggests *Wireless Fidelity*, compared with the long-established audio equipment certification term *High Fidelity* or [*Hi-Fi*](http://en.wikipedia.org/wiki/Hi-Fi). *Wireless Fidelity* has often been used, even by the Wi-Fi Alliance itself in its press releases and documents, the term may also be found in a white paper on Wi-Fi from [ITAA](http://en.wikipedia.org/wiki/Information_Technology_Association_of_America). However, based on Phil Belanger's statement, there has been a dispute whether the term Wi-Fi was supposed to mean anything at all.

The term *Wi-Fi*, first used commercially in August 1999, was coined by a brand consulting firm called[Interbrand](http://en.wikipedia.org/wiki/Interbrand) Corporation that had been hired by the Alliance to determine a name that was "a little catchier than 'IEEE 802.11b Direct Sequence'." Mr Belanger also said, Interbrand invented *Wi-Fi* as a play on words with [*Hi-Fi*](http://en.wikipedia.org/wiki/Hi-Fi), and also created the [yin yang](http://en.wikipedia.org/wiki/Yin_and_yang)-style Wi-Fi logo. The term Wireless Fidelity was used later as an explanation what Wi-Fi means.

The Wi-Fi Alliance initially used an [advertising slogan](http://en.wikipedia.org/wiki/Advertising_slogan) for Wi-Fi "The Standard for Wireless Fidelity",but later removed the phrase from their marketing. Despite this, some documents from the Alliance dated 2003 and 2004 still contain the term *Wireless Fidelity*. There was also no official statement for dropping the term.

The yin yang logo indicates that a product had been certified for [interoperability](http://en.wikipedia.org/wiki/Interoperability).

Advantages and challenges

[](http://en.wikipedia.org/wiki/File:WiFi-detector.jpg)

[http://en.wikipedia.org/skins-1.5/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:WiFi-detector.jpg)

A keychain size Wi-Fi detector.

**Operational advantages**

Wi-Fi allows [local area networks](http://en.wikipedia.org/wiki/Local_area_network) (LANs) to be deployed without wires for client devices, 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.

Wireless network adapters are now built into most laptops. The price of [chipsets](http://en.wikipedia.org/wiki/Chipset) for Wi-Fi continues to drop, making it an economical networking option included in even more devices. Wi-Fi has become widespread in corporate infrastructures.

Different competitive brands of access points and client network interfaces are inter-operable at a basic level of service. Products designated as "Wi-Fi Certified" by the Wi-Fi Alliance are backwards compatible. Wi-Fi is a global set of standards. Unlike [mobile phones](http://en.wikipedia.org/wiki/Mobile_phone), any standard Wi-Fi device will work anywhere in the world.

Wi-Fi is widely available in more than 220,000 public hotspots and tens of millions of homes and corporate and university campuses worldwide.The current version of [Wi-Fi Protected Access](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access)encryption (WPA2) is considered secure, provided a strong [passphrase](http://en.wikipedia.org/wiki/Passphrase) is used. New protocols for Quality of Service ([WMM](http://en.wikipedia.org/wiki/Wireless_Multimedia_Extensions)) make Wi-Fi more suitable for latency-sensitive applications (such as voice and video), and power saving mechanisms (WMM Power Save) improve battery operation.

**Limitations**

Spectrum assignments and operational limitations are not consistent worldwide. Most of Europe allows for an additional 2 channels beyond those permitted in the U.S. for the 2.4 GHz band. (1–13 vs. 1–11); Japan has one more on top of that (1–14). Europe, as of 2007, was essentially homogeneous in this respect. A very confusing aspect is the fact that a Wi-Fi signal actually occupies five channels in the 2.4 GHz band resulting in only three non-overlapped channels in the U.S.: 1, 6, 11, and three or four in Europe: 1, 5, 9, 13 can be used if all the equipment on a specific area can be guaranteed not to use 802.11b at all, even as fallback or beacon. [Equivalent isotropically radiated power](http://en.wikipedia.org/wiki/Equivalent_isotropically_radiated_power) (EIRP) in the EU is limited to 20 [dBm](http://en.wikipedia.org/wiki/DBm" \o "DBm) (100 mW).

**Reach**

[](http://en.wikipedia.org/wiki/File:Long_Distance_802.11_Wi-Fi_-_dish,_Venezuela.jpg)

[http://en.wikipedia.org/skins-1.5/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:Long_Distance_802.11_Wi-Fi_-_dish,_Venezuela.jpg)

Large [satellite dish](http://en.wikipedia.org/wiki/Satellite_dish) modified for[long-range Wi-Fi](http://en.wikipedia.org/wiki/Long-range_Wi-Fi) communications in[Venezuela](http://en.wikipedia.org/wiki/Venezuela)

Wi-Fi networks have limited range. A typical [wireless router](http://en.wikipedia.org/wiki/Wireless_router) using[802.11b](http://en.wikipedia.org/wiki/IEEE_802.11#802.11b) or [802.11g](http://en.wikipedia.org/wiki/IEEE_802.11#802.11g) with a stock antenna might have a range of 32 m (120 ft) indoors and 95 m (300 ft) outdoors. The new IEEE 802.11n however, can exceed that range by more than double.Range also varies with frequency band. Wi-Fi in the 2.4 GHz frequency block has slightly better range than Wi-Fi in the 5 GHz frequency block. Outdoor range with improved (directional) antennas can be several kilometres or more with line-of-sight. In general, the maximum amount of power that a Wi-Fi device can transmit is limited by local regulations, such as [FCC Part 15](http://en.wikipedia.org/wiki/FCC_Part_15) in USA.

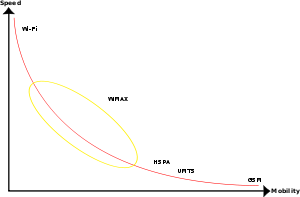
Wi-Fi performance decreases roughly quadratically as distance increases at constant radiation levels.

Due to reach requirements for wireless LAN applications, power consumption is fairly high compared to some other standards. Technologies such as [Bluetooth](http://en.wikipedia.org/wiki/Bluetooth), which are designed to support wireless [PAN](http://en.wikipedia.org/wiki/Personal_area_network) applications, provide a much shorter propagation range of <10m (ref. e.g. IEEE Std. 802.15.4 section 1.2 scope) and so in general have a lower power consumption. Other low-power technologies such as [ZigBee](http://en.wikipedia.org/wiki/ZigBee" \o "ZigBee) have fairly long range, but much lower data rate. The high power consumption of Wi-Fi makes battery life a concern for mobile devices.

A number of "no new wires" technologies have been developed to provide alternatives to Wi-Fi for applications in which Wi-Fi's indoor range is not adequate and where installing new wires (such as [CAT-5](http://en.wikipedia.org/wiki/CAT-5)) is not possible or cost-effective. One example is the [ITU-T](http://en.wikipedia.org/wiki/ITU-T) [G.hn](http://en.wikipedia.org/wiki/G.hn) standard for high speed [Local area networks](http://en.wikipedia.org/wiki/Local_area_network) using existing home wiring ([coaxial cables](http://en.wikipedia.org/wiki/Ethernet_over_coax), phone lines and [power lines](http://en.wikipedia.org/wiki/Power_line_communication)). Although [G.hn](http://en.wikipedia.org/wiki/G.hn) does not provide some of the advantages of Wi-Fi (such as mobility or outdoor use), it's designed for applications (such as [IPTV](http://en.wikipedia.org/wiki/IPTV) distribution) where indoor range is more important than mobility.

Due to the complex nature of [radio propagation](http://en.wikipedia.org/wiki/Radio_propagation) at typical Wi-Fi frequencies, particularly the effects of signal reflection off trees and buildings, Wi-Fi signal strength can only be predicted generally for any given area in relation to a transmitter. This effect does not apply equally to [long-range Wi-Fi](http://en.wikipedia.org/wiki/Long-range_Wi-Fi), since longer links typically operate from towers that broadcast above the surrounding foliage.

**Mobility**

[](http://en.wikipedia.org/wiki/File:Wimax.svg)

[http://en.wikipedia.org/skins-1.5/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:Wimax.svg)

Speed vs. Mobility of wireless systems: Wi-Fi, [HSPA](http://en.wikipedia.org/wiki/High_Speed_Packet_Access),[UMTS](http://en.wikipedia.org/wiki/UMTS" \o "UMTS), [GSM](http://en.wikipedia.org/wiki/GSM)

Because of the very limited practical range of Wi-Fi, mobile use is essentially confined to such applications as inventory taking machines in warehouses or retail spaces, [barcode](http://en.wikipedia.org/wiki/Barcode) reading devices at check-out stands or receiving / shipping stations. Mobile use of Wi-Fi over wider ranges is limited to move, use, as for instance in an automobile moving from one hotspot to another (known as [Wardriving](http://en.wikipedia.org/wiki/Wardriving" \o "Wardriving)). Other wireless technologies are more suitable as illustrated in the graphic.

**Data security risks**

The most common wireless [encryption](http://en.wikipedia.org/wiki/Encryption) standard,[Wired Equivalent Privacy](http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy" \o "Wired Equivalent Privacy) or WEP, has been shown to be easily breakable even when correctly configured. [Wi-Fi Protected Access](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) (WPA and WPA2) encryption, which became available in devices in 2003, aimed to solve this problem. Wi-Fi [access points](http://en.wikipedia.org/wiki/Wireless_access_point) typically default to an encryption-free (*open*) mode. Novice users benefit from a zero-configuration device that works out of the box, but this default is without any [wireless security](http://en.wikipedia.org/wiki/Wireless_security#Counteracting_risks) enabled, providing open wireless access to their LAN. To turn security on requires the user to configure the device, usually via a software [graphical user interface](http://en.wikipedia.org/wiki/Graphical_user_interface) (GUI). Wi-Fi networks that are unencrypted can be monitored and data (including personal information) may be recorded, but may be protected by other means, such as a [virtual private network](http://en.wikipedia.org/wiki/Virtual_private_network) or by secure [Hypertext Transfer Protocol](http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol) ([HTTPS](http://en.wikipedia.org/wiki/HTTPS)) and [Transport Layer Security](http://en.wikipedia.org/wiki/Transport_Layer_Security).

**Population**

Many 2.4 GHz [802.11b](http://en.wikipedia.org/wiki/IEEE_802.11#802.11b) and [802.11g](http://en.wikipedia.org/wiki/IEEE_802.11#802.11g) access points default to the same channel on initial startup, contributing to congestion on certain channels. To change the channel of operation for an access point requires the user to configure the device.

**Channel pollution**

Standardization is a process driven by market forces. Interoperability issues between non-Wi-Fi brands or proprietary deviations from the standard can still disrupt connections or lower throughput speeds on all user's devices that are within range, to include the non-Wi-Fi or proprietary product. Moreover, the usage of the ISM band in the 2.45 GHz range is also common to [Bluetooth](http://en.wikipedia.org/wiki/Bluetooth), [WPAN](http://en.wikipedia.org/wiki/Personal_area_network)-[CSS](http://en.wikipedia.org/wiki/Chirp_spread_spectrum), [ZigBee](http://en.wikipedia.org/wiki/ZigBee" \o "ZigBee) and any new system will take its share.

Wi-Fi pollution, or an excessive number of access points in the area, especially on the same or neighboring channel, can prevent access and interfere with the use of other access points by others, caused by overlapping channels in the 802.11g/b spectrum, as well as with decreased [signal-to-noise ratio](http://en.wikipedia.org/wiki/Signal-to-noise_ratio) (SNR) between access points. This can be a problem in high-density areas, such as large apartment complexes or office buildings with many Wi-Fi access points. Additionally, other devices use the 2.4 GHz band: microwave ovens, security cameras, [ZigBee](http://en.wikipedia.org/wiki/ZigBee" \o "ZigBee) devices, [Bluetooth](http://en.wikipedia.org/wiki/Bluetooth) devices and (in some countries)[Amateur radio](http://en.wikipedia.org/wiki/Amateur_radio), [video senders](http://en.wikipedia.org/wiki/Video_sender), cordless phones and baby monitors, all of which can cause significant additional interference. It is also an issue when municipalities,[[38]](http://en.wikipedia.org/wiki/Wi-Fi" \l "cite_note-37) or other large entities such as universities, seek to provide large area coverage. This openness is also important to the success and widespread use of 2.4 GHz Wi-Fi.

Hardware

**Standard devices**

[](http://en.wikipedia.org/wiki/File:RouterBoard_112_with_U.FL-RSMA_pigtail_and_R52_miniPCI_Wi-Fi_card.jpg)

[http://en.wikipedia.org/skins-1.5/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:RouterBoard_112_with_U.FL-RSMA_pigtail_and_R52_miniPCI_Wi-Fi_card.jpg)

An [embedded](http://en.wikipedia.org/wiki/Embedded_system) RouterBoard 112 with[U.FL](http://en.wikipedia.org/wiki/U.FL)-[RSMA](http://en.wikipedia.org/wiki/SMA_connector) pigtail and R52 [mini PCI](http://en.wikipedia.org/wiki/Mini_PCI) Wi-Fi card widely used by [wireless](http://en.wikipedia.org/wiki/Wireless) [Internet](http://en.wikipedia.org/wiki/Internet) service providers ([WISPs](http://en.wikipedia.org/wiki/Wireless_Internet_service_provider)) in the [Czech Republic](http://en.wikipedia.org/wiki/Czech_Republic).

[](http://en.wikipedia.org/wiki/File:3GN_.jpg)

[http://en.wikipedia.org/skins-1.5/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:3GN_.jpg)

OSBRiDGE 3GN - [802.11n](http://en.wikipedia.org/wiki/802.11n)Access Point and [UMTS/GSM](http://en.wikipedia.org/wiki/High-Speed_Downlink_Packet_Access)Gateway in one device.

[](http://en.wikipedia.org/wiki/File:Wireless_adaptor_USB.jpg)

[http://en.wikipedia.org/skins-1.5/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:Wireless_adaptor_USB.jpg)

[USB](http://en.wikipedia.org/wiki/USB) wireless adapter

A [wireless access point](http://en.wikipedia.org/wiki/Wireless_access_point) (WAP) connects a group of wireless devices to an adjacent wired [LAN](http://en.wikipedia.org/wiki/LAN). An access point is similar to a [network hub](http://en.wikipedia.org/wiki/Network_hub), relaying [data](http://en.wikipedia.org/wiki/Data_(computing)) between connected wireless devices in addition to a (usually) single connected wired device, most often an ethernet hub or switch, allowing wireless devices to communicate with other wired devices.

[Wireless adapters](http://en.wikipedia.org/wiki/Wireless_network_interface_card) allow devices to connect to a wireless network. These adapters connect to devices using various external or internal interconnects such as [PCI](http://en.wikipedia.org/wiki/Conventional_PCI" \o "Conventional PCI),[miniPCI](http://en.wikipedia.org/wiki/MiniPCI), [USB](http://en.wikipedia.org/wiki/Universal_Serial_Bus), [ExpressCard](http://en.wikipedia.org/wiki/ExpressCard" \o "ExpressCard), Cardbus and [PC Card](http://en.wikipedia.org/wiki/PC_Card). Most newer laptop computers are equipped with internal adapters. Internal cards are generally more difficult to install.

Wireless [routers](http://en.wikipedia.org/wiki/Router) integrate a Wireless Access Point, ethernet [switch](http://en.wikipedia.org/wiki/Network_switch), and internal Router firmware application that provides [IP](http://en.wikipedia.org/wiki/Internet_Protocol) [Routing](http://en.wikipedia.org/wiki/Routing" \o "Routing),[NAT](http://en.wikipedia.org/wiki/Network_address_translation), and [DNS](http://en.wikipedia.org/wiki/Domain_Name_System) forwarding through an integrated [WAN](http://en.wikipedia.org/wiki/Wide_area_network) interface. A wireless router allows wired and wireless ethernet LAN devices to connect to a (usually) single WAN device such as [cable modem](http://en.wikipedia.org/wiki/Cable_modem) or[DSL modem](http://en.wikipedia.org/wiki/DSL_modem). A wireless router allows all three devices (mainly the access point and router) to be configured through one central utility. This utility is most usually an integrated [web server](http://en.wikipedia.org/wiki/Web_server) which serves web pages to wired and wireless LAN clients and often optionally to WAN clients. This utility may also be an application that is run on a desktop computer such as Apple's [AirPort](http://en.wikipedia.org/wiki/AirPort).

Wireless [network bridges](http://en.wikipedia.org/wiki/Network_bridge) connect 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](http://en.wikipedia.org/wiki/OSI_model#Layer_2:_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.

Wireless range extenders or wireless repeaters can extend the range of an existing wireless network. Range extenders can be strategically placed to elongate a signal area or allow for the signal area to reach around barriers such as those created in L-shaped corridors. Wireless devices connected through repeaters will suffer from an increased latency for each hop. Additionally, a wireless device connected to any of the repeaters in the chain will have a throughput that is limited by the weakest link between the two nodes in the chain from which the connection originates to where the connection ends.

**Distance records**

Distance records (using non-standard devices) include 382 km (237 mi) in June 2007, held by Ermanno Pietrosemoli and EsLaRed of Venezuela, transferring about 3 MB of data between mountain tops of El Aguila and Platillon.[[39]](http://en.wikipedia.org/wiki/Wi-Fi#cite_note-38)[[40]](http://en.wikipedia.org/wiki/Wi-Fi#cite_note-39) The[Swedish Space Agency](http://en.wikipedia.org/wiki/Swedish_National_Space_Board) transferred data 310 km (193 mi), using 6 watt amplifiers to reach an overhead stratospheric balloon.[[41]](http://en.wikipedia.org/wiki/Wi-Fi#cite_note-40)

**Embedded systems**

[](http://en.wikipedia.org/wiki/File:Ezurio_wism2_small.jpg)

[http://en.wikipedia.org/skins-1.5/common/images/magnify-clip.png](http://en.wikipedia.org/wiki/File:Ezurio_wism2_small.jpg)

Embedded serial-to-Wi-Fi module

Wi-Fi availability in the home is on the increase. This extension of the Internet into the home space will increasingly be used for remote monitoring. Examples of remote monitoring include security systems and tele-medicine. In all these kinds of implementation, if the Wi-Fi provision is provided using a system running one of operating systems mentioned above, then it becomes unfeasible due to weight, power consumption and cost issues.

Increasingly in the last few years (particularly as of early 2007), embedded Wi-Fi modules have become available which come with a real-time operating system and provide a simple means of wireless enabling any device which has and communicates via a serial port.This allows simple monitoring devices – for example, a portable ECG monitor hooked up to a patient in their home – to be created. This Wi-Fi enabled device effectively becomes part of the Internet cloud and can communicate with any other node on the Internet. The data collected can hop via the home's Wi-Fi access point to anywhere on the Internet.

These Wi-Fi modules are designed so that designers need minimal Wi-Fi knowledge to wireless-enable their products.

Network security

The main issue with wireless network security is its simplified access to the network compared to traditional wired networks such as [ethernet](http://en.wikipedia.org/wiki/Ethernet" \o "Ethernet). With wired networking it is necessary to either gain access to a building, physically connecting into the internal network, or break through an external [firewall](http://en.wikipedia.org/wiki/Firewall). Most business networks protect sensitive data and systems by attempting to disallow external access. Thus being able to get wireless reception provides an attack vector, if encryption is not used or can be defeated.[[45]](http://en.wikipedia.org/wiki/Wi-Fi#cite_note-44)

Attackers who have gained access to a Wi-Fi network can use DNS spoofing attacks very effectively against any other user of the network, because they can see the DNS requests made, and often respond with a spoofed answer before the queried DNS server has a chance to reply.[[46]](http://en.wikipedia.org/wiki/Wi-Fi#cite_note-45)

**Securing methods**

A common but unproductive measure to deter unauthorized users is to suppress the AP's [SSID](http://en.wikipedia.org/wiki/Service_set_(802.11_network)) broadcast, "hiding" it. This is ineffective as a security method because the SSID is broadcast in the clear in response to a client SSID query. Another unproductive method is to only allow computers with known [MAC addresses](http://en.wikipedia.org/wiki/MAC_address) to join the network. The fault with this method is MAC addresses can often, but not always, be set by a user (spoofed) with minimal effort. If the eavesdropper has the ability to change his MAC address, then they may join the network by [spoofing](http://en.wikipedia.org/wiki/Spoofing_attack) an authorized address.

[Wired Equivalent Privacy](http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) (WEP) encryption was designed to protect against casual snooping, but is now deprecated. Tools such as [AirSnort](http://en.wikipedia.org/wiki/AirSnort" \o "AirSnort) or [Aircrack-ng](http://en.wikipedia.org/wiki/Aircrack-ng" \o "Aircrack-ng) can quickly recover WEP encryption keys. Once it has seen 5-10 million encrypted packets, AirSnort can determine the encryption password in under a second;[[47]](http://en.wikipedia.org/wiki/Wi-Fi" \l "cite_note-46) newer tools such as aircrack-ptw can use [Klein's attack](http://en.wikipedia.org/wiki/RC4#Klein.27s_Attack) to crack a WEP key with a 50% success rate using only 40,000 packets.

To counteract this in 2002, the [Wi-Fi Alliance](http://en.wikipedia.org/wiki/Wi-Fi_Alliance) approved [Wi-Fi Protected Access](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) (WPA) which uses [TKIP](http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol" \o "Temporal Key Integrity Protocol)as a stopgap solution for legacy equipment. Though more secure than WEP, it has outlived its designed lifetime, has known attack vectors and is no longer recommended.

In 2004, the full [IEEE 802.11i](http://en.wikipedia.org/wiki/IEEE_802.11i-2004) (WPA2) encryption standards were released. If used with a [802.1X](http://en.wikipedia.org/wiki/802.1X) server or in [pre-shared key](http://en.wikipedia.org/wiki/Pre-shared_key) mode with a [strong and uncommon passphrase](http://en.wikipedia.org/wiki/Password_strength) WPA2 is still considered secure, as of 2009.

**Piggybacking**

During the early popular adoption of [802.11](http://en.wikipedia.org/wiki/802.11), providing open access points for anyone within range to use was encouraged to cultivate [wireless community networks](http://en.wikipedia.org/wiki/Wireless_community_network);[[48]](http://en.wikipedia.org/wiki/Wi-Fi#cite_note-47) particularly since people on average use only a fraction of their downstream bandwidth at any given time.

Recreational logging and mapping of other people's access points has become known as [wardriving](http://en.wikipedia.org/wiki/Wardriving" \o "Wardriving). It is also common for people to use open (unencrypted) Wi-Fi networks as a free service, termed [piggybacking](http://en.wikipedia.org/wiki/Piggybacking_(internet_access)). Indeed, many access points are intentionally installed without security turned on so that they can be used as a free service. Providing access to one's Internet connection in this fashion may be contrary to the Terms of Service or contract with the [ISP](http://en.wikipedia.org/wiki/ISP). These activities do not result in sanctions in most jurisdictions, however legislation and [case law](http://en.wikipedia.org/wiki/Case_law) differ considerably across the world. A proposal to leave [graffiti](http://en.wikipedia.org/wiki/Graffiti) describing available services was called [warchalking](http://en.wikipedia.org/wiki/Warchalking" \o "Warchalking). In a [Florida](http://en.wikipedia.org/wiki/Florida) court case, owner laziness was determined not to be a valid excuse Piggybacking is often unintentional. Most access points are configured without encryption by default, and operating systems such as [Windows XP SP2](http://en.wikipedia.org/wiki/Windows_XP_SP2), [Mac OS X](http://en.wikipedia.org/wiki/Mac_OS_X) or [Ubuntu Linux](http://en.wikipedia.org/wiki/Ubuntu_Linux" \o "Ubuntu Linux) may be configured to automatically connect to any available wireless network. 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](http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol) and [Zeroconf](http://en.wikipedia.org/wiki/Zeroconf" \o "Zeroconf)) this could possibly lead wireless users to send sensitive data to the wrong middle man when seeking a destination. For example, a user could inadvertently use an insecure network to login to a [website](http://en.wikipedia.org/wiki/Website), thereby making the login credentials available to anyone listening, if the website is using an insecure protocol like [HTTP](http://en.wikipedia.org/wiki/HTTP).