Wi-Fi

From Wikipedia, the free encyclopedia

For the radio station, see WIFI (AM).

Wi-Fi (or **WiFi**) is a local area wireless computer networking technology that allows electronic devices to network, mainly using the 2.4 gigahertz (12 cm) UHF and 5 gigahertz (6 cm) SHF ISM radio bands.

Wi-Fi

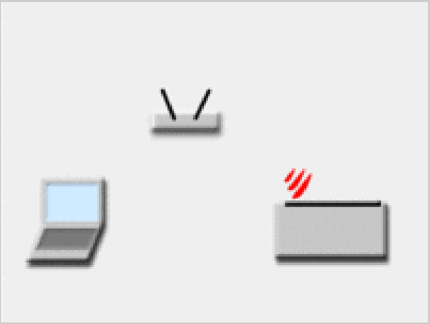
Developed by	Wi-Fi Alliance
Compatible hardware	mobile phones, personal computers, gaming consoles

The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network" (WLAN) product based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards.[1] However, the term "Wi-Fi" is used in general English as a synonym for "WLAN" since most modern WLANs are based on these standards. "Wi-Fi" is a trademark of the Wi-Fi Alliance. The "Wi-Fi Certified" trademark can only be used by Wi-Fi products that successfully complete Wi-Fi Alliance interoperability certification testing.

Many devices can use Wi-Fi, e.g. personal computers, video-game consoles, smartphones, digital cameras, tablet computers and digital audio players. These can connect to a network resource such as the Internet via a wireless network access point. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometres achieved by using multiple overlapping access points.

Wi-Fi can be less secure than wired connections, such as Ethernet, precisely because an intruder does not need a physical connection. Web pages that use TLS are secure, but unencrypted internet access can easily be detected by intruders. Because of this, Wi-Fi has adopted various encryption technologies. The early encryption WEP proved easy to break. Higher quality protocols (WPA, WPA2) were added later. An optional feature added in 2007, called Wi-Fi Protected Setup (WPS), had a serious flaw that allowed an attacker to recover the router's password.[2] The Wi-Fi Alliance has since updated its test plan and certification program to ensure all newly certified devices resist attacks.

Contents



Depiction of a device sending information wirelessly to another device, both connected to the local network, in order to print a document.

History

Main article: IEEE 802.11 § History

In 1971, ALOHAnet connected the Hawaiian Islands with a UHF wireless packet network. ALOHAnet and the ALOHA protocol were early forerunners to Ethernet, and later the IEEE 802.11 protocols, respectively.

A 1985 ruling by the U.S. Federal Communications Commission released the ISM band for unlicensed use.[3] These frequency bands are the same ones used by equipment such as microwave ovens and are subject to interference.

In 1991, NCR Corporation with AT&T Corporation invented the precursor to 802.11, intended for use in cashier systems. The first wireless products were under the name WaveLAN.

The Australian radio-astronomer John O'Sullivan developed a key patent used in Wi-Fi as a by-product of a Commonwealth Scientific and Industrial Research Organisation (CSIRO) research project, "a failed experiment to detect exploding mini black holes the size of an atomic particle".[4] In 1992 and 1996, CSIRO obtained patents[5] for a method later used in Wi-Fi to "unsmear" the signal.[6]

The first version of the 802.11 protocol was released in 1997, and provided up to 2 Mbit/s link speeds. This was updated in 1999 with 802.11b to permit 11 Mbit/s link speeds, and this proved to be popular.

In 1999, the Wi-Fi Alliance formed as a trade association to hold the Wi-Fi trademark under which most products are sold.[7]

Wi-Fi uses a large number of patents held by many different organizations.[8] In April 2009, 14 technology companies agreed to pay CSIRO Rs34,752.17 million for infringements on CSIRO patents.[9] This led to Australians labeling Wi-Fi as an Australian invention,[10] though this has been the subject of some controversy.[11][12] CSIRO won a further Rs30,581.91 million settlement for Wi-Fi patent-infringements in 2012 with global firms in the United States required to pay the CSIRO licensing rights estimated to be worth an additional Rs139.01 billion in royalties.[9][13][14]

The name 'Wi-Fi'

The term *Wi-Fi*, commercially used at least as early as August 1999,[15] was coined by brand-consulting firm Interbrand Corporation. The Wi-Fi Alliance had hired Interbrand to determine a name that was "a little catchier than 'IEEE 802.11b Direct Sequence'".[16][17][18] Phil Belanger, a founding member of the Wi-Fi Alliance who presided over the selection of the name "Wi-Fi", also stated that Interbrand invented *Wi-Fi* as a play on words with *Hi-Fi*, and also created the Wi-Fi logo.

The Wi-Fi Alliance used the "nonsense" advertising slogan "The Standard for Wireless Fidelity" for a short time after the brand name was invented, leading to the misconception that Wi-Fi was an abbreviation of "Wireless Fidelity".[16][19][20] The yin-yang Wi-Fi logo indicates the certification of a product for interoperability.[19]

Non-Wi-Fi technologies intended for fixed points, such as Motorola Canopy, are usually described as fixed wireless. Alternative wireless technologies include mobile phone standards, such as 2G, 3G, 4G or LTE.

The name is often written as **WiFi** or **Wifi**, but these are not approved by the Wi-Fi Alliance.

Wi-Fi certification

See also: Wi-Fi Alliance

The IEEE does not test equipment for compliance with their standards. The non-profit Wi-Fi Alliance was formed in 1999 to fill this void — to establish and enforce standards for interoperability and backward compatibility, and to promote wireless local-area-network technology. As of 2010, the Wi-Fi Alliance consisted of more than 375 companies from around the world.[21][22] The Wi-Fi Alliance enforces the use of the Wi-Fi brand to technologies based on the IEEE 802.11 standards from the IEEE. This includes wireless local area network (WLAN) connections, device to device connectivity (such as Wi-Fi Peer to Peer aka Wi-Fi Direct), Personal area network (PAN), local area network (LAN) and even some limited wide area network (WAN) connections. Manufacturers with membership in the Wi-Fi Alliance, whose products pass the certification process, gain the right 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 security standards, and the EAP 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.[23]

Not every Wi-Fi device is submitted for certification. The lack of Wi-Fi certification does not necessarily imply that a device is incompatible with other Wi-Fi devices. If it is compliant or partly compatible, the Wi-Fi Alliance may not object to its description as a Wi-Fi device though technically only certified devices are approved. The Wi-Fi Alliance may or may not sanction derivative terms, such as Super Wi-Fi, coined by the US Federal Communications Commission (FCC) to describe proposed networking in the UHF TV band in the US.

IEEE 802.11 standard

Main article: IEEE 802.11

The IEEE 802.11 standard is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5, and 60 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997, and has had subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand. While each amendment is officially revoked when it is incorporated in the latest version of the standard, the corporate world tends to market to the revisions because they concisely denote capabilities of their products. As a result, in the market place, each revision tends to become its own standard.

Uses

To connect to a Wi-Fi LAN, a computer has to be equipped with a wireless network interface controller. The combination of computer and interface controller is called a *station*. For all stations that share a single radio frequency communication channel, transmissions on this channel are received by all stations within range. The transmission is not guaranteed to be delivered and is therefore a best-effort delivery mechanism. A carrier wave is used to transmit the data. The data is organised in packets, referred to as "Ethernet frames".

The Linksys WRT54G contains a router with an 802.11b/g radio (common in the early 2000s) and two antennas

Internet access

Wi-Fi technology may be used to provide Internet access to devices that are within the range of a wireless network that is connected to the Internet. The coverage of one or more interconnected access points (*hotspots*) can extend from an area as small as a few rooms to as large as many square kilometres. Coverage in the larger area may require a group of access points with overlapping coverage. For example, public outdoor Wi-Fi technology has been used successfully in wireless mesh networks in London, UK. An international example is FON.

Wi-Fi provides service in private homes, businesses, as well as in public spaces at Wi-Fi hotspots set up either free-of-charge or commercially, often using a captive portal webpage for access. Organizations and businesses, such as airports, hotels, and restaurants, often provide free-use hotspots to attract customers. Enthusiasts or authorities who wish to provide services or even to promote business in selected areas sometimes provide free Wi-Fi access.

A sticker indicating to the public that a location is within range of a Wi-Fi network. A dot with curved lines radiating from it is a common symbol for Wi-Fi, representing a point transmitting a signal.[24]

Routers that incorporate a digital subscriber line modem or a cable modem and a Wi-Fi access point, often set up in homes and other buildings, provide Internet access and internetworking to all devices connected to them, wirelessly or via cable.

Similarly, battery-powered routers may include a cellular Internet radiomodem and Wi-Fi access point. When subscribed to a cellular data carrier, they allow nearby Wi-Fi stations to access the Internet over 2G, 3G, or 4G networks using the tethering technique. Many smartphones have a built-in capability of this sort, including those based on Android, BlackBerry, Bada, iOS (iPhone), Windows Phone and Symbian, though carriers often disable the feature, or charge a separate fee to enable it, especially for customers with unlimited data plans. "Internet packs" provide standalone facilities of this type as well, without use of a smartphone; examples include the MiFi- and WiBro-branded devices. Some laptops that have a cellular modem card can also act as mobile Internet Wi-Fi access points.

Wi-Fi also connects places that normally don't have network access, such as kitchens and garden sheds.

City-wide Wi-Fi

Further information: Municipal wireless network

In the early 2000s, many cities around the world announced plans to construct city-wide Wi-Fi networks. There are many successful examples; in 2004, Mysore became India's first Wi-Fi-enabled city. A company called WiFiyNet has set up hotspots in Mysore, covering the complete city and a few nearby villages.[25]

In 2005, St. Cloud, Florida and Sunnyvale, California, became the first cities in the United States to offer city-wide free Wi-Fi (from MetroFi).[26] Minneapolis has generated Rs166.81 million in profit annually for its provider.[27]

In May 2010, London, UK, Mayor Boris Johnson pledged to have London-wide Wi-Fi by 2012.[28] Several boroughs including Westminster and Islington[29][30] already had extensive outdoor Wi-Fi coverage at that point.

An outdoor Wi-Fi access point

Officials in South Korea's capital are moving to provide free Internet access at more than 10,000 locations around the city, including outdoor public spaces, major streets and densely populated residential areas. Seoul will grant leases to KT, LG Telecom and SK Telecom. The companies will invest Rs6,116.38 million in the project, which will be completed in 2015.[31]

Campus-wide Wi-Fi

Many traditional university campuses in the developed world provide at least partial Wi-Fi coverage. Carnegie Mellon University built the first campus-wide wireless Internet network, called Wireless Andrew, at its Pittsburgh campus in 1993 before Wi-Fi branding originated.[32][33][34] By February 1997 the CMU wifi zone was fully operational. Many universities collaborate in providing Wi-Fi access to students and staff through the eduroam international authentication infrastructure.

Direct computer-to-computer communications

Wi-Fi also allows communications directly from one computer to another without an access point intermediary. This is called *ad hoc* Wi-Fi transmission. This wireless ad hoc network mode has proven popular with multiplayer handheld game consoles, such as the Nintendo DS, PlayStation Portable, digital cameras, and other consumer electronics devices. Some devices can also share their Internet connection using ad hoc, becoming hotspots or "virtual routers".[35]

Similarly, the Wi-Fi Alliance promotes the specification Wi-Fi Direct for file transfers and media sharing through a new discovery- and security-methodology.[36] Wi-Fi Direct launched in October 2010.[37]

Another mode of direct communication over Wi-Fi is Tunneled Direct Link Setup (TDLS), which enables two devices on the same Wi-Fi network to communicate directly, instead of via the access point.[38]

Wi-Fi radio spectrum

A keychain-size Wi-Fi detector

Main article: list of WLAN channels

802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 Rules and Regulations. Because of this choice of frequency band, 802.11b and g equipment may occasionally suffer interference from microwave ovens, cordless telephones, and Bluetooth devices.

Spectrum assignments and operational limitations are not consistent worldwide: Australia and Europe allow for an additional two channels beyond the 11 permitted in the United States for the 2.4 GHz band (1–13), while Japan has three more (1–14). In the US and other countries, 802.11a and 802.11g devices may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations.

A Wi-Fi signal occupies five channels in the 2.4 GHz band. Any two channel numbers that differ by five or more, such as 2 and 7, do not overlap. The oft-repeated adage that channels 1, 6, and 11 are the *only* non-overlapping channels is, therefore, not accurate. Channels 1, 6, and 11 are the only *group of three* non-overlapping channels in North America and the United Kingdom. In Europe and Japan using Channels 1, 5, 9, and 13 for 802.11g and 802.11n is recommended.

802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping channels rather than the 2.4 GHz ISM frequency band, where adjacent channels overlap.

Interference

For more details on this topic, see Electromagnetic interference at 2.4 GHz.

Wi-Fi connections can be disrupted or the internet speed lowered by having other devices in the same area. Many 2.4 GHz 802.11b and 802.11g access-points default to the same channel on initial startup, contributing to congestion on certain channels. Wi-Fi pollution, or an excessive number of access points in the area, especially on the neighboring channel, can prevent access and interfere with other devices' use of other access points, caused by overlapping channels in the 802.11g/b spectrum, as well as with decreased signal-to-noise ratio (SNR) between access points. This can become a problem in high-density areas, such as large apartment complexes or office buildings with many Wi-Fi access points. It is advised to only use channel 1-6-11.

Additionally, other devices use the 2.4 GHz band: microwave ovens, ISM band devices, security cameras, ZigBee devices, Bluetooth devices, video senders, cordless phones, baby monitors,[39] and (in some countries) Amateur radio all of which can cause significant additional interference. It is also an issue when municipalities[40] or other large entities (such as universities) seek to provide large area coverage.

Service set identifier (SSID)

In addition to running on different channels, multiple Wi-Fi networks can share channels.

A service set is the set of all the devices associated with a particular Wi-Fi network. The service set can be local, independent, extended or mesh.

Each service set has an associated identifier, the Service Set Identifier (SSID), which consists of 32 bytes that identifies the particular network. The SSID is configured within the devices that are considered part of the network, and it is transmitted in the packets. Receivers ignore wireless packets from other networks with a different SSID.

Throughput

As the 802.11 specifications evolved to support higher throughput, the bandwidth requirements also increased to support them. 802.11n uses double the radio spectrum/bandwidth (40 MHz) compared to 802.11a or 802.11g (20 MHz). This means there can be only one 802.11n network on the 2.4 GHz band at a given location, without interference to/from other WLAN traffic. 802.11n can also be set to limit itself to 20 MHz bandwidth to prevent interference in dense community.

Many newer consumer devices support the latest 802.11ac standard, which uses the 5 GHz band exclusively and is capable of multi-station WLAN throughput of at least 1 gigabit per second. According to a study, devices with the 802.11ac specification are expected to be common by 2015 with an estimated one billion spread around the world.[41]

Hardware

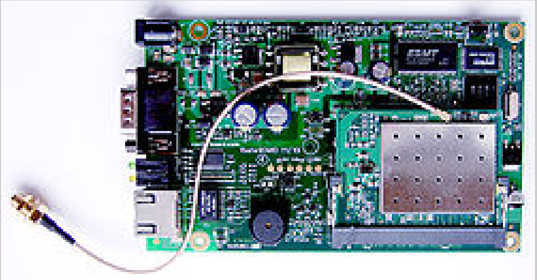
Wi-Fi allows cheaper deployment of local area networks (LANs). Also spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless LANs.

Manufacturers are building wireless network adapters into most laptops. The price of chipsets for Wi-Fi continues to drop, making it an economical networking option included in even more devices.

Different competitive brands of access points and client network-interfaces can inter-operate at a basic level of service. Products designated as "Wi-Fi Certified" by the Wi-Fi Alliance are backwards compatible. Unlike mobile phones, any standard Wi-Fi device will work anywhere in the world.

Standard devices

A wireless access point (WAP) connects a group of wireless devices to an adjacent wired LAN. An access point resembles a network hub, relaying data 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.



An embedded RouterBoard 112 with U.FL-RSMA pigtail and R52 mini PCI Wi-Fi card widely used by wireless Internet service providers (WISPs) in the Czech Republic

Wireless adapters allow devices to connect to a wireless network. These adapters connect to devices using various external or internal interconnects such as PCI, miniPCI, USB, ExpressCard, Cardbus and PC Card. As of 2010, most newer laptop computers come equipped with built in internal adapters.

Wireless routers integrate a Wireless Access Point, Ethernet switch, and internal router firmware application that provides IP routing, NAT, and DNS forwarding through an integrated WAN-interface. A wireless router allows wired and wireless Ethernet LAN devices to connect to a (usually) single WAN device such as a cable modem or a 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 usually an integrated web server that is accessible to wired and wireless LAN clients and often optionally to WAN clients. This utility may also be an application that is run on a computer, as is the case with as Apple's AirPort, which is managed with the AirPort Utility on Mac OS X and iOS.[42]

OSBRiDGE 3GN – 802.11n Access Point and UMTS/GSM Gateway in one device

Wireless network bridges connect a wired network to a wireless network. A bridge differs from an access point: 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.

Wireless range-extenders or wireless repeaters can extend the range of an existing wireless network. Strategically placed range-extenders can elongate a signal area or allow for the signal area to reach around barriers such as those pertaining in L-shaped corridors. Wireless devices connected through repeaters will suffer from an increased latency for each hop, as well as from a reduction in the maximum data throughput that is available. In addition, the effect of additional users using a network employing wireless range-extenders is to consume the available bandwidth faster than would be the case where but a single user migrates around a network employing extenders. For this reason, wireless range-extenders work best in networks supporting very low traffic throughput requirements, such as for cases where but a single user with a Wi-Fi equipped tablet migrates around the combined extended and non-extended portions of the total connected network. Additionally, a wireless device connected to any of the repeaters in the chain will have a data throughput that is also limited by the "weakest link" existing in the chain between where the connection originates and where the connection ends. Networks employing wireless extenders are also more prone to degradation from interference from neighboring access points that border portions of the extended network and that happen to occupy the same channel as the extended network.

An Atheros Wi-Fi N draft adaptor with built in Bluetooth on a Sony Vaio E series laptop

The security standard, Wi-Fi Protected Setup, allows embedded devices with limited graphical user interface to connect to the Internet with ease. Wi-Fi Protected Setup has 2 configurations: The Push Button configuration and the PIN configuration. These embedded devices are also called The Internet of Things and are low-power, battery-operated embedded systems. A number of Wi-Fi manufacturers design chips and modules for embedded Wi-Fi, such as GainSpan.[43]

Embedded systems

Increasingly in the last few years (particularly as of 2007), embedded Wi-Fi modules have become available that incorporate a real-time operating system and provide a simple means of wirelessly enabling any device which has and communicates via a serial port.[44] This allows the design of simple monitoring devices. An example is a portable ECG device monitoring a patient at home. This Wi-Fi-enabled device can communicate via the Internet.[45]

USB wireless adapter

These Wi-Fi modules are designed by OEMs so that implementers need only minimal Wi-Fi knowledge to provide Wi-Fi connectivity for their products.

In June 2014 Texas Instruments introduced the first ARM Cortex-M4 with an onboard dedicated WiFi MCU, the SimpleLink CC3200. Developers are now able to design Embedded systems to connect to the Internet of Things (IoT) using a single chip.

Range

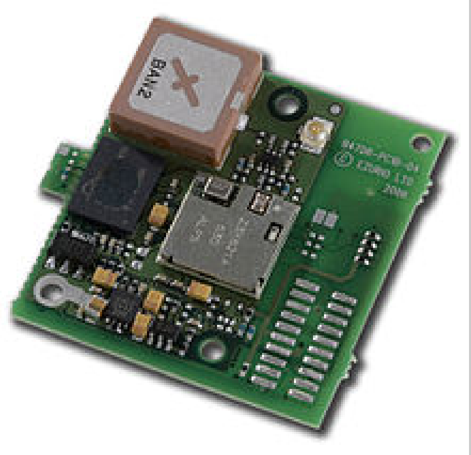
See also: Long-range Wi-Fi

The Wi-Fi signal range depends on the frequency band, radio power output, antenna gain and antenna type as well as the modulation technique. Line-of-sight is the thumbnail guide but reflection and refraction can have a significant impact.

An access point compliant with either 802.11b or 802.11g, using the stock antenna might have a range of 100 m (330 ft). The same radio with an external semi parabolic antenna (15db gain) might have a range over 20 miles.

Higher gain rating (dBi) indicates further deviation (generally toward the horizontal) from a theoretical, perfect isotropic radiator, and therefore the further the antenna can project a usable signal, as compared to a similar output power on a more isotropic antenna.[46] For example, an 8 dBi antenna used with a 100 mW driver will have a similar horizontal range to a 6 dBi antenna being driven at 500 mW. Note that this assumes that radiation in the vertical is lost; this may not be the case in some situations, especially in large buildings or within a waveguide. In the above example, a directional waveguide could cause the low power 6 dBi antenna to project much further in a single direction than the 8 dBi antenna which is not in a waveguide, even if they are both being driven at 100 mW.

IEEE 802.11n, however, can more than double the range.[47] 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 used by 802.11a (and optionally by 802.11n). On wireless routers with detachable antennas, it is possible to improve range by fitting upgraded antennas which have higher gain in particular directions. Outdoor ranges can be improved to many kilometers through the use of high gain directional antennas at the router and remote device(s). In general, the maximum amount of power that a Wi-Fi device can transmit is limited by local regulations, such as FCC Part 15 in the US. Equivalent isotropically radiated power (EIRP) in the European Union is limited to 20 dBm (100 mW).


Embedded serial-to-Wi-Fi module

To reach requirements for wireless LAN applications, Wi-Fi has fairly high power consumption compared to some other standards. Technologies such as Bluetooth (designed to support wireless personal area network (PAN) applications) provide a much shorter propagation range between 1 and 100m[48] and so in general have a lower power consumption. Other low-power technologies such as ZigBee have fairly long range, but much lower data rate. The high power consumption of Wi-Fi makes battery life in mobile devices a concern.

Researchers have developed a number of "no new wires" technologies 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-6) is not possible or cost-effective. For example, the ITU-T G.hn standard for high speed local area networks uses existing home wiring (coaxial cables, phone lines and power lines). Although G.hn does not provide some of the advantages of Wi-Fi (such as mobility or outdoor use), it is designed for applications (such as IPTV distribution) where indoor range is more important than mobility.

Due to the complex nature of radio propagation at typical Wi-Fi frequencies, particularly the effects of signal reflection off trees and buildings, algorithms can only approximately predict Wi-Fi signal strength for any given area in relation to a transmitter.[49] This effect does not apply equally to long-range Wi-Fi, since longer links typically operate from towers that transmit above the surrounding foliage.

The practical range of Wi-Fi essentially confines mobile use to such applications as inventory-taking machines in warehouses or in retail spaces, barcode-reading devices at check-out stands, or receiving/shipping stations. Mobile use of Wi-Fi over wider ranges is limited, for instance, to uses such as in an automobile moving from one hotspot to another. Other wireless technologies are more suitable for communicating with moving vehicles.

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 the mountain-tops of El Águila and Platillon.[50][51] The Swedish Space Agency transferred data 420 km (260 mi), using 6 watt amplifiers to reach an overhead stratospheric balloon.[52]

Multiple access points

Increasing the number of Wi-Fi access points provides network redundancy, better range, support for fast roaming and increased overall network-capacity by using more channels or by defining smaller cells. Except for the smallest implementations (such as home or small office networks), Wi-Fi implementations have moved toward "thin" access points, with more of the network intelligence housed in a centralized network appliance, relegating individual access points to the role of "dumb" transceivers. Outdoor applications may use mesh topologies.

When multiple access points are deployed they are often configured with the same SSID and security settings to form an 'extended service set.' Wi-Fi client devices will typically connect to the access point that can provide the strongest signal within that service set.

Network security

Main article: Wireless security

The main issue with wireless network security is its simplified access to the network compared to traditional wired networks such as Ethernet. With wired networking, one must either gain access to a building (physically connecting into the internal network), or break through an external firewall. To enable Wi-Fi, one merely needs to be within the range of the Wi-Fi network. Most business networks protect sensitive data and systems by attempting to disallow external access. Enabling wireless connectivity reduces security if the network uses inadequate or no encryption.[53][54][55]

An attacker who has gained access to a Wi-Fi network router can initiate a DNS spoofing attack against any other user of the network by forging a response before the queried DNS server has a chance to reply.[56]

Data security risks

The most common wireless encryption-standard, Wired Equivalent Privacy (WEP), has been shown to be easily breakable even when correctly configured. Wi-Fi Protected Access (WPA and WPA2) encryption, which became available in devices in 2003, aimed to solve this problem. Wi-Fi access points 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 does not enable any wireless security, providing open wireless access to a LAN. To turn security on requires the user to configure the device, usually via a software graphical user interface (GUI). On unencrypted Wi-Fi networks connecting devices can monitor and record data (including personal information). Such networks can only be secured by using other means of protection, such as a VPN or secure Hypertext Transfer Protocol over Transport Layer Security (HTTPS).

Wi-Fi Protected Access encryption (WPA2) is considered secure, provided a strong passphrase is used. A proposed modification to WPA2 is WPA-OTP or WPA3, which stores an on-chip optically generated onetime pad on all connected devices which is periodically updated via strong encryption then hashed with the data to be sent or received. This would be unbreakable using any (even quantum) computer system as the hashed data is essentially random and no pattern can be detected if it is implemented properly. Main disadvantage is that it would need multi-GB storage chips so would be expensive for the consumers.

Securing methods

A common measure to deter unauthorized users involves hiding the access point's name by disabling the SSID broadcast. While effective against the casual user, it is ineffective as a security method because the SSID is broadcast in the clear in response to a client SSID query. Another method is to only allow computers with known MAC addresses to join the network,[57] but determined eavesdroppers may be able to join the network by spoofing an authorized address.

Wired Equivalent Privacy (WEP) encryption was designed to protect against casual snooping but it is no longer considered secure. Tools such as AirSnort or Aircrack-ng can quickly recover WEP encryption keys.[58] Because of WEP's weakness the Wi-Fi Alliance approved Wi-Fi Protected Access (WPA) which uses TKIP. WPA was specifically designed to work with older equipment usually through a firmware upgrade. Though more secure than WEP, WPA has known vulnerabilities.

The more secure WPA2 using Advanced Encryption Standard was introduced in 2004 and is supported by most new Wi-Fi devices. WPA2 is fully compatible with WPA.[59]

A flaw in a feature added to Wi-Fi in 2007, called Wi-Fi Protected Setup, allows WPA and WPA2 security to be bypassed and effectively broken in many situations. The only remedy as of late 2011 is to turn off Wi-Fi Protected Setup,[60] which is not always possible.

Virtual Private Networks are often used to secure Wi-Fi.

Piggybacking

Main article: Piggybacking (Internet access)
Further information: Legality of piggybacking

Piggybacking refers to access to a wireless Internet connection by bringing one's own computer within the range of another's wireless connection, and using that service without the subscriber's explicit permission or knowledge.

During the early popular adoption of 802.11, providing open access points for anyone within range to use was encouraged to cultivate wireless community networks,[61] 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. 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 breach the Terms of Service or contract with the ISP. These activities do not result in sanctions in most jurisdictions; however, legislation and case law differ considerably across the world. A proposal to leave graffiti describing available services was called warchalking.[62] A Florida court case determined that owner laziness was not to be a valid excuse.

Piggybacking often occurs unintentionally - a technically unfamiliar user might not change the default "unsecured" settings to their access point and operating systems can be configured to connect automatically 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 has a stronger signal. 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 middle-man when seeking a destination (see Man-in-the-middle attack). For example, a user could inadvertently use an unsecure network to log into a website, thereby making the login credentials available to anyone listening, if the website uses an unsecure protocol such as HTTP.

Safety

Further information: Wireless electronic devices and health

The World Health Organization (WHO) says "there is no risk from low level, long-term exposure to Wi-Fi networks" and the United Kingdom's Health Protection Agency reports that exposure to Wi-Fi for a year results in the "same amount of radiation from a 20-minute mobile phone call".[63][64] A review of studies involving 725 people who claimed electromagnetic hypersensitivity, "...suggests that 'electromagnetic hypersensitivity' is unrelated to the presence of EMF, although more research into this phenomenon is required."[65]

See also

- Indoor positioning system
- Li-Fi
- List of WLAN channels
- San Francisco Digital Inclusion Strategy
- Super Wi-Fi - IEEE 802.22 proposal to use television bands
- Wi-Fi Alliance
- Wi-Fi operating system support
- Wireless Broadband Alliance
- Wireless network interface controller (WNIC)

References

1. What is Wi-Fi? – A Word Definition From the Webopedia Computer Dictionary (http://www.webopedia.com/TERM/W/Wi_Fi.html)
2. "Brute forcing Wi-Fi Protected Setup" (http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf) (PDF). Retrieved 2013-06-15.
3. "Authorization of Spread Spectrum Systems Under Parts 15 and 90 of the FCC Rules and Regulations" (http://www.marcus-spectrum.com/documents/81413RO.txt) (TXT). Federal Communications Commission. June 18, 1985. Retrieved 2007-08-31.
4. Phil Mercer (August 11, 2012). "Wi-fi, dual-flush loos and eight more Australian inventions" (http://www.bbc.co.uk/news/magazine-20071644). BBC News.
5. EP 0599632 (http://worldwide.espacenet.com/textdoc?DB=EPODOC&IDX=EP0599632)
6. Sygall, David (December 7, 2009). "How Australia's top scientist earned millions from Wi-Fi" (http://www.smh.com.au/technology/sci-tech/how-australias-top-scientist-earned-millions-from-wifi-20091207-kep4.html). *The Sydney Morning Herald*.
7. "Wi-Fi Alliance: Organization" (http://www.wi-fi.org/organization.php). *Official industry association Web site*. Retrieved August 23, 2011.
8. IEEE-SA – IEEE 802.11 and Amendments Patent Letters of Assurance (http://standards.ieee.org/about/sasb/patcom/pat802_11.html)
9. Moses, Asher (June 1, 2010). "CSIRO to reap 'lazy billion' from world's biggest tech companies" (http://www.theage.com.au/technology/enterprise/csiro-to-reap-lazy-billion-from-worlds-biggest-tech-companies-20100601-wsu2.html). *The Age* (Melbourne). Retrieved 8 June 2010.
10. World changing Aussie inventions – Australian Geographic (http://www.australiangeographic.com.au/journal/world-changing-aussie-inventions.htm)
11. How the Aussie government "invented WiFi" and sued its way to Rs59,773.73 million | Ars Technica (http://arstechnica.com/tech-policy/news/2012/04/how-the-aussie-government-invented-wifi-and-sued-its-way-to-430-million.ars)
12. "Australia's Biggest Patent Troll Goes After AT&T, Verizon and T-Mobile" (http://www.cbsnews.com/8301-505124_162-43340647/australias-biggest-patent-troll-goes-after-at038t-verizon-and-t-mobile/). *CBS News*.
13. Australian scientists cash in on Wi-Fi invention: SMH 1 April 2012 (http://www.smh.com.au/it-pro/government-it/australian-scientists-cash-in-on-wifi-invention-20120331-1w5gx.html)
14. CSIRO wins legal battle over Wi-Fi patent: ABC 1 April 2012 (http://www.abc.net.au/news/2012-04-01/csiro-receives-multi-million-dollar-payment-for-wifi-technology/3925814)
15. "Statement of Use, s/n 75799629, US Patent and Trademark Office Trademark Status and Document Retrieval" (http://tsdr.uspto.gov/documentviewer?caseId=sn75799629&docId=IPC20070420145537#docIndex=19&page=3). August 23, 2005. Retrieved 2014-09-21. "first used the Certification Mark ... as early as August 1999"
16. "WiFi isn't short for "Wireless Fidelity" " (http://boingboing.net/2005/11/08/wifi-isnt-short-for.html). boingboing.net. 2005-11-08. Retrieved 2012-12-21.
17. "Wireless Fidelity' Debunked" (http://www.wi-fiplanet.com/columns/article.php/3674591). Wi-Fi Planet. 2007-04-27. Retrieved 2007-08-31.

18. "What is the True Meaning of Wi-Fi?" (http://www.teleclick.ca/2005/12/what-is-the-true-meaning-of-wi-fi/). Teleclick. Retrieved 2007-08-31.
19. "Securing Wi-Fi Wireless Networks with Today's Technologies" (http://www.netsense.info/downloads/Whitepaper_Wi-Fi_Networks2-6-03.pdf) (PDF). Wi-Fi Alliance. February 6, 2003. Retrieved June 25, 2015.
20. "WPA Deployment Guidelines for Public Access Wi-Fi Networks" (http://www.wi-fi.org/files/wp_6_WPA%20Deployment%20for%20Public%20Access_10-28-04.pdf) (PDF). Wi-Fi Alliance. 2004-10-28. Retrieved 2009-11-30.
21. The Wi-Fi Alliance also developed technology that expanded the applicability of Wi-Fi, including a simple set up protocol (Wi-Fi Protected Set Up) and a peer to peer connectivity technology (Wi-Fi Peer to Peer) "Wi-Fi Alliance: Organization" (http://www.wi-fi.org/organization.php). www.wi-fi.org. Retrieved 2009-10-22.
22. "Wi-Fi Alliance: White Papers" (http://www.wi-fi.org/wp/wifi-alliance-certification/). www.wi-fi.org. Retrieved 2009-10-22.
23. "Wi-Fi Alliance: Programs" (http://www.wi-fi.org/certification_programs.php). www.wi-fi.org. Retrieved 2009-10-22.
24. Marziah Karch (1 September 2010). *Android for Work: Productivity for Professionals* (http://books.google.com/books?id=6tLAyQLSzG0C). Apress. ISBN 978-1-4302-3000-7. Retrieved 11 November 2012.
25. The Telegraph – Say hello to India's first wirefree city (http://www.telegraphindia.com/1060820/asp/opinion/story_6632793.asp)
26. "Sunnyvale Uses MetroFi" (https://web.archive.org/20150722113251/http://www.besttech.com.tr/urun/bq100-gsm-role-kontrol/). besttech.com.tr. Archived from the original (http://www.besttech.com.tr/urun/bq100-gsm-role-kontrol/) on July 22, 2015. Retrieved 2008-07-16.
27. Alexander, Steve; Brandt, Steve (December 5, 2010). "Minneapolis moves ahead with wireless" (http://www.startribune.com/business/111286134.html). The Star Tribune. Retrieved December 5, 2010.
28. "London-wide wi-fi by 2012 pledge" (http://news.bbc.co.uk/2/hi/uk_news/england/london/8692103.stm). *BBC News*. 2010-05-19. Retrieved 2010-05-19.
29. "City of London Fires Up Europe's Most Advanced Wi-Fi Network" (http://www.govtech.com/dc/118717). www.govtech.com. Retrieved 2007-05-14.
30. Wearden, Graeme (2005-04-18). "London gets a mile of free Wi-Fi" (http://www.zdnet.com/article/london-gets-a-mile-of-free-wi-fi/). ZDNet. Retrieved 2015-01-06.
31. "Seoul Moves to Provide Free City-Wide WiFi Service" (http://blogs.voanews.com/breaking-news/2011/06/15/seoul-moves-to-provide-free-city-wide-wifi-service/). VOANEWS.COM. Retrieved 1 April 2012.
32. Deb Smit (October 5, 2011). "How Wi-Fi got its start on the campus of CMU, a true story" (http://popcitymedia.com/innovationnews/wifi100511.aspx). Pop City Media. Retrieved October 6, 2011.
33. "Wireless Andrew: Creating the World's First Wireless Campus" (http://www.cmu.edu/corporate/news/2007/features/wireless_andrew.shtml). Carnegie Mellon University. 2007. Retrieved October 6, 2011.
34. Wolter Lemstra; Vic Hayes; John Groenewegen (2010). *The innovation journey of Wi-Fi: the road to global success* (http://books.google.com/books?id=-OMoL5Irm08C&pg=PA121). Cambridge University Press. p. 121. ISBN 978-0-521-19971-1. Retrieved October 6, 2011.
35. "Wireless Home Networking with Virtual WiFi Hotspot" (http://techsansar.com/internetworking/wireless-home-networking-virtual-wifi-hotspot-2946/). Techsansar.com. 2011-01-24. Retrieved 2011-10-14.
36. "Wi-Fi Direct allows device-to-device links" (http://www.networkworld.com/news/2009/101409-wi-fi-direct.html?hpg1=bn).
37. "Wi-Fi gets personal: Groundbreaking Wi-Fi Direct launches today" (http://www.wi-fi.org/news-events/newsroom/wi-fi-gets-personal-groundbreaking-wi-fi-direct-launches-today). Wi-Fi Alliance. October 25, 2010. Retrieved June 25, 2015.
38. "What is Wi-Fi Certified TDLS?" (http://www.wi-fi.org/knowledge-center/faq/what-is-wi-fi-certified-tdls).
39. Delia C. "WiFi baby monitor security" (https://www.monitorshq.com/6-easy-steps-to-protect-your-baby-monitor-from-hackers/). MonitorsHQ.com. Retrieved 2014-09-12.
40. Wilson, Tracy V. "How Municipal WiFi Works" (http://computer.howstuffworks.com/municipal-wifi.htm). computer.howstuffworks.com. Retrieved 2008-03-12.
41. Murph, Darren. "Study: 802.11ac devices to hit the one billion mark in 2015, get certified in 2048" (http://www.engadget.com/2011/02/08/study-802-11ac-devices-to-hit-the-one-billion-mark-in-2015-get/). *Engadget*. Retrieved 25 August 2014.

42. "Apple.com Airport Utility Product Page" (http://www.apple.com/airportextreme/features/utility.html). Apple, Inc. Retrieved 2011-06-14.
43. GainSpan specifically designs for Wi-Fi technology between Wi-Fi devices. Extremely useful. "GainSpan low-power, embedded Wi-Fi" (http://www.gainspan.com/technology/technology_overview.php). www.gainspan.com. Retrieved 2010.
44. "Quatech Rolls Out Airborne Embedded 802.11 Radio for M2M Market" (http://edageek.com/2008/04/18/embedded-wifi-radio/). Retrieved 2008-04-29.
45. "CIE article on embedded Wi-Fi for M2M applications" (http://wifiscan.fr/research/article_19742.htm). Retrieved 2014-11-28.
46. http://www.dslreports.com/forum/r15405199-Somebody-explain-dBi
47. "802.11n Delivers Better Range" (http://www.wi-fiplanet.com/tutorials/article.php/3680781). *Wi-Fi Planet*. 2007-05-31.
48. [1] (http://janmagnet.files.wordpress.com/2008/07/comparison-ieee-802-standards.pdf) section 1.2 (scope)
49. "WiFi Mapping Software: Footprint" (http://www.alyrica.net/node/20). Alyrica Networks, Inc. Retrieved 2008-04-27.
50. "Ermanno Pietrosemoli has set a new record for the longest communication Wi-Fi link" (http://interred.wordpress.com/2007/06/18/ermanno-pietrosemoli-has-set-a-new-record-for-the-longest-communication-wi-fi-link/). Retrieved 2008-03-10.
51. "Wireless technology is irreplaceable for providing access in remote and scarcely populated regions" (http://www.apc.org/en/news/strategic/world/wireless-technology-irreplaceable-providing-access). Retrieved 2008-03-10.
52. "Long Distance WiFi Trial" (http://www.eslared.org.ve/articulos/Long%20Distance%20WiFi%20Trial.pdf) (PDF). Retrieved 2008-03-10.
53. "802.11 X Wireless Network in a Business Environment – Pros and Cons." (http://networkbits.net/wireless-printing/80211-g-pros-cons-of-a-wireless-network-in-a-business-environment/). NetworkBits.net. Retrieved 2008-04-08.
54. "Free Wi-Fi? User beware: Open connections to Internet are full of security dangers, hackers, ID thieves" (http://www.app.com/article/20130701/NJNEWS/307010010/Free-Wi-Fi-User-beware-Open-connections-Internet-full-security-dangers). Larry Higgs – *Asbury Park Press*.
55. Gittleson, Kim (28 March 2014) Data-stealing Snoopy drone unveiled at Black Hat (http://www.bbc.co.uk/news/technology-26762198) BBC News, Technology, Retrieved 29 March 2014
56. Bernstein, Daniel J. (2002). "DNS forgery" (http://cr.yp.to/djbdns/forgery.html). Retrieved 2010-03-24. "An attacker with access to your network can easily forge responses to your computer's DNS requests."
57. Mateti, Prabhaker (2005). "Hacking Techniques in Wireless Networks" (http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm#_Toc77524658). Dayton, Ohio: Department of Computer Science and Engineering Wright State University. Retrieved 2010-02-28.
58. "Wireless Vulnerabilities & Exploits" (http://www.wirelessve.org/entries/show/WVE-2005-0020). wirelessve.org. Retrieved 2008-04-15.
59. "WPA2 Security Now Mandatory for Wi-Fi CERTIFIED Products" "WPA2 Security Now Mandatory for Wi-Fi CERTIFIED Products" (http://www.wi-fi.org/pressroom_overview.php?newsid=16). *Wi-Fi Alliance*.
60. http://www.kb.cert.org/vuls/id/723755 US CERT Vulnerability Note VU#723755
61. "NoCat's goal is to bring you Infinite Bandwidth Everywhere for Free" (http://nocat.net/). Nocat.net. Retrieved 2011-10-14.
62. "Let's Warchalk" (http://www.blackbeltjones.com/warchalking/warchalking0_9.pdf) (PDF). Matt Jones. Retrieved 2008-10-09.
63. "Q&A: Wi-fi health concerns" (http://news.bbc.co.uk/2/hi/technology/6677051.stm). BBC News. 2007-05-21. Retrieved 2011-10-14.
64. "Electromagnetic Hypersensitivity (EMS)" (http://www.who.int/mediacentre/factsheets/fs296/en/), 2011
65. " "Electromagnetic Hypersensitivity: A Systematic Review of Provocation Studies ", 2005" (https://www.ncbi.nlm.nih.gov/pubmed/15784787). Psychosomaticmedicine.org. 2005-03-01. Retrieved 2014-05-30.

Further reading

- The WNDW Authors (1 Mar 2013). Butler, Jane, ed. *Wireless Networking in the Developing World (Third Edition)* (PDF). ISBN 978-1484039359.

External links

- Interactive History of Wi-Fi (http://getvoip.com/history-of-wifi/)
- Major global Wi-Fi conference series (http://www.wifiinnovationsummit.com/)

Look up ***Wi-Fi*** in Wiktionary, the free dictionary.

Wikimedia Commons has media related to ***Wi-Fi***.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Wi-Fi&oldid=681605336"

Categories: Wi-Fi | 1999 introductions | IEEE 802.11 | Networking standards | Wireless networking

- This page was last modified on 18 September 2015, at 07:54.