**Table of Contents**

|  |  |  |
| --- | --- | --- |
| S. No. | Topic | Page No. |
| 1 | Abstract | 6 |
| 2 | Introduction | 6 |
| 3 | History and the Wi-Fi Alliance | 7 |
| 4  4.1  4.2  4.3  4.4  4.5  4.6 | The Working of Wi-Fi  Distance Records  Embedded Systems  Multiple Access points  Piggybacking  Connecting to Wi-Fi  Internet Access | 8  12  13  13  13  14  15 |
| 5 | Wireless Technology Standards | 16 |
| 6  6.1  6.2  6.3 | Properties  Interoperability  Speed and Range  Interference | 17  17  17  18 |
| 7  7.1  7.2  7.3 | Networks  Simple Home Network  City-wide Wi-Fi  Campus-wide Wi-Fi | 18  18  19  19 |
| 8  8.1  8.2  8.3  8.4  8.5  8.6  8.7  8.8  8.9 | Issues of Data Security  Wide Spread use of WEP  Wireless Encryption Protocol(WEP) Explained  WEP’s Major Weakness  The Difference between WEP & WAP  Network Encryption using WPA Personal/PSK  Wi-Fi Protected Access (WPA) Address WEP’s shortcomings.  Securing a Network  Passphrase quality & Lifespan  Safety tips for on the road Wi-Fi | 20  21  22  22  23  23  23  24  25  25 |
| 9  9.1  9.2  9.3  9.4 | Special Features  Wi-Fi CERTIFIED ac  Wi-Fi CERTIFIED Miracast  Wi-Fi CERTIFIED Passpoint  Wi-Fi Direct | 26  26  27  27  28 |
| 10  10.1  10.2 | Advantages and Limitations  Advantages  Limitations | 28  28  29 |
| 11 | Issues of Safety & Health | 30 |
| 12 | Conclusion | 32 |
| 13 | Appendix | 33 |
| 14 | References | 35 |

**Section 1: Abstract**

Wi-Fi is a fast growing technology used to connect to the internet without any wires or burdensome cables. Wi-Fi technology uses a radio technology called 802.11b for the wireless connectivity. 802.11 buses 2.4GHz of band frequency spectrum with a bandwidth of 11Mbps (802.11a-5GHz, 54Mbps & 802.11g-2.44GHz, 54Mbps). In this paper we have discussed Wi-Fi in great detail, I have talked about how it works, its properties, its special features, how secure it is, how we can make it more secure and its advantages & limitations etc. The Wi-Fi technology finds its great utility in almostly all the devices such as mobile phones, smart phones, tablets, personal computers, digital cameras etc. Wi-Fi technology is so widely used now that 25% of all the households in the world use Wi-Fi. It lets one transfer files, send e-mails, browse videos, make projects, stay in touch with people etc.

Though there exist many other wireless technologies such as Bluetooth, Wi-Fi competes them with by providing a much higher data transfer rate and the transmission of the data over a large distance. Though Wi-Fi is an advantageous and a powerful technology, it has its disadvantages to. Interference with due to walls, windows, furniture and microwave ovens is a major problem which can’t be totally eliminated but it can be controlled sufficiently. The data transmitted through Wi-Fi is prone to hacking. Anyone can easily detect and connect to a Wi-Fi signal. It is every important to use security for Wi-Fi networks like WEP, WPA or WPA2.

**SECTION 2: Introduction**

Wi-Fi is a popular [wireless](http://www.webopedia.com/TERM/W/wireless.html) networking technology that provides networking uses radio waves to provide high-speed [Internet](http://www.webopedia.com/TERM/I/Internet.html) and [network](http://www.webopedia.com/TERM/N/network.html) connection. It allows electronic devices to exchange data wirelessly in a computer network. The [Wi-Fi Alliance](http://www.webopedia.com/TERM/W/Wi_Fi_Alliance.html) owns the Wi-Fi and defines it as any "wireless local area network ([WLAN](http://www.webopedia.com/TERM/W/WLAN.html)) products that are based on the Institute of Electrical and Electronics Engineers' ([IEEE](http://www.webopedia.com/TERM/I/IEEE.html)) 802.11 standards." The Wi-Fi products which complete Wi-Fi Alliance [interoperability](http://en.wikipedia.org/wiki/Interoperability) certification testing successfully can use the "Wi-Fi CERTIFIED" trademark. A device that is able to use Wi-Fi (such as a personal computer, video-game console, [smart phone](http://en.wikipedia.org/wiki/Smartphone), digital camera, [tablet](http://en.wikipedia.org/wiki/Tablet_computer) or digital audio player) can connect to a network resource such as the Internet through a [wireless network access point](http://en.wikipedia.org/wiki/Wireless_access_point). Wi-Fi products are capable of doing everything from sending email to web browsing and linking international video conference calls. It can even link you to the Internet from a plane 10,000 feet in the air. Such access points (or [hotspot](http://en.wikipedia.org/wiki/Hotspot_(Wi-Fi))s) have a range of about 20 meters (65 feet) indoors and a greater range outdoors.

However, Wi-Fi is less secure than wired connections (such as [Ethernet](http://en.wikipedia.org/wiki/Ethernet)) because an intruder doesn’t need a physical connection. Web pages that use [SSL](http://en.wikipedia.org/wiki/Transport_Layer_Security) are safe but unencrypted internet access could easily be detected by intruders. Now, Wi-Fi has adopted various encryption technologies. The early encryption [WEP](http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) was easy to break. Higher quality protocols ([WPA, WPA2](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access)) are now used. An optional feature was added in 2007, called [Wi-Fi Protected Setup](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup) (WPS), it had a serious flaw that allowed the attacker to recover the router's password. The Wi-Fi Alliance has since then updated its test plan and certification program to ensure that all the newly certified devices resist attacks.

# SECTION III: History & the Wi-Fi Alliance

The 802.11 technology has its origins in 1985 ruled by the US Federal Communications Commission that released the [ISM band](http://en.wikipedia.org/wiki/ISM_band) for unlicensed use. In the year 1991, [NCR Corporation & AT&T](http://en.wikipedia.org/wiki/NCR_Corporation) Corporation invented precursor to 802.11 for the use in cashier systems. The first wireless product was under the name [WaveLAN](http://en.wikipedia.org/wiki/WaveLAN). Mr. [Vic Hayes](http://en.wikipedia.org/wiki/Vic_Hayes) is called the "father of Wi-Fi", due to his involvement in negotiation of the initial standards within the [IEEE](http://en.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers) while he chaired the work group. A patent was obtained by the Australian organization CSIRO in 1992 and1996, for a method later used in Wi-Fi to "unsmear" the signal. This led to Wi-Fi being considered an Australian invention, but it is subjected to controversy. In 1999, an international consortium of engineering experts of many technology companies began to work together through an organization called IEEE (Institute of Electrical and Electronic Engineers, known as "I-triple E"), to develop industrial standards for how new wireless products should interact with one-another.  The Wi-Fi Alliance® was born out of this cooperation as a trade association which would hold the Wi-Fi trademark under which products are sold. It takes those standards and test labs to certify that all 802.11-based products meet the standards of interoperability and security, making the term [Wi-Fi](http://www.webopedia.com/TERM/W/Wi_Fi.html) as a global brand name. The group was formerly known as the Wireless Ethernet Compatibility Alliance (WECA) but later changed its name in October 2002 to reflect better the Wi-Fi brand it wanted to build. The main technology behind Wi-Fi was developed by the radio-astronomer [John O'Sullivan](http://en.wikipedia.org/wiki/John_O%27Sullivan_(engineer)) as a by-product of a research project, "a failed experiment to detect exploding mini black holes the size of an atomic particle".

### The term Wi-Fi, was first used commercially around August 2000, it was coined by a brand-consulting firm called [Interbrand](http://en.wikipedia.org/wiki/Interbrand) Corporation. The Wi-Fi Alliance hired Interbrand to select a name "a little catchier than 'IEEE 802.11b Direct Sequence'". Belanger stated that Interbrand invented Wi-Fi as a [play of words](http://en.wikipedia.org/wiki/Pun)  [Hi-Fi](http://en.wikipedia.org/wiki/High_fidelity) (high fidelity), and also made the Wi-Fi logo.

The Wi-Fi Alliance originally used the [advertising slogan](http://en.wikipedia.org/wiki/Advertising_slogan), "The Standard for Wireless Fidelity", for Wi-Fi though it was removed later. Although, some documents of the Alliance dated 2003 and 2004 still contain the term Wireless Fidelity. No official statement was made related to dropping of the term.

The [yin-yang](http://en.wikipedia.org/wiki/Yin-yang) symbol used in Wi-Fi logo indicates the certification of the product for [interoperability](http://en.wikipedia.org/wiki/Interoperability).

Non-Wi-Fi technologies which are intended for fixed points like [Motorola Canopy](http://en.wikipedia.org/wiki/Motorola_Canopy) are usually described as [fixed wireless](http://en.wikipedia.org/wiki/Fixed_wireless). Other wireless technologies include mobile phone standards like [2G](http://en.wikipedia.org/wiki/2G), [3G](http://en.wikipedia.org/wiki/3G) or [4G](http://en.wikipedia.org/wiki/4G).

**SECTION IV: The Working of Wi-Fi**

The word wireless can be defined as “no wires”. It can also be described in networking technology as the connection between the senders and receivers connected by radio waves or/and microwaves. Like a wired network, a wireless network or Wireless Local Area Network (WLAN) links a group of computers. It is generally easier, faster and cheaper to set up as wireless doesn’t require costly wiring. Also with a wired network is in place already, a wireless network can be a cost-effective way to expand or augment.

Wi-Fi works with no physical wired connection between receiver and sender by using radio frequency (RF) technology which is a frequency within the electromagnetic spectrum associated with radio wave propagation. When the RF current is supplied to the antenna, an electromagnetic field is created which is then able to propagate in space. The cornerstone of any wireless network is called an access point (AP). The primary job of an access point is to broadcast a wireless signal that computers can detect and "tune" into. Since wireless networks are usually connected to wire ones, an access point also often serves as a link to the resources available on the wired network, like an Internet connection.

In order to connect to an access point and join a wireless network the computers must be equipped with wireless network adapters. These are often inbuilt in computers but if not then any computer or notebook can be made wireless-capable through the use of an add-on adapter plugging into an empty USB port, expansion slot, or for notebooks – PC Card slot can be used.

A radio wave is an electromagnetic wave that can propagate through water, walls, air, some objects and the vacuum of outer space. The wave contains both electrical and magnetic field that are perpendicular to each other. Both the fields vary periodically in frequency and amplitude. The fields vary perpendicularly to the direction of propagation of the radio wave.

The radio wave can be generated by applying an alternating current to a dipole antenna. The frequency of alternating current can be considered to be 2.4 gigahertz (2.4 GHz).

Electromagnetic waves consist of the propagation of oscillating electric field and magnetic field components. As the radio wave propagates out from the dipole antenna source, it will decrease in amplitude as it travels farther from the source due to loss factors as it travels through a medium.

The frequency of the electromagnetic wave can be determined from the time period (T). The time period between the start and end of one cycle of the waveform is the wave period, T. The frequency of the electromagnetic wave is related to the period by the formula,

f = 1/T

f = frequency in Hertz

T = time period in seconds

From this relationship, the period for a wave with a frequency of 2.4 GHz is 0.4166 x 10-9 (billionths of a second or nanoseconds) which is very fast. From renowned physicists, Maxwell and Hertz, the wavelength and frequency of an electromagnetic wave are related to the velocity of light by the equation.

Frequency (f) x Wavelength (l) = Velocity of Light (c)

Which can be expressed as:

F x 1 = c = 3 x 108 meters per second

f = frequency in Hertz

l = wavelength in meters c = 3 x 108E meters per second (E = exponent).

Frequency is measured in cycles per second, written in Hertz and is abbreviated as Hz. A gigahertz is one billion Hertz, represented by GZ.

The frequency of 2.4 GHz, utilized in the IEEE 802.11b and 802.11g standard, has a wavelength of 4.92inches. The wavelength of IEEE 802.11a at standard frequency of 5 GHz would be about 2.36 inches. The proposed new Wi-Fi specification 802.11n operates on both 2.4 and 5 GHz frequencies. The Federal Communications Commission (FCC) regulates the frequency assignments for the use in the United States. Here the focus is on the 2.4 GHz frequency band ranging from 2.4000 to 2.4835 GHz that can be utilized without an FCC license. A public & unlicensed area of the electromagnetic spectrum that is utilized for 802.11b WLAN operation. Therefore we will be using the unlicensed 2.4 GHz band for the wireless network examples.

A typical radio system will consist of a transmitter with a transmitting antenna which will send radio waves through some media to a receiving antenna connected to a receiver. The radio system transmits information (data packets within a radio frequency modulation scheme) to the transmitter. The RF signal which contains the data packets is transmitted through an antenna which converts the signal into an electromagnetic wave. The transmission medium is free space through which the electromagnetic wave propagates. The electromagnetic wave is intercepted by the receiving antenna which converts it back to an RF signal which is the same as the transmitted RF signal. After that the received RF signal is demodulated by the receiver to yield the original information.  
A wireless access point (WAP) connects a group of wireless devices to an adjacent wire LAN.

The access point resembles a network hub, relaying data between devices connected wirelessly in addition to a single connected wired device. It allows wireless devices to communicate with other wired devices.

Wireless adapters allow devices to connect to a wireless network. These adapters connect to other devices using various internal or external interconnects such as USB, Express Card, and PCI etc. Till 2010, many new laptop computers come which are equipped with built in internal adapters.

Wireless routers integrate a Wireless Ethernet switch, internal router firmware application and Access Point which provides [NAT](http://en.wikipedia.org/wiki/Network_address_translation), [DNS](http://en.wikipedia.org/wiki/Domain_Name_System), [IP](http://en.wikipedia.org/wiki/Internet_Protocol) routing forwarding through an integrated [WAN](http://en.wikipedia.org/wiki/Wide_area_network)-interface. Wireless router enables wired & wireless Ethernet LAN devices to connect to a single WAN device such as a [DSL modem](http://en.wikipedia.org/wiki/DSL_modem) or a [cable modem](http://en.wikipedia.org/wiki/Cable_modem). A wireless router allows all three devices mainly the access point and router to be configured through one central utility. This is integrated web server utility that is accessible to wired and wireless LAN clients and often optionally to WAN clients. This utility can also be an application that runs on the computer, as in the case of Apple's [AirPort](http://en.wikipedia.org/wiki/AirPort), which is controlled with the [AirPort Utility](http://en.wikipedia.org/wiki/AirPort_Utility) on [Mac OS X](http://en.wikipedia.org/wiki/Mac_OS_X) & iOS.

Wireless [network bridges](http://en.wikipedia.org/wiki/Bridging_(networking)) connect a wired network to a wireless network. A bridge is different from an access point. The 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 are used to connect two wired networks over a wireless link. It is useful in situations where a wired connection may be unavailable like between two separate homes.

Wireless range-extenders or wireless repeaters can extend the range of an existing wireless network. Strategically placed range-extenders will elongate a signal area. It allow for the signal area to reach around barriers such as those pertaining in L-shaped corridors. Wireless devices connected by repeaters; suffer from an increased latency for each hop as well as from a reduction in the maximum data throughput that becomes available. Additionally, when many users use a network employing wireless range-extenders the consumption of the available bandwidth becomes faster than the single user migrating around a network employing extenders. For this, wireless range-extenders work best in networks supporting very low traffic throughput requirements. Especially for cases where the single user with a Wi-Fi equipped tablet migrates around the combined extended and non-extended portions of the total connected network. Furthermore, a wireless device connected to any of the repeaters in the chain will have a data throughput. It is limited by the "weakest link" existing in the chain between the starting and ending of connection. Networks employing wireless extenders are also more prone to degradation from interference from neighboring access points. The access point border the portions of the extended network which happen to occupy the same channel as the extended network.

The security standard and Wi-Fi Protected Setup allows embedded devices with limited graphical user interface to connect to the Internet easily. Wi-Fi Protected Setup has two configurations: The Push Button configuration and the PIN configuration. These embedded devices are also known as The Internet of Things. They are low-power, battery-operated embedded systems. A lot of Wi-Fi manufacturers design chips and modules for embedded Wi-Fi, such as Gain Span.

**Distance records**

Distance records (using non-standard devices) included 382 km in June 2007 was held by EsLaRed and Ermanno Pietrosemoli of Venezuela which transfers about 3 MB of data between the mountain-tops of  Platillon and [El Águila](http://en.wikipedia.org/wiki/Pico_El_%C3%81guila). The [Swedish Space Agency](http://en.wikipedia.org/wiki/Swedish_National_Space_Board) transferred data of about 420 km, using 6 watt amplifiers to reach an overhead stratospheric ballon.

**Embedded systems**

|  |  |  |
| --- | --- | --- |
| Increasingly in the few last years, embedded Wi-Fi module has become available that incorporate a real-time operating system and also provide a simple means of wirelessly enabling any device which has and can communicates via the serial port. This permits the design of simple monitoring devices. An instance can be of a portable ECG device monitoring a patient at home. These Wi-Fi-enabled devices can interact via the Internet.  These Wi-Fi modules have been designed by OEMs so that implementers need only minimal Wi-Fi knowledge to provide Wi-Fi connectivity for their products.  **Multiple access points**  Increasing the number of Wi-Fi access points provides network redundancy, support pro fast [roaming](http://en.wikipedia.org/wiki/Roaming) & improved overall network-capacity. This can be done by using more channels or by defining smaller cells. Apart from the smallest implementations (such as home or small office networks), Wi-Fi implementations have moved towards "thin" access points with more of the network intelligence housed in a centralized network appliance, relegating each access points to the role of "dumb" transceivers. Outdoor applications are used in [mesh](http://en.wikipedia.org/wiki/Mesh_networking) topologies.  **Piggybacking**  Piggybacking refers to access to a wireless Internet connection by bringing one's own computer within the range of another's wireless connection. This involves using that service without the subscriber's explicit knowledge or permission.  During the early popular adoption of [802.11](http://en.wikipedia.org/wiki/IEEE_802.11), providing open access points for everyone within the range to use was encouraged to cultivate [wireless community networks](http://en.wikipedia.org/wiki/Wireless_community_network). Particularly for the people since on average they use only a fraction of their downstream bandwidth at any given time.  Recreational logging and mapping of other people's access points is called [wardriving](http://en.wikipedia.org/wiki/Wardriving). Many access points are indeed installed intentionally without security turned on so that they can be used as a free service. Giving access to one's Internet connection may breach the terms of service or contract with the [ISP](http://en.wikipedia.org/wiki/Internet_service_provider). These activities don’t effect in sanction in most jurisdictions. Nevertheless, [case law](http://en.wikipedia.org/wiki/Case_law) and legislation differ considerably around the world. A suggestion to leave [graffiti](http://en.wikipedia.org/wiki/Graffiti) describing available services was called [warchalking](http://en.wikipedia.org/wiki/Warchalking). A [Florida](http://en.wikipedia.org/wiki/Florida) court case found that owner’s laziness was not a valid excuse. Piggybacking Piggybacking often occurs by accident, as most access points are configured without encryption by default. The operating systems can be configured to connect automatically to any available wireless network. The user who happens to start up a laptop in the vicinity of an access point may find that the computer has joined the network without any visible indication. Moreover, the user intending to join one network may instead end up on another one if the latter has a stronger signal. In amalgamation with automatic discovery of other network resources this could possibly lead to wireless users to send sensitive data to the wrong middle-man when they seek a destination. 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.  Connecting to Wi-Fi To connect to a Wi-Fi LAN, the computer has to be equipped with a [wireless network interface controller](http://en.wikipedia.org/wiki/Wireless_network_interface_controller). The combination of interface controller and computer is called the station. All stations share the same single radio frequency communication channel. Transmissions on the channel are received by all stations within the range. The hardware does not signal the user of when the transmission was delivered and is hence called a [best-effort delivery](http://en.wikipedia.org/wiki/Best-effort_delivery) mechanism. A carrier wave transmits the data in packets which are referred as "[Ethernet frames](http://en.wikipedia.org/wiki/Ethernet_frame)". Each station is constantly tuned on the radio frequency communication channel to pick up available transmissions.  Internet access A Wi-Fi-enabled device can connect to the Internet within the range of a [wireless network](http://en.wikipedia.org/wiki/Wireless_network) which is configured to permit it. The coverage of one or more interconnected [access points](http://en.wikipedia.org/wiki/Wireless_access_point)  is called hotspots which can extend from an area as small as a few rooms to as large as many square miles. Coverage in the larger area which may require a group of access points with overlapping coverage. Outdoor public Wi-Fi technology is used successfully in [wireless mesh networks](http://en.wikipedia.org/wiki/Wireless_mesh_network) in London, UK.  Wi-Fi provides service in high street chains, independent businesses and private homes, as well as in public spaces. The Wi-Fi hotspots set up are either free-of-charge or commercialized. Organizations and [businesses](http://en.wikipedia.org/wiki/Business), such as hotels, restaurants, and airports, often provide free use of hotspots to pull customers. Enthusiasts and authorities that wish to provide services or even to promote business in selected areas sometimes provide free Wi-Fi access.  [Routers](http://en.wikipedia.org/wiki/Router_(computing)) 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 buildings providing Internet access and [internetworking](http://en.wikipedia.org/wiki/Internetworking) to all devices connected to them either wirelessly or via cable.  There are battery-powered routers that include a cellular mobile Internet radio modem and Wi-Fi access point. They allow nearby Wi-Fi stations to access the Internet over 2G, 3G, or 4G networks when subscribed to a cellular phone carrier. Many smart phones have a built-in capability, including those based on [Bada](http://en.wikipedia.org/wiki/Bada_(operating_system)),  [Android](http://en.wikipedia.org/wiki/Android_(operating_system)), [Windows Phone](http://en.wikipedia.org/wiki/Windows_Phone), Symbian and [iOS](http://en.wikipedia.org/wiki/IOS) [iPhone](http://en.wikipedia.org/wiki/IPhone). Though carriers more often than not disable the feature or charge a separate fee to enable it especially for customers with unlimited data plans. "Internet packs" offer standalone facilities of this type as well without the use of a smartphones. Examples include the [MiFi](http://en.wikipedia.org/wiki/MiFi)- and [WiBro](http://en.wikipedia.org/wiki/WiBro)-branded devices. A number of laptops also 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. SECTION V: Wireless Technology StandardsThe most common [wireless technology standards](http://www.webopedia.com/TERM/8/802_11.html) are the following:  * 802.11b: The first widely used wireless networking technology, known as 802.11b (more commonly called Wi-Fi), made its first debut almost a decade ago, but is used still. * 802.11g: In 2003, a follow-on version called 802.11g appeared which offered superior performance (that is, speed and range) and remains today's most common wireless networking technology. * 802.11n: Another improved standard called 802.11n was developed in 2009. It uses multiple antennas to increase data rates from 54 Mbit/s to 600 Mbit/s.   https://upload.wikimedia.org/wikipedia/commons/6/62/Protocol_Stack_of_802.11.JPGFor more please see appendix  SECTION VI: Properties  Interoperability  Products from any of the more than 500 Wi-Fi Alliance member companies that are certified will work together, so users can mix-and-match Wi-Fi CERTIFIED products with the confidence that they will work together.  Speed and Range  When one buys a piece of wireless network hardware, it will often quote wildly optimistic performance figures (i.e., how fast it can transmit data). As a general rule, one should assume that in the best-case scenario, they will get roughly one-third of the advertised performance. Speed varies based on wireless networking standards. Also, the more computers you have connected to a wireless access point the less data each will be able to send and receive. Just like the speed of a wireless network which varies greatly, so can the range  A typical wireless access point which uses [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 may have a range of 35 m (120 ft) indoors and 100 m (300 ft) outdoors. [IEEE 802.11n](http://en.wikipedia.org/wiki/IEEE_802.11#802.11n), on the other hand, can have more than double the range.  Range also tends to vary with the frequency band. Wi-Fi in the 2.4 GHz frequency band has slightly better range than Wi-Fi in the 5 GHz frequency band. In wireless routers with detachable antennas, the range can be improved by fitting upgraded antennas which have higher gain in particular directions. As you might expect, the closer one is to an access point, the stronger the signal & the faster the connection speed. The range and speed one gets out of wireless network will also depend on the kind of environment in which it is operating. This brings up the subject of interference.   |  | | --- | |  |  InterferenceAnything which alters, modifies, or disrupts a [signal](http://en.wikipedia.org/wiki/Signal_(electrical_engineering)) as it is traveling along a channel between a [source](http://en.wikipedia.org/wiki/Communication_source) and a receiver. Electromagnetic interference is disturbance that affects an electrical circuit due to either electromagnetic induction or [electromagnetic radiation](http://en.wikipedia.org/wiki/Electromagnetic_radiation) emitted from an external source. 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 a excessive no. of access points in a area, especially in the neighboring channel, can thwart access and interfere with other devices' use of other access points, caused due to overlapping channels in 802.11g/b spectrum, also with decreased [signal-to-noise ratio](http://en.wikipedia.org/wiki/Signal-to-noise_ratio) (SNR) between access points. This is become a problem in high-density areas, such as office building or large apartment complexes with many Wi-Fi access points. The potential for interference is especially large indoors, where diverse types of building materials (concrete, wood, drywall, metal, glass and so on) can reflect or absorb radio waves, which affect the strength and consistency of a wireless network's signal. Additionally, other devices use the 2.4 GHz band: - [ISM band](http://en.wikipedia.org/wiki/ISM_band) devices, microwave ovens, security cameras, Bluetooth devices, [video senders](http://en.wikipedia.org/wiki/Video_sender), cordless phones, and (in some countries) [Amateur radio](http://en.wikipedia.org/wiki/Amateur_radio) all of which can cause significant additional interference. It is also an issue when municipalitiesor other large entities (such as universities) seek to provide large area coverage. One can't avoid interference entirely, but mostly it is not significant enough to affect the usability of the network. If it does, one can usually minimize the interference by relocating wireless networking hardware or using specialized [antennas](http://www.webopedia.com/TERM/a/antenna.html).  SECTION VII: Networks  Simple Home Network The most familiar type of Wi-Fi network for personal use is called an infrastructure network - where each device connects to a central point which manages the communications, such as the use of a home broadband internet connection.  The broadband modem connects the network to the Internet through a service provider (e.g. cable or DSL). The Wi-Fi gateway (may be a router or access point depending upon the network), connects the devices on one’s network to each other and allows them to share the Internet connection created by the broadband modem.  The broadband modem & gateway may sometimes be a single device that performs multiple functions. City-wide Wi-Fi In the early 2000s, many cities around the world announced plans to construct city-wide Wi-Fi networks. There are a lot of successful examples: [Mysore](http://en.wikipedia.org/wiki/Mysore) became India's first Wi-Fi-enabled city in 2004 and second in the world following [Jerusalem](http://en.wikipedia.org/wiki/Jerusalem). A company called WiFiyNet has set up hotspots in Mysore, enveloping the complete city and some nearby villages.  In 2005, [Sunnyvale, California](http://en.wikipedia.org/wiki/Sunnyvale,_California), became the first city in the United States to offer city-wide free Wi-Fi, and [Minneapolis](http://en.wikipedia.org/wiki/Minneapolis) has generated $1.2 million in profit annually for [its provider](http://en.wikipedia.org/wiki/Minneapolis_wireless_internet_network).  In May 2010, [London](http://en.wikipedia.org/wiki/London), UK, Mayor [Boris Johnson](http://en.wikipedia.org/wiki/Boris_Johnson) pledged to have London-wide Wi-Fi by 2012. Several regions including Westminster and Islington already have extensive outdoor Wi-Fi coverage.  Officials in South Korea's capital are moving to provide free Internet access at more than ten thousand locations around the city, including major streets, densely populated residential areas and outdoor public spaces. Seoul will grant leases to KT, LG Telecom & SK Telecom. The companies will invest $44 million in the projects, which will complete in 2015. Campus-wide Wi-Fi Many traditional college campuses in the United States provide at least partial wireless Wi-Fi Internet coverage. [Carnegie Mellon University](http://en.wikipedia.org/wiki/Carnegie_Mellon_University) was the first to build a campus-wide wireless Internet network, know as [Wireless Andrew](http://en.wikipedia.org/wiki/Wireless_Andrew), at its [Pittsburgh](http://en.wikipedia.org/wiki/Pittsburgh) campus in 1993 before Wi-Fi branding was originated. In Europe many universities collaborate in providing Wi-Fi access to students and staff through the[eduroam](http://en.wikipedia.org/wiki/Eduroam) international authentication infrastructure.  In 2000, [Drexel University](http://en.wikipedia.org/wiki/Drexel_University) in Philadelphia became the United States' first major university to offer completely wireless Internet access across its entire campus. The [Far Eastern University](http://en.wikipedia.org/wiki/Far_Eastern_University) which is in [Manila](http://en.wikipedia.org/wiki/Manila) is the first university in the [Philippines](http://en.wikipedia.org/wiki/Philippines) to implement a campus-wide Wi-Fi coverage. Amity University was India’s first Wi-Fi campus. SECTION VIII: Issues of Data Security In the same way that all one need to pick up a local radio station is a radio, all anybody needs to connect to a wireless network within nearby range is a wireless-equipped computer. A common measure to deter unauthorized users involves hiding the access point's name by disabling the [SSID](http://en.wikipedia.org/wiki/Service_set_(802.11_network)) broadcast. It is effective against the casual user but it is not an effective security method because the SSID is broadcast in the clear in response to a client SSID query. One more technique is to allow only those computers to join the network whose MAC addresses are known. But determined eavesdroppers may still be able to join the network by [spoofing](http://en.wikipedia.org/wiki/MAC_spoofing) an authorized address. Wireless network hardware supports several standard encryption schemes; the most common is Wired Equivalent Privacy ([WEP](http://www.webopedia.com/TERM/W/WEP.html)), Wi-Fi Protected Access ([WPA](http://www.webopedia.com/TERM/W/WPA.html)), and Wi-Fi Protected Access 2 ([WPA2](http://www.webopedia.com/TERM/W/WPA2.html)). [Wired Equivalent Privacy](http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) (WEP) encryption was designed to protect against casual snooping but it is no longer thought of as secure. Tools like [AirSnort](http://en.wikipedia.org/wiki/AirSnort) or [Aircrack-ng](http://en.wikipedia.org/wiki/Aircrack-ng) can quickly recover WEP encryption keys. Later the [Wi-Fi Alliance](http://en.wikipedia.org/wiki/Wi-Fi_Alliance) approved the [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). WPA’s design was specifically made to work with older equipment usually through a firmware upgrade. Though it is more secure than WEP, WPA also has vulnerabilities.  The more secure [WPA2](http://en.wikipedia.org/wiki/WPA2) using [Advanced Encryption Standard](http://en.wikipedia.org/wiki/Advanced_Encryption_Standard) which was introduced in 2004 and is supported by most new Wi-Fi devices. WPA2 is totally compatible with WPA.  A flaw in a feature added to Wi-Fi in 2007, called [Wi-Fi Protected Setup](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup), allowed WPA and WPA2 security to be bypassed and effectively broken in many situations. The only remedy till late 2011 was to turn off Wi-Fi Protected Setup, which was not always possible.  Unless one intend to provide public access to their wireless network — and put their business data or their own personal data at risk — one should consider encryption mandatory. Unencrypted Wi-Fi networks can only be secured by using other means of protection, like a [VPN](http://en.wikipedia.org/wiki/Virtual_private_network) or [Hypertext Transfer Protocol](http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol) secure ([HTTPS](http://en.wikipedia.org/wiki/HTTP_Secure)) over [Transport Layer Security](http://en.wikipedia.org/wiki/Transport_Layer_Security).   |  | | --- | | **DID YOU KNOW...**  ad-hoc mode is an 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP). Ad-hoc mode is also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS). Ad-hoc mode is useful for establishing a network where wireless infrastructure does not exist or where services are not required. |  The Widespread Use of WEP Extensive use of WEP is absolutely understandable given that to the layman, the similar abbreviations WEP and WPA do not convey any meaningful difference between the two security methods (and they may even imply equivalence. In addition, WEP is almost always presented first by the security interface of most broadband routers since WEP comes before WPA both historically and alphabetically). Even if a router is years old, it most certainly will support some form of WPA (and if it doesn't, upgrade it to the latest firmware). The easiest-to-use & most widely supported version is WPA Personal, sometimes known as WPA Pre-Shared Key (PSK). Wireless Encryption Protocol (WEP) Explained Short for Wired Equivalent Privacy (or Wireless Encryption Protocol), [WEP](http://www.webopedia.com/TERM/W/WEP.html) is a part of the IEEE [802.11](http://www.webopedia.com/TERM/8/802_11.html) wireless networking standard and it was designed to provide the same level of security as that of a wired [LAN](http://www.webopedia.com/TERM/L/local_area_network_LAN.html). As wireless networks broadcast messages using radio, they are vulnerable to eavesdroppers. WEP offers protection by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. WEP was the encryption scheme considered to be the initial standard for first generation wireless networking devices. Nevertheless, it has been discovered that WEP is not as it was secure as once believed to be. WEP is used at the two most lowest layers of the [OSI model](http://www.webopedia.com/DidYouKnow/Computer_Science/2006/understanding_layers.asp) - the data link and physical layers; it therefore does not offer end-to-end security. WEP's Major Weakness WEP's major weakness is its use of static encryption keys. When one sets up a router with a WEP encryption key, that one key has to be used by every device on that network to encrypt every packet that's transmitted. But just because that packets are encrypted doesn't prevent them from being intercepted, and because of some esoteric technical flaws it's entirely possible for an eavesdropper to intercept enough WEP-encrypted packets to eventually deduce what the key is.  This problem used to be something you could mitigate by periodically changing the WEP key (which is why routers generally allow you to store upto four keys). But very few users bother to do this as changing WEP keys is inconvenient and time-consuming because it has to be done not just on the router, but on every device that is connected to it. As a result, most people set up a single key and then continue using it ad infinitum.  Even worse, for those that do change the WEP key, new research & development reinforce how even changing WEP keys frequently is no longer sufficient to protect a WLAN. The process of 'cracking' a WEP key used to require that a malicious hacker intercept millions of packets plus spend a fair amount of time and computing power. Researchers in computer science department of a German university recently demonstrated the capability to compromise a WEP-protected network rapidly. After spending not more than a minute intercepting data (fewer than  100,000 packets in all) they were able to intercept a WEP key in just three seconds.  The Differences between WEP and WPA  WPA has been the mainstream technology for years now, but WEP remains a standard feature on virtually every wireless router on store shelves today.  When using a wireless [access point](http://www.webopedia.com/DidYouKnow/_index.asp) or [router](http://www.webopedia.com/TERM/R/router.html) it is important to remember that if one can send information from one device and receive it on another, anyone else within the range might also be able to receive that information. When you want to protect data send via wireless connection, security and protection is of given through [encryption](http://www.webopedia.com/TERM/E/encryption.html) schemes that come with your wireless hardware you can enable.  Network Encryption Using WPA Personal/PSK  To encrypt a network with WPA Personal/PSK one has to provide their router with a plain-English passphrase between 8 and 63 characters long and not some encryption key. Using a technology called TKIP (for Temporal Key Integrity Protocol), passphrase, and the network SSID, are used to generate unique encryption keys for each wireless client. Those encryption keys are constantly and regularly changed. (Although WEP supports passphrases, it does so to more easily create static keys, which usually comprise of the hex characters 0-9 and A-F).  If WPA is properly configured, it offers infinitely better protection than WEP, but this isn't to say that WPA security is iron-clad, because let's face it, what form of security really is? With that in mind, avoiding dictionary words in both the [SSID](http://www.webopedia.com/TERM/S/SSID.html) and WPA passphrase (and having as long a passphrase as possible) will provide a lot better protection than using "linksys" and your dog's name. Wi-Fi Protected Access (WPA) Address WEP's Shortcomings It wasn't long before a new technology called [WPA](http://www.webopedia.com/TERM/W/WPA.html), or Wi-Fi Protected Access was launched to address many of WEP's deficiencies. WPA intends to provide stronger wireless data encryption than WEP, but not everyone has been able to take up this new wireless encryption technology. In order to use WPA all the devices in the network must be configured for WPA.  If a device is not configured for WPA, it will fall back to a lesser WEP encryption scheme, enabling the wireless device communication on the network. The WPA technology was designed to work with existing Wi-Fi products that have been enabled with WEP (i.e., as a software upgrade to existing hardware), but the technology includes two enhancements over WEP:   * Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, also by adding an integrity-checking feature which ensures that the keys have not been tampered with. * User authentication, which is not there in WEP, through the extensible authentication protocol ([EAP](http://www.webopedia.com/TERM/E/EAP.html)). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is comparatively easy to be sniffed out and stolen. EAP is built on a more protected public-key encryption system to ensure that only authorized network users can access the network.   WPA has been a mainstream technology for many years now, but WEP remains a standard feature on practically every wireless router on store shelves at present. Even though it is mainly there for backward compatibility with the oldest hardware, if reports and studies are precise, a noteworthy proportion of WLANs operating today (especially those used in homes) are still using outdated and insecure WEP for their encryption.  Securing a New Network   1. Change the network name (SSID) from the default name 2. Change the administrative credentials (username and password) that control the configuration settings of your Access Point/Router/Gateway 3. Enable WPA2-Personal (aka WPA2-PSK) with AES encryption 4. Then create a network passphrase that will meet the recommended guidelines 5. Enable WPA2 security features on the device and enter the passphrase for the network  Passphrase Quality & Lifespan A secure network passphrase greatly enhances network security. In general, increasing the length, the complexity and the randomness - all improve the quality of a passphrase. Passphrase should be at least 8 characters long, and should include a mixture of upper & lower case letters and symbols. Passphrase should not contain a word found in a dictionary and should not include personal information like ID number, name, phone no., address, etc.  One should periodically change the passphrase on their network to increase security. Safety tips for on the road Wi-Fi Once users have experienced the convenience and freedom of working wirelessly, they would like to take their Wi-Fi on the road. These are some tips for securing Wi-Fi devices when they are used away from the home network.   * **Enable WPA2 security:** All the Wi-Fi client devices (laptops, handsets, and other Wi-Fi enabled products) should use WPA2. * **Configure to approve new connections**: Many devices are set by default to sense and automatically connect to any available wireless network. Configuring your device to request approval before connecting gives one greater control over their connections. * **Disable sharing**: Your Wi-Fi-enabled devices may automatically enable themselves to sharing / connecting with other devices when attaching to a wireless network. File & printer sharing may be common in business and home networks, but one should avoid this in a public networks like hotels, restaurants, or airport hotspots.  SECTION IX: SPECIAL FEATURESWi-Fi CERTIFIED™ ac Wi-Fi CERTIFIED products contain a logo identifying which features have been tested and that the product has met all the standards of the notation.  Wi-Fi CERTIFIED ac is the first generation of Wi-Fi that delivers up to a gigabit per second data rate, it connects demanding applications like multimedia streaming & fast file transfer on tablets, handsets and other devices.  The IEEE doesn’t test equipment for compliance with their standards. The [non-profit](http://en.wikipedia.org/wiki/Non-profit) organization of Wi-Fi Alliance was formed in 1999 to correct this and for establishing & enforcing standards for interoperability & [backward compatibility](http://en.wikipedia.org/wiki/Backward_compatibility), and to support [wireless](http://en.wikipedia.org/wiki/Wireless) local-area-network technologies. Till 2010, the Wi-Fi Alliance had more than 375 companies around the world. The Wi-Fi Alliance enforced the use of Wi-Fi brand on technologies based on the [IEEE 802.11](http://en.wikipedia.org/wiki/IEEE_802.11) standards from the [Institute of Electrical and Electronics Engineers](http://en.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers). This included [wireless local area network](http://en.wikipedia.org/wiki/Wireless_LAN) (WLAN) connections, device to device connectivity (such as Wi-Fi Peer to Peer aka Wi-Fi Direct), [Personal area network](http://en.wikipedia.org/wiki/Personal_area_network) (PAN), [local area network](http://en.wikipedia.org/wiki/Local_area_network) (LAN) and some limited [wide area network](http://en.wikipedia.org/wiki/Wide_area_network) (WAN) connections. Manufacturers with membership of Wi-Fi Alliance, whose products satisfy the certification process, gain the right to mark their products with the Wi-Fi logo.  The certification process requires conformance to the IEEE 802.11 radio standards, the [WPA & WPA2](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) security standards, and the [EAP](http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol) standards of authentication. Certification may also include tests of IEEE 802.11 draft standards, interaction with mobile-phone technology in converged devices, and features related to security set-up, multimedia, & power-saving.  Not every Wi-Fi device is submitted for certification. The lack of certification doesn’t entail that a device is incompatible with other Wi-Fi devices or if it is compliant or partly compatible. The Wi-Fi Alliance will not object to its description as a Wi-Fi devicethough only certified devices are approved. Terms like [Super Wi-Fi](http://en.wikipedia.org/wiki/Super_Wi-Fi), given by the US [Federal Communications Commission](http://en.wikipedia.org/wiki/Federal_Communications_Commission) (FCC) to illustrate proposed networking in UHF TV band in the USA, may or may not be sanctioned. Wi-Fi CERTIFIED Miracast™ Wi-Fi CERTIFIED Miracast™ provides seamless displaying of videos between devices, without the use of cables or network connections. Users can view pictures from smart phones on the television screen, share a laptop screen with conference room projector, and watch live shows from a home cable box on a tablet. Miracast connections are formed by using Wi-Fi CERTIFIED Wi-Fi Direct™, so access to Wi-Fi® network is not required. The ability to make a connection is inbuilt in the Miracast-certified device.  The technology works well across devices of any brand. Connections are easily set up and are convenient to use since the devices select the appropriate settings automatically. Miracast supports premium content—like Blu-ray feature films, live television shows, sports, or any other copy-protected premium content. Wi-Fi CERTIFIED Passpoint™ Today, there are more than a million hotspots around the world - and that number is growing exponentially.  Prediction by Informa Telecoms and Media is that there will be 5.8million hotspots all around the world by 2015.  This growth is driven by mobile service providers.  As the number of hotspots increases over the next few years, using them will become easier.  Right now, connecting in most hotspot environments can be cumbersome - users typically have to search for and select a network then request the connection to the access point (AP) each time, and in most cases, have to re-enter their authentication credentials. But a new program by the device makers and service providers in the Wi-Fi industry is changing all of that.  Wi-Fi CERTIFIED Passpoint™ transforms the way users connect to Wi-Fi hotspot networks by making the process of finding and getting access to the right network seamless.  It also provides WPA2™ security protection. Mobile devices, such as handsets and tablets that are certified for Passpoint may still use the existing hotspots. In a Passpoint-enabled hotspot, one finds a newly-smooth connectivity experience.  As Passpoint-enabled hotspots multiply, users can use Wi-Fi roaming.  Mobile service providers are working together to define mechanisms for subscribers to “roam” to one another’s hotspots.  Wi-Fi Direct™  Wi-Fi CERTIFIED Wi-Fi Direct™ is a certification mark launched in 2010 for devices supporting a game-changing new technology enabling Wi-Fi devices like computers, laptops, smart phones etc to connect directly without an access point intermediary, making it simple and convenient to do stuff like print, share, sync and display. Products having the Wi-Fi Direct certification mark can connect to one another without joining a traditional home, office or hotspot network. This is called ad hoc Wi-Fi transmission. The [wireless ad hoc network](http://en.wikipedia.org/wiki/Wireless_ad_hoc_network) mode has become popular with [multiplayer](http://en.wikipedia.org/wiki/Multiplayer_video_game) [handheld game consoles](http://en.wikipedia.org/wiki/Handheld_game_console), digital cameras and other electronics. Some devices can also share their Internet connection using ad-hoc, becoming hotspots or "virtual routers".  Devices can make a one-to-one connection, or a group of devices can connect at the same time. Connecting of Wi-Fi Direct-certified devices is easy & simple. It can be done by pushing a button. Furthermore, all the Wi-Fi Direct connections are protected by WPA2™. With Wi-Fi Direct, one doesn’t need an access point or internet connection.  SECTION X: Advantages and Limitations Advantages Wi-Fi allows cheap deployment of [local area networks](http://en.wikipedia.org/wiki/Local_area_network) (LANs). It is helpful in places where cables cannot be setup, such as outdoor areas and historical buildings.  Manufacturers are building wireless network adapters into most laptops. The price of [chipsets](http://en.wikipedia.org/wiki/Chipset) for Wi-Fi is continuously dropping, which makes it an economical networking option to be 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](http://en.wikipedia.org/wiki/Backwards_compatible). Unlike [mobile phones](http://en.wikipedia.org/wiki/Mobile_phone), any standard Wi-Fi device will work anywhere in the world.  [Wi-Fi Protected Access](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) encryption (WPA2) is said to be most secure, if a strong [passphrase](http://en.wikipedia.org/wiki/Passphrase) is used. New protocols for [quality-of-service](http://en.wikipedia.org/wiki/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). Power saving mechanisms (WMM Power Save) extend the battery life. Limitations Spectrum assignments and operational limitations are not consistent worldwide: most of Europe allows for an additional two channels beyond those permitted in the US for the 2.4 GHz band (1–13 vs. 1–11), while Japan has one more on top of that (1–14). As of 2007, Europe is essentially homogeneous in this respect.  A Wi-Fi signal uses five channels in the 2.4 GHz band. It uses any two channel numbers which differ by five or more, like 2 and 7, as they don’t overlap. The often-repeated myth that channels 1, 6, and 11 are the only non-overlapping channels is, hence, not accurate. But channels 1, 6, & 11 are the only group of the three non-overlapping channels in the U.S. Thought it is recommended for Europe and Japan to use channels 1, 5, 9, and 13 for 802.11g and 802.11n.  [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) (100 mW).  The current 'fastest' norm, 802.11n, uses double radio spectrum/bandwidth (40 MHz) than [802.11a](http://en.wikipedia.org/wiki/IEEE_802.11#802.11a) or 802.11g (20 MHz). This indicates that only one 802.11n network on a 2.4GHz band can be setup at a given loation, without interference to/from other WLAN traffic. 802.11n may also be set to use 20 MHz bandwidth only to prevent interference in dense community.  SECTION XI: Issues of Safety & Health  James Hrynyshyn wrote about the effects on health in Nova Scotia due to the installation of a tower to provide wireless internet to the area.  “I think over a period of time it will change the DNA of the garlic because it shakes up the molecules,” he said.  East Link uses microwave transmission for providing high-speed internet access in rural areas outside its wired network.  Levine moved to the country to get away from pollution, but he sees the radiation from towers as another type of pollution.  “I view it with dread, fear and panic,” said he. “I don’t want to grow food under those conditions.”  To do estimations, one should know about how light carries its energy. It’s almostly accurate to think of light as a stream of particles known as photons, every photon has a specific amount of energy which is proportional to its frequency. Light also has wave properties like diffraction and interference which can’t be described in terms of photons, but for this purpose we don’t have to consider the wave properties. One just has to remember that these photons do possess wave nature and are not only particles in the conventional sense of particles. With that as a caveat, one can truly say that light comes in photons and all photons have a certain energy. The energy of a photon is given by:  i-d4bb9fe09d6b78eb832985821d8a307f-1.png  This gives the energy of a photon in electron volts given the wavelength is in nanometers. Visible light ranges from around 750 nanometers in red end to 380 in blue end and in terms of energy the formula gives the range of photons from approximately 1.6 to 3.3 electron volts. This is nearly in order of the energies involved in electron energy levels, which is the basis of chemistry. Chemical reactions are capable of making visible light (glow stocks, fireflies, etc) and light can make chemical reactions happen (camera film & dye fading etc). Ultraviolet light from sun is of a shorter wavelength of about 300 nanometers or so from which one should protect them self. These are about 4.2 electron volt and strong enough to excite more energetic electron energy levels and also dissociate molecules. If it’s a DNA molecule, they damage & break due to absorbing of the photons which eventually leads to skin cancer and other numerous health problems.  WiFi operates in the 2.4 GHz frequency range, which is same as a microwave oven. The wavelength of that light is about 125 million nanometers. Hence each photon carries almost exactly 1/100,000 of an eV worth of energy. This energy is nowhere near the ~1+ energies involved in electron energy levels, and have this kind of radiation can’t cause any damage to DNA. The energy just isn’t enough. In addition, by the quantum nature of electron energy levels, one can’t stack up 100,000 microwave photons to cause a 1 eV transition. One has to actually have a 1 eV photon. (Technically there is something called as multi-photon transition, but it’s nature is strongly nonlinear with a probability that’s very low for 2 photon transitions & exponentially worse as the number increases. 100,000 is not possible at all.)  Now the question arises if microwave photons cannot damage the DNA, how are they able to cook food and boil water in the microwave oven? The response is easy: the energy they possess is more than enough to excite the much less energetic rotational & vibrational states of the molecules. The motion caused produces heat. The total power output of a WiFi transmitter is of magnitude less than a microwave oven by many orders – 1 watt tends to be the upper limit for home & business transmitters, so any person standing around will absorb only a minute fraction of that minute fraction. The increase in temperature from absorbing WiFi signals can’t be measured, and mathematically speaking it is itself dwarfed by other radio/microwave sources like mobile phones, broadcast radio and TV.  WiFi cannot hurt anyone, neither their DNA nor their crops.  The [World Health Organization](http://en.wikipedia.org/wiki/World_Health_Organization) (WHO) said that "there is no risk from low level, long-term exposure to Wi-Fi networks." The UK’s [Health Protection Agency](http://en.wikipedia.org/wiki/Health_Protection_Agency) reported that the exposure to Wi-Fi for a year results in the "same amount of radiation from a 20-minute mobile phone call."  A small percentage of Wi-Fi users have reported adverse health issues due to repeat exposure and use of Wi-Fi, though there was no publication of any effects being observed in the [double-blind study](http://en.wikipedia.org/wiki/Double-blind_study). A review of the study involved 725 people that claimed [electromagnetic hypersensitivity](http://en.wikipedia.org/wiki/Electromagnetic_hypersensitivity) found no evidence of the claim by those people.  One study claimed in preliminary results, that "laptops (Wi-Fi mode) on the lap near the testicles can decrease male fertility". Another small model test of (fifteen males and fifteen females) found a decrease in the [P300](http://en.wikipedia.org/wiki/P300_(neuroscience)) event-related potential ([ERP](http://en.wikipedia.org/wiki/Event-related_potential)) of males but not of female subjects while engaging in some [working memory](http://en.wikipedia.org/wiki/Working_memory) oriented linguistic task during Wi-Fi exposure.  SECTION XII: CONCLUSION  After spending more than two months collecting information about Wi-Fi from various books, papers, journals, reports, websites etc I have come to realize that Wi-Fi is much bigger than the connection I use at home or in college. It is connecting the world. The advancements in this field of technology in such a short time span has been nothing but astonishing and it shows primary desire of human to stay connected in a perfect way. Wi-Fi alliance has been a remarkable gift to the enthusiasts of wireless networking.  There is a lot more scope in this field. A lot of work can be done towards increasing the speed and range of Wi-Fi. The speed one gets is one third of the speed promised and that too decreases with the increase in distance from the access point. The problem of interference if dealt with completely will make Wi-Fi shine even brighter. The main problem is the problem of security which requires the maximum amount of work. A lot has been done – WEP gave way to WPA and WPA2, yet it is not enough. Most people still use WEP which should change, more awareness to common man should be give regarding newer security programs and configuring them should be made very user friendly.  SECTION XIII: APPENDIX 802.11 Today's Wi-Fi products are designated by a Dewey Decimal-like system, developed by the IEEE to differentiate between various technology families.  Wi-Fi products are identified as 802.11, and are then further identified by a lower case letter that identifies which specific technology is in operation, such as 802.11a.  Each certification set is defined by a set of features that relate to performance, frequency and bandwidth.  Each generation also furthers security enhancements. Wi-Fi CERTIFIED products are tested to ensure that they work with previous generations of Wi-Fi products that operate in the same frequency band.  There are several specifications in the 802.11 family:   * **802.11** — applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum ([FHSS](http://www.webopedia.com/TERM/F/FHSS.html)) or direct sequence spread spectrum ([DSSS](http://www.webopedia.com/TERM/D/DSSS.html)). * [**802.11a**](http://www.webopedia.com/TERM/8/802_11a.html) — an extension to 802.11 that applies to wireless LANs and provides up to 54-Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than [FHSS](http://www.webopedia.com/TERM/F/FHSS.html) or [DSSS](http://www.webopedia.com/TERM/D/DSSS.html). * [**802.11b**](http://www.webopedia.com/TERM/8/802_11b.html) (also referred to as 802.11 High Rate or Wi-Fi) — an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1-Mbps) in the 2.4 GHz band. 802.11b uses only [DSSS](http://www.webopedia.com/TERM/D/DSSS.html). 802.11b was 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet. * [**802.11e**](http://www.webopedia.com/TERM/8/802_11e.html) — a wireless draft standard that defines the **Q**uality **o**f **S**ervice ([QoS](http://www.webopedia.com/TERM/Q/QoS.html)) support for LANs, and is an enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications. 802.11e adds QoS features and multimedia support to the existing IEEE 802.11b and IEEE 802.11a wireless standards, while maintaining full backward compatibility with these standards. * [**802.11g**](http://www.webopedia.com/TERM/8/802_11g.html) — applies to wireless LANs and is used for transmission over short distances at up to 54-Mbps in the 2.4 GHz bands. * [**802.11n**](http://www.webopedia.com/TERM/8/802_11n.html) — 802.11n builds upon previous 802.11 standards by adding**m**ultiple-**i**nput **m**ultiple-**o**utput ([MIMO](http://www.webopedia.com/TERM/M/MIMO.html)). The additional transmitter and receiver antennas allow for increased data throughput through spatial multiplexing and increased range by exploiting the spatial diversity through coding schemes like Alamouti coding. The real speed would be 100 Mbit/s (even 250 Mbit/s in PHY level), and so up to 4-5 times faster than 802.11g. * [**802.11ac**](http://www.webopedia.com/TERM/8/802_11ac.html) — 802.11ac builds upon previous 802.11 standards, particularly the 802.11n standard, to deliver data rates of 433Mbps per spatial stream, or 1.3Gbps in a three-antenna (three streams) design. The 802.11ac specification operates only in the 5 GHz frequency range and features support for wider channels (80MHz and 160MHz) and beam forming capabilities by default to help achieve its higher wireless speeds. * [**802.11ad**](http://www.webopedia.com/TERM/8/802_11ad.html) — 802.11ad is a wireless specification under development that will operate in the 60GHz frequency band and offer much higher transfer rates than previous 802.11 specs, with a theoretical maximum transfer rate of up to 7Gbps ([Gigabits per second](http://www.webopedia.com/TERM/G/Gbps.html)). * [**802.11r**](http://www.webopedia.com/TERM/8/802_11r.html) - 802.11r, also called Fast **B**asic **S**ervice **S**et ([BSS](http://www.webopedia.com/TERM/B/Basic_Service_Set.html)) Transition, supports [VoWi-Fi](http://www.webopedia.com/TERM/V/VoWiFi.html) handoff between access points to enable [VoIP](http://www.webopedia.com/TERM/V/VoIP.html) roaming on a [Wi-Fi](http://www.webopedia.com/TERM/W/Wi_Fi.html) network with [802.1X](http://www.webopedia.com/TERM/8/802_1x.html) authentication. * [**802.1X**](http://www.webopedia.com/TERM/8/802_1x.html) — Not to be confused with 802.11x (which is the term used to describe the family of 802.11 standards) 802.1X is an IEEE standard for port-based Network Access Control that allows network administrators to restricted use of IEEE 802 LAN service access points to secure communication between authenticated and authorized devices.   SECTION XIV: REFERENCES  Abstract and full paper on WI-FI TECHNOLOGY. (2013). Retrieved from Creative world9 website: http://www.creativeworld9.com/2011/03/abstract-and-full-paper-on-wi-fi.html  Abstract and full paper on WI-FI TECHNOLOGY. (2011, August 5). Retrieved May 25, 2013, from http://www.creativeworld9.com/2011/03/abstract-and-full-paper-on-wi-fi.html  Electromagnetic interference at 2.4 GHz - Wikipedia, the free encyclopedia. (2013). Retrieved May 18, 2013, from http://en.wikipedia.org/wiki/Electromagnetic\_interference\_at\_2.4\_GHz  Interference (communication) - Wikipedia, the free encyclopedia. (2013). Retrieved May 30, 2013, from http://en.wikipedia.org/wiki/Interference\_(communication)  IT business edge (2013). What is Wi-Fi? - An IT Definition From Webopedia.com. Retrieved May 15, 2013, from http://www.webopedia.com/TERM/W/Wi\_Fi.html  Lowe, D. (2008). Book V: Wireless Networking. In Networking: All-in-one Desk Reference(3rd ed.). New Delhi, India: Wiley.  Parvatha (2013). Wifi - Research Paper - Parvatha03. Retrieved from studymode website: http://www.studymode.com/essays/Wifi-642922.html  Springer, M. (2009, September 17). WiFi and Radiation – Built on Facts. Retrieved May 30, 2013, from http://scienceblogs.com/builtonfacts/2009/09/17/wifi-and-radiation/  Tanenbaum, A. S. (2003). Computer Networks (4th ed.). New Jersery, US: Prentice-Hall.  Vigneri, R. (2013). Radio physics for wireless devices and networking. Retrieved from http://hosteddocs.ittoolbox.com/RV100908a.pdf  Wi-Fi - Wikipedia, the free encyclopedia. (n.d.). Retrieved May 11, 2013, from http://en.wikipedia.org/wiki/Wi-Fi  Wi-Fi Alliance (2013). Wi-Fi Alliance. Retrieved May 11, 2103, from http://www.wi-fi.org/discover-and-learn |