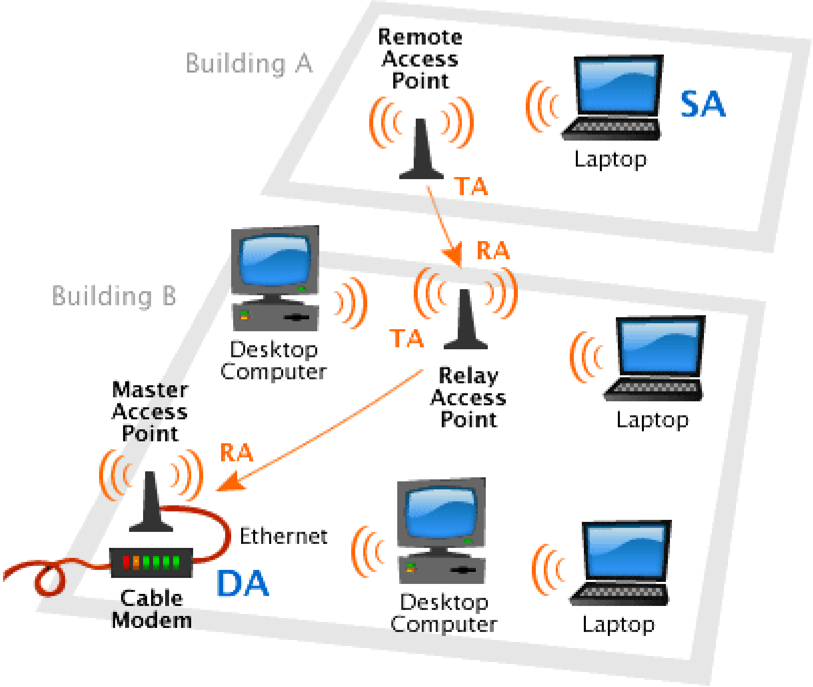
Wi Fi (Wireless Fidelity) is a generic term that refers to the IEEE 802.11 set of standards for wireless local area networks (WLANs). Wi Fi is a trademark of the Wi-Fi Alliance, founded in 1999 as Wireless Internet Compatibility Alliance (WICA), comprising more than 300 companies, whose products are certified by the Wi-Fi Alliance, based on the IEEE 802.11 standards. The Wi-Fi Alliance tests the wireless components to their own terms of reference. Products that pass become Wi-Fi certified and may carry the Wi-Fi logo. Only products of Wi-Fi Members are tested, because they pay membership and per-item fees. Absence of the Wi-Fi logo does not necessarily mean non-compliance with the standard. Wi-Fi certification is provided for technology used in home networks, mobile phones, video games, and other devices that require wireless networking. It covers IEEE 802.11 standards, including 802.11a, 802.11b, 802.11g, and 802.11n.

How a Wi Fi Network Works

Wi-Fi is supported by most personal computer operating systems, many game consoles, laptops, smartphones, printers, and other peripherals. The basic principle behind Wi Fi is almost the same as a walkie talkie. A Wi Fi hotspot is created by installing an access point to an internet connection. An access point acts as a base station. When a Wi Fi enabled device encounters a hotspot the device can then connect to that network wirelessly.

A single access point can support upto 30 users and can function whithin a range of 100-150 feet indoors and upto 300 feet outdoors. Many access points can be connected to each other via ethernet cables to create a single large network.



A roof mounted Wi Fi antennae

The Elements of a Wi Fi Network

A Wi Fi network is composed of the following main 3 components -

- **Access Point (AP)** – The AP is a wireless LAN transceiver or “base station” that can connect one or many wireless devices simultaneously to the internet.
- **Wi-Fi Cards –** They accept the wireless signal and relay information. They can be internal and external.(eg. PCMCIA card for laptop and PCI card for desktop PC)**.**
- **Safeguards –** Firewalls and anti- virus software protect networks from unauthorized access and keep information safe and secure.

The Wi Fi Technology

Wi Fi networks use the IEEE 802.11 technology standards for WLAN.
IEEE 802.11 is a set of standards carrying out wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are implemented by the IEEE LAN/MAN Standards Committee (IEEE 802).

Protocols

802.11-1997 (802.11 legacy)

The original version of the standard IEEE 802.11 was released in 1997 and clarified in 1999, but is today obsolete. It specified two net bit rates of 1 or 2 megabits per second (Mbit/s), plus forward error correction code. It specifed three alternative physical layer technologies: **diffuse infrared** operating at 1 Mbit/s; **frequency-hopping** spread spectrum operating at 1 Mbit/s or 2 Mbit/s; and **direct-sequence** spread spectrum operating at 1 Mbit/s or 2 Mbit/s. The latter two radio technologies used microwave transmission over the Industrial Scientific Medical frequency band at 2.4 GHz. Some earlier WLAN technologies used lower frequencies, such as the U.S. 900 MHz ISM band.

FHSS

Frequency-hopping spread spectrum (FHSS) is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver. It is utilized as a multiple access method in the frequency-hopping code division multiple access (FH-CDMA) scheme.

A spread-spectrum transmission offers three main advantages over a fixed-frequency transmission:

1. Spread-spectrum signals are highly resistant to narrowband interference. The process of re-collecting a spread signal spreads out the interfering signal, causing it to recede into the background.
2. Spread-spectrum signals are difficult to intercept. An FHSS signal simply appears as an increase in the background noise to a narrowband receiver. An eavesdropper would only be able to intercept the transmission if they knew the pseudorandom sequence.
3. Spread-spectrum transmissions can share a frequency band with many types of conventional transmissions with minimal interference. The spread-spectrum signals add minimal noise to the narrow-frequency communications, and vice versa. As a result, bandwidth can be utilized more efficiently.

Typically, the initiation of an FHSS communication is as follows

1. The initiating party sends a request via a predefined frequency or control channel.

2. The receiving party sends a number, known as a seed.

3. The initiating party uses the number as a variable in a predefined algorithm, which calculates the sequence of frequencies that must be used. Most often the period of the frequency change is predefined, as to allow a single base station to serve multiple connections.

4. The initiating party sends a synchronization signal via the first frequency in the

calculated sequence, thus acknowledging to the receiving party it has correctly calculated the sequence.

5. The communication begins, and both the receiving and the sending party change their frequencies along the calculated order, starting at the same point in time.

In some uses, most often military, a predefined frequency-hopping sequence is negotiated, and after completing the first step the procedure is continued from number .

The overall bandwidth required for frequency hopping is much wider than that required to transmit the same information using only one carrier frequency. However, because transmission occurs only on a small portion of this bandwidth at any given time, the effective interference bandwidth is really the same. Whilst providing no extra protection against wideband thermal noise, the frequency-hopping approach does reduce the degradation caused by narrowband interferers.

One of the challenges of frequency-hopping systems is to synchronize the transmitter and receiver. One approach is to have a guarantee that the transmitter will use all the channels in a fixed period of time. The receiver can then find the transmitter by picking a random channel and listening for valid data on that channel. The transmitter's data is identified by a special sequence of data that is unlikely to occur over the segment of data for this channel and the segment can have a checksum for integrity and further identification. The transmitter and receiver can use fixed tables of channel sequences so that once synchronized they can maintain communication by following the table. On each channel segment, the transmitter can send its current location in the table.

In the US, FCC part 15 on unlicensed system in the 900MHz and 2.4GHz bands permits more power than non-spread spectrum systems. Both frequency hopping and direct sequence systems can transmit at 1 Watt. The limit is increased from 1 milliwatt to 1 watt or a thousand times increase. The Federal Communications Commission (FCC) prescribes a minimum number of channels and a maximum dwell time for each channel.

In a real multipoint radio system, space allows multiple transmissions on the same frequency to be possible using multiple radios in a geographic area. This creates the possibility of system data rates that are higher than the Shannon limit for a single channel. Spread spectrum systems do not violate the Shannon limit. Spread spectrum systems rely on excess signal to noise ratios for sharing of spectrum. This property is also seen in MIMO and DSSS systems. Beam steering and directional antennas also facilitate increased system performance by providing isolation between remote radios.

DSSS

In telecommunications, direct-sequence spread spectrum (DSSS) is a modulation technique. As with other spread spectrum technologies, the transmitted signal takes up more bandwidth than the information signal that is being modulated. The name 'spread spectrum' comes from the fact that the carrier signals occur over the full bandwidth (spectrum) of a device's transmitting frequency.

1. It phase-modulates a sine wave pseudorandomly with a continuous string of pseudonoise (PN) code symbols called "chips", each of which has a much shorter duration than an information bit. That is, each information bit is modulated by a sequence of much faster chips. Therefore, the chip rate is much higher than the information signal bit rate.
2. It uses a signal structure in which the sequence of chips produced by the transmitter is known a priori by the receiver. The receiver can then use the same PN sequence to counteract the effect of the PN sequence on the received signal in order to reconstruct the information signal.

Direct-sequence spread-spectrum transmissions multiply the data being transmitted by a "noise" signal. This noise signal is a pseudorandom sequence of 1 and −1 values, at a frequency much higher than that of the original signal, thereby spreading the energy of the original signal into a much wider band.

The resulting signal resembles white noise, like an audio recording of "static". However, this noise-like signal can be used to exactly reconstruct the original data at the receiving end, by multiplying it by the same pseudorandom sequence (because 1 × 1 = 1, and −1 × −1 = 1). This process, known as "de-spreading", mathematically constitutes a correlation of the transmitted PN sequence with the PN sequence that the receiver believes the transmitter is using.

For de-spreading to work correctly, the transmit and receive sequences must be synchronized. This requires the receiver to synchronize its sequence with the transmitter's sequence via some sort of timing search process. However, this apparent drawback can be a significant benefit: if the sequences of multiple transmitters are synchronized with each other, the relative synchronizations the receiver must make between them can be used to determine relative timing, which, in turn, can be used to calculate the receiver's position if the transmitters' positions are known. This is the basis for many satellite navigation systems.

The resulting effect of enhancing signal to noise ratio on the channel is called process gain. This effect can be made larger by employing a longer PN sequence and more chips per bit, but physical devices used to generate the PN sequence impose practical limits on attainable processing gain.

If an undesired transmitter transmits on the same channel but with a different PN sequence (or no sequence at all), the de-spreading process results in no processing gain for that signal. This effect is the basis for the code division multiple access (CDMA) property of DSSS, which allows multiple transmitters to share the same channel within the limits of the cross-correlation properties of their PN sequences.

As this description suggests, a plot of the transmitted waveform has a roughly bell-shaped envelope centered on the carrier frequency, just like a normal AM transmission, except that the added noise causes the distribution to be much wider than that of an AM transmission.

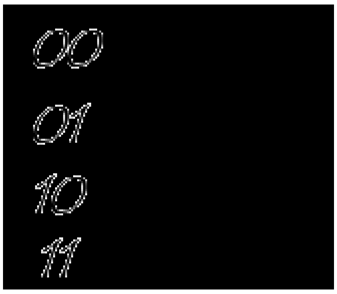
In contrast, frequency-hopping spread spectrum pseudo-randomly re-tunes the carrier, instead of adding pseudo-random noise to the data, which results in a uniform frequency distribution whose width is determined by the output range of the pseudo-random number generator.

Infrared technology

The IEEE 802.11 standard also provides for an alternative to radio waves: infrared light. The primary feature of infrared technology is the use of a light wave to transmit data. These transmissions travel mono-directionally, whether by using a direct line of sight or reflected off a surface. The non-diffuse nature of light waves offers a higher level of security.

With infrared technology, it is possible to send data at 1 to 2 Mbits per second by using a kind of modulation called **PPM** (*pulse position modulation*).

PPM modulation involves transmitting constant-amplitude pulses and encoding information based on its pulse position. A transfer speed of 1 Mbps is reached with 16-PPM modulation, while 2 Mbps is reached with 4-PPM modulation, which allows two bits of data to be encoded with four possible positions.



Orthogonal Frequency Division Multiplexing

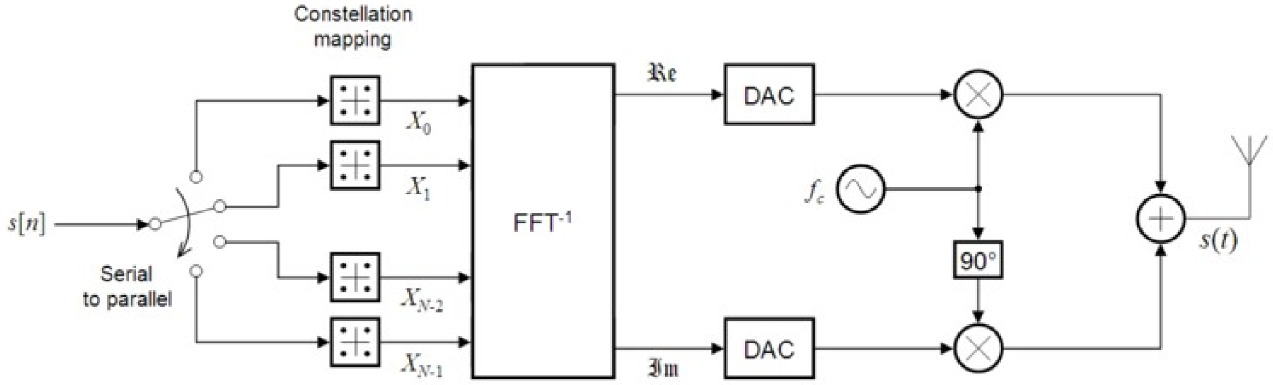
Orthogonal frequency-division multiplexing (OFDM) — essentially identical to Coded OFDM (COFDM) and Discrete multi-tone modulation (DMT) — is a frequency-division multiplexing (FDM) scheme utilized as a digital multi-carrier modulation method. A large number of closely-spaced orthogonal sub-carriers are used to carry data. The data is divided into several parallel data streams or channels, one for each sub-carrier. Each sub-carrier is modulated with a conventional modulation scheme (such as quadrature amplitude modulation or phase shift keying) at a low symbol rate, maintaining total data rates similar to conventional single-carrier modulation schemes in the same bandwidth.

OFDM has developed into a popular scheme for wideband digital communication, whether wireless or over copper wires, used in applications such as digital television and audio broadcasting, wireless networking and broadband internet access.

The primary advantage of OFDM over single-carrier schemes is its ability to cope with severe channel conditions — for example, attenuation of high frequencies in a long copper wire, narrowband interference and frequency-selective fading due to multipath — without complex equalization filters. Channel equalization is simplified because OFDM may be viewed as using many slowly-modulated narrowband signals rather than one rapidly-modulated wideband signal. The low symbol rate makes the use of a guard interval between symbols affordable, making it possible to handle time-spreading and eliminate intersymbol interference (ISI). This mechanism also facilitates the design of single-frequency networks, where several adjacent transmitters send the same signal simultaneously at the same frequency, as the signals from multiple distant transmitters may be combined constructively, rather than interfering as would typically occur in a traditional single-carrier system.

Transmitter

An OFDM carrier signal is the sum of a number of orthogonal sub-carriers, with baseband data on each sub-carrier being independently modulated commonly using some type of quadrature amplitude modulation (QAM) or phase-shift keying (PSK). This composite baseband signal is typically used to modulate a main RF carrier.



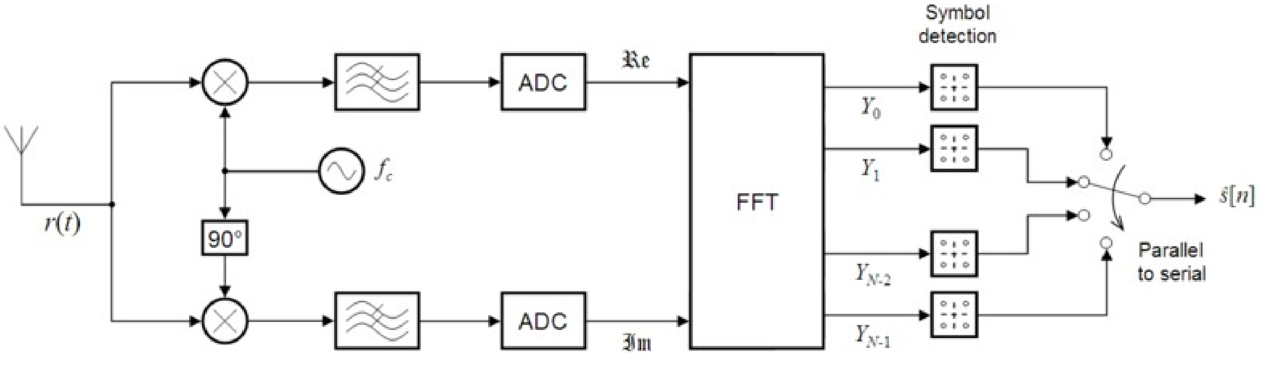
s[n] is a serial stream of binary digits. By inverse multiplexing, these are first demultiplexed into N parallel streams, and each one mapped to a (possibly complex) symbol stream using some modulation constellation (QAM, PSK, etc.). Note that the constellations may be different, so some streams may carry a higher bit-rate than others.

An inverse FFT is computed on each set of symbols, giving a set of complex time-domain samples. These samples are then quadrature-mixed to passband in the standard way. The real and imaginary components are first converted to the analogue domain using digital-to-analogue converters (DACs); the analogue signals are then used to modulate cosine and sine waves at the carrier frequency, f_c, respectively.

These signals are then summed to give the transmission signal, $s(t)$.

The linearity requirement is demanding, especially for transmitter RF output circuitry where amplifiers are often designed to be non-linear in order to minimise power consumption. In practical OFDM systems a small amount of peak clipping is allowed to limit the PAPR in a judicious tradeoff against the above consequences. However, the transmitter output filter which is required to reduce out-of-band spurs to legal levels has the effect of restoring peak levels that were clipped, so clipping is not an effective way to reduce PAPR.

Receiver



The receiver picks up the signal r(t), which is then quadrature-mixed down to baseband using cosine and sine waves at the carrier frequency. This also creates signals centered on 2fc, so low-pass filters are used to reject these. The baseband signals are then sampled and digitised using analogue-to-digital converters (ADCs), and a forward FFT is used to convert back to the frequency domain.

This returns N parallel streams, each of which is converted to a binary stream using an appropriate symbol detector. These streams are then re-combined into a serial stream, {\hat s}[n], which is an estimate of the original binary stream at the transmitter.

Mathematical Description

If N sub-carriers are used, and each sub-carrier is modulated using M alternative symbols, the OFDM symbol alphabet consists of MN combined symbols.

The low-pass equivalent OFDM signal is expressed as:

$$\nu(t) = \sum_{k=0}^{N-1} X_k e^{j2\pi kt/T}, \quad 0 \le t < T,$$

where {Xk} are the data symbols, N is the number of sub-carriers, and T is the OFDM symbol time. The sub-carrier spacing of 1 / T makes them orthogonal over each symbol period; this property is expressed as:

$$\frac{1}{T}\int_0^T \left(e^{j2\pi k_1 t/T}\right)^* \left(e^{j2\pi k_2 t/T}\right) dt$$
$$= \frac{1}{T}\int_0^T e^{j2\pi(k_2-k_1)t/T} dt = \delta_{k_1 k_2}$$

where (\cdot)^* denotes the complex conjugate operator and \delta\, is the Kronecker delta.

To avoid intersymbol interference in multipath fading channels, a guard interval of length Tg is inserted prior to the OFDM block. During this interval, a cyclic prefix is transmitted such that the signal in the interval

$$-T_\mathrm{g} \le t < 0$$

equals the signal in the interval

$$(T - T_g) \leq t < T$$

The OFDM signal with cyclic prefix is thus -

$$\nu(t) = \sum_{k=0}^{N-1} X_k e^{j2\pi kt/T}, \quad -T_g \leq t < T$$

The low-pass signal above can be either real or complex-valued. Real-valued low-pass equivalent signals are typically transmitted at baseband—wireline applications such as DSL use this approach. For wireless applications, the low-pass signal is typically complex-valued; in which case, the transmitted signal is up-converted to a carrier frequency fc. In general, the transmitted signal can be represented as:

$$\begin{aligned} s(t) &= \Re\left\{\nu(t)e^{j2\pi f_c t}\right\} \\ &= \sum_{k=0}^{N-1} |X_k| \cos\left(2\pi[f_c + k/T]t + \arg[X_k]\right) \end{aligned}$$

802.11a

Release date	Op. Frequency	Throughput (typ.)	Net bit rate (max.)	Gross bit rate (max.)	Range (indoor)
October 1999	5 GHz	27 Mbit/s[4]	54 Mbit/s	72 Mbit/s	~35 m[*citation needed*]

The 802.11a standard uses the same data link layer protocol and frame format as the original standard, but an OFDM based air interface (physical layer). It operates in the 5 GHz band with a maximum net data rate of 54 Mbit/s, plus error correction code, which yields realistic net achievable throughput in the mid-20 Mbit/s[*citation needed*].

Since the 2.4 GHz band is heavily used to the point of being crowded, using the relatively un-used 5 GHz band gives 802.11a a significant advantage. However, this high carrier frequency also brings a disadvantage: The effective overall range of 802.11a is less than that of 802.11b/g; and in theory 802.11a signals cannot penetrate as far as those for 802.11b because they are absorbed more readily by walls and other solid objects in their path due to their smaller wavelength. In practice 802.11b typically has a higher distance range at low speeds (802.11b will reduce speed to 5 Mbit/s or even 1 Mbit/s at low signal strengths). However, at higher speeds, 802.11a typically has the same or higher range due to less interference.

802.11b

Release date	Frequency band	Throughput (typ.)	Net bit rate (max.)	Range (indoor)
October 1999	2.4 GHz	~5 Mbit/s[4]	11 Mbit/s	~30 m[*citation needed*]

802.11b has a maximum raw data rate of 11 Mbit/s and uses the same media access method defined in the original standard. 802.11b products appeared on the market in early 2000, since 802.11b is a direct extension of the modulation technique defined in the original standard. The dramatic increase in throughput of 802.11b (compared to the original standard) along with simultaneous substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

802.11b devices suffer interference from other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include: microwave ovens, Bluetooth devices, baby monitors and cordless telephones.

[edit] 802.11g

Release date	Op. Frequency	Throughput (typ.)	Net bit rate (max.)	Gross bit rate (max.)	Range (indoor)
June 2003	2.4 GHz	~22 Mbit/s[4]	54 Mbit/s	128 Mbit/s	~up to 100 m[*citation needed*]

In June 2003, a third modulation standard was ratified: 802.11g. This works in the 2.4 GHz band (like 802.11b), but uses the same OFDM based transmission scheme as 802.11a. It operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 19 Mbit/s average throughput[*citation needed*]. 802.11g hardware is fully backwards compatible with 802.11b hardware and therefore is encumbered with legacy issues that reduce throughput when compared to 802.11a by ~21%.

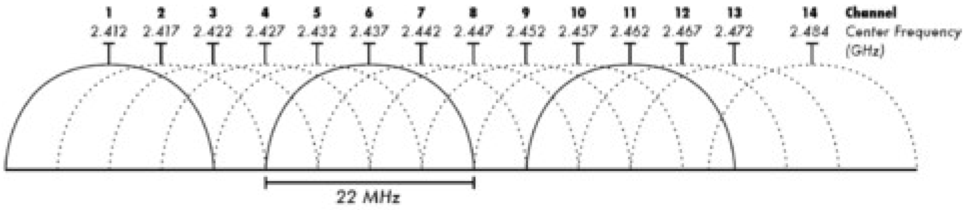
The then-proposed 802.11g standard was rapidly adopted by consumers starting in January 2003, well before ratification, due to the desire for higher data rates, and reductions in manufacturing costs. By summer 2003, most dual-band 802.11a/b products became dual-band/tri-mode, supporting a and b/g in a single mobile adapter card or access point. Details of making b and g work well together occupied much of the lingering technical process; in an 802.11g network, however, activity of an 802.11b participant will reduce the data rate of the overall 802.11g network.

Like 802.11b, 802.11g devices suffer interference from other products operating in the 2.4 GHz band.

Channels and International Compatibility

802.11 divides each of the above-described bands into channels, analogously to how radio and TV broadcast bands are carved up but with greater channel width and overlap. For example the 2.4000–2.4835 GHz band is divided into 13 channels each of width 22 MHz but spaced only 5 MHz apart, with channel 1 centred on 2.412 GHz and 13 on 2.472 GHz to which Japan adds a 14th channel 12 MHz above channel 13.

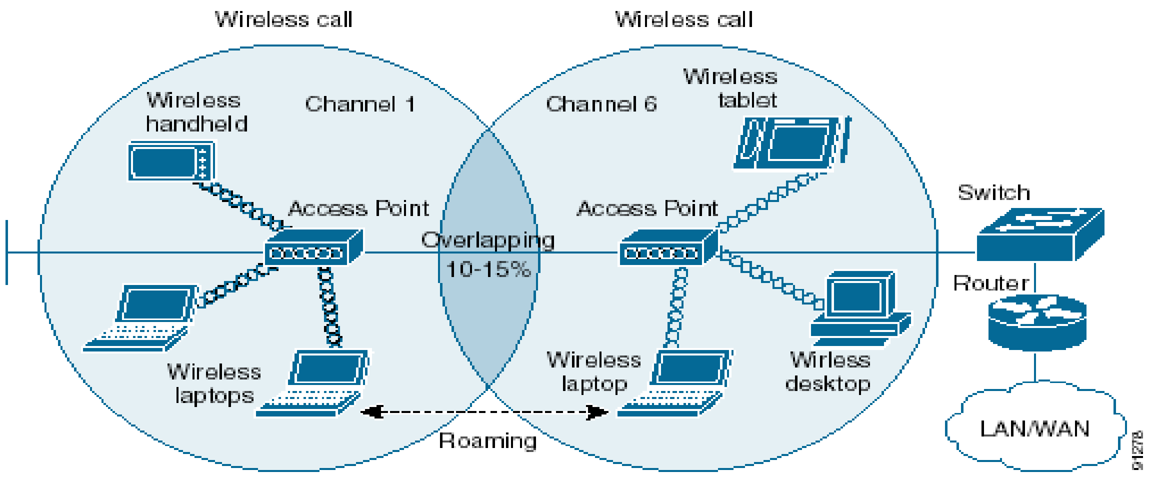
Availability of channels is regulated by country, constrained in part by how each country allocates radio spectrum to various services.



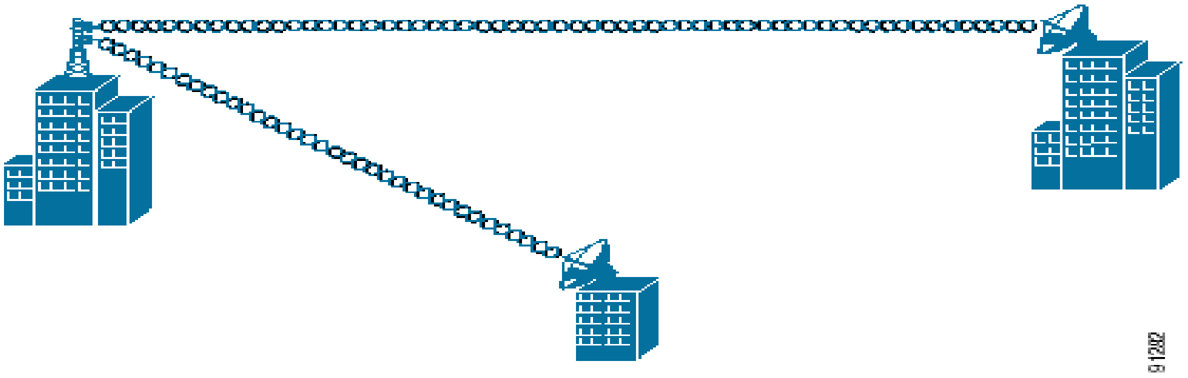
<u>Wi Fi</u> <u>Network Topologies</u>

- **AP based topology (Infrastructure mode) –** The client communicates through access point. BSA – RF coverage is provided by an AP. The ESA consists of 2 or more BSA and includes 10-15% overlap to allow roaming.

Figure 1-3 Typical WLAN



- **Peer to Peer topology –** AP is not required and client devices within a cell can communicate directly with each other. It is useful for setting up of a wireless network quickly and easily.
- **Point to Point multipoint bridge topology –** This is used to connect a LAN in one building to LANs in other buildings even if the buildings are miles apart. These conditions recieve a clear line of sight between buildings. The line of sight varies based on the type of wireless bridge and antennae used as well as the environmental conditions.



<u>Hardware</u>

Standard devices

A wireless access point (WAP) connects a group of wireless devices to an adjacent wired LAN. An access point is similar to 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.

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. Most newer laptop computers are equipped with internal adapters. Internal cards are generally more difficult to install.

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 cable modem or DSL modem. A wireless router allows all three devices (mainly the access point and router) to be configured through one central utility. This utility is most usually an integrated web server which serves web pages to wired and wireless LAN clients and often optionally to WAN clients. This utility may also be an application that is run on a desktop computer such as Apple's AirPort.

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

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

Distance Records

Distance records (using non-standard devices) include 382 km (237 mi) in June 2007, held by Ermanno Pietrosemoli and EsLaRed of Venezuela, transferring about 3 MB of data between mountain tops of El Aguila and Platillon. The Swedish Space Agency transferred data 310 km (193 mi), using 6 watt amplifiers to reach an overhead stratospheric balloon.

Embedded Systems

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

Increasingly in the last few years (particularly as of early 2007), embedded Wi-Fi modules have become available which come with a real-time operating system and provide a simple means of wireless enabling any device which has and communicates via a serial port.[12] This allows simple monitoring devices – for example, a portable ECG monitor hooked up to a patient in their home – to be created. This Wi-Fi enabled device effectively becomes part of the internet cloud and can communicate with any other node on the internet. The data collected can hop via the home's Wi-Fi access point to anywhere on the internet. [13]

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

Embedded serial-to-Wi-Fi module

Network 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 it is necessary to get past either gain access to a building, physically connecting into the internal network or break through an external firewall. With wireless it is necessary only to get reception and spend as long as you want snooping without alerting the network owner. Most business networks protect sensitive data and systems by attempting to disallow external access. Thus being able to get wireless reception (and thus possibly break the encryption) becomes an attack vector on the network as well.

Attackers who have gained access to a Wi-Fi network can use DNS spoofing attacks very effectively against any other user of the network, because they can see the DNS requests made, and often respond with a spoofed answer before the queried DNS server has a chance to reply.

Threats To The Network

1) **Eavesdropping –** Eavesdropping is an easy to perform and almost impossible to detect technique. By default, everything is transmitted in clear text usernames, passwords etc.. and no security is offered by the transmission medium. Different tools are available to cause eavesdropping, network sniffers , protocol analyzers and password collectors etc. With the right equipmemt it is possible to eavesdrop traffic from a few kilometers away.

2) **MITM attack –** Attacker spoofes a disassociate message from the victim and the victim starts to look for a new access point, and the attacker advertises his own AP on a different channel, using the real Ap's MAC address. The attacker connects to the real AP using victim's MAC address.

3) **Denial Of Service –** This is an attack on the transmission freuency used and causes frequency jamming. Attacks on MAC layer causes spoofed deauthentication/disassociation messages and can target one specific user. Attacks on higher layered protocol (TCP/IP protocol) -> SYN flooding.

4) **Piggybacking** - 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; particularly since people on average use only a fraction of their upstream bandwidth at any given time. Recreational logging and mapping of other people's access points has become known as wardriving. It is also common for people to use open (unencrypted) Wi-Fi networks as a free service, termed piggybacking. Indeed, many access points are intentionally installed without security turned on so that they can be used as a free service. These activities do not result in sanctions in most jurisdictions, however legislation and cause law differ considerably across the world. A proposal to leave graffiti describing available services was called warchalking. Piggybacking is often unintentional. Most access points are configured without encryption by default, and operating systems such as Windows XP SP2 and Mac OS X may be configured to automatically connect to any available wireless network. A user who happens to start up a laptop in the vicinity of an access point may find the computer has joined the network without any visible indication. Moreover, a user intending to join one network may instead end up on another one if the latter's signal is stronger. In combination with automatic discovery of other network resources (see DHCP 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 insecure network to login to a website, thereby making the login credentials available to anyone listening, if the website is using an insecure protocol like HTTP, rather than a secure protocol like HTTPS.

Requirements for Wi Fi security

The requirements for Wi Fi security can be broken down into two primary components -

- Authentication

  User Authentication

  Server Authentication

- Privacy

Authentication requires maintaining a record of the users that have secure access to the system and keeps unauthorized users off the network.

For User authentication an authentication server is used which asks for a password and a username whenever a user desires to login to the network.

The risk involved in this is the fact that the data (username and password) are sent before secure transmission path is established. It is also prone to passive eavesdropping by the attacker.

The solution to this problem is to establish an encrypted channel before sending username and password.

The next level of authentication is the – Server Authentication for which a digital certificate is used and validation of the digital certificate occurs automatically whithin the client software.

Security Techniques

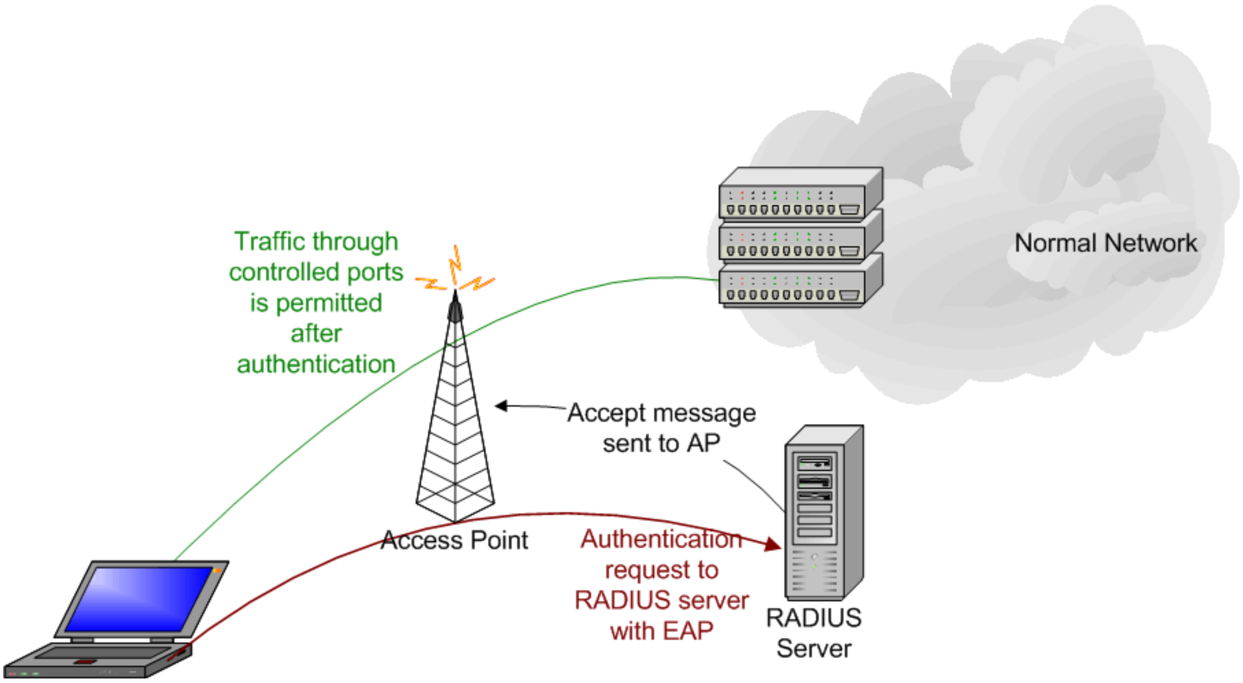
1) **Service Set Identifier** – SSID is used to identify an 802.11 network and it can be preconfigured or advertised in beacon broadcast. It is transmitted in clear text and thus provides very little security.
2) **Wired Equivalent Privacy (WEP)** - WEP was included as the privacy of the original IEEE 802.11 standard ratified in September 1999. WEP uses the stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity. It was deprecated as a wireless privacy mechanism in 2004, but for legacy purposes is still documented in the current standard. Basic WEP encryption: RC4 keystream XORed with plaintextStandard 64-bit WEP uses a 40 bit key (also known as WEP-40), which is concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key. At the time that the original WEP standard was being drafted, U.S. Government export restrictions on cryptographic technology limited the key size. Once the restrictions were lifted, all of the major manufacturers eventually implemented an extended 128-bit WEP protocol using a 104-bit key size (WEP-104). A 128-bit WEP key is almost always entered by users as a string of 26 hexadecimal (base 16) characters (0-9 and A-F). Each character represents four bits of the key. 26 digits of four bits each gives 104 bits; adding the 24-bit IV produces the final 128-bit WEP key. A 256-bit WEP system is available from some vendors, and as with the 128-bit key system, 24 bits of that is for the IV, leaving 232 actual

bits for protection. These 232 bits are typically entered as 58 hexadecimal characters. (58 × 4 = 232 bits) + 24 IV bits = 256-bit WEP key. Key size is not the only major security limitation in WEP. Cracking a longer key requires interception of more packets, but there are active attacks that simulate the necessary traffic. There are other weaknesses in WEP, including the possibility of IV collisions and altered packets,that are not helped at all by a longer key.

Two methods of authentication can be used with WEP: Open System authentication and Shared Key authentication. For the sake of clarity, we discuss WEP authentication in the Infrastructure mode (ie, between a WLAN client and an Access Point), but the discussion applies to the Ad-Hoc mode as well. In Open System authentication, the WLAN client need not provide its credentials to the Access Point during authentication. Thus, any client, regardless of its WEP keys, can authenticate itself with the Access Point and then attempt to associate. In effect, no authentication (in the true sense of the term) occurs. After the authentication and association, WEP can be used for encrypting the data frames. At this point, the client needs to have the right keys. In Shared Key authentication, WEP is used for authentication. A four-way challenge-response handshake is used.The client station sends an authentication request to the Access Point. The Access Point sends back a clear-text challenge. The client has to encrypt the challenge text using the configured WEP key, and send it back in another authentication request. The Access Point decrypts the material, and compares it with the clear-text it had sent. Depending on the success of this comparison, the Access Point sends back a positive or negative response.

3) **802.1x Access Control** – This is designated as a general purpose network access control mechanism and isn't Wi fi specific. Authentication of each client connected to an AP is done with a radius server (for Ethernet). The RADIUS server, which “tells” the access point whether access to controlled ports should be allowed or not.

- AP forces the user into an unauthorized state
- User sends an EAP start message
- AP returns and EAP message requesting the user's identity
- Identity sent by user is then forwarded to the authentication server by AP
- Authentication server authenticates user and returns an accept or reject message back to the AP
- If accept message is return, the AP changes the client's state to authorized and normal traffic flows


Traffic through controlled ports is permitted after authentication
Normal Network
Accept message sent to AP
Access Point
Authentication request to RADIUS server with EAP
RADIUS Server

4) **Wi-Fi Protected Access** (**WPA** and **WPA2**) is a certification program created by the WI FI alliance to indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks. This protocol was created in response to several serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP). The protocol implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. Specifically, theTemporal Key Integrity Protocol (TKIP), was brought into WPA. TKIP uses RC4 dynamic encryption keys and per packet key mixing function. It also uses a mesage integrity code that ensures the integrity of data being transferred.

WPA comes in two flavours

WPA-PSK

- Uses a pre shared key
- For SOHO environments
- Single master key used for all users

WPA Enterprise

- For large organizations
- Most secure method
- Unique keys for each user
- Separate username & password for each user

Data is encrypted and protection against eavesdropping and man in the middle attacks is ensured DOS attacks also cannot be used.

Advantages Of a Wireless Network

- Mobility
- Ease of installation
- Flexibility
- Cost
- Reliability
- Security
- Use unlicensed part of the radio spectrum
- Roaming
- Speed

Disadvantages Of a Wireless Network

- Interference
- Degradation in performance
- High power consumption
- Limited range