

WIRELESS FIDELITY (Wi-Fi)

Authors

Ankit goyal, 5th semester, Information Technology

College

Jaipur engineering college and research
Center (J.E.C.R.C),
Jaipur

Email address

ankit@ankitgoyal.com

2008

CONTENTS

- 1) Introduction to Wi-Fi
- 2) Wireless network
- 3) IEEE
- 4) IEEE 802.11 Standards
- 5) IEEE Standards table
- 6) Architecture of 802.11
- 7) Elements of Wi-Fi
- 8) Working of Wi-Fi
- 9) Wireless Hotspot
- 10) Applications
- 11) Advantages
- 12) Security
 - WEP
- 13) Future (WIMAX)

Wi-Fi

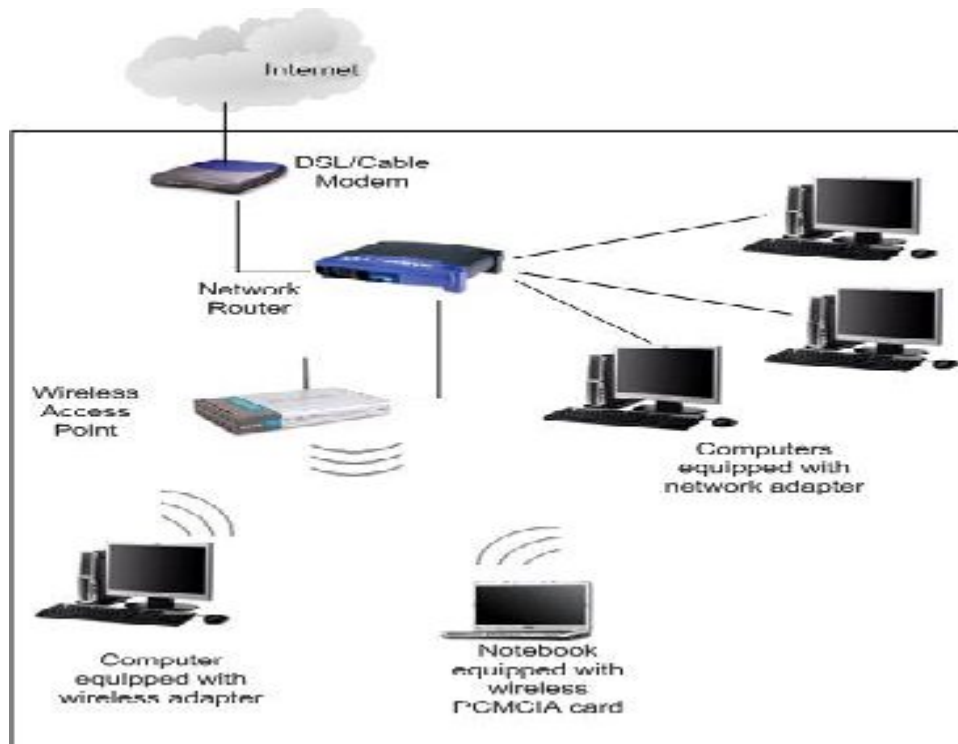
INTRODUCTION

Most people have heard of Wi-Fi (or WLAN) technology at some time or other, but not everyone is totally clear on what it is. Wi-Fi is abbreviated as “Wireless Fidelity”. It is a limited range wireless networking protocol, based on 802.11 standards. Wi-Fi connectivity allows users, to transfer digital data without wire, at the speed of broadband.

Wi-Fi is a data transmission system designed to provide location independent network, access between computing devices by using radio waves rather than cable infrastructure. It provides users, wireless access to the services of the corporate network across a building or a campus.

The Institute of Electrical and Electronics Engineers (IEEE) has ratified 802.11 specifications as a standard for WLANs. This version of 802.11 provides 1 Mbps and 2Mbps data transfer rates. Like all other 802 standards, 802.11 focuses on the bottom two levels of the OSI model, physical layer and the data link layer. Network users can access LAN almost from anywhere, without restrictions.

There are 11 channels in Wi-Fi; each channel has a slightly different frequency. Collision of the network can be avoided by using different Channels.



WIRELESS NETWORK

Wireless network is set up by using radio signal frequency to communicate among computers and other network devices. Sometimes it's also referred to as Wi-Fi network or WLAN. Wi-Fi network is getting popular, nowadays, with ease in its setting.

Both broadband cable as well as DSL modem to access internet, works with Wireless network. The two main components of Wireless network are wireless router or access point and the wireless clients. By attaching a wireless router to a cable/DSL modem, Wireless network start operating. Wireless clients can be setup by adding wireless card to each computer and if switch port is available, computers can be connected directly by cable.

If there is a wired Ethernet network at home, a wireless access point can be attached to the existing network router to have wireless access at home.

The IEEE 802.11 standards specify two operating modes:

- 1) **Infrastructure mode:** it is used to connect computers with wireless network adapters (also known as wireless clients), to an existing wired network with the help of wireless router or access point.
- 2) **Ad hoc mode:** it is used to connect wireless clients directly together, without the need for a wireless router or access point. An ad hoc network consists of up to 9 wireless clients, which send their data directly to each other.

In its simplest form, a wireless mesh network is a collection of wireless devices maintaining RF connectivity to create a seamless path for data packets to travel.

The Internet router determines a path between the user and the physical backbone. In the wireless mesh environment, a network can be envisioned as a collection of access points, routers, or end users (equipped with wireless receiver/transmitters) that are free to move arbitrarily but maintain a reliable communication that sends and receive messages. Each data packet traveling on the Internet backbone has a different sequential path of nodes even though the source and destination are the same.

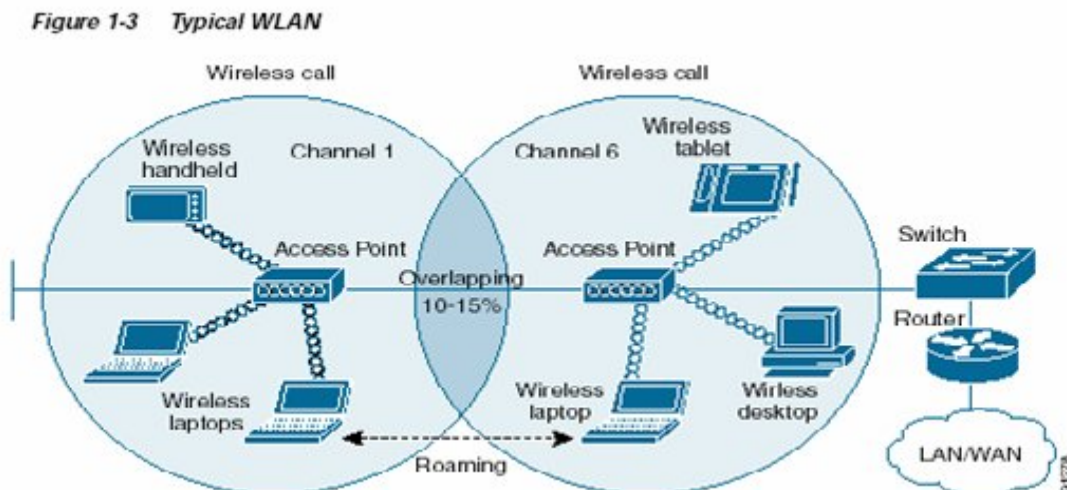
The fundamental structure of a WLAN is the peer-to-peer or peer-to-multipoint communication between two wireless devices. The purpose is forming a collection of wireless devices that maintain connectivity with each other while transferring or routing data in a random manner.

Wireless network works on two topologies:

1) In **peer-to-peer (P-to-P) configuration**, each wireless link replaces a single communication cable and can converse reliably as long as the two end points are close enough to escape the effects of Radio Frequency (RF) interference or signal loss

2) A **peer-to-multipoint (P-to-Mp) system** has one centralized administrator (or hub) that associates with multiple nodes instead of peer-to-peer collaboration. In general, a reliable connection is dependent upon the distance between the wireless devices; thus, forming a wireless circle (or cell) that one must stay within to maintain communication with others.

WLAN can reach a radius of 500 feet indoors and 1000 feet outdoors, but antennas, transmitters and other access devices can be used to widen that area. WLANs require a wired access point that plugs all the wireless devices into the wired network.



INSTITUTE OF ELECTRICAL AND ELECTRONICS
ENGINEERING
(IEEE)

Wi-Fi refers to any system that uses the 802.11 standard, which was developed by the Institute of Electrical and Electronics Engineers (IEEE) and released in 1997. The term Wi-Fi, which is alternatively spelled WiFi, Wi-fi, or wifi, was pushed by the Wi-Fi Alliance, a trade group that pioneered commercialization of the technology.

IEEE is one of the leading standards-making organizations in the world. IEEE performs its standards making and maintaining functions through the IEEE Standards Association (IEEE-SA).

One of the more notable IEEE standards is the IEEE 802 LAN/MAN group of standards which includes the IEEE 802.3 Ethernet standard and the IEEE 802.11 Wireless Networking standard.

The IEEE standards development process can be broken down into seven basic steps, as follows:

- 1) ***Securing Sponsorship***: An IEEE-approved organization must sponsor a standard. A sponsoring organization is in charge of coordinating and supervising the standard development from inception to completion. The professional societies within IEEE serve as the natural sponsor for many standards.
- 2) ***Requesting Project Authorization***: To gain authorization for the standard a Project Authorization Request (PAR) is submitted to the IEEE-SA Standards Board. The New Standards Committee (NesCom) of the IEEE-SA Standards Board reviews the PAR and makes a recommendation to the Standards Board about whether to approve the PAR.
- 3) ***Assembling a Working Group***: After the PAR is approved, a "working group" of individuals affected by, or interested in, the standard is organized to develop the standard. IEEE-SA rules ensure that all Working Group meetings are open and that anyone has the right to attend and contribute to the meetings
- 4) ***Drafting the Standard***: The Working Group prepares a draft of the proposed standard. Generally, the draft follows the IEEE Standards Style Manual that sets "guidelines" for the clauses and format of the standards document.

5) **Balloting**: Once a draft of the standard is finalized in the Working Group, the draft is submitted for Balloting approval. The IEEE Standards Department sends an invitation-to-ballot to any individual who has expressed an interest in the subject matter of the standard.

Anyone who responds positively to the invitation-to-ballot becomes a member of the balloting group, as long as the individual is an IEEE member or has paid a balloting fee. The IEEE requires that a proposed draft of the standard receive a response rate of 75% (i.e., at least 75% of potential ballots are returned) and that, of the responding ballots, at least 75% approve the proposed draft of the standard. If the standard is not approved, the process returns to the drafting of the standard step in order to modify the standard document to gain approval of the balloting group.

6) **Review Committee**: After getting 75% approval, the draft standard, along with the balloting comments, are submitted to the IEEE-SA Standards Board Review Committee (RevCom). The RevCom reviews the proposed draft of the standard against the IEEE-SA Standards Board Bylaws and the stipulations set forth in the IEEE-SA Standards Board Operations Manual. The RevCom then makes a recommendation about whether to approve the submitted draft of the standard document.

7) **Final Vote**: Each member of the IEEE-SA Standards Board places a final vote on the submitted standard document. It takes a majority vote of the Standards Board to gain final approval of the standard. In general, if the RevCom recommends approval, the Standards Board will vote to approve the standard.

IEEE 802 Standards	
802.1	Bridging & Management
802.2	Logical Link Control
802.3	Ethernet - CSMA/CD Access Method
802.4	Token Passing Bus Access Method
802.5	Token Ring Access Method
802.6	Distributed Queue Dual Bus Access Method
802.7	Broadband LAN
802.8	Fiber Optic
802.9	Integrated Services LAN
802.10	Security
802.11	Wireless LAN
802.12	Demand Priority Access
802.14	Medium Access Control
802.15	Wireless Personal Area Networks
802.16	Broadband Wireless Metro Area Networks
802.17	Resilient Packet Ring

IEEE 802.11 STANDARDS **(WIRELESS LAN)**

IEEE 802.11 is a set of standards for wireless local area network (WLAN) computer communication, developed by the IEEE LAN/MAN Standards Committee (IEEE 802) in the 5 GHz and 2.4 GHz public spectrum bands.

Although the terms 802.11 and Wi-Fi are often used interchangeably, the Wi-Fi Alliance uses the term "Wi-Fi" to define a slightly different set of overlapping standards. In some cases, market demand has led the Wi-Fi Alliance to begin certifying products before amendments to the 802.11 standard are complete.

The 802.11 family includes over-the-air modulation techniques that use the same basic protocol. The most popular are those defined by the 802.11b and 802.11g protocols, and are amendments to the original standard. 802.11a was the first wireless networking standard, but 802.11b was the first widely accepted one, followed by 802.11g and 802.11n.

IEEE 802.11 (legacy mode): The original version of the standard IEEE 802.11, released in 1997 and clarified in 1999, specified two raw data rates of 1 and 2 megabits per second (Mbit/s) to be transmitted in Industrial Scientific Medical frequency band at 2.4 GHz. Legacy 802.11 was rapidly supplemented (and popularized) by 802.11b.

IEEE 802.11a: The 802.11a standard uses the same core protocol as the original standard, operates in 5 GHz band with a maximum raw data rate of 54 Mbit/s, which yields realistic net achievable throughput in the mid-20 Mbit/s. 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 slight disadvantage: The effective overall range of 802.11a is slightly less than that of 802.11b/g; 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.

IEEE 802.11b: 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.

IEEE 802.11g: This works in the 2.4 GHz band (like 802.11b) but operates at a maximum raw data rate of 54 Mbit/s, or about 19 Mbit/s net throughputs. 802.11g hardware is fully backwards compatible with 802.11b hardware.

The then-proposed 802.11g standard was rapidly adopted by consumers starting in January 2003, well before ratification, due to the desire for higher speeds, 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 by a 802.11b participant will reduce the speed of the overall 802.11g network.

Like 802.11b, 802.11g 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.

IEEE 802.11n: 802.11n is a proposed amendment which improves upon the previous 802.11 standards by adding multiple-input multiple-output (MIMO) and many other newer features. Though there are already many products on the market based on Draft 2.0 of this proposal, the TGn workgroup is not expected to finalize the amendment until November 2008

802.11 STANDARDS TABLE

- IEEE 802.11a** - 54 Mbit/s, 5 GHz standard
- IEEE 802.11b** - Enhancements to 802.11 to support 5.5 and 11 Mbit/s
- IEEE 802.11c** - Bridge operation procedures; included in the IEEE 802.1D standard
- IEEE 802.11d** - International (country-to-country) roaming extensions (2001)
- IEEE 802.11e** - Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11F** - Inter-Access Point Protocol (2003) Withdrawn February 2006
- IEEE 802.11g** - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h** - Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i** - Enhanced security (2004)
- IEEE 802.11j** - Extensions for Japan (2004)
- IEEE 802.11-2007** - A new release of the standard that includes amendments a, b, d, e, g, h, i & j. (July 2007)
- IEEE 802.11k** - Radio resource measurement enhancements (proposed - 2007?)
- IEEE 802.11l** - (reserved and will not be used)
- IEEE 802.11m** - Maintenance of the standard. Recent edits became 802.11-2007. (Ongoing)
- IEEE 802.11n** - Higher throughput improvements using MIMO (multiple input, multiple output antennas) (September 2008)
- IEEE 802.11o** - (reserved and will not be used)
- IEEE 802.11p** - WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (working - 2009?)
- IEEE 802.11q** - (reserved and will not be used, can be confused with 802.1Q VLAN trunking)
- IEEE 802.11r** - Fast roaming Working "Task Group r" - 2007?
- IEEE 802.11s** - ESS Extended Service Set Mesh Networking (working - 2008?)
- IEEE 802.11t** - Wireless Performance Prediction (WPP) - test methods and metrics Recommendation (working - 2008?)
- IEEE 802.11u** - Networking with non-802 networks (for example, cellular) (proposal evaluation - ?)

IEEE 802.11v - Wireless network management (early proposal stages - ?)

IEEE 802.11w - Protected Management Frames (early proposal stages - 2008?)

IEEE 802.11x - (reserved and will not be used, can be confused with 802.1x Network Access Control)

IEEE 802.11y - 3650-3700 MHz Operation in the U.S. (March 2008?)

IEEE 802.11z - Extensions to Direct Link Setup (DLS) (Aug. 2007 - Dec. 2011)

IEEE 802.16- (like WiMax)

	802.11a	802.11b	802.11g	802.11n
Standard approved by IEEE	January 2000	December 1999	June 2003	Expected in 2007
Maximum data rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Different data rate configurations	8	4	12	576
Typical range	75 feet	100 feet	150 feet	150 feet
Modulation technologies (1)	OFDM	DSSS, CCK	DSSS, CCK, OFDM	DSSS, CCK, OFDM+
RF band	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz and 5 GHz
Number of spatial streams and antennas	1	1	1	Up to 4
Channel width	20 MHz	20 MHz	20 MHz	20 MHz or 40 MHz
Number of channels	23	3	3	26

IEEE 802.11 ARCHITECTURE

Each computer, mobile, portable or fixed, is referred to as a station in 802.11. When two or more stations come together to communicate with each other, they form a basic service set (BSS). A BSS that stands alone and is not connected to a base is called an Independent Basic Service Set (IBSS) or is referred to as an Ad-hoc network. An Ad-hoc network is a network where stations communicate only peer-to-peer. There is no base and no one gives permission to talk. Two or more BSS's are interconnected using a Distribution system or DS. This concept of DS increases network coverage. Each BSS becomes a component of an extended, large network. Entry to the DS is accomplished with the use of Access Point (AP). An access point is a station, thus addressable. So, data moves between the BSS and the DS with the help of these access points.

Creating large and complex network using BSS and DS leads us to the next level of hierarchy, the Extended Service Sets or ESS. The beauty of the ESS is the entire network looks like an independent basic service set to the Logical Link Control Layer (LLC). This means that station within the ESS can communicate or even move between BSS transparently to the LLC.

One of the requirements of IEEE 802.11 is that it can be used with existing wired networks. 802.11 solved this challenge with the use of a Portal. A portal is the logical integration between wired LANs and 802.11.

The implementation of the DS is not specified by 802.11. A point to point bridge connecting LANs in two separate buildings could become a DS. While the implementation for the DS is not specified, 802.11 do not specify the services, which the DS must support.

Services are divided into two sections:

- 1) Station Services(SS)
- 2) Distribution System Services(DSS)

There are five services provided the DSS

- 1) Association
- 2) Reassociation
- 3) Disassociation
- 4) Distribution
- 5) Integration

The first three services deal with station mobility. If a station is moving within its own BSS or is not moving, the station mobility is termed No-transition. If a station moves between BSS's within the same ESS, its mobility is termed BSS-transition. If the station moves between BSS's of different ESS's it is ESS transition. A station must affiliate itself with the BSS infrastructure if it wants to use the LAN. This is done by associating itself with an access point.

Association supports no-transition mobility but is not enough to support BSS-transition. Enter Reassociation. This service allows the station to switch its association from one AP to another. Both association and reassociation are initiated by the station. Dissociation is when the association between the station and the AP is terminated.

Distribution and integration are the remaining DSS's. Distribution is simple getting the data from the sender to the intended receiver. The message is sent to the local AP (output AP) that the recipient is associated with.

Station services are:

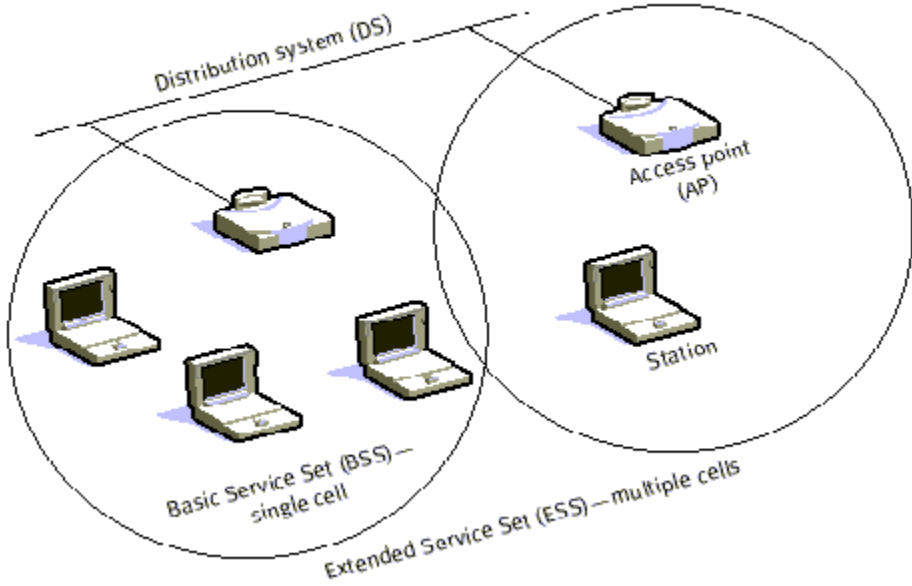
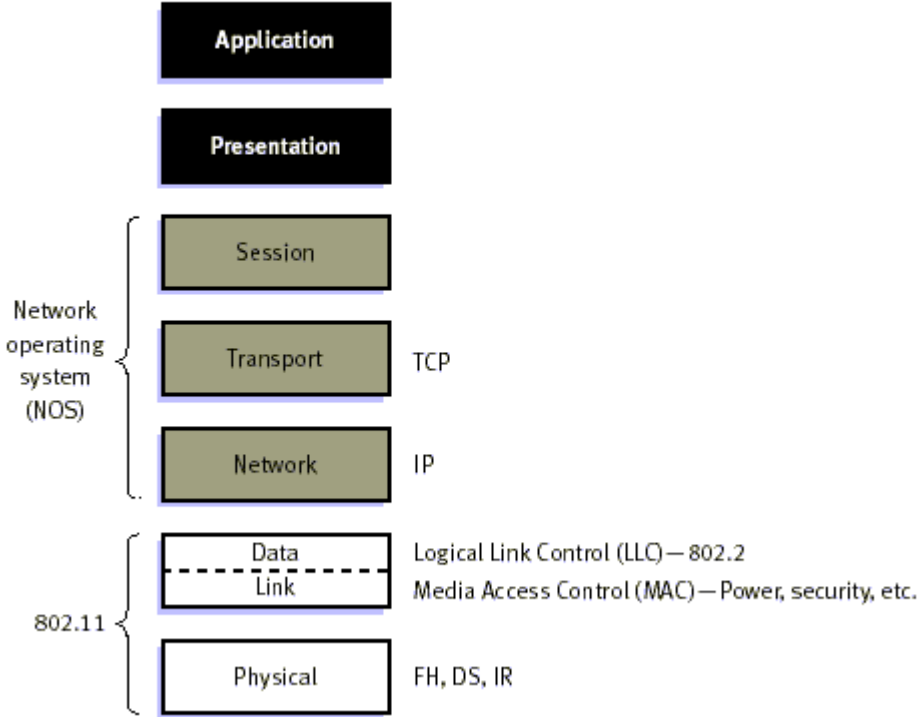
- 1) Authentication
- 2) Deauthentication
- 3) Privacy
- 4) MAC Service Data Unit (MSDU) Delivery

In order to control access to the network, station must first establish their identity. Before you are acknowledge and allowed to converse, you must first pass a series of tests to ensure that you are who you say you are. That is really all authentication is.

There are two types of authentication services offered by 802.11.

The first is Open System Authentication. This means that anyone who attempt to authenticate will receive authentication. The second type is Shared Key Authentication. In order to become authenticated the user must be in possession of a shared secret. The shared secret is implemented with the use of the Wired Equivalent Privacy (WEP) privacy algorithm. The shared secret is delivered to all station ahead of time in some secure method. Deauthentication is when either the station or AP wishes to terminates a stations authentication. When this happens the station is automatically disassociation. Privacy is an encryption algorithm, which is used so that other 802.11 users cannot eavesdrop on your LAN traffic. IEEE 802.11 specifies Wired Equivalent Privacy (WEP) as an optional algorithm to satisfy privacy.

MSDU delivery ensures that the information in the MAC service data unit is delivered between the medium access control service access points.

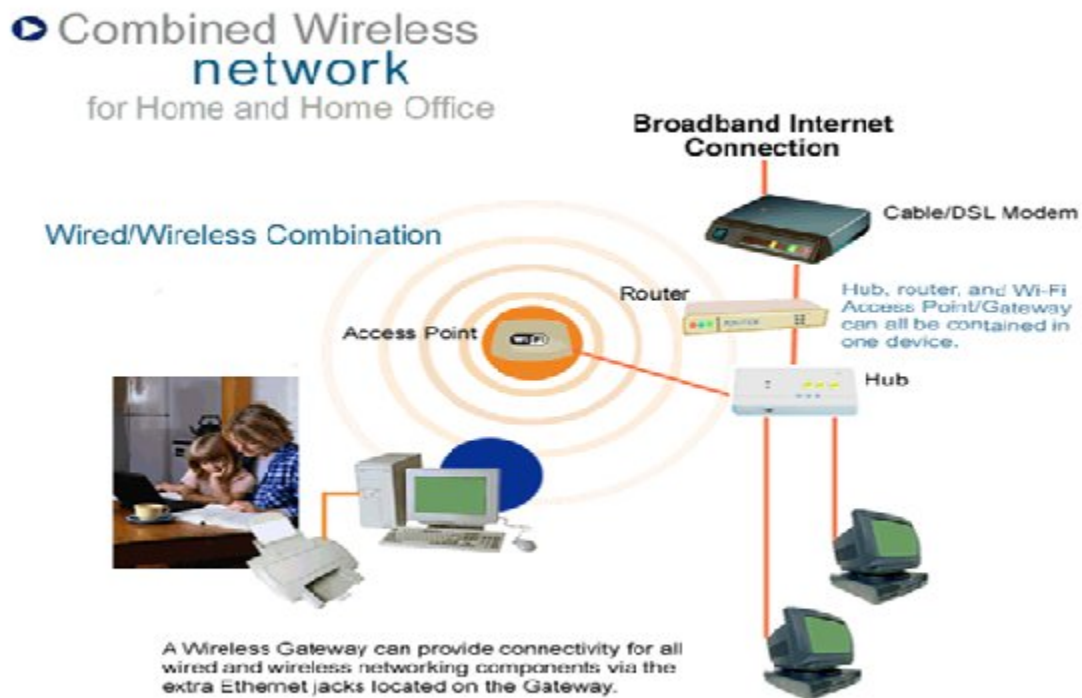


ELEMENT OF WIFI

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 (e.g. PCMCIA Card for Laptop and PCI Card for Desktop PC)

Safeguards - Firewalls and anti-virus software protect networks from uninvited users and keep information secure.



WORKING OF WI-FI

Wireless router receives the signal and decodes it. It sends the information to the Internet using a physical, wired Ethernet connection.

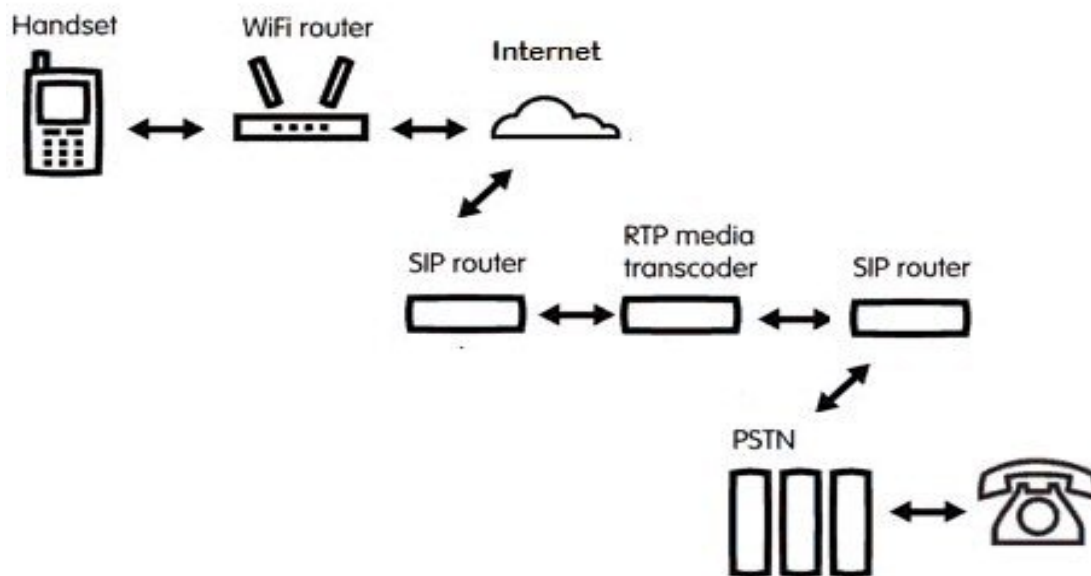
In a Wi-Fi network, computers with Wi-Fi network cards connect wirelessly to a wireless router

Radio waves are electromagnetic waves, just like the light we see. Radio waves can transmit information in a sine wave, which can hold more information more accurately.

Once radio waves are in the air on a particular frequency, a tuner in range must then pick them up and convert the sine wave back into usable information. Tuners work based on another physics principle known as Resonance. In a radio, the tuner resonates at a particular frequency it's tuned to, so only those waves will be amplified. The net result is that waves of a set frequency are picked out of the air and amplified far above the strength of the other waves. Thus, tuners select which radio wave to tune.

After the signal is picked out from among all the radio noise in the air, another component called a demodulator subtracts the carrier signal from the radio wave to obtain the original signal.

Wi-Fi works by radio transmission, usually in the unlicensed 2.4 GHz ISM Band. Wi-Fi transmission is essentially FM transmission, in that the frequency is changed to transmit data. E.g. 2.4 GHz Wi-Fi uses something called complementary code keying to vary frequency and send data.

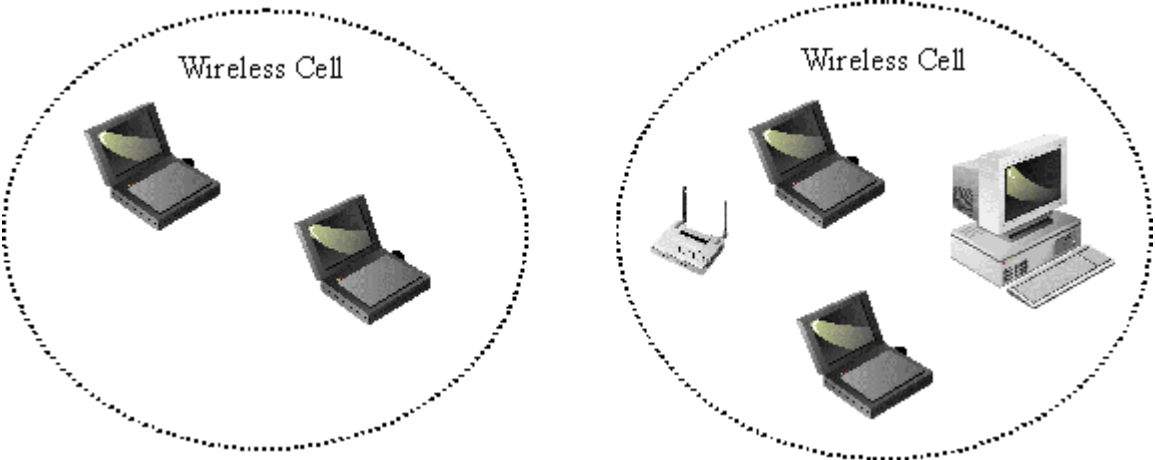


WIRELESS HOTSPOT

Wi-Fi networks can either be "open", such that anyone can use them, or "closed", in which case a password is needed. An area blanketed in wireless access is often called a **WIRELESS HOTSPOT**.

A hotspot is a venue that offers Wi-Fi access. The public can use a laptop, WiFi phone, or other suitable portable device to access the Internet. Of the estimated 150 million laptops, 14 million PDAs, and other emerging Wi-Fi devices sold per year for the last few years, most include the Wi-Fi feature.

For venues that have broadband service, offering wireless access is as simple as purchasing one AP and connecting the AP with the gateway box. Hotspots are often found at restaurants, train stations, airports, libraries, hotels, hospitals, coffee shops, bookstores, fuel stations, department stores, supermarkets and other public places. Many universities and schools have wireless networks in their campus.



SECURITY

1) *Concealment of the SSID:*

Wireless access points designed to IEEE 802.11 standards have the options to broadcast 'beacon' packets. These may be read by any 802.11 compliant devices and contain the include information such as the Service Set Identifier (SSID) of the AP (an identifier used to differentiate between wireless access points) and the data rates supported by the AP. One security measure offered by WLAN is concealment. This can be achieved when access points turn off their beacon. Without the information in the beacon packets, specifically the SSID, a host cannot join a WLAN. This is because they will not be able to easily detect that the network exists. This is often referred to as a closed network.

2) *Authentication and Association:*

The main mechanism for WLAN is the authentication and association process. This mechanism denies access to hosts who fail to procedure by ignoring packets sent from them (apart than further authentication/association packets). The standard stipulates that association should be performed straight after a host has been authenticated.

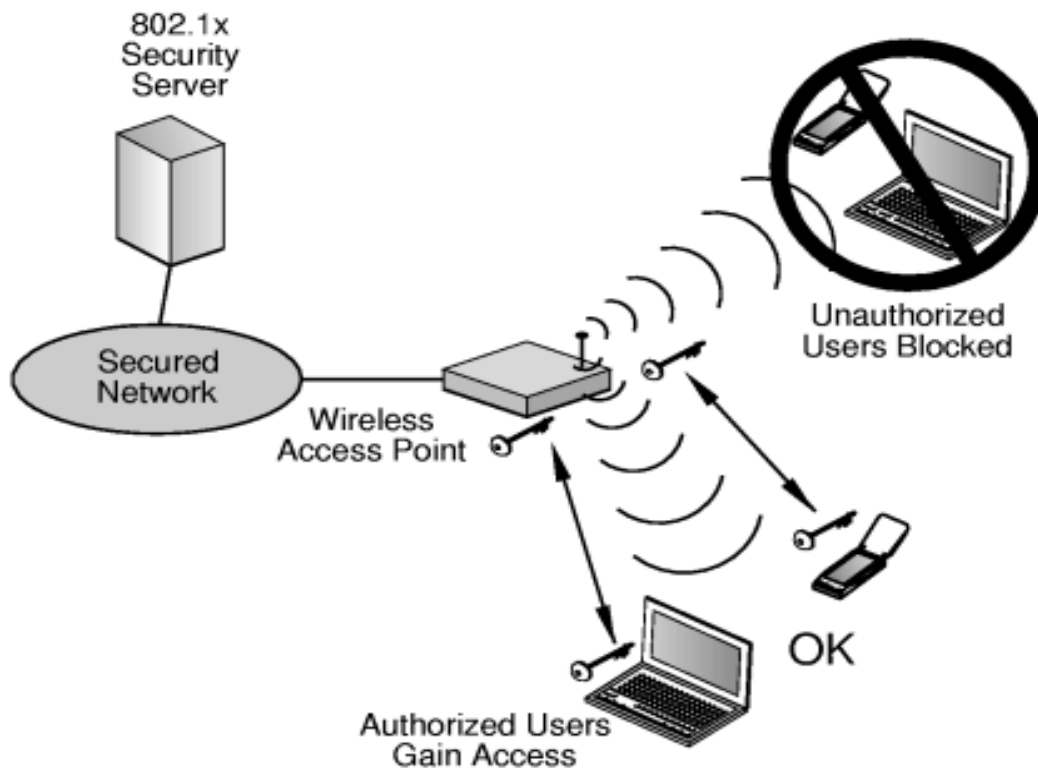
Authentication is the process of determining whether a particular host is authorized to connect to network. Two authentication methods are available:

- ***Open system authentication*** - Any host that requires authentication is granted access.
- ***Shared key authentication*** - Uses a challenge-response mechanism to test initiators knowledge of the networks shared-secret WEP key.
 1. The initiator sends a packets requesting authentication and receives a response containing a piece of fixed-length, randomly generated challenge text.
 2. The initiator must encode this challenge text using the WEP algorithm and WEP key
 3. If this, when deciphered by the responder, matches the challenge text initially sent then the responder transmits a success message. This process is then repeated with the initiator as the responder and vice-versa to provide mutual authentication. Association is the process of establishing a connection between a host device and (usually) an AP. Association is performed by an authentication host and as follows:

- The host sends an association request message, containing the SSID and data rates it can support, among other information.
- This provokes an association response from the AP. The association will fail if the AP does not provide the SSID requested. However, if the association was successfully, an association ID and certain other information will be provided.
- Once successfully associated, an host can exchange message with the AP.

3) *Access Control Lists:*

Access control, although not actually part of the 802.11 standard, has become a common security technique used in WLAN. This works when an administration provides the AP with a list of MAC addresses, known as the access control list. This list states which addresses are allowed or denied access.



WEP (WIRED EQUIVALENT PROTOCOL)

Perhaps the most commonly known and most effective security measure available in 802.11 is WEP (Wired Equivalent Protocol). This protocol is designed to enforce similar security levels for wireless networks as for their wired equivalents. The protocol works by using a reversible stream cipher, based on a shared-secret key known as the WEP key, to encrypt the body of 'private' messages. By using WEP, it is expected that eavesdropping will be effectively prevented, as any intercepted packets will be effectively prevented, as any intercepted packets will contain only encrypted information.

Security is one of the first concerns of people deploying a Wireless LAN, the 802.11 committee has addressed the issue by providing what is called WEP (Wired Equivalent Privacy).

The main concerns of users are that an intruder would not be able to:

- Access the Network resources by using similar Wireless LAN equipment, and
- Be able to capture the Wireless LAN traffic (eavesdropping)

Preventing Access to Network Resources:

This is done by the use of an Authentication mechanism where a station needs to prove knowledge of the current key; this is very similar to the Wired LAN privacy, on the sense that an intruder needs to enter the premises (by using a physical key) in order to connect his workstation to the wired LAN.

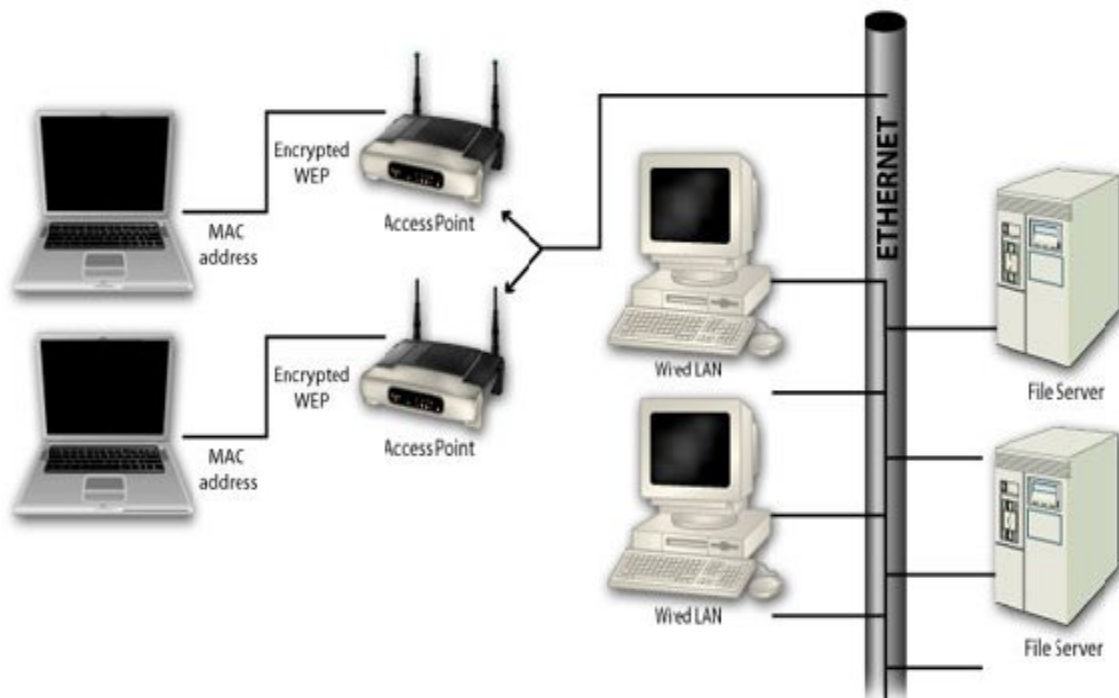
Eavesdropping:

Eavesdropping is prevented by the use of the WEP algorithm, which is a Pseudo Random Number Generator (PRNG), initialized by a shared secret key. This PRNG outputs a key sequence of pseudo-random bits equal in length to the largest possible packet, which is combined with the outgoing/incoming packet producing the packet transmitted in the air.

The WEP algorithm is a simple algorithm, which has the following properties:

Reasonable strong: Brute-force attack to this algorithm is difficult because of the fact that every frame is sent with an Initialization Vector, which restarts the PRNG for each frame.

Self Synchronizing: The algorithm synchronized again for each message, this is needed in order to work on a connectionless environment, where packets may get lost (as any LAN).



APPLICATIONS OF WI-FI

Common applications for Wi-Fi include Internet, VoIP phone access, and gaming, network connectivity for consumer electronics such as televisions, DVD players, and digital cameras.

Advantages of wireless include mobility and elimination of unsightly cables

Wireless networks are easy to find. Any user within 200 feet or so (about 61 meters) of the access point can then connect to the Internet, though for good transfer rates, distances of 100 feet (30.5 meters) or less are more common. Boosters that extend the range of a wireless are also available.

The freedom to roam offers numerous user benefits for a variety of work environments, such as:

- 1) Immediate bedside access to patient information for doctors and hospital staff
- 2) Easy, real-time network access for on-site consultants or auditors
Improved database access for roving supervisors such as production line managers, warehouse auditors, or construction engineers
- 3) Simplified network configuration with minimal MIS involvement for temporary setups such as trade shows or conference rooms
- 4) Faster access to customer information for service vendors and retailers, resulting in better service and improved customer satisfaction
Location-independent access for network administrators, for easier on-site troubleshooting and support
- 5) Real-time access to study group meetings and research links for students

ADVANTAGES OF WI-FI

- 1) Wi-Fi allows LAN to be deployed without cabling for client devices, typically reducing the costs of network development deployment and expansion.
- 2) Spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless LANs.
- 3) The price of chipsets for Wi-Fi continues to drop, making it an economical networking option included in ever more devices.
- 4) Products designed as “Wi-Fi certified” by the Wi-Fi Alliance are backwards interoperable. Wi-Fi is a global set of standards. Unlike mobile telephones, any standard Wi-Fi devices will work anywhere in the world.
- 5) New protocols for Quality of service (WMM) make Wi-Fi more suitable for latency- sensitive applications (such as voice and video), and power saving mechanisms (WMM Power Save) improve battery operation.
- 6) Because of the comfortable and quick installation people often replace bold wired LANs with Wi-Fi. Such connection allows moving your machine around the place without losing the Internet or other network resources.
- 7) However, building Wi-Fi network is often the cheapest way to achieve the desired connection with the surroundings. The price of a single wireless adapter is decreasing almost every day, so making a large network area by means of Wi-Fi is the most reasonable way.
- 8) **Quick, easy setup:** setting up a wireless network may sound like a daunting task, but it's actually a pretty straightforward process. Wi-Fi networks don't require professional installation, and, best of all, there are no holes to drill or wires to run through walls
- 9) **Fast data transfer rates:** With transfer speeds up to 54 megabits (Mb) per second (6.75 megabytes), 802.11g is currently the fastest commercially available Wi-Fi protocol on the market.

FUTURE

WiMax (Worldwide Interoperability for Microwave Access) is a wireless broadband technology, which supports point to multi-point (PMP) broadband wireless access.

WiMax is basically a new shorthand term for IEEE Standard 802.16, which was designed to support the European standards. 802.16's predecessors (like 802.11a) were not very accommodative of the European standards, per se. The IEEE wireless standard has a range of up to 30 miles, and can deliver broadband at around 75 megabits per second. This is theoretically, 20 times faster than a commercially available wireless broadband.

The 802.16, WiMax standard was published in March 2002 and provided updated information on the Metropolitan Area Network (MAN) technology. The extension given in the March publication, extended the line-of-sight fixed wireless MAN standard, focused solely on a spectrum from 10 GHz to 60+ GHz.

This extension provides for non-line of sight access in low frequency bands like 2 - 11 GHz. These bands are sometimes unlicensed. This also boosts the maximum distance from 31 to 50 miles and supports PMP (point to multipoint) and mesh technologies.

The IEEE approved the 802.16 standards in June 2004, and three working groups were formed to evaluate and rate the standards.

WiMax can be used for wireless networking like the popular Wi-Fi. WiMax, a second-generation protocol, allows higher data rates over longer distances, efficient use of bandwidth, and avoids interference almost to a minimum.

Wi-Max can be termed partially a successor to the Wi-Fi protocol, which is measured in feet, and works, over shorter distances.