What is Wi-Fi ?

WiFi stands for **Wi**reless **Fi**delity. WiFiIt is based on the IEEE 802.11 family of standards and is primarily a local area networking (LAN) technology designed to provide in-building broadband coverage.

Current WiFi systems support a peak physical-layer data rate of 54 Mbps and typically provide indoor coverage over a distance of 100 feet.

WiFi has become the *de facto* standard for *last mile* broadband connectivity in homes, offices, and public hotspot locations. Systems can typically provide a coverage range of only about 1,000 feet from the access point.

WiFi offers remarkably higher peak data rates than do 3G systems, primarily since it operates over a larger 20 MHz bandwidth, but WiFiWiFi systems are not designed to support high-speed mobility.

One significant advantage of WiFi over WiMAX and 3G is its wide availability of terminal devices. A vast majority of laptops shipped today have a built-in WiFi interface. WiFi interfaces are now also being built into a variety of devices, including personal data assistants (PDAs), cordless phones, cellular phones, cameras, and media players.

WiFi is Half Duplex

All WiFi networks are contention-based TDD systems, where the access point and the mobile stations all vie for use of the same channel. Because of the shared media operation, all WiFi networks are half duplex.

There are equipment vendors who market WiFi mesh configurations, but those implementations incorporate technologies that are not defined in the standards.

Channel Bandwidth

The WiFi standards define a fixed channel bandwidth of 25 MHz for 802.11b and 20 MHz for either 802.11a or g networks.

Wi-Fi - Working Concepts

Radio Signals

Radio Signals are the keys, which make WiFi networking possible. These radio signals transmitted from WiFi antennas are picked up by WiFi receivers, such as computers and cell phones that are equipped with WiFi cards. Whenever, a computer receives any of the signals within the range of a WiFi network, which is usually 300 — 500 feet for antennas, the WiFi card reads the signals and thus creates an internet connection between the user and the network without the use of a cord.

Access points, consisting of antennas and routers, are the main source that transmit and receive radio waves. Antennas work stronger and have a longer radio transmission with a radius of 300-500 feet, which are used in public areas while the weaker yet effective router is more suitable for homes with a radio transmission of 100-150 feet.

WiFi Cards

You can think of WiFi cards as being invisible cords that connect your computer to the antenna for a direct connection to the internet.

WiFi cards can be **external** or **internal**. If a WiFi card is not installed in your computer, then you may purchase a USB antenna attachment and have it externally connect to your USB port, or have an antenna-equipped expansion card installed directly to the computer (as shown in the figure given above). For laptops, this card will be a PCMCIA card which you insert to the PCMCIA slot on the laptop.

WiFi Hotspots

A WiFi hotspot is created by installing an access point to an internet connection. The access point transmits a wireless signal over a short distance. It typically covers around 300 feet. When a WiFi enabled device such as a Pocket PC encounters a hotspot, the device can then connect to that network wirelessly.

Most hotspots are located in places that are readily accessible to the public such as airports, coffee shops, hotels, book stores, and campus environments. 802.11b is the most common specification for hotspots worldwide. The 802.11g standard is

backwards compatible with .11b but .11a uses a different frequency range and requires separate hardware such as an a, a/g, or a/b/g adapter. The largest public WiFi networks are provided by private internet service providers (ISPs); they charge a fee to the users who want to access the internet.

Hotspots are increasingly developing around the world. In fact, T-Mobile USA controls more than 4,100 hotspots located in public locations such as Starbucks, Borders, Kinko's, and the airline clubs of Delta, United, and US Airways. Even select McDonald's restaurants now feature WiFi hotspot access.

Any notebook computer with integrated wireless, a wireless adapter attached to the motherboard by the manufacturer, or a wireless adapter such as a PCMCIA card can access a wireless network. Furthermore, all Pocket PCs or Palm units with Compact Flash, SD I/O support, or built-in WiFi, can access hotspots.

Some Hotspots require WEP key to connect, which is considered as private and secure. As for open connections, anyone with a WiFi card can have access to that hotspot. So in order to have internet access under WEP, the user must input the WEP key code.

Wi-Fi - IEEE Standards

The 802.11 standard is defined through several specifications of WLANs. It defines an over-the-air interface between a wireless client and a base station or between two wireless clients.

There are several specifications in the 802.11 family –

- **802.11** – This pertains to wireless LANs and provides 1 - or 2-Mbps transmission in the 2.4-GHz band using either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS).
- **802.11a** – This is an extension to 802.11 that pertains to wireless LANs and goes as fast as 54 Mbps in the 5-GHz band. 802.11a employs the orthogonal frequency division multiplexing (OFDM) encoding scheme as opposed to either FHSS or DSSS.
- **802.11b** – The 802.11 high rate WiFi is an extension to 802.11 that pertains to wireless LANs and yields a connection as fast as 11 Mbps transmission (with a fallback to 5.5, 2, and 1 Mbps depending on strength of signal) in the 2.4-GHz band. The 802.11b specification uses only DSSS. Note that 802.11b was actually an amendment to the original 802.11 standard added in 1999 to permit wireless functionality to be analogous to hard-wired Ethernet connections.
- **802.11g** – This pertains to wireless LANs and provides 20+ Mbps in the 2.4-GHz band.

Here is the technical comparison between the three major WiFi standards.

Feature	WiFi (802.11b)	WiFi (802.11a/g)
PrimaryApplication	Wireless LAN	Wireless LAN
Frequency Band	2.4 GHz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)
Channel Bandwidth	25 MHz	20 MHz
Half/Full Duplex	Half	Half
Radio Technology	Direct Sequence Spread Spectrum	OFDM (64-channels)

Bandwidth	<=0.44 bps/Hz	≤=2.7 bps/Hz
Efficiency		
Modulation	QPSK	BPSK, QPSK, 16-, 64-QAM
FEC	None	Convolutional Code
Encryption	Optional- RC4m (AES in 802.11i)	Optional- RC4(AES in 802.11i)
Mobility	In development	In development
Mesh	Vendor Proprietary	Vendor Proprietary
Access Protocol	CSMA/CA	CSMA/CA

Wi-Fi - Access Protocols

IEEE 802.11 wireless LANs use a media access control protocol called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). While the name is similar to Ethernet's Carrier Sense Multiple Access with Collision Detection (CSMA/CD), the operating concept is totally different.

WiFi systems are the half duplex shared media configurations, where all stations transmit and receive on the same radio channel. The fundamental problem of a radio system is that a station cannot *hear* while it is sending, and hence it is impossible to detect a collision. Because of this, the developers of the 802.11 specifications came up with a collision avoidance mechanism called the **Distributed Control Function** (DCF).

According to DCF, a WiFi station will transmit only when the channel is clear. All transmissions are acknowledged, so if a station does not receive an acknowledgement, it assumes a collision occurred and retries after a random waiting interval.

The incidence of collisions will increase as the traffic increases or in situations where mobile stations cannot hear each other.

Wi-Fi - Quality of Service (QoS)

There are plans to incorporate quality of service (QoS) capabilities in WiFi technology with the adoption of the IEEE 802.11e standard. The 802.11e standard will include two operating modes, either of which can be used to improve service for voice −

- WiFi Multimedia Extensions (WME) − Mandatory
- WiFi Scheduled Multimedia (WSM) − Optional

WiFi Multimedia Extensions (WME)

WiFi Multimedia Extensions use a protocol called Enhanced Multimedia Distributed Control Access (EDCA), which is an extension of an enhanced version of the Distributed Control Function (DCF) defined in the original 802.11 MAC.

The *enhanced* part is that EDCA will define eight levels of access priority to the shared wireless channel. Like the original DCF, the EDCA access is a contention-based protocol that employs a set of waiting intervals and back-off timers designed to avoid collisions. However, with DCF all stations use the same values and hence have the same priority for transmitting on the channel.

With EDCA, each of the different access priorities is assigned a different range of waiting intervals and back-off counters. Transmissions with higher access priority are assigned shorter intervals. The standard also includes a packet-bursting mode that allows an access point or a mobile station to reserve the channel and send 3- to 5-packets in a sequence.

WiFi Scheduled Multimedia (WSM)

True consistent delay services can be provided with the optional WiFi Scheduled Multimedia (WSM). WSM operates like the little used Point Control Function (PCF) defined with the original 802.11 MAC.

In WSM, the access point periodically broadcasts a control message that forces all stations to treat the channel as busy and not attempt to transmit. During that period, the access point polls each station that is defined for time sensitive service.

To use the WSM option, devices need to send a traffic profile describing bandwidth, latency, and jitter requirements. If the access point does not have sufficient resources to meet the traffic profile, it will return a *busy signal*.

Wi-Fi - Security

Security has been one of the major deficiencies in WiFi, though better encryption systems are now becoming available. Encryption is optional in WiFi, and three different techniques have been defined. These techniques are given here −

Wired Equivalent Privacy (WEP)

An RC4-based 40-or 104-bit encryption with a static key.

WiFi Protected Access (WPA)

This is a new standard from the WiFi Alliance that uses the 40 or 104-bit WEP key, but it changes the key on each packet. That changing key functionality is called the Temporal Key Integrity Protocol (TKIP).

IEEE 802.11i/WPA2

The IEEE is finalized the 802.11i standard, which is based on a far more robust encryption technique called the Advanced Encryption Standard. The WiFi Alliance designate products that comply with the 802.11i standard as WPA2.

However, implementing 802.11i requires a hardware upgrade.

Wi-Fi - Network Services

The picture has become somewhat confused as service providers started using WiFi to deliver services for which it was not originally designed. The two major examples of this are wireless ISPs and city-wide WiFi mesh networks.

Wireless ISPs (WISPs)

One business that grew out of WiFi was the Wireless ISP (WISP). This is an idea of selling an Internet access service using wireless LAN technology and a shared Internet connection in a public location designated as a hot spot.

From a technical standpoint, access to the service is limited based on the transmission range of the WLAN technology. You have to be in the hot spot (i.e. within 100m of the access point) to use it. From a business standpoint, users either subscribe to a particular carrier's service for a monthly fee or access the service on a demand basis at a fee per hour. While the monthly fee basis is most cost effective, there are few intercarrier access arrangements, so you have to be in a hot spot operated by your carrier in order to access your service.

City-Wide Mesh Networks

To address the limited range, vendors like Mesh Networks and Tropos Networks have developed mesh network capabilities using WiFi's radio technology.

The idea of a radio mesh network is that messages can be relayed through a number of access points to a central network control station. These networks can typically support mobility as connections are handed off from access point to access point as the mobile station moves.

Some municipalities are using WiFi mesh networks to support public safety applications (i.e. terminals in police cruisers) and to provide Internet access to the community (i.e. the city-wide hot spot).

Wi-Fi - Radio Modulation

WiFi systems use two primary radio transmission techniques.

- **802.11b (<=11 Mbps)** − The 802.11b radio link uses a direct sequence spread spectrum technique called **complementary coded keying** (CCK). The bit stream is processed with a special coding and then modulated using Quadrature Phase Shift Keying (QPSK).
- **802.11a and g (<=54 Mbps)** − The 802.11a and g systems use 64-channel orthogonal frequency division multiplexing (OFDM). In an OFDM modulation system, the available radio band is divided into a number of sub-channels and some of the bits are sent on each. The transmitter encodes the bit streams on the 64 subcarriers using Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK), or one of two levels of Quadrature Amplitude Modulation (16, or 64-QAM). Some of the transmitted information is redundant, so the receiver does not have to receive all of the sub-carriers to reconstruct the information.

The original 802.11 specifications also included an option for frequency **hopping spread spectrum** (FHSS), but that has largely been abandoned.

Adaptive Modulation

WiFi uses adaptive modulation and varying levels of forward error correction to optimize transmission rate and error performance.

As a radio signal loses power or encounters interference, the error rate will increase. Adaptive modulation means that the transmitter will automatically shift to a more robust, though less efficient, modulation technique in those adverse conditions.

Wi-Fi - Major Issues

There are a few issues that are assumed to be the cause behind the sluggish adoption of WiFi technology −

- **Security Problems** − Security concerns have held back WiFi adoption in the corporate world. Hackers and security consultants have demonstrated how easy it can be to crack

the current security technology known as wired equivalent privacy (WEP) used in most WiFi connections. A hacker can break into a WiFi network using readily available materials and software.

- **Compatibility and Interoperability** − One of the major problems with WiFi is its compatibility and interoperability. For example, 802.11a products are not compatible with 802.11b products. Due to different operating frequencies, 802.11a hotspots would not help an 802.11b client. Due to lack of standardization, harmonization, and certification, different vendors come out with products that do not work with each other.
- **Billing Issues** − WiFi vendors are also looking for ways to solve the problem of back-end integration and billing, which have dogged the roll-out of commercial WiFi hotspots. Some of the ideas under consideration for WiFi billing such as per day, per hour, and unlimited monthly connection fees.

Wi-Fi - Summary

WiFi is a universal wireless networking technology that utilizes radio frequencies to transfer data. WiFi allows high-speed Internet connections without the use of cables.

The term WiFi is a contraction of "wireless fidelity" and commonly used to refer to wireless networking technology. The WiFi Alliance claims rights in its uses as a certification mark for equipment certified to 802.11x standards.

WiFi is a freedom – freedom from wires. It allows you to connect to the Internet from just about anywhere — a coffee shop, a hotel room, or a conference room at work. What's more – it is almost 10 times faster than a regular dial-up connection. WiFi networks operate in the unlicensed 2.4 radio bands, with an 11 Mbps (802.11b) or 54 Mbps (802.11a) data rate, respectively.

To access WiFi, you need WiFi enabled devices (laptops or PDAs). These devices can send and receive data wirelessly in any location equipped with WiFi access.

What is Next?

Now, the focus in wireless is shifting to wide area, i.e., WiMax. WiMax, short for Worldwide Interoperability for Microwave Access, is defined in IEEE 802.16 standards. It is designed to deliver a metro area broadband wireless access (BWA) service, and is being promoted by the WiMax Forum.

WiMAX is quite similar to WiFi, but on a much larger scale and at faster speeds. A nomadic version would keep WiMAX-enabled devices connected over a large area, much like today's cell phones.