1. INTRODUCTION

Wi-Fi, or Wireless Fidelity, is freedom: it allows you to connect to the Internet from your home, a bed in a hotel room or at a conference room at work without wires. How? Wi-Fi is a wireless technology like a cell phone. Wi-Fi enabled computers send and receives data indoors and out: anywhere within the range of a base station. And the best thing of all, it’s fast. In fact, it’s several times faster than the fastest cable modem connection.

However, you only have true freedom to be connected anywhere if your computer is configured with a Wi-Fi CERTIFIED radio (a PC Card or similar device). Wi-Fi certification means that you will be able to connect anywhere there are other Wi-Fi CERTIFIED products—whether you are at home, the office or corporate campus, or in airports, hotels, coffee shops and other public areas equipped with a Wi-Fi access available.

Wi-Fi certification comes from the Wi-Fi Alliance, a nonprofit international trade organization that tests 802.11-based wireless equipment to make sure it meets the Wi-Fi standard and works with all other manufacturers’ Wi-Fi equipment on the market.
2. WIRELESS NETWORKING COMPONENTS

Wi-Fi is a friendly term for IEEE 802.11b Ethernet standard. It operates in the unlicensed frequency band of 2.4 GHz with a maximum data rate of 11 Mbps.

IEEE 802.11b wireless networking consists of the following components:

- **Stations**

  A station (STA) is a network node that is equipped with a wireless network device. A personal computer with a wireless network adapter is known as a wireless client. Wireless clients can communicate directly with each other or through a wireless access point (AP). Wireless clients are mobile.

[Figure 1. Wireless station]

- **Wireless Access Points**

  A wireless AP is a wireless network node that acts as a bridge between STAs and a wired network. A wireless AP contains:
• At least one interface that connects the wireless AP to an existing wired network (such as an Ethernet backbone).
• A wireless network device with which it creates wireless connections with STAs.
• IEEE 802.1D bridging software, so that it can act as a transparent bridge between the wireless and wired networks.

The wireless AP is similar to a cellular phone network's base station. Wireless clients communicate with both the wired network and other wireless clients through the wireless AP. Wireless APs are not mobile and act as peripheral bridge devices that extend a wired network.

Figure 2. Access point
3. **OPERATION MODES**

IEEE 802.11 defines two operating modes: Ad hoc mode and Infrastructure mode.

**AD HOC MODE:** In ad hoc mode, also known as peer-to-peer mode, wireless clients communicate directly with each other (without the use of a wireless AP). Two or more wireless clients who communicate using ad hoc mode form an Independent Basic Service Set (IBSS). Ad hoc mode is used to connect wireless clients when a wireless AP is not present.

![Ad Hoc Network Diagram](Image)

**Figure 3:** The ad-hoc network structure in the 802.11 protocol

**INFRASTRUCTURE MODE:** In infrastructure mode, there is at least one wireless AP and one wireless client. The wireless client uses the wireless AP to access the resources of a wired network. The wired network can be an
organization intranet or the Internet, depending on the placement of the wireless AP.

Figure 4: The infrastructure network structure in the 802.11 protocol

A single wireless AP that supports one or multiple wireless clients is known as a Basic Service Set (BSS). A set of two or more wireless APs that are connected to the same wired network is known as an Extended Service Set (ESS). An ESS is a single logical network segment (also known as a subnet), and is identified by its Service Set Identifier (SSID). If the available physical areas of the wireless APs in an ESS overlap, then a wireless client can roam,
or move from one location (with a wireless AP) to another (with a different wireless AP) while maintaining Network layer connectivity.

4. RADIO TECHNOLOGY

Wi-Fi network uses radio technology called IEEE 802.11b to provide secure, fast, reliable, wireless connectivity. 11b defines the physical layer and media access control (MAC) sublayer for communications across a shared, wireless local area network (WLAN). At the physical layer, IEEE 802.11b operates at the radio frequency of 2.45 gigahertz (GHz) with a maximum bit rate of 11 Mbps. It uses the direct sequence spread spectrum (DSSS) transmission technique. At the MAC sublayer of the Data Link layer, 802.11b uses the carrier sense multiple access with collision avoidance (CSMA/CA) media access control (MAC) protocol

DIRECT SEQUENCE SPREAD SPECTRUM

Direct Sequence is the best known Spread Spectrum Technique. A DSSS transmitter converts an incoming data stream into a symbol stream where each symbol represents a group of one or more bits. Using a phase varying modulation technique, DSSS transmitter modulates or multiplies each symbol with a noise like code called ‘chip’ sequence. This is also called processing gain. The multiplication operation in a DSSS transmitter artificially increases the used bandwidth based on the length of chip sequence.
When receiving the DSSS signal, a matched filter correlator is used. The correlator removes the PN sequence and recovers the original data stream.
As shown in figure, the PN sequence spreads the transmitted bandwidth of the resulting signal (thus the term, “spread spectrum”) and reduces peak power. Note however, that total power is unchanged. Upon reception, the signal is correlated with the same PN sequence to reject narrow band interference and recover the original binary data (Fig. 5b). Regardless of whether the data rate is 1, 2, 5.5, or 11 Mbps, the channel bandwidth is about 20 MHz for DSSS systems. Therefore, the ISM band will accommodate up to three non-overlapping channels.

![Figure 6a. Effect of PN Sequence on Transmit Spectrum](image1)

![Figure 6b. Received Signal is Correlated with PN to Recover Data and Reject Interference](image2)
The basic access method for 802.11 is the Distributed Coordination Function (DCF) which uses Carrier Sense Multiple Access / Collision Avoidance (CSMA / CA). This requires each station to listen for other users. If the channel is idle, the station may transmit. However if it is busy, each station waits until transmission stops, and then enters into a random back off procedure. This prevents multiple stations from seizing the medium immediately after completion of the preceding transmission.
Packet reception in DCF requires acknowledgement as shown in figure. The period between completion of packet transmission and start of the ACK frame is one Short Inter Frame Space (SIFS). ACK frames have a higher priority than other traffic. Fast acknowledgement is one of the salient features of the 802.11 standard, because it requires ACKs to be handled at the MAC sublayer.

Transmissions other than ACKs must wait at least one DCF inter frame space (DIFS) before transmitting data. If a transmitter senses a busy medium, it determines a random back-off period by setting an internal timer to an integer number of slot times. Upon expiration of a DIFS, the timer begins to decrement. If the timer reaches zero, the station may begin transmission. However, if the channel is seized by another station before the timer reaches zero, the timer setting is retained at the decremented value for subsequent transmission.

**OPERATION BASICS**

When a wireless adapter is turned on, it begins to scan across the wireless frequencies for wireless APs and other wireless clients in ad hoc mode. Assuming that the wireless client is configured to operate in infrastructure mode, the wireless adapter chooses a wireless AP with which to connect. This selection is made automatically by using SSID and signal strength and frame error rate information. Next, the wireless adapter switches to the assigned channel of the selected wireless AP and negotiates the use of a port. This is known as establishing an association.
If the signal strength of the wireless AP is too low, the error rate too high, or if instructed by the operating system (in the case of Windows XP), the wireless adapter scans for other wireless APs to determine whether a different wireless AP can provide a stronger signal or lower error rate. If such a wireless AP is located, the wireless adapter switches to the channel of that wireless AP and negotiates the use of a port. This is known as reassociation.

Reassociation with a different wireless AP can occur for several reasons. The signal can weaken as either the wireless adapter moves away from the wireless AP or the wireless AP becomes congested with too much traffic or interference. By switching to another wireless AP, the wireless adapter can distribute the load to other wireless APs, increasing the performance for other wireless clients. You can achieve contiguous coverage over large areas by placing your wireless APs so that their signal areas overlap slightly. As a wireless client roams across different signal areas, it can associate and reassociate from one wireless AP to another, maintaining a continuous logical connection to the wired network.

RANGE IN A Wi-Fi NETWORK

One of the factors that affect the range of a Wi-Fi network is the distance of the client devices to your base station. In an open area with no walls, furniture or interfering radio devices you may be able to get a range of 500 feet or more from your base station to the Wi-Fi equipped computer. In fact you could get a signal from up to a mile away depending on the antennas you use and environmental conditions.
Many base stations can also act as relay stations for your network. For example if you locate one Wi-Fi equipped computer 100 feet away from your base station, another Wi-Fi computer 100 feet away in another direction and then position your base station in the middle, you can create a network with a range of 200 feet from the Wi-Fi computer to the other.

Wi-Fi, or IEEE 802.11b, speed decreases the farther you move away from your network. For example when you are close to the base station your Wi-Fi computer should be able to get the full 11Mbps data rate. Move farther away, and depending on the environment, the data rate will drop to 2Mbps, and finally to 1Mbps. But getting just 1Mbps throughput is still a perfectly acceptable performance level. 1Mbps is faster than most DSL and cable connections, which means it’s still a satisfactory high speed transmission if you are sending and receiving e-mail, cruising the internet or just performing data entry tasks from a mobile computer.

<table>
<thead>
<tr>
<th>AREA</th>
<th>Maximum Range</th>
<th>Range at 11Mbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outdoors/open Space with standard antennae</td>
<td>750-1000 feet</td>
<td>150-350 feet</td>
</tr>
<tr>
<td>Office/light industrial setting</td>
<td>250-350 feet</td>
<td>100-150 feet</td>
</tr>
<tr>
<td>Residential setting</td>
<td>125-200 feet</td>
<td>60-80 feet</td>
</tr>
</tbody>
</table>
5. SECURITY

Because wireless is a shared medium, everything that is transmitted or received over a wireless network can be intercepted. Encryption and authentication are always considered when developing a wireless networking system. The goal of adding these security features is to make wireless traffic as secure as wired traffic.

The IEEE 802.11 standard defines the following mechanisms for wireless security:

- Authentication through the open system and shared key authentication types
- Data confidentiality through Wired Equivalent Privacy (WEP)

Open system authentication does not provide authentication, only identification using the wireless adapter's MAC address. Open system authentication is used when no authentication is required. Some wireless APs allow the configuration of the MAC addresses of allowed wireless clients. However, this is not secure because the MAC address of a wireless client can be spoofed.

Shared key authentication verifies that an authenticating wireless client has knowledge of a shared secret. The 802.11 standard currently assumes that the shared key is delivered to participating STAs through a secure channel that is independent of IEEE 802.11. In practice, this secret is manually configured for both the wireless AP and client. Because the shared key authentication secret must be distributed manually, this method of authentication does not scale to a large infrastructure mode network (for example, corporate campuses and public places, such as malls and airports).
Additionally, shared key authentication is not secure and is not recommended for use.

**WIRED EQUIVALENT PRIVACY (WEP)**

WEP utilizes a *symmetric algorithm* known as a stream cipher, for encryption. A symmetric algorithm is one that relies on the concept of a single *shared key* (as opposed to a public key) that is used at one end to encrypt *plaintext* (the data) into *ciphertext* (the encrypted data), and at the other end to decrypt it - convert the ciphertext back to plaintext. Thus, the sender and the receiver share the same key, and it must be kept secret.

*Stream ciphers* encrypt data as it is received, as opposed to *block ciphers* that collect data in a buffer and then encrypt it a block at a time. Stream ciphers are used for applications requiring hardware implementation.

**WEP VULNERABILITIES**

Three key difficulties were identified:

1. WEP uses a single, static shared key. It remains the same unless a network administrator manually changes it on all devices in the WLAN, a task that becomes ever more daunting as the size of the WLAN increases.

2. At the time of its introduction, WEP employed a necessarily short 40-bit encryption scheme. The scheme was the maximum allowed by US export standards at that time. In 1997, the US government deemed the export of data cryptography to be as threatening to national security as the export of weapons of mass destruction. By necessity, Wi-Fi security had to be weak.
if the specification was to be adopted as an international standard and if products were to be freely exported.

3. Other technical problems contributed to its vulnerability, including attacks that could lead to the recovery of the WEP key itself.

VIRTUAL PRIVATE NETWORKS (VPNs)

Virtual Private Network technology (VPN) has been used to secure communications among remote locations via the Internet since the 1990s. A familiar and already widely used technology in the enterprise, it can readily be extended to Wi-Fi WLAN segments on existing wired networks. Although VPNs were originally developed to provide point-to-point encryption for long Internet connections between remote users and their corporate networks, they have recently been deployed in conjunction with Wi-Fi WLANs. When a WLAN client uses a VPN tunnel, communications data remains encrypted until it reaches the VPN gateway, which sits behind the wireless AP. Thus, intruders are effectively blocked from intercepting all network communications. Since the VPN encrypts the entire link from the PC to the VPN gateway in the heart of the corporate network, the wireless network segment between the PC and the AP is also encrypted. This is why VPNs have been recommended to help secure Wi-Fi.

While VPNs are generally considered an enterprise solution, integrated products that offer VPN pass-through connections, firewalls and routers are available to accommodate telecommuters who work from home. Although they provide excellent security, VPNs are not self-managing. User credentials and, often, VPN software must be distributed to each client. However, when properly installed, VPNs extend the high level of security they provide on wired networks to WLANs. In fact, some Wi-Fi vendors
themselves have utilized VPNs in networks to secure their own internal Wi-Fi networks.

**Wi-Fi PROTECTED ACCESS**

Wi-Fi Protected Access is a specification of standards-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN systems. Designed to run on existing hardware as a software upgrade, Wi-Fi Protected Access is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. When properly installed, it will provide wireless LAN users with a high level of assurance that their data will remain protected and that only authorized network users can access the network.

Wi-Fi Protected Access had several design goals, i.e.,: be a strong, interoperable, security replacement for WEP, be software upgradeable to existing Wi-Fi CERTIFIED products, be applicable for both home and large enterprise users, and be available immediately. To meet these goals, two primary security enhancements needed to be made. Wi-Fi Protected Access was constructed to provide an improved data encryption, which was weak in WEP, and to provide user authentication, which was largely missing in WEP.

*Enhanced Data Encryption through TKIP*

To improve data encryption, Wi-Fi Protected Access utilizes its Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named *Michael*, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all WEP’s known vulnerabilities.
6. ADVANTAGES

It’s flexible: With a wireless network you and your staff can have uninterrupted access to people, information and tools as you and they move through the workplace with your mobile PC.

It’s responsive: As you change your business operations your wireless network can change with you.

It’s customized: Your wireless network can be configured the way you want it.-even combined with your current wired network.

It’s fast: From 11 to 54 Mbps throughput and advanced roaming capabilities provide reliable access to e-mail, the Internet, file sharing and other network resources away from the desk.

It’s cost-effective: Expand and extend your existing network by simply adding more adapters and access points. Planning is a no brainier as you need to buy only what you need.

It’s secure: Current standards utilizes 64- and 128-bit WEP encryption and help guard the network from intruders and protect data in transit. Add in technology and you have increased WLAN protection important for mission-critical data.
7. **LIMITATIONS**

- It has a limited bandwidth of about 83.5 MHz.

- Frequency spectrum used by IEEE 802.11b is shared by many other systems like microwave ovens, cordless phones etc. This frequency sharing causes interference problem.

- Security techniques are not reliable yet.
8. FUTURE TRENDS

IEEE 802.11a

The 802.11a supplement to 802.11 was published in 1999. It uses Orthogonal Frequency Division Multiplexing (OFDM) to provide data rates to 54 Mbps in the 5 GHz U-NII bands. In addition to being uncrowded, more spectrums in the U-NII bands allow room for 12 non-overlapping channels, compared to just three in the 2.4 GHz ISM bands. Both of these factors make operating in the U-NII bands far less prone to interference.

However, at 5 GHz, more path loss occurs due to increased absorption of the RF energy by walls and other solid objects. This, combined with a decrease in range due to the higher data rates, may require that more access points be installed to effectively cover an area comparable to that of 802.11b.

IEEE 802.11g

The 802.11g task group is working on a supplement to the 802.11 standard that defines a technology for operation at 2.4 GHz that offers higher data rates (up to 22 Mbps) using OFDM, while remaining backwards compatible to 802.11b. When compared to 802.11a, 802.11g offers the advantages of lower cost, backwards compatibility to existing 802.11b equipment, and less path loss than 802.11a. This translates into higher data rates for a given range, or increased range for a given data rate.
9. CONCLUSION

Wi-Fi provides freedom: freedom to physically move around your home or business and still stay connected to the Internet or local network; freedom to grow and move an office or business without having to install new cables and wires; freedom to be connected while traveling and on the road. Wireless “HotSpots” (airports, hotels, coffee shops, convention centers and any other place where someone can connect to a wireless network) are being installed worldwide. All this means Wi-Fi truly does provide unprecedented freedom. Plus, it is cool, and it is fun – as those in the know say, “Once you go wireless, you will never want to use a cable again.”

There are real and measurable benefits to using a wireless network versus a standard wired network. For a home installation customer, the greatest benefit is that there are no wires needed: you don’t need to drill holes in walls and floors; you don’t need to drag cables or hide them under rugs. One Wi-Fi access point can provide network access for any typically sized home. And if you live in a rental or a historical building, you may not be allowed to drill holes— that makes wireless your only solution.

Wi-Fi use is growing fast in homes, public access areas and businesses—both large and small. The Wi-Fi Alliance is active with many industry organizations and is working closely with manufacturers to make sure that existing Wi-Fi gear is compatible with wireless technologies developed in future.
10. REFERENCES


2. www.wikipedia.org


4. www.wi-fi.org