A

Seminar report

On

Wi-Fi Technology

Submitted in partial fulfillment of the requirement for the award of degree of Electronics

SUBMITTED TO:
www.studymafia.org

SUBMITTED BY:
www.studymafia.org

Preface

I have made this report file on the topic **Wi-Fi Technology**; I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

Acknowledgement

I would like to thank respected Mr…….. and Mr. ……..for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a seminar report. It helped me a lot to realize of what we study for.

Secondly, I would like to thank my parents who patiently helped me as i went through my work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.

Thirdly, I would like to thank my friends who helped me to make my work more organized and well-stacked till the end.

Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

Last but clearly not the least, I would thank The Almighty for giving me strength to complete my report on time.

Abstract

Wi-Fi is a Wireless technology that uses the radio frequency to transmit data through air. With the rise of Wireless Fidelity (Wi-Fi) , technology comes the rise of the hotspot -public access Wireless Local Area Networks (WLANs) that allow anyone with a Wi-Fi capable notebook or PDA to connect to the Internet or a corporate intranet in airports, hotels, coffee shops, or even campgrounds and fast food restaurants.

Wi-Fi hotspots are expected to have an important role in future provisioning of "anywhere, anytime" connectivity. They are quickly being deployed at locations that tend to attract nomadic users, such as cafes, airports, hotels, and conference centers

This paper contributes an alternative billing architecture using *virtual prepaid tokens* (VPTs) and experimentally evaluates its performance. Users buy VPTs at the point and time of access, using a third-party online payment server. Therefore, such an account is more flexible than is a conventional pay-per-use account, which can be used only to purchase access from a specific provider or set of providers.

Unlike physical prepaid tokens, VPTs allow a user to order and obtain Internet access from a provider in less than 15 s, even if the user has no previous or subsequent relationship with that provider or that provider's aggregator. Simultaneous support for captive-portal and 802.1x authentication allows hotspots to provide recent Wi-Fi security improvements to those clients whose configuration supports them, without disrupting legacy clients. Improvements include mutual authentication between client and hotspot and link-layer packet encryption and authentication with dynamic per-session keys.

Introduction

. Billing is often cited as a problem area that contributes to low hotspot utilization. Existing billing methods have drawbacks that turn away many potential users. Three of the most common methods are subscription, pay-per-use account, and prepaid token.

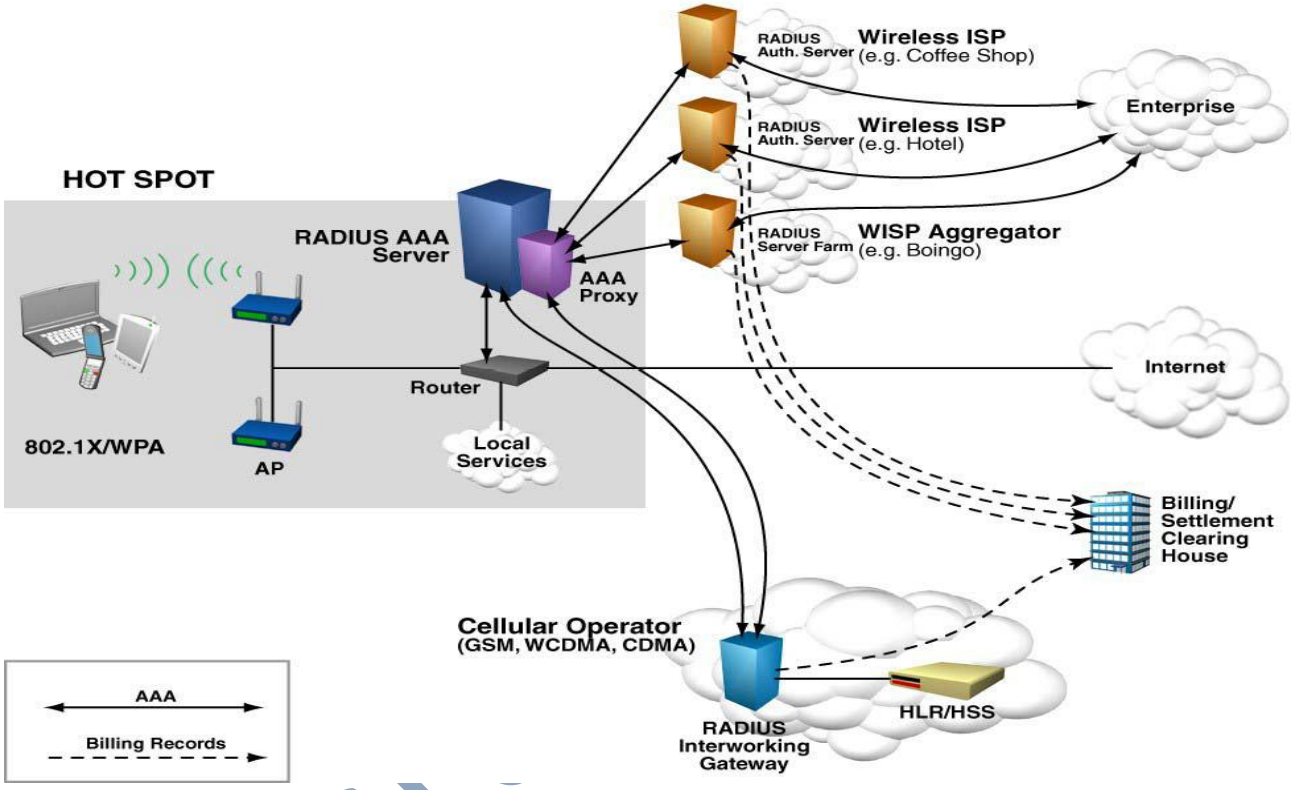


Fig1: A typical Hot spot Architecture integrated with WPA security.

Even though subscriptions provide a steady revenue stream and the convenience of a fixed price and single monthly payment to the user, Users may be concerned about provider reliability. Instead of a subscription, users may set up a pay-peruse account with a provider. Pay-per-use accounts typically draw funds automatically from one of the user's bank or credit card accounts, when the user gains access. Pay-per-use accounts can be less wasteful than subscriptions to sporadic users. Moreover, a user may occasionally need access in places that are not served (directly or by agreement) by any of the providers that serve areas more frequently visited by the user. In the latter cases, users may prefer prepaid tokens (PPTs). PPTs contain an id and password that are typically revealed by scratching a card and are activated after first use

for a limited time. A user does not need to set up any account to buy such a token; payment may be, e.g., by cash or credit card. Prepaid tokens offer little risk to users. In many cases (e.g., at an airport), vendor location may be inconvenient or not obvious. Moreover, a vendor location may be closed when a token is needed.

Experiments show that users arriving at a hotspot can buy a VPT and gain full Internet connectivity in less than 15 seconds, i.e. much less time than it would take to buy and activate a physical token. VPTs can be used in hotspots that employ a captive portal or 802.1x to authenticate users. Most current hotspots use a captive portal, but 802.1x enables much better security. In particular, 802.1x enables mutual authentication between user and hotspot and encryption keys at the link layer.

Wi-Fi Security Techniques

- Service Set Identifier (SSID)
- Wired Equivalent Privacy (WEP)
- 802.1X Access Control
- Wireless Protected Access (WPA)
- IEEE 802.11i

Service Set Identifier (SSID)

- SSID is used to identify an 802.11 network
- It can be pre-configured or advertised in beacon broadcast
- It is transmitted in clear text
- Provide very little security

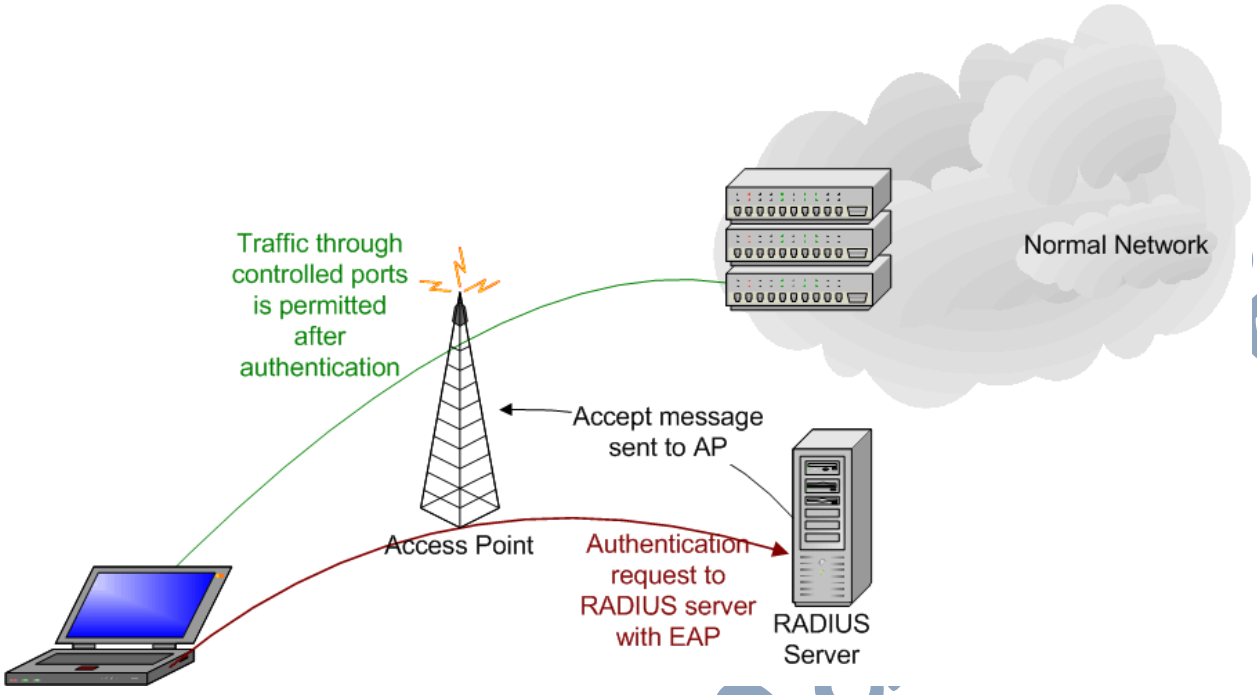
Wired Equivalent Privacy (WEP)

- Provide same level of security as by wired network
- Original security solution offered by the IEEE 802.11 standard
- Uses RC4 encryption with pre-shared keys and 24 bit initialization vectors (IV)
- key schedule is generated by concatenating the shared secret key with a random generated 24-bit IV
- 32 bit ICV (Integrity check value)
- No. of bits in keyschedule is equal to sum of length of the plaintext and ICV
- 64 bit preshared key-WEP
- 128 bit preshared key-WEP2
- Encrypt data only between 802.11 stations.once it enters the wired side of the network (between access point) WEP is no longer valid
- Security Issue with WEP
    - Short IV

    - Static key
- Offers very little security at all

802.1X Access Control

- Designed as a general purpose network access control mechanism
    - Not Wi-Fi specific
- Authenticate each client connected to AP (for WLAN) or switch port (for Ethernet)
- Authentication is done with 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 send an EAP start message
    - AP return an EAP message requesting the user’s identity
    - Identity send by user is then forwared to the authentication server by AP
    - Authentication server authenticate user and return 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



Wireless Protected Access (WPA)

- WPA is a specification of standard based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN system.
- User Authentication
    - 802.1x
    - EAP
- TKIP (Temporal Key Integrity Protocol) encryption
    - RC4, dynamic encryption keys (session based)
        - 48 bit IV
        - per packet key mixing function
    - Fixes all issues found from WEP
- Uses Message Integrity Code (MIC) Michael
    - Ensures data integrity

- Old hardware should be upgradeable to WPA
- WPA comes in two flavors
    - WPA-PSK
        - use pre-shared key
        - For SOHO environments
        - Single master key used for all users
    - WPA Enterprise
        - For large organisation
        - Most secure method
        - Unique keys for each user
        - Separate username & password for each user

How Wi-Fi Works?

If you want to understand wireless networking at its simplest level, think about a pair of walkie-talkies that you might purchase at Market. These are small radios that can transmit and receive radio signals.

When you talk into a Walkie-Talkie, your voice is picked up by a microphone, encoded onto a radio frequency and transmitted with the antenna. Another walkie-talkie can receive the transmission with its antenna, decode your voice from the radio signal and drive a speaker.

The two basic components of a Wi-Fi network are a computer device outfitted with a low-power radio and another radio-equipped gadget known as an access point, which is wired to the Internet or a local network. The two communicate with each other over a free slice of the radio spectrum reserved for consumer use and inhabited by microwave ovens and cordless phones.

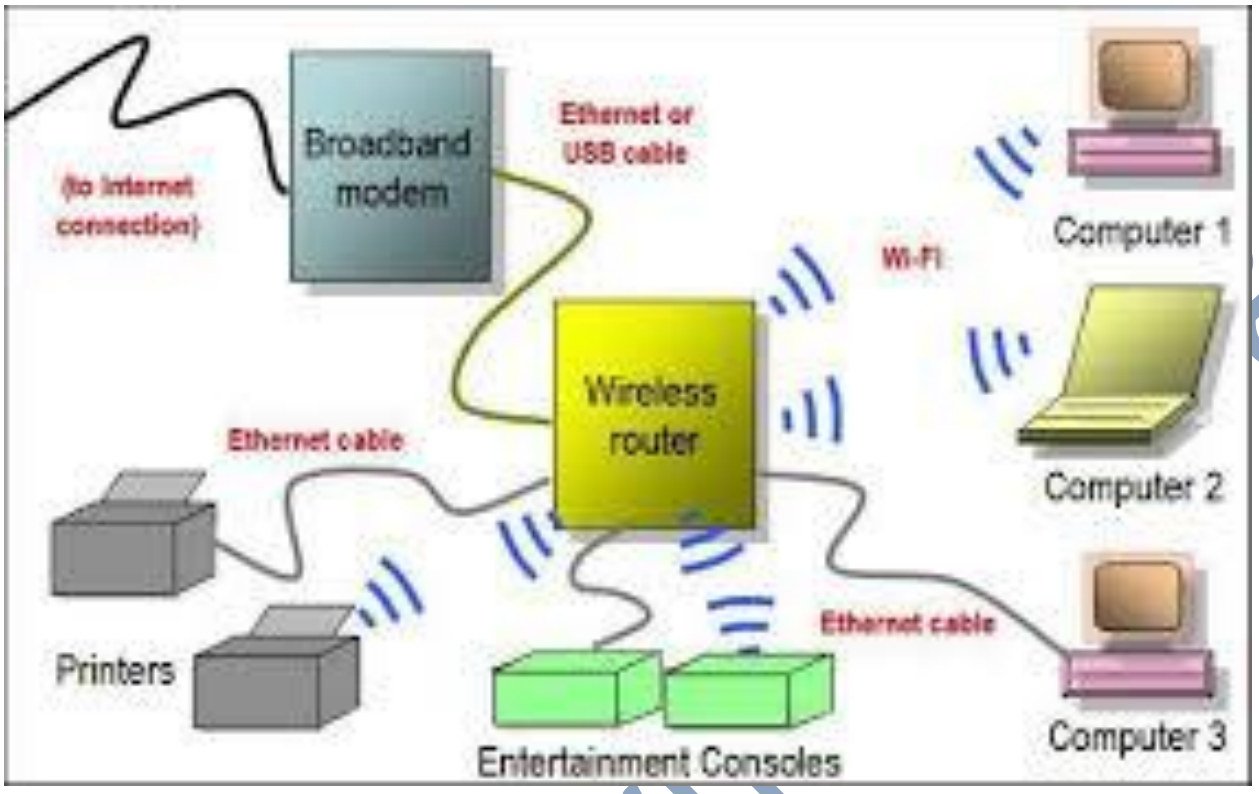
First of all devices called laptop or home pc or any network which want to access internet or connected to their network to another office network. They want to insert wi-fi card which card give facilities to access wireless networking.

They first of all connected to the access point which give the connection Gate to connect to the internet after that signals go to the computer server which is wired connected to the access point .and computer server connected to internet server. Which provide the internet facilities to computer or they also using another office network through transmitter.

Now the question is that how they converted signal to transmit data? in that In the small figure you saw that computer data combined with addressing and codes for security. And this combined signals send to transmitter and in the last antenna convert them into radio waves.

Our wireless Wi-Fi network gives instant and convenient access to the internet at cafe's and meeting room hotspots through out Brindabella Bussiness park as well as the airport terminal direct internet access is provided by approved internet service providers with a variety of global roaming providers supported where approved and arranged by tenants, IT departments and with layers of security suiting every requirement, wireless networking is also available directed into tenancies to access your business applications and emails at even higher speeds

And utilizing tenants own interest gateways. The Wi-Fi infrastructure is operated and managed by Camberra international airport.



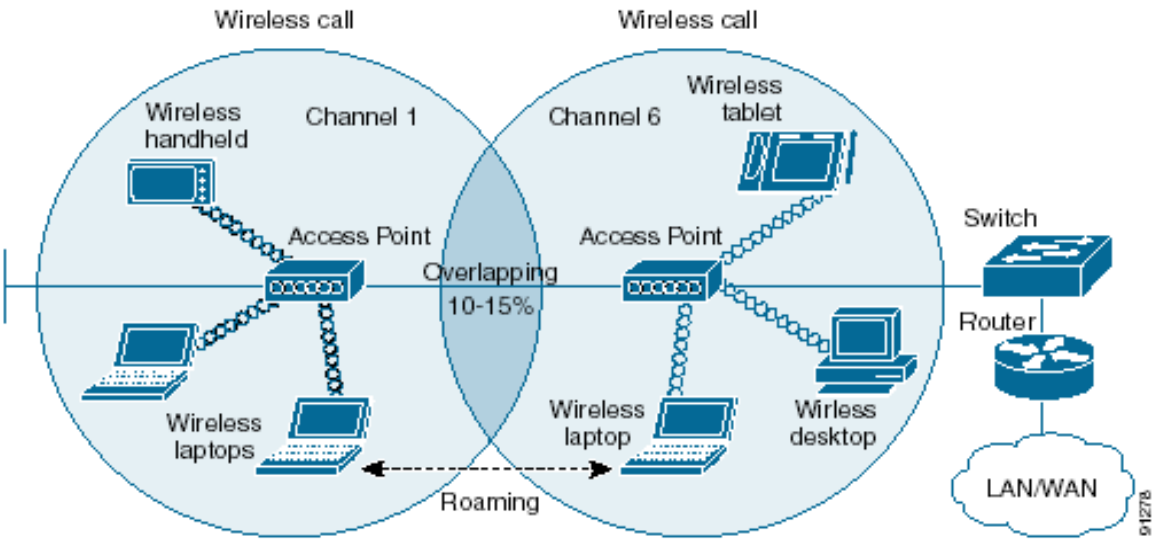
Wi-Fi Network Topologies

- AP-based topology (Infrastructure Mode)
- Peer-to-peer topology (Ad-hoc Mode)
- Point-to-multipoint bridge topology

AP-based topology

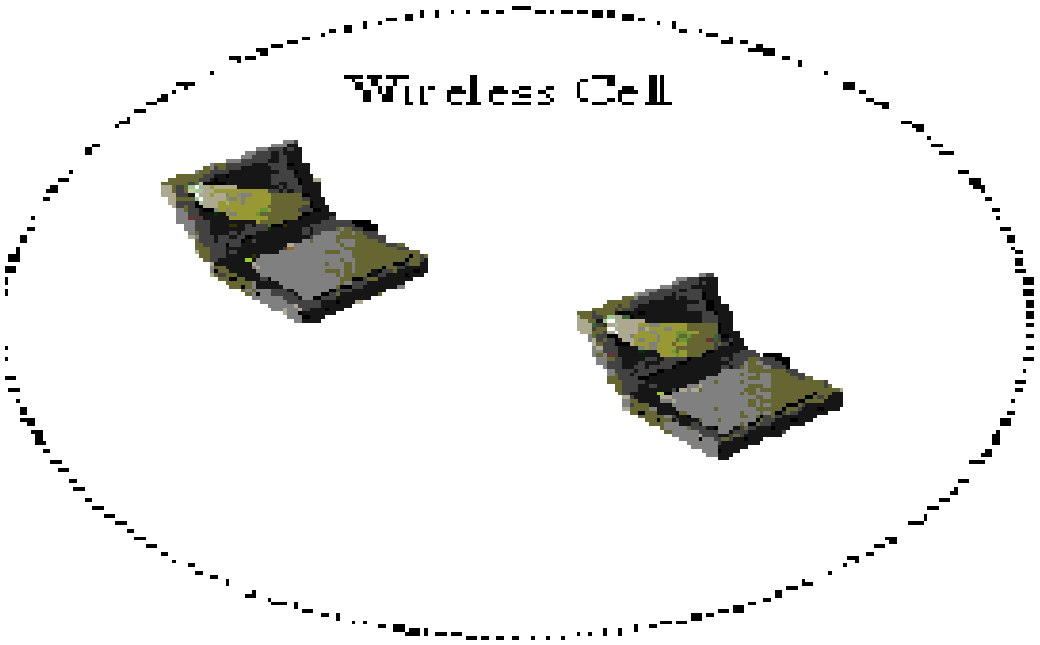
- The client communicate through Access Point.
- BSA-RF coverage provided by an AP.
- ESA-It consists of 2 or more BSA.
- ESA cell includes 10-15% overlap to allow roaming.

Figure 1-3 Typical WLAN



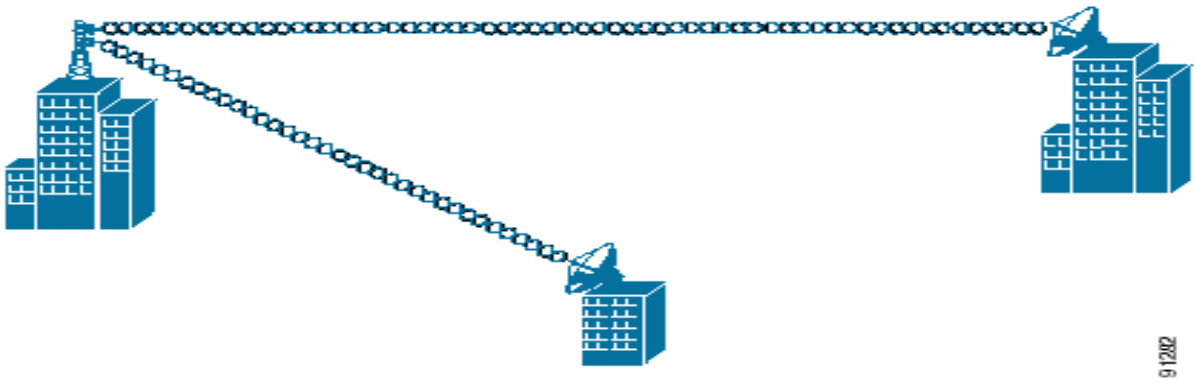
Peer-to-peer topology

- AP is not required.
- 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-multipoint bridge topology

This is used to connect a LAN in one building to a LANs in other buildings even if the buildings are miles apart.These conditions receive a clear line of sight between buildings. The line-of-sight range varies based on the type of wireless bridge and antenna used as well as the environmental conditions.



Advantages

- **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.
- **Responsive**: As you change your business operations your wireless network can change with you.
- **Customized:** Your wireless network can be configured the way you want it.-even combined with your current wired network.
- **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.
- **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.
- **Secure:** Current standards utilize 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.

  In addition to the hard benefits of increased efficiency, productivity, manageability and cost savings, wireless networks will certainly make a ËœThis is a technology savvy companyâ„¢ statement to the world.

Disadvantages

- Spectrum assignments and operational limitations are not consistent worldwide.
- Power consumption is fairly high compared to some other low-bandwidth standards.
- Wi-Fi networks have limited range.
- Wi-Fi pollution, or an excessive number of access points in the area, especially on the same or neighboring channel, can prevent access and interfere with the use of other access points by others.

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.

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 wites 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.

Reference

www.google.com

www.wikipedia.com

www.studymafia.org