Wi-Fi

Presented by
Taniya Vanasatit

Introduction

Have you ever wondered how computers are connected to each other under the wireless? What is the technology beneath those flexibility and convenience? The answers for those questions are "**Wi-Fi**." Wi-Fi is stand for *wireless fidelity*. It is actually another name for IEEE 802.11b. It is a trade term promulgated by the Wireless Ethernet Compatibility Alliance (WECA), a group founded by Cisco, 3Com, Intersil, Agere, Nokia, and Symbol and now supported by more than 100 companies. "Wi-Fi" is used in place of 802.11b[1] in the same way that "Ethernet" is used in place of IEEE 802.3. Products certified as Wi-Fi by WECA are interoperable with each other even if they are from different manufacturers. A user with a Wi-Fi product can use any brand of Access Point with any other brand of client hardware that is built to the Wi-Fi standard.

Cutting off the technical part, Wi-Fi will allow us to connect to the Internet from any places in your room without putting a cable line on. On the other hand, Wi-Fi enabled computers to send and receive data indoor and outdoor; anywhere within the range of a base station. And the best thing is it is several times faster then the fastest cable modem connection.

The Wi-Fi Technology

Wi-Fi uses radio Technology called IEEE802.11b or 802.11a to provide secure, reliable, fast wireless connectivity. Wi-Fi networks operate in the unlicensed 2.4 GHz radio bands, with an 11 Mbps (802.11b) or 54 Mbps (802.11a) data rate, so they can provide real-world performance similar to the basic 10BaseT1[2] wired Ethernet networks.

The WLAN standards were started with the 802.11 standard, developed in 1997 by the IEEE. This base standard allowed data transmission of up to 2 Mbps. Overtime, this standard has been developed. These enchanted are recognized by the addition of a letter to the original 802.11 standard, such as 802.11a and 802.11b. This list below is a list of 802.11 standards.

802.11	The original WLAN standard. Support 1 Mbps to 2 Mbps
802.11a	High speed WLAN standard for 5GHx band, support 54 Mbps
802.11b[3]	WLAN standard for 2.4 GHz band. Supports 11 Mbps.

[1] The 802.11b standard operates in the 2.4GHz range and offers a data speeds up to 11Mbps. 802.11b is the de facto standard for Wi-Fi services because of its availability and low price (although 802.11g will now quickly become the standard).

[2] 10 Megabit per second baseband Ethernet specification using two pairs of twisted-pair cabling (Category 3, 4 or 5): one pair for transmitting data and the other for receiving data. 10BaseT has a distinct limit of approximately 100 meters per segment

[3] The 802.11b specification makes data speed lower than 802.11a but since the product didn't become available until 2001 so it isn't as widely developed as 802.11b.

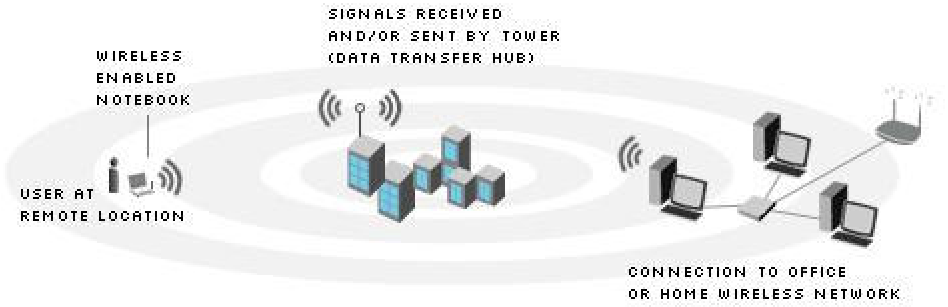
802.11e	Address quality of service requirement for all IEE WLAN radio interface
802.11g	Establish an additional modulation technique for 2.4 GHZ band. Intended to provide speeds up to 54 Mbps.
802.11h	Defines the spectrum management of the 5 GHz band for use in Europe and in Asia Pacific
802.11i	Address the current security weakness for both authentication and encryption protocols. The standard encompasses 802.1x, TKIP, and protocols

Wireless is developing in three areas of technology: Personal Area of Networking (PAN), Local Area Networking and the Wide Area Networking (WAN).

PAN: Personal Area of Networking technology is based on a specification called Bluetooth which utilizes radio frequency to transmit voice and data over a short distance. Bluetooth is cable-replacement technologies that wirelessly synchronizes data across devices and create invisible access to networks.

LAN: A wireless LAN is a network providing wireless peer to peer (PC-to-PC, PC-to-hub, or printer-to-hub) and point-to-point (LAN-to-LAN) connectivity with in the building or campus. Wireless LANs (WLAN) also provide public wireless access to the Internet through public spaces such as airports, hotel lounges, or cafes which we call those places as “hot spots.”

WAN: This technology is based on digital mobile phone system. It provides 2.5 GHz or 3 GHz transmission rate to access data and information from any location in the range of a cell tower to a data-enable network. A wireless Wide Area network uses long-range connection to provide access on much larger area than wireless LANs. Since they work on the same network as cellular phone, anywhere you can get cell phone, you can get access to a wireless WAN.

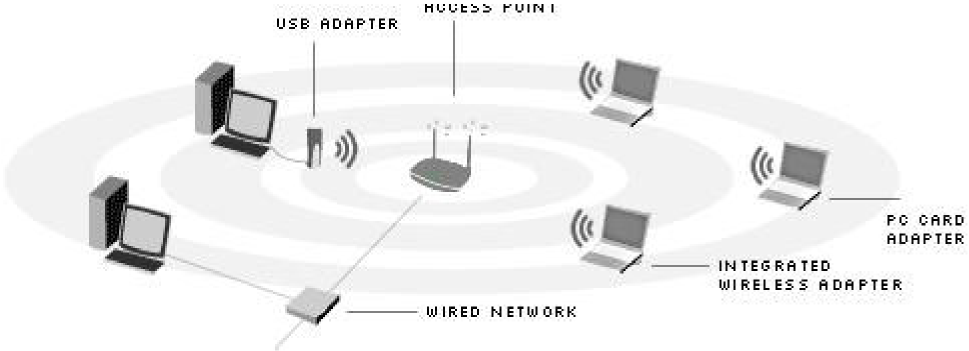

WIRELESS ENABLED NOTEBOOK
SIGNALS RECEIVED AND/OR SENT BY TOWER (DATA TRANSFER HUB)
USER AT REMOTE LOCATION
CONNECTION TO OFFICE OR HOME WIRELESS NETWORK

Wireless Network Setup

The two main components for setting up the wireless network are access points and client adapters

<u>*Access Points and Bridge Routers*</u>: These devices control the data transfers in the network. They are working like a hub by connecting multiple computers and devices together, but the different is we do it wirelessly. They also provide a connection between the wireless network and a previously existing wired network. For bridge, it provides a connection for a high-speed modem and a basic routing capacity for various computers.

<u>*Client Adapters*</u>*: PC cards, USB devices and modules*: This network card will integrate computer with the network.



We can configure wireless network in multiple ways; starting from a wireless access point that let users connect to a large network, or hook on the Internet from hotspot around the corner. In this report, we can separate wireless connection in six areas.

1. <u>*Ad Hoc Network*</u>: An ad hoc (or peer-to-peer) network is an independent area network such as setting up wireless connection at home. This type of network is not connected to a wire infrastructure and where all stations are connected directly to one another.
2. <u>*Infrastructure Network*</u>: This configuration is when WLAN clients connect to the corporate network through a wireless access point.
3. <u>*Hotspot*</u>: There are a lot of wide varieties of public meeting such as coffee shop, airport or hotel, which provide a free access to Internet. To get an access to this hotspot, a PC (notebook) need to be configured with Wi-Fi CERTIFIED[4] technology, then the notebook can send and receive data anywhere within the range of wireless LAN base station.
4. <u>*Point-to-Point Bridge*</u>: A bridge architecture connects two networks together such as interconnect network between two building. The access point will connect multiple users while the bridges will connect between the networks.
5. <u>*Point to-Multiple Bridge*</u>: This happened when we want to connect three or more LANs that may be located on different floor in a building or across buildings.

[4] The Wi-Fi certified is assurance that the product has met rigorous interoperability testing requirements to assure products from different vendors will work together

6. *Ethernet to Wireless Bridge*: An Ethernet to wireless bridge connects a single device that has an Ethernet port but not an 802.11 network interface card (NIC), such as a network printer.

Wi-Fi access control mechanism

There are three mechanisms to make wireless access more secure
1. Service Set Identifier (SSID)
2. Media Access Control (MAC)
3. RADIUS Authentication and Authorization
4. Wired Equivalent Privacy (WEP)

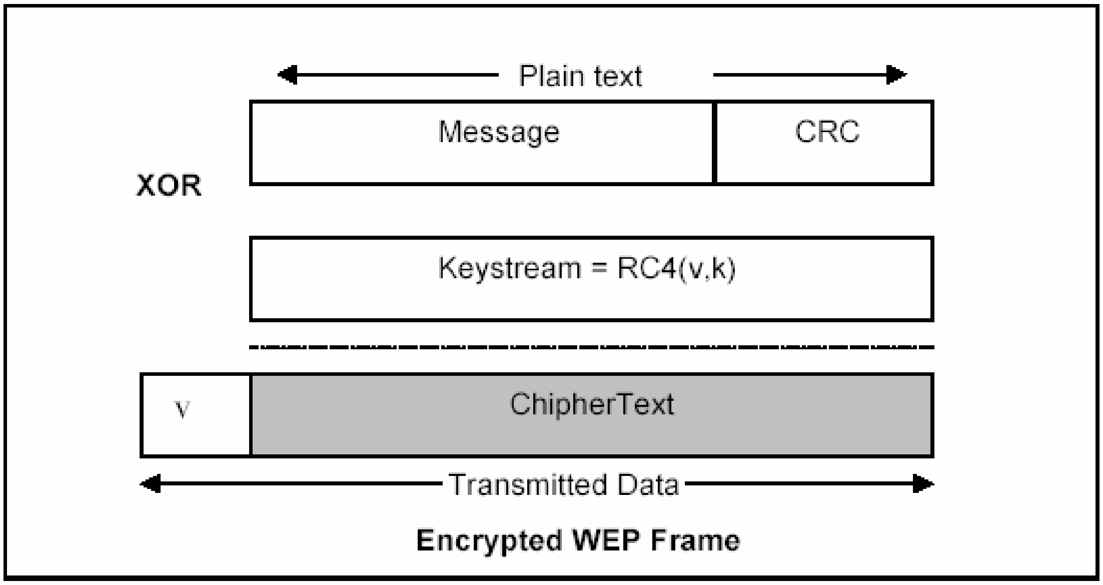
Service set Identifier (SSID): it is a 32-character unique identifier attached to the header of packets sent over wireless LAN that act as a password when a mobile device tried to connect to the wireless station. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to specific WLAN must use the same SSID. A device will not be permitted to join the wireless base unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is name that identifies a wireless network.

Media Access Control Address (MAC): is the hardware address that uniquely identifies each node of a network. Wireless system uses Access Control List (ACL) to permit associations by known MAC address to manage access from others. As part of the 802.11b standard, every Wi-Fi radio has its unique Media Access Control (MAC) number allocated by the manufacturer. To secure the systems, system administrator can program a Wi-Fi access point to accept only a certain MAC address and filter out all others. However, programming all the authorized users' MAC addresses into all the company's access points can be an difficult task for a large organization and can be time consuming, but for the home technology enthusiast it can be quite effective.

RADIUS (Remote Access Dial-Up User Service): This becomes another standard technology, which starting implemented in many major corporations to protect access to wireless network. RADIUS is a user name and password scheme that enables only approved users to access the network; it does not affect or encrypt data. The first time a user wants access to the network, secure files or net locations, he or she must input his or her name and password and submit it over the network to the RADIUS server. The server then verifies that the individual has an account and, if so, ensures that the person uses the correct password before she or he can get on the network.

RADIUS can be set up to provide different access levels or classes of access. For example, one level can provide blanket access to the Internet; another can provide access to the Internet as well as to e-mail communications; yet another account class can provide access to the Net, email and the secure business file server.

Wired Equivalent Privacy protocol (WEP): is an encryption scheme that protects WLAN data streams (link-level data) between clients and APs (Access Points) as specified by the 802.11. WEP relies on a secret key *k* shared between the communicating parties to protect the body of a transmitted frame of data.



First, we compute an integrity checksum on the message. The WEP protocol uses an integrity checksum field to ensure that packets for not get modified in transit. The checksum is implemented as a CRC-32 checksum. It is not a cryptographically secure authentication code because CRC's are designed to detect random errors in the message. Then we concatenate the message to obtain a plaintext. In the second stage, we encrypt the plaintext using RC4[5] algorithm with initialization vector (IV)[6] to generate a keystream. Then we exclusive-or (XOR) the plaintext with the keystream to get ciphertext, which is the transmitted data.

To decrypt a frame protected by WEP, the recipient simply reverses the encryption process. First, it regenerated the keystream RC4 and XOR it against the ciphertext to recover the initial plaintext. Next, the recipient verifies that the checksum on the decrypted plaintext. This ensures that only frames with a valid checksum will be accepted by the receiver.

As the result, the WEP protocol tends to enforce three main security goals.

1. *Confidentiality*: The fundamental goal of WEP is to prevent casual privacy invasion.
2. *Access control*: the second goal is to protect an access to a wireless network infrastructure. The 802.11 standard includes this kind of control is

[5] RC4 encryption algorithm devised by Ron Rivest (the "R" in RSA) of RSA Security Inc.

[6] The IV is included in the unencrypted portion of the transmission so that the receiver can know what IV to use when deriving the keystream of decryption.

an optional feature. That is the system can discard all packets that are not properly encrypted using WEP.

3. *Data Integrity*: The related goal is to prevent tampering with transmitted messages the integrity checksum field is included for this purpose.

The claimed security of the WEP protocol is the difficulty to discover the secret key. There are two classes of WEP implementation. First one the classic WEP, and another is the extended version developed by some vendor to provide more security with the larger keys. The WEP standard specifies the use of 40 bit keys. This key length is short enough to make brute-force attacks practical to individuals and organization with fairly modest computing resource. With this reason, to extend the protocol to use larger keys, which we call "128-bit" though this technology uses only 104-bit key, will extend the renders brute-force attacks impossible for even the most resourceful of adversaries given today's technology.

WPA - New Security Technology

WEP provides data confidentiality using a stream cipher called RC4 algorithm. Stream ciphers operate by expanding a secret key (40-bit key). As far as we learn, decryption a message consists of generating the identical keystream based on the initialization vector (IV) and secret key and XORing it with the ciphertext. However WEP has been shown to have some flaws which lead to a number of system break-ins.

First, a well-known pitfall of ciphertext is that encrypting two messages under the same IV can reveal information about both messages. In other word, XORing the two ciphertexts together causes the keystream to cancel out and the result is the XOR of the two plaintexts ($P1 \oplus P2$). As it shows below (. is a symbol for XOR).

$$C1 = P1 \oplus RC4(v,k)$$
$$C2 = P2 \oplus RC4(v,k)$$

Then

$$\begin{aligned} C1 \oplus C2 &= (P1 \oplus RC4(v,k)) \oplus (P2 \oplus RC4(v,k)) \\ &= P1 \oplus P2 \end{aligned}$$

Thus, we can say that the attacks happen when the duplicate keystream of the ciphertexts is used more than once with an intruder has the partial knowledge of some of the plaintext.

The WEP standard also has architectural flaws. The IV field used by WEP is only 24 bits wide, that almost guarantees that the same IV will be reused for multiple messages, so "an implementation that use a random 24-bit IV for each packet will be expected to incur collision after transmitting just 5000 packets, which is only a few minutes of transmission. " [1]

IV is not the only security flaw which WEP choose to ignore; another WEP's chief weakness is the use of a static key to initialize an encryption. Remember about the 40-bit keys for encryption? This 40-bit key is entered manually on the AP (Access Point) and on all clients that communicate with the AP. This key doesn't change unless it is manually entered on all devices. This is a tedious task for a large organization.

After recognizing the security concerns of WEP, Enterasys, Proxim, Symbol Technologies and Microsoft are together brought a solution to the weakness in WEP. The result is the Wi-Fi Protected Access (WPA). WPA improves security and, optionally, allows operation without the need for an authentication server. As Michael Disabato wrote in Business Communications Review as "WPA is a marked improvement over WEP. Using WPA on enterprise WLANs will reduce the need for additional protection mechanisms. Home users will gain increased levels of protection for their networks, and this will be important when those networks are used to connect back to the enterprise." [2]

The goal for developing WPA is
1. A software or firmware upgrade to existing access points and NICs[7]
2. Inexpensive in terms of time and cost to implement
3. Cross-Vendor compatible
4. Suitable for enterprise, small sites, home networks
5. Runs in enterprise mode or pre-shared key (PSK) mode

The Wi-Fi Protected Access will solved the problem of WEP by using TKIP (Temporal key integrity protocol) and 802.1x mechanism. Both will provide dynamic key encryption and mutual authentication for clients. WPA periodically generates a unique key for each client which will protect against packet forgeries.

WPA introduces the new algorithms, called TKIP and a message integrity code (referred to as "Michael") to WEP. TKIP includes extended 48-bit initialization vectors together with associated sequencing rules, per-packet construction, key derivation and distribution function. "TKIP increases the size of the key from 40 to 128 bits and replaces WEP's single static key with keys that are dynamically generated and distributed by the authentication server. "[3] After the server accept client's credential (RADIUS - Remote Access Dial-Up User Service), the server will produce a unique master or "pair-wise" key for that computing session. TKIP distributes this key to client and the Access Point then setup the key management system. It uses the pair-wire key to dynamically generate the unique data encryption key, which then will be used to encrypt every packet that is wirelessly communicated during that user's session. With the 128-bit key, TKIP can randomly generate 500 trillion possible keys that can be used on a given packet. As the result, TKIP replaces WEP with a new encryption algorithm that is stronger than the WEP's. Therefore, this TKIP feature has to combine with the 802.1X standard. The protocol in 802.1x is called EAP encapsulation over LANs.

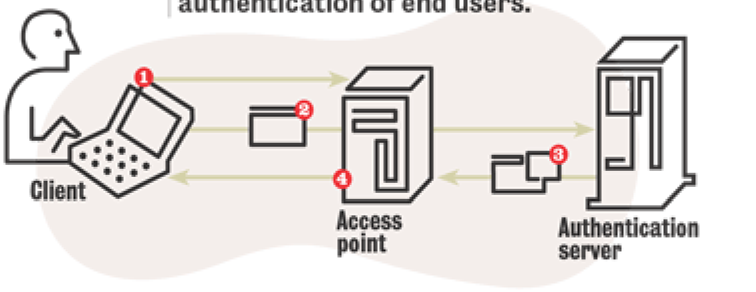
[7] The WPA can be installed on existing hardware via firmware upgrades rather than hardware replacement.

EAP handles the presentation of user's credential in form of digital certificates such as unique usernames and passwords, smart cards, or any other identity credential that the IT administrator is comfortable deploying. With EAP, 802.1X creates a framework, which client workstation mutually authenticates with the authentication server and then passed on those credential to the authentication (RADIUS) server. This mutual authentication prevents users from accidentally connecting to unauthorized APs on the Wi-Fi network and also ensures that users who access the network are the ones whom send the user's credentials to authentication server via the AP. If the server accepts the user's credentials, the matched TKIP key will be sent to both client and the AP. This is a four-way handshake, which the client and AP acknowledge one another and install the keys to complete the process. 802.1X (EAP) is together with TKIP will create a more secure environment for the wireless network.

■ HOW IT WORKS

802.1X Authentication

802.1X authentication for wireless LANs provides centralized, server-based authentication of end users.



1 A client sends a "start" message to an access point, which requests the identity of the client.

2 The client replies with a response packet containing an identity, and the access point forwards the packet to an authentication server.

3 The authentication server sends an "accept" packet to the access point.

4 The access point places the client port in authorized state, and traffic is allowed to proceed.

TKIP also provides the followings facilities: [4]

- The verification of the security configuration after the encryption keys are determined.
- The synchronized changing of the unicast encryption key for each frame.
- The determination of a unique starting unicast encryption key for each preshared key authentication.

For users at homes or small offices (SOHO environments), who might lack the budget for install RADIUS (as we known that it's used for client prove of credential). WPA offers these users with the benefits of WPA security through the use of a "preshared key" (PSK) or password. This PSK will still provide user with the same strong TKIP encryption, and key management. The different will be a password, which will need to manually enter on client devices and on the AP. This password will then also use for authentication - encrypt the packet per packet key construction and key management.

The second added feature in WPA is MIC, which stands for the Message Integrity Check. "The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, the data is assumed to have been tampered with and the packet is dropped." [3]

Sometime we call MIC, as Michael for WPA. Michael specifies a new algorithm that calculates using 8-byte Massage Integrity Check. The MIC will be placed between the data portion of the IEEE message frame.

WPA has optional of replacement WEP encryption with the use of Advanced Encryption Standard (AES)[8]. This type of WPA, we call WPA2. AES has already been adopted as an official government standard by the U.S. Department of Commerce and the National Institute of Standards and Technology (NIST). NIST selected Rijndael as the proposed AES algorithm at the end of a very long and complex evaluation process. This algorithm is designed by Joan Daemen and Vincent Rijmen. At a minimum, the AES algorithm would have to implement symmetric key cryptography as a block and support a block size of 128 bits and key sizes of 128, 192, and 256 bits. This means that there are approximately: 3.4 x 10_{38} possible 128-bit keys, 6.2 x 10_{57} possible 192-bit keys; and 1.1 x 10_{77} possible 256-bit keys. AES will be defined in counter cipher-block chaining mode (CCM)[9] and will support the Independent Basic Service Set (IBSS) to enable security between client workstations operating in ad hoc mode. AES doesn't support through a firmware update to existing wireless equipment because of the need for higher performing processors.

The different between WEP and WPA shows as the table below

	WEP	**WPA**
Encryption	Flawed, cracked by scientist and hacker	Fixed all WEP flaws
	40-bit keys	128-bit keys
	Static-same key used by everyone on the network	Dynamic session keys. Per user per session, per packet keys
	Manual distribution of keys – hand typed into each device	Automatic distribution of keys
Authentication	Flawed, user WEP key itself to authentication	Strong user authentication utilizing 802.1X and EAP

[8] To learn more about AES encryption, visit http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael-ammended.pdf

[9] CCM is a conventional authenticated-encryption scheme obtained from a 128-bit block cipher. The mechanism has been adopted as the mandatory encryption algorithm in an IEEE 802.11 draft standard

By greatly expending the size of keys, the number of keys in use, and by creating an integrity checking mechanism, as the result TKIP magnifies the complexity and difficulty involved in decoding data on a Wi-Fi network.

It seems like WPA fixed all known problems with WEP but there is one issue that WPA forgot to think about that is denial-of-service (Dos) attacks. “Potential Dos attacks are a significant risk for any application where loss of wireless access affects life, profits or reputation. A hacker easily can bring down a WPA protected network by sending at least two packets using the wrong key each second. When this occurs, the access point assumes that a hacker is trying to gain access to the network. The access point shuts off all connection for one minute to avoid the possible compromise of resource on the network. Thus, a continuous string of unauthorized data can keep the network from operating indefinitely, which means you should have a backup-process ready for critical application.” [5]

Although WPA is still not a perfect security for wireless system, Wi-Fi alliance tries to develop the secure scheme to make the wireless system more attractive and secure as we can see from the attempts to develop WPA2 which use the encryption scheme of AES algorithm. This security technology will be released as a new security standard for all Wi-Fi products. WPA as a subset of WPA2 does greatly enhances data protection and access control on existing and future Wi-Fi wireless LANs.

The challenge of Wi-Fi Roaming

Thinking about the ability to working at the airport on a laptop via Wi-Fi hotspot and then continue via cellular network until we can get into out office and switch to a traditional LAN. Roaming is difficult in part because the technologies used in different systems don’t always guarantee that it will work together. And also sometime authentication systems aren’t always compatible.

There are several technical issues involving Wi-Fi roaming.

- Authentication Technology: It would be a difficult thing for users that have to login and logout everytime when they are roaming in different network. If we cannot make this convenience to user then using Wi-Fi network would be less attractive for the future.
- Business related roaming issues: Since different company has distinct ways to provide and charge user for a service, to reach roaming agreement that is satisfy the different in company’s business goal would be a hard decision.

With this reason, five WLAN vendors, counting Symbol, Nomadix, Funk Software, Service Factory and TSI and five WLAN public access service providers, consists of Wayport, Tele2, Wificom, Fatport and Open Point Networks, have established the WISP Association. The association will certify its members by providing a single global service mark, called Pass-One, which WISP members will be able to user as a recognition toll for the end-users, as the same idea as credit card industry.

Conclusion

Wi-Fi brings user with the new convince, so I am not surprise if in the near future we will see people is searching Internet while they are taking a bus or we will see public computers for searching Internet in every the street corner as we have the public telephones. Wi-Fi technology is being developed to have more secure, reliability and convenience. A lot of companies forecast the great profit from Wi-Fi industry, so developing technology for Wi-Fi will also be more standardize and global wide.

References

[1] Nikita Borisove, Ian Goldberg, and David Wagner. *Intercepting Mobil communication: The insecurity of 802.11* thesis paper, http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

[2] C. Michael Disabato, *Wi-Fi Protected Access Finally Arrives*, Business Communications Review, pp. 42–46, May 2003.

[3] White Paper, Wi-Fi Alliance, Wi-Fi Protected Access: Strong, standards*based, interoperable security for today's*

[4] Microsoft Knowledge Base Article – 815485: *Overview of the WPA Wireless Security Update in Windows XP,* http://support.microsoft.com

[5] Jim Geier*, WPA plugs holes in WEP*, Network World, March 31st, 2003

[6] Steven J. Vaughan-Nicholos, *The challenge of Wi-Fi Roaming*, Technology News, July 2003.

[7] White Paper, *Wi-Fi is everywhere!*, June 11th, 2003.

[8] Gateway Computer – Wireless Center, *Why Go Wireless?*, http://www.gateway.com/work/products/wireless

[9] E-business Strategies, *802.11b/WiFi and Bluetooth*, http://www.ebstrategy.com/books/M-business

[10] Intel.com, *Wireless LAN Configuration* http://www.intel.com/business/bss/swapps/wireless/solutions