# WIRELESS ACCESS CONTROL

LEE TECK PING

A report submitted in partial fulfilment
of the requirements for the award
of the degree of
Bachelor of Computer Science (Computer Systems & Network)

Faculty of Computer Systems & Software Engineering
University College of Engineering & Technology Malaysia

DECEMBER, 2005

## ABSTRACT

Wireless, a technology introduced to replace the wired connection is widely used in today's work and industry segment. However, in wireless technology, user from outside are allowed to access the internet and private network in a wireless network area, as they are not authenticated. Here, The WachSpot system, a prototype developed to controlling the wireless user's access by using the login authentication technique and a small wireless hotspot architecture created for the implementation of the prototype. HTML and PHP programming languages have been chosen to design the system while Microsoft Access for storing the user data. A study has been conducted on types of access points, IP address and architecture that are suitable for WachSpot implementation. In order to make the development of system completed, planning has been prepared, the data collected, software and hardware requirements needed were analyzed to come out with the use case model and system architecture consist of user, access point and access server only. All interfaces have been generated by using the HTML and PHP while the implementation of system has been completed before the prototype is tested. The success of implementation and development of this project is expected to increase the security in wireless network by requiring the user to register a new account and login through the system to access the internet.

# ABSTRAK

Teknologi tanpa wayar yang diperkenalkan untuk menggantikan penggunaan teknologi wayar telah meluas digunakan dalam kerja dan bahagain industri hari ini. Akan tetapi, dalam teknologi tanpa wayar, seseorang pengguna dari luar kawasan berhak untuk melayari internet serta rangkaian dalaman kawasan rangkaian tanpa wayar tanpa pengesahan dilakukan terhadap mereka. Di sini, sistem WachSpot, prototaip telah dibangunkan untuk mengawal pencapaian pengguna tanpa wayar dengan menggunakan teknik pengesahan kemasukan dan reka bentuk hotspot tanpa wayar telah dibina untuk perlaksanaan prototaip ini. Bahasa HTML dan PHP telah dipilih untuk mereka bentuk sistem tersebut manakala Microsoft Access untuk penyimpanan maklumat pengguna. Pembelajaran telah dibuat ke atas jenis-jenis access point, alamat IP serta reka bentuk yang sesuai untuk membangunkan WachSpot. Untuk memastikan pembangunan projek berjalan lancar, persediaan projek telah dilaksanakan dan maklumat tentang perisian serta alatan telah dianalisa untuk menghasilkan model use case dan reka bentuk sistem yang merangkumi pengguna, access point serta komputer pengesahan sahaja. Semua reka bentuk sistem dibina menggunakan HTML dan PHP sementara perlaksanaan disiapkan dulu sebelum pengujian prototaip dijalankan. Daripada projek ini, diharap ia dapat meningkatkan keselamatan dalam rangkaian tanpa wayar dengan keprluan pengguna untuk mendaftar dan masuk ke internet melalui sistem ini.

# TABLE OF CONTENTS


| CHAPTER | TITLE | PAGE |
|---|---|---|
| TITLE PAGE | | i |
| DECLARATION | | ii |
| DEDICATION | | iii |
| ACKNOWLEDGEMENT | | iv |
| ABSTRACT | | v |
| ABSTRAK | | vi |
| TABLE OF CONTENTS | | vii |
| LIST OF TABLES | | x |
| LIST OF FIGURES | | xi |
| LIST OF ABBREVIATIONS | | xiii |
| LIST OF APPENDICES | | xv |
| 1 | INTRODUCTION | 1 |
| | 1.1 Introduction | 1 |
| | 1.2 Problem Statement | 2 |
| | 1.3 Objectives | 2 |
| | 1.4 Scopes | 2 |
| | 1.5 Organization of the Report | 3 |
| 2 | LITERATURE REVIEW | 4 |
| | 2.1 Introduction | 4 |
| | 2.2 Wireless Access Point | 4 |
| | 2.2.1 AVAYA Wireless Access Point-AP3 | 6 |

2.2.2 Cisco Aironet Access Points 6

2.2.3 D-LINK DWL-1000 AP+ Access Point 7

2.3 IP Addresses 7

2.3.1 Static versus Dynamic IP Addresses 8

2.4 Network Address Translation 9

2.5 802.11 Standard Basic 11

2.5.1 802.11b 12

2.5.2 802.11a 12

2.5.3 802.11g 13

2.6 Hotspot 13

2.6.1 Hotspot Architecture 14

2.6.1.1 Small Hotspot 15

2.6.1.2 Medium-sized Hotspot 16

**3 METHODOLOGY** 18

3.1 Introduction 18

3.2 Project Planning 19

3.3 Analysis 19

3.3.1 Software Requirements 20

3.3.2 Hardware Requirements 20

3.3.2.1 Wireless Access Point 20

3.3.2.2 Communication Media 21

3.3.2.3 Server 21

3.4 System Design 22

3.4.1 Use-case Diagram 22

3.4.2 System Overview 25

3.4.2.1 Wireless User 26

3.4.2.2 Wireless Access Point 26

3.4.2.3 Access Server 26

3.4.3 Interface Design 27

3.4.3.1 Login Form 27

3.4.3.2 Sign Up 28

3.4.3.3 Change Password 29

| | | | |
|---|---|---|---|
| | | 3.4.3.4 User Information | 30 |
| | 3.5 | Implementation | 30 |
| | | 3.5.1 Server Configuration | 31 |
| | | 3.5.2 Get the Login Page | 31 |
| | | 3.5.3 Flow of the System | 32 |
| | 3.6 | Testing | 33 |
| **4** | **RESULT AND DISCUSSION** | | 36 |
| | 4.1 | Introduction | 36 |
| | 4.2 | Results | 36 |
| | | 4.2.1 Valid User | 36 |
| | | 4.2.2 New User | 40 |
| | | 4.2.3 User Log Information | 40 |
| | 4.3 | Discussion | 41 |
| | 4.4 | Constraints | 42 |
| | 4.5 | Assumption and Further Research | 42 |
| **5** | **CONCLUSION** | | 44 |
| **REFERENCES** | | | 45 |
| **APPENDICES A – C** | | | 48 - 73 |

# LIST OF TABLES


| TABLE NO | TITLE | PAGE |
|---|---|---|
| 2.1 | Types of access points | 5 |
| 2.2 | Differences between static and dynamic IP addresses | 9 |
| 2.3 | Summarizes of 802.11b, 802.11a and 802.11g | 13 |
| 3.1 | Minimum requirements for server | 21 |
| 3.2 | User information | 30 |

# LIST OF FIGURES


| FIGURE NO | TITLE | PAGE |
|---|---|---|
| 2.1 | Wireless access point | 4 |
| 2.2 | Location of NAT | 9 |
| 2.3 | Small hotspot network topology | 15 |
| 2.4 | Medium-sized wireless network | 17 |
| 3.1 | Phases involved in the development of WachSpot | 18 |
| 3.2 | Use-case diagram of WachSpot system | 22 |
| 3.3 | Sequence diagram login (User) | 23 |
| 3.4 | Sequence diagram logout (User) | 23 |
| 3.5 | Sequence diagram login, view user and logout (admin) | 24 |
| 3.6 | Overview of WachSpot system | 25 |
| 3.7 | Interface design for login form | 27 |
| 3.8 | Pseudo-code behind submit button (login form) | 27 |
| 3.9 | Sign up form | 28 |
| 3.10 | Pseudo-code behind submit button (sign up form) | 28 |
| 3.11 | Change password form | 29 |
| 3.12 | Pseudo-code behind submit button (change password form) | 29 |
| 3.13 | Diagram of hardware setup | 31 |
| 3.14 | Flow of the WachSpot system for login page | 33 |
| 3.15 | Testing for invalid username and password | 34 |
| 3.16 | Testing of empty account sign up form | 35 |
| 3.17 | Testing of username has chosen | 35 |
| 4.1 | User input | 37 |
| 4.2 | Redirect page and info box | 37 |
| 4.3 | User default page and info Box | 38 |
| 4.4 | Change password | 39 |

| | | |
|---|---|---|
| 4.5 | Logout | 39 |
| 4.6 | Create new account | 40 |
| 4.7 | User log | 41 |

## LIST OF ABBREVIATIONS

| | | |
|---|---|---|
| AAA | - | Authentication, Authorization and Accounting |
| AP | - | Access Point |
| ADSL | - | Asymmetric Digital Subscriber Line |
| CAT5 | - | Category 5 |
| CPU | - | Computer Processing Unit |
| DHCP | - | Dynamic Host Configuration Protocol |
| DNS | - | Domain Name Service |
| DSL | - | Digital Subscriber Line |
| DSSS | - | Direct Sequence Spread Spectrum |
| FHSS | - | Frequency Hoping Spread Spectrum |
| HTML | - | HyperText Markup Language |
| HTTP | - | HyperText Transfer Protocol |
| IEEE | - | Institute of Electrical and Electronics Engineers |
| IOS | - | Internetwork Operating System |
| IP | - | Internet Protocol |
| IPSec | - | Internet Protocol Security |
| ISDN | - | Integrated Services Digital Network |
| ISP | - | Internet Service Provider |
| L2TP | - | Level Two Tunnelling Protocol |
| LAN | - | Local Area Network |
| MAC | - | Media Access Control |
| NAT | - | Network Address Translation |
| NAPT | - | Network Address Port Translator |
| NIC | - | Network Interface Card |
| PAT | - | Port Address Translation |
| PC | - | Personal Computer |

| | | |
|---|---|---|
| PCM/CIA | - | Personal Computer Memory Card International Association |
| PDA | - | Personal Digital Assistant |
| PHP | - | Hypertext Preprocessor |
| PPPoE | - | Point to Point Protocol over Ethernet |
| PPTP | - | Point-to-Point Tunnelling Protocol |
| QoS | - | Quality of Service |
| RADIUS | - | Remote Access Dial-In User Service |
| SDLC | - | Software Development Life Cycle |
| SST | - | Shiva Smart Tunnelling |
| TCP | - | Transmission Control Protocol |
| UDP | - | User Datagram Protocol |
| USB | - | Universal Serial Bus |
| UTP | - | Unshielded Twisted Pair |
| VLAN | - | Virtual Local Area Network |
| VPN | - | Virtual Private Network |
| WAN | - | Wide Area Network |
| WEP | - | Wired Equivalent Privacy |
| Wi-Fi | - | Wireless Fidelity |
| WISP | - | Wireless Internet Service Provider |
| WLAN | - | Wireless Local Area Network |

# LIST OF APPENDICES


| APPENDIX | TITLE | PAGE |
|---|---|---|
| A | Gantt Chart for Project Development Plan | 49 |
| B1 | Avaya Wireless AP-3 - Wireless access point | 53 |
| B2 | DWL-1000AP+ AirPremier Enterprise 2.4GHz Wireless AP | 55 |
| B3 | CISCO Aironet 1200 Series Access Points | 57 |
| B4 | LevelOne 11g Broadband Router (WBR-3406TX) | 63 |
| C | User Manual for WachSpot | 65 |

# CHAPTER 1

# INTRODUCTION

## 1.1 Introduction

Wireless Local Area Networks (WLANs), technology that were designed to replace wired LAN connection are now increasing in popularity. The early research by Motorola in middle 80's, showed that the wired connection LANs cost were becoming exorbitant, especially in large office building. Wireless LANs have introduced frequently used in enterprise network. WLAN gives the functionality of traditional wired infrastructure but with more flexibility. Users enjoy the freedom of being able to use laptop anywhere in campus or building (Liska, 2003 pg179) to access to internet.

Generally, 802.11 is the standard for WLAN connection, as defined by IEEE. The 802.11 specification only defines the physical layer and MAC address portion of wireless Ethernet (Liska, 2003 pg179). Although wireless is convenient to use and minimizes the need for expensive wired connection, wireless has inherent security risks such as spoofing and denial of service.

Any user who has laptop with wireless card is able to enjoy the usage of internet as long as they can get the signal from access point. However, there will a security issue in which attacker can easily gain access to the private network. Therefore, a prototype, Wireless Access Control (WachSpot) is developed to control the access of wireless user in a small wireless network.

## 1.2 Problem Statement

Without the development of the system, some security risks will occur. For example:

i. Any outside user can access to the private network and public network at any location of the wireless area as long as they have the wireless PCM/CIA or USB wireless card installed on the laptop and can get the signal from the access point. Once they get the IP address distributed by the access point, they are allowed to access the internet without any requirement for registration or payment for the internet services.

ii. The network in a wireless LAN is not in secure mechanism since all the wireless user are not auhenticated before they can access to the internet.

## 1.3 Objective

The objectives of this project are

i. To develop a prototype for controlling the wireless LAN user access where wireless user are authenticated and authorized through a login page and before being allowed to access the internet.

ii. Creating and implementing a small wireless hotspot.

## 1.4 Scope

The scope of this project are:

i. Only develop an access control for small wireless LAN network with capacity of 30 users using login authentication method.

ii. HMTL and PHP are used for code generation and Microsoft Access as the database management system.

iii. The prototype developed is focused on the user authentication before users can access the internet and database is used for store user registration and user log information only.

## 1.5 Organization of the Report

The first chapter of this report provides the introduction to the prototype developed. With the problems occurred in previous system and technologies, the objective and scope for the system is well defined in the chapter.

In chapter two, the background information that related to development of this project is studied and discussed. A studied is conducted on types of wireless access point's technologies, IP addresses, Network Address Translation (NAT), wireless 802.11 standards and wireless Hotspot network architecture.

Chapter three explains the method chosen to use as a guideline in the development of the system. The phases in developing and implementing system are project planning and requirements analysis, system design, implementation and testing of the prototype.

The results or outputs from the testing of the prototype are presented in the chapter four. The strengths and limitations of the system are discussed as well as with the further research technique to enhance the prototype system.

Finally, chapter five summarizes the report of the WachSpot system.

# CHAPTER 2

# LITERATURE REVIEW

## 2.1 Introduction

In the process to develop a prototype for controlling wireless user access, a research and study on wireless technologies and hotspot has been done. All the terms and approaches related are defined and discuss in this chapter. Wireless access point, TCP/IP standard, types of Wireless LAN to be created, IP addresses, hotspot architecture and several types of software and hardware approaches is discuss in next section.

## 2.2 Wireless Access Point

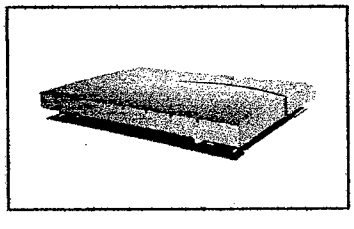

**Figure 2.1:** Wireless Access Point

Wireless access points, technologies that refer to 802.11 standards are specially configured devices on wireless LAN that connect wireless communication devices together to create wireless network (Wikipedia, 2005). Figure 2.1 shows the example of access point used in today where it can acts as a connection point

between wireless and wired network. Access points used in home and small businesses are generally small devices with featuring network adapter and antenna as its support for Wi-Fi wireless communication standards also (Mitchell, 2005). Multiple access points can be connected to a wired LAN, providing continuous network connectivity in a campus or offices. There are two types of access point's hardware and integrated access point (Allen Comp, 2005). The description of both access points are shown in the table below.

**Table 2.1:** Types of access points

| **Types of access point** | **Hardware** | **Integrated** |
|---|---|---|
| **Description** | Use as an extension of an existing wired network and provide additional access in remote areas. | Provide the features of a router and are connected to a high-speed connection such as DSL or cable modem. Generally, both wired and wireless access is provided in one unit. |
| **Example** | 3Com AirConnect | Integrated PPPoE |

For a simple wireless network, a single access point can serve only 10 users but many newer access points can support up to 255 users (Mitchell, 2005). However, when there are more computers connected to the access point, the network performance, reliability and efficiency of accessing the network will slow down as the bandwidth of access point is decrease as well. Several categories of wireless access point that are studied and discuss are AVAYA AP-3, Cisco Aironet and D-LINK access points. A brief description of each types of access point is discussed while the features and specifications are show as in the Appendix B.

### 2.2.1 AVAYA Wireless Access Point-AP3

The AP-3 Wireless Access Point extends the range of wired Ethernet networks. Its dual slot architecture provides both 11 Mbps and/or 54 Mbps connectivity to wireless user, making it an ideal solution for enterprise used. The flexibility of upgrade the software by changing the wireless cards to make the past investments could be protected by using high performance, 2.4 GHz 802.11b wireless card.

Besides deliver great performance, AP-3 also provides security capabilities to make sure the confidentiality of all wireless transmissions. The AP-3 supports a list of standard-based security, such as Wired Equivalent Privacy (WEP), RADIUS authentication, dynamic key exchange and MAC-based access control lists. The integrated network management capability of wireless AP-3 makes it easily to embed into medium or large enterprises (Avaya, 2004).

### 2.2.2 Cisco Aironet Access Points

Cisco system enables wireless LAN clients to meet varying technical and business needs with the Cisco Aironet 1100 and 1200 series access points. Both series are based on Cisco IOS Software and offer key features that extend intelligent networking features to the wireless LAN including:

i. VLAN support – with the VLAN support, traffic on network can be segmented and differentiated services can be offered to different user groups.
ii. QoS support – User can provide QoS for high-priority traffic, example voice and video.
iii. Proxy mobile IP support – allow roaming between subnets without losing connectivity (Cisco, 2002).

### 2.2.3 D-LINK DWL-1000 AP+ Access Point

D-Link AirPremier™ DWL-1000AP+ access point is a enterprise access point that introduced to wireless connectivity in which has capability of data transfer rate up to 22 Mbps with 802.1x support to increase wireless security. There are five modes that DWL-1000AP+ can be configure to perform as wireless access point, point-to-point bridge with another AP, point-to-multipoint wireless bridge, wireless client or wireless repeater.

While in access point mode, load-balancing feature is offered to maximize the wireless bandwidth available to wireless users by sharing the load between groups of access points. Additionally, redundancy feature along with 802.1x support is provided to allow access point to be configured to backup a primary access point. Those features make the access point is a best solution for wireless hotspot deployment, create and extending wireless LAN in offices and workplaces. Compatibility with the IEEE 802.11b standard makes DWL-1000AP+ is interoperable with all existing 802.11b devices (D-Link Corporation, 2005).

## 2.3 IP Addresses

Internet Protocol (IP) address is 32-bit number identifier assigned for each device on a TCP/IP network. When an e-mail is send, Internet Protocol of TCP/IP includes the IP address in the delivered message to destination e-mail address. At the other end, the recipient can see IP address of the e-mail sender and responded message is send using IP address received. IP address consists of four numbers separate by period called "dotted-quad" and each number could be zero to 255 (WhatIsMyIPAddress.com, 2005). For example, 150.0.0.1 could be an IP address. The four numbers in an IP address are used in different ways to identify a particular network and a host on that network.

In term of network, Internet Protocol (IP) is basically the set of rules for communications between networks (Steve, 2005). Each network must know its own address on the internet. Within an isolated network, IP addresses can assign randomly as long as each one is unique. However, registered IP addresses are required when connecting a private network to the Internet to avoid any duplicates.

TCP/IP routing views IP address as two parts: a network part and a host part. The network part of the address identifies the network the machine is connected to while the rest of the address on host part defines particular machine on that network (Mansfield, 2003). The size of the network and host parts depends on the class of the address, and is determined by address network mask. The network mask is a binary mask with 1s in the network part of the address, and 0 in the host part.

The various size of network comes out with five different address classes to consider. The class A network is use for large many devices such as major international company. There are 126 network with 16 million hosts is support on class A. Class B address is used for medium sized network, college campus and large offices and supports up to 65,000 hosts. But class C addresses are commonly use for small networks with fewer than 256 devices. This class only support for 254 hosts on each network. Other classes such as class D is use for multicast addresses and class E addresses for experimental purpose only.

### 2.3.1 Static versus Dynamic IP Addresses

In many nowadays corporate networks and online services, dynamic IP addresses is use using DHCP rather than static with increased usage of internet. A wireless user would communicate with the internet by using static or dynamic IP addresses. The differences between static and dynamic IP addresses are shown in the Table 2.2.

**Table 2.2:** Differences between static and dynamic IP addresses

| Types of IP | Static | Dynamic |
|---|---|---|
| Description | Permanent address on the internet assigned by network administrator or Internet Service Provider (ISP). | Temporary address assign by a DHCP server that maintains and assigns a pool of IP addresses. |
| Change of IP | IP addresses are reserved and don't change over time. | IP address changes each time a user connect to the network. |
| Function | One IP address is issue to each user and provide limited number of IP addresses | Provide economize on the remaining number of IP addresses over the internet. |
| Range of usage | Suitable for commercial leased lines and servers so that the same address can always be reached. | Use by residential internet connection, whether broadband or dialup user who does not run servers. |

## 2.4 Network Address Translation

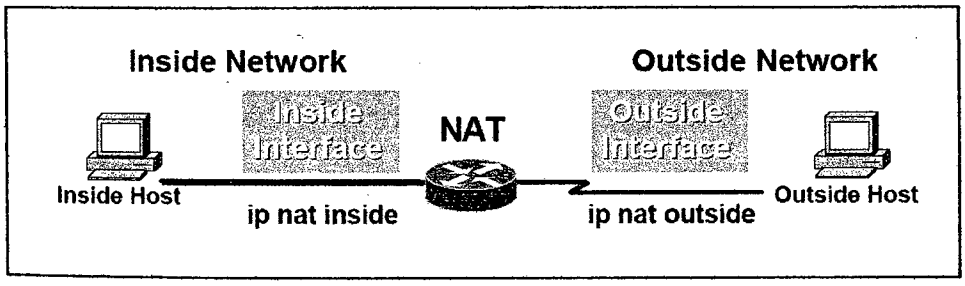


**Figure 2.2:** Location of NAT (Cisco, 2001)

Network Address Translation (NAT) is a method of connecting multiple computers to the internet using one IP address. As shown in the Figure 2.2, interface on the router are divide into inside and outside interface. NAT is the device on the

router that translates the Internet Protocol (IP) address used within inside interface to a different IP address known within outside interface or vice versa but never happens between the same types of interface (Cisco, 2001). World shortage of IP addresses, security needs and ease and flexibility of network administration have make movement towards increase use of NAT (Egevang, 1994). NATs are nowadays used between the home, small office LAN and WLAN and the Internet.

There are two different variations of NAT, basic NAT and NAPT. Translation of basic NAT on IP address only whereas NAPT translate both the IP address and TCP/UDP port into a single network and new port numbers (Lucenius, 2004). In a network, NAT is included as part of router and often as part of corporate firewall. NAT table is created to do global-to-local and local-to-global IP address mapping. NAT can also be used in conjunction with policy routing. NAT can be statically defined or it can be set up to dynamically translate from and to a pool of IP addresses.

Benefits that provided by NAT gateways are:

i. Firewall protection for internal network which allow only specifically designated servers with accessible from the internet. Internal network security is enhanced since the assigned addresses to wireless users are hidden from outside world.
ii. Automatic client computer configuration control
iii. Packet level filtering and routing.
iv. Typically, organizations that change service providers are not allowed to re-addressing. NAT eliminate the cost for the need of host renumbering by allowing re-addressing to occur at the gateway, allowing time to convert internal hosts to the new network number.
v. NAT replaces the source address with a routable address and enables privately addressed hosts to access registered networks, such as the Internet, without requiring globally unique IP addresses on end hosts.

Network Address Translation that is used by firewall, router and computers is sits between an internal network and the outside WAN. NAT has many forms and can work in several ways:

i. Static NAT - Mapping an unregistered IP address to a registered IP address on a one-to-one basis. Particularly useful when a device needs to be accessible from outside the network.

ii. Dynamic NAT - Maps an unregistered IP address to a registered IP address from a group of registered IP addresses.

iii. Overloading - A form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address by using different ports. This is known also as PAT (Port Address Translation), single address NAT or port-level multiplexed NAT.

iv. Overlapping - When the IP addresses used on your internal network are registered IP addresses in use on another network, the router must maintain a lookup table of these addresses so that it can intercept them and replace them with registered unique IP addresses. It is important to note that the NAT router must translate the "internal" addresses to registered unique addresses as well as translate the "external" registered addresses to addresses that are unique to the private network. This can be done either through static NAT or by using DNS and implementing dynamic NAT.

## 2.5 802.11 Standard Basic

*If any one technology has emerged in the past few years that will be explosive in its impact, it's 802.11* [Gates, 2002]

The 802.11 is one of the earliest WLAN standard defined in 1997 by the Institute of Electrical and Electronics Engineers (IEEE). As mentioned by Bill Gates, the 802.11 technology has emerged in the past few years. The standard specifies infrared, Frequency Hoping Spread Spectrum Radio (FHSS) and Direct Sequence Spread Spectrum Radio (DSSS) physical layer operations at either 1 or 2 Mbps with 2.4 GHz frequency to transmit data (Arun, 2001). As the maximum bandwidth supported by 802.11 was too slow for many applications, the ordinary

802.11 wireless product was not longer being manufactured. There are three newer and faster physical layer standard introduced to address some of the problems in 802.11: 802.11b, 802.11a and 802.11g. Detail descriptions of each standard are provided in next section and the summary of these standards are shown in Table 2.3.

### 2.5.1 802.11b

802.11b, the most popular and widely use standard, is the extension to the original 802.11 standard and is approved to create a standards-based technology that could span multiple physical encoding types. The approval allowed the standard to support up to 22 Mbps bandwidth. The 802.11b standard, also known as WiFi, Wireless Fidelity is designed to have a transmission range of about 30 to 100 meters and operate in the 2.4 GHz frequency using DSSS (Direct Sequence Spread Spectrum) technology (Albert, 2002). 802.11b is a best solution to implement a wireless network in which the cost is fewer with more signal range. A laptop fitted with PCM/CIA or USB wireless card that connects via the air to an access point can be connected to corporate network at speed of 11 Mbps.

### 2.5.2 802.11a

Although the 802.11a standard was ratified in 1999, products based on the standard did not begin shipping in volume until 2002. Unlike the 802.11b standard, devices that support the 802.11a standard operate in the 5 GHz frequency range (Liska, 2003). The standard support higher data rates up to 54 Mbps per channel as for commercial and industry usage purposes. With higher frequency, the range of 802.11a is limited and the signals have difficulty penetrating walls and other obstructions. So, 802.11a devices are not compatible with wireless LAN devices that operate at 2.4 GHz frequency range. Although cost to implement 802.11a is the highest with shorter range signal but it provides higher data throughput, greater